paloalto TECHDOCS

# PAN-OS® 관리자 가이드

Version 10.2



docs.paloaltonetworks.com

## Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

## About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

## Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2021-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

June 6, 2022

# Table of Contents


시작하기 ..... 21
- 방화벽을 관리 네트워크에 통합 ..... 22
  - 비즈니스 연속성을 위한 액세스 전략 결정 ..... 22
  - 관리 전략 결정 ..... 23
  - 초기 구성 수행 ..... 23
  - 외부 서비스에 대한 네트워크 액세스 설정 ..... 30
- 방화벽 등록 ..... 37
  - 새 지원 계정 생성 및 방화벽 등록 ..... 37
  - 방화벽 등록 ..... 39
  - (선택 사항) Day 1 구성 수행 ..... 42
  - 방화벽 라인 카드 등록 ..... 45
- 인터페이스 및 영역을 사용하여 네트워크 분할 ..... 46
  - 공격 표면 감소에 대한 네트워크 세분화 ..... 46
  - 인터페이스 및 영역 구성 ..... 46
- 기본 보안 정책 설정 ..... 51
- 네트워크 트래픽 평가 ..... 56
- 무료 WildFire 포워딩 가능 ..... 58
- 방화벽 배포를 완료하기 위한 모범 사례 ..... 61

구독 ..... 63
- 방화벽과 함께 사용할 수 있는 구독 ..... 64
- 구독 라이선스 활성화 ..... 68
- 라이선스가 만료되면 어떻게 되나요? ..... 70
- Palo Alto Networks 클라우드 서비스를 위한 향상된 애플리케이션 로그 ..... 73
  - Cortex XDR ..... 73
  - IoT 보안 ..... 75

방화벽 관리 ..... 79
- 관리 인터페이스 ..... 80
- 웹 인터페이스 사용 ..... 81
  - 웹 인터페이스 실행 ..... 81
  - 배너, 오늘의 메시지 및 로고 구성 ..... 82
  - 관리자 로그인 활동 표시기를 사용하여 계정 오용 감지 ..... 84
  - 관리 작업 관리 및 모니터링 ..... 86
  - 방화벽 구성 변경 사항 커밋, 유효성 검사 및 미리 보기 ..... 87
  - 선택적 구성 변경 커밋 ..... 89
  - 구성 테이블 데이터 내보내기 ..... 90



©2023 Palo Alto Networks, Inc.

전역 찾기를 사용하여 방화벽 또는 Panorama 관리 서버 검색 ..... 91
구성 변경을 제한하기 위한 잠금 관리 ..... 93
구성 백업 관리 ..... 95
방화벽 구성 저장 및 내보내기 ..... 95
방화벽 구성 변경 사항 되돌리기 ..... 96
방화벽 관리자 관리 ..... 99
관리 역할 유형 ..... 99
관리자 역할 프로파일 구성 ..... 100
관리 인증 ..... 107
관리 계정 및 인증 구성 ..... 108
관리자 활동 추적 구성 ..... 115
참조: 웹 인터페이스 관리자 액세스 ..... 117
웹 인터페이스 액세스 권한 ..... 117
Panorama 웹 인터페이스 액세스 권한 ..... 184
참조: 포트 번호 사용 ..... 189
관리 기능에 사용되는 포트 ..... 189
HA에 사용되는 포트 ..... 190
Panorama에 사용되는 포트 ..... 191
GlobalProtect에 사용되는 포트 ..... 193
사용자 ID에 사용되는 포트 ..... 193
IPsec에 사용되는 포트 ..... 195
라우팅에 사용되는 포트 ..... 195
DHCP에 사용되는 포트 ..... 196
인프라에 사용되는 포트 ..... 196
방화벽을 출하시 기본 설정으로 재설정 ..... 198
방화벽 부트스트랩 ..... 199
USB 플래시 드라이브 지원 ..... 199
샘플 init-cfg.txt 파일 ..... 200
방화벽 부트스트래핑을 위한 USB 플래시 드라이브 준비 ..... 201
USB 플래시 드라이브를 사용하여 방화벽 부트스트랩 ..... 204

**디바이스 원격 측정 ..... 207**

디바이스 원격 분석 개요 ..... 208
디바이스 원격 분석 수집 및 전송 간격 ..... 209
디바이스 원격 분석 관리 ..... 210
디바이스 원격 분석 사용 ..... 210
디바이스 원격 분석 비활성화 ..... 210
디바이스 원격 분석에서 수집하는 데이터 관리 ..... 211
기록 디바이스 원격 분석 관리 ..... 211


 ©2023 Palo Alto Networks, Inc.

디바이스 원격 분석 모니터링 ..... 213
디바이스 원격 분석에서 수집하는 데이터 샘플링 ..... 214

**인증 ..... 215**

인증 유형 ..... 216
외부 인증 서비스 ..... 216
다단계 인증 ..... 216
SAML ..... 217
Kerberos ..... 218
TACACS+ ..... 219
RADIUS ..... 220
LDAP ..... 221
로컬 인증 ..... 221
인증 배포 계획 ..... 223
다단계 인증 구성 ..... 225
RSA SecurID와 방화벽 간의 MFA 구성 ..... 229
Okta와 방화벽 간의 MFA 구성 ..... 238
Duo와 방화벽 간에 MFA 구성 ..... 248
SAML 인증 구성 ..... 258
Kerberos Single Sign-On (SSO) 구성 ..... 263
Kerberos 서버 인증 구성 ..... 266
TACACS+ 인증 구성 ..... 267
RADIUS 인증 구성 ..... 270
LDAP 인증 구성 ..... 274
인증 서버에 대한 연결 타임아웃 ..... 276
인증 서버 타임아웃 설정 지침 ..... 276
PAN-OS 웹 서버 타임아웃 수정 ..... 277
인증 포털 세션 타임아웃 수정 ..... 277
로컬 데이터베이스 인증 구성 ..... 278
인증 프로파일 및 시퀀스 구성 ..... 279
인증 서버 연결 테스트 ..... 283
인증 정책 ..... 285
인증 타임스탬프 ..... 285
인증 정책 구성 ..... 286
인증 문제 해결 ..... 289

**인증서 관리 ..... 291**

키 및 인증서 ..... 292
기본 신뢰할 수 있는 인증서 당국(C) ..... 295

 ©2023 Palo Alto Networks, Inc.

인증서 해지 ..... 296
인증서 해지 목록(CRL) ..... 296
온라인 인증서 상태 프로토콜(OCSP) ..... 297
인증서 배포 ..... 298
인증서 해지 상태에 대한 확인 설정 ..... 299
OCSP 응답자 구성 ..... 299
인증서의 해지 상태 확인 구성 ..... 300
SSL/TLS 복호화에 사용되는 인증서의 해지 상태 확인 구성 ..... 300
마스터 키 구성 ..... 302
마스터 키 암호화 ..... 305
마스터 키 암호화 수준 구성 ..... 306
방화벽 HA 쌍에서 키 암호화 마스터 ..... 307
마스터 키 암호화 로그 ..... 307
AES-256-GCM을 위한 고유한 마스터 키 암호화 ..... 308
인증서 받기 ..... 309
자체 서명된 루트 CA 인증서 생성 ..... 309
인증서 생성 ..... 310
인증서 및 개인 키 가져오기 ..... 311
외부 CA로부터 인증서 받기 ..... 312
디바이스 인증서 설치 ..... 313
SCEP를 사용하여 인증서 배포 ..... 314
인증서 및 개인 키 내보내기 ..... 318
인증서 프로파일 구성 ..... 319
SSL/TLS 서비스 프로파일 구성 ..... 321
SSH 서비스 프로파일 구성 ..... 322
SSH 관리 프로파일 생성 ..... 322
SSH HA 프로파일 생성 ..... 331
인바운드 관리 트래픽에 대한 인증서 교체 ..... 341
SSL 포워딩 프록시 서버 인증서의 키 크기 구성 ..... 342
인증서 취소 및 갱신 ..... 343
인증서 취소 ..... 343
인증서 갱신 ..... 343
하드웨어 보안 모듈을 사용한 보안 키 ..... 344
HSM을 통한 연결 설정 ..... 344
HSM을 사용하여 마스터 키 암호화 ..... 350
HSM에 개인 키 저장 ..... 351
HSM 배포 관리 ..... 352

**고가용성 ..... 353**

 ©2023 Palo Alto Networks, Inc.

HA 개요 ..... 354
HA 컨셉 ..... 355
HA 모드 ..... 355
HA 링크 및 백업 링크 ..... 356
디바이스 우선 순위 및 선점 ..... 363
페일오버 ..... 363
활성/패시브 HA에 대한 LACP 및 LLDP 사전 협상 ..... 364
부동 IP 주소 및 가상 MAC 주소 ..... 365
ARP 로드 공유 ..... 367
경로 기반 중복성 ..... 368
HA 타이머 ..... 369
세션 소유자 ..... 371
세션 설정 ..... 372
활성/활성 HA 모드의 NAT ..... 374
활성/활성 HA 모드의 ECMP ..... 374
활성/패시브 HA 설정 ..... 376
활성/패시브 HA의 전제 조건 ..... 376
활성/패시브 HA에 대한 구성 지침 ..... 377
활성/패시브 HA 구성 ..... 379
HA 페일오버 조건 정의 ..... 386
장애 조치 확인 ..... 389
활성/활성 HA 설정 ..... 390
활성/활성 HA의 전제 조건 ..... 390
활성/활성 HA 구성 ..... 391
활성/활성 사용 사례 확인 ..... 397
HA 클러스터링 개요 ..... 412
HA 클러스터링 모범 사례 및 프로비저닝 ..... 415
HA 클러스터링 구성 ..... 417
HA1 SSH 키 새로 고침 및 키 옵션 구성 ..... 420
HA 방화벽 상태 ..... 429
참조: HA 동기화 ..... 431
활성/수동 HA에서 동기화되지 않는 설정은 무엇입니까? ..... 431
활성/활성 HA에서 동기화되지 않는 설정은 무엇입니까? ..... 433
시스템 런타임 정보의 동기화 ..... 437

**모니터링 ..... 441**

대시보드 사용 ..... 442
애플리케이션 명령 센터 사용 ..... 444
ACC—우선 검토 ..... 444

 ©2023 Palo Alto Networks, Inc.

ACC 탭 ..... 446
ACC 위젯 ..... 448
위젯 설명 ..... 449
ACC 필터 ..... 455
ACC와 상호 작용 ..... 457
사용 사례: ACC - 정보 검색의 경로 ..... 460
앱 범위 보고서 사용 ..... 467
요약 보고서 ..... 467
변경 모니터 보고서 ..... 468
위협 모니터 보고서 ..... 469
위협 지도 보고서 ..... 470
네트워크 모니터 보고서 ..... 471
트래픽 맵 보고서 ..... 472
자동화된 연동 엔진 사용 ..... 474
자동화된 연동 엔진 개념 ..... 474
상관 개체 보기 ..... 475
상관 이벤트 해석 ..... 476
ACC에서 손상된 호스트 위젯 사용 ..... 478
패킷 캡처 가져오기 ..... 479
패킷 캡처 유형 ..... 479
하드웨어 오프로드 비활성화 ..... 480
사용자 지정 패킷 캡처 수행 ..... 480
위협 패킷 캡처 수행 ..... 485
애플리케이션 패킷 캡처 수행 ..... 487
관리 인터페이스에서 패킷 캡처 수행 ..... 490
애플리케이션 및 위협 모니터링 ..... 493
로그 보기 및 관리 ..... 494
로그 유형 및 심각도 수준 ..... 494
로그 보기 ..... 501
필터 로그 ..... 502
로그 내보내기 ..... 503
로그 스토리지 할당량 및 만료 기간 구성 ..... 504
SCP 또는 FTP 서버로 로그 내보내기 예약 ..... 504
차단 목록 모니터링 ..... 506
보고서 보기 및 관리 ..... 507
보고서 유형 ..... 507
보고서 보기 ..... 508
보고서의 만료 기간 및 실행 시간 구성 ..... 509
사전 정의된 보고서 비활성화 ..... 509

 ©2023 Palo Alto Networks, Inc.

맞춤 보고서 ..... 509
사용자 정의 보고서 생성 ..... 512
봇넷 보고서 생성 ..... 515
SaaS 애플리케이션 사용 보고서 생성 ..... 517
PDF 요약 보고서 관리 ..... 520
사용자/그룹 활동 보고서 생성 ..... 522
보고서 그룹 관리 ..... 523
이메일 전송을 위한 보고서 예약 ..... 524
보고서 저장 용량 관리 ..... 525
정책 규칙 사용 보기 ..... 527
모니터링을 위해 외부 서비스 사용 ..... 532
로그 포워딩 구성 ..... 533
이메일 경고 구성 ..... 538
모니터링에 Syslog 사용 ..... 540
Syslog 모니터링 구성 ..... 540
Syslog 필드 설명 ..... 544
SNMP 모니터링 및 트랩 ..... 638
SNMP 지원 ..... 638
SNMP 관리자를 사용하여 MIB 및 개체 탐색 ..... 639
방화벽 보안 네트워크 요소에 대한 SNMP 서비스 활성화 ..... 642
SNMP를 사용하여 통계 모니터링 ..... 642
SNMP 관리자로 트랩 포워딩 ..... 644
지원되는 MIB ..... 646
HTTP/S 대상에 로그 포워딩 ..... 655
NetFlow 모니터링 ..... 658
NetFlow 내보내기 구성 ..... 658
NetFlow 템플릿 ..... 660
SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자 ..... 665
모니터 트랜시버 ..... 668

**User-ID ..... 669**

사용자 ID 개요 ..... 670
사용자 ID 개념 ..... 672
그룹 매핑 ..... 672
사용자 매핑 ..... 672
사용자 ID 사용 ..... 677
사용자를 그룹으로 매핑합니다 ..... 681
사용자에게 IP 주소 매핑 ..... 687
사용자 ID 에이전트에 대한 전용 서비스 계정 생성 ..... 687

 ©2023 Palo Alto Networks, Inc.

Windows 사용자 ID 에이전트를 사용하여 사용자 매핑 구성 ..... 707
PAN-OS 통합 사용자 ID 에이전트를 사용하여 사용자 매핑 구성 ..... 719
WinRM을 사용하여 서버 모니터링 구성 ..... 723
사용자 매핑을 위해 Syslog 발신자를 모니터링하도록 사용자 ID 구성 ..... 731
인증 포털을 사용하여 사용자 이름에 IP 주소 매핑 ..... 742
터미널 서버 사용자를 위한 사용자 매핑 구성 ..... 748
XML API를 사용하여 사용자 매핑을 사용자 ID로 보내기 ..... 757
사용자 및 그룹 기반 정책 활성화 ..... 759
계정이 여러 개인 사용자를 위한 정책 사용 ..... 760
사용자 ID 구성 확인 ..... 762
대규모 네트워크에 사용자 ID 배포 ..... 765
수많은 매핑 정보 소스에 대한 사용자 ID 배포 ..... 765
HTTP 헤더에 사용자 이름 삽입 ..... 769
데이터 및 인증 타임스탬프 재배포 ..... 771
가상 시스템 전체에서 사용자 ID 매핑 공유 ..... 777

**App-ID ..... 781**

App-ID 개요 ..... 782
간소화된 앱 ID 정책 규칙 ..... 783
태그를 사용하여 애플리케이션 필터 생성 ..... 783
사용자 지정 태그를 기반으로 애플리케이션 필터 생성 ..... 784
앱 ID 및 HTTP/2 검사 ..... 786
사용자 지정 또는 알 수 없는 애플리케이션 관리 ..... 788
신규 및 수정된 App-ID 관리 ..... 789
신규 및 수정된 앱-아이디를 가장 잘 통합하는 워크플로 ..... 789
콘텐츠 릴리스에서 신규 앱 및 수정된 앱-아이디 보기 ..... 790
신규 및 수정된 App-ID가 보안 정책에 미치는 영향 보기 ..... 792
중요한 신규 앱-아이디가 허용되도록 보장 ..... 792
신규 앱-아이디 모니터링 ..... 793
앱 ID 사용 안 함 및 사용 ..... 794
정책에 애플리케이션 개체 사용 ..... 796
애플리케이션 그룹 생성 ..... 796
애플리케이션 필터 생성 ..... 797
사용자 지정 애플리케이션 생성 ..... 797
애플리케이션 종속성 해결 ..... 801
기본 포트에서 애플리케이션 안전하게 활성화 ..... 803
암시적 지원이 있는 애플리케이션 ..... 805
보안 정책 규칙 최적화 ..... 809
정책 최적화 프로그램 개념 ..... 810

 ©2023 Palo Alto Networks, Inc.

포트 기반을 앱 ID 기반 보안 정책 규칙으로 마이그레이션 ..... 817
규칙 복제 마이그레이션 사용 사례: 웹 브라우징 및 SSL 트래픽 ..... 824
기존 규칙에 애플리케이션 추가 ..... 827
사용되지 않는 애플리케이션을 사용하여 보안 정책 규칙 식별 ..... 829
애플리케이션 사용 통계에 대한 고가용성 ..... 832
정책 최적화 프로그램을 비활성화하는 방법 ..... 832
App-ID 클라우드 엔진 ..... 834
앱 ID 클라우드 엔진 배포 준비 ..... 836
앱 ID 클라우드 엔진 사용 또는 비활성화 ..... 840
App-ID 클라우드 엔진 처리 및 사용 ..... 840
신규 앱 뷰어(정책 최적화 프로그램) ..... 844
정책 최적화 프로그램을 사용하여 애플리케이션 필터에 앱 추가 ..... 845
정책 최적화 프로그램을 사용하여 애플리케이션에 앱 추가 ..... 848
정책 최적화 프로그램을 사용하여 규칙에 직접 앱 추가 ..... 851
RMA 방화벽(ACE) 교체 ..... 854
라이선스 만료 또는 비활성화 ACE의 영향 ..... 854
클라우드 콘텐츠 롤백으로 인한 커밋 실패 ..... 855
App-ID Cloud Engine 문제 해결 ..... 856
SaaS 앱 ID 정책 추천 ..... 859
SaaS 정책 추천 가져오기 ..... 860
업데이트된 SaaS 정책 권장 사항 가져오기 ..... 862
삭제된 SaaS 정책 권장 사항 제거 ..... 863
애플리케이션 수준 게이트웨이 ..... 864
SIP 애플리케이션 수준 게이트웨이(ALG) 비활성화 ..... 866
HTTP 헤더를 사용하여 SaaS 애플리케이션 액세스 관리 ..... 867
SaaS 사용자 지정 헤더 이해 ..... 867
사전 정의된 SaaS 애플리케이션 유형에 사용되는 도메인 ..... 870
사전 정의된 형식을 사용하여 HTTP 헤더 삽입 항목 생성 ..... 871
사용자 지정 HTTP 헤더 삽입 항목 생성 ..... 872
데이터 센터 애플리케이션에 대한 사용자 지정 타임아웃 유지 ..... 874

**Device-ID ..... 877**

디바이스 ID 개요 ..... 878
디바이스 ID 배포 준비 ..... 882
디바이스 ID 구성 ..... 887
디바이스 ID 관리 ..... 890
디바이스 ID에 대한 CLI 명령 ..... 892

**위협 방지 ..... 895**


 ©2023 Palo Alto Networks, Inc.

위협 방지 정보 ..... 897
고급 위협 방지 ..... 898
레이어 4 및 레이어 7 이베이전으로부터 네트워크를 보호하기 위한 모범 사례 ..... 899
바이러스 백신, Palo Alto Networks 및 취약점 보호 설정 ..... 910
DNS 보안 ..... 913
DNS 보안 정보 ..... 913
클라우드 제공 DNS 서명 및 보호 ..... 914
DNS 보안 분석 ..... 915
DNS 보안 활성화 ..... 918
DNS 보안 데이터 수집 및 로깅 ..... 924
DNS 쿼리를 사용하여 네트워크에서 감염된 호스트 식별 ..... 926
DNS 싱크홀링 작동 방식 ..... 926
DNS 싱크홀링 구성 ..... 927
사용자 지정 도메인 목록에 대한 DNS 싱크홀링 구성 ..... 928
네트워크의 로컬 서버에 대한 싱크홀 IP 주소 구성 ..... 930
악의적인 도메인에 연결하려고 시도한 감염된 호스트 보기 ..... 933
데이터 필터링 ..... 937
데이터 필터링 프로파일 생성 ..... 937
사전 정의된 데이터 필터링 패턴 ..... 940
인라인 클라우드 분석 구성 ..... 943
WildFire Inline ML ..... 948
WildFire Inline ML 구성 ..... 948
파일 차단 설정 ..... 952
무차별 대입 공격 방지 ..... 955
무차별 암호 대입 서명에 대한 작업 및 트리거 조건 사용자 지정 ..... 956
회피 서명 활성화 ..... 960
차단된 IP 주소 모니터링 ..... 961
위협 서명 카테고리 ..... 964
위협 예외 생성 ..... 972
사용자 정의 서명 ..... 974
위협 보고서 모니터링 및 Get ..... 975
위협 카테고리를 기반으로 활동 모니터링 및 맞춤 리포트 생성 ..... 975
위협 서명에 대해 자세히 알아보기 ..... 977
네트워크 트래픽에 대한 AutoFocus 위협 인텔리전스 ..... 980
Palo Alto Networks와 위협 인텔리전스 공유 ..... 986
위협 예방 리소스 ..... 987

**복호화 ..... 989**

복호화 개요 ..... 990

 ©2023 Palo Alto Networks, Inc.

복호화 개념 ..... 992
복호화 정책용 키 및 인증서 ..... 992
SSL 포워드 프록시 ..... 994
SSL 포워드 프록시 복호화 프로파일 ..... 996
SSL 인바운드 검사 ..... 998
SSL 인바운드 검사 복호화 프로파일 ..... 1001
SSL 프로토콜 설정 복호화 프로파일 ..... 1002
SSH 프록시 ..... 1004
SSH 프록시 복호화 프로파일 ..... 1006
비복호화 프로파일 ..... 1007
ECC(타원 곡선 암호화) 인증서에 대한 SSL 복호화 ..... 1009
SSL 복호화를 위한 PFS(완전한 순방향 보안) 지원 ..... 1009
SSL 복호화 및 주체 대체 이름(SAN) ..... 1010
TLSv1.3 복호화 ..... 1010
암호 해독된 세션에 대해 고가용성이 지원되지 않음 ..... 1013
복호화 미러링 ..... 1013
복호화 배포 준비 ..... 1014
이해 관계자와 협력하여 복호화 배포 전략 개발 ..... 1014
PKI 롤아웃 계획 개발 ..... 1016
복호화 방화벽 배포 크기 조정 ..... 1017
단계적으로 우선 순위가 지정된 배포 계획 ..... 1019
해독할 트래픽 정의 ..... 1021
복호화 프로파일 생성 ..... 1022
복호화 정책 규칙 생성 ..... 1025
SSL 포워드 프록시 구성 ..... 1029
SSL 인바운드 검사 구성 ..... 1034
SSH 프록시 구성 ..... 1039
복호화되지 않은 트래픽에 대한 서버 인증서 확인 구성 ..... 1040
복호화 제외 ..... 1041
Palo Alto Networks / 사전 정의된 복호화 제외 ..... 1042
기술적인 이유로 복호화에서 서버 제외 ..... 1043
로컬 복호화 제외 캐시 ..... 1044
정책 기반 복호화 제외 생성 ..... 1046
개인 키 내보내기 차단 ..... 1050
개인 키 생성 및 차단 ..... 1050
개인 키 가져오기 및 차단 ..... 1051
IKE 게이트웨이에 대한 프라이빗 키 가져오기 및 차단 ..... 1052
개인 키 차단 확인 ..... 1055
사용자가 SSL 복호화를 옵트아웃할 수 있도록 설정 ..... 1057

 ©2023 Palo Alto Networks, Inc.

일시적으로 SSL 복호화 사용 안 함 1059
복호화 포트 미러링 구성 1060
복호화 확인 1063
복호화 문제 해결 및 모니터링 1067
복호화 애플리케이션 명령 센터 위젯 1068
복호화 로그 1072
복호화를 위한 맞춤 리포트 템플릿 1087
프록시 유형 및 TLS 버전별로 지원되지 않는 매개 변수 1088
복호화 문제 해결 워크플로 예제 1089
복호화 기능을 위한 무료 라이선스 활성화 1110

**URL 필터링 1111**

Palo Alto Networks URL 필터링 솔루션 정보 1112
고급 URL 필터링 작동 방식 1113
로컬 인라인 분류 1115
URL 필터링 사용 사례 1116
URL 카테고리 1119
보안 중심 URL 카테고리 1119
악성 URL 카테고리 1120
확인된 URL 카테고리 1122
URL 카테고리에 따라 취할 수 있는 정책 조치 1122
URL 필터링 배포 계획 1126
URL 필터링 모범 사례 1129
고급 URL 필터링 구독 활성화 1131
URL 필터링 구성 1133
URL 필터링 구성 테스트 1137
URL 필터링 확인 1137
Advanced URL 필터링 확인 1137
인라인 분류 설정 1140
웹 활동 모니터링 1145
네트워크 사용자의 웹 활동 모니터링 1145
사용자 활동 보고서 보기 1147
사용자 지정 URL 필터링 보고서 구성 1149
사용자가 방문한 페이지만 기록 1153
사용자 지정 URL 카테고리 생성 1154
URL 카테고리 예외 1157
URL 카테고리 예외 목록에 대한 기본 지침 1157
URL 카테고리 예외 목록에 대한 와일드카드 지침 1159
URL 카테고리 예외 목록 - 예시 1160

 ©2023 Palo Alto Networks, Inc.

URL 필터링 프로파일에서 외부 동적 목록 사용 ..... 1163
특정 사이트에 대한 암호 액세스 허용 ..... 1165
자격 증명 피싱 방지 ..... 1168
회사 자격 증명 제출 확인 방법 ..... 1168
Windows User-ID 에이전트로 자격 증명 감지 구성 ..... 1170
자격 증명 피싱 방지 설정 ..... 1172
세이프서치 시행 ..... 1176
검색 공급자를 위한 안전 검색 설정 ..... 1176
엄격한 안전 검색이 활성화되지 않은 경우 검색 결과 차단 ..... 1179
투명하게 사용자를 위한 세이프서치 활성화 ..... 1182
URL 필터링 응답 페이지 ..... 1187
URL 필터링 응답 페이지 사용자 지정 ..... 1191
HTTP 헤더 로깅 ..... 1193
URL 카테고리 변경 요청 ..... 1194
온라인으로 변경 요청하기 ..... 1194
일괄 변경 요청하기 ..... 1195
방화벽에서 변경 요청하기 ..... 1196
URL 필터링 문제 해결 ..... 1198
고급 URL 필터링 활성화 문제 ..... 1198
PAN-DB 클라우드 연결 문제 ..... 1198
미해결로 분류된 URL ..... 1199
잘못된 분류 ..... 1200
PAN-DB 프라이빗 클라우드 ..... 1203
PAN-DB 프라이빗 클라우드용 M-600 어플라이언스 ..... 1203
PAN-DB 사설 클라우드 설정 ..... 1205
SSL/TLS 핸드셰이크 검사 활성화 ..... 1214

**서비스 품질 ..... 1219**

QoS 개요 ..... 1220
QoS 개념 ..... 1222
애플리케이션 및 사용자를 위한 QoS ..... 1222
QoS 정책 ..... 1222
QoS 프로파일 ..... 1223
QoS 클래스 ..... 1223
QoS 우선 순위 큐 ..... 1224
QoS 대역폭 관리 ..... 1224
QoS 송신 인터페이스 ..... 1225
일반 텍스트 및 터널링된 트래픽을 위한 QoS ..... 1226
QoS 구성 ..... 1227

 ©2023 Palo Alto Networks, Inc.

가상 시스템에 대한 QoS 구성 ..... 1234
DSCP 분류를 기반으로 QoS 적용 ..... 1241
QoS 사용 사례 ..... 1244
사용 사례: 단일 사용자를 위한 QoS ..... 1244
사용 사례: 음성 및 비디오 애플리케이션을 위한 QoS ..... 1246

**VPN ..... 1251**

VPN 배포 ..... 1252
사이트 간 VPN 개요 ..... 1253
사이트 간 VPN 개념 ..... 1254
IKE 게이트웨이 ..... 1254
터널 인터페이스 ..... 1254
터널 모니터링 ..... 1255
VPN용 인터넷 키 교환 (IKE) ..... 1255
IKEv2 ..... 1258
사이트 간 VPN 설정 ..... 1262
IKE 게이트웨이 설정 ..... 1262
암호화 프로파일 정의 ..... 1268
IPsec 터널 설정 ..... 1271
터널 모니터링 설정 ..... 1275
IKE 게이트웨이 또는 IPSec 터널 활성화/비활성화, 새로 고침 또는 다시 시작 ... 1277
VPN 연결 테스트 ..... 1278
VPN 오류 메시지 해석 ..... 1279
사이트 간 VPN 빠른 구성 ..... 1281
정적 라우팅을 사용하는 사이트 간 VPN ..... 1281
OSPF를 사용하는 사이트 간 VPN ..... 1285
정적 및 동적 라우팅을 사용하는 사이트 간 VPN ..... 1291

**대규모 VPN(LSVPN) ..... 1299**

LSVPN 개요 ..... 1300
LSVPN용 인터페이스 및 영역 생성 ..... 1301
GlobalProtect LSVPN 구성 요소 간에 SSL 활성화 ..... 1303
인증서 배포 에 대해 ..... 1303
GlobalProtect LSVPN 구성 요소에 서버 인증서 배포 ..... 1303
SCEP를 사용하여 GlobalProtect Satellite에 클라이언트 인증서 배포 ..... 1306
위성 인증을 위해 포털 구성 ..... 1309
LSVPN을 위한 글로벌 보호 게이트웨이 구성 ..... 1310
LSVPN을 위한 글로벌 보호 포털 구성 ..... 1314
LSVPN 전제 조건 작업에 대한 글로벌 보호 포털 ..... 1314


 ©2023 Palo Alto Networks, Inc.

포털 구성 ..... 1314
위성 구성 정의 ..... 1315
LSVPN에 가입할 위성 준비 ..... 1319
LSVPN 구성 확인 ..... 1322
LSVPN 빠른 구성 ..... 1323
정적 라우팅을 갖춘 기본 LSVPN 구성 ..... 1323
동적 라우팅을 갖춘 Advanced LSVPN 구성 ..... 1325
iBGP를 갖춘 Advanced LSVPN 구성 ..... 1328

**정책 ..... 1335**

정책 유형 ..... 1336
보안 정책 ..... 1337
보안 정책 규칙의 구성 요소 ..... 1337
보안 정책 조치 ..... 1343
보안 정책 규칙 생성 ..... 1344
정책 개체 ..... 1348
보안 프로파일 ..... 1350
보안 프로파일 그룹 생성 ..... 1357
기본 보안 프로파일 그룹 설정 또는 재정의 ..... 1358
규칙 베이스 내에서 규칙 추적 ..... 1360
규칙 번호 ..... 1360
규칙 UUID ..... 1361
정책 규칙 설명, 태그 및 감사 설명 적용 ..... 1366
정책 규칙 또는 개체를 다른 가상 시스템으로 이동 또는 복제 ..... 1368
주소 개체를 사용하여 IP 주소 표시 ..... 1369
주소 개체 ..... 1369
주소 개체 생성 ..... 1370
태그를 사용하여 개체를 그룹화하고 시각적으로 구별하기 ..... 1372
태그 생성 및 적용 ..... 1372
태그 수정 ..... 1373
태그 그룹별 규칙 보기 ..... 1373
정책에서 외부 동적 목록 사용 ..... 1376
외부 동적 목록 ..... 1376
외부 동적 목록에 대한 형식 지정 지침 ..... 1379
내장 외부 동적 목록 ..... 1381
외부 동적 목록에 액세스하도록 방화벽 구성 ..... 1382
EDL 호스팅 서비스에서 외부 동적 목록에 액세스하도록 방화벽 구성 ..... 1385
웹 서버에서 외부 동적 목록 검색 ..... 1391
외부 동적 목록 항목 보기 ..... 1391

 ©2023 Palo Alto Networks, Inc.

외부 동적 목록에서 항목 제외 1392
외부 동적 목록에 대한 정책 시행 1393
인증에 실패한 외부 동적 목록 찾기 1396
외부 동적 목록에 대한 인증 비활성화 1397
동적으로 IP 주소 및 태그 등록 1399
정책에서 동적 사용자 그룹 사용 1401
자동 태그 지정을 사용하여 보안 작업 자동화 1404
가상 환경의 변화 모니터링 1408
가상 네트워크에서 변경 사항을 추적하기 위해 VM 모니터링 사용 1408
Cloud Platforms의 가상 머신에서 모니터링되는 속성 1410
정책에서 동적 주소 그룹 사용 1414
동적 IP 주소 및 태그에 대한 CLI 명령 1418
업스트림 디바이스 뒤에 있는 엔드포인트 및 사용자에 대한 정책 시행 1420
소스 사용자 기반 정책에 XFF 값 사용 1420
보안 정책 및 로깅에서 XFF IP 주소 값 사용 1421
XFF 헤더의 IP 주소를 사용하여 이벤트 문제 해결 1424
정책 기반 포워딩 1426
PBF 1426
정책 기반 포워딩 규칙 생성 1428
사용 사례: 이중 ISP를 통한 아웃바운드 액세스를 위한 PBF 1432
테스트 정책 규칙 1440

**가상 시스템 1441**

가상 시스템 개요 1442
가상 시스템 구성 요소 및 세분화 1442
가상 시스템의 이점 1443
가상 시스템에 대한 사례 사용 1443
가상 시스템에 대한 플랫폼 지원 및 라이선스 1444
가상 시스템에 대한 관리 역할 1444
가상 시스템을 위한 공유 개체 1445
가상 시스템 간의 통신 1446
방화벽을 떠나야 하는 VSYS 간 트래픽 1446
방화벽 내에 남아 있는 VSYS 간 트래픽 1446
VSYS 간 통신은 두 세션을 사용합니다 1448
공유 게이트웨이 1450
외부 영역 및 공유 게이트웨이 1450
공유 게이트웨이에 대한 네트워킹 고려 사항 1451
가상 시스템 구성 1452
방화벽 내에서 가상 시스템 간 통신 구성 1458

 ©2023 Palo Alto Networks, Inc.

공유 게이트웨이 구성 ..... 1459
가상 시스템에 대한 서비스 경로 사용자 지정 ..... 1460
가상 시스템을 위한 서비스 경로 사용자 지정 ..... 1460
가상 시스템당 로깅을 위한 PA-7000 시리즈 방화벽 구성 ..... 1461
가상 시스템 또는 방화벽별로 관리 액세스 구성 ..... 1464
다른 기능을 가진 가상 시스템 기능 ..... 1466

**영역 보호 및 DoS 보호 ..... 1467**
영역을 사용한 네트워크 세그멘테이션 ..... 1468
영역은 네트워크를 어떻게 보호합니까? ..... 1469
존 디펜스 ..... 1470
존 디펜스 툴 ..... 1470
구역 방어 도구는 어떻게 작동합니까? ..... 1472
DoS 보호를 위한 방화벽 배치 ..... 1473
플러드 임계값 설정을 위한 기준 CPS 측정 ..... 1473
영역 보호 프로파일 ..... 1475
패킷 버퍼 보호 ..... 1479
DoS 보호 프로파일 및 정책 규칙 ..... 1481
영역 보호를 구성하여 네트워크 보안 강화 ..... 1487
정찰 보호 구성 ..... 1487
패킷 기반 공격 보호 구성 ..... 1488
프로토콜 보호 구성 ..... 1489
패킷 버퍼 보호 구성 ..... 1494
대기 시간을 기준으로 패킷 버퍼 보호 구성 ..... 1495
이더넷 SGT 보호 구성 ..... 1495
신규 세션의 홍수에 대한 DoS 보호 ..... 1497
다중 세션 DoS 공격 ..... 1497
단일 세션 DoS 공격 ..... 1501
신규 세션의 범람으로부터 DoS 보호 구성 ..... 1501
단일 세션 DoS 공격 종료 ..... 1504
온칩 패킷 디스크립터를 과하게 사용하는 세션 식별 ..... 1505
커밋 없이 세션 삭제 ..... 1508

**인증 ..... 1509**
FIPS 및 공통 기준 지원 활성화 ..... 1510
유지 보수 복구 도구(MRT)에 액세스 ..... 1510
작동 모드를 FIPS-CC 모드로 변경 ..... 1512
FIPS-CC 보안 기능 ..... 1515
FIPS-CC 모드에서 실행되는 방화벽 또는 어플라이언스에서 스왑 메모리 스크럽 ..... 1517

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

# 시작하기

다음 주제에서는 새로운 Palo Alto Networks 차세대 방화벽을 배포하는 데 도움이 되는 자세한 단계를 제공합니다. 새 방화벽을 네트워크에 통합하는 방법과 기본 보안 정책을 설정하는 방법에 대한 세부 정보를 제공합니다. 네트워크 보안 요구 사항을 해결하기 위해 보안 플랫폼 기능을 계속 배포하는 방법에 대한 지침은 방화벽 배포 완료를 위한 모범 사례를 검토하십시오.

- 방화벽을 관리 네트워크에 통합
- 방화벽 등록
- 인터페이스 및 영역을 사용하여 네트워크 분할
- 기본 보안 정책 설정
- 네트워크 트래픽 평가
- 무료 WildFire 포워딩 가능
- 방화벽 배포를 완료하기 위한 모범 사례

# 방화벽을 관리 네트워크에 통합

모든 Palo Alto Networks 방화벽은 방화벽 관리 기능을 수행하는 데 사용할 수 있는 대역 외 관리 포트(MGT)를 제공합니다. MGT 포트를 사용하여 방화벽의 관리 기능과 데이터 처리 기능을 분리하여 방화벽에 대한 접근을 보호하고 성능을 향상시킵니다. 웹 인터페이스를 사용하는 경우 향후 방화벽 관리를 위해 대역 내 데이터 포트를 사용할 계획이더라도 MGT 포트에서 모든 초기 구성 작업을 수행해야 합니다.

라이선스 검색, 방화벽의 위협 요소 및 애플리케이션 서명 업데이트와 같은 일부 관리 작업에는 인터넷 액세스가 필요합니다. MGT 포트에 대한 외부 액세스를 활성화하지 않으려면 대역 내 데이터 포트를 설정하여 필요한 외부 서비스(서비스 경로 사용)에 대한 액세스를 제공하거나 업데이트를 정기적으로 수동으로 업로드할 계획을 세워야 합니다.

인터넷이나 엔터프라이즈 보안 경계 내의 다른 신뢰할 수 없는 영역에서 관리 인터페이스에 액세스할 수 있도록 설정하지 마십시오. 이는 전용 관리 포트(*MGT*)를 사용하거나 데이터 포트를 관리 인터페이스로 구성했는지의 여부와 관계없이 적용됩니다. 방화벽을 관리 네트워크에 통합할 때 관리 액세스 모범 사례에 따라 성공적인 공격을 방지하는 방식으로 방화벽 및 기타 보안 디바이스에 대한 관리 액세스를 보호하고 있는지 확인하십시오.

다음 항목에서는 새 방화벽을 관리 네트워크에 통합하고 기본 보안 구성에 배포하는 데 필요한 초기 구성 단계를 수행하는 방법에 대해 설명합니다.

- 비즈니스 연속성을 위한 액세스 전략 결정
- 관리 전략 결정
- 초기 구성 수행
- 외부 서비스에 대한 네트워크 액세스 설정

다음 주제에서는 단일 *Palo Alto Networks* 차세대 방화벽을 네트워크에 통합하는 방법을 설명합니다. 그러나 중복성을 위해 고가용성 구성에서 한 쌍의 방화벽을 배포하는 것을 고려하십시오.

## 비즈니스 연속성을 위한 액세스 전략 결정

비즈니스 연속성 계획에는 정전 및 일반 통신 채널을 통해 이러한 디바이스에 연결하지 못하게 하는 기타 이벤트 중에 방화벽 및 Panorama를 비롯한 중요한 디바이스에 연결하는 방법에 대한 조항이 포함되어야 합니다. 대역외(OOB) 네트워크의 디바이스에 연결하고 관리하는 기능을 사용하면 기본 네트워크 및 전원이 다운되었을 때 비즈니스를 계속 실행할 수 있습니다. 비즈니스 연속성은 네트워크 아키텍처의 핵심 고려 사항이어야 합니다.

***OOB*** 네트워크는 원격으로 디바이스에 액세스하고 관리하는 안전한 방법이며 기본 통신 채널을 사용하지 않습니다. 대신 ***OOB*** 네트워크는 주 채널이 실패하고 기본 네트워크와 다른 전원 소스가 있는 경우 항상 사용할 수 있는 별도의 통신 채널을 사용합니다. 네트워크 아키텍처에 따라 기본 네트워크와 ***OOB*** 네트워크를 모두 사용하여 일상적인 작업에서 디바이스에 액세스하고 관리할 수 있습니다.

OOB 네트워크는 기본 액세스 네트워크와 동시에 실패할 수 있는 전원 또는 네트워크에 의존해서는 안 됩니다. 디바이스에 대한 OOB 액세스를 설계하는 방법은 네트워크 아키텍처와 비즈니스 고려 사항에 따라


©2023 Palo Alto Networks, Inc.

다르므로 연결을 보장하는 "한 가지 크기에 모두 맞는" 방법은 없습니다. 그러나 OOB 액세스 네트워크의 목표를 충족하는 방법을 이해하는 데 도움이 되는 지침이 있습니다.

- 전원 고려 사항 - OOB 네트워크에 일반 액세스 네트워크에 사용하는 것보다 다른 전원(별도의 회로 또는 보호 또는 배터리 전원 공급 소스)을 사용합니다. 일반 네트워크에 대한 전원이 꺼져도 OOB 네트워크의 전원이 손실되지 않습니다.

  배전 디바이스(PDU) 컨트롤을 사용하여 원격으로 디바이스의 전원을 켜고 끕니다.
- 보안 연결 방법 - OOB 네트워크에 안전하게 연결하는 방법(예: 터미널 서버 디바이스, 모뎀 또는 직렬 콘솔 서버)에는 여러 가지가 있습니다. OOB 액세스에 사용할 수 있는 보안 네트워크의 예로는 LTE, 전화 접속 및 광대역(일반 광대역 네트워크와 완전히 분리됨) 네트워크가 있습니다. 사용하는 연결 방법은 비즈니스 요구 사항 및 네트워크 아키텍처에 따라 다릅니다.

  선택한 방법에 관계없이 연결은 강력한 암호화 및 인증으로 안전해야 합니다. 방화벽 및 Panorama에 대한 관리 연결을 보호하는 방법에 대한 조언은 관리 액세스 모범 사례를 참조하십시오.

  이더넷 LAN을 통한 강력한 인증으로 SSH를 사용하여 원격으로 OOB 네트워크에 연결하거나 직렬 연결을 통해 전화를 걸 수 있습니다. 아웃바운드 연결은 직렬입니다.

## 관리 전략 결정

Palo Alto Networks 방화벽은 로컬에서 구성 및 관리하거나 Palo Alto Networks 중앙 집중식 보안 관리 시스템인 Panorama를 사용하여 중앙에서 관리할 수 있습니다. 네트워크에 6개 이상의 방화벽이 배포된 경우 Panorama를 사용하여 다음과 같은 이점을 얻을 수 있습니다.

- 구성, 정책, 소프트웨어 및 동적 콘텐츠 업데이트 관리의 복잡성과 관리 오버헤드를 줄입니다. Panorama에서 디바이스 그룹 및 템플릿을 사용하면 방화벽에서 로컬로 방화벽별 구성을 효과적으로 관리하고 모든 방화벽 또는 디바이스 그룹에 공유 정책을 적용할 수 있습니다.
- 관리되는 모든 방화벽에서 데이터를 집계하고 네트워크의 모든 트래픽에 대한 가시성을 확보합니다. Panorama의 ACC(Application Command Center)는 모든 방화벽에 대한 통합 보고를 위한 단일 창을 제공하므로 네트워크 트래픽, 보안 사고 및 관리 수정 사항을 중앙에서 분석, 조사 및 보고할 수 있습니다.

다음 절차에서는 로컬 웹 인터페이스를 사용하여 방화벽을 관리하는 방법을 설명합니다. 중앙 집중식 관리를 위해 Panorama를 사용하려면 먼저 초기 구성을 수행하고 방화벽이 Panorama에 연결할 수 있는지 확인하십시오. 그 시점부터 Panorama를 사용하여 방화벽을 중앙에서 구성할 수 있습니다.

## 초기 구성 수행

기본적으로 PA 시리즈 방화벽에는 192.168.1.1의 IP 주소와 관리자/관리자의 사용자 이름/암호가 있습니다. 보안상의 이유로 다른 방화벽 구성 작업을 계속하기 전에 이러한 설정을 변경해야 합니다. MGT 인터페이스에서 방화벽 관리에 이 인터페이스를 사용하지 않거나 방화벽의 콘솔 포트에 직접 직렬 연결을 사용하더라도 이러한 초기 구성 작업을 수행해야 합니다.

**STEP 1 |** 방화벽을 설치하고 전원을 연결합니다.



방화벽 모델에 이중 전원 공급 디바이스가 있는 경우 중복성을 위해 두 번째 전원 공급 디바이스를 연결합니다. 자세한 내용은 모델에 대한 하드웨어 참조 가이드를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 네트워크 관리자로부터 필요한 정보를 수집합니다.

- MGT 포트의 IP 주소
- 넷마스크(netmask)
- 기본 게이트웨이
- DNS 서버 주소

**STEP 3 |** 컴퓨터를 방화벽에 연결합니다.

방화벽에 다음 방법 중 하나에서 연결할 수 있습니다.

- 컴퓨터에서 콘솔 포트에 직렬 케이블을 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 방화벽에 연결합니다. 부팅 시퀀스가 완료될 때까지 몇 분 간 기다립니다. 방화벽이 준비되면 방화벽 이름(예: **PA-220 로그인**)이 변경됩니다.
- 컴퓨터에서 방화벽의 MGT 포트에 RJ-45 이더넷 케이블을 연결합니다. 브라우저에서 **https://192.168.1.1**로 이동합니다.

> 이 ***URL***에 액세스하려면 컴퓨터의 ***IP*** 주소를 ***192.168.1.0/24*** 네트워크의 주소***(***예***:*** ***192.168.1.2)***로 변경해야 할 수 있습니다***.***

**STEP 4 |** 메시지가 표시되면 방화벽에 로그인합니다.

기본 사용자 이름과 암호(관리자/관리자)를 사용하여 로그인해야 합니다. 방화벽이 초기화되기 시작합니다.

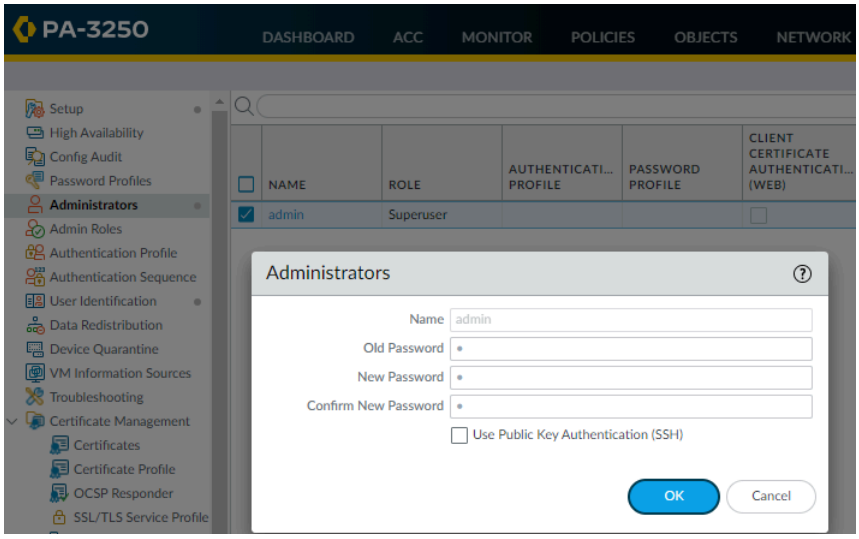

©2023 Palo Alto Networks, Inc.

**STEP 5 |** 관리자 계정에 대한 보안 암호를 설정합니다.

*PAN-OS 9.0.4*부터는 사전 정의된 기본 관리자 암호(관리자/관리자)를 디바이스의 첫 번째 로그인에서 변경해야 합니다. 새 암호는 최소 *8*자여야 하며 최소 한 개의 소문자와 하나의 대문자 문자와 하나의 숫자 또는 특수 문자를 포함해야 합니다.

암호 강도에 대한 모범 사례를 사용하여 엄격한 암호를 확인하고 암호 복잡성 설정을 검토해야 합니다.

1. 디바이스 > 관리자를 선택합니다.
2. 관리자 역할을 선택합니다.
3. 현재 기본 암호와 새 암호를 입력합니다.




4. 확인을 클릭하여 설정을 저장합니다.

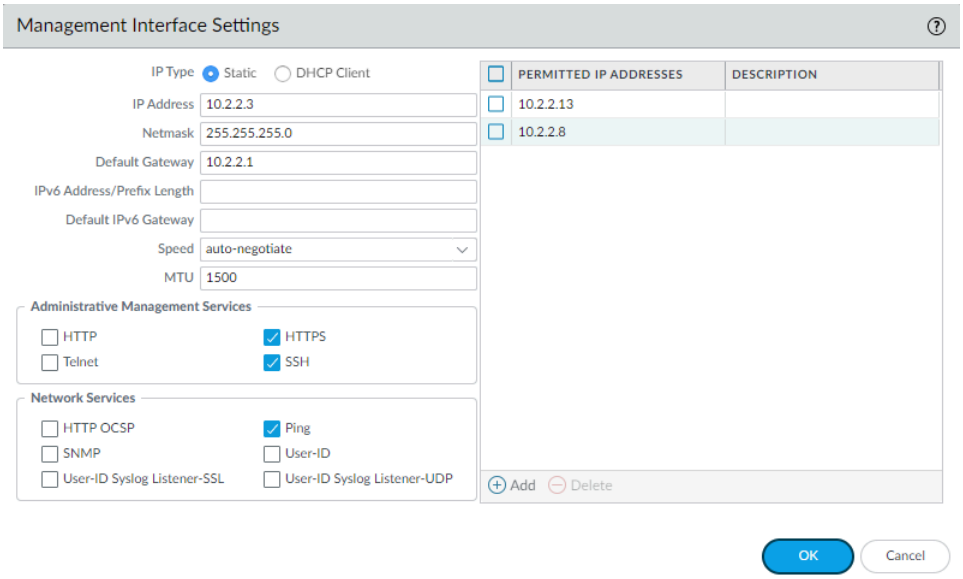

©2023 Palo Alto Networks, Inc.

**STEP 6 |** MGT 인터페이스를 구성합니다.

1. 디바이스 > 설정 > 인터페이스를 선택하고 관리 인터페이스를 수정합니다.
2. 다음 방법 중 하나를 사용하여 MGT 인터페이스에 대한 주소 설정을 구성합니다.
   - MGT 인터페이스에 대한 정적 IP 주소 설정을 구성하려면 **IP** 유형을 고정으로 설정하고 **IP** 주소, 넷마스크**(netmask)** 및 기본 게이트웨이를 입력합니다.
   - MGT 인터페이스 주소 설정을 동적으로 구성하려면 **IP** 유형을 **DHCP** 클라이언트로 설정합니다. 이 방법을 사용하려면 관리 인터페이스를 DHCP 클라이언트로 구성해야 합니다.

   관리 인터페이스에 대한 무단 액세스를 방지하려면 관리자가 ***MGT*** 인터페이스에 액세스할 수 있는 허용된 ***IP*** 주소를 추가하는 것이 관리 모범 사례입니다.
3. 속도를 자동 협상으로 설정합니다.
4. 인터페이스에서 허용할 관리 서비스를 선택합니다.

   이러한 서비스는 일반 텍스트를 사용하고 다른 서비스만큼 안전하지 않고 관리자 자격 증명을 손상시킬 수 있으므로 ***Telnet*** 및 ***HTTP***를 선택하지 않았는지 확인합니다.



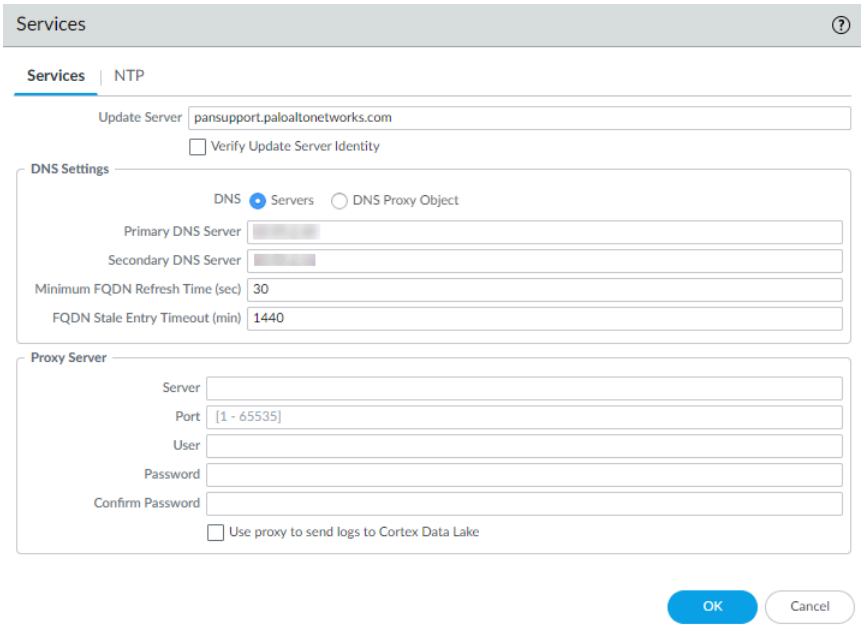

5. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** DNS, 서버 업데이트 및 프록시 서버 설정을 구성합니다.

방화벽에서 하나 이상의 ***DNS*** 서버를 수동으로 구성해야 합니다. 그렇지 않으면 호스트 이름을 확인할 수 없습니다. ***ISP***와 같은 다른 소스의 ***DNS*** 서버 설정을 사용하지 않습니다.

1. 디바이스 > 설정 > 서비스를 선택합니다.
   - 다중 가상 시스템 플랫폼의 경우 전역을 선택한 다음 서비스 섹션을 편집합니다.
   - 단일 가상 시스템 플랫폼의 경우 서비스 섹션을 편집합니다.
2. 서비스 탭에서 **DNS**의 경우 다음 중 하나를 선택합니다.
   - 서버 - 기본 **DNS** 서버 주소와 보조 **DNS** 서버 주소를 입력합니다.
   - **DNS Proxy Object** - 드롭다운에서 전역 DNS 서비스를 구성하는 데 사용할 **DNS** 프록시를 선택하거나 **DNS** 프록시를 클릭하여 새 DNS 프록시 개체를 구성합니다.

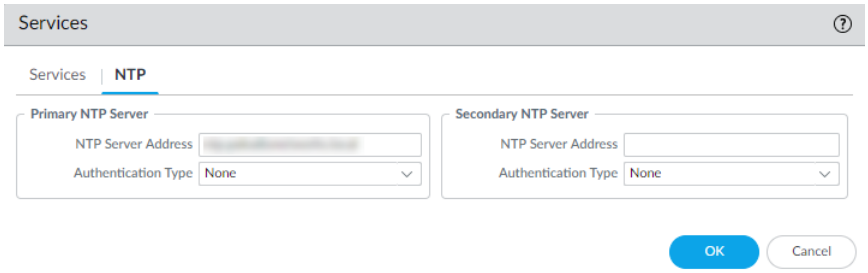



3. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 날짜 및 시간(NTP) 설정을 구성합니다.

1. 디바이스 > 설정 > 서비스를 선택합니다.
   - 다중 가상 시스템 플랫폼의 경우 전역을 선택한 다음 서비스 섹션을 편집합니다.
   - 단일 가상 시스템 플랫폼의 경우 서비스 섹션을 편집합니다.
2. **NTP** 탭에서 인터넷에서 시간 서버의 가상 클러스터를 사용하려면 호스트 이름 `pool.ntp.org`를 기본 **NTP** 서버로 입력하거나 다음을 입력합니다. 기본 NTP 서버의 IP 주소입니다.




3. (선택 사항) 보조 **NTP** 서버 주소를 입력합니다.
4. (선택 사항) 인증 유형에 대해 NTP 서버에서 시간 업데이트를 인증하려면 각 서버에 대해 다음 중 하나를 선택합니다.
   - 없음(기본값) NTP 인증을 비활성화합니다.
   - 대칭 키 - 방화벽은 대칭 키 교환(공유 암호)을 사용하여 시간 업데이트를 인증합니다.
     - 키 **ID** - 키 ID(1-65534)를 입력합니다.
     - 알고리즘 - NTP인증(**MD5** 또는 **SHA1**)에서 사용할 알고리즘을 선택합니다.
   - 자동키 - 방화벽은 자동 키(공개 키 암호화)를 사용하여 시간 업데이트를 인증합니다.
5. 확인을 클릭합니다.

**STEP 9 |** (선택 사항) 필요에 따라 일반 방화벽 설정을 구성합니다.

1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 수정합니다.
2. 방화벽에 대한 호스트 이름을 입력하고 네트워크 도메인 이름을 입력합니다. 도메인 이름은 레이블일 뿐입니다. 도메인에 가입하는 데 사용되지 않습니다.
3. 로그인하려는 사용자에게 방화벽 관리 기능에 액세스하려면 권한이 필요하다는 사실을 알리는 로그인 배너 텍스트를 입력합니다.

   가장 좋은 방법은 환영하는 표현을 사용하지 않는 것입니다. 또한 법률팀에 배너 메시지를 검토하여 무단 액세스가 금지되어 있음을 적절히 경고하는지 확인하도록 요청해야 합니다.
4. 위도 및 경도를 입력하여 세계 지도에 방화벽을 정확하게 배치할 수 있습니다.
5. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 10 |** 변경 사항을 커밋합니다.

구성 변경 내용을 저장하면 ***IP*** 주소가 변경되어 웹 인터페이스에 대한 연결이 손실됩니다**.**

웹 인터페이스의 오른쪽 상단에 커밋을 클릭합니다. 방화벽은 변경 내용을 저장하는 데 최대 90초가 걸릴 수 있습니다.

**STEP 11 |** 방화벽을 네트워크에 연결합니다.

1. 컴퓨터에서 방화벽을 분리합니다.
2. (PA-5450을 제외한 모든 방화벽) RJ-45 이더넷 케이블을 사용하여 MGT 포트를 관리 네트워크의 스위치 포트에 연결합니다. 방화벽을 자동으로 협상할 수 있도록 케이블을 연결한 스위치 포트를 확인합니다.
3. (PA-5450만 해당) Palo Alto Networks 인증 SFP/SFP+ 트랜시버 및 케이블을 사용하여 MGT 포트를 관리 네트워크의 스위치 포트에 연결합니다.

**STEP 12 |** 방화벽에 SSH 관리 세션을 엽니다.

PuTTY와 같은 터미널 에뮬레이션 소프트웨어를 사용하여 할당된 새 IP 주소를 사용하여 방화벽에 SSH 세션을 시작합니다.


©2023 Palo Alto Networks, Inc.

**STEP 13 |** Palo Alto Networks 업데이트 서버와 같은 방화벽 관리에 필요한 외부 서비스에 대한 네트워크 액세스를 확인합니다.

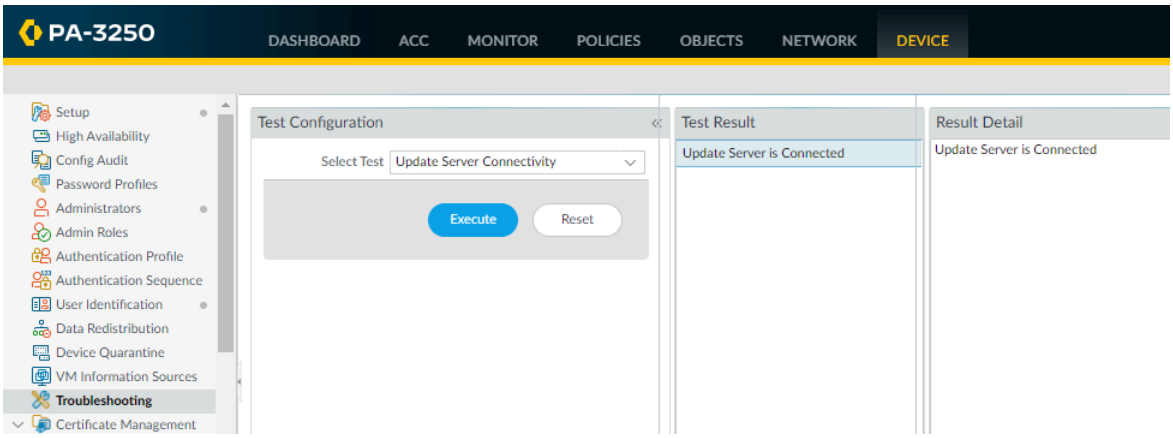
다음 방법 중 하나에서 이 작업을 수행할 수 있습니다.

- MGT 인터페이스에 대한 외부 네트워크 액세스를 허용하지 않으려면 필요한 서비스 업데이트를 검색하기 위해 데이터 포트를 설정해야 합니다. 외부 서비스에 대한 네트워크 액세스 설정을 계속합니다.
- MGT 인터페이스에 대한 외부 네트워크 액세스를 허용하려는 경우 연결이 있는지 확인한 다음 방화벽 등록 및 구독 라이선스 활성화을(를) 진행합니다.

1. 업데이트 서버 연결 테스트를 사용하여 Palo Alto Networks 업데이트 서버에 대한 네트워크 연결을 다음 예제와 같이 확인합니다.

   **1.** 디바이스 > 트러블슈팅을 선택한 다음 테스트 드롭다운 선택에서 서버 연결 업데이트를 선택합니다.

   **2.** 업데이트 서버 연결 테스트를 실행합니다.




2. Palo Alto Networks 업데이트 서버에서 방화벽에 대한 지원 권한에 대한 정보를 검색하려면 다음 CLI 명령을 사용합니다.

```
request support check
```

연결이 있는 경우 업데이트 서버가 방화벽의 지원 상태로 응답합니다. 방화벽이 아직 등록되지 않은 경우 업데이트 서버는 다음 메시지를 반환합니다.

```
https://www.paloaltonetworks.com/company/contact-us.html
 Support Home https://www.paloaltonetworks.com/support/tabs/
overview로 문의해 주십시오. 이 업데이트 서버에서 디바이스를 찾을 수 없습
니다.
```

## 외부 서비스에 대한 네트워크 액세스 설정

기본적으로 방화벽은 MGT 인터페이스를 사용하여 DNS 서버, 콘텐츠 업데이트 및 라이선스 검색과 같은 원격 서비스에 액세스합니다. 관리 네트워크에 대한 외부 네트워크 액세스를 사용하지 않으려면 대역내


©2023 Palo Alto Networks, Inc.

데이터 포트를 설정하여 필요한 외부 서비스에 대한 액세스를 제공하고 서비스 경로를 설정하여 외부 서비스에 액세스하는 데 사용할 포트를 방화벽에 지시해야 합니다.

인터넷이나 엔터프라이즈 보안 경계 내의 다른 신뢰할 수 없는 영역에서 관리 액세스를 사용하도록 설정하지 마십시오. 관리 액세스 모범 사례 에 따라 방화벽을 올바르게 보호하고 있는지 확인합니다.

이 작업을 수행하려면 방화벽 인터페이스, 영역 및 정책에 익숙해야 합니다. 이러한 항목에 대한 자세한 내용은 인터페이스 및 영역 구성 및 기본 보안 정책 설정을 참조하십시오.

**STEP 1 |** 외부 서비스에 액세스하는 데 사용할 인터페이스를 결정하고 스위치 또는 라우터 포트에 연결합니다.

사용하는 인터페이스에는 고정 IP 주소가 있어야 합니다.

**STEP 2 |** 웹 인터페이스에 로그인합니다.

웹 브라우저에서 보안 연결(https)을 사용하여 초기 구성 중에 할당한 새 IP 주소와 암호(https://<IP address>)를 사용하여 로그인합니다. 인증서 경고가 표시되지만 정상입니다. 웹 페이지를 계속 진행합니다.

**STEP 3 |** (선택 사항) 방화벽은 포트 이더넷 1/1과 이더넷 1/2(및 해당 기본 보안 정책 및 영역) 사이의 기본 가상 와이어 인터페이스로 미리 구성됩니다. 이 가상 와이어 구성을 사용하지 않으려면 사용자가 정의한 다른 인터페이스 설정을 방해하지 않도록 구성을 수동으로 삭제해야 합니다.

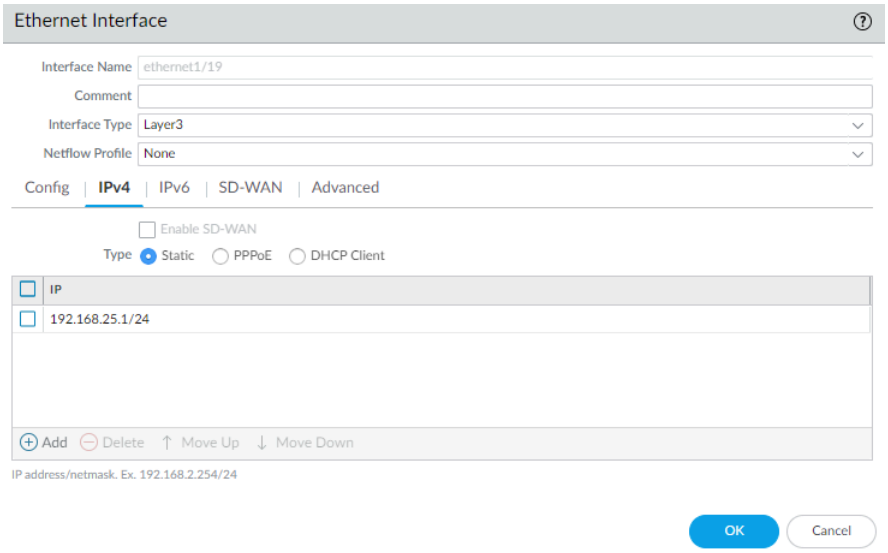
다음 순서로 구성을 삭제해야 합니다.

1. 기본 보안 정책을 삭제하려면 정책 > 보안을 선택하고 규칙을 선택한 다음 삭제를 클릭합니다.
2. 기본 가상 와이어를 삭제하려면 네트워크 > 가상 와이어를 선택하고 가상 와이어를 선택한 다음 삭제를 클릭합니다.
3. 기본 신뢰 및 비신뢰 영역을 삭제하려면 네트워크 > 영역을 선택하고 각 영역을 선택한 다음 삭제를 클릭합니다.
4. 인터페이스 구성을 삭제하려면 네트워크 > 인터페이스를 선택한 다음 각 인터페이스(ethernet1/1 및 ethernet1/2)를 선택하고 삭제를 클릭합니다.
5. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 관리 서비스에 대한 외부 액세스에 사용할 인터페이스를 구성합니다.

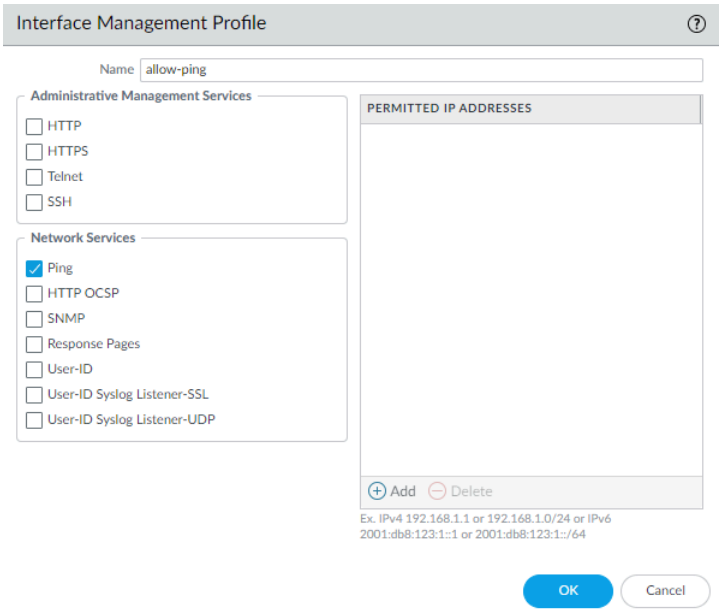
1. 네트워크 > 인터페이스를 선택하고 1단계에서 케이블을 연결한 인터페이스에 해당하는 인터페이스를 선택합니다.
2. 인터페이스 유형을 선택합니다. 여기에서 선택은 네트워크 토폴로지에 따라 다르지만 이 예에서는 **Layer3**에 대한 단계를 보여줍니다.
3. 구성 탭에서 보안 영역 드롭다운을 확장하고 새 영역을 선택합니다.
4. 영역 대화 상자에서 새 영역의 이름(예: 관리)을 입력한 다음 확인을 클릭합니다.
5. **IPv4** 탭을 선택하고 고정 라디오 버튼을 선택한 다음 IP 섹션에서 추가를 클릭하고 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다. 예: 192.168.1.254/24. 이 인터페이스에서 고정 IP 주소를 사용해야 합니다.




6. 고급 > 기타 정보를 선택하고 관리 프로파일 드롭다운을 확장한 다음 새 관리 프로파일을 선택합니다.
7. 프로파일의 이름(예: allow_ping)을 입력한 다음 인터페이스에서 허용할 서비스를 선택합니다. 외부 서비스에 대한 액세스를 허용하려면 **Ping**을 활성화한 다음 확인만 클릭하면 됩니다.


©2023 Palo Alto Networks, Inc.

이러한 서비스는 방화벽에 대한 관리 액세스를 제공하므로 이 인터페이스에서 허용할 관리 활동에 해당하는 서비스만 선택합니다. 예를 들어 ***HTTP*** 또는 ***Telnet***은 일반 텍스트로 전송되므로 안전하지 않으므로 활성화하지 마십시오. 또는 웹 인터페이스 또는 ***CLI***를 통해 방화벽 구성 작업에 ***MGT*** 인터페이스를 사용하려는 경우 인터페이스를 통한 무단 액세스를 방지하기 위해 ***HTTP, HTTPS, SSH*** 또는 ***Telnet***을 활성화하지 마십시오(***HTTPS*** 또는 ***SSH***를 허용해야 하는 경우 이 시나리오에서는 특정 세트의 허용된 ***IP*** 주소에 대한 액세스를 제한합니다. 자세한 내용은 인터페이스 관리 프로파일을 사용하여 액세스 제한을 참조하십시오.




8. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

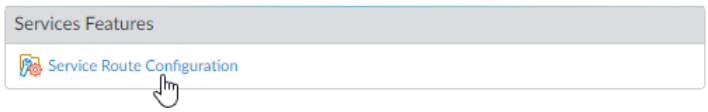

©2023 Palo Alto Networks, Inc.

**STEP 5 |** 서비스 경로를 구성합니다.

기본적으로 방화벽은 MGT 인터페이스를 사용하여 필요한 외부 서비스에 액세스합니다. 방화벽에서 외부 서비스에 요청을 보내는 데 사용하는 인터페이스를 변경하려면 서비스 경로를 편집해야 합니다.

이 예에서는 전역 서비스 경로를 설정하는 방법을 보여 줍니다. 글로벌 기반이 아닌 가상 시스템 기반으로 외부 서비스에 대한 네트워크 액세스를 설정하는 방법에 대한 자세한 내용은 가상 시스템의 서비스에 대한 서비스 경로 사용자 지정을 참조하십시오.

1. 디바이스 > 설정 > 서비스 > 글로벌을 선택하고 서비스 경로 구성을 클릭합니다.




   라이선스를 활성화하고 최신 콘텐츠 및 소프트웨어 업데이트를 가져오려면 ***DNS***, ***Palo Alto Networks*** 서비스, ***URL*** 업데이트 및 자동 초점에 대한 서비스 경로를 변경해야 합니다.

2. 사용자 정의 라디오 버튼을 클릭하고 다음 중 하나를 선택합니다.

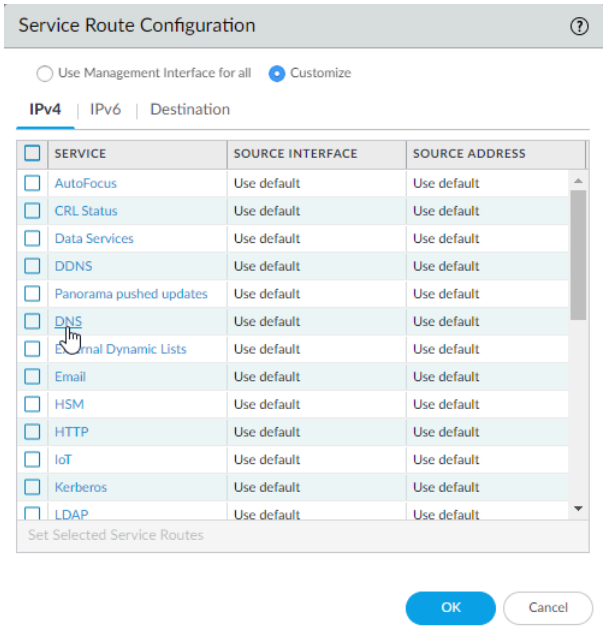
   - 사전 정의된 서비스의 경우 **IPv4** 또는 **IPv6**을 선택한 다음 서비스에 대한 링크를 클릭합니다. 소스 주소에 대한 드롭다운 목록을 제한하려면 소스 인터페이스를 선택한 다음 방금 구성한 인터페이스를 선택합니다. 그런 다음 소스 주소(해당 인터페이스의)를 서비스 경로로 선택합니다.

     선택한 인터페이스에 대해 둘 이상의 IP 주소가 구성된 경우 소스 주소 드롭다운을 사용하여 IP 주소를 선택할 수 있습니다.

   - 사용자 지정 대상에 대한 서비스 경로를 생성하려면 [대상]을 선택한 다음 [추가]를 클릭합니다. 대상 IP 주소를 입력합니다. 대상 주소가 이 주소와 일치하는 수신 패킷은 이 서비스 경로에 대해 지정한 소스 주소를 소스로 사용합니다. 소스 주소에 대한 드롭다운을 제한하려면 소

 ©2023 Palo Alto Networks, Inc.

스 인터페이스를 선택합니다. 선택한 인터페이스에 대해 둘 이상의 IP 주소가 구성된 경우 소스 주소 드롭다운을 사용하여 IP 주소를 선택할 수 있습니다.




3. 확인을 클릭하여 설정을 저장합니다.
4. 수정할 각 서비스 경로에 대해 위의 5.2 - 5.3단계를 반복합니다.
5. 변경 사항을 커밋합니다.

**STEP 6 |** 외부 인터페이스 및 연결된 영역을 구성한 다음 방화벽이 내부 영역에서 외부 영역으로 서비스 요청을 보내도록 허용하는 보안 정책 규칙을 생성합니다.

1. 네트워크 > 인터페이스를 선택한 다음 외부 인터페이스를 선택합니다. 인터페이스 유형으로 **Layer3**을 선택한 다음 **IPv4** 또는 **IPv6** 탭에서 **IP** 주소 추가를 선택한 다음 구성 탭에서 인터넷과 같은 연결된 보안 영역을 생성합니다. 이 인터페이스에는 고정 IP 주소가 있어야 합니다. 이 인터페이스에서 관리 서비스를 설정할 필요가 없습니다.
2. 내부 네트워크에서 Palo Alto Networks 업데이트 서버로의 트래픽을 허용하는 보안 규칙을 설정하려면 정책 > 보안을 선택하고 추가를 클릭하십시오.

보안 정책 규칙을 만들 때는 포트 기반 규칙 대신 애플리케이션 기반 규칙을 사용하여 포트, 프로토콜, 회피 전술 또는 사용 중인 암호화에 관계없이 기본 애플리케이션을 정확하게 식별할 수 있도록 하는 것이 가장 좋습니다. 서비스는 항상 애플리케이션 기본값으로 설정된 상태로 둡니다. 이 경우 업데이트 서버*(*및 기타 *Palo Alto Networks* 서비스*)*에 대한 액세스를 허용하는 보안 정책 규칙을 생성합니다.

| | NAME | Source ZONE | Destination ZONE | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|
| 1 | Palo Alto Networks Services | Management | Internet | paloalto-dns-security<br>paloalto-logging-service<br>paloalto-updates<br>paloalto-wildfire-cloud | application-... | Allow |


©2023 Palo Alto Networks, Inc.

**STEP 7 |** NAT 정책 규칙을 생성합니다.

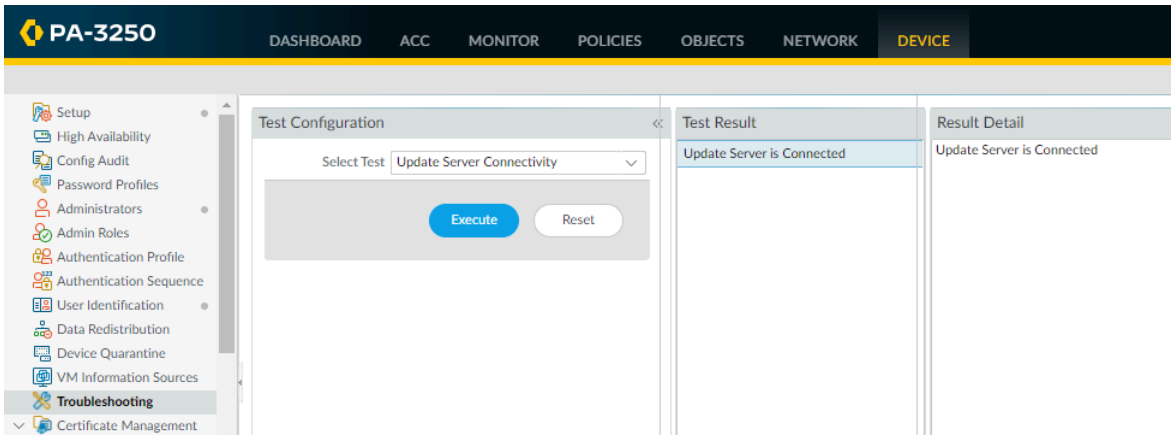
1. 내부 인터페이스에서 프라이빗 IP 주소를 사용하는 경우 주소를 공개적으로 라우팅할 수 있는 주소로 변환하는 소스 NAT 규칙을 만들어야 합니다. 정책 > **NAT**를 선택한 다음 추가를 클릭합니다. 최소한 규칙의 이름을 정의하고(일반 탭), 소스 및 대상 영역을 지정하고, 이 경우 인터넷으로 관리(**Original Packet** 탭), 다음을 정의해야 합니다. 소스 주소 변환 설정(**Translated Packet** 탭)을 선택한 다음 확인을 클릭합니다.
2. 변경 사항을 커밋합니다.

| | | Original Packet | | | Translated Packet | |
|---|---|---|---|---|---|---|
| | NAME | SOURCE ZONE | DESTINATION ZONE | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| 1 | Source NAT | Management | Internet | any | dynamic-ip-and-port | none |

**STEP 8 |** 디바이스 > 문제 해결을 선택한 다음, 기본 게이트웨이를 포함하고 **Ping** 연결 테스트를 사용하는 데이터 포트에서 외부 서비스 및 업데이트 서버 연결 테스트를 사용하는 Palo Alto Networks 업데이트 서버로 연결되어 있는지 확인합니다 이 예제에서는 Palo Alto 네트워크 업데이트 서버에 대한 방화벽 연결을 테스트합니다.

필요한 네트워크 연결이 있는지 확인한 후 방화벽 등록 및 구독 라이선스 활성화을(를) 계속합니다.

1. 테스트 선택 드롭다운에서 서버 업데이트를 선택합니다.
2. Palo Alto Networks 업데이트 서버 연결 테스트를 실행합니다.




3. 방화벽 CLI에 액세스하고 다음 명령을 사용하여 Palo Alto Networks 업데이트 서버에서 방화벽에 대한 지원 권한에 대한 정보를 검색합니다.

```
request support check
```

연결이 있는 경우 업데이트 서버가 방화벽의 지원 상태로 응답합니다. 방화벽이 등록되지 않았으므로 업데이트 서버는 다음 메시지를 반환합니다.

```
https://www.paloaltonetworks.com/company/contact-us.html
 Support Home https://www.paloaltonetworks.com/support/tabs/
overview로 문의해 주십시오. 이 업데이트 서버에서 디바이스를 찾을 수 없습
니다.
```

 ©2023 Palo Alto Networks, Inc.

# 방화벽 등록

지원 및 기타 라이선스 및 구독을 활성화하려면 먼저 방화벽을 등록해야 합니다. 그러나 방화벽을 등록하려면 먼저 활성 지원 계정이 있어야 합니다. 활성 지원 계정이 있는지의 여부에 따라 다음 작업 중 하나를 수행합니다.

- 활성 지원 계정이 없으면 새 지원 계정 생성 및 방화벽 등록을(를) 합니다.
- 이미 활성 지원 계정이 있는 경우 방화벽 등록할 준비가 된 것입니다.
- 등록된 방화벽에서 (선택 사항) Day 1 구성 수행.
- 방화벽이 NPC(네트워크 처리 카드)와 같은 라인 카드를 사용하는 경우, 방화벽 라인 카드 등록.

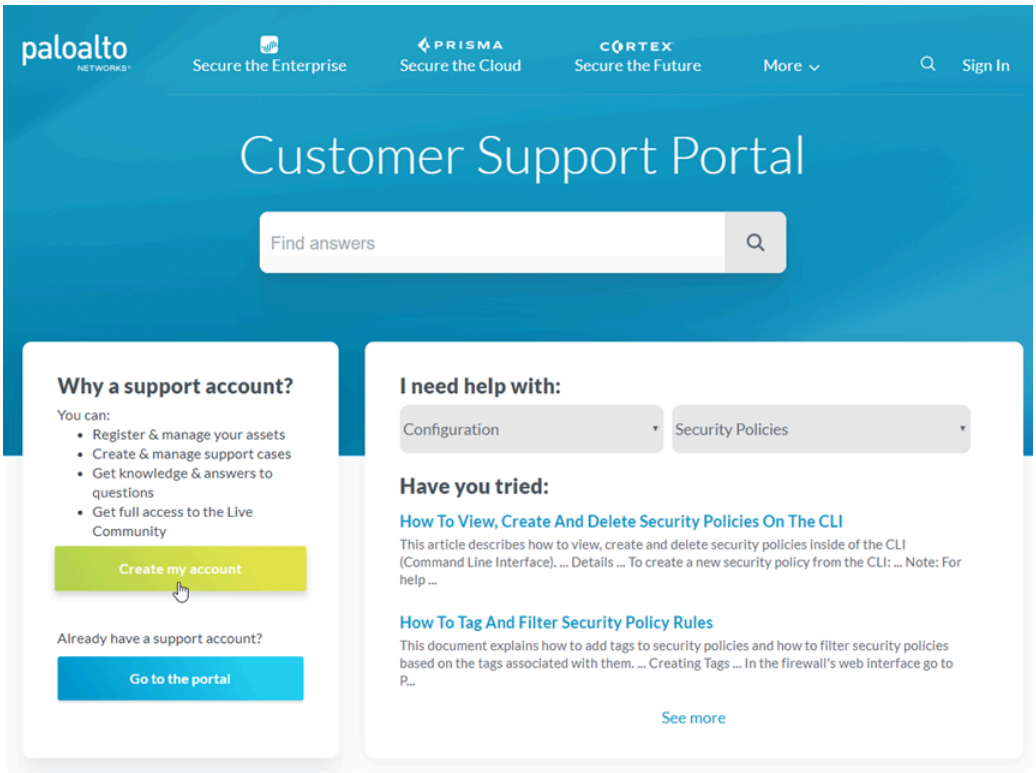
VM-시리즈 방화벽을 등록하는 경우 지침은 VM-시리즈 배포 가이드를 참조하십시오.

## 새 지원 계정 생성 및 방화벽 등록

활성 Palo Alto Networks 지원 계정이 아직 없는 경우 새 지원 계정을 만들 때 방화벽을 등록해야 합니다.

**STEP 1 |** Palo Alto Networks 고객 지원 포털로 이동합니다.

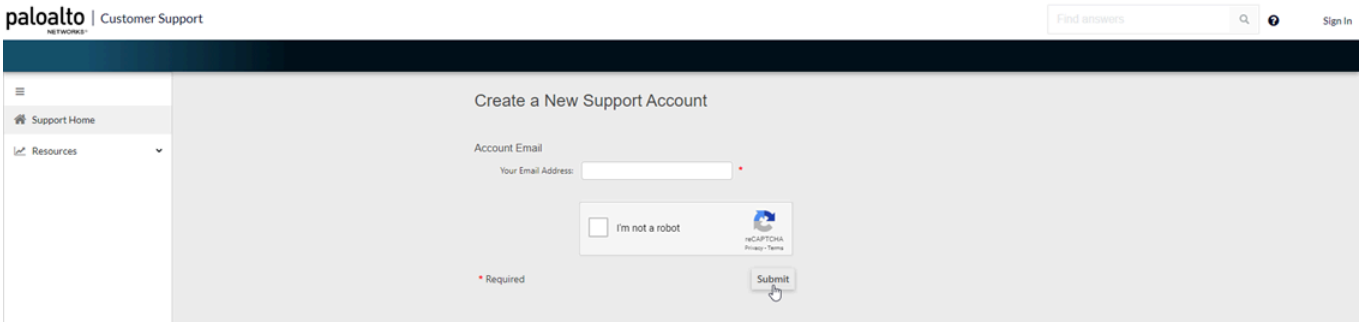
**STEP 2 |** 내 계정 생성를 클릭합니다.



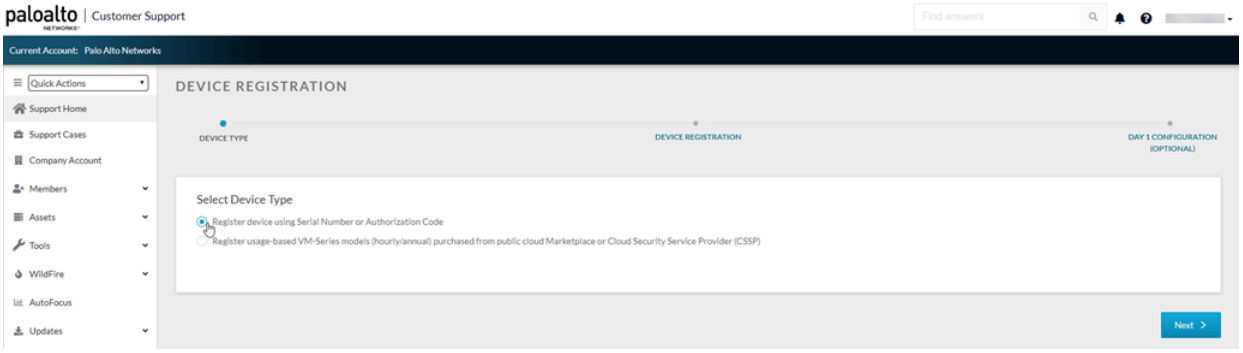


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 이메일 주소를 입력하고 로봇이 아닙니다를 선택한 다음 제출을 클릭합니다.




**STEP 4 |** 일련 번호 또는 인증 코드를 사용하여 디바이스 등록을 선택하고 다음을 클릭합니다.

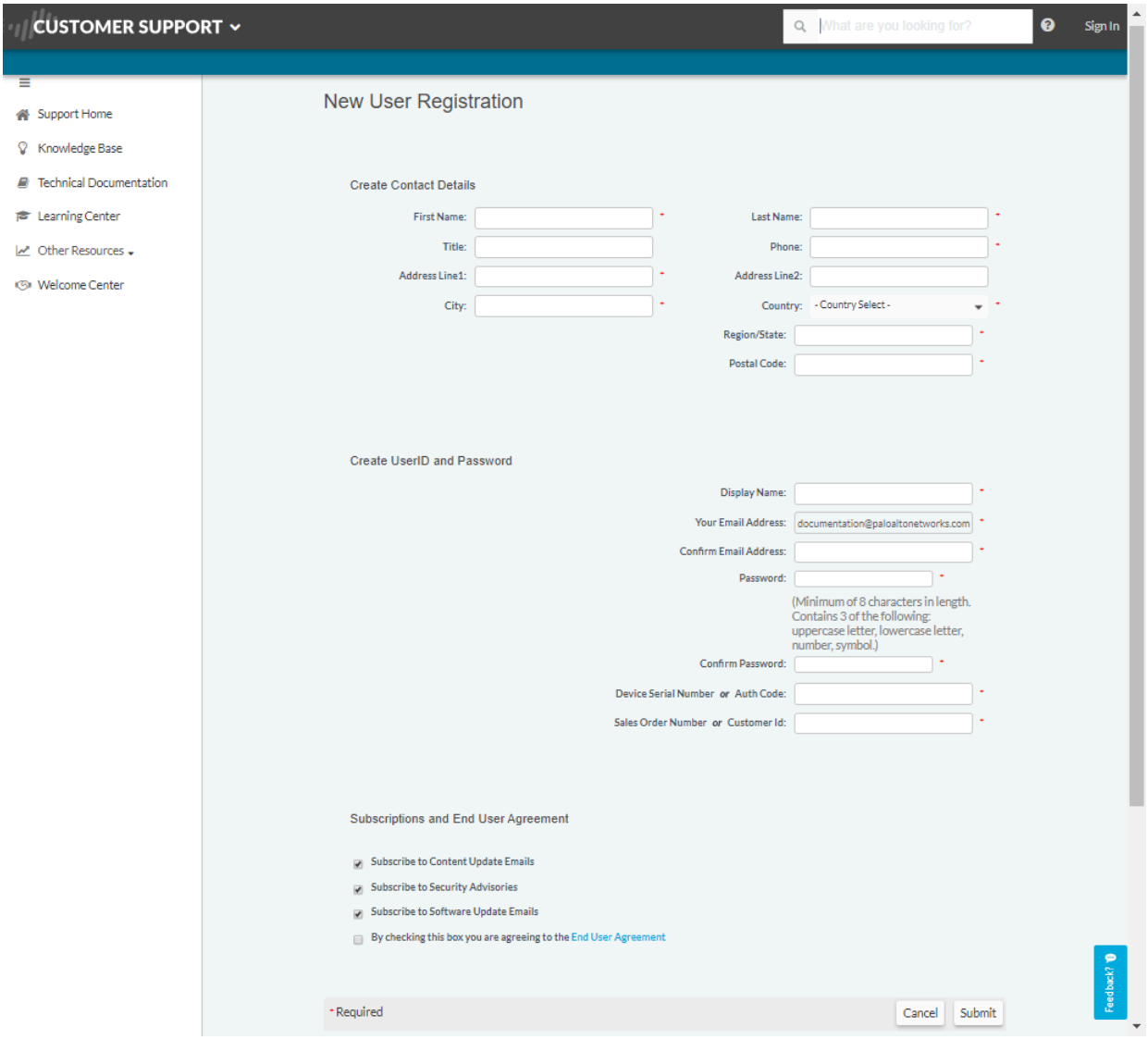




©2023 Palo Alto Networks, Inc.

**STEP 5 |** 등록 양식을 작성하십시오.

1. 이 계정을 소유할 조직 내 사람의 연락처 세부정보를 입력합니다. 필수 필드는 빨간색 별표로 표시됩니다.
2. 계정의 사용자 ID 및 암호를 만듭니다. 필수 필드는 빨간색 별표로 표시됩니다.
3. 디바이스 일련번호 또는 인증 코드를 입력합니다.
4. 판매 주문 번호 또는 고객 **ID**를 입력하십시오.
5. 항상 최신 업데이트 및 보안 권고에 대한 알림을 받을 수 있도록 콘텐츠 업데이트 이메일 구독, 보안 권고 구독 및 소프트웨어 업데이트 이메일 구독을 수행합니다.
6. 최종 사용자 계약에 동의하고 제출하려면 체크박스를 선택합니다.




## 방화벽 등록

활성 Palo Alto Networks 고객 지원 계정이 이미 있는 경우 다음 작업을 수행하여 방화벽을 등록하십시오.


©2023 Palo Alto Networks, Inc.

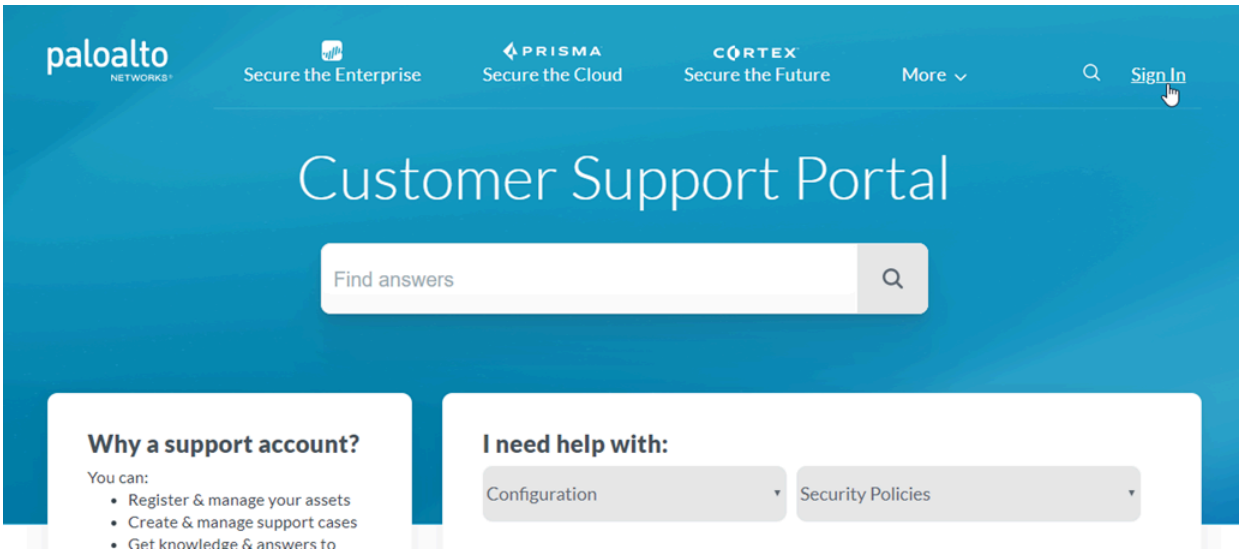
**STEP 1 |** 방화벽 웹 인터페이스에 로그인합니다.

웹 브라우저에서 보안 연결(https)을 사용하여 초기 구성 중에 할당한 새 IP 주소와 암호(https://<IP address>)를 사용하여 로그인합니다.

**STEP 2 |** 일련번호를 찾아 클립보드에 복사합니다.

대시보드 화면의 일반 정보 섹션에서 일련번호를 찾습니다.

**STEP 3 |** Palo Alto Networks 고객 지원 포털로 이동하고 아직 로그인하지 않았다면 지금 로그인하십시오.

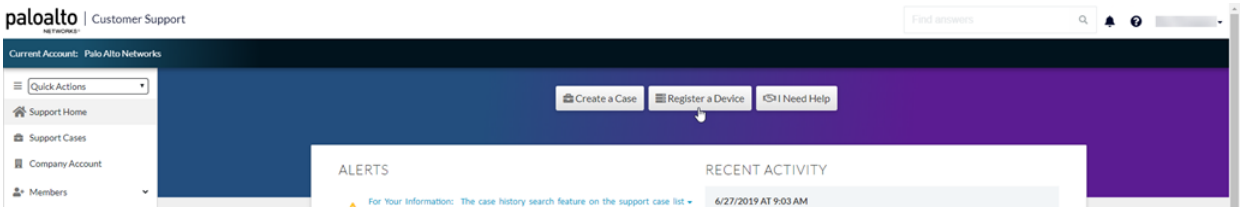




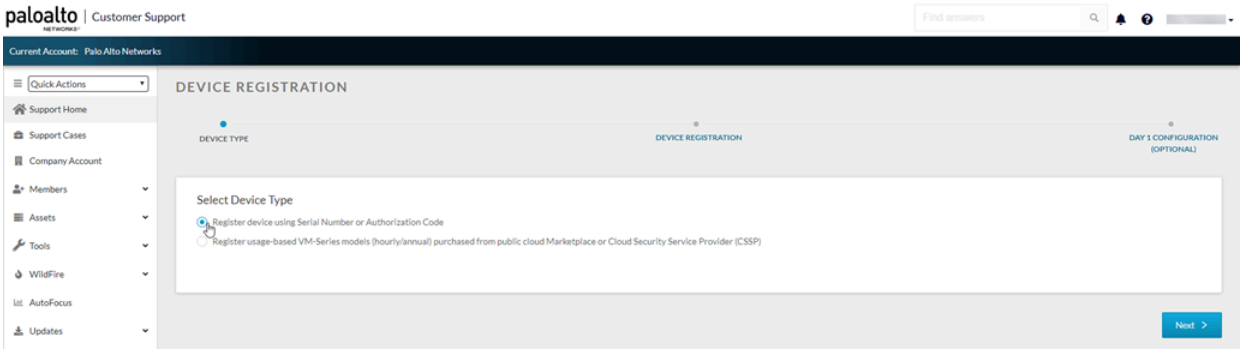
©2023 Palo Alto Networks, Inc.

**STEP 4 |** 방화벽을 등록합니다.

1. 지원 홈 페이지에서 디바이스 등록을 클릭합니다.

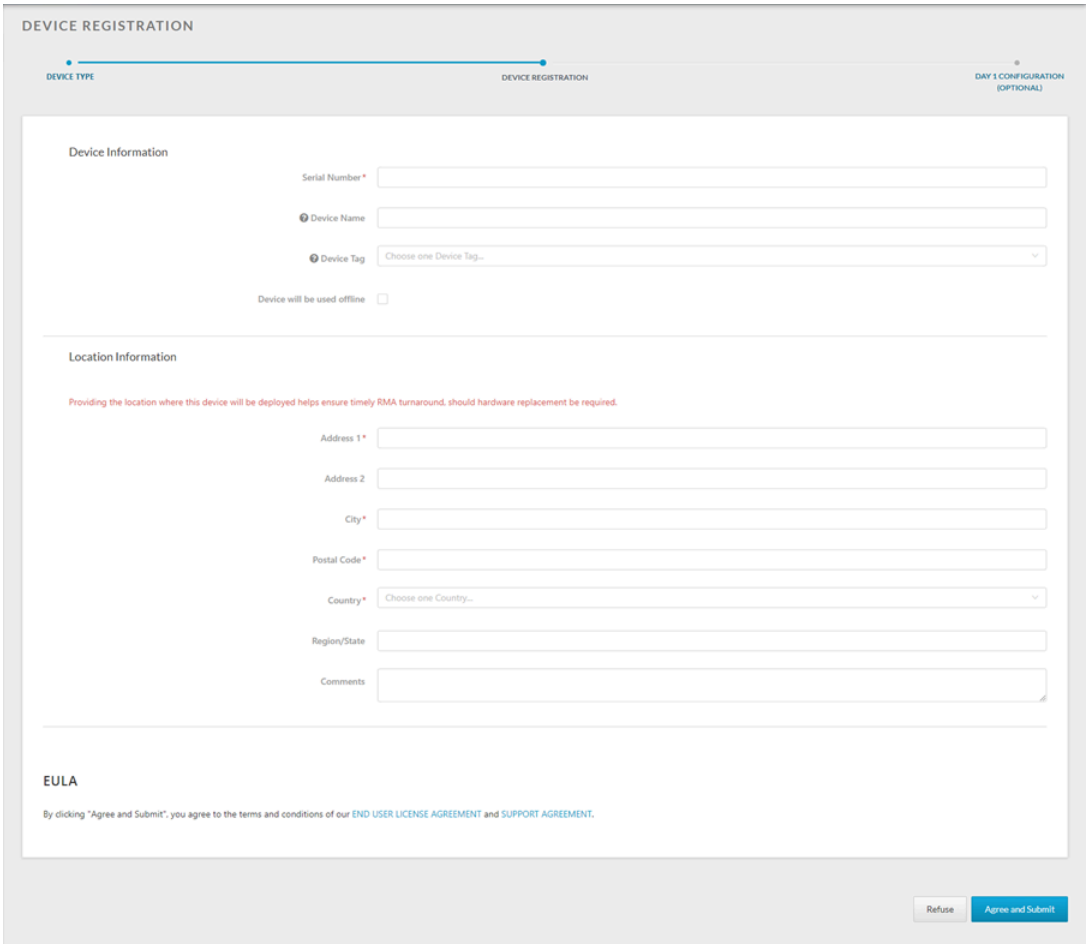



2. 일련 번호 또는 인증 코드를 사용하여 디바이스 등록을 선택한 후 다음을 클릭합니다.




3. 방화벽 일련 번호를 입력합니다(방화벽 대시보드에서 복사하여 붙여넣을 수 있음).
4. (선택사항) 디바이스 이름 및 디바이스 태그를 입력합니다.
5. (선택 사항) 디바이스가 인터넷에 연결되어 있지 않으면 디바이스를 오프라인으로 사용 확인란을 선택한 다음 드롭다운에서 사용하려는 **OS** 릴리스를 선택합니다.
6. 주소, 시, 우편번호 및 국가를 포함하여 방화벽을 배포할 위치에 대한 정보를 제공합니다.
7. 최종 사용자 사용권 계약(EULA) 및 지원 계약을 읽은 다음 동의 및 제출합니다.


©2023 Palo Alto Networks, Inc.




디바이스에서 방금 등록한 방화벽 항목을 볼 수 있습니다.

**STEP 5 |** (라인 카드가 있는 방화벽) 방화벽의 라인 카드에 대한 지원을 받으려면 방화벽 라인 카드 등록을(를) 확인하십시오.

## (선택 사항) Day 1 구성 수행

방화벽을 등록한 후 Day 1 구성을 실행할 수 있습니다. Day 1 구성 도구는 Palo Alto Networks 모범 사례에 따른 구성 템플릿을 제공하며, 이를 시작점으로 사용하여 나머지 구성을 구축할 수 있습니다.

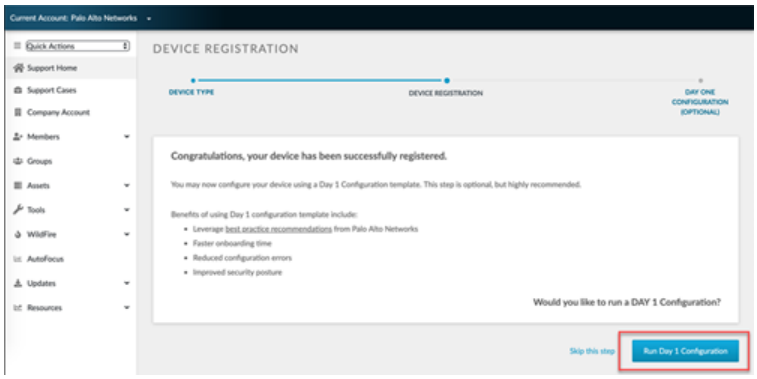
Day 1 구성 템플릿의 이점은 다음과 같습니다.

- 구현 시간 단축
- 구성 오류 감소
- 향상된 보안 태세

다음 단계에 따라 Day 1 구성을 수행하십시오.

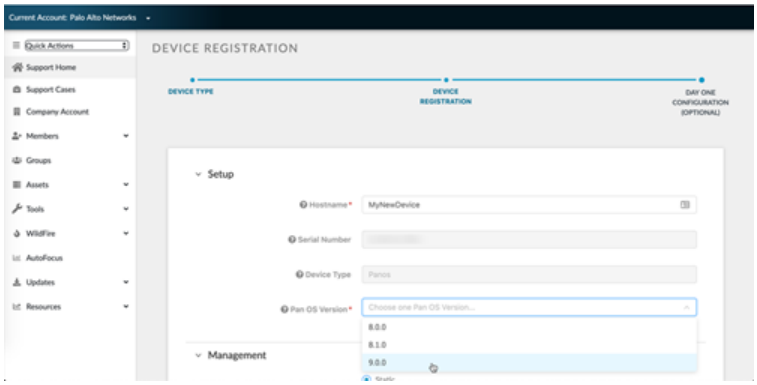

©2023 Palo Alto Networks, Inc.

**STEP 1 |** 방화벽을 등록한 후 표시되는 페이지에서 **Day 1** 구성 실행을 선택합니다.




방화벽을 이미 등록했지만 *Day 1* 구성을 실행하지 않은 경우 도구 > ***Day 1*** 구성 실행을 선택하여 고객 지원 포털 홈 페이지에서 실행할 수도 있습니다.

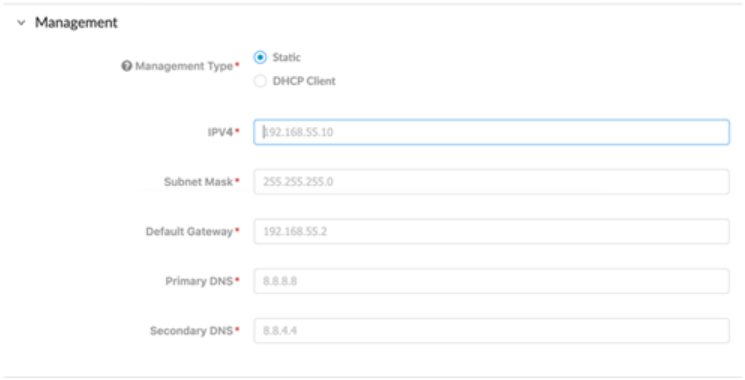
**STEP 2 |** 새 디바이스의 호스트 이름 및 **Pan OS** 버전을 입력하고 선택적으로 일련 번호 및 디바이스 유형을 입력합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 관리에서 관리 유형에 대해 정적 또는 **DHCP** 클라이언트를 선택합니다.

정적을 선택하려면 **IPV4**, 서브넷 마스크 및 기본 게이트웨이 필드를 작성해야 합니다.

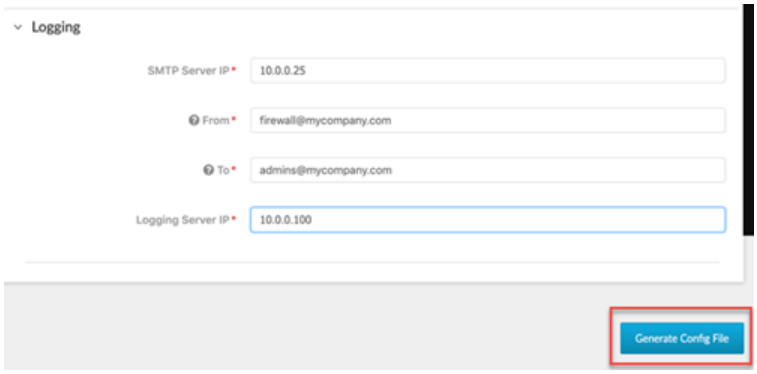



**DHCP** 클라이언트를 선택하려면 기본 **DNS**와 보조 **DNS**만 입력하면 됩니다. DHCP 클라이언트 모드로 구성된 디바이스는 관리 인터페이스가 로컬 DHCP 서버에서 IP 주소를 받도록 하거나 알려진 모든 매개변수를 채웁니다.




**STEP 4 |** 로깅 아래의 모든 필드를 작성하십시오.

**STEP 5 |** 구성 파일 생성을 클릭합니다.

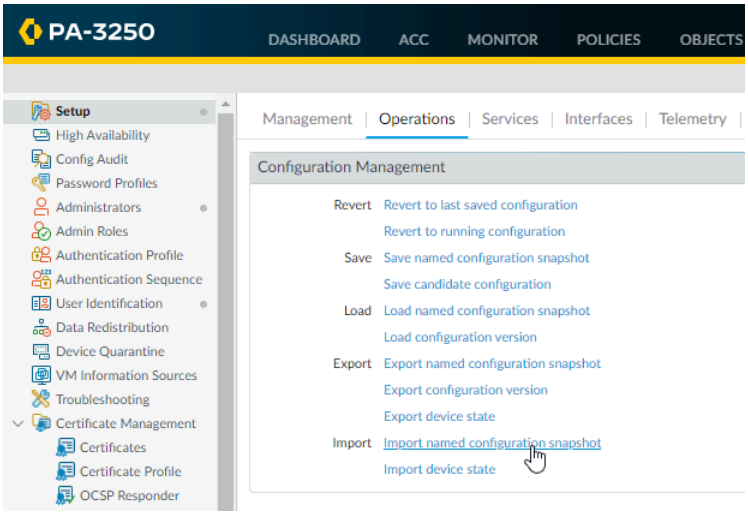




©2023 Palo Alto Networks, Inc.

**STEP 6 |** 방화벽에 다운로드한 Day 1 구성 파일을 가져오고 로드하려면:

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 설정 > 작업을 선택합니다.
3. 명명된 구성 스냅숏 가져오기를 클릭합니다.
4. 파일을 선택합니다.




## 방화벽 라인 카드 등록

다음 방화벽은 문제 해결 및 반품 지원을 받기 위해 등록해야 하는 라인 카드를 사용합니다.

- PA-7000 시리즈 방화벽
- PA-5450 방화벽

Palo Alto Networks 고객 지원 계정이 없는 경우 새 지원 계정 생성 및 방화벽 등록의 단계에 따라 계정을 만드십시오. 고객 지원 계정을 생성하고 방화벽을 등록한 후 이 지침으로 돌아가십시오.

**STEP 1 |** Palo Alto Networks 고객 지원 포털로 이동하고 아직 로그인하지 않았다면 지금 로그인하십시오.

**STEP 2 |** 자산 > 라인 카드/광학/**FRU**를 선택합니다.

**STEP 3 |** 구성 요소를 등록합니다.

**STEP 4 |** 라인 카드의 Palo Alto Networks 판매 주문 번호를 판매 주문 번호 필드에 입력하여 등록 가능한 라인 카드를 표시합니다.

**STEP 5 |** 일련번호 필드에 섀시 일련번호를 입력하여 라인 카드를 방화벽에 등록합니다. 아래의 위치 정보는 방화벽의 등록 정보를 기반으로 자동으로 채워집니다.

**STEP 6 |** 동의 및 제출을 클릭하여 법적 조건에 동의합니다. **Assets** > **Line Cards/Optics/FRUs** 아래에 등록된 라인 카드를 표시하도록 시스템이 업데이트됩니다.


©2023 Palo Alto Networks, Inc.

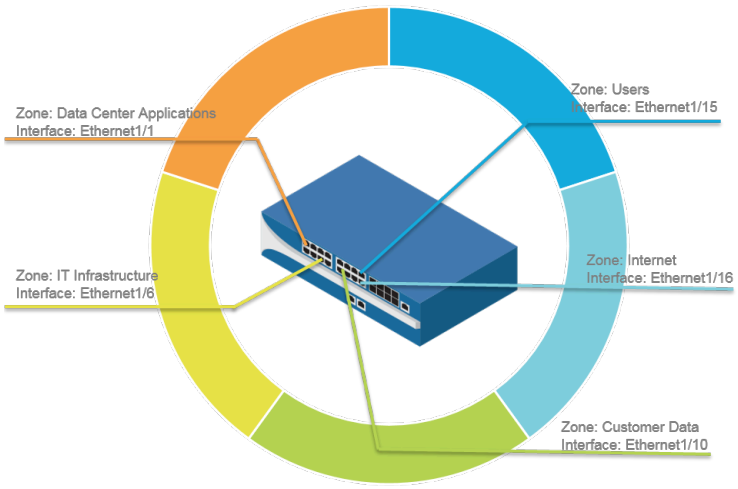
# 인터페이스 및 영역을 사용하여 네트워크 분할

방화벽이 트래픽을 관리하고 제어하려면 트래픽이 방화벽을 통과해야 합니다. 물리적으로 트래픽은 인터페이스를 통해 방화벽에 들어오고 나갑니다. 방화벽은 패킷이 보안 정책 규칙과 일치하는지의 여부에 따라 패킷에서 작동하는 방법을 결정합니다. 가장 기본적인 수준에서 각 보안 정책 규칙은 트래픽의 출처를 식별하고 트래픽의 이동 위치를 식별해야 합니다. Palo Alto Networks의 차세대 방화벽에서는 보안 정책 규칙이 영역 간에 적용됩니다. 영역은 방화벽에 연결되고 방화벽에 의해 제어되는 네트워크 세그먼트를 나타내는 인터페이스(물리적 또는 가상)의 그룹입니다. 트래픽을 허용하는 보안 정책 규칙이 있는 경우 영역 간에만 트래픽이 흐를 수 있으므로 이것이 1차 방어선입니다. 영역을 세분화할수록 민감한 애플리케이션 및 데이터에 대한 액세스에 대한 제어가 강화되고 네트워크 전체에서 측면으로 이동하는 멀웨어에 대한 보호 기능이 강화됩니다. 예를 들어 고객 데이터를 저장하는 데이터베이스 서버에 대한 액세스를 Customer Data라는 영역으로 분할할 수 있습니다. 그런 다음 특정 사용자 또는 사용자 그룹만 고객 데이터 영역에 액세스하도록 허용하는 보안 정책을 정의하여 해당 세그먼트에 저장된 데이터에 대한 무단 내부 또는 외부 액세스를 방지할 수 있습니다.

- 공격 표면 감소에 대한 네트워크 세분화
- 인터페이스 및 영역 구성

## 공격 표면 감소에 대한 네트워크 세분화

다음 다이어그램은 영역을 사용한 네트워크 분할의 매우 기본적인 예를 보여줍니다. 영역(영역 간 트래픽을 허용하는 해당 보안 정책 규칙)을 더 세분화할수록 네트워크의 공격 노출 영역이 줄어듭니다. 트래픽은 영역 내에서 자유롭게 플로우될 수 있지만(영역 내 트래픽) 트래픽은 허용하는 보안 정책 규칙을 정의할 때까지 영역 사이(영역 간 트래픽)에 플로우될 수 없기 때문입니다. 또한 인터페이스는 영역에 할당할 때까지 트래픽을 처리할 수 없습니다. 따라서 네트워크를 세분화된 영역으로 분할하면 민감한 애플리케이션이나 데이터에 대한 액세스를 더 잘 제어할 수 있으며 악의적인 트래픽이 네트워크 내에서 통신 채널을 설정하는 것을 방지할 수 있으므로 네트워크에 대한 공격이 성공할 가능성을 줄일 수 있습니다.




## 인터페이스 및 영역 구성

네트워크를 분할할 방법과 분할을 달성하기 위해 생성해야 하는 영역(각 영역에 매핑할 인터페이스)을 식별한 후에는 방화벽에서 인터페이스 및 영역 구성을 시작할 수 있습니다. 연결하려는 네트워크의 각 부분

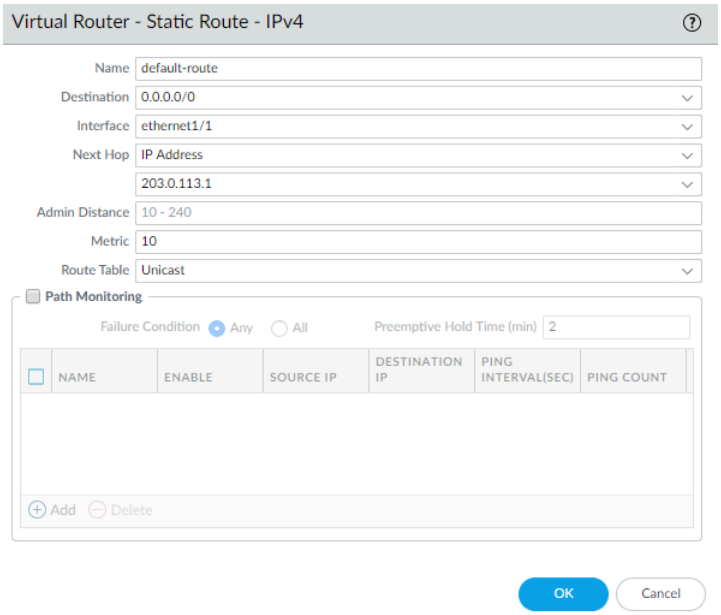

©2023 Palo Alto Networks, Inc.

에 대한 토폴로지를 지원하도록 방화벽에서 인터페이스를 구성합니다. 다음 워크플로는 레이어 3 인터페이스를 구성하고 영역에 할당하는 방법을 보여줍니다. 다른 유형의 인터페이스 배포(예: 가상 와이어 인터페이스 또는 레이어 2 인터페이스)를 사용하여 방화벽을 통합하는 방법에 대한 자세한 내용은 PAN-OS 네트워킹 관리자 가이드를 참조하십시오.

방화벽은 이더넷 *1/1*과 이더넷 *1/2*(및 해당 기본 보안 정책 및 가상 라우터*)* 포트 간의 기본 가상 와이어 인터페이스로 사전 구성되어 제공됩니다. 기본 가상 와이어를 사용하지 않으려는 경우 계속 진행하기 전에 수동으로 구성을 삭제하고 변경 사항을 커밋하여 정의한 다른 설정을 방해하지 않도록 해야 합니다. 기본 가상 회선 및 관련 보안 정책 및 영역을 삭제하는 방법에 대한 지침은 외부 서비스에 대한 네트워크 액세스 설정의 *3*단계를 참조하십시오.

**STEP 1 |** 인터넷 라우터에 대한 기본 경로를 구성합니다.

1. 네트워크 > 가상 라우터를 선택한 다음 기본 링크를 선택하여 가상 라우터 대화 상자를 엽니다.
2. 정적 경로탭을 선택하고추가를 클릭합니다. 경로 이름을 입력하고 대상 필드에 경로를 입력합니다(예: 0.0.0.0/0).
3. 다음 홉 필드에서 **IP** 주소 라디오 버튼을 선택한 다음 인터넷 게이트웨이의 IP 주소와 넷마스크(예: 203.0.113.1)를 입력합니다.

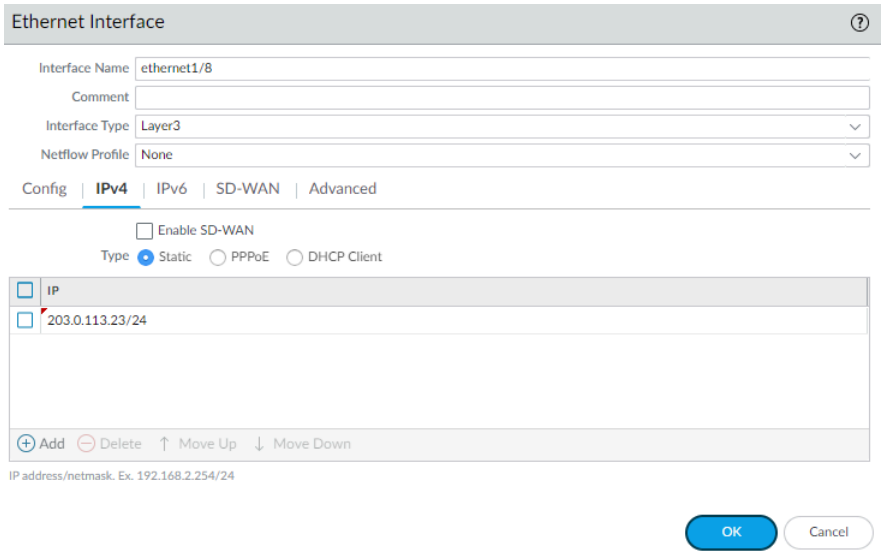



4. 확인을 두 번 클릭하여 가상 라우터 구성을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 외부 인터페이스(인터넷에 연결하는 인터페이스)를 구성합니다.

1. 네트워크 > 인터페이스를 선택한 다음 구성할 인터페이스를 선택합니다. 이 예에서는 Ethernet1/8을 외부 인터페이스로 구성하고 있습니다.
2. 인터페이스 유형을 선택합니다. 여기에서 선택은 인터페이스 토폴로지에 따라 다르지만 이 예에서는 **Layer3**에 대한 단계를 보여줍니다.
3. 구성 탭의 보안 영역 드롭다운에서 새 영역을 선택합니다. 영역 대화 상자에서 새 영역의 이름(예: 인터넷)을 정의한 다음 확인을 클릭합니다.
4. 가상 라우터드롭다운에서기본값을 선택합니다.
5. 인터페이스에 IP 주소를 할당하려면 **IPv4** 탭을 선택한 다음 IP 섹션에서 추가를 클릭한 다음 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 203.0.113.23/24).




6. 인터페이스를 핑(ping)할 수 있도록 하려면 고급 > 기타 정보를 선택한 다음 관리 프로파일 드롭다운을 확장한 다음 새 관리 프로파일을 선택합니다. 프로파일의 이름을 입력하고 핑**(ping)**을 선택한 다음 확인을 클릭합니다.
7. 인터페이스 구성을 저장하려면 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 내부 네트워크에 연결하는 인터페이스를 구성합니다.

이 예에서 인터페이스는 개인 ***IP*** 주소를 사용하는 네트워크 세그먼트에 연결합니다. 사설 ***IP*** 주소는 외부로 라우팅할 수 없으므로 NAT를 구성해야 합니다.

1. 네트워크 > 인터페이스를 선택한 다음 구성할 인터페이스를 선택합니다. 이 예에서는 사용자가 연결하는 내부 인터페이스로 Ethernet1/15를 구성하고 있습니다.
2. 인터페이스 유형으로 **Layer3**을 선택합니다.
3. 구성 탭에서 보안 영역 드롭다운을 확장하고 새 영역을 선택합니다. 영역 대화 상자에서 새 영역의 이름(예: 사용자)을 정의한 다음 확인을 클릭합니다.
4. 이전에 사용한 것과 동일한 가상 라우터(이 예에서는 기본값)를 선택합니다.
5. 인터페이스에 IP 주소를 할당하려면 **IPv4** 탭을 선택한 다음 IP 섹션에서 추가를 클릭한 다음 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 192.168.1.4/24).
6. 인터페이스를 핑(ping)할 수 있도록 하려면 방금 생성한 관리 프로파일을 선택합니다.
7. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

**STEP 4 |** 데이터 센터 애플리케이션에 연결하는 인터페이스를 구성합니다.

민감한 애플리케이션이나 데이터에 대한 무단 액세스를 방지하고 데이터 센터 내에서 맬웨어가 측면으로 이동할 가능성을 제거하기 위해 세분화된 영역을 정의해야 합니다.

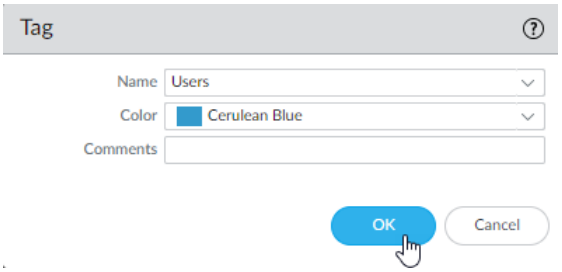
1. 구성할 인터페이스를 선택합니다.
2. 인터페이스 유형 드롭다운에서 **Layer3**을 선택합니다. 이 예에서는 데이터 센터 애플리케이션에 대한 액세스를 제공하는 인터페이스로 Ethernet1/1을 구성하고 있습니다.
3. 구성 탭에서 보안 영역 드롭다운을 확장하고 새 영역을 선택합니다. 영역 대화 상자에서 새 영역의 이름(예: 데이터 센터 애플리케이션)을 정의한 다음 확인을 클릭합니다.
4. 이전에 사용한 것과 동일한 가상 라우터(이 예에서는 기본값)를 선택합니다.
5. 인터페이스에 IP 주소를 할당하려면 **IPv4** 탭을 선택한 다음 IP 섹션에서 추가를 클릭한 다음 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 10.1.1.1/24).
6. 인터페이스를 핑(ping)할 수 있도록 하려면 생성한 관리 프로파일을 선택합니다.
7. 인터페이스 구성을 저장하려면 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** (선택 사항) 각 영역에 대한 태그를 생성합니다.

태그를 사용하면 정책 규칙을 시각적으로 스캔할 수 있습니다.

1. 개체 > 태그를 선택한 다음 추가합니다.
2. 영역 이름을 선택합니다.
3. 태그 색상을 선택한 다음 확인을 클릭합니다.




**STEP 6 |** 인터페이스 구성을 저장합니다.

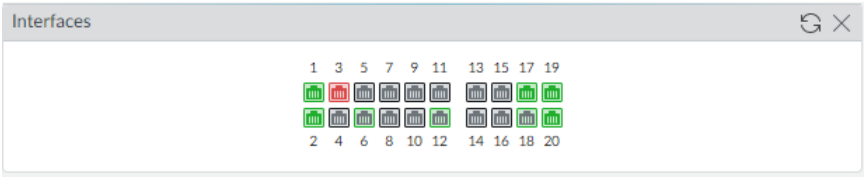
커밋을 클릭합니다.

**STEP 7 |** 방화벽에 케이블을 연결합니다.

구성한 인터페이스에서 각 네트워크 세그먼트의 해당 스위치 또는 라우터에 케이블을 통해 직접 연결합니다.

**STEP 8 |** 인터페이스가 활성 상태인지 확인합니다.

대시보드를 선택한 다음 구성한 인터페이스가 인터페이스 위젯에서 녹색으로 표시되는지 확인합니다.





©2023 Palo Alto Networks, Inc.

# 기본 보안 정책 설정

일부 영역을 정의하고 인터페이스에 연결했으므로 이제 보안 정책 생성을 시작할 준비가 되었습니다. 방화벽은 트래픽을 허용하는 보안 정책 규칙이 있는 경우를 제외하고 한 영역에서 다른 영역으로의 트래픽 플로우를 허용하지 않습니다. 패킷이 방화벽 인터페이스에 들어가면 방화벽은 패킷의 속성을 보안 정책 규칙과 비교하여 속성을 기반으로 소스 및 대상 보안 영역, 소스 및 대상 IP 주소, 애플리케이션, 사용자, 서비스 등의 세션을 차단할지 허용할지 결정합니다. 방화벽은 보안 정책 규칙 베이스에 대해 왼쪽에서 오른쪽으로, 위에서 아래로 들어오는 트래픽을 평가한 다음 일치하는 첫 번째 보안 규칙에 지정된 작업(예: 패킷 허용, 거부 또는 삭제 여부)을 수행합니다. 즉, 방화벽이 예상대로 정책을 시행할 수 있도록 보다 구체적인 규칙이 규칙 베이스의 맨 위에 있고 보다 일반적인 규칙이 맨 아래에 있도록 보안 정책 규칙 베이스의 규칙을 정렬해야 합니다.

보안 정책 규칙이 패킷을 허용하더라도 트래픽에 위협이 없는 것은 아닙니다. 방화벽이 보안 정책 규칙에 따라 허용하는 트래픽을 검색할 수 있도록 하려면 각 규칙(사용할 수 있는 프로파일은 구입한 구독에 따라 다름)에 URL 필터링, 안티바이러스, 안티스파이웨어, 파일 차단 및 WildFire 분석을 포함한 보안 프로파일도 추가해야 합니다. 기본 보안 정책을 생성할 때 사전 정의된 보안 프로파일을 사용하여 네트워크에 허용된 트래픽에 위협이 있는지 검사합니다. 나중에 필요에 따라 이러한 프로파일을 사용자 환경에 맞게 사용자 지정할 수 있습니다.

다음 워크플로를 사용하여 네트워크 인프라, 데이터 센터 애플리케이션 및 인터넷에 대한 액세스를 가능하게 하는 매우 기본적인 보안 정책을 설정합니다. 이렇게 하면 방화벽을 설정하고 실행할 수 있으므로 방화벽을 성공적으로 구성했는지 확인할 수 있습니다. 그러나 이 초기 정책은 네트워크를 보호할 만큼 포괄적이지 않습니다. 방화벽을 성공적으로 구성하고 네트워크에 통합했는지 확인한 후에는 공격으로부터 네트워크를 보호하면서 애플리케이션 액세스를 안전하게 활성화하는 모범 사례 인터넷 게이트웨이 보안 정책을 생성합니다.

**STEP 1 |** (선택 사항) 기본 보안 정책 규칙을 삭제합니다.

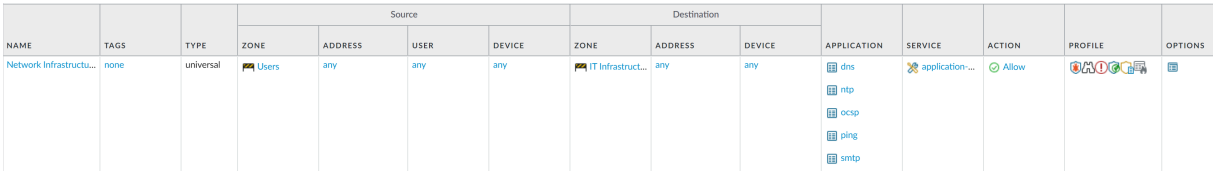
기본적으로 방화벽에는 트러스트 영역에서 언트러스트 영역으로의 모든 트래픽을 허용하는 ***rule1***이라는 보안 정책 규칙이 포함되어 있습니다. 규칙을 삭제하거나 영역 명명 규칙을 반영하도록 규칙을 수정할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 네트워크 인프라 리소스에 대한 액세스를 허용합니다.

1. 정책 > 보안을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. 소스 탭에서 소스 영역을 사용자로 설정합니다.
4. 대상 탭에서 대상 영역을 **IT** 인프라로 설정합니다.

   가장 좋은 방법은 대상 주소 필드의 주소 개체를 사용하여 특히 일반적으로 악용되는 *DNS* 및 *SMTP*와 같은 서비스에 대해서만 특정 서버 또는 서버 그룹에 대한 액세스를 활성화하는 것입니다. 사용자를 특정 대상 서버 주소로 제한하면 데이터 유출과 명령 및 제어 트래픽이 *DNS* 터널링과 같은 기술을 통해 통신을 설정하는 것을 방지할 수 있습니다.
5. 애플리케이션 탭에서 안전하게 활성화하려는 네트워크 서비스에 해당하는 애플리케이션을 추가합니다. 예를 들어, **dns**, **ntp**, **ocsp**, **ping** 및 **smtp**를 선택합니다.
6. 서비스/**URL** 카테고리 탭에서 서비스를 **application-default**로 설정된 상태로 유지합니다.
7. 작업 탭에서 작업 설정을 허용으로 설정합니다.
8. 프로파일 유형을 프로파일로 설정하고 정책 규칙에 연결할 다음 보안 프로파일을 선택합니다.
   - 바이러스 백신의 경우 기본값을 선택합니다.
   - 취약성 보호에 대해 강력을 선택하십시오.
   - 안티스파이웨어의 경우 강력을 선택합니다.
   - **URL** 필터링의 경우 기본값을 선택합니다.
   - 파일 차단의 경우 기본 파일 차단을 선택합니다.
   - **WildFire** 분석의 경우 기본값을 선택합니다.
9. 세션 종료 시 로그가 활성화되어 있는지 확인합니다. 보안 정책 규칙과 일치하는 트래픽만 기록됩니다.
10. 확인을 클릭합니다.

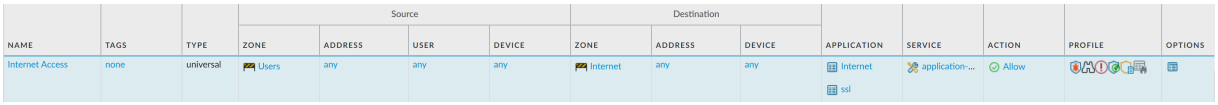



 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 일반 인터넷 애플리케이션에 대한 액세스를 활성화합니다.

이것은 네트워크의 트래픽에 대한 정보를 수집할 수 있는 임시 규칙입니다. 사용자가 액세스해야 하는 애플리케이션에 대해 더 많은 정보를 얻은 후에는 허용할 애플리케이션에 대해 정보에 입각한 결정을 내리고 각 사용자 그룹에 대해 보다 세분화된 애플리케이션 기반 규칙을 만들 수 있습니다.

1. 정책 > 보안을 선택하고 규칙을 추가합니다.
2. 일반 탭에서 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. 소스 탭에서 소스 영역을 사용자로 설정합니다.
4. 대상 탭에서 대상 영역을 인터넷으로 설정합니다.
5. 애플리케이션 탭에서 애플리케이션 필터를 추가하고 이름을 입력합니다. 합법적인 웹 기반 애플리케이션에 안전하게 액세스하려면 애플리케이션 필터의 카테고리를 일반 인터넷으로 설정한 다음 확인을 클릭합니다. 암호화된 사이트에 대한 액세스를 활성화하려면 **ssl** 애플리케이션을 추가합니다.
6. 서비스/**URL** 카테고리 탭에서 서비스를 **application-default**로 설정된 상태로 유지합니다.
7. 작업 탭에서 작업 설정을 허용으로 설정합니다.
8. 프로파일 유형을 프로파일로 설정하고 정책 규칙에 연결할 다음 보안 프로파일을 선택합니다.
   - 바이러스 백신의 경우 기본값을 선택합니다.
   - 취약성 보호에 대해 강력을 선택하십시오.
   - 안티스파이웨어의 경우 강력을 선택합니다.
   - **URL** 필터링의 경우 기본값을 선택합니다.
   - 파일 차단의 경우 엄격한 파일 차단을 선택합니다.
   - **WildFire** 분석의 경우 기본값을 선택합니다.
9. 세션 종료 시 로그가 활성화되어 있는지 확인합니다. 보안 규칙과 일치하는 트래픽만 기록됩니다.
10. 확인을 클릭합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 데이터 센터 애플리케이션에 대한 액세스를 활성화합니다.

1. 정책 > 보안을 선택하고 규칙을 추가합니다.
2. 일반 탭에서 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. 소스 탭에서 소스 영역을 사용자로 설정합니다.
4. 대상 탭에서 대상 영역을 데이터 센터 애플리케이션으로 설정합니다.
5. 애플리케이션 탭에서 안전하게 활성화하려는 네트워크 서비스에 해당하는 애플리케이션을 추가합니다. 예를 들어 **activesync**, **imap**, **kerberos**, **ldap**, **ms-exchange** 및 **ms-lync**을 선택합니다.
6. 서비스/**URL** 카테고리 탭에서 서비스를 **application-default**로 설정된 상태로 유지합니다.
7. 작업 탭에서 작업 설정을 허용으로 설정합니다.
8. 프로파일 유형을 프로파일로 설정하고 정책 규칙에 연결할 다음 보안 프로파일을 선택합니다.
   - 바이러스 백신의 경우 기본값을 선택합니다.
   - 취약성 보호의 경우 강력을 선택하십시오.
   - **Anti-Spyware**의 경우 강력을 선택하십시오.
   - **URL** 필터링의 경우 기본값 선택
   - 파일 차단의 경우 기본 파일 차단을 선택합니다.
   - **WildFire** 분석의 경우 기본값을 선택합니다.
9. 세션 종료 시 로그가 활성화되어 있는지 확인합니다. 보안 규칙과 일치하는 트래픽만 기록됩니다.
10. 확인을 클릭합니다.

| | | | Source | | | | Destination | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| NAME | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | ACTION | PROFILE | OPTIONS |
| Data Center Applica... | none | universal | Users | any | any | any | Datacenter ... | any | any | activesync<br>imap<br>kerberos<br>ldap<br>ms-exchange<br>ms-lync | application-... | Allow | | |

**STEP 5 |** 방화벽에서 실행 중인 구성에 정책 규칙을 저장합니다.

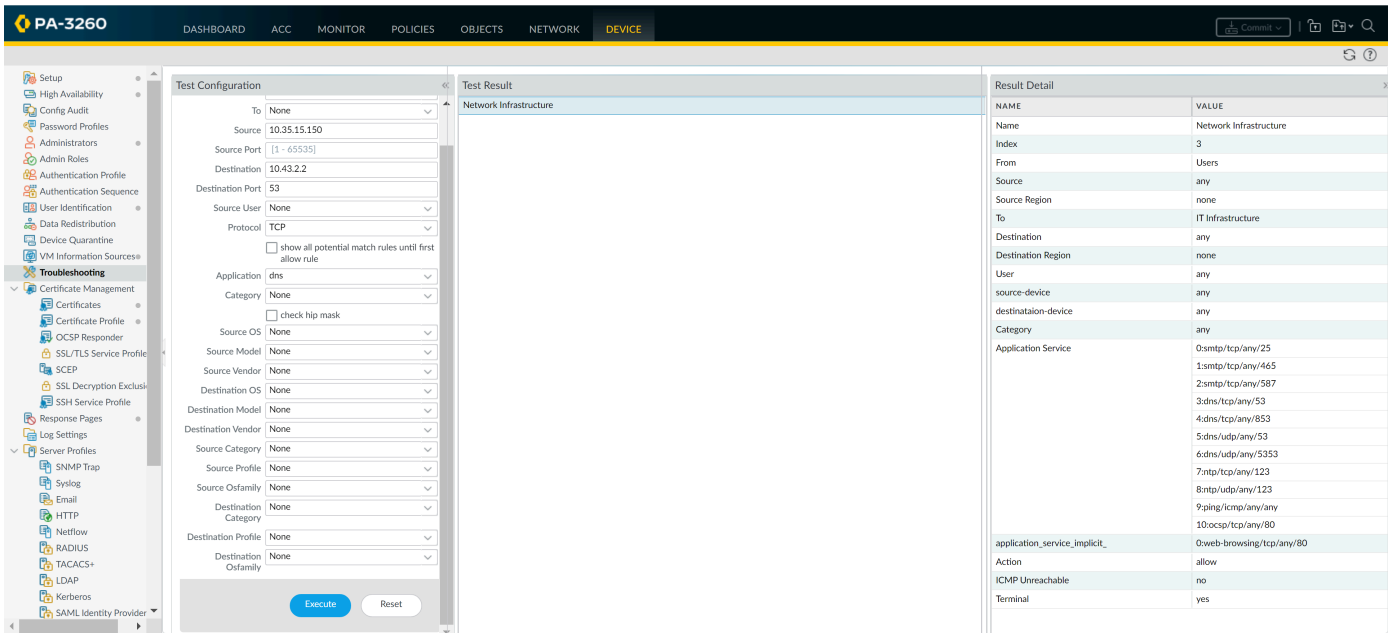
커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 기본 정책을 효과적으로 설정했는지 확인하려면 보안 정책 규칙이 평가되고 있는지 테스트하고 트래픽 플로우에 적용되는 보안 정책 규칙을 결정하십시오.

예를 들어 데이터 센터의 DNS 서버에 DNS 쿼리를 보낼 때 IP 주소가 10.35.14.150인 사용자 영역의 클라이언트에 적용될 정책 규칙을 확인하려면 다음을 수행합니다.

1. 디바이스 > 문제 해결을 선택하고 보안 정책 일치를 선택합니다(테스트 선택).
2. 소스 및 대상 IP 주소를 입력합니다.
3. 프로토콜을 입력합니다.
4. **dns** 선택(애플리케이션)
5. 보안 정책 일치 테스트를 실행합니다.




 ©2023 Palo Alto Networks, Inc.

# 네트워크 트래픽 평가

이제 기본 보안 정책이 있으므로 ACC(애플리케이션 명령 센터) 통계 및 데이터, 트래픽 로그 및 위협 로그를 검토하여 네트워크의 추세를 관찰할 수 있습니다. 이 정보를 사용하여 보다 세분화된 보안 정책 규칙을 만들어야 하는 위치를 식별합니다.

- 애플리케이션 명령 센터를 사용하고 자동화된 상관 관계 엔진을 사용합니다.

  ACC에서 네트워크에서 가장 많이 사용되는 애플리케이션과 고위험 애플리케이션을 검토합니다. ACC는 로그 정보를 그래픽으로 요약하여 네트워크를 통과하는 애플리케이션, 네트워크를 사용하는 애플리케이션(사용자 ID 사용 가능) 및 네트워크에서 발생하는 문제를 실시간으로 식별하는 데 도움이 되는 콘텐츠의 잠재적 보안 영향을 강조 표시합니다. 그런 다음 이 정보를 사용하여 원치 않는 애플리케이션을 차단하는 적절한 보안 정책 규칙을 만드는 동시에 애플리케이션을 안전한 방식으로 허용하고 사용하도록 설정합니다.

  **ACC** > 위협 활동의 손상된 호스트 위젯은 네트워크의 잠재적으로 손상된 호스트와 이벤트를 확증하는 로그 및 일치 증거를 표시합니다.

- 네트워크 보안 정책 규칙에 필요한 업데이트/수정사항을 확인하고 변경 사항을 구현합니다.

  예:

  - 일정, 사용자 또는 그룹에 따라 웹 콘텐츠를 허용할지의 여부를 평가합니다.
  - 애플리케이션 내에서 특정 애플리케이션 또는 기능을 허용하거나 제어할 수 있습니다.
  - 콘텐츠를 해독하고 검사합니다.
  - 위협과 악용을 허용하지만 스캔합니다.

  보안 정책을 구체화하고 사용자 지정 보안 프로파일을 첨부하는 방법에 대한 자세한 내용은 보안 정책 규칙 및 보안 프로파일을 만드는 방법을 참조하십시오.

- 로그 보기.

  구체적으로 트래픽 및 위협 로그를 봅니다(로그 > 모니터).

  트래픽 로그는 보안 정책을 정의하고 트래픽을 기록하도록 설정하는 방법에 따라 달라집니다. 그러나 ***ACC***의 애플리케이션 사용 위젯은 정책 구성에 관계없이 애플리케이션 및 통계를 기록하므로 네트워크에서 허용되는 모든 트래픽을 표시하므로 정책에서 허용되는 영역 간 트래픽과 암시적으로 허용되는 동일한 영역 트래픽이 포함됩니다.

- 로그 스토리지 할당량 및 만료 기간을 구성합니다.

  로그의 아티팩트에 대한 AutoFocus 인텔리전스 요약을 검토합니다. 아티팩트는 방화벽에서 기록된 이벤트와 관련된 항목, 속성, 활동 또는 동작입니다. 인텔리전스 요약은 WildFire가 아티팩트를 감지한 세

 ©2023 Palo Alto Networks, Inc.

션 및 샘플 수를 보여줍니다. WildFire 평결 정보(양성, 그레이웨어, 맬웨어) 및 AutoFocus 매칭 태그를 사용하여 네트워크의 잠재적 위험을 확인합니다.



***Palo Alto Networks*** 위협 인텔리전스 팀인 Unit 42에서**,** 만든 ***AutoFocus*** 태그는 네트워크의 고급 타겟 캠페인 및 위협에 주의를 환기시합니다**.**

AutoFocus 인텔리전스 요약에서 아티팩트에 대한 AutoFocus 검색을 시작하고 전역, 산업 및 네트워크 컨텍스트 내에서 해당 보급성을 평가할 수 있습니다.

- 네트워크 사용자의 웹 활동 모니터링.

  URL 필터링 로그를 검토하여 경고, 거부된 카테고리/URL을 검색합니다. URL 로그는 트래픽이 경고, 계속, 재정의 또는 블록 동작과 연결된 URL 필터링 프로파일이 있는 보안 규칙과 일치할 때 생성됩니다.


©2023 Palo Alto Networks, Inc.

# 무료 WildFire 포워딩 가능

WildFire는 알 수 없는 샘플(파일 및 이메일 링크)을 분석 및 실행하고 악성, 피싱, 그레이웨어(grayware) 또는 양성으로 샘플을 판별하는 클라우드 기반 가상 환경입니다. WildFire를 활성화하면 Palo Alto Networks 방화벽이 분석을 위해 알려지지 않은 샘플을 WildFire로 포워딩할 수 있습니다 새로 발견된 멀웨어의 경우 WildFire는 멀웨어를 탐지하는 서명을 생성합니다. 이 서명은 활성 WildFire 구독이 있는 모든 방화벽에 대해 실시간으로 검색할 수 있습니다. 이를 통해 전 세계의 모든 Palo Alto 차세대 방화벽이 단일 방화벽에서 발견한 멀웨어를 탐지하고 예방할 수 있습니다. 멀웨어 서명은 종종 동일한 멀웨어 계열의 여러 변종과 일치하므로 방화벽에서 이전에는 볼 수 없었던 새로운 멀웨어 변종을 차단합니다. Palo Alto Networks 위협 연구팀은 악성코드 변종에서 수집한 위협 인텔리전스를 사용하여 악성 IP 주소, 도메인 및 URL을 차단합니다.

기본 WildFire 서비스는 Palo Alto Networks 차세대 방화벽의 일부로 포함되어 있으며 WildFire 구독이 필요하지 않습니다. 기본 WildFire 서비스를 사용하면 방화벽이 이동식 실행 파일(PE)을 포워딩하도록 설정할 수 있습니다. 또한 WildFire 구독이 없지만 위협 방지 구독이 있는 경우 바이러스 백신 업데이트의 일부로 24-48시간마다 WildFire가 식별하는 멀웨어에 대한 서명을 받을 수 있습니다.

기본 WildFire 서비스 외에도 방화벽을 사용하려면 WildFire 구독이 필요합니다.

- 실시간으로 최신 WildFire 서명을 받아보세요.
- 악성 PE(휴대용 실행 파일), ELF 및 MS Office 파일, PowerShell 및 셸 스크립트가 를 사용하여 WildFire Inline ML실시간으로 네트워크에 들어오는 것을 방지합니다.
- 분석을 위해 Advanced 파일 형식 및 이메일 링크를 포워딩합니다.
- WildFire API를 사용합니다.
- WildFire 어플라이언스를 사용하여 WildFire 프라이빗 클라우드 또는 WildFire 하이브리드 클라우드를 호스팅

WildFire 구독이 있는 경우 WildFire를 시작하여 구독을 최대한 활용하십시오. 그렇지 않으면 다음 단계를 수행하여 기본 WildFire 포워딩을 사용하도록 설정합니다.

**STEP 1 |** 방화벽이 등록되어 있고 유효한 지원 계정과 필요한 구독이 있는지 확인합니다.

1. Palo Alto Networks CSP(고객 지원 포털)에 로그인하고 왼쪽 탐색 창에서 자산 > 디바이스를 선택합니다.
2. 방화벽이 나열되는지 확인합니다. 목록에 없으면 새 디바이스 등록을 선택한 다음 방화벽 등록을 계속합니다.
3. (선택 사항) 위협 방지 구독이 있는 경우 구독 라이선스 활성화.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽에 로그인하고 WildFire 포워딩 설정을 구성합니다.

1. 디바이스 > 설정 > **WildFire**를 선택한 다음 일반 설정을 편집합니다.
2. 파일을 **WildFire** 글로벌 클라우드(미국)에 포워딩하도록 **`wildfire.paloaltonetworks.com`**에 WildFire 퍼블릭 클라우드 필드를 설정합니다.

   또한 위치 및 조직의 요구 사항에 따라 파일을 ***WildFire*** 리전 클라우드 또는 프라이빗 클라우드로 포워딩할 수 있습니다.
3. WildFire 분석을 위해 방화벽이 포워딩하는 PE의 파일 크기 제한을 검토합니다. 방화벽이 포워딩할 수 있는 PE의 크기 제한을 10MB까지 설정합니다.

   WildFire 모범 사례로 ***PE***의 크기 제한을 사용 가능한 최대 제한인 ***10MB***로 설정합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 3 |** 방화벽이 분석을 위해 PE를 포워딩하도록 설정합니다.

1. 개체 > 보안 프로파일 > **WildFire** 분석 및 새 프로파일 규칙 추가를 선택합니다.
2. 새 프로파일 규칙의 이름을 지정합니다.
3. 포워딩 규칙을 추가하고 이름을 입력합니다.
4. 파일 형식 열에서 포워딩 규칙에 **pe** 파일을 추가합니다.
5. 분석 열에서 퍼블릭 클라우드를 선택하여 PE를 WildFire 퍼블릭 클라우드로 포워딩합니다.
6. 확인을 클릭합니다.

**STEP 4 |** 방화벽에서 허용하는 트래픽에 새 WildFire 분석 프로파일을 적용합니다.

1. 정책 > 보안을 선택한 다음 기존 정책 규칙을 선택하거나 기본 보안 정책 설정에 설명된 대로 새 정책 규칙을 생성합니다.
2. 작업을 선택한 다음 프로파일 설정 섹션에서 프로파일 유형을 프로파일로 설정합니다.
3. 방금 만든 **WildFire Analysis** 프로파일을 선택하여 이 정책 규칙이 허용하는 모든 트래픽에 해당 프로파일 규칙을 적용합니다.
4. 확인을 클릭합니다.

**STEP 5 |** WildFire 분석을 위해 방화벽이 복호화된 SSL 트래픽을 포워딩하도록 설정합니다.

**STEP 6 |** WildFire 모범 사례를 검토하고 구현하여 WildFire 탐지 및 예방 기능을 최대한 활용하고 있는지 확인합니다.

**STEP 7 |** 구성 업데이트를 커밋합니다.

**STEP 8 |** 방화벽이 PE 파일을 WildFire 퍼블릭 클라우드로 포워딩하는지 확인합니다.

WildFire 분석을 위해 방화벽이 성공적으로 제출한 PE에 대한 로그 항목을 보려면 로그 > **WildFire** 제출 > 모니터링을 선택합니다. 평결 열에는 WildFire가 PE를 악성, 그레이웨어 또는 양성으로 발견했는지의 여부가 표시됩니다. WildFire는 이메일 링크에만 피싱 판결을 할당합니다. Action 열은 방화벽에서 샘플을 허용하는지 아니면 차단했는지를 나타냅니다. 심각도 열은 샘플이 중요, 높음, 보통, 낮음, 정보 등의 값을 사용하여 조직에 제기하는 위협의 양을 나타냅니다.


©2023 Palo Alto Networks, Inc.

**STEP 9 |** (위협 방지 구독만 해당) 위협 차단 구독이 있지만 WildFire 구독이 없는 경우에도 24~48시간마다 WildFire 서명 업데이트를 받을 수 있습니다.

1. 디바이스 > 동적 업데이트를 선택합니다.
2. 방화벽이 다운로드되도록 예약되어 있는지 확인하고 안티바이러스 업데이트를 설치합니다.


©2023 Palo Alto Networks, Inc.

# 방화벽 배포를 완료하기 위한 모범 사례

방화벽을 네트워크에 통합하고 기본 보안 기능을 사용하도록 설정되었으므로 고급 기능 구성을 시작할 수 있습니다. 다음은 다음에 고려해야 할 몇 가지 사항입니다.

- 관리 액세스 모범 사례에 따라 관리 인터페이스를 올바르게 보호하고 있는지 확인합니다.
- 애플리케이션을 안전하게 활성화하고 네트워크를 공격으로부터 보호하기 위해 모범 사례 보안 정책 규칙 기준을 구성합니다. 모범 사례 페이지로 이동하여 방화벽 배포에 대한 보안 정책 모범 사례를 선택합니다.
- 고가용성 설정 -고가용성(HA)은 두 개의 방화벽을 그룹에 배치하고 해당 구성 및 세션 테이블이 동기화되어 네트워크에서 단일 오류가 발생하지 않도록 하는 구성입니다. 방화벽 피어 간의 하트비트 연결은 피어가 다운될 경우 원활한 페일오버를 보장합니다. 두 방화벽 클러스터를 설정하면 중복성이 제공되며 비즈니스 연속성을 보장할 수 있습니다.
- 사용자 식별(사용자 ID)-사용자ID 사용- 사용자 ID는 개별 IP 주소가 아닌 사용자와 그룹을 기반으로 정책을 생성하고 보고를 수행할 수 있는 Palo Alto Networks 차세대 방화벽 기능입니다.
- 복호화을 가능하게 -Palo Alto Networks 방화벽은 가시성, 제어 및 세분화 된 보안을 위해 트래픽을 해독하고 검사할 수 있는 기능을 제공합니다. 방화벽에서 복호화를 사용하여 악의적인 콘텐츠가 네트워크에 유입되거나 중요한 콘텐츠가 네트워크를 암호화되거나 터널로 된 트래픽으로 숨기지 않도록 합니다.
- 레이어 4 및 레이어 7 이베이전에서 네트워크를 보호하기 위한 모범 사례를 준수하십시오.
- Palo Alto Networks와 위협 인텔리전스 공유 - 방화벽이 정기적으로 애플리케이션, 위협 및 디바이스 건강에 대한 정보를 Palo Alto Networks로 수집하고 전송할 수 있도록 허용합니다. 원격 분석에는 수동형 DNS 모니터링을 활성화하고 보안 정책 규칙, 방화벽 로그 또는 방화벽 성능에 영향을 미치지 않고 실험 테스트 서명이 백그라운드에서 실행되도록 하는 옵션이 포함되어 있습니다. Palo Alto Networks 고객은 Palo Alto Networks가 방화벽의 위협 방지 기능을 개선하기 위해 사용하는 원격 분석에서 수집된 인텔리전스의 혜택을 누릴 수 있습니다.


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

# 구독

방화벽에서 작동하는 모든 구독 및 서비스에 대해 알아보고 구독 라이선스를 활성화하여 시작하십시오.

- 방화벽과 함께 사용할 수 있는 구독
- 구독 라이선스 활성화
- 라이선스가 만료되면 어떻게 되나요?
- Palo Alto Networks 클라우드 서비스를 위한 향상된 애플리케이션 로그



***Cortex XDR***™와 같은 특정 클라우드 서비스는 방화벽과 직접 통합되지 않지만 네트워크 활동에 대한 가시성을 위해 ***Cortex Data Lake***에 저장된 데이터에 의존합니다. 향상된 애플리케이션 로깅은 ***Cortex Data Lake*** 구독과 함께 제공되는 기능으로, 방화벽이 피질 ***XDR***이 비정상적인 네트워크 활동을 감지하는 데 사용하는 데 특별히 사용할 수 있는 데이터를 수집할 수 있습니다. 향상된 애플리케이션 로깅을 켜는 것은 Cortex XDR 모범 사례입니다.

# 방화벽과 함께 사용할 수 있는 구독

다음 Palo Alto Networks 구독은 특정 방화벽 기능의 잠금을 해제하거나 방화벽이 Palo Alto Networks 클라우드 제공 서비스(또는 둘 다)를 활용할 수 있도록 합니다. 여기에서 방화벽과 함께 작동하기 위해 구독이 필요한 각 서비스 또는 기능에 대해 자세히 알아볼 수 있습니다. 구독을 활성화하려면 먼저 구독 라이선스 활성화을(를) 해야 합니다. 일단 활성화되면 대부분의 구독 서비스는 동적 콘텐츠 업데이트를 사용하여 방화벽에 신규 및 업데이트된 기능을 제공할 수 있습니다.

| 방화벽과 함께 사용할 수 있는 구독 | |
|---|---|
| **IoT** 보안 | IoT Security 솔루션은 차세대 방화벽과 연동하여 네트워크에서 IoT 디바이스의 실시간 인벤토리를 동적으로 검색하고 유지 관리합니다. AI 및 머신 러닝 알고리즘을 통해 IoT Security 솔루션은 처음으로 접하는 IoT 디바이스 유형을 분류하는 경우에도 높은 수준의 정확도를 달성합니다. 또한 동적이기 때문에 IoT 디바이스 인벤토리는 항상 최신 상태로 유지됩니다. 또한 IoT Security는 IoT 디바이스 트래픽을 제어하는 정책 권장사항의 자동 생성과 방화벽 정책에 사용할 IoT 디바이스 속성의 자동 생성을 제공합니다.<br>• IoT 보안 시작하기. |
| **PAN-OS SD-WAN** | PAN-OS 소프트웨어가 이미 제공하는 업계 최고의 보안 외에도 지능적이고 동적인 경로 선택을 제공합니다. Panorama에서 관리하는 PAN-OS SD-WAN 구현에는 다음이 포함됩니다.<br>• 중앙 집중식 구성 관리<br>• 자동 VPN 토폴로지 생성<br>• 트래픽 분배<br>• 모니터링 및 문제 해결<br>• PAN-OS SD-WAN 시작하기 |
| 위협 방지 | 위협 방지는 다음을 제공합니다.<br>• 안티바이러스, 안티스파이웨어(명령 및 제어) 및 취약점 보호.<br>• 악성 호스트로부터 네트워크를 보호하는 데 사용할 수 있는 기본 외부 동적 목록입니다.<br>• 악성 도메인에 연결하려고 시도하는 감염된 호스트를 식별하는 기능.<br>• 위협 방지 시작하기 |
| 고급 위협 방지 | 위협 방지에 포함된 모든 기능 외에도 고급 Threat Prevention 서브스크립션은 Palo Alto Networks에서 수집한 충실도가 높은 위협 인텔리전스에 대해 학습된 딥 러닝 모델을 활용하여 네트워크를 보호하는 인라인 클라우드 기반 위협 탐지 및 예방 엔진을 제공하며, 모 |


©2023 Palo Alto Networks, Inc.

| 방화벽과 함께 사용할 수 있는 구독 | |
|---|---|
| | 든 네트워크 트래픽을 검사하여 회피적이고 알려지지 않은 명령 및 제어(C2) 위협으로부터 보호합니다.<br>• 지능형 위협 방지 시작하기 |
| **DNS** 보안 | 고급 예측 분석 및 기계 학습을 사용하여 DNS 서명을 생성할 수 있는 확장 가능한 클라우드 기반 서비스인 DNS Security를 쿼리하여 향상된 DNS 싱크홀링 기능을 제공합니다. 이 서비스는 Palo Alto Networks에서 생산되는 지속적으로 확장되는 DNS 기반 위협 인텔리전스에 대한 완전한 액세스를 제공합니다.<br>DNS 보안을 설정하려면 먼저 위협 방지 라이선스를 구입하여 설치해야 합니다.<br>• DNS 보안 시작하기 |
| **URL** 필터링 | 웹 액세스뿐만 아니라 동적 URL 카테고리를 기반으로 사용자가 온라인 콘텐츠와 상호 작용하는 방식을 제어할 수 있는 기능을 제공합니다. 사용자가 회사 자격 증명을 제출할 수 있는 사이트를 제어하여 자격 증명 도용을 방지할 수도 있습니다.<br>URL 필터링을 설정하려면 지원되는 URL 필터링 데이터베이스인 PAN-DB에 대한 구독을 구입하여 설치해야 합니다. PAN-DB를 사용하면 PAN-DB 퍼블릭 클라우드 또는 PAN-DB 프라이빗 클라우드에 대한 액세스를 설정할 수 있습니다.<br>***URL*** 필터링은 더 이상 독립 실행형 구독으로 사용할 수 없습니다. ***URL*** 필터링에 포함된 모든 기능은 고급 ***URL*** 필터링 구독에 포함됩니다.<br>• URL 필터링 시작하기 |
| 고급 **URL** 필터링 | 고급 URL 필터링은 클라우드 기반 ML 기반 웹 보안 엔진을 사용하여 웹 트래픽에 대한 ML 기반 검사를 실시간으로 수행합니다. 따라서 URL 데이터베이스 및 대역 외 웹 크롤링에 대한 의존도를 줄여 표적 피싱, 웹 제공 멀웨어 및 익스플로이트, 명령 및 제어, 소셜 엔지니어링 및 기타 유형의 웹 공격을 비롯한 파일리스(file-less) 웹 기반 고급 공격을 탐지하고 예방할 수 있습니다.<br>• 고급 URL 필터링 시작하기 |
| **WildFire** | 위협 방지 라이선스의 일부로 기본 WildFire® 지원이 포함되어 있지만 WildFire 구독 서비스는 위협, 빈번한 WildFire 서명 업데이트, 고급 파일 형식 포워딩 (APK, PDF, Microsoft Office 및 자바 애플릿)뿐만 아니라 WildFire API를 사용하여 파일을 업로드하는 기능을 사용할 수 있습니다. 방화벽이 온프레미스 WF-500 어플라이언스로 파일을 포워딩하는 경우에도 WildFire 구독이 필요합니다. |


©2023 Palo Alto Networks, Inc.

| 방화벽과 함께 사용할 수 있는 구독 | |
|---|---|
| | • WildFire 시작하기 |
| **AutoFocus** | AutoFocus 포털의 위협 인텔리전스를 사용하여 방화벽 트래픽 로그에 대한 그래픽 분석을 제공하고 네트워크의 잠재적 위험을 식별합니다. 활성 라이선스를 사용하면 방화벽에 기록된 로그를 기반으로 AutoFocus 검색을 열 수도 있습니다.<br>• AutoFocus 시작하기 |
| **Cortex Data Lake** | 클라우드 기반의 중앙 집중식 로그 스토리지 및 집계를 제공합니다. Cortex Data Lake는 Cortex XDR, IoT 보안, 프리즈마 액세스, 트랩 관리 서비스 등 기타 여러 클라우드 제공 서비스를 지원하기 위해 필요하거나 권장되는 서비스입니다.<br>• Cortex Data Lake 시작하기 |
| **GlobalProtect Gateway** | 모빌리티 솔루션 및/또는 대규모 VPN 기능을 제공합니다. 기본적으로 라이선스 없이 GlobalProtect 포털 및 게이트웨이(HIP 확인 없이)를 배포할 수 있습니다. 고급 GlobalProtect 기능(HIP 검사 및 관련 콘텐츠 업데이트, GlobalProtect 모바일 앱, IPv6 연결 또는 GlobalProtect 클라이언트리스 VPN)을 사용하려면 각 게이트웨이에 대한 GlobalProtect 게이트웨이 라이선스가 필요합니다.<br>• GlobalProtect 시작하기 |
| 가상 시스템 | 이 라이선스는 영구 라이선스이며 PA-3200 시리즈 방화벽에서 여러 가상 시스템을 지원하는 데 필요합니다. 또한 PA-5200 시리즈, PA-5400 시리즈 및 PA-7000 시리즈 방화벽에서 기본적으로 제공되는 기본 수를 초과하여 가상 시스템 수를 늘리려면 가상 시스템 라이선스를 구입해야 합니다 (기본 번호는 플랫폼마다 다름). PA-220, PA-400 시리즈, PA-800 시리즈, PA-3400 시리즈 및 VM 시리즈 방화벽은 가상 시스템을 지원하지 않습니다.<br>• 가상 시스템 시작하기 |
| 엔터프라이즈 데이터 손실 방지**(DLP)** | 민감한 정보의 무단 액세스, 오용, 추출 및 공유에 대한 클라우드 기반 보호 기능을 제공합니다. Enterprise DLP는 머신 러닝 기반 데이터 분류, 정규 표현식 또는 키워드를 사용하는 수백 개의 데이터 패턴, 그리고 볼 연산을 사용하여 집단 데이터 유형을 스캔하는 데이터 프로파일을 사용하여 유휴 및 이동 중인 민감한 데이터를 정확하게 탐지하고 일관되게 정책을 시행할 수 있는 단일 엔진을 제공합니다.<br>• 엔터프라이즈 데이터 손실 방지 시작하기 |
| **SaaS** 보안 인라인 | SaaS 보안 솔루션은 Cortex Data 레이크와 연동하여 네트워크에서 사용 중인 모든 SaaS 애플리케이션을 검색합니다. SaaS 보안 인라인은 수천 개의 섀도우 IT 애플리케이션과 해당 사용자 및 사용 세부 정보를 검색할 수 있습니다. 또한 SaaS 보안 인라인은 기존 Palo |


©2023 Palo Alto Networks, Inc.

| 방화벽과 함께 사용할 수 있는 구독 | |
|---|---|
| | Alto Networks 방화벽에서 SaaS 정책 규칙 권장 사항을 원활하게 적용합니다. 또한 앱 ID 클라우드 엔진(ACE)에는 SaaS 보안 인라인이 필요합니다.<br>• SaaS 보안 인라인 시작하기 |


©2023 Palo Alto Networks, Inc.

# 구독 라이선스 활성화

방화벽에서 새 라이선스를 활성화하려면 다음 단계를 따르십시오.

복호화 미러링 기능을 사용하려면 무료 라이선스를 활성화하여 기능을 잠금 해제해야 합니다. 이러한 기능을 사용하려면 대신 복호화 기능을 위한 무료 라이선스 활성화의 단계를 따라야 합니다.

**STEP 1 |** 구입한 라이선스의 활성화 코드를 찾습니다.

구독을 구매하면 Palo Alto Networks 고객 서비스에서 각 구독과 연결된 활성화 코드가 나열된 이메일을 받게 됩니다. 이 이메일을 찾을 수 없는 경우 계속하기 전에 고객 지원에 문의하여 활성화 코드를 받으십시오.

**STEP 2 |** 지원 라이선스를 활성화하십시오.

유효한 지원 라이선스가 없으면 PAN-OS 소프트웨어를 업데이트할 수 없습니다.

1. 웹 인터페이스에 로그인한 다음디바이스 > 지원을 선택합니다.
2. 인증 코드를 사용하여 지원 활성화를 클릭합니다.
3. 인증 코드를 입력한 다음 확인을 클릭합니다.

**STEP 3 |** 구매한 각 라이선스를 활성화합니다.

**Device** > **Licenses**를 선택한 후 다음 방법 중 하나로 라이선스 및 구독을 활성화합니다.

- 라이선스 서버에서 라이선스 키 검색 - 고객 지원 포털에서 라이선스를 활성화한 경우 이 옵션을 사용합니다.
- 인증 코드를 사용하여 기능 활성화 - 이전에 지원 포털에서 활성화되지 않은 라이선스에 대한 인증 코드를 사용하여 구매한 구독을 활성화하려면 이 옵션을 사용합니다. 메시지가 표시되면 인증 코드를 입력한 다음 확인을 클릭합니다.
- 수동으로 라이선스 키 업로드 - 방화벽이 Palo Alto Networks 고객 지원 포털에 연결되어 있지 않은 경우 이 옵션을 사용합니다. 이 경우 인터넷에 연결된 컴퓨터의 지원 사이트에서 라이선스 키 파일을 다운로드한 후 방화벽에 업로드해야 합니다.

고객 지원 포털 *API*를 사용하여 활성화를 자동화하려면 라이선스 활성화 프로세스를 참조하십시오. 이 프로세스는 하드웨어 및 *VM* 시리즈 방화벽 모두에서 작동합니다.

**STEP 4 |** 라이선스가 성공적으로 활성화되었는지 확인

**Device** > **Licenses** 페이지에서 라이선스가 성공적으로 활성화되었는지 확인합니다. 예를 들어 WildFire 라이선스를 활성화한 후 라이선스가 유효한지 확인해야 합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** (WildFire 구독만 해당) 커밋을 수행하여 WildFire 구독 활성화를 완료합니다.

WildFire 구독을 활성화한 후 방화벽이 Advanced 파일 형식 포워딩을 시작하려면 커밋이 필요합니다. 다음 중 하나를 수행해야 합니다.

- 보류 중인 변경 사항을 커밋합니다.
- 이제 WildFire 구독에서 지원되는 Advanced 파일 유형이 WildFire Analysis 프로파일 규칙에 포함되어 있는지 확인하십시오. 규칙을 변경할 필요가 없으면 규칙 설명을 약간 수정하고 커밋을 수행합니다.

 ©2023 Palo Alto Networks, Inc.

# 라이선스가 만료되면 어떻게 되나요?

Palo Alto Networks 구독은 방화벽에 추가 기능 및/또는 Palo Alto Networks 클라우드 제공 서비스에 대한 액세스를 제공합니다. 라이선스가 만료된 후 30일 이내인 경우 구독이 갱신되거나 만료될 때까지 매일 시스템 로그에 경고 메시지가 표시됩니다. 라이선스가 만료되면 일부 구독은 제한된 용량으로 계속 작동하고 다른 구독은 완전히 작동을 중지합니다. 여기에서 각 구독이 만료되면 어떻게 되는지 확인할 수 있습니다.

정확한 라이선스 만료 시점은 다음 날 오전 *12:00(GMT* 기준*)*입니다. 예를 들어 라이선스가 *1/20*에 종료될 예정인 경우 그날 남은 시간 동안 기능을 사용할 수 있습니다. 새로운 날이 시작되는 *1*월 *21*일 오전 *12:00(GMT)*에 라이선스가 만료됩니다. 모든 라이선스 관련 기능은 방화벽에 구성된 시간대에 관계없이 그리니치 표준시*(GMT)*에서 작동합니다.

| 구독 | 만료 동작 |
|---|---|
| 위협 예방 | 라이선스가 만료되었음을 나타내는 경고가 시스템 로그에 나타납니다.<br>여전히 다음을 수행할 수 있습니다.<br>• 수동으로 또는 자동 일정의 일부로 새 애플리케이션 전용 콘텐츠 업데이트를 설치하지 않는 한 라이선스가 만료될 때 설치된 서명을 사용하십시오. 그렇게 하면 업데이트가 기존 위협 서명을 삭제하고 더 이상 위협 서명에 대한 보호를 받지 못합니다.<br>• Custom App-ID™ 및 위협 서명을 사용하고 수정합니다.<br>더 이상 다음을 수행할 수 없습니다.<br>• 새 서명을 설치합니다.<br>• 서명을 이전 버전으로 롤백합니다. |
| DNS 보안 | 여전히 다음을 수행할 수 있습니다.<br>• 활성 Threat Prevention 라이선스가 있는 경우 로컬 DNS 서명을 사용합니다.<br>더 이상 다음을 수행할 수 없습니다.<br>• 새 DNS 서명을 받으세요. |
| Advanced URL 필터링 / URL 필터링 | 여전히 다음을 수행할 수 있습니다.<br>• 사용자 지정 URL 카테고리를 사용하여 정책을 시행합니다.<br>더 이상 다음을 수행할 수 없습니다.<br>• 캐시된 PAN-DB 카테고리에 대한 업데이트를 가져옵니다.<br>• PAN-DB URL 필터링 데이터베이스에 연결합니다.<br>• PAN-DB URL 카테고리를 가져옵니다. |


©2023 Palo Alto Networks, Inc.

| 구독 | 만료 동작 |
| --- | --- |
| | • Advanced URL 필터링을 사용하여 실시간으로 URL 요청을 분석합니다. |
| WildFire | 여전히 다음을 수행할 수 있습니다.<br>• 분석을 위해 PE를 포워딩합니다.<br>• 활성 Threat Prevention 구독이 있는 경우 24-48시간마다 서명 업데이트를 받으십시오.<br>더 이상 다음을 수행할 수 없습니다.<br>• WildFire 퍼블릭 및 프라이빗 클라우드를 통해 5분 업데이트를 받으세요.<br>• SMTP 및 POP3 이메일 메시지에 포함된 APK, Flash 파일, PDF, Microsoft Office 파일, Java 애플릿, Java 파일(.jar 및 .class), HTTP/HTTPS 이메일 링크와 같은 Advanced 파일 유형을 포워딩합니다.<br>• WildFire API를 사용합니다.<br>• WildFire 어플라이언스를 사용하여 WildFire 프라이빗 클라우드 또는 WildFire 하이브리드 클라우드를 호스팅합니다. |
| AutoFocus | 여전히 다음을 수행할 수 있습니다.<br>• 3개월의 유예 기간 동안 AutoFocus 데이터와 함께 외부 동적 목록을 사용합니다.<br>더 이상 다음을 수행할 수 없습니다.<br>• AutoFocus 포털에 액세스합니다.<br>• 모니터 로그 또는 ACC 아티팩트에 대한 AutoFocus 인텔리전스 요약을 봅니다. |
| Cortex Data Lake | 여전히 다음을 수행할 수 있습니다.<br>• 30일의 유예 기간 동안 로그 데이터를 저장한 후 삭제합니다.<br>• 30일의 유예 기간이 끝날 때까지 Cortex Data Lake에 로그를 포워딩합니다. |
| GlobalProtect | 여전히 다음을 수행할 수 있습니다.<br>• Windows 및 macOS를 실행하는 엔드포인트용 앱을 사용합니다.<br>• 단일 또는 다중 내부/외부 게이트웨이를 구성합니다.<br>더 이상 다음을 수행할 수 없습니다.<br>• iOS, Android, Chrome OS 및 Windows 10 UWP용 Linux OS 앱 및 모바일 앱에 액세스합니다. |


©2023 Palo Alto Networks, Inc.

| 구독 | 만료 동작 |
| --- | --- |
| | • 외부 게이트웨이에 IPv6을 사용합니다.<br>• HIP 검사를 실행합니다.<br>• 클라이언트리스 VPN을 사용하십시오.<br>• 대상 도메인, 클라이언트 프로세스 및 비디오 스트리밍 애플리케이션을 기반으로 분할 터널링을 시행합니다. |
| VM-Series | VM 시리즈 배포 가이드를 참조하십시오. |
| 지원 | 더 이상 다음을 수행할 수 없습니다.<br>• 소프트웨어 업데이트를 받습니다.<br>• VM 이미지를 다운로드합니다.<br>• 기술 지원의 이점을 누리십시오. |


©2023 Palo Alto Networks, Inc.

# Palo Alto Networks 클라우드 서비스를 위한 향상된 애플리케이션 로그

방화벽은 Cortex XDR 및 IoT Security와 같은 Palo Alto Networks 앱 및 서비스의 네트워크 활동에 대한 가시성을 높이는 데이터를 수집할 수 있습니다. 이러한 향상된 애플리케이션 로그는 Palo Alto Networks 앱 및 서비스가 소비하고 처리하도록 엄격하게 설계되었습니다. 방화벽이나 Panorama에 향상된 애플리케이션 로그를 볼 수 없습니다. 로깅 서비스로 로그를 보내는 방화벽만 향상된 애플리케이션 로그를 생성할 수 있습니다.

다음 절차에 따라 Cortex XDR 및 IoT 보안에 대한 향상된 애플리케이션 로그에 대한 로그 전달을 사용하도록 설정합니다.

- Cortex XDR
- IoT 보안

## Cortex XDR

향상된 애플리케이션 로그가 수집하는 데이터 유형의 예로는 DNS 쿼리 레코드, URL에 액세스하는 데 사용되는 웹 브라우저 또는 도구를 지정하는 HTTP 헤더 사용자 에이전트 필드 및 DHCP 자동 IP 주소 할당에 대한 정보가 포함됩니다. 예를 들어 DHCP 정보를 사용하면 Cortex XDR™ IP 주소 대신 호스트 이름을 기반으로 비정상적인 활동을 경고할 수 있습니다. 이를 통해 Cortex XDR을 사용하는 보안 분석가가 사용자의 활동이 자신의 역할 범위 내에 있는지, 그렇지 않은 경우 활동을 중지하기 위한 조치를 보다 신속하게 수행할 수 있는지를 의미 있게 평가할 수 있습니다.

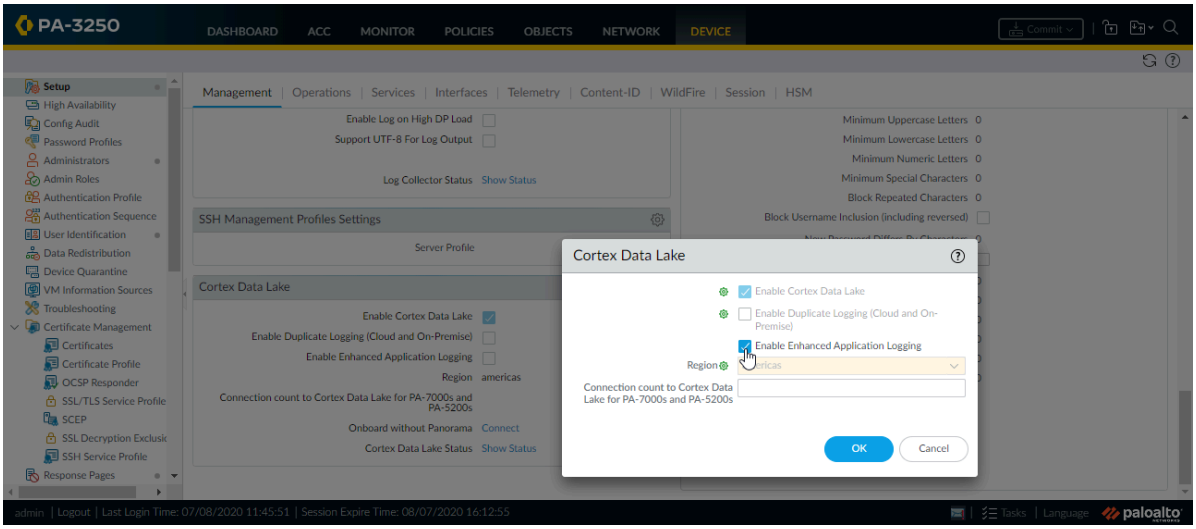
가장 포괄적인 향상된 애플리케이션 로그 집합을 활용하려면 Windows 기반 User-ID 에이전트및 PAN-OS 통합 User-ID 에이전트에 대한 사용자 ID 배포를 활성화해야 하며 방화벽 사용자 ID 로그에 반영되지는 않지만 특정 사용자와 네트워크 활동을 연결하는 데 유용합니다.

향상된 애플리케이션 로그를 Cortex Data Lake에 포워딩하려면 향상된 애플리케이션 로깅을 전역으로 설정한 다음 보안 별 규칙 기준으로 사용하도록 설정합니다(로그 포워딩 프로파일 사용). 전역 설정이 필요하며 세션 기반이 아닌 트래픽에 대한 데이터를 캡처합니다(예: ARP 요청). 보안별 정책 규칙 설정은 강력히 권장됩니다. 향상된 애플리케이션 로그의 대부분은 보안 정책 규칙이 적용하는 세션 기반 트래픽에서 수집됩니다.

**STEP 1 |** 향상된 애플리케이션 로깅에는 Cortex Data Lake 구독이 필요하며 사용자 ID도 권장됩니다. 다음은 Cortex Data Lake로 시작하고 사용자 ID를 활성화하는 단계입니다.


©2023 Palo Alto Networks, Inc.

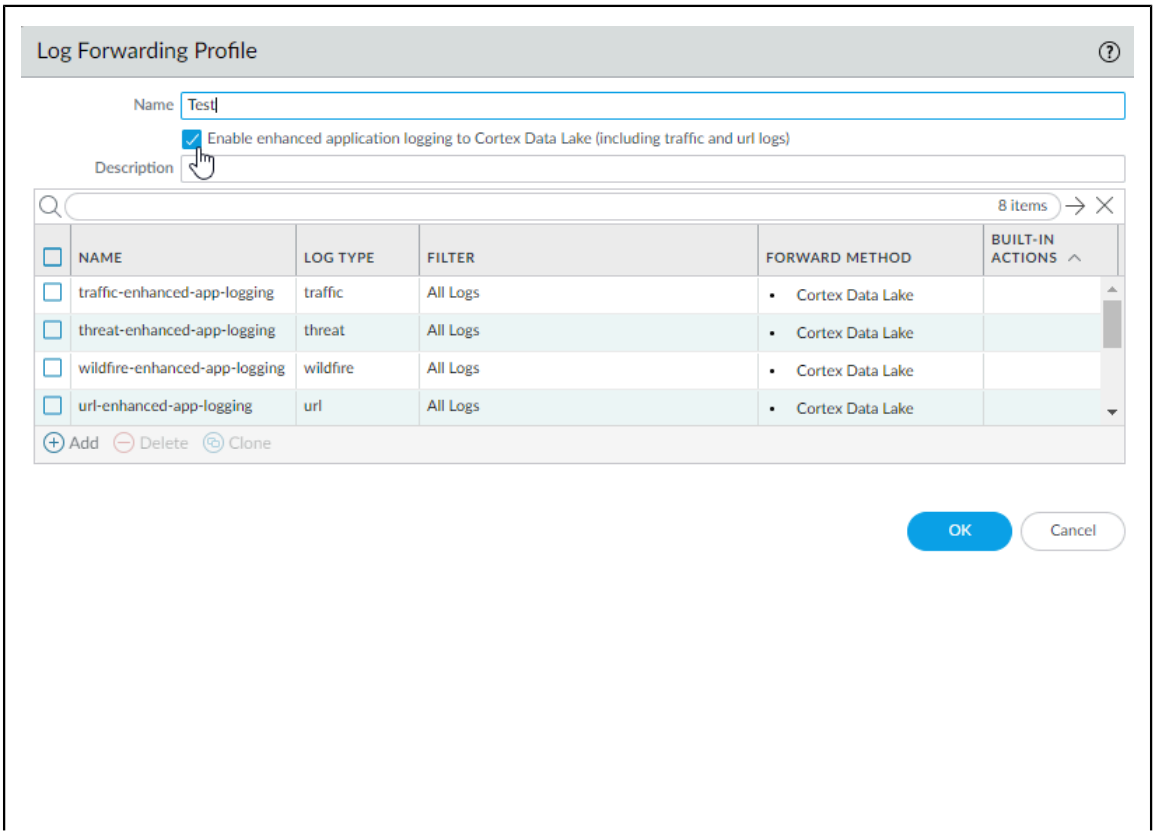
**STEP 2 |** 방화벽에서 향상된 애플리케이션 로깅을 사용하도록 설정하려면 디바이스 > 설정 > 관리 > **Cortex Data Lake**를 선택한 다음 Cortex Data Lake 설정을 편집합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 확장된 가시성을 원하는 트래픽을 제어하는 보안 정책 규칙에 대한 향상된 애플리케이션 로깅을 계속 활성화합니다.

1. 개체 > 로그 포이딩을 선택한 다음 로그 포워딩 프로파일을 추가하거나 수정합니다.
2. 프로파일을 업데이트하여 향상된 애플리케이션 로깅을 **Cortex Data Lake(**트래픽 및 **URL** 로그 포함**)**로 사용하도록 설정합니다.




로그 포싱 프로파일에서 향상된 애플리케이션 로깅을 사용하도록 설정하면 향상된 애플리케이션 로깅에 필요한 로그 유형을 지정하는 일치 목록이 프로파일에 자동으로 추가됩니다.

3. 확인을 클릭하여 프로파일을 저장하고 필요에 따라 많은 프로파일을 계속 업데이트합니다.
4. 업데이트한 로그 포워딩 프로파일이 보안 정책 규칙에 첨부되어 규칙과 일치하는 트래픽에 대한 로그 생성 및 포워딩을 트리거합니다.

   **1.** 정책 > 보안을 선택하여 각 보안 정책 규칙에 연결된 프로파일을 봅니다.

   **2.** 규칙에 연결된 로그 포워딩 프로파일을 업데이트하려면 규칙을 추가하거나 편집하고 정책 > 보안 > 작업 > 로그 포워딩을 선택한 다음 향상된 애플리케이션 로깅으로 활성화된 로그 포워딩 프로파일을 선택합니다.

## IoT 보안

IoT Security에 대한 방화벽 설정의 한 부분에는 로그 전달 프로파일을 만들어 보안 정책 규칙에 적용하는 작업이 포함됩니다. 프로파일을 각 규칙에 개별적으로 적용할 수 있지만 더 간단한 방법은 미리 정의된 로그 전달 프로파일을 선택하여 원하는 만큼 대량으로 적용하는 것입니다. 다음 단계에서는 미리 정의된 로그 전달 프로파일을 보안 정책 규칙에 대량으로 추가하는 이 방법을 설명합니다.

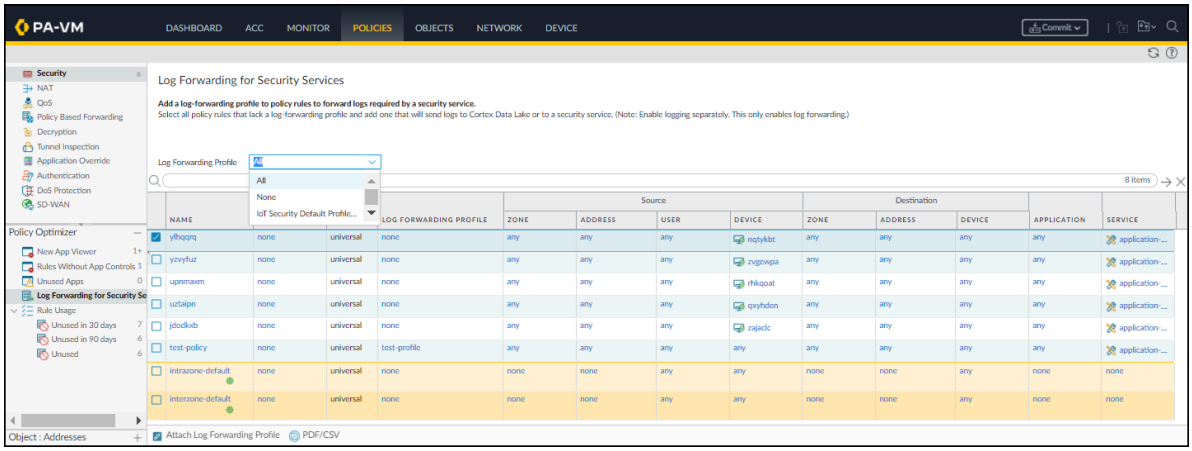

©2023 Palo Alto Networks, Inc.

이 워크플로를 사용하려면 이미 보안 정책 규칙을 구성하고 규칙에 대한 로깅을 활성화하고 향상된 애플리케이션 로깅으로 로깅 서비스를 활성화해야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** IoT 보안에 대한 로그 전달 프로파일을 보안 정책 규칙에 적용합니다.

1. 차세대 방화벽에 로그인하고 정책 최적화 섹션에서 정책 > 보안 서비스에 대한 로그 전달을 선택합니다.
2. 로그 전달 프로파일이 있는 규칙과 없는 규칙을 포함하여 모든 보안 정책 규칙을 보려면 로그 전달 프로파일에 대해 모두를 선택합니다.

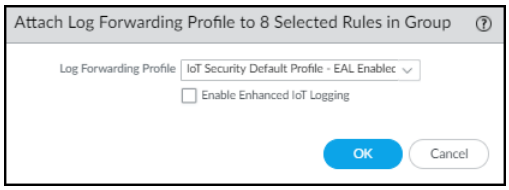



3. 로깅 서비스로 로그를 전달할 규칙을 선택합니다.
4. 페이지 하단에 로그 포워딩 프로파일을 첨부합니다.
5. 기본 로그 전달 프로파일을 규칙에 적용하려면 **IoT** 보안 기본 프로파일 **- EAL** 사용 및 확인을 선택합니다.

   기본 프로파일은 EAL(향상된 애플리케이션 로그)을 포함하여 필요한 모든 로그 유형을 IoT 보안에 제공하도록 미리 구성되어 있습니다.

   > ***IoT*** 보안 기본 프로파일에서 ***EAL(Enhanced Application Logging)***이 이미 활성화되어 있으므로 향상된 ***IoT*** 로깅을 활성화할 필요가 없습니다.


©2023 Palo Alto Networks, Inc.




또는

아직 없는 기존 Log Forwarding 프로파일에 EAL 전달을 추가하려면 Log Forwarding Profile 목록에서 선택하고 **Enable Enhanced IoT Logging**을 선택한 다음 **OK**를 선택합니다.

향상된 ***IoT*** 로깅을 활성화하면 *PAN-OS*는 선택한 로그 전달 프로파일 자체를 업데이트하므로 동일한 로그 전달 프로파일을 사용하는 모든 규칙에서 향상된 로그 전달을 활성화합니다.

PAN-OS는 선택한 로그 전달 프로파일을 아직 없는 규칙에 추가하고 이전에 할당된 프로파일을 이 규칙으로 바꿉니다.

**STEP 2 |** 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

# 방화벽 관리

관리자는 웹 인터페이스, CLI 및 API 관리 인터페이스를 사용하여 Palo Alto Networks 방화벽을 구성, 관리 및 모니터링할 수 있습니다. 관리 인터페이스에 대한 역할 기반 관리 액세스를 사용자 지정하여 특정 작업 또는 권한을 특정 관리자에게 위임할 수 있습니다.

관리 네트워크와 방화벽 및 Panorama 관리 인터페이스를 보호하는 방법은 관리 액세스 모범 사례를 참조하십시오.


- 관리 인터페이스
- 웹 인터페이스 사용
- 구성 백업 관리
- 방화벽 관리자 관리
- 참조: 웹 인터페이스 관리자 액세스
- 참조: 포트 번호 사용
- 방화벽을 출하시 기본 설정으로 재설정
- 방화벽 부트스트랩

# 관리 인터페이스

다음 사용자 인터페이스를 사용하여 Palo Alto Networks 방화벽을 관리할 수 있습니다.

> 인터넷이나 엔터프라이즈 보안 경계 내의 다른 신뢰할 수 없는 영역에서 관리 액세스를 사용하도록 설정하지 마십시오. 관리 액세스 모범 사례 에 따라 방화벽을 올바르게 보호하고 있는지 확인합니다.

- 웹 인터페이스를 사용하여 비교적 쉽게 구성 및 모니터링 작업을 수행할 수 있습니다. 이 그래픽 인터페이스를 사용하면 HTTPS(권장) 또는 HTTP를 사용하여 방화벽에 액세스할 수 있으며 관리 작업을 수행하는 가장 좋은 방법입니다.
- 명령줄 인터페이스(CLI)를 사용하여 SSH(권장), 텔넷 또는 콘솔 포트를 통해 명령을 연속적으로 입력하여 일련의 작업을 수행할 수 있습니다. CLI는 작동 및 구성의 두 가지 명령 모드를 지원하는 단순한 인터페이스로, 각각 명령과 명령문의 고유한 레이어 구조가 있습니다. 명령의 중첩 구조 및 구문에 익숙해지면 CLI를 통해 빠른 응답 시간과 관리 효율성을 얻을 수 있습니다.
- XML API를 사용하여 운영을 간소화하고 내부적으로 개발된 기존 애플리케이션 및 리포지토리와 통합할 수 있습니다. XML API는 HTTP/HTTPS 요청 및 응답을 사용하여 구현되는 웹 서비스입니다.
- Panoramoram를 사용하여 여러 방화벽에 대한 웹 기반 관리, 보고 및 로그 수집을 수행합니다. Panorama 웹 인터페이스는 방화벽 웹 인터페이스와 유사하지만 중앙 집중식 관리를 위한 추가 기능이 있습니다.


©2023 Palo Alto Networks, Inc.

# 웹 인터페이스 사용

다음 항목에서는 방화벽 웹 인터페이스를 사용하는 방법에 대해 설명합니다. 웹 인터페이스의 특정 탭과 필드에 대한 자세한 내용은 Web Interface Reference Guide를 참조하십시오.

- 웹 인터페이스 실행
- 배너, 오늘의 메시지 및 로고 구성
- 관리자 로그인 활동 표시기를 사용하여 계정 오용 감지
- 관리 작업 관리 및 모니터링
- 방화벽 구성 변경 사항 커밋, 유효성 검사 및 미리 보기
- 선택적 구성 변경 커밋
- 구성 테이블 데이터 내보내기
- 전역 찾기를 사용하여 방화벽 또는 Panorama 관리 서버 검색
- 구성 변경을 제한하기 위한 잠금 관리

## 웹 인터페이스 실행

웹 인터페이스에 액세스하기 위해 다음 웹 브라우저가 지원됩니다.

- Internet Explorer 11+
- Firefox 3.6+
- Safari 5+
- Chrome 11+

웹 인터페이스를 시작하려면 다음 작업을 수행하십시오.

**STEP 1 |** 인터넷 브라우저를 실행하고 URL 필드(https://<IP address>)에 방화벽의 IP 주소를 입력합니다.



기본적으로 관리(*MGT*) 인터페이스는 웹 인터페이스에 대한 ***HTTPS*** 액세스만 허용합니다. 다른 프로토콜을 활성화하려면 디바이스 > 설정 > 인터페이스를 선택한 다음 관리 인터페이스를 편집하십시오.

**STEP 2 |** 계정에 사용되는 인증 유형에 따라 방화벽에 로그인합니다. 방화벽에 처음 로그인하는 경우 사용자 이름과 암호에 기본값인 **admin**을 사용합니다.

- **SAML - Single Sign-On(SSO)** 사용을 클릭합니다. 방화벽이 관리자에 대한 권한 부여(역할 할당)를 수행하는 경우 사용자 이름을 입력하고 계속하십시오. SAML ID 공급자(IdP)가 권한 부여를 수행하는 경우 사용자 이름을 입력하지 않고 계속합니다. 두 경우 모두 방화벽이 사용자를 IdP로 리디렉션하여 사용자 이름과 암호를 입력하라는 메시지를 표시합니다. IdP에 인증하면 방화벽 웹 인터페이스가 표시됩니다.
- 다른 유형의 인증 - 사용자 이름과 암호를 입력합니다. 로그인 페이지에 배너와 체크박스가 있는 경우 로그인 배너를 읽고 아래 진술에 동의하고 확인합니다를 선택합니다. 그런 다음 로그인을 클릭합니다.

**STEP 3 |** 일별 메시지를 읽고 닫습니다.


©2023 Palo Alto Networks, Inc.

# 배너, 오늘의 메시지 및 로고 구성

로그인 배너는 로그인 페이지에 추가할 수 있는 선택적 텍스트이므로 관리자가 로그인하기 전에 알아야 할 정보를 볼 수 있습니다. 예를 들어 방화벽의 무단 사용에 대한 제한 사항을 사용자에게 알리는 메시지를 추가할 수 있습니다.

웹 인터페이스의 상단에 오버레이 텍스트를 강조하는 컬러 밴드를 추가하여 관리자가 방화벽 관리를 위한 분류 수준과 같은 중요한 정보를 볼 수 있도록 웹 인터페이스의 맨위(헤더 배너) 및 아래쪽(바닥 배너)을 추가할 수 있습니다.

로그인하면 오늘의 메시지 대화상자가 자동으로 표시됩니다. 대화 상자에는 Palo Alto Networks가 소프트웨어 또는 콘텐츠 릴리스와 관련된 중요한 정보를 강조하기 위해 포함된 메시지가 표시됩니다. 관리자가 임박한 시스템 다시 시작과 같은 정보를 볼 수 있도록 하나의 사용자 지정 메시지를 추가하여 작업에 영향을 줄 수 있습니다.

로그인 페이지와 웹 인터페이스의 헤더에 표시되는 기본 로고를 조직의 로고로 바꿀 수 있습니다.

**STEP 1 |** 로그인 배너를 구성합니다.

1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 수정합니다.
2. 로그인 배너(최대 3,200자)를 입력합니다.
3. (선택 사항) 관리자가 로그인 배너를 승인하도록 강제 관리자를 선택하여 관리자가 로그인 버튼을 활성화하기 위해 배너 텍스트 위의 아래 문 체크박스를 선택하도록 합니다.
4. 확인을 클릭합니다.

**STEP 2 |** 오늘의 메시지를 설정합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 배너 및 메시지 설정을 편집합니다.
2. 오늘의 메시지를 활성화합니다.
3. 오늘의 메시지(최대 3,200자)를 입력합니다.

   메시지를 입력하고 확인을 클릭한 후, 이후에 로그인한 관리자와 브라우저를 새로 고치는 활성 관리자는 새 메시지 또는 업데이트된 메시지를 즉시 참조하면 커밋이 필요하지 않습니다. 이렇게 하면 다른 관리자에게 구성 변경에 영향을 줄 수 있는 임박한 커밋을 알릴 수 있습니다. 메시지가 지정하는 커밋 시간에 따라 관리자는 변경 내용을 완료, 저장 또는 취소할지의 여부를 결정할 수 있습니다.
4. (선택 사항) 다시 표시 안 함(기본값이 비활성화됨)을 선택하여 관리자에게 첫 번째 로그인 세션 다음 날의 메시지를 억제할 수 있는 옵션을 제공합니다. 각 관리자는 자신의 로그인 세션에 대해서만 메시지를 억제할 수 있습니다. 당일 대화 상자의 메시지에서 각 메시지에는 자체 억제 옵션이 있습니다.
5. (선택 사항) 하루 대화 상자의 메시지에 대한 헤더 제목을 입력합니다(기본값은 오늘의 메시지).


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 헤더 및 푸터 배너를 구성합니다.



밝은 배경색과 대조적인 텍스트 색상은 관리자가 배너를 파악하고 읽을 가능성을 높일 수 있습니다. 조직의 분류 수준에 해당하는 색상을 사용할 수도 있습니다.

1. 헤더 배너(최대 3,200자)를 입력합니다.
2. (선택 사항) 다른 헤더와 풋터 배너를 사용하기 위해 동일한 배너 헤더와 푸터(기본적으로 활성화)를 지웁니다.
3. 헤더와 푸터 배너가 다른 경우 푸터 배너(최대 3,200자)를 입력합니다.
4. 확인을 클릭합니다.

**STEP 4 |** 로그인 페이지와 헤더의 로고를 교체합니다.



모든 로고 이미지의 최대 크기는 *128KB*입니다. 지원되는 파일 형식은 *png* 및 *jpg*입니다. 방화벽은 인터레이스된 이미지 파일, 알파 채널이 포함된 이미지 및 *GIF* 파일 형식을 지원하지 않습니다.

1. 디바이스 > 설정 > 작업을 선택한 다음 기타 섹션에서 사용자 지정 로고를 클릭합니다.
2. 로그인 화면 로고와 메인 **UI(**헤더**)** 로고에 대해 다음 단계를 수행합니다.
   1. 업로드를 클릭합니다.
   2. 로고 이미지를 선택하고 열기를 클릭합니다.

      이미지를 미리 볼 수 있으므로 돋보기 아이콘을 클릭하여 *PAN-OS*가 어떻게 자르는지 확인할 수 있습니다.
   3. 닫기를 클릭합니다.
3. 변경 사항을 커밋합니다.

**STEP 5 |** 배너, 당일 메시지 및 로고가 예상대로 표시되는지 확인합니다.

1. 로그아웃하여 선택한 새 로고가 표시되는 로그인 페이지로 돌아갑니다.
2. 로그인 자격 증명을 입력하고 배너를 검토한 다음 아래 진술에 동의합니다를 선택하여 로그인 버튼을 활성화한 다음 로그인을 선택합니다.

   대화 상자에는 오늘의 메시지가 표시됩니다. Palo Alto Networks가 포함된 메시지는 동일한 대화 상자의 별도의 페이지에 표시됩니다. 페이지를 탐색하려면 대화 상자의 측면을 따라 오른쪽 또는 왼쪽 화살표를 클릭하거나 대화 상자 하단의 페이지 선택기를 ●○○○ 클릭합니다.
3. (선택 사항) 구성된 메시지와 Palo Alto Networks가 포함된 메시지에 대해 다시 표시하지 않음을 선택할 수 있습니다.
4. 웹 인터페이스에 액세스하려면 당일 대화 상자의 메시지를 닫습니다.

   헤더 및 푸터 배너는 구성한 텍스트와 색상이 있는 모든 웹 인터페이스 페이지에 표시됩니다. 웹 인터페이스에 대해 선택한 새 로고가 헤더 배너 아래에 표시됩니다.

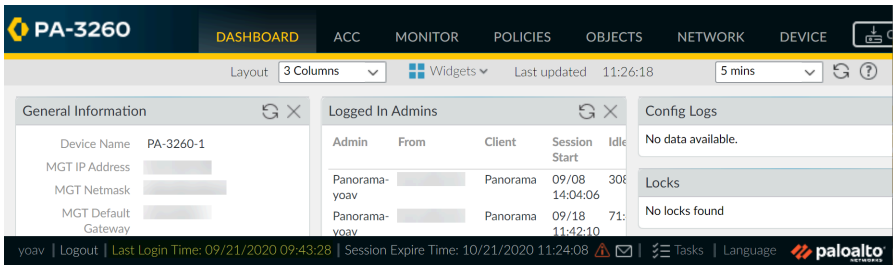

©2023 Palo Alto Networks, Inc.

# 관리자 로그인 활동 표시기를 사용하여 계정 오용 감지

마지막 로그인 시간 및 실패한 로그인 시도 표시기는 Palo Alto Networks 방화벽 또는 Panorama 관리 서버에서 관리자 계정의 오용을 감지하는 시각적 방법을 제공합니다. 마지막 로그인 정보를 사용하여 다른 사람이 귀하의 자격 증명을 사용하여 로그인했는지 확인하고 로그인 시도 실패 표시기를 사용하여 귀하의 계정이 무차별 대입 공격의 대상인지 확인하십시오.

**STEP 1 |** 로그인 활동 표시기를 보고 계정의 최근 활동을 모니터링하십시오.

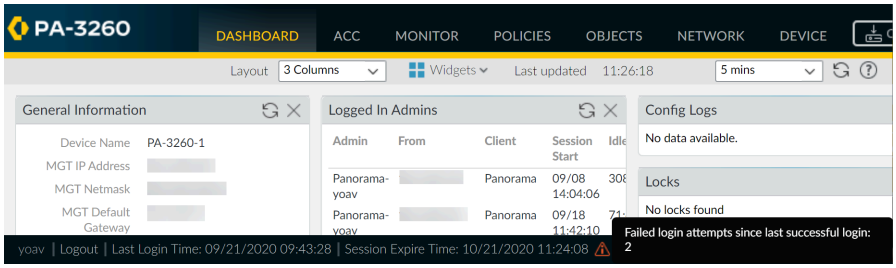
1. 방화벽 또는 Panorama 관리 서버의 웹 인터페이스에 로그인합니다.
2. 창 왼쪽 하단에 있는 마지막 로그인 세부 정보를 보고 타임스탬프가 마지막 로그인과 일치하는지 확인합니다.




3. 실패한 로그인 시도에 대한 마지막 로그인 시간 정보의 오른쪽에 있는 주의 기호를 찾으십시오.

   마지막 로그인 성공 이후 계정을 사용하여 로그인 시도 실패가 한 번 이상 발생한 경우 로그인 실패 표시가 나타납니다.

   **1.** 주의 기호가 표시되면 해당 기호 위로 마우스를 가져가서 실패한 로그인 시도 횟수를 표시합니다.



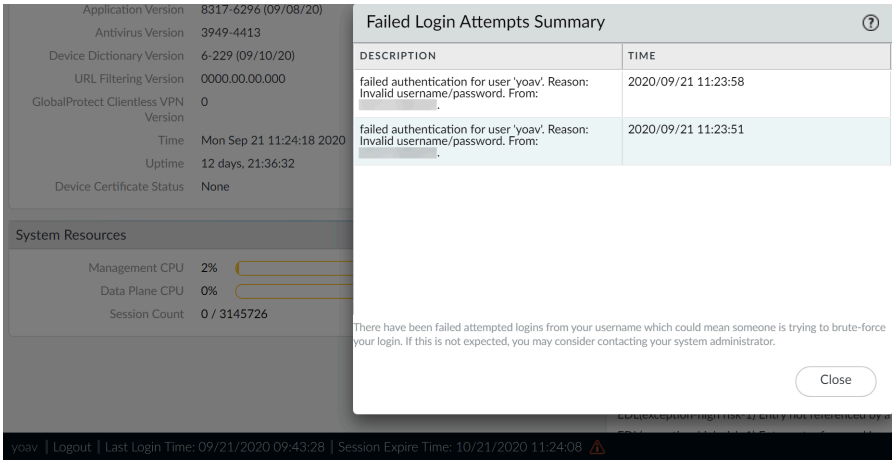

   **2.** 실패한 로그인 시도 요약을 보려면 주의 기호를 클릭하십시오. 세부 정보에는 관리자 계정 이름, 로그인 실패 이유, 소스 IP 주소, 날짜 및 시간이 포함됩니다.

   성공적으로 로그인했다가 로그아웃하면 실패한 로그인 카운터가 *0*으로 재설정되어 다음에 로그인할 때 새로운 실패한 로그인 세부 정보가 있는 경우 이를 볼 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽 또는 Panorama 관리 서버에 계속 로그인을 시도하는 호스트를 찾습니다.

1. 실패한 로그인 시도 요약을 보려면 실패한 로그인 주의 기호를 클릭하십시오.
2. 로그인을 시도한 호스트의 원본 IP 주소를 찾아 기록합니다. 예를 들어, 다음 그림은 여러 번 실패한 로그인 시도를 보여줍니다.




3. 네트워크 관리자와 협력하여 식별한 IP 주소를 사용하는 사용자와 호스트를 찾으십시오.

   무차별 대입 공격을 수행하는 시스템을 찾을 수 없으면 향후 공격을 방지하기 위해 계정 이름을 바꾸는 것이 좋습니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 계정 도용을 감지한 경우 다음 조치를 취하십시오.

1. 모니터 > 로그 > 구성을 선택한 다음 구성 변경 사항 및 커밋 기록을 확인하여 본인도 모르는 사이에 변경 사항을 적용하는 데 계정이 사용되었는지 확인합니다.
2. 디바이스 > 구성 감사를 선택하여 현재 구성과 자격 증명을 사용하여 변경된 것으로 의심되는 구성 직전에 실행 중인 구성을 비교합니다. Panorama를 사용하여 이 작업을 수행할 수도 있습니다.

   새 계정을 만드는 데 관리자 계정이 사용된 경우 구성 감사를 수행하면 승인되지 않은 계정과 관련된 변경 사항도 감지하는 데 도움이 됩니다.
3. 로그가 삭제되었거나 계정을 사용하여 부적절하게 변경되었는지 확인하기 어려운 경우 구성을 알려진 양호한 구성으로 되돌립니다.

   이전 구성을 커밋하기 전에 올바른 설정이 포함되어 있는지 검토하십시오. 예를 들어 되돌리는 구성에 최근 변경 사항이 포함되어 있지 않을 수 있으므로 백업 구성을 커밋한 후 해당 변경 사항을 적용하십시오.

   다음 모범 사례를 사용하여 권한 있는 계정에 대한 무차별 대입 공격을 방지하십시오.

   - 인증 프로파일 또는 관리 인터페이스의 인증 설정(디바이스 > 설정 > 관리 > 인증 설정)에서 시도 실패 횟수 및 잠금 시간(분)을 설정하여 방화벽이 권한 있는 계정을 잠그기 전에 허용되는 실패 시도 횟수를 제한합니다.
   - 인터페이스 관리 프로파일을 사용하여 액세스 제한
   - 권한 있는 계정에 복잡한 암호를 적용합니다.

## 관리 작업 관리 및 모니터링

작업 관리자는 마지막 방화벽 재부팅 이후 사용자와 다른 관리자가 시작한 모든 작업(예: 수동 커밋) 또는 방화벽이 시작한(예: 예약된 보고서 생성) 작업에 대한 세부 정보를 표시합니다. 작업 관리자를 사용하여 실패한 작업 문제를 해결하고, 완료된 커밋과 관련된 경고를 조사하고, 대기 중인 커밋에 대한 세부 정보를 보거나, 보류 중인 커밋을 취소할 수 있습니다.

또한 시스템 로그를 확인하여 방화벽의 시스템 이벤트를 모니터링하거나 구성 로그를 확인하여 방화벽 구성 변경 사항을 모니터링할 수 있습니다.

**STEP 1 |** 웹 인터페이스 하단에서 작업을 클릭합니다.

**STEP 2 |** 실행 중인 작업(진행 중) 또는 모든 작업(기본값)만 표시합니다. 선택적으로 유형별로 작업을 필터링합니다.

- 작업 - 관리자 시작 커밋, 방화벽 시작 커밋, 소프트웨어 또는 콘텐츠 다운로드 및 설치.
- 보고서 - 예약된 보고서입니다.
- 요청 기록 - 대시보드 또는 모니터 페이지에 액세스하여 트리거하는 쿼리를 기록합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 다음 작업 중 하나를 수행합니다.

- 작업 세부 정보 표시 또는 숨디바이스 - 기본적으로 작업 관리자는 각 작업에 대한 유형, 상태, 시작 시간 및 메시지를 표시합니다. 작업의 종료 시간 및 작업 ID를 보려면 해당 열을 표시하도록 디스플레이를 수동으로 구성해야 합니다. 열을 표시하거나 숨기려면 열 머리글에서 드롭다운을 열고 열을 선택한 다음 필요에 따라 열 이름을 선택하거나 선택 취소합니다.
- 경고 또는 실패 조사 - 작업 세부 정보를 보려면 메시지 열의 항목을 읽으십시오. 열에 **메시지가 너무 많다고 표시**되면 유형 열에서 해당 항목을 클릭하여 자세한 정보를 확인하십시오.
- 커밋 설명 표시 - 관리자가 커밋을 구성할 때 설명을 입력한 경우 메시지 열에서 커밋 설명을 클릭하여 설명을 표시할 수 있습니다.
- 대기열에서 커밋 위치 확인 - 메시지 열은 진행 중인 커밋의 대기열 위치를 나타냅니다.
- 보류 중인 커밋 취소 - 커밋 대기열 지우기를 클릭하여 보류 중인 모든 커밋을 취소합니다(사전 정의된 관리 역할에만 사용 가능). 개별 커밋을 취소하려면 해당 커밋에 대한 작업 열에서 **x**를 클릭합니다(커밋은 방화벽이 큐에서 제거할 때까지 큐에 남아 있음). 진행 중인 커밋은 취소할 수 없습니다.

## 방화벽 구성 변경 사항 커밋, 유효성 검사 및 미리 보기

커밋은 방화벽 구성에 대해 보류 중인 변경 사항을 활성화하는 프로세스입니다. 관리자 또는 위치별로 보류 중인 변경 사항을 필터링한 다음 해당 변경 사항만 미리 보고, 확인하거나 커밋할 수 있습니다. 위치는 특정 가상 시스템, 공유 정책 및 개체 또는 공유 디바이스 및 네트워크 설정일 수 있습니다.

방화벽은 이전 커밋이 진행 중인 동안 새 커밋을 시작할 수 있도록 커밋 요청을 큐에 넣습니다. 방화벽은 커밋이 시작된 순서대로 커밋을 수행하지만 방화벽에 의해 시작된 자동 커밋(예: FQDN 새로 고침)에 우선 순위를 둡니다. 그러나 대기열에 관리자가 시작한 최대 커밋 수가 이미 있는 경우 새 커밋을 시작하기 전에 방화벽이 보류 중인 커밋 처리를 완료할 때까지 기다려야 합니다. 보류 중인 커밋을 취소하거나 모든 상태의 커밋에 대한 세부 정보를 보려면 관리 작업 관리 및 모니터링을 참조하십시오.

커밋을 시작하면 방화벽은 변경 사항을 활성화하기 전에 변경 사항의 유효성을 확인합니다. 유효성 검사 출력은 커밋을 차단하는 조건(오류) 또는 알아야 할 중요한 조건(경고)을 표시합니다. 예를 들어 유효성 검사는 커밋이 성공하기 위해 수정해야 하는 잘못된 경로 대상을 나타낼 수 있습니다. 확인 프로세스를 통해 커밋하기 전에 오류를 찾아 수정할 수 있습니다(실행 중인 구성은 변경되지 않음). 이것은 고정된 커밋 창이 있고 커밋이 오류 없이 성공하는지 확인하려는 경우에 유용합니다.

Panorama™ 관리 서버에서 활성화 및 관리하는 경우 관리 방화벽은 로컬에서 커밋되거나 Panorama에서 푸시된 구성을 로컬로 테스트하여 새로운 변경 사항이 Panorama와 관리 방화벽 간의 연결을 끊지 않는지 확인합니다. 커밋된 구성이 Panorama와 관리 방화벽 간의 연결을 끊으면 방화벽이 자동으로 커밋에 실패하고 구성이 이전 실행 구성으로 되돌아갑니다. 또한 Panorama 관리 서버에서 관리하는 방화벽은 60분마다 Panorama에 대한 연결을 테스트하고 관리 방화벽이 더 이상 Panorama에 성공적으로 연결할 수 없음을 감지하면 구성을 이전 실행 구성으로 되돌립니다.

커밋, 유효성 검사, 미리보기, 저장 및 되돌리기 작업은 마지막 커밋 이후에 변경된 사항에만 적용됩니다. 구성을 마지막 커밋 이전의 상태로 복원하려면 이전에 백업한 구성을 로드해야 합니다.

여러 관리자가 동시 세션 동안 구성을 변경하는 것을 방지하려면 구성 변경을 제한하기 위한 잠금 관리를 참조하십시오.

**STEP 1 |** 커밋, 유효성 검사 또는 미리 볼 구성 변경 범위를 구성합니다.

1. 웹 인터페이스 상단에서 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

2. 다음 옵션 중 하나를 선택합니다.
   - 모든 변경 사항 커밋**(**기본값**)** - 관리 권한이 있는 모든 변경 사항에 커밋을 적용합니다. 이 옵션을 선택하면 커밋 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 커밋 범위가 결정됩니다.
   - 커밋 변경 작성자 - 관리자 또는 위치별로 커밋 범위를 필터링할 수 있습니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링할 수 있는 변경 사항이 결정됩니다.

   다른 관리자의 변경 사항을 커밋하려면 로그인에 사용한 계정에 운용 관리자 역할 또는 다른 관리자를 위한 커밋 권한이 활성화된 관리자 역할 프로파일이 할당되어야 합니다.
3. (선택 사항) 커밋 범위를 관리자별로 필터링하려면 커밋 변경자를 선택한 다음 인접한 링크를 클릭한 다음 관리자를 선택한 다음 확인을 클릭합니다.
4. (선택 사항) 위치별로 필터링하려면 커밋 변경자를 선택한 다음 커밋 범위에서 제외할 변경 사항을 선택 취소합니다.

   포함 및 제외된 구성 변경 간의 종속성으로 인해 유효성 검사 오류가 발생하면 모든 변경 사항을 포함하여 커밋을 수행합니다. 예를 들어, 가상 시스템에 대한 변경 사항을 커밋할 때 해당 가상 시스템에서 동일한 규칙 베이스에 대한 규칙을 추가, 삭제 또는 재배치한 모든 관리자의 변경 사항을 포함해야 합니다.

**STEP 2 |** 커밋이 활성화할 변경 사항을 미리 봅니다.

예를 들어, 모든 변경 사항을 기억하지 못하고 모든 변경 사항을 활성화하고 싶지 않은 경우에 유용할 수 있습니다.

방화벽은 커밋 범위에서 선택한 구성을 실행 중인 구성과 비교합니다. 미리보기 창은 구성을 나란히 표시하고 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)인 변경 사항을 나타냅니다.

변경 사항을 미리 보고 각 강조 표시된 차이 전후에 표시할 비교 구성 파일의 줄 수인 컨텍스트 줄을 선택합니다. 이러한 추가 행은 미리보기 출력을 웹 인터페이스의 설정과 연관시키는 데 도움이 됩니다. 변경 사항 검토가 끝나면 미리보기 창을 닫습니다.

미리보기 결과가 새 브라우저 창에 표시되기 때문에 브라우저에서 팝업을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 허용 단계를 참조하십시오.

**STEP 3 |** 변경 사항을 커밋할 개별 설정을 미리 봅니다.

이는 설정 유형 및 변경한 사람과 같은 변경 사항에 대한 세부 정보를 알고자 할 때 유용할 수 있습니다.

1. 변경 요약을 클릭합니다.
2. (선택 사항) 열 이름별로 그룹화(예: 설정 유형).
3. 변경 사항 검토를 마치면 변경 사항 요약 대화 상자를 닫습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 커밋이 성공할 수 있도록 커밋하기 전에 변경 사항을 확인하십시오.

1. 변경 사항을 확인합니다.

   결과에는 실제 커밋이 표시할 모든 오류와 경고가 표시됩니다.
2. 유효성 검사 결과가 식별하는 모든 오류를 해결합니다.

**STEP 5 |** 구성 변경 사항을 커밋합니다.

변경 사항을 커밋하고 확인하고 활성화합니다.

보류 중(아직 취소할 수 있음), 진행 중, 완료됨 또는 실패한 커밋에 대한 세부 정보를 보려면 관리 작업 관리 및 모니터링을 참조하십시오.

## 선택적 구성 변경 커밋

구성 변경은 자주 발생하며 일반적으로 다른 구성 변경 사항을 알지 못하는 여러 관리자가 수행합니다. 커밋되는 구성 개체를 제어하고 불완전한 구성이 방화벽에 커밋되는 것을 방지하는 것이 중요합니다. 보류 중인 모든 구성 변경 내용을 커밋하는 대신 커밋할 구성 개체를 선택할 수 있습니다. 선택적 커밋이 성공하면 시스템 로그가 생성됩니다.

커밋할 특정 개체를 선택하는 기능을 사용하면 커밋할 준비가 되지 않은 구성 변경을 수행하는 다른 관리자를 방해하지 않고 여러 관리자가 구성 변경을 효과적으로 수행할 수 있습니다. 구성 변경을 선택적으로 커밋하는 기능을 활용하면 정의된 운영 절차를 유지하면서 작업 범위 내에 정의되지 않은 독립적인 구성 변경을 성공적으로 수행할 수 있습니다.

**STEP 1 |** 방화벽 웹 인터페이스에 로그인합니다.

**STEP 2 |** 방화벽 및 커밋에서 구성 변경을 수행합니다.

**STEP 3 |** 커밋 범위를 커밋 변경 사항으로 변경하여 커밋할 구성 변경 사항을 선택합니다.

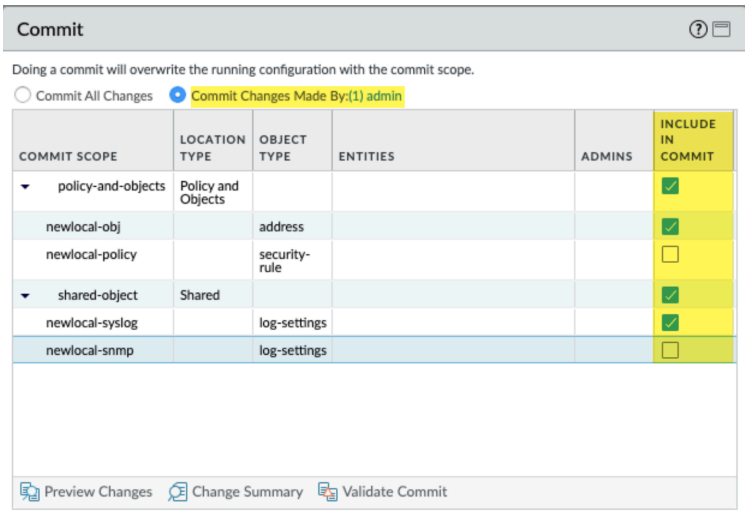
푸시 범위에는 현재 로그인한 관리자의 이름이 표시됩니다. 관리자 이름을 클릭하여 커밋되지 않은 구성을 변경한 관리자 목록을 봅니다.

**STEP 4 |** (선택 사항) 보류 중인 구성 변경 내용을 미리 보고 유효성을 검사하여 선택한 구성 개체를 커밋할지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 커밋합니다.

커밋 상태 페이지는 커밋된 구성 변경을 수행한 관리자와 커밋된 구성 변경 위치를 표시합니다.



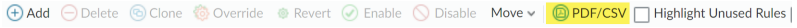

# 구성 테이블 데이터 내보내기

정책 규칙, 구성 개체 및 Panorama ™ 및 방화벽의 IPS 서명을 내보내 외부 감사인에 대한 규정 준수를 입증하고 방화벽 구성에 대한 정기적인 검토를 수행하고 방화벽 정책에 대한 보고서를 생성합니다. 이렇게 하면 감사자에게 방화벽 및 어플라이언스에 직접 액세스할 수 있도록 하거나, 스크린샷을 찍거나, XML API에 액세스하여 구성 보고서를 생성할 필요가 없습니다. 웹 인터페이스에서 정책, 개체, 네트워크, 방화벽 및 Panorama 구성에 대한 구성 테이블 데이터와 PDF 또는 CSV 파일에서 바이러스 백신, 안티 스파이웨어 및 취약점 보호 보안 프로파일의 서명 예외를 내보낼 수 있습니다.

구성 테이블 내보내기는 인쇄 기능처럼 작동하므로 생성된 파일을 Panorama 또는 방화벽으로 다시 가져올 수 없습니다. 데이터를 PDF 파일로 내보내고 테이블 데이터가 50,000행을 초과하면 데이터가 여러 PDF 파일로 분할됩니다(예: <report-name>_part1.pdf 및 <report-name>_part2.pdf). 데이터를 CSV로 내보낼 때 파일에서 데이터를 단일 파일로 내보냅니다. 이러한 내보내기 형식을 사용하면 보고서 기준과 일치하는 필터를 적용하고 PDF 보고서 내에서 검색하여 특정 데이터를 신속하게 찾을 수 있습니다. 또한 구성 테이블 데이터를 내보낼 때 이벤트를 기록하기 위해 시스템 로그가 생성됩니다.

**STEP 1 |** 웹 인터페이스를 실행하고 내보내는 데 필요한 구성 데이터를 식별합니다.

**STEP 2 |** 내보내는 데 필요한 구성 데이터를 생성하기 위해 필요에 따라 필터를 적용하고 **PDF/CSV**를 클릭합니다.




 ©2023 Palo Alto Networks, Inc.

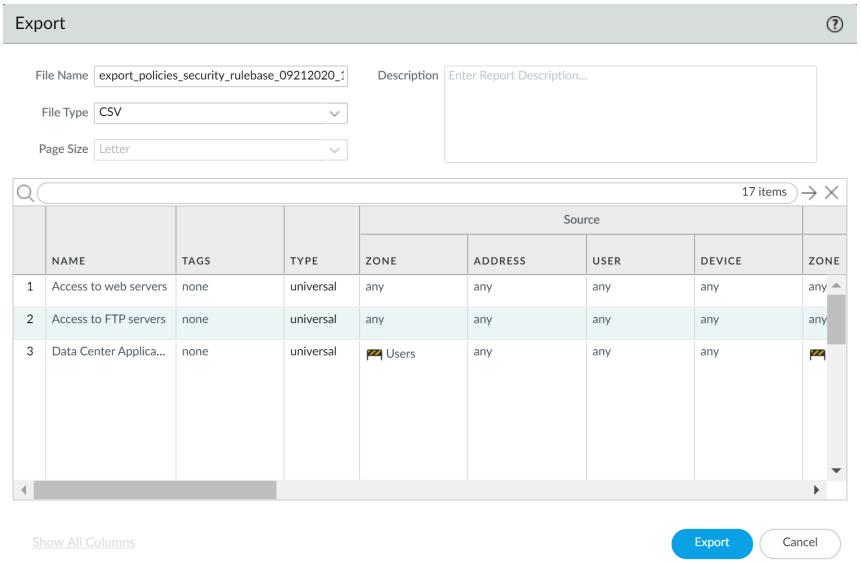
**STEP 3 |** 구성 테이블 내보내기 보고서 구성:

1. 파일 이름을 입력합니다.
2. 파일 형식을 선택합니다.
3. (선택 사항) 보고서 설명을 입력합니다.
4. 구성 테이블 데이터가 적용한 필터와 일치하는지 확인합니다.

   모든 열 표시를 선택하여 적용된 모든 필터를 표시합니다.

**STEP 4 |** 구성 테이블 데이터를 내보냅니다.

구성 테이블 내보내기는 인쇄 기능처럼 작동하며 생성된 파일을 Panorama 또는 방화벽으로 다시 가져올 수 없습니다.




**STEP 5 |** 내보낸 파일을 저장하려면 위치를 선택합니다.

## 전역 찾기를 사용하여 방화벽 또는 Panorama 관리 서버 검색

전역 찾기를 사용하면 IP 주소, 개체 이름, 정책 규칙 이름, 위협 ID, UUID 또는 애플리케이션 이름과 같은 특정 문자열에 대해 방화벽이나 Panorama에서 후보 구성을 검색할 수 있습니다. 구성 개체 및 설정을 검색하는 것 외에도 관리자가 수행한 수동 커밋을 작업 ID 또는 작업 유형별로 검색하거나 방화벽 또는 Panorama에서 수행한 자동 커밋을 수행할 수 있습니다. 검색 결과는 카테고리별로 그룹화되며 웹 인터페이스의 구성 위치에 대한 링크를 제공하므로 문자열이 참조되는 모든 위치를 쉽게 찾을 수 있습니다. 또한 검색 결과는 검색 용어 또는 문자열에 의존하거나 참조하는 다른 개체를 식별하는 데 도움이 됩니다. 예를 들어 보안 프로파일을 사용하지 않는 경우 글로벌 찾기에 프로파일 이름을 입력하여 프로파일의 모든 인스턴스를 찾은 다음 각 인스턴스를 클릭하여 구성 페이지로 이동하여 필요한 변경을 수행합니다. 모든 참조가 제거된 후 프로파일을 삭제할 수 있습니다. 종속성이 있는 모든 구성 항목에 대해 이 작업을 수행할 수 있습니다.

동영상을 시청하십시오.


©2023 Palo Alto Networks, Inc.

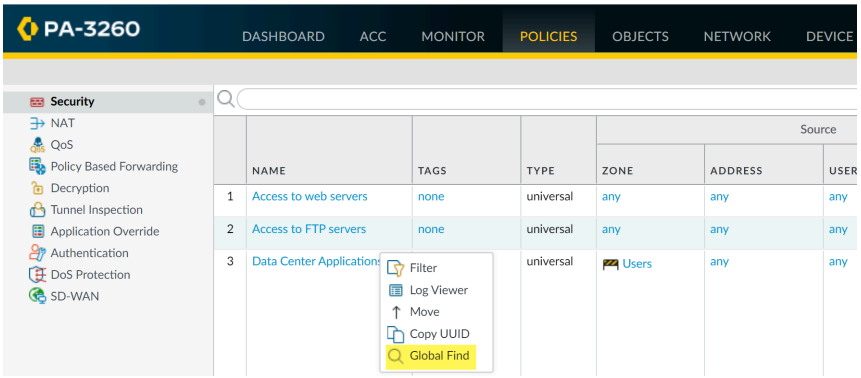
전역 찾기는 동적 콘텐츠(예: 로그, 주소 범위 또는 할당된 *DHCP* 주소)를 검색하지 않습니다. *DHCP*의 경우 *DNS* 항목과 같은 *DHCP* 서버 특성을 검색할 수 있지만 사용자에게 할당된 개별 주소는 검색할 수 없습니다. 전역 찾기는 사용자/그룹이 정책에 정의되어 있지 않으면 *User-ID*로 식별되는 개별 사용자 또는 그룹 이름도 검색하지 않습니다. 일반적으로 방화벽이 구성에 기록하는 콘텐츠만 검색할 수 있습니다.

- 웹 인터페이스의 오른쪽 위에 있는 검색 아이콘을 클릭하여 전역 찾기를 실행합니다.

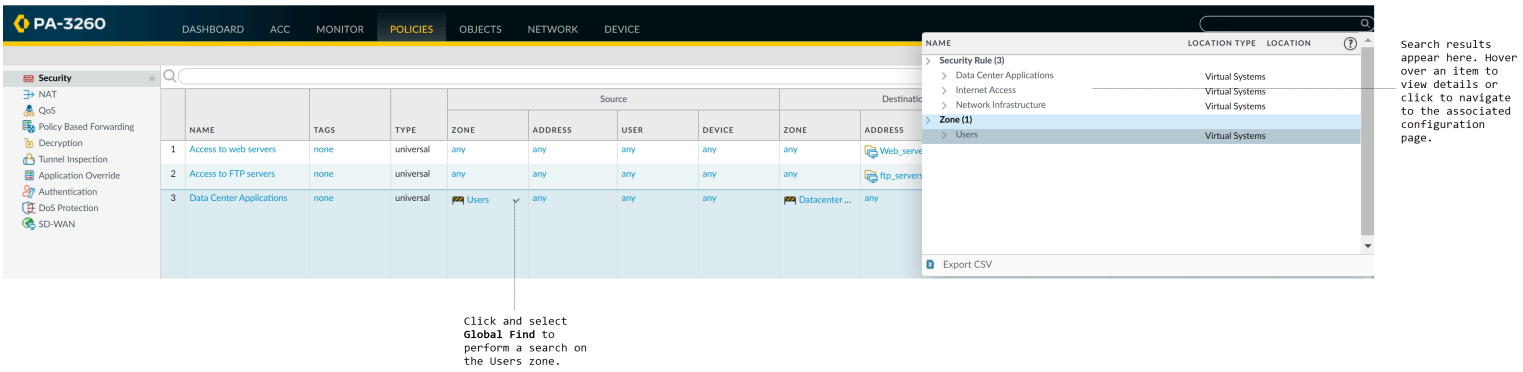



 ©2023 Palo Alto Networks, Inc.

- 구성 영역 내에서 전역 찾기에 액세스하려면 항목 옆에 있는 드롭다운을 클릭하고 전역 찾기를 선택합니다.




예를 들어 **Users**라는 영역에서 전역 찾기를 클릭하여 영역이 참조되는 각 위치에 대한 후보 구성을 검색합니다. 다음 화면 캡처는 사용자 영역에 대한 검색 결과를 보여 줍니다.




검색 팁:

- 여러 가상 시스템을 사용하도록 설정한 방화벽에서 검색을 시작하거나 사용자 지정 관리 역할 유형이 정의된 경우 전역 찾기는 관리자가 권한을 가진 방화벽 영역에 대한 결과만 반환합니다. Panorama 디바이스 그룹에도 동일하게 적용됩니다.
- 검색어의 공백은 AND 연산으로 처리됩니다. 예를 들어, **corp policy**를 검색하면 구성에 corp 및 policy가 있는 인스턴스가 검색 결과에 포함됩니다.
- 정확한 구문을 찾으려면 구를 따옴표로 묶습니다.
- 키워드를 5개 이하로 입력하거나 따옴표로 정확히 일치하는 구문을 사용합니다.
- 이전 검색을 다시 실행하려면 웹 인터페이스의 오른쪽 위에 있는 검색을 클릭하여 최근 20개 검색 목록을 확인합니다. 목록에서 항목을 클릭하여 해당 검색을 다시 실행합니다. 검색 기록은 각 관리자 계정마다 고유합니다.
- UUID를 검색하려면 UUID를 복사하여 붙여넣어야 합니다.

## 구성 변경을 제한하기 위한 잠금 관리

구성 잠금을 사용하여 수동으로 잠금을 제거하거나 방화벽이 자동으로 잠금을 제거할 때까지(커밋 후) 다른 관리자가 후보 구성을 변경하거나 구성 변경을 커밋하지 못하도록 할 수 있습니다. 잠금은 관리자가 동시 로그인 세션 동안 동일한 설정이나 상호 의존적인 설정에 대해 충돌하는 변경을 하지 않도록 합니다.


©2023 Palo Alto Networks, Inc.

방화벽은 커밋 요청을 대기열에 넣고 관리자가 커밋을 시작한 순서대로 수행합니다. 자세한 내용은 방화벽 구성 변경 내용 커밋, 유효성 검사 및 미리 보기를 참조하십시오. 대기 중인 커밋의 상태를 보려면 관리 작업 관리 및 모니터링을 참조하십시오.

- 현재 잠금에 대한 세부 정보를 봅니다.

  예를 들어 다른 관리자가 잠금을 설정했는지 확인하고 잠금을 설명하기 위해 입력한 설명을 읽을 수 있습니다.

  웹 인터페이스 상단의 자물쇠를 클릭합니다. 인접한 숫자는 현재 잠금 수를 나타냅니다.

- 구성을 잠급니다.
  1. 웹 인터페이스 상단의 자물쇠를 클릭합니다.

     잠금 이미지는 기존 잠금이인지 설정되어 있지 않은지에 따라 달라집니다.
  2. 잠금을 선택하고 잠금 유형을 선택합니다.
     - 구성 - 다른 관리자가 후보 구성을 변경하지 못하도록 차단합니다.
     - 커밋 - 다른 관리자가 후보 구성에 대한 변경 사항을 커밋하지 못하도록 차단합니다.
  3. (여러 가상 시스템이 있는 방화벽만) 특정 가상 시스템 또는 공유 위치에 대한 구성을 잠그려면 위치를 선택합니다.
  4. (선택 사항) 다른 관리자가 잠금 이유를 이해할 수 있도록 설명을 입력하는 것이 가장 좋습니다.
  5. 확인을 클릭하고 닫기를 클릭합니다.

- 구성을 잠금 해제합니다.

  구성을 잠근 운용 관리자 또는 관리자만 수동으로 잠금을 해제할 수 있습니다. 그러나 방화벽은 커밋 작업을 완료한 후 자동으로 잠금을 제거합니다.

  1. 웹 인터페이스 상단의 자물쇠를 클릭합니다.
  2. 목록에서 잠금 항목을 선택합니다.
  3. 잠금 제거, 확인, 닫기를 차례로 클릭합니다.

- 후보 구성을 변경할 때 커밋 잠금을 자동으로 적용하도록 방화벽을 구성합니다. 이 설정은 모든 관리자에게 적용됩니다.
  1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 수정합니다.
  2. 커밋 잠금 자동 획득을 선택한 다음 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 구성 백업 관리

방화벽에서 실행 중인 구성은 커밋한 모든 설정으로 구성되므로 현재 네트워크에서 다양한 유형의 트래픽을 차단하거나 허용하는 정책 규칙과 같이 활성 상태입니다. 후보 구성은 실행 중인 구성의 복사본과 마지막 커밋 이후에 변경한 비활성 변경 내용입니다. 실행 중인 또는 후보 구성의 백업 버전을 저장하면 나중에 해당 버전을 복원할 수 있습니다. 예를 들어 커밋 유효성 검사에서 현재 후보 구성에 수정할 것보다 많은 오류가 있음을 보여 주는 경우 이전 후보 구성을 복원할 수 있습니다. 먼저 백업을 저장하지 않고 현재 실행 중인 구성으로 되돌릴 수도 있습니다. 내부 검토 또는 감사를 위해 구성의 특정 부분을 내보내야 하는 경우 구성 테이블 데이터를 내보낼수 있습니다.

커밋 작업에 대한 자세한 내용은 커밋, 유효성 검사 및 미리 보기 방화벽 구성 변경 사항을 참조하십시오.

- 방화벽 구성 저장 및 내보내기
- 방화벽 구성 변경 사항 되돌리기

## 방화벽 구성 저장 및 내보내기

후보 구성의 백업을 방화벽의 영구 저장소에 저장하면 나중에 해당 백업으로 되돌릴 수 있습니다(방화벽 구성 변경 사항 되돌리기 참조). 이 기능은 시스템 이벤트나 관리자 작업으로 인해 방화벽이 재부팅될 경우 손실될 수 있는 변경 사항을 보존하는 데 유용합니다. 다시 부팅하면 PAN-OS가 실행 중인 구성의 현재 버전으로 자동 되돌아갑니다. 이 구성은 방화벽이 running-config.xml 파일에 저장합니다. 백업 저장은 현재 실행 중인 구성보다 이전의 방화벽 구성으로 되돌리려는 경우에도 유용합니다. 방화벽은 후보 구성을 영구 스토리지에 자동으로 저장하지 않습니다. 후보 구성을 기본 스냅숏 파일(.snapshot.xml) 또는 사용자 지정 이름의 스냅숏 파일로 수동으로 저장해야 합니다. 방화벽은 스냅숏 파일을 로컬에 저장하지만 외부 호스트로 내보낼 수 있습니다.

마지막 커밋 또는 재부팅 이후의 변경 사항을 되돌리기 위해 구성 백업을 저장할 필요가 없습니다. 변경 사항 되돌리기 > 구성을 선택하면 됩니다(방화벽 구성 변경 사항 되돌리기 참조).

설정을 편집하고 [확인]을 클릭하면 방화벽이 후보 구성을 업데이트하지만 백업 스냅숏은 저장하지 않습니다.

또한 변경 사항을 저장해도 활성화되지 않습니다. 변경 내용을 활성화하려면 커밋을 수행합니다(방화벽 구성 변경 내용 커밋, 유효성 검사 및 미리 보기 참조).

*Palo Alto Networks*는 방화벽 외부의 호스트에 중요한 구성을 백업할 것을 권장합니다.

**STEP 1 |** 방화벽이 재부팅될 때 보존할 변경 내용이 포함된 경우 후보 구성의 로컬 백업 스냅숏을 저장합니다.

이러한 변경 사항은 현재 로그인 세션에서 완료할 수 없는 변경과 같이 커밋할 준비가 되지 않은 변경 사항입니다.

기본 스냅숏 파일(.snapshot.xml)을 모든 관리자가 변경한 내용으로 덮어쓰려면 다음 단계 중 하나를 수행합니다.


©2023 Palo Alto Networks, Inc.

- 디바이스 > 설정 > 작업 및 후보 구성 저장을 선택합니다.
- 운용 관리자 역할이 할당된 관리자 계정 또는 다른 관리자를 위해 저장 권한이 활성화된 관리자 역할 프로파일로 방화벽에 로그인합니다. 그런 다음 웹 인터페이스 상단에서 구성 > 변경 사항 저장을 선택한 다음 모든 변경 사항 저장 및 저장을 선택합니다.

기본 스냅숏 파일을 덮어쓰지 않고 모든 관리자가 변경한 내용을 모두 포함하는 스냅숏을 생성하려면 다음과 같이 하십시오.

1. 디바이스 > 설정 > 작업 및 이름이 지정된 구성 스냅샷 저장을 선택합니다.
2. 새 구성 파일 또는 기존 구성 파일의 이름을 지정합니다.
3. 확인을 클릭하고 닫기를 클릭합니다.

기본 스냅숏 파일의 일부를 덮어쓰지 않고 후보 구성에 대한 특정 변경 사항만 저장하려면:

1. 원하는 변경 내용을 저장하는 데 필요한 역할 권한이 있는 관리자 계정으로 방화벽에 로그인합니다.
2. 웹 인터페이스 상단에서 구성 > 변경사항 저장을 선택합니다.
3. 변경 사항 저장을 선택합니다.
4. 관리자별로 저장 범위를 필터링하려면 **<administrator-name>**을 클릭하고 관리자를 선택한 다음 확인을 클릭합니다.
5. 위치별로 저장 범위를 필터링하려면 제외할 위치를 선택 취소합니다. 위치는 특정 가상 시스템, 공유 정책 및 개체 또는 공유 디바이스 및 네트워크 설정일 수 있습니다.
6. 저장을 클릭하고 새 구성 파일 또는 기존 구성 파일의 이름을 지정한 다음 확인을 클릭합니다.

**STEP 2 |** 후보 구성, 실행 중인 구성 또는 방화벽 상태 정보를 방화벽 외부의 호스트로 내보냅니다.

[디바이스 > 설정 > 작업]을 선택한 다음 내보내기 옵션을 클릭합니다.

- 명명된 구성 스냅숏 내보내기 - 현재 실행 중인 구성, 지정된 후보 구성 스냅숏 또는 이전에 불러온 구성(후보 또는 실행 중)을 내보냅니다. 방화벽은 지정한 이름의 XML 파일로 구성을 내보냅니다.
- 구성 버전 내보내기 —XML 파일로 내보낼 실행 중인 구성의 버전을 선택합니다. 방화벽은 구성이 변경될 때마다 버전을 생성합니다.
- 디바이스 상태 내보내기 —방화벽 상태 정보를 번들로 내보냅니다. 실행 중인 구성 외에도 상태 정보에는 Panorama에서 푸시된 디바이스 그룹 및 템플릿 설정이 포함됩니다. 방화벽이 GlobalProtect 포털인 경우 정보에는 인증서 정보, 새틀라이트 목록 및 새틀라이트 인증 정보도 포함됩니다. 방화벽이나 포털을 교체하는 경우 상태 번들을 가져와 교체에 대해 내보낸 정보를 복원할 수 있습니다.

## 방화벽 구성 변경 사항 되돌리기

작업을 되돌리면 현재 후보 구성의 설정을 다른 구성의 설정으로 바꿉니다. 변경 내용을 수동으로 재구성하는 대신 여러 설정의 변경 내용을 단일 작업으로 취소하려는 경우에 유용합니다.

마지막 커밋 이후 방화벽 구성에 대한 보류 중인 변경 내용을 되돌릴 수 있습니다. 방화벽은 관리자 또는 위치에 의해 보류 중인 변경 내용을 필터링하는 옵션을 제공합니다. 위치는 특정 가상 시스템, 공유 정책 및 개체 또는 공유 디바이스 및 네트워크 설정일 수 있습니다. 현재 실행 중인 구성보다 일찍 실행 중인 후보 구성에 대한 스냅숏 파일을 저장한 경우(방화벽 저장 및 내보내기 구성 참조) 해당 스냅숏으로 되돌릴

 ©2023 Palo Alto Networks, Inc.

수도 있습니다. 스냅숏으로 되돌리면 마지막 커밋 전에 존재했던 후보 구성을 복원할 수 있습니다. 방화벽은 변경 내용을 커밋할 때마다 새 버전의 실행 중인 구성을 자동으로 저장하며 이러한 버전을 복원할 수 있습니다.

- 현재 실행 중인 구성(running-config.xml 파일)으로 되돌립니다.

  이 작업은 마지막 커밋 이후 후보 구성에 대한 변경 내용을 취소합니다.

  모든 관리자가 변경한 모든 변경 내용을 되돌리려면 다음 단계 중 하나를 수행합니다.

  - 디바이스 > 설정 > 작업을 선택한 다음 실행 중인 구성으로 되돌리고 예를 클릭하여 작업을 확인합니다.
  - 수퍼사용자 역할 또는 다른 관리자에 대한 커밋 권한이 활성화된 관리자 역할 프로파일이 할당된 관리 계정으로 방화벽에 로그인합니다. 그런 다음 웹 인터페이스 상단에서 구성 > 변경사항 되돌리기를 선택한 다음 모든 변경사항 되돌리기 및 되돌리기를 선택합니다.

  후보 구성에 대한 특정 변경 내용만 되돌리려면 다음을 수행합니다.

  1. 원하는 변경 내용을 되돌리는 데 필요한 역할 권한이 있는 관리 계정을 사용하여 방화벽에 로그인합니다.

     커밋 작업을 제어하는 권한도 되돌리기 작업을 제어합니다.

  2. 웹 인터페이스 상단에서 구성 > 변경 사항 되돌리기를 선택합니다.
  3. 변경 사항 되돌리기를 선택합니다.
  4. 관리자별로 되돌리기 범위를 필터링하려면 **<administrator-name>**을 클릭하고 관리자를 선택한 다음 확인을 클릭합니다.
  5. 위치로 되돌리기 범위를 필터링하려면 제외할 위치를 선택 취소합니다.
  6. 변경 사항을 되돌립니다.

- 후보 구성의 기본 스냅숏으로 돌아갑니다.

  웹 인터페이스 상단에서 구성 > 변경사항 저장을 클릭할 때 생성하거나 덮어쓰는 스냅숏입니다.

  1. 디바이스 > 설정 > 작업 및 마지막으로 저장한 구성으로 되돌리기를 선택합니다.
  2. 예를 클릭하여 작업을 확인합니다.
  3. (선택 사항) 실행 중인 구성을 스냅샷으로 덮어쓰려면 커밋을 클릭합니다.

- 방화벽에 저장된 실행 중인 구성의 이전 버전으로 돌아갑니다.

  방화벽은 구성이 변경될 때마다 버전을 생성합니다.

  1. 디바이스 > 설정 > 작업 및 구성 버전 로드를 선택합니다.
  2. 구성 버전을 선택한 다음 확인을 클릭합니다.
  3. (선택 사항) 실행 중인 구성을 방금 복원한 버전으로 덮어쓰려면 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

- 다음 중 하나로 되돌립니다.
  - 이전에 불러온 실행 중인 구성의 사용자 지정 명명 버전
  - 기본 스냅숏 대신 사용자 지정 후보 구성 스냅숏
    1. 디바이스 > 설정 > 작업을 선택하고 이름이 지정된 구성 스냅샷 로드를 클릭합니다.
    2. 스냅샷 이름을 선택하고 확인을 클릭합니다.
    3. (선택 사항) 실행 중인 구성을 스냅샷으로 덮어쓰려면 커밋을 클릭합니다.

- 이전에 외부 호스트로 내보낸 실행 중인 또는 후보 구성으로 되돌아갑니다.
  1. 디바이스 > 설정 > 작업을 선택하고 이름이 지정된 구성 스냅샷 가져오기, 찾아보기를 차례로 클릭합니다. 외부 호스트에서 구성 파일을 선택하고 확인을 클릭합니다.
  2. 이름이 지정된 구성 스냅샷 로드를 클릭하고 방금 가져온 구성 파일의 이름을 선택한 다음 확인을 클릭합니다.
  3. (선택 사항) 실행 중인 구성을 방금 가져온 스냅샷으로 덮어쓰려면 커밋을 클릭합니다.

- 방화벽에서 내보낸 상태 정보를 복원합니다.

  실행 중인 구성 외에도 상태 정보에는 Panorama에서 푸시된 디바이스 그룹 및 템플릿 설정이 포함됩니다. 방화벽이 GlobalProtect 포털인 경우 정보에는 인증서 정보, 새틀라이트 목록 및 새틀라이트 인증 정보도 포함됩니다. 방화벽이나 포털을 교체하는 경우 상태 번들을 가져와 교체에 대한 정보를 복원할 수 있습니다.

  상태 정보 가져오기:

  1. 디바이스 > 설정 > 작업을 선택하고 디바이스 상태 가져오기, 상태로 찾아보기를 차례로 클릭합니다. 번들을 선택하고 확인을 클릭합니다.
  2. (선택 사항) 가져온 상태 정보를 실행 중인 구성에 적용하려면 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 방화벽 관리자 관리

관리 계정은 Palo Alto Networks 방화벽 관리자의 역할과 인증 방법을 지정합니다. 모든 Palo Alto Networks 방화벽에는 방화벽에 대한 전체 읽기-쓰기 액세스(운용 관리자 액세스라고도 함)를 제공하는 사전 정의된 기본 관리 계정(admin)이 있습니다.

가장 좋은 방법은 방화벽의 관리 또는 보고 기능에 액세스해야 하는 각 사람에 대해 별도의 관리 계정을 만드는 것입니다. 이렇게 하면 무단 구성으로부터 방화벽을 더 잘 보호할 수 있고 개별 관리자의 작업을 기록할 수 있습니다. 성공적인 공격을 방지하는 방식으로 방화벽 및 기타 보안 디바이스에 대한 관리 액세스를 보호하려면 관리 액세스 모범 사례를 따라야 합니다.

- 관리 역할 유형
- 관리자 역할 프로파일 구성
- 관리 인증
- 관리 계정 및 인증 구성
- 관리자 활동 추적 구성

## 관리 역할 유형

역할은 관리자가 방화벽에 액세스하는 유형을 정의합니다. 관리자 유형은 다음과 같습니다.

- 역할 기반— 웹 인터페이스, CLI 및 XML API의 기능 영역에 대한 보다 세분화된 액세스 제어를 위해 구성할 수 있는 사용자 지정 역할입니다. 예를 들어 웹 인터페이스의 방화벽 및 네트워크 구성 영역에 대한 액세스를 제공하는 운영 직원에 대한 관리자 역할 프로파일과 보안 정책 정의, 로그 및 보고서에 대한 액세스를 제공하는 보안 관리자를 위한 별도의 프로파일을 만들 수 있습니다. 여러 가상 시스템이 있는 방화벽에서는 역할이 모든 가상 시스템 또는 특정 가상 시스템에 대한 액세스를 정의하는지의 여부를 선택할 수 있습니다. 제품에 새 기능이 추가되면 해당 액세스 권한으로 역할을 업데이트해야 합니다. 방화벽은 사용자 지정 역할 정의에 새 기능을 자동으로 추가하지 않습니다. 사용자 지정 관리자 역할에 대해 구성할 수 있는 권한에 대한 자세한 내용은 참조를 참조하십시오. 웹 인터페이스 관리자 액세스.
- 동적— 방화벽에 대한 액세스를 제공하는 기본 역할입니다. 새 기능이 추가되면 방화벽은 동적 역할의 정의를 자동으로 업데이트합니다. 수동으로 업데이트할 필요가 없습니다. 다음 표에는 동적 역할과 연결된 액세스 권한이 나열됩니다.

| 동적 역할 | 권한 |
|---|---|
| 운용 관리자 | 새 관리자 계정 및 가상 시스템 정의를 포함하여 방화벽에 대한 전체 액세스 권한입니다. Superuser 권한이 있는 관리 사용자를 만들려면 운용 관리자 사용자 권한이 있어야 합니다. |
| 운용 관리자(읽기 전용) | 방화벽에 대한 읽기 전용 액세스입니다. |
| 디바이스 관리자 | 새 계정 또는 가상 시스템을 정의하는 것을 제외한 모든 방화벽 설정에 대한 전체 액세스 권한입니다. |


©2023 Palo Alto Networks, Inc.

| 동적 역할 | 권한 |
| --- | --- |
| 디바이스 관리자(읽기 전용) | 암호 프로파일(액세스 없음) 및 관리자 계정(로그인한 계정만 표시됨)을 제외한 모든 방화벽 설정에 대한 읽기 전용 액세스입니다. |
| 가상 시스템 관리자 | 방화벽에서 선택한 가상 시스템에 액세스하여 가상 시스템의 특정 측면을 생성하고 관리할 수 있습니다. 가상 시스템 관리자는 네트워크 인터페이스, VLAN, 가상 와이어, 가상 라우터, IPSec 터널, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다. |
| 가상 시스템 관리자(읽기 전용) | 방화벽에서 선택한 가상 시스템과 가상 시스템의 특정 측면에 대한 읽기 전용 액세스입니다. 읽기 전용 액세스 권한이 있는 가상 시스템 관리자는 네트워크 인터페이스, VLAN, 가상 와이어, 가상 라우터, IPSec 터널, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다. |

## 관리자 역할 프로파일 구성

관리 역할 프로파일을 사용하면 중요한 회사 정보와 최종 사용자의 개인 정보 보호를 보장하기 위해 세분화된 관리 액세스 권한을 정의할 수 있습니다.

최소 권한 액세스 원칙에 따라 관리자가 자신의 작업을 수행하기 위해 액세스해야 하는 관리 인터페이스 영역에만 액세스할 수 있도록 하는 관리자 역할 프로파일을 만들고 관리 액세스 모범 사례를 따릅니다.

**STEP 1 |** 디바이스 > 관리자 역할을 선택한 다음 추가를 클릭합니다.

**STEP 2 |** 역할을 식별하려면 이름을 입력합니다.

**STEP 3 |** 역할의 범위로 디바이스 또는 가상 시스템을 선택합니다.

**STEP 4 |** 웹 **UI** 및 **REST API** 탭에서 각 기능 영역의 아이콘을 클릭하여 원하는 설정으로 전환합니다. 활성화, 읽기 전용 또는 비활성화를 합니다. **XML API** 탭의 경우 사용 설정 또는 비활성화합니다. 웹 **UI** 옵션에 대한 자세한 내용은 웹 인터페이스 액세스 권한을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 명령줄 탭을 선택한 다음 CLI 액세스 옵션을 선택합니다. 역할 범위는 사용 가능한 옵션을 제어합니다.

- 디바이스 역할:
  - 없음 - CLI 액세스는 허용되지 않습니다(기본값).
  - 수퍼유저 - 전체 액세스. 새 관리자 계정 및 가상 시스템을 정의할 수 있습니다. 수퍼유저만 수퍼유저 권한을 가진 사용자(관리자)를 만들 수 있습니다.
  - 슈퍼리더 - 전체 읽기 전용 액세스.
  - **deviceadmin** - 새 계정 또는 가상 시스템을 정의하는 것을 제외한 모든 설정에 대한 전체 액세스.
  - **devicereader** - 암호 프로파일(액세스 없음) 및 관리자 계정(로그인한 계정만 표시됨)을 제외한 모든 설정에 대한 읽기 전용 액세스.
- 가상 시스템 역할:
  - 없음 - 액세스가 허용되지 않습니다(기본값).
  - **vsysadmin** - 가상 시스템의 특정 측면을 생성하고 관리하기 위해 특정 가상 시스템에 액세스합니다. 정적 및 동적 라우팅, 인터페이스 IP 주소, IPSec 터널, VLAN, 가상 와이어, 가상 라우터, GRE 터널, DCHP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일을 포함한 방화벽 수준 또는 네트워크 수준 기능에 대한 액세스를 활성화하지 않습니다.
  - **vsysreader** - 가상 시스템의 특정 측면에 대한 특정 가상 시스템에 대한 읽기 전용 액세스. 정적 및 동적 라우팅, 인터페이스 IP 주소, IPSec 터널, VLAN, 가상 와이어, 가상 라우터, GRE 터널, DCHP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일을 포함한 방화벽 수준 또는 네트워크 수준 기능에 대한 액세스를 활성화하지 않습니다.

**STEP 6 |** 확인을 클릭하여 프로파일을 저장합니다.

**STEP 7 |** 관리자에게 역할을 할당합니다. 방화벽 관리자 계정 구성을 참조하십시오.

## 예제 관리자 역할 프로파일 구성

이 예제에서는 잠재적인 문제를 조사하기 위해 액세스해야 하는 SOC(보안 운영 센터) 관리자의 관리자 역할 프로파일을 보여 주겠습니다. SOC 관리자는 방화벽의 여러 영역에 대한 읽기 액세스가 필요하지만 일반적으로 쓰기 액세스가 필요하지 않습니다. 이 예제에서는 관리자 역할 프로파일의 탭 네 개를 모두 다루며 각 단계는 프로파일이 SOC 관리자에 대한 특정 액세스 영역을 활성화하거나 비활성화하는 이유를 설명합니다.

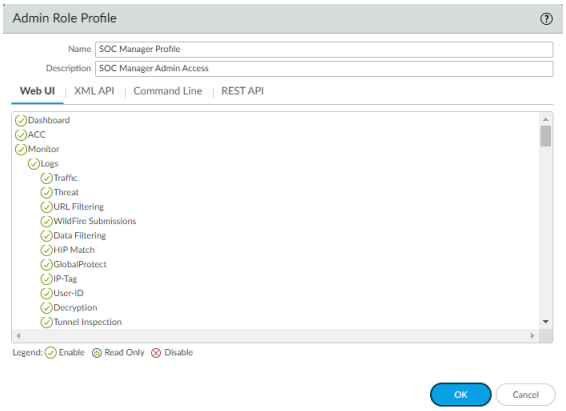
이것은 가상의 ***SOC*** 관리자를 위한 예제 프로파일입니다. 관리자가 관리하는 기능과 작업을 수행하는 데 필요한 액세스에 따라 관리자에 대한 관리 역할 프로파일을 구성합니다. 불필요한 액세스를 사용하지 마십시오. 동일한 업무를 공유하는 각 관리 그룹과 고유한 의무가 있는 관리자에 대해 별도의 프로파일을 생성합니다. 각 관리자는 업무를 수행하는 데 필요한 정확한 액세스 수준을 가져야 하며 그 이상으로 액세스할 수 없어야 합니다.

 ©2023 Palo Alto Networks, Inc.

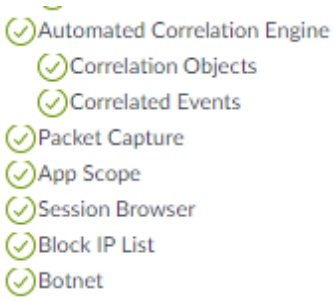
**STEP 1 |** 웹 UI 액세스 권한을 구성합니다. 웹 UI 화면의 각 스니핑에는 웹 UI 사용 권한이 다른 영역이 표시됩니다. 권한은 웹 UI에 탭이 표시되고 다른 작업에 대한 사용 권한뒤에 표시되는 순서대로 방화벽 탭에 의해 나열됩니다.

방화벽의 대시보드, **ACC**및 모니터 > 로그 영역에는 구성 요소가 포함되지 않습니다. 모든 개체는 정보를 보유하고 있습니다(읽기 전용이므로 사용 및 비활성화 간에만 전환할 수 있음). SOC 관리자는 잠재적인 문제를 조사해야 하므로 SOC 관리자는 이러한 탭의 정보에 액세스해야 합니다.

프로파일 이름과 설명을 통해 프로파일의 목표를 쉽게 이해할 수 있습니다. 이 스니핑에는 모든 **Logs** 사용 권한이 표시되지는 않지만 이 프로파일에 대해 모두 사용할 수 있습니다.



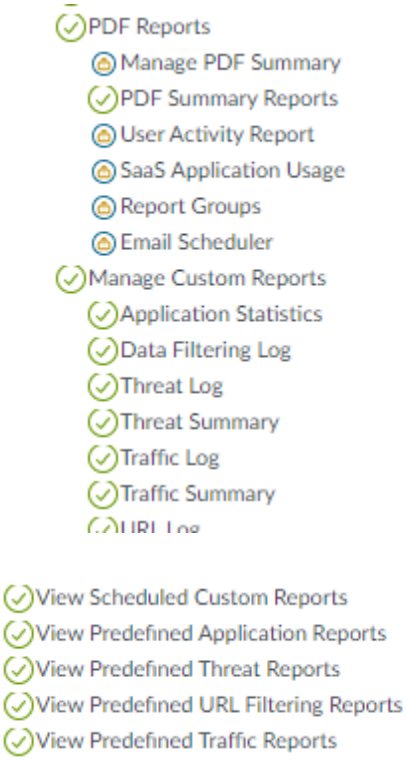

다음 스니핑에는 모니터 탭에서 자세한 정보 개체에 대한 사용 권한이 표시됩니다. SOC 관리자는 이러한 도구를 사용하여 잠재적인 문제를 조사하므로 액세스가 필요합니다.



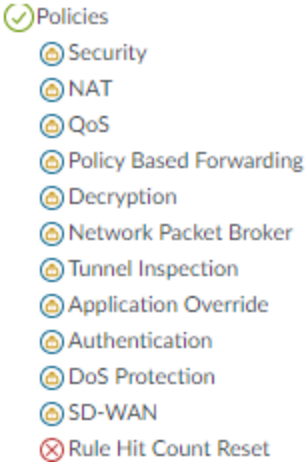

다음 두 개의 스닙에는 PDF 보고서, 맞춤 리포트 및 모니터 탭에서 사전 정의된 보고서에 대한 사용 권한이 표시됩니다. SOC 관리자는 정보를 수집하기 위해 PDF 보고서에 액세스해야 하지만 이 예에서는 SOC 관리자가 보고서를 구성할 필요가 없으므로 읽기 전용으로 액세스할 수 있습니다(요약 보고서는 구성할 수 없습니다). 그러나 SOC 관리자는 특정 잠재적인 문제를 조사하기 위해 맞춤 리포트를 관리해야 하므로 모든 맞춤 리포트(스닙에 표시되지 않은 보고서 포함)에 대한 전체 액세스 권한이 부여됩


©2023 Palo Alto Networks, Inc.

니다. 마지막으로 SOC 관리자는 잠재적인 문제를 조사하기 위해 사전 정의된 보고서에 액세스해야 합니다.



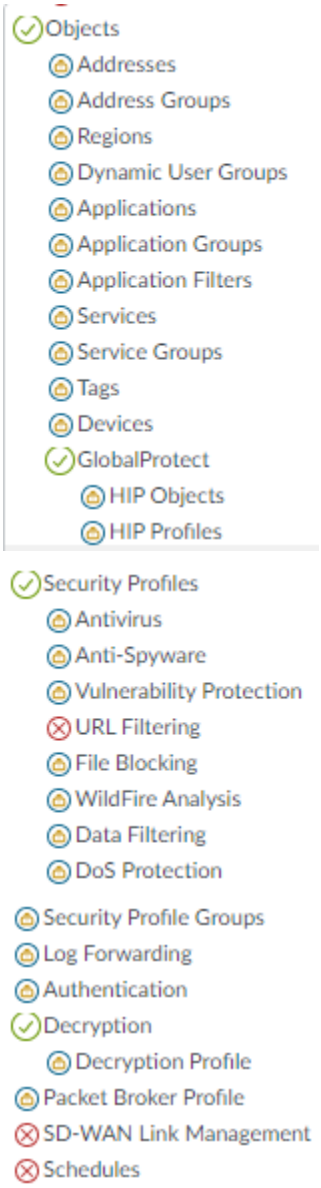

SOC 관리자는 방화벽을 구성하는 관리자가 아닌 조사자이므로 규칙 적중 수를 재설정하는 경우를 제외하고 정책 탭에 대한 권한은 읽기 전용입니다. 규칙 적중 수를 재설정하는 것은 SOC Manager의 임무 중 하나가 아니며 히트 수를 변경하면 다른 관리자에게 부정적인 영향을 미치거나 혼동할 수 있으므로 액세스가 비활성화됩니다. 읽기 액세스를 통해 SOC 관리자는 SOC 관리자가 의심되는 정책 구성에 문제가 발생했을 수 있습니다.




개체 탭에 대한 권한은 동일한 이유로 읽기 전용으로 읽기 전용입니다. SOC 관리자의 업무에 포함되지 않은 영역의 경우 액세스가 비활성화됩니다. 이 예제에서는 SOC Manager에서 이 예제에서 다른

 ©2023 Palo Alto Networks, Inc.

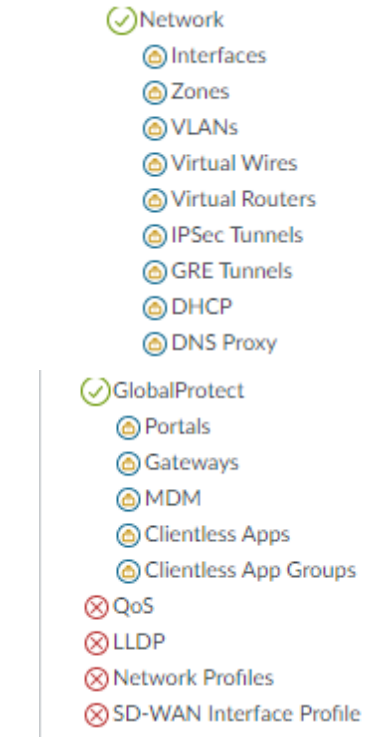
관리자의 통제하에 있는 **URL** 필터링, **SD-WAN** 링크 관리 및 일정을 제외한 모든 개체에 대한 개체 구성을 조사할 수 있는 읽기 전용 액세스 권한이 있습니다.



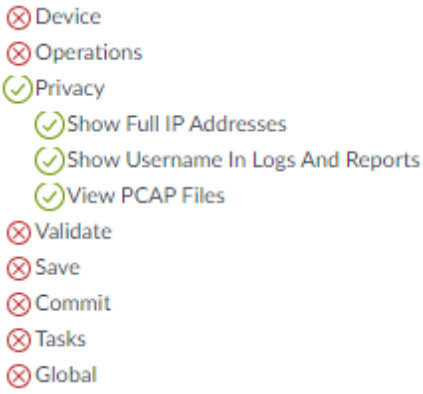

네트워크 탭 권한의 경우 시나리오와 유사합니다. SOC Manager는 개체를 구성할 필요는 없지만 문제를 조사하기 위해 정보가 필요할 수 있으므로 읽기 전용 액세스는 SOC 관리자가 조사해야 할 영역에

 ©2023 Palo Alto Networks, Inc.

할당됩니다. 이 예제에서는 이러한 항목이 SOC 관리자의 업무에 포함되지 않으므로 QoS, LLDP, 네트워크 프로파일 또는 SD-WAN 인터페이스 프로파일에 대한 액세스가 비활성화됩니다.



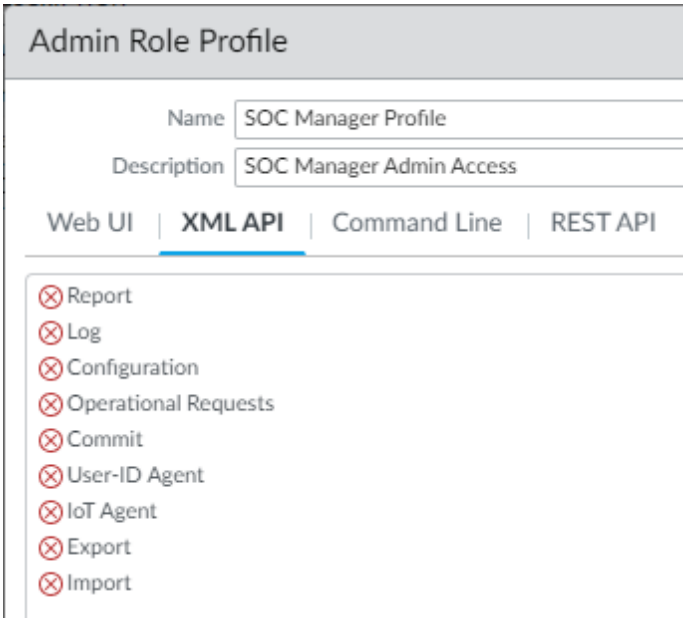

이 예제에서는 SOC 관리자가 조사를 위해 디바이스 탭 기능에 액세스할 필요가 없으므로 모든 디바이스 탭 권한이 차단됩니다. 또한 조사에 커밋 작업이나 나머지 작업에 대한 액세스가 필요하지 않으므로 이러한 사용 권한도 차단됩니다.




 ©2023 Palo Alto Networks, Inc.

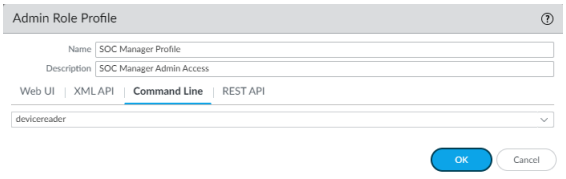
**STEP 2 |** XML API 액세스 권한을 구성합니다.

다음 스니핑은 SOC 관리자가 XML API 명령을 사용하여 방화벽에 액세스하지 않기 때문에 SOC 관리자에 대해 모든 XML API 사용 권한이 비활성화되어 있음을 보여 줍니다.




**STEP 3 |** 명령줄(CLI) 액세스 권한을 구성합니다.

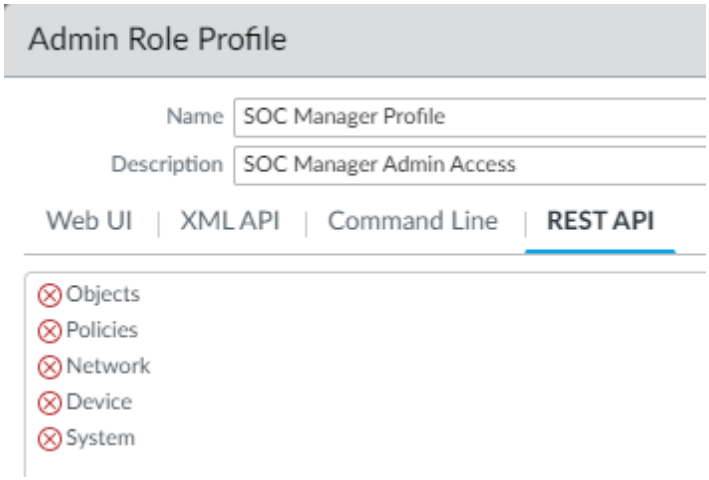
CLI 액세스 권한은 SOC 관리자가 로그 및 기타 모니터링 도구에 액세스해야 하며 잠재적인 문제를 조사하기 위해 특정 구성을 볼 수 있어야 하기 때문에 SOC 관리자에 대해서만 읽기 전용입니다. 그러나 SOC 관리자는 방화벽을 구성하지 않으므로 구성 권한이 할당되지 않습니다. SOC 관리자가 암호 프로파일이나 다른 관리 계정에 액세스할 필요가 없기 때문에 액세스 수준은 슈퍼리더 대신 디바이스 판독기로 설정됩니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** REST API 액세스 권한 구성.

SOC 관리자는 REST API 명령을 사용하여 방화벽에 액세스하지 않으므로 모든 REST API 액세스가 비활성화됩니다.




## 관리 인증

방화벽 관리자에 대해 다음 유형의 인증 및 권한 부여(역할 및 액세스 도메인 할당)를 구성할 수 있습니다.

| 인증 방법 | 권한 부여 방법 | 설명 |
|---|---|---|
| 로컬 | 로컬 | 관리 계정 자격 증명 및 인증 메커니즘은 방화벽에 로컬입니다. 방화벽에 로컬인 사용자 데이터베이스가 있거나 없는 계정을 정의할 수 있습니다. 로컬 데이터베이스 사용의 장단점은 로컬 인증을 참조하십시오. 방화벽을 사용하여 역할 할당을 관리하지만 액세스 도메인은 지원되지 않습니다. 자세한 내용은 방화벽 관리자에 대한 로컬 또는 외부 인증 구성을 참조하십시오. |
| SSH 키 | 로컬 | 관리 계정은 방화벽에 로컬이지만 CLI에 대한 인증은 SSH 키를 기반으로 합니다. 방화벽을 사용하여 역할 할당을 관리하지만 액세스 도메인은 지원되지 않습니다. 자세한 내용은 CLI에 대한 SSH 키 기반 관리자 인증 구성을 참조하십시오. |
| 인증서 | 로컬 | 관리 계정은 방화벽에 대해 로컬이지만 웹 인터페이스에 대한 인증은 클라이언트 인증서를 기반으로 합니다. 방화벽을 사용하여 역할 할당을 관리하지만 액세스 도메인은 지원되지 않습니다. 자세한 내용은 웹 인터페이스에 대한 인증서 기반 관리자 인증 구성을 참조하십시오. |
| 외부 서비스 | 로컬 | 방화벽에서 로컬로 정의하는 관리 계정은 외부 Multi-Factor Authentication, SAML, Kerberos, TACACS+, RADIUS 또는 LDAP 서버에 정의된 계정에 대한 참조 역할을 합니다. 외부 서버가 인증을 수행합니다. 방화벽을 사용하여 역할 할당을 관리하지만 액세스 도메인은 |


©2023 Palo Alto Networks, Inc.

| 인증 방법 | 권한 부여 방법 | 설명 |
|---|---|---|
| | | 지원되지 않습니다. 자세한 내용은 방화벽 관리자에 대한 로컬 또는 외부 인증 구성을 참조하십시오. |
| 외부 서비스 | 외부 서비스 | 관리 계정은 외부 SAML, TACACS+ 또는 RADIUS 서버에서 정의됩니다. 서버는 인증과 권한 부여를 모두 수행합니다. 인증을 위해 TACACS+ 또는 RADIUS 서버에서 VSA(Vendor-Specific Attributes)를 정의하거나 SAML 서버에서 SAML 속성을 정의합니다. PAN-OS는 속성을 관리자 역할, 액세스 도메인, 사용자 그룹 및 방화벽에서 정의한 가상 시스템에 매핑합니다. 자세한 내용은 다음을 참조하세요.<br>• SAML 인증 구성<br>• TACACS+ 인증 구성<br>• RADIUS 인증 구성 |

## 관리 계정 및 인증 구성

인증 프로파일을 이미 구성했거나(인증 프로파일 및 시퀀스 구성 참조) 관리자를 인증하는 데 필요하지 않은 경우 방화벽 관리자 계정을 구성할 준비가 된 것입니다. 그렇지 않으면 아래 나열된 다른 절차 중 하나를 수행하여 특정 유형의 인증에 대한 관리 계정을 구성합니다.

- 방화벽 관리자 계정 구성
- 방화벽 관리자에 대한 로컬 또는 외부 인증 구성
- 웹 인터페이스에 대한 인증서 기반 관리자 인증 구성
- CLI에 대한 SSH 키 기반 관리자 인증 구성
- API 키 수명 구성

### 방화벽 관리자 계정 구성

관리 계정은 방화벽 관리자의 역할과 인증 방법을 지정합니다. 역할을 할당하고 인증을 수행하는 데 사용하는 서비스는 계정을 방화벽, 외부 서버 또는 둘 다에 추가할지의 여부를 결정합니다(관리 인증 참조). 인증 방법이 로컬 방화벽 데이터베이스 또는 외부 서비스에 의존하는 경우 관리 계정을 추가하기 전에 인증 프로파일을 구성해야 합니다(관리 계정 및 인증 구성 참조). 인증 프로파일을 이미 구성했거나 방화벽 데이터베이스 없이 로컬 인증을 사용하려는 경우 다음 단계를 수행하여 방화벽에 관리 계정을 추가합니다.



방화벽의 관리 또는 보고 기능에 액세스해야 하는 각 사람에 대해 별도의 관리 계정을 생성합니다. 이렇게 하면 무단 구성으로부터 방화벽을 더 잘 보호하고 개별 관리자의 작업을 기록할 수 있습니다.

관리 액세스 모범 사례를 따라 성공적인 공격을 방지하는 방식으로 방화벽 및 기타 보안 디바이스에 대한 관리 액세스를 보호하고 있는지 확인하십시오.

**STEP 1 |** 지원되는 관리자 계정 수를 수정합니다.


©2023 Palo Alto Networks, Inc.

일반 작동 모드 또는 FIPS-CC 모드에서 방화벽에 대해 지원되는 총 동시 관리 계정 세션 수를 구성합니다. 최대 4개의 동시 관리 계정 세션을 허용하거나 무제한의 동시 관리 계정 세션을 지원하도록 방화벽을 구성할 수 있습니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 최대 세션 수를 편집하여 모든 관리자 및 사용자 계정에 허용되는 지원되는 동시 세션 수(범위는 **0**~ **4**)를 지정합니다.

   관리자 계정을 무제한으로 지원하도록 방화벽을 구성하려면 **0**을 입력합니다.
3. 관리 계정에 대한 최대 세션 시간(분)을 편집합니다. 기본값은 **720**분입니다.
4. 확인을 클릭합니다.
5. 커밋합니다.



방화벽 CLI에 로그인하여 지원되는 총 동시 세션 수를 구성할 수도 있습니다.

```
admin> configure
```

```
admin# set deviceconfig setting management admin-session
 max-session-count <0-4>
```

```
admin# set deviceconfig setting management admin-session
 max-session-time <0, 60-1499>
```

```
admin# commit
```

**STEP 2 |** 디바이스 > 관리자를 선택하고 계정을 추가합니다.

**STEP 3 |** 사용자 이름을 입력합니다.

방화벽이 로컬 사용자 데이터베이스를 사용하여 계정을 인증하는 경우 데이터베이스의 계정에 대해 지정한 이름을 입력합니다(로컬 데이터베이스에 사용자 그룹 추가 참조).

**STEP 4 |** 관리자에 대해 구성한 경우 인증 프로파일 또는 시퀀스를 선택합니다.

방화벽이 계정에 대한 로컬 사용자 데이터베이스 없이 로컬 인증을 사용하는 경우 없음(기본값)을 선택한 다음 암호를 입력합니다.

**STEP 5 |** 관리자 유형을 선택합니다.

사용자에 대한 사용자 지정 역할을 구성한 경우 역할 기반을 선택한 다음 관리자 역할 프로파일을 선택합니다. 그렇지 않으면 동적(기본값)을 선택한 다음 동적 역할을 선택합니다. 동적 역할이 가상 시스템 관리자인 경우 가상 시스템 관리자가 관리할 수 있는 가상 시스템을 하나 이상 추가합니다.

**STEP 6 |** (선택 사항) 방화벽이 로컬 사용자 데이터베이스 없이 로컬로 인증하는 관리자용 암호 프로파일을 선택합니다. 자세한 내용은 암호 프로파일 정의를 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** 확인 및 커밋을 클릭합니다.

## 방화벽 관리자에 대한 로컬 또는 외부 인증 구성

로컬 인증 및 외부 인증 서비스를 사용하여 방화벽에 액세스하는 관리자를 인증할 수 있습니다. 이러한 인증 방법을 묻는 관리자는 사용자 이름 및 암호를 입력하기 위한 로그인 페이지와 같은 하나 이상의 인증 문제에 응답하도록 요청합니다.

외부 서비스를 사용하여 인증 및 권한 부여(역할 및 도메인 할당에 액세스)를 모두 관리하는 경우 다음을 참조하십시오.

- SAML 인증 구성
- TACACS+ 인증 구성
- RADIUS 인증 구성

챌린지 응답 메커니즘 없이 관리자를 인증하려면 인증서 기반 관리자 인증을 웹 인터페이스에 구성하고 CLI로 SSH 키 기반 관리자 인증을 구성할 수 있습니다.

**STEP 1 |** (외부 인증만) 방화벽이 관리자를 인증하기 위해 외부 서버에 연결할 수 있도록 합니다.

서버 프로파일 구성:

- RADIUS 서버 프로파일을 추가합니다.

  방화벽이 RADIUS를 통해 MFA(다단계 인증) 서비스와 통합되는 경우 RADIUS 서버 프로파일을 추가해야 합니다. 이 경우 MFA 서비스는 모든 인증 요소(과제)를 제공합니다. 방화벽이 벤더 API를 통해 MFA 서비스와 통합되는 경우에도 첫 번째 요소에 대해 RADIUS 서버 프로파일을 사용할 수 있지만 추가 요소에는 MFA 서버 프로파일이 필요합니다.
- MFA 서버 프로파일을 추가합니다.
- TACACS+ 서버 프로파일을 추가합니다.
- SAML IdP 서버 프로파일을 추가합니다. Kerberos Single Sign-On(SSO)과 SAML SSO를 결합할 수 없으며 한 가지 유형의 SSO 서비스만 사용할 수 있습니다.
- Kerberos 서버 프로파일을 추가합니다.
- LDAP 서버 프로파일을 추가합니다.

**STEP 2 |** (로컬 데이터베이스 인증만 해당) 방화벽에 로컬인 사용자 데이터베이스를 구성합니다.

1. 로컬 데이터베이스에 사용자 계정을 추가합니다.
2. (선택 사항) 사용자 그룹을 로컬 데이터베이스에 추가합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** (로컬 인증만) 암호 복잡성 및 만료 설정을 정의합니다.

이러한 설정은 공격자가 암호를 추측하기 어렵게 하여 무단 액세스로부터 방화벽을 보호하는 데 도움이 됩니다.

1. 모든 로컬 관리자에 대한 글로벌 암호 복잡성 및 만료 설정을 정의합니다. 설정은 암호 대신 암호 해시를 지정한 로컬 데이터베이스 계정에는 적용되지 않습니다(로컬 인증 참조).
   1. 디바이스 > 설정 > 관리를 선택한 다음 최소 암호 복잡성 설정을 편집합니다.
   2. 활성화를 선택합니다.
   3. 암호 설정을 정의하고 확인을 클릭합니다.
2. 암호 프로파일을 정의합니다.

   전역 암호 만료 설정을 재정의하려는 관리자 계정에 프로파일을 할당합니다. 프로파일은 로컬 데이터베이스와 연결되지 않은 계정에서만 사용할 수 있습니다(로컬 인증참조).
   1. 디바이스 > 암호 프로파일을 선택한 다음 프로파일을 추가합니다.
   2. 프로파일을 식별하려면 이름을 입력합니다.
   3. 암호 만료 설정을 정의하고 확인을 클릭합니다.

**STEP 4 |** (Kerberos SSO만) Kerberos 키탭을 생성합니다.

키 탭은 방화벽에 대한 Kerberos 계정 정보가 들어 있는 파일입니다. Kerberos SSO를 지원하려면 네트워크에 Kerberos 인프라가 있어야 합니다.

**STEP 5 |** 인증 프로파일을 구성합니다.



관리 계정이 여러 유형의 서버에 저장되는 경우 각 형식에 대한 인증 프로파일을 생성하고 모든 프로파일을 인증 시퀀스에 추가할 수 있습니다.

인증 프로파일 및 시퀀스를 구성합니다. 인증 프로파일에서 인증 서비스 유형 및 관련 설정을 지정합니다.

- 외부 서비스 - 외부 서비스 유형을 선택한 다음 이를 위해 만든 서버 프로파일을 선택합니다.
- 로컬 데이터베이스 인증 - 유형을 로컬 데이터베이스로 설정합니다.
- 데이터베이스가 없는 로컬 인증 - 없음으로 형식을 설정합니다
- **Kerberos SSO** - **Kerberos** 영역을 지정하고 **Kerberos Keytab**을 가져옵니다.

**STEP 6 |** 인증 프로파일 또는 시퀀스를 관리자 계정에 할당합니다.

1. 방화벽 관리자 계정을 구성합니다.
   - 구성한 인증 프로파일 또는 시퀀스를 할당합니다.
   - (로컬 데이터베이스 인증만)로컬 데이터베이스에 추가한 사용자 계정의 이름을 지정합니다.
2. 변경 사항을 커밋합니다.
3. (선택 사항) 테스트 인증 서버 연결성은 방화벽이 인증 프로파일을 사용하여 관리자를 인증할 수 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

## 웹 인터페이스에 대한 인증서 기반 관리자 인증 구성

방화벽 웹 인터페이스에 대한 암호 기반 인증에 대한 보다 안전한 대안으로 방화벽에 로컬인 관리자 계정에 대한 인증서 기반 인증을 구성할 수 있습니다. 인증서 기반 인증에는 암호 대신 디지털 서명의 교환 및 확인이 포함됩니다.

모든 관리자에 대해 인증서 기반 인증을 구성하면 방화벽의 모든 관리자에 대한 사용자 이름/암호 로그인이 비활성화됩니다. 그 후 관리자는 로그인하기 위해 인증서를 요구합니다.

**STEP 1 |** 방화벽에서 인증 기관(CA) 인증서를 생성합니다.

이 CA 인증서를 사용하여 각 관리자의 클라이언트 인증서에 서명합니다.

자체 서명된 루트 CA 인증서를 생성합니다.

또는 엔터프라이즈 *CA* 또는 타사 *CA*에서 인증서 및 개인 키를 가져옵니다.

**STEP 2 |** 웹 인터페이스에 대한 액세스를 보호하기 위해 인증서 프로파일을 구성합니다.

인증서 프로파일을 구성합니다.

- 사용자 이름 필드를 제목으로 설정합니다.
- CA 인증서 섹션에서 방금 만들거나 불러온 **CA** 인증서를 추가합니다.

**STEP 3 |** 관리자 인증을 위해 인증서 프로파일을 사용하도록 방화벽을 구성합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 관리자 인증을 위해 생성한 인증서 프로파일을 선택한 다음 확인을 클릭합니다.

**STEP 4 |** 클라이언트 인증서 인증을 사용하도록 관리자 계정을 구성합니다.

방화벽 웹 인터페이스에 액세스할 각 관리자에 대해 방화벽 관리자 계정을 구성하고 클라이언트 인증서 인증만 사용을 선택합니다.

엔터프라이즈 CA에서 생성한 클라이언트 인증서를 이미 배포한 경우 8단계로 건너뜁니다. 그렇지 않으면 5단계로 이동합니다.

**STEP 5 |** 각 관리자에 대한 클라이언트 인증서를 생성합니다.

인증서를 생성합니다. 서명자 드롭다운에서 자체 서명된 루트 CA 인증서를 선택합니다.

**STEP 6 |** 클라이언트 인증서를 내보냅니다.

1. 인증서 및 개인 키를 내보냅니다.
2. 변경 사항을 커밋합니다. 방화벽이 다시 시작하고 로그인 세션을 종료합니다. 그 이후에는 관리자가 생성한 클라이언트 인증서가 있는 클라이언트 시스템에서만 웹 인터페이스에 액세스할 수 있습니다.

**STEP 7 |** 웹 인터페이스에 액세스할 각 관리자의 클라이언트 시스템으로 클라이언트 인증서를 가져옵니다.

웹 브라우저 설명서를 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 관리자가 웹 인터페이스에 액세스할 수 있는지 확인하십시오.

1. 클라이언트 인증서가 있는 컴퓨터의 브라우저에서 방화벽 IP 주소를 엽니다.
2. 메시지가 표시되면 불러온 인증서를 선택한 다음 확인을 클릭합니다. 브라우저에 인증서 경고가 표시됩니다.
3. 브라우저 예외 목록에 인증서를 추가합니다.
4. 로그인을 클릭합니다. 웹 인터페이스는 사용자 이름이나 암호를 묻는 메시지 없이 나타나야 합니다.

## CLI에 대한 SSH 키 기반 관리자 인증 구성

SSH(Secure Shell)를 사용하여 Palo Alto Networks 방화벽의 CLI에 액세스하는 관리자의 경우 SSH 키는 암호보다 더 안전한 인증 방법을 제공합니다. SSH 키는 무차별 대입 공격의 위험을 대부분 제거하고 이중 인증(키 및 암호) 옵션을 제공하며 네트워크를 통해 암호를 보내지 않습니다. 또한 SSH 키를 사용하면 자동화된 스크립트가 CLI에 액세스할 수 있습니다.

**STEP 1 |** SSH 키 생성 도구를 사용하여 관리자의 클라이언트 시스템에서 비대칭 키 쌍을 생성합니다.

지원되는 키 형식은 IETF SECSH 및 Open SSH입니다. 지원되는 알고리즘은 DSA(1,024비트) 및 RSA(768-4,096비트)입니다.

키 쌍을 생성하는 명령은 SSH 클라이언트 설명서를 참조하십시오.

공개 키와 개인 키는 별도의 파일입니다. 방화벽이 액세스할 수 있는 위치에 둘 다 저장합니다. 보안 강화를 위해 암호를 입력하여 개인 키를 암호화합니다. 방화벽은 로그인하는 동안 관리자에게 이 암호를 입력하라는 메시지를 표시합니다.

**STEP 2 |** 공개 키 인증을 사용하도록 관리자 계정을 구성합니다.

1. 방화벽 관리자 계정을 구성합니다.
   - SSH 키 인증이 실패할 경우 대체로 사용할 인증 방법을 구성합니다. 관리자에 대한 인증 프로파일을 구성한 경우 드롭다운에서 선택합니다. 없음을 선택하면 암호와 암호 확인을 입력해야 합니다.
   - 공개 키 인증**(SSH)** 사용을 선택한 다음 키 가져오기를 선택한 다음 방금 생성한 공개 키를 찾아 확인을 클릭합니다.
2. 변경 사항을 커밋합니다.

**STEP 3 |** 개인 키를 사용하여 방화벽에 인증하도록 SSH 클라이언트를 구성합니다.

관리자의 클라이언트 시스템에서 이 작업을 수행합니다. 단계는 SSH 클라이언트 설명서를 참조하십시오.

**STEP 4 |** 관리자가 SSH 키 인증을 사용하여 방화벽 CLI에 액세스할 수 있는지 확인하십시오.

1. 관리자의 클라이언트 시스템에서 브라우저를 사용하여 방화벽 IP 주소로 이동합니다.
2. 방화벽 CLI에 관리자로 로그인합니다. 사용자 이름을 입력하면 다음 출력이 표시됩니다(키 값은 예시임).

```
공개 키로 인증 "dsa-key-20130415"
```

3. 메시지가 표시되면 키를 생성할 때 정의한 암호를 입력합니다.

 ©2023 Palo Alto Networks, Inc.

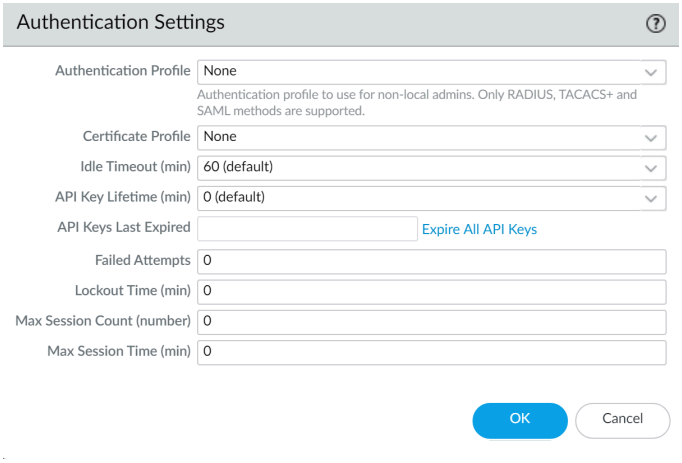
## API 키 수명 구성

방화벽 및 Panorama의 API 키를 사용하면 XML API 및 REST API에 대한 API 호출을 인증할 수 있습니다. 이러한 키는 보안 태세의 중요한 요소인 방화벽 및 Panorama에 대한 액세스 권한을 부여하므로 모범 사례로 API 키 수명을 지정하여 정기적인 키 교체를 시행하십시오. 키 수명을 지정한 후 API 키를 다시 생성할 때 각 키는 고유합니다.

새 키를 주기적으로 재생성하라는 메시지를 표시하는 키 수명을 설정하는 것 외에도 하나 이상의 키가 손상된 경우 현재 유효한 모든 API 키를 취소할 수도 있습니다. 키 취소는 현재 유효한 모든 키를 만료시키는 방법입니다.

**STEP 1 |** 디바이스 > 설정 > 관리를 선택합니다.

**STEP 2 |** 인증 설정을 편집하여 **API** 키 수명**(**분**)**을 지정합니다.



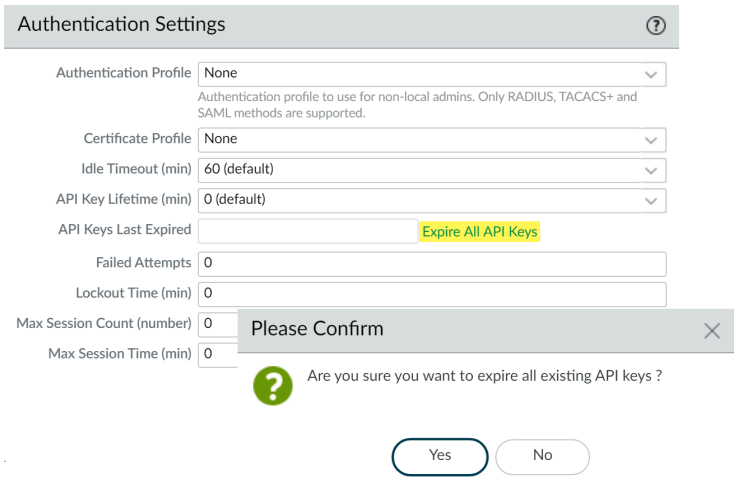

API 키 수명을 설정하여 손상을 방지하고 우발적인 노출의 영향을 줄이십시오. 기본적으로 API 키 수명은 0으로 설정되며 이는 키가 만료되지 않음을 의미합니다. 키가 자주 교체되고 다시 생성될 때 각 키가 고유하도록 하려면 1-525600분 범위의 유효 기간을 지정해야 합니다. API 키가 유효한 수명을 지정하는 방법을 결정하려면 기업의 감사 및 규정 준수 정책을 참조하십시오.

**STEP 3 |** 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (모든 API 키를 취소할 경우) 현재 유효한 API 키를 재설정하려면 모든 **API** 키 만료를 선택합니다.

키 수명을 방금 설정했고 새 용어를 준수하도록 모든 API 키를 재설정하려는 경우 기존 키를 모두 만료할 수 있습니다.




확인 시 키가 취소되고 **API** 키가 마지막으로 만료된 시간에 대한 타임스탬프를 볼 수 있습니다.

## 관리자 활동 추적 구성

방화벽 웹 인터페이스 및 CLI에서 관리자 활동을 추적하여 방화벽 전반의 활동을 실시간으로 보고합니다. 관리자 계정이 손상되었다고 믿을 만한 이유가 있는 경우 이 관리자 계정이 웹 인터페이스 전체에서 탐색한 위치 또는 실행한 운영 명령에 대한 전체 기록이 있으므로 세부적으로 분석하고 관리자가 취한 모든 불완전한 조치에 대응할 수 있습니다.

이벤트가 발생하면 관리자가 웹 인터페이스를 탐색하거나 CLI에서 운영 명령이 실행될 때마다 감사 로그가 생성되어 지정된 syslog 서버로 포워딩됩니다. 실행된 각 탐색 또는 추천에 대해 감사 로그가 생성됩니다. 예를 들어 새 주소 개체를 생성하려는 경우를 생각해 보십시오. 개체를 클릭하면 감사 로그가 생성되고 주소를 클릭하면 두 번째 감사 로그가 생성됩니다.

감사 로그는 syslog 서버로 포워딩된 syslog로만 볼 수 있으며 방화벽 웹 인터페이스에서는 볼 수 없습니다. 감사 로그는 syslog 서버로만 포워딩할 수 있고 Cortex Data Lake(CDL)로 포워딩할 수 없으며 방화벽에 로컬로 저장되지 않습니다.

**STEP 1 |** 방화벽에서 관리자 활동에 대한 감사 로그를 전달하도록 syslog 서버 프로파일을 구성합니다.

이 단계는 방화벽에서 관리자 활동을 추적하기 위한 감사 로그를 성공적으로 저장하는 데 필요합니다.

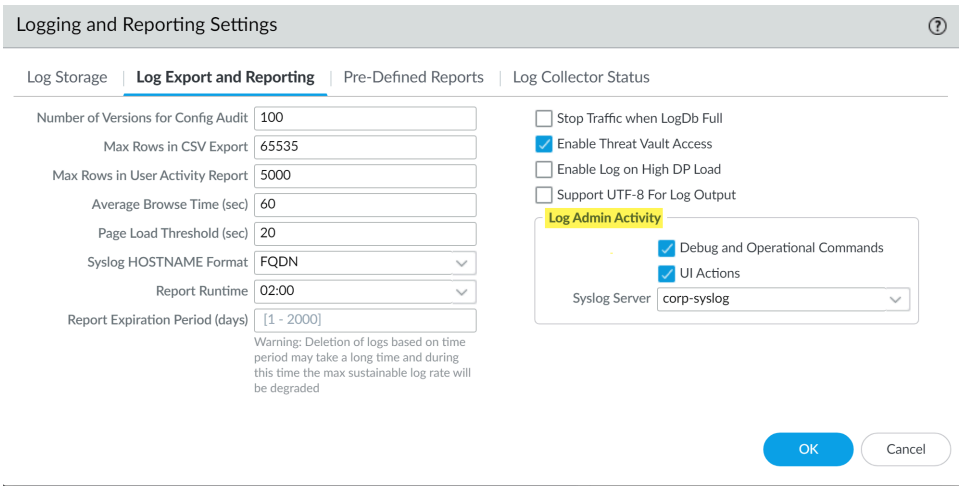
1. 방화벽 웹 인터페이스에 로그인합니다.
2. syslog 서버 프로파일을 구성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 관리자 활동 추적을 구성합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.
2. 로그 내보내기 및 보고를 선택합니다.
3. 관리자 활동 기록 섹션에서 추적할 관리자 활동을 구성합니다.
   - 작동 명령 - 관리자가 CLI에서 작동 또는 디버그 명령을 실행하거나 웹 인터페이스에서 트리거된 작동 명령을 실행할 때 감사 로그를 생성합니다. PAN-OS 작동 및 디버그 명령의 전체 목록은 CLI 작동 명령 레이어를 참조하십시오.
   - **UI** 작업 - 관리자가 웹 인터페이스 전체를 탐색할 때 감사 로그를 생성합니다. 여기에는 구성 탭 간 탐색과 탭 내의 개별 개체가 포함됩니다.

     예를 들어, 관리자가 **ACC**에서 정책 탭으로 이동할 때 감사 로그가 생성됩니다. 또한 관리자가 **Objects** > **Addresses**에서 **Objects** > **Tags**로 이동할 때 감사 로그가 생성됩니다.
   - **Syslog** 서버 - 감사 로그를 포워딩할 대상 syslog 서버 프로파일을 선택합니다.
4. 확인을 클릭합니다.
5. 커밋을 선택합니다.




 ©2023 Palo Alto Networks, Inc.

# 참조: 웹 인터페이스 관리자 액세스

전체 방화벽 또는 하나 이상의 가상 시스템(여러 가상 시스템을 지원하는 플랫폼에서)에 대한 권한을 구성할 수 있습니다. 해당 디바이스 또는 가상 시스템 지정 내에서 동적 관리자 역할과 연결된 고정된 권한보다 더 세분화된 사용자 지정 관리자 역할에 대한 권한을 구성할 수 있습니다.

세분화된 수준에서 권한을 구성하면 하위 수준 관리자가 특정 정보에 액세스할 수 없습니다. 방화벽 관리자에 대한 사용자 지정 역할(방화벽 관리자 계정 구성 참조), Panorama 관리자 또는 디바이스 그룹 및 템플릿 관리자(Panorama 관리자 가이드 참조)를 만들 수 있습니다. 하나 이상의 가상 시스템을 할당할 수 있는 사용자 지정 역할 기반 관리자 계정에 관리자 역할을 적용합니다. 다음 항목에서는 사용자 지정 관리자 역할에 대해 구성할 수 있는 권한을 설명합니다.

- 웹 인터페이스 액세스 권한
- Panorama 웹 인터페이스 액세스 권한

## 웹 인터페이스 액세스 권한

역할 기반 관리자가 웹 인터페이스의 특정 탭에 액세스하지 못하도록 하려면 해당 탭을 비활성화하면 연결된 역할 기반 관리 계정을 사용하여 로그인할 때 관리자가 해당 탭을 볼 수 없습니다. 예를 들어, 디바이스 및 네트워크 탭에 대한 액세스만 제공하는 운영 직원을 위한 관리자 역할 프로파일과 개체, 정책 및 모니터 탭에 대한 액세스를 제공하는 보안 관리자를 위한 별도의 프로파일을 만들 수 있습니다.

관리자 역할은 디바이스 또는 가상 시스템 라디오 버튼으로 정의된 디바이스 수준 또는 가상 시스템 수준에서 적용할 수 있습니다. 가상 시스템을 선택하면 이 프로파일에 할당된 관리자는 할당된 가상 시스템으로 제한됩니다. 또한 해당 관리자는 **Device** > **Setup** > **Services** > **Virtual Systems** 탭만 사용할 수 있으며 전역 탭은 사용할 수 없습니다.

다음 주제는 웹 인터페이스의 다른 부분에 관리자 역할 권한을 설정하는 방법을 설명합니다.

- 웹 인터페이스 탭에 대한 액세스 정의
- 모니터 탭에 대한 세분화된 액세스 제공
- 정책 탭에 대한 세분화된 액세스 제공
- 개체 탭에 대한 세분화된 액세스 제공
- 네트워크 탭에 대한 세분화된 액세스 제공
- 디바이스 탭에 대한 세분화된 액세스 제공
- 관리자 역할 프로파일에서 사용자 개인 정보 설정 정의
- 관리자 액세스 제한 커밋 및 유효성 검사 기능
- 전역 설정에 대한 세분화된 액세스 제공
- Panorama 탭에 대한 세분화된 액세스 제공
- 운영 설정에 대한 세분화된 액세스 제공


©2023 Palo Alto Networks, Inc.

## 웹 인터페이스 탭에 대한 액세스 정의

다음 표에서는 관리자 역할 프로파일(디바이스 > 관리자 역할)에 할당할 수 있는 최상위 액세스 권한에 대해 설명합니다. 웹 인터페이스의 최상위 탭에서 읽기 전용 액세스 권한을 사용하도록 설정, 비활성화 또는 정의할 수 있습니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 대시보드 | 대시보드 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자가 탭을 표시하지 않으며 대시보드 위젯에 액세스할 수 없습니다. | 예 | 아니요 | 예 |
| ACC | 애플리케이션 명령 센터(ACC)에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 **ACC** 탭이 웹 인터페이스에 표시되지 않습니다. ACC에 대한 액세스를 제공하면서 사용자의 개인 정보를 보호하려는 경우 개인 정보 > 보호 쇼 전체 **IP**주소 옵션 및/또는 로그 및 보고서 표시 옵션에서 사용자 이름 표시 옵션을 비활성화할 수 있습니다. | 예 | 아니요 | 예 |
| 모니터 | 모니터 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 모니터 탭을 볼 수 없으며 로그, 패킷 캡처, 세션 정보, 보고서 또는 앱 범위에 액세스할 수 없습니다. 관리자가 볼 수 있는 모니터링 정보를 보다 세부적으로 제어하려면 모니터 옵션을 활성화된 상태로 두고 모니터 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | 예 | 아니요 | 예 |
| 정책 | 정책 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 정책 탭을 볼 수 없으며 정책 정보에 액세스할 수 없습니다. 예를 들어 특정 유형의 정책에 대한 액세스를 활성화하거나 정책 정보에 대한 읽기 전용 액세스를 활성화하기 위해 관리자가 볼 수 있는 정책 정보를 보다 세부적으로 제어하려면 정책 옵션을 활성화한 상태로 두고 활성화하거나 정책 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 비활성화합니다. | 예 | 아니요 | 예 |
| 개체 | 개체 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 개체 탭을 볼 수 없으며 개체, 보안 프로파일, 로그 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 포워딩 프로파일, 복호화 프로파일 또는 일정에 액세스할 수 없습니다. 관리자가 볼 수 있는 개체를 보다 세부적으로 제어하려면 개체 옵션을 활성화한 상태로 두고 개체 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | | | |
| 네트워크 | 네트워크 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 탭을 볼 수 없으며 인터페이스, 영역, VLAN, 가상 와이어, 가상 라우터, IPsec 터널, DHCP, DNS 프록시, GlobalProtect 또는 QoS 구성 정보 또는 네트워크 프로파일에 액세스할 수 없습니다. 관리자가 볼 수 있는 개체를 보다 세부적으로 제어하려면 네트워크 옵션을 활성화된 상태로 두고 네트워크 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | 예 | 아니요 | 예 |
| 디바이스 | 디바이스 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 디바이스 탭을 볼 수 없으며 사용자 ID, 고가용성, 서버 프로파일 또는 인증서 구성 정보와 같은 방화벽 전체 구성 정보에 액세스할 수 없습니다. 관리자가 볼 수 있는 개체를 보다 세분화하여 제어하려면 개체 옵션을 사용하도록 설정한 다음 디바이스 탭에 대한 세부 액세스 제공에 설명된 대로 탭의 특정 노드를 활성화하거나 비활성화합니다.<br><br>디바이스 탭에 대한 전체 액세스를 사용하도록 설정하더라도 역할 기반 관리자에 대한 관리자 역할 또는 관리자 노드에 대한 액세스를 활성화할 수 없습니다. | 예 | 아니요 | 예 |

## 모니터 탭에 대한 세분화된 액세스 제공

경우에 따라 관리자가 모니터 탭의 모든 영역이 아닌 일부 영역을 볼 수 있도록 할 수 있습니다. 예를 들어 중요한 사용자 데이터가 포함되어 있지 않기 때문에 작업 관리자를 구성 및 시스템 로그로만 제한할 수 있습니다. 관리자 역할 정의의 이 섹션은 관리자가 볼 수 있는 모니터 탭의 영역을 지정하지만 로그 및 보고서에서 사용자명을 볼 수 있는 기능을 비활성화하는 것과 같이 이 섹션의 권한을 개인 정보 보호 권한과


©2023 Palo Alto Networks, Inc.

결합할 수도 있습니다. 그러나 한 가지 명심해야 할 점은 역할에서 해당 기능을 비활성화하더라도 시스템 생성 보고서에는 여전히 사용자명과 IP 주소가 표시된다는 것입니다. 이러한 이유로 관리자가 개인 사용자 정보를 볼 수 없도록 하려면 다음 표에 설명된 대로 특정 보고서에 대한 액세스를 비활성화하십시오.

다음 표에는 사용 가능한 모니터 탭 액세스 수준과 관리자 역할이 나열되어 있습니다.

디바이스 그룹 및 템플릿 역할은 해당 역할에 할당된 액세스 도메인 내에 있는 디바이스 그룹에 대한 로그 데이터만 볼 수 있습니다.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| 모니터 | 모니터 탭에 대한 액세스를 활성화하거나 비활성화합니다. 비활성화된 경우 관리자는 이 탭이나 연결된 로그 또는 보고서를 볼 수 없습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 로그 | 모든 로그 파일에 대한 액세스를 활성화하거나 비활성화합니다. 이 권한을 활성화된 상태로 두고 관리자에게 표시되지 않도록 하려는 특정 로그를 비활성화할 수도 있습니다. 하나 이상의 로그에 대한 액세스를 계속 제공하면서 사용자의 개인 정보를 보호하려면 **Privacy** > **Show Full IP Addresses** 옵션 및/또는 **Show User Names In Logs And Reports** 옵션을 비활성화할 수 있습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 트래픽 | 관리자가 트래픽 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 위협 | 관리자가 위협 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| URL 필터링 | 관리자가 URL 필터링 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | | 디바이스 그룹/템플릿: 예 | | | |
| WildFire Submissions | 관리자가 WildFire 로그를 볼 수 있는지의 여부를 지정합니다. 이러한 로그는 WildFire 구독이 있는 경우에만 사용할 수 있습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 데이터 필터링 | 관리자가 데이터 필터링 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| HIP 매치 | 관리자가 HIP 일치 로그를 볼 수 있는지의 여부를 지정합니다. HIP Match 로그는 GlobalProtect 라이선스(가입)가 있는 경우에만 사용할 수 있습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| GlobalProtect | 관리자가 GlobalProtect 로그를 볼 수 있는지의 여부를 지정합니다. 이러한 로그는 GlobalProtect 라이선스(가입)가 있는 경우에만 사용할 수 있습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| User-ID | 관리자가 사용자 ID 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| GTP | 모바일 네트워크 운영자가 GTP 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 터널 검사 | 관리자가 터널 검사 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| SCTP | 모바일 네트워크 운영자가 SCTP(Stream Control Transmission Protocol) 로그를 볼 수 있는지의 여부를 지정합니다.<br><br>***SCTP*** 로그, 사용자 정의 보고서 또는 ***Panorama*** 및 디바이스 그룹/템플릿에 대한 사전 정의된 보고서에 대한 관리자 액세스를 제어하려면 먼저 ***Panorama***(디바이스 > 설정 > 관리)에서 ***SCTP***를 활성화해야 합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 구성 | 관리자가 구성 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |
| 체계 | 관리자가 시스템 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |
| 알람 | 관리자가 시스템 생성 알람을 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 인증 | 관리자가 인증 로그를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| 자동화된 연동 엔진 | 방화벽에서 생성된 상관 관계 개체 및 상호 연관된 이벤트 로그에 대한 액세스를 활성화하거나 비활성화합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 상관 개체 | 관리자가 상관 개체를 보고 활성화/비활성화할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 상관 이벤트 | 관리자가 상관 이벤트를 보고 활성화/비활성화할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 패킷 캡처 | 관리자가 모니터 탭에서 패킷 캡처(pcaps)를 볼 수 있는지의 여부를 지정합니다. 패킷 캡처는 원시 흐름 데이터이므로 사용자 IP 주소가 포함될 수 있습니다. 전체 **IP** 주소 표시 권한을 비활성화해도 pcap의 IP 주소가 난독화되지 않으므로 사용자 개인 정보가 우려되는 경우 패킷 캡처 권한을 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 아니요<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 앱 범위 | 관리자가 앱 범위 가시성 및 분석 도구를 볼 수 있는지의 여부를 지정합니다. 앱 범위를 활성화하면 모든 앱 범위 차트에 액세스할 수 있습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 세션 브라우저 | 관리자가 방화벽에서 현재 실행 중인 세션을 찾아보고 필터링할 수 있는지의 여부를 지정합니다. 세션 브라우저는 원시 플로우 데이터를 표시하므로 사용자 IP 주소가 포함될 수 있습니다. 전체 **IP** 주소 표시 권한을 비활성화해도 세션 브라우저에서 IP 주소가 난독화되지 않으므로 사용자 개인 정보가 우려되는 경 | 방화벽: 예<br>Panorama: 아니요<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 우 세션 브라우저 권한을 비활성화해야 합니다. | | | | |
| 차단 IP 목록 | 관리자가 차단 목록을 보고(활성화 또는 읽기 전용) 목록에서 항목을 삭제할 수 있는지(활성화)를 지정합니다. 설정을 비활성화하면 관리자가 차단 목록에서 항목을 보거나 삭제할 수 없습니다. | 방화벽: 예<br>Panorama: 문맥 전환 UI 아래: 예<br>템플릿: 예 | 예 | 예 | 예 |
| 봇넷 | 관리자가 봇넷 분석 보고서를 생성 및 볼 수 있는지 또는 읽기 전용 모드에서 봇넷 보고서를 볼 수 있는지의 여부를 지정합니다. 전체 **IP** 주소 표시 권한을 비활성화해도 예약된 봇넷 보고서에서 IP 주소가 난독화되지 않으므로 사용자 개인 정보가 우려되는 경우 봇넷 권한을 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 아니요<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| PDF 보고서 | 모든 PDF 보고서에 대한 액세스를 활성화하거나 비활성화합니다. 이 권한을 활성화된 상태로 두고 관리자에게 표시되지 않도록 하려는 특정 PDF 보고서를 비활성화할 수도 있습니다. 하나 이상의 보고서에 대한 액세스를 계속 제공하면서 사용자의 개인 정보를 보호하려면 **Privacy** > **Show Full IP Addresses** 옵션 및/또는 **Show User Names In Logs And Reports** 옵션을 비활성화할 수 있습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| PDF 요약 관리 | 관리자가 PDF 요약 보고서 정의를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. 읽기 전용 액세스 권한이 있는 관리자는 PDF 요약 보고서 정의를 볼 수 있지만 추가하거나 삭제할 수는 없습니다. 이 옵션을 비활성화하면 관리자는 보고서 정의를 보거나 추가/삭제할 수 없습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| PDF 요약 보고서 | 관리자가 모니터 > 보고서에서 생성된 PDF 요약 보고서를 볼 수 있는지의 여부를 지정합니다. 이 옵션을 비활성화하면 **PDF** 요약 보고서 카테고리가 보고서 노드에 표시되지 않습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 사용자 활동 보고서 | 관리자가 사용자 활동 보고서 정의를 보거나 추가 또는 삭제할 수 있고 보고서를 다운로드할 수 있는지의 여부를 지정합니다. 읽기 전용 액세스 권한이 있는 관리자는 사용자 활동 보고서 정의를 볼 수 있지만 추가, 삭제 또는 다운로드할 수는 없습니다. 이 옵션을 비활성화하면 관리자는 이 카테고리의 PDF 보고서를 볼 수 없습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |
| SaaS 애플리케이션 사용 보고서 | 관리자가 SaaS 애플리케이션 사용 보고서를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. 관리자는 읽기 전용 액세스 권한으로 SaaS 애플리케이션 사용 보고서 정의를 볼 수 있지만 추가하거나 삭제할 수는 없습니다. 이 옵션을 비활성화하면 관리자는 보고서 정의를 보거나 추가 또는 삭제할 수 없습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |
| 보고서 그룹 | 관리자가 보고서 그룹 정의를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. 읽기 전용 액세스 권한이 있는 관리자는 보고서 그룹 정의를 볼 수 있지만 추가하거나 삭제할 수는 없습니다. 이 옵션을 비활성화하면 관리자는 이 카테고리의 PDF 보고서를 볼 수 없습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |
| 이메일 스케줄러 | 관리자가 이메일에 대한 보고서 그룹을 예약할 수 있는지의 여부를 지정합니다. 이메일로 전송되는 생성된 보고서에는 **Privacy** > **Show** | 방화벽: 예<br>Panorama: 예 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | **Full IP Addresses** 옵션 및/또는 **Show User Names In Logs And Reports** 옵션을 비활성화해도 제거되지 않는 민감한 사용자 데이터가 포함될 수 있으며 관리자가 표시하지 않는 로그 데이터도 표시할 수 있기 때문입니다. 액세스 권한이 있는 경우 사용자 개인 정보 요구 사항이 있는 경우 이메일 스케줄러 옵션을 비활성화해야 합니다. | 디바이스 그룹/템플릿: 예 | | | |
| 맞춤 보고서 관리 | 모든 사용자 정의 보고서 기능에 대한 액세스를 활성화하거나 비활성화합니다. 이 권한을 활성화된 상태로 두고 관리자가 액세스할 수 없도록 하려는 특정 사용자 정의 보고서 카테고리를 비활성화할 수도 있습니다. 하나 이상의 보고서에 대한 액세스를 계속 제공하면서 사용자의 개인 정보를 보호하려면 **Privacy** > **Show Full IP Addresses** 옵션 및/또는 **Show User Names In Logs And Reports** 옵션을 비활성화할 수 있습니다.<br><br>요청 시 실행이 아닌 실행이 예약된 보고서에는 *IP* 주소와 사용자 정보가 표시됩니다. 이 경우 해당 보고 영역에 대한 접근을 제한해야 합니다. 또한 맞춤 리포트 기능은 관리자 역할에서 제외된 로그에 포함된 로그 데이터가 포함된 보고서를 생성하는 기능을 제한하지 않습니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 애플리케이션 통계 | 관리자가 애플리케이션 통계 데이터베이스의 데이터를 포함하는 사 | 방화벽: 예<br>Panorama: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 용자 정의 보고서를 작성할 수 있는지의 여부를 지정합니다. | 디바이스 그룹/템플릿: 예 | | | |
| 데이터 필터링 로그 | 관리자가 데이터 필터링 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 위협 로그 | 관리자가 위협 로그의 데이터를 포함하는 맞춤 리포트를 생성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 위협 요약 | 관리자가 위협 요약 데이터베이스의 데이터를 포함하는 맞춤 리포트를 생성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 트래픽 로그 | 관리자가 트래픽 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 트래픽 요약 | 관리자가 트래픽 요약 데이터베이스의 데이터를 포함하는 사용자 정의 보고서를 작성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| URL 로그 | 관리자가 URL 필터링 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| URL 요약 | 관리자가 URL 요약 데이터베이스의 데이터를 포함하는 사용자 지정 보고서를 만들 수 있는지 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| HIP 매치 | 관리자가 HIP 일치 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| GlobalProtect | 관리자가 GlobalProtect 로그의 데이터를 포함하는 사용자 정의 보고서를 작성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| WildFire Log | 관리자가 WildFire 로그의 데이터를 포함하는 사용자 정의 보고서를 생성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| GTP 로그 | 모바일 네트워크 운영자가 GTP 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| GTP 요약 | 모바일 네트워크 운영자가 GTP 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 터널 로그 | 관리자가 터널 검사 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 터널 요약 | 관리자가 터널 요약 데이터베이스의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| SCTP 로그 | 모바일 네트워크 운영자가 SCTP 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| SCTP 요약 | 모바일 네트워크 운영자가 SCTP 요약 데이터베이스의 데이터를 포함하는 사용자 정의 보고서를 작성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| User-ID | 관리자가 사용자 ID 로그의 데이터를 포함하는 사용자 정의 보고서를 작성할 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 인증 | 관리자가 인증 로그의 데이터를 포함하는 맞춤 리포트를 만들 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 예약된 맞춤 보고서 보기 | 관리자가 생성하도록 예약된 사용자 정의 보고서를 볼 수 있는지의 여부를 지정합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 사전 정의된 애플리케이션 보고서 보기 | 관리자가 애플리케이션 보고서를 볼 수 있는지의 여부를 지정합니다. 개인 정보 보호 권한은 **Monitor** > **Reports** 노드에서 사용 가능한 보고서에 영향을 미치지 않으므로 사용자 개인 정보 요구 사항이 있는 경우 보고서에 대한 액세스를 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 사전 정의된 위협 보고서 보기 | 관리자가 위협 보고서를 볼 수 있는지의 여부를 지정합니다. 개인 정보 보호 권한은 **Monitor** > **Reports** 노드에서 사용 가능한 보고서에 영향을 미치지 않으므로 사용자 개인 | 방화벽: 예<br>Panorama: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 정보 요구 사항이 있는 경우 보고서에 대한 액세스를 비활성화해야 합니다. | 디바이스 그룹/템플릿: 예 | | | |
| 사전 정의된 URL 필터링 보고서 보기 | 관리자가 URL 필터링 보고서를 볼 수 있는지의 여부를 지정합니다. 개인 정보 보호 권한은 **Monitor** > **Reports** 노드에서 사용 가능한 보고서에 영향을 미치지 않으므로 사용자 개인 정보 요구 사항이 있는 경우 보고서에 대한 액세스를 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 사전 정의된 트래픽 보고서 보기 | 관리자가 트래픽 보고서를 볼 수 있는지의 여부를 지정합니다. 개인 정보 보호 권한은 **Monitor** > **Reports** 노드에서 사용 가능한 보고서에 영향을 미치지 않으므로 사용자 개인 정보 요구 사항이 있는 경우 보고서에 대한 액세스를 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 사전 정의된 GTP 보고서 보기 | 모바일 네트워크 운영자가 GTP 보고서를 볼 수 있는지의 여부를 지정합니다. 개인 정보 보호 권한은 보고서 > 모니터링 노드에서 사용 가능한 보고서에 영향을 미치지 않으므로 사용자 개인 정보 요구 사항이 있는 경우 보고서에 대한 액세스를 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |
| 사전 정의된 SCTP 보고서 보기 | 모바일 네트워크 운영자가 SCTP 보고서를 볼 수 있는지의 여부를 지정합니다. 개인 정보 보호 권한은 **Monitor** > **Reports** 노드에서 사용 가능한 보고서에 영향을 미치지 않으므로 사용자 개인 정보 요구 사항이 있는 경우 보고서에 대한 액세스를 비활성화해야 합니다. | 방화벽: 예<br>Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |

## 정책 탭에 대한 세분화된 액세스 제공

관리자 역할 프로파일에서 정책 옵션을 사용하도록 설정한 경우 정의하려는 역할에 필요한 경우 탭 내의 특정 노드에 대해 읽기 전용 액세스를 사용하거나 사용하지 않도록 설정하거나 읽기 전용 액세스를 제공


©2023 Palo Alto Networks, Inc.

할 수 있습니다. 특정 정책 유형에 대한 액세스를 활성화하면 정책 규칙을 보거나, 추가하거나, 삭제할 수 있습니다. 특정 정책에 대한 읽기 전용 액세스를 활성화하면 관리자가 해당 정책 규칙 기준을 볼 수 있지만 규칙을 추가하거나 삭제할 수는 없습니다. 특정 유형의 정책에 대한 액세스를 사용하지 않도록 설정하면 관리자가 정책 규칙 기반을 볼 수 없습니다.

특정 사용자(사용자명 또는 IP 주소 기준)를 기반으로 하는 정책을 명시적으로 정의해야 하므로 전체 IP 주소 또는 사용자명을 볼 수 없도록 설정하는 개인 정보 보호 설정은 정책 탭에 적용되지 않습니다. 따라서 사용자 개인 정보 제한에서 제외된 관리자에게만 정책 탭에 대한 액세스를 허용해야 합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 보안 | 관리자가 보안 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자가 보안 규칙 기준을 볼 수 없도록 하려면 이 권한을 비활성화하십시오. | 예 | 예 | 예 |
| NAT | 관리자가 NAT 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자가 NAT 규칙베이스를 볼 수 없도록 하려면 이 권한을 비활성화합니다. | 예 | 예 | 예 |
| QoS | 관리자가 QoS 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자가 QoS 규칙베이스를 볼 수 없도록 하려면 이 권한을 사용하지 않도록 설정합니다. | 예 | 예 | 예 |
| 정책 기반 포워딩 | 관리자가 PBF(정책 기반 포워딩) 규칙을 보거나 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자에게 PBF 규칙 기반이 표시되지 않도록 하려면 이 권한을 비활성화합니다. | 예 | 예 | 예 |
| 복호화 | 관리자가 복호화 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자에게 복호화 규칙 기반이 표 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 시되지 않도록 하려면 이 권한을 사용하지 않도록 설정합니다. | | | |
| 네트워크 패킷 브로커 | 관리자가 네트워크 패킷 브로커 정책 규칙을 보거나 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 사용하도록 설정합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자가 인터페이스에서 네트워크 패킷 브로커 룰베이스(rulebase)를 볼 수 없도록 하려면 이 권한을 사용하지 않도록 설정합니다. | 예 | 예 | 예 |
| 터널 검사 | 관리자가 터널 검사 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자에게 터널 검사 규칙 기반이 표시되지 않도록 하려면 이 권한을 사용하지 않도록 설정합니다. | 예 | 예 | 예 |
| 애플리케이션 재정의 | 관리자가 애플리케이션 우선 적용 정책 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자가 애플리케이션 재정의 룰베이스(rulebase)를 볼 수 없도록 하려면 이 권한을 비활성화합니다. | 예 | 예 | 예 |
| 인증 | 관리자가 인증 정책 규칙을 확인, 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자에게 인증 규칙 기반이 표시되지 않도록 하려면 이 권한을 비활성화하십시오. | 예 | 예 | 예 |
| DoS 보호 | 관리자가 DoS 방어 규칙을 확인, 추가 및/또는 삭제할 수 있도록 허용하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자가 DoS 방어 규칙 기준을 보지 못하게 하려면 이 권한을 비활성화하십시오. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| SD-WAN | 관리자가 SD-WAN 정책 규칙을 보거나 추가 및/또는 삭제할 수 있도록 하려면 이 권한을 활성화합니다. 관리자가 규칙을 볼 수 있지만 수정할 수는 없도록 하려면 권한을 읽기 전용으로 설정합니다. 관리자에게 SD-WAN 정책 규칙 기반이 표시되지 않도록 하려면 이 권한을 사용하지 않도록 설정합니다. | 예 | 예 | 예 |

## 객체 탭에 대한 세분화된 액세스 제공

개체는 간소화된 규칙 정의를 위해 IP 주소, URL, 애플리케이션 또는 서비스와 같은 특정 정책 필터 값을 그룹화하는 컨테이너입니다. 예를 들어 주소 개체에는 DMZ 영역의 웹 및 애플리케이션 서버에 대한 특정 IP 주소 정의가 포함될 수 있습니다.

개체 탭 전체에 대한 액세스를 허용할지의 여부를 결정할 때 관리자에게 정책 정의에 대한 책임이 있는지의 여부를 결정합니다. 그렇지 않은 경우 관리자는 탭에 액세스할 필요가 없습니다. 그러나 관리자가 정책을 생성해야 하는 경우 탭에 대한 액세스를 활성화한 다음 노드 수준에서 세분화된 액세스 권한을 제공할 수 있습니다.

특정 노드에 대한 액세스를 활성화하면 관리자에게 해당 개체 유형을 보고, 추가하고, 삭제할 수 있는 권한을 부여할 수 있습니다. 읽기 전용 액세스 권한을 부여하면 관리자가 이미 정의된 개체를 볼 수 있지만 작성하거나 삭제할 수는 없습니다. 노드를 사용하지 않도록 설정하면 관리자가 웹 인터페이스에서 노드를 볼 수 없습니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 주소 | 관리자가 보안 정책에 사용할 주소 개체를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 주소 그룹 | 관리자가 보안 정책에 사용할 주소 그룹 개체를 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 지역 | 관리자가 보안, 복호화 또는 DoS 정책에 사용할 영역 개체를 확인, 추가 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 애플리케이션 | 관리자가 정책에 사용할 애플리케이션 개체를 확인, 추가 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 애플리케이션 그룹 | 관리자가 정책에 사용할 애플리케이션 그룹 개체를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 애플리케이션 필터 | 관리자가 반복 검색을 단순화하기 위해 애플리케이션 필터를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 서비스 | 관리자가 응용 프로그램에서 사용할 수 있는 포트 번호를 제한하는 정책 규칙을 만드는 데 사용할 서비스 개체를 보거나 추가하거나 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| 서비스 그룹 | 관리자가 보안 정책에 사용할 서비스 그룹 개체를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 태그 | 관리자가 방화벽에 정의된 태그를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| GlobalProtect | 관리자가 HIP 개체 및 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. GlobalProtect 수준에서 두 개체 유형에 대한 액세스를 제한하거나 GlobalProtect 권한을 사용하도록 설정하고 HIP 개체 또는 HIP 프로파일 액세스를 제한하여 보다 세부적으로 제어할 수 있습니다. | 예 | 아니요 | 예 |
| HIP 오브젝트 | 관리자가 HIP 프로파일을 정의하는 데 사용되는 HIP 개체를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. HIP 개체도 HIP 일치 로그를 생성합니다. | 예 | 예 | 예 |
| 클라이언트가 없는 앱 | 관리자가 GlobalProtect VPN 클라이언트 없는 애플리케이션을 보거나, 추가하거나, 수정하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 클라이언트가 없는 앱 그룹 | 관리자가 GlobalProtect VPN 클라이언트 없는 애플리케이션 그룹을 확인, 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| HIP 프로파일 | 관리자가 보안 정책에 사용하거나 HIP 일치 로그를 생성하기 위해 HIP 프로파일을 보거나 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | | | |
| 외부 동적 목록 | 관리자가 보안 정책에 사용할 외부 동적 목록을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 사용자 지정 개체 | 관리자가 사용자 지정 스파이웨어 및 취약성 서명을 볼 수 있는지의 여부를 지정합니다. 이 수준에서 모든 사용자 지정 서명에 대한 액세스를 활성화 또는 비활성화하도록 액세스를 제한하거나 사용자 지정 개체 권한을 활성화한 다음 각 서명 유형에 대한 액세스를 제한하여 보다 세부적인 제어를 제공할 수 있습니다. | 예 | 아니요 | 예 |
| 데이터 패턴 | 관리자가 사용자 지정 취약점 보호 프로파일을 만드는 데 사용할 사용자 지정 데이터 패턴 서명을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 스파이웨어 | 관리자가 사용자 지정 취약점 보호 프로파일을 만드는 데 사용할 사용자 지정 스파이웨어 서명을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 취약성 | 관리자가 사용자 지정 취약점 보호 프로파일을 만드는 데 사용할 사용자 지정 취약점 서명을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| URL 카테고리 | 관리자가 정책에 사용할 사용자 지정 URL 카테고리를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 보안 프로파일 | 관리자가 보안 프로파일을 볼 수 있는지의 여부를 지정합니다. 이 레벨에서 모든 보안 프로파일에 대한 액세스를 활성화 또는 비활성화하도록 액세스를 제한하거나 보안 프로파일 권한을 활성화한 다음 각 프로파일 유형에 대한 액세스를 제한하여 보다 세부적인 제어를 제공할 수 있습니다. | 예 | 아니요 | 예 |
| 안티바이러스 | 관리자가 바이러스 백신 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 안티-스파이웨어 | 관리자가 안티 스파이웨어 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 취약성 보호 | 관리자가 취약점 보호 프로파일을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| URL 필터링 | 관리자가 URL 필터링 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 파일 차단 | 관리자가 파일 차단 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| WildFire Analysis | 관리자가 WildFire 분석 프로파일을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 데이터 필터링 | 관리자가 데이터 필터링 프로파일을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| DoS 보호 | 관리자가 DoS 방어 프로파일을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| GTP 프로텍션 | 모바일 네트워크 운영자가 GTP 보호 프로파일을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| SCTP 보호 | 모바일 네트워크 운영자가 SCTP(스트림 제어 전송 프로토콜) 보호 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 보안 프로파일 그룹 | 관리자가 보안 프로파일 그룹을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 로그 포워딩 | 관리자가 로그 포워딩 프로파일을 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 인증 | 관리자가 인증 적용 개체를 보거나, 추가하거나, 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 복호화 프로파일 | 관리자가 복호화 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| SD-WAN 링크 관리 | 관리자가 경로 품질, SaaS 품질, 트래픽 분산 및 오류 수정 프로파일을 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 아니요 | 예 |
| 경로 품질 프로파일 | 관리자가 SD-WAN 경로 품질 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| SaaS 품질 프로파일 | 관리자가 SD-WAN SaaS 품질 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 트래픽 배포 프로파일 | 관리자가 SD-WAN 트래픽 배포 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 오류 수정 프로파일 | 관리자가 SD-WAN 오류 수정 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 패킷 브로커 프로파일 | 관리자가 패킷 브로커 프로파일을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 스케줄 | 관리자가 보안 정책을 특정 날짜 및/또는 시간 범위로 제한하기 위한 일정을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |

## 네트워크 탭에 대한 세분화된 액세스 제공

전체적으로 네트워크 탭에 대한 액세스를 허용할지의 여부를 결정할 때 관리자가 GlobalProtect 관리를 포함한 네트워크 관리 책임을 맡을지 여부를 결정합니다. 그렇지 않은 경우 관리자는 탭에 액세스할 필요가 없습니다.

노드 수준에서 네트워크 탭에 대한 액세스를 정의할 수도 있습니다. 특정 노드에 대한 액세스를 사용하도록 설정하면 관리자에게 해당 네트워크 구성을 보고 추가 및 삭제할 수 있는 권한을 부여합니다. 읽기 전용 액세스를 제공하면 관리자는 이미 정의된 구성을 볼 수 있지만 만들거나 삭제할 수는 없습니다. 노드를 사용하지 않도록 설정하면 관리자가 웹 인터페이스에서 노드를 볼 수 없습니다.


©2023 Palo Alto Networks, Inc.

여러 라우팅 액세스 수준이 표시되며 기기에 대해 고급 라우팅이 활성화된 경우에만 적용됩니다. 이 경우 논리적 라우터가 가상 라우터를 대체합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 인터페이스 | 관리자가 인터페이스 구성을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 영역 | 관리자가 영역을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| VLAN | 관리자가 VLAN을 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 가상 와이어 | 관리자가 가상 와이어를 보거나 추가하거나 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 가상 라우터 | 관리자가 가상 라우터를 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 라우팅 | (고급 라우팅 엔진) 관리자가 고급 라우팅 엔진의 라우팅 필드를 보거나, 추가, 수정 또는 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| 논리적 라우터 | (고급 라우팅 엔진) 관리자가 논리적 라우터를 보거나, 추가하거나, 수정하거나, 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| 라우팅 프로파일 | (고급 라우팅 엔진) 관리자가 라우팅 프로파일을 보거나, 추가하거나, 수정하거나, 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| BGP | (고급 라우팅 엔진) 관리자가 논리적 라우터를 보거나, 추가하거나, 수정하거나, 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| BFD | (고급 라우팅 엔진) 관리자가 논리적 라우터를 보거나, 추가하거나, 수정하거나, 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| OSPF | (고급 라우팅 엔진) 관리자가 OSPFv2 라우팅 프로필을 보고, 추가, 수정 또는 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| OSPFv3 | (고급 라우팅 엔진) 관리자가 OSPFv3 라우팅 프로필을 보고, 추가, 수정 또는 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| RIPv2 | (고급 라우팅 엔진) 관리자가 RIPv2 라우팅 프로필을 보고, 추가, 수정 또는 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| 필터 | (고급 라우팅 엔진) 관리자가 필터를 보고, 추가, 수정 또는 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| 멀티캐스트 | (고급 라우팅 엔진) 관리자가 IPv4 멀티캐스트 라우팅 프로필을 확인, 추가, 수정 또는 삭제할 수 있는지 여부를 지정합니다. | 예 | 예 | 예 |
| IPSec 터널 | 관리자가 IPSec 터널 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| GRE 터널 | 관리자가 GRE 터널 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| DHCP | 관리자가 DHCP 서버 및 DHCP 릴레이 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| DNS 프록시 | 관리자가 DNS 프록시 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| GlobalProtect | 관리자가 GlobalProtect 포털 및 게이트웨이 구성을 보고, 추가, 수정할 수 있는지의 여부를 지정합니다. GlobalProtect 기능에 대한 액세스를 완전히 비활성화하거나 GlobalProtect 권한을 사용하도록 설정한 다음 역할을 포털 또는 게이트웨이 구성 영역으로 제한할 수 있습니다. | 예 | 아니요 | 예 |
| 포털 | 관리자가 GlobalProtect 포털 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 게이트웨이 | 관리자가 GlobalProtect 게이트웨이 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| MDM | 관리자가 GlobalProtect MDM 서버 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 디바이스 차단 목록 | 관리자가 디바이스 차단 목록을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 클라이언트가 없는 앱 | 관리자가 GlobalProtect 클라이언트가 없는 VPN 애플리케이션을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 클라이언트가 없는 앱 그룹 | 관리자가 GlobalProtect 클라이언트가 없는 VPN 애플리케이션 그룹을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| QoS | 관리자가 QoS 구성을 보거나 추가, 수정 또는 삭제할 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| LLDP | 관리자가 LLDP 구성추가, 수정 또는 삭제를 볼 수 있는지의 여부를 지정합니다. | 예 | 예 | 예 |
| 네트워크 프로파일 | 아래 설명된 모든 네트워크 설정을 활성화하거나 비활성화하도록 기본 상태를 설정합니다. | 예 | 아니요 | 예 |
| GlobalProtect IPSec 암호화 | 네트워크 프로파일 > **GlobalProtect IPSec Crypto** 노드에 대한 액세스를 제어합니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 GlobalProtect 게이트웨이와 클라이언트 간의 VPN 터널에서 해당 노드를 보거나 인증 및 암호화를 위한 알고리즘을 구성하지 않습니다.<br>읽기 전용으로 권한을 설정한 경우 관리자는 기존 GlobalProtect IPSec 암호화 프로파일을 볼 수 있지만 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |
| IKE 게이트웨이 | 네트워크 프로파일 > **IKE** 게이트웨이 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 **IKE** 게이트웨이 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 노드를 보거나 피어 게이트웨이와 IKE 프로토콜 협상을 수행하는 데 필요한 구성 정보가 포함된 게이트웨이를 정의합니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 IKE 게이트웨이를 볼 수 있지만 게이트웨이를 추가하거나 편집할 수 없습니다. | | | |
| IPSec 암호화 | 네트워크 프로파일 > **IPSec** 암호화 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 네트워크 프로파일 > **IPSec** 암호화 노드를 볼 수 없으며 IPSec SA 협상을 기반으로 하는 VPN 터널에서 식별, 인증 및 암호화를 위한 프로토콜 및 알고리즘을 지정할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 IPSec 암호화 구성을 볼 수 있지만 구성을 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |
| IKE 암호화 | 디바이스가 정보를 교환하여 안전한 통신을 보장하는 방법을 제어합니다. IPsec SA 협상(IKEv1 Phase-1)을 기반으로 VPN 터널에서 식별, 인증 및 암호화를 위한 프로토콜 및 알고리즘을 지정합니다. | 예 | 예 | 예 |
| 모니터 | 네트워크 프로파일 > 모니터노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 프로파일 > 모니터 노드를 보거나 IPSec 터널을 모니터링하고 정책 기반 포워딩(PBF) 규칙에 대한 다음 홉 디바이스를 모니터링하는 데 사용되는 모니터 프로파일을 만들거나 편집할 수 있습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 모니터 프로파일 구성을 볼 수 있지만 구성을 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |
| 인터페이스 Mgmt | 네트워크 프로파일 > 인터페이스**Mgmt** 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 프로파일 > 인터페이스**Mgmt** 노드를 보거나 방화벽을 관리하는 데 사용되는 프로토콜을 지정할 수 있습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 인터페이스 관리 프로파일 구성을 볼 수 있지만 구성을 추가하거나 편집할 수 없습니다. | | | |
| 존 보호 | 네트워크 프로파일 > 영역 보호 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 프로파일 > 영역 보호 노드를 보거나 방화벽이 지정된 보안 영역의 공격에 대응하는 방식을 결정하는 프로파일을 구성할 수 있습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 영역 보호 프로파일 구성을 볼 수 있지만 구성을 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |
| QoS 프로파일 | 네트워크 프로파일 > **QoS** 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 프로파일 > **QoS** 노드를 보거나 QoS 트래픽 클래스가 처리되는 방식을 결정하는 QoS 프로파일을 구성할 수 있습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 QoS 프로파일 구성을 볼 수 있지만 구성을 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |
| LLDP 프로파일 | 네트워크 프로파일 > **LLDP** 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 프로파일 > **LLDP** 노드를 보거나 방화벽의 인터페이스가 링크 레이어 검색 프로토콜에 참여할 수 있는지의 여부를 제어하는 LLDP 프로파일을 구성할 수 있습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 LLDP 프로파일 구성을 볼 수 있지만 구성을 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |
| BFD 프로파일 | 네트워크 프로파일 > **BFD** 프로파일 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 프로파일 > **BFD** 프로파일 노드를 보거나 BFD 프로파일을 구성할 수 없습니다. 양방향 포워딩 감지(BFD) 프로파일을 사용하면 하나 이상의 정적 경로 또는 라우팅 프로토콜에 적용할 BFD 설정을 구성할 수 있습니다. 따라서 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | BFD는 실패한 링크 또는 BFD 피어를 감지하고 빠른 페일오버를 할 수 있습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 BFD 프로파일을 볼 수 있지만 BFD 프로파일을 추가하거나 편집할 수 없습니다. | | | |
| SD-WAN 인터페이스 프로파일 | **SD-WAN** 인터페이스 프로파일 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 **SD-WAN**인터페이스 프로파일 노드가 표시되지 않거나 SD-WAN 인터페이스 프로파일을 구성할 수 없습니다. SD-WAN 인터페이스 프로파일은 ISP 연결의 특성을 정의하고 링크 속도와 방화벽이 링크를 모니터링하는 빈도를 지정합니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 SD-WAN 인터페이스 프로파일을 볼 수 있지만 추가하거나 편집할 수 없습니다. | 예 | 예 | 예 |

## 디바이스 탭에 대한 세분화된 액세스 제공

디바이스 탭에 대한 세분화된 액세스 권한을 정의하려면 관리자 역할 프로파일(**Device** > **Admin** 역할)을 만들거나 편집할 때 **WebUI** 탭에서 디바이스 노드까지 아래로 스크롤합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 설정 | 설정 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 설정 노드를 볼 수 없거나 관리, 작업, 서비스, 콘텐츠 ID, WildFire 또는 세션 설정 정보와 같은 방화벽 전체 설정 구성 정보에 액세스할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |
| 관리 | 관리 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 호스트 이름, 도메인, 시간대, 인증, 로깅 및 보고, Panorama 연결, 배너, 메시지, 암호 복잡성 설정 등과 같은 설정을 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 운영 | 운영 및 원격 측정 및 위협 인텔리전스 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 다음을 수행할 수 없습니다.<br>• 방화벽 구성을 로드합니다.<br>• 방화벽 구성을 저장하거나 되돌립니다.<br>이 권한은 디바이스 > 작업 옵션에만 적용됩니다. 저장 및 커밋 권한은 관리자가 ***Config*** > ***Save*** 및 ***Config*** > ***Revert*** 옵션을 통해 구성을 저장하거나 되돌릴 수 있는지의 여부를 제어합니다.<br>• 사용자 정의 로고를 생성합니다.<br>• 방화벽 설정의 SNMP 모니터링을 구성합니다.<br>• 통계 서비스 기능을 구성합니다.<br>• 원격 분석 및 위협 인텔리전스 설정을 구성합니다.<br>사전 정의된 운용 관리자 역할이 있는 관리자만 방화벽 구성을 내보내거나 가져오고 방화벽을 종료할 수 있습니다.<br>사전 정의된 운용 관리자 또는 디바이스 관리자 역할이 있는 관리자만 방화벽을 재부팅하거나 데이터플레인을 다시 시작할 수 있습니다.<br>특정 가상 시스템에 대한 액세스만 허용하는 역할을 가진 관리자는 **Device** > **Operations** 옵션을 통해 방화벽 구성을 로드, 저장 또는 되돌릴 수 없습니다. | 예 | 예 | 예 |
| 서비스 | 서비스 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 DNS 서버, 업데이트 서버, 프록시 서버 또는 NTP 서버에 대한 서비스를 구성하거나 서비스 경로를 설정할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| Content-ID | **Content-ID** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 URL 필터링 또는 Content-ID를 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |
| WildFire | **WildFire** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 WildFire 설정을 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |
| 세션 | 세션 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 TCP, UDP 또는 ICMP에 대한 세션 설정 또는 타임아웃을 구성하거나 복호화 또는 VPN 세션 설정을 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |
| HSM | **HSM** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 하드웨어 보안 모듈을 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성을 볼 수 있지만 변경할 수는 없습니다. | 예 | 예 | 예 |
| 고가용성 | 고가용성 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 고가용성 노드를 볼 수 없거나 일반 설정 정보 또는 링크 및 경로 모니터링과 같은 방화벽 전반의 고가용성 구성 정보에 액세스할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 고가용성 구성 정보를 볼 수 있지만 구성 절차를 수행할 수 없습니다. | 예 | 예 | 예 |
| 구성 감사 | 구성 감사 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 구성 감사 노드를 볼 수 없으며 방화벽 전체 구성 정보에 액세스할 수 없습니다. | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 관리자 | 관리자 노드에 대한 액세스를 제어합니다. 이 기능은 읽기 전용 액세스에만 허용될 수 있습니다.<br>이 권한을 비활성화하면 관리자는 관리자 노드를 볼 수 없거나 자신의 관리자 계정에 대한 정보에 액세스할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 자신의 관리자 계정에 대한 구성 정보를 볼 수 있습니다. 방화벽에 구성된 다른 관리자 계정에 대한 정보는 표시되지 않습니다. | 아니요 | 예 | 예 |
| 관리자 역할 | 관리 역할 노드에 대한 액세스를 제어합니다. 이 기능은 읽기 전용 액세스에만 허용될 수 있습니다.<br>이 권한을 비활성화하면 관리자는 관리자 역할 노드를 볼 수 없으며 관리자 역할 프로파일 구성과 관련된 방화벽 전체 정보에 액세스할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 방화벽에 구성된 모든 관리자 역할에 대한 구성 정보를 볼 수 있습니다. | 아니요 | 예 | 예 |
| 인증 프로파일 | 인증 프로파일 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 인증 프로파일 노드를 볼 수 없거나 RADIUS, TACACS+, LDAP, Kerberos, SAML, 다단계 인증(MFA) 또는 로컬 데이터베이스 인증 설정을 지정하는 인증 프로파일을 만들거나 편집할 수 없습니다. PAN-OS는 인증 프로파일을 사용하여 방화벽 관리자와 인증 포털 또는 GlobalProtect 최종 사용자를 인증합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 인증 프로파일 정보를 볼 수 있지만 인증 프로파일을 만들거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| 인증 순서 | 인증 시퀀스 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 인증 시퀀스 노드를 볼 수 없으며 인증 시퀀스를 생성 또는 편집할 수 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 이 권한을 읽기 전용으로 설정하면 관리자는 인증 프로파일 정보를 볼 수 있지만 인증 시퀀스를 생성하거나 편집할 수는 없습니다. | | | |
| 가상 시스템 | 가상 시스템 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 가상 시스템을 보거나 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 가상 시스템을 볼 수 있지만 구성을 추가하거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| 공유 게이트웨이 | 공유 게이트웨이 노드에 대한 액세스를 제어합니다. 공유 게이트웨이를 통해 가상 시스템은 외부 통신을 위한 공통 인터페이스를 공유할 수 있습니다.<br>이 권한을 비활성화하면 관리자가 공유 게이트웨이를 보거나 구성할 수 없습니다.<br>권한 상태가 읽기 전용으로 설정된 경우 현재 구성된 공유 게이트웨이를 볼 수 있지만 구성을 추가하거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| 사용자 식별 | 사용자 식별 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 사용자 식별 노드를 볼 수 없거나 사용자 매핑, 연결 보안, User-ID 에이전트, 터미널 서버 에이전트, 그룹 매핑 설정 또는 인증 포털 설정과 같은 방화벽 전체의 사용자 식별 구성 정보에 액세스할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 구성 정보를 볼 수 있지만 구성 절차를 수행할 수 없습니다. | 예 | 예 | 예 |
| VM 정보 소스 | VM 인벤토리를 자동으로 수집하도록 방화벽/Windows User-ID 에이전트를 구성할 수 있는 **VM** 정보 소스 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **VM** 정보 소스 노드를 볼 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 구성된 VM 정보 소스를 볼 수 있지만 소스를 추가, 편집 또는 삭제할 수는 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 이 권한은 디바이스 그룹 및 템플릿 관리자에게 제공되지 않습니다. | | | |
| 인증서 관리 | 아래에 설명된 모든 인증서 설정에 대해 기본 상태를 활성화 또는 비활성화하도록 설정합니다. | 예 | 아니요 | 예 |
| 인증서 | 인증서 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 인증서 노드를 볼 수 없으며 디바이스 인증서 또는 신뢰할 수 있는 기본 인증 기관에 대한 정보를 구성하거나 액세스할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 인증서 구성 정보를 볼 수 있지만 구성 절차를 수행할 수 없습니다. | 예 | 예 | 예 |
| 인증서 프로파일 | 인증서 프로파일 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 인증서 프로파일 노드를 볼 수 없거나 인증서 프로파일을 만들 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 현재 방화벽에 대해 구성되어 있지만 인증서 프로파일을 만들거나 편집할 수 없는 인증서 프로파일을 볼 수 있습니다. | 예 | 예 | 예 |
| OCSP 응답자 | **OCSP** 응답자 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 **OCSP** 응답자 노드를 볼 수 없거나 방화벽에 의한 인증서 문제의 해지 상태를 확인하는 데 사용할 서버를 정의할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 **OCSP** 응답자 구성을 볼 수 있지만 OCSP 응답자 구성을 만들거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| SSL/TLS 서비스 프로파일 | **SSL/TLS** 서비스 프로파일 노드에 대한 액세스를 제어합니다.<br>이 권한을 비활성화하면 관리자가 노드를 볼 수 없거나 SSL/TLS를 사용하는 방화벽 서비스에 대한 인증서 및 프로토콜 버전 또는 버전 범위를 지정하는 프로파일을 구성할 수 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 이 권한을 읽기 전용으로 설정하면 관리자는 기존 SSL/TLS 서비스 프로파일을 볼 수 있지만 생성하거나 편집할 수는 없습니다. | | | |
| SCEP | **SCEP** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 노드를 볼 수 없거나 고유한 디바이스 인증서를 발급하기 위한 Simple Certificate Enrollment Protocol(SCEP) 설정을 지정하는 프로파일을 정의할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 기존 SCEP 프로파일을 볼 수 있지만 만들거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| SSL 복호화 제외 | **SSL** 복호화 제외 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 노드를 볼 수 없거나 SSL 복호화가 사용자 지정 제외를 추가하는 것을 볼 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 기존 SSL 복호화 예외를 볼 수 있지만 생성하거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| SSH 서비스 프로필 | **SSL/TLS** 서비스 프로파일 노드에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자가 노드를 보거나 Palo Alto Networks 관리 및 HA(고가용성) 어플라이언스에 대한 SSH 연결에 대한 매개 변수를 지정하도록 프로파일을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 기존 SSL/TLS 서비스 프로파일을 볼 수 있지만 생성하거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| 응답 페이지 | 응답 페이지 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 응답 페이지 노드를 볼 수 없거나 요청된 웹 페이지 또는 파일 대신 다운로드되어 표시되는 사용자 정의 HTML 메시지를 정의할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 응답 페이지 구성을 볼 수 있지만 응답 페이지 구성을 만들거나 편집할 수는 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 로그 설정 | 아래에 설명된 모든 로그 설정에 대해 기본 상태를 활성화 또는 비활성화하도록 설정합니다. | 예 | 아니요 | 예 |
| 체계 | 로그 설정 > 시스템 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Log Settings** > **System** 노드를 보거나 방화벽이 Panorama 또는 외부 서비스(예: syslog 서버)로 포워딩하는 로그를 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 로그 설정 > 시스템 설정을 볼 수 있지만 설정을 추가, 편집 또는 삭제할 수는 없습니다. | 예 | 예 | 예 |
| 구성 | 로그 설정 > 구성 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Log Settings** > **Configuration** 노드를 보거나 방화벽이 Panorama 또는 외부 서비스(예: syslog 서버)에 포워딩할 구성 로그를 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 로그 설정 > 구성 설정을 볼 수 있지만 설정을 추가, 편집 또는 삭제할 수는 없습니다. | 예 | 예 | 예 |
| User-ID | 로그 설정 > 사용자 **ID** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Log Settings** > **User-ID** 노드를 보거나 방화벽이 Panorama 또는 외부 서비스(예: syslog 서버)에 포워딩할 사용자 ID를 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 **Log Settings** > **User-ID** 설정을 볼 수 있지만 설정을 추가, 편집 또는 삭제할 수는 없습니다. | 예 | 예 | 예 |
| HIP 매치 | 로그 설정 > **HIP** 일치 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 로그 설정 > **HIP** 일치 노드를 볼 수 없거나 방화벽이 Panorama 또는 외부 서비스(예: syslog 서버)로 포워딩하는 일치하는 호스트 정보 프로파일(HIP)을 지정할 수 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | HIP 일치 로그는 GlobalProtect 엔드포인트에 적용되는 보안 정책 규칙에 대한 정보를 제공합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 로그 설정 > **HIP** 설정을 볼 수 있지만 설정을 추가, 편집 또는 삭제할 수는 없습니다. | | | |
| GlobalProtect | 로그 설정 > **GlobalProtect** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Log Settings** > **GlobalProtect** 노드를 보거나 방화벽이 Panorama 또는 외부 서비스(예: syslog 서버)에 포워딩할 GlobalProtect를 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 **Log Settings** > **GlobalProtect** 설정을 볼 수 있지만 설정을 추가, 편집 또는 삭제할 수는 없습니다. | 예 | 예 | 예 |
| 상관 관계 | 로그 설정 > 상관 관계 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Log Settings** > **Correlation** 노드를 보거나 상관 관계 로그 포워딩 설정이나 태그 소스 또는 대상 IP 주소를 추가, 삭제 또는 수정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 로그 설정 > 상관 관계 설정을 볼 수 있지만 설정을 추가, 편집 또는 삭제할 수는 없습니다. | 예 | 예 | 예 |
| 알람 설정 | 로그 설정 > 알람 설정 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Log Settings** > **Alarm Settings** 노드를 보거나 보안 정책 규칙(또는 규칙 그룹)이 구성 가능한 기간 내에 반복적으로 적중될 때 방화벽이 생성하는 알림을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽에 대한 로그 설정 > 경보 설정을 볼 수 있지만 설정을 편집할 수는 없습니다. | 예 | 예 | 예 |
| 로그 관리 | 로그 설정 > 로그 관리 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 는 로그 설정 > 로그 관리 노드를 보거나 표시된 로그를 지울 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 로그 설정 > 로그 관리 정보를 볼 수 있지만 로그를 지울 수는 없습니다. | | | |
| 서버 프로파일 | 아래에 설명된 모든 서버 프로파일 설정에 대해 기본 상태를 활성화 또는 비활성화하도록 설정합니다. | 예 | 아니요 | 예 |
| SNMP 트랩 | 서버 프로파일 > **SNMP** 트랩 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 서버 프로파일 > **SNMP** 트랩 노드를 볼 수 없거나 시스템 로그 항목에 사용할 하나 이상의 SNMP 트랩 대상을 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **SNMP** 트랩 로그 정보를 볼 수 있지만 SNMP 트랩 대상을 지정할 수는 없습니다. | 예 | 예 | 예 |
| Syslog | 서버 프로파일 > **Syslog** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Server Profiles** > **Syslog** 노드를 볼 수 없거나 하나 이상의 syslog 서버를 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 **Server Profiles** > **Syslog** 정보를 볼 수 있지만 syslog 서버를 지정할 수는 없습니다. | 예 | 예 | 예 |
| 이메일 | 서버 프로파일 > 이메일 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 서버 프로파일 > 이메일 노드를 볼 수 없거나 시스템 및 구성 로그 항목에 대한 이메일 알림을 활성화하는 데 사용할 수 있는 이메일 프로파일을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > 이메일 정보를 볼 수 있지만 이메일 서버 프로파일을 구성할 수는 없습니다. | 예 | 예 | 예 |
| HTTP | 서버 프로파일 > **HTTP** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 자는 서버 프로파일 > **HTTP** 노드를 볼 수 없거나 모든 로그 항목을 HTTP 대상으로 포워딩하는 데 사용할 수 있는 HTTP 서버 프로파일을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **HTTP** 정보를 볼 수 있지만 HTTP 서버 프로파일을 구성할 수는 없습니다. | | | |
| Netflow | 서버 프로파일 > **Netflow** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 서버 프로파일 > **Netflow** 노드를 볼 수 없거나 내보낸 데이터를 수신할 NetFlow 서버와 함께 내보내기 빈도를 지정하는 NetFlow 서버 프로파일을 정의할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **Netflow** 정보를 볼 수 있지만 Netflow 프로파일을 정의할 수는 없습니다. | 예 | 예 | 예 |
| RADIUS | 서버 프로파일 > **RADIUS** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Server Profiles** > **RADIUS** 노드를 볼 수 없거나 인증 프로파일에서 식별된 RADIUS 서버에 대한 설정을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **RADIUS** 정보를 볼 수 있지만 RADIUS 서버에 대한 설정을 구성할 수는 없습니다. | 예 | 예 | 예 |
| TACACS+ | 서버 프로파일 > **TACACS+** 노드에 대한 액세스를 제어합니다.<br>이 권한을 비활성화하면 관리자는 인증 프로파일이 참조하는 TACACS+ 서버에 대한 설정을 구성하거나 노드를 볼 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 기존 TACACS+ 서버 프로파일을 볼 수 있지만 추가하거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| LDAP | 서버 프로파일 > **LDAP** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 자는 서버 프로파일 > **LDAP** 노드를 볼 수 없거나 인증 프로파일을 통해 인증에 사용할 LDAP 서버에 대한 설정을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **LDAP** 정보를 볼 수 있지만 LDAP 서버에 대한 설정을 구성할 수는 없습니다. | | | |
| Kerberos | 서버 프로파일 > **Kerberos** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 서버 프로파일 > **Kerberos** 노드를 볼 수 없거나 사용자가 기본적으로 도메인 컨트롤러에 인증할 수 있도록 허용하는 Kerberos 서버를 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **Kerberos** 정보를 볼 수 있지만 Kerberos 서버에 대한 설정을 구성할 수는 없습니다. | 예 | 예 | 예 |
| SAML ID 공급자 | 서버 프로파일 > **SAML ID** 공급자 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 노드를 보거나 SAML ID 공급자(IdP) 서버 프로파일을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **SAML ID** 공급자 정보를 볼 수 있지만 SAML IdP 서버 프로파일을 구성할 수는 없습니다. | 예 | 예 | 예 |
| 다단계 인증 | **Server Profiles** > **Multi Factor Authentication** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 노드를 보거나 MFA(다단계 인증) 서버 프로파일을 구성할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 서버 프로파일 > **SAML IdP** 정보를 볼 수 있지만 MFA 서버 프로파일을 구성할 수는 없습니다. | | | |
| 로컬 사용자 데이터베이스 | 아래에 설명된 모든 로컬 사용자 데이터베이스 설정에 대해 기본 상태를 활성화 또는 비활성화하도록 설정합니다. | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 사용자 | 로컬 사용자 **Database** > **Users** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 로컬 사용자 데이터베이스 > 사용자 노드를 볼 수 없거나 원격 액세스 사용자, 방화벽 관리자 및 인증 포털 사용자에 대한 인증 정보를 저장하기 위해 방화벽에 로컬 데이터베이스를 설정하지 않습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 로컬 사용자 데이터베이스 > 사용자 정보를 볼 수 있지만 인증 정보를 저장하기 위해 방화벽에 로컬 데이터베이스를 설정할 수는 없습니다. | 예 | 예 | 예 |
| 사용자 그룹 | 로컬 사용자 **Database** > **Users** 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 로컬 사용자 데이터베이스 > 사용자 노드를 볼 수 없거나 로컬 데이터베이스에 사용자 그룹 정보를 추가할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 로컬 사용자 데이터베이스 > 사용자 정보를 볼 수 있지만 로컬 데이터베이스에 사용자 그룹 정보를 추가할 수는 없습니다. | 예 | 예 | 예 |
| 액세스 도메인 | 액세스 도메인 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 액세스 도메인 노드를 볼 수 없거나 액세스 도메인을 생성 또는 편집할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 액세스 도메인 정보를 볼 수 있지만 액세스 도메인을 생성하거나 편집할 수는 없습니다. | 예 | 예 | 예 |
| 예약된 로그 내보내기 | 예약된 로그 내보내기 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 예약된 로그 내보내기 노드를 볼 수 없거나 로그 내보내기를 예약하고 파일 전송 프로토콜(FTP) 서버에 CSV 형식으로 저장하거나 보안 복사(SCP)를 사용하여 방화벽과 원격 호스트 간에 데이터를 안전하게 전송할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 예약된 로그 내보내기 프로파일 정보를 볼 수 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 있지만 로그 내보내기를 예약할 수는 없습니다. | | | |
| 소프트웨어 | 소프트웨어 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 소프트웨어 노드를 볼 수 없거나 Palo Alto Networks에서 제공하는 최신 버전의 PAN-OS 소프트웨어를 볼 수 없으며 각 버전의 릴리스 정보를 읽고 다운로드 및 설치할 릴리스를 선택할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 소프트웨어 정보를 볼 수 있지만 소프트웨어를 다운로드하거나 설치할 수는 없습니다. | 예 | 예 | 예 |
| GlobalProtect 클라이언트 | **GlobalProtect** 클라이언트 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **GlobalProtect** 클라이언트 노드를 보거나 사용 가능한 GlobalProtect 릴리스를 보거나 코드를 다운로드하거나 GlobalProtect 앱을 활성화할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 사용 가능한 **GlobalProtect** 클라이언트 릴리스를 볼 수 있지만 앱 소프트웨어를 다운로드하거나 설치할 수는 없습니다. | 예 | 예 | 예 |
| 동적 업데이트 | 동적 업데이트 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자가 동적 업데이트 노드를 볼 수 없거나 최신 업데이트를 보거나 각 업데이트에 대한 릴리스 정보를 읽거나 업로드 및 설치할 업데이트를 선택할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 사용 가능한 동적 업데이트 릴리스를 보고 릴리스 정보를 읽을 수 있지만 소프트웨어를 업로드하거나 설치할 수는 없습니다. | 예 | 예 | 예 |
| 라이선스 | 라이선스 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 라이선스 노드를 볼 수 없으며 설치된 라이선스를 보거나 라이선스를 활성화할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 설치된 라이선스를 볼 수 있지만 라이선스 관리 기능은 수행할 수 없습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 지원 | 지원 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 지원 노드를 보거나 지원을 활성화하거나 Palo Alto Networks의 프로덕션 및 보안 경고에 액세스할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 지원 노드를 보고 프로덕션 및 보안 경고에 액세스할 수 있지만 지원을 활성화할 수는 없습니다. | 예 | 예 | 예 |
| 마스터 키 및 진단 | 마스터 키 및 진단 노드에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 마스터 키 및 진단 노드를 볼 수 없거나 방화벽에서 개인 키를 암호화하기 위해 마스터 키를 지정할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 마스터 키 및 진단 노드를 보고 지정되었지만 새 마스터 키 구성을 추가하거나 편집할 수 없는 마스터 키에 대한 정보를 볼 수 있습니다. | 예 | 예 | 예 |
| 정책 제안 | **IoT** 및 **SaaS** 정책 규칙 권장 사항에 대한 액세스를 제어합니다. 이러한 권한을 비활성화하면 비활성화하는 권한에 따라 관리자가 **Policy Recommendation** > **IoT** 노드, **Policy Recommendation** > **SaaS** 노드 또는 둘 다를 볼 수 없습니다.<br>이러한 권한을 읽기 전용으로 설정하면 관리자는 노드를 볼 수 있지만 정책 규칙을 가져오거나 정보를 편집할 수는 없습니다. | 예 | 예 | 예 |

## 관리자 역할 프로파일에서 사용자 개인 정보 설정 정의

관리자가 액세스할 수 있는 비공개 최종 사용자 데이터를 정의하려면 관리자 역할 프로파일( **Device** > **Admin** 역할)을 만들거나 편집할 때 **WebUI** 탭에서 개인 정보 옵션까지 아래로 스크롤합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 개인 정보 | 아래에 설명된 모든 개인 정보 설정에 대해 기본 상태를 활성화 또는 비활성화하도록 설정합니다. | 예 | 해당 사항 없음 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 전체 IP 주소 표시 | 비활성화하면 Palo Alto 방화벽을 통해 실행되는 트래픽에서 얻은 전체 IP 주소가 로그나 보고서에 표시되지 않습니다. 일반적으로 표시되는 IP 주소 대신 해당 서브넷이 표시됩니다.<br><br>***Monitor*** **>** ***Reports***를 통해 인터페이스에 표시되는 예약된 보고서와 예약된 이메일을 통해 전송되는 보고서는 여전히 전체 ***IP*** 주소를 표시합니다. 이 예외 때문에 모니터 탭에서 다음 설정을 비활성화로 설정하는 것이 좋습니다. 맞춤형 보고서, 애플리케이션 보고서, 위협 보고서, ***URL*** 필터링 보고서, 트래픽 보고서 및 이메일 스케줄러. | 예 | 해당 사항 없음 | 예 |
| 로그 및 보고서에 사용자 이름 표시 | 비활성화하면 Palo Alto Networks 방화벽을 통해 실행되는 트래픽에서 얻은 사용자 이름이 로그나 보고서에 표시되지 않습니다. 사용자 이름이 일반적으로 표시되는 열은 비어 있습니다.<br><br>모니터 **>** 보고서를 통해 인터페이스에 표시되는 예약된 보고서 또는 이메일 스케줄러를 통해 전송된 보고서에는 여전히 사용자 이름이 표시됩니다. 이 예외 때문에 모니터 탭에서 다음 설정을 비활성화로 설정하는 것이 좋습니다. 맞춤형 보고서, 애플리케이션 보고서, 위협 보고서, ***URL*** 필터링 보고서, 트래픽 보고서 및 이메일 스케줄러. | 예 | 해당 사항 없음 | 예 |
| PCAP 파일 보기 | 비활성화하면 트래픽, 위협 및 데이터 필터링 로그에서 일반적으로 사용할 수 있는 패킷 캡처 파일이 표시되지 않습니다. | 예 | 해당 사항 없음 | 예 |


©2023 Palo Alto Networks, Inc.

## 관리자 액세스 제한 커밋 및 유효성 검사 기능

관리자 역할 프로파일(디바이스 > 관리자 역할)을 만들거나 편집할 때 커밋(및 되돌리기)에 대한 액세스를 제한하려면 **WebUI** 탭에서 커밋, 저장, 및 유효성 검사로 스크롤합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 커밋 | 아래 설명된 모든 커밋 및 되돌리기 권한에 대해 기본 상태를 활성화하거나 비활성화하도록 설정합니다. | 예 | 해당 사항 없음 | 예 |
| 디바이스 | 비활성화된 경우 관리자는 관리자가 방화벽 구성에 대해 변경한 내용을 커밋하거나 되돌릴 수 없습니다. | 예 | 해당 사항 없음 | 예 |
| 다른 관리자에 대한 커밋 | 비활성화된 경우 관리자는 다른 관리자가 방화벽 구성에 대해 변경한 내용을 커밋하거나 되돌릴 수 없습니다. | 예 | 해당 사항 없음 | 예 |
| 저장 | 아래에 설명된 모든 저장 작업 권한에 대해 기본 상태를 사용하도록 설정하거나 비활성화합니다. | 예 | 해당 사항 없음 | 예 |
| 부분 저장 | 비활성화하면 관리자는 관리자가 자신의 변경 내용을 포함하여 방화벽 구성에 대한 변경 내용을 저장할 수 없습니다. | 예 | 해당 사항 없음 | 예 |
| 다른 관리자 대상 저장 | 비활성화하면 관리자는 다른 관리자가 방화벽 구성에 대한 변경 내용을 저장할 수 없습니다. | 예 | 해당 사항 없음 | 예 |
| 확인 | 비활성화되면 관리자가 구성을 확인할 수 없습니다. | 예 | 해당 사항 없음 | 예 |

## 전역 설정에 대한 세분화된 액세스 제공

관리자 역할 프로파일(디바이스 > 관리자역할)을 만들거나 편집할 때 액세스할 수 있는 전역 설정 및 관리자를 정의하려면 **WebUI** 탭의 전역 옵션으로 스크롤합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 글로벌 | 아래 설명된 모든 전역 설정을 활성화하거나 비활성화하도록 기본 상태를 설정합니다. 실제로 이 설정은 현재 시스템 알람에만 적용됩니다. | 예 | 해당 사항 없음 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 시스템 알람 | 비활성화된 경우 관리자는 생성된 경보를 보거나 인정할 수 없습니다. | 예 | 해당 사항 없음 | 예 |

## Panorama 탭에 대한 세분화된 액세스 제공

다음 표에는 **Panorama** 탭 액세스 수준과 사용할 수 있는 사용자 지정 Panorama 관리자 역할이 나열됩니다. 방화벽 관리자는 이러한 권한에 액세스할 수 없습니다.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| 설정 | 관리자가 관리, 운영 및 원격 측정, 서비스, Content-ID, **WildFire**, 세션 또는 **HSM**를 포함하는 Panorama 설정 정보를 보거나 편집할 수 있는지 여부를 지정합니다.<br>권한을 다음과 같은 것으로 설정하면 다음을 수행합니다.<br>• 읽기 전용 관리자는 정보를 볼 수 있지만 편집할 수는 없습니다.<br>• 이 권한을 사용하지 않도록 설정하면 관리자는 정보를 보거나 편집할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 고가용성 | 관리자가 Panorama 관리 서버에 대한 HA(고가용성) 설정을 보고 관리할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 관리 서버에 대한 HA 구성 정보를 볼 수 있지만 구성을 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 관리 서버에 대한 HA 구성 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| 구성 감사 | 관리자가 Panorama 구성 감사를 실행할 수 있는지의 여부를 지정합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 구성 감사를 실행할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |
| 관리자 | 관리자가 Panorama 관리자 계정 세부 정보를 볼 수 있는지의 여부를 지정합니다.<br>이 함수에 대한 전체 액세스를 활성화할 수는 없습니다. 동적 역할을 하는 Panorama 관리자만 Panorama 관리자를 추가, 편집 또는 삭제할 수 있습니다. 읽기 전용 액세스를 통해 관리자는 자신의 계정에 대한 정보를 볼 수 있지만 다른 Panorama 관리자 계정은 볼 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 자신의 권한을 포함하여 Panorama 관리자 계정에 대한 정보를 볼 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 아니요 | 예 | 예 |
| 관리자 역할 | 관리자가 Panorama 관리자 역할을 볼 수 있는지의 여부를 지정합니다.<br>이 함수에 대한 전체 액세스를 활성화할 수는 없습니다. 동적 역할을 하는 Panorama 관리자만 사용자 지정 Panorama 역할을 추가, 편집 또는 삭제할 수 있습니다. 읽기 전용 액세스를 통해 관리자는 Panorama 관리자 역할 구성을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 관리자 역할을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 아니요 | 예 | 예 |
| 액세스 도메인 | 관리자가 Panorama 관리자의 액세스 도메인 구성을 보거나, 추가, 편집, 삭제하거나 복사할 수 있는 | Panorama: 예 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 지의 여부를 지정합니다. 이 권한은 액세스 도메인에 할당된 디바이스 그룹, 템플릿 및 방화벽 컨텍스트에 액세스하지 않고 액세스 도메인 구성에만 액세스할 수 있습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 액세스 도메인 구성을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 액세스 도메인 구성을 보거나 관리할 수 없습니다. | 디바이스 그룹/템플릿: 아니요<br>액세스 도메인에 할당된 디바이스 그룹 및 템플릿 관리자에게 액세스 도메인을 할당하여 해당 액세스 도메인에 할당된 디바이스 그룹, 템플릿 및 방화벽 컨텍스트 내에서 구성 및 모니터링 데이터에 액세스할 수 있습니다. | | | |
| 인증 프로파일 | 관리자가 Panorama 관리자의 인증 프로파일을 보거나 추가, 편집, 삭제 또는 복사할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 인증 프로파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 인증 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 인증 순서 | 관리자가 Panorama 관리자를 위해 인증 시퀀스를 보거나, 추가, 편집, 삭제하거나 복사할 수 있는지의 여부를 지정합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 인증 시퀀스를 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 인증 시퀀스를 보거나 관리할 수 없습니다. | | | | |
| 사용자 식별 | 관리자가 사용자 ID 연결 보안을 구성하고 데이터 재배포 지점(예: User-ID 에이전트)을 보거나 추가, 편집 또는 삭제할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 사용자 ID 연결 보안 및 재배포 지점에 대한 설정을 볼 수 있지만 설정을 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 사용자 ID 연결 보안 또는 재배포 지점에 대한 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 관리되는 디바이스 | 관리자가 방화벽을 관리되는 디바이스로 보거나 추가, 편집 또는 삭제할 수 있는지의 여부를 지정하고 소프트웨어 또는 콘텐츠 업데이트를 설치합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 관리되는 방화벽을 볼 수 있지만 업데이트를 추가, 삭제, 태그 또는 설치할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 관리되는 방화벽에서 업데이트를 보거나, 추가, 편집, 태그, 삭제 또는 설치할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예<br>(장치 그룹 및 템플릿 역할 없음) | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 디바이스 배포 권한이 있는 관리자는 ***Panorama*** > 디바이스 배포를 선택하여 관리되는 방화벽에 업데이트를 설치할 수 있습니다. | | | | |
| 템플릿 | 관리자가 템플릿 및 템플릿 스택(template stack)을 보거나 편집, 추가 또는 삭제할 수 있는지의 여부를 지정합니다.<br>읽기 전용으로 권한을 설정하면 관리자는 템플릿 및 스택 구성을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자가 템플릿 및 스택 구성을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예<br>디바이스 그룹 및 템플릿 관리자는 해당 관리자에게 할당된 액세스 도메인 내에 있는 템플릿 및 스택만 볼 수 있습니다. | 예<br>(디바이스 그룹 및 템플릿 관리자 없음) | 예 | 예 |
| 디바이스 그룹 | 관리자가 디바이스 그룹을 보거나 편집, 추가 또는 삭제할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 디바이스 그룹 구성을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 디바이스 그룹 구성을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예<br>디바이스 그룹 및 템플릿 관리자는 해당 관리자에게 할당된 액세스 도메인 내에 있는 디바이스 그룹만 액세스할 수 있습니다. | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| 관리되는 컬렉터 | 관리자가 관리되는 수집렉터를 보거나 편집, 추가 또는 삭제할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 관리되는 컬렉터 구성을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 관리되는 수집기 구성을 보거나 편집, 추가 또는 삭제할 수 없습니다.<br>디바이스 배포 권한이 있는 관리자는 ***Panorama*** > 디바이스 배포 옵션을 사용하여 관리되는 수집기에 업데이트를 설치할 수 있습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 수집기 그룹 | 관리자가 Collector 그룹을 보거나 편집, 추가 또는 삭제할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Collector 그룹을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Collector 그룹을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| VMware Service Manager | 관리자가 VMware 서비스 관리자 설정을 보고 편집할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 설정을 볼 수 있지만 관련 구성 또는 운영 절차를 수행할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관 | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 련 구성 또는 운영 절차를 수행할 수 없습니다. | | | | |
| 인증서 관리 | 모든 Panorama 인증서 관리 권한에 대한 기본 상태(활성화 또는 비활성화)를 설정합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |
| 인증서 | 관리자가 인증서를 조회, 편집, 생성, 삭제, 취소, 갱신 또는 내보내기를 할 수 있는지의 여부를 지정합니다. 이 권한은 관리자가 HA 키를 가져오거나 내보낼 수 있는지의 여부도 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 인증서를 볼 수 있지만 인증서 또는 HA 키를 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 인증서 또는 HA 키를 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 인증서 프로파일 | 관리자가 Panorama 인증서 프로파일을 보거나, 추가, 편집, 삭제하거나 복사할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 인증서 프로파일을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 인증서 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| SSL/TLS 서비스 프로파일 | 관리자가 SSL/TLS 서비스 프로파일을 보거나, 추가, 편집, 삭제하거나 복사할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 SSL/TLS 서비스 프로 | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 SSL/TLS 서비스 프로파일을 보거나 관리할 수 없습니다. | | | | |
| 로그 설정 | 모든 로그 설정 권한에 대해 기본 상태(활성화 또는 비활성화)를 설정합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |
| 체계 | 관리자가 시스템 로그를 외부 서비스(syslog, 전자 메일, SNMP 트랩 또는 HTTP 서버)로 포워딩하는 것을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 시스템 로그 포워딩 설정을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한은 ***Panorama*** 및 로그 수집기에서 생성하는 시스템 로그에만 해당됩니다. 수집기 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 시스템 로그에 대한 포워딩을 제어합니다. 디바이스 > 로그설정 > 시스템 권한은 방화벽에서 외부 서비스로 직접 포워딩되는 로그 포워딩(로그 수집기 집계 제외)을 제어합니다. | | | | |
| 구성 | 관리자가 Config 로그의 포워딩을 제어하는 설정을 외부 서비스(syslog, 전자 메일, SNMP 트랩 또는 HTTP 서버)에 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Config 로그 포워딩 설정을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한은 ***Panorama*** 및 로그 수집기에서 생성하는 구성 로그에만 해당됩니다. 수집기 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 구성 로그에 대한 포워딩을 제어합니다. 디바이스 > 로그 설정 > 구성 권한은 방화벽에서 외부 서비스로 직접 전송하는 로그 포워딩(로그 수집기 집계 제외)을 제어합니다. | | | | |
| User-ID | 관리자가 외부 서비스(syslog, 전자 메일, SNMP 트랩 또는 HTTP 서버)에 사용자 ID 로그를 포워딩하는 것을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Config 로그 포워딩 설정을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한은 ***Panorama***가 생성하는 ***User-ID*** 로그만 관련이 있습니다. 수집기 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 ***User-ID*** 로그에 대한 포워딩을 제어합니다. 디바이스 > 로그설정 > User-ID 권한은 방화벽에서 외부 서비스로 직접 포워딩되는 로그 포워딩(로그 컬렉터에 대한 집계 없이)을 제어합니다. | | | | |
| HIP 매치 | 관리자가 레거시 모드의 Panorama 가상 어플라이언스에서 외부 서비스(syslog, 이메일, SNMP 트랩 또는 HTTP 서버)로 HIP 매치 로그의 포워딩을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 HIP 일치 로그의 포워딩 설정을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 컬렉터 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 ***HIP*** 매치 로그에 대한 포워딩을 제어합니다. 디바이스 > 로그 설정 > HIP 일치 권한은 방화벽에서 외부 서비스로 직접 로그 포워딩을 제어합니다(로그 수집기에서 집계하지 않음). | | | | |
| GlobalProtect | 관리자가 레거시 모드의 Panorama 가상 어플라이언스에서 외부 서비스(syslog, 이메일, SNMP 트랩 또는 HTTP 서버)로 GlobalProtect 로그의 포워딩을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 GlobalProtect 로그의 포워딩 설정을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 수집기 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 *GlobalProtect* 로그에 대한 포워딩을 제어합니다. 디바이스 > 로그 설정 > ***GlobalProtect*** 권한은 방화벽에서 외부 서비스로 직접 포워딩되는 로그 포워딩(로그 수집기 집계 제외)을 제어합니다. | | | | |
| 상관 관계 | 관리자가 레거시 모드의 파노라마 가상 어플라이언스에서 외부 서비스(syslog, 이메일, SNMP 트랩 또는 HTTP 서버)로 상관 관계 로그의 전달을 제어하는 설정을 보고 구성할 수 있는지 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 상관 관계 로그 포워딩 설정을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다.<br>수집기 그룹 권한(파노라마 > 수집기 그룹)은 *Panorama* 모드의 *Panorama M*-시리즈 기기 또는 *Panorama* 가상 기기에서 상관 관계 로그 전달을 제어합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| 트래픽 | 관리자가 레거시 모드의 Panorama 가상 어플라이언스에서 외부 서비스(syslog, 이메일, SNMP 트랩 또는 HTTP 서버)로 트래픽 로그의 포워딩을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 트래픽 로그의 포워딩 설정을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다.<br>수집기 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 트래픽 로그에 대한 포워딩을 제어합니다. 로그 포워딩 권한(개체 > 로그 포워딩)은 방화벽에서 외부 서비스로 직접 포워딩되는 것을 제어합니다(로그 수집기의 집계 없이). | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 위협 | 관리자가 레거시 모드의 Panorama 가상 어플라이언스에서 외부 서비스(syslog, 이메일, SNMP 트랩 또는 HTTP 서버)에 위협 로그의 포워딩을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 위협 로그의 포워딩 설정을 볼 수 있지만 관리할 수는 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다.<br><br>수집기 그룹 권한(***Panorama*** > 컬렉터그룹)은 로그 컬렉터가 방화벽에서 받는 위협 로그에 대한 포워딩을 제어합니다. 로그 포워딩 권한(개체 > 로그포워딩)은 방화벽에서 외부 서비스로 직접 포워딩되는 것을 제어합니다(로그 수집기의 집계 없이). | | | | |
| WildFire | 관리자가 레거시 모드의 Panorama 가상 어플라이언스에서 외부 서비스(syslog, 이메일, SNMP 트랩 또는 HTTP 서버)로 WildFire 로그의 포워딩을 제어하는 설정을 보고 구성할 수 있는지의 여부를 지정합니다.<br><br>이 권한을 읽기 전용으로 설정하면 관리자는 WildFire 로그의 포워딩 설정을 볼 수 있지만 관리할 수는 없습니다.<br><br>이 권한을 사용하지 않도록 설정하면 관리자는 설정을 보거나 관리할 수 없습니다. | Panorama: 예<br><br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 컬렉터 그룹 권한(***Panorama*** > 컬렉터 그룹)은 로그 컬렉터가 방화벽에서 받는 ***WildFire*** 로그에 대한 포워딩을 제어합니다. 로그 포워딩 권한(개체 > 로그 포워딩)은 방화벽에서 외부 서비스로 직접 포워딩되는 것을 제어합니다(로그 수집기의 집계 없이). | | | | |
| 서버 프로파일 | 모든 서버 프로파일 권한에 대해 기본 상태(활성화 또는 비활성화)를 설정합니다.<br>이러한 권한은 ***Panorama*** 또는 로그 컬렉터에서 로그를 포워딩하는 데 사용되는 서버 프로파일과 ***Panorama*** 관리자를 인증하는 데 사용되는 서버 프로파일만 관련이 있습니다. 디바이스 > 서버 프로필 권한은 방화벽에서 외부 서비스로 직접 로그를 전달하고 방화벽 관리자를 인증하는 데 사용되는 서버 프로필에 대한 액세스를 제어합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| SNMP 트랩 | 관리자가 SNMP 트랩 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 SNMP 트랩 서버 프로파일을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 SNMP 트랩 서버 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| Syslog | 관리자가 Syslog 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Syslog 서버 프로파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Syslog 서버 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 이메일 | 관리자가 전자 메일 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 전자 메일 서버 프로파일을 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 전자 메일 서버 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| RADIUS | 관리자가 Panorama 관리자를 인증하는 데 사용되는 RADIUS 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한을 읽기 전용으로 설정하면 관리자는 RADIUS 서버 프로파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 RADIUS 서버 프로파일을 보거나 관리할 수 없습니다. | | | | |
| TACACS+ | 관리자가 Panorama 관리자를 인증하는 데 사용되는 TACACS+ 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 프로파일 레퍼런스를 인증하는 TACACS+ 서버에 대한 노드 또는 설정을 확인할 수 없습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 기존 TACACS+ 서버 프로파일을 볼 수 있지만 추가하거나 편집할 수는 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| LDAP | 관리자가 Panorama 관리자를 인증하는 데 사용되는 LDAP 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 LDAP 서버 프로파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 LDAP 서버 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| Kerberos | 관리자가 Panorama 관리자를 인증하는 데 사용되는 Kerberos 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Kerberos 서버 프로 | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Kerberos 서버 프로파일을 보거나 관리할 수 없습니다. | | | | |
| SAML ID 공급자 | 관리자가 Panorama 관리자를 인증하는 데 사용되는 SAML ID 공급자(IDP) 서버 프로파일을 보고 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 SAML IdP 서버 프로파일을 볼 수 있지만 관리할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 SAML IdP 서버 프로파일을 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 예약된 구성 내보내기 | 관리자가 예약된 Panorama 구성 내보내기를 보거나, 추가, 편집, 삭제하거나 복사할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 예약된 내보내기를 볼 수 있지만 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 예약된 내보내기를 보거나 관리할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 아니요 | 예 |
| 소프트웨어 | 관리자가 Panorama 관리 서버에 설치된 소프트웨어 업데이트에 대한 정보를 볼 수 있는지의 여부를 지정합니다. 업데이트를 다운로드, 업로드 또는 설치하고, 관련 릴리스 노트를 봅니다.<br>이 권한을 읽기 전용으로 설정한 경우 관리자는 Panorama 소프트웨어 업데이트에 대한 정보를 보 | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 고 관련 릴리스 메모를 볼 수 있지만 관련 작업을 수행할 수 없습니다.<br><br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 소프트웨어 업데이트를 보거나, 연결된 릴리스 메모를 보거나, 관련 작업을 수행할 수 없습니다.<br><br>***Panorama*** > 디바이스 배포 > 소프트웨어 권한은 전용 로그 수집기에 배포된 방화벽 및 ***Panorama*** 소프트웨어에 배포된 ***PAN-OS*** 소프트웨어에 대한 액세스를 제어합니다. | | | | |
| 동적 업데이트 | 관리자가 Panorama 관리 서버에 설치된 콘텐츠 업데이트에 대한 정보를 볼 수 있는지의 여부(예: WildFire 업데이트)를 지정합니다. 업데이트를 다운로드, 업로드, 설치 또는 되돌리기고, 관련 릴리스 노트를 봅니다.<br><br>이 권한을 읽기 전용으로 설정한 경우 관리자는 Panorama 콘텐츠 업데이트에 대한 정보를 보고 관련 릴리스 메모를 볼 수 있지만 관련 작업을 수행할 수 없습니다.<br><br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 콘텐츠 업데이트를 보거나, 연결된 릴리스 메모를 보거나, 관련 작업을 수행할 수 없습니다. | Panorama: 예<br><br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | ***Panorama*** > 디바이스 배포 > 동적 업데이트 권한은 방화벽 및 전용 로그 수집기에 배포된 콘텐츠 업데이트에 대한 액세스를 제어합니다. | | | | |
| 지원 | 관리자가 Panorama 지원 라이선스 정보, 제품 경고 및 보안 경고를 볼 수 있는지의 여부를 지정하고, 지원 라이선스를 활성화하고 케이스를 관리합니다. 운용 관리자만 기술 지원 파일을 생성할 수 있습니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 지원 정보, 제품 경고 및 보안 경고를 볼 수 있지만 지원 라이선스를 활성화하거나 기술 지원 파일을 생성하거나 케이스를 관리할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하는 경우 관리자는 Panorama 지원 정보, 제품 경고 또는 보안 경고를 볼 수 없습니다. 지원 라이선스를 활성화하거나 기술 지원 파일을 생성하거나 서비스 케이스를 관리합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 아니요 | 예 | 예 | 예 |
| 디바이스 배포 | 방화벽 및 로그 컬렉터에 라이선스 및 소프트웨어 또는 콘텐츠 업데이트를 배포하는 것과 관련된 모든 권한에 대해 기본 상태, 활성화 또는 비활성화됨을 설정합니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | ***Panorama*** > 소프트웨어 및 ***Panorama*** > 동적 업데이트 권한은 *Panorama* 관리 서버에 설치된 소프트웨어 및 콘텐츠 업데이트를 제어합니다. | | | | |
| 소프트웨어 | 관리자가 방화벽 및 로그 컬렉터에 설치된 소프트웨어 업데이트에 대한 정보를 볼 수 있는지의 여부를 지정합니다. 업데이트를 다운로드, 업로드 또는 설치하고, 관련 릴리스 노트를 봅니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 소프트웨어 업데이트에 대한 정보를 확인하고 관련 릴리스 메모를 볼 수 있지만 방화벽 또는 전용 로그 수집기에 업데이트를 배포할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 소프트웨어 업데이트에 대한 정보를 보거나, 관련 릴리스 메모를 보거나, 방화벽 또는 전용 로그 수집기에 업데이트를 배포할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |
| GlobalProtect 클라이언트 | 관리자가 방화벽에서 GlobalProtect 앱 소프트웨어 업데이트에 대한 정보를 볼 수 있는지의 여부를 지정합니다. 업데이트를 다운로드, 업로드 또는 활성화하고 관련 릴리스 노트를 봅니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 GlobalProtect 앱 소프트웨어 업데이트에 대한 정보를 확인하고 관련 릴리스 메모를 볼 수 있지만 방화벽에서 업데이트를 활성화할 수는 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 이 권한을 사용하지 않도록 설정하면 관리자는 GlobalProtect 앱 소프트웨어 업데이트에 대한 정보를 보거나, 관련 릴리스 메모를 보거나, 방화벽에서 업데이트를 활성화할 수 없습니다. | | | | |
| 동적 업데이트 | 관리자가 방화벽 및 전용 로그 수집기에 설치된 콘텐츠 업데이트(예: 애플리케이션 업데이트)에 대한 정보를 볼 수 있는지의 여부를 지정합니다. 업데이트를 다운로드, 업로드 또는 설치하고, 관련 릴리스 노트를 봅니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 콘텐츠 업데이트에 대한 정보를 확인하고 관련 릴리스 메모를 볼 수 있지만 방화벽 또는 전용 로그 수집기에 업데이트를 배포할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 콘텐츠 업데이트에 대한 정보를 보거나, 관련 릴리스 메모를 보거나, 방화벽 또는 전용 로그 수집기에 업데이트를 배포할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |
| 라이선스 | 관리자가 방화벽 라이선스를 보고 새로 고치고 활성화할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 방화벽 라이선스를 볼 수 있지만 해당 라이선스를 새로 고치거나 활성화할 수는 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 방화벽 라이선스를 보거나 새로 고치거나 활성화할 수 없습니다. | Panorama: 예<br>디바이스 그룹/템플릿: 예 | 예 | 예 | 예 |
| 마스터 키 및 진단 | 관리자가 Panorama에서 개인 키를 암호화하는 마스터 키를 보고 | Panorama: 예 | 예 | 예 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 관리자 역할 가용성 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|---|
| | 구성할 수 있는지의 여부를 지정합니다.<br>이 권한을 읽기 전용으로 설정하면 관리자는 Panorama 마스터 키 구성을 볼 수 있지만 변경할 수 없습니다.<br>이 권한을 사용하지 않도록 설정하면 관리자는 Panorama 마스터 키 구성을 보거나 편집할 수 없습니다. | 디바이스 그룹/템플릿: 아니요 | | | |

## 운영 설정에 대한 세분화된 액세스 제공

관리자가 액세스할 수 있는 작업 설정을 정의하려면 방화벽에 대한 관리자 역할 프로파일을 만들거나 편집할 때(디바이스 > 관리자 역할) 웹 **UI** 탭에서 작업 옵션까지 아래로 스크롤합니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 재부팅 | 방화벽을 다시 시작합니다. 방화벽은 모든 사용자를 로그아웃하고, PAN-OS 소프트웨어와 활성 구성을 다시 로드하고, 기존 세션을 닫고 기록하고, 재부팅을 시작한 관리자의 이름을 보여주는 시스템 로그 항목을 생성합니다. | 예 | 해당 사항 없음 | 예 |
| 기술 지원 파일 생성 | Palo Alto Networks 지원 팀이 방화벽에서 발생할 수 있는 문제를 해결하는 데 사용할 수 있는 기술 지원 시스템 파일을 생성합니다. | 예 | 해당 사항 없음 | 예 |
| 통계 덤프 파일 생성 | 방화벽에 대해 지난 7일 동안의 네트워크 트래픽을 요약하는 XML 보고서 세트를 생성하고 다운로드합니다. | 예 | 해당 사항 없음 | 예 |
| 핵심 파일 다운로드 | 방화벽에서 시스템 프로세스 오류가 발생하면 프로세스와 실패한 이유에 대한 세부 정보가 포함된 코어 파일이 자동으로 생성됩니다. 이 코어 파일을 다운로드하여 Palo Alto Networks 지원 사례에 업로드하여 문제 해결에 대한 추가 지원을 받을 수 있습니다. | 예 | 해당 사항 없음 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 디버그 및 관리 Pcap 파일 다운로드 | 방화벽에서 패킷 캡처 실패가 발생하면 실패한 이유에 대한 디버그 및 관리 세부 정보가 포함된 패킷 캡처(pcap) 파일을 생성합니다. 파일을 다운로드한 후 Palo Alto Networks 지원 사례에 업로드하여 문제 해결에 대한 지원을 받으십시오. | 예 | 해당 사항 없음 | 예 |

## Panorama 웹 인터페이스 액세스 권한

사용자 지정 Panorama 관리자 역할을 사용하면 Panorama의 옵션에 대한 액세스를 정의하고 디바이스 그룹 및 템플릿(정책, 개체, 네트워크, 디바이스 탭)에 대한 액세스만 허용하는 기능을 정의할 수 있습니다.

생성할 수 있는 관리자 역할은 **Panorama**, 디바이스 그룹 및 템플릿입니다. 디바이스 그룹 및 템플릿 관리자 역할 프로파일에는 CLI 액세스 권한을 할당할 수 없습니다. CLI에 대한 운용 관리자 권한을 **Panorama** Admin Role 프로파일에 할당하면 해당 역할을 가진 관리자는 할당한 웹 인터페이스 권한에 관계없이 모든 기능에 액세스할 수 있습니다.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 대시보드 | 대시보드 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자가 탭을 표시하지 않으며 대시보드 위젯에 액세스할 수 없습니다. | 예 | 아니요 | 예 |
| ACC | 애플리케이션 명령 센터(ACC)에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 **ACC** 탭이 웹 인터페이스에 표시되지 않습니다. ACC에 대한 액세스를 제공하면서 사용자의 개인 정보를 보호하려는 경우 개인 정보 > 보호 쇼 전체 **IP**주소 옵션 및/또는 로그 및 보고서 표시 옵션에서 사용자 이름 표시 옵션을 비활성화할 수 있습니다. | 예 | 아니요 | 예 |
| 모니터 | 모니터 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 모니터 탭을 볼 수 없으며 로그, 패킷 캡처, 세션 정보, 보고서 또는 앱 범위에 액세스할 수 없습니다. 관리자가 볼 수 있는 모니터링 정보를 보다 세부적으로 제어하려면 모니터 옵션을 활성화된 상태로 두고 모니터 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 정책 | 정책 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 정책 탭을 볼 수 없으며 정책 정보에 액세스할 수 없습니다. 예를 들어 특정 유형의 정책에 대한 액세스를 활성화하거나 정책 정보에 대한 읽기 전용 액세스를 활성화하기 위해 관리자가 볼 수 있는 정책 정보를 보다 세부적으로 제어하려면 정책 옵션을 활성화한 상태로 두고 활성화하거나 정책 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 비활성화합니다. | 예 | 아니요 | 예 |
| 개체 | 개체 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 개체 탭을 볼 수 없으며 개체, 보안 프로파일, 로그 포워딩 프로파일, 복호화 프로파일 또는 일정에 액세스할 수 없습니다. 관리자가 볼 수 있는 개체를 보다 세부적으로 제어하려면 개체 옵션을 활성화한 상태로 두고 개체 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | 예 | 아니요 | 예 |
| 네트워크 | 네트워크 탭에 대한 액세스를 제어합니다. 이 권한을 사용하지 않도록 설정하면 관리자는 네트워크 탭을 볼 수 없으며 인터페이스, 영역, VLAN, 가상 와이어, 가상 라우터, IPsec 터널, DHCP, DNS 프록시, GlobalProtect 또는 QoS 구성 정보 또는 네트워크 프로파일에 액세스할 수 없습니다. 관리자가 볼 수 있는 개체를 보다 세부적으로 제어하려면 네트워크 옵션을 활성화된 상태로 두고 네트워크 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | 예 | 아니요 | 예 |
| 디바이스 | 디바이스 탭에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 디바이스 탭을 볼 수 없으며 사용자 ID, 고가용성, 서버 프로파일 또는 인증서 구성 정보와 같은 방화벽 전체 구성 정보에 액세스할 수 없습니다. 관리자가 볼 수 있는 개체를 보다 세부적으로 제어하려면 디바이스 옵션을 활성화된 상태로 두고 디바이스 탭에 대한 세분화된 액세스 제공에 | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| | 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다.<br><br>디바이스 탭에 대한 전체 액세스를 활성화하더라도 역할 기반 관리자에 대해 관리자 역할 또는 관리자 노드에 대한 액세스를 활성화할 수 없습니다. | | | |
| Panorama | **Panorama** 탭에 대한 액세스를 제어합니다. 이 권한을 비활성화하면 관리자는 **Panorama** 탭을 볼 수 없으며 관리 디바이스, 관리 수집기 또는 수집기 그룹과 같은 Panorama 전체 구성 정보에 액세스할 수 없습니다.<br><br>관리자가 볼 수 있는 개체를 보다 세부적으로 제어하려면 **Panorama** 옵션을 활성화된 상태로 두고 Panorama 탭에 대한 세분화된 액세스 제공에 설명된 대로 탭에서 특정 노드를 활성화 또는 비활성화합니다. | 예 | 아니요 | 예 |
| 개인 정보 | 관리자 역할 프로파일의 사용자 개인 정보 설정 정의에 설명된 개인 정보 설정에 대한 액세스를 제어합니다. | 예 | 아니요 | 예 |
| 확인 | 비활성화되면 관리자가 구성을 확인할 수 없습니다. | 예 | 아니요 | 예 |
| 저장 | 아래에 설명된 모든 저장 권한에 대한 기본 상태(활성화 또는 비활성화)를 설정합니다(부분 저장 및 다른 관리자용으로 저장). | 예 | 아니요 | 예 |
| • 부분 저장 | 비활성화된 경우 관리자는 관리자가 Panorama 구성에 대해 수행한 변경 사항을 저장할 수 없습니다. | 예 | 아니요 | 예 |
| • 다른 관리자 대상 저장 | 비활성화되면 관리자는 다른 관리자가 Panorama 구성에 수행한 변경 사항을 저장할 수 없습니다. | 예 | 아니요 | 예 |
| 커밋 | 아래에 설명된 모든 커밋, 푸시 및 되돌리기 권한(Panorama, 디바이스 그룹, 템플릿, 강제 템플릿 값, 수집기 그룹, WildFire 어플라이언스 클러스터)에 대한 기본 상태(활성화 또는 비활성화)를 설정합니다. | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| • Panorama | 비활성화되면 관리자는 자신의 변경 사항을 포함하여 관리자가 수행한 구성 변경 사항을 커밋하거나 되돌릴 수 없습니다. | 예 | 아니요 | 예 |
| • 다른 관리자 대상 커밋 | 비활성화되면 관리자는 다른 관리자가 수행한 구성 변경 사항을 커밋하거나 되돌릴 수 없습니다. | 예 | 아니요 | 예 |
| • 모든 변경 사항 푸시 | 사용하지 않도록 설정하면 관리자가 수행한 모든 구성 변경 내용을 관리자가 푸시할 수 없습니다. | 예 | 아니요 | 예 |
| • 다른 관리자를 위해 푸시 | 사용하지 않도록 설정하면 관리자가 수행한 모든 구성 변경 내용을 관리자가 푸시할 수 없습니다. | 예 | 아니요 | 예 |
| • 개체 수준 변경 사항 | 사용하지 않도록 설정하면 관리자가 푸시할 개별 구성 개체를 선택할 수 없습니다. | 예 | 아니요 | 예 |
| 디바이스 그룹 | 비활성화되면 관리자는 디바이스 그룹에 변경 사항을 푸시할 수 없습니다. | 예 | 아니요 | 예 |
| 템플릿 | 비활성화되면 관리자는 템플릿에 변경 사항을 푸시할 수 없습니다. | 예 | 아니요 | 예 |
| 강제 템플릿 값 | 이 권한은 범위 선택 푸시 대화 상자에서 템플릿 값 강제 적용 옵션에 대한 액세스를 제어합니다.<br>비활성화된 경우 관리자는 로컬 방화벽 구성에서 재정의된 설정을 Panorama가 템플릿에서 푸시하는 설정으로 바꿀 수 없습니다.<br>강제 템플릿 값이 활성화된 구성을 푸시하면 방화벽에서 재정의된 모든 값이 템플릿의 값으로 바뀝니다. 이 옵션을 사용하기 전에 방화벽에서 재정의된 값을 확인하여 커밋으로 인해 재정의된 값을 교체함으로써 발생하는 예기치 않은 네트워크 중단이나 문제가 발생하지 않는지 확인하십시오. | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

| 액세스 수준 | 설명 | 사용 | 읽기 전용 | 비활성화 |
|---|---|---|---|---|
| 수집기 그룹 | 비활성화되면 관리자는 수집기 그룹에 변경 사항을 푸시할 수 없습니다. | 예 | 아니요 | 예 |
| WildFire 어플라이언스 클러스터 | 비활성화되면 관리자는 WildFire 어플라이언스 클러스터에 변경 사항을 푸시할 수 없습니다. | 예 | 아니요 | 예 |
| 작업 | 비활성화되면 관리자는 작업 관리자에 액세스할 수 없습니다. | 예 | 아니요 | 예 |
| 글로벌 | 전역 설정에 대한 세분화된 액세스 제공에 설명된 전역 설정(시스템 경보)에 대한 액세스를 제어합니다. | 예 | 아니요 | 예 |


©2023 Palo Alto Networks, Inc.

# 참조: 포트 번호 사용

다음 표에는 방화벽과 Panorama가 서로 통신하거나 네트워크의 다른 서비스와 통신하는 데 사용하는 포트가 나열됩니다.


- 관리 기능에 사용되는 포트
- HA에 사용되는 포트
- Panorama에 사용되는 포트
- GlobalProtect에 사용되는 포트
- 사용자 ID에 사용되는 포트
- IPsec에 사용되는 포트
- 라우팅에 사용되는 포트
- DHCP에 사용되는 포트
- 인프라에 사용되는 포트


## 관리 기능에 사용되는 포트

방화벽과 Panorama는 관리 기능을 위해 다음 포트를 사용합니다.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| 22 | TCP | 클라이언트 시스템에서 방화벽 CLI 인터페이스로의 통신에 사용됩니다. |
| 80 | TCP | 방화벽이 OCSP 응답자로 작동할 때 OCSP(온라인 인증서 상태 프로토콜) 업데이트를 수신 대기하는 포트입니다. |
| 123 | UDP | 방화벽이 NTP 업데이트에 사용하는 포트입니다. |
| 443 | TCP | 클라이언트 시스템에서 방화벽 웹 인터페이스로의 통신에 사용됩니다. 이는 가상 네트워크에서 VM 모니터링을 사용하여 변경 사항을 추적할 때 방화벽 및 User-ID 에이전트가 업데이트를 수신 대기하는 포트이기도 합니다.<br>AWS 환경 모니터링을 위해 사용되는 유일한 포트입니다.<br>VMware vCenter/ESXi 환경을 모니터링하는 경우 수신 포트는 기본적으로 443으로 설정되지만 구성 가능합니다. |
| 4443 | TCP | HTTPS의 대체 SSL 포트로 사용됩니다. |
| 162 | UDP | 방화벽, Panorama 또는 로그 수집기가 트랩을 SNMP 관리자로 포워딩하는 데 사용하는 포트를 지정합니다. |


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| | | 이 포트는 ***Palo Alto Networks*** 방화벽에서 열 필요가 없습니다. 이 포트에서 수신 대기하도록 ***SNMP(Simple Network Management Protocol)*** 관리자를 구성해야 합니다. 자세한 내용은 ***SNMP*** 관리 소프트웨어 설명서를 참조하십시오. |
| 161 | UDP | 방화벽이 SNMP 관리자의 폴링 요청(GET 메시지)을 수신 대기하는 포트입니다. |
| 514<br>514<br>6514 | TCP<br>UDP<br>SSL | 방화벽, Panorama 또는 Log Collector가 Syslog Monitoring 구성인 경우 syslog 서버에 로그를 보내는 데 사용하는 포트와 PAN-OS가 User-ID 에이전트 또는 Windows 기반 User-ID 에이전트를 통합한 포트 ID 에이전트는 인증 syslog 메시지를 수신 대기합니다. |
| 2055 | UDP | NetFlow 내보내기를 구성하는 경우 방화벽이 NetFlow 레코드를 NetFlow 수집기로 보내는 데 사용하는 기본 포트이지만 구성 가능합니다. |
| 5008 | TCP | Port GlobalProtect Mobile Security Manager는 GlobalProtect 게이트웨이의 HIP 요청을 수신 대기합니다.<br>타사 MDM 시스템을 사용하는 경우 MDM 공급업체의 요구에 따라 다른 포트를 사용하도록 게이트웨이를 구성할 수 있습니다. |
| 6080<br>6081<br>6082 | TCP<br>TLS 1.2<br>TCP | User-ID™ 인증 포털에 사용되는 포트:<br>• NTLM(NT LAN Manager) 인증용 6080<br>• SSL/TLS 서버 프로파일이 없는 인증 포털의 경우 6081<br>• SSL/TLS 서버 프로파일이 있는 인증 포털의 경우 6082 |
| 10443 | SSL | 방화벽 및 Panorama가 위협에 대한 컨텍스트 정보를 제공하거나 위협 조사를 Threat Vault 및 AutoFocus로 원활하게 전환하는 데 사용하는 포트입니다. |

## HA에 사용되는 포트

고가용성(HA) 피어로 구성된 방화벽은 상태 정보(HA1 제어 링크)를 유지 관리하고 데이터(HA2 데이터 링크)를 동기화하기 위해 서로 통신할 수 있어야 합니다. 능동형/능동형 HA 배포에서 피어 방화벽은 세션을 소유한 HA 피어에도 패킷을 포워딩해야 합니다. HA3 링크는 레이어 2(MAC-in-MAC) 링크이며 레이어 3 주소 지정 또는 암호화를 지원하지 않습니다.


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| 28769<br>28260 | TCP<br>TCP | HA 피어 방화벽 간의 일반 텍스트 통신을 위한 HA1 제어 링크에 사용됩니다. HA1 링크는 레이어 3 링크이며 IP 주소가 필요합니다. |
| 28 | TCP | HA 피어 방화벽 간의 암호화된 통신(TCP를 통한 SSH)을 위한 HA1 제어 링크에 사용됩니다. |
| 28770 | TCP | HA1 백업 링크에 대한 수신 포트. |
| 28771 | TCP | 하트비트 백업에 사용됩니다. Palo Alto Networks는 HA1 또는 HA1 백업 링크에 대역 내 포트를 사용하는 경우 MGT 인터페이스에서 하트비트 백업을 활성화할 것을 권장합니다. |
| 99<br>29281 | IP<br>UDP | HA2 링크가 HA 쌍의 방화벽 간에 세션, 포워딩 테이블, IPSec 보안 연결 및 ARP 테이블을 동기화하는 데 사용됩니다. HA2 링크의 데이터 흐름은 항상 단방향입니다(HA2 연결 유지 제외). 능동형 방화벽(능동형/수동형) 또는 능동형-기본(능동형/능동형)에서 수동형 방화벽(능동형/수동형) 또는 능동형-보조(능동형/능동형)로 플로우됩니다. HA2 링크는 Layer 2 링크이며 기본적으로 ether type 0x7261을 사용합니다.<br>HA 데이터 링크는 또한 전송으로 IP(프로토콜 번호 99) 또는 UDP(포트 29281)를 사용하도록 구성할 수 있으며, 따라서 HA 데이터 링크가 서브넷을 확장할 수 있습니다. |

## Panorama에 사용되는 포트

Panorama는 다음 포트를 사용합니다.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| 22 | TCP | 클라이언트 시스템에서 Panorama CLI 인터페이스로의 통신에 사용됩니다. |
| 443 | TCP | 클라이언트 시스템에서 Panorama 웹 인터페이스로의 통신에 사용됩니다. |
| 444 | TCP | Panorama와 Cortex Data Lake 간의 통신에 사용됩니다. |
| 3978 | TCP | Panorama와 관리형 방화벽 또는 관리형 수집기 간의 통신과 수집기 그룹의 관리형 수집기 간의 통신에 사용됩니다.<br>• Panorama와 방화벽 간의 통신용입니다. 이 연결은 관리되는 방화벽에서 Panorama로 시작되며 방화벽이 로그를 Panorama로 포워딩하고 Panorama가 구성 변경 사항을 방 |


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| | | 화벽으로 푸시하는 양방향 데이터 교환을 용이하게 합니다. 컨텍스트 전환 명령은 동일한 연결을 통해 전송됩니다.<br>• 로그 수집기는 이 대상 포트를 사용하여 로그를 Panorama로 포워딩합니다.<br>• Panorama 모드에서 M-시리즈 어플라이언스의 기본 Log Collector 및 Dedicated Log Collector와 통신합니다. |
| 28443 | TCP | 관리되는 디바이스(방화벽 및 로그 수집기)에서 Panorama로부터 소프트웨어 및 콘텐츠 업데이트를 검색하는 데 사용됩니다.<br>***PAN-OS 8.x*** 이상의 버전을 실행하는 디바이스만 이 포트를 통해 ***Panorama***에서 업데이트를 검색합니다. 이전 릴리스를 실행하는 디바이스의 경우 ***Panorama***는 포트 ***3978***을 통해 업데이트 패키지를 푸시합니다. |
| 28769(5.1 이상)<br>28260(5.0 이상)<br>49160(5.0 이하) | TCP<br>TCP<br>TCP | 일반 텍스트 통신을 사용하는 Panorama HA 피어 간의 HA 연결 및 동기화에 사용됩니다. 어느 피어에서든 통신을 시작할 수 있습니다. |
| 28 | TCP | 암호화된 통신(TCP를 통한 SSH)을 사용하는 Panorama HA 피어 간의 HA 연결 및 동기화에 사용됩니다. 어느 피어에서든 통신을 시작할 수 있습니다.<br>로그 배포를 위해 수집기 그룹의 로그 수집기 간의 통신에 사용됩니다. |
| 28270(6.0 이상)<br>49190(5.1 이하) | TCP | 로그 배포를 위해 Collector Group의 Log Collector 간 통신에 사용됩니다. |
| 2049 | TCP | Panorama 가상 어플라이언스에서 NFS 데이터스토어에 로그를 쓰는 데 사용합니다. |
| 10443 | SSL | Panorama가 위협에 대한 컨텍스트 정보를 제공하거나 위협 조사를 Threat Vault 및 AutoFocus로 원활하게 전환하는 데 사용하는 포트입니다. |


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 23000 ~ 23999 | TCP, UDP 또는 SSL | Panorama와 Traps ESM 구성 요소 간의 Syslog 통신에 사용됩니다. |

## GlobalProtect에 사용되는 포트

GlobalProtect는 다음 포트를 사용합니다.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 443 | TCP | GlobalProtect 앱과 포털 또는 GlobalProtect 앱과 게이트웨이 간의 통신과 SSL 터널 연결에 사용됩니다.<br>GlobalProtect 게이트웨이는 또한 이 포트를 사용하여 GlobalProtect 앱에서 호스트 정보를 수집하고 호스트 정보 프로파일(HIP) 검사를 수행합니다. |
| 4501 | UDP | GlobalProtect 앱과 게이트웨이 간의 IPSec 터널 연결에 사용됩니다. |

루프백 인터페이스를 사용하여 다른 포트 및 주소에서 GlobalProtect에 대한 액세스를 제공하는 방법에 대한 팁은 GlobalProtect 포털 페이지를 모든 포트에서 액세스하도록 구성할 수 있습니까?를 참조하십시오.

## 사용자 ID에 사용되는 포트

User-ID는 사용자 IP 주소를 사용자명 및 그룹 구성원 자격에 매핑하여 사용자 또는 그룹 기반 정책과 네트워크의 사용자 활동에 대한 가시성을 가능하게 하는 기능입니다(예: 위협의 피해자가 될 수 있는 사용자를 신속하게 추적할 수 있음). 이 매핑을 수행하려면, 그룹 매핑 및 사용자 매핑을 수행하도록 네트워크에서 방화벽, User-ID 에이전트(Windows 기반 시스템에 설치되거나 방화벽에서 실행되는 PAN-OS 통합 에이전트) 및/또는 터미널 서버 에이전트가 디렉터리 서비스에 연결할 수 있어야 합니다. 또한 에이전트가 방화벽 외부의 시스템에서 실행 중인 경우 방화벽에 대한 사용자명 매핑에 IP 주소를 통신하기 위해 방화벽에 연결할 수 있어야 합니다. 다음 표에는 User-ID에 대한 통신 요구 사항과 연결을 설정하는 데 필요한 포트 번호가 나와 있습니다.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 389 | TCP | 방화벽이 LDAP 서버에 연결하는 데 사용하는 포트(일반 텍스트 또는 전송 레이어 보안 시작(TLS 시작)를 사용하여 사용자를 그룹에 매핑합니다. |
| 3268 | TCP | 방화벽이 Active Directory 글로벌 카탈로그 서버(일반 텍스트 또는 시작 TLS)에 연결하여 사용자를 그룹에 매핑하는 데 사용하는 포트입니다. |


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| 636 | TCP | 사용자를 그룹에 매핑하기 위해 LDAP 서버와의 SSL을 통한 LDAP 연결에 방화벽이 사용하는 포트입니다. |
| 3269 | TCP | 사용자를 그룹에 매핑하기 위해 Active Directory 글로벌 카탈로그 서버와의 SSL을 통한 LDAP 연결에 방화벽이 사용하는 포트입니다. |
| 514<br>6514 | TCP<br>UDP<br>SSL | 사용자 매핑을 위해 Syslog 보낸 사람을 모니터링하도록 User-ID를 구성한 경우 User-ID 에이전트가 인증 syslog 메시지를 수신하는 포트입니다. 포트는 에이전트 및 프로토콜 유형에 따라 다릅니다.<br>• PAN-OS 통합 User-ID 에이전트—SSL의 경우 포트 6514와 UDP용 포트 514입니다.<br>• Windows 기반 User-ID 에이전트—TCP 및 UDP 모두에 대한 포트 514입니다. |
| 5007 | TCP | 방화벽이 User-ID 또는 터미널 서버 에이전트에서 사용자 매핑 정보를 수신하는 포트입니다. 에이전트는 새 매핑이나 업데이트된 매핑을 인식할 때마다 타임스탬프와 함께 IP 주소 및 사용자명 매핑을 전송합니다. 또한 방화벽에 정기적으로 연결하여 알려진 매핑을 새로 고칩니다. |
| 5006 | TCP | User-ID 에이전트가 XML API 요청을 수신하는 포트입니다. 이 통신의 소스는 일반적으로 API를 호출하는 스크립트를 실행하는 시스템입니다. |
| 88 | UDP/TCP | User-ID 에이전트가 Kerberos 서버에 인증하는 데 사용하는 포트입니다. 방화벽은 먼저 UDP를 시도하고 TCP로 폴백합니다. |
| 1812 | UDP | User-ID 에이전트가 RADIUS 서버를 인증하는 데 사용하는 포트입니다. |
| 49 | TCP | User-ID 에이전트가 TACACS+ 서버에 인증하는 데 사용하는 포트입니다. |
| 135 | TCP | User-ID 에이전트가 Microsoft Remote Procedure Call(RPC) 엔드포인트 매퍼와의 TCP 기반 WMI 연결을 설정하는 데 사용하는 포트입니다. 그런 다음 엔드포인트 매퍼는 49152-65535 포트 범위에서 임의로 할당된 포트를 에이전트에 할당합니다. 에이전트는 이 연결을 사용하여 Exchange Server 또는 AD 서버 보안 로그, 세션 테이블에 대한 RPC 쿼리를 생성합니다. 터미널 서버에 액세스하는 데 사용되는 포트이기도 합니다.<br>또한 User-ID 에이전트는 이 포트를 사용하여 클라이언트 시스템에 연결하여 WMI(Windows 관리 계측) 프로빙을 수행합니다. |


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| 139 | TCP | User-ID 에이전트가 보안 로그 및 세션 정보에 대한 RPC 쿼리를 보낼 수 있도록 AD 서버에 TCP 기반 NetBIOS 연결을 설정하는 데 사용하는 포트입니다.<br>또한 User-ID 에이전트는 이 포트를 사용하여 NetBIOS 검색을 위해 클라이언트 시스템에 연결합니다(Windows 기반 User-ID 에이전트에서만 지원됨). |
| 445 | TCP | User-ID 에이전트가 사용자 로그온 정보(인쇄 스풀러 및 네트워크 로그온)에 액세스하기 위해 AD 서버에 TCP 기반 SMB 연결을 사용하여 AD(Active Directory)에 연결하는 데 사용하는 포트입니다. |
| 5985 | HTTP | User-ID 에이전트가 HTTP를 통한 WinRM 프로토콜로 보안 로그 및 세션 정보를 모니터링하는 데 사용하는 포트입니다. |
| 5986 | HTTPS | User-ID 에이전트가 HTTPS를 통해 WinRM 프로토콜을 사용하여 보안 로그 및 세션 정보를 모니터링하는 데 사용하는 포트입니다. |
| 5009 | TCP | 방화벽이 터미널 서버 에이전트에 연결하는 데 사용하는 포트입니다. |

## IPsec에 사용되는 포트

방화벽 및 Panorama는 IPSec 기능을 위해 다음 포트를 사용합니다.

| 대상 포트 | 프로토콜 | 설명 |
|---|---|---|
| 500 | UDP | 원격 IKE 피어와 연결하기 위해 Management Plane(MP)에서 IKE가 사용하는 포트입니다. |
| 4500 | UDP | 원격 IKE 피어와 연결하기 위해 Management Plane(MP)에서 IKE가 사용하는 포트입니다. |
| 4510 | UDP | 데이터 플레인에서 IKE에 요청을 보내는 데 사용하는 포트입니다. |
| 4511 | UDP | `keymgr`에 요청을 보내기 위해 데이터플레인에서 사용하는 포트입니다. |

## 라우팅에 사용되는 포트

방화벽과 Panorama는 라우팅 기능에 다음 포트를 사용합니다.


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 179 | TCP | BGP에서 피어를 연결하는 데 사용하는 포트입니다. |
| 3784<br>3785<br>4784 | UDP | BGP에서 피어를 연결하는 데 사용하는 포트입니다. |
| 520 | UDP | RIPv2에 사용되는 포트입니다. |
| 89 | IP | OSPF에 사용되는 포트입니다. |
| 103 | IP | PIM(프로토콜 독립 멀티캐스트)에 사용되는 포트입니다. |

## DHCP에 사용되는 포트

방화벽과 Panorama는 DHCP 기능을 위해 다음 포트를 사용합니다.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 67<br>68<br>546<br>547 | UDP | DHCP 서버 수신 포트로 사용되는 포트입니다. |

## 인프라에 사용되는 포트

방화벽과 Panorama는 인프라 기능을 위해 다음 포트를 사용합니다.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 111 | TCP/UDP | 포트 매퍼로 사용되는 포트입니다. |
| 23 | TCP/UDP | Telnet 애플리케이션 프로토콜에 사용되는 포트입니다. |
| 69 | TCP/UDP | TFTP에 사용되는 포트입니다. |
| 2049 | TCP/UDP | NFS(네트워크 파일 시스템)에 사용되는 포트입니다. |
| 28260 | TCP | 내부 프로세스를 위해 내부 sysd IPC 통신에 사용되는 포트입니다. |


©2023 Palo Alto Networks, Inc.

| 대상 포트 | 프로토콜 | 설명 |
| --- | --- | --- |
| 28261 | TCP | 내부 프로세스를 관리하기 위해 내부 masterd 애플리케이션에서 사용하는 포트입니다. |
| 동적 | TCP/UDP | NFS 작업에서 관리부의 호스트 데이터플레인 파일 시스템에 사용하는 동적 포트입니다. |


©2023 Palo Alto Networks, Inc.

# 방화벽을 출하시 기본 설정으로 재설정

방화벽을 공장 기본값으로 재설정하면 모든 구성 설정과 로그가 손실됩니다.

**STEP 1 |** 방화벽에 대한 콘솔 연결을 설정합니다.

1. 컴퓨터에서 콘솔 포트에 직렬 케이블을 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 방화벽에 연결합니다.

   컴퓨터에 *9*핀 직렬 포트가 없으면 *USB*-직렬 포트 커넥터를 사용하십시오.

2. 로그인 자격 증명을 입력합니다.
3. 다음 CLI 명령을 입력합니다.

   **디버그 시스템 유지 관리 모드**

   방화벽은 유지 관리 모드에서 재부팅됩니다.

**STEP 2 |** 시스템을 공장 기본 설정으로 재설정합니다.

1. 방화벽이 재부팅되면 **Enter** 키를 눌러 유지 관리 모드 메뉴로 이동합니다.
2. **공장 초기화**를 선택한 다음 **Enter** 키를 누릅니다.
3. **공장 초기화**를 선택한 다음 **Enter** 키를 다시 누릅니다.

   방화벽은 구성 설정 없이 재부팅됩니다. 방화벽에 로그인하기 위한 기본 사용자명과 암호는 admin/admin입니다.

   방화벽에서 초기 구성을 수행하고 네트워크 연결을 설정하려면 관리 네트워크에 방화벽 통합을 참조하십시오.


©2023 Palo Alto Networks, Inc.

# 방화벽 부트스트랩

부트스트래핑은 인터넷 액세스 여부와 관계없이 네트워크에서 작동하도록 방화벽을 구성하고 라이선스를 부여하는 프로세스를 가속화합니다. 부트스트랩을 사용하면 Panorama에 연결하고 전체 구성을 얻을 수 있도록 기본 구성 파일(init-cfg.txt)로 방화벽을 구성할지 또는 기본 구성 및 선택적 bootstrap.xml 파일로 방화벽을 완전히 구성할지 선택할 수 있습니다.

- USB 플래시 드라이브 지원
- 샘플 init-cfg.txt 파일
- 방화벽 부트스트래핑을 위한 USB 플래시 드라이브 준비
- USB 플래시 드라이브를 사용하여 방화벽 부트스트랩

## USB 플래시 드라이브 지원

하드웨어 기반 Palo Alto Networks 방화벽을 부트스트랩하는 USB 플래시 드라이브는 다음 중 하나를 지원해야 합니다.

- 파일 할당 테이블 32(FAT32)
- 세 번째 확장 파일 시스템(ext3)

방화벽은 USB2.0 또는 USB3.0 연결을 사용하는 다음 플래시 드라이브에서 부트스트랩할 수 있습니다.

| 지원되는 **USB** 플래시 드라이브 |
| --- |
| Kingston<br>• Kingston SE9 8GB (2.0)<br>• Kingston SE9 16GB (3.0)<br>• Kingston SE9 32GB (3.0) |
| SanDisk<br>• SanDisk Cruzer Fit CZ33 8GB (2.0)<br>• SanDisk Cruzer Fit CZ33 16GB (2.0)<br>• SanDisk Cruzer CZ36 16GB (2.0)<br>• SanDisk Cruzer CZ36 32GB (2.0)<br>• SanDisk Extreme CZ80 32GB (3.0) |
| Silicon Power<br>• Silicon Power Jewel 32GB (3.0)<br>• Silicon Power Blaze 16GB (3.0) |
| PNY |


©2023 Palo Alto Networks, Inc.

| 지원되는 **USB** 플래시 드라이브 |
| --- |
| • PNY Attache 16GB (2.0)<br>• PNY Turbo 32GB (3.0) |

## 샘플 init-cfg.txt 파일

부트스트랩 프로세스에는 init-cfg.txt 파일이 필요합니다. 이 파일은 텍스트 편집기를 사용하여 만드는 기본 구성 파일입니다. 이 파일을 생성하려면 5을 참조하십시오. 다음 샘플 init-cfg.txt 파일은 파일에서 지원되는 매개변수를 보여줍니다. 제공해야 하는 매개변수는 굵게 표시됩니다.

| 샘플 **init-cfg.txt**(고정 **IP** 주소) | 샘플 **init-cfg.txt**(**DHCP** 클라이언트) |
| --- | --- |
| **type=static ip-address=10.5.107.19 default-gateway=10.5.107.1 netmask=255.255.25**<br>**address=2001:400:f00::1/64 ipv6-default-gateway=2001:400:f00::2**<br>hostname=Ca-FW-DC1 panorama-server=10.5.107.20 panorama-server-2=10.5.107.21<br>tplname=FINANCE_TG4<br>dgname=finance_dg dns-primary=10.5.6.6 dns-secondary=10.5.6.7 op-command-modes=multi-vsys,jumbo-frame<br>dhcp-send-hostname=no dhcp-send-client-id=no dhcp-accept-server-hostname=no dhcp-accept-server-domain=no | **type=dhcp-client** ip-address=<br>default-gateway= netmask=<br>ipv6-address= ipv6-default-gateway= hostname=Ca-FW-DC1<br>panorama-server=10.5.107.20<br>panorama-server-2=10.5.107.21<br>tplname=FINANCE_TG4<br>dgname=finance_dg dns-primary=10.5.6.6 dns-secondary=10.5.6.7 op-command-modes=multi-vsys,jumbo-frame<br>dhcp-send-hostname=yes dhcp-send-client-id=yes dhcp-accept-server-hostname=yes<br>dhcp-accept-server-domain=yes |

다음 표에서는 init-cfg.txt 파일의 필드에 대해 설명합니다. 유형은 필수 항목입니다. 유형이 고정인 경우 IP 주소, 기본 게이트웨이 및 넷마스크가 필요하거나 IPv6 주소 및 IPv6 기본 게이트웨이가 필요합니다.

| 필드 | 설명 |
| --- | --- |
| 유형 | (필수) 관리 IP 주소 유형: 정적 또는 dhcp-client. |
| ip-address | (IPv4 고정 관리 주소에 필요) IPv4 주소입니다. 유형이 dhcp-client인 경우 방화벽은 이 필드를 무시합니다. |
| default-gateway | (IPv4 고정 관리 주소에 필요) 관리 인터페이스용 IPv4 기본 게이트웨이. 유형이 dhcp-client인 경우 방화벽은 이 필드를 무시합니다. |
| 넷마스크 | (IPv4 고정 관리 주소에 필요) IPv4 넷마스크. 유형이 dhcp-client인 경우 방화벽은 이 필드를 무시합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 | 설명 |
| --- | --- |
| ipv6-address | (IPv6 고정 관리 주소의 경우 필수) 관리 인터페이스의 IPv6 주소 및 / prefix 길이입니다. 유형이 dhcp-client인 경우 방화벽은 이 필드를 무시합니다. |
| ipv6-default-gateway | (IPv6 고정 관리 주소에 필요) 관리 인터페이스용 IPv6 기본 게이트웨이. 유형이 dhcp-client인 경우 방화벽은 이 필드를 무시합니다. |
| 호스트 이름 | (선택 사항) 방화벽의 호스트 이름입니다. |
| Panorama 서버 | (권장) 기본 Panorama 서버의 IPv4 또는 IPv6 주소. |
| panorama-server-2 | (선택 사항) 보조 Panorama 서버의 IPv4 또는 IPv6 주소. |
| tplname | (권장) Panorama 템플릿 이름. |
| dgname | (권장) Panorama 디바이스 그룹 이름. |
| dns-primary | (선택 사항) 기본 DNS 서버의 IPv4 또는 IPv6 주소입니다. |
| dns-secondary | (선택 사항) 보조 DNS 서버의 IPv4 또는 IPv6 주소입니다. |
| vm-auth-key | (VM 시리즈 방화벽만 해당) 가상 머신 인증 키. |
| op-command-modes | (선택 사항) multi-vsys, jumbo-frame 또는 둘 모두를 쉼표로 구분하여 입력합니다. 부트스트랩하는 동안 여러 가상 시스템 및 점보 프레임을 활성화합니다. |
| dhcp-send-hostname | (DHCP 클라이언트 유형만 해당) DHCP 서버는 yes 또는 no 값을 결정합니다. 그렇다면 방화벽은 호스트 이름을 DHCP 서버로 보냅니다. |
| dhcp-send-client-id | (DHCP 클라이언트 유형만 해당) DHCP 서버는 yes 또는 no 값을 결정합니다. 그렇다면 방화벽은 클라이언트 ID를 DHCP 서버로 보냅니다. |
| dhcp-accept-server-hostname | (DHCP 클라이언트 유형만 해당) DHCP 서버는 yes 또는 no 값을 결정합니다. 그렇다면 방화벽은 DHCP 서버에서 호스트 이름을 수락합니다. |
| dhcp-accept-server-domain | (DHCP 클라이언트 유형만 해당) DHCP 서버는 yes 또는 no 값을 결정합니다. 그렇다면 방화벽은 DHCP 서버에서 DNS 서버를 수락합니다. |

## 방화벽 부트스트래핑을 위한 USB 플래시 드라이브 준비

USB 플래시 드라이브를 사용하여 물리적 방화벽을 부트스트랩할 수 있습니다. 그러나 이렇게 하려면 PAN-OS 7.1.0 이상 이미지를 실행하고 방화벽을 공장 기본 설정으로 재설정해야 합니다. 보안상의 이유로 방화벽이 공장 기본 상태이거나 모든 개인 데이터가 삭제된 경우에만 부트스트랩할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 주문 이행 이메일에서 지원 구독에 대한 일련번호(S/N) 및 인증 코드를 받으십시오.

**STEP 2 |** 고객 지원 포털에서 새 방화벽의 S/N을 등록합니다.

1. support.paloaltonetworks.com으로 이동하여 로그인하고 자산 > 기기 > 새 기기 등록 > 일련 번호 또는 인증 코드를 사용하여 기기 등록을 선택합니다.
2. 방화벽 등록 단계를 따릅니다.
3. 제출을 클릭합니다.

**STEP 3 |** 라이선스 키를 생성하는 고객 지원 포털에서 인증 코드를 활성화합니다.

1. support.paloaltonetworks.com으로 이동하여 로그인하고 왼쪽 탐색 창에서 **Assets** > **Devices**를 선택합니다.
2. 방금 등록한 각 기기 S/N에 대해 작업 링크(연필 아이콘)를 클릭합니다.
3. 라이선스 활성화에서 인증 코드 활성화를 선택합니다.
4. 인증 코드를 입력하고 동의 및 제출을 클릭합니다.

**STEP 4 |** Panorama에서 S/N을 추가합니다.

Panorama 관리자 안내서의 관리 디바이스로 방화벽 추가의 1단계를 완료하십시오.

**STEP 5 |** init-cfg.txt 파일을 생성합니다.

부트스트랩 매개변수를 제공하는 필수 파일인 init-cfg.txt 파일을 생성합니다. 필드는 샘플 init-cfg.txt 파일에 설명되어 있습니다.



***init-cfg.txt*** 파일이 없으면 부트스트랩 프로세스가 실패하고 방화벽은 일반 부팅 순서의 기본 구성으로 부팅됩니다.

각 필드의 키와 값 사이에는 공백이 없습니다. 관리 서버 측에서 구문 분석하는 동안 오류가 발생하므로 공백을 추가하지 마십시오.

파일 이름 앞에 S/N을 추가하여 여러 init-cfg.txt 파일(다른 원격 사이트에 대해 각각 하나씩)을 가질 수 있습니다. 예:

0008C200105-init-cfg.txt

0008C200107-init-cfg.txt

추가된 파일 이름이 없으면 방화벽은 init-cfg.txt 파일을 사용하고 부트스트랩을 진행합니다.

**STEP 6 |** (선택 사항) bootstrap.xml 파일을 생성합니다.

선택적 bootstrap.xml 파일은 기존 프로덕션 방화벽에서 내보낼 수 있는 완전한 방화벽 구성입니다.

1. 기기 > 설정 > 작업 > 이름이 지정된 구성 스냅샷 내보내기를 선택합니다.
2. 저장된 구성 또는 실행 중인 구성의 이름을 선택합니다.
3. 확인을 클릭합니다.
4. 파일 이름을 **`bootstrap.xml`**로 바꿉니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 고객 지원 포털에서 부트스트랩 번들을 생성하고 다운로드합니다.

물리적 방화벽의 경우 부트스트랩 번들은 /license 및 /config 디렉토리만 필요합니다.

다음 방법 중 하나를 사용하여 부트스트랩 번들을 생성하고 다운로드합니다.

- 방법 **1**을 사용하여 원격 사이트에 특정한 부트스트랩 번들을 생성합니다(init-cfg.txt 파일이 하나만 있음).
- 방법 **2**를 사용하여 여러 사이트에 대해 하나의 부트스트랩 번들을 생성합니다.

방법 **1**

1. 로컬 시스템에서 support.paloaltonetworks.com으로 이동하여 로그인합니다.
2. 자산을 선택합니다.
3. 부트스트랩하려는 방화벽의 S/N을 선택합니다.
4. 부트스트랩 컨테이너를 선택합니다.
5. 선택을 클릭합니다.
6. 생성한 init-cfg.txt 파일을 업로드하고 엽니다.
7. (선택 사항) 생성한 bootstrap.xml 파일과 파일 업로드를 선택합니다.

   동일한 모델 및 *PAN-OS* 버전의 방화벽에서 *bootstrap.xml* 파일을 사용해야 합니다.
8. 부트스트랩 컨테이너 다운로드를 선택하여 **bootstrap_<S/N>_<date>.tar.gz**라는 tar.gz 파일을 로컬 시스템에 다운로드합니다. 이 부트스트랩 컨테이너에는 방화벽의 S/N과 연결된 라이센스 키가 포함되어 있습니다.

방법 **2**

두 개의 최상위 디렉토리인 /license 및 /config가 있는 로컬 시스템에 tar.gz 파일을 생성합니다. 파일 이름 앞에 S/N이 추가된 모든 라이선스와 모든 init-cfg.txt 파일을 포함합니다.

고객 지원 포털에서 다운로드한 라이선스 키 파일은 라이선스 파일 이름에 S/N이 있습니다. PAN-OS는 부트스트랩 프로세스를 수행하는 동안 방화벽 S/N에 대해 파일 이름의 S/N을 확인합니다.

**STEP 8 |** SCP(Secure Copy) 또는 TFTP를 사용하여 생성한 tar.gz 파일을(PAN-OS 7.1.0 이상 이미지를 실행하는 방화벽으로) 가져옵니다.

CLI에 액세스하고 다음 명령 중 하나를 입력합니다.

- **<host IP address>에서 tftp 가져오기 부트스트랩 번들 파일 <path and filename>**

  예:

  **tftp import bootstrap-bundle file /home/userx/bootstrap/devices/pa5000.tar.gz from 10.1.2.3**
- **scp import bootstrap-bundle from <<user>@<host>:<path to file>>**

  예:

  **scp import bootstrap-bundle from userx@10.1.2.3:/home/userx/bootstrap/devices/pa200_bootstrap_bundle.tar.gz**


©2023 Palo Alto Networks, Inc.

**STEP 9 |** USB 플래시 드라이브를 준비합니다.

1. 이전 단계에서 사용한 방화벽에 USB 플래시 드라이브를 삽입합니다.
2. "**pa5000.tar.gz**" 대신 tar.gz 파일 이름을 사용하여 다음 CLI 작동 명령을 입력합니다. 이 명령은 USB 플래시 드라이브를 포맷하고 파일의 압축을 풀고 USB 플래시 드라이브의 유효성을 검사합니다.

   ```
   request system bootstrap-usb prepare from pa5000.tar.gz
   ```
3. 계속하려면 **y**를 누르십시오. USB 드라이브가 준비되면 다음 메시지가 표시됩니다.

   ```
   USB 준비가 성공적으로 완료되었습니다.
   ```
4. 방화벽에서 USB 플래시 드라이브를 제거합니다.
5. 필요한 만큼 USB 플래시 드라이브를 준비할 수 있습니다.

**STEP 10 |** USB 플래시 드라이브를 원격 사이트로 포워딩합니다.

방법 2를 사용하여 부트스트랩 번들을 만든 경우 동일한 USB 플래시 드라이브 콘텐츠를 여러 원격 사이트에서 방화벽 부트스트랩에 사용할 수 있습니다. 콘텐츠를 여러 USB 플래시 드라이브 또는 여러 번 사용되는 단일 USB 플래시 드라이브로 번역할 수 있습니다.

## USB 플래시 드라이브를 사용하여 방화벽 부트스트랩

신규 Palo Alto Networks 방화벽과 부트스트랩 파일이 로드된 USB 플래시 드라이브를 받은 후 방화벽을 부트스트랩할 수 있습니다.

*Microsoft Windows* 및 *Apple Mac* 운영 체제는 드라이브가 *ext4* 파일 시스템을 사용하여 포맷되었기 때문에 부트스트랩 *USB* 플래시 드라이브를 읽을 수 없습니다. *USB* 드라이브를 읽으려면 타사 소프트웨어를 설치하거나 *Linux* 시스템을 사용해야 합니다.

**STEP 1 |** 방화벽은 공장 기본 상태이거나 모든 개인 데이터가 삭제되어 있어야 합니다.

**STEP 2 |** 회사 본사와의 연결을 보장하려면 이더넷 케이블을 사용하여 MGT(관리 인터페이스)를 다음 중 하나에 연결하여 방화벽 케이블을 연결합니다.

- 업스트림 모뎀
- 스위치 또는 라우터의 포트
- 벽면의 이더넷 잭

**STEP 3 |** USB 플래시 드라이브를 방화벽의 USB 포트에 삽입하고 방화벽의 전원을 켭니다. 출하 시 기본 방화벽 부트스트랩은 USB 플래시 드라이브에서 자체적으로 실행됩니다.

방화벽이 구성되면 방화벽 상태 표시등이 노란색에서 녹색으로 바뀝니다. 자동 커밋이 성공했습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 부트스트랩 완료를 확인합니다. 부트스트랩 동안 콘솔에서 기본 상태 로그를 볼 수 있으며 프로세스가 완료되었는지 확인할 수 있습니다.

1. init-cfg.txt 파일에 Panorama 값(panorama-server, tplname 및 dgname)을 포함했다면 Panorama 관리 디바이스, 디바이스 그룹 및 템플릿 이름을 확인하십시오.
2. 웹 인터페이스에 액세스하고 대시보드 > 위젯 > 시스템을 선택하거나 CLI 작동 명령 **show system info** 및 **show config running** 사용하여 일반 시스템 설정 및 구성을 확인합니다.
3. 디바이스 > 라이선스를 선택하거나 CLI 작동 명령 **request license info**를 사용하여 라이선스 설치를 확인합니다.
4. Panorama가 구성된 경우 Panorama에서 콘텐츠 버전 및 소프트웨어 버전을 관리합니다. Panorama가 구성되지 않은 경우 웹 인터페이스를 사용하여 콘텐츠 버전 및 소프트웨어 버전을 관리합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** (Panorama 관리 방화벽만 해당) 디바이스 등록 인증 키를 만들어 방화벽에 추가합니다.

이는 Panorama 관리에 부트스트랩된 방화벽을 성공적으로 추가하는 데 필요합니다. 디바이스 등록 인증 키의 수명은 한정되어 있으며 init-cfg.txt 파일에 디바이스 등록 인증 키를 포함하는 것은 지원되지 않습니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
3. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 키 수명을 지정하여 인증 키를 사용하여 새 방화벽을 온보딩할 수 있는 기간을 제한합니다.
   - 개수 - 인증 키를 사용하여 새 방화벽을 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 이 인증 키가 방화벽만 인증하는 데 사용되도록 지정합니다.

     모두를 선택하여 디바이스 등록 인증 키를 사용하여 방화벽, 로그 수집기 및 *WildFire* 어플라이언스를 온보딩할 수 있습니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 방화벽을 지정하기 위해 하나 이상의 디바이스 일련 번호를 입력합니다.
4. 확인을 클릭합니다.

   메시지가 표시되면 인증 키 복사 및 닫기를 수행합니다.
5. 방화벽 웹 인터페이스에 로그인합니다.

   방화벽 CLI에 로그인하여 디바이스 등록 인증 키를 추가할 수도 있습니다.

   ```
   admin> request authkey set <auth key>
   ```
6. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
7. 이전 단계에서 복사한 디바이스 등록 인증 키를 붙여넣고 확인을 클릭합니다.
8. 커밋합니다.
9. Panorama 웹 인터페이스 에 로그인하고 **Panorama** > 관리형 디바이스 > 요약을 선택하여 방화벽이 Panorama에 **연결되어** 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# 디바이스 원격 측정

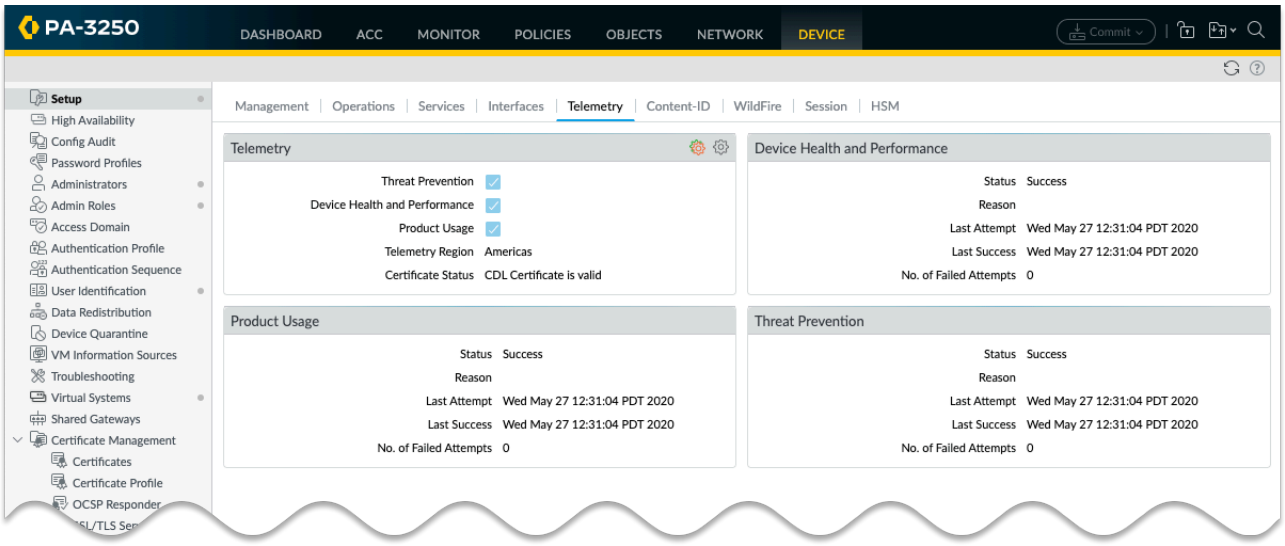
디바이스 원격 분석은 차세대 방화벽 또는 Panorama에 대한 데이터를 수집하고 Cortex Data Lake에 데이터를 업로드하여 Palo Alto Networks와 공유합니다. 이 데이터는 원격 분석 앱을 구동하고 위협 인텔리전스를 공유하는 데 사용됩니다.


- 디바이스 원격 분석 개요
- 디바이스 원격 분석 수집 및 전송 간격
- 디바이스 원격 분석 관리
- 디바이스 원격 분석 모니터링
- 디바이스 원격 분석에서 수집하는 데이터 샘플링

# 디바이스 원격 분석 개요

디바이스 원격 측정은 차세대 방화벽 또는 Panorama에 대한 데이터를 수집하고 데이터를 Cortex Data Lake에 업로드하여 Palo Alto Networks와 공유합니다. 이 데이터는 차세대 방화벽 및 Panorama를 쉽게 모니터링하고 관리할 수 있는 클라우드 기반 애플리케이션인 원격 측정 앱을 구동하는 데 사용됩니다. 이러한 앱은 디바이스 상태, 성능, 용량 계획 및 구성에 대한 가시성을 향상시킵니다. 이러한 앱을 통해 Palo Alto Networks가 제공하는 제품과 서비스에서 누리는 혜택을 극대화할 수 있습니다.

원격 측정 데이터는 위협 인텔리전스를 공유하는 데도 사용되며, 향상된 침입 방지, 보안 서명 평가는 물론 PAN-DB URL 필터링, DNS 기반 명령 및 제어(C2) 서명 및 WildFire 내에서 향상된 멀웨어 탐지 기능을 제공합니다.




원격 측정 데이터는 제한된 기간 동안 디바이스에 로컬로 수집 및 저장됩니다. 이 데이터는 데이터의 대상 지역을 구성한 경우에만 Palo Alto Networks와 공유됩니다. 조직에 Cortex Data Lake 라이선스가 있는 경우 Cortex Data Lake 인스턴스가 있는 동일한 지역으로만 데이터를 보낼 수 있습니다. 조직에 Cortex Data Lake 라이선스가 없는 경우 이 데이터를 공유하려면 디바이스 인증서를 설치해야 합니다. 이 경우 개인 정보 및 데이터 저장에 관한 모든 해당 지역 법률을 준수해야 하지만 사용 가능한 지역을 선택할 수 있습니다.

원격 측정 데이터는 사전 정의된 수집 인터벌로 수집되고 Palo Alto Networks와 공유됩니다. 데이터 카테고리를 활성화/비활성화하여 데이터 수집 및 공유 여부를 제어할 수 있습니다. 데이터 수집 및 전송의 현재 상태를 모니터링할 수도 있습니다.

마지막으로 방화벽이 원격 분석 목적으로 수집하는 데이터의 라이브 샘플을 얻을 수 있습니다. 각 메트릭에 대한 개인 정보 보호를 포함하여 Palo Alto Networks와 공유할 수 있는 모든 원격 측정 메트릭에 대한 전체 설명은 PAN-OS Device Telemetry Metrics Reference Guide를 참조하십시오.

원격 분석이 활성화되어 있는 동안 자동으로 생성된 사용자 ***_cliadmin***이 대시보드의 ***Logged in Admins*** 아래에 나타날 수 있습니다. 이 사용자는 원격 분석 수집을 위해서만 만들어집니다.


©2023 Palo Alto Networks, Inc.

# 디바이스 원격 분석 수집 및 전송 간격

PAN-OS는 고정된 인터벌으로 원격 측정 데이터를 수집하고 전송합니다. 컬렉션은 메트릭별로 정의되며 다음 중 하나일 수 있습니다.

- 20분마다.
- 매시간마다.
- 매일

원격 분석은 데이터 번들로 수집됩니다. 각 번들은 데이터 전송 시점까지 수집된 모든 데이터의 집합체입니다. 이러한 번들은 1시간마다 한 번씩 발생하는 전송 이벤트까지 디바이스에 저장됩니다. 번들이 Palo Alto Networks로 성공적으로 전송되면 디바이스에서 삭제됩니다.

Palo Alto Networks에 번들을 보내는 동안 오류가 발생하면 방화벽은 10분을 기다린 후 다시 시도합니다. 방화벽은 성공할 때까지 또는 새 원격 측정 데이터를 수집하기 위한 저장 공간이 필요할 때까지 계속해서 번들을 보내려고 시도합니다.

정기적인 전송 인터벌마다 방화벽은 해당 이벤트에 대해 예약된 번들을 보내는 것으로 시작합니다. 이러한 번들을 성공적으로 전송한 후 방화벽은 이전 전송 이벤트에서 저장했을 수 있는 실패한 번들을 보냅니다.


©2023 Palo Alto Networks, Inc.

# 디바이스 원격 분석 관리

디바이스 원격 분석을 관리하려면 다음을 수행할 수 있습니다.

- 디바이스 원격 분석 사용
- 디바이스 원격 분석 비활성화
- 디바이스 원격 분석에서 수집하는 데이터 관리
- 기록 디바이스 원격 분석 관리

## 디바이스 원격 분석 사용

기본적으로 어플라이언스는 Palo Alto Networks와 데이터를 공유하지 않습니다. 공유가 활성화된 경우 다음을 수행하여 모든 디바이스 원격 측정 공유를 중지할 수 있습니다. **Device** > **Setup** > **Telemetry**, **Enable Telemetry** 체크박스의 선택을 취소한 다음 변경 사항을 커밋합니다.

데이터가 Palo Alto Networks와 공유되도록 Device Telemetry를 활성화하려면:

**STEP 1 |** Cortex Data Lake를 활성화합니다.

1. 조직에 Cortex Data Lake 라이선스가 없는 경우 디바이스에 아직 디바이스 인증서가 설치되어 있지 않으면 디바이스 인증서를 설치하십시오.

   조직에 Cortex Data Lake 라이선스가 있는 경우 활성화되어 있는지 확인하십시오.
2. 방화벽이 Cortex Data Lake에 데이터를 보낼 수 있도록 네트워크가 올바르게 구성되어 있는지 확인하십시오.

**STEP 2 |** 디바이스 > 설정 > 원격 측정으로 이동

**STEP 3 |** 원격 측정 위젯을 편집합니다.

**STEP 4 |** 원격 분석 대상에서 지역을 선택합니다. 조직에서 Cortex Data Lake를 사용하는 경우 Cortex Data Lake가 사용하도록 구성된 지역을 사용해야 합니다.

**STEP 5 |** 확인을 클릭한 다음 변경 사항을 커밋합니다.

## 디바이스 원격 분석 비활성화

차세대 방화벽이 Palo Alto Networks와 데이터를 공유하도록 구성된 경우 다음을 통해 이 공유를 비활성화할 수 있습니다.

**STEP 1 |** 디바이스 > 설정 > 원격 측정으로 이동

**STEP 2 |** 원격 측정 위젯을 편집합니다.

**STEP 3 |** 원격 분석 활성화 체크박스를 선택 취소합니다.

**STEP 4 |** 확인을 클릭한 다음 변경 사항을 커밋합니다.

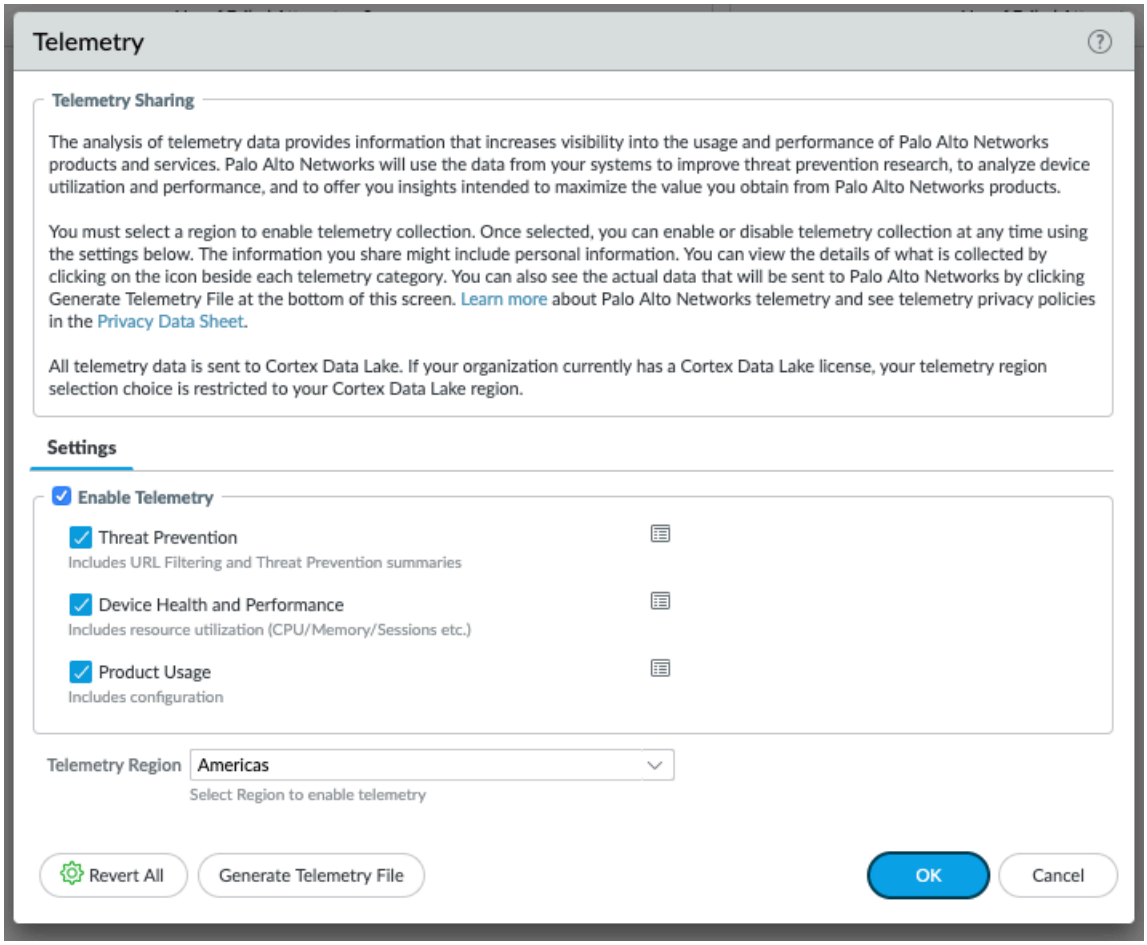
**STEP 5 |** 현재 Cortex Data Lake에 저장된 모든 원격 측정 데이터는 방화벽이 업로드한 후 1년이 지나면 자동으로 제거됩니다. 선택적으로 원격 측정을 비활성화한 후 이 시간 동안 데이터가 Cortex Data


©2023 Palo Alto Networks, Inc.

Lake에 상주하지 않도록 하려면 지원 티켓을 열고 Palo Alto Networks에 원격 측정 데이터를 제거하도록 요청하십시오.

## 디바이스 원격 분석에서 수집하는 데이터 관리

디바이스 > 설정 > 원격 분석을 선택하여 현재 수집된 원격 분석 카테고리를 확인합니다. 이러한 카테고리를 변경하려면 원격 분석 위젯을 편집합니다. 방화벽에서 수집하지 않을 카테고리를 선택 취소하고 확인을 수행한 다음 변경 사항을 커밋합니다.




모든 디바이스 원격 분석 공유를 중지하려면 원격 분석 사용 상자의 선택을 취소한 다음 변경 사항을 커밋합니다.

## 기록 디바이스 원격 분석 관리

PAN-OS 10.2 릴리스에 대해 디바이스 원격 분석이 크게 변경되었습니다. 10.0 이전에는 원격 분석 데이터가 주로 위협 인텔리전스를 위해 관심을 보였습니다. 10.0 현재 위협 인텔리전스 메트릭은 여전히 디바이스에서 수집한 데이터의 큰 부분을 차지하지만 디바이스의 상태, 성능 및 구성과 관련된 훨씬 더 많은 데이터가 수집됩니다.

즉, PAN-OS 10.2 디바이스 원격 측정은 이전 릴리스에 대해 수집된 데이터를 확장합니다. 또한 PAN-OS 10.2는 이전 릴리스와 다른 클라우드 위치로 원격 분석 데이터를 보냅니다. 그러나 PAN-OS 10.0을 실행


©2023 Palo Alto Networks, Inc.

하는 차세대 방화벽에 대한 기록 원격 분석 지원은 여전히 존재합니다. 유일한 차이점은 10.2 디바이스 원격 분석 사용자 인터페이스가 이 기록 데이터 수집을 관리할 수 없다는 것입니다.

기존 차세대 방화벽이 있고 기록 원격 분석 데이터 카테고리가 활성화된 경우 PAN-OS 10.2로 업그레이드하면 방화벽이 이 정보를 계속 수집하고 공유합니다. 이 원격 분석 데이터 공유를 해제하려면 다음 CLI 명령을 사용합니다.

```
set deviceconfig system update-schedule statistics-service
 application-reports no set deviceconfig system update-schedule
 statistics-service threat-prevention-reports no set deviceconfig
 system update-schedule statistics-service threat-prevention-
information no set deviceconfig system update-schedule statistics-
service threat-prevention-pcap no set deviceconfig system
 update-schedule statistics-service passive-dns-monitoring no set
 deviceconfig system update-schedule statistics-service url-reports
 no set deviceconfig system update-schedule statistics-service
 health-performance-reports no set deviceconfig system update-
schedule statistics-service file-identification-reports no
```

10.2 방화벽이 있고 이 원격 분석 공유가 꺼져 있지만 Palo Alto Networks와 이 데이터를 공유하려는 경우 다음을 사용하여 설정할 수 있습니다.

```
set deviceconfig system update-schedule statistics-service
 application-reports yes set deviceconfig system update-schedule
 statistics-service threat-prevention-reports yes set deviceconfig
 system update-schedule statistics-service threat-prevention-
information yes set deviceconfig system update-schedule statistics-
service threat-prevention-pcap yes set deviceconfig system
 update-schedule statistics-service passive-dns-monitoring yes set
 deviceconfig system update-schedule statistics-service url-reports
 yes set deviceconfig system update-schedule statistics-service
 health-performance-reports yes set deviceconfig system update-
schedule statistics-service file-identification-reports yes
```

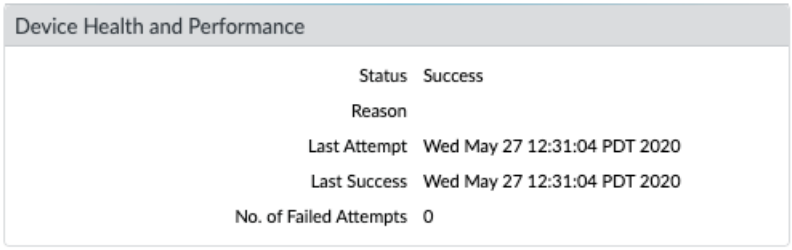
어플라이언스가 다음 CLI 명령을 사용하여 이 기록 원격 분석 데이터를 수집하고 공유하는지 확인할 수 있습니다.

```
show deviceconfig system update-schedule statistics-service
```


©2023 Palo Alto Networks, Inc.

# 디바이스 원격 분석 모니터링

PAN-OS는 각 원격 측정 카테고리에 대한 공유 상태를 보여줍니다. 각 메트릭 카테고리에 대한 위젯은 **Device** > **Setup** > **Telemetry**에서 사용할 수 있습니다.



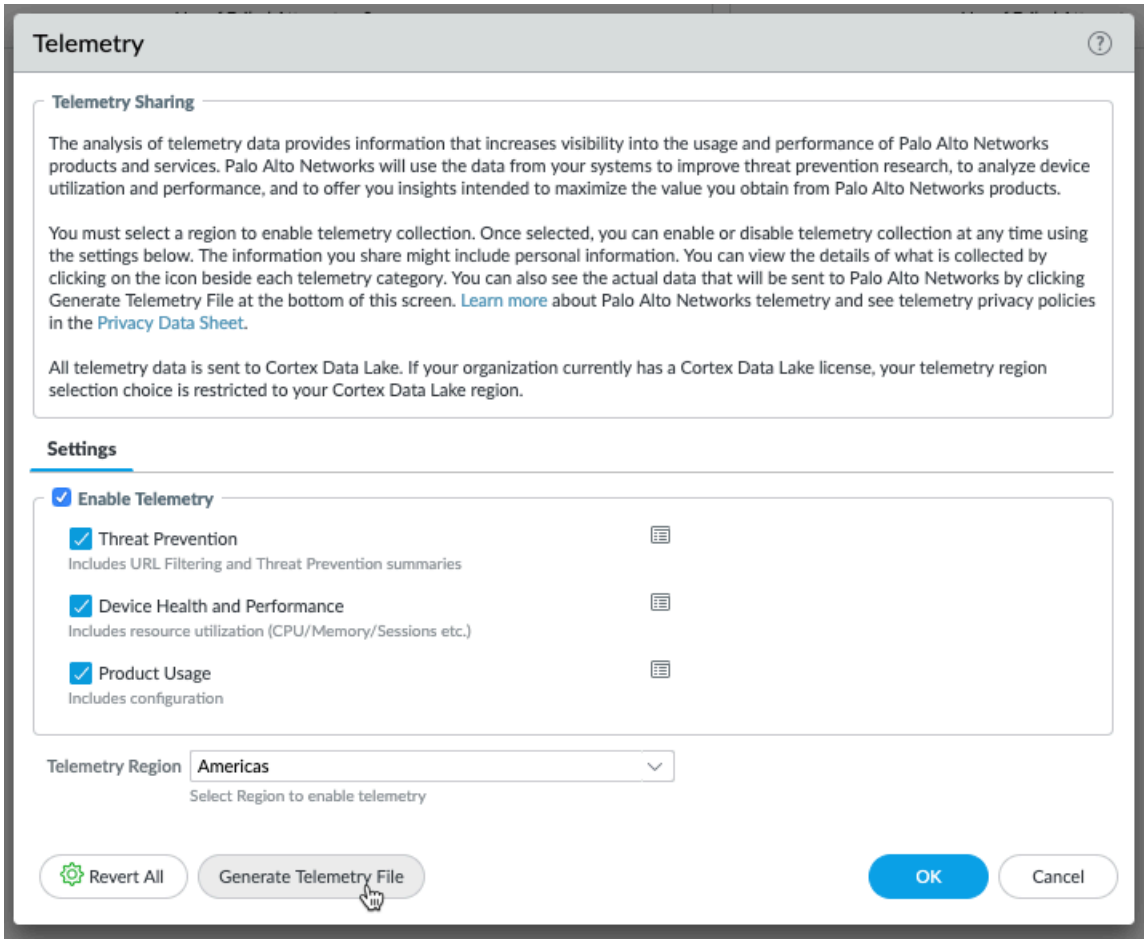

오류가 발생하면 디바이스는 다음 전송 시간에 전송 시도를 다시 시도합니다. 문제가 지속되면 디바이스가 Cortex Data Lake에 데이터를 보내도록 올바르게 구성되어 있는지 확인하십시오.

- 조직에 Cortex Data Lake 라이선스가 있는 경우 Cortex Data Lake 라이선스가 활성화되었고 방화벽이 Cortex Data Lake를 사용하도록 구성되었는지 확인합니다.
- 조직에 Cortex Data Lake 라이선스가 없는 경우 디바이스 인증서를 설치했는지 확인하고 네트워크가 Cortex Data Lake에 대한 트래픽을 허용하도록 구성되어 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# 디바이스 원격 분석에서 수집하는 데이터 샘플링

디바이스 원격 측정이 Palo Alto Networks와 수집하고 공유하는 데이터의 라이브 예제를 다운로드할 수 있습니다. 이렇게 하려면 디바이스 > 설정 > 원격 분석으로, 이동하여 원격 분석 위젯을 편집합니다. 그런 다음 원격 분석 파일 생성을 클릭합니다.




데이터 수집은 방화벽의 속도에 따라 몇 분 정도 소요됩니다. 프로세스가 완료되면 디바이스 원격 분석 데이터 다운로드를 클릭합니다. 원격 분석 번들은 압축된 타르 볼이며 기본 브라우저 다운로드 디렉토리에 배치됩니다.

디바이스 원격 분석이 Palo Alto Networks와 수집하고 공유하는 모든 메트릭에 대한 설명은 PAN-OS 디바이스 원격 분석 메트릭 참조 가이드를 참조하십시오.


©2023 Palo Alto Networks, Inc.

# 인증

인증은 합법적인 사용자만 액세스할 수 있도록 사용자의 ID를 확인하여 서비스 및 애플리케이션을 보호하는 방법입니다. 여러 방화벽과 Panorama 기능에는 인증이 필요합니다. 관리자는 방화벽과 Panorama의 웹 인터페이스, CLI 또는 XML API에 액세스하도록 인증합니다. 최종 사용자는 인증 포털 또는 GlobalProtect를 통해 인증하여 다양한 서비스 및 애플리케이션에 액세스합니다. 네트워크를 보호하고 기존 보안 인프라를 수용하는 동시에 원활한 사용자 환경을 보장하기 위해 여러 인증 서비스 중에서 선택할 수 있습니다.

공용 키 인프라가 있는 경우 사용자가 로그인 문제에 수동형으로 응답하지 않고도 인증을 사용하도록 인증서를 배포할 수 있습니다(인증서 관리 참조). 또는 인증서 외에도 사용자가 하나 이상의 방법을 사용하여 인증해야 하는 대화형 인증을 구현할 수 있습니다. 다음 항목은 다양한 유형의 대화형 인증을 구현, 테스트 및 문제 해결하는 방법을 설명합니다.

- 인증 유형
- 인증 배포 계획
- 다단계 인증 구성
- SAML 인증 구성
- Kerberos Single Sign-On(SSO) 구성
- Kerberos 서버 인증 구성
- TACACS+ 인증 구성
- RADIUS 인증 구성
- LDAP 인증 구성
- 인증 서버에 대한 연결 시간 제한
- 로컬 데이터베이스 인증 구성
- 인증 프로파일 및 시퀀스 구성
- 인증 서버 연결 테스트
- 인증 정책
- 인증 문제 해결

# 인증 유형

- 외부 인증 서비스
- 다단계 인증
- SAML
- Kerberos
- TACACS+
- RADIUS
- LDAP
- 로컬 인증

## 외부 인증 서비스

방화벽과 Panorama는 외부 서버를 사용하여 웹 인터페이스에 대한 관리 액세스를 제어하고 인증 포털 및 GlobalProtect를 통해 서비스 또는 애플리케이션에 대한 최종 사용자 액세스를 제어할 수 있습니다. 이 컨텍스트에서 서비스가 네트워크에 대해 내부(예: Kerberos) 또는 외부(예: SAML ID 공급자)인지의 여부와 관계없이 방화벽 또는 Panorama에 로컬이 아닌 인증 서비스는 외부로 간주됩니다. 방화벽과 Panorama가 통합할 수 있는 서버 유형에는 Multi-Factor Authentication(MFA), SAML, Kerberos, TACACS+, RADIUS 및 LDAP가 있습니다. 방화벽 및 Panorama가 지원하는 로컬 인증 서비스를 사용할 수도 있지만 일반적으로 다음을 제공하는 외부 서비스가 더 좋습니다.

- 외부 ID 저장소의 모든 사용자 계정을 중앙에서 관리합니다. 지원되는 모든 외부 서비스는 최종 사용자와 관리자에게 이 옵션을 제공합니다.
- 계정 권한 부여의 중앙 관리(역할 및 액세스 도메인 할당). SAML, TACACS+ 및 RADIUS는 관리자를 위해 이 옵션을 지원합니다.
- 사용자가 여러 서비스 및 애플리케이션에 액세스하기 위해 한 번만 인증할 수 있는 SSO(Single Sign-On). SAML 및 Kerberos는 SSO를 지원합니다.
- 민감한 서비스와 애플리케이션을 보호하기 위한 다양한 유형(요소)의 여러 인증 문제. MFA 서비스는 이 옵션을 지원합니다.

외부 서비스를 통한 인증에는 방화벽이 서비스에 연결하는 방법을 정의하는 서버 프로파일이 필요합니다. 각 애플리케이션 및 사용자 집합에 대해 사용자 지정하는 설정을 정의하는 인증 프로파일에 서버 프로파일을 할당합니다. 예를 들어, 웹 인터페이스에 액세스하는 관리자에 대해 하나의 인증 프로파일을 구성하고 GlobalProtect 포털에 액세스하는 최종 사용자에 대해 다른 프로파일을 구성할 수 있습니다. 자세한 내용은 인증 프로파일 및 시퀀스 구성을 참조하십시오.

## 다단계 인증

MFA(다단계 인증)를 구성하여 각 사용자가 매우 민감한 서비스 및 애플리케이션에 액세스할 때 여러 메서드(요인)를 사용하여 인증할 수 있습니다. 예를 들어 사용자가 로그인 암호를 입력한 다음 중요한 재무 문서에 액세스하기 전에 전화로 받는 확인 코드를 입력하도록 강제할 수 있습니다. 이 방법을 사용하면 공격자가 암호를 훔치는 것만으로 네트워크의 모든 서비스와 애플리케이션에 액세스하지 못하도록 하는 데 도움이 됩니다. 물론 모든 서비스 및 애플리케이션에 동일한 수준의 보호가 필요한 것은 아니며 사용자가 자


©2023 Palo Alto Networks, Inc.

주 액세스하는 덜 민감한 서비스 및 애플리케이션에는 MFA가 필요하지 않을 수 있습니다. 다양한 보안 요구 사항을 수용하기 위해 특정 서비스, 애플리케이션 및 최종 사용자를 기반으로 MFA 또는 단일 인증 요소(예: 로그인 자격 증명 또는 인증서)를 트리거하는 인증 정책 규칙을 구성할 수 있습니다.

적용할 인증 요소 수와 유형을 선택할 때 정책 평가가 사용자 경험에 미치는 영향을 이해하는 것이 중요합니다. 사용자가 서비스 또는 애플리케이션을 요청하면 방화벽이 먼저 인증 정책을 평가합니다. 요청이 인증 정책 규칙과 MFA 사용 가능과 일치하는 경우 방화벽에는 인증 포털 웹 양식이 표시되므로 사용자가 첫 번째 요소를 인증할 수 있습니다. 인증이 성공하면 방화벽에 각 추가 요소에 대한 MFA 로그인 페이지가 표시됩니다. 일부 MFA 서비스는 사용자에게 2~4개의 요소를 선택하라는 메시지를 표시하므로 일부 요소를 사용할 수 없는 경우에 유용합니다. 모든 요인에 대해 인증이 성공하면 방화벽은 요청된 서비스 또는 애플리케이션에 대한 보안 정책을 평가합니다.



사용자 워크플로우를 방해하는 인증 과제의 빈도를 줄이려면 Kerberos 또는 SAML ***Single Sign-On(SSO)*** 인증을 사용하도록 첫 번째 요소를 구성합니다.

***GlobalProtect***에 대한 ***MFA***를 구현하려면 다단계 인증 알림을 용이하게 하기 위해 GlobalProtect 구성을 참조하십시오.

인증 시퀀스에서는 ***MFA*** 인증 프로파일을 사용할 수 없습니다.

인증 정책을 통한 최종 사용자 인증의 경우 방화벽은 여러 MFA 플랫폼(Duo v2, Okta Adaptive, PingID 및 RSA SecurID)과 직접 통합할 뿐만 아니라 다른 모든 MFA 플랫폼에 대한 RADIUS 또는 SAML을 통합합니다. GlobalProtect 포털 및 게이트웨이에 대한 원격 사용자 인증및 Panorama 및 PAN-OS 웹 인터페이스에 대한 관리자 인증을 위해 방화벽은 RADIUS 및 SAML만 사용하는 MFA 공급업체와 통합됩니다.

방화벽은 다음과 같은 MFA 요소를 지원합니다.

| 요소 | 설명 |
|---|---|
| 푸시 | 엔드포인트 디바이스(예: 휴대폰 또는 태블릿)는 사용자에게 인증을 허용하거나 거부하라는 메시지를 표시합니다. |
| 짧은 메시지 서비스(SMS) | 엔드포인트 디바이스의 SMS 메시지는 사용자에게 인증을 허용하거나 거부하라는 메시지를 표시합니다. 경우에 따라 엔드포인트 디바이스는 사용자가 MFA 로그인 페이지에 입력해야 하는 코드를 제공합니다. |
| 보이스 | 자동 전화 통화는 사용자가 전화의 키를 누르거나 MFA 로그인 페이지에 코드를 입력하여 인증하라는 메시지를 표시합니다. |
| 일회성 암호(OTP) | 엔드포인트 디바이스는 자동으로 생성된 영숫자 문자열을 제공하며, 이 문자열은 사용자가 MFA 로그인 페이지에 입력하여 단일 트랜잭션 또는 세션에 대한 인증을 사용하도록 설정합니다. |

## SAML

SAML(보안 어설션 마크업 언어) 2.0을 사용하여 방화벽 또는 Panorama 웹 인터페이스에 액세스하는 관리자와 조직 내부 또는 외부의 웹 애플리케이션에 액세스하는 최종 사용자를 인증할 수 있습니다. 각 사

 ©2023 Palo Alto Networks, Inc.

용자가 많은 애플리케이션에 액세스하고 각 애플리케이션에 대한 인증이 사용자 생산성을 저해하는 환경에서는 한 번의 로그인으로 여러 애플리케이션에 액세스할 수 있도록 SAML SSO(Single Sign-On)를 구성할 수 있습니다. 마찬가지로 SAML 단일 로그아웃(SLO)을 사용하면 사용자가 한 세션에서 로그아웃하여 여러 애플리케이션의 세션을 종료할 수 있습니다. SSO는 웹 인터페이스에 액세스하는 관리자와 GlobalProtect 또는 인증 포털을 통해 애플리케이션에 액세스하는 최종 사용자가 사용할 수 있습니다. SLO는 관리자와 GlobalProtect 최종 사용자가 사용할 수 있지만 인증 포털 최종 사용자는 사용할 수 없습니다. 방화벽 또는 Panorama에서 SAML 인증을 구성할 때 관리자 권한 부여에 대한 SAML 특성을 지정할 수 있습니다. SAML 특성을 사용하면 디렉터리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 대개 방화벽이나 Panorama에서 설정을 다시 구성하는 것보다 쉽습니다.

관리자는 ***SAML***을 사용하여 방화벽 또는 ***Panorama***의 ***CLI***에 인증할 수 없습니다.

인증 시퀀스에서는 ***SAML*** 인증 프로파일을 사용할 수 없습니다.

SAML 인증에는 애플리케이션에 대한 액세스를 제어하는 서비스 공급자(방화벽 또는 Panorama) 와 사용자를 인증하는 PingFederate와 같은 ***ID*** 공급자(IdP)가 필요합니다. 사용자가 서비스 또는 애플리케이션을 요청하면 방화벽 또는 Panorama가 요청을 가로채고 인증을 위해 사용자를 IdP로 리디렉션합니다. 그런 다음 IdP가 사용자를 인증하고 인증의 성공 또는 실패를 나타내는 ***SAML*** 어설션을 반환합니다. 인증 포털 최종 사용자를 위한 SAML 인증은 인증 포털을 통해 애플리케이션에 액세스하는 최종 사용자에 대한 SAML 인증을 보여 줍니다.

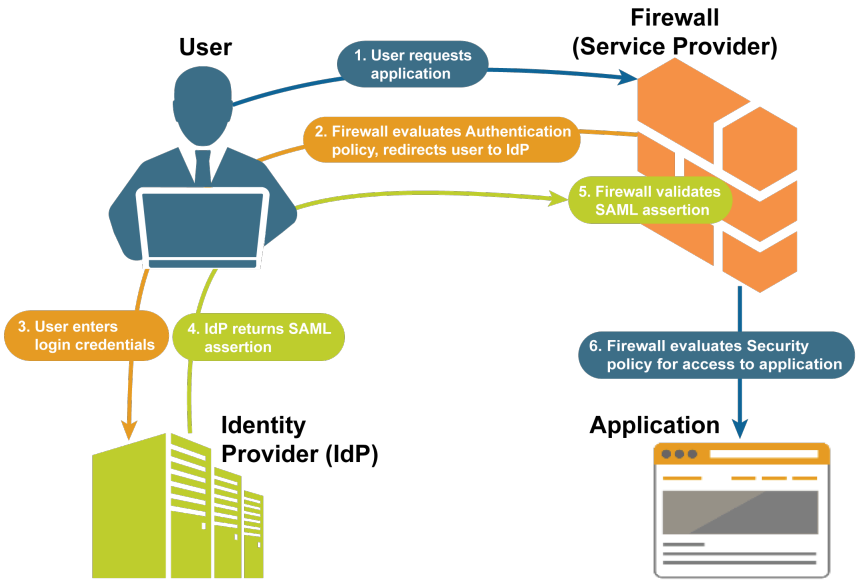



그림 **1:** 인증 포털 최종 사용자를 위한 **SAML** 인증

## Kerberos

Kerberos는 당사자를 식별하기 위해 고유 키(티켓이라고 함)를 사용하여 안전하지 않은 네트워크를 통해 당사자 간의 안전한 정보 교환을 가능하게 하는 인증 프로토콜입니다. 방화벽과 Panorama는 관리자와 최종 사용자를 위한 두 가지 유형의 Kerberos 인증을 지원합니다.

- **Kerberos** 서버 인증 - Kerberos 서버 프로파일을 사용하면 사용자가 기본적으로 Active Directory 도메인 컨트롤러 또는 Kerberos V5 호환 인증 서버에 인증할 수 있습니다. 이 인증 방법은 대화형이므로

 ©2023 Palo Alto Networks, Inc.

사용자가 사용자 이름과 암호를 입력해야 합니다. 구성 단계는 Kerberos 서버 인증 구성을 참조하십시오.

- **Kerberos SSO(Single Sign-On)** - Kerberos V5 SSO를 지원하는 네트워크는 사용자에게 네트워크에 대한 초기 액세스(예: Microsoft Windows 로그인)에 대해서만 로그인하라는 메시지를 표시합니다. 이 초기 로그인 후 사용자는 SSO 세션이 만료될 때까지 다시 로그인하지 않고도 네트워크의 모든 브라우저 기반 서비스(예: 방화벽 웹 인터페이스)에 액세스할 수 있습니다. (Kerberos 관리자가 SSO 세션 기간을 설정합니다.) Kerberos SSO와 다른 외부 인증 서비스(예: TACACS+ 서버)를 모두 활성화하면 방화벽은 먼저 SSO를 시도하고 실패한 경우에만 인증을 위해 외부 서비스로 대체합니다. Kerberos SSO를 지원하려면 네트워크에 다음이 필요합니다.
  - 인증 서버(AS) 및 티켓 부여 서비스(TGS)가 있는 키 배포 센터(KDC)를 포함한 Kerberos 인프라.
  - 사용자를 인증할 방화벽 또는 Panorama용 Kerberos 계정. 방화벽 또는 Panorama의 보안 주체 이름과 해시된 암호가 포함된 파일인 Kerberos 키탭을 생성하려면 계정이 필요합니다. SSO 프로세스에는 키탭(keytab)이 필요합니다.

  구성 단계는 Kerberos Single Sign-On 구성을 참조하십시오.

  ***Kerberos SSO**는 **Kerberos** 환경 내부에 있는 서비스 및 애플리케이션에만 사용할 수 있습니다. 외부 서비스 및 애플리케이션에 대해 **SSO**를 활성화하려면 SAML을 사용합니다.*

## TACACS+

TACACS+(터미널 액세스 컨트롤러 액세스 제어 시스템 플러스)는 중앙 집중식 서버를 통해 인증 및 권한 부여를 가능하게 하는 프로토콜 제품군입니다. TACACS+는 사용자명과 암호를 암호화하여 암호만 암호화하는 RADIUS보다 더 안전합니다. TACACS+는 TCP를 사용하기 때문에 더 안정적이지만 RADIUS는 UDP를 사용합니다. 방화벽의 최종 사용자 또는 관리자와 Panorama의 관리자에 대해 TACACS+ 인증을 구성할 수 있습니다. 선택적으로 TACACS+ VSA(Vendor-Specific Attributes)를 사용하여 관리자 권한 부여를 관리할 수 있습니다. TACACS+ VSA를 사용하면 방화벽 및 Panorama에서 설정을 재구성하는 대신 디렉터리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다.

방화벽 및 Panorama는 다음 TACACS+ 속성 및 VSA를 지원합니다. TACACS+ 서버에서 이러한 VSA를 정의하는 단계는 TACACS+ 서버 설명서를 참조하십시오.

| 이름 | 값 |
|---|---|
| 서비스 | 이 속성은 VSA를 Palo Alto Networks에 특정한 것으로 식별하는 데 필요합니다. 값을 **PaloAlto**로 설정해야 합니다. |
| 프로토콜 | 이 속성은 VSA를 Palo Alto Networks 디바이스와 관련된 것으로 식별하는 데 필요합니다. 값을 **방화벽**으로 설정해야 합니다. |
| PaloAlto-Admin-Role | 방화벽의 기본(동적) 관리 역할 이름 또는 사용자 지정 관리 역할 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 이름 | 값 |
| --- | --- |
| PaloAlto-Admin-Access-Domain | 방화벽 관리자에 대한 액세스 도메인의 이름(디바이스 > 액세스 도메인 페이지에서 구성). 방화벽에 여러 가상 시스템이 있는 경우 이 VSA를 정의합니다. |
| PaloAlto-Panorama-Admin-Role | Panorama의 기본(동적) 관리 역할 이름 또는 사용자 지정 관리 역할 이름. |
| PaloAlto-Panorama-Admin-Access-Domain | 디바이스 그룹 및 템플릿 관리자의 액세스 도메인 이름(**Panorama** > **Access** 도메인 페이지에서 구성). |
| PaloAlto-User-Group | 인증 프로파일의 허용 목록에 있는 사용자 그룹의 이름입니다. |

## RADIUS

리워드(원격 인증 전화 접속 사용자 서비스)는 중앙 집중식 인증 및 승인을 제공하는 광범위하게 지원되는 네트워킹 프로토콜입니다. 방화벽의 최종 사용자 또는 관리자및 Panorama의 관리자에 대한 RADIUS 인증을 구성할 수 있습니다. 선택적으로 RADIUS 공급업체별 특성(VSA)을 사용하여 관리자 권한 부여를 관리할 수 있습니다. RADIUS VSA를 사용하면 방화벽과 Panorama의 설정을 재구성하는 대신 디렉터리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 다음을 위해 RADIUS 서버를 사용하도록 방화벽을 구성할 수도 있습니다.

- GlobalProtect 엔드포인트에서 VSA 수집.
- 다단계 인증구현 .

RADIUS 서버로 인증 요청을 보낼 때 방화벽과 Panorama는 인증 프로세스를 시작하는 서비스에 대한 인증 시퀀스에 프로파일이 할당된 경우에도 인증 프로파일 이름을 NAS(네트워크 액세스 서버)로 사용합니다.

방화벽과 Panorama는 다음과 같은 RADIUS VSA를 지원합니다. RADIUS 서버에서 VSA를 정의하려면 공급업체 코드(Palo Alto Networks 방화벽 또는 Panorama의 경우 25461)와 VSA 이름과 번호를 지정해야 합니다. 일부 VSA에는 값도 필요합니다. 이러한 VSA를 정의하는 단계는 RADIUS 서버 설명서를 참조하십시오.

또는 Palo Alto Networks 방화벽과 RADIUS 서버가 서로 통신하는 데 사용하는 인증 특성을 정의하는 Palo Alto Networks RADIUS 사전을 다운로드하고 RADIUS 서버에 설치하여 RADIUS 바이너리 데이터에 대한 특성을 매핑할 수 있습니다.

서버의 사용자에 대한 동적 관리자 역할을 사전 정의하는 경우 소문자를 사용하여 역할을 지정합니다*(예:**SuperUser**가 아닌 **superuser**를 입력).*

*Cisco* 보안 액세스 제어 서버*(ACS)*에서 *Advanced* 공급자 옵션을 구성할 때 ***Vendor Length Field Size***와 ***Vendor Type Field Size***를 모두 ***1***로 설정해야 합니다. 그렇지 않으면 인증이 실패합니다.

 ©2023 Palo Alto Networks, Inc.

| 이름 | 숫자 | 값 |
|---|---|---|
| 관리자 계정 관리 및 인증을 위한 VSA | | |
| PaloAlto-Admin-Role | 1 | 방화벽의 기본(동적) 관리 역할 이름 또는 사용자 지정 관리 역할 이름입니다. |
| PaloAlto-Admin-Access-Domain | 2 | 방화벽 관리자에 대한 액세스 도메인의 이름(디바이스 > 액세스 도메인 페이지에서 구성). 방화벽에 여러 가상 시스템이 있는 경우 이 VSA를 정의합니다. |
| PaloAlto-Panorama-Admin-Role | 3 | Panorama의 기본(동적) 관리 역할 이름 또는 사용자 지정 관리 역할 이름. |
| PaloAlto-Panorama-Admin-Access-Domain | 4 | 디바이스 그룹 및 템플릿 관리자에 대한 액세스 도메인의 이름(**Panorama** > 액세스 도메인 페이지에서 구성). |
| PaloAlto-User-Group | 5 | 인증 프로파일 레퍼런스 사용자 그룹의 이름입니다. |
| GlobalProtect 엔드포인트에서 RADIUS 서버로 포워딩된 VSA | | |
| PaloAlto-User-Domain | 6 | 이러한 VSA를 정의할 때 값을 지정하지 마십시오. |
| PaloAlto-Client-Source-IP | 7 | |
| PaloAlto-Client-OS | 8 | |
| PaloAlto-Client-Hostname | 9 | |
| PaloAlto-GlobalProtect-Client-Version | 10 | |

## LDAP

LDAP(Lightweight Directory Access Protocol)는 정보 디렉토리에 액세스하기 위한 표준 프로토콜입니다. 최종 사용자와 방화벽 및 Panorama 관리자에 대해 LDAP 인증을 구성할 수 있습니다.

LDAP 서버에 연결하도록 방화벽을 구성하면 IP 주소 대신 사용자 및 사용자 그룹을 기반으로 정책 규칙을 정의할 수도 있습니다. 해당 단계는 사용자를 그룹에 매핑 및 사용자 및 그룹 기반 정책 활성화를 참조하십시오.

## 로컬 인증

방화벽과 Panorama는 관리자와 최종 사용자에게 로컬 인증을 제공하지만 대부분의 경우 중앙 계정 관리를 제공하기 때문에 외부 인증 서비스가 바람직합니다. 그러나 조직에서 정규 계정에 대해 예약하는 디렉터리 서버를 통해 관리하지 않는 특별한 사용자 계정이 필요할 수 있습니다. 예를 들어 디렉터리 서버가


©2023 Palo Alto Networks, Inc.

다운된 경우에도 방화벽에 액세스할 수 있도록 방화벽에 로컬인 운용 관리자 계정을 정의할 수 있습니다. 이러한 경우 다음 로컬 인증 방법을 사용할 수 있습니다.

- **(**방화벽 전용**)** 로컬데이터베이스 인증 -로컬 데이터베이스 인증을 구성하려면 방화벽에서 로컬로 실행되고 사용자 계정(사용자 이름 및 암호 또는 해시된 암호)과 사용자 그룹이 포함된 데이터베이스를 생성합니다. 이러한 유형의 인증은 일반 텍스트 암호가 아닌 해시된 암호만 알고 있는 경우 기존 유닉스 계정의 자격 증명을 재사용하는 사용자 계정을 만드는 데 유용합니다. 로컬 데이터베이스 인증은 인증 프로파일과 연결되어 있으므로 Kerberos Single Sign-On(SSO) 또는 MFA(다단계 인증)와 같은 다양한 인증 설정이 필요한 배포를 수용할 수 있습니다. 자세한 내용은 인증 프로파일 및 시퀀스 구성을 참조하십시오. 인증 프로파일을 사용하는 관리자 계정의 경우 암호 복잡성 및 만료 설정이 적용되지 않습니다. 이 인증 방법은 방화벽(Panorama 제외)에 액세스하는 관리자와 인증 포털 또는 GlobalProtect를 통해 서비스 및 애플리케이션에 액세스하는 최종 사용자가 사용할 수 있습니다.
- 데이터베이스가 없는 로컬 인증 -방화벽이나 Panorama에서 로컬로 실행되는 사용자 및 사용자 그룹의 데이터베이스를 만들지 않고도 방화벽 관리 계정 또는 Panorama 관리 계정을 구성할 수 있습니다. 이 메서드는 인증 프로파일과 연결되지 않으므로 Kerberos SSO 또는 MFA와 결합할 수 없습니다. 그러나 암호 프로파일을 허용하는 유일한 인증 방법으로 개별 계정을 전역 설정과 다른 암호 만료 설정과 연결할 수 있습니다. (자세한 내용은 암호 복잡성 및 만료 설정 정의)를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 인증 배포 계획

다음은 인증 포털을 통해 서비스 및 애플리케이션에 액세스하는 방화벽 및 최종 사용자에게 액세스하는 관리자를 위한 인증 솔루션을 구현하기 전에 고려해야 할 주요 질문입니다.

최종 사용자와 관리자 모두의 경우 다음을 고려하십시오.

- 기존 보안 인프라를 어떻게 활용할 수 있습니까? 일반적으로 방화벽을 기존 인프라와 통합하는 것은 방화벽 서비스에 대한 새로운 별도의 솔루션을 설정하는 것보다 빠르고 저렴합니다. 방화벽은 다단계 인증,SAML, 커베로스, TACACS+, RADIUS 및 LDAP 서버와 통합할 수 있습니다. 사용자가 네트워크 외부에 있는 서비스 및 애플리케이션에 액세스하는 경우 SAML을 사용하여 방화벽을 외부 및 내부 서비스 및 애플리케이션 모두에 대한 액세스를 제어하는 IDP(IDP)와 통합할 수 있습니다.
- 사용자 환경을 어떻게 최적화할 수 있습니까? 사용자가 수동으로 인증하지 않고 공개 키 인프라가 있는 경우 인증서 인증을 구현할 수 있습니다. 또 다른 옵션은 사용자가 로그인 한 후 여러 서비스 및 애플리케이션에 액세스할 수 있도록 Kerberos 또는 SAML Single Sign-On(SSO)을 구현하는 것입니다. 네트워크에 추가 보안이 필요한 경우 인증서 인증을 대화형(시도 응답) 인증과 결합할 수 있습니다.
- 조직에서 정규 계정에 대해 예약하는 디렉터리 서버를 통해 관리하지 않는 특별한 사용자 계정이 필요합니까? 예를 들어 디렉터리 서버가 다운된 경우에도 방화벽에 액세스할 수 있도록 방화벽에 로컬인 운용 관리자 계정을 정의할 수 있습니다. 이러한 특수 목적 계정에 대해 로컬 인증을 구성할 수 있습니다.

  외부 인증 서비스는 일반적으로 중앙 계정 관리, 신뢰할 수 있는 인증 서비스 및 일반적으로 로 로깅 및 문제 해결 기능을 제공하기 때문에 로컬 인증에 바람직합니다.
- 사용자 계정의 사용자명이 제대로 포맷되어 있습니까? SAML, Kerberos, TACACS+, RADIUS 및 LDAP 인증을 활용하려면 모든 사용자명이 정규 표현 리눅스 로그인 이름 규칙을 준수해야 합니다. 사용자명에는 해당 형식이 있어야 합니다**[a-zA-Z0-9_.][a-zA-Z0-9_.-]{0,30}[a-zA-Z0-9_.$-]**.

  즉, 다음을 의미합니다.

  - 사용자명의 첫 번째 문자는 상위 또는 소문자 알파벳 문자, 숫자(0-9) 또는 **_**(밑줄) 또는 **.**(마침표)여야 합니다.
  - 첫 번째 문자와 마지막 문자 이외에 사용자명에는 상위 또는 소문자 알파벳 문자, 숫자(0-9) 및 **_**(밑줄), **.**(마침표) 또는 **-**(대시)가 포함될 수 있습니다. 최대 길이는 첫 번째 문자와 마지막 문자를 제외한 30자입니다.
  - 사용자명의 마지막 문자는 상위 또는 소문자 알파벳 문자, 숫자(0-9) 또는 **_**(밑줄), **.**(마침표), **$** 또는 **-**(대시)일 수 있습니다.

  PAN-OS 관리자만 정규 표현 Linux 로그인 이름 규칙을 준수해야 합니다. GlobalProtect 및 캡티브 포털 사용자에게는 필요하지 않습니다.

최종 사용자의 경우 다음을 고려하십시오.

- 어떤 서비스 및 애플리케이션이 다른 서비스보다 더 민감합니까? 예를 들어 검색 엔진보다 주요 재무 문서에 대한 더 강력한 인증을 원할 수 있습니다. 가장 중요한 서비스 및 애플리케이션을 보호하려면 MFA(다단계 인증)를 구성하여 각 사용자가 해당 서비스 및 애플리케이션에 액세스할 때 여러 메서드(요인)를 사용하여 인증하도록 할 수 있습니다. 다양한 보안 요구 사항을 수용하기 위해 특정 서비스, 애플리케이션 및 최종 사용자를 기반으로 MFA 또는 단일 요소 인증(예: 로그인 자격 증명 또는 인증

 ©2023 Palo Alto Networks, Inc.

서)을 트리거하는 인증 정책 구성 규칙입니다. 공격 면적을 줄이는 다른 방법에는 허용된 애플리케이션에 대한 네트워크 세분화 및 사용자 그룹이 포함됩니다.

관리자의 경우 다음을 고려하십시오.

- 외부 서버를 사용하여 모든 관리 계정에 대한 권한을 중앙집중적으로 관리합니까? 외부 서버에서 공급업체별 특성(VSA)을 정의하면 방화벽의 설정을 재구성하는 대신 디렉터리 서비스를 통해 관리 역할 할당을 신속하게 변경할 수 있습니다. 또한 VSA를 사용하면 여러 가상 시스템을 사용하는 방화벽 관리자에 대한 액세스 도메인을 지정할 수 있습니다. SAML, TACACS+ 및 RADIUS는 외부 승인을 지원합니다.

 ©2023 Palo Alto Networks, Inc.

# 다단계 인증 구성

중요한 서비스 및 애플리케이션을 보호하기 위해 멀티 팩터 인증(MFA)을 사용하려면 첫 번째 인증 요소에 대한 웹 양식을 표시하고 인증 타임스탬프를 기록하도록 인증 포털을 구성해야 합니다. 방화벽은 타임스탬프를 사용하여 인증 정책 규칙의 타임아웃를 평가합니다. 추가 인증 요소를 활성화하려면 RADIUS 또는 벤더 API를 통해 방화벽을 MFA 공급업체와 통합할 수 있습니다. 인증 정책을 평가한 후 방화벽이 보안 정책을 평가하므로 두 정책 유형 모두에 대한 규칙을 구성해야 합니다.

***Palo Alto Networks***는 애플리케이션 콘텐츠 업데이트를 통해 MFA 벤더를 지원합니다. 즉, ***Panoramor***를 사용하여 디바이스 그룹 구성을 방화벽에 푸시하는 경우 공급업체 지원 불일치를 방지하기 위해 ***Panoramoram***와 동일한 애플리케이션 업데이트를 방화벽에 설치해야 합니다.

***MFA*** 벤더 ***API*** 통합은 인증 정책을 통한 최종 사용자 인증에만 지원됩니다. ***GlobalProtect*** 포털 또는 게이트웨이에 대한 원격 사용자 인증 또는 ***PAN-OS*** 또는 ***Panorama*** 웹 인터페이스에 대한 관리자 인증의 경우 ***RADIUS*** 또는 ***SAML***을 통해 지원되는 ***MFA*** 벤더만 사용할 수 있습니다. 공급업체 ***API***를 통한 ***MFA*** 서비스는 이러한 사용 사례에서 지원되지 않습니다.

**STEP 1 |** 리디렉션 모드에서 인증 포털을 구성하여 첫 번째 인증 요소에 대한 웹 양식을 표시하고, 인증 타임스탬프를 기록하고, 사용자 매핑을 업데이트합니다.

**STEP 2 |** 다음 서버 프로파일 중 하나를 구성하여 방화벽이 첫 번째 인증 요소에 대해 사용자를 인증하는 서비스에 연결하는 방법을 정의합니다.

- RADIUS 서버 프로파일을 추가합니다. 이는 방화벽이 RADIUS를 통해 MFA 공급업체와 통합되는 경우에 필요합니다. 이 경우 MFA 벤더는 첫 번째 및 모든 추가 인증 요소를 제공하므로 다음 단계(MFA 서버 프로파일 구성)를 건너뛸 수 있습니다. 방화벽이 API를 통해 MFA 벤더와 통합되는 경우에도 첫 번째 요소에 RADIUS 서버 프로파일을 사용할 수 있지만 추가 요소에 대해서는 MFA 서버 프로파일이 필요합니다.
- SAML IdP 서버 프로파일을 추가합니다.
- Kerberos 서버 프로파일을 추가합니다.
- TACACS+ 서버 프로파일을 추가합니다.
- LDAP 서버 프로파일을 추가합니다.

대부분의 경우 첫 번째 인증 요소에는 외부 서비스를 사용하는 것이 좋습니다. 하지만 로컬 데이터베이스 인증 구성을 다른 방법으로 구성할 수 있습니다.

**STEP 3 |** MFA 서버 프로파일을 추가합니다.

프로파일은 방화벽이 MFA 서버에 연결하는 방법을 정의합니다. 첫 번째 요소 다음에 각 인증 요소에 대해 별도의 프로파일을 추가합니다. 방화벽은 벤더 API를 통해 이러한 MFA 서버와 통합됩니다. 최대


©2023 Palo Alto Networks, Inc.

3개의 추가 요인을 지정할 수 있습니다. 각 MFA 벤더는 한 가지 요소를 제공하지만 일부 벤더는 사용자가 여러 요소 중 하나를 선택할 수 있도록 합니다.

1. 디바이스 > 서버 프로파일 > 다단계 인증을 선택하고 프로파일을 추가합니다.
2. 이름을 입력하여 MFA 서버를 식별합니다.
3. MFA 서버에 대한 보안 연결을 설정할 때 방화벽에서 MFA 서버 인증서의 유효성을 검사하는 데 사용할 인증서 프로파일을 선택합니다.
4. 배포한 **MFA** 공급업체를 선택합니다.
5. 각 공급업체 속성의 값을 구성합니다.

   속성은 방화벽이 MFA 서버에 연결하는 방법을 정의합니다. 각 공급업체 유형에는 서로 다른 속성과 값이 필요합니다. 자세한 내용은 공급업체 설명서를 참조하십시오.
6. 확인을 클릭하여 프로파일을 저장합니다.

**STEP 4 |** 인증 프로파일을 구성합니다.

프로파일은 사용자가 응답해야 하는 인증 요소의 순서를 정의합니다.

1. 디바이스 > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 인증 프로파일을 식별할 이름을 입력합니다.
3. 첫 번째 인증 요소로 유형을 선택하고 해당하는 서버 프로파일을 선택합니다.
4. 구성한 MFA 서버 프로파일을 요소, 추가 인증 요소 사용 및 추가를 선택합니다.

   방화벽은 나열된 순서대로 위에서 아래로 각 MFA 서비스를 호출합니다.
5. 확인을 클릭하여 인증 프로파일을 저장합니다.

**STEP 5 |** 인증 시행 개체를 구성합니다.

개체는 각 인증 프로파일을 인증 포털 메서드와 연결합니다. 이 방법은 첫 번째 인증 챌린지(요소)가 투명하거나 사용자 응답이 필요한지의 여부를 결정합니다.

구성한 인증 프로파일을 선택한 다음 첫 번째 요소에 대한 인증 방법을 사용자에게 알려주는 메시지를 입력합니다. 인증 포털 웹 양식에 메시지가 표시됩니다.



인증 방법을 브라우저 챌린지로 설정하면 ***Kerberos SSO*** 인증이 실패한 경우에만 인증 포털 웹 양식이 표시됩니다. 그렇지 않으면 첫 번째 요소에 대한 인증이 자동으로 수행되므로 사용자에게 웹 양식이 표시되지 않습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 인증 정책 규칙을 구성합니다.

규칙은 보호하려는 서비스 및 애플리케이션 및 인증해야 하는 사용자와 일치해야 합니다.

1. 정책 > 인증을 선택한 다음 규칙을 **A**추가합니다.
2. 규칙을 식별하기 위해 이름을 입력합니다.
3. 소스를 선택한 다음 특정 영역 및 IP 주소 추가를 선택하거나 모든 영역 또는 IP 주소를 선택합니다.

   이 규칙은 지정된 IP 주소 또는 지정된 영역의 인터페이스에서 오는 트래픽에만 적용됩니다.
4. 사용자를 선택한 다음 규칙이 적용되는 원본 사용자 및 사용자 그룹을 선택하거나 추가합니다(기본값은 모두).
5. 대상을 선택한 다음 특정 영역 및 IP 주소 추가를 선택하거나 모든 영역 또는 IP 주소를 선택합니다.

   IP 주소는 액세스를 제어하려는 리소스(예: 서버)일 수 있습니다.
6. 서비스**/URL** 카테고리를 선택한 다음 규칙이 액세스를 제어하는 서비스 및 서비스 그룹을 선택하거나 추가합니다(기본값은 **service-http**).
7. 규칙이 액세스를 제어하는 URL 카테고리를 선택하거나 추가합니다(기본값은 임의). 예를 들어 가장 중요한 내부 사이트를 지정하는 사용자 지정 URL 카테고리를 만들 수 있습니다.
8. 작업을 선택한 다음 생성한 인증 적용 개체를 선택합니다.
9. 서비스 및 애플리케이션에 대한 반복적인 액세스에 대해 방화벽이 사용자에게 한 번만 인증하라는 메시지를 표시하는 타임아웃 기간(기본값 60)을 지정합니다.

   타임아웃은 더 엄격한 보안**(**인증 프롬프트 간 시간 단축**)**과 사용자 경험**(**인증 프롬프트 간 더 긴 시간**)** 간의 절충점입니다**.** 더 빈번한 인증은 데이터 센터와 같은 중요한 시스템 및 민감한 영역에 대한 액세스를 위한 올바른 선택인 경우가 많습니다**.** 덜 빈번한 인증은 종종 네트워크 페리미터와 사용자 경험이 핵심인 기업에 올바른 선택입니다**.**
10. 규칙을 저장하려면 확인을 클릭합니다.

**STEP 7 |** MFA 로그인 페이지를 사용자 지정합니다.

방화벽은 사용자에게 MFA 요소를 인증하는 방법과 인증 상태(진행 중, 성공 또는 실패)를 표시하는 방법을 알려주는 이 페이지를 표시합니다.

1. 디바이스 > 응답 페이지를 선택하고 **MFA** 로그인 페이지를 선택합니다.
2. 미리 정의된 응답 페이지를 선택하고 페이지를 클라이언트 시스템으로 내보내기합니다.
3. 클라이언트 시스템에서 HTML 편집기를 사용하여 다운로드한 응답 페이지를 사용자 지정하고 고유한 파일 이름으로 저장합니다.
4. 방화벽의 MFA 로그인 페이지 대화 상자로 돌아가서 사용자 정의 페이지를 가져오기하고, 찾아보기하여 파일 가져오기를 선택하고, 대상을 선택합니다. (가상 시스템 또는 공유 위치), 확인을 클릭하고 닫기를 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** 사용자가 인증이 필요한 서비스 및 애플리케이션에 액세스할 수 있도록 허용하는 보안 정책 규칙을 구성합니다.

1. 보안 정책 규칙을 생성합니다.
2. 변경 사항을 커밋합니다.



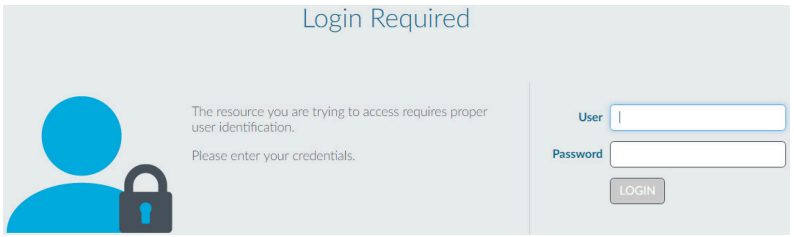
방화벽의 자동화된 상관 관계 엔진은 여러 상관 관계 개체를 사용하여 네트워크에서 *MFA*와 관련된 자격 증명 악용을 나타낼 수 있는 이벤트를 감지합니다. 이벤트를 검토하려면 *[*자동 상관 관계 엔진 상관 관계 > 이벤트 > 모니터링*]*을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** 방화벽이 MFA를 시행하는지 확인합니다.

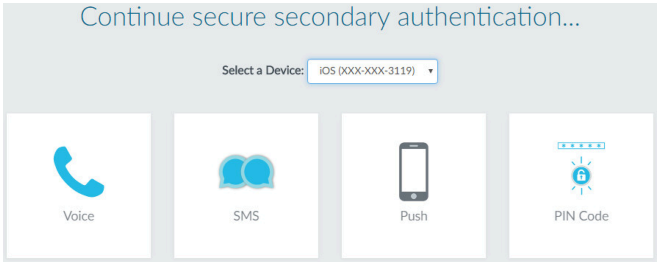
1. 인증 규칙에 지정된 소스 사용자 중 하나로 네트워크에 로그인합니다.
2. 규칙에 지정된 서비스 또는 애플리케이션 중 하나와 일치하는 서비스 또는 애플리케이션을 요청합니다.

   방화벽은 첫 번째 인증 요소에 대한 인증 포털 웹 양식을 표시합니다. 이 페이지에는 인증 적용 개체에 입력한 메시지가 포함되어 있습니다. 예:




3. 첫 번째 인증 챌린지에 대한 사용자 자격 증명을 입력합니다.

   그러면 방화벽이 다음 인증 요소에 대한 MFA 로그인 페이지를 표시합니다. 예를 들어 MFA 서비스에서 음성, SMS, 푸시 또는 PIN 코드(OTP) 인증 방법을 선택하라는 메시지를 표시할 수 있습니다. 푸시를 선택하면 휴대폰에서 인증을 승인하라는 메시지가 표시됩니다.




4. 다음 요소에 대해 인증합니다.

   방화벽에 인증 성공 또는 실패 메시지가 표시됩니다. 인증이 성공하면 방화벽은 다음 인증 요소(있는 경우)에 대한 MFA 로그인 페이지를 표시합니다.

   각 MFA 요소에 대해 이 단계를 반복합니다. 모든 요소에 대해 인증하면 방화벽이 보안 정책을 평가하여 서비스 또는 애플리케이션에 대한 액세스를 허용할지의 여부를 결정합니다.
5. 방금 액세스한 서비스 또는 애플리케이션의 세션을 종료합니다.
6. 동일한 서비스 또는 애플리케이션에 대해 새 세션을 시작합니다. 인증 규칙에서 구성한 제한 시간 내에 이 단계를 수행해야 합니다.

   방화벽은 재인증 없이 액세스를 허용합니다.
7. 타임아웃 기간이 만료될 때까지 기다렸다가 동일한 서비스나 애플리케이션을 요청하십시오.

   방화벽은 재인증하라는 메시지를 표시합니다.

## RSA SecurID와 방화벽 간의 MFA 구성

다중 요소 인증을 사용하면 사용자가 네트워크 리소스에 액세스하도록 허용하기 전에 여러 요소를 사용하여 사용자의 신원을 확인함으로써 회사 자산을 보호할 수 있습니다. 방화벽과 RSA SecurID Access Cloud Authentication Service 간에 MFA(다중 요소 인증)를 활성화하려면 먼저 여러 요소를 사용하여 사용자를 인증하도록 방화벽을 구성하는 데 필요한 세부 정보를 갖도록 RSA SecurID 서비스를 구성해야 합니다.


©2023 Palo Alto Networks, Inc.

RSA SecurID 액세스 콘솔에서 필요한 구성을 수행한 후 RSA SecurID와 통합하도록 방화벽을 구성할 수 있습니다.

*Palo Alto Networks*의 차세대 방화벽은 *RSA SecurID Access Cloud Authentication Service*와 통합됩니다. *RSA SecurID*와 *MFA API* 통합은 클라우드 기반 서비스에 대해서만 지원되며 두 번째 요소가 공급업체별 *API*를 사용하는 경우 온프레미스 인증 관리자에 대한 *2*단계 인증을 지원하지 않습니다. 이 통합에 필요한 최소 콘텐츠 버전은 *752* 및 *PAN-OS 8.0.2*입니다.

- RSA SecurID Access Cloud 인증 서비스 세부 정보 가져오기
- RSA SecurID를 사용하여 MFA에 대한 방화벽 구성

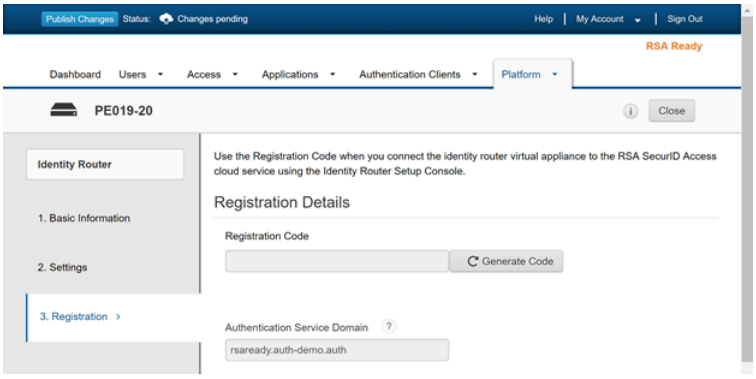
## RSA SecurID Access Cloud 인증 서비스 세부 정보 가져오기

방화벽과 RSA SecurID Access Cloud Authentication Service 간에 사용자 인증 요청을 안전하게 포워딩하려면 먼저 RSA SecurID Access Console로 이동하여 RSA Access ID, 인증 서비스 URL 및 클라이언트 API 키를 구성해야 합니다. 방화벽은 서비스를 인증하고 서비스와 상호 작용해야 합니다. 방화벽은 또한 RSA Approve 또는 RSA Tokencode 인증 방법을 사용하여 ID 소스를 인증하는 액세스 정책 ID가 필요합니다.

- **RSA SecurID API** 키 생성 - RSA SecurID 액세스 콘솔에 로그온하고 내 계정 > 회사 설정 > 인증 **API** 키를 선택합니다. 새 키를 추가한 다음 설정 저장 및 변경사항 게시를 수행합니다.

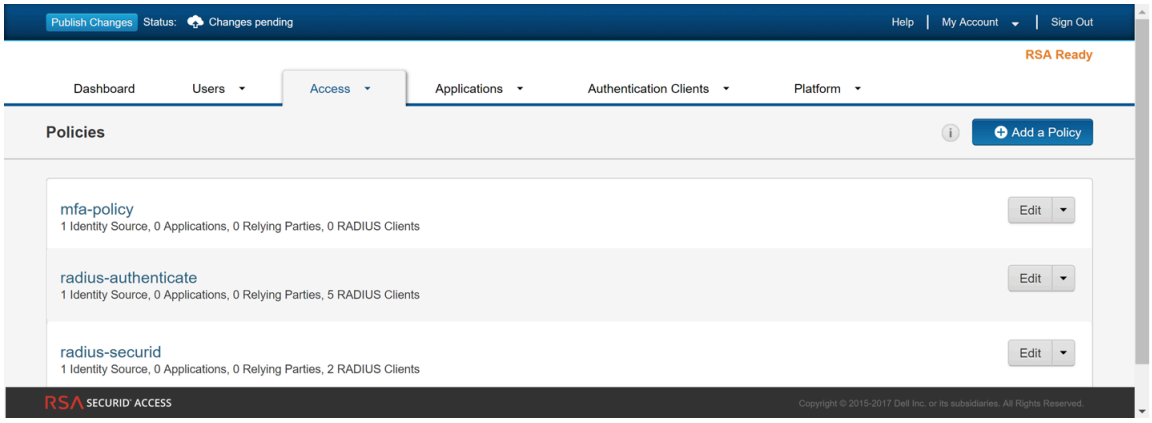



- 방화벽이 연결해야 하는 **RSA SecurID** 액세스 엔드포인트 **API(**인증 서비스 도메인**)** 가져오기 - 플랫폼 > **Identity** 라우터를 선택하고 ID 라우터를 수정하고 인증 서비스 도메인을 기록합니다. 이 예에서는 https://rsaready.auth-demo.auth입니다.




 ©2023 Palo Alto Networks, Inc.

- 액세스 정책 **ID** 가져오기 - 액세스 > 정책을 선택하고 방화벽이 RSA SecurID 서비스에 대한 인증 클라이언트 역할을 하도록 허용하는 액세스 정책의 이름을 기록해 둡니다. RSA Approve 또는 RSA Tokencode 인증 방법만 사용하도록 정책을 구성해야 합니다.




## RSA SecurID를 사용하여 MFA에 대한 방화벽 구성

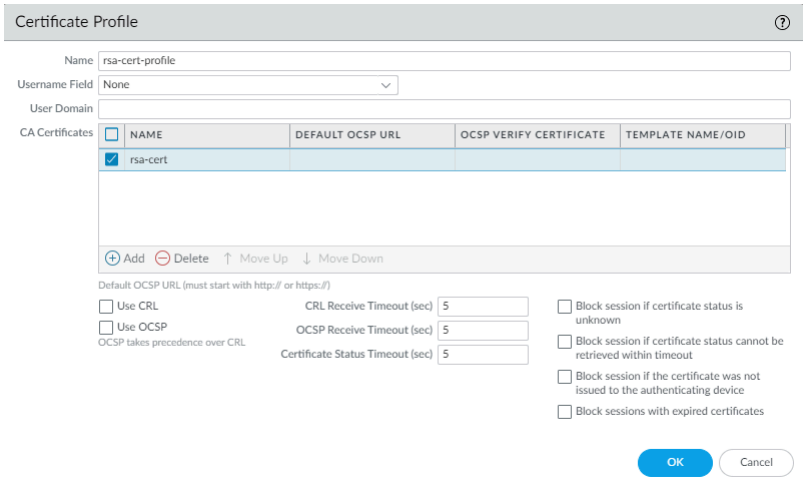
RSA SecurID Access Cloud 인증 서비스 세부 정보를 불러온 후에는 MFA가 호출될 때 사용자에게 RSA SecurID 토큰을 입력하라는 메시지를 표시하도록 방화벽을 구성할 수 있습니다.

**STEP 1 |** RSA SecurID Access 엔드포인트 API에서 제공하는 SSL 인증서를 신뢰하도록 방화벽을 구성합니다.

1. RSA SecurID Access 엔드포인트에서 SSL 인증서를 내보내고 방화벽으로 가져옵니다.

   방화벽과 RSA SecurID Access 엔드포인트 API 간의 신뢰를 활성화하려면 자체 서명된 인증서 또는 인증서 서명에 사용된 CA 인증서를 가져와야 합니다.

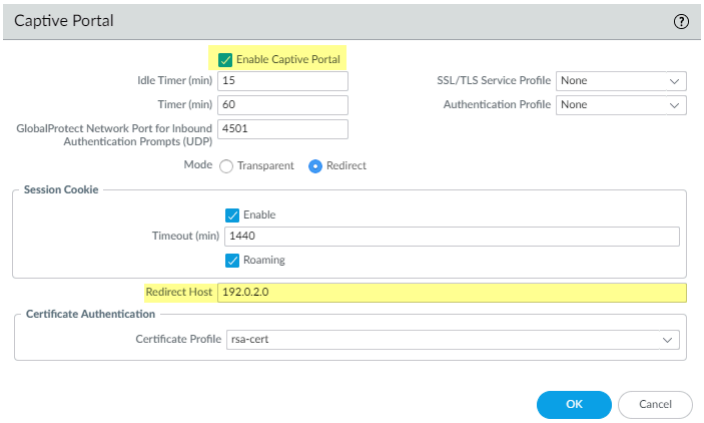
2. 인증서 프로파일 구성(디바이스 > 인증서 관리 > 인증서 프로파일을 구성하고 추가 클릭) .





©2023 Palo Alto Networks, Inc.

**STEP 2 |** 인증 포털(디바이스 > 사용자 식별 > 인증 포털 설정)을 리디렉션 모드에서 구성하여 웹 양식을 표시하고 RSA SecureID에 인증합니다. 리디렉션 호스트를 웹 요청이 리디렉션되는 방화벽의 레이어 3 인터페이스 IP 주소로 확인되는 IP 주소 또는 호스트 이름(이름에 마침표 없음)으로 지정해야 합니다.

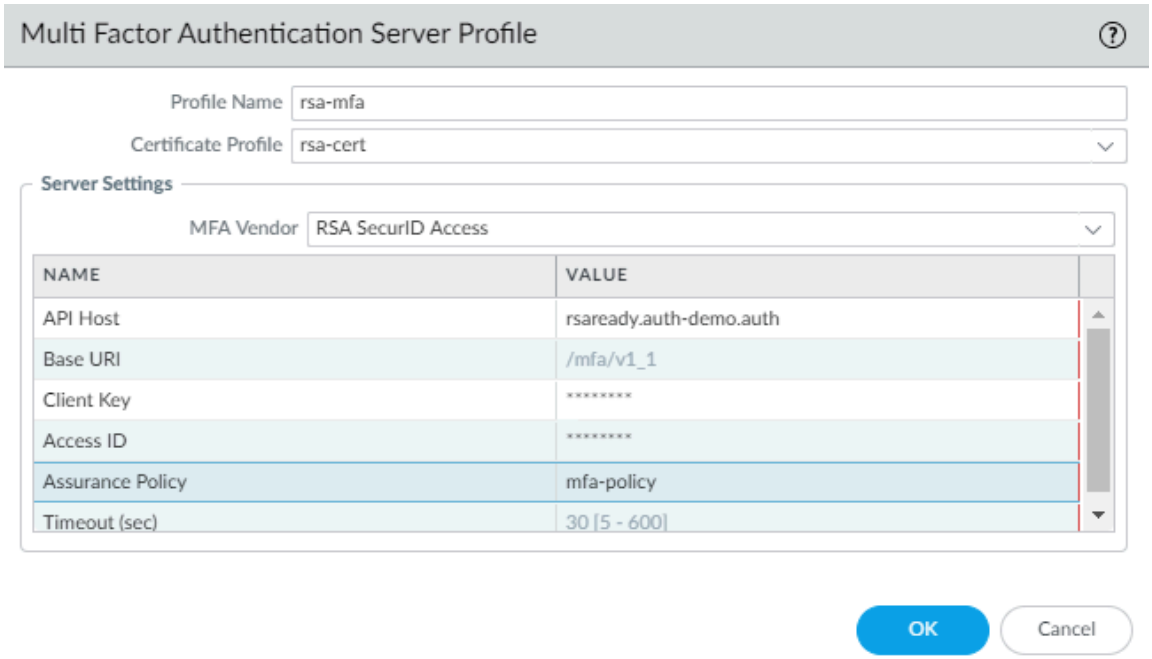




©2023 Palo Alto Networks, Inc.

**STEP 3 |** 방화벽이 RSA SecurID 클라우드 서비스와 연결해야 하는 방법을 지정하도록 다단계 인증 서버 프로파일을 구성합니다(디바이스 > 서버 프로파일 > **Multi Factor Authentication**및추가클릭).

1. 이름을 입력하여 MFA 서버 프로파일을 식별합니다.
2. 이전에 생성한 인증서 프로파일(이 예에서는 rsa-cert-profile)을 선택합니다. 방화벽은 RSA SecurID 클라우드 서비스와의 보안 연결을 설정할 때 이 인증서를 사용합니다.
3. **MFA** 공급업체 드롭다운에서 **RSA SecurID Access**를 선택합니다.
4. RSA SecurID Access Cloud 인증 서비스 세부정보 가져오기에서 기록한 각 속성에 대해 값을 구성합니다.
   - **API** 호스트 - 방화벽이 연결되어야 하는 RSA SecurID Access API 엔드포인트의 호스트 이름 또는 IP 주소(이 예에서는 rsaready.auth-demo.auth)를 입력합니다.
   - 기본 **URI** - 기본값(/mfa/v1_1)을 수정하지 마십시오.
   - 클라이언트 키 - RSA SecurID 클라이언트 키를 입력합니다.
   - 액세스 **ID** - RSA SecurID 액세스 ID를 입력합니다.
   - 보증 정책 - 이 예에서는 RSA SecurID 액세스 정책 이름인 mfa-policy를 입력합니다.
   - 타임아웃 - 기본값은 30초입니다.



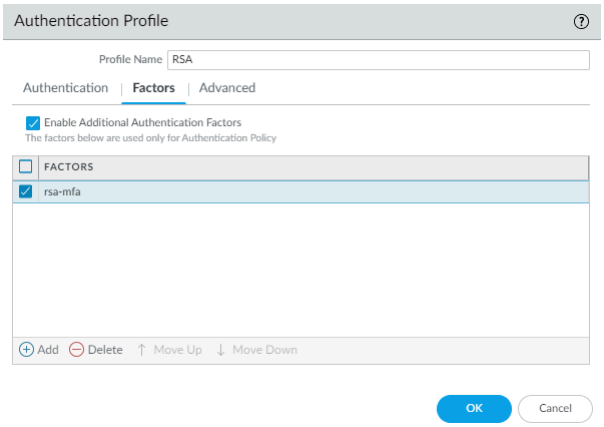

5. 프로파일을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 인증 프로파일을 구성합니다(디바이스 > 인증 프로파일 및 추가 클릭).

프로파일은 사용자가 응답해야 하는 인증 요소의 순서를 정의합니다.

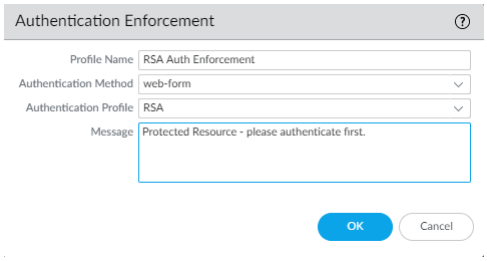
1. 첫 번째 인증 요소로 유형을 선택하고 해당하는 서버 프로파일을 선택합니다.
2. 이 예의 앞부분에서 만든 rsa-mfa 서버 프로파일을 요소, 추가 인증 요소 활성화 및 추가를 선택합니다.




3. 확인을 클릭하여 인증 프로파일을 저장합니다.

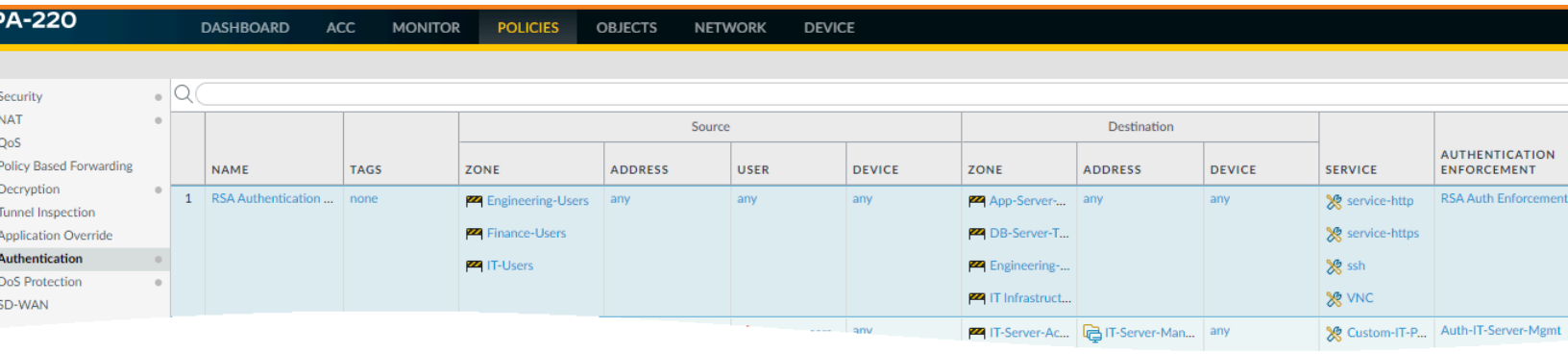
**STEP 5 |** 인증 시행 개체를 구성합니다. (개체 > 인증 및 추가 클릭).

이 예에서 방금 정의한 RSA라는 인증 프로파일을 선택해야 합니다.




**STEP 6 |** 인증 정책 규칙을 구성합니다. (정책 > 인증 및 추가 클릭)

인증 정책 규칙은 보호하려는 서비스 및 애플리케이션과 일치해야 하고 인증해야 하는 사용자를 지정하고 인증 프로파일을 트리거하는 인증 적용 개체를 포함해야 합니다. 이 예에서 RSA SecurID Access는 RSA Auth Enforcement라는 인증 시행 개체를 사용하여 HTTP, HTTPS, SSH 및 VNC 트래픽에 액세스하는 모든 사용자를 인증합니다(작업에서 인증 시행 개체 선택).




 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 방화벽에서 변경 사항을 커밋합니다.

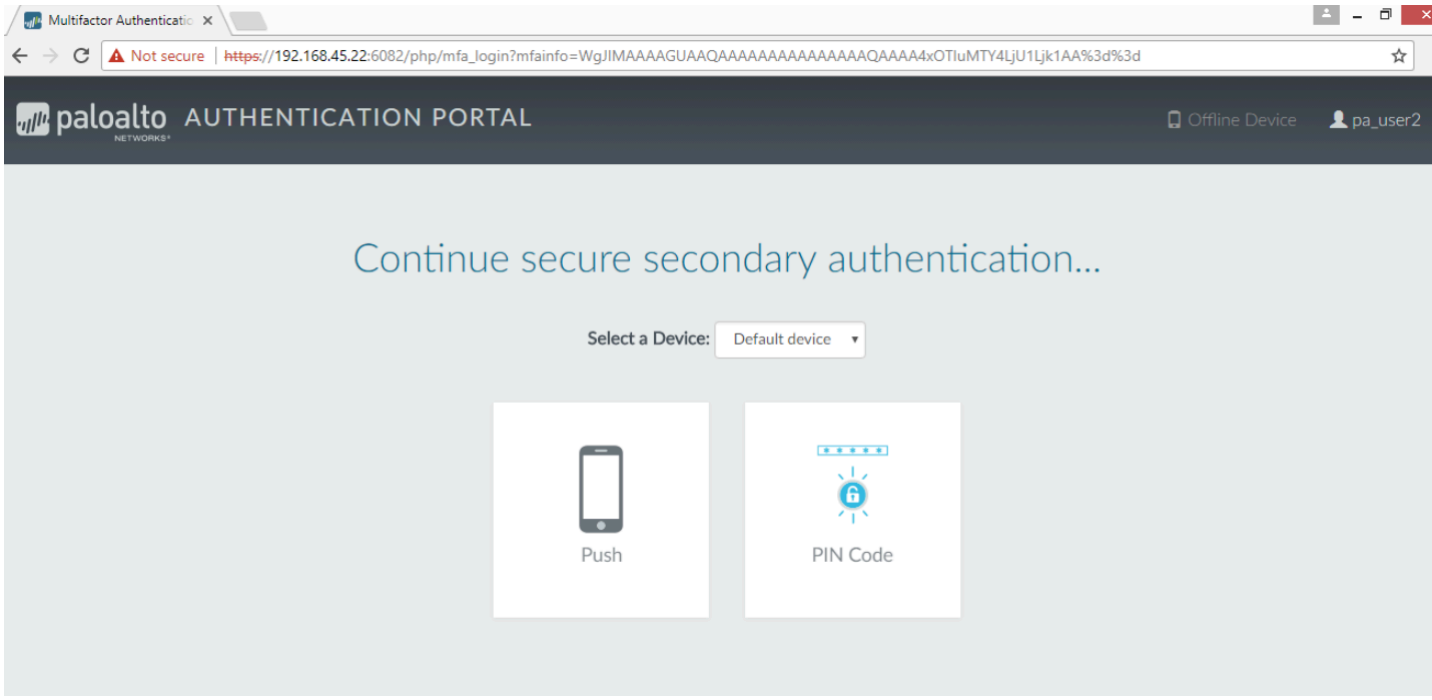

©2023 Palo Alto Networks, Inc.

**STEP 8 |** 활성화한 푸시 또는 PIN 코드 인증 방법을 사용하여 RSA SecurID를 사용하여 네트워크의 사용자를 보호하고 있는지 확인합니다.

1. 푸시 인증

   **1.** 네트워크의 사용자에게 웹 브라우저를 실행하고 웹사이트에 액세스하도록 요청합니다. 이전에 정의한 리디렉션 호스트에 대한 IP 주소 또는 호스트 이름이 있는 인증 포털 페이지가 표시되어야 합니다.

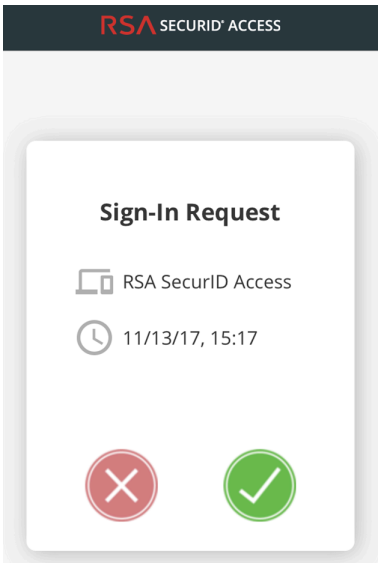
   **2.** 사용자가 첫 번째 인증 요소에 대한 자격 증명을 입력한 다음 보조 인증 요소로 계속 진행하고 푸시를 선택하는지 확인합니다.




   **3.** 사용자 모바일 디바이스의 RSA SecurID Access 애플리케이션에서 로그인 요청을 확인합니다.

   **4.** 사용자에게 모바일 디바이스에서 로그인 요청을 수락하도록 요청하고 방화벽이 인증 성공 알림을 수신할 때까지 몇 초 동안 기다립니다. 사용자는 요청된 웹사이트에 액세스할 수 있어야 합니다.

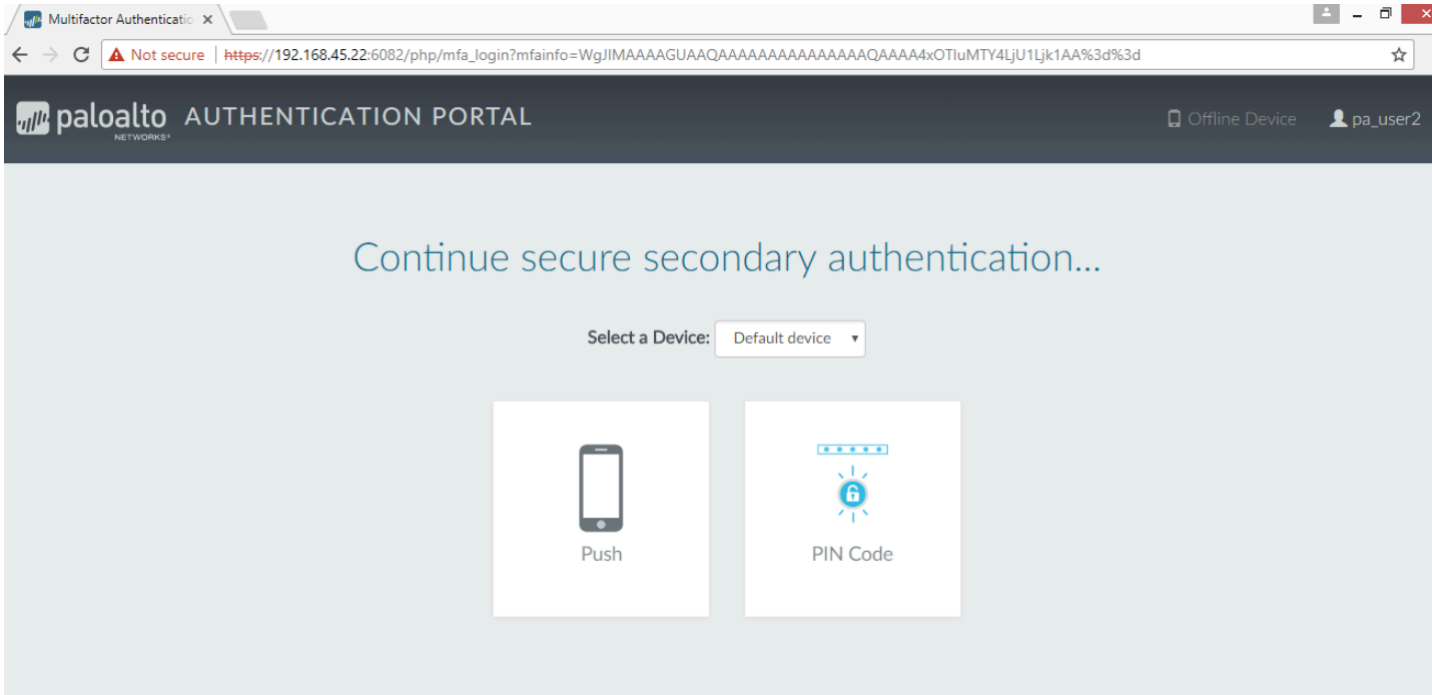

©2023 Palo Alto Networks, Inc.




인증 실패를 테스트하려면 모바일 디바이스에서 로그인 요청을 거부합니다.

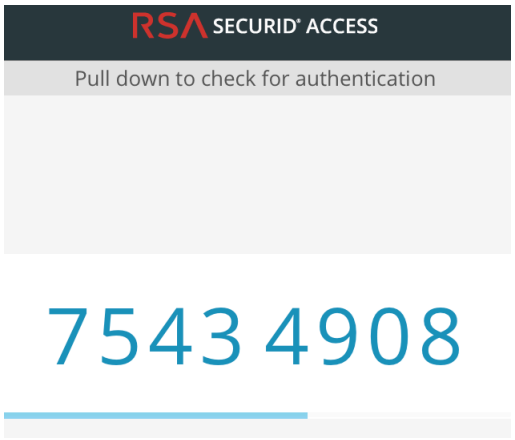
2. **PIN** 코드 인증

   1. 네트워크의 사용자에게 웹 브라우저를 실행하고 웹사이트에 액세스하도록 요청합니다. 이전에 정의한 리디렉션 호스트의 IP 주소 또는 호스트 이름이 있는 인증 포털 페이지가 표시되어야 합니다.
   2. 사용자가 첫 번째 인증 요소에 대한 자격 증명을 입력한 다음 보조 인증 요소로 계속 진행하고 **PIN** 코드를 선택하는지 확인합니다.




   3. 사용자 모바일 디바이스의 RSA SecurID Access 애플리케이션에 **PIN** 코드가 표시되는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.




4. 사용자에게 웹 브라우저의 **PIN** 입력**...** 프롬프트에서 PIN 코드를 복사하도록 요청하고 제출을 클릭합니다. 방화벽이 인증 성공 알림을 수신할 때까지 몇 초 동안 기다립니다. 사용자는 요청된 웹사이트에 액세스할 수 있어야 합니다.

## Okta와 방화벽 간의 MFA 구성

다중 요소 인증을 사용하면 사용자가 네트워크 리소스에 액세스하도록 허용하기 전에 여러 요소를 사용하여 사용자의 ID를 확인함으로써 회사 자산을 보호할 수 있습니다.

방화벽과 Okta ID 관리 서비스 간에 멀티 팩터 인증(MFA)을 활성화하려면:

- Okta 설정
- Okta와 통합되도록 방화벽 구성
- Okta를 사용하여 MFA 검증

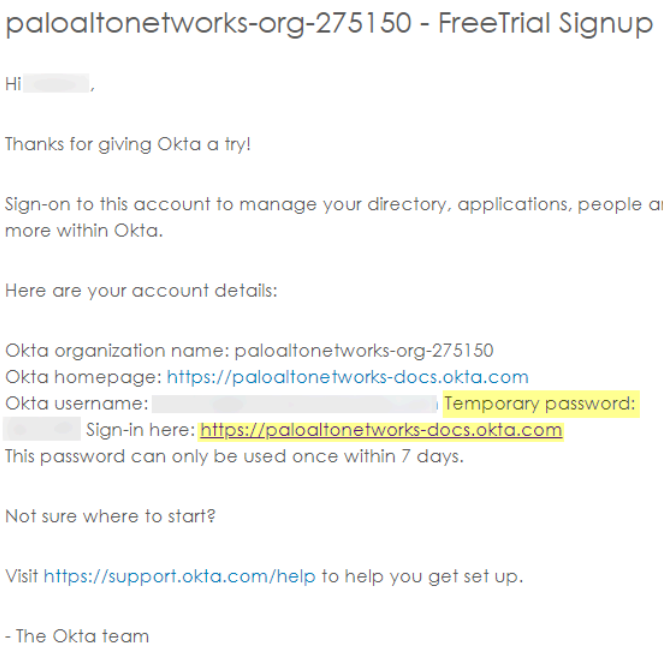
### Okta 설정

Okta 관리 포털에 로그인하여 사용자 계정을 생성하고, Okta MFA 정책을 정의하고, 방화벽에서 Okta를 사용하여 MFA를 구성하는 데 필요한 토큰 정보를 얻습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** Okta 관리자 사용자 계정을 생성합니다.

1. 이메일 주소와 이름을 제출한 다음 시작하기를 클릭합니다.
2. 확인 이메일의 링크를 클릭하고 포함된 임시 암호를 사용하여 Okta Admin Portal에 로그인합니다.



paloaltonetworks-org-275150 - FreeTrial Signup

Hi ,

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: paloaltonetworks-org-275150
Okta homepage: https://paloaltonetworks-docs.okta.com
Okta username: Temporary password:
Sign-in here: https://paloaltonetworks-docs.okta.com
This password can only be used once within 7 days.

Not sure where to start?

Visit https://support.okta.com/help to help you get set up.

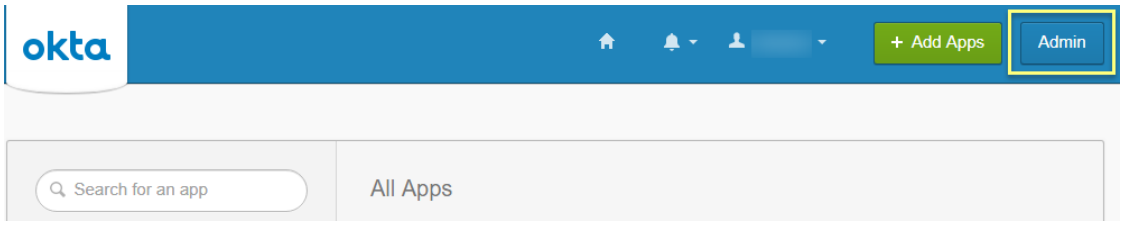
- The Okta team

3. 최소 8자, 소문자 1개, 대문자 1개, 숫자를 포함하며 사용자 아이디의 일부를 포함하지 않는 새 암호를 생성합니다.
4. 암호 미리 알림 질문을 선택한 다음 답을 입력합니다.
5. 보안 이미지를 선택한 다음 내 계정 생성을 선택합니다.

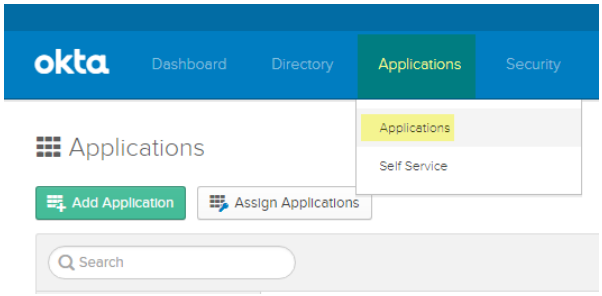
 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** Okta 서비스를 구성합니다.

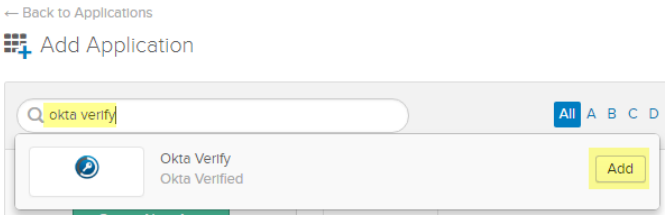
로그인하고 ***Okta*** 관리 포털로 리디렉션되지 않으면 오른쪽 상단에서 관리를 선택합니다.




1. Okta 대시보드에서 Okta 관리자 자격 증명으로 로그인한 다음 애플리케이션 > 애플리케이션을 선택합니다.



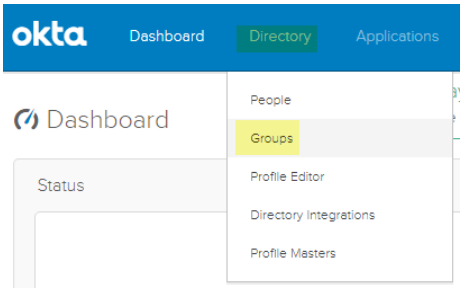

2. 애플리케이션 추가를 선택합니다.
3. **Okta** 검증을 검색합니다.
4. 추가, 완료 순으로 선택합니다.



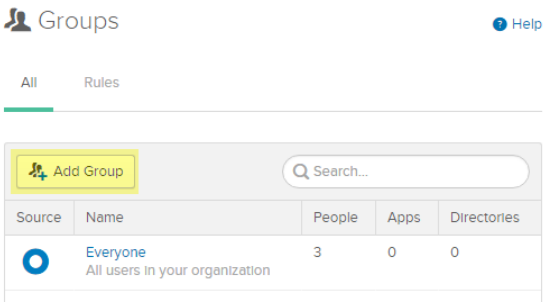

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 하나 이상의 사용자 그룹을 만들어 사용자를 분류(예: 디바이스별, 정책 또는 부서별)하고 Okta Verify 애플리케이션을 할당합니다.

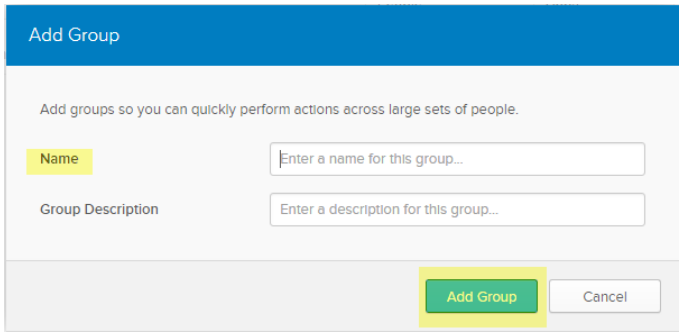
1. 디렉토리 > 그룹을 선택합니다.




2. 그룹 추가를 클릭합니다.

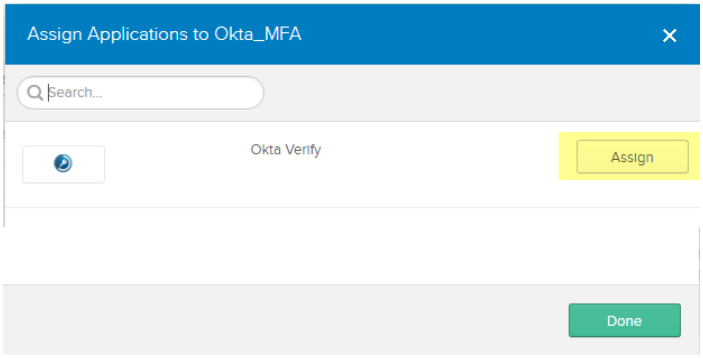



3. 그룹 이름을 입력하고 선택적으로 그룹 설명을 입력한 다음 그룹 추가를 입력합니다.




기본 그룹 ***Everyone***에는 Okta 구성의 첫 번째 단계에서 조직에 대해 구성된 모든 사용자가 포함됩니다.

4. 생성한 그룹을 선택한 다음 앱 관리를 선택합니다.
5. 2단계에서 추가한 Okta 검증 애플리케이션을 할당합니다.

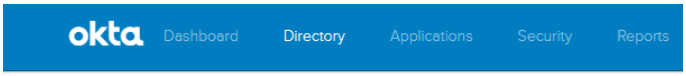


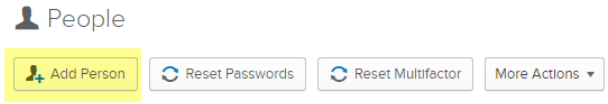

 ©2023 Palo Alto Networks, Inc.

6. 애플리케이션이 할당되면 완료를 클릭합니다.
7. MFA용 Okta Verify 애플리케이션을 사용할 모든 그룹에 대해 이 프로세스를 반복합니다.

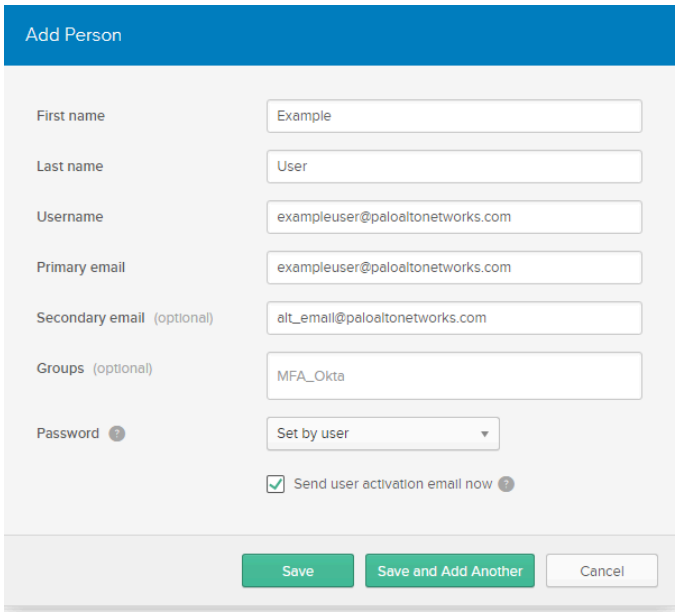
**STEP 4 |** 사용자를 추가하고 그룹에 할당합니다.

1. Okta 대시보드에서 디렉토리 > 사람 > 사람 추가를 선택합니다.




2. 사용자의 이름, 성 및 사용자 이름을 입력합니다. 사용자 이름은 자동으로 채워지는 기본 이메일과 방화벽에 입력한 사용자 이름과 일치해야 합니다. 선택적으로 사용자의 대체 이메일 주소를 보조 이메일로 입력할 수 있습니다.




3. 이 사용자와 연결할 그룹 또는 그룹의 이름을 입력하십시오. 입력을 시작하면 그룹 이름이 자동으로 채워집니다.
4. 지금 사용자 활성화 이메일 보내기를 선택한 다음 저장을 선택하여 단일 사용자를 추가하거나 저장 및 다른 사람 추가를 선택하여 사용자를 계속 추가합니다.

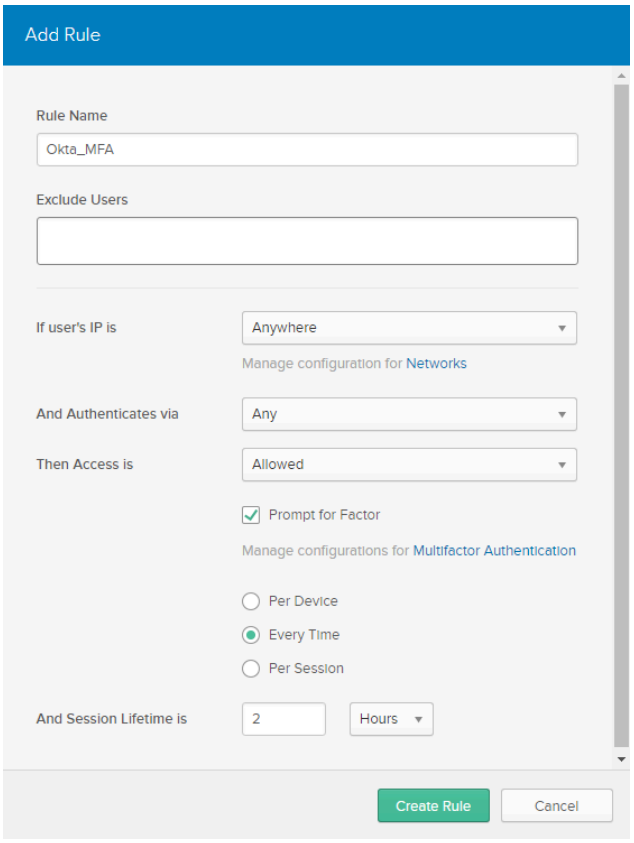

©2023 Palo Alto Networks, Inc.

**STEP 5 |** 사용자에게 테스트 정책을 할당합니다.

1. 보안 > 인증 > 사인온을 선택합니다.

   사용자에게 MFA로 로그인하라는 메시지를 표시하지 않는 기본 규칙이 있는 기본 정책이 있습니다.

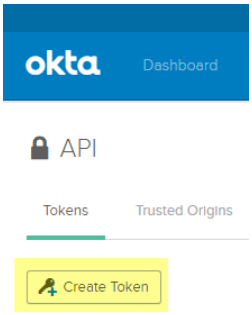
2. 규칙 이름을 입력하고 계수 프롬프트를 선택하여 MFA 프롬프트를 적용하고 프롬프트 유형(디바이스당, 매번 또는 세션당)을 선택한 다음 규칙 생성을 선택합니다.



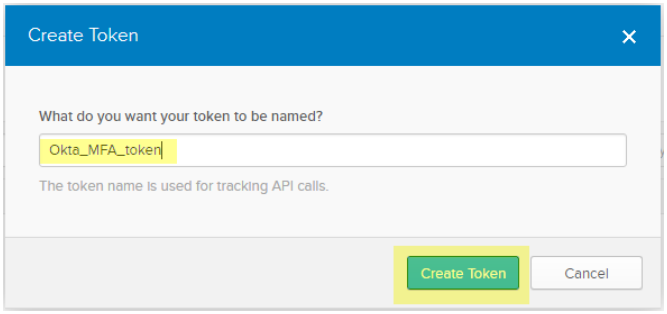

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** Okta 인증 토큰 정보는 한 번만 표시되므로 안전한 장소에 기록하십시오.

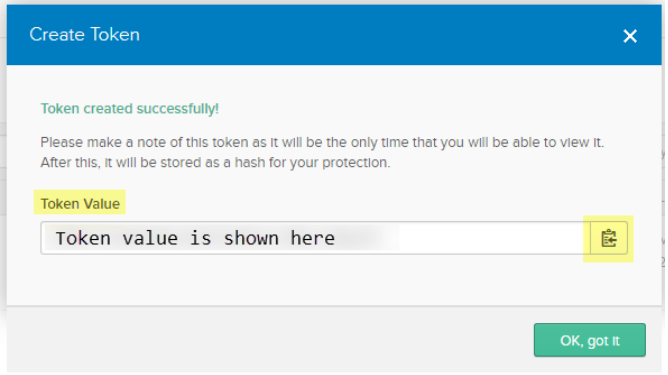
1. 보안 > **API** > 토큰을 선택합니다.
2. 토큰 만들기를 선택합니다.



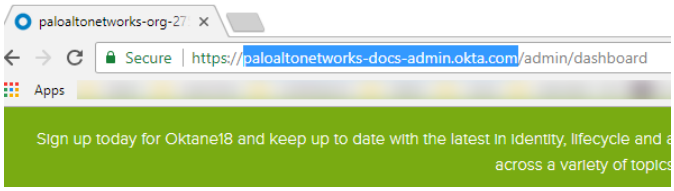

3. 토큰의 이름을 입력한 다음 토큰 만들기를 입력합니다.




4. 토큰 값을 복사합니다.
   클립보드에 복사 버튼을 클릭하여 토큰 값을 클립보드에 복사할 수 있습니다.

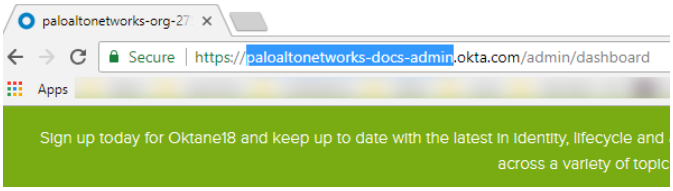



5. Okta 관리자 대시보드의 URL에서 **`https://`** 뒤의 URL 부분을 **`/admin`**까지 복사하여 **API** 호스트로 사용합니다.




6. 이 URL에서 조직으로 사용할 도메인 **`okta.com`**을 생략합니다.


©2023 Palo Alto Networks, Inc.




예를 들어 위의 Okta 관리 대시보드 URL 예에서 **https://paloaltonetworks-doc-admin.okta.com/admin/dashboard**은 다음과 같습니다.

- API 호스트 이름은 **paloaltonetworks-doc-admin.okta.com**입니다.
- 조직은 **paloaltonetworks-doc-admin**입니다.

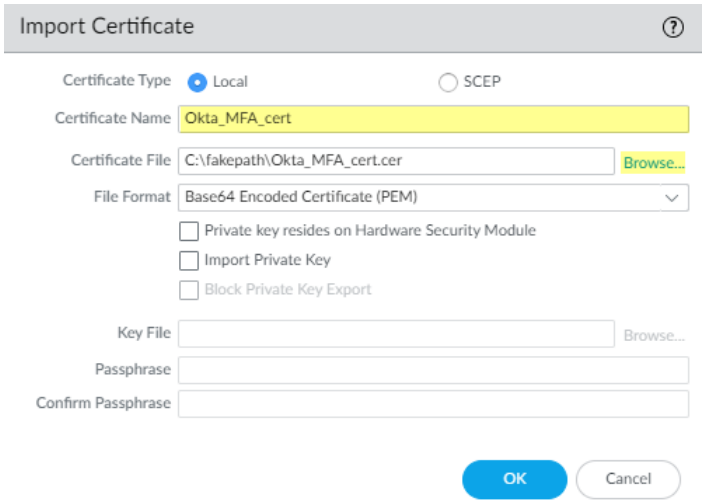
**STEP 7 |** Base-64 인코딩을 사용하여 인증서 체인의 모든 인증서를 내보냅니다.

1. 브라우저에 따라 다음 방법 중 하나를 사용하여 체인의 모든 인증서를 내보냅니다.
   - **Chrome** - **F12** 키를 누른 다음 보안 > 인증서 보기 > 세부 정보 > 파일에 복사를 선택합니다.
   - **Firefox** - 옵션 > 개인 정보 및 보안 > 인증서 보기 > 내보내기를 선택합니다.
   - **Internet Explorer** - 설정 > 인터넷 옵션 > 콘텐츠 > 인증서 > 내보내기를 선택합니다.
2. 인증서 내보내기 마법사를 사용하여 체인의 모든 인증서를 내보내고 **Base-64 encoded X.509**를 형식으로 선택합니다.

## Okta와 통합되도록 방화벽 구성

필수 조건으로 Okta를 사용하여 인증할 모든 사용자를 매핑했는지 확인합니다.

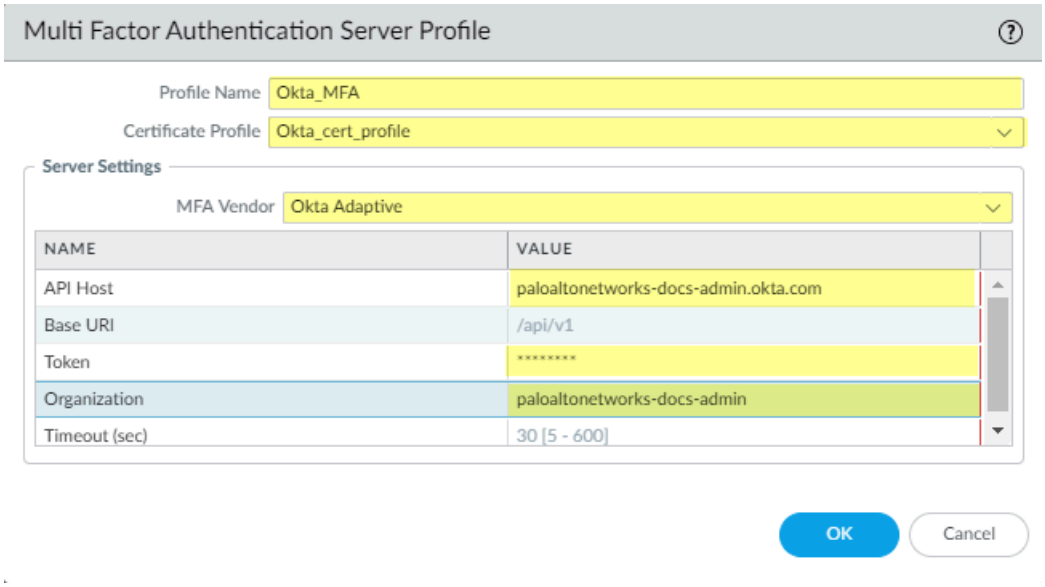
**STEP 1 |** 방화벽의 인증서 체인에 있는 모든 인증서를 가져오고 불러온 CA 인증서(루트 및 중간)를 인증서 프로파일에 추가합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** Okta에 대한 멀티 팩터 인증 서버 프로파일을 추가합니다.

1. 디바이스 > 서버 프로파일 > 다단계 인증을 선택합니다.
2. MFA 서버 프로파일을 추가합니다.

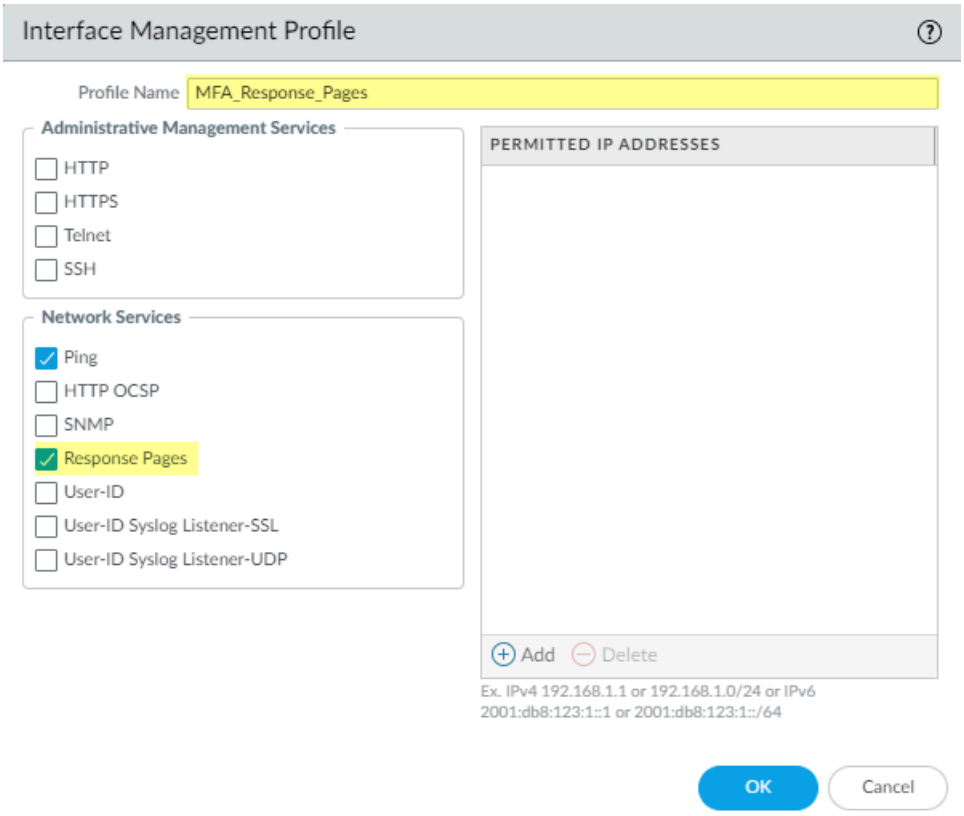



3. 프로파일 이름을 입력합니다.
4. Okta와 통합되도록 방화벽 구성의 1단계에서 생성한 인증서 프로파일을 선택합니다.
5. **Okta Adaptive**를 **MFA** 공급업체로 선택합니다.
6. Okta와 통합하도록 방화벽 구성의 4단계에서 **API** 호스트, 토큰 및 조직을 입력합니다.

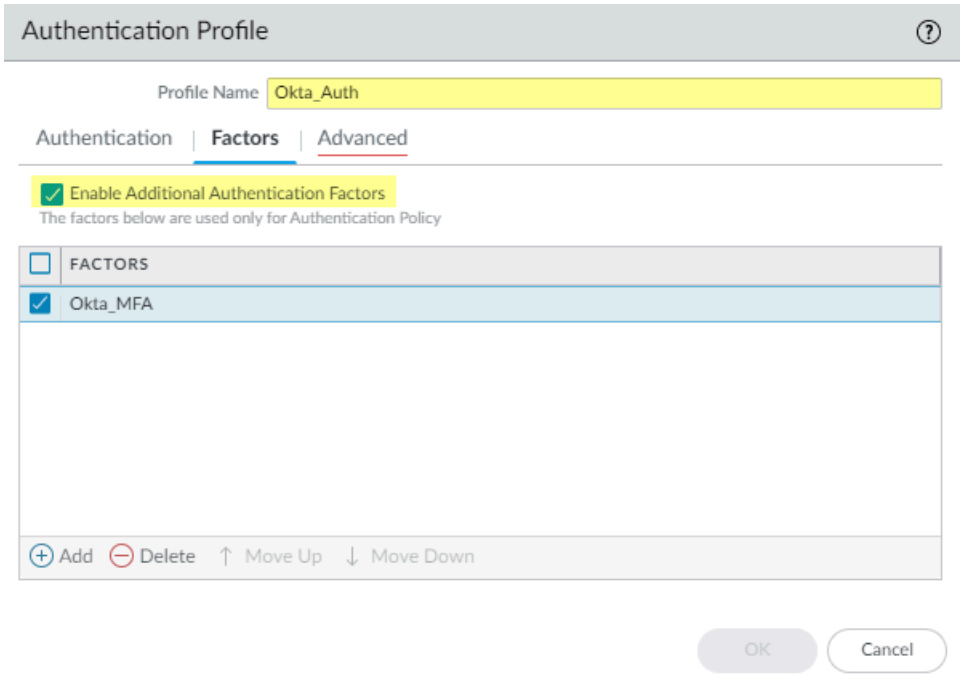
**STEP 3 |** 리디렉션 모드를 사용하여 인증 포털을 구성하여 사용자를 MFA 공급업체의 챌린지로 리디렉션합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 인터페이스 관리 프로파일에서 응답 페이지를 활성화하여 사용자를 응답 페이지 챌린지로 리디렉션합니다.




**STEP 5 |** 인증 프로파일을 만들고 MFA 공급업체를 요소로 추가합니다(3단계의 다단계 인증 구성 참조).





©2023 Palo Alto Networks, Inc.

**STEP 6 |** 식별된 사용자가 MFA 공급업체를 사용하여 문제에 응답하도록 하려면 소스 영역에서 User-ID를 활성화합니다.

**STEP 7 |** MFA 공급업체를 사용하고 인증 정책 규칙을 생성할 인증 시행 개체를 생성합니다(인증 정책 구성, 4단계 및 5단계 참조).

**STEP 8 |** 변경 사항을 커밋합니다.

### Okta를 사용하여 MFA 검증

**STEP 1 |** 사용자가 등록 이메일을 받고, 계정을 활성화했으며, 디바이스에 Okta Verify 앱을 다운로드했는지 확인합니다.

**STEP 2 |** 응답 페이지 챌린지를 묻는 웹사이트로 이동합니다.

조직에서 ***PKI*** 할당 인증서 대신 자체 서명된 인증서를 사용하는 경우 사용자가 클릭하여 챌린지에 액세스해야 한다는 보안 경고가 표시됩니다.

**STEP 3 |** Okta 자격 증명을 사용하여 응답 페이지에 로그인합니다.

**STEP 4 |** 디바이스가 챌린지 푸시 알림을 수신하는지 확인합니다.

**STEP 5 |** 사용자가 디바이스에서 푸시 알림을 수락하여 챌린지를 인증한 후 페이지에 성공적으로 액세스할 수 있는지 확인합니다.

## Duo와 방화벽 간에 MFA 구성

다중 요소 인증(MFA)을 사용하면 여러 요소를 사용하여 사용자가 네트워크 리소스에 액세스하도록 허용하기 전에 사용자의 ID를 확인함으로써 회사 자산을 보호할 수 있습니다. Duo ID 관리 서비스를 사용하여 방화벽으로 인증하는 방법에는 여러 가지가 있습니다.

- GlobalProtect Gateway 및 RADIUS 서버 프로파일을 사용하는 VPN 로그인에 대한 2단계 인증(PAN-OS 7.0 이상에서 지원됨).
- 인증 포털 및 MFA 서버 프로파일을 사용한 API 기반 통합(Duo 인증 프록시 또는 SAML IdP 필요 없음 - PAN-OS 8.0 이상에서 지원됨).
- 온프레미스 서버용 SAML 통합(PAN-OS 8.0 이상에서 지원됨).

방화벽과 Duo 간에 SAML MFA를 활성화하여 방화벽에 대한 관리 액세스를 보호하려면 다음 단계를 따르세요.

- Duo Access Gateway로 SAML MFA용 Duo 구성
- Duo와 통합하도록 방화벽 구성
- Duo로 MFA 확인

### Duo Access Gateway로 SAML MFA용 Duo 구성

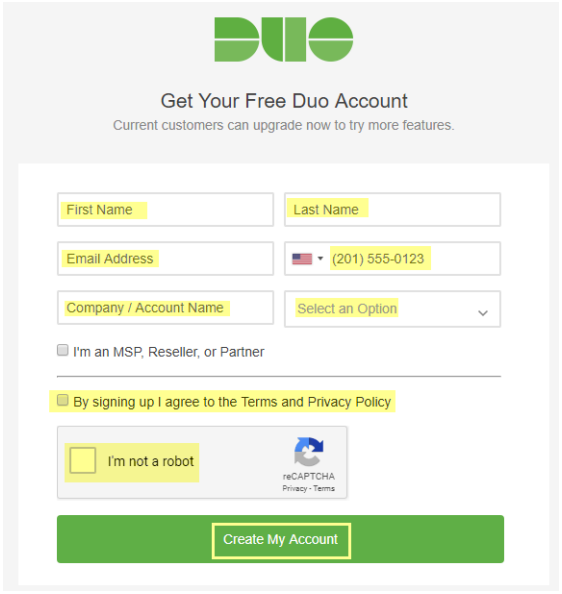
시작하기 전에 DMZ 영역의 온프레미스 서버에 DAG(DuoAccessGateway)를 배포했는지 확인하십시오.

Duo 관리자 계정을 생성하고 리소스에 액세스하기 전에 사용자를 인증하도록 Duo Access Gateway를 구성합니다.

 ©2023 Palo Alto Networks, Inc.

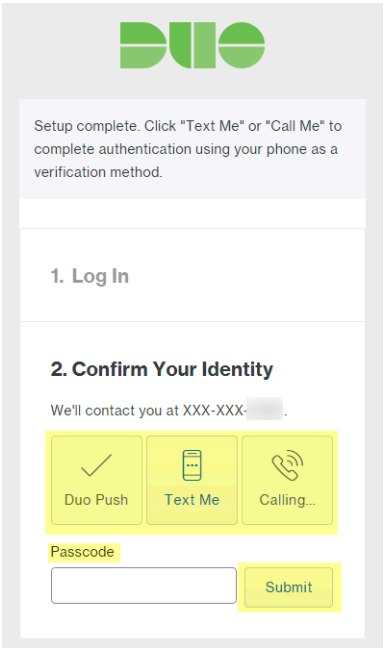
**STEP 1 |** Duo 관리자 계정을 만드세요.

1. Duo 계정 생성 페이지에서 이름, 성, 이메일 주소, 휴대전화 번호, 회사를 입력합니다**. /** 계정 이름, 조직의 직원 수를 선택합니다.
2. 약관 및 개인정보 보호정책에 동의하고 내 계정 생성에 대한 reCAPTCHA 챌린지에 응답합니다.




**STEP 2 |** Duo 관리자 계정을 확인하십시오.

1. 인증 확인 방법(듀오푸시, 문자메세지, 전화걸기**...**)을 선택하십시오.
2. 받은 암호를 입력하고 제출하여 계정을 확인하십시오.

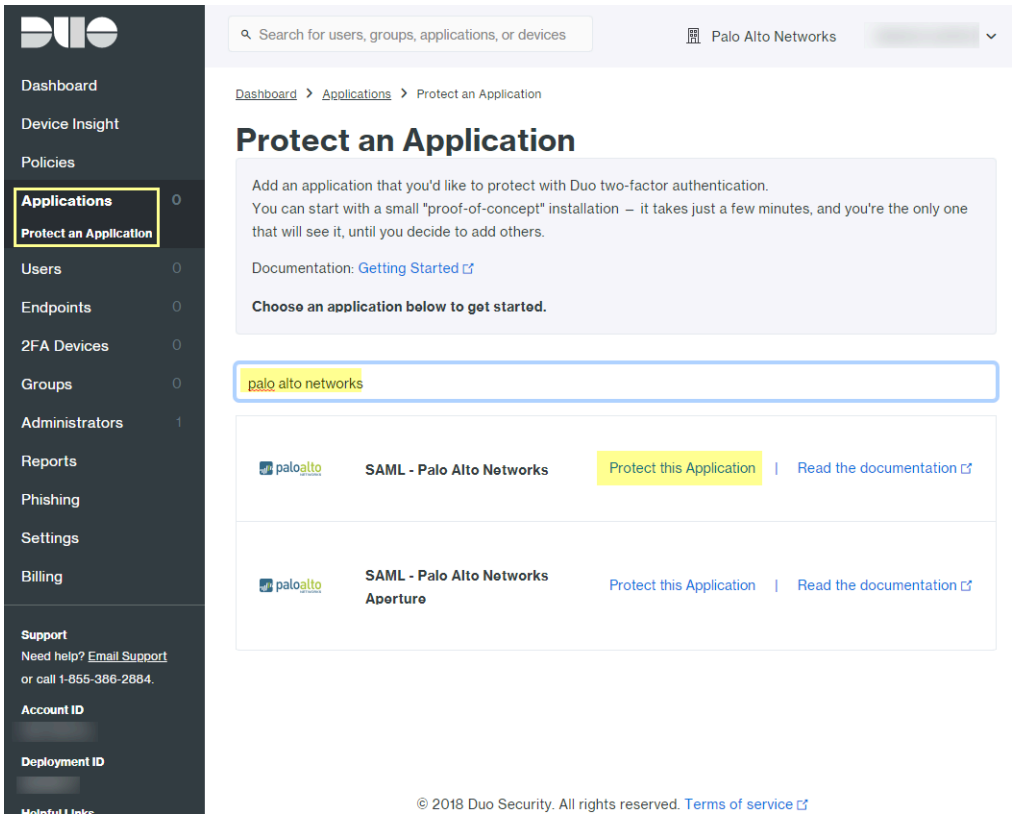



 ©2023 Palo Alto Networks, Inc.

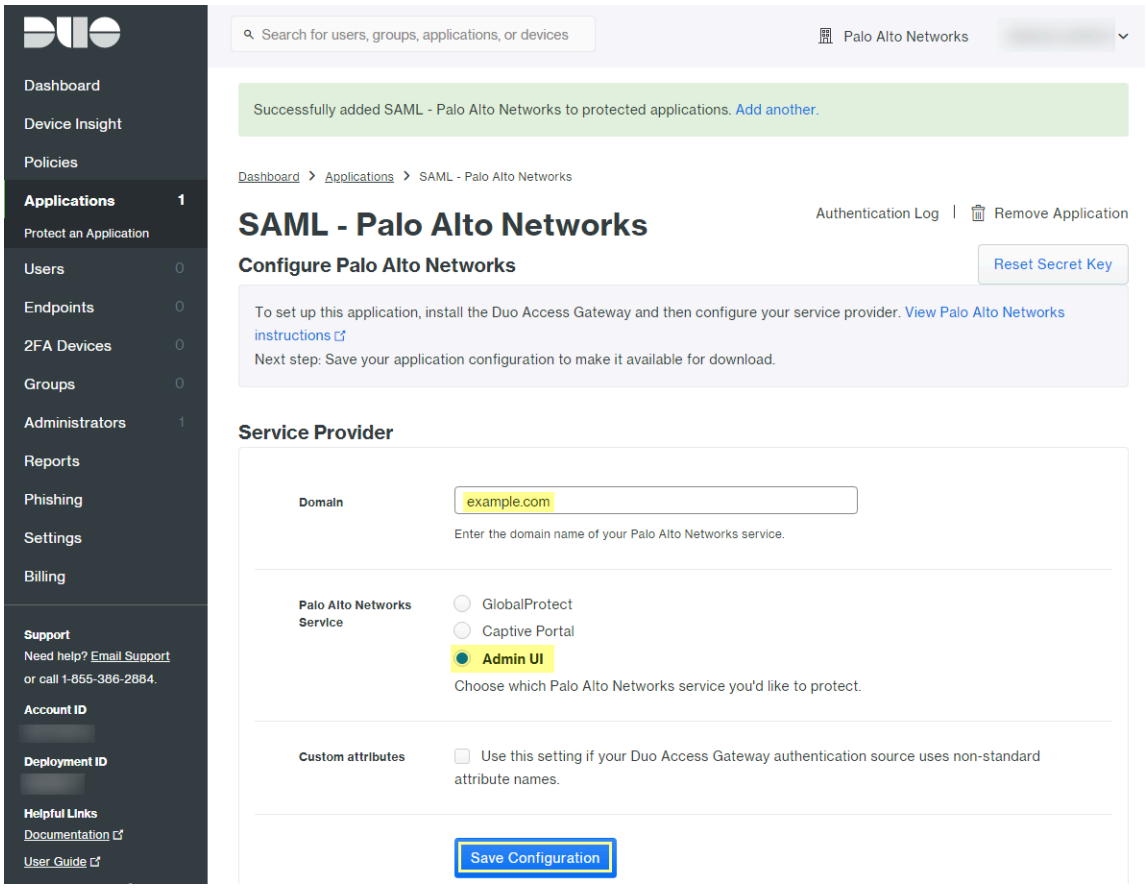
**STEP 3 |** SAML용으로 Duo 서비스를 구성합니다.

구성을 생성한 후 페이지 상단에서 구성 파일을 다운로드합니다.

1. Duo 관리자 패널에서 애플리케이션 > 애플리케이션 보호를 선택합니다.
2. **Palo Alto Networks**를 입력하여 애플리케이션을 검색합니다.
3. 결과 목록에서 **SAML - Palo Alto Networks**를 찾은 다음 이 애플리케이션 보호를 찾습니다.

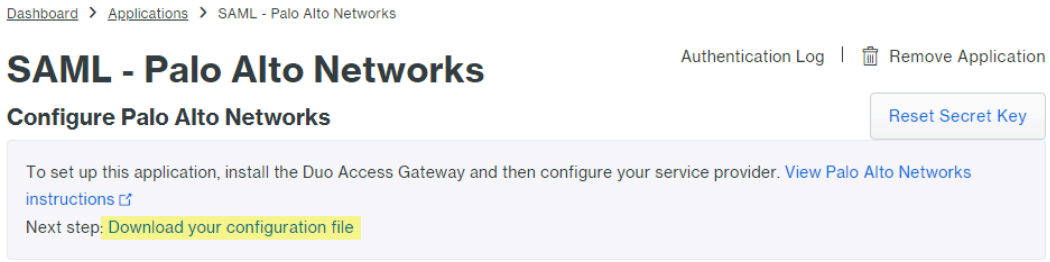



4. 도메인을 입력합니다.
5. **Palo Alto Networks Service**로 관리 **UI**를 선택합니다.
6. 정책 및 기타 설정 및 구성 저장을 구성합니다.




7. 구성 파일을 다운로드합니다.

   파일 다운로드 링크는 페이지 상단에 있습니다.




**STEP 4 |** 구성 파일을 Duo Access Gateway(DAG)에 업로드합니다.

1. DAG 관리 콘솔에서 애플리케이션을 선택합니다.
2. 파일 선택을 클릭하고 다운로드한 구성 파일을 선택한 다음 업로드합니다.
3. 설정 > 세션 관리에서 사용자 에이전트 바인딩을 비활성화한 다음 설정 저장을 비활성화합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** DAG 관리 콘솔에서 Active Directory 또는 OpenLDAP 서버를 인증 소스로 구성하고 메타데이터 파일을 다운로드합니다.

1. DAG 관리 콘솔에 로그인합니다.
2. 인증 소스 > 활성 소스 설정에서 소스 유형(Active Directory 또는 OpenLDAP)을 선택하고 활성 소스 설정을 선택합니다.
3. 소스 구성에서 속성을 입력합니다.
   - Active Directory의 경우 **`mail,sAMAccountName,userPrincipalName,objectGUID`**를 입력합니다.
   - OpenLDAP의 경우 **`mail,uid`**를 입력합니다.
   - 사용자 정의 속성의 경우 목록 끝에 추가하고 각 속성을 쉼표로 구분합니다. 기존 속성을 삭제하지 마십시오.
4. 설정을 저장하여 구성을 저장합니다.
5. 애플리케이션 > 메타데이터를 선택한 다음 **XML** 메타데이터 다운로드를 클릭하여 방화벽으로 가져오는 데 필요한 XML 메타데이터를 다운로드합니다.

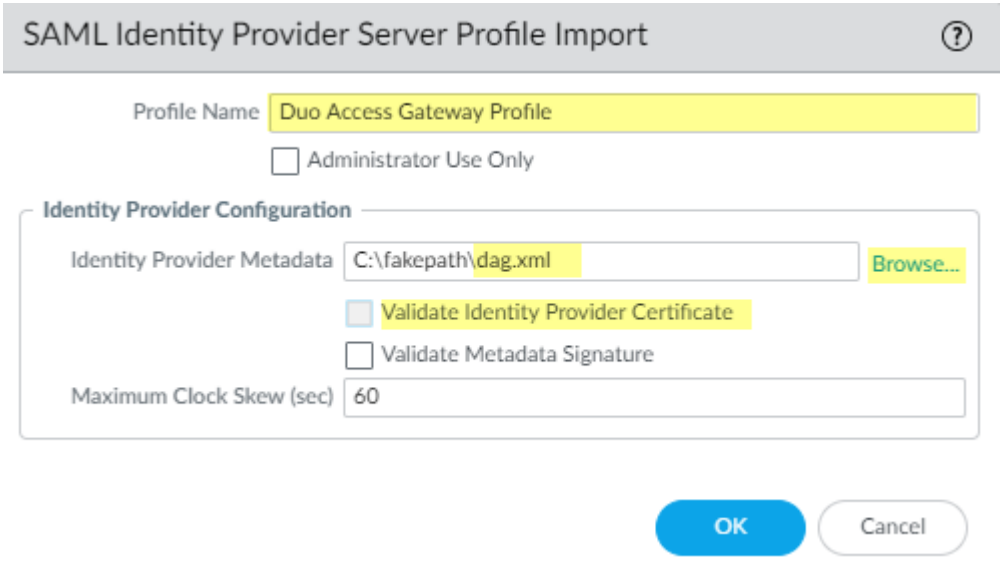
   파일 이름은 dag.xml입니다. 이 파일에는 방화벽으로 Duo 계정을 인증하기 위한 민감한 정보가 포함되어 있으므로 이 정보가 손상될 위험을 피하기 위해 파일을 안전한 위치에 보관해야 합니다.

## Duo와 통합하도록 방화벽 구성


©2023 Palo Alto Networks, Inc.

**STEP 1 |** Duo 메타데이터를 가져옵니다.

1. 방화벽 웹 인터페이스에 로그온합니다.
2. 방화벽에서 디바이스 > 서버 프로파일 > **SAML ID** 공급자 > 가져오기를 선택합니다.
3. 프로파일 이름을 입력합니다.
4. 찾아보기하여 **Identity Provider Metadata** 파일(**dag.xml**)을 찾습니다.
5. Duo Access Gateway가 IdP에 대한 서명 인증서로 자체 서명된 인증서를 제공하는 경우 **ID** 공급자 인증서를 확인할 수 없습니다. 이 경우 CVE-2020-2021에 대한 노출을 완화하기 위해 PAN-OS 10.2를 사용하고 있는지 확인하십시오.

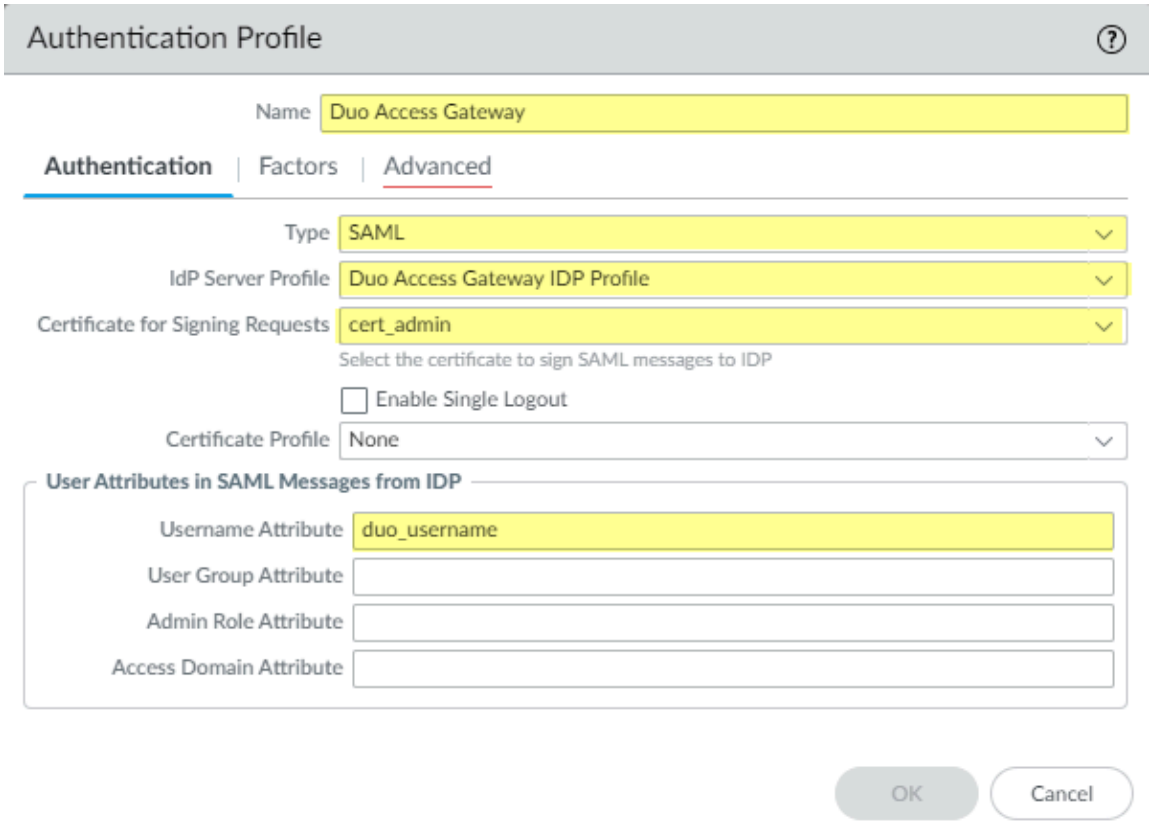



 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 인증 프로파일을 추가합니다.

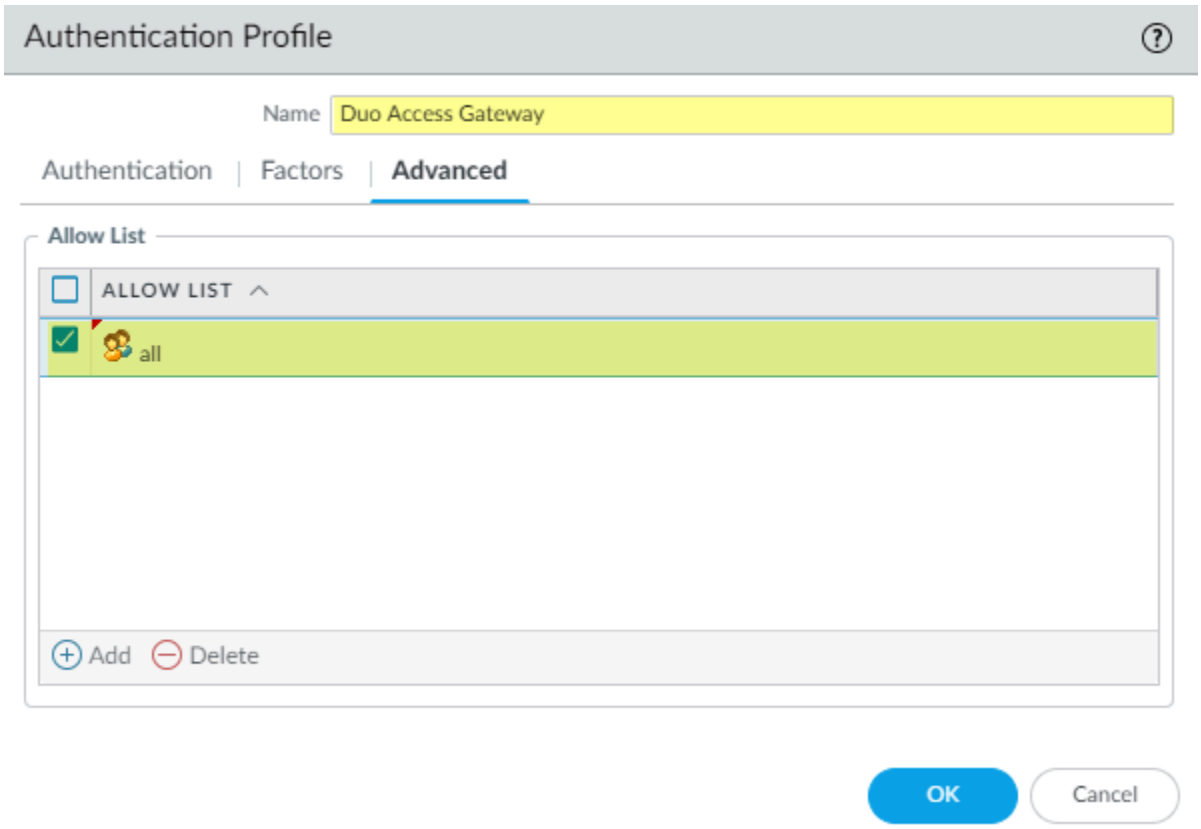
인증 프로파일은 Duo를 관리자 로그인 자격 증명의 유효성을 검사하는 ID 공급자로 허용합니다.

1. 인증 프로파일을 추가합니다.
2. 프로파일 이름을 입력합니다.
3. 인증 유형으로 **SAML**을 선택합니다.
4. **Duo Access Gateway** 프로파일을 **IdP** 서버 프로파일로 선택합니다.
5. 서명 요청용 인증서에 대해 Duo Access Gateway와의 SAML 통신에 사용할 인증서를 선택합니다.
6. 사용자 이름 속성으로 **duo_username**을 입력합니다.




7. 고급을 선택하여 허용 목록을 추가합니다.
8. 모두를 선택한 다음 확인을 클릭합니다.
9. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

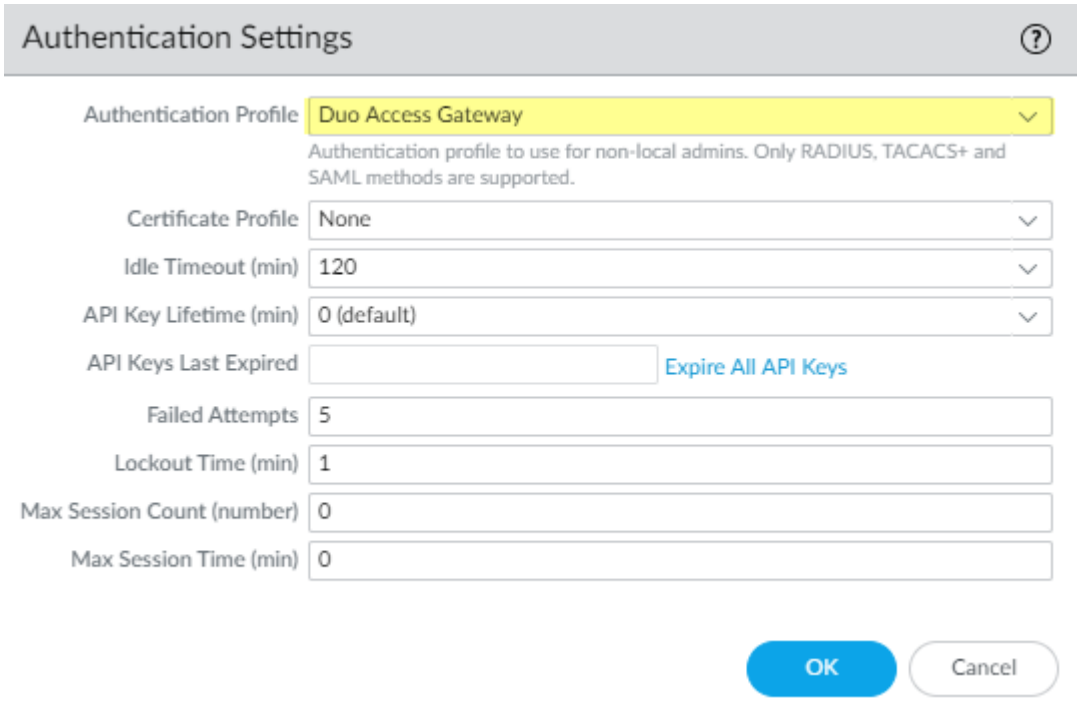




©2023 Palo Alto Networks, Inc.

**STEP 3 |** 방화벽이 Duo를 사용한 SAML 인증에 사용하는 인증 설정을 지정합니다.

1. 디바이스 > 설정 > 관리를 선택하고 인증 설정을 수정합니다.
2. **Duo Access Gateway**를 인증 프로파일로 선택한 다음 확인을 클릭합니다.



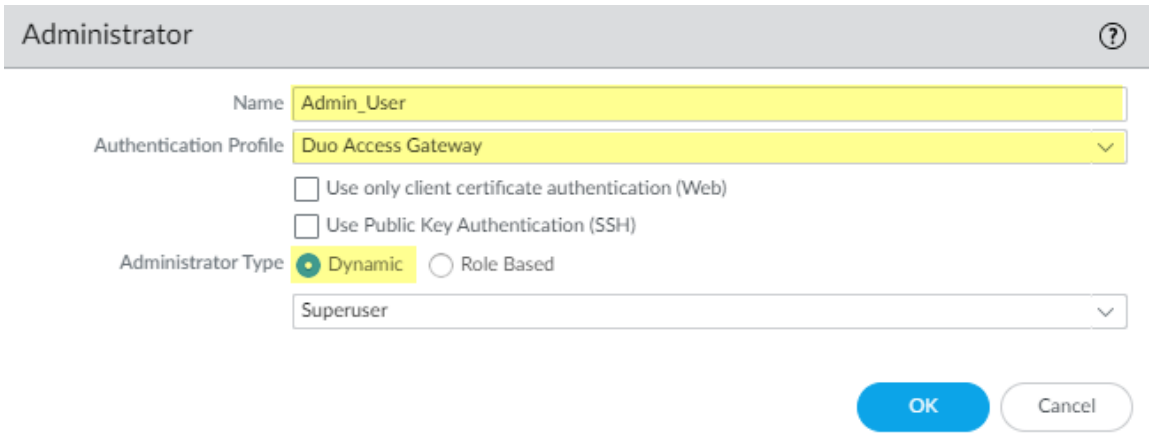

3. 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** Duo를 사용하여 방화벽에 인증할 관리자의 계정을 추가합니다.

1. 디바이스 > 관리자를 선택하고 계정을 추가합니다.
2. 사용자 이름을 입력합니다.
3. **Duo Access Gateway**를 인증 프로파일로 선택합니다.
4. 관리자 유형을 선택한 다음 확인을 클릭합니다.

   사용자에 대한 사용자 지정 역할을 사용하려면 역할 기반을 선택합니다. 그렇지 않으면 동적을 선택합니다. 관리자가 Duo에서 SSO를 사용하여 로그인하도록 하려면 모든 현재 관리자에게 인증 프로파일을 할당하십시오.




## Duo로 MFA 확인

**STEP 1 |** 방화벽의 웹 인터페이스에 로그인합니다.

**STEP 2 |** 싱글 사인온 사용 및 계속을 선택합니다.

**STEP 3 |** Duo Access Gateway 로그인 페이지에서 로그인 자격 증명을 입력합니다.

**STEP 4 |** 인증방법(푸시 알림, 전화 통화, 암호 입력)을 선택하십시오.

인증에 성공하면 방화벽 웹 인터페이스로 리디렉션됩니다.


©2023 Palo Alto Networks, Inc.

# SAML 인증 구성

SAML SSO(Single Sign-On) 및 SLO(Single Logout)를 구성하려면 방화벽과 IdP를 서로 등록하여 통신을 활성화해야 합니다. IdP가 등록 정보가 포함된 메타데이터 파일을 제공하는 경우 방화벽으로 가져와 IdP를 등록하고 IdP 서버 프로파일을 생성할 수 있습니다. 서버 프로파일은 IdP에 연결하는 방법을 정의하고 IdP가 SAML 메시지에 서명하는 데 사용하는 인증서를 지정합니다. 방화벽용 인증서를 사용하여 SAML 메시지에 서명할 수도 있습니다. 인증서 사용은 방화벽과 IdP 간의 통신을 보호하기 위한 요구 사항입니다.

Palo Alto Networks는 암호화된 SAML 어설션과 같은 대체 접근 방식 대신 모든 SAML 트랜잭션의 기밀성을 보장하기 위해 HTTPS를 요구합니다. SAML 트랜잭션에서 처리되는 모든 메시지의 무결성을 보장하기 위해 Palo Alto Networks는 모든 메시지에 암호화 방식으로 서명하는 디지털 인증서를 요구합니다.

다음 절차에서는 최종 사용자 및 방화벽 관리자에 대한 SAML 인증을 구성하는 방법을 설명합니다. Panorama 관리자에 대한 SAML 인증을 구성할 수도 있습니다.

***SSO***는 관리자와 ***GlobalProtect*** 및 인증 포털 최종 사용자가 사용할 수 있습니다**.** ***SLO***는 관리자와 ***GlobalProtect*** 최종 사용자가 사용할 수 있지만 인증 포털 최종 사용자는 사용할 수 없습니다**.**

관리자는 ***SAML***을 사용하여 방화벽 웹 인터페이스에 인증할 수 있지만 ***CLI***에는 인증할 수 없습니다**.**

**STEP 1 |** IdP 및 방화벽이 SAML 메시지에 서명하는 데 사용할 인증서를 가져옵니다.

인증서가 키 사용 속성을 지정하지 않으면 서명 메시지를 포함한 모든 사용이 기본적으로 허용됩니다. 이 경우 모든 방법으로 인증서를 얻을 수 있습니다.

인증서가 키 사용 속성을 지정하는 경우 속성 중 하나는 디지털 서명이어야 하며, 이는 방화벽이나 Panorama에서 생성한 인증서에서 사용할 수 없습니다. 이 경우 인증서를 가져와야 합니다.

- 방화벽이 **SAML** 메시지에 서명하는 데 사용하는 인증서 - 엔터프라이즈 CA(인증 기관) 또는 타사 CA에서 인증서를 가져옵니다.
- **IdP**가 **SAML** 메시지에 서명하는 데 사용하는 인증서(모든 배포에 필요) - IdP에서 인증서가 포함된 메타데이터 파일을 가져옵니다(다음 단계 참조). IdP 인증서는 다음 알고리즘으로 제한됩니다.

  공개 키 알고리즘 - RSA(1,024비트 이상) 및 ECDSA(모든 크기). FIPS/CC 모드의 방화벽은 RSA(2,048비트 이상) 및 ECDSA(모든 크기)를 지원합니다.

  서명 알고리즘 - SHA1, SHA256, SHA384 및 SHA512. FIPS/CC 모드의 방화벽은 SHA256, SHA384 및 SHA512를 지원합니다.

**STEP 2 |** SAML IdP 서버 프로파일을 추가합니다.

서버 프로파일은 IdP를 방화벽에 등록하고 연결 방법을 정의합니다.

이 예에서는 방화벽이 자동으로 서버 프로파일을 생성하고 연결, 등록 및 IdP 인증서 정보를 채울 수 있도록 IdP에서 SAML 메타데이터 파일을 가져옵니다.

***IdP***가 메타데이터 파일을 제공하지 않는 경우 디바이스 **>** 서버 프로파일 **>** ***SAML ID*** 공급자**,** 서버 프로파일 추가를 선택한 다음 정보를 수동으로 입력합니다***(***값은 ***IdP*** 관리자에게 문의***).***


©2023 Palo Alto Networks, Inc.

1. IdP에서 방화벽으로 메타데이터를 업로드할 수 있는 클라이언트 시스템으로 SAML 메타데이터 파일을 내보냅니다.

   파일에 지정된 인증서는 이전 단계에 나열된 요구 사항을 충족해야 합니다. 파일 내보내기에 대한 지침은 IdP 설명서를 참조하십시오.
2. 디바이스 > 서버 프로파일 > **SAML ID** 공급자 또는 Panorama™에서 **Panorama** > **Server** 프로파일 > **SAML ID** 공급자를 선택한 다음 메타데이터 파일을 방화벽으로 가져옵니다.
3. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
4. **ID** 공급자 메타데이터 파일을 찾습니다.
5. IdP 인증서의 해지 상태 및 선택적으로 신뢰 체인의 유효성을 검사하려면 **ID** 공급자 인증서 확인(기본값)을 선택합니다.

   이 옵션을 활성화하려면 인증 기관(CA)이 IdP의 서명 인증서를 발급해야 합니다. IdP의 서명 인증서를 발급한 CA가 있는 인증서 프로파일을 생성해야 합니다. 인증 프로파일에서 SAML 서버 프로파일과 인증서 프로파일을 선택하여 IdP 인증서를 확인합니다.

   IdP 서명 인증서가 자체 서명된 인증서인 경우 신뢰 체인이 없습니다. 따라서 이 옵션을 활성화할 수 없습니다. 방화벽은 항상 SAML 응답 또는 어설션의 서명을 ID 제공자 인증서 확인 옵션의 활성화 여부와 관계없이 구성한 **ID** 제공자 인증서에 대해 확인합니다. IdP가 자체 서명된 인증서를 제공하는 경우 PAN-OS 10.2를 사용하여 CVE-2020-2021에 대한 노출을 완화하고 있는지 확인하십시오.

   인증서의 유효성을 검사하여 손상되지 않았는지 확인하고 보안을 개선합니다.
6. 방화벽이 IdP 메시지를 검증하는 순간 IdP와 방화벽의 시스템 시간 사이에 허용되는 초 단위의 차이인 **Maximum Clock Skew**를 입력합니다(기본값은 60, 범위는 1~900). 차이가 이 값을 초과하면 인증이 실패합니다.
7. 확인을 클릭하여 서버 프로파일을 저장합니다.
8. 서버 프로파일 이름을 클릭하여 프로파일 설정을 표시합니다. 불러온 정보가 올바른지 확인하고 필요한 경우 편집하십시오.
9. IdP 메타데이터를 가져오든 IdP 정보를 수동으로 입력하든 항상 SAML ID 제공자의 서명 인증서가 서버 프로파일에 대한 **ID** 제공자 인증서이고 IdP가 서명된 SAML 응답, 주장 또는 둘 다를 전송하는지 확인하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 인증 프로파일을 구성합니다.

프로파일은 사용자 집합에 공통적인 인증 설정을 정의합니다.

1. 디바이스 > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. 유형을 **SAML**로 설정합니다.
4. 구성한 **IdP** 서버 프로파일을 선택합니다.
5. 서명 요청에 대한 인증서를 선택합니다.

   방화벽은 이 인증서를 사용하여 IdP에 보내는 메시지에 서명합니다. 엔터프라이즈 CA에서 생성한 인증서를 가져오거나 방화벽 또는 Panorama에서 생성된 루트 CA를 사용하여 인증서를 생성할 수 있습니다.
6. (선택 사항) 싱글 로그아웃을 활성화합니다(기본적으로 비활성화되어 있음).
7. 방화벽이 **IdP** 인증서의 유효성을 검사하는 데 사용할 인증서 프로파일을 선택합니다.
8. IdP 메시지가 사용자를 식별하는 데 사용하는 사용자 이름 속성을 입력합니다(기본 사용자 이름).

   사용자에 대한 동적 관리자 역할을 사전 정의할 때 소문자를 사용하여 역할을 지정하십시오(예: ***superreader***가 아니라 ***superreader*** 입력). *IdP ID* 저장소에서 관리자 권한 부여를 관리하는 경우 관리자 역할 속성 및 액세스 도메인 속성도 지정하십시오.
9. 고급을 선택한 다음 이 인증 프로파일로 인증할 수 있는 사용자 및 사용자 그룹을 추가합니다.
10. 확인을 클릭하여 인증 프로파일을 저장합니다.

**STEP 4 |** 인증이 필요한 방화벽 애플리케이션에 인증 프로파일을 할당합니다.

1. 인증 프로파일 할당:
   - 방화벽에서 로컬로 관리하는 관리자 계정. 이 예에서는 이 절차의 뒷부분에서 SAML 구성을 확인하기 전에 방화벽 관리자 계정을 구성합니다.
   - IdP ID 저장소에서 외부적으로 관리하는 관리자 계정입니다. 디바이스 > 설정 > 관리를 선택한 다음 인증 설정을 편집한 다음 구성한 인증 프로파일을 선택합니다.
   - 최종 사용자가 인증 포털을 통해 액세스하는 서비스 및 애플리케이션을 보호하는 인증 정책 규칙입니다. 인증 정책 구성을 참조하십시오.
   - 최종 사용자가 액세스하는 GlobalProtect 포털 및 게이트웨이.
2. 변경 사항을 커밋합니다.

   방화벽은 SAML IdP 서버 프로파일에 할당한 **IdP** 인증서의 유효성을 검사합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** SAML 메타데이터 파일을 생성하여 IdP에 방화벽 애플리케이션(관리 액세스, 인증 포털 또는 GlobalProtect)을 등록합니다.

1. 디바이스 > 인증 프로파일을 선택한 다음 구성한 인증 프로파일의 인증 열에서 메타데이터를 클릭합니다.
2. 서비스 드롭다운에서 등록할 애플리케이션을 선택합니다.
   - 관리(기본값) - 웹 인터페이스에 대한 관리 액세스입니다.
   - 인증 포털 - 인증 포털을 통해 서비스 및 애플리케이션에 대한 최종 사용자 액세스.
   - 전역 보호 - GlobalProtect를 통해 서비스 및 애플리케이션에 대한 최종 사용자 액세스.
3. (인증 포털 또는 GlobalProtect만 해당) **Vsysname Combo**의 경우 인증 포털 설정 또는 GlobalProtect 포털이 정의된 가상 시스템을 선택합니다.
4. 등록할 애플리케이션에 따라 인터페이스, IP 주소 또는 호스트 이름을 입력합니다.
   - 관리 - 관리 선택에서 인터페이스(기본값)를 선택한 다음 웹 인터페이스에 대한 관리 액세스를 위해 활성화된 인터페이스를 선택합니다. 기본 선택은 MGT 인터페이스의 IP 주소입니다.
   - 인증 포털 - **IP** 호스트 이름에 대해 리디렉션 호스트의 IP 주소 또는 호스트 이름을 입력합니다(디바이스 > 사용자 식별 > 인증 포털 설정 참조).
   - 전역 보호 - **IP** 호스트 이름에 GlobalProtect 포털 또는 게이트웨이의 호스트 이름 또는 IP 주소를 입력합니다.
5. 확인을 클릭하고 메타데이터 파일을 클라이언트 시스템에 저장합니다.
6. 메타데이터 파일을 IdP 서버로 가져와 방화벽 애플리케이션을 등록합니다. 지침은 IdP 설명서를 참조하십시오.

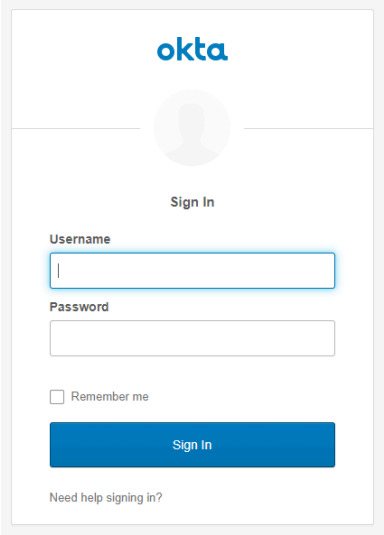
 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 사용자가 SAML SSO를 사용하여 인증할 수 있는지 확인합니다.

예를 들어 SAML이 로컬 관리자 계정을 사용하여 웹 인터페이스에 액세스하기 위해 작동하는지 확인하려면 다음을 수행합니다.

1. 방화벽 웹 인터페이스의 URL로 이동합니다.
2. **Single Sign-On(SSO)** 사용을 클릭합니다.
3. 관리자의 사용자 이름을 입력합니다.
4. 계속을 클릭합니다.

   방화벽은 로그인 페이지를 표시하는 IdP에 인증하도록 리디렉션합니다. 예:




5. SSO 사용자 이름과 암호를 사용하여 로그인합니다.

   IdP에서 성공적으로 인증하면 웹 인터페이스를 표시하는 방화벽으로 다시 리디렉션됩니다.
6. 방화벽 관리자 계정을 사용하여 다른 SSO 애플리케이션에 대한 액세스를 요청하십시오.

   액세스 성공은 SAML SSO 인증이 성공했음을 나타냅니다.

 ©2023 Palo Alto Networks, Inc.

# Kerberos Single Sign-On (SSO) 구성

Palo Alto Networks 방화벽 및 Panorama는 Kerberos V5 Single Sign-On(SSO)을 지원하여 관리자를 웹 인터페이스에 인증하고 최종 사용자는 인증 포털에 대해 인증합니다. Kerberos SSO를 사용하도록 설정한 경우 사용자는 네트워크에 처음 액세스할 때만 로그인해야 합니다(예: Microsoft Windows에 로그인). 이 초기 로그인 후 사용자는 SSO 세션이 만료될 때까지 다시 로그인하지 않고도 네트워크의 모든 브라우저 기반 서비스(예: 방화벽 웹 인터페이스)에 액세스할 수 있습니다.

**STEP 1 |** Kerberos 키탭을 생성합니다.

keytab은 방화벽의 사용자 이름과 암호를 포함하는 파일이며 SSO 프로세스에 필요합니다. 인증 프로파일 및 시퀀스에서 Kerberos를 구성하면 방화벽이 먼저 Kerberos SSO 호스트 이름을 확인합니다. 호스트 이름을 제공하면 방화벽은 keytab에서 호스트 이름과 일치하는 서비스 사용자 이름을 검색하고

 ©2023 Palo Alto Networks, Inc.

해당 키탭(keytab)만 복호화에 사용합니다. 호스트 이름을 제공하지 않으면 방화벽은 Kerberos를 사용하여 성공적으로 인증할 수 있을 때까지 인증 순서의 각 키탭(keytab)을 시도합니다.

*Kerberos SSO* 호스트 이름이 방화벽으로 전송된 요청에 포함되어 있으면 호스트 이름이 키탭*(keytab)*의 서비스 사용자 이름과 일치해야 합니다. 그렇지 않으면 *Kerberos* 인증 요청이 전송되지 않습니다.

1. Active Directory 서버에 로그인하고 명령 프롬프트를 엽니다.
2. 다음 명령을 입력하여 GlobalProtect 또는 인증 포털에 대한 SPN(서비스 사용자 이름)을 <*service_account_username*> 등록합니다. 여기서 <*portal_fqdn*> 변수는 변수입니다.
   **setspn -s HTTP/<*portal_fqdn*> <*service_account_username*>**
3. 방화벽에 대한 Kerberos 계정을 만듭니다. 단계는 Kerberos 설명서를 참조하십시오.
4. KDC에 로그인하고 명령 프롬프트를 엽니다.
5. 다음 명령을 입력합니다. 여기서 <*portal_fqdn*>, <*kerberos_realm*>, <*netbios_name*>, <*service_account_username*>, <*password*>, <*filename*> 및 <*algorithm*>은(는) 변수입니다.
   **ktpass /princ HTTP <*portal_fqdn*>@<*kerberos_realm*> /mapuser <*netbios_name*>\<*service_account_username*> /pass <*password*>/out <*filename*>.keytab /ptype KRB5_NT_PRINCIPAL /crypto <*algorithm*>**

   <*kerberos_realm*> 값은 모두 대문자여야 합니다*(*예: ***ad1.example.com***이 아니라 ***AD1.EXAMPLE.COM*** 입력*)*.

   방화벽이 *FIPS/CC* 모드에 있는 경우 알고리즘은 반드시 ***aes128-cts-hmac-***샤***1-96*** 또는 ***aes256-cts-hmac-sha1-96***이어야 합니다. 그렇지 않으면 ***des3-cbc-sha1*** 또는 ***arcfour-hmac***을 사용할 수도 있습니다. *AES(*고급 암호화 표준*)* 알고리즘을 사용하려면 *KDC*의 기능 수준이 *Windows Server 2012* 이상이어야 하며 방화벽 계정에 대해 *AES* 암호화를 사용하도록 설정해야 합니다.

   *keytab*의 알고리즘은 *TGS*가 클라이언트에 발행하는 서비스 티켓의 알고리즘과 일치해야 합니다. *Kerberos* 관리자는 서비스 티켓이 사용하는 알고리즘을 결정합니다.

**STEP 2 |** 인증 프로파일 및 시퀀스를 구성하여 사용자 집합에 공통적인 Kerberos 설정 및 기타 인증 옵션을 정의합니다.

- **Kerberos** 영역(일반적으로 영역이 대문자인 경우를 제외하고 사용자의 DNS 도메인)을 입력합니다.
- 방화벽에 대해 만든 **Kerberos** 키탭**(Keytab)**을 가져옵니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 인증이 필요한 방화벽 애플리케이션에 인증 프로파일을 할당합니다.

- 웹 인터페이스에 대한 관리 액세스 - 방화벽 관리자 계정을 구성하고 구성한 인증 프로파일을 할당합니다.
- 서비스 및 애플리케이션에 대한 최종 사용자 액세스 - 구성한 인증 프로파일을 인증 적용 개체에 할당합니다. 개체를 구성할 때 인증 방법을 브라우저 챌린지로 설정하십시오. 인증 정책 규칙에 개체를 할당합니다. 최종 사용자에 대한 인증을 구성하는 전체 절차는 인증 정책 구성을 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# Kerberos 서버 인증 구성

Kerberos를 사용하여 Active Directory 도메인 컨트롤러 또는 Kerberos V5 호환 인증 서버에 대해 최종 사용자 및 방화벽 또는 Panorama 관리자를 기본적으로 인증할 수 있습니다. 이 인증 방법은 대화형이므로 사용자가 사용자 이름과 암호를 입력해야 합니다.

인증에 ***Kerberos*** 서버를 사용하려면 ***IPv4*** 주소를 통해 서버에 액세스할 수 있어야 합니다. ***IPv6*** 주소는 지원되지 않습니다.

**STEP 1 |** Kerberos 서버 프로파일을 추가합니다.

프로파일은 방화벽이 Kerberos 서버에 연결하는 방법을 정의합니다.

1. Panorama™에서 디바이스 > 서버 프로파일 > **Kerberos** 또는 **Panorama** > **Server** 프로파일 > **Kerberos**를 선택한 다음 서버 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. 각 서버를 추가하고 **Kerberos** 서버의 이름(서버 식별용), IPv4 주소 또는 FQDN, 서버와의 통신을 위한 선택적 포트 번호(기본값 88)를 지정합니다.

   ***FQDN*** 주소 개체를 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소를 적용하려면 변경 사항을 커밋해야 합니다.
4. 확인을 클릭하여 변경 사항을 프로파일에 저장합니다.

**STEP 2 |** 서버 프로파일을 인증 프로파일 및 시퀀스 구성에 할당합니다.

인증 프로파일은 사용자 집합에 공통적인 인증 설정을 정의합니다.

**STEP 3 |** 인증이 필요한 방화벽 애플리케이션에 인증 프로파일을 할당합니다.

- 웹 인터페이스에 대한 관리 액세스 - 방화벽 관리자 계정을 구성하고 구성한 인증 프로파일을 할당합니다.
- 서비스 및 애플리케이션에 대한 최종 사용자 액세스 - 구성한 인증 프로파일을 인증 적용 개체에 할당하고 개체를 인증 정책 규칙에 할당합니다. 최종 사용자에 대한 인증을 구성하는 전체 절차는 인증 정책 구성을 참조하십시오.

**STEP 4 |** 방화벽이 인증 서버 연결을 테스트하여 사용자를 인증할 수 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# TACACS+ 인증 구성

최종 사용자와 방화벽 또는 Panorama 관리자에 대해 TACACS+ 인증을 구성할 수 있습니다. TACACS+ 서버를 사용하여 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여(역할 및 액세스 도메인 할당)를 관리할 수도 있습니다. 모든 사용자에 대해 방화벽 또는 Panorama가 서버에 연결하는 방법을 정의하는 TACACS+ 서버 프로파일을 구성해야 합니다. 그런 다음 공통 인증 설정이 필요한 각 사용자 집합의 인증 프로파일에 서버 프로파일을 할당합니다. 인증 프로파일로 수행하는 작업은 TACACS+ 서버가 인증하는 사용자에 따라 다릅니다.

- 최종 사용자 - 인증 적용 개체에 인증 프로파일을 할당하고 개체를 인증 정책 규칙에 할당합니다. 전체 절차는 인증 정책 구성을 참조하십시오.
- 방화벽 또는 **Panorama**에서 로컬로 관리되는 권한이 있는 관리 계정 - 방화벽 관리자 또는 Panorama 관리자 계정에 인증 프로파일을 할당합니다.
- **TACACS+** 서버에서 관리되는 권한 부여가 있는 관리 계정 - 다음 절차에서는 방화벽 관리자를 위한 TACACS+ 인증 및 권한 부여를 구성하는 방법을 설명합니다. Panorama 관리자의 경우 PanoramaAdministrators에 대한 TACACS+ 인증 구성을 참조하십시오.

**STEP 1 |** TACACS+ 서버 프로파일을 추가합니다.

프로파일은 방화벽이 TACACS+ 서버에 연결하는 방법을 정의합니다.

1. Panorama™에서 디바이스 > 서버 프로파일 > **TACACS+** 또는 **Panorama** > 서버 프로파일 > **TACAS+**를 선택한 다음 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. (선택 사항) 관리자에 대한 액세스를 제한하려면 관리자만 사용을 선택합니다.
4. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–20).
5. 방화벽이 TACACS+ 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.

   *TACACS+* 서버가 해당 프로토콜을 지원하는 경우 ***CHAP***를 선택하십시오. ***PAP***보다 더 안전합니다.
6. 각 TACACS+ 서버를 추가하고 다음을 입력합니다.
   - 서버를 식별하는 이름
   - **TACACS+** 서버 IP 주소 또는 FQDN. FQDN 주소 개체를 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소에 대한 변경 사항을 적용해야 합니다.
   - **Secret**/**Confirm Secret**(사용자 이름과 암호를 암호화하는 키)
   - 인증 요청을 위한 서버 포트(기본값: 49)
7. 확인을 클릭하여 서버 프로파일을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** TACACS+ 서버 프로파일을 인증 프로파일에 할당합니다.

인증 프로파일은 사용자 집합에 공통적인 인증 설정을 정의합니다.

1. 디바이스 > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. 유형을 **TACACS+**로 설정합니다.
4. 구성한 서버 프로파일을 선택합니다.
5. TACACS+ 서버에 정의된 VSA에서 사용자 그룹 정보를 수집하려면 TACACS+에서 사용자 그룹 검색을 선택합니다.

   방화벽은 인증 프로파일 허용 목록에서 지정한 그룹과 그룹 정보와 일치합니다.
6. 고급을 선택한 다음 허용 목록에서 이 인증 프로파일로 인증할 수 있는 사용자와 그룹을 추가합니다.
7. 확인을 클릭하여 인증 프로파일을 저장합니다.

**STEP 3 |** 모든 관리자에 대한 인증 프로파일을 사용하도록 방화벽을 구성합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 구성한 인증 프로파일을 선택한 다음 확인을 클릭합니다.

**STEP 4 |** 관리자에 대한 권한 부여 설정을 정의하는 역할 및 액세스 도메인을 구성합니다.

TACACS+ 서버에서 TACACS+ VSA를 이미 정의한 경우 방화벽의 역할 및 액세스 도메인에 지정하는 이름은 VSA 값과 일치해야 합니다.

1. 관리자가 사전 정의된(동적) 역할 대신 사용자 지정 역할을 사용하는 경우 관리자 역할 프로파일을 구성합니다.
2. 방화벽에 두 개 이상의 가상 시스템이 있는 경우 액세스 도메인 구성 - 디바이스 > 액세스 도메인을 선택하고 액세스 도메인을 추가하고 다음을 입력합니다. 이름을 입력하여 액세스 도메인을 식별하고 관리자가 액세스할 각 가상 시스템을 추가한 다음 확인을 클릭합니다.

**STEP 5 |** 방화벽에서 변경 내용을 활성화하기 위해 변경 내용을 커밋합니다.

**STEP 6 |** 관리자를 인증하고 권한을 부여하도록 TACACS+ 서버를 구성합니다.

다음 단계를 수행하기 위한 특정 지침은 TACACS+ 서버 설명서를 참조하십시오.

1. 방화벽 IP 주소 또는 호스트 이름을 TACACS+ 클라이언트로 추가합니다.
2. 관리자 계정을 추가합니다.

   인증 프로토콜로 ***CHAP***를 선택한 경우 역으로 암호화된 암호로 계정을 정의해야 합니다. 그렇지 않으면 ***CHAP*** 인증이 실패합니다.
3. 각 관리자의 역할, 액세스 도메인 및 사용자 그룹에 대해 TACACS+ VSA를 정의합니다.

   사용자에 대한 동적 관리자 역할을 사전 정의하는 경우 하위 사례를 사용하여 역할을 지정합니다(예: ***SuperUser***가 아닌 운용  관리자를 입력).

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** TACACS+ 서버가 관리자에 대한 인증 및 권한 부여를 수행하는지 확인합니다.

1. TACACS+ 서버에 추가한 관리자 계정을 사용하여 방화벽 웹 인터페이스에 로그인합니다.
2. 관리자와 연결된 역할에 대해 허용되는 웹 인터페이스 페이지만 액세스할 수 있는지 확인합니다.
3. 모니터, 정책 및 개체 탭에서 관리자와 연결된 액세스 도메인에 대해 허용되는 가상 시스템만 액세스할 수 있는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.

# RADIUS 인증 구성

최종 사용자 및 방화벽 또는 Panorama 관리자를 위해 RADIUS 인증을 구성할 수 있습니다. 관리자의 경우 RADIUS를 사용하여 공급업체별 특성(VSA)을 정의하여 권한 부여(역할 및 도메인 할당에 액세스)를 관리할 수 있습니다. 또한 RADIUS를 사용하여 관리자 및 최종 사용자를 위한 MFA(다단계 인증)를 구현할 수도 있습니다. RADIUS 인증을 사용하도록 설정하려면 방화벽 또는 Panorama가 서버에 연결하는 방식을 정의하는 RADIUS 서버 프로파일을 구성해야 합니다(아래 1단계 참조). 그런 다음 공통 인증 설정이 필요한 각 사용자 집합에 대해 서버 프로파일을 인증 프로파일에 할당합니다(아래 5단계 참조). 인증 프로파일로 수행하는 일은 RADIUS 서버가 인증하는 사용자에 따라 달라집니다.

- 최종 사용자 - 인증 적용 개체에 인증 프로파일을 할당하고 개체를 인증 정책 규칙에 할당합니다. 전체 절차에 대해 인증 정책 구성을 참조하십시오.

  또한 클라이언트 시스템을 구성하여 ***GlobalProtect*** 포털 또는 게이트웨이에 인증 프로파일을 할당하여 ***RADIUS*** 공급 업체별 특성***(***VSA***)***을 ***RADIUS*** 서버에 보낼 수도 있습니다**.** 그런 다음 ***RADIUS*** 관리자는 이러한 ***VSA***를 기반으로 관리 작업을 수행할 수 있습니다**.**

- 방화벽 또는 **Panorama**에서 로컬로 관리되는 권한 부여가 있는 관리 계정-방화벽 관리자 또는 Panorama 관리자 계정에 인증 프로파일을 할당합니다.
- **RADIUS** 서버에서 관리되는 권한 부여가 있는 관리 계정-다음 절차는 방화벽 관리자에 대한 RADIUS 인증 및 권한 부여를 구성하는 방법을 설명합니다. Panorama 관리자의 경우 Panorama 관리자에 대한 RADIUS 인증 구성을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** RADIUS 서버 프로파일을 추가합니다.

프로파일은 방화벽이 RADIUS 서버에 연결하는 방식을 정의합니다.

1. 디바이스 > 서버 프로파일 > **RADIUS** 또는 **Panorama** > 서버 프로파일 > 을 선택합니다**.** **Panorama™**에서 **RADIUS** 및 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. (선택 사항) 관리자에 대한 액세스를 제한하려면 관리자만 사용을 선택합니다.
4. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–120).

   서버 프로파일을 사용하여 방화벽을 *MFA* 서비스와 통합하는 경우 사용자에게 인증할 수 있는 충분한 시간을 제공하는 간격을 입력합니다**.** 예를 들어 *MFA* 서비스가 *OTP(*일회성 암호*)*를 입력하라는 메시지를 표시하는 경우 사용자는 엔드포인트 디바이스에서 *OTP*를 확인한 다음 *MFA* 로그인 페이지에 *OTP*를 입력해야 합니다**.**
5. 재시도 횟수를 입력합니다.
6. 방화벽이 RADIUS 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **PEAP-MSCHAPv2**)을 선택합니다.

   다단계 인증(MFA) 환경에서 사용자를 인증하는 데 사용할 요인에 따라 적절한 인증 프로토콜을 선택합니다.

   - 사용자 이름**,** 암호 및 푸시**(**자동으로 트리거된 대역 외 요청**)**: 모든 인증 프로토콜에서 지원
   - 푸시**,** 암호**,** 토큰 및 **PIN(**암호**,** 토큰 또는 **PIN**이 함께 제공되는 경우**)**: PAP, PEAP with GTC, EAP-TTLS with PAP
   - 사용자 이름**,** 암호**,** 토큰**, PIN,** 질문 응답**(**암호**,** 토큰 또는 **PIN**이 함께 제공된 경우**)** : GTC에서 PAP 및 PEAP 지원

   EAP 인증 방법(PEAP-MSCHAPv2, GTC를 사용하는 PEAP 또는 PAP이 있는 EAP)을 선택하면 RADIUS 서버가 전송 레이어 보안(TLS) 1.1 이상을 지원하고 RADIUS 서버의 루트 및 중간 인증서 기관(C)이 RADIUS 서버 프로파일과 연결된 인증서 프로파일에 포함되어 있는지 확인합니다. EAP 메서드를 선택한 다음 올바르게 구성된 인증서 프로파일을 RADIUS 프로파일과 연결하지 않으면 인증이 실패합니다.
7. 각 RADIUS 서버를 추가하고 다음을 입력합니다.
   - 서버를 식별하는 이름
   - **RADIUS** 서버 IP 주소 또는 FQDN. FQDN을 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소가 적용되기 위해 변경을 커밋해야 합니다.
   - 비밀/비밀 확인 비밀은 암호를 암호화하는 열쇠이며 길이는 최대 64자일 수 있습니다.
   - 인증 요청을 위한 서버 포트(기본값은 1812)
8. 확인을 클릭하여 서버 프로파일을 저장합니다.

중복성을 위해 방화벽을 사용할 시퀀스에 여러 RADIUS 서버를 추가합니다. EAP 메서드를 선택한 경우 인증 시퀀스를 구성하여 사용자가 인증 과제에 성공적으로 응답할 수 있는지 확인합니다. EAP를 사용하는 대체 인증 방법은 없습니다. 사용자가 인증 챌린지에 실패하고 다른 인증 방법을 허용하는 인증 시퀀스를 구성하지 않은 경우 인증이 실패합니다.

**STEP 2 |** GlobalProtect에서 PEAP-MSCHAPv2를 사용하는 경우 만료 후 사용자가 암호를 변경할 수 있도록 허용하여 GlobalProtect 사용자가 만료된 암호를 변경하여 로그인할 수 있도록 허용합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** (PEAP-MSCHAPv2, GTC를 사용한 PEAP 또는 PAP전용 EAP-TTLS) 서버로 인증한 후 생성된 외부 터널에서 사용자의 ID를 익명으로 만들고 외부 **ID**를 익명으로 확인하려면 선택합니다.

> 전체 체인이 익명 사용자에 대한 액세스를 허용하도록 ***RADIUS*** 서버를 구성해야 합니다. 일부 ***RADIUS*** 서버 구성은 익명 외부 ***IP***를 지원하지 않을 수 있으며 옵션을 지워야 할 수 있습니다. 삭제되면 ***RADIUS*** 서버는 사용자 이름을 지우는 텍스트로 전송합니다.

**STEP 4 |** EAP 인증 방법을 선택하는 경우인증서 프로파일을 선택합니다.

**STEP 5 |** RADIUS 서버 프로파일을 인증 프로파일에 할당합니다.

인증 프로파일은 사용자 집합에 공통적인 인증 설정을 정의합니다.

1. 디바이스 > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 인증 프로파일을 식별할 이름을 입력합니다.
3. 유형을 **RADIUS**로 설정합니다.
4. 구성한 서버 프로파일을 선택합니다.
5. **RADIUS**에서 사용자 그룹 검색을 선택하여 RADIUS 서버에 정의된 VSA에서 사용자 그룹 정보를 수집합니다.

   방화벽은 인증 프로파일 허용 목록에서 지정한 그룹과 그룹 정보와 일치합니다.
6. 고급을 선택한 다음 허용 목록에서 이 인증 프로파일로 인증할 수 있는 사용자와 그룹을 추가합니다.
7. 확인을 클릭하여 인증 프로파일을 저장합니다.

**STEP 6 |** 모든 관리자에 대한 인증 프로파일을 사용하도록 방화벽을 구성합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 구성한 인증 프로파일을 선택한 다음 확인을 클릭합니다.

**STEP 7 |** 관리자에 대한 권한 부여 설정을 정의하는 역할 및 액세스 도메인을 구성합니다.

RADIUS 서버에서 RADIUS VSA를 이미 정의한 경우 방화벽의 역할 및 액세스 도메인에 대해 지정한 이름이 VSA 값과 일치해야 합니다.

1. 관리자가 사전 정의된(동적) 역할 대신 사용자 지정 역할을 사용하는 경우 관리자 역할 프로파일을 구성합니다.
2. 방화벽에 두 개 이상의 가상 시스템이 있는 경우 액세스 도메인을 구성합니다.

   **1.** 디바이스 > 액세스 도메인을 선택한 다음 액세스 도메인을 추가하고 이름을 입력하여 액세스 도메인을 식별합니다.

   **2.** 관리자가 액세스할 각 가상 시스템을 추가한 다음 확인을 클릭합니다.

**STEP 8 |** 방화벽에서 변경 내용을 활성화하기 위해 변경 내용을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** RADIUS 서버를 구성하여 관리자를 인증하고 승인합니다.

다음 단계를 수행할 특정 지침은 RADIUS 서버 설명서를 참조하십시오.

1. 방화벽 IP 주소 또는 호스트 이름을 RADIUS 클라이언트로 추가합니다.
2. 관리자 계정을 추가합니다.

   ***RADIUS*** 서버 프로파일이 ***CHAP***를 인증 프로토콜로 지정하는 경우 가역적으로 암호화된 암호로 계정을 정의해야 합니다. 그렇지 않으면 ***CHAP*** 인증이 실패합니다.
3. 방화벽에 대한 공급업체 코드(25461)를 정의하고 각 관리자의 역할, 액세스 도메인 및 사용자 그룹에 대한 RADIUS VSA를 정의합니다.

   사용자에 대한 동적 관리자 역할을 사전 정의하는 경우 하위 사례를 사용하여 역할을 지정합니다(예: **SuperUser**가 아닌 **운용 관리자**를 입력).

   ***ACS***에서 고급 공급업체 옵션을 구성할 때 공급업체 길이 필드 크기와 공급업체 유형 필드 크기를 모두 ***1***로 설정해야 합니다. 그렇지 않으면 인증이 실패합니다.
4. EAP 방법을 선택한 경우 방화벽은 클라이언트가 아닌 서버의 유효성을 검사합니다. 클라이언트의 유효성을 보장하기 위해 IP 주소 또는 하위 도메인으로 클라이언트를 제한합니다.

**STEP 10 |** RADIUS 서버가 관리자에 대한 인증 및 권한을 수행하는지 확인합니다.

1. RADIUS 서버에 추가한 관리자 계정을 사용하여 방화벽 웹 인터페이스에 로그인합니다.
2. 관리자와 연결된 역할에 대해 허용되는 웹 인터페이스 페이지만 액세스할 수 있는지 확인합니다.
3. 모니터, 정책 및 개체 탭에서 관리자와 연결된 액세스 도메인에 대해 허용되는 가상 시스템만 액세스할 수 있는지 확인합니다.
4. 모니터 > 인증에서 인증 프로토콜을 확인합니다.
5. 다음 CLI 명령을 사용하여 인증서 프로파일의 연결 및 유효성을 테스트합니다.

```
admin@PA-220 > test authentication authentication-profile
 auth-profile username <username> password <password>
```


©2023 Palo Alto Networks, Inc.

# LDAP 인증 구성

LDAP를 사용하여 인증 포털을 통해 애플리케이션이나 서비스에 액세스하는 최종 사용자를 인증하고 웹 인터페이스에 액세스하는 방화벽 또는 Panorama 관리자를 인증할 수 있습니다.

*LDAP* 서버에 연결하여 사용자 그룹을 기반으로 정책 규칙을 정의할 수도 있습니다. 자세한 내용은 그룹에 사용자 매핑을 참조하십시오.

**STEP 1 |** LDAP 서버 프로파일을 추가합니다.

프로파일은 방화벽이 LDAP 서버에 연결하는 방법을 정의합니다.

1. 디바이스 > 서버 프로파일 > **LDAP** 또는 **Panorama** > 서버 프로파일 > 을 선택하거나 **Panorama™**의 **LDAP** 및 서버 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. (Multi-VSYS에만 해당) 프로파일을 사용할 수 있는 위치를 선택합니다.
4. (선택 사항) 관리자에 대한 액세스를 제한하려면 관리자만 사용을 선택합니다.
5. LDAP 서버를 추가합니다(최대 4개). 각 서버에 대해 이름(서버 식별), **LDAP** 서버 IP 주소 또는 FQDN 및 서버 포트(기본값 389)를 입력합니다.

   *FQDN* 주소 개체를 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소에 대한 변경 사항을 적용해야 합니다.
6. 서버 유형을 선택합니다.
7. 기본 **DN**을 선택합니다.

   디렉터리의 기본 DN을 식별하려면 **Active Directory** 도메인 및 트러스트 Microsoft 관리 콘솔 스냅인을 열고 최상위 도메인의 이름을 사용합니다.
8. 바인딩 **DN** 및 암호를 입력하여 인증 서비스에서 방화벽을 인증할 수 있도록 합니다.

   *Bind DN* 계정에는 *LDAP* 디렉토리를 읽을 수 있는 권한이 있어야 합니다.
9. 바인딩 타임아웃 및 검색 타임아웃(초)을 입력합니다. 기본값은 모두 30입니다.
10. 재시도 간격(초)을 입력합니다(기본값은 60).
11. **SSL/TLS** 보안 연결 필요(기본적으로 활성화됨) 옵션을 활성화합니다. 엔드포인트가 사용하는 프로토콜은 서버 포트에 따라 다릅니다.
    - 389(기본값) - TLS(특히, 디바이스는 초기 일반 텍스트 연결을 TLS로 업그레이드하는 StarTTLS 작업을 사용합니다.)
    - 636 - SSL
    - 기타 포트 - 디바이스가 먼저 TLS를 사용하려고 합니다. 디렉터리 서버가 TLS를 지원하지 않으면 디바이스가 SSL로 폴백됩니다.
12. (선택 사항) 보안을 강화하려면 SSL/TLS 연결에 대해 디렉터리 서버가 제공하는 인증서를 엔드포인트에서 확인할 수 있도록 **SSL** 세션에 대한 서버 인증서 확인 옵션을 활성화합니다. 확인을

 ©2023 Palo Alto Networks, Inc.

활성화하려면 **SSL/TLS** 보안 연결 필요 옵션도 활성화해야 합니다. 확인이 성공하려면 인증서가 다음 조건 중 하나를 충족해야 합니다.

- 디바이스 인증서 목록에 있습니다. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서**.** 필요한 경우 인증서를 디바이스로 가져옵니다.
- 인증서 서명자는 신뢰할 수 있는 인증 기관 목록에 있습니다. 디바이스 > 인증서 관리 > 인증서 > 기본 신뢰할 수 있는 인증 기관.

13. 확인을 클릭하여 서버 프로파일을 저장합니다.

**STEP 2 |** 서버 프로파일을 인증 프로파일 및 시퀀스 구성에 할당하여 다양한 인증 설정을 정의합니다.

**STEP 3 |** 인증이 필요한 방화벽 애플리케이션에 인증 프로파일을 할당합니다.

- 웹 인터페이스에 대한 관리 액세스 - 방화벽 관리자 계정을 구성하고 구성한 인증 프로파일을 할당합니다.
- 서비스 및 애플리케이션에 대한 최종 사용자 액세스 - 최종 사용자에 대한 인증을 구성하는 전체 절차는 인증 정책 구성을 참조하십시오.

**STEP 4 |** 방화벽이 인증 서버 연결을 테스트하여 사용자를 인증할 수 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# 인증 서버에 대한 연결 타임아웃

방화벽 또는 Panorama에 액세스하는 관리자와 인증 포털을 통해 서비스 또는 애플리케이션에 액세스하는 최종 사용자를 인증하기 위해 외부 인증 서비스를 사용하도록 방화벽을 구성할 수 있습니다. 연결할 수 없는 인증 서버에 지속적으로 연결하려고 시도하여 방화벽이 리소스를 낭비하지 않도록 하려면 방화벽이 연결을 중지한 후 타임아웃 간격을 설정할 수 있습니다. 방화벽이 인증 서버에 연결하는 방식을 정의하는 서버 프로파일에서 타임아웃을 설정합니다. 타임아웃 값을 선택할 때 방화벽 리소스를 보존해야 하는 필요성과 인증 서버가 방화벽에 응답하는 방식에 영향을 주는 일반적인 네트워크 지연을 고려하는 것이 목표입니다.

- 인증 서버 타임아웃 설정 지침
- PAN-OS 웹 서버 타임아웃 수정
- 인증 포털 세션 타임아웃 수정

## 인증 서버 타임아웃 설정 지침

다음은 방화벽이 외부 인증 서비스에 연결하려는 시도에 대한 시간 제한을 설정하기 위한 몇 가지 지침입니다.

- 특정 서버에 대한 서버 프로파일에서 설정한 타임아웃 외에도 방화벽에는 전역 PAN-OS 웹 서버 타임아웃이 있습니다. 이 글로벌 타임아웃은 방화벽 웹 인터페이스 또는 PAN-OS XML API에 대한 관리 액세스를 인증하기 위해 방화벽이 외부 서버에 연결하고 인증 포털을 통해 애플리케이션 또는 서비스에 대한 최종 사용자 액세스를 인증할 때 적용됩니다. 전역 시간 제한은 기본적으로 30초입니다(범위는 3~125). 서버 프로파일이 연결 시도를 허용하는 총 시간과 같거나 커야 합니다. 서버 프로파일의 총 시간은 타임아웃 값에 재시도 횟수와 서버 수를 곱한 값입니다. 예를 들어 RADIUS 서버 프로파일이 3초 제한 시간, 3회의 재시도 및 4대의 서버를 지정하는 경우 프로파일에서 연결 시도를 허용하는 총 시간은 36초(3 x 3 x 4)입니다. 필요한 경우 PAN-OS 웹 서버 타임아웃을 수정합니다.

  > 인증 실패가 표시되지 않는 한 ***PAN-OS*** 웹 서버 타임아웃을 변경하지 마십시오. 타임아웃을 너무 높게 설정하면 방화벽의 성능이 저하되거나 인증 요청이 중단될 수 있습니다. 인증 로그에서 인증 실패를 검토할 수 있습니다.

- 방화벽은 최종 사용자가 인증 포털 웹 양식의 인증 질문에 응답하는 데 걸리는 시간을 정의하는 인증 포털 세션 타임아웃을 적용합니다. 웹 양식은 사용자가 인증 정책 규칙과 일치하는 서비스 또는 애플리케이션을 요청할 때 표시됩니다. 세션 시간 제한은 기본적으로 30초입니다(범위는 1~1,599,999). PAN-OS 웹 서버 타임아웃 이상이어야 합니다. 필요한 경우 인증 포털 세션 타임아웃을 수정합니다. PAN-OS 웹 서버 및 인증 포털 세션 타임아웃을 늘리면 방화벽의 성능이 저하되거나 인증 요청이 중단될 수 있습니다.

  > 인증 포털 세션 타임아웃은 방화벽이 ***IP*** 주소-사용자 이름 매핑을 유지하는 기간을 결정하는 타이머와 관련이 없습니다.

- 타임아웃은 인증 시퀀스에 대해 누적됩니다. 예를 들어, 두 개의 인증 프로파일이 있는 인증 시퀀스의 경우를 생각해 보십시오. 하나의 인증 프로파일은 3초 제한 시간, 3회의 재시도 및 4회의 서버가 있는 RADIUS 서버 프로파일을 지정합니다. 다른 인증 프로파일은 3초 제한 시간과 2개의 서버가 있는 TACACS+ 서버 프로파일을 지정합니다. 방화벽이 해당 인증 순서로 사용자 계정을 인증할 수 있는 가장 긴 시간은 42초입니다. RADIUS 서버 프로파일의 경우 36초, TACACS+ 서버 프로파일의 경우 6초.


©2023 Palo Alto Networks, Inc.

- Kerberos 서버에 대해 구성할 수 없는 시간 제한은 Kerberos 서버 프로파일에 지정된 각 서버에 대해 17초입니다.
- 다른 서버 유형에 대한 타임아웃 및 관련 설정을 구성하려면 다음을 참조하십시오.
  - MFA 서버 프로파일을 추가합니다.
  - SAML IdP 서버 프로파일을 추가합니다.
  - TACACS+ 서버 프로파일을 추가합니다.
  - RADIUS 서버 프로파일을 추가합니다.
  - LDAP 서버 프로파일을 추가합니다.

## PAN-OS 웹 서버 타임아웃 수정

PAN-OS 웹 서버 타임아웃은 인증 서버 프로파일의 타임아웃에 해당 프로파일의 서버 수 및 재시도 횟수를 곱한 값과 같거나 커야 합니다.

인증 실패가 표시되지 않는 한 ***PAN-OS*** 웹 서버 타임아웃을 변경하지 마십시오. 타임아웃을 너무 높게 설정하면 방화벽의 성능이 저하되거나 인증 요청이 중단될 수 있습니다. 인증 로그에서 인증 실패를 검토할 수 있습니다.

**STEP 1 |** 방화벽 CLI에 액세스합니다.

**STEP 2 |** 다음 명령을 입력하여 PAN-OS 웹 서버 시간 초과를 설정합니다. 여기서 ***<value>***은 초 단위입니다(기본값은 30, 범위는 3~125).

```
> configure # set deviceconfig setting l3-service timeout <value>
 # commit
```

## 인증 포털 세션 타임아웃 수정

인증 포털 세션 타임아웃은 PAN-OS 웹 서버 타임아웃과 같거나 커야 합니다. 자세한 내용은 인증 서버에 대한 연결 시간 표시를 참조하십시오.

***PAN-OS*** 웹 서버 및 인증 포털 세션 타임아웃을 높일수록 인증 포털이 사용자에게 응답하는 속도가 느려집니다.

**STEP 1 |** 디바이스 > 설정 > 세션을 선택하고 세션 시간 초과를 수정합니다.

**STEP 2 |** 새 인증 포털 값(기본값은 30, 범위는 1~1,599,999)을 입력하고 확인을 클릭합니다.

**STEP 3 |** 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 로컬 데이터베이스 인증 구성

방화벽 웹 인터페이스에 액세스하는 관리자를 인증하고 인증 포털 또는 GlobalProtect를 통해 애플리케이션에 액세스하는 최종 사용자를 인증하도록 방화벽에 로컬인 사용자 데이터베이스를 구성할 수 있습니다. 로컬 데이터베이스로 로컬 인증을 구성하려면 다음 단계를 수행하십시오.

외부 인증 서비스는 중앙 계정 관리의 이점을 제공하기 때문에 일반적으로 로컬 인증보다 선호됩니다.

데이터베이스 없이 로컬 인증을 구성할 수도 있지만 방화벽 또는 Panorama 관리자만 사용할 수 있습니다.

**STEP 1 |** 로컬 데이터베이스에 사용자 계정을 추가합니다.

1. 디바이스 > 로컬 사용자 데이터베이스 > 사용자를 선택하고 추가를 클릭합니다.
2. 관리자의 사용자 이름을 입력합니다.
3. 암호 및 암호 확인을 입력하거나 암호 해시를 입력합니다.
4. 계정(기본적으로 활성화됨)을 활성화하고 확인을 클릭합니다.

**STEP 2 |** 로컬 데이터베이스에 사용자 그룹을 추가합니다.

사용자에게 그룹 멤버십이 필요한 경우 필요합니다.

1. 디바이스 > 로컬 사용자 데이터베이스 > 사용자 그룹을 선택하고 추가를 클릭합니다.
2. 그룹을 식별할 이름을 입력합니다.
3. 그룹의 구성원인 각 사용자를 추가하고 확인을 클릭합니다.

**STEP 3 |** 인증 프로파일을 구성합니다.

인증 프로파일은 사용자 집합에 공통적인 인증 설정을 정의합니다. 인증 유형을 로컬 데이터베이스로 설정합니다.

**STEP 4 |** 인증 프로파일을 관리자 계정 또는 최종 사용자에 대한 인증 정책 규칙에 할당합니다.

- 관리자 - 방화벽 관리자 계정 구성:

  이 절차의 앞부분에서 정의한 사용자의 이름을 지정합니다.

  계정에 대해 구성한 인증 프로파일을 할당합니다.
- 최종 사용자 - 최종 사용자에 대한 인증을 구성하는 전체 절차는 인증 정책 구성을 참조하십시오.

**STEP 5 |** 방화벽이 인증 서버 연결을 테스트하여 사용자를 인증할 수 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# 인증 프로파일 및 시퀀스 구성

인증 프로파일은 방화벽 웹 인터페이스에 액세스하는 관리자 및 인증 포털 또는 GlobalProtect는 애플리케이션에 액세스하는 최종 사용자의 로그인 자격 증명의 유효성을 검사하는 인증 서비스를 정의합니다. 이 서비스는 방화벽이 제공하는 로컬 인증 또는 외부 인증 서비스일 수 있습니다. 인증 프로파일은 Kerberos Single Sign-On(SSO)과 같은 옵션도 정의합니다.

일부 네트워크에는 여러 사용자 및 사용자 그룹에 대한 여러 데이터베이스(예: TACACS+ 및 LDAP)가 있습니다. 이러한 경우 사용자를 인증하려면 인증 시퀀스(로그인 시 방화벽이 사용자와 일치하는 인증 프로파일의 순위가 지정된 순서)를 구성합니다. 방화벽은 사용자를 성공적으로 인증할 때까지 순서대로 각 프로파일을 확인합니다. 시퀀스의 모든 프로파일에 대해 인증이 실패하는 경우에만 사용자의 액세스가 거부됩니다. 시퀀스는 멀티 팩터 인증(MFA) 및 SAML을 제외하고 방화벽이 지원하는 모든 인증 서비스를 기반으로 하는 인증 프로파일을 지정할 수 있습니다.

**STEP 1 |** (외부 서비스만 해당) 사용자 인증을 위해 방화벽을 외부 서버에 연결할 수 있도록 설정합니다.

1. 외부 서버를 설정합니다. 자세한 내용은 서버 설명서를 참조하십시오.
2. 사용하는 인증 서비스 유형에 맞게 서버 프로파일을 구성합니다.
   - RADIUS 서버 프로파일을 추가합니다.

     방화벽이 ***RADIUS***를 통해 ***MFA*** 서비스와 통합되는 경우 ***RADIUS*** 서버 프로파일을 추가해야 합니다**.** 이 경우 ***MFA*** 서비스는 모든 인증 요소를 제공합니다**.** 방화벽이 벤더 ***API***를 통해 ***MFA*** 서비스와 통합되는 경우에도 첫 번째 요소에 대해 ***RADIUS*** 서버 프로파일을 사용할 수 있지만 추가 요소에는 ***MFA*** 서버 프로파일이 필요합니다**.**

   - MFA 서버 프로파일을 추가합니다.
   - SAML IdP 서버 프로파일을 추가합니다.
   - Kerberos 서버 프로파일을 추가합니다.
   - TACACS+ 서버 프로파일을 추가합니다.
   - LDAP 서버 프로파일을 추가합니다.

**STEP 2 |** (로컬 데이터베이스 인증만 해당) 방화벽에 로컬인 사용자 데이터베이스를 구성합니다.

방화벽에 로컬인 사용자 ID 저장소를 기반으로 로컬 인증을 구성할 각 사용자 및 사용자 그룹에 대해 다음 단계를 수행합니다.

1. 로컬 데이터베이스에 사용자 계정을 추가합니다.
2. (선택 사항) 사용자 그룹을 로컬 데이터베이스에 추가합니다.

**STEP 3 |** (Kerberos SSO에만 해당) Kerberos Single Sign-On(SSO)이 기본 인증 서비스인 경우 방화벽에 대한 Kerberos 키 탭을 생성합니다.

Kerberos 키탭을 생성합니다. 키 탭은 방화벽에 대한 Kerberos 계정 정보가 들어 있는 파일입니다. Kerberos SSO를 지원하려면 네트워크에 Kerberos 인프라가 있어야 합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 인증 프로파일을 구성합니다.

다음 중 하나 또는 둘 다를 정의합니다.

- **Kerberos SSO** - 방화벽이 먼저 SSO 인증을 시도합니다. 실패하면 지정된 인증 유형으로 폴백(fall back)됩니다.
- 외부 인증 또는 로컬 데이터베이스 인증 - 방화벽은 사용자에게 로그인 자격 증명을 입력하라는 메시지를 표시하고 외부 서비스 또는 로컬 데이터베이스를 사용하여 사용자를 인증합니다.

1. 디바이스 > 인증 프로파일을 선택한 다음 인증 프로파일 추가 를 선택합니다.
2. 인증 프로파일을 식별할 이름을 입력합니다.
3. 인증 서비스 유형을 선택합니다.
   - 다중 요소 인증을 사용하는 경우 선택한 유형이 첫 번째 인증 요소에만 적용됩니다. 요인 탭에서 추가 MFA 요소에 대한 서비스를 선택합니다.
   - **RADIUS**, **TACACS+**, **LDAP** 또는 **Kerberos**를 선택한 경우 [서버 프로파일을 선택합니다.
   - **LDAP**를 선택한 경우 서버 프로파일을 선택한 다음 로그인 속성을 정의합니다. Active Directory의 경우 **SAMAccountName**을 값으로 입력합니다.
   - **SAML**을 선택하는 경우 **IdP** 서버 프로파일을 선택합니다.
   - 클라우드 인증 서비스를 선택하는 경우 방화벽과 통신하도록 Cloud ID Engine 인스턴스를 구성합니다. 클라우드 자격 증명 엔진에 대한 자세한 내용은 클라우드 ID 엔진 시작 가이드를 참조하십시오.
4. Kerberos SSO를 활성화하려면 **Kerberos** 영역(일반적으로 영역이 대문자인 경우를 제외하고 사용자의 DNS 도메인) 을 입력하고 방화벽 또는 Panorama용으로 생성한 **Kerberos** 키 탭을 임포트합니다.
5. (MFA에만 해당) 요인, 추가 인증 요소 활성화 및 구성한 MFA 서버 프로파일 추가를 선택합니다.

   방화벽은 나열된 순서대로 위에서 아래로 각 MFA 서비스를 호출합니다.
6. 고급을 선택한 다음 이 프로파일로 인증할 수 있는 사용자 및 그룹 추가를 선택합니다.

   로컬 데이터베이스에서 사용자 및 그룹을 선택하거나, 사용자를 그룹에 매핑하도록 방화벽을 구성한 경우 Active Directory와 같은 LDAP 기반 디렉터리 서비스에서 사용자 및 그룹을 선택할 수 있습니다. 기본적으로 목록은 비어 있으므로 사용자가 인증할 수 없습니다.

   그룹 매핑 구성에 정의된 사용자 지정 그룹을 선택할 수도 있습니다.
7. (선택 사항) 방화벽에서 서버에 인증 요청을 보내기 전에 사용자 정보를 수정하려면 사용자 이름 수정자를 구성합니다.
   - **%USERDOMAIN%\%USERINPUT%** - 원본에 도메인이 포함되지 않은 경우(예: samAccountName 사용) 방화벽이 사용자 이름 앞에 지정한 사용자 도메인을 추가합니다. 원본에 도메인이 포함된 경우 방화벽이 해당 도메인을 사용자 도메인으로 바꿉니다. 사용자 도메인이 비어 있으면 방화벽이 인증 서버로 요청을 보내기 전에 방화벽이 소스에서 수신하는 사용자 정보에서 도메인을 제거합니다.

     *LDAP* 서버는 *samAccountName*에서 백슬래시를 지원하지 않으므로 이 옵션을 사용하여 *LDAP* 서버를 인증하지 마십시오.


©2023 Palo Alto Networks, Inc.

- **%USERINPUT%** - (기본값) 방화벽은 사용자 정보를 원본에서 수신하는 형식으로 인증 서버로 보냅니다.
- **%USERINPUT%@%USERDOMAIN%** - 원본에 도메인이 포함되어 있지 않으면 방화벽이 사용자 이름 뒤에 사용자 도메인 값을 추가합니다. 원본에 도메인이 포함된 경우 방화벽은 해당 도메인을 사용자 도메인 값으로 바꿉니다. 사용자 도메인이 비어 있으면 방화벽이 인증 서버로 요청을 보내기 전에 방화벽이 소스에서 수신하는 사용자 정보에서 도메인을 제거합니다.
- 없음 - 수동으로 **None**을 입력하는 경우:
  - LDAP 및 Kerberos 서버 프로파일의 경우 방화벽은 소스에서 수신한 도메인을 사용하여 적절한 인증 프로파일을 선택한 다음 서버에 인증 요청을 보낼 때 도메인을 제거합니다. 이렇게 하면 인증 시퀀스 중에 사용자 도메인을 포함할 수 있지만 방화벽이 인증 요청을 서버로 보내기 전에 도메인을 제거할 수 있습니다. 예를 들어 LDAP 서버 프로파일과 samAccountName을 특성으로 사용하는 경우 방화벽이 도메인이 아닌 사용자 이름만 필요한 인증 서버로 도메인을 보내지 않도록 이 옵션을 사용합니다.
  - RADIUS 서버 프로파일의 경우:
    - 소스에서 **domain\username** 형식으로 사용자 정보를 보내는 경우 방화벽은 사용자 정보를 동일한 형식으로 서버에 보냅니다.
    - 소스에서 사용자 **username@domain** 형식으로 사용자 정보를 보내는 경우 방화벽은 서버에 보내기 전에 사용자 정보를 **domain\username** 형식으로 정규화합니다.
    - 소스에서 사용자 이름만 보내는 경우 방화벽은 **domain\username** 이름 형식으로 정보를 서버에 보내기 전에 지정한 **사용자 도메인**을 추가합니다.
  - 로컬 데이터베이스, TACACS+ 및 SAML의 경우 방화벽은 사용자 정보를 원본에서 수신하는 형식으로 인증 서버로 보냅니다.

8. 확인을 클릭하여 인증 프로파일을 저장합니다.

**STEP 5 |** 인증 시퀀스를 구성합니다.

방화벽에서 사용자를 인증하기 위해 여러 인증 프로파일을 시도하도록 하려는 경우 필요합니다. 방화벽은 한 프로파일이 사용자를 성공적으로 인증할 때까지 위에서 아래 순서로 프로파일을 평가합니다.

1. 디바이스 > 인증 시퀀스를 선택한 다음 인증 시퀀스 추가를 선택합니다.
2. 인증 시퀀스를 식별할 이름을 입력합니다.

   인증 프로세스를 신속히 처리하려면 도메인을 사용하여 인증 프로파일을 결정합니다. 방화벽은 순서에 따라 인증 프로파일의 사용자 도메인 또는 ***Kerberos*** 영역에 로그인하는 동안 사용자가 입력하는 도메인 이름과 일치시키고 해당 프로파일을 사용하여 사용자를 인증합니다. 방화벽에서 일치하는 항목을 찾지 못하거나 이 옵션을 비활성화하면 방화벽은 위에서 아래로 순서대로 프로파일을 시도합니다.
3. 각 인증 프로파일을 추가합니다. 프로파일의 평가 순서를 변경하려면 프로파일을 선택한 다음 위로 이동 또는 아래로 이동을 선택합니다.
4. 확인을 클릭하여 인증 시퀀스를 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 방화벽 관리자용 관리 계정이나 최종 사용자의 인증 정책에 인증 프로파일 또는 시퀀스를 할당합니다.

- 관리자 - 관리자 권한 부여를 관리하는 방법에 따라 인증 프로파일을 할당합니다.

  방화벽에서 로컬로 관리되는 인증 - 방화벽 관리자 계정 구성.

  SAML, TACACS+ 또는 RADIUS 서버에서 관리되는 인증 - 기기 > 설정 > 관리, 인증 설정을 수정하고 인증 프로파일을 선택합니다.
- 최종 사용자 - 최종 사용자에 대한 인증을 구성하는 전체 절차는 인증 정책 구성을 참조하십시오.

**STEP 7 |** 방화벽이 인증 서버 연결을 테스트하여 사용자를 인증할 수 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# 인증 서버 연결 테스트

테스트 인증 기능을 사용하면 방화벽 또는 Panorama가 인증 프로파일에 지정된 인증 서버와 통신할 수 있는지의 여부와 특정 사용자에 대한 인증 요청이 성공하는지의 여부를 확인할 수 있습니다. 웹 인터페이스에 액세스하는 관리자를 인증하거나 GlobalProtect 또는 인증 포털을 통해 애플리케이션에 액세스하는 최종 사용자를 인증하는 인증 프로파일을 테스트할 수 있습니다. 후보 구성에 대한 인증 테스트를 수행하여 커밋하기 전에 구성이 올바른지 확인할 수 있습니다.

**STEP 1 |** 인증 프로파일을 구성합니다. 테스트하기 전에 인증 프로파일 또는 서버 프로파일 구성을 커밋할 필요가 없습니다.

**STEP 2 |** 방화벽 CLI에 로그인합니다.

**STEP 3 |** (여러 가상 시스템이 있는 방화벽) 테스트 명령이 액세스할 대상인 가상 시스템을 정의합니다.

이는 테스트 인증 명령이 테스트할 사용자를 찾을 수 있도록 여러 가상 시스템이 있는 방화벽에서 필요합니다.

다음을 입력하여 대상 가상 시스템을 정의합니다.

```
admin@PA-325060> set system setting target-vsys <vsys-name>
```

예를 들어, 사용자가 vsys2에 정의되어 있으면 다음을 입력하십시오.

```
admin@PA-3250> set system setting target-vsys vsys2
```

***target-vsys*** 옵션은 로그인 세션당 있으며, 방화벽은 사용자가 로그오프할 때 옵션을 지웁니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 다음 명령을 입력하여 인증 프로파일을 테스트합니다.

```
admin@PA-3250> test authentication authentication-
profile <authentication-profile-name> username <username> password
```

예를 들어, **bsimpson**이라는 사용자에 대해 **my-profile**이라는 인증 프로파일을 테스트하려면 다음을 입력하십시오.

```
admin@PA-3250> test authentication authentication-profile my-
profile username bsimpson password
```

***test*** 명령을 실행할 때 인증 프로파일과 서버 프로파일의 이름은 대소문자를 구분합니다. 또한 인증 프로파일에 정의된 사용자명 수정자가 있는 경우 사용자명과 함께 수정자를 입력해야 합니다. 예를 들어, ***bsimpson***이라는 사용자에 대해 사용자명 수정자 ***%USERINPUT%@%USERDOMAIN%***을 추가하고 도메인 이름이 ***mydomain.com***인 경우 사용자명으로 ***bsimpson@mydomain.com***을 입력합니다. 이렇게 하면 방화벽이 인증 서버에 올바른 자격 증명을 보낼 수 있습니다. 이 예에서 *mydomain.com*은 인증 프로파일의 사용자 도메인 필드에 정의한 도메인입니다.

**STEP 5 |** 테스트 출력을 봅니다.

인증 프로파일이 올바르게 구성된 경우 출력에 `인증 성공`이 표시됩니다. 구성 문제가 있는 경우 구성 문제를 해결하는 데 도움이 되는 정보가 출력에 표시됩니다.

출력 결과는 테스트 중인 인증 유형 및 문제 유형과 관련된 여러 요인에 따라 달라집니다. 예를 들어, *RADIUS*와 *TACACS+*는 서로 다른 기본 라이브러리를 사용하므로 두 유형 모두에 존재하는 동일한 문제는 서로 다른 오류를 생성합니다. 또한 인증 서버 프로파일에 잘못된 포트나 *IP* 주소를 사용하는 등 네트워크 문제가 있는 경우 출력 오류가 구체적이지 않습니다. 이는 테스트 명령이 방화벽과 인증 서버 간의 초기 핸드쉐이크를 수행하여 문제에 대한 세부 정보를 확인할 수 없기 때문입니다.


©2023 Palo Alto Networks, Inc.

# 인증 정책

인증 정책을 사용하면 최종 사용자가 서비스 및 애플리케이션에 액세스하기 전에 인증할 수 있습니다. 사용자가 서비스 또는 애플리케이션을 요청할 때마다(예: 웹 페이지 방문) 방화벽은 인증 정책을 평가합니다. 일치하는 인증 정책 규칙에 따라 방화벽은 로그인 및 암호, 음성, SMS, 푸시 또는 OTP(일회용 암호) 인증과 같은 하나 이상의 방법(요소)을 사용하여 인증하라는 메시지를 표시합니다. 첫 번째 요소는 사용자가 인증 포털 웹 양식을 통해 인증하는 것입니다. 추가 요소의 경우 사용자는 멀티 팩터 인증(MFA) 로그인 페이지를 통해 인증합니다.



***GlobalProtect***에 대한 인증 정책을 구현하려면 다중 요소 인증 알림을 사용하도록 GlobalProtect 구성을 참조하십시오.

사용자가 모든 요소에 대해 인증하면 방화벽이 보안 정책을 평가하여 서비스 또는 애플리케이션에 대한 액세스를 허용할지의 여부를 결정합니다.

사용자 워크플로를 방해하는 인증 문제의 빈도를 줄이기 위해 후속 액세스가 아닌 서비스 및 애플리케이션에 대한 초기 액세스에 대해서만 사용자가 인증하는 타임아웃 기간을 지정할 수 있습니다. 인증 정책은 인증 포털과 통합되어 타임아웃을 평가하고 사용자 기반 정책 및 보고서를 활성화하는 데 사용되는 타임스탬프를 기록합니다.

User-ID는 인증 중에 방화벽이 수집하는 사용자 정보를 기반으로 새 IP 주소와 사용자 이름 간 매핑을 만들거나 매핑 정보가 변경된 경우 해당 사용자에 대한 기존 매핑을 업데이트합니다. 방화벽은 User-ID 로그를 생성하여 추가 및 업데이트를 기록합니다. 또한 방화벽은 인증 규칙과 일치하는 각 요청에 대해 인증 로그를 생성합니다. 중앙 집중식 모니터링을 선호하는 경우 User-ID 또는 인증 로그를 기반으로 보고서를 구성하고 다른 로그 유형과 마찬가지로 Panorama 또는 외부 서비스로 로그를 포워딩할 수 있습니다.

- 인증 타임스탬프
- 인증 정책 구성

## 인증 타임스탬프

인증 정책 규칙을 구성할 때 사용자가 후속 액세스가 아닌 서비스 및 애플리케이션에 대한 초기 액세스에 대해서만 인증하는 타임아웃 기간을 지정할 수 있습니다. 목표는 서비스와 애플리케이션을 보호해야 하는 필요성과 사용자 워크플로에 대한 중단을 최소화해야 하는 필요성 사이에서 균형을 유지하는 시간 제한을 지정하는 것입니다. 사용자가 인증할 때 방화벽은 첫 번째 인증 질문(요소)에 대한 타임스탬프와 추가 MFA(다중 요소 인증) 요소에 대한 타임스탬프를 기록합니다. 사용자가 이후에 인증 규칙과 일치하는 서비스 및 애플리케이션을 요청하면 방화벽은 각 타임스탬프와 관련하여 규칙에 지정된 타임아웃을 평가합니다. 즉, 타임아웃가 만료되면 방화벽이 요소별로 인증 문제를 재발행합니다. 사용자 매핑 및 인증 타임스탬프를 재배포하면 모든 방화벽이 모든 사용자에 대해 인증 정책 타임아웃을 일관되게 적용합니다.



방화벽은 각 ***MFA*** 공급업체에 대해 별도의 타임스탬프를 기록합니다. 예를 들어 Duo v2 및 ***PingID*** 서버를 사용하여 ***MFA*** 요인에 대한 챌린지를 발행하는 경우 방화벽은 ***Duo*** 요인에 대한 응답에 대해 하나의 타임스탬프를 기록하고 ***PingID*** 요인에 대한 응답에 대해 하나의 타임스탬프를 기록합니다.

제한 시간 내에 하나의 인증 규칙에 대해 성공적으로 인증한 사용자는 다른 규칙이 보호하는 서비스나 애플리케이션에 액세스할 수 있습니다. 그러나 이 이식성은 동일한 인증 요소를 트리거하는 규칙에만 적용


©2023 Palo Alto Networks, Inc.

됩니다. 예를 들어, TACACS+ 인증을 트리거하는 규칙에 대해 성공적으로 인증한 사용자는 액세스 요청이 두 규칙에 대해 제한 시간 내에 있더라도 SAML 인증을 트리거하는 규칙에 대해 다시 인증해야 합니다.

각 인증 규칙의 타임아웃와 인증 포털 설정에 정의된 전역 타이머를 평가할 때(인증 포털 구성 참조) 방화벽은 사용자에게 먼저 만료되는 설정에 대해 재인증하라는 메시지를 표시합니다. 재인증 시 방화벽은 규칙에 대한 새 인증 타임스탬프를 기록하고 인증 포털 타이머의 시간 카운트를 재설정합니다. 따라서 다른 인증 규칙에 대해 다른 타임아웃 기간을 활성화하려면 인증 포털 타이머를 규칙의 타임아웃과 같거나 더 높은 값으로 설정하십시오.

## 인증 정책 구성

인증 포털을 통해 서비스에 액세스하는 최종 사용자에 대한 인증 정책을 구성하려면 다음 단계를 수행하십시오. 시작하기 전에 보안 정책이 사용자가 인증이 필요한 서비스 및 URL 카테고리에 액세스할 수 있도록 허용하는지 확인하십시오.

**STEP 1 |** 인증 포털을 구성합니다. MFA(Multi-Factor Authentication) 서비스를 사용하여 사용자를 인증하는 경우 모드를 리디렉션으로 설정해야 합니다.

**STEP 2 |** 다음 서비스 중 하나를 사용하여 사용자를 인증하도록 방화벽을 구성합니다.

- 외부 인증 서비스 - 방화벽이 서비스에 연결하는 방법을 정의하도록 서버 프로파일을 구성합니다.
- 로컬 데이터베이스 인증 - 각 사용자 계정을 방화벽의 로컬 사용자 데이터베이스에 추가합니다.
- Kerberos SSO(Single Sign-On) - 방화벽에 대한 Kerberos 키 탭을 생성합니다. 선택적으로 Kerberos SSO를 기본 인증 서비스로 사용하도록 방화벽을 구성할 수 있으며 SSO가 실패하는 경우 외부 서비스 또는 로컬 데이터베이스 인증으로 대체할 수 있습니다.

**STEP 3 |** 동일한 인증 서비스 및 설정이 필요한 각 사용자 및 인증 정책 규칙 집합에 대한 인증 프로파일 및 시퀀스를 구성합니다.

인증 서비스 유형 및 관련 설정을 선택합니다.

- 외부 서비스 - 외부 서버 유형을 선택한 다음 생성한 서버 프로파일을 선택합니다.
- 로컬 데이터베이스 인증 - 유형을 로컬 데이터베이스로 설정합니다. 고급 설정에서 생성한 인증 포털 사용자 및 사용자 그룹을 추가합니다.
- **Kerberos SSO** - **Kerberos** 영역을 지정하고 **Kerberos Keytab**을 가져옵니다.

**STEP 4 |** 인증 시행 개체를 구성합니다.

개체는 각 인증 프로파일을 인증 포털 메서드와 연결합니다. 이 방법은 첫 번째 인증 챌린지(요소)가 투명하거나 사용자 응답이 필요한지의 여부를 결정합니다.

1. 개체 > 인증을 선택한 다음 개체를 추가합니다.
2. 개체를 식별할 이름을 입력합니다.
3. 인증 프로파일에 지정한 인증 서비스 유형에 대한 인증 방법 선택:
   - **browser-challenge** - 사용자가 로그인 자격 증명을 입력하도록 하는 대신 클라이언트 브라우저가 첫 번째 인증 요소에 응답하도록 하려면 이 방법을 선택합니다. 이 방법의 경우 인증 프로파일에서 Kerberos SSO를 구성해야 합니다. 브라우저 챌린지가 실패하면 방화벽은 웹 양식 방법으로 대체합니다.

 ©2023 Palo Alto Networks, Inc.

- **web-form** - 방화벽이 사용자가 로그인 자격 증명을 입력할 수 있도록 인증 포털 웹 양식을 표시하도록 하려면 이 방법을 선택합니다.

4. 구성한 인증 프로파일을 선택합니다.
5. 인증 포털 웹 양식이 표시할 메시지를 입력하여 사용자에게 첫 번째 인증 요소를 인증하는 방법을 알려줍니다.
6. 확인을 클릭하여 개체를 저장합니다.

**STEP 5 |** 인증 정책 규칙을 구성합니다.

동일한 인증 서비스 및 설정이 필요한 각 사용자, 서비스 및 URL 카테고리 집합에 대한 규칙을 생성합니다.

방화벽은 인증 정책이 기본 인증 적용 개체(예: ***default-browser-challenge***)를 사용하는 경우 인증 포털 타임아웃를 적용하지 않습니다. 사용자가 인증 포털 타임아웃 후에 재인증하도록 요구하려면 기본 인증 개체에 대한 규칙을 복제하고 기본 인증 개체에 대한 기존 규칙보다 먼저 이동시킵니다.

1. 정책 > 인증을 선택한 다음 규칙을 **A**추가합니다.
2. 규칙을 식별하기 위해 이름을 입력합니다.
3. 소스를 선택한 다음 특정 영역 및 IP 주소 추가를 선택하거나 모든 영역 또는 IP 주소를 선택합니다.

   이 규칙은 지정된 IP 주소 또는 지정된 영역의 인터페이스에서 오는 트래픽에만 적용됩니다.
4. 사용자를 선택한 다음 규칙이 적용되는 원본 사용자 및 사용자 그룹을 선택하거나 추가합니다(기본값은 모두).
5. 규칙이 적용되는 호스트 정보 프로파일을 선택하거나 추가합니다(기본값은 임의).
6. 대상을 선택한 다음 특정 영역 및 IP 주소 추가를 선택하거나 모든 영역 또는 IP 주소를 선택합니다.

   IP 주소는 액세스를 제어하려는 리소스(예: 서버)일 수 있습니다.
7. 서비스/**URL** 카테고리를 선택한 다음 규칙이 액세스를 제어하는 서비스 및 서비스 그룹을 선택하거나 추가합니다(기본값은 **service-http**).
8. 규칙이 액세스를 제어하는 URL 카테고리를 선택하거나 추가합니다(기본값은 임의). 예를 들어 가장 중요한 내부 사이트를 지정하는 사용자 지정 URL 카테고리를 만들 수 있습니다.
9. 작업을 선택한 다음 생성한 인증 적용 개체를 선택합니다.
10. 서비스 및 애플리케이션에 대한 반복적인 액세스에 대해 방화벽이 사용자에게 한 번만 인증하라는 메시지를 표시하는 타임아웃 기간(기본값 60)을 지정합니다.

    타임아웃은 더 엄격한 보안(인증 프롬프트 간 시간 단축)과 사용자 경험(인증 프롬프트 간 더 긴 시간) 간의 절충점입니다. 더 빈번한 인증은 데이터 센터와 같은 중요한 시스템 및 민감한 영역에 대한 액세스를 위한 올바른 선택인 경우가 많습니다. 덜 빈번한 인증은 종종 네트워크 페리미터와 사용자 경험이 핵심인 기업에 올바른 선택입니다.
11. 규칙을 저장하려면 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

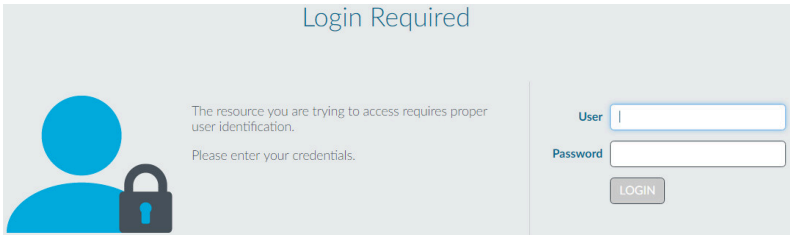
**STEP 6 |** (MFA만 해당) MFA 로그인 페이지를 사용자 지정합니다.

방화벽은 사용자가 추가 MFA 요소에 대해 인증할 수 있도록 이 페이지를 표시합니다.

**STEP 7 |** 방화벽이 인증 정책을 시행하는지 확인하십시오.

1. 인증 정책 규칙에 지정된 소스 사용자 중 하나로 네트워크에 로그인합니다.
2. 규칙에 지정된 것과 일치하는 서비스 또는 URL 카테고리를 요청하십시오.

   방화벽은 첫 번째 인증 요소에 대한 인증 포털 웹 양식을 표시합니다. 예:




   하나 이상의 ***MFA*** 서비스를 사용하도록 방화벽을 구성한 경우 추가 인증 요소에 대해 인증하십시오.

3. 방금 액세스한 서비스 또는 URL에 대한 세션을 종료합니다.
4. 동일한 서비스 또는 애플리케이션에 대해 새 세션을 시작합니다. 인증 규칙에서 구성한 제한 시간 내에 이 단계를 수행해야 합니다.

   방화벽은 재인증 없이 액세스를 허용합니다.
5. 타임아웃 기간이 만료될 때까지 기다렸다가 동일한 서비스나 애플리케이션을 요청하십시오.

   방화벽은 재인증하라는 메시지를 표시합니다.

**STEP 8 |** (선택 사항) 데이터 및 인증 타임스탬프 재배포을(를) 수행하여 모든 사용자에 대해 시간 제한을 일관되게 적용하도록 인증 정책을 시행하는 다른 방화벽에 적용합니다.


©2023 Palo Alto Networks, Inc.

# 인증 문제 해결

사용자가 Palo Alto Networks 방화벽 또는 Panorama에 대한 인증에 실패하거나 인증 프로세스가 예상보다 오래 걸리는 경우 인증 관련 정보를 분석하면 실패 또는 지연이 다음으로 인한 것인지 판단하는 데 도움이 됩니다.

- 사용자 동작 - 예를 들어, 잘못된 자격 증명을 입력한 후 사용자가 잠기거나 대량의 사용자가 동시에 액세스를 시도합니다.
- 시스템 또는 네트워크 문제 - 예를 들어 인증 서버에 액세스할 수 없습니다.
- 구성 문제 - 예를 들어 인증 프로파일의 허용 목록에 있어야 하는 모든 사용자가 있는 것은 아닙니다.

다음 CLI 명령은 이러한 문제를 해결하는 데 도움이 되는 정보를 표시합니다.

| 작업 | 명령 |
| --- | --- |
| 인증 프로파일(**auth-profile**), 인증 시퀀스(**is-seq**) 또는 가상 시스템(**vsys**)과 연결된 잠긴 사용자 계정 수를 표시합니다.<br><br>사용자의 잠금을 해제하려면 다음 운영 명령을 사용합니다.<br><br>**> request authentication [unlock -admin \| unlock-user]** | **PA-220> show authentication locked-users { vsys <value> \| auth-profile <value> \| is-seq {yes \| no} {auth-profile \| vsys} <value> }** |
| 디버그 인증 명령을 사용하여 인증 이벤트 문제를 해결합니다.<br><br>**show** 옵션을 사용하여 인증 요청 통계 및 현재 디버깅 수준을 표시합니다.<br><br>• **show** 는 인증 서비스(authd)의 현재 디버깅 수준을 표시합니다.<br>• **show-active-requests**는 인증 요청, 허용 목록, 잠긴 사용자 계정 및 Multi-Factor Authentication(MFA) 요청에 대한 활성 검사 수를 표시합니다.<br>• **show-pending-requests**는 인증 요청, 허용 목록, 잠긴 사용자 계정 및 MFA 요청에 대해 보류 중인 검사 수를 표시합니다.<br>• **connection-show**는 모든 인증 서버 또는 특정 프로토콜 유형에 대한 인증 요청 및 응답 통계를 표시합니다. | **PA-220> debug authentication { on {debug \| dump \| error \| info \| warn} \| show \| show-active-requests \| show-pending-requests \| connection-show \| { connection-id \| protocol-type { Kerberos connection-id <value> \| LDAP connection-id <value> \| RADIUS connection-id <value> \| TACACS+ connection-id <value> \| } connection-debug-on \| { connection-id \| debug-prefix \| protocol-type { Kerberos connection-id <value> \| LDAP connection-id <value> \| RADIUS connection-id <value> \| TACACS+ connection-id <value> \| } connection-debug-off \| { connection-id \|** |


©2023 Palo Alto Networks, Inc.

| 작업 | 명령 |
| --- | --- |
| **connection-debug** 옵션을 사용하여 인증 디버깅을 사용하거나 사용하지 않도록 설정합니다.<br>• **on** 옵션을 사용하여 authd에 대한 디버깅을 활성화하거나 **off** 옵션을 사용하여 디버깅을 비활성화합니다.<br>• 모든 인증 서버 또는 특정 프로토콜 유형에 대해 디버깅을 비활성화하려면 **connection-debug-on** 옵션을 사용하거나 **connection-debug-off** 옵션을 사용합니다. | **protocol-type { Kerberos connection-id <value> \| LDAP connection-id <value> \| RADIUS connection-id <value> \| TACACS+ connection-id <value> \| } connection-debug-on }** |
| 인증서 프로파일의 연결 및 유효성을 테스트합니다. | PA-220> test authentication authentication-profile auth-profile username <*username*>password <*password*> |
| 모니터 > 로그 > 인증에 표시된 인증 **ID**를 사용하여 특정 인증 문제를 해결합니다. | PA-220> grep <*Authentication ID*> |

 ©2023 Palo Alto Networks, Inc.

# 인증서 관리

다음 주제에서는 Palo Alto Networks® 방화벽 및 Panorama가 사용하는 다양한 키와 인증서, 그리고 이를 획득하고 관리하는 방법에 대해 설명합니다.


- 키 및 인증서
- 기본 신뢰할 수 있는 인증 기관(C)
- 인증서 해지
- 인증서 배포
- 인증서 해지 상태에 대한 확인 설정
- 마스터 키 구성
- 마스터 키 암호화
- 인증서 받기
- 인증서 및 개인 키 내보내기
- 인증서 프로파일 구성
- SSL/TLS 서비스 프로파일 구성
- SSH 서비스 프로파일 구성
- 인바운드 관리 트래픽에 대한 인증서 교체
- SSL 포워딩 프록시 서버 인증서의 키 크기 구성
- 인증서 취소 및 갱신
- 하드웨어 보안 모듈을 사용한 보안 키

# 키 및 인증서

통신 보안 세션에서 당사자 간의 신뢰를 보장하기 위해 Palo Alto Networks 방화벽과 Panorama는 디지털 인증서를 사용합니다. 각 인증서에는 일반 텍스트를 암호화하거나 암호 텍스트를 복호화하는 암호화 키가 포함되어 있습니다. 각 인증서에는 발급자의 ID를 인증하는 디지털 서명도 포함되어 있습니다. 발급자는 인증 당사자의 신뢰할 수 있는 인증서 기관(CA) 목록에 있어야 합니다. 선택적으로 인증 당사자는 발급자가 인증서를 해지하지 않았는지 확인합니다(인증서 해지참조).

Palo Alto Networks 방화벽과 Panorama는 다음 애플리케이션에서 인증서를 사용합니다.

- 인증 포털, MFA(다단계 인증) 및 방화벽 또는 Panorama에 대한 웹 인터페이스 액세스에 대한 사용자 인증입니다.
- GlobalProtect VPN에 대한 디바이스 인증(원격 사용자 대 사이트 또는 대규모).
- Internet Key Exchange(IKE)가 있는 IPSec Site-to-Site VPN용 디바이스 인증.
- 외부 동적 목록(EDL) 유효성 검사입니다.
- User-ID 에이전트 및 TS 에이전트 액세스.
- 인바운드 및 아웃바운드 SSL 트래픽의 복호화.

  방화벽은 트래픽을 복호화하여 정책 규칙을 적용한 다음 트래픽을 최종 대상으로 포워딩하기 전에 다시 암호화합니다. 아웃바운드 트래픽의 경우 방화벽은 포워드 프록시 서버 역할을 하며 대상 서버에 대한 SSL/TLS 연결을 설정합니다. 방화벽은 자신과 클라이언트 간의 연결을 보호하기 위해 서명 인증서를 사용하여 대상 서버 인증서의 복사본을 자동으로 생성합니다.

다음 표는 Palo Alto Networks 방화벽과 Panorama에서 사용하는 키와 인증서에 대해 설명합니다. 모범 사례로 각 사용량에 대해 서로 다른 키와 인증서를 사용합니다.

표 **1: Palo Alto Networks** 디바이스 키**/**인증서

| 키/인증서 사용 | 설명 |
|---|---|
| 관리 액세스 | 방화벽 또는 Panorama 관리 인터페이스(HTTPS 웹 인터페이스에 대한 HTTPS 액세스)에 대한 보안 액세스는 MGT 인터페이스에 대한 서버 인증서(또는 방화벽 또는 Panorama가 MGT를 사용하지 않는 경우 데이터플레인에 지정된 인터페이스)와 선택적으로 관리자를 인증하는 인증서가 필요합니다. |
| 인증 포털 | 인증 정책이 HTTPS 리소스에 액세스하는 사용자를 식별하는 배포에서 인증 포털 인터페이스에 대한 서버 인증서를 지정합니다. 인증 포털을 구성하여 사용자를 식별하는 인증서(대화형 인증 대신 또는 대화형 인증 외)를 사용하도록 구성하면 클라이언트 인증서도 배포합니다. 인증 포털에 대한 자세한 내용은 인증 포털을 사용하여 사용자 이름에 대한 IP 주소 매핑을 참조하십시오. |
| 포워드 트러스트 | 아웃바운드 SSL/TLS 트래픽의 경우, 포워드 프록시 역할을 하는 방화벽이 대상 서버의 인증서에 서명한 CA를 신뢰하는 경우 방화벽은 포워드 신뢰 CA 인증서를 사용하여 클라이언트에 제출할 대상 서버 인증서의 복사본을 생성합니다. 개인 키 크기를 설정하려면 SSL 포워드 프록시 서버 인증서의 키 크기 |


©2023 Palo Alto Networks, Inc.

| 키/인증서 사용 | 설명 |
| --- | --- |
| | 구성을 참조하십시오. 보안을 추가하면 하드웨어 보안 모듈에 키를 저장합니다(자세한 내용은 하드웨어 보안 모듈이 있는 보안 키 참조). |
| 언트러스트를 포워딩합니다. | 아웃바운드 SSL/TLS 트래픽의 경우, 포워드 프록시 역할을 하는 방화벽이 대상 서버의 인증서에 서명한 CA를 신뢰하지 않는 경우 방화벽은 포워드 언트러스트 CA 인증서를 사용하여 클라이언트에 제출할 대상 서버 인증서의 복사본을 생성합니다. |
| SSL 인바운드 검사 | 검사 및 정책 적용을 위해 인바운드 SSL/TLS 트래픽을 복호화하는 키입니다. 이 애플리케이션의 경우 SSL/TLS 인바운드 검사의 적용을 받는 각 서버에 대한 개인 키방화벽으로 가져옵니다. SSL 인바운드 검사 구성을 참조하십시오.<br><br>*PAN-OS 8.0*부터 방화벽은 ***ECDHE(Elliptic-Curve Diffie-Hellman Ephemeral)*** 알고리즘을 사용하여 엄격한 인증서 검사를 수행합니다. 즉, 방화벽이 중간 인증서를 사용하는 경우 *PAN-OS 8.0* 또는 이후 릴리스로 업그레이드한 후 웹 서버에서 방화벽으로 인증서를 다시 가져와 서버 인증서를 중간 인증서와 결합해야 합니다(체인 인증서 설치). 그렇지 않으면 체인에 중간 인증서가 있는 ***SSL*** 인바운드 검사 세션이 실패합니다. 체인 인증서를 설치하려면 다음을 수행하십시오.<br>**1.** 메모장과 같은 일반 텍스트 편집기에서 각 인증서(*.cer*) 파일을 엽니다.<br>**2.** 아래에 포함된 각 서명자와 함께 맨 위에 서버 인증서가 있는 각 인증서를 양끝에 붙여넣습니다.<br>**3.** 파일을 텍스트(*.txt*) 또는 인증서(*.cer*) 파일로 저장합니다(파일 이름에 빈 공백이 포함될 수 없음).<br>**4.** 결합된(체인) 인증서를 방화벽으로 가져옵니다. |
| SSL 제외 인증서 | SSL/TLS 복호화에서 제외할 서버에 대한 인증서입니다. 예를 들어 SSL 복호화를 사용하도록 설정하지만 네트워크에 방화벽이 트래픽을 복호화해서는 안 되는 서버(예: HR 시스템의 웹 서비스)가 포함된 경우 해당 인증서를 방화벽에 가져오고 SSL 제외 인증서로 구성합니다. 복호화 제외를 참조하십시오. |
| GlobalProtect | GlobalProtect 구성 요소 간의 모든 상호 작용은 SSL/TLS 연결을 통해 발생합니다. 따라서 GlobalProtect 배포의 일환으로 모든 GlobalProtect 포털, 게이트웨이 및 모바일 보안 관리자에 대한 서버 인증서를 배포합니다. 선택적으로 사용자를 인증하기 위한 인증서를 배포합니다. |


©2023 Palo Alto Networks, Inc.

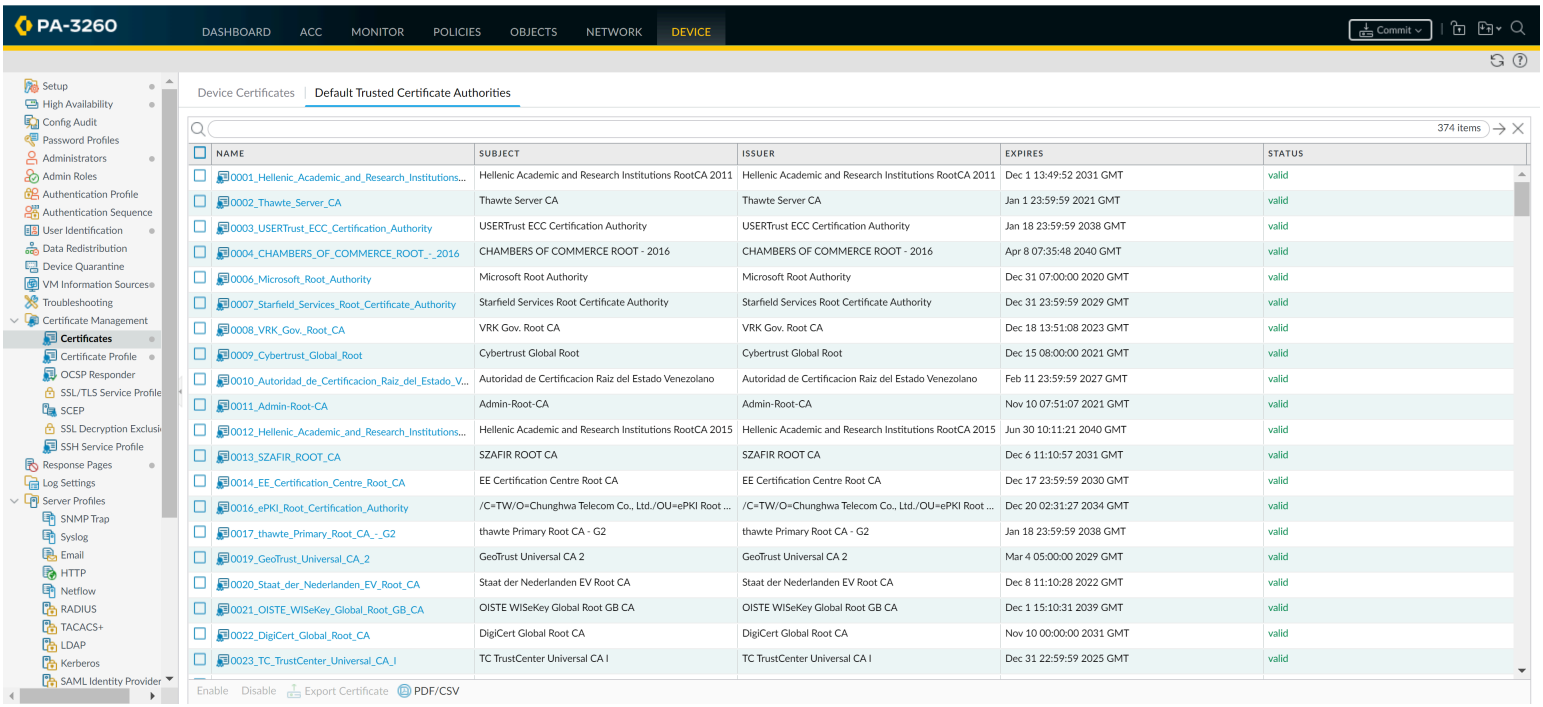
| 키/인증서 사용 | 설명 |
| --- | --- |
| | ***GlobalProtect*** 대규모 VPN(LSVPN) 기능에는 ***CA*** 서명 인증서가 필요합니다. |
| 사이트 간 VPN(IKE) | 사이트 간 IPSec VPN 배포에서 피어 디바이스는 IKE(Internet Key Exchange) 게이트웨이를 사용하여 보안 채널을 설정합니다. IKE 게이트웨이는 인증서 또는 미리 공유된 키를 사용하여 피어를 서로 인증합니다. 방화벽에서 IKE 게이트웨이를 정의할 때 인증서 또는 키를 구성하고 할당합니다. 사이트 간 VPN 개요를 참조하십시오. |
| 마스터 키 | 방화벽은 마스터 키를 사용하여 모든 개인 키와 암호를 암호화합니다. 네트워크에 개인 키를 저장하기 위한 안전한 위치가 필요한 경우 HSM(하드웨어 보안 모듈)에 저장된 암호화(래핑) 키를 사용하여 마스터 키를 암호화할 수 있습니다. 자세한 내용은 HSM을 사용하여 마스터 키 암호화를 참조하십시오. |
| Secure Syslog | 방화벽과 syslog 서버 간의 보안 연결을 사용하도록 설정하는 인증서입니다. Syslog 필드 설명을 참조하십시오. |
| 신뢰할 수 있는 루트 CA | 방화벽이 신뢰하는 CA에서 발급한 루트 인증서의 지정입니다. 방화벽은 자체 서명된 루트 CA 인증서를 사용하여 다른 애플리케이션(예: SSL 포워드 프록시)에 대한 인증서를 자동으로 발급할 수 있습니다.<br><br>또한 방화벽이 다른 방화벽과 보안 연결을 설정해야 하는 경우 인증서를 발행하는 루트 CA가 방화벽의 신뢰할 수 있는 루트 CA 목록에 있어야 합니다. |
| 디바이스 간 통신 | 기본적으로 Panorama, 방화벽 및 로그 컬렉터는 관리 및 로그 포워딩에 사용되는 SSL/TLS 연결에 사전 정의된 인증서 집합을 사용합니다. 그러나 배포 시 디바이스에 사용자 지정 인증서를 배포하여 이러한 연결을 향상시킬 수 있습니다. 이러한 인증서는 Panorama HA 피어 간의 SSL/TLS 연결을 보호하는 데도 사용할 수 있습니다. |


©2023 Palo Alto Networks, Inc.

# 기본 신뢰할 수 있는 인증서 당국(C)

방화벽은 기본적으로 가장 일반적이고 신뢰할 수 있는 기관(CA)을 신뢰합니다. 이러한 신뢰할 수 있는 인증서 공급자는 방화벽이 인터넷에 대한 연결을 보호하는 데 필요한 인증서를 발급할 책임이 있습니다.

기본적으로 방화벽이 신뢰하는 CD 목록을 보고 관리하려면, 디바이스 > 인증서 관리 > 인증서 > 기본 신뢰할 수 있는 인증서 권한을 선택합니다.




추가할 수 있는 유일한 추가 CD는 조직에서 요구하는 신뢰할 수 있는 엔터프라이즈 CO입니다.인증서 받기를 참조합니다.


©2023 Palo Alto Networks, Inc.

# 인증서 해지

Palo Alto Networks 방화벽과 Panorama는 디지털 인증서를 사용하여 통신 보안 세션에서 당사자 간의 신뢰를 보장합니다. 인증서의 해지 상태를 확인하도록 방화벽 또는 Panorama를 구성하면 추가 보안이 제공됩니다. 해지된 인증서를 제시하는 당사자는 신뢰할 수 없습니다. 인증서가 체인의 일부인 경우 방화벽 또는 Panorama는 해지 상태를 확인할 수 없는 루트 CA 인증서를 제외한 체인의 모든 인증서 상태를 확인합니다.

다양한 상황에 따라 만료 날짜 이전에 인증서가 무효화될 수 있습니다. 몇 가지 예로는 이름 변경, 주체와 인증 기관 간의 연결 변경(예: 직원 해고), 개인 키 손상(알려졌거나 의심되는)이 있습니다. 이러한 상황에서 인증서를 발급한 인증 기관은 인증서를 취소해야 합니다.

방화벽 및 Panorama는 인증서 해지 상태를 확인하기 위해 다음과 같은 방법을 지원합니다. 두 방법을 모두 구성하는 경우 방화벽 또는 Panorama는 먼저 OCSP 방법을 시도합니다. OCSP 서버를 사용할 수 없는 경우 CRL 방법을 사용합니다.

- 인증서 해지 목록(CRL)
- 온라인 인증서 상태 프로토콜(OCSP)

***PAN-OS***에서 인증서 해지 상태 확인은 선택적 기능입니다**.** 인증 포털**,** ***GlobalProtect,*** 사이트 간 ***IPSec VPN,*** 방화벽 또는 ***Panorama***에 대한 웹 인터페이스 액세스에 대한 사용자 및 디바이스 인증을 정의하는 인증서 프로파일에 대해 인증서가 인증되지 않았는지 확인하는 것이 모범 사례입니다**.** 취소되었습니다**.**

## 인증서 해지 목록(CRL)

각 인증 기관(CA)은 정기적으로 CRL(인증서 해지 목록)을 공용 리포지토리에 발행합니다. CRL은 일련번호로 해지된 인증서를 식별합니다. CA가 인증서를 해지한 후 다음 CRL 업데이트에는 해당 인증서의 일련번호가 포함됩니다. 방화벽은 DER(Distinguished Encoding Rules) 및 PEM(Privacy Enhanced Mail) 형식의 CRL을 지원합니다.

Palo Alto Networks 방화벽은 방화벽의 신뢰할 수 있는 CA 목록에 나열된 모든 CA에 대해 마지막으로 발급된 CRL을 다운로드하고 캐시합니다. 캐싱은 검증된 인증서에만 적용됩니다. 방화벽이 인증서의 유효성을 검사하지 않은 경우 방화벽 캐시는 발급 CA에 대한 CRL을 저장하지 않습니다. 또한 캐시는 만료될 때까지 CRL만 저장합니다.

여러 ***CRL*** 배포 지점***(CDP)***을 구성하고 방화벽이 첫 번째 ***CDP***에 연결할 수 없는 경우 방화벽은 나머지 ***CDP***를 확인하지 않습니다**.** 잘못된 ***CRL*** 요청을 리디렉션하려면 DNS 프록시를 대체 서버로 구성합니다**.**

인바운드 및 아웃바운드 SSL/TLS 트래픽의 복호화에 사용되는 인증서의 해지 상태를 확인하는 데 CRL을 사용하려면 SSL/TLS 복호화에 사용되는 인증서의 해지 상태 확인 구성을 참조하십시오.

사용자 및 디바이스를 인증하는 인증서의 해지 상태를 확인하는 데 CRL을 사용하려면 인증서 프로파일을 구성하고 애플리케이션과 관련된 인터페이스에 할당합니다. 인증 포털, GlobalProtect(원격 사용자 간 또는 대규모), 사이트 간 IPSec VPN 또는 Palo Alto Networks 방화벽 또는 Panorama에 대한 웹 인터페이스 액세스. 자세한 내용은 인증서의 해지 상태 확인 구성을 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 온라인 인증서 상태 프로토콜(OCSP)

SSL/TLS 세션을 설정할 때 클라이언트는 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증 인증서의 해지 상태를 확인할 수 있습니다. 인증 클라이언트는 인증서의 일련번호가 포함된 요청을 OCSP 응답자(서버)로 보냅니다. 응답자는 인증서를 발급한 인증 기관(CA)의 데이터베이스를 검색하고 상태(양호, 취소 또는 알 수 없음)를 포함하는 응답을 클라이언트에 반환합니다. OCSP 방식의 장점은 CRL의 발행 빈도(시간별, 일별, 주별)에 의존하지 않고 실시간으로 상태를 확인할 수 있다는 것입니다.

Palo Alto Networks 방화벽은 방화벽의 신뢰할 수 있는 CA 목록에 나열된 모든 CA에 대한 OCSP 상태 정보를 다운로드하고 캐시합니다. 캐싱은 검증된 인증서에만 적용됩니다. 방화벽이 인증서의 유효성을 검사하지 않은 경우 방화벽 캐시는 발급 CA에 대한 OCSP 정보를 저장하지 않습니다. 기업에 자체 공개 키 인프라(PKI)가 있는 경우 방화벽을 OCSP 응답자로 구성할 수 있습니다(OCSP 응답자 구성 참조).

방화벽이 SSL 포워딩 프록시로 작동할 때 인증서의 해지 상태를 확인하는 데 OCSP를 사용하려면 SSL/TLS 복호화에 사용되는 인증서의 해지 상태 확인 구성 아래 단계를 수행하십시오.

다음 애플리케이션은 인증서를 사용하여 사용자 및/또는 디바이스를 인증합니다. 인증 포털, GlobalProtect(원격 사용자 간 또는 대규모), 사이트 간 IPSec VPN 및 Palo Alto Networks 방화벽 또는 Panorama에 대한 웹 인터페이스 액세스. 인증서의 해지 상태를 확인하기 위해 OCSP를 사용하려면:

- OCSP 응답자를 구성합니다(방화벽을 OCSP 응답자로 구성하는 경우).
- 방화벽에서 HTTP OCSP 서비스를 활성화합니다(방화벽을 OCSP 응답자로 구성하는 경우).
- 각 애플리케이션에 대한 인증서를 만들거나 얻습니다.
- 각 애플리케이션에 대한 인증서 프로파일을 구성합니다.
- 관련 애플리케이션에 인증서 프로파일을 할당합니다.

OCSP 응답자를 사용할 수 없는 상황을 처리하려면 CRL을 대체 방법으로 구성하십시오. 자세한 내용은 인증서의 해지 상태 확인 구성을 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 인증서 배포

Palo Alto Networks 방화벽 또는 Panorama용 인증서를 배포하는 기본 접근 방식은 다음과 같습니다.

- 신뢰할 수 있는 타사 **CA**에서 인증서 가져오기 - VeriSign 또는 GoDaddy와 같은 신뢰할 수 있는 타사 인증 기관(CA)에서 인증서를 얻을 때의 이점은 일반 브라우저에 루트 CA 인증서가 포함되어 있기 때문에 신뢰할 수 있는 루트 인증서 저장소의 알려진 CA에서 최종 클라이언트가 이미 인증서를 신뢰할 수 있다는 것입니다. 따라서 최종 클라이언트가 방화벽 또는 Panorama와 보안 연결을 설정해야 하는 애플리케이션의 경우 루트 CA 인증서를 최종 클라이언트에 미리 배포하지 않아도 되도록 최종 클라이언트가 신뢰하는 CA에서 인증서를 구입하십시오. (일부 이러한 애플리케이션은 GlobalProtect 포털 또는 GlobalProtect Mobile Security Manager입니다.) 그러나 대부분의 타사 CA는 서명 인증서를 발급할 수 없습니다. 따라서 이 유형의 인증서는 방화벽에서 인증서를 발급해야 하는 애플리케이션(예: SSL/TLS 복호화 및 대규모 VPN)에 적합하지 않습니다. 외부 CA에서 인증서 받기를 참조하십시오.
- 엔터프라이즈 **CA**에서 인증서 가져오기 - 자체 내부 CA가 있는 엔터프라이즈는 이를 사용하여 방화벽 애플리케이션에 대한 인증서를 발급하고 방화벽으로 가져올 수 있습니다. 이점은 최종 클라이언트가 이미 엔터프라이즈 CA를 신뢰하고 있다는 것입니다. 필요한 인증서를 생성하여 방화벽으로 가져오거나 방화벽에서 CSR(인증서 서명 요청)을 생성하고 서명을 위해 엔터프라이즈 CA로 보낼 수 있습니다. 이 방법의 이점은 개인 키가 방화벽을 벗어나지 않는다는 것입니다. 엔터프라이즈 CA는 방화벽이 인증서를 자동으로 생성하는 데 사용하는 서명 인증서를 발급할 수도 있습니다(예: GlobalProtect 대규모 VPN 또는 SSL/TLS 복호화이 필요한 사이트). 인증서 및 개인 키 가져오기를 참조하십시오.
- 자체 서명된 인증서 생성 - 방화벽에서 자체 서명된 루트 CA 인증서를 생성하고 이를 사용하여 다른 방화벽 애플리케이션에 대한 인증서를 자동으로 발급할 수 있습니다.

> 이 방법을 사용하여 최종 클라이언트가 인증서를 신뢰해야 하는 애플리케이션에 대한 인증서를 생성하는 경우 루트 ***CA*** 인증서가 신뢰할 수 있는 루트 인증서 저장소에 없기 때문에 최종 사용자에게 인증서 오류가 표시됩니다. 이를 방지하려면 자체 서명된 루트 ***CA*** 인증서를 모든 최종 사용자 시스템에 배포하십시오. 인증서를 수동형으로 배포하거나 ***Active Directory GPO***(그룹 정책 개체)와 같은 중앙 집중식 배포 방법을 사용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

# 인증서 해지 상태에 대한 확인 설정

인증서의 해지 상태를 확인하기 위해 방화벽은 OCSP(온라인 인증서 상태 프로토콜) 및/또는 CRL(인증서 해지 목록)을 사용합니다. 이러한 방법에 대한 자세한 내용은 인증서 해지를 참조하십시오. 두 방법을 모두 구성하면 방화벽이 먼저 OCSP를 시도하고 OCSP 응답자를 사용할 수 없는 경우에만 CRL 메서드로 폴백됩니다. 엔터프라이즈에 자체 PKI(공개 키 인프라)가 있는 경우 OCSP 응답자로 작동하도록 방화벽을 구성할 수 있습니다.

다음 항목에서는 인증서 해지 상태를 확인하기 위해 방화벽을 구성하는 방법에 대해 설명합니다.

- OCSP 응답자 구성
- 인증서의 해지 상태 확인 구성
- SSL/TLS 복호화에 사용되는 인증서의 해지 상태 확인 구성

## OCSP 응답자 구성

OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 해지 상태를 확인하려면 OCSP 응답자(서버)에 액세스하도록 방화벽을 구성해야 합니다. OCSP 응답자를 관리하는 엔터티는 타사 인증 기관(CA)일 수 있습니다. 기업에 자체 PKI(공개 키 인프라)가 있는 경우 외부 OCSP 응답자를 사용하거나 방화벽 자체를 OCSP 응답자로 구성할 수 있습니다. OCSP에 대한 자세한 내용은 인증서 해지를 참조하십시오.

새 인증서(디바이스 > 인증서 관리 > 인증서)를 생성할 때만 ***OCSP*** 응답자 인증서 프로파일을 구성하십시오. 방화벽이 ***AIA***(기관 정보 액세스) 필드를 적절한 ***URL***로 채우도록 새 인증서를 생성할 때 ***OCSP*** 응답자를 지정한 다음 인증서 프로파일에 새 인증서를 지정합니다. 인증서 프로파일을 구성해도 기존 인증서 또는 루트 ***CA***에 대한 인증서 프로파일은 무시되지 않습니다.

***OCSP*** 유효성 검사를 활성화하거나 인증서 프로파일에서 인증서의 ***AIA*** 필드를 재정의할 수 있습니다. 인증서 프로파일 구성은 ***GlobalProtect***와 같이 방화벽에서 호스팅되는 서비스에 인증하는 인증서에 사용되는 인증서 유효성 검사 메커니즘을 결정합니다.

**STEP 1 |** 외부 OCSP 응답자를 정의하거나 방화벽 자체를 OCSP 응답자로 구성합니다.

1. 디바이스 > 인증서 관리 > **OCSP** 응답자를 선택한 다음 추가를 클릭합니다.
2. 응답자를 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분합니다. 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 사용해야 합니다.
3. 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.
4. 호스트 이름 필드에 OCSP 응답자의 호스트 이름(권장) 또는 IP 주소를 입력합니다. IPv4 또는 IPv6 주소를 입력할 수 있습니다. 이 값에서 PAN-OS는 URL을 자동으로 파생하여 확인 중인 인증서에 추가합니다.

   방화벽 자체를 OCSP 응답자로 구성하는 경우 호스트 이름은 방화벽이 OCSP 서비스에 사용하는 인터페이스의 IP 주소로 확인되어야 합니다.
5. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽이 OCSP 응답자 인터페이스에 대한 관리 인터페이스를 사용하도록 하려면 방화벽에서 OCSP 통신을 활성화합니다. 그렇지 않으면 다음 단계를 계속하여 대체 인터페이스를 구성합니다.

1. 디바이스 > 설정 > 인터페이스 > 관리를 선택합니다.
2. 네트워크 서비스 섹션에서 **HTTP OCSP** 체크박스를 선택한 다음 확인을 클릭합니다.

**STEP 3 |** 대체 인터페이스를 OCSP 응답자 인터페이스로 사용하려면 OCSP 서비스에 사용되는 인터페이스에 인터페이스 관리 프로파일을 추가합니다.

1. 네트워크 > 네트워크 프로파일 > 인터페이스 관리를 선택합니다.
2. 추가를 클릭하여 새 프로파일을 생성하거나 기존 프로파일의 이름을 클릭합니다.
3. **HTTP OCSP** 확인란을 선택하고 확인을 클릭합니다.
4. 네트워크 > 인터페이스를 선택한 다음 방화벽이 OCSP 서비스에 사용할 인터페이스 이름을 클릭합니다. 1단계에서 지정한 OCSP 호스트 이름은 이 인터페이스의 IP 주소로 확인되어야 합니다.
5. 고급 > 기타 정보를 선택한 다음 구성한 인터페이스 관리 프로파일을 선택합니다.
6. 확인 및 커밋을 클릭합니다.

## 인증서의 해지 상태 확인 구성

방화벽과 Panorama는 인증 포털, GlobalProtect, 사이트 간 IPSec VPN 및 방화벽/Panorama에 대한 웹 인터페이스 액세스와 같은 애플리케이션에 대한 사용자와 디바이스를 인증하기 위해 인증서를 사용합니다. 보안을 향상시키기 위해 방화벽 또는 Panorama를 구성하여 디바이스/사용자 인증에 사용하는 인증서의 해지 상태를 확인하는 것이 좋습니다.

**STEP 1 |** 각 애플리케이션에 대한 인증서 프로파일을 구성합니다.

프로파일에 하나 이상의 루트 CA 인증서를 할당하고 방화벽이 인증서 해지 상태를 확인하는 방법을 선택합니다.

다양한 애플리케이션에서 사용하는 인증서에 대한 자세한 내용은 키 및 인증서를 참조하십시오.

**STEP 2 |** 관련 애플리케이션에 인증서 프로파일을 할당합니다.

인증서 프로파일을 할당하는 단계는 인증서 프로파일이 필요한 애플리케이션에 따라 다릅니다.

## SSL/TLS 복호화에 사용되는 인증서의 해지 상태 확인 구성

방화벽은 인바운드 및 아웃바운드 SSL/TLS 트래픽을 해독하여 위협에 대한 트래픽을 검사합니다. 트래픽을 허용하고 암호 프로파일을 규칙에 적용할 수 있는 보안 정책 규칙을 만들 때 해당 트래픽을 해독하는 유사한 복호화 정책 규칙을 생성합니다. 트래픽을 해독하지 않으면 방화벽은 보안 프로파일을 사용하여 트래픽을 검사할 수 없습니다(표시되지 않는 내용을 검사할 수 없습니다). 방화벽은 트래픽을 포워딩하기 전에 다시 암호화합니다. (SSL 인바운드 검사 및 SSL 포워드 프록시 참조.) 방화벽을 구성하여 다음과 같이 복호화에 사용되는 인증서의 해지 상태를 확인할 수 있습니다.

***SSL/TLS*** 복호화 인증서에 대한 해지 상태 확인을 사용하도록 설정하면 세션을 설정하는 프로세스에 시간이 추가됩니다. 세션 시간 종료 전에 확인이 완료되지 않으면 사이트에 액세스하려는 첫 번째 시도가 실패할 수 있습니다. 이러한 이유로 기본적으로 확인이 비활성화됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 해지 상태 요청에 대한 서비스별 시간 지정 간격을 정의합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 기능 섹션에서 암호 해독 인증서 해지 설정을 선택합니다.
2. 방화벽이 온라인 인증서 상태 프로토콜(OCSP) 또는 CRL(인증서 해지 목록) 방법을 사용하여 인증서 해지 상태를 확인하는지의 여부에 따라 다음 단계 중 하나 또는 둘 다를 수행합니다. 방화벽이 둘 다 사용하는 경우 먼저 OCSP를 시도합니다. OCSP 응답자를 사용할 수 없는 경우 방화벽은 CRL 메서드를 시도합니다.
   - CRL 섹션에서 사용 체크박스를 선택한 다음 타임아웃 수신을 입력합니다. 방화벽이 CRL 서비스에서 응답을 기다리는 것을 중지하는 간격(1-60초)입니다.
   - OCSP 섹션에서 사용 체크박스를 선택한 다음 타임아웃 수신을 입력합니다. 이는 방화벽이 OCSP 응답자의 응답을 기다리는 것을 중지하는 간격(1-60초)입니다.

   2단계에서 지정한 인증서 상태 시간 계산값에 따라 방화벽은 타임아웃 수신 간격 중 하나 또는 둘 다 통과하기 전에 타임아웃을 등록할 수 있습니다.

**STEP 2 |** 해지 상태 요청에 대한 총 시간 지정 간격을 정의합니다.

인증서 상태 타임아웃을 입력합니다. 방화벽이 인증서 상태 서비스에서 응답을 기다리는 것을 멈추고 3단계에서 선택적으로 정의하는 세션 차단 논리를 적용하는 간격(1-60초)입니다. 인증서 상태 타임아웃은 다음 OCSP/CRL 타임아웃 수신과 같습니다.

- OCSP와 CRL 모두를 사용하도록 설정하는 경우 방화벽은 인증서 상태 타임아웃 값 또는 두 개의 수신 타임아웃 값의 집계 중 더 짧은 간격이 경과한 후 요청 타임아웃를 등록합니다.
- OCSP만 사용하도록 설정한 경우 방화벽은 인증서 상태 타임아웃 값 또는 OCSP 수신 타임아웃 값 중 더 짧은 간격이 경과한 후 요청 타임아웃을 등록합니다.
- CRL만 사용하도록 설정하는 경우 방화벽은 인증서 상태 타임아웃 값 또는 CRL 수신 시간 초과 값 중 더 짧은 간격이 경과한 후 요청 타임아웃를 등록합니다.

**STEP 3 |** 알 수 없는 인증서 상태 또는 해지 상태 리퀘스트 타임아웃에 대한 차단 동작을 정의합니다.

OCSP 또는 CRL 서비스가 알 수 없는 인증서 해지 상태를 반환할 때 방화벽이 SSL/TLS 세션을 차단하려면 알 수 없는 인증서 상태 체크박스가 있는 블록 세션을 선택합니다. 그렇지 않으면 방화벽이 세션으로 진행됩니다.

리퀘스트 타임아웃을 등록한 후 방화벽이 SSL/TLS 세션을 차단하려면 인증서 상태 확인 타임아웃 체크박스에 대한 블록 세션을 선택합니다. 그렇지 않으면 방화벽이 세션으로 진행됩니다.

**STEP 4 |** 확인 및 커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 마스터 키 구성

모든 방화벽과 Panorama 관리 서버에는 구성의 모든 개인 키와 암호를 암호화하여 보안을 보호하는 기본 마스터 키가 있습니다(예: SSL 포워드 프록시 복호화에 사용되는 개인 키).

암호화에 고유한 마스터 키를 사용하도록 가능한 한 빨리 기본 마스터 키를 변경합니다.

HA(고가용성) 구성에서는 마스터 키가 HA 피어 간에 동기화되지 않으므로 두 방화벽에서 동일한 마스터 키를 사용해야 합니다. 그렇지 않으면 HA 동기화가 제대로 작동하지 않습니다.

Panorama를 사용하여 방화벽을 관리하는 경우 Panorama 및 관리되는 모든 방화벽에서 동일한 마스터 키를 구성하거나 관리되는 각 방화벽에 대해 고유한 마스터 키를 구성할 수 있습니다. HA 구성에서 관리되는 방화벽의 경우 각 HA 피어에 대해 동일한 마스터 키를 구성해야 합니다. Panorama™ 관리 서버에서 방화벽을 관리하는 경우 Panorama에서 마스터 키 관리를 참조하십시오.

마스터 키를 안전한 위치에 보관해야 합니다. 마스터 키를 복구할 수 없으며 기본 마스터 키를 복원하는 유일한 방법은 방화벽을 공장 기본 설정으로 재설정하는 것입니다.

**STEP 1 |** 구성을 백업합니다.

**STEP 2 |** (HA에만 해당) 구성 동기화를 사용하지 않도록 설정합니다.

방화벽 HA 쌍에 새 마스터 키를 배포하기 전에 이 단계가 필요합니다.

방화벽 HA 쌍에 새 마스터 키를 배포하기 전에 구성 동기화를 사용하지 않도록 설정해야 합니다. Panorama 관리 방화벽의 경우 새 마스터 키를 배포하기 전에 구성 동기화를 비활성화하지 않으면 Panorama에서 기본 방화벽에 대한 연결이 끊어집니다.

1. 디바이스 > 고가용성 > 일반을 선택하고 설정을 수정합니다.
2. 구성 동기화 사용을 비활성화(지우기)한 다음 확인을 클릭합니다.
3. 구성 변경 사항을 커밋합니다.

**STEP 3 |** 디바이스 > 마스터 키 및 진단을 선택하고 마스터 키 섹션을 수정합니다.

**STEP 4 |** 현재 마스터 키가 있는 경우 입력합니다.

**STEP 5 |** 새 새 마스터 키를 정의한 다음 새 마스터 키 확인을 정의합니다. 키에는 정확히 16자여야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 마스터 키 수명을 지정하려면 키가 만료되는 일 및/또는 시간을 입력합니다.

현재 키가 만료되기 전에 새 마스터 키를 구성해야 합니다. 마스터 키가 만료되면 방화벽 또는 Panorama가 유지 관리 모드에서 자동으로 재부팅됩니다. 그런 다음 방화벽을 공장 기본 설정으로 재설정해야합니다.

디바이스가 수행하는 암호화 수에 따라 수명을 *2*년 이하로 설정합니다. 디바이스가 수행하는 암호화가 많을수록 설정해야 하는 수명이 단축됩니다. 마스터 키를 변경하기 전에 고유한 암호화가 무효화되지 않는 것이 중요합니다. 각 마스터 키는 마스터 키 값과 초기화 벡터*(IV)* 값을 기반으로 최대 $2^{32}$개의 고유한 암호화를 제공할 수 있습니다. $2^{32}$개의 고유한 암호화가 끝나면 암호화가 반복되며*(*더 이상 고유하지 않습니다*)* 보안 위험이 있습니다.

마스터 키에 대한 미리 알림 값*(*다음 단계 참조*)*을 설정하고 미리 알림이 발생하면 마스터 키를 변경합니다.

**STEP 7 |** 방화벽이 만료 알람을 생성할 때 마스터 키가 만료되기까지의 일 및 시간 수를 지정하는 알림 시간을 입력합니다. 방화벽은 자동으로 시스템 알람 대화 상자를 열어 알람을 표시합니다.

예약된 유지 관리 기간에 만료되기 전에 새 마스터 키를 구성할 수 있는 충분한 시간을 제공하도록 미리 알림을 설정합니다. 미리 알림 시간이 만료되고 방화벽 또는 *Panorama*가 알림 로그를 보내면 마스터 키를 변경하면 수명이 만료될 때까지 기다리지 마십시오. 그룹화된 디바이스의 경우 모든 디바이스*(*예 *: Panorama*가 관리하는 방화벽 및 방화벽 *HA* 쌍*)*를 추적하고 그룹의 모든 디바이스에 대한 알림 값이 만료되면 마스터 키를 변경합니다.

만료 알람이 표시되도록 하려면 디바이스 > 로그 설정을 선택한 다음 알람 설정을 편집하고 알람을 사용하도록 설정합니다.

**STEP 8 |** 자동 갱신 마스터 키를 활성화하여 마스터 키를 자동으로 갱신하도록 방화벽을 구성합니다. 동일한 마스터 키로 자동 갱신을 구성하려면 동일한 마스터 키를 갱신할 일 수 및/또는 시간을 지정합니다. 키 확장을 통해 방화벽은 계속 작동하고 네트워크 보안을 계속할 수 있습니다. 기존 마스터 키 수명이 곧 만료되는 경우 새 키를 구성하기 위해 대체할 수 없습니다.

마스터 키를 자동으로 갱신하는 것은 이점과 위험이 있습니다. 이점은 마스터 키 수명 연장은 수명이 만료되기 전에 마스터 키를 변경하지 않으면서 보호된다는 것입니다. 위험은 마스터 키와 함께 디바이스가 수행하는 암호화 수가 마스터 키가 생성할 수 있는 고유 암호화 수($2^{32}$개의 고유 암호화)를 초과하는 경우 암호화가 반복되고 보안 위험이 발생한다는 것입니다.

마스터 키가 만료되면*(*자동으로 갱신하지 않고 적시에 교체하지 않음*)* 디바이스는 유지 관리 모드로 전환됩니다.

자동 갱신 마스터 키를 사용하도록 설정하면 총 시간*(*수명 및 자동 갱신 시간*)*은 디바이스의 고유한 암호화가 무효화되지 않도록 설정합니다. 예를 들어 디바이스가 마스터 키의 고유 암호화 수를 *2*년 반 동안 소비한다고 생각되면 *2*년 동안 수명을 설정하고 미리 알림 시간을 *60*일로 설정하고 자동 갱신 마스터 키를 *60-90*일로 설정하여 수명이 만료되기 전에 새 마스터 키를 구성하는 추가 시간을 제공할 수 있습니다. 그러나 수명 만료 전에 마스터 키를 변경하여 디바이스가 암호화를 반복하지 않도록 하는 것이 가장 좋습니다.

마스터 키를 구성할 때 사용 가능한 다음 유지 관리 기간이 만료될 때까지의 일 수를 고려하여 키 수명이 만료된 후 자동으로 갱신합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** (선택사항)보안을 추가하려면 **HSM**을 사용하여 마스터 키를 암호화할지의 여부를 선택합니다. 자세한 내용은 HSM을 사용하여 마스터 키 암호화를 참조하십시오.

**STEP 10 |** 확인 및 커밋을 클릭합니다.

**STEP 11 |** (HA에만 해당) 구성 동기화를 다시 사용하도록 설정합니다.

1. 디바이스 > 고가용성 > 일반을 선택하고 설정을 수정합니다.
2. 구성 동기화 사용을 활성화(선택)한 다음 확인을 클릭합니다.
3. 구성 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 마스터 키 암호화

물리적 및 가상 Palo Alto Networks 디바이스에서는 AES-256-CBC 또는 AES-256-GCM(PAN-OS 10.0에 도입) 암호화 알고리즘을 사용하여 키 및 암호와 같은 데이터를 암호화하는 마스터 키를 구성할 수 있습니다. AES-256-GCM은 AES-256-CBC보다 더 강력한 암호화를 제공하고 보안 태세를 향상시킵니다. 또한 기본 무결성 검사도 포함되어 있습니다. 마스터 키는 구성된 암호화 알고리즘을 사용하여 방화벽과 Panorama에 저장된 중요한 데이터를 암호화합니다. 암호화 알고리즘을 AES-256-GCM로 설정하면 HSM을 사용하여 HSM에 저장된 암호화 키로 마스터 키를 암호화할 수 있습니다.

마스터 키가 데이터를 암호화하는 데 사용하는 기본 암호화 알고리즘은 AES-256-CBC이며, 마스터 키는 PAN-OS 10.0 이전에 사용한 것과 동일한 알고리즘입니다. AES-256-CBC는 Panorama로 방화벽을 관리할 때 관리되는 방화벽이 다른 PAN-OS 릴리스에 있을 수 있으며 PAN-OS 10.2보다 일찍 출시된 PAN-OS의 방화벽은 AES-256-GCM을 지원하지 않기 때문에 기본 암호화 수준입니다. Panorama가 관리되는 디바이스에서 사용할 수 있는 가장 낮은 수준의 암호화를 사용해야 하는 이유입니다. 예를 들어 일부 관리되는 디바이스가 PAN-OS 10.2를 실행하고 일부 실행 이전 버전을 실행하는 경우 Panorama는 AES-256-CBC를 사용해야 합니다. 그러나 관리되는 모든 디바이스가 PAN-OS 10.2 이상 실행되면 Panorama와 관리되는 모든 디바이스는 AES-256-GCM을 사용할 수 있습니다.

***Panorama*** 및 해당 관리 디바이스에서 동일한 암호화 수준을 사용하고 방화벽 쌍에서 동일한 암호화 수준을 사용합니다. 디바이스를 업그레이드하여 가능한 가장 강력한 암호화 알고리즘을 사용합니다. 모든 ***Panorama*** 관리 디바이스가 ***PAN-OS 10.0***을 실행하는 경우 모든 디바이스에서 ***AES-256-GCM***을 사용합니다. 서로 다른 암호화 수준을 사용하는 관리되는 디바이스 또는 페어링된 디바이스의 구성이 동기화되지 않을 수 있습니다.

암호화 알고리즘을 AES-256-GCM로 변경하면 디바이스는 AES-256-CBC 대신 암호화하여 중요한 데이터를 암호화합니다. 한 알고리즘에서 다른 알고리즘으로 변경하면 다음을 지정할 수도 있습니다.

- 새 알고리즘으로 기존 암호화된 데이터를 다시 암호화합니다.
- 기존 데이터를 이전 암호화 알고리즘으로 암호화하고 새(향후) 암호화에 대해서만 새 알고리즘을 사용합니다.

기본적으로 암호화 알고리즘을 변경할 때 디바이스는 새 알고리즘을 사용하여 기존 암호화된 데이터를 다시 암호화하고 새 데이터를 암호화합니다. ***Panorama***로 디바이스를 관리하는 경우 다양한 버전의 ***PAN-OS***에 있을 수 있으며 최신 암호화 알고리즘을 지원하지 않을 수 있습니다. 암호화 알고리즘을 변경하거나 이미 암호화된 데이터를 다시 암호화하기 전에 ***Panorama*** 및 관리되는 디바이스가 지원하는 암호화 알고리즘을 이해해야 합니다.

- 마스터 키 암호화 수준 구성
- 방화벽 HA 쌍에서 키 암호화 마스터
- 마스터 키 암호화 로그
- AES-256-GCM을 위한 고유한 마스터 키 암호화


©2023 Palo Alto Networks, Inc.

# 마스터 키 암호화 수준 구성

CLI를 사용하여 마스터 키 암호화 알고리즘 수준과 현재 암호화된 모든 데이터를 새 암호화 알고리즘 수준으로 다시 암호화할지의 여부를 구성합니다. 키워드의 순서에 따라 암호화 수준을 변경하거나 암호화 수준을 변경하고 이전에 암호화된 데이터를 다시 암호화할지의 여부도 지정할 수 있습니다.

다음 작동 CLI 명령은 암호화 수준을 변경하고 지정된 암호화 수준으로 현재 암호화된 모든 데이터를 자동으로 다시 암호화합니다.

```
admin@PA-NGFW>request encryption-level level <0|1|2>
```

다음 작동 CLI 명령은 암호화 수준을 변경하고 현재 암호화된 모든 데이터를 새 암호화 수준으로 다시 암호화할지 여부를 지정합니다.

```
admin@PA-NGFW>request encryption-level re-encrypt <yes|no> level <0|
1|2>
```

| 키워드 | 옵션 |
|---|---|
| 수준 | **0** = 기본 알고리즘(AES-256-CBC)을 사용하여 데이터 암호화<br>**1** = AES-256-CBC 알고리즘을 사용하여 데이터 암호화<br>**2** = AES-256-GCM 알고리즘을 사용하여 데이터 암호화<br>방화벽은 현재 암호화된 모든 데이터를 다시 암호화하고 지정된 알고리즘을 사용하여 새로운 민감한 데이터를 암호화합니다. 기존 암호화 데이터를 새 알고리즘으로 다시 암호화하지 않으려면 명령 문자열에 **re-encrypt no**를 지정하십시오. 이렇게 하면 방화벽이 이미 암호화한 데이터를 방화벽이 자동으로 다시 암호화하는 것을 방지할 수 있습니다.<br>*Panorama* 및 모든 관리 디바이스*(*또는 *HA* 쌍의 두 디바이스 모두*)*가 *PAN-OS 10.2* 이상을 실행하고 *AES-256-GCM*을 사용하도록 모든 디바이스를 구성하는 경우에만 *AES-256-GCM*을 사용하십시오. 다른 암호화 수준을 사용하는 관리 또는 페어링된 디바이스는 동기화되지 않을 수 있습니다. |
| 재암호화 | **no** = 현재 암호화된 데이터를 다시 암호화하지 않습니다. 방화벽은 현재 암호화된 데이터를 다시 암호화하지 않습니다. 현재 암호화된 데이터는 방화벽이 원래 데이터를 암호화하는 데 사용했던 알고리즘으로 암호화된 상태를 유지합니다. 방화벽은 지정된 알고리즘을 사용하여 향후 중요한 데이터를 암호화합니다. |


©2023 Palo Alto Networks, Inc.

| 키워드 | 옵션 |
| --- | --- |
| | **yes** = 지정된 알고리즘으로 현재 암호화된 데이터를 다시 암호화하고 해당 알고리즘을 사용하여 향후 민감한 데이터를 암호화합니다. |

작동 CLI 명령 **show system masterkey-properties**를 사용하여 현재 디바이스에 구성된 암호화 알고리즘(레벨)을 확인합니다. 예를 들면 다음과 같습니다.

```
admin@PA-NGFW>show system masterkey-properties
```

```
마스터 키는 다음에서 만료됩니다: 지정되지 않은 미리 알림은 다음에서 시작됩니다:
 hsm에서 지정되지 않은 마스터 키: 마스터 키 수명을 자동으로 갱신하지 않음: 0 암
호화 수준: 1
```

출력은 현재 암호화 수준이 AES-256-CBC인 1임을 보여줍니다.

이전 버전의 PAN-OS로 다운그레이드하면 다운그레이드된 PAN-OS 버전이 지원하는 수준으로 암호화 알고리즘을 자동으로 되돌리고 해당 수준을 사용하여 암호화된 데이터를 자동으로 재암호화하여 디바이스가 필요에 따라 데이터를 복호화하고 사용할 수 있도록 합니다. 예를 들어, 디바이스가 PAN-OS 10.2 버전을 사용하며 AES-256-GCM을 암호화 알고리즘으로 사용하고(이전 버전의 PAN-OS에서는 지원되지 않음) PAN-OS 9.1 버전으로 다운그레이드하면 디바이스가 다시 암호화된 데이터를 PAN-OS 9.1 버전에서 지원되는 AES-256-CBC로 암호화합니다.

## 방화벽 HA 쌍에서 키 암호화 마스터

방화벽 고가용성(HA) 쌍에서 AES-256-GCM 암호화 수준을 사용하려면 두 방화벽이 AES-256-GCM을 지원하도록 두 방화벽 모두 PAN-OS 10.0을 실행해야 합니다. HA 쌍의 방화벽 중 하나가 PAN-OS 10.0보다 이전 버전을 실행하는 경우 AES-256-GCM을 사용할 수 없습니다. 두 방화벽이 모두 PAN-OS 10.0에 있는 경우 두 방화벽 모두 AES-256-CBC 또는 AES-256-GCM 암호화 키를 디코딩할 수 있으므로 둘 중 하나의 암호화 수준을 사용할 수 있습니다. 그러나 두 방화벽은 동기화되지 않을 가능성을 피하기 위해 동일한 암호화 수준을 사용해야 합니다.



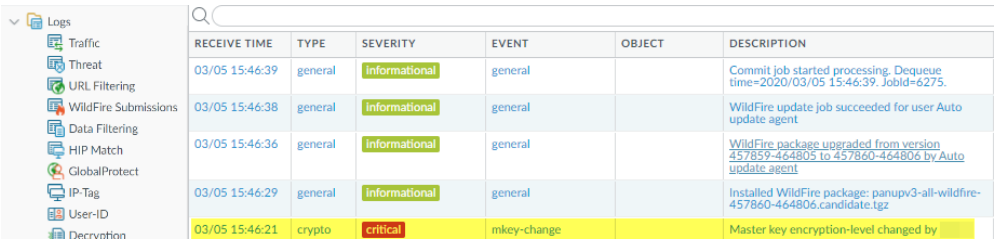
*HA* 쌍의 두 방화벽에서 *AES-256-GCM* 암호화를 사용합니다. *AES-256-GCM*을 사용하든 *AES-256-CBC*를 사용하든 두 방화벽에서 동일한 알고리즘을 사용하십시오.

두 방화벽이 모두 PAN-OS 10.0을 실행하는 HA 쌍에서 방화벽의 암호화 수준을 변경하기 위해 HA를 비활성화할 필요가 없습니다.

## 마스터 키 암호화 로그

마스터 키 암호화 알고리즘(레벨)을 변경할 때 방화벽은 시스템 로그(모니터 > 로그 > 시스템)를 생성합니다.


©2023 Palo Alto Networks, Inc.




마스터 키 암호화에 대한 모든 시스템 로그를 보려면 유형 암호화: **(subtype eq crypto)**의 모든 로그를 표시하는 필터를 생성합니다.

## AES-256-GCM을 위한 고유한 마스터 키 암호화

마스터 키는 고유한 조합이 소진되기 전에 유한한 수의 고유한 암호화만 생성할 수 있으며 암호화를 반복해야 합니다. 방화벽은 초기화 벡터(IV)와 함께 AES-256-GCM 암호화 알고리즘을 사용하여 고유한 암호화를 생성합니다. IV는 각 암호화가 고유하도록 암호화를 생성하는 데 한 번만 사용해야 하는 임의의 숫자입니다.

마스터 키와 IV를 사용하는 각 암호화는 위조 공격을 방지하기 위해 고유해야 합니다. 방화벽은 인증된 암호화가 동일한 IV 및 동일한 키를 사용하여 둘 이상의 고유한 입력 데이터 세트에서 생성될 확률이 $2^{32}$ 이하인 고유성 요구 사항을 충족합니다.

IV가 모든 고유 값을 실행할 때 IV 값이 반복됩니다. IV 값이 반복될 때 동일한 마스터 키와 반복되는 IV 값을 사용하여 데이터를 암호화한다는 것은 이전에 다른 데이터에 사용했던 암호화와 동일하다는 의미입니다. 방화벽이 둘 이상의 민감한 데이터에 동일한 암호화(마스터 키 및 IV 값 조합)를 사용하지 못하도록 시스템의 고유 암호화가 다 떨어지기 전에 마스터 키를 변경합니다. 고유한 암호화 조합을 반복하거나 재사용해서는 안 됩니다.

마스터 키를 변경해야 하는 시기를 추적하려면 각 어플라이언스(디바이스 > 마스터키 및 진단 및 마스터 키 편집)에서 마스터 키 수명 및 미리 알림 값을 설정합니다. 마스터 키 암호화의 예상 볼륨을 기반으로 값을 보수적으로 설정하여 모든 암호화가 고유하고 암호화 조합이 반복되거나 재사용되지 않도록 합니다.

 ©2023 Palo Alto Networks, Inc.

# 인증서 받기


- 자체 서명된 루트 CA 인증서 생성
- 인증서 생성
- 인증서 및 개인 키 가져오기
- 외부 CA로부터 인증서 받기
- 디바이스 인증서 설치
- SCEP를 사용하여 인증서 배포


## 자체 서명된 루트 CA 인증서 생성

자체 서명된 루트 인증서 기관(CA) 인증서는 인증서 체인에서 가장 많이 사용되는 인증서입니다. 방화벽은 이 인증서를 사용하여 다른 용도로 인증서를 자동으로 발급할 수 있습니다. 예를 들어 방화벽은 SSL/TLS 복호화 및 GlobalProtect 대규모 VPN의 위성에 대한 인증서를 발급합니다.

방화벽과 보안 연결을 설정할 때 원격 클라이언트는 인증서를 발급한 루트 CA를 신뢰해야 합니다. 그렇지 않으면 클라이언트 브라우저에 인증서가 유효하지 않으며(보안 설정에 따라) 연결을 차단할 수 있다는 경고가 표시됩니다. 이를 방지하기 위해 자체 서명된 루트 CA 인증서를 생성한 후 클라이언트 시스템으로 가져옵니다.

> *Palo Alto Networks* 방화벽 또는 *Panorama*에서는 *CA* 인증서인 경우에만 자체 서명된 인증서를 생성할 수 있습니다.

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

**STEP 2 |** 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.

**STEP 3 |** 생성을 클릭합니다.

**STEP 4 |** **GlobalProtect_CA**와 같은 인증서 이름을 입력합니다. 이 이름은 대소문자를 구별하며 방화벽에 최대 63자 또는 Panorama에서 최대 31자까지 가질 수 있습니다. 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 사용해야 합니다.

**STEP 5 |** 공통 이름 필드에 이 인증서를 사용하는 서비스를 구성하는 인터페이스의 FQDN(권장) 또는 IP 주소를 입력합니다.

**STEP 6 |** 방화벽에 둘 이상의 vsys가 있고 모든 vsys에서 인증서를 사용할 수 있게 하려면 공유 확인란을 선택합니다.

**STEP 7 |** 인증서를 자체 서명으로 지정하려면 서명자 필드를 비워 둡니다.

**STEP 8 |** (필수) 인증서 기관 체크박스를 선택합니다.

**STEP 9 |** **OCSP** 응답자 필드를 비워 두십시오. 해지 상태 확인은 루트 CA 인증서에는 적용되지 않습니다.

**STEP 10 |** 생성 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 인증서 생성

Palo Alto Networks 방화벽 및 Panorama는 인증서를 사용하여 SSL/TLS 복호화, 인증 포털, GlobalProtect, 사이트 간 IPSec VPN 및 방화벽/Panorama에 대한 웹 인터페이스 액세스를 비롯한 여러 애플리케이션에서 클라이언트, 서버, 사용자 및 디바이스를 인증합니다. 각 용도에 대한 인증서 생성: 자세한 내용은 키 및 인증서를 참조하십시오.

인증서를 생성하려면 먼저 자체 서명된 루트 CA 인증서를 생성하거나 인증서를 가져와 서명해야 합니다(인증서 및 개인 키 가져오기). 인증서 해지 상태를 확인하기 위해 OCSP(온라인 인증서 상태 프로토콜)를 사용하려면 인증서를 생성하기 전에 OCSP 응답자를 구성하십시오.

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

**STEP 2 |** 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.

**STEP 3 |** 생성을 클릭합니다.

**STEP 4 |** GlobalProtect 엔드포인트에 SCEP 인증서를 배포하지 않으려면 로컬(기본값)을 인증서 유형으로 선택합니다.

**STEP 5 |** 인증서 이름을 입력합니다. 이 이름은 대소문자를 구별하며 방화벽에 최대 63자 또는 Panorama에서 최대 31자까지 가질 수 있습니다. 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 사용해야 합니다.

**STEP 6 |** 공통 이름 필드에 이 인증서를 사용하는 서비스를 구성하는 인터페이스의 FQDN(권장) 또는 IP 주소를 입력합니다.

**STEP 7 |** 방화벽에 둘 이상의 vsys가 있고 모든 vsys에서 인증서를 사용할 수 있게 하려면 공유 확인란을 선택합니다.

**STEP 8 |** 서명자 필드에서 인증서를 발급할 루트 CA 인증서를 선택합니다.

**STEP 9 |** (선택 사항) 개인 키 내보내기를 차단할지 여부를 선택합니다.



인증서를 내보낼 때 개인 키가 내보내지지 않도록 하려면 이 설정을 활성화합니다.

이 설정을 사용하도록 설정하는 경우 ***Panorama*** 또는 다른 방화벽으로 인증서를 가져오는 경우 연결된 개인 키를 수동으로 가져와야 합니다. ***Panorama***가 관리하는 방화벽의 경우 인증서를 가져온 관리형 방화벽에 구성 변경 사항을 성공적으로 푸시하려면 개인 키가 필요합니다.

**STEP 10 |** (선택 사항) **OCSP** 응답자를 선택합니다.

**STEP 11 |** 키 생성 알고리즘의 경우 **RSA**(기본값) 또는 타원 곡선 **DSA**(ECDSA)를 선택합니다. ECDSA는 이를 지원하는 클라이언트 브라우저 및 운영 체제에 권장됩니다.



***PAN-OS 6.1*** 및 이전 릴리스를 실행하는 방화벽은 ***Panorama***™에서 푸시한 모든 ***ECDSA*** 인증서를 삭제하고 ***ECDSA*** 인증 기관***(CA)***에서 서명한 모든 ***RSA*** 인증서는 해당 방화벽에서 유효하지 않습니다.

하드웨어 보안 모듈(HSM)을 사용하여 SSL/TLS 복호화에 사용되는 ECDSA 키를 저장할 수 없습니다.


©2023 Palo Alto Networks, Inc.

**STEP 12 |** 인증서 키 길이를 정의하려면 비트 수를 선택하십시오. 숫자가 높을수록 더 안전하지만 처리 시간이 더 오래 걸립니다.

**STEP 13 |** 다이제스트 알고리즘을 선택합니다. 가장 안전한 것부터 가장 낮은 것까지 옵션은 **sha512**, **sha384**, **sha256** (기본값), **sha1** 및 **md5**입니다.

*TLSv1.2*에 의존하는 방화벽 서비스*(*예*:* 웹 인터페이스에 대한 관리자 액세스*)*를 요청할 때 사용되는 클라이언트 인증서는 다이제스트 알고리즘으로 ***sha512***를 가질 수 없습니다*.* 클라이언트 인증서는 더 낮은 다이제스트 알고리즘*(*예*: **sha384**)*을 사용해야 하며 방화벽 서비스에 대한 SSL/TLS 서비스 프로파일을 구성할 때 최대 버전을 ***TLSv1.1***로 제한해야 합니다*.*

**STEP 14 |** 만료에 인증서가 유효한 일 수 (기본값은 365) 를 입력합니다.

**STEP 15 |** (선택 사항) 인증서 특성을 추가하여 인증서를 사용할 방화벽 및 서비스를 고유하게 식별합니다.

호스트 이름*(DNS* 이름*)* 속성을 추가하는 경우*,* 호스트 이름이 인증서의 개체 대체 이름*(SAN)* 필드를 채우고 일부 브라우저에서는 인증서가 보호하는 도메인을 지정하기 위해 *SAN*이 필요하기 때문에 일반 이름과 일치시키는 것이 가장 이상적입니다*.* 또한 공통 이름과 일치하는 호스트 이름은 *GlobalProtect*에 필수입니다*.*

**STEP 16 |** 생성을 클릭하고 디바이스 인증서 페이지에서 인증서 이름을 클릭합니다.

방화벽의 시간대에 관계없이 항상 인증서 유효 기간 및 만료 날짜*/*시간에 해당하는 *GMT(*그리니치 표준시*)*가 표시됩니다*.*

**STEP 17 |** 방화벽에서 사용하려는 인증서에 해당하는 체크박스를 선택합니다.

예를 들어, 방화벽이 이 인증서를 사용하여 syslog를 외부 syslog 서버로 안전하게 포워딩하는 경우 보안 **Syslog**용 인증서 체크박스를 선택합니다.

**STEP 18 |** 확인 및 커밋을 클릭합니다.

## 인증서 및 개인 키 가져오기

기업에 자체 공개 키 인프라(PKI)가 있는 경우 CA(엔터프라이즈 인증서 기관)에서 인증서 및 개인 키를 방화벽으로 가져올 수 있습니다. 엔터프라이즈 CA 인증서(신뢰할 수 있는 타사 CA에서 구입한 대부분의 인증서와 달리)는 SSL/TLS 복호화 또는 대규모 VPN과 같은 애플리케이션에 대한 CA 인증서를 자동으로 발급할 수 있습니다.

*Palo Alto Networks* 방화벽 또는 *Panorama*에서는 *CA* 인증서인 경우에만 자체 서명된 인증서를 가져올 수 있습니다*.*

자체 서명된 루트 *CA* 인증서를 모든 클라이언트 시스템에 가져오는 대신 클라이언트가 이미 엔터프라이즈 *CA*와 신뢰 관계를 맺고 배포를 간소화하기 때문에 엔터프라이즈 *CA*에서 인증서를 가져오는 것이 좋습니다*.*

가져올 인증서가 인증서 체인의 일부인 경우 전체 체인을 가져오는 것이 좋습니다*.*

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 엔터프라이즈 CA에서 방화벽이 인증에 사용할 인증서 및 개인 키를 내보냅니다.

개인 키를 내보낼 때 는 전송키를 암호화하기 위해 암호를 입력해야 합니다. 관리 시스템이 인증서 및 키 파일에 액세스할 수 있는지 확인합니다. 키를 방화벽에 가져올 때 동일한 암호를 복호화하려면 동일한 암호를 입력해야 합니다.

**STEP 2 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

**STEP 3 |** 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.

**STEP 4 |** 가져오기를 클릭하고 인증서 이름을 입력합니다. 이 이름은 대소문자를 구별하며 방화벽에 최대 63자 또는 Panorama에서 최대 31자까지 가질 수 있습니다. 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 사용해야 합니다.

**STEP 5 |** 모든 가상 시스템에서 인증서를 사용할 수 있도록 하려면 공유 확인란을 선택합니다. 이 확인란은 방화벽이 여러 가상 시스템을 지원하는 경우에만 나타납니다.

**STEP 6 |** CA에서 받은 인증서 파일의 경로와 이름을 입력하거나 파일을 찾으려면 찾아보기를 입력합니다.

**STEP 7 |** 파일 형식 선택:

- 암호화된 개인 키 및 인증서**(PKCS12**)-키와 인증서가 단일 컨테이너(인증서 파일)에 있는 기본 및 가장 일반적인 형식입니다. 하드웨어 보안 모듈(HSM)이 이 인증서의 개인 키를 저장하는 경우 하드웨어 보안 모듈 체크박스에 있는 개인 키를 선택합니다.
- **Base64** 인코딩된 인증서**(PEM)** - 인증서와 별도로 키를 가져와야 합니다. HSM(하드웨어 보안 모듈)이 이 인증서의 개인 키를 저장하는 경우 하드웨어 보안 모듈 체크박스에 있는 개인 키를 선택한 후 다음 단계를 건너뜁니다. 그렇지 않으면 개인 키 가져오기 체크박스를 선택한 다음 키 파일을 입력하거나 찾아보기를 한 후 다음 단계로 계속 이동합니다.

> *(Panorama 관리 방화벽)* 인증서가 성공적으로 생성될 때 개인 키 내보내기 차단을 활성화한 경우 개인 키 가져오기가 필요합니다**.** ***Panorama*** 관리 서버에서 관리 방화벽으로 구성 변경 사항을 푸시합니다**.**

**STEP 8 |** 개인 키를 암호화하는 데 사용되는 암호를 입력하고 다시 입력(확인)합니다.

**STEP 9 |** 확인을 클릭합니다. 디바이스 인증서 페이지에는 불러온 인증서가 표시됩니다.

## 외부 CA로부터 인증서 받기

외부 인증 기관(CA)에서 인증서를 얻을 때의 이점은 개인 키가 방화벽을 벗어나지 않는다는 것입니다. 외부 CA에서 인증서를 얻으려면 인증서 서명 요청(CSR)을 생성하여 CA에 제출하십시오. CA가 지정된 특성을 가진 인증서를 발급한 후 방화벽으로 가져옵니다. CA는 잘 알려진 공용 CA 또는 엔터프라이즈 CA일 수 있습니다.

OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 해지 상태를 확인하려면 CSR을 생성하기 전에 OCSP 응답자를 구성하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 외부 CA에서 인증서를 요청합니다.

1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.
2. 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.
3. 생성을 클릭합니다.
4. 인증서 이름을 입력합니다. 이 이름은 대소문자를 구별하며 방화벽에 최대 63자 또는 Panorama에서 최대 31자까지 가질 수 있습니다. 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 사용해야 합니다.
5. 공통 이름 필드에 이 인증서를 사용하는 서비스를 구성하는 인터페이스의 FQDN(권장) 또는 IP 주소를 입력합니다.
6. 방화벽에 둘 이상의 vsys가 있고 모든 vsys에서 인증서를 사용할 수 있게 하려면 공유 확인란을 선택합니다.
7. 서명자 필드에서 외부 기관**(CSR)**을 선택합니다.
8. 해당하는 경우**OCSP** 응답자를 선택합니다.
9. (선택 사항) 인증서 특성을 추가하여 인증서를 사용할 방화벽 및 서비스를 고유하게 식별합니다.

   호스트 이름 속성을 추가하는 경우 일반 이름과 일치해야 합니다***(GlobalProtect***의 경우 필수**).** 호스트 이름은 인증서의 주체 대체 이름 필드를 채웁니다**.**
10. 생성을 클릭합니다. 디바이스 인증서 탭에 상태가 **보류 중**인 CSR이 표시됩니다.

**STEP 2 |** CA에 CSR을 제출합니다.

1. CSR을 선택한 다음 내보내기를 클릭하여 .csr 파일을 로컬 컴퓨터에 저장합니다.
2. .csr 파일을 CA에 업로드합니다.

**STEP 3 |** 인증서를 가져옵니다.

1. CA가 CSR에 대한 응답으로 서명된 인증서를 보낸 후 디바이스 인증서 탭으로 돌아가 가져오기를 클릭합니다.
2. CSR 생성에 사용된 인증서 이름을 입력합니다.
3. CA에서 보낸 PEM 인증서 파일의 경로와 이름을 입력하거나 찾아봅니다.
4. 확인을 클릭합니다. 디바이스 인증서 탭에 상태가 **유효한** 인증서가 표시됩니다.

**STEP 4 |** 인증서를 구성합니다.

1. 인증서 이름을 클릭합니다.
2. 방화벽에서 사용하려는 인증서에 해당하는 체크박스를 선택합니다. 예를 들어, 방화벽이 이 인증서를 사용하여 syslog를 외부 syslog 서버로 안전하게 포워딩하는 경우 보안 **Syslog**용 인증서 체크박스를 선택합니다.
3. 확인 및 커밋을 클릭합니다.

## 디바이스 인증서 설치

차세대 방화벽은 디바이스 텔레메트리 및 IoT와 같은 클라우드 서비스를 활용할 수 있습니다. 이렇게 하려면 디바이스 인증서를 설치하여 Palo Alto Networks CSP(고객 지원 포털) 에서 방화벽을 성공적으로 인

 ©2023 Palo Alto Networks, Inc.

증하여 이러한 클라우드 서비스를 활용해야 합니다. 디바이스 인증서가 필요한 상황은 기능마다 다르므로 기능의 설정 설명서에서 이 작업을 수행해야 한다고 명시한 경우에만 디바이스 인증서를 설치하십시오.

디바이스 인증서는 한 번만 설치하면 됩니다. 디바이스 인증서를 사용하는 모든 기능은 방화벽에 설치된 인증서를 사용합니다(이미 존재하는 경우).

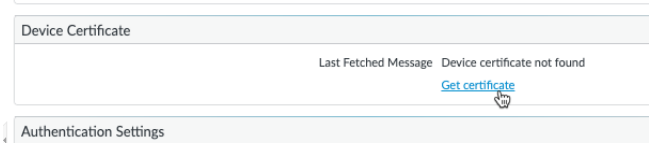
Panorama가 관리하는 방화벽에 디바이스 인증서를 설치할 수 있습니다. 디바이스 인증서를 단일 차세대 방화벽에 직접 설치하려는 경우(즉, Panorama를 사용하지 않는 경우)

**STEP 1 |** 일회용 암호(OTP)를 생성합니다.

1. 고객 지원 포털에 로그인합니다.
2. 자산 > 디바이스 인증서 및 **OTP** 생성을 선택합니다.
3. 디바이스 유형에서 차세대 방화벽용 **OTP** 생성을 선택합니다.
4. **PAN OS** 디바이스 일련 번호를 선택합니다.
5. **OTP**를 생성하고 OTP를 복사합니다.

**STEP 2 |** 차세대 방화벽에 관리자 사용자로 로그인합니다.

**STEP 3 |** 디바이스 > 설정 > 관리 > 디바이스 인증서 및 인증서 가져오기를 선택합니다.




**STEP 4 |** 생성한 일회용 암호를 붙여넣고 확인을 클릭합니다.

**STEP 5 |** 차세대 방화벽이 인증서를 성공적으로 검색하고 설치합니다.

## SCEP를 사용하여 인증서 배포

엔터프라이즈 PKI에 간단한 인증서 등록 프로토콜(SCEP) 서버가 있는 경우 SCEP 프로파일을 구성하여 고유한 클라이언트 인증서의 생성 및 배포를 자동화할 수 있습니다. SCEP 작업은 SCEP 클라이언트가 인증서를 요청하고 SCEP 클라이언트에 인증서를 보낼 때 엔터프라이즈 PKI가 사용자 별 인증서를 생성한다는 점에서 동적입니다. 그런 다음 SCEP 클라이언트는 클라이언트 디바이스에 인증서를 투명하게 배포합니다.

GlobalProtect를 사용하여 SCEP 프로파일을 사용하여 각 GlobalProtect 사용자에게 사용자 별 클라이언트 인증서를 할당할 수 있습니다. 이 사용의 경우 GlobalProtect 포털은 엔터프라이즈 PKI의 SCEP 서버에 대한 SCEP 클라이언트 역할을 합니다. 또한 SCEP 프로파일을 사용하여 Palo Alto Networks 디바이스에 클라이언트 인증서를 할당하여 관리 액세스 및 디바이스 간 통신을 위해 다른 Palo Alto Networks 디바이스와 상호 인증을 받을 수 있습니다.

**STEP 1 |** SCEP 프로파일을 생성합니다.

1. 디바이스 > 인증서 관리 > **SCEP**를 선택한 다음 새 프로파일을 추가합니다.
2. 이름을 입력하여 SCEP 프로파일을 식별합니다.
3. 이 프로파일이 여러 가상 시스템 기능을 갖춘 방화벽용인 경우 가상 시스템 또는 공유를 프로파일을 사용할 수 있는 위치로 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** (선택 사항) SCEP 기반 인증서 생성을 보다 안전하게 만들려면 각 인증서 요청에 대해 PKI와 포털 간에 SCEP 챌린지-응답 메커니즘을 구성합니다.

이 메커니즘을 구성한 후에는 해당 작업이 보이지 않으며 사용자의 추가 입력이 필요하지 않습니다.

미국 표준 준수 연방 정보 처리 표준(FIPS)은 동적 SCEP 챌린지를 사용하고 HTTPS를 사용하는 서버 **URL**을 지정합니다.

다음 옵션 중 하나를 선택합니다.

- 없음—(기본값) SCEP 서버는 인증서를 발급하기 전에 포털에 이의를 제기하지 않습니다.
- 고정—PKI 인프라의 SCEP 서버에서 등록 챌린지 암호를 얻은 다음 암호 필드에 암호를 입력합니다.
- 동적—선택한 사용자 이름과 암호(PKI 관리자의 자격 증명)와 포털 클라이언트가 이러한 자격 증명을 제출하는 SCEP **Server URL**을 입력합니다. 자격 증명을 사용하여 각 인증서 요청에 따라 포털에 대한 OTP 암호를 투명하게 생성하는 SCEP 서버로 인증합니다. (각 인증서 요청 후 **등록 질문 암호는** 필드에서 화면 새로고침을 한 후 이 OTP 변경 사항을 볼 수 있습니다.) PKI는 각 새 암호를 포털에 철저하게 전달한 다음 인증서 요청에 암호를 사용합니다.

**STEP 3 |** 포털이 클라이언트 인증서를 요청하고 받을 수 있도록 SCEP 서버와 포털 간의 연결 설정을 지정합니다.

인증서의 제목 이름에 토큰을 지정하여 클라이언트 디바이스 또는 사용자에 대한 추가 정보를 포함할 수 있습니다.

포털에는 SCEP 서버에 대한 CSR 요청의 토큰 값 및 호스트 ID가 포함됩니다.

1. 포털이 PKI의 SCEP 서버에 연결하는 데 사용하는 서버 **URL**을 구성합니다(예: `http://10.200.101.1/certsrv/mscep/`).
2. **CA-IDENT** 이름 필드에 문자열(최대 255자)을 입력하여 SCEP 서버를 식별합니다.
3. SCEP 서버에서 생성된 인증서에 사용할 제목 이름을 입력합니다. 제목에는 **<속성>=<값>** 형식의 고유 이름이어야 하며 공통 이름(**CN=<변수>**)을 포함해야 합니다. CN은 다음과 같은 동적 토큰을 지원합니다.
   - `$USERNAME`—포털이 특정 사용자에 대한 인증서를 요청할 수 있도록 하려면 이 토큰을 사용합니다. GlobalProtect에서 이 변수를 사용하려면 그룹 매핑을 사용하도록 설정해야 합니다. 사용자가 입력한 사용자 이름은 사용자 그룹 매핑 테이블의 이름과 일치해야 합니다.
   - `$EMAILADDRESS`—이 토큰을 사용하여 특정 이메일 주소와 연결된 인증서를 요청합니다. 이 변수를 사용하려면 그룹 매핑을 활성화하고 서버 프로파일의 메일 도메인 섹션에서 메일 속성을 구성해야 합니다. GlobalProtect가 사용자의 이메일 주소를 식별할 수 없는 경우 고유한 ID를 생성하고 CN을 해당 값으로 채웁니다.
   - `$HOSTID`-디바이스에 대한 인증서만 요청하려면 호스트 ID 토큰을 지정합니다. 사용자가 포털에 로그인을 시도하면 엔드포인트은 호스트 ID 값을 포함하는 식별 정보를 보냅니다. 호스트 ID 값은 디바이스 유형, GUID(Windows) MAC 인터페이스(Mac), Android ID(Android 디바이스), UDID(iOS 디바이스) 또는 GlobalProtect(Chrome)가 할당하는 고유 이름에 따라 다릅니다.

 ©2023 Palo Alto Networks, Inc.

- **$UDID**—UDID 공통 이름 속성을 사용하여 Palo Alto Networks 디바이스 간의 상호 인증을 위해 고객의 디바이스 UDID를 기반으로 인증서를 요청합니다.

GlobalProtect 포털이 SCEP 설정을 에이전트로 푸시하면 제목 이름의 CN 부분이 인증서 소유자의 실제 값(예: **O=acme, CN=johndoe**)으로 대체됩니다.

4. 제목 대체 이름 유형을 선택합니다.

제목 대체 이름 유형에 고정 항목을 사용합니다. 방화벽은 ***$USERNAME***와 같은 동적 토큰을 지원하지 않습니다.

- **RFC 822**이름—인증서의 제목 또는 제목 대체 이름 확장에 이메일 이름을 입력합니다.
- **DNS** 이름—인증서를 평가하는 데 사용되는 DNS 이름을 입력합니다.
- 균일한 리소스 식별자—클라이언트가 인증서를 가져오는 리소스의 이름을 입력합니다.
- 없음—인증서에 대한 속성을 지정하지 마십시오.

**STEP 4 |** (선택 사항) 인증서에 대한 암호화 설정을 구성합니다.

- 인증서의 키 길이(비트수)를 선택합니다.

  방화벽이 FIPS-CC 모드이고 키 생성 알고리즘이 RSA인 경우. RSA 키는 2,048비트 이상이어야 합니다.
- 인증서 서명 요청(CSR) : sha1, sha256 또는 sha384에 대한 다이제스트 알고리즘을 나타내는 **CSR**에 대한 다이제스트를 선택합니다.

**STEP 5 |** (선택 사항) 서명 또는 암호화에 대해 인증서의 허용된 사용을 구성합니다.

- 이 인증서를 서명에 사용하려면 디지털 서명 체크박스로 사용하십시오. 이렇게 하면 엔드포인트이 인증서의 개인 키를 사용하여 디지털 서명의 유효성을 검사할 수 있습니다.
- 이 인증서를 암호화에 사용하려면 키 암호화 체크박스 사용을 선택합니다. 이렇게 하면 클라이언트가 인증서의 개인 키를 사용하여 SCEP 서버에서 발급한 인증서와 함께 설정된 HTTPS 연결을 통해 교환된 데이터를 암호화할 수 있습니다.

**STEP 6 |** (선택 사항) 포털이 올바른 SCEP 서버에 연결되어 있는지 확인하려면 **CA** 인증서 지문을 입력합니다. 지문 필드의 SCEP 서버 인터페이스에서 이 지문을 가져옵니다.

1. SCEP 서버의 관리 UI에 대한 URL을 입력합니다(예 **: http://<hostname or IP>/CertSrv/mscep_admin/**).
2. 지문을 복사하여 **CA** 인증서 지문 필드에 입력합니다.

**STEP 7 |** SCEP 서버와 방화벽 간에 상호 SSL 인증을 사용하도록 설정합니다. 미국 규정을 준수해야 합니다. 연방 정보 처리 표준(FIPS).

*FIPS-CC* 작업은 방화벽 로그인 페이지와 상태 표시줄에 표시됩니다.

SCEP 서버의 루트 **CA** 인증서를 선택합니다. 선택적으로 클라이언트 인증서를 선택하여 SCEP 서버와 방화벽 간에 상호 SSL 인증을 사용하도록 설정할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 구성을 저장하고 커밋합니다.

1. 설정을 저장하고 SCEP 구성을 닫도록 확인을 클릭합니다.
2. 구성을 커밋합니다.

포털은 SCEP 프로파일의 설정을 사용하여 CA 인증서를 요청하려고 시도하고 포털을 호스팅하는 방화벽에 저장합니다. 성공하면 CA 인증서가 디바이스 > 인증서 관리 > 인증서에 표시됩니다.

**STEP 9 |** (선택 사항) SCEP 프로파일을 저장한 후 포털에서 인증서를 얻지 못하면 포털에서 수동형으로 인증서 서명 요청(CSR)을 생성할 수 있습니다.

1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 생성을 클릭합니다.
2. 인증서 이름을 입력합니다. 이 이름은 공백을 포함할 수 없습니다.
3. 회사 PKI에 CSR을 제출하는 데 사용할 **SCEP** 프로파일을 선택합니다.
4. 확인을 클릭하여 요청을 제출하고 인증서를 생성합니다.


©2023 Palo Alto Networks, Inc.

# 인증서 및 개인 키 내보내기

Palo Alto Networks는 엔터프라이즈 PKI(공개 키 인프라)를 사용하여 조직에서 인증서와 개인 키를 배포하는 것이 좋습니다. 그러나 필요한 경우 방화벽이나 Panorama에서 인증서와 개인 키를 내보낼 수도 있습니다. 다음과 같은 경우 내보낸 인증서와 개인 키를 사용할 수 있습니다.

- 웹 인터페이스에 대한 인증서 기반 관리자 인증 구성
- 포털 및 게이트웨이에 대한 GlobalProtect 에이전트/앱 인증을 구성하려면 GlobalProtect LSVPN 구성 요소 간 SSL 활성화
- SSL 포워드 프록시 복호화
- 외부 CA로부터 인증서 받기

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

**STEP 2 |** 방화벽에 둘 이상의 가상 시스템(vsys)이 있는 경우 인증서에 대해 위치(특정 vsys 또는 공유)를 선택합니다.

**STEP 3 |** 인증서를 선택하고 내보내기를 클릭한 다음 파일 형식을 선택합니다.

- **Base64**로 인코딩된 인증서**(PEM)** - 기본 형식입니다. 가장 일반적이며 인터넷에서 가장 광범위한 지원을 제공합니다. 내보낸 파일에 개인 키가 포함되도록 하려면 개인 키 내보내기 체크박스를 선택합니다.
- 암호화된 개인 키 및 인증서**(PKCS12)** - 이 형식은 PEM보다 안전하지만 일반적이지 않거나 광범위하게 지원되지는 않습니다. 내보낸 파일에는 자동으로 개인 키가 포함됩니다.
- 이진 인코딩 인증서**(DER)** - 더 많은 운영 체제 유형이 다른 형식보다 이 형식을 지원합니다. 키가 아닌 인증서만 내보낼 수 있습니다. 개인 키 내보내기 체크박스와 암호 필드는 무시합니다.

**STEP 4 |** 파일 형식이 PKCS12 또는 PEM이고 개인 키 내보내기 체크박스를 선택한 경우 개인 키를 암호화하려면 암호 및 암호 확인을 입력합니다. 인증서와 키를 클라이언트 시스템으로 가져올 때 이 암호를 사용합니다.



**(*Panorama* 관리 방화벽)** 인증서를 생성 또는 가져오기할 때 개인 키 내보내기 차단을 활성화한 경우 개인 키를 가져오고 내보낸 인증서를 가져올 때 키 파일을 추가합니다**.** 이는 인증서를 가져온 관리되는 방화벽으로 ***Panorama***에서 구성 변경 내용을 성공적으로 푸시하는 데 필요합니다**.**

**STEP 5 |** 확인을 클릭하고 인증서/키 파일을 컴퓨터에 저장합니다.


©2023 Palo Alto Networks, Inc.

# 인증서 프로파일 구성

인증서 프로파일은 인증 포털, 디바이스 인증, 다단계 인증(MFA), GlobalProtect, site-to-site IPSec VPN, EDL(외부 동적 목록) 유효성 검사, DDNS(동적 DNS), User-ID 에이전트 및 TS 에이전트 액세스, Palo Alto Networks 방화벽에 대한 웹 인터페이스 액세스 또는 Panorama에 대한 사용자 및 디바이스 인증을 정의합니다. 프로파일은 사용할 인증서, 인증서 해지 상태를 확인하는 방법 및 해당 상태가 액세스를 제한하는 방법을 지정합니다. 각 애플리케이션에 대한 인증서 프로파일을 구성합니다.



인증서 프로파일에 대해 ***OCSP(***온라인 인증서 상태 프로토콜***)*** 및 ***CRL(***인증서 해지 목록***)*** 상태 확인을 활성화하여 인증서가 해지되지 않았는지 확인하는 것이 가장 좋습니다**.** ***OCSP*** 서버를 사용할 수 없는 경우 방화벽이 ***CRL***을 사용하도록 ***OCSP*** 및 ***CRL***을 모두 사용하도록 설정합니다**.** 이러한 방법에 대한 자세한 내용은 인증서 해지를 참조하십시오**.**

**STEP 1 |** 할당할 CA(인증 기관) 인증서를 가져옵니다.

다음 단계 중 하나를 수행하여 프로파일에 할당할 CA 인증서를 가져옵니다. 하나 이상을 할당해야 합니다.

- 인증서를 생성합니다.
- 엔터프라이즈 CA에서 인증서를 내보낸 다음 방화벽으로 가져옵니다(3 단계 참조).

**STEP 2 |** 인증서 프로파일을 식별합니다.

1. 디바이스 > 인증서 관리 > 인증서 프로파일을 선택한 다음 추가를 클릭합니다.
2. 프로파일을 식별하려면 이름을 입력합니다. 이름은 대/소문자를 구분하며 고유해야 하며 방화벽에서 최대 63자를 사용할 수 있으며 Panorama에서는 문자, 숫자, 공백, 하이픈 및 밑줄만 포함하는 최대 31자를 사용할 수 있습니다.
3. 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.

**STEP 3 |** 하나 이상의 인증서를 할당합니다.

각 CA 인증서에 대해 다음 단계를 수행합니다.

1. CA 인증서 표에서 추가를 클릭합니다.
2. **CA** 인증서를 선택합니다. 또는 인증서를 가져오려면 가져오기를 클릭하고 인증서 이름을 입력한 다음 엔터프라이즈 CA에서 내보낸 인증서 파일에 찾아보기를 입력하고 확인을 클릭합니다.
3. (선택 사항) 방화벽이 OCSP를 사용하여 인증서 해지 상태를 확인하는 경우 기본 동작을 재정의하도록 다음 필드를 구성합니다. 대부분의 배포에서는 이러한 필드가 적용되지 않습니다.
   - 기본적으로 방화벽은 인증서의 AIA(기관 정보 액세스) 정보를 사용하여 OCSP 응답자 정보를 추출합니다. AIA 정보를 재정의하려면 기본 **OCSP URL**(**`http://`**또는 **`https://`**로 시작)을 입력합니다.
   - 기본적으로 방화벽은 **CA** 인증서 필드에서 선택한 인증서를 사용하여 OCSP 응답의 유효성을 검사합니다. 유효성 검사에 다른 인증서를 사용하려면 **OCSP CA** 인증서 확인 필드에서 선택합니다.
4. 확인을 클릭합니다. CA 인증서 테이블에는 할당된 인증서가 표시됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 인증서 해지 상태 및 연결된 차단 동작을 확인하는 방법을 정의합니다.

1. **CRL** 사용 및/또는 **OCSP** 사용을 선택합니다. 둘 다 선택하면 방화벽이 먼저 OCSP를 시도하고 OCSP 응답자를 사용할 수 없는 경우에만 CRL 방법으로 폴백합니다.
2. 확인 방법에 따라 **CRL** 수신 타임아웃 및/또는 **OCSP** 수신 타임아웃을 입력합니다. 이 간격은 방화벽이 CRL/OCSP 서비스의 응답을 기다리는 것을 중지하는 간격(1~60초)입니다.
3. 인증서 상태 타임아웃을 입력합니다. 방화벽이 인증서 상태 서비스의 응답 대기를 중지하고 사용자가 정의한 세션 차단 논리를 적용하는 간격(1~60초)입니다. 인증서 상태 타임아웃은 다음과 같이 OCSP/CRL 수신 타임아웃과 관련됩니다.
   - OCSP와 CRL 모두를 사용하도록 설정하는 경우 방화벽은 인증서 상태 타임아웃 값 또는 두 개의 수신 타임아웃 값의 집계 중 더 짧은 간격이 경과한 후 요청 타임아웃를 등록합니다.
   - OCSP만 사용하도록 설정한 경우 방화벽은 인증서 상태 타임아웃 값 또는 OCSP 수신 타임아웃 값 중 더 짧은 간격이 경과한 후 요청 타임아웃을 등록합니다.
   - CRL만 사용하도록 설정하는 경우 방화벽은 인증서 상태 타임아웃 값 또는 CRL 수신 시간 초과 값 중 더 짧은 간격이 경과한 후 요청 타임아웃를 등록합니다.
4. OCSP 또는 CRL 서비스가 인증서 해지 상태를 알 수 없음으로 반환할 때 방화벽이 세션을 차단하도록 하려면 인증서 상태를 알 수 없는 경우 세션 차단을 선택합니다. 그렇지 않으면 방화벽이 세션을 허용합니다.
5. OCSP 또는 CRL 요청 타임아웃를 등록한 후 방화벽이 세션을 차단하도록 하려면 타임아웃 내에 인증서 상태를 검색할 수 없는 경우 세션 차단을 선택합니다. 그렇지 않으면 방화벽이 세션을 허용합니다.
6. (**GlobalProtect**에만 해당) 클라이언트 인증서 주체의 일련번호 속성이 GlobalProtect 앱이 엔드포인트에 대해 보고하는 호스트 ID와 일치하지 않을 때 방화벽에서 세션을 차단하도록 하려면 인증 디바이스에 인증서가 발급되지 않은 경우 세션 차단을 선택합니다.

**STEP 5 |** 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# SSL/TLS 서비스 프로파일 구성

Palo Alto Networks 방화벽 및 Panorama는 SSL/TLS 서비스 프로파일을 사용하여 SSL/TLS 서비스에 대해 인증서 및 허용되는 프로토콜 버전을 지정합니다. 방화벽 및 Panorama는 인증 포털, GlobalProtect 포털 및 게이트웨이, 관리(MGT) 인터페이스의 인바운드 트래픽, URL 관리 재정의 기능 및 User-ID™ syslog 수신 서비스에 SSL/TLS를 사용합니다. 프로토콜 버전을 정의하면 프로파일을 사용하여 서비스를 요청하는 클라이언트와의 통신 보안에 사용할 수 있는 암호 제품군을 제한할 수 있습니다. 이렇게 하면 방화벽이나 Panorama가 알려진 취약점이 있는 SSL/TLS 버전을 피할 수 있도록 하여 네트워크 보안이 향상됩니다. 서비스 요청에 지정된 범위를 벗어난 프로토콜 버전이 포함된 경우 방화벽 또는 Panorama는 지원되는 버전으로 연결을 다운그레이드하거나 업그레이드합니다.

방화벽 서비스를 요청하는 클라이언트 시스템에서 ***CTL***(인증서 신뢰 목록)에는 ***SSL/TLS*** 서비스 프로파일에 지정된 인증서를 발급한 ***CA***(인증 기관) 인증서가 포함되어야 합니다. 그렇지 않으면 방화벽 서비스를 요청할 때 사용자에게 인증서 오류가 표시됩니다. 대부분의 타사 ***CA*** 인증서는 기본적으로 클라이언트 브라우저에 있습니다. 엔터프라이즈 또는 방화벽 생성 ***CA*** 인증서가 발급자인 경우 해당 ***CA*** 인증서를 클라이언트 브라우저의 ***CTL***에 배포해야 합니다.

**STEP 1 |** 원하는 각 서비스에 대해 방화벽에서 인증서를 생성하거나 가져옵니다(인증서 획득 참조).

***SSL/TLS*** 서비스 프로파일에는 ***CA*** 인증서가 아닌 서명된 인증서만 사용하십시오.

**STEP 2 |** 디바이스 > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.

**STEP 3 |** 방화벽에 둘 이상의 가상 시스템(vsys)이 있는 경우 프로파일을 사용할 수 있는 위치(vsys 또는 **Shared**)를 선택합니다.

**STEP 4 |** 추가를 클릭하고 프로파일을 식별할 이름을 입력합니다.

**STEP 5 |** 방금 획득한 인증서를 선택합니다.

**STEP 6 |** 서비스에서 사용할 수 있는 프로토콜 범위를 정의합니다.

- 최소 버전에 대해 가장 먼저 허용되는 TLS 버전을 선택합니다. **TLSv1.0**(기본값), **TLSv1.1** 또는 **TLSv1.2**.
- 최대 버전의 경우 허용된 최신 TLS 버전을 선택합니다. **TLSv1.0**, **TLSv1.1**, **TLSv1.2** 또는 **Max**(사용 가능한 최신 버전). 기본값은 최대입니다.

가장 좋은 방법은 최소 버전을 ***TLSv1.2***로, 최대 버전을 최대로 설정하는 것입니다.

*PAN-OS 8.0* 이상의 버전을 실행하는 ***FIPS/CC*** 모드의 방화벽에서 ***TLSv1.1***은 지원되는 가장 빠른 *TLS* 버전입니다. ***TLSv1.0***을 선택하지 마십시오.

*TLSv1.2*에 의존하는 방화벽 서비스를 요청할 때 사용되는 클라이언트 인증서는 다이제스트 알고리즘으로 *SHA512*를 가질 수 없습니다. 클라이언트 인증서는 더 낮은 다이제스트 알고리즘(예: *SHA384*)을 사용하거나 방화벽 서비스에 대해 최대 버전을 ***TLSv1.1***로 제한해야 합니다.

**STEP 7 |** 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# SSH 서비스 프로파일 구성

SSH 서비스 프로파일을 사용하면 SSH 매개 변수를 사용자 지정하여 Palo Alto Networks 관리 및 HA(고가용성) 어플라이언스에 대한 SSH 연결의 보안 및 무결성을 향상시킬 수 있습니다. 기본적으로 SSH는 모든 암호, 키 교환 알고리즘 및 메시지 인증 코드를 지원하므로 연결이 공격에 취약합니다. SSH 서비스 프로파일을 사용하면 SSH 서버가 지원하는 알고리즘을 제한할 수 있습니다. 새 호스트 키를 생성하고 SSH 세션 키 재생 및 교환을 위한 데이터 볼륨, 시간 및 패킷 기반 임계값을 지정할 수도 있습니다.

SSH 서버 인스턴스에 따라 관리 또는 HA SSH 서비스 프로파일을 구성합니다. 방화벽 또는 Panorama™ 웹 인터페이스(여러 방화벽 또는 어플라이언스에서 설정을 적용하는 경우) 또는 CLI에서 프로파일을 구성할 수 있습니다.

최대 *4*개의 관리 및 *4*개의 *HA* 서버 프로파일을 구성할 수 있습니다.

컬렉터 그룹의 각 전용 로그 컬렉터*(*로그 컬렉터 모드의 *M* 시리즈 또는 *Panorama* 가상 어플라이언스*)*에 대해 동일한 *SSH* 연결 설정을 사용하려면 *Panorama* 관리 서버에서 *SSH* 서비스 프로파일을 구성하고, 변경 내용을 *Panorama*로 커밋한 다음 로그 컬렉터로 구성을 푸시합니다. ***set log-collector-group <name> general-setting management ssh*** 명령을 사용하여 *CLI*에서 이러한 단계를 수행할 수도 있습니다.

- SSH 관리 프로파일 생성
- SSH HA 프로파일 생성

## SSH 관리 프로파일 생성

관리 연결에 대한 SSH 설정을 사용자 지정하려면 SSH 관리 프로파일을 만들어야 합니다.

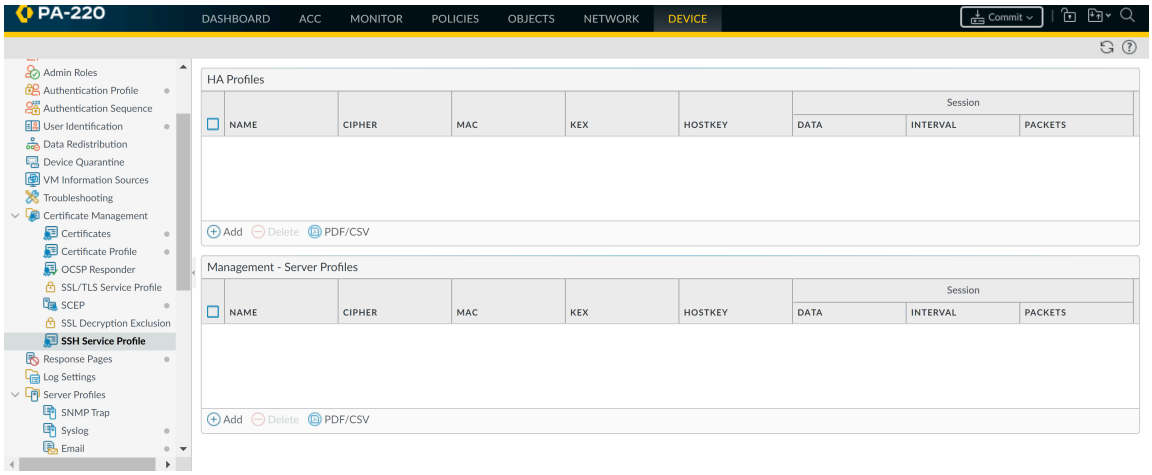
*CLI*에서 기존 관리 프로파일을 구성하거나 업데이트할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 관리 생성 - 서버 프로파일.

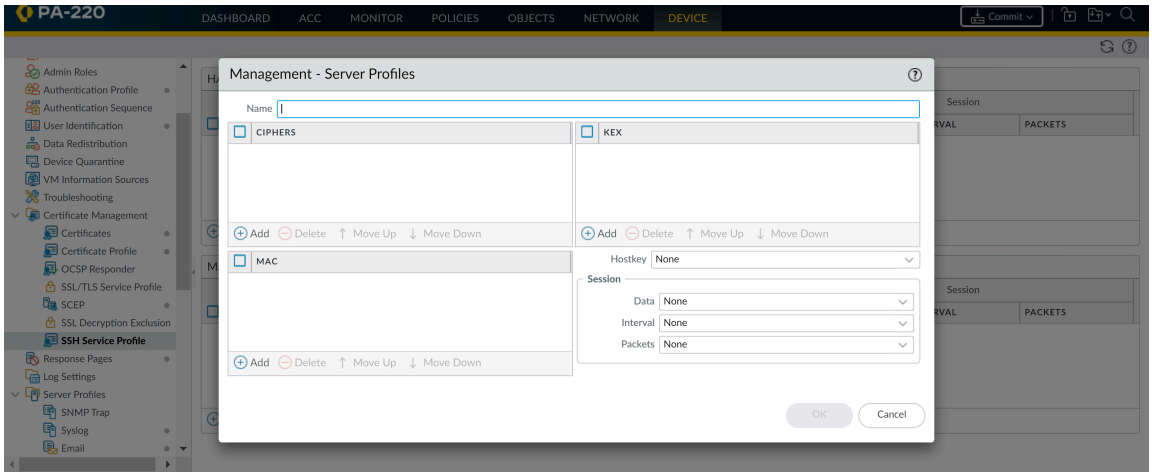
1. 디바이스 > 인증 관리 > **SSH** 서비스 프로파일을 선택합니다.
2. 관리 추가 - 서버 프로파일입니다.


©2023 Palo Alto Networks, Inc.





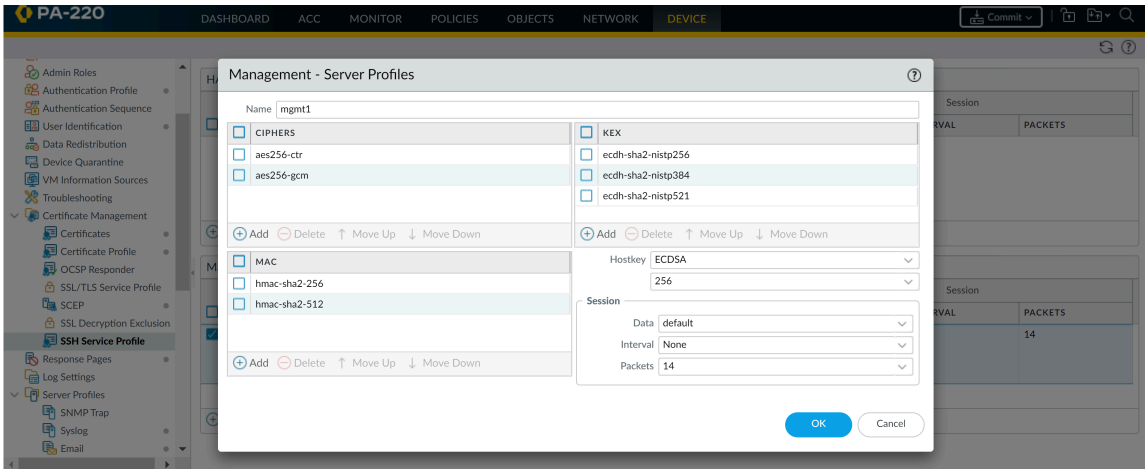
©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

3. 프로파일을 식별하려면 이름을 입력합니다.
4. (선택 사항) 프로파일이 지원하는 암호, 메시지 인증 코드 또는 키 교환 알고리즘을 추가합니다.
5. (선택 사항) 호스트키와 키 길이를 선택합니다.
6. (선택 사항) SSH 세션 키 재설정 매개변수에 대한 값 입력: 데이터, 간격 및 패킷.


©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

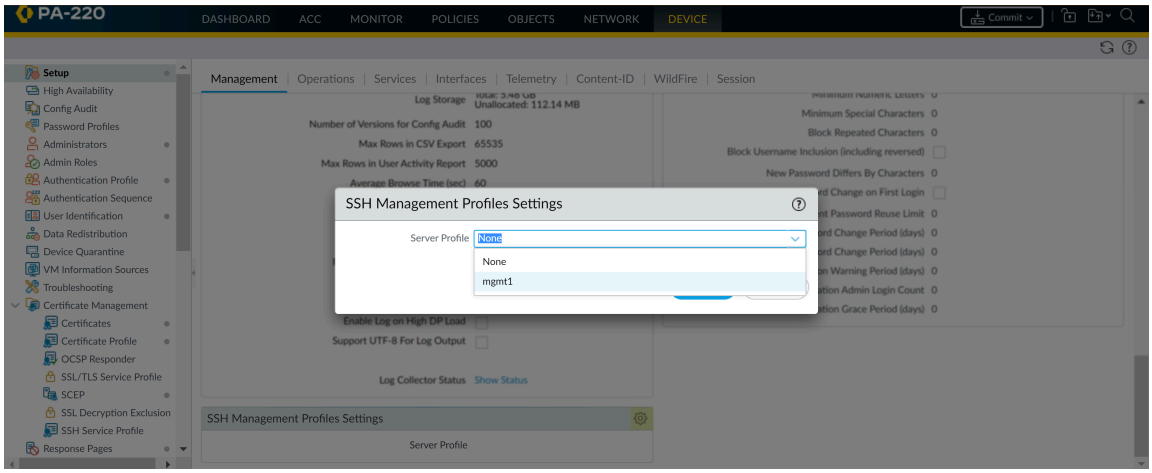
7. 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 적용할 관리 프로파일을 선택합니다.

1. 디바이스 > 설정 > 관리를 선택합니다. SSH 관리 프로파일 설정에서 기존 프로파일을 선택합니다.

 ©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

2. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 3 |** CLI에서 관리 SSH 서비스를 다시 시작하여 프로파일을 적용합니다.

새 프로파일을 적용할 때마다 연결을 다시 시작하거나 사용 중 의 프로파일을 변경해야 합니다. 이렇게 하면 어플라이언스가 재부팅됩니다. 새 구성은 활성 세션에 영향을 주지 않습니다. 프로파일은 후속 연결(또는 세션)에 적용됩니다.

1. admin@PA-3260> **set ssh service-restart mgmt**

## SSH HA 프로파일 생성

HA 쌍에서 어플라이언스 간의 SSH 통신을 보호하려면 SSH HA 프로파일을 만들어야 합니다. 프로파일을 생성 전에 어플라이언스 간에 HA 연결을 설정해야 합니다. HA 연결이 설정되지 않은 경우 제어 링크 연결에서 암호화를 사용하도록 설정하고 HA 키를 네트워크 위치로 내보내고 피어에서 HA 키를 가져와야 합니다. (능동형/수동형 HA 구성 또는 능동형/능동형 HA 구성을 참조하십시오.)

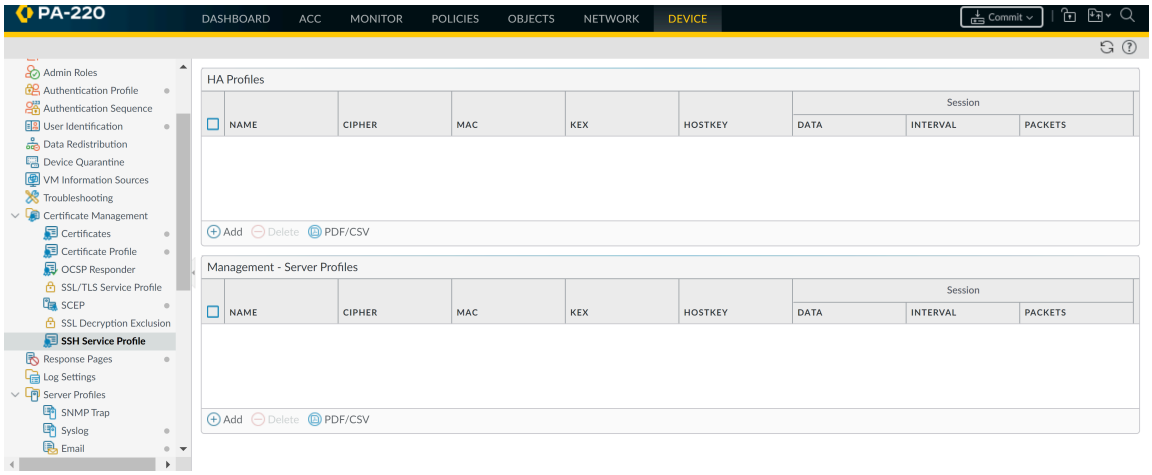
***CLI***에서 기존 HA 프로파일을 구성하거나 업데이트할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

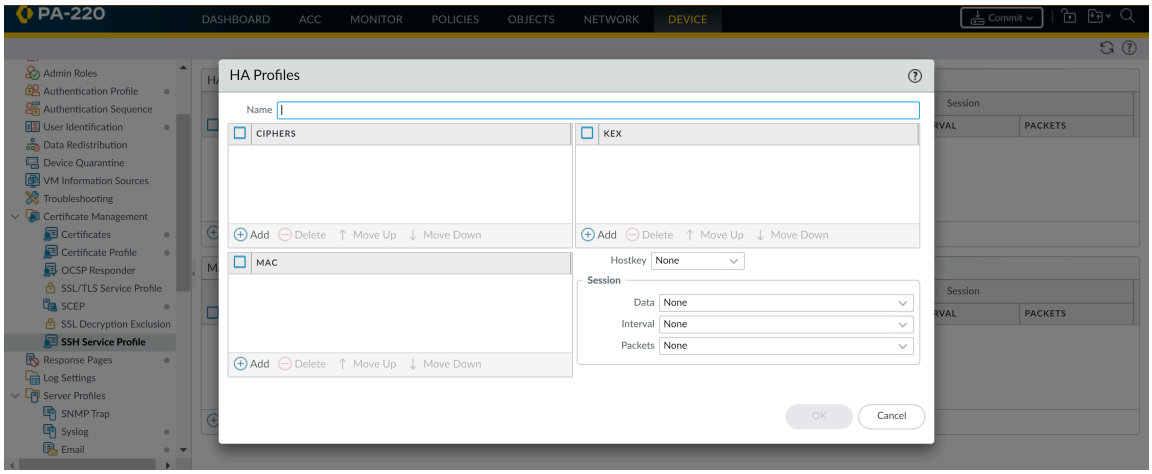
**STEP 1 |** HA 프로파일을 생성합니다.

1. 디바이스 > 인증 관리 > **SSH** 서비스 프로파일을 선택합니다.
2. HA 프로파일을 추가합니다.

 ©2023 Palo Alto Networks, Inc.



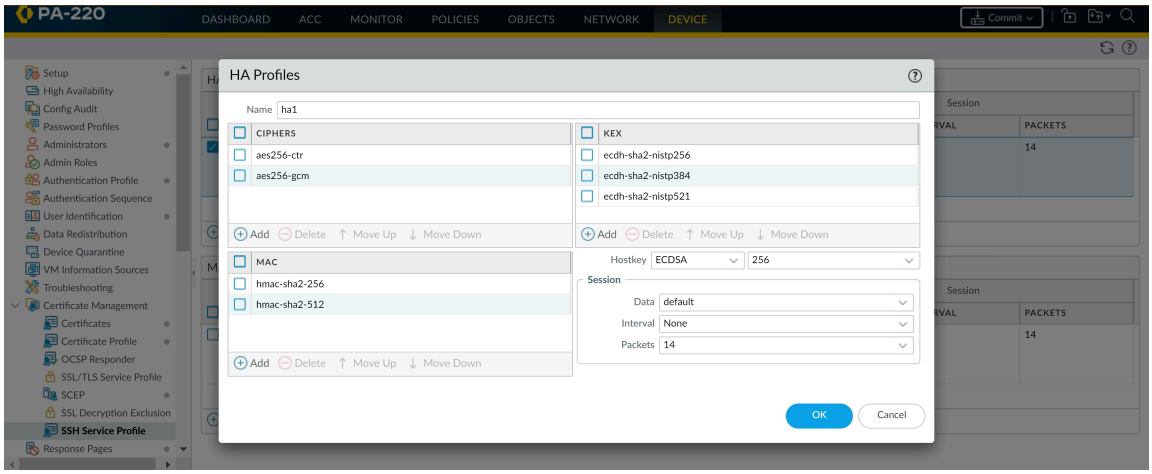

 ©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

3. 프로파일을 식별하려면 이름을 입력합니다.
4. (선택 사항) 프로파일이 지원하는 암호, 메시지 인증 코드 또는 키 교환 알고리즘을 추가합니다.
5. (선택 사항) 호스트키와 키 길이를 선택합니다.
6. (선택 사항) SSH 세션 키 재설정 매개변수에 대한 값 입력: 데이터, 간격 및 패킷.


©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

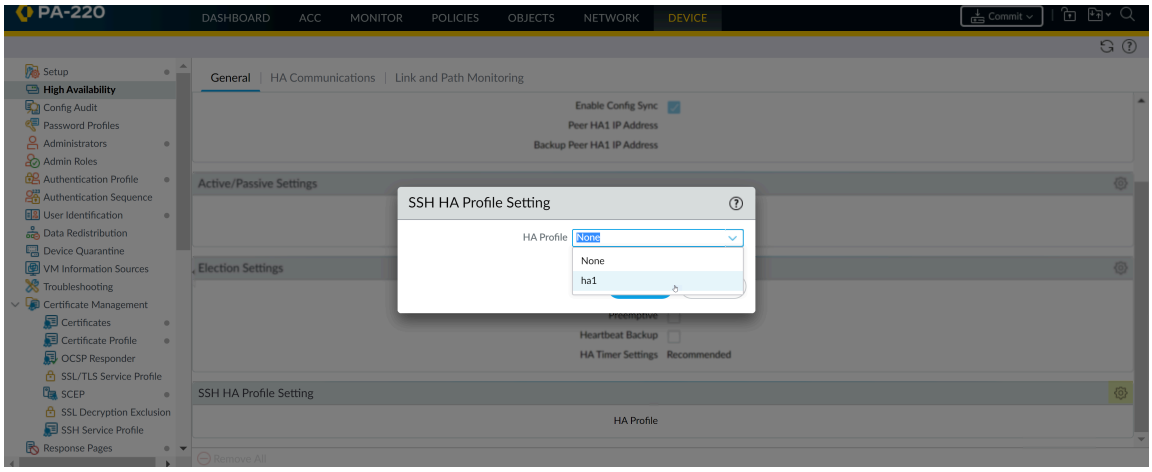
7. 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 적용할 HA 프로파일을 선택합니다.

1. 디바이스 > 고가용성 > 일반을 선택합니다. SSH HA 프로파일 설정에서 기존 프로파일을 선택합니다.

 ©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

2. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 3 |** CLI에서 HA1 SSH 서비스를 다시 시작하여 프로파일을 적용합니다.

새 프로파일을 적용할 때마다 연결을 다시 시작하거나 사용 중 의 프로파일을 변경해야 합니다. 이렇게 하면 어플라이언스가 재부팅됩니다. 새 구성은 활성 세션에 영향을 주지 않습니다. 프로파일은 후속 연결(또는 세션)에 적용됩니다.

1. admin@PA-3260> **set ssh service-restart ha**

   *HA* 쌍 간의 연결이 설정되고 *SSH* 서비스 다시 시작과 함께 가동 중지 시간을 최소화하려는 경우 다음 명령을 사용할 수 있습니다. *HA* 연결이 설정되지 않은 경우 *SSH* 서비스를 다시 시작해야 합니다.

   - *(HA1* 백업이 구성됨*) admin@PA-3260>* 고가용성 세션 재설정 요청
   - *(HA1* 백업이 구성되지 않았거나 *HA1* 백업 링크가 다운됨*)admin@PA-3260>* 고가용성 세션 재설정 강제 요청

     *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있습니다. 이로 인해 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. *(HA1* 백업이 구성될 때 강제 적용 옵션을 사용하면 아무런 효과가 없습니다.*)*


©2023 Palo Alto Networks, Inc.

# 인바운드 관리 트래픽에 대한 인증서 교체

방화벽 또는 Panorama를 처음 부팅하면 관리(MGT) 인터페이스 및 HTTPS 관리 트래픽을 지원하는 다른 인터페이스(방화벽만 해당)를 통해 웹 인터페이스 및 XML API에 대한 HTTPS 액세스를 활성화하는 기본 인증서가 자동으로 생성됩니다. (자세한 내용은 인터페이스 관리 프로파일을 사용하여 액세스 제한 참조). 인바운드 관리 트래픽의 보안을 향상시키려면 기본 인증서를 조직을 위해 특별히 발급된 새 인증서로 바꾸십시오.

기본 인증서를 보거나 수정하거나 삭제할 수 없습니다.

관리 트래픽을 보호하려면 관리 계정 및 인증 구성도 해야 합니다.

**STEP 1 |** 관리자의 클라이언트 시스템에 방화벽 또는 Panorama를 인증하는 인증서를 가져옵니다.

클라이언트 시스템이 이미 신뢰하는 인증서를 사용하여 인증서 배포를 단순화할 수 있습니다. 따라서 엔터프라이즈 인증 기관(CA)에서 인증서 및 개인 키 가져오기 또는 외부 CA에서 인증서 가져오기를 권장합니다. 클라이언트 시스템의 신뢰할 수 있는 루트 인증서 저장소에는 이미 신뢰를 보장하는 연결된 루트 CA 인증서가 있을 수 있습니다.

방화벽이나 ***Panorama***에서 인증서를 생성하면 루트 ***CA*** 인증서가 클라이언트 시스템의 신뢰할 수 있는 루트 인증서 저장소에 없기 때문에 관리자에게 인증서 오류가 표시됩니다. 이를 방지하기 위해 자체 서명된 루트 ***CA*** 인증서를 모든 클라이언트 시스템에 배포합니다.

인증서를 얻는 방법에 관계없이 향상된 보안을 위해 ***sha256*** 이상의 다이제스트 알고리즘을 권장합니다.

**STEP 2 |** SSL/TLS 서비스 프로파일을 구성합니다.

방금 획득한 인증서를 선택합니다.

보안을 강화하려면 인바운드 관리 트래픽에 대해 ***Min Version***(가장 빠른 허용 ***TLS*** 버전)을 ***TLSv1.2***로 설정하는 것이 좋습니다. 또한 모든 서비스에 대해 이 프로파일을 다시 사용하는 대신 각 방화벽 또는 ***Panorama*** 서비스에 대해 다른 ***SSL/TLS*** 서비스 프로파일을 사용하는 것이 좋습니다.

**STEP 3 |** 인바운드 관리 트래픽에 SSL/TLS 서비스 프로파일을 적용합니다.

1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 수정합니다.
2. 방금 구성된 **SSL/TLS** 서비스 프로파일을 선택합니다.
3. 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# SSL 포워딩 프록시 서버 인증서의 키 크기 구성

SSL 포워딩 프록시 세션에서 클라이언트에 응답할 때 방화벽은 대상 서버가 제공하는 인증서 사본을 생성하고 이 사본을 사용하여 클라이언트와의 연결을 설정합니다. 기본적으로 방화벽은 대상 서버가 제공한 인증서와 동일한 키 크기의 인증서를 생성합니다. 그러나 다음과 같이 방화벽 생성 인증서의 키 크기를 변경할 수 있습니다.

**STEP 1 |** 디바이스 > 설정 > 세션을 선택하고 암호 해독 설정 섹션에서 **SSL** 전달 프록시 설정을 클릭합니다.

**STEP 2 |** 키 크기 선택:

- 대상 호스트에서 정의 - 방화벽은 대상 서버 인증서를 기반으로 클라이언트와 SSL 프록시 세션을 설정하기 위해 생성하는 인증서의 키 크기와 해싱 알고리즘을 결정합니다. 대상 서버가 1,024비트 RSA 키를 사용하는 경우 방화벽은 1,024비트 RSA 키가 있는 인증서를 생성합니다. 대상 서버가 1,024비트보다 큰 키의 크기(예: 2,048비트 또는 4,096비트)를 사용하는 경우 방화벽은 2,048비트의 RSA 키를 사용하는 인증서를 생성합니다. 대상 서버가 SHA-1 해싱 알고리즘을 사용하는 경우 방화벽은 SHA-1 해싱 알고리즘으로 인증서를 생성합니다. 대상 서버가 SHA-1보다 강력한 해싱 알고리즘을 사용하는 경우 방화벽은 SHA-256 알고리즘을 사용하여 인증서를 생성합니다. 이것이 기본 설정입니다.
- **1024**비트 **RSA** - 방화벽은 대상 서버 인증서의 키 크기에 관계없이 1,024비트 RSA 키 및 SHA-256 해싱 알고리즘을 사용하는 인증서를 생성합니다. 2013년 12월 31일부로 공용 CA(인증 기관) 및 주로 사용되는 브라우저는 2,048비트 미만의 키를 사용하는 X.509 인증서를 제한적으로 지원합니다. 향후 보안 설정에 따라 이러한 키가 제공되면 브라우저에서 사용자에게 경고하거나 SSL/TLS 세션을 완전히 차단할 수 있습니다.
- **2048**비트 **RSA** - 방화벽은 대상 서버 인증서의 키 크기에 관계없이 2,048비트 RSA 키 및 SHA-256 해싱 알고리즘을 사용하는 인증서를 생성합니다. 공용 CA 및 널리 사용되는 브라우저는 1,024비트 키보다 더 나은 보안을 제공하는 2,048비트 키를 지원합니다.

키 크기 설정을 변경하면 현재 인증서 캐시가 지워집니다.

**STEP 3 |** 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 인증서 취소 및 갱신


- 인증서 취소
- 인증서 갱신


## 인증서 취소

다양한 상황에 따라 만료 날짜 이전에 인증서가 무효화될 수 있습니다. 몇 가지 예로는 이름 변경, 주체와 인증 기관 간의 연결 변경(예: 직원 해고), 개인 키 손상(알려졌거나 의심되는)이 있습니다. 이러한 상황에서 인증서를 발급한 인증서 기관(CA)은 인증서를 취소해야 합니다. 다음 작업은 방화벽이 CA인 인증서를 해지하는 방법에 대해 설명합니다.

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

**STEP 2 |** 방화벽이 여러 가상 시스템을 지원하는 경우 탭에 위치 드롭다운이 표시됩니다. 인증서가 속한 가상 시스템을 선택합니다.

**STEP 3 |** 취소할 인증서를 선택합니다.

**STEP 4 |** 취소를 클릭합니다. PAN-OS는 즉시 인증서 상태를 취소하도록 설정하고 온라인 인증서 상태 프로토콜(OCSP) 응답자 캐시 또는 CRL(인증서 해지 목록)에 일련번호를 추가합니다. 커밋을 수행할 필요는 없습니다.

## 인증서 갱신

인증서가 만료되거나 곧 만료되면 유효성 기간을 재설정할 수 있습니다. 외부 인증서 기관(CA)이 인증서에 서명하고 방화벽이 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 해지 상태를 확인하는 경우 방화벽은 OCSP 응답자 정보를 사용하여 인증서 상태를 업데이트합니다(OCSP 응답자 구성 참조). 방화벽이 인증서를 발급한 CA인 경우 방화벽은 일련번호는 다르지만 속성은 이전 인증서와 동일한 새 인증서로 교체합니다.

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

**STEP 2 |** 방화벽에 둘 이상의 가상 시스템(vsys) 이 있는 경우 인증서의 위치(vsys 또는 공유)를 선택합니다.

**STEP 3 |** 갱신할 인증서를 선택하고갱신을 클릭합니다.

**STEP 4 |** 새 만료 인터벌을 입력합니다(일 단위).

**STEP 5 |** 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 하드웨어 보안 모듈을 사용한 보안 키

HSM(하드웨어 보안 모듈)은 디지털 키를 관리하는 물리적 디바이스입니다. HSM은 안전한 저장 및 디지털 키 생성을 제공합니다. 승인되지 않은 사용 및 잠재적인 공격자로부터 이러한 자료를 논리적 및 물리적으로 보호합니다.

Palo Alto Networks 방화벽 및 Panorama와 통합된 HSM 클라이언트는 SSL/TLS 복호화(SSL 순방향 프록시 및 SSL 인바운드 검사 모두)에 사용되는 개인 키에 대한 보안을 강화합니다. 또한 HSM을 사용하여 마스터 키를 암호화할 수 있습니다.

다음 주제에서는 HSM을 방화벽 또는 Panorama와 통합하는 방법에 대해 설명합니다.

- HSM을 통한 연결 설정
- HSM을 사용하여 마스터 키 암호화
- HSM에 개인 키 저장
- HSM 배포 관리

## HSM을 통한 연결 설정

HSM 클라이언트는 PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈 및 VM 시리즈 방화벽과 통합되며 Panorama 관리 서버(가상 및 M 시리즈 어플라이언스 모두)와 통합되어 다음 HSM 공급업체와 함께 사용할 수 있습니다.

- **nCipher nShield Connect** - 지원되는 클라이언트 버전은 PAN-OS 릴리스에 따라 다릅니다.
  - PAN-OS 10.2는 클라이언트 버전 12.40.2를 지원합니다(이전 어플라이언스의 경우 클라이언트 버전 11.50까지 역호환 가능).
  - PAN-OS 9.1, 9.0 및 8.1은 클라이언트 버전 12.30을 지원합니다.
  - PAN-OS 8.0 및 이전 릴리스는 클라이언트 버전 11.62를 지원합니다.
- **SafeNet** 네트워크 - 지원되는 클라이언트 버전은 PAN-OS 릴리스에 따라 다릅니다.
  - PAN-OS 10.2는 클라이언트 버전 5.4.2 및 7.2를 지원합니다.
  - PAN-OS 9.1 및 9.0은 클라이언트 버전 5.4.2 및 6.3을 지원합니다.
  - PAN-OS 8.1은 클라이언트 버전 5.4.2 및 6.2.2를 지원합니다.
  - PAN-OS 8.0.2 이상 PAN-OS 8.0 릴리스(PAN-OS 7.1.10 이상 PAN-OS 7.1 릴리스)는 클라이언트 버전 5.2.1, 5.4.2 및 6.2.2를 지원합니다.

HSM 서버 버전은 이러한 클라이언트 버전과 호환되어야 합니다. 클라이언트-서버 버전 호환성 매트릭스는 HSM 공급자 설명서를 참조하십시오. 방화벽 또는 Panorama에서 다음 절차를 사용하여 SafeNet HSM 서버와 호환되는 SafeNet 네트워크 클라이언트 버전을 선택합니다.

*HSM* 서버를 업그레이드한 후 다운그레이드하는 것은 옵션이 아닐 수 있습니다.

- 세이프넷 네트워크 HSM을 통한 연결 설정
- nCipher nShield 커넥트 HSM으로 연결 설정


©2023 Palo Alto Networks, Inc.

- SafeNet 클라이언트 RPM 패킷 관리자를 설치합니다.
  1. 디바이스 > 설정 > **HSM**을 선택하고 **HSM** 클라이언트 버전 선택(하드웨어 보안 작업 설정)을 선택합니다.
  2. HSM 서버 버전에 맞게 버전 **5.4.2**(기본값) 또는 **7.2**를 선택합니다.
  3. 확인을 클릭합니다.
  4. (방화벽에서 HSM 버전을 변경하는 경우에만 필요) 버전 변경이 성공하면 방화벽에서 새 HSM 버전으로 변경하기 위해 재부팅하라는 메시지를 표시합니다. 메시지가 표시되면 예를 클릭합니다.
  5. 마스터 키가 방화벽에 없으면 클라이언트 버전 업그레이드가 실패합니다. 메시지를 닫고 마스터 키를 방화벽에 로컬로 설정합니다.
     - 하드웨어 보안 모듈 공급자를 편집하고 **HSM**으로 보호된 마스터 키 옵션을 비활성화(지우기)합니다.
     - 확인을 클릭합니다.
     - **Device** > **Master** 키 및 진단을 선택하여 마스터 키를 편집합니다.
     - 현재 마스터 키를 입력하십시오. 그런 다음 동일한 키를 새 마스터 키로 입력한 다음 새 마스터 키 확인을 입력할 수 있습니다.
     - 확인을 클릭합니다.
     - **HSM** 클라이언트 버전 선택을 위해 처음 4단계를 반복하고 다시 재부팅합니다.

## 세이프넷 네트워크 **HSM**을 통한 연결 설정

Palo Alto Networks 방화벽(HSM 클라이언트)과 SafeNet 네트워크 HSM 서버 간의 연결을 설정하려면 서버의 IP 주소를 지정하고 방화벽을 서버에 인증하기 위한 암호를 입력한 다음 서버에 방화벽을 등록해야 합니다. HSM 클라이언트를 구성하기 전에 HSM 서버의 방화벽에 대한 파티션을 만든 다음 방화벽의 SafeNet 네트워크 클라이언트 버전이 SafeNet Network HSM 서버와 호환되는지 확인합니다(HSM과의 연결 설정 참조).

HSM과 방화벽이 연결되기 전에 HSM은 방화벽 IP 주소를 기반으로 방화벽을 인증합니다. 따라서 DHCP를 통해 할당된 동적 주소가 아닌 정적 IP 주소를 사용하도록 방화벽을 구성해야 합니다. 런타임 동안 방화벽 IP 주소가 변경되면 HSM의 작업이 작동을 중지합니다.

*HSM* 구성은 고가용성*(HA)* 방화벽 피어 간에 동기화되지 않습니다**.** 따라서 각 피어에서 별도로 *HSM*을 구성해야 합니다**.** 능동형*/*수동형 *HA* 구성에서 수동으로 하나의 페일오버를 수행하여 *HSM*에 대한 각 *HA* 피어를 개별적으로 구성하고 인증해야 합니다**.** 이 초기 수동 페일오버 후에는 페일오버가 제대로 작동하기 위해 사용자 상호 작용이 필요하지 않습니다**.**

**STEP 1 |** 각 SafeNet 네트워크 HSM에 대한 연결 설정을 정의합니다.

1. 방화벽 웹 인터페이스에 로그인하고 디바이스 > 설정 > **HSM**을 선택합니다.
2. 하드웨어 보안 모듈 공급자 설정을 편집하고 **Provider Configured**를 **SafeNet Network HSM**으로 설정합니다.
3. 다음과 같이 각 HSM 서버를 추가합니다. 고가용성(HA) HSM 구성에는 두 개 이상의 서버가 필요합니다. 최대 16개의 HSM 서버 클러스터를 가질 수 있습니다. 클러스터의 모든 HSM 서버는 동일한 SafeNet 버전을 실행해야 하며 별도로 인증해야 합니다. 클러스터 전체에서 키를 복사하

 ©2023 Palo Alto Networks, Inc.

려는 경우에만 SafeNet 클러스터를 사용해야 합니다. 또는 최대 16개의 SafeNet HSM 서버를 추가하여 독립적으로 작동할 수 있습니다.

1. HSM 서버에 대한 모듈 이름(최대 31자 문자열)을 입력합니다.
2. HSM 서버 주소에 IPv4 주소를 입력합니다.

4. (HA만) 고가용성을 선택하고 자동 복구 재시도 값을 지정합니다(HSM 클라이언트가 이전에 HSM 서버에 대한 연결 복구를 시도하는 최대 횟수). HSM HA 피어 서버로 장애 조치, 범위는 0 ~ 500, 기본값은 0) 고가용성 그룹 이름(최대 31자 길이의 ASCII 문자열)을 입력합니다.

   두 개 이상의 ***HSM*** 서버를 구성하는 경우 모범 사례는 고가용성을 활성화하는 것입니다. 그렇지 않으면 방화벽은 추가 ***HSM*** 서버를 사용하지 않습니다.

5. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 2 |** (선택 사항) 방화벽이 관리 인터페이스를 통해 연결하지 않도록 하려면 HSM에 연결하도록 서비스 경로를 구성합니다(기본값).

***HSM***에 대한 서비스 경로를 구성하는 경우 ***clear session all*** *CLI* 명령을 실행하면 모든 기존 ***HSM*** 세션이 지워져 모든 ***HSM*** 상태가 다운되었다가 다시 활성화됩니다. ***HSM***이 복구되는 데 필요한 몇 초 동안 모든 ***SSL/TLS*** 작업이 실패합니다.

1. 디바이스 > 설정 > 서비스를 선택하고 서비스 경로 구성을 클릭합니다.
2. 서비스 경로를 맞춤설정합니다. **IPv4** 탭은 기본적으로 활성화되어 있습니다.
3. 서비스 열에서 **HSM**을 클릭합니다.
4. HSM에 대한 소스 인터페이스를 선택합니다.
5. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 3 |** 방화벽을 구성하여 HSM에 인증합니다.

1. 디바이스 > 설정 및 하드웨어 보안 모듈 설정을 선택합니다.
2. HSM 서버 이름을 선택합니다.
3. 인증 및 신뢰 인증서에 대해 자동 또는 수동을 선택합니다.
4. 관리자 암호를 입력하여 HSM에 대한 방화벽을 인증합니다.
5. 확인을 클릭합니다.

   방화벽이 HSM에 대한 인증을 시도하고 상태 메시지를 표시합니다.

6. 확인을 다시 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 방화벽을 HSM 서버와 HSM 클라이언트로 등록하고 방화벽을 HSM 서버의 파티션에 할당합니다.

> *HSM*에 동일한 *<cl-name>*이(가) 이미 등록된 방화벽이 있는 경우 먼저 ***client delete -client <cl-name>***를 실행하여 중복 등록을 제거해야 합니다. 여기서 *<cl-name>*은 삭제할 등록된 클라이언트(방화벽)의 이름입니다.

1. 원격 시스템에서 HSM에 로그인합니다.
2. **client register -c <cl-name> -ip <fw-ip-addr>** CLI 명령을 사용하여 방화벽을 등록합니다. 여기서 *<cl-name>*은 HSM에서 사용하기 위해 방화벽에 할당하는 이름이고 *<fw-ip-addr>*은 해당 방화벽의 IP 주소입니다.
3. **client assignpartition -c <cl-name> -p <partition-name>** CLI 명령을 사용하여 방화벽에 파티션을 할당합니다. 여기서 *<cl-name>*는 **client register** 명령을 사용하여 방화벽에 할당한 이름이고 *<partition-name>*는 이 방화벽에 할당하려는 이전에 구성된 파티션의 이름입니다.

**STEP 5 |** HSM 파티션에 연결할 방화벽을 구성합니다.

1. 디바이스 > 설정 > **HSM**을 선택하고 디스플레이를 새로 고칩니다( ).
2. **HSM** 파티션 설정(하드웨어 보안 작업 설정).
3. 파티션 암호를 입력하여 HSM의 파티션에 대한 방화벽을 인증합니다.
4. 확인을 클릭합니다.

**STEP 6 |** (HA만) 이전 인증, 등록 및 파티션 연결 단계를 반복하여 기존 HA 그룹에 다른 HSM을 추가합니다.

> 구성에서 *HSM*을 제거하면 이전 파티션 연결 단계를 반복하여 *HA* 그룹에서 삭제된 *HSM*을 제거합니다.

**STEP 7 |** HSM을 사용하여 방화벽 연결 및 인증을 확인합니다.

1. 디바이스 > 설정 > **HSM**을 선택하고 인증 및 연결 상태를 확인합니다.
   - 녹색 - 방화벽이 성공적으로 인증되어 HSM에 연결되었습니다.
   - 빨간색 - 방화벽이 HSM에 대한 인증에 실패했거나 HSM에 대한 네트워크 연결이 끊어졌습니다.
2. 하드웨어 보안 모듈 상태에서 다음 열을 확인하여 인증 상태를 확인합니다.
   - 일련번호 - 방화벽이 HSM에 성공적으로 인증된 경우 HSM 파티션의 일련번호입니다.
   - 파티션 - 방화벽에 할당된 HSM의 파티션 이름입니다.
   - 모듈 상태 - HSM 연결의 현재 상태입니다. 하드웨어 보안 모듈 상태가 HSM을 표시하는 경우 이 값은 항상 인증됩니다.

## nCipher nShield 커넥트 HSM으로 연결 설정

nCipher nShield Connect HSM을 사용하는 조직의 모든 방화벽(HSM 클라이언트)에 대한 키 데이터를 동기화하려면 원격 파일 시스템(RFS)을 허브로 설정해야 합니다. 방화벽의 nShield Connect 클라이언트 버전이 nShield Connect 서버와 호환되는지 확인하려면 HSM으로 연결 설정을 참조하십시오.


©2023 Palo Alto Networks, Inc.

HSM과 방화벽이 연결되기 전에 HSM은 해당 IP 주소를 기반으로 방화벽을 인증합니다. 따라서 DHCP를 통해 할당된 동적 주소가 아닌 고정 IP 주소를 사용하도록 방화벽을 구성해야 합니다. (런타임 중에 방화벽 IP 주소가 변경되면 HSM에 대한 작업이 작동을 멈춥니다.)

*HSM* 구성은 고가용성*(HA)* 방화벽 피어 간에 동기화되지 않습니다. 따라서 각 피어에서 별도로 *HSM*을 구성해야 합니다. 능동형/수동형 *HA* 구성에서 수동으로 하나의 페일오버를 수행하여 *HSM*에 대한 각 *HA* 피어를 개별적으로 구성하고 인증해야 합니다. 이 초기 수동 페일오버 후에는 페일오버가 제대로 작동하기 위해 사용자 상호 작용이 필요하지 않습니다.

**STEP 1 |** 각 nCipher nShield Connect HSM에 대한 연결 설정을 정의합니다.

1. 방화벽 웹 인터페이스에 로그인하고 디바이스 > 설정 > **HSM**을 선택합니다.
2. 하드웨어 보안 모듈 공급자 설정을 편집하고 **Provider Configured**를 **nShield Connect**로 설정합니다.
3. 다음과 같이 각 HSM 서버를 추가합니다. HA HSM 구성에는 두 개의 서버가 필요합니다.
   1. HSM 서버의 모듈 이름을 입력합니다. 최대 31자의 ASCII 문자열이 될 수 있습니다.
   2. HSM 서버 주소에 IPv4 주소를 입력합니다.
4. 원격 파일 시스템 주소에 IPv4 주소를 입력합니다.
5. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 2 |** (선택 사항) 방화벽이 관리 인터페이스를 통해 연결하지 않도록 하려면 HSM에 연결하도록 서비스 경로를 구성합니다(기본값).

*HSM*에 대한 서비스 경로를 구성하는 경우 ***clear session all*** *CLI* 명령을 실행하면 모든 기존 *HSM* 세션이 지워져 모든 *HSM* 상태가 다운되었다가 다시 활성화됩니다. *HSM*이 복구되는 데 필요한 몇 초 동안 모든 *SSL/TLS* 작업이 실패합니다.

1. 디바이스 > 설정 > 서비스를 선택하고 서비스 경로 구성을 클릭합니다.
2. 서비스 경로를 맞춤설정합니다. **IPv4** 탭은 기본적으로 활성화되어 있습니다.
3. 서비스 열에서 **HSM**을 클릭합니다.
4. HSM에 대한 소스 인터페이스를 선택합니다.
5. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 3 |** 방화벽을 HSM 서버에 HSM 클라이언트로 등록합니다.

이 단계에서는 nShield Connect HSM의 전면 패널 인터페이스를 사용하는 절차를 간략하게 설명합니다. 자세한 내용은 nCipher 문서를 참조하십시오.

1. nCipher nShield Connect HSM의 전면 패널 디스플레이에 로그인합니다.
2. 오른쪽 탐색 버튼을 사용하여 시스템 > 시스템 구성 > 클라이언트 구성 > 새 클라이언트를 선택합니다.
3. 방화벽 IP 주소를 입력합니다.
4. 시스템 > 시스템 구성 > 클라이언트 구성 > 원격 파일 시스템을 선택하고 클라이언트 컴퓨터의 IP 주소를 입력합니다. RFS를 설정합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 방화벽에서 연결을 수락하도록 RFS를 구성합니다.

1. Linux 클라이언트에서 RFS에 로그인합니다.
2. **ankneti *<ip-address>*** CLI를 실행하여 클라이언트에 HSM을 인증하는 $K_{NETI}$ 키의 전자 일련 번호(ESN) 및 해시를 가져옵니다. 여기서 *<ip-address>*는 HSM IP 주소입니다.

   예:

   ```
   anonkneti 192.0.2.1
   ```

   ```
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```

   이 예에서 `B1E2-2D4C-E6A2`는 ESN이고 `5a2e5107e70d525615a903f6391ad72b1c03352c`는 $K_{NETI}$ 키의 해시입니다.
3. 운용 관리자 계정에서 다음 명령을 사용하여 RFS를 설정합니다.

   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```

   *<ip-address>*은 HSM의 IP 주소, *<ESN>*은 전자 일련 번호, *<hash-Kneti-key>*는 $K_{>NETI}$ 키의 해시입니다.

   다음 예에서는 이 절차에서 얻은 값을 사용합니다.

   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2
    5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. RFS에서 HSM 클라이언트 제출을 허용하려면 다음 명령을 사용하십시오.

   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```

   여기서 *<FW-IPaddress>*은(는) 방화벽 IP 주소입니다.

**STEP 5 |** 방화벽을 HSM에 인증합니다.

1. 방화벽 웹 인터페이스에서 디바이스 > 설정 > **HSM** 및 하드웨어 보안 모듈 설정을 선택합니다.
2. 확인을 클릭합니다.

   방화벽이 HSM에 대한 인증을 시도하고 상태 메시지를 표시합니다.
3. 확인을 클릭합니다.

**STEP 6 |** 디바이스 > 설정 > **HSM** 및 원격 파일 시스템과 동기화를 선택하여 방화벽을 RFS와 동기화합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** HSM을 사용하여 방화벽 연결 및 인증을 확인합니다.

1. 디바이스 > 설정 > **HSM**을 선택하고 인증 및 연결 상태를 확인합니다.
   - 녹색 - 방화벽이 성공적으로 인증되어 HSM에 연결되었습니다.
   - 빨간색 - 방화벽이 HSM에 대한 인증에 실패했거나 HSM에 대한 네트워크 연결이 끊어졌습니다.
2. 하드웨어 보안 모듈 상태를 확인하여 인증 상태를 확인합니다.
   - 이름 - HSM의 이름입니다.
   - **IP** 주소 - HSM의 IP 주소입니다.
   - 모듈 상태 - HSM 연결의 현재 상태: **인증됨** 또는 **인증되지 않음**.

## HSM을 사용하여 마스터 키 암호화

마스터 키는 방화벽과 Panorama의 모든 개인 키와 암호를 암호화합니다. 개인 키를 보안 위치에 저장하는 보안 요구 사항이 있는 경우 HSM에 저장된 암호화 키를 사용하여 마스터 키를 암호화할 수 있습니다. 방화벽 또는 Panorama 방화벽에서 암호 또는 개인 키를 복호화 하는 데 필요한 때마다 마스터 키를 복호화 하는 HSM을 요청합니다. 일반적으로 HSM은 보안이 강화될 수 있도록 방화벽이나 Panorama와 분리된 매우 안전한 위치에 있습니다.

HSM은 래핑 키를 사용하여 마스터 키를 암호화합니다. 보안을 유지하려면 이 래핑 키를 변경(새로 고쳐야 합니다).

다음 항목에서는 마스터 키를 처음에 암호화하는 방법과 마스터 키 암호화를 새로 고치는 방법에 대해 설명합니다.

- 마스터 키 암호화
- 마스터 키 암호화 새로 고침

### 마스터 키 암호화

이전에 방화벽에서 마스터 키를 암호화하지 않은 경우 다음 절차를 사용하여 암호화합니다. 키를 처음으로 암호화하거나 새 마스터 키를 정의하고 암호화하려는 경우 이 절차를 사용하십시오. 이전에 암호화된 키의 암호화를 새로 고치려면 마스터 키 암호화 새로 고침을 참조하십시오.

**STEP 1 |** 디바이스 > 마스터 키 및 진단을 선택합니다.

**STEP 2 |** 마스터 키 필드에 방화벽의 모든 개인 키와 암호를 암호화하는 데 현재 사용되는 키를 지정하십시오.

**STEP 3 |** 마스터 키를 변경하는 경우 새 마스터 키를 입력하고 확인합니다.

**STEP 4 |** **HSM** 확인란을 선택합니다.

- 수명 - 마스터 키가 만료되는 날짜 및 시간입니다(범위 1-730일).
- 미리 알림 시간 - 사용자에게 임박한 만료 알림이 표시되는 만료 전 날짜 및 시간입니다(1–365일 범위).

**STEP 5 |** 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

### 마스터 키 암호화 새로 고침

가장 좋은 방법은 마스터 키를 암호화하는 래핑 키를 교체하여 주기적으로 마스터 키 암호화를 새로 고치는 것입니다. 회전 빈도는 애플리케이션에 따라 다릅니다. 래핑 키는 HSM에 있습니다. 다음 명령은 SafeNet Network 및 nCipher nShield Connect HSM에 대해 동일합니다.

**STEP 1 |** 방화벽 CLI에 로그인합니다.

**STEP 2 |** 다음 CLI 명령을 사용하여 HSM의 마스터 키에 대한 래핑 키를 교체합니다.

```
> request hsm mkey-wrapping-key-rotation
```

마스터 키가 HSM에서 암호화된 경우 CLI 명령은 HSM에서 새 래핑 키를 생성하고 새 래핑 키로 마스터 키를 암호화합니다.

마스터 키가 HSM에서 암호화되지 않은 경우 CLI 명령은 나중에 사용할 수 있도록 HSM에서 새 래핑 키를 생성합니다.

이전 래핑 키는 이 명령으로 삭제되지 않습니다.

## HSM에 개인 키 저장

보안을 추가하려면 HSM을 사용하여 SSL/TLS 복호화에 사용되는 개인 키를 보호할 수 있습니다.

- SSL 포워드 프록시 - HSM은 SSL/TLS 포워드 프록시 작업에 인증서에 서명하는 전방 트러스트 인증서의 개인 키를 저장할 수 있습니다. 그런 다음 방화벽은 클라이언트에 인증서를 포워딩하기 전에 서명을 위해 이러한 작업 중에 생성되는 인증서를 HSM으로 보냅니다.
- SSL 인바운드 검사 - HSM은 SSL/TLS 인바운드 검사를 수행하는 내부 서버에 대한 개인 키를 저장할 수 있습니다.

DHE 또는 ECDHE 키 교환 알고리즘을 사용하여 SSL 복호화에 대한 완벽한 전방 기밀성(PFS) 지원을 가능하게 하는 경우 HSM을 사용하여 SSL 인바운드 검사의 개인 키를 저장할 수 있습니다. 또한 HSM을 사용하여 TLSv1.3을 사용하지 않는 한 SSL 포워드 프록시 또는 SSL 인바운드 검사 복호화에 사용되는 ECDSA 키를 저장할 수도 있습니다. TLSv1.3 트래픽의 경우 PAN-OS는 SSL 포워드 프록시에 대해서만 HSM을 지원합니다. SSL 인바운드 검사용 HSM은 지원하지 않습니다.

**STEP 1 |** HSM에서 복호화 배포에 사용되는 인증서 및 개인 키를 가져오거나 생성합니다.

HSM에서 인증서 및 개인 키를 가져오거나 생성하는 방법에 대한 지침은 HSM 설명서를 참조하십시오.

**STEP 2 |** (nCipher nShield 연결만) nCiphernShield 원격 파일 시스템에서 방화벽에 키 데이터를 동기화합니다.

세이프넷 네트워크 *HSM*과의 동기화는 자동입니다.

1. 방화벽 웹 인터페이스에 액세스하고 디바이스 > 설정 > **HSM**을 선택합니다.
2. 원격 파일 시스템과 동기화(하드웨어 보안 작업 설정).


©2023 Palo Alto Networks, Inc.

**STEP 3 |** HSM 저장 키에 해당하는 인증서를 가져옵니다.

1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 가져오기를 클릭합니다.
2. 인증서 이름을 입력합니다.
3. HSM에서 인증서 파일을 찾아보기합니다.
4. 파일 형식을 선택합니다.
5. 하드웨어 보안 모듈에 있는 개인 키를 선택합니다.
6. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 4 |** (전달 신뢰 인증서만) SSL/TLS 전달 프록시에서 사용할 인증서를 활성화합니다.

1. 편집을 위해 3단계에서 가져온 인증서를 엽니다.
2. 신뢰 인증서 전달을 선택합니다.
3. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 5 |** 인증서를 방화벽으로 성공적으로 가져왔는지 확인합니다.

3단계에서 불러온 인증서를 찾아 키 열의 아이콘을 확인합니다.

- 잠금 아이콘 - 인증서의 개인 키는 HSM에 있습니다.
- 오류 아이콘 - 개인 키는 HSM에 없거나 HSM이 제대로 인증되거나 연결되지 않습니다.

## HSM 배포 관리

HSM 배포를 관리하기 위해 다음 작업을 수행할 수 있습니다.

- HSM 구성 설정을 봅니다.

  디바이스 > 설정 > **HSM**을 선택합니다.

- 자세한 HSM 정보를 표시합니다.

  하드웨어 보안 작업 섹션에서 자세한 정보 표시를 선택합니다.

  HSM 서버, HSM HA 상태 및 HSM 하드웨어에 대한 정보가 표시됩니다.

- 지원 파일 내보내기입니다.

  하드웨어 보안 작업 섹션에서 내보내기 지원 파일을 선택합니다.

  방화벽의 HSM 구성 문제를 해결할 때 고객 지원을 돕기 위해 테스트 파일이 만들어집니다.

- HSM 구성을 재설정합니다.

  하드웨어 보안 작업 섹션에서 **HSM** 구성 재설정을 선택합니다.

  이 옵션을 선택하면 모든 HSM 연결이 제거됩니다. 이 옵션을 사용한 후 모든 인증 절차를 반복해야 합니다.


©2023 Palo Alto Networks, Inc.

# 고가용성

HA(고가용성)는 두 개의 방화벽이 한 그룹에 배치되거나 최대 16개의 방화벽이 HA 클러스터에 배치되고 해당 구성이 동기화되어 네트워크에서 단일 장애 지점을 방지하는 배포입니다. 방화벽 피어 간의 하트비트 연결은 피어가 다운될 경우 원활한 페일오버를 보장합니다. HA를 설정하면 중복성이 제공되며 비즈니스 연속성을 보장할 수 있습니다.


- HA 개요
- HA 컨셉
- 활성/패시브 HA 설정
- 활성/활성 HA 설정
- HA 클러스터링 개요
- HA 클러스터링 모범 사례 및 프로비저닝
- HA 클러스터링 구성
- HA1 SSH 키 새로 고침 및 키 옵션 구성
- HA 방화벽 상태
- 참조: HA 동기화
- CLI 치트 시트 - HA

# HA 개요

두 개의 Palo Alto Networks 방화벽을 HA 쌍으로 구성하거나 최대 16개의 방화벽을 HA 클러스터의 피어 구성원으로 구성할 수 있습니다. 클러스터의 피어는 HA 쌍 또는 독립 실행형 방화벽일 수 있습니다. HA를 사용하면 피어 방화벽이 실패하는 경우 대체 방화벽을 사용할 수 있도록 하여 가동 중지 시간을 최소화할 수 있습니다. HA 쌍 또는 클러스터의 방화벽은 방화벽의 전용 또는 대역 내 HA 포트를 사용하여 네트워크, 개체 및 정책 구성과 같은 데이터를 동기화하고 상태 정보를 유지 관리합니다. 관리 인터페이스 IP 주소 또는 관리자 프로파일, HA 특정 구성, 로그 데이터 및 ACC(Application Command Center) 정보와 같은 방화벽 관련 구성은 피어 간에 공유되지 않습니다.

HA 쌍에서 통합된 애플리케이션 및 로그 보기의 경우 Palo Alto Networks 중앙 집중식 관리 시스템인 Panorama를 사용해야 합니다. Panorama 관리자 안내서에서 컨텍스트 전환 - 방화벽 또는 Panorama를 참조하십시오. 활성/패시브 HA의 전제 조건 및 활성/활성 HA의 전제 조건을(를) 참조하십시오. Panorama를 사용하여 HA 클러스터 구성원을 프로비저닝하는 것이 좋습니다. HA 클러스터링 모범 사례 및 프로비저닝에 문의하십시오.

HA 쌍 또는 HA 클러스터의 방화벽에 장애가 발생하고 피어 방화벽이 트래픽 보안 작업을 인계받는 경우 이벤트를 페일오버(Failover)라고 합니다. 페일오버를 트리거하는 조건은 다음과 같습니다.

- 모니터링되는 인터페이스 중 하나 이상이 실패합니다. (링크 모니터링)
- 방화벽에 지정된 하나 이상의 대상에 연결할 수 없습니다. (경로 모니터링)
- 방화벽은 하트비트 폴링에 응답하지 않습니다. (하트비트 폴링 및 헬로 메시지)
- 패킷 경로 상태 모니터링으로 알려진 중요한 칩 또는 소프트웨어 구성 요소가 실패합니다.

Palo Alto Networks 방화벽은 몇 가지 예외를 제외하고 세션 및 구성 동기화를 통해 상태 저장 능동형/수동형 또는 능동형/능동형 고가용성을 지원합니다.

- Azure의 VM 시리즈 방화벽 및 AWS의 VM 시리즈 방화벽은 능동형/수동형 HA만 지원합니다.

  AWS에서 Amazon Elastic Load Balancing(ELB) 서비스로 방화벽을 배포할 때 방화벽은 HA를 지원하지 않습니다(이 경우 ELB 서비스는 페일오버 기능을 제공함).
- Google Cloud Platform의 VM 시리즈 방화벽은 HA를 지원하지 않습니다.

HA 클러스터링을 구성하려면 HA 개념 및 HA 클러스터링 개요을(를) 이해하는 것으로 시작하십시오.


©2023 Palo Alto Networks, Inc.

# HA 컨셉

다음 항목은 Palo Alto Networks 방화벽에서 HA가 작동하는 방식에 대한 개념 정보를 제공합니다.

- HA 모드
- HA 링크 및 백업 링크
- 디바이스 우선 순위 및 선점
- 페일오버
- 활성/패시브 HA에 대한 LACP 및 LLDP 사전 협상
- 부동 IP 주소 및 가상 MAC 주소
- ARP 로드 공유
- 경로 기반 중복성
- HA 타이머
- 세션 소유자
- 세션 설정
- 활성/활성 HA 모드의 NAT
- 활성/활성 HA 모드의 ECMP

## HA 모드

다음 두 가지 모드 중 하나로 HA 쌍으로 방화벽을 설정할 수 있습니다.

- 능동형/수동형 - 한 방화벽은 트래픽을 능동적으로 관리하고 다른 방화벽은 동기화되어 장애가 발생할 경우 능동 상태로 전환할 준비가 됩니다. 이 모드에서는 두 방화벽이 동일한 구성 설정을 공유하며 경로, 링크, 시스템 또는 네트워크 오류가 발생할 때까지 트래픽을 능동적으로 관리합니다. 능동형 방화벽에 장애가 발생하면 수동형 방화벽이 능동 상태로 전환되어 원활하게 인계되며 동일한 정책을 적용하여 네트워크 보안을 유지합니다. 능동형/수동형 HA는 가상 와이어, 레이어 2 및 레이어 3 배포에서 지원됩니다.
- 능동형/능동형 - 두 방화벽이 모두 활성 상태이며 트래픽을 처리하고 동시에 작동하여 세션 설정 및 세션 소유권을 처리합니다. 두 방화벽은 세션 테이블과 라우팅 테이블을 개별적으로 유지 관리하고 서로 동기화합니다. 능동형/능동형 HA는 가상 와이어 및 레이어 3 배포에서 지원됩니다.

  능동형/능동형 HA 모드에서는 방화벽이 DHCP 클라이언트를 지원하지 않습니다. 또한 능동형 기본 방화벽만 DHCP 릴레이로 작동할 수 있습니다. 능동형-보조 방화벽이 DHCP 브로드캐스트 패킷을 수신하면 해당 패킷을 삭제합니다.

  능동형/능동형 구성은 트래픽의 로드 밸런싱을 수행하지 않습니다. 피어로 트래픽을 전송하여 로드 공유를 수행할 수 있지만 부하 분산은 발생하지 않습니다. 두 방화벽에 공유 세션을 로드하는 방법에는 ***ECMP***, 다중 ***ISP*** 및 로드 밸런서 사용이 포함됩니다.

능동형/수동형 또는 능동형/수동형 모드를 사용할지 결정할 때 다음과 같은 차이점을 고려하십시오.


©2023 Palo Alto Networks, Inc.

- 능동형/수동형 모드는 설계가 단순합니다. 능동형/수동형 모드에서 라우팅 및 트래픽 플로우 문제를 훨씬 쉽게 해결할 수 있습니다. 능동형/수동형 모드는 레이어 2 배포를 지원합니다. 능동형/능동형 모드는 지원하지 않습니다.
- 능동형/능동형 모드에는 보다 복잡한 네트워크를 만들 수 있는 Advanced 설계 개념이 필요합니다. 능동형/능동형 HA를 구현하는 방법에 따라 적절한 페일오버를 제공하기 위해 두 방화벽 모두에서 네트워킹 프로토콜 활성화, NAT 풀 복제 및 유동 IP 주소 배포와 같은 추가 구성이 필요할 수 있습니다. 두 방화벽 모두 능동형으로 트래픽을 처리하기 때문에 방화벽은 세션 소유자 및 세션 설정이라는 추가 개념을 사용하여 레이어 7 콘텐츠 검사를 수행합니다. 각 방화벽에 자체 라우팅 인스턴스가 필요하고 항상 두 방화벽에서 완전한 실시간 중복성이 필요한 경우 능동형/능동형 모드를 사용하는 것이 좋습니다. 능동형/능동형 모드는 페일오버 속도가 빠르며 능동형/수동형 모드보다 피크 트래픽 플로우를 더 잘 처리할 수 있습니다. 두 방화벽 모두 능동형으로 트래픽을 처리하기 때문입니다.

  능동형/능동형 모드에서는 ***HA*** 쌍을 사용하여 한 방화벽이 일반적으로 처리할 수 있는 것보다 많은 트래픽을 일시적으로 처리할 수 있습니다. 그러나 한 방화벽에 장애가 발생하면 모든 트래픽이 ***HA*** 쌍의 나머지 방화벽으로 리디렉션되기 때문에 이것이 표준이 아니어야 합니다. 설계에서는 콘텐츠 검사가 활성화된 상태에서 나머지 방화벽이 트래픽 로드의 최대 용량을 처리할 수 있도록 허용해야 합니다. 설계에서 나머지 방화벽의 용량을 초과하면 지연 시간이 길어지거나 애플리케이션 오류가 발생할 수 있습니다.

능동형/수동형 모드에서 방화벽을 설정하는 방법에 대한 자세한 내용은 능동형/수동형 HA 설정을 참조하십시오. 능동형/능동형 모드에서 방화벽을 설정하는 방법에 대한 자세한 내용은 능동형/능동형 HA 설정을 참조하십시오.

HA 클러스터에서는 모든 구성원이 활성으로 간주됩니다. HA 클러스터에 HA 쌍을 추가한 후에도 능동형/수동형 관계를 유지할 수 있는 클러스터의 HA 쌍을 제외하고 수동형 방화벽의 개념이 없습니다.

## HA 링크 및 백업 링크

HA 쌍의 방화벽은 HA 링크를 사용하여 데이터를 동기화하고 상태 정보를 유지합니다. 방화벽의 일부 모델에는 전용 HA 포트(제어 링크(HA1) 및 데이터 링크(HA2))가 있는 반면 다른 모델에서는 대역 내 포트를 HA 링크로 사용해야 합니다.

- 전용 HA 포트가 있는 방화벽의 경우 이러한 포트를 사용하여 방화벽 간의 통신 및 동기화를 관리합니다. 자세한 내용은 Palo Alto Networks 방화벽의 HA 포트를 참조하십시오.
- PA-220 및 PA-220R 방화벽과 같이 전용 HA 포트가 없는 방화벽의 경우 모범 사례로 HA1 포트용 관리 포트를 사용하고 HA1 백업용 데이터플레인 포트를 사용하십시오.

  전용 ***HA*** 포트가 없는 방화벽의 경우 환경을 기반으로 ***HA1*** 및 ***HA1*** 백업에 사용할 포트를 결정하고 가장 적게 사용하고 가장 적게 혼잡한 포트를 파악합니다. ***HA1***을 최상의 인터페이스에 할당하고 ***HA1*** 백업을 다른 인터페이스에 할당합니다.

HA 클러스터의 HA 피어는 독립 실행형 구성원과 HA 쌍의 조합일 수 있습니다. HA 클러스터 구성원은 HA4 링크 및 HA4 백업 링크를 사용하여 세션 상태 동기화를 수행합니다. HA1(제어 링크), HA2(데이터 링크) 및 HA3(패킷 포워딩 링크)은 HA 쌍이 아닌 클러스터 구성원 간에 지원되지 않습니다.


©2023 Palo Alto Networks, Inc.

| HA 링크 및 백업 링크 | 설명 |
| --- | --- |
| 제어 링크 | HA1 링크는 헬로, 하트비트, HA 상태 정보, 라우팅을 위한 Management Plane(MP) 동기화, 사용자 ID 정보를 교환하는 데 사용됩니다. 방화벽은 또한 이 링크를 사용하여 피어와 구성 변경 사항을 동기화합니다. HA1 링크는 레이어 3 링크이며 IP 주소가 필요합니다.<br><br>ICMP는 HA 피어 간에 하트비트를 교환하는 데 사용됩니다.<br><br>HA1에 사용되는 포트 - 일반 텍스트 통신을 위한 TCP 포트 28769 및 28260. 암호화된 통신을 위한 포트 28(TCP를 통한 SSH).<br><br>HA1 링크에서 암호화를 활성화하면 HA1 SSH 키 새로 고침 및 키 옵션 구성도 할 수 있습니다. |
| 데이터 링크 | HA2 링크는 HA 쌍의 방화벽 간에 세션, 포워딩 테이블, IPSec 보안 연결 및 ARP 테이블을 동기화하는 데 사용됩니다. HA2 링크의 데이터 흐름은 항상 단방향입니다(HA2 연결 유지 제외). 능동형 또는 능동형-기본 방화벽에서 수동형 또는 능동형-보조 방화벽으로 이동합니다. HA2 링크는 Layer 2 링크이며 기본적으로 ether type 0x7261을 사용합니다.<br><br>HA2에 사용되는 포트 - IP(프로토콜 번호 99) 또는 UDP(포트 29281)를 전송으로 사용하도록 HA 데이터 링크를 구성할 수 있으므로 HA 데이터 링크가 서브넷을 확장할 수 있습니다. |
| HA1 및 HA2 백업 링크 | HA1 및 HA2 링크에 중복성을 제공합니다. 전용 백업 링크를 사용할 수 없는 경우 대역 내 포트를 HA1 및 HA2 연결 모두에 대한 백업 링크에 사용할 수 있습니다. 백업 HA 링크를 구성할 때 다음 지침을 고려하십시오.<br>• 기본 및 백업 HA 링크의 IP 주소는 서로 겹치지 않아야 합니다.<br>• HA 백업 링크는 기본 HA 링크와 다른 서브넷에 있어야 합니다.<br>• HA1-백업 및 HA2-백업 포트는 별도의 물리적 포트에 구성해야 합니다. HA1 백업 링크는 포트 28770 및 28260을 사용합니다.<br>• PA-3200 시리즈 방화벽은 HA1 백업 링크에 대해 IPv6 주소를 지원하지 않으며 IPv4 주소를 사용합니다.<br><br>*Palo Alto Networks*는 ***HA1*** 또는 ***HA1*** 백업 링크에 대역 내 포트를 사용하는 경우 하트비트 백업***(MGT*** 인터페이스에서 포트 ***28771*** 사용***)***을 활성화할 것을 권장합니다**.** |
| 패킷 포워딩 링크 | HA1 및 HA2 링크 외에도 능동형/능동형 배포에는 전용 HA3 링크도 필요합니다. 방화벽은 세션 설정 및 비대칭 트래픽 플로우 중에 피어로 패킷을 포워딩하기 위해 이 링크를 사용합니다. HA3 링크는 MAC-in-MAC 캡슐화를 사용하는 레이어 2 링크입니다. 레이어 3 주소 지정 또는 암호화를 지원하지 않습니다. PA-7000 시리즈 방화벽은 NPC 간의 세션을 일대일로 동기화합니다. PA-800 시리즈, PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈 및 PA-5400 시리즈 방화벽에서 통합 인터페이스를 HA3 링크로 구성할 수 있습니다. 집계 인터페이스는 HA3 링크에 대한 중복성을 제공할 수도 있습 |


©2023 Palo Alto Networks, Inc.

| HA 링크 및 백업 링크 | 설명 |
|---|---|
| | 니다. HA3 링크에 대한 백업 링크를 구성할 수 없습니다. PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈 및 PA-7000 시리즈 방화벽에서 전용 HSCI 포트는 HA3 링크를 지원합니다. 방화벽은 HA3 링크를 통과하는 패킷에 독점 패킷 헤더를 추가하므로 이 링크를 통한 MTU는 포워딩되는 최대 패킷 길이보다 커야 합니다. |
| HA4 링크 및 HA4 백업 링크 | HA4 링크 및 HA4 백업 링크는 동일한 클러스터 ID를 가진 모든 HA 클러스터 구성원 간에 세션 캐시 동기화를 수행합니다. 클러스터 구성원 간의 HA4 링크는 레이어 2 연결 유지 메시지를 보내고 받아 클러스터 구성원 간의 연결 실패를 감지합니다. 방화벽 대시보드에서 HA4 및 HA4 백업 링크의 상태를 봅니다. |

## Palo Alto Networks 방화벽의 HA 포트

고가용성(HA) 구성에서 두 개의 Palo Alto Networks® 방화벽을 연결할 때 HA 링크 및 백업 링크에 전용 HA 포트를 사용하는 것이 좋습니다. 이러한 전용 포트에는 HA 제어 및 동기화 트래픽에 사용되는 HA1, HA1-A 및 HA1-B 레이블이 지정된 HA1 포트가 포함됩니다. 및 HA 세션 설정 트래픽에 사용되는 HA2 및 HSCI(High Speed Chassis Interconnect) 포트. PA-5200 시리즈 방화벽에는 HA1 트래픽에 대해 구성할 수 있는 AUX-1 및 AUX-2라는 레이블이 붙은 다목적 보조 포트가 있습니다.

세션 설정 및 비대칭 트래픽 플로우(능동형/능동형 HA만 해당) 중에 피어 방화벽으로 패킷을 포워딩하는 데 사용되는 HA3용 HSCI 포트를 구성할 수도 있습니다. HSCI 포트는 HA2 트래픽, HA3 트래픽 또는 둘 다에 사용할 수 있습니다.

*HA1* 및 *AUX* 링크는 *Management Plane(MP)*에 있는 기능에 대한 동기화를 제공합니다. 관리 플레인에서 전용 *HA* 인터페이스를 사용하면 데이터 플레인을 통해 동기화 패킷을 포워딩할 필요가 없으므로 대역 내 포트를 사용하는 것보다 더 효율적입니다.

방화벽에 전용 *HA* 포트(예: *PA-220* 및 *PA-400* 시리즈)가 없는 경우 데이터 포트를 *HA* 인터페이스로 구성할 수 있습니다. 방화벽에 전용 *HA* 포트가 있지만 전용 *HA* 백업 포트가 없는 경우 전용 *HA* 포트에 대한 백업으로 데이터 포트를 구성할 수도 있습니다.

네트워크 문제가 있는 경우 발생할 수 있는 *HA* 링크 및 통신 문제를 피하기 위해 가능하면 항상 *HA* 쌍의 두 방화벽 사이에 *HA* 포트를 직접 연결합니다(스위치나 라우터를 통하지 않음).

다음 표를 사용하여 전용 HA 포트와 HA 링크 및 백업 링크를 연결하는 방법에 대해 알아보십시오.


©2023 Palo Alto Networks, Inc.

| 모델 | 전면 패널 전용 포트 |
| --- | --- |
| PA-800 시리즈 방화벽 | • **HA1** 및 **HA2** - 두 HA 모드에서 HA1 및 HA2에 사용되는 이더넷 10Mbps/100Mbps/1000Mbps 포트입니다.<br>  • **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1 포트를 쌍의 두 번째 방화벽에 있는 HA1 포트에 직접 연결하거나 스위치나 라우터를 통해 이러한 포트를 함께 연결합니다.<br>  • **HA2** 트래픽의 경우 - 첫 번째 방화벽의 HA2 포트를 쌍의 두 번째 방화벽에 있는 HA2 포트에 직접 연결하거나 스위치나 라우터를 통해 이러한 포트를 함께 연결합니다. |
| PA-3200 시리즈 방화벽 | • **HA1-A** 및 **HA1-B** - 두 HA 모드에서 HA1 트래픽에 사용되는 이더넷 10Mbps/100Mbps/1000Mbps 포트.<br>  • **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1-A 포트를 쌍의 두 번째 방화벽에 있는 HA1-A 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>  • **HA1-A** 연결에 대한 백업 - 첫 번째 방화벽의 HA1-B 포트를 쌍의 두 번째 방화벽에 있는 HA1-B 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br><br>  방화벽 데이터플레인이 장애 또는 수동형 재시작으로 인해 재시작되면 ***HA1-B*** 링크도 재시작됩니다. 이 문제가 발생하고 ***HA1-A*** 링크가 연결 및 구성되지 않은 경우 스플릿 브레인 상태가 발생합니다. 따라서 중복성을 제공하고 스플릿 브레인 문제를 방지하기 위해 ***HA1-A*** 포트와 ***HA1-B*** 포트를 연결하고 구성하는 것이 좋습니다.<br><br>  ***PAN-OS*** 또는 ***Panorama***를 통해 방화벽의 ***SFP*** 포트를 ***HA1-A*** 및 ***HA1-B*** 포트로 다시 매핑할 수 있습니다.<br>• **HSCI** - HSCI 포트는 HA 구성에서 2개의 PA-3200 시리즈 방화벽을 연결하는 레이어 1 SFP+ 인터페이스입니다. HA2 연결, HA3 연결 또는 둘 다에 이 포트를 사용합니다.<br><br>  HSCI 포트를 통해 포워딩되는 트래픽은 라우팅하거나 전환할 수 없는 원시 레이어 1 트래픽입니다. 따라서 HSCI 포트를 서로 직접 연결해야 합니다(첫 번째 방화벽의 HSCI 포트에서 두 번째 방화벽의 HSCI 포트로). |


©2023 Palo Alto Networks, Inc.

| 모델 | 전면 패널 전용 포트 |
| --- | --- |
| PA-3400 시리즈 방화벽 | • **HA1-A** 및 **HA1-B** - 두 HA 모드에서 HA1 트래픽에 사용되는 이더넷 10Mbps/100Mbps/1000Mbps 포트.<br>  • **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1-A 포트를 쌍의 두 번째 방화벽에 있는 HA1-A 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>  • **HA1-A** 연결에 대한 백업 - 첫 번째 방화벽의 HA1-B 포트를 쌍의 두 번째 방화벽에 있는 HA1-B 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **HSCI** - HSCI 포트는 HA 구성에서 2개의 PA-3400 시리즈 방화벽을 연결하는 레이어 1 SFP+ 인터페이스입니다. HA2 연결, HA3 연결 또는 둘 다에 이 포트를 사용합니다.<br>HSCI 포트를 통해 포워딩되는 트래픽은 라우팅이나 전환이 불가능한 원시 레이어 1 트래픽입니다. 따라서 HSCI 포트를 서로 직접 연결해야 합니다(첫 번째 방화벽의 HSCI 포트에서 두 번째 방화벽의 HSCI 포트로). |
| PA-5200 시리즈 방화벽 | • **HA1-A** 및 **HA1-B** - 두 HA 모드에서 HA1 트래픽에 사용되는 이더넷 10Mbps/100Mbps/1000Mbps 포트.<br>  • **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1-A 포트를 쌍의 두 번째 방화벽에 있는 HA1-A 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>  • **HA1-A** 연결에 대한 백업 - 첫 번째 방화벽의 HA1-B 포트를 쌍의 두 번째 방화벽에 있는 HA1-B 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **HSCI** - HSCI 포트는 HA 구성에서 2개의 PA-5200 시리즈 방화벽을 연결하는 레이어 1 인터페이스입니다. HA2 연결, HA3 연결 또는 둘 다에 이 포트를 사용합니다.<br>*PA-5220* 방화벽의 ***HSCI*** 포트는 ***QSFP+*** 포트이고 ***PA-5250***, ***PA-5260*** 및 ***PA-5280*** 방화벽의 ***HSCI*** 포트는 ***QSFP28*** 포트입니다.<br>HSCI 포트를 통해 포워딩되는 트래픽은 라우팅이나 전환이 불가능한 원시 레이어 1 트래픽입니다. 따라서 HSCI 포트를 서로 직접 연결해야 합니다(첫 번째 방화벽의 HSCI 포트에서 두 번째 방화벽의 HSCI 포트로). |
| PA-5200 시리즈 방화벽(계속) | • **AUX-1** 및 **AUX-2** - 보조 SFP+ 포트는 HA1, 관리 기능 또는 Panorama로의 로그 포워딩을 위해 구성할 수 있는 다목적 포트입니다. |


©2023 Palo Alto Networks, Inc.

| 모델 | 전면 패널 전용 포트 |
| --- | --- |
| | 이러한 기능 중 하나를 위해 파이버 연결이 필요할 때 이 포트를 사용하십시오.<br>• **HA1** 트래픽의 경우 - 첫 번째 방화벽의 AUX-1 포트를 쌍의 두 번째 방화벽에 있는 AUX-1 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **AUX-1** 연결에 대한 백업 - 첫 번째 방화벽의 AUX-2 포트를 쌍의 두 번째 방화벽에 있는 AUX-2 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다. |
| PA-5400 시리즈 방화벽(PA-5410, PA-5420 및 PA-5430) | • **HA1-A** 및 **HA1-B** - 두 HA 모드에서HA1 트래픽에 사용되는 이더넷 1Gbps/10Gbps 포트.<br>• **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1-A 포트를 쌍의 두 번째 방화벽에 있는 HA1-A 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **HA1-A** 연결에 대한 백업 - 첫 번째 방화벽의 HA1-B 포트를 쌍의 두 번째 방화벽에 있는 HA1-B 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **HSCI** - HSCI 포트는 HA 구성에서 2개의 PA-5400 시리즈 방화벽을 연결하는 레이어 1 SFP+ 인터페이스입니다. HA2 연결, HA3 연결 또는 둘 다에 이 포트를 사용합니다.<br>HSCI 포트를 통해 포워딩되는 트래픽은 라우팅이나 전환이 불가능한 원시 레이어 1 트래픽입니다. 따라서 HSCI 포트를 서로 직접 연결해야 합니다(첫 번째 방화벽의 HSCI 포트에서 두 번째 방화벽의 HSCI 포트로). |
| PA-5450 방화벽 | • **HA1-A** 및 **HA1-B** - 두 HA 모드에서 HA1 트래픽에 사용되는 SFP/SFP+ 1Gbps/10Gbps 포트.<br>• **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1-A 포트를 쌍의 두 번째 방화벽에 있는 HA1-A 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **HA1-A** 연결에 대한 백업 - 첫 번째 방화벽의 HA1-B 포트를 쌍의 두 번째 방화벽에 있는 HA1-B 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다. |


©2023 Palo Alto Networks, Inc.

| 모델 | 전면 패널 전용 포트 |
| --- | --- |
| | • **HSCI-A** 및 **HSCI-B** - HSCI 포트는 HA 구성에서 2개의 PA-5450 방화벽을 연결하는 레이어 1 QSFP+ 인터페이스입니다. HA2 연결, HA3 연결 또는 둘 다에 이 포트를 사용합니다.<br><br>HSCI 포트를 통해 포워딩되는 트래픽은 라우팅하거나 전환할 수 없는 원시 레이어 1 트래픽입니다. 따라서 이러한 포트를 다음과 같이 연결해야 합니다.<br><br>• **HA2** 및 **HA3** 트래픽의 경우 - 첫 번째 방화벽의 HSCI-A 포트를 두 번째 방화벽의 HSCI-A 포트에 직접 연결합니다.<br>• **HSCI-A** 연결에 대한 백업 - 첫 번째 방화벽의 HSCI-B 포트를 두 번째 방화벽의 HSCI-B 포트에 직접 연결합니다. |
| PA-7000 시리즈 방화벽 | • **HA1-A** 및 **HA1-B** - 두 HA 모드에서 HA1 트래픽에 사용되는 이더넷 10Mbps/100Mbps/1000Mbps 포트.<br><br>• **HA1** 트래픽의 경우 - 첫 번째 방화벽의 HA1-A 포트를 쌍의 두 번째 방화벽에 있는 HA1-A 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br>• **HA1-A** 연결에 대한 백업 - 첫 번째 방화벽의 HA1-B 포트를 쌍의 두 번째 방화벽에 있는 HA1-B 포트에 직접 연결하거나 스위치나 라우터를 통해 함께 연결합니다.<br><br>*NPC* 데이터 포트 또는 관리*(MGT)* 포트에서는 *HA1* 연결을 구성할 수 없습니다.<br><br>• **HSCI-A** 및 **HSCI-B** - HSCI 포트는 HA 구성에서 2개의 PA-7000 시리즈 방화벽을 연결하는 레이어 1 QSFP+ 인터페이스입니다. HA2 연결, HA3 연결 또는 둘 다에 이 포트를 사용합니다.<br><br>HSCI 포트를 통해 포워딩되는 트래픽은 라우팅하거나 전환할 수 없는 원시 레이어 1 트래픽입니다. 따라서 이러한 포트를 다음과 같이 연결해야 합니다.<br><br>• **HA2** 및 **HA3** 트래픽의 경우 - 첫 번째 방화벽의 HSCI-A 포트를 두 번째 방화벽의 HSCI-A 포트에 직접 연결합니다.<br><br>*HA2* 또는 *HA2/HA3* 트래픽의 경우 *PA-7000* 시리즈 방화벽은 *NPC* 간에 세션을 일대일로 동기화합니다.<br><br>• **HSCI-A** 연결에 대한 백업 - 첫 번째 방화벽의 HSCI-B 포트를 두 번째 방화벽의 HSCI-B 포트에 직접 연결합니다. |


©2023 Palo Alto Networks, Inc.

| 모델 | 전면 패널 전용 포트 |
| --- | --- |
| | ***HA2*** 및 ***HA2-Backup*** 링크는 ***HSCI*** 포트 대신 데이터플레인 인터페이스를 사용하도록 구성할 수 있습니다. 그러나 이렇게 구성된 경우 ***HA2*** 및 ***HA2-Backup*** 링크 모두 데이터플레인 인터페이스를 사용해야 합니다. ***HA2*** 또는 ***HA2-Backup***용 데이터플레인 포트와 ***HSCI*** 포트가 혼합되면 ***Commit*** 오류가 발생합니다. 이는 ***PA-7050-SMC***, ***PA-7080-SMC***, ***PA-7050-SMC-B*** 및 ***PA-7080-SMC-B***에 적용됩니다. |

## 디바이스 우선 순위 및 선점

능동형-수동형 HA 쌍의 방화벽에는 활성 역할을 맡아야 하는 방화벽에 대한 기본 설정을 나타내는 디바이스 우선 순위 값이 할당될 수 있습니다. 트래픽을 적극적으로 보호하기 위해 HA 쌍에서 특정 방화벽을 사용해야 하는 경우 두 방화벽 모두에서 선점 동작을 사용하도록 설정하고 각 방화벽에 디바이스 우선 순위 값을 할당해야 합니다. 숫자 값이 낮아 우선 순위가 높은 방화벽은 능동형으로 지정됩니다. 다른 방화벽은 수동형 방화벽입니다.

능동형-능동형 HA 쌍의 경우에도 마찬가지입니다. 그러나 디바이스 ***ID***는 디바이스 우선 순위 값을 할당하는 데 사용됩니다. 마찬가지로 디바이스 ID의 숫자 값이 낮을수록 우선 순위가 높습니다. 우선 순위가 높은 방화벽은 활성 기본 방화벽이 되고 쌍으로 연결된 방화벽은 능동형-기본 방화벽이 됩니다.

기본적으로 방화벽에서 선점은 사용하지 않도록 설정되며 두 방화벽 모두에서 사용하도록 설정해야 합니다. 선점형 작동을 사용하면 장애로부터 복구된 후 우선 순위가 높은 방화벽(숫자 값이 낮음)을 능동형 또는 능동형-기본 방화벽으로 재개할 수 있습니다. 선점이 발생하면 이벤트가 시스템 로그에 기록됩니다.

## 페일오버

한 방화벽에서 오류가 발생하고 HA 쌍의 피어(또는 HA 클러스터의 피어)가 트래픽 보안 작업을 인수하는 경우 해당 이벤트를 페일오버(***failover***)라고 합니다. 예를 들어 HA 쌍의 방화벽에서 모니터링되는 메트릭이 실패할 경우 페일오버가 트리거됩니다. 방화벽이 방화벽 장애를 감지하기 위해 모니터링하는 메트릭은 다음과 같습니다.

- 하트비트 폴링 및 헬로 메시지

  방화벽은 헬로 메시지와 하트비트를 사용하여 피어 방화벽이 응답하고 작동하는지 확인합니다. 헬로 메시지는 방화벽의 상태를 확인하기 위해 구성된 헬로 인터벌로 한 피어에서 다른 피어로 전송됩니다. 하트비트는 제어 링크를 통해 HA 피어에 대한 ICMP 핑이며, 피어는 핑에 응답하여 방화벽이 연결되어 응답하는지 확인합니다. 기본적으로 하트비트 인터벌은 1000밀리초입니다. 1000밀리초마다 ping이 전송되고 연속적으로 세 번의 하트비트 손실이 있는 경우 페일오버가 발생합니다. 페일오버를 트리거하는 HA 타이머에 대한 자세한 내용은 HA 타이머를 참조하십시오.

- 링크 모니터링

  방화벽에서 모니터링할 물리적 인터페이스 그룹(링크 그룹)을 지정할 수 있으며 방화벽은 그룹의 각 링크 상태(링크 업 또는 링크 다운)를 모니터링합니다. 링크 그룹에 대한 실패 조건을 결정합니다. 그룹의


©2023 Palo Alto Networks, Inc.

모든 링크 작동 중지 또는 모든 링크가 다운되면 링크 그룹 장애가 발생하지만 반드시 페일오버가 아닐 수도 있습니다.

여러 링크 그룹을 만들 수 있습니다. 따라서 링크 그룹 집합의 고장 조건도 확인할 수 있습니다. 모든 링크 그룹이 실패하거나 모든 링크 그룹이 실패하여 페일오버가 트리거되는 시기를 결정합니다. 기본 동작은 모든 링크 그룹의 임의 링크 실패로 인해 방화벽이 모니터링되는 개체의 오류를 나타내기 위해 HA 상태를 비작동(능동형/활성 모드의 임시 상태)으로 변경하도록 하는 것입니다.

- 경로 모니터링

  방화벽에서 모니터링할 IP 주소의 대상 IP 그룹을 지정할 수 있습니다. 방화벽은 ICMP ping을 사용하여 네트워크에서 미션 크리티컬 IP 주소로의 전체 경로를 모니터링하여 IP 주소의 도달 가능성을 확인합니다. 핑의 기본 인터벌은 200ms입니다. 10개의 연속 핑(기본값)이 실패하면 IP 주소에 연결할 수 없는 것으로 간주됩니다. 대상 IP 그룹의 IP 주소에 대한 실패 조건을 지정합니다. 그룹에서 연결할 수 없는 모든 IP 주소 또는 모든 IP 주소에 연결할 수 없습니다. 가상 와이어, VLAN 또는 가상 라우터의 경로 그룹에 대해 여러 대상 IP 그룹을 지정할 수 있습니다. 경로 그룹에서 대상 IP 그룹의 실패 조건을 지정합니다. 경로 그룹 실패를 구성하는 임의 또는 모두 여러 가상 와이어 경로 그룹, VLAN 경로 그룹 및 가상 라우터 경로 그룹을 구성할 수 있습니다.

  또한 다음과 같이 글로벌 고장 조건을 결정할 수 있습니다. 모든 경로 그룹에 장애가 발생하거나 모든 경로 그룹에 장애가 발생하여 페일오버가 트리거되는 시점을 결정합니다. 기본 동작은 **Any** 가상 와이어, VLAN 또는 가상 라우터 경로 그룹의 **Any** 대상 IP 그룹에서 IP 주소 중 **Any**에 연결할 수 없게 되어 방화벽이 발생한다는 것입니다. 모니터링 대상의 실패를 나타내기 위해 HA 상태를 비기능(또는 활성/활성 모드의 임시 상태)으로 변경합니다.

위에 나열된 페일오버 트리거 외에도 관리자가 방화벽을 일시 중단하거나 선점이 발생할 때도 페일오버가 발생합니다.

PA-3200 시리즈, PA-5200 시리즈 및 PA-7000 시리즈 방화벽에서는 내부 상태 확인이 실패할 경우 페일오버가 발생할 수 있습니다. 이 상태 확인은 구성할 수 없으며 FPGA 및 CPU와 같은 중요한 구성 요소를 모니터링할 수 있도록 활성화됩니다. 또한 모든 플랫폼에서 일반 상태 확인이 수행되어 페일오버가 발생합니다.

다음은 HA 클러스터의 구성원인 PA-7000 시리즈 방화벽에서 NPC(네트워크 처리 카드)에 장애가 발생할 경우 발생하는 현상에 대해 설명합니다.

- HA 클러스터링 세션 캐시(다른 구성원의 세션 복사본)를 보유하는 데 사용 중인 NPC가 다운되면 방화벽이 작동하지 않습니다. 이 경우 세션 배포 디바이스(예: 로드 밸런서)는 방화벽이 다운되었음을 감지하고 세션 로드를 클러스터의 다른 구성원에게 분산해야 합니다.
- 클러스터 구성원의 NPC가 다운되고 해당 NPC에서 링크 모니터링 또는 경로 모니터링이 활성화되지 않은 경우 PA-7000 시리즈 방화벽 구성원은 작동 상태를 유지하지만 하나의 NPC가 다운되었기 때문에 용량이 더 낮습니다.
- 클러스터 구성원의 NPC가 다운되고 해당 NPC에서 링크 모니터링 또는 경로 모니터링이 활성화된 경우 PA-7000 시리즈 방화벽이 작동하지 않고 세션 분배 디바이스(예: 로드 밸런서)가 방화벽이 다운하고 클러스터의 다른 구성원에게 세션 로드를 분산하여 작동 중임을 감지해야 합니다.

## 활성/패시브 HA에 대한 LACP 및 LLDP 사전 협상

방화벽이 LACP 또는 LLDP를 사용하는 경우 페일오버 시 해당 프로토콜을 협상하면 1초 미만의 페일오버가 방지됩니다. 그러나 패시브 방화벽의 인터페이스를 활성화하여 페일오버(failover) 전에 LACP 및

 ©2023 Palo Alto Networks, Inc.

LLDP를 협상할 수 있습니다. 따라서 수동형 또는 비기능 HA 상태의 방화벽은 LACP 또는 LLDP를 사용하여 인접 디바이스와 통신할 수 있습니다. 이러한 사전 협상은 페일오버 속도를 높입니다.

VM 시리즈 방화벽을 제외한 모든 방화벽 모델은 이더넷 또는 AE 인터페이스가 레이어 2, 레이어 3 또는 가상 와이어 배포에 있는지의 여부에 따라 사전 협상 구성을 지원합니다. HA 수동형 방화벽은 다음 두 가지 방법 중 하나로 LACP 및 LLDP 패킷을 처리합니다.

- 활성 - 방화벽에는 인터페이스에 구성된 LACP 또는 LLDP가 있으며 각각 LACP 또는 LLDP 사전 협상에 적극적으로 참여합니다.
- 수동형 - LACP 또는 LLDP가 인터페이스에 구성되지 않고 방화벽이 프로토콜에 참여하지 않지만 방화벽 양쪽의 피어가 각각 LACP 또는 LLDP를 사전 협상할 수 있도록 합니다.

다음 표는 통합 이더넷(AE) 및 이더넷 인터페이스에서 지원되는 배포를 표시합니다.

| 인터페이스 배포 | **AE** 인터페이스 | 이더넷 인터페이스 |
|---|---|---|
| 레이어 2의 LACP | 능동형 | 지원되지 않음 |
| 레이어 3의 LACP | 능동형 | 지원되지 않음 |
| 가상 와이어의 LACP | 지원되지 않음 | 수동형 |
| 레이어 2의 LLDP | 능동형 | 능동형 |
| 레이어 3의 LLDP | 능동형 | 능동형 |
| 가상 와이어의 LLDP | 능동형 | • LLDP 자체가 구성된 경우 활성화됩니다.<br>• LLDP 자체가 구성되지 않은 경우 수동형입니다. |

사전 협상은 하위 인터페이스 또는 터널 인터페이스에서 지원되지 않습니다.

LACP 또는 LLDP 사전 협상을 구성하려면 네트워크에서 LACP 또는 LLDP를 사용하는 경우 더 빠른 페일오버를 위해 능동형/수동형 HA에 대한 LACP 및 LLDP 사전 협상 활성화(선택 사항) 단계를 참조하십시오.

## 부동 IP 주소 및 가상 MAC 주소

HA 능동형/능동형 모드의 레이어 3 배포에서 유동 IP 주소를 할당할 수 있습니다. 유동 IP 주소는 링크나 방화벽이 실패할 경우 한 HA 방화벽에서 다른 방화벽으로 이동합니다. 유동 IP 주소를 소유한 방화벽의 인터페이스는 가상 MAC 주소로 ARP 요청에 응답합니다.

VRRP(가상 라우터 중복 프로토콜)와 같은 기능이 필요한 경우 유동 IP 주소를 사용하는 것이 좋습니다. 유동 IP 주소는 VPN 및 소스 NAT를 구현하는 데도 사용할 수 있으므로 해당 서비스를 제공하는 방화벽이 실패할 때 지속적인 연결이 가능합니다.

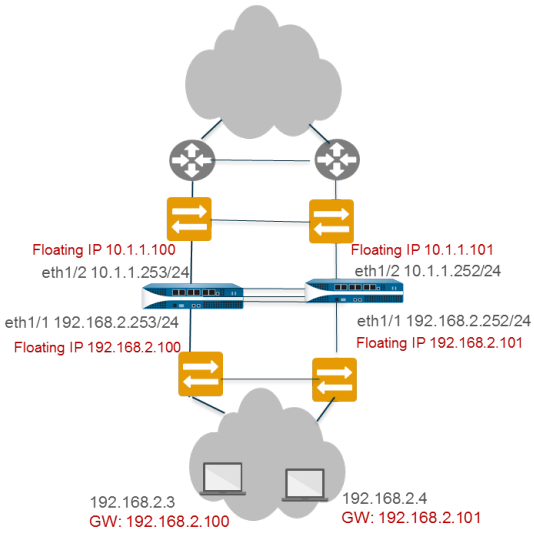
아래 그림과 같이 각 HA 방화벽 인터페이스에는 고유한 IP 주소와 유동 IP 주소가 있습니다. 인터페이스 IP 주소는 방화벽에 로컬로 유지되지만 고정 IP 주소는 방화벽 오류 시 방화벽 간에 이동합니다. 유동 IP 주

 ©2023 Palo Alto Networks, Inc.

소를 기본 게이트웨이로 사용하도록 최종 호스트를 구성하여 두 HA 피어로 트래픽을 로드 밸런싱할 수 있습니다. 외부 로드 밸런서를 사용하여 트래픽을 로드 밸런싱할 수도 있습니다.

링크 또는 방화벽이 실패하거나 경로 모니터링 이벤트로 인해 페일오버가 발생하면 유동 IP 주소와 가상 MAC 주소가 기능 방화벽으로 넘어갑니다. (아래 그림에서 각 방화벽에는 두 개의 유동 IP 주소와 가상 MAC 주소가 있으며 방화벽이 실패하면 모두 이동합니다.) 작동하는 방화벽은 트래픽을 자체적으로 리디렉션하기 위해 유동 IP 주소 및 MAC 주소 소유권 변경을 알리기 위해 연결된 스위치의 MAC 테이블을 업데이트하는 무료 ARP를 보냅니다.

실패한 방화벽이 복구되면 기본적으로 유동 IP 주소와 가상 MAC 주소가 유동 IP 주소가 바인딩된 디바이스 ID [0 또는 1]을 사용하여 방화벽으로 다시 이동합니다. 특히, 실패한 방화벽이 복구된 후 온라인 상태가 됩니다. 현재 능동형 방화벽은 방화벽이 다시 온라인 상태인지 확인하고 처리 중인 유동 IP 주소가 기본적으로 자체 또는 다른 방화벽에 속하는지 확인합니다. 유동 IP 주소가 원래 다른 디바이스 ID에 바인딩된 경우 방화벽은 자동으로 이를 다시 제공합니다. (이 기본 동작에 대한 대안은 사용 사례를 참조하세요. 능동형-기본 방화벽에 연결된 유동 IP 주소로 능동형/능동형 HA를 구성합니다.)




HA 쌍의 각 방화벽은 유동 IP 주소 또는 ARP 부하 공유 IP 주소가 있는 각 인터페이스에 대한 가상 MAC 주소를 생성합니다.

가상 MAC 주소 형식(PA-7000, PA-5200 및 PA-3200 시리즈 방화벽 이외의 방화벽)은 00-1B-17-00-xx-yy이며, 여기서 00-1B-17은 공급업체 ID이고(이 경우 Palo Alto Networks의 경우), 00은 고정되어 있으며, xx는 다음 그림과 같이 Device ID와 Group ID를 나타내고, yy는 Interface ID를 나타냅니다.

| 7 | 6 | 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 |
|---|---|---|---|
| Device-ID | 0 | Group-ID | Interface-ID |

PA-7000, PA-5200 및 PA-3200 시리즈 방화벽의 가상 MAC 주소 형식은 B4-0C-25-xx-xx-xx이며, 여기서 B4-0C-25는 Palo Alto Networks의 공급업체 ID입니다. 다음 24비트는 다음과 같이 디바이스 ID, 그룹 ID 및 인터페이스 ID를 나타냅니다.

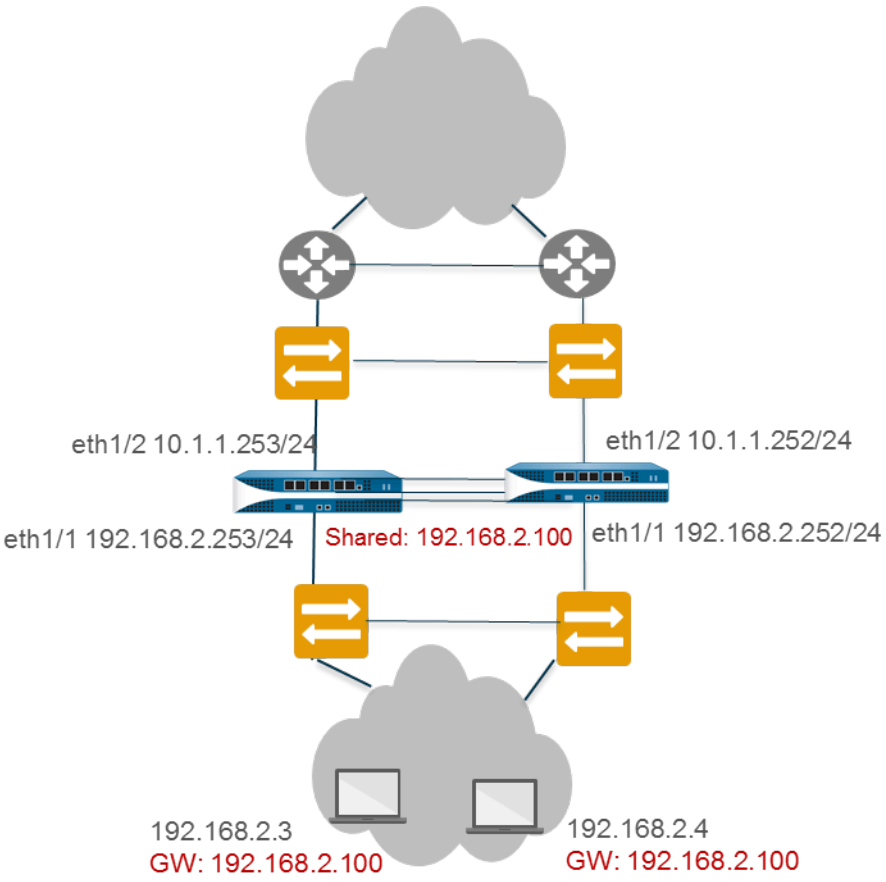

©2023 Palo Alto Networks, Inc.

| 765 | 4 | 321076 | 5432 | 1076543210 |
|---|---|---|---|---|
| 111 | Device-ID | Group-ID | 0000 | Interface-ID |

새로운 능동형 방화벽이 인수되면 연결된 각 인터페이스에서 무상 ARP를 보내 연결된 레이어 2 스위치에 가상 MAC 주소의 새 위치를 알립니다. 유동 IP 주소를 구성하려면 사용 사례를 참조하십시오. 유동 IP 주소를 사용하여 능동형/능동형 HA를 구성합니다.

## ARP 로드 공유

레이어 3 인터페이스 배포 및 활성/활성 HA 구성에서 ARP 로드 공유를 사용하면 방화벽이 IP 주소를 공유하고 게이트웨이 서비스를 제공할 수 있습니다. 방화벽과 최종 호스트 사이에 Layer 3 디바이스가 존재하지 않는 경우, 즉 최종 호스트가 방화벽을 기본 게이트웨이로 사용하는 경우에만 ARP 부하 공유를 사용합니다.



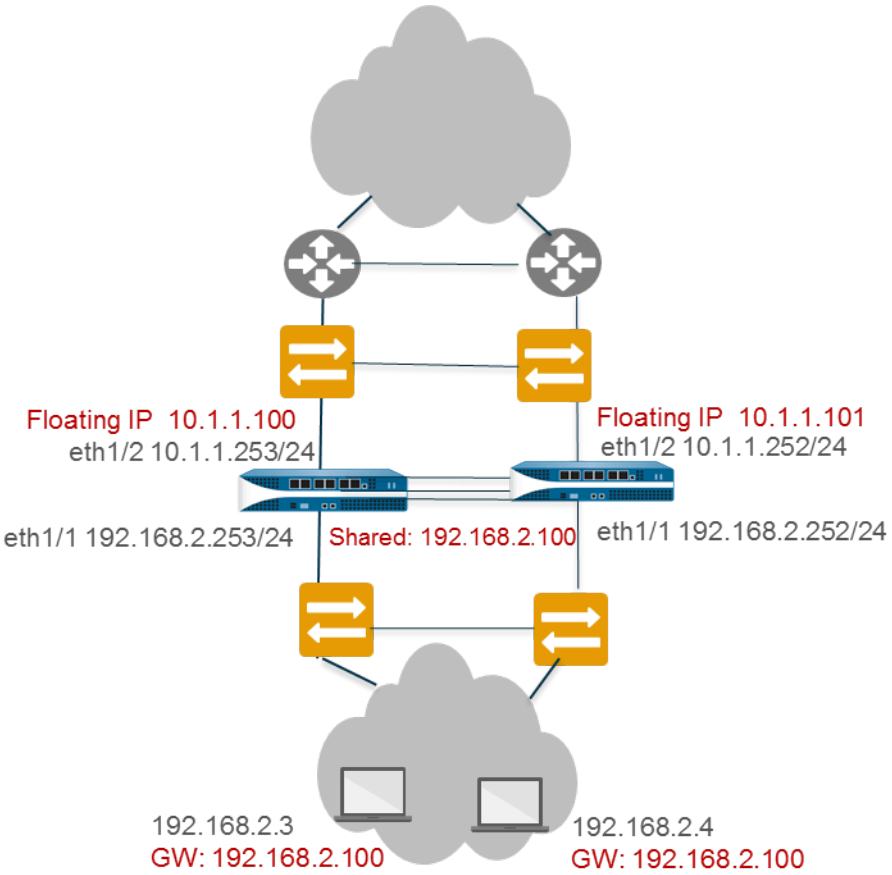

이러한 시나리오에서 모든 호스트는 단일 게이트웨이 IP 주소로 구성됩니다. 방화벽 중 하나는 가상 MAC 주소를 사용하여 게이트웨이 IP 주소에 대한 ARP 요청에 응답합니다. 각 방화벽에는 공유 IP 주소에 대해 생성된 고유한 가상 MAC 주소가 있습니다. ARP 요청에 응답할 방화벽을 제어하는 로드 공유 알고리즘을 구성할 수 있습니다. ARP 요청의 소스 IP 주소의 해시 또는 모듈로를 계산하여 결정됩니다.

최종 호스트는 게이트웨이로부터 ARP 응답을 수신한 후 MAC 주소를 캐시하고 호스트의 모든 트래픽은 ARP 캐시의 수명 동안 가상 MAC 주소로 응답한 방화벽을 통해 라우팅됩니다. ARP 캐시의 수명은 최종 호스트 운영 체제에 따라 다릅니다.


©2023 Palo Alto Networks, Inc.

링크나 방화벽이 실패하면 유동 IP 주소와 가상 MAC 주소가 기능 방화벽으로 넘어갑니다. 기능 방화벽은 연결된 스위치의 MAC 테이블을 업데이트하기 위해 불필요한 ARP를 전송하여 실패한 방화벽에서 자체적으로 트래픽을 리디렉션합니다. 사용 사례 참조: ARP 부하 공유를 사용하여 Active/Active HA를 구성합니다.

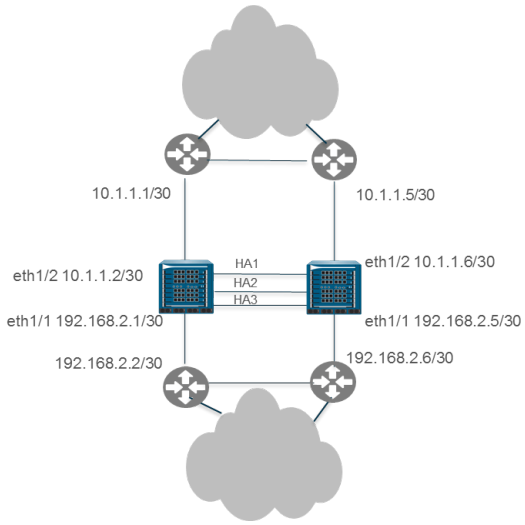
유동 IP 주소를 사용하여 HA 방화벽의 WAN 측에서 인터페이스를 구성하고 ARP 부하 공유를 위해 공유 IP 주소로 HA 방화벽의 LAN 측에서 인터페이스를 구성할 수 있습니다. 예를 들어, 아래 그림은 업스트림 WAN 에지 라우터에 대한 유동 IP 주소와 LAN 세그먼트의 호스트에 대한 ARP 부하 공유 주소를 보여줍니다.




## 경로 기반 중복성

레이어 3 인터페이스 배포 및 능동형/능동형 HA 구성에서 방화벽은 스위치가 아닌 라우터에 연결됩니다. 방화벽은 동적 라우팅 프로토콜을 사용하여 최상의 경로(비대칭 경로)를 결정하고 HA 쌍 간에 공유를 로드합니다. 이러한 시나리오에서는 유동 IP 주소가 필요하지 않습니다. 링크, 모니터링되는 경로 또는 방화벽이 실패하거나 BFD(양방향 포워딩 감지)가 링크 실패를 감지하면 라우팅 프로토콜(RIP, OSPF 또는 BGP)이 작동 중인 방화벽으로의 트래픽 재라우팅을 처리합니다. 고유한 IP 주소로 각 방화벽 인터페이스를 구성합니다. IP 주소는 구성된 방화벽에 로컬로 유지됩니다. 방화벽이 실패하면 디바이스 간에 이동하지 않습니다. 사용 사례 참조: 경로 기반 중복으로 능동형/능동형 HA를 구성합니다.


©2023 Palo Alto Networks, Inc.




# HA 타이머

고가용성(HA) 타이머는 방화벽이 방화벽 장애를 감지하고 페일오버를 트리거하도록 합니다. HA 쌍에 대한 타이머 구성의 복잡성을 줄이기 위해 세 가지 프로파일 중에서 선택할 수 있습니다. **Recommended**, **Aggressive** 및 **Advanced**. 이러한 프로파일은 특정 방화벽 플랫폼에 대한 최적의 HA 타이머 값을 자동으로 채워 HA 배포 속도를 높일 수 있습니다.

일반적인 페일오버 타이머 설정에는 권장 프로파일을 사용하고 보다 빠른 페일오버 타이머 설정에는 **Aggressive** 프로파일을 사용합니다. **Advanced** 프로파일을 사용하면 네트워크 요구 사항에 맞게 타이머 값을 사용자 지정할 수 있습니다.

다음 표는 프로파일에 포함된 각 타이머와 다양한 하드웨어 모델의 현재 사전 설정 값(권장/적극)에 대해 설명합니다. 이 값은 현재 참조용이며 후속 릴리스에서 변경될 수 있습니다.

*HA* 클러스터의 구성원에 영향을 미치는 타이머는 HA 클러스터링 구성에 설명되어 있습니다.

| 타이머 | 설명 | **PA-7000** 시리즈<br>**PA-5200** 시리즈<br>**PA-3200** 시리즈 | **PA-800** 시리즈<br>**PA-220**<br>**VM-Series** | **Panorama** 가상 어플라이언스<br>**Panorama M** 시리즈 |
|---|---|---|---|---|
| 모니터 장애 유지 시간(ms) | 경로 모니터 또는 링크 모니터 실패 후 방화벽이 능동형 상태로 유지되는 인터벌입니다. 이 설정은 인접 디바이스의 간헐적인 플래핑으로 인한 HA 페일오버를 방지하기 위해 권장됩니다. | 0/0 | 0/0 | 0/0 |


©2023 Palo Alto Networks, Inc.

| 타이머 | 설명 | **PA-7000** 시리즈<br>**PA-5200** 시리즈<br>**PA-3200** 시리즈 | **PA-800** 시리즈<br>**PA-220**<br>**VM-Series** | **Panorama** 가상 어플라이언스<br>**Panorama M** 시리즈 |
|---|---|---|---|---|
| 선점 보류 시간(분) | 수동형 또는 능동형-보조 방화벽이 활성 또는 능동형-기본 방화벽으로 인계되기 전에 대기하는 시간입니다. | 1/1 | 1/1 | 1/1 |
| 하트비트 인터벌(ms) | HA 피어가 ICMP(ping) 형식으로 하트비트 메시지를 교환하는 빈도입니다. | 1000/1000 | 2000/1000 | 2000/1000 |
| 프로모션 보류 시간(ms) | 수동형 방화벽(능동형/수동형 모드) 또는 능동형-보조 방화벽(능동형/능동형 모드)이 HA 피어와의 통신이 끊어진 후 능동형 또는 능동형-기본 방화벽으로 인계받기 전에 대기하는 시간입니다. 이 보류 시간은 피어 실패 선언이 이루어진 후에만 시작됩니다. | 2000/500 | 2000/500 | 2000/500 |
| 추가 마스터 보류 시간(ms) | Monitor Fail Hold Up Time(범위는 0~60,000, 기본값은 500)과 동일한 이벤트에 적용되는 시간 인터벌(밀리초)입니다. 추가 시간 인터벌은 능동형/수동형 모드의 능동형 방화벽과 능동형/능동형 모드의 능동형-기본 방화벽에만 적용됩니다. 두 방화벽에서 동일한 링크/경로 모니터 오류가 동시에 발생할 때 페일오버를 피하기 위해 이 타이머를 사용하는 것이 좋습니다. | 500/500 | 500/500 | 7000/5000 |
| 헬로 인터벌(ms) | 다른 방화벽의 HA 기능이 작동하는지 확인하기 | 8000/8000 | 8000/8000 | 8000/8000 |


©2023 Palo Alto Networks, Inc.

| 타이머 | 설명 | **PA-7000** 시리즈<br>**PA-5200** 시리즈<br>**PA-3200** 시리즈 | **PA-800** 시리즈<br>**PA-220**<br>**VM-Series** | **Panorama** 가상 어플라이언스<br>**Panorama M** 시리즈 |
|---|---|---|---|---|
| | 위해 전송되는 헬로 패킷 사이의 인터벌(밀리초)입니다(범위는 8,000 ~ 60,000, 기본값은 8,000). | | | |
| 플랩 맥스 | 다음 중 하나가 발생하면 플랩이 계산됩니다.<br>• 선점 가능 방화벽은 활성화된 후 20분 이내에 활성 상태를 벗어납니다.<br>• 링크 또는 경로가 작동한 후 10분 동안 유지되지 않습니다.<br>실패한 선점 또는 비기능 루프의 경우 이 값은 방화벽이 일시 중단되기 전에 허용되는 최대 플랩 수를 나타냅니다(범위 0~16, 기본값은 3). | 3/3 | 3/3 | 해당 없음 |

## 세션 소유자

HA 액티브/액티브 구성에서는 두 방화벽이 동시에 활성화되므로 두 방화벽 간에 패킷을 분산할 수 있습니다. 이러한 배포를 위해서는 방화벽이 세션 소유권과 세션 설정이라는 두 가지 기능을 수행해야 합니다. 일반적으로 쌍의 각 방화벽은 이러한 기능 중 하나를 수행하므로 비대칭으로 라우팅된 환경에서 발생할 수 있는 경쟁 조건을 방지합니다.

세션의 세션 소유자는 최종 호스트에서 새 세션의 첫 번째 패킷을 수신하는 방화벽 또는 능동형-기본 상태의 방화벽(기본 디바이스)으로 구성합니다. 기본 디바이스가 구성되어 있지만 첫 번째 패킷을 수신하는 방화벽이 활성-기본 상태가 아닌 경우 방화벽은 HA3 링크를 통해 피어 방화벽(세션 소유자)에 패킷을 포워딩합니다.

세션 소유자는 App-ID, Content-ID 및 세션에 대한 위협 검사와 같은 모든 레이어 7 처리를 수행합니다. 세션 소유자는 세션에 대한 모든 트래픽 로그도 생성합니다.

세션 소유자가 실패하면 피어 방화벽이 세션 소유자가 됩니다. 기존 세션은 작동 중인 방화벽으로 페일오버되며 해당 세션에 대해 레이어 7 처리를 사용할 수 없습니다. 방화벽이 장애로부터 복구되면 기본적으로 장애 이전에 소유한 모든 세션이 원래 방화벽으로 되돌아갑니다. 레이어 7 처리는 다시 시작되지 않습니다.


©2023 Palo Alto Networks, Inc.

세션 소유권을 기본 디바이스로 구성하면 세션 설정도 기본 디바이스로 기본 설정됩니다.

*Palo Alto Networks*는 특정 사용 사례에서 달리 명시하지 않는 한 세션 소유자를 첫 번째 패킷으로 설정하고 세션 설정을 *IP Modulo*로 설정하는 것이 좋습니다. 세션 소유자를 *First Packet*으로 설정하면 *HA3* 링크 전체의 트래픽이 줄어들고 피어 간에 데이터플레인 로드를 분산하는 데 도움이 됩니다.

세션 소유자 및 세션 설정을 기본 디바이스로 설정하면 능동형-기본 방화벽이 모든 트래픽 처리를 수행합니다. 다음 이유 중 하나로 이 설정을 구성할 수 있습니다.

- 방화벽 간에 패킷 처리가 분리되지 않도록 로그와 *PCAP*를 캡처하고 문제를 해결하고 있습니다.
- 능동형/능동형 *HA* 쌍이 능동형/수동형 *HA* 페어처럼 작동하도록 할 수 있습니다. 사용 사례: 능동형-기본 방화벽에 바인딩된 부동 IP 주소를 사용하여 능동형/능동형 HA 구성을(를) 참조하십시오.

## 세션 설정

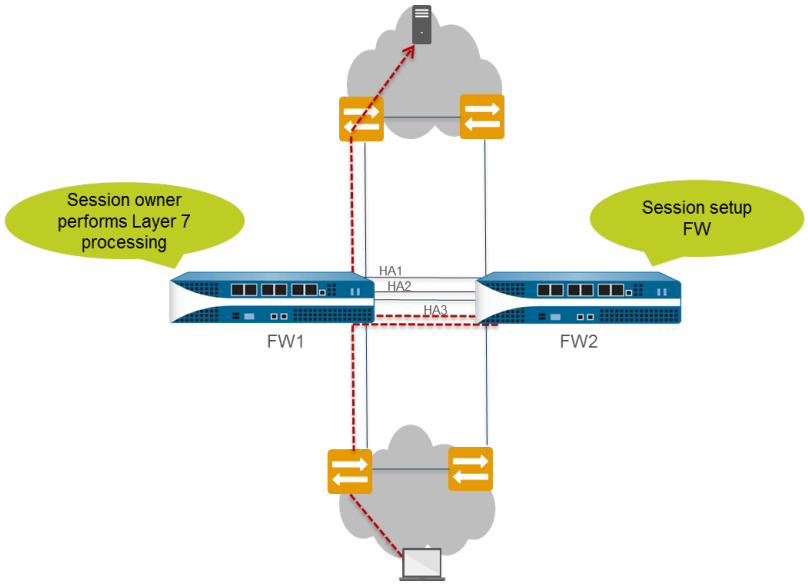
세션 설정 방화벽은 새 세션을 설정하는 데 필요한 레이어 2 ~ 레이어 4 처리를 수행합니다. 세션 설정 방화벽도 세션 소유자의 NAT 풀을 사용하여 NAT를 수행합니다. 다음 세션 설정 로드 공유 옵션 중 하나를 선택하여 능동형/능동형 구성에서 세션 설정 방화벽을 결정합니다.

| 세션 설정 옵션 | 설명 |
|---|---|
| **IP Modulo** | 방화벽은 소스 IP 주소의 패리티를 기반으로 세션 설정 로드를 분산합니다. 이것은 세션 설정을 공유하는 결정적인 방법입니다. |
| **IP** 해시 | 방화벽은 소스 및 대상 IP 주소의 해시를 사용하여 세션 설정 책임을 분산합니다. |
| 기본 디바이스 | 활성-기본 방화벽은 항상 세션을 설정합니다. 하나의 방화벽만 모든 세션 설정 책임을 수행합니다. |
| 첫 번째 패킷 | 세션의 첫 번째 패킷을 수신한 방화벽은 세션 설정을 수행합니다. |

- 세션 소유자와 세션 설정 책임을 로드 공유하려면 세션 소유자를 *First Packet*으로 설정하고 세션 설정을 *IP* 모듈로로 설정합니다. 권장되는 설정입니다.
- 문제 해결을 수행하거나 로그 또는 *pcap*을 캡처하거나 능동형/능동형 *HA* 쌍이 능동형/수동형 *HA* 쌍처럼 작동하도록 하려면 세션 소유자와 세션 설정을 모두 기본 디바이스로 설정하여 능동형-기본 디바이스가 모든 트래픽 처리를 수행합니다. 사용 사례 참조: 활성-기본 방화벽에 바인딩된 유동 IP 주소를 사용하여 능동형/능동형 HA를 구성합니다.

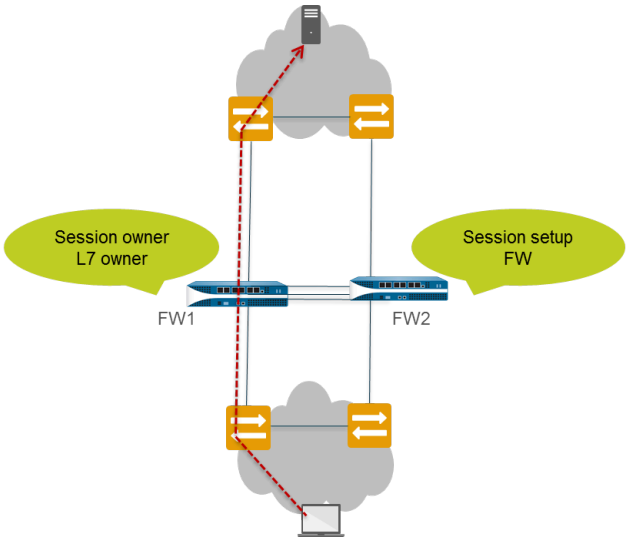

©2023 Palo Alto Networks, Inc.

방화벽은 HA3 링크를 사용하여 필요한 경우 세션 설정을 위해 피어에 패킷을 보냅니다. 다음 그림과 텍스트는 방화벽 FW1이 새 세션에 대해 수신하는 패킷의 경로를 설명합니다. 빨간색 점선은 HA3 링크를 통해 FW1이 패킷을 FW2로 포워딩하고 FW2가 패킷을 다시 FW1로 포워딩함을 나타냅니다.




- 최종 호스트는 FW1에 패킷을 보냅니다.
- FW1은 패킷의 내용을 검사하여 기존 세션과 일치시킵니다. 세션 일치가 없으면 FW1은 새 세션에 대한 첫 번째 패킷을 수신한 것으로 판단하여 세션 소유자가 됩니다(세션 소유자 선택이 첫 번째 패킷으로 설정되어 있다고 가정).
- FW1은 구성된 세션 설정 로드 공유 옵션을 사용하여 세션 설정 방화벽을 식별합니다. 이 예에서 FW2는 세션 설정을 수행하도록 구성됩니다.
- FW1은 HA3 링크를 사용하여 첫 번째 패킷을 FW2로 보냅니다.
- FW2는 세션을 설정하고 레이어 7 처리를 위해 패킷을 FW1에 반환합니다(있는 경우).
- 그런 다음 FW1은 패킷을 이그레스(egress) 인터페이스에서 대상으로 포워딩합니다.

다음 그림과 텍스트는 기존 세션과 일치하는 패킷의 경로를 설명합니다.





©2023 Palo Alto Networks, Inc.

- 최종 호스트는 FW1에 패킷을 보냅니다.
- FW1은 패킷의 내용을 검사하여 기존 세션과 일치시킵니다. 세션이 기존 세션과 일치하면 FW1이 패킷을 처리하고 패킷을 이그레스(egress) 인터페이스에서 대상으로 보냅니다.

## 활성/활성 HA 모드의 NAT

능동형/능동형 HA 구성:

- 각 동적 IP(DIP) NAT 규칙과 동적 IP 및 포트(DIPP) NAT 규칙을 디바이스 ID 0 또는 디바이스 ID 1에 바인딩해야 합니다.
- 각 고정 NAT 규칙을 디바이스 ID 0, 디바이스 ID 1, 두 디바이스 ID 모두 또는 능동형-기본 상태의 방화벽에 바인딩해야 합니다.

따라서 방화벽 중 하나가 새 세션을 만들 때 디바이스 ID **0** 또는 디바이스 ID **1** 바인딩은 방화벽과 일치하는 NAT 규칙을 결정합니다. 디바이스 바인딩은 일치를 생성하기 위해 세션 소유자 방화벽을 포함해야 합니다.

세션 설정 방화벽은 NAT 정책 일치를 수행하지만 NAT 규칙은 세션 소유자를 기준으로 평가됩니다. 즉, 세션 소유자 방화벽에 바인딩된 NAT 규칙에 따라 세션이 변환됩니다. NAT 정책 일치를 수행하는 동안 방화벽은 세션 소유자 방화벽에 바인딩되지 않은 모든 NAT 규칙을 건너뜁니다.

예를 들어 디바이스 ID가 1인 방화벽이 세션 소유자 및 세션 설정 방화벽이라고 가정합니다. 디바이스 ID가 1인 방화벽이 세션을 NAT 규칙과 일치시키려고 할 때 디바이스 ID 0에 바인딩된 모든 규칙을 건너뜁니다. 방화벽은 세션 소유자와 NAT 규칙의 디바이스 ID가 일치하는 경우에만 NAT 변환을 수행합니다.

피어 방화벽이 변환에 다른 IP 주소를 사용할 때 일반적으로 디바이스별 NAT 규칙을 생성합니다.

피어 방화벽 중 하나가 실패하면 활성 방화벽은 NAT 트래픽을 포함하여 실패한 방화벽에서 동기화된 세션에 대한 트래픽을 계속 처리합니다. 소스 NAT 구성에서 하나의 방화벽이 실패하는 경우:

- NAT 규칙의 변환된 IP 주소로 사용되는 유동 IP 주소는 남아 있는 방화벽으로 전달됩니다. 따라서 페일오버되는 기존 세션은 여전히 이 IP 주소를 사용합니다.
- 모든 새 세션은 살아남은 방화벽이 자연적으로 소유하는 디바이스별 NAT 규칙을 사용합니다. 즉, 살아남은 방화벽은 디바이스 ID와 일치하는 NAT 규칙만 사용하여 새 세션을 변환합니다. 실패한 디바이스 ID에 바인딩된 모든 NAT 규칙을 무시합니다.

NAT가 있는 능동형/능동형 HA의 예는 다음을 참조하십시오.

- 사용 사례: 유동 IP 주소를 사용하여 소스 DIPP NAT로 능동형/능동형 HA 구성
- 사용 사례: 능동형/능동형 HA 방화벽에 대해 별도의 소스 NAT IP 주소 풀 구성
- 사용 사례: 대상 NAT를 사용하여 ARP 로드 공유를 위한 능동형/능동형 HA 구성
- 사용 사례: 레이어 3에서 대상 NAT를 사용하여 ARP 로드 공유에 대한 능동형/능동형 HA 구성

## 활성/활성 HA 모드의 ECMP

능동형/능동형 HA 피어가 실패하면 해당 세션은 새로운 능동형-기본 방화벽으로 전송되며, 이 방화벽은 실패한 방화벽에서 사용하던 것과 동일한 이그레스(egress) 인터페이스를 사용하려고 시도합니다. 방화벽이 ECMP 경로 사이에서 해당 인터페이스를 발견하면 전송된 세션은 동일한 이그레스(egress) 인터페이스와 경로를 사용합니다. 이 동작은 사용 중인 ECMP 알고리즘에 관계없이 발생합니다. 동일한 인터페이스를 사용하는 것이 바람직합니다.


©2023 Palo Alto Networks, Inc.

ECMP 경로가 원래 이그레스(egress) 인터페이스와 일치하지 않는 경우에만 활성 기본 방화벽이 새 ECMP 경로를 선택합니다.

능동형/능동형 피어에서 동일한 인터페이스를 구성하지 않은 경우 페일오버 시 능동형-프라이머리 방화벽이 FIB 테이블에서 다음으로 최상의 경로를 선택합니다. 따라서 ECMP 알고리즘에 따라 기존 세션이 배포되지 않을 수 있습니다.


©2023 Palo Alto Networks, Inc.

# 활성/패시브 HA 설정


- 활성/패시브 HA의 전제 조건
- 활성/패시브 HA에 대한 구성 지침
- 활성/패시브 HA 구성
- HA 페일오버 조건 정의
- 장애 조치 확인


## 활성/패시브 HA의 전제 조건

Palo Alto 네트워크 방화벽에서 고가용성을 설정하려면 다음 요구 사항을 충족하는 방화벽 쌍이 필요합니다.

- 동일한 모델 - 쌍의 두 방화벽은 모두 동일한 하드웨어 모델 또는 가상 머신 모델이어야 합니다.
- 동일한 **PAN-OS** 버전 - 두 방화벽 모두 동일한 PAN-OS 버전을 실행해야 하며 애플리케이션, URL 및 위협 데이터베이스에서 각각 최신 상태여야 합니다.
- 동일한 다중 가상 시스템 기능 - 두 방화벽 모두 다중 가상 시스템 기능을 활성화하거나 비활성화해야 합니다. 활성화된 경우 각 방화벽에는 고유한 다중 가상 시스템 라이선스가 필요합니다.
- 동일한 유형의 인터페이스 - 전용 HA 링크 또는 인터페이스 유형 HA로 설정된 대역 내 포트와 관리 포트의 조합입니다.
  - HA 피어 간의 HA1(제어) 연결에 대한 IP 주소를 결정합니다. 두 피어의 HA1 IP 주소는 직접 연결되거나 동일한 스위치에 연결된 경우 동일한 서브넷에 있어야 합니다.

    전용 HA 포트가 없는 방화벽의 경우 제어 연결을 위해 관리 포트를 사용할 수 있습니다. 관리 포트를 사용하면 두 방화벽의 관리 평면 간에 직접 통신 링크가 제공됩니다. 그러나 관리 포트는 피어 간에 직접 케이블로 연결되지 않으므로 네트워크를 통해 이 두 인터페이스를 연결하는 경로가 있는지 확인하십시오.
  - HA2(데이터) 연결을 위한 전송 방법으로 레이어 3을 사용하는 경우 HA2 링크의 IP 주소를 결정합니다. HA2 연결이 라우팅된 네트워크를 통해 통신해야 하는 경우에만 레이어 3을 사용하십시오. HA2 링크의 IP 서브넷은 HA1 링크의 IP 서브넷 또는 방화벽의 데이터 포트에 할당된 다른 서브넷과 겹치지 않아야 합니다.
- 동일한 라이선스 세트 - 라이선스는 각 방화벽에 고유하며 방화벽 간에 공유할 수 없습니다. 따라서 두 방화벽에 동일하게 라이선스를 부여해야 합니다. 두 방화벽에 동일한 라이선스 세트가 없으면 구성 정보를 동기화하고 원활한 페일오버를 위한 패리티를 유지할 수 없습니다.



기존 방화벽이 있고 ***HA*** 목적으로 새 방화벽을 추가하려는 경우 새 방화벽에 기존 구성이 있는 경우 새 방화벽에서 방화벽을 공장 기본 설정으로 재설정하는 것이 가장 좋습니다. 이렇게 하면 새 방화벽이 깨끗한 구성을 갖게 됩니다. ***HA***를 구성한 후 기본 방화벽의 구성을 새로 도입된 방화벽과 깨끗한 구성으로 동기화합니다.


©2023 Palo Alto Networks, Inc.

# 활성/패시브 HA에 대한 구성 지침

HA에서 활성(PeerA) 패시브(PeerB) 쌍을 설정하려면 방화벽과 각 방화벽에서 일부 독립적으로(일치하지 않는) 모두에서 동일한 몇 가지 옵션을 구성해야합니다. 이러한 HA 설정은 방화벽 간에 동기화되지 않습니다. 동기화되지 않은 내용에 대한 자세한 내용은 참조: HA 동기화을(를) 참조하십시오.

다음 체크리스트는 두 방화벽에서 동일하게 구성해야 하는 설정을 자세히 설명합니다.

- 두 방화벽 모두에서 HA를 사용하도록 설정해야 합니다.
- 두 방화벽모두에서 동일한 그룹 ID 값을 구성해야 합니다. 방화벽은 그룹 ID 값을 사용하여 구성된 모든 인터페이스에 대한 가상 MAC 주소를 생성합니다. 가상 MAC 주소에 대한 정보는 부동 IP 주소 및 가상 MAC 주소를 참조하십시오. 새 활성형 방화벽이 인계되면 연결된 각 인터페이스에서 Gratuitous ARP 메시지를 보내 가상 MAC 주소의 새 위치의 연결된 레이어 2 스위치를 알립니다.
- 대역 내 포트를 HA 링크로 사용하는 경우 HA1 및 HA2 링크의 인터페이스를 HA 유형 HA로 설정해야 합니다.
- 두 방화벽모두에서 HA 모드를 활성 패시브로 설정합니다.
- 필요한 경우 두 방화벽 모두에서 선점을 사용하도록 설정합니다. 그러나 디바이스 우선 순위 값은 동일해서는 안 됩니다.
- 필요한 경우 두 방화벽에서 HA1 링크(HA 피어 간의 통신용)에서 암호화를 구성합니다.


©2023 Palo Alto Networks, Inc.

- 사용 중인 HA1 및 HA1 백업 포트의 조합을 기반으로 다음 권장 사항을 사용하여 하트비트 백업을 사용하도록 설정해야 하는지의 여부를 결정합니다.

  > ***HA** 기능(**HA1** 및 **HA1** 백업)은 **DHCP** 주소 지정(**DHCP** 클라이언트로 설정된 **IP** 유형)을 위해 구성된 경우 관리 인터페이스에서 지원되지 않습니다. 예외는 관리 인터페이스가 **DHCP** 클라이언트로 구성되고 **HA1** 및 **HA1** 백업 링크를 지원하는 **AWS** 및 **Azure**입니다.*

  - HA1: 전용 HA1 포트

    HA1 백업: 전용 HA1 포트

    **권장:** 하트비트 백업 활성화
  - HA1: 전용 HA1 포트

    HA1 백업: 밴드 내 포트

    **권장:** 하트비트 백업 활성화
  - HA1: 전용 HA1 포트

    HA1 백업: 관리 포트

    **권장:** 하트비트 백업을 활성화하지 마십시오.
  - HA1: 밴드 내 포트

    HA1 백업: 밴드 내 포트

    **권장:** 하트비트 백업 활성화
  - HA1: 관리 포트

    HA1 백업: 밴드 내 포트

    **권장:** 하트비트 백업을 활성화하지 마십시오.

다음 표에는 각 방화벽에서 독립적으로 구성해야 하는 HA 설정이 나열됩니다. 피어 간에 자동으로 동기화되지 않는 다른 구성 설정에 대한 자세한 내용은 참조: HA 동기화을(를) 참조하십시오.

| 독립 구성 설정 | PeerA | PeerB |
|---|---|---|
| 제어 링크 | 이 방화벽(PeerA)에서 구성된 HA1 링크의 IP 주소입니다. | 이 방화벽(PeerB)에서 구성된 HA1 링크의 IP 주소입니다. |
| | 전용 HA 포트가 없는 방화벽의 경우 제어 링크에 관리 포트 IP 주소를 사용합니다. | |
| 데이터 링크<br><br>데이터 링크 정보는 HA를 사용하도록 설정하고 방화벽 간에 제어 링크가 설 | 기본적으로 HA2 링크는 이더넷/레이어 2를 사용합니다.<br><br>레이어 3 연결을 사용하는 경우 이 방화벽(PeerA)의 데이터 링크에 대한 IP 주소를 구성합니다. | 기본적으로 HA2 링크는 이더넷/레이어 2를 사용합니다.<br><br>레이어 3 연결을 사용하는 경우 이 방화벽(PeerB)의 데이터 링크에 대한 IP 주소를 구성합니다. |

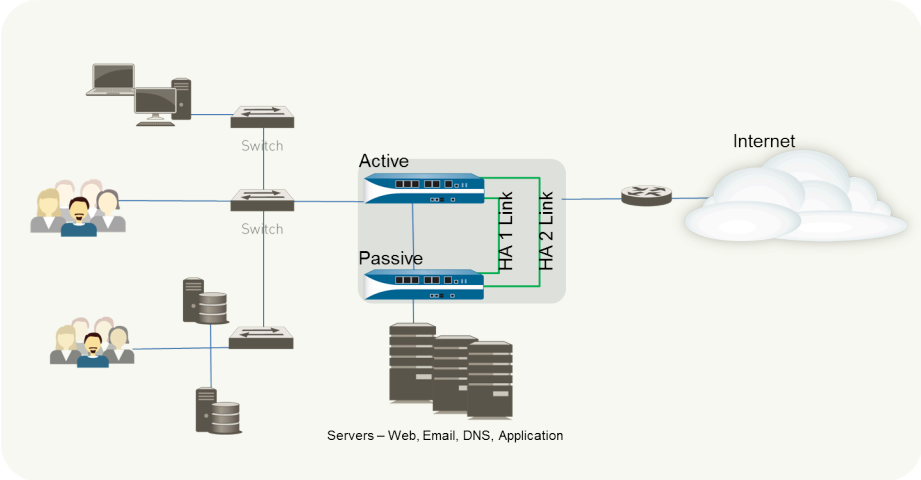

©2023 Palo Alto Networks, Inc.

| 독립 구성 설정 | PeerA | PeerB |
| --- | --- | --- |
| 정된 후 방화벽 간에 동기화됩니다. | | |
| 디바이스 우선 순위(선취점을 사용하도록 설정된 경우 필수) | 활성을 만들려는 방화벽은 피어보다 숫자 값이 낮아야 합니다. 따라서 피어 A가 활성형 방화벽으로 작동하는 경우 기본 값을 100으로 유지하고 PeerB에서 값을 증가시키면 됩니다.<br>방화벽에 디바이스 우선 순위 값이 동일한 경우 HA1의 MAC 주소를 타이 브레이커로 사용합니다. | PeerB가 수동적인 경우 디바이스 우선 순위 값을 PeerA의 설정보다 큰 숫자로 설정합니다. 예를 들어 값을 110으로 설정합니다. |
| 링크 모니터링-이 방화벽의 중요한 트래픽을 처리하고 오류 조건을 정의하는 하나 이상의 물리적 인터페이스를 모니터링합니다. | 페일오버를 트리거하기 위해 오류 조건(전부 또는 모든)을 모니터링하고 정의하려는 방화벽의 물리적 인터페이스를 선택합니다. | 이 방화벽에서 모니터링하려는 유사한 물리적 인터페이스 집합을 선택한 다음 페일오버를 트리거하기 위해 오류 조건(전부 또는 모든)을 정의합니다. |
| 경로 모니터링-방화벽이 ICMP 핑(ping)을 사용하여 응답성을 확인할 수 있는 하나 이상의 대상 IP 주소를 모니터링합니다. | 실패 조건(전부 또는 모든), 핑(ping) 간격 및 핑(ping) 수를 정의합니다. 이는 상호 연결된 다른 네트워킹 디바이스의 가용성을 모니터링하는 데 특히 유용합니다. 예를 들어 서버에 연결하는 라우터의 가용성, 서버 자체에 대한 연결 또는 트래픽 플로우에 있는 다른 중요한 디바이스를 모니터링합니다.<br>모니터링 중인 노드/디바이스가 특히 로드 중에 있을 때 경로 모니터링 실패를 일으키고 페일오버를 트리거할 수 있으므로 응답하지 않을 수 있는지 확인합니다. | PeerB의 페일오버 트리거를 결정하기 위해 모니터링할 수 있는 유사한 디바이스 또는 대상 IP 주소를 선택합니다. 실패 조건(전부 또는 모든), 핑(ping) 간격 및 핑(ping) 수를 정의합니다. |

## 활성/패시브 HA 구성

다음 예에서 토폴로지에 설명된 대로 능동형/수동형 배포에서 방화벽 쌍을 구성하는 방법을 보여 줍니다.


©2023 Palo Alto Networks, Inc.




능동형/수동형 HA 쌍을 구성하려면 먼저 첫 번째 방화벽에서 다음 워크플로를 완료한 다음 두 번째 방화벽에서 단계를 반복합니다.

**STEP 1 |** HA 포트를 연결하여 방화벽 간의 물리적 연결을 설정합니다.

- 전용 HA 포트가 있는 방화벽의 경우 이더넷 케이블을 사용하여 피어의 전용 HA1 포트와 HA2 포트를 연결합니다. 피어가 서로 직접 연결된 경우 크로스오버 케이블을 사용하십시오.
- 전용 HA 포트가 없는 방화벽의 경우 HA2 링크와 백업 HA1 링크에 대해 두 개의 데이터 인터페이스를 선택합니다. 그런 다음 이더넷 케이블을 사용하여 두 방화벽에서 이러한 대역 내 HA 인터페이스를 연결합니다.

HA1 링크에 관리 포트를 사용하고 관리 포트가 네트워크를 통해 서로 연결할 수 있는지 확인하십시오.

**STEP 2 |** 관리 포트에서 핑(ping)을 활성화합니다.

핑(ping)을 활성화하면 관리 포트가 하트비트 백업 정보를 교환할 수 있습니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 편집합니다.
2. 인터페이스에서 허용되는 서비스로 핑**(ping)**을 선택합니다.

**STEP 3 |** 방화벽에 전용 HA 포트가 없는 경우 데이터 포트를 HA 포트로 작동하도록 설정합니다.

전용 HA 포트가 있는 방화벽의 경우 다음 단계를 계속합니다.

1. 네트워크 > 인터페이스를 선택합니다.
2. 사용하려는 포트에서 링크가 작동하는지 확인하십시오.
3. 인터페이스를 선택한 다음 인터페이스 유형을 **HA**로 설정합니다.
4. 링크 속도 및 링크 듀플렉스 설정을 적절하게 설정합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** HA 모드 및 그룹 ID를 설정합니다.

1. 디바이스 > 고가용성 > 일반을 선택한 다음 설치 섹션을 편집합니다.
2. 그룹 **ID**와 쌍에 대한 설명을 선택적으로 설정합니다. 그룹 ID는 네트워크의 각 HA 쌍을 고유하게 식별합니다. 동일한 브로드캐스트 도메인을 공유하는 HA 쌍이 여러 개 있는 경우 각 쌍에 대해 고유한 그룹 ID를 설정해야 합니다.
3. 모드를 능동형 수동으로 설정합니다.

**STEP 5 |** 제어 링크 연결을 설정합니다.

이 예제에서는 인터페이스 유형 HA로 설정된 대역 내 포트를 보여 줍니다.

관리 포트를 제어 링크로 사용하는 방화벽의 경우 IP 주소 정보가 자동으로 미리 채워집니다.

1. 디바이스 > 고가용성 > 일반에서 제어 링크(HA1) 섹션을 편집합니다.
2. HA1 링크로 사용하기 위해 케이블을 연결한 포트를 선택합니다.
3. **IPv4/IPv6** 주소 및 넷마스크를 설정합니다.

   HA1 인터페이스가 별도의 서브넷에 있는 경우 게이트웨이의 IP 주소를 입력합니다. 방화벽이 직접 연결되어 있거나 동일한 VLAN에 있는 경우 게이트웨이 주소를 추가하지 마십시오.

**STEP 6 |** (선택 사항) 제어 링크 연결에 대한 암호화를 사용하도록 설정합니다.

이것은 일반적으로 두 개의 방화벽이 직접 연결되지 않은 경우, 즉 포트가 스위치나 라우터에 연결된 경우 링크를 보호하는 데 사용됩니다.

1. 한 방화벽에서 HA 키를 내보내고 피어 방화벽으로 가져옵니다.
   1. 디바이스 > 인증서 관리 > 인증서를 선택합니다.
   2. **HA** 키 내보내기를 선택합니다. 피어가 액세스할 수 있는 네트워크 위치에 HA 키를 저장합니다.
   3. 피어 방화벽에서 디바이스 > 인증서 관리 > 인증서를 선택한 다음 **HA** 키 가져오기를 선택하여 키를 저장한 위치를 찾아 피어로 가져옵니다.
   4. 두 번째 방화벽에서 이 프로세스를 반복하여 두 디바이스에서 HA 키를 교환합니다.
2. 디바이스 > 고가용성 > 일반을 선택한 다음 제어 링크(HA1) 섹션을 편집합니다.
3. 암호화 활성화를 선택합니다.

   암호화를 사용하도록 설정하면 ***HA*** 방화벽 구성을 완료한 후 HA1 SSH 키 새로 고침 및 키 옵션 구성을(를) 수행할 수 있습니다.

**STEP 7 |** 백업 제어 링크 연결을 설정합니다.

1. 디바이스 > 고가용성 > 일반에서 제어 링크(HA1 백업) 섹션을 편집합니다.
2. HA1 백업 인터페이스를 선택한 다음 **IPv4/IPv6** 주소 및 넷마스크를 설정합니다.

   *PA-3200* 시리즈 방화벽은 ***HA1*** 백업 제어 링크에 대해 ***IPv6*** 주소를 지원하지 않으며 ***IPv4*** 주소를 사용합니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 방화벽 간의 데이터 링크 연결(HA2) 및 백업 HA2 연결을 설정합니다.

1. 디바이스 > 고가용성 > 일반에서 데이터 링크(HA2) 섹션을 편집합니다.
2. 데이터 링크 연결에 사용할 포트를 선택합니다.
3. 전송 방법을 선택합니다. 기본값은 이더넷이며 HA 쌍이 직접 연결되거나 스위치를 통해 연결될 때 작동합니다. 네트워크를 통해 데이터 링크 트래픽을 라우팅해야 하는 경우 전송 모드로 **IP** 또는 **UDP**를 선택합니다.
4. IP 또는 UDP를 전송 방법으로 사용하는 경우 **IPv4/IPv6** 주소와 넷마스크를 입력합니다.
5. 세션 동기화 활성화가 선택되었는지 확인합니다.
6. HA 피어 간의 HA2 데이터 링크에 대한 모니터링을 활성화하려면 **HA2** 연결 유지를 선택합니다. 설정된 임계값(기본값은 10000ms)에 따라 장애가 발생하면 정의된 조치가 발생합니다. 능동형/수동형 구성의 경우 HA2 유지 오류가 발생할 때 중요한 시스템 로그 메시지가 생성됩니다.

   두 방화벽 에서 *HA2* 유지 방지 옵션을 구성하거나 *HA* 쌍의 방화벽을 하나만 구성할 수 있습니다. 한 방화벽에서만 옵션을 사용하도록 설정하면 해당 방화벽만 활성화된 상태로 메시지를 보냅니다. 오류가 발생하면 다른 방화벽에 알림이 전송됩니다.
7. 데이터 링크**(HA2** 백업**)** 섹션을 편집하고 인터페이스를 선택한 다음 **IPv4/IPv6** 주소 및 넷마스크를 추가합니다.

**STEP 9 |** 제어 링크가 전용 HA 포트 또는 대역 내 포트를 사용하는 경우 하트비트 백업을 활성화하십시오.

컨트롤 링크에 관리 포트를 사용하는 경우 하트비트 백업을 활성화할 필요가 없습니다.

1. 디바이스 > 고가용성 > 일반에서 일렉션(Election) 설정을 편집합니다.
2. 하트비트 백업을 선택합니다.

   방화벽 간에 하트비트가 전송되도록 하려면 두 피어의 관리 포트가 서로 라우팅할 수 있는지 확인해야 합니다.

   심장 박동 백업을 사용하면 분할 뇌 상황을 방지 할 수 있습니다. 분할 뇌는 *HA1* 링크가 다운되면 방화벽이 심장 박동을 놓치게 할 때 발생합니다. 이러한 상황에서 각 피어는 상대방이 다운되어 실행 중인 서비스를 시작하려고 시도하여 스플릿 브레인*(split brain)*을 유발한다고 믿습니다. 하트비트 백업 링크가 활성화되면 중복된 하트비트와 인사 메시지가 관리 포트를 통해 전송되므로 스플릿 브레인*(split brain)*이 방지됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 10 |** 디바이스 우선 순위를 설정하고 선점을 사용하도록 설정합니다.

이 설정은 특정 방화벽이 기본 활성형 방화벽인지 확인해야 만 필요합니다. 자세한 내용은 디바이스 우선 순위 및 선점을 참조하십시오.

1. 디바이스 > 고가용성 > 일반에서 일렉션(Election) 설정을 편집합니다.
2. 디바이스 우선 순위에서 숫자 값을 설정합니다. 더 높은 우선 순위를 할당하려는 방화벽에서 더 낮은 숫자 값을 설정해야 합니다.

   두 방화벽 모두 디바이스 우선 순위 값이 같으면 ***HA1*** 제어 링크에서 ***MAC*** 주소가 가장 낮은 방화벽이 활성형 방화벽이 됩니다.
3. 선점을 선택합니다.

   능동형 방화벽과 수동형 방화벽 모두에서 선제적으로 사용하도록 설정해야 합니다.

**STEP 11 |** (선택 사항) HA 타이머를 수정합니다.

기본적으로 HA 타이머 프로파일은 권장 프로파일로 설정되며 대부분의 HA 배포에 적합합니다.

1. 디바이스 > 고가용성 > 일반에서 일렉션(Election) 설정을 편집합니다.
2. 장애 조치를 더 빠르게 트리거하려면 적극적 프로파일을 선택합니다. 고급을 선택하여 설정에서 장애 조치를 트리거하기 위한 사용자 정의 값을 정의합니다.

   프로파일에 포함된 개별 타이머의 사전 설정 값을 보려면 고급을 선택한 다음 권장 로드 또는 적극적 로드를 클릭합니다. 하드웨어 모델에 대한 사전 설정 값이 화면에 표시됩니다.

**STEP 12 |** (선택 사항) 수동 방화벽에서 HA 포트의 링크 상태를 수정합니다.

수동형 링크 상태는 기본적으로 종료로 되어 있습니다. ***HA***를 활성화하면 활성형 방화벽의 ***HA*** 포트에 대한 링크 상태가 녹색이고 수동형 방화벽의 링크 상태가 다운되고 빨간색으로 표시됩니다.

링크 상태를 자동으로 설정하면 패시브 방화벽이 페일오버 발생 시 인계하는 데 걸리는 시간을 줄이고 링크 상태를 모니터링할 수 있습니다.

수동형 방화벽의 링크 상태를 유지하고 물리적 인터페이스에 케이블 상태를 반영 하도록 하려면 다음을 따릅니다.

1. 디바이스 > 고가용성 > 일반에서 활성 수동 설정을 편집합니다.
2. 수동형 링크 상태를 자동으로 설정합니다.

   자동 옵션은 패시브 방화벽이 페일오버 발생 시 인계하는 데 걸리는 시간을 줄입니다.

   인터페이스는 녹색(케이블 구성 및 상승)을 표시하지만 페일오버가 트리거될 때까지 모든 트래픽을 계속 삭제합니다.

   수동형 링크 상태를 수정할 때 인접한 디바이스가 방화벽의 링크 상태에만 따라 트래픽을 수동형 방화벽으로 포워딩하지 않는지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 13 |** HA를 활성화합니다.

1. 디바이스 > 고가용성 > 일반을 선택한 다음 설치 섹션을 편집합니다.
2. **HA** 활성화를 선택합니다.
3. 구성 동기화 활성화를 선택합니다. 이 설정을 사용하면 활성 방화벽과 수동 방화벽 간의 구성 설정을 동기화할 수 있습니다.
4. 피어 **HA1 IP** 주소에서 피어의 컨트롤 링크에 할당된 IP 주소를 입력합니다.

   전용 HA 포트가 없는 방화벽의 경우 피어가 HA1 링크에 대한 관리 포트를 사용하는 경우 피어의 관리 포트 IP 주소를 입력합니다.
5. 백업 **HA1 IP** 주소를 입력합니다.


©2023 Palo Alto Networks, Inc.

**STEP 14 |** (선택 사항) 네트워크가 LACP 또는 LLDP를 사용하는 경우 더 빠른 페일오버에 대한 LACP 및 LLDP 사전 협상 을 활성화합니다.

사전 협상이 활성 모드에서 작동하려면 프로토콜에 대한 ***HA*** 사전 협상을 구성하기 전에 LACP 및 LLDP를 활성화합니다.

1. 12단계에서 링크 상태를 자동으로 설정해야 합니다.
2. 네트워크 > 인터페이스 > 이더넷을 선택합니다.
3. LACP 활성 사전 협상을 활성화하려면 다음을 수행하십시오.
   1. 레이어 2 또는 레이어 3 배포에서 AE 인터페이스를 선택합니다.
   2. **LACP** 탭을 선택합니다.
   3. **HA** 수동형 상태에서 활성화를 선택합니다.
   4. 확인을 클릭합니다.

      사전 협상에는 능동형 및 수동형 방화벽에 고유한 인터페이스 ***MAC*** 주소가 필요하므로 능동형-수동형 ***HA***에 대해 동일한 시스템 ***MAC*** 주소를 선택할 수도 없습니다.
4. LACP 패시브 사전 협상을 활성화하려면 다음을 수행합니다.
   1. 가상 와이어 배포에서 이더넷 인터페이스를 선택합니다.
   2. 고급 탭을 선택합니다.
   3. **LACP** 탭을 선택합니다.
   4. **HA** 수동형 상태에서 활성화를 선택합니다.
   5. 확인을 클릭합니다.
5. LLDP 활성 사전 협상을 활성화하려면 다음을 수행하십시오.
   1. 레이어 2, 레이어 3 또는 가상 와이어 배포에서 이더넷 인터페이스를 선택합니다.
   2. 고급 탭을 선택합니다.
   3. **LLDP** 탭을 선택합니다.
   4. **HA** 수동형 상태에서 활성화를 선택합니다.
   5. 확인을 클릭합니다.

      가상 와이어 배포에 대한 ***LLDP*** 패시브 사전 협상을 허용하려면 14.e단계를 수행하지만 ***LLDP*** 자체를 활성화하지는 않습니다.

**STEP 15 |** 구성 변경 내용을 저장합니다.

커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 16 |** 두 방화벽 구성을 완료한 후 방화벽이 능동형/수동형 HA에 페어링되어 있는지 확인합니다.

1. 두 방화벽 모두에서 대시보드에 액세스하고 고가용성 위젯을 확인합니다.
2. 활성형 방화벽에서 피어에 대한 동기화를 클릭합니다.
3. 방화벽이 다음과 같이 페어링되고 동기화되어 있는지 확인합니다.
   - 수동형 방화벽의 경우: 로컬 방화벽의 상태는 수동형으로 표시되어야 하며 실행 중인 구성은 동기화된 것으로 표시되어야 합니다.
   - 능동형 방화벽의 경우: 로컬 방화벽의 상태가 활성 상태로 표시되어야 하며 실행 구성은 동기화됨으로 표시되어야 합니다.

## HA 페일오버 조건 정의

다음 작업을 수행하여 링크 모니터링 또는 경로 모니터링을 사용하여 페일오버 조건을 정의함으로써 트래픽 보안 작업이 이전에 활성 상태인 방화벽에서 해당 HA 피어로 포워딩되는 이벤트인 HA 쌍의 방화벽이 페일오버되는 원인을 설정합니다. HA 개요에서는 페일오버를 유발하는 조건을 설명합니다.

가상 라우터, VLAN 또는 가상 와이어별로 여러 IP 경로 그룹을 모니터링할 수 있습니다. 하나 이상의 IP 주소를 사용하여 각 경로 그룹을 활성화하고 각 경로 그룹에 고유한 피어 실패 조건을 지정할 수 있습니다. 또한 활성 방화벽의 상태를 확인하기 위해 "임의" 또는 "모두" 실패 검사를 사용하여 경로 그룹 수준과 더 광범위한 가상 라우터나 VLAN 또는 가상 와이어 그룹 수준에서 이러한 장애 조건을 설정할 수 있습니다.

PAN-OS 10.0으로 업그레이드하면 방화벽이 현재 모니터링되는 대상 IP 주소를 새로 생성된 대상 그룹으로 자동으로 전송하고 해당 그룹에 기본 경로 모니터링 이름을 제공합니다. 새 대상 그룹은 경로 그룹 수준에서 이전 페일오버 조건을 유지합니다.

*VLAN* 경로 모니터링은 *PAN-OS 10.0*의 능동형/능동형 *HA* 페어링과 호환되지 않으므로 *PAN-OS 10.2*로 업그레이드하기 전에 능동형/능동형 *HA*에서 모든 *VLAN* 경로 모니터링 구성을 삭제해야 합니다. 이전의 능동형/능동형 *HA* 구성을 유지하면 자동 커밋이 실패합니다.

경로 모니터링을 사용하도록 설정하기 전에 가상 라우터, VLAN 또는 가상 와이어나 이러한 논리적 네트워킹 구성 요소의 조합을 설정해야 합니다. 가상 라우터 및 가상 와이어의 경로 모니터링은 능동형/활성 및 능동형/수동형 HA 배포 모두와 호환되지만 VLAN의 경로 모니터링은 능동형/수동형 쌍에서만 지원됩니다.

경로 모니터링을 활성화하기 전에 다음 작업을 수행해야 합니다.

- 가상 라우터의 대상 IP 그룹에 대한 연결 가능성을 확인합니다.
- 경로 모니터링을 사용하도록 설정할 VLAN에 구성된 인터페이스가 포함되어 있는지 확인합니다.
- 적절한 대상 IP 주소에서 핑(ping)을 수신하는 데 사용할 원본 IP 주소를 가져옵니다.

*SNMPv3*을 사용하여 방화벽을 모니터링하는 경우 *SNMPv3* 엔진 *ID*가 *HA* 쌍 간에 동기화됩니다. *SNMP* 설정에 대한 자세한 내용은 SNMP 관리자로 트랩 포워딩을 참조하십시오. *EngineID*는 방화벽 일련번호를 사용하여 생성되므로 *VM* 시리즈 방화벽에서 각 방화벽에 대해 고유한 *EngineID*를 얻으려면 유효한 라이선스를 적용해야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** HA 링크 모니터링을 구성하려면 모니터링할 방화벽의 물리적 인터페이스 그룹(링크 업 또는 링크 다운)을 지정합니다.

1. 디바이스 > 고가용성 > 링크 및 경로 모니터링을 선택합니다.
2. 링크 모니터링 섹션에서 이름별로 링크 그룹을 추가합니다.
3. 링크 그룹을 활성화하려면 사용을 선택합니다.
4. 링크 그룹의 인터페이스에 대한 실패 조건을 선택합니다. 임의(기본값) 또는 모두
5. 모니터할 인터페이스를 추가합니다.
6. 확인을 클릭합니다.

**STEP 2 |** (선택 사항) 방화벽에 구성된 링크 그룹 집합에 대한 실패 조건을 수정합니다.

기본적으로 방화벽은 모니터링되는 링크 그룹에 장애가 발생하면 페일오버를 트리거합니다.

1. 링크 모니터링 섹션을 편집합니다.
2. 실패 조건을 임의(기본값) 또는 모두로 설정합니다.
3. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 가상 와이어, VLAN 또는 가상 라우터(또는 고급 라우팅 엔진의 경우 논리적 라우터)에 대한 HA 경로 모니터링을 구성하려면 방화벽이 네트워크 연결을 확인하기 위해 ping할 대상 IP 주소를 지정합니다.

1. 경로 모니터링 섹션에서 가상 와이어 경로 추가, **VLAN** 경로 추가 또는 가상 라우터 경로 추가(또는 논리적 라우터 경로 추가)(고급 라우팅 엔진의 경우)를 선택합니다.
2. 가상 와이어, VLAN, 가상 라우터 경로 그룹 또는 논리적 라우터 경로 그룹의 이름을 입력합니다.
3. (가상 와이어 경로 또는 VLAN 경로에만 해당) 가상 와이어 또는 VLAN을 통해 대상 IP 주소를 핑(ping)하는 데 사용할 소스 **IP** 주소를 입력합니다.
4. 경로 그룹을 활성화하려면 사용을 선택합니다.
5. 이 경로 그룹에 실패를 초래하는 실패 조건을 선택합니다. **Any**(기본값)는 이 경로 그룹에 있는 하나 이상의 대상 IP 그룹이 실패할 때 발행하거나 **All**은 이 경로 그룹의 모든 대상 IP 그룹이 실패할 때 발행합니다.
6. 핑 인터벌(밀리초)을 입력합니다. 대상 IP 주소로 전송되는 ICMP 메시지 인터벌(범위는 200~60,000이며 기본값은 200) 입니다.
7. 실패를 선언하기 전에 실패해야 하는 핑(ping)의 **Ping** 횟수를 입력합니다(범위는 3 - 10, 기본값은 10).
8. 대상 **IP** 그룹 이름을 추가하고 입력합니다.
9. 핑(ping)에 하나 이상의 대상 **IP** 주소를 추가합니다.
10. 대상 IP 그룹에 대한 경로 모니터링을 사용하려면 사용을 선택합니다.
11. 이 대상 IP 그룹에 대한 실패를 초래하는 실패 조건을 선택합니다. **Any**(기본값)는 나열된 하나 이상의 IP 주소에 연결할 수 없는 경우 실패를 나타내고 **All**은 나열된 모든 IP 주소에 연결할 수 없는 경우 실패를 나타냅니다.
12. 확인을 두 번 클릭합니다.
13. (Panorama에만 해당) 적절한 Panorama 템플릿을 선택하여 경로 모니터링 구성을 장비에 푸시합니다.

> 가상 와이어, *VLAN* 또는 가상 라우터에 대한 *HA* 경로 모니터링을 *PAN-OS 10.0* 이상의 버전을 실행하는 방화벽에만 푸시할 수 있습니다. *PAN-OS 10.0* 이전 릴리스를 실행하는 방화벽*(*예*: 9.1.x* 또는 *9.0.x)*으로 구성을 푸시하려고 하면 커밋이 실패하거나 커밋이 경로 그룹에서 대상 *IP* 주소를 제거할 수 있습니다.
>
> 하나의 대상 *IP* 그룹을 포함하는 *HA* 경로 그룹만 *PAN-OS 9.1* 및 이전 릴리스를 실행하는 관리되는 방화벽에 대해 지원됩니다.

> 다른 *PAN-OS* 릴리스를 실행하는 관리되는 방화벽에 대해 *Panorama*에서 대상 *IP* 주소를 관리하려면 *PAN-OS 10.0* 이상 릴리스를 실행하는 관리되는 방화벽에 대한 별도의 템플릿과 *PAN-OS 9.1* 및 이전 릴리스를 실행하는 관리되는 방화벽에 대한 별도의 템플릿을 만듭니다. 이렇게 하면 여러 대상 *IP* 그룹을 만든 경우 대상 *IP* 주소 구성을 보다 정확하게 제어할 수 있으며 관리되는 방화벽이 성공적으로 장애 조치되도록 할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) 방화벽에 구성된 경로 그룹 집합에 대한 실패 조건을 수정합니다.

기본적으로 방화벽은 모니터링되는 경로 그룹에 장애가 발생하면 페일오버를 트리거합니다.

1. 경로 모니터링 섹션을 편집합니다.
2. 어플라이언스에서 경로 모니터링을 활성화하려면 사용을 선택합니다.
3. 모니터링되는 하나 이상의 가상 라우터, VLAN 또는 가상 와이어가 다운되었을 때 이 방화벽에 대한 오류를 발생시키려면 실패 조건을 모두(기본값)로 설정합니다. 모니터링되는 모든 가상 라우터, VLAN 또는 가상 와이어가 다운되었을 때 이 방화벽에 대한 오류를 발생시키려면 모두를 선택합니다.
4. 확인을 클릭합니다.

**STEP 5 |** 커밋합니다.

## 장애 조치 확인

HA 구성이 제대로 작동하는지 테스트하려면 수동 페일오버를 트리거하고 방화벽 전환 상태가 성공적으로 확인되는지 확인하십시오.

**STEP 1 |** 능동형 방화벽을 일시 중단합니다.

디바이스 > 고가용성 > 운영 명령을 선택한 다음 로컬 디바이스 일시 중단 링크를 클릭합니다.

**STEP 2 |** 수동형 방화벽이 능동형 상태로 인계되었는지 확인합니다.

대시보드에서 수동형 방화벽 상태가 고가용성 위젯에서 활성 상태로 변경되는지 확인합니다.

**STEP 3 |** 일시 중단된 방화벽을 작동 상태로 복원합니다. 몇 분 동안 기다린 다음 선점이 활성화된 경우 선점이 발생했는지 확인합니다.

1. 이전에 일시 중단된 방화벽에서 디바이스 > 고가용성 > 운영 명령을 선택한 다음 로컬 디바이스 기능 링크를 클릭합니다.
2. 대시보드의 고가용성 위젯에서 방화벽이 능동형 방화벽으로 인수되었는지 확인하고 피어가 이제 수동 상태임을 확인합니다.


©2023 Palo Alto Networks, Inc.

# 활성/활성 HA 설정


- 활성/활성 HA의 전제 조건
- 활성/활성 HA 구성
- 활성/활성 사용 사례 확인


## 활성/활성 HA의 전제 조건

방화벽에서 능동형/능동형 HA를 설정하려면 다음 요구 사항을 충족하는 한 쌍의 방화벽이 필요합니다.

- 동일한 모델 - 쌍의 방화벽은 동일한 하드웨어 모델이어야 합니다.
- 동일한 **PAN-OS** 버전 - 방화벽은 동일한 PAN-OS 버전을 실행해야 하며 애플리케이션, URL 및 위협 데이터베이스에서 각각 최신 상태여야 합니다.
- 동일한 다중 가상 시스템 기능 - 두 방화벽 모두 다중 가상 시스템 기능을 활성화하거나 비활성화해야 합니다. 활성화된 경우 각 방화벽에는 고유한 다중 가상 시스템 라이선스가 필요합니다.
- 동일한 유형의 인터페이스 - 전용 HA 링크 또는 인터페이스 유형 HA로 설정된 대역 내 포트와 관리 포트의 조합입니다.
  - HA 인터페이스는 DHCP에서 얻은 IP 주소가 아닌 고정 IP 주소로만 구성해야 합니다(AWS가 DHCP 주소를 사용할 수 있는 경우 제외). HA 피어 간의 HA1(제어) 연결에 대한 IP 주소를 결정합니다. 피어의 HA1 IP 주소는 직접 연결되거나 동일한 스위치에 연결된 경우 동일한 서브넷에 있어야 합니다.

    전용 HA 포트가 없는 방화벽의 경우 제어 연결을 위해 관리 포트를 사용할 수 있습니다. 관리 포트를 사용하면 두 방화벽의 관리 평면 간에 직접 통신 링크가 제공됩니다. 그러나 관리 포트는 피어 간에 직접 케이블로 연결되지 않으므로 네트워크를 통해 이 두 인터페이스를 연결하는 경로가 있는지 확인하십시오.
  - HA2(데이터) 연결을 위한 전송 방법으로 레이어 3을 사용하는 경우 HA2 링크의 IP 주소를 결정합니다. HA2 연결이 라우팅된 네트워크를 통해 통신해야 하는 경우에만 레이어 3을 사용하십시오. HA2 링크의 IP 서브넷은 HA1 링크의 IP 서브넷 또는 방화벽의 데이터 포트에 할당된 다른 서브넷과 겹치지 않아야 합니다.
  - 각 방화벽에는 HA3 링크에 대한 전용 인터페이스가 필요합니다. PA-7000 시리즈, PA-5400 시리즈, PA-3400 시리즈 및 PA-3200 시리즈 방화벽은 HA3용 HSCI 포트를 사용합니다. PA-5200 시리즈 방화벽은 HA3용 HSCI 포트를 사용하거나 중복성을 위해 HA3용 데이터플레인 포트에서 집계 인터페이스를 구성할 수 있습니다. 나머지 플랫폼에서는 데이터플레인 포트의 집계 인터페이스를 중복성을 위한 HA3 링크로 구성할 수 있습니다.
- 동일한 라이선스 세트 - 라이선스는 각 방화벽에 고유하며 방화벽 간에 공유할 수 없습니다. 따라서 두 방화벽에 동일하게 라이선스를 부여해야 합니다. 두 방화벽에 동일한 라이선스 세트가 없으면 구성 정보를 동기화하고 원활한 페일오버를 위한 패리티를 유지할 수 없습니다.

> 기존 방화벽이 있고 ***HA*** 목적으로 새 방화벽을 추가하려는 경우 새 방화벽에 기존 구성이 있는 경우 새 방화벽에서 방화벽을 공장 기본 설정으로 재설정하는 것이 좋습니다. 이렇게 하면 새 방화벽이 깨끗한 구성을 갖게 됩니다. ***HA***를 구성한 후 기본 방화벽의 구성을 깨끗한 구성으로 새로 도입된 방화벽과 동기화합니다. 로컬 ***IP*** 주소도 구성해야 합니다.


©2023 Palo Alto Networks, Inc.

# 활성/활성 HA 구성

다음 절차에서는 능동형/능동형 구성에서 방화벽을 구성하기 위한 기본 워크플로를 설명합니다. 그러나 시작하기 전에 특정 네트워크 환경에 더 적합한 구성 예제를 보려면 능동형/능동형 사용 사례 결정을 참조하십시오.

*HA* 방화벽 사이에 스위치가 있는 경우 ***HA3*** 링크를 연결하는 스위치 포트는 ***HA3*** 링크의 ***MAC-in-MAC*** 캡슐화와 관련된 오버헤드를 처리하기 위해 점보 프레임을 지원해야 합니다.

능동형/능동형을 구성하려면 먼저 한 피어에서 다음 단계를 완료한 다음 두 번째 피어에서 완료하여 각 피어에서 디바이스 ID를 다른 값(0 또는 1)으로 설정해야 합니다.

**STEP 1 |** HA 포트를 연결하여 방화벽 간의 물리적 연결을 설정합니다.

각 사용 사례에 대해 방화벽은 모든 하드웨어 모델이 될 수 있습니다. 모델에 해당하는 ***HA3*** 단계를 선택하십시오.

- 전용 HA 포트가 있는 방화벽의 경우 이더넷 케이블을 사용하여 피어의 전용 HA1 포트와 HA2 포트를 연결합니다. 피어가 서로 직접 연결된 경우 크로스오버 케이블을 사용하십시오.
- 전용 HA 포트가 없는 방화벽의 경우 HA2 링크와 백업 HA1 링크에 대해 두 개의 데이터 인터페이스를 선택합니다. 그런 다음 이더넷 케이블을 사용하여 두 방화벽에서 이러한 대역 내 HA 인터페이스를 연결합니다. HA1 링크에 관리 포트를 사용하고 관리 포트가 네트워크를 통해 서로 연결할 수 있는지 확인하십시오.
- HA3의 경우:
  - PA-7000 시리즈 방화벽에서 첫 번째 섀시의 HSCI-A(고속 섀시 상호 연결)를 두 번째 섀시의 HSCI-A에 연결하고 첫 번째 섀시의 HSCI-B를 두 번째 섀시의 HSCI-B에 연결합니다.
  - PA-5450 방화벽에서 첫 번째 섀시의 HSCI-A를 두 번째 섀시의 HSCI-A에 연결하고 첫 번째 섀시의 HSCI-B를 두 번째 섀시의 HSCI-B에 연결합니다.
  - PA-5400 시리즈 방화벽(하나의 HSCI 포트가 있음)에서 첫 번째 섀시의 HSCI 포트를 두 번째 섀시의 HSCI 포트에 연결합니다.
  - PA-5200 시리즈 방화벽(하나의 HSCI 포트가 있음)에서 첫 번째 섀시의 HSCI 포트를 두 번째 섀시의 HSCI 포트에 연결합니다. PA-5200 시리즈 방화벽에서 HA3용 데이터 포트를 사용할 수도 있습니다.
  - PA-3400 시리즈 방화벽(하나의 HSCI 포트가 있음)에서 첫 번째 섀시의 HSCI 포트를 두 번째 섀시의 HSCI 포트에 연결합니다.
  - PA-3200 시리즈 방화벽(하나의 HSCI 포트가 있음)에서 첫 번째 섀시의 HSCI 포트를 두 번째 섀시의 HSCI 포트에 연결합니다.
  - 다른 모든 하드웨어 모델에서는 HA3용 데이터플레인 인터페이스를 사용합니다.

**STEP 2 |** 관리 포트에서 핑(ping)을 활성화합니다.

핑(ping)을 활성화하면 관리 포트가 하트비트 백업 정보를 교환할 수 있습니다.

1. 디바이스 > 설정 > 관리에서 관리 인터페이스 설정을 수정합니다.
2. 인터페이스에서 허용되는 서비스로 핑**(ping)**을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 방화벽에 전용 HA 포트가 없는 경우 데이터 포트를 HA 포트로 작동하도록 설정합니다.

전용 HA 포트가 있는 방화벽의 경우 다음 단계를 계속합니다.

1. 네트워크 > 인터페이스를 선택합니다.
2. 사용하려는 포트에서 링크가 작동하는지 확인하십시오.
3. 인터페이스를 선택한 다음 인터페이스 유형을 **HA**로 설정합니다.
4. 링크 속도 및 링크 듀플렉스 설정을 적절하게 설정합니다.

**STEP 4 |** 능동형/능동형 HA를 활성화하고 그룹 ID를 설정합니다.

1. 디바이스 > 고가용성 > 일반에서 설정을 편집합니다.
2. **HA** 활성화를 선택합니다.
3. 두 방화벽에 대해 동일해야 하는 그룹 **ID**를 입력합니다. 방화벽은 그룹 ID를 사용하여 가상 MAC 주소(범위는 1~63)를 계산합니다.
4. (선택 사항) 설명을 입력합니다.
5. 모드에서 활성 활성을 선택합니다.

**STEP 5 |** 디바이스 ID를 설정하고 동기화를 활성화하고 피어 방화벽에서 제어 링크를 식별합니다.

1. 디바이스 > 고가용성 > 일반에서 설정을 편집합니다.
2. 다음과 같이 디바이스 **ID**를 선택합니다.
   - 첫 번째 피어를 구성할 때 디바이스 **ID**를 **0**으로 설정합니다.
   - 두 번째 피어를 구성할 때 디바이스 **ID**를 **1**로 설정합니다.
3. 구성 동기화 활성화를 선택합니다. 이 설정은 두 방화벽 구성을 동기화하는 데 필요합니다(기본적으로 사용됨).
4. 피어 방화벽에 있는 HA1 제어 링크의 IP 주소인 피어 **HA1 IP** 주소를 입력합니다.
5. (선택 사항) 피어 방화벽의 백업 제어 링크의 IP 주소인 백업 피어 **HA1 IP** 주소를 입력합니다.
6. 확인을 클릭합니다.

**STEP 6 |** 디바이스 ID가 낮은 방화벽이 장애 복구 시 활성-기본 방화벽을 선점할지의 여부를 결정합니다.

1. 디바이스 > 고가용성 > 일반에서 선택 설정을 편집합니다.
2. 방화벽 중 하나가 장애에서 복구된 후 디바이스 ID가 더 낮은 방화벽이 자동으로 활성-기본 작업을 재개하도록 하려면 선점을 선택합니다. 선점이 발생하려면 두 방화벽 모두 선점을 선택해야 합니다.

   복구된 방화벽을 활성-기본 방화벽으로 수동으로 만들 때까지 활성-기본 역할이 현재 방화벽과 함께 유지되도록 하려면 선점을 선택하지 않은 상태로 둡니다.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** 제어 링크가 전용 HA 포트 또는 대역 내 포트를 사용하는 경우 하트비트 백업을 활성화하십시오.

제어 링크에 관리 포트를 사용하는 경우 하트비트 백업을 활성화할 필요가 없습니다.

1. 디바이스 > 고가용성 > 일반에서 선택 설정을 편집합니다.
2. 하트비트 백업을 선택합니다.

   방화벽 간에 하트비트가 전송되도록 하려면 두 피어의 관리 포트가 서로 라우팅할 수 있는지 확인해야 합니다.

   하트비트 백업을 활성화하면 분할 브레인 상황을 방지할 수 있습니다. 스플릿 브레인은 ***HA1*** 링크가 다운되면 방화벽이 여전히 작동하지만 방화벽이 하트비트를 놓칠 때 발생합니다. 이러한 상황에서 각 피어는 다른 피어가 다운된 것으로 믿고 실행 중인 서비스를 시작하려고 시도하여 스플릿 브레인을 발생시킵니다. 하트비트 백업을 활성화하면 중복 하트비트와 인사 메시지가 관리 포트를 통해 전송되기 때문에 스플릿 브레인을 방지합니다.

**STEP 8 |** (선택 사항) HA 타이머를 수정합니다.

기본적으로 HA 타이머 프로파일은 권장 프로파일로 설정되며 대부분의 HA 배포에 적합합니다.

1. 디바이스 > 고가용성 > 일반에서 선택 설정을 편집합니다.
2. 보다 빠른 페일오버를 트리거하려면 **Aggressive**를 선택합니다. 설정에서 페일오버를 트리거하기 위한 사용자 지정 값을 정의하려면 고급을 선택합니다.

   프로파일에 포함된 개별 타이머의 사전 설정 값을 보려면 고급을 선택한 다음 권장 로드 또는 적극적 로드를 클릭합니다. 하드웨어 모델에 대한 사전 설정 값이 화면에 표시됩니다.

**STEP 9 |** 제어 링크 연결을 설정합니다.

이 예에서는 인터페이스 유형 HA로 설정된 대역 내 포트를 사용합니다.

관리 포트를 제어 링크로 사용하는 방화벽의 경우 IP 주소 정보가 자동으로 미리 채워집니다.

1. 디바이스 > 고가용성 > 일반에서 제어 링크(HA1)를 편집합니다.
2. HA1 링크로 사용하기 위해 케이블을 연결한 포트를 선택합니다.
3. **IPv4/IPv6** 주소 및 넷마스크를 설정합니다.

   HA1 인터페이스가 별도의 서브넷에 있는 경우 게이트웨이의 IP 주소를 입력합니다. 방화벽이 직접 연결된 경우 게이트웨이 주소를 추가하지 마십시오.


©2023 Palo Alto Networks, Inc.

**STEP 10 |** (선택 사항) 제어 링크 연결에 대한 암호화를 사용하도록 설정합니다.

이것은 일반적으로 두 개의 방화벽이 직접 연결되지 않은 경우, 즉 포트가 스위치나 라우터에 연결된 경우 링크를 보호하는 데 사용됩니다.

1. 한 방화벽에서 HA 키를 내보내고 피어 방화벽으로 가져옵니다.
   1. 디바이스 > 인증서 관리 > 인증서를 선택합니다.
   2. **HA** 키 내보내기를 선택합니다. 피어가 액세스할 수 있는 네트워크 위치에 HA 키를 저장합니다.
   3. 피어 방화벽에서 디바이스 > 인증서 관리 > 인증서를 선택한 다음 **HA** 키 가져오기를 선택하여 키를 저장한 위치를 찾아 피어로 가져옵니다.
2. 디바이스 > 고가용성 > 일반에서 제어 링크(HA1)를 편집합니다.
3. 암호화 활성화를 선택합니다.

   암호화를 사용하도록 설정하면 ***HA*** 방화벽 구성을 완료한 후 HA1 SSH 키 새로 고침 및 키 옵션 구성을(를) 수행할 수 있습니다.

**STEP 11 |** 백업 제어 링크 연결을 설정합니다.

1. 디바이스 > 고가용성 > 일반에서 제어 링크(HA1 백업)를 편집합니다.
2. HA1 백업 인터페이스를 선택한 다음 **IPv4/IPv6** 주소 및 넷마스크를 설정합니다.

   *PA-3200* 시리즈 방화벽은 ***HA1*** 백업 제어 링크에 대해 ***IPv6*** 주소를 지원하지 않으며 ***IPv4*** 주소를 사용합니다.

**STEP 12 |** 방화벽 간의 데이터 링크 연결(HA2) 및 백업 HA2 연결을 설정합니다.

1. 디바이스 > 고가용성 > 일반에서 데이터 링크(HA2)를 편집합니다.
2. 데이터 링크 연결에 사용할 포트를 선택합니다.
3. 전송 방법을 선택합니다. 기본값은 이더넷이며 HA 쌍이 직접 연결되거나 스위치를 통해 연결될 때 작동합니다. 네트워크를 통해 데이터 링크 트래픽을 라우팅해야 하는 경우 전송 모드로 **IP** 또는 **UDP**를 선택합니다.
4. IP 또는 UDP를 전송 방법으로 사용하는 경우 **IPv4/IPv6** 주소와 넷마스크를 입력합니다.
5. 세션 동기화 활성화가 선택되었는지 확인합니다.
6. HA 피어 간의 HA2 데이터 링크에 대한 모니터링을 활성화하려면 **HA2** 연결 유지를 선택합니다. 설정된 임계값(기본값은 10000ms)에 따라 장애가 발생하면 정의된 조치가 발생합니다.


©2023 Palo Alto Networks, Inc.

HA2 연결 유지 오류가 발생하면 시스템에서 중요한 시스템 로그 메시지를 생성하거나 구성에 따라 데이터 플레인을 분할합니다.

두 방화벽에서 또는 *HA* 쌍에서 방화벽 하나만에서 *HA2* 연결 유지 옵션을 구성할 수 있습니다. 옵션이 하나의 방화벽에서만 활성화된 경우 해당 방화벽만 연결 유지 메시지를 보냅니다. 장애가 발생하면 다른 방화벽에 알립니다.

분할 데이터 플레인은 두 피어의 데이터 플레인이 독립적으로 작동하도록 하는 동시에 고가용성 상태를 *Active-Primary* 및 *Active-Secondary*로 유지합니다. 데이터 플레인을 분할하도록 방화벽이 하나만 구성된 경우 분할 데이터 플레인은 다른 디바이스에도 적용됩니다.

7. 데이터 링크**(HA2** 백업**)** 섹션을 편집하고 인터페이스를 선택한 다음 **IPv4/IPv6** 주소 및 넷마스크를 추가합니다.
8. 확인을 클릭합니다.

**STEP 13 |** 패킷 포워딩을 위한 HA3 링크를 구성합니다.

1. 디바이스 > 고가용성 > 능동형**/**능동형 구성에서 패킷 포워딩을 편집합니다.
2. **HA3** 인터페이스의 경우 능동형/능동형 HA 피어 간에 패킷을 포워딩하는 데 사용할 인터페이스를 선택합니다. Layer 2 전송이 가능한 전용 인터페이스여야 하며 인터페이스 유형 **HA**로 설정되어야 합니다.
3. HA 피어에 구성된 모든 가상 라우터를 강제로 동기화하려면 **VR** 동기화를 선택합니다. 가상 라우터가 동적 라우팅 프로토콜에 대해 구성되지 않은 경우 선택합니다. 두 피어는 교환 네트워크를 통해 동일한 다음 홉 라우터에 연결되어야 하며 정적 라우팅만 사용해야 합니다.
4. **QoS** 동기화를 선택하여 모든 물리적 인터페이스에서 QoS 프로파일 선택을 동기화합니다. 두 피어의 링크 속도가 비슷하고 모든 물리적 인터페이스에서 동일한 QoS 프로파일이 필요한 경우 선택합니다. 이 설정은 네트워크 탭의 QoS 설정 동기화에 영향을 줍니다. QoS 정책은 이 설정에 관계없이 동기화됩니다.

**STEP 14 |** (선택 사항) 임시 보류 시간을 수정합니다.

1. 디바이스 > 고가용성 > 능동형**/**능동형 구성에서 패킷 포워딩을 편집합니다.
2. 임시 보류 시간**(**초**)**에 방화벽이 실패 후 복구된 후 임시 상태를 유지하는 시간(초)을 입력합니다(범위는 10-600, 기본값은 60).


©2023 Palo Alto Networks, Inc.

**STEP 15 |** 세션 소유자 및 세션 설정을 구성합니다.

1. 디바이스 > 고가용성 > 능동형/능동형 구성에서 패킷 포워딩을 편집합니다.
2. 세션 소유자 선택에서 다음 중 하나를 선택합니다.
   - 첫 번째 패킷 - 새 세션의 첫 번째 패킷을 수신하는 방화벽이 세션 소유자입니다(권장 설정). 이 설정은 HA3에서 트래픽을 최소화하고 피어 간에 트래픽을 공유합니다.
   - 기본 디바이스 - 활성-기본 상태에 있는 방화벽이 세션 소유자입니다.
3. 세션 설정에서 다음 중 하나를 선택합니다.
   - **IP Modulo** - 방화벽은 패킷의 소스 및 대상 IP 주소에 대해 XOR 작업을 수행하고 그 결과에 따라 세션을 설정할 HA 피어를 선택합니다.
   - 기본 디바이스 - 활성-기본 방화벽이 모든 세션을 설정합니다.
   - 첫 번째 패킷 - 새 세션의 첫 번째 패킷을 수신하는 방화벽이 세션 설정(권장 설정)을 수행합니다.

     세션 소유자 및 세션 설정을 위한 첫 번째 패킷으로 시작한 다음 부하 분산에 따라 다른 옵션 중 하나로 변경할 수 있습니다.
   - **IP** 해시 - 방화벽은 소스 IP 주소 또는 소스 및 대상 IP 주소 조합의 해시를 사용하여 세션 설정 책임을 분산합니다.
4. 확인을 클릭합니다.

**STEP 16 |** HA 가상 주소를 구성합니다.

유동 IP 주소와 가상 MAC 주소 또는 ARP 부하 공유를 사용하려면 가상 주소가 필요합니다.

1. 디바이스 > 고가용성 > 능동형/능동형 구성에서 가상 주소를 추가합니다.
2. 인터페이스를 입력하거나 선택합니다.
3. **IPv4** 또는 **IPv6** 탭을 선택한 다음 추가를 클릭합니다.
4. **IPv4** 주소 또는 **IPv6** 주소를 입력합니다.
5. 유형:
   - 가상 IP 주소를 유동 IP 주소로 구성하려면 유동을 선택합니다.
   - **ARP** 부하 공유를 선택하여 가상 IP 주소를 공유 IP 주소로 구성하고 ARP 부하 공유 구성으로 건너뜁니다.

**STEP 17 |** 유동 IP 주소를 구성합니다.

1. 능동형/능동형 HA 쌍이 능동형/수동형 HA 쌍처럼 작동하도록 하려면 능동형-기본 디바이스에 바인딩된 유동 **IP**를 선택하지 마십시오.
2. 디바이스 **0** 우선 순위 및 디바이스 **1** 우선 순위에 대해 각각 디바이스 ID 0 및 디바이스 ID 1로 구성된 방화벽의 우선 순위를 입력합니다. 상대 우선 순위는 방금 구성한 유동 IP 주소를 소유하는 피어를 결정합니다(범위는 0-255). 우선 순위 값이 가장 낮은 방화벽(우선 순위가 가장 높음)은 부동 IP 주소를 소유합니다.
3. 인터페이스의 링크 상태가 다운될 때 방화벽이 페일오버 주소를 사용하도록 하려면 링크 상태가 다운된 경우 페일오버 주소를 선택하십시오.
4. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 18 |** ARP 로드 공유를 구성합니다.

디바이스 선택 알고리즘은 부하 공유를 제공하기 위해 ARP 요청에 응답하는 HA 방화벽을 결정합니다.

1. 디바이스 선택 알고리즘에 대해 다음 중 하나를 선택합니다.
   - **IP Modulo** - ARP 요청에 응답하는 방화벽은 ARP 요청자의 IP 주소 패리티를 기반으로 합니다.
   - **IP** 해시 - ARP 요청에 응답하는 방화벽은 ARP 요청자의 IP 주소 해시를 기반으로 합니다.
2. 확인을 클릭합니다.

**STEP 19 |** HA 페일오버 조건을 정의합니다.

**STEP 20 |** 구성을 커밋합니다.

## 활성/활성 사용 사례 확인

어떤 유형의 사용 사례가 있는지 확인한 다음 해당 절차를 선택하여 능동형/능동형 HA를 구성합니다.

경로 기반 중복성, 부동 IP 주소 및 가상 MAC 주소 또는 ARP 로드 공유을 사용하는 경우 해당 절차를 선택합니다.

- 사용 사례: 경로 기반 중복성으로 능동형/능동형 HA 구성
- 사용 사례: 유동 IP 주소를 사용하여 능동형/능동형 HA 구성
- 사용 사례: ARP 로드 쉐어링으로 활성/활성 HA 구성

능동형/수동형 배포처럼 작동하는 레이어 3 능동형/능동형 HA 배포를 원하는 경우 다음 절차를 선택하십시오.

- 사용 사례: 능동형-기본 방화벽에 바인딩된 부동 IP 주소를 사용하여 능동형/능동형 HA 구성

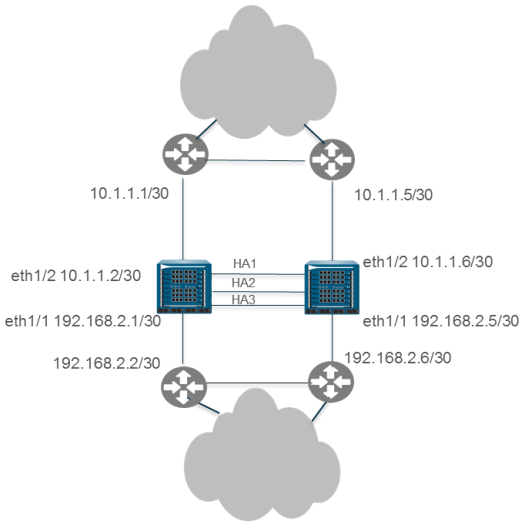
활성/활성 HA 모드의 NAT을(를) 구성하는 경우 다음 절차를 참조하십시오.

- 사용 사례: 유동 IP 주소를 사용하여 소스 DIPP NAT로 능동형/능동형 HA 구성
- 사용 사례: 능동형/능동형 HA 방화벽에 대해 별도의 소스 NAT IP 주소 풀 구성
- 사용 사례: 대상 NAT를 사용하여 ARP 로드 공유를 위한 능동형/능동형 HA 구성
- 사용 사례: 레이어 3에서 대상 NAT를 사용하여 ARP 로드 공유에 대한 능동형/능동형 HA 구성

### 사용 사례: 경로 기반 중복성으로 능동형/능동형 HA 구성

다음 레이어 3 토폴로지에서는 Route 기반 중복성을 사용하는 능동형/능동형 HA 환경에서 두 개의 PA-7050 방화벽을 보여 줍니다. 방화벽은 OSPF 영역에 속합니다. 링크 또는 방화벽이 실패하면 OSPF는 트래픽을 작동하는 방화벽으로 리디렉션하여 중복성을 처리합니다.

 ©2023 Palo Alto Networks, Inc.




**STEP 1 |** 활성/활성 HA를 구성합니다.

1단계부터 15단계까지 수행합니다.

**STEP 2 |** OSPF를 구성합니다.

OSPF를 참조하십시오.

**STEP 3 |** HA 페일오버 조건을 정의합니다.

HA 페일오버 조건을 정의합니다.

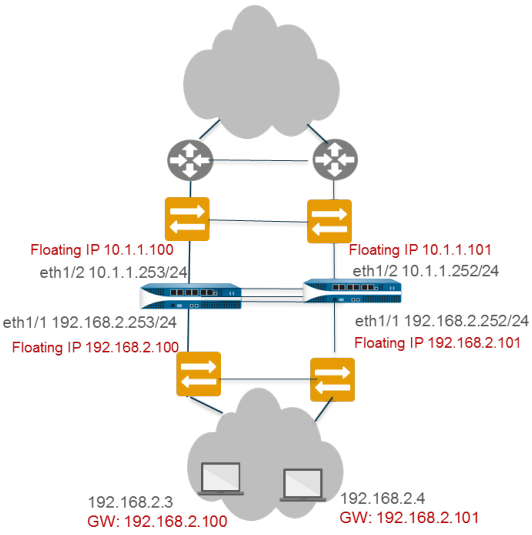
**STEP 4 |** 구성을 커밋합니다.

**STEP 5 |** 첫 번째 방화벽에 대해 디바이스 ID **0**을 선택한 경우 5단계를 제외한 동일한 방식으로 피어 방화벽을 구성하고 피어 방화벽에 대해 디바이스 ID **1**을 선택합니다.

## 사용 사례: 유동 IP 주소를 사용하여 능동형/능동형 HA 구성

이 레이어 3 인터페이스 예에서 HA 방화벽은 스위치에 연결하고 부동 IP 주소를 사용하여 링크 또는 방화벽 오류를 처리합니다. 최종 호스트는 각각 HA 방화벽 중 하나의 유동 IP 주소인 게이트웨이로 구성됩니다. 유동 IP 주소 및 가상 MAC 주소의 내용을 참조하십시오.


©2023 Palo Alto Networks, Inc.




**STEP 1 |** 활성/활성 HA를 구성합니다.

1단계부터 15단계까지 수행합니다.

**STEP 2 |** HA 가상 주소를 구성합니다.

유동 IP 주소 및 가상 MAC 주소를 사용하려면 가상 주소가 필요합니다.

1. 디바이스 > 고가용성 > 능동형/능동형 구성에서 가상 주소를 추가합니다.
2. 인터페이스를 입력하거나 선택합니다.
3. **IPv4** 또는 **IPv6** 탭을 선택한 다음 추가를 클릭합니다.
4. **IPv4** 주소 또는 **IPv6** 주소를 입력합니다.
5. 유형에 대해 부동을 선택하여 가상 IP 주소를 유동 IP 주소로 구성합니다.

**STEP 3 |** 유동 IP 주소를 구성합니다.

1. 능동형-기본 디바이스에 바인딩된 유동 **IP**를 선택하지 마십시오.
2. 디바이스 **0** 우선 순위 및 디바이스 **1** 우선 순위에 대해 각각 디바이스 ID 0 및 디바이스 ID 1로 구성된 방화벽의 우선 순위를 입력합니다. 상대적 우선 순위는 방금 구성한 부동 IP 주소를 소유하는 피어를 결정합니다(범위는 0 ~ 255). 우선 순위 값이 가장 낮은 방화벽(우선 순위가 가장 높음)은 부동 IP 주소를 소유합니다.
3. 인터페이스의 링크 상태가 다운될 때 방화벽이 페일오버 주소를 사용하도록 하려면 링크 상태가 다운된 경우 페일오버 주소를 선택하십시오.
4. 확인을 클릭합니다.

**STEP 4 |** PA-7000 시리즈 방화벽 이외의 방화벽에서 점보 프레임을 활성화합니다.

능동형/능동형 HA 구성의 19단계를 수행합니다.

**STEP 5 |** HA 페일오버 조건 정의

**STEP 6 |** 구성을 커밋합니다.

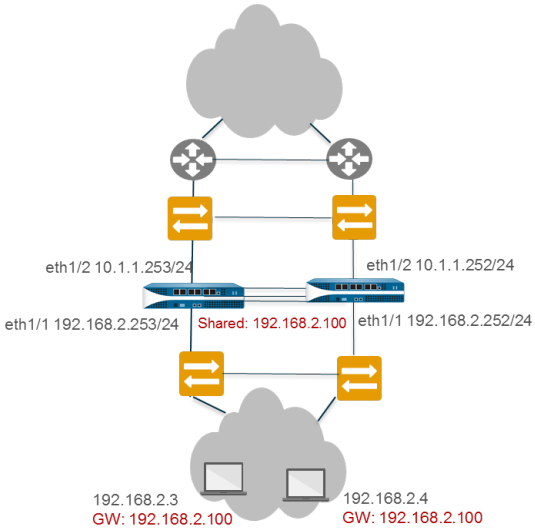
 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 다른 디바이스 ID를 선택하는 것을 제외하고는 피어 방화벽을 동일한 방식으로 구성합니다.

예를 들어 첫 번째 방화벽에 대해 디바이스 ID **0**을 선택한 경우 피어 방화벽의 디바이스 ID **1**을 선택합니다.

## 사용 사례: ARP 로드 쉐어링으로 활성/활성 HA 구성

이 예제에서는 레이어 3 배포의 호스트는 HA 방화벽의 게이트웨이 서비스가 필요합니다. 방화벽은 ARP 로드 공유를 허용하는 단일 공유 IP 주소로 구성됩니다. 최종 호스트는 HA 방화벽의 공유 IP 주소인 동일한 게이트웨이로 구성됩니다.




**STEP 1 |** 능동형/능동형 HA 구성의 1단계부터 15단계까지 수행합니다.

**STEP 2 |** HA 가상 주소를 구성합니다.

가상 주소는 ARP 로드 공유를 허용하는 공유 IP 주소입니다.

1. 디바이스 > 고가용성 > 활성/활성 구성 > 가상 주소를 선택하고 추가를 클릭합니다.
2. 인터페이스를 입력하거나 선택합니다.
3. **IPv4** 또는 **IPv6** 탭을 선택한 다음 추가를 클릭합니다.
4. **IPv4** 주소 또는 **IPv6** 주소를 입력합니다.
5. 유형에 대해 **ARP** 로드 공유를 선택하면 두 피어가 ARP Load-Sharing에 가상 IP 주소를 사용할 수 있습니다.

**STEP 3 |** ARP 로드 공유를 구성합니다.

디바이스 선택 알고리즘은 부하 공유를 제공하기 위해 ARP 요청에 응답하는 HA 방화벽을 결정합니다.

1. 디바이스 선택 알고리즘에 대해 다음 중 하나를 선택합니다.
   - **IP Modulo** - ARP 요청에 응답하는 방화벽은 ARP 요청자의 IP 주소 패리티를 기반으로 합니다.
   - **IP** 해시 - ARP 요청에 응답하는 방화벽은 ARP 요청자의 IP 주소 해시를 기반으로 합니다.
2. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** PA-7000 시리즈 방화벽 이외의 방화벽에서 점보 프레임을 활성화합니다.

**STEP 5 |** HA 페일오버 조건 정의

**STEP 6 |** 구성을 커밋합니다.

**STEP 7 |** 다른 디바이스 ID를 선택하는 것을 제외하고는 피어 방화벽을 동일한 방식으로 구성합니다.

예를 들어 첫 번째 방화벽에 대해 디바이스 ID **0**을 선택한 경우 피어 방화벽의 디바이스 ID **1**을 선택합니다.

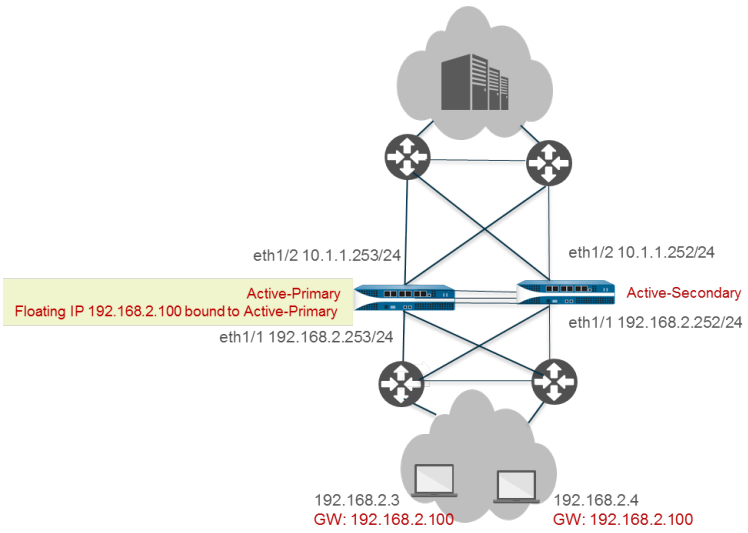
## 사용 사례: 능동형-기본 방화벽에 바인딩된 부동 IP 주소를 사용하여 능동형/능동형 HA 구성

미션 크리티컬 데이터 센터에서는 두 레이어 3 HA 방화벽이 경로 모니터링에 참여하여 두 방화벽에서 업스트림으로 경로 장애를 감지할 수 있도록 할 수 있습니다. 또한 부동 IP 주소가 바인딩된 디바이스 ID로 반환되는 부동 IP 주소가 아니라 복구된 방화벽이 다시 복원된 방화벽으로 반환되는지의 여부나 시기를 제어하는 것이 좋습니다. (이 기본 동작은 유동 IP 주소 및 가상 MAC 주소에 설명되어 있습니다.)

이 사용 사례에서는 부동 IP 주소와 활성-기본 역할이 복구된 HA 피어로 다시 이동하는 시기를 제어합니다. 능동형/능동형 HA 방화벽은 능동형-기본 상태인 방화벽에 바인딩하는 단일 유동 IP 주소를 공유합니다. 하나의 유동 IP 주소만 있으면 네트워크 트래픽이 주로 단일 방화벽으로 흐르기 때문에 이 능동형/능동형 배포는 능동형/수동형 배포와 같은 기능을 합니다.

이 사용 사례에서는 레이어 3에서 작동하는 가상 포트 채널(VPC)이 있는 Cisco Nexus 7010 스위치가 방화벽에 연결됩니다. 부동 IP 주소에 대한 경로 기본 설정을 사용하여 방화벽의 북쪽과 남쪽 레이어 3 스위치(라우터 피어)를 구성해야 합니다. 즉, 라우터 피어의 라우팅 테이블이 유동 IP 주소에 대한 최상의 경로를 갖도록 네트워크를 설계해야 합니다. 이 예에서는 유동 IP 주소에 대한 경로가 더 낮은 메트릭(유동 IP 주소에 대한 경로가 기본 설정)을 사용하고 트래픽을 수신하도록 적절한 지표와 함께 고정 경로를 사용합니다. 고정 경로를 사용하는 대신 부동 IP 주소를 OSPF 라우팅 프로토콜로 재배포하도록 네트워크를 설계하는 것입니다(OSPF를 사용하는 경우).

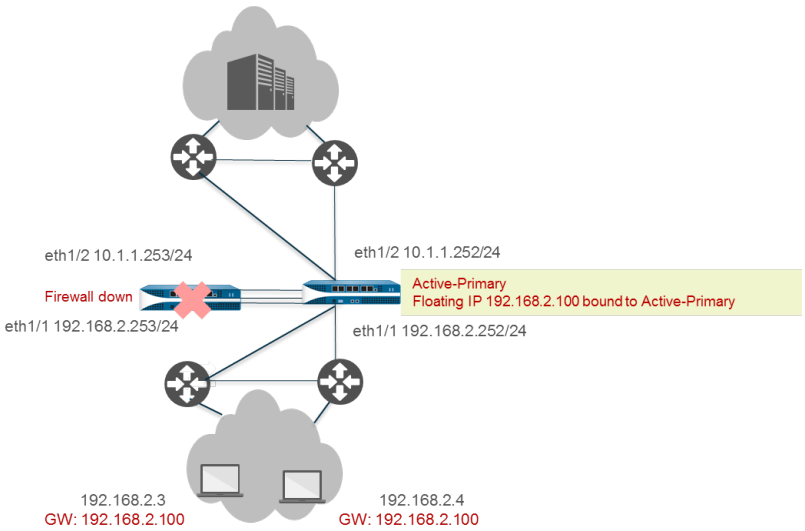
다음 토폴로지는 능동형-기본 방화벽에 바인딩된 부동 IP 주소를 보여 줍니다. 이 주소는 처음에는 왼쪽에 있는 방화벽인 피어 A입니다.




페일오버 시 능동형-기본 방화벽(피어 A)이 다운되고 능동형-보조 방화벽(피어 B)이 능동형-기본 피어로 인수되면 부동 IP 주소가 피어 B로 이동합니다(다음 그림 참조). 피어 A가 복구하고 능동형-보조 방화벽이

 ©2023 Palo Alto Networks, Inc.

되더라도 피어 B는 능동형-기본 방화벽으로 유지되며 트래픽은 피어 B로 계속 이동합니다. 피어 A가 능동형-기본 방화벽으로 다시 설정될지의 여부나 시기를 결정합니다.




부동 IP 주소를 능동형-기본 방화벽에 바인딩하면 방화벽이 다양한 HA 방화벽 상태 간에 이동할 때 부동 IP 주소 소유권을 결정하는 방법을 보다 효과적으로 제어할 수 있습니다. 다음과 같은 이점이 있습니다.

- 두 방화벽에서 경로 모니터링을 위한 능동형/능동형 HA 구성을 가질 수 있지만, 부동 IP 주소로 포워딩되는 트래픽은 항상 능동형-기본 방화벽으로 이동하기 때문에 방화벽이 능동형/수동형 HA 구성과 같은 기능을 갖도록 할 수 있습니다.

두 방화벽에서 선점을 사용하지 않도록 설정하면 다음과 같은 추가 이점이 있습니다.

- 활성 보조 방화벽이 위아래로 펄럭이는 경우 부동 IP 주소는 HA 방화벽 간에 앞뒤로 이동하지 않습니다.
- 수동으로 트래픽을 다시 포워딩하기 전에 복구된 방화벽 및 인접 구성 요소의 기능을 검토할 수 있습니다. 이 작업은 편리한 다운타임에 수행할 수 있습니다.
- 유동 IP 주소를 소유하는 방화벽을 제어할 수 있으므로 능동형-기본 방화벽에 새 세션과 기존 세션의 모든 흐름을 유지하여 HA3 링크의 트래픽을 최소화할 수 있습니다.

- 유동 *IP* 주소를 지원하는 인터페이스에서 *HA* 링크 모니터링을 구성하여 각 *HA* 피어가 링크 장애를 신속하게 감지하고 해당 피어로 페일오버할 수 있도록 하는 것이 좋습니다. 두 *HA* 피어 모두 작동하려면 링크 모니터링이 있어야 합니다.
- 방화벽이 피어로 페일오버할 수 있도록 경로가 실패할 경우 각 *HA* 피어에 알리도록 *HA* 경로 모니터링을 구성하는 것이 좋습니다. 부동 *IP* 주소는 항상 능동형-기본 방화벽에 바인딩되므로 경로가 다운되고 경로 모니터링이 사용되지 않으면 방화벽이 자동으로 피어로 페일오버할 수 없습니다.

능동형-기본 방화벽에 바인딩된 부동 *IP* 주소에 대해서는 *NAT*를 구성할 수 없습니다.

**STEP 1 |** 활성/활성 HA 구성의 1단계부터 5단계까지 수행합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** (선택 사항) 선점을 비활성화합니다.

선점을 사용하지 않도록 설정하면 복구된 방화벽이 능동형-기본 방화벽이 되는 시기를 완전히 제어할 수 있습니다.

1. 디바이스 > 고가용성 > 일반에서 일렉션(Election) 설정을 편집합니다.
2. 활성화된 경우 선점형 선택을 취소합니다.
3. 확인을 클릭합니다.

**STEP 3 |** 능동형/능동형 HA 구성의 7단계부터 14단계까지 수행합니다.

**STEP 4 |** 세션 소유자 및 세션 설정을 구성합니다.

1. 디바이스 > 고가용성 > 능동형/능동형 구성에서 패킷 포워딩을 편집합니다.
2. 세션 소유자 선택의 경우 기본 디바이스를 선택하는 것이 좋습니다. 활성-기본 상태에 있는 방화벽은 세션 소유자입니다.

   또는 세션 소유자 선택에서 첫 번째 패킷을 선택한 다음 세션 설정에서 기본 디바이스 또는 첫 번째 패킷을 선택할 수 있습니다.
3. 세션 설정에서 기본 디바이스 - 능동형-기본 방화벽이 모든 세션을 설정합니다. 능동형/능동형 구성이 능동형-기본 방화벽에서 모든 활동을 유지하므로 능동형/수동형 구성처럼 동작하도록 하려면 이 설정을 사용하는 것이 좋습니다.

   또한 비대칭 트래픽이 *HA* 쌍으로 포워딩될 가능성을 없애기 위해 네트워크를 엔지니어링해야 합니다. 이렇게 하지 않고 트래픽이 능동형-보조 방화벽으로 이동하는 경우 세션 소유자 선택 및 세션 설정을 기본 디바이스로 설정하면 트래픽이 *HA3*을 통과하여 세션 소유권 및 세션 설정을 위해 능동형-기본 방화벽으로 이동합니다.
4. 확인을 클릭합니다.

**STEP 5 |** HA 가상 주소를 구성합니다.

1. 디바이스 > 고가용성 > 활성/활성 구성 > 가상 주소를 선택하고 추가를 클릭합니다.
2. 인터페이스를 입력하거나 선택합니다.
3. **IPv4** 또는 **IPv6** 탭을 선택하고 **IPv4** 주소 또는 **IPv6** 주소를 추가합니다.
4. 유형에 대해 가상 IP 주소를 유동 IP 주소로 구성하는 부동을 선택합니다.
5. 확인을 클릭합니다.

**STEP 6 |** 유동 IP 주소를 능동형-기본 방화벽에 바인딩합니다.

1. 능동형-기본 디바이스에 바인딩된 유동 **IP**를 선택합니다.
2. 인터페이스의 링크 상태가 다운될 때 방화벽이 페일오버 주소를 사용하도록 하려면 링크 상태가 다운된 경우 페일오버 주소를 선택하십시오.
3. 확인을 클릭합니다.

**STEP 7 |** PA-7000 시리즈 방화벽 이외의 방화벽에서 점보 프레임을 활성화합니다.

**STEP 8 |** 구성을 커밋합니다.


©2023 Palo Alto Networks, Inc.

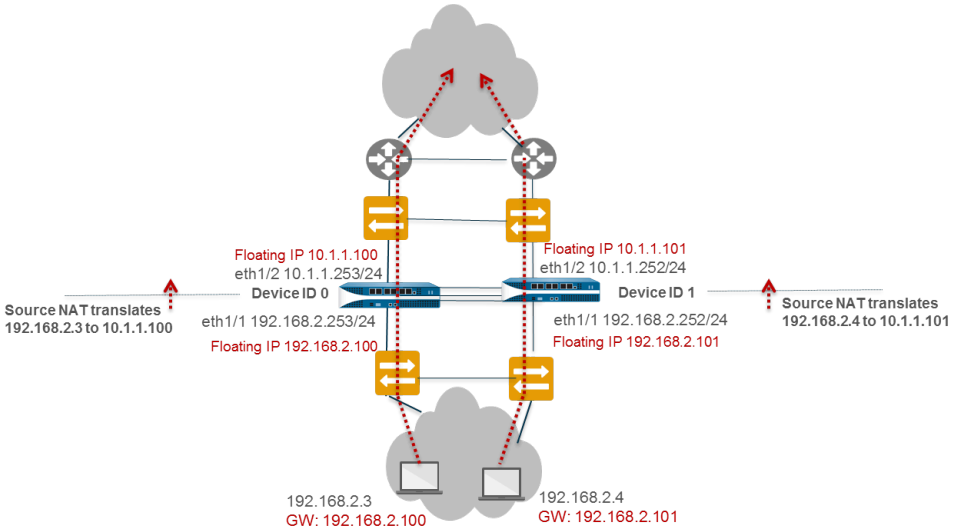
**STEP 9 |** 다른 디바이스 ID를 선택하는 것을 제외하고는 피어 방화벽을 동일한 방식으로 구성합니다.

예를 들어 첫 번째 방화벽에 대해 디바이스 ID **0**을 선택한 경우 피어 방화벽의 디바이스 ID **1**을 선택합니다.

## 사용 사례: 유동 IP 주소를 사용하여 소스 DIPP NAT로 능동형/능동형 HA 구성

이 Layer 3 인터페이스 예제는 능동형/능동형 HA 모드에서 소스 NAT를 사용합니다. 레이어 2 스위치는 브로드캐스트 도메인을 생성하여 사용자가 방화벽의 북쪽과 남쪽에 있는 모든 곳에 연결할 수 있도록 합니다.

PA-3050-1에는 디바이스 ID 0이 있고 HA 피어인 PA-3050-2에는 디바이스 ID 1이 있습니다. 이 사용 사례에서 NAT는 소스 IP 주소와 포트 번호를 이그레스(egress) 인터페이스에 구성된 유동 IP 주소로 변환합니다. 각 호스트는 각 방화벽의 Ethernet1/1에 있는 유동 IP 주소인 기본 게이트웨이 주소로 구성됩니다. 단일 방화벽에서 두 NAT 규칙을 구성하고, 단일 방화벽에서 두 NAT 규칙을 모두 구성하고 피어 방화벽과 동기화되지만 하나는 각 디바이스 ID에 바인딩됩니다.




**STEP 1 |** PA-3050-2(디바이스 ID 1)에서 능동형/능동형 HA 구성의 1단계부터 3단계까지 수행합니다.

**STEP 2 |** 능동형/능동형 HA를 활성화합니다.

1. 디바이스 > 고가용성 > 일반에서 설정을 편집합니다.
2. **HA** 활성화를 선택합니다.
3. 두 방화벽에 대해 동일해야 하는 그룹 **ID**를 입력합니다. 방화벽은 그룹 ID를 사용하여 가상 MAC 주소(범위는 1~63)를 계산합니다.
4. 모드에서 활성 활성을 선택합니다.
5. 디바이스 **ID**를 **1**로 설정합니다.
6. 구성 동기화 활성화를 선택합니다. 이 설정은 두 방화벽 구성을 동기화하는 데 필요합니다(기본적으로 사용됨).
7. 피어 방화벽에 있는 HA1 제어 링크의 IP 주소인 피어 **HA1 IP** 주소를 입력합니다.
8. (선택 사항) 피어 방화벽의 백업 제어 링크의 IP 주소인 백업 피어 **HA1 IP** 주소를 입력합니다.
9. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 활성/활성 HA를 구성합니다.

6단계부터 14단계까지 완료하십시오.

**STEP 4 |** 세션 소유자 및 세션 설정을 구성합니다.

1. 디바이스 > 고가용성 > 능동형/능동형 구성에서 패킷 포워딩을 편집합니다.
2. 세션 소유자 선택에 대해 첫 번째 패킷을 선택합니다. 새 세션의 첫 번째 패킷을 수신하는 방화벽이 세션 소유자입니다.
3. 세션 설정의 경우 **IP** 모듈로를 선택합니다. 소스 IP 주소의 패리티를 기반으로 세션 설정 로드를 분산합니다.
4. 확인을 클릭합니다.

**STEP 5 |** HA 가상 주소를 구성합니다.

1. 디바이스 > 고가용성 > 활성/활성 구성 > 가상 주소를 선택하고 추가를 클릭합니다.
2. 인터페이스 eth1/1을 선택합니다.
3. **IPv4**를 선택하고 10.1.1.101의 **IPv4** 주소를 추가합니다.
4. 유형에 대해 가상 IP 주소를 유동 IP 주소로 구성하는 부동을 선택합니다.

**STEP 6 |** 유동 IP 주소를 구성합니다.

1. 능동형-기본 디바이스에 바인딩된 유동 **IP**를 선택하지 마십시오.
2. 인터페이스의 링크 상태가 다운될 때 방화벽이 페일오버 주소를 사용하도록 하려면 링크 상태가 다운된 경우 페일오버 주소를 선택하십시오.
3. 확인을 클릭합니다.

**STEP 7 |** PA-7000 시리즈 이외의 방화벽에서 점보 프레임을 활성화합니다.

**STEP 8 |** HA 페일오버 조건을 정의합니다.

**STEP 9 |** 구성을 커밋합니다.

**STEP 10 |** 다음 변경 사항을 제외하고 동일한 설정으로 피어 방화벽 PA-3050-1을 구성합니다.

- 디바이스 **ID 0**을 선택합니다.
- 10.1.1.100의 HA 가상 주소를 구성합니다.
- 디바이스 **1** 우선 순위에 255를 입력합니다. 디바이스 **0** 우선 순위에 0을 입력합니다.

이 예에서 디바이스 ID 0은 우선 순위 값이 낮으므로 우선 순위가 높습니다. 따라서 디바이스 ID가 0인 방화벽(PA-3050-1)은 유동 IP 주소 10.1.1.100을 소유합니다.


©2023 Palo Alto Networks, Inc.

**STEP 11 |** 여전히 PA-3050-1에서 디바이스 ID 0에 대한 소스 NAT 규칙을 생성합니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 이 예에서 디바이스 ID 0에 대한 소스 NAT 규칙으로 식별하는 규칙의 이름을 입력합니다.
3. **NAT** 유형으로 **ipv4**(기본값)를 선택합니다.
4. 소스 패킷에서 소스 영역에 대해 **Any**를 선택합니다.
5. 대상 영역에서 외부 네트워크용으로 생성한 영역을 선택합니다.
6. 대상 인터페이스, 서비스, 소스 주소 및 대상 주소가 모두로 설정된 상태를 유지하도록 허용합니다.
7. 변환된 패킷의 경우 변환 유형에 대해 동적 **IP** 및 포트를 선택합니다.
8. 주소 유형에 대해 인터페이스 주소를 선택합니다. 이 경우 변환된 주소는 인터페이스의 IP 주소가 됩니다. 유동 IP 주소 10.1.1.100의 인터페이스(이 예에서는 eth1/1)와 **IP** 주소를 선택합니다.
9. 활성/활성 **HA** 바인딩 탭에서 활성/활성 **HA** 바인딩에 대해 **0**을 선택하여 NAT 규칙을 디바이스 ID 0에 바인딩합니다.
10. 확인을 클릭합니다.

**STEP 12 |** 디바이스 ID 1에 대한 소스 NAT 규칙을 생성합니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 이 예에서 디바이스 ID 1에 대한 소스 NAT 규칙으로 식별하는 데 도움이 되는 정책 규칙의 이름을 입력합니다.
3. **NAT** 유형으로 **ipv4**(기본값)를 선택합니다.
4. 소스 패킷에서 소스 영역에 대해 **Any**를 선택합니다. 대상 영역에서 외부 네트워크용으로 생성한 영역을 선택합니다.
5. 대상 인터페이스, 서비스, 소스 주소 및 대상 주소가 모두로 설정된 상태를 유지하도록 허용합니다.
6. 변환된 패킷의 경우 변환 유형에 대해 동적 **IP** 및 포트를 선택합니다.
7. 주소 유형에 대해 인터페이스 주소를 선택합니다. 이 경우 변환된 주소는 인터페이스의 IP 주소가 됩니다. 유동 IP 주소 10.1.1.101의 인터페이스(이 예에서는 eth1/1)와 **IP** 주소를 선택합니다.
8. 활성/활성 **HA** 바인딩 탭에서 활성/활성 **HA** 바인딩에 대해 **1**을 선택하여 NAT 규칙을 디바이스 ID 1에 바인딩합니다.
9. 확인을 클릭합니다.

**STEP 13 |** 구성을 커밋합니다.

## 사용 사례: 능동형/능동형 HA 방화벽에 대해 별도의 소스 NAT IP 주소 풀 구성

활성/활성 HA 모드의 NAT 소스에 대해 IP 주소 풀을 사용하려면 각 방화벽에 고유한 풀이 있어야 하며, 이 풀은 NAT 규칙의 디바이스 ID에 바인딩됩니다.

주소 개체와 NAT 규칙은 동기화되므로(능동형/수동형 및 능동형/능동형 모드 모두) HA 쌍의 방화벽 중 하나만 구성해야 합니다.


©2023 Palo Alto Networks, Inc.

이 예에서는 IP 주소 풀 10.1.1.140-10.1.1.150을 포함하는 Dyn-IP-Pool-dev0이라는 주소 개체를 구성합니다. 또한 IP 주소 풀 10.1.1.160-10.1.1.170을 포함하는 Dyn-IP-Pool-dev1이라는 주소 개체를 구성합니다. 첫 번째 주소 개체는 디바이스 ID 0에 바인딩됩니다. 두 번째 주소 개체는 디바이스 ID 1에 바인딩됩니다.

**STEP 1 |** 하나의 HA 방화벽에서 주소 개체를 생성합니다.

1. 개체 > 주소를 선택하고 주소 개체 이름을 추가합니다(이 예에서는 Dyn-IP-Pool- 개발0.
2. 유형에 대해 **IP** 범위를 선택하고 범위 10.1.1.140-10.1.1.150을 입력합니다.
3. 확인을 클릭합니다.
4. 이 단계를 반복하여 **IP** 범위가 10.1.1.160-10.1.1.170인 Dyn-IP-Pool-dev1이라는 다른 주소 개체를 구성합니다.

**STEP 2 |** 디바이스 ID 0에 대한 소스 NAT 규칙을 생성합니다.

1. 정책 > **NAT**을 선택하고 이름이 있는 NAT 정책 규칙을 추가합니다(예: Src-NAT- dev0).
2. 원본 패킷의 경우 소스 영역에 대해 임의를 선택합니다.
3. 대상 영역에서 언트러스트와 같이 소스 주소를 변환할 대상 영역을 선택합니다.
4. 변환된 패킷의 경우 변환 유형으로 동적 **IP** 및 포트를 선택합니다.
5. 변환된 주소에 대해 디바이스 ID 0에 속하는 주소 풀에 대해 생성한 주소 개체를 추가합니다. Dyn-IP-Pool-dev0.
6. 능동형/능동형 **HA** 바인딩의 경우 **0**을 선택하여 NAT 규칙을 디바이스 ID 0에 바인딩합니다.
7. 확인을 클릭합니다.

**STEP 3 |** 디바이스 ID 1에 대한 소스 NAT 규칙을 생성합니다.

1. 정책 > **NAT**를 선택한 다음 이름이 있는 NAT 정책 규칙 추가를 선택합니다(예: Src-NAT-dev1).
2. 원본 패킷의 경우 소스 영역에 대해 임의를 선택합니다.
3. 대상 영역에서 언트러스트와 같이 소스 주소를 변환할 대상 영역을 선택합니다.
4. 변환된 패킷의 경우 변환 유형으로 동적 **IP** 및 포트를 선택합니다.
5. 변환된 주소에 대해 디바이스 ID 1에 속하는 주소 풀에 대해 생성한 주소 개체를 추가합니다. Dyn-IP-Pool-dev1.
6. 능동형/능동형 **HA** 바인딩의 경우 **1**을 선택하여 NAT 규칙을 디바이스 ID 1에 바인딩합니다.
7. 확인을 클릭합니다.

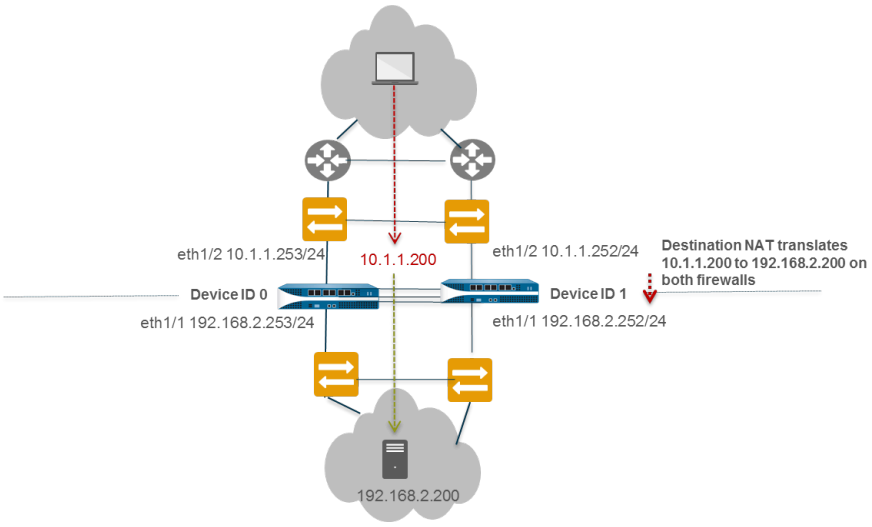
**STEP 4 |** 구성을 커밋합니다.

## 사용 사례: 대상 NAT를 사용하여 ARP 로드 공유를 위한 능동형/능동형 HA 구성

이 Layer 3 인터페이스 예제는 Active/Active HA 모드에서 NAT를 사용하고 대상 NAT가 있는 ARP 로드 공유를 사용합니다. 두 HA 방화벽 모두 수신 인터페이스 MAC 주소를 사용하여 대상 NAT 주소에 대한 ARP 요청에 응답합니다. 대상 NAT는 공용 공유 IP 주소(이 예에서는 10.1.1.200)를 서버의 사설 IP 주소(이 예에서는 192.168.2.200)로 변환합니다.

HA 방화벽이 대상 10.1.1.200에 대한 트래픽을 수신하면 두 방화벽이 모두 ARP 요청에 응답할 수 있어 네트워크가 불안정해질 수 있습니다. 잠재적인 문제를 방지하려면 대상 NAT 규칙을 능동형-기본 방화벽에 바인딩하여 ARP 요청에 응답하도록 능동형-기본 상태에 있는 방화벽을 구성합니다.

 ©2023 Palo Alto Networks, Inc.




**STEP 1 |** PA-3050-2(디바이스 ID 1)에서 활성/활성 HA 구성의 1단계부터 3단계까지 수행합니다.

**STEP 2 |** 능동형/능동형 HA를 활성화합니다.

1. 디바이스 > 고가용성 > 일반에서 설정을 편집합니다.
2. **HA** 활성화를 선택합니다.
3. 두 방화벽에 대해 동일해야 하는 그룹 **ID**를 입력합니다. 방화벽은 그룹 ID를 사용하여 가상 MAC 주소(범위는 1~63)를 계산합니다.
4. (선택 사항) 설명을 입력합니다.
5. 모드에서 활성 활성을 선택합니다.
6. 디바이스 **ID**를 **1**로 선택합니다.
7. 구성 동기화 활성화를 선택합니다. 이 설정은 두 방화벽 구성을 동기화하는 데 필요합니다(기본적으로 사용됨).
8. 피어 방화벽에 있는 HA1 제어 링크의 IP 주소인 피어 **HA1 IP** 주소를 입력합니다.
9. (선택 사항) 피어 방화벽의 백업 제어 링크의 IP 주소인 백업 피어 **HA1 IP** 주소를 입력합니다.
10. 확인을 클릭합니다.

**STEP 3 |** 능동형/능동형 HA 구성의 6~15단계를 수행합니다.

**STEP 4 |** HA 가상 주소를 구성합니다.

1. 디바이스 > 고가용성 > 활성/활성 구성 > 가상 주소를 선택하고 추가를 클릭합니다.
2. 인터페이스 eth1/1을 선택합니다.
3. **IPv4**를 선택하고 10.1.1.200의 **IPv4** 주소를 추가합니다.
4. **Type**에 대해 **ARP Load Sharing**을 선택합니다. 그러면 가상 IP 주소가 두 피어가 ARP Load-Sharing에 사용할 수 있도록 구성됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** ARP 로드 공유를 구성합니다.

디바이스 선택 알고리즘은 부하 공유를 제공하기 위해 ARP 요청에 응답하는 HA 방화벽을 결정합니다.

1. 디바이스 선택 알고리즘에 대해 **IP** 모듈로를 선택합니다. ARP 요청에 응답하는 방화벽은 ARP 요청자의 IP 주소의 패리티를 기반으로 합니다.
2. 확인을 클릭합니다.

**STEP 6 |** PA-7000 시리즈 이외의 방화벽에서 점보 프레임을 활성화합니다.

**STEP 7 |** HA 페일오버 조건을 정의합니다.

**STEP 8 |** 구성을 커밋합니다.

**STEP 9 |** 2단계에서 디바이스 **ID 0**를 선택하는 것을 제외하고 동일한 설정으로 피어 방화벽 PA-3050-1(디바이스 ID 0)을 구성합니다.

**STEP 10 |** PA-3050-1(디바이스 ID 0)에서 능동형-기본 방화벽이 ARP 요청에 응답하도록 대상 NAT 규칙을 생성합니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 이 예에서 레이어 2 ARP에 대한 대상 NAT 규칙으로 식별하는 규칙의 이름을 입력합니다.
3. **NAT** 유형으로 **ipv4**(기본값)를 선택합니다.
4. 소스 패킷에서 소스 영역에 대해 **Any**를 선택합니다.
5. 대상 영역에서 외부 네트워크용으로 생성한 Untrust 영역을 선택합니다.
6. 대상 인터페이스, 서비스 및 소스 주소가 모두로 설정된 상태를 유지하도록 허용합니다.
7. 대상 주소에 대해 10.1.1.200을 지정합니다.
8. 변환된 패킷의 경우 소스 주소 변환은 안 함으로 유지됩니다.
9. 대상 주소 변환의 경우 이 예제 192.168.1.200에서 대상 서버의 개인 IP 주소를 입력합니다.
10. 능동형/능동형 **HA** 바인딩 탭에서 능동형/능동형 **HA** 바인딩에 대해 기본을 선택하여 NAT 규칙을 능동형-기본 상태의 방화벽에 바인딩합니다.
11. 확인을 클릭합니다.

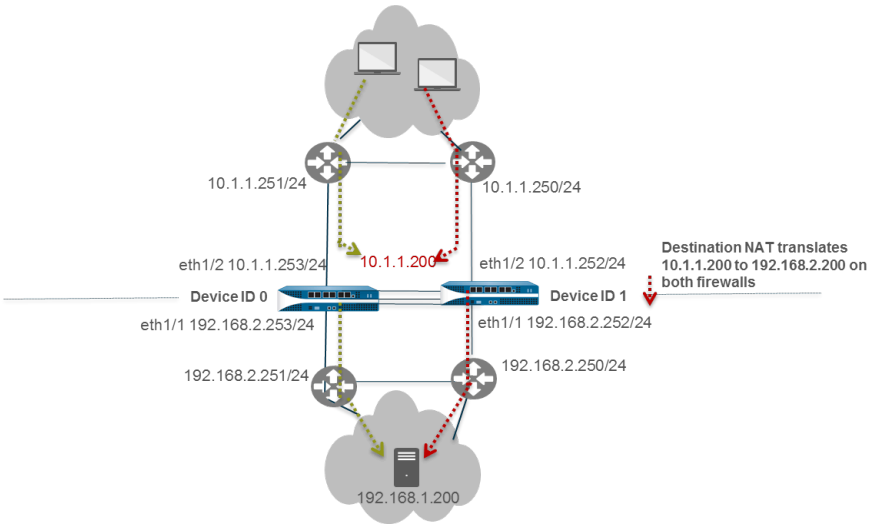
**STEP 11 |** 구성을 커밋합니다.

## 사용 사례: 레이어 3에서 대상 NAT를 사용하여 ARP 로드 공유에 대한 능동형/능동형 HA 구성

이 레이어 3 인터페이스 예제에서는 능동형/능동형 HA 모드 및 ARP 로드 쉐어링에서 NAT를 사용합니다. PA-3050-1에는 디바이스 ID 0이 있고 HA 피어인 PA-3050-2에는 디바이스 ID 1이 있습니다.

이 사용의 경우 두 HA 방화벽 모두 대상 NAT 주소에 대한 ARP 요청에 응답해야 합니다. 트래픽은 트러스트 해제 구역의 WAN 라우터중 하나에서 방화벽에 도달할 수 있습니다. 대상 NAT는 공용 IP 주소를 서버의 개인 IP 주소로 변환합니다. 구성에는 두 방화벽이 ARP 요청에 응답할 수 있도록 두 디바이스 ID에 바인딩된 하나의 대상 NAT 규칙이 필요합니다.

 ©2023 Palo Alto Networks, Inc.




**STEP 1 |** PA-3050-2(디바이스 ID 1)에서 능동형/능동형 HA 구성의 1단계부터 3단계까지 수행합니다.

**STEP 2 |** 능동형/능동형 HA를 활성화합니다.

1. 디바이스 > 고가용성 > 일반 > 설정을 선택하고 수정합니다.
2. **HA** 활성화를 선택합니다.
3. 두 방화벽에 대해 동일해야 하는 그룹 **ID**를 입력합니다. 방화벽은 그룹 ID를 사용하여 가상 MAC 주소(범위는 1~63)를 계산합니다.
4. (선택 사항) 설명을 입력합니다.
5. 모드에서 활성 활성을 선택합니다.
6. 디바이스 **ID**를 **1**로 선택합니다.
7. 구성 동기화 활성화를 선택합니다. 이 설정은 두 방화벽 구성을 동기화하는 데 필요합니다(기본적으로 사용됨).
8. 피어 방화벽에 있는 HA1 제어 링크의 IP 주소인 피어 **HA1 IP** 주소를 입력합니다.
9. ( 선택사항) 피어 방화벽에 있는 백업 제어 링크의 IP 주소인 백업 피어 **HA1 IP** 주소를 입력합니다.
10. 확인을 클릭합니다.

**STEP 3 |** 활성/활성 HA를 구성합니다.

6단계부터 15단계까지 수행합니다.

**STEP 4 |** HA 가상 주소를 구성합니다.

1. 디바이스 > 고가용성 > 활성/활성 구성 > 가상 주소를 선택하고 추가를 클릭합니다.
2. 인터페이스 eth1/2를 선택합니다.
3. **IPv4**를 선택하고 10.1.1.200의 **IPv4** 주소를 추가합니다.
4. **Type**에 대해 **ARP Load Sharing**을 선택합니다. 그러면 가상 IP 주소가 두 피어가 ARP Load-Sharing에 사용할 수 있도록 구성됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** ARP 로드 공유를 구성합니다.

디바이스 선택 알고리즘은 부하 공유를 제공하기 위해 ARP 요청에 응답하는 HA 방화벽을 결정합니다.

1. 디바이스 선택 알고리즘에 대해 다음 중 하나를 선택합니다.
   - **IP Modulo** - ARP 요청에 응답하는 방화벽은 ARP 요청자의 IP 주소 패리티를 기반으로 합니다.
   - **IP** 해시 - ARP 요청에 응답하는 방화벽은 ARP 요청자의 소스 IP 주소와 대상 IP 주소의 해시를 기반으로 합니다.
2. 확인을 클릭합니다.

**STEP 6 |** PA-7000 시리즈 방화벽 이외의 방화벽에서 점보 프레임을 활성화합니다.

**STEP 7 |** HA 페일오버 조건을 정의합니다.

**STEP 8 |** 구성을 커밋합니다.

**STEP 9 |** 디바이스 **ID**를 **1**이 아닌 **0**으로 설정하는 것을 제외하고 동일한 설정으로 피어 방화벽 PA-3050-1(디바이스 ID 0)을 구성합니다.

**STEP 10 |** 여전히 PA-3050-1(디바이스 ID 0)에서 디바이스 ID 0과 디바이스 ID 1 모두에 대한 대상 NAT 규칙을 생성합니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 이 예에서 레이어 3 ARP에 대한 대상 NAT 규칙으로 식별하는 규칙의 이름을 입력합니다.
3. **NAT** 유형으로 **ipv4**(기본값)를 선택합니다.
4. 소스 패킷에서 소스 영역에 대해 **Any**를 선택합니다.
5. 대상 영역에서 외부 네트워크용으로 생성한 Untrust 영역을 선택합니다.
6. 대상 인터페이스, 서비스 및 소스 주소가 모두로 설정된 상태를 유지하도록 허용합니다.
7. 대상 주소에 대해 10.1.1.200을 지정합니다.
8. 변환된 패킷의 경우 소스 주소 변환은 안 함으로 유지됩니다.
9. 대상 주소 변환의 경우 이 예제 192.168.1.200에서 대상 서버의 개인 IP 주소를 입력합니다.
10. 능동형/능동형 **HA** 바인딩 탭에서 능동형/능동형 **HA** 바인딩의 경우 NAT 규칙을 디바이스 ID 0과 디바이스 ID 1에 모두 바인딩하도록 선택합니다.
11. 확인을 클릭합니다.

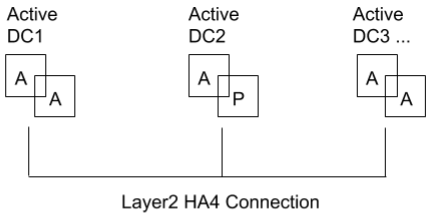
**STEP 11 |** 구성을 커밋합니다.

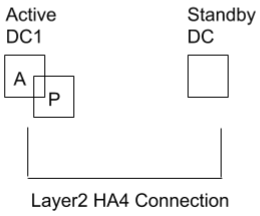

©2023 Palo Alto Networks, Inc.

# HA 클러스터링 개요

다수의 Palo Alto Networks® 방화벽 모델은 이제 최대 16개 방화벽의 고가용성(HA) 클러스터에서 방화벽 간의 세션 상태 동기화를 지원합니다. HA 클러스터 피어는 세션을 동기화하여 데이터 센터 또는 수평 확장 방화벽이 있는 대규모 보안 검사 지점의 장애로부터 보호합니다. 네트워크 중단 또는 방화벽이 다운되는 경우 세션은 클러스터의 다른 방화벽으로 페일오버됩니다. 이러한 동기화는 다음 사용 사례에서 특히 유용합니다.

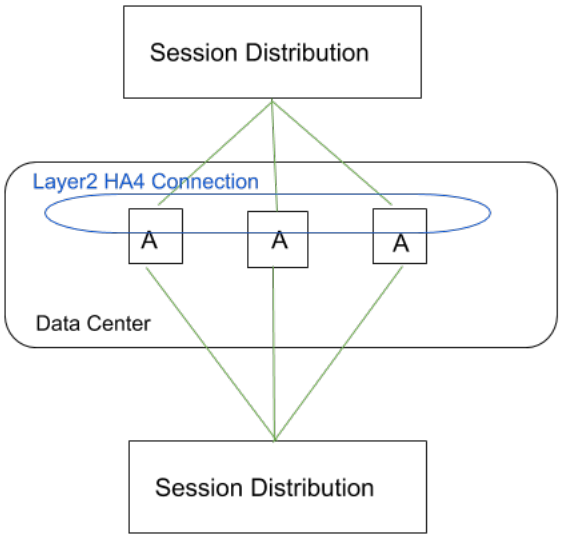
한 가지 사용 사례는 HA 피어가 여러 데이터 센터에 분산되어 데이터 센터 내 또는 데이터 센터 간에 단일 장애 지점이 없는 경우입니다. 두 번째 다중 데이터 센터 사용 사례는 한 데이터 센터가 활성 상태이고 다른 데이터 센터가 대기 상태인 경우입니다.




세 번째 HA 클러스터링 사용 사례는 수평적 확장으로, 단일 데이터 센터에 HA 클러스터 구성원을 추가하여 보안을 확장하고 세션 생존성을 보장합니다.


©2023 Palo Alto Networks, Inc.




HA 클러스터는 레이어 3 또는 가상 와이어 배포를 지원합니다. 클러스터의 HA 피어는 HA 쌍과 독립 실행형 클러스터 구성원의 조합일 수 있습니다. HA 클러스터에서 모든 구성원은 활성으로 간주됩니다. HA 클러스터에 추가한 후 능동형/수동형 관계를 유지할 수 있는 HA 쌍을 제외하고는 수동형 방화벽의 개념이 없습니다.

모든 클러스터 구성원은 세션 상태를 공유합니다. 새 방화벽이 HA 클러스터에 가입하면 클러스터의 모든 방화벽이 모든 기존 세션을 동기화하도록 트리거합니다. HA4 및 HA4 백업 연결은 동일한 클러스터 ID를 가진 모든 클러스터 구성원 간에 세션 상태를 동기화하는 전용 클러스터 링크입니다. 클러스터 구성원 간의 HA4 링크는 클러스터 구성원 간의 연결 실패를 감지합니다. HA1(제어 링크), HA2(데이터 링크) 및 HA3(패킷 포워딩 링크)은 HA 쌍이 아닌 클러스터 구성원 간에 지원되지 않습니다.

페일오버되지 않은 일반 세션의 경우 세션 소유자인 방화벽만 트래픽 로그를 생성합니다. 페일오버된 세션의 경우 새 세션 소유자(페일오버된 트래픽을 수신하는 방화벽)가 트래픽 로그를 생성합니다.

HA 클러스터링을 지원하는 방화벽 모델과 클러스터당 지원되는 최대 구성원 수는 다음과 같습니다.

| 방화벽 모델 | 클러스터당 지원되는 구성원 수 |
|---|---|
| PA-3200 시리즈 | 6 |
| PA-3400 시리즈 | 6 |
| PA-5200 시리즈 | 16 |
| PA-5400 시리즈 | 8 |
| 다음 카드 중 하나 이상이 있는 PA-7000 시리즈 방화벽: PA-7000-100G-NPC, PA-7000-20GQXM-NPC, PA-7000-20GXM-NPC | PA-7080: 4<br>PA-7050: 6 |


©2023 Palo Alto Networks, Inc.

| 방화벽 모델 | 클러스터당 지원되는 구성원 수 |
|---|---|
| VM-300 | 6 |
| VM-500 | 6 |
| VM-700 | 16 |

HA 클러스터링은 퍼블릭 클라우드 배포에서 지원되지 않습니다. HA 클러스터링 구성을(를) 시작하기 전에 HA 클러스터링 모범 사례 및 프로비저닝을(를) 고려하십시오.


©2023 Palo Alto Networks, Inc.

# HA 클러스터링 모범 사례 및 프로비저닝

다음은 HA 클러스터링에 대한 프로비저닝 요구 사항 및 모범 사례입니다.

- 프로비저닝 요구 사항 및 모범 사례
  - HA 클러스터 멤버는 동일한 방화벽 모델이어야 하며 동일한 PAN-OS® 버전을 실행해야 합니다.

    업그레이드할 때 방화벽 구성원은 다른 버전의 한 구성원과 세션을 계속 동기화합니다.
  - 모든 클러스터 구성원 간에 동기화된 모든 구성 및 정책을 유지하려면 Panorama를 사용하여 HA 클러스터 구성원을 프로비저닝하는 것이 좋습니다.
  - 일관된 정책 시행 및 콘텐츠 검사 기능을 보장하려면 HA 클러스터 구성원에게 동일한 구성 요소에 대한 라이선스가 있어야 합니다.
  - 라이선스 불일치 및 기능 손실을 방지하려면 라이선스가 동시에 만료되어야 합니다.
  - 모든 클러스터 구성원은 일관된 보안 적용을 위해 동일한 버전의 동적 콘텐츠 업데이트로 실행되어야 합니다.
  - 세션이 다른 클러스터 구성원으로 성공적으로 페일오버하려면 HA 클러스터 구성원이 동일한 영역 이름을 공유해야 합니다. 예를 들어 링크가 다운되어 **internal**이라는 수신 영역으로 이동하는 세션이 삭제되었다고 가정합니다. 해당 세션이 클러스터의 HA 방화벽 피어로 페일오버하려면 해당 피어에 **internal**이라는 영역도 있어야 합니다.
  - 클라이언트-서버 및 서버-클라이언트 흐름은 보안 콘텐츠 스캔이 발생하기 위해 정상(비장애) 조건에서 동일한 방화벽으로 돌아가야 합니다. 비대칭 트래픽은 삭제되지 않지만 보안을 위해 스캔할 수는 없습니다.
- 세션 동기화 모범 사례
  - 전용 HA 통신 인터페이스는 데이터플레인 인터페이스를 통해 사용해야 합니다. HSCI 인터페이스는 HA4에 사용되지 않습니다. 이를 통해 HA 쌍과 클러스터 세션 동기화를 분리하여 세션 동기화를 위한 최대 대역폭과 안정성을 보장할 수 있습니다.
  - 데이터플레인 인터페이스를 사용하는 경우 HA4의 크기가 적절해야 합니다. 이렇게 하면 클러스터 구성원 간에 동기화되는 최상의 세션 상태가 보장됩니다.
  - 모범 사례는 HA4 통신 링크를 위한 전용 클러스터 네트워크를 사용하여 클러스터 구성원 간에 적절한 대역폭과 정체되지 않고 대기 시간이 짧은 연결을 보장하는 것입니다.
  - 네트워크를 설계하고 트래픽 엔지니어링을 수행하여 세션이 방화벽 간에 성공적으로 동기화되기 전에 네트워크가 세션 소유자에서 클러스터 구성원으로 트래픽을 조정하는 가능한 경쟁 조건을 방지합니다. Layer2 HA4 연결은 HA 구성원 간의 시기적절한 동기화를 허용하기 위해 충분한 대역폭과 짧은 대기 시간을 가져야 합니다. HA4 대기 시간은 피어링 디바이스가 클러스터 구성원 간에 트래픽을 전환할 때 발생하는 대기 시간보다 낮아야 합니다.
  - 비대칭 흐름을 최소화하도록 네트워크를 설계하십시오. 세션 설정에는 완전한 TCP 3방향 핸드쉐이크를 보려면 클러스터 구성원 한 명이 필요합니다.


©2023 Palo Alto Networks, Inc.

- 상태 확인 모범 사례
  - 클러스터의 HA 쌍에서 HA1, HA2 및 HA4에 대한 HA 백업 통신 링크를 사용하여 활성/수동 쌍을 구성합니다. HA1, HA2, HA3 및 HA4에 대한 HA 백업 통신 링크를 사용하여 능동형/활성 쌍을 구성합니다.
  - 모든 클러스터 멤버에서 HA4 백업 링크를 구성합니다.


©2023 Palo Alto Networks, Inc.

# HA 클러스터링 구성

HA 클러스터링에 대해 알아보고 HA 클러스터링 모범 사례 및 프로비저닝 HA 방화벽을 클러스터의 구성원으로 구성하기 전에 다음을 따릅니다.

**STEP 1 |** 인터페이스를 HA 인터페이스로 설정합니다(추후에 HA4 링크로 할당).

1. 네트워크 > 인터페이스 > 이더넷을 선택한 다음 인터페이스를 선택합니다(예: ethernet1/1).
2. **HA**로 인터페이스 유형을 선택합니다.
3. 확인을 클릭합니다.
4. 이 단계를 반복하여 HA4 백업 링크로 사용할 다른 인터페이스를 구성합니다.

**STEP 2 |** HA 클러스터링을 사용하도록 설정합니다.

1. 디바이스 > 고가용성 > 일반을 선택한 다음 클러스터링 설정을 편집합니다.
2. 클러스터 참여를 활성화합니다.
3. 모든 구성원이 세션 상태를 공유할 수 있는 HA 클러스터의 고유한 숫자 ID인 클러스터 **ID**를 입력합니다. 범위는 1~99입니다.
4. 짧고 유용한 클러스터 설명을 입력합니다.
5. (선택 사항) 클러스터 동기화 타임아웃**(min)** 변경은 다른 클러스터 멤버(예: 알 수 없는 상태)가 클러스터를 완전히 동기화되지 못하도록 하는 경우 로컬 방화벽이 활성 상태로 가기 전에 대기하는 최대 시간(분)이며, 범위는 0-30이며, 기본값은 0입니다.
6. (선택 사항) 모니터 실패 보류 종료 시간**(분)**을 변경하며, 이는 다운 링크가 백업되어 있는지 확인하기 위해 다시 테스트된 시간(분)입니다(범위는 1 ~ 60, 기본값은 1).
7. 확인을 클릭합니다.

**STEP 3 |** HA4 링크를 구성합니다.

1. **HA** 통신을 선택한 다음 클러스터링 링크 섹션에서 HA4 섹션을 편집합니다.
2. 첫 번째 단계에서 구성한 인터페이스를 HA4 링크의 포트가 될 **HA** 인터페이스로 선택합니다(예: ethernet1/1).
3. 로컬 HA4 인터페이스의 **IPv4/IPv6** 주소를 입력합니다.
4. 넷마스크를 입력합니다.
5. (선택 사항) **HA4** 유지  임계값**(ms)**을 변경하여 클러스터 멤버가 작동하고 있다는 것을 알기 위해 클러스터 멤버로부터 유지를 받아야 하는 기간을 지정합니다. 범위는 5,000에서 60,000사이, 기본값은 10,000입니다.
6. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** HA4 백업 링크를 구성합니다.

1. HA4 백업 섹션을 편집합니다.
2. 첫 번째 단계에서 구성한 다른 인터페이스를 HA4 백업 링크의 포트가 될 **HA** 인터페이스로 선택합니다.
3. 로컬 HA4 백업 인터페이스의 **IPv4/IPv6** 주소를 입력합니다.
4. 넷마스크를 입력합니다.
5. 확인을 클릭합니다.

**STEP 5 |** HA 쌍의 로컬 멤버와 HA 피어를 포함한 HA 클러스터의 모든 멤버를 지정합니다.

1. 클러스터 구성을 선택합니다.
2. (지원되는 방화벽에서) 피어 멤버의 디바이스 일련번호를 추가합니다.
3. (Panorama) 드롭다운에서 디바이스를 추가하고 선택한 다음 디바이스 이름을 입력합니다.
4. 클러스터에서 HA 피어의 **HA4 IP** 주소를 입력합니다.
5. 클러스터에 HA 피어의 **HA4** 백업 **IP** 주소를 입력합니다.
6. 식별한 피어와 세션 동기화를 활성화합니다.
7. (선택 사항) 유용한 설명을 입력합니다.
8. 확인을 클릭합니다.
9. 디바이스를 선택한 다음 사용하도록 설정합니다.

**STEP 6 |** 링크 및 경로 모니터링을 통해 HA 페일오버 조건을 정의합니다.

**STEP 7 |** 커밋합니다.

**STEP 8 |** (Panorama 전용) HA 클러스터에서 HA 방화벽 목록을 새로 고칩니다.

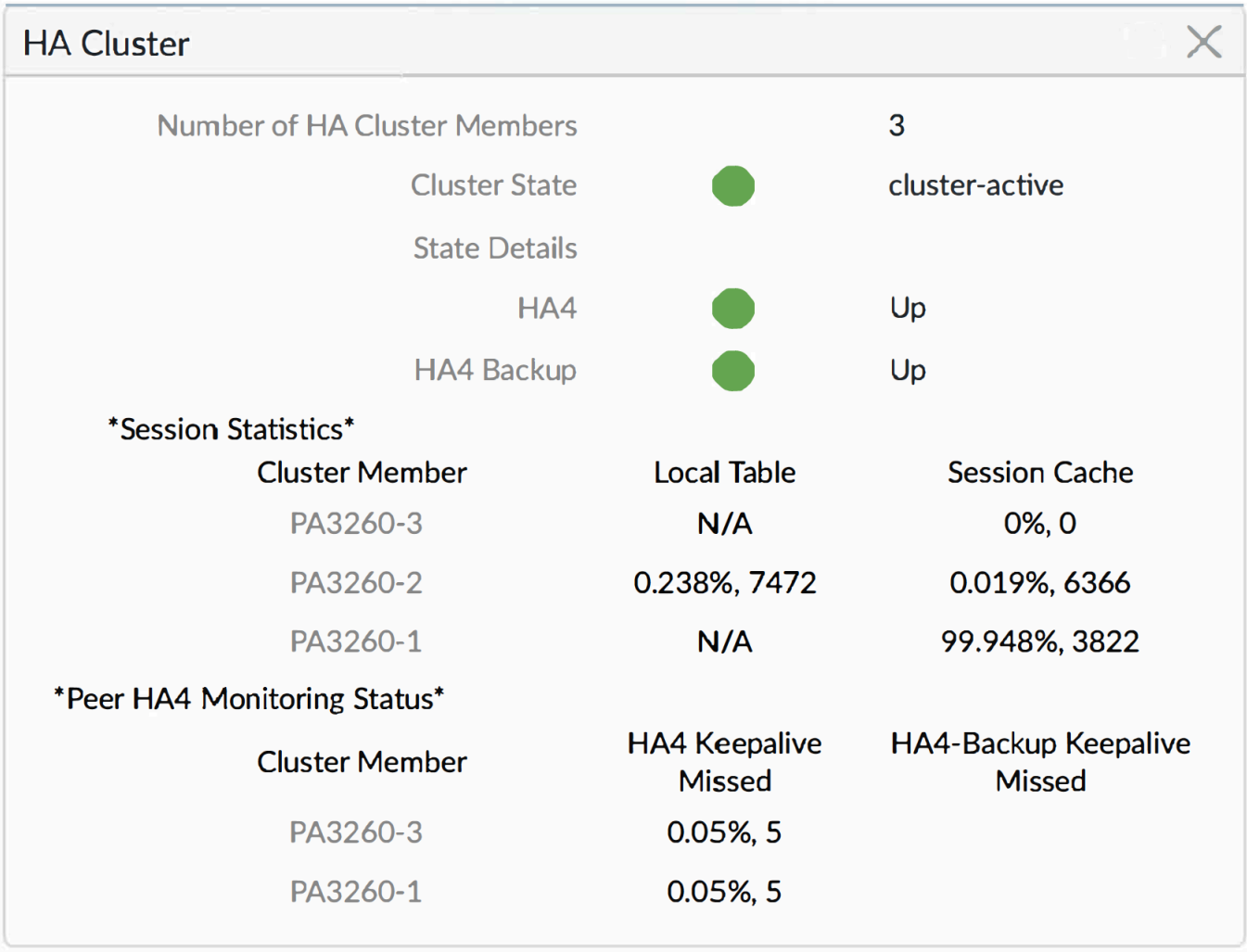
1. 템플릿에서 디바이스 > 고가용성 > 클러스터 구성을 선택합니다.
2. 화면 하단에서 새로 고침을 클릭합니다.

**STEP 9 |** UI에서 HA 클러스터 정보를 봅니다.

1. 대시보드를 선택합니다.
2. HA 클러스터 필드를 봅니다. 위쪽 섹션에는 클러스터 상태와 HA4 연결을 표시하여 클러스터 상태를 한눈에 제공합니다. HA4 및 HA4 백업 표시기는 다음 중 하나가 됩니다. 녹색은 클러스터 멤버의 링크 상태가 최대임을 나타냅니다. 빨간색은 모든 클러스터 멤버의 링크 상태가 다운됨을 나타냅니다. 노란색은 다른 클러스터 멤버의 상태가 다운되는 동안 일부 클러스터 구성원의 링크 상태가 위로 있음을 나타냅니다. 회색은 구성되지 않음을 나타냅니다. 중앙 섹션에는 로컬 세션 테이블 및 세션 캐시 테이블의 용량이 표시되므로 테이블의 전체를 모니터링하고 방화

 ©2023 Palo Alto Networks, Inc.

벽 업그레이드를 계획할 수 있습니다. 아래 쪽 섹션은 HA4 및 HA4 백업 링크의 통신 오류를 표시하여 구성원 간의 정보를 동기화하는 데 문제가 발생할 수 있습니다.


HA Cluster

| | | |
|---|---|---|
| Number of HA Cluster Members | | 3 |
| Cluster State | | cluster-active |
| State Details | | |
| HA4 | | Up |
| HA4 Backup | | Up |

*Session Statistics*

| Cluster Member | Local Table | Session Cache |
|---|---|---|
| PA3260-3 | N/A | 0%, 0 |
| PA3260-2 | 0.238%, 7472 | 0.019%, 6366 |
| PA3260-1 | N/A | 99.948%, 3822 |

*Peer HA4 Monitoring Status*

| Cluster Member | HA4 Keepalive Missed | HA4-Backup Keepalive Missed |
|---|---|---|
| PA3260-3 | 0.05%, 5 | |
| PA3260-1 | 0.05%, 5 | |

**STEP 10 |** CLI에 액세스하여 HA 클러스터 및 HA4 링크 정보를 보고 다른 HA 클러스터링 작업을 수행합니다.

*HA* 클러스터 플랩 통계를 볼 수 있습니다. *HA* 디바이스가 일시 중단된 기능으로 이동하면 클러스터 플랩 수가 재설정되고 그 반대의 경우도 마찬가지입니다. 클러스터 플랩 카운트는 작동하지 않는 보류 시간이 만료되면 재설정됩니다.


©2023 Palo Alto Networks, Inc.

# HA1 SSH 키 새로 고침 및 키 옵션 구성

모든 Palo Alto Networks 방화벽에는 SSH(보안 쉘) 사전 구성된 방화벽이 있으며 HA(고가용성) 방화벽은 동시에 SSH 서버 및 SSH 클라이언트 역할을 할 수 있습니다. 능동형/수동형 또는 능동형/능동형 HA를 구성할 때 HA 방화벽 간의 HA1(제어 링크) 연결에 대한 암호화를 사용하도록 설정할 수 있습니다. 특히 방화벽이 동일한 사이트에 없는 경우 HA 피어 간의 암호화를 통해 HA1 트래픽을 보호하는 것이 좋습니다. HA1 제어 링크에서 암호화를 활성화한 후 CLI를 사용하여 SSH 서비스 프로파일을 생성하고 HA 방화벽 간의 연결을 보호할 수 있습니다.

SSH 서비스 프로파일을 사용하면 기본 호스트 키 유형을 변경하고, HA1 제어 링크에 대한 새 공용 및 비공개 SSH 호스트 키 쌍을 생성하고, 다른 SSH HA1 설정을 구성할 수 있습니다. HA 피어를 다시 시작하지 않고 새 호스트 키와 구성된 설정을 방화벽에 적용할 수 있습니다. 방화벽은 피어로 HA1 세션을 다시 설정하여 구성 변경 내용을 동기화합니다. 또한 HA1 및 HA1 백업 세션을 다시 설정하기 위한 시스템 로그(하위 유형은 **ha**)를 생성합니다.

다음 예제에서는 암호화를 활성화하고 CLI에 액세스한 후 HA1에 대한 다양한 SSH 설정을 구성하는 방법을 보여 줍니다. (SSH 관리 서버 프로파일의 예는 SSH 키 새로 고침 및 관리 인터페이스 연결을 위한 키 옵션 구성을 참조하십시오.)

암호화를 사용하도록 설정해야 하며 다음 작업을 수행하기 전에 ***HA*** 쌍에서 제대로 작동해야 합니다.

FIPS-CC 모드에서, ***HA1*** 제어 링크를 구성하는 경우 세션 키에 대한 자동 키 재조정***(rekeying)*** 매개 변수를 설정해야 합니다.

컬렉터 그룹의 각 전용 로그 컬렉터***(***로그 컬렉터 모드의 ***M*** 시리즈 또는 ***Panorama*** 가상 어플라이언스***)***에 대해 동일한 ***SSH*** 연결 설정을 사용하려면 ***Panorama*** 관리 서버에서 ***SSH*** 서비스 프로파일을 구성하고, 변경 내용을 ***Panorama***로 커밋한 다음 로그 컬렉터로 구성을 푸시합니다. ***set log-collector-group <name> general-setting management ssh*** 명령을 사용할 수 있습니다.

- SSH 서비스 프로파일을 만들어 HA 방화벽 간의 SSH 연결을 보다 잘 제어할 수 있습니다.

  이 예제는 설정을 구성하지 않고 HA 프로파일을 생성합니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*>**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. 새 프로파일이 만들어졌는지 확인하고 기존 프로파일에 대한 설정을 보려면 다음을 수행합니다.

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles**


©2023 Palo Alto Networks, Inc.

- (선택사항)SSH 서버를 설정하여 HA1 세션에 지정된 암호화 암호(cipher)만 사용합니다.

  기본적으로 HA1 SSH는 CLI HA 세션의 암호화를 위해 지원되는 모든 암호를 허용합니다. 하나 이상의 암호를 설정하면 SSH 서버는 연결하는 동안 해당 암호만 광고하고 SSH 클라이언트(HA 피어)가 다른 암호를 사용하여 연결하려고 하면 서버가 연결을 종료합니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ciphers ha-profiles *<name>* ciphers *<cipher>***

     **aes128-cbc**—암호 블록 체인을 가진 AES 128 비트 암호

     **aes128-ctr**—카운터 모드가 있는 AES 128비트 암호

     **Aes128-gcm**—GCM이 있는 AES 128비트 암호(갈로이스/카운터 모드)

     **aes192-cbc**—암호 블록 체인을 가진 AES 192 비트 암호

     **Aes192-ctr**—카운터 모드가 있는 AES 192비트 암호

     **aes256-cbc**—암호 블록 체인을 가진 AES 256 비트 암호

     **aes256-ctr** - 카운터 모드가 있는 AES 256비트 암호

     **Aes256-gcm**—GCM이 있는 AES 256비트 암호
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
  6. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

     *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으므로 *HA* 피어 간에 간단한 스플릿 브레인*(split brain)* 상태가 발생합니다. *(HA1* 백업이 구성될 때 힘 옵션을 사용하면 아무런 효과가 없습니다.*)*
  7. 암호가 업데이트되었는지 확인하려면 다음을 수행합니다.

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles ciphers**

- (선택 사항) 기본 호스트 키 유형을 설정합니다.

  HA1 제어 링크에서 암호화를 사용하도록 설정하면 방화벽은 변경하지 않는 한 기본 호스트 키 유형의 RSA 2048을 사용합니다. HA1 SSH 연결은 **기본 호스트 키 유형**만 사용하여 HA 피어를 인증합니다(암호화된 세션이 그 사이에 설정되기 전에). 기본 호스트 키 형식을 변경할 수 있습니다. 선택 사항은 ECDSA 256, 384 또는 521 또는 RSA 2048, 3072 또는 4096입니다. RSA 키 길이가 길어지거나 RSA가 아닌 ECDSA를 선호하는 경우 기본 호스트 키 유형을 변경합니다. 이 예제는 기본 호스트 키 유

 ©2023 Palo Alto Networks, Inc.

형을 256비트의 ECDSA 키로 설정합니다. 또한 HA 피어를 다시 시작하지 않고 새 호스트 키를 사용하여 HA1 연결을 다시 설정합니다.

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> default-hostkey key-type ECDSA key-length 256**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   *HA* 방화벽 간에 *HA* 연결을 이미 설정해야 합니다. 방화벽이 아직 *HA* 연결을 설정하지 않은 경우 제어 링크 연결에서 암호화를 사용하도록 설정하고 *HA* 키를 네트워크 위치로 내보내고 피어에서 *HA* 키를 가져와야 합니다. 능동형/수동형 *HA* 구성 또는 능동형/능동형 HA구성을 참조하십시오.
6. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
7. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

   *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으며, 이로 인해 두 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. (*HA1* 백업이 구성될 때 **힘** 옵션을 사용하면 아무런 효과가 없습니다.)
8. 호스트 키가 업데이트되었는지 확인하려면 다음을 수행합니다.

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> default-hostkey**


©2023 Palo Alto Networks, Inc.

- (선택사항)HA1 컨트롤 링크를 통해 SSH에 대해 선택한 암호 집합에서 암호를 삭제합니다.

  이 예제는 128비트 키로 AES CBC 암호를 삭제합니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **delete deviceconfig system ssh profiles ha-profiles <*name*> ciphers aes128-cbc**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
  6. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

     *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으며, 이로 인해 두 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. (*HA1* 백업이 구성될 때 강제 옵션을 사용하면 아무 효과가 없습니다.

  7. 암호가 삭제되었는지 확인하려면 다음을 수행합니다.

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> ciphers**


©2023 Palo Alto Networks, Inc.

- (선택사항)HA1 SSH 서버가 지원하는 세션 키 교환 알고리즘을 설정합니다.

  기본적으로 HA 서버(HA 방화벽)는 모든 키 교환 알고리즘을 HA 피어 방화벽에 광고합니다.

  *ECDSA* 기본 키 형식을 사용하는 경우 *ECDH* 키 알고리즘을 사용하는 것이 가장 좋습니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> kex <*value*>**

     **diffie-hellman-group14-sha1**—SHA1 해시가 있는 Diffie-Hellman 그룹 14

     **ecdh-sha2-nistp256**—SHA2-256 해시를 사용하는 NIST(National Institute of Standards and Technology) P-256에 대한 타원 곡선 Diffie-Hellman

     **ecdh-sha2-nistp384**—SHA2-384 해시를 사용하는 NIST P-384를 통한 타원 곡선 Diffie-Hellman

     **ecdh-sha2-nistp521**—SHA2-521 해시를 사용하는 NIST P-521에 대한 타원 곡선 Diffie-Hellman
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
  6. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

     *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으며, 이로 인해 두 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. (*HA1* 백업이 구성될 때 **강제** 옵션을 사용하면 아무 효과가 없습니다.
  7. 키 교환 알고리즘이 업데이트되었는지 확인하려면 다음을 수행합니다.

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**


©2023 Palo Alto Networks, Inc.

- (선택사항)HA1 SSH 서버가 지원하는 메시지 인증 코드(MAC)를 설정합니다.

  기본적으로 서버는 모든 MAC 알고리즘을 클라이언트에 알립니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> mac <*value*>**

     **hmac-sha1**—SHA1 암호화 해시와 MAC

     **hmac-sha2-256**—SHA2-256 암호화 해시와 MAC

     **hmac-sha2-512**—SHA2-512 암호화 해시와 MAC
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
  6. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

     *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으며, 이로 인해 두 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. *(강제* 옵션을 사용하면 *HA1* 백업이 구성될 때 아무런 영향을 주지 않습니다.
  7. MAC 알고리즘이 업데이트되었는지 확인하려면 다음을 수행합니다.

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**


©2023 Palo Alto Networks, Inc.

- (선택사항) HA1 SSH에 대한 ECDSA 또는 RSA 호스트 키를 재생하여 기존 키를 교체하고 HA 피어를 다시 시작하지 않고 새 키를 사용하여 HA 피어 간에 HA1 세션을 다시 설정합니다.

  HA 피어는 호스트 키를 사용하여 서로를 인증합니다. 이 예제는 ECDSA 256 기본 호스트 키를 재생합니다.

  호스트 키를 재생해도 기본 호스트 키 유형이 변경되지 않습니다. 사용 중인 기본 호스트 키를 다시 생성하려면 재생생성시 기본 호스트 키 유형과 길이를 지정해야 합니다. 기본 호스트 키 유형이 아닌 호스트 키를 재생하면 사용하지 않는 키가 재생되므로 효과가 없습니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh regenerate-hostkeys ha key-type ECDSA key-length 256**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

     *HA* 방화벽 간에 *HA* 연결을 이미 설정해야 합니다. 방화벽이 아직 *HA* 연결을 설정하지 않은 경우 제어 링크 연결에서 암호화를 사용하도록 설정하고 *HA* 키를 네트워크 위치로 내보내고 피어에서 *HA* 키를 가져와야 합니다. 능동형/수동형 *HA* 구성 또는 능동형/능동형 HA구성을 참조하십시오.
  6. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
  7. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

     *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으며, 이로 인해 두 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. *(HA1* 백업이 구성될 때 **힘** 옵션을 사용하면 아무런 효과가 없습니다.*)*

- (선택사항)HA1 컨트롤 링크를 통해 SSH에 대해 세션 키의 자동 키 재설정(rekey)링이 발생할 때를 설정하도록 키 재설정(rekeying) 매개 변수를 설정합니다.

  세션 키는 HA 피어 간의 트래픽을 암호화하는 데 사용됩니다. 설정할 수 있는 매개 변수는 데이터 볼륨(메가바이트), 시간 인터벌(초), 패킷 수입니다. 하나의 키 재설정(rekey) 매개 변수가 구성된 값에 도달하면 SSH는 키 교환을 시작합니다.

  재구성한 매개 변수가 키 재설정(rekeying)이 발생하자마자 해당 값에 도달할지 확실하지 않은 경우 두 번째 또는 세 번째 매개 변수를 설정할 수 있습니다. 구성된 값에 도달하는 첫 번째 매개 변수는 키 재설정(rekeying)을 프롬프트한 다음 방화벽이 모든 키 재설정(rekey) 매개 변수를 재설정합니다.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data 32**

     키 재설정(rekey)은 이전 키 재설정(rekey) 다음에 데이터 볼륨(메가바이트)이 전송된 후에 발생합니다. 기본값은 사용하는 암호를 기반으로 하며 범위는 1GB에서 4GB까지입니다. 범위는

 ©2023 Palo Alto Networks, Inc.

10MB ~ 4,000MB입니다. 또는 **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data default** 명령을 입력할 수 있으며, 데이터 매개변수를 사용 중인 개별 암호의 기본값으로 설정합니다.

3. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey interval 3600**

   키 재설정(rekey)은 이전 키 재설정(rekey) 다음에 지정된 시간 인터벌(초)이 지나간 후에 발생합니다. 기본적으로 시간 기반 키 재설정(rekey)이 비활성화됩니다(없음으로 설정됨). 범위는 10 ~ 3,600입니다.

4. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey packets 27**

   키 재설정(rekey)은 정의된 패킷수($2^n$)가 이전 키 재설정(rekey) 다음에 전송된 후에 발생합니다. 예를 들어 14는 키 재입력이 발생하기 전에 최대 $2^{14}$ 패킷이 전송되도록 구성합니다. 기본값은 $2^{28}$입니다. 범위는 12에서 27($2^{12}$에서 $2^{27}$)입니다. 또는 **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey packages default**를 입력하여 패킷 매개변수를 $2^{28}$로 설정할 수 있습니다.

   트래픽 및 네트워크 속도 유형에 따라 재키 매개 변수를 선택합니다*(FIPS-CC* 요구 사항 이외에 해당 변수가 귀하에게 적용됩니다*).* 매개 변수를 너무 낮게 설정하여 *SSH* 성능에 영향을 미치지 마십시오.

5. admin@PA-3250# **commit**
6. admin@PA-3250# **exit**
7. (HA1 백업 구성됨) admin@PA-3250> **request high-availability session-reestablish**
8. (HA1 백업이 구성되지 않았거나 HA1 백업 링크가 다운됨) admin@PA-3250> **request high-availability session-reestablish force**

   *HA1* 백업이 없는 경우 방화벽이 *HA1* 세션을 다시 설정하도록 강제할 수 있으며, 이로 인해 두 *HA* 피어 간에 짧은 분할 브레인 상태가 발생합니다. *(HA1* 백업이 구성될 때 **힘** 옵션을 사용하면 아무런 효과가 없습니다.*)*

9. 변경 내용을 확인하려면 다음을 수행합니다.

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> session-rekey**


©2023 Palo Alto Networks, Inc.

- 프로파일을 선택한 다음 HA1 SSH 서비스를 다시 시작하여 프로파일을 활성화합니다.
  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh ha ha-profile <*name*>**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **set ssh service-restart ha**
  6. 올바른 프로파일이 사용 중인지 확인하려면 다음을 수행합니다.

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh ha**


©2023 Palo Alto Networks, Inc.

# HA 방화벽 상태

HA 방화벽은 다음 상태 중 하나에 있을 수 있습니다.

| **HA** 방화벽 상태 | 다음의 경우 발생 | 설명 |
|---|---|---|
| 1차 | A/P 또는 A/A | HA 쌍에 조인할 때 방화벽의 일시적인 상태입니다. 방화벽은 피어를 발견하고 협상이 시작될 때까지 부팅 후 이 상태로 유지됩니다. 타임아웃 이후에 HA 협상이 시작되지 않으면 방화벽이 활성화됩니다. |
| 능동형 | A/P | 능동형/수동형 구성에서 능동형 방화벽의 상태입니다. |
| 수동형 | A/P | 능동형/수동형 구성에서 수동형 방화벽의 상태입니다. 수동형 방화벽은 네트워크에 중단 없이 능동형 방화벽이 될 준비가 되어 있습니다. 수동형 방화벽은 다른 트래픽을 처리하지는 않지만:<br>• 수동형 링크 상태 자동이 구성된 경우 수동형 방화벽이 라우팅 프로토콜을 실행하고 링크 및 경로 상태를 모니터링하고 있으며 LACP 및 LLDP 사전 협상이 각각 구성된 경우 패시브 방화벽이 LACP 및 LLDP를 미리 협상합니다.<br>• 수동형 방화벽은 흐름 상태, 런타임 개체 및 구성을 동기화합니다.<br>• 수동형 방화벽은 헬로 프로토콜을 사용하여 능동형 방화벽의 상태를 모니터링하고 있습니다. |
| 능동형-기본 | A/A | 능동형/능동형 구성에서는 User-ID 에이전트에 연결하고 DHCP 서버 및 DHCP 릴레이를 실행하고 NAT 및 PBF 규칙을 능동형 기본 방화벽의 디바이스 ID와 일치시키는 방화벽 상태입니다. 이 상태의 방화벽은 세션을 소유하고 세션을 설정할 수 있습니다. |
| 능동형-보조 | A/A | 능동형/능동형 구성에서는 User-ID 에이전트에 연결하고 DHCP 서버를 실행하고 NAT 및 PBF 규칙을 능동형 보조 방화벽의 디바이스 ID와 일치시키는 방화벽 상태입니다. 능동형 보조 상태의 방화벽은 DHCP 릴레이를 지원하지 않습니다. 이 상태의 방화벽은 세션을 소유하고 세션을 설정할 수 있습니다. |
| 임시 | A/A | 다음 중 하나에 의해 발생하는 방화벽 상태(능동형/능동형 구성)입니다.<br>• 방화벽의 실패.<br>• 모니터링된 개체(링크 또는 경로)의 실패입니다.<br>• 방화벽은 일시 중단되거나 작동하지 않는 상태로 남깁니다.<br>임시 상태의 방화벽은 피어의 세션 및 구성을 동기화합니다. |


©2023 Palo Alto Networks, Inc.

| HA 방화벽 상태 | 다음의 경우 발생 | 설명 |
|---|---|---|
| | | • 가상 와이어 배포에서 방화벽이 경로 오류로 인해 임시 상태로 입력하고 패킷을 포워딩하도록 받으면 처리를 위해 HA3 링크를 통해 피어 방화벽으로 패킷을 보냅니다. 피어 방화벽은 패킷을 처리하고 HA3 링크를 통해 방화벽으로 다시 보내 회귀 인터페이스를 전송합니다. 이 동작은 가상 와이어 배포에서 포워딩 경로를 유지합니다.<br>• 레이어 3 배포에서 임시 상태의 방화벽이 패킷을 받으면 피어 방화벽이 세션을 소유하거나 설정하는 HA3 링크를 통해 해당 패킷을 보냅니다. 네트워크 토폴로지에 따라 이 방화벽은 패킷을 대상으로 보내거나 포워딩을 위해 임시 상태로 피어로 다시 보냅니다.<br>실패한 경로 또는 링크가 지워지거나 실패한 방화벽이 잠정 상태에서 능동형 보조 상태로 전환되면 잠정 보류 시간이 트리거되고 라우팅 수렴이 발생합니다. 방화벽은 라우팅 어택을 빌드하고 패킷을 처리하기 전에 경로 테이블을 채우려고 시도합니다. 이 타이머가 없으면 복구 방화벽이 즉시 능동형 보조 상태로 입력되고 필요한 경로가 없기 때문에 패킷을 자동으로 폐기합니다.<br>방화벽이 일시 중단된 상태를 벗어나면 링크가 작동되고 수신 패킷을 처리할 수 있게 된 후 잠정 보류 시간 동안 잠정 상태가 됩니다.<br>잠정 보류 시간 범위(초)는 비활성화(0초) 또는 10-600 범위에서 비활성화할 수 있으며 기본값은 60입니다. |
| 비기능성 | A/P 또는 A/A | 패킷 포워딩, VR 동기화 또는 QoS 동기화에 대해 구성된 오직 하나의 방화벽과 같이 데이터플레인 오류 또는 구성 불일치로 인한 오류 상태입니다.<br>능동형/수동형 모드에서는 임시 상태에 나열된 모든 원인은 작동하지 않는 상태를 유발합니다. |
| 일시 중단 | A/P 또는 A/A | 디바이스가 비활성화되어 데이터 트래픽을 포워딩하지 않으며 HA 통신이 여전히 발생하지만 디바이스는 HA 일렉션(election) 프로세스에 참여하지 않습니다. 사용자 개입 없이는 HA 기능 상태로 이동할 수 없습니다. |


©2023 Palo Alto Networks, Inc.

# 참조: HA 동기화

HA 쌍의 두 피어에서 구성 동기화를 사용하도록 설정한 경우 한 피어에서 구성하는 대부분의 구성 설정이 커밋 시 다른 피어와 자동으로 동기화됩니다. 구성 충돌을 피하려면 항상 능동형(능동형/수동형) 또는 능동형-기본(능동형/능동형) 피어에서 구성을 변경하고 추가 구성을 변경하기 전에 변경 사항이 피어에 동기화될 때까지 기다리십시오.

커밋된 구성만 ***HA*** 피어 간에 동기화됩니다**.** ***HA*** 동기화 시 커밋 대기열의 모든 구성은 동기화되지 않습니다**.**

다음 항목에서는 각 방화벽에서 독립적으로 구성해야 하는 구성 설정을 식별합니다(이러한 설정은 HA 피어에서 동기화되지 않음).

- 활성/수동 HA에서 동기화되지 않는 설정은 무엇입니까?
- 활성/활성 HA에서 동기화되지 않는 설정은 무엇입니까?
- 시스템 런타임 정보의 동기화

## 활성/수동 HA에서 동기화되지 않는 설정은 무엇입니까?

능동형/수동형 배포에서 HA 쌍의 각 방화벽에 대한 다음 설정을 구성해야 합니다. 이러한 설정은 한 피어에서 다른 피어로 동기화되지 않습니다.

| 구성 항목 | 능동형/수동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| 관리 인터페이스 설정 | 모든 관리 구성 설정은 다음을 포함하여 각 방화벽에서 개별적으로 구성되어야 합니다.<br>• **Device** > **Setup** > **Management** > 일반 설정 - 호스트 이름, 도메인, 로그인 배너, SSL/TLS 서비스 프로파일(및 관련 인증서), 시간대, 로케일, 날짜, 시간, 위도, 경도.<br>• 디바이스 > 설정 > 관리 > 인터페이스 설정-IP 유형, IP 주소, 넷 마스크, 기본 게이트웨이, IPv6 주소 /프리픽스 길이, 기본 IPv6 게이트웨이, 속도, MTU, 및 서비스(HTTP, HTTP OCSP, HTTPS, 텔넷, SSH, 핑(ping), SNMP, User-ID, User-ID Syslog 청취자-SSL, User-ID Syslog Listener-SSL, User-ID SYlog-SSL) UDP |
| 다중 가상 시스템 기능 | PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈 및 PA-7000 시리즈 방화벽에서 기본적으로 제공되는 기본 수 이상으로 가상 시스템 수를 늘리려면 쌍의 각 방화벽에서 가상 시스템 라이센스를 활성화해야 합니다.<br>또한 각 방화벽에서 다중 가상 시스템 기능을 활성화해야 합니다(디바이스 > 설정 > 관리 > 일반 설정). |
| Panorama 설정 | 각 방화벽에서 다음 Panorama 설정을 지정합니다(**Device** > **Setup** > **Management** > 설정). |


©2023 Palo Alto Networks, Inc.

| 구성 항목 | 능동형/수동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| | • **Panorama** 서버<br>• **Panorama** 정책 및 개체 비활성화 및 디바이스 및 네트워크 템플릿 비활성화 |
| SNMP | 디바이스 > 설정 > 운영 > **SNMP** 설정 |
| 서비스 | 디바이스 > 설정 > 서비스 |
| 글로벌 서비스 경로 | 디바이스 > 설정 > 서비스 > 서비스 경로 구성 |
| 원격 측정 및 위협 인텔리전스 설정 | 디바이스 > 설정 > 원격 분석 및 위협 인텔리전스 |
| 데이터 보호 | 디바이스 > 설정 > **Content-ID** > 데이터 보호 관리 |
| 점보 프레임 | 디바이스 > 설정 > 세션 > 세션 설정 > 점보 프레임 활성화 |
| 패킷 버퍼 보호 | 디바이스 > 설정 > 세션 > 세션 설정 > 패킷 버퍼 보호<br>네트워크 > 영역 > 패킷 버퍼 보호 활성화 |
| 포워딩 프록시 서버 인증서 설정 | 디바이스 > 설정 > 세션 > 암호 해독 설정 > **SSL** 전달 프록시 설정 |
| HSM으로 보호되는 마스터 키 | 디바이스 > 설정 > **HSM** > 하드웨어 보안 모듈 공급자 > **HSM**으로 보호되는 마스터 키 |
| 로그 내보내기 설정 | 디바이스 > 예약된 로그 내보내기 |
| 소프트웨어 업데이트 | 소프트웨어 업데이트를 사용하면 각 방화벽에 별도로 다운로드하여 설치하거나 한 피어에 다운로드하고 업데이트를 다른 피어에 동기화할 수 있습니다. 각 피어(디바이스 > 소프트웨어)에 업데이트를 설치해야 합니다. |
| GlobalProtect 에이전트 패키지 | GlobalProtect 앱 업데이트를 사용하면 각 방화벽에 별도로 다운로드하여 설치하거나 한 피어에 다운로드하고 다른 피어에 업데이트를 동기화할 수 있습니다. 각 피어(**Device** > **GlobalProtect Client**)에서 별도로 활성화해야 합니다. |
| 콘텐츠 업데이트 | 콘텐츠 업데이트를 사용하면 각 방화벽에 별도로 다운로드하여 설치하거나 한 피어에 다운로드하고 업데이트를 다른 피어에 동기화할 수 있습니다. 각 피어에 업데이트를 설치해야 합니다(디바이스 > 동적 업데이트). |
| Licenses/ Subscriptions | 디바이스 > 라이선스 |


©2023 Palo Alto Networks, Inc.

| 구성 항목 | 능동형/수동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| 지원 구독 | 디바이스 > 지원 |
| 마스터 키 | 마스터 키는 HA 쌍의 각 방화벽에서 동일해야 하지만 각 방화벽(**Device** > **Master** 키 및 진단)에 수동으로 입력해야 합니다.<br>마스터 키를 변경하기 전에 두 피어에서 구성 동기화를 비활성화(**Device** > **High Availability** > **General** > **Setup** 및 구성 동기화 활성화 체크박스 선택 취소)한 다음 키를 변경한 후 다시 활성화해야 합니다. |
| 보고서, 로그 및 대시보드 설정 | 기록 데이터, 보고서 및 대시보드 데이터 및 설정(열 표시, 위젯)은 피어 간에 동기화되지 않습니다. 그러나 보고서 구성 설정은 동기화됩니다. |
| HA 설정 | 디바이스 > 고가용성 |
| 규칙 사용 데이터 | 적중 횟수, 만든 날짜 및 수정한 날짜와 같은 규칙 사용 데이터는 피어 간에 동기화되지 않습니다. 각 방화벽에 대한 정책 규칙 적중 수 데이터를 보려면 각 방화벽에 로그인해야 하고, HA 방화벽 피어에 대한 정보를 보려면 Panorama를 사용해야 합니다. |
| SSL을 통한 디바이스 관리 및 Syslog 통신용 인증서 전용 | 디바이스 > 인증서 관리 > 인증서<br>디바이스 관리 또는 SSL을 통한 syslog 통신에 사용되는 인증서는 HA 피어와 동기화되지 않습니다.<br>관리 인터페이스에 사용되는 인증서는 동기화되지 않고 다를 수 있지만 인증서 항목의 이름은 활성 및 수동 디바이스에 대해 동일해야 합니다. |
| 인증서 프로파일의 인증서 | 디바이스 > 인증서 관리 > 인증서 프로파일 |
| 디바이스 관리 전용 SSL/TLS 서비스 프로파일 | 디바이스 > 인증서 관리 > **SSL/TLS** 서비스 프로파일<br>디바이스 관리용 SSL/TLS 서비스 프로파일은 HA 피어와 동기화되지 않습니다. |
| 디바이스 ID 및 IoT 보안 | IP 주소-디바이스 매핑 및 정책 규칙 권장 사항은 HA 피어와 동기화되지 않습니다. |

## 활성/활성 HA에서 동기화되지 않는 설정은 무엇입니까?

능동형/능동형 배포의 HA 쌍에 있는 각 방화벽에서 다음 설정을 구성해야 합니다. 이러한 설정은 한 피어에서 다른 피어로 동기화되지 않습니다.


©2023 Palo Alto Networks, Inc.

| 구성 항목 | 능동형/능동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| 관리 인터페이스 설정 | 다음을 포함하여 각 방화벽에서 모든 관리 설정을 개별적으로 구성해야 합니다.<br>• **Device** > **Setup** > **Management** > 일반 설정 - 호스트 이름, 도메인, 로그인 배너, SSL/TLS 서비스 프로파일(및 관련 인증서), 시간대, 로케일, 날짜, 시간, 위도, 경도.<br>• **Device** > **Setup** > **Management** > 관리 인터페이스 설정 - IP 주소, 넷마스크, 기본 게이트웨이, IPv6 주소/접두어 길이, 기본 IPv6 게이트웨이, 속도, MTU 및 서비스(HTTP, HTTP OCSP, HTTPS, Telnet, SSH, Ping, SNMP, User-ID, 사용자 -ID Syslog 수신기-SSL, User-ID Syslog 수신기-UDP) |
| 다중 가상 시스템 기능 | PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈 및 PA-7000 시리즈 방화벽에서 기본적으로 제공되는 기본 수 이상으로 가상 시스템 수를 늘리려면 쌍의 각 방화벽에서 가상 시스템 라이센스를 활성화해야 합니다.<br>또한 각 방화벽에서 다중 가상 시스템 기능을 활성화해야 합니다(디바이스 > 설정 > 관리 > 일반 설정). |
| Panorama 설정 | 각 방화벽에서 다음 Panorama 설정을 지정합니다(**Device** > **Setup** > **Management** > 설정).<br>• **Panorama** 서버<br>• **Panorama** 정책 및 개체 비활성화 및 디바이스 및 네트워크 템플릿 비활성화 |
| SNMP | 디바이스 > 설정 > 운영 > **SNMP** 설정 |
| 서비스 | 디바이스 > 설정 > 서비스 |
| 글로벌 서비스 경로 | 디바이스 > 설정 > 서비스 > 서비스 경로 구성 |
| 원격 측정 및 위협 인텔리전스 설정 | 디바이스 > 설정 > 원격 분석 및 위협 인텔리전스 |
| 데이터 보호 | 디바이스 > 설정 > **Content-ID** > 데이터 보호 관리 |
| 점보 프레임 | 디바이스 > 설정 > 세션 > 세션 설정 > 점보 프레임 활성화 |
| 패킷 버퍼 보호 | 디바이스 > 설정 > 세션 > 세션 설정 > 패킷 버퍼 보호<br>네트워크 > 영역 > 패킷 버퍼 보호 활성화 |


©2023 Palo Alto Networks, Inc.

| 구성 항목 | 능동형/능동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| 포워딩 프록시 서버 인증서 설정 | 디바이스 > 설정 > 세션 > 암호 해독 설정 > **SSL** 전달 프록시 설정 |
| HSM 구성 | 디바이스 > 설정 > **HSM** |
| 로그 내보내기 설정 | 디바이스 > 예약된 로그 내보내기 |
| 소프트웨어 업데이트 | 소프트웨어 업데이트를 사용하면 각 방화벽에 별도로 다운로드하여 설치하거나 한 피어에 다운로드하고 업데이트를 다른 피어에 동기화할 수 있습니다. 각 피어(디바이스 > 소프트웨어)에 업데이트를 설치해야 합니다. |
| GlobalProtect 에이전트 패키지 | GlobalProtect 앱 업데이트를 사용하면 각 방화벽에 별도로 다운로드하여 설치하거나 한 피어에 다운로드하고 다른 피어에 업데이트를 동기화할 수 있습니다. 각 피어(**Device** > **GlobalProtect Client**)에서 별도로 활성화해야 합니다. |
| 콘텐츠 업데이트 | 콘텐츠 업데이트를 사용하면 각 방화벽에 별도로 다운로드하여 설치하거나 한 피어에 다운로드하고 업데이트를 다른 피어에 동기화할 수 있습니다. 각 피어에 업데이트를 설치해야 합니다(디바이스 > 동적 업데이트). |
| Licenses/ Subscriptions | 디바이스 > 라이선스 |
| 지원 구독 | 디바이스 > 지원 |
| 이더넷 인터페이스 IP 주소 | IP 주소(**Network** > **Interface** > **Ethernet**)를 제외한 모든 이더넷 인터페이스 구성 설정이 동기화됩니다. |
| 루프백 인터페이스 IP 주소 | IP 주소(**Network** > **Interface** > **Loopback**)를 제외한 모든 루프백 인터페이스 구성 설정이 동기화됩니다. |
| 터널 인터페이스 IP 주소 | IP 주소(**Network** > **Interface** > **Tunnel**)를 제외한 모든 터널 인터페이스 구성 설정이 동기화됩니다. |
| LACP 시스템 우선 순위 | 각 피어에는 능동형/능동형 배포에서 고유한 LACP 시스템 ID가 있어야 합니다(**Network** > **Interface** > **Ethernet** > **Add Aggregate Group** > **System Priority**). |
| VLAN 인터페이스 IP 주소 | IP 주소(**Network** > **Interface** > **VLAN**)를 제외한 모든 VLAN 인터페이스 구성 설정이 동기화됩니다. |
| 가상 라우터 | 가상 라우터 구성은 VR 동기화(디바이스 > 고가용성 > 능동형/능동형 구성 > 패킷 포워딩)를 활성화한 경우에만 동기화됩니다. 이 작업을 수행할지의 여부는 비대칭 라우팅 여부를 포함하여 네트워크 설계에 따라 다릅니다. |


©2023 Palo Alto Networks, Inc.

| 구성 항목 | 능동형/능동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| IPSec 터널 | IPSec 터널 구성 동기화는 유동 IP 주소(디바이스 > 고가용성 > 능동형/능동형 구성 > 가상 주소)를 사용하도록 가상 주소를 구성했는지의 여부에 따라 다릅니다. 유동 IP 주소를 구성한 경우 이러한 설정이 자동으로 동기화됩니다. 그렇지 않으면 각 피어에서 이러한 설정을 독립적으로 구성해야 합니다. |
| GlobalProtect 포털 구성 | GlobalProtect 포털 구성 동기화는 유동 IP 주소(**Network** > **GlobalProtect** > **Portals**)를 사용하도록 가상 주소를 구성했는지의 여부에 따라 다릅니다. 유동 IP 주소를 구성한 경우 GlobalProtect 포털 구성 설정이 자동으로 동기화됩니다. 그렇지 않으면 각 피어에서 독립적으로 포털 설정을 구성해야 합니다. |
| GlobalProtect 게이트웨이 구성 | GlobalProtect 게이트웨이 구성 동기화는 유동 IP 주소(**Network** > **GlobalProtect** > **Gateways**)를 사용하도록 가상 주소를 구성했는지의 여부에 따라 다릅니다. 유동 IP 주소를 구성한 경우 GlobalProtect 게이트웨이 구성 설정이 자동으로 동기화됩니다. 그렇지 않으면 각 피어에서 독립적으로 게이트웨이 설정을 구성해야 합니다. |
| QoS | QoS 구성은 **QoS** 동기화(디바이스 > 고가용성 > 능동형/능동형 구성 > 패킷 포워딩)를 활성화한 경우에만 동기화됩니다. 예를 들어 각 링크의 대역폭이 다르거나 서비스 공급자를 통해 대기 시간이 다른 경우 QoS 설정을 동기화하지 않도록 선택할 수 있습니다. |
| LLDP | LLDP 상태 또는 개별 방화벽 데이터는 능동형/능동형 구성(**Network** > **Network Profiles** > **LLDP**)에서 동기화되지 않습니다. |
| BFD | BFD 구성 또는 BFD 세션 데이터는 능동형/능동형 구성(**Network** > **Network Profiles** > **BFD Profile**)에서 동기화되지 않습니다. |
| IKE 게이트웨이 | IKE 게이트웨이 구성 동기화는 유동 IP 주소(네트워크 > **IKE** 게이트웨이)를 사용하도록 가상 주소를 구성했는지의 여부에 따라 다릅니다. 유동 IP 주소를 구성한 경우 IKE 게이트웨이 구성 설정이 자동으로 동기화됩니다. 그렇지 않으면 각 피어에서 독립적으로 IKE 게이트웨이 설정을 구성해야 합니다. |
| 마스터 키 | 마스터 키는 HA 쌍의 각 방화벽에서 동일해야 하지만 각 방화벽(**Device** > **Master** 키 및 진단)에 수동으로 입력해야 합니다.<br>마스터 키를 변경하기 전에 두 피어에서 구성 동기화를 비활성화(**Device** > **High Availability** > **General** > **Setup** 및 구성 동기화 활성화 체크박스 선택 취소)한 다음 키를 변경한 후 다시 활성화해야 합니다. |
| 보고서, 로그 및 대시보드 설정 | 로그 데이터, 보고서, 대시보드 데이터 및 설정(열 표시, 위젯)은 피어 간에 동기화되지 않습니다. 그러나 보고서 구성 설정은 동기화됩니다. |
| HA 설정 | • 디바이스 > 고가용성 |


©2023 Palo Alto Networks, Inc.

| 구성 항목 | 능동형/능동형에서 동기화되지 않는 것은 무엇입니까? |
|---|---|
| | • (예외는 동기화를 수행하는 디바이스 > 고가용성 > 능동형/능동형 구성 > 가상 주소입니다.) |
| 규칙 사용 데이터 | 적중 횟수, 만든 날짜 및 수정한 날짜와 같은 규칙 사용 데이터는 피어 간에 동기화되지 않습니다. 각 방화벽에 대한 정책 규칙 적중 수 데이터를 보려면 각 방화벽에 로그인해야 하고, HA 방화벽 피어에 대한 정보를 보려면 Panorama를 사용해야 합니다. |
| SSL을 통한 디바이스 관리 및 Syslog 통신용 인증서 전용 | 디바이스 > 인증서 관리 > 인증서<br>디바이스 관리 또는 SSL을 통한 syslog 통신에 사용되는 인증서는 HA 피어와 동기화되지 않습니다. |
| 인증서 프로파일의 인증서 | 디바이스 > 인증서 관리 > 인증서 프로파일 |
| 디바이스 관리 전용 SSL/TLS 서비스 프로파일 | 디바이스 > 인증서 관리 > **SSL/TLS** 서비스 프로파일<br>디바이스 관리용 SSL/TLS 서비스 프로파일은 HA 피어와 동기화되지 않습니다. |
| 디바이스 ID 및 IoT 보안 | IP 주소-디바이스 매핑 및 정책 규칙 권장 사항은 HA 피어와 동기화되지 않습니다. |

## 시스템 런타임 정보의 동기화

다음 표에는 HA 피어 간에 동기화되는 시스템 런타임 정보가 요약되어 있습니다.

| 런타임 정보 | 구성이 동기화되었습니까? | | HA 링크 | 세부 |
|---|---|---|---|---|
| | A/P | A/A | | |
| **Management Plane(MP)** | | | | |
| 사용자 - 그룹 매핑 | 예 | 예 | HA1 | |
| 가상 시스템 간의 사용자 매핑 | 예 | 예 | HA1 | |
| 사용자 - IP 주소 매핑 | 예 | 예 | HA1 | A/A 구성에서는 액티브-프라이머리 피어만 User-ID 서버 또는 에이전트에 연결되고 액티브-보조 피어에는 연결되지 않습니다. 액티브-프라이머리 피어가 일시 |


©2023 Palo Alto Networks, Inc.

| 런타임 정보 | 구성이 동기화되었습니까? | | HA 링크 | 세부 |
|---|---|---|---|---|
| | A/P | A/A | | |
| | | | | 중단되거나 오프라인 상태인 경우 액티브-보조 피어가 User-ID 서버 또는 에이전트에 연결됩니다. |
| DHCP 리스(서버) | 예 | 예 | HA1 | HA 피어의 PAN-OS 버전이 일치하지 않으면 DHCP 리스(서버) 구성 정보가 동기화되지 않습니다. |
| DNS 캐시 | 아니요 | 아니요 | 해당 사항 없음 | |
| FQDN 새로 고침 | 아니요 | 아니요 | 해당 사항 없음 | |
| IKE SAS [보안 협회] (1단계) | 아니요 | 아니요 | 해당 사항 없음 | |
| 포워드 정보 베이스(FIB) | 예 | 아니요 | HA1 | |
| 멀티캐스트 FIB (MFIB) | 예 | 아니요 | HA1 | |
| PAN-DB URL 캐시 | 예 | 아니요 | HA1 | 이는 데이터베이스를 디스크에 백업할 때(URL 데이터베이스 버전이 업데이트되는 경우 8시간마다) 또는 방화벽이 재부팅될 때 동기화됩니다. |
| 콘텐츠(수동 동기화) | 예 | 예 | HA1 | |
| PPPoE, PPPoE 리스 | 예 | 예 | HA1 | |
| DHCP 클라이언트 설정 및 리스 | 예 | 예 | HA1 | HA 피어의 PAN-OS 버전이 일치하지 않으면 DHCP 클라이언트 설정 및 리스 구성 정보가 동기화되지 않습니다. |
| SSL VPN 로그인 사용자 목록 | 예 | 예 | HA1 | |


©2023 Palo Alto Networks, Inc.

| 런타임 정보 | 구성이 동기화되었습니까? | | HA 링크 | 세부 |
|---|---|---|---|---|
| | A/P | A/A | | |
| 데이터플레인 | | | | |
| 세션 테이블 | 예 | 예 | HA2 | • 능동형/수동형 피어는 ICMP 또는 호스트 세션 정보를 동기화하지 않습니다.<br>• 능동형/능동형 피어는 호스트 세션, 멀티캐스트 세션 또는 BFD 세션 정보를 동기화하지 않습니다.<br>호스트 세션은 방화벽 인터페이스 중 하나 또는 *GP* 터널을 *ping*하는 *ICMP* 세션과 같이 방화벽 인터페이스 중 하나에서 종료된 세션입니다. |
| ARP 테이블 | 예 | 아니요 | HA2 | |
| 멀티캐스트 세션 테이블 | 예 | 아니요 | HA2 | |
| ND(neighbor discovery) 테이블 | 예 | 아니요 | HA2 | |
| MAC 테이블 | 예 | 아니요 | HA2 | |


©2023 Palo Alto Networks, Inc.

| 런타임 정보 | 구성이 동기화되었습니까? | | HA 링크 | 세부 |
|---|---|---|---|---|
| | A/P | A/A | | |
| IPsec SAS [보안 연결] (2단계) | 예 | 예 | HA2 | |
| IPSec 시퀀스 번호(재생 방지) | 예 | 예 | HA2 | |
| DoS 차단 목록 항목 | 아니요 | 아니요 | 해당 사항 없음 | |
| 가상 MAC | 예 | 예 | HA2 | |
| SCTP 연결 | 예 | 아니요 | HA2 | |


©2023 Palo Alto Networks, Inc.

# 모니터링

잠재적인 문제를 사전에 방지하고 필요할 때 발생 대응을 가속화하기 위해 방화벽은 사용자 지정 가능하고 유익한 보고서를 사용하여 트래픽 및 사용자 패턴에 대한 인텔리전스를 제공합니다. 대시보드, ACC(Application Command Center), 보고서 및 방화벽의 로그를 통해 네트워크 활동을 모니터링할 수 있습니다. 로그를 모니터링하고 정보를 필터링하여 사전 정의되거나 사용자 정의된 보기로 보고서를 생성할 수 있습니다. 예를 들어 사전 정의된 템플릿을 사용하여 사용자 활동에 대한 보고서를 생성하거나 보고서 및 로그를 분석하여 네트워크의 비정상적인 동작을 해석하고 트래픽 패턴에 대한 맞춤 리포트를 생성할 수 있습니다. 시각적으로 매력적인 네트워크 활동 프레젠테이션을 위해 대시보드와 ACC에는 관심 있는 정보를 찾기 위해 상호 작용할 수 있는 위젯, 차트 및 테이블이 포함되어 있습니다. 또한 모니터링되는 정보를 이메일 알림, syslog 메시지, SNMP 트랩 및 NetFlow 레코드와 같은 외부 서비스로 포워딩하도록 방화벽을 구성할 수 있습니다.


- 대시보드 사용
- 애플리케이션 명령 센터 사용
- 앱 범위 보고서 사용
- 자동화된 연동 엔진 사용
- 패킷 캡처 가져오기
- 애플리케이션 및 위협 모니터링
- 로그 보기 및 관리
- 차단 목록 모니터링
- 보고서 보기 및 관리
- 정책 규칙 사용 보기
- 모니터링을 위해 외부 서비스 사용
- 로그 포워딩 구성
- 이메일 경고 구성
- 모니터링에 Syslog 사용
- SNMP 모니터링 및 트랩
- HTTP(S) 대상으로 로그 포워딩
- NetFlow 모니터링

# 대시보드 사용

대시보드 탭 위젯에는 소프트웨어 버전, 각 인터페이스의 작동 상태, 리소스 사용률 및 위협, 구성 및 시스템 로그에서 가장 최근 항목 중 최대 10개까지 일반 방화벽 정보가 표시됩니다. 사용 가능한 모든 위젯은 기본적으로 표시되지만 각 관리자는 필요에 따라 개별 위젯을 제거하고 추가할 수 있습니다. 대시보드 또는 개별 위젯을 업데이트하려면 새로 고침 아이콘 을 클릭합니다. 자동 새로 고침 간격을 변경하려면 드롭다운에서 간격을 선택합니다(**1**분, **2**분, **5**분 또는 수동). 대시보드에 위젯을 추가하려면 위젯 드롭다운을 클릭하고 카테고리를 선택한 다음 위젯 이름을 선택합니다. 위젯을 삭제하려면 제목 표시줄에서 을 클릭합니다. 다음 표는 대시보드 위젯에 대해 설명합니다.

| 대시보드 차트 | 설명 |
|---|---|
| 상위 애플리케이션 | 대부분의 세션으로 애플리케이션을 표시합니다. 블록 크기는 세션의 상대적 수(숫자를 볼 수 있는 블록을 마우스 위로)를 나타내며 색상은 녹색(가장 낮은)에서 빨간색(최고)까지 보안 위험을 나타냅니다. 애플리케이션을 클릭하여 애플리케이션 프로파일을 봅니다. |
| 고위험 애플리케이션 | 상위 애플리케이션과 유사하지만 가장 많은 세션이 있는 가장 위험도가 높은 애플리케이션을 표시합니다. |
| 일반 정보 | 방화벽 이름, 모델, PAN-OS 소프트웨어 버전, 애플리케이션, 위협 및 URL 필터링 정의 버전, 현재 날짜 및 시간 및 마지막 다시 시작 이후의 시간 길이가 표시됩니다. |
| 인터페이스 상태 | 각 인터페이스가 위(녹색), 아래(빨간색) 또는 알 수 없는 상태(회색)인지의 여부를 나타냅니다. |
| 위협 로그 | 위협 로그의 마지막 10개 항목에 대한 위협 ID, 애플리케이션 및 날짜 및 시간을 표시합니다. 위협 ID는 URL 필터링 프로파일을 위반하는 멀웨어 설명 또는 URL입니다. |
| 구성 로그 | 구성 로그의 마지막 10개 항목에 대한 관리자 사용자명, 클라이언트(웹 또는 CLI) 및 날짜 및 시간을 표시합니다. |
| 데이터 필터링 로그 | 데이터 필터링 로그에서 마지막 60분 동안의 설명과 날짜 및 시간을 표시합니다. |
| URL 필터링 로그 | URL 필터링 로그에서 마지막 60분 동안의 설명과 날짜 및 시간을 표시합니다. |
| 시스템 로그 | 시스템 로그의 마지막 10개 항목에 대한 설명 및 날짜 및 시간을 표시합니다.<br><br>**구성** **설치** 항목은 구성 변경이 성공적으로 커밋했음을 나타냅니다. |


©2023 Palo Alto Networks, Inc.

| 대시보드 차트 | 설명 |
| --- | --- |
| 시스템 리소스 | 관리 CPU 사용량, 데이터플레인 사용량 및 세션 수가 방화벽을 통해 설정된 세션 수를 표시합니다. |
| 관리자로 로그인 | 현재 로그인한 각 관리자에 대해 소스 IP 주소, 세션 유형(웹 또는 CLI) 및 세션 시작 시간을 표시합니다. |
| ACC 위험 요소 | 지난 주 동안 처리된 네트워크 트래픽의 평균 위험 요소(1~5)를 표시합니다. 값이 높을수록 위험이 더 높습니다. |
| 고가용성 | HA(고가용성)가 활성화된 경우 녹색(활성), 노란색(수동) 또는 검은색(기타)과 같은 로컬 및 피어 방화벽의 HA 상태를 나타냅니다. HA에 대한 자세한 내용은 고가용성을(를) 참조하십시오. |
| 잠금 | 관리자가 수행한 구성 잠금을 표시합니다. |


©2023 Palo Alto Networks, Inc.

# 애플리케이션 명령 센터 사용

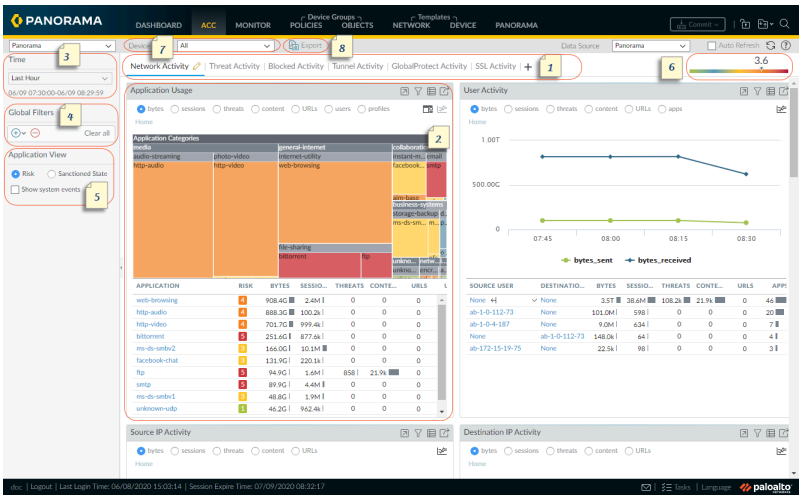
애플리케이션 명령 센터(ACC)는 네트워크를 통과하는 애플리케이션, 사용자, URL, 위협 및 콘텐츠에 대한 대화형 그래픽 요약입니다. ACC는 방화벽 로그를 사용하여 트래픽 패턴에 대한 가시성과 위협에 대한 실행 가능한 정보를 제공합니다. ACC 레이아웃에는 네트워크 활동, 위협 활동 및 차단된 활동에 대한 탭 보기가 포함되며 각 탭에는 네트워크 트래픽을 더 잘 시각화하기 위한 관련 위젯이 포함됩니다. 그래픽 표현을 사용하면 데이터와 상호 작용하고 네트워크의 이벤트 간의 관계를 시각화하여 변칙을 발견하거나 네트워크 보안 규칙을 향상시킬 방법을 찾을 수 있습니다. 네트워크의 개인화된 뷰의 경우 사용자 지정 탭을 추가하고 가장 중요한 정보를 드릴다운할 수 있는 위젯을 포함할 수도 있습니다.

> **ACC** 위젯 및 내보낸 **ACC** 보고서를 포함한 **ACC** 데이터는 세션 종료 시 기록에 대해 활성화한 보안 정책 규칙 데이터를 사용합니다. **ACC**에서 볼 것으로 예상되는 일부 데이터가 표시되지 않으면 트래픽 및 위협 로그를 확인하여 보안 정책 규칙과 일치하는 생성된 모든 새 로그를 **ACC**에서 볼 수 있도록 필요에 따라 수정할 올바른 보안 정책 규칙을 결정합니다.

- ACC—우선 검토
- ACC 탭
- ACC 위젯(위젯 설명)
- ACC 필터
- ACC와 상호 작용
- 사용 사례: ACC - 정보 검색의 경로

## ACC—우선 검토

ACC를 빠르게 둘러보세요.




 ©2023 Palo Alto Networks, Inc.

| ACC—우선 검토 | | |
|---|---|---|
|  | 탭 | ACC에는 네트워크 트래픽, 위협 활동 및 차단된 활동에 대한 가시성을 제공하는 3개의 사전 정의된 탭이 있습니다. 각 탭에 대한 정보는 ACC 탭을 참조하십시오. |
|  | 위젯 | 각 탭에는 해당 탭과 관련된 이벤트/트렌드를 가장 잘 나타내는 기본 위젯 세트가 포함되어 있습니다. 위젯을 사용하면 다음 필터를 사용하여 데이터를 조사할 수 있습니다.<br>• 바이트(입력 및 출력)<br>• 세션<br>• 콘텐츠(파일 및 데이터)<br>• URL 카테고리<br>• 위협(및 수)<br>각 위젯에 대한 정보는 ACC 위젯을 참조하세요. |
|  | 시간 | 각 위젯의 차트 또는 그래프는 요약 및 기록 보기를 제공합니다. 사용자 지정 범위를 선택하거나 지난 15분에서 최대 지난 90일 또는 지난 30일까지의 사전 정의된 기간을 사용할 수 있습니다. 선택한 기간은 ACC의 모든 탭에 적용됩니다.<br>기본적으로 데이터를 렌더링하는 데 사용되는 기간은 15분 간격으로 업데이트된 마지막 시간입니다. 날짜 및 시간 간격이 화면에 표시됩니다(예: 11:40에 시간 범위는 01/12 10:30:00-01/12 11:29:59). |
|  | 전역 필터 | 전역 필터를 사용하면 모든 위젯과 모든 탭에 필터를 설정할 수 있습니다. 차트/그래프는 데이터를 렌더링하기 전에 선택한 필터를 적용합니다. 필터 사용에 대한 정보는 ACC 필터를 참조하십시오. |
|  | 애플리케이션 보기 | 애플리케이션 보기를 사용하면 네트워크에서 사용 중인 승인 및 비승인 애플리케이션 또는 네트워크에서 사용 중인 애플리케이션의 위험 수준별로 ACC 보기를 필터링할 수 있습니다. 녹색은 승인된 애플리케이션, 파란색은 승인되지 않은 애플리케이션, 노란색은 부분적으로 승인된 애플리케이션을 나타냅니다. 부분적으로 승인된 애플리케이션은 승인된 상태가 혼합된 애플리케이션입니다. 이는 애플리케이션이 승인된 것으로 일관되게 태그가 지정되었음을 나타냅니다. 예를 들어 여러 가상 시스템에 대해 활성화된 방화벽에서 하나 이상의 |


©2023 Palo Alto Networks, Inc.

| ACC—우선 검토 | | |
|---|---|---|
| | | 가상 시스템 또는 Panorama의 디바이스 그룹 내 하나 이상의 방화벽에서 승인될 수 있습니다. |
| 6 | 위험 요소 | 위험 요소(1=최저, 5=최고)는 네트워크에서 사용되는 애플리케이션을 기반으로 한 상대적 위험을 나타냅니다. 위험 요소는 애플리케이션이 파일을 공유할 수 있는지의 여부, 오용 경향이 있는지 또는 방화벽 회피를 시도하는지의 여부와 같은 관련 위험 수준을 평가하기 위해 차단된 위협, 손상된 호스트 또는 맬웨어 호스트/도메인에 대한 트래픽의 수와 같은 다양한 요소를 사용합니다. |
| 7 | 원천 | ACC 디스플레이에 사용되는 데이터입니다. 옵션은 방화벽과 Panorama에 따라 다릅니다.<br>방화벽에서 여러 가상 시스템에 대해 활성화된 경우 가상 시스템 드롭다운을 사용하여 모든 가상 시스템 또는 선택한 가상 시스템의 데이터를 포함하도록 ACC 디스플레이를 변경할 수 있습니다.<br>Panorama에서 디바이스 그룹 드롭다운을 선택하여 모든 디바이스 그룹 또는 선택한 디바이스 그룹의 데이터를 포함하도록 ACC 디스플레이를 변경할 수 있습니다.<br>또한 Panorama에서 데이터 원본을 **Panorama** 데이터 또는 원격 디바이스 데이터로 변경할 수 있습니다. 원격 디바이스 데이터는 모든 관리 방화벽이 PAN-OS 7.0.0 이상의 버전인 경우에만 사용할 수 있습니다. 특정 디바이스 그룹에 대한 디스플레이를 필터링하면 **Panorama** 데이터가 데이터 소스로 사용됩니다. |
| 8 | 내보내기 | 현재 선택된 탭에 표시된 위젯을 PDF로 내보낼 수 있습니다. PDF가 다운로드되어 컴퓨터의 웹 브라우저와 연결된 다운로드 폴더에 저장됩니다. |

## ACC 탭

ACC에는 네트워크 활동, 위협 활동 및 차단된 활동을 볼 수 있는 다음과 같은 사전 정의된 탭이 있습니다.

| 탭 | 설명 |
|---|---|
| 네트워크 활동 | 다음을 포함하여 네트워크의 트래픽 및 사용자 활동에 대한 개요를 표시합니다.<br>• 사용 중인 상위 애플리케이션 |


©2023 Palo Alto Networks, Inc.

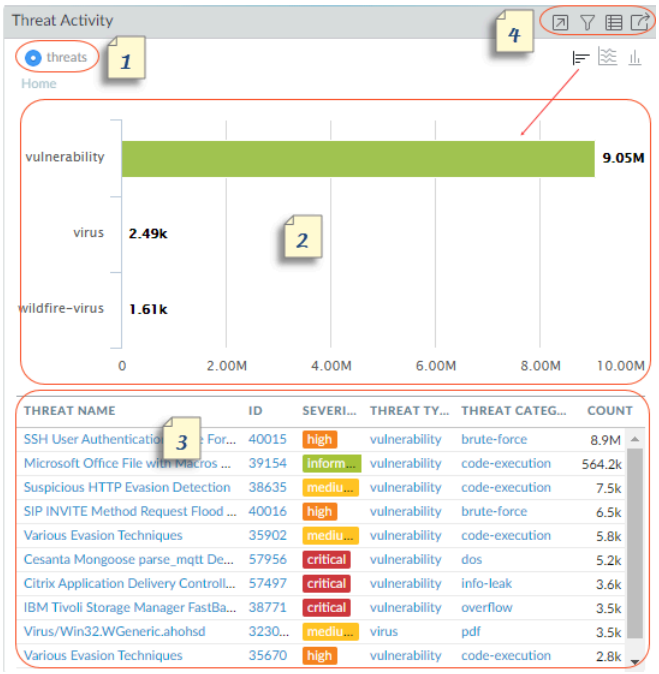
| 탭 | 설명 |
| --- | --- |
| | • 트래픽을 생성하는 상위 사용자(사용자가 액세스한 바이트, 콘텐츠, 위협 또는 URL에 대한 드릴다운 포함)<br>• 트래픽 일치가 발생하는 가장 많이 사용되는 보안 규칙<br>또한 소스 또는 대상 영역, 지역 또는 IP 주소, 수신 또는 송신 인터페이스, 그리고 네트워크에서 가장 일반적으로 사용되는 디바이스의 운영 체제와 같은 GlobalProtect 호스트 정보별로 네트워크 활동을 볼 수도 있습니다. |
| 위협 활동 | 취약점, 스파이웨어, 바이러스, 악성 도메인 또는 URL을 방문하는 호스트, 파일 유형 및 애플리케이션별 상위 WildFire 제출, 비표준 포트를 사용하는 애플리케이션 등 상위 위협에 초점을 맞춰 네트워크의 위협에 대한 개요를 표시합니다. 이 탭의 손상된 호스트 위젯(위젯은 일부 플랫폼에서만 지원됨)은 더 나은 시각화 기술로 탐지를 보완합니다. 상관 이벤트 탭(**Automated Correlation Engine** > **Correlated Events**)의 정보를 사용하여 소스 사용자/IP 주소 및 심각도별로 정렬된 네트워크의 손상된 호스트에 대한 집계 보기를 제공합니다. |
| 차단된 활동 | 네트워크에 들어오지 못하도록 차단된 트래픽에 중점을 둡니다. 이 탭의 위젯을 사용하면 애플리케이션 이름, 사용자 이름, 위협 이름, 차단된 콘텐츠(파일 차단 프로파일에 의해 차단된 파일 및 데이터)로 거부된 활동을 볼 수 있습니다. 또한 위협, 콘텐츠 및 URL을 차단하기 위해 일치하는 상위 보안 규칙을 나열합니다. |
| 터널 활동 | 터널 검사 정책에 따라 방화벽이 검사한 터널 트래픽의 활동을 표시합니다. 정보에는 터널 ID, 모니터 태그, 사용자 및 GRE(Generic Routing Encapsulation), GPRS(General Packet Radio Service) GTP-U(Tunneling Protocol for User Data) 및 비암호화 IPSec과 같은 터널 프로토콜을 기반으로 하는 터널 사용이 포함됩니다. |
| **GlobalProtect** 활동 | GlobalProtect 배포에서 사용자 활동의 개요를 표시합니다. 정보에는 사용자 수 및 사용자 연결 횟수, 사용자가 연결한 게이트웨이, 연결 실패 횟수 및 실패 이유, 사용된 인증 방법 및 GlobalProtect 앱 버전 요약, 격리된 엔드포인트 수가 포함됩니다.<br>또한 이 탭에는 격리된 디바이스의 차트 보기 요약이 표시됩니다. 차트 상단에 있는 토글을 사용하여 GlobalProtect가 디바이스를 검역하도록 한 작업, GlobalProtect가 디바이스를 검역한 이유 및 검역된 디바이스의 위치별 검역된 디바이스를 확인합니다. |
| **SSL** 활동 | 방화벽에서 TLS/SSL 복호화 활동의 개요를 표시합니다. 정보에는 네트워크의 성공 및 실패한 복호화 활동, 프로토콜, 인증서 및 버전 문제와 같은 복호화 실패 이유, TLS 버전, 키 교환 알고리즘, 복호화 및 복호화 트래픽의 양과 유형이 포함됩니다.<br>ACC 정보를 사용하여 네트워크에서 복호화가 작동하는 방식을 평가한 다음 복호화 로그을(를) 사용하여 세부 정보를 드릴다운합니다. |


©2023 Palo Alto Networks, Inc.

또한 ACC와 상호 작용을(를) 수행하여 네트워크 모니터링 요구 사항을 충족하는 사용자 정의 레이아웃 및 위젯으로 사용자 정의 탭을 생성하고 내보내며 다른 관리자와 공유할 수 있습니다.

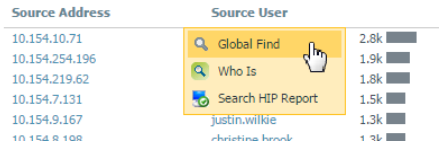
## ACC 위젯

각 탭의 위젯은 대화형입니다. ACC 필터를 설정하고 각 테이블 또는 그래프에 대한 세부 정보를 드릴다운하거나 탭에 포함된 위젯을 사용자 정의하여 필요한 정보에 집중할 수 있습니다. 각 위젯이 표시하는 내용에 대한 자세한 내용은 위젯 설명을 참조하십시오.




| 위젯 | | |
|---|---|---|
| 1 | 확인 | 바이트, 세션, 위협, 개수, 콘텐츠, URL, 악성, 양성, 파일, 애플리케이션, 데이터, 프로파일, 개체, 사용자별로 데이터를 정렬할 수 있습니다. 사용 가능한 옵션은 위젯에 따라 다릅니다. |
| 2 | 그래프 | 그래픽 표시 옵션은 트리맵, 선 그래프, 가로 막대 그래프, 누적 영역 그래프, 누적 막대 그래프 및 맵입니다. 사용 가능한 옵션은 위젯에 따라 다릅니다. 상호 작용 경험도 각 그래프 유형에 따라 다릅니다. 예를 들어, 비표준 포트를 사용하는 애플리케이션용 위젯을 사용하면 트리맵과 선 그래프 중에서 선택할 수 있습니다.<br><br>디스플레이를 드릴다운하려면 그래프를 클릭합니다. 클릭한 영역이 필터가 되어 선택 항목을 확대하고 선택 항목에 대한 보다 세부적인 정보를 볼 수 있습니다. |


©2023 Palo Alto Networks, Inc.

| 위젯 | | |
|---|---|---|
| 3 | 테이블 | 그래프를 렌더링하는 데 사용된 데이터의 자세한 보기는 그래프 아래의 표에 제공됩니다. 다음과 같은 여러 가지 방법으로 테이블과 상호 작용할 수 있습니다.<br>• 클릭하여 테이블의 속성에 대한 로컬 필터를 설정합니다. 그래프가 업데이트되고 테이블이 로컬 필터를 사용하여 정렬됩니다. 그래프와 테이블에 표시되는 정보는 항상 동기화됩니다.<br>• 테이블의 속성 위에 마우스를 놓고 드롭다운에서 사용 가능한 옵션을 사용합니다.<br> |
| 4 | 작업 | 보기 최대화 - 위젯을 확대하고 더 큰 화면 공간에서 더 많은 정보를 볼 수 있는 테이블을 볼 수 있습니다.<br>로컬 필터 설정 - ACC 필터를 추가하여 위젯 내에서 표시를 구체화할 수 있습니다. 이 필터를 사용하여 위젯을 사용자 정의하십시오. 이러한 사용자 정의는 로그인 간에 유지됩니다.<br>로그로 이동 - 로그(모니터 > 로그 > **<log-type>** 탭)로 직접 이동할 수 있습니다. 로그는 그래프가 렌더링되는 기간을 사용하여 필터링됩니다.<br>로컬 및 글로벌 필터를 설정한 경우 로그 쿼리는 기간과 필터를 연결하고 결합된 필터 세트와 일치하는 로그만 표시합니다.<br>내보내기—그래프를 PDF로 내보낼 수 있습니다. PDF가 다운로드되어 컴퓨터에 저장됩니다. 웹 브라우저와 연결된 다운로드 폴더에 저장됩니다. |

## 위젯 설명

ACC의 각 탭에는 다른 위젯 세트가 포함되어 있습니다.

 ©2023 Palo Alto Networks, Inc.

| 위젯 | 설명 |
|---|---|
| 네트워크 활동 - 네트워크의 트래픽 및 사용자 활동에 대한 개요를 표시합니다. | |
| 애플리케이션 사용 | 표에는 네트워크에서 사용되는 상위 10개 애플리케이션이 표시되며, 네트워크에서 사용되는 나머지 애플리케이션은 모두 집계되어 기타 애플리케이션으로 표시됩니다. 그래프는 애플리케이션 카테고리, 하위 카테고리 및 애플리케이션별로 모든 애플리케이션을 표시합니다. 이 위젯을 사용하여 네트워크에서 사용 중인 애플리케이션을 검색하고 대역폭, 세션 수, 파일 전송, 가장 많은 위협 트리거 및 URL 액세스를 사용하는 주요 애플리케이션에 대해 알려줍니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 트리맵, 영역, 열, 선(차트는 선택한 속성별 정렬에 따라 다름) |
| 사용자 활동 | 가장 많은 양의 트래픽을 생성하고 콘텐츠를 얻기 위해 네트워크 리소스를 소비한 네트워크에서 가장 활동적인 상위 10명의 사용자를 표시합니다. 이 위젯을 사용하여 바이트, 세션, 위협, 콘텐츠(파일 및 패턴), 방문한 URL을 기준으로 정렬된 사용량에 대해 상위 사용자를 모니터링합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 영역, 열, 선(차트는 선택한 속성별 정렬에 따라 다름) |
| 원본 **IP** 활동 | 네트워크에서 활동을 시작한 디바이스의 상위 10개 IP 주소 또는 호스트 이름을 표시합니다. 다른 모든 디바이스는 집계되어 기타 디바이스로 표시됩니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 영역, 열, 선(차트는 선택한 속성별 정렬에 따라 다름) |
| 대상 **IP** 활동 | 네트워크에서 사용자가 액세스한 상위 10개 대상의 IP 주소 또는 호스트 이름을 표시합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 영역, 열, 선(차트는 선택한 속성별 정렬에 따라 다름) |
| 소스 지역 | 사용자가 네트워크에서 활동을 시작한 전 세계 상위 10개 지역(기본 제공 또는 사용자 정의 지역)을 표시합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 지도, 막대 |
| 대상 지역 | 네트워크의 사용자가 콘텐츠에 액세스하는 세계 지도의 상위 10개 대상 영역(내장 또는 사용자 정의 영역)을 표시합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL |


©2023 Palo Alto Networks, Inc.

| 위젯 | 설명 |
| --- | --- |
| | 사용 가능한 차트: 지도, 막대 |
| **GlobalProtect** 호스트 정보 | GlobalProtect 에이전트가 실행 중인 호스트의 상태에 대한 정보를 표시합니다. 호스트 시스템은 GlobalProtect 엔드포인트입니다. 이 정보는 GlobalProtect 앱에서 제출한 데이터가 방화벽에 정의한 HIP 개체 또는 HIP 프로파일과 일치할 때 생성되는 HIP 일치 로그 항목에서 가져옵니다. HIP 일치 로그가 없는 경우 이 위젯은 비어 있습니다. HIP 개체 및 HIP 프로파일을 만들고 정책 일치 기준으로 사용하는 방법을 알아보려면 HIP 기반 정책 시행 구성을 참조하십시오.<br>속성 정렬: 프로파일, 개체, 운영 체제<br>사용 가능한 차트: 막대 |
| 규칙 사용 | 네트워크에서 가장 많은 트래픽을 허용한 상위 10개 규칙을 표시합니다. 이 위젯을 사용하여 가장 일반적으로 사용되는 규칙을 보고, 사용 패턴을 모니터링하고, 규칙이 네트워크 보안에 효과적인지의 여부를 평가할 수 있습니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 선 |
| 인그레스**(ingress)** 인터페이스 | 네트워크에 트래픽을 허용하는 데 가장 많이 사용되는 방화벽 인터페이스를 표시합니다.<br>정렬 속성: 바이트, 보낸 바이트, 받은 바이트<br>사용 가능한 차트: 선 |
| 이그레스**(Egress)** 인터페이스 | 네트워크를 나가는 트래픽이 가장 많이 사용하는 방화벽 인터페이스를 표시합니다.<br>정렬 속성: 바이트, 보낸 바이트, 받은 바이트<br>사용 가능한 차트: 선 |
| 소스 영역 | 네트워크에 트래픽을 허용하는 데 가장 많이 사용되는 영역을 표시합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 선 |
| 목적지 영역 | 네트워크 외부로 나가는 트래픽이 가장 많이 사용하는 영역을 표시합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 선 |
| 위협 활동 - 네트워크의 위협에 대한 개요를 표시합니다. | |


©2023 Palo Alto Networks, Inc.

| 위젯 | 설명 |
| --- | --- |
| 손상된 호스트 | 네트워크에서 손상되었을 가능성이 있는 호스트를 표시합니다. 이 위젯은 상관 관계 로그의 이벤트를 요약합니다. 각 소스 사용자/IP 주소에 대해 일치를 트리거한 상관 개체와 상관 이벤트 로그에서 수집된 일치 증거에서 집계된 일치 수를 포함합니다. 자세한 내용은 자동 연동 엔진 사용을 참조하십시오.<br>PA-5200 시리즈, PA-7000 시리즈 및 Panorama에서 사용할 수 있습니다.<br>속성 정렬: 심각도(기본값) |
| 악성 **URL**을 방문하는 호스트 | 네트워크의 호스트(IP 주소/호스트 이름)가 악성 URL에 액세스한 빈도를 표시합니다. 이러한 URL은 PAN-DB의 분류를 기반으로 하는 악성코드로 알려져 있습니다.<br>속성 정렬: 개수<br>사용 가능한 차트: 선 |
| 악성 도메인을 해결하는 호스트 | DNS 서명과 일치하는 상위 호스트를 표시합니다. 악성 URL의 호스트 이름 또는 도메인을 확인하려고 시도하는 네트워크의 호스트. 이 정보는 네트워크의 DNS 활동 분석에서 수집됩니다. 수동 DNS 모니터링, 네트워크에서 생성된 DNS 트래픽, 방화벽에 DNS 싱크홀을 구성한 경우 샌드박스에 표시되는 활동, Palo Alto Networks 고객이 사용할 수 있는 악성 DNS 소스에 대한 DNS 보고서를 활용합니다.<br>속성 정렬: 개수<br>사용 가능한 차트: 선 |
| 위협 활동 | 네트워크에서 본 위협을 표시합니다. 이 정보는 Antivirus, Anti-Spyware 및 Vulnerability Protection 프로파일과 WildFire에서 보고한 바이러스의 서명 일치를 기반으로 합니다.<br>속성 정렬: 위협<br>사용 가능한 차트: 막대, 영역, 열 |
| 애플리케이션별 **WildFire** 활동 | WildFire 제출을 가장 많이 생성한 애플리케이션을 표시합니다. 이 위젯은 WildFire 제출 로그의 악성 및 양성 판정을 사용합니다.<br>정렬 속성: 악성, 양성<br>사용 가능한 차트: 막대, 선 |
| 파일 유형별 **WildFire** 활동 | 파일 유형별로 위협 벡터를 표시합니다. 이 위젯은 WildFire 제출을 가장 많이 생성한 파일 유형을 표시하고 WildFire 제출 로그의 악성 및 양성 판정을 사용합니다. 이 데이터를 사용할 수 없으면 위젯이 비어 있습니다.<br>정렬 속성: 악성, 양성<br>사용 가능한 차트: 막대, 선 |


©2023 Palo Alto Networks, Inc.

| 위젯 | 설명 |
| --- | --- |
| 비표준 포트를 사용하는 애플리케이션 | 비표준 포트에서 네트워크에 진입하는 애플리케이션을 표시합니다. 포트 기반 방화벽에서 방화벽 규칙을 마이그레이션한 경우 이 정보를 사용하여 애플리케이션의 기본 포트에서만 트래픽을 허용하는 정책 규칙을 만드십시오. 필요한 경우 비표준 포트에서 트래픽을 허용하도록 예외를 만들거나 사용자 지정 애플리케이션을 만듭니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 트리맵, 선 |
| 비표준 포트에서 애플리케이션을 허용하는 규칙 | 기본이 아닌 포트에서 애플리케이션을 허용하는 보안 정책 규칙을 표시합니다. 그래프에는 모든 규칙이 표시되고 테이블에는 상위 10개 규칙이 표시되고 나머지 규칙의 데이터는 다른 것으로 집계됩니다.<br>이 정보는 애플리케이션이 포트를 호핑하는지 아니면 네트워크에 몰래 침입하는지 평가할 수 있도록 하여 네트워크 보안의 허점을 식별하는 데 도움이 됩니다. 예를 들어 애플리케이션의 기본 포트를 제외한 모든 포트에서 트래픽을 허용하는 규칙이 있는지 확인할 수 있습니다. 예를 들어 애플리케이션 기본 포트(포트 53은 DNS의 표준 포트임)에서 DNS 트래픽을 허용하는 규칙이 있다고 가정해 보겠습니다. 이 위젯은 포트 53을 제외한 모든 포트에서 네트워크로의 DNS 트래픽을 허용하는 모든 규칙을 표시합니다.<br>속성 정렬: 바이트, 세션, 위협, 콘텐츠, URL<br>사용 가능한 차트: 트리맵, 선 |
| 차단된 활동 - 네트워크로 들어오는 것이 차단된 트래픽에 중점을 둡니다. | |
| 차단된 애플리케이션 활동 | 네트워크에서 거부된 애플리케이션을 표시하고 네트워크에서 차단한 위협, 콘텐츠 및 URL을 볼 수 있습니다.<br>속성 정렬: 위협, 콘텐츠, URL<br>사용 가능한 차트: 트리맵, 영역, 열 |
| 차단된 사용자 활동 | 보안 정책 규칙에 첨부된 안티바이러스, 안티스파이웨어, 파일 차단 또는 URL 필터링 프로파일의 일치 항목에 의해 차단된 사용자 요청을 표시합니다.<br>속성 정렬: 위협, 콘텐츠, URL<br>사용 가능한 차트: 막대, 영역, 열 |
| 차단된 위협 | 네트워크에서 성공적으로 거부된 위협을 표시합니다. 이러한 위협은 방화벽의 동적 콘텐츠 업데이트를 통해 사용할 수 있는 안티바이러스 서명, 취약성 서명 및 DNS 서명과 일치했습니다.<br>속성 정렬: 위협<br>사용 가능한 차트: 막대, 영역, 열 |


©2023 Palo Alto Networks, Inc.

| 위젯 | 설명 |
| --- | --- |
| 차단된 콘텐츠 | 네트워크 진입이 차단된 파일 및 데이터를 표시합니다. 파일 차단 보안 프로파일 또는 데이터 필터링 보안 프로파일에 정의된 기준에 따라 보안 정책이 액세스를 거부했기 때문에 콘텐츠가 차단되었습니다.<br>정렬 속성: 파일, 데이터<br>사용 가능한 차트: 막대, 영역, 열 |
| 활동을 차단하는 보안 정책 | 네트워크로 들어오는 트래픽을 차단하거나 제한한 보안 정책 규칙을 표시합니다. 이 위젯은 네트워크에 대한 액세스가 거부된 위협, 콘텐츠 및 URL을 표시하므로 이를 사용하여 정책 규칙의 효율성을 평가할 수 있습니다. 이 위젯은 정책에 정의한 거부 규칙으로 인해 차단된 트래픽을 표시하지 않습니다.<br>속성 정렬: 위협, 콘텐츠, URL<br>사용 가능한 차트: 막대, 영역, 열 |
| **GlobalProtect** 활동 - GlobalProtect 배포의 사용자 활동 정보를 표시합니다. | |
| 성공적인 **GlobalProtect** 연결 활동 | 선택한 기간 동안 GlobalProtect 연결 활동의 차트 보기를 표시합니다. 차트 상단의 토글을 사용하여 사용자, 포털 및 게이트웨이, 위치별 연결 통계 간에 전환합니다.<br>속성 정렬: 사용자, 포털/게이트웨이, 위치<br>사용 가능한 차트: 막대, 선 |
| 실패한 **GlobalProtect** 연결 활동 | 선택한 기간 동안 실패한 GlobalProtect 연결 활동의 차트 보기를 표시합니다. 차트 상단의 토글을 사용하여 사용자, 포털 및 게이트웨이, 위치별 연결 통계 간에 전환합니다. 연결 문제를 식별하고 해결하는 데 도움이 되도록 이유 차트 또는 그래프를 볼 수도 있습니다. 이 차트에서 ACC는 오류, 소스 사용자, 공용 IP 주소 및 기타 정보를 표시하여 문제를 신속하게 식별하고 해결할 수 있도록 합니다.<br>속성 정렬: 사용자, 포털/게이트웨이, 이유, 위치<br>사용 가능한 차트: 막대, 선 |
| **GlobalProtect** 배포 활동 | 배포의 차트 보기 요약을 표시합니다. 차트 상단의 토글을 사용하여 인증 방법, GlobalProtect 앱 버전 및 운영 체제 버전별 사용자 분포를 확인합니다.<br>속성 정렬: 인증 방법, globalprotect 앱 버전, OS<br>사용 가능한 차트: 막대, 선 |
| **GlobalProtect** 검역 활동 | 격리된 디바이스의 차트 보기 요약을 표시합니다. 차트 상단에 있는 토글을 사용하여 GlobalProtect가 디바이스를 검역하도록 한 작업, GlobalProtect가 디바이스를 검역한 이유 및 검역된 디바이스의 위치별 검역된 디바이스를 확인합니다. |


©2023 Palo Alto Networks, Inc.

| 위젯 | 설명 |
| --- | --- |
| | 속성 정렬: 작업, 이유, 위치<br>사용 가능한 차트: 막대, 선 |
| **SSL** 활동 - 네트워크의 SSL/TLS 활동에 대한 정보를 표시합니다. | |
| 교통 활동 | 총 세션 수 또는 바이트별로 SSL/TLS 활동을 비 SSL/TLS 활동과 비교하여 표시합니다. |
| **SSL/TLS** 활동 | TLS 버전 및 애플리케이션 또는 SNI별로 성공적인 TLS 연결을 표시합니다. 이 위젯은 약한 TLS 프로토콜 버전을 허용함으로써 얼마나 많은 위험을 감수하고 있는지 이해하는 데 도움이 됩니다. 약한 프로토콜을 사용하는 애플리케이션 및 SNI를 식별하면 각각을 평가하고 비즈니스상의 이유로 액세스를 허용해야 하는지의 여부를 결정할 수 있습니다. 비즈니스 목적으로 애플리케이션이 필요하지 않은 경우 트래픽을 허용하는 대신 차단할 수 있습니다. 드릴다운하고 자세한 정보를 보려면 애플리케이션 또는 SNI를 클릭하십시오. |
| 복호화 실패 이유 | 인증서 또는 프로토콜 문제와 같은 복호화 실패의 원인을 SNI별로 표시합니다. 이 정보를 사용하여 복호화 정책이나 프로파일 구성 오류 또는 취약한 프로토콜이나 알고리즘을 사용하는 트래픽으로 인해 발생하는 문제를 감지합니다. SNI당 세션 수를 드릴다운하고 분리하려면 실패 이유를 클릭하거나 해당 SNI에 대한 실패를 보려면 SNI를 클릭하십시오. |
| 성공적인 **TLS** 버전 활동 | 세션 또는 바이트별로 복호화 및 복호화되지 않은 트래픽의 양을 표시합니다. 복호화되지 않은 트래픽은 정책, 잘못된 정책 구성 또는 복호화 제외 목록(디바이스 > 인증서 관리 > **SSL** 복호화 제외)에 의해 복호화에서 제외될 수 있습니다. |
| 성공적인 키 교환 활동 | 알고리즘별, 애플리케이션별 또는 SNI별 성공적인 키 교환 활동을 표시합니다. 키 교환 알고리즘을 클릭하여 해당 알고리즘에 대한 활동을 확인하거나 애플리케이션 또는 SNI를 클릭하여 해당 애플리케이션 또는 SNI에 대한 키 교환 활동을 확인합니다. |

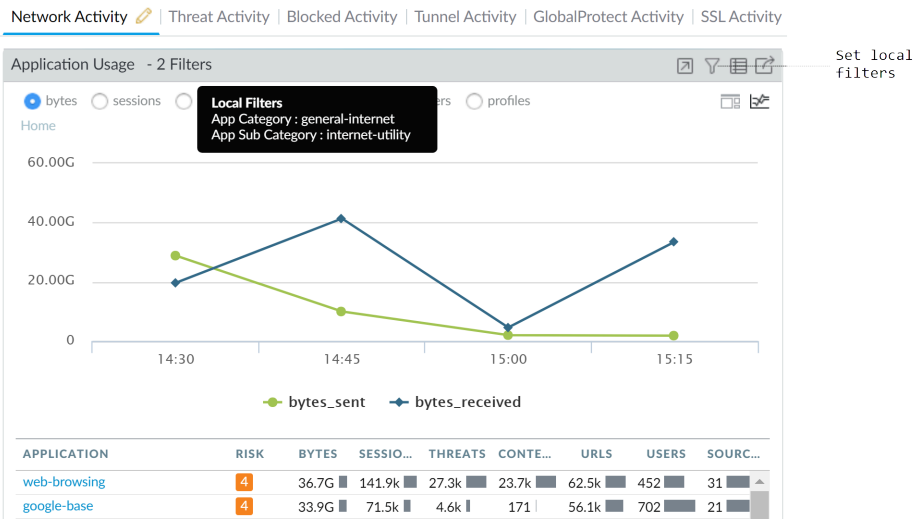
## ACC 필터

ACC 위젯의 그래프와 테이블을 사용하면 필터를 사용하여 표시되는 데이터의 범위를 좁히므로 특정 특성을 격리하고 보다 자세히 보고 싶은 정보를 분석할 수 있습니다. ACC는 위젯과 전역 필터의 동시 사용을 지원합니다.

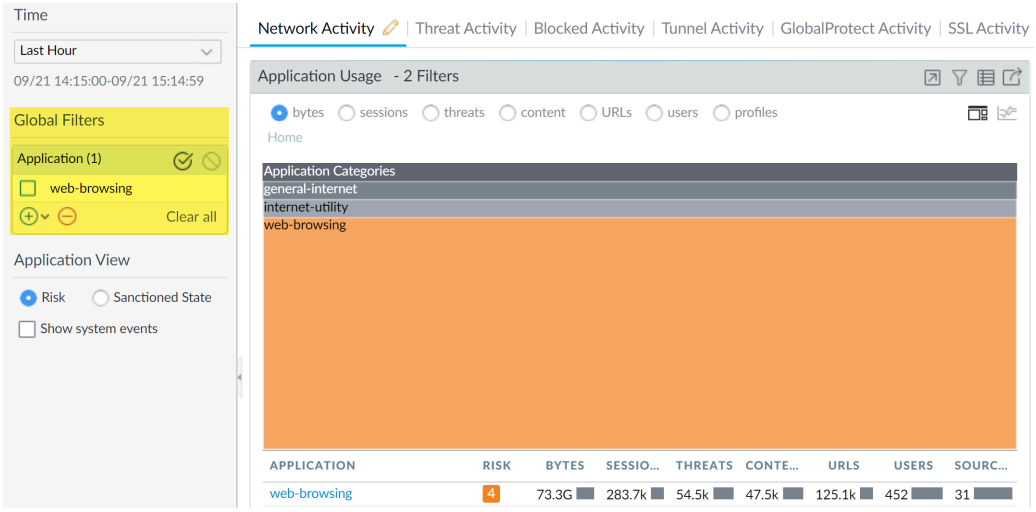
- 위젯 필터—특정 위젯에 로컬 필터인 위젯 필터를 적용합니다. 위젯 필터를 사용하면 그래프와 상호 작용하고 디스플레이를 사용자 지정하여 세부 정보를 드릴다운하고 특정 위젯에서 모니터링할 정보에 액

 ©2023 Palo Alto Networks, Inc.

세스할 수 있습니다. 재부팅 간에 지속되는 위젯 필터를 만들려면 로컬 필터 설정 옵션을 사용해야 합니다.




- 전역 필터— ACC의 모든 탭에 전역 필터를 적용합니다. 전역 필터를 사용하면 현재 관심 있는 세부 정보 주위에 디스플레이를 피벗하고 현재 디스플레이에서 관련없는 정보를 제외할 수 있습니다. 예를 들어 특정 사용자 및 애플리케이션과 관련된 모든 이벤트를 보려면 사용자 이름과 애플리케이션을 전역 필터로 적용하고 ACC의 모든 탭및 위젯을 통해 사용자와 애플리케이션과 관련된 정보만 볼 수 있습니다. 전역 필터는 영구적이지 않습니다.




다음과 같은 세 가지 방법으로 전역 필터를 적용할 수 있습니다.

- 테이블에서 전역 필터 설정—모든 위젯의 테이블에서 특성을 선택한 다음 특성을 전역 필터로 적용합니다.
- 위젯 필터를 전역 필터에 추가합니다—특성 위로 마우스를 가져가고 특성 오른쪽에 있는 화살표 아이콘을 클릭합니다. 이 옵션을 사용하면 위젯에 사용되는 로컬 필터를 높이고 전 세계적으로 특성을 적용하여 ACC의 모든 탭에서 디스플레이를 업데이트할 수 있습니다.
- 전역 필터 정의—ACC의 전역 필터 창을 사용하여 필터를 정의합니다.

이러한 필터 사용에 대한 자세한 내용은 ACC와 상호 작용을(를) 참조하십시오.


©2023 Palo Alto Networks, Inc.

# ACC와 상호 작용

ACC 디스플레이를 사용자 지정하고 구체화하려면 탭을 추가, 삭제, 내보내기 및 가져오고, 위젯을 추가 및 삭제하고, 로컬 및 전역 필터를 설정하고, 위젯과 상호 작용할 수 있습니다.

- 탭을 추가합니다.
  1. 탭 목록을 따라 ➕ 아이콘을 선택합니다.
  2. 보기 이름을 추가합니다. 이 이름은 탭의 이름으로 사용됩니다. 최대 5개의 탭을 추가할 수 있습니다.

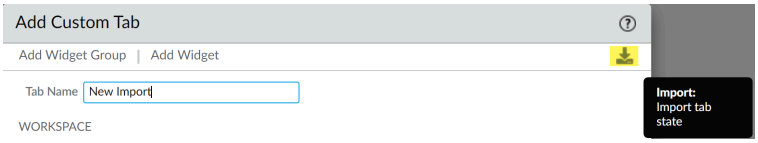
- 탭을 편집합니다.

  탭을 선택한 다음 탭 이름 옆에 있는 연필 아이콘을 클릭하여 탭을 편집합니다. 예: Threat Activity .

  탭을 편집하면 탭에 표시되는 위젯을 추가하거나 삭제하거나 재설정할 수 있습니다. 탭의 위젯 레이아웃을 변경할 수도 있습니다.

  탭을 기본 탭으로 저장하려면 를 선택합니다.

- 탭 내보내기 및 가져오기.
  1. 탭을 선택한 다음 탭 이름 옆에 있는 연필 아이콘을 클릭하여 탭을 편집합니다.
  2. 아이콘을 선택하여 현재 탭을 .txt 파일로 내보냅니다. 이 .txt 파일을 다른 관리자와 공유할 수 있습니다.
  3. 탭을 다른 방화벽의 새 탭으로 가져오려면 탭 목록을 따라 ➕ 아이콘을 선택하고 이름을 추가하고 가져오기 아이콘을 클릭한 후 .txt 파일을 찾아 선택합니다.




- 탭에 포함된 위젯을 확인합니다.
  1. 탭을 선택한 다음 연필 아이콘을 클릭하여 편집합니다.
  2. 위젯 추가 드롭다운을 선택한 다음 체크박스를 선택한 위젯을 확인합니다.

- 위젯 또는 위젯 그룹을 추가합니다.
  1. 새 탭을 추가하거나 미리 정의된 탭을 편집합니다.
  2. 위젯 추가를 선택한 다음 추가할 위젯에 해당하는 체크박스를 선택합니다. 최대 12개의 위젯을 선택할 수 있습니다.
  3. (선택 사항) 2열 레이아웃을 생성하려면 위젯 그룹 추가를 선택합니다. 위젯을 드래그하고 2열 디스플레이에 놓을 수 있습니다. 위젯을 레이아웃으로 드래그하면 자리 표시자가 위젯을 삭제할 수 있습니다.

  위젯 그룹의 이름을 지정할 수 없습니다.


©2023 Palo Alto Networks, Inc.

- 탭 또는 위젯 그룹/위젯을 삭제합니다.
  1. 사용자 지정 탭을 삭제하려면 탭을 선택한 다음 X 아이콘을 클릭합니다. 
     

     미리 정의된 탭은 삭제할 수 없습니다.
  2. 위젯 그룹/위젯을 삭제하려면 탭을 편집하고 작업 영역 섹션에서 오른쪽의 [X] 아이콘을 클릭합니다. 삭제를 취소할 수 없습니다.

- 탭에서 기본 위젯을 재설정합니다.

  차단된 활동 탭과 같이 사전 정의된 탭에서는 하나 이상의 위젯을 삭제할 수 있습니다. 탭의 기본 위젯 집합을 포함하도록 레이아웃을 재설정하려면 탭을 편집하고 보기 재설정을 클릭합니다.

- 영역, 열 또는 줄 그래프의 세부 정보를 확대합니다.

  확대 기능의 작동 방식을 지켜보십시오.

  그래프의 영역을 클릭하고 드래그하여 확대합니다. 예를 들어 줄 그래프를 확대하면 다시 쿼리가 트리거되고 방화벽이 선택한 기간 동안 데이터를 가져옵니다. 이는 단순한 배율이 아닙니다.

- 테이블 드롭다운을 사용하여 특성에 대한 자세한 정보를 찾습니다.
  1. 테이블의 특성 위로 마우스를 가져가서 드롭다운을 확인합니다.
  2. 드롭다운을 클릭하여 사용 가능한 옵션을 확인합니다.
     - 전역 찾기 - 전역 찾기를 사용하여 방화벽 또는 Panorama 관리 서버 검색후보 구성의 모든 위치에서 속성(사용자 이름/IP 주소, 개체 이름, 정책 규칙 이름, 위협 ID 또는 애플리케이션 이름)에 대한 참조.
     - 값 - 위협 ID 또는 애플리케이션 이름 또는 주소 개체의 세부 정보를 표시합니다.
     - **Who Is** - IP 주소에 대한 도메인 이름(*WHOIS*) 조회를 수행합니다. 조회는 등록된 사용자 또는 인터넷 리소스의 할당인을 저장하는 데이터베이스를 쿼리합니다.
     - **HIP** 보고서 검색 - 사용자 이름 또는 IP 주소를 사용하여 HIP 일치 보고서에서 일치 항목을 찾습니다.

- 위젯 필터를 설정합니다.

  표(그래프 아래)의 특성을 클릭하여 위젯 필터로 적용할 수도 있습니다.

  1. 위젯을 선택한 다음 아이콘을 클릭합니다.
  2. 아이콘을 클릭하여 적용할 필터를 추가합니다.
  3. 적용을 클릭합니다. 이러한 필터는 재부팅 전반에 걸쳐 지속됩니다.

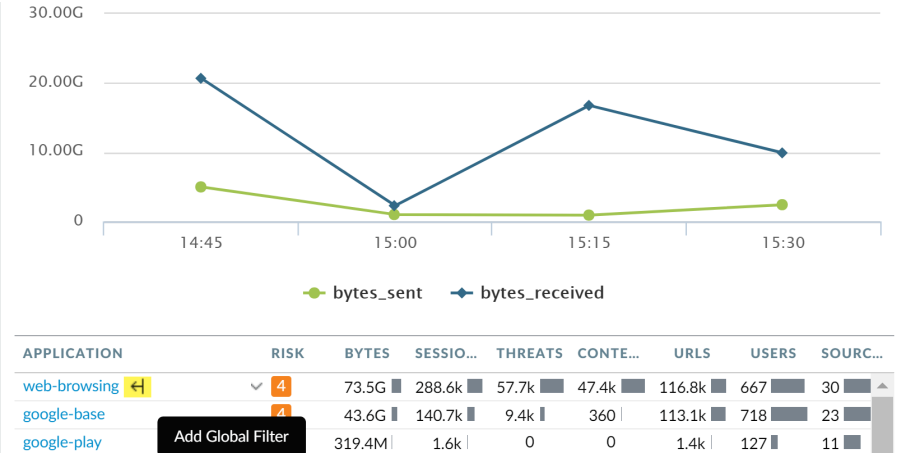
     활성 위젯 필터는 위젯 이름 옆에 표시됩니다.

 ©2023 Palo Alto Networks, Inc.

- 위젯 필터 무효화(negate)
  1. 아이콘을 클릭하여 로컬 필터 설정 대화 상자를 표시합니다.
  2. 필터를 추가한 다음 무효화(negate) 아이콘을 클릭합니다.

- 테이블에서 전역 필터를 설정합니다.

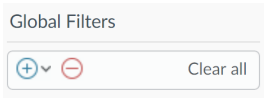
  차트 아래 표의 속성 위로 마우스를 가져가고 특성 오른쪽에 있는 화살표 아이콘을 클릭합니다.




- 전역 필터 창을 사용하여 전역 필터를 설정합니다.

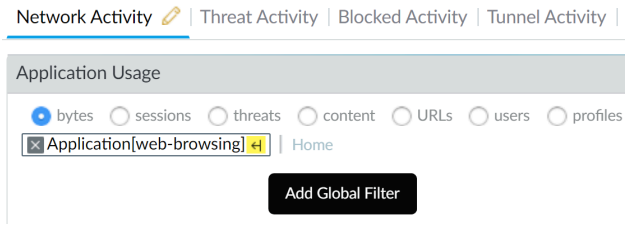
  글로벌 필터의 동작을 시청하세요.

  1. ACC 왼쪽에 있는 전역 필터 창을 찾습니다.




  2. 아이콘을 클릭하여 적용할 수 있는 필터 목록을 봅니다.

- 위젯 필터를 전역 필터로 승격합니다.
  1. 위젯의 테이블에서 속성에 대한 링크를 클릭합니다. 속성을 위젯 필터로 설정합니다.
  2. 필터를 전역 필터로 승격하려면 필터 오른쪽에 있는 화살표를 선택합니다.




 ©2023 Palo Alto Networks, Inc.

- 필터를 제거합니다.

  아이콘을 클릭하여 필터를 제거합니다.

  - 전역 필터의 경우: 전역 필터 창에 있습니다.
  - 위젯 필터의 경우: 아이콘을 클릭하여 로컬 필터 설정 대화 상자를 표시한 다음 필터를 선택한 다음 아이콘을 클릭합니다.

- 모든 필터를 지웁니다.

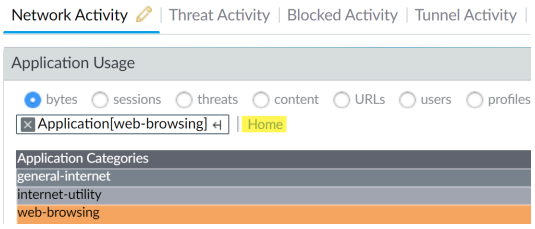
  - 전역 필터의 경우: 전역 필터 아래의 모든 단추 지우기 단추를 클릭합니다.
  - 위젯 필터의 경우: 위젯을 선택한 다음 아이콘을 클릭합니다. 그런 다음 설정 로컬 필터 대화 상자에서 모든 단추 지우기 단추를 클릭합니다.

- 사용 중인 필터를 확인합니다.

  - 전역 필터의 경우: 적용된 전역 필터 의 수는 전역 필터 아래왼쪽 창에 표시됩니다.
  - 위젯 필터의 경우: 위젯에 적용된 위젯 필터의 수는 위젯 이름 옆에 표시됩니다. 필터를 보려면 아이콘을 클릭합니다.

- 위젯에서 디스플레이를 재설정합니다.

  - 위젯 필터를 설정하거나 그래프로 드릴링하는 경우 홈 링크를 클릭하여 위젯에서 디스플레이를 재설정합니다.




# 사용 사례: ACC - 정보 검색의 경로

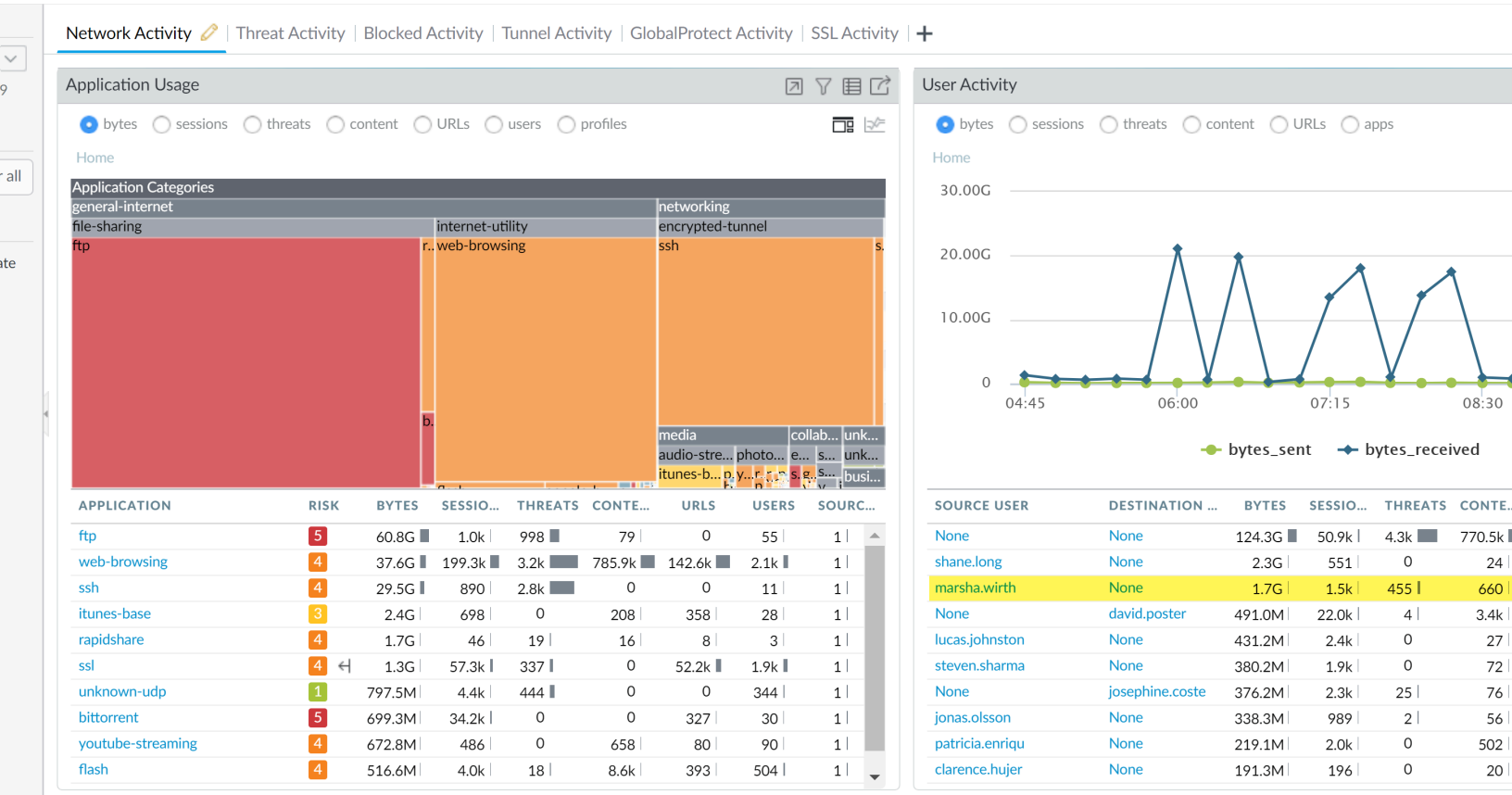
ACC에는 네트워크 트래픽 분석을 위한 시작점으로 사용할 수 있는 풍부한 정보가 있습니다. ACC를 사용하여 관심 있는 이벤트를 찾는 예를 살펴보겠습니다. 이 예에서는 ACC를 사용하여 합법적인 사용자가 자신의 작업에 대해 책임을 지도록 하고, 무단 활동을 감지 및 추적하고, 네트워크에서 손상된 호스트와 취약한 시스템을 감지 및 진단하는 방법을 보여줍니다.

ACC의 위젯과 필터를 사용하면 데이터를 분석하고 관심 이벤트 또는 우려되는 이벤트를 기반으로 보기를 필터링할 수 있습니다. 관심을 불러일으키는 이벤트를 추적하고, 탭의 PDF를 직접 내보내고, 원시 로그에 액세스하고, 추적하려는 활동의 개인화된 보기를 저장할 수 있습니다. 이러한 기능을 통해 활동을 모니터링하고 악의적인 활동으로부터 네트워크를 강화하기 위한 정책 및 대응책을 개발할 수 있습니다. 이 섹션에서는 다양한 탭에서 ACC와 상호 작용 위젯을 생성하고, 위젯 필터를 사용하여 드릴다운하고, 글로벌 필터를 사용하여 ACC 보기를 피벗하고, 발생 대응 또는 IT 팀과 공유하기 위해 PDF를 내보냅니다.

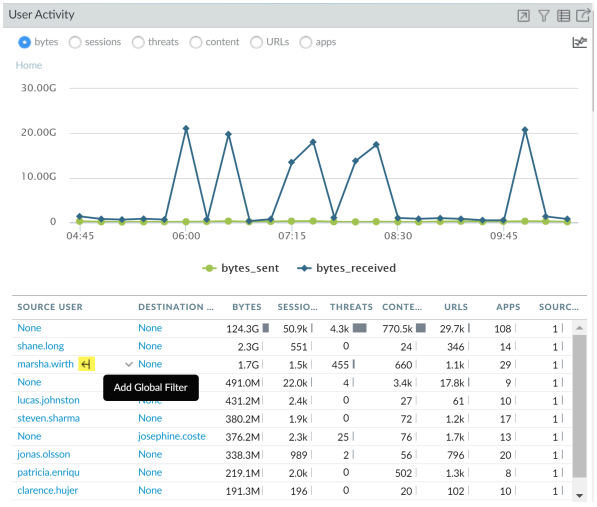
언뜻 보면 **ACC** > **Network Activity** 탭에서 Application Usage 및 User Activity 위젯을 볼 수 있습니다. 사용자 활동 위젯은 사용자 Marsha Wirth가 지난 1시간 동안 154MB의 데이터를 전송했음을 보여줍니다. 이 볼륨은 네트워크의 다른 사용자보다 거의 6배 많습니다. 지난 몇 시간 동안의 추세를 보려면 기간을

 ©2023 Palo Alto Networks, Inc.

지난 **6**시간으로 확장하십시오. 그러면 이제 Marsha의 활동은 1,500개 세션에서 1.7GB였으며 455개의 위협 서명을 트리거했습니다.




Marsha는 많은 양의 데이터를 전송했기 때문에 사용자명을 전역 필터(ACC 필터)로 적용하고 ACC의 모든 보기를 Marsha의 트래픽 활동으로 피벗합니다.

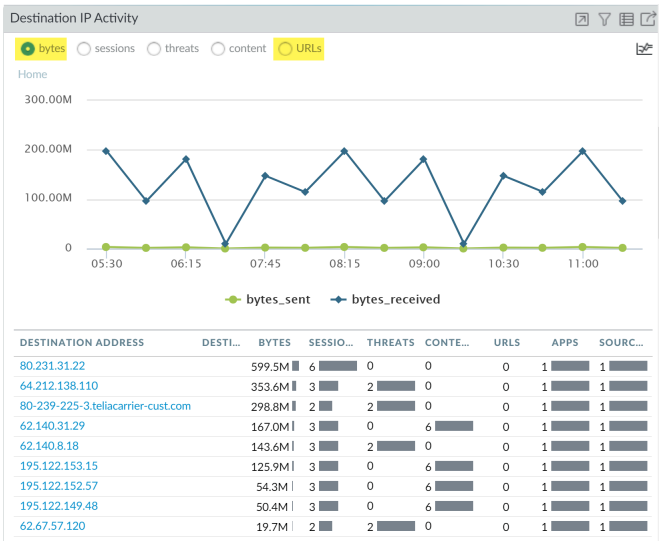



이제 애플리케이션 사용 탭에 Martha가 사용한 상위 애플리케이션이 파일 공유 URL 카테고리에 속하는 스위스 소유의 파일 호스팅 사이트인 Rapidshare로 표시됩니다. 추가 검토를 위해 Rapidshare를 전역 필터로 추가하고 Rapidshare의 맥락에서 Marsha의 활동을 봅니다.

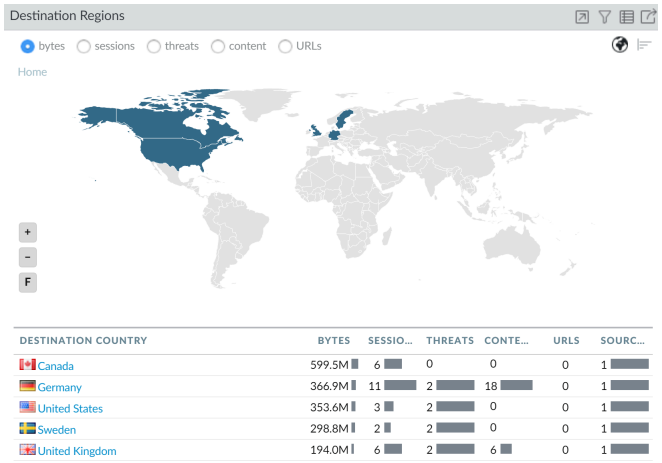

©2023 Palo Alto Networks, Inc.

회사 사용을 위해 ***Rapidshare***를 승인할지의 여부를 고려하십시오. 이 사이트에 대한 업로드를 허용해야 하고 대역폭을 제한하기 위해 ***QoS*** 정책이 필요합니까?

Marsha가 통신한 IP 주소를 보려면 **Destination IP Activity** 위젯을 확인하고 바이트 및 URL별로 데이터를 봅니다.

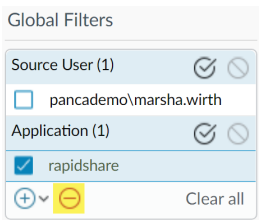



Marsha가 통신한 국가를 찾으려면 대상 지역 위젯에서 세션을 정렬하십시오.



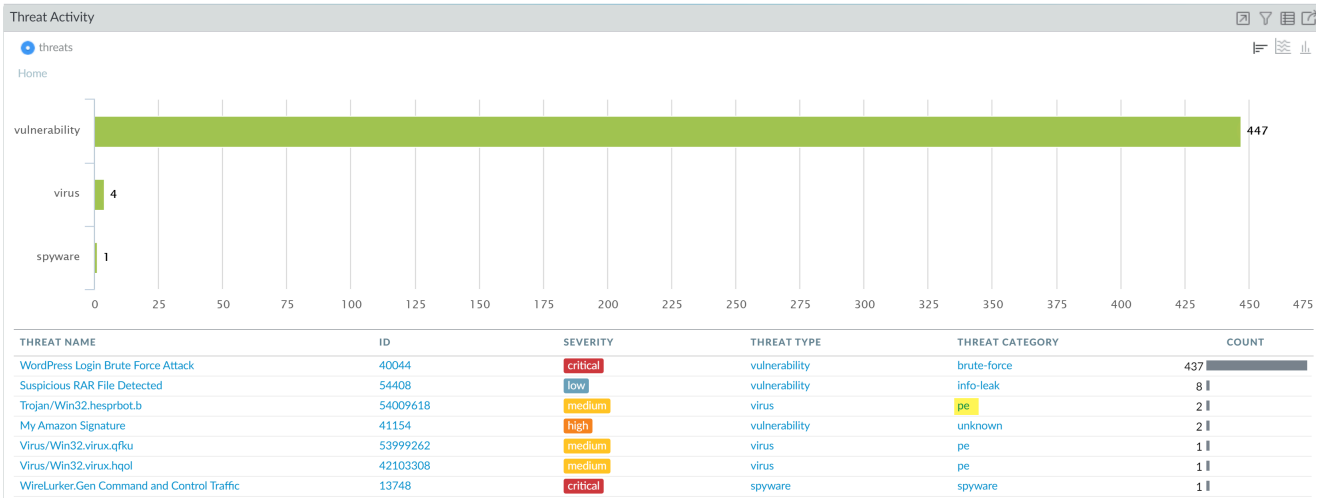

이 데이터에서 네트워크의 사용자인 Marsha가 캐나다, 독일, 스웨덴, 영국 및 미국에서 세션을 설정했음을 확인할 수 있습니다. 그녀는 각 목적지 국가와의 세션에서 2개의 위협을 기록했습니다.

위협 관점에서 Marsha의 활동을 보려면 Rapidshare에 대한 전역 필터를 제거하십시오.



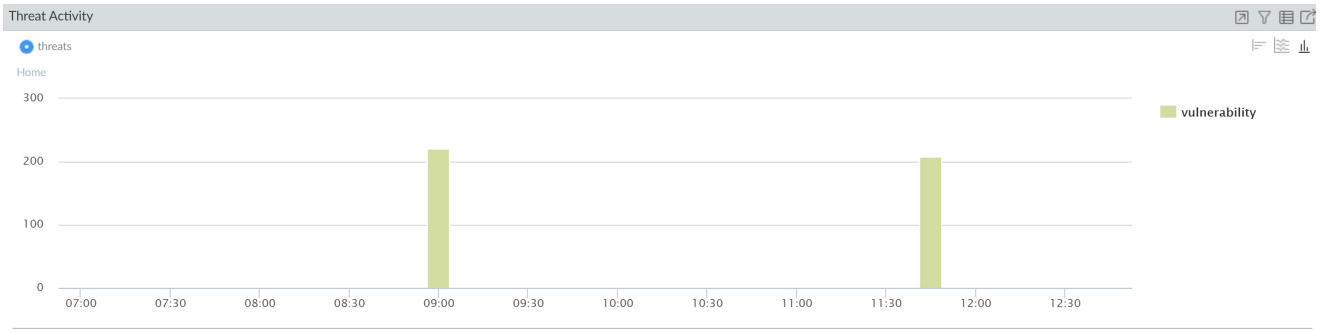

 ©2023 Palo Alto Networks, Inc.

위협 활동 탭의 위협 활동 위젯에서 위협을 봅니다. 위젯은 그녀의 활동이 무차별 대입, 정보 유출, PE(이동식 실행 파일) 및 스파이웨어 위협 카테고리에서 452개의 취약점에 대한 일치를 트리거했음을 표시합니다. 이러한 취약점 중 일부는 심각도가 매우 높습니다.




| THREAT NAME | ID | SEVERITY | THREAT TYPE | THREAT CATEGORY | COUNT |
|---|---|---|---|---|---|
| WordPress Login Brute Force Attack | 40044 | critical | vulnerability | brute-force | 437 |
| Suspicious RAR File Detected | 54408 | low | vulnerability | info-leak | 8 |
| Trojan/Win32.hesprbot.b | 54009618 | medium | virus | pe | 2 |
| My Amazon Signature | 41154 | high | vulnerability | unknown | 2 |
| Virus/Win32.virux.qfku | 53999262 | medium | virus | pe | 1 |
| Virus/Win32.virux.hqol | 42103308 | medium | virus | pe | 1 |
| WireLurker.Gen Command and Control Traffic | 13748 | critical | spyware | spyware | 1 |

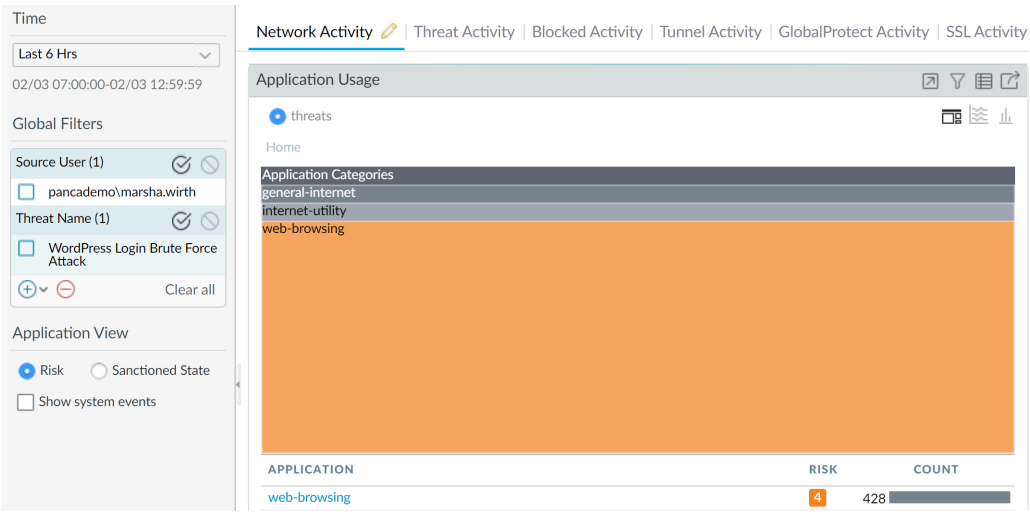
각 취약점에 대해 자세히 알아보려면 그래프를 클릭하고 검토 범위를 좁히십시오. 클릭할 때마다 위젯에 로컬 필터가 자동으로 적용됩니다.




| THREAT NAME | ID | SEVERITY | THREAT TYPE | THREAT CATEGORY | COUNT |
|---|---|---|---|---|---|
| WordPress Login Brute Force Attack | 40044 | critical | vulnerability | brute-force | 428 |

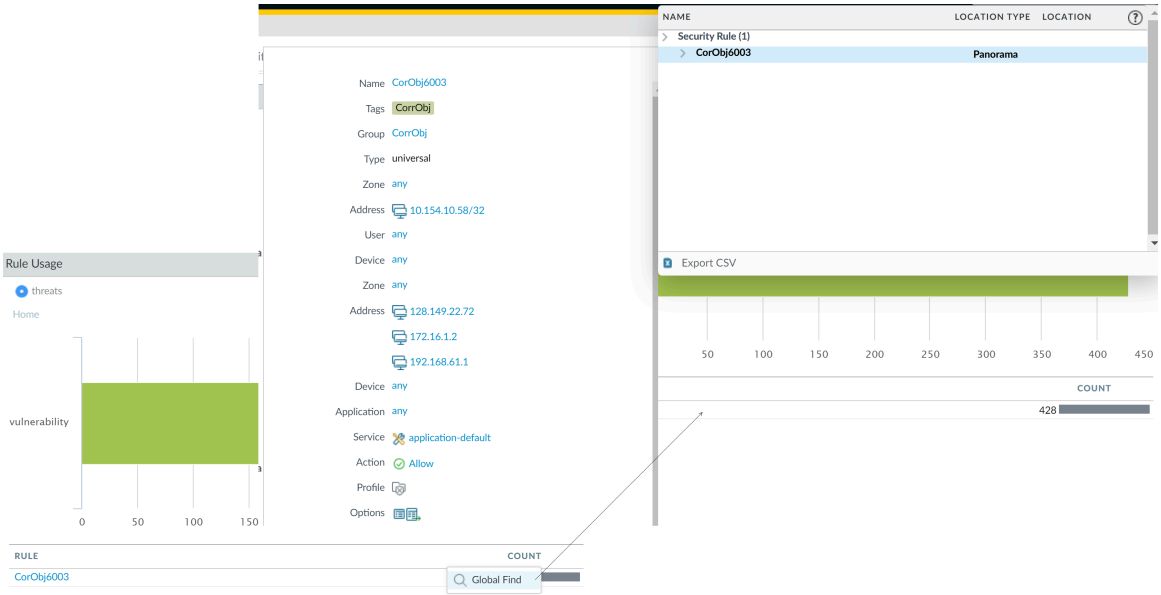
이름으로 각 위협을 검토하기 위해 **WordPress** 로그인 무차별 대입 공격에 대한 전역 필터를 만들 수 있습니다. 그런 다음 네트워크 활동 탭에서 사용자 활동 위젯을 봅니다. 탭은 자동으로 필터링되어 Marsha에 대한 위협 활동을 표시합니다(스크린샷의 전역 필터 참조).


©2023 Palo Alto Networks, Inc.




이 Microsoft 코드 실행 취약점은 imap 애플리케이션에 의해 이메일을 통해 트리거되었습니다. 현재 Martha에게 IE 취약점과 이메일 첨부 관련 취약점이 발견되고 아마도 해당 컴퓨터에 패치가 필요하다는 것을 확인할 수 있습니다. 이제 차단된 활동 탭에서 차단된 위협 위젯으로 이동하여 이러한 취약점 중 얼마나 많은 취약점이 차단되었는지 확인할 수 있습니다.

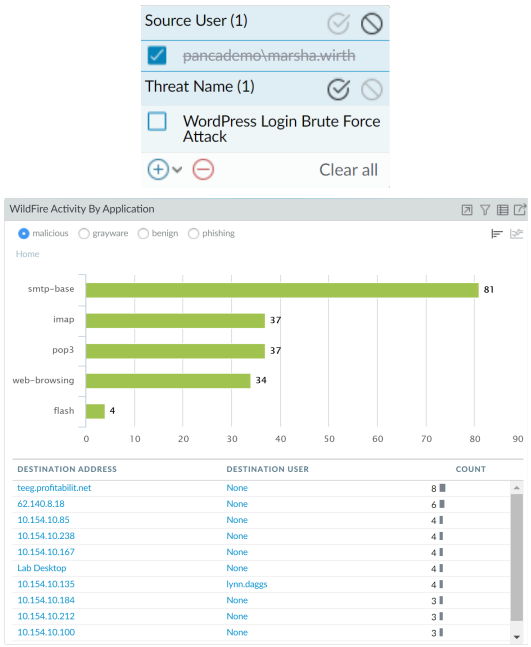
또는 네트워크 활동 탭에서 규칙 사용 위젯을 확인하여 네트워크에 침입한 취약점 수와 이 트래픽을 허용한 보안 규칙을 발견하고 전역 찾기 기능을 사용하여 보안 규칙으로 직접 이동할 수 있습니다.



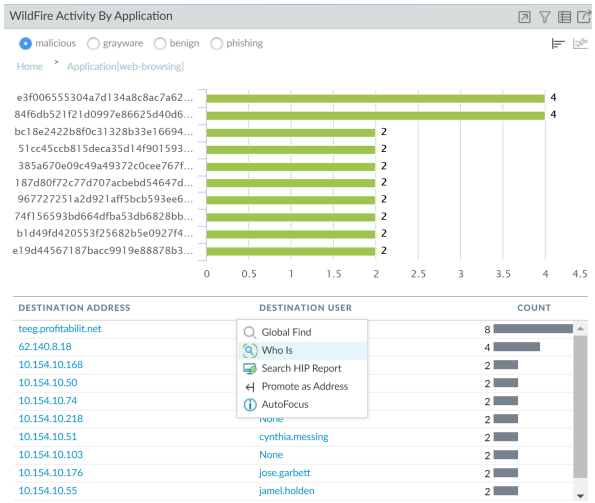

그런 다음 웹 브라우징을 사용하여 공격자를 드릴하여 대상을 공격합니다. 이러한 악성 IP 주소를 제한하거나 네트워크 리소스에 액세스할 수 있는 IP 주소를 보다 좁게 정의하도록 보안 정책 규칙을 수정하는 것이 좋습니다.

웹 브라우징을 통해 위협이 기록되었는지 검토하려면 위협 활동 탭의 애플리케이션별 **WildFire** 활동 위젯에서 Marsha의 활동을 확인하십시오. Marsha가 악의적인 활동을 하지 않았음을 확인할 수 있지만 다른 사용자가 웹 탐색 애플리케이션에 의해 손상되지 않았는지 확인하려면 Marsha를 전역 필터로 무효화하고 웹 탐색을 통해 위협을 유발한 다른 사용자를 찾습니다.


©2023 Palo Alto Networks, Inc.




그래프에서 imap에 대한 막대를 클릭하고 애플리케이션과 관련된 인바운드 위협을 자세히 살펴봅니다. IP 주소가 등록된 사람을 찾으려면 공격자 IP 주소 위로 마우스를 가져간 다음 드롭다운에서 **Who Is** 링크를 선택합니다.




이 IP 주소의 세션 수가 높기 때문에 차단된 활동 탭에서 차단된 콘텐츠 및 차단된 위협 위젯에서 이 IP 주소와 관련된 이벤트를 확인하십시오. 차단된 활동 탭을 사용하면 네트워크의 호스트가 손상된 경우 정책 규칙이 콘텐츠 또는 위협을 차단하는 데 효과적인지의 여부를 확인할 수 있습니다.

ACC의 **PDF** 내보내기 기능을 사용하여 현재 보기를 내보내고(데이터의 스냅샷 생성) 이를 사고 대응 팀에 보냅니다. 위젯에서 직접 위협 로그를 보려면 아이콘을 클릭하여 로그로 이동할 수도 있습니다. 쿼리가 자동으로 생성되고 관련 로그만 화면에 표시됩니다(예: **Monitor** > **Logs** > **Threat Logs**).

이제 ACC를 사용하여 네트워크 데이터/트렌드를 검토하여 가장 많은 트래픽을 생성하는 애플리케이션 또는 사용자와 네트워크에서 볼 수 있는 위협에 대한 책임이 있는 애플리케이션을 찾았습니다. 어떤 애플리케이션, 사용자가 트래픽을 생성했는지 식별하고, 애플리케이션이 기본 포트에 있었는지, 어떤 정책 규칙이 트래픽을 네트워크로 허용했는지 확인하고, 네트워크 측면에서 위협이 확산되고 있는지의 여부를 확

 ©2023 Palo Alto Networks, Inc.

인할 수 있었습니다. 또한 네트워크의 호스트가 통신하는 지리적 위치인 대상 IP 주소를 식별했습니다. 검토에서 얻은 결론을 사용하여 사용자와 네트워크를 보호할 수 있는 목표 지향적인 정책을 만드십시오.


©2023 Palo Alto Networks, Inc.

# 앱 범위 보고서 사용

App Scope 보고서는 잘못된 동작을 정확히 파악하여 대부분의 네트워크 대역폭을 차지하는 사용자 및 애플리케이션, 네트워크 위협 식별을 위한 가시성 및 분석 도구를 제공합니다.

App Scope 보고서를 사용하면 비정상적인 동작인지 예기치 않은지 빠르게 확인할 수 있습니다. 각 보고서는 네트워크에 대한 동적 사용자 정의 창을 제공합니다. 마우스를 차트에 놓고 선이나 막대를 클릭하면 ACC에서 특정 애플리케이션, 애플리케이션 카테고리, 사용자 또는 소스에 대한 자세한 정보가 열립니다. 모니터 > 앱 범위의 앱 범위 차트는 다음과 같은 기능을 제공합니다.

- 검토하려는 차트 세부 정보만 보려면 범례의 속성을 전환합니다. 차트에서 데이터를 포함하거나 제외할 수 있으므로 규모를 변경하고 세부 정보를 보다 면밀히 검토할 수 있습니다.
- 막대 차트의 특성을 클릭하고 ACC의 관련 세션으로 드릴다운합니다. 모든 막대 차트에서 애플리케이션 이름, 애플리케이션 카테고리, 위협 이름, 위협 카테고리, 소스 IP 주소 또는 대상 IP 주소를 클릭하여 특성을 필터링하고 ACC의 관련 세션을 봅니다.
- 차트 또는 맵을 PDF 또는 이미지로 내보냅니다. 휴대성과 오프라인 보기를 위해 차트와 맵을 PDF 또는 PNG 이미지로 내보낼 수 있습니다.

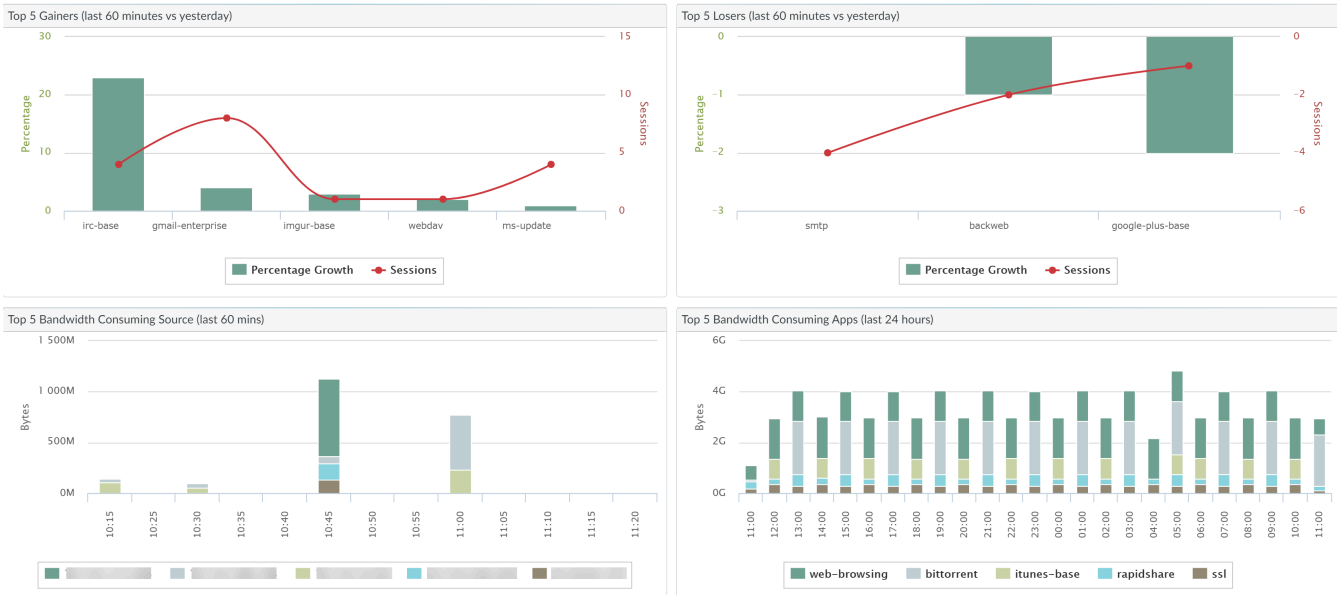
다음 앱 범위 보고서를 사용할 수 있습니다.

- 요약 보고서
- 변경 모니터 보고서
- 위협 모니터 보고서
- 위협 지도 보고서
- 네트워크 모니터 보고서
- 트래픽 맵 보고서

## 요약 보고서

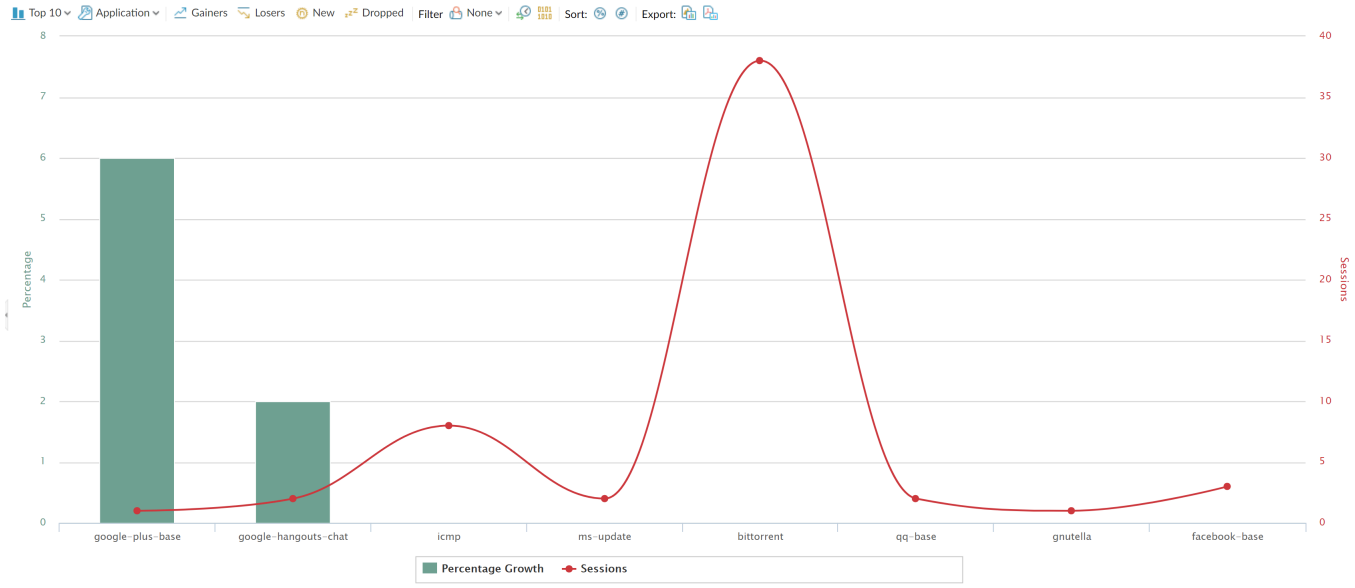
앱 범위 요약보고서(앱 범위 > 요약 > 모니터)에는 상위 5개 승자, 패자 및 대역폭 소모 애플리케이션, 애플리케이션 카테고리, 사용자 및 소스에 대한 차트가 표시됩니다.


©2023 Palo Alto Networks, Inc.




# 변경 모니터 보고서

앱 범위 변경 모니터 보고서(앱 범위 > 변경 모니터 > 모니터링)는 지정된 기간 동안의 변경 내용을 표시합니다. 예를 들어 다음 차트에는 지난 24시간 기간과 비교하여 지난 시간 동안 사용된 상위 애플리케이션이 표시됩니다. 상위 애플리케이션은 세션 수에 따라 결정되고 백분율로 정렬됩니다.




변경 모니터 보고서에는 다음 버튼과 옵션이 포함되어 있습니다.

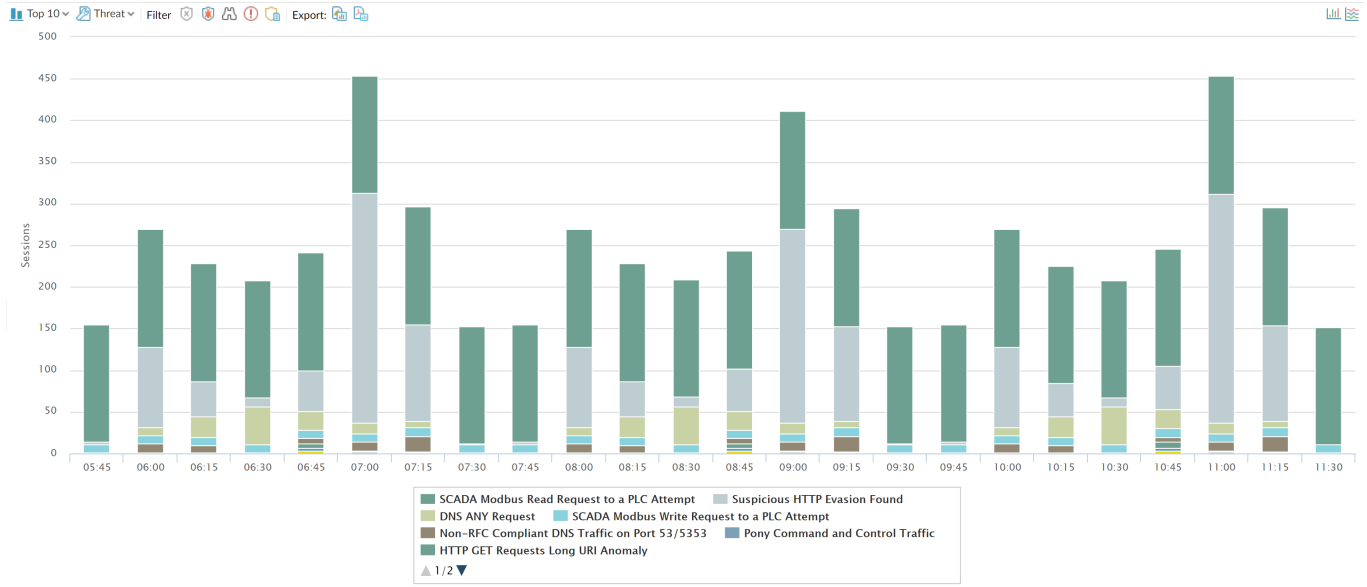
| 버튼 | 설명 |
|---|---|
| 상위 **10**개 | 차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다. |

 ©2023 Palo Alto Networks, Inc.

| 버튼 | 설명 |
|---|---|
| 애플리케이션 | 보고된 항목의 유형을 결정합니다. 애플리케이션, 애플리케이션 카테고리, 소스 또는 대상. |
| 우세자 | 측정된 기간 동안 증가한 품목의 측정을 표시합니다. |
| 열세자 | 측정된 기간 동안 감소한 품목의 측정값을 표시합니다. |
| 신규 | 측정된 기간 동안 추가된 품목의 측정값을 표시합니다. |
| 드롭 | 측정된 기간 동안 단종된 품목의 측정값을 표시합니다. |
| 필터 | 선택한 항목만 표시하려면 필터를 적용합니다. 없음은 모든 항목을 표시하지 않습니다. |
| | 세션 또는 바이트 정보를 표시할지의 여부를 결정합니다. |
| 정렬 | 항목을 백분율 또는 원시 성장별로 정렬할지의 여부를 결정합니다. |
| 내보내기 | 그래프를 .png 이미지 또는 PDF로 내보냅니다. |
| 비교 | 변경 측정이 수행되는 기간을 지정합니다. |

## 위협 모니터 보고서

앱 범위 위협 모니터 보고서(앱 범위 > 모니터링 > 위협 모니터)에는 선택한 기간 동안의 최상위 위협 수가 표시됩니다. 예를 들어 다음 그림은 지난 6시간 동안의 상위 10개 위협 유형을 보여 줍니다.




 ©2023 Palo Alto Networks, Inc.

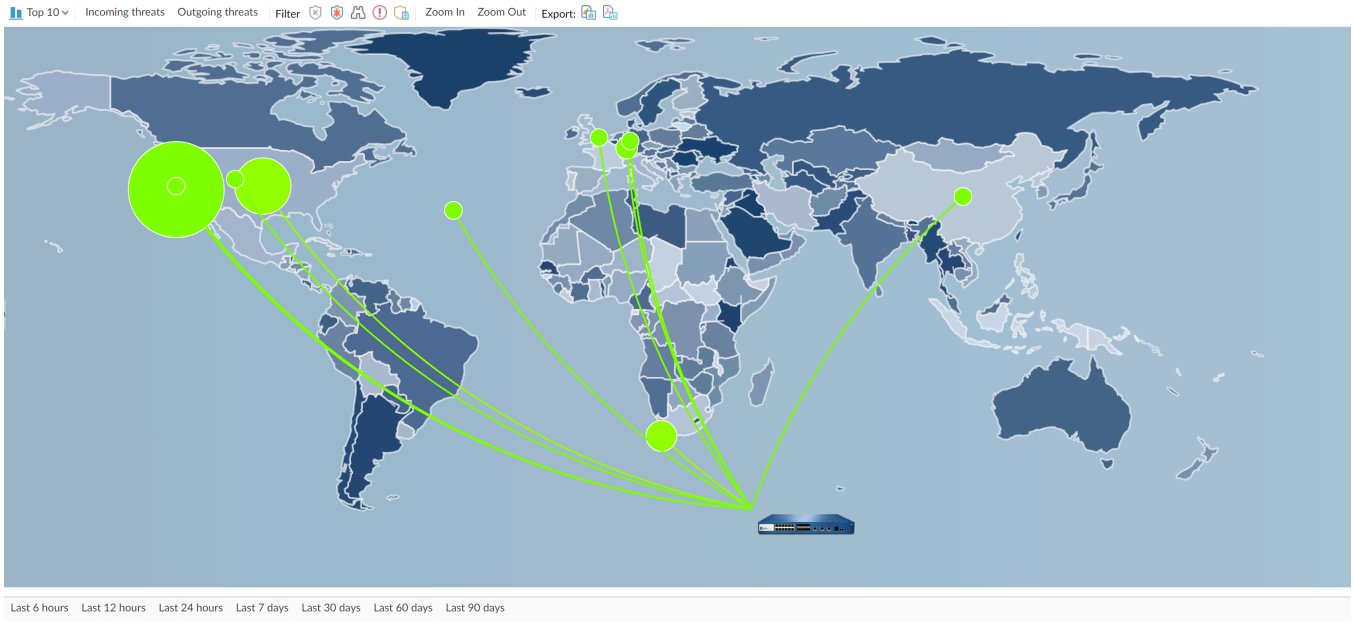
각 위협 유형은 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 위협 모니터 보고서에는 다음 버튼과 옵션이 포함되어 있습니다.

| 단추 | 설명 |
|---|---|
| 상위 **10**개 | 차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다. |
| 위협 | 측정된 항목의 유형을 결정합니다. 위협, 위협 카테고리, 소스 또는 대상. |
| 필터 | 선택한 항목 유형만 표시하려면 필터를 적용합니다. |
|  | 누적된 열 차트 또는 누적 된 영역 차트에 정보가 표시되는지의 여부를 결정합니다. |
| 내보내기 | 그래프를 .png 이미지 또는 PDF로 내보냅니다. |
|  | 측정이 수행되는 기간을 지정합니다. |

## 위협 지도 보고서

앱 범위 위협 맵 보고서(앱 범위 > 위협 맵 > 모니터링)에는 심각도를 포함한 위협에 대한 지리적 보기가 표시됩니다. 각 위협 유형은 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다.

방화벽은 위협 맵을 만들기 위해 지리적 위치를 사용합니다. 방화벽은 방화벽에서 지리적 위치 좌표(디바이스 > 설정 > 관리 일반 설정 섹션)를 지정하지 않은 경우 위협 맵 화면 하단에 배치됩니다.



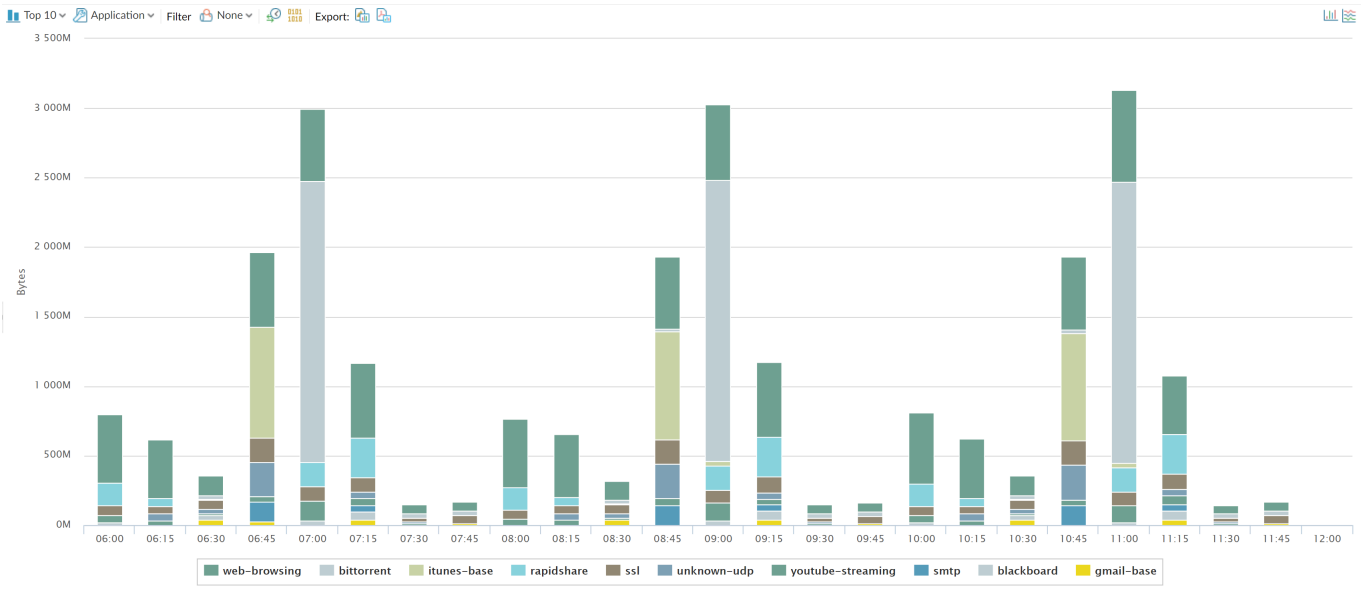

위협 지도 보고서에는 다음 버튼과 옵션이 포함되어 있습니다.

 ©2023 Palo Alto Networks, Inc.

| 단추 | 설명 |
| --- | --- |
| 상위 **10**개 | 차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다. |
| 들어오는 위협 | 들어오는 위협을 표시합니다. |
| 외부 위협 | 나가는 위협을 표시합니다. |
| 파일러 | 선택한 항목 유형만 표시하려면 필터를 적용합니다. |
| 확대/축소 및 축소 | 맵을 확대 및 축소합니다. |
| 내보내기 | 그래프를 .png 이미지 또는 PDF로 내보냅니다. |
| Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days | 측정이 수행되는 기간을 나타냅니다. |

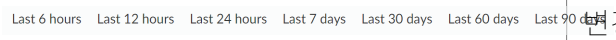
## 네트워크 모니터 보고서

앱 범위 네트워크 모니터 보고서(모니터링 > 앱 범위 > 네트워크 모니터)는 지정된 기간 동안 서로 다른 네트워크 기능에 전념하는 대역폭을 표시합니다. 각 네트워크 함수는 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 예를 들어 아래 이미지는 세션 정보를 기반으로 지난 7일 동안의 애플리케이션 대역폭을 보여줍니다.




네트워크 모니터 보고서에는 다음 버튼과 옵션이 포함되어 있습니다.

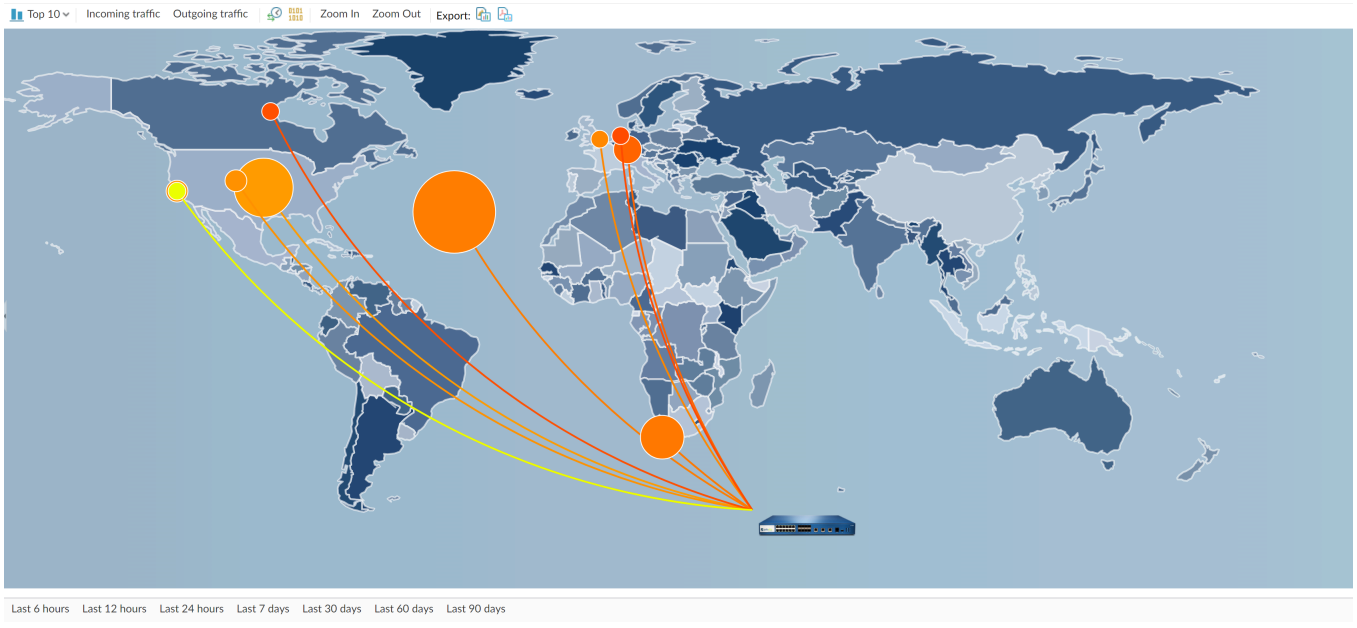
 ©2023 Palo Alto Networks, Inc.

| 단추 | 설명 |
| --- | --- |
| 상위 **10**개 | 차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다. |
| 애플리케이션 | 보고된 항목의 유형을 결정합니다. 애플리케이션, 애플리케이션 카테고리, 소스 또는 대상. |
| 필터 | 선택한 항목만 표시하려면 필터를 적용합니다. 없음은 모든 항목을 표시하지 않습니다. |
|  | 세션 또는 바이트 정보를 표시할지의 여부를 결정합니다. |
| 내보내기 | 그래프를 .png 이미지 또는 PDF로 내보냅니다. |
|  | 정보가 누적 세로 막대형 차트 또는 누적 영역 차트에 표시되는지의 여부를 결정합니다. |
|  | 변경 측정이 수행되는 기간을 나타냅니다. |

## 트래픽 맵 보고서

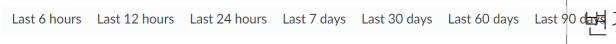
앱 범위 트래픽 맵(앱 범위 > 트래픽 맵 > 모니터링) 보고서에는 세션 또는 흐름에 따라 트래픽 플로우의 지리적 뷰가 표시됩니다.

방화벽은 트래픽 맵을 만들기 위해 지리적 위치를 사용합니다. 방화벽은 방화벽에서 지리적 위치 좌표(디바이스 > 설정 > 관리 일반 설정 섹션)를 지정하지 않은 경우 트래픽 맵 화면 하단에 배치됩니다.




각 트래픽 유형은 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 트래픽 맵 보고서에는 다음 버튼과 옵션이 포함되어 있습니다.


©2023 Palo Alto Networks, Inc.

| 버튼 | 설명 |
| --- | --- |
| 상위 **10**개 | 차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다. |
| 들어오는 위협 | 들어오는 위협을 표시합니다. |
| 나가는 위협 | 나가는 위협을 표시합니다. |
|  | 세션 또는 바이트 정보를 표시할지의 여부를 결정합니다. |
| 확대/축소 및 축소 | 맵을 확대 및 축소합니다. |
| 내보내기 | 그래프를 .png 이미지 또는 PDF로 내보냅니다. |
|  | 변경 측정이 수행되는 기간을 나타냅니다. |

 ©2023 Palo Alto Networks, Inc.

# 자동화된 연동 엔진 사용

자동화된 상관 관계 엔진은 방화벽의 로그를 사용하여 네트워크에서 실행 가능한 이벤트를 감지하는 분석 도구입니다. 엔진은 결합된 경우 네트워크에서 손상될 가능성이 있는 호스트 또는 기타 상위 수준 결론을 나타내는 일련의 관련 위협 이벤트를 연관시킵니다. 네트워크의 손상된 호스트와 같은 위험 영역을 정확히 찾아내어 위험을 평가하고 네트워크 리소스 악용을 방지하기 위한 조치를 취할 수 있습니다. 자동화된 연동 엔진은 상관 개체를 사용하여 패턴에 대한 로그를 분석하고 일치가 발생하면 상관 이벤트를 생성합니다.

다음 모델은 자동화된 상관 관계 엔진을 지원합니다.

- *Panorama - M* 시리즈 어플라이언스 및 가상 어플라이언스
- *PA-7000* 시리즈 방화벽
- *PA-5450* 방화벽
- *PA-5200* 시리즈 방화벽
- *PA-3200* 시리즈 방화벽


- 자동화된 연동 엔진 개념
- 상관 개체 보기
- 상관 이벤트 해석
- ACC에서 손상된 호스트 위젯 사용


## 자동화된 연동 엔진 개념

자동화된 연동 엔진은 상관 개체를 사용하여 패턴에 대한 로그를 분석하고 일치가 발생하면 상관 이벤트를 생성합니다.


- 상관 개체
- 상관 이벤트


### 상관 개체

상관 관계 개체는 일치하는 패턴을 지정하는 정의 파일, 조회에 사용할 데이터 원본 및 이러한 패턴을 찾을 기간을 지정합니다. 패턴은 방화벽에서 다음 데이터 원본(또는 로그)을 쿼리하는 조건의 부울 구조입니다: 애플리케이션 통계, 트래픽, 트래픽 요약, 위협 요약, 위협, 데이터 필터링 및 URL 필터링. 각 패턴에는 심각도 등급이 있으며 악의적인 활동을 나타내기 위해 정의된 시간 제한 내에서 패턴 일치가 발생해야 하는 횟수에 대한 임계값이 있습니다. 매치 조건이 충족되면 상관 관계가 있는 이벤트가 기록됩니다.

상관 관계 개체는 격리된 네트워크 이벤트를 연결하고 보다 중요한 이벤트를 나타내는 패턴을 찾을 수 있습니다. 이러한 개체는 의심스러운 IP 활동, 알려진 명령 및 제어 활동, 알려진 취약점 악용 또는 봇넷 활동을 포함하여 의심스러운 트래픽 패턴 및 네트워크 이상을 식별하며, 상관 관계가 있을 때 네트워크의 호스트가 손상되었을 가능성이 높은 것으로 나타냅니다. 상관 관계 개체는 Palo Alto Networks 위협 연구 팀에 의해 정의되고 개발되며 방화벽과 Panorama에 대한 주간 동적 업데이트와 함께 제공됩니다. 새 상관

 ©2023 Palo Alto Networks, Inc.

관계 개체를 얻으려면 방화벽에 위협 방지 라이선스가 있어야 합니다. Panorama업데이트를 하려면 지원 라이선스가 필요합니다.

상관 개체에 정의된 패턴은 정적 이거나 동적일 수 있습니다. WildFire에서 관찰된 패턴을 포함하는 상관 관계는 동적이며, WildFire에서 감지한 맬웨어 패턴을 네트워크 또는 Panorama의 트랩 보호 엔드포인트에서 볼 수 있는 호스트가 시작한 명령 및 제어 활동과 상관관계를 지정할 수 있습니다. 예를 들어 호스트가 WildFire 클라우드에 파일을 제출하고 판정이 악의적인 경우 상관 관계 개체는 클라우드에서 볼 수 있는 동일한 동작을 나타내는 네트워크의 다른 호스트 또는 클라이언트를 찾습니다. 맬웨어 샘플이 DNS 쿼리를 수행하고 맬웨어 도메인으로 검색한 경우 상관 관계 개체는 유사한 이벤트에 대한 로그를 구문 분석합니다. 호스트의 활동이 클라우드의 분석과 일치하면 심각도 가중 상관 관계가 높은 이벤트가 기록됩니다.

### 상관 이벤트

상관 관계 개체에 정의된 패턴과 임계값이 네트워크의 트래픽 패턴과 일치할 때 상관 관계가 있는 이벤트가 기록됩니다. 상관 이벤트 해석 및 이벤트의 그래픽 표시를 보려면 ACC에서 손상된 호스트 위젯 사용을(를) 참조하십시오.

## 상관 개체 보기

방화벽에서 현재 사용 가능한 상관 관계 개체를 볼 수 있습니다.

**STEP 1 |** 모니터 > 자동 상관 엔진 > 상관 개체를 선택합니다. 목록의 모든 개체는 기본적으로 활성화되어 있습니다.

| TITLE | CATEGORY | STATE | DESCRIPTION |
|---|---|---|---|
| Multiple User from One Endpoint MFA Credential Theft | credential-theft-abuse | active | This correlation object detects multiple account abuse from a possibly compromised endpoint |
| WildFire C2 | compromised-host | active | This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network. |
| WildFire and Traps ESM Correlated C2 | compromised-host | active | This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware. |
| Single Account and Endpoint MFA Credential Theft | credential-theft-abuse | active | This correlation object detects activity from a possibly compromised user account from a single endpoint |
| Compromise Activity Sequence | compromised-host | active | This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain. |
| Exploit Kit Activity | compromised-host | active | This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature. |
| Single Account 1 FA Multiple Endpoints Credential Timeouts | credential-theft-abuse | active | This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account |
| Beacon Detection | compromised-host | active | This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc. |
| Single Account and Endpoint MFA Credential Timeout | credential-theft-abuse | active | This correlation object detects timedout MFA authentication attempts from a single endpoint using single account |
| Multiple Endpoint MFA Credential Timeout Abuse | credential-theft-abuse | active | This correlation object detects timed out second factor authentications from multiple endpoints using a single user account |
| Multiple Endpoint MFA Credential Abuse | credential-theft-abuse | active | This correlation object detects activity from multiple endpoints using a single user account |
| Exploit Kit Delivering XOR obfuscated malware | compromised-host | active | This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities. |
| Single Account 1 FA Credential Abuse | credential-theft-abuse | active | This correlation object detects timed out first factor authentications from an endpoint using a single user account |


©2023 Palo Alto Networks, Inc.

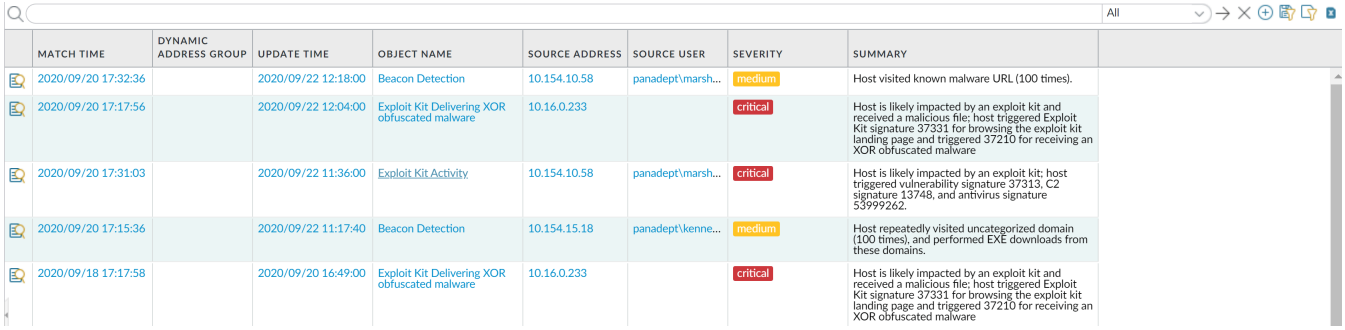
**STEP 2 |** 각 상관 관계 개체에 대한 세부 정보를 봅니다. 각 개체는 다음 정보를 제공합니다.

- 이름 및 제목 - 이름과 제목은 상관 관계 개체가 감지하는 활동 유형을 나타냅니다. 이름 열은 기본적으로 보기에서 숨겨져 있습니다. 개체의 정의를 보려면 열 숨디바이스를 해제하고 이름 링크를 클릭합니다.
- **ID** - 상관 개체를 식별하는 고유 번호입니다. 이 열도 기본적으로 숨겨져 있습니다. ID는 6000 시리즈에 있습니다.
- 카테고리 - 네트워크, 사용자 또는 호스트에 발생하는 위협이나 피해의 종류에 대한 분류입니다. 현재 모든 개체는 네트워크에서 손상된 호스트를 식별합니다.
- 상태 - 상관 관계 개체가 활성화(active) 또는 비활성화(inactive)되었는지의 여부를 나타냅니다. 목록의 모든 개체는 기본적으로 활성화되어 있으므로 활성화됩니다. 이러한 개체는 위협 인텔리전스 데이터를 기반으로 하고 Palo Alto Networks 위협 연구 팀에서 정의하므로 네트워크에서 악의적인 활동을 추적하고 탐지하기 위해 개체를 활성 상태로 유지하십시오.
- 설명 - 방화벽 또는 Panorama가 로그를 분석할 일치 조건을 지정합니다. 이는 악의적인 활동 또는 의심스러운 호스트 동작의 가속화 또는 확대를 식별하기 위해 일치하는 조건의 순서를 설명합니다. 예를 들어, **Compromise Lifecycle** 개체는 스캔 또는 조사 활동으로 시작하여 악용으로 진행하고 알려진 악성 도메인에 대한 네트워크 접촉으로 마무리하는 3단계 에스컬레이션에서 전체 공격 수명 주기에 관련된 호스트를 감지합니다.

자세한 내용은 자동화된 연동 엔진 개념 및 자동화된 연동 엔진 사용을(를) 참조하십시오.

## 상관 이벤트 해석

**Monitor** > **Automated Correlation Engine** > **Correlated Events** 탭에서 각 상호 연관된 이벤트에 대해 생성된 로그를 보고 분석할 수 있습니다.




상관 이벤트 다음 세부 정보가 포함됩니다.

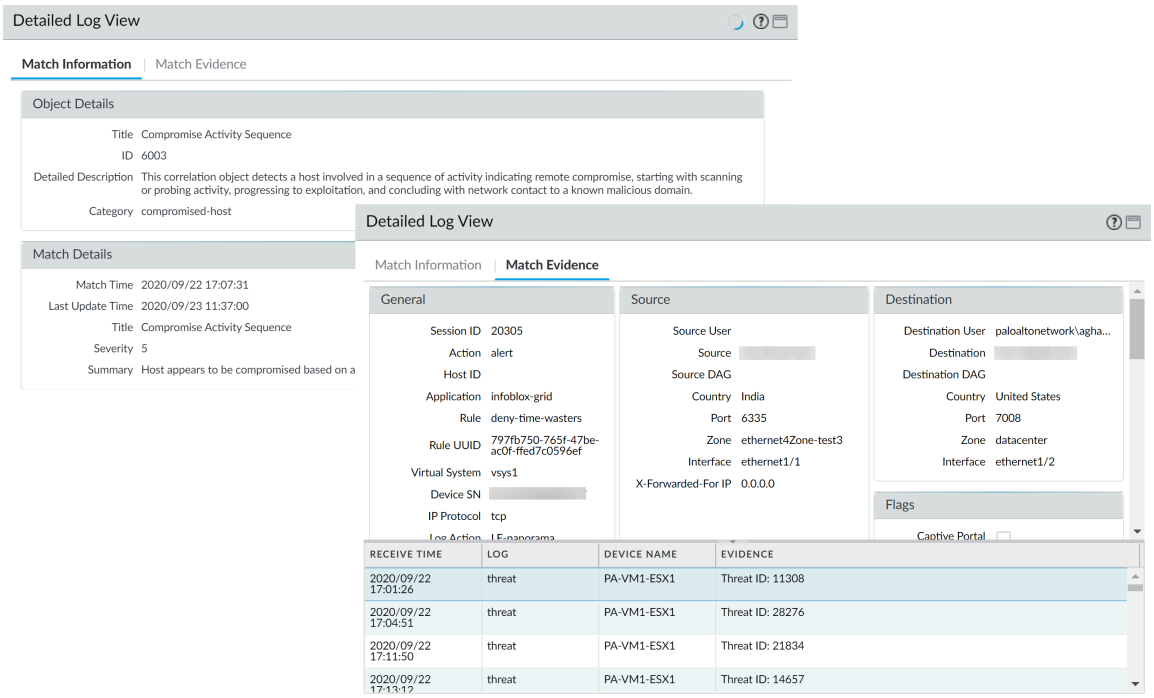
| 필드 | 설명 |
|---|---|
| 매치 타임 | 상관 관계 개체가 일치를 트리거한 시간입니다. |
| 업데이트 시간 | 이벤트가 매칭 기록과 함께 최종적으로 업데이트된 시간입니다. 방화벽이 상호 연관된 개체에 정의된 이벤트 패턴 또는 시퀀스에 대한 기록을 수집하면 상호 연관된 이벤트 로그의 타임스탬프가 업데이트됩니다. |
| 개체 이름 | 일치를 트리거한 상관 관계 개체의 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 | 설명 |
| --- | --- |
| 소스 주소 | 트래픽이 시작된 네트워크의 사용자/디바이스 IP 주소입니다. |
| 소스 사용자 | User-ID이(가) 활성화된 경우 디렉토리 서버의 사용자 및 사용자 그룹 정보입니다. |
| 심각도<br><br>원하는 심각도 수준에 대해 이메일, *SNMP* 또는 *syslog* 메시지를 사용하여 경고를 보내도록 방화벽 또는 *Panorama*를 구성하려면 모니터링을 위해 외부 서비스 사용을(를) 참조하십시오. | 경기의 긴급성과 영향을 나타내는 등급입니다. 심각도 수준은 손상 또는 확대 패턴의 정도와 발생 빈도를 나타냅니다. 상호 연관된 개체는 주로 위협을 탐지하기 위한 것이므로 상호 연관된 이벤트는 일반적으로 네트워크에서 손상된 호스트 식별과 관련되며 심각도는 다음을 의미합니다.<br>• 위험 - 에스컬레이션 패턴을 나타내는 상호 연관된 이벤트를 기반으로 호스트가 손상되었음을 확인합니다. 예를 들어, WildFire에서 악성 판정을 받은 파일을 수신한 호스트가 해당 악성 파일에 대해 WildFire 샌드박스에서 관찰된 것과 동일한 명령 및 제어 활동을 나타낼 때 중요한 이벤트가 기록됩니다.<br>• 높음 - 특정 호스트에서 생성한 명령 및 제어 활동과 일치하는 네트워크의 모든 위치에서 탐지된 멀웨어와 같은 여러 위협 이벤트 간의 상호 연관성을 기반으로 호스트가 손상될 가능성이 매우 높음을 나타냅니다.<br>• 중간 - 스크립팅된 명령 및 제어 활동을 제안하는 알려진 악성 URL에 대한 반복적인 방문과 같은 하나 이상의 의심스러운 이벤트 탐지를 기반으로 호스트가 손상될 가능성이 있음을 나타냅니다.<br>• 낮음 - 악성 URL 또는 동적 DNS 도메인 방문과 같은 하나 이상의 의심스러운 이벤트 탐지를 기반으로 호스트가 손상되었을 수 있음을 나타냅니다.<br>• 정보 - 의심스러운 활동을 식별하는 데 총체적으로 유용할 수 있지만 이벤트 자체가 심각하지는 않은 이벤트를 감지합니다. |
| 요약 | 상관 관계가 있는 이벤트에 수집된 증거를 요약한 설명입니다. |

아이콘을 클릭하면 경기에 대한 모든 증거가 포함된 자세한 로그 보기가 표시됩니다.

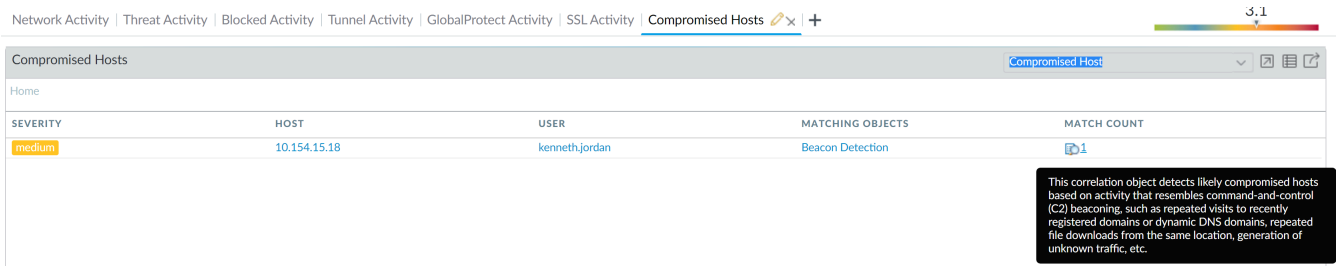

©2023 Palo Alto Networks, Inc.




| 탭 | 설명 |
|---|---|
| 매칭 정보 | 개체 세부 정보: 매칭을 트리거한 상관 개체에 대한 정보를 표시합니다. |
| | 매칭 세부사항: 매칭 시간, 매칭 증거의 마지막 업데이트 시간, 이벤트 심각도 및 이벤트 요약을 포함하는 매칭 세부 정보에 대한 요약입니다. |
| 매칭 증거 | 상호 연관된 이벤트를 확증하는 모든 증거를 제시합니다. 각 세션에 대해 수집된 증거에 대한 자세한 정보를 나열합니다. |

# ACC에서 손상된 호스트 위젯 사용

**ACC** > 위협 활동의 손상된 호스트 위젯은 상관 이벤트를 집계하고 심각도별로 정렬합니다. 이벤트를 트리거한 소스 IP 주소/사용자, 일치하는 상관 관계 개체 및 개체가 일치된 횟수가 표시됩니다. 일치 횟수 링크를 사용하여 일치 증거 세부 정보로 이동합니다.




자세한 내용은 자동화된 연동 엔진 사용 및 애플리케이션 명령 센터 사용을(를) 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 패킷 캡처 가져오기

모든 Palo Alto Networks 방화벽을 사용하면 방화벽의 관리 인터페이스 및 네트워크 인터페이스를 통과하는 트래픽의 패킷 캡처(pcaps)를 수행할 수 있습니다. 데이터 플레인에서 패킷 캡처를 수행할 때 방화벽이 모든 트래픽을 캡처하도록 하드웨어 오프로드 비활성화을(를) 해야 할 수도 있습니다.

> 패킷 캡처는 ***CPU***를 매우 많이 사용하며 방화벽 성능을 저하시킬 수 있습니다**.** 필요한 경우에만 이 기능을 사용하고 필요한 패킷을 수집한 후에는 이 기능을 끄십시오**.**

- 패킷 캡처 유형
- 하드웨어 오프로드 비활성화
- 사용자 지정 패킷 캡처 수행
- 위협 패킷 캡처 수행
- 애플리케이션 패킷 캡처 수행
- 관리 인터페이스에서 패킷 캡처 수행

## 패킷 캡처 유형

수행할 작업에 따라 활성화할 수 있는 패킷 캡처 유형은 다음과 같습니다.

- 사용자 지정 패킷 캡처 - 방화벽은 사용자가 정의한 필터를 기반으로 모든 트래픽 또는 특정 트래픽에 대한 패킷을 캡처합니다. 예를 들어 특정 소스 및 대상 IP 주소 또는 포트와 주고받는 패킷만 캡처하도록 방화벽을 구성할 수 있습니다. 그런 다음 패킷 캡처를 사용하여 네트워크 관련 문제를 해결하거나 애플리케이션 특성을 수집하여 사용자 정의 애플리케이션 서명을 작성하거나 Palo Alto Networks의 애플리케이션 서명을 요청할 수 있습니다. 사용자 지정 패킷 캡처 수행을(를) 참조하십시오.
- 위협 패킷 캡처 - 방화벽은 바이러스, 스파이웨어 또는 취약성을 감지하면 패킷을 캡처합니다. 안티바이러스, 안티스파이웨어 및 취약점 보호 보안 프로파일에서 이 기능을 사용하도록 설정합니다. 패킷 캡처를 보거나 내보낼 수 있는 링크가 위협 로그의 두 번째 열에 나타납니다. 이러한 패킷 캡처는 위협에 대한 컨텍스트를 제공하여 공격의 성공 여부를 확인하거나 공격자가 사용하는 방법에 대해 자세히 알아보는 데 도움이 됩니다. 또한 이러한 유형의 pcap을 Palo Alto Networks에 제출하여 거짓양성 또는 거짓음성으로 느껴질 경우 위협을 다시 분석할 수 있습니다. 위협 패킷 캡처 수행을(를) 참조하십시오.
- 애플리케이션 패킷 캡처 - 방화벽은 사용자가 정의한 특정 애플리케이션 및 필터를 기반으로 패킷을 캡처합니다. 패킷 캡처를 보거나 내보내는 링크는 패킷 캡처 규칙과 일치하는 트래픽에 대한 트래픽 로그의 두 번째 열에 나타납니다. 애플리케이션 패킷 캡처 수행을(를) 참조하십시오.
- 관리 인터페이스 패킷 캡처 - 방화벽이 MGT(관리 인터페이스)에서 패킷을 캡처합니다. 패킷 캡처는 외부 인증 서비스에 대한 방화벽 관리 인증, 소프트웨어 및 콘텐츠 업데이트, 로그 전달, SNMP 서버와의 통신, GlobalProtect 및 인증 포털에 대한 인증 요청과 같이 인터페이스를 통과하는 서비스 문제를 해결할 때 유용합니다. 관리 인터페이스에서 패킷 캡처 수행을(를) 참조하십시오.
- **GTP** 이벤트 패킷 캡처 - 방화벽은 GTP-in-GTP, 최종 사용자 IP 스푸핑 및 비정상적인 GTP 메시지와 같은 단일 GTP 이벤트를 캡처하여 모바일 네트워크 운영자가 GTP 문제 해결을 더 쉽게 수행할 수 있도록 합니다. 모바일 네트워크 보호 프로파일에서 패킷 캡처를 사용하도록 설정합니다.


©2023 Palo Alto Networks, Inc.

## 하드웨어 오프로드 비활성화

Palo Alto Networks 방화벽의 네트워크 데이터 포트를 통과하는 트래픽에 대한 패킷 캡처는 데이터플레인 CPU에 의해 수행됩니다. 관리 인터페이스를 통과하는 트래픽을 캡처하려면 관리 인터페이스에서 패킷 캡처를 수행해야하며, 이 경우 관리 평면에서 패킷 캡처가 수행됩니다.

데이터 평면에서 패킷 캡처가 수행되면 패킷 캡처 필터는 방화벽, 드롭 및 송신 캡처 단계와 비교하여 인그레스(ingress) 스테이지에서 다르게 사용됩니다. 인그레스(ingress) 단계는 패킷 캡처 필터를 사용하여 필터와 일치하는 개별 패킷을 캡처 파일에 복사합니다. 패킷 구문 분석 검사에 실패한 패킷은 캡처되기 전에 삭제됩니다. 방화벽, 드롭 및 송신 캡처 단계는 동일한 패킷 캡처 필터를 사용하여 필터와 일치하는 모든 새 세션을 표시합니다. 세션 테이블에 기록된 각 세션은 클라이언트 간 및 서버 간 연결, 어느 방향으로든 플래그가 지정된 세션과 일치하는 트래픽을 모두 식별하므로 방화벽 단계 및 전송 단계 캡처 파일에 복사됩니다. 마찬가지로 플래그가 지정된 세션과 일치하는 양방향으로 삭제된 트래픽(사후 수신 단계)은 드롭 스테이지 캡처 파일에 복사됩니다.

네트워크 프로세서를 포함하는 방화벽 모델에서 Palo Alto Networks의 특정 미리 결정된 기준을 충족하는 트래픽은 네트워크 프로세서에서 처리하기 위해 오프로드될 수 있습니다. 이러한 오프로드된 트래픽은 데이터 비행기 CPU에 도달하지 않으므로 캡처되지 않습니다. 오프로드된 트래픽을 캡처하려면 CLI를 사용하여 하드웨어 오프로드 기능을 해제해야 합니다.

오프로드될 수 있는 일반적인 유형의 트래픽에는 복호화되지 않은 SSL 및 SSH 트래픽(암호화되는 트래픽은 초기 SSL/SSH 세션 설정을 넘어 유용하게 검사할 수 없음), 네트워크 프로토콜(예: OSPF, BGP, RIP), 애플리케이션 재정의 정책과 일치하는 트래픽이 포함됩니다. ARP, 모든 비 IP 트래픽, IPSec 및 VPN 세션과 같은 일부 유형의 트래픽은 오프로드되지 않습니다. 개별 SYN, FIN 및 RST 패킷은 오프로드된 세션 트래픽의 경우에도 오프로드되지 않으며 네트워크 프로세서에서 인식되면 항상 데이터 플레인 CPU로 포워딩됩니다.

하드웨어 오프로드는 다음 방화벽에서 지원됩니다. *PA-3200* 시리즈, *PA-5200* 시리즈 및 *PA-7000* 시리즈 방화벽.

하드웨어 오프로드를 사용하지 않도록 설정하지 않도록 설정하여 데이터 평면 *CPU* 사용량이 증가할 수 있습니다. 데이터 플레인 *CPU* 사용량이 이미 높은 경우 하드웨어 오프로드를 비활성화하기 전에 유지 관리 기간을 예약할 수 있습니다.

**STEP 1 |** 다음 CLI 명령을 실행하여 하드웨어 오프로드를 비활성화합니다.

```
admin@PA-7050>set session offload no
```

**STEP 2 |** 방화벽이 필요한 트래픽을 캡처한 후 다음 CLI 명령을 실행하여 하드웨어 오프로드를 활성화합니다.

```
admin@PA-7050>set session offload yes
```

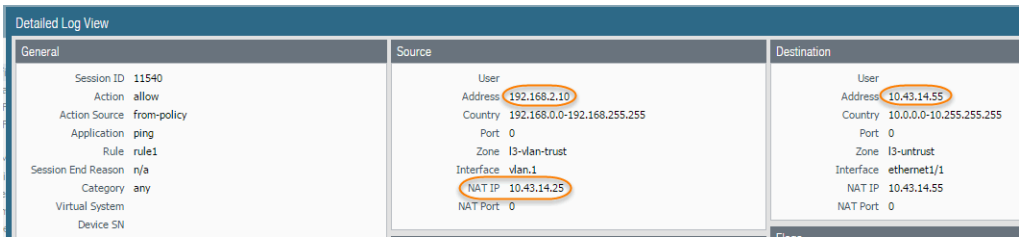
## 사용자 지정 패킷 캡처 수행

사용자 지정 패킷 캡처를 사용하면 방화벽이 캡처할 트래픽을 정의할 수 있습니다. 모든 트래픽을 캡처하려면 하드웨어 오프로드 비활성화이(가) 필요할 수 있습니다.

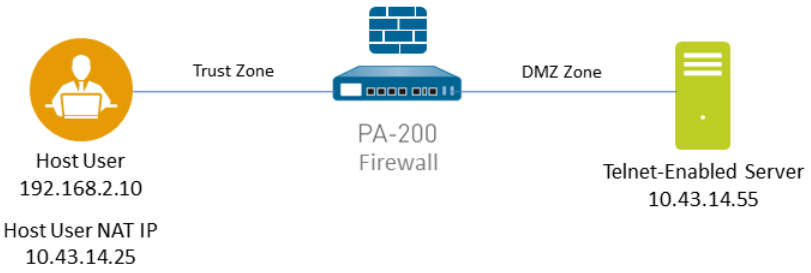

©2023 Palo Alto Networks, Inc.

**STEP 1 |** 패킷 캡처를 시작하기 전에 캡처하려는 트래픽의 속성을 식별하십시오.

예를 들어 두 시스템 간의 트래픽에 대한 소스 IP 주소, 소스 NAT IP 주소 및 대상 IP 주소를 확인하려면 소스 시스템에서 대상 시스템으로 핑(ping)을 수행합니다. 핑(ping)이 완료되면 MonitorTraffic 으로 이동하여 두 시스템의 트래픽 로그를 찾습니다. 로그의 첫 번째 열에 있는 상세 로그 보기 아이콘을 클릭하고 소스 주소, 소스 NAT IP 및 대상 주소를 확인합니다.




다음 예에서는 패킷 캡처를 사용하여 트러스트 영역의 사용자에서 DMZ 영역의 서버로의 Telnet 연결 문제를 해결하는 방법을 보여줍니다.





©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽이 관심 있는 트래픽만 캡처하도록 패킷 캡처 필터를 설정합니다.

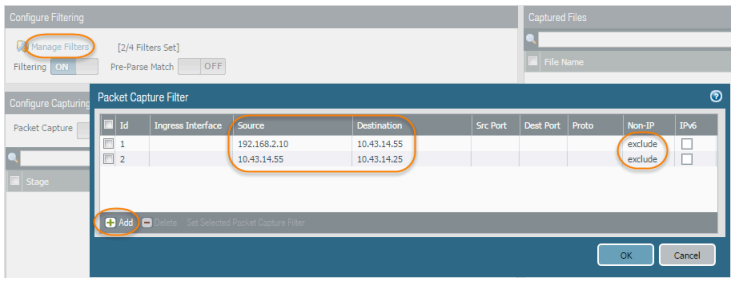
필터를 사용하면 패킷 캡처에 필요한 정보를 더 쉽게 찾을 수 있으며 방화벽이 패킷 캡처를 수행하는 데 필요한 처리 능력을 줄일 수 있습니다. 모든 트래픽을 캡처하려면 필터를 정의하지 않고 필터 옵션을 해제한 상태로 두십시오.

예를 들어 방화벽에서 NAT를 구성한 경우 두 개의 필터를 적용해야 합니다. 첫 번째 것은 pre-NAT 소스 IP 주소를 대상 IP 주소로 필터링하고 두 번째 것은 대상 서버에서 소스 NAT IP 주소로의 트래픽을 필터링합니다.

1. 모니터 패킷 캡처를 선택합니다.
2. 창 하단의 모든 설정 지우기를 클릭하여 기존 캡처 설정을 지웁니다.
3. 필터 관리를 클릭하고 추가를 클릭합니다.
4. Id 1을 선택하고 Source 필드에 관심 있는 소스 IP 주소를 입력하고 Destination 필드에 대상 IP 주소를 입력합니다.

   예를 들어 소스 IP 주소 **192.168.2.10**과 대상 IP 주소 **10.43.14.55**를 입력합니다. 캡처를 추가로 필터링하려면 브로드캐스트 트래픽과 같은 비 IP 트래픽을 제외하도록 Non-IP를 설정합니다.
5. 두 번째 필터를 추가하고 Id 2를 선택합니다.

   예를 들어, Source 필드에 **10.43.14.55**를 입력하고 Destination 필드에 **10.43.14.25**를 입력합니다. 비 IP 드롭다운 메뉴에서 제외를 선택합니다.




6. 확인을 클릭합니다.

**STEP 3 |** 필터링을 켜기로 설정합니다.

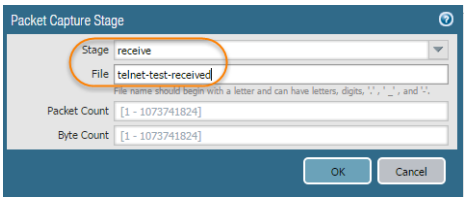

©2023 Palo Alto Networks, Inc.

**STEP 4 |** 패킷 캡처를 트리거하는 트래픽 단계와 캡처된 콘텐츠를 저장하는 데 사용할 파일 이름을 지정합니다. 각 단계의 정의를 보려면 패킷 캡처 페이지에서 도움말 아이콘을 클릭하십시오.

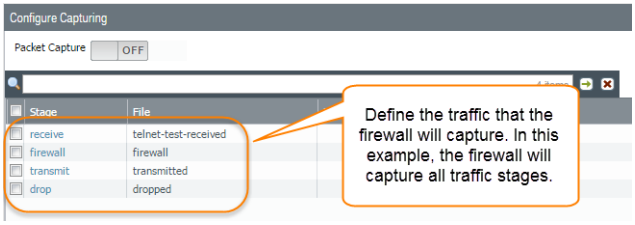
예를 들어, 모든 패킷 캡처 단계를 구성하고 각 단계의 파일 이름을 정의하려면 다음 절차를 수행하십시오.

1. 패킷 캡처 구성에 단계를 추가하고 결과 패킷 캡처에 대한 파일 이름을 정의합니다.

   예를 들어, 스테이지로 수신을 선택한 다음 파일 이름을 telnet-test-received로 설정합니다.

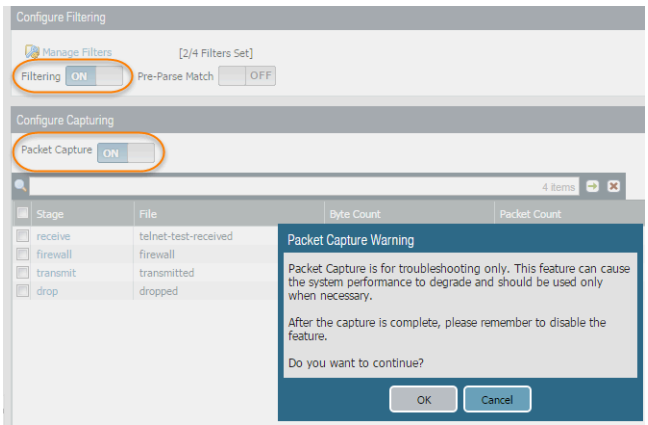



2. 계속해서 캡처하려는 각 단계(수신, 방화벽, 전송 및 삭제)를 추가하고 각 단계에 대해 고유한 파일 이름을 설정합니다.




**STEP 5 |** 패킷 캡처를 켜기로 설정합니다.

방화벽이나 어플라이언스는 시스템 성능이 저하될 수 있음을 경고합니다. 확인을 클릭하여 경고를 확인합니다. 필터를 정의하는 경우 패킷 캡처는 성능에 거의 영향을 미치지 않지만 방화벽이 분석하려는 데이터를 캡처한 후에는 항상 패킷 캡처를 꺼야 합니다.



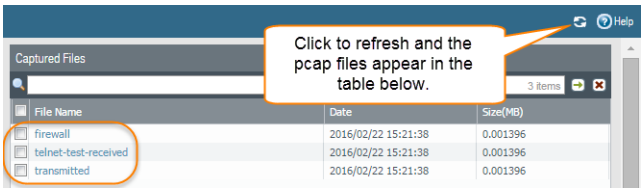

**STEP 6 |** 정의한 필터와 일치하는 트래픽을 생성합니다.

이 예의 경우 소스 시스템(192.168.2.10)에서 다음 명령을 실행하여 소스 시스템에서 Telnet 지원 서버로의 트래픽을 생성합니다.

```
telnet 10.43.14.55
```

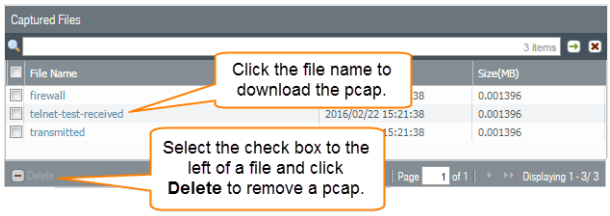

©2023 Palo Alto Networks, Inc.

**STEP 7 |** 패킷 캡처를 해제로 설정한 다음 새로 고침 아이콘을 클릭하여 패킷 캡처 파일을 확인합니다.




이 경우 삭제된 패킷이 없었으므로 방화벽이 삭제 단계에 대한 파일을 생성하지 않았습니다.

**STEP 8 |** 파일 이름 열에서 파일 이름을 클릭하여 패킷 캡처를 다운로드합니다.




**STEP 9 |** 네트워크 패킷 분석기를 사용하여 패킷 캡처 파일을 봅니다.

이 예에서 수신된.pcap 패킷 캡처는 192.168.2.10의 소스 시스템에서 10.43.14.55의 Telnet 지원 서버로의 실패한 Telnet 세션을 보여줍니다. 소스 시스템이 서버에 Telnet 요청을 보냈지만 서버가 응답하지 않았습니다. 이 예에서 서버에 Telnet이 활성화되어 있지 않을 수 있으므로 서버를 확인하십시오.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.2.10 | 10.43.14.55 | TCP | | 66 49525 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 2 | 3.002415 | 192.168.2.10 | 10.43.14.55 | TCP | | 66 49525 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 3 | 9.008679 | 192.168.2.10 | 10.43.14.55 | TCP | | 62 49525 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |

**STEP 10 |** 대상 서버(10.43.14.55)에서 Telnet 서비스를 활성화하고 패킷 캡처를 켜서 새 패킷 캡처를 수행합니다.

**STEP 11 |** 패킷 캡처를 트리거할 트래픽을 생성합니다.

소스 시스템에서 Telnet 지원 서버로 Telnet 세션을 다시 실행하십시오.

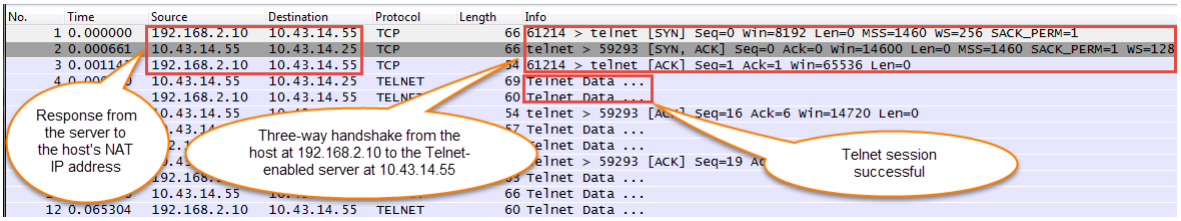
```
telnet 10.43.14.55
```


©2023 Palo Alto Networks, Inc.

**STEP 12 |** 수신된.pcap 파일을 다운로드하여 열고 네트워크 패킷 분석기를 사용하여 봅니다.

다음 패킷 캡처는 이제 192.168.2.10의 호스트 사용자에서 10.43.14.55의 Telnet 사용 서버로의 성공적인 Telnet 세션을 보여줍니다.

*NAT* 주소 *10.43.14.25*도 표시됩니다. 서버가 응답하면 *NAT* 주소에 응답합니다. 호스트와 서버 간의 *3*방향 핸드쉐이크에 표시된 대로 세션이 성공한 것을 볼 수 있으며 *Telnet* 데이터가 표시됩니다.




## 위협 패킷 캡처 수행

방화벽이 위협을 탐지할 때 패킷 캡처(pcap)를 수행하도록 구성하려면 바이러스 백신, 안티 스파이웨어 및 취약점 보호 보안 프로파일에서 패킷 캡처를 활성화합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 보안 프로파일에서 패킷 캡처 옵션을 활성화합니다.

일부 보안 프로파일을 사용하면 단일 패킷 캡처 또는 확장 캡처를 정의할 수 있습니다. 확장 캡처를 선택하는 경우 캡처 길이를 정의합니다. 이렇게 하면 방화벽이 더 많은 패킷을 캡처하여 위협과 관련된 추가 컨텍스트를 제공할 수 있습니다.

주어진 위협에 대한 작업이 허용되는 경우 방화벽은 위협 로그를 트리거하지 않고 패킷을 캡처하지 않습니다. 작업이 경고인 경우 패킷 캡처를 단일 패킷 또는 확장 캡처로 설정할 수 있습니다. 모든 차단 작업(삭제, 차단 및 재설정 작업)은 단일 패킷을 캡처합니다. 디바이스의 콘텐츠 패키지에 따라 기본 작업이 결정됩니다.

1. 개체 > 보안 프로파일을 선택한 다음 다음과 같이 지원되는 프로파일에 대해 패킷 캡처 옵션을 활성화합니다.
   - 바이러스 백신 - 사용자 정의 바이러스 백신 프로파일을 선택한 다음 바이러스 백신 탭에서 패킷 캡처 체크박스를 선택합니다.
   - 안티스파이웨어 - 사용자 지정 안티스파이웨어 프로파일을 선택한 다음 **DNS** 서명 탭을 클릭한 다음 패킷 캡처 드롭다운에서 단일 패킷 또는 확장 캡처를 선택합니다.
   - 취약성 보호 - 사용자 지정 취약성 보호 프로파일을 선택한 다음 규칙 탭에서 추가를 클릭하여 새 규칙을 추가하거나 기존 규칙을 선택합니다. 패킷 캡처를 단일 패킷 또는 확장 캡처로 설정합니다.

   프로파일에 서명 예외가 정의되어 있으면 예외 탭을 클릭하고 서명에 대한 패킷 캡처 열에서 단일 패킷 또는 확장 캡처를 설정합니다.
2. (선택 사항) 프로파일에 대해 확장 캡처를 선택한 경우 확장 패킷 캡처 길이를 정의합니다.
   1. **Device** > **Setup** > **Content-ID**를 선택한 다음 Content-ID 설정을 편집합니다.
   2. 확장된 패킷 캡처 길이**(**패킷**)** 섹션에서 방화벽이 캡처할 패킷 수를 지정합니다(범위는 1-50, 기본값은 5).
   3. 확인을 클릭합니다.

**STEP 2 |** 보안 정책 규칙에 보안 프로파일(패킷 캡처 사용)을 추가합니다.

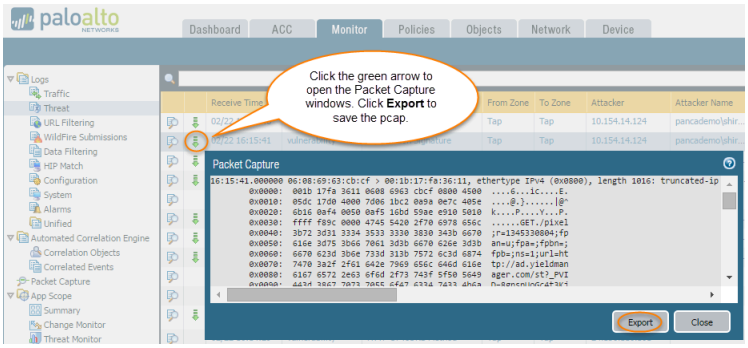
1. 정책 > 보안을 선택하고 규칙을 선택합니다.
2. 작업 탭을 선택합니다.
3. 프로파일 설정 섹션에서 패킷 캡처가 활성화된 프로파일을 선택합니다.

   예를 들어 바이러스 백신 드롭다운을 클릭하고 패킷 캡처가 활성화된 프로파일을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 위협 로그에서 패킷 캡처를 보거나 내보냅니다.

1. 모니터 > 로그 > 위협을 선택합니다.
2. 관심 있는 로그 항목의 두 번째 열에 있는 녹색 패킷 캡처 아이콘 을 클릭합니다. 패킷 캡처를 직접 보거나 시스템으로 내보냅니다.




# 애플리케이션 패킷 캡처 수행

다음 항목에서는 애플리케이션 패킷 캡처를 수행하도록 방화벽을 구성할 수 있는 두 가지 방법에 대해 설명합니다.

- 알 수 없는 애플리케이션에 대한 패킷 캡처 수행
- 맞춤형 애플리케이션 패킷 캡처 수행

## 알 수 없는 애플리케이션에 대한 패킷 캡처 수행

Palo Alto Networks 방화벽은 방화벽이 식별할 수 없는 애플리케이션이 포함된 세션에 대해 패킷 캡처를 자동으로 생성합니다. 일반적으로 알 수 없는 트래픽(tcp, udp 또는 non-syn-tcp)으로 분류되는 유일한 애플리케이션은 아직 App-ID 서명이 없거나 네트워크의 내부 또는 사용자 지정 애플리케이션 또는 잠재적 위협인 상용 애플리케이션입니다. 이러한 패킷 캡처를 사용하여 알 수 없는 애플리케이션과 관련된 추가 컨텍스트를 수집하거나 정보를 사용하여 잠재적 위협에 대한 트래픽을 분석할 수 있습니다. 보안 정책을 통해 제어하거나 사용자 지정 애플리케이션 서명을 작성한 다음 사용자 지정 서명을 기반으로 보안 규칙을 만들어 사용자 지정 또는 알 수 없는 애플리케이션을 관리할 수도 있습니다. 애플리케이션이 상용 애플리케이션인 경우 패킷 캡처를 Palo Alto Networks에 제출하여 App-ID 서명을 생성할 수 있습니다.

**STEP 1 |** 알 수 없는 애플리케이션 패킷 캡처가 활성화되어 있는지 확인합니다(이 옵션은 기본적으로 활성화되어 있음).

1. 알 수 없는 애플리케이션 캡처 설정을 보려면 다음 CLI 명령을 실행하십시오.

```
admin@PA-220>show running application setting | match  “Unknown capture”
```

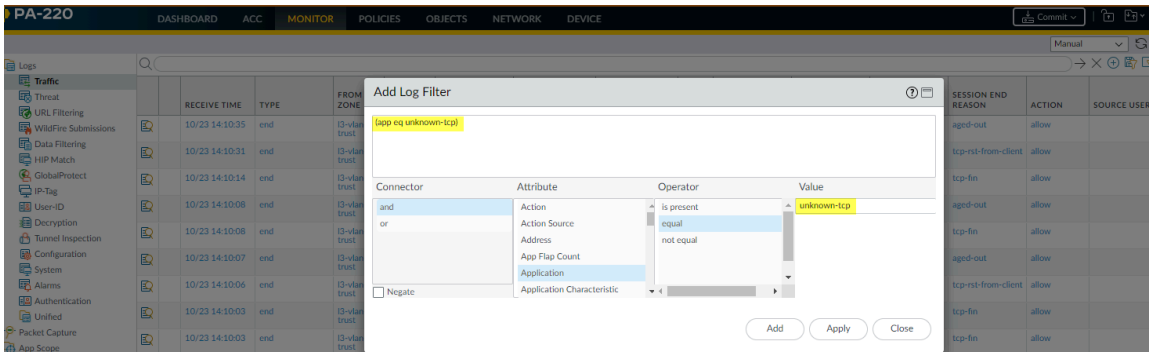
2. 알 수 없는 캡처 설정 옵션이 꺼져 있으면 활성화합니다.

```
admin@PA-220>set application dump-unknown yes
```

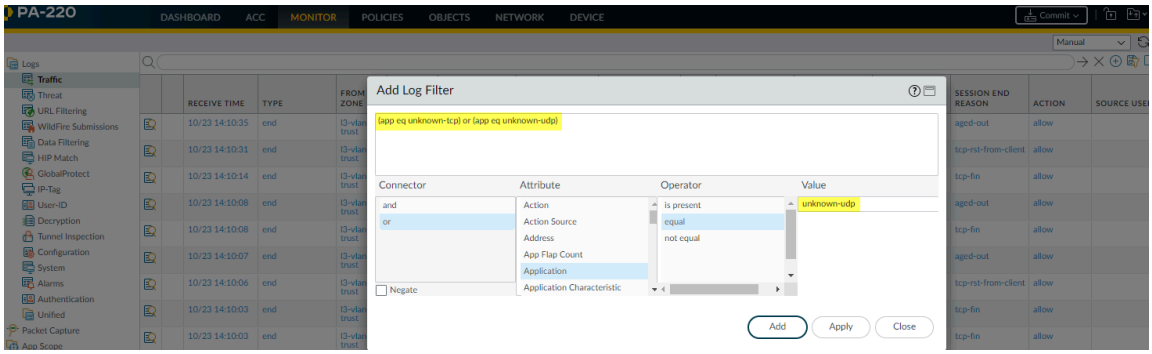

©2023 Palo Alto Networks, Inc.

**STEP 2 |** 트래픽 로그를 필터링하여 알 수 없는 TCP 및 UDP 애플리케이션을 찾습니다.

1. 모니터 > 로그 > 트래픽을 선택합니다.
2. 필터 추가를 클릭하고 필터의 알 수 없는 TCP 부분을 생성합니다(**Connector** = "and", **Attribute** = "Application", **Operator** = "equal"이고 **Value**로 "unknown-tcp"를 입력한 다음 **Add**를 클릭하여 필터에 쿼리를 추가합니다.

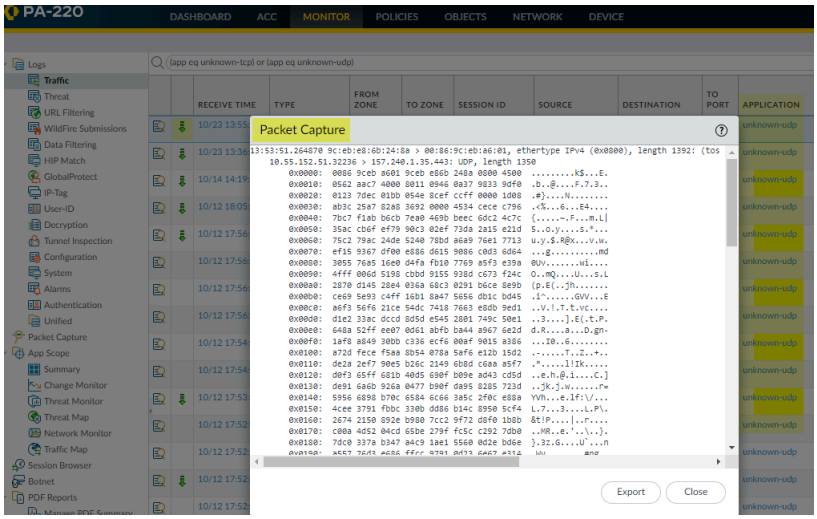



3. 필터의 알 수 없는 UDP 부분을 생성합니다(**Connector** = "or", **Attribute** = "Application", **Operator** = "equal", "unknown- udp"를 값으로 지정한 다음 추가를 클릭하여 필터에 쿼리를 추가합니다.




4. 적용을 클릭하여 로그 화면 쿼리 필드에 필터를 배치합니다.

**STEP 3 |** 쿼리 필드 옆에 있는 필터 적용 화살표를 클릭하여 필터를 실행한 다음 패킷 캡처 아이콘 을 클릭하여 패킷 캡처를 보거나 로컬 시스템으로 내보내기합니다.




 ©2023 Palo Alto Networks, Inc.

## 맞춤형 애플리케이션 패킷 캡처 수행

사용자가 정의한 애플리케이션 이름과 필터를 기반으로 패킷 캡처를 수행하도록 Palo Alto Networks 방화벽을 구성할 수 있습니다. 그런 다음 패킷 캡처를 사용하여 애플리케이션 제어 문제를 해결할 수 있습니다. 애플리케이션 패킷 캡처를 구성할 때 App-ID 데이터베이스에 정의된 애플리케이션 이름을 사용해야 합니다. Applipedia를 사용하거나 **Objects** > **Applications**의 방화벽 웹 인터페이스에서 모든 App-ID 애플리케이션 목록을 볼 수 있습니다.

**STEP 1 |** PuTTY와 같은 터미널 에뮬레이션 애플리케이션을 사용하여 방화벽에 대한 SSH 세션을 시작합니다.

**STEP 2 |** 애플리케이션 패킷 캡처를 켜고 필터를 정의합니다.

```
admin@PA-220>set application dump on application <application-name>
 rule <rule-name>
```

예를 들어 Social Networking Apps라는 보안 규칙과 일치하는 연결된 기반 애플리케이션에 대한 패킷을 캡처하려면 다음 CLI 명령을 실행합니다.

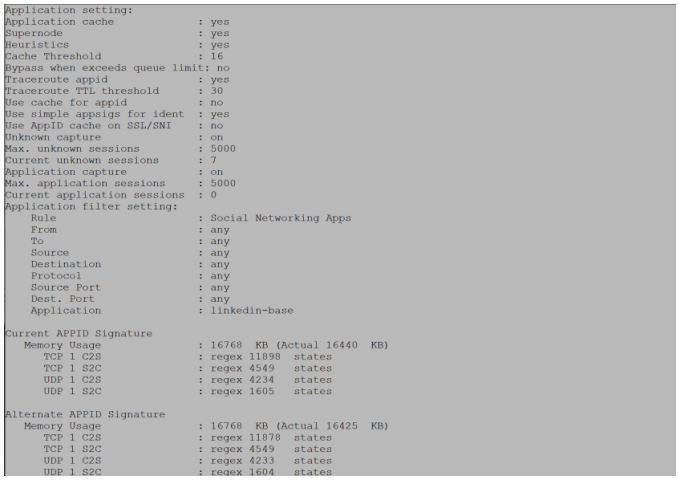
```
admin@PA-220>set application dump on application linkedin-base rule
 "Social Networking Apps"
```



소스 *IP* 주소 및 대상 *IP* 주소와 같은 다른 필터를 적용할 수도 있습니다.

**STEP 3 |** 패킷 캡처 출력을 보고 올바른 필터가 적용되었는지 확인합니다. 패킷 캡처를 활성화하면 출력이 표시됩니다.

다음 출력은 이제 애플리케이션 캡처 필터링이 소셜 네트워킹 앱 규칙과 일치하는 트래픽에 대한 링크드인 기반 애플리케이션을 기반으로 함을 확인합니다.



```
Application setting:
Application cache            : yes
Supernode                    : yes
Heuristics                   : yes
Cache Threshold              : 16
Bypass when exceeds queue limit: no
Traceroute appid             : yes
Traceroute TTL threshold     : 30
Use cache for appid          : no
Use simple appsigs for ident : yes
Use AppID cache on SSL/SNI   : no
Unknown capture              : on
Max. unknown sessions        : 5000
Current unknown sessions     : 7
Application capture          : on
Max. application sessions    : 5000
Current application sessions : 0
Application filter setting:
    Rule                     : Social Networking Apps
    From                     : any
    To                       : any
    Source                   : any
    Destination              : any
    Protocol                 : any
    Source Port              : any
    Dest. Port               : any
    Application              : linkedin-base

Current APPID Signature
   Memory Usage              : 16768  KB (Actual 16440  KB)
      TCP 1 C2S              : regex 11898  states
      TCP 1 S2C              : regex 4549   states
      UDP 1 C2S              : regex 4234   states
      UDP 1 S2C              : regex 1605   states

Alternate APPID Signature
   Memory Usage              : 16768  KB (Actual 16425  KB)
      TCP 1 C2S              : regex 11878  states
      TCP 1 S2C              : regex 4549   states
      UDP 1 C2S              : regex 4233   states
      UDP 1 S2C              : regex 1604   states
```

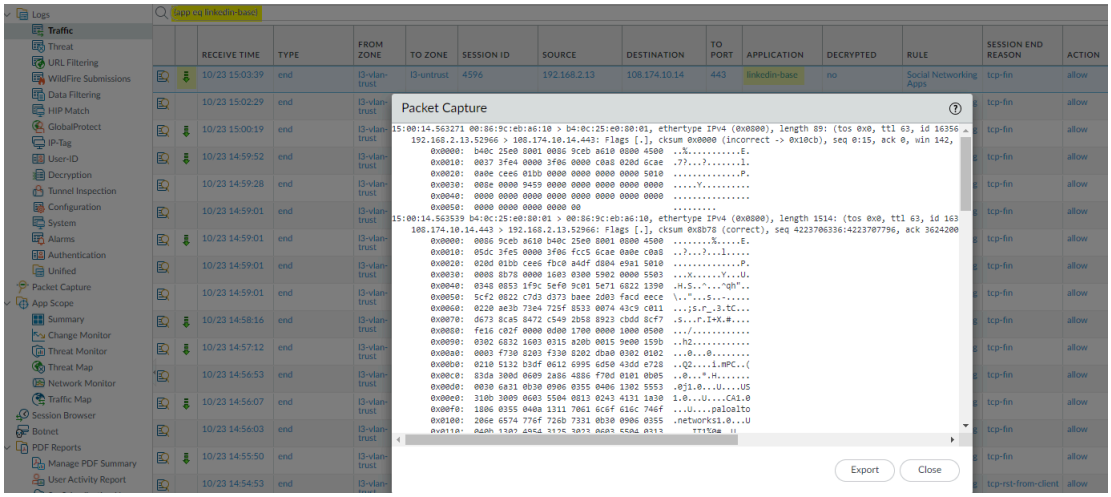
**STEP 4 |** 웹 브라우저에서 linkedin.com에 액세스하고 일부 LinkedIn 작업을 수행하여 LinkedIn 트래픽을 생성한 후 다음 CLI 명령을 실행하여 애플리케이션 패킷 캡처를 끕니다.

```
admin@PA-220>set application dump off
```


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 패킷 캡처 보기/내보내기

1. 방화벽의 웹 인터페이스에 로그인하고 모니터 > 로그 > 트래픽을 선택합니다.
2. 관심 있는 로그 항목에서 녹색 패킷 캡처 아이콘 을 클릭합니다.
3. 패킷 캡처를 직접 보거나 컴퓨터로 내보냅니다. 다음 화면 캡처는 링크드인 기반 패킷 캡처를 보여줍니다.




## 관리 인터페이스에서 패킷 캡처 수행

**tcpdump** CLI 명령을 사용하면 Palo Alto Networks 방화벽에서 관리 인터페이스(MGT)를 통과하는 패킷을 캡처할 수 있습니다.

각 플랫폼에는 ***tcpdump***가 캡처하는 기본 바이트 수가 있습니다. *PA-220* 방화벽은 각 패킷에서 *68*바이트의 데이터를 캡처하고 그 이상의 데이터는 잘립니다. *PA-7000* 시리즈 방화벽 및 *VM* 시리즈 방화벽은 각 패킷에서 *96*바이트의 데이터를 캡처합니다. ***tcpdump***가 캡처할 패킷 수를 정의하려면 ***snaplen***(스냅 길이) 옵션(범위 *0-65535*)을 사용하십시오. ***snaplen***을 *0*으로 설정하면 방화벽이 전체 패킷을 캡처하는 데 필요한 최대 길이를 사용합니다.

**STEP 1 |** PuTTY와 같은 터미널 에뮬레이션 애플리케이션을 사용하여 방화벽에 대한 SSH 세션을 시작합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** MGT 인터페이스에서 패킷 캡처를 시작하려면 다음 명령을 실행합니다.

```
admin@PA-220>tcpdump filter “<filter-option> <IP-address>” snaplen
 length
```

예를 들어 관리자가 RADIUS를 사용하여 방화벽에 인증할 때 생성되는 트래픽을 캡처하려면 RADIUS 서버의 대상 IP 주소(이 예에서는 10.5.104.99)를 필터링합니다.

```
admin@PA-220>tcpdump filter “dst 10.5.104.99” snaplen 0
```

src(소스 IP 주소), 호스트, 네트를 필터링할 수도 있고 콘텐츠를 제외할 수도 있습니다. 예를 들어 서브넷을 필터링하고 모든 SCP, SFTP 및 SSH 트래픽(포트 22 사용)을 제외하려면 다음 명령을 실행합니다.

```
admin@PA-220>tcpdump filter “net 10.5.104.0/24 and not port 22”
 snaplen 0
```

***tcpdump***가 패킷 캡처를 수행할 때마다 내용을 *mgmt.pcap*이라는 파일에 저장합니다. 이 파일은 ***tcpdump***를 실행할 때마다 덮어씁니다.

**STEP 3 |** 관심 있는 트래픽이 MGT 인터페이스를 통과한 후 Ctrl + C를 눌러 캡처를 중지합니다.

**STEP 4 |** 다음 명령을 실행하여 패킷 캡처를 봅니다.

```
admin@PA-220> view-pcap mgmt-pcap mgmt.pcap
```

다음 출력은 MGT 포트(10.5.104.98)에서 RADIUS 서버(10.5.104.99)로의 패킷 캡처를 보여줍니다.

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius:
 RADIUS, 액세스 요청(1), ID: 0x00 길이: 89 09:55:29.144354 arp reply
 10.5.104.98 is-at 00:25:90:23:94:98 (oui Unknown) 09:55:29.379290
 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, 액세스 요청(1),
 ID: 0x00 길이: 70 09:55:34.379262 arp who-has 10.5.104.99 tell
 10.5.104.98
```


©2023 Palo Alto Networks, Inc.

**STEP 5 |** (선택 사항) SCP(또는 TFTP)를 사용하여 방화벽에서 패킷 캡처를 내보냅니다. 예를 들어 SCP를 사용하여 패킷 캡처를 내보내려면 다음 명령을 실행합니다.

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap
 to <username@host:path>
```

예를 들어 pcap을 10.5.5.20의 SCP 지원 서버와 temp-SCP라는 임시 폴더로 내보내려면 다음 CLI 명령을 실행합니다.

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to
 admin@10.5.5.20:c:/temp-SCP
```

방화벽이 패킷 캡처를 SCP 지원의 c:\temp-SCP 폴더에 복사할 수 있도록 SCP 서버의 계정에 대한 로그인 이름과 암호를 입력합니다.

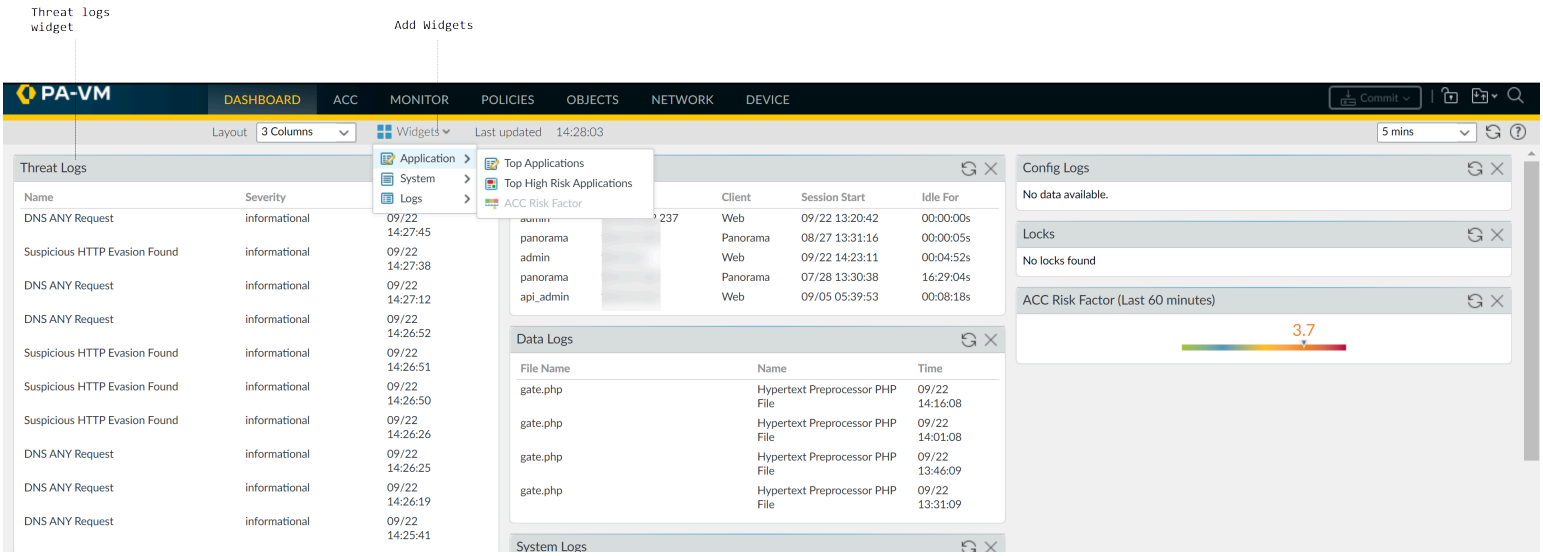
**STEP 6 |** 이제 Wireshark와 같은 네트워크 패킷 분석기를 사용하여 패킷 캡처 파일을 볼 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

# 애플리케이션 및 위협 모니터링

모든 Palo Alto Networks의 차세대 방화벽에는 프로토콜, 암호화 또는 회피 전략에 관계없이 네트워크를 통과하는 애플리케이션을 식별하는 App-ID 기술이 탑재되어 있습니다. 그런 다음 애플리케이션 명령 센터 사용을(를) 하여 애플리케이션을 모니터링할 수 있습니다. ACC는 다양한 로그 데이터베이스의 데이터를 그래픽으로 요약하여 네트워크를 통과하는 애플리케이션, 현재 사용자 및 잠재적 보안 영향을 강조합니다. ACC는 App-ID가 수행하는 지속적인 트래픽 분류를 사용하여 동적으로 업데이트됩니다. 애플리케이션이 포트나 동작을 변경하면 App-ID는 계속해서 트래픽을 확인하고 결과를 ACC에 표시합니다. URL 카테고리, 위협 및 데이터에 대한 추가 가시성을 통해 네트워크 활동에 대한 완전하고 균형 잡힌 그림을 제공합니다. ACC를 사용하면 네트워크를 통과하는 트래픽에 대해 매우 빠르게 파악한 다음 해당 정보를 보다 정보에 입각한 보안 정책으로 변환할 수 있습니다.

대시보드 사용을(를) 하여, 네트워크를 모니터링할 수도 있습니다.




콘텐츠 전송 네트워크 인프라를 검토하여 방화벽에 로깅된 이벤트가 보안 위험을 초래하는지 확인합니다. AutoFocus 인텔리전스 요약은 네트워크 및 글로벌 규모의 로그와 관련된 속성, 활동 또는 동작의 보급과 이에 연결된 WildFire 버딕트(verdict) 및 AutoFocus 태그를 보여줍니다. AutoFocus 구독이 활성화되면 이 정보를 사용하여 네트워크의 특정 위협을 추적하는 맞춤형 AutoFocus 경고를 생성할 수 있습니다.


©2023 Palo Alto Networks, Inc.

# 로그 보기 및 관리

로그는 방화벽의 시스템 이벤트 또는 방화벽이 모니터링하는 네트워크 트래픽 이벤트에 대한 감사 추적을 제공하는 자동으로 생성되고 타임스탬프가 찍힌 파일입니다. 로그 항목에는 공격자의 애플리케이션 유형 또는 IP 주소와 같이 기록된 이벤트와 관련된 속성, 활동 또는 동작인 아티팩트가 포함됩니다. 각 로그 유형은 별도의 이벤트 유형에 대한 정보를 기록합니다. 예를 들어 방화벽은 스파이웨어, 취약점 또는 바이러스 서명과 일치하는 트래픽을 기록하기 위해 위협 로그를 생성하거나 방화벽에서 포트 스캔 또는 호스트 스윕 활동에 대해 구성된 임계값과 일치하는 DoS 공격을 기록합니다.

- 로그 유형 및 심각도 수준
- 로그 보기
- 필터 로그
- 로그 내보내기
- 로그 스토리지 할당량 및 만료 기간 구성
- SCP 또는 FTP 서버로 로그 내보내기 예약

## 로그 유형 및 심각도 수준

모니터 > 로그 페이지에서 다음 로그 유형을 볼 수 있습니다.

- 트래픽 로그
- 위협 로그
- URL 필터링 로그
- WildFire 제출 로그
- 데이터 필터링 로그
- 상관 로그
- 터널 검사 로그
- 구성 로그
- 시스템 로그
- HIP 매치 로그
- GlobalProtect 로그
- IP 태그 로그
- 사용자 ID 로그
- 복호화 로그
- 알람 로그
- 인증 로그
- 통합 로그


©2023 Palo Alto Networks, Inc.

## 트래픽 로그

트래픽 로그는 각 세션의 시작과 끝 항목을 표시합니다. 각 항목에는 날짜 및 시간, 소스 및 대상 영역, 소스 및 대상 동적 주소 그룹, 주소 및 포트, 애플리케이션 이름, 트래픽 플로우에 적용된 보안 규칙, 규칙 작업(허용, 거부 또는 삭제), 인그레스 및 이그레스(Egress) 인터페이스, 바이트 수 및 세션 종료 이유에 대한 정보가 포함됩니다.

동적 주소 그룹에는 트래픽 일치 규칙에 동적 주소 그룹이 포함된 경우에만 로그에 나타납니다. *IP* 주소가 두 개 이상의 동적 주소 그룹에 나타나면 방화벽은 소스 *IP* 주소와 함께 최대 *5*개의 동적 주소 그룹을 로그에 표시합니다.

유형 열은 항목이 세션의 시작 또는 종료를 위한 것인지의 여부를 나타냅니다. 작업 열은 방화벽이 세션을 허용, 거부 또는 삭제했는지의 여부를 나타냅니다. 드롭은 트래픽을 차단한 보안 규칙이 애플리케이션을 지정했음을 나타내는 반면 거부는 규칙이 특정 애플리케이션을 식별했음을 나타냅니다. 규칙이 특정 서비스에 대한 모든 트래픽을 삭제하는 경우와 같이 방화벽이 애플리케이션을 식별하기 전에 트래픽을 삭제하는 경우 애플리케이션 열은 적용 불가로 표시됩니다.

항목 옆을 클릭하면 ICMP 항목이 동일한 소스와 대상 간의 여러 세션을 집계하는지의 여부(이 경우 개수 열 값이 1보다 큼)와 같은 세션에 대한 추가 세부 정보를 볼 수 있습니다.

*PAN-OS 10.2*에 도입된 복호화 로그가 비활성화되면 방화벽은 *HTTP/2* 로그를 트래픽 로그로 보냅니다. 그러나 복호화 로그가 활성화되면 방화벽은 *HTTP/2* 로그를 터널 검사 로그로 보내면*(*복호화 로그 비활성화 시 *HTTP/2* 로그를 트래픽 로그로 전송*),* 따라서 *HTTP/2* 이벤트에 대한 트래픽 로그 대신 터널 검사 로그를 확인해야 합니다.

## 위협 로그

위협 로그는 트래픽이 방화벽의 보안 규칙에 연결된 보안 프로파일 중 하나와 일치할 때 항목을 표시합니다. 각 항목에는 날짜와 시간: 위협 유형(예 : 바이러스 또는 스파이웨어), 위협 설명 또는 URL(이름 열), 소스 및 대상 영역, 주소, 소스 및 대상 동적 주소 그룹 및 포트, 애플리케이션 이름, 알람 작업(예: 허용 또는 차단) 및 심각도 수준이 포함됩니다.

동적 주소 그룹에는 트래픽 일치 규칙에 동적 주소 그룹이 포함된 경우에만 로그에 나타납니다. *IP* 주소가 두 개 이상의 동적 주소 그룹에 나타나면 방화벽은 소스 *IP* 주소와 함께 최대 *5*개의 동적 주소 그룹을 로그에 표시합니다.

개별 위협 로그 항목에 대한 자세한 내용을 보려면 다음을 참조하십시오.

- 위협 항목 옆을 클릭하여 항목이 동일한 소스과 대상 간에 동일한 유형의 여러 위협을 집계하는지의 여부(이 경우 Count 열 값이 하나보다 큰 경우)와 같은 형식의 여러 위협을 집계하는지의 여부와 같은 세부 정보를 봅니다.
- 방화벽을 패킷 캡처 가져오기로 구성한 경우 항목 옆에 있는 를 클릭하여 캡처된 패킷에 액세스합니다.

다음 표는 위협 심각도 수준을 요약합니다.


©2023 Palo Alto Networks, Inc.

| 심각성 | 설명 |
| --- | --- |
| 심각 | 널리 배포된 소프트웨어의 기본 설치에 영향을 주는 것과 같은 심각한 위협은 서버의 루트 손상을 초래하고 공격자에게 익스플로잇 코드가 널리 사용됩니다. 공격자는 일반적으로 개별 피해자에 대한 특별한 인증 자격 증명이나 지식이 필요하지 않으며 대상을 조작하여 특수 기능을 수행할 필요가 없습니다. |
| 높**dma** | 중요해질 수 있지만 완화 요인이 있는 위협, 예를 들어 악용하기 어렵거나 권한이 높아지지 않거나 큰 피해자 풀이 없을 수 있습니다.<br>WildFire 제출물은 악의적인 판결과 허용하도록 설정된 작업 집합이 높은 항목으로 기록됩니다. |
| 중간 | 대상을 손상시키지 않는 DoS 공격이나 공격자가 피해자와 동일한 LAN에 있어야 하는 익스플로잇과 같이 영향이 최소화되는 사소한 위협은 비표준 구성 또는 모호한 애플리케이션에만 영향을 미치거나 매우 제한된 액세스를 제공합니다.<br>• 악의적인 판정과 기존 WildFire 서명 심각도에 따라 블록 또는 경고 작업이 있는 위협 로그 항목은 Medium으로 기록됩니다. |
| 낮음 | 조직의 인프라에 거의 영향을 미치지 않는 경고 수준 위협입니다. 그들은 일반적으로 로컬 또는 물리적 시스템 액세스를 필요로하고 종종 피해자 개인 정보 보호 또는 DoS 문제 및 정보 유출을 초래할 수 있습니다.<br>• 데이터 필터링 프로파일 일치항목이 낮음으로 기록됩니다.<br>• WildFire 제출 로그 항목에는 그레이웨어 판정과 모든 작업이 낮음으로 기록됩니다. |
| 정보 제공 | 즉각적인 위협이 되지는 않지만 존재할 수 있는 더 심각한 문제에 주의를 환기시키는 의심스러운 사건입니다.<br>• URL 필터링 로그 항목은 정보 로그 항목으로 기록됩니다.<br>• WildFire 제출물은 악성 판정으로 항목을 기록하고 모든 작업은 정보로 기록됩니다.<br>• 모든 판정과 차단 및 전달로 설정된 작업이 있는 WildFire 제출 로그 항목은 정보용으로 기록됩니다.<br>• 모든 베리딕트와 차단으로 설정된 작업이 있는 로그 항목은 정보용으로 기록됩니다. |

## URL 필터링 로그

URL 필터링로그(모니터 > 로그 > **URL** 필터링)는 보안 정책 규칙에서 모니터링되는 URL 범주에 대한 트래픽에 대한 포괄적인 정보를 표시합니다. 각 세션에 대해 기록된 속성 또는 속성에는 **수신 시간, 범주, URL, 영역에서 영역, 소스 및 소스 사용자**가 포함됩니다. 가장 관심 있는 속성만 표시되도록 로그 보기를 사용자 정의할 수 있습니다. 방화벽은 다음과 같은 경우 URL 필터링 로그 항목을 생성합니다.

- 트래픽은 일치 기준으로 URL 범주가 있는 보안 정책 규칙과 일치합니다. 규칙은 트래픽에 대해 다음 작업 중 하나를 적용합니다.**거부, 삭제 또는 재설정(클라이언트, 서버, 둘 다)**.


©2023 Palo Alto Networks, Inc.

- 트래픽은 URL 필터링 프로파일이 연결된 보안 정책 규칙과 일치합니다. 프로파일의 범주에 대한 사이트 액세스는 **경고**, **차단**, **계속** 또는 **재정의**로 설정됩니다.

> 기본적으로 허용으로 설정된 범주는 ***URL*** 필터링 로그 항목을 생성하지 않습니다. 예외는 로그 전달을 구성하는 경우입니다.
>
> 방화벽이 허용하지만 더 많은 가시성을 원하는 카테고리에 대한 트래픽을 기록하도록 하려면 ***URL*** 필터링 프로파일에서 이러한 카테고리에 대한 사이트 액세스를 경고로 설정하십시오.

## WildFire 제출 로그

방화벽은 WildFire Analysis 프로파일 설정(**Objects** > **Security Profiles** > **WildFire Analysis**)을 기반으로 분석을 위해 샘플(파일 및 이메일 링크)을 WildFire 클라우드로 포워딩합니다. 방화벽은 WildFire가 샘플의 정적 및 동적 분석을 완료한 후 포워딩하는 각 샘플에 대해 WildFire 제출 로그 항목을 생성합니다. WildFire 제출 로그 항목에는 샘플에 대한 방화벽 작업(허용 또는 차단), 제출된 샘플에 대한 WildFire 판정 및 샘플의 심각도 수준이 포함됩니다.

다음 표에는 WildFire 판결이 요약되어 있습니다.

| 평결 | 설명 |
|---|---|
| 온화한 | 항목이 WildFire 분석 양성 판정을 받았음을 나타냅니다. 양성으로 분류된 파일은 안전하며 악의적인 동작을 나타내지 않습니다. |
| 그레이웨어 | 항목이 WildFire 분석 그레이웨어 판정을 받았음을 나타냅니다. 그레이웨어로 분류된 파일은 직접적인 보안 위협이 되지는 않지만 눈에 띄는 행동을 보일 수 있습니다. 그레이웨어에는 애드웨어, 스파이웨어 및 BHO(브라우저 도우미 개체)가 포함될 수 있습니다. |
| 피싱 | WildFire가 링크에 피싱 분석 결과를 할당했음을 나타냅니다. 피싱 판정은 링크가 사용자에게 표시된 사이트로 연결되는 자격 증명 피싱 활동을 나타냅니다. |
| 악성 | 항목이 WildFire 분석에서 악성 판정을 받았음을 나타냅니다. 악성으로 분류된 샘플은 보안에 위협이 될 수 있습니다. 멀웨어에는 바이러스, C2(명령 및 제어), 웜, 트로이 목마, 원격 액세스 도구(RAT), 루트킷 및 봇넷이 포함될 수 있습니다. 멀웨어로 식별된 샘플의 경우 WildFire 클라우드는 향후 노출을 방지하기 위해 서명을 생성 및 배포합니다.<br><br>***C2*** 샘플은 ***WildFire*** 분석 보고서 및 ***WildFire*** 분석 데이터에 의존하는 기타 ***Palo Alto Networks*** 제품에서 ***C2***로 분류됩니다. 그러나 해당 평결은 번역되고 방화벽에 의해 악성으로 분류됩니다. |

## 데이터 필터링 로그

데이터 필터링 로그는 신용 카드 번호와 같은 중요한 정보가 방화벽이 보호하는 영역을 벗어나는 것을 방지하는 보안 규칙에 대한 항목을 표시합니다. 데이터 필터링 프로파일 정의에 대한 자세한 내용은 데이터 필터링을(를) 참조하십시오.

이 로그 유형은 파일 차단 프로파일에 대한 정보도 표시합니다. 예를 들어 규칙이 .exe 파일을 차단하면 로그에 차단된 파일이 표시됩니다.


©2023 Palo Alto Networks, Inc.

## 상관 로그

방화벽은 상관 개체에 정의된 패턴 및 임계값이 네트워크의 트래픽 패턴과 일치할 때 상관 이벤트를 기록합니다. 이벤트의 그래픽 표시를 상관 이벤트 해석 및 확인하려면 ACC에서 손상된 호스트 위젯 사용을(를) 참조하십시오.

다음 표에는 상관 관계 로그 심각도 수준이 요약되어 있습니다.

| 심각성 | 설명 |
|---|---|
| 심각한 | 에스컬레이션 패턴을 나타내는 상관 이벤트를 기반으로 호스트가 손상되었는지 확인합니다. 예를 들어, WildFire에서 악성 판정을 받은 파일을 수신한 호스트가 해당 악성 파일에 대해 WildFire 샌드박스에서 관찰된 것과 동일한 명령 및 제어 활동을 나타낼 때 중요한 이벤트가 기록됩니다. |
| 높은 | 특정 호스트에서 생성되는 명령 및 제어 활동과 일치하는 네트워크 어디에서나 탐지된 맬웨어와 같은 여러 위협 이벤트 간의 상관 관계를 기반으로 호스트가 손상될 가능성이 매우 높음을 나타냅니다. |
| 중간 | 스크립팅된 명령 및 제어 활동을 제안하는 알려진 악성 URL에 대한 반복적인 방문과 같은 하나 이상의 의심스러운 이벤트 탐지를 기반으로 호스트가 손상될 가능성이 있음을 나타냅니다. |
| 낮은 | 악성 URL 또는 동적 DNS 도메인 방문과 같은 하나 이상의 의심스러운 이벤트 탐지를 기반으로 호스트가 손상될 수 있음을 나타냅니다. |
| 정보 제공 | 의심스러운 활동을 식별하는 데 전체적으로 유용할 수 있는 이벤트를 감지합니다. 각 이벤트는 반드시 그 자체로 중요하지 않습니다. |

## 터널 검사 로그

터널 검사 로그는 터널 세션에 대한 트래픽 로그와 같습니다. 암호화되지 않은 터널 세션의 항목을 표시합니다. 방화벽은 이중 계산을 방지하기 위해 내부 흐름만 트래픽 로그에 저장하고 터널 세션을 터널 검사 로그에 보냅니다. 터널 검사 로그 항목에는 수신 시간(로그 수신 날짜 및 시간), 터널 ID, 모니터 태그, 세션 ID, 터널 세션에 적용된 보안 규칙, 세션의 바이트 수, 상위 세션 ID(터널 세션의 세션 ID), 소스 주소 , 소스 사용자 및 소스 영역, 대상 주소, 대상 사용자 및 대상 영역이 포함됩니다.

> ***PAN-OS 10.2***에 도입된 복호화 로그가 활성화되면 방화벽이 ***HTTP/2*** 로그를 터널 검사 로그로 전달하게 되어**(**복호화 로그가 비활성화되면 ***HTTP/2*** 로그가 트래픽 로그로 전송할 때**),** ***HTTP/2*** 이벤트에 대한 트래픽 로그 대신 터널 검사 로그를 확인해야 합니다**.** 이 경우 ***HTTP/2*** 트래픽에 대한 ***App-ID***를 얻으려면 터널 콘텐츠 검사도 활성화해야 합니다**.**

자세한 로그 보기를 클릭하면 사용된 터널 프로토콜, 터널 콘텐츠 검사 여부를 나타내는 플래그 등 항목에 대한 세부 정보를 볼 수 있습니다. 상위 세션이 있는 세션에만 Tunnel Inspected 플래그가 설정되어 세션이 터널 내 터널(2가지 수준의 캡슐화)에 있음을 의미합니다. 터널의 첫 번째 외부 헤더에는 Tunnel Inspected 플래그가 설정되지 않습니다.


©2023 Palo Alto Networks, Inc.

### 구성 로그

구성 로그는 방화벽 구성의 변경 사항에 대한 항목을 표시합니다. 각 항목에는 날짜와 시간, 관리자 사용자 이름, 관리자가 변경한 IP 주소, 클라이언트 유형(웹, CLI 또는 Panorama), 실행된 명령 유형, 명령 상태(성공 또는 실패), 구성 경로 및 변경 전후의 값이 포함됩니다.

### 시스템 로그

시스템 로그에는 방화벽의 각 시스템 이벤트에 대한 항목이 표시됩니다. 각 항목에는 날짜 및 시간, 이벤트 심각도 및 이벤트 설명이 포함됩니다. 다음 표에는 시스템 로그 심각도 수준이 요약되어 있습니다. 시스템 로그 메시지의 일부 목록과 해당 심각도 수준은 시스템 로그 이벤트를 참조하십시오.

| 심각성 | 설명 |
|---|---|
| 심각한 | HA(고가용성) 페일오버 및 링크 장애를 포함한 하드웨어 장애 |
| 높은 | LDAP 및 RADIUS 서버와 같은 외부 디바이스와의 연결이 끊어지는 등 심각한 문제가 있습니다. |
| 중간 | 안티바이러스 패키지 업그레이드와 같은 중간 수준 알림. |
| 낮은 | 사용자 암호 변경과 같은 사소한 심각도 알림. |
| 정보 제공 | 로그인/로그오프, 관리자 이름 또는 암호 변경, 구성 변경 및 기타 심각도 수준에 포함되지 않는 기타 모든 이벤트 |

## HIP 매치 로그

GlobalProtect HIP(Host Information Profile) 일치를 사용하면 네트워크에 액세스하는 최종 디바이스의 보안 상태(예: 디스크 암호화를 사용하도록 설정했는지의 여부)에 대한 정보를 수집할 수 있습니다. 방화벽은 정의한 HIP 기반 보안 규칙을 준수하여 특정 호스트에 대한 액세스를 허용하거나 거부할 수 있습니다. HIP 일치 로그는 규칙에 대해 구성한 HIP 개체 또는 HIP 프로파일과 일치하는 트래픽 플로우를 표시합니다.

## GlobalProtect 로그

GlobalProtect 로그는 GlobalProtect와 관련된 다음 로그를 표시합니다.

- GlobalProtect 시스템 로그.

  GlobalProtect 인증 이벤트 로그는 **Monitor** > **Logs** > **System**에 남아 있습니다. 그러나 GlobalProtect 로그의 인증 방법 열에는 로그인에 사용된 인증 방법이 표시됩니다.
- LSVPN/위성 이벤트.
- GlobalProtect 포털 및 게이트웨이 로그.
- 클라이언트리스 VPN 로그.


©2023 Palo Alto Networks, Inc.

## IP 태그 로그

IP 태그 로그에는 소스 IP 주소가 방화벽에 등록되거나 등록되지 않은 방법과 시기 및 해당 주소에 적용된 방화벽 태그가 표시됩니다. 또한 각 로그 항목에는 구성된 타임아웃(구성된 경우)과 User-ID 에이전트 VM 정보 소스 및 자동 태그 지정과 같은 IP 주소-태그 매핑 정보의 원본이 표시됩니다. 자세한 내용은 IP 주소 및 태그를 동적으로 등록하는 방법을 참조하십시오.

## 사용자 ID 로그

User-ID 로그에는 매핑 정보의 소스 및 사용자가 인증된 시간과 같은 IP 주소-사용자명 매핑 및 인증 타임스탬프에 대한 정보가 표시됩니다. 이 정보를 사용하여 User-ID 및 인증 문제를 해결할 수 있습니다. 예를 들어 방화벽이 사용자에 대해 잘못된 정책 규칙을 적용하는 경우 로그를 보고 해당 사용자가 올바른 IP 주소에 매핑되었는지의 여부와 그룹 연결이 올바른지의 여부를 확인할 수 있습니다.

## 복호화 로그

복호화 로그는 기본적으로 실패한 TLS 핸드쉐이크에 대한 항목을 표시하고 복호화 정책에 사용하도록 설정하는 경우 성공적인 TLS 핸드쉐이크에 대한 항목을 표시할 수 있습니다. 성공적인 핸드쉐이크를 위해 항목을 사용하도록 설정하고 로그에 대한 시스템 리소스(로그 공간)가 있는지 확인합니다.

암호 해독 로그에는 문제를 해결하는 데 도움이 되는 복호화 문제 해결 및 모니터링 방대한 양의 정보가 포함되어 있습니다. 로그에서 활성화할 수 있는 다양한 유형의 정보의 62개의 열이 있으며 개별 로그(, 돋보기)를 선택한 다음 단일 세부 정보 보기에서 세부 정보를 볼 수 있습니다. 다음과 같은 인증서, 암호 제품군 및 오류 정보를 볼 수 있습니다: 제목 공통 이름, 발급자 공통 이름, 루트 공통 이름, 루트 상태, 인증서 키 유형 및 크기, 인증서 시작 및 종료 날짜, 인증서 일련번호, 인증서 지문, TLS 버전, 키 교환 알고리즘, 암호화 알고리즘, 협상 EC 곡선, 인증 알고리즘, SNI, 프록시 유형, 오류 정보(암호, HSM, 리소스, 이력서, 프로토콜, 기능, 인증서, 버전 및 오류 인덱스(조회할 수 있는 코드).

## 알람 로그

알람은 특정 유형의 이벤트 수(예: 암호화 및 복호화 오류)가 해당 이벤트 유형에 대해 구성된 임계값을 초과했음을 나타내는 방화벽 생성 메시지입니다. 알람을 활성화하고 알람 임계값을 구성하려면 디바이스 > 로그 설정을 선택한 다음 알람 설정을 편집합니다.

알람을 생성할 때 방화벽은 알람 로그를 생성하고 시스템 알람 대화 상자를 열어 알람을 표시합니다. 대화 상자를 닫은 후 웹 인터페이스 하단의 알람()을 클릭하여 언제든지 다시 열 수 있습니다. 방화벽이 특정 알람에 대한 대화 상자를 자동으로 열지 않도록 하려면 승인되지 않은 경보 목록에서 알람을 선택한 다음 알람을 승인합니다.

## 인증 로그

인증 로그는 최종 사용자가 인증 정책 규칙에 의해 액세스가 제어되는 네트워크 리소스에 액세스하려고 할 때 발생하는 인증 이벤트에 대한 정보를 표시합니다. 이 정보를 사용하여 액세스 문제를 해결하고 필요에 따라 인증 정책을 조정할 수 있습니다. 상관 관계 개체와 함께 인증 로그를 사용하여 무차별 암호 공격과 같은 네트워크에서 의심스러운 활동을 식별할 수도 있습니다.

선택적으로 시간 외 이벤트를 기록하도록 인증 규칙을 구성할 수 있습니다. 이러한 시간 시간은 사용자가 리소스에 대해 한 번만 인증해야 하지만 반복적으로 액세스할 수 있는 기간과 관련이 있습니다. 시간 지정에 대한 정보를 확인하면 조정 여부를 결정하는 데 도움이 됩니다(자세한 내용은 인증 타임스탬프 참조).


©2023 Palo Alto Networks, Inc.

시스템 로그는 ***GlobalProtect*** 및 웹 인터페이스에 대한 관리자 액세스와 관련된 인증 이벤트를 기록합니다.

### 통합 로그

통합 로그는 단일 보기에 표시되는 트래픽, 위협, URL 필터링, WildFire 제출 및 데이터 필터링 로그의 항목입니다. 통합 로그 보기를 사용하면 각 로그 유형을 개별적으로 검색하는 대신 한 곳에서 다양한 로그 유형의 최신 항목을 검토하고 필터링할 수 있습니다. 필터 영역에서 효과적인 쿼리(⋙)를 클릭하여 통합 로그 보기에 항목을 표시할 로그 유형을 선택합니다.

통합 로그 보기에는 볼 수 있는 권한이 있는 로그 항목만 표시됩니다. 예를 들어 WildFire 제출 로그를 볼 수 있는 권한이 없는 관리자는 통합 로그를 볼 때 WildFire 제출 로그 항목을 볼 수 없습니다. 관리 역할 유형은(는) 이러한 권한을 정의합니다.

***AutoFocus***에서 원격 검색을 설정하여 방화벽에서 대상 검색을 수행하면 검색 결과가 통합 로그 보기에 표시됩니다.

## 로그 보기

방화벽의 다른 로그 유형을 표 형식으로 볼 수 있습니다. 방화벽은 모든 로그 파일을 로컬로 저장하고 기본적으로 구성 및 시스템 로그를 자동으로 생성합니다. 다른 유형의 로그에 대한 항목 생성을 트리거하는 보안 규칙에 대해 자세히 알아보려면 로그 유형 및 심각도 수준을(를) 참조하십시오.

방화벽을 syslog 메시지, 전자 메일 알림 또는 SNMP(간단한 네트워크 관리 프로토콜) 트랩으로 로그를 포워딩할 수 있도록 구성하려면, 모니터링을 위해 외부 서비스 사용을(를) 합니다.

**STEP 1 |** 확인할 로그 유형을 선택합니다.

1. 모니터 > 로그를 선택합니다.
2. 목록에서 로그 유형을 선택합니다.

   방화벽에는 확인할 권한이 있는 로그만 표시됩니다. 예를 들어 관리 계정에 ***WildFire*** 제출 기록 로그를 볼 수 있는 권한이 없는 경우 방화벽에 로그 페이지에 액세스할 때 해당 로그 유형이 표시되지 않습니다. 관리 역할 유형은(는) 권한을 정의합니다.

**STEP 2 |** (선택 사항) 로그 열 표시를 사용자 지정합니다.

1. 열 머리글 오른쪽에 있는 화살표를 클릭하고 열을 선택합니다.
2. 목록에서 표시할 열을 선택합니다. 로그는 선택 항목과 일치하도록 자동으로 업데이트됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 로그 항목에 대한 추가 세부 정보를 봅니다.

- 특정 로그 항목에 대해 스파이글래스()를 클릭합니다. 자세한 로그 보기에는 세션의 소스 및 대상에 대한 자세한 정보와 로그 입력과 관련된 세션 목록이 있습니다.
- (위협 로그만) 항목 옆에 있는 를 클릭하여 위협의 로컬 패킷 캡처에 액세스합니다. 로컬 패킷 캡처를 사용하도록 설정하려면 패킷 캡처 가져오기을(를) 참조하십시오.
- (트래픽, 위협, URL 필터링, WildFire 서브미션, 데이터 필터링 및 통합 로그만) 로그 항목에 대한 AutoFocus 위협 데이터를 봅니다.

  1. AutoFocus 위협 인텔리전스 활성화.

     *Panorama*에서 *AutoFocus*를 활성화하여 *AutoFocus* 및/또는 *PAN-OS 7.0* 및 이전 릴리스 버전(***Panorama*** > 설정 > 관리 > 자동 초점)을 실행하는 방화벽을 포함하여 모든 *Panorama* 로그 항목에 대한 자동 초점 위협 데이터를 볼 수있습니다.

  2. IP 주소, URL, 사용자 에이전트, 위협 이름(하위 유형: 바이러스 및 Wildfire 바이러스만), 파일 이름 또는 SHA-256 해시 위로 마우스를 가져가세요.
  3. 드롭다운()을 클릭하고 자동 초점 선택을 선택합니다.
  4. 콘텐츠 전송 네트워크 인프라.

다음 단계...

- 필터 로그.
- 로그 내보내기.
- 로그 스토리지 할당량 및 만료 기간 구성.

## 필터 로그

각 로그에는 표시할 로그 항목의 기준을 설정할 수 있는 필터 영역이 있습니다. 로그를 필터링하는 기능은 특정 속성이나 특성을 가진 방화벽의 이벤트에 초점을 맞추는 데 유용합니다. 개별 로그 항목과 연결된 개체별로 로그를 필터링합니다.

예를 들어 규칙 UUID로 필터링하면 이름이 비슷한 여러 규칙 중에서도 찾으려는 특정 규칙을 쉽게 찾아낼 수 있습니다. 규칙 세트가 매우 크고 많은 규칙을 포함하는 경우 규칙의 UUID를 필터로 사용하면 결과 페이지를 탐색하지 않고도 찾아야 하는 특정 규칙이 강조 표시됩니다.



**STEP 1 |** (통합 로그만 해당) 통합 로그 표시에 포함할 로그 유형을 선택합니다.

1. 유효 검색어().
2. 목록에서 하나 이상의 로그 유형(**traffic**, **Threat**, **url**, **data** 및 **wildfire**)을 선택합니다.
3. 확인을 클릭합니다. 통합 로그는 선택한 로그 유형의 항목만 표시하도록 업데이트됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 필터 필드에 필터를 추가합니다.

> 아티팩트의 값이 연산자(예: ***has*** 또는 ***in***)와 일치하면 구문 오류가 발생하지 않도록 값을 따옴표로 묶습니다. 예를 들어 대상 국가별로 필터링하고 *IN*을 값으로 사용하여 *IN*을 *INDIA*로 지정하는 경우 필터를 ***(dstloc eq "IN")***로 입력합니다.

- 로그 항목에서 하나 이상의 아티팩트(예: 트래픽과 연결된 애플리케이션 유형 및 공격자의 IP 주소)를 클릭합니다. 예를 들어, 로그 항목의 소스 **10.0.0.25** 및 애플리케이션 웹 브라우징을 클릭하여 로그에 두 개체가 모두 포함된 항목만 표시합니다(AND 검색).
- 필터 필드에 추가할 개체를 지정하려면 필터 추가()를 클릭합니다.
- 이전에 저장한 필터를 추가하려면 필터 로드()를 클릭합니다.

**STEP 3 |** 로그에 필터를 적용합니다.

필터 적용()을 클릭합니다. 현재 필터와 일치하는 로그 항목만 표시하도록 로그가 새로 고쳐집니다.

**STEP 4 |** (선택 사항) 자주 사용하는 필터를 저장합니다.

1. 필터 저장()을 클릭합니다.
2. 필터의 이름을 입력합니다.
3. 확인을 클릭합니다. 필터 로드()를 클릭하여 저장된 필터를 볼 수 있습니다.

다음 단계...

- 로그 보기.
- 로그 내보내기.

## 로그 내보내기

로그 유형의 내용을 CSV(쉼표로 구분된 값) 형식의 보고서로 내보낼 수 있습니다. 기본적으로 보고서에는 최대 2,000개의 로그 항목 행이 포함됩니다.

**STEP 1 |** 보고서에 표시할 행 수를 설정합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 수정합니다.
2. 로그 내보내기 및 보고탭을 클릭합니다.
3. **CSV** 내보내기에서 최대 행 수(최대 1048576개 행)를 편집합니다.
4. 확인을 클릭합니다.

**STEP 2 |** 로그를 다운로드합니다.

1. CSV로 내보내기()를 클릭합니다. 다운로드 상태를 보여주는 진행률 표시줄이 나타납니다.
2. 다운로드가 완료되면 파일 다운로드를 클릭하여 로컬 폴더에 로그 복사본을 저장합니다. 다운로드한 로그의 열 머리글에 대한 설명은 Syslog 필드 설명을 참조하십시오.

다음 단계...

SCP 또는 FTP 서버로 로그 내보내기를 예약합니다.

 ©2023 Palo Alto Networks, Inc.

## 로그 스토리지 할당량 및 만료 기간 구성

방화벽은 만료 기간을 초과하는 로그를 자동으로 삭제합니다. 방화벽은 로그 유형의 저장소 할당량에 도달하면 만료 기간을 설정하지 않더라도 공간을 생성하기 위해 해당 유형의 오래된 로그를 자동으로 삭제합니다.

로그를 수동으로 삭제하려면 ***Device > Log*** 설정을 선택한 다음 로그 관리 섹션에서 유형별로 로그를 지우는 링크를 클릭합니다.

**STEP 1 |** 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.

**STEP 2 |** 로그 저장소를 선택하고 각 로그 유형에 대해 할당량**(%)**을 입력합니다. 백분율 값을 변경하면 대화 상자가 새로 고쳐져 해당 절대값(Quota GB/MB 열)이 표시됩니다.

**STEP 3 |** 각 로그 유형(범위는 1-2,000)에 대한 최대 일수(만료 기간)를 입력합니다. 필드는 기본적으로 비어 있으므로 로그가 만료되지 않습니다.

방화벽은 고가용성***(HA)*** 쌍 간에 만료 기간을 동기화합니다**.** 활성 ***HA*** 피어만 로그를 생성하기 때문에 패시브 피어는 페일오버가 발생하고 로그 생성을 시작하지 않는 한 삭제할 로그가 없습니다**.**

**STEP 4 |** 확인 및 커밋을 클릭합니다.

## SCP 또는 FTP 서버로 로그 내보내기 예약

트래픽, 위협, URL 필터링, 데이터 필터링, HIP 일치 및 WildFire 제출 로그를 SCP(Secure Copy) 서버 또는 FTP(파일 전송 프로토콜) 서버로 내보내도록 예약할 수 있습니다. 내보낼 각 로그 유형에 대해 이 작업을 수행합니다.

CLI에서 SCP(보안 복사) 명령을 사용하여 전체 로그 데이터베이스를 ***SCP*** 서버로 내보내고 다른 방화벽으로 가져올 수 있습니다**.** 로그 데이터베이스가 너무 커서 내보내기 또는 가져오기가 다음 플랫폼에서 실용적이지 않기 때문에 이러한 옵션을 지원하지 않습니다**.** ***PA-7000*** 시리즈 방화벽***(***모든 ***PAN-OS*** 릴리스***), Panorama 6.0*** 이상의 버전을 실행하는 ***Panorama*** 가상 어플라이언스 및 ***Panorama M***-시리즈 어플라이언스***(***모든 ***Panorama*** 릴리스***).***

**STEP 1 |** 디바이스 > 예약된 로그 내보내기를 선택하고 추가를 클릭합니다.

**STEP 2 |** 예약된 로그 내보내기의 이름을 입력하고 활성화합니다.

**STEP 3 |** 내보낼 로그 유형을 선택합니다.

**STEP 4 |** 매일 예약된 내보내기 시작 시간을 선택합니다. 옵션은 24시간제(00:00 - 23:59)에 대해 15분 단위로 증가합니다.

**STEP 5 |** 프로토콜을 선택하여 로그를 내보냅니다. **SCP**(보안) 또는 **FTP**.

**STEP 6 |** 서버의 호스트 이름 또는 IP 주소를 입력합니다.

**STEP 7 |** 포트 번호를 입력합니다. 기본적으로 FTP는 포트 21을 사용하고 SCP는 포트 22를 사용합니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 내보낸 로그를 저장할 경로 또는 디렉터리를 입력합니다.

**STEP 9 |** 사용자 이름을 입력하고 필요한 경우 암호(및 암호 확인)를 입력하여 서버에 액세스합니다.

**STEP 10 |** **(**FTP 전용**)**방화벽이 FTP 서버와의 데이터 연결을 시작하는 FTP 수동 모드를 사용하려면 **FTP** 수동 모드 사용을 선택합니다. 기본적으로 방화벽은 FTP 서버가 방화벽과의 데이터 연결을 시작하는 FTP 활성 모드를 사용합니다. FTP 서버가 지원하는 것과 네트워크 요구 사항에 따라 모드를 선택하십시오.

**STEP 11 |** **(**SCP 전용**) SCP** 서버 연결 테스트를 클릭합니다. 연결을 설정하기 전에 방화벽은 SCP 서버의 호스트 키를 수락해야 합니다.

> *Panorama* 템플릿을 사용하여 로그 내보내기 일정을 구성하는 경우 템플릿 구성을 방화벽에 커밋한 후 이 단계를 수행해야 합니다. 템플릿 커밋 후 각 방화벽에 로그인하여 로그 내보내기 일정을 열고 테스트 ***SCP*** 서버 연결을 클릭합니다.

**STEP 12 |** 확인 및 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 차단 목록 모니터링

방화벽이 차단 목록에 IP 주소를 배치하도록 하는 두 가지 방법이 있습니다.

- IP 연결 차단 규칙을 사용하여 취약점 보호 프로파일을 구성하고 해당 프로파일을 영역에 적용하는 보안 정책에 적용합니다.
- 보호 작업 및 초당 최대 연결 속도를 지정하는 분류된 DoS 방어 프로파일을 사용하여 DoS 방어 정책 규칙을 구성합니다. 들어오는 패킷이 DoS 방어 정책과 일치하고 최대 속도를 초과하고 차단 기간 및 분류된 정책 규칙을 소스 IP 주소를 포함하도록 지정한 경우 방화벽은 문제가 되는 소스 IP 주소를 차단 목록에 추가합니다.

위에서 설명한 경우, 방화벽은 하드웨어에서 해당 패킷이 CPU 또는 패킷 버퍼 리소스를 사용하기 전에 트래픽을 자동으로 차단합니다. 공격 트래픽이 하드웨어의 차단 용량을 초과하면 방화벽은 소프트웨어의 IP 차단 메커니즘을 사용하여 트래픽을 차단합니다.

방화벽은 취약점 보호 프로파일 또는 DoS 방어 정책 규칙에 따라 하드웨어 차단 목록 항목을 자동으로 생성합니다. 규칙의 소스 주소는 하드웨어 차단 목록의 소스 IP 주소입니다.

차단 목록의 항목은 형식 열에서 하드웨어(hw) 또는 소프트웨어(sw)에 의해 차단되었는지의 여부를 나타냅니다. 화면 아래쪽에 다음이 표시됩니다.

- 차단된 IP 주소 수 중 차단된 총 **IP** 수입니다.
- 방화벽에서 사용한 차단 목록의 백분율입니다.

차단 목록에 있는 주소에 대한 세부 정보를 보려면 소스 IP 주소에 마우스를 갖다 대고 아래쪽 화살표 링크를 클릭합니다. 주소에 대한 정보를 제공하는 Network Solutions Who Is 기능을 표시하는 Who Is 링크를 클릭하십시오.

취약점 보호 프로파일을 구성하는 방법에 대한 자세한 내용은 무차별 대입 서명에 대한 작업 및 트리거 조건 사용자 지정을 참조하십시오. 차단 목록 및 DoS 방어 프로파일에 대한 자세한 내용은 새 세션 플러딩에 대한 DoS 보호를 참조하십시오.


©2023 Palo Alto Networks, Inc.

# 보고서 보기 및 관리

방화벽의 보고 기능을 사용하면 네트워크를 계속 모니터링하고, 정책을 검증하고, 사용자를 안전하고 생산적으로 유지하기 위해 네트워크 보안을 유지 관리하는 데 집중할 수 있습니다.

- 보고서 유형
- 보고서 보기
- 보고서의 만료 기간 및 실행 시간 구성
- 사전 정의된 보고서 비활성화
- 맞춤 보고서
- 사용자 정의 보고서 생성
- 봇넷 보고서 생성
- SaaS 애플리케이션 사용 보고서 생성
- PDF 요약 보고서 관리
- 사용자/그룹 활동 보고서 생성
- 보고서 그룹 관리
- 이메일 전송을 위한 보고서 예약
- 보고서 저장 용량 관리

## 보고서 유형

방화벽에는 현재 사용하거나 특정 데이터 및 실행 가능한 작업에 대한 요구 사항을 충족하는 맞춤 리포트를 작성하거나 사전 정의된 및 맞춤 리포트를 결합하여 필요한 정보를 컴파일할 수 있는 사전 정의된 보고서가 포함되어 있습니다. 방화벽은 다음과 같은 유형의 보고서를 제공합니다.

- 사전 정의된 보고서—네트워크의 트래픽에 대한 빠른 요약을 볼 수 있습니다. 사전 정의된 보고서 제품군은 애플리케이션, 트래픽, 위협 및 URL 필터링과 같은 네 가지 카테고리로 제공됩니다. 보고서 보기을(를) 참조하십시오.
- 사용자 또는 그룹 활동 보고서-특정 사용자 또는 사용자 그룹에 대한 애플리케이션 사용 및 URL 활동에 대한 주문형 보고서를 예약하거나 만들 수 있습니다. 보고서에는 URL 카테고리와 개별 사용자에 대한 예상 찾아보기 시간 계산이 포함됩니다. 사용자/그룹 활동 보고서 생성을(를) 참조하십시오.
- 맞춤 리포트— 포함할 조건 및 열을 필터링하여 표시하려는 정보를 정확하게 표시하는 맞춤 리포트 생성 및 일정을 지정합니다. 보고서 데이터에 대한 보다 구체적인 드릴다운을 위한 쿼리 빌더도 포함될 수도 있습니다. 사용자 정의 보고서 생성을(를) 참조하십시오.
- **PDF** 요약 보고서-위협, 애플리케이션, 추세, 트래픽 및 URL 필터링 카테고리에서 최대 18개의 사전 정의된 또는 맞춤 리포트/그래프를 하나의 PDF 문서로 집계합니다. PDF 요약 보고서 관리을(를) 참조하십시오.
- 봇넷 보고서-행동 기반 메커니즘을 사용하여 네트워크에서 봇넷에 감염된 잠재적 호스트를 식별할 수 있습니다. 봇넷 보고서 생성을(를) 참조하십시오.
- 보고서 그룹—사용자 정의 보고서와 사전 정의된 보고서를 보고서 그룹으로 결합하고 한 명 이상의 수신자에게 이메일로 전송되는 단일 PDF를 컴파일합니다. 보고서 그룹 관리을(를) 참조하십시오.


©2023 Palo Alto Networks, Inc.

보고서는 요청 시, 되풀이 일정에 따라 생성될 수 있으며 이메일 전송을 예약할 수 있습니다.

## 보고서 보기

방화벽은 매일 생성되는 40개 이상의 사전 정의된 보고서를 제공합니다. 방화벽에서 직접 이러한 보고서를 볼 수 있습니다. 맞춤 보고서 및 요약 보고서를 볼 수도 있습니다.

방화벽에 보고서를 저장하기 위해 약 200MB의 스토리지가 할당됩니다. 이 제한은 PA-7000 시리즈 및 PA-5200 시리즈 방화벽에 대해서만 재구성할 수 있습니다. 다른 모든 방화벽 모델의 경우 방화벽이 기간을 초과하는 보고서를 삭제할 수 있도록 보고서의 만료 기간 및 실행 시간 구성을(를) 할 수 있습니다. 방화벽이 저장소 한도에 도달하면 만료 기간을 설정하지 않아도 이전 보고서를 자동으로 삭제하여 공간을 생성합니다. 방화벽에서 시스템 리소스를 보존하는 또 다른 방법은 사전 정의된 보고서 비활성화을(를) 사용하는 것입니다. 보고서를 장기간 보관하려면 보고서(아래 설명 참조) 또는 이메일 전송을 위한 보고서 예약을(를) 내보낼 수 있습니다.

다른 보고서와 달리 사용자/그룹 활동 보고서는 방화벽에 저장할 수 없습니다. 요청 시 사용자/그룹 활동 보고서 생성을(를) 하거나 이메일 전송을 예약해야 합니다.

**STEP 1 |** (VM-50, VM-50 라이트 및 PA-200 방화벽에만 해당) 사전 정의된 보고서 생성을 활성화합니다.

기본적으로 사전 정의된 보고서는 리소스를 절약하기 위해 *VM-50, VM-50 Lite* 및 *PA-200* 방화벽에서 비활성화되어 있습니다.

1. 디바이스 > 설정 > 관리를 선택하고 로깅 및 보고를 수정합니다.
2. 사전 정의된 보고서를 선택하고 사전 정의된 보고서를 활성화(선택)합니다.
3. 생성하려는 사전 정의된 보고서를 선택(활성화)하고 확인을 클릭합니다.
4. 구성 변경 사항을 커밋합니다.
5. 방화벽 CLI에 액세스하여 사전 정의된 보고서를 활성화합니다.

   이 단계는 Panorama™ 관리 서버에서 푸시된 사전 정의된 로컬 보고서 및 사전 정의된 보고서에 필요합니다.

   ```
   admin> debug predefined-default enable
   ```

**STEP 2 |** 모니터 > 보고서를 선택합니다.

보고서는 페이지 오른쪽의 섹션(유형)으로 그룹화됩니다. 맞춤 보고서, 애플리케이션 보고서, 트래픽 보고서, 위협 보고서, **URL** 필터링 보고서 및 **PDF** 요약 보고서.

**STEP 3 |** 보려는 보고서를 선택하십시오. 그러면 보고서 페이지에 전날의 보고서가 표시됩니다.

다른 날짜에 대한 보고서를 보려면 페이지 오른쪽 하단의 달력에서 날짜를 선택한 다음 보고서를 선택합니다. 다른 섹션에서 보고서를 선택하면 날짜 선택이 현재 날짜로 재설정됩니다.

**STEP 4 |** 보고서를 오프라인으로 보려면 보고서를 PDF, CSV 또는 XML 형식으로 내보낼 수 있습니다. 페이지 하단에서 **PDF**로 내보내기, **CSV**로 내보내기 또는 **XML**로 내보내기를 클릭한 다음 파일을 인쇄하거나 저장합니다.


©2023 Palo Alto Networks, Inc.

## 보고서의 만료 기간 및 실행 시간 구성

만료 기간 및 실행 시간은 모두 보고서 유형에 적용되는 전역 설정입니다. 새 보고서를 실행한 후 방화벽은 만료 기간을 초과하는 보고서를 자동으로 삭제합니다.

**STEP 1 |** 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집한 다음 로그 내보내기 및 보고 탭을 선택합니다.

**STEP 2 |** 보고서 런타임을 24시간제 일정에서 한 시간으로 설정합니다(기본값은 02:00, 범위는 00:00[자정]~23:00).

**STEP 3 |** 보고서 만료 기간을 일 단위로 입력합니다(기본값은 만료 없음, 범위는 1-2,000).

방화벽이 보고서를 저장하기 위해 할당하는 저장소는 변경할 수 없습니다. 약 ***200MB***로 사전 정의되어 있습니다. 방화벽은 저장소 최대값에 도달하면 보고서 만료 기간을 설정하지 않아도 오래된 보고서를 자동으로 삭제하여 공간을 생성합니다.

**STEP 4 |** 확인 및 커밋을 클릭합니다.

## 사전 정의된 보고서 비활성화

방화벽에는 매일 자동으로 생성되는 약 40개의 사전 정의된 보고서가 포함되어 있습니다. 이들 중 일부 또는 전부를 사용하지 않는 경우 선택한 보고서를 비활성화하여 방화벽의 시스템 리소스를 절약할 수 있습니다.

비활성화할 사전 정의된 보고서가 보고서 그룹이나 PDF 요약 보고서에 포함되어 있지 않은지 확인합니다. 그렇지 않으면 방화벽이 데이터 없이 PDF 요약 보고서 또는 보고서 그룹을 렌더링합니다.

**STEP 1 |** 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.

**STEP 2 |** 사전 정의된 보고서 탭을 선택한 다음 비활성화할 각 보고서의 체크박스를 선택 취소합니다. 사전 정의된 모든 보고서를 비활성화하려면 모두 선택 해제를 누릅니다.

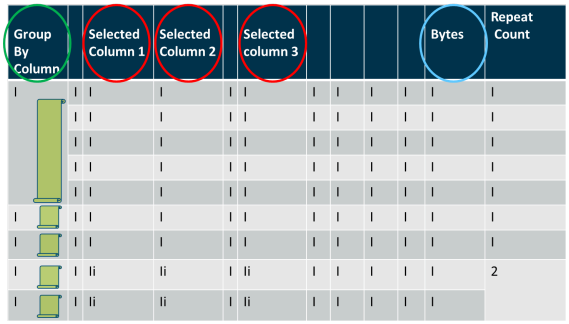
**STEP 3 |** 확인 및 커밋을 클릭합니다.

## 맞춤 보고서

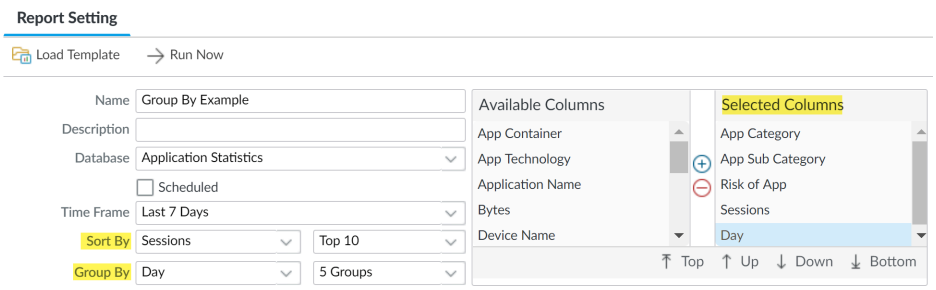
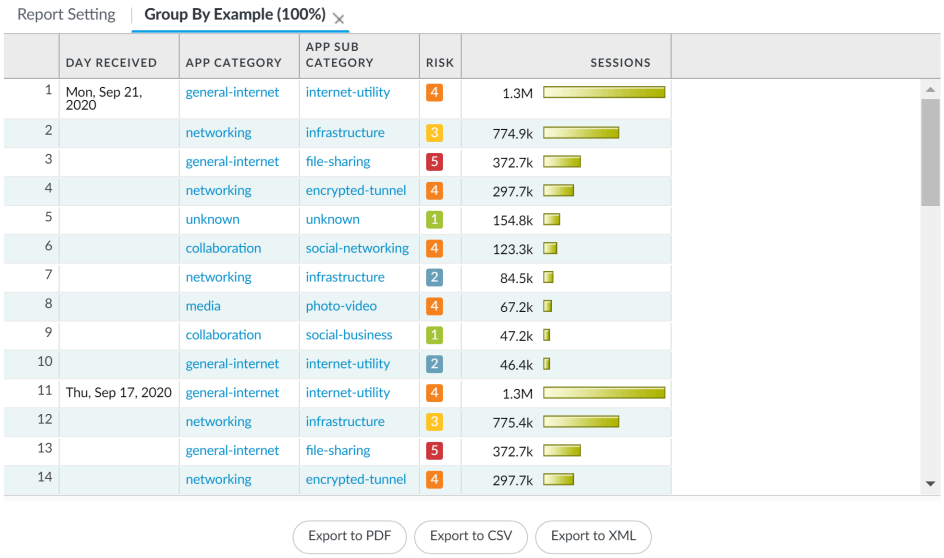
의도적인 맞춤 보고서를 만들려면 위협과 같이 검색하고 분석하려는 정보의 속성 이나 핵심 부분뿐만 아니라 규칙 UUID로 그룹화하는 가장 좋은 방법뿐만 아니라 각 위협 유형에 적용되는 규칙을 볼 수 있습니다. 해당 내용은 맞춤 보고서에서 다음 선택을 하는 데 있어 도움을 줍니다.

| 선택 | 설명 |
|---|---|
| 데이터베이스 | 다음 데이터베이스 유형 중 하나에 대한 보고서를 기반으로 할 수 있습니다.<br>• 요약 데이터베이스 - 이러한 데이터베이스는 애플리케이션 통계, 트래픽, 위협, URL 필터링 및 터널 검사 로그에 사용할 수 있습니다. 방화벽은 자세한 로그를 15분 간격으로 집계합니다. 보고서를 생성할 때 더 빠른 응답 시간을 사용하도록 설정하려면 방화벽은 데이터를 압축합니다: 중복 세션 |


©2023 Palo Alto Networks, Inc.

| 선택 | 설명 |
| --- | --- |
| | 은 반복 카운터로 그룹화되고 증가하며 일부 속성(열)은 요약에서 제외됩니다.<br>• 자세한 로그 - 이러한 데이터베이스는 로그를 항목별로 분류하고 각 로그 항목에 대한 모든 속성(열)을 나열합니다.<br>자세한 로그에 기반한 보고서는 실행하는 데 훨씬 더 오래 걸리며 절대적으로 필요한 경우가 아니면 권장되지 않습니다. |
| 특성 | 일치 기준으로 사용할 열입니다. 특성은 보고서에서 선택할 수 있는 열입니다. 사용 가능한 열, 목록에서 데이터 일치 및 세부 정보(선택한 열)를 집계하기 위한 선택 기준을 추가할 수 있습니다. |
| 정렬별/ 그룹별 | 정렬별 및 그룹별 기준을 사용하면 보고서의 데이터를 구성/분할할 수 있습니다.<br>정렬별 옵션은 집계에 사용되는 특성을 지정합니다. 정렬할 특성을 선택하지 않으면 보고서는 집계 없이 첫 번째 N 결과 수를 반환합니다.<br>그룹별 옵션을 사용하면 특성을 선택한 다음 데이터 그룹화의 앵커로 사용할 수 있습니다. 그런 다음 보고서의 모든 데이터는 상위 5, 10, 25 또는 50 그룹 집합에 표시됩니다. 예를 들어 시간을 그룹별 선택으로 선택한 다음 24시간 동안 상위 25개 그룹을 원할 때 보고서 결과는 24시간 동안 시간 단위로 생성됩니다. 보고서의 첫 번째 열은 시간이 될 것이며 다음 열 집합은 선택한 보고서 열의 나머지 집합이 됩니다. |
| | 다음 예제에서는 보고서를 생성할 때 선택한 열 및 정렬별/ 그룹별 기준이 함께 작동하는 방법을 보여 줍니다.<br><br>빨간색(위)으로 동그라미가 된 열은 보고서를 생성하기 위해 일치하는 속성인 선택한 열을 묘사합니다. 데이터 원본의 각 로그 항목은 구문 분석되고 이러한 열이 일치합니다. 여러 세션이 선택한 열에 대해 동일한 값을 가지고 있는 경우 세션이 집계되고 반복 수(또는 세션)가 증가합니다.<br>파란색으로 동그라미가 된 열은 선택한 정렬 순서를 나타냅니다. 정렬 순서(정렬 **By**)를 지정하면 선택한 특성에 의해 데이터가 정렬되고 집계됩니다.<br>녹색 동그라미로 구성된 열은 보고서의 앵커 역할을 하는 그룹별 선택을 나타냅니다. 그룹별 열은 상위 N 그룹을 필터링하는 일치 기준으로 사용됩니다. |


©2023 Palo Alto Networks, Inc.

| 선택 | 설명 |
| --- | --- |
| | 그런 다음 상위 N 그룹 각각에 대해 보고서는 선택한 다른 모든 열에 대한 값을 열거합니다. |
| | 예를 들어 보고서에 다음과 같은 선택 항목이 있는 경우:<br><br><br>출력은 다음과 같이 표시됩니다.<br><br><br>보고서는 일 단위에 의해 고정되고 세션에 의해 정렬됩니다. 지난 **7**일 동안 최대 트래픽이 있는 5일(**5**개 그룹)을 나열합니다. 데이터는 선택한 열-앱 카테고리, 앱 하위 카테고리 및 위험에 대해 매일 상위 **5**개 세션으로 열거됩니다. |
| 시간 프레임 | 데이터를 분석하려는 날짜 범위입니다. 사용자 지정 범위를 정의하거나 마지막 15분에서 마지막 30일까지의 기간을 선택할 수 있습니다. 보고서는 주문형으로 실행되거나 일일 또는 주간 케이던스로 실행되도록 예약할 수 있습니다. |
| 쿼리 빌더 | 쿼리 빌더를 사용하면 특정 쿼리를 정의하여 선택한 특성을 더 구체화할 수 있습니다. 이를 통해 **and** 및 **or** 연산자와 일치 기준을 사용하여 보고서에서 원하는 내용을 확인한 다음 보고서에서 쿼리와 일치하거나 부정하는 데이터를 포함하거나 제외할 수 있습니다. 쿼리를 사용하면 보고서에서 보다 집중된 정보 데이터 정렬을 생성할 수 있습니다. |


©2023 Palo Alto Networks, Inc.

# 사용자 정의 보고서 생성

방화벽이 즉시(요청 시) 또는 일정에 따라(매일 밤) 생성하는 맞춤 보고서를 구성할 수 있습니다. 용도에 따라 맞춤 보고서를 만드는 데 사용할 수 있는 선택 사항을 이해하려면 맞춤 보고서를 참조하십시오.

방화벽에서 예약된 맞춤 보고서를 생성한 후 향후 출력을 변경하기 위해 구성을 수정하면 해당 보고서의 이전 결과가 무효화될 위험이 있습니다. 예약된 보고서 구성을 수정해야 하는 경우 모범 사례는 새 보고서를 만드는 것입니다.

**STEP 1 |** 모니터 > 관리 맞춤 보고서를 선택합니다.

**STEP 2 |** 추가를 클릭한 다음 보고서의 이름을 입력합니다.

사전 정의된 템플릿을 기반으로 보고서를 작성하려면 템플릿 로드를 클릭하고 템플릿을 선택합니다. 그런 다음 템플릿을 편집하고 맞춤 보고서로 저장할 수 있습니다.

**STEP 3 |** 보고서에 사용할 데이터베이스를 선택합니다.

맞춤 보고서를 만들 때마다 로그 보기 보고서가 자동으로 만들어집니다. 이 보고서는 맞춤 보고서를 작성하는 데 사용된 로그를 보여 줍니다. 로그 보기 보고서는 맞춤 보고서와 동일한 이름을 사용하지만 보고서 이름에 구문(로그 보기)을 추가합니다.

보고서 그룹을 만들 때 맞춤 보고서에 로그 보기 보고서를 포함할 수 있습니다. 자세한 내용은 보고서 그룹 관리를 참조하십시오.

**STEP 4 |** 매일 밤 보고서를 실행하려면 예약됨 체크박스를 선택합니다. 그러면 측면의 보고서 열에서 보고서를 볼 수 있습니다.

*Panorama*™ 관리 서버의 *Cortex Data Lake*에 저장된 로그를 사용하여 예약된 사용자 지정 보고서를 생성하려면 클라우드 서비스 플러그인 *1.8* 이상 릴리스를 *Panorama*에 설치해야 합니다.

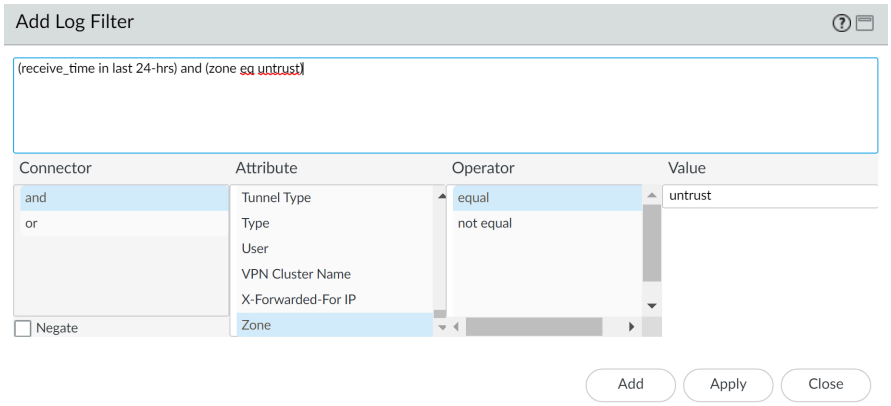
**STEP 5 |** 필터링 기준을 정의합니다. 시간 프레임, 정렬 기준, 그룹화 기준 기본 설정을 선택하고 보고서에 표시해야 하는 열을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** **(**선택 사항**)** 선택 기준을 더 세분화하려면 쿼리 빌더 속성을 선택합니다. 보고서 쿼리를 작성하려면 다음을 지정하고 추가를 클릭합니다. 전체 쿼리를 생성하기 위해 필요에 따라 반복합니다.

- 커넥터(Connector) - 추가할 표현식 앞에 올 커넥터(및/또는)를 선택합니다.
- 부정 - 쿼리를 부정으로 해석하려면 이 체크박스를 선택합니다. 예를 들어 최근 24시간 동안의 항목과 일치하도록 선택하거나 언트러스트 영역에서 시작된 항목인 경우 무효화 옵션을 사용하면 지난 24시간 내에 있지 않거나 언트러스트 영역에 속하지 않은 항목과 일치합니다.
- 속성 - 데이터 요소를 선택합니다. 사용 가능한 옵션은 데이터베이스 선택에 따라 다릅니다.
- 연산자 - 속성을 적용할지의 여부를 결정하는 기준을 선택합니다(예: =). 사용 가능한 옵션은 데이터베이스 선택에 따라 다릅니다.
- 값 - 일치시킬 속성 값을 지정합니다.

예를 들어 다음 그림(**트래픽 로그** 데이터베이스 기반)에서는 지난 24시간 동안 트래픽 로그 항목이 수신되었고 언트러스트 영역에서 전송된 경우 일치하는 쿼리를 보여 줍니다.



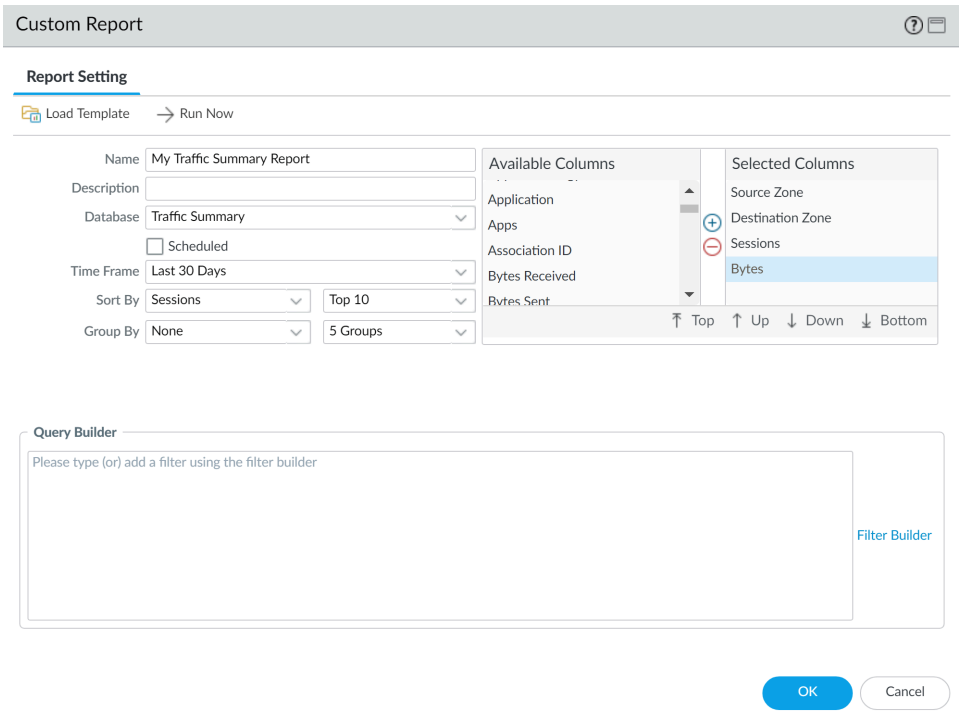

**STEP 7 |** 보고서 설정을 테스트하려면 지금 실행을 선택합니다. 보고서에 표시되는 정보를 변경하는 데 필요한 대로 설정을 수정합니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 확인을 클릭하여 사용자 정의 보고서를 저장합니다.

맞춤 보고서의 예

지난 30일간의 트래픽 요약 데이터베이스를 사용하는 간단한 보고서를 설정하고 상위 10개 세션별로 데이터를 정렬하려는 경우 이러한 세션이 요일별로 5개 그룹으로 그룹화됩니다. 다음과 같이 맞춤 보고서를 설정합니다.




보고서의 PDF 출력은 다음과 같습니다.

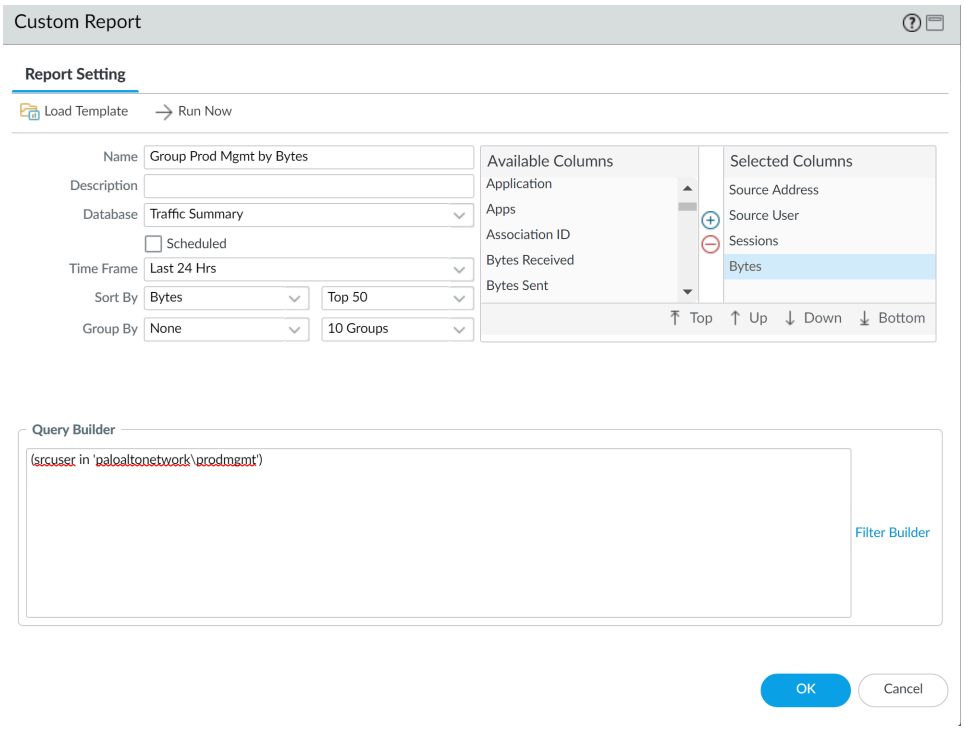
# My Traffic Summary Report

ca1demo.paloaltonetworks.com : 2016/01/25 10:34:39 - 2016/02/24 10:34:38

| Source Zone | Destination Zone | App Category | Application | Sessions | Bytes |
|---|---|---|---|---|---|
| Tap | Tap | general-internet | web-browsing | 74.54 M | 2.47 T |
| Tap | Tap | networking | dns | 52.03 M | 28.93 G |
| Tap | Tap | networking | ssl | 18.01 M | 678.13 G |
| Tap | Tap | general-internet | bittorrent | 9.80 M | 1.62 T |
| Tap | Tap | general-internet | google-base | 4.48 M | 168.99 G |
| Tap | Tap | unknown | insufficient-data | 4.45 M | 31.30 G |
| Tap | Tap | collaboration | facebook-base | 4.09 M | 99.14 G |
| Tap | Tap | networking | ntp | 4.07 M | 3.29 G |
| Tap | Tap | collaboration | blackboard | 2.84 M | 186 G |
| Tap | Tap | collaboration | smtp | 1.92 M | 172.57 G |
| Tap | Tap | networking | icmp | 1.36 M | 320.49 M |
| Tap | Tap | general-internet | gnutella | 1.17 M | 17.84 G |
| Tap | Tap | collaboration | myspace-base | 1.10 M | 35.22 G |
| Tap | Tap | general-internet | ping | 1.06 M | 86.21 M |
| Tap | Tap | general-internet | flash | 1.01 M | 168.14 G |

이제 쿼리 빌더를 사용하여 사용자 그룹 내 네트워크 리소스의 최상위 소비자를 나타내는 맞춤 보고서를 생성하려면 다음과 같이 보고서를 설정합니다.


©2023 Palo Alto Networks, Inc.




보고서에는 제품 관리 사용자 그룹의 최상위 사용자가 바이트 단위로 정렬되어 표시됩니다.

# 봇넷 보고서 생성

봇넷 보고서를 사용하면 휴리스틱 및 행동 기반 메커니즘을 사용하여 네트워크에서 잠재적인 멀웨어 또는 봇넷에 감염된 호스트를 식별할 수 있습니다. 봇넷 활동 및 감염된 호스트를 평가하기 위해 방화벽은 위협, URL 및 데이터 필터링 로그의 사용자 및 네트워크 활동 데이터를 PAN-DB의 멀웨어 URL 목록, 알려진 동적 DNS 도메인 공급자 및 지난 30일 이내에 등록된 도메인과 연동시킵니다. 해당 사이트를 방문한 호스트 및 IRC(Internet Relay Chat) 서버와 통신하거나 알 수 없는 애플리케이션을 사용한 호스트를 식별하도록 보고서를 구성할 수 있습니다. 멀웨어는 IP 차단을 피하기 위해 종종 동적 DNS를 사용하는 반면 IRC 서버는 자동화된 기능을 위해 봇을 사용하는 경우가 많습니다.

방화벽에서 봇넷 보고서를 사용하려면 위협 예방 및 ***URL*** 필터링 라이선스가 필요합니다**.** 봇넷 보고서에서 사용하는 지표 외에 추가 지표를 기반으로 의심스러운 활동을 모니터링하기 위해 자동화된 연동 엔진 사용을**(**를**)** 할 수 있습니다**.** 그러나 봇넷 보고서는 새로 등록된 도메인을 지표로 사용하는 유일한 도구입니다**.**

- 봇넷 보고서 구성
- 봇넷 보고서 출력 해석

## 봇넷 보고서 구성

봇넷 보고서를 예약하거나 요청 시 실행할 수 있습니다. 행동 기반 탐지에는 해당 기간 동안 여러 로그의 트래픽을 연관시켜야 하기 때문에 방화벽은 24시간마다 예약된 봇넷 보고서를 생성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 가능한 봇넷 활동을 나타내는 트래픽 유형을 정의합니다.

1. 모니터 > 봇넷을 선택하고 페이지 오른쪽에서 구성을 클릭합니다.
2. 보고서에 포함될 각 HTTP 트래픽 유형에 대한 개수를 활성화하고 정의합니다.

   **Count** 값은 보고서가 더 높은 신뢰도 점수(봇넷 감염 가능성이 높음)로 연결된 호스트를 나열하기 위해 발생해야 하는 각 트래픽 유형의 최소 이벤트 수를 나타냅니다. 이벤트 수가 개수보다 적으면 보고서에 더 낮은 신뢰도 점수가 표시되거나(특정 트래픽 유형의 경우) 호스트 항목이 표시되지 않습니다. 예를 들어 **Malware URL** 방문에 대해 **Count**를 3으로 설정하면 3개 이상의 알려진 맬웨어 URL을 방문하는 호스트가 3개 미만을 방문하는 호스트보다 점수가 더 높게 됩니다. 자세한 내용은 봇넷 보고서 출력 해석을(를) 참조하십시오.
3. 알 수 없는 TCP 또는 알 수 없는 UDP 애플리케이션과 관련된 트래픽과 연결된 호스트가 보고서에 포함될지의 여부를 결정하는 임계값을 정의합니다.
4. IRC 서버와 관련된 트래픽을 포함하려면 **IRC** 확인란을 선택합니다.
5. 확인을 클릭하여 보고서 구성을 저장합니다.

**STEP 2 |** 보고서를 예약하거나 요청 시 실행합니다.

1. 페이지 오른쪽에서 보고서 설정을 클릭합니다.
2. 테스트 실행 시간 프레임 드롭다운에서 보고서의 시간 간격을 선택합니다.
3. 보고서에 포함할 행 수를 선택합니다.
4. **(**선택 사항**)** 쿼리 작성기에 쿼리를 추가하여 소스/대상 IP 주소, 사용자 또는 영역과 같은 속성별로 보고서 출력을 필터링합니다.

   예를 들어, IP 주소 10.3.3.15에서 시작된 트래픽에 잠재적인 봇넷 활동이 없다는 것을 미리 알고 있는 경우 보고서 출력에서 해당 호스트를 제외하는 쿼리로 **`Not(10.0.1.35`**의 **`addr.src)`**을 추가합니다. 자세한 내용은 봇넷 보고서 출력 해석을(를) 참조하십시오.
5. 보고서를 매일 실행하려면 예약됨을 선택한 다음 보고서를 즉시 실행하려면 지금 실행을 클릭합니다.
6. 확인 및 커밋을 클릭합니다.

## 봇넷 보고서 출력 해석

봇넷 보고서에는 보고서를 구성할 때 의심스러운 것으로 정의한 트래픽과 연결된 각 호스트에 대한 행이 표시됩니다. 각 호스트에 대해 보고서에는 봇넷 감염 가능성을 나타내기 위해 1에서 5의 신뢰도 점수가 표시됩니다. 여기서 5는 가장 높은 가능성을 나타냅니다. 점수는 위협 심각도 수준에 해당합니다. 1은 정보 제공, 2는 낮음, 3은 중간, 4는 높음, 5는 심각입니다. 방화벽은 점수의 기준이 됩니다.

- 트래픽 유형 - 특정 HTTP 트래픽 유형은 봇넷 활동을 포함할 가능성이 더 높습니다. 예를 들어 보고서에서는 URL 대신 IP 도메인을 탐색하는 호스트보다 알려진 멀웨어 URL을 방문하는 호스트에 더 높은 신뢰도를 할당합니다. 이 두 활동을 모두 의심스러운 것으로 정의했다고 가정합니다.
- 이벤트 수 - 더 많은 수의 의심스러운 이벤트와 연결된 호스트는 사용자가 정의한 임계값(개수 값)을 기준으로 신뢰도 점수가 더 높습니다봇넷 보고서 구성.
- 실행 파일 다운로드 - 보고서는 실행 파일을 다운로드하는 호스트에 더 높은 신뢰도를 부여합니다. 실행 파일은 다양한 감염의 일부이며, 다른 유형의 의심스러운 트래픽과 결합하면 손상된 호스트에 대한 조사의 우선 순위를 정하는 데 도움이 될 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

보고서 출력을 검토할 때 방화벽이 봇넷 활동을 평가하는 데 사용하는 소스(예: PAN-DB의 멀웨어 URL 목록)에 차이가 있을 수 있습니다. 또한 이러한 소스에서 안전하다고 생각하는 트래픽을 식별할 수도 있습니다. 두 경우 모두를 보완하기 위해 봇넷 보고서 구성일 때 쿼리 필터를 추가할 수 있습니다.

## SaaS 애플리케이션 사용 보고서 생성

SaaS 애플리케이션 사용 PDF 보고서는 위험 및 제재 상태별로 SaaS 애플리케이션 활동을 쉽게 탐색할 수 있는 두 부분으로 구성된 보고서입니다. 승인된 애플리케이션은 네트워크에서 사용하도록 공식적으로 승인한 애플리케이션입니다. SaaS 애플리케이션은 개체 > 애플리케이션의 애플리케이션 세부 정보 페이지에서 특성 SaaS=yes인 애플리케이션이며 다른 모든 애플리케이션은 비 SaaS로 간주됩니다. SaaS 또는 비 SaaS 애플리케이션을 승인했음을 나타내려면 승인됨이라는 사전 정의된 태그로 태그를 지정해야 합니다. 방화벽과 Panorama는 이 사전 정의된 태그가 없는 모든 애플리케이션을 네트워크에서 사용하도록 승인되지 않은 것으로 간주합니다.

- 보고서의 첫 번째 부분은 승인된 애플리케이션과 승인되지 않은 애플리케이션을 비교하여 보고 기간 동안 네트워크의 SaaS 애플리케이션에 대한 주요 결과를 제시하고 사용량, 규정 준수 및 데이터 전송에 따른 제재 상태를 기반으로 상위 애플리케이션을 나열합니다. 고위험 애플리케이션 사용 범위를 식별하고 탐색하는 데 도움이 되도록 보고서의 위험한 특성이 있는 애플리케이션 섹션에는 다음과 같은 불리한 호스팅 특성을 가진 SaaS 애플리케이션이 나열되어 있습니다: 획득한 인증, 과거 데이터 파기, IP 기반 제한에 대한 지원, 재정상 실행 가능성 및 서비스 조건. 또한 네트워크에서 사용되는 총 애플리케이션 수, 이러한 애플리케이션에서 사용하는 대역폭, 이러한 애플리케이션을 사용하는 사용자 수, SaaS 애플리케이션을 가장 많이 사용하는 상위 사용자 그룹, 승인되거나 승인되지 않은 SaaS 애플리케이션을 통해 가장 많은 양의 데이터를 전송하는 상위 사용자 그룹. 보고서의 이 첫 번째 부분은 또한 사용된 최대 애플리케이션 수, 사용자 수 및 각 애플리케이션 하위 카테고리에서 전송된 데이터(바이트) 양에 따라 나열된 상위 SaaS 애플리케이션 하위 카테고리를 강조 표시합니다.
- 보고서의 두 번째 부분은 보고서의 첫 번째 부분에 나열된 각 애플리케이션 하위 카테고리에 대한 SaaS 및 비 SaaS 애플리케이션에 대한 자세한 탐색 정보에 중점을 둡니다. 하위 카테고리의 각 애플리케이션에 대해 데이터를 전송한 상위 사용자, 차단되거나 경고된 상위 파일 형식, 각 애플리케이션에 대한 상위 위협에 대한 정보도 포함됩니다. 또한 보고서의 이 섹션에서는 방화벽이 WildFire 분석을 위해 제출한 각 애플리케이션에 대한 샘플과 양성 및 악성으로 결정된 샘플 수를 집계합니다.

이 보고서의 통찰력을 사용하여 비즈니스 크리티컬 및 승인된 SaaS 애플리케이션 목록을 통합하고 멀웨어 전파 및 데이터 유출에 불필요한 위험을 초래하는 승인되지 않고 위험한 애플리케이션을 제어하기 위한 정책을 시행하십시오.

사전 정의된 ***SaaS*** 애플리케이션 사용 보고서는 지정된 날짜에 네트워크에서 실행되는 상위 ***100***개의 ***SaaS*** 애플리케이션***(SaaS*** 애플리케이션 특성이 있는 애플리케이션을 의미**,** ***SaaS=yes)***을 나열하는 일일 보고서 보기을***(***를***)*** 형식으로 계속 사용할 수 있습니다**.** 이 보고서는 승인된 애플리케이션에 대한 가시성을 제공하는 것이 아니라 네트워크에서 사용 중인 모든 ***SaaS*** 애플리케이션에 대한 가시성을 제공합니다**.**


©2023 Palo Alto Networks, Inc.

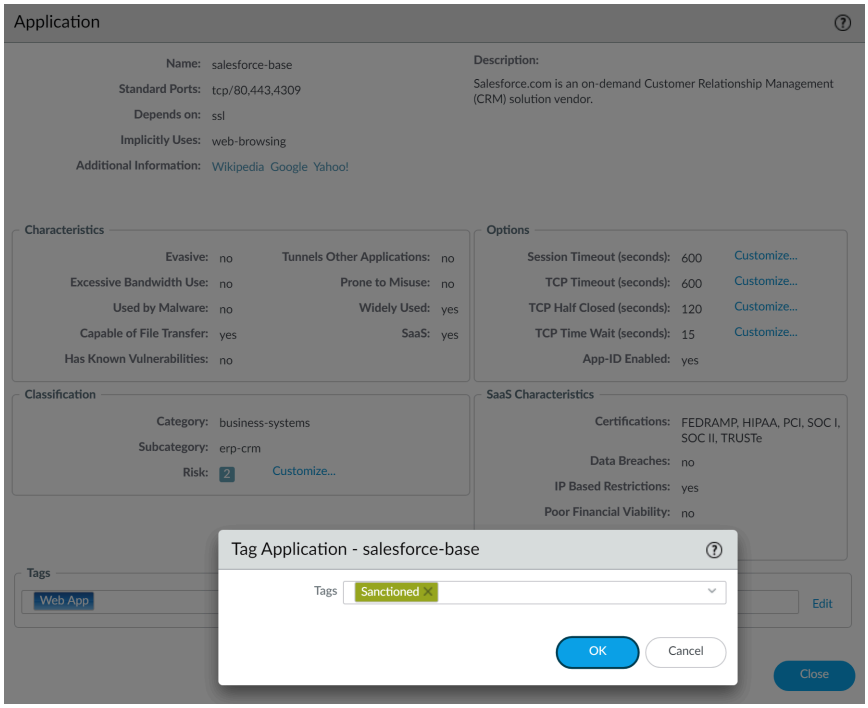
**STEP 1 |** 네트워크에서 사용하도록 승인한 애플리케이션에 승인된 태그를 지정합니다.

정확하고 유익한 보고서를 생성하려면 여러 가상 시스템이 있는 방화벽과 ***Panorama***의 디바이스 그룹에 속하는 방화벽 전반에 걸쳐 승인된 애플리케이션에 일관되게 태그를 지정해야 합니다. 동일한 애플리케이션이 한 가상 시스템에서 승인된 것으로 태그가 지정되고 다른 가상 시스템에서는 승인되지 않은 경우 또는 ***Panorama***에서 애플리케이션이 상위 디바이스 그룹에서 승인되지 않았지만 하위 디바이스 그룹에서 승인된 것으로 태그 지정된 경우(또는 그 반대의 경우), ***SaaS*** 애플리케이션 사용 보고서는 애플리케이션이 부분적으로 승인된 것으로 보고하며 결과는 중복됩니다.

예시: Box가 vsys1에서 승인되고 Google Drive가 vsys2에서 승인되면 vsys1의 Google Drive 사용자는 승인되지 않은 SaaS 애플리케이션의 사용자로 계산되고 vsys2의 Box 사용자는 승인되지 않은 SaaS 애플리케이션의 사용자로 계산됩니다. 보고서의 주요 결과는 승인된 애플리케이션 2개와 승인되지 않은 애플리케이션 2개가 있는 네트워크에서 총 2개의 고유한 SaaS 애플리케이션이 발견되었음을 강조합니다.

1. 개체 > 애플리케이션을 선택합니다.
2. 애플리케이션을 편집하려면 애플리케이션 이름을 클릭하고 태그 섹션에서 수정을 선택합니다.
3. 태그 드롭다운에서 승인됨을 선택합니다.

   사전 정의된 승인 태그(Sanctioned)를 사용해야 합니다. 다른 태그를 사용하여 애플리케이션을 승인했음을 나타내면 방화벽이 태그를 인식하지 못하고 보고서가 부정확해집니다.




4. 확인 및 닫기를 클릭하여 열려 있는 모든 대화 상자를 종료합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** SaaS 애플리케이션 사용 보고서를 구성합니다.

1. 모니터 > **PDF** 보고서 > **SaaS** 애플리케이션 사용을 선택합니다.
2. 추가를 클릭하고 이름을 입력하고 보고서의 기간을 선택합니다(기본값은 지난 **7**일).

   기본적으로 보고서에는 상위 ***SaaS*** 및 비 ***SaaS*** 애플리케이션 하위 카테고리에 대한 자세한 정보가 포함되어 있어 페이지 수와 파일 크기에 따라 보고서가 커질 수 있습니다. 파일 크기를 줄이고 페이지 수를 ***10***페이지로 제한하려면 보고서에 자세한 애플리케이션 카테고리 정보 포함 체크박스를 선택 취소합니다.

3. 보고서에 로그를 포함할지 여부를 선택합니다.

   ***PAN-OS 10.0.2*** 이상 릴리스에서 ***Cortex Data Lake***의 로그에서 생성된 보고서는 선택한 영역의 로그만 포함하여 지원합니다.

   - 모든 사용자 그룹 및 영역 - 보고서에는 로그에서 사용할 수 있는 모든 보안 영역 및 사용자 그룹에 대한 데이터가 포함됩니다.

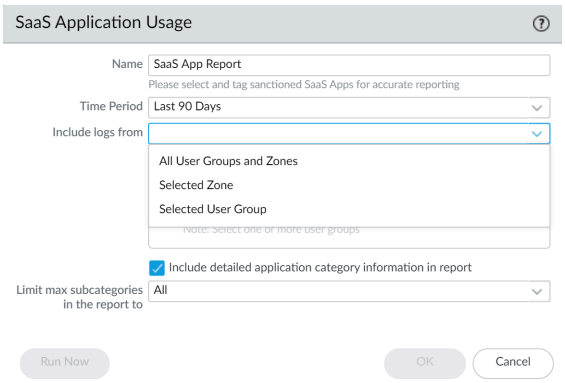
     보고서에 특정 사용자 그룹을 포함하려면 보고서에 사용자 그룹 정보 포함을 선택한 다음 그룹 관리 링크를 클릭하여 포함할 그룹을 선택합니다. 방화벽 또는 Panorama가 선택한 사용자 그룹에 대한 로그를 필터링할 수 있도록 1개에서 최대 25개의 사용자 그룹을 추가해야 합니다. 포함할 그룹을 선택하면 보고서는 기타라는 하나의 그룹으로 모든 사용자 그룹을 집계합니다.
   - 선택한 영역 - 보고서는 지정된 보안 영역에 대한 데이터를 필터링하고 해당 영역의 데이터만 포함합니다.

     보고서에 특정 사용자 그룹을 포함하려면 보고서에 사용자 그룹 정보 포함을 선택한 다음 선택한 영역에 대한 그룹 관리 링크를 클릭하여 보고서에 포함할 이 영역 내의 사용자 그룹을 선택합니다. 방화벽 또는 Panorama가 보안 영역 내에서 선택한 사용자 그룹에 대한 로그를

 ©2023 Palo Alto Networks, Inc.

필터링할 수 있도록 1개에서 최대 25개의 사용자 그룹을 추가해야 합니다. 포함할 그룹을 선택하면 보고서는 기타라는 하나의 그룹으로 모든 사용자 그룹을 집계합니다.

- 선택한 사용자 그룹 - 보고서는 지정된 사용자 그룹에 대한 데이터만 필터링하고 선택한 사용자 그룹에 대한 SaaS 애플리케이션 사용 정보를 포함합니다.




4. 보고서에 모든 애플리케이션 하위 카테고리를 포함할지(기본값) 또는 보고서의 최대 하위 카테고리를 상위 **10, 15, 20** 또는 **25**개 카테고리로 제한할지(기본값은 모든 하위 카테고리)를 선택합니다.
5. 지금 실행을 클릭하여 지난 7일 및 지난 30일 기간에 대한 요청 시 보고서를 생성합니다. 보고서가 새 탭에서 열리므로 브라우저에서 팝업 차단기가 비활성화되어 있는지 확인하십시오.
6. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 3 |** 이메일 전송을 위한 보고서 예약.

지난 90일 보고서는 이메일 전송을 위해 예약해야 합니다.

PA-220R 및 PA-800 시리즈 방화벽에서 SaaS 애플리케이션 사용 보고서는 이메일에 PDF 첨부 파일로 전송되지 않습니다. 대신 이메일에는 웹 브라우저에서 보고서를 열 때 클릭해야 하는 링크가 포함되어 있습니다.

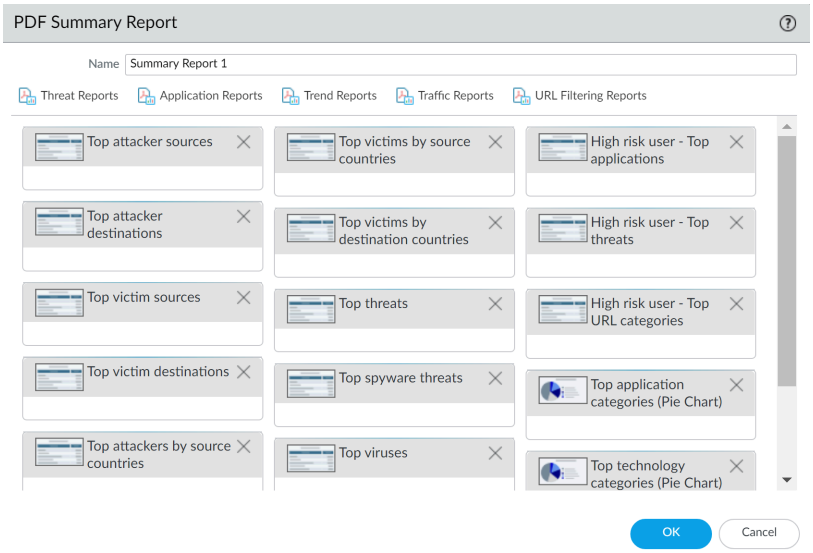
## PDF 요약 보고서 관리

PDF 요약 보고서에는 각 카테고리의 상위 5개(상위 50위 대신)에 대한 데이터를 기반으로 기존 보고서에서 컴파일된 정보가 포함되어 있습니다. 여기에는 다른 보고서에서 사용할 수 없는 추세 차트도 포함됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** **PDF** 요약 보고서를 설정합니다.

1. 모니터 > **PDF** 보고서 > **PDF** 요약 관리를 선택합니다.
2. 추가를 클릭한 다음 보고서의 이름을 입력합니다.
3. 각 보고서 그룹에 대한 드롭다운을 사용하고 PDF 요약 보고서를 디자인할 요소를 하나 이상 선택합니다. 최대 18개의 보고서 요소를 포함할 수 있습니다.




상위 위협 선택은 *PDF* 요약 보고서의 사전 정의된 위젯 열에서 최상위 공격으로 표시됩니다.

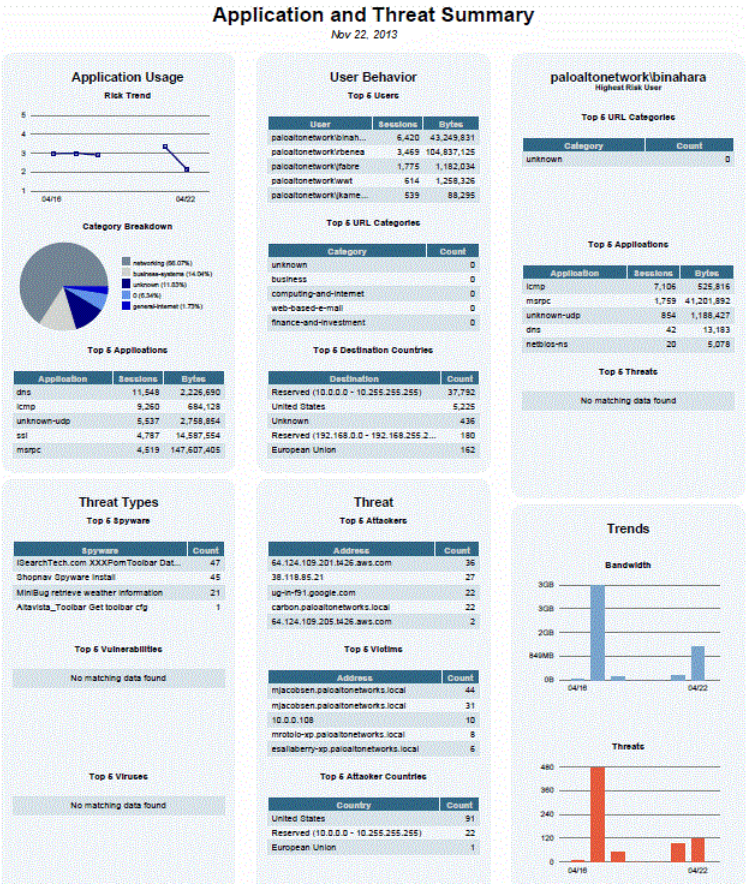
- 보고서에서 요소를 제거하려면 **x** 아이콘을 클릭하거나 적절한 보고서 그룹에 대한 드롭다운에서 선택 영역을 지웁니다.
- 보고서를 다시 정렬하려면 요소 아이콘을 드래그하고 보고서의 다른 영역으로 놓습니다.

4. 확인을 클릭하여 보고서를 저장합니다.
5. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 보고서를 봅니다.

PDF 요약 보고서를 다운로드하고 보려면 보고서 보기을(를) 참조하십시오.




다음 요약 섹션은 다음 ***PDF*** 요약 보고서 요소를 참조합니다.

- 상위 ***5***개 공격 - 최상위 위협 요소를 말합니다.
- 상위 ***5***가지 위협 - 고위험 사용자**-** 최고 위협 요소를 말합니다.
- 상위 위협 보고서는 상위 위협 요소의 전체 위협 목록을 나타냅니다.

## 사용자/그룹 활동 보고서 생성

사용자/그룹 활동 보고서는 개별 사용자 또는 사용자 그룹의 웹 활동을 요약합니다. 두 보고서에는 **URL** 카테고리별 브라우징 요약 및 사용자 활동 보고서만 포함하는 시간 계산, 검색을 제외한 동일한 정보가 포함됩니다.

방화벽에서 사용자 및 사용자 그룹 목록에 액세스하도록 User-ID을(를) 구성해야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 사용자/그룹 활동 보고서에 대한 찾아보기 횟수 및 로그 수를 구성합니다.

기본 값을 변경하려는 경우에만 필요합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집한 다음 로그 내보내기 및 보고 탭을 선택합니다.
2. 사용자 활동 보고서의 최대 행 수에 대해 자세한 사용자 활동 보고서가 지원하는 최대 행 수를 입력합니다(범위는 1-1048576, 기본값은 5000). 보고서가 분석하는 로그 수를 결정합니다.
3. 사용자가 웹 페이지를 탐색하는 데 걸리는평균 탐색 시간(초)을 입력합니다(범위는 0-300, 기본값은 60). 평균 검색 시간 경과 후 이루어진 모든 요청은 새로운 브라우징 활동으로 간주됩니다. 계산에서는 사용자가 방문한 페이지만 기록(URL 필터링 로그에 기록됨)을(를) 기준으로 사용하고 첫 번째 요청 시간(시작 시간)과 평균 탐색 시간 사이에 로드된 모든 새 웹 페이지를 무시합니다. 예를 들어 평균 찾아보기 시간을 2분으로 설정하고 사용자가 웹 페이지를 열고 해당 페이지를 5분 동안 보는 경우 해당 페이지의 찾아보기 시간은 2분이 됩니다. 이 작업은 방화벽이 사용자가 지정된 페이지를 보는 정도를 확인할 수 없기 때문에 수행됩니다. 평균 검색 시간 계산은 웹 광고 및 콘텐츠 전송 네트워크로 분류된 사이트를 무시합니다.
4. 페이지 로드 임계값의 경우 페이지 요소가 페이지에 로드되는 예상 시간(초)을 입력합니다(기본값은 20). 첫 번째 페이지 로드와 페이지 로드 임계값 사이에 발생하는 모든 요청은 페이지의 요소로 가정됩니다. 페이지 로드 임계값 외부에서 발생하는 모든 요청은 사용자가 페이지 내에서 링크를 클릭한 것으로 간주됩니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 2 |** 사용자/그룹 활동 보고서를 생성합니다.

1. 모니터 > **PDF** 보고서 > 사용자 활동 보고서를 선택합니다.
2. 추가를 클릭한 다음 보고서의 이름을 입력합니다.
3. 보고서 생성:
   - 사용자 활동 보고서 - 사용자를 선택한 다음 사용자의 사용자 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
   - 그룹 활동 보고서 - 그룹을 선택한 다음 사용자 그룹의 그룹 이름을 선택합니다.
4. 보고서의 기간을 선택합니다.
5. (선택 사항)보고서에 자세한 URL 로그를 포함하도록 상세 브라우징 체크박스(기본값 삭제됨)를 선택합니다.

   상세 브라우징 정보에는 선택한 사용자 또는 사용자 그룹에 대한 대량의 로그(수천 개의 로그)가 포함될 수 있으며 보고서를 대용량으로 만들 수 있습니다.
6. 요청 시 보고서를 실행하려면 지금 실행을 클릭합니다.
7. 보고서 구성을 저장하려면 확인을 클릭합니다. 방화벽에서 사용자/그룹 활동 보고서의 출력을 저장할 수 없습니다. 이메일 배달을 위해 보고서를 예약하려면 이메일 전송을 위한 보고서 예약을(를) 참조하십시오.

## 보고서 그룹 관리

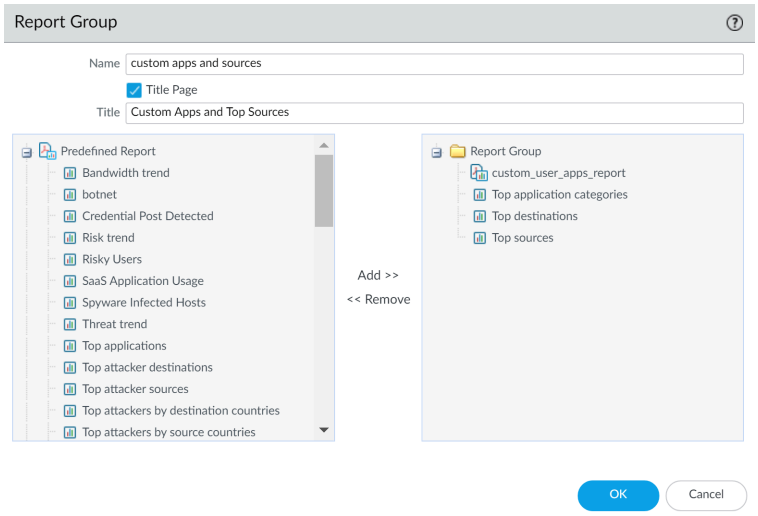
보고서 그룹을 사용하면 시스템에서 컴파일하여 단일 통합 PDF 보고서로 보낼 수 있는 보고서 세트를 생성할 수 있으며, 여기에는 선택적 제목 페이지와 모든 구성 보고서가 포함됩니다.

 ©2023 Palo Alto Networks, Inc.

보고서 그룹을 설정합니다.

보고서에 이메일에 보고서 그룹을 설정해야 합니다.

1. 이메일 서버 프로파일을 만듭니다.
2. 보고서 그룹을 정의합니다. 보고서 그룹은 사전 정의된 보고서, PDF 요약 보고서, 맞춤 보고서 및 로그 뷰 보고서를 단일 PDF로 컴파일할 수 있습니다.
   1. 모니터 > 보고서 그룹을 선택합니다.
   2. 추가를 클릭한 다음 보고서 그룹에 대한 이름을 입력합니다.
   3. (선택사항) 제목 페이지를 선택한 다음 PDF 출력에 대한 제목을 추가합니다.
   4. 왼쪽 열에서 보고서를 선택한 다음 추가를 클릭하여 각 보고서를 오른쪽의 보고서 그룹으로 이동합니다.




로그 뷰 보고서는 맞춤 보고서를 만들 때마다 자동으로 만들어지고 맞춤 보고서와 동일한 이름을 사용하는 보고서 유형입니다. 이 보고서에는 맞춤 보고서의 내용을 빌드하는 데 사용된 로그가 표시됩니다.

로그 뷰 데이터를 포함하려면 보고서 그룹을 만들 때 맞춤 보고서 목록에 맞춤 보고서를 추가한 다음 로그 뷰 목록에서 일치하는 보고서 이름을 선택하여 로그 뷰 보고서를 추가합니다. 보고서에는 맞춤 보고서 데이터와 맞춤 보고서를 만드는 데 사용된 로그 데이터가 포함됩니다.

   5. 설정을 저장하려면 확인을 클릭합니다.
   6. 보고서 그룹을 사용하려면 이메일 전송에 대한 일정 보고서를 참조하십시오.

## 이메일 전송을 위한 보고서 예약

보고서는 매일 포워딩하도록 예약하거나 매주 지정된 날짜에 포워딩할 수 있습니다. 예약된 보고서는 오전 2:00부터 실행되며 모든 예약된 보고서가 생성된 후 이메일 포워딩이 시작됩니다.

**STEP 1 |** 모니터 > **PDF** 보고서 > 이메일 스케줄러를 선택하고 추가를 클릭합니다.

**STEP 2 |** 일정을 식별할 이름을 입력합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 이메일 전달을 위한 보고서 그룹을 선택합니다. 보고서 그룹을 설정하려면 보고서 그룹 관리를 참조하십시오.

**STEP 4 |** 이메일 프로파일의 경우 보고서 포워딩에 사용할 이메일 서버 프로파일을 선택하거나 이메일 프로파일 링크를 클릭하여 이메일 서버 프로파일을 생성합니다.

**STEP 5 |** 반복서 보고서를 생성하고 보낼 빈도를 선택합니다.

**STEP 6 |** 이메일 주소 재정의 필드를 사용하면 지정된 수신자에게만 이 보고서를 보낼 수 있습니다. 필드에 수신자를 추가하면 방화벽은 이메일 서버 프로파일에 구성된 수신자에게 보고서를 보내지 않습니다. 보고서가 이메일 서버 프로파일에 정의된 관리자나 수신자가 아닌 다른 사람의 주의를 끌 경우에 이 옵션을 사용하십시오.

**STEP 7 |** 확인 및 커밋을 클릭합니다.

## 보고서 저장 용량 관리

기본적으로 방화벽에는 방화벽에서 생성된 보고서에 대한 200MB의 전용 저장소가 포함되어 있습니다. 특히 PA-7000 시리즈 및 PA-5200 시리즈 방화벽의 경우 새 보고서를 성공적으로 생성하려면 사용 가능한 보고서 저장소 공간의 용량을 늘려야 할 수 있습니다.

**STEP 1 |** 방화벽 CLI에 액세스합니다.

**STEP 2 |** 방화벽의 현재 보고서 저장소 용량 확인:

명령 출력에는 보고서 저장소 크기를 바이트에 표시합니다. 이 절차의 경우 방화벽에는 기본 200MB 보고서 저장소 용량이 있습니다.

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

209715200
```

**STEP 3 |** 보고서 저장소 용량을 확장하는 데 할당할 수 있는 충분한 저장소가 방화벽 전체에 있는지 확인합니다.

```
admin> show system disk-space
```

```
admin@ISP-CONDOR-B(active)> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        12G  8.9G  2.0G  83% /
none            7.9G   52K  7.9G   1% /dev
/dev/sda5        16G  8.5G  5.9G  59% /opt/pancfg
/dev/sda6        12G  5.8G  5.0G  54% /opt/panrepo
tmpfs           7.9G  247M  7.6G   4% /dev/shm
/dev/sda8        22G  8.7G   12G  43% /opt/panlogs
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 필요에 따라 보고서 저장소 용량을 늘립니다.

예를 들어 보고서 저장소 크기를 1GB로 늘리고 있습니다.

```
admin> request report-storage-size set size <0-4>
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size set size 1

cfg.report-storage-size-gb: 1
```

**STEP 5 |** 보고서 저장소 용량이 이전 단계에서 설정된 양으로 증가했는지 확인합니다.

```
admin> request report-storage-size show
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

1073741824
```

 ©2023 Palo Alto Networks, Inc.

# 정책 규칙 사용 보기

보안, NAT, QoS, PBF(정책 기반 포워딩), 복호화, 터널 검사, 애플리케이션 재정의, 인증 또는 DoS 방어 규칙이 트래픽과 일치하는 횟수를 확인하여 변화가 필요한 환경 및 보안에 따라 방화벽 정책을 최신 상태로 유지합니다. 서버가 폐기되거나 서비스에 대한 임시 액세스가 더 이상 필요하지 않은 경우와 같이 공격자가 초과 프로비저닝된 액세스를 악용하지 못하도록 하려면 정책 규칙 적중 횟수 데이터를 사용하여 사용하지 않는 규칙을 식별하고 제거합니다.

정책 규칙 사용 데이터를 사용하면 규칙 추가 및 규칙 변경을 검증하고 규칙이 사용된 기간을 모니터링할 수 있습니다. 예를 들어 포트 기반 규칙을 앱 기반 규칙으로 마이그레이션할 때 포트 기반 규칙 위에 앱 기반 규칙을 생성하고 포트 기반 규칙과 일치하는 트래픽이 있는지 확인합니다. 마이그레이션 후 적중 횟수 데이터는 트래픽이 포트 기반 규칙이 아닌 앱 기반 규칙과 일치하는지 확인하여 포트 기반 규칙을 제거하는 것이 안전한지의 여부를 판단하는 데 도움이 됩니다. 정책 규칙 적중 횟수는 규칙이 액세스 시행에 효과적인지의 여부를 결정하는 데 도움이 됩니다.

규칙 적중 횟수 데이터를 재설정하여 기존 규칙의 유효성을 검사하거나 지정된 기간 내의 규칙 사용량을 측정할 수 있습니다. 정책 규칙 적중 수 데이터는 방화벽이나 Panorama에 저장되지 않으므로 적중 수를 재설정(지우기)한 후에는 데이터를 더 이상 사용할 수 없습니다.

정책 규칙 베이스를 필터링한 후 관리자는 정책 최적화 프로그램에서 직접 정책 규칙을 삭제, 비활성화, 활성화 및 태그 지정하는 조치를 취할 수 있습니다. 예를 들어 사용하지 않는 규칙을 필터링한 다음 검토를 위해 태그를 지정하여 규칙 베이스에서 안전하게 삭제할 수 있는지 또는 유지할 수 있는지 결정할 수 있습니다. 관리자가 정책 최적화 프로그램에서 직접 조치를 취할 수 있도록 함으로써 규칙 수명 주기 관리를 단순화하고 방화벽이 과도하게 프로비저닝되지 않도록 하는 데 필요한 관리 오버헤드를 줄일 수 있습니다.

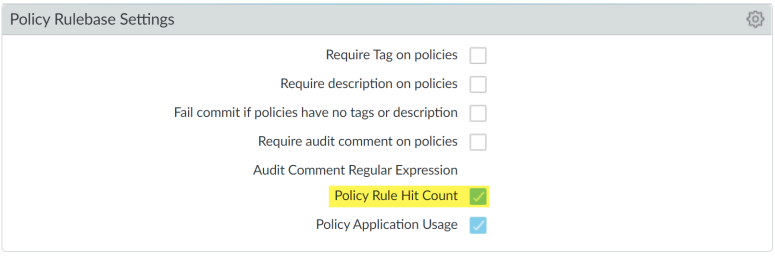
규칙 적중 수 데이터는 고가용성(*HA*) 배포에서 방화벽 간에 동기화되지 않으므로 각 방화벽에 대한 정책 규칙 적중 수 데이터를 보려면 각 방화벽에 로그인해야 하거나 *Panorama*를 사용하여 *HA* 방화벽 피어에 대한 정보를 확인해야 합니다.

정책 규칙 사용 데이터는 보안 정책 규칙 최적화을(를) 사용하여 먼저 마이그레이션하거나 정리할 규칙을 결정할 때도 유용합니다.

**STEP 1 |** 웹 인터페이스 실행.

**STEP 2 |** 정책 규칙 적중 횟수가 활성화되어 있는지 확인합니다.

1. 정책 규칙 베이스 설정(디바이스 > 설정 > 관리)으로 이동합니다.
2. 정책 규칙 적중 횟수가 활성화되어 있는지 확인합니다.




**STEP 3 |** 정책을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 각 정책 규칙에 대한 정책 규칙 사용 보기:

- 적중 횟수 - 트래픽이 정책 규칙에 정의한 기준과 일치한 횟수입니다. 규칙을 수동으로 재설정하거나 이름을 변경하지 않는 한 재부팅, 데이터플레인 다시 시작 및 업그레이드를 통해 지속됩니다.
- 최종 적중 - 트래픽이 규칙과 일치했을 때의 가장 최근 타임스탬프입니다.
- 최초 적중 - 트래픽이 이 규칙과 일치한 첫 번째 인스턴스입니다.
- 수정됨 - 정책 규칙이 마지막으로 수정된 날짜 및 시간입니다.
- 생성됨 - 정책 규칙이 생성된 날짜 및 시간입니다.

*Panorama*가 *PAN-OS 8.1*을 실행 중일 때 규칙이 생성되었고 정책 규칙 적중 횟수 설정이 활성화된 경우 *PAN-OS 9.0*으로 업그레이드할 때 첫 번째 적중 날짜 및 시간이 생성 날짜 및 시간으로 사용됩니다. 정책 규칙 적중 횟수 설정이 비활성화되었을 때 *PAN-OS 8.1*에서 규칙이 생성되었거나 *Panorama*가 *PAN-OS 8.0* 또는 이전 릴리스를 실행할 때 규칙이 생성된 경우 규칙의 생성 날짜는 날짜 및 시간이 됩니다. *Panorama*를 *PAN-OS 9.0*으로 성공적으로 업그레이드했습니다.

| | | Source | | | Rule Usage | | | | |
|---|---|---|---|---|---|---|---|---|---|
| NAME | T... | Z... | A... | U... | HIT COUNT | LAST HIT | FIRST HIT | MODIFIED | CREATED |
| /ideo | n... | a... | a... | a... | 2424328 | 2020-09-22 11:33:00 | 2019-07-30 10:12:57 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| Video Streaming | n... | a... | a... | a... | 14337228 | 2020-09-22 16:26:58 | 2019-07-30 10:12:57 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| `cavenger | n... | a... | a... | a... | 321760616 | 2020-09-22 16:27:10 | 2019-07-30 10:12:57 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| Web Traffic | n... | a... | a... | a... | 1509584361 | 2020-09-22 16:27:10 | 2019-07-30 10:12:02 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| iperf | n... | a... | a... | a... | 5 | 2019-10-15 14:54:31 | 2019-10-11 13:08:28 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |

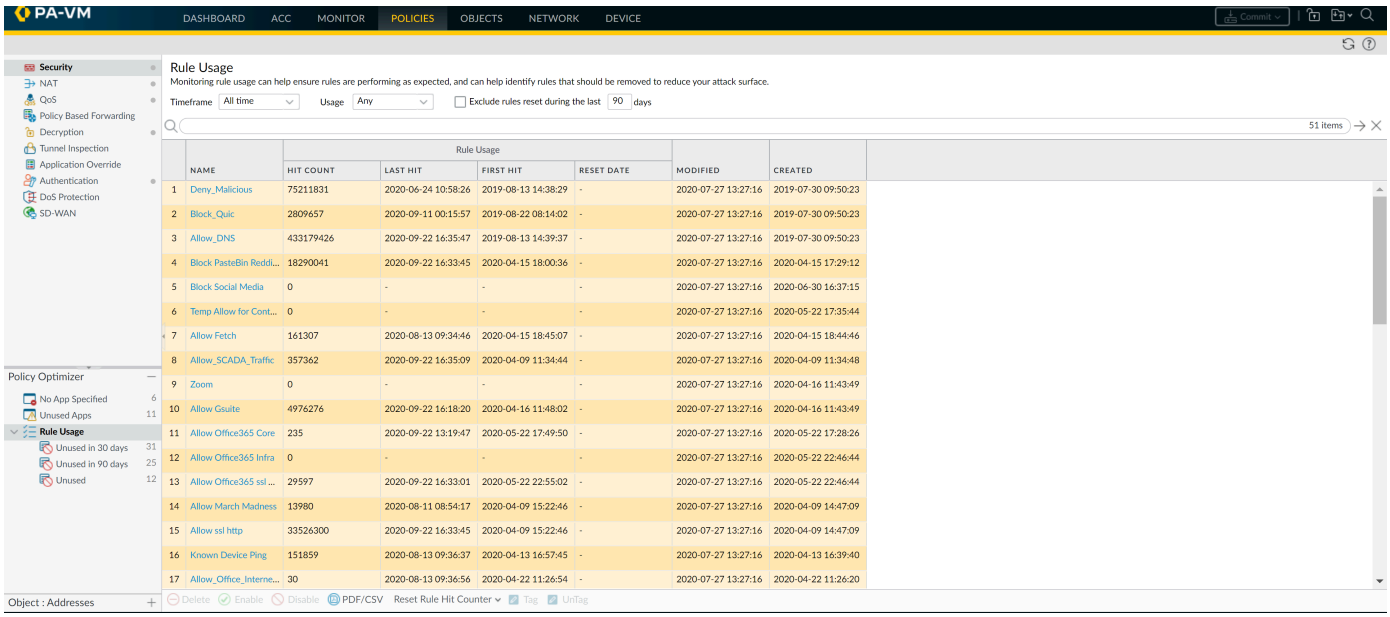
**STEP 5 |** 정책 최적화 대화 상자에서 규칙 사용 필터를 봅니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 선택한 규칙 베이스에서 규칙을 필터링합니다.

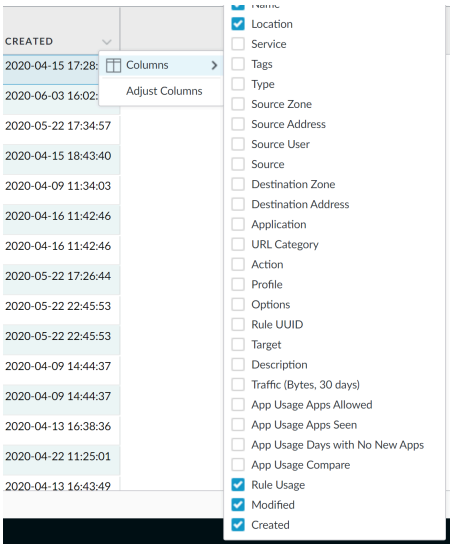
규칙 사용 필터를 사용하여 지정된 기간 내의 규칙 사용을 평가합니다. 예를 들어, 지난 *30*일 이내에 사용하지 않은 규칙에 대해 선택한 규칙 베이스를 필터링합니다. 작성된 날짜 및 수정한 날짜와 같은 다른 규칙 속성을 사용하여 규칙 사용을 평가할 수도 있습니다. 이를 통해 검토할 올바른 규칙 세트를 필터링할 수 있습니다. 이 데이터를 사용하여 규칙 수명 주기를 관리하고 네트워크 공격 면적을 줄이기 위해 규칙을 제거해야 하는지의 여부를 결정할 수 있습니다.

1. 필터링할 기간을 선택하거나 사용자 지정 기간을 지정합니다.
2. 필터링할 규칙 사용을 선택합니다.
3. (선택 사항) 규칙에 대한 규칙 사용 데이터를 재설정한 경우 지난 ***<number of days>***일 동안 재설정된 규칙 제외를 확인하고 규칙이 재설정된 이후 지정한 일수를 기준으로 규칙을 제외할 시기를 결정합니다. 지정된 일 수 전에 재설정된 규칙만 필터링된 결과에 포함됩니다.

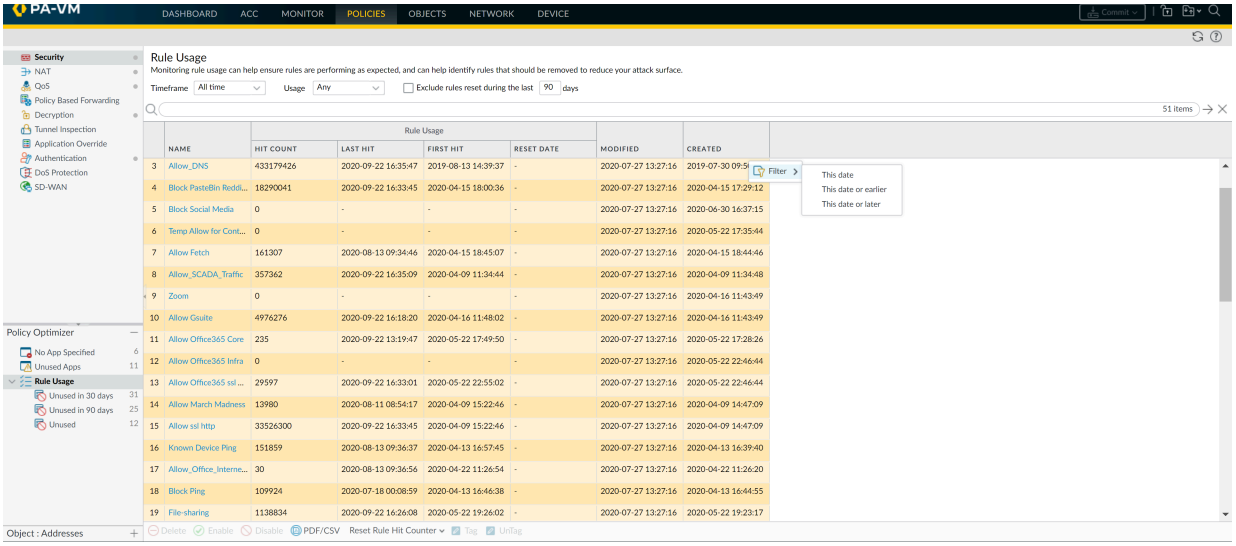



4. (선택 사항) 규칙 데이터를 기반으로 검색 필터 지정
   1. 열 머리글 및 열 위로 커서를 가져갑니다.
   2. 필터에 표시하거나 사용하려는 추가 열을 추가합니다.

 ©2023 Palo Alto Networks, Inc.




3. 필터에서 필터링할 열 데이터 위에 커서를 놓습니다. 날짜가 포함된 데이터의 경우 이 날짜, 이 날짜 이전 또는 이 날짜 이후를 사용하여 필터링할지의 여부를 선택합니다.
4. 필터(→)를 적용합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 하나 이상의 사용하지 않는 정책 규칙에 대해 조치를 취하십시오.

1. 사용하지 않는 정책 규칙을 하나 이상 선택하십시오.
2. 다음 작업 중 하나를 수행합니다.
   - 삭제 - 선택한 정책 규칙을 하나 이상 삭제합니다.
   - 활성화 - 비활성화된 경우 선택한 정책 규칙을 하나 이상 활성화합니다.
   - 비활성화 - 선택한 정책 규칙을 하나 이상 비활성화합니다.
   - 태그 - 하나 이상의 선택한 정책 규칙에 하나 이상의 그룹 태그를 적용합니다. 정책 규칙에 태그를 지정하려면 그룹 태그가 이미 존재해야 합니다.
   - 태그 해제 - 하나 이상의 선택한 정책 규칙에서 하나 이상의 그룹 태그를 제거합니다.
3. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 모니터링을 위해 외부 서비스 사용

외부 서비스를 사용하여 방화벽을 모니터링하면 중요한 이벤트에 대한 경고를 수신하고, 전용 장기 저장 소가 있는 시스템에 모니터링된 정보를 보관하고, 타사 보안 모니터링 도구와 통합할 수 있습니다. 다음은 외부 서비스를 사용하는 일반적인 몇 가지 시나리오입니다.

- 중요한 시스템 이벤트 또는 위협에 대한 즉각적인 알림을 받으려면 SNMP를 사용하여 통계 모니터링, SNMP 관리자로 트랩 포워딩 또는 전자 메일 경고 구성을 수행할 수 있습니다.
- 워크플로 또는 작업을 자동화하기 위해 API를 노출하는 타사 서비스에 HTTP 기반 API 요청을 직접 보냅니다. 예를 들어 외부 시스템에 의존하여 syslog 메시지 또는 SNMP 트랩을 HTTP 요청으로 변환하는 대신 정의된 기준과 일치하는 로그를 포워딩하여 ServiceNow에서 발생 티켓을 만들 수 있습니다. HTTP 요청의 URL, HTTP 헤더, 파라미터 및 페이로드를 수정하여 방화벽 로그의 속성을 기반으로 작업을 트리거할 수 있습니다. HTTP(S) 대상으로 로그 포워딩을 참조하십시오.
- 장기 로그 저장 및 중앙 집중식 방화벽 모니터링의 경우 로그 데이터를 syslog 서버로 보내도록 Syslog 모니터링을 구성할 수 있습니다. 이를 통해 Splunk 또는 ArcSight와 같은 타사 보안 모니터링 도구와 통합할 수 있습니다.
- 방화벽 인터페이스를 통과하는 IP 트래픽에 대한 통계를 모니터링하기 위해 NetFlow 내보내기를 구성하여 NetFlow 수집기에서 통계를 볼 수 있습니다.

방화벽에서 외부 서비스로 직접 또는 방화벽에서 Panorama로 로그 포워딩을 구성한 다음 서버에 로그를 포워딩하도록 Panorama를 구성할 수 있습니다. 로그를 포워딩할 위치를 결정할 때 고려해야 할 요소는 로그 포워딩 옵션을 참조하십시오.

*Panorama*에서는 *NetFlow* 레코드를 집계할 수 없으며 방화벽에서 *NetFlow* 수집기로 직접 전송해야 합니다.


©2023 Palo Alto Networks, Inc.

# 로그 포워딩 구성

여러 방화벽을 사용하여 네트워크 트래픽을 제어 및 분석하는 환경에서는 단일 방화벽이 모니터링하는 트래픽에 대한 로그와 보고서만 표시할 수 있습니다. 여러 방화벽에 로그인하면 모니터링이 번거로울 수 있으므로 모든 방화벽의 로그를 Panorama 또는 외부 서비스로 포워딩하여 네트워크 활동에 대한 전체적인 가시성을 보다 효율적으로 달성할 수 있습니다. 모니터링을 위해 외부 서비스 사용인 경우 방화벽은 로그를 syslog 메시지, SNMP 트랩, 이메일 알림과 같은 필요한 형식으로 자동 변환하거나 로그 세부정보를 HTTP(S) 서버로 보내기 위한 HTTP 페이로드로 변환합니다. 조직의 일부 팀이 작업과 관련된 로그만 모니터링하여 효율성을 높일 수 있는 경우 위협 유형 또는 원본 사용자와 같은 모든 로그 특성을 기반으로 포워딩 필터를 만들 수 있습니다. 예를 들어 맬웨어 공격을 조사하는 보안 운영 분석가는 유형 특성이 Wildfire 바이러스로 설정된 위협 로그에만 관심이 있을 수 있습니다.

방화벽에서 직접 외부 서비스로 또는 방화벽에서 ***Panorama***로 로그를 포워딩한 다음 로그를 서버로 포워딩하도록 Panorama를 구성할 수 있습니다. 로그를 포워딩할 위치를 결정할 때 고려해야 할 요소는 로그 포워딩 옵션을 참조하십시오.

CLI에서 SCP(보안 복사) 명령을 사용하여 전체 로그 데이터베이스를 ***SCP*** 서버로 내보내고 다른 방화벽으로 가져올 수 있습니다. 로그 데이터베이스가 너무 커서 내보내기 또는 가져오기가 ***PA-7000*** 시리즈 방화벽에서 실용적이지 못하기 때문에 이러한 옵션을 지원하지 않습니다. 또한 모든 플랫폼에서 웹 인터페이스를 보고서 보기 및 관리에 사용할 수 있지만 전체 로그 데이터베이스가 아닌 로그 유형별로만 사용할 수 있습니다.

**STEP 1 |** 로그 정보를 수신할 각 외부 서비스에 대한 서버 프로파일을 구성합니다.

별도의 프로파일을 사용하여 로그 속성별로 필터링된 여러 로그 집합을 다른 서버로 보낼 수 있습니다. 가용성을 높이려면 단일 프로파일에 여러 서버를 정의합니다.

다음 서버 프로파일 중 하나 이상을 구성합니다.

- (TLS를 통한 SMTP에 필요함) 아직 작성하지 않은 경우 전자 메일 서버에 대한 인증서 프로파일을 생성합니다.
- 2 SNMP 관리자(트랩 서버)가 방화벽 트랩을 해석할 수 있도록 하려면, Palo Alto Networks 지원되는 MIB을(를) SNMP 관리자에 로드하고 필요한 경우 컴파일해야 합니다. 자세한 내용은 SNMP 관리 소프트웨어 설명서를 참조하십시오.
- syslog 서버에 클라이언트 인증이 필요한 경우 5도 수행해야 합니다.
- HTTP 서버 프로파일을 구성합니다(HTTP/S 대상에 로그 포워딩 참조).

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 로그 포워딩 프로파일을 생성합니다.

프로파일은 트래픽, 위협, WildFire 제출, URL 필터링, 데이터 필터링, 터널 및 인증 로그의 대상을 정의합니다.

1. 개체 > 로그 포워딩 및 프로파일 추가를 선택합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.

   방화벽이 프로파일을 새 보안 규칙 및 영역에 자동으로 할당하도록 하려면 **default**를 입력합니다. 기본 프로파일을 원하지 않거나 기존 기본 프로파일을 재정의하려면 보안 규칙 및 영역에 프로파일을 할당할 때 프로파일을 식별하는 데 도움이 되는 이름을 입력합니다.

   > ***default***라는 로그 포워딩 프로파일이 없는 경우 새 보안 규칙(로그 포워딩 필드) 및 새 보안 영역 (로그 설정 필드)에서 프로파일 선택은 기본적으로 없음으로 설정됩니다. 단, 선택 사항을 변경할 수는 있습니다.

3. 하나 이상의 일치 목록 프로파일을 추가합니다.

   프로파일은 로그 쿼리 필터, 포워딩 대상 및 태깅과 같은 자동 작업을 지정합니다. 각 일치 리스트 프로파일에 대해 다음을 수행합니다.

   1. 프로파일을 식별하려면 이름을 입력합니다.
   2. 로그 유형을 선택합니다.
   3. 필터 드롭다운에서 필터 빌더를 선택합니다. 다음을 지정하고 각 쿼리를 추가합니다.
      - 커넥터 로직(및/또는)
      - 로그 속성
      - 포함 또는 제외 논리를 정의하는 연산자
      - 일치시킬 쿼리의 속성 값
   4. 로그를 로그 수집기 또는 **Panorama** 관리 서버로 포워딩하려면 Panorama를 선택합니다.
   5. 모니터링에 사용하는 각 외부 서비스 유형(SNMP, 전자 메일, Syslog 및 HTTP)에 대해 하나 이상의 서버 프로파일을 추가합니다.

4. (선택 사항, GlobalProtect만 해당) 보안 정책과 함께 로그 포워딩 프로파일을 사용하여 GlobalProtect를 사용하여 디바이스를 자동으로 격리하는 경우 기본 제공 작업 영역에서 검역소를 선택합니다.
5. 확인을 클릭하여 로그 포워딩 프로파일을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 정책 규칙 및 네트워크 영역에 로그 포워딩 프로파일을 할당합니다.

보안, 인증 및 DoS 보호 규칙은 로그 포워딩을 지원합니다. 이 예에서는 프로파일을 보안 규칙에 할당합니다.

로그 포워딩을 트리거할 각 규칙에 대해 다음 단계를 수행합니다.

1. 정책 > 보안을 선택한 다음 규칙을 편집합니다.
2. 작업을 선택한 다음 생성한 로그 포워딩 프로파일을 선택합니다.
3. 프로파일 유형을 프로파일 또는 그룹으로 설정한 다음 다음에 대해 로그 생성 및 포워딩을 트리거하는 데 필요한 보안 프로파일 또는 그룹 프로파일을 선택합니다.
   - 위협 로그 - 트래픽이 규칙에 할당된 모든 보안 프로파일과 일치해야 합니다.
   - 와일드파이어 제출 로그 - 트래픽이 규칙에 할당된 WildFire 분석 프로파일과 일치해야 합니다.
4. 트래픽 로그의 경우 세션 시작 시 로그 및/또는 세션 종료 시 로그를 선택합니다.
5. 규칙을 저장하려면 확인을 클릭합니다.

**STEP 4 |** 시스템, 구성, 상관 관계, 글로벌 보호, HIP 일치 및 사용자 ID 로그에 대한 대상을 구성합니다.

*Panorama*는 방화벽에서 상관 관계 로그를 집계하는 대신 수신한 방화벽 로그를 기반으로 상관 관계 로그를 생성합니다.

1. 디바이스 > 로그 설정을 선택합니다.
2. 방화벽이 포워딩할 각 로그 유형에 대해서는 단계 하나 이상의 일치 목록 프로파일 추가를 참조하십시오.

**STEP 5 |** (PA-7000 시리즈 방화벽에만 해당) 로그 포워딩을 수행하도록 로그 카드 인터페이스를 구성합니다.

*PAN-OS 10.1*부터는 더 이상 관리 인터페이스를 사용하거나 데이터 플레인 인터페이스를 통해 서비스 경로를 사용하여 시스템 로그를 전달할 수 없습니다. *PAN-OS 10.1* 이상을 실행하는 *PA-7000* 시리즈 방화벽에서 시스템 로그를 전달하는 유일한 방법은 *LFC(*로그 전달 카드*)*를 구성하는 것입니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 인터페이스 추가를 클릭합니다.
2. 슬롯 및 인터페이스 이름을 선택합니다.
3. 인터페이스 유형을 로그 카드로 설정합니다.
4. **IP** 주소, 기본 게이트웨이 및 (IPv4 전용) 넷마스크를 입력합니다.
5. 고급을 선택한 다음 링크 속도, 링크 이중 및 링크 상태를 지정합니다.

   이러한 필드는 기본적으로 ***auto***로 설정되어 있으며, 방화벽이 연결을 기반으로 값을 자동으로 결정하도록 지정합니다. 그러나 모든 연결에 권장되는 최소 링크 속도는 ***1000****(Mbps)* 입니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** (PA-5450 방화벽만 해당) 로그 전달을 수행하도록 로그 인터페이스를 구성합니다.

관리 인터페이스를 사용하여 로그를 *Panorama* 또는 *Cortex Data Lake*로 전달하는 경우에는 이 단계가 필요하지 않습니다. 관리 인터페이스는 기본적으로 로그 전달을 처리하며 로그 인터페이스를 구성할 필요가 없습니다.

- (PAN-OS 10.2.0 및 10.2.1) 로그 전달을 위해 특정 서비스 경로를 구성하지 않는 한 관리 인터페이스는 기본적으로 로그 전달을 처리합니다.
- (PAN-OS 10.2.2 이상 릴리스) 로그 전달을 위해 로그 인터페이스 또는 특정 서비스 경로를 구성하지 않는 한 관리 인터페이스는 기본적으로 로그 전달을 처리합니다. 로그 인터페이스가 구성되고 커밋되면 모든 내부 로깅, CDL, SNMP, HTTP 및 Syslog가 로그 인터페이스에 의해 전달됩니다.

*SNMP*, *HTTP* 및 *Syslog*와 같은 모든 서비스는 관리 또는 데이터 인터페이스를 통해 라우팅됩니다. 서비스에 대한 특정 서비스 경로를 지정하는 경우 해당 서비스 경로는 인터페이스를 통한 로그 전달에 대해 우선 순위가 지정됩니다.

구성 중인 로그 인터페이스가 관리 인터페이스와 동일한 서브네트워크에 있지 않은지 확인하십시오. 동일한 서브네트워크에서 두 인터페이스를 모두 구성하면 연결 문제가 발생하고 로그 전달에 잘못된 인터페이스가 사용될 수 있습니다.

로그 포트(*LOG-1* 및 *LOG-2*)는 기본적으로 *LAG*(링크 집계 그룹)로 번들됩니다. 두 포트를 모두 활용하려면 *LAG* 인식 스위치에 연결해야 합니다.

1. 디바이스 > 설정 > 관리를 선택합니다.
2. 로그 인터페이스의 상단 메뉴 표시줄에서 설정 기어를 선택합니다.
3. **IP** 주소, 넷마스크 및 기본 게이트웨이 필드를 입력합니다.

   네트워크에서 IPv6을 사용하는 경우 **IPv6** 주소 및 **IPv6** 기본 게이트웨이 필드를 대신 입력합니다.

   로그 인터페이스가 *IP* 주소로 구성되면 방화벽과 *Panorama* 간의 통신이 관리 인터페이스(기본값)에서 처리되는 것에서 로그 인터페이스로 자동 전환됩니다.
4. 링크 속도, 링크 이중화 및 링크 상태를 지정합니다.

   이러한 필드는 기본적으로 ***auto***로 설정되어 있으며, 방화벽이 연결을 기반으로 값을 자동으로 결정하도록 지정합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** 변경 사항을 커밋하고 확인합니다.

1. 변경 사항을 커밋합니다.
2. 구성한 로그 대상이 방화벽 로그를 수신하고 있는지 확인합니다.
   - Panorama - 방화벽이 Panorama 모드에서 Panorama 가상 장비나 M 시리즈 어플라이언스에 로그를 포워딩하는 경우 Panorama가 로그를 수신하기 전에 수집기 그룹을 구성해야 합니다. 그런 다음 로그 포워딩을 확인할 수 있습니다.
   - 이메일 서버 - 지정된 수신자가 로그를 이메일 알림으로 받고 있는지 확인합니다.
   - Syslog 서버 - 로그를 syslog 메시지로 수신하고 있는지 확인하려면 syslog 서버 설명서를 참조하십시오.
   - SNMP 관리자 - SNMP 관리자를 사용하여 MIB 및 개체 탐색 로그를 SNMP 트랩으로 수신하고 있는지 확인합니다.
   - HTTP 서버 - HTTP/S 대상에 로그 포워딩.


©2023 Palo Alto Networks, Inc.

# 이메일 경고 구성

시스템, 구성, HIP 일치, 상관 관계, 위협, WildFire 제출 및 트래픽 로그에 대한 이메일 경고를 구성할 수 있습니다. 별도의 프로파일을 사용하여 각 로그 유형에 대한 이메일 알림을 다른 서버로 보낼 수 있습니다. 가용성을 높이려면 단일 프로파일에 여러 서버(최대 4개)를 정의합니다.

가장 좋은 방법은 방화벽이 이메일을 서버로 릴레이하기 전에 방화벽이 이메일 서버를 인증하도록 ***TLS(***전송 레이어 보안***)***를 구성하는 것입니다**.** 이렇게 하면 스팸이나 맬웨어를 보내는 데 사용할 수 있는 ***SMTP(Simple Mail Transfer Protocol)*** 릴레이와 피싱 공격에 사용할 수 있는 이메일 스푸핑과 같은 악의적인 활동을 방지하는 데 도움이 됩니다**.**

**STEP 1 |** (TLS를 통한 SMTP에 필요함) 아직 작성하지 않은 경우 전자 메일 서버에 대한 인증서 프로파일을 생성합니다.

**STEP 2 |** 디바이스 > 서버 프로파일 > 이메일을 선택합니다.

**STEP 3 |** 이메일 서버 프로파일을 추가하고 이름을 입력합니다.

**STEP 4 |** 표시되는 읽기 전용 창에서 이메일 서버를 추가하고 이름을 입력합니다.

**STEP 5 |** 방화벽에 둘 이상의 가상 시스템(vsys)이 있는 경우 이 프로파일을 사용할 수 있는 위치(vsys 또는 **Shared**)를 선택합니다.

**STEP 6 |** (선택 사항) 이메일 표시 이름을 입력하여 이메일의 보낸 사람 필드에 표시할 이름을 지정합니다.

**STEP 7 |** 방화벽에서 이메일을 보내는 이메일 주소를 입력합니다.

**STEP 8 |** 방화벽에서 이메일을 보낼 이메일 주소를 입력합니다.

**STEP 9 |** (선택 사항) 두 번째 계정으로 이메일을 보내려면 추가 수신자의 주소를 입력합니다. 수신자는 한 명만 추가할 수 있습니다. 여러 수신자의 경우 메일 그룹의 이메일 주소를 추가합니다.

**STEP 10 |** 이메일을 보내는 데 사용할 **Email Gateway**의 IP 주소 또는 호스트 이름을 입력합니다.

**STEP 11 |** 이메일 서버에 연결하는 데 사용할 프로토콜 유형을 선택합니다.

- 인증되지 않은 **SMTP** - 인증 없이 이메일 서버에 연결하려면 SMTP를 사용합니다. 기본 포트는 25이지만 선택적으로 다른 포트를 지정할 수 있습니다. 이 프로토콜은 TLS를 통한 SMTP와 동일한 보안을 제공하지 않지만 이 프로토콜을 선택하는 경우 다음 단계를 건너뜁니다.
- **SMTP over TLS** -(권장) TLS를 사용하여 이메일 서버에 연결하기 위해 인증을 요구합니다. TLS 인증을 구성하려면 다음 단계를 계속하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 12 |** (SMTP over TLS만 해당) TLS 인증을 사용하여 이메일 서버에 연결하도록 방화벽을 구성합니다.

1. (선택 사항) 이메일 서버에 연결하는 데 사용할 포트를 지정합니다(기본값은 587).
2. **TLS** 버전 - TLS 버전(**1.1** 또는 **1.2**을 지정합니다.

   *Palo Alto Networks*는 최신 *TLS* 버전을 사용할 것을 강력히 권장합니다.
3. 방화벽 및 이메일 서버에 대한 인증 방법을 선택합니다.
   - 자동 - 방화벽과 이메일 서버가 인증 방법을 결정하도록 허용합니다.
   - 로그인 - 사용자 이름과 암호에 Base64 인코딩을 사용하고 별도로 전송합니다.
   - 일반 - 사용자명과 암호에 Base64 인코딩을 사용하고 함께 전송합니다.
4. 이메일 서버로 인증할 인증서 프로파일을 선택합니다.
5. 이메일을 보내는 계정의 사용자 이름과 암호를 입력한 다음 암호 확인을 입력합니다.
6. (선택 사항) 방화벽이 이메일 서버를 성공적으로 인증할 수 있는지 확인하려면 연결 테스트를 수행할 수 있습니다.

**STEP 13 |** 확인을 클릭하여 이메일 서버 프로파일을 저장합니다.

**STEP 14 |** (선택 사항) 사용자 지정 로그 형식 탭을 선택한 다음 전자 메일 메시지 형식을 사용자 지정합니다. 다양한 로그 유형에 대한 사용자 지정 형식을 만드는 방법에 대한 자세한 내용은 공통 이벤트 형식 구성 가이드를 참조하십시오.

**STEP 15 |** 트래픽, 위협 및 WildFire 제출 로그에 대한 이메일 경고를 구성합니다.

1. 로그 포워딩 프로파일 생성을 참조하십시오.
   1. 개체 > 로그 포워딩을 선택한 다음 추가를 클릭한 다음 프로파일을 식별할 이름을 입력합니다.
   2. 각 로그 유형 및 각 심각도 수준 또는 WildFire 판정에 대해 이메일 서버 프로파일을 선택한 다음 확인을 클릭합니다.
2. 정책 규칙 및 네트워크 영역에 로그 포워딩 프로파일 할당을 참조하십시오.

**STEP 16 |** 시스템, 구성, HIP 일치 및 상관 관계 로그에 대한 이메일 경고를 구성합니다.

1. 디바이스 > 로그 설정을 선택합니다.
2. 시스템 및 상관 관계 로그의 경우 각 심각도 수준을 클릭하고 이메일 서버 프로파일을 선택한 다음 확인을 클릭합니다.
3. 구성 및 HIP 일치 로그의 경우 섹션을 편집하고 이메일 서버 프로파일을 선택한 다음 확인을 클릭합니다.
4. 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 모니터링에 Syslog 사용

Syslog는 표준 로그 전송 메커니즘으로, 라우터, 방화벽, 프린터 등 다양한 네트워크 디바이스의 로그 데이터를 여러 공급자의 중앙 리포지토리로 취합하여 보관, 분석 및 보고할 수 있습니다. Palo Alto Networks 방화벽은 생성하는 모든 유형의 로그를 외부 syslog 서버로 포워딩할 수 있습니다. 안정적이고 안전한 로그 포워딩을 위해 TCP 또는 TLS(TLSv1.2만 해당)를 사용하고 비보안 포워딩에는 UDP를 사용할 수 있습니다.

- Syslog 모니터링 구성
- Syslog 필드 설명

## Syslog 모니터링 구성

Palo Alto Networks 방화벽을 모니터링하기 위해 Syslog를 사용하려면 Syslog 서버 프로파일을 생성하고 각 로그 유형에 대한 로그 설정에 할당합니다. 선택적으로 syslog 메시지에 사용되는 헤더 형식을 구성하고 TLSv1.2를 통해 syslog에 대한 클라이언트 인증을 활성화할 수 있습니다.

CEF 포맷 syslog 이벤트, 컬렉션의 경우 기본 ***syslog*** 구성을 편집해야 합니다. 기본 ***syslog*** 모니터링 구성은 ***CEF syslog*** 이벤트 콜렉션에 대해 지원되지 않습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** Syslog 서버 프로파일을 구성합니다.

별도의 프로파일을 사용하여 각 로그 유형에 대한 ***syslogs***를 다른 서버로 보낼 수 있습니다. 가용성을 높이려면 단일 프로파일에 여러 서버*(*최대 *4*개*)*를 정의합니다.

1. 디바이스 > 서버 프로파일 > **Syslog**를 선택합니다.
2. 추가를 클릭하고 프로파일 이름을 입력합니다.
3. 방화벽에 둘 이상의 가상 시스템(vsys)이 있는 경우 이 프로파일을 사용할 수 있는 위치(vsys 또는 **Shared**)를 선택합니다.
4. 각 syslog 서버에 대해 방화벽이 연결하는 데 필요한 정보 추가를 클릭하고 입력합니다.
   - 이름 - 서버 프로파일에 대한 고유 이름입니다.
   - **syslog** 서버-IP 주소 또는 syslog 서버의 완전 인증된 도메인 이름(FQDN).

     *FQDN*을 구성하고 ***UDP*** 전송을 사용하는 경우 방화벽이 *FQDN*을 해결할 수 없는 경우 방화벽은 *FQDN*의 기존 *IP* 주소 해결을 ***Syslog Server*** 주소로 사용합니다.
   - 전송 - **TCP**, **UDP**, 또는 **SSL(TLS)**을 syslog 서버와 통신하기 위한 프로토콜로 선택합니다. **SSL**의 경우 방화벽은 TLSv1.2에 한하여 지원합니다.
   - 포트 - syslog 메시지를 보낼 포트 번호(기본값은 포트 514의 UDP)이며 방화벽과 syslog 서버에서 동일한 포트 번호를 사용해야 합니다.
   - 형식 - 사용할 syslog 메시지 형식을 선택합니다. **BSD**(기본값) 또는 **IETF**. 전형적으로 **BSD** 형식은 UDP를 사용하고 **IETF** 형식은 TCP 또는 SSL/TLS를 사용합니다.
   - 시설 - syslog 표준 값(기본값은 **LOG_USER**)을 선택하여 syslog 서버 구현에서 우선 순위(PRI) 필드를 계산합니다. PRI 필드를 사용하여 syslog 메시지를 관리하는 방법에 매핑되는 값을 선택합니다.
5. (선택사항)방화벽이 보내는 syslog 메시지의 형식을 사용자 지정하려면 사용자 지정 로그 형식 탭을 선택합니다. 다양한 로그 유형에 대한 사용자 지정 형식을 만드는 방법에 대한 자세한 내용은 공통 이벤트 형식 구성 가이드를 참조하십시오.
6. 확인을 클릭하여 서버 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 트래픽, 위협 및 WildFire 제출 로그에 대한 syslog 포워딩을 구성합니다.

1. 로그를 전달하도록 방화벽을 구성합니다. 자세한 내용은 로그 포싱 프로파일 생성 단계를 참조하십시오.
   1. 개체 > 로그 포워딩을 선택한 다음 추가를 클릭한 다음 프로파일을 식별할 이름을 입력합니다.
   2. 각 로그 유형 및 각 심각도 수준 또는 WildFire 판정에 대해 **Syslog** 서버 프로파일을 선택한 다음 확인을 클릭합니다.
2. 로그 전달 프로파일을 보안 정책에 할당하여 로그 생성 및 전달을 트리거합니다. 자세한 내용은 정책 규칙 및 네트워크 영역에 로그 포싱 프로파일을 할당하는 단계를 참조하십시오.
   1. 정책 > 보안을 선택한 다음 정책 규칙을 선택합니다.
   2. 작업 탭을 선택한 다음 만든 로그 포워드 프로파일을 선택합니다.
   3. 프로파일 유형 드롭다운에서 프로파일 또는 그룹을 선택한 다음 로그 생성 및 포워딩을 트리거하는 데 필요한 보안 프로파일 또는 그룹 프로파일을 선택합니다.
   4. 트래픽 로그의 경우 세션 시작 시 로그 중 하나 또는 둘 다를 선택한 다음 세션 종료 체크박스에서의 로그 중 하나 또는 둘 다를 선택한 다음 확인을 클릭합니다.

   로그 포워딩 프로파일을 구성하고 프로파일을 정책 규칙에 할당하는 자세한 내용은 로그 포워딩 구성을(를) 참조하십시오.

**STEP 3 |** 시스템, Config, HIP 매치 및 상관 관계 로그에 대한 syslog 포워딩을 구성합니다.

1. 디바이스 > 로그 설정을 선택합니다.
2. 시스템 및 상관 관계 로그의 경우 각 심각도 수준을 클릭하고 **Syslog** 서버 프로파일을 선택한 다음 확인을 클릭합니다.
3. Config, HIP 일치 및 상관 관계 로그의 경우 섹션을 편집하고 **Syslog** 서버 프로파일을 선택한 다음 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) syslog 메시지의 헤더 형식을 구성합니다.

로그 데이터에는 로그를 생성한 방화벽의 고유 식별자가 포함됩니다. 헤더 형식을 선택하면 일부 SIEM(보안 정보 및 이벤트 관리) 서버의 로그 데이터를 필터링하고 보고할 수 있는 유연성이 향상됩니다.

이 설정은 전역 설정이며 방화벽에서 구성된 모든 Syslog 서버 프로파일에 적용됩니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.
2. 로그 내보내기 및 보고 탭을 선택한 다음 Syslog HOSTNAME 형식을 선택합니다.
   - **FQDN**(기본값)-송신 방화벽에 정의된 호스트 이름과 도메인 이름을 연결합니다.
   - **hostname** - 송신 방화벽에 정의된 호스트 이름을 사용합니다.
   - **ipv4** 주소 - 로그를 보내는 데 사용되는 방화벽 인터페이스의 IPv4 주소를 사용합니다. 기본적으로 이것은 MGT 인터페이스입니다.
   - **ipv6** 주소 - 로그를 보내는 데 사용되는 방화벽 인터페이스의 IPv6 주소를 사용합니다. 기본적으로 이것은 MGT 인터페이스입니다.
   - 없음 - 방화벽에서 호스트 이름 필드를 구성취소한 상태로 둡니다. 로그를 보낸 방화벽에 대한 식별자가 없습니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 5 |** TLSv1.2를 통해 syslog 통신을 보호하기 위해 인증서를 생성합니다.

syslog 서버가 클라이언트 인증을 사용하는 경우에만 필요합니다. syslog 서버는 인증서를 사용하여 방화벽이 syslog 서버와 통신할 수 있는 권한이 있는지 확인합니다.

다음 조건을 충족하는지 확인합니다.

- 개인 키는 전송 방화벽에서 사용할 수 있어야 합니다. 키는 HSM(하드웨어 보안 모듈)에 상주할 수 없습니다.
- 인증서의 제목과 발급자가 동일하지 않아야 합니다.
- syslog 서버와 송신 방화벽에는 동일한 신뢰할 수 있는 인증서 기관(CA)이 서명한 인증서가 있어야 합니다. 또는 방화벽에서 자체 서명된 인증서를 생성하고 방화벽에서 인증서를 내보내고 syslog 서버로 가져올 수 있습니다.
- TLS를 통해 Syslog 서버에 대한 연결은 온라인 인증서 상태 프로토콜(OCSP)을 사용하거나 신뢰 체인의 각 인증서가 이러한 확장 중 하나 또는 둘 다를 지정하는 한 CRL(인증서 해지 목록)을 사용하

 ©2023 Palo Alto Networks, Inc.

여 유효성을 검사합니다. 그러나 OCSP 또는 CRL 오류를 우회할 수 없으므로 인증서 체인이 유효한지 확인하고 OCSP 또는 CRL을 사용하여 각 인증서를 확인할 수 있어야 합니다.

1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 생성을 클릭합니다.
2. 인증서 이름을 입력합니다.
3. 공통 이름 필드에 는 방화벽의 IP 주소를 입력하여 syslog 서버에 로그를 보내는 것입니다.
4. 서명자에서 syslog 서버와 송신 방화벽이 모두 신뢰하는 신뢰할 수 있는 CA 또는 자체 서명된 CA를 선택합니다.

   인증서는 인증서 기관이나 외부 기관(인증서 서명 요청[CSR])이 될 수 없습니다.
5. 생성을 클릭합니다. 방화벽은 인증서와 키 쌍을 생성합니다.
6. 인증서 이름을 클릭하여 편집하고 보안 **Syslog** 체크박스 인증서를 선택한 다음 확인을 클릭합니다.

**STEP 6 |** 변경 내용을 커밋하고 syslog 서버의 로그를 검토합니다.

1. 커밋을 클릭합니다.
2. 로그를 검토하려면 syslog 관리 소프트웨어 설명서를 참조하십시오. Syslog 필드 설명을 검토할 수도 있습니다.

**STEP 7 |** (선택 사항) FQDN 새로 고침 시 syslog 서버에 대한 연결을 종료하도록 방화벽을 구성합니다.

FQDN을 사용하여 syslog 서버 프로파일을 구성할 때 방화벽은 FQDN 이름이 변경될 경우 기본적으로 syslog 서버에 대한 연결을 유지합니다.

예를 들어 기존 syslog 서버를 다른 FQDN 이름을 사용하는 새 syslog 서버로 대체했습니다. 방화벽이 새 FQDN 이름을 사용하여 새 syslog 서버에 연결하려면 방화벽을 구성하여 이전 syslog 서버에 대한 연결을 자동으로 종료하고 새 FQDN 이름을 사용하여 새 syslog 서버에 대한 연결을 설정할 수 있습니다.

1. 방화벽 CLI에 로그인합니다.
2. FQDN 새로 고침 시 syslog 서버에 대한 연결을 종료하도록 방화벽을 구성합니다.

```
admin> set syslogng fqdn-refresh yes
```

## Syslog 필드 설명

다음 항목에는 Palo Alto Networks 방화벽이 외부 서버로 포워딩할 수 있는 각 로그 유형의 표준 필드와 심각도 수준, 사용자 지정 형식 및 이스케이프 시퀀스가 나열됩니다. 구문 분석을 용이하게 하기 위해 구분 기호는 쉼표입니다. 각 필드는 쉼표로 구분된 값(CSV) 문자열입니다. FUTURE_USE 태그는 방화벽이 현재 구현하지 않는 필드에 적용됩니다.

*WildFire* 제출 기록 은 위협 로그의 하위 유형이며 동일한 *syslog* 형식을 사용합니다.

- 트래픽 로그 필드
- 위협 로그 필드
- URL 필터링 로그 필드


©2023 Palo Alto Networks, Inc.

- 데이터 필터링 로그 필드
- HIP 매치 로그 필드
- GlobalProtect 로그 필드
- IP 태그 로그 필드
- 사용자 ID 로그 필드
- 복호화 로그 필드
- 터널 검사 로그 필드
- SCTP 로그 필드
- 구성 로그 필드
- 인증 로그 필드
- 시스템 로그 필드
- 상관 이벤트 로그 필드
- GTP 로그 필드
- 사용자 정의 로그/이벤트 형식
- 이스케이프 시퀀스(Escape Sequences)


## 트래픽 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성된 시간, 소스 주소, 대상 주소, NAT 소스 IP, NAT 대상 IP, 규칙 이름, 소스 사용자, 대상 사용자, 애플리케이션, 가상 시스템, 소스 영역 , 대상 영역, 인바운드 인터페이스, 아웃바운드 인터페이스, 로그 작업, FUTURE_USE, 세션 ID, 반복 횟수, 소스 포트, 대상 포트, NAT 소스 포트, NAT 대상 포트, 플래그, 프로토콜, 작업, 바이트, 보낸 바이트, 받은 바이트, 패킷 , 시작 시간, 경과 시간, 카테고리, FUTURE_USE, 시퀀스 번호, 작업 플래그, 소스 국가, 대상 국가, FUTURE_USE, 보낸 패킷, 수신된 패킷, 세션 종료 이유, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 레벨 3, 디바이스 그룹 레이어 구조 레벨 4, 가상 시스템 이름, 디바이스 이름, 작업 소스, 소스 VM UUID, 대상 VM UUID, 터널 ID/IMSI, 모니터 태그/IMEI, 상위 세션 ID, 상위 시작 시간, 터널 유형, SCTP 연결 아이디, SC TP 청크, SCTP 청크 전송, SCTP 청크 수신, 규칙 UUID, HTTP/2 연결, 앱 플랩 수, 정책 ID, 링크 스위치, SD-WAN 클러스터, SD-WAN 디바이스 유형, SD-WAN 클러스터 유형, SD-WAN 사이트 , 동적 사용자 그룹 이름, XFF 주소, 소스 디바이스 카테고리, 소스 디바이스 프로파일, 소스 디바이스 모델, 소스 디바이스 공급자, 소스 디바이스 OS 제품군, 소스 디바이스 OS 버전, 소스 호스트 이름, 소스 Mac 주소, 대상 디바이스 카테고리, 대상 디바이스 프로파일, 대상 디바이스 모델, 대상 디바이스 공급자, 대상 디바이스 OS 제품군, 대상 디바이스 OS 버전, 대상 호스트 이름, 대상 Mac 주소, 컨테이너 ID, POD 네임스페이스, POD 이름, 소스 외부 동적 목록, 대상 외부 동적 목록, 호스트 ID, 일련번호, 소스 동적 주소 그룹, 대상 동적 주소 그룹, 세션 소유자, 고해상도 타임스탬프, 슬라이스 서비스 유형, 슬라이스 구분자, 애플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 앱 라이선스 특성, 애플리케이션 컨테이너, 터널링된 애플리케이션, 애플리케이션 SaaS, 애플리케이션 승인 상태, 오프로드

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |

 ©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 TRAFFIC입니다. |
| 위협/콘텐츠 유형(subtype) | 트래픽 로그의 하위 유형 값은 시작, 종료, 삭제 및 거부입니다.<br>• 시작 - 세션 시작됨<br>• 종료 - 세션이 종료됨<br>• 삭제 - 애플리케이션이 식별되기 전에 삭제된 세션이며 세션을 허용하는 규칙이 없습니다.<br>• 거부 - 애플리케이션이 식별된 후 세션이 삭제되고 차단 규칙이 있거나 세션을 허용하는 규칙이 없습니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 원래 세션 소스 IP 주소입니다. |
| 대상 주소(dst) | 원래 세션 대상 IP 주소입니다. |
| NAT 소스 IP(natsrc) | 소스 NAT가 수행된 경우 사후 NAT 소스 IP 주소입니다. |
| NAT 데스티네이션 IP(natdst) | 대상 NAT가 수행된 경우 사후 NAT 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션이 일치한 규칙의 이름입니다. |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 대상 사용자(dstuser) | 세션이 대상으로 지정된 사용자의 사용자 이름입니다. |
| 애플리케이션(app) | 세션과 연결된 애플리케이션입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션이 소싱된 영역입니다. |
| 대상 영역(to) | 세션이 예정된 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |
| 세션 ID(sessionid) | 각 세션에 적용되는 내부 숫자 식별자입니다. |
| 반복 수(반복) | 동일한 소스 IP, 대상 IP, 애플리케이션 및 하위 유형이 있는 세션 수는 5초 이내에 표시됩니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| NAT 소스 포트(natsport) | Post-NAT 소스 포트입니다. |
| NAT 대상 포트(natdport) | NAT 이후 대상 포트입니다. |
| 플래그(flags) | 세션에 대한 세부 정보를 제공하는 32비트 필드입니다. 이 필드는 로깅된 값으로 값을 AND 지정하여 디코딩할 수 있습니다.<br>• 0x80000000 - 세션에 패킷 캡처(PCAP)가 있습니다.<br>• 0x40000000 - 클라이언트가 여러 경로를 사용하여 대상 호스트에 연결할 수 있도록 하는 옵션이 활성화됩니다.<br>• 0x20000000 - WildFire 공용 또는 사설 클라우드 채널을 사용하여 분석을 위해 샘플을 제출했는지 여부를 나타냅니다.<br>• 0x10000000 - 최종 사용자에 의한 엔터프라이즈 자격 증명 제출이 감지됨<br>• 0x08000000 - 흐름의 소스가 허용 목록에 있으며 정찰 보호 대상이 아닙니다.<br>• 0x02000000 - IPv6 session<br>• 0x01000000 - SSL 세션의 암호가 복호화됩니다(SSL 프록시).<br>• 0x00800000 - URL 필터링을 통해 세션이 거부되었습니다.<br>• 0x00400000 - 세션에 NAT 변환이 수행되었습니다.<br>• 0x00200000 - 세션에 대한 사용자 정보가 인증 포털을 통해 캡처되었습니다.<br>• 0x00100000 - 애플리케이션 트래픽이 비표준 대상 포트에 있습니다.<br>• 0x00080000 - X-포워딩됨-프록시의 값이 소스 사용자 필드에 있음<br>• 0x00040000 - 로그는 http 프록시 세션 내의 트랜잭션에 해당합니다(프록시 트랜잭션). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 0x00020000 - 클라이언트-서버 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00010000 - 서버 대 클라이언트 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00008000 - 세션이 컨테이너 페이지 액세스임(컨테이너 페이지)<br>• 0x00002000 - 세션이 암시적 애플리케이션 종속성 처리에 대한 규칙과 일시적으로 일치합니다. PAN-OS 5.0.0 이상에서 사용할 수 있습니다.<br>• 0x00000800 - 대칭 반환은 이 세션의 트래픽을 포워딩하는 데 사용됩니다.<br>• 0x00000400 - 복호화된 트래픽이 미러 포트를 통해 일반 텍스트로 전송되고 있습니다.<br>• 0x00000100 - 외부 터널의 탑재량을 검사하는 중입니다. |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 가능한 값은 다음과 같습니다.<br>• allow - 정책에 의해 세션이 허용됨<br>• deny - 정책에 의해 세션이 거부되었습니다.<br>• drop - 세션이 자동으로 삭제되었습니다.<br>• drop ICMP - 호스트 또는 애플리케이션에 ICMP 연결할 수 없는 메시지와 함께 세션이 자동으로 삭제되었습니다.<br>• reset both - 세션이 종료되고 TCP 재설정이 연결의 양쪽으로 전송됩니다.<br>• 클라이언트 재설정 - 세션이 종료되고 TCP 재설정이 클라이언트로 전송되었습니다.<br>• 서버 재설정 - 세션이 종료되고 TCP 재설정이 서버로 전송되었습니다. |
| 바이트(bytes) | 세션의 총 바이트 수(전송 및 수신). |
| 보낸 바이트(bytes_sent) | 세션의 클라이언트에서 서버로의 바이트 수입니다. |
| 수신된 바이트(bytes_received) | 세션의 서버-클라이언트 방향의 바이트 수입니다. |
| 패킷(packets) | 세션의 총 패킷 수(전송 및 수신). |
| 시작 시간(시작) | 세션 시작 시간입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 경과 시간(경과) | 세션의 경과 시간입니다. |
| 카테고리(category) | 세션과 연결된 URL 카테고리(해당되는 경우). |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 소스 국가(srcloc) | 개인 주소의 출처 국가 또는 내부 지역 최대 길이는 32바이트입니다. |
| 대상 국가(dstloc) | 개인 주소의 경우 대상 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 보낸 패킷(pkts_sent) | 세션에 대한 클라이언트-서버 패킷 수입니다. |
| 수신된 패킷(pkts_received) | 세션에 대한 서버-클라이언트 패킷 수입니다. |
| 세션 종료 이유(session_end_reason) | 세션이 종료된 이유입니다. 종료 원인이 여러 개인 경우 이 필드에는 가장 높은 우선 순위 이유만 표시됩니다. 가능한 세션 종료 이유 값은 우선 순위(첫 번째가 가장 높음)에 따라 다음과 같습니다.<br>• 위협 - 방화벽이 재설정, 삭제 또는 차단(IP 주소) 작업과 관련된 위협을 감지했습니다.<br>• policy-deny - 세션이 거부 또는 삭제 작업이 있는 보안 규칙과 일치했습니다.<br>• 세션이 클라이언트 인증을 사용하거나 세션이 만료됨, 신뢰할 수 없는 발급자, 알 수 없는 상태 또는 상태 확인 타임아웃 중 하나에 해당하는 서버 인증서를 사용할 때 SSL 포워드 프록시 복호화 또는 SSL 인바운드 검사를 차단하도록 방화벽을 구성했기 때문에 세션이 종료되었습니다. 이 세션 종료 이유는 서버 인증서가 bad_certificate, unsupported_certificate, certificate_revoked, access_denied 또는 no_certificate_RESERVED(SSLv3만 해당) 유형의 치명적인 오류 경고를 생성할 때도 표시됩니다.<br>• Decrypt-unsupport-param - 세션이 지원되지 않는 프로토콜 버전, 암호 또는 SSH 알고리즘을 사용할 때 SSL 포워드 프록시 복호화 또는 SSL 인바운드 검사를 차단하도록 방화벽을 구성했기 때문에 세션이 종료되었습니다. 이 세션 종료 이유는 세션이 unsupported_extension, expected_message 또는 handshake_failure 유형의 치명적인 오류 경고를 생성할 때 표시됩니다.<br>• 복호화 오류 - 방화벽 리소스 또는 하드웨어 보안 모듈(HSM)을 사용할 수 없을 때 SSL 포워드 프록시 복호화 또는 SSL 인바운드 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | 검사를 차단하도록 방화벽을 구성했기 때문에 세션이 종료되었습니다. 이 세션 종료 이유는 또한 SSL 오류가 있는 SSL 트래픽을 차단하도록 방화벽을 구성했거나 Decrypt-cert-validation 및 Decrypt-unsupport-param 종료 이유에 대해 나열된 것 이외의 치명적인 오류 경고를 생성한 경우에도 표시됩니다.<br>• tcp-rst-from-client - 클라이언트가 서버에 TCP 재설정을 보냈습니다.<br>• tcp-rst-from-server - 서버가 클라이언트에 TCP 재설정을 보냈습니다.<br>• resources-unavailable - 시스템 리소스 제한으로 인해 세션이 삭제되었습니다. 예를 들어, 세션이 흐름당 허용되는 비순차 패킷 수 또는 글로벌 비순차 패킷 대기열을 초과했을 수 있습니다.<br>• tcp-fin - 연결에 있는 두 호스트 모두 세션을 닫기 위해 TCP FIN 메시지를 보냈습니다. |
| | • tcp-reuse - 세션이 재사용되고 방화벽이 이전 세션을 닫습니다.<br>• decoder - 디코더는 프로토콜 내에서 새로운 연결(예: HTTP-Proxy)을 감지하고 이전 연결을 종료합니다.<br>• old-out - 세션이 만료되었습니다.<br>• unknown - 이 값은 다음 상황에 적용됩니다.<br>  • 앞의 이유가 다루지 않는 세션 종료(예: **clear session all** 명령).<br>  • 세션 최종 이유 필드(PAN-OS 6.1보다 오래된 릴리스)를 지원하지 않는 PAN-OS 릴리스에서 생성된 로그의 경우 현재 PAN-OS 릴리스로 업그레이드한 후 또는 로그를 방화벽에 로드한 후 값을 **알 수 없습니다**.<br>  • Panorama에서 PAN-OS 버전이 세션 종료 이유를 지원하지 않는 방화벽에서 받은 로그는 **알 수 없는** 값을 갖습니다.<br>• 해당 없음 - 이 값은 트래픽 로그 유형이 **끝나지** 않을 때 적용됩니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 작업 소스(action_source) | 애플리케이션을 허용하거나 차단하기 위해 취한 조치가 애플리케이션 또는 정책에 정의되었는지의 여부를 지정합니다. 작업은 세션에 대한 허용, 거부, 삭제, 서버 재설정, 클라이언트 재설정 또는 둘 다 재설정이 될 수 있습니다. |
| 소스 VM UUID(src_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 소스 범용 고유 식별자를 식별합니다. |
| 대상 VM UUID(dst_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 대상 범용 고유 식별자를 식별합니다. |
| 터널 ID/IMSI(tunnelid/imsi) | IMSI(International Mobile Subscriber Identity)는 GSM/UMTS/EPS 시스템에서 각 모바일 가입자에게 할당되는 고유 번호입니다. IMSI는 10진수(0~9)로만 구성되며 허용되는 최대 자릿수는 15입니다. |
| 모니터 태그/IMEI(모니터 태그/imei) | IMEI(International Mobile Equipment Identity)는 각 이동국 장비에 할당된 고유한 15자리 또는 16자리 숫자입니다. |
| 부모 요소 세션 ID(parent_session_id) | 이 세션이 터널링되는 세션의 ID입니다. 내부 터널(두 수준의 터널링인 경우) 또는 내부 내용(한 수준의 터널링인 경우)에만 적용됩니다. |
| 부모 요소 시작 시간(parent_start_time) | 년/월/일 시간:분:초, 부모 요소 터널 세션이 시작된 시입니다. |
| 터널 유형(tunnel) | GRE 또는 IPsec과 같은 터널 유형입니다. |
| SCTP 연결 ID(assoc_id) | 두 SCTP 엔드포인트 간의 연결에 대한 모든 연결을 식별하는 번호입니다. |
| SCTP 청크(chunks) | 연결을 위해 보내고 받은 SCTP 청크의 합계입니다. |
| SCTP 청크 전송(chunks_sent) | 연결을 위해 보낸 SCTP 청크 수입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| SCTP 청크 수신(chunks_received) | 연결에 대해 수신된 SCTP 청크 수입니다. |
| 규칙 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| HTTP/2 연결(http2_connection) | 다음 값 중 하나를 표시하여 트래픽이 HTTP/2 연결을 사용했는지 식별합니다.<br>• 상위 세션 ID - HTTP/2 연결<br>• 0 - SSL 세션 |
| 앱 플랩 수(link_change_count) | 세션 중에 발생한 링크 플랩의 수입니다. |
| 정책 ID(policy_id) | SD-WAN 정책의 이름입니다. |
| 링크 스위치(link_switches) | 최대 4개의 링크 플랩 항목을 포함하며 각 항목에는 링크 이름, 링크 태그, 링크 유형, 물리적 인터페이스, 타임스탬프, 읽은 바이트, 입력한 바이트, 링크 상태 및 링크 플랩 원인이 포함됩니다. |
| SD-WAN 클러스터(sdwan_cluster) | SD-WAN 클러스터의 이름입니다. |
| SD-WAN 디바이스 유형(sdwan_device_type) | 디바이스 유형(**허브** 또는 **분기**). |
| SD-WAN 클러스터 유형(sdwan_cluster_type) | 클러스터 유형(**메시** 또는 **허브 스포크**). |
| SD-WAN 사이트(sdwan_site) | SD-WAN 사이트의 이름입니다. |
| 동적 사용자 그룹 이름(dynusergroup_name) | 세션을 시작한 사용자가 포함된 동적 사용자 그룹의 이름입니다. |
| XFF 주소(xff_ip) | 웹 페이지를 요청한 사용자의 IP 주소 또는 요청이 통과한 마지막 디바이스 옆에 있는 IP 주소입니다. 요청이 하나 이상의 프록시, 로드 밸런서 또는 기타 업스트림 디바이스를 통과하는 경우 방화벽은 최신 디바이스의 IP 주소를 표시합니다. |
| 소스 디바이스 카테고리(src_category) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 카테고리입니다. |
| 소스 디바이스 프로파일(src_profile) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 디바이스 프로파일입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 소스 디바이스 모델(src_model) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 모델입니다. |
| 소스 디바이스 공급업체(src_vendor) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 공급업체입니다. |
| 소스 디바이스 OS 패밀리(src_osfamily) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 유형입니다. |
| 소스 디바이스 OS 버전(src_osversion) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 버전입니다. |
| 소스 호스트 이름 (src_host) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 호스트 이름입니다. |
| 소스 MAC 주소(src_mac) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 MAC 주소입니다. |
| 대상 디바이스 카테고리(dst_category) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 카테고리입니다. |
| 대상 디바이스 프로파일(dst_profile) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 대상 디바이스 모델(dst_model) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 모델입니다. |
| 대상 디바이스 공급업체(dst_vendor) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 벤더입니다. |
| 대상 디바이스 OS 제품군(dst_osfamily) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 유형입니다. |
| 대상 디바이스 OS 버전(dst_osversion) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 버전입니다. |
| 대상 호스트 이름(dst_host) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 호스트 이름입니다. |
| 대상 MAC 주소(dst_mac) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 MAC 주소입니다. |
| 컨테이너 ID(container_id) | 애플리케이션 POD가 배포된 쿠버네티스 노드에 있는 PAN-NGFW POD의 컨테이너 ID. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| POD 네임스페이스(pod_namespace) | 보안이 설정되는 애플리케이션 POD의 네임스페이스입니다. |
| 포드 이름(pod_name) | 보안이 유지되는 애플리케이션 POD입니다. |
| 소스 외부 동적 목록(src_edl) | 트래픽의 원본 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 대상 외부 동적 목록(dst_edl) | 트래픽의 대상 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 호스트 ID(hostid) | 고유 ID GlobalProtect는 호스트를 식별하기 위해 할당합니다. |
| 사용자 디바이스 일련번호(serialnumber) | 사용자의 컴퓨터 또는 디바이스의 일련번호입니다. |
| 원본 동적 주소 그룹(src_dag) | 원래 세션 소스 동적 주소 그룹입니다. |
| 대상 동적 주소 그룹(dst_dag) | 원래 대상 소스 동적 주소 그룹입니다. |
| 세션 소유자(session_owner) | HA 페일오버 시 세션 테이블 데이터가 동기화된 HA 클러스터의 원래 고가용성(HA) 피어 세션 소유자입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 슬라이스 서비스 유형(nsdsai_sst) | 네트워크 슬라이스 ID의 A 슬라이스 서비스 유형입니다. |
| 슬라이스 구분자(nsdsai_sd) | 네트워크 슬라이스 ID의 슬라이스 구분자입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |
| 애플리케이션 카테고리(category_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking<br>• saas |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 터널링된 응용 프로그램(tunneled_app) | 터널링된 응용 프로그램의 이름입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 **1**을 표시하고 SaaS 애플리케이션이 아닌 경우 **0**을 표시합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 애플리케이션이 승인되면 **1**을 표시하고 애플리케이션이 승인되지 않은 경우 **0**을 표시합니다. |
| 오프로드(offloaded) | 트래픽 흐름이 오프로드된 경우 **1**을 표시하고 트래픽 흐름이 오프로드되지 않은 경우 **0**를 표시합니다. |

## 위협 로그 필드

형식: FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성 시간, 소스 주소, 대상 주소, NAT 소스 IP, NAT 대상 IP, 규칙 이름, 소스 사용자, 대상 사용자, 애플리케이션, 가상 시스템, 소스 영역, 대상 영역, 인바운드 인터페이스, 아웃바운드 인터페이스, 로그작업, FUTURE_USE, 세션 ID, 반복 횟수, 소스 포트, 대상 포트, NAT 소스 포트, NAT 대상 포트, 플래그, IP 프로토콜, 작업, URL/파일 이름, 위협 ID, 카테고리, 심각도, 방향, 시퀀스 번호, 작업 플래그, 소스 위치, 대상 위치, FUTURE_USE, 콘텐츠 유형, PCAP_ID, 파일다이제스트, 클라우드, URL 인덱스, 사용자 에이전트, 파일 유형, X 포워딩 대상, 참조자, 발신자, 제목, 수신자, 보고서 ID, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 수준 3, 디바이스 그룹 레이어 수준 4, 가상 시스템 이름, 디바이스 이름, FUTURE_USE, 소스 VM UUID,대상 VM UUID, HTTP 메서드, 터널 ID/IMSI, 모니터 태그/IMEI, 상위 세션 ID, 상위 세션 ID, 상위 시작 시간, 터널 유형, 위협 카테고리, 콘텐츠 버전, FUTURE_USE, SCTP 연결 ID, 페이로드 프로토콜 ID, HTTP 헤더, URL 카테고리 목록, 규칙 UUID, HTTP/2 연결, 동적 사용자 그룹 이름, XFF 주소, 소스디바이스 카테고리, 소스 디바이스 프로파일, 소스 디바이스 모델, 소스 디바이스 공급자, 소스 디바이스 OS 제품군, 소스 디바이스 OS 버전, 소스 호스트 이름, 소스 MAC 주소, 대상 디바이스 카테고리, 대상 디바이스 프로파일, 대상 디바이스 모델, 대상 디바이스 공급자, 대상 디바이스 OS 제품군,대상 디바이스 OS 버전, 대상 호스트 이름, 대상 MAC 주소, 컨테이너 ID, POD 네임스페이스, POD 이름, 소스 외부 동적 목록, 대상 외부 동적 목록, 호스트 ID, 일련번호, 도메인 EDL, 소스 동적 주소 그룹, 대상 동적 주소 그룹, 부분 해시,고해상도 타임스탬프, 이유, 근거, 슬라이스 서비스 유형, 애플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 애플리케이션 특성, 애플리케이션 컨테이너, 애플리케이션 SaaS, 애플리케이션 승인 상태

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial #) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 THEAT 입니다. |
| 위협/콘텐츠 유형(subtype) | 위협 로그의 하위 유형입니다. 값에는 다음이 포함됩니다.<br>• 데이터 - 데이터 필터링 프로파일과 일치하는 데이터 패턴입니다.<br>• 파일 - 파일 차단 프로파일과 일치하는 파일 형식입니다.<br>• 플러드 - 영역 보호 프로파일을 통해 탐지된 플러드. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 패킷 - 영역 보호 프로파일에 의해 트리거되는 패킷 기반 공격 보호입니다.<br>• 검사 - 영역 보호 프로파일을 통해 검색된 검사입니다.<br>• 스파이웨어 - 안티 스파이웨어 프로파일을 통해 탐지된 스파이웨어입니다.<br>• url - URL 필터링 로그.<br>• ML-바이러스 - 바이러스 백신 프로파일을 통해 WildFire 인라인 ML에 의해 탐지된 바이러스입니다.<br>• 바이러스 - 바이러스 백신 프로파일을 통해 탐지된 바이러스입니다.<br>• 취약점 - 취약점 보호 프로파일을 통해 탐지된 취약점 악용입니다.<br>• WildFire - 방화벽이 WildFire 분석 프로파일에 따라 WildFire에 파일을 제출할 때 생성되는 WildFire 판정이며, 판정(로깅 중인 내용에 따라 멀웨어, 피싱, 그레이웨어 또는 악성)이 WildFire 제출 로그에 기록됩니다.<br>• verdict-virus - 바이러스 백신 프로파일을 통해 탐지된 바이러스입니다. |
| 시간 생성(time_generated 또는 cef-formatted-time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 원래 세션 소스 IP 주소입니다. |
| 대상 주소(dst) | 원래 세션 대상 IP 주소입니다. |
| NAT 소스 IP(natsrc) | 소스 NAT가 수행된 경우 NAT 이후 소스 IP 주소입니다. |
| NAT 데스티네이션 IP(natdst) | 대상 NAT가 수행된 경우 사후 NAT 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션이 일치한 규칙의 이름입니다. |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 대상 사용자(dstuser) | 세션이 대상으로 지정된 사용자의 사용자 이름입니다. |
| 애플리케이션(app) | 세션과 연결된 애플리케이션입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션이 소싱된 영역입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 대상 영역(to) | 세션이 예정된 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |
| 세션 ID(sessionid) | 각 세션에 적용되는 내부 숫자 식별자입니다. |
| 반복 수(반복) | 소스 IP, 대상 IP, 애플리케이션 및 콘텐츠/위협 유형이 5초 내에 동일한 세션 수입니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| NAT 소스 포트(natsport) | Post-NAT 소스 포트입니다. |
| NAT 대상 포트(natdport) | NAT 이후 대상 포트입니다. |
| 플래그(flags) | 세션에 대한 세부 정보를 제공하는 32비트 필드입니다. 이 필드는 로깅된 값으로 값을 AND 지정하여 디코딩할 수 있습니다.<br>• 0x80000000 - 세션에 패킷 캡처(PCAP)가 있습니다.<br>• 0x40000000 - 클라이언트가 여러 경로를 사용하여 대상 호스트에 연결할 수 있도록 하는 옵션이 활성화됩니다.<br>• 0x20000000 - 판단을 위해 파일이 와일드파이어에 제출됨<br>• 0x10000000 - 최종 사용자에 의한 엔터프라이즈 자격 증명 제출이 감지됨<br>• 0x08000000 - 흐름에 대한 소스가 허용 목록에 있으며 정찰 보호 대상이 아닙니다.<br>• 0x02000000 - IPv6 session<br>• 0x01000000 - SSL 세션의 암호가 복호화됩니다(SSL 프록시).<br>• 0x00800000 - URL 필터링을 통해 세션이 거부되었습니다.<br>• 0x00400000 - 세션에 NAT 변환이 수행되었습니다.<br>• 0x00200000 - 세션에 대한 사용자 정보가 인증 포털을 통해 캡처되었습니다.<br>• 0x00100000 - 애플리케이션 트래픽이 비표준 대상 포트에 있습니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 0x00080000 - X-포워딩됨-프록시의 값이 소스 사용자 필드에 있음<br>• 0x00040000 - log는 http 프록시 세션 내의 트랜잭션에 해당합니다(프록시 트랜잭션).<br>• 0x00020000 - 클라이언트-서버 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00010000 - 서버 대 클라이언트 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00008000 - 세션이 컨테이너 페이지 액세스입니다(컨테이너 페이지).<br>• 0x00002000 - 세션이 암시적 애플리케이션 종속성 처리에 대한 규칙과 일시적으로 일치합니다. PAN-OS 5.0.0 이상에서 사용할 수 있습니다.<br>• 0x00000800 - 대칭 반환은 이 세션의 트래픽을 포워딩하는 데 사용됩니다.<br>• 0x00000400 - 복호화된 트래픽이 미러 포트를 통해 일반 텍스트로 전송되고 있습니다.<br>• 0x00000010 - 외부 터널의 탑재량을 검사하는 중입니다. |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 값은 경고, 허용, 거부, 삭제, 전체 패킷 드롭, 클라이언트 재설정, 서버 재설정, 모두 재설정, 블록 URL입니다.<br>• alert - 위협 또는 URL이 감지되었지만 차단되지 않음<br>• allow - 플러드 감지 경고<br>• deny - 플러드 감지 메커니즘이 활성화되고 구성에 따라 트래픽을 거부합니다.<br>• drop - 위협이 탐지되어 연결된 세션이 삭제되었습니다.<br>• reset-client - 위협이 감지되고 TCP RST가 클라이언트로 전송됩니다.<br>• reset-server - 위협이 감지되고 TCP RST가 서버로 전송됩니다.<br>• reset-both - 위협이 탐지되고 TCP RST가 클라이언트와 서버 모두로 전송됩니다.<br>• block-url - 차단되도록 설정된 URL 카테고리와 일치하여 URL 요청이 차단되었습니다.<br>• block-ip - 위협이 감지되고 클라이언트 IP가 차단됨<br>• 랜덤 드롭 - 플러드 감지 및 패킷이 임의로 삭제됨<br>• sinkhole - DNS 싱크홀 활성화<br>• syncookie-sent-syncookie 알림 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • blockk-continue(URL 하위 유형에만 해당) - HTTP 요청이 차단되고 진행 확인을 위한 버튼가 있는 [계속] 페이지로 리디렉션됩니다.<br>• continue(URL 하위 유형만 해당) - block-continue 요청이 진행될 수 있음을 나타내는 block-continue URL 계속 페이지에 대한 응답<br>• block-override(URL 하위 유형만 해당) - HTTP 요청이 차단되고 계속하려면 방화벽 관리자의 암호 코드가 필요한 관리자 재정의 페이지로 리디렉션됩니다.<br>• override-lockout(URL 하위 유형만 해당) - 소스 IP에서 실패한 관리자 재정의 패스 코드 시도가 너무 많습니다. 이제 블록 재정의 리디렉션 페이지에서 IP가 차단되었습니다.<br>• override(URL 하위 유형만 해당) - 올바른 패스 코드가 제공되고 요청이 허용되는 블록 오버라이드 페이지에 대한 응답<br>• block(WildFire만 해당) - 파일이 방화벽에 의해 차단되어 Wildfire에 업로드되었습니다. |
| URL/파일 이름(기타) | 가변 길이의 필드입니다. 파일 이름은 최대 63자까지 사용할 수 있습니다. URL은 최대 1023자까지 사용할 수 있습니다.<br>하위 유형이 url일 때 실제 URI<br>하위 유형이 file인 경우 파일 이름 또는 파일 형식<br>하위 유형이 바이러스인 경우 파일 이름<br>하위 유형이 WildFire 바이러스인 경우 파일 이름<br>하위 유형이 WildFire인 경우 파일 이름<br>해당되는 경우 하위 유형이 취약성인 경우 URL 또는 파일 이름<br>위협 카테고리가 **domain-edl**인 경우 URL<br>호스트 헤더 불일치가 감지되면 SNI 도메인이 스푸핑됩니다(고유한 위협 ID 86467로 식별됨). |
| 위협/콘텐츠 이름(위협) | 알려진 위협 및 사용자 지정 위협에 대한 Palo Alto Networks 설명 문자열 뒤에 일부 하위 유형의 경우 괄호 안에 64비트 숫자 식별자가 옵니다.<br>• 8000 - 8099 - 스캔 감지<br>• 8500 - 8599 - 플러드 감지<br>• 9999 - URL 필터링 로그<br>• 10000 - 19999 - 스파이웨어 폰 홈 탐지<br>• 20000 - 29999 - 스파이웨어 다운로드 탐지<br>• 30000 - 44999 - 취약점 악용 탐지<br>• 52000 - 52999 - 파일 형식 검색 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 60000 - 69999 - 데이터 필터링 감지<br>도메인 EDL 필드가 채워지면 이 필드는 동일한 값으로 채워집니다.<br>이전 릴리스에서 사용된 바이러스 탐지, ***WildFire*** 서명 피드 및 ***DNS C2*** 서명에 대한 위협 ***ID*** 범위가 영구적인 전역 고유 ***ID***로 대체되었습니다. 업데이트된 보고서를 생성하고 위협 로그 및 ***ACC*** 활동을 필터링하려면 위협/콘텐츠 유형(하위 유형) 및 위협 카테고리(***thr_category***) 필드 이름을 참조하십시오. |
| 카테고리(category) | URL 하위 유형의 경우 URL 카테고리입니다. WildFire 하위 유형의 경우 파일에 대한 판결이며 'malware', 'phishing', 'grayware' 또는 'benign'입니다. 다른 하위 유형의 경우 값은 'any'입니다. |
| 심각도(severity) | 위협과 관련된 심각도입니다. 값은 정보, 낮음, 보통, 높음, 중요입니다. |
| 방향(direction) | 클라이언트-서버 또는 서버-클라이언트 공격 방향을 나타냅니다.<br>• 0 - 위협의 방향은 클라이언트에서 서버로 향함<br>• 1 - 위협의 방향은 서버에서 클라이언트까지 |
| 시퀀스 번호(seqno) | 64비트 로그 입력 식별자가 순차적으로 증분됩니다. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 소스 국가(srcloc) | 개인 주소의 소스 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 대상 국가(dstloc) | 개인 주소의 경우 대상 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 콘텐츠 유형(contenttype) | 하위 유형이 URL인 경우에만 적용됩니다.<br>HTTP 응답 데이터의 콘텐츠 유형입니다. 최대 길이는 32바이트입니다. |
| PCAP ID(pcap_id) | 패킷 캡처(pcap) ID는 위협 pcap 파일과 해당 흐름의 일부로 취해진 확장 PCAP의 상관 관계를 나타내는 ID를 나타내는 서명되지 않은 64 비트 정수입니다. 모든 위협 로그에는 pcap_id 0(연결된 pcap 없음) 또는 확장 pcap 파일을 참조하는 ID가 포함됩니다. |
| 파일 다이제스트(filedigest) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | filedigest 문자열은 WildFire 서비스에서 분석하기 위해 전송된 파일의 이진 해시를 표시합니다. |
| 클라우드(cloud) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br><br>클라우드 문자열은 분석을 위해 파일이 업로드된 WildFire 어플라이언스(프라이빗) 또는 WildFire 클라우드(퍼블릭)의 FQDN을 표시합니다. |
| URL 인덱스(URL_idx) | URL 필터링 및 WildFire 하위 유형에 사용됩니다.<br><br>애플리케이션이 TCP keepalives를 사용하여 일정 기간 동안 연결을 열어 두는 경우 해당 세션의 모든 로그 항목은 단일 세션 ID를 갖습니다. 이러한 경우 여러 URL 항목을 포함하는 단일 위협 로그(및 세션 ID) 가 있는 경우 url_idx는 단일 세션 내에서 각 로그 항목의 순서를 상호 연관시킬 수 있는 카운터입니다.<br><br>예를 들어 방화벽이 분석을 위해 WildFire에 포워딩한 파일의 URL을 알아보려면 WildFire 제출 로그에서 세션 ID와 url_idx를 찾아 URL 필터링 로그에서 동일한 세션 ID와 url_idx를 검색합니다. 세션 ID 및 url_idx와 일치하는 로그 항목에는 WildFire로 포워딩된 파일의 URL이 포함됩니다. |
| 사용자 에이전트(user_agent) | URL 필터링 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br><br>사용자 에이전트 필드는 사용자가 URL에 액세스하는 데 사용한 웹 브라우저를 지정합니다(예: Internet Explorer). 이 정보는 HTTP 요청에서 서버로 전송됩니다. |
| 파일 형식(filetype) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br><br>WildFire 분석을 위해 방화벽이 포워딩한 파일 유형을 지정합니다. |
| X-포워드-대상(xff) | URL 필터링 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br><br>HTTP 헤더의 X-Forwarded-Ford 필드에는 웹 페이지를 요청한 사용자의 IP 주소가 들어 있습니다. 이 기능을 사용하면 사용자의 IP 주소를 식별할 수 있으므로 네트워크에 사용자 IP 주소를 패킷 헤더의 소스 IP 주소 필드에 있는 자체 주소로 대체하는 프록시 서버가 있는 경우 특히 유용합니다. |
| 리퍼러(referer) | URL 필터링 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br><br>HTTP 헤더의 Referer 필드에는 사용자를 다른 웹 페이지에 연결한 웹 페이지의 URL이 포함되어 있습니다. 이 URL은 사용자를 요청 중인 웹 페이지로 리디렉션(참조)한 소스입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 발신자(sender) | 전자 메일을 발신자의 이름을 지정합니다. |
| 제목(subject) | 이메일의 제목을 지정합니다. |
| 수신자(recipient) | 이메일 수신자 이름을 지정합니다. |
| 보고서 ID(reportid) | 데이터 필터링 및 WildFire 하위 유형에만 해당됩니다. 다른 모든 유형은 이 필드를 사용하지 않습니다.<br>방화벽, WildFire 클라우드 또는 WildFire 어플라이언스에 대한 분석 요청을 식별합니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 소스 VM UUID(src_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 소스 범용 고유 식별자를 식별합니다. |
| 대상 VM UUID(dst_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 대상 범용 고유 식별자를 식별합니다. |
| HTTP 메소드(http_method) | URL 필터링 로그에서만 가능합니다. 웹 요청에 사용되는 HTTP 메소드에 대해 설명합니다. 다음 메서드만 기록됩니다. 연결, 삭제, 가져오기, 헤드, 옵션, 게시, 넣기. |
| Tunnel ID/ IMSI(tunnel_id/imsi) | IMSI(International Mobile Subscriber Identity)는 GSM/UMTS/EPS 시스템에서 각 모바일 가입자에게 할당되는 고유 번호입니다. IMSI는 10진수(0~9)로만 구성되며 허용되는 최대 자릿수는 15입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 모니터 태그/IMEI(모니터 태그/imei) | IMEI(International Mobile Equipment Identity)는 각 이동국 장비에 할당된 고유한 15자리 또는 16자리 숫자입니다. |
| 부모 요소 세션 ID(parent_session_id) | 이 세션이 터널링되는 세션의 ID입니다. 내부 터널(두 수준의 터널링인 경우) 또는 내부 내용(한 수준의 터널링인 경우)에만 적용됩니다. |
| 상위 세션 시작 시간(parent_start_time) | 년/월/일 시간:분:초, 부모 요소 터널 세션이 시작된 시입니다. |
| 터널 유형(tunnel) | GRE 또는 IPsec과 같은 터널 유형입니다. |
| 위협 카테고리(thr_category) | 다양한 유형의 위협 서명을 분류하는 데 사용되는 위협 카테고리에 대해 설명합니다.<br>도메인 외부 동적 목록에서 로그를 생성한 경우 **domain-edl**이 이 필드를 채웁니다. |
| 콘텐츠 버전(contentver) | 로그가 생성될 때 방화벽의 애플리케이션 및 위협 버전입니다. |
| SCTP 연결 ID(assoc_id) | 두 SCTP 엔드포인트 간의 연결에 대한 모든 연결을 식별하는 번호입니다. |
| 페이로드 프로토콜 ID(ppid) | 데이터 청크의 데이터 부분에 있는 페이로드에 대한 프로토콜의 ID입니다. |
| HTTP 헤더(http_headers) | 방화벽의 URL 로그 항목에 삽입된 HTTP 헤더를 나타냅니다. |
| URL 카테고리 목록(url_category_list) | 방화벽에서 정책을 적용하는 데 사용한 URL 필터링 카테고리를 나열합니다. |
| 규칙 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| HTTP/2 연결(http2_connection) | 다음 값 중 하나를 표시하여 트래픽이 HTTP/2 연결을 사용하는지의 여부를 식별합니다.<br>• TCP 연결 세션 ID - 세션이 HTTP/2입니다.<br>• 0 - 세션이 HTTP/2가 아닙니다. |
| 동적 사용자 그룹 이름(dynusergroup_name) | 세션을 시작한 사용자가 포함된 동적 사용자 그룹의 이름입니다. |
| XFF 주소(xff_ip) | 웹 페이지를 요청한 사용자의 IP 주소 또는 요청이 통과한 마지막 디바이스 옆에 있는 IP 주소입니다. 요청이 하나 이상의 프록시, 로드 밸런서 또는 기타 업스트림 디바이스를 통과하는 경우 방화벽은 최신 디바이스의 IP 주소를 표시합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 소스 디바이스 카테고리(src_category) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 카테고리입니다. |
| 소스 디바이스 프로파일(src_profile) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 소스 디바이스 모델(src_model) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 모델입니다. |
| 소스 디바이스 공급업체(src_vendor) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 공급업체입니다. |
| 소스 디바이스 OS 패밀리(src_osfamily) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 유형입니다. |
| 소스 디바이스 OS 버전(src_osversion) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 버전입니다. |
| 소스 호스트 이름(src_host) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 호스트 이름입니다. |
| 소스 MAC 주소(src_mac) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 MAC 주소입니다. |
| 대상 디바이스 카테고리(dst_category) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 카테고리입니다. |
| 대상 디바이스 프로파일(dst_profile) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 대상 디바이스 모델(dst_model) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 모델입니다. |
| 대상 디바이스 공급업체(dst_vendor) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 벤더입니다. |
| 대상 디바이스 OS 제품군(dst_osfamily) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 유형입니다. |
| 대상 디바이스 OS 버전(dst_osversion) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 버전입니다. |
| 대상 호스트 이름(dst_host) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 호스트 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 대상 MAC 주소(dst_mac) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 MAC 주소입니다. |
| 컨테이너 ID(container_id) | 애플리케이션 POD가 배포된 쿠버네티스 노드에 있는 PAN-NGFW POD의 컨테이너 ID. |
| POD 네임스페이스(pod_namespace) | 보안이 설정되는 애플리케이션 POD의 네임스페이스입니다. |
| 포드 이름(pod_name) | 보안이 유지되는 애플리케이션 POD입니다. |
| 소스 외부 동적 목록(src_edl) | 트래픽의 원본 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 대상 외부 동적 목록(dst_edl) | 트래픽의 대상 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 호스트 ID(hostid) | 고유 ID GlobalProtect는 호스트를 식별하기 위해 할당합니다. |
| 사용자 디바이스 일련번호(serialnumber) | 사용자의 컴퓨터 또는 디바이스의 일련번호입니다. |
| 도메인 EDL(domain_edl) | 트래픽의 도메인 이름을 포함하는 외부 동적 목록의 이름입니다. |
| 원본 동적 주소 그룹(src_dag) | 원래 세션 소스 동적 주소 그룹입니다. |
| 대상 동적 주소 그룹(dst_dag) | 원래 대상 소스 동적 주소 그룹입니다. |
| 부분 해시(partial_hash) | 기계 학습 부분 해시. |
| 고해상도 타임스탬프(high_res timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br><br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |
| 이유(reason) | 데이터 필터링 작업의 이유 |
| 자리맞추기(justification) | 데이터 필터링 작업에 대한 정당성. |
| 슬라이스 서비스 유형(nssai_sst) | 네트워크 슬라이스 ID의 A 슬라이스 서비스 유형입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |
| 애플리케이션 카테고리(category_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking<br>• saas |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 터널링된 응용 프로그램(tunneled_app) | 터널링된 응용 프로그램의 이름입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 **1**을 표시하고 SaaS 애플리케이션이 아닌 경우 **0**을 표시합니다. |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 애플리케이션이 승인되면 **1**을 표시하고 애플리케이션이 승인되지 않은 경우 **0**을 표시합니다. |
| 클라우드 보고서 ID(cloud_reportid) | (PAN-OS 10.2.0) 방화벽에서 보낸 DLP 클라우드 서비스에서 검색한 파일의 고유한 32자 ID입니다.<br>(PAN-OS 10.2.1 이상 릴리스) 방화벽에서 보낸 DLP 클라우드 서비스에서 스캔한 파일의 고유한 67자 ID입니다.<br>DLP 클라우드 서비스가 이미 스캔하고 클라우드 보고서 ID를 생성한 파일에 대해 동일한 클라우드 보고서 ID가 표시됩니다. |

## URL 필터링 로그 필드

형식: FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성 시간, 소스 주소, 대상 주소, NAT 소스 IP, NAT 대상 IP, 규칙 이름, 소스 사용자, 대상 사용자, 애플리케이션, 가상 시스템, 소스 국가, 대상 국가, 인바운드 인터페이스, 아웃바운드 인터페이스, 로그작업, FUTURE_USE, 세션 ID, 반복 횟수, 소스 포트, 대상 포트, NAT 소스 포트, NAT 대상 포트, 플래그, IP 프로토콜, 작업, URL/파일 이름, 위협 ID, 카테고리, 심각도, 방향, 시퀀스 번호, 작업 플래그, 소스 위치, 대상 위치, FUTURE_USE, 콘텐츠 유형, PCAP_ID, 파일다이제스트, 클라우드, URL 인덱스, 사용자 에이전트, 파일 유형, X 포워딩 대상, 참조자, 발신자, 제목, 수신자, 보고서 ID, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 수준 3, 디바이스 그룹 레이어 수준 4, 가상 시스템 이름, 디바이스 이름, FUTURE_USE, 소스 VM UUID,대상 VM UUID, HTTP 메서드, 터널 ID/IMSI, 모니터 태그/IMEI, 상위 세션 ID, 상위 세션 ID, 상위 시작 시간, 터널 유형, 위협 카테고리, 콘텐츠 버전, FUTURE_USE, SCTP 연결 ID, 페이로드 프로토콜 ID, HTTP 헤더, URL 카테고리 목록, 규칙 UUID, HTTP/2 연결, 동적 사용자 그룹 이름, XFF 주소, 소스디바이스 카테고리, 소스 디바이스 프로파일, 소스 디바이스 모델, 소스 디바이스 공급자, 소스 디바이스 OS 제품군, 소스 디바이스 OS 버전, 소스 호스트 이름, 소스 MAC 주소, 대상 디바이스 카테고리, 대상 디바이스 프로파일, 대상 디바이스 모델, 대상 디바이스 공급자, 대상 디바이스 OS 제품군,대상 디바이스 OS 버전, 대상 호스트 이름, 대상 MAC 주소, 컨테이너 ID, POD 네임스페이스, POD 이름, 소스 외부 동적 목록, 대상 외부 동적 목록, 호스트 ID, 일련번호, 도메인 EDL, 소스 동적 주소 그룹, 대상 동적 주소 그룹, 부분 해시,고해상도 타임스탬프, 이유, 근거, 슬라이스 서비스 유형, 애플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 애플리케이션 특성, 애플리케이션 컨테이너, 애플리케이션 SaaS, 애플리케이션 승인 상태


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial #) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 THEAT 입니다. |
| 위협/콘텐츠 유형(subtype) | 위협 로그의 하위 유형 값은 url입니다. |
| 시간 생성(time_generated 또는 cef-formatted-time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 원래 세션 소스 IP 주소입니다. |
| 대상 주소(dst) | 원래 세션 대상 IP 주소입니다. |
| NAT 소스 IP(natsrc) | 소스 NAT가 수행된 경우 NAT 이후 소스 IP 주소입니다. |
| NAT 데스티네이션 IP(natdst) | 대상 NAT가 수행된 경우 사후 NAT 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션이 일치한 규칙의 이름입니다. |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 대상 사용자(dstuser) | 세션이 대상으로 지정된 사용자의 사용자 이름입니다. |
| 애플리케이션(app) | 세션과 연결된 애플리케이션입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션이 소싱된 영역입니다. |
| 대상 영역(to) | 세션이 예정된 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 세션 ID(sessionid) | 각 세션에 적용되는 내부 숫자 식별자입니다. |
| 반복 수(반복) | 소스 IP, 대상 IP, 애플리케이션 및 콘텐츠/위협 유형이 5초 내에 동일한 세션 수입니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| NAT 소스 포트(natsport) | Post-NAT 소스 포트입니다. |
| NAT 대상 포트(natdport) | NAT 이후 대상 포트입니다. |
| 플래그(flags) | 세션에 대한 세부 정보를 제공하는 32비트 필드입니다. 이 필드는 로깅된 값으로 값을 AND 지정하여 디코딩할 수 있습니다.<br>• 0x80000000 - 세션에 패킷 캡처(PCAP)가 있습니다.<br>• 0x40000000 - 클라이언트가 여러 경로를 사용하여 대상 호스트에 연결할 수 있도록 하는 옵션이 활성화됩니다.<br>• 0x20000000 - 판단을 위해 파일이 와일드파이어에 제출됨<br>• 0x10000000 - 최종 사용자에 의한 엔터프라이즈 자격 증명 제출이 감지됨<br>• 0x08000000 - 흐름에 대한 소스가 허용 목록에 있으며 정찰 보호 대상이 아닙니다.<br>• 0x02000000 - IPv6 session<br>• 0x01000000 - SSL 세션의 암호가 복호화됩니다(SSL 프록시).<br>• 0x00800000 - URL 필터링을 통해 세션이 거부되었습니다.<br>• 0x00400000 - 세션에 NAT 변환이 수행되었습니다.<br>• 0x00200000 - 세션에 대한 사용자 정보가 인증 포털을 통해 캡처되었습니다.<br>• 0x00100000 - 애플리케이션 트래픽이 비표준 대상 포트에 있습니다.<br>• 0x00080000 - X-포워딩됨-프록시의 값이 소스 사용자 필드에 있음<br>• 0x00040000 - log는 http 프록시 세션 내의 트랜잭션에 해당합니다(프록시 트랜잭션).<br>• 0x00020000 - 클라이언트-서버 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00010000 - 서버 대 클라이언트 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00008000 - 세션이 컨테이너 페이지 액세스입니다(컨테이너 페이지). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 0x00002000 - 세션이 암시적 애플리케이션 종속성 처리에 대한 규칙과 일시적으로 일치합니다. PAN-OS 5.0.0 이상에서 사용할 수 있습니다.<br>• 0x00000800 - 대칭 반환은 이 세션의 트래픽을 포워딩하는 데 사용됩니다.<br>• 0x00000400 - 복호화된 트래픽이 미러 포트를 통해 일반 텍스트로 전송되고 있습니다.<br>• 0x00000010 - 외부 터널의 탑재량을 검사하는 중입니다. |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 취한 조치 값은 경고, 허용, 차단 URL, 차단 계속, 계속, 차단 재정의, 재정의-잠금, 재정의입니다.<br>• alert - 위협 또는 URL이 감지되었지만 차단되지 않음<br>• allow - 플러드 감지 경고<br>• block-url - 차단되도록 설정된 URL 카테고리와 일치하여 URL 요청이 차단되었습니다.<br>• block-continue - HTTP 요청이 차단되고 확인 버튼이 있는 계속 페이지로 리디렉션됩니다.<br>• 계속 - 계속 차단 URL에 대한 응답으로 차단 계속 요청이 계속 진행되도록 허용되었음을 나타내는 페이지 계속<br>• block-override - HTTP 요청이 차단되고 계속하려면 방화벽 관리자의 암호가 필요한 관리자 무시 페이지로 리디렉션됩니다.<br>• override-lockout - 소스 IP에서 너무 많은 관리자 재정의 패스 코드 시도에 실패했습니다. 이제 블록 재정의 리디렉션 페이지에서 IP가 차단되었습니다.<br>• override - 올바른 패스 코드가 제공되고 요청이 허용되는 차단 무시 페이지에 대한 응답 |
| URL/파일 이름(기타) | 가변 길이의 필드입니다. URL은 최대 1023자입니다.<br>하위 유형이 url일 때 실제 URL입니다.<br>위협 카테고리가 **domain-edl**인 경우 URL. |
| 위협/콘텐츠 이름(위협) | 알려진 위협 및 사용자 지정 위협에 대한 Palo Alto Networks 설명 문자열 뒤에 일부 하위 유형의 경우 괄호 안에 64비트 숫자 식별자가 옵니다.<br>• 8000 - 8099 - 스캔 감지<br>• 8500 - 8599 - 플러드 감지<br>• 9999 - URL 필터링 로그 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 10000 - 19999 - 스파이웨어 폰 홈 탐지<br>• 20000 - 29999 - 스파이웨어 다운로드 탐지<br>• 30000 - 44999 - 취약점 악용 탐지<br>• 52000 - 52999 - 파일 형식 검색<br>• 60000 - 69999 - 데이터 필터링 감지<br>도메인 EDL 필드가 채워지면 이 필드는 동일한 값으로 채워집니다.<br> 이전 릴리스에서 사용된 바이러스 탐지, ***WildFire*** 서명 피드 및 ***DNS C2*** 서명에 대한 위협 ***ID*** 범위가 영구적인 전역 고유 ID로 대체되었습니다. 업데이트된 보고서를 생성하고 위협 로그 및 ***ACC*** 활동을 필터링하려면 위협/콘텐츠 유형(하위 유형) 및 위협 카테고리(***thr_category***) 필드 이름을 참조하십시오. |
| 카테고리(category) | URL 하위 유형의 경우 URL 카테고리입니다. WildFire 하위 유형의 경우 파일에 대한 판결이며 'malware', 'phishing', 'grayware' 또는 'benign'입니다. 다른 하위 유형의 경우 값은 'any'입니다. |
| 심각도(severity) | 위협과 관련된 심각도입니다. 값은 정보, 낮음, 보통, 높음, 중요입니다. |
| 방향(direction) | 공격 방향을 나타냅니다.<br>• 클라이언트에서 서버로<br>• 서버에서 클라이언트로 |
| 시퀀스 번호(seqno) | 64비트 로그 입력 식별자가 순차적으로 증분됩니다. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 소스 국가(srcloc) | 개인 주소의 소스 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 대상 국가(dstloc) | 개인 주소의 경우 대상 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 콘텐츠 유형(contenttype) | HTTP 응답 데이터의 콘텐츠 유형입니다. 최대 길이는 32바이트입니다. |
| PCAP ID(pcap_id) | 패킷 캡처(pcap) ID는 위협 pcap 파일과 해당 흐름의 일부로 취해진 확장 PCAP의 상관 관계를 나타내는 ID를 나타내는 서명되지 않은 64 비트 정수입니다. 모든 위협 로그에는 pcap_id 0(연결된 pcap 없음) 또는 확장 pcap 파일을 참조하는 ID가 포함됩니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 파일 다이제스트(filedigest) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>filedigest 문자열은 WildFire 서비스에서 분석하기 위해 전송된 파일의 이진 해시를 표시합니다. |
| 클라우드(cloud) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>클라우드 문자열은 분석을 위해 파일이 업로드된 WildFire 어플라이언스(프라이빗) 또는 WildFire 클라우드(퍼블릭)의 FQDN을 표시합니다. |
| URL 인덱스(URL_idx) | 애플리케이션이 TCP keepalives를 사용하여 일정 기간 동안 연결을 열어두는 경우 해당 세션의 모든 로그 항목은 단일 세션 ID를 갖습니다. 이러한 경우 여러 URL 항목을 포함하는 단일 위협 로그(및 세션 ID) 가 있는 경우 url_idx는 단일 세션 내에서 각 로그 항목의 순서를 상호 연관시킬 수 있는 카운터입니다.<br>예를 들어 방화벽이 분석을 위해 WildFire에 포워딩한 파일의 URL을 알아보려면 WildFire 제출 로그에서 세션 ID와 url_idx를 찾아 URL 필터링 로그에서 동일한 세션 ID와 url_idx를 검색합니다. 세션 ID 및 url_idx와 일치하는 로그 항목에는 WildFire로 포워딩된 파일의 URL이 포함됩니다. |
| 사용자 에이전트(user_agent) | 사용자 에이전트 필드는 사용자가 URL에 액세스하는 데 사용한 웹 브라우저를 지정합니다(예: Internet Explorer). 이 정보는 HTTP 요청에서 서버로 전송됩니다. |
| 파일 형식(filetype) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>WildFire 분석을 위해 방화벽이 포워딩한 파일 유형을 지정합니다. |
| X-포워드-대상(xff) | HTTP 헤더의 X-Forwarded-Ford 필드에는 웹 페이지를 요청한 사용자의 IP 주소가 들어 있습니다. 이 기능을 사용하면 사용자의 IP 주소를 식별할 수 있으므로 네트워크에 사용자 IP 주소를 패킷 헤더의 소스 IP 주소 필드에 있는 자체 주소로 대체하는 프록시 서버가 있는 경우 특히 유용합니다. |
| 리퍼러(referer) | HTTP 헤더의 Referer 필드에는 사용자를 다른 웹 페이지에 연결한 웹 페이지의 URL이 포함되어 있습니다. 이 URL은 사용자를 요청 중인 웹 페이지로 리디렉션(참조)한 소스입니다. |
| 발신자(sender) | 전자 메일을 발신자의 이름을 지정합니다. |
| 제목(subject) | 이메일의 제목을 지정합니다. |
| 수신자(recipient) | 이메일 수신자 이름을 지정합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 보고서 ID(reportid) | 데이터 필터링 및 WildFire 하위 유형에만 해당됩니다. 다른 모든 유형은 이 필드를 사용하지 않습니다.<br>방화벽, WildFire 클라우드 또는 WildFire 어플라이언스에 대한 분석 요청을 식별합니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 소스 VM UUID(src_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 소스 범용 고유 식별자를 식별합니다. |
| 대상 VM UUID(dst_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 대상 범용 고유 식별자를 식별합니다. |
| HTTP 메소드(http_method) | 웹 요청에 사용되는 HTTP 메소드에 대해 설명합니다. 다음 메서드만 기록됩니다. 연결, 삭제, 가져오기, 헤드, 옵션, 게시, 넣기. |
| Tunnel ID/ IMSI(tunnel_id/imsi) | IMSI(International Mobile Subscriber Identity)는 GSM/UMTS/EPS 시스템에서 각 모바일 가입자에게 할당되는 고유 번호입니다. IMSI는 10진수(0~9)로만 구성되며 허용되는 최대 자릿수는 15입니다. |
| 모니터 태그/IMEI(모니터 태그/imei) | IMEI(International Mobile Equipment Identity)는 각 이동국 장비에 할당된 고유한 15자리 또는 16자리 숫자입니다. |
| 부모 요소 세션 ID(parent_session_id) | 이 세션이 터널링되는 세션의 ID입니다. 내부 터널(두 수준의 터널링인 경우) 또는 내부 내용(한 수준의 터널링인 경우)에만 적용됩니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 상위 세션 시작 시간(parent_start_time) | 년/월/일 시간:분:초, 부모 요소 터널 세션이 시작된 시입니다. |
| 터널 유형(tunnel) | GRE 또는 IPsec과 같은 터널 유형입니다. |
| 위협 카테고리(thr_category) | 다양한 유형의 위협 서명을 분류하는 데 사용되는 위협 카테고리에 대해 설명합니다.<br>도메인 외부 동적 목록에서 로그를 생성한 경우 **domain-edl**이 이 필드를 채웁니다. |
| 콘텐츠 버전(contentver) | 로그가 생성될 때 방화벽의 애플리케이션 및 위협 버전입니다. |
| SCTP 연결 ID(assoc_id) | 두 SCTP 엔드포인트 간의 연결에 대한 모든 연결을 식별하는 번호입니다. |
| 페이로드 프로토콜 ID(ppid) | 데이터 청크의 데이터 부분에 있는 페이로드에 대한 프로토콜의 ID입니다. |
| HTTP 헤더(http_headers) | 방화벽의 URL 로그 항목에 삽입된 HTTP 헤더를 나타냅니다. |
| URL 카테고리 목록(url_category_list) | 방화벽에서 정책을 적용하는 데 사용한 URL 필터링 카테고리를 나열합니다. |
| 규칙 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| HTTP/2 연결(http2_connection) | 다음 값 중 하나를 표시하여 트래픽이 HTTP/2 연결을 사용하는지의 여부를 식별합니다.<br>• TCP 연결 세션 ID - 세션이 HTTP/2입니다.<br>• 0 - 세션이 HTTP/2가 아닙니다. |
| 동적 사용자 그룹 이름(dynusergroup_name) | 세션을 시작한 사용자가 포함된 동적 사용자 그룹의 이름입니다. |
| XFF 주소(xff_ip) | 웹 페이지를 요청한 사용자의 IP 주소 또는 요청이 통과한 마지막 디바이스 옆에 있는 IP 주소입니다. 요청이 하나 이상의 프록시, 로드 밸런서 또는 기타 업스트림 디바이스를 통과하는 경우 방화벽은 최신 디바이스의 IP 주소를 표시합니다. |
| 소스 디바이스 카테고리(src_category) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 카테고리입니다. |
| 소스 디바이스 프로파일(src_profile) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 디바이스 프로파일입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 소스 디바이스 모델(src_model) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 모델입니다. |
| 소스 디바이스 공급업체(src_vendor) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 공급업체입니다. |
| 소스 디바이스 OS 패밀리(src_osfamily) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 유형입니다. |
| 소스 디바이스 OS 버전(src_osversion) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 버전입니다. |
| 소스 호스트 이름(src_host) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 호스트 이름입니다. |
| 소스 MAC 주소(src_mac) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 MAC 주소입니다. |
| 대상 디바이스 카테고리(dst_category) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 카테고리입니다. |
| 대상 디바이스 프로파일(dst_profile) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 대상 디바이스 모델(dst_model) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 모델입니다. |
| 대상 디바이스 공급업체(dst_vendor) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 벤더입니다. |
| 대상 디바이스 OS 제품군(dst_osfamily) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 유형입니다. |
| 대상 디바이스 OS 버전(dst_osversion) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 버전입니다. |
| 대상 호스트 이름(dst_host) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 호스트 이름입니다. |
| 대상 MAC 주소(dst_mac) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 MAC 주소입니다. |
| 컨테이너 ID(container_id) | 애플리케이션 POD가 배포된 쿠버네티스 노드에 있는 PAN-NGFW POD의 컨테이너 ID. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| POD 네임스페이스(pod_namespace) | 보안이 설정되는 애플리케이션 POD의 네임스페이스입니다. |
| 포드 이름(pod_name) | 보안이 유지되는 애플리케이션 POD입니다. |
| 소스 외부 동적 목록(src_edl) | 트래픽의 원본 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 대상 외부 동적 목록(dst_edl) | 트래픽의 대상 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 호스트 ID(hostid) | 고유 ID GlobalProtect는 호스트를 식별하기 위해 할당합니다. |
| 사용자 디바이스 일련번호(serialnumber) | 사용자의 컴퓨터 또는 디바이스의 일련번호입니다. |
| 도메인 EDL(domain_edl) | 트래픽의 도메인 이름을 포함하는 외부 동적 목록의 이름입니다. |
| 원본 동적 주소 그룹(src_dag) | 원래 세션 소스 동적 주소 그룹입니다. |
| 대상 동적 주소 그룹(dst_dag) | 원래 대상 소스 동적 주소 그룹입니다. |
| 부분 해시(partial_hash) | 기계 학습 부분 해시. |
| 고해상도 타임스탬프(high_res timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm) |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | 고해상도 타임스탬프는 *PAN-OS 10.1* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |
| 이유(reason) | URL 필터링 작업의 이유입니다. |
| 자리맞추기(justification) | URL 필터링 작업의 근거. |
| 슬라이스 서비스 유형(nssai_sst) | 네트워크 슬라이스 ID의 A 슬라이스 서비스 유형입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |
| 애플리케이션 카테고리(category_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking<br>• saas |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 터널링된 응용 프로그램(tunneled_app) | 터널링된 응용 프로그램의 이름입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 예 , SaaS 애플리케이션이 아닌 경우 아니요를 표시합니다. |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 애플리케이션이 승인된 경우 예를 표시하고 애플리케이션이 승인되지 않은 경우 아니오를 표시합니다. |
| 클라우드 보고서 ID(cloud_reportid) | (PAN-OS 10.2.0) 방화벽에서 보낸 DLP 클라우드 서비스에서 검색한 파일의 고유한 32자 ID입니다.<br>(PAN-OS 10.2.1 이상 릴리스) 방화벽에서 보낸 DLP 클라우드 서비스에서 스캔한 파일의 고유한 67자 ID입니다.<br>DLP 클라우드 서비스가 이미 스캔하고 클라우드 보고서 ID를 생성한 파일에 대해 동일한 클라우드 보고서 ID가 표시됩니다. |

## 데이터 필터링 로그 필드

형식: FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성 시간, 소스 주소, 대상 주소, NAT 소스 IP, NAT 대상 IP, 규칙 이름, 소스 사용자, 대상 사용자, 애플리케이션, 가상 시스템, 소스 국가, 대상 국가, 인바운드 인터페이스, 아웃바운드 인터페이스, 로그작업, FUTURE_USE, 세션 ID, 반복 횟수, 소스 포트, 대상 포트, NAT 소스 포트, NAT 대상 포트, 플래그, IP 프로토콜, 작업, URL/파일 이름, 위협 ID, 카테고리, 심각도, 방향, 시퀀스 번호, 작업 플래그, 소스 위치, 대상 위치, FUTURE_USE, 콘텐츠 유형, PCAP_ID, 파일다이제스트, 클라우드, URL 인덱스, 사용자 에이전트, 파일 유형, X 포워딩 대상, 참조자, 발신자, 제목, 수신자, 보고서 ID, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 수준 3, 디바이스 그룹 레이어 수준 4, 가상 시스템 이름, 디바이스 이름, FUTURE_USE, 소스 VM UUID,대상 VM UUID, HTTP 메서드, 터널 ID/IMSI, 모니터 태그/IMEI, 상위 세션 ID, 상위 세션 ID, 상위 시작 시간, 터널 유형, 위협 카테고리, 콘텐츠 버전, FUTURE_USE, SCTP 연결 ID, 페이로드 프로토콜 ID, HTTP 헤더, URL 카테고리 목록, 규칙 UUID, HTTP/2 연결, 동적 사용자 그룹 이름, XFF 주소, 소스디바이스 카테고리, 소스 디바이스 프로파일, 소스 디바이스 모델, 소스 디바이스 공급자, 소스 디바이스 OS 제품군, 소스 디바이스 OS 버전, 소스 호스트 이름, 소스 MAC 주소, 대상 디바이스 카테고리, 대상 디바이스 프로파일, 대상 디바이스 모델, 대상 디바이스 공급자, 대상 디바이스 OS 제품군,대상 디바이스 OS 버전, 대상 호스트 이름, 대상 MAC 주소, 컨테이너 ID, POD 네임스페이스, POD 이름, 소스 외부 동적 목록, 대상 외부 동적 목록, 호스트 ID, 일련번호, 도메인 EDL, 소스 동적 주소 그룹, 대상 동적 주소 그룹, 부분 해시,고해상도 타임스탬프, 이유, 근거, 슬라이스 서비스 유형, 애플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 애플리케이션 특성, 애플리케이션 컨테이너, 애플리케이션 SaaS, 애플리케이션 승인 상태


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial #) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(유형) | 로그 유형을 지정합니다. 값은 THEAT 입니다. |
| 위협/콘텐츠 유형(subtype) | 위협 로그의 하위 유형; 값은 데이터, dlp, dlp-non-file, file입니다. |
| 시간 생성(time_generated 또는 cef-formatted-time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 원래 세션 소스 IP 주소입니다. |
| 대상 주소(dst) | 원래 세션 대상 IP 주소입니다. |
| NAT 소스 IP(natsrc) | 소스 NAT가 수행된 경우 NAT 이후 소스 IP 주소입니다. |
| NAT 데스티네이션 IP(natdst) | 대상 NAT가 수행된 경우 사후 NAT 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션이 일치한 규칙의 이름입니다. |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 대상 사용자(dstuser) | 세션이 대상으로 지정된 사용자의 사용자 이름입니다. |
| 애플리케이션(app) | 세션과 연결된 애플리케이션입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션이 소싱된 영역입니다. |
| 대상 영역(to) | 세션이 예정된 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 세션 ID(sessionid) | 각 세션에 적용되는 내부 숫자 식별자입니다. |
| 반복 수(repeatcnt) | 소스 IP, 대상 IP, 애플리케이션 및 콘텐츠/위협 유형이 5초 내에 동일한 세션 수입니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| NAT 소스 포트(natsport) | Post-NAT 소스 포트입니다. |
| NAT 대상 포트(natdport) | NAT 이후 대상 포트입니다. |
| 플래그(flags) | 세션에 대한 세부 정보를 제공하는 32비트 필드입니다. 이 필드는 로깅된 값으로 값을 AND 지정하여 디코딩할 수 있습니다.<br>• 0x80000000 - 세션에 패킷 캡처(PCAP)가 있습니다.<br>• 0x40000000 - 클라이언트가 여러 경로를 사용하여 대상 호스트에 연결할 수 있도록 하는 옵션이 활성화됩니다.<br>• 0x20000000 - 판단을 위해 파일이 와일드파이어에 제출됨<br>• 0x10000000 - 최종 사용자에 의한 엔터프라이즈 자격 증명 제출이 감지됨<br>• 0x08000000 - 흐름에 대한 소스가 허용 목록에 있으며 정찰 보호 대상이 아닙니다.<br>• 0x02000000 - IPv6 session<br>• 0x01000000 - SSL 세션의 암호가 복호화됩니다(SSL 프록시).<br>• 0x00800000 - URL 필터링을 통해 세션이 거부되었습니다.<br>• 0x00400000 - 세션에 NAT 변환이 수행되었습니다.<br>• 0x00200000 - 세션에 대한 사용자 정보가 인증 포털을 통해 캡처되었습니다.<br>• 0x00100000 - 애플리케이션 트래픽이 비표준 대상 포트에 있습니다.<br>• 0x00080000 - X-포워딩됨-프록시의 값이 소스 사용자 필드에 있음<br>• 0x00040000 - log는 http 프록시 세션 내의 트랜잭션에 해당합니다(프록시 트랜잭션).<br>• 0x00020000 - 클라이언트-서버 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00010000 - 서버 대 클라이언트 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00008000 - 세션이 컨테이너 페이지 액세스입니다(컨테이너 페이지). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 0x00002000 - 세션이 암시적 애플리케이션 종속성 처리에 대한 규칙과 일시적으로 일치합니다. PAN-OS 5.0.0 이상에서 사용할 수 있습니다.<br>• 0x00000800 - 대칭 반환은 이 세션의 트래픽을 포워딩하는 데 사용됩니다.<br>• 0x00000400 - 복호화된 트래픽이 미러 포트를 통해 일반 텍스트로 전송되고 있습니다.<br>• 0x00000010 - 외부 터널의 탑재량을 검사하는 중입니다. |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 값은 경고, 허용, 거부, 삭제, 전체 패킷 드롭, 클라이언트 재설정, 서버 재설정, 모두 재설정, 블록 URL입니다.<br>• alert - 검색되었지만 차단되지 않은 일치하는 데이터를 포함하는 트래픽<br>• 허용(dlp 하위 유형에만 해당) - 홍수 감지 경고<br>• block(dlp 및 WildFire 하위 유형만 해당) - 일치하는 데이터가 감지되었지만 차단된 트래픽<br>• block-continue(dlp 하위 유형에만 해당) - 일치하는 데이터가 포함된 트래픽이 차단되고 계속 확인을 위한 단추가 있는 계속 페이지로 리디렉션됩니다<br>• 계속(dlp 하위 유형만 해당) - 블록 계속 요청이 계속 진행되도록 허용되었음을 나타내는 블록 계속 페이지에 대한 응답<br>• deny - 플러드 감지 메커니즘이 활성화되고 구성에 따라 트래픽을 거부합니다. |
| URL/파일 이름(기타) | 가변 길이의 필드입니다. 파일 이름은 최대 63자까지 사용할 수 있습니다.<br>하위 유형이 dlp인 경우 파일 이름<br>위협 카테고리가 **domain-edl**인 경우 URL. |
| 위협/콘텐츠 이름(위협) | 알려진 위협 및 사용자 지정 위협에 대한 Palo Alto Networks 설명 문자열 뒤에 일부 하위 유형의 경우 괄호 안에 64비트 숫자 식별자가 옵니다.<br>• 8000 - 8099 - 스캔 감지<br>• 8500 - 8599 - 플러드 감지<br>• 9999 - URL 필터링 로그<br>• 10000 - 19999 - 스파이웨어 폰 홈 탐지<br>• 20000 - 29999 - 스파이웨어 다운로드 탐지 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 30000 - 44999 - 취약점 악용 탐지<br>• 52000 - 52999 - 파일 형식 검색<br>• 60000 - 69999 - 데이터 필터링 감지<br>도메인 EDL 필드가 채워지면 이 필드는 동일한 값으로 채워집니다.<br>이전 릴리스에서 사용된 바이러스 탐지, ***WildFire*** 서명 피드 및 ***DNS C2*** 서명에 대한 위협 ***ID*** 범위가 영구적인 전역 고유 ID로 대체되었습니다. 업데이트된 보고서를 생성하고 위협 로그 및 ***ACC*** 활동을 필터링하려면 위협/콘텐츠 유형(하위 유형) 및 위협 카테고리(***thr_category***) 필드 이름을 참조하십시오. |
| 카테고리(category) | URL 하위 유형의 경우 URL 카테고리입니다. WildFire 하위 유형의 경우 파일에 대한 판결이며 '멀웨어', '피싱', '그레이웨어' 또는 '악성'입니다. 다른 하위 유형의 경우 값은 'any'입니다. |
| 심각도(severity) | 위협과 관련된 심각도입니다. 값은 정보, 낮음, 보통, 높음, 중요입니다. |
| 방향(direction) | 공격 방향을 나타냅니다.<br>• 클라이언트에서 서버로<br>• 서버에서 클라이언트로 |
| 시퀀스 번호(seqno) | 64비트 로그 입력 식별자가 순차적으로 증분됩니다. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 소스 국가(srcloc) | 개인 주소의 소스 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 대상 국가(dstloc) | 개인 주소의 경우 대상 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 콘텐츠 유형(contenttype) | 하위 유형이 URL인 경우에만 적용됩니다.<br>HTTP 응답 데이터의 콘텐츠 유형입니다. 최대 길이는 32바이트입니다. |
| PCAP ID(pcap_id) | 패킷 캡처(pcap) ID는 위협 pcap 파일과 해당 흐름의 일부로 취해진 확장 PCAP의 상관 관계를 나타내는 ID를 나타내는 서명되지 않은 64 비트 정수입니다. 모든 위협 로그에는 pcap_id 0(연결된 pcap 없음) 또는 확장 pcap 파일을 참조하는 ID가 포함됩니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 파일 다이제스트(filedigest) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>filedigest 문자열은 WildFire 서비스에서 분석하기 위해 전송된 파일의 이진 해시를 표시합니다. |
| 클라우드(cloud) | WildFire 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>클라우드 문자열은 분석을 위해 파일이 업로드된 WildFire 어플라이언스(프라이빗) 또는 WildFire 클라우드(퍼블릭)의 FQDN을 표시합니다. |
| URL 인덱스(URL_idx) | URL 필터링 및 WildFire 하위 유형에 사용됩니다.<br>애플리케이션이 TCP keepalives를 사용하여 일정 기간 동안 연결을 열어 두는 경우 해당 세션의 모든 로그 항목은 단일 세션 ID를 갖습니다. 이러한 경우 여러 URL 항목을 포함하는 단일 위협 로그(및 세션 ID) 가 있는 경우 url_idx는 단일 세션 내에서 각 로그 항목의 순서를 상호 연관시킬 수 있는 카운터입니다.<br>예를 들어 방화벽이 분석을 위해 WildFire에 포워딩한 파일의 URL을 알아보려면 WildFire 제출 로그에서 세션 ID와 url_idx를 찾아 URL 필터링 로그에서 동일한 세션 ID와 url_idx를 검색합니다. 세션 ID 및 url_idx와 일치하는 로그 항목에는 WildFire로 포워딩된 파일의 URL이 포함됩니다. |
| 사용자 에이전트(user_agent) | URL 필터링 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>사용자 에이전트 필드는 사용자가 URL에 액세스하는 데 사용한 웹 브라우저를 지정합니다(예: Internet Explorer). 이 정보는 HTTP 요청에서 서버로 전송됩니다. |
| 파일 형식(filetype) | 방화벽이 분석을 위해 전달한 파일 형식을 지정합니다. |
| X-포워드-대상(xff) | URL 필터링 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>HTTP 헤더의 X-Forwarded-Ford 필드에는 웹 페이지를 요청한 사용자의 IP 주소가 들어 있습니다. 이 기능을 사용하면 사용자의 IP 주소를 식별할 수 있으므로 네트워크에 사용자 IP 주소를 패킷 헤더의 소스 IP 주소 필드에 있는 자체 주소로 대체하는 프록시 서버가 있는 경우 특히 유용합니다. |
| 리퍼러(referer) | URL 필터링 하위 유형에만 해당하며 다른 모든 유형에서는 이 필드를 사용하지 않습니다.<br>HTTP 헤더의 Referer 필드에는 사용자를 다른 웹 페이지에 연결한 웹 페이지의 URL이 포함되어 있습니다. 이 URL은 사용자를 요청 중인 웹 페이지로 리디렉션(참조)한 소스입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 발신자(sender) | 이메일을 발신자의 이름을 지정합니다. |
| 제목(subject) | 이메일의 제목을 지정합니다. |
| 수신자(recipient) | 이메일 수신자 이름을 지정합니다. |
| 보고서 ID(reportid) | 방화벽, WildFire 클라우드 또는 WildFire 어플라이언스에 대한 분석 요청을 식별합니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 소스 VM UUID(src_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 소스 범용 고유 식별자를 식별합니다. |
| 대상 VM UUID(dst_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 대상 범용 고유 식별자를 식별합니다. |
| HTTP 메소드(http_method) | URL 필터링 로그에서만 가능합니다. 웹 요청에 사용되는 HTTP 메소드에 대해 설명합니다. 다음 메서드만 기록됩니다. 연결, 삭제, 가져오기, 헤드, 옵션, 게시, 넣기. |
| Tunnel ID/ IMSI(tunnel_id/imsi) | IMSI(International Mobile Subscriber Identity)는 GSM/UMTS/EPS 시스템에서 각 모바일 가입자에게 할당되는 고유 번호입니다. IMSI는 10진수(0~9)로만 구성되며 허용되는 최대 자릿수는 15입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 모니터 태그/IMEI(모니터 태그/imei) | IMEI(International Mobile Equipment Identity)는 각 이동국 장비에 할당된 고유한 15자리 또는 16자리 숫자입니다. |
| 부모 요소 세션 ID(parent_session_id) | 이 세션이 터널링되는 세션의 ID입니다. 내부 터널(두 수준의 터널링인 경우) 또는 내부 내용(한 수준의 터널링인 경우)에만 적용됩니다. |
| 상위 세션 시작 시간(parent_start_time) | 년/월/일 시간:분:초, 부모 요소 터널 세션이 시작된 시입니다. |
| 터널 유형(tunnel) | GRE 또는 IPsec과 같은 터널 유형입니다. |
| 위협 카테고리(thr_category) | 다양한 유형의 위협 서명을 분류하는 데 사용되는 위협 카테고리에 대해 설명합니다.<br>도메인 외부 동적 목록에서 로그를 생성한 경우 **domain-edl**이 이 필드를 채웁니다. |
| 콘텐츠 버전(contentver) | 로그가 생성될 때 방화벽의 애플리케이션 및 위협 버전입니다. |
| SCTP 연결 ID(assoc_id) | 두 SCTP 엔드포인트 간의 연결에 대한 모든 연결을 식별하는 번호입니다. |
| 페이로드 프로토콜 ID(ppid) | 데이터 청크의 데이터 부분에 있는 페이로드에 대한 프로토콜의 ID입니다. |
| HTTP 헤더(http_headers) | 방화벽의 URL 로그 항목에 삽입된 HTTP 헤더를 나타냅니다. |
| URL 카테고리 목록(url_category_list) | 방화벽에서 정책을 적용하는 데 사용한 URL 필터링 카테고리를 나열합니다. |
| 규칙 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| HTTP/2 연결(http2_connection) | 다음 값 중 하나를 표시하여 트래픽이 HTTP/2 연결을 사용하는지의 여부를 식별합니다.<br>• TCP 연결 세션 ID - 세션이 HTTP/2입니다.<br>• 0 - 세션이 HTTP/2가 아닙니다. |
| 동적 사용자 그룹 이름(dynusergroup_name) | 세션을 시작한 사용자가 포함된 동적 사용자 그룹의 이름입니다. |
| XFF 주소(xff_ip) | 웹 페이지를 요청한 사용자의 IP 주소 또는 요청이 통과한 마지막 디바이스 옆에 있는 IP 주소입니다. 요청이 하나 이상의 프록시, 로드 밸런서 또는 기타 업스트림 디바이스를 통과하는 경우 방화벽은 최신 디바이스의 IP 주소를 표시합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 소스 디바이스 카테고리(src_category) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 카테고리입니다. |
| 소스 디바이스 프로파일(src_profile) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 소스 디바이스 모델(src_model) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 모델입니다. |
| 소스 디바이스 공급업체(src_vendor) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 공급업체입니다. |
| 소스 디바이스 OS 패밀리(src_osfamily) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 유형입니다. |
| 소스 디바이스 OS 버전(src_osversion) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 버전입니다. |
| 소스 호스트 이름(src_host) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 호스트 이름입니다. |
| 소스 MAC 주소(src_mac) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 MAC 주소입니다. |
| 대상 디바이스 카테고리(dst_category) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 카테고리입니다. |
| 대상 디바이스 프로파일(dst_profile) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 대상 디바이스 모델(dst_model) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 모델입니다. |
| 대상 디바이스 공급업체(dst_vendor) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 벤더입니다. |
| 대상 디바이스 OS 제품군(dst_osfamily) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 유형입니다. |
| 대상 디바이스 OS 버전(dst_osversion) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 버전입니다. |
| 대상 호스트 이름(dst_host) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 호스트 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 대상 MAC 주소(dst_mac) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 MAC 주소입니다. |
| 컨테이너 ID(container_id) | 애플리케이션 POD가 배포된 쿠버네티스 노드에 있는 PAN-NGFW POD의 컨테이너 ID. |
| POD 네임스페이스(pod_namespace) | 보안이 설정되는 애플리케이션 POD의 네임스페이스입니다. |
| 포드 이름(pod_name) | 보안이 유지되는 애플리케이션 POD입니다. |
| 소스 외부 동적 목록(src_edl) | 트래픽의 원본 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 대상 외부 동적 목록(dst_edl) | 트래픽의 대상 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 호스트 ID(hostid) | 고유 ID GlobalProtect는 호스트를 식별하기 위해 할당합니다. |
| 사용자 디바이스 일련번호(serialnumber) | 사용자의 컴퓨터 또는 디바이스의 일련번호입니다. |
| 도메인 EDL(domain_edl) | 트래픽의 도메인 이름을 포함하는 외부 동적 목록의 이름입니다. |
| 원본 동적 주소 그룹(src_dag) | 원래 세션 소스 동적 주소 그룹입니다. |
| 대상 동적 주소 그룹(dst_dag) | 원래 대상 소스 동적 주소 그룹입니다. |
| 부분 해시(partial_hash) | 기계 학습 부분 해시. |
| 고해상도 타임스탬프(high_res timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br><br>고해상도 타임스탬프는 *PAN-OS 10.1* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |
| 이유(reason) | 데이터 필터링 작업의 이유 |
| 자리맞추기(justification) | 데이터 필터링 작업에 대한 정당성. |
| 슬라이스 서비스 유형(nssai_sst) | 네트워크 슬라이스 ID의 A 슬라이스 서비스 유형입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |
| 애플리케이션 카테고리(category_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking<br>• saas |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 터널링된 애플리케이션(tunneled_app) | 터널링된 애플리케이션의 이름입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 예 , SaaS 애플리케이션이 아닌 경우 아니요를 표시합니다. |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 애플리케이션이 승인된 경우 예를 표시하고 애플리케이션이 승인되지 않은 경우 아니오를 표시합니다. |
| 클라우드 보고서 ID(cloud_reportid) | (PAN-OS 10.2.0) 방화벽에서 보낸 DLP 클라우드 서비스에서 검색한 파일의 고유한 32자 ID입니다.<br>(PAN-OS 10.2.1 이상 릴리스) 방화벽에서 보낸 DLP 클라우드 서비스에서 스캔한 파일의 고유한 67자 ID입니다.<br>DLP 클라우드 서비스가 이미 스캔하고 클라우드 보고서 ID를 생성한 파일에 대해 동일한 클라우드 보고서 ID가 표시됩니다. |

## HIP 매치 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, 위협 / 콘텐츠 유형, FUTURE_USE, 생성 된 시간, 소스 사용자, 가상 시스템, 기계 이름, 운영 체제, 소스 주소, HIP, 반복 카운트, HIP 유형, FUTURE_USE, FUTURE_USE, 시퀀스 번호, 동작 플래그, 디바이스 그룹 레이어 구조 레벨 1, 디바이스 그룹 레이어 구조 레벨 2, 디바이스 그룹 레이어 구조 레벨 3, 디바이스 그룹 레이어 구조 레벨 4, 디바이스 그룹 레이어 구조 레벨 4, 가상 시스템 이름, 디바이스 이름, 가상 시스템 ID, IPv6 소스 주소, 호스트 ID, 사용자 디바이스 일련번호, 디바이스 MAC 주소, 고해상도 타임스탬프

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 HIP 매치입니다. |
| 위협/콘텐츠 유형(subtype) | HIP 매치 로그의 하위 유형(미사용). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 가상 시스템(vsys) | HIP 일치 로그와 연결된 가상 시스템입니다. |
| 머신 이름(machinename) | 사용자 컴퓨터의 이름입니다. |
| 운영 체제(os) | 사용자의 컴퓨터 또는 디바이스(또는 클라이언트 시스템에 설치된 운영 체제)입니다. |
| 소스 주소(src) | 소스 사용자의 IP 주소입니다. |
| HIP(matchname) | HIP 개체 또는 프로파일의 이름입니다. |
| 반복 수(repeatcnt) | HIP 프로파일이 일치하는 횟수입니다. |
| HIP 타입(matchtype) | HIP 필드가 HIP 오브젝트 또는 HIP 프로파일을 나타내는지의 여부입니다. |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |
| IPv6 시스템 주소(srcipv6) | 사용자의 컴퓨터 또는 디바이스의 IPv6 주소입니다. |
| 호스트 ID(hostid) | 고유 ID GlobalProtect는 호스트를 식별하기 위해 할당합니다. |
| 사용자 디바이스 일련번호(serialnumber) | 사용자의 컴퓨터 또는 디바이스의 일련번호입니다. |
| 디바이스 MAC 주소(mac) | 사용자의 컴퓨터 또는 디바이스의 MAC 주소입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |

## GlobalProtect 로그 필드

포맷: FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성 시간, 가상 시스템, 이벤트 ID, 단계, 인증 방법, 터널 유형, 소스 사용자, 소스 지역, 머신 이름, 공용 IP, 공용 IPv6, 사설 IP,


©2023 Palo Alto Networks, Inc.

Private IPv6, 호스트 ID, 일련번호, 클라이언트 버전, 클라이언트 OS, 클라이언트 OS 버전, 반복 횟수, 이유, 오류, 설명, 상태, 위치, 로그인 시간, 연결 방법, 오류 코드, 포털, 시퀀스 번호, 작업 플래그 , 고해상도 타임스탬프, 선택 유형, 응답 시간, 우선 순위, 시도된 게이트웨이, 게이트웨이, 디바이스 그룹 레이어 레벨 1, 디바이스 그룹 레이어 레벨 2, 디바이스 그룹 레이어 레벨 3, 디바이스 그룹 레이어 레벨 4, 가상 시스템 이름, 디바이스 이름, 가상 시스템 ID

| 필드 이름 | 설명 |
|---|---|
| 수신 시간(receive_time) | 관리부에서 로그를 받은 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 GLOBALPROTECT입니다. |
| 위협/콘텐츠 유형(subtype) | 위협 로그의 하위 유형입니다. 값에는 다음이 포함됩니다.<br>• 데이터 - 데이터 필터링 프로파일과 일치하는 데이터 패턴입니다.<br>• 파일 - 파일 차단 프로파일과 일치하는 파일 형식입니다.<br>• 플러드 - 영역 보호 프로파일을 통해 탐지된 플러드.<br>• 패킷 - 영역 보호 프로파일에 의해 트리거되는 패킷 기반 공격 보호입니다.<br>• 검사 - 영역 보호 프로파일을 통해 검색된 검사입니다.<br>• 스파이웨어 - 안티 스파이웨어 프로파일을 통해 탐지된 스파이웨어입니다.<br>• url - URL 필터링 로그.<br>• 바이러스 - 바이러스 백신 프로파일을 통해 탐지된 바이러스입니다.<br>• 취약점 - 취약점 보호 프로파일을 통해 탐지된 취약점 악용입니다.<br>• WildFire - 방화벽이 WildFire 분석 프로파일에 따라 WildFire에 파일을 제출할 때 생성된 WildFire 판정과 결과(로깅 대상에 따라 악성, 피싱, 그레이웨어 또는 양성)가 WildFire 제출 로그에 기록됩니다.<br>• verdict-virus - 바이러스 백신 프로파일을 통해 탐지된 바이러스입니다. |
| 생성 시간(time_generated) | 데이터 플레인에서 로그가 생성된 시간입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 이벤트 ID(eventid) | 이벤트 이름을 표시하는 문자열입니다. |
| 스테이지(stage) | 연결 단계를 표시하는 문자열(예: **before-login**, **login** 또는 **tunnel**). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
|---|---|
| 인증 방식(auth_method) | **LDAP**, **RADIUS** 또는 **SAML**과 같은 인증 유형을 표시하는 문자열입니다. |
| 터널 유형(tunnel_type) | 터널 유형(SSLVPN 또는 IPSec). |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 소스 영역(srcregion) | 세션을 시작한 사용자의 지역입니다. |
| 머신 이름(machinename) | 사용자 컴퓨터의 이름입니다. |
| 공개 IP(public_ip) | 세션을 시작한 사용자의 공용 IP 주소입니다. |
| 공용 IPv6(public_ipv6) | 세션을 시작한 사용자의 공용 IPv6 주소입니다. |
| 사설 IP(private_ip) | 세션을 시작한 사용자의 개인 IP 주소입니다. |
| 프라이빗 IPv6(private_ipv6) | 세션을 시작한 사용자의 개인 IPv6 주소입니다. |
| 호스트 ID(hostid) | GlobalProtect가 호스트를 식별하기 위해 할당하는 고유 ID입니다. |
| 일련번호(serialnumber) | 사용자 컴퓨터 또는 디바이스의 일련번호입니다. |
| 클라이언트 버전(client_ver) | 클라이언트의 GlobalProtect 앱 버전입니다. |
| 클라이언트 OS(client_os) | 클라이언트 디바이스의 OS 유형(예: Windows 또는 Linux)입니다. |
| 클라이언트 OS 버전(client_os_ver) | 클라이언트 디바이스의 OS 버전입니다. |
| 반복 수(반복) | GlobalProtect가 지난 5초 동안 감지한 소스 IP 주소, 대상 IP 주소, 애플리케이션 및 하위 유형이 동일한 세션 수입니다. |
| 이유(reason) | 격리 이유를 보여주는 문자열입니다. |
| 오류(error) | 이벤트에서 발생한 오류를 보여주는 문자열입니다. |
| 설명(opaque) | 발생한 이벤트에 대한 추가 정보입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 상태(status) | 이벤트의 상태(성공 또는 실패)입니다. |
| 위치(location) | GlobalProtect 포털 또는 게이트웨이의 관리자 정의 위치를 표시하는 문자열입니다. |
| 로그인 시간(login_duration) | 사용자가 로그인에서 로그아웃까지 GlobalProtect 게이트웨이에 연결된 시간(초)입니다. |
| 연결 방법(connect_method) | GlobalProtect 앱이 게이트웨이에 연결하는 방법을 보여주는 문자열(예: **온디맨드** 또는 **사용자 로그온**). |
| 오류 코드(error_code) | 발생한 오류와 관련된 정수입니다. |
| 포털(portal) | GlobalProtect 포털 또는 게이트웨이의 이름입니다. |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 게이트웨이 선택 방법(selection_type) | 게이트웨이에 연결하기 위해 선택한 연결 방법입니다.<br>• Manual - GlobalProtect 앱이 수동형으로 연결할 게이트웨이입니다.<br>• 기본 설정 - GlobalProtect 앱이 연결할 기본 게이트웨이입니다.<br>• Auto - 게이트웨이에 할당된 우선 순위와 응답 시간에 따라 최적의 게이트웨이에 자동으로 연결합니다. |
| SSL 응답 시간(response_time) | 터널 설정 중 엔드포인트에서 측정된 선택한 게이트웨이의 SSL 응답 시간(밀리초)입니다. |
| 게이트웨이 우선순위(priority) | GlobalProtect 앱이 연결할 수 있는 가장 높음(1), 높음(2), 중간(3), 낮음(4) 또는 가장 낮음(5)을 기반으로 하는 게이트웨이의 우선 순위입니다. |
| 시도한 게이트웨이(attempted_gateways) | 게이트웨이 이름, SSL 응답 시간 및 우선 순위를 사용하여 각 게이트웨이 연결 시도에 대해 수집되는 필드(다중 게이트웨이 구성에서 게이트웨이 우선 순위 참조). 각 필드 항목은 `g82-gateway,12,3`과 같이 쉼표로 구분됩니다. 각 게이트웨이 항목은 `g83-gateway,10,2;g84-gateway,-1,1`과 같이 세미콜론으로 구분됩니다. |
| 게이트웨이 이름(gateway) | 포털 구성에 지정된 게이트웨이의 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |

## IP 태그 로그 필드

포맷: FUTURE_USE , 수신 시간, 시리얼, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성 시간, 가상 시스템, 소스 IP, 태그 이름, 이벤트 ID, 반복 횟수, 타임아웃, 데이터 소스 이름, 데이터 소스 유형, 데이터 소스 하위 유형, 시퀀스 번호 , 작업 플래그, DG 레이어 구조 레벨 1, DG 레이어 구조 레벨 2, DG 레이어 구조 레벨 3, DG 레이어 구조 레벨 4, 가상 시스템 이름, 디바이스 이름, 가상 시스템 ID, 고해상도 타임스탬프

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | Management Plane(MP)에서 로그를 수신한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 IPTAG입니다. |
| 위협/콘텐츠 유형(subtype) | HIP 일치 로그의 하위 유형입니다(미사용). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 생성된 시간(time_generated 또는 time_generated) | 데이터플레인에서 로그가 생성된 시간입니다. |
| 가상 시스템(vsys) | HIP 매치 로그와 연결된 가상 시스템입니다. |
| 소스 IP(src) | 소스 사용자의 IP 주소입니다. |
| 태그 이름(tag_name) | 소스 IP 주소에 매핑된 태그입니다. |
| 이벤트 ID(event_id) | 이벤트 이름을 표시하는 문자열입니다. |
| 반복 수(repeatcnt) | 5초 이내에 본 소스 IP, 대상 IP, 애플리케이션 및 하위 유형이 동일한 세션 수입니다. |
| 타임아웃(timeout) | 소스 IP 주소에 대한 IP 주소-태그 매핑이 만료되기 전의 시간입니다. |
| 데이터 소스 이름(datasourcename) | 매핑 정보가 수집되는 소스의 이름입니다. |
| 데이터 소스 유형(datasource_type) | 매핑 정보가 수집되는 소스입니다. |
| 데이터 소스 하위 유형(datasource_subtype) | 데이터 소스 내에서 IP 주소-사용자 이름 매핑을 식별하는 데 사용되는 메커니즘입니다. |
| 시퀀스 번호(seqno) | 64비트 로그 입력 식별자가 순차적으로 증분됩니다. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지의 여부를 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 일련의 식별 번호입니다. 로그를 생성하는 방화벽(또는 가상 시스템)은 이 구조에 포함되지 않은 공유 디바이스 그룹(레벨 0)을 제외한 디바이스 그룹 레이어 구조의 각 상위 항목의 식별 번호를 포함합니다.<br><br>로그 값이 12, 34, 45, 0이면 디바이스 그룹 45에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되었으며 상위 그룹은 34와 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용하십시오.<br><br>API 쿼리:<br><br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |
| 고해상도 타임스탬프(high_res timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 `1969-12-31T16:00:00:000-8:00` 타임스탬프를 표시합니다. |

## 사용자 **ID** 로그 필드

유형: FUTURE_USER, 수신 시간, 일련번호, 유형, 위협 / 콘텐츠 유형, FUTURE_USE, 생성 된 시간, 가상 시스템, 소스 IP, 사용자, 데이터 소스 이름, 이벤트 ID, 반복 카운트, 타임아웃 임계값, 소스 포트, 대상 포트, 데이터 소스, 데이터 소스 유형, 시퀀스 번호, 액션 플래그, 디바이스 그룹 레이어 구조 수준 1, 디바이스 그룹 레이어 구조 수준 2, 디바이스 그룹 레이어 구조 수준 3, 디바이스 그룹 레이어 구조 수준 4, 가상 시스템 이름, 디바이스 이름, 가상 시스템 ID, 팩터 유형, 요인 완료 시간, 요인 번호, FUTURE_USE, FUTURE_USE, 사용자 그룹 플래그, 소스별 사용자, 고해상도 타임스탬프


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 USERID입니다. |
| 위협/콘텐츠 유형(subtype) | User-ID 로그의 하위 유형. 값은 로그인, 로그아웃, 레지스터 태그 및 등록 취소 태그입니다.<br>• 로그인-사용자가 로그인했습니다.<br>• 로그아웃-사용자가 로그아웃했습니다.<br>• 등록 태그-태그 또는 태그가 사용자에 대해 등록된 것을 나타냅니다.<br>• 등록 취소 태그-태그 또는 태그가 사용자에 대해 등록되지 않은 것을 나타냅니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터플레인에서 로그가 생성된 시간입니다. |
| 가상 시스템(vsys) | 구성 로그와 연결된 가상 시스템입니다. |
| 소스 IP(ip) | 원래 세션 소스 IP 주소입니다. |
| 사용자(user) | 최종 사용자를 식별합니다. |
| 데이터 소스 이름(datasourcename) | IP(포트)-사용자 매핑을 보내는 User-ID 소스입니다. |
| 이벤트 ID(eventid) | 이벤트 이름을 표시하는 문자열입니다. |
| 반복 수(repeatcnt) | 동일한 소스 IP, 대상 IP, 애플리케이션 및 하위 유형이 있는 세션 수는 5초 이내에 표시됩니다. |
| 타임아웃 임계값(timeout) | 그 후 IP/사용자 매핑이 지워집니다. |
| 소스 포트(beginport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(endport) | 세션에서 사용하는 대상 포트입니다. |
| 데이터 소스(datasource) | 매핑 정보가 수집되는 소스입니다. |
| 데이터 소스 유형(datasourcetype) | 데이터 소스 내에서 IP/사용자 매핑을 식별하는 데 사용되는 메커니즘입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 시퀀스 번호(seqno) | 로그를 생성한 방화벽의 일련번호입니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br><br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br><br>API 쿼리: **/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>** |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |
| 계수 유형(factortype) | 다중 요소 인증이 있을 때 사용자를 인증하는 데 사용되는 공급자입니다. |
| 요인 완료 시간(factorcompletiontime) | 인증이 완료된 시간입니다. |
| 요인 번호(factorno) | 기본 인증(1) 또는 추가 요인(2, 3)의 사용을 나타냅니다. |
| 사용자 그룹 플래그(ugflags) | 사용자 그룹 매핑 중에 찾은 사용자 그룹 인지의 여부를 표시합니다. 지원되는 값은 다음과 같습니다.<br>• 사용자 그룹 발견-사용자가 그룹에 매핑될 수 있는지의 여부를 나타냅니다.<br>• 중복 사용자 - 사용자 그룹에서 중복 사용자가 발견되었는지의 여부를 나타냅니다. 사용자 그룹이 없는 경우 **N/A**를 표시합니다. |
| 소스별 사용자(userbysource) | IP 주소-사용자명 매핑을 통해 소스에서 받은 사용자명을 나타냅니다. |
| 고해상도 타임스탬프(high_res timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br><br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br><br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |

## 복호화 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, 구성 버전, 생성 시간, 소스 주소, 대상 주소, NAT 소스 IP, NAT 대상 IP, 규칙, 소스 사용자, 대상 사용자, 애플리케이션, 가상 시스템, 소스 영역, 대상 영역, 인바운드 인터페이스, 아웃바운드 인터페이스, 로그작업, 로깅된 시간, 세션 ID, 반복 횟수, 소스 포트, 대상 포트, NAT 소스 포트, NAT 대상 포트, 플래그, IP 프로토콜, 작업, 터널, FUTURE_USE, FUTURE_USE, 소스 VM UUID, 대상 VM UUID, 규칙의 UUID, 클라이언트에서 방화벽까지의 단계, 서버 간 방화벽 단계, TLS 버전, 키 교환알고리즘, 암호화 알고리즘, 해시 알고리즘, 정책 이름, 타원 곡선, 오류 인덱스, 루트 상태, 체인 상태, 프록시 유형, 인증서 일련번호, 지문, 인증서 시작 날짜, 인증서 종료 날짜, 인증서 버전, 인증서 크기, 일반 이름 길이, 발급자 일반 이름 길이, 루트 공통 이름 길이, SNI 길이, 인증서 플래그, 주체 일반 이름, 발급자 주체 일반 이름, 루트 주체 일반 이름, 서버 이름 표시, 오류, 컨테이너 ID, POD 네임스페이스, POD 이름, 소스 외부 동적 목록, 대상 외부 동적 목록, 소스 동적 주소 그룹, 대상 동적 주소 그룹, 고해상도 타임스탬프, 소스 디바이스 카테고리, 소스 디바이스 프로파일, 소스 디바이스 모델, 소스 디바이스 공급업체, 소스 디바이스 OS 제품군, 소스 디바이스 OS 버전, 소스 호스트 이름, 소스 Mac 주소, 대상 디바이스 카테고리, 대상 디바이스 프로파일, 대상 디바이스 모델, 대상 디바이스 공급업체, 대상 디바이스 OS 제품군, 대상 디바이스 OS 버전, 대상 호스트 이름, 대상 Mac 주소, 시퀀스 번호, 작업 플래그, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 수준 3, 디바이스 그룹 레이어 수준 4, 가상 시스템 이름, 디바이스 이름, 가상시스템 ID, 애플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 애플리케이션 속성, 애플리케이션 컨테이너, 애플리케이션 SaaS, 애플리케이션 승인 상태


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
|---|---|
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(일련) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(유형) | 로그 유형을 지정합니다. 값은 복호화입니다. |
| 위협/콘텐츠 유형(subtype) | 복호화 로그에는 사용되지 않습니다. |
| 구성 버전(config_ver) | 소프트웨어 버전입니다. |
| 생성 시간(time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 원래 세션 소스 IP 주소입니다. |
| 대상 주소(dst) | 원래 세션 대상 IP 주소입니다. |
| NAT 소스 IP(natsrc) | 소스 NAT가 수행된 경우 사후 NAT 소스 IP 주소입니다. |
| NAT 데스티네이션 IP(natdst) | 대상 NAT가 수행된 경우 사후 NAT 대상 IP 주소입니다. |
| 규칙(rule) | 세션 트래픽을 제어하는 보안 정책 규칙입니다. |
| 소스 사용자(srcuser) | 세션을 시작한 사용자의 사용자 이름입니다. |
| 대상 사용자(dstuser) | 세션이 대상으로 지정된 사용자의 사용자 이름입니다. |
| 애플리케이션(app) | 세션과 연결된 애플리케이션입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션이 소싱된 영역입니다. |
| 대상 영역(to) | 세션이 예정된 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 로그 액션(logset) | 세션에 적용된 로그 포워딩 프로파일입니다. |
| 기록 시간(time_received) | 로그를 수신한 시간입니다. |
| 세션 ID(sessionid) | 각 세션에 적용되는 내부 숫자 식별자입니다. |
| 반복 수(repeatcnt) | 소스 IP, 대상 IP, 애플리케이션 및 콘텐츠/위협 유형이 5초 내에 동일한 세션 수입니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| NAT 소스 포트(natsport) | Post-NAT 소스 포트입니다. |
| NAT 대상 포트(natdport) | NAT 이후 대상 포트입니다. |
| 플래그(flags) | 세션에 대한 세부 정보를 제공하는 32비트 필드입니다. 이 필드는 로깅된 값으로 값을 AND 지정하여 디코딩할 수 있습니다.<br>• 0x80000000 - 세션에 패킷 캡처(PCAP)가 있습니다.<br>• 0x40000000 - 클라이언트가 여러 경로를 사용하여 대상 호스트에 연결할 수 있도록 하는 옵션이 활성화됩니다.<br>• 0x20000000 - 판단을 위해 파일이 와일드파이어에 제출됨<br>• 0x10000000 - 최종 사용자에 의한 엔터프라이즈 자격 증명 제출이 감지됨<br>• 0x08000000 - 흐름의 소스가 허용 목록에 있으며 정찰 보호 대상이 아닙니다.<br>• 0x02000000 - IPv6 session<br>• 0x01000000 - SSL 세션의 암호가 복호화됩니다(SSL 프록시).<br>• 0x00800000—URL 필터링을 통해 세션이 거부되었습니다.<br>• 0x00400000—세션에 NAT 변환이 수행되었습니다.<br>• 0x00200000—세션에 대한 사용자 정보가 인증 포털을 통해 캡처되었습니다.<br>• 0x00100000—애플리케이션 트래픽이 비표준 대상 포트에 있습니다.<br>• 0x00080000 —X-포워딩됨-프록시의 값이 소스 사용자 필드에 있음<br>• 0x00040000—로그는 http 프록시 세션 내의 트랜잭션에 해당합니다(프록시 트랜잭션). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • 0x00020000—클라이언트-서버 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00010000—서버 대 클라이언트 흐름은 정책 기반 포워딩의 적용을 받습니다.<br>• 0x00008000—세션이 컨테이너 페이지 액세스임(컨테이너 페이지)<br>• 0x00002000—세션이 암시적 애플리케이션 종속성 처리에 대한 규칙과 일시적으로 일치합니다. PAN-OS 5.0.0 이상에서 사용할 수 있습니다.<br>• 0x00000800—대칭 반환은 이 세션의 트래픽을 포워딩하는 데 사용됩니다.<br>• 0x00000400 - 복호화된 트래픽이 미러 포트를 통해 일반 텍스트로 전송되고 있습니다.<br>• 0x00000100—외부 터널의 탑재량을 검사하는 중입니다. |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 가능한 값은 다음과 같습니다.<br>• allow—정책에 의해 세션이 허용됨<br>• deny—정책에 의해 세션이 거부되었습니다.<br>• drop - 세션이 자동으로 삭제되었습니다.<br>• drop ICMP - 호스트 또는 애플리케이션에 ICMP 연결할 수 없는 메시지와 함께 세션이 자동으로 삭제되었습니다.<br>• reset both - 세션이 종료되고 TCP 재설정이 연결의 양쪽으로 전송됩니다.<br>• 클라이언트 재설정 - 세션이 종료되고 TCP 재설정이 클라이언트로 전송되었습니다.<br>• reset server - 세션이 종료되고 TCP 재설정이 서버로 전송됩니다 |
| 터널(tunnel) | 터널 유형. |
| 소스 VM UUID(src_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 소스 범용 고유 식별자입니다. |
| 대상 VM UUID(dst_uuid) | VMware NSX 환경에서 게스트 가상 시스템에 대한 대상 범용 고유 식별자입니다. |
| 규칙에 대한 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 클라이언트에서 방화벽으로 연결되는 단계(hs_stage_c2f) | 클라이언트에서 방화벽으로 연결되는 TLS 핸드쉐이크 단계(예: 클라이언트 인사말, 서버 인사말, 인증서, 클라이언트/서버 키 교환 등) |
| 방화벽 대 서버 단계(hs_stage_f2s) | 방화벽에서 서버로의 TLS 핸드쉐이크 단계입니다. |
| TLS 버전(tls_버전) | 세션에 사용되는 TLS 프로토콜 버전입니다. |
| 키 교환 알고리즘(tls_keyxchg) | 세션에 사용되는 키 교환 알고리즘입니다. |
| 암호화 알고리즘(tls_enc) | AES-128-CBC, AES-256-GCM 등과 같은 세션 데이터를 암호화하는 데 사용되는 알고리즘입니다. |
| 해시 알고리즘(tls_auth) | 세션에 사용되는 인증 알고리즘(예: SHA, SHA256, SHA384 등)입니다. |
| 정책 이름(policy_name) | 세션과 연결된 복호화 정책의 이름입니다. |
| 타원 곡선(ec_curve) | 클라이언트와 서버가 협상하고 ECDHE 암호 제품군을 사용하는 연결에 사용하는 타원 암호화 곡선입니다. |
| 오류 인덱스(err_index) | 발생한 오류 유형: 암호, 리소스, 다시 시작, 버전, 프로토콜, 인증서, 기능 또는 HSM |
| 루트 상태(root_status) | 루트 인증서의 상태(예: 신뢰할 수 있음, 신뢰할 수 없음 또는 검사되지 않음)입니다. |
| 체인 상태(chain_status) | 체인이 신뢰할 수 있는지의 여부. 값은 다음과 같습니다.<br>• 검사되지 않음<br>• 언트러스티드(Untrusted)<br>• 트러스티드(Trusted)<br>• 불완전 |
| 프록시 유형(proxy_type) | 복호화 프록시 유형(예: 포워드 프록시의 경우 포워딩, 인바운드 검사의 경우 인바운드, 복호화되지 않은 트래픽의 경우 비복호화, GlobalProtect 등) |
| 인증서 일련 번호(cert_serial) | 인증서의 고유 식별자입니다(인증서 발급자가 생성함). |
| 인증서 지문(fingerprint) | x509 바이너리 형식의 인증서 해시입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
|---|---|
| 인증서 시작 날짜(notbefore) | 인증서가 유효하게 된 시간입니다(이 시간 이전에 인증서가 유효하지 않음). |
| 인증서 종료 날짜(notafter) | 인증서가 만료되는 시간입니다(이 시간 이후에는 인증서가 유효하지 않게 됨). |
| 인증서 버전(cert_ver) | 인증서 버전(V1, V2 또는 V3) 입니다. |
| 인증서 크기(cert_size) | 인증서 키 크기입니다. |
| 일반 이름 길이(cn_len) | 주체 일반 이름의 길이입니다. |
| 발급자 일반 이름 길이(issuer_len) | 발급자 일반 이름의 길이입니다. |
| 루트 일반 이름 길이(rootcn_len) | 루트 공통 이름의 길이입니다. |
| SNI 길이(sni_len) | 서버 이름 표시(hostname)의 길이입니다. |
| 인증서 플래그(cert_flags) | 인증서 플래그는 7개의 값을 반환할 수 있습니다.<br>• 세션이 재개되었습니다(b_resume_session).<br>• 인증서(주체) 일반 이름이 잘림(b_issuer_cn_truncated)<br>• 발급자 일반 이름이 잘렸습니다(b_issuer_cn_truncated림).<br>• 루트 일반 이름이 잘립니다(b_root_cn_truncated).<br>• 서버 이름 표시(SNI)가 잘렸습니다(b_sni_truncated).<br>• 인증서 유형, RSA 또는 ECDSA(b_cert_type)<br>• 미사용(padding3) |
| 주체 일반 이름(cn) | 도메인 이름(인증서가 보호하는 서버의 이름) |
| 발급자 일반 이름(issuer_cn) | 인증서의 내용을 확인한 조직의 이름입니다. |
| 루트 일반 이름(root_cn) | 루트 인증 기관의 이름입니다. |
| 서버 이름 표시 (sni) | 클라이언트가 연결하려는 서버의 호스트 이름입니다. SNI를 사용하면 각 웹 사이트에 고유한 SNI가 있으므로 서버에서 여러 웹사이트를 호스팅하고 동일한 IP 주소 및 TCP 포트에 여러 인증서를 표시할 수 있습니다. |
| 오류(error) | 이벤트에서 발생한 오류를 보여 주는 문자열입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
|---|---|
| 컨테이너 ID(container_id) | 방화벽이 클라우드 컨테이너에서 실행되는 경우 컨테이너를 식별하는 고유한 영숫자 문자열입니다. |
| POD 네임스페이스(pod_namespace) | 쿠버네티스 파드 네임스페이스의 이름. |
| 포드 이름(pod_name) | 쿠버네티스 파드의 이름. |
| 소스 외부 동적 목록(src_edl) | 트래픽의 원본 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 대상 외부 동적 목록(dst_edl) | 트래픽의 대상 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 원본 동적 주소 그룹(src_dag) | Device-ID가 트래픽의 소스로 식별하는 동적 주소 그룹입니다. |
| 대상 동적 주소 그룹(dst_dag) | Device-ID가 트래픽의 대상으로 식별하는 동적 주소 그룹입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 필드의 형식은 YYYY-MM-DDTHH:SS:SSSTZD입니다.<br>• **YYYY**—4자리 연도<br>• **MM** - 두 자릿수 의 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 소스 디바이스 카테고리(src_category) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 카테고리입니다. |
| 소스 디바이스 프로파일(src_profile) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 소스 디바이스 모델(src_model) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 모델입니다. |
| 소스 디바이스 공급업체(src_vendor) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 공급업체입니다. |
| 소스 디바이스 OS 패밀리(src_osfamily) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 유형입니다. |
| 소스 디바이스 OS 버전(src_osversion) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 버전입니다. |
| 소스 호스트 이름(src_host) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 호스트 이름입니다. |
| 소스 MAC 주소(src_mac) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 MAC 주소입니다. |
| 대상 디바이스 카테고리(dst_category) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 카테고리입니다. |
| 대상 디바이스 프로파일(dst_profile) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 대상 디바이스 모델(dst_model) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 모델입니다. |
| 대상 디바이스 공급업체(dst_vendor) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 벤더입니다. |
| 대상 디바이스 OS 제품군(dst_osfamily) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 유형입니다. |
| 대상 디바이스 OS 버전(dst_osversion) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 운영 체제 버전입니다. |
| 대상 호스트 이름(dst_host) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 호스트 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 대상 MAC 주소(dst_mac) | Device-ID가 트래픽의 대상으로 식별하는 디바이스의 MAC 주소입니다. |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자입니다. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |
| 애플리케이션 카테고리(카테고리_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • saas |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 **1**을 표시하고 SaaS 애플리케이션이 아닌 경우 **0**을 표시합니다. |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 신청이 승인되면 **1**을 표시하고 신청이 승인되지 않은 경우 **0**을 표시합니다. |

## 터널 검사 로그 필드

형식: FUTURE_USE, 수신 시간, 일련번호, 유형, 하위 유형, FUTURE_USE, 생성된 시간, 소스 주소, 대상 주소, NAT 소스 IP, NAT 대상 IP, 규칙 이름, 소스 사용자, 대상 사용자, 애플리케이션, 가상 시스템, 소스 영역, 대상 영역, 인바운드 인터페이스, 아웃 바운드 인터페이스, 로그 작업, FUTURE_USE, 세션 ID, 반복 카운트, 소스 포트, 대상 포트, NAT 소스 포트, NAT 대상 포트, 플래그, 프로토콜, 작업, 심각도, 서열 번호, 작업 플래그, 소스 위치, 대상 위치, 디바이스 그룹 레이어 구조 수준 1, 디바이스 그룹 레이어 구조 수준 2, 디바이스 그룹 레이어 구조 수준 3, 디바이스 그룹 레이어 구조 수준 4, 가상 시스템 이름, 디바이스 이름, 터널 ID/IMSI, 모니터 태그/IMEI, 부모 요소 세션 ID, 부모 요소 시작 시간, 터널, 바이트, 바이트, 보낸 바이트, 바이트, 바이트 수신, 패킷, 패킷 전송, 패킷 수신, 최대 캡슐화, 알 수없는 프로토콜, 엄격한 검사, 터널 조각, 세션 생성, 세션 폐쇄, 세션 종료 이유, 작업 소스, 시작 시간, 경과 시간, 터널 검사 규칙, 원격 사용자 IP, 원격 사용자 ID, 규칙 UUID, PCAP ID, 동적 사용자 그룹, 소스 외부 동적 목록, 대상 외부 동적 목록, 고해상도 타임스탬프, 슬라이스 문자, A 슬라이스 문자, 슬라이스 문자, A 슬라이스 문자, PDU 세션 ID, 애플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 애플리케이션 특성, 애플리케이션 컨테이너, 애플리케이션 SaaS, 애플리케이션 제재 상태


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | Management Plane(MP)에서 로그를 수신한 월, 일 및 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 세션과 관련된 로그 유형: 시작 또는 종료. |
| 위협/콘텐츠 유형(subtype) | 트래픽 로그의 하위 유형 값은 시작, 종료, 삭제 및 거부입니다.<br>• 시작 - 세션 시작됨<br>• 종료 - 세션이 종료됨<br>• 삭제 - 애플리케이션이 식별되기 전에 삭제된 세션이며 세션을 허용하는 규칙이 없습니다.<br>• 거부 - 애플리케이션이 식별된 후 세션이 삭제되고 차단 규칙이 있거나 세션을 허용하는 규칙이 없습니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 세션에 있는 패킷의 소스 IP 주소입니다. |
| 대상 주소(dst) | 세션에 있는 패킷의 대상 IP 주소입니다. |
| NAT 소스 IP(natsrc) | 소스 NAT가 수행된 경우 사후 NAT 소스 IP 주소입니다. |
| NAT 데스티네이션 IP(natdst) | 대상 NAT가 수행된 경우 사후 NAT 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션에 적용되는 보안 정책 규칙의 이름입니다. |
| 소스 사용자(srcuser) | 세션에서 패킷의 소스 사용자 ID입니다. |
| 대상 사용자(dstuser) | 세션에서 패킷의 대상 사용자 ID입니다. |
| 애플리케이션(app) | 세션에서 사용되는 터널링 프로토콜입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션에 있는 패킷의 소스 영역입니다. |
| 대상 영역(to) | 세션에 있는 패킷의 대상 영역입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |
| 세션 ID(sessionid) | 기록 중인 세션의 세션 ID입니다. |
| 반복 수(반복) | 동일한 소스 IP, 대상 IP, 애플리케이션 및 하위 유형이 있는 세션 수는 5초 이내에 표시됩니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| NAT 소스 포트(natsport) | Post-NAT 소스 포트입니다. |
| NAT 대상 포트(natdport) | NAT 이후 대상 포트입니다. |
| 플래그(flags) | 세션에 대한 세부 정보를 제공하는 32비트 필드입니다. 이 필드는 로깅된 값으로 값을 AND 지정하여 디코딩할 수 있습니다.<br>• 0x80000000 - 세션에는 패킷 캡처(PCAP)가 있습니다.<br>• 0x02000000 - IPv6 세션<br>• 0x01000000 - SSL 세션이 복호화되었습니다(SSL 프록시)<br>• 0X00800000 - 세션은 URL 필터링을 통해 거부되었습니다.<br>• 0x00400000 - 세션에 NAT 번역이 수행됩니다(NAT)<br>• 0x00200000 - 세션에 대한 사용자 정보가 인증 포털을 통해 캡처되었습니다.<br>• 0x00080000 - X-포워딩됨-프록시의 값이 소스 사용자 필드에 있음<br>• 0x00040000 - log는 http 프록시 세션 내의 트랜잭션에 해당합니다(프록시 트랜잭션).<br>• 0x00008000 - 세션이 컨테이너 페이지 액세스입니다(컨테이너 페이지).<br>• 0x00002000 - 세션이 암시적 애플리케이션 종속성 처리에 대한 규칙과 일시적으로 일치합니다. PAN-OS 5.0.0 이상에서 사용할 수 있습니다.<br>• 0x00000800 - 대칭 반환은 이 세션의 트래픽을 포워딩하는 데 사용되었습니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 가능한 값은 다음과 같습니다.<br>• 허용-세션은 정책에 의해 허용되었습니다.<br>• 거부- 세션은 정책에 의해 거부되었습니다.<br>• 드롭-세션은 알림 없이 삭제되었습니다.<br>• ICMP 드롭- ICMP에 연결할 수 없는 메시지로 세션이 자동으로 삭제되었습니다.<br>• 두 세션 재설정- 세션이 종료되고 TCP 재설정이 연결의 양쪽으로 전송됩니다.<br>• 클라이언트 재설정- 세션이 종료되고 TCP 재설정이 클라이언트로 전송됩니다.<br>• 서버 재설정- 세션이 종료되고 TCP 재설정이 서버로 전송됩니다. |
| 심각도(severity) | 이벤트와 관련된 심각도 값은 정보 제공, 낮음, 중간, 높음, 중요입니다. |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. 이 필드는 PA-7000 시리즈 방화벽에서 지원되지 않습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 소스 위치(srcloc) | 개인 주소의 출처 국가 또는 내부 지역 최대 길이는 32바이트입니다. |
| 대상 위치(dstloc) | 개인 주소의 경우 대상 국가 또는 내부 지역입니다. 최대 길이는 32바이트입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=`<br><show><dg-hierarchy></dg-hierarchy></show> |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 터널 ID(tunnelid) | 검사 중인 터널의 ID 또는 모바일 사용자의 IMSI(International Mobile Subscriber Identity) ID입니다. |
| 모니터 태그(monitortag) | 터널 검사 정책 규칙 또는 모바일 디바이스의 국제 모바일 장비 ID(IMEI) ID에 대해 구성한 이름을 모니터링합니다. |
| 부모 요소 세션 ID(parent_session_id) | 이 세션이 터널링되는 세션의 ID입니다. 내부 터널(두 수준의 터널링인 경우) 또는 내부 내용(한 수준의 터널링인 경우)에만 적용됩니다. |
| 부모 요소 시작 시간(parent_start_time) | 년/월/일 시간:분:초, 부모 요소 터널 세션이 시작된 시입니다. |
| 터널 유형(tunnel) | GRE 또는 IPsec과 같은 터널 유형입니다. |
| 바이트(bytes) | 세션의 바이트 수입니다. |
| 보낸 바이트(bytes_sent) | 세션의 클라이언트에서 서버로의 바이트 수입니다. |
| 수신된 바이트(bytes_received) | 세션의 서버-클라이언트 방향의 바이트 수입니다. |
| 패킷(packets) | 세션의 총 패킷 수(전송 및 수신). |
| 보낸 패킷(pkts_sent) | 세션에 대한 클라이언트-서버 패킷 수입니다. |
| 수신된 패킷(pkts_received) | 세션에 대한 서버-클라이언트 패킷 수입니다. |
| 최대 캡슐화(max_encap) | 패킷이 터널 검사 정책 규칙에서 구성된 최대 캡슐화 수준을 초과했기 때문에 방화벽이 삭제한 패킷 수(최대 터널 검사 수준 이상 인 경우 패킷을 드롭). |
| 알 수 없는 프로토콜(unknown_proto) | 터널 검사 정책 규칙(터널 내부의 알 수 없는 프로토콜인 경우 패킷을 드롭)에서 활성화된 알 수 없는 프로토콜을 포함하기 때문에 방화벽이 삭제한 패킷 수입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 엄격한 검사(strict_check) | 패킷의 터널 프로토콜 헤더가 터널 프로토콜에 대한 RFC를 준수하지 못했기 때문에 방화벽이 삭제된 패킷수(터널 검사 정책 규칙에서 활성화된 경우 패킷을 드롭). |
| 터널 조각(tunnel_fragment) | 조각화 오류로 인해 방화벽이 삭제된 패킷 수입니다. |
| 생성된 세션(sessions_created) | 생성된 내부 세션 수입니다. |
| 세션 종료(sessions_closed) | 완료/닫힌 세션 수입니다. |
| 세션 종료 이유(session_end_reason) | 세션이 종료된 이유입니다. 종료 원인이 여러 개인 경우 이 필드에는 가장 높은 우선 순위 이유만 표시됩니다. 가능한 세션 종료 이유 값은 우선 순위(첫 번째가 가장 높음)에 따라 다음과 같습니다.<br>• 위협 - 방화벽이 재설정, 삭제 또는 차단(IP 주소) 작업과 관련된 위협을 감지했습니다.<br>• policy-deny - 세션이 거부 또는 삭제 작업이 있는 보안 규칙과 일치했습니다.<br>• 복호화-인증-유효성 검사- 세션이 클라이언트 인증을 사용할 때 또는 세션이 만료, 신뢰할 수 없는 발급자, 알 수 없는 상태 또는 상태 확인 시간 종료와 같은 조건 중 어느 것이 있는 서버 인증서를 사용할 때 SSL 전방 프록시 복호화 또는 SSL 인바운드 검사를 차단하도록 방화벽을 구성했기 때문에 세션이 종료되었습니다. 이 세션 종료 이유는 서버 인증서가 bad_certificate, unsupported_certificate, certificate_revoked, access_denied 또는 no_certificate_RESERVED(SSLv3만)의 치명적인 오류 경고를 생성하는 경우에도 표시됩니다.<br>• Decrypt-unsupport-param - 세션이 지원되지 않는 프로토콜 버전, 암호 또는 SSH 알고리즘을 사용할 때 SSL 포워드 프록시 복호화 또는 SSL 인바운드 검사를 차단하도록 방화벽을 구성했기 때문에 세션이 종료되었습니다. 이 세션 종료 이유는 세션이 unsupported_extension, expected_message 또는 handshake_failure 유형의 치명적인 오류 경고를 생성할 때 표시됩니다.<br>• 복호화 오류 - 방화벽 리소스 또는 하드웨어 보안 모듈(HSM)을 사용할 수 없을 때 SSL 포워드 프록시 복호화 또는 SSL 인바운드 검사를 차단하도록 방화벽을 구성했기 때문에 세션이 종료되었습니다. 이 세션 종료 이유는 암호 해독-인증서 유효성 검사 및 암호 해독-비지원-매개변수 종료 이유에 대해 나열되지 않은 치명적인 오류 경고를 생성하거나 SSH 오류가 있는 SSL 트래픽을 차단하도록 방화벽을 구성한 경우에도 표시됩니다.<br>• tcp-rst-from-client - 클라이언트가 서버에 TCP 재설정을 보냈습니다.<br>• tcp-rst-from-server - 서버가 클라이언트에 TCP 재설정을 보냈습니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | • resources-unavailable - 시스템 리소스 제한으로 인해 세션이 삭제되었습니다. 예를 들어, 세션이 흐름당 허용되는 비순차 패킷 수 또는 글로벌 비순차 패킷 대기열을 초과했을 수 있습니다.<br>• tcp-fin- 연결의 호스트 하나 또는 두 호스트가 세션을 닫기 위해 TCP FIN 메시지를 보냈습니다.<br>• tcp-reuse - 세션이 재사용되고 방화벽이 이전 세션을 닫습니다.<br>• decoder - 디코더는 프로토콜 내에서 새로운 연결(예: HTTP-Proxy)을 감지하고 이전 연결을 종료합니다.<br>• old-out - 세션이 만료되었습니다.<br>• unknown - 이 값은 다음 상황에 적용됩니다.<br>  • 앞의 이유가 다루지 않는 세션 종료(예: **clear session all** 명령).<br>  • 세션 최종 이유 필드(PAN-OS 6.1보다 오래된 릴리스)를 지원하지 않는 PAN-OS 릴리스에서 생성된 로그의 경우 현재 PAN-OS 릴리스로 업그레이드한 후 또는 로그를 방화벽에 로드한 후 값을 **알 수 없습니다**.<br>  • Panorama에서 PAN-OS 버전이 세션 종료 이유를 지원하지 않는 방화벽에서 받은 로그는 **알 수 없는** 값을 갖습니다.<br>• 해당 없음 - 이 값은 트래픽 로그 유형이 **끝나지** 않을 때 적용됩니다. |
| 작업 소스(action_source) | 애플리케이션을 허용하거나 차단하기 위해 취한 조치가 애플리케이션 또는 정책에 정의되었는지의 여부를 지정합니다. 작업은 세션에 대한 허용, 거부, 삭제, 서버 재설정, 클라이언트 재설정 또는 둘 다 재설정이 될 수 있습니다. |
| 시작 시간(시작) | 세션이 시작된 연도/월/일 시간:분:초. |
| 경과 시간(경과) | 세션의 경과 시간입니다. |
| 터널 검사 규칙(tunnel_insp_rule) | 클리어텍스트 터널 트래픽과 일치하는 터널 검사 규칙의 이름입니다. |
| 원격 사용자 IP(remote_user_ip) | 원격 사용자의 IPv4 또는 IPv6 주소입니다. |
| 원격 사용자 ID(remote_user_id) | 원격 사용자의 IMSI ID 및 사용 가능한 경우 하나의 IMEI ID 또는 하나의 MSISDN ID. |
| 보안 규칙 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| PCAP ID(pcap_id) | 방화벽에서 pcap 파일의 위치를 정의하는 고유한 패킷 캡처 ID입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 동적 사용자 그룹 이름(dynusergroup_name) | 세션을 시작한 사용자가 포함된 동적 사용자 그룹의 이름입니다. |
| 소스 외부 동적 목록(src_edl) | 트래픽의 원본 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 대상 외부 동적 목록(dst_edl) | 트래픽의 대상 IP 주소를 포함하는 외부 동적 목록의 이름입니다. |
| 고해상도 타임스탬프(high_res timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00.000-8:00* 타임스탬프를 표시합니다. |
| 슬라이스 차별화기(nssai_sd) | 네트워크 슬라이스 ID의 슬라이스 구분자입니다. |
| 슬라이스 서비스 유형(nssai_sd) | 네트워크 슬라이스 ID의 A 슬라이스 서비스 유형입니다. |
| PDU 세션 ID(pdu_session_id) | 터널 내부의 L4 세그먼트 컬렉션에 대한 세션 ID입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 애플리케이션 카테고리(category_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking<br>• saas |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 **1**을 표시하고 SaaS 애플리케이션이 아닌 경우 **0**을 표시합니다. |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 애플리케이션이 승인되면 **1**을 표시하고 애플리케이션이 승인되지 않은 경우 **0**을 표시합니다. |

## SCTP 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, FUTURE_USE, FUTURE_USE, 생성된 시간, 소스 주소, 대상 주소, FUTURE_USE, FUTURE_USE, 규칙 이름, FUTURE_USE, FUTURE_USE, FUTURE_USE, 가상 시스템, 소스 영역, 대상 영역, 인바운드 인터페이스, 아웃바운드 인터페이스 , 로그 작업, FUTURE_USE, 세션 ID, 반복 횟수, 소스 포트, 대상 포트, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, IP 프로토콜, 작업, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 수준 3, 디바이스 그룹 레이어 구조 레벨 4, 가상 시스템 이름, 디바이스 이름, 시퀀스 번호, FUTURE_USE, SCTP 연결 ID, 페이로드 프로토콜 ID, 심각도, SCTP 청크 유형,

 ©2023 Palo Alto Networks, Inc.

FUTURE_USE, SCTP 확인 태그 1, SCTP 확인 태그 2, SCTP 원인 코드, 직경 앱 ID , 직경 명령 코드, 직경 AVP 코드, SCTP 스트림 ID, SCTP 연결 종료 이유, Op 코드, SCCP 발신자 SSN, SCCP 발신자 전체 제목, SCTP 필터, SCTP 청크, SCTP 청크 전송, SCTP 청크 수신 ived, 패킷, 보낸 패킷, 수신된 패킷, 규칙에 대한 UUID, 고해상도 타임스탬프

| 필드 이름 | 설명 |
|---|---|
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 SCTP입니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 원래 세션 소스 IP 주소입니다. |
| 대상 주소(dst) | 원래 세션 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션에 적용되는 보안 정책 규칙의 이름입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션이 소싱된 영역입니다. |
| 대상 영역(to) | 세션이 예정된 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |
| 세션 ID(sessionid) | 각 세션에 적용되는 내부 숫자 식별자입니다. |
| 반복 수(repeatcnt) | 동일한 소스 IP, 대상 IP, 애플리케이션 및 하위 유형이 있는 세션 수는 5초 이내에 표시됩니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 가능한 값은 다음과 같습니다.<br>• 허용 - 정책에서 세션을 허용했습니다.<br>• 거부 - 정책에 의해 세션이 거부되었습니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| SCTP 연결 ID(assoc_id) | 각 SCTP 연결에 적용되는 내부 56비트 숫자 논리 식별자입니다. |
| 페이로드 프로토콜 ID(ppid) | 이 이벤트를 트리거한 데이터 청크에서 PPID(페이로드 프로토콜 ID)를 식별합니다. PPID는 IANA(Internet Assigned Numbers Authority)에서 할당합니다. |
| 심각도(severity) | 이벤트와 관련된 심각도 값은 정보 제공, 낮음, 중간, 높음, 중요입니다. |
| SCTP 청크 유형(sctp_chunk_type) | 제어 또는 데이터와 같이 청크에 포함된 정보 유형을 설명합니다. |
| SCTP 이벤트 유형(sctp_event_type) | SCTP 보호 프로파일이 SCTP 트래픽에 적용될 때 SCTP 청크 또는 패킷별로 트리거되는 이벤트를 정의합니다. 또한 SCTP 연결의 시작 또는 종료에 의해 트리거됩니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| SCTP 확인 태그 1(verif_tag_1) | 수신된 SCTP 패킷이 현재 SCTP 연결에 속하는지 확인하고 endpoint2의 유효성을 검사하기 위해 연결을 시작하는 endpoint1에서 사용합니다. |
| SCTP 확인 태그 2(verif_tag_2) | 수신된 SCTP 패킷이 현재 SCTP 연결에 속하는지 확인하고 endpoint1의 유효성을 검사하기 위해 endpoint2에서 사용합니다. |
| SCTP 원인 코드(sctp_cause_code) | 동일한 SCTP 연결의 다른 엔드포인트에 오류 조건의 이유를 지정하기 위해 엔드포인트에서 보냅니다. |
| 다이어미터 앱 ID(diam_app_id) | 이벤트를 트리거한 데이터 청크의 직경 애플리케이션입니다. Diameter 애플리케이션 ID는 IANA(Internet Assigned Numbers Authority)에서 할당합니다. |
| 지름 명령 코드(diam_cmd_code) | 이벤트를 트리거한 데이터 청크의 직경 명령 코드입니다. 직경 명령 코드는 IANA(Internet Assigned Numbers Authority)에서 할당합니다. |
| 직경 AVP 코드(diam_avp_code) | 이벤트를 트리거한 데이터 청크의 직경 AVP 코드입니다. |
| SCTP 스트림 ID(stream_id) | 이벤트를 트리거한 데이터 청크를 포워딩하는 스트림의 ID입니다. |
| SCTP 연결 종료 이유(assoc_end_reason) | 연결이 종료된 이유입니다. 종료 원인이 여러 개인 경우 우선 순위가 가장 높은 이유가 표시됩니다. 내림차순 우선 순위에서 가능한 세션 종료 이유는 다음과 같습니다.<br>• shutdown-from-endpoint(최고) - 엔드포인트가 **SHUTDOWN**을 전송합니다.<br>• abort-from-endpoint - 엔드포인트가 **ABORT**를 보냅니다.<br>• unknown(최저) - 연결이 만료되었거나 연결 종료 이유가 과거의 이유 중 하나로 처리되지 않았습니다(예: 모든 세션 종료 명령). |
| 연산 코드(op_code) | 이벤트를 트리거한 데이터 청크에서 MAP 또는 CAP와 같은 애플리케이션 레이어 SS7 프로토콜의 작동 코드를 식별합니다. |
| SCCP 발신자 SSN(sccp_calling_ssn) | 이벤트를 트리거한 데이터 청크의 SCCP(Signaling Connection Control Part) 발신자 하위 시스템 번호(SSN)입니다. |
| SCCP 발신자 전체 제목(sccp_calling_gt) | 이벤트를 트리거한 데이터 청크의 SCCP(Signaling Connection Control Part) 발신자 GT(Global Title). |
| SCTP 필터(sctp_filter) | SCTP 청크가 일치하는 필터의 이름입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| SCTP 청크(chunks) | 연결에 대한 총 청크(전송 및 수신) 수입니다. |
| SCTP 청크 전송(chunks_sent) | 연결을 위한 endpoint1(연결을 시작함)-endpoint2 청크의 수입니다. |
| SCTP 청크 수신(chunks_received) | 연결에 대한 endpoint2-to-endpoint1(연결 시작) 청크의 수입니다. |
| 패킷(packets) | 세션의 총 패킷 수(전송 및 수신). |
| 보낸 패킷(pkts_sent) | 세션에 대한 클라이언트-서버 패킷 수입니다. |
| 수신된 패킷(pkts_received) | 세션에 대한 서버-클라이언트 패킷 수입니다. |
| 규칙에 대한 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00:000-8:00* 타임스탬프를 표시합니다. |

## 인증 로그 필드

포맷**:** FUTURE_USE, 수신 시간, 일련번호, 유형, 위협 / 콘텐츠 유형, FUTURE_USE, 생성된 시간, 가상 시스템, 소스 IP, 사용자, 정규화 사용자, 개체, 인증 정책, 반복 카운트, 인증 ID, 공급 업체, 로그 액션, 서버 프로파일, 설명, 클라이언트 유형, 이벤트 유형, 요인 번호, 시퀀스 번호, 액션 플래그, 디바이스 그룹 레이어


©2023 Palo Alto Networks, Inc.

구조 1, 디바이스 그룹 레이어 구조 2, 디바이스 그룹 레이어 구조 3, 디바이스 그룹 레이어 구조 4, 가상 시스템 이름, 디바이스 이름, 가상 시스템 ID, 인증 프로토콜, 규칙에 대한 UUID, 고해상도 타임스탬프, 소스 디바이스 카테고리, 소스 디바이스 프로파일, 소스 디바이스 모델, 소스 디바이스 공급 업체, 소스 디바이스 OS 패밀리, 소스 디바이스 OS 버전, 소스 호스트 이름, 소스 Mac 주소, 리전, FUTURE_USE, 사용자 에이전트, 세션 ID

| 필드 이름 | 설명 |
|---|---|
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 디바이스의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 인증입니다. |
| 위협/콘텐츠 유형(subtype) | 시스템 로그의 하위 유형: 로그를 생성하는 시스템 데몬을 지칭합니다. 값은 crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn입니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 IP(ip) | 원래 세션 소스 IP 주소입니다. |
| 사용자(user) | 최종 사용자가 인증됩니다. |
| 사용자 정규화(normalize_user) | 인증되는 사용자 이름의 정규화된 버전(예: 사용자 이름에 도메인 이름을 부수기). |
| 개체(object) | 시스템 이벤트와 연결된 개체의 이름입니다. |
| 인증 정책(authpolicy) | 보호된 리소스에 대한 액세스를 허용하기 전에 인증을 위해 호출된 정책입니다. |
| 반복 횟수(repeatcnt) | 동일한 소스 IP, 대상 IP, 애플리케이션 및 하위 유형이 있는 세션 수는 5초 이내에 표시됩니다. |
| 인증 ID(authid) | 기본 인증 및 추가(다중 요소) 인증에 걸쳐 제공되는 고유 ID입니다. |
| 공급업체(vendor) | 추가 요소 인증을 제공하는 공급업체입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 서버 프로파일(serverprofile) | 인증에 사용되는 인증 서버입니다. |
| 설명(desc) | 추가 인증 정보입니다. |
| 클라이언트 유형(clienttype) | 인증 포털과 같은 인증을 완료하는 데 사용되는 클라이언트 유형입니다. |
| 이벤트 유형(event) | 인증 시도의 결과입니다. |
| 요인 번호(factorno) | 기본 인증(1) 또는 추가 요인(2, 3)의 사용을 나타냅니다. |
| 시퀀스 번호(seqno) | 64비트 로그 입력 식별자가 순차적으로 증분됩니다. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |
| 인증 프로토콜(authproto) | 서버에서 사용하는 인증 프로토콜을 나타냅니다. 예를 들어, GTC와 PEAP입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 규칙에 대한 UUID(rule_uuid) | 규칙을 영구적으로 식별하는 UUID입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 시간(밀리초)입니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 의 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 ***1969-12-31T16:00:00:000-8:00*** 타임스탬프를 표시합니다. |
| 소스 디바이스 카테고리(src_category) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 카테고리입니다. |
| 소스 디바이스 프로파일(src_profile) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 디바이스 프로파일입니다. |
| 소스 디바이스 모델(src_model) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 모델입니다. |
| 소스 디바이스 공급업체(src_vendor) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 공급업체입니다. |
| 소스 디바이스 OS 패밀리(src_osfamily) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 유형입니다. |
| 소스 디바이스 OS 버전(src_osversion) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 운영 체제 버전입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
|---|---|
| 소스 호스트 이름(src_host) | Device-ID가 트래픽의 소스로 식별하는 디바이스의 호스트 이름입니다. |
| 소스 MAC 주소(src_mac) | 디바이스 ID가 트래픽의 소스로 식별하는 디바이스의 MAC 주소입니다. |
| 지역(Region) | 트래픽이 발생하는 지리적 영역입니다. |
| 사용자 에이전트(user_agent) | HTTP 요청 헤더 **사용자 에이전트**의 문자열입니다. |
| 세션 ID | 트래픽 세션을 고유하게 식별하는 문자열입니다. |

## 구성 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, 하위 유형, FUTURE_USE, 생성된 시간, 호스트, 가상 시스템, 명령, 관리자, 클라이언트, 결과, 구성 경로, 변경 전 세부 정보, 변경 후 세부 정보, 시퀀스 번호, 작업 플래그, 디바이스 그룹 레이어 레벨 1, 디바이스 그룹 레이어 레벨 2, 디바이스 그룹 레이어 레벨 3, 디바이스 그룹 레이어 레벨 4, 가상 시스템 이름, 디바이스 이름, 디바이스 그룹, 감사 설명

| 필드 이름 | 설명 |
|---|---|
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 디바이스의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 CONFIG입니다. |
| 위협/콘텐츠 유형(subtype) | 구성 로그의 하위 유형입니다(미사용). |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 호스트(host) | 클라이언트 시스템의 호스트 이름 또는 IP 주소 |
| 가상 시스템(vsys) | 구성 로그와 연결된 가상 시스템 |
| 명령(cmd) | 관리자가 수행하는 명령 값은 추가, 복제, 커밋, 삭제, 편집, 이동, 이름 바꾸기, 설정입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 관리자(admin) | 구성을 수행하는 관리자의 사용자 이름 |
| 클라이언트(client) | 관리자가 사용하는 클라이언트 값은 웹 및 CLI입니다. |
| 결과(result) | 구성 작업의 결과입니다. 값은 Submitted, Succeeded, Failed 및 Unauthorized입니다. |
| 구성 경로(path) | 발행된 구성 명령의 경로입니다(최대 512바이트 길이). |
| 변경 전 세부 정보(before_change_detail) | 이 필드는 사용자 정의 로그에만 있습니다. 기본 형식이 아닙니다.<br>여기에는 구성 변경 전의 전체 xpath가 포함됩니다. |
| 변경 후 세부 정보(after_change_detail) | 이 필드는 사용자 정의 로그에만 있습니다. 기본 형식이 아닙니다.<br>여기에는 구성 변경 후 전체 xpath가 포함됩니다. |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 디바이스 그룹(dg_id) | Panorama™ 관리 서버에서 관리하는 경우 방화벽이 속한 디바이스 그룹입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 감사 코멘트(comment) | 정책 규칙 구성 변경에 입력한 감사 주석입니다. |

## 시스템 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, 콘텐츠/위협 유형, FUTURE_USE, 생성된 시간, 가상 시스템, 이벤트 ID, 개체, FUTURE_USE, FUTURE_USE, 모듈, 심각도, 설명, 시퀀스 번호, 작업 플래그, 디바이스 그룹 레이어 구조 수준 1, 디바이스 그룹 레이어 레벨 2, 디바이스 그룹 레이어 레벨 3, 디바이스 그룹 레이어 레벨 4, 가상 시스템 이름, 디바이스 이름, FUTURE_USE, FUTURE_USE, 고해상도 타임스탬프

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 SYSTEM입니다. |
| 위협/콘텐츠 유형(subtype) | 시스템 로그의 하위 유형: 로그를 생성하는 시스템 데몬을 지칭합니다. 값은 암호화, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn입니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 가상 시스템(vsys) | 구성 로그와 연결된 가상 시스템입니다. |
| 이벤트 ID(eventid) | 이벤트 이름을 표시하는 문자열입니다. |
| 개체(object) | 시스템 이벤트와 연결된 개체의 이름입니다. |
| 모듈(module) | 이 필드는 하위 유형 필드의 값이 일반인 경우에만 유효합니다. 로그를 생성하는 하위 시스템에 대한 추가 정보를 제공합니다. 값은 일반, 관리, 인증, 하, 업그레이드, 섀시입니다. |
| 심각도(severity) | 이벤트와 관련된 심각도 값은 정보 제공, 낮음, 중간, 높음, 중요입니다. |
| 설명(opaque) | 이벤트에 대한 자세한 설명(최대 512바이트). |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 시퀀스 번호(seqno) | 순차적으로 증가하는 64비트 로그 항목 식별자. 각 로그 유형에는 고유한 숫자 공간이 있습니다. |
| 작업 플래그(actionflags) | 로그가 Panorama로 포워딩되었는지 나타내는 비트 필드입니다. |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm) |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| | 고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 *1969-12-31T16:00:00.000-8:00* 타임스탬프를 표시합니다. |

## 상관 이벤트 로그 필드

**포맷:** FUTURE_USE, 수신 시간, 일련번호, 유형, 콘텐츠/위협 유형, FUTURE_USE, 생성 시간, 소스 주소, 소스 사용자, 가상 시스템, 카테고리, 심각도, 디바이스 그룹 레이어 수준 1, 디바이스 그룹 레이어 수준 2, 디바이스 그룹 레이어 수준 3, 디바이스 그룹 레이어 수준 4, 가상 시스템 이름, 디바이스 이름, 가상 시스템 ID, 개체 이름, 개체 ID , 증거

| 필드 이름 | 설명 |
| --- | --- |
| 시간 획득(receive_time 또는 receive_time) | 관리 평면에서 로그를 획득한 시간입니다. |
| 일련번호(serial) | 로그를 생성한 디바이스의 일련번호입니다. |
| 유형(유형) | 로그 유형을 지정합니다. 값은 상관 관계입니다. |
| 콘텐츠/위협 유형(하위 유형) | 시스템 로그의 하위 유형: 로그를 생성하는 시스템 데몬을 지칭합니다. 값은 암호화, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn입니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 이벤트를 시작한 사용자의 IP 주소입니다. |
| 소스 사용자(srcuser) | 이벤트를 시작한 사용자의 사용자 이름입니다. |
| 가상 시스템(vsys) | 구성 로그와 연결된 가상 시스템입니다. |
| 카테고리(category) | 네트워크, 사용자 또는 호스트에 제기된 위협 또는 피해의 종류에 대한 요약입니다. |
| 심각도(severity) | 이벤트와 관련된 심각도 값은 정보 제공, 낮음, 중간, 높음, 중요입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 디바이스 그룹 레이어 구조(dg_hier_level_4 dg_hier_level_1) | 디바이스 그룹 레이어 구조 내에서 디바이스 그룹의 위치를 나타내는 식별 번호 시퀀스입니다. 로그를 생성하는 방화벽(또는 가상 시스템)에는 디바이스 그룹 레이어 구조의 각 조상의 식별 번호가 포함됩니다. 공유 디바이스 그룹(레벨 0)은 이 구조에 포함되지 않습니다.<br>로그 값이 12, 34, 45, 0인 경우 디바이스 그룹(45)에 속하는 방화벽(또는 가상 시스템)에 의해 로그가 생성되고 그 조상은 34, 12임을 의미합니다. 값 12, 34 또는 45에 해당하는 디바이스 그룹 이름을 보려면 다음 방법 중 하나를 사용합니다.<br>API 쿼리:<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 가상 시스템 이름(vsys_name) | 세션과 연결된 가상 시스템의 이름; 여러 가상 시스템에 대해 활성화된 방화벽에서만 유효합니다. |
| 디바이스 이름(device_name) | 세션이 기록된 방화벽의 호스트 이름입니다. |
| 가상 시스템 ID(vsys_id) | Palo Alto Networks 방화벽의 가상 시스템의 고유 식별자입니다. |
| 개체 이름(objectname) | 일치된 상관 관계 개체의 이름입니다. |
| 개체 ID(object_id) | 시스템 이벤트와 연결된 개체의 이름입니다. |
| 증거(evidence) | 호스트가 상관 개체에 정의된 조건과 일치한 횟수를 나타내는 요약 문입니다. 예를 들어 호스트는 알려진 멀웨어 URL을 방문했습니다(19회). |

## GTP 로그 필드

형식: FUTURE_USE, 수신 시간, 일련번호, 유형, 위협/콘텐츠 유형, FUTURE_USE, 생성된 시간, 소스 주소, 대상 주소, FUTURE_USE, FUTURE_USE, 규칙 이름, FUTURE_USE, FUTURE_USE, 애플리케이션, 가상 시스템, 소스 영역, 대상 영역, 인바운드 인터페이스 , 아웃바운드 인터페이스, 로그 작업, FUTURE_USE, 세션 ID, FUTURE_USE, 소스 포트, 대상 포트, FUTURE_USE, FUTURE_USE, FUTURE_USE, 프로토콜, 작업, GTP 이벤트 유형, MSISDN, 액세스 포인트 이름, 무선 액세스 기술, GTP 메시지 유형, 최종 사용자 IP 주소, 터널 엔드포인트 식별자1, 터널 엔드포인트 식별자2, GTP 인터페이스, GTP 원인, 심각도, 서비스 국가 MCC, 서비스 네트워크 MNC, 지역 코드, 셀 ID, GTP 이벤트 코드, FUTURE_USE, FUTURE_USE, 소스 위치, 대상 위치, FUTURE_USE, FUTURE_USE , FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, 터널 ID/IMSI, 모니터 태그/IMEI, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_U, FUTURE_U, FU SE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, 시작 시간, 경과 시간, 터널 검사 규칙, 원격 사용자 IP, 원격 사용자 ID, 규칙의 UUID, PCAP ID, 고해상도 타임스탬프, A Slice 서비스 유형, A Slice 차별화 요소, 애


©2023 Palo Alto Networks, Inc.

플리케이션 하위 카테고리, 애플리케이션 카테고리, 애플리케이션 기술, 애플리케이션 위험, 애플리케이션 특성, 애플리케이션 컨테이너, 애플리케이션 SaaS, 애플리케이션 승인 상태

| 필드 이름 | 설명 |
|---|---|
| 시간 획득(receive_time 또는 receive_time) | Management Plane(MP)에서 로그를 받은 월, 일 및 시간입니다. |
| 일련번호(serial) | 로그를 생성한 방화벽의 일련번호입니다. |
| 유형(type) | 로그 유형을 지정합니다. 값은 GTP입니다. |
| 위협/콘텐츠 유형(subtype) | 트래픽 로그의 하위 유형 값은 시작, 종료, 삭제 및 거부입니다.<br>• 시작 - 세션 시작됨<br>• 종료 - 세션이 종료됨<br>• 삭제 - 애플리케이션이 식별되기 전에 삭제된 세션이며 세션을 허용하는 규칙이 없습니다.<br>• 거부 - 애플리케이션이 식별된 후 세션이 삭제되고 차단 규칙이 있거나 세션을 허용하는 규칙이 없습니다. |
| 생성된 시간(time_generated 또는 time_generated) | 데이터 평면에서 로그가 생성된 시간입니다. |
| 소스 주소(src) | 세션에 있는 패킷의 소스 IP 주소입니다. |
| 대상 주소(dst) | 세션에 있는 패킷의 대상 IP 주소입니다. |
| 규칙 이름(rule) | 세션에 적용되는 보안 정책 규칙의 이름입니다. |
| 애플리케이션(app) | 세션에서 사용되는 터널링 프로토콜입니다. |
| 가상 시스템(vsys) | 세션과 연결된 가상 시스템입니다. |
| 소스 영역(from) | 세션에 있는 패킷의 소스 영역입니다. |
| 대상 영역(to) | 세션에 있는 패킷의 대상 영역입니다. |
| 인바운드 인터페이스(inbound_if) | 세션이 소싱된 인터페이스입니다. |
| 아웃바운드 인터페이스(outbound_if) | 세션이 대상으로 지정된 인터페이스입니다. |
| 로그 작업(logset) | 세션에 적용된 정보 포워딩 프로파일을 기록합니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 세션 ID(sessionid) | 기록 중인 세션의 세션 ID입니다. |
| 소스 포트(sport) | 세션에서 사용하는 소스 포트입니다. |
| 대상 포트(dport) | 세션에서 사용하는 대상 포트입니다. |
| IP 프로토콜(proto) | 세션과 연결된 IP 프로토콜입니다. |
| 액션(action) | 세션에 대해 수행된 작업입니다. 가능한 값은 다음과 같습니다.<br>• allow - 정책에 의해 세션이 허용됨<br>• deny - 정책에 의해 세션이 거부되었습니다. |
| GTP 이벤트 유형(event_type) | GTP 보호 프로파일의 체크인이 GTP 트래픽에 적용될 때 GTP 메시지에 의해 트리거되는 이벤트를 정의합니다. 또한 GTP 세션의 시작 또는 종료에 의해 트리거됩니다. |
| MSISDN(msisdn) | 국가 코드, 국가 대상 코드 및 가입자로 구성된 모바일 가입자와 관련된 서비스 ID입니다. 최대 15자리의 10진수(0-9)로만 구성됩니다. |
| 액세스 포인트 이름(apn) | 모바일 네트워크에서 패킷 데이터 네트워크 데이터 게이트웨이(PGW)/게이트웨이 GPRS 지원 노드에 대한 참조. 필수 APN 네트워크 식별자와 선택적 APN 운영자 식별자로 구성됩니다. |
| 무선 액세스 기술(rat) | 무선 액세스에 사용되는 기술 유형입니다. 예를 들어 EUTRAN, WLAN, Virtual, HSPA Evolution, GAN 및 GERAN이 있습니다. |
| GTP 메시지 유형(msg_type) | GTP 메시지 유형을 나타냅니다. |
| 끝 IP 주소(end_ip_adr) | PGW/GGSN에서 할당한 이동 가입자의 IP 주소입니다. |
| 터널 엔드포인트 식별자1(teid1) | 네트워크 노드에서 GTP 터널을 식별합니다. TEID1은 GTP 메시지의 첫 번째 TEID입니다. |
| 터널 엔드포인트 식별자2(teid2) | 네트워크 노드에서 GTP 터널을 식별합니다. TEID2는 GTP 메시지의 두 번째 TEID입니다. |
| GTP 인터페이스(gtp_interface) | GTP 메시지가 수신되는 3GPP 인터페이스입니다. |
| GTP 원인(Cause_code) | 네트워크 노드의 GTP 요청 수락 또는 거부에 대한 정보를 제공하는 정보 요소를 포함하는 로그 응답의 GTP 원인 값입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 심각도(severity) | 이벤트와 관련된 심각도 값은 정보 제공, 낮음, 중간, 높음, 중요입니다. |
| 서비스 네트워크 MCC(mcc) | 서비스를 제공하는 핵심 네트워크 사업자의 모바일 국가 코드입니다. |
| 서비스 네트워크 MNC(mnc) | 서비스를 제공하는 핵심 네트워크 사업자의 모바일 네트워크 코드입니다. |
| 지역 번호(area_code) | PLMN(Public Land Mobile Network) 내의 영역입니다. |
| 셀 ID(cell_id) | 지역 코드 내의 기지국. |
| GTP 이벤트 코드(event_code) | GTP 이벤트를 설명하는 이벤트 코드입니다. |
| 소스 위치(srcloc) | 개인 주소의 출처 국가 또는 내부 지역 최대 길이는 32바이트입니다. |
| 대상 위치(dstloc) | 개인 주소의 대상 국가 또는 내부 지역 최대 길이는 32바이트입니다. |
| 터널 ID/IMSI(imsi) | IMSI(International Mobile Subscriber Identity)는 GSM/UMTS/EPS 시스템에서 각 모바일 가입자에게 할당되는 고유 번호입니다. IMSI는 10진수(0~9)로만 구성되며 허용되는 최대 자릿수는 15입니다. |
| 모니터 태그/IMEI(imei) | IMEI(International Mobile Equipment Identity)는 각 이동국 장비에 할당된 고유한 15자리 또는 16자리 숫자입니다. |
| 시작 시간(시작) | 세션 시작 시간입니다. |
| 경과 시간(경과) | 세션의 경과 시간입니다. |
| 터널 검사 규칙 (tunnel_insp_rule) | 일반 텍스트 터널 트래픽과 일치하는 터널 검사 규칙의 이름 |
| 원격 사용자 IP(remote_user_ip) | 원격 사용자가 사용하는 IPv4 또는 IPv6 주소입니다. |
| 원격 사용자 ID(remote_user_id) | 원격 사용자의 IMSI ID, 사용 가능한 경우 하나의 IMEI ID 및/또는 하나의 MSISDN ID. |
| 규칙에 대한 UUID(rule_uuid) | 규칙에 대한 범용 고유 ID입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| PCAP ID(pcap_id) | 방화벽에 저장된 pcap 파일을 찾는 데 사용되는 고유한 패킷 캡처 ID입니다. |
| 고해상도 타임스탬프(high_res_timestamp) | 관리 평면에서 로그를 수신한 지 밀리초 만에 로그를 받았습니다.<br>이 신규 필드의 형식은 YYYY-MM-DDThh:ss:ssSTZD입니다.<br>• **YYYY** - 4자리 연도<br>• **MM** - 두 자릿수 달<br>• **DD** - 월중 두 자리 일(01~31)<br>• **T** - 타임스탬프의 시작을 나타내는 표시<br>• **hh** - 24시간 사용 2자리 시간(00~23)<br>• **mm** - 두 자리 분(00~59)<br>• **ss** - 두 자리 초(00 ~ 60)<br>• **sss** - 밀리초의 하나 이상의 숫자<br>• **TZD** - 표준 시간대 지정자(+hh:mm 또는 -hh:mm)<br>고해상도 타임스탬프는 *PAN-OS 10.2* 및 이후 릴리스를 실행하는 관리되는 방화벽에서 수신된 로그에 대해 지원됩니다. *PAN-OS 9.1*을 실행하는 관리되는 방화벽에서 수신된 로그는 로그를 받은 시기에 관계없이 ***1969-12-31T16:00:00:000-8:00*** 타임스탬프를 표시합니다. |
| 슬라이스 서비스 유형(nsdsai_sst) | 네트워크 슬라이스 ID의 A 슬라이스 서비스 유형입니다. |
| 슬라이스 구분자(nsdsai_sd) | 네트워크 슬라이스 ID의 슬라이스 구분자입니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |
| 애플리케이션 카테고리(카테고리_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 카테고리입니다. 값은 다음과 같습니다.<br>• business-systems<br>• collaboration<br>• general-internet<br>• media<br>• networking<br>• saas |


©2023 Palo Alto Networks, Inc.

| 필드 이름 | 설명 |
| --- | --- |
| 애플리케이션 기술(technology_of_app) | 애플리케이션 구성 속성에 지정된 애플리케이션 기술입니다. 값은 다음과 같습니다.<br>• browser-based<br>• client-server<br>• network-protocol<br>• peer-to-peer |
| 애플리케이션 위험(risk_of_app) | 애플리케이션과 관련된 위험 수준입니다(1=가장 낮음 - 5=가장 높음). |
| 애플리케이션 속성(characteristic_of_app) | 애플리케이션의 적용 가능한 속성을 쉼표로 구분한 목록 |
| 애플리케이션 컨테이너(container_of_app) | 애플리케이션의 상위 애플리케이션입니다. |
| 애플리케이션 SaaS(is_saas_of_app) | SaaS 애플리케이션인 경우 **1**을 표시하고 SaaS 애플리케이션이 아닌 경우 **0**을 표시합니다. |
| 애플리케이션 승인 상태(sanctioned_state_of_app) | 애플리케이션이 승인되면 **1**을 표시하고 애플리케이션이 승인되지 않은 경우 **0**을 표시합니다. |
| 애플리케이션 하위 카테고리(subcategory_of_appp) | 애플리케이션 구성 속성에 지정된 애플리케이션 하위 카테고리입니다. |

## 시스템 로그 심각도

syslog 심각도는 로그 유형 및 내용을 기반으로 설정됩니다.

| 로그 유형/심각도 | 시스템 로그 심각도 |
| --- | --- |
| 트래픽 | 정보 |
| 구성 | 정보 |
| 위협/시스템 - 정보 | 정보 |
| 위협/시스템 - 낮음 | 알림 |
| 위협/시스템 - 중간 | 경고 |
| 위협/시스템 - 높음 | 경고 |


©2023 Palo Alto Networks, Inc.

| 로그 유형/심각도 | 시스템 로그 심각도 |
|---|---|
| Threat/System - Critical | 심각한 |

## 사용자 정의 로그/이벤트 형식

외부 로그 구문 분석 시스템과의 통합을 용이하게 하기 위해 방화벽을 사용하면 로그 형식을 사용자 지정할 수 있습니다. 또한 사용자 지정 키를 추가할 수도 있습니다. 값 속성 쌍입니다. 사용자 지정 메시지 형식은 디바이스 > 서버 프로파일 > **Syslog** > **Syslog**서버 프로파일 > 사용자 지정로그 형식으로 구성할 수 있습니다.

ArcSight 공통 이벤트 형식(CEF) 호환 로그 서식을 얻으려면 CEF 구성 가이드를 참조하십시오.

## 이스케이프 시퀀스(Escape Sequences)

쉼표 또는 이중 견적이 포함된 모든 필드는 이중 따옴표로 구분되어 있습니다. 또한 필드 내부에 이중 견적이 나타나면 다른 이중 견적으로 앞서 탈출합니다. 뒤로 호환성을 유지하려면 위협 로그의 Misc 필드는 항상 이중 따옴표로 구분되어 있습니다.


©2023 Palo Alto Networks, Inc.

# SNMP 모니터링 및 트랩

다음 항목에서는 Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스가 SNMP를 구현하는 방법과 SNMP 모니터링 및 트랩 전송을 구성하는 절차를 설명합니다.

- SNMP 지원
- SNMP 관리자를 사용하여 MIB 및 개체 탐색
- 방화벽 보안 네트워크 요소에 대한 SNMP 서비스 활성화
- SNMP를 사용하여 통계 모니터링
- SNMP 관리자로 트랩 포워딩
- 지원되는 MIB

## SNMP 지원

SNMP 관리자를 사용하여 방화벽, Panorama 또는 WF-500 어플라이언스 및 처리 트래픽에 대한 이벤트 기반 경고 및 운영 통계를 모니터링할 수 있습니다. 통계 및 트랩은 리소스 제한, 시스템 변경 또는 오류, 멀웨어 공격을 식별하는 데 도움이 될 수 있습니다. 로그 데이터를 트랩으로 포워딩하여 경고를 구성하고 SNMP 관리자의 GET 메시지(요청)에 대한 응답으로 통계 포워딩을 활성화합니다. 각 트랩 및 통계에는 개체 식별자(OID)가 있습니다. 관련 OID는 모니터링을 활성화하기 위해 SNMP 관리자에 로드하는 MIB(Management Information Bases) 내에서 레이어적으로 구성됩니다.

이벤트가 ***SNMP*** 트랩 생성을 트리거하면***(***예***:*** 인터페이스 다운***)*** 방화벽***, Panorama*** 가상 어플라이언스***, M-***시리즈 어플라이언스 및 ***WF-500*** 어플라이언스는 대신 해당 ***SNMP*** 개체***(***예***:*** 인터페이스 ***MIB)***를 업데이트하여 응답합니다***. 10***초마다 발생하는 모든 개체의 주기적인 업데이트를 기다리는 것입니다***.*** 이렇게 하면 이벤트를 확인하기 위해 개체를 폴링할 때 ***SNMP*** 관리자가 최신 정보를 표시할 수 있습니다***.***

방화벽, Panorama 및 WF-500 어플라이언스는 SNMP 버전 2c 및 버전 3을 지원합니다. 네트워크의 다른 디바이스가 지원하는 버전과 네트워크 보안 요구 사항에 따라 사용할 것을 결정하십시오. SNMPv3는 SNMPv2c보다 더 안전하고 시스템 통계에 대한 더 세분화된 액세스 제어를 가능하게 합니다. 다음 표에는 각 버전의 보안 기능이 요약되어 있습니다. SNMP를 사용하여 통계를 모니터링하고 SNMP 관리자로 트랩을 포워딩할 때 버전을 선택한 다음 보안 기능을 구성합니다.

| **SNMP**버전 | 인증 | 메시지 개인 정보 보호 | 메시지 무결성 | **MIB** 액세스 세분성 |
|---|---|---|---|---|
| SNMPv2c | 커뮤니티 문자열 | 아니오(일반 텍스트) | 아니요 | 디바이스의 모든 MIB에 대한 SNMP 커뮤니티 액세스 |
| SNMPv3 | EngineID, 사용자명 및 인증 암호(암호에 대한 SHA 해싱) | SNMP 메시지의 AES(128, 192 또는 256) 암호화를 위한 개인 정보 암호 | 예 | 특정 OID를 포함하거나 제외하는 보기를 기반으로 하는 사용자 액세스 |


©2023 Palo Alto Networks, Inc.

SNMP 구현은 방화벽이 SNMP 관리자에게 트랩을 포워딩하는 동시에 로그 수집기로도 로그를 포워딩하는 배포를 보여줍니다. 또는 방화벽 트랩을 SNMP 관리자로 포워딩하도록 로그 수집기를 구성할 수 있습니다. 이러한 배포에 대한 자세한 내용은 중앙 집중식 로깅 및 보고의 로그 포워딩 옵션을 참조하십시오. 모든 배포에서 SNMP 관리자는 방화벽, Panorama 또는 WF-500 어플라이언스에서 직접 통계를 가져옵니다. 이 예에서는 단일 SNMP 관리자가 트랩과 통계를 모두 수집하지만 네트워크에 더 적합한 경우 이러한 기능에 대해 별도의 관리자를 사용할 수 있습니다.

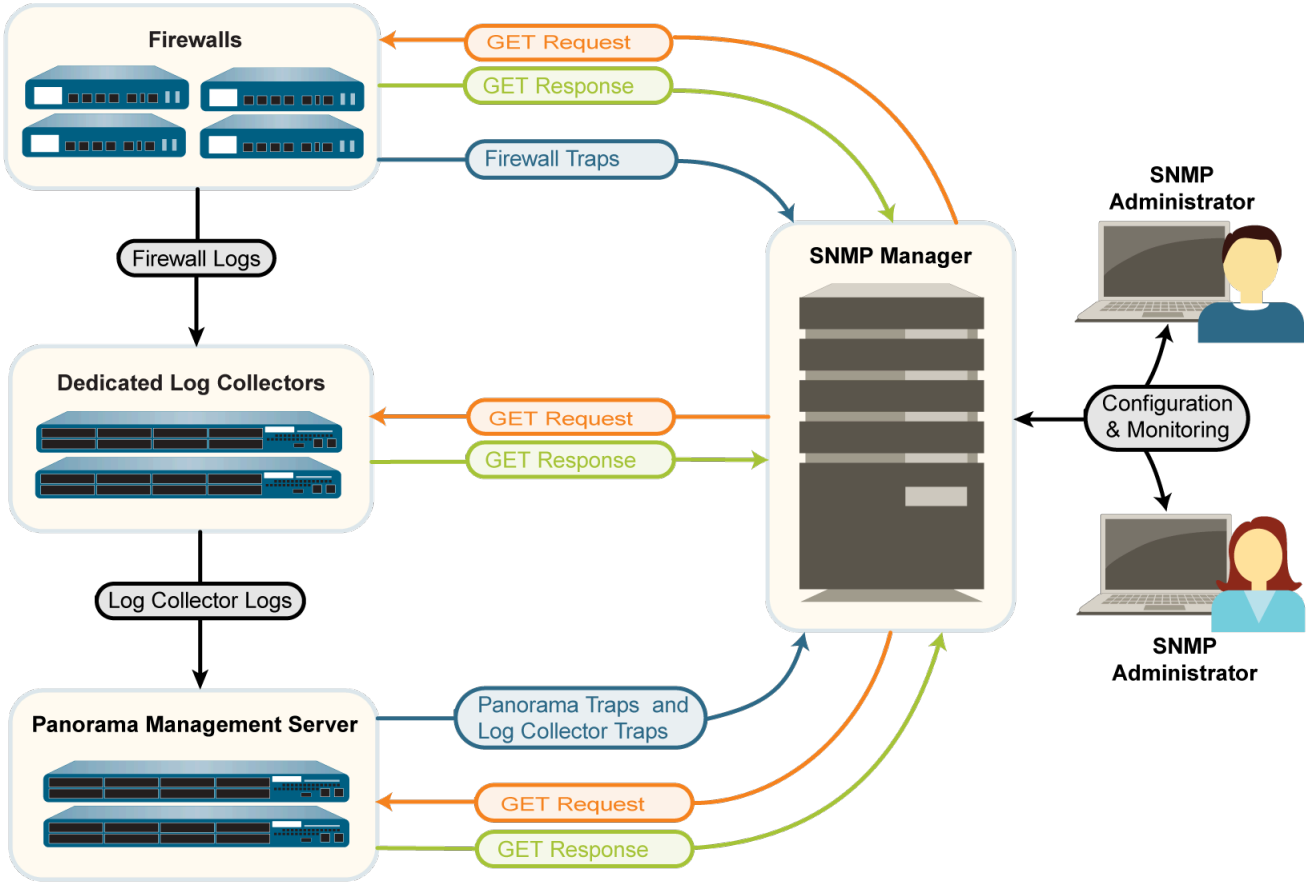



그림 **2: SNMP** 구현

## SNMP 관리자를 사용하여 MIB 및 개체 탐색

Palo Alto Networks 방화벽, Panorama 또는 WF-500 어플라이언스를 모니터링하는 데 SNMP를 사용하려면 먼저 SNMP 관리자에 지원되는 MIB을(를) 로드하고 모니터링하려는 시스템 통계 및 트랩에 해당하는 개체 식별자(OID)를 결정해야 합니다. 다음 항목에서는 SNMP 관리자에서 OID 및 MIB를 찾는 방법에 대한 개요를 제공합니다. 이러한 작업을 수행하는 특정 단계는 SNMP 관리 소프트웨어를 참조하십시오.

- 알려진 OID가 포함된 MIB 식별
- MIB 실행
- 시스템 통계 또는 트랩에 대한 OID 식별

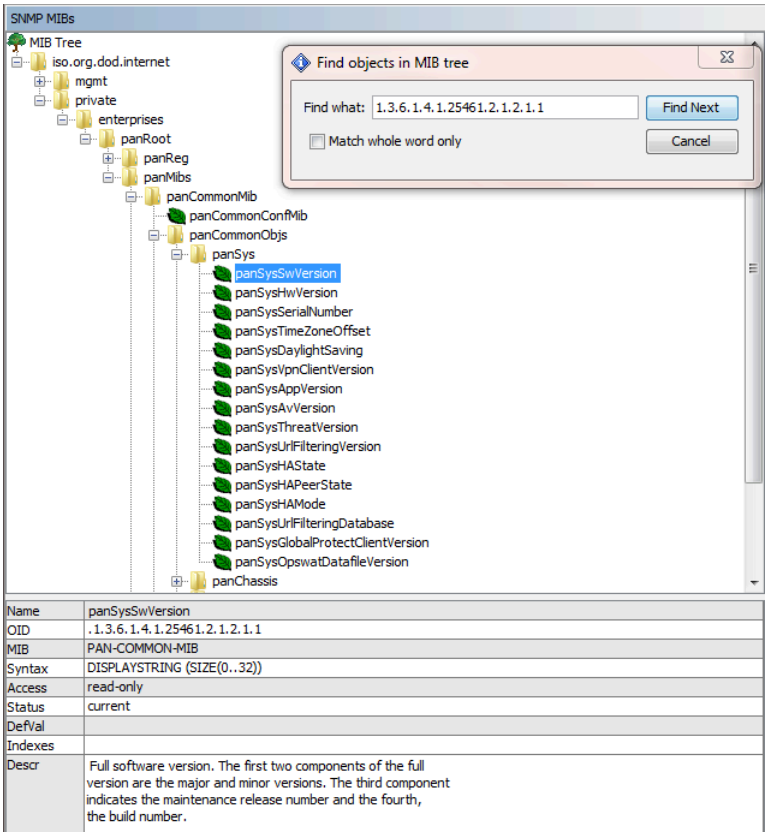

©2023 Palo Alto Networks, Inc.

## 알려진 OID가 포함된 MIB 식별

특정 SNMP 개체(통계 또는 트랩)에 대한 OID를 이미 파악한 상태이고 유사한 개체의 OID를 파악하고자 모니터링할 수 있는 경우 알려진 OID가 포함된 MIB를 탐색할 수 있습니다.

**STEP 1 |** 모든 지원되는 MIB을(를) SNMP 관리자에 로드합니다.

**STEP 2 |** 알려진 OID에 대해 전체 MIB 트리를 검색합니다. 검색 결과는 OID에 대한 MIB 경로와 OID에 대한 정보(예: 이름, 상태 및 설명)를 표시합니다. 그런 다음 동일한 MIB에서 다른 OID를 선택하여 관련 정보를 볼 수 있습니다.

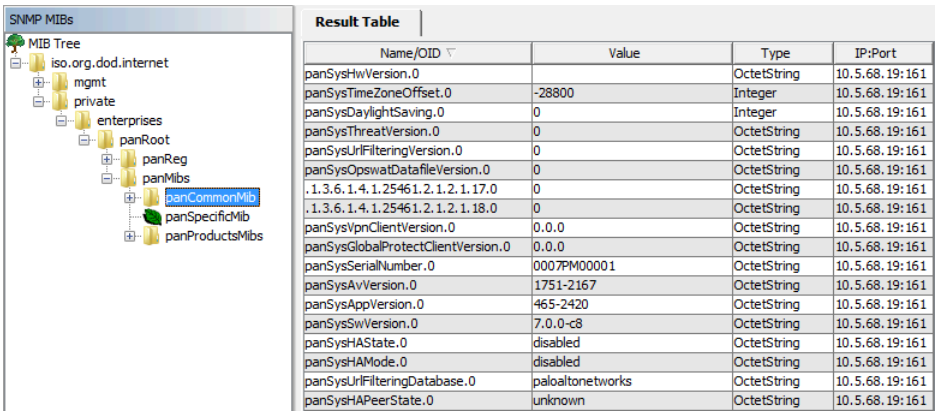



**STEP 3 |** **(**선택 사항**)** MIB 실행 모든 개체를 표시합니다.

## MIB 실행

모니터링에 사용할 수 있는 SNMP 개체(시스템 통계 및 트랩)를 보려면 특정 MIB의 모든 개체를 표시하는 것이 유용할 수 있습니다. 이렇게 하려면 SNMP 관리자에 지원되는 MIB을(를) 로드하고 원하는 MIB에서 실행을 수행합니다. Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스가 지원하는 트랩을 나열하려면 panCommonEventEventsV2 MIB를 살펴보십시오. 다음 예에서 PAN-COMMON-MIB.my을(를) 탐색하면 특정 통계에 대한 다음 OID 목록과 해당 값이 표시됩니다.

 ©2023 Palo Alto Networks, Inc.




| Name/OID | Value | Type | IP:Port |
|---|---|---|---|
| panSysHwVersion.0 | | OctetString | 10.5.68.19:161 |
| panSysTimeZoneOffset.0 | -28800 | Integer | 10.5.68.19:161 |
| panSysDaylightSaving.0 | 0 | Integer | 10.5.68.19:161 |
| panSysThreatVersion.0 | 0 | OctetString | 10.5.68.19:161 |
| panSysUrlFilteringVersion.0 | 0 | OctetString | 10.5.68.19:161 |
| panSysOpswatDatafileVersion.0 | 0 | OctetString | 10.5.68.19:161 |
| .1.3.6.1.4.1.25461.2.1.2.1.17.0 | 0 | OctetString | 10.5.68.19:161 |
| .1.3.6.1.4.1.25461.2.1.2.1.18.0 | 0 | OctetString | 10.5.68.19:161 |
| panSysVpnClientVersion.0 | 0.0.0 | OctetString | 10.5.68.19:161 |
| panSysGlobalProtectClientVersion.0 | 0.0.0 | OctetString | 10.5.68.19:161 |
| panSysSerialNumber.0 | 0007PM00001 | OctetString | 10.5.68.19:161 |
| panSysAvVersion.0 | 1751-2167 | OctetString | 10.5.68.19:161 |
| panSysAppVersion.0 | 465-2420 | OctetString | 10.5.68.19:161 |
| panSysSwVersion.0 | 7.0.0-c8 | OctetString | 10.5.68.19:161 |
| panSysHAState.0 | disabled | OctetString | 10.5.68.19:161 |
| panSysHAMode.0 | disabled | OctetString | 10.5.68.19:161 |
| panSysUrlFilteringDatabase.0 | paloaltonetworks | OctetString | 10.5.68.19:161 |
| panSysHAPeerState.0 | unknown | OctetString | 10.5.68.19:161 |

## 시스템 통계 또는 트랩에 대한 **OID** 식별

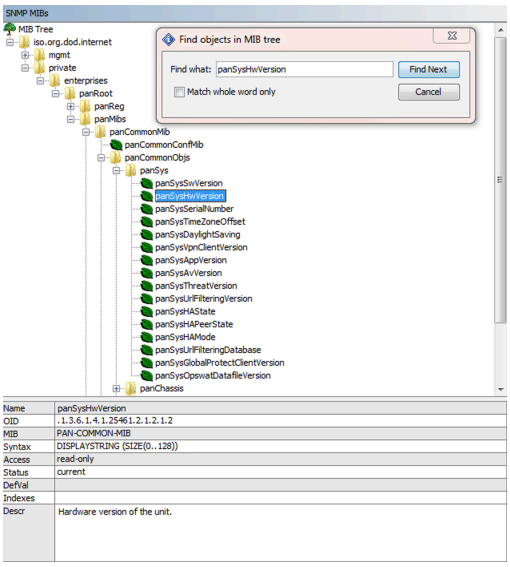
SNMP 관리자를 사용하여 Palo Alto Networks 방화벽, Panorama 또는 WF-500 어플라이언스를 모니터링하려면 모니터링하려는 시스템 통계 및 트랩의 OID를 알아야 합니다.

**STEP 1 |** 지원되는 MIB를 검토하여 원하는 통계 유형이 포함된 MIB를 결정하십시오. 예를 들어, PAN-COMMON-MIB.my에는 하드웨어 버전 정보가 포함되어 있습니다. panCommonEventEventsV2 MIB에는 Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스가 지원하는 모든 트랩이 포함되어 있습니다.

**STEP 2 |** 텍스트 편집기에서 MIB를 열고 키워드 검색을 수행합니다. 예를 들어 PAN-COMMON-MIB에서 검색 문자열로 하드웨어 버전을 사용하면 panSysHwVersion 개체를 식별합니다.

```
panSysHwVersion OBJECT-TYPE SYNTAX DisplayString (SIZE(0..128))
 MAX-ACCESS read-only STATUS current DESCRIPTION "Hardware version
 of the unit." ::= {panSys 2}
```

**STEP 3 |** MIB 브라우저에서 MIB 트리에서 식별된 개체 이름을 검색하여 해당 OID를 표시합니다. 예를 들어 panSysHwVersion 개체의 OID는 1.3.6.1.4.1.25461.2.1.2.1.2입니다.




 ©2023 Palo Alto Networks, Inc.

# 방화벽 보안 네트워크 요소에 대한 SNMP 서비스 활성화

SNMP(단순 네트워크 관리 프로토콜)를 사용하여 Palo Alto Networks 방화벽의 보안 영역 내에 있는 네트워크 요소(예: 스위치 및 라우터)를 모니터링하거나 관리하려면 해당 요소에 대해 SNMP 서비스를 허용하는 보안 규칙을 만들어야 합니다.

*Palo Alto Networks* 방화벽, *Panorama* 또는 *WF-500* 어플라이언스에 대한 *SNMP* 모니터링을 활성화하기 위한 보안 규칙은 필요하지 않습니다. 자세한 내용은 SNMP를 사용하여 통계 모니터링을(를) 참조하십시오.

**STEP 1 |** 애플리케이션 그룹을 생성합니다.

1. 개체 > 애플리케이션 그룹을 선택한 다음 추가를 클릭합니다.
2. 애플리케이션 그룹을 식별할 이름을 입력합니다.
3. 추가를 클릭하고 **snmp**를 입력한 다음 드롭다운에서 **snmp** 및 **snmp-trap**을 선택합니다.
4. 확인을 클릭하여 애플리케이션 그룹을 저장합니다.

**STEP 2 |** SNMP 서비스를 허용하는 보안 규칙을 생성합니다.

1. 정책 > 보안을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 규칙의 이름을 입력합니다.
3. 소스 및 대상 탭에서 추가를 클릭하고 트래픽의 소스 영역과 대상 영역을 입력합니다.
4. 애플리케이션 탭에서 추가를 클릭하고 방금 생성한 애플리케이션 그룹의 이름을 입력한 다음 드롭다운에서 선택합니다.
5. 동작 탭에서 동작이 허용으로 설정되어 있는지 확인한 다음 확인 및 커밋을 클릭합니다.

# SNMP를 사용하여 통계 모니터링

SNMP(Simple Network Management Protocol) 관리자가 Palo Alto Networks 방화벽에서 수집하는 통계는 네트워크(시스템 및 연결)의 상태를 측정하고, 리소스 제한을 식별하고, 트래픽 또는 처리 부하를 모니터링하는 데 도움이 될 수 있습니다. 통계에는 인터페이스 상태(작동 또는 작동 중지), 활성 사용자 세션, 동시 세션, 세션 사용률, 온도 및 시스템 가동 시간과 같은 정보가 포함됩니다.

*SNMP* 관리자를 구성하여 *Palo Alto Networks* 방화벽*(SET* 메시지 사용*)*을 제어할 수 없고, 단지 그로부터 통계 수집*(GET* 메시지 사용*)*을 할 수 있습니다. *Palo Alto Networks* 방화벽에 *SNMP*를 구현하는 방법에 대한 자세한 내용은 SNMP 지원을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 방화벽에서 통계를 가져오도록 SNMP 관리자를 구성합니다.

다음 단계는 SNMP 관리자에서 수행하는 작업의 개요를 제공합니다. 특정 단계의 경우 SNMP 관리자의 설명서를 참조하십시오.

1. SNMP 관리자가 방화벽 통계를 해석할 수 있도록 하려면 Palo Alto Networks 방화벽에 지원되는 MIB를 로드하고 필요한 경우 컴파일합니다.
2. SNMP 관리자가 모니터링할 각 방화벽에 대해 방화벽에 대한 연결 설정(IP 주소 및 포트) 및 인증 설정(SNMPv2c 커뮤니티 문자열 또는 SNMPv3 EngineID/사용자 이름/비밀번호)을 정의합니다.

   모든 ***Palo Alto Networks*** 방화벽은 포트 ***161***을 사용합니다**.**

   SNMP 관리자는 여러 방화벽에 대해 동일하거나 다른 연결 및 인증 설정을 사용할 수 있습니다. 설정은 방화벽에서 SNMP를 구성할 때 정의한 설정과 일치해야 합니다(3 단계 참조). 예를 들어, SNMPv2c를 사용하는 경우 방화벽을 구성할 때 정의하는 커뮤니티 문자열은 해당 방화벽의 SNMP 관리자에서 정의한 커뮤니티 문자열과 일치해야 합니다.
3. 모니터링할 통계의 OID(개체 식별자)를 결정합니다. 예를 들어, 방화벽의 세션 사용률을 모니터링하기 위해 MIB 브라우저는 이 통계가 PAN-COMMON-MIB.my의 OID 1.3.6.1.4.1.25461.2.1.2.3.1.0에 해당함을 보여줍니다. 자세한 내용은 SNMP 관리자를 사용하여 MIB 및 개체를 탐색하는 방법을 참조하십시오.
4. 원하는 OID를 모니터링하도록 SNMP 관리자를 구성합니다.

**STEP 2 |** 방화벽 인터페이스에서 SNMP 트래픽을 활성화합니다.

이것은 SNMP 관리자로부터 통계 요청을 수신할 인터페이스입니다.

***PAN-OS***는 고가용성***(HA)*** 구성에서 방화벽에 대한 관리***(MGT)*** 인터페이스 설정을 동기화하지 않습니다**.** 각 ***HA*** 피어에 대한 인터페이스를 구성해야 합니다**.**

방화벽 웹 인터페이스에서 이 단계를 수행합니다.

- MGT 인터페이스에서 SNMP 트래픽을 활성화하려면 **Device** > **Setup** > **Interfaces**를 선택한 다음 관리 인터페이스를 편집하고 **SNMP**를 선택한 다음 확인 및 커밋을 클릭합니다.
- 다른 인터페이스에서 SNMP 트래픽을 활성화하려면 SNMP 서비스에 대한 인터페이스 관리 프로파일을 생성하고 SNMP 요청을 수신할 인터페이스에 프로파일을 할당합니다. 인터페이스 유형은 레이어 3 이더넷이어야 합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** SNMP 관리자의 통계 요청에 응답하도록 방화벽을 구성합니다.

*PAN-OS*는 고가용성*(HA)* 구성에서 방화벽에 대한 *SNMP* 응답 설정을 동기화하지 않습니다. 각 *HA* 피어에 대해 이러한 설정을 구성해야 합니다.

1. 디바이스 > 설정 > 작업을 선택하고 기타 섹션에서 **SNMP** 설정을 클릭합니다.
2. SNMP 버전을 선택하고 인증 값을 다음과 같이 구성합니다. 버전 세부 정보는 SNMP 지원을 참조하십시오.
   - **V2c** - SNMP 관리자 및 모니터링되는 디바이스의 커뮤니티를 식별하고 커뮤니티 구성원을 서로 인증하기 위한 암호 역할을 하는 **SNMP** 커뮤니티 문자열을 입력합니다.

     모범 사례로 기본 커뮤니티 문자열을 공개하지 마십시오.

   - **V3** - 하나 이상의 SNMP 보기 그룹과 하나의 사용자를 생성합니다. 사용자 계정과 보기는 방화벽이 트랩을 포워딩하고 SNMP 관리자가 방화벽 통계를 얻을 때 인증, 개인 정보 보호 및 액세스 제어를 제공합니다.
     - 보기 - 각 보기는 쌍을 이루는 OID 및 비트별 마스크입니다. OID는 MIB를 지정하고 마스크(16진수 형식)는 해당 MIB 내부(일치 포함) 또는 외부(일치 제외)에 액세스할 수 있는 개체를 지정합니다. 첫 번째 목록에서 추가를 클릭하고 보기 그룹의 이름을 입력합니다. 그룹의 각 보기에 대해 추가를 클릭하고 보기 이름, **OID**, 일치 옵션(포함 또는 제외) 및 마스크를 구성합니다.
     - 사용자 - 두 번째 목록에서 추가를 클릭하고, 사용자 아래에 사용자 이름을 입력하고, 드롭다운에서 보기 그룹을 선택한 다음, SNMP 관리자에 인증하는 데 사용되는 인증 암호(**Auth Password**)를 입력하고, 개인 정보 암호(**Priv Password**)를 입력합니다. SNMP 관리자에 대한 SNMP 메시지를 암호화하는 데 사용됩니다.
3. 확인 및 커밋을 클릭합니다.

**STEP 4 |** SNMP 관리자에서 방화벽 통계를 모니터링합니다.

자세한 내용은 SNMP 관리자 설명서를 참조하십시오.

방화벽 인터페이스와 관련된 통계를 모니터링할 때 *SNMP* 관리자의 인터페이스 인덱스를 방화벽 웹 인터페이스의 인터페이스 이름과 일치시켜야 합니다. 자세한 내용은 SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자를 참조하십시오.

## SNMP 관리자로 트랩 포워딩

간단한 네트워크 관리 프로토콜(SNMP) 트랩은 즉시 주의가 필요한 시스템 이벤트(Palo Alto Networks 방화벽의 하드웨어 또는 소프트웨어의 오류 또는 변경) 또는 위협(방화벽 보안 규칙과 일치하는 트래픽)을 경고할 수 있습니다.

*Palo Alto Networks* 방화벽이 지원하는 트랩 목록을 보려면 *SNMP* 관리자를 사용하여 *panCommonEventEventsV2 MIB*에 액세스하십시오. 자세한 내용은 SNMP 관리자를 사용하여 MIB 및 개체를 탐색하는 방법을 참조하십시오.

*Palo Alto Networks* 방화벽이 *SNMP*를 구현하는 방법에 대한 자세한 내용은 SNMP 지원을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** SNMP 관리자가 수신하는 트랩을 해석하도록 합니다.

Palo Alto Networks 방화벽에 대해 지원되는 MIB를 로드하고 필요한 경우 컴파일합니다. 특정 단계의 경우 SNMP 관리자의 설명서를 참조하십시오.

**STEP 2 |** SNMP 트랩 서버 프로파일을 구성합니다.

프로파일은 방화벽이 SNMP 관리자(트랩 서버)에 액세스하는 방법을 정의합니다. 각 프로파일에 대해 최대 4명의 SNMP 관리자를 정의할 수 있습니다.

선택적으로 서로 다른 로그 유형, 심각도 수준 및 *WildFire* 판정에 대해 별도의 *SNMP* 트랩 서버 프로파일을 구성합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 서버 프로파일 > **SNMP** 트랩을 선택합니다.
3. 추가를 클릭하고 프로파일 이름을 입력합니다.
4. 방화벽에 둘 이상의 가상 시스템(vsys)이 있는 경우 이 프로파일을 사용할 수 있는 위치(vsys 또는 **Shared**)를 선택합니다.
5. SNMP 버전을 선택하고 인증 값을 다음과 같이 구성합니다. 버전 세부 정보는 SNMP 지원을 참조하십시오.
   - **V2c** - 각 서버에 대해 서버 이름, IP 주소(**SNMP**관리자) 및 커뮤니티 문자열 추가를 클릭하고 입력합니다. 커뮤니티 문자열은 SNMP 관리자 및 모니터링되는 디바이스의 커뮤니티를 식별하고 커뮤니티 구성원을 서로 인증하는 암호 역할을 합니다.

     모범 사례로 기본 커뮤니티 문자열을 공개하지 마십시오.

   - **V3** - 각 서버에 대해 추가를 클릭하고 서버 이름, IP 주소(**SNMP Manager**), SNMP 사용자를 입력합니다. 계정(SNMP 관리자에 정의된 사용자 이름과 일치해야 함), 방화벽을 고유하게 식별하는 데 사용되는 **EngineID**(방화벽 일련번호를 사용하려면 필드를 비워 둘 수 있음), 인증 암호(인증 암호)는 서버 인증에 사용되며 개인 정보 암호(**Priv Password**)는 서버에 대한 SNMP 메시지를 암호화하는 데 사용됩니다.
6. 확인을 클릭하여 서버 프로파일을 저장합니다.

**STEP 3 |** 로그 포워딩을 구성합니다.

1. 트래픽, 위협 및 WildFire 트랩의 대상을 구성:
   1. 로그 포워딩 프로파일을 생성합니다. 각 로그 유형과 각 심각도 수준 또는 WildFire 판정에 대해 **SNMP** 트랩 서버 프로파일을 선택합니다.
   2. 정책 규칙 및 네트워크 영역에 로그 포워딩 프로파일을 할당합니다. 규칙과 영역은 트랩 생성 및 포워딩을 트리거합니다.
2. 시스템, 구성, 사용자 ID, HIP 일치 및 상관 관계 로그에 대한 대상을 구성합니다. 각 로그(트랩) 유형 및 심각도 수준에 대해 **SNMP** 트랩 서버 프로파일을 선택합니다.
3. 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** SNMP 관리자의 트랩을 모니터링합니다.

SNMP 관리자의 설명서를 참조하십시오.

방화벽 인터페이스와 관련된 트랩을 모니터링할 때는 ***SNMP*** 관리자의 인터페이스 인덱스와 방화벽 웹 인터페이스의 인터페이스 이름을 일치시켜야 합니다. 자세한 내용은 SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자를 참조하십시오.

## 지원되는 MIB

다음 표에는 Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스가 지원하는 단순 네트워크 관리 프로토콜(SNMP) 관리 정보 베이스(MIB)가 나와 있습니다. MIB에 정의된 개체(시스템 통계 및 트랩)를 모니터링하려면 이러한 MIB를 SNMP 관리자에 로드해야 합니다. 자세한 내용은 SNMP 관리자를 사용하여 MIB 및 개체를 탐색하는 방법을 참조하십시오.

| **MIB** 타입 | 지원되는 **MIB** |
|---|---|
| 표준 - 인터넷 엔지니어링 태스크 포스(IETF)는 대부분의 표준 MIB를 유지 관리합니다. IETF 웹사이트에서 MIB를 다운로드할 수 있습니다.<br><br>*Palo Alto Networks* 방화벽, *Panorama* 및 *WF-500* 어플라이언스는 이러한 모든 *MIB*에서 모든 *OID*(개체)를 지원하지는 않습니다. 지원되는 *OID*에 대한 개요는 지원되는 *MIB* 링크를 참조하십시오. | MIB-II<br>IF-MIB<br>호스트 리소스 MIB<br>엔터티-MIB<br>엔티티-센서-MIB<br>엔터티-상태-MIB<br>IEEE 802.3 LAG MIB<br>LLDP-V2-MIB.my<br>BFD-STD-MIB |
| 엔터프라이즈 - Palo Alto Networks 기술 문서 포털에서 엔터프라이즈 MIB를 다운로드할 수 있습니다. | PAN-COMMON-MIB.my<br>PAN-GLOBAL-REG-MIB.my<br>PAN-GLOBAL-TC-MIB.my<br>PAN-LC-MIB.my<br>PAN-PRODUCT-MIB.my<br>PAN-ENTITY-EXT-MIB.my |


©2023 Palo Alto Networks, Inc.

| MIB 타입 | 지원되는 MIB |
|---|---|
| | PAN-TRAPS.my |

## MIB-II

MIB-II는 TCP/IP 기반 네트워크에서 네트워크 관리 프로토콜에 대한 개체 식별자(OID)를 제공합니다. 이 MIB를 사용하여 시스템 및 인터페이스에 대한 일반 정보를 모니터링합니다. 예를 들어 인터페이스 유형(ifType 개체)별로 대역폭 사용 추세를 분석하여 트래픽 볼륨의 급증을 수용하기 위해 방화벽에 해당 유형의 인터페이스가 더 필요한지의 여부를 결정할 수 있습니다.

Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스는 다음 개체 그룹만 지원합니다.

| 개체 그룹 | 설명 |
|---|---|
| 체계 | 하드웨어 모델, 시스템 가동 시간, FQDN 및 물리적 위치와 같은 시스템 정보를 제공합니다. |
| 인터페이스 | 유형, 현재 대역폭(속도), 작동 상태(예: 작동 또는 작동 중지), 폐기된 패킷과 같은 물리적 및 논리적 인터페이스에 대한 통계를 제공합니다. 논리적 인터페이스 지원에는 VPN 터널, 집계 그룹, 레이어 2 하위 인터페이스, 레이어 3 하위 인터페이스, 루프백 인터페이스 및 VLAN 인터페이스가 포함됩니다. |

RFC 1213은 이 MIB를 정의합니다.

## IF-MIB

IF-MIB는 인터페이스 유형(물리적 및 논리적)과 MIB-II에 정의된 것보다 큰 카운터(64K)를 지원합니다. 이 MIB를 사용하여 MIB-II가 제공하는 것 외에 인터페이스 통계를 모니터링합니다. 예를 들어 PA-5200 시리즈 방화벽의 10G 인터페이스와 같은 고속 인터페이스(2.2Gps 이상)의 현재 대역폭을 모니터링하려면 MIB- II 의 ifSpeed 개체 대신 IF-MIB의 ifHighSpeed 개체를 확인해야 합니다. IF-MIB 통계는 네트워크 용량을 평가할 때 유용할 수 있습니다.

Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스는 송수신된 멀티캐스트 및 브로드캐스트 패킷 수, 인터페이스가 무차별 모드인지의 여부, 인터페이스가 무차별 모드인지 그리고 물리적 커넥터가 있는지의 여부와 같은 인터페이스 정보를 제공하는 IF-MIB에서 ifXTable만 지원합니다.

RFC 2863은 이 MIB를 정의합니다.

## 호스트 리소스 MIB

HOST-RESOURCES-MIB는 호스트 컴퓨터 리소스에 대한 정보를 제공합니다. 이 MIB를 사용하여 CPU 및 메모리 사용 통계를 모니터링합니다. 예를 들어, 현재 CPU 로드(hrProcessorLoad 개체)를 확인하면 방화벽의 성능 문제를 해결하는 데 도움이 될 수 있습니다.

Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스는 다음 개체 그룹의 일부를 지원합니다.


©2023 Palo Alto Networks, Inc.

| 개체 그룹 | 설명 |
|---|---|
| hrDevice | CPU 부하, 저장 용량 및 파티션 크기와 같은 정보를 제공합니다. hrProcessorLoad OID는 패킷을 처리하는 코어의 평균을 제공합니다.<br>다중 데이터플레인(DP)이 있는 PA-7000 및 PA-5200 시리즈 방화벽의 경우 개별 데이터플레인 프로세서 사용률을 모니터링할 수 있습니다. 사용률이 서비스 가용성 문제를 방지하기 위해 각 DP 프로세서에 대한 특정 임계값에 도달할 때 경고를 설정합니다. |
| hrSystem | 시스템 가동 시간, 현재 사용자 세션 수, 현재 프로세스 수와 같은 정보를 제공합니다. |
| hrStorage | 사용된 스토리지의 양과 같은 정보를 제공합니다. |

RFC 2790은 이 MIB를 정의합니다.

## 엔터티-MIB

ENTITY-MIB는 여러 논리적 및 물리적 구성 요소에 대한 OID를 제공합니다 이 MIB를 사용하여 시스템에 로드되는 물리적 구성 요소(예: 팬 및 온도 센서)를 확인하고 모델 및 일련번호와 같은 관련 정보를 확인합니다. 이러한 구성요소의 색인 번호를 사용하여 ENTITY-SENSOR-MIB 및 ENTITY-STATE-MIB에서 작동 상태를 확인할 수도 있습니다.

Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스는 ENTPhysicalTable 그룹의 일부만 지원합니다.

| 개체 | 설명 |
|---|---|
| entPhysicalIndex | 디스크 슬롯과 디스크 드라이브가 포함된 단일 네임스페이스 |
| entPhysicalDescr | 구성 요소 설명입니다. |
| entPhysicalVendorType | 사용 가능한 경우 sysObjectID(PAN-PRODUCT-MIB.my 참조)(섀시 및 모듈 개체). |
| entPhysicalContainedIn | 이 구성 요소를 포함하는 구성 요소에 대한 EntPhysicalIndex의 값입니다. |
| entPhysicalClass | 섀시(3), 슬롯용 컨테이너(5), 전원 공급 디바이스(6), 팬(7), 각 온도 또는 기타 환경에 대한 센서(8) 및 각 라인 카드용 모듈(9) |
| entPhysicalParentRelPos | 형제 구성 요소 중 이 하위 구성 요소의 상대적 위치입니다. 형제 구성 요소는 EntPhysicalEntry 구성 요소로 정의되며, 이 구성 요소는 EntPhysicalContainedIn 및 entPhysicalClass 개체 각각에 대해 동일한 인스턴스 값을 공유합니다. |


©2023 Palo Alto Networks, Inc.

| 개체 | 설명 |
| --- | --- |
| entPhysicalName | 관리(MGT) 인터페이스에서 회선 카드 이름 지정을 허용하는 경우에만 지원됩니다. |
| entPhysicalHardwareRev | 공급업체별 구성 요소 하드웨어 버전입니다. |
| entPhysicalFirwareRev | 공급업체별 구성 요소 펌웨어 버전입니다. |
| entPhysicalSoftwareRev | 공급업체별 구성 요소 소프트웨어 버전입니다. |
| entPhysicalSerialNum | 공급업체별 구성 요소 일련번호입니다. |
| entPhysicalMfgName | 구성 요소 제조업체 이름입니다. |
| entPhysicalMfgDate | 구성요소가 제조된 날짜입니다. |
| entPhysicalModelName | 디스크 모델 번호입니다. |
| entPhysicalAlias | 네트워크 관리자가 구성 요소에 대해 지정한 별칭입니다. |
| entPhysicalAssetID | 네트워크 관리자가 구성 요소에 대해 지정한 사용자 할당 자산 추적 식별자입니다. |
| entPhysicalIsFRU | 구성 요소가 필드 교체 디바이스(FRU)인지의 여부를 나타냅니다. |
| entPhysicalUris | 구성요소의 CLEI(공용 언어 장비 식별자) 번호입니다(예: URN:CLEI:CNME120ARA). |

RFC 4133은 이 MIB를 정의합니다.

## ENTITY-SENSOR-MIB

ENTITY-SENSOR-MIB는 엔터티-MIB이(가) 정의하는 것 이상으로 네트워킹 장비의 물리적 센서에 대한 지원을 추가합니다. 이 MIB를 ENTITY-MIB와 함께 사용하여 시스템의 물리적 구성 요소(예: 팬 및 온도 센서)의 작동 상태를 모니터링합니다. 예를 들어, 환경 조건으로 인해 발생할 수 있는 문제를 해결하기 위해 ENTITY-MIB(entPhysicalDescr 개체)의 엔터티 인덱스를 ENTITY-SENSOR-MIB의 작동 상태 값(entPhysSensorOperStatus 개체)에 매핑할 수 있습니다. 다음 예에서는 PA-3020 방화벽의 모든 팬과 온도 센서가 작동하고 있습니다.

 ©2023 Palo Alto Networks, Inc.

| Name/OID | Value |
|---|---|
| entPhysicalDescr.1 | PA-3020 |
| entPhysicalDescr.2 | Fan #1 RPM |
| entPhysicalDescr.3 | Fan #2 RPM |
| entPhysicalDescr.4 | Fan #3 RPM |
| entPhysicalDescr.5 | Fan #4 RPM |
| entPhysicalDescr.6 | Temperature @ Ocelot |
| entPhysicalDescr.7 | Temperature @ Switch |
| entPhysicalDescr.8 | Temperature @ Cavium |
| entPhysicalDescr.9 | Temperature @ Intel PHY |
| entPhysicalDescr.10 | Temperature @ Switch Core |
| entPhysicalDescr.11 | Temperature @ Cavium Core |
| entPhySensorOperStatus.2 | ok (1) |
| entPhySensorOperStatus.3 | ok (1) |
| entPhySensorOperStatus.4 | ok (1) |
| entPhySensorOperStatus.5 | ok (1) |
| entPhySensorOperStatus.6 | ok (1) |
| entPhySensorOperStatus.7 | ok (1) |
| entPhySensorOperStatus.8 | ok (1) |
| entPhySensorOperStatus.9 | ok (1) |
| entPhySensorOperStatus.10 | ok (1) |
| entPhySensorOperStatus.11 | ok (1) |

동일한 ***OID***가 다른 플랫폼의 다른 센서를 참조할 수 있습니다. 대상 플랫폼에 대한 ***ENTITY-MIB***를 사용하여 값을 설명과 일치시키십시오.

Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스는 entPhySensorTable 그룹의 일부만 지원합니다. 지원되는 부분은 플랫폼에 따라 다르며 열(섭씨 온도) 및 팬(RPM) 센서만 포함합니다.

RFC 3433은 ENTITY-SENSOR-MIB를 정의합니다.

## ENTITY-STATE-MIB

ENTITY-STATE-MIB는 섀시 기반 플랫폼에서 구성 요소의 관리 및 작동 상태를 포함하여 엔터티-MIB에서 정의하는 것 이상의 물리적 구성 요소 상태에 대한 정보를 제공합니다. 이 MIB를 ENTITY-MIB와 함께 사용하여 PA-7000 시리즈 또는 PA-5450 방화벽의 구성 요소(예: 라인 카드, 팬 트레이 및 전원 공급 디바이스)의 작동 상태를 모니터링합니다. 예를 들어 위협 로그에 대한 로그 포워딩 문제를 해결하려면 ENTITY-MIB(entPhysicalDescr 개체)에서 ENTITY-STATE-MIB의 운영 상태 값(entStateOper 개체)에 로그 처리 카드(LPC) 인덱스를 매핑할 수 있습니다. 운영 상태 값은 숫자를 사용하여 상태를 나타냅니다. 알 수 없는 경우 1개, 비활성화용 2개, 활성화된 경우 3개, 테스트용 4. PA-7000 시리즈 및 PA-5450 방화벽은 이 MIB를 지원하는 유일한 Palo Alto Networks 방화벽입니다.

RFC 4268은 ENTITY-STATE-MIB를 정의합니다.

## IEEE 802.3 LAG MIB

IEEE 802.3 LAG MIB를 사용하여 링크 집계 제어 프로토콜(집계 인터페이스 그룹의 LACP)이 활성화된 집계 그룹의 상태를 모니터링하십시오. 방화벽이 LACP 이벤트를 기록할 때 문제 해결에 유용한 트랩도 생성합니다. 예를 들어, 트랩은 방화벽과 LACP 피어 간의 트래픽 중단이 연결 끊김 또는 일치하지 않는 인터페이스 속도 및 이중 값으로 인해 발생했는지의 여부를 알려줄 수 있습니다.

PAN-OS는 LACP에 대해 다음 SNMP 테이블을 구현합니다.

***dot3adTablesLastChanged*** 개체는 ***dot3adAggTable, dot3adAggPortListTable*** 및 ***dot3adAggPortTable***에 대한 가장 최근 변경 시간을 나타냅니다.

| 테이블 | 설명 |
|---|---|
| 집계 구성 테이블(dot3adAggTable) | 이 테이블에는 방화벽과 연결된 모든 집계 그룹에 대한 정보가 포함되어 있습니다. 각 집계 그룹에는 하나의 항목이 있습니다.<br>일부 테이블 개체에는 dot3adAggIndex 개체가 설명하는 제한 사항이 있습니다. 이 인덱스는 로컬 시스템이 집계 그룹에 할당하는 고유 식별자입니다. |


©2023 Palo Alto Networks, Inc.

| 테이블 | 설명 |
| --- | --- |
| | 포함하는 개체의 종속 관리 개체 중에서 집계 그룹 인스턴스를 식별합니다. 식별자는 읽기 전용입니다.<br><br>***ifTable MIB(***인터페이스 항목 목록***)***는 논리적 인터페이스를 지원하지 않으므로 집계 그룹에 대한 항목이 없습니다**.** |
| 집계 포트 목록 테이블(dot3adAggPortListTable) | 이 표에는 방화벽의 각 집계 그룹과 연결된 포트가 나열되어 있습니다. 각 집계 그룹에는 하나의 항목이 있습니다.<br><br>dot3adAggPortListPorts 속성은 집계 그룹과 연결된 전체 포트 집합을 나열합니다. 목록의 각 비트 세트는 포트 구성원을 나타냅니다. 섀시가 아닌 플랫폼의 경우 64비트 값입니다. 섀시 플랫폼의 경우 값은 8개의 64비트 항목 배열입니다. |
| 집계 포트 테이블(dot3adAggPortTable) | 이 테이블에는 방화벽의 집계 그룹과 연결된 모든 포트에 대한 LACP 구성 정보가 포함되어 있습니다. 각 포트에는 하나의 항목이 있습니다. 테이블에는 집계 그룹과 연결되지 않은 포트에 대한 항목이 없습니다. |
| LACP 통계 테이블(dot3adAggPortStatsTable) | 이 테이블에는 방화벽의 집계 그룹과 연결된 모든 포트에 대한 링크 집계 정보가 포함되어 있습니다. 각 포트에는 하나의 행이 있습니다. 테이블에는 집계 그룹과 연결되지 않은 포트에 대한 항목이 없습니다. |

IEEE 802.3 LAG MIB에는 다음과 같은 LACP 관련 트랩이 포함됩니다.

| 트랩 이름 | 설명 |
| --- | --- |
| panLACPLostConnectivityTrap | 피어에서 방화벽에 대한 연결이 끊어졌습니다. |
| panLACPUnresponsiveTrap | 피어가 방화벽에 응답하지 않습니다. |
| panLACPNegoFailTrap | 피어와의 LACP 협상에 실패했습니다. |
| panLACPSpeedDuplexTrap | 방화벽과 피어의 링크 속도와 이중 설정이 일치하지 않습니다. |
| panLACPLinkDownTrap | 집계 그룹의 인터페이스가 다운되었습니다. |
| panLACPLacpDownTrap | 집계 그룹에서 인터페이스가 제거되었습니다. |
| panLACPLacpUpTrap | 인터페이스가 집계 그룹에 추가되었습니다. |

MIB 정의는 IEEE 802.3 LAG MIB를 참조하십시오.


©2023 Palo Alto Networks, Inc.

## LLDP-V2-MIB.my

LLDP-V2-MIB를 사용하여 LLDP(Link Layer Discovery Protocol) 이벤트를 모니터링합니다. 예를 들어 lldpV2StatsRxPortFramesDiscardedTotal 개체를 확인하여 어떤 이유로든 삭제된 LLDP 프레임 수를 확인할 수 있습니다. Palo Alto Networks 방화벽은 LLDP를 사용하여 인접 디바이스와 해당 기능을 검색합니다. LLDP는 특히 핑(ping) 또는 트레이스라우트(traceroute) 유틸리티가 방화벽을 감지하지 못하는 가상 와이어 배포의 경우 문제 해결을 더 쉽게 생성합니다.

Palo Alto Networks 방화벽은 다음을 제외한 모든 LLDP-V2-MIB 개체를 지원합니다.

- 다음 lldpV2Statistics 개체:
  - lldpV2StatsRemTablesLastChangeTime
  - lldpV2StatsRemTablesInserts
  - lldpV2StatsRemTablesDeletes
  - lldpV2StatsRemTablesDrops
  - lldpV2StatsRemTablesAgeouts
- 다음 lldpV2RemoteSystemsData 개체:
  - lldpV2RemOrgDefInfoTable 테이블
  - lldpV2RemTable 테이블에서 : lldpV2RemTimeMark

RFC 4957은 이 MIB를 정의합니다.

## BFD-STD-MIB

BFD(Bidirectional Forwarding Detection) MIB를 사용하여 인터페이스, 데이터 링크 또는 실제 엔진과 같은 두 포워딩 엔진 간의 양방향 경로에 대한 오류 경고를 모니터링하고 수신합니다. 예를 들어 bfdSessState 개체를 확인하여 포워딩 엔진 간의 BFD 세션 상태를 볼 수 있습니다. Palo Alto Networks 구현에서 포워딩 엔진 중 하나는 방화벽 인터페이스이고 다른 하나는 인접한 구성된 BFD 피어입니다.

RFC 7331은 이 MIB를 정의합니다.

## PAN-COMMON-MIB.my

PAN-COMMON-MIB를 사용하여 Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스에 대한 다음 정보를 모니터링합니다.

| 개체 그룹 | 설명 |
|---|---|
| panSys | 시스템 소프트웨어/하드웨어 버전, 동적 콘텐츠 버전, 일련번호, HA 모드/상태 및 전역 카운터와 같은 개체를 포함합니다.<br><br>전역 카운터에는 서비스 거부(DoS), IP 조각화, TCP 상태 및 삭제된 패킷과 관련된 카운터가 포함됩니다. 이러한 카운터를 추적하면 DoS 공격, 시스템 또는 연결 오류 또는 리소스 제한으로 인한 트래픽 불규칙성을 모니터링할 수 있습니다. PAN-COMMON-MIB는 방화벽용 전역 카운터를 지원하지만 Panorama용은 지원하지 않습니다. |

 ©2023 Palo Alto Networks, Inc.

| 개체 그룹 | 설명 |
|---|---|
| panChassis | 섀시 유형 및 M-시리즈 어플라이언스 모드(Panorama 또는 로그 수집기). |
| panSession | 세션 사용 정보. 예를 들어 방화벽 또는 특정 가상 시스템의 총 활성 세션 수입니다. |
| panMgmt | 방화벽에서 Panorama 관리 서버로의 연결 상태입니다. |
| panGlobalProtect | GlobalProtect 게이트웨이 사용률(백분율), 허용되는 최대 터널 및 활성 터널 수. |
| panLogCollector | 로깅 비율, 로그 할당량, 디스크 사용량, 보존 기간, 로그 중복성(활성화 또는 비활성화), 방화벽에서 Log Collector로의 포워딩 상태, Log Collector에서 외부 서비스로의 포워딩 상태 및 상태를 포함한 각 Log Collector에 대한 로깅 통계 방화벽-로그 수집기 연결. |
| panDeviceLogging | 로깅 속도, 디스크 사용량, 보존 기간, 개별 방화벽에서 Panorama 및 외부 서버로의 포워딩 상태, 방화벽-Log Collector 연결 상태를 포함한 각 방화벽에 대한 로깅 통계. |

## PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my에는 Palo Alto Networks 엔터프라이즈 MIB 모듈의 다양한 하위 트리에 대한 글로벌 최상위 OID 정의가 포함되어 있습니다. 이 MIB에는 모니터링할 개체가 포함되어 있지 않습니다. 다른 MIB에서 참조하는 경우에만 필요합니다.

## PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my는 Palo Alto Networks 엔터프라이즈 MIB 모듈에 있는 개체의 텍스트 값에 대한 규칙(예: 문자 길이 및 허용되는 문자)을 정의합니다. 모든 Palo Alto Networks 제품은 이러한 규칙을 사용합니다. 이 MIB에는 모니터링할 개체가 포함되어 있지 않습니다. 다른 MIB에서 참조하는 경우에만 필요합니다.

## PAN-LC-MIB.my

PAN-LC-MIB.my 로그 컬렉터(로그 컬렉터 모드의 M-시리즈 어플라이언스)가 구현하는 관리되는 개체의 정의가 포함되어 있습니다. 이 MIB를 사용하여 로깅 속도, 로그 데이터베이스 저장소 기간(일) 및 로그 컬렉터의 각 논리 디스크(최대 4개)의 디스크 사용량(MB)을 모니터링합니다. 예를 들어 이 정보를 사용하여 아카이빙을 위해 외부 서버(예: syslog 서버)에 로그 컬렉터 또는 포워딩 로그를 추가해야 하는지의 여부를 확인할 수 있습니다.

## PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my는 모든 Palo Alto Networks 제품에 대한 sysObjectID OID를 정의합니다. 이 MIB에는 모니터링할 개체가 포함되어 있지 않습니다. 다른 MIB에서 참조하는 경우에만 필요합니다.


©2023 Palo Alto Networks, Inc.

## PAN-ENTITY-EXT-MIB.my

PAN-ENTITY-EXT-MIB.my를 엔터티-MIB과 함께 사용하여 PA-7000 시리즈 또는 PA-5450 방화벽의 물리적 구성요소(예: 팬 트레이 및 전원 공급 디바이스)의 전력 사용량을 모니터링합니다. 이는 이 MIB를 지원하는 유일한 두 개의 Palo Alto Networks 방화벽입니다. 예를 들어 로그 포워딩 문제를 해결할 때 LPC(로그 처리 카드)의 전원 사용량을 확인할 수 있습니다. ENTY-MIB(ENTPhysicalDescr 개체)의 LPC 인덱스를 PAN-ENTITY-EXT-MIB(PANENTRYFRU모델 전원 사용 개체)의 값에 매핑할 수 있습니다.

## PAN-TRAPS.my

PAN-TRAPS.my를 사용하여 생성된 모든 트랩의 전체 목록과 이에 대한 정보(예: 설명)를 확인하십시오. Palo Alto Networks 방화벽, Panorama 및 WF-500 어플라이언스가 지원하는 트랩 목록은 PAN-COMMON-MIB.my **panCommonEvents** > **panCommonEventsEvents** > **panCommonEventEventsV2** 개체를 참조하십시오.


©2023 Palo Alto Networks, Inc.

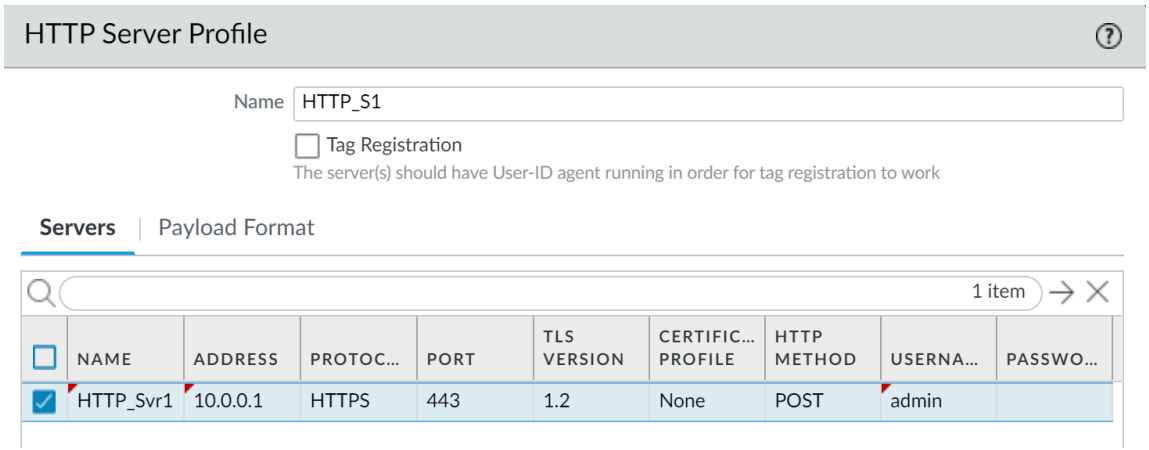
# HTTP/S 대상에 로그 포워딩

방화벽과 Panorama™는 로그를 HTTP/S 서버로 전달할 수 있습니다. 이벤트가 발생할 때 외부 HTTP 기반 서비스에서 작업을 트리거하기 위해 모든 로그 또는 특정 로그를 포워딩하도록 선택할 수 있습니다. 로그를 HTTP 서버로 포워딩할 때 방화벽 로그의 속성을 기반으로 하는 작업을 트리거하도록 HTTP 기반 API 요청을 타사 서비스에 직접 전송하도록 방화벽을 구성합니다. API를 노출하는 HTTP 기반 서비스에서 작동하도록 방화벽을 구성하고 HTTP 요청의 URL, HTTP 헤더, 파라미터 및 페이로드를 수정하여 통합 요구 사항을 충족할 수 있습니다.

**STEP 1 |** HTTP 서버 프로파일을 만들어 로그를 HTTP/S 대상으로 포워딩합니다.

HTTP 서버 프로파일을 사용하면 서버에 액세스하는 방법을 지정하고 HTTP/S 대상으로 로그를 포워딩하는 형식을 정의할 수 있습니다. 기본적으로 방화벽은 관리 포트를 사용하여 이러한 로그를 포워딩합니다. 그러나 기기 > 설정 > 서비스 > 서비스 경로 구성에서 다른 소스 인터페이스와 IP 주소를 할당할 수 있습니다.

1. 디바이스 > 서버 프로파일 > **HTTP** 및 새 프로파일 추가를 선택합니다.
2. 서버 프로파일의 이름을 지정하고 위치를 선택합니다. 프로파일은 모든 가상 시스템에서 공유되거나 특정 가상 시스템에 속할 수 있습니다.
3. 각 서버에 대한 세부 정보를 추가합니다. 각 프로파일에는 최대 4개의 서버가 있을 수 있습니다.
4. 이름 및 IP주소를 입력합니다.
5. 프로토콜(**HTTP** 또는 **HTTPS**)을 선택합니다. 기본 포트는 각각 80 또는 443이지만 HTTP 서버가 수신하는 포트와 일치하도록 포트 번호를 수정할 수 있습니다.
6. 서버에서 지원되는 **TLS** 버전(**1.0**, **1.1** 또는 **1.2**(기본값))을 선택합니다.
7. 서버와의 TLS 연결에 사용할 인증서 프로파일을 선택합니다.
8. 타사 서비스가 지원하는 **HTTP** 메서드(**DELETE**, **GET**, **POST**(기본값) 또는 **PUT**)를 선택합니다.
9. (선택 사항) 필요한 경우 서버 인증을 위한 사용자 이름 및 암호를 입력합니다.
10. (선택 사항) 서버 연결 테스트를 선택하여 방화벽과 HTTP/S 서버 간의 네트워크 연결을 확인합니다.

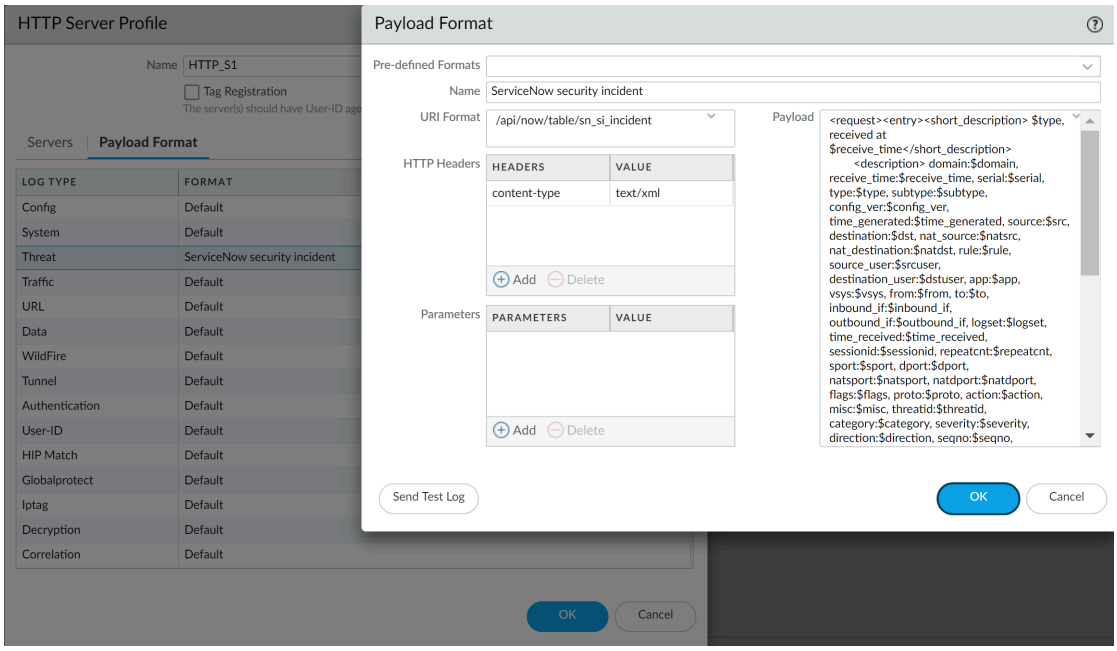



 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** HTTP 요청에 대한 페이로드 형식을 선택합니다.

1. HTTP 요청 형식을 정의하려는 각 로그 유형에 대한 로그 유형 링크를 선택하십시오.
2. 미리 정의된 형식(콘텐츠 업데이트를 통해 사용 가능)을 선택하거나 사용자 지정 형식을 만듭니다.

   사용자 지정 형식을 만드는 경우 **URI**는 HTTP 서비스의 리소스 엔드포인트입니다. 방화벽은 앞에서 정의한 IP 주소에 URI를 추가하여 HTTP 요청에 대한 URL을 구성합니다. URI 및 페이로드 형식이 타사 벤더가 요구하는 구문과 일치하는지 확인합니다. HTTP 헤더, 파라미터 및 값 쌍, 요청 페이로드 내에서 선택한 로그 유형에서 지원되는 모든 속성을 사용할 수 있습니다.

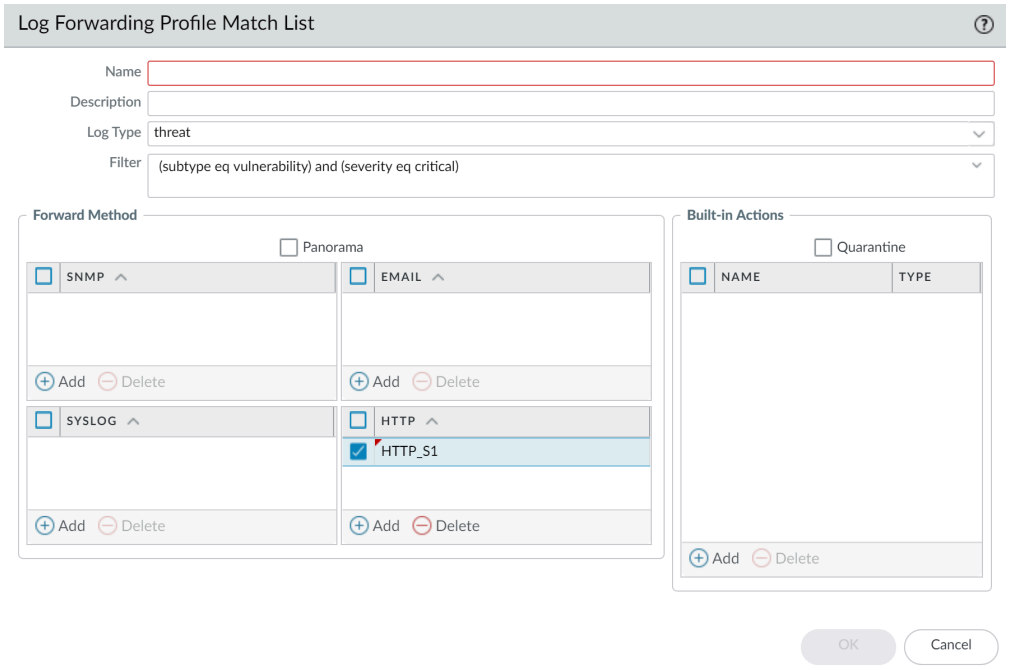



3. 테스트 로그를 보내 HTTP 서버가 요청을 수신하는지 확인합니다. 대화식으로 테스트 로그를 보낼 때 방화벽은 형식을 그대로 사용하며 변수를 방화벽 로그의 값으로 대체하지 않습니다. HTTP 서버가 404 응답을 보내는 경우 서버가 요청을 성공적으로 처리할 수 있도록 매개 변수에 대한 값을 제공합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 방화벽이 로그를 HTTP 서버로 포워딩하는 시기에 대한 일치 조건을 정의하고 사용할 HTTP 서버 프로파일을 연결합니다.

1. 워크플로를 트리거할 로그 유형을 선택합니다.
   - 사용자 작업(예: 트래픽, 위협 또는 인증 로그)과 관련된 로그에 대한 로그 포워딩 프로파일(개체 > 로그 포워딩)을 추가합니다.
   - 구성 또는 시스템 로그와 같은 시스템 이벤트와 관련된 로그에 대해 디바이스 > 로그 설정을 선택합니다.
2. 로그 유형을 선택하고 새로운 필터 빌더를 사용하여 일치 기준을 정의하십시오.
3. HTTP 대상에 로그를 포워딩하기 위한 HTTP 서버 프로파일을 추가합니다.




 ©2023 Palo Alto Networks, Inc.

# NetFlow 모니터링

NetFlow는 방화벽이 인터페이스를 수신하는 IP 트래픽에 대한 통계를 내보내는 데 사용할 수 있는 업계 표준 프로토콜입니다. 방화벽은 통계를 NetFlow 필드로 NetFlow 수집기에 내보냅니다. NetFlow 수집기는 보안, 관리, 회계 및 문제 해결을 위해 네트워크 트래픽을 분석하는 데 사용하는 서버입니다. 모든 Palo Alto Networks 방화벽은 NetFlow 버전 9를 지원합니다. 방화벽은 양방향이 아닌 단방향 NetFlow만 지원합니다. 방화벽은 인터페이스의 모든 IP 패킷에서 NetFlow 처리를 수행하며 샘플링된 NetFlow를 지원하지 않습니다. 레이어 3, 레이어 2, 가상 와이어, 탭, VLAN, 루프백 및 터널 인터페이스에 대한 NetFlow 레코드를 내보낼 수 있습니다. 집계 이더넷 하위 인터페이스의 경우 그룹 내에서 데이터가 흐르는 개별 하위 인터페이스에 대한 레코드를 내보낼 수 있습니다. NetFlow 수집기에서 방화벽 인터페이스를 식별하려면 SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자을(를) 참조하십시오. 방화벽은 표준 및 엔터프라이즈(PAN-OS 관련)를 지원하며NetFlow 템플릿, NetFlow 수집기가 NetFlow 필드를 복호화하는 데 사용합니다.

- NetFlow 내보내기 구성
- NetFlow 템플릿

## NetFlow 내보내기 구성

NetFlow 수집기를 사용하여 네트워크 트래픽 들어오는 방화벽 인터페이스를 분석하려면 다음 단계를 수행하여 NetFlow 레코드 내보내기를 구성합니다.

**STEP 1 |** NetFlow 서버 프로파일을 생성합니다.

프로파일은 내보낸 레코드를 수신할 NetFlow 컬렉터를 정의하고 내보내기 매개 변수를 지정합니다.

1. 디바이스 > 서버 프로파일 > **NetFlow**를 선택하고 프로파일을 추가합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. NetFlow 수집기의 요구 사항에 따라 방화벽이 NetFlow 템플릿을 분(기본값은 30) 및 패킷(내보낸 레코드 - 기본값은 20)으로 새로 고치는 속도를 지정합니다. 방화벽은 두 임계값을 통과한 후 템플릿을 새로 고칩니다.
4. 방화벽이 레코드를 내보내는 빈도인 활성 시간 초과를 지정합니다(기본값은 5).
5. 방화벽에서 앱 ID 및 User-ID 필드를 내보내도록 하려면 **PAN-OS** 필드 유형을 선택합니다.
6. 레코드를 수신할 각 NetFlow 컬렉터(프로파일당 최대 2개)를 추가합니다. 각 컬렉터에 대해 다음을 지정합니다.
   - 컬렉터를 식별하는 이름입니다.
   - **NetFlow** 서버 호스트 이름 또는 IP 주소입니다.
   - 액세스 포트(기본값 2055).
7. 확인을 클릭하여 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 분석하려는 트래픽이 수신되는 방화벽 인터페이스에 NetFlow 서버 프로파일을 할당합니다.

이 예에서는 기존 이더넷 인터페이스에 프로파일을 할당합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 인터페이스 이름을 클릭하여 수정합니다.

   레이어 *3*, 레이어 *2*, 가상 와이어, 탭, *VLAN*, 루프백 및 터널 인터페이스에 대한 *NetFlow* 레코드를 내보낼 수 있습니다. 집계 이더넷 인터페이스의 경우 그룹 내에서 데이터가 흐르는 개별 하위 인터페이스에 대한 레코드를 내보낼 수 있습니다.

2. 구성한 NetFlow 서버 프로파일(**NetFlow** 프로파일)을 선택한 다음 확인을 클릭합니다.

**STEP 3 |** **(PA-7000** 시리즈**, PA-5400** 시리즈 및 **PA-5200** 시리즈 방화벽에 필요**)** 방화벽이 사용할 인터페이스에 대한 서비스 경로 구성 NetFlow 레코드를 전송합니다.

PA-7000 시리즈, PA-5400 시리즈 및 PA-5200 시리즈 방화벽에서 NetFlow 레코드를 전송하는 데 관리(MGT) 인터페이스를 사용할 수 없습니다. 다른 방화벽 모델의 경우 서비스 경로는 선택 사항입니다. 모든 방화벽에서 NetFlow 레코드를 전송하는 인터페이스는 방화벽이 레코드를 수집하는 인터페이스와 같지 않아도 됩니다.

1. 디바이스 > 설정 > 서비스를 선택합니다.
2. **(**여러 가상 시스템이 있는 방화벽**)** 다음 중 하나를 선택합니다.
   - 글로벌 - 서비스 경로가 방화벽의 모든 가상 시스템에 적용되는 경우 이 옵션을 선택합니다.
   - 가상 시스템 - 서비스 경로가 특정 가상 시스템에 적용되는 경우 이 옵션을 선택합니다. 위치를 가상 시스템으로 설정합니다.
3. 서비스 경로 구성을 선택하고 사용자 지정합니다.
4. 인터페이스에서 사용하는 프로토콜(**IPv4** 또는 **IPv6**)을 선택합니다. 필요한 경우 두 프로토콜 모두에 대한 서비스 경로를 구성할 수 있습니다.
5. 서비스 열에서 **Netflow**를 클릭합니다.
6. 소스 인터페이스를 선택합니다.

   모두, 기본값 사용 및 ***MGT***는 *PA-7000* 시리즈, *PA-5400* 시리즈 또는 *PA-5200* 시리즈 방화벽에서 *NetFlow* 레코드를 전송하는 데 사용할 수 있는 유효한 인터페이스 옵션이 아닙니다.

7. 소스 주소(IP 주소)를 선택합니다.
8. 확인을 두 번 클릭하여 변경 사항을 저장합니다.

**STEP 4 |** 변경 사항을 커밋합니다.

**STEP 5 |** NetFlow 수집기에서 방화벽 트래픽을 모니터링합니다.

NetFlow 컬렉터 설명서를 참조하십시오.

통계를 모니터링할 때는 *NetFlow Collector*의 인터페이스 인덱스를 방화벽 웹 인터페이스의 인터페이스 이름과 일치시켜야 합니다. 자세한 내용은 SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자를 참조하십시오.

NetFlow 전송 문제를 해결하려면 운영 CLI 명령 `디버그 로그-수신기 NetFlow 통계`를 사용합니다.

 ©2023 Palo Alto Networks, Inc.

# NetFlow 템플릿

NetFlow 수집기는 템플릿을 사용하여 방화벽이 내보내는 필드를 복호화합니다. 방화벽은 내보낸 데이터 유형에 따라 템플릿을 선택합니다. IPv4 또는 IPv6 트래픽, NAT 유무에 관계없이 표준 또는 엔터프라이즈별(PAN-OS 특정) 필드. 방화벽은 주기적으로 템플릿을 새로 고쳐 사용할 템플릿을 다시 평가하고(내보낸 데이터 유형이 변경되는 경우) 선택한 템플릿의 필드에 변경 내용을 적용합니다. NetFlow 내보내기 구성을 할 때 NetFlow 수집기의 요구 사항에 따라 시간 간격과 내보낸 레코드 수를 기반으로 새로 고침 빈도를 설정합니다. 방화벽은 두 임계값을 통과한 후 템플릿을 새로 고칩니다.

Palo Alto Networks 방화벽은 다음과 같은 NetFlow 템플릿을 지원합니다.

| 템플렛 | ID |
|---|---|
| IPv4 표준 | 256 |
| IPv4 엔터프라이즈 | 257 |
| IPv6 표준 | 258 |
| IPv6 엔터프라이즈 | 259 |
| NAT 표준이 있는 IPv4 | 260 |
| NAT 엔터프라이즈가 있는 IPv4 | 261 |
| NAT 표준이 있는 IPv6 | 262 |
| NAT 엔터프라이즈가 있는 IPv6 | 263 |

다음 표에는 방화벽이 보낼 수 있는 NetFlow 필드와 이를 정의하는 템플릿이 나열되어 있습니다.

| 값 | 필드 | 설명 | 템플릿 |
|---|---|---|---|
| 1 | IN_BYTES | IP 흐름과 관련된 바이트 수에 대해 길이 N * 8비트가 있는 들어오는 카운터입니다. 기본적으로 N은 4입니다. | 모든 템플릿 |
| 2 | IN_PKTS | IP 광선과 연결된 패킷 수에 대한 길이 N * 8 비트가 있는 들어오는 카운터입니다. 기본적으로 N은 4입니다. | 모든 템플릿 |
| 4 | 프로토콜 | IP 프로토콜 바이트. | 모든 템플릿 |
| 5 | TOS | ingress 인터페이스를 입력할 때 서비스 바이트 설정 유형입니다. | 모든 템플릿 |


©2023 Palo Alto Networks, Inc.

| 값 | 필드 | 설명 | 템플릿 |
|---|---|---|---|
| 6 | TCP_FLAGS | 이 흐름의 모든 TCP 플래그의 합계입니다. | 모든 템플릿 |
| 7 | L4_SRC_PORT | TCP/UDP 소스 포트 번호(예: FTP, 텔넷 또는 이와 동급). | 모든 템플릿 |
| 8 | IPV4_SRC_ADDR | IPv4 소스 주소입니다. | IPv4 표준<br>IPv4 엔터프라이즈<br>IPv4(NAT 표준)<br>IPv4(NAT 엔터프라이즈) |
| 10 | INPUT_SNMP | 입력 인터페이스 인덱스입니다. 값 길이는 기본적으로 2바이트이지만 값이 높을 수 있습니다. Palo Alto Networks 방화벽이 인터페이스 인덱스를 생성하는 방법에 대한 자세한 내용은 SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자를 참조하십시오. | 모든 템플릿 |
| 11 | L4_DST_PORT | TCP/UDP 대상 포트 번호(예: FTP, Telnet 또는 이와 동급). | 모든 템플릿 |
| 12 | IPV4_DST_ADDR | IPv4 대상 주소입니다. | IPv4 표준<br>IPv4 엔터프라이즈<br>IPv4(NAT 표준)<br>IPv4(NAT 엔터프라이즈) |
| 14 | OUTPUT_SNMP | 출력 인터페이스 인덱스입니다. 값 길이는 기본적으로 2바이트이지만 값이 높을 수 있습니다. Palo Alto Networks 방화벽이 인터페이스 인덱스를 생성하는 방법에 대한 자세한 내용은 SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자를 참조하십시오. | 모든 템플릿 |
| 21 | LAST_SWITCHED | 이 흐름의 마지막 패킷이 전환되었을 때의 시스템 가동 시간(밀리초)입니다. | 모든 템플릿 |


©2023 Palo Alto Networks, Inc.

| 값 | 필드 | 설명 | 템플릿 |
|---|---|---|---|
| 22 | FIRST_SWITCHED | 이 흐름의 첫 번째 패킷이 전환되었을 때의 시스템 가동 시간(밀리초)입니다. | 모든 템플릿 |
| 27 | IPV6_SRC_ADDR | IPv6 소스 주소입니다. | IPv6 표준<br>IPv6 엔터프라이즈<br>IPv6(NAT 표준)<br>IPv6(NAT 엔터프라이즈) |
| 28 | IPV6_DST_ADDR | IPv6 대상 주소입니다. | IPv6 표준<br>IPv6 엔터프라이즈<br>IPv6(NAT 표준)<br>IPv6(NAT 엔터프라이즈) |
| 32 | ICMP_TYPE | 인터넷 제어 메시지 프로토콜(ICMP) 패킷 유형입니다. 이는 다음과 같이 보고됩니다.<br>ICMP 유형 * 256 + ICMP 코드 | 모든 템플릿 |
| 61 | 방향 | 흐름 방향:<br>• 0 = ingress<br>• 1 = egress | 모든 템플릿 |
| 148 | flowId | 관측 도메인 내에서 고유한 흐름의 식별자입니다. IP 주소 및 포트 번호와 같은 흐름 키가 보고되지 않거나 별도의 레코드에 보고되지 않은 경우 이 정보 요소를 사용하여 다른 흐름을 구분할 수 있습니다. flowID는 트래픽 및 위협 로그의 세션 ID 필드에 해당합니다. | 모든 템플릿 |
| 233 | firewallEvent | 방화벽 이벤트를 나타냅니다.<br>• 0 = 무효 - 사용되지 않았습니다.<br>• 1 = 플로우 생성 - NetFlow 데이터 레코드는 새 플로우에 대한 것입니다. | 모든 템플릿 |


©2023 Palo Alto Networks, Inc.

| 값 | 필드 | 설명 | 템플릿 |
|---|---|---|---|
| | | • 2 = 플로우 삭제 - NetFlow 데이터 레코드는 플로우의 끝에 대한 것입니다.<br>• 3 = 플로우 거부 - NetFlow 데이터 레코드는 방화벽 정책이 거부된 플로우를 나타냅니다.<br>• 4 = 플로우 경고 - 사용되지 않았습니다.<br>• 5 = 플로우 업데이트 - NetFlow 데이터 레코드는 NetFlow 서버 프로파일에 구성된 활성 타임아웃 기간보다 오래 지속되는 플로우인 장기 지속 플로우에 대해 전송됩니다. | |
| 225 | postNATSourceIPv4Address | 이 정보 요소의 정의는 패킷이 인터페이스를 통과한 후 네트워크 주소 변환 중에 생성된 방화벽이 수정된 값을 보고한다는 점을 제외하면 sourceIPv4Address의 정의와 동일합니다. | IPv4(NAT 표준)<br>IPv4(NAT 엔터프라이즈) |
| 226 | postNATDestinationIPv4Address | 이 정보 요소의 정의는 패킷이 인터페이스를 통과한 후 네트워크 주소 변환 중에 방화벽이 생성한 수정된 값을 보고한다는 점을 제외하고는 destinationIPv4Address의 정의와 동일합니다. | IPv4(NAT 표준)<br>IPv4(NAT 엔터프라이즈) |
| 227 | postNAPTSourceTransportPort | 이 정보 요소의 정의는 패킷이 인터페이스를 통과한 후 네트워크 주소 포트 변환 중에 생성된 방화벽이 수정된 값을 보고한다는 점을 제외하면 sourceTransportPort의 정의와 동일합니다. | IPv4(NAT 표준)<br>IPv4(NAT 엔터프라이즈) |
| 228 | postNAPTDestinationTransportPort | 이 정보 요소의 정의는 패킷이 인터페이스를 통과한 후 네트워크 주소 포트 변환 중에 방화벽이 생성한 수정된 값을 보고한다는 점을 제외하고는 destinationTransportPort의 정의와 동일합니다. | IPv4(NAT 표준)<br>IPv4(NAT 엔터프라이즈) |


©2023 Palo Alto Networks, Inc.

| 값 | 필드 | 설명 | 템플릿 |
|---|---|---|---|
| 281 | postNATSourceIPv6Address | 이 정보 요소의 정의는 패킷이 인터페이스를 통과한 후 NAT64 네트워크 주소 변환 중에 생성된 방화벽이 수정된 값을 보고한다는 점을 제외하면 정보 요소 sourceIPv6Address의 정의와 동일합니다. IPv6 헤더에서 소스 주소 필드의 정의에 대한 RFC 2460을 참조하십시오. NAT64 사양의 경우 RFC 6146을 참조하십시오. | IPv6(NAT 표준)<br>IPv6(NAT 엔터프라이즈) |
| 282 | postNATDestinationIPv6Address | 이 정보 요소의 정의는 패킷이 인터페이스를 통과한 후 NAT64 네트워크 주소 변환 동안 방화벽이 생성한 수정된 값을 보고한다는 점을 제외하고 정보 요소 destinationIPv6Address의 정의와 동일합니다. IPv6 헤더에서 대상 주소 필드의 정의에 대한 RFC 2460을 참조하십시오. NAT64 사양의 경우 RFC 6146을 참조하십시오. | IPv6(NAT 표준)<br>IPv6(NAT 엔터프라이즈) |
| 346 | privateEnterpriseNumber | Palo Alto Networks를 식별하는 고유한 개인 엔터프라이즈 번호입니다. 25461. | IPv4 엔터프라이즈<br>IPv4(NAT 엔터프라이즈)<br>IPv6 엔터프라이즈<br>IPv6(NAT 엔터프라이즈) |
| 56701 | App-ID | App-ID가 식별한 애플리케이션의 이름입니다. 이름은 최대 32바이트일 수 있습니다. | IPv4 엔터프라이즈<br>IPv4(NAT 엔터프라이즈)<br>IPv6 엔터프라이즈<br>IPv6(NAT 엔터프라이즈) |
| 56702 | User-ID | 사용자 ID가 식별한 사용자 이름입니다. 이름은 최대 64바이트일 수 있습니다. | IPv4 엔터프라이즈<br>IPv4(NAT 엔터프라이즈)<br>IPv6 엔터프라이즈<br>IPv6(NAT 엔터프라이즈) |


©2023 Palo Alto Networks, Inc.

# SNMP 관리자 및 NetFlow 수집기의 방화벽 인터페이스 식별자

NetFlow 수집기(NetFlow 모니터링 참조) 또는 SNMP 관리자(SNMP 모니터링 및 트랩 참조)를 사용하여 Palo Alto Networks 방화벽을 모니터링하는 경우 인터페이스 인덱스(SNMP ifindex 개체)는 특정 흐름을 수행하는 인터페이스를 식별합니다(SNMP 관리자의 인터페이스 인덱스 참조). 반면 방화벽 웹 인터페이스는 인터페이스 이름을 인덱스가 아닌 식별자(예: ethernet1/1)로 사용합니다. NetFlow 수집기 또는 SNMP 관리자에 표시되는 통계가 어떤 방화벽 인터페이스에 적용되는지 이해하려면 인터페이스 인덱스를 인터페이스 이름과 일치시킬 수 있어야 합니다.

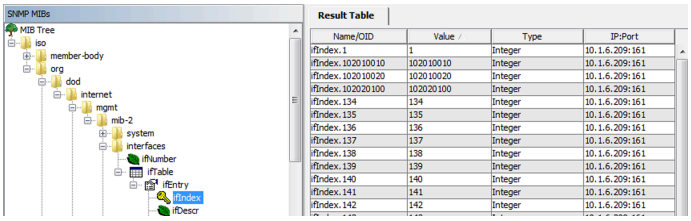



그림 **3: SNMP** 관리자의 인터페이스 인덱스

방화벽에서 인덱스를 계산하는 데 사용하는 공식을 이해하면 인덱스를 이름과 일치시킬 수 있습니다. 수식은 플랫폼 및 인터페이스 유형(물리적 또는 논리적)에 따라 다릅니다.

물리적 인터페이스 인덱스의 범위는 1-9999이며 방화벽은 다음과 같이 계산합니다.

| 방화벽 플랫폼 | 계산 | 예제 인터페이스 인덱스 |
|---|---|---|
| VM-Series | 관리 포트 수+물리적 포트 오프셋<br>• 관리 포트 수 - 상수 1입니다.<br>• 물리적 포트 오프셋 - 물리적 포트 번호입니다. | VM-100 방화벽, Eth1/4 =<br>1(관리 포트 수) + 4(물리적 포트) = **5** |
| PA-220, PA-220R, PA-800 시리즈 | 관리 포트 수+물리적 포트 오프셋<br>• 관리 포트 수 - 이 값은 상수가 5개입니다.<br>• 물리적 포트 오프셋 - 물리적 포트 번호입니다. | PA-5200 시리즈 방화벽, Eth1/4 =<br>5(관리 포트 수) + 4(물리적 포트) = **9** |
| PA-3200 시리즈, PA-5200 시리즈 | 관리 포트 수+물리적 포트 오프셋<br>• 관리 포트 수 - 이 값은 상수 4개입니다.<br>• 물리적 포트 오프셋 - 물리적 포트 번호입니다. | PA-5200 시리즈 방화벽, Eth1/4 =<br>4(관리 포트 수) + 4(물리적 포트) = **8** |


©2023 Palo Alto Networks, Inc.

| 방화벽 플랫폼 | 계산 | 예제 인터페이스 인덱스 |
|---|---|---|
| PA-7000 시리즈 | (최대 포트* 슬롯) +물리적 포트 오프셋+관리 포트 수<br>• 최대 포트 - 상수는 64입니다.<br>• 슬롯 - 네트워크 인터페이스 카드의 섀시 슬롯 번호입니다.<br>• 물리적 포트 오프셋 - 물리적 포트 번호입니다.<br>• 관리 포트 수 - 이 값은 상수가 5개입니다. | PA-7000 시리즈 방화벽, Eth3/9 =<br>[64(최대 포트) * 3(슬롯)] + 9(물리적 포트) + 5(관리 포트 수) = **206** |

모든 플랫폼에 대한 논리적 인터페이스 인덱스는 방화벽에서 다음과 같이 계산하는 9자리 숫자입니다.

| 인터페이스 유형 | 범위 | 숫자 **9** | 숫자 **7-8** | 숫자 **5-6** | 숫자 **1-4** | 예제 인터페이스 인덱스 |
|---|---|---|---|---|---|---|
| 레이어 3 서브인터페이스 | 101010001-199999999 | 유형: 1 | 인터페이스 슬롯: 1-9(01-09) | 인터페이스 포트: 1-9(01-09) | 하위 인터페이스: suffix 1-9999(0001-9999) | Eth1/5.22 = 100000000(타입) + 10000000(슬롯) + 50000(포트) + 22(suffix) = **101050022** |
| 레이어 2 서브인터페이스 | 101010001-199999999 | 유형: 1 | 인터페이스 슬롯: 1-9(01-09) | 인터페이스 포트: 1-9(01-09) | 하위 인터페이스: suffix 1-9999(0001-9999) | Eth2/3.6 = 100000000(타입) + 20000000(슬롯) + 30000(포트) + 6(suffix) = **102030006** |
| Vwire 하위 인터페이스 | 101010001-199999999 | 유형: 1 | 인터페이스 슬롯: 1-9(01-09) | 인터페이스 포트: 1-9(01-09) | 하위 인터페이스: suffix 1-9999(0001-9999) | Eth4/2.312 = 100000000(타입) + 40000000(슬롯) + 20000(포트) + 312(suffix) = **104020312** |
| VLAN | 200000001-200009999 | 유형: 2 | 00 | 00 | VLAN 접미사: 1-9999(0001-9999) | VLAN.55 = 200000000(type) + 55(suffix) = **200000055** |
| 루프백 | 300000001-300009999 | 유형: 3 | 00 | 00 | 루프백 접미사: 1-9999(0001-9999) | Loopback.55 = 300000000(type) + 55(suffix) = **300000055** |


©2023 Palo Alto Networks, Inc.

| 인터페이스 유형 | 범위 | 숫자 **9** | 숫자 **7-8** | 숫자 **5-6** | 숫자 **1-4** | 예제 인터페이스 인덱스 |
|---|---|---|---|---|---|---|
| 터널 | 400000001-400009999 | 유형: 4 | 00 | 00 | 터널 접미사: 1-9999(0001-9999) | 터널.55 = 400000000(유형) +55(suffix) = **400000055** |
| 집계 그룹 | 500010001-500089999 | 유형: 5 | 00 | AE 접미사: 1-8(01-08) | 하위 인터페이스: suffix 1-9999(0001-9999) | AE5.99 = 500000000(type) + 50000(AE Suffix) + 99(suffix) = **500050099** |


©2023 Palo Alto Networks, Inc.

# 모니터 트랜시버

물리적 어플라이언스 또는 디바이스의 트랜시버 상태를 모니터링하여 보다 쉽게 설치하고 문제를 해결할 수 있습니다. 볼 수 있는 진단은 전송된 바이어스 전류, 전송된 전력, 수신된 전력, 트랜시버 온도 및 전원 공급 디바이스 전압입니다. 트랜시버 모니터링을 지원하는 디바이스 목록은 아래를 참조하십시오.

- PA-800 시리즈
- PA-3200 시리즈
- PA-5200 시리즈
- PA-5450 방화벽
- PA-7000 시리즈

명령줄 인터페이스를 사용하여 트랜시버 모니터링을 실행합니다. 사용 가능한 모든 CLI 명령은 다음 표를 참조하십시오.



호환되지 않는 트랜시버에서 명령을 실행하는 경우 *CLI*는 읽을 수 없는 진단 정보에 대해 *'n/a'*를 반환합니다.

| CLI | 정의 |
|---|---|
| **show transceiver <interface name>** | 각 진단에 대한 값과 함께 지정된 트랜시버의 요약을 봅니다.<br>예:<br>**admin@PA-7080> show transceiver ethernet11/25**<br>CLI는 온도, 전압, 전류, Tx 전원 및 Rx 전원에 대한 값을 반환합니다. |
| **show transceiver <interface name>** | 공급업체 정보 및 링크 길이를 포함하여 더 자세한 트랜시버 사양을 받습니다. CLI는 더 자세한 진단 정보도 제공합니다. |
| **show transceiver all** | 모든 활성 트랜시버 목록과 각 진단에 대한 요약을 봅니다. |
| **show transceiver-detail all** | 디바이스의 각 트랜시버에 대한 포괄적인 세부 정보를 얻으십시오. |


©2023 Palo Alto Networks, Inc.

# User-ID

IP 주소와 달리 사용자 ID는 효과적인 보안 인프라의 필수 구성 요소입니다. 누가 네트워크에서 각 애플리케이션을 사용하고 있고 누가 위협을 가했거나 파일을 전송하고 있는지 알면 보안 정책을 강화하고 사고 대응 시간을 줄일 수 있습니다. Palo Alto Networks 방화벽의 표준 기능인 User-ID™를 사용하면 다양한 저장소에 저장된 사용자 정보를 활용할 수 있습니다. 다음 주제에서는 User-ID 및 구성 방법에 대한 자세한 내용을 제공합니다.


- 사용자 ID 개요
- 사용자 ID 개념
- 사용자 ID 사용
- 사용자를 그룹으로 매핑합니다.
- 사용자에게 IP 주소 매핑
- 사용자 및 그룹 기반 정책 활성화
- 계정이 여러 개인 사용자를 위한 정책 사용
- 사용자 ID 구성 확인
- 대규모 네트워크에 사용자 ID 배포

# 사용자 ID 개요

User-ID™를 사용하면 다양한 기술을 사용하여 네트워크의 모든 사용자를 식별할 수 있으므로 Microsoft Windows, Apple iOS, Mac OS, Android 및 Linux® /UNIX를 비롯한 다양한 액세스 방법과 운영 체제를 사용하여 모든 위치에서 사용자를 식별할 수 있습니다. IP 주소 대신 사용자가 누구인지 알면 다음을 수행할 수 있습니다.

- 가시성 - 사용자를 기반으로 애플리케이션 사용량을 파악하는 기능이 향상되어 네트워크 활동에 대한 보다 관련성 있는 그림을 얻을 수 있습니다. User-ID의 역할은 네트워크에서 이상하거나 익숙하지 않은 애플리케이션을 발견할 때 분명해집니다. 보안 팀은 ACC 또는 로그 뷰어를 사용하여 애플리케이션의 정의, 사용자, 대역폭 및 세션 사용량, 애플리케이션 트래픽의 소스 및 대상 및 관련 위협을 식별할 수 있습니다.
- 정책 제어 - 사용자 정보를 보안 정책 규칙에 연결하면 네트워크를 통과하는 애플리케이션을 안전하게 활성화하고 애플리케이션에 대한 비즈니스 요구 사항이 있는 사용자만 액세스할 수 있습니다. 예를 들어 인사 서비스(예: Workday 또는 Service Now)에 액세스할 수 있는 SaaS 애플리케이션과 같은 일부 애플리케이션은 네트워크의 알려진 모든 사용자가 사용할 수 있어야 합니다. 그러나 보다 민감한 애플리케이션의 경우 이러한 애플리케이션이 필요한 사용자만 액세스할 수 있도록 하여 공격 영역을 줄일 수 있습니다. 예를 들어 IT 지원 담당자가 합법적으로 원격 데스크톱 애플리케이션에 액세스해야 할 수도 있지만 대부분의 사용자는 그렇지 않습니다.
- 로깅, 보고, 포렌식 - 보안 사고가 발생하는 경우 IP 주소가 아닌 사용자 정보를 기반으로 포렌식 분석 및 보고를 통해 사고를 보다 완벽하게 파악할 수 있습니다. 예를 들어 사전 정의된 사용자/그룹 활동을 사용하여 개별 사용자 또는 사용자 그룹의 웹 활동 요약을 보거나 SaaS 애플리케이션 사용 보고서를 사용하여 승인되지 않은 SaaS 애플리케이션을 통해 가장 많은 데이터를 전송하는 사용자를 확인할 수 있습니다.

사용자 및 그룹 기반 정책을 적용하려면 방화벽이 수신하는 패킷의 IP 주소를 사용자명에 매핑할 수 있어야 합니다. User-ID는 이 사용자 매핑 정보를 수집하는 많은 메커니즘을 제공합니다. 예를 들어 User-ID 에이전트는 로그인 이벤트에 대한 서버 로그를 모니터링하고 인증 서비스에서 syslog 메시지를 수신합니다. 에이전트가 매핑하지 않은 IP 주소에 대한 매핑을 식별하려면 HTTP 요청을 인증 포털 로그인으로 리디렉션하도록 인증 정책을(를) 구성할 수 있습니다. 사용자 환경에 맞게 사용자 매핑 메커니즘을 조정할 수 있으며, 여러 사이트에서 서로 다른 메커니즘을 사용하여 항상 모든 위치에서 모든 사용자가 애플리케이션에 안전하게 액세스할 수 있도록 할 수 있습니다.


©2023 Palo Alto Networks, Inc.

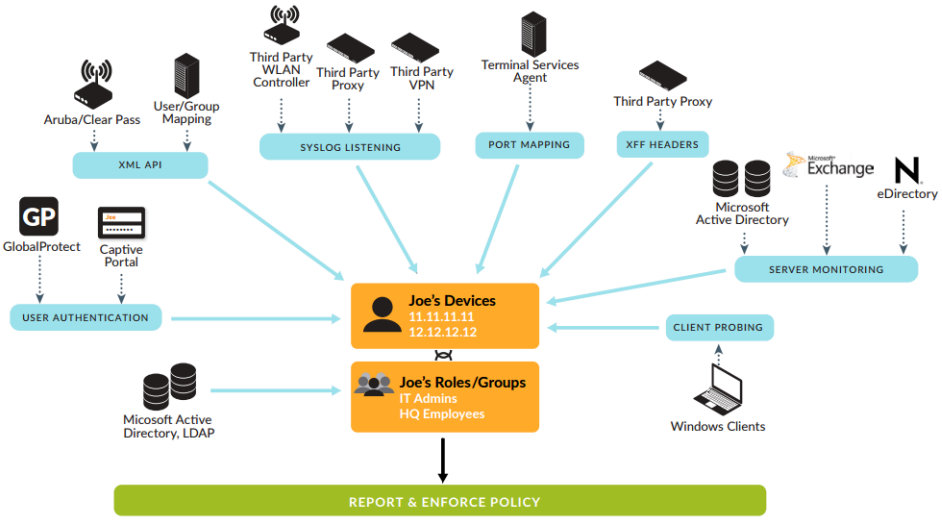



그림 **4: User-ID**

사용자 및 그룹 기반 정책을 적용하려면 정책 규칙을 정의할 때 그룹을 선택할 수 있도록 방화벽에 사용 가능한 모든 사용자 및 해당 그룹의 구성원 자격 목록이 필요합니다. 방화벽은 LDAP 디렉토리 서버에 직접 연결하거나 디렉토리 서버와의 XML API 통합을 사용하여 그룹 매핑 정보를 수집합니다.

User-ID 작동 방식에 대한 정보는 사용자 ID 개념, User-ID 설정에 대한 지침은 사용자 ID 사용을(를) 참조하십시오.

방화벽이 ***IP*** 주소를 사용자명에 매핑하기 전에 사용자의 소스 ***IP*** 주소가 ***NAT*** 변환이 적용되는 환경에서는 ***User-ID***가 작동하지 않습니다.


©2023 Palo Alto Networks, Inc.

# 사용자 ID 개념


- 그룹 매핑
- 사용자 매핑


## 그룹 매핑

먼저 사용자 또는 그룹을 기반으로 정책 규칙을 정의하려면 방화벽이 디렉터리 서버에 연결하고 인증하는 방법을 정의하는 LDAP 서버 프로파일을 생성합니다. 방화벽은 Microsoft Active Directory(AD), Novell eDirectory 및 Sun ONE 디렉터리 서버를 비롯한 다양한 디렉터리 서버를 지원합니다. 또한 서버 프로파일은 방화벽이 디렉터리를 검색하여 그룹 목록과 해당 멤버 목록을 검색하는 방법을 정의합니다. 방화벽에서 기본적으로 지원되지 않는 디렉터리 서버를 사용하는 경우 XML API를 사용하여 그룹 매핑 기능을 통합할 수 있습니다. 그런 다음 사용자를 그룹으로 매핑합니다. 및 사용자 및 그룹 기반 정책 활성화에 대한 그룹 매핑 구성을 만들 수 있습니다.

새 사용자가 그룹에 추가될 때마다 규칙을 업데이트할 필요가 없으므로 개별 사용자가 아닌 그룹 구성원 자격에 따라 정책 규칙을 정의하면 관리가 간소화됩니다. 그룹 매핑을 구성할 때 정책 규칙에서 사용할 수 있는 그룹을 제한할 수 있습니다. 디렉터리 서비스에 이미 있는 그룹을 지정하거나 LDAP 필터를 기반으로 사용자 지정 그룹을 정의할 수 있습니다. 사용자 지정 그룹을 정의하는 것은 LDAP 서버에서 새 그룹을 만들거나 기존 그룹을 변경하는 것보다 더 빠를 수 있으며 LDAP 관리자가 개입할 필요는 없습니다. 사용자 ID는 필터와 사용자 지정 그룹과 일치하는 모든 LDAP 디렉터리 사용자를 매핑합니다. 예를 들어 마케팅 부서의 계약자가 소셜 네트워킹 사이트에 액세스할 수 있는 보안 정책을 원할 수 있습니다. 해당 부서에 대해 Active Directory 그룹이 없는 경우 LDAP 특성 부서가 마케팅으로 설정된 사용자와 일치하는 LDAP 필터를 구성할 수 있습니다. 사용자 그룹을 기반으로 하는 로그 쿼리 및 보고서에는 사용자 지정 그룹이 포함됩니다.

## 사용자 매핑

사용자와 그룹 이름을 아는 것은 퍼즐의 한 조각에 불과합니다. 또한 방화벽은 보안 규칙을 적절하게 적용할 수 있도록 어떤 IP 주소가 어떤 사용자에게 매핑되는지 알아야 합니다. 사용자 ID 개요은(는) 네트워크에서 사용자와 그룹을 식별하는 데 사용되는 다양한 방법을 보여주고 사용자 매핑과 그룹 매핑이 함께 작동하여 사용자 및 그룹 기반 보안 적용 및 가시성을 활성화하는 방법을 보여줍니다. 다음 항목은 사용자 매핑의 다양한 방법을 설명합니다.


- 서버 모니터링
- 포트 매핑
- Syslog
- XFF 헤더
- 사용자 이름 헤더 삽입
- 인증 정책 및 인증 포털
- GlobalProtect
- XML API
- 클라이언트 프로빙


 ©2023 Palo Alto Networks, Inc.

### 서버 모니터링

사용자 ID 에이전트(네트워크의 도메인 서버에서 실행되는 Windows 기반 에이전트 또는 방화벽에서 실행되는 PAN-OS 통합 User-ID 에이전트)를 모니터링하는 서버를 통해 지정된 Microsoft Exchange Server, 로그인 이벤트를 위한 도메인 컨트롤러 또는 Novell eDirectory 서버에 대한 보안 이벤트 로그를 모니터링합니다. 예를 들어 AD 환경에서 Kerberos 티켓 부여 또는 갱신, Exchange 서버 액세스(구성된 경우) 및 파일 및 인쇄 서비스 연결에 대한 보안 로그를 모니터링하도록 User-ID 에이전트를 구성할 수 있습니다. 이러한 이벤트를 보안 로그에 기록하려면 성공적인 계정 로그인 이벤트를 기록하도록 AD 도메인을 구성해야 합니다. 또한 사용자가 도메인의 모든 서버에 로그인할 수 있으므로 모든 서버에 대한 서버 모니터링을 설정하여 모든 사용자 로그인 이벤트를 캡처해야 합니다. 자세한 내용은 Windows 사용자 ID 에이전트를 사용하여 사용자 매핑 구성 또는 PAN-OS 통합 사용자 ID 에이전트를 사용하여 사용자 매핑 구성을(를) 참조하십시오.

### 포트 매핑

Microsoft Terminal Server 또는 Citrix 환경과 같은 다중 사용자 시스템이 있는 환경에서는 많은 사용자가 동일한 IP 주소를 공유합니다. 이 경우 사용자-IP 주소 매핑 프로세스에는 각 클라이언트의 소스 포트에 대한 지식이 필요합니다. 이러한 유형의 매핑을 수행하려면 Windows/Citrix 터미널 서버 자체에 Palo Alto Networks 터미널 서버 에이전트를 설치하여 다양한 사용자 프로세스에 대한 소스 포트 할당을 중재해야 합니다. Linux 터미널 서버와 같이 터미널 서버 에이전트를 지원하지 않는 터미널 서버의 경우 XML API를 사용하여 로그인 및 로그아웃 이벤트에서 사용자 매핑 정보를 User-ID로 보낼 수 있습니다. 구성에 대한 자세한 내용은 터미널 서버 사용자를 위한 사용자 매핑 구성을(를) 참조하십시오.

## XFF 헤더

네트워크의 사용자와 방화벽 사이에 프록시 서버가 배포된 경우 방화벽은 콘텐츠를 요청한 클라이언트의 IP 주소가 아니라 프록시가 포워딩하는 HTTP/HTTPS 트래픽의 소스 IP 주소로 프록시 서버 IP 주소를 볼 수 있습니다. 대부분의 경우 프록시 서버는 콘텐츠를 요청했거나 요청이 시작된 클라이언트의 실제 IPv4 또는 IPv6 주소가 포함된 트래픽 패킷에 XFF(X-Forwarded-For) 헤더를 추가합니다. 이러한 경우 User-ID가 IP 주소를 사용자 이름에 매핑할 수 있도록 XFF에서 최종 사용자 IP 주소를 추출하도록 방화벽을 구성할 수 있습니다. 이를 통해 정책 및 로깅 소스 사용자에 대해 XFF 값을 사용할 수 있으므로 프록시 서버 뒤에 있는 사용자가 웹 기반에 안전하게 액세스할 수 있도록 사용자 기반 정책을 시행할 수 있습니다.

### 사용자 이름 헤더 삽입

사용자 기반 정책을 시행하기 위해 Palo Alto Networks 방화벽이 있는 보조 시행 디바이스를 구성할 때 보조 디바이스는 방화벽에서 IP 주소-사용자명 매핑을 갖지 않을 수 있습니다. User-ID를 다운스트림 디바이스로 전송하는 경우 프록시와 같은 추가 디바이스를 배포해야 하거나 사용자 경험에 부정적인 영향을 미칠 수 있습니다(예: 사용자가 여러 번 로그인해야 함). 사용자 발신 트래픽의 HTTP 헤더에 도메인과 사용자명을 동적으로 추가하여 Palo Alto Networks 방화벽과 함께 사용하는 모든 보조 디바이스가 사용자 정보를 수신하고 사용자 기반 정책을 시행하도록 할 수 있습니다. 트래픽 헤더에 사용자명과 도메인을 삽입하여 사용자의 ID를 포함하면 사용자 경험이나 추가 인프라 배포에 부정적인 영향을 주지 않으면서 사용자 기반 정책을 시행할 수 있습니다.

### 인증 정책 및 인증 포털

경우에 따라 사용자 ID 에이전트는 사용자가 로그인하지 않았거나 도메인 서버가 지원하지 않는 Linux와 같은 운영 체제를 사용하는 경우와 같이 서버 모니터링 또는 기타 방법을 사용하여 IP 주소를 사용자 이름에 매핑할 수 없습니다. 다른 경우에는 사용자 ID 에이전트가 사용자 매핑을 수행하는 데 사용하는 방법에 관계없이 중요한 애플리케이션에 액세스할 때 사용자가 인증하도록 할 수 있습니다. 이러한 모든 경우 인

 ©2023 Palo Alto Networks, Inc.

증 정책 구성을 구성하고 인증 포털을 사용하여 IP 주소를 사용자 이름으로 매핑할수 있습니다. 인증 정책 규칙과 일치하는 모든 웹 트래픽(HTTP 또는 HTTPS)은 사용자가 인증 포털을 통해 인증하라는 메시지를 표시합니다. 다음 인증 포털 인증 방법을 사용할 수 있습니다.

- 브라우저 챌린지- 사용자가 응답해야 하는 로그인 프롬프트 수를 줄이려면 Kerberos Single Sign-On(SSO) 사용.
- 웹 양식 - 다단계, 인증, SAML Single Sign-On(SSO), Kerberos,, TACACS+, RADIUS,, LDAP, 또는 로컬 인증을 사용합니다.
- 클라이언트 인증서 인증.

## Syslog

환경에 사용자를 인증하는 기존 네트워크 서비스가 있을 수 있습니다. 이러한 서비스에는 무선 컨트롤러, 802.1x 디바이스, Apple Open Directory 서버, 프록시 서버 및 기타 NAC(네트워크 액세스 제어) 메커니즘이 포함됩니다. 로그인 및 로그아웃 이벤트에 대한 정보가 포함된 syslog 메시지를 보내도록 이러한 서비스를 구성하고 해당 메시지를 구문 분석하도록 User-ID 에이전트를 구성할 수 있습니다. User-ID 에이전트는 로그인 이벤트를 구문 분석하여 IP 주소를 사용자명에 매핑하고 로그아웃 이벤트를 구문 분석하여 오래된 매핑을 삭제합니다. 오래된 매핑을 삭제하는 것은 IP 주소 할당이 자주 변경되는 환경에서 특히 유용합니다.

PAN-OS 통합 User-ID 에이전트와 Windows 기반 User-ID 에이전트는 모두 Syslog 구문 분석 프로파일을 사용하여 syslog 메시지를 구문 분석합니다. 서비스가 다른 형식으로 메시지를 보내는 환경에서 각 형식에 대한 사용자 지정 프로파일을 생성하고 여러 프로파일을 각 syslog 발신자과 연결할 수 있습니다. PAN-OS 통합 User-ID 에이전트를 사용하는 경우 Palo Alto Networks가 애플리케이션 콘텐츠 업데이트를 통해 제공하는 사전 정의된 Syslog Parse 프로파일을 사용할 수도 있습니다.

Syslog 메시지는 User-ID 에이전트가 메시지를 구문 분석하려면 다음 기준을 충족해야 합니다.

- 각 메시지는 한 줄의 텍스트 문자열이어야 합니다. 줄 바꿈에 허용되는 구분 기호는 새 줄(**\n**) 또는 캐리지 리턴과 새 줄(**\r\n**)입니다.
- 개별 메시지의 최대 크기는 8,000바이트입니다.
- UDP를 통해 전송된 메시지는 단일 패킷에 포함되어야 합니다. SSL을 통해 전송된 메시지는 여러 패킷에 걸쳐 있을 수 있습니다. 단일 패킷에는 여러 메시지가 포함될 수 있습니다.

구성에 대한 자세한 내용은 사용자 매핑을 위해 Syslog 발신자를 모니터링하도록 사용자 ID 구성을(를) 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

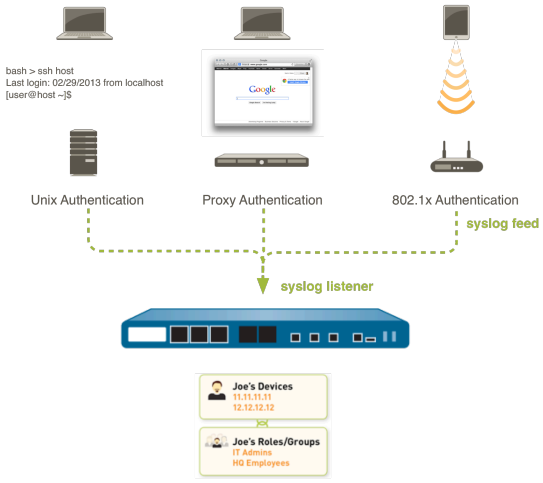



그림 **5: Syslog**와 사용자 **ID** 통합

## GlobalProtect

모바일 또는 로밍 사용자의 경우 GlobalProtect 엔드포인트는 사용자 매핑 정보를 방화벽에 직접 제공합니다. 이 경우 모든 GlobalProtect 사용자는 방화벽에 대한 VPN 액세스를 위해 로그인 자격 증명을 입력해야 하는 엔드포인트에서 실행되는 앱을 보유합니다. 그런 다음 가시성 및 사용자 기반 보안 정책 적용을 위해 이 로그인 정보가 방화벽의 User-ID 사용자 매핑 테이블에 추가됩니다. GlobalProtect 사용자는 네트워크에 대한 액세스 권한을 얻기 위해 인증을 받아야 하므로 IP 주소와 사용자 이름 간의 매핑을 명시적으로 알 수 있습니다. 이는 애플리케이션이나 서비스에 대한 액세스를 허용하기 위해 사용자가 누구인지 확인해야 하는 민감한 환경에서 최상의 솔루션입니다. GlobalProtect 설정에 대한 자세한 내용은 GlobalProtect 관리자 안내서를 참조하십시오.

## XML API

인증 포털 및 기타 표준 사용자 매핑 방법은 특정 유형의 사용자 액세스에 대해 작동하지 않을 수 있습니다. 예를 들어, 표준 방법은 타사 VPN 솔루션에서 연결하는 사용자 또는 802.1x 지원 무선 네트워크에 연결하는 사용자의 매핑을 추가할 수 없습니다. 이러한 경우 PAN-OS XML API를 사용하여 로그인 이벤트를 캡처하고 PAN-OS 통합 User-ID 에이전트로 보낼 수 있습니다. 자세한 내용은 XML API를 사용하여 사용자 매핑을 사용자 ID로 보내기을(를) 참조하십시오.

### 클라이언트 프로빙

***Palo Alto Networks***는 높은 수준의 보안 네트워크에서 사용자 ***ID*** 정보를 얻는 데 권장되는 방법이 아니기 때문에 클라이언트 검색을 비활성화할 것을 강력히 권장합니다.

Palo Alto Networks는 다음과 같은 잠재적 위험 때문에 클라이언트 프로빙 사용을 권장하지 않습니다.

- 클라이언트 검색은 엔드포인트에서 다시 보고된 데이터를 신뢰하기 때문에 잘못 구성되면 보안 위험에 노출될 수 있습니다. 신뢰할 수 없는 외부 인터페이스에서 활성화하면 에이전트가 사용자 이름, 도메인 이름, 사용자 ID 에이전트 서비스 계정의 암호 해시와 같은 민감한 정보가 포함된 클라이언트 프로브를 네트워크 외부로 보냅니다. 서비스 계정을 올바르게 구성하지 않으면 공격자가 자격 증명을 악용하여 네트워크에 침투하여 추가 액세스 권한을 얻을 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

- 클라이언트 프로빙은 대부분의 사용자가 내부 네트워크의 Windows 워크스테이션에 있는 레거시 네트워크용으로 설계되었지만 다양한 디바이스 및 운영 체제에서 로밍 및 모바일 사용자 기반을 지원하는 오늘날의 보다 현대적인 네트워크에는 적합하지 않습니다.
- 클라이언트 검색은 많은 양의 네트워크 트래픽을 생성할 수 있습니다(매핑된 IP 주소의 총 수를 기준으로 함).

대신 Palo Alto Networks는 사용자 매핑을 위해 다음과 같은 대체 방법을 사용할 것을 강력히 권장합니다.

- 도메인 컨트롤러 및 Syslog 또는 XML API와의 통합과 같이 더 격리되고 신뢰할 수 있는 소스를 사용하여 모든 디바이스 유형 또는 운영 체제에서 사용자 매핑 정보를 안전하게 캡처합니다.
- 인증된 사용자에게만 액세스를 허용하도록 인증 정책 및 인증 포털을 구성합니다.

User-ID 에이전트는 두 가지 유형의 클라이언트 조사를 지원합니다.

- Windows 사용자 ID 에이전트를 사용하는 NetBIOS 검색.
- PAN-OS 통합 사용자 ID 에이전트 또는 Windows 사용자 ID 에이전트를 사용하는 WMI 검색.

> 클라이언트 프로빙은 사용자 매핑 방법으로 권장되지 않지만 활성화하려는 경우 ***Palo Alto Networks***는 ***NetBIOS*** 프로빙보다 ***WMI*** 프로빙을 사용할 것을 강력히 권장합니다.

Microsoft Windows 환경에서 기존 사용자 매핑이 여전히 유효한지 확인하거나 아직 매핑되지 않은 IP 주소에 대한 사용자 이름을 얻기 위해 정기적으로 WMI(Windows Management Instrumentation) 또는 NetBIOS 검색을 사용하여 클라이언트 시스템을 검색하도록 User-ID 에이전트를 구성할 수 있습니다.

신뢰할 수 있는 영역에서 검색을 활성화하도록 선택하면 에이전트는 각 학습된 IP 주소를 주기적으로(기본적으로 20분 주기이지만 변경 가능) 검색하여 동일한 사용자가 여전히 로그인되어 있는지 확인합니다. 또한 방화벽은 사용자 매핑이 없는 IP 주소를 발견하면 즉각적인 조사를 위해 해당 주소를 에이전트에 보냅니다.

자세한 내용은 Windows 사용자 ID 에이전트를 사용하여 사용자 매핑 구성 또는 PAN-OS 통합 사용자 ID 에이전트를 사용하여 사용자 매핑 구성을 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 사용자 ID 사용

IP 주소와 달리 사용자 ID는 효과적인 보안 인프라의 필수 구성 요소입니다. 누가 네트워크에서 각 애플리케이션을 사용하고 있고 누가 위협을 전송했거나 파일을 전송하고 있는지 알면 보안 정책을 강화하고 사고 대응 시간을 줄일 수 있습니다. User-ID를 사용하면 가시성, 사용자 및 그룹 기반 정책 제어, 향상된 로깅, 보고 및 포렌식을 위해 다양한 리포지토리에 저장된 사용자 정보를 활용할 수 있습니다.

**STEP 1 |** 사용자 기반 액세스 제어가 필요한 요청을 보낼 사용자가 포함된 소스 영역에서 User-ID를 활성화합니다.

신뢰할 수 있는 영역에서만 ***User-ID***를 활성화합니다**.** 외부의 신뢰할 수 없는 영역**(**예**:** 인터넷**)**에서 사용자 ***ID*** 및 클라이언트 검색을 활성화하면 프로브가 보호된 네트워크 외부로 전송되어 사용자 ***ID*** 에이전트 서비스 계정 이름**,** 도메인 이름 정보 및 공격자가 보호된 서비스 및 애플리케이션에 대한 무단 액세스를 얻을 수 있는 암호화된 암호 해시가 공개될 수 있습니다**.**

1. 네트워크 > 영역을 선택한 다음 영역 이름을 클릭합니다.
2. 사용자 식별을 활성화하고 확인을 클릭합니다.

**STEP 2 |** User-ID 에이전트에 대한 전용 서비스 계정을 생성합니다.

가장 좋은 방법은 서비스 계정이 손상된 경우 공격 노출 영역을 줄이기 위해 활성화하는 사용자 ***ID*** 옵션을 지원하는 데 필요한 최소한의 권한 집합으로 서비스 계정을 만드는 것입니다**.**

Windows 기반 User-ID 에이전트 또는 PAN-OS 통합 User-ID 에이전트를 사용하여 사용자 로그인 및 로그아웃 이벤트에 대해 도메인 컨트롤러, Microsoft Exchange 서버 또는 Windows 클라이언트를 모니터링하려는 경우에 필요합니다.

**STEP 3 |** 사용자를 그룹으로 매핑합니다.

이렇게 하면 방화벽이 LDAP 디렉터리에 연결하고 그룹 매핑 정보를 검색할 수 있으므로 정책을 만들 때 사용자 이름과 그룹 이름을 선택할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 사용자에게 IP 주소를 매핑합니다.



가장 좋은 방법은 보안 수준이 높은 네트워크에서 사용자 매핑 방법으로 클라이언트 검색을 활성화하지 않는 것입니다. 클라이언트 프로빙은 많은 양의 네트워크 트래픽을 생성할 수 있으며 잘못 구성되면 보안에 위협이 될 수 있습니다.

이 작업을 수행하는 방법은 사용자가 있는 위치와 사용 중인 시스템 유형, 네트워크에서 사용자에 대한 로그인 및 로그아웃 이벤트를 수집하는 시스템에 따라 다릅니다. 사용자 매핑을 활성화하려면 하나 이상의 User-ID 에이전트를 구성해야 합니다.

- Windows User-ID 에이전트를 사용하여 사용자 매핑을 구성합니다.
- PAN-OS 통합 User-ID 에이전트를 사용하여 사용자 매핑을 구성합니다.
- 사용자 매핑을 위해 Syslog 발신자를 모니터링하도록 사용자 ID를 구성합니다.
- 터미널 서버 사용자에 대한 사용자 매핑을 구성합니다.
- XML API를 사용하여 사용자 ID에 사용자 매핑을 보냅니다.
- HTTP 헤더에 사용자 이름 삽입.

**STEP 5 |** 사용자 매핑에서 포함 및 제외할 네트워크를 지정합니다.



가장 좋은 방법은 항상 ***User-ID***에 포함하거나 제외할 네트워크를 지정하는 것입니다. 이를 통해 신뢰할 수 있는 자산만 조사하고 원치 않는 사용자 매핑이 예기치 않게 생성되지 않도록 할 수 있습니다.

포함하고 제외할 네트워크를 지정하는 방법은 Windows 기반 User-ID 에이전트를 사용하는지 PAN-OSintegrated User-ID 에이전트를 사용하는지에 따라 다릅니다.

**STEP 6 |** 인증 정책 및 인증 포털을 구성합니다.

방화벽은 인증 정책 규칙과 일치하는 서비스, 애플리케이션 또는 URL 카테고리를 요청할 때 최종 사용자를 인증하기 위해 인증 포털을 사용합니다. 방화벽은 인증 중에 수집된 사용자 정보를 기반으로 새 사용자 매핑을 생성하거나 기존 매핑을 업데이트합니다. 인증 중에 수집된 매핑 정보는 다른 사용자 ID 방법을 통해 수집된 정보보다 우선합니다.

1. 인증 포털을 구성합니다.
2. 인증 정책을 구성합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 사용자 및 그룹 기반 정책 시행을 활성화합니다.



가능하면 사용자가 아닌 그룹을 기반으로 규칙을 생성합니다. 이렇게 하면 사용자 기반이 변경될 때마다 규칙(커밋이 필요함)을 지속적으로 업데이트할 필요가 없습니다.

사용자 ID를 구성한 후 보안 규칙의 소스 또는 대상을 정의할 때 사용자 이름 또는 그룹 이름을 선택할 수 있습니다.

1. 정책 > 보안 및 새 규칙 추가를 선택하거나 기존 규칙 이름을 클릭하여 편집합니다.
2. 사용자를 선택한 후 다음 방법 중 하나로 규칙에서 일치시킬 사용자 및 그룹을 지정합니다.
   - 특정 사용자 또는 그룹을 일치 기준으로 선택하려면 소스 사용자 섹션에서 추가를 클릭하여 방화벽 그룹 매핑 기능으로 검색된 사용자 및 그룹 목록을 표시합니다. 규칙에 추가할 사용자 또는 그룹을 선택합니다.
   - 인증되었거나 인증되지 않은 사용자를 일치시키고 특정 사용자 또는 그룹 이름을 알 필요가 없는 경우 원본 사용자 목록 위의 드롭다운에서 알려진 사용자 또는 알 수 없음을 선택합니다.
3. 나머지 규칙을 적절하게 구성한 다음 확인을 클릭하여 저장합니다. 보안 규칙의 다른 필드에 대한 자세한 내용은 기본 보안 정책 설정을 참조하십시오.

**STEP 8 |** 보안 정책 규칙을 만들어 신뢰할 수 있는 영역 내에서 사용자 ID를 안전하게 활성화하고 사용자 ID 트래픽이 네트워크에서 나가는 것을 방지합니다.

모범 사례 인터넷 게이트웨이 보안 정책에 따라 사용자 ID 애플리케이션(`paloalto-userid-agent`)이 에이전트(Windows 에이전트와 PAN-OS 통합 에이전트 모두)가 서비스를 모니터링하고 방화벽에 매핑을 배포하는 영역에서만 허용되도록 합니다. 상세 내용:

- 에이전트가 있는 영역과 모니터링되는 서버가 있는 영역(또는 에이전트를 호스팅하는 특정 시스템과 모니터링되는 서버 사이) 간에 `paloalto-userid-agent` 애플리케이션을 허용합니다.
- 에이전트와 사용자 매핑이 필요한 방화벽 사이, 사용자 매핑을 재배포하는 방화벽과 정보를 재배포하는 방화벽 간에 `paloalto-userid-agent` 애플리케이션을 허용합니다.
- 인터넷 영역과 같은 외부 영역에 대한 `paloalto-userid-agent` 애플리케이션을 거부합니다.

**STEP 9 |** XFF(X-Forwarded-For) 헤더에서 사용자 IP 주소를 가져오도록 방화벽을 구성합니다.

방화벽이 인터넷과 프록시 서버 사이에 있을 때 방화벽이 보는 패킷의 IP 주소는 사용자가 아닌 프록시 서버에 대한 것입니다. 대신 사용자 IP 주소의 가시성을 활성화하려면 사용자 매핑에 XFF 헤더를 사용하도록 방화벽을 구성하십시오. 이 옵션이 활성화되면 방화벽은 연결된 사용자 및 그룹에 대한 제어 및 가시성을 활성화하기 위해 정책에서 참조된 사용자 이름과 IP 주소를 일치시킵니다. 자세한 내용은 프록시 서버를 통해 연결된 사용자 식별을 참조하십시오.

1. 디바이스 > 설정 > 콘텐츠 **ID**를 선택하고 X-Forwarded-For Headers 설정을 수정합니다.
2. **User-ID**에서 **X-Forwarded-For Header**를 선택합니다.

   ***Strip-X-Forwarded-For Header***를 선택해도 정책 규칙의 사용자 속성에 ***XFF*** 헤더 사용이 비활성화되지 않습니다. 방화벽은 사용자 속성에 사용한 후에만 ***XFF*** 값을 ***0***으로 생성합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 10 |** HA(고가용성) 구성을 사용하는 경우 동기화를 사용하도록 설정합니다.

가장 좋은 방법은 활성 방화벽과 수동형 방화벽 간에 그룹 매핑과 사용자 매핑이 동기화되도록 ***HA*** 구성에 대해 항상 구성 동기화 활성화 옵션을 활성화하는 것입니다.

1. 디바이스 > 고가용성 > 일반을 선택한 다음 설치 섹션을 편집합니다.
2. **HA** 활성화를 선택합니다.
3. 구성 동기화 활성화를 선택합니다.
4. 피어 방화벽에 있는 HA1 제어 링크의 IP 주소인 피어 **HA1 IP** 주소를 입력합니다.
5. (선택 사항) 피어 방화벽의 백업 제어 링크의 IP 주소인 백업 피어 **HA1 IP** 주소를 입력합니다.
6. 확인을 클릭합니다.

**STEP 11 |** 변경 사항을 커밋합니다.

변경 사항을 커밋하여 활성화합니다.

**STEP 12 |** 사용자 ID 구성을 확인합니다.

사용자 매핑 및 그룹 매핑을 구성한 후 구성이 제대로 작동하는지 확인하고 애플리케이션 및 서비스에 대한 사용자 및 그룹 액세스를 안전하게 활성화하고 모니터링할 수 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

# 사용자를 그룹으로 매핑합니다.

개별 사용자가 아닌 사용자 그룹 구성원을 기반으로 정책 규칙을 정의하면 그룹 구성원이 변경될 때마다 규칙을 업데이트할 필요가 없으므로 관리가 간소화됩니다. 각 방화벽 또는 Panorama가 모든 정책에서 참조할 수 있는 고유한 사용자 그룹의 수는 모델에 따라 다릅니다. 자세한 내용은 호환성 매트릭스를 참조하십시오.

다음 절차에 따라 방화벽을 활성화하여 LDAP 디렉토리에 연결하고 그룹 매핑 정보를 검색할 수 있습니다. 그런 다음 사용자 및 그룹 기반 정책을 사용하도록 설정할 수 있습니다.



다음은 *AD(Active Directory)* 환경에서 그룹 매핑을 위한 모범 사례입니다.

- 도메인이 하나인 경우 *LDAP* 서버 프로파일이 있는 그룹 매핑 구성이 하나만 있으면 최상의 연결을 제공하는 도메인 컨트롤러에 방화벽을 연결할 수 있습니다. 중복성을 위해 *LDAP* 서버 프로파일에 도메인 컨트롤러를 최대 *4*개까지 추가할 수 있습니다. 해당 도메인에 대해 여러 그룹 매핑 구성을 추가하여 단일 도메인에 대해 도메인 컨트롤러 *4*개 이상으로 중복성을 늘릴 수는 없습니다.
- 여러 도메인 및/또는 여러 포리스트가 있는 경우 방화벽을 각 도메인/포리스트의 도메인 서버에 연결하는 *LDAP* 서버 프로파일을 사용하여 그룹 매핑 구성을 만들어야 합니다. 별도의 포리스트에 고유한 사용자 이름을 확인하는 단계를 수행합니다.
- 유니버설 그룹이 있는 경우 *LDAP* 서버 프로파일을 만들어 포트 *3268* 또는 *SSL*용 *3269*에서 글로벌 카탈로그 서버의 루트 도메인에 연결한 다음 다른 *LDAP* 서버 프로파일을 만들어 포트 *389*의 루트 도메인 컨트롤러에 연결합니다. 이렇게 하면 모든 도메인 및 하위 도메인에서 사용자 및 그룹 정보를 사용할 수 있습니다.
- 이 속성은 정책 구성, 로그 및 보고서에서 사용자를 식별하기 때문에, 그룹 매핑을 사용하기 전에 사용자 기반 보안 정책에 대한 기본 사용자 이름을 구성합니다.

**STEP 1 |** LDAP 서버 프로파일을 추가합니다.

프로파일은 방화벽이 그룹 매핑 정보를 수집하는 디렉터리 서버에 연결하는 방법을 정의합니다.



동일한 기본 *DN(*고유 이름*)* 또는 *LDAP* 서버를 사용하는 여러 그룹 매핑 구성을 만드는 경우 그룹 매핑 구성에 겹치는 그룹*(*예를 들어, 하나의 그룹 매핑 구성에 대한 포함 목록에는 다른 그룹 매핑 구성에도 있는 그룹이 포함될 수 없음*)*이 포함될 수 없습니다.

1. 디바이스 > 서버 프로파일 > **LDAP**를 선택하고 서버 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.

 ©2023 Palo Alto Networks, Inc.

3. LDAP 서버를 추가합니다. 프로파일에 서버를 최대 4개까지 추가할 수 있지만 유형이 같아야 합니다. 각 서버에 대해 이름(서버 식별), **LDAP** 서버 IP 주소 또는 FQDN 및 서버 포트(기본값 389)를 입력합니다.
4. 서버 유형을 선택합니다.

   선택한 항목(예: **active-directory**)에 따라 방화벽이 그룹 매핑 설정에서 올바른 LDAP 속성을 자동으로 채웁니다. 그러나 LDAP 스키마를 사용자 정의한 경우에는 기본 설정을 수정해야 할 수 있습니다.
5. 기본 **DN**의 경우 방화벽에서 사용자 및 그룹 정보 검색을 시작할 LDAP 트리 위치의 DN(식별 이름)을 입력합니다.
6. 바인드 **DN**, 암호 및 암호 확인에 LDAP 트리에 바인딩하기 위한 인증 자격 증명을 입력합니다.

   바인딩 **DN**은 정규화된 LDAP 이름(예: `cn=관리자, cn=사용자, dc=acme, dc=로컬`) 또는 사용자 계정 이름(예: `administrator@acme.local`)일 수 있습니다.
7. 바인딩 타임아웃 및 검색 타임아웃(초)을 입력합니다. 기본값은 모두 30입니다.
8. 확인을 클릭하여 서버 프로파일을 저장합니다.

**STEP 2 |** 그룹 매핑 구성에서 서버 설정을 구성합니다.

1. 디바이스 > 사용자 식별 > 그룹 매핑 설정을 선택합니다.
2. 그룹 매핑 구성을 추가합니다.
3. 고유 이름을 입력하여 그룹 매핑 구성을 식별합니다.
4. 방금 만든 LDAP 서버 프로파일을 선택합니다.
5. (선택 사항) 업데이트 간격(초)을 지정합니다. 그룹 매핑 구성에 대한 업데이트가 있는지 LDAP 원본을 확인하는 빈도에 따라 값(범위는 60 - 86400, 기본값은 3600)을 입력합니다. LDAP 소스에 여러 그룹이 포함되어 있는 경우 너무 낮은 값은 모든 그룹을 매핑하는 데 충분한 시간을 허용하지 않을 수 있습니다.
6. (선택 사항) 기본적으로 사용자 도메인 필드는 비어 있습니다. 방화벽이 AD(Active Directory) 서버의 도메인 이름을 자동으로 검색합니다. 값을 입력하면 방화벽이 LDAP 소스에서 검색하는 모든 도메인 이름을 무시합니다. 대부분의 구성에서 값을 입력해야 하는 경우 NetBIOS 도메인 이름을 입력합니다(예: **`example.com`**이 아닌 **`example`**).

   Global Catalog를 사용하는 경우 값을 입력하면 다른 도메인의 사용자 및 그룹을 포함하여 이 서버의 모든 사용자 및 그룹의 도메인 이름이 바뀝니다.
7. (선택 사항) 그룹 매핑을 위해 방화벽이 추적하는 그룹을 필터링하려면 그룹 개체 섹션에 검색 필터(LDAP 쿼리) 및 개체 클래스를 입력합니다. (그룹 정의).
8. (선택 사항) 그룹 매핑을 위해 방화벽이 추적하는 사용자를 필터링하려면 사용자 개체 섹션에 검색 필터(LDAP 쿼리) 및 개체 클래스를 입력합니다.(사용자 정의).
9. 그룹 매핑 구성이 사용(기본값 사용)인지 확인합니다.

**STEP 3 |** (선택 사항) 사용자 및 그룹 매핑을 위해 수집할 사용자 및 그룹 특성을 정의합니다. 이 단계는 도메인 이외의 디렉터리 속성을 기반으로 사용자를 매핑하려는 경우에 필요합니다.

1. User-ID 소스에서 사용자 이름만 전송하고 사용자 이름이 조직 전체에서 고유한 경우 디바이스 > 사용자 식별 > 사용자 매핑 > 설정을 선택한 다음 설정 섹션을 편집하여 그룹 매핑 중에 LDAP 서버에서 수집된 고유한 사용자 이름이 정책과 연결된 사용자와 일치하는지 방화벽이 확인하고

 ©2023 Palo Alto Networks, Inc.

원본 프로파일의 도메인을 덮어쓰지 않도록 하려면 도메인 없이 일치하는 사용자 이름을 허용합니다.

이 옵션을 사용하도록 설정하기 전에 매핑을 수집하는 사용자 *ID* 소스(예: GlobalProtect 또는 인증 포털)를 포함하는 *LDAP* 그룹에 대한 그룹 매핑을 구성합니다. 변경 사항을 커밋하면 *User-ID* 소스가 도메인 없이 사용자 이름을 채웁니다. 그룹 매핑 중에 수집된 사용자 이름만 도메인 없이 일치시킬 수 있습니다. *User-ID* 소스에서 사용자 정보를 여러 형식으로 보내고 이 옵션을 사용하도록 설정하는 경우 방화벽에서 수집한 속성에 고유한 프리픽스가 있는지 확인합니다. 이 옵션을 활성화한 경우 사용자를 올바르게 식별하려면 그룹 매핑의 모든 속성이 고유해야 합니다. 사용자 이름이 고유하지 않으면 방화벽이 디버그 로그에 오류를 기록합니다.

2. 디바이스 > 사용자 식별 > 그룹 매핑 설정 > 추가 > 사용자 및 그룹 속성 > 을 선택합니다. 사용자 속성을 선택한 다음 사용자 식별을 위해 수집하려는 디렉토리 속성을 입력합니다. 방화벽에서 사용자를 식별하고 방화벽이 User-ID 원본에서 받는 다른 형식을 재정의하는 보고서 및 로그에서 사용자를 나타내는 기본 사용자 이름을 지정합니다.

   서버 프로파일 유형을 선택하면 방화벽이 사용자 및 그룹 특성에 대한 값을 자동으로 채웁니다. User-ID 소스가 전송하는 사용자 정보에 따라 올바른 속성을 구성해야 할 수 있습니다.

   - 사용자 계정 이름**(UPN)**: **`userPrincipalName`**
   - **NetBios** 이름: **`sAMAccountName`**
   - 이메일 **ID**: 해당 이메일의 디렉토리 속성
   - 여러 형식: User-ID 소스를 사용 설정하기 전에 사용자 디렉터리에서 사용자 매핑 속성을 검색합니다.

   기본 사용자 이름을 지정하지 않으면 방화벽은 각 서버 프로파일 유형에 대해 다음 기본값을 사용합니다.

| 속성 | Active Directory | Novell eDirectory 또는 Sun ONE Directory Server |
|---|---|---|
| Primary Username | `sAMAccountName` | `uid` |
| E-Mail | `mail` | `mail` |
| Alternate Username 1 | `userPrincipalName` | None. |
| 그룹 이름 | `이름` | `cn` |
| 그룹 멤버 | `멤버` | `멤버` |

3. (선택 사항) 이메일 주소 형식과 최대 세 가지 대체 사용자 이름 형식을 지정합니다.
4. 디바이스 > 사용자 식별 > 그룹 매핑 설정 > 추가 > 사용자 및 그룹 속성 > 그룹 속성을 선택하고 및 그룹 이름, 그룹 구성원 및 이메일 주소 형식을 지정합니다.

   방화벽이 LDAP 서버에서 디렉터리 특성을 수집하기 전에 커밋해야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 정책 규칙에서 사용할 수 있는 그룹을 제한합니다.

정책 규칙을 특정 그룹으로 제한하려는 경우에만 필요합니다. 그룹 포함 목록과 사용자 지정 그룹 목록의 합산 최대값은 그룹 매핑 구성당 640개 항목입니다. 각 항목은 단일 그룹 또는 그룹 목록일 수 있습니다. 기본적으로 그룹을 지정하지 않으면 정책 규칙에서 모든 그룹을 사용할 수 있습니다.

사용자가 만든 모든 사용자 지정 그룹은 인증 프로파일의 허용 목록(인증 프로파일 및 시퀀스 구성)에서도 사용할 수 있습니다.

1. 디렉터리 서비스에서 기존 그룹을 추가합니다.
   1. 그룹 포함 목록을 선택합니다.
   2. 정책 규칙에 표시할 사용 가능한 그룹을 선택한 다음 포함된 그룹에 추가(⊕)합니다.
2. 기존 사용자 그룹과 일치하지 않는 사용자 특성을 기반으로 정책 규칙을 적용하려면 LDAP 필터를 기반으로 사용자 지정 그룹을 생성합니다.
   1. 사용자 지정 그룹을 선택한 다음 그룹 추가를 선택합니다.
   2. 현재 방화벽 또는 가상 시스템의 그룹 매핑 구성에서 고유한 그룹 이름을 입력합니다.

      이름에 기존 AD 그룹 도메인의 DN(고유 이름)과 동일한 값이 있는 경우 방화벽은 정책 및 로그와 같은 해당 이름에 대한 모든 참조에서 사용자 지정 그룹을 사용합니다.
   3. **LDAP** 필터를 최대 2,048자의 UTF-8 문자로 지정하고 확인을 클릭합니다.

      방화벽은 LDAP 필터의 유효성을 검사하지 않으므로 정확한지 확인하는 것은 사용자가 선택할 수 있습니다.

      *LDAP* 디렉토리 서버에 미치는 성능 영향을 최소화하려면 필터에 인덱싱된 속성만 사용합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

   정책 및 개체에서 사용자 지정 그룹을 사용할 수 있으려면 먼저 커밋해야 합니다.

**STEP 5 |** 변경 사항을 커밋합니다.

정책 및 개체에서 사용자 지정 그룹을 사용하려면 먼저 커밋해야 하며 방화벽이 LDAP 서버에서 특성을 수집할 수 있으려면 먼저 커밋해야 합니다.

*LDAP* 서버에서 그룹 매핑 정보를 검색하도록 방화벽을 구성한 후 검색하는 그룹을 기반으로 정책을 구성하기 전에 방화벽이 그룹 매핑 캐시를 새로 고칠 때까지 기다리거나 캐시를 수동으로 새로 고치는 것이 가장 좋습니다. 현재 정책에서 사용할 수 있는 그룹을 확인하려면 방화벽 CLI에 액세스하고 ***show user group*** 명령을 실행합니다. 방화벽이 다음에 그룹 매핑 캐시를 새로 고칠 시기를 확인하려면 **사용자 그룹 매핑 통계 표시** 명령을 실행하고 **다음 작업**을 확인합니다. 캐시를 수동으로 새로 고치려면 ***debug user-id refresh group-mapping all*** 명령을 실행합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 사용자 및 그룹 매핑에서 사용자를 올바르게 식별했는지 확인합니다.

1. 디바이스 > 사용자 식별 > 그룹 매핑 > 그룹 포함 목록을 선택하여 방화벽이 모든 그룹을 가져왔는지 확인합니다.
2. 모든 사용자 특성이 올바르게 캡처되었는지 확인하려면 다음 CLI 명령을 사용합니다.

```
show user user-attributes user all
```

UPN(사용자 계정 이름), 기본 사용자 이름, 이메일 속성 및 구성된 대체 사용자 이름에 대한 정규화된 형식은 모든 사용자에 대해 표시됩니다.

```
admin@PA-VM-8.1> show user user-attributes user all
```

```
Primary: nam\sam-user Email: sam-user@nam.com
```

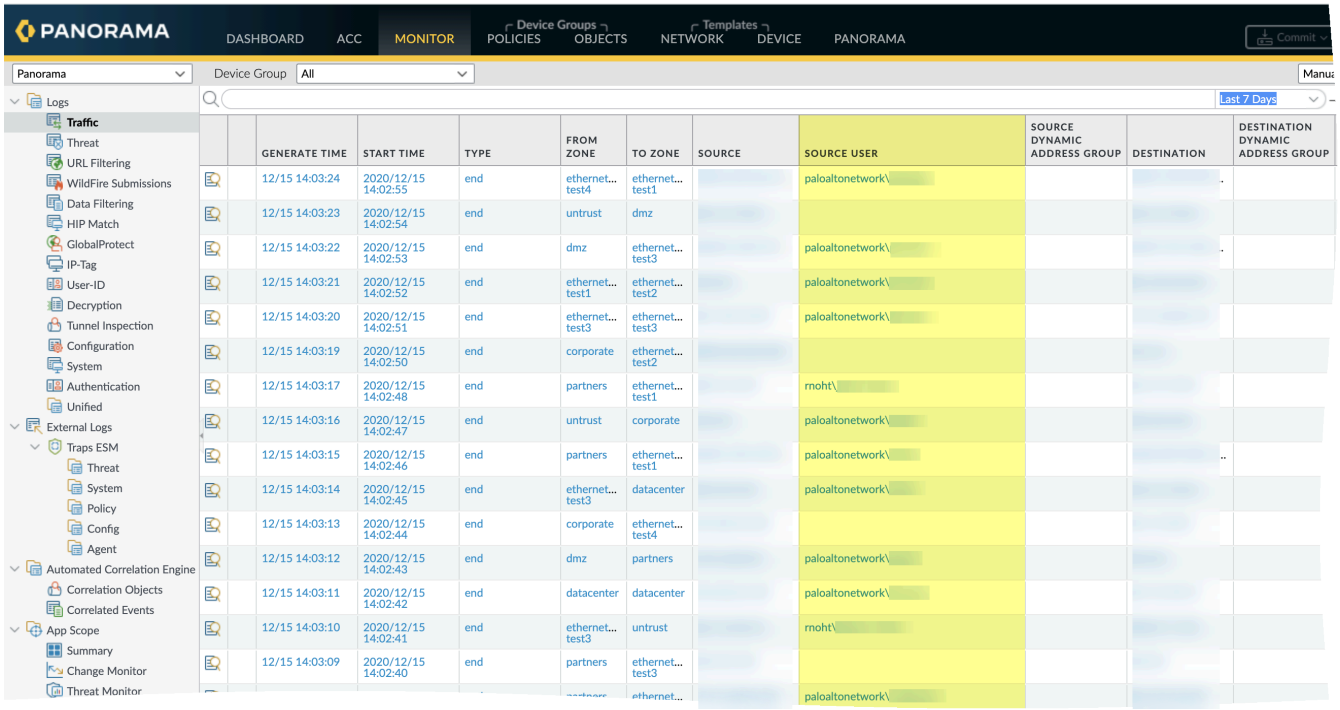
```
Alt User Names:1) nam.com\sam-user
```

```
2) nam\sam-user-upn
```

```
3) sam-user-upn@nam.local
```

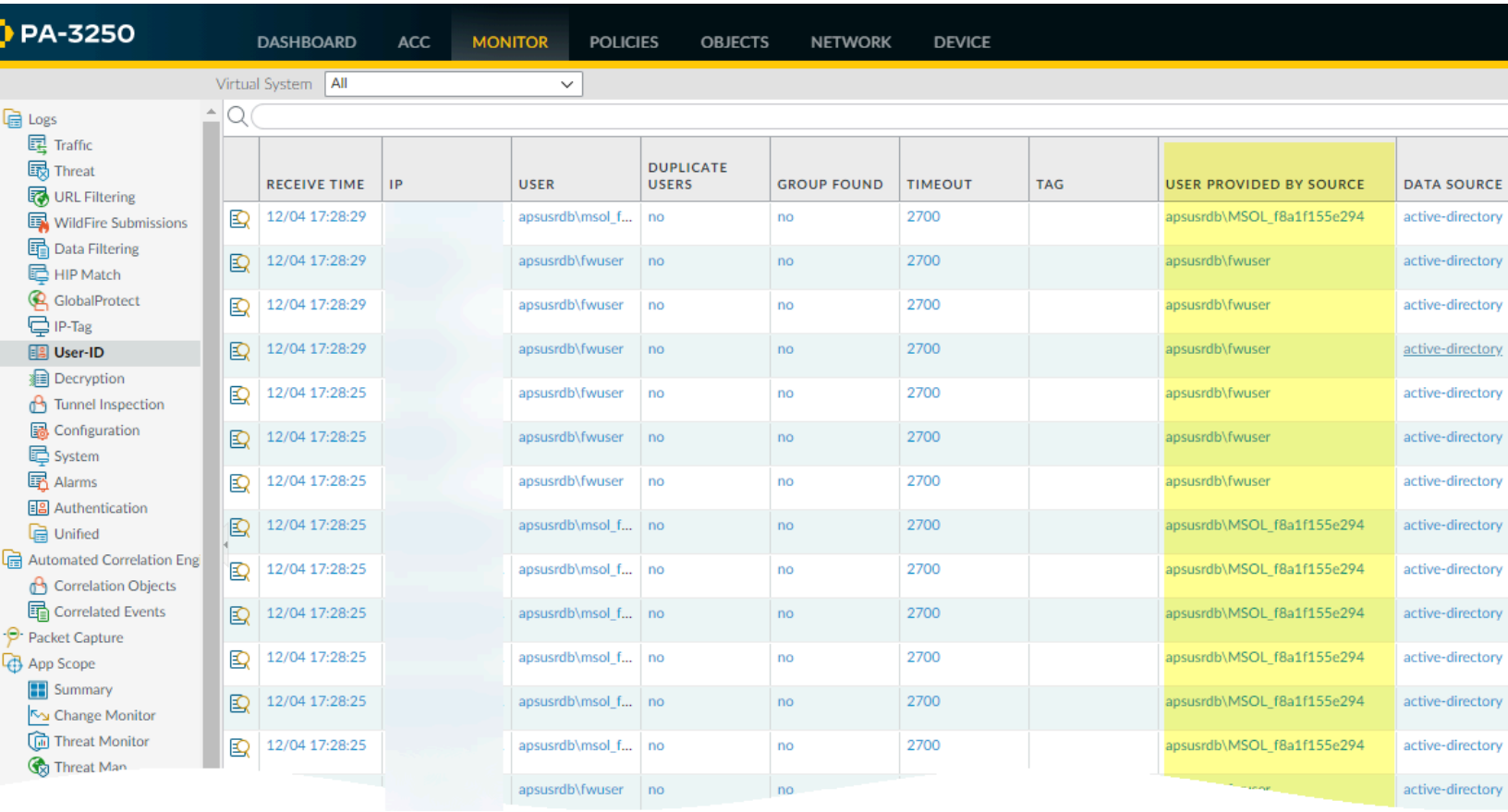
```
4) sam-user@nam.com
```

3. 사용자 이름이 모니터 > 로그 > 트래픽 아래의 소스 사용자 열에 올바르게 표시되는지 확인합니다.




 ©2023 Palo Alto Networks, Inc.

4. 사용자가 모니터 > 로그 > 사용자 **ID** 아래의 소스에서 제공한 사용자 열에서 올바른 사용자 이름에 매핑되었는지 확인합니다.




 ©2023 Palo Alto Networks, Inc.

# 사용자에게 IP 주소 매핑

사용자 ID는 IP 주소를 사용자 이름에 매핑하는 다양한 방법을 제공합니다. 사용자 매핑 구성을 시작하기 전에 사용자가 로그인하는 위치, 액세스하는 서비스 및 액세스 권한을 제어하는 데 필요한 애플리케이션 및 데이터를 고려합니다. 이렇게 하면 사용자를 식별할 수 있는 에이전트 또는 통합 유형이 표시됩니다.

계획이 있으면 애플리케이션 및 리소스에 대한 사용자 기반 액세스 및 가시성을 활성화하는 데 필요한 다음 방법 중 하나 이상을 사용하여 사용자 매핑을 구성할 수 있습니다.

- 도메인 서버에 로그인하지 않은 Linux 클라이언트를 실행하는 사용자(예: 도메인에 로그인하지 않는 사용자)가 있는 사용자는 인증 포털을 사용하여 IP 주소를 사용자 이름으로 매핑할 수 있습니다. 인증 정책과 함께 인증 포털을 사용하면 모든 사용자가 가장 중요한 애플리케이션 및 데이터에 액세스할 수 있도록 인증할 수 있습니다.
- 사용자가 Exchange 서버, 도메인 컨트롤러, eDirectory 서버 또는 Windows 클라이언트에 로그인할 때 사용자를 매핑하려면 User-ID 에이전트를 구성해야 합니다.
  - PAN-OS 통합 사용자 ID 에이전트를 사용하여 사용자 매핑 구성
  - Windows 사용자 ID 에이전트를 사용하여 사용자 매핑 구성
- Microsoft 터미널 서버 또는 Citrix 메타프레임 프레젠테이션 서버 또는 제닉스와 같은 Windows 환경에서 다중 사용자 시스템을 실행하는 클라이언트가 있는 경우, 사용자 매핑을 위한 Palo Alto Networks 터미널 서버(TS) 에이전트 구성. Windows에서 실행되지 않는 다중 사용자 시스템의 경우 PAN-OS XML API를 사용하여 터미널 서버에서 사용자 매핑을 검색할수 있습니다.
- 무선 컨트롤러, 802.1x 디바이스, Apple 오픈 디렉토리 서버, 프록시 서버 또는 기타 NAC(네트워크 액세스 제어) 메커니즘과 같은 사용자를 인증하는 기존 네트워크 서비스에서 사용자 매핑을 얻으려면 사용자 매핑을 위해 Syslog 발신자를 모니터링하도록 사용자 ID를 구성합니다.

  ***PAN-OS*** 통합 에이전트만 ***TLS***를 통해 청취하는 ***syslog***를 지원하기 때문에 방화벽에서 ***Windows*** 에이전트 또는 ***PAN-OS*** 통합 ***User-ID*** 에이전트를 구성하여 네트워크 서비스에서 인증 ***syslog*** 메시지를 수신하도록 구성할 수 있으며 이는 선호되는 구성입니다.
- 네트워크의 다른 디바이스가 사용자를 식별하고 사용자 기반 정책을 적용할 수 있도록 나가는 트래픽에 대한 헤더에 사용자 이름과 도메인을 포함하려면, HTTP 헤더에 사용자 이름 삽입을(를) 할 수 있습니다.
- 가상 시스템 전체에서 사용자 ID 매핑 공유하려면 가상 시스템을 User-ID 허브로 구성할 수 있습니다.
- 다른 방법을 사용하여 매핑할 수 없는 다른 클라이언트의 경우 XML API를 사용하여 사용자 매핑을 사용자 ID로 보낼수 있습니다.
- 대규모 네트워크에는 사용자 및 그룹 매핑을 위해 방화벽이 쿼리하는 수백 개의 정보 원본이 있을 수 있으며 매핑 정보를 기반으로 정책을 적용하는 수많은 방화벽이 있을 수 있습니다. User-ID 에이전트가 매핑하기 전에 매핑 정보를 집계하여 이러한 네트워크에 대한 사용자 ID 관리를 간소화할 수 있습니다. 일부 방화벽을 구성하여 매핑 정보를 재배포하여 방화벽 및 정보 소스가 쿼리 프로세스에서 사용하는 리소스를 줄일 수도 있습니다. 자세한 내용은 대규모 네트워크에서 사용자 ID 배포를 참조하십시오.

## 사용자 ID 에이전트에 대한 전용 서비스 계정 생성

Windows 기반 User-ID 에이전트 또는 PAN-OS 통합 User-ID 에이전트를 사용하여 Exchange 서버, 도메인 컨트롤러, eDirectory 서버 또는 Windows 클라이언트에 로그인할 때 사용자를 매핑하려면 해당


©2023 Palo Alto Networks, Inc.

사용자에 대한 전용 서비스 계정을 생성하고 에이전트가 모니터링할 각 도메인의 도메인 컨트롤러에서 User-ID 에이전트에 대한 전용 서비스 계정을 만듭니다.

User-ID 에이전트는 보안 이벤트에 대한 로그를 기반으로 사용자를 매핑합니다. User-ID 에이전트가 사용자를 성공적으로 매핑할 수 있도록 하려면 매핑 소스가 로그온 감사, Kerberos 인증 서비스 감사 및 Kerberos 서비스 티켓 작업 감사 이벤트에 대한 로그를 생성하는지 확인하십시오. 소스는 최소한 다음 이벤트에 대한 로그를 생성해야 합니다.

- 로그온 성공(4624)
- 인증 티켓 부여(4768)
- 서비스 티켓 부여(4769)
- 갱신된 티켓(4770)

서비스 계정에 필요한 권한은 사용하려는 사용자 매핑 방법 및 설정에 따라 다릅니다. 예를 들어 PAN-OS 통합 User-ID 에이전트를 사용하는 경우 서비스 계정에는 사용자 세션을 모니터링하기 위한 서버 운영자 권한이 필요합니다. Windows 기반 User-ID 에이전트를 사용하는 경우 서비스 계정에는 사용자 세션을 모니터링하기 위한 서버 운영자 권한이 필요하지 않습니다. User-ID 서비스 계정이 손상될 위험을 줄이려면 항상 에이전트에 필요한 최소한의 권한 집합으로 계정을 구성하십시오.

- 지원되는 Windows 서버에 Windows 기반 User-ID 에이전트를 설치하는 경우 Windows User-ID 에이전트에 대한 서비스 계정을 구성하십시오.
- 방화벽에서 PAN-OS 통합 User-ID 에이전트를 사용하는 경우 PAN-OS 통합 User-ID 에이전트에 대한 서비스 계정을 구성합니다.

***User-ID***는 사용자 매핑 정보를 안전하게 수집하기 위한 다양한 방법을 제공합니다. 로컬 네트워크에 연결된 ***Windows*** 데스크톱에서만 사용자 매핑이 필요한 환경을 위해 설계된 일부 레거시 기능에는 권한 있는 서비스 계정이 필요합니다. 권한 있는 서비스 계정이 손상되면 네트워크가 공격에 노출됩니다. 가장 좋은 방법은 클라이언트 조사 및 세션 모니터링과 같이 손상될 경우 위협이 될 수 있는 권한이 필요한 레거시 기능을 사용하지 않는 것입니다.

## Windows User-ID 에이전트에 대한 서비스 계정 구성

Windows User-ID 에이전트가 사용자 매핑을 수집하기 위해 모니터링할 서비스 및 호스트에 액세스할 수 있도록 전용 AD(Active Directory) 서비스 계정을 생성합니다. 에이전트가 모니터링할 각 도메인에 서비스 계정을 생성해야 합니다. 서비스 계정에 필요한 권한을 활성화한 후 Windows User-ID 에이전트를 사용하여 사용자 매핑을 구성합니다.

다음 워크플로는 필요한 모든 권한을 자세히 설명하고 위협을 유발할 수 있는 권한이 필요한 사용자 ***ID*** 기능에 대한 지침을 제공하므로 전반적인 보안 태세를 손상시키지 않고 사용자를 가장 잘 식별하는 방법을 결정할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** User-ID 에이전트에 대한 AD 서비스 계정을 생성합니다.

에이전트가 모니터링할 각 도메인에 서비스 계정을 생성해야 합니다.

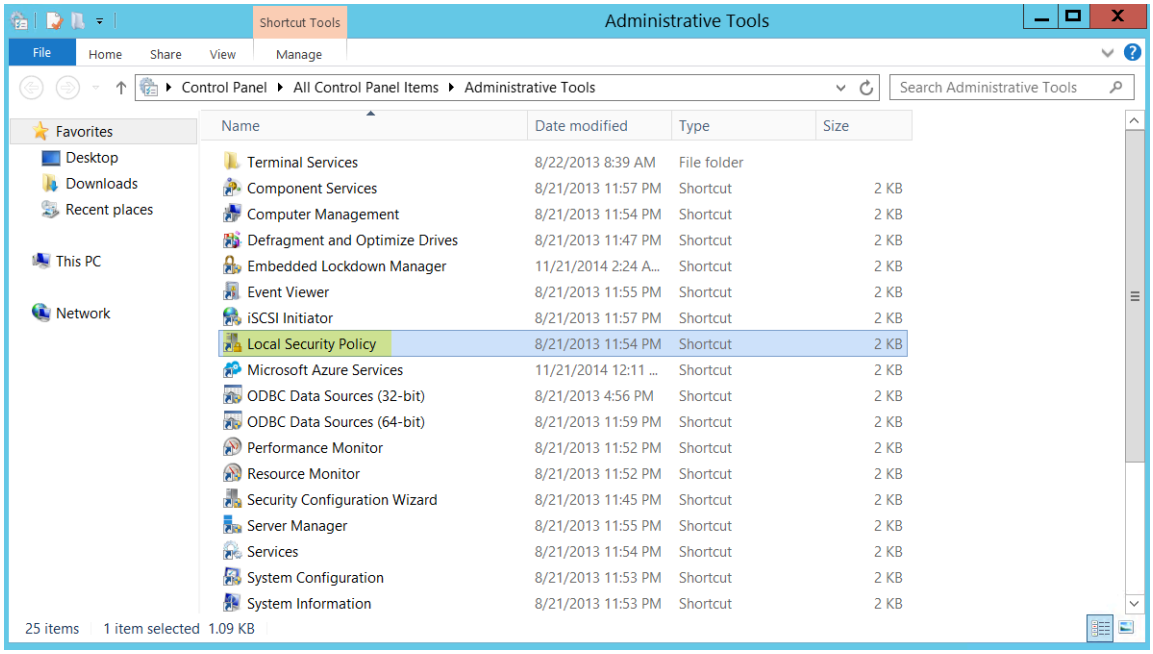
1. 도메인 컨트롤러에 로그인합니다.
2. Windows 아이콘(⊞)을 마우스 오른쪽 버튼으로 클릭하고 검색하여 **Active Directory 사용자 및 컴퓨터**를 실행하고 애플리케이션을 시작합니다.
3. 탐색 창에서 도메인 트리를 열고 관리 서비스 계정을 마우스 오른쪽 버튼으로 클릭하고 새로 만들기 > 사용자를 선택합니다.
4. 사용자의 이름, 성, 사용자 로그온 이름을 입력하고 다음을 클릭합니다.
5. 암호 및 암호 확인을 입력하고 다음 및 마침을 클릭합니다.

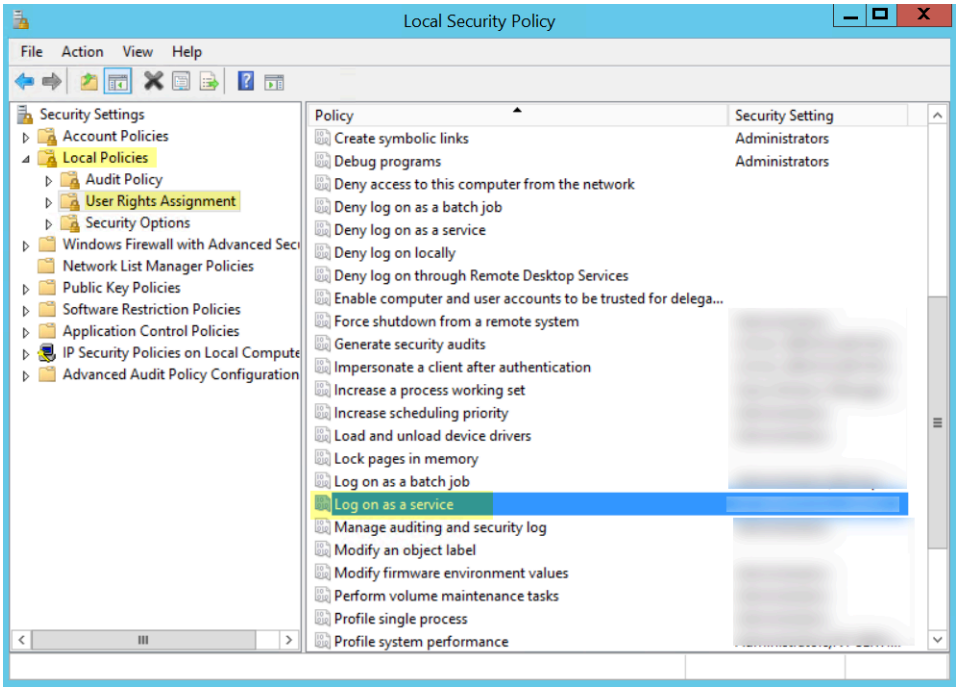
 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 서비스 계정이 서비스로 로그온할 수 있도록 로컬 또는 그룹 정책을 구성합니다.

서비스로 로그온할 수 있는 권한은 에이전트 호스트인 Windows 서버에서만 로컬로 필요합니다.

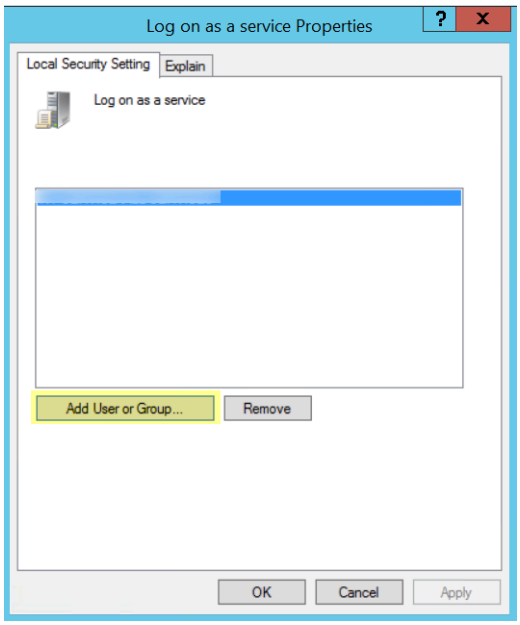
- 권한을 로컬로 할당하려면:

1. 제어판 > 관리 도구 > 로컬 보안 정책을 선택합니다.
2. 

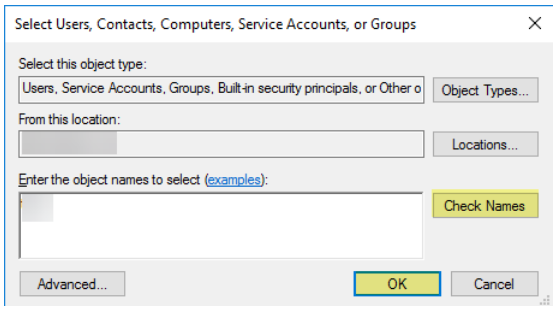
3. 로컬 정책 > 사용자 권한 할당 > 서비스 로그온을 선택합니다.


4. 사용자 또는 그룹을 추가하여 서비스 계정을 추가합니다.

 ©2023 Palo Alto Networks, Inc.

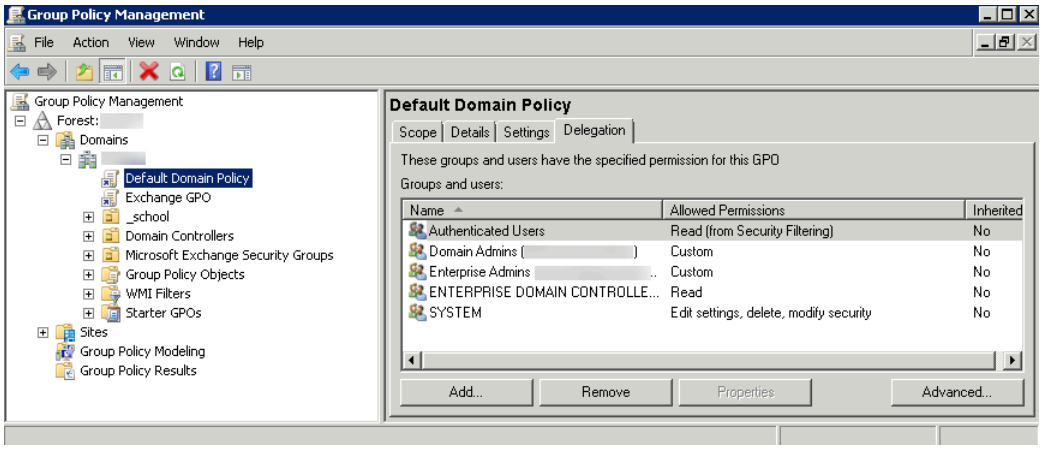



5. **domain\username** 이름 형식으로 선택할 개체 이름**(**서비스 계정 이름**)**을 입력하고 확인을 클릭합니다.



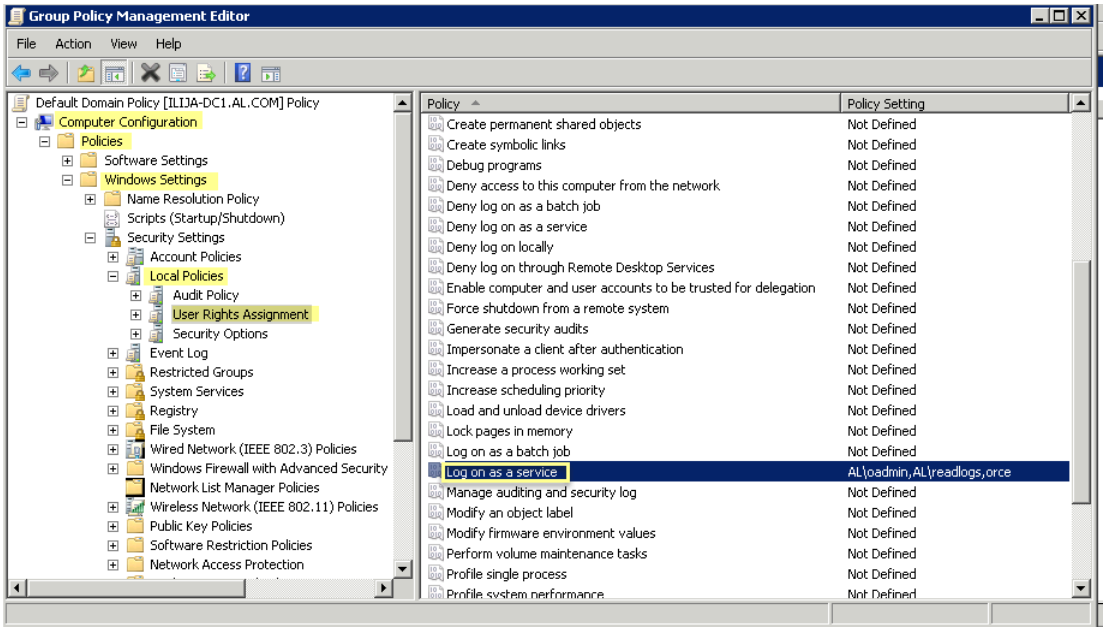

- 여러 서버에 Windows User-ID 에이전트를 설치하는 경우 그룹 정책을 구성하려면 그룹 정책 관리 편집기를 사용하십시오.

1. 시작 > 그룹 정책 관리 > **<your domain>** > 기본 도메인 정책 > 작업 > 수정을 선택합니다**.** 에이전트 호스트인 **Windows** 서버의 경우.



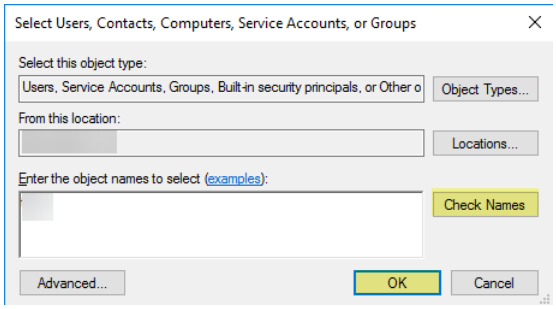

 ©2023 Palo Alto Networks, Inc.

2. 컴퓨터 구성 > 정책 > **Windows** 설정 > 보안 설정 > 로컬 정책 > 사용자 권한 할당을 선택합니다.




3. 서비스로 로그온을 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.
4. 사용자 또는 그룹 추가하여 서비스 계정 사용자 이름 또는 기본 제공 그룹을 추가한 다음 확인을 두 번 클릭합니다.

   관리자는 기본적으로 이 권한을 가집니다.




**STEP 3 |** WMI를 사용하여 사용자 데이터를 수집하려면 모니터링되는 서버에서 WMI 쿼리를 사용할 수 있도록 서비스 계정에 DCOM 권한을 할당합니다.

1. **Active Directory** 사용자 및 컴퓨터 > **<your domain>** > 기본 > 분산 **COM** 사용자를 선택합니다.
2. 속성 > 구성원 > 추가를 마우스 오른쪽 버튼으로 클릭하고 서비스 계정 이름을 입력합니다.

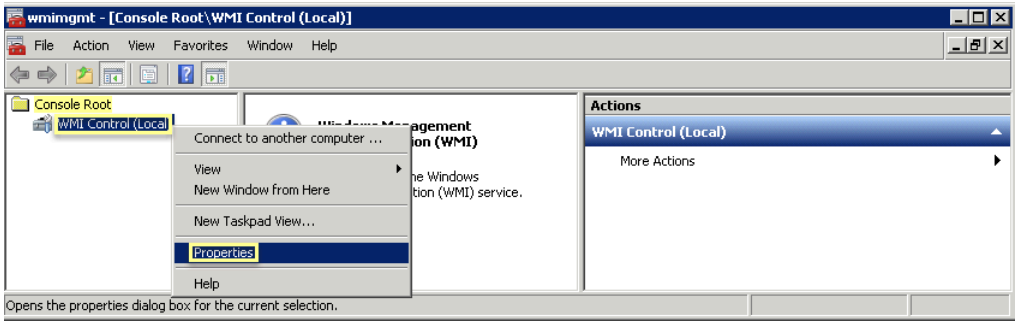

©2023 Palo Alto Networks, Inc.

**STEP 4 |** WMI 검색을 사용하려는 경우 계정이 CIMV2 네임스페이스를 읽고 검색할 클라이언트 시스템에 필요한 권한을 할당할 수 있도록 설정합니다.

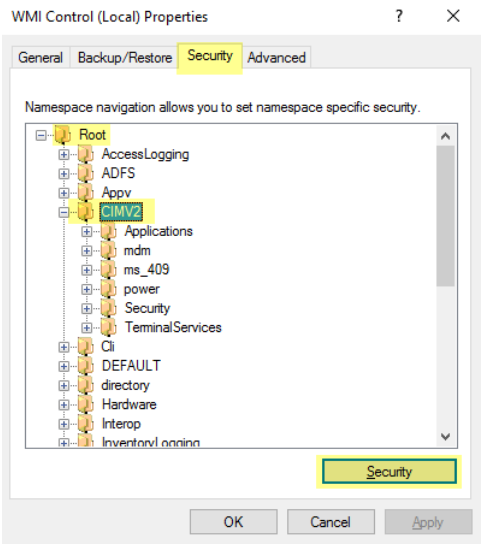
보안 수준이 높은 네트워크에서 클라이언트 프로빙을 활성화하지 마십시오. 클라이언트 프로빙은 많은 양의 네트워크 트래픽을 생성할 수 있으며 잘못 구성되면 보안에 위협이 될 수 있습니다. 대신 도메인 컨트롤러와 같이 더 독립되고 신뢰할 수 있는 소스에서 사용자 매핑 정보를 수집하고 *Syslog* 또는 *XML API*와의 통합을 통해 수집하며, *Windows* 클라이언트 대신 모든 디바이스 유형 또는 운영 체제에서 사용자 매핑 정보를 안전하게 캡처할 수 있다는 추가 이점이 있습니다.

User-ID 에이전트가 사용자 매핑 정보를 조사할 각 클라이언트 시스템에서 다음 작업을 수행합니다.

1. Windows 아이콘()을 마우스 오른쪽 버튼으로 클릭하고 검색하여 **wmimgmt.msc**를 찾은 다음 WMI 관리 콘솔을 시작합니다.
2. 콘솔 트리에서 **WMI Control**을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.




3. 보안 탭을 선택한 다음 루트 > **CIMV2**를 선택하고 보안 버튼을 클릭합니다.

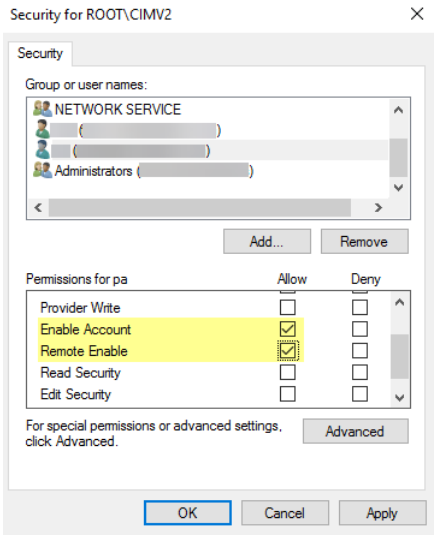



4. 생성한 서비스 계정의 이름을 추가하고 이름을 확인하여 항목을 확인한 다음 확인을 클릭합니다.

   계정 이름을 쿼리하려면 위치를 변경하거나 고급을 클릭해야 할 수 있습니다. 자세한 내용은 대화 상자 도움말을 참조하십시오.

5. **<Username>**에 대한 권한 섹션에서 계정 활성화 및 원격 활성화 권한을 허용합니다.

 ©2023 Palo Alto Networks, Inc.

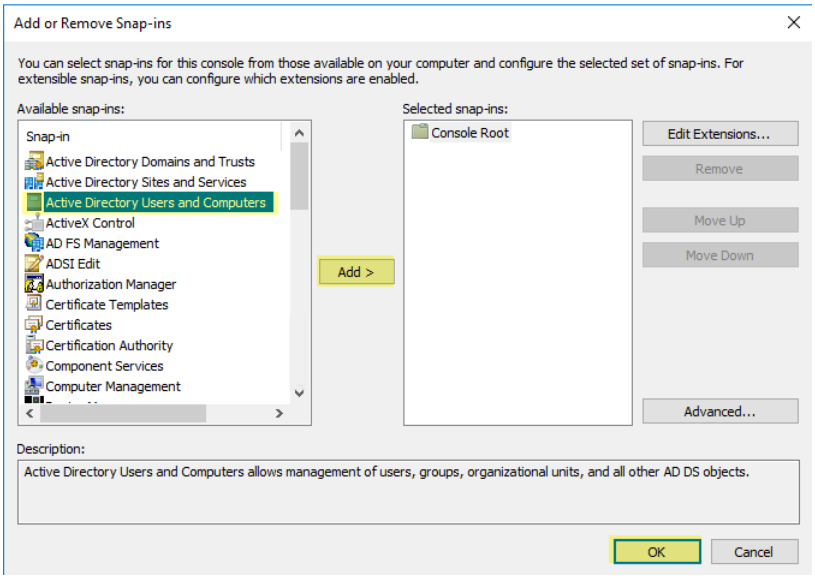



6. 확인을 두 번 클릭합니다.
7. 로컬 사용자 및 그룹 MMC 스냅인(lusrmgr.msc)을 사용하여 조사할 시스템의 로컬 DCOM(Distributed Component Object Model) 사용자 및 원격 데스크톱 사용자 그룹에 서비스 계정을 추가합니다.

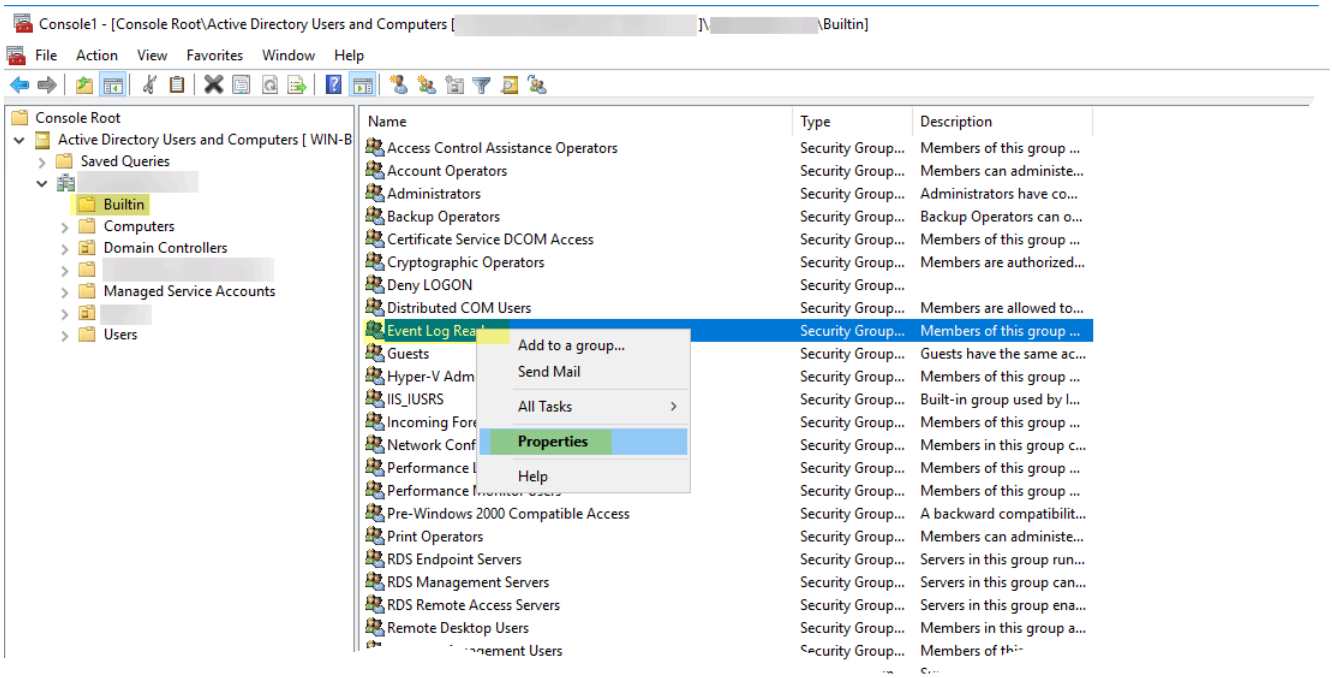
 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 서버 모니터링을(를) 사용하여 사용자를 식별하려면 서비스 계정이 보안 로그 이벤트를 읽을 수 있도록 이벤트 로그 판독기 기본 제공 그룹에 서비스 계정을 추가하십시오.

1. User-ID 에이전트가 읽을 로그가 포함된 도메인 컨트롤러 또는 Exchange 서버에서, 또는 Windows 로그 포워딩의 이벤트를 수신하는 구성원 서버에서 **Start** > **Run**을 선택한 다음 **MMC**를 입력합니다.
2. 파일 > 스냅인 추가/제거 > **Active Directory** 사용자 및 컴퓨터 > 추가를 선택한 다음 확인하여 MMC를 실행하고 Active Directory 사용자 및 컴퓨터 스냅인을 시작합니다.

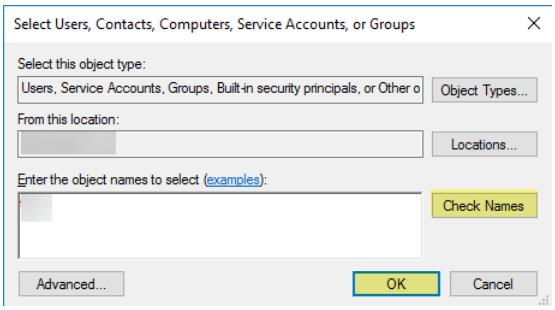



3. 도메인의 Builtin 폴더로 이동하고 **Event Log Readers** 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Properties** > **Members**를 선택합니다.




4. 서비스 계정을 추가한 다음 이름 확인을 클릭하여 적절한 개체 이름이 있는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.



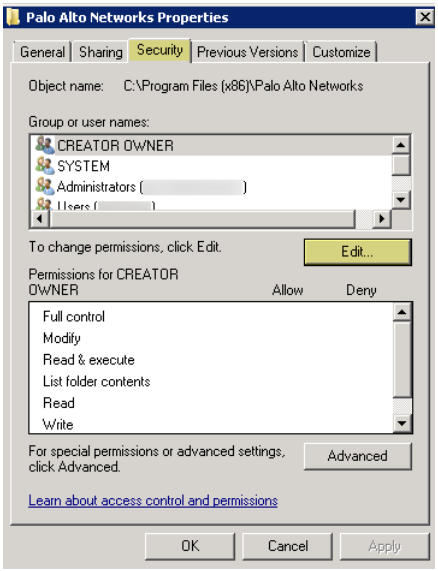

5. 확인을 두 번 클릭하여 설정을 저장합니다.
6. 기본 제공 이벤트 로그 리더 그룹이 서비스 계정을 구성원으로 나열하는지 확인합니다(이벤트 로그 리더 > 속성 > 구성원).

 ©2023 Palo Alto Networks, Inc.

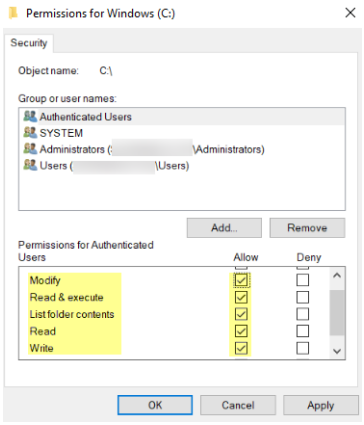
**STEP 6 |** 서비스 계정이 에이전트의 설치 폴더에 액세스하여 구성을 읽고 로그를 작성할 수 있도록 설치 폴더에 계정 권한을 할당하십시오.

User-ID 에이전트에 대해 구성한 서비스 계정이 도메인 관리자 또는 User-ID 에이전트 서버 호스트의 로컬 관리자가 아닌 경우에만 이 단계를 수행하면 됩니다.

1. Windows 탐색기에서 **`C:\Program Files(x86)\Palo Alto Networks`**로 이동하고 폴더를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
2. 보안 탭에서 편집을 클릭합니다.




3. **User-ID** 에이전트 서비스 계정을 추가하고 수정, 읽기 및 실행, 폴더 내용 나열에 대한 허용 권한, 읽기, 쓰기를 차례로 클릭한 다음 확인을 클릭하여 계정 설정을 저장합니다.

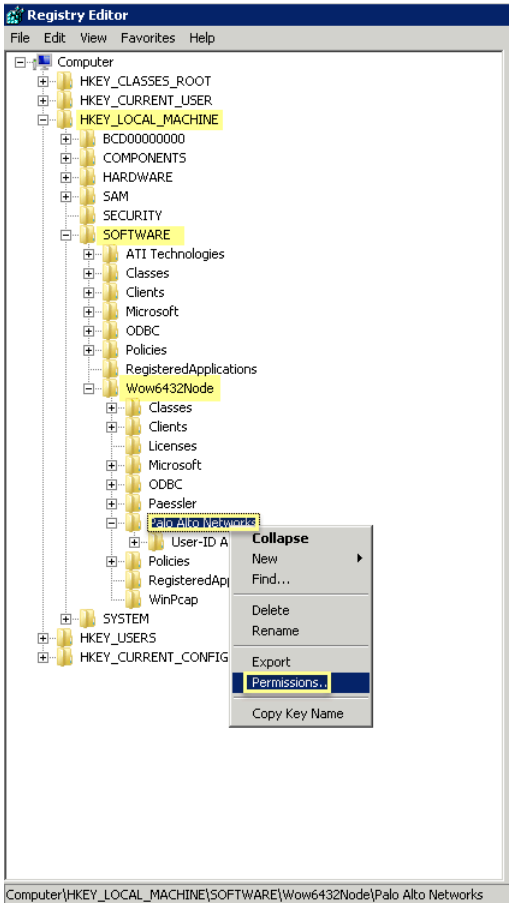



개별 권한을 구성하지 않으려면 대신 모든 권한을 허용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

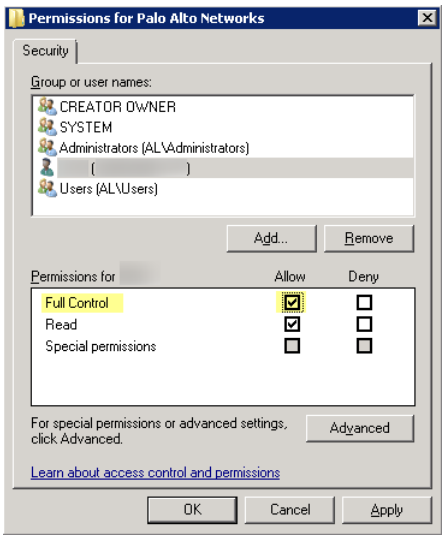
**STEP 7 |** 에이전트가 구성을 변경할 수 있도록 하려면(예: 다른 로깅 수준을 선택하는 경우) User-ID 에이전트 레지스트리 하위 트리에 서비스 계정 권한을 부여합니다.

1. **Start** > **Run**을 선택한 다음 **regedt32**를 입력하고 다음 위치 중 하나에서 Palo Alto Networks 하위 트리로 이동합니다.
   - **32**비트 시스템 - `HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`
   - **64-bit systems** - `HKEY_LOCAL_MACHINE\Software\WOW6432Node\PaloAlto Networks`
2. **Palo Alto Networks** 노드를 마우스 오른쪽 버튼으로 클릭하고 권한을 선택합니다.




3. User-ID 서비스 계정에 모든 권한을 할당한 다음 확인을 클릭하여 설정을 저장합니다.

 ©2023 Palo Alto Networks, Inc.




**STEP 8 |** 필요하지 않은 서비스 계정 권한을 비활성화합니다.

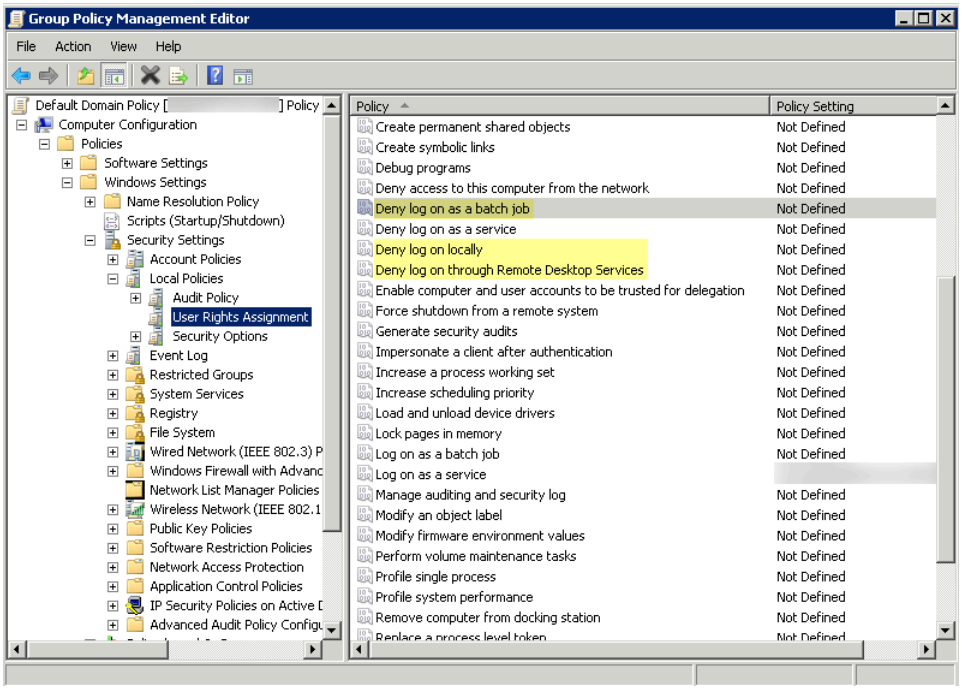
User-ID 서비스 계정에 최소한의 계정 권한 집합이 있는지 확인하면 계정이 손상된 경우 공격 대상을 줄일 수 있습니다.

사용자 ID 계정에 필요한 최소 권한이 있는지 확인하려면 계정에 대한 다음 권한을 거부하십시오.

- **User-ID** 서비스 계정에 대한 대화형 로그온 거부 - User-ID 서비스 계정에는 Active Directory 보안 이벤트 로그를 읽고 구문 분석하는 권한이 필요하지만 서버 또는 도메인 시스템에 대화형으로 로그온하는 기능은 필요하지 않습니다. 그룹 정책을 사용하거나 관리 서비스 계정을 사용하여 이 권한을 제한할 수 있습니다(자세한 내용은 Microsoft TechNet 참조).
  1. 그룹 정책 관리 편집기 > 기본 도메인 정책 > 컴퓨터 구성 > 정책 > **Windows** 설정 > 보안 설정 > 사용자 권한 할당을 선택합니다.
  2. 일괄 작업으로 로그온 거부, 로컬 로그온 거부 및 원격 데스크톱 서비스를 통한 로그온 거부에서 속성을 마우스 오른쪽 버튼을 클릭합니다.

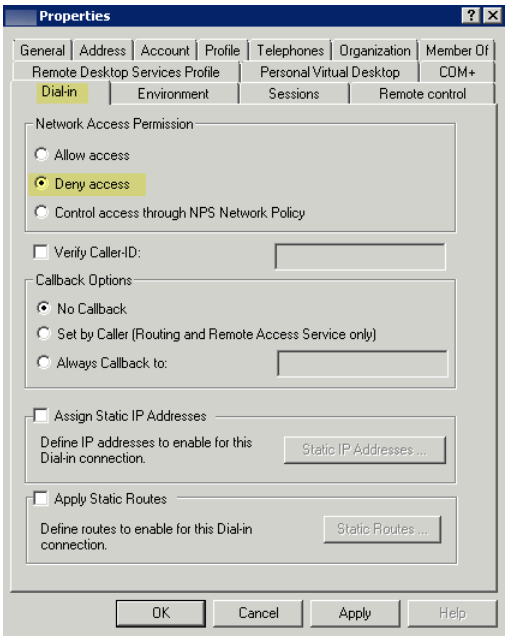
 ©2023 Palo Alto Networks, Inc.

3. 이 정책 설정 정의 > 사용자 또는 그룹 추가를 선택하고 서비스 계정 이름을 추가한 다음 확인을 클릭합니다.




- 사용자 **ID** 서비스 계정에 대한 원격 액세스 거부 - 공격자가 해당 계정을 사용하여 네트워크 외부에서 네트워크에 액세스하는 것을 방지합니다.

  1. 시작 > 실행을 선택하고 **MMC**를 입력한 다음 파일 > 스냅인 추가/제거 > **Active Directory** 사용자 및 컴퓨터 > 사용자를 선택합니다.
  2. 서비스 계정 이름을 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.
  3. 전화 접속을 선택한 다음 네트워크 액세스 권한을 거부합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** 다음 단계로 Windows User-ID 에이전트를 사용하여 사용자 매핑을 구성합니다.

## PAN-OS 통합 User-ID 에이전트에 대한 서비스 계정 구성

PAN-OS 통합 User-ID 에이전트가 사용자 매핑을 수집하기 위해 모니터링할 서비스 및 호스트에 액세스하기 위한 전용 AD(Active Directory) 서비스 계정을 생성합니다. 에이전트가 모니터링할 각 도메인에 서비스 계정을 생성해야 합니다. 서비스 계정에 필요한 권한을 활성화한 후 PAN-OS 통합 User-ID 에이전트를 사용하여 사용자 매핑을 구성합니다.

다음 워크플로는 필요한 모든 권한을 자세히 설명하고 위협을 유발할 수 있는 권한이 필요한 사용자 *ID* 기능에 대한 지침을 제공하므로 전반적인 보안 태세를 손상시키지 않고 사용자를 가장 잘 식별하는 방법을 결정할 수 있습니다.

**STEP 1 |** User-ID 에이전트에 대한 AD 서비스 계정을 생성합니다.

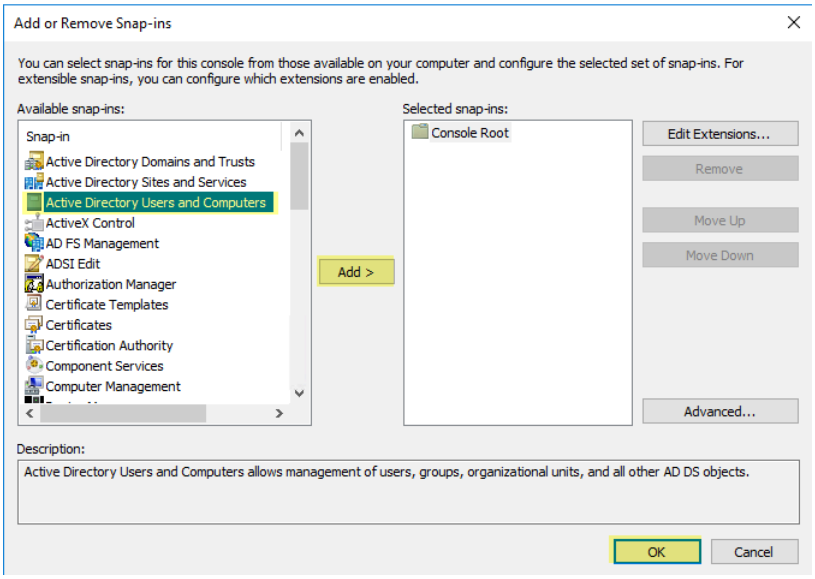
에이전트가 모니터링할 각 도메인에 서비스 계정을 생성해야 합니다.

1. 도메인 컨트롤러에 로그인합니다.
2. Windows 아이콘()을 마우스 오른쪽 버튼으로 클릭하고 검색하여 **Active Directory 사용자 및 컴퓨터**를 실행하고 애플리케이션을 시작합니다.
3. 탐색 창에서 도메인 트리를 열고 관리 서비스 계정을 마우스 오른쪽 버튼으로 클릭하고 새로 만들기 > 사용자를 선택합니다.
4. 사용자의 이름, 성, 사용자 로그온 이름을 입력하고 다음을 클릭합니다.
5. 암호 및 암호 확인을 입력하고 다음 및 마침을 클릭합니다.

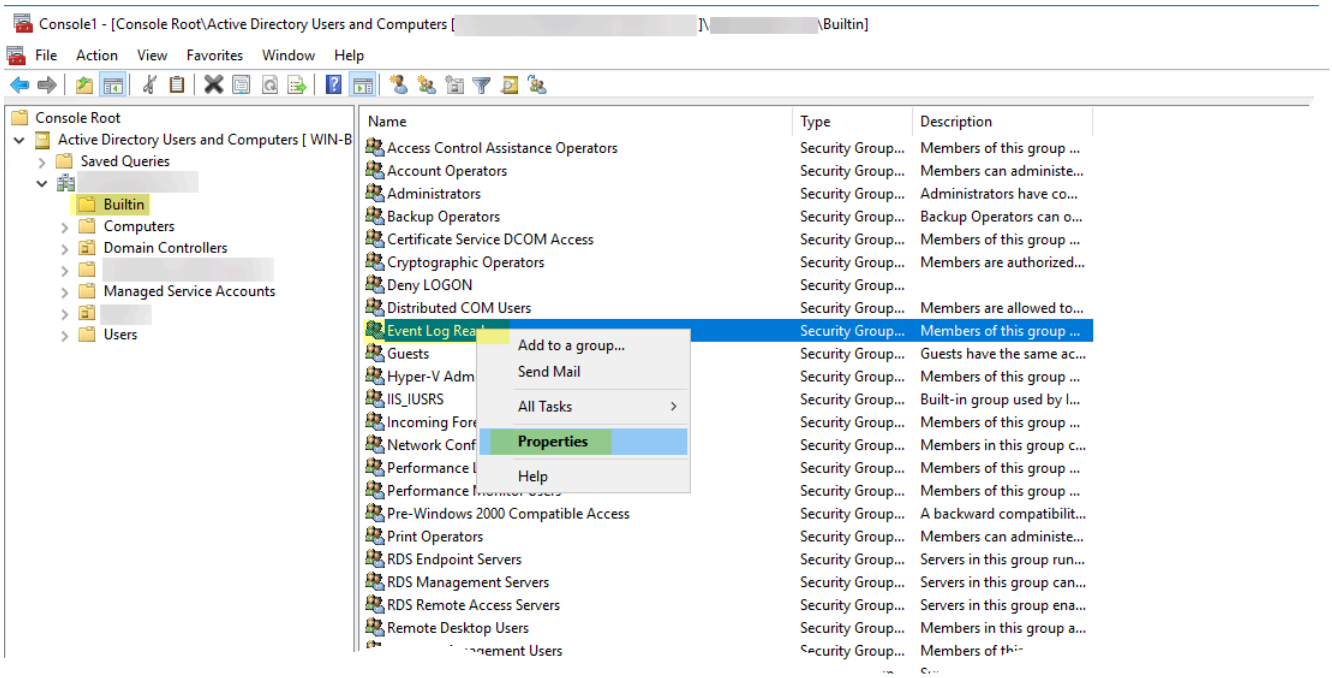

©2023 Palo Alto Networks, Inc.

**STEP 2 |** 서버 모니터링을(를) 사용하여 사용자를 식별하려면 서비스 계정이 보안 로그 이벤트를 읽을 수 있도록 이벤트 로그 판독기 기본 제공 그룹에 서비스 계정을 추가하십시오.

1. User-ID 에이전트가 읽을 로그가 포함된 도메인 컨트롤러 또는 Exchange 서버에서, 또는 Windows 로그 포워딩의 이벤트를 수신하는 구성원 서버에서 **Start** > **Run**을 선택한 다음 **MMC**를 입력합니다.
2. 파일 > 스냅인 추가/제거 > **Active Directory** 사용자 및 컴퓨터 > 추가를 선택한 다음 확인하여 MMC를 실행하고 Active Directory 사용자 및 컴퓨터 스냅인을 시작합니다.

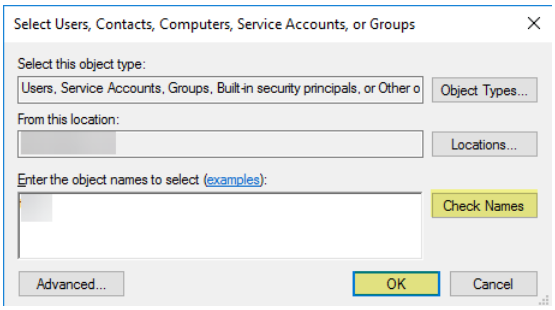



3. 도메인의 Builtin 폴더로 이동하고 **Event Log Readers** 그룹을 마우스 오른쪽 버튼으로 클릭하고 **Properties** > **Members**를 선택합니다.




4. 서비스 계정을 추가한 다음 이름 확인을 클릭하여 적절한 개체 이름이 있는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.




5. 확인을 두 번 클릭하여 설정을 저장합니다.
6. 기본 제공 이벤트 로그 리더 그룹이 서비스 계정을 구성원으로 나열하는지 확인합니다(이벤트 로그 리더 > 속성 > 구성원).

**STEP 3 |** WMI를 사용하여 사용자 데이터를 수집하려면 모니터링되는 서버에서 WMI 쿼리를 사용할 수 있도록 서비스 계정에 DCOM 권한을 할당합니다.

1. **Active Directory** 사용자 및 컴퓨터 > **<your domain>** > 기본 > 분산 **COM** 사용자를 선택합니다.
2. 속성 > 구성원 > 추가를 마우스 오른쪽 버튼으로 클릭하고 서비스 계정 이름을 입력합니다.

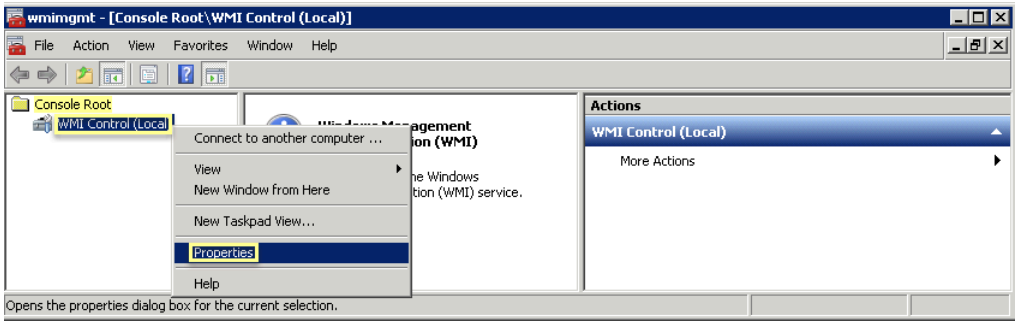

©2023 Palo Alto Networks, Inc.

**STEP 4 |** WMI 검색을 사용하려는 경우 모니터링할 도메인 컨트롤러에서 CIMV2 네임스페이스를 읽을 수 있도록 서비스 계정을 활성화하고 검색할 클라이언트 시스템에 필요한 권한을 할당합니다.

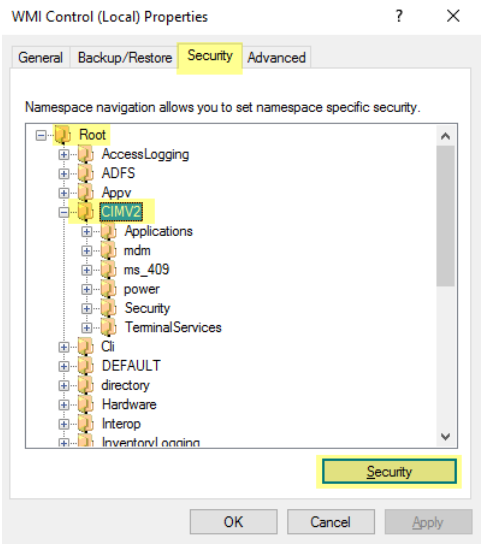
보안 수준이 높은 네트워크에서 클라이언트 프로빙을 활성화하지 마십시오. 클라이언트 프로빙은 많은 양의 네트워크 트래픽을 생성할 수 있으며 잘못 구성되면 보안에 위협이 될 수 있습니다. 대신 도메인 컨트롤러와 같이 더 독립되고 신뢰할 수 있는 소스에서 사용자 매핑 정보를 수집하고 *Syslog* 또는 *XML API*와의 통합을 통해 수집하며, *Windows* 클라이언트 대신 모든 디바이스 유형 또는 운영 체제에서 사용자 매핑 정보를 안전하게 캡처할 수 있다는 추가 이점이 있습니다.

User-ID 에이전트가 사용자 매핑 정보를 조사할 각 클라이언트 시스템에서 다음 작업을 수행합니다.

1. Windows 아이콘()을 마우스 오른쪽 버튼으로 클릭하고 검색하여 **wmimgmt.msc**를 찾은 다음 WMI 관리 콘솔을 시작합니다.
2. 콘솔 트리에서 **WMI Control**을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.




3. 보안 탭을 선택한 다음 루트 > **CIMV2**를 선택하고 보안 버튼을 클릭합니다.

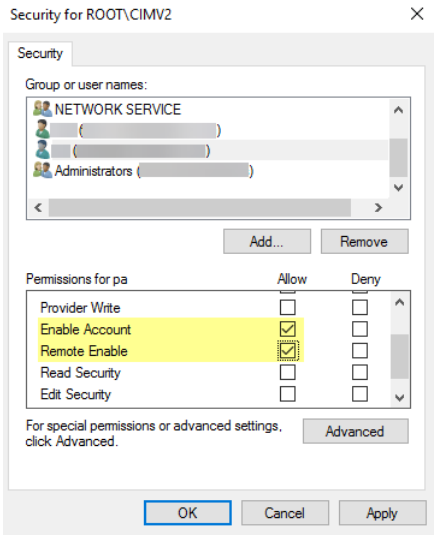



4. 생성한 서비스 계정의 이름을 추가하고 이름을 확인하여 항목을 확인한 다음 확인을 클릭합니다.

계정 이름을 쿼리하려면 위치를 변경하거나 고급을 클릭해야 할 수 있습니다. 자세한 내용은 대화 상자 도움말을 참조하십시오.

5. **<Username>**에 대한 권한 섹션에서 계정 활성화 및 원격 활성화 권한을 허용합니다.


©2023 Palo Alto Networks, Inc.




6. 확인을 두 번 클릭합니다.
7. 로컬 사용자 및 그룹 MMC 스냅인(lusrmgr.msc)을 사용하여 조사할 시스템의 로컬 DCOM(Distributed Component Object Model) 사용자 및 원격 데스크톱 사용자 그룹에 서비스 계정을 추가합니다.

**STEP 5 |** (권장하지 않음) 에이전트가 사용자 매핑 정보에 대해 Windows 서버를 폴링하기 위해 사용자 세션을 모니터링할 수 있도록 하려면 서비스 계정에 서버 운영자 권한을 할당하십시오.

이 그룹에는 서버를 종료하고 다시 시작할 수 있는 권한도 있으므로 사용자 세션 모니터링이 매우 중요한 경우에만 이 그룹에 계정을 할당하십시오.

1. **Active Directory** 사용자 및 컴퓨터 > **<your domain>** > 기본 > 서버 운영자 그룹을 선택합니다.
2. 속성 > 구성원 > 추가 서비스 계정 이름 추가를 마우스 오른쪽 버튼으로 클릭합니다.

**STEP 6 |** 필요하지 않은 서비스 계정 권한을 비활성화합니다.

User-ID 서비스 계정에 최소한의 계정 권한 집합이 있는지 확인하면 계정이 손상된 경우 공격 대상을 줄일 수 있습니다.

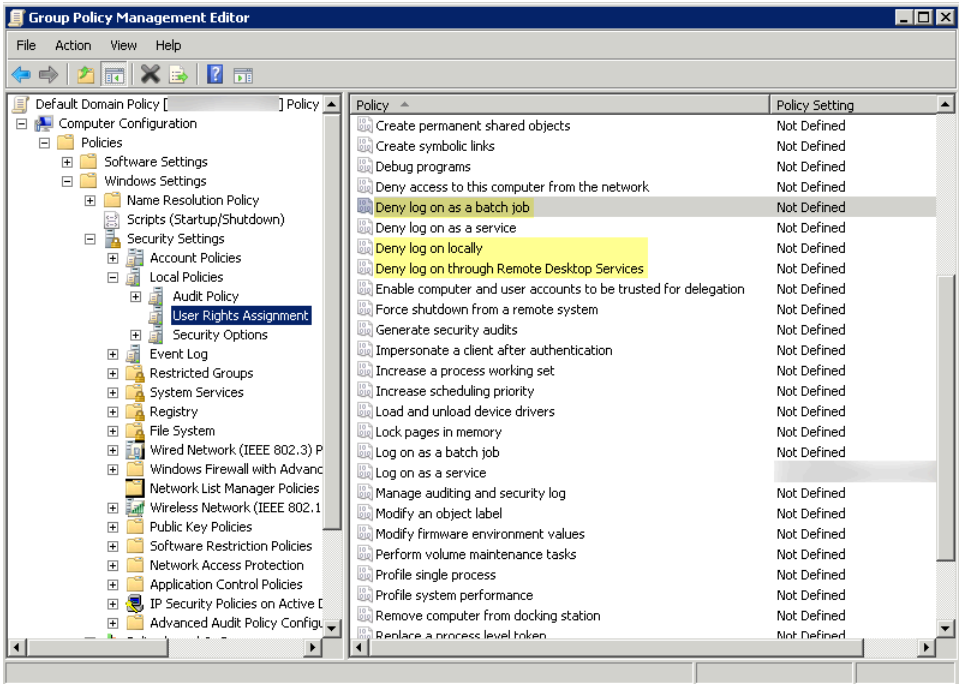
사용자 ID 계정에 필요한 최소 권한이 있는지 확인하려면 계정에 대한 다음 권한을 거부하십시오.

- **User-ID** 서비스 계정에 대한 대화형 로그온 거부 - User-ID 서비스 계정에는 Active Directory 보안 이벤트 로그를 읽고 구문 분석하는 권한이 필요하지만 서버 또는 도메인 시스템에 대화형으로 로그온하는 기능은 필요하지 않습니다. 그룹 정책을 사용하거나 관리 서비스 계정을 사용하여 이 권한을 제한할 수 있습니다(자세한 내용은 Microsoft TechNet 참조).

  **1.** 그룹 정책 관리 편집기 > 기본 도메인 정책 > 컴퓨터 구성 > 정책 > **Windows** 설정 > 보안 설정 > 사용자 권한 할당을 선택합니다.

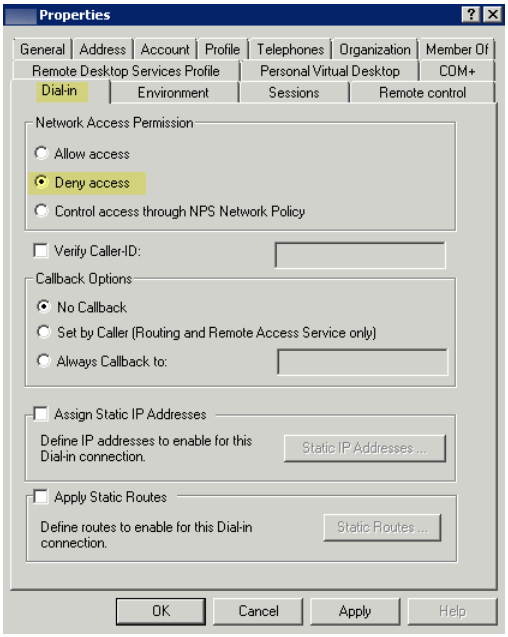

©2023 Palo Alto Networks, Inc.

2. 일괄 작업으로 로그온 거부, 로컬 로그온 거부 및 원격 데스크톱 서비스를 통한 로그온 거부의 경우 속성을 마우스 오른쪽 버튼으로 클릭하고 이 정책 설정 정의 > 사용자 또는 그룹 추가를 선택하고 서비스 계정 이름을 추가한 다음 확인을 클릭합니다.




- 사용자 **ID** 서비스 계정에 대한 원격 액세스 거부 - 공격자가 해당 계정을 사용하여 네트워크 외부에서 네트워크에 액세스하는 것을 방지합니다.

  1. 시작 > 실행, **MMC** 입력, 파일 > 스냅 추가/제거**- in** > **Active Directory** 사용자 및 컴퓨터 > 사용자.
  2. 서비스 계정 이름을 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.
  3. 전화 접속을 선택한 다음 네트워크 액세스 권한을 거부합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 다음 단계로 PAN-OS 통합 User-ID 에이전트를 사용하여 사용자 매핑을 구성합니다.

# Windows 사용자 ID 에이전트를 사용하여 사용자 매핑 구성

대부분의 경우 대부분의 네트워크 사용자는 모니터링되는 도메인 서비스에 로그인합니다. 이러한 사용자의 경우 Palo Alto Networks User-ID 에이전트는 로그인 이벤트에 대해 서버를 모니터링하고 IP 주소와 사용자 이름 매핑을 수행합니다. User-ID 에이전트를 구성하는 방법은 환경의 크기와 도메인 서버의 위치에 따라 다릅니다. 가장 좋은 방법은 모니터링할 서버 근처에서 User-ID 에이전트를 찾는 것입니다. 이는 사용자 매핑을 위한 대부분의 트래픽이 에이전트와 모니터링되는 서버 사이에서 발생하고 에이전트에서 방화벽으로의 트래픽(마지막 업데이트 이후 사용자 매핑의 델타)만 소량 발생하기 때문입니다.

다음 항목에서는 User-ID 에이전트를 설치 및 구성하는 방법과 에이전트에서 사용자 매핑 정보를 검색하도록 방화벽을 구성하는 방법에 대해 설명합니다.

- Windows 기반 사용자 ID 에이전트 설치
- 사용자 매핑을 위한 Windows 사용자 ID 에이전트 구성

## Windows 기반 사용자 ID 에이전트 설치

다음 절차는 도메인의 구성원 서버에 User-ID 에이전트를 설치하고 필요한 권한으로 서비스 계정을 설정하는 방법을 보여줍니다. 업그레이드하는 경우 설치 프로그램이 자동으로 이전 버전을 제거합니다. 그러나 설치 프로그램을 실행하기 전에 config.xml 파일을 백업하는 것이 좋습니다.

***Windows*** 기반 ***User-ID*** 에이전트 설치를 위한 시스템 요구 사항 및 지원되는 서버 ***OS*** 버전에 대한 정보는 User-ID 에이전트 릴리스 정보 및 Palo Alto Networks 호환성 매트릭스를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** User-ID 에이전트가 사용자 매핑을 수집하기 위해 모니터링할 서비스 및 호스트에 액세스할 수 있도록 전용 Active Directory 서비스 계정을 생성합니다.

User-ID 에이전트에 대한 전용 서비스 계정을 생성하고 Windows User-ID 에이전트에 필요한 권한을 부여하십시오.

1. 로컬 또는 그룹 정책을 구성하여 서비스 계정이 서비스로 로그온할 수 있도록 합니다.

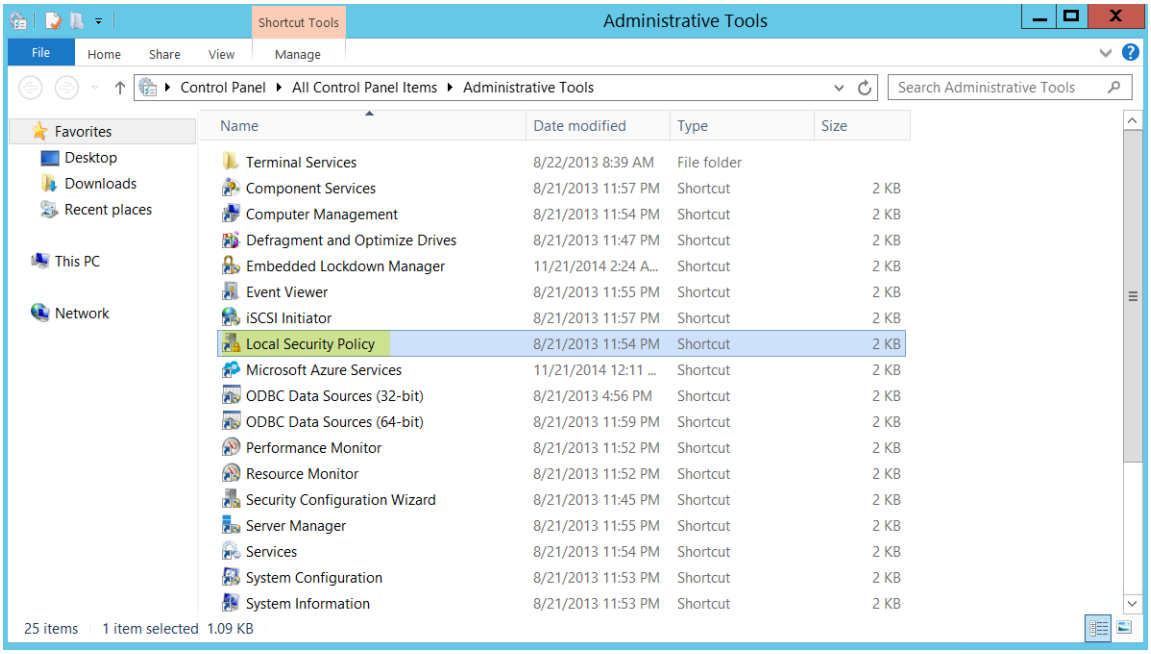
   **1.** 여러 서버에 Windows 기반 User-ID 에이전트를 설치하는 경우 그룹 정책을 구성하려면 에이전트 호스트인 Windows 서버에 대해 그룹 정책 관리 > 기본 도메인 정책 > 컴퓨터 구성 > 정책 > **Windows** 설정 > 보안 설정 > 로컬 정책 > 사용자 권한 할당을 선택합니다.

   **2.** 서비스로 로그온을 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.

   **3.** 서비스 계정 사용자 이름 또는 기본 제공 그룹을 추가합니다(관리자는 기본적으로 이 권한을 가집니다).

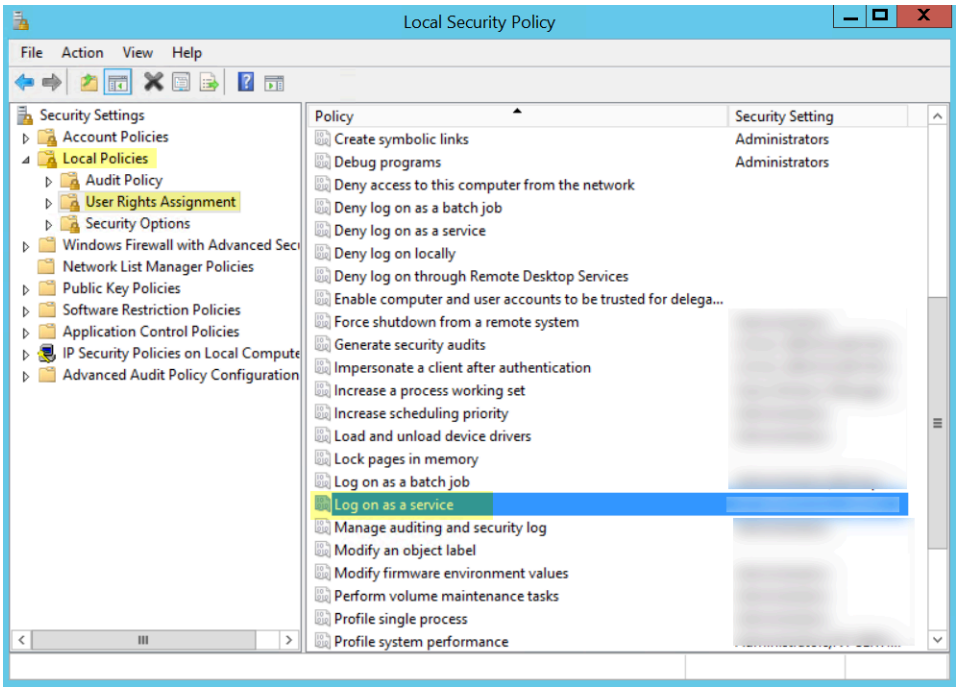
   서비스로 로그온할 수 있는 권한은 에이전트 호스트인 ***Windows*** 서버에서만 로컬로 필요합니다. ***User-ID*** 에이전트를 하나만 사용하는 경우 다음 안내에 따라 에이전트 호스트에서 로컬로 권한을 부여할 수 있습니다.

   **1.** 로컬로 권한을 할당하려면 제어판 > 관리 도구 > 로컬 보안 정책을 선택합니다.

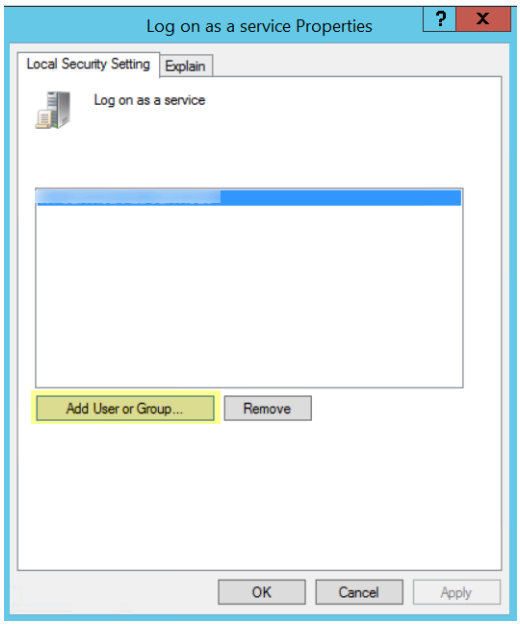



   **2.** 로컬 정책 > 사용자 권한 할당 > 서비스 로그온을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

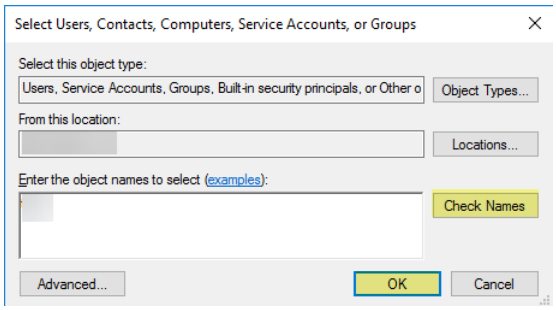



3. 사용자 또는 그룹을 추가하여 서비스 계정을 추가합니다.




4. 서비스 계정 이름을 **도메인\사용자 이름** 형식으로 선택할 개체 이름 입력 입력 필드에 입력하고 확인을 클릭합니다.

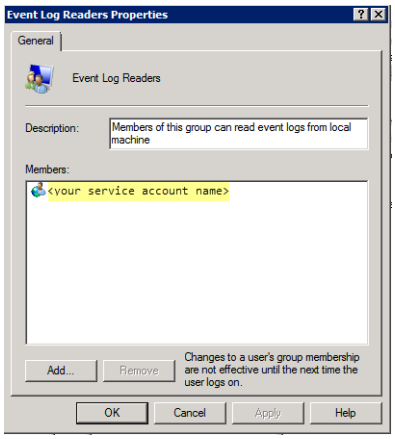

©2023 Palo Alto Networks, Inc.




서비스 계정 이름이 유효한지 확인하려면 이름을 확인하세요.

2. 서버 모니터링을 사용하여 사용자를 식별하려면 이벤트 로그 판독기 기본 제공 그룹에 서비스 계정을 추가하여 보안 로그 이벤트를 읽을 수 있는 권한을 활성화하십시오.

   1. User-ID 에이전트가 읽을 로그가 포함된 도메인 컨트롤러 또는 Exchange 서버 또는 Windows 로그 포워딩에서 이벤트를 수신하는 구성원 서버에서 MMC를 실행하고 Active Directory 사용자 및 컴퓨터 스냅인을 시작합니다.
   2. 도메인의 Builtin 폴더로 이동하고 이벤트 로그 판독기 그룹을 마우스 오른쪽 버튼으로 클릭하고 그룹에 추가를 선택하여 속성 대화 상자를 엽니다.
   3. 추가를 클릭하고 사용하도록 User-ID 서비스를 구성한 서비스 계정의 이름을 입력한 다음 이름 확인을 클릭하여 적절한 개체 이름이 있는지 확인합니다.
   4. 확인을 두 번 클릭하여 설정을 저장합니다.
   5. 기본 제공 이벤트 로그 판독기 그룹이 서비스 계정을 구성원으로 나열하는지 확인합니다.

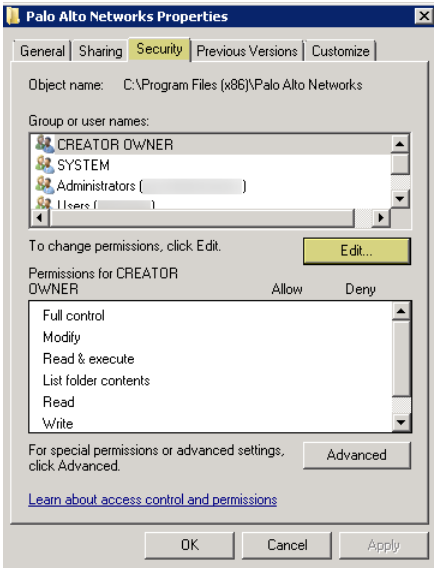



3. 서비스 계정이 에이전트의 설치 폴더에 액세스하여 구성을 읽고 로그를 작성할 수 있도록 설치 폴더에 계정 권한을 할당하십시오.

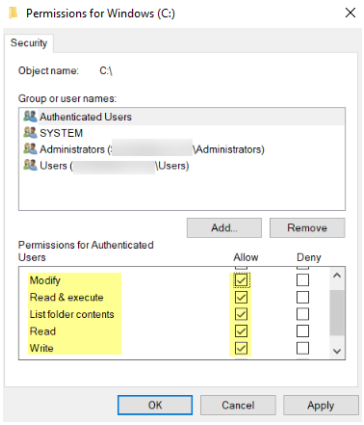
   User-ID 에이전트에 대해 구성한 서비스 계정이 도메인 관리자 또는 User-ID 에이전트 서버 호스트의 로컬 관리자가 아닌 경우에만 이 단계를 수행하면 됩니다.

   1. Windows 탐색기에서 32비트 시스템의 경우 **C:\Program Files(x86)\Palo Alto Networks**로 이동하고 폴더를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
   2. 보안 탭에서 편집을 클릭합니다.


©2023 Palo Alto Networks, Inc.




3. User-ID 에이전트 서비스 계정을 추가하고 수정, 읽기 및 실행, 폴더 내용 나열, 읽기 및 쓰기 권한을 할당한 다음 확인을 클릭하여 계정 설정을 저장합니다.




서비스 계정이 ***User-ID*** 에이전트의 레지스트리 키에 액세스하도록 허용하려면 모든 권한을 허용합니다.

4. User-ID 에이전트 레지스트리 하위 트리에 서비스 계정 권한을 부여합니다.
   1. **`regedt32`**를 실행하고 다음 위치에서 Palo Alto Networks 하위 트리로 이동합니다. `HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`.
   2. Palo Alto Networks 노드를 마우스 오른쪽 버튼으로 클릭하고 권한을 선택합니다.
   3. User-ID 서비스 계정에 모든 권한을 할당한 다음 확인을 클릭하여 설정을 저장합니다.

**STEP 2 |** User-ID 에이전트를 설치할 위치를 결정하십시오.

User-ID 에이전트는 MSRPC(Microsoft 원격 프로시저 호출)를 사용하여 도메인 컨트롤러 및 Exchange 서버 로그를 쿼리합니다. 초기 연결 중에 에이전트는 로그에서 가장 최근의 50,000개 이벤트를 사용자를 매핑하도록 전송합니다. 각 후속 연결에서 에이전트는 도메인 컨트롤러와의 마지막 통

 ©2023 Palo Alto Networks, Inc.

신보다 늦은 타임스탬프로 이벤트를 전송합니다. 따라서 모니터링할 서버가 있는 각 사이트에는 항상 하나 이상의 User-ID 에이전트를 설치하십시오.

- 지원되는 OS 버전 중 하나를 실행하는 시스템에 User-ID 에이전트를 설치해야 합니다. 호환성 매트릭스의 "운영 체제(OS) 호환성 User-ID 에이전트"를 참조하십시오. 시스템은 또한 최소 요구 사항을 충족해야 합니다(User-ID 에이전트 릴리스 정보 참조).
- User-ID 에이전트를 호스팅하는 시스템이 모니터링할 서버와 동일한 도메인의 구성원인지 확인합니다.
- 가장 좋은 방법은 모니터링할 서버 가까이에 User-ID 에이전트를 설치하는 것입니다. User-ID 에이전트와 방화벽 사이보다 User-ID 에이전트와 모니터링되는 서버 사이에 더 많은 트래픽이 있으며, 따라서 모니터링되는 서버에 가까운 에이전트를 찾으면 대역폭 사용이 최적화됩니다.
- 가장 포괄적인 사용자 매핑을 보장하려면 매핑하려는 사용자에 대한 인증을 처리하는 모든 도메인 컨트롤러를 모니터링해야 합니다. 모든 리소스를 효율적으로 모니터링하려면 여러 User-ID 에이전트를 설치해야 할 수 있습니다.
- 자격 증명 감지에 User-ID 에이전트를 사용하는 경우 RODC(읽기 전용 도메인 컨트롤러)에 설치해야 합니다. 이를 위해 별도의 에이전트를 배포하는 것이 가장 좋습니다. RODC에 설치된 User-ID 에이전트를 사용하여 IP 주소를 사용자에게 매핑하지 마십시오. 자격 증명 검색을 위한 User-ID 에이전트 설치 프로그램의 이름은 UaCredInstall64-xxxmsi입니다.

**STEP 3 |** User-ID 에이전트 설치 프로그램을 다운로드합니다.



방화벽에서 실행 중인 ***PAN-OS*** 버전과 동일한 ***User-ID*** 에이전트 버전을 설치합니다. ***PAN-OS*** 버전과 일치하는 ***User-ID*** 에이전트 버전이 없으면 ***PAN-OS*** 버전에 가장 가까운 최신 버전을 설치합니다.

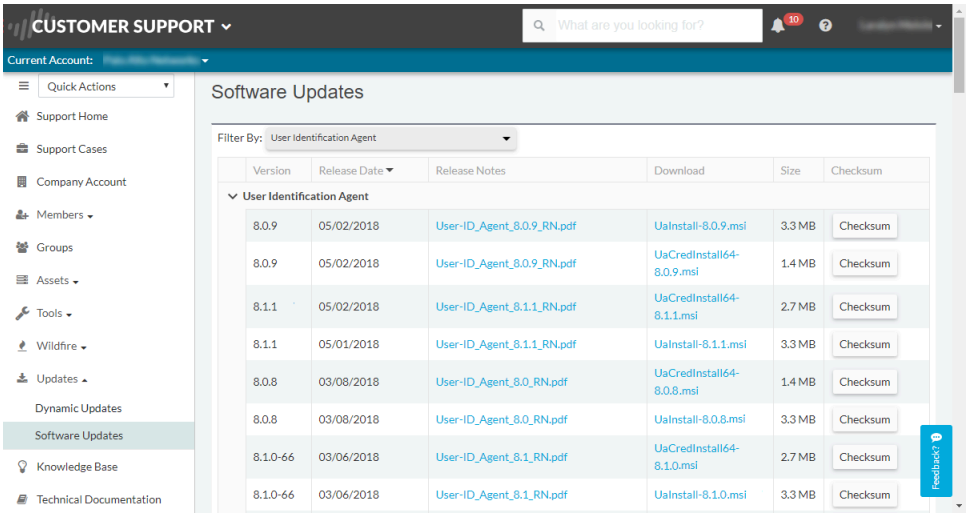
1. Palo Alto Networks 고객 지원 포털에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택합니다.
3. **Filter By**를 **User Identification Agent**로 설정하고 해당 다운로드 열에서 설치하려는 User-ID 에이전트 버전을 선택합니다. 파일 이름은 다음 형식을 사용합니다. `UaInstall-xxxmsi`(여

 ©2023 Palo Alto Networks, Inc.

기서 x는 버전 번호를 나타냄). 예를 들어 10.0 버전의 User-ID 에이전트를 다운로드하려면 **UaInstall-10.0.0-0.msi**를 선택합니다.

자격 증명 감지에 User-ID 에이전트를 사용하는 경우 대신 **UaCredInstall64-xxxmsi** 파일을 다운로드하십시오. 자격 증명 감지에 사용자 ID를 사용하는 경우에만 **UaCredInstall64-xxxmsi**를 다운로드하여 설치하십시오.

4. 에이전트를 설치하려는 시스템에 파일을 저장합니다.




**STEP 4 |** 설치 프로그램을 관리자로 실행합니다.

1. Windows 시작 메뉴를 열고 명령 프롬프트 프로그램을 마우스 오른쪽 버튼으로 클릭한 다음 **Run as administrator**를 선택합니다.
2. 명령줄에서 다운로드한 .msi 파일을 실행합니다. 예를 들어 .msi 파일을 바탕 화면에 저장한 경우 다음을 입력합니다.

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```

3. 설치 프롬프트에 따라 기본 설정을 사용하여 에이전트를 설치합니다. 기본적으로 에이전트는 **C:\Program Files(x86)\Palo Alto Networks**에 설치되지만 다른 위치로 이동할 수 있습니다.
4. 설치가 완료되면 설정 창을 닫습니다.

**STEP 5 |** User-ID Agent 애플리케이션을 관리자로 실행합니다.

Windows 시작 메뉴를 열고 **User-ID Agent** 프로그램을 마우스 오른쪽 버튼으로 클릭하고 관리자 권한으로 실행을 선택합니다.

애플리케이션을 설치하거나 구성 변경 사항을 커밋하거나 애플리케이션을 제거하려면 *User-ID* 에이전트 애플리케이션을 관리자로 실행해야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** (선택 사항) User-ID 에이전트가 로그인하는 데 사용하는 서비스 계정을 변경합니다.

기본적으로 에이전트는 .msi 파일을 설치하는 데 사용되는 관리자 계정을 사용합니다. 계정을 제한된 계정으로 변경하려면:

1. 사용자 식별 > 설정을 선택한 다음 편집을 클릭합니다.
2. 인증 탭을 선택한 다음 **Active Directory**의 사용자 이름 필드에 User-ID 에이전트가 사용할 서비스 계정 이름을 입력합니다.
3. 지정된 계정의 암호를 입력합니다.
4. 서비스 계정 자격 증명을 사용하여 서비스를 다시 시작하려면 User-ID 에이전트 구성에 대한 변경 사항을 커밋합니다.

**STEP 7 |** (선택 사항) Windows User-ID 에이전트와 방화벽 간의 상호 인증을 위해 고유한 인증서를 할당합니다.

1. 다음 방법 중 하나를 사용하여 Windows 사용자 ID 에이전트에 대한 인증서를 가져옵니다. PEM(Privacy Enhanced Mail) 형식의 서버 인증서와 서버 인증서의 암호화된 키를 업로드합니다.
   - 인증서를 생성하고 Windows User-ID 에이전트에 업로드하기 위해 내보냅니다.
   - 엔터프라이즈 CA(인증 기관)에서 인증서를 내보내고 Windows User-ID 에이전트에 업로드합니다.
2. Windows User-ID 에이전트에 서버 인증서를 추가합니다.
   1. Windows User-ID 에이전트에서 서버 인증서를 선택한 다음 추가를 클릭하십시오.
   2. CA에서 받은 인증서 파일의 경로와 이름을 입력하거나 인증서 파일을 찾습니다.
   3. 개인 키 암호를 입력합니다.
   4. 확인을 클릭한 다음 커밋을 클릭합니다.
3. 방화벽에 인증서를 업로드하여 Windows User-ID 에이전트의 ID를 확인하십시오.
4. 클라이언트 디바이스(방화벽 또는 Panorama)에 대한 인증서 프로파일을 구성합니다.
   1. 디바이스 > 인증서 관리 > 인증서 프로파일을 선택합니다.
   2. 인증서 프로파일을 구성합니다.

      ***Windows User-ID*** 에이전트 및 터미널 서버***(TS)***에이전트에 대해 하나의 인증서 프로파일만 할당할 수 있습니다**.** 따라서 인증서 프로파일에는 연결된 사용자 ***ID*** 및 ***TS*** 에이전트에 업로드된 인증서를 발급한 모든 인증 기관이 포함되어야 합니다**.**
5. 방화벽에서 인증서 프로파일을 할당합니다.
   1. 디바이스 > 사용자 식별 > 연결 보안을 선택한 다음 편집 버튼을 클릭합니다.
   2. 이전 단계에서 구성한 사용자 **ID** 인증서 프로파일을 선택합니다.
   3. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** Windows 기반 User-ID 에이전트로 자격 증명 감지 구성.

Windows 기반 User-ID 에이전트를 사용하여 자격 증명 제출을 감지하고 자격 증명 피싱을 방지하려면 Windows 기반 User-ID 에이전트에 User-ID 자격 증명 서비스를 설치해야 합니다. 이 추가 기능은 RODC(읽기 전용 도메인 컨트롤러)에만 설치할 수 있습니다.

## 사용자 매핑을 위한 **Windows** 사용자 **ID** 에이전트 구성

Palo Alto Networks 윈도우 User-ID 에이전트는 네트워크의 서버에 연결하는 Windows 서비스(예: 활성 디렉터리 서버, Microsoft Exchange 서버 및 Novell eDirectory 서버)는 로그인 이벤트에 대한 로그를 모니터링합니다. 에이전트는 이 정보를 사용하여 IP 주소를 사용자 이름에 매핑합니다. Palo Alto Networks 방화벽은 User-ID 에이전트에 연결하여 이 사용자 매핑 정보를 검색하여 IP 주소가 아닌 사용자 이름으로 사용자 활동에 대한 가시성을 구현하고 사용자 및 그룹 기반 보안 적용을 가능하게 합니다.

***User-ID*** 에이전트에서 지원하는 서버 ***OS*** 버전에 대한 자세한 내용은 User-ID 에이전트 릴리스 노트에서 "운영 체제***(OS)*** 호환성 ***User-ID*** 에이전트"를 참조하십시오.

**STEP 1 |** User-ID 에이전트가 모니터링하여 사용자 매핑 정보에 IP 주소를 수집하는 서버를 정의합니다.

User-ID 에이전트는 최대 100개의 서버를 모니터링할 수 있으며, 그중 최대 50개의 서버가 syslog 발신자일 수 있습니다.

필요한 모든 매핑을 수집하려면 ***User-ID*** 에이전트가 로그인 이벤트가 포함된 모든 서버의 보안 로그 파일을 모니터링하려면 사용자가 로그인하는 모든 서버에 연결해야 합니다.

1. Windows 시작 메뉴를 열고 User-ID 에이전트를 선택합니다.
2. 사용자 식별 검색 을 선택합니다.
3. 화면의 서버 섹션에서 추가를 클릭합니다.
4. 모니터링할 서버의 이름 및 서버 주소를 입력합니다. 네트워크 주소는 FQDN 또는 IP 주소일 수 있습니다.
5. 서버 유형(Microsoft Active Directory, Microsoft Exchange, Novell eDirectory 또는 Syslog Sender)을 선택하고 그런 다음 확인을 클릭하여 서버 항목을 저장합니다. 모니터링할 각 서버에 대해 이 단계를 반복합니다.
6. (선택 사항) Windows User-ID 에이전트가 DNS 조회를 사용하여 네트워크에서 도메인 컨트롤러를 자동으로 검색할 수 있도록 하려면 자동 검색을 클릭합니다. Windows User-ID 에이전트가 검색할 새 도메인 컨트롤러가 있는 경우 새 도메인 컨트롤러를 검색할 때마다 자동 검색을 클릭합니다.

   자동 검색은 로컬 도메인에서만 도메인 컨트롤러를 찾습니다. ***Exchange*** 서버, ***eDirectory*** 서버 및 ***syslog*** 발신자를 수동으로 추가해야 합니다.
7. (선택 사항) 방화벽이 매핑 정보를 위해 구성된 서버를 폴링하는 빈도를 조정하려면 사용자 식별설정 및 를 선택합니다. 설정 섹션을 편집합니다. 서버 모니터 탭에서 서버 로그 모니터 주파

 ©2023 Palo Alto Networks, Inc.

수(초) 필드의 값을 수정합니다. 이전 도메인 컨트롤러 또는 대기 시간이 높은 링크가 있는 환경에서 이 필드의 값을 5초로 늘립니다.

서버 세션 읽기 사용 설정이 선택되지 않았는지 확인합니다. 이 설정에서는 ***User-ID*** 에이전트에 모든 사용자 세션을 읽을 수 있도록 서버 운영자 권한이 있는 ***Active Directory*** 계정이 있어야 합니다. 대신 ***syslog*** 또는 ***XML API*** 통합을 사용하여 무선 컨트롤러 및 네트워크 액세스 컨트롤러***(NAC)***와 같은 모든 디바이스 유형 및 운영 체제***(Windows*** 대신***)***에 대한 로그인 및 로그아웃 이벤트를 캡처하는 소스를 모니터링합니다.

8. 확인을 클릭하여 설정을 저장합니다.

**STEP 2 |** Windows User-ID 에이전트가 사용자 ID에 포함하거나 제외해야 하는 하위 네트워크를 지정합니다.

기본적으로 사용자 ID는 모니터링 중인 서버에 액세스하는 모든 사용자를 매핑합니다.

모범 사례로 상담원이 내부 리소스와만 통신하고 권한이 없는 사용자가 매핑되지 않도록 사용자 ***ID***에서 포함하고 제외할 네트워크를 필수 지정합니다. 조직 내부 사용자가 로그인하는 하위 네트워크에서만 사용자 ***ID***를 사용하도록 설정해야 합니다.

1. 사용자 식별 검색 을 선택합니다.
2. 구성된 네트워크 포함/제외 목록에 항목을 추가하고 항목에 대한 이름을 입력하고 네트워크 주소로 하위 네트워크의 IP 주소 범위를 입력합니다.
3. 네트워크를 포함하거나 제외할지의 여부를 선택합니다.
   - 지정된 네트워크 포함 - 지정된 하위 네트워크에만 로그인한 사용자로 사용자 매핑을 제한하려는 경우 이 옵션을 선택합니다. 예를 들어 10.0.0.0/8을 포함하는 경우 에이전트는 해당 하위 네트워크의 사용자를 매핑하고 다른 모든 사용자를 제외합니다. 에이전트가 다른 하위 네트워크에서 사용자를 매핑하려면 다음 단계를 반복하여 목록에 네트워크를 추가해야 합니다.
   - 지정된 네트워크 제외 - 에이전트가 포함을 위해 추가한 하위 네트워크의 하위 집합을 제외하려는 경우에만 이 옵션을 선택합니다. 예를 들어 10.0.0.0/8을 포함하고 10.2.50.0/22를 제외하면 에이전트는 10.2.50.0/22를 제외한 10.0.0.0/8의 모든 하위 네트워크에서 사용자를 매핑하고 10.0.0.0/8 외부의 모든 하위 네트워크를 제외합니다.

     포함 프로파일을 추가하지 않고 제외 프로파일을 추가하는 경우 ***User-ID*** 에이전트는 추가한 프로파일뿐만 아니라 모든 하위 네트워크를 제외합니다.
4. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** (선택사항) Novell eDirectory 서버에 연결할 에이전트를 구성한 경우 에이전트가 디렉터리 검색 방법을 지정해야 합니다.

1. 사용자 식별 설정 을 선택하고 창의 설정 섹션에서 수정을 클릭합니다.
2. eDirectory 탭을 선택한 후 다음 필드를 완료합니다.
   - 검색 기본 - 에이전트 쿼리의 시작점 또는 루트 컨텍스트(예: `dc=domain1,dc=예제, dc=com`).
   - 고유 이름 바인딩 - 예를 들어 `cn=admin, ou=IT, dc=domain1, dc=example, dc=com` 등 디렉토리에 바인딩하는 데 사용할 계정입니다.
   - 바인딩 암호 - 바인딩 계정 암호입니다. 에이전트는 구성 파일에 암호화된 암호를 저장합니다.
   - 검색 필터 - 사용자 항목에 대한 검색 쿼리(기본값은 `objectClass=Person`)입니다.
   - 서버 도메인 프리픽스 - 사용자를 고유하게 식별하는 프리픽스입니다. 두 개의 서로 다른 디렉터리에서 이름이 같은 다른 사용자와 같이 이름 공간이 겹치는 경우에만 필요합니다.
   - SSL 사용 - 전자 디렉토리 바인딩에 SSL을 사용하도록 체크박스를 선택합니다.
   - 서버 인증서 확인 - SSL을 사용할 때 eDirectory 서버 인증서를 확인하기 위해 체크박스를 선택합니다.

**STEP 4 |** (적극 권장) 클라이언트 프로빙을 사용하지 않도록 설정합니다.

*Palo Alto Networks*는 보안이 높은 네트워크에서 클라이언트 프로빙을 비활성화하는 것이 좋습니다. 클라이언트 프로빙은 올바르게 구성되지 않으면 보안 위협을 야기할 수 있습니다. 자세한 내용은 클라이언트 프로빙을 참조하십시오.

1. 클라이언트 검사 탭에서 WMI 검사 활성화 확인란이 활성화되어 있으면 선택을 취소합니다.
2. 활성화된 경우 NetBIOS 프로빙 체크박스를 선택 해제합니다.

   *Palo Alto Networks*는 도메인 컨트롤러 또는 Syslog 또는 XML API와의 통합과 같은 독립되고 신뢰할 수 있는 소스에서 사용자 매핑 정보를 수집하여 모든 디바이스 유형 또는 운영 체제에서 사용자 매핑 정보를 안전하게 캡처할 것을 적극 권장합니다.

   클라이언트 프로빙을 사용하도록 설정해야 하는 경우 ***WMI*** 프로빙 사용 체크박스과 클라이언트 프로빙 탭에서 선택합니다. 이 메서드의 잠재적인 보안 위험으로 인해 방화벽이 다른 방법을 사용하여 사용자 매핑을 가져올 수 없는 경우에만 ***NetBIOS*** 프로빙 체크박스를 선택합니다. 그런 다음 각 검증된 클라이언트에 대한 ***Windows*** 방화벽에 원격 관리 예외를 추가하여 ***Windows*** 방화벽이 클라이언트 검증을 허용할 수 있도록 합니다. 각 프로브 클라이언트 ***PC***는 ***Windows*** 방화벽에서 포트 ***139***를 허용해야 하며 파일 및 프린터 공유 서비스를 사용하도록 설정해야 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 구성을 저장합니다.

확인을 클릭하여 User-ID 에이전트 설정 설정을 저장한 다음 커밋을 클릭하여 User-ID 에이전트를 다시 시작하고 새 설정을 로드합니다.

**STEP 6 |** (선택사항) 키오스크 계정과 같은 IP 주소-사용자 이름 매핑을 제공할 필요가 없는 사용자 집합을 정의합니다.

타이틀 **ignore_user_list**를 사용하여 에이전트 호스트의 텍스트 문서로 **ignore-user**을 저장하고 .txt 파일 확장을 사용하여 에이전트가 설치된 도메인 서버의 User-ID 에이전트 폴더에 저장합니다.

무시할 사용자 계정을 나열하며 목록에 추가할 수 있는 계정 수에는 제한이 없습니다. 각 사용자 계정 이름은 별도의 줄에 있어야 합니다. 예:

```
SPAdmin SPInstall TFSReport
```

별표를 와일드카드 문자로 사용하여 여러 사용자 이름과 일치하지만 항목의 마지막 문자로만 사용할 수 있습니다. 예를 들어 **corpdomain\it-admin***은 사용자 이름이 **관리자** 문자열로 시작하는 **corpdomain** 도메인의 모든 관리자와 일치합니다. 또한 **ignore-user** 목록을 사용하여 인증 포털을 사용하여 인증하려는 사용자를 식별할 수도 있습니다.

사용자 무시 목록에 항목을 추가한 후 중지하고 서비스에 대한 연결을 다시 시작해야 합니다.

**STEP 7 |** User-ID 에이전트에 연결할 방화벽을 구성합니다.

방화벽은 사용자 ***ID*** 자격 증명 서비스 추가 기능을 사용하여 회사 자격 증명 제출을 검색하는 ***Windows*** 기반 ***User-ID*** 에이전트 하나만 연결할 수 있습니다. 자격 증명 피싱 방지를 위해 이 서비스를 사용하는 방법에 대한 자세한 내용은 Windows 기반 User-ID 에이전트를 사용하여 자격 증명 검색 구성을 참조하십시오.

사용자 매핑을 수신하려면 User-ID 에이전트에 연결하려는 각 방화벽에서 다음 단계를 완료합니다.

1. 디바이스 데이터 재배포에이전트 를 선택하고 추가를 클릭합니다.
2. 에이전트의 이름을 입력합니다.
3. 호스트 및 포트를 사용하여에이전트를 추가합니다.
4. User-ID 에이전트가 설치된 Windows 호스트의 IP 주소를 입력합니다.
5. 에이전트가 사용자 매핑 요청을 수신할 포트 번호(1-65535)를 입력합니다. 이 값은 User-ID 에이전트에서 구성된 값과 일치해야 합니다. 기본적으로 포트는 방화벽과 최신 버전의 User-ID 에이전트에서 5007로 설정됩니다. 그러나 일부 이전 User-ID 에이전트 버전은 포트 2010을 기본값으로 사용합니다.
6. 데이터 유형으로 IP 사용자 매핑을 선택합니다.
7. 구성이 활성화됨인지 확인한 다음 확인을 클릭합니다.
8. 변경 사항을 커밋합니다.
9. 연결됨 상태가 연결됨(녹색 표시등)으로 표시되는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** User-ID 에이전트가 IP 주소를 사용자 이름으로 성공적으로 매핑하고 방화벽이 에이전트에 연결할 수 있는지 확인합니다.

1. User-ID 에이전트를 실행하고 사용자 식별을 선택합니다.
2. 에이전트 상태에 에이전트 실행 중이 표시되는지 확인합니다. 에이전트가 실행되고 있지 않으면 시작을 클릭합니다.
3. User-ID 에이전트가 모니터링되는 서버에 연결할 수 있는지 확인하려면 각 서버에 대한 상태가 연결되어 있는지 확인합니다.
4. 방화벽이 User-ID 에이전트에 연결할 수 있는지 확인하려면 연결된 각 디바이스에 대한 상태가 연결되어 있는지 확인합니다.
5. User-ID 에이전트가 IP 주소를 사용자 이름으로 매핑하고 있는지 확인하려면 모니터링을 선택한 다음 매핑 테이블이 채워졌는지 확인합니다. 특정 사용자를 검색하거나 목록에서 사용자 매핑 삭제를 수행할 수도 있습니다.

## PAN-OS 통합 사용자 ID 에이전트를 사용하여 사용자 매핑 구성

다음 절차는 IP 주소-사용자 이름 매핑을 위해 방화벽에서 PAN-OS® 통합 User-ID™ 에이전트를 구성하는 방법을 설명합니다. 통합 User-ID 에이전트는 NetBIOS 클라이언트 프로빙(WMI 프로빙 지원)을 제외하고 Windows 기반 에이전트와 동일한 작업을 수행합니다.

**STEP 1 |** 사용자 매핑 정보를 수집하기 위해 방화벽이 모니터링할 서비스 및 호스트에 액세스하려면 User-ID 에이전트에 대한 Active Directory 서비스 계정을 생성합니다.

User-ID 에이전트에 대한 전용 서비스 계정을 생성합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽이 사용자 매핑 정보를 수집하기 위해 모니터링할 서버를 정의합니다.

방화벽당 최대 100개의 모니터링되는 서버 내에서 단일 가상 시스템에 대해 50개 이하의 syslog 발신자를 정의할 수 있습니다.

필요한 모든 매핑을 수집하려면 방화벽이 로그인 이벤트가 포함된 모든 서버의 보안 로그 파일을 모니터링할 수 있도록 사용자가 로그인하는 모든 서버에 방화벽을 연결해야 합니다.

1. 디바이스 > 사용자 식별 > 사용자 매핑을 선택합니다.
2. 서버를 추가합니다(서버 모니터링 섹션).
3. 서버를 식별할 이름을 입력합니다.
4. 서버 유형을 선택합니다.
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - 시스템 로그 발신자
5. (Microsoft Active Directory 및 Microsoft Exchange만 해당) 서버의 보안 로그 및 세션 정보를 모니터링하는 데 사용할 전송 프로토콜을 선택합니다.
   - **WMI** - 방화벽과 모니터링되는 서버는 WMI(Windows Management Instrumentation)를 사용하여 통신합니다.
   - **WinRM-HTTP** - 방화벽과 모니터링되는 서버는 상호 인증에 Kerberos를 사용하고 모니터링되는 서버는 협상된 Kerberos 세션 키를 사용하여 방화벽과의 통신을 암호화합니다.
   - **WinRM-HTTPS** - 방화벽과 모니터링되는 서버는 HTTPS를 사용하여 통신하고 기본 인증을 사용하거나 Kerberos를 상호 인증에 사용합니다.

   Windows 원격 관리(WinRM) 옵션을 선택하는 경우 WinRM을 사용하여 서버 모니터링 구성을(를) 해야 합니다.
6. (Microsoft Active Directory, Microsoft Exchange 및 Novell eDirectory만) 서버의 네트워크 주소를 입력합니다.

   Kerberos와 함께 WinRM을 사용하는 경우 ***FDQN(***정규화된 도메인 이름***)***을 입력해야 합니다. 기본 인증으로 WinRM을 사용하거나 ***WMI***를 사용하여 서버를 모니터링하려는 경우 ***IP*** 주소 또는 ***FQDN***을 입력할 수 있습니다.

   ***WMI***를 사용하여 서버를 모니터링하려면 ***IP*** 주소, 서비스 계정 이름***(***모든 서버 모니터링이 동일한 도메인에 있는 경우***)*** 또는 ***FQDN(***정규화된 도메인 이름***)***을 지정합니다. ***FQDN***을 지정하는 경우 ***FQDN\sAMAccountName*** 형식 대신***(DLN)\sAMAccountName*** 형식의 하위 로그온 이름을 사용하십시오. 예를 들어 ***example.com\user.services***가 아닌 ***example\user.services***를 사용하십시오. ***FQDN***을 지정하면 방화벽은 ***WMI***를 지원하지 않는 ***Kerberos***를 사용하여 인증을 시도합니다.


©2023 Palo Alto Networks, Inc.

7. (Syslog Sender만) 서버 **Type**으로 **Syslog Sender**를 선택하면 PAN-OS 통합 사용자 ID 에이전트를 Syslog 수신기로 구성.
8. (Novell eDirectory만) 선택한 서버 프로파일이 활성화됨인지 확인하고 확인을 클릭합니다.
9. (선택사항) DNS 조회를 사용하여 네트워크에서 도메인 컨트롤러를 자동으로 검색하도록 방화벽을 구성합니다.

   자동 검색 기능은 도메인 컨트롤러 전용입니다. 모니터링할 ***Exchange*** 서버 또는 ***eDirectory*** 서버를 수동으로 추가해야 합니다.

**STEP 3 |** (선택 사항) 방화벽이 매핑 정보에 대해 Windows 서버를 폴링하는 빈도를 지정합니다. 이것은 마지막 쿼리의 끝과 다음 쿼리의 시작 사이에 해당하는 인터벌입니다.

도메인 컨트롤러가 많은 요청을 처리하는 경우 쿼리 간의 지연이 지정된 값을 초과할 수 있습니다.

1. **Palo Alto Networks** 사용자 **ID** 에이전트 설정을 편집합니다.
2. 서버 모니터 탭을 선택하고 서버 로그 모니터 빈도를 초 단위로 지정합니다(범위는 1~3,600, 기본값은 2). 이전 도메인 컨트롤러 또는 대기 시간이 긴 링크가 있는 환경에서는 이 빈도를 최소 5초로 설정합니다.

   세션 활성화 옵션이 활성화되어 있지 않은지 확인하십시오. 이 옵션을 사용하려면 ***User-ID*** 에이전트에 서버 운영자 권한이 있는 ***Active Directory*** 계정이 있어야 모든 사용자 세션을 읽을 수 있습니다. 대신 ***Syslog*** 또는 ***XML API*** 통합을 사용하여 무선 컨트롤러 및 ***NAC(***네트워크 액세스 제어***)*** 디바이스와 같은 모든 디바이스 유형 및 운영 체제***(Windows***만 아님***)***에 대한 로그인 및 로그아웃 이벤트를 캡처하는 소스를 모니터링하십시오.
3. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 4 |** PAN-OS 통합 User-ID 에이전트가 사용자 매핑에 포함하거나 제외해야 하는 하위 네트워크를 지정합니다.

기본적으로 사용자 ID는 모니터링 중인 서버에 액세스하는 모든 사용자를 매핑합니다.

가장 좋은 방법은 에이전트가 내부 리소스와만 통신하고 권한이 없는 사용자가 매핑되는 것을 방지하기 위해 항상 포함할 네트워크와 선택적으로 ***User-ID***에서 제외할 네트워크를 지정하는 것입니다. 조직 내부의 사용자가 로그인하는 하위 네트워크에서만 사용자 매핑을 활성화해야 합니다.

1. 디바이스 > 사용자 식별 > 사용자 매핑을 선택합니다.
2. 네트워크 포함/제외에 항목을 추가하고 항목의 이름을 입력합니다. 항목이 활성화됨인지 확인합니다.
3. 네트워크 주소를 입력한 다음 포함할지 제외할지 선택합니다.
   - 포함 - 지정된 하위 네트워크에 로그인한 사용자에게만 사용자 매핑을 제한하려면 이 옵션을 선택합니다. 예를 들어 10.0.0.0/8을 포함하는 경우 에이전트는 해당 하위 네트워크의 사용자를 매핑하고 다른 모든 사용자를 제외합니다. 에이전트가 다른 하위 네트워크에서 사용자를 매핑하려면 다음 단계를 반복하여 목록에 네트워크를 추가해야 합니다.

 ©2023 Palo Alto Networks, Inc.

- 제외 - 포함하기 위해 추가한 하위 네트워크의 하위 집합을 제외하도록 에이전트를 구성하려면 이 옵션을 선택합니다. 예를 들어 10.0.0.0/8을 포함하고 10.2.50.0/22를 제외하면 에이전트는 10.2.50.0/22를 제외한 10.0.0.0/8의 모든 하위 네트워크에서 사용자를 매핑하고 10.0.0.0/8 외부의 모든 하위 네트워크를 제외합니다.

  포함 프로파일을 추가하지 않고 제외 프로파일을 추가하는 경우 ***User-ID*** 에이전트는 추가한 프로파일뿐만 아니라 모든 하위 네트워크를 제외합니다.

4. 확인을 클릭합니다.

**STEP 5 |** 방화벽이 Windows 리소스에 액세스하는 데 사용할 계정에 대한 도메인 자격 증명을 설정합니다. 이는 WMI 검색뿐만 아니라 Exchange 서버 및 도메인 컨트롤러를 모니터링하는 데 필요합니다.

1. **Palo Alto Networks** 사용자 **ID** 에이전트 설정을 편집합니다.
2. 서버 모니터 계정 탭을 선택하고 User-ID 에이전트가 사용할 서비스 계정의 사용자 이름 및 암호를 입력합니다. 클라이언트를 조사하고 서버를 모니터링합니다. **domain\username**구문을 사용하여 사용자 이름을 입력합니다.
3. WinRM을 사용하여 서버를 모니터링하는 경우 모니터링 중인 서버를 인증하도록 방화벽을 구성합니다.
   - 기본 인증으로 WinRM을 사용하려면 서버에서 WinRM을 활성화하고 기본 인증을 구성하고 서비스 계정 도메인의 **DNS** 이름을 지정합니다.
   - Kerberos와 함께 WinRM을 사용하려면 아직 구성하지 않은 경우 Kerberos 서버 프로파일을 구성한 다음 **Kerberos** 서버 프로파일을 선택합니다.

**STEP 6 |** (선택 사항, 권장하지 않음) WMI 검색을 구성합니다(PAN-OS 통합 User-ID 에이전트는 NetBIOS 검색을 지원하지 않음).

보안 수준이 높은 네트워크에서는 ***WMI*** 검색을 활성화하지 마십시오. 클라이언트 프로빙은 많은 양의 네트워크 트래픽을 생성할 수 있으며 잘못 구성되면 보안에 위협이 될 수 있습니다.

1. 클라이언트 검사 탭에서 검사 활성화.
2. (선택 사항) 마지막 프로브 요청의 끝과 다음 요청의 시작 사이의 간격(분)을 정의하려면 프로브 간격을 지정하십시오.

   필요한 경우 User-ID 에이전트가 학습된 모든 IP 주소를 조사하기에 충분한 시간을 갖도록 값을 늘립니다(범위는 1~1440, 기본값은 20).

   요청 로드가 높으면 관찰된 요청 간의 지연이 지정된 간격을 크게 초과할 수 있습니다.

3. 확인을 클릭합니다.
4. 검색된 각 클라이언트에 대해 Windows 방화벽에 원격 관리 예외를 추가하여 Windows 방화벽이 클라이언트 검색을 허용하는지 확인하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** (선택 사항) 키오스크 계정과 같이 IP 주소-사용자 이름 매핑이 필요하지 않은 사용자 계정 집합을 정의합니다.

> 클라이언트가 아닌 ***User-ID*** 에이전트인 방화벽에 사용자 무시 목록을 정의합니다. 클라이언트 방화벽에서 사용자 무시 목록을 정의하는 경우 목록의 사용자는 재배포 중에 계속 매핑됩니다.

사용자 목록 무시 탭에서 사용자 매핑에서 제외할 각 사용자 이름을 추가합니다. 사용자 무시 목록을 사용하여 인증 포털을 사용하여 강제로 인증하려는 사용자를 식별할 수도 있습니다. 별표를 와일드카드 문자로 사용하여 여러 사용자 이름과 일치시킬 수 있지만 항목의 마지막 문자로만 사용할 수 있습니다. 예를 들어 **corpdomain\it-admin***은 사용자 이름이 **it#admin** 문자열로 시작하는 **corpdomain** 도메인의 모든 관리자와 일치합니다. 사용자 매핑에서 제외할 항목을 최대 5,000개까지 추가할 수 있습니다.

**STEP 8 |** 구성 변경을 활성화하십시오.

확인 및 커밋을 클릭합니다.

**STEP 9 |** 구성을 확인합니다.

1. 방화벽 CLI에 액세스합니다.
2. 다음 조작 명령을 입력하십시오.

```
> show user server-monitor state all
```

3. 웹 인터페이스의 디바이스 > 사용자 식별 > 사용자 매핑 탭에서 서버 모니터링을 위해 구성한 각 서버의 상태가 **연결됨**인지 확인합니다.

## WinRM을 사용하여 서버 모니터링 구성

WinRM(Windows 원격 관리)을 사용하여 서버를 모니터링하도록 PAN-OS 통합 User-ID 에이전트를 구성할 수 있습니다. WinRM 프로토콜을 사용하면 서버 이벤트를 모니터링하여 사용자 이벤트를 IP 주소에 매핑할 때 속도, 효율성 및 보안이 향상됩니다. PAN-OS 통합 User-ID 에이전트는 Windows Server 2012 Active Directory 및 Microsoft Exchange Server 2012 이상의 버전에서 WinRM 프로토콜을 지원합니다.

WinRM을 사용하여 서버 모니터링을 구성하는 세 가지 방법이 있습니다.

- 기본 인증을 사용하여 HTTPS를 통한 WinRM 구성 - 방화벽은 User-ID 에이전트에 대한 서비스 계정의 사용자 이름과 암호를 사용하여 모니터링되는 서버를 인증하고 방화벽은 사용자-ID 인증서 프로파일을 사용하여 모니터링되는 서버를 인증합니다.
- Kerberos를 사용하여 HTTP를 통한 WinRM 구성 - 방화벽과 모니터링되는 서버는 상호 인증에 Kerberos를 사용하고 모니터링되는 서버는 협상된 Kerberos 세션 키를 사용하여 방화벽과의 통신을 암호화합니다.
- Kerberos를 사용하여 HTTPS를 통해 WinRM 구성 - 방화벽과 모니터링되는 서버는 HTTPS를 사용하여 통신하고 Kerberos를 상호 인증에 사용합니다.

 ©2023 Palo Alto Networks, Inc.

## 기본 인증을 사용하여 HTTPS를 통한 WinRM 구성

기본 인증과 함께 HTTPS를 사용하도록 WinRM을 구성하면 방화벽은 SSL을 사용하는 보안 터널에서 서비스 계정에 대한 자격 증명을 전송합니다.

**STEP 1 |** 모니터링하려는 서버에 대한 원격 관리 사용자 및 CIMV2 권한으로 서비스 계정을 구성합니다.

**STEP 2 |** 모니터링 중인 Windows 서버에서 Windows 서버가 WinRM과 함께 사용할 수 있도록 인증서에서 지문을 얻고 WinRM을 활성화합니다.

관리자 권한이 있는 계정을 사용하여 모니터링하려는 서버에서 *WinRM*을 구성해야 합니다. 보안을 위한 모범 사례로 이 계정은 *1*단계의 서비스 계정과 동일한 계정이 아니어야 합니다.

1. 인증서가 로컬 컴퓨터 인증서 저장소(인증서(로컬 컴퓨터) > 개인 > 인증서)에 설치되었는지 확인합니다.

   로컬 컴퓨터 인증서 저장소가 표시되지 않으면 Microsoft 관리 콘솔을 시작하고(**Run** > **MMC** > 시작) 인증서 스냅인을 추가합니다(파일 > 스냅인 > 인증서 > 추가/제거 > **AddComputer** > 계정 > **NextFinish** 추가).
2. 인증서를 열고 일반 > 세부정보 > 표시**: <All>**를 선택합니다.
3. 지문을 선택한 다음 복사합니다.
4. 방화벽이 WinRM을 사용하여 Windows 서버에 연결할 수 있도록 하려면 **`winrm quickconfig`** 명령을 입력합니다.
5. **y**를 입력하여 변경 사항을 확인한 다음 출력에 `WinRM 서비스 시작됨`이 표시되는지 확인합니다.

   WinRM이 활성화된 경우 출력에 `WinRM 서비스가 이미 이 시스템에서 실행 중`이라고 표시됩니다. 추가로 필요한 구성 변경을 확인하라는 메시지가 표시됩니다.
6. WinRM이 HTTPS를 사용하여 통신하는지 확인하려면 **`winrm enumerate winrm/config/listener`** 명령을 입력하고 출력에 `Transport = HTTPS`가 표시되는지 확인합니다.

   기본적으로 WinRM/HTTPS는 포트 5986을 사용합니다.
7. Windows 서버 명령 프롬프트에서 **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`** 명령을 입력합니다. 여기서 *hostname*은 호스트 이름입니다. Windows 서버 및 인증서 지문은 인증서에서 복사한 값입니다.

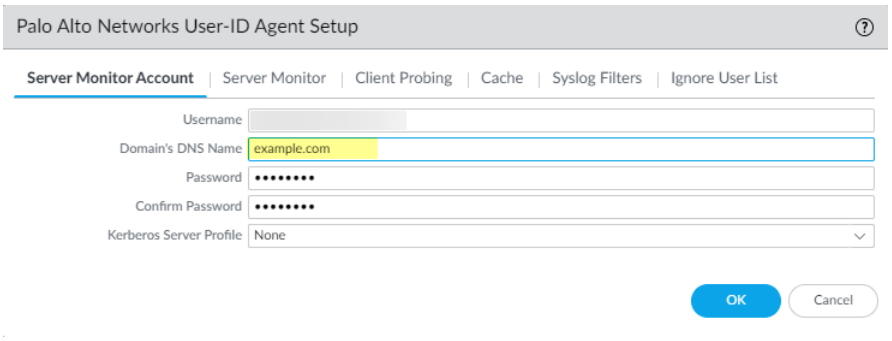
   명령 프롬프트*(Powershell* 아님*)*를 사용하고 인증서 지문에서 공백을 제거하여 *WinRM*이 인증서의 유효성을 검사할 수 있도록 합니다.
8. Windows 서버 명령 프롬프트에서 다음 명령을 입력합니다.

   ```
   c:\> winrm set winrm/config/client/auth @{Basic="true"}
   ```
9. **`winrm get winrm/config/service/Auth`** 명령을 입력하고 `Basic = true`인지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** PAN-OS 통합 User-ID 에이전트와 모니터링되는 서버 간의 기본 인증을 활성화합니다.

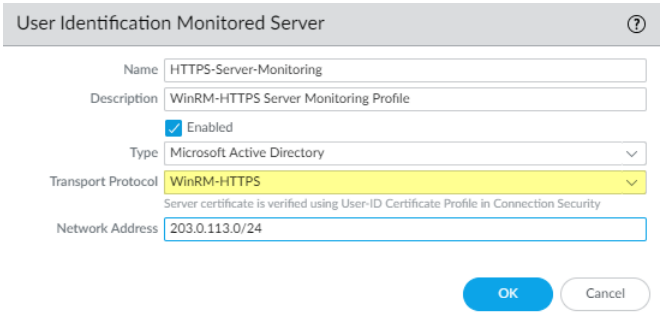
1. 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks** 사용자 **ID** 에이전트 설정 > 서버 모니터 계정을 선택합니다.
2. **도메인\사용자 이름** 형식으로 User-ID 에이전트가 서버를 모니터링하는 데 사용할 서비스 계정의 사용자 이름을 입력합니다.
3. 서버 모니터 계정의 도메인 **DNS** 이름을 입력합니다.




4. 서비스 계정의 암호 및 암호 확인을 입력합니다.
5. 확인을 클릭합니다.

**STEP 4 |** PAN-OS 통합 User-ID 에이전트에 대한 서버 모니터링을 구성합니다.

1. Microsoft 서버 유형(**Microsoft Active Directory** 또는 **Microsoft Exchange**)을 선택합니다.
2. HTTPS를 통한 WinRM(Windows 원격 관리)을 사용하여 서버 보안 로그 및 세션 정보를 모니터링하려면 **Win-RM-HTTPS**를 전송 프로토콜로 선택합니다.

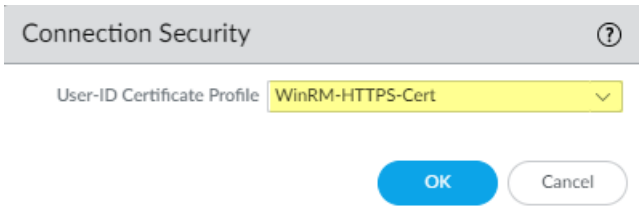



3. 서버의 IP 주소 또는 FQDN 네트워크 주소를 입력합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** PAN-OS 통합 User-ID 에이전트가 WinRM-HTTPS를 사용하여 모니터링되는 서버와 통신할 수 있도록 하려면 Windows 서버가 WinRM에 사용하는 서비스 인증서의 루트 인증서를 방화벽으로 성공적으로 가져왔는지 확인하고 User-ID 인증서 프로파일이 포함된 인증서를 다음과 연결합니다.

1. 디바이스 > 사용자 식별 > 연결 보안을 선택합니다.
2. 편집을 클릭합니다.
3. 사용자 **ID** 인증서 프로파일에 사용할 Windows 서버 인증서를 선택합니다.




4. 확인을 클릭합니다.

**STEP 6 |** 변경 사항을 커밋합니다.

**STEP 7 |** 모니터링되는 각 서버의 상태가 연결됨(디바이스 > 사용자 식별 > 사용자 매핑)인지 확인합니다.

## Kerberos를 사용하여 HTTP를 통한 WinRM 구성

Kerberos를 사용하여 HTTP를 통한 WinRM을 구성하면 방화벽과 모니터링되는 서버는 상호 인증에 Kerberos를 사용하고 모니터링되는 서버는 협상된 Kerberos 세션 키를 사용하여 방화벽과의 통신을 암호화합니다.

*Kerberos*가 있는 *WinRM*은 *aes128-cts-hmac-sha1-96* 및 *aes256-cts-hmac-sha1-96* 암호를 지원합니다. 모니터링하려는 서버가 *RC4*를 사용하는 경우 모니터링하려는 서버의 레지스트리 설정에서 *Windows* 업데이트를 다운로드하고 *Kerberos*용 *RC4*를 비활성화해야 합니다.

**STEP 1 |** 모니터링하려는 서버에 대한 원격 관리 사용자 및 CIMV2 권한으로 서비스 계정을 구성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 모니터링 중인 Windows 서버에서 WinRM이 활성화되어 있는지 확인합니다.

관리자 권한이 있는 계정을 사용하여 모니터링하려는 서버에서 ***WinRM***을 구성해야 합니다. 보안을 위한 모범 사례로 이 계정은 ***1***단계의 서비스 계정과 동일한 계정이 아니어야 합니다.

1. 방화벽이 WinRM을 사용하여 Windows 서버에 연결할 수 있도록 하려면 **`winrm quickconfig`** 명령을 입력합니다.
2. **`y`**를 입력하여 변경 사항을 확인한 다음 출력에 `WinRM 서비스 시작됨`이 표시되는지 확인합니다.

   WinRM이 활성화된 경우 출력에 `WinRM 서비스가 이미 이 시스템에서 실행 중`이라고 표시됩니다. 추가로 필요한 구성 변경을 확인하라는 메시지가 표시됩니다.
3. WinRM이 HTTP를 사용하여 통신하는지 확인하려면 **`winrm enumerate winrm/config/listener`** 명령을 입력하고 출력에 `Transport = HTTP`가 표시되는지 확인합니다.

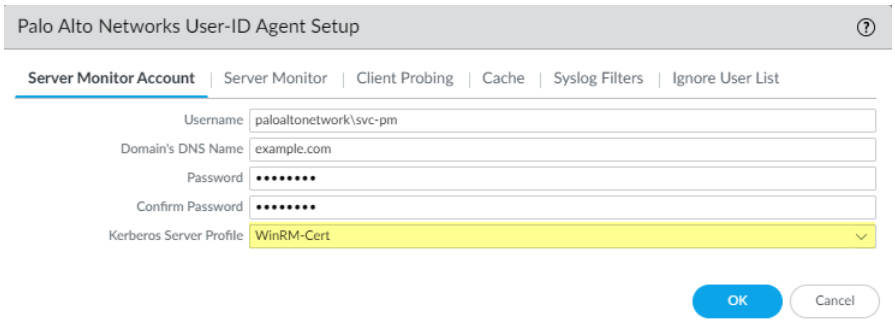
   기본적으로 WinRM/HTTP는 포트 5985를 사용합니다.
4. 명령 **`winrm get winrm/config/service/Auth`**을 입력하고 `Kerberos = true`인지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** PAN-OS 통합 User-ID 에이전트와 모니터링되는 서버가 Kerberos를 사용하여 인증할 수 있도록 합니다.

1. 초기 구성 중에 그렇게 하지 않은 경우 성공적인 Kerberos 협상을 위해 NTP(날짜 및 시간) 설정을 구성합니다.
2. 방화벽에서 Kerberos 서버 프로파일을 구성하여 서버에 인증하여 보안 로그 및 세션 정보를 모니터링합니다.
3. 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks** 사용자 **ID** 에이전트 설정 > 서버 모니터 계정을 선택합니다.
4. **도메인\사용자 이름** 형식으로 User-ID 에이전트가 서버를 모니터링하는 데 사용할 서비스 계정의 사용자 이름을 입력합니다.
5. 서버 모니터 계정의 도메인 **DNS** 이름을 입력합니다.

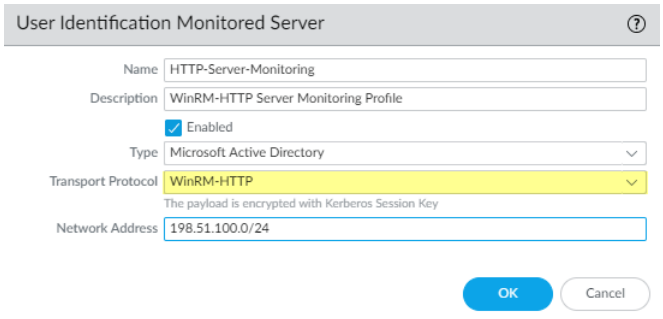
   Kerberos는 도메인 이름을 사용하여 서비스 계정을 찾습니다.
6. 서비스 계정의 암호 및 암호 확인을 입력합니다.
7. 3.2단계에서 구성한 **Kerberos** 서버 프로파일을 선택합니다.




8. 확인을 클릭합니다.

**STEP 4 |** PAN-OS 통합 User-ID 에이전트에 대한 서버 모니터링을 구성합니다.

1. Microsoft 서버 유형(**Microsoft Active Directory** 또는 **Microsoft Exchange**)을 구성합니다.
2. **WinRM-HTTP**를 전송 프로토콜로 선택하여 HTTP를 통한 WinRM(Windows 원격 관리)을 사용하여 서버 보안 로그 및 세션 정보를 모니터링합니다.




3. 서버의 FQDN 네트워크 주소를 입력합니다.

   Kerberos를 사용하는 경우 네트워크 주소는 FDQN(정규화된 도메인 이름)이어야 합니다.

**STEP 5 |** 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 모니터링되는 각 서버의 상태가 연결됨(디바이스 > 사용자 식별 > 사용자 매핑)인지 확인합니다.

## Kerberos를 사용하여 HTTPS를 통해 WinRM 구성

Kerberos를 사용하여 HTTPS를 통해 WinRM을 구성하면 방화벽과 모니터링되는 서버가 HTTPS를 사용하여 통신하고 Kerberos를 상호 인증에 사용합니다.

*Kerberos*가 있는 *WinRM*은 *aes128-cts-hmac-sha1-96* 및 *aes256-cts-hmac-sha1-96* 암호를 지원합니다. 모니터링하려는 서버가 *RC4*를 사용하는 경우 모니터링하려는 서버의 레지스트리 설정에서 *Windows* 업데이트를 다운로드하고 *Kerberos*용 *RC4*를 비활성화해야 합니다.

**STEP 1 |** 모니터링하려는 서버에 대한 원격 관리 사용자 및 CIMV2 권한으로 서비스 계정을 구성합니다.

**STEP 2 |** 모니터링 중인 Windows 서버에서 Windows 서버가 WinRM과 함께 사용할 수 있도록 인증서에서 지문을 얻고 WinRM을 활성화합니다.

관리자 권한이 있는 계정을 사용하여 모니터링하려는 서버에서 *WinRM*을 구성해야 합니다. 보안을 위한 모범 사례로 이 계정은 *1*단계의 서비스 계정과 동일한 계정이 아니어야 합니다.

1. 인증서가 로컬 컴퓨터 인증서 저장소(인증서**(**로컬 컴퓨터**)** > 개인 > 인증서)에 설치되었는지 확인합니다.

   로컬 컴퓨터 인증서 저장소가 표시되지 않으면 Microsoft 관리 콘솔을 시작하고(**Run** > **MMC** > 시작) 인증서 스냅인을 추가합니다(파일 > 스냅인 > 인증서 > 추가**/**제거 > **AddComputer** > 계정 > **NextFinish** 추가).
2. 인증서를 열고 일반 > 세부정보 > 표시**: <All>**를 선택합니다.
3. 지문을 선택한 다음 복사합니다.
4. 방화벽이 WinRM을 사용하여 Windows 서버에 연결할 수 있도록 하려면 **`winrm quickconfig`** 명령을 입력합니다.
5. **y**를 입력하여 변경 사항을 확인한 다음 출력에 `WinRM 서비스 시작됨`이 표시되는지 확인합니다.

   WinRM이 활성화된 경우 출력에 `WinRM 서비스가 이미 이 시스템에서 실행 중`이라고 표시됩니다. 추가로 필요한 구성 변경을 확인하라는 메시지가 표시됩니다.
6. WinRM이 HTTPS를 사용하여 통신하는지 확인하려면 **`winrm enumerate winrm/config/listener`** 명령을 입력합니다. 그런 다음 출력에 `Transport = HTTPS`가 표시되는지 확인합니다.

   기본적으로 WinRM/HTTPS는 5986을 사용합니다.
7. Windows 서버 명령 프롬프트에서 **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate`**

 ©2023 Palo Alto Networks, Inc.

***Thumbprint"}*** 명령을 입력합니다. 여기서 *hostname*은 호스트 이름입니다. Windows 서버 및 인증서 지문은 인증서에서 복사한 값입니다.

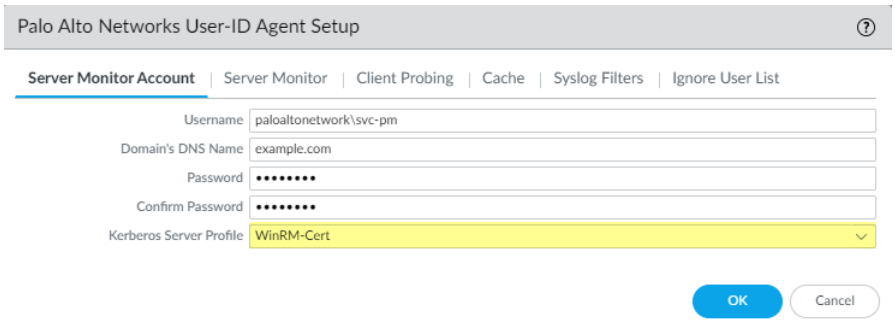
명령 프롬프트*(Powershell* 아님*)*를 사용하고 인증서 지문에서 공백을 제거하여 *WinRM*이 인증서의 유효성을 검사할 수 있도록 합니다.

8. **`winrm get winrm/config/service/Auth`** 명령을 입력하고 `Basic = false` 및 `Kerberos= true`인지 확인합니다.

**STEP 3 |** PAN-OS 통합 User-ID 에이전트와 모니터링되는 서버가 Kerberos를 사용하여 인증할 수 있도록 합니다.

1. 초기 구성 중에 그렇게 하지 않은 경우 성공적인 Kerberos 협상을 위해 NTP(날짜 및 시간) 설정을 구성합니다.
2. 방화벽에서 Kerberos 서버 프로파일을 구성하여 서버에 인증하여 보안 로그 및 세션 정보를 모니터링합니다.
3. 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks** 사용자 **ID** 에이전트 설정 > 서버 모니터 계정을 선택합니다.
4. **도메인\사용자 이름** 형식으로 User-ID 에이전트가 서버를 모니터링하는 데 사용할 서비스 계정의 사용자 이름을 입력합니다.
5. 서버 모니터 계정의 도메인 **DNS** 이름을 입력합니다.

   Kerberos는 도메인 이름을 사용하여 서비스 계정을 찾습니다.
6. 서비스 계정의 암호 및 암호 확인을 입력합니다.
7. **3.2**단계에서 생성한 **Kerberos** 서버 프로파일을 선택합니다.

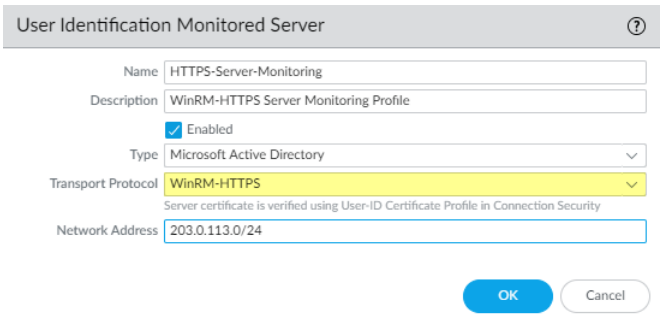



8. 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** PAN-OS 통합 User-ID 에이전트에 대한 서버 모니터링을 구성합니다.

1. Microsoft 서버 유형(**Microsoft Active Directory** 또는 **Microsoft Exchange**)을 구성합니다.
2. HTTPS를 통한 WinRM(Windows 원격 관리)을 사용하여 서버 보안 로그 및 세션 정보를 모니터링하려면 **Win-RM-HTTPS**를 전송 프로토콜로 선택합니다.



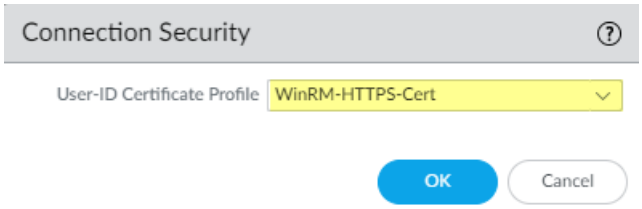

3. 서버의 FQDN 네트워크 주소를 입력합니다.

   Kerberos를 사용하는 경우 네트워크 주소는 FDQN(정규화된 도메인 이름)이어야 합니다.

**STEP 5 |** PAN-OS 통합 User-ID 에이전트가 WinRM-HTTPS를 사용하여 모니터링되는 서버와 통신할 수 있도록 하려면 Windows 서버가 WinRM에 사용하는 서비스 인증서의 루트 인증서를 방화벽으로 성공적으로 가져왔는지 확인하고 User-ID 인증서 프로파일이 포함된 인증서를 다음과 연결합니다.

방화벽은 동일한 인증서를 사용하여 모니터링되는 모든 서버를 인증합니다.

1. 디바이스 > 사용자 식별 > 연결 보안을 선택합니다.
2. 편집을 클릭합니다.
3. 사용자 **ID** 인증서 프로파일에 사용할 Windows 서버 인증서를 선택합니다.




4. 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

**STEP 6 |** 모니터링되는 각 서버의 상태가 연결됨(디바이스 > 사용자 식별 > 사용자 매핑)인지 확인합니다.

## 사용자 매핑을 위해 Syslog 발신자를 모니터링하도록 사용자 ID 구성

사용자를 인증하는 기존 네트워크 서비스에서 IP 주소-사용자 이름 매핑을 얻으려면 PAN-OS 통합 User-ID 에이전트 또는 Windows 기반 User-ID 에이전트를 구성하여 해당 서비스의 Syslog 메시지를 구문 분석할 수 있습니다. 사용자 매핑을 최신 상태로 유지하려면 User-ID 에이전트를 구성하여 방화벽이 오래된 매핑을 자동으로 삭제하도록 로그아웃 이벤트에 대한 syslog 메시지를 구문 분석할 수도 있습니다.

- PAN-OS 통합 사용자 ID 에이전트를 Syslog 수신기로 구성


©2023 Palo Alto Networks, Inc.

- Windows 사용자 ID 에이전트를 Syslog 수신기로 구성

## PAN-OS 통합 사용자 ID 에이전트를 Syslog 수신기로 구성

PAN-OS 통합 User-ID 에이전트가 syslog 모니터링을 통해 새 사용자 매핑을 생성하고 오래된 매핑을 제거하도록 구성하려면 먼저 Syslog Parse 프로파일을 정의하십시오. User-ID 에이전트는 프로파일을 사용하여 syslog 메시지에서 로그인 및 로그아웃 이벤트를 찾습니다. ***syslog*** 발신자(사용자를 인증하는 네트워크 서비스)가 다른 형식으로 syslog 메시지를 포워딩하는 환경에서는 각 syslog 형식에 대한 프로파일을 구성하십시오. Syslog 메시지는 User-ID 에이전트가 구문 분석할 수 있는 특정 기준을 충족해야 합니다(Syslog 참조). 이 절차에서는 다음 형식의 예를 사용합니다.

- **Login events** - `[Tue Jul 5 13:15:04 2016 CDT] Administratorauthentication success User:johndoe1 Source:192.168.3.212`
- **Logout events** - `[Tue Jul 5 13:18:05 2016CDT] User logout successful User:johndoe1 Source:192.168.3.212`

Syslog 구문 분석 프로파일을 구성한 후 모니터링할 User-ID 에이전트의 syslog 보낸 사람을 지정합니다.

**STEP 1 |** 특정 syslog 보낸 사람에 대해 사전 정의된 Syslog Parse 프로파일이 있는지 확인합니다.

Palo Alto Networks는 애플리케이션 콘텐츠 업데이트를 통해 사전 정의된 여러 프로파일을 제공합니다. 사전 정의된 프로파일은 방화벽에 전역적으로 적용되는 반면 사용자 지정 프로파일은 단일 가상 시스템에만 적용됩니다.

지정된 콘텐츠 릴리스의 모든 새 ***Syslog Parse*** 프로파일은 필터를 정의하는 데 사용되는 특정 정규식과 함께 해당 릴리스 노트에 문서화되어 있습니다.

1. 최신 애플리케이션 또는 애플리케이션 및 위협 업데이트를 설치합니다.
   1. 디바이스 > 동적 업데이트를 선택한 다음 지금 확인하십시오.
   2. 새 업데이트를 다운로드하고 설치합니다.
2. 사용 가능한 사전 정의된 Syslog Parse 프로파일을 확인합니다.
   1. **Device** > **User Identification** > **User Mapping**을 선택한 다음 서버 모니터링 섹션에서 추가를 클릭합니다.
   2. 유형을 **Syslog** 보낸 사람으로 설정하고 필터 섹션에서 추가를 클릭합니다. 필요한 Syslog Parse 프로파일을 사용할 수 있는 경우 사용자 지정 프로파일을 정의하는 단계를 건너뜁니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 사용자 매핑을 생성 및 삭제하기 위해 사용자 지정 Syslog Parse 프로파일을 정의합니다.

각 프로파일은 로그인 이벤트(사용자 매핑 생성) 또는 로그아웃 이벤트(매핑 삭제)를 식별하기 위해 syslog 메시지를 필터링하지만 단일 프로파일은 두 가지를 모두 수행할 수 없습니다.

1. syslog 발신자가 생성하는 syslog 메시지를 검토하여 로그인 및 로그아웃 이벤트 구문을 식별합니다. 이렇게 하면 Syslog 구문 분석 프로파일을 만들 때 일치하는 패턴을 정의할 수 있습니다.

   ***syslog*** 메시지를 검토하는 동안 도메인 이름이 포함되어 있는지의 여부도 확인합니다. 그렇지 않고 사용자 매핑에 도메인 이름이 필요한 경우 ***User-ID*** 에이전트가 모니터링하는 ***syslog*** 발신자를 정의할 때 기본 도메인 이름을 입력합니다(이 절차의 뒷부분).

2. 디바이스 > 사용자 식별 > 사용자 매핑을 선택하고 Palo Alto Networks 사용자 ID 에이전트 설정을 편집합니다.
3. **Syslog** 필터를 선택하고 Syslog Parse 프로파일을 추가합니다.
4. **Syslog** 구문 분석 프로파일을 식별하는 이름을 입력합니다.
5. syslog 메시지에서 로그인 또는 로그아웃 이벤트를 찾으려면 구문 분석의 유형을 선택합니다.
   - 정규식 식별자 - 정규식.
   - 필드 식별자 - 텍스트 문자열.

   다음 단계에서는 이러한 구문 분석 유형을 구성하는 방법을 설명합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** (정규식 식별자 구문 분석만 해당) 정규식 일치 패턴을 정의합니다.

*syslog* 메시지에 독립형 공백이나 탭이 구분 기호로 포함되어 있으면 공백에 **\s**를 사용하고 탭에 **\t**를 사용합니다.

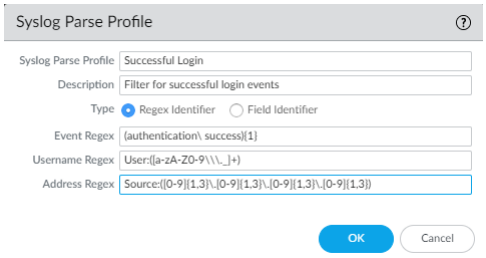
1. 찾고자 하는 이벤트 유형에 대한 이벤트 정규식을 입력합니다.
   - 로그인 이벤트 - 예제 메시지의 경우 **regex(authentication\ success){1}**는 문자열 **authenticationsuccess**의 첫 번째 **{1}** 인스턴스를 추출합니다.
   - 로그아웃 이벤트 - 예제 메시지의 경우 정규식 **(logout\ successful){1}**은 **logoutssuccessful** 문자열의 첫 번째 **{1}** 인스턴스를 추출합니다.

   공백 앞의 백슬래시(\)는 공백을 특수 문자로 취급하지 않도록 정규식 엔진에 지시하는 표준 정규식 이스케이프 문자입니다.
2. 사용자 이름의 시작을 식별하기 위해 사용자 이름 정규식을 입력합니다.

   예제 메시지에서 정규식 **User:([a-zA-Z0-9\\\._]+)**는 문자열 **User:johndoe1**과 일치하고 **johndoe1**을 사용자 이름으로 식별합니다.
3. 주소 정규식을 입력하여 syslog 메시지의 IP 주소 부분을 식별합니다.

   예제 메시지에서 정규식 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})**는 IPv4 주소 **Source:192.168.3.212**와 일치합니다.

   다음은 regex를 사용하여 로그인 이벤트를 식별하는 완료된 Syslog Parse 프로파일의 예입니다.




4. 확인을 두 번 클릭하여 프로파일을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (필드 식별자 구문 분석만 해당) 문자열 일치 패턴을 정의합니다.

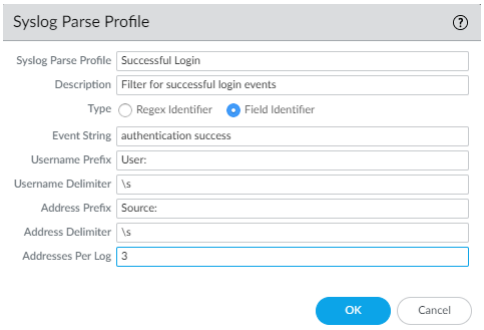
1. 찾으려는 이벤트 유형을 식별하는 이벤트 문자열을 입력합니다.
   - 로그인 이벤트 - 예제 메시지의 경우 문자열 **`authentication success`**는 로그인 이벤트를 식별합니다.
   - 로그아웃 이벤트 - 예제 메시지의 경우 **`logoutssuccessful`** 문자열은 로그아웃 이벤트를 식별합니다.
2. 사용자 이름 프리픽스를 입력하여 syslog 메시지에서 사용자 이름 필드의 시작을 식별합니다. 필드는 \s(공백의 경우) 또는 \t(탭의 경우)와 같은 정규식을 지원하지 않습니다.

   예제 메시지에서 **`사용자:`**는 사용자 이름 필드의 시작을 식별합니다.
3. syslog 메시지에서 사용자 이름 필드의 끝을 나타내는 사용자 이름 구분 기호를 입력합니다. 독립형 공간을 나타내려면 **`\s`**를 사용하고 탭을 나타내려면 **`\t`**을 사용합니다.
4. syslog 메시지에서 IP 주소 필드의 시작을 식별하려면 주소 프리픽스를 입력하십시오. 필드는 \s(공백의 경우) 또는 \t(탭의 경우)와 같은 정규식을 지원하지 않습니다.

   예제 메시지에서 **`Source:`**는 주소 필드의 시작을 식별합니다.
5. syslog 메시지에서 IP 주소 필드의 끝을 나타내는 주소 구분 기호를 입력합니다.

   예를 들어 구분 기호가 줄 바꿈임을 나타내려면 **`\n`**을 입력합니다.

   다음은 문자열 일치를 사용하여 로그인 이벤트를 식별하는 완료된 Syslog 구문 분석 프로파일의 예입니다.




6. 확인을 두 번 클릭하여 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 방화벽이 모니터링하는 syslog을 보낸 사람을 지정합니다.

방화벽당 최대 100개의 모니터링되는 서버 내에서 단일 가상 시스템에 대해 50개 이하의 syslog 발신자를 정의할 수 있습니다.

방화벽은 이 목록에 없는 발신자로부터 받은 모든 syslog 메시지를 삭제합니다.

1. 디바이스 > 사용자 식별 > 사용자 매핑을 선택하고 서버 모니터링 목록에 항목을 추가합니다.
2. 보낸 사람을 식별할 이름을 입력합니다.
3. 보낸 사람 프로파일이 활성화되어 있는지 확인합니다(기본값은 활성화됨).
4. 유형을 **Syslog** 발신자로 설정하십시오.
5. syslog 발신자의 네트워크 주소(IP 주소)를 입력합니다.
6. **SSL**(기본값) 또는 **UDP**를 연결 유형으로 선택합니다.

   방화벽이 ***syslog*** 메시지를 수신하는 데 사용하는 ***TLS*** 인증서를 선택하려면 디바이스 > 사용자 식별 > 사용자 매핑 > ***Palo Alto Networks User-ID*** 에이전트 설정을 선택하십시오. 설정을 편집하고 서버 모니터를 선택한 다음 방화벽이 ***syslog*** 메시지를 수신하는 데 사용할 ***TLS*** 인증서가 포함된 ***Syslog*** 서비스 프로파일을 선택합니다.

   ***PAN-OS*** 통합 ***User-ID*** 에이전트는 ***SSL*** 및 ***UDP***를 통해서만 ***syslog***를 수락합니다. 그러나 ***UDP***는 신뢰할 수 없는 프로토콜이고 신뢰할 수 있는 ***syslog*** 보낸 사람이 보낸 메시지인지 확인할 수 있는 방법이 없기 때문에 ***UDP***를 사용하여 ***syslog*** 메시지를 받을 때는 주의해야 합니다. ***syslog*** 메시지를 특정 소스 ***IP*** 주소로 제한할 수 있지만 공격자는 여전히 ***IP*** 주소를 스푸핑하여 잠재적으로 승인되지 않은 ***syslog*** 메시지를 방화벽에 주입할 수 있습니다.

   트래픽이 암호화되어 있으므로 항상 ***SSL***을 사용하여 ***syslog*** 메시지를 수신합니다(***UDP***는 트래픽을 일반 텍스트로 전송). ***UDP***를 사용해야 하는 경우 신뢰할 수 없는 호스트가 ***UDP*** 트래픽을 방화벽으로 보내는 것을 방지하기 위해 ***syslog*** 발신자와 클라이언트가 모두 안전한 전용 네트워크에 있는지 확인하십시오.

   SSL을 사용하여 연결하는 syslog 발신자는 활성 SSL 연결이 있는 경우에만 연결됨 상태를 표시합니다. UDP를 사용하는 Syslog 발신자는 상태 값을 표시하지 않습니다.
7. 보낸 사람이 지원하는 각 syslog 형식에 대해 Syslog 구문 분석 프로파일을 필터 목록에 추가합니다. 로그인(기본값) 또는 로그아웃 중에서 각 프로파일이 식별하도록 구성된 이벤트 유형을 선택합니다.
8. (선택 사항) syslog 메시지에 도메인 정보가 없고 사용자 매핑에 도메인 이름이 필요한 경우 매핑에 추가할 기본 도메인 이름을 입력합니다.
9. 확인을 클릭하여 설정을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 방화벽이 사용자 매핑을 수집하는 데 사용하는 인터페이스에서 syslog 수신기 서비스를 활성화합니다.

1. 네트워크 > 네트워크 프로파일 > 인터페이스 관리를 선택하고 기존 인터페이스 관리 프로파일을 수정하거나 새 프로파일을 추가합니다.
2. 서버 모니터링 목록에서 syslog 발신자에 대해 정의한 프로토콜을 기반으로 **User-ID Syslog Listener-SSL** 또는 **User-ID Syslog Listener-UDP** 또는 둘 다를 선택합니다.

   수신 포트*(UDP*의 경우 *514*, *SSL*의 경우 *6514)*는 구성할 수 없으며, 관리 서비스를 통해서만 활성화됩니다.

3. 확인을 클릭하여 인터페이스 관리 프로파일을 저장합니다.

   인터페이스에서 *User-ID Syslog Listener* 서비스를 활성화한 후에도 인터페이스는 *User-ID* 모니터링 서버 구성에 해당 항목이 있는 보낸 사람의 *syslog* 연결만 수락합니다. 방화벽은 목록에 없는 보낸 사람의 연결이나 메시지를 삭제합니다.

4. 방화벽이 사용자 매핑을 수집하는 데 사용하는 인터페이스에 인터페이스 관리 프로파일을 할당합니다.
   1. 네트워크 > 인터페이스를 선택한 다음 인터페이스를 편집합니다.
   2. 고급 > 기타 정보를 선택한 다음 방금 추가한 인터페이스 관리 프로파일을 선택한 다음 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

**STEP 7 |** 사용자가 로그인 및 로그아웃할 때 방화벽이 사용자 매핑을 추가 및 삭제하는지 확인합니다.

CLI 명령을 사용하여 *syslog* 발신자, *syslog* 메시지 및 사용자 매핑에 대한 추가 정보를 볼 수 있습니다.

1. 모니터링되는 syslog 발신자가 로그인 및 로그아웃 이벤트 메시지를 생성하는 클라이언트 시스템에 로그인합니다.
2. 방화벽 CLI에 로그인합니다.
3. 방화벽이 로그인 사용자 이름을 클라이언트 IP 주소에 매핑했는지 확인합니다.

```
> show user ip-user-mapping ip <ip-address> IP
 address:    192.0.2.1 (vsys1) User:          localdomain
\username From:          SYSLOG
```

4. 클라이언트 시스템에서 로그아웃합니다.
5. 방화벽이 사용자 매핑을 삭제했는지 확인합니다.

```
> show user ip-user-mapping ip <ip-address> No matched record
```

## Windows 사용자 ID 에이전트를 Syslog 수신기로 구성

새 사용자 매핑을 생성하고 syslog 모니터링을 통해 오래된 매핑을 제거하도록 Windows 기반 User-ID 에이전트를 구성하려면 Syslog Parse 프로파일을 정의하여 시작합니다. User-ID 에이전트는 프로파일을 사용하여 syslog 메시지에서 로그인 및 로그아웃 이벤트를 찾습니다. *syslog* 발신자(사용자를 인증하는 네트

 ©2023 Palo Alto Networks, Inc.

워크 서비스)가 다른 형식으로 syslog 메시지를 포워딩하는 환경에서는 각 syslog 형식에 대한 프로파일을 구성하십시오. Syslog 메시지는 User-ID 에이전트가 구문 분석할 수 있는 특정 기준을 충족해야 합니다(Syslog 참조). 이 절차에서는 다음 형식의 예를 사용합니다.

- 로그인 이벤트 - `[Tue Jul 5 13:15:04 2016 CDT] 관리자 인증 성공 User:johndoe1 Source:192.168.3.212`
- 로그아웃 이벤트 - `[Tue Jul 5 13:18:05 2016 CDT] 사용자 로그아웃 성공 User:johndoe1 Source:192.168.3.212`

Syslog Parse 프로파일을 구성한 후 User-ID 에이전트가 모니터링하는 syslog 발신자를 지정합니다.

***Windows User-ID** 에이전트는 **TCP** 및 **UDP**에 대해서만 **syslogs**를 허용합니다. 그러나 **UDP**는 신뢰할 수 없는 프로토콜이고 신뢰할 수 있는 **syslog** 보낸 사람이 보낸 메시지인지 확인할 수 있는 방법이 없기 때문에 **UDP**를 사용하여 **syslog** 메시지를 받을 때는 주의해야 합니다. **syslog** 메시지를 특정 소스 **IP** 주소로 제한할 수 있지만 공격자는 여전히 **IP** 주소를 스푸핑하여 잠재적으로 승인되지 않은 **syslog** 메시지를 방화벽에 주입할 수 있습니다. 모범 사례로 **UDP** 대신 **TCP**를 사용합니다. 두 경우 모두 **syslog** 보낸 사람 및 클라이언트가 모두 전용 보안 **VLAN**에 있는지 확인하여 신뢰할 수 없는 호스트가 **User-ID** 에이전트에 **syslogs**를 보내지 못하도록 합니다.*

**STEP 1 |** 아직 없는 경우 Windows 기반 User-ID 에이전트를 배포합니다.

1. Windows 기반 사용자 ID 에이전트 설치.
2. User-ID 에이전트에 연결할 방화벽을 구성합니다.

**STEP 2 |** 사용자 매핑을 생성 및 삭제하기 위해 사용자 지정 Syslog Parse 프로파일을 정의합니다.

각 프로파일은 로그인 이벤트(사용자 매핑 생성) 또는 로그아웃 이벤트(매핑 삭제)를 식별하기 위해 syslog 메시지를 필터링하지만 단일 프로파일은 두 가지를 모두 수행할 수 없습니다.

1. syslog 발신자가 생성하는 syslog 메시지를 검토하여 로그인 및 로그아웃 이벤트 구문을 식별합니다. 이렇게 하면 Syslog 구문 분석 프로파일을 만들 때 일치하는 패턴을 정의할 수 있습니다.

   ***syslog** 메시지를 검토하는 동안 도메인 이름이 포함되어 있는지의 여부도 확인합니다. 그렇지 않고 사용자 매핑에 도메인 이름이 필요한 경우 **User-ID** 에이전트가 모니터링하는 **syslog** 발신자를 정의할 때 기본 도메인 이름을 입력합니다(이 절차의 뒷부분).*

2. Windows 시작 메뉴를 열고 **User-ID** 에이전트를 선택합니다.
3. 사용자 식별 > 설정을 선택하고 설정을 수정합니다.
4. **Syslog**, **Syslog** 서비스 활성화 및 Syslog 구문 분석 프로파일을 추가를 선택합니다.
5. 프로파일 이름 및 설명을 입력합니다.
6. syslog 메시지에서 로그인 및 로그아웃 이벤트를 찾으려면 구문 분석의 유형을 선택합니다.
   - 정규식 - 정규식.
   - 필드 - 텍스트 문자열입니다.

   다음 단계에서는 이러한 구문 분석 유형을 구성하는 방법을 설명합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** (**Regex** 구문 분석만)레텍스 일치 패턴을 정의합니다.

syslog 메시지에 독립형 공백이나 탭이 구분 기호로 포함되어 있으면 공백에 **\s**를 사용하고 탭에 **\t**를 사용합니다.

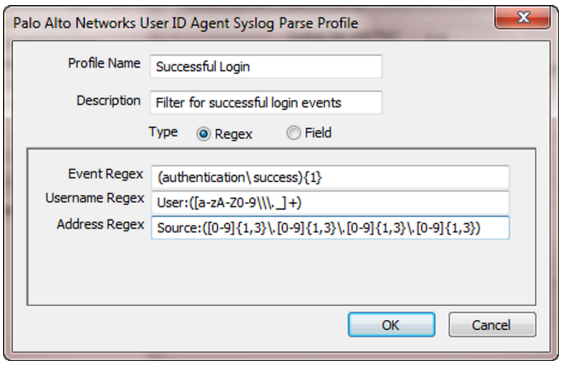
1. 찾고자 하는 이벤트 유형에 대한 이벤트 정규식을 입력합니다.
   - 로그인 이벤트 - 예제 메시지의 경우 regex**(authentication\ success){1}**은 문자열 인증 성공의 첫 번째 **{1}** 인스턴스를 추출합니다.
   - 로그아웃 이벤트 - 예제 메시지의 경우, regex **(logout\ successful){1}**은 문자열 로그아웃의 첫 번째 **{1}** 인스턴스를 성공적으로 추출합니다.

   공백 앞의 백슬래시는 공백을 특수 문자로 취급하지 않도록 정규식 엔진에 지시하는 표준 정규식 확장 문자입니다.
2. 사용자 이름의 시작을 식별하기 위해 사용자 이름 정규식을 입력합니다.

   예제 메시지에서 정규식 **User:([a-zA-Z0-9\\\._]+)**는 문자열 User:johndoe1과 일치하고 **johndoe1**을 사용자 이름으로 식별합니다.
3. 주소 정규식을 입력하여 syslog 메시지의 IP 주소 부분을 식별합니다.

   예제 메시지에서 정규식 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})**는 IPv4 주소 Source:192.168.3.212와 일치합니다.

   다음은 regex를 사용하여 로그인 이벤트를 식별하는 완료된 Syslog Parse 프로파일의 예입니다.




4. 확인을 두 번 클릭하여 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** (필드 식별자 구문 분석만 해당) 문자열 일치 패턴을 정의합니다.

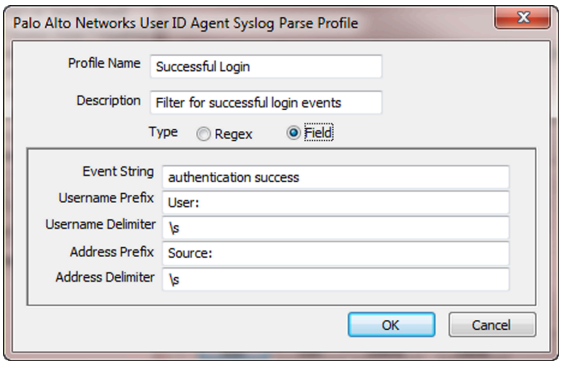
1. 찾으려는 이벤트 유형을 식별하는 이벤트 문자열을 입력합니다.
   - 로그인 이벤트 - 예제 메시지의 경우 문자열 **`authentication success`**는 로그인 이벤트를 식별합니다.
   - 로그아웃이벤트 - 예제 메시지의 경우 문자열 **`로그아웃 성공`** 로그아웃 이벤트를 식별합니다.
2. 사용자 이름 프리픽스를 입력하여 syslog 메시지에서 사용자 이름 필드의 시작을 식별합니다. 필드는 \s(공백의 경우) 또는 \t(탭의 경우)와 같은 정규식을 지원하지 않습니다.

   예제 메시지에서 **`사용자:`**는 사용자 이름 필드의 시작을 식별합니다.
3. syslog 메시지에서 사용자 이름 필드의 끝을 나타내는 사용자 이름 구분 기호를 입력합니다. 독립형 공간을 나타내려면 **`\s`**를 사용하고 탭을 나타내려면 **`\t`**을 사용합니다.
4. syslog 메시지에서 IP 주소 필드의 시작을 식별하려면 주소 프리픽스를 입력하십시오. 필드는 \s(공백의 경우) 또는 \t(탭의 경우)와 같은 정규식을 지원하지 않습니다.

   예제 메시지에서 **`Source:`**는 주소 필드의 시작을 식별합니다.
5. syslog 메시지에서 IP 주소 필드의 끝을 나타내는 주소 구분 기호를 입력합니다.

   예를 들어 구분 기호가 줄 바꿈임을 나타내려면 **`\n`**을 입력합니다.

   다음은 문자열 일치를 사용하여 로그인 이벤트를 식별하는 완료된 Syslog 구문 분석 프로파일의 예입니다.




6. 확인을 두 번 클릭하여 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** User-ID 에이전트가 모니터링하는 syslog 발신자를 지정합니다.

User-ID 에이전트가 모니터링할 수 있는 모든 유형의 최대 100개 서버 내에서 최대 50개의 syslog 발신자가 될 수 있습니다.

User-ID 에이전트는 이 목록에 없는 발신자로부터 받은 syslog 메시지를 삭제합니다.

1. 사용자 식별 > 검색을 선택하고 서버 목록에 항목을 추가합니다.
2. 보낸 사람을 식별할 이름을 입력합니다.
3. syslog 발신자의 서버 주소(IP 주소 또는 FQDN)를 입력합니다.
4. 서버 유형을 **Syslog Sender**로 설정합니다.
5. (선택사항)syslog 메시지의 사용자 이름으로 현재 도메인을 재정의하거나 syslog 메시지에 도메인이 포함되어 있지 않은 경우 도메인을 사용자 이름으로 준비하려면 기본 도메인 이름을 입력합니다.
6. 보낸 사람이 지원하는 각 syslog 형식에 대해 Syslog 구문 분석 프로파일을 필터 목록에 추가합니다. 식별하도록 각 프로파일을 구성한 이벤트 유형(로그인(기본값) 또는 로그아웃)을 선택한 다음 확인을 클릭합니다.
7. 확인을 클릭하여 설정을 저장합니다.
8. User-ID 에이전트 구성에 대한 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 사용자가 로그인하고 나갈 때 User-ID 에이전트가 사용자 매핑을 추가하고 삭제했는지 확인합니다.



CLI 명령을 사용하여 ***syslog*** 발신자, ***syslog*** 메시지 및 사용자 매핑에 대한 추가 정보를 볼 수 있습니다.

1. 모니터링되는 syslog 발신자가 로그인 및 로그아웃 이벤트 메시지를 생성하는 클라이언트 시스템에 로그인합니다.
2. User-ID 에이전트가 로그인 사용자 이름을 클라이언트 IP 주소에 매핑했는지 확인합니다.
   1. User-ID 에이전트에서 모니터링을 선택합니다.
   2. 필터 필드에 사용자 이름 또는 IP 주소를 입력하여 검색하고, 목록이 매핑을 표시했는지 확인합니다.
3. 방화벽이 User-ID 에이전트로부터 사용자 매핑을 받았는지 확인합니다.
   1. 방화벽 CLI에 로그인합니다.
   2. 다음 명령을 실행합니다.

      ```
      > show user ip-user-mapping ip <ip-address>
      ```

      방화벽이 사용자 매핑을 받은 경우 출력은 다음과 유사합니다.

      ```
      IP address:    192.0.2.1 (vsys1) User:          localdomain
      \username From:          SYSLOG
      ```
4. 클라이언트 시스템에서 로그아웃합니다.
5. User-ID 에이전트가 사용자 매핑을 제거했는지 확인합니다.
   1. User-ID 에이전트에서 모니터링을 선택합니다.
   2. 필터 필드에 사용자 이름 또는 IP 주소를 입력하여 검색하고, 목록이 매핑을 표시하지 않는지 확인합니다.
6. 방화벽이 사용자 매핑을 삭제했는지 확인합니다.
   1. 방화벽 CLI에 액세스합니다.
   2. 다음 명령을 실행합니다.

      ```
      > show user ip-user-mapping ip <ip-address>
      ```

      방화벽이 사용자 매핑을 삭제하면 출력에 다음이 표시됩니다.

      ```
      일치하는 레코드 없음
      ```

## 인증 포털을 사용하여 사용자 이름에 IP 주소 매핑

사용자가 인증 정책 규칙과 일치하는 웹 트래픽(HTTP 또는 HTTPS)을 시작하면 방화벽은 사용자에게 인증 포털을 통해 인증하라는 메시지를 표시합니다. 이렇게 하면 가장 민감한 애플리케이션과 데이터에 누가 액세스하는지 정확히 알 수 있습니다. 방화벽은 인증 중에 수집된 사용자 정보를 기반으로 새 IP 주

 ©2023 Palo Alto Networks, Inc.

소-사용자 이름 매핑을 생성하거나 해당 사용자에 대한 기존 매핑을 업데이트합니다. 이 사용자 매핑 방법은 방화벽이 서버 모니터링과 같은 다른 방법을 통해 매핑을 학습할 수 없는 환경에서 유용합니다. 예를 들어 Linux 클라이언트의 사용자와 같이 모니터링되는 도메인 서버에 로그인하지 않은 사용자가 있을 수 있습니다.

- 인증 포털 인증 방법
- 인증 포털 모드
- 인증 포털 구성

## 인증 포털 인증 방법

인증 포털은 다음 방법을 사용하여 웹 요청이 인증 정책 규칙과 일치하는 사용자를 인증합니다.

| 인증 방법 | 설명 |
|---|---|
| Kerberos SSO | 방화벽은 Kerberos Single Sign-On(SSO)을 사용하여 브라우저에서 투명하게 사용자 자격 증명을 얻습니다. 이 방법을 사용하려면 네트워크에 인증 서버와 티켓 부여 서비스가 있는 KDC(키 배포 센터)를 포함한 Kerberos 인프라가 필요합니다. 방화벽에는 Kerberos 계정이 있어야 합니다.<br>Kerberos SSO 인증이 실패하면 방화벽은 인증 정책 및 인증 포털 구성에 따라 웹 양식 또는 클라이언트 인증서 인증으로 대체합니다. |
| 웹 양식 | 방화벽은 인증을 위해 웹 요청을 웹 양식으로 리디렉션합니다. 이 방법의 경우 Multi-Factor Authentication(MFA), SAML, Kerberos, TACACS+, RADIUS 또는 LDAP 인증을 사용하도록 인증 정책을 구성할 수 있습니다. 사용자가 로그인 자격 증명을 수동형으로 입력해야 하지만 이 방법은 모든 브라우저 및 운영 체제에서 작동합니다. |
| 클라이언트 인증서 인증 | 방화벽은 사용자를 인증하기 위해 유효한 클라이언트 인증서를 제시하도록 브라우저에 프롬프트를 표시합니다. 이 방법을 사용하려면 각 사용자 시스템에 클라이언트 인증서를 프로비저닝하고 방화벽에서 해당 인증서를 발급하는 데 사용되는 신뢰할 수 있는 CA(인증 기관) 인증서를 설치해야 합니다. |

## 인증 포털 모드

인증 포털 모드는 방화벽이 인증을 위한 웹 요청을 캡처하는 방법을 정의합니다.

| 모드 | 설명 |
|---|---|
| 투명 | 방화벽은 인증 정책 규칙에 따라 브라우저 트래픽을 가로채고 원래 대상 URL을 가장하여 HTTP 401을 발행하여 인증을 호출합니다. 그러나 방화벽에는 대상 URL에 대한 실제 인증서가 없기 때문에 브라우저는 보안 사이트에 액세스하려는 사용자에게 인증서 오류를 표시 |


©2023 Palo Alto Networks, Inc.

| 모드 | 설명 |
| --- | --- |
| | 합니다. 따라서 레이어 2 또는 가상 와이어 배포와 같이 절대적으로 필요한 경우에만 이 모드를 사용하십시오. |
| 리디렉션 | 방화벽은 알 수 없는 HTTP 또는 HTTPS 세션을 가로채서 HTTP 302 리디렉션을 사용하여 방화벽의 레이어 3 인터페이스로 리디렉션하여 인증을 수행합니다. 이것은 더 나은 최종 사용자 경험을 제공하기 때문에 선호되는 모드입니다(인증서 오류 없음). 그러나 추가 레이어 3 구성이 필요합니다. 리디렉션 모드의 또 다른 이점은 세션 쿠키를 사용하여 사용자가 타임아웃가 만료될 때마다 다시 매핑할 필요 없이 인증된 사이트를 계속 탐색할 수 있다는 것입니다. 이는 세션이 열려 있는 한 IP 주소가 변경될 때 다시 인증할 필요가 없기 때문에 한 IP 주소에서 다른 IP 주소로 로밍하는 사용자에게 특히 유용합니다(예: 회사 LAN에서 무선 네트워크로).<br><br>Kerberos SSO를 사용하는 경우 브라우저가 신뢰할 수 있는 사이트에만 자격 증명을 제공하므로 리디렉션 모드를 사용해야 합니다. 다단계 인증을(를) 사용하여 인증 포털 사용자를 인증하는 경우에도 리디렉션 모드가 필요합니다. |

## 인증 포털 구성

다음 절차는 PAN-OS 통합 User-ID 에이전트를 구성하여 인증 정책 규칙과 일치하는 웹 요청을 방화벽 인터페이스(리디렉션 호스트)로 리디렉션하여 인증 포털 인증을 설정하는 방법을 보여 줍니다.

SSL 인바운드 검사는 인증 포털 리디렉션을 지원하지 않습니다. 인증 포털 리디렉션 및 복호화을 사용하려면 SSL 포워드 프록시를 사용해야 합니다.

사용자들이 인증 포털을 통해 액세스하는 애플리케이션에는 민감도에 따라 서로 다른 인증 방법과 설정이 필요합니다. 모든 인증 요구 사항을 수용하기 위해 기본 및 사용자 지정 인증 적용 개체를 사용할 수 있습니다. 각 개체는 인증 프로파일 및 인증 포털 인증 메서드와 인증 규칙을 연결합니다.

- 기본 인증 적용 개체—여러 인증 규칙을 동일한 전역 인증 프로파일과 연결하려는 경우 기본 개체를 사용합니다. 인증 포털을 구성하기 전에 이 인증 프로파일을 구성한 다음 인증 포털 설정에 할당해야 합니다. MFA(다단계 인증)가 필요한 인증 규칙의 경우 기본 인증 적용 개체를 사용할 수 없습니다.
- 사용자 지정 인증 적용 개체— 전역 프로파일과 다른 인증 프로파일이 필요한 각 인증 규칙에 대한 사용자 지정 개체를 사용합니다. 사용자 지정 개체는 MFA가 필요한 인증 규칙에 필수입니다. 사용자 지정 개체를 사용하려면 인증 포털을 구성할 때 인증 프로파일을 생성하고 개체에 할당합니다.

인증 포털 웹 양식 또는 Kerberos SSO를 통해 인증하는 경우에만 인증 프로파일이 필요합니다. 또는 이러한 메서드 외에도 다음 프로시저에서 클라이언트 인증서 인증을 구현하는 방법도 설명합니다.

다른 사용자 ***ID*** 기능(사용자 매핑 및 그룹 매핑) 없이 인증 포털을 사용하는 경우 ***User-ID*** 에이전트를 구성할 필요가 없습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 방화벽이 들어오는 웹 요청에 사용할 인터페이스를 구성하고, 사용자를 인증하고, 디렉터리 서버와 통신하여 사용자 이름을 IP 주소로 매핑합니다.

방화벽이 인증 서버 또는 User-ID 에이전트에 연결되면 기본적으로 관리 인터페이스를 사용합니다. 모범 사례로 서비스 경로를 구성하여 인증 서버 또는 User-ID 에이전트에 연결하여 관리 네트워크를 격리합니다.

1. (MGT 인터페이스만)디바이스 > 설정 > 인터페이스를 선택한 다음 관리 인터페이스를 편집하고, **User-ID**를 선택한 다음 확인을 클릭합니다.
2. (MGT가 아닌 인터페이스만) 방화벽이 들어오는 웹 요청 및 디렉터리 서버와의 통신에 사용할 레이어 3 인터페이스에 인터페이스 관리 프로파일을 할당합니다. 인터페이스 관리 프로파일에서 응답 페이지 및 **User-ID**를 사용하도록 설정해야 합니다.
3. (MGT가 아닌 인터페이스만)방화벽이 사용자를 인증하는 데 사용할 인터페이스에 대한 서비스 경로를 구성합니다. 방화벽에 두 개 이상의 가상 시스템(vsys)이 있는 경우 서비스 경로는 전역 또는 vsys에 특정할 수 있습니다. 서비스에는 **LDAP**와 다음이 포함되어야 합니다.
   - **Kerberos,**, **RADIUS,**, **TACACS+**, 또는 다단계 인증 - 사용하는 모든 인증 서비스에 대한 서비스 경로를 구성합니다.
   - **UID** 에이전트 - 사용자 및 그룹 기반 정책을 사용하도록 설정한 경우에만 이 서비스를 구성합니다.
4. (리디렉션 모드만) 레이어 3 인터페이스의 IP 주소를 리디렉션 호스트로 매핑하는 DNS 주소(A) 레코드를 생성합니다. Kerberos SSO를 사용하는 경우 동일한 매핑을 수행하는 DNS 포인터(PTR) 레코드도 추가해야 합니다.

네트워크가 방화벽 인터페이스에서 디렉터리 서버에 대한 액세스를 지원하지 않는 경우 Windows User-ID 에이전트를 사용하여 사용자 매핑을 구성해야 합니다.

**STEP 2 |** 도메인 이름 시스템(DNS)이 도메인 컨트롤러 주소를 해결하도록 구성되어 있는지 확인합니다.

적절한 해상도를 확인하려면 서버 FQDN을 핑(ping)합니다. 예:

```
admin@PA-220> ping host dc1.acme.com
```

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 인증 포털 인증서를 신뢰하도록 클라이언트를 구성합니다.

리디렉션 모드에 필요한 경우 인증서 오류를 표시하지 않고 사용자를 투명하게 리디렉션합니다. 자체 서명된 인증서를 생성하거나 외부 인증서 기관(CA)이 서명한 인증서를 가져올 수 있습니다.

자체 서명된 인증서를 사용하려면 루트 CA 인증서를 생성하고 인증 포털에 사용할 인증서에 서명하는 데 사용합니다.

1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.
2. 자체 서명된 루트 CA 인증서를 생성하거나 CA 인증서를 가져옵니다(인증서 및 개인 키 가져오기 참조).
3. 인증 포털에 사용할 인증서를 생성합니다. 다음 필드를 구성해야 합니다.
   - 공통 이름 - 레이어 3 인터페이스에 대한 인트라넷 호스트의 DNS 이름을 입력합니다.
   - 서명자 - 방금 만들거나 불러온 CA 인증서를 선택합니다.
   - 인증서 속성 - 추가를 클릭하고 유형에 대해 **IP**를 선택한 다음 값에 대해 방화벽이 요청을 리디렉션할 대상인 Layer 3 인터페이스의 IP 주소를 입력합니다.
4. SSL/TLS 서비스 프로파일을 구성합니다. 방금 생성한 인증 포털 인증서를 프로파일에 할당합니다.

   ***SSL/TLS*** 서비스 프로파일을 할당하지 않으면 방화벽은 기본적으로 ***TLS 1.2***를 사용합니다. 다른 ***TLS*** 버전을 사용하려면 사용할 ***TLS*** 버전에 대해 ***SSL/TLS*** 서비스 프로파일을 구성합니다.
5. 인증서를 신뢰하도록 클라이언트를 구성합니다.
   1. 만든 CA 인증서를 내보내거나 불러온 것입니다.
   2. 브라우저를 수동으로 구성하거나 활성 디렉터리(AD) 그룹 정책 개체(GPO)의 신뢰할 수 있는 루트에 인증서를 추가하여 신뢰할 수 있는 루트 CA로 인증서를 모든 클라이언트 브라우저에 가져옵니다.

**STEP 4 |** (선택 사항) 클라이언트 인증서 인증을 구성합니다.

클라이언트 인증서 인증을 위해 인증 프로파일이나 시퀀스가 필요하지 않습니다. 인증 프로파일/시퀀스와 인증서 인증을 모두 구성하는 경우 사용자는 둘 다 사용하여 인증해야 합니다.

1. 루트 CA 인증서를 사용하여 인증 포털을 통해 인증할 각 사용자에 대한 클라이언트 인증서를 생성합니다. 이 경우 CA는 일반적으로 방화벽이 아니라 엔터프라이즈 CA입니다.
2. PEM 형식의 CA 인증서를 방화벽이 액세스할 수 있는 시스템으로 내보냅니다.
3. 방화벽에 CA 인증서 가져오기: 인증서 및 개인 키 가져오기를 참조하십시오. 불러온 후 불러온 인증서를 클릭하고 신뢰할 수 있는 루트 **CA**를 선택한 다음 확인을 클릭합니다.
4. 인증서 프로파일을 구성합니다.
   - 사용자 이름 필드 드롭다운에서 사용자 ID 정보가 포함된 인증서 필드를 선택합니다.
   - **CA** 인증서 목록에서 가져오기만 하면 추가를 클릭하고 방금 불러온 CA 인증서를 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** (선택 사항) Apple Captive Network Assistant에 대한 인증 포털을 구성합니다.

이 단계는 Apple Captive Network Assistant(CNA)와 인증 포털을 사용하는 경우에만 필요합니다. CNA와 인증 포털을 사용하려면 다음 단계를 수행합니다.

1. 리디렉션 호스트(IP 주소뿐만 아니라)에 FQDN을 지정했는지 확인합니다.
2. 지정된 FQDN에 대해 공개적으로 서명된 인증서를 사용하는 SSL/TLS 서비스 프로파일을 선택합니다.
3. 인증 포털에 지원되는 요청 수를 조정하기 위해 입력해야 하는 명령: **set deviceconfig setting ctd cap-portal-ask-requests *<threshold-value>***

   기본적으로 방화벽에는 인증 포털의 속도 제한 임계값이 있으며, 요청 수를 2초마다 하나의 요청으로 제한합니다. CNA는 이 제한을 초과할 수 있는 여러 요청을 전송하므로 TCP 재설정과 CNA의 오류가 발생할 수 있습니다. 권장 임계값은 5입니다(기본값은 1). 이 값은 2초마다 최대 5개의 요청을 허용합니다. 환경에 따라 다른 값을 구성해야 할 수 있습니다. 현재 값이 요청 수를 처리하기에 충분하지 않으면 값을 늘립니다.

**STEP 6 |** 인증 포털 설정을 구성합니다.

1. 디바이스 > 사용자 **ID** > 인증 포털 설정을 선택한 다음 설정을 수정합니다.
2. 인증 포털을 활성화합니다(기본값이 활성화되어 있음).
3. 사용자가 인증 포털을 통해 인증한 후 방화벽이 사용자에 대한 IP 주소-사용자 이름 매핑을 유지하는 최대 시간인 타이머를 지정합니다(기본값은 60, 범위는 1~1,440). 타이머가 만료되면 방화

 ©2023 Palo Alto Networks, Inc.

벽은 인증 정책 규칙에서 타임아웃을 평가하는 데 사용되는 매핑 및 관련 인증 타임스탬프를 제거합니다.

각 인증 정책 규칙에서 인증 포털 타이머 및 타임 아웃 값을 평가할 때 방화벽은 사용자에게 먼저 만료되는 설정에 대해 다시 인증하라는 메시지를 표시합니다. 다시 인증하면 방화벽은 인증 포털 타이머의 타임 카운트를 재설정하고 사용자에 대한 새 인증 타임스탬프를 기록합니다. 따라서 서로 다른 인증 규칙에 대해 다른 타임아웃 기간을 사용하도록 설정하려면 인증 포털 타이머를 규칙 타임 아웃과 같거나 높은 값으로 설정합니다.

4. TLS를 통해 리디렉션 요청을 위해 만든 **SSL/TLS** 서비스 프로파일을 선택합니다. SSL/TLS 서비스 프로파일 구성을 참조하십시오.
5. 모드를 선택합니다(이 예에서 리디렉션).
6. (리디렉션 모드만 해당) 웹 요청이 리디렉션되는 방화벽의 레이어 3 인터페이스 IP 주소로 확인되는 인트라넷 호스트 이름(이름에 마침표가 없는 호스트 이름)인 리디렉션 호스트를 지정합니다.

   사용자가 Kerberos Single Sign-On(SSO)을 통해 인증하는 경우 리디렉션 호스트는 Kerberos 키 탭에 지정된 호스트 이름과 같아야 합니다.
7. 사용할 가을 다시 인증 방법을 선택합니다.
   - 클라이언트 인증서 인증을 사용하려면 만든 인증서 프로파일을 선택합니다.
   - 대화형 또는 SSO 인증에 대한 전역 설정을 사용하려면 구성한 인증 프로파일을 선택합니다.
   - 대화형 또는 SSO 인증에 대한 인증 정책 규칙별 설정을 사용하려면 인증 정책을 구성할 때 인증 적용 개체에 인증 프로파일을 할당합니다.
8. 확인을 클릭하고 인증 포털 구성을 커밋합니다.

**STEP 7 |** 다음 단계...

사용자가 서비스 또는 애플리케이션을 요청할 때 인증을 트리거하는 인증 정책 규칙을 구성하기 전까지는 방화벽에 인증 포털 웹 양식이 사용자에게 표시되지 않습니다.

## 터미널 서버 사용자를 위한 사용자 매핑 구성

개별 터미널 서버 사용자는 동일한 IP 주소를 가지고 있는 것으로 보이므로 IP 주소-사용자 이름 매핑은 특정 사용자를 식별하기에 충분하지 않습니다. Windows 기반 터미널 서버에서 특정 사용자를 식별하기 위해 Palo Alto Networks TS 에이전트(터미널 서버 에이전트)는 각 사용자에게 포트 범위를 할당합니다. 그런 다음 TS 에이전트는 할당된 포트 범위에 대해 연결된 모든 방화벽에 알립니다. 이를 통해 방화벽은 IP 주소-포트-사용자 매핑 테이블을 생성하고 사용자 및 그룹 기반 보안 정책 시행을 활성화할 수 있습니다. Windows가 아닌 터미널 서버의 경우 사용자 매핑 정보를 추출하도록 PAN-OS XML API를 구성합니다. 두 방법 모두에 다음 값이 적용됩니다.

- 기본 포트 범위: 1025 ~ 65534
- 사용자당 블록 크기: 200
- 다중 사용자 시스템의 최대 수: 2,500

TS 에이전트가 지원하는 터미널 서버 및 각 방화벽 모델에서 지원되는 TS 에이전트 수에 대한 정보는 Palo Alto Networks 호환성 매트릭스 및 제품 비교 도구를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

다음 섹션에서는 터미널 서버 사용자에 대한 사용자 매핑을 구성하는 방법에 대해 설명합니다.

- 사용자 매핑을 위한 Palo Alto Networks 터미널 서버(TS) 에이전트 구성
- PAN-OS XML API를 사용하여 터미널 서버에서 사용자 매핑 검색

## 사용자 매핑을 위한 **Palo Alto Networks** 터미널 서버**(TS)** 에이전트 구성

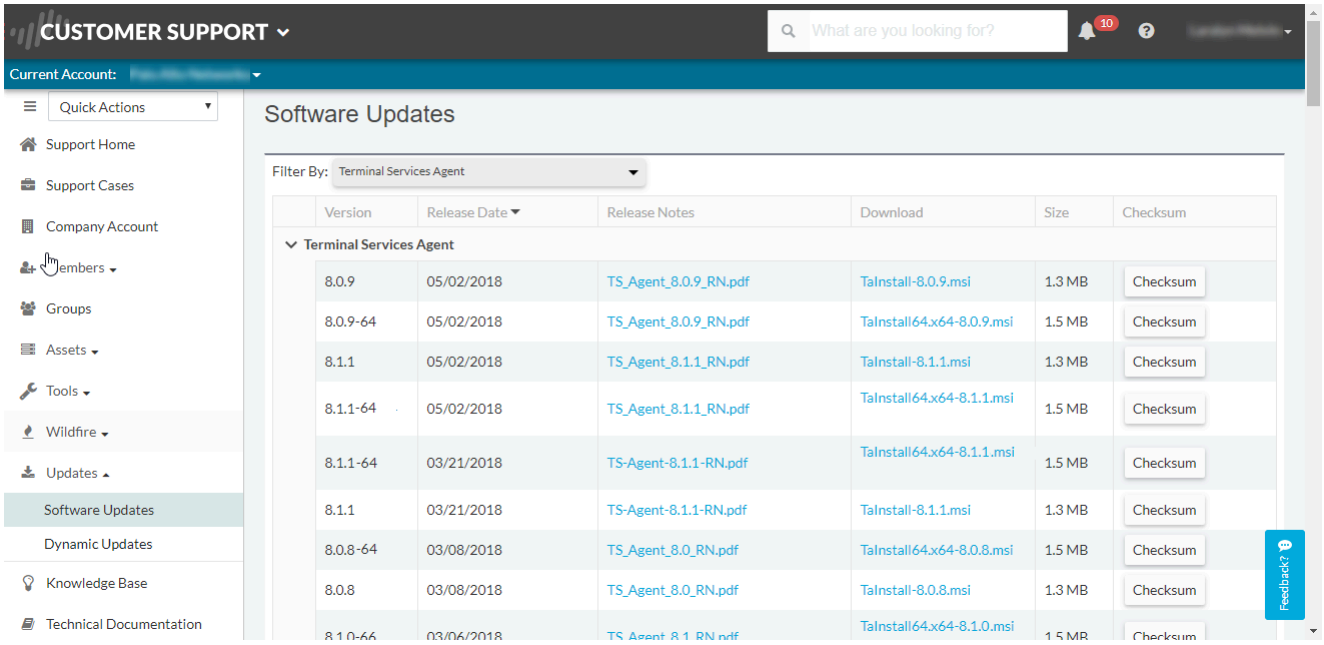
다음 절차에 따라 터미널 서버에 TS 에이전트를 설치 및 구성합니다. 모든 사용자를 매핑하려면 사용자가 로그인하는 모든 터미널 서버에 TS 에이전트를 설치해야 합니다.

***TS*** 에이전트 ***7.0*** 이상의 버전을 사용하는 경우 ***TS*** 에이전트 호스트에서 모든 ***Sophos*** 바이러스 백신 소프트웨어를 비활성화하십시오. 그렇지 않으면 바이러스 백신 소프트웨어가 ***TS*** 에이전트가 할당하는 원본 포트를 덮어씁니다.

기본값, 범위 및 기타 사양에 대한 자세한 내용은 터미널 서버 사용자를 위한 사용자 매핑 구성을(를) 참조하십시오. ***TS*** 에이전트가 지원하는 터미널 서버와 각 방화벽 모델에서 지원하는 ***TS*** 에이전트 수에 대한 정보는 Palo Alto Networks 호환성 매트릭스를 참조하십시오.

**STEP 1 |** TS 에이전트 설치 프로그램을 다운로드합니다.

1. Palo Alto Networks 고객 지원 포털에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택합니다.
3. 필터 기준을 터미널 서비스 에이전트로 설정하고 해당 다운로드 열에서 설치할 에이전트 버전을 선택합니다. 예를 들어 TS 에이전트 9.0을 다운로드하려면 **TaInstall-9.0.msi**를 선택합니다.
4. 에이전트를 설치할 시스템에 `TaInstall.x64-x.x.x-xx.msi` 또는 `TaInstall-x.x.x-xx.msi` 파일을 저장합니다. Windows 시스템이 32비트 또는 64비트 OS를 실행하는지의 여부에 따라 적절한 버전을 선택해야 합니다.




**STEP 2 |** 설치 프로그램을 관리자로 실행합니다.

1. Windows 시작 메뉴를 열고 명령 프롬프트 프로그램을 마우스 오른쪽 버튼으로 클릭한 다음 관리자 권한으로 실행합니다.


©2023 Palo Alto Networks, Inc.

2. 명령줄에서 다운로드한 .msi 파일을 실행합니다. 예를 들어 **TaInstall-9.0.msi** 파일을 바탕 화면에 저장한 경우 다음을 입력합니다.

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>TaInstall-9.0.0-1.msi
```

3. 설치 프롬프트에 따라 기본 설정을 사용하여 에이전트를 설치합니다. 설치 프로그램은 **C:\ProgramFiles\Palo Alto Networks\Terminal Server Agent**에 에이전트를 설치합니다.

   올바른 포트 할당을 확인하려면 기본 터미널 서버 에이전트 설치 폴더 위치를 사용해야 합니다.

4. 설치가 완료되면 설정 대화상자를 닫습니다.

   기존 설치보다 최신 드라이버가 있는 *TS* 에이전트 버전으로 업그레이드하는 경우 설치 마법사는 업그레이드 후 시스템을 재부팅하라는 메시지를 표시합니다.

**STEP 3 |** TS 에이전트가 최종 사용자에게 할당할 포트 범위를 정의합니다.

시스템 소스 포트 할당 범위 및 시스템 예약 소스 포트는 비사용자 세션에 할당되는 포트 범위를 지정합니다. 이 필드의 값이 사용자 트래픽에 대해 지정한 포트와 겹치지 않는지 확인하십시오. 이러한 값은 해당 *Windows* 레지스트리 설정을 편집해야만 변경할 수 있습니다. *TS* 에이전트는 세션 *0*에서 내보낸 네트워크 트래픽에 대해 포트를 할당하지 않습니다.

1. Windows 시작 메뉴를 열고 터미널 서버 에이전트를 선택하여 터미널 서버 에이전트 애플리케이션을 시작합니다.
2. 에이전트를 구성(사이드 메뉴)합니다.
3. 소스 포트 할당 범위를 입력합니다(기본값은 20,000-39,999). TS 에이전트가 사용자 매핑을 위해 할당할 전체 포트 번호 범위입니다. 지정한 포트 범위는 시스템 소스 포트 할당 범위와 겹칠 수 없습니다.
4. (선택 사항) 소스 포트 할당 내에 TS 에이전트가 사용자 세션에 할당하지 않도록 하려는 포트 또는 포트 범위가 있는 경우 예약된 소스 포트로 지정합니다. 여러 범위를 포함하려면 공백 없이 쉼표를 사용합니다(예: **2000-3000,3500,4000-5000**).
5. 터미널 서버에 로그인할 때 각 개별 사용자에게 할당할 포트 수를 지정합니다(사용자당 포트 할당 시작 크기). 기본값은 200입니다.
6. 터미널 서버 에이전트가 개별 사용자에게 할당할 수 있는 최대 포트 수인 사용자당 포트 할당 최대 크기를 지정합니다.
7. 사용자가 할당된 포트가 부족한 경우 사용자의 트래픽 처리를 계속할지 여부를 지정합니다. 사용 가능한 포트가 모두 사용되었을 때 포트 바인딩 실패 옵션은 기본적으로 활성화되어 있으며, 이는 모든 포트가 사용될 때 애플리케이션이 트래픽 전송에 실패함을 나타냅니다. 사용자가 포트가 부족할 때 애플리케이션을 계속 사용할 수 있도록 하려면 이 옵션을 비활성화(해제)하지만 그렇게 하면 이 트래픽이 User-ID로 식별되지 않을 수 있습니다.
8. 터미널 서버를 종료하려고 할 때 응답을 중지하면 종료 시 에이전트 드라이버 분리 옵션을 활성화하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) TS 에이전트와 방화벽 간의 상호 인증을 위해 자체 인증서를 할당합니다.

1. 엔터프라이즈 PKI에서 TS 에이전트용 인증서를 얻거나 방화벽에서 생성합니다. 서버 인증서의 개인 키를 암호화해야 하며 인증서를 PEM 파일 형식으로 업로드해야 합니다. 다음 작업 중 하나를 수행하여 인증서를 업로드합니다.
   - 인증서를 생성하고 내보냅니다.
   - 엔터프라이즈 CA(인증 기관)에서 인증서를 내보냅니다.
2. TS 에이전트에 서버 인증서를 추가합니다.
   1. TS 에이전트에서 서버 인증서 및 새 인증서 추가를 선택합니다.
   2. CA에서 받은 인증서 파일의 경로와 이름을 입력하거나 인증서 파일을 찾습니다.
   3. 개인 키 암호를 입력합니다.
   4. 확인을 클릭합니다.
   5. 변경 사항을 커밋합니다.

   > *TS* 에이전트는 다음 정보와 함께 포트 *5009*에서 자체 서명된 인증서를 사용합니다. 발급자: *CN*=터미널 서버 에이전트, *OU*=엔지니어링, *O=Palo Alto Networks, L=Santa Clara, S*=캘리포니아, *C=US*제목: *CN*=터미널 서버 에이전트, *OU*=엔지니어링, *O=Palo Alto Networks, L*=산타클라라, *S*=캘리포니아, *C*=미국
3. 방화벽에 대한 인증서 프로파일을 구성하고 할당합니다.
   1. 디바이스 > 인증서 관리 > 인증서 프로파일을 선택하여 인증서 프로파일을 구성합니다.

      > *Windows User-ID* 에이전트 및 *TS* 에이전트에 대해 하나의 인증서 프로파일만 할당할 수 있습니다. 따라서 인증서 프로파일에는 연결된 *Windows* 사용자 *ID* 및 *TS* 에이전트에 업로드된 인증서를 발급한 모든 인증 기관이 포함되어야 합니다.
   2. 디바이스 > 사용자 식별 > 연결 보안을 선택합니다.
   3. (⚙)를 편집하고 이전 단계에서 구성한 인증서 프로파일을 사용자 **ID** 인증서 프로파일로 선택합니다.
   4. 확인을 클릭합니다.
   5. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 터미널 서버 에이전트에 연결하도록 방화벽을 구성합니다.

사용자 매핑을 수신하기 위해 터미널 서버 에이전트에 연결하려는 각 방화벽에서 다음 단계를 완료하십시오.

1. 디바이스 > 사용자 식별 > 터미널 서버 에이전트를 선택하고 새 TS 에이전트를 추가합니다.
2. 터미널 서버 에이전트의 이름을 입력합니다.
3. 터미널 서버 에이전트가 설치된 Windows 호스트의 호스트 이름 또는 IP 주소를 입력합니다.

   호스트 이름 또는 IP 주소는 고정 IP 주소로 확인되어야 합니다. 기존 호스트 이름을 변경하면 새 호스트 이름을 확인하기 위해 변경 사항을 커밋할 때 TS 에이전트가 재설정됩니다. 호스트 이름이 여러 IP 주소로 확인되는 경우 TS 에이전트는 목록의 첫 번째 주소를 사용합니다.
4. (선택 사항) 나가는 트래픽의 소스 IP 주소로 나타날 수 있는 대체 **IP** 주소의 호스트 이름 또는 IP 주소를 입력합니다.

   호스트 이름 또는 IP 주소는 고정 IP 주소로 확인되어야 합니다. 최대 8개의 IP 주소 또는 호스트 이름을 입력할 수 있습니다.
5. 에이전트가 사용자 매핑 요청을 수신할 포트 번호를 입력합니다. 이 값은 터미널 서버 에이전트에 구성된 값과 일치해야 합니다. 기본적으로 포트는 방화벽과 에이전트에서 5009로 설정됩니다. 방화벽에서 변경하는 경우 터미널 서버 에이전트 구성 대화 상자의 수신 포트도 동일한 포트로 변경해야 합니다.
6. 구성이 활성화됨인지 확인한 다음 확인을 클릭합니다.
7. 변경 사항을 커밋합니다.
8. 연결됨 상태가 연결된 상태(녹색 표시등)로 표시되는지 확인합니다.

**STEP 6 |** 터미널 서버 에이전트가 IP 주소를 사용자 이름에 성공적으로 매핑하고 방화벽이 에이전트에 연결할 수 있는지 확인합니다.

1. Windows 시작 메뉴를 열고 터미널 서버 에이전트를 선택합니다.
2. 연결 목록에 있는 각 방화벽의 연결 상태가 **연결됨**인지 확인하여 방화벽이 연결할 수 있는지 확인합니다.
3. 터미널 서버 에이전트가 포트 범위를 사용자 이름(사이드 메뉴의 모니터)에 성공적으로 매핑하고 매핑 테이블이 채워져 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** (Windows 2012 R2 서버만 해당) 해당 브라우저를 사용하는 각 사용자에 대해 Microsoft Internet Explorer에서 향상된 보호 모드를 비활성화합니다.

이 작업은 Google Chrome 또는 Mozilla Firefox와 같은 다른 브라우저에서는 필요하지 않습니다.

모든 사용자에 대해 향상된 보호 모드를 비활성화하려면 로컬 보안 정책을 사용하십시오.

Windows Server에서 다음 단계를 수행하십시오.

1. 인터넷 익스플로러를 시작합니다.
2. 설정 > 인터넷 옵션 > 고급을 선택하고 보안 섹션으로 스크롤합니다.
3. 향상된 보호 모드 사용 옵션을 비활성화(지우기)합니다.
4. 확인을 클릭합니다.

*Internet Explorer*에서 *Palo Alto Networks*는 향상된 보호 모드와 다른 보호 모드를 비활성화하지 않을 것을 권장합니다.

## PAN-OS XML API를 사용하여 터미널 서버에서 사용자 매핑 검색

PAN-OS XML API는 표준 HTTP 요청을 사용하여 데이터를 송수신합니다. API 호출은 cURL과 같은 명령 줄 유틸리티에서 직접 수행하거나 RESTful 서비스를 지원하는 스크립팅 또는 애플리케이션 프레임워크를 사용하여 수행할 수 있습니다.

Windows 이외의 터미널 서버가 사용자 매핑 정보를 방화벽에 직접 보낼 수 있도록 하려면 사용자 로그인 및 로그아웃 이벤트를 추출하고 이를 사용하여 PAN-OS XML API 요청 형식에 입력하는 스크립트를 생성합니다. 그런 다음 cURL 또는 wget을 사용하여 XML API 요청을 방화벽에 제출하고 통신 보안을 위해 방화벽의 API 키를 제공하는 메커니즘을 정의합니다. 터미널 서버와 같은 다중 사용자 시스템에서 사용자 매핑을 만들려면 다음 API 메시지를 사용해야 합니다.

- **<multiusersystem>**—방화벽에서 XML API 다중 사용자 시스템에 대한 구성을 설정합니다. 이 메시지는 터미널 서버 IP 주소(해당 터미널 서버의 모든 사용자에 대한 소스 주소)를 정의할 수 있도록 합니다. 또한 **<multiusersystem>** 설정 메시지는 사용자 매핑에 할당할 소스 포트 번호의 범위와 로그인 시 각 개별 사용자에게 할당할 포트 수(블록 크기). 기본 소스 포트 할당 범위(1025-65534)와 블록 크기(200)를 사용하려는 경우 방화벽에 **<multiusersystem>** 설정 이벤트를 보낼 필요가 없습니다. 대신 방화벽은 첫 번째 사용자 로그인 이벤트 메시지를 수신하면 기본 설정을 사용하여 XML API 다중 사용자 시스템 구성을 자동으로 생성합니다.
- **<blockstart>** - 사용자에게 할당된 시작 소스 포트 번호를 나타내기 위해 **<login>** 및 **<logout>** 메시지와 함께 사용됩니다. 그런 다음 방화벽은 블록 크기를 사용하여 로그인 메시지의 IP 주소와 사용자명에 매핑할 포트 번호의 실제 범위를 결정합니다. 예를 들어, **<blockstart>** 값이 13200이고 다중 사용자 시스템에 대해 구성된 블록 크기가 300인 경우 사용자에게 할당된 실제 소스 포트 범위는 13200에서 13499까지입니다. 사용자가 시작한 각 연결은 할당된 범위 내에서 고유한 소스 포트 번호를 사용해야 합니다. 그러면 방화벽이 사용자 및 그룹 기반 보안 규칙을 적용하기 위해 IP 주소-포트-사용자 매핑을 기반으로 사용자를 식별할 수 있습니다. 사용자가 할당된 모든 포트를 모두 소모하면 터미널 서버는 사용자에게 새 **<login>** 포트 범위를 할당하는 새 메시지를 보내야 방화벽이 IP 주소-포트-사용자 매핑을 업데이트할 수 있습니다. 또한 단일 사용자명에 여러 포트 블록을 동시에 매핑할 수 있습니다. 방화벽은 **<blockstart>** 매개변수가 포함된 **<logout>** 메시지를 수신하면 매핑 테이블에서 해당 IP 주소-포트-사용자 매핑을 제거합니다. 방화벽이 사용자 이름과 IP 주소가 포함

 ©2023 Palo Alto Networks, Inc.

된 **<logout>** 메시지를 수신하지만 **<blockstart>**은 수신하지 않으면 테이블에서 사용자를 제거합니다. 또한 방화벽이 IP 주소만 포함된 **<logout>** 메시지를 수신하는 경우 다중 사용자 시스템 및 연결된 모든 매핑을 제거합니다.

터미널 서버가 방화벽으로 보내는 *XML* 파일에는 여러 메시지 유형이 포함될 수 있으며 메시지 순서가 파일 내에서 특정 순서일 필요는 없습니다. 그러나 여러 메시지 유형이 포함된 *XML* 파일을 받으면 방화벽은 다중 사용자 시스템 요청을 먼저 처리한 다음 로그인, 로그아웃 순으로 처리합니다.

다음 워크플로는 PAN-OS XML API를 사용하여 Windows 이외의 터미널 서버에서 방화벽으로 사용자 매핑을 보내는 방법의 예를 제공합니다.

**STEP 1 |** 방화벽과 터미널 서버 간의 API 통신을 인증하는 데 사용할 API 키를 생성합니다. 키를 생성하려면 관리 계정에 대한 로그인 자격 증명을 제공해야 합니다. 이 API는 XML API 권한이 활성화된 역할 기반 관리자를 포함하여 모든 관리자가 사용할 수 있습니다.

암호의 특수 문자는 *URL/* 백분율로 인코딩되어야 합니다.

브라우저에서 방화벽에 로그인합니다. 그런 다음 방화벽에 대한 API 키를 생성하려면 새 브라우저 창을 열고 다음 URL을 입력합니다.

```
https://<Firewall-IPaddress>/api/?
type=keygen&user=<username>&password=<password>
```

여기서 **<Firewall-IPaddress>**은(는) 방화벽의 IP 주소 또는 FQDN이고 **<username>** 및 **<password>**은(는) 방화벽의 관리 사용자 계정에 대한 자격 증명입니다. . 예:

```
https://10.1.2.5/api/?type=keygen&user=admin&password=admin
```

방화벽이 키를 포함하는 메시지로 응답합니다. 예를 들면 다음과 같습니다.

```
<response status="success">    <result>
       <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
    </result> </response>
```


©2023 Palo Alto Networks, Inc.

**STEP 2 |** (선택 사항) 터미널 서버 에이전트가 사용하는 사용자당 포트 범위와 블록 크기를 지정하기 위해 터미널 서버가 보낼 설정 메시지를 생성합니다.

터미널 서버 에이전트가 설치 메시지를 보내지 않으면 방화벽은 첫 번째 로그인 메시지를 수신하면 다음 기본 설정을 사용하여 자동으로 터미널 서버 에이전트 구성을 생성합니다.

- 기본 포트 범위: 1025 ~ 65534
- 사용자당 블록 크기: 200
- 다중 사용자 시스템의 최대 수: 1,000

다음은 샘플 설정 메시지를 보여 줍니다.

```
<uid-message> <payload> <multiusersystem> <entry ip="10.1.1.23"
 startport="20000"          endport="39999" blocksize="100/"> </
multiusersystem> </payload> <type>업데이트</type> <version>1.0</
version> </uid-message>
```

여기서 **entry ip**은 터미널 서버 사용자에게 할당된 IP 주소를 지정하고, **startport** 및 **endport**는 개별 사용자에게 포트를 할당할 때 사용할 포트 범위를 지정하고, **blocksize**는 각 사용자에게 할당할 포트 수를 지정합니다. 최대 블록 크기는 4000이며 각 다중 사용자 시스템은 최대 1000개의 블록을 할당할 수 있습니다.

사용자 정의 블록 크기 및 포트 범위를 정의하는 경우 범위 내의 모든 포트가 할당되고 인터벌이나 사용되지 않는 포트가 없도록 값을 구성해야 합니다. 예를 들어 포트 범위를 1000—1499로 설정하면 블록 크기를 200이 아닌 100으로 설정할 수 있습니다. 이는 200으로 설정하면 범위 끝에 사용되지 않는 포트가 있기 때문입니다.

**STEP 3 |** 로그인 이벤트를 추출하는 스크립트를 생성하고 방화벽으로 보낼 XML 입력 파일을 생성합니다.

스크립트에서 포트 중복 없이 고정된 경계에서 포트 번호 범위 할당을 적용해야 합니다. 예를 들어, 포트 범위가 1000—1999이고 블록 크기가 200인 경우 허용되는 블록 시작 값은 1000, 1200, 1400, 1600 또는 1800이 됩니다. 1001, 1300 또는 1850의 블록스타트 값은 해당 범위의 포트 번호 중 일부가 사용되지 않는 상태로 남아 있기 때문에 허용되지 않습니다.



터미널 서버가 방화벽으로 보내는 로그인 이벤트 페이로드에는 여러 로그인 이벤트가 포함될 수 있습니다.

다음은 PAN-OS XML 로그인 이벤트의 입력 파일 형식을 보여 줍니다.

```
<uid-message> <payload> <login> <entry name="acme\jjaso"
 ip="10.1.1.23" blockstart="20000"> <entry name="acme\jparker"
 ip="10.1.1.23" blockstart="20100"> <entry name="acme\ccrisp"
```

 ©2023 Palo Alto Networks, Inc.

```
 ip="10.1.1.23" blockstart="21000"> </login> </payload> <type>업데이
트</type> <version>1.0</version> </uid-message>
```

방화벽은 이 정보를 사용하여 사용자 매핑 테이블을 채웁니다. 위 예에서 추출한 매핑을 기반으로 방화벽이 소스 주소와 포트가 10.1.1 23:20101인 패킷을 수신한 경우 정책 적용을 위해 요청을 사용자 jparker에 매핑합니다.

각 다중 사용자 시스템은 최대 *1,000*개의 포트 블록을 할당할 수 있습니다.

**STEP 4 |** 로그아웃 이벤트를 추출하는 스크립트를 생성하고 방화벽으로 보낼 XML 입력 파일을 생성합니다.

`blockstart` 매개 변수가 포함된 `로그아웃` 이벤트 메시지를 수신하면 방화벽은 해당 IP 주소-포트-사용자 매핑을 제거합니다. `로그아웃` 메시지에 사용자명과 IP 주소가 포함되어 있지만 `blockstart` 매개 변수는 없는 경우 방화벽은 사용자에 대한 모든 매핑을 제거합니다. `로그아웃` 메시지에 IP 주소만 포함된 경우 방화벽은 다중 사용자 시스템 및 모든 관련 매핑을 제거합니다.

다음은 PAN-OS XML 로그아웃 이벤트의 입력 파일 형식을 보여 줍니다.

```
<uid-message> <payload> <logout> <entry name="acme\jjaso"
 ip="10.1.1.23" blockstart="20000"> <entry name="acme\ccrisp"
 ip="10.1.1.23"> <entry ip="10.2.5.4"> </logout> </payload>
 <type>업데이트</type> <version>1.0</version> </uid-message>
```

다음 *CLI* 명령을 사용하여 방화벽에서 다중 사용자 시스템 항목을 지울 수도 있습니다:
***xml-api*** `다중 사용자 시스템 지우기`

**STEP 5 |** 작성한 스크립트에 XML API를 사용하여 할당된 포트 블록 범위가 터미널 서버의 사용자에게 할당된 실제 소스 포트와 일치하고 사용자가 로그아웃하거나 포트 할당이 변경될 때 매핑이 제거되도록 동적으로 적용하는 방법이 포함되어 있는지 확인합니다.

이를 수행하는 한 가지 방법은 netfilter NAT 규칙을 사용하여 uid를 기반으로 XML API를 통해 할당된 특정 포트 범위 뒤에 사용자 세션을 숨기는 것입니다. 예를 들어 사용자 ID jjaso를 가진 사용자가 SNAT(소스 네트워크 주소 변환) 값 10.1.1에 매핑되도록 하려면 23:20000-20099 만드는 스크립트에 다음이 포함되어야 합니다.

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner
 jjaso -p tcp -j SNAT --to-source 10.1.1.23:20000-20099
```

마찬가지로 만든 스크립트는 사용자가 로그아웃하거나 포트 할당이 변경될 때 IP 테이블 라우팅 구성이 SNAT 매핑을 동적으로 제거하도록 해야 합니다.

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 방화벽으로 전송하기 위해 설정, 로그인 및 로그아웃 이벤트가 포함된 XML 입력 파일을 wget 또는 cURL 메시지로 패키징하는 방법을 정의합니다.

**wget**을 사용하여 방화벽에 파일을 적용하려면 다음과 같이 하십시오**.**

```
> wget --post file <filename>  “https://<Firewall-
IPaddress>/api/?type=user-id&key=<key>&file-
name=<input_filename.xml>&client=wget&vsys=<VSYS_name>”
```

예를 들어, wget을 사용하여 **k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg** 키를 사용하여 10.2.5.11에 있는 방화벽에 login.xml이라는 입력 파일을 보내는 구문은 다음과 같습니다.

```
> wget --post file login.xml  “https://10.2.5.11/api/?type=user-
id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&file-
name=login.xml&client=wget&vsys=vsys1”
```

**cURL**을 사용하여 방화벽에 파일을 적용하려면 다음과 같이 하십시오**.**

```
> curl --form file=@<filename> https://<Firewall-IPaddress>/api/?
type=user-id&key=<key>&vsys=<VSYS_name>
```

예를 들어, cURL을 사용하여 **k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg** 키를 사용하여 10.2.5.11에 있는 방화벽에 login.xml이라는 입력 파일을 보내는 구문은 다음과 같습니다.

```
> curl --form file@login.xml  “https://10.2.5.11/api/?type=user-
id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&vsys=vsys1”
```

**STEP 7 |** 방화벽이 터미널 서버로부터 로그인 이벤트를 성공적으로 수신하고 있는지 확인합니다.

방화벽에 대한 SSH 연결을 열고 다음 CLI 명령을 실행하여 구성을 확인합니다.

터미널 서버가 **XML**을 통해 방화벽에 연결되어 있는지 확인하려면**:**

```
admin@PA-5250> show user xml-api multiusersystem Host Vsys
 Users Blocks ----------------------------------------
 10.5.204.43   vsys1      5         2
```

방화벽이 **XML**을 통해 터미널 서버로부터 매핑을 받고 있는지 확인하려면 다음과 같이 하십시오**.**

```
admin@PA-5250> show user ip-port-user-mapping all Global max host
 index 1, host hash count 1 XML API Multi-user System 10.5.204.43
 Vsys 1, Flag 3 Port range: 20000 - 39999 Port size: start 200;
 max 2000 Block count 100, port count 20000 20000-20199: acme
\administrator Total host: 1
```

## XML API를 사용하여 사용자 매핑을 사용자 ID로 보내기

User-ID는 사용자 매핑 정보를 얻기 위한 여러 가지 기본 제공 방법을 제공합니다. 그러나 사용자 정보를 캡처하지만 기본적으로 User-ID와 통합할 수 없는 애플리케이션이나 디바이스가 있을 수 있습니다. 예를 들어 내부적으로 개발된 사용자 정의 애플리케이션이나 표준 사용자 매핑 방법이 지원하지 않는 디바이

 ©2023 Palo Alto Networks, Inc.

스가 있을 수 있습니다. 이러한 경우 PAN-OS XML API를 사용하여 정보를 PAN-OS 통합 User-ID 에이전트 또는 방화벽으로 직접 보내는 사용자 지정 스크립트를 만들 수 있습니다. PAN-OS XML API는 표준 HTTP 요청을 사용하여 데이터를 송수신합니다. API 호출은 cURL과 같은 명령줄 유틸리티에서 직접 수행하거나 POST 및 GET 요청을 지원하는 스크립팅 또는 애플리케이션 프레임워크를 사용하여 수행할 수 있습니다.

외부 시스템에서 사용자 매핑 정보를 PAN-OS 통합 User-ID 에이전트에 보낼 수 있도록 하려면 사용자 로그인 및 로그아웃 이벤트를 추출하는 스크립트를 생성하고 해당 이벤트를 PAN-OS XML API 요청에 대한 입력으로 사용합니다. 그런 다음 XML API 요청을 방화벽에 제출하는 메커니즘을 정의하고(예: cURL 사용) 방화벽의 API 키를 사용하여 통신 보안을 수행합니다. 자세한 내용은 PAN-OS XML API 사용 가이드를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 사용자 및 그룹 기반 정책 활성화

사용자 ID를 활성화한 후 특정 사용자 및 그룹에 적용되는 보안 정책을 구성할 수 있습니다. 사용자 기반 정책 제어에는 애플리케이션 정보(어떤 카테고리 및 하위 카테고리에 속하는지, 기본 기술 또는 애플리케이션 속성이 무엇인지 포함)도 포함될 수 있습니다. 아웃바운드 또는 인바운드 방향에서 사용자 또는 사용자 그룹을 기반으로 애플리케이션을 안전하게 사용하도록 정책 규칙을 정의할 수 있습니다.

사용자 기반 정책의 예는 다음과 같습니다.

- IT 부서만 표준 포트에서 SSH, 텔넷 및 FTP와 같은 도구를 사용할 수 있도록 합니다.
- 헬프 데스크 서비스 그룹이 Slack을 사용하도록 허용합니다.
- 모든 사용자가 Facebook을 읽을 수 있도록 허용하지만 Facebook 앱 사용을 차단하고 마케팅 직원에게 게시를 제한합니다.

 ©2023 Palo Alto Networks, Inc.

# 계정이 여러 개인 사용자를 위한 정책 사용

조직의 사용자에게 여러 책임이 있는 경우 해당 사용자는 여러 사용자 이름(계정)을 가질 수 있습니다. 각 사용자 이름(계정)은 특정 서비스 세트에 액세스할 수 있는 고유한 권한을 가지지만 모든 사용자 이름은 동일한 IP 주소(사용자의 클라이언트 시스템)를 공유합니다. 그러나 User-ID 에이전트는 정책을 적용하기 위해 하나의 IP 주소(또는 터미널 서버 사용자의 경우 IP 주소 및 포트 범위)를 하나의 사용자 이름에만 매핑할 수 있으며 에이전트가 매핑할 사용자 이름을 예측할 수 없습니다. 사용자의 모든 사용자 이름에 대한 액세스를 제어하려면 규칙, 사용자 그룹 및 User-ID 에이전트를 조정해야 합니다.

예를 들어 방화벽에 사용자 이름 corp_user가 전자 메일에 액세스하도록 허용하는 규칙과 admin_user 사용자 이름이 MySQL 서버에 액세스하도록 허용하는 규칙이 있다고 가정합니다. 사용자는 동일한 클라이언트 IP 주소의 사용자 이름 중 하나로 로그인합니다. User-ID 에이전트가 IP 주소를 corp_user에 매핑하면 사용자가 corp_user 또는 admin_user로 로그인하는지의 여부와 관계없이 방화벽은 해당 사용자를 corp_user로 식별하고 전자 메일에 대한 액세스는 허용하지만 MySQL 서버에는 액세스하지 않습니다. 반면 User-ID 에이전트가 IP 주소를 admin_user에 매핑하면 방화벽은 로그인에 관계없이 항상 사용자를 admin_user로 식별하고 이메일이 아닌 MySQL 서버에 대한 액세스를 허용합니다. 다음 단계에서는 이 예에서 두 규칙을 모두 적용하는 방법을 설명합니다.

**STEP 1 |** 고유한 액세스 권한이 필요한 각 서비스에 대해 사용자 그룹을 구성합니다.

이 예에서 각 그룹은 단일 서비스(이메일 또는 MySQL 서버)에 사용됩니다. 그러나 동일한 권한이 필요한 서비스 집합에 대해 각 그룹을 구성하는 것이 일반적입니다(예: 모든 기본 사용자 서비스에 대해 하나의 그룹, 모든 관리 서비스에 대해 하나의 그룹).

사용자가 필요로 하는 서비스에 액세스할 수 있는 사용자 그룹이 조직에 이미 있는 경우 덜 제한된 서비스에 사용되는 사용자 이름을 해당 그룹에 추가하기만 하면 됩니다. 이 예에서 전자 메일 서버는 MySQL 서버보다 덜 제한된 액세스가 필요하며 corp_user는 전자 메일에 액세스하기 위한 사용자 이름입니다. 따라서 전자 메일에 액세스할 수 있는 그룹(corp_employees)과 MySQL 서버에 액세스할 수 있는 그룹(네트워크 서비스)에 corp_user를 추가합니다.

특정 기존 그룹에 사용자 이름을 추가하는 것이 조직의 관행을 위반하는 경우 LDAP 필터를 기반으로 사용자 지정 그룹을 만들 수 있습니다. 이 예에서는 network_services가 다음과 같이 구성하는 사용자 지정 그룹이라고 가정합니다.

1. 디바이스 > 사용자 식별 > 그룹 매핑 설정을 선택한 다음 고유한 이름을 가진 그룹 매핑 구성을 추가합니다.
2. LDAP 서버 프로파일을 선택한 다음 사용 체크박스가 활성화되어 있는지 확인합니다.
3. 사용자 지정 그룹 탭을 선택한 다음 network_services가 있는 사용자 지정 그룹을 이름으로 추가합니다.
4. corp_user의 LDAP 속성과 일치하는 **LDAP** 필터를 지정하고 확인을 클릭합니다.
5. 확인 및 커밋을 클릭합니다.



나중에 덜 제한된 서비스를 위해 그룹에 속한 다른 사용자에게 더 제한된 서비스에 액세스하는 추가 사용자 이름이 주어지면 더 제한된 서비스를 위해 해당 사용자 이름을 그룹에 추가할 수 있습니다. 이 시나리오는 반대의 경우보다 더 일반적입니다. 더 제한된 서비스에 대한 액세스 권한을 가진 사용자는 일반적으로 이미 덜 제한된 서비스에 액세스할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방금 구성한 그룹을 기반으로 사용자 액세스를 제어하는 규칙을 구성합니다.

자세한 내용은 사용자 및 그룹 기반 정책 적용 사용을 참조하십시오.

1. corp_employees 그룹이 전자 메일에 액세스할 수 있도록 허용하는 보안 규칙을 구성합니다.
2. network_services 그룹이 MySQL 서버에 액세스할 수 있도록 허용하는 보안 규칙을 구성합니다.

**STEP 3 |** User-ID 에이전트의 무시 목록을 구성합니다.

이렇게 하면 User-ID 에이전트가 클라이언트 IP 주소를 방금 구성한 규칙에 할당된 그룹의 구성원인 사용자 이름에만 매핑합니다. 무시 목록에는 해당 그룹의 구성원이 아닌 사용자의 모든 사용자 이름이 포함되어야 합니다.

이 예에서는 Windows 기반 User-ID 에이전트의 무시 목록에 admin_user를 추가하여 클라이언트 IP 주소를 corp_user에 매핑하도록 합니다. 이렇게 하면 사용자가 corp_user로 로그인하든 admin_user로 로그인하든 방화벽이 사용자를 corp_user로 식별하고 corp_user가 규칙이 참조하는 그룹의 구성원이기 때문에 사용자가 구성한 두 규칙을 모두 적용합니다.

1. **`ignore_user_list.txt`** 파일을 만듭니다.
2. 파일을 열고 admin_user를 추가합니다.

   나중에 더 많은 사용자 이름을 추가할 경우 각각 별도의 줄에 있어야 합니다.
3. 에이전트가 설치된 도메인 서버의 User-ID 에이전트 폴더에 파일을 저장합니다.

> ***PAN-OS** 통합 **User-ID** 에이전트를 사용하는 경우 무시 목록을 구성하는 방법에 대한 지침은 PAN-OS 통합 User-ID 에이전트를 사용하여 사용자 매핑 구성을 참조하십시오.*

**STEP 4 |** 제한된 서비스에 대한 엔드포인트 인증을 구성합니다.

이를 통해 엔드포인트는 사용자의 자격 증명을 확인하고 여러 사용자 이름을 가진 사용자가 액세스할 수 있도록 하는 기능을 유지할 수 있습니다.

이 예에서는 network_services 그룹의 구성원인 corp_user가 MySQL 서버에 서비스 요청을 보내도록 허용하는 방화벽 규칙을 구성했습니다. 이제 인증된 사용자 이름(admin_user)의 로그인 자격 증명을 입력하라는 메시지를 표시하여 권한이 없는 사용자 이름(예: corp_user)에 응답하도록 MySQL 서버를 구성해야 합니다.

> *사용자가 **admin_user**로 네트워크에 로그인하면 **admin_user** 자격 증명을 다시 입력하라는 메시지를 표시하지 않고도 **MySQL** 서버에 액세스할 수 있습니다.*

이 예에서 corp_user와 admin_user는 모두 전자 메일 계정을 가지고 있으므로 전자 메일 서버는 사용자가 네트워크에 로그인할 때 입력한 사용자 이름에 관계없이 추가 자격 증명을 요구하지 않습니다.

이제 방화벽이 여러 사용자 이름을 가진 사용자에 대해 규칙을 적용할 준비가 되었습니다.


©2023 Palo Alto Networks, Inc.

# 사용자 ID 구성 확인

사용자 및 그룹 매핑을 구성하고 보안 정책에서 User-ID를 활성화하고 인증 정책을 구성한 후 User-ID가 제대로 작동하는지 확인해야 합니다.

**STEP 1 |** 방화벽 CLI에 액세스합니다.

**STEP 2 |** 그룹 매핑이 작동하는지 확인합니다.

CLI에서 다음 작업 명령을 입력합니다.

```
> show user group-mapping statistics
```

**STEP 3 |** 사용자 매핑이 작동하는지 확인합니다.

PAN-OS 통합 User-ID 에이전트를 사용하는 경우 다음 명령을 사용하여 CLI에서 이를 확인할 수 있습니다.

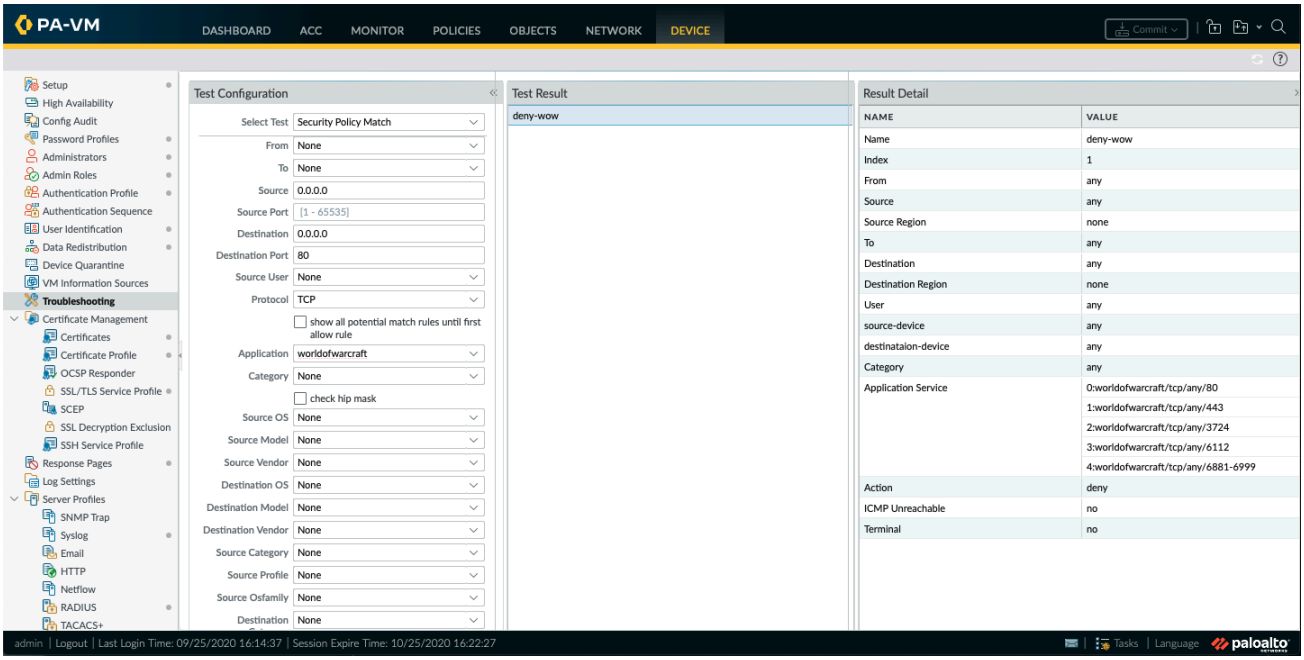
```
> show user ip-user-mapping-mp all
 IP              Vsys  From  User         Timeout (sec)
 ------------------------------------------------------
 192.168.201.1 vsys1 UIA   acme\george            210
 192.168.201.11 vsys1 UIA   acme\duane             210
 192.168.201.50 vsys1 UIA   acme\betsy             210
 192.168.201.10 vsys1 UIA   acme\administrator     210
 192.168.201.100 vsys1 AD    acme\administrator     748 Total: 5
 users *: WMI probe succeeded
```


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 보안 정책 규칙을 테스트합니다.

- User-ID가 활성화된 영역의 시스템에서 사이트 및 애플리케이션에 액세스하여 정책에 정의한 규칙을 테스트하고 트래픽이 예상대로 허용 및 거부되는지 확인합니다.
- 실행 중인 구성의 문제를 해결하여 정책이 올바르게 구성되었는지 확인할 수도 있습니다. 예를 들어 사용자가 월드 오브 워크래프트를 플레이하지 못하도록 차단하는 규칙이 있다고 가정합니다. 다음과 같이 정책을 테스트할 수 있습니다.

  1. 디바이스 > 문제 해결을 선택하고 테스트 선택 드롭다운에서 보안 정책 일치를 선택합니다.
  2. 소스 및 대상 IP 주소로 **0.0.0.0**을 입력합니다. 그러면 모든 소스 및 대상 IP 주소에 대해 정책 일치 테스트가 실행됩니다.
  3. 대상 포트를 입력합니다.
  4. 프로토콜을 입력합니다.
  5. 보안 정책 일치 테스트를 실행합니다.




**STEP 5 |** 인증 정책 및 인증 포털 구성을 테스트합니다.

1. 동일한 영역에서 Mac OS 시스템과 같이 디렉터리의 구성원이 아닌 시스템으로 이동하고 영역 외부의 시스템에 핑(ping)을 시도합니다. ping은 인증 없이 작동해야 합니다.
2. 동일한 시스템에서 브라우저를 열고 정의한 인증 규칙과 일치하는 대상 영역의 웹사이트로 이동합니다. 인증 포털 웹 양식이 표시되고 로그인 자격 증명을 묻는 메시지가 표시되어야 합니다.
3. 올바른 자격 증명을 사용하여 로그인하고 요청한 페이지로 리디렉션되었는지 확인합니다.
4. 다음과 같이 **test authentication-policy-match** 작동 명령을 사용하여 인증 정책을 테스트할 수도 있습니다.

```
> test authentication-policy-match from corporate to internet
 source 192.168.201.10 destination 8.8.8.8  Matched rule:
 'authentication portal' action: web-form
```


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 로그 파일에 사용자 이름이 표시되는지 확인합니다.

로그 페이지(**Monitor** > **Logs** > **Traffic** 등)를 선택한 다음 소스 사용자 열에 사용자 이름이 표시되는지 확인합니다.

**STEP 7 |** 보고서에 사용자 이름이 표시되는지 확인합니다.

1. 모니터 > 보고서를 선택합니다.
2. 사용자 이름이 포함된 보고서 유형을 선택합니다. 예를 들어 거부된 애플리케이션 보고서의 소스 사용자 열에는 애플리케이션에 액세스를 시도한 사용자 목록이 표시되어야 합니다.


©2023 Palo Alto Networks, Inc.

# 대규모 네트워크에 사용자 ID 배포

대규모 네트워크에는 방화벽이 쿼리하여 IP 주소를 사용자 이름에 매핑하고 사용자 이름을 사용자 그룹에 매핑하는 수백 개의 정보 소스가 있을 수 있습니다. User-ID 에이전트에서 사용자 매핑 및 그룹 매핑 정보를 수집하기 전에 사용자 매핑 및 그룹 매핑 정보를 집계하여 이러한 네트워크에 대한 User-ID 관리를 단순화하여 필요한 에이전트 수를 줄일 수 있습니다.

대규모 네트워크에는 매핑 정보를 사용하여 정책을 적용하는 수많은 방화벽이 있을 수도 있습니다. 직접 쿼리하는 대신 재배포를 통해 매핑 정보를 획득하도록 일부 방화벽을 구성하면 방화벽 및 정보 소스가 쿼리 프로세스에서 사용하는 리소스를 줄일 수 있습니다. 또한 재배포를 통해 사용자가 로컬 소스(예: 지역 디렉터리 서비스)에 의존하지만 원격 서비스 및 애플리케이션(예: 글로벌 데이터 센터 애플리케이션)에 액세스해야 하는 경우 방화벽에서 사용자 기반 정책을 적용할 수 있습니다.

인증 정책 구성을(를) 하는 경우 방화벽은 인증 질문에 대한 사용자 응답과 관련된 인증 타임스탬프도 재배포해야 합니다. 방화벽은 타임스탬프를 사용하여 인증 정책 규칙의 타임아웃을 평가합니다. 타임아웃를 사용하면 인증에 성공한 사용자가 나중에 제한 시간 내에 다시 인증하지 않고도 서비스 및 애플리케이션을 요청할 수 있습니다. 타임스탬프를 재배포하면 처음에 사용자에게 액세스 권한을 부여하는 방화벽이 나중에 해당 사용자에 대한 액세스를 제어하는 방화벽과 동일하지 않더라도 각 사용자에 대해 일관된 타임아웃를 적용할 수 있습니다.

여러 가상 시스템을 구성한 경우 가상 시스템을 User-ID 허브로 선택하여 가상 시스템 간에 IP 주소와 사용자 이름 매핑 정보를 공유할 수 있습니다.

- 수많은 매핑 정보 소스에 대한 사용자 ID 배포
- 데이터 및 인증 타임스탬프 재배포
- 가상 시스템 전체에서 사용자 ID 매핑 공유

## 수많은 매핑 정보 소스에 대한 사용자 ID 배포

Windows 로그 포워딩 및 글로벌 카탈로그 서버를 사용하여 Microsoft AD(Active Directory) 도메인 컨트롤러 또는 Exchange 서버의 대규모 네트워크에서 사용자 매핑 및 그룹 매핑을 단순화할 수 있습니다. 이러한 방법은 User-ID 에이전트가 매핑 정보를 수집하기 전에 매핑 정보를 집계하여 User-ID 관리를 단순화하여 필요한 에이전트 수를 줄입니다.

- Windows 로그 포워딩 및 글로벌 카탈로그 서버
- 대규모 사용자 ID 배포 계획
- Windows 로그 포워딩 구성
- 수많은 매핑 정보 소스에 대한 사용자 ID 구성

### Windows 로그 포워딩 및 글로벌 카탈로그 서버

각 User-ID 에이전트는 최대 100개의 서버를 모니터링할 수 있으므로 방화벽에는 수백 개의 AD 도메인 컨트롤러 또는 Exchange 서버가 있는 네트워크를 모니터링하려면 여러 User-ID 에이전트가 필요합니다. 수많은 User-ID 에이전트를 만들고 관리하려면, 특히 새 도메인 컨트롤러를 추적하기 어려운 네트워크를 확장하는 경우 상당한 관리 오버헤드가 수반됩니다. Windows 로그 포워딩을 사용하면 모니터링할 서버 수를 줄여 관리할 User-ID 에이전트 수를 줄여 관리 오버헤드를 최소화할 수 있습니다. Windows 로그 포

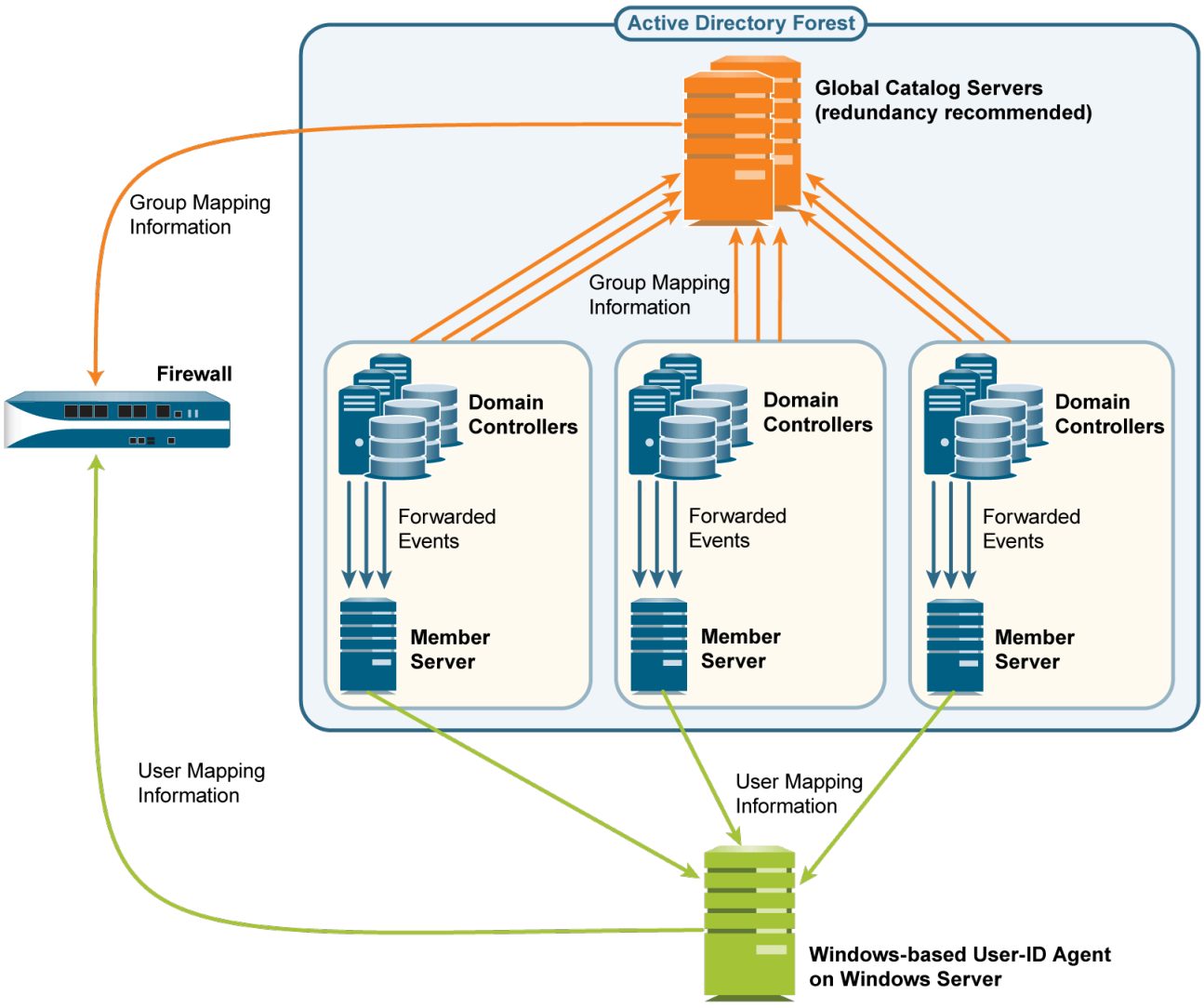
 ©2023 Palo Alto Networks, Inc.

워딩을 구성하면 여러 도메인 컨트롤러가 User-ID 에이전트가 사용자 매핑 정보를 수집하는 단일 도메인 구성원으로 로그인 이벤트를 내보냅니다.

윈도우 서버 버전 *2012* 및 *2012 R2*에 대한 윈도우 로그 포워딩을 구성할 수 있습니다. *Windows* 로그 포워딩은 타사 서버에서는 사용할 수 없습니다.

대규모 네트워크에서 그룹 매핑 정보를 수집하려면 도메인 컨트롤러에서 계정 정보를 받는 글로벌 카탈로그 서버를 쿼리하도록 방화벽을 구성할 수 있습니다.

다음 그림에서는 방화벽이 Windows 기반 User-ID 에이전트를 사용하는 대규모 네트워크의 사용자 매핑 및 그룹 매핑을 보여 줍니다. 이 배치가 네트워크에 적합한지 확인하려면 대규모 사용자 ID 배포 계획을(를) 참고하십시오.




## 대규모 사용자 ID 배포 계획

사용자 ID 구현에 Windows 로그 포워딩 및 글로벌 카탈로그 서버를 사용할지의 여부를 결정할 때 시스템 관리자에게 문의하여 다음을 결정하십시오.


©2023 Palo Alto Networks, Inc.

- 도메인 컨트롤러가 로그인 이벤트를 구성원 서버로 포워딩하는 데 필요한 대역폭입니다. 대역폭은 도메인 컨트롤러의 로그인 속도(분당 로그인 수)와 각 로그인 이벤트의 바이트 크기의 배수입니다.

  도메인 컨트롤러는 전체 보안 로그를 포워딩하지 않고 로그인당 사용자 매핑 프로세스에 필요한 이벤트(Windows Server 2012 및 MS Exchange용 이벤트 4개)만 포워딩합니다.
- 다음 네트워크 요소가 필요한 대역폭을 지원하는지의 여부:
  - 도메인 컨트롤러 - 이벤트 포워딩과 관련된 처리 부하를 지원해야 합니다.
  - 구성원 서버 - 이벤트 수신과 관련된 처리 부하를 지원해야 합니다.
  - 연결 - 도메인 컨트롤러, 구성원 서버 및 글로벌 카탈로그 서버의 지리적 분포(로컬 또는 원격)는 요인입니다. 일반적으로 원격 배포는 더 적은 대역폭을 지원합니다.

### Windows 로그 포워딩 구성

Windows 로그 포워딩을 구성하려면 Windows 서버에서 그룹 정책을 구성할 수 있는 관리자 권한이 필요합니다. 도메인 컨트롤러에서 로그인 이벤트를 수집하는 구성원 서버인 모든 ***Windows*** 이벤트 수집기에서 Windows 로그 포워딩을 구성합니다. 다음은 작업의 개요입니다. 특정 단계는 Windows Server 설명서를 참조하십시오.

**STEP 1 |** 각 Windows 이벤트 수집기에서 이벤트 수집을 사용하도록 설정하고 도메인 컨트롤러를 이벤트 원본으로 추가하고 이벤트 컬렉션 쿼리(구독)를 구성합니다. 구독에서 지정하는 이벤트는 도메인 컨트롤러 플랫폼에 따라 다릅니다.

- 윈도우 서버 **2012(R2** 포함**)** 및 **2016** 또는 **MS** 익스체인지 - 필수 이벤트의 이벤트 ID는 4768(인증 티켓 부여됨), 4769(서비스 티켓 부여됨), 4770(티켓이 갱신됨) 및 4624(로그온 성공)입니다.

  가능한 한 빨리 이벤트를 포워딩하려면 구독을 구성할 때 지연 시간을 최소화합니다.

User-ID 에이전트는 포워딩된 기본 이벤트 위치가 아니라 Windows 이벤트 수집기의 보안 로그를 모니터링합니다. 이벤트 로깅 경로를 보안 로그로 변경하려면 각 Windows 이벤트 수집기에서 다음 단계를 수행하십시오.

1. 이벤트 뷰어를 엽니다.
2. 보안 로그를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. 로그 경로(기본값 **%SystemRoot%\System32\Winevt\Logs\security.evtx**)를 복사하고 확인을 클릭합니다.
4. 포워딩된 이벤트 폴더를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
5. 보안 로그의 값을 붙여 넣어 기본 로그 경로(**%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx**)를 바꾼 다음 **[**확인**]**을 클릭합니다.

**STEP 2 |** 도메인 컨트롤러에서 WinRM(Windows 원격 관리)을 사용하도록 그룹 정책을 구성합니다.

**STEP 3 |** 도메인 컨트롤러에서 Windows 이벤트 포워딩을 사용하도록 그룹 정책을 구성합니다.

## 수많은 매핑 정보 소스에 대한 사용자 **ID** 구성

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 로그인 이벤트를 수집하는 멤버 서버에서 Windows 로그 포워딩을 구성합니다.

Windows 로그 포워딩을 구성합니다. 이 단계에서는 Windows 서버에서 그룹 정책을 구성하기 위한 관리 권한이 필요합니다.

**STEP 2 |** Windows 기반 User-ID 에이전트를 설치합니다.

구성원 서버에 액세스할 수 있는 Windows 서버에 Windows 기반 User-ID 에이전트를 설치합니다. User-ID 에이전트를 호스팅하는 시스템이 모니터링할 서버와 동일한 도메인의 구성원인지 확인합니다.

**STEP 3 |** User-ID 에이전트를 구성하여 구성원 서버에서 사용자 매핑 정보를 수집합니다.

1. Windows 기반 User-ID 에이전트를 시작합니다.
2. 사용자 식별 > 검색을 선택하고 도메인 컨트롤러에서 이벤트를 수신할 각 구성원 서버에 대해 다음 단계를 수행합니다.
   1. 서버 섹션에서 이름 추가를 클릭하고 이름을 입력하여 구성원 서버를 식별합니다.
   2. 서버 주소 필드에 구성원 서버의 FQDN 또는 IP 주소를 입력합니다.
   3. 서버 유형의 경우 **Microsoft** 활성 디렉터리를 선택합니다.
   4. 확인을 클릭하여 서버 항목을 저장합니다.
3. 나머지 User-ID 에이전트 설정을 구성합니다(사용자 매핑을 위한 Windows 기반 User-ID 에이전트 구성 참조).
4. 사용자 ID 소스가 여러 형식의 사용자 이름을 제공하는 경우 사용자를 그룹으로 매핑합니다.할 때 기본 사용자 이름 형식을 지정합니다.

   기본 사용자 이름은 방화벽에서 사용자를 식별하고 사용자 ID 소스가 제공하는 형식에 관계없이 보고서 및 로그에서 사용자를 나타내는 사용자 이름입니다.

**STEP 4 |** LDAP 서버 프로파일을 구성하여 방화벽이 그룹 매핑 정보에 대해 전역 카탈로그 서버(최대 4개)에 연결하는 방법을 지정합니다.



가용성을 개선하려면 중복성에 대해 적어도 두 개의 글로벌 카탈로그 서버를 사용합니다.

로컬 도메인 그룹(하위 도메인)이 아닌 범용 그룹에 대해서만 그룹 매핑 정보를 수집할 수 있습니다.

1. 디바이스 > 서버 프로파일 > **LDAP**를 선택하고 추가를 클릭한 다음 프로파일의 이름을 입력합니다.
2. 서버 섹션에서 각 글로벌 카탈로그에 대해 추가를 클릭하고 서버 이름, IP 주소(**LDAP** 서버) 및 포트를 입력합니다. 일반 텍스트 또는 전송 레이어 보안시작(TLS시작) 연결의 경우 포트 3268을 사용합니다. SSL 연결을 통해 LDAP의 경우 포트 3269를 사용합니다. 연결이 SSL을 통해 TLS 시작 또는 LDAP를 사용하는 경우 **SSL/TLS** 보안 연결 체크박스를 선택합니다.
3. 기본 **DN** 필드에서 방화벽이 그룹 매핑 정보(예: `DC=acbdomain, DC=com`)를 검색하기 시작하는 글로벌 카탈로그 서버에서 포인트의 고유 이름(DN)을 입력합니다.
4. 유형에 대해 **active-directory**를 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** LDAP 서버 프로파일을 구성하여 방화벽이 도메인 매핑 정보를 포함하는 서버(최대 4개)에 연결하는 방법을 지정합니다.

사용자 ID는 이 정보를 사용하여 DNS 도메인 이름을 NetBIOS 도메인 이름에 매핑합니다. 이 매핑은 정책 규칙에서 일관된 도메인/사용자 이름 레퍼런스를 보장합니다.

가용성을 개선하려면 이중화에 대해 두 개 이상의 서버를 사용합니다.

해당 단계는 다음 필드를 제외하고 이전 단계에서 글로벌 카탈로그에 대해 만든 LDAP 서버 프로파일과 동일합니다.

- **LDAP** 서버 - 도메인 매핑 정보가 포함된 도메인 컨트롤러의 IP 주소를 입력합니다.
- 포트 - 일반 텍스트 또는 TLS 연결 시작의 경우 포트 **389**를 사용합니다. SSL 연결을 통해 LDAP의 경우 포트 636을 사용합니다. 연결이 SSL을 통해 TLS 시작 또는 LDAP를 사용하는 경우 **SSL/TLS** 보안 연결 체크박스를 선택합니다.
- 기본 **DN** - 방화벽이 도메인 매핑 정보를 검색하기 시작하는 도메인 컨트롤러에서 지점의 DN을 선택합니다. 값은 문자열로 시작해야 합니다: `cn=partitions,cn=configuration`(예: `cn=partitions,cn=configuration,DC=acbdomain,DC=com`).

**STEP 6 |** 만든 각 LDAP 서버 프로파일에 대한 그룹 매핑 구성을 생성합니다.

1. 디바이스 > 사용자 식별 > 그룹 매핑 설정을 선택합니다.
2. 추가를 클릭하고 이름을 입력하여 그룹 매핑 구성을 식별합니다.
3. LDAP 서버 프로파일을 선택하고 활성화됨 확인란이 선택되어 있는지 확인합니다.

   글로벌 카탈로그 및 도메인 매핑 서버가 보안 규칙보다 더 많은 그룹을 참조하는 경우 그룹 포함 목록 및/또는 사용자 지정 그룹 목록을 구성하여 사용자 ***ID***가 매핑을 수행하는 그룹을 제한합니다.
4. 확인 및 커밋을 클릭합니다.

## HTTP 헤더에 사용자 이름 삽입

사용자 기반 정책을 시행하기 위해 Palo Alto Networks 방화벽이 있는 보조 시행 어플라이언스를 구성할 때 보조 어플라이언스는 방화벽에서 IP 주소-사용자 이름 매핑을 갖지 않을 수 있습니다. 사용자 정보를 다운스트림 어플라이언스로 전송하려면 프록시와 같은 추가 어플라이언스를 배포해야 하거나 사용자 경험에 부정적인 영향을 미칠 수 있습니다(예: 사용자가 여러 번 로그인해야 함). HTTP 헤더에서 사용자 ID를 공유하면 사용자 경험에 부정적인 영향을 미치거나 추가 인프라를 배포하지 않고 사용자 기반 정책을 시행할 수 있습니다.

이 기능을 구성할 때 URL 프로파일을 보안 정책에 적용하고 변경 사항을 커밋하면 방화벽이 다음을 수행합니다.

1. 원본 사용자에 대한 그룹 매핑의 기본 사용자 이름 형식으로 사용자 및 도메인 값을 채웁니다.
2. Base64를 사용하여 이 정보를 인코딩합니다.
3. Base64로 인코딩된 헤더를 페이로드에 추가합니다.
4. 트래픽을 다운스트림 어플라이언스로 라우팅합니다.

 ©2023 Palo Alto Networks, Inc.

사용자가 특정 도메인에 액세스할 때만 사용자 이름과 도메인을 포함하려면 목록의 도메인이 HTTP 요청의 호스트 헤더와 일치할 때만 도메인 목록을 구성하면 방화벽이 헤더를 삽입합니다.

다운스트림 어플라이언스와 사용자 정보를 공유하려면 먼저 사용자 ID를 활성화하고 그룹 매핑을 구성해야 합니다.

헤더에 사용자 이름과 도메인을 포함하려면 방화벽에서 사용자의 ***IP*** 주소-사용자 이름 매핑이 필요합니다. 사용자가 매핑되지 않은 경우 방화벽은 헤더의 도메인과 사용자 이름 모두에 대해 ***Base64*** 인코딩으로 ***unknown***을 삽입합니다.

HTTPS 트래픽의 헤더에 사용자 이름과 도메인을 포함하려면 먼저 암호 해독 프로파일을 생성하여 HTTPS 트래픽을 해독해야 합니다..

이 기능은 포워드 프록시 복호화 트래픽을 지원합니다.

**STEP 1 |** 생성 또는 **URL** 필터링 프로파일을 수정합니다.

*URL* 필터링 프로파일에 대한 작업이 도메인에 대해 **차단**된 경우 방화벽은 헤더를 삽입하지 않습니다.

**STEP 2 |** 사전 정의된 유형을 사용하여 HTTP 헤더 삽입 항목을 만들거나 편집합니다.

각 프로파일에 대해 최대 5개의 헤더를 정의할 수 있습니다.

**STEP 3 |** 헤더 유형으로 동적 필드를 선택합니다.

**STEP 4 |** 헤더를 삽입할 도메인을 추가합니다. 사용자가 목록의 도메인에 액세스하면 방화벽이 지정된 헤더를 삽입합니다.

**STEP 5 |** 새 헤더를 추가하거나 **X-Authenticated-User**를 선택하여 수정합니다.

**STEP 6 |** 헤더 값 형식(**($domain)\($user)** 또는 **WinNT://($domain)/($user)**)을 선택하거나 **($domain)** 및 **($user)** 동적 토큰을 사용하여 고유한 형식을 입력합니다(예: UserPrincipalName의 경우 **($user)@($domain)** ).

동일한 동적 토큰(***($user)*** 또는 ***($domain)***)을 값당 두 번 이상 사용하지 마십시오.

각 값은 최대 512자일 수 있습니다. 방화벽은 그룹 매핑 프로파일의 기본 사용자 이름을 사용하여 **($user)** 및**($domain)** 동적 토큰을 채웁니다. 예:

- 기본 사용자 이름이 sAMAccountName인 경우 **($user)** 값은 sAMAccountName이고 **($domain)** 값은 NetBios 도메인 이름입니다.
- 기본 사용자 이름이 UserPrincipalName인 경우 **($user)** 사용자 계정 이름(프리픽스) 및 **($domain)**은 DNS(Domain Name System) 이름입니다.

**STEP 7 |** (선택 사항) 헤더 삽입에 대한 로깅을 활성화하려면 로그를 선택합니다.

**STEP 8 |** HTTP 또는 HTTPS 트래픽에 대한 보안 정책 규칙에 URL 필터링 프로파일을 적용합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** 확인을 두 번 선택하여 HTTP 헤더 구성을 확인합니다.

**STEP 10 |** 변경 사항을 커밋합니다.

**STEP 11 |** 방화벽이 HTTP 헤더에 사용자 이름과 도메인을 포함하는지 확인합니다.

- **show user user-ids all** 명령을 사용하여 그룹 매핑이 올바른지 확인합니다.
- **show counter global name ctd_header_insert** 명령을 사용하여 방화벽이 삽입한 HTTP 헤더 수를 확인합니다.
- 7단계에서 로깅을 구성한 경우 삽입된 Base64 인코딩 페이로드에 대한 로그를 확인합니다(예: **corpexample\testuser**는 로그에 **Y29ycGV4YW1wbGVcdGVzdHVzZXI=**로 표시됨).

## 데이터 및 인증 타임스탬프 재배포

대규모 네트워크에서는 모든 방화벽을 구성하여 매핑 정보 소스를 직접 쿼리하는 대신 일부 방화벽을 구성하여 재분배를 통해 매핑 정보를 수집하여 리소스 사용을 간소화할 수 있습니다.

터미널 서버*(TS)*에이전트를 제외한 모든 방법을 통해 수집된 사용자 매핑 정보를 재배포할 수 있습니다. 그룹 매핑 또는 HIP 일치 정보를 재배포할 수 없습니다.

*Panorama*를 사용하여 방화벽 및 방화벽 로그를 처리하는 경우 *Panorama*를 사용하여 사용자 ID 재배포를 관리할 수 있습니다. *Panorama*를 활용하는 것은 사용자 *ID* 정보를 재배포하기 위해 방화벽 간에 추가 연결을 만드는 것보다 더 간단한 솔루션입니다.

인증 정책을 구성하는 경우 방화벽은 사용자가 애플리케이션 및 서비스에 액세스하도록 인증할 때 생성된 인증 타임스탬프도 재배포해야 합니다. 방화벽은 타임스탬프를 사용하여 인증 정책 규칙의 타임아웃을 평가합니다. 타임아웃를 사용하면 인증에 성공한 사용자가 나중에 제한 시간 내에 다시 인증하지 않고도 서비스 및 애플리케이션을 요청할 수 있습니다. 타임스탬프를 다시 배포하면 네트워크의 모든 방화벽에서 일관된 타임아웃을 적용할 수 있습니다.

방화벽은 동일한 재배포 흐름의 일부로 데이터 및 인증 타임스탬프를 공유합니다. 각 정보 유형에 대해 별도로 재배포를 구성할 필요가 없습니다.

- 데이터 재배포를 위한 방화벽 배포
- 데이터 재배포 구성

### 데이터 재배포를 위한 방화벽 배포

대규모 네트워크에서는 모든 방화벽을 구성하여 데이터 원본을 직접 쿼리하는 대신 일부 방화벽을 구성하여 재분배를 통해 데이터를 수집하여 리소스 사용을 간소화할 수 있습니다. 또한 데이터 재배포는 세분성을 제공하므로 선택한 디바이스만 지정한 정보 유형만 재배포할 수 있습니다. 또한 서브넷 및 범위를 사용하여 IP 사용자 매핑 또는 IP 태그 매핑을 필터링하여 방화벽이 정책을 적용하는 데 필요한 매핑만 수집하도록 할 수도 있습니다.

데이터 재배포는 단방향(에이전트가 클라이언트에 데이터를 제공) 또는 양방향일 수 있으며 에이전트와 클라이언트가 동시에 데이터를 보내고 받을 수 있습니다.

데이터를 재배포하려면 다음 아키텍처 유형을 사용할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

- 단일 영역에 대한 허브 및 스포크 아키텍처**:**

  방화벽 간에 데이터를 재배포하려면 허브 및 스포크 아키텍처를 모범 사례로 사용합니다. 이 구성에서 허브 방화벽은 Windows User-ID 에이전트, Syslog Server, 도메인 컨트롤러 또는 기타 방화벽과 같은 소스에서 데이터를 수집합니다. 재분배 클라이언트 방화벽을 구성하여 허브 방화벽에서 데이터를 수집합니다.

  예를 들어 허브(복원력을 위한 VM-50 쌍으로 구성)는 사용자 매핑의 사용자 ID 소스에 연결할 수 있습니다. 그런 다음 허브는 사용자 매핑을 사용하는 클라이언트 방화벽이 정책을 적용하여 데이터를 수신하도록 허브에 연결할 때 사용자 매핑을 재배포할 수 있습니다.

- 여러 영역에 대한 멀티 허브 및 스포크 아키텍처**:**

  여러 지역에 방화벽을 배포하고 사용자가 로그인하는 위치에 관계없이 정책을 일관되게 적용할 수 있도록 이러한 모든 지역의 방화벽에 데이터를 배포하려는 경우 여러 지역에 대해 다중 허브 및 스포크 아키텍처를 사용할 수 있습니다.

  먼저 각 리전에서 방화벽을 구성하여 소스에서 데이터를 수집합니다. 이 방화벽은 재배포를 위한 로컬 허브 역할을 합니다. 이 방화벽은 해당 지역의 모든 소스에서 데이터를 수집하여 클라이언트 방화벽에 재배포할 수 있도록 합니다. 그런 다음 클라이언트 방화벽을 해당 지역 및 기타 모든 지역의 재분배 허브에 연결하도록 구성하여 클라이언트 방화벽이 모든 허브의 모든 데이터를 갖도록 합니다.

  방화벽이 데이터를 보내고 받아야 하는 경우 지역 내에서 양방향 재배포를 활성화하는 것이 좋습니다. 예를 들어 방화벽이 원격 사용자를 위한 GlobalProtect 게이트웨이 역할을 하고 로컬 사용자를 위한 분기 방화벽인 경우 방화벽은 원격 사용자를 위해 수집한 사용자 매핑을 허브 방화벽으로 보내고 허브 방화벽에서 로컬 사용자의 사용자 매핑을 수신해야 합니다.

- 레이어 아키텍처**:**

  데이터를 재배포하려면 레이어 아키텍처를 사용할 수도 있습니다. 예를 들어 사용자 ID 정보와 같은 데이터를 재배포하려면 각 레이어에 하나 이상의 방화벽이 있는 레이어에서 재배포 순서를 구성합니다. 하단 레이어에서 PAN-OS는 방화벽에서 실행되는 User-ID 에이전트와 Windows 서버에서 실행되는 Windows 기반 User-ID 에이전트가 IP 주소를 사용자 이름에 매핑합니다. 각 상위 레이어에는 매핑 정보 및 인증 타임스탬프를 받는 방화벽이 아래 레이어에 최대 100개의 재분배 포인트에서 수신됩니다. 최상위 방화벽은 모든 레이어의 매핑 및 타임스탬프를 집계합니다. 이 배포는 하위 레이어 방화벽에서 제공하는 해당 도메인의 사용자 하위 집합에 대해 최상위 방화벽 및 지역별 정책 또는 기능별 정책의 모든 사용자에 대한 정책을 구성할 수 있는 옵션을 제공합니다.

  이 시나리오에서는 세 레이어의 방화벽이 로컬 사무실에서 지역 사무소로 매핑 및 타임스탬프를 재배포한 다음 글로벌 데이터 센터로 재분배합니다. 모든 정보를 집계하는 데이터 센터 방화벽은 모든 정보를 다른 데이터 센터 방화벽과 공유하므로 모든 사용자가 정책을 적용하고 전체 네트워크에서 사용자에 대한 보고서를 생성할 수 있습니다. 하단 레이어 방화벽만 User-ID 에이전트를 사용하여 디렉터리 서버를 쿼리합니다.

  User-ID 에이전트쿼리가 쿼리하는 정보 원본은 시퀀스의 최대 10홉에 포함되지 않습니다. 그러나 매핑 정보를 방화벽으로 포워딩하는 Windows 기반 User-ID 에이전트는 계산을 합니다. 또한 이 예제에서는 맨 위 레이어에 한 데이터 센터 방화벽에서 정보를 집계하는 첫 번째 홉과 다른 데이터 센터 방화벽과 정보를 공유하는 두 번째 홉이 있습니다.

## 데이터 재배포 구성

데이터 재배포를 구성하기 전에:

 ©2023 Palo Alto Networks, Inc.

- ☐ 재배포 아키텍처를 계획합니다. 고려해야 할 몇 가지 요인은 다음과 같습니다.
  - 모든 데이터 유형에 대한 정책을 적용할 방화벽과 데이터 하위 집합에 대한 지역 또는 기능별 정책을 적용할 방화벽은 무엇입니까?
  - 재분배 시퀀스가 모든 데이터를 집계하는 데 얼마나 많은 홉(hop)이 필요합니까? 사용자 매핑에 허용되는 최대 홉의 수는 10개이며 IP 주소-사용자 이름 매핑 및 IP 주소 - 태그 매핑에 허용되는 최대 홉의 수는 하나입니다.
  - 사용자 매핑 정보 소스를 쿼리하는 방화벽 수를 최소화하려면 어떻게 해야 합니까? 쿼리 방화벽 수가 적을수록 처리 부하가 방화벽과 소스 모두에 있습니다.
- ☐ 재배포 에이전트가 클라이언트에 재배포할 데이터를 가져오는 데이터 원본 구성:
  - PAN-OS 통합 사용자 ID 에이전트 또는 Windows 기반 사용자 ID 에이전트
  - 의 사용자 매핑동적 주소 그룹에 대한 IP 주소 대 태그 매핑
  - 동적 사용자 그룹 에 대한 사용자 이름 대 태그 매핑
  - GlobalProtect for HIP 기반 정책 시행
  - 디바이스 검역을 위한 데이터(Panorama만)
- ☐ 인증 정책을 구성합니다.

데이터 재배포는 다음과 같은 것으로 구성됩니다.

- 정보를 제공하는 재배포 에이전트
- 정보를 수신하는 재배포 클라이언트

데이터 재배포 시퀀스에서 방화벽에서 다음 단계를 수행합니다.

**STEP 1 |** 재분배 클라이언트 방화벽에서 방화벽, Panorama 또는 Windows User-ID 에이전트를 데이터 재배포 에이전트로 구성합니다.

1. 디바이스 > 데이터 재배포 > 에이전트를 선택합니다.
2. 재배포 에이전트를 추가하고 이름을 입력합니다.
3. 에이전트가 활성화되어 있는지 확인합니다.

**STEP 2 |** 일련 번호 또는 호스트 및 포트를 사용하여 에이전트를 추가합니다.

- 일련번호를 사용하여 에이전트를 추가하려면 재분배 에이전트로 사용할 방화벽의 일련번호를 선택합니다.
- 호스트 및 포트 정보를 사용하여 에이전트를 추가하려면:
  1. 호스트에 대한 정보를 입력합니다.
  2. 호스트가 **LDAP** 프록시인지 여부를 선택합니다.
  3. 포트를 입력합니다(기본값은 5007, 범위는 1~65535).
  4. (여러 가상 시스템만 해당) 재배포 에이전트로 사용할 가상 시스템을 식별하려면 수집기 이름을 입력합니다.
  5. (여러 가상 시스템만 해당) 재배포 에이전트로 사용하려는 가상 시스템의 **Collector Pre-Shared Key**를 입력하고 확인합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 에이전트가 재배포할 하나 이상의 데이터 유형을 선택합니다.

- **IP** 사용자 매핑-사용자 ID에 대한 IP 주소-사용자 이름 매핑.
- **IP** 태그 - 동적 주소 그룹을 위한 IP 주소 간 매핑입니다.
- 사용자 태그 - 동적 사용자 그룹을 위한 사용자 이름 - 태그 매핑입니다.
- **HIP** - HIP 개체와 프로파일을 포함하는 GlobalProtect의 호스트 정보 프로파일(HIP) 데이터입니다.
- 격리 목록 - GlobalProtect가 격리된 것으로 식별하는 디바이스입니다.

**STEP 4 |** (여러 가상 시스템만) 데이터를 재배포할 수 있는 수집기로 가상 시스템을 구성합니다.

방화벽이 수신하지만 데이터를 재배포하지 않는 경우 이 단계를 건너뜁니다.



다른 방화벽이나 동일한 방화벽에서 가상 시스템 간에 정보를 재배포할 수 있습니다. 두 경우 모두 각 가상 시스템은 재배포 순서에서 하나의 홉으로 계산됩니다.

1. 디바이스 > 데이터 재배포 > 수집기 설정을 선택합니다.
2. 데이터 재배포 에이전트 설정을 편집합니다.
3. 이 방화벽 또는 가상 시스템을 User-ID 에이전트로 식별하려면 수집기 이름 및 사전 공유 키를 입력하십시오.
4. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 5 |** (선택 사항이지만 권장) 데이터 재배포에 포함할 네트워크와 데이터 재배포에서 제외할 네트워크를 구성합니다.

IP 주소-태그 매핑 또는 IP 주소 - 사용자 이름 매핑을 다시 배포할 때 네트워크 및 하위 네트워크를 포함하거나 제외할 수 있습니다.



모범 사례로 에이전트가 내부 리소스와만 통신하고 있는지 확인하기 위해 포함하고 제외할 네트워크를 항상 지정합니다.

1. 디바이스 > 데이터 재배포 > 네트워크 포함/제외를 선택합니다.
2. 항목을 추가하고 이름을 입력합니다.
3. 항목이 활성화됨인지 확인합니다.
4. 항목을 포함할지 또는 제외할지 선택합니다.
5. 항목에 대한 네트워크 주소를 입력합니다.
6. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 방화벽이 사용자 ID 정보에 대한 다른 방화벽을 쿼리하는 데 사용하는 서비스 경로를 구성합니다.

방화벽이 Windows 기반 User-ID 에이전트에서만 사용자 매핑 정보 또는 다른 방화벽 대신 정보 소스(예: 디렉터리 서버)에서 직접 사용자 매핑 정보를 수신하는 경우 이 단계를 건너뜁니다.

1. 디바이스 > 설정 > 서비스를 선택합니다.
2. (여러 가상 시스템이 있는 방화벽만) 전역(방화벽 전체 서비스 경로의 경우) 또는 가상 시스템(가상 시스템별 서비스 경로의 경우)을 선택합니다. 그런 다음 서비스 경로를 구성합니다.
3. 서비스 경로 구성을 클릭하고 사용자 지정을 선택한 다음 네트워크 프로토콜에 따라 **IPv4** 또는 **IPv6**를 선택합니다. 네트워크에서 두 프로토콜을 모두 사용하는 경우 두 프로토콜에 대한 서비스 경로를 구성합니다.
4. **UID** 에이전트를 선택한 다음 소스 인터페이스 및 소스 주소를 선택합니다.
5. 서비스 경로를 저장하려면 확인을 두 번 클릭합니다.

**STEP 7 |** 다른 방화벽이 데이터를 재배포할 때 방화벽이 응답하도록 합니다.

방화벽이 수신하지만 데이터를 재배포하지 않는 경우 이 단계를 건너뜁니다.

사용자 **ID** 서비스를 사용하도록 설정하여 인터페이스 관리 프로파일을 구성하고 프로파일을 방화벽 인터페이스에 할당합니다.

**STEP 8 |** (선택사항이지만 권장) 엔터프라이즈 PKI의 사용자 지정 인증서를 사용하여 재배포 클라이언트에서 재배포 에이전트에 대한 고유한 신뢰 체인을 설정합니다.

1. 재분배 클라이언트 방화벽에서 나가는 연결에 사용할 사용자 지정 SSL 인증서 프로파일을 생성합니다.
2. 디바이스 > 설정 > 관리 > 보안 통신 설정을 선택합니다.
3. 설정을 수정합니다.
4. 사용자 지정 보안 서버 통신 옵션을 선택합니다.
5. 하위 단계 1에서 생성한 인증서 프로파일을 선택합니다.
6. 확인을 클릭합니다.
7. 데이터 재배포를 위한 통신을 사용자 정의합니다.
8. 변경 사항을 커밋합니다.
9. 다음 CLI 명령을 입력하여 인증서 프로파일(**SSL 구성**)이 **사용자 지정 인증서**를 사용하는지 확인합니다. **재배포 에이전트 상태 표시 *<agent-name>***( 여기서 *<agent-name>*은 재배포 에이전트 또는 User-ID 에이전트의 이름입니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** (선택 사항이지만 권장) 재분배 에이전트에서 재배포 클라이언트에 대한 고유한 신뢰 체인을 설정하려면 엔터프라이즈 PKI의 사용자 지정 인증서를 사용합니다.

1. 재분배 에이전트 방화벽에서 들어오는 연결에 사용할 방화벽에 대한 사용자 지정 SSL/TLS 서비스 프로파일을 생성합니다.
2. 디바이스 > 설정 > 관리 > 보안 통신 설정을 선택합니다.
3. 설정을 수정합니다.
4. 사용자 지정 보안 서버 통신 옵션을 선택합니다.
5. 1단계에서 만든 **SSL/TLS** 서비스 프로파일을 선택합니다.
6. 확인을 클릭합니다.
7. 변경 사항을 커밋합니다.
8. **show redistribution service status** CLI 명령을 입력하여 인증서 프로파일(**SSL 구성**)이 **사용자 지정 인증서**를 사용하는지 확인합니다.

**STEP 10 |** 에이전트가 클라이언트에 데이터를 올바르게 재배포하는지 확인합니다.

1. 에이전트 통계(디바이스 > 데이터 재배포 > 에이전트)를 보고 클라이언트 방화벽이 받은 매핑 수와 같이 재배포 에이전트에 대한 활동의 요약을 보려면 상태를 선택합니다.
2. 연결된 상태가 예인지 확인합니다.
3. 에이전트에서 CLI에 액세스하고 **show redistribution service status** CLI 명령을 입력하여 재배포 상태를 확인합니다.
4. 에이전트에서 **show redistribution service client all** CLI 명령을 입력하여 재배포 클라이언트를 봅니다.
5. 클라이언트에서 **show redistribution service client all** CLI 명령을 입력하여 재배포 상태를 확인합니다.
6. 사용자 ID 로그에서 소스 이름(모니터 > 로그 > 사용자 **ID**을 확인하여 방화벽이 재배포 에이전트로부터 매핑을 수신하는지 확인합니다.
7. 클라이언트에서 IP-Tag 로그(**Monitor** > **Logs** > **IP-Tag**)를 보고 클라이언트 방화벽이 데이터를 수신하는지 확인합니다.
8. 클라이언트에서 **show user ip-user-mapping all** CLI 명령을 입력하고 방화벽이 **From** 매핑을 수신하는 소스가 **REDIST**인지 확인합니다.

**STEP 11 |** (선택 사항) 데이터 재배포를 해결하려면 추적 경로 옵션을 사용하도록 설정합니다.

traceroute 옵션을 사용하도록 설정하면 데이터를 수신하는 방화벽이 해당 IP 주소를 **<route>** 필드에 추가합니다. 이 필드는 데이터가 통과한 모든 방화벽 IP 주소 목록입니다. 이 옵션을 사용하면 재배포 경로의 모든 PAN-OS 디바이스에 PAN-OS 버전 10.0을 사용해야 합니다. 재배포 경로의 PAN-OS 디바이스가 PAN-OS 9.1.x 또는 이전 버전을 사용하는 경우 해당 디바이스에서 추적 경로 정보가 종료됩니다.

1. 소스가 시작된 재배포 에이전트에서 다음 CLI 명령을 입력합니다. **debug user-id test cp-login traceroute yes ip-address *<ip-address>* user *<username>*** (여기서 ***<ip-address>***은 확인하려는 IP 주소-사용자 이름 매핑의 IP 주소이고 ***<username>*** 는 확인하려는 IP 주소-사용자 이름 매핑의 사용자 이름입니다.

 ©2023 Palo Alto Networks, Inc.

2. 추적 경로를 구성한 방화벽 클라이언트에서 방화벽이 **show user ip-user-mapping all** CLI 명령을 입력하여 데이터를 재배포하는지 확인합니다..

   방화벽은 매핑(**SeqNumber**)을 생성하고 사용자가 GlobalProtect(**GP 사용자**)를 가지고 있는지의 여부를 확인하기 위한 타임스탬프를 표시합니다.

```
admin > show user ip-user-mapping-mp ip 192.0.2.0 IP address:
 192.0.2.0 (vsys1) User: jimdoe From: REDIST Timeout:
 889s Created: 11s ago Origin: 198.51.100.0 SeqNumber:
 15895329682-67831262 GP User: No Local HIP: No Route Node 0:
 198.51.100.0 (vsys1) Route Node 1: 198.51.100.1 (vsys1)
```

## 가상 시스템 전체에서 사용자 ID 매핑 공유

여러 가상 시스템이 있는 경우 User-ID™ 소스 구성을 단순화하려면 단일 가상 시스템에서 사용자 ID 소스를 구성하여 IP 주소-사용자명 매핑 및 사용자명-그룹 매핑을 방화벽의 다른 모든 가상 시스템과 공유하십시오.

단일 가상 시스템을 ***User-ID*** 허브로 구성하면 특히 트래픽이 사용자가 액세스하려는 리소스를 기반으로 여러 가상 시스템을 통과하는 경우 여러 가상 시스템에서 소스를 구성할 필요가 없어 사용자 매핑이 간소화됩니다(예를 들어, 학생이 서로 다른 가상 시스템에서 트래픽을 관리하는 서로 다른 부서에 액세스하는 학업 네트워킹 환경의 경우).

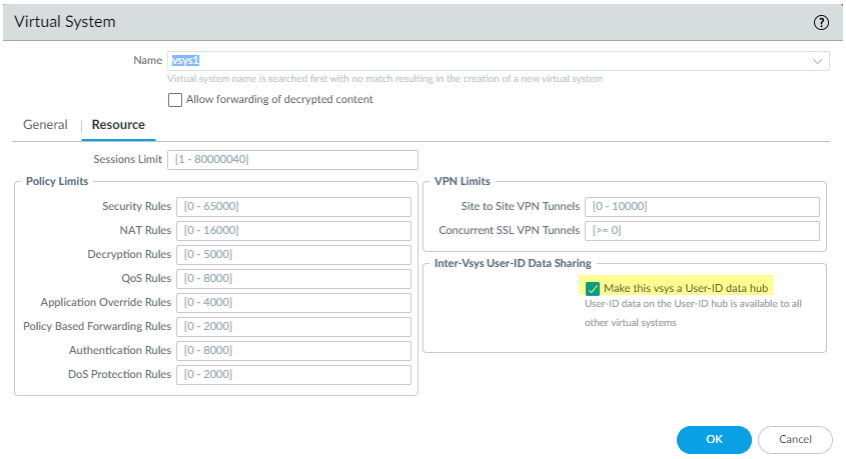
사용자 또는 그룹을 매핑하기 위해 방화벽은 로컬 가상 시스템의 매핑 테이블을 사용하고 해당 사용자 또는 그룹에 대한 정책을 적용합니다. 방화벽이 해당 사용자의 트래픽이 시작된 가상 시스템에서 사용자 또는 그룹에 대한 매핑을 찾지 못하면 방화벽은 허브에 쿼리하여 해당 사용자에 대한 IP 주소-사용자명 정보 또는 해당 그룹에 대한 그룹 매핑 정보를 가져옵니다. 방화벽이 User-ID 허브와 로컬 가상 시스템 모두에서 매핑을 찾는 경우 방화벽은 로컬에서 학습한 매핑을 사용합니다. 로컬 방화벽의 매핑이 가상 시스템 허브의 매핑과 다른 경우 방화벽은 로컬 매핑을 사용합니다.

User-ID 허브를 구성한 후 가상 시스템은 사용자 기반 정책 시행을 위해 사용자를 식별하거나 로그 또는 보고서에 사용자 이름을 표시해야 할 때 User-ID 허브의 매핑 테이블을 사용할 수 있지만 소스는 로컬에서 사용할 수 없습니다. 허브를 선택하면 방화벽이 다른 가상 시스템의 매핑을 유지하므로 허브에서 사용자 ID 소스를 통합하는 것이 좋습니다. 그러나 특정 소스의 매핑을 공유하지 않으려면 사용자 또는 그룹 매핑을 수행하도록 개별 가상 시스템을 구성할 수 있습니다.

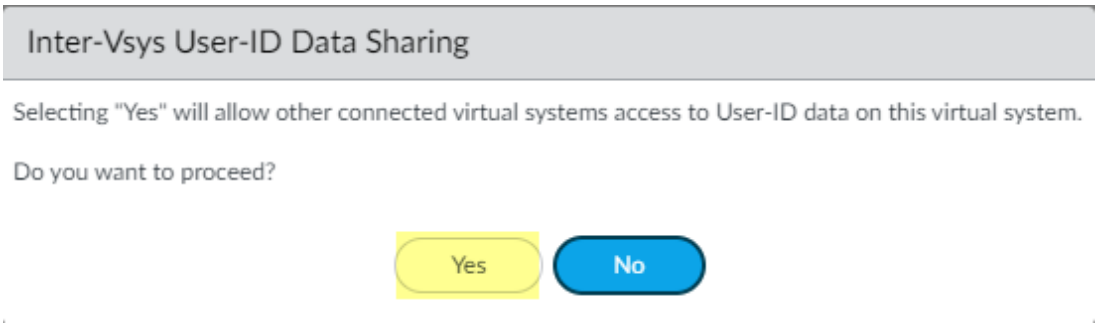
 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 가상 시스템을 User-ID 허브로 할당합니다.

1. 디바이스 > 가상 시스템을 선택한 다음 사용자 ID 소스를 통합한 가상 시스템을 선택하십시오.
2. 리소스 탭에서 이 **vsys**를 **User-ID** 데이터 허브로 생성하고 예를 클릭하여 확인합니다. 그런 다음 확인을 클릭합니다.

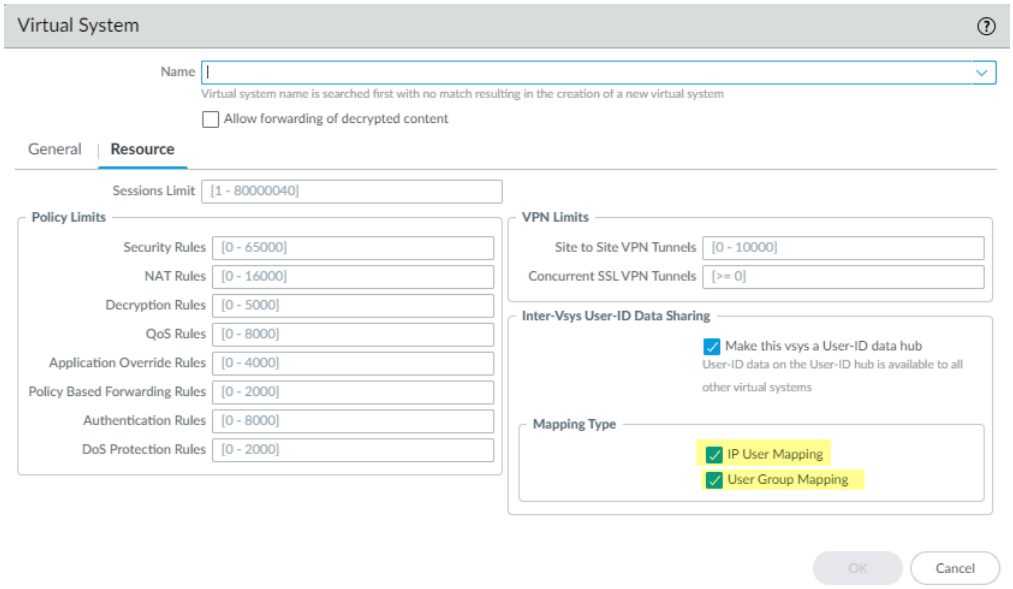



**STEP 2 |** 예를 클릭하여 확인합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 공유할 매핑 유형을 선택한 다음 확인을 클릭합니다.




- **IP** 사용자 매핑 - 다른 가상 시스템과 IP 주소-사용자명 매핑 정보를 공유합니다.
- 사용자 그룹 매핑 - 다른 가상 시스템과 그룹 매핑 정보를 공유합니다.

매핑 유형을 하나 이상 선택해야 합니다.

**STEP 4 |** 사용자 ID 소스를 통합하고 사용자 ID 허브로 사용하려는 가상 시스템으로 마이그레이션하십시오.

이는 운영 단순성을 위해 사용자 ID 구성을 통합합니다. 허브가 서버를 모니터링하고 이전에 다른 가상 시스템에서 모니터링한 에이전트에 연결하도록 구성하면 허브는 각 가상 시스템이 독립적으로 수집하는 대신 사용자 매핑 정보를 수집합니다. 특정 가상 시스템의 매핑을 공유하지 않으려면 허브로 사용되지 않을 가상 시스템에서 해당 매핑을 구성합니다.

가상 시스템 및 방화벽에서 기본 사용자명에 동일한 형식을 사용합니다.

1. 불필요하거나 오래된 소스를 제거하십시오.
2. Windows 기반 또는 통합 에이전트에 대한 모든 구성과 XML API를 사용하여 사용자 매핑을 보내는 모든 소스를 식별하고 사용자 ID 허브로 사용하려는 가상 시스템에 복사합니다.

   허브에서 현재 가상 시스템에 구성된 모든 사용자 *ID* 소스를 구성할 수 있습니다. 그러나 터미널 서버 에이전트의 *IP* 주소 및 포트-사용자명 매핑 정보는 사용자 *ID* 허브와 연결된 가상 시스템 간에 공유되지 않습니다.
3. User-ID가 매핑에 포함하거나 매핑에서 제외해야 하는 하위 네트워크를 지정합니다.
4. 정의 사용자 목록 무시.
5. 다른 모든 가상 시스템에서 User-ID 허브에 있는 모든 소스를 제거합니다.

**STEP 5 |** 변경 사항을 커밋하여 User-ID 허브를 활성화하고 통합 소스에 대한 매핑 수집을 시작합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** User-ID 허브가 사용자 및 그룹을 매핑하는지 확인합니다.

1. **show user ip-user-mapping all** 명령을 사용하여 IP 주소-사용자 이름 매핑과 매핑을 제공하는 가상 시스템을 표시합니다.
2. **show user user-id-agent statistics** 명령을 사용하여 User-ID 허브 역할을 하는 가상 시스템을 표시합니다.
3. 허브가 다음 CLI 명령을 사용하여 그룹 매핑을 공유하고 있는지 확인합니다.
   - 사용자 그룹 매핑 통계 표시
   - 사용자 그룹 매핑 상태 모두 표시
   - 사용자 그룹 목록 표시
   - 사용자 그룹 이름 표시 *<group-name>*

 ©2023 Palo Alto Networks, Inc.

# App-ID

네트워크에서 애플리케이션을 안전하게 활성화하기 위해 Palo Alto Networks 차세대 방화벽은 애플리케이션 및 웹 관점(App-ID 및 URL 필터링)을 모두 제공하여 모든 범위의 법률, 규제, 생산성 및 리소스 활용 위험으로부터 보호합니다.

App-ID를 사용하면 네트워크의 애플리케이션에 대한 가시성을 확보할 수 있으므로 작동 방식을 배우고 동작 특성과 상대적 위험을 이해할 수 있습니다. 이 애플리케이션 지식을 통해 원하는 애플리케이션을 활성화, 검사 및 구체화하고 원치 않는 애플리케이션을 차단하는 보안 정책 규칙을 생성하고 적용할 수 있습니다. 트래픽을 허용하는 정책 규칙을 정의하면 App-ID가 추가 구성 없이 트래픽을 분류하기 시작합니다.

신규 및 수정된 App-ID는 애플리케이션 및 위협 콘텐츠 업데이트의 일부로 릴리스됩니다. 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례에 따라 애플리케이션 및 위협 서명을 최신 상태로 원활하게 유지합니다.


- App-ID 개요
- 간소화된 앱 ID 정책 규칙
- 앱 ID 및 HTTP/2 검사
- 사용자 지정 또는 알 수 없는 애플리케이션 관리
- 신규 및 수정된 App-ID 관리
- 정책에 애플리케이션 개체 사용
- 기본 포트에서 애플리케이션 안전하게 활성화
- 암시적 지원이 있는 애플리케이션
- 보안 정책 규칙 최적화
- App-ID 클라우드 엔진
- SaaS 앱 ID 정책 추천
- 애플리케이션 수준 게이트웨이
- SIP 애플리케이션 수준 게이트웨이(ALG) 비활성화
- HTTP 헤더를 사용하여 SaaS 애플리케이션 액세스 관리
- 레거시 애플리케이션에 대한 사용자 지정 시간 관리

# App-ID 개요

Palo Alto Networks 방화벽에서만 사용할 수 있는 특허 받은 트래픽 분류 시스템인 App-ID는 포트, 프로토콜, 암호화(SSH 또는 SSL) 또는 애플리케이션에서 사용하는 기타 회피 전술과 상관없이 애플리케이션이 무엇인지 결정합니다. 애플리케이션 서명, 애플리케이션 프로토콜 디코딩 및 휴리스틱과 같은 여러 분류 메커니즘을 네트워크 트래픽 스트림에 적용하여 애플리케이션을 정확하게 식별합니다.

App-ID가 네트워크를 통과하는 애플리케이션을 식별하는 방법은 다음과 같습니다.

- 트래픽은 정책과 일치하여 네트워크에서 허용되는지의 여부를 확인합니다.
- 그런 다음 고유한 애플리케이션 속성 및 관련 트랜잭션 특성을 기반으로 애플리케이션을 식별하기 위해 허용된 트래픽에 서명이 적용됩니다. 서명은 또한 애플리케이션이 기본 포트에서 사용 중인지 아니면 비표준 포트를 사용 중인지 확인합니다. 정책에서 트래픽을 허용하는 경우 트래픽에 위협이 있는지 검색하고 추가로 분석하여 애플리케이션을 보다 세부적으로 식별합니다.
- App-ID에서 암호화(SSL 또는 SSH)가 사용 중이고 복호화 정책 규칙이 있는 것으로 확인되면 세션이 해독되고 애플리케이션 서명이 해독된 플로우에 다시 적용됩니다.
- 그런 다음 알려진 프로토콜에 대한 디코더를 사용하여 추가 컨텍스트 기반 서명을 적용하여 프로토콜 내부에서 터널링할 수 있는 애플리케이션을 감지합니다(예: Yahoo! HTTP에서 사용되는 인스턴트 메신저). 디코더는 트래픽이 프로토콜 사양을 준수하는지 확인하고 NAT 통과를 지원하며 SIP 및 FTP와 같은 애플리케이션을 위한 동적 핀홀을 엽니다.
- 특히 회피적이고 고급 서명 및 프로토콜 분석을 통해 식별할 수 없는 애플리케이션의 경우 휴리스틱 또는 행동 분석을 사용하여 애플리케이션의 ID를 확인할 수 있습니다.

애플리케이션이 식별되면 정책 검사는 애플리케이션을 처리하는 방법을 결정합니다. 예를 들어 위협 차단 또는 허용 및 검사, 무단 파일 전송 및 데이터 패턴 검사, QoS를 사용한 형태 형성 등이 있습니다.


©2023 Palo Alto Networks, Inc.

# 간소화된 앱 ID 정책 규칙

단일 정책 규칙을 사용하여 공통 속성을 가진 광범위한 애플리케이션 집합을 안전하게 활성화합니다(예: 사용자에게 웹 기반 애플리케이션에 대한 광범위한 액세스 권한을 부여하거나 모든 엔터프라이즈 VoIP 애플리케이션을 안전하게 활성화). Palo Alto Networks는 공통 속성을 가진 애플리케이션을 연구하는 작업을 수행하고 동적 콘텐츠 업데이트의 태그를 통해 이를 제공합니다. 관련 내용:

- 오류를 최소화하고 시간을 절약합니다.
- 새로 출시된 애플리케이션을 처리하기 위해 자동으로 업데이트되는 정책을 생성하는 데 도움이 됩니다.
- Policy Optimizer를 사용하여 App-ID 기반 규칙 집합으로의 전환을 단순화합니다.

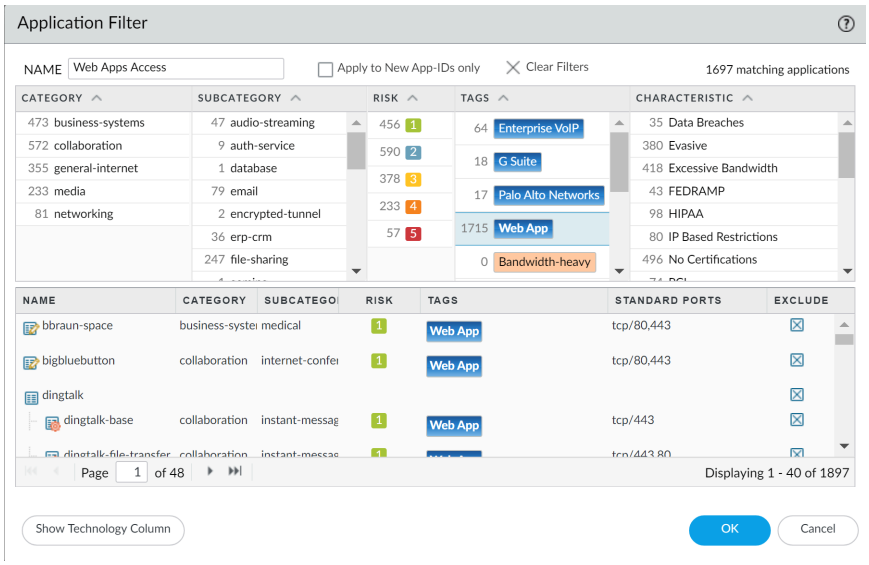
그러면 방화벽은 태그 기반 애플리케이션 필터를 사용하여 새 애플리케이션이 추가될 때마다 정책 규칙을 검토하거나 업데이트할 필요 없이 새롭고 업데이트된 App-ID를 동적으로 적용할 수 있습니다. 특정 태그에서 애플리케이션을 제외하도록 선택하면 새 콘텐츠 업데이트에서 해당 제외를 적용합니다. 또한 자체 태그를 사용하여 정책 요구 사항에 따라 애플리케이션 유형을 정의할 수 있습니다.

- 태그를 사용하여 애플리케이션 필터 생성
- 사용자 지정 태그를 기반으로 애플리케이션 필터 생성

## 태그를 사용하여 애플리케이션 필터 생성

**STEP 1 |** 하나 이상의 태그를 사용하여 애플리케이션 필터를 생성합니다.

둘 이상의 태그를 선택하는 경우 애플리케이션은 필터에 포함할 두 태그를 일치시켜야 합니다.




**STEP 2 |** (선택 사항)제외열의 확인란을 선택하여 필터에서 태그를 제외합니다.

**STEP 3 |** 보안 정책 규칙을 만들고 애플리케이션 탭에서 새 애플리케이션 필터를 추가합니다.

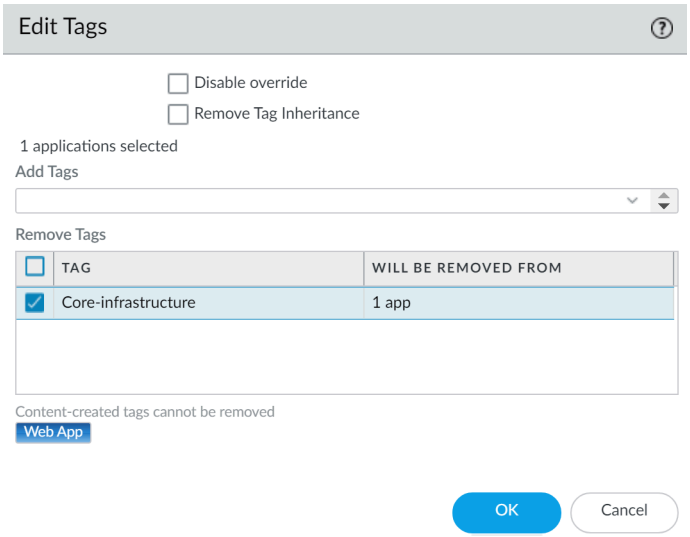
**STEP 4 |** 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 사용자 지정 태그를 기반으로 애플리케이션 필터 생성

**STEP 1 |** 사용자 지정 태그를 생성하고 앱-아이디에 적용됩니다.

1. (선택 사항) 애플리케이션에서 태그를 제거합니다.
2. 애플리케이션을 필터링하거나 검색한 다음 특정 애플리케이션을 선택하여 태그를 제거합니다.
3. 태그를 편집하고 제거할 태그를 선택합니다.

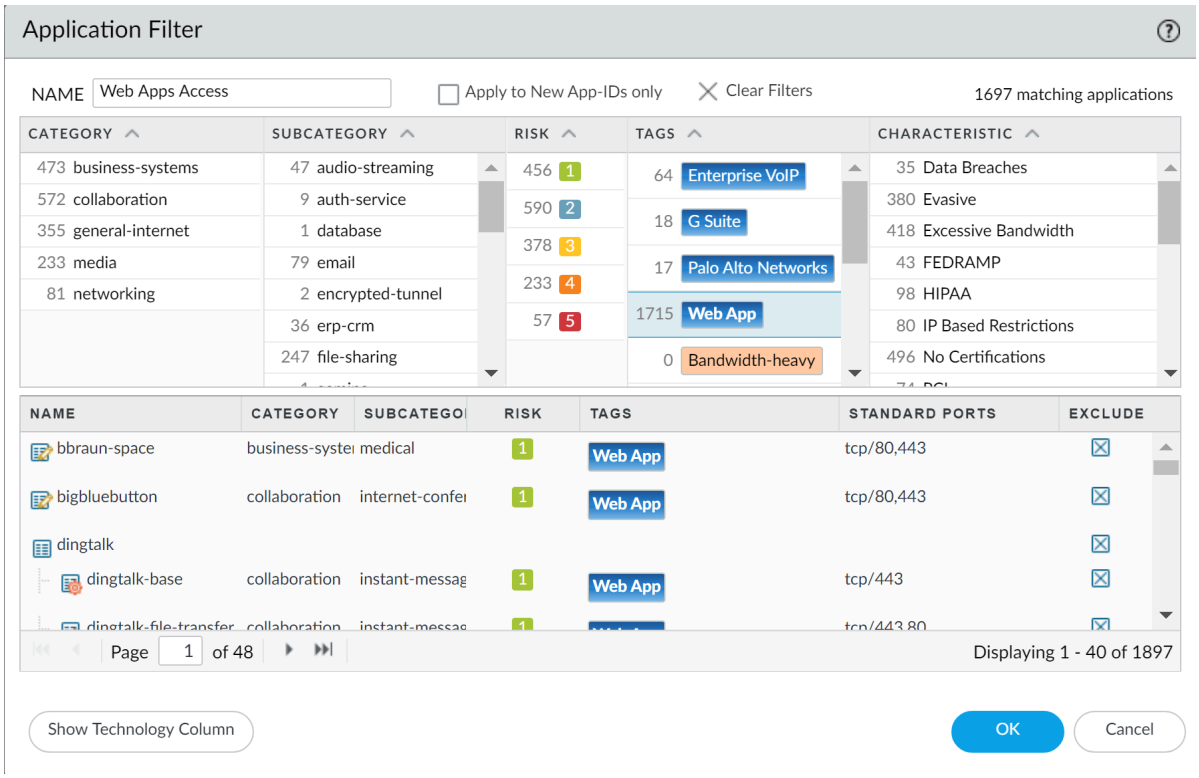



4. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 하나 이상의 태그를 사용하여 애플리케이션 필터를 생성합니다.

둘 이상의 태그를 선택하는 경우 애플리케이션은 필터에 포함할 두 태그를 일치시켜야 합니다.



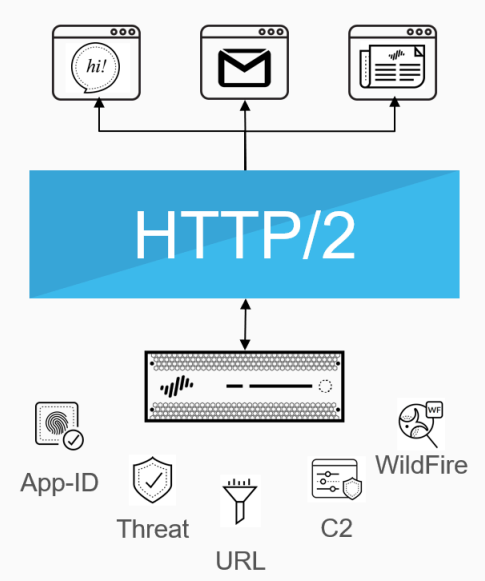

**STEP 3 |** 보안 정책 규칙을 만들고 애플리케이션 탭에서 새 애플리케이션 필터를 추가합니다.

**STEP 4 |** 변경 사항을 커밋합니다.

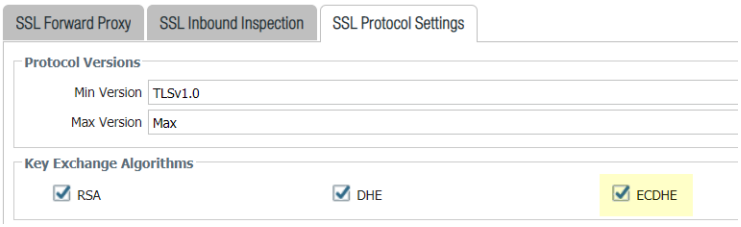

©2023 Palo Alto Networks, Inc.

# 앱 ID 및 HTTP/2 검사

이제 방화벽의 추가 구성 없이 HTTP/2를 통해 실행되는 애플리케이션을 안전하게 활성화할 수 있습니다. 더 많은 웹사이트가 HTTP/2를 계속 채택함에 따라 방화벽은 스트림별로 보안 정책과 모든 위협 탐지 및 예방 기능을 적용할 수 있습니다. HTTP/2 트래픽에 대한 이러한 가시성을 통해 HTTP/2를 통해 서비스를 제공하는 웹 서버를 보호하고 사용자가 HTTP/2가 제공하는 속도 및 리소스 효율성 향상의 이점을 누릴 수 있습니다.




방화벽은 SSL 복호화가 활성화된 경우 기본적으로 HTTP/2 트래픽을 처리하고 검사합니다. HTTP/2 검사가 올바르게 작동하려면 방화벽을 활성화하여 ECDHE(타원형 곡선 Diffie-Hellman)를 SSL 세션의 핵심 교환 알고리즘으로 사용해야 합니다. ECDHE는 기본적으로 활성화되어 있지만 개체 > 복호화 > 프로파일 > **SSL** 복호화 > **SSL** 프로토콜 설정을 선택하여 활성화되어 있는지 확인할 수 있습니다.



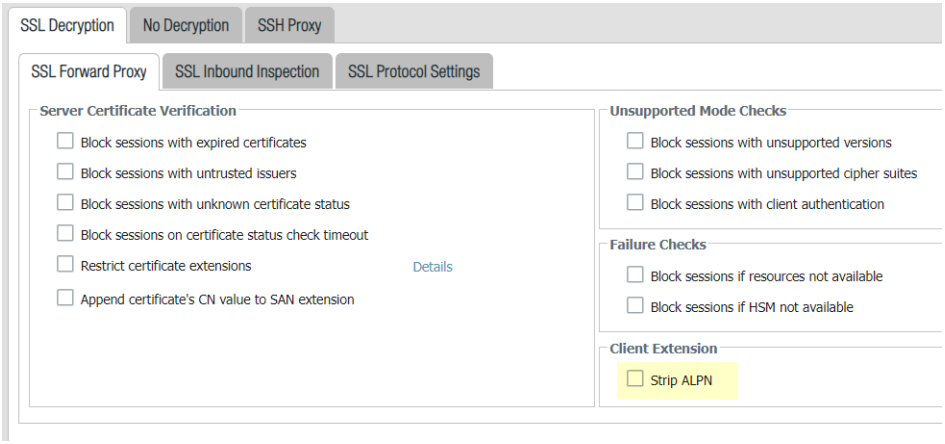

*PAN-OS 10.2*에 도입된 복호화 로그가 활성화되면 터널 콘텐츠 검사를 활성화하여 *HTTP/2* 트래픽에 대한 앱 *ID*를 얻어야 합니다.

대상 트래픽에 대한 HTTP/2 검사를 비활성화하거나 전체를 비활성화할 수 있습니다.


©2023 Palo Alto Networks, Inc.

- 대상 트래픽에 대한 HTTP/2 검사를 사용하지 않도록 설정합니다.

  ALPN(애플리케이션 레이어 프로토콜 협상) TLS 확장에 포함된 값을 제거하려면 방화벽을 지정해야 합니다. ALPN은 HTTP/2 연결을 보호하는 데 사용되며, 이 TLS 확장에 대해 지정된 값이 없는 경우 방화벽은 HTTP/2 트래픽을 HTTP/1.1로 다운그레이드하거나 알 수 없는 TCP 트래픽으로 분류합니다.




  1. 개체 > 암호 해독 > 암호 해독 프로파일 > **SSL** 암호 해독 > **SSL** 전달 프록시를 선택한 다음 스트립 **ALPN**을 선택합니다.
  2. 복호화 프로파일을 복호화 정책(정책 > 복호화)에 연결하여 정책과 일치하는 트래픽에 대한 HTTP/2 검사를 끕니다.
  3. 변경 사항을 커밋합니다.

- 전체 HTTP/2 검사를 사용하지 않도록 설정합니다.

  `set deviceconfig setting http2 enable no` CLI 명령을 사용하고 변경 내용을 커밋합니다. 방화벽은 HTTP/2 트래픽을 알 수 없는 TCP 트래픽으로 분류합니다.


©2023 Palo Alto Networks, Inc.

# 사용자 지정 또는 알 수 없는 애플리케이션 관리

Palo Alto Networks는 새로운 App-ID 서명을 식별하기 위해 매주 애플리케이션 업데이트를 제공합니다. 기본적으로 App-ID는 방화벽에서 항상 활성화되며 잘 알려진 애플리케이션을 식별하기 위해 일련의 서명을 활성화할 필요가 없습니다. 일반적으로 ACC 및 트래픽 로그에서 알 수 없는 트래픽(tcp, udp 또는 non-syn-tcp)으로 분류되는 유일한 애플리케이션은 App-ID, 네트워크의 내부 또는 사용자 지정 애플리케이션 또는 잠재적인 위협에 아직 추가되지 않은 상용 애플리케이션입니다.

경우에 따라 방화벽은 다음과 같은 이유로 애플리케이션을 알 수 없는 것으로 보고할 수 있습니다.

- 불완전한 데이터 - 핸드쉐이크가 발생했지만 타임아웃 전에 데이터 패킷이 전송되지 않았습니다.
- 데이터 부족 - 핸드쉐이크가 발생한 후 하나 이상의 데이터 패킷이 발생했습니다. 그러나 애플리케이션을 식별하기에 충분한 데이터 패킷이 교환되지 않았습니다.

알 수 없는 애플리케이션을 처리하는 데 사용할 수 있는 선택 사항은 다음과 같습니다.

- 알 수 없는 TCP, 알 수 없는 UDP 또는 소스 영역, 대상 영역 및 IP 주소의 조합으로 알 수 없는 애플리케이션을 제어하는 보안 정책을 생성합니다.
- Palo Alto Networks에서 App-ID 요청 - 네트워크를 통과하는 애플리케이션을 검사하고 제어하려는 경우 알 수 없는 트래픽에 대해 패킷 캡처를 기록할 수 있습니다. 패킷 캡처에서 애플리케이션이 상용 애플리케이션인 것으로 밝혀지면 이 패킷 캡처를 App-ID 개발을 위해 Palo Alto Networks에 제출할 수 있습니다. 내부 애플리케이션인 경우 사용자 지정 App-ID를 생성하거나 애플리케이션 재정의 정책을 정의할 수 있습니다.
- 사용자 지정 애플리케이션 생성 서명을 사용하여 보안 정책에 첨부하거나 사용자 지정 애플리케이션을 생성하고 애플리케이션 재정의 정책을 정의합니다. 사용자 지정 애플리케이션을 사용하면 특성, 카테고리 및 하위 카테고리, 위험, 포트, 시간 제한과 같은 내부 애플리케이션의 정의를 사용자 지정하고 세분화된 정책 제어를 실행하여 네트워크에서 식별되지 않은 트래픽의 범위를 최소화할 수 있습니다. 맞춤형 애플리케이션을 생성하면 **ACC** 및 트래픽 로그에서 애플리케이션을 올바르게 식별할 수 있으며 네트워크의 애플리케이션에 대한 감사/보고에 유용합니다. 사용자 지정 애플리케이션의 경우 애플리케이션을 고유하게 식별하는 서명 및 패턴을 지정하고 애플리케이션을 허용하거나 거부하는 보안 정책에 첨부할 수 있습니다.

  또는 방화벽이 빠른 경로를 사용하여 사용자 지정 애플리케이션을 처리하도록 하려는 경우(레이어 7 검사에 App-ID를 사용하는 대신 레이어 4 검사) 애플리케이션 재정의 정책 규칙에서 사용자 지정 애플리케이션을 참조할 수 있습니다. 사용자 지정 애플리케이션으로 애플리케이션을 재정의하면 Layer-7 검사인 App-ID 엔진에서 세션이 처리되지 않습니다. 대신 방화벽이 세션을 Layer-4에서 정기적인 상태 저장 검사 방화벽으로 처리하도록 하여 애플리케이션 처리 시간을 절약합니다.

  예를 들어, 호스트 헤더 ***www.mywebsite.com***에서 트리거되는 사용자 지정 애플리케이션을 빌드하는 경우 패킷은 먼저 웹 브라우징으로 식별된 다음 사용자 지정 애플리케이션(상위 애플리케이션이 웹 브라우징임)과 일치합니다. 상위 애플리케이션은 웹 브라우징이기 때문에 맞춤형 애플리케이션은 Layer-7에서 검사되고 콘텐츠와 취약점이 있는지 검사됩니다.

  애플리케이션 재정의를 정의하면 방화벽이 Layer-4에서 처리를 중지합니다. 사용자 지정 애플리케이션 이름은 로그에서 식별하는 데 도움이 되도록 세션에 할당되며 트래픽에서 위협이 검색되지 않습니다.


©2023 Palo Alto Networks, Inc.

# 신규 및 수정된 App-ID 관리

신규 및 수정된 App-ID는 애플리케이션 및 위협 콘텐츠 업데이트의 일부로 방화벽에 포워딩됩니다. 신규 및 수정된 App-ID를 사용하면 방화벽이 보안 정책을 더욱 정확하게 시행할 수 있지만 콘텐츠 업데이트 릴리스가 설치될 때 발생할 수 있는 보안 정책 시행의 변경 사항은 애플리케이션 가용성에 영향을 미칠 수 있습니다. 이러한 이유로 최신 위협 방지 기능을 사용할 수 있도록 콘텐츠 업데이트를 가장 잘 배포하는 방법에 대해 생각하고 신규 및 수정된 App-ID를 최대한 활용하도록 보안 정책을 조정해야 합니다.

다음 옵션을 사용하면 기존 정책 시행에 대한 새로운 App-ID의 영향을 평가하고, App-ID를 비활성화(및 활성화)하고, 정책 규칙을 원활하게 업데이트하여 새로 식별된 애플리케이션을 보호하고 적용할 수 있습니다.

- 신규 및 수정된 앱-아이디를 가장 잘 통합하는 워크플로
- 콘텐츠 릴리스에서 신규 앱 및 수정된 앱-아이디 보기
- 신규 및 수정된 App-ID가 보안 정책에 미치는 영향 보기
- 중요한 신규 앱-아이디가 허용되도록 보장
- 신규 앱-아이디 모니터링
- 앱 ID 사용 안 함 및 사용

콘텐츠 업데이트에서 제공되는 애플리케이션 태그를 사용하는 간소화된 앱 ID 정책 규칙도 활용할 수 있습니다.

## 신규 및 수정된 앱-아이디를 가장 잘 통합하는 워크플로

이 마스터 워크플로를 참조하여 먼저 애플리케이션 및 위협 콘텐츠 업데이트를 설정한 다음 신규 및 수정된 App-ID를 보안 정책에 부합하도록 통합합니다. 콘텐츠 업데이트를 배포하는 데 필요한 모든 것이 여기에서 참조됩니다.

**STEP 1 |** 애플리케이션 및 위협 콘텐츠 업데이트 배포에 대한 접근 방식으로 비즈니스 요구 사항을 조정하십시오.

애플리케이션 및 위협 콘텐츠 업데이트가 작동하는 방식에 대해 알아보고 조직이 중요 업무 또는 보안 우선인지 확인하십시오. 이들 중 비즈니스에 가장 중요한 것이 무엇인지 이해하면 콘텐츠 업데이트에 최적화된 배포 방법을 결정하고 비즈니스 요구 사항을 충족하기 위해 모범 사례를 적용하는 데 도움이 됩니다. 방화벽 배포(데이터 센터 또는 경계) 또는 사무실 위치(원격 또는 본사)에 따라 두 접근 방식을 혼합하여 적용하려는 경우가 있습니다.

**STEP 2 |** 조직의 네트워크 보안 및 애플리케이션 가용성 요구 사항에 따라 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례를 검토하고 적용합니다.

**STEP 3 |** 인증 또는 소프트웨어 개발 애플리케이션과 같이 네트워크 전체에 영향을 미칠 수 있는 신규 App-ID를 항상 허용하도록 보안 정책 규칙을 구성합니다.

신규 App-ID 특성은 최신 콘텐츠 릴리스에 도입된 App-ID에만 일치합니다. 보안 정책에 사용하면 중요한 카테고리에 속하는 App-ID에 대한 지속적인 가용성을 보장하면서 신규 App-ID를 기반으로 보안 정책을 미세 조정할 수 있는 한 달의 시간을 제공합니다(중요한 신규 App-ID가 허용되는지 확인).


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 애플리케이션 및 위협 콘텐츠 업데이트 배포 일정을 설정합니다. 여기에는 필요한 보안 정책 업데이트를 수행할 시간이 될 때까지 신규 App-ID 설치를 지연하는 옵션이 포함됩니다(신규 **App-ID** 임계값 사용).

**STEP 5 |** 콘텐츠 업데이트 설치 일정을 설정한 후에는 정기적으로 체크 인하고 콘텐츠 릴리스에서 새 앱과 수정된 App-ID를 확인해야 합니다.

**STEP 6 |** 그런 다음 신규 및 수정된 App-ID가 보안 정책에 미치는 영향을 확인하고 필요에 따라 보안 정책을 조정할 수 있습니다.

**STEP 7 |** 새 App-ID를 모니터링하여 네트워크의 신규 App-ID 활동을 확인하여 가장 효과적인 보안 정책 업데이트를 수행할 수 있는 최적의 준비를 합니다.

## 콘텐츠 릴리스에서 신규 앱 및 수정된 앱-아이디 보기

다운로드한 콘텐츠 업데이트와 설치된 콘텐츠 업데이트 모두에 대해 업데이트에 포함된 새 앱 ID와 수정된 앱 ID 목록을 볼 수 있습니다. 전체 애플리케이션 세부 정보가 제공되며 네트워크 전체에 영향을 미치는 애플리케이션 업데이트(예: LDAP 또는 IKE)는 정책 검토를 위해 권장되는 것으로 눈에 띄게 표시됩니다. 수정된 앱 ID의 경우 애플리케이션 세부 정보도 현재 적용 범위가 확장되거나 더 정확하게 어떻게 적용되는지를 설명합니다.

**STEP 1 |** 디바이스 > 동적 업데이트를 선택한 다음 지금 확인을 선택하여 사용 가능한 콘텐츠 업데이트 목록을 새로 고칩니다.

**STEP 2 |** 다운로드했거나 현재 설치된 콘텐츠 릴리스의 경우 작업 열에서 앱 검토 링크를 클릭하여 해당 릴리스에서 새로 식별되고 수정된 애플리케이션에 대한 세부 정보를 확인합니다.

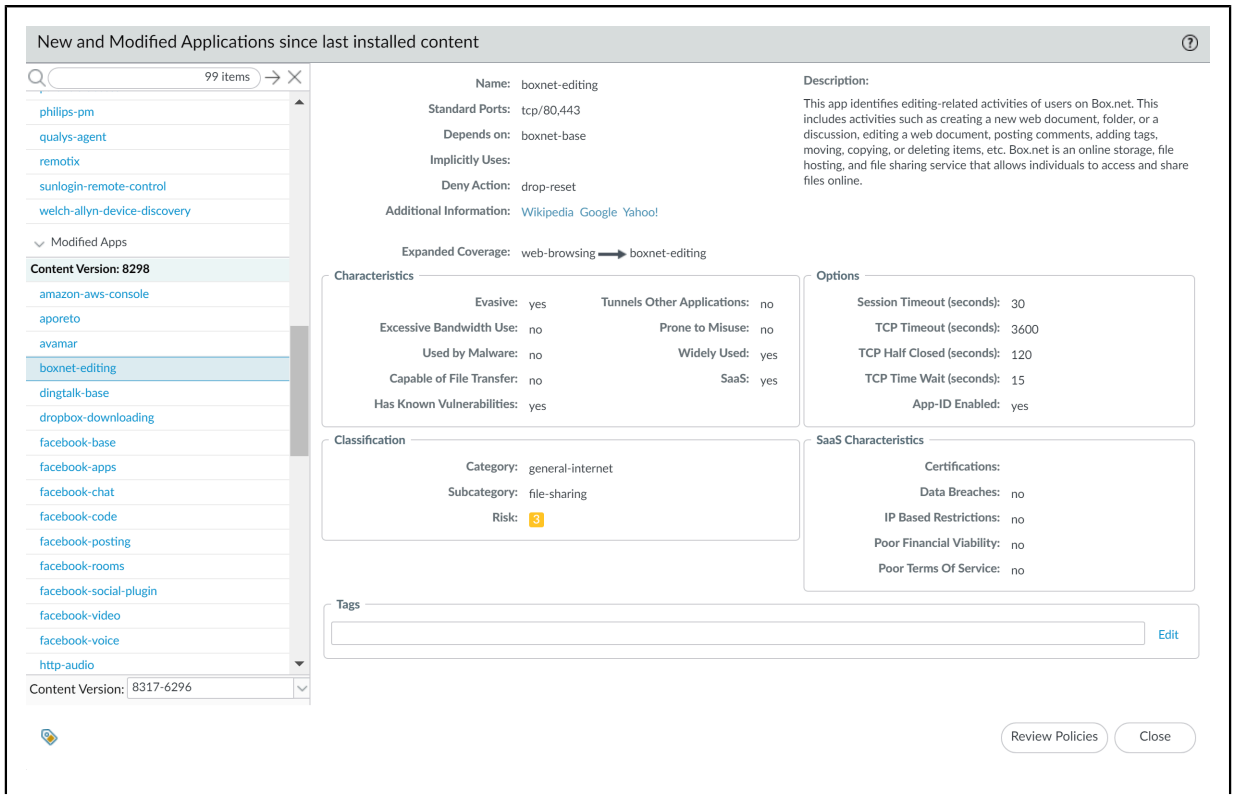
Applications and Threats **Last checked:** 2020/09/23 01:02:02 PDT **Schedule:** Every Wednesday at 01:02 (Download only)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8292-6181 | panupv2-all-apps-8292-6181 | Apps | Full | 47 MB | | 2020/07/13 11:46:39 PDT | ✓ previously | | Revert | Release Notes |
| 8317-6296 | panupv2-all-apps-8317-6296 | Apps | Full | 48 MB | | 2020/09/08 17:55:10 PDT | | ✓ | Review Policies<br>Review Apps | Release Notes |
| 8320-6309 | panupv2-all-contents-8320-6309 | Apps, Threats | Full | 56 MB | 192cfd8c2ff0058c188d0... | 2020/09/14 18:13:54 PDT | | | Download | Release Notes |
| 8320-6310 | panupv2-all-contents-8320-6310 | Apps, Threats | Full | 57 MB | 2436f79a8f02aeef37b82... | 2020/09/15 10:19:15 PDT | | | Download | Release Notes |
| 8321-6311 | panupv2-all-contents-8321-6311 | Apps, Threats | Full | 56 MB | d3ac74a854c08527869cf... | 2020/09/15 13:44:29 PDT | | | Download | Release Notes |
| 8321-6312 | panupv2-all-contents-8321-6312 | Apps, Threats | Full | 57 MB | a4275ee394b5d942c09e... | 2020/09/15 14:26:20 PDT | | | Download | Release Notes |

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 이 콘텐츠 릴리스에서 최신 콘텐츠 버전 이후에 소개하거나 수정한 앱 ID를 검토합니다.

새 앱 ID와 수정된 앱 ID는 별도로 나열됩니다. 각각에 대한 전체 애플리케이션 세부 정보가 제공되며, Palo Alto Networks가 네트워크 전체에 영향을 미칠 것으로 예상하는 앱 ID는 정책 검토를 위해 권장되는 것으로 플래그가 지정됩니다.




정책 적용에 미칠 수 있는 영향을 평가하는 데 사용할 수 있는 새로운 앱 ID 세부 정보는 다음과 같습니다.

- 종속 대상 —이 애플리케이션 ID가 애플리케이션을 고유하게 식별하는 데 사용하는 애플리케이션 서명을 나열합니다. 종속 항목 필드에 나열된 애플리케이션 서명 중 하나가 비활성화된 경우 종속 앱 ID도 비활성화됩니다.
- 이전 식별자 —애플리케이션을 고유하게 식별하기 위해 새 앱 ID가 설치되기 전에 애플리케이션과 일치하는 앱 ID를 나열합니다.
- 앱 **ID** 사용 - 콘텐츠 업데이트를 설치하기 전에 앱 ID 서명을 수동으로 비활성화하도록 선택하지 않는 한 콘텐츠 릴리스를 다운로드할 때 모든 앱 ID가 활성화된 것으로 표시됩니다.

수정된 앱 ID의 경우 세부 정보에는 다음 정보가 포함됩니다. 적용 범위 확대, 가양성 제거 및 애플리케이션 메타데이터 변경 확장 적용 범위 및 가양성 제거 필드는 모두 애플리케이션의 적용 범위가 변경된 방식(보다 포괄적이거나 구체적임)을 나타내며 시계 아이콘은 특정 애플리케이션 세부 정보가 업데이트되는 메타데이터 변경을 나타냅니다.

**STEP 4 |** 검색 결과에 따라 정책 검토를 클릭하여 새 앱 ID와 수정된 앱 ID가 보안 정책 적용에 어떤 영향을 미치는지 확인합니다. 신규 및 수정된 App-ID가 보안 정책에 미치는 영향 보기.


©2023 Palo Alto Networks, Inc.

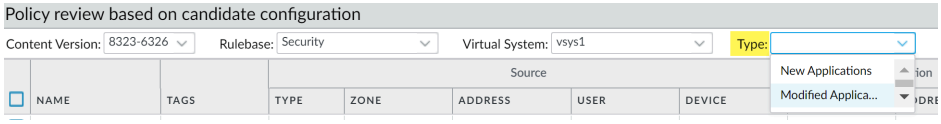
# 신규 및 수정된 App-ID가 보안 정책에 미치는 영향 보기

새로 분류되고 수정된 App-ID는 방화벽이 트래픽을 적용하는 방식을 변경할 수 있습니다. 콘텐츠 업데이트 정책 검토를 수행하여 신규 및 수정된 App-ID가 보안 정책에 미치는 영향을 확인하고 필요한 조정을 쉽게 수행합니다. 다운로드한 콘텐츠와 설치된 콘텐츠 모두에 대해 콘텐츠 업데이트 정책 검토를 수행할 수 있습니다.

**STEP 1 |** 디바이스 > 동적 업데이트를 선택합니다.

**STEP 2 |** 콘텐츠 릴리스에서 도입하거나 수정하는 각 App-ID에 대해 자세히 알아보려면 콘텐츠 릴리스의 신규 및 수정된 App-ID를 참조하십시오.

**STEP 3 |** 다운로드하거나 현재 설치된 콘텐츠 릴리스의 경우 작업 열에서 정책 검토를 클릭합니다. 후보 구성 대화 상자를 기반으로 하는 정책 검토를 통해 콘텐츠 버전별로 필터링하고 특정 릴리스에 도입된 신규 또는 수정된 App-ID를 볼 수 있습니다(규칙 베이스, 가상 시스템 및 애플리케이션).




**STEP 4 |** 현재 애플리케이션을 시행하는 정책 규칙을 보려면 애플리케이션 드롭다운에서 App-ID를 선택합니다. 표시된 규칙은 새 App-ID가 설치되기 전에 애플리케이션과 일치하는 App-ID를 기반으로 합니다(애플리케이션이 새 App-ID 이전과 같이 이전에 식별된 애플리케이션 서명 목록을 보려면 애플리케이션 세부 정보 보기).

**STEP 5 |** 정책 검토에 제공된 세부 정보를 사용하여 App-ID가 설치될 때 적용되도록 정책 규칙 업데이트를 계획하거나 App-ID가 포함된 콘텐츠 릴리스 버전이 현재 설치된 경우 변경 사항이 즉시 적용됩니다.

선택한 정책에 앱을 추가하거나 선택한 정책에서 앱을 제거할 수 있습니다.

# 중요한 신규 앱-아이디가 허용되도록 보장

신규 앱 ID로 인해 특정 애플리케이션에 속한 것으로 새로 식별된 트래픽에 대한 정책 적용이 변경될 수 있습니다. 보안 정책 적용에 대한 영향을 완화하기 위해 보안 정책 규칙에서 신규 앱 **ID** 특성을 사용하면 신규 앱 ID가 설치될 때 구성을 변경하지 않고도 규칙이 항상 가장 최근에 도입된 앱 ID를 적용하도록 할 수 있습니다. 신규 App-ID의 특성은 항상 가장 최근에 설치된 콘텐츠 릴리스의 신규 앱 ID에만 일치합니다. 새 콘텐츠 릴리스가 설치되면 신규 App-ID 특성이 해당 콘텐츠 릴리스 버전의 신규 앱 ID에만 자동으로 일치하기 시작합니다.

모든 신규 앱 ID를 적용하거나 보안 정책 규칙을 대상으로 네트워크 전체에 영향을 미치거나 심각한 영향을 미칠 수 있는 특정 유형의 신규 앱 ID를 적용할 수 있습니다(예: 인증 또는 소프트웨어 개발 애플리케이션만 적용). 보안 정책 규칙을 허용으로 설정하여 앱 ID 릴리스에서 중요한 애플리케이션에 대해 확장되거나 더 정확한 적용 범위가 도입되더라도 방화벽이 해당 애플리케이션을 계속 허용하도록 합니다.

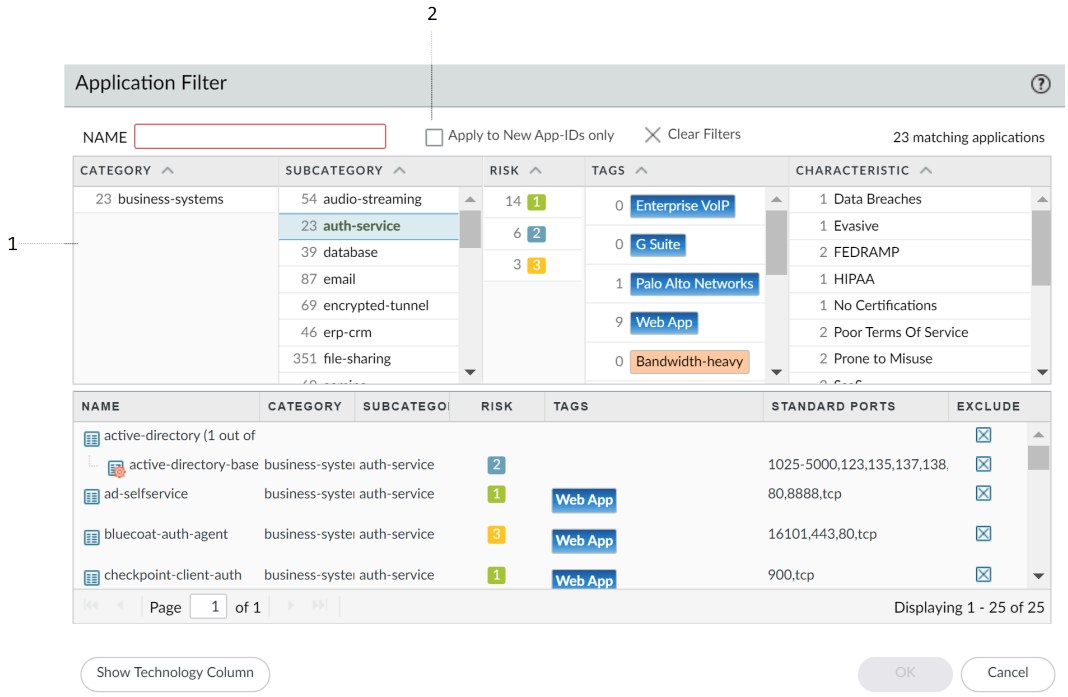
신규 앱 ID는 매월 릴리스되므로 최신 앱 ID를 허용하는 정책 규칙은 한 달의 기간(또는 방화벽에서 일정에 따라 콘텐츠 업데이트를 설치하지 않는 경우 다음에 수동으로 콘텐츠를 설치할 때까지)을 제공하여 새로 분류된 애플리케이션이 보안 정책 적용에 미치는 영향과 필요한 모든 조정을 수행하는지 평가합니다.

**STEP 1 |** 개체 > 애플리케이션 필터 및 새 애플리케이션 필터 추가를 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 하위 카테고리 또는 특성을 기반으로 지속적인 가용성을 보장하려는 새 애플리케이션 유형을 정의합니다. 예를 들어 인증을 수행하거나 지원하는 것으로 알려진 새로 설치된 애플리케이션이 모두 허용되도록 하려면 “auth-service” 카테고리를 선택합니다.

**STEP 3 |** 설치 즉시 허용할 새 애플리케이션의 유형을 좁혀서 새 애플리케이션 **ID**에만 적용을 선택합니다.




**STEP 4 |** 정책 > 보안을 선택한 다음 일치하는 트래픽을 허용하도록 구성된 보안 정책 규칙을 추가하거나 편집합니다.

**STEP 5 |** 애플리케이션을 선택한 다음 새 애플리케이션 필터를 정책 규칙에 일치 조건으로 추가합니다.

**STEP 6 |** 확인 및 커밋을 클릭하여 변경 사항을 저장합니다.

**STEP 7 |** 신규 앱 ID에 도입된 적용 변경 사항을 고려하여 보안 정책을 계속 조정하려면 다음과 같이 하세요.

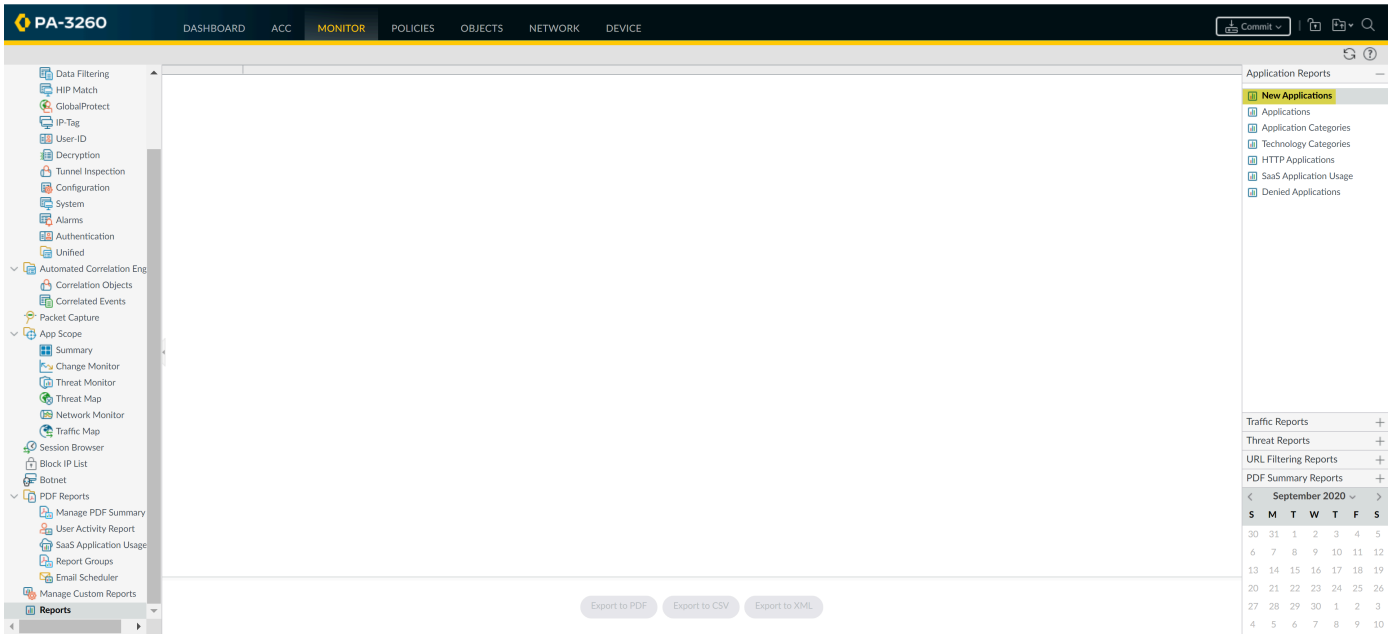
- 신규 앱 ID 모니터링 —신규 App-ID 활동을 모니터링하고 보고서를 가져옵니다.
- 콘텐츠 릴리스의 신규 앱 ID 및 수정된 앱 ID를 참조하십시오. 새로 설치된 앱 ID가 기존 보안 정책 규칙에 어떤 영향을 미치는지 확인하십시오.

## 신규 앱-아이디 모니터링

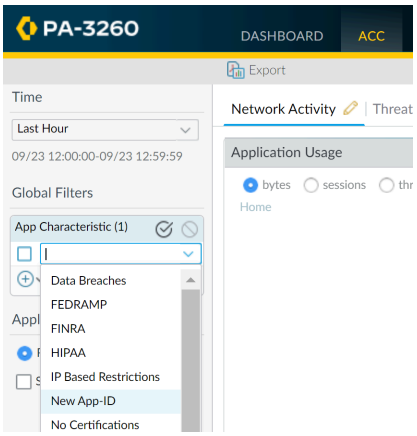
새 **App-ID** 특성을 사용하면 네트워크의 새 애플리케이션을 모니터링할 수 있으므로 수행하려는 보안 정책 업데이트를 더 잘 평가할 수 있습니다. ACC의 새 앱 ID 특성을 사용하여 네트워크의 새 애플리케이션에 대한 가시성을 확보하고 새로 분류된 애플리케이션 활동을 자세히 설명하는 보고서를 생성합니다. 배운 내용은 가장 최근에 분류된 App-ID를 적용하기 위해 보안 정책을 업데이트하는 방법에 대한 올바른 결정을 내리는 데 도움이 될 수 있습니다. ACC에서 보고서를 생성하기 위해 사용하든지 상관없이(또는 중요한 새 App-ID가 허용되는지 확인하기 위해), 새 App-ID 특성은 항상 가장 최근에 설치된 콘텐츠 릴리스의 새 App-ID에만 일치합니다. 새 콘텐츠 릴리스가 설치되면 신규 App-ID 특성이 해당 콘텐츠 릴리스 버전의 신규 앱 ID에만 자동으로 일치하기 시작합니다.


©2023 Palo Alto Networks, Inc.

- 특히 새로운 애플리케이션(최신 콘텐츠 릴리스에서만 도입된 애플리케이션)에 대한 세부 정보가 포함된 보고서를 생성합니다.




- ACC를 사용하여 새 애플리케이션 활동 모니터링: **ACC**를 선택한 다음 전역 필터에서 **Application** > **Application Characteristics** > **New App-ID**를 선택합니다.




# 앱 ID 사용 안 함 및 사용

최신 위협 방지 기능을 즉시 활용하고 나중에 App-ID를 활성화하려는 경우 콘텐츠 릴리스에 도입된 모든 App-ID를 비활성화할 수 있으며 특정 애플리케이션에 대해 App-ID를 비활성화할 수 있습니다.

App-ID를 참조하는 정책 규칙은 활성화된 App-ID를 기반으로 트래픽과만 일치하고 적용합니다.

특정 App-ID는 비활성화할 수 없으며 활성화된 상태만 허용합니다. 비활성화할 수 없는 앱 ID에는 다른 앱 ID(예: unknown-tcp)에서 암시적으로 사용하는 애플리케이션 서명이 포함됩니다. 기본 App-ID를 비활성화하면 기본 App-ID에 의존하는 App-ID도 비활성화될 수 있습니다. 예를 들어 facebook-base를 비활성화하면 다른 모든 Facebook App-ID가 비활성화됩니다.


©2023 Palo Alto Networks, Inc.

- 콘텐츠 릴리스 또는 예약된 콘텐츠 업데이트의 모든 App-ID를 비활성화합니다.

  이 옵션을 사용하면 위협으로부터 보호할 수 있지만 나중에 App-ID를 활성화할 수 있는 옵션을 제공하므로 Palo Alto Networks는 정기적으로 App-ID를 비활성화하는 대신 보안 정책을 신규 App-ID 임시 허용하여 구성할 것을 권장합니다. 이 규칙은 항상 최신 콘텐츠 릴리스에만 도입된 신규 App-ID를 허용합니다. 신규 App-ID를 포함하는 콘텐츠 업데이트는 한 달에 한 번만 릴리스되므로 신규 App-ID를 평가하고 필요한 경우 신규 App-ID를 포함하도록 보안 정책을 조정할 시간이 주어지며 동시에 중요한 애플리케이션은 영향을 받지 않습니다.

  - 콘텐츠 릴리스에 도입된 모든 신규 App-ID를 비활성화하려면 어플라이언스 > 동적 업데이트를 선택한 다음 애플리케이션 및 위협 콘텐츠 릴리스를 설치합니다. 메시지가 표시되면 콘텐츠 업데이트에서 신규 앱 비활성화를 선택합니다. 앱을 비활성화하고 콘텐츠 업데이트 설치를 계속하려면 체크박스를 선택합니다.
  - **Device** > **Dynamic Updates** 페이지에서 일정을 선택합니다. 콘텐츠 릴리스의 다운로드 및 설치에 대해 콘텐츠 업데이트에서 신규 앱 비활성화를 선택합니다.

- 한 번에 하나의 애플리케이션 또는 여러 애플리케이션에 대해 App-ID를 비활성화합니다.

  - 단일 애플리케이션 또는 여러 애플리케이션을 동시에 빠르게 비활성화하려면 개체 > 애플리케이션을 클릭합니다. 하나 이상의 애플리케이션 체크박스를 선택한 다음 비활성화를 클릭합니다.
  - 단일 애플리케이션에 대한 세부 정보를 검토한 다음 해당 애플리케이션에 대한 App-ID를 비활성화하려면 개체 > 애플리케이션 및 **App-ID** 비활성화를 선택합니다. 이 단계를 사용하여 보류 중인 App-ID(App-ID를 포함하는 콘텐츠 릴리스가 방화벽에 다운로드되지만 설치되지는 않음) 또는 설치된 App-ID를 모두 비활성화할 수 있습니다.

- 앱 ID를 활성화합니다.

  **Objects** > **Applications**를 선택하여 이전에 비활성화한 App-ID를 활성화합니다. 하나 이상의 애플리케이션 체크박스를 선택한 다음 활성화를 클릭하거나 특정 애플리케이션에 대한 세부 정보를 열고 **App-ID** 활성화를 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 정책에 애플리케이션 개체 사용

애플리케이션 개체를 사용하여 보안 정책이 애플리케이션을 처리하는 방법을 정의합니다.

- 애플리케이션 그룹 생성
- 애플리케이션 필터 생성
- 사용자 지정 애플리케이션 생성
- 애플리케이션 종속성 해결

## 애플리케이션 그룹 생성

애플리케이션 그룹은 정책에서 유사하게 처리하려는 애플리케이션이 포함된 개체입니다. 애플리케이션 그룹은 조직 내에서 사용하도록 명시적으로 승인한 애플리케이션에 대한 액세스를 활성화하는 데 유용합니다. 승인된 애플리케이션을 그룹화하면 규칙 베이스 관리가 간소화됩니다. 지원하는 애플리케이션에 변경 사항이 있을 때 개별 정책 규칙을 업데이트하는 대신 영향을 받는 애플리케이션 그룹만 업데이트할 수 있습니다.

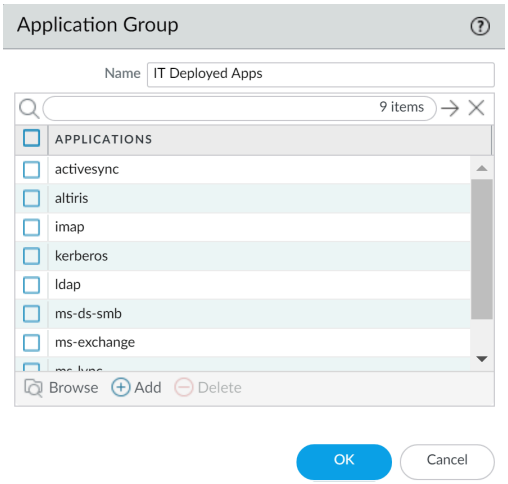
애플리케이션을 그룹화하는 방법을 결정할 때 승인된 애플리케이션에 대한 액세스를 적용하고 각 정책 목표에 맞는 애플리케이션 그룹을 만드는 방법을 고려하십시오. 예를 들어 IT 관리자만 액세스할 수 있도록 허용할 일부 애플리케이션과 조직의 알려진 사용자가 사용할 수 있도록 하려는 다른 애플리케이션이 있을 수 있습니다. 이 경우 이러한 정책 목표 각각에 대해 별도의 애플리케이션 그룹을 생성합니다. 일반적으로 기본 포트에서만 애플리케이션에 대한 액세스를 활성화하려고 하지만 이에 대한 예외인 애플리케이션을 그룹화하고 별도의 규칙에서 해당 애플리케이션에 대한 액세스를 적용할 수 있습니다.

**STEP 1 |** 개체 > 애플리케이션 그룹을 선택합니다.

**STEP 2 |** 그룹을 추가하고 설명이 포함된 이름을 지정합니다.

**STEP 3 |** (선택 사항) Panorama에서 공유 개체로 액세스하거나 다중 가상 시스템 방화벽의 모든 가상 시스템에서 사용하기 위해 공유 위치에 개체를 생성하려면 공유를 선택합니다.

**STEP 4 |** 그룹에 원하는 애플리케이션을 추가한 다음 확인을 클릭합니다.





©2023 Palo Alto Networks, Inc.

**STEP 5 |** 구성을 커밋합니다.

## 애플리케이션 필터 생성

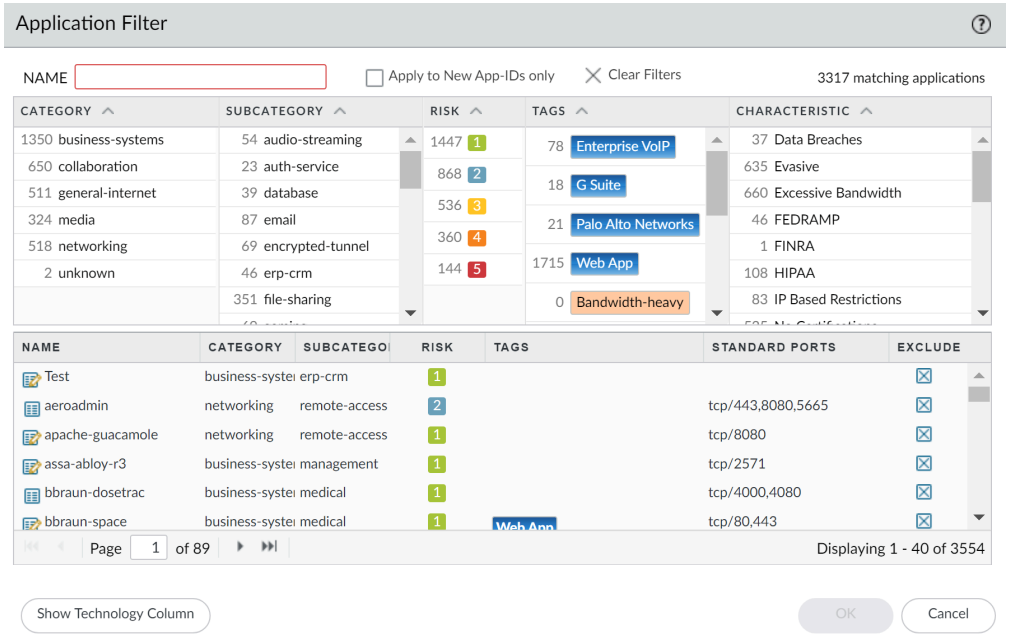
애플리케이션 필터는 카테고리, 하위 카테고리, 기술, 위험 계수 및 특성을 포함하여 정의하는 애플리케이션 특성을 기반으로 애플리케이션을 동적으로 그룹화하는 개체입니다. 이는 명시적으로 승인하지는 않지만 사용자가 액세스할 수 있도록 하려는 애플리케이션에 대한 액세스를 안전하게 활성화하려는 경우에 유용합니다. 예를 들어 직원들이 비즈니스용으로 자신의 사무실 프로그램(예: 에버노트, Google 문서 또는 Microsoft Office 365)을 선택할 수 있도록 할 수 있습니다. 이러한 유형의 애플리케이션을 안전하게 사용하도록 설정하려면 카테고리 비즈니스 시스템과 하위 카테고리 사무실 프로그램에 일치하는 애플리케이션 필터를 만들 수 있습니다. 새 애플리케이션 사무실 프로그램이 등장하고 신규 앱-ID가 생성되면 이러한 새로운 애플리케이션은 정의된 필터와 자동으로 일치합니다. 필터에 대해 정의된 특성과 일치하는 애플리케이션을 안전하게 사용하도록 정책 규칙 베이스를 추가로 변경할 필요가 없습니다.

**STEP 1 |** 개체 > 애플리케이션 필터를 선택합니다.

**STEP 2 |** 필터를 추가하고 설명이 포함된 이름을 지정합니다.

**STEP 3 |** (선택 사항) Panorama에서 공유 개체로 액세스하거나 다중 가상 시스템 방화벽의 모든 가상 시스템에서 사용하기 위해 공유 위치에 개체를 생성하려면 공유를 선택합니다.

**STEP 4 |** 카테고리, 하위 카테고리, 기술, 위험 및 특성 섹션에서 속성 값을 선택하여 필터를 정의합니다. 값을 선택하면 대화 상자 하단에 있는 일치하는 애플리케이션 목록이 좁아지는 것을 알 수 있습니다. 필터 특성을 안전하게 사용하도록 설정하려는 애플리케이션 유형에 맞게 조정한 경우 확인을 클릭합니다.




**STEP 5 |** 구성을 커밋합니다.

## 사용자 지정 애플리케이션 생성

애플리케이션을 안전하게 사용하도록 설정하려면 항상 모든 포트에서 모든 트래픽을 분류해야 합니다. App-ID를 사용하면 일반적으로 알 수 없는 트래픽(tcp, udp 또는 비syn-tcp)으로 분류되는 유일한 애플리


©2023 Palo Alto Networks, Inc.

케이션인 ACC 및 트래픽 로그는 아직 네트워크의 App-ID, 내부 또는 사용자 지정 애플리케이션에 추가되지 않았거나 잠재적인 위협에 추가되지 않은 상용 애플리케이션입니다.

아직 ***App-ID***가 없는 상용 애플리케이션에 대한 알 수 없는 트래픽이 있는 경우 http://researchcenter.paloaltonetworks.com/submit-an-application/에서 신규 앱 ***ID*** 요청서를 제출할 수 있습니다.

내부 사용자 지정 애플리케이션이 알 수 없는 트래픽으로 표시되지 않도록 하려면 사용자 지정 애플리케이션을 생성합니다. 그런 다음 네트워크에서 확인되지 않은 트래픽 범위를 최소화하여 공격 표면을 줄이기 위해 이러한 애플리케이션에 대한 세분화된 정책 제어를 수행할 수 있습니다. 또한 사용자 지정 애플리케이션을 만들면 ACC 및 Traffic 로그의 애플리케이션을 올바르게 식별할 수 있으므로 네트워크의 애플리케이션을 감사/보고할 수 있습니다.

사용자 지정 애플리케이션을 만들려면 해당 특성, 카테고리 및 하위 카테고리, 위험, 포트, 타임아웃과 같은 애플리케이션 특성을 정의해야 합니다. 또한 방화벽이 트래픽 플로우 자체(서명)에 맞게 사용할 수 있는 패턴이나 값을 정의해야 합니다. 마지막으로 사용자 지정 애플리케이션을 허용하거나 거부하는 보안 정책에 첨부하거나 애플리케이션 그룹에 추가하거나 애플리케이션 필터에 일치시킬 수 있습니다. 또한 월드컵 축구 또는 3월의 광란에 대한 ESPN3-비디오와 같은 화제성이 있는 임시 애플리케이션을 식별하기 위해 사용자 정의 애플리케이션을 만들 수 있습니다.

사용자 지정 애플리케이션 서명을 만들기 위해 올바른 데이터를 수집하려면 패킷 캡처와 데이터 그램의 형성 방식을 잘 이해해야 합니다. 서명이 너무 광범위하게 만들어지면 실수로 다른 유사한 트래픽이 포함될 수 있습니다. 너무 좁게 정의된 경우 패턴과 엄격하게 일치하지 않으면 트래픽이 감지를 회피합니다.

사용자 지정 애플리케이션은 방화벽의 별도의 데이터베이스에 저장되며 이 데이터베이스는 주간 앱 ***ID*** 업데이트의 영향을 받지 않습니다.

방화벽이 프로토콜 내부 터널링될 수 있는 애플리케이션을 감지할 수 있도록 지원하는 애플리케이션 프로토콜 디코더에는 콘텐츠 릴리스 버전 *609*의 다음이 포함됩니다**: *FTP, HTTP, IMAP, POP3, SMB* 및 *SMTP.***

다음은 사용자 지정 애플리케이션을 만드는 방법에 대한 기본 예입니다.

**STEP 1 |** 사용자 지정 서명을 작성하는 데 사용할 수 있는 애플리케이션에 대한 정보를 수집합니다.

이렇게 하려면 애플리케이션에 대한 이해와 애플리케이션에 대한 액세스를 제어하는 방법을 이해해야 합니다. 예를 들어 사용자가 애플리케이션 내에서 수행할 수 있는 작업(예: 업로드, 다운로드 또는 라이브 스트리밍)을 제한할 수 있습니다. 또는 애플리케이션을 허용하지만 QoS 치안을 적용할 수 있습니다.

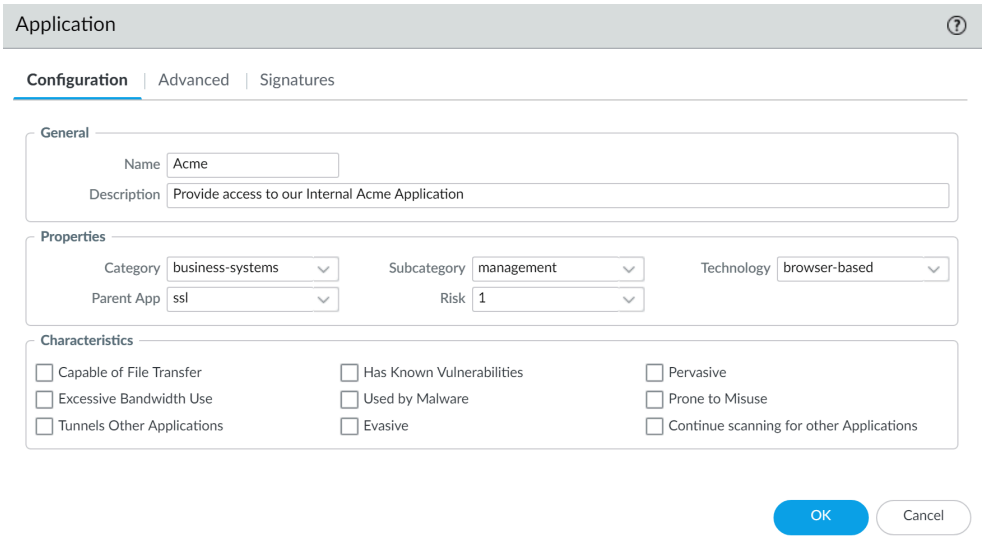
- 사용자 지정 애플리케이션 서명을 기반으로 하는 애플리케이션에 대한 고유한 특성을 찾을 수 있도록 애플리케이션 패킷을 캡처합니다. 이를 수행하는 한 가지 방법은 클라이언트 시스템에서 Wireshark와 같은 프로토콜 분석기를 실행하여 클라이언트와 서버 간의 패킷을 캡처하는 것입니다. 생성 패킷 캡처(PCAP)에서 각 세션 유형을 찾을 수 있도록 업로드 및 다운로드와 같은 애플리케이션에서 다른 작업을 수행합니다.

 ©2023 Palo Alto Networks, Inc.

- 기본적으로 방화벽은 알 수 없는 모든 트래픽에 대한 패킷 캡처를 사용하므로 방화벽이 클라이언트와 서버 사이에 있는 경우 트래픽 로그에서 직접 알 수 없는 트래픽에 대한 패킷 캡처를 볼 수 있습니다.
- 패킷 캡처를 사용하여 애플리케이션 트래픽과 고유하게 일치하는 서명을 만드는 데 사용할 수 있는 패킷 컨텍스트에서 패턴이나 값을 찾습니다. 예를 들어 HTTP 응답 또는 요청 헤더, URI 경로 또는 호스트 이름에서 문자열 패턴을 찾습니다. 애플리케이션 서명을 만드는 데 사용할 수 있는 다른 문자열 컨텍스트에 대한 정보와 패킷에서 해당 값을 찾을 수 있는 위치에 대한 자세한 내용은 사용자 지정 보안 서명 생성를 참조하십시오.

**STEP 2 |** 사용자 지정 애플리케이션을 추가합니다.

1. 개체 > 애플리케이션을 선택하고 추가를 클릭합니다.
2. 구성 탭에서 다른 관리자가 애플리케이션을 만든 이유를 이해하는 데 도움이 되도록 사용자 정의 애플리케이션에 대한 이름 및 설명을 입력합니다.
3. (선택 사항) Panorama에서 공유 개체로 액세스하거나 다중 가상 시스템 방화벽의 모든 가상 시스템에서 사용하기 위해 공유 위치에 개체를 생성하려면 공유를 선택합니다.
4. 애플리케이션 속성 및 특성을 정의합니다.




**STEP 3 |** 기본 프로토콜, 애플리케이션이 실행되는 포트 번호, 타임아웃 값 및 트래픽에서 수행할 수 있는 모든 유형의 검색과 같은 애플리케이션에 대한 세부 정보를 정의합니다.

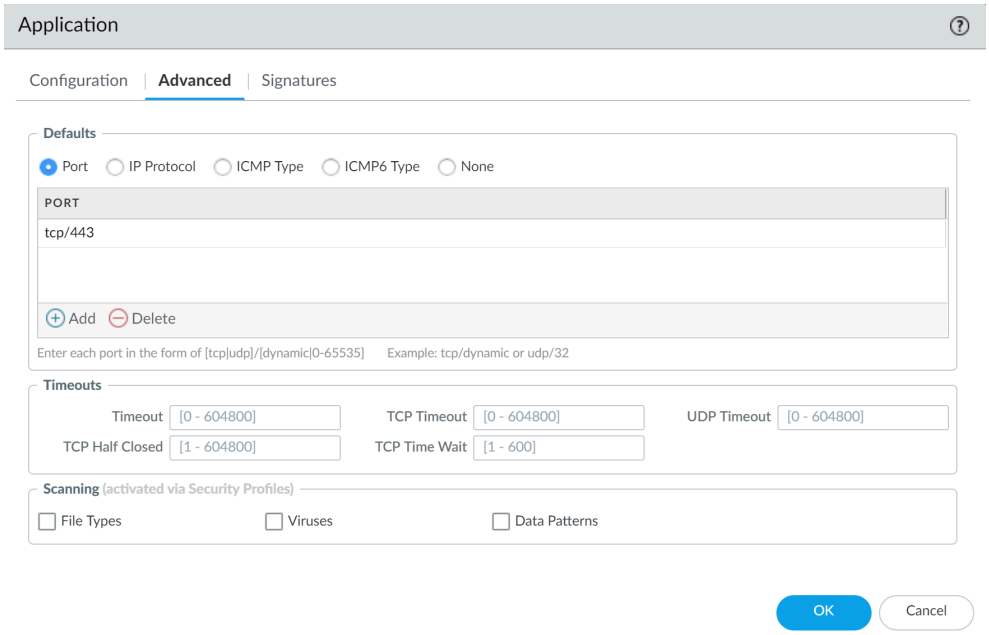
고급 탭에서 방화벽이 애플리케이션 프로토콜을 식별할 수 있는 설정을 정의합니다.

- 애플리케이션에서 사용하는 기본 포트 또는 프로토콜을 지정합니다.
- 세션 타임아웃 값을 지정합니다. 타임아웃 값을 지정하지 않으면 기본 시간 설정 값이 사용됩니다.
- 애플리케이션 트래픽에서 수행할 추가 검색 유형을 나타냅니다.

예를 들어 SSL을 통해 실행되지만 포트 4443(SSL의 기본 포트 대신 443)을 사용하는 사용자 지정 TCP 기반 애플리케이션을 만들려면 포트 번호를 지정합니다. 사용자 지정 애플리케이션에 대한 포트

 ©2023 Palo Alto Networks, Inc.

번호를 추가하면 방화벽에서 추가 포트를 여는 대신 애플리케이션의 기본 포트를 사용하는 정책 규칙을 만들 수 있습니다. 이렇게 하면 보안 태세가 향상됩니다.




**STEP 4 |** 방화벽이 새 애플리케이션에 대한 트래픽을 일치시키는 데 사용할 기준을 정의합니다.

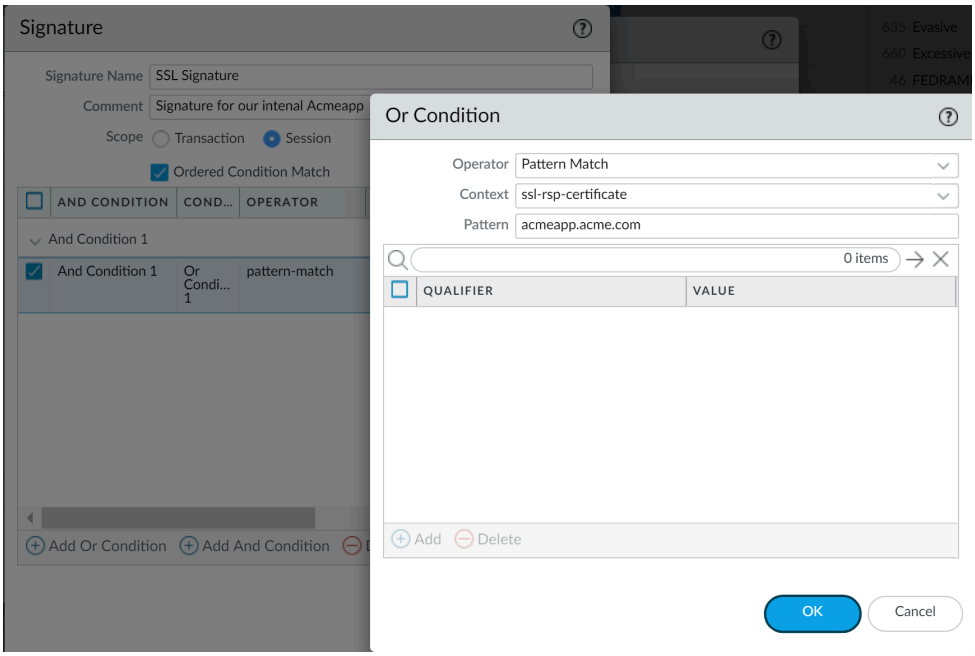
패킷 캡처에서 수집한 정보를 사용하여 방화벽이 애플리케이션 트래픽의 패턴과 일치하는 데 사용할 수 있는 고유한 문자열 컨텍스트 값을 지정합니다.

1. 서명 탭에서 추가를 클릭하고 서명 이름을 정의하고 선택적으로 설명을 정의하여 이를 사용하려는 방법에 대한 정보를 제공합니다.
2. 전체 세션 또는 단일 트랜잭션과 일치하는지 여부와 같이 서명의 범위를 지정합니다.
3. 추가 및 조건 또는 추가 또는 조건을 클릭하여 서명을 정의할 조건을 지정합니다.
4. 연산자를 선택하여 사용할 일치 조건 유형을 정의합니다. 패턴 일치또는같음.
   - 패턴 일치를 선택한 경우 컨텍스트를 선택한 다음 정규식을 사용하여 선택한 컨텍스트와 일치하도록 패턴을 정의합니다. 선택적으로 추가를 클릭하여 수식어/값 쌍을 정의합니다. 한정자 목록은 선택한 컨텍스트에 따라 다릅니다.
   - 등등에서, 선택한 경우 컨텍스트를 선택한 다음 정규 식을 사용하여 패킷 헤더의 바이트 위치를 정의하여 선택한 컨텍스트와 일치합니다. 첫 번째 **4**바이트 또는 두 번째 **4**바이트 중에


©2023 Palo Alto Networks, Inc.

서 선택하십시오. 마스크(예: 0xffffff00) 및 값(예: 0xaabbccdd)의 4바이트 hex 값을 정의합니다.

예를 들어 내부 애플리케이션 중 하나에 대한 사용자 지정 애플리케이션을 만드는 경우 **ssl-rsp-**인증서 컨텍스트를 사용하여 서버의 SSL 협상의 인증서 응답 메시지에 대한 패턴 일치를 정의하고 여기에 표시된 메시지의 서버의 공통 이름과 일치하는 패턴을 만들 수 있습니다.




5. 일치하는 각 조건에 대해 4.c 및 4.d 단계를 반복합니다.
6. 방화벽이 서명 정의를 일치시키려고 시도하는 순서가 중요한 경우 **Ordered Condition Match** 확인란이 선택되어 있는지 확인한 다음 적절한 순서로 평가되도록 조건을 정렬합니다. 조건 또는 그룹을 선택한 다음 위로 이동하거나 아래로 이동을 클릭합니다. 한 그룹에서 다른 그룹으로 조건을 이동할 수 없습니다.
7. 확인을 클릭하여 서명 정의를 저장합니다.

**STEP 5 |** 애플리케이션을 저장합니다.

1. 사용자 지정 애플리케이션 정의를 저장하려면 확인을 클릭합니다.
2. 커밋을 클릭합니다.

**STEP 6 |** 트래픽이 예상대로 사용자 지정 애플리케이션과 일치하는지 확인합니다.

1. 새 애플리케이션을 허용하도록 정책 > 보안 및 보안 정책 추가 규칙을 선택합니다.
2. 방화벽과 애플리케이션 사이에 있는 클라이언트 시스템에서 애플리케이션을 실행한 다음 트래픽 로그(트래픽 > 모니터링)를 확인하여 새 애플리케이션과 일치하는 트래픽이 있는지 확인하고 정책 규칙에 따라 처리되고 있는지 확인합니다.

## 애플리케이션 종속성 해결

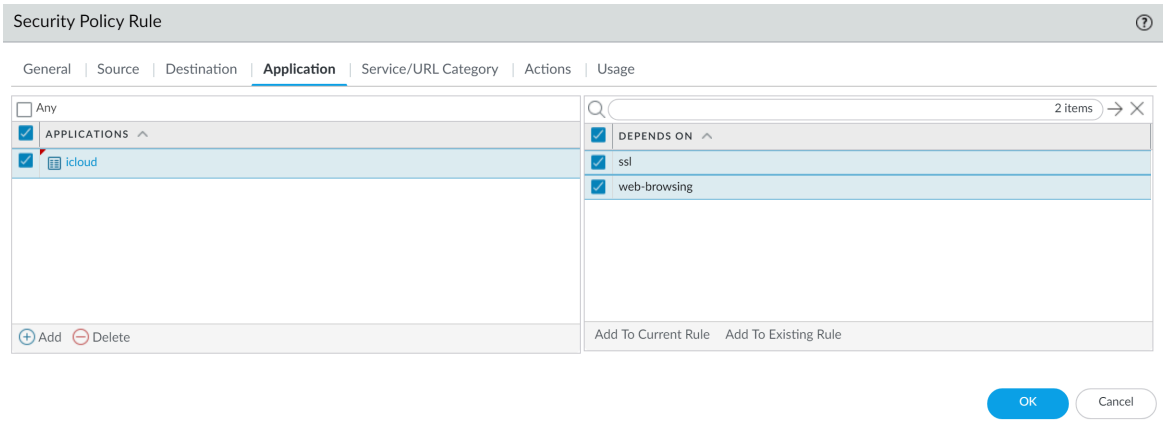
새 보안 정책 규칙을 만들 때와 커밋을 수행할 때 애플리케이션 종속성을 볼 수 있습니다. 정책에 모든 애플리케이션 종속성을 포함하지 않는 경우 연결된 보안 정책 규칙에 직접 액세스하여 필요한 애플리케이션을 추가할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 보안 정책 규칙을 생성합니다.

**STEP 2 |** 규칙이 허용하거나 차단할 애플리케이션을 지정합니다.

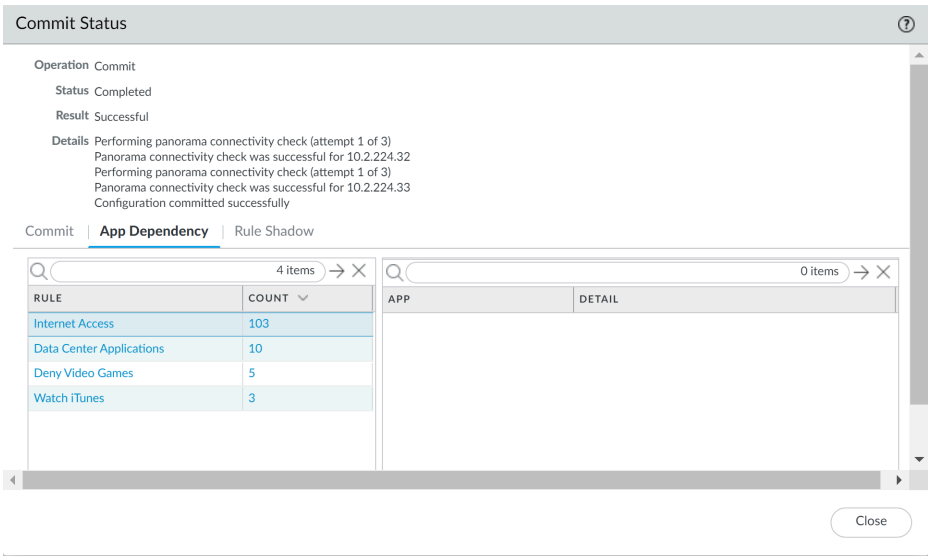
1. 애플리케이션 탭에서 안전하게 활성화할 애플리케이션 애플리케이션을 추가합니다. 여러 애플리케이션을 선택하거나 애플리케이션 그룹 또는 애플리케이션 필터를 사용할 수 있습니다.
2. 선택한 애플리케이션에 대한 종속성을 보고 현재 규칙에 추가하거나 기존 규칙에 추가합니다.




3. 기존 규칙에 추가하는 경우 규칙을 선택하고 확인을 클릭합니다.

**STEP 3 |** 확인을 클릭하고 변경 사항을 커밋합니다.

1. 앱 종속성 탭에서 커밋 경고를 검토합니다.




2. 포함되지 않은 애플리케이션 종속성을 보려면 개수를 선택합니다.
3. 규칙을 선택하여 정책을 열고 종속성을 추가합니다.

   종속 애플리케이션을 해결하거나 커밋에 대한 경고를 계속 생성합니다.

4. 확인을 클릭하고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 기본 포트에서 애플리케이션 안전하게 활성화

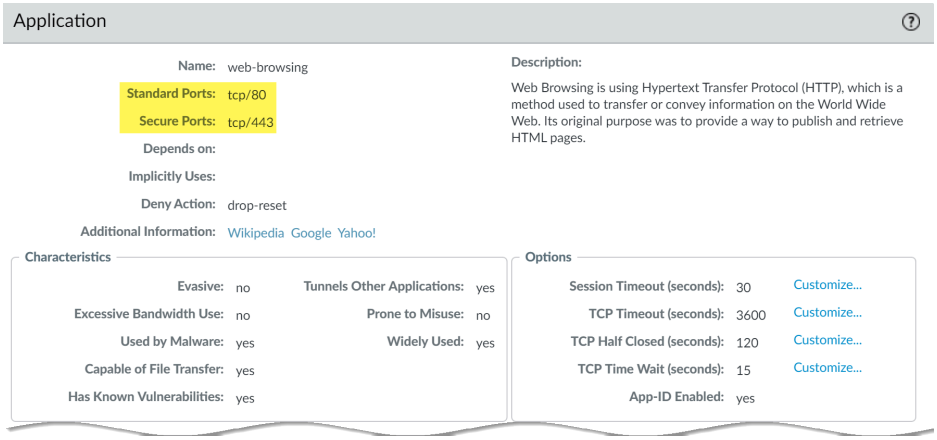
비정상적인 포트에서 실행되는 애플리케이션은 기존 포트 기반 보호를 우회하려는 공격자를 나타낼 수 있습니다. 애플리케이션 기본값은 이러한 유형의 이베이전을 방지하고 가장 일반적으로 사용되는 포트에서 애플리케이션을 안전하게 활성화할 수 있는 쉬운 방법을 제공하는 Palo Alto Networks 방화벽의 기능입니다. 애플리케이션 기본값은 애플리케이션 기반 보안 정책에 대한 모범 사례입니다. 관리 오버헤드를 줄이고 포트 기반 정책으로 인해 발생하는 보안 격차를 줄입니다.

- 오버헤드 감소 - 애플리케이션 간 매핑을 조사하고 유지 관리하는 대신 비즈니스 요구 사항에 따라 간단한 애플리케이션 기반 보안 정책 규칙을 작성합니다. App-ID가 있는 모든 애플리케이션에 대한 기본 포트를 정의했습니다.
- 더 강력한 보안 - 애플리케이션이 기본 포트에서만 실행되도록 하는 것이 보안 모범 사례입니다. 애플리케이션 기본값은 애플리케이션이 예기치 않은 방식으로 작동하는 경우 보안을 손상시키지 않고 중요한 애플리케이션을 사용할 수 있도록 합니다.

  또한 애플리케이션이 사용하는 기본 포트는 애플리케이션이 암호화되었는지 아니면 일반 텍스트인지에 따라 달라질 수 있습니다. 포트 기반 정책에서는 애플리케이션이 암호화를 설명하는 데 사용할 수 있는 모든 기본 포트를 열어야 합니다. 열린 포트는 공격자가 보안 정책을 우회하기 위해 활용할 수 있는 보안 격차를 유발합니다. 그러나 애플리케이션 기본값은 암호화된 애플리케이션 트래픽과 일반 텍스트 애플리케이션 트래픽을 구분합니다. 이는 암호화 여부와 관계없이 애플리케이션에 대한 기본 포트를 적용할 수 있음을 의미합니다.

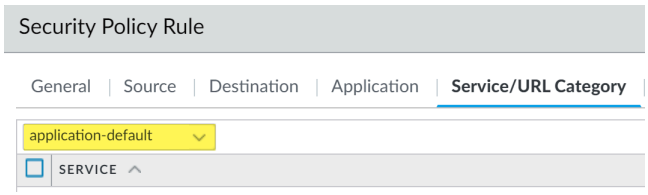
  예를 들어 애플리케이션 기본값이 없으면 웹 브라우징 트래픽을 활성화하려면 포트 80과 443을 열어야 합니다. 두 포트 모두에서 일반 텍스트와 암호화된 웹 브라우징 트래픽을 모두 허용하게 됩니다. 애플리케이션 기본값이 켜져 있으면 방화벽은 포트 80에서만 일반 텍스트 웹 브라우징 트래픽을, 포트 443에서는 SSL 터널링된 트래픽을 엄격하게 적용합니다.

애플리케이션이 기본적으로 사용하는 포트를 보려면 Applipedia를 방문하거나 개체 > 애플리케이션를 선택합니다. 애플리케이션 세부 정보에는 애플리케이션의 표준 포트(일반 텍스트일 때 가장 일반적으로 사용하는 포트)가 포함됩니다. 웹 브라우징의 경우 SMTP, FTP, LDAP, POP3 및 IMAP 세부 정보에는 애플리케이션의 보안 포트(애플리케이션이 암호화될 때 사용하는 포트)도 포함됩니다.




정책 > 보안을 선택한 다음 기본 포트에서만 애플리케이션을 적용하도록 규칙을 추가하거나 수정합니다.


©2023 Palo Alto Networks, Inc.




애플리케이션 기반 보안 정책의 일부로 ***SSL*** 복호화과 함께 애플리케이션 기본값을 사용하는 것이 모범 사례입니다. 또한 서비스가 ***service-http*** 및 ***service-https***로 설정된 웹 브라우징 트래픽을 제어하는 기존 보안 정책 규칙이 있는 경우 해당 규칙을 업데이트하여 ***application-default***를 대신 사용해야 합니다.


©2023 Palo Alto Networks, Inc.

# 암시적 지원이 있는 애플리케이션

특정 애플리케이션을 허용하는 정책을 만들 때는 애플리케이션이 의존하는 다른 애플리케이션도 허용해야 합니다. 대부분의 경우 방화벽이 종속성을 확인하고 암시적으로 허용할 수 있으므로 트래픽 플로우를 위해 종속 애플리케이션에 대한 액세스를 명시적으로 허용할 필요가 없습니다. 이 암시적 지원은 HTTP, SSL, MS-RPC 또는 RTSP를 기반으로 하는 사용자 지정 애플리케이션에도 적용됩니다. 방화벽이 종속 애플리케이션을 정시에 결정할 수 없는 애플리케이션은 정책을 정의할 때 종속 애플리케이션을 명시적으로 허용해야 합니다. 다음 중 하나를 사용하여 애플리케이션 기반 보안 정책 워크플로 내에서 애플리케이션 종속성을 결정할 수 있습니다.

- 정책 최적화 프로그램
- 태그를 사용하여 애플리케이션 필터 생성
- 사용자 지정 태그를 기반으로 애플리케이션 필터 생성
- 애플리케이션 종속성 해결

필요한 경우 Applipedia도 사용할 수 있습니다.

다음 표에는 방화벽이 암시적으로 지원하는 애플리케이션이 나열되어 있습니다(Content Update 595 기준).

| 애플리케이션 | 암시적 지원 |
|---|---|
| 360-safeguard-update | http |
| apple-update | http |
| apt-get | http |
| as2 | http |
| avg-update | http |
| avira-antivir-update | http, ssl |
| blokus | rtmp |
| bugzilla | http |
| clubcooee | http |
| corba | http |
| cubby | http, ssl |
| dropbox | ssl |


©2023 Palo Alto Networks, Inc.

| 애플리케이션 | 암시적 지원 |
|---|---|
| esignal | http |
| evernote | http, ssl |
| ezhelp | http |
| facebook | http, ssl |
| facebook-chat | jabber |
| facebook-social-plugin | http |
| fastviewer | http, ssl |
| forticlient-update | http |
| good-for-enterprise | http, ssl |
| google-cloud-print | http, ssl, jabber |
| google-desktop | http |
| google-talk | jabber |
| google-update | http |
| gotomypc-desktop-sharing | citrix-jedi |
| gotomypc-file-transfer | citrix-jedi |
| gotomypc-printing | citrix-jedi |
| hipchat | http |
| iheartradio | ssl, http, rtmp |
| infront | http |
| instagram | http, ssl |
| issuu | http, ssl |
| java-update | http |
| jepptech-updates | http |


©2023 Palo Alto Networks, Inc.

| 애플리케이션 | 암시적 지원 |
|---|---|
| kerberos | rpc |
| kik | http, ssl |
| lastpass | http, ssl |
| logmein | http, ssl |
| mcafee-update | http |
| megaupload | http |
| metatrader | http |
| mocha-rdp | t_120 |
| mount | rpc |
| ms-frs | msrpc |
| ms-rdp | t_120 |
| ms-scheduler | msrpc |
| ms-service-controller | msrpc |
| nfs | rpc |
| oovoo | http, ssl |
| paloalto-updates | ssl |
| panos-global-protect | http |
| panos-web-interface | http |
| pastebin | http |
| pastebin-posting | http |
| pinterest | http, ssl |
| portmapper | rpc |
| prezi | http, ssl |


©2023 Palo Alto Networks, Inc.

| 애플리케이션 | 암시적 지원 |
|---|---|
| rdp2tcp | t_120 |
| renren-im | jabber |
| roboform | http, ssl |
| salesforce | http |
| stumbleupon | http |
| supremo | http |
| symantec-av-update | http |
| trendmicro | http |
| trillian | http, ssl |
| twitter | http |
| whatsapp | http, ssl |
| xm-radio | rtsp |


©2023 Palo Alto Networks, Inc.

# 보안 정책 규칙 최적화

Policy Optimizer는 레거시 보안 정책 규칙 기반을 App-ID 기반 규칙베이스로 마이그레이션하는 간단한 워크플로를 제공합니다. 이렇게 하면 공격 영역을 줄이고 애플리케이션에 대한 가시성을 확보하여 안전하게 활성화할 수 있으므로 보안을 강화할 수 있습니다. Policy Optimizer는 포트 기반 규칙을 식별하므로 애플리케이션 가용성을 저하시키지 않고 애플리케이션 기반 허용 규칙으로 변환하거나 포트 기반 규칙의 애플리케이션을 기존 애플리케이션 기반 규칙에 추가할 수 있습니다. 또한 과도하게 프로비저닝된 앱 ID 기반 규칙(사용하지 않는 애플리케이션으로 구성된 앱 ID 규칙)을 식별합니다. Policy Optimizer를 사용하면 먼저 마이그레이션할 포트 기반 규칙의 우선 순위를 지정하고, 사용하지 않는 애플리케이션을 허용하는 애플리케이션 기반 규칙을 식별하며, 적중 횟수와 같은 규칙 사용 특성을 분석할 수 있습니다.

포트 기반 규칙을 애플리케이션 기반 규칙으로 변환하면 허용할 애플리케이션을 선택한 다음 다른 모든 애플리케이션을 거부할 수 있으므로 네트워크에서 원치 않는 트래픽과 잠재적으로 악의적인 트래픽을 제거하므로 보안 상태가 향상됩니다. 애플리케이션 트래픽을 기본 포트로 제한하는 것과 결합하여(서비스를 **application-default**로 설정) 애플리케이션 기반 규칙으로 변환하면 회피 애플리케이션이 비표준 포트에서 실행되는 것을 방지할 수도 있습니다.

이 기능은 다음 경우에 사용할 수 있습니다.

- PAN-OS 버전 9.0을 실행하고 앱 ID가 활성화된 방화벽입니다.
- PAN-OS 버전 9.0을 실행하는 Panorama. Panorama가 정책 최적화 프로그램 기능을 사용하기 위해 관리하는 방화벽을 업그레이드할 필요가 없습니다. 그러나 규칙 사용 기능(정책 규칙 사용 모니터링)을 사용하려면 관리되는 방화벽이 PAN-OS 8.1 이상을 실행해야 합니다. 관리되는 방화벽이 로그 수집기에 연결되는 경우 해당 로그 컬렉터도 PAN-OS 버전 9.0을 실행해야 합니다. 로그 처리 카드(LPC) 가 있는 관리형 PA-7000 시리즈 방화벽도 PAN-OS 8.1 이상을 실행할 수 있습니다.
- Cortex Data Lake 호환성을 위해 Cloud Services 플러그인 2.0 Innovation 이상이 설치된 PAN-OS 10.0.3 이상을 실행하는 Panorama.

> ***PA-7000*** 시리즈 방화벽은 ***PA-7000*** 시리즈 방화벽 로그 처리 카드***(LPC)***와 고성능 ***PA-7000*** 시리즈 방화벽 로그 전달 카드***(LFC)***의 두 가지 로깅 카드를 지원합니다. ***LPC***와 달리 ***LFC***에는 로그를 로컬로 저장할 디스크가 없습니다. 대신 ***LFC***는 모든 로그를 ***Panorama*** 또는 ***syslog*** 서버와 같은 하나 이상의 외부 로깅 시스템으로 포워딩합니다. ***LFC***를 사용하는 경우 트래픽 로그가 로컬에 저장되지 않기 때문에 정책 최적화 프로그램에 대한 애플리케이션 사용 정보가 방화벽에 표시되지 않습니다. ***LPC***를 사용하는 경우 트래픽 로그가 방화벽에 로컬로 저장되므로 정책 최적화 프로그램에 대한 애플리케이션 사용 정보가 방화벽에 표시됩니다.

이 기능을 사용하여 다음을 수행합니다.

- 포트 기반 규칙을 애플리케이션 기반 규칙으로 마이그레이션 - 트래픽 로그를 종합하고 애플리케이션을 포트 기반 규칙에 수동으로 매핑하는 대신 Policy Optimizer를 사용하여 포트 기반 규칙을 식별하고 각 규칙과 일치하는 애플리케이션을 나열하면 허용할 애플리케이션을 선택하고 안전하게 활성화할 수 있습니다. 레거시 포트 기반 규칙을 애플리케이션 기반 허용 규칙으로 변환하면 비즈니스 애플리케이션이 지원되며 악성 활동과 관련된 모든 애플리케이션을 차단할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

- 과도하게 프로비저닝된 애플리케이션 기반 규칙 식별 - 너무 광범위한 규칙은 네트워크에서 사용하지 않는 애플리케이션을 허용하여 공격 표면을 증가시키고 악의적인 트래픽을 의도하지 않게 허용할 위험을 증가시킵니다.

  보안 정책 규칙에서 사용하지 않는 애플리케이션을 제거하여 공격 표면을 줄이고 규칙 기반을 깨끗하게 유지하십시오. 네트워크에서 아무도 사용하지 않는 애플리케이션을 허용하지 마십시오.

- 보안 정책 규칙에 앱 **ID** 클라우드 엔진**(ACE)** 애플리케이션 추가 - SaaS 보안 인라인 구독이 있는 경우 정책 최적화 프로그램의 새 앱 뷰어를 사용하여 보안 정책에서 클라우드 제공 앱 ID를 관리할 수 있습니다. ACE 설명서에서는 정책 최적화 프로그램을 사용하여 클라우드 제공 앱 ID에 대한 가시성을 확보하고 제어하는 방법을 설명합니다.

  이 섹션의 정책 최적화 프로그램 예제는 ***SaaS*** 보안 인라인 구독이 없는 방화벽을 묘사하기 때문에 새 앱 뷰어를 표시하지 않습니다.

레거시 방화벽에서 ***Palo Alto Networks*** 디바이스로 구성을 마이그레이션하려면 애플리케이션 기반 정책으로 마이그레이션하는 모범 사례를 참조하십시오.

정렬을 수행하면 rulebase의 규칙 순서가 변경되므로 보안 > 정책에서 보안 정책 규칙을 정렬할 수 없습니다. 그러나 정책 > 보안 > 정책 최적화 프로그램에서 정책 최적화 프로그램에서는 규칙 순서에 영향을 주지 않는 정렬 옵션을 제공하므로 규칙을 정렬하여 변환하거나 정리할 규칙의 우선 순위를 지정할 수 있습니다. 지난 30일 동안의 트래픽 양, 규칙에 표시된 애플리케이션 수, 새 애플리케이션이 없는 일 수 및 허용된 애플리케이션 수(과도하게 프로비전된 규칙의 경우)를 기준으로 규칙을 정렬할 수 있습니다.

Policy Optimizer는 사전 프로덕션 규칙의 유효성 검사 및 기존 규칙 문제 해결 등 다른 방법으로도 사용할 수 있습니다. 정책 최적화 프로그램은 일시적인 애플리케이션이 규칙에 계산되지 않도록 세션 종료 시 로그만 적용하고 세션 시작 시 로그를 무시합니다.

리소스 제약으로 인해 ***VM-50 Lite*** 가상 방화벽은 정책 최적화 프로그램을 지원하지 않습니다.

- 정책 최적화 프로그램 개념
- 포트 기반을 앱 ID 기반 보안 정책 규칙으로 마이그레이션
- 규칙 복제 마이그레이션 사용 사례: 웹 브라우징 및 SSL 트래픽
- 기존 규칙에 애플리케이션 추가
- 사용되지 않는 애플리케이션을 사용하여 보안 정책 규칙 식별
- 애플리케이션 사용 통계에 대한 고가용성
- 정책 최적화 프로그램을 비활성화하는 방법

## 정책 최적화 프로그램 개념

이 기능의 지원에 대해 자세히 알아보려면 다음 항목을 검토하세요.

- 보안 정책 규칙 정렬 및 필터링
- 애플리케이션 사용 데이터 지우기

 ©2023 Palo Alto Networks, Inc.

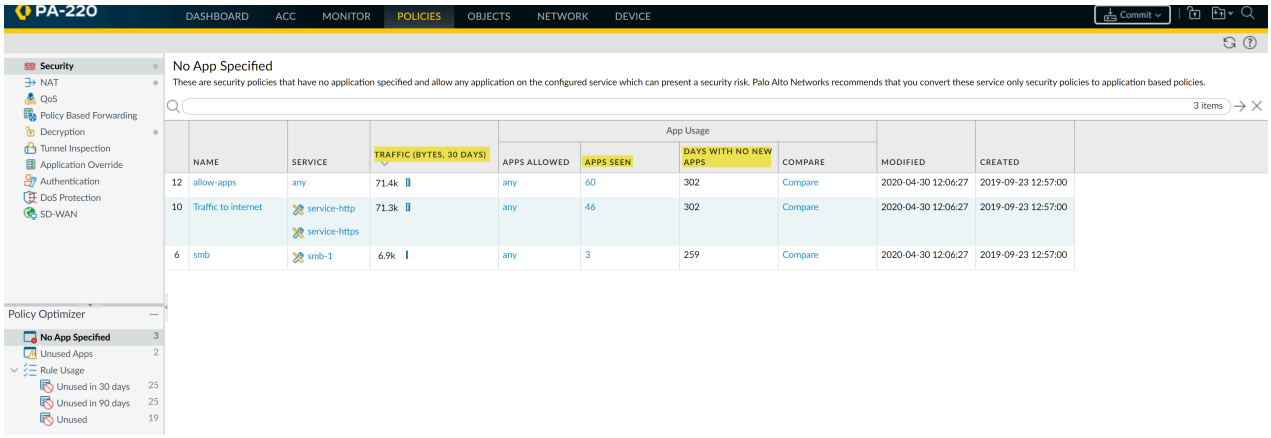
## 보안 정책 규칙 정렬 및 필터링

보안 정책 규칙을 필터링하여 애플리케이션이 구성되지 않은 규칙인 포트 기반 규칙을 볼 수 있습니다(**Policies** > **Security** > **Policy Optimizer** > **No App Specified**). 애플리케이션이 구성된 규칙을 확인하도록 필터링할 수도 있지만 트래픽은 구성된 애플리케이션 중 일부만 일치합니다. 규칙이 초과 프로비저닝되고 규칙에 표시되지 않는 애플리케이션이 포함됩니다(**Policies** > **Security** > **Policy Optimizer** > **Unused Apps**). 또한 SaaS 보안 인라인 라이선스가 있는 경우 새 앱 뷰어를 사용하여 새 App-ID ACE(Cloud Engine) 애플리케이션을 본 규칙을 필터링할 수 있습니다(이를 수행하는 방법은 ACE 설명서 참조). 다양한 유형의 통계를 기반으로 필터링된 정책 규칙을 정렬하여 포트 기반에서 애플리케이션 기반 규칙으로 변환하거나 먼저 정리할 규칙의 우선 순위를 지정할 수 있습니다.

정책 > 보안에서 규칙을 필터링하거나 정렬할 수 없습니다. 그렇게 하면 규칙 베이스의 정책 규칙 순서가 변경되기 때문입니다. ***Policies* > *Security* > *Policy Optimizer* > *No App Specified*, *Policies* > *Security* > *Policy Optimizer* > *Unused Apps*** 및 ***Policies* > *Security* > *Policy Optimizer* > *New App Viewer*(*SaaS* 인라인 보안 구독이 있는 경우)** 필터링 및 정렬는 규칙 베이스의 규칙 순서를 변경하지 않습니다.

여러 열 헤더를 클릭하여 애플리케이션 사용 통계를 기반으로 규칙을 정렬할 수 있습니다. 또한 정책 규칙 사용 보기을(를) 하여, 사용하지 않는 규칙을 식별 및 제거하여 보안 위험을 줄이고 정책 규칙 기반을 체계적으로 유지할 수 있습니다. 규칙 사용 추적을 사용하면 새 규칙 추가 및 규칙 변경을 신속하게 검증하고 작업 및 문제 해결 작업에 대한 규칙 사용을 모니터링할 수 있습니다.


©2023 Palo Alto Networks, Inc.




- 트래픽(바이트, **30**일) - 지난 30일 동안 규칙에 표시된 트래픽 양입니다. 30일 기간은 기본적으로 현재 가장 많은 트래픽과 일치하는 규칙을 목록의 맨 위에 배치합니다(시간이 길수록 목록의 맨 위에 남아 있는 이전 규칙이 더 강조됩니다. 트래픽이 더 이상 표시되지 않을 수 있음). 순서를 반대로 하려면 클릭하십시오.
- 표시되는 앱 - 가장 많이 또는 가장 적게 표시되는 애플리케이션이 있는 규칙을 맨 위에 배치합니다. 방화벽은 애플리케이션 데이터를 자동으로 제거하지 않습니다.

  방화벽은 약 *1*시간마다 표시된 앱을 업데이트합니다. 그러나 많은 양의 애플리케이션 트래픽 또는 많은 수의 규칙이 있는 경우 업데이트하는 데 *1*시간 이상 걸릴 수 있습니다. 규칙에 애플리케이션을 추가한 후 트래픽 로그를 실행하기 전에 최소 한 시간 이상 기다렸다가 애플리케이션의 로그 정보를 확인합니다.
- 새 앱이 없는 날짜 - 마지막 새 애플리케이션이 규칙과 일치한 이후 가장 많거나 적은 날짜가 있는 규칙을 맨 위에 배치합니다.
- (사용하지 않는 앱만 해당) 허용된 앱 - 규칙에 구성된 가장 많거나 적은 애플리케이션이 있는 규칙을 맨 위에 배치합니다.

애플리케이션 사용 통계는 다음 기준을 충족하는 규칙에 대한 애플리케이션만 계산합니다.


©2023 Palo Alto Networks, Inc.

- 규칙의 작업은 허용이어야 합니다.
- 규칙의 로그 설정은 세션 종료 시 로그여야 합니다(기본 로그 설정). 세션 시작 시 기록하는 규칙은 일시적인 애플리케이션 계산을 방지하기 위해 무시됩니다.
- 유효한 트래픽은 규칙과 일치해야 합니다. 예를 들어, 충분한 트래픽이 방화벽을 통과하여 애플리케이션을 식별하기 전에 세션이 종료되면 계산되지 않습니다. 다음 트래픽 유형은 유효하지 않으므로 Policy Optimizer 통계에 포함되지 않습니다.
  - 불충분한 데이터
  - 해당 없음
  - non-syn-tcp
  - 불완전

  트래픽 로그(**Monitor** > **Logs** > 트래픽)를 필터링하여 이러한 유형 중 하나로 식별된 트래픽을 볼 수 있습니다. 예를 들어 불완전한 것으로 식별된 모든 트래픽을 보려면 필터 **(app eq incomplete)**를 사용하십시오.

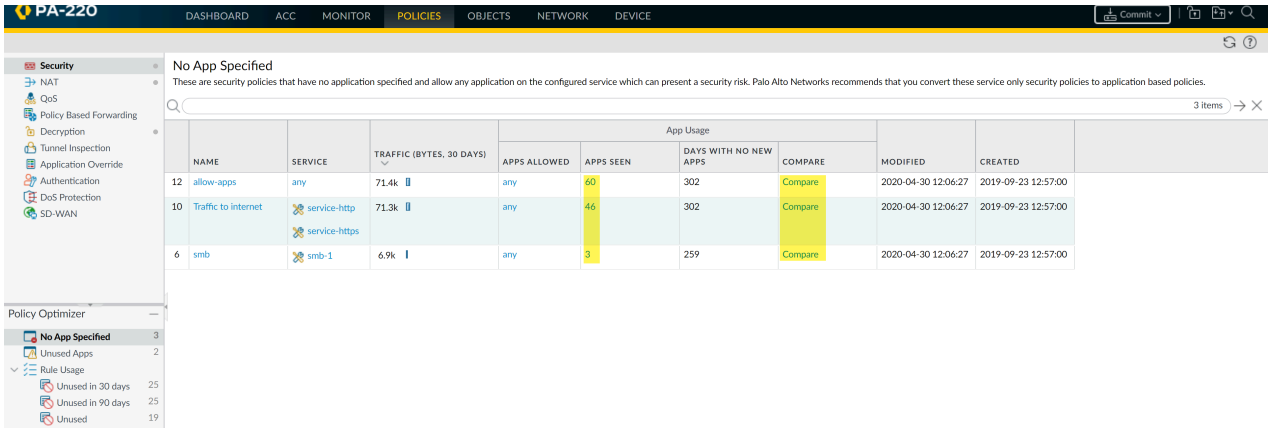
이러한 기준이 충족되지 않으면 애플리케이션은 표시된 앱과 같은 통계에 포함되지 않고 새로운 앱이 없는 날과 같은 통계에 영향을 미치지 않으며 애플리케이션 목록에 나타나지 않습니다.

방화벽은 *interzone-default* 및 *intrazone-default* 보안 정책 규칙에 대한 애플리케이션 사용 통계를 추적하지 않습니다.

규칙의 *UUID*가 변경되면 *UUID* 변경으로 인해 방화벽이 해당 규칙을 다른(새) 규칙으로 보기 때문에 해당 규칙에 대한 애플리케이션 사용 통계가 재설정됩니다.

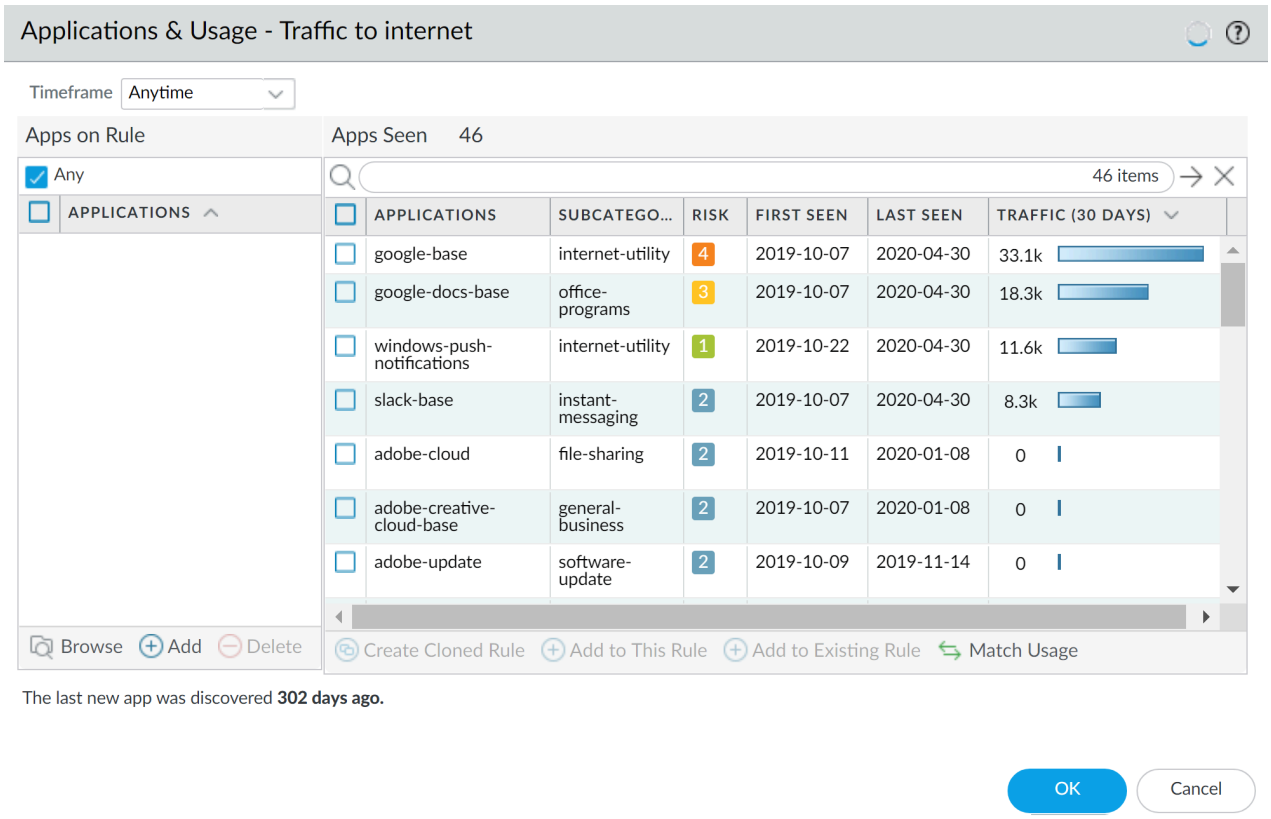
규칙에 표시된 애플리케이션을 보고 정렬하려면 규칙의 행에서 비교를 클릭하거나 표시된 앱에서 숫자를 클릭합니다.

 ©2023 Palo Alto Networks, Inc.




**Policies** > **Security** > **Policy Optimizer** > **No App Specified** 및 **Policies** > **Security** > **Policy Optimizer** > **Unused Apps**에서 볼 수 있는 규칙의 경우 비교 또는 표시된 앱 수를 클릭하면 애플리케이션 및 사용량이 표시되어 규칙에 표시된 애플리케이션과 이를 정렬할 수 있는 기능을 볼 수 있습니다. 애플리케이션 및 사용은 포트 기반을 앱 ID 기반 보안 정책 규칙으로 마이그레이션및 규칙에서 사용하지 않는 애플리케이션을 제거하는 곳이기도 합니다.


©2023 Palo Alto Networks, Inc.




규칙에 표시되는 애플리케이션을 6가지 모두 표시된 앱 통계로 정렬할 수 있습니다(표시된 앱은 실시간으로 업데이트되지 않으며 트래픽 양 및 규칙 수에 따라 업데이트하는 데 1시간 이상 소요됨).

- 애플리케이션 - 애플리케이션 이름은 알파벳순입니다. 규칙의 서비스에 대해 특정 포트 또는 포트 범위를 구성하고(서비스는 임의일 수 없음) 애플리케이션에 대한 표준(애플리케이션 기본) 포트가 있고 구성된 포트가 애플리케이션 기본 포트와 일치하지 않는 경우 노란색 , 애플리케이션 옆에 삼각형 경고 아이콘이 나타납니다.
- 하위 카테고리 - 애플리케이션 콘텐츠 메타데이터에서 파생된 애플리케이션 하위 카테고리별 알파벳순입니다.
- 위험 - 애플리케이션의 위험 등급에 따릅니다.
- 최초 확인 - 규칙에서 애플리케이션이 최초 확인된 날짜입니다. 타임 스탬프 해결은 하루 단위입니다(시간 단위가 아님).
- 최종 확인 - 규칙에서 애플리케이션이 최종으로 확인된 날짜입니다. 타임 스탬프 해결은 하루 단위입니다(시간 단위가 아님).
- 트래픽**(30일)** - 지난 30일 동안 규칙과 일치하는 트래픽(바이트)이 기본 정렬 방법입니다.

특정 기간(언제든지, 지난 **7**일, 지난 **15**일 또는 지난 **30**일)에 대한 통계를 표시하도록 기간을 설정합니다.


©2023 Palo Alto Networks, Inc.

트래픽(*30*일)은 항상 지난 *30*일 동안의 트래픽만 바이트 단위로 표시합니다. 기간을 변경해도 트래픽(*30*일)바이트 측정 기간은 변경되지 않습니다.

열 머리글을 클릭하면 표시 순서가 바뀌고 같은 열을 다시 클릭하면 순서가 바뀝니다. 예를 들어 위험을 클릭하여 애플리케이션을 저위험에서 고위험으로 정렬합니다. 위험을 다시 클릭하여 애플리케이션을 고위험에서 저위험으로 정렬합니다.

방화벽은 정책 최적화 프로그램에 대한 애플리케이션 사용 통계를 실시간으로 보고하지 않으므로 보고서 실행을 대체하지 않습니다.

- 방화벽은 허용된 앱, 표시된 앱 및 애플리케이션 및 사용에 나열된 애플리케이션을 실시간이 아닌 약 1시간마다 업데이트합니다. 트래픽 양이 많거나 규칙이 많은 경우 업데이트 시간이 더 오래 걸릴 수 있습니다. 규칙에 애플리케이션을 추가한 후 트래픽 로그를 실행하기 전에 최소 한 시간 이상 기다렸다가 애플리케이션의 로그 정보를 확인합니다.

  방화벽은 약 1시간마다 표시된 앱을 업데이트합니다. 그러나 많은 양의 애플리케이션 트래픽 또는 많은 수의 규칙이 있는 경우 업데이트하는 데 1시간 이상 걸릴 수 있습니다. 규칙에 애플리케이션을 추가한 후 트래픽 로그를 실행하기 전에 최소 한 시간 이상 기다렸다가 애플리케이션의 로그 정보를 확인합니다.
- 방화벽은 매일 자정 디바이스에서 애플리케이션 및 사용량에서 새 앱이 없는 날과 처음 본 날짜 및 마지막으로 본 날짜를 업데이트합니다.
- 많은 수의 애플리케이션이 있는 규칙의 경우 애플리케이션 사용 통계를 처리하는 데 시간이 더 오래 걸릴 수 있습니다.
- 애플리케이션이 많은 규칙 수가 많은 보안 정책 규칙 베이스의 경우 애플리케이션 사용 통계를 처리하는 데 시간이 더 오래 걸릴 수 있습니다.
- Panorama에서 관리하는 방화벽의 경우 애플리케이션 사용 데이터는 개별 방화벽에 로컬로 구성된 규칙이 아니라 Panorama가 방화벽에 푸시하는 규칙에 대해서만 볼 수 있습니다.

## 애플리케이션 사용 데이터 지우기

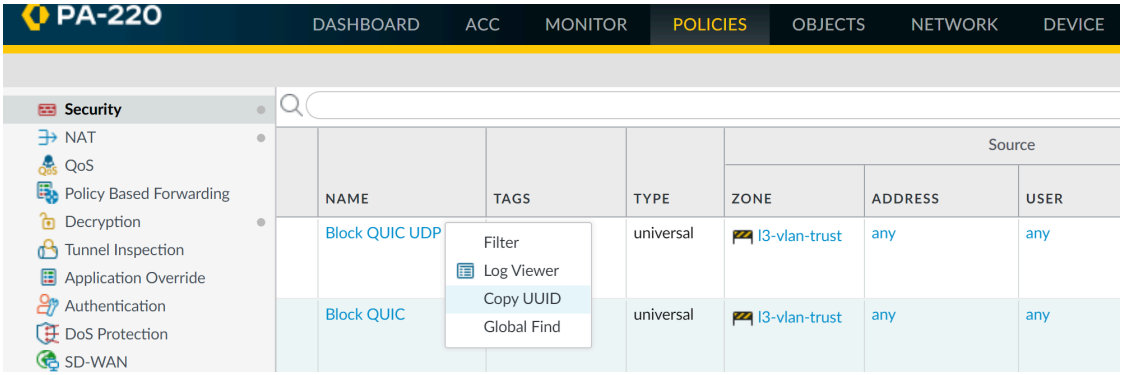
CLI 명령을 사용하여 개별 보안 정책 규칙에 대한 애플리케이션 사용 데이터를 지우고 확인한 앱 및 기타 애플리케이션 사용 데이터를 재설정할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 지우려는 애플리케이션 사용 데이터가 있는 보안 정책 규칙의 UUID를 찾으십시오.

UI에서 UUID를 찾는 방법에는 두 가지가 있습니다.

- 정책 > 보안의 규칙 **UUID** 열에서 UUID를 복사합니다.
- 정책 > 보안의 규칙 이름 드롭다운 메뉴에서 **UUID** 복사를 선택합니다.




**STEP 2 |** UI에서 CLI로 전환합니다.

UI에서 캡처한 UUID를 사용하여 규칙의 애플리케이션 사용 데이터를 지웁니다.

```
admin@PA-VM>clear policy-app-usage-data ruleuuid <uuid-value>
```

규칙의 UUID를 값으로 붙여넣거나 입력하고 명령을 실행하여 규칙의 애플리케이션 사용 데이터를 지웁니다.

## 포트 기반을 앱 ID 기반 보안 정책 규칙으로 마이그레이션

레거시 방화벽에서 Palo Alto Networks 차세대 방화벽으로 전환할 때 포트의 모든 애플리케이션을 허용하는 많은 수의 포트 기반 규칙을 상속받아 모든 애플리케이션이 열려 있는 포트를 사용할 수 있으므로 공격 면적이 증가합니다. 정책 최적화 프로그램은 레거시 포트 기반 보안 정책 규칙에 있는 모든 애플리케이션을 식별하고 해당 규칙에 허용하려는 애플리케이션을 선택할 수 있는 간단한 워크플로우를 제공합니다. 포트 기반 규칙을 애플리케이션 기반 규칙으로 마이그레이션하여 공격 면적을 줄이고 네트워크의 애플리케이션을 안전하게 활성화합니다. 정책 최적화 프로그램을 사용하여 새 애플리케이션을 추가할 때 규칙 기준을 유지관리합니다.

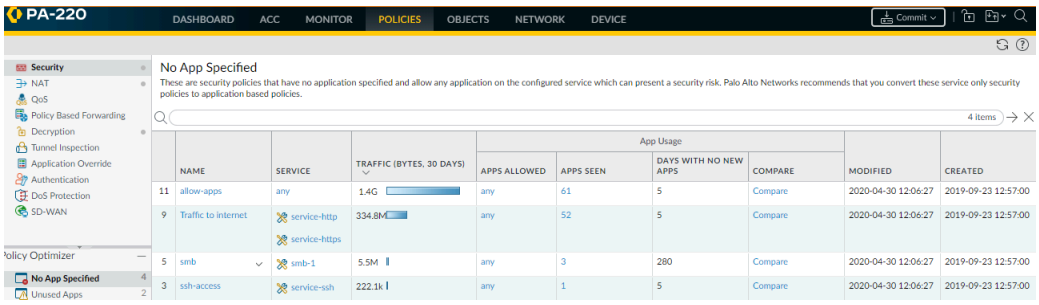
우선 순위가 지정된 방식으로 한 번에 몇 가지 포트 기반 규칙을 애플리케이션 기반 규칙으로 마이그레이션합니다. 점진적인 변환은 한 번에 큰 규칙 베이스를 마이그레이션하는 것보다 안전하며 새 애플리케이션 기반 규칙이 필요한 애플리케이션을 제어하는지 쉽게 확인할 수 있습니다. 정책 최적화를 사용하여 먼저 변환할 규칙의 우선 순위를 지정합니다.

레거시 방화벽에서 *Palo Alto Networks* 디바이스로 구성을 마이그레이션하려면 애플리케이션 기반 정책으로 마이그레이션하는 모범 사례를 참조하세요.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 포트 기반 규칙을 식별합니다.

포트 기반 규칙에는 구성(허용) 애플리케이션이 없습니다. 정책 > 보안 > 정책 최적화 도구 > 지정된 앱 없음은 모든 포트 기반 규칙을 표시합니다(허용된 앱은 모두입니다).




**STEP 2 |** 먼저 변환할 포트 기반 규칙의 우선 순위를 지정합니다.

정책 > 보안 > 정책 최적화 프로그램 > 지정 없음을 사용하면 규칙 기준에서 순서에 영향을 주지 않고 규칙을 정렬할 수 있으며 비즈니스 목표 및 위험 허용 오차에 따라 전환에 대한 규칙의 우선 순위를 지정하는 데 도움이 되는 기타 정보를 제공합니다.

- 트래픽**(**바이트**, 30**일**)** - (정렬하려면 클릭합니다.) 현재 대부분의 트래픽과 일치하는 규칙은 목록의 맨 위에 있습니다. 기본 정렬 순서입니다.
- 표시된 앱 - (정렬하려면 클릭합니다.) 포트 기반 규칙과 일치하는 많은 수의 합법적인 애플리케이션은 애플리케이션, 사용자 및 소스 및 대상을 엄격하게 정의하는 여러 애플리케이션 기반 규칙으로 대체해야 함을 나타낼 수 있습니다. 예를 들어 포트 기반 규칙이 다양한 디바이스 집합에서 여러 사용자 그룹에 대한 여러 애플리케이션의 트래픽을 제어하는 경우 애플리케이션을 합법적인 사용자 및 디바이스와 페어링하여 공격 표면을 줄이고 가시성을 높이는 별도의 규칙을 생성합니다. (표시된 앱 번호 또는 비교를 클릭하면 규칙과 일치하는 애플리케이션이 표시됩니다.)

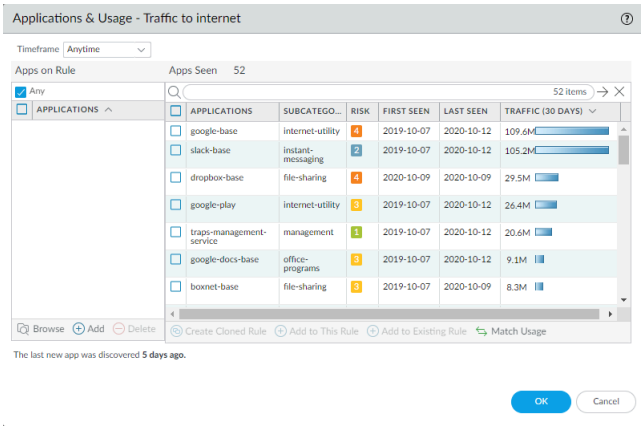
  방화벽은 표시된 앱을 거의 매 시간마다 업데이트합니다**.** 그러나 많은 양의 애플리케이션 트래픽 또는 많은 수의 규칙이 있는 경우 업데이트하는 데 ***1***시간 이상 걸릴 수 있습니다**.** 규칙에 애플리케이션을 추가한 후 트래픽 로그를 실행하기 전에 최소 한 시간 이상 기다렸다가 애플리케이션의 로그 정보를 확인합니다**.**
- 새 앱이 없는 요일-(정렬하려면 클릭합니다.) 포트 기반 규칙에서 볼 수 있는 애플리케이션이 안정화되면 규칙이 성숙하고, 변환이 실수로 합법적인 애플리케이션을 배제하지 않으며, 더 이상 새 애플리케이션이 규칙과 일치하지 않을 것이라고 확신할 수 있습니다. 최근에 수정되지 않은 이전 규칙도 더 안정적일 수 있으므로 생성 및 수정된 날짜는 규칙의 안정성을 평가하는 데 도움이 됩니다.
- 적중 횟수 - 선택한 기간 동안 가장 많이 일치하는 규칙을 표시합니다. 적중 카운터를 재설정하고 제외 기간을 일 단위로 지정하는 규칙을 제외할 수 있습니다. 최근에 재설정된 적중 카운터가 있는 규칙을 제외하면 카운터가 재설정되었음을 몰랐기 때문에 예상보다 적은 수의 적중을 표시하는 규칙에 대한 오해를 방지할 수 있습니다.

  또한 ***Hit Count***를 정책 규칙 사용 보기**(**으**)**로 사용하여 사용하지 않는 규칙을 식별하고 제거하여 보안 위험을 줄이고 규칙 기준을 체계적으로 유지할 수 있습니다**.**


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 가장 높은 우선 순위 규칙부터 포트 기반 규칙에 표시된 앱을 검토합니다.

지정된 앱 없음에서 비교 또는 표시된 앱의 숫자를 클릭하여 포트와 일치하는 애플리케이션을 나열하는 애플리케이션 및 사용을 엽니다. 지정된 기간에 대한 기반 규칙, 각 애플리케이션의 위험, 최초 확인 날짜, 마지막 확인 및 지난 30일 동안의 트래픽 양입니다.




지난 7일, 15일 또는 30일 동안 포트 기반 규칙에서 볼 수 있는 애플리케이션을 또는 규칙의 수명 기간 동안 확인할 수 있습니다(상시). 마이그레이션 규칙의 경우 상시 규칙과 일치하는 애플리케이션에 대한 가장 완벽한 평가를 제공합니다.

표시된 앱을검색하고 필터링할 수 있지만 표시된 앱을 업데이트하는 데 1시간 이상이 걸린다는 점을 명심하십시오. 열 헤더를 클릭하여 표시된 앱을 주문할 수도 있습니다. 예를 들어 트래픽**(30일)**을 클릭하여 가장 최근 트래픽이 있는 애플리케이션을 목록 맨 위로 가져오거나 하위 카테고리를 클릭하여 하위 카테고리별로 애플리케이션을 구성할 수 있습니다.

최초 확인 및 최종 확인 데이터에 대한 측정의 세분성은 하루이므로 규칙을 정의하는 날에는 이 두 열의 날짜가 동일합니다. 두 번째 날에 방화벽이 애플리케이션에서 트래픽을 볼 때 날짜의 차이가 표시됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 규칙에서 허용하려는 애플리케이션을 지정하려면 규칙을 복제하거나 애플리케이션을 추가합니다.

애플리케이션 및 사용에서 포트 기반 규칙을 다음 두 가지 방법 중 하나에서 애플리케이션 기반 규칙으로 변환합니다.

- 규칙 복제 - 원래 포트 기반 규칙을 보존하고 복제된 애플리케이션 기반 규칙을 규칙베이스 바로 위에 배치합니다.
- 규칙에 애플리케이션 추가 - 원래 포트 기반 규칙을 새 애플리케이션 기반 규칙으로 대체하고 원래 규칙을 삭제합니다.

  기존 애플리케이션 기반 규칙이 있고 포트 기반 규칙에서 해당 규칙으로 애플리케이션을 마이그레이션하려는 경우 새 규칙을 복제하거나 애플리케이션을 추가하여 포트 기반 규칙을 변환하는 대신 기존 규칙에 애플리케이션 추가을(를) 할 수 있습니다.

일부 애플리케이션은 분기별 또는 연간 이벤트와 같은 인터벌로 네트워크에 나타납니다. 기록이 최신 활동을 캡처할 만큼 길지 않은 경우 이러한 애플리케이션이 애플리케이션 및 사용 화면에 표시되지 않을 수 있습니다.

규칙을 복제하거나 규칙에 애플리케이션을 추가하면 원래 규칙에 대한 다른 내용도 변경되지 않습니다. 규칙에 추가한 애플리케이션을 제외하고 원래 규칙의 구성은 동일하게 유지됩니다. 예를 들어 원래 규칙의 서비스에서 모든 애플리케이션을 허용하거나 특정 서비스를 지정한 경우 서비스를 애플리케이션 기본값으로 변경하여 허용된 애플리케이션을 새 규칙의 기본 포트로 제한해야 합니다.

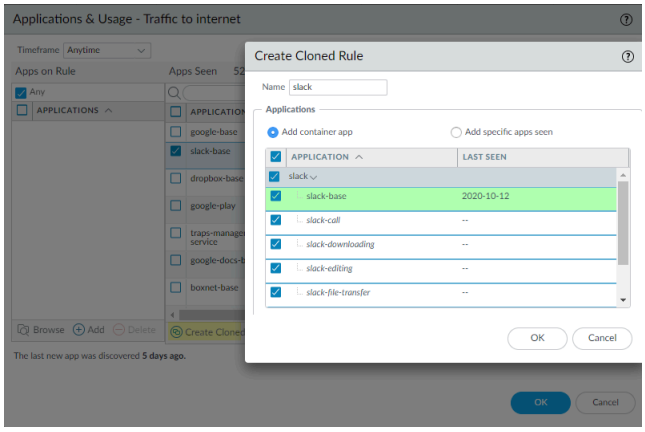
복제는 특히 애플리케이션 및 사용에 규칙과 일치하는 잘 알려진 애플리케이션이 몇 개 이상 표시되는 경우 규칙을 마이그레이션하는 가장 안전한 방법입니다(규칙 복제 마이그레이션 사용 사례: 웹 브라우징 및 SSL 트래픽는 관련 예시임). 복제는 원래 포트 기반 규칙을 보존하고 복제된 애플리케이션 기반 규칙 아래에 배치되므로 복제된 규칙과 일치하지 않는 트래픽이 포트 기반 규칙으로 이동하기 때문에 애플리케이션 가용성을 잃을 위험이 없습니다. 합법적인 애플리케이션의 트래픽이 적절한 기간 동안 포트 기반 규칙에 맞지 않으면 해당 규칙의 마이그레이션을 완료하도록 제거할 수 있습니다.

포트 기반 규칙을 복제하려면 다음을 수행합니다.

1. 표시된 앱에서 복제된 규칙에서 원하는 각 애플리케이션 옆의 체크박스를 클릭합니다. 표시된 앱을 업데이트하는 데 1시간 이상이 걸립니다.
2. 복제된 규칙 생성을 클릭합니다. 복제된 규칙 생성 대화 상자에서 복제된 규칙(이 예제의 "슬랙(slack)")의 이름을 지정하고 필요한 경우 동일한 컨테이너 및 애플리케이션 종속성에 다른 애플리

 ©2023 Palo Alto Networks, Inc.

케이션을 추가합니다. 예를 들어 슬랙 베이스 애플리케이션을 선택하여 규칙을 복제하려면 다음을 수행합니다.




녹색 텍스트는 복제할 선택한 애플리케이션입니다. 컨테이너 애플리케이션(슬랙**(slack)**)은 회색 행에 있습니다. 기울임꼴에 나열된 애플리케이션은 규칙에 표시되지 않았지만 선택한 애플리케이션과 동일한 컨테이너에 있는 애플리케이션입니다. 규칙에 본 개별 애플리케이션은 일반 글꼴에 있습니다. 모든 애플리케이션은 기본적으로 복제된 규칙에 포함됩니다(컨테이너의 모든 애플리케이션을 추가하는 컨테이너 앱 추가가 기본적으로 선택됨).

3. 컨테이너의 모든 애플리케이션을 허용하려면 컨테이너 앱 추가를 선택합니다. 또한 애플리케이션이 컨테이너 앱에 추가되면 규칙이 자동으로 추가되기 때문에 규칙을 "향후 증거"합니다.

   컨테이너의 일부 개별 애플리케이션에 대한 액세스를 제한하려면 사용자가 액세스하지 않으려는 각 개별 애플리케이션 옆의 체크박스를 선택 취소합니다. 컨테이너 앱의 검사도 해제되므로 나중에 컨테이너에 새 애플리케이션을 허용하려면 해당 애플리케이션을 개별적으로 추가해야 합니다.

   컨테이너 앱의 선택을 취소하면 모든 앱의 선택이 없으며 복제된 규칙에 포함하려는 앱을 수동으로 선택합니다.

4. 애플리케이션 종속성이 애플리케이션 아래 상자에 나열되어 있는 경우(이 예제에는 없음) 애플리케이션을 선택합니다. 선택한 애플리케이션은 실행하려면 이러한 애플리케이션 종속성이 필요합니다. 일반적인 종속성에는 **ssl** 및 웹 브라우징이 포함됩니다.
5. 확인을 클릭하여 규칙베이스의 포트 기반 규칙 바로 위에 새 애플리케이션 기반 규칙을 추가합니다.
6. 구성을 커밋합니다.

규칙을 복제하고 구성 커밋을 선택하면 복제된 규칙에 대해 선택한 애플리케이션이 원래 포트 기반 규칙의 표시된 앱 목록에서 제거됩니다. 예를 들어 포트 기반 규칙에 16개의 표시된 앱이 있고 복제된 규칙에 대해 두 개의 개별 애플리케이션과 하나의 종속 애플리케이션을 선택한 경우 복제 후, 포트 기반 규칙은 선택한 세 개의 애플리케이션이 포트 기반 규칙(16-3 = 13)에서 제거되었기 때문에 13개의 표시된 앱을 표시합니다. 복제된 규칙에는 규칙의 앱에 추가된 세 가지 애플리케이션이 표시됩니다.

컨테이너 앱으로 복제된 규칙을 만드는 것은 약간 다르게 작동합니다. 예를 들어 포트 기반 규칙에는 16개의 표시된 앱이 있고 복제된 규칙에 대해 하나의 개별 애플리케이션과 컨테이너 앱을 선택합니다. 컨테이너 앱에는 5개의 개별 애플리케이션이 있으며 하나의 종속 애플리케이션이 있습니다. 복제 후 복제된 규칙은 7개의 규칙 준수 앱**(Apps on Rule)**(개별 애플리케이션, 컨테이너 앱의 5개 개별 애플리케이션, 컨테이너 앱의 종속 애플리케이션)을 표시합니다. 그러나 원래 포트 기반 규칙에서 표시된


©2023 Palo Alto Networks, Inc.

앱은 개별 애플리케이션, 컨테이너 앱 및 컨테이너 앱의 종속 애플리케이션만 포트 기반 규칙에서 제거되므로 13개의 애플리케이션을 표시합니다.

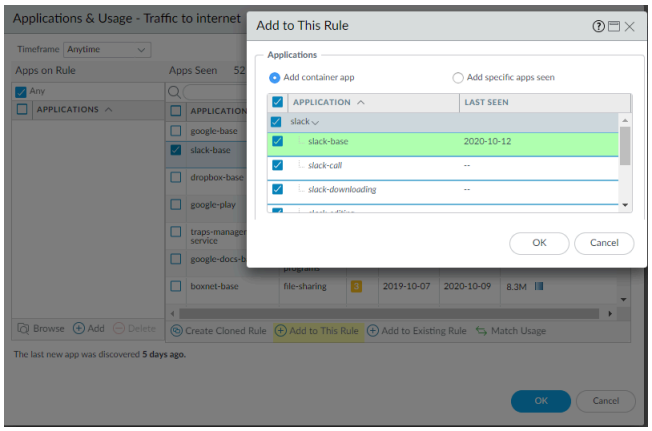
복제와 달리 포트 기반 규칙에 애플리케이션을 추가하면 규칙이 결과 애플리케이션 기반 규칙으로 바뀝다. 규칙에 애플리케이션을 추가하는 것은 복제보다 간단하지만 규칙에 있어야 하는 애플리케이션을 실수로 놓칠 수 있으므로 위험하며 원래 포트 기반 규칙은 더 이상 실수로 누락되지 않습니다. 그러나 잘 알려진 몇 가지 애플리케이션에만 적용되는 포트 기반 규칙에 애플리케이션을 추가하면 규칙이 애플리케이션 기반 규칙으로 빠르게 마이그레이션됩니다. 예를 들어 TCP 포트 22에 대한 트래픽만 제어하는 포트 기반 규칙의 경우 유일한 합법적인 애플리케이션은 SSH이므로 규칙에 애플리케이션을 추가하는 것이 안전합니다.

기존 보안 정책 규칙의 애플리케이션 탭을 사용하여 애플리케이션을 추가해도 앱 표시된 앱 또는 규칙에서 앱이 변경되지 않습니다. 정확한 애플리케이션 사용 정보를 유지하려면 포트 기반 규칙을 애플리케이션 기반 규칙으로 교체할 때 표시된 앱에서 이 규칙에 추가 또는 사용 일치(또는 복제된 규칙을 생성하거나 대신 기존 애플리케이션 기반 규칙에 애플리케이션 추가)를 사용하여 애플리케이션을 추가하십시오.

애플리케이션을 추가하여 포트 기반 규칙을 애플리케이션 기반 규칙으로 대체하는 세 가지 방법이 있습니다(표시된 앱의 이 규칙에 추가 및 사용 일치 및 규칙의 앱에서 추가).

- 표시된 앱(규칙과 일치하는 애플리케이션)에서 이 규칙 애플리케이션에 추가를 합니다. 표시된 앱을 업데이트하는 데 1시간 이상이 걸립니다.

  1. 규칙에 표시된 앱에서 애플리케이션을 선택합니다.
  2. 이 규칙에 추가를 클릭합니다. 이 규칙 추가 대화 상자에서 필요한 경우 동일한 컨테이너 앱 및 애플리케이션 종속성에 다른 애플리케이션을 추가합니다. 예를 들어 규칙에 슬랙 베이스를 추가하려면 다음을 수행합니다.




복제된 규칙 생성 대화 상자와 마찬가지로 이 규칙에 추가되는 녹색 텍스트는 규칙에 추가할 선택한 애플리케이션입니다. 컨테이너앱(슬랙)이 회색 행에 있습니다. 기울임꼴에 나열된 애플리케이션은 규칙에 표시되지 않았지만 선택한 애플리케이션과 동일한 컨테이너에 있는 애플리케이션입니다. 규칙에 본 개별 애플리케이션은 일반 글꼴에 있습니다. 모든 애플리케이션은 기본


©2023 Palo Alto Networks, Inc.

적으로 복제된 규칙에 포함됩니다(컨테이너의 모든 애플리케이션을 추가하는 컨테이너 앱 추가가 기본적으로 선택됨).

3. 컨테이너의 모든 애플리케이션을 허용하려면 컨테이너 앱 추가를 선택합니다. 또한 애플리케이션이 컨테이너 앱에 추가되면 규칙이 자동으로 추가되기 때문에 규칙을 "향후 증거"합니다.

   컨테이너의 일부 개별 애플리케이션에 대한 액세스를 제한하려면 사용자가 액세스하지 않으려는 각 개별 애플리케이션 옆의 체크박스를 선택 취소합니다. 컨테이너 앱의 검사도 해제되므로 나중에 컨테이너에 새 애플리케이션을 허용하려면 해당 애플리케이션을 개별적으로 추가해야 합니다.

   컨테이너 앱의 선택을 취소하면 모든 앱의 선택이 없으며 복제된 규칙에 포함하려는 앱을 수동으로 선택합니다.

4. 애플리케이션 종속성이 애플리케이션 아래 상자에 나열되어 있는 경우(이 예제에는 없음) 애플리케이션을 선택합니다. 선택한 애플리케이션은 실행하려면 이러한 애플리케이션 종속성이 필요합니다.

5. 포트 기반 규칙을 새 애플리케이션 기반 규칙으로 바꾸려면 확인을 클릭합니다.

이 규칙에 추가하고 구성을 커밋하면 새 애플리케이션 기반 규칙이 더 이상 허용하지 않기 때문에 추가하지 않은 애플리케이션이 앱에서 제거됩니다. 예를 들어 규칙에 16개의 표시된 앱이 있고 3개의 애플리케이션을 이 규칙에 추가하는 경우 결과 새 규칙은 표시된 앱에 추가된 3개의 애플리케이션만 표시합니다.

컨테이너 앱으로이 규칙에 추가하면 약간 다르게 작동합니다. 예를 들어 포트 기반 규칙에는 16개의 표시된 앱이 있고 새 규칙에 추가할 하나의 개별 애플리케이션과 컨테이너 앱을 선택합니다. 컨테이너 앱에는 5개의 개별 애플리케이션이 있으며 하나의 종속 애플리케이션이 있습니다. 규칙에 애플리케이션을 추가하면 새 규칙에 7개의 규칙 준수 앱(개별 애플리케이션, 컨테이너 앱의 개별 애플리케이션 5개, 컨테이너 앱의 종속 애플리케이션)이 표시됩니다. 그러나 표시된 앱에는 개별 애플리케이션, 컨테이너 앱 및 컨테이너 앱의 종속 애플리케이션이 해당 목록에서 제거되므로 13개의 애플리케이션이 표시됩니다.

- 한 번의 클릭으로 규칙에 있는 모든 표시된 앱을 한 번에 규칙에 추가합니다(사용 일치).

  포트 기반 규칙은 모든 애플리케이션을 허용하므로 표시된 앱에는 필요하지 않거나 안전하지 않은 애플리케이션이 포함될 수 있습니다. 규칙이 합법적인 비즈니스 목적으로 잘 알려진 소수의 애플리케이션을 확인한 경우에만 규칙을 변환하려면 사용 일치를 사용하십시오. 좋은 예는 *SSH* 트래픽만 허용해야 하는 *TCP* 포트 *22*이므로 *SSH*가 포트 *22*를 여는 포트 기반 규칙에서 볼 수 있는 유일한 애플리케이션인 경우 사용 일치를 할 수 있습니다.

  1. 표시된 앱에서 사용 일치를 클릭합니다. 표시된 앱을 업데이트하는 데 1시간 이상이 걸립니다. 표시된 앱의 모든 애플리케이션은 규칙의 앱에복사됩니다.
  2. 확인을 클릭하여 애플리케이션 기반 규칙을 생성하고 포트 기반 규칙을 바꿉시다.

- 규칙에 적용할 애플리케이션을 알고 있는 경우 규칙 준수 앱에서 수동으로 애플리케이션을 추가할 수 있습니다. 그러나 이 매서드는 기존 보안 정책 규칙 애플리케이션 탭을 사용하는 것과 동일하며 표시된 앱 또는 규칙 준수 앱을 변경하지 않습니다. 정확한 애플리케이션 사용 정보를 유지하려면 표시된 앱에서 이 규칙에 추가, 복제된 규칙 생성 또는 사용 일치를 사용하여 규칙을 변환하십시오.

  1. 규칙의 앱에서 추가(또는 찾아보기)하고 규칙에 추가할 애플리케이션을 선택합니다. 이는 애플리케이션 탭에 애플리케이션을 추가하는 것과 같습니다.

 ©2023 Palo Alto Networks, Inc.

2. 확인을 클릭하여 규칙에 애플리케이션을 추가하고 포트 기반 규칙을 새 애플리케이션 기반 규칙으로 바꿉니다.

   이 매서드는 애플리케이션 탭을 사용하여 애플리케이션을 추가하는 것과 동일하므로 애플리케이션 종속성을 추가하는 대화 상자가 팝업되지 않습니다.

**STEP 5 |** 각 애플리케이션 기반 규칙에 대해 **Service**를 **application-default**로 설정합니다.

업무상 특정 클라이언트와 서버 간의 비표준 포트에서 애플리케이션(예: 내부 사용자 지정 애플리케이션)을 허용해야 하는 경우 필요한 애플리케이션, 소스 및 대상으로만 예외를 제한하십시오. 애플리케이션 기본 포트를 사용할 수 있도록 사용자 지정 애플리케이션을 다시 작성하는 것이 좋습니다.

**STEP 6 |** 구성을 커밋합니다.

**STEP 7 |** 규칙을 모니터링합니다.

- 복제된 규칙 - 원래 포트 기반 규칙을 모니터링하여 애플리케이션 기반 규칙이 원하는 트래픽과 일치하는지 확인합니다. 포트 기반 규칙과 일치하는 애플리케이션을 허용하려는 경우 애플리케이션 기반 규칙에 추가하거나 다른 애플리케이션 기반 규칙을 복제합니다. 네트워크에서 원하지 않는 애플리케이션만 적절한 시간 동안 포트 기반 규칙과 일치하는 경우 복제된 규칙은 강력하고(제어하려는 모든 애플리케이션 트래픽을 포착) 안전하게 제거할 수 있습니다.
- 애플리케이션이 추가된 규칙 - 몇 가지 잘 알려진 애플리케이션이 있는 포트 기반 규칙만 애플리케이션 기반 규칙으로 직접 변환하기 때문에 대부분의 경우 규칙은 처음부터 잘 작동합니다. 변환된 규칙을 모니터링하여 예상 트래픽이 규칙과 일치하는지 확인합니다. 예상보다 트래픽이 적은 경우 규칙에서 필요한 애플리케이션을 모두 허용하지 않을 수 있습니다. 예상보다 많은 트래픽이 있는 경우 이 규칙은 원치 않는 트래픽을 허용할 수 있습니다. 사용자가 비즈니스 목적으로 필요한 애플리케이션에 액세스할 수 없는 경우 규칙(또는 다른 규칙)이 너무 타이트할 수 있습니다.

## 규칙 복제 마이그레이션 사용 사례: 웹 브라우징 및 SSL 트래픽

TCP 포트 80(HTTP 웹 브라우징) 및 443(HTTPS SSL)에서 웹 액세스를 허용하는 포트 기반 규칙은 열려 있는 포트를 사용하는 애플리케이션을 제어할 수 없습니다. 많은 웹 애플리케이션이 있으므로 웹 트래픽을 허용하는 일반적인 규칙은 수천 개의 애플리케이션을 허용하며 그중 상당수는 네트워크에서 원하지 않습니다.

이 사용 사례는 모든 웹 애플리케이션을 원하는 애플리케이션만 허용하는 애플리케이션 기반 정책으로 마이그레이션하는 방법을 보여 주므로 허용하도록 선택한 애플리케이션을 안전하게 활성화할 수 있습니다. 많은 애플리케이션을 볼 수 있는 규칙의 경우 추가가 포트 기반 규칙을 대체하므로 원래 포트 기반 규칙을 복제하는 것이 규칙에 애플리케이션을 추가하는 것보다 안전하므로 실수로 중요한 애플리케이션을 추가하는 것을 잊어버리면 애플리케이션 가용성에 영향을 줍니다. 또한 포트 기반 규칙을 대체하는 **Match Usage**를 사용하면 규칙이 확인한 모든 애플리케이션을 허용하게 되며 이는 특히 웹 검색 트래픽에서 위험할 수 있습니다.

규칙을 복사하면 원래 포트 기반 규칙을 유지하고 복사된 규칙이 규칙베이스의 포트 기반 규칙 바로 위에 배치되므로 규칙을 모니터링할 수 있습니다. 또한 복사를 사용하면 포트 기반 웹 트래픽 규칙과 같은 다양한 애플리케이션이 표시되는 규칙을 여러 애플리케이션 기반 규칙으로 분할하여 다양한 애플리케이션 그룹을 다르게 처리할 수 있습니다. 복사된 규칙(또는 규칙)에서 허용하는 데 필요한 모든 애플리케이션을 허용한다고 확신하는 경우 포트 기반 규칙을 제거할 수 있습니다.


©2023 Palo Alto Networks, Inc.

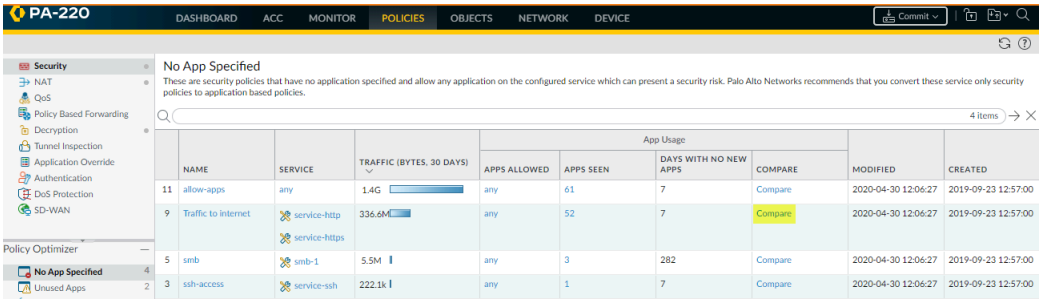
이 예에서는 포트 기반 웹 트래픽 규칙을 복제하여 웹 기반 파일 공유 트래픽(포트 기반 규칙에 표시되는 애플리케이션 트래픽의 하위 집합)에 대한 애플리케이션 기반 규칙을 생성합니다.

이 예제는 새 앱 뷰어를 사용하여 ***ACE(***앱 ***ID*** 클라우드 엔진***)*** 애플리케이션을 복사하는 데 적용되지 않습니다***(***이 작업을 수행하는 방법에 대한 예시는 ACE 설명서 참조***). ACE***에는 SaaS 보안 인라인 라이선스가 필요합니다**.**

**STEP 1 |** 포트 기반 규칙을 보려면 정책 > 보안 > 정책 최적화도구 > 지정된 앱 없음으로 이동합니다.

**STEP 2 |** 마이그레이션할 규칙에 대해 비교를 클릭합니다.

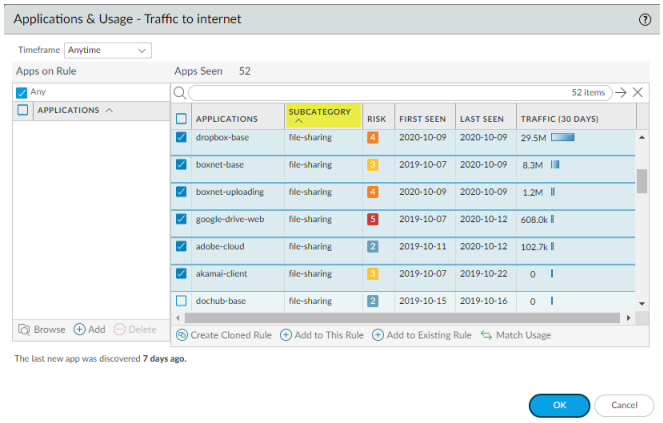
이 예에서 웹 액세스를 허용하는 포트 기반 규칙의 이름은 인터넷 트래픽입니다.




**STEP 3 |** 정렬 옵션을 사용하여 표시된 앱에서 허용할 애플리케이션을 검토하고 선택합니다.

표시된 앱의 수는 약 ***1***시간마다 업데이트되므로 예상보다 많은 애플리케이션이 표시되지 않으면 약 ***1***시간 후에 다시 확인하십시오**.** 방화벽의 부하에 따라 이러한 필드가 업데이트되는 데 ***1***시간 이상 걸릴 수 있습니다**.**

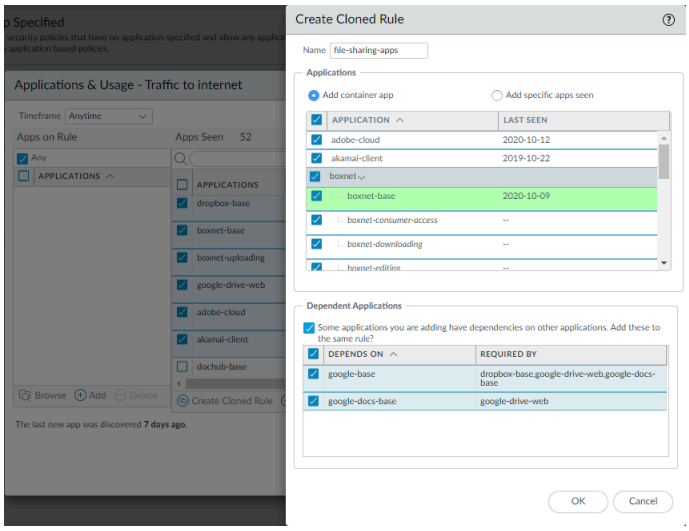
예를 들어 하위 카테고리를 클릭하여 애플리케이션을 정렬하고 파일 공유 하위 카테고리로 스크롤한 다음 허용하려는 애플리케이션을 선택합니다. 또는 파일 공유 애플리케이션에 대한 필터링(검색)을 수행할 수 있습니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 복제된 규칙 만들기를 클릭하고 복제된 규칙(이 예에서는 파일 공유 앱)을 이름으로 지정합니다.

복제된 규칙 만들기는 선택한 애플리케이션을 녹색으로 음영 처리하고 컨테이너 앱은 회색으로 음영 처리하며 컨테이너의 개별 애플리케이션은 이탤릭체로 표시되며 규칙에 일반 텍스트 글꼴로 표시됩니다. 애플리케이션을 스크롤하는 것은 모든 컨테이너 앱과 개별 애플리케이션을 보여줍니다.




복사된 규칙 생성에는 선택한 애플리케이션에 대한 종속 애플리케이션도 표시됩니다. 이 예에서 선택한 애플리케이션 중 일부를 실행하려면 google-base 및 google-docs-base 애플리케이션이 필요합니다(필수).

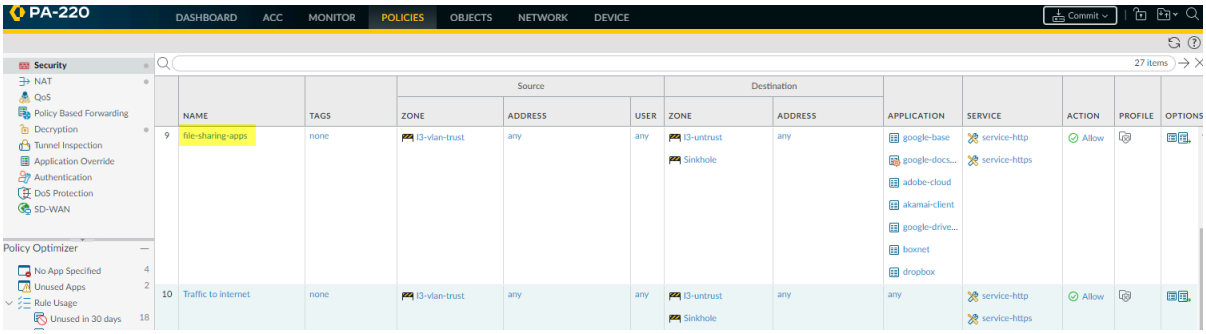
**STEP 5 |** 복사된 규칙에서 원하는 애플리케이션을 선택합니다.

포함하지 않으려는 애플리케이션의 경우 컨테이너 앱의 선택을 해제하는 해당 상자의 선택을 취소합니다. 컨테이너 앱을 포함하지 않으면 새 앱이 컨테이너에 추가될 때 규칙에 자동으로 추가되지 않습니다.

컨테이너 앱의 선택을 취소하면 컨테이너의 모든 개별 애플리케이션의 선택이 없으며 수동으로 추가할 앱을 선택해야 합니다.

**STEP 6 |** 확인을 클릭하여 복사된 규칙을 생성합니다.

**STEP 7 |** 정책 > 보안에서 복제된 규칙(file-sharing-apps)이 원래 포트 기반 규칙 위에 있는 규칙 베이스(인터넷 트래픽)에 삽입됩니다.




**STEP 8 |** 규칙 이름을 클릭하여 원래 포트 기반 규칙의 속성을 상속하는 복사된 규칙을 편집합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** 서비스**/URL** 카테고리 탭의 서비스에서 service-http 및 service-https를 삭제합니다.

이렇게 하면 서비스가 **application-default**로 변경되어 애플리케이션이 비표준 포트를 사용하는 것을 방지하고 공격 표면을 더욱 줄일 수 있습니다.

업무상 특정 클라이언트와 서버 간의 비표준 포트에서 애플리케이션**(**예**:** 내부 사용자 지정 애플리케이션**)**을 허용해야 하는 경우 필요한 애플리케이션**,** 소스 및 대상으로만 예외를 제한하십시오**.** 애플리케이션 기본 포트를 사용할 수 있도록 사용자 지정 애플리케이션을 다시 작성하는 것이 좋습니다**.**

**STEP 10 |** 소스, 사용자 및 대상 탭에서 올바른 위치(영역, 서브넷)의 올바른 사용자에게만 적용되도록 규칙을 강화합니다.

예를 들어, 웹에서 파일을 공유해야 하는 비즈니스상의 이유가 있는 사용자 그룹으로만 웹 파일 공유 활동을 제한할 수 있습니다.

**STEP 11 |** 확인을 클릭합니다.

**STEP 12 |** 구성을 커밋합니다.

**STEP 13 |** 애플리케이션 기반 규칙만 네트워크에서 허용하려는 애플리케이션만 허용할 때까지 포트 기반 웹 액세스 규칙의 다른 애플리케이션 카테고리에 대한 프로세스를 반복합니다.

허용하려는 트래픽이 포트 기반 규칙이 더 이상 필요하지 않다고 확신할 수 있을 만큼 충분한 시간 동안 원래 포트 기반 규칙에 도달하지 않으면 규칙 베이스에서 포트 기반 규칙을 제거할 수 있습니다.

## 기존 규칙에 애플리케이션 추가

어떤 경우에는 이미 존재하는 규칙에 포트 기반 규칙에서 학습된(표시된) 애플리케이션을 추가할 수 있습니다. 예를 들어, 관리자는 인터넷 액세스를 허용하는 포트 기반 규칙(포트 80/443 규칙)에서 일반 비즈니스 웹 애플리케이션에 대한 복제된 애플리케이션 기반 규칙을 생성할 수 있습니다. 관리자는 추후에 포트 기반 인터넷 액세스 규칙이 보다 일반적인 비즈니스 애플리케이션을 확인하여 일부 또는 전체를 복제된 애플리케이션 기반 규칙에 추가하려고 한다는 것을 알게 됩니다(동일한 유형의 애플리케이션에 대해 다른 애플리케이션 기반 규칙을 복제하면 불필요한 규칙과 규칙 기반을 복잡하게 함).

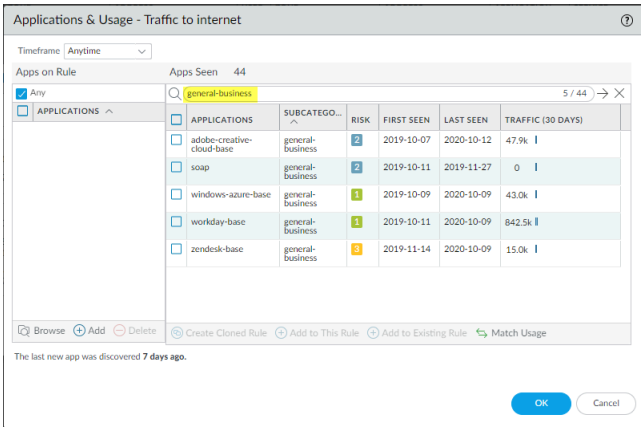
이 예에서는 일반 비즈니스 트래픽을 제어하는 애플리케이션 기반 보안 정책 규칙이 이미 존재하거나 규칙 복제 마이그레이션 사용 사례: 웹 브라우징 및 SSL 트래픽과(와) 유사하게 포트 기반 인터넷 액세스 규칙에서 복제되었다고 가정합니다. 이 예에서는 포트 기반 인터넷 액세스 규칙에서 애플리케이션 기반 규칙을 복제하고 웹 기반 애플리케이션에서 비표준 포트를 사용하지 못하도록 새 규칙의 서비스를 애플리케이션 기본값으로 변경했습니다.

기존 애플리케이션 기반 규칙에 애플리케이션을 추가하는 것 외에도 기존 포트 기반 규칙에 애플리케이션을 추가할 수 있습니다**.** 이렇게 하면 규칙에 추가하는 애플리케이션에 대해 포트 기반 규칙이 애플리케이션 기반 규칙으로 변환됩니다**.** 이렇게 하면 규칙으로 이동하여 서비스를 애플리케이션-디폴트값으로 변경하여 애플리케이션이 비표준 포트를 사용하지 못하도록 합니다**(**또한 규칙에 구성된 서비스가 애플리케이션과 일치하지 않을 수 있음**).**

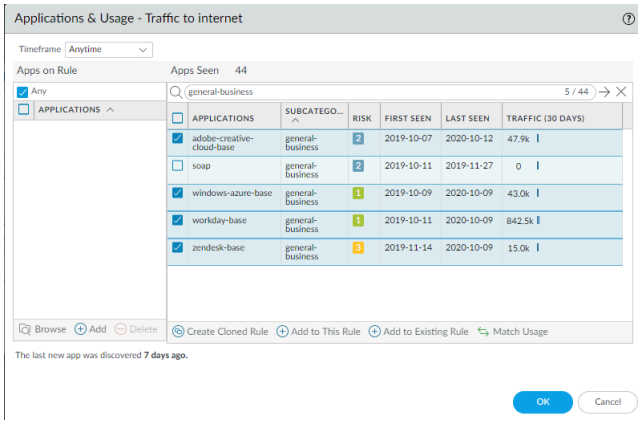
이 예는 신규 앱 뷰어를 사용하여 기존 규칙에 ***ACE(App-ID Cloud Engine)*** 애플리케이션을 추가하는 데 적용되지 않습니다**(**이를 수행하는 방법에 대한 예는 ACE 설명서 참조**).** ***ACE***에는 SaaS 보안 인라인 라이선스가 필요합니다**.**

 ©2023 Palo Alto Networks, Inc.

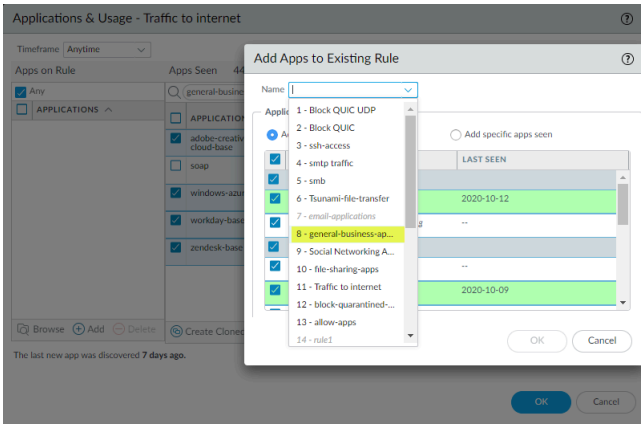
**STEP 1 |** 포트 기반 인터넷 액세스 규칙을 확인하고 규칙이 일반 비즈니스 애플리케이션을 확인했으며 일부 애플리케이션을 비즈니스 목적으로 허용해야 함을 발견했습니다.




**STEP 2 |** 기존 규칙에 추가할 일반 비즈니스 앱을 선택합니다.




**STEP 3 |** 기존 규칙에 추가를 클릭하고 애플리케이션을 추가할 규칙의 이름(이 예에서는 일반 비즈니스 애플리케이션)을 선택합니다. 이 예에서는 **general-business-applications**입니다.

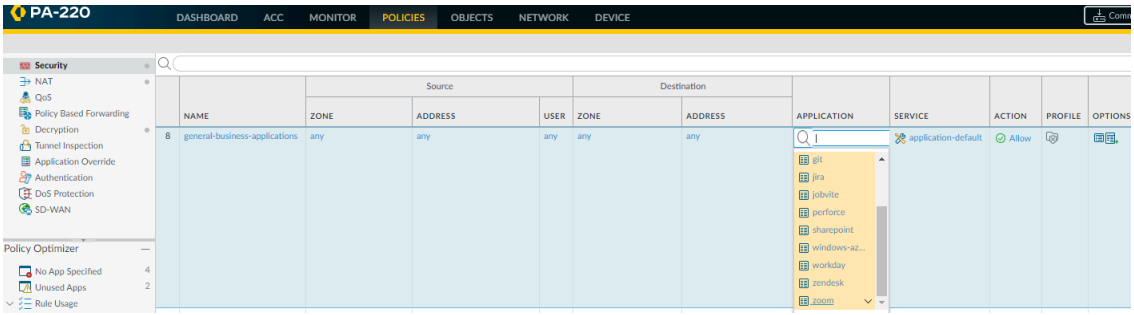



**STEP 4 |** 기존 규칙에 앱 추가에서 확인을 클릭하여 선택한 애플리케이션을 **general-business-applications** 규칙에 추가합니다.

**STEP 5 |** 애플리케이션 및 사용에서 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 업데이트된 규칙은 이제 규칙의 원래 애플리케이션과 방금 추가한 애플리케이션을 제어합니다.




# 사용되지 않는 애플리케이션을 사용하여 보안 정책 규칙 식별

많은 수의 애플리케이션을 허용하는 애플리케이션 기반 보안 정책 규칙이 있는 경우 사용하지 않는 애플리케이션(규칙에 표시되지 않는 애플리케이션)을 제거하여 규칙과 일치하는 트래픽에서 실제로 표시되는 애플리케이션만 허용하도록 규칙을 강화할 수 있습니다. 보안 정책 규칙에서 사용하지 않는 애플리케이션을 식별하고 제거하는 것은 공격 면적을 줄여 보안 태세를 강화하는 모범 사례입니다.

**STEP 1 |** 사용하지 않는 애플리케이션이 있는 보안 정책 규칙을 식별합니다.

**Policies** > **Security** > **Policy Optimizer** > **Unused Apps**는 규칙과 일치하지 않는 애플리케이션으로 구성된 모든 애플리케이션 기반 규칙을 표시합니다. 이는 이러한 규칙이 네트워크에서 사용할 수 없는 애플리케이션을 허용한다는 것을 의미합니다(또는 다른 규칙이 해당 규칙을 섀도잉하여 규칙과 일치할 것으로 예상되는 트래픽이 규칙 베이스의 이전 규칙과 일치함).

허용된 앱 및 표시된 앱의 수는 약 *1*시간마다 업데이트되므로 규칙에 따라 애플리케이션을 구성하고 허용된 앱이 예상만큼 많지 않은 경우 약 *1*시간 후에 다시 확인하십시오. 방화벽의 부하에 따라 이러한 필드가 업데이트되는 데 *1*시간 이상 걸릴 수 있습니다.

**STEP 2 |** 사용하지 않는 애플리케이션이 있는 규칙 중 먼저 수정할 규칙의 우선 순위를 지정합니다.

**Policies** > **Security** > **Policy Optimizer** > **Unused Apps**를 사용하면 규칙 베이스의 순서에 영향을 주지 않고 규칙을 정렬할 수 있으며 비즈니스 목표와 위험 허용 범위에 따라 정리할 규칙의 우선 순위를 정하는 데 도움이 되는 기타 정보를 제공합니다.

- 허용된 앱(허용 목록에 있는 애플리케이션의 수)과 표시된 앱(규칙에 실제로 표시되는 허용된 애플리케이션의 수)의 차이는 각각에 구성된 애플리케이션의 수를 보여주지만, 규칙이 과도하게 프로비저닝된 정도를 나타내는 규칙에 실제로 표시되지 않습니다. 규칙에서 허용된 애플리케이션 수를 기준으로 정렬하려면 허용된 앱을 클릭하고 규칙에 실제로 표시되는 애플리케이션 수를 기준으로 정렬하려면 표시된 앱을 클릭합니다.
- 신규 앱이 없는 날짜(정렬하려면 클릭)는 새 애플리케이션이 규칙에 마지막으로 적용한 이후의 일수를 보여줍니다. 이는 규칙이 완성되어 아직 확인되지 않은 애플리케이션을 볼 수 없을 가능성을 나타냅니다. 신규 앱이 없는 기간이 길수록 새 애플리케이션이 규칙에 도달할 가능성이 줄어들고 규칙이 허용하는 모든 애플리케이션을 알게 될 가능성이 높아집니다.
- 생성 및 수정 날짜는 또한 규칙에 표시되지 않은 애플리케이션이 나중에 표시될 수 있는지 또는 규칙에 적중할 것으로 예상되는 모든 애플리케이션이 규칙에 표시되는지 이해할 수 있을 정도로 규칙이 완성되었는지의 여부를 결정하는 데 도움이 됩니다. 규칙이 수정된 이후 시간이 길수록 규칙이 완성될 가능성이 높아집니다. (**Created**와 **Modified**가 같으면 규칙이 수정되지 않은 것입니다.)

 ©2023 Palo Alto Networks, Inc.

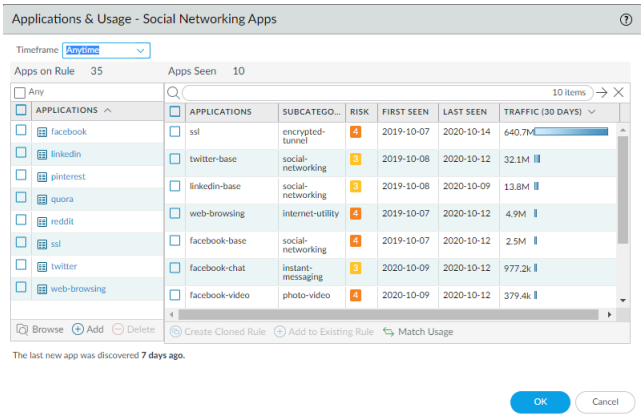
- 적중 횟수 - 선택한 기간 동안 가장 많이 일치하는 규칙을 표시합니다. 적중 카운터를 재설정하고 제외 기간을 일 단위로 지정하는 규칙을 제외할 수 있습니다. 최근에 재설정된 적중 카운터가 있는 규칙을 제외하면 카운터가 재설정되었음을 몰랐기 때문에 예상보다 적은 수의 적중을 표시하는 규칙에 대한 오해를 방지할 수 있습니다.

  또한 적중 횟수를 정책 규칙 사용 보기까지 사용할 수 있습니다.

트래픽**(Bytes, 30일)**을 클릭하여 지난 30일 동안 규칙에서 확인한 트래픽 양을 기준으로 정렬할 수도 있습니다. 이 정보를 사용하여 먼저 수정할 규칙의 우선 순위를 지정하십시오. 예를 들어 허용된 앱과 표시된 앱 간의 차이가 가장 크고 신규 앱이 없는 일수가 가장 많은 규칙의 우선 순위를 지정할 수 있습니다. 이러한 규칙에는 사용되지 않는 애플리케이션 수가 가장 많고 가장 완성도가 높기 때문입니다.

**STEP 3 |** 규칙에서 표시되는 앱을 검토합니다.

사용하지 않는 앱에서 비교 또는 본 앱 열의 숫자를 클릭하여 규칙에 구성된 애플리케이션(규칙의 앱)과 규칙에 표시된 앱을 표시하는 애플리케이션 및 사용을 엽니다.

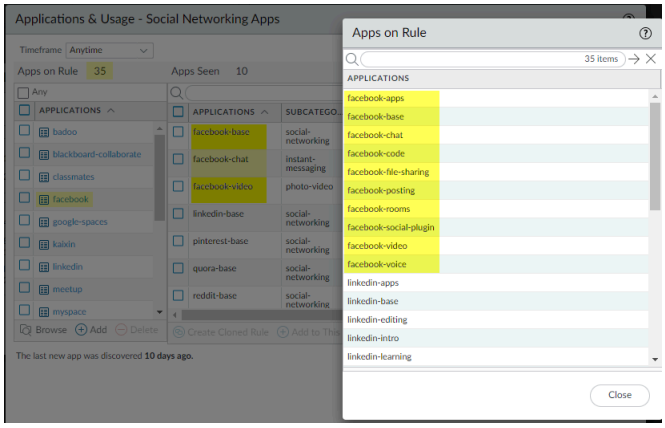



- 본 앱 옆에 있는 숫자(이 예에서는 10)는 규칙과 일치하는 애플리케이션의 수입니다. 방화벽이 표시된 앱을 업데이트하는 데 최소 1시간이 걸립니다.
- 규칙의 앱 옆에 있는 숫자(이 예에서는 35개)는 규칙에 구성된 애플리케이션의 수로 컨테이너 앱의 각 애플리케이션을 계산하여 산정됩니다(컨테이너 앱 자체는 제외). 규칙에 컨테이너 앱을 구성하는 경우 규칙은 컨테이너 앱의 개별 애플리케이션을 허용합니다. 애플리케이션 목록에는 규칙에서 수동으로 구성한 애플리케이션만 표시되기 때문에 규칙에서 컨테이너 앱을 구성할 때 애플리케이션은 컨테이너 앱만 표시하고 컨테이너의 모든 개별 애플리케이션은 표시하지 않습니다(개별 애플리케이션도 수동으로 구성하지 않는 한 규칙에 따름). 이러한 이유로 규칙에 있는 앱의 수는 애플리케이션 목록에 표시되는 애플리케이션의 수와 동일하지 않을 수 있습니다.
- 규칙의 앱 옆에 있는 숫자를 클릭하면 규칙의 모든 개별 애플리케이션을 볼 수 있습니다.

  이 예제 규칙에는 10개의 앱이 표시되지만(규칙과 일치하는 애플리케이션) 규칙에 따라 **35**개의 앱이 허용됩니다. **facebook** 컨테이너 앱은 규칙에 구성되고 규칙은 개별 애플리케이션 facebook-base, facebook-chat 및 facebook-video(**Apps Seen**)의 트래픽을 확인합니다. **Apps on Rule** 번호


©2023 Palo Alto Networks, Inc.

를 클릭하면 **Apps on Rule** 대화 상자에 허용된 개별 애플리케이션이 표시되지만 컨테이너 앱 자체는 표시되지 않습니다.




팝업 대화 상자에서 애플리케이션을 추가하거나 삭제할 수 없습니다.

규칙에 표시된 앱과 규칙에 있는 앱을 비교합니다. 규칙의 애플리케이션이 사용되지 않는 경우(애플리케이션이 표시되지 않거나 **Apps Seen**에서 허용된 컨테이너에 애플리케이션이 표시되지 않음) 공격 면적을 줄이기 위해 규칙에서 애플리케이션을 제거하는 것이 좋습니다. 분기별 또는 연간 이벤트와 같이 주기적으로 사용되는 애플리케이션을 고려하십시오. 이 애플리케이션은 충분한 기간 동안 조사하지 않으면 사용되지 않는 것처럼 보일 수 있습니다. 기간을 사용하면 규칙에 표시된 앱의 기간을 선택할 수 있습니다. 규칙 기간 동안 표시되는 모든 애플리케이션을 보려면 **Anytime**(항상)을 선택합니다. **No App Specified** 대화 상자의 생성 또는 수정 날짜와 주기적인 이벤트 사이의 시간에 따라 규칙이 주기적으로 사용되는 모든 애플리케이션을 볼 수 있을 만큼 충분히 오랫동안 방화벽에 있지 않았을 수 있습니다.

**STEP 4 |** 규칙에서 사용하지 않는 애플리케이션을 제거합니다.

규칙에 따라 앱에서 애플리케이션을 삭제(또는 추가)하여 애플리케이션을 수동으로 제거(또는 추가)하거나 사용량 일치를 사용하여 규칙에 표시된 앱을 추가하고 규칙에서 일치하는 트래픽이 확인되지 않은 애플리케이션을 클릭 한 번으로 삭제합니다.

규칙에서 애플리케이션을 수동으로 제거하려면 규칙의 앱에서 애플리케이션을 선택한 다음 삭제합니다. 규칙에서 애플리케이션을 제거하기 전에 주기적 이벤트에 필요한 애플리케이션이 없는지 확인하십시오. (보안 정책 규칙의 애플리케이션 탭에서 애플리케이션을 추가하거나 삭제할 수도 있습니다.)

사용 일치는 규칙에 표시된 앱을 규칙의 앱으로 이동하고 규칙에서 사용하지 않는 모든 애플리케이션을 제거합니다.

정책 > 보안 및 지정된 앱 없음에서 포트 기반을 앱 ID 기반 보안 정책 규칙으로 마이그레이션로 규칙을 복제할 수 있습니다. 사용하지 않는 앱에서 시작하는 규칙은 복제할 수 없습니다.

**STEP 5 |** 구성을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 업데이트된 규칙을 모니터링하고 사용자 피드백을 받고 업데이트된 규칙이 허용하려는 애플리케이션을 허용하고 주기적으로 사용되는 애플리케이션을 실수로 차단하지 않도록 합니다.

> 허용된 앱 및 본 앱의 수는 약 *1*시간마다 업데이트됩니다. 규칙에서 사용하지 않는 애플리케이션을 모두 제거한 후에는 방화벽이 디스플레이를 업데이트할 때까지 규칙이 ***Policies > Security > Policy Optimzer > Unused Apps***에 나열된 상태로 유지됩니다. 방화벽이 디스플레이를 업데이트하고 허용된 앱 수가 본 앱의 수와 같으면 사용하지 않는 앱 화면에 규칙이 더 이상 표시되지 않습니다. 그러나 방화벽의 부하에 따라 이러한 필드가 업데이트되는 데 *1*시간 이상 걸릴 수 있습니다.

## 애플리케이션 사용 통계에 대한 고가용성

두 개의 방화벽을 고가용성(HA) 쌍으로 구성하는 경우 애플리케이션 사용 통계는 애플리케이션에 대한 트래픽 로그를 생성하는 방화벽에 대해 로컬입니다. 애플리케이션 사용 통계를 볼 수 있는 위치는 부분적으로 HA 구성에 따라 다릅니다.

- 능동형/수동형 - 능동형 디바이스는 애플리케이션 사용 통계를 생성합니다. 수동형 디바이스에 사용자 트래픽이 없는 경우 활성 디바이스만 애플리케이션 사용 통계를 표시합니다. 수동형 디바이스가 트래픽을 본 경우 수동형 디바이스는 본 트래픽의 애플리케이션 사용 통계만 표시합니다.

  페일오버에서 애플리케이션 사용 통계는 새로 활성화된 디바이스(페일오버 이전에 수동형이었던 디바이스)에서 생성된 트래픽 로그만을 기반으로 합니다.
- 능동형/능동형 - 세션을 소유한 디바이스는 해당 세션에 대한 트래픽 로그를 생성하므로 세션에 대한 애플리케이션 사용 통계는 세션을 소유한 디바이스에서만 사용할 수 있습니다. 하나의 능동형 디바이스가 세션을 소유하는 경우 다른 능동형 디바이스는 해당 세션의 애플리케이션 사용 통계를 표시하지 않습니다.

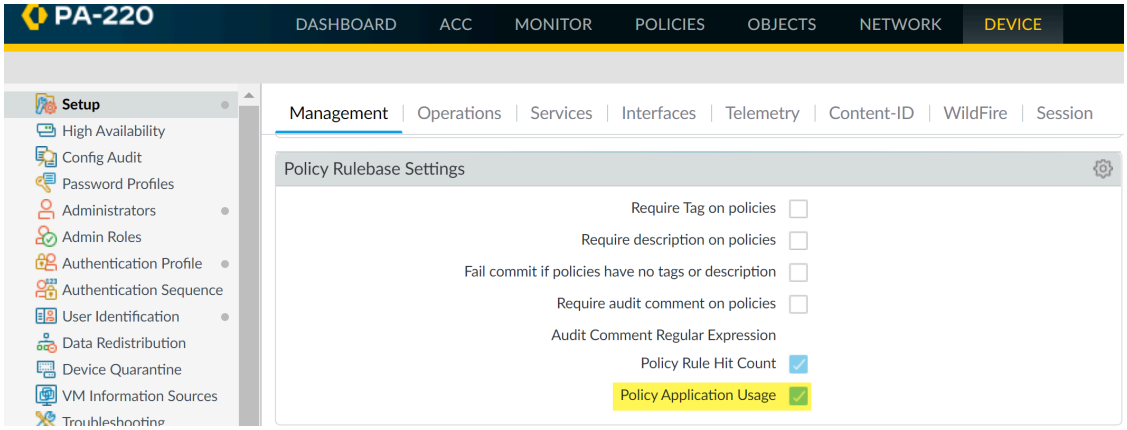
## 정책 최적화 프로그램을 비활성화하는 방법

Policy Optimizer는 기본적으로 활성화되어 있습니다. Policy Optimizer는 포트 기반을 앱 ID 기반 보안 정책 규칙으로 마이그레이션 및 사용되지 않는 애플리케이션을 사용하여 보안 정책 규칙 식별을(를) 쉽게 만드는 많은 기능을 제공하고, 규칙에서 사용하지 않는 애플리케이션을 제거하지만 기능을 비활성화하려면 할 수 있습니다.

**STEP 1 |** 디바이스 > 설정 > 관리 > 정책 규칙 베이스 설정으로 이동합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 정책 애플리케이션 사용 체크박스를 선택하여 기능을 활성화하고 체크박스를 선택 취소하여 기능을 비활성화합니다.




 ©2023 Palo Alto Networks, Inc.

# App-ID 클라우드 엔진

App-ID Cloud Engine(ACE)은 방화벽 또는 Panorama가 Palo Alto Networks 콘텐츠 팀의 사전 정의된 특정 App-ID가 없는 애플리케이션에 대해 클라우드에서 App-ID를 다운로드할 수 있도록 하는 신규 서비스입니다. 이들은 방화벽이 SSL, 웹 브라우징, unknown-tcp 또는 unknown-udp 트래픽으로 식별하는 애플리케이션입니다. 보안 정책 규칙에서 ACE App-ID를 사용하여 해당 애플리케이션에 대한 가시성을 확보하고 제어하고 정책 최적화 프로그램을 사용하여 보안 정책에서 애플리케이션을 추가 및 관리합니다. 다른 유형의 정책 규칙에서는 ACE App-ID를 사용할 수 없습니다. ACE:

- 애플리케이션을 식별하고 제어하기 위해 알려진 App-ID의 수를 크게 늘립니다. ACE가 애플리케이션에 대한 신규 App-ID를 정의하면 방화벽에서 사용할 수 있게 됩니다.
- 방화벽에 대한 신규 App-ID의 가용성 및 포워딩 속도를 높입니다.
- 보안 정책 규칙에서 애플리케이션 필터를 사용하여 보안 정책에 애플리케이션 추가 속도를 높이고 자동화할 수 있습니다.
- 이전에 ssl, 웹 브라우징, unknown-tcp 또는 unknown-udp로 식별된 애플리케이션에 대한 가시성을 크게 높입니다.

*ACE*에는 SaaS 보안 인라인 구독이 필요합니다. *ACE*를 사용하는 각 어플라이언스에는 유효한 디바이스 인증서가 설치되어 있어야 합니다.

*PAN-OS 10.1* 이상을 지원하는 모든 하드웨어 플랫폼은 *ACE*를 지원하고 *ACE*를 사용하려는 모든 어플라이언스에는 *PAN-OS 10.2* 이상이 필요합니다. *Panorama*는 *SaaS Security Inline* 라이선스가 설치되지 않은 방화벽이나 *10.1* 이전 버전의 *PAN-OS*를 실행하는 방화벽에 *ACE* 기반 정책 또는 개체를 푸시하고 커밋할 수 없습니다.

*ACE*는 미국, *APAC* 및 *EU GCP* 지역에서 지원됩니다. 지역은 *CDL* 지역에 따라 자동으로 선택됩니다.

방화벽이 해당 지역에 대해 올바른 콘텐츠 클라우드 *FQDN*(디바이스 > 설정 > ***Content-ID*** > 콘텐츠 클라우드 설정)을 사용하는지 확인하고 필요한 경우 *FQDN*을 변경합니다.

- 미국 - ***hawkeye.services-edge.paloaltonetworks.com***
- *EU* - ***eu.hawkeye.services-edge.paloaltonetworks.com***
- *APAC* - ***apac.hawkeye.services-edge.paloaltonetworks.com***

트래픽 페이로드를 포함한 *ACE* 데이터는 선택한 지역의 서버로 전송됩니다. 해당 지역 외부에 있는 *Content Cloud FQDN*을 지정하는 경우(예: *EU* 지역에 있지만 *APAC* 지역 *FQDN*을 지정하는 경우) 해당 국가 또는 조직의 개인정보 보호 및 법적 규정을 위반할 수 있습니다.


©2023 Palo Alto Networks, Inc.

사전 정의된 콘텐츠 제공 App-ID는 한 달에 한 번 새 애플리케이션을 제공하며 보안 정책 규칙에 대한 변경 사항을 이해하기 위해 신규 App-ID를 설치하기 전에 분석해야 합니다. 월별 주기와 분석 필요성으로 인해 정책에 신규 App-ID가 채택되는 속도가 느려집니다. Palo Alto Networks는 사용자가 검토해야 하는 월별 콘텐츠 업데이트를 통해 신규 App-ID를 계속 제공할 것이지만 ACE는 처음에 다음 네 가지 유형 중 하나로 식별된 애플리케이션에 주문형 App-ID를 제공하여 신규 App-ID의 채택을 개선합니다.

- **ssl** - 암호화된 SSL 트래픽은 가장 일반적인 유형의 네트워크 트래픽이며, 대부분의 전문가는 전체 트래픽의 90%를 초과한다고 주장합니다. 해당 트래픽을 해독하지 않거나 해독할 수 없는 경우 방화벽은 종종 이를 실제 기본 애플리케이션이 아닌 SSL로만 식별할 수 있습니다.
- 웹 브라우징 - 애플리케이션이 너무 많아 콘텐츠 제공 App-ID가 계속 증가하는 양을 따라잡을 수 없기 때문에, 방화벽은 암호화되지 않은 웹 브라우징 트래픽을 구체적으로 식별할 수 없습니다.
- **unknown-tcp** 및 **unknown-udp** - 이 트래픽은 내부 또는 사용자 지정 애플리케이션이거나 알 수 없는 외부 애플리케이션일 수 있습니다. 지능적인 액세스 결정을 내리고 트래픽을 제어 및 검사하기 위한 적절한 보안 정책 규칙을 구성할 수 있도록 특정 App-ID로 해당 트래픽을 식별하는 것이 중요합니다.

ACE는 이러한 애플리케이션에 대한 특정 식별 정보를 제공하므로 사용자가 해당 애플리케이션을 이해하고 정책에서 적절하게 제어할 수 있습니다.

*ACE App-ID*는 다른 유형의 공용 애플리케이션을 식별하지 않으며 개인 및 사용자 지정 애플리케이션을 식별하지 않습니다. *ACE App-ID* 카탈로그에는 사전 정의된 콘텐츠 제공 *App-ID*가 포함되어 있지 않습니다. 콘텐츠가 포함된 *App-ID*는 매월 지속적으로 콘텐츠 업데이트를 제공합니다.

방화벽이 ssl, 웹 브라우징, unknown-tcp 또는 unknown-udp 트래픽을 만나면 방화벽은 분석을 위해 페이로드를 ACE로 보냅니다. ACE 데이터베이스에 일치하는 App-ID가 있는 경우 ACE는 App-ID를 요청하는 방화벽에 반환합니다. ACE에 트래픽에 대해 일치하는 App-ID가 없는 경우 ACE는 페이로드를 기계 학습(ML) 엔진으로 보냅니다. ML 엔진은 페이로드를 분석하고 휴먼 콘텐츠 팀과 함께 신규 App-ID를 개발하고 애플리케이션과 관련이 없는 트래픽을 삭제합니다. 개발이 완료되면 ML 엔진은 신규 App-ID를 ACE 데이터베이스에 업로드하고 요청하는 방화벽(및 기타 방화벽)은 App-ID를 다운로드하여 보안 정책에서 사용할 수 있습니다.

*App-ID*가 있는 *ACE*에서 애플리케이션을 검색하는 데 몇 분이 걸리고 신규 *App-ID*를 개발해야 하는 경우 더 오래 걸릴 수 있으므로 클라우드 애플리케이션 감지는 방화벽에서 인라인되지 않습니다. 방화벽은 애플리케이션 트래픽을 처리하기 위한 판정을 기다리지 않습니다. 방화벽은 *ACE*에서 *App-ID*를 받을 때까지 트래픽을 *ssl*, *web-browsing*, *unknown-tcp* 또는 *unknown-udp*로 처리한 다음 사용자가 새 *App-ID*를 받고 보안 정책에서 사용할 때까지 이러한 방식으로 트래픽을 계속 처리합니다.

*ACE*가 활성화되고 *ACE* 클라우드 *App-ID*가 보안 정책 규칙 또는 애플리케이션 그룹에서 여전히 사용 중인 후 방화벽 또는 *Panorama*를 다운그레이드하면 해당 절차가 실패합니다. 실패 이유는 다운그레이드하기 위해 구성에서 제거해야 하는 개체를 나열합니다. 구성에서 해당 개체를 제거하고 구성을 커밋하면 다운그레이드가 성공합니다.

- 앱 ID 클라우드 엔진 배포 준비
- 앱 ID 클라우드 엔진 사용 또는 비활성화
- App-ID 클라우드 엔진 처리 및 사용


©2023 Palo Alto Networks, Inc.

- 신규 앱 뷰어(정책 최적화 프로그램)
- 정책 최적화 프로그램을 사용하여 애플리케이션 필터에 앱 추가
- 정책 최적화 프로그램을 사용하여 애플리케이션에 앱 추가
- 정책 최적화 프로그램을 사용하여 규칙에 직접 앱 추가
- RMA 방화벽(ACE) 교체
- 라이선스 만료 또는 비활성화 ACE의 영향
- 클라우드 콘텐츠 롤백으로 인한 커밋 실패
- App-ID Cloud Engine 문제 해결

## 앱 ID 클라우드 엔진 배포 준비

방화벽이 App-ID ACE(Cloud Engine)를 사용하기 전에 수행해야 할 몇 가지 온보딩 작업이 있습니다. 독립 실행형 방화벽에 ACE를 배포하거나 Panorama를 사용하여 관리 방화벽에 ACE를 배포할 수 있습니다.

방화벽이 ACE를 사용하여 이전에 ssl, 웹 브라우징, unknown-tcp 및 unknown-udp 트래픽으로 식별된 트래픽에 대한 특정 App-ID를 제공할 수 있으려면 PAN-OS 관리자와 SaaS 보안 관리자가 협력하여 다음을 수행해야 합니다.

- ACE 방화벽을 관리하는 Panorama 어플라이언스를 포함하여 ACE를 사용할 각 어플라이언스에 유효한 디바이스 인증서를 설치하십시오. (PAN-OS 관리자.)
- ACE를 사용할 각 방화벽에서 SaaS 보안 인라인을 활성화합니다. Panorama는 라이선스가 필요하지 않습니다. (SaaS 보안 관리자.)
- 방화벽과 ACE 간의 통신을 위한 서비스 경로를 구성합니다. (PAN-OS 관리자.)
- ACE를 사용할 방화벽을 관리하는 Panorama 어플라이언스에서 ACE를 활성화합니다. (PAN-OS 관리자.)

  방화벽에서 ***ACE***는 ***SaaS Security Inline***을 활성화한 후 기본적으로 활성화됩니다.

- ACE 트래픽을 허용하는 보안 정책 규칙을 생성합니다. (PAN-OS 관리자.)
- 방화벽에서 Cortex Data Lake(CDL)로의 로그 포워딩을 구성합니다. (PAN-OS 관리자.)

다음 절차의 적절한 단계에서 ***PAN-OS*** 관리자는 ***SaaS*** 보안 관리자에게 배포가 ***SaaS*** 보안 인라인 활성화를 위한 준비가 되었음을 알려야 합니다. ***SaaS Security Inline***을 활성화한 후 ***SaaS Security Inline*** 관리자는 ***PAN-OS*** 관리자에게 ***PAN-OS*** 디바이스에서 배포를 완료할 준비가 되었음을 알려야 합니다. 원활한 배포를 위해서는 관리자 간의 커뮤니케이션이 필수적입니다.

요구 사항:

- 독립 실행형 방화벽, Panorama 어플라이언스 및 관리 방화벽은 PAN-OS 10.2 이상을 실행해야 합니다.
- 모든 ACE 방화벽은 SaaS 보안 인라인 라이선스를 구매해야 합니다. Panorama는 ACE 방화벽을 관리하거나 ACE 구성을 관리 방화벽에 푸시하기 위한 라이선스가 필요하지 않습니다.


©2023 Palo Alto Networks, Inc.

- 모든 ACE 어플라이언스는 위치에 따라 미국, APAC 또는 EU GCP 지역에 연결할 수 있어야 합니다(지역은 CDL 지역에 따라 자동으로 선택됨).

  방화벽이 해당 지역에 대해 올바른 콘텐츠 클라우드 FQDN(디바이스 > 설정 > **Content-ID** > 콘텐츠 클라우드 설정)을 사용하는지 확인하고 필요한 경우 FQDN을 변경합니다.

  - 미국 - **hawkeye.services-edge.paloaltonetworks.com**
  - EU - **eu.hawkeye.services-edge.paloaltonetworks.com**
  - APAC - **apac.hawkeye.services-edge.paloaltonetworks.com**

  트래픽 페이로드를 포함한 ACE 데이터는 선택한 지역의 서버로 전송됩니다. 해당 지역 외부에 있는 Content Cloud FQDN을 지정하는 경우(예: EU 지역에 있지만 APAC 지역 FQDN을 지정하는 경우) 해당 국가 또는 조직의 개인정보 보호 및 법적 규정을 위반할 수 있습니다.

PAN-OS 관리자는 절차의 처음 두 단계를 완료한 다음 활성화를 위해 SaaS Security Inline 관리자에게 포워딩합니다(3단계). 활성화 후 SaaS Security Inline 관리자는 나머지 절차를 PAN-OS 관리자에게 포워딩하여 PAN-OS 디바이스에서 완료합니다.

**STEP 1 |** 방화벽과 Panorama(사용하는 경우)를 온라인으로 전환합니다. (PAN-OS 관리자.)

**STEP 2 |** 장치 인증서를 개별 방화벽에 설치하여 클라우드 서비스를 사용하거나 파노라마를 사용하여 관리되는 방화벽용 장치 인증서를 설치할 수 있습니다. (PAN-OS 관리자.)

*SaaS* 보안 관리자에게 다음 단계를 넘깁니다.

**STEP 3 |** ACE를 사용할 모든 방화벽에서 SaaS 보안 인라인을 활성화합니다. 활성화하면 방화벽에서 ACE가 활성화됩니다. (SaaS 보안 관리자.)

*Panorama*는 *ACE*를 사용하는 방화벽을 관리하기 위해 *SaaS* 보안 인라인 라이선스가 필요하지 않습니다. 관리되는 방화벽에만 라이선스가 필요하며 라이선스는 다음 단계에 표시된 대로 수동으로 검색해야 합니다.

나머지 단계는 *PAN-OS* 관리자에게 넘깁니다.

**STEP 4 |** 각 방화벽에서 SaaS 보안 인라인 라이선스(Panorama에는 라이선스가 필요 없음)를 검색하고 활성화되었는지 확인합니다. (PAN-OS 관리자.)

SaaS 보안 관리자의 활성화는 방화벽에 대한 라이선스를 설정하므로 고객 지원 포털로 이동하거나 인증 코드를 얻을 필요가 없습니다.

1. 디바이스 > 라이선스 > 라이선스 관리로 이동하고 라이선스 서버에서 라이선스 키 검색을 선택하여 라이선스를 검색합니다.
2. 디바이스 > 라이선스를 확인하여 SaaS 보안 인라인 라이선스가 활성 상태인지 확인합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 방화벽이 App-ID 클라우드 엔진과 통신할 수 있도록 데이터 서비스(데이터플레인) 서비스 경로를 구성합니다. (PAN-OS 관리자.)

*Panorama*에서 관리 방화벽으로 이 구성을 푸시할 수 있습니다. *Panorama*와 관리 방화벽은 모두 *PAN-OS 10.2* 이상을 실행해야 합니다.

기본적으로 방화벽은 관리 인터페이스를 데이터 서비스 경로의 소스 인터페이스로 사용하지만 이 단계의 뒷부분에 나와 있는 것처럼 데이터 서비스의 소스 인터페이스 및 소스 주소로 클라우드 서비스에 연결할 수 있는 데이터플레인 인터페이스를 구성하는 것이 좋습니다.

방화벽의 문제는 명시적 프록시가 관리 인터페이스에 구성되어 있고 이를 데이터 서비스 경로에 사용하는 경우 관리 인터페이스가 클라우드 애플리케이션 및 서명을 관리하는 지식 클라우드 서비스(KCS)에만 연결할 수 있다는 것입니다. 명시적 프록시가 관리 인터페이스에 구성된 경우 기존 ACE App-ID에 대해 애플리케이션 페이로드를 확인하고 판정을 제공하는 DCS(Detection Cloud Service)에 연결할 수 없습니다. KCS 및 DCS는 ACE 클라우드의 서비스입니다. 관리 인터페이스에 명시적 프록시가 구성되어 있으면 모든 서비스에 연결할 수 없기 때문에 ACE에 대한 데이터 서비스 경로에 사용할 수 없습니다. 이 경우 방화벽의 데이터플레인 인터페이스를 사용하여 데이터 서비스에 연결해야 합니다.

*Panorama*는 기본적으로 관리 포트를 사용하여 *KCS*에 연결하고 *DCS*에 연결하지 않습니다.

기본 관리 인터페이스를 사용하는 대신 데이터 플레인 인터페이스에서 서비스 경로를 구성하려면:

1. 디바이스 > 설정 > 서비스를 선택한 다음 서비스 기능에서 서비스 경로 구성을 선택합니다.
2. 서비스 경로를 맞춤설정합니다.
3. **IPv4** 프로토콜을 선택합니다.
4. 서비스 열에서 데이터 서비스를 클릭하여 서비스 경로 소스 대화 상자를 엽니다.
5. 소스 인터페이스 및 소스 주소를 선택합니다(관리 인터페이스일 수 없음).

   소스 인터페이스는 인터넷에 연결되어 있어야 합니다. 가장 좋은 방법은 클라우드 서비스에 연결되는 데이터플레인 인터페이스를 사용하는 것입니다. 소스 인터페이스 및 주소 생성에 대한 자세한 내용은 인터페이스 구성 및 주소 개체 생성을 참조하십시오.
6. 확인을 클릭하여 소스 인터페이스와 주소를 설정합니다.
7. 확인을 클릭하여 서비스 경로 구성을 설정합니다.
8. 정책 > 보안을 선택하고 이 절차의 앞부분에서 지정한 소스 인터페이스의 트래픽을 FQDN 주소로 허용하는 보안 정책 규칙을 추가합니다. **kcs.ace.tpcloud.paloaltonetworks**(모든 지역의 KCS 서비스) 및 **hawkeye.services-edge.paloaltonetworks.com**(미국 지역 DCS 서비스)인 KCS 및 DCS 서비스의 경우 ), **eu.hawkeye.services-edge.paloaltonetworks.com**(EU 지역 DCS 서비스) 또는

 ©2023 Palo Alto Networks, Inc.

**apac.hawkeye.services-edge.paloaltonetworks.com**(APAC 지역 DCS 서비스) .

또한 신규 또는 기존 보안 정책 규칙에 인증서 확인을 위해 **ocsp.paloaltonetworks.com** 및 **crl.paloaltonetworks.com**의 두 FQDN을 추가하고 허용합니다.

마지막으로 **paloalto-ace**, **paloalto-ace-kcs** 및 **paloalto-dlp-service**의 세 가지 애플리케이션을 허용하여 ACE 트래픽을 허용하도록 보안 정책 규칙을 추가하거나 수정합니다.

**STEP 6 |** 방화벽에서 hawkeye.services-edge.paloaltonetworks.com 및 kcs.ace.tpcloud.paloaltonetworks에 연결할 수 있고 Panorama 디바이스에서 kcs.ace.tpcloud.paloaltonetworks에 연결할 수 있는지 확인합니다. (PAN-OS 관리자.)

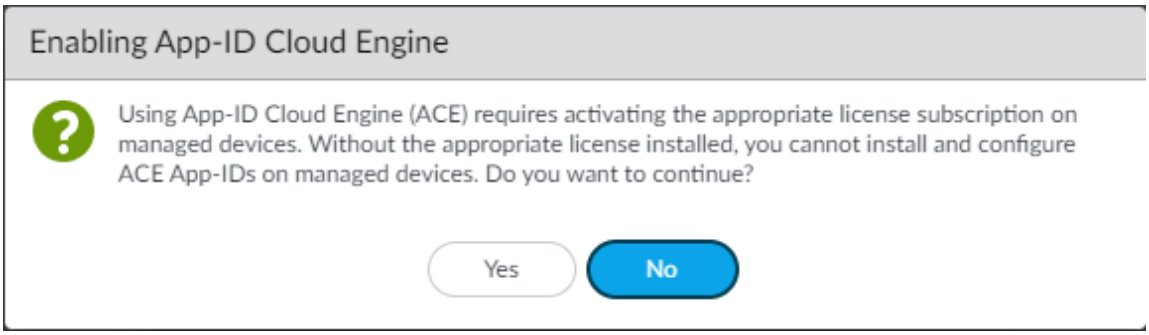
운영 명령 `admin@fw1> show cloud-appid connection-to-cloud`를 실행합니다. 출력은 연결이 작동하는지의 여부와 라이선스가 설치되었는지의 여부를 알려줍니다.

**STEP 7 |** (Panorama에만 해당) ACE 지원 방화벽을 관리하는 Panorama 어플라이언스에서 ACE를 활성화합니다. (PAN-OS 관리자.)

ACE는 Panorama에서 기본적으로 비활성화되어 있습니다.

*ACE* 사용 방화벽이 없는 관리되는 그룹에 *ACE* 구성을 푸시하면*(*그룹의 일부 또는 모든 방화벽에 *ACE*가 활성화되지 않음*)* 푸시가 실패합니다**.**

1. 파노라마 > 설정 > **ACE** > 설정으로 이동합니다.
2. 수정(⚙)을 클릭한 다음 **App-ID Cloud Engine** 비활성화를 선택 취소합니다.
3. 확인을 클릭합니다.
4. **App-ID** 클라우드 엔진 사용 대화 상자가 나타납니다.




   예를 클릭하여 ACE를 활성화합니다.
5. 변경 사항을 커밋합니다.

**STEP 8 |** App-ID 카탈로그가 다운로드될 때까지 기다립니다. (PAN-OS 관리자.)

콘텐츠 제공 App-ID는 4,000개 미만입니다. ACE 카탈로그를 다운로드하면 방화벽에 수천 개의 애플리케이션이 더 표시되며 **Objects** > **Applications**를 확인하거나 운영 CLI 명령 `show cloud-appid cloud-app-data application all`을 사용하여 새 App-ID를 확인하여 확인할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 9 |** (Panorama만 해당) 원하는 구성을 관리되는 방화벽으로 푸시합니다. (PAN-OS 관리자.)

**STEP 10 |** Cortex Data Lake(CDL)에 대한 로그 포워딩을 구성하고 보안 정책 규칙에서 올바른 로그 포워딩 프로파일로 로그 포워딩을 활성화하십시오. (PAN-OS 관리자.)

> ***SaaS*** 가시성과 ***SaaS App-ID*** 정책 권장 사항을 지원하려면 CDL에 대한 SaaS 보안 인라인 연결이 필요합니다. ***SaaS Security Inline***이 제대로 작동하려면 최소한 트래픽 로그와 ***URL*** 로그를 ***CDL***로 포워딩해야 합니다.

## 앱 ID 클라우드 엔진 사용 또는 비활성화

앱 ID 클라우드 엔진(ACE)은 Panorama에서 기본적으로 비활성화되어 있으며 SaaS 보안 인라인 라이선스가 설치되면 방화벽에서 기본적으로 활성화됩니다. ACE 사용 방화벽을 관리하는 Panorama 어플라이언스에서 ACE를 사용하도록 설정해야 합니다.

ACE 사용 또는 사용 안 함:

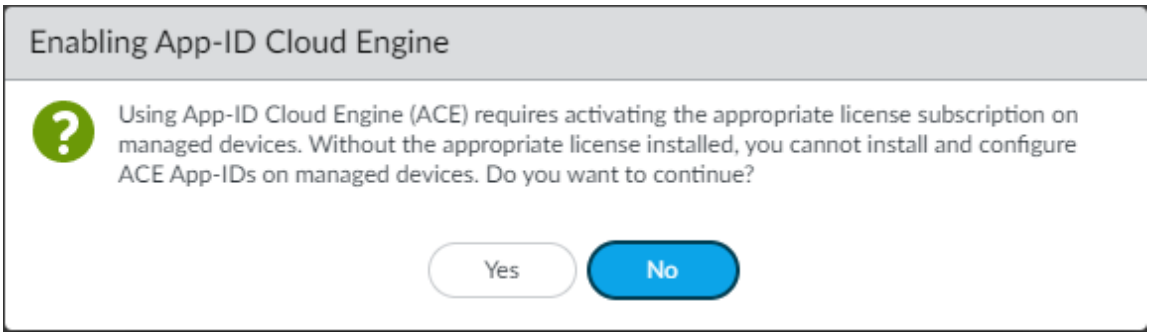
**STEP 1 |** 방화벽의 디바이스 > 설정 > **ACE** > 설정 또는 Panorama의 **Panorama** > 설정 > **ACE** > 설정으로 이동합니다.

**STEP 2 |** 편집(⚙)을 클릭한 다음 앱**-ID** 클라우드 엔진 사용 안 함을 선택 취소하여 ACE를 활성화하거나 앱**-ID** 클라우드 엔진 사용 안 함을 선택하여 ACE를 비활성화합니다.

ACE는 기본적으로 비활성화되어 있습니다.

**STEP 3 |** 확인을 클릭합니다.

**STEP 4 |** (ACE를 사용하도록 설정한 경우에만) ACE를 사용하도록 설정하면 **App-ID** 클라우드 엔진 사용 대화 상자가 나타납니다.




방화벽 또는 Panorama 관리 방화벽에 SaaS 보안 인라인 라이선스가 설치되어 있는 경우 예를 클릭하여 ACE를 사용하도록 설정합니다.

**STEP 5 |** 변경 사항을 커밋합니다.

## App-ID 클라우드 엔진 처리 및 사용

방화벽이 App-ID ACE(Cloud Engine) App-ID를 다운로드할 때 방화벽이 동일한 애플리케이션에 대해 해당 App-ID를 처리하는 방법과 방화벽이 ACE App-ID를 처리하는 방법을 이해하는 것이 중요합니다. Palo Alto Networks 콘텐츠 팀은 사전 정의된 콘텐츠 기반 App-ID를 개발하고 애플리케이션 콘텐츠 업데이트를 통해 수정된 신규 App-ID로 업데이트합니다(업데이트에 유효한 지원 계약 필요).

 ©2023 Palo Alto Networks, Inc.

ACE에는 SaaS 보안 인라인 라이선스가 필요합니다. ACE를 지원하지 않는 방화벽에는 사전 정의된 콘텐츠 기반 App-ID만 있습니다. ACE App-ID 카탈로그에는 콘텐츠 기반 App-ID가 포함되어 있지 않습니다.

보안 정책 규칙에서는 ***ACE App-ID***만 사용할 수 있습니다. 다른 유형의 정책 규칙에서는 ***ACE App-ID***를 사용할 수 없습니다.

- 방화벽이 App-ID 클라우드 엔진에 처음 연결할 때 방화벽은 사용 가능한 ACE App-ID의 카탈로그를 다운로드하고 보안 정책에서 해당 App-ID를 사용할 수 있습니다. 전체 서명을 다운로드하지 않습니다. 카탈로그를 사용하면 방화벽에서 애플리케이션을 본 적이 없는 경우에도 보안 정책에서 ACE App-ID를 사용할 수 있습니다. ACE는 카탈로그 업데이트를 방화벽에 정기적으로 푸시하여 방화벽이 최신 ACE App-ID에 액세스할 수 있도록 합니다.

  애플리케이션이 ssl, 웹 브라우징, unknown-tcp 또는 unknown udp로 식별되는 방화벽에 도착하고 방화벽에 서명이 없으면 방화벽은 페이로드를 ACE로 보냅니다. ACE에 트래픽에 대한 App-ID가 있는 경우 ACE는 전체 서명을 방화벽으로 다시 보냅니다. 트래픽이 ACE 서명과 일치하지 않으면 ACE는 페이로드를 기계 학습(ML) 엔진으로 보냅니다. ML 엔진은 페이로드를 분석하고 휴먼 콘텐츠 팀과 함께 신규 App-ID를 개발하고 애플리케이션과 관련이 없는 트래픽을 삭제합니다. ML 엔진은 신규 App-ID를 ACE로 보내고 방화벽을 요청하면 이를 다운로드하여 보안 정책에서 사용할 수 있습니다.

  ***App-ID***가 있는 ***ACE***에서 애플리케이션을 검색하는 데 몇 분이 걸리고 신규 ***App-ID***를 개발해야 하는 경우 더 오래 걸릴 수 있으므로 클라우드 애플리케이션 감지는 방화벽에서 인라인되지 않습니다. 방화벽은 애플리케이션 트래픽을 처리하기 위한 판정을 기다리지 않습니다. 방화벽은 ***ACE***에서 ***App-ID***를 받을 때까지 트래픽을 ***ssl***, ***web-browsing***, ***unknown-tcp*** 또는 ***unknown-udp***로 처리한 다음 사용자가 새 ***App-ID***를 받고 보안 정책에서 사용할 때까지 이러한 방식으로 트래픽을 계속 처리합니다.

- 방화벽이 ACE에서 App-ID를 요청하면 방화벽은 트래픽을 보유하지 않고 ACE에서 App-ID를 받을 때까지 평소와 같이 트래픽을 계속 처리합니다.
- 방화벽은 콘텐츠 제공 App-ID를 처리하는 것과 다르게 ACE에서 다운로드한 클라우드 App-ID를 처리합니다. 방화벽은 기존 보안 정책에 따라 ACE App-ID를 사용하기 때문에 방화벽에 설치하기 전에 새 ACE App-ID가 보안 정책에 어떤 영향을 미치는지 검사할 필요가 없습니다. 기존 보안 정책 규칙은 보안 정책에서 ACE App-ID를 명시적으로 사용할 때까지 새 ACE App-ID를 제어합니다. 예:

  1. 애플리케이션은 "ssl"로만 식별되며 SSL 트래픽을 허용하는 보안 정책 규칙이 있으므로 SSL 규칙이 해당 애플리케이션을 허용합니다.
  2. 방화벽은 SSL 애플리케이션을 확인하고 페이로드를 ACE로 보냅니다.
  3. ACE는 실제 애플리케이션을 식별합니다. 애플리케이션이 ACE 데이터베이스에 있는 경우 ACE는 해당 App-ID를 방화벽으로 보냅니다. ACE에 App-ID가 없는 새 애플리케이션인 경우 ACE는 페이로드를 ML 엔진으로 포워딩합니다. 방화벽은 ML Engine과 휴먼 콘텐츠 팀이 App-ID를 할당하고 ACE에 보낼 때까지 App-ID를 수신하지 않습니다.
  4. SSL 트래픽을 허용하는 규칙은 App-ID가 더 이상 "ssl"이 아니더라도 새로 식별된 애플리케이션을 계속 허용합니다. (단, 보안 정책에서 신규 ACE App-ID를 사용하는 경우 해당 정책이 트래픽을 제어합니다. 마찬가지로 이전에 웹 브라우징, unknown-tcp 및 unknown-udp로 식별된 트래픽은 보


©2023 Palo Alto Networks, Inc.

안 정책에서 ACE App-ID를 사용할 때까지 이러한 유형의 트래픽을 제어하는 보안 정책 규칙을 계속 따릅니다.)

> ***ACE App-ID***와 달리 ***App-ID***가 사전 정의된 콘텐츠가 제공된 ***App-ID***인 경우 ***SSL*** 트래픽을 허용하는 규칙이 더 이상 애플리케이션과 일치하지 않습니다. 방화벽은 보안 정책 규칙에서 명시적으로 허용하지 않는 경우 이를 차단합니다.

이 동작의 예외는 다른 보안 정책 규칙이 ACE에서 트래픽에 부여한 App-ID를 지정하는 경우입니다. 특정 App-ID가 있는 보안 정책 규칙이 덜 구체적인 SSL App-ID가 있는 규칙보다 우선합니다. 실제 App-ID를 지정하는 규칙이 차단 규칙인 경우 SSL 트래픽을 허용하는 규칙이 있어도 해당 애플리케이션이 차단됩니다. 보다 구체적인(세부적인) App-ID가 있는 규칙이 방화벽이 작동하는 규칙입니다.

> 이 예에서 직접 또는 애플리케이션 필터 또는 애플리케이션 그룹을 사용하여 기존 또는 복제된 규칙에 이전에 ***"ssl"***로 식별된 애플리케이션의 클라우드 ***App-ID***를 추가하면 해당 규칙이 애플리케이션을 제어합니다. 애플리케이션이 다른 규칙에서 구체적으로 식별되기 때문에 ***"ssl"*** 규칙이 더 이상 애플리케이션을 제어하지 않습니다.

보안 정책 규칙에 새 ACE App-ID를 명시적으로 추가하지 않으면 방화벽은 ACE App-ID를 보유하고 ssl, web-browsing, unknown-tcp 또는 unknown-udp 트래픽으로 식별되기 전에 해당 애플리케이션을 제어했던 것과 동일한 규칙으로 계속 제어합니다. 예를 들어 방화벽이 unknown-tcp로 식별된 애플리케이션을 확인한 다음 트래픽에 대한 ACE App-ID를 수신하지만 보안 정책 규칙에서 해당 ACE App-ID를 사용하지 않는 경우 방화벽은 여전히 해당 트래픽을 제어합니다. unknown-tcp 트래픽을 제어하는 규칙을 사용하여 unknown-tcp 트래픽을 차단하면 트래픽이 차단되고 unknown-tcp 트래픽을 허용하면 트래픽이 허용됩니다.

- 방화벽은 일부 정보를 캐시에 저장하여 방화벽이 캐시를 확인하고 클라우드에 데이터를 반복적으로 보내고 판정을 요청하는 것을 방지할 수 있도록 합니다. 방화벽이 ACE의 판정을 기다리는 경우 방화벽은 동일한 애플리케이션 데이터를 두 번 포워딩하지 않습니다.
- 특정 컨테이너 앱 및 해당 기능 애플리케이션은 모두 클라우드 기반 App-ID이거나 모든 콘텐츠 기반 App-ID입니다. 하나의 App-ID 포워딩 메서드는 컨테이너 앱과 모든 기능 앱을 정의합니다.
- 클라우드 기반, 콘텐츠 제공 및 사용자 정의 App-ID 이름이 겹치는 경우 우선 순위는 다음과 같습니다.
  1. 사용자 지정 **App-ID** - 이러한 App-ID는 다른 모든 App-ID보다 우선하며 방화벽이 동일한 App-ID를 가진 ACE 애플리케이션을 다운로드하려고 하면 동일한 방화벽에 있는 두 애플리케이션이 동일한 App-ID를 가질 수 없기 때문에 커밋이 실패합니다.

     이 경우 사용자 지정 애플리케이션의 이름을 변경할 수 있으며 사용자 지정 애플리케이션이 ACE 애플리케이션과 동일한 애플리케이션인 경우 사용자 지정 애플리케이션을 삭제하고 ACE 애플리케이션을 사용할 수 있습니다.
  2. 콘텐츠 기반의 사전 정의된 **App-ID** - 이러한 App-ID는 ACE 클라우드 App-ID 정의보다 우선합니다.
  3. **ACE** 클라우드 **App-ID** - 사용자 지정 및 콘텐츠 기반 App-ID가 ACE App-ID 정의보다 우선합니다.
- App-ID가 컨테이너 앱과 일치하는 경우 방화벽은 컨테이너 앱의 App-ID와 모든 기능 앱을 다운로드합니다. 예를 들어 방화벽이 facebook 컨테이너 앱을 검색하면 facebook-base, facebook-chat, facebook-post 등도 검색합니다.


©2023 Palo Alto Networks, Inc.

- ACE App-ID에 대해 다음 작업 중 하나를 수행하면 방화벽이 특정 ACE App-ID를 기반으로 작업을 수행하기 때문에 애플리케이션의 이전 SSL, 웹 브라우징, unknown-tcp 또는 unknown-udp App-ID를 기반으로 하는 대신 보안 정책이 해당 ACE App-ID를 처리하는 방식에 영향을 줍니다.
  - 애플리케이션 필터를 만들어 보안 정책에 ACE App-ID 추가를 자동화합니다.

    애플리케이션 필터를 사용하여 보안 정책 규칙에 ***ACE App-ID*** 추가를 자동화합니다. 신규 ***App-ID***가 애플리케이션 필터와 일치하면 방화벽이 자동으로 필터에 추가합니다. 보안 정책 규칙에서 해당 애플리케이션 필터를 사용하는 경우 규칙은 필터에 자동으로 추가된 신규 ***App-ID***에 대한 애플리케이션 트래픽을 제어합니다. 다시 말해, 애플리케이션 필터는 ***ACE App-ID***를 자동으로 보호하여 최소한의 노력으로 최대한의 애플리케이션 가시성과 제어를 확보할 수 있는 "간편 버튼"입니다.
  - 애플리케이션 그룹에 App-ID를 추가합니다.
  - 정책 최적화 프로그램을 사용하여 복제된 규칙이나 기존 규칙 또는 기존 애플리케이션 필터나 애플리케이션 그룹에 App-ID를 추가합니다. 정책 최적화 프로그램을 사용하여 정책 최적화 프로그램 도구 내에서 직접 새 애플리케이션 필터 및 애플리케이션 그룹을 생성할 수 있습니다. 정책 최적화 프로그램의 정렬 및 필터링 도구를 사용하여 작업할 규칙의 우선 순위를 지정하고 해당 규칙과 일치하는 ACE App-ID의 수를 평가하십시오.
  - ACE App-ID를 새 보안 정책 규칙이나 기존 보안 정책 규칙에 직접 추가합니다.

  클라우드 App-ID를 보안 정책 규칙에 직접 추가하거나 애플리케이션 필터 또는 애플리케이션 그룹을 사용하여 추가하면 해당 규칙이 애플리케이션을 제어합니다. 클라우드 제공 App-ID를 제어하기 위해 이러한 작업 중 하나를 수행할 때까지 방화벽은 기존 ssl, 웹 브라우징, unknown-tcp 또는 unknown-udp 보안 정책 규칙을 사용하여 ACE 애플리케이션을 제어합니다.
- 애플리케이션 필터를 생성할 때 필터에서 SSL 및 웹 브라우징을 제외하십시오. SSL과 웹 브라우징은 함께 모든 브라우저 기반 클라우드 애플리케이션과 일치하므로 SSL과 웹 브라우징을 포함하는 애플리케이션 필터는 모든 브라우저 기반 클라우드 애플리케이션과 일치합니다.
- 능동형/수동형 고가용성:
  - 능동형 방화벽은 ACE 카탈로그를 수동형 방화벽과 동기화하여 카탈로그가 동일하도록 합니다.
  - 수동형 방화벽은 능동형 방화벽이 될 때까지 ACE에 대한 연결을 시작하지 않습니다.
- 능동형/능동형 고가용성: 각 디바이스는 카탈로그와 서명을 별도로 가져오기 때문에 카탈로그와 서명이 동기화되지 않습니다. 그러나 카탈로그가 피어에서 동기화되지 않고 ACE App-ID가 보안 정책 규칙에서 참조되는 경우 커밋이 실패합니다. 피어 HA 방화벽 카탈로그가 동기화되지 않은 경우 업데이트가 디바이스에 도달하고 다시 동기화될 때까지 몇 분 정도 기다리십시오.


©2023 Palo Alto Networks, Inc.

- 다음과 같은 경우 관리되는 방화벽에 대한 Panorama 커밋 전체/푸시 실패가 발생합니다.
  - 관리형 방화벽에는 유효한 SaaS 보안 인라인 라이선스가 없으므로 ACE 카탈로그가 없습니다. 이 경우 푸시된 구성에서 ACE 개체를 제거하고 다시 시도하십시오.
  - 관리되는 방화벽과 ACE 간의 연결이 끊어지고 푸시된 구성에 방화벽의 ACE 카탈로그에 없는 애플리케이션이 포함됩니다. 이 경우 방화벽이 카탈로그를 업데이트할 수 있도록 ACE 클라우드에 대한 연결을 확인하고 필요한 경우 연결을 다시 설정하십시오.

    운영 CLI 명령 **`show cloud-appid connection-to-cloud`**는 클라우드 연결 상태 및 ACE 클라우드 서버 URL을 제공합니다.
  - Panorama의 ACE 카탈로그와 관리 방화벽의 ACE 카탈로그가 동기화되지 않아 방화벽 카탈로그에 없는 ACE 앱이 포함된 구성이 푸시됩니다. 방화벽과 ACE 간의 연결이 설정되어 있으면 몇 분 안에 오래된 카탈로그가 자동으로 업데이트되어 문제를 해결합니다. (5분 정도 기다렸다가 다시 시도하십시오.)

    > *CLI 명령 **`debug cloud-appid cloud-manual-pull check-cloud-app-data`**를 사용하여 카탈로그를 수동형으로 업데이트할 수도 있습니다.*
- 파일 차단, 바이러스 백신, WildFire 및 DLP 프로파일과 같은 일부 보안 프로파일은 애플리케이션을 프로파일의 일부로 지정할 수 있습니다. 보안 프로파일에서는 콘텐츠 제공 App-ID만 지원됩니다. ACE App-ID는 보안 프로파일에서 지원되지 않습니다. ACE App-ID는 보안 정책 규칙에서만 사용하기 위한 것입니다.
- ACE App-ID는 보안 정책에 대해서만 지원되기 때문에 애플리케이션 재정의, PBF(정책 기반 포워딩), QoS 또는 SD-WAN 정책 규칙에서는 지원되지 않습니다.

> *애플리케이션 재정의 또는 **PBF** 규칙 구성에서 **ACE App-ID**를 볼 수 없습니다. 그러나 **ACE App-ID**는 **QoS** 및 **SD-WAN** 정책 규칙 구성에서 볼 수 있고(선택 가능) 규칙에 적용된 애플리케이션 그룹 또는 애플리케이션 필터에 있을 수 있습니다. 이러한 규칙에서 **ACE App-ID**를 사용하는 경우 정책은 애플리케이션 트래픽을 제어하지 않으며 애플리케이션 트래픽에 영향을 미치지 않습니다. 규칙에 **ACE App-ID**가 추가된 경우에도 규칙이 **ACE App-ID** 트래픽에 적용되지 않습니다.*

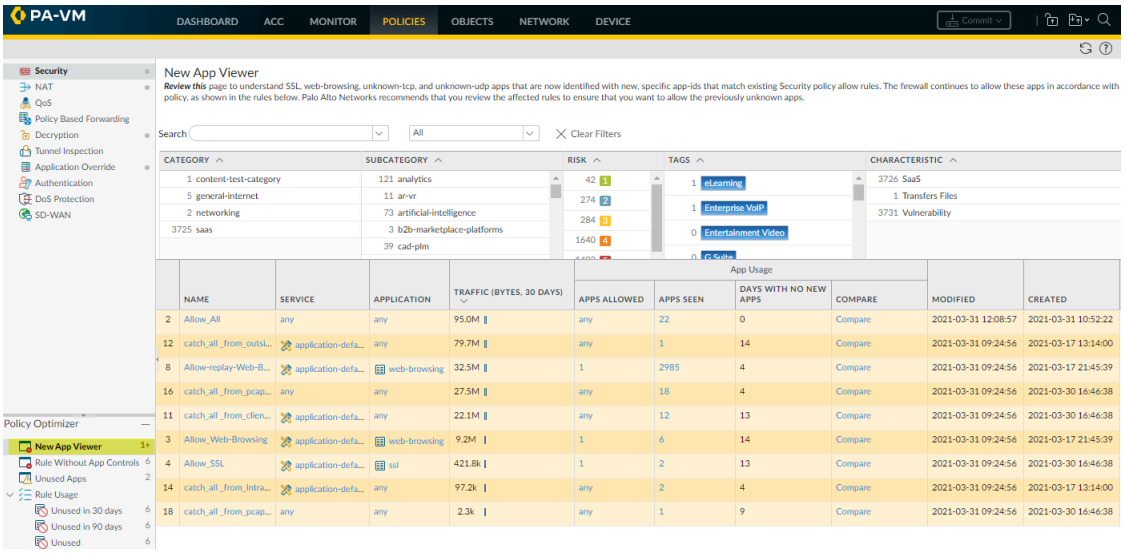
## 신규 앱 뷰어(정책 최적화 프로그램)

Policy Optimizer **New App Viewer**는 ACE에서 다운로드한 클라우드 App-ID와 일치하는 보안 정책 규칙을 보여줍니다. Policy Optimizer를 사용하여 새로 식별된 애플리케이션을 관리하고 복사된 규칙이나 기존 규칙에 추가할 수 있습니다. 정책 > 보안을 선택하여 인터페이스의 정책 최적화 부분에 새 앱 뷰어를 표시한 다음 새 앱 뷰어를 선택합니다.

화면 상단은**Objects** > **Application Filters**와 유사합니다. 유사한 방식으로 작동하며 화면 하단에 표시된 보안 정책 규칙을 필터링합니다. 카테고리, 하위 카테고리 등으로 애플리케이션을 허용하는 규칙을 필터링할 수 있습니다. 필터링에 사용할 수 있는 유일한 카테고리 및 하위 카테고리는 화면 하단에 나열된 규칙의 새 애플리케이션과 일치하는 것이므로 없는 애플리케이션을 필터링하는 데 시간을 낭비하지 않아도 됩니다.

규칙을 필터링하면 필터링된 애플리케이션이 포함된 규칙만 화면 하단에 표시됩니다. 필터에서 앱을 보지 못한 규칙은 목록에서 제거됩니다. (필터를 제거하면 모두 다시 볼 수 있습니다.)


©2023 Palo Alto Networks, Inc.




표시된 앱 열의 숫자를 클릭하여 애플리케이션 및 사용량 대화상자를 열고 보안 정책에서 방화벽이 클라우드 기반 애플리케이션을 처리하는 방식을 변경합니다. 애플리케이션 필터, 애플리케이션 그룹, 정책 최적화 프로그램을 사용하거나 규칙에 ACE App-ID를 직접 추가하여 보안 정책 규칙에 ACE App-ID를 추가합니다. 클라우드 제공 App-ID를 제어하기 위해 이러한 작업 중 하나를 수행할 때까지, 방화벽은 트래픽을 SSL, 웹 브라우징, unknown-tcp 또는 unknown-udp 트래픽으로 계속 보고 기존 ssl, 웹 브라우징, unknown- tcp 또는 unknown-udp 애플리케이션을 제어하는 보안 정책 규칙입니다.

## 정책 최적화 프로그램을 사용하여 애플리케이션 필터에 앱 추가

App-ID Cloud Engine(ACE 및/또는 콘텐츠 제공 App-ID)의 App-ID를 신규 또는 기존 애플리케이션 필터에 추가하여 보안 정책에서 클라우드 App-ID를 제어하는 방법을 자동화하십시오. 새 ACE App-ID가 애플리케이션 필터와 일치하면 방화벽이 이를 필터에 자동으로 추가합니다. 보안 정책 규칙에서 애플리케이션 필터를 사용하는 경우 규칙은 새 ACE App-ID가 방화벽에 도착하고 필터에 추가될 때 자동으로 제어합니다.

***ACE***는 이전에 ***ssl***, 웹 브라우징, 알 수 없는 ***tcp*** 또는 알 수 없는 ***UDP***로 식별된 애플리케이션에 대한 앱 ***ID***를 제공합니다.

애플리케이션 필터를 사용하는 것은 다음과 같은 이유로 모범 사례입니다.

- 보안 태세를 개선하십시오. 애플리케이션 필터는 트래픽을 보다 일반적인 SSL, 웹 브라우징, unknown-tcp 또는 unknown-udp 규칙과 일치시키는 대신 특정 유형의 애플리케이션 트래픽을 처리하도록 특별히 설계한 보안 정책 규칙에 신규 ACE App-ID를 자동으로 추가합니다.
- 시간을 절약. 방화벽 관리자는 정책에 새 ACE App-ID를 자동으로 추가하고 관리자의 추가 노력이 필요하지 않도록 다양한 유형의 트래픽을 처리하도록 애플리케이션 필터를 구성할 수 있습니다.

애플리케이션 필터를 생성할 때 필터에서 ***SSL*** 및 웹 브라우징을 제외하십시오. ***SSL***과 웹 브라우징은 함께 모든 브라우저 기반 클라우드 애플리케이션과 일치하므로 ***SSL***과 웹 브라우징을 포함하는 애플리케이션 필터는 모든 브라우저 기반 클라우드 애플리케이션과 일치합니다.

Policy Optimizer를 사용하여 ACE App-ID를 애플리케이션 필터에 추가하고 필터를 복제 또는 기존 규칙에 적용하고 보안 정책에서 ACE App-ID를 제어합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 정책 > 보안으로 이동한 다음정책 최적화 프로그램 > 신규 앱 뷰어를 선택합니다.

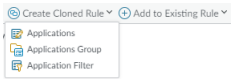
방화벽이 ACE App-ID로 트래픽을 식별한 경우 왼쪽 탐색 창의 신규 앱 뷰어 옆에 숫자가 표시됩니다. 화면에 클라우드 App-ID와 일치하는 보안 정책 규칙이 표시됩니다.

**STEP 2 |** 애플리케이션 및 사용 대화 상자에서 규칙과 일치하는 클라우드 제공 애플리케이션을 보려면 보안 정책 규칙에 대해 표시되는 앱에서 숫자를 클릭합니다.

**STEP 3 |** 기존 또는 새 애플리케이션 필터에 추가할 애플리케이션을 선택합니다.

하위 카테고리, 위험, 지난 30일 동안 본 트래픽 양 또는 애플리케이션이 처음 또는 마지막으로 표시되었을 때 표시되는 **Apps**에서 애플리케이션을 정렬하고 필터링할 수 있습니다.

**STEP 4 |** 애플리케이션 처리 방식에 따라 복제된 규칙 생성 또는 기존 규칙에 추가에서 애플리케이션 필터를 선택합니다.



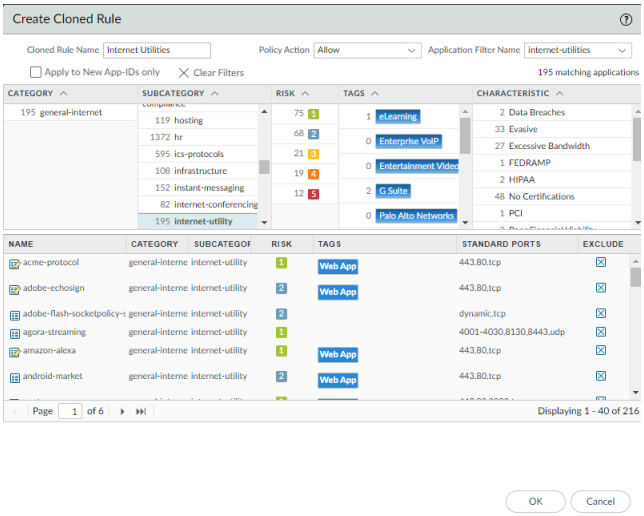

복제된 규칙 생성을 사용하여 복제할 수 있는 최대 애플리케이션 수는 *1,000*개의 애플리케이션입니다. *1,000*개 이상의 애플리케이션이 다른 규칙으로 이동하는 경우 기존 규칙에 추가를 대신 사용합니다. 애플리케이션을 새 규칙으로 이동하려면 먼저 규칙을 만든 다음 (정책 > 보안) 정책 최적화 프로그램을 사용하여 규칙을 해당 규칙에 추가합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 복제된 규칙 또는 기존 규칙에 대한 애플리케이션 필터를 선택하거나 생성합니다. 정책 최적화 프로그램을 사용하여 애플리케이션 필터를 만드는 것은 개체 > 애플리케이션 필터를 사용하여 애플리케이션 필터를 만드는 것과 거의 동일합니다. 동일한 필터링 도구와 옵션을 사용합니다.

복제된 규칙 생성:

1. 복제된 규칙 이름(복제된 규칙의 이름으로 원래 규칙 바로 위에 있는 보안 정책 규칙 베이스에 표시됨)을 입력합니다.
2. 정책 작업(허용 또는 거부)을 선택합니다.
3. 메뉴에서 애플리케이션 필터 이름을 선택하거나 새 애플리케이션 필터의 이름을 입력합니다.
4. 필터를 신규 **App-ID**에만 적용할지 아니면 모든 App-ID에 적용할지 선택합니다.
5. 카테고리, 하위 카테고리, 위험, 태그 및 특성 값을 사용하여 애플리케이션 필터에 추가할 애플리케이션 유형을 필터링합니다. 방화벽은 필터 기준을 충족하는 새 애플리케이션을 애플리케이션 필터에 자동으로 추가합니다.

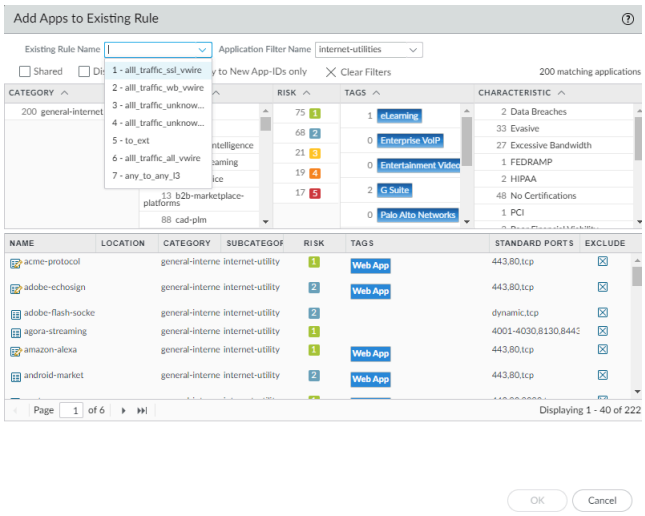



6. 확인을 클릭하여 새 또는 기존 애플리케이션 필터에 애플리케이션을 추가합니다. 방화벽에는 애플리케이션 필터의 3단계에서 선택한 애플리케이션이 포함됩니다.
7. 변경 사항을 커밋합니다.

기존 규칙에 추가:

1. 기존 규칙 이름을 선택하여 선택한 애플리케이션을 애플리케이션 필터의 기존 규칙에 추가합니다.
2. 메뉴에서 애플리케이션 필터 이름을 선택하거나 새 애플리케이션 필터의 이름을 입력합니다.
3. 애플리케이션 필터가 공유되는지의 여부, 필터에 대한 애플리케이션 특성 재정의를 비활성화할지의 여부, 필터를 신규 **App-ID**에만 적용할지 또는 모든 App-ID에 적용할지의 여부를 선택합니다.
4. 카테고리, 하위 카테고리, 위험, 태그 및 특성 값을 사용하여 애플리케이션 필터에 추가할 애플리케이션 유형을 필터링합니다. 방화벽은 필터 기준을 충족하는 새 애플리케이션을 애플리케이션 필터에 자동으로 추가합니다.


©2023 Palo Alto Networks, Inc.




5. 확인을 클릭하여 새 또는 기존 애플리케이션 필터에 애플리케이션을 추가합니다. 방화벽에는 애플리케이션 필터의 3단계에서 선택한 애플리케이션이 포함됩니다.
6. 변경 사항을 커밋합니다.

## 정책 최적화 프로그램을 사용하여 애플리케이션에 앱 추가

App-ID Cloud Engine(ACE 및/또는 콘텐츠 제공 App-ID)의 App-ID를 신규 또는 기존 애플리케이션 그룹에 추가하고 보안 정책 규칙의 애플리케이션 그룹을 사용하여 보안 정책의 클라우드 App-ID를 제어합니다.

***ACE**는 이전에 **ssl**, 웹 브라우징, 알 수 없는 **tcp** 또는 알 수 없는 **UDP**로 식별된 애플리케이션에 대한 앱 **ID**를 제공합니다.*

Policy Optimizer를 사용하여 ACE App-ID를 애플리케이션 그룹에 추가하고 그룹을 복제 또는 기존 규칙에 적용하고 보안 정책에서 ACE App-ID를 제어합니다.

**STEP 1 |** 정책 > 보안으로 이동한 다음정책 최적화 프로그램 > 신규 앱 뷰어를 선택합니다.

방화벽 또는 Panorama가 ACE App-ID를 다운로드한 경우 왼쪽 탐색 창의 신규 앱 뷰어 옆에 숫자가 표시됩니다. 화면에 다운로드한 클라우드 앱 ID와 일치하는 보안 정책 규칙이 표시됩니다.

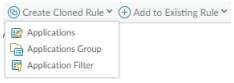
**STEP 2 |** 애플리케이션 및 사용 대화 상자에서 규칙과 일치하는 클라우드 제공 애플리케이션을 보려면 보안 정책 규칙에 대해 표시되는 앱에서 숫자를 클릭합니다.

**STEP 3 |** 기존 또는 새 애플리케이션 그룹에 추가할 애플리케이션을 선택합니다.

하위 카테고리, 위험, 지난 30일 동안 본 트래픽 양 또는 애플리케이션이 처음 또는 마지막으로 표시되었을 때 표시되는 **Apps**에서 애플리케이션을 정렬하고 필터링할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 애플리케이션 처리 방식에 따라 복제된 규칙 생성 또는 기존 규칙에 추가에서 애플리케이션 그룹을 선택합니다.




복제된 규칙 생성을 사용하여 복제할 수 있는 최대 애플리케이션 수는 *1,000*개의 애플리케이션입니다. *1,000*개 이상의 애플리케이션이 다른 규칙으로 이동하는 경우 기존 규칙에 추가를 대신 사용합니다. 애플리케이션을 새 규칙으로 이동하려면 먼저 규칙을 만든 다음 (정책 > 보안) 정책 최적화 프로그램을 사용하여 규칙을 해당 규칙에 추가합니다.

**STEP 5 |** 복제된 규칙 또는 기존 규칙에 대한 애플리케이션 그룹을 선택하거나 생성합니다. 정책 최적화 프로그램을 사용하여 애플리케이션 그룹을 만드는 것은 개체 > 애플리케이션 그룹을 사용하여 애플리케이션 그룹을 만드는 것과 유사합니다.

복제된 규칙 생성:

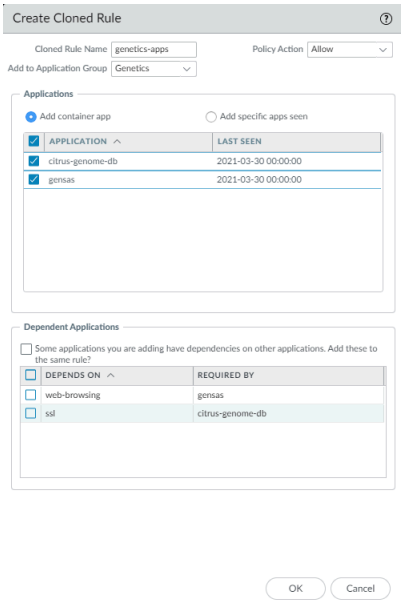
1. 복제된 규칙 이름(복제된 규칙의 이름으로 원래 규칙 바로 위에 있는 보안 정책 규칙 베이스에 표시됨)을 입력합니다.
2. 정책 작업(허용 또는 거부)을 선택합니다.
3. 애플리케이션 그룹에 추가에서 에서 선택한 애플리케이션을 추가할 애플리케이션 그룹을 선택합니다.
4. 컨테이너 앱 추가(기본값) 또는 표시된 특정 앱 추가만 선택할 수 있습니다.

   컨테이너 앱을 추가할 때 아직 방화벽에서 볼 수 없는 기능 앱을 포함하여 해당 컨테이너에 있는 모든 기능 앱도 추가합니다. 예를 들어 “페이스 북”컨테이너 앱을 추가하면 페이스 북 기반, 페이스 북 채팅, 페이스 북 게시 등과 컨테이너에 추가된 향후 애플리케이션이 추가됩니다. 컨테이너 앱 및 해당 기능 앱에는 애플리케이션 그룹을 추가하는 보안 정책 규칙이 적용됩니다. 컨테이너 앱을 선택하면 기본적으로 컨테이너의 앱에 대한 보안이 미래에도 보장되고 자동화되므로 해당 컨테이너의 신규 앱을 보안 정책에 수동으로 추가할 필요가 없습니다.

   표시된 특정 앱만 추가하면 선택한 애플리케이션만 애플리케이션 그룹에 추가됩니다. 동일한 컨테이너 앱의 새 애플리케이션이 방화벽에 도착하면 애플리케이션 그룹이 이를 제어하지 않으며 신규 앱을 처리하는 방법을 수동으로 결정해야 합니다.
5. 경우에 따라 애플리케이션 그룹에 배치하려는 애플리케이션이 작동하려면 다른 애플리케이션이 필요합니다(의존). 이러한 경우 복제된 규칙 생성 대화 상자에 종속 애플리케이션이 포함되며, 여기서

 ©2023 Palo Alto Networks, Inc.

해당 애플리케이션을 복제된 규칙에 추가할지의 여부를 선택할 수 있습니다. 종속 애플리케이션을 규칙에 추가하여 선택한 애플리케이션이 제대로 작동하는지 확인합니다.



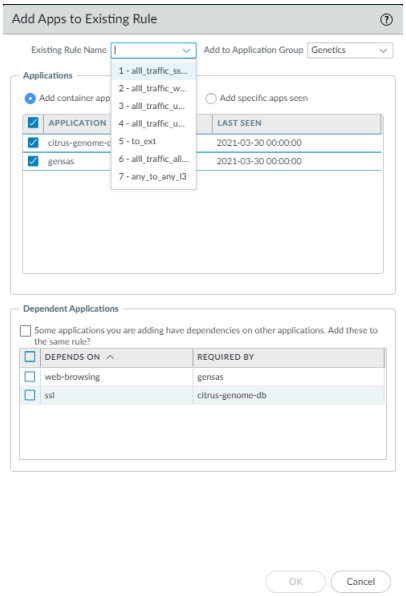

6. 확인을 클릭하여 새 애플리케이션 또는 기존 애플리케이션 그룹에 애플리케이션을 추가합니다.
7. 변경 사항을 커밋합니다.

기존 규칙에 앱 추가:

1. 기존 규칙 이름을 선택하여 선택한 애플리케이션을 애플리케이션 그룹의 기존 규칙에 추가합니다.
2. 애플리케이션 그룹에 추가에서 애플리케이션 그룹을 선택하거나 새 애플리케이션 그룹의 이름을 입력합니다.
3. 규칙 복제와 마찬가지로 컨테이너 앱 추가 또는 표시된 특정 앱 추가 여부를 선택할 수 있습니다. 컨테이너 앱을 추가하면 컨테이너의 모든 기능 앱과 해당 컨테이너에 추가되는 향후 앱이 모두 추가됩니다. 특정 앱만 추가하면 선택한 특정 앱만 추가됩니다.
4. 규칙 복제와 마찬가지로 경우에 따라 애플리케이션 그룹에 배치하려는 애플리케이션이 작동하려면 다른 애플리케이션이 필요합니다(상호 보완). 이러한 경우 기존 규칙에 앱 추가 대화 상자에 종속 애플리케이션이 포함되며, 여기서 해당 애플리케이션을 복제된 규칙에 추가할지의 여부를 선택할 수


©2023 Palo Alto Networks, Inc.

있습니다. 종속 애플리케이션을 규칙에 추가하여 선택한 애플리케이션이 제대로 작동하는지 확인합니다.




5. 확인을 클릭하여 새 애플리케이션 또는 기존 애플리케이션 그룹에 애플리케이션을 추가합니다.
6. 변경 사항을 커밋합니다.

## 정책 최적화 프로그램을 사용하여 규칙에 직접 앱 추가

정책 최적화 프로그램을 사용하여 복제된 규칙 또는 기존 규칙에 앱 ID Cloud Engine(ACE 및/또는 콘텐츠 제공 앱 ID)를 직접 추가할 수 있습니다. 그러나 애플리케이션 필터를 사용하여 ACE 앱 ID가 방화벽에 도달하면 수동으로 추가하는 대신 보안 정책에 자동으로 추가하는 것이 좋습니다.

***ACE***는 이전에 ***ssl***, 웹 브라우징, 알 수 없는 ***tcp*** 또는 알 수 없는 ***UDP***로 식별된 애플리케이션에 대한 앱 ***ID***를 제공합니다.

**STEP 1 |** 정책 > 보안으로 이동한 다음정책 최적화 프로그램 > 신규 앱 뷰어를 선택합니다.

방화벽 또는 Panorama가 ACE App-ID를 다운로드한 경우 왼쪽 탐색 창의 신규 앱 뷰어 옆에 숫자가 표시됩니다. 화면에 다운로드한 클라우드 앱 ID와 일치하는 보안 정책 규칙이 표시됩니다.

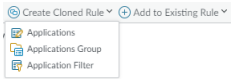
**STEP 2 |** 애플리케이션 및 사용 대화 상자에서 규칙과 일치하는 클라우드 제공 애플리케이션을 보려면 보안 정책 규칙에 대해 표시되는 앱에서 숫자를 클릭합니다.

**STEP 3 |** 기존 또는 복제된 보안 정책 규칙에 추가할 애플리케이션을 선택합니다.

하위 카테고리, 위험, 지난 30일 동안 본 트래픽 양 또는 애플리케이션이 처음 또는 마지막으로 표시되었을 때 표시되는 **Apps**에서 애플리케이션을 정렬하고 필터링할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 애플리케이션을 처리하는 방법에 따라 복제된 규칙 생성 또는 기존 규칙에 추가에서 애플리케이션을 선택합니다.




복제된 규칙 생성을 사용하여 복제할 수 있는 최대 애플리케이션 수는 *1,000*개의 애플리케이션입니다. *1,000*개 이상의 애플리케이션이 다른 규칙으로 이동하는 경우 기존 규칙에 추가를 대신 사용합니다. 애플리케이션을 새 규칙으로 이동하려면 먼저 규칙을 만든 다음 (정책 > 보안) 정책 최적화 프로그램을 사용하여 규칙을 해당 규칙에 추가합니다.

**STEP 5 |** 복제된 규칙 또는 기존 규칙에 선택한 애플리케이션을 추가합니다.

복제된 규칙 생성:

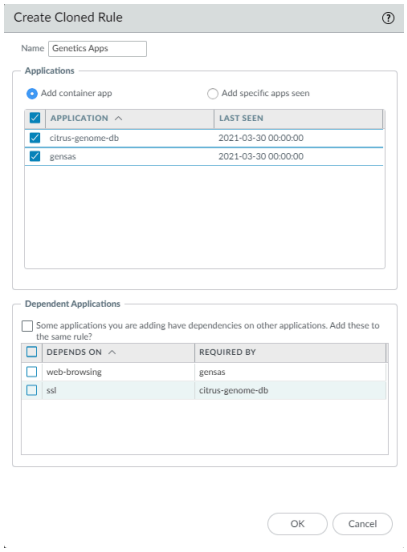
1. 이름(복제된 규칙의 이름으로, 원래 규칙 바로 상위의 보안 정책 규칙 베이스에 표시됨)을 입력합니다. 복제된 규칙에는 원래 규칙과 동일한 작업(허용 또는 거부)이 있습니다.
2. 컨테이너 앱 추가(기본값) 또는 표시된 특정 앱 추가만 선택할 수 있습니다.

   컨테이너 앱을 추가할 때 아직 방화벽에서 볼 수 없는 기능 앱을 포함하여 해당 컨테이너에 있는 모든 기능 앱도 추가합니다. 예를 들어 “페이스 북”컨테이너 앱을 추가하면 페이스 북 기반, 페이스 북 채팅, 페이스 북 게시 등과 컨테이너에 추가된 향후 애플리케이션이 추가됩니다. 컨테이너 및 해당 기능 앱에는 복제 중인 보안 정책 규칙이 적용됩니다. 컨테이너 앱을 선택하면 기본적으로 컨테이너의 앱에 대한 보안이 미래에도 보장되고 자동화되므로 해당 컨테이너의 신규 앱을 보안 정책에 수동으로 추가할 필요가 없습니다.

   표시된 특정 앱만 추가하면 선택한 애플리케이션만 복제된 규칙에 추가됩니다. 동일한 컨테이너 앱의 새 애플리케이션이 방화벽에 도착하면 복제된 규칙이 해당 애플리케이션을 제어하지 않으므로 신규 앱을 처리하는 방법을 수동으로 결정해야 합니다.
3. 경우에 따라 규칙에 추가하려는 애플리케이션이 작동하려면 다른 애플리케이션에 의존해야 합니다. 이러한 경우 복제된 규칙 생성 대화 상자에 종속 애플리케이션이 포함되며, 여기서 해당 애플리

 ©2023 Palo Alto Networks, Inc.

케이션을 복제된 규칙에 추가할지의 여부를 선택할 수 있습니다. 종속 애플리케이션을 규칙에 추가하여 선택한 애플리케이션이 제대로 작동하는지 확인합니다.



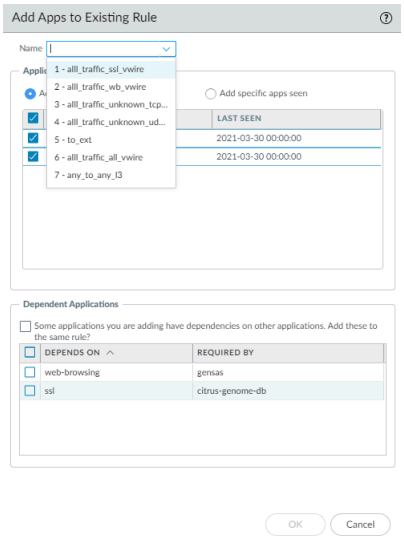

4. 확인을 클릭하여 복제된 규칙에 애플리케이션을 추가합니다.
5. 변경 사항을 커밋합니다.

기존 규칙에 앱 추가:

1. 선택한 애플리케이션을 추가할 기존 규칙의 이름을 선택합니다.
2. 애플리케이션을 추가하기 위해 규칙을 복제하는 것과 마찬가지로 컨테이너 앱 추가 또는 표시된 특정 앱 추가 중에서 선택할 수 있습니다. 컨테이너 앱을 추가하면 컨테이너의 모든 기능 앱과 해당 컨테이너에 추가되는 향후 앱이 모두 추가됩니다. 특정 앱만 추가하면 선택한 특정 앱만 추가됩니다.
3. 규칙 복제의 경우와 마찬가지로 규칙에 추가하려는 애플리케이션이 작동하려면 다른 애플리케이션에 의존해야 하는 경우도 있습니다. 이러한 경우 기존 규칙에 앱 추가 대화 상자에 종속 애플리케이


©2023 Palo Alto Networks, Inc.

션이 포함되며, 여기서 해당 애플리케이션을 복제된 규칙에 추가할지의 여부를 선택할 수 있습니다. 종속 애플리케이션을 규칙에 추가하여 선택한 애플리케이션이 제대로 작동하는지 확인합니다.




4. 확인을 클릭하여 기존 규칙에 애플리케이션을 추가합니다.
5. 변경 사항을 커밋합니다.

## RMA 방화벽(ACE) 교체

RMA(Return Merchandise Authorization)가 있는 경우 관리 방화벽에서 구성을 복원하려면 다음 절차를 따르십시오.

- RMA 방화벽 교체를 시작하기 전에 검토하십시오.
- Panorama에서 이전 방화벽의 일련번호를 새 방화벽의 일련번호로 바꿉니다.
- 방화벽 CLI에서 방화벽이 온라인 상태이고 Knowledge Service에 연결되어 있는지 확인하여 방화벽이 클라우드 애플리케이션 카탈로그를 다운로드할 수 있도록 합니다.

  1. 방화벽 CLI에 액세스합니다.
  2. 운영 모드에서 클라우드 App-ID 연결을 확인합니다.

     ```
     admin@vm1> show cloud-appid connection-to-cloud
     ```

     방화벽이 클라우드에 연결되어 있는 경우 show 명령은 다음을 반환합니다.

     ```
     ACE Cloud server: kcs.ace.tpcloud.paloaltonetworks.com:443Cloud connection: connected
     ```

     연결에 대한 정보도 표시됩니다. 방화벽이 클라우드에 연결되어 있지 않으면 DNS 서비스가 작동하는지 확인하고 다른 네트워크 관련 연결 문제가 있는지 확인합니다.
- 방화벽이 App-ID 클라우드에 연결된 상태에서 교체 후 방화벽 구성을 복원합니다.

## 라이선스 만료 또는 비활성화 ACE의 영향

방화벽에서 APP-ID 클라우드 엔진(ACE)을 사용하도록 설정하고, ACE 앱-ID를 방화벽에 다운로드한 다음 애플리케이션 필터 및 보안 정책 규칙과 같은 개체에서 해당 앱 ID를 사용하는 경우 SaaS 보안 인라인


©2023 Palo Alto Networks, Inc.

라이선스가 만료되거나 ACE를 사용하지 않도록 설정하는 경우 어떻게 되는지 이해해야 합니다. 에이스와 SaaS 보안 인라인 라이선스가 만료되는 비활성화는 다운로드한 ACE App-ID, ACE App-ID 카탈로그, ACE App-ID를 제어하는 보안 정책 규칙 및 ACE App-ID를 포함하는 개체에 영향을 미칩니다. 달리 명시되지 않는 한 효과는 동일합니다.

- ACE 앱-ID는 방화벽에 남아 있지만 방화벽은 보안 정책에 ACE 앱-ID를 적용하는 것을 중지합니다.

  ACE 앱-ID를 제어하는 보안 정책 규칙은 규칙에 표시되어 있더라도 더 이상 ACE 앱-ID를 제어하지 않습니다. SSL, 웹 브라우징, 알 수 없는 tcp 또는 방화벽에서 ACE가 활성화되기 전에 알 수 없는 udp 규칙에 의해 제어된 트래픽은 SaaS 보안 인라인 라이선스및 활성화 및/또는 ACE를 활성화하거나 이러한 규칙을 변경할 때까지 해당 규칙에 의해 다시 제어됩니다.
- ACE App-IDs에 기반한 보안 정책 규칙의 시행은 라이선스 만료 후 4-6시간 이내에 중지됩니다(라이선스 상태를 주기적으로 확인하는 타이머 기준).

  ACE 앱-ID를 기반으로 하는 보안 정책 규칙의 적용은 방화벽에서 비활성화된 ACE를 커밋한 직후에 중지됩니다.

  > ***SaaS*** 보안 인라인 라이선스가 여전히 유효하고 활성 상태인 경우에도 ***ACE*** 앱-***ID***를 기반으로 보안 정책 규칙 적용을 중지합니다.
- ACE 앱-ID 카탈로그는 방화벽과 Panorama에 남아 있지만 클라우드 엔진은 더 이상 카탈로그를 업데이트하지 않습니다.
- 방화벽에서 ACE로의 연결은 더 이상 작동하지 않습니다. ACE를 다시 활성화하거나 SaaS 보안 인라인 라이선스를 갱신하는 경우 모든 카탈로그 업데이트를 다운로드하는 데 시간이 걸릴 수 있습니다.
- SaaS 보안 인라인 라이선스가 만료되면 ACE 서비스는 4-6시간 이내에 작동을 중지합니다.

  > ***Panorama***는 ***SaaS*** 보안 인라인 라이선스가 필요하지 않으므로 ***Panorama***에서 만료할 수 있는 라이선스가 없습니다. 그러나 관리되는 방화벽에서 라이선스가 만료되면 보안 정책 또는 애플리케이션 그룹에 ***ACE*** 구성이 포함된 경우 ***Panorama***에서 해당 방화벽으로 구성이 실패합니다.
- 애플리케이션 필터 및 애플리케이션 그룹과 같은 개체는 변경되지 않지만 ACE 앱-ID가 여전히 표시되어 있더라도 해당 개체에 배치한 ACE App-ID는 더 이상 적용되지 않습니다.
- SaaS 정책 권장 사항을 사용하는 경우 방화벽은 더 이상 SaaS 정책 권장 사항을 가져올 수 없으므로 SaaS 관리자는 새 정책 권장 사항을 방화벽에 푸시할 수 없습니다. 라이선스 만료 전에 다운로드된 정책 권장 사항은 구성에 남아 있지만 적용되지는 않습니다(라이선스가 만료되거나 ACE가 비활성화된 경우 ACE App-ID로 구성된 보안 정책과 동일한 동작).

## 클라우드 콘텐츠 롤백으로 인한 커밋 실패

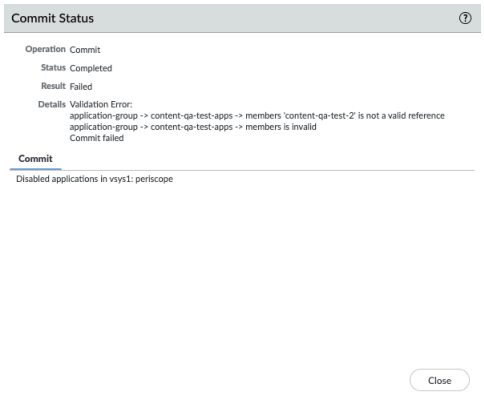
가능성은 매우 낮지만 잘못된 메타데이터나 애플리케이션 문제로 인해 ACE App-ID를 롤백(되돌리기)해야 할 수도 있습니다. ACE가 App-ID를 되돌려야 하고 보안 정책 규칙(직접 또는 애플리케이션 그룹)에서 해당 App-ID를 사용한 경우 해당 애플리케이션이 보안 정책 규칙 및 개체에서 제거될 때까지 커밋 작업이 실패합니다.

App-ID를 롤백해야 하는 경우 ACE는 ACE 카탈로그에서 가장 최근에 제공된 클라우드 기반 App-ID, 서명, 메타데이터, 카테고리, 하위 카테고리 및 태그를 모두 되돌립니다. 카탈로그에서 App-ID를 제거하면 방화벽에서 제거되므로 App-ID가 보안 정책에서 사용될 때 커밋 작업이 실패합니다.


©2023 Palo Alto Networks, Inc.

보안 정책에서 *ACE*가 롤백해야 했던 애플리케이션을 사용하지 않은 경우 구성에 영향을 주지 않고 커밋 작업이 성공합니다.

ACE 콘텐츠 롤백 후 구성을 커밋하려고 하면 커밋 실패 메시지에 ACE가 되돌린 애플리케이션이 나열됩니다(예: 유효성 검사 오류).




문제를 해결하려면 규칙에 직접 추가되었는지 또는 애플리케이션 그룹을 사용하여 추가되었는지에 관계없이 나열된 애플리케이션을 보안 정책 규칙에서 제거해야 합니다. 애플리케이션이 애플리케이션 그룹에서 사용되는 경우 애플리케이션 그룹에서 제거합니다.

이 예에서 **content-qa-test-2**는 애플리케이션 그룹 **content-qa-test-apps**에서 참조되는 복구된 애플리케이션입니다. 애플리케이션 그룹에서 **content-qa-test-2**를 제거하면 커밋 작업이 성공합니다.

## App-ID Cloud Engine 문제 해결

이 항목에서는 ACE(App-ID Cloud Engine)에 대한 일반적인 문제 해결 정보를 제공합니다.

- 어플라이언스에 유효한 SaaS 보안 인라인 라이선스가 있는지 확인하려면 작동 CLI 명령 **show cloud-appid connection-to-cloud**를 실행하십시오. 문제가 있는 경우 명령은 다음 메시지를 반환합니다.

  **ACE 오류: 라이선스 확인에 실패했습니다. SaaS 라이선스가 설치되어 있는지 확인하고 activeCloud 연결: 실패**

  또한 출력에는 마지막으로 성공한 연결 시간이 표시됩니다. 예를 들면 다음과 같습니다. **마지막으로 성공한 gRPC 연결: 2021-05-20 16:00:00 -0800 PDT**

  라이선스가 설치되어 있고 ACE에 대한 연결이 양호하면 이 명령은 ACE 클라우드 서버 연결에 대한 URL 및 상태 **클라우드 연결: 연결됨**과 함께 연결 통계 및 인증서 유효 날짜를 포함한 디바이스 인증서 상태를 반환합니다.
- 관리 방화벽에 대한 Panorama commit all/push가 실패합니다. 다음 조건 중 하나라도 존재하는지 확인하고 수리하십시오.
  - 관리 방화벽에 유효한 SaaS 보안 인라인 라이선스가 있습니까? 그렇지 않은 경우 ACE 카탈로그가 없고 모두 커밋/푸시 작업이 실패합니다. 관리 방화벽이 ACE App-ID를 처리하도록 할지의 여부에


©2023 Palo Alto Networks, Inc.

따라 푸시된 구성에서 ACE 개체를 제거하고 다시 시도하거나 관리 방화벽에 유효한 SaaS 보안 인라인 라이선스를 설치하고 카탈로그가 다운로드될 때까지 기다리십시오.

콘텐츠 제공 ***App-ID***는 ***4,000***개 미만입니다. ***ACE*** 카탈로그를 다운로드하면 방화벽에 수천 개의 추가 애플리케이션이 표시되며 ***Objects*** > ***Applications***를 확인하거나 운영 ***CLI*** 명령 ***show cloud-appid cloud-app-data application all***을 사용하여 새로운 ***App-ID***를 확인하여 확인할 수 있습니다.

- 관리 방화벽과 ACE 간의 연결이 끊어졌습니까? ACE 클라우드에 대한 연결을 확인하고 필요한 경우 연결을 복원하십시오.

  운영 CLI 명령 **show cloud-appid connection-to-cloud**는 클라우드 연결 상태 및 ACE 클라우드 서버 URL을 제공합니다.

- Panorama의 ACE 카탈로그와 관리 방화벽의 ACE 카탈로그가 동기화되지 않아 방화벽 카탈로그에 없는 ACE 앱이 포함된 구성이 푸시됩니다. 방화벽과 ACE 간의 연결이 설정되어 있으면 몇 분 안에 오래된 카탈로그가 자동으로 업데이트되어 문제를 해결합니다. (5분 정도 기다렸다가 다시 시도하십시오.)

  운영 ***CLI*** 명령 ***debug cloud-appid cloud-manual-pull check-cloud-app-data***를 실행하여 카탈로그를 수동으로 업데이트할 수도 있습니다.

- 방화벽이 모두 PAN-OS 10.2 이상을 실행하고 있습니까? (ACE 애플리케이션 및 개체를 참조하는 구성을 PAN-10 10.2 이전 버전을 실행하는 방화벽으로 푸시하는 것은 허용되지 않습니다.)

- ACE 구성이 있는 HA 쌍(능동형/능동형 또는 능동형/수동형)에서 **show session all** 또는 **show session id <id>** 운영 명령을 실행하면 ACE 애플리케이션의 출력에 전역 App-ID 번호가 애플리케이션 이름 대신 표시될 수 있습니다. 방화벽은 데이터 플레인에 클라우드 애플리케이션 데이터가 있는 경우에만 애플리케이션 이름을 표시합니다. 그렇지 않은 경우 방화벽은 대신 애플리케이션에 대한 전역 App-ID 번호를 표시합니다.
- ACE(gRPC 연결)에 대한 연결을 재설정하려면 운영 CLI 명령 **debug cloud-appid reset connection-to-cloud**를 실행합니다.
- 작동 CLI 명령 **show cloud-appid cloud-app-data application**을 사용하여 어플라이언스에 다운로드된 ACE 애플리케이션을 봅니다. 다운로드한 모든 앱 또는 개별 앱을 App-ID 또는 애플리케이션 이름으로 볼 수 있습니다.
- 작동 CLI 명령 **show cloud-appid signature-dp pending-request**를 사용하여 ACE App-ID에 대한 보류 중인 요청을 봅니다. 출력에는 방화벽이 ACE에 요청을 보낸 횟수(시도)가 포함됩니다. 11번의 시도 후에 보내기 작업이 타임아웃됩니다.
- 운영 CLI 명령 **show cloud-appid**에는 더 유용한 옵션이 있습니다.

```
관리자 @PAN -ACE-VM-1> 클라우드 앱을 보여줄까요?> app-objects-in-
policy 정책에서 참조한 애플리케이션 필터/애플리케이션 그룹 표시 > 앱-필터그
룹-매핑 > 일치하는 필터 및 그룹에 애플리케이션 표시 > 애플리케이션 UI용 애플
리케이션 정보 표시 > 애플리케이션 필터 > 애플리케이션 필터에 클라우드 앱 표시
 > 애플리케이션 그룹 클라우드 앱 표시애플리케이션 그룹에서 > 클라우드 애플리
케이션 데이터 > 클라우드 애플리케이션, 컨테이너 및 메타데이터 표시 > 클라우드
에 연결 > 클라우드 애플리케이션 서버에 gRPC 연결 상태 표시 > ha-info 클라우
드 애플리케이션 고가용성 통계 표시 > overlap-appid 사전 정의된 콘텐츠로 중
복 애플리케이션 표시 >signature-dp DP에서 사용된 클라우드 서명 및 애플리케이
```


©2023 Palo Alto Networks, Inc.

```
션 표시 > 작업 관리 플레인에서 작업 표시 > 트랜잭션 클라우드 애플리케이션 트랜
잭션 표시 > 버전 Cloud-AppID 버전 표시
```

- ACE의 전역 카운터를 보려면 작동 CLI 명령 **show counter global filter value all category cad**(**cad**는 "cloud app-identification"을 나타냄)를 실행합니다.
- ACE, DLP 및 IoT와 같은 서비스에 대해 공유 메모리와 주고받는 바이트 및 패킷에 대한 통계를 확인하려면 **show ctd-agent statistics**를 실행합니다.
- 사용자 인터페이스에서 볼 때와 CLI에서 볼 때 애플리케이션 필터와 일치하는 애플리케이션 수 사이에 불일치가 있는 경우 이는 방화벽이 사용자 인터페이스와 CLI에서 일치하는 애플리케이션을 계산하는 방식 때문입니다.
  - **Objects** > **Application Filters**의 애플리케이션 필터를 보면 방화벽이 실제로 해당 애플리케이션을 보고 해당 App-ID를 다운로드했는지의 여부와 관계없이 방화벽이 ACE 카탈로그에서 일치하는 모든 애플리케이션을 표시하며 개수에는 해당 애플리케이션이 모두 포함됩니다.
  - **show cloud-appid application-filter** 작동 명령을 사용하여 CLI에서 애플리케이션 필터를 보면 방화벽은 방화벽이 ACE App-ID를 다운로드한 일치하는 애플리케이션의 수만 표시합니다.

  이러한 이유로 사용자 인터페이스는 동일한 애플리케이션 필터에 대해 CLI보다 일치하는 애플리케이션을 더 많이 표시할 수 있습니다.

  > ***CLI*** 대 사용자 인터페이스에서 애플리케이션 그룹을 볼 때 동일한 사항이 애플리케이션 그룹에 적용됩니다.

- ACE App-ID는 보안 정책에 대해서만 지원됩니다. ACE App-ID는 다른 정책 유형에 대해 지원되지 않습니다.

  그러나 QoS 또는 SD-WAN 정책을 구성할 때 ACE App-ID가 표시되고(선택 가능) 규칙에 적용된 애플리케이션 그룹 또는 애플리케이션 필터에 있을 수 있지만 QoS 또는 SD-WAN 정책에 추가하면 애플리케이션 트래픽에 영향을 미치지 않습니다. (QoS 및 SD-WAN 정책은 애플리케이션 트래픽을 제어하지 않습니다.)


©2023 Palo Alto Networks, Inc.

# SaaS 앱 ID 정책 추천

SaaS 애플리케이션의 급증으로 인해 모든 애플리케이션에 특정 앱 ID를 할당하고, 해당 애플리케이션에 대한 가시성을 확보하고, 이를 제어하기가 어렵습니다. SSL, 웹 브라우징 또는 "모든" 애플리케이션을 허용하는 보안 정책 규칙은 네트워크에 보안 위험을 초래할 수 있는 승인되지 않은 SaaS 애플리케이션을 허용할 수 있습니다. 이러한 애플리케이션에 대한 가시성을 확보하고 방화벽에서 이를 제어하기 위해 SaaS 보안 관리자는App-ID 클라우드 엔진(ACE)에서 제공하는 특정 SaaS 앱 ID가 포함된 보안 정책 규칙을 PAN-OS 방화벽 관리자에게 추천할 수 있습니다. PAN-OS 관리자는 SaaS 보안 인라인 구독이 있는 방화벽에서 이러한 규칙을 가져올 수 있습니다.

***SaaS*** 정책 권장 사항은 SaaS 보안 인라인 구독이 필요합니다 ***SaaS*** 정책 권장 엔진을 사용하는 각 어플라이언스는 유효한 디바이스 인증서를 생성 및 설치하거나 Panorama를 사용하여 유효한 디바이스 인증서를 생성 및 설치해야 합니다.

***SaaS*** 가시성을 위해 ***Cortex Data Lake(***CDL***)***에 대한 SaaS 보안 인라인 연결이 필요합니다. ***CDL***로 로그 포워딩을 구성하고 보안 정책 규칙에서 올바른 로그 포워딩 프로파일을 사용하여 로그 포워딩을 사용하도록 설정합니다. ***SaaS Security Inline***이 제대로 작동하려면 최소한 트래픽 로그와 ***URL*** 로그를 ***CDL***로 포워딩해야 합니다.

***PAN-OS 10.2*** 이상을 지원하는 모든 하드웨어 플랫폼은 ***SaaS*** 정책 권장 사항을 지원하고 ***SaaS*** 정책 권장 사항을 사용하려는 모든 어플라이언스는 ***PAN-OS 10.2*** 이상이 필요합니다. ***Panorama***는 ***SaaS*** 보안 인라인 라이선스가 설치되어 있지 않은 방화벽이나 ***10.1***보다 이전 버전의 ***PAN-OS***를 실행하는 방화벽으로 ***SaaS*** 정책 권장 사항을 푸시하고 커밋할 수 없습니다.

- ***SaaS*** 보안 관리자 가이드에서는 보안 정책 규칙 권장 사항을 만든 다음 방화벽에 푸시하는 SaaS 보안 관리자의 절차에 대해 설명합니다.
- ***PAN-OS*** 관리자 안내서에서는 PAN-OS 관리자가 SaaS 보안 관리자로부터 정책 권장 사항을 가져오고 관리하는 방법에 대해 설명합니다.

SaaS 보안 관리자는 새 규칙을 생성하고 애플리케이션, 사용자 및 그룹을 규칙에 추가하고 규칙 작업을 설정합니다. 규칙 작업은 허용 또는 차단이 될 수 있습니다. 푸시된 규칙에 대해 다른 작업은 허용되지 않습니다. 그런 다음 SaaS 보안 관리자가 해당 어플라이언스에 규칙을 푸시하면 방화벽 인터페이스(디바이스 > 정책 권장 사항 > **SaaS**)에 규칙이 나타납니다.

PAN-OS 관리자는 권장 규칙을 평가하고 방화벽에 구현할지의 여부를 결정합니다. PAN-OS 관리자가 규칙을 구현하기로 선택한 경우 관리자는 이 규칙을 방화벽으로 가져오고 방화벽 규칙베이스에서 정책 규칙을 배치할 위치를 선택합니다. PAN-OS 관리자가 정책 권장 사항을 가져오면 방화벽이 필요한 HIP 프로파일, 태그 및 애플리케이션 그룹을 자동으로 생성합니다(PAN-OS 관리자는 수동으로 수행할 필요가 없음).

***SaaS*** 보안 관리자가 정책 권장 사항과 함께 보안 프로파일을 푸시하고 해당 프로파일이 방화벽에 없으면 방화벽 가져오기가 실패합니다. 프로파일이 이미 방화벽에 있는 경우 가져오기가 성공합니다.


©2023 Palo Alto Networks, Inc.

SaaS 보안 관리자가 정책 규칙 권장 사항을 업데이트하면 PAN-OS 관리자가 업데이트를 확인하고 방화벽으로 가져옵니다. SaaS 보안 관리자가 정책 규칙 권장 사항을 삭제하면 PAN-OS 관리자는 작업을 보고 방화벽 보안 정책 규칙 기준에서 규칙을 삭제합니다.

***SaaS Security*** 인라인 라이선스가 만료되면 방화벽이 더 이상 ***SaaS*** 정책 권장 사항을 가져오지 않으므로 새로운 권장 사항이 표시되지 않습니다. 그러나 이미 불러온 보안 정책 규칙은 계속 작동합니다.

***ACE***를 사용하지 않도록 설정하면 방화벽이 더 이상 새 클라우드 애플리케이션 서명 및 앱 ***ID***를 받지 않으며 방화벽이 새 ***ACE*** 앱 ***ID***를 기반으로 ***SaaS*** 정책 권장 사항을 가져올 수 없습니다.

ACE 배포 프로세스(클라우드에 연결, 디바이스 인증서 설치, SaaS 보안 포털에서 라이선스 활성화 및 Panorama 및 방화벽으로 푸시 등)도 SaaS 정책 권장 사항을 설정합니다.

모든 어플라이언스를 최신 위협 콘텐츠 업데이트로 업데이트합니다.

이 새로운 기능에 대한 사용자 인터페이스 추가 사항은 다음과 같습니다.

- 디바이스 > 정책 권장 사항 > **SaaS**는 SaaS 관리자의 정책 권장 사항을 표시하고 방화벽 관리자가 권장 SaaS 정책을 가져오고, 업데이트하고, 제거하고, 제어할 수 있도록 합니다. 이 페이지에는 정책에 대해 SaaS 관리자가 구성한 애플리케이션 그룹이 포함됩니다.
- 역할 기반 인터페이스 액세스(디바이스 > 관리자 역할)에는 SaaS 정책 권장 사항 권한에 대한 웹 **UI** 탭에 새로운 옵션이 추가되었습니다. 디바이스 > 정책 권장 사항 > **SaaS**.
- SaaS 정책 권장 사항은 인터페이스의 태그 열에 표시되는 **SaaSecurity** 권장 태그가 자동으로 지정됩니다.

SaaS 관리자가 푸시한 SaaS 정책 권장 사항을 가져오고 업데이트하고 SaaS 관리자가 삭제한 SaaS 정책 권장 사항을 제거할 수 있습니다.

- SaaS 정책 추천 가져오기
- 업데이트된 SaaS 정책 권장 사항 가져오기
- 삭제된 SaaS 정책 권장 사항 제거

## SaaS 정책 추천 가져오기

SaaS 보안 관리자가 보안 정책 규칙 권장 사항을 PAN-OS 방화벽에 푸시하면 PAN-OS 방화벽 관리자는 방화벽에서 해당 규칙을 가져와 정책 권장 사항의 애플리케이션에 대한 가시성과 제어 권한을 얻을 수 있습니다.

SaaS 관리자의 정책 권장 사항 및 푸시 절차는 ***SaaS*** 보안 관리자 가이드를 참조하십시오. 이 절차는 PAN-OS 관리자가 정책 권장 사항을 가져오는 방법을 보여줍니다.

***SaaS*** 보안 관리자가 정책 권장 사항과 함께 보안 프로파일을 푸시하고 해당 프로파일이 방화벽에 없으면 방화벽 가져오기가 실패합니다. 프로파일이 이미 방화벽에 있는 경우 가져오기가 성공합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 디바이스 > 정책 권장사항 > **SaaS** 및 **Panorama** > 정책 권장사항 > **Panorama**의 **SaaS**에는 SaaS 관리자가 푸시한 모든 SaaS 정책 권장 사항이 표시됩니다. Panorama에서 관리 방화벽으로 정책 권장 사항을 푸시합니다.

**STEP 2 |** 새로 고침( ) 디바이스 > 정책 권장 사항 > **SaaS**(또는 **Panorama** > 정책 권장 사항 > **SaaS**) SaaS 정책 권장 사항이 최신 상태인지 확인합니다.

> *Panorama*에서 관리되는 방화벽으로 정책 권장 사항을 푸시할 때마다 방화벽의 페이지를 새로고침( )하여 권장 사항이 최신 상태인지 확인하십시오.

새로 푸시된 정책 권장 사항이 화면 상단에 나타납니다. 활성 권장 사항은 활성 값을 표시하고 사용 가능한 새 업데이트는 예 값을 표시합니다.

**STEP 3 |** 새 정책 권장 사항을 선택합니다.

한 번에 하나의 정책 권장 사항을 가져옵니다. 애플리케이션 열에는 각 정책 권장 사항에 대한 애플리케이션 그룹이 표시됩니다. 그룹 이름을 클릭하면 해당 그룹의 애플리케이션을 볼 수 있습니다.

디바이스 열에는 SaaS 관리자가 규칙에 대해 구성한 소스 디바이스가 표시됩니다. "SaaS"라는 용어는 소스 디바이스 앞에 옵니다. 소스 디바이스는 다음과 같을 수 있습니다.

- MCD - 관리되는 호환 디바이스
- MNCD - 관리되는 비준수 디바이스
- UMCD - 관리되지 않는 호환 디바이스
- UMNCD - 관리되지 않는 비준수 디바이스

예를 들어 **SaaS - MCD**는 관리되는 규정 준수 소스 디바이스를 나타냅니다.

**STEP 4 |** 가져오기 정책 규칙.

정책 규칙 가져오기 대화 상자에서:

- 이름 - 규칙의 의도를 설명하는 이름을 사용하여 불러온 규칙의 이름을 지정합니다.

  > 보안 정책 규칙 베이스에 이미 있는 규칙 이름을 지정하면 불러온 규칙이 기존 규칙을 덮어씁니다.

- 사후 규칙 - 불러온 SaaS 규칙을 배치할 규칙을 선택합니다. 방화벽의 규칙 베이스와 새 규칙이 기존 규칙에 어떤 영향을 미칠 수 있는지 생각해 보십시오. 규칙을 선택하지 않으면(규칙 미선택) 규칙은 보안 정책 규칙 베이스의 맨 위에 배치됩니다. 경우에 따라 규칙을 배치할 위치가 아닙니다. 예를 들어 QUIC 프로토콜 차단과 같이 특정 차단 규칙이 항상 규칙 베이스의 맨 위에 있기를 원할 수 있습니다. 불러온 규칙의 의도를 인식하고 기존 규칙을 섀도잉하지 않도록 주의하십시오.

설명은 SaaS 관리자가 규칙을 생성할 때 입력한 설명에서 가져옵니다. 변경하거나 그대로 둘 수 있습니다.

> 가져오기 프로세스는 정책 권장 사항의 애플리케이션에 대한 애플리케이션 그룹을 자동으로 생성합니다. 애플리케이션 그룹의 이름은 ***SaaS*** 보안 관리자가 규칙에 부여한 이름에서 파생됩니다. 방화벽은 또한 ***SaaS*** 관리자가 규칙에 적용한 모든 ***HIP*** 프로파일 및 태그를 자동으로 생성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 확인을 클릭하여 규칙을 가져와서 사후 규칙에서 선택한 위치의 보안 정책 규칙 베이스에 추가합니다.

**STEP 6 |** "보안 정책 규칙을 성공적으로 업데이트했습니다"라는 상태 메시지가 표시되면 확인을 클릭합니다.

이제 위치 열에 방화벽의 규칙 위치(vsys)가 표시되며, 이는 SaaS 관리자가 규칙을 푸시한 vsys에 해당합니다.

**STEP 7 |** 가져온 정책 규칙이 지정된 위치의 보안 정책 규칙 베이스(보안 > 정책)에 있고 방화벽이 연결된 개체를 생성했는지 확인합니다.

예를 들어 다음에 대한 보안 정책 규칙을 확인합니다.

- 규칙의 소스 디바이스가 채워지고 소스 탭에 규칙에 대한 소스 디바이스가 표시됩니다.
- 애플리케이션 그룹은 규칙의 애플리케이션 탭을 채웁니다.
- 연결된 프로파일이 규칙(작업 탭)에 연결됩니다.

또한 다음을 확인하십시오.

- 개체 > 애플리케이션 그룹에는 불러온 애플리케이션 그룹이 표시됩니다.
- **Objects** > **GlobalProtect** > **HIP** 개체 및 **Objects** > **GlobalProtect** > **HIP** 프로파일은 규칙을 사용하여 SaaS 보안 관리자가 푸시한 HIP 정보를 표시합니다.

## 업데이트된 SaaS 정책 권장 사항 가져오기

SaaS 보안 관리자가 보안 정책 규칙 권장 사항을 PAN-OS 방화벽(또는 Panorama)에 푸시하면 PAN-OS 관리자는 해당 규칙을 가져와 정책 권장 사항의 애플리케이션에 대한 가시성과 제어를 얻을 수 있습니다. 그러나 SaaS 관리자가 예를 들어 애플리케이션을 추가하거나 제거하여 규칙을 업데이트하는 경우 방화벽에서도 규칙을 업데이트해야 합니다.

*SaaS* 보안 관리자가 신규 또는 업데이트된 애플리케이션 그룹, *HIP* 프로파일 또는 태그를 푸시하면 방화벽이 자동으로 해당 개체를 생성하거나 업데이트합니다. *SaaS* 보안 관리자가 정책 권장 사항 업데이트로 보안 프로파일을 푸시하고 해당 프로파일이 방화벽에 없으면 방화벽 가져오기가 실패합니다. 프로파일이 이미 방화벽에 있는 경우 가져오기가 성공합니다.

**STEP 1 |** 새로 고침( ) 디바이스 > 정책 권장 사항 > **SaaS**(또는 **Panorama** > 정책 **Recommendation** > **SaaS**) SaaS 관리자가 방화벽에 푸시한 최신 SaaS 정책 권장 사항을 모두 볼 수 있습니다.

**STEP 2 |** 사용 가능한 새 업데이트를 확인합니다.

사용 가능한 새 업데이트 열의 값이 아니오이면 규칙에 대한 업데이트가 없는 것입니다. 값이 예이면 SaaS 관리자가 방화벽에 대한 규칙 업데이트를 푸시한 것입니다. 또한 활성 권장 사항은 활성 값을 표시합니다.

**STEP 3 |** 규칙이 제어하는 업데이트된 애플리케이션 목록을 보려면 애플리케이션 열에서 애플리케이션 그룹 이름을 클릭하십시오.

**STEP 4 |** 업데이트할 정책 권장 사항을 선택합니다.

한 번에 하나의 정책 권장 사항만 업데이트합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 정책을 가져오려면 정책 규칙 가져오기를 클릭합니다(규칙에 대한 업데이트가 없으면 이 옵션이 회색으로 표시되고 선택할 수 없음).

정책 규칙 가져오기 대화 상자가 나타납니다. 이름은 이미 채워져 있으며 규칙을 이미 가져왔기 때문에 변경할 수 없습니다. 대화 상자에서 규칙을 변경할 수도 없지만 보안 정책 규칙 베이스에서 규칙의 위치를 변경하려는 경우 보안 정책 규칙의 위치를 변경하는 것과 같은 방식으로 **Policies** > **Security**에서 변경할 수 있습니다. 설명을 변경하거나 그대로 둘 수 있습니다.

**STEP 6 |** 확인을 클릭합니다.

**STEP 7 |** 변경 확인에서 예를 클릭하여 업데이트된 규칙을 가져옵니다(또는 변경된 규칙을 가져오지 않으려면 아니오를 클릭).

방화벽은 애플리케이션 그룹, HIP 프로파일 및 규칙과 연결된 태그를 자동으로 변경합니다.

## 삭제된 SaaS 정책 권장 사항 제거

SaaS 보안 관리자가 보안 정책 규칙 권장 사항을 PAN-OS 어플라이언스에 푸시하면 PAN-OS 관리자는 이러한 규칙을 가져와 정책 권장 사항에서 애플리케이션을 보고 제어할 수 있습니다. 그러나 SaaS 보안 관리자가 규칙을 삭제하는 경우 PAN-OS 장비에서도 해당 규칙을 삭제해야 합니다.

SaaS Security 관리자가 규칙을 삭제하면 활성 권장 사항 열에 제거된 값이 표시됩니다(유효한 규칙의 경우 값이 활성 상태임).

**STEP 1 |** SaaS 보안 관리자가 제거한 규칙을 선택합니다. 한 번에 제거할 규칙을 하나만 선택할 수 있습니다.



규칙을 더 이상 가져올 수 없으므로 정책 규칙 가져오기 옵션이 회색으로 표시됩니다.

**STEP 2 |** 권장 사항 매핑 제거를 클릭합니다.

이렇게 하면 방화벽에서 보안 정책 규칙의 로컬 매핑이 제거됩니다. 예를 들어 위치, 사용자 및 규칙에 대한 매핑이 삭제됩니다. 권장 사항 매핑 제거 대화 상자에는 규칙이 제거된 위치를 알 수 있도록 규칙의 위치가 표시됩니다.

**STEP 3 |** 확인을 클릭합니다.

**STEP 4 |** 변경 확인 대화 상자에서 예를 눌러 정책 권장 사항 데이터베이스에서 규칙을 제거합니다.



이 작업은 정책 권장 사항 규칙 목록에서만 규칙을 제거합니다. 보안 정책 규칙 기준에서 규칙을 제거하지는 않습니다. 규칙베이스에서 규칙을 수동으로 제거해야 합니다.

**STEP 5 |** 정책 권장 사항 매핑이 제거되었음을 확인하는 상태 대화 상자가 나타나지만 보안 정책 규칙 기준에서 규칙을 제거해야 합니다.

**STEP 6 |** 정책 > 보안으로 이동하여 보안 정책 규칙 베이스에서 규칙을 삭제합니다.


©2023 Palo Alto Networks, Inc.

# 애플리케이션 수준 게이트웨이

Palo Alto Networks 방화벽은 포트 및 프로토콜별로 트래픽을 분류하지 않습니다. 대신 App-ID 기술을 사용하여 고유한 속성과 트랜잭션 특성을 기반으로 애플리케이션을 식별합니다. 그러나 일부 애플리케이션에서는 방화벽이 핀홀을 동적으로 열어 연결을 설정하고 세션 매개변수를 결정하며 데이터 전송에 사용할 포트를 협상해야 합니다. 이러한 애플리케이션은 애플리케이션 레이어 페이로드를 사용하여 애플리케이션이 데이터 연결을 여는 동적 TCP 또는 UDP 포트와 통신합니다. 이러한 애플리케이션의 경우 방화벽은 ALG(Application Level Gateway) 역할을 하며 제한된 시간 동안 데이터를 전송하거나 트래픽을 제어하기 위해 핀홀을 엽니다. 방화벽은 또한 필요할 때 페이로드의 NAT 재작성을 수행합니다.

- ***H.323(H.225* 및 *H.248) ALG***는 게이트키퍼 라우팅 모드에서 지원되지 않습니다.
- 방화벽이 ***SIP(Session Initiation Protocol)***에 대한 ***ALG*** 역할을 하는 경우 기본적으로 페이로드에서 ***NAT***를 수행하고 미디어 포트에 대한 동적 핀홀을 엽니다. 경우에 따라 환경에서 사용 중인 ***SIP*** 애플리케이션에 따라 ***SIP*** 엔드포인트에는 클라이언트에 내장된 ***NAT*** 인텔리전스가 있습니다. 이러한 경우 방화벽이 신호 세션을 수정하지 못하도록 ***SIP ALG*** 기능을 비활성화해야 할 수 있습니다. ***SIP ALG***가 비활성화된 경우 ***App-ID***에서 세션이 ***SIP***라고 판단하면 페이로드가 변환되지 않고 동적 핀홀이 열리지 않습니다. SIP ALG(애플리케이션 수준 게이트웨이) 비활성화를 참조하십시오.

***DIPP(동적 IP 및 포트) NAT***를 사용하는 경우 ***Palo Alto Networks*** 방화벽 ***ALG*** 디코더는 ***SIP*** 헤더(연락처 및 ***Via*** 필드) 아래에 ***IP*** 및 포트(***Sent-by Address*** 및 ***Sent-by Port***) 조합이 필요합니다. 언급된 헤더를 번역하고 이를 기반으로 예측 세션을 엽니다.

다음 표는 IPv4, NAT, IPv6, NPTv6 및 NAT64 ALG를 나열하고 ALG가 각 프로토콜(예: SIP)을 지원하는지의 여부를 확인 표시로 나타냅니다.

| App-ID | IPv4 | NAT | IPv6 | NPTv6 | NAT64 |
|---|---|---|---|---|---|
| SIP | ✓ | ✓ | ✓ | — | — |
| SCCP | ✓ | ✓ | ✓ | — | — |
| MGCP | ✓ | ✓ | — | — | — |
| FTP | ✓ | ✓ | ✓ | ✓ | — |
| RTSP | ✓ | ✓ | ✓ | ✓ | — |
| MySQL | ✓ | ✓ | — | — | — |
| Oracle/SQLNet/TNS | ✓ | ✓ | ✓ | ✓ | — |

 ©2023 Palo Alto Networks, Inc.

| App-ID | IPv4 | NAT | IPv6 | NPTv6 | NAT64 |
|---|---|---|---|---|---|
| RPC | ✓ | ✓ | — | — | — |
| RSH | ✓ | ✓ | — | — | — |
| UNIStim | ✓ | ✓ | — | — | — |
| H.225 | ✓ | ✓ | — | — | — |
| H.248 | ✓ | ✓ | — | — | — |


©2023 Palo Alto Networks, Inc.

# SIP 애플리케이션 수준 게이트웨이(ALG) 비활성화

Palo Alto Networks 방화벽은 SIP(Session Initiation Protocol) ALG(Application-level Gateway)를 사용하여 NAT가 활성화된 방화벽에서 동적 핀홀을 엽니다. 그러나 VoIP와 같은 일부 애플리케이션에는 클라이언트 애플리케이션에 NAT 인텔리전스가 내장되어 있습니다. 이러한 경우 방화벽의 SIP ALG가 신호 세션을 방해하여 클라이언트 애플리케이션의 작동을 중지할 수 있습니다.

이 문제에 대한 한 가지 솔루션은 SIP에 대한 애플리케이션 재정의 정책을 정의하는 것이지만 이 접근 방식을 사용하면 App-ID 및 위협 탐지 기능이 비활성화됩니다. 더 나은 접근 방식은 App-ID 또는 위협 탐지를 비활성화하지 않는 SIP ALG를 비활성화하는 것입니다.

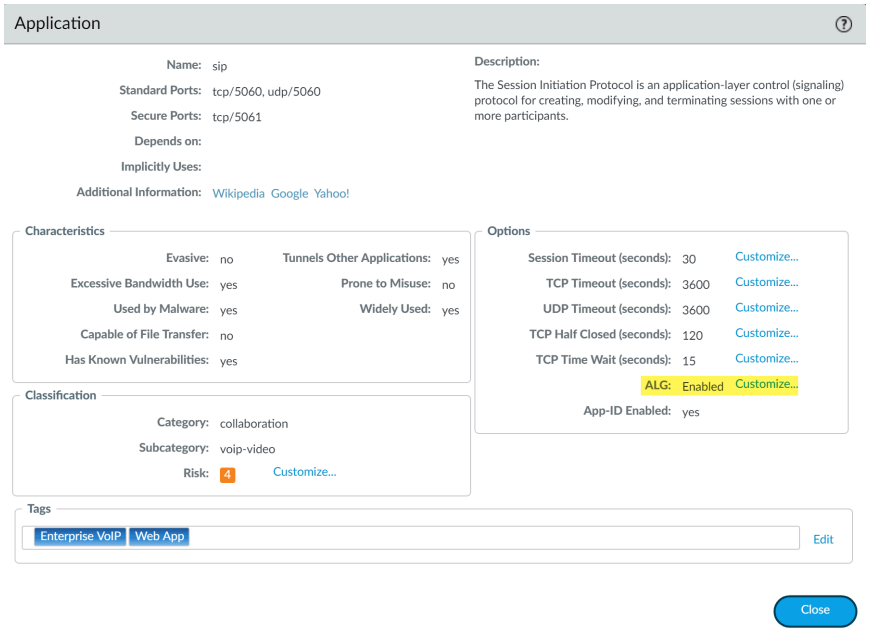
다음 절차에서는 SIP ALG를 비활성화하는 방법을 설명합니다.

**STEP 1 |** 개체 > 애플리케이션을 선택합니다.

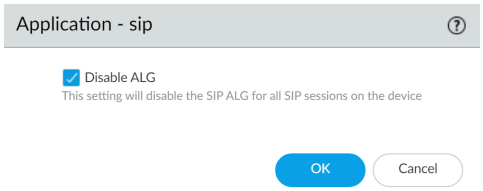
**STEP 2 |** **sip** 애플리케이션을 선택합니다.

**sip** 애플리케이션을 찾는 데 도움이 되도록 검색 상자에 sip를 입력할 수 있습니다.

**STEP 3 |** 애플리케이션 대화 상자의 옵션 섹션에서 **ALG**에 대해 사용자 지정...을 선택합니다.




**STEP 4 |** 애플리케이션 - sip 대화 상자에서 **ALG** 비활성화 체크박스를 선택한 다음 확인을 클릭합니다.




**STEP 5 |** 애플리케이션 대화 상자를 닫고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# HTTP 헤더를 사용하여 SaaS 애플리케이션 액세스 관리

SaaS 애플리케이션의 승인되지 않은 사용은 일반적으로 애플리케이션의 소비자 버전에 액세스하여 사용자가 네트워크 외부로 민감한 정보를 전송하는 방법이 될 수 있습니다. 그러나 특정 개인이나 조직에 대해 이러한 애플리케이션의 엔터프라이즈 버전에 대한 액세스를 허용해야 하는 경우 SaaS 애플리케이션을 완전히 차단할 수 없습니다.

사용자 지정 HTTP 헤더를 사용하여 특정 엔터프라이즈 계정을 허용하면서 SaaS 소비자 계정을 허용하지 않을 수 있습니다. 많은 SaaS 애플리케이션은 특정 HTTP 헤더에 포함된 정보를 기반으로 애플리케이션에 대한 액세스를 허용하거나 허용하지 않습니다. 사전 정의된 유형을 사용하여 HTTP 헤더 삽입 항목을 생성하여 Google G Suite 및 Microsoft Office 365와 같은 널리 사용되는 SaaS 애플리케이션에 대한 액세스를 관리할 수 있습니다. Palo Alto Networks®는 콘텐츠 업데이트를 사용하여 이러한 애플리케이션에 특정한 사전 정의된 규칙 세트를 유지 관리하고 사전 정의된 새로운 규칙 세트를 추가합니다.

또한 서비스 액세스를 제한하기 위해 HTTP 헤더를 사용하는 SaaS 애플리케이션에 대한 액세스를 관리하려는 경우 Palo Alto Networks가 사전 정의된 규칙 세트를 제공하지 않은 경우 사용자 지정 HTTP 헤더 삽입 항목을 생성할 수 있습니다.

상용 SaaS 애플리케이션은 항상 SSL을 사용하므로 HTTP 헤더 삽입을 수행하려면 복호화가 필요합니다. 트래픽이 업스트림 방화벽에 의해 아직 복호화되지 않은 경우 SSL 포워딩 프록시 복호화를 사용하여 트래픽을 복호화하도록 방화벽을 구성할 수 있습니다.

이 기능을 사용하기 위해 ***URL*** 필터링 라이선스가 필요하지 않습니다.

HTTP 헤더를 사용하여 SaaS 애플리케이션을 관리하는 방법을 이해하려면 다음을 참조하십시오.

- SaaS 사용자 지정 헤더 이해
- 사전 정의된 SaaS 애플리케이션 유형에 사용되는 도메인
- 사전 정의된 형식을 사용하여 HTTP 헤더 삽입 항목 생성
- 사용자 지정 HTTP 헤더 삽입 항목 생성

## SaaS 사용자 지정 헤더 이해

시작하기 전에 관리 중인 SaaS 애플리케이션과 함께 사용할 사용자 지정 HTTP 헤더를 이해해야 합니다. 이러한 헤더로 수행할 수 있는 작업과 목표를 달성하기 위해 지정해야 하는 정보를 이해해야 합니다.

사용자 정의 헤더를 사용하는 SaaS 애플리케이션이 항상 이를 사용하여 계정 유형에 대한 액세스를 제어하는 것은 아닙니다. 예를 들어 Palo Alto Networks®는 네트워크 사용자가 제한된 콘텐츠에 액세스할 수 있는지의 여부를 결정하는 YouTube 맞춤 헤더에 대한 사전 정의된 지원을 제공합니다.

또한 액세스를 제어하려는 SaaS 애플리케이션에 대한 설명서를 읽어서 해당 애플리케이션에 사용해야 하는 헤더를 이해해야 합니다.


©2023 Palo Alto Networks, Inc.

*HTTP* 헤더 삽입에는 다음 제한이 적용됩니다.

- 헤더 이름 문자 길이: *100.*
- 헤더 값 문자 길이: *16K*

일부 *SaaS* 애플리케이션은 이러한 제한을 초과하는 사용자 지정 헤더 이름을 정의하거나 해당 사용자 지정 헤더에 값을 할당할 수 있습니다. 이러한 상황은 드물지만 *SaaS* 애플리케이션이 이러한 문자 길이 제한 중 하나 또는 둘 다를 초과하면 차세대 방화벽이 해당 *SaaS* 애플리케이션에 대한 액세스를 성공적으로 관리할 수 없습니다.

다음 표에는 Palo Alto Networks가 사전 정의된 지원을 제공하는 SaaS 애플리케이션에 사용할 수 있는 헤더가 나열되어 있습니다. 각 헤더에는 해당 헤더와 관련된 추가 정보에 대한 링크도 포함되어 있습니다.

| 애플리케이션 | 헤더 | 상세 정보 |
|---|---|---|
| **Dropbox** | `X-Dropbox-allowed-Team-Ids` | www.dropbox.com/help/business/network-control<br><br>승인된 Enterprise Dropbox 계정에 대한 액세스를 허용할 수 있습니다. 이 헤더의 값은 Dropbox 관리 콘솔의 네트워크 제어 섹션에서 얻을 수 있는 비즈니스 계정의 팀 ID입니다. 또한 동일한 위치에서 이 기능을 활성화해야 합니다.<br><br>이 헤더를 관리하는 방법과 Dropbox 클라이언트를 활성화하여 트래픽을 복호화하는 방법에 대한 자세한 내용은 Dropbox 계정 담당자에게 문의하세요. |
| **Google G Suite** | `X-GooGApps-Allowed-Domains` | support.google.com/a/answer/1668854?hl=en<br><br>도메인에서 특정 Google 계정에 대한 액세스를 허용할 수 있습니다. 이 헤더에 부여하는 값은 도메인과 하위 도메인입니다.<br><br>Google 애플리케이션의 헤더를 성공적으로 삽입하려면 다음도 수행해야 합니다. |


©2023 Palo Alto Networks, Inc.

| 애플리케이션 | 헤더 | 상세 정보 |
| --- | --- | --- |
| | | 1. 다음 카테고리 및 URL을 포함하는 SSL암호 해독 프로파일을 만듭니다.<br>• 비즈니스 및 경제<br>• 컴퓨터 및 인터넷 정보<br>• 콘텐츠 배달 네트워크<br>• 인터넷 통신 및 전화<br>• 저위험<br>• 온라인 저장 및 백업<br>• 검색 엔진<br>• 웹 기반 이메일<br>• drive.google.com<br>• *.google.com<br>• *.googleusercontent.com<br>• *.gstatic.com<br>2. HTTP 헤더 삽입은 현재 HTTP/2에 대해 지원되지 않습니다. 헤더를 삽입하려면 적절한 복호화 프로파일에서 **Strip ALPN** 기능을 사용하여 HTTP/2 연결을 HTTP/1.1로 다운그레이드하십시오. 자세한 내용은 앱 ID 및 HTTP/2 검사을(를) 참조하십시오.<br>3. 방화벽이 이 프로토콜에 대한 헤더 삽입을 지원하지 않기 때문에 QUIC(빠른 UDP 인터넷 연결) App-ID를 차단하는 규칙을 생성하고 보안 정책의 맨 위에 배치합니다. 그렇게 하면 앱은 이전 단계에서 방화벽이 처리하는 TLS를 통한 HTTP/2 사용으로 되돌아갑니다. |
| **Microsoft Office 365** | 테넌트에 대한 액세스 제한<br>`Restrict-Access-Context` | docs.microsoft.com/en-us/azure/active-directory/active-directory-tenant-restrictions<br>사용자에게 액세스를 허용할 테넌트 목록을 `Restrict-Access-To-Tenants`에 제공합니다. 테넌트에 등록된 모든 도메인을 사용하여 이 목록에서 테넌트를 식별할 수 있습니다.<br>`Restrict-Access-Context`에 테넌트 제한을 설정하는 디렉터리 ID를 제공합니다. Azure Portal에서 디렉터리 ID를 찾을 수 있습니다. 관리자로 로그인하고 **Azure Active Directory**를 선택한 다음 속성을 선택합니다. |


©2023 Palo Alto Networks, Inc.

| 애플리케이션 | 헤더 | 상세 정보 |
|---|---|---|
| **YouTube** | `YouTube-Restrict` | support.google.com/a/answer/6214622?hl=en<br>사용자가 볼 수 있기를 원하는 비디오 유형에 대한 정보와 함께 이 헤더를 제공합니다. **Strict** 또는 **Moderate** 설정을 지정할 수 있습니다. 이러한 다양한 설정에 대한 자세한 내용은 support.google.com/a/answer/6212415를 참조하세요. |

## 사전 정의된 SaaS 애플리케이션 유형에 사용되는 도메인

SaaS 애플리케이션은 HTTPS를 사용하므로 이 트래픽에 사용자 지정 헤더를 삽입하려면 사용자 지정 헤더를 복호화해야 합니다. 방화벽에서 사용할 수 있는 포워드 프록시 복호화를 사용하여 사용자 지정 헤더를 복호화하는 경우 트래픽과 연결된 도메인을 식별하여 암호를 복호화하려는 특정 HTTPS 트래픽을 식별해야 합니다. 다음 표에는 Palo Alto Networks®가 사전 정의된 규칙을 제공한 각 SaaS 애플리케이션에 대한 관련 도메인이 나와 있습니다.

| 애플리케이션 | 도메인 |
|---|---|
| **Dropbox** | `*.dropbox.com` |
| **G Suite** | `*.google.com`<br>`gmail.com` |
| **Microsoft Office 365** | `login.microsoftonline.com`<br>`login.microsoft.com`<br>`login.windows.net` |
| **YouTube** | `www.youtube.com`<br>`m.youtube.com`<br>`youtubei.googleapis.com`<br>`youtube.googleapis.com`<br>`www.youtube-nocookie.com` |


©2023 Palo Alto Networks, Inc.

# 사전 정의된 형식을 사용하여 HTTP 헤더 삽입 항목 생성

**STEP 1 |** 이미 HTTPS 트래픽을 복호화하는 업스트림 디바이스가 없는 경우 SSL 포워드 프록시 구성을 사용하여 복호화를 구성합니다.

> ***Dropbox***에 ***SSL*** 복호화를 구성하는 경우 ***SSL*** 트래픽을 허용하도록 ***Dropbox*** 클라이언트도 구성해야 합니다. 이러한 절차는 ***Dropbox*** 전용이며 비공개입니다. 이러한 절차를 받으려면 ***Dropbox*** 계정 담당자에게 문의하십시오.

1. 관리 중인 SaaS 애플리케이션에 대한 사용자 지정 URL 카테고리를 추가합니다(개체 > 사용자 지정 개체 > **URL** 카테고리).
2. 카테고리에 대한 이름을 지정합니다.
3. 관리 중인 SaaS 애플리케이션과 관련된 도메인 또는 헤더에 사용자 이름과 도메인을 삽입하려는 도메인을 추가합니다. 사전 정의된 SaaS 애플리케이션 각각에 사용하는 도메인 목록은 사전 정의된 SaaS 애플리케이션 유형에 사용되는 도메인을 참조하십시오. HTTP 헤더에 사용자 이름과 도메인을 포함하도록 방화벽을 구성하는 방법에 대한 자세한 내용은 HTTP 헤더에 사용자 이름 삽입을(를) 참조하십시오.

   각 도메인 이름은 최대 254자까지 가능하며 각 항목에 대해 최대 50개의 도메인을 식별할 수 있습니다. 도메인 목록은 와일드카드(예: **`*.example.com`**)를 지원합니다. 가장 좋은 방법은 와일드카드(예: **`*.*.*`**)를 중첩하지 않고 동일한 URL 프로파일 내에서 도메인을 겹치지 않는 것입니다.
4. SaaS 애플리케이션 관리의 경우 복호화 정책 규칙을 생성하고 이 절차를 따를 때 다음을 구성합니다.
   - 서비스/**URL** 카테고리 탭에서 이전 단계에서 만든 **URL** 카테고리를 추가합니다.
   - 옵션 탭에서 작업이 복호화로 설정되어 있고 형식이 **SSL** 포워드 프록시로 설정되어 있는지 확인합니다.

**STEP 2 |** URL 필터링 프로파일을 편집하거나 추가합니다.

**STEP 3 |** **URL** 필터링 프로파일 대화 상자에서 **HTTP** 헤더 삽입을 선택합니다.

**STEP 4 |** 항목을 추가합니다.

1. 이 항목에 대해 이름(최대 100자)을 지정합니다.
2. 사전 정의된 유형을 선택합니다.

   그러면 도메인 및 헤더 목록이 채워집니다.
3. 각 헤더에 대해 값을 입력합니다.

   각 헤더 값에는 최대 16K 문자가 포함될 수 있습니다.
4. (선택 사항) 헤더에 대한 삽입 활동의 로깅을 활성화하려면 로그를 선택합니다.

   허용된 트래픽은 기록되지 않으므로 허용된 트래픽에 대해 헤더 삽입이 기록되지 않습니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** HTTP 헤더 삽입 URL 필터링 프로파일을 포함하도록 추가 또는 보안 정책 규칙(정책 > 보안)을 수정합니다. .

- SaaS 애플리케이션 관리의 경우 사용자가 이 헤더 삽입 규칙을 구성 중인 SaaS 애플리케이션에 액세스할 수 있도록 허용합니다.
- HTTP 헤더에 사용자 이름과 도메인을 포함하려면 URL 필터링 프로파일을 HTTP 또는 HTTPS 트래픽에 대한 보안 정책 규칙에 적용합니다.

1. 2단계에서 편집하거나 생성한 URL 필터링 프로파일(작업 > **URL** 필터링)을 선택합니다.
2. 확인을 클릭하여 저장한 다음 변경 사항을 커밋합니다.

**STEP 6 |** 방화벽이 헤더를 올바르게 삽입하는지 확인합니다.

- SaaS 애플리케이션 관리의 경우 엔드포인트에서 SaaS 애플리케이션에 대한 액세스가 예상대로 작동하는지 확인합니다.

1. 액세스할 수 있을 것으로 예상되는 계정 또는 콘텐츠에 액세스해 봅니다. SaaS 계정이나 콘텐츠에 액세스할 수 없는 경우 구성이 작동하지 않습니다.
2. 예상되는 계정이나 콘텐츠에 액세스하려고 차단됩니다. SaaS 계정 또는 콘텐츠에 액세스할 수 있는 경우 구성이 작동하지 않습니다.
3. 이전 단계가 모두 예상대로 작동하면 로그 보기(4.4단계에서 로깅을 구성한 경우)를 수행할 수 있으며 기록된 HTTP 헤더 삽입 활동이 표시되어야 합니다.

## 사용자 지정 HTTP 헤더 삽입 항목 생성

**STEP 1 |** 이미 HTTPS 트래픽을 해독하는 업스트림 디바이스가 없는 경우 SSL 전달 프록시를 구성합니다.

1. 관리 중인 SaaS 애플리케이션에 대한 사용자 정의 URL 카테고리를 추가합니다(개체 > 사용자 정의 개체 > **URL** 카테고리).
2. 카테고리에 대한 이름을 지정합니다.
3. 관리하는 SaaS 애플리케이션에 특정 도메인을 추가합니다.
4. 복호화 정책 규칙을 생성하고 이 절차를 따르면서 다음을 구성합니다.
   - 서비스/**URL** 카테고리 탭에서 이전 단계에서 만든 **URL** 카테고리를 추가합니다.
   - 옵션 탭에서 작업이 복호화로 설정되어 있고 형식이 **SSL** 포워드 프록시로 설정되어 있는지 확인합니다.

**STEP 2 |** URL 필터링 프로파일을 편집하거나 만듭니다.

**STEP 3 |** URL 필터링 프로파일 대화 상자에서 **HTTP** 헤더 삽입을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 항목을 추가합니다.

1. 이 항목의 이름을 지정합니다.
2. 유형으로 사용자 정의를 선택합니다.
3. 도메인 목록에 도메인을 추가합니다.

   최대 50개의 도메인을 추가할 수 있으며 각 도메인 이름에는 최대 256자까지 가질 수 있으며, 와일드카드가 지원됩니다(예: *.example.com).

   ***HTTP*** 헤더 삽입은 이 목록의 도메인이 ***HTTP*** 요청의 호스트 헤더의 도메인과 일치할 때 발생합니다.
4. 헤더 목록에 헤더를 추가합니다.

   최대 5개의 헤더를 추가할 수 있으며 각 헤더에는 최대 100자까지 가질 수 있지만 공백은 포함되지 않습니다.
5. 각 헤더에 대해값을 입력합니다.

   각 헤더 값에는 최대 16K 문자가 포함될 수 있습니다.
6. (선택 사항) 헤더에 대한 삽입 활동을 기록합니다.
7. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 5 |** 이 헤더 삽입 규칙을 구성하는 SaaS 애플리케이션에 사용자가 액세스할 수 있도록 하는 보안 정책규칙(정책 > 보안)을 추가하거나 편집합니다.

1. 2단계에서 편집하거나 생성한 URL 필터링 프로파일(작업 > **URL** 필터링)을 선택합니다.
2. 확인을 클릭하여 저장한 다음 변경 사항을 커밋합니다.

**STEP 6 |** SaaS 애플리케이션에 대한 액세스가 예상대로 작동하는지 확인합니다. 네트워크에 연결된 엔드포인트에서:

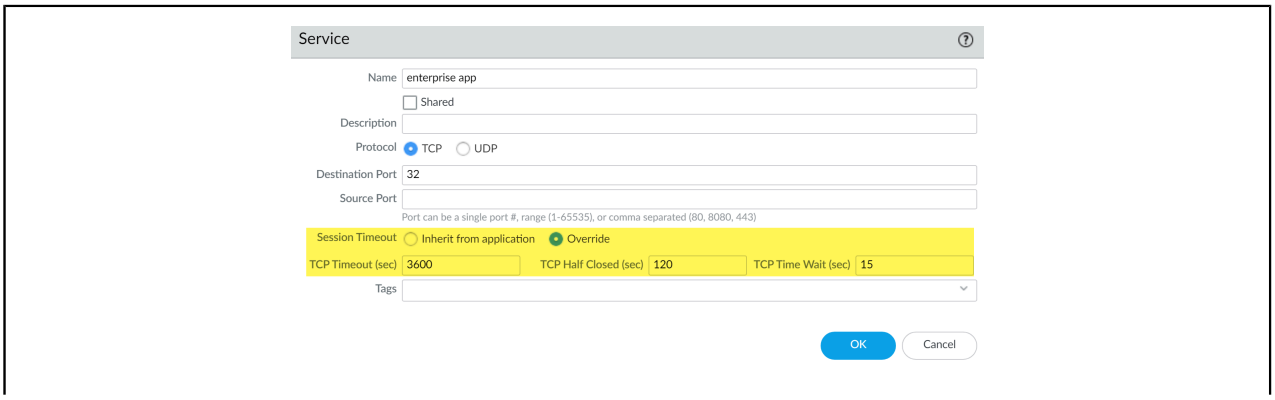
1. 액세스할 수 있을 것으로 예상되는 계정 또는 콘텐츠에 액세스해 봅니다. SaaS 계정 또는 콘텐츠에 액세스할 수 없는 경우 구성이 작동하지 않는 것입니다.
2. 차단될 것으로 예상되는 계정 또는 콘텐츠에 액세스해 봅니다. SaaS 계정 또는 콘텐츠에 액세스할 수 있으면 구성이 작동하지 않는 것입니다.
3. 앞의 두 단계가 모두 예상대로 작동하면 로그 확인이 가능하며(4.6단계에서 로깅을 구성한 경우), 기록된 HTTP 헤더 삽입 작업이 표시됩니다.


©2023 Palo Alto Networks, Inc.

# 데이터 센터 애플리케이션에 대한 사용자 지정 타임아웃 유지

포트 기반 정책에서 애플리케이션 기반 정책으로 이동할 때 애플리케이션에 대한 사용자 지정 타임아웃을 쉽게 유지 관리합니다. 이 방법을 사용하여 App-ID를 재정의하거나(애플리케이션 가시성을 잃음) 맞춤 App-ID를 생성(시간 및 조사 소모)하는 대신 맞춤 제한 시간을 유지 관리합니다.

시작하려면 서비스 개체:




그런 다음 정책 규칙에 서비스 개체를 추가하여 규칙이 적용하는 애플리케이션에 맞춤 제한 시간을 적용합니다.

다음 단계에서는 애플리케이션에 맞춤 제한 시간을 적용하는 방법을 설명합니다. 사용자 그룹에 사용자 지정 시간 초과를 적용하려면 동일한 단계를 수행할 수 있지만 시간 초과를 적용할 사용자를 적용하는 보안 정책 규칙에 서비스 개체를 추가해야 합니다.

**STEP 1 |** 서비스 개체를 추가하거나 수정하려면 개체 > 서비스를 선택합니다.

보안 정책 규칙에 대한 일치 기준을 정의할 때 서비스 개체를 생성할 수도 있습니다. 정책 > 보안 > 서비스**/URL** 카테고리를 선택하고 규칙이 적용되는 애플리케이션 트래픽에 적용할 새 서비스 개체를 추가합니다.

**STEP 2 |** 사용할 서비스의 프로토콜(TCP 또는 UDP)을 선택합니다.

**STEP 3 |** 대상 포트 번호 또는 서비스에서 사용하는 포트 번호 범위를 입력합니다.

**STEP 4 |** 서비스에 대한 세션 타임아웃을 정의합니다.

- 애플리케이션에서 상속(기본값) - 서비스 기반 타임아웃가 적용되지 않습니다. 대신 애플리케이션 타임아웃을 적용하십시오.
- 재정의 - 서비스에 대한 사용자 지정 세션 타임아웃을 정의합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 애플리케이션 타임아웃을 재정의하고 사용자 정의 세션 타임아웃을 정의하도록 선택한 경우 다음을 계속하십시오.

- **TCP** 타임아웃 값을 입력하여 데이터 전송이 시작된 후 TCP 세션이 열린 상태로 유지될 수 있는 최대 시간(초)을 설정합니다. 이 시간이 만료되면 세션이 닫힙니다. 값 범위는 1 - 604800이며 기본값은 3600초입니다.
- **TCP Half Closed** 값을 입력하여 첫 번째 FIN 패킷 수신과 두 번째 FIN 패킷 또는 RST 패킷 수신 사이에 세션이 세션 테이블에 남아 있는 최대 시간(초)을 설정합니다. 타이머가 만료되면 세션이 닫힙니다. 값 범위는 1 - 604800이며 기본값은 120초입니다.
- **TCP** 대기 시간 값을 입력하여 두 번째 FIN 패킷 또는 RST 패킷을 수신한 후 세션이 세션 테이블에 남아 있는 최대 시간(초)을 설정합니다. 타이머가 만료되면 세션이 닫힙니다. 값 범위는 1 - 600이며 기본값은 15초입니다.

**STEP 6 |** 확인을 클릭하여 서비스 개체를 저장합니다.

**STEP 7 |** 정책 > 보안을 선택한 다음 정책 규칙을 추가 또는 수정하여 제어하려는 애플리케이션 트래픽을 제어합니다.

**STEP 8 |** 서비스/**URL** 카테고리를 선택하고 방금 생성한 서비스 개체를 보안 정책 규칙에 추가합니다.

**STEP 9 |** 확인을 클릭하고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

# Device-ID


- 디바이스 ID 개요
- 디바이스 ID 배포 준비
- 디바이스 ID 구성
- 디바이스 ID 관리
- 디바이스 ID에 대한 CLI 명령

# 디바이스 ID 개요

2020 Unit 42 IoT 위협 보고서에 따르면 평균 기업의 모든 네트워크 연결 디바이스 중 30 %가 IoT입니다. 이로 인해 악의적인 사용자가 악용할 가능성이 많아 지속적으로 증가하는 위험 영역이 나타납니다. 또한 이러한 디바이스를 식별하면 오래된 운영 소프트웨어와 같은 취약점으로부터 어떻게 보호합니까? 방화벽에서 Device-ID™를 사용하면 네트워크의 이벤트에 대한 디바이스 컨텍스트를 얻고, 해당 디바이스에 대한 정책 규칙 권장 사항을 얻고, 디바이스를 기반으로 정책 규칙을 작성하고, 권장 사항을 기반으로 보안 정책을 시행할 수 있습니다.

사용자 ID가 사용자 기반 정책을 제공하고 App-ID가 앱 기반 정책을 제공하는 방법과 마찬가지로 Device-ID는 IP 주소 또는 위치 변경사항과 관계없이 디바이스를 기반으로 하는 정책 규칙을 제공합니다. Device-ID를 사용하면 디바이스에 대한 추적성을 제공하고 네트워크 이벤트를 특정 디바이스와 연결하여 이벤트가 디바이스와 관련된 방식에 대한 컨텍스트를 확보하고 시간이 지남에 따라 변경될 수 있는 사용자, 위치 또는 IP 주소 대신 디바이스와 연결된 정책을 작성할 수 있습니다. 보안, 복호화, 서비스 품질(QoS) 및 인증 정책에서 디바이스 ID를 사용할 수 있습니다.

방화벽에서 Device-ID 기능을 사용하려면 IoT Security 구독을 구매하고 IoT Security 온보딩 프로세스 중에 방화벽을 선택해야 합니다. IoT 보안 구독에는 두 가지 유형이 있습니다.

- IoT 보안 구독
- IoT 보안 – DRDL(데이터 레이크) 구독이 필요하지 않음

첫 번째 구독을 통해 방화벽은 로깅 서비스로 데이터 로그를 보내고, 로깅 서비스는 분석을 위해 IoT Security로 스트리밍하고 저장을 위해 Cortex Data Lake 인스턴스로 스트리밍합니다. 데이터 레이크 인스턴스는 새 인스턴스이거나 기존 인스턴스일 수 있습니다. 두 번째 구독을 통해 방화벽은 데이터 로그를 로깅 서비스로 보내 분석을 위해 IoT Security로 스트리밍하지만 저장을 위해 Cortex Data Lake 인스턴스로 스트리밍하지 않습니다. IoT 보안 및 DRDL(IoT 보안) 구독은 IoT 보안 및 디바이스 ID 측면에서 동일한 기능을 제공한다는 점에 유의해야 합니다.

IoT 보안에 대한 연결을 허용하려면 방화벽에 디바이스 라이선스가 필요합니다. 로깅 서비스에 대한 연결을 허용하려면 로깅 서비스 라이선스가 필요합니다. 또한 방화벽은 IoT Security 및 로깅 서비스에 연결할 때 자체 인증을 위해 디바이스 인증서가 필요합니다.

방화벽에서 PAN-OS 버전 8.1.0을 PAN-OS 9.1.x에서 사용하는 경우 IoT 보안 라이선스는 디바이스에 대한 디바이스 분류, 동작 분석 및 위협 분석을 제공합니다. PAN-OS 10.0 이상을 사용하는 경우 Device-ID를 사용하여 IP 주소-디바이스 매핑을 사용하여 네트워크 이벤트에 대한 디바이스 컨텍스트를 확인하고, IoT Security를 사용하여 이러한 디바이스에 대한 정책 규칙 권장 사항을 가져오고, 보고서 및 ACC의 디바이스에 대한 가시성을 확보할 수 있습니다.

***PAN-OS** 버전 **10.0** 이상을 사용하는 **Panorama** 또는 방화벽에서 디바이스 기반 보안 정책을 만들 수 있습니다. 보안 정책을 적용하려면 디바이스에 유효한 **IoT** 보안 라이선스가 있어야 합니다.*

IoT Security 앱은 디바이스를 식별하고 분류하기 위해 방화벽의 로그, 네트워크 프로토콜 및 세션의 메타데이터를 사용합니다. 여기에는 디바이스 식별과 관련이 없는 개인 정보 또는 데이터가 포함되지 않습니다. 메타데이터는 또한 디바이스에 대해 예상되는 동작의 기초를 형성한 다음 해당 디바이스에 허용할 트래픽 및 프로토콜을 정의하는 정책 규칙 권장 사항에 대한 기준을 설정합니다.


©2023 Palo Alto Networks, Inc.

방화벽이 IoT 보안에서 보안 정책 규칙 권장 사항 및 IP 주소 간 매핑을 가져오면 방화벽은 디바이스 인증서를 에지 서버로 전송하여 인증합니다. 에지 서버는 자체 인증서를 전송하여 방화벽에 자신을 인증합니다. 방화벽은 온라인 인증서 상태 프로토콜(OCSP)을 사용하여 TCP 포트 80에서 HTTP를 사용하여 다음 사이트에 대해 확인하여 서버인증서를 확인합니다.

- ocsp.int-x3.letsencrypt.org
- isrg.trustid.ocscp.identrust.com
- crl.identrust.com

Panorama는 Panorama가 IoT 보안에서 정책 규칙 권장 사항을 가져오는 경우 가장자리 서버의 인증서를 검증하기 위해 동일한 검사를 수행합니다.

IoT Security가 네트워크에 이미 있는 Palo Alto Networks 방화벽을 사용하여 네트워크의 디바이스를 식별하고 분류한 후 새 디바이스 또는 타사 솔루션을 구현할 필요가 없으므로 Device-ID는 이 데이터를 활용하여 디바이스와 정책 규칙을 일치시키고 네트워크 이벤트에 대한 디바이스 컨텍스트를 제공할 수 있습니다. 방화벽이나 Panorama가 트래픽, 앱, 사용자, 디바이스 및 위협에 대해 제공하는 가시성을 통해 네트워크 이벤트를 개별 디바이스로 즉시 추적하고 해당 디바이스를 보호하기 위한 보안 정책 규칙 권장 사항을 얻을 수 있습니다.

***VM-50** 시리즈, **VM-200, CN** 시리즈를 제외하고 **PAN-OS 10.0**을 지원하고 **Device-ID**와 **IoT Security** 앱을 지원하는 모든 방화벽 플랫폼입니다.*

디바이스에 대한 분류 수준은 여섯 가지(속성이라고도 함)가 있습니다.

| 속성 | 예시 |
|---|---|
| 카테고리 | 프린터 |
| 프로파일 | Sharp 프린터 |
| 모델 | MX-6070N |
| OS 버전 | ThreadX 5 |
| OS 제품군 | ThreadX RTOS |
| 공급자 | SHARP Corporation |

네트워크의 디바이스에 대한 정책 규칙 권장 사항을 얻으려면 방화벽은 트래픽을 관찰하여 향상된 애플리케이션 로그(EAL)를 생성합니다. 그런 다음 방화벽은 EAL을 로깅 서비스로 전달합니다. IoT Security 앱은 분석을 위해 로깅 서비스에서 로그를 수신하고, IP 주소-디바이스 매핑을 제공하고, 디바이스에 대한 최신 정책 규칙 권장사항을 생성합니다. IoT 보안 앱을 사용하여 이러한 정책 규칙 권장 사항을 검토하고 이러한 디바이스에 대한 보안 정책을 만들 수 있습니다. IoT 보안 앱에서 정책 규칙을 활성화한 후 방화벽 또는 Panorama로 가져오고 보안 정책을 커밋합니다.

방화벽은 네트워크에서 DHCP 브로드캐스트 및 유니캐스트 트래픽을 관찰하여 동적으로 할당된 네트워크 설정이 있는 디바이스를 식별할 수 있어야 합니다. IoT 보안은 고정 IP 디바이스도 지원합니다. 방화벽이 관찰할 수 있는 트래픽이 많을수록 디바이스에 대한 정책 규칙 권장 사항이 더 정확하고 디바이스에 대

 ©2023 Palo Alto Networks, Inc.

한 IP 주소-디바이스 매핑이 더 빠르고 정확합니다. 디바이스가 IP 주소를 얻기 위해 DHCP 트래픽을 보내면 방화벽은 이러한 유형의 요청을 관찰하고 로깅 서비스로 보낼 EAL을 생성하며, 여기서 IoT Security는 분석을 위해 해당 요청에 액세스합니다.

> ***L2*** 인터페이스에서 트래픽을 관찰하려면 해당 인터페이스에 대한 ***VLAN***을 구성해야 합니다. 방화벽이 인터페이스를 ***DHCP*** 릴레이의 ***L3*** 인터페이스로 처리하도록 허용하면 트래픽이나 성능에 영향을 주지 않고 ***DHCP*** 브로드캐스트 트래픽을 관찰할 수 있습니다.

방화벽은 트래픽을 기반으로 디바이스를 감지한 다음 해당 디바이스에 대한 보안 정책을 적용해야 하기 때문에 방화벽은 디바이스에 대한 보안 정책을 적용하여 디바이스에서 메타데이터를 수집하는 센서와 집행자 역할을 합니다. IoT 보안 앱은 DHCP 트래픽을 보내는 즉시 새 디바이스를 자동으로 감지하고 첫 주 내에 디바이스의 95%를 식별할 수 있습니다.

각 애플리케이션에는 원칙적으로 방화벽이나 Panorama로 가져오는 개별 권장 사항이 있습니다. 권장 사항을 가져올 때 방화벽이나 Panorama 권장 사항에서 디바이스 동작을 정의하기 위해 적어도 두 개의 개체를 생성합니다.

- 트래픽이 발생하는 디바이스를 식별하는 소스 디바이스 개체
- 디바이스, IP 주소 또는 완전 인증 도메인 이름(FQDN)일 수 있는 트래픽에 대한 허용 대상을 식별하는 대상 개체 하나 이상

방화벽이나 Panorama에 이미 디바이스 개체가 있는 경우 방화벽이나 Panorama는 새 디바이스 개체를 만드는 대신 디바이스 개체를 업데이트합니다. 이러한 디바이스 개체를 보안, 인증, 복호화 및 서비스 품질(QoS) 정책에서 사용할 수 있습니다.

또한 방화벽은 각 규칙에 두 개의 태그를 할당합니다.

- 카테고리(예: `NetworkDevice -TrendNet`)를 포함하여 소스 디바이스를 식별하는 디바이스입니다.
- 규칙이 IoT 정책 규칙 권장 사항임을 나타내는 규칙(`IoTSecurityRecommended`)입니다.

> 방화벽이 규칙에 할당하는 태그는 동기화되지 않은 경우 매핑을 복원하는 유일한 방법이므로 태그를 편집하거나 제거하지 마십시오.

디바이스 ID의 최적의 배포 및 운영을 위해 다음 모범 사례를 권장합니다.

- 네트워크에 중앙에 있는 방화벽에 디바이스 ID를 배포합니다. 예를 들어 환경이 큰 경우 IP 주소 관리(IPAM) 디바이스에서 상류인 방화벽에 디바이스 ID를 배포합니다. 환경이 작은 경우 DHCP 서버 역할을 하는 방화벽에 디바이스 ID를 배포합니다.
- 초기 배포 중에 Device-ID가 네트워크에서 메타데이터를 최소 14일 동안 수집하도록 허용합니다. 디바이스가 매일 활성화되지 않은 경우 식별 프로세스가 더 오래 걸릴 수 있습니다.
- 가장 중요한 디바이스 순서로 디바이스 기반 정책을 작성하여 가장 중요하지 않은 방식으로 작성합니다. 우선순위 지정 기준:

  1. 등급(보안 네트워크 디바이스 우선)
  2. 중요 디바이스(예: 서버 또는 MRI 기계)
  3. 환경별 디바이스(예: 화재 경보기 및 배지 판독기) )
  4. 소비자용 IoT 기기(예: 스마트 시계 또는 스마트 스피커)

 ©2023 Palo Alto Networks, Inc.

- 내부 영역에 대해서만 영역별 단위로 디바이스 ID를 사용하도록 설정합니다.

 ©2023 Palo Alto Networks, Inc.

# 디바이스 ID 배포 준비

Device-ID 배포를 위해 네트워크를 준비하려면 다음 사전 배포 작업을 완료하여 방화벽이 EAL(Enhanced Application Log)을 생성하고 Cortex Data Lake에 전송하여 정책 규칙 권장 사항 생성을 위해 IoT Security에서 처리 및 분석할 수 있도록 합니다.

**STEP 1 |** 아직 설치하지 않았다면 방화벽 또는 파노라마에 기기 인증서를 설치하세요.

장치 인증서는 로깅 서비스 및 IoT Security에 연결할 때 방화벽을 인증합니다.

*Panorama*를 사용하여 여러 방화벽을 관리하는 경우 *Palo Alto Networks*는 디바이스 *ID* 배포의 모든 방화벽을 *PAN-OS 10.0* 또는 이후 버전으로 업그레이드하는 것이 좋습니다. 디바이스를 일치 기준으로 사용하는 규칙을 생성하고 *Panorama*가 *PAN-OS 9.1* 또는 이전 버전을 사용하는 방화벽으로 규칙을 푸시하는 경우 방화벽이 지원되지 않아 디바이스 일치 기준을 생략하여 정책 규칙 트래픽 일치에 문제가 발생할 수 있습니다.

**STEP 2 |** 방화벽에 장치 라이선스와 로깅 서비스 라이선스를 설치합니다.

이렇게 하려면 디바이스 > 라이선스를 클릭한 다음 라이선스 관리 섹션에서 라이선스 서버에서 라이선스 키 검색을 선택합니다. 그러면 방화벽에 로깅 서비스 및 IoT 보안에 대한 라이선스가 설치됩니다.

로깅 서비스 라이선스는 방화벽이 로깅 서비스에 연결할 수 있도록 허용합니다.

장치 라이선스는 방화벽이 IoT Security에 연결할 수 있도록 허용합니다.

**STEP 3 |** (L2 인터페이스만) 방화벽이 DHCP 브로드캐스트 트래픽을 관찰할 수 있도록 각 L2 인터페이스에 대해 VLAN 인터페이스를 만듭니다.

**STEP 4 |** (선택 사항) Device-ID 및 IoT 보안에 필요한 트래픽을 허용하도록 서비스 경로를 구성합니다.

기본적으로 방화벽은 관리 인터페이스를 사용합니다. 다른 인터페이스를 사용하려면 다음 단계를 완료하십시오.

1. 기기 > 설정 > 서비스를 선택한 다음 서비스 경로 구성을 선택합니다.
2. 서비스 경로를 맞춤설정합니다.
3. **IPv4** 프로토콜을 선택합니다.

   *Device-ID* 및 *IoT Security*는 *IPv6*을 지원하지 않습니다.

4. 서비스 열에서 데이터 서비스를 선택합니다.
5. 소스 인터페이스및소스 주소를 선택합니다.
6. 확인을 두 번 클릭합니다.

**STEP 5 |** App-ID를 사용하여 Device-ID 및 IoT 보안에 필요한 트래픽을 허용합니다.

| 용도 | App-ID |
|---|---|
| 정책 규칙 권장 사항을 검색하고 IoT Security 앱과 방화벽 또는 Panorama 간의 트래픽을 허용합니다. | **paloalto-iot-security** |


©2023 Palo Alto Networks, Inc.

| 용도 | App-ID |
|---|---|
| 모든 EAL 및 모든 세션 로그에 대한 트래픽을 허용합니다. | **paloalto-logging-service** |
| IoT 보안 동적 업데이트 및 디바이스 사전 업데이트를 검색합니다. | **paloalto-updates** |

*Device-ID*를 사용하는 *Palo Alto Networks* 차세대 방화벽과 인터넷 사이에 타사 방화벽이 있는 경우 차세대 방화벽이 미주에 있는 경우 ***iot.services-edge.paloaltonetworks.com:443*** 에 액세스할 수 있는지 확인하십시오. 지역, *EU* 지역의 경우 ***eu.iot.services-edge.paloaltonetworks.com:443*** , 아시아 태평양 지역의 경우 ***apac.iot.services-edge.paloaltonetworks.com:443*** 입니다.

**STEP 6 |** 인터넷과 Panorama 및 Panorama 관리 차세대 방화벽 사이에 타사 방화벽이 있는 경우 Device-ID 및 IoT 보안에 필요한 트래픽을 허용하는지 확인하십시오.

| 용도 | 주소 | TCP 포트 |
|---|---|---|
| (PAN-OS 버전 10.0.3 이상) 지역 FQDN을 수신하면 Device-ID가 IoT 보안에서 IP 주소-디바이스 매핑 및 정책 규칙 권장 사항을 검색할 수 있습니다. | **enforcer.iot.services-edge.paloaltonetworks.com** | 443 |
| (PAN-OS 버전 10.0.0~10.0.2 이상) Device-ID가 IoT Security에서 정책 규칙 권장 사항 및 IP 주소-디바이스 매핑을 수신하도록 허용합니다. | 미주 지역<br>**iot.services-edge.paloaltonetworks.com**<br>EU 지역<br>**eu.iot.services-edge.paloaltonetworks.com**<br>아시아 태평양 지역<br>**apac.iot.services-edge.paloaltonetworks.com** | 443 |
| (PAN-OS 버전 10.0.0 이상) 차세대 방화벽이 업데이트 서버에서 장치 사전 파일을 다운로드하도록 합니다. | **updates.paloaltonetworks.com** | 443 |
| (PAN-OS 버전 10.0.0 이상) Panorama가 로그에 대한 쿼 | 미주 지역<br>**iot.services-edge.paloaltonetworks.com** | 443 |


©2023 Palo Alto Networks, Inc.

| 용도 | 주소 | TCP 포트 |
|---|---|---|
| 리를 로깅 서비스로 보내도록 합니다. | EU 지역<br>**eu.iot.services-edge.paloaltonetworks.com**<br>아시아 태평양 지역<br>**apac.iot.services-edge.paloaltonetworks.com** | |
| (IoT 보안 구독 + Cortex Data Lake) Cortex Data Lake에 로그를 전달합니다. | Cortex Data Lake에 필요한 TCP 포트 및 FQDN을참조하십시오. | |

*PAN-OS* 버전 *10.0.0 - 10.0.2*는 기본적으로 미주 지역의 에지 서비스 *FQDN*에 연결합니다(*iot.services-edge.paloaltonetworks.com*). 이러한 *PAN-OS* 버전을 실행하는 방화벽의 경우 *EU* 지역(*eu.iot.services-edge.paloaltonetworks.com*) 또는 아시아 태평양 지역(*apac.iot.services-edge.paloaltonetworks.com*)의 *FQDN*에 연결할 수 있습니다. 수동으로 구성해야 합니다. *PAN-OS* 버전 *10.0.3* 이상의 경우 방화벽은 *IoT* 보안 온보딩 프로세스 중에 설정된 지역을 기반으로 사용할 올바른 *FQDN*을 자동으로 검색합니다. 수동으로 설정할 필요가 없습니다.

**STEP 7 |** 인터넷과 Panorama 및 Panorama 관리 차세대 방화벽 사이에 타사 방화벽이 있는 경우 Device-ID 및 IoT 보안에 필요한 트래픽을 허용하는지 확인하십시오.

| 용도 | 주소 | TCP 포트 |
|---|---|---|
| (PAN-OS 버전 10.0.3 이상) 지역 FQDN을 수신하면 Device-ID가 IoT 보안에서 IP 주소-디바이스 매핑 및 정책 규칙 권장 사항을 검색할 수 있습니다. | **enforcer.iot.services-edge.paloaltonetworks.com** | 443 |
| (PAN-OS 버전 10.0.0~10.0.2 이상) Device-ID가 IoT Security에서 정책 규칙 권장 사항 및 IP 주소-디바이스 매핑을 수신하도록 허용합니다. | 미주 지역<br>**iot.services-edge.paloaltonetworks.com**<br>EU 지역<br>**eu.iot.services-edge.paloaltonetworks.com**<br>아시아 태평양 지역<br>**apac.iot.services-edge.paloaltonetworks.com** | 443 |


©2023 Palo Alto Networks, Inc.

| 용도 | 주소 | TCP 포트 |
|---|---|---|
| (PAN-OS 버전 10.0.0 이상) 차세대 방화벽이 업데이트 서버에서 장치 사전 파일을 다운로드하도록 합니다. | **updates.paloaltonetworks.com** | 443 |
| (IoT 보안 구독 + Cortex Data Lake) Cortex Data Lake에 로그를 전달합니다. | Cortex Data Lake에 필요한 TCP 포트 및 FQDN을참조하십시오. | |

**STEP 8 |** DHCP 트래픽에 대한 로그를 관찰하고 생성하도록 방화벽을 구성한 다음 IoT Security에서 처리 및 분석할 수 있도록 로그를 포워딩합니다.

- 방화벽이 DHCP 서버 역할을 하는 경우:
  1. 향상된 애플리케이션 로깅을 활성화합니다.
  2. 로그 전달 프로필을 생성하여 처리를 위해 로그를 로깅 서비스로 전달합니다.
  3. (PA-3200, PA-5200, PA-5450 또는 PA-7000에서는 지원되지 않음) **DHCP** 브로드캐스트 세션 옵션(기기 > 설정 > 세션 > 세션 설정).
  4. 보안 정책 규칙을 생성하여 **dhcp**을 **Application** 유형으로 허용합니다.
- 방화벽이 DHCP 서버가 아닌 경우 방화벽이 클라이언트에서 수신하는 DHCP 트래픽에 대해 EAL을 생성할 수 있도록 인터페이스를 DHCP 릴레이 에이전트로 구성합니다.
- DHCP 서버가 방화벽 인터페이스와 동일한 네트워크 세그먼트에 있는 경우 DHCP 서버 앞에 가상 유선 인터페이스를 배포하여 방화벽이 성능에 미치는 영향을 최소화하면서 초기 DHCP 교환의 모든 패킷에 대해 EAL을 생성하도록 합니다.
  1. 해당 영역으로 가상 회선 인터페이스를 구성하고 멀티캐스트 방화벽 옵션(네트워크 > 가상 회선 > 추가).
  2. 가상 와이어 영역 간에 DHCP 서버로 들어오고 나가는 DHCP 트래픽을 허용하는 규칙을 구성합니다. 정책은 서버가 현재 관찰하는 모든 기존 트래픽을 허용하고 나머지 규칙과 동일한 로그 포워딩 프로파일을 사용해야 합니다.
  3. DHCP 서버가 IP 주소를 새 요청에 임대로 할당하기 전에 활성 상태인지 확인하도록 허용하려면 DHCP 서버에서 서브넷의 나머지 부분으로 핑(ping)을 허용하도록 규칙을 구성하십시오.
  4. 트래픽 일치에 대한 로그를 포워딩하지 않는 DHCP 서버에서 들어오고 나가는 다른 모든 트래픽을 허용하도록 규칙을 구성합니다.
  5. 첫 번째 가상 와이어 인터페이스를 사용하도록 DHCP 서버 호스트를 구성하고 두 번째 가상 와이어 인터페이스를 사용하도록 네트워크 스위치를 구성합니다. 케이블 연결을 최소화하기 위해


©2023 Palo Alto Networks, Inc.

DHCP 서버 호스트를 방화벽에 직접 연결하는 대신 스위칭 인프라에서 격리된 VLAN을 사용할 수 있습니다.

- 네트워크의 현재 구성 또는 토폴로지로 인해 방화벽이 일반적으로 관찰하지 않는 DHCP 트래픽에 대한 가시성을 얻기 위해 탭 인터페이스를 사용하려는 경우 다음 구성을 모범 사례로 사용하십시오.
  1. 탭 인터페이스 및 해당 영역을 구성합니다.
  2. 나머지 규칙과 동일한 로그 전달 프로필을 사용하는 DHCP 트래픽과 일치하도록 규칙을 구성합니다.
  3. 방화벽의 세션 부하를 최소화하려면 다른 모든 트래픽을 삭제하도록 규칙을 구성하십시오.
  4. 탭 인터페이스를 네트워크 스위치의 포트 미러에 연결합니다.
- 네트워크 트래픽이 방화벽에 표시되지 않는 장치에 대한 데이터를 수집하려면 ERSPAN(Encapsulated Remote Switched Port Analyzer)을 사용하여 네트워크 스위치에서미러링된 트래픽을 GRE(Generic Routing Encapsulation) 터널을 통해 방화벽으로 보냅니다.

**STEP 9 |** 보안 정책 규칙에 로그 전달 프로필을 적용합니다.

IoT 보안에 대해미리 정의된 로그 전달 프로필을 규칙에 적용하거나 기존 프로필을 업데이트하거나 새 프로필을 만들어필요한 유형의 로그를 로깅 서비스에 전달하도록 합니다.

 ©2023 Palo Alto Networks, Inc.

# 디바이스 ID 구성

다음 작업을 완료하여 IoT 보안에서 방화벽 또는 Panorama로 IP 주소-디바이스 매핑 및 정책 규칙 권장 사항을 가져옵니다.



***Panorama***를 사용하여 여러 방화벽을 관리하는 경우 ***Palo Alto Networks***는 디바이스 ***ID*** 배포의 모든 방화벽을 ***PAN-OS 10.0*** 또는 이후 버전으로 업그레이드하는 것이 좋습니다. 디바이스를 일치 기준으로 사용하는 규칙을 생성하고 ***Panorama***가 ***PAN-OS 9.1*** 또는 이전 버전을 사용하는 방화벽으로 규칙을 푸시하는 경우 방화벽이 지원되지 않아 **디바이스** 일치 기준을 생략하여 정책 규칙 트래픽 일치에 문제가 발생할 수 있습니다.

**STEP 1 |** 허브에서 IoT 보안 라이선스를 활성화합니다.

1. IoT 보안 라이선스를 활성화하기 위해 이메일에서 받은 지침을 따르십시오.
2. IoT 보안 앱을 초기화합니다. 자세한 내용은 IoT 보안 시작하기 및 IoT 보안 모범 사례를 참조하십시오.
3. IoT 보안 정책을 적용하는 데 사용할 방화벽에 라이선스를 적용합니다.
4. 방화벽 또는 Panorama에서 라이선스를 새로 고칩니다.

**STEP 2 |** IoT 보안 앱에서 IoT 보안 정책을 정의합니다.

1. IoT 보안 앱에서 소스 디바이스 개체를 선택합니다.
2. 원본 디바이스 개체에 대한 새 정책 규칙 집합을 생성합니다.

   IoT 보안 앱으로 보안 정책 생성에 대한 자세한 내용은 보안 정책 권장 정책을 참조하십시오.
3. 변경 사항을 확인하기 위해 정책 규칙을 활성화합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** IP 주소-디바이스 매핑 및 정책 규칙 권장 사항을 방화벽 또는 Panorama로 가져옵니다.

1. 정책 규칙 권장 사항을 가져옵니다.
   - 방화벽에서 디바이스 > 정책 권장 > **IoT**를 선택합니다.
   - Panorama의 경우 **Panorama** > 정책 권장 사항 > **IoT**를 선택한 다음 Panorama가 관리하는 방화벽에 정책 규칙을 푸시합니다.

     푸시한 후 정책을 방화벽에 적용하려면 정책 규칙 권장 사항-정책 규칙 매핑을 생성하기 위해 방화벽의 정책 규칙을 동기화해야 합니다.

   정책 권장을 선택하면 방화벽 또는 Panorama가 IoT 보안과 통신하여 최신 정책 규칙 권장 사항을 가져옵니다. 정책 규칙 권장 사항은 방화벽이나 Panorama에 캐시되지 않습니다.

   ***IoT Security***는 디바이스에 대한 신뢰할 수 있는 동작을 사용하여 정책 규칙 권장 사항을 생성하므로 규칙의 기본 작업이 허용됩니다.
2. 소스 디바이스 프로파일을 선택합니다.
3. 대상 디바이스 프로파일 및 허용된 애플리케이션이 올바른지 확인합니다.
4. 정책 규칙을 가져오려면 정책 가져오기 규칙을 선택합니다.
5. (Panorama만 해당) 정책 규칙을 가져오려는 디바이스 그룹의 위치를 선택합니다.
6. 정책 규칙의 이름을 입력합니다.
7. (Panorama만) 대상 유형 (사전 규칙 기반 또는 사후 규칙 기반)을 선택합니다.
8. 규칙 이후를 선택하여 규칙베이스에서 규칙의 배치를 정의합니다.
   - 규칙 선택 없음 - 규칙을 규칙베이스의 맨 위에 배치합니다.
   - 기본 값 - 나열된 규칙 이후에 규칙을 배치합니다.

   보안 정책에서 디바이스 ***ID*** 규칙은 디바이스에 적용되는 기존 규칙 앞에 있어야 합니다.
9. 각 정책 규칙 권장 사항에 대해 이 프로세스를 반복하여 필요한 대상에 대한 각 디바이스 개체에 대한 액세스를 허용하는 규칙을 생성합니다.
10. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 4 |** 디바이스 ID를 사용하여 디바이스를 검색하고 보안 정책을 적용하려는 각 영역에서 디바이스 ID를 사용하도록 설정합니다.

기본적으로 Device-ID는 활성화된 영역의 모든 하위 네트워크를 매핑합니다. 포함 목록 및 제외 목록에서 Device-ID가 매핑하는 하위 네트워크를 수정할 수 있습니다.

가장 좋은 방법은 소스 영역에서 ***Device-ID***를 활성화하여 디바이스를 감지하고 보안 정책을 시행하는 것입니다. 내부 영역에 대해서만 디바이스 ***ID***를 사용하도록 설정합니다.

1. 네트워크 > 영역을 선택합니다.
2. 디바이스 ID를 사용하도록 설정하려는 영역을 선택합니다.
3. 디바이스 식별을 활성화한 다음 확인을 클릭합니다.

**STEP 5 |** 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 보안 정책이 올바른지 확인합니다.

1. 정책을 선택한 다음 정책 규칙 권장 사항에서 만든 규칙을 선택합니다.

   IoT Security는 소스 디바이스 개체와 태그를 포함하는 설명을 할당하여 소스 디바이스 개체를 식별하고 이 규칙은 IoT 보안에서 권장사항입니다.

   디바이스 개체 이름은 고유해야 합니다.

2. 소스 탭을 선택한 다음 소스 디바이스 프로파일을 확인합니다.
3. 대상 탭을 선택한 다음 대상 디바이스 프로파일을 확인합니다.
4. 애플리케이션 탭을 선택한 다음 애플리케이션을 확인합니다.
5. 작업 탭을 선택한 다음 작업을 확인합니다(기본값은 허용).
6. 탐색을 사용하여 Cortex Data Lake가 로그를 수신하는지 확인하고 수신한 로그를 검토합니다.

**STEP 7 |** IoT 보안 정책 규칙 권장 사항이 없는 모든 디바이스에 대해 사용자 지정 디바이스 개체를 생성합니다.

예를 들어, 정책 규칙 권장 사항을 사용하여 랩톱 및 스마트폰과 같은 기존 IT 디바이스를 보호할 수 없으므로 보안 정책에서 사용할 이러한 유형의 디바이스에 대한 디바이스 개체를 수동으로 생성해야 합니다. 사용자 지정 디바이스 개체에 대한 자세한 내용은 디바이스 ID 관리을(를) 참조하십시오.

**STEP 8 |** 디바이스 개체를 사용하여 정책 규칙을 적용하고 잠재적인 문제를 모니터링하고 식별합니다.

다음 목록에는 디바이스 개체에 대한 몇 가지 예제 사용 사례가 포함됩니다.

- 보안, 인증, QoS 및 복호화 정책에서 원본 디바이스 개체 및 대상 디바이스 개체를 사용합니다.
- 복호화 로그를 사용하여 오류를 식별하고 암호화를 해독하는 데 가장 중요한 자산이 있는 자산을 식별합니다.
- ACC에서 디바이스 개체 활동을 확인하여 새 디바이스 및 디바이스 동작을 추적합니다.
- 디바이스 개체를 사용하여 맞춤 리포트(예: 인시던트 보고서 또는 감사)를 생성합니다.


©2023 Palo Alto Networks, Inc.

# 디바이스 ID 관리

정책 규칙 권장 사항 및 디바이스 개체가 최신인지 확인하거나 정책 규칙 권장 사항 매핑을 복원하기 위해 필요에 따라 다음 작업을 수행합니다.

**STEP 1 |** 새 업데이트 사용 가능한 열에 해당 권장 사항에 대한 예가 표시될 때마다 정책 규칙 권장 사항을 업데이트합니다.

디바이스가 새로운 기능을 확보함에 따라 IoT Security는 방화벽 또는 Panorama에서 허용해야 하는 추가 트래픽 또는 프로토콜을 조언하기 위해 정책 규칙 권장 사항을 업데이트합니다. 매일 IoT 보안에서 업데이트를 확인하고 가능한 한 빨리 정책 규칙 권장 사항을 업데이트하십시오.

1. IoT 보안 앱에서 정책 규칙을 편집한 후 다음을 클릭합니다.
2. 새 권장 사항을 선택하고 다음을 클릭합니다.
3. 변경 내용을 저장합니다.
4. 방화벽 또는 Panorama에서 정책 규칙 가져오기를 클릭한 다음 예를 클릭하여 현재 규칙을 덮어쓸 것임을 확인합니다.

   이 작업은 규칙 자체가 아니라 규칙에 대한 권장 사항을 덮어씁니다.

5. (Panorama 전용)모든 디바이스 그룹에 대한 이전 단계를 반복합니다.
6. 변경 사항을 커밋합니다.

**STEP 2 |** 디바이스 사전에서 디바이스 개체를 검토, 업데이트 및 유지 관리합니다.

*IoT* 보안 정책 규칙 권장 사항이 없는 디바이스에 대해 디바이스 개체를 만들어야 합니다. 예를 들어 *IoT* 보안 정책 규칙 권장 사항을 사용하여 랩톱 및 스마트폰과 같은 기존 *IT* 디바이스를 보호할 수 없으므로 이러한 유형의 디바이스에 대한 디바이스 개체를 생성하고 보안 정책에 사용하여 이러한 디바이스를 보호해야 합니다.

1. 개체 > 디바이스를 선택합니다.
2. 디바이스 개체를 추가합니다.
3. 목록을 찾아보기하거나 키워드를 사용하여 검색합니다.

   검색 결과에는 여러 유형의 디바이스 개체 특성(예: 카테고리 및 프로파일 모두)이 포함될 수 있습니다.
4. 맞춤 디바이스 개체를 추가하려면 디바이스 개체에 대한 이름과 선택적으로 설명을 입력합니다.

   항상 각 디바이스 개체에 대해 고유한 이름을 사용합니다. 디바이스 개체에 대한 설명의 태그를 정책 규칙 권장 사항에서 변경하지 마십시오.
5. (Panorama만) 이 디바이스 개체를 다른 디바이스 그룹에서 사용할 수 있도록 하려면 공유 옵션을 선택합니다.
6. 디바이스 개체의 속성(카테고리, **OS**, 프로파일, **Osfamily**, 모델 및 공급업체)을 선택합니다.
7. 확인을 클릭하여 변경 사항을 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 예를 들어 이전 구성을 복원하는 경우 정책 규칙 권장 규칙 매핑이 동기화되지 않을 수 있습니다. 또한 Panorama에서 Panorama가 관리하는 방화벽에 정책 규칙을 푸시한 후 각 방화벽의 매핑을 동기화해야 합니다. 매핑을 동기화하려면 다음을 수행합니다.

- 방화벽에서 디바이스 > 정책 권장 > **IoT** > 동기화 정책 규칙을 선택합니다.
- Panorama의 경우 **Panorama** > 정책 추천 > **IoT** > 동기화 정책 규칙을 선택합니다.

방화벽 또는 Panorama는 규칙 베이스의 모든 규칙을 검사하여 IoT 보안 정책 규칙 권장 사항으로 규칙을 식별하고 소스 디바이스 개체 정보를 가져오고 로컬 정책 규칙 권장 데이터베이스를 다시 채우는 태그를 확인합니다.

**STEP 4 |** 더 이상 필요하지 않은 정책 규칙 권장 사항을 삭제합니다.

정책 규칙 권장 사항이 더 이상 적용되지 않는 경우 이를 제거할 수 있습니다. 업데이트된 보안 정책을 적용하려면 정책 규칙 권장 사항에 대한 규칙도 제거해야 합니다.

1. IoT 보안 앱에서 삭제를 선택합니다.
2. 제거 상태 표시를 클릭하여 제거에 대한 이 권장 사항을 선택합니다.
3. 매핑을 제거합니다.
   - 방화벽에서 디바이스 > 정책 권장사항 > **IoT** > 정책 매핑 제거를 선택합니다.
   - Panorama의 경우 디바이스 > 정책 권장 > **IoT** > 정책 매핑 제거를 선택한 다음 매핑을 제거할 위치를 선택합니다.
4. 매핑 제거를 확인하려면 예를 클릭합니다.
5. 정책 > 보안을 선택합니다. Panorama의 경우 정책 > 보안 > 사전 규칙/사후 규칙을 선택합니다.
6. 제거할 정책 규칙 권장 사항에 대한 규칙을 선택한 다음 삭제를 선택합니다.
7. 변경 사항을 커밋합니다.

**STEP 5 |** CLI 명령을 사용하여 방화벽과 IoT 보안 사이의 문제를 해결합니다.


©2023 Palo Alto Networks, Inc.

# 디바이스 ID에 대한 CLI 명령

다음 CLI 명령을 사용하여 방화벽과 IoT Security 간의 문제를 해결하기 위한 정보를 봅니다. 일반적으로 나가는 데이터에 대한 **eal** show counters를 포함하는 CLI 명령과 들어오는 데이터에 대한 **icd** show counters가 포함된 CLI 명령입니다.

| 예시 | 명령 |
|---|---|
| EAL(고급 애플리케이션 로깅) 카운터(예: 방화벽과 Cortex Data Lake 간의 연결 수 및 로그 볼륨)를 봅니다. | **show iot eal all** |
| 방화벽과 Cortex Data Lake 간의 연결에 대해 자세히 알아보십시오. | **show iot eal conn** |
| PAN-OS 버전 및 일련번호와 같은 평면(데이터 평면 또는 관리 평면)별 EAL 카운터 요약을 봅니다. | **show iot eal dpi-eal** |
| 평면(데이터 평면 또는 관리 평면) 및 프로토콜별로 EAL 카운터를 봅니다. | **show iot eal dpi-stats all** |
| 프로토콜별로 EAL 카운터를 봅니다. | **show iot eal dpi-stats subtype dhcp\|http** |
| 호스트 정보 프로파일(HIP) 일치 보고서 카운터의 요약을 봅니다. | **show iot eal hipreport-eal** |
| EAL 로그 응답 시간 카운터를 봅니다. | **show iot eal response-time** |
| 방화벽과 IoT Security 앱 간의 에지 서비스 연결 상태에 대한 세부 정보와 IP 주소-디바이스 매핑 및 정책 규칙 권장 사항에 대한 카운터를 확인합니다. | **show iot icd statistics all** |
| 에지 서비스에 대한 연결을 위한 카운터를 봅니다. | **show iot icd statistics conn** |
| IP 주소-디바이스 매핑에 대한 카운터를 봅니다. | **show iot icd statistics verdict** |
| 방화벽에서 모든 IP 주소-디바이스 매핑을 봅니다. | **show iot ip-device-mapping-mp all** |
| 특정 IP 주소에 대한 IP 주소-디바이스 매핑을 봅니다. | **show iot ip-device-mapping-mp ip *IP-address*** |
| 데이터 평면에서 IP 주소-디바이스 매핑 목록을 봅니다. | **show iot ip-device-mapping all** |


©2023 Palo Alto Networks, Inc.

| 예시 | 명령 |
| --- | --- |
| 관리 평면에서 IP 주소-디바이스 매핑을 지웁니다. | **debug iot clear-all type device** |
| 데이터 평면에서 IP 주소 대 디바이스 매핑을 지웁니다. | **clear user-cache all** |


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

# 위협 방지

Palo Alto Networks®의 차세대 방화벽 위협 침입 방지 구독은 위협 환경의 전체 영역에 대처하기 위해 다각적인 탐지 메커니즘을 사용하여 상용 위협 및 고급 지속적 위협(APT)으로부터 네트워크를 보호하고 보호합니다. 위협 방지 솔루션은 다음 세 가지 구독으로 구성됩니다.

- 위협 방지 - 핵심 위협 방지 구독은 다양한 Palo Alto Networks 서비스에서 수집한 악성 트래픽 데이터에서 생성된 서명을 기반으로 합니다. 이러한 서명은 방화벽에서 다음과 같은 특정 위협에 기반한 보안 정책을 적용하는 데 사용됩니다: C2(명령 및 제어), 다양한 유형의 알려진 맬웨어 및 취약성 악용; 방화벽의 App-ID 및 User-ID 식별 기술과 결합하여 컨텍스트 데이터를 상호 참조하여 세분화된 정책을 생성할 수 있습니다. 위협 완화 정책의 일환으로 알려지거나 위험한 파일 형식과 IP 주소를 식별하고 차단할 수도 있으며, 이 중 방탄 서비스 공급자 및 알려진 악성 IP를 지정하는 목록을 포함하여 미리 만들어진 여러 범주를 사용할 수 있습니다. 특수 도구 및 소프트웨어를 사용하는 경우 고유한 취약성 서명을 만들어 네트워크의 고유한 요구 사항에 맞게 침입 방지 기능을 사용자 지정할 수 있습니다.
- 고급 위협 방지 - 고급 위협 방지 클라우드 서비스는 인라인 딥 러닝 및 기계 학습 모델을 사용하여 이전에는 볼 수 없었던 알려지지 않은 C2 위협을 회피적으로 실시간으로 시행합니다. 대기 시간이 매우 짧은 네이티브 클라우드 서비스인 이 확장 가능하고 무한히 확장 가능한 솔루션은 모델 교육 개선 사항을 통해 항상 최신 상태로 유지됩니다. 고급 위협 방지 라이선스에는 위협 방지에 포함된 모든 이점이 포함됩니다.
- DNS 보안 - 고급 DNS 기반 위협으로부터 조직을 보호하도록 설계된 DNS 보안 클라우드 서비스입니다. DNS Security는 다양한 위협 인텔리전스 원본에 고급 기계 학습 및 예측 분석을 적용하여 향상된 DNS 서명 집합을 생성하고 DNS 요청에 대한 실시간 분석을 제공하여 새로 생성된 악성 도메인으로부터 네트워크를 보호합니다. DNS 보안은 DNS 터널링, DNS 재바인딩 공격, 자동 생성을 사용하여 만든 도메인, 맬웨어 호스트 등을 비롯한 다양한 C2 위협을 탐지할 수 있습니다. DNS 보안은 완전한 DNS 위협 범위를 위해 고급 위협 방지 또는 위협 방지 구독이 필요하고 이와 함께 작동합니다.

Palo Alto Networks 침입 방지 구독은 함께 작동하여 공격 프로세스의 다양한 단계에서 체인을 가로채고 끊는 포괄적인 솔루션을 제공하고 네트워크 인프라의 보안 침해를 방지하는 가시성을 제공합니다.

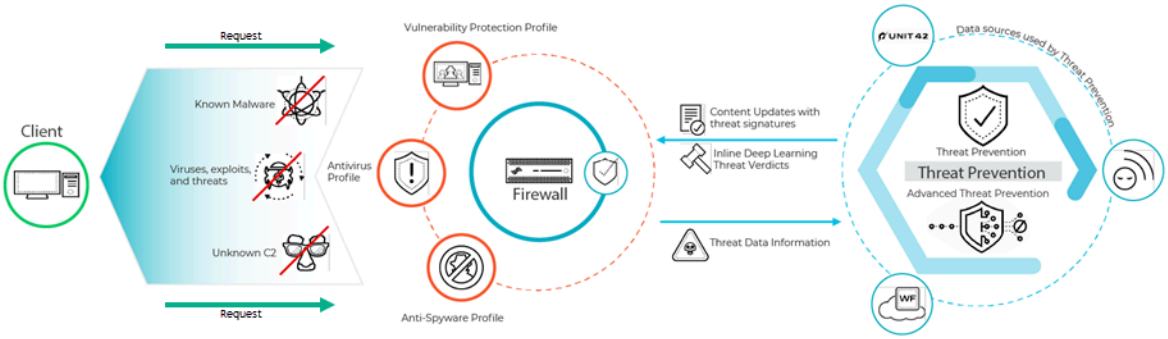

- 위협 방지 정보
- 고급 위협 방지
- 레이어 4 및 레이어 7 이베이전으로부터 네트워크를 보호하기 위한 모범 사례
- 바이러스 백신, Palo Alto Networks 및 취약점 보호 설정
- DNS 보안
- DNS 쿼리를 사용하여 네트워크에서 감염된 호스트 식별
- 데이터 필터링 설정
- 사전 정의된 데이터 필터링 패턴
- 데이터 필터링 프로파일 생성
- 인라인 클라우드 분석 구성
- WildFire Inline ML
- 파일 차단 설정

- 무차별 대입 공격 방지
- 무차별 암호 대입 서명에 대한 작업 및 트리거 조건 사용자 지정
- 회피 서명 활성화
- 차단된 IP 주소 모니터링
- 위협 서명 카테고리
- 위협 예외 생성
- 사용자 정의 서명
- 위협에 대해 자세히 알아보기 및 평가
- Palo Alto Networks와 위협 인텔리전스 공유
- 위협 예방 리소스


 ©2023 Palo Alto Networks, Inc.

# 위협 방지 정보

위협 예방은 방화벽 및 클라우드에서 작동하는 구성 요소가 있는 다계층 방지 시스템을 사용하여 모든 포트와 프로토콜에서 악성 코드, 취약점 악용 및 C2(명령 및 제어)를 탐지하고 차단할 수 있는 IPS(침입 방지 시스템) 솔루션입니다. 위협 예방 클라우드는 Palo Alto Networks 서비스의 결합된 위협 데이터를 사용하여 다양한 탐지 서비스를 운영하여 각각 특정 식별 가능한 패턴을 가진 서명을 생성하고, 위협과 악성 행동이 일치하는 경우 방화벽에서 보안 정책을 시행하는 데 사용합니다. 이러한 서명은 위협 유형에 따라 분류되며 고유한 식별자 번호가 할당됩니다. 이러한 시그니처에 해당하는 위협을 탐지하기 위해 방화벽은 비정상적인 특성을 나타내는 네트워크 트래픽을 검사하고 분류하는 분석 엔진을 작동합니다. 시그니처 기반 탐지 메커니즘 외에도 고급 위협 예방은 알려지지 않은 회피형 C2 위협을 방지하기 위해 보완적인 인라인 탐지 시스템을 제공합니다. 고급 위협 예방 클라우드는 제로 데이 위협이 네트워크에 침입하는 것을 방지하기 위해 요청별로 방화벽에서 인라인 분석 기능을 활성화하는 확장 가능한 딥 러닝 모델을 운영합니다.




방화벽에서 사용하는 위협 서명은 바이러스 백신, 스파이웨어 방지, 취약성의 세 가지 유형으로 크게 분류되며 해당 보안 프로파일에서 사용자 정의 정책을 시행하는 데 사용됩니다.

*Palo Alto Networks* 클라우드 제공 보안 서비스는 위협 서명 대신 파일 형식을 지정할 수 있는 파일 형식 서명뿐만 아니라 해당 서비스에 대한 ***WildFire*** 및 ***DNS C2*** 서명도 생성합니다**.** 예를 들어 서명 예외로**.**

- 안티바이러스 서명은 웜, 트로이 목마 및 스파이웨어 다운로드를 비롯한 다양한 유형의 맬웨어 및 바이러스를 탐지합니다.
- 안티스파이웨어 서명은 손상된 호스트의 C2 스파이웨어가 폰홈 또는 외부 C2 서버로 신호를 보내려는 시도를 탐지합니다.
- 취약성 서명은 악용 시스템 취약성을 감지합니다.

서명에는 연결된 기본 작업과 함께 기본 심각도 수준이 있습니다. 예를 들어, 매우 악의적인 위협의 경우 둘 다 재설정 설정입니다. 이 설정은 Palo Alto Networks의 보안 권장 사항을 기반으로 합니다.

전문화된 내부 애플리케이션이 있는 배포 또는 오픈 소스 Snort 및 suricata 규칙이 사용되는 타사 인텔리전스 피드가 있는 배포에서는 맞춤형 보호를 위해 맞춤형 서명을 생성할 수 있습니다.

방화벽은 일일 안티바이러스 콘텐츠와 주간 애플리케이션 및 위협 콘텐츠 업데이트라는 두 가지 업데이트 패키지 형태로 서명 업데이트를 수신합니다. 안티바이러스 콘텐츠 업데이트에는 안티바이러스 및 안티스파이웨어 보안 프로파일에서 각각 사용하는 안티바이러스 서명 및 DNS(C2) 서명이 포함되며, 애플리케이션 및 위협 콘텐츠 업데이트에는 취약성 및 안티스파이웨어 보안 프로파일에서 사용되는 취약성 및 안티


©2023 Palo Alto Networks, Inc.

스파이웨어 서명이 포함됩니다. 업데이트 패키지에는 다른 서비스 및 하위 기능에서 활용하는 추가 콘텐츠도 포함됩니다. 자세한 내용은 동적 콘텐츠 업데이트를 참조하십시오.

## 고급 위협 방지

고급 위협 방지는 기존 위협 방지 라이선스와 함께 작동하여 C2(고급 및 회피적 명령 및 제어) 위협에 대한 보호 기능을 제공하는 클라우드 제공 보안 서비스입니다. 이를 통해 인라인 탐지기를 사용하여 실시간 트래픽 검사를 사용하여 알려지지 않은 위협을 방지할 수 있습니다. 고급 위협 방지 클라우드의 이러한 딥 러닝, ML 기반 탐지 엔진은 고급 C2 및 스파이웨어 위협에 대한 트래픽을 분석하여 제로 데이 위협으로부터 사용자를 보호합니다. 클라우드 기반 검색 엔진을 작동하면 사용자가 업데이트 패키지를 다운로드하거나 리소스를 소비할 수 있는 프로세스 집약적인 방화벽 기반 분석기를 운영할 필요 없이 자동으로 업데이트되고 배포되는 다양한 탐지 메커니즘에 액세스할 수 있습니다. 클라우드 기반 탐지 엔진 로직은 WildFire의 C2 트래픽 데이터 세트를 사용하여 지속적으로 모니터링 및 업데이트되며 고도로 정확한 탐지 향상을 위해 사람의 개입을 제공하는 Palo Alto Networks 위협 연구원의 추가 지원이 제공됩니다. 고급 위협 방지 딥 러닝 엔진은 HTTP, HTTP2, SSL, 알 수 없는 UDP 및 알 수 없는 TCP 애플리케이션을 통한 C2 기반 위협 분석을 지원합니다. 추가 분석 모델은 콘텐츠 업데이트를 통해 제공되지만 기존 모델에 대한 향상된 기능은 방화벽 업데이트가 필요 없는 클라우드 측 업데이트로 수행됩니다. 고급 위협 방지는 스파이웨어 방지 보안 프로파일에 있는 인라인 클라우드 분석에서 활성화되고 구성됩니다.

 ©2023 Palo Alto Networks, Inc.

# 레이어 4 및 레이어 7 이베이전으로부터 네트워크를 보호하기 위한 모범 사례

대부분의 레이어 4 및 레이어 7 공격으로부터 네트워크를 모니터링하고 보호하기 위한 몇 가지 권장 사항이 있습니다.

- 최신 PAN-OS 소프트웨어 버전 및 콘텐츠 릴리스 버전으로 업그레이드하여 최신 보안 업데이트를 받으십시오. 콘텐츠 및 소프트웨어 업데이트 설치를 참조하십시오.
- DNS 보안 활성화(위협 방지 및 DNS 보안 구독 라이선스 필요)을(를) 통해, 악의적인 DNS 요청을 싱크홀합니다. Palo Alto Networks는 안티 스파이웨어 프로파일에서 다음 DNS 보안 카테고리 구성 설정을 사용할 것을 권장합니다.

| SIGNATURE SOURCE | LOG SEVERITY | POLICY ACTION | PACKET CAPTURE |
|---|---|---|---|
| : Palo Alto Networks Content | | | |
| default-paloalto-dns | | sinkhole | extended-capture |
| : DNS Security | | | |
| Command and Control Domains | default (high) | sinkhole | extended-capture |
| Dynamic DNS Hosted Domains | default (informational) | sinkhole | disable |
| Grayware Domains | default (low) | sinkhole | disable |
| Malware Domains | default (medium) | sinkhole | disable |
| Parked Domains | default (informational) | sinkhole | disable |
| Phishing Domains | default (low) | sinkhole | disable |
| Proxy Avoidance and Anonymizers | default (low) | sinkhole | disable |
| Newly Registered Domains | default (informational) | sinkhole | disable |

  - 로그 심각도 설정의 경우 기본 설정을 사용합니다.
  - 정책 작업의 경우 모든 서명 소스를 싱크홀로 설정합니다.
  - 패킷 캡처의 경우 명령 및 제어 도메인을 확장 캡처로 설정합니다. 다른 모든 카테고리는 기본 설정으로 둡니다.

  관련 안티 스파이웨어 설정에 대한 자세한 내용은 모범 사례 인터넷 게이트웨이 안티 스파이웨어 프로파일을 참조하십시오.
- 활성 고급 위협 방지 구독이 있는 경우 인라인 클라우드 분석을 활성화하여 지능형 C2 위협을 실시간으로 차단합니다. 각 분석 엔진의 기본 작업은 경보이며, 해당 위협이 감지되면 위협 로그를 생성합니다. 그러나 Palo Alto Networks는 모든 분석 모델 작업을 **Reset-Both**로 설정할 것을 권장합니다. 이렇게 하면 일치하는 패킷이 삭제되고 클라이언트와 서버에 RST가 전송되어 연결이 끊어지고 위협 로그 항목이 생성됩니다.
- DNS 프록시 역할을 하고 회피 서명을 사용하도록 방화벽을 설정합니다.

  ***DNS*** 프록시는 방화벽 보안 정책 엔진의 일부가 아닙니다**.** 대신 ***TLS/HTTP*** 이베이전을 방지하는 데 중요한 도메인 대 ***IP*** 매핑을 유지하면서 ***DNS*** 호스트 이름을 확인하도록 방화벽에 지시합니다**.**

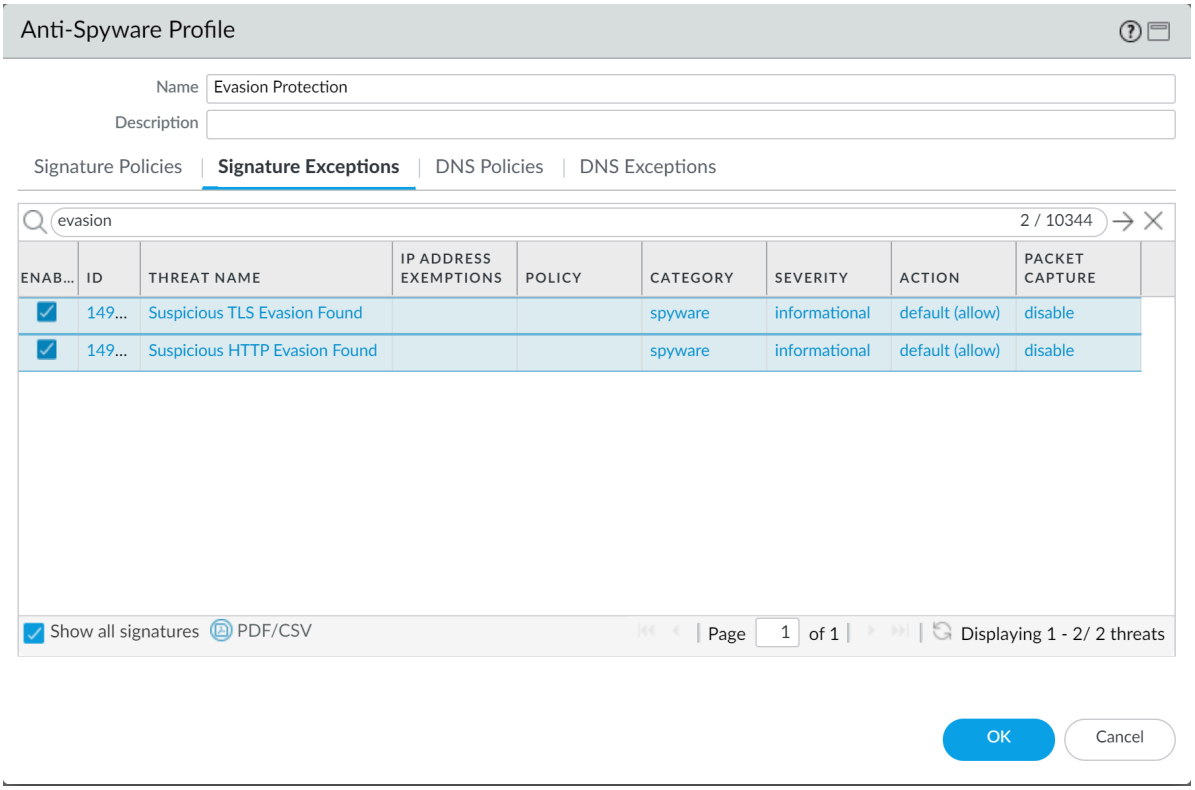
  - DNS 프록시 개체를 구성합니다.

    DNS 프록시 역할을 할 때 방화벽은 DNS 요청을 해결하고 호스트 이름-IP 주소 매핑을 캐시하여 향후 DNS 쿼리를 빠르고 효율적으로 해결합니다.
  - 회피 서명 활성화

    조작된 HTTP 또는 TLS 요청을 탐지하는 이베이전 서명은 클라이언트가 원래 DNS 요청에 지정된 도메인이 아닌 다른 도메인에 연결할 때 경고를 보낼 수 있습니다. 이베이전 서명을 활성화하기 전

 ©2023 Palo Alto Networks, Inc.

에 DNS 프록시를 구성해야 합니다. DNS 프록시가 없으면 이베이전 서명은 DNS 로드 밸런싱 구성의 DNS 서버가 동일한 DNS 요청에 대한 응답으로 동일한 리소스를 호스팅하는 서버에 대해 방화벽과 클라이언트에 다른 IP 주소를 반환할 때 경고를 트리거할 수 있습니다.



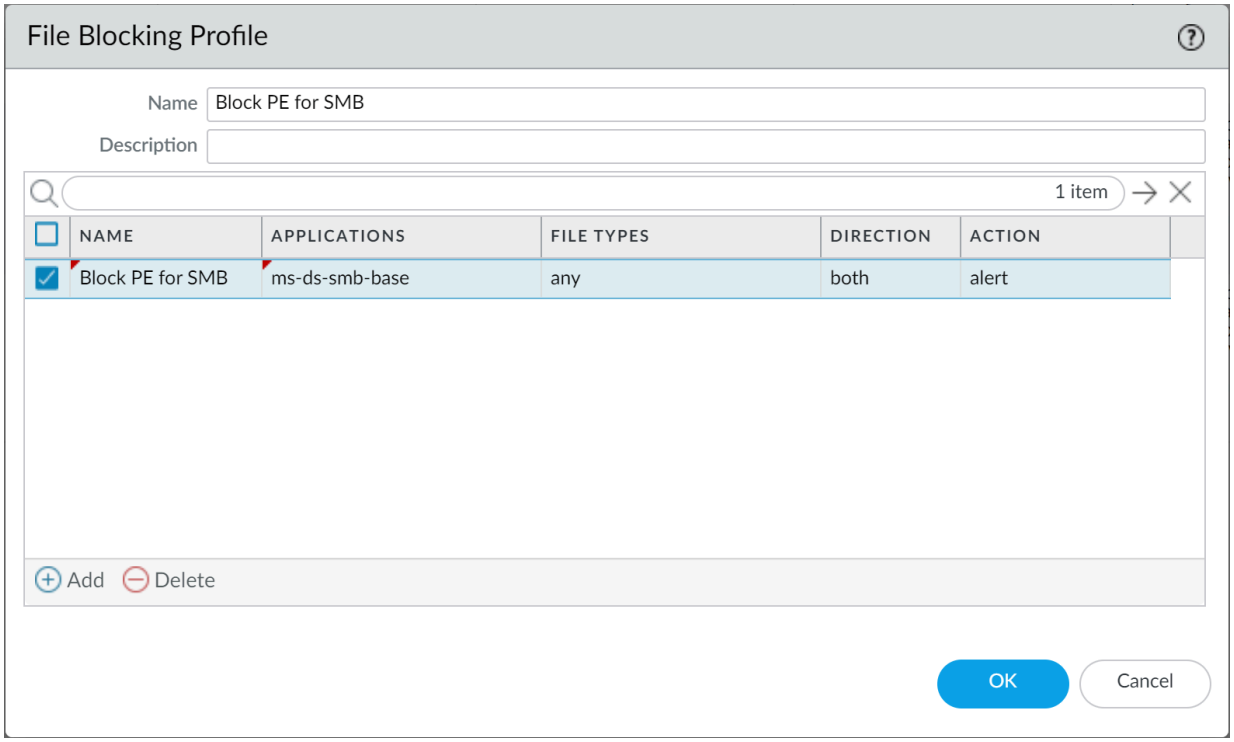

- Prisma Access를 운영하거나 내부 DNS 서버가 없는 네트워크를 운영하는 배포의 경우 기본 싱크홀 FQDN(sinkhole.paloaltonetworks.com) 대신 Palo Alto Networks 싱크홀 IP 주소(72.5.65.111)를 사용하도록 DNS 정책을 구성합니다.

  스파이웨어 방지 프로파일에서 사용하는 DNS 싱크홀을 사용하면 방화벽이 싱크홀 작업에 대해 구성된 카테고리와 지정된 싱크홀 서버와 일치하는 도메인에 대한 DNS 쿼리에 대한 응답을 위조하여 손상된 호스트를 식별하는 데 도움을 줄 수 있습니다. 기본 싱크홀 FQDN을 사용하는 경우 방화벽은 내부 DNS 서버가 CNAME 레코드를 확인할 것으로 예상하여 클라이언트에 대한 응답으로 CNAME 레코드를 전송하므로 클라이언트에서 구성된 싱크홀 서버로의 악의적인 통신이 기록되고 쉽게 식별할 수 있습니다. 그러나 클라이언트가 Prisma Access를 운영 중이거나, 내부 DNS 서버가 없는 네트워크에 있거나, CNAME을 A 레코드 응답으로 제대로 확인할 수 없는 다른 소프트웨어 또는 도구를 사용하는 경우 DNS 요청이 삭제되어 위협 분석에 중요한 트래픽 로그 세부 정보가 불완전해집니다.
- 서버의 경우 각 서버에서 제재하는 애플리케이션만 허용하도록 보안 정책 규칙을 만듭니다. 애플리케이션의 표준 포트가 서버의 수신 포트와 일치하는지 확인하십시오. 예를 들어, SMTP 트래픽만 이메일 서버에 허용되도록 하려면 애플리케이션을 **smtp**로 설정하고 서비스를 애플리케이션 기본값으로 설정


©2023 Palo Alto Networks, Inc.

합니다. 서버가 표준 포트의 하위 집합만 사용하는 경우(예: SMTP 서버가 포트 587만 사용하고 SMTP 애플리케이션에 25 및 587로 정의된 표준 포트가 있는 경우), 포트 587만 포함하는 새 사용자 지정 서비스를 만들고 보안 정책 규칙에서 application-default 대신 해당 새 서비스를 사용합니다. 또한 특정 소스 및 대상 영역과 IP 주소 집합에 대한 액세스를 제한해야 합니다.

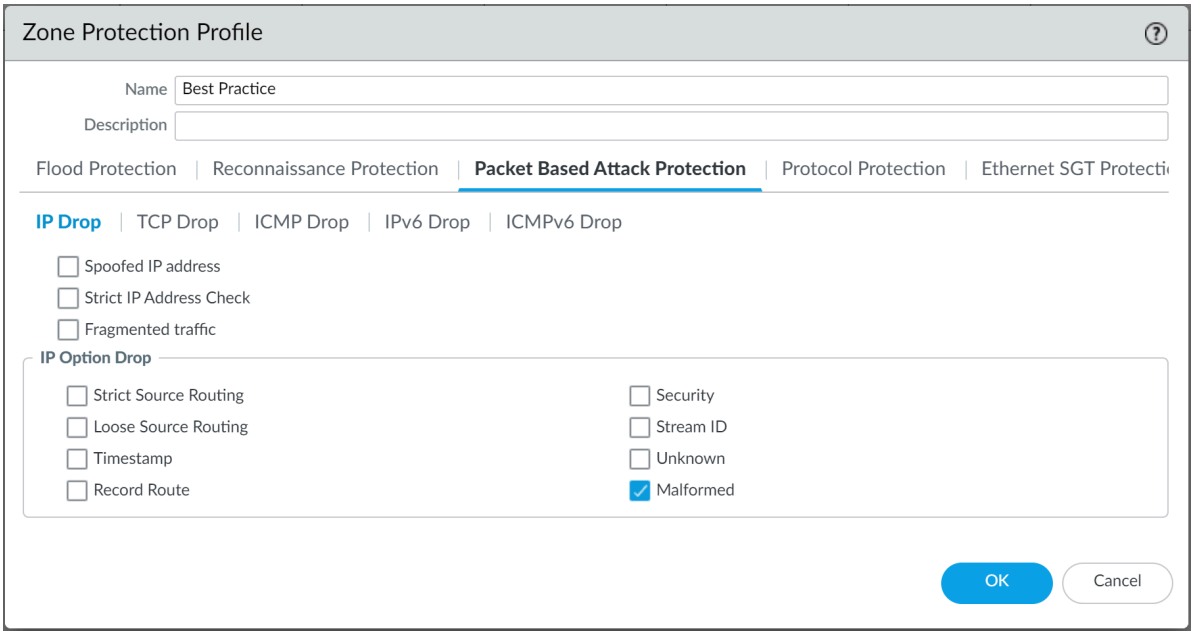
- 보안 정책을 사용하여 알 수 없는 모든 애플리케이션과 트래픽을 차단합니다. 일반적으로 알 수 없는 트래픽으로 분류되는 유일한 애플리케이션은 네트워크의 내부 또는 사용자 지정 애플리케이션과 잠재적 위협입니다. 알 수 없는 트래픽은 비준수 애플리케이션 또는 비정상적이거나 비정상적인 프로토콜이거나 둘 다 차단되어야 하는 비표준 포트를 사용하는 알려진 애플리케이션일 수 있습니다. 사용자 지정 또는 알 수 없는 애플리케이션 관리를 참조하십시오.
- 인터넷 기반 SMB(Server Message Block) 트래픽에 대한 PE(Portable Executable) 파일 형식이 트러스트에서 비신뢰 영역(ms-ds-smb 애플리케이션)으로 이동하는 것을 차단하도록 파일 차단을 설정합니다.




- PE(휴대용 실행 파일), ELF 및 MS Office 파일, PowerShell 및 셸 스크립트의 악성 변형을 실시간으로 차단합니다. WildFire Inline ML을(를) 활성화하면 방화벽에서 기계 학습을 사용하여 파일을 동적으로 분석할 수 있습니다. 이 추가 안티바이러스 보호 레이어는 WildFire 기반 서명을 보완하여 서명이 아직 존재하지 않는 파일에 대한 확장된 적용 범위를 제공합니다.


©2023 Palo Alto Networks, Inc.

- 패킷 기반 공격으로부터 보호하도록 구성된 영역 보호 프로파일을 생성합니다(네트워크 > 네트워크 프로파일 > 영역 보호).
  - **Malformed** IP 패킷을 삭제하는 옵션을 선택합니다(패킷 기반 공격 보호 > **IP** 드롭).




  - 삭제 불일치 겹치는 **TCP** 세그먼트 옵션(패킷 기반 공격 보호 > **TCP** 드롭)을 활성화합니다.

    공격자는 중복되지만 다른 데이터로 의도적으로 연결을 구성함으로써 연결 의도를 잘못 해석하고 의도적으로 거짓 긍정 또는 거짓 부정을 유도하려고 시도합니다. 공격자는 또한 IP 스푸핑 및 시퀀스 번호 예측을 사용하여 사용자의 연결을 가로채고 해당 연결에 자신의 데이터를 삽입합니다. 불일치 중복 **TCP** 세그먼트 옵션을 선택하면 PAN-OS가 일치하지 않고 중복 데이터가 있는 프레임을 버


©2023 Palo Alto Networks, Inc.

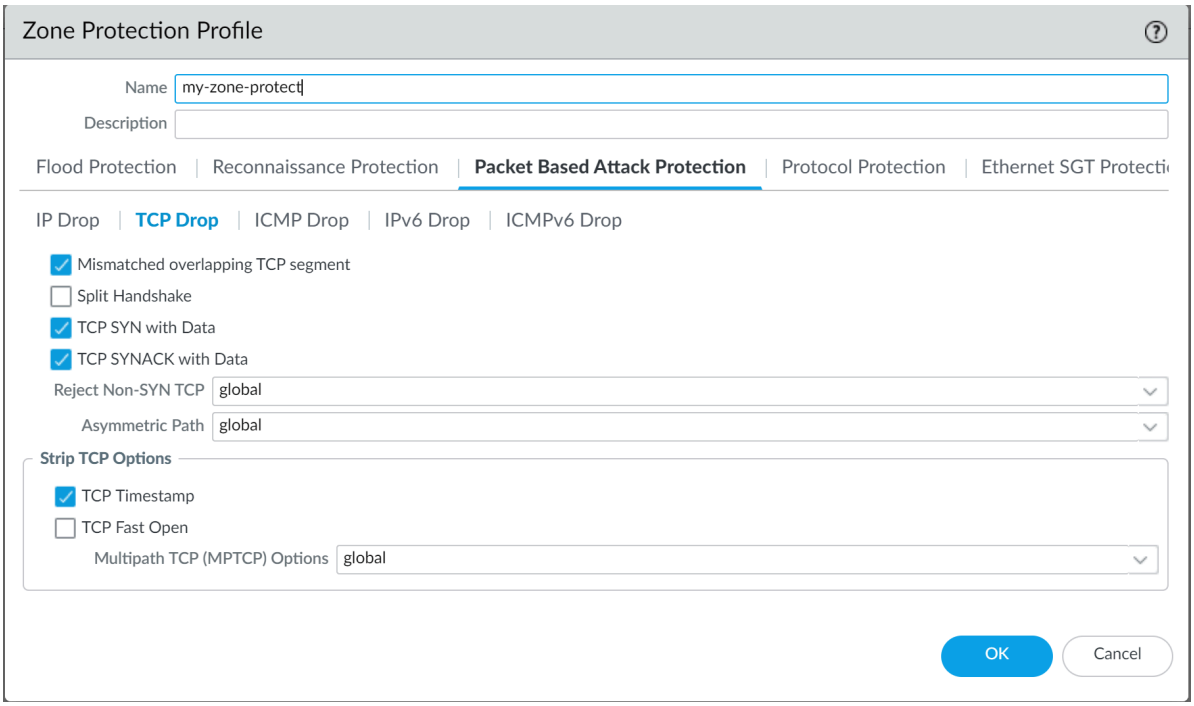
리도록 지정합니다. 수신된 세그먼트는 다른 세그먼트 내에 포함되어 있거나 다른 세그먼트의 일부와 겹칠 때 또는 다른 완전한 세그먼트를 포함할 때 삭제됩니다.

- 데이터가 있는 **TCP SYN** 삭제를 활성화하고 데이터 옵션이 있는 **TCP SYNACK**을 삭제합니다(패킷 기반 공격 보호 > **TCP** 삭제).

  3방향 핸드셰이크 중에 페이로드에 데이터가 포함된 SYN 및 SYN-ACK 패킷을 삭제하면 페이로드에 포함된 맬웨어를 차단하고 TCP 핸드셰이크가 완료되기 전에 무단 데이터 추출을 방지하여 보안을 강화합니다.

- 방화벽이 패킷을 포워딩하기 전에 SYN 패킷에서 TCP 타임스탬프를 제거합니다(패킷 기반 공격 보호 > **TCP** 삭제).

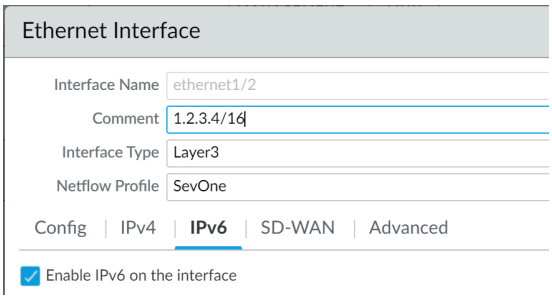
  스트립 **TCP** 옵션 **- TCP** 타임스탬프 옵션을 활성화하면 TCP 연결의 양쪽 끝에 있는 TCP 스택이 TCP 타임스탬프를 지원하지 않습니다. 이렇게 하면 동일한 시퀀스 번호에 대해 여러 패킷에서 다른 타임스탬프를 사용하는 공격을 방지할 수 있습니다.



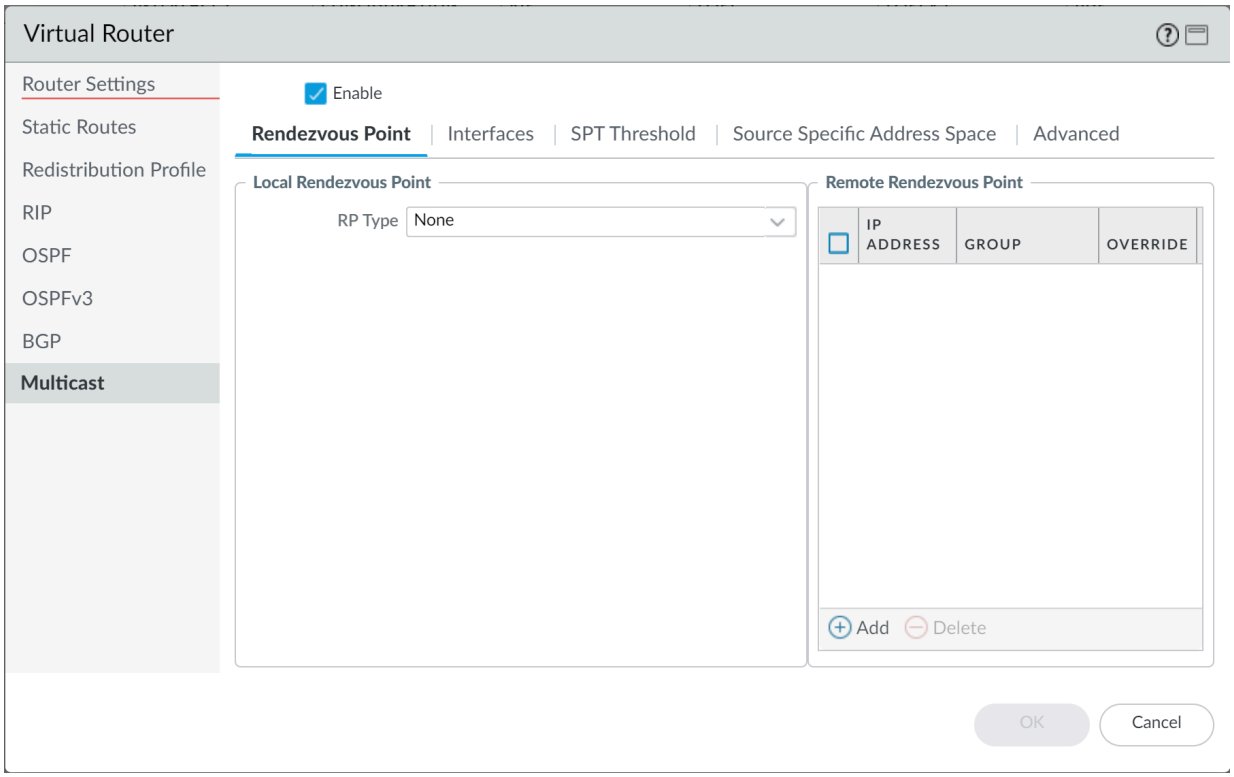

 ©2023 Palo Alto Networks, Inc.

- 네트워크 호스트에서 IPv6 주소를 구성하는 경우 아직 활성화되지 않은 경우 IPv6 지원을 활성화해야 합니다( 네트워크 > 인터페이스 > 이더넷 **> IPv6**).

  IPv6 지원을 활성화하면 IPv6 호스트에 대한 액세스가 허용되고 IPv4 패킷에 캡슐화된 IPv6 패킷도 필터링되므로 IPv4 멀티캐스트 주소를 통한 IPv6이 네트워크 정찰에 활용되지 않습니다.




- 방화벽이 멀티캐스트 트래픽에 대한 정책을 시행할 수 있도록 멀티캐스트 트래픽 지원을 활성화합니다(네트워크 > 가상 라우터 > 멀티캐스트).




 ©2023 Palo Alto Networks, Inc.

- **UDP** 콘텐츠 검사 대기열을 초과하는 데이터그램 포워딩 및 **TCP** 콘텐츠 검사 대기열을 초과하는 세그먼트 포워딩 옵션을 비활성화합니다(디바이스 > 설정 > 콘텐츠 **ID** > 콘텐츠 **ID** 설정).

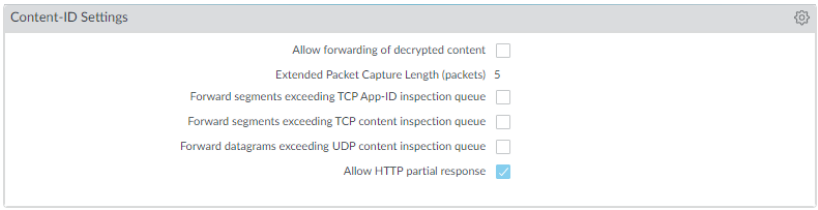
  기본적으로 TCP 또는 UDP 콘텐츠 검사 대기열이 가득차면 방화벽은 대기열 제한인 64를 초과하는 TCP 세그먼트 또는 UDP 데이터그램에 대한 콘텐츠 검사를 건너뜁니다. 이 옵션을 비활성화하면 방화벽이 허용하는 모든 TCP 및 UDP 데이터그램에 대한 콘텐츠 검사가 보장됩니다. 특정 상황에서만(예: 방화벽 플랫폼의 크기가 사용 사례에 맞게 적절하지 않은 경우) 이 설정을 비활성화하면 성능에 영향을 줄 수 있습니다.

- **HTTP** 부분 응답 허용(디바이스 > 설정 > **Content-ID** > **Content-ID** 설정)을 비활성화합니다.

  HTTP 부분 응답 옵션을 사용하면 클라이언트가 파일의 일부만 가져올 수 있습니다. 전송 경로에 있는 차세대 방화벽이 악성 파일을 식별하여 삭제하면 RST 패킷으로 TCP 세션을 종료합니다. 웹 브라우저가 HTTP 헤더 범위 옵션을 구현하면 파일의 나머지 부분만 가져오기 위해 새 세션을 시작할 수 있습니다. 이렇게 하면 방화벽이 초기 세션에 대한 컨텍스트 부족으로 인해 동일한 서명을 다시 트리거하는 것을 방지할 수 있으며, 동시에 웹 브라우저가 파일을 재조립하고 악성 콘텐츠를 포워딩할 수 있습니다. 이 옵션을 비활성화하면 이러한 일이 발생하지 않습니다.

  HTTP 부분 응답 허용은 기본적으로 방화벽에서 활성화되어 있습니다. 이는 최대 가용성을 제공하지만 성공적인 사이버 공격의 위험이 증가합니다. 최대 보안을 위해 이 옵션을 비활성화하면 악성 활동으로 인해 방화벽이 원래 세션을 종료한 후 웹 브라우저가 새 세션을 시작하여 파일의 나머지 부분을 가져오는 것을 방지할 수 있습니다. HTTP 부분 응답을 비활성화하면 RANGE 헤더를 사용하는 HTTP 기반 데이터 전송에 영향을 미치며, 이로 인해 특정 애플리케이션에 서비스 이상이 발생할 수 있습니다. HTTP 부분 응답을 비활성화한 후 비즈니스 크리티컬 애플리케이션의 작동을 검증하십시오.

  업무상 중요한 애플리케이션에서 HTTP 데이터 전송 중단이 발생하는 경우 해당 특정 애플리케이션에 대한 애플리케이션 재정의 정책을 만들 수 있습니다. 애플리케이션 재정의는 앱 ID(위협 및 콘텐츠 검사 포함) 를 우회하므로 특정 비즈니스 크리티컬 애플리케이션에 대해서만 애플리케이션 재정의 정책을 만들고 소스 및 대상을 지정하여 규칙을 제한합니다(최소 권한 액세스 원칙). 필요한 경우가 아니면 애플리케이션 재정의 정책을 생성하지 마십시오. 애플리케이션 재정의 정책에 대한 자세한 내용은 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0을 참조하십시오.

- 프로토콜 변칙과 심각도가 낮거나 높은 모든 취약점을 차단하는 취약점 보호 프로파일을 생성합니다.

  프로토콜 변칙은 프로토콜 동작이 표준 및 호환 사용에서 벗어날 때 발생합니다. 예를 들어, 잘못된 패킷, 잘못 작성된 애플리케이션 또는 비표준 포트에서 실행되는 애플리케이션은 모두 비정상적인 프로토콜로 간주되어 이베이전 도구로 사용될 수 있습니다.

  비즈니스의 최우선 순위가 애플리케이션 가용성인 미션 크리티컬 네트워크인 경우 일정 기간 동안 프로토콜 변칙에 대해 경고하여 중요한 내부 애플리케이션이 비표준 방식으로 확립된 프로토콜을 사용하지 않도록 해야 합니다. 특정 중요 애플리케이션이 프로토콜 변칙 서명을 트리거하는 경우 해당 애플리케이션을 프로토콜 변칙 적용에서 제외할 수 있습니다. 이렇게 하려면 프로토콜 변칙을 허용하는 다른


©2023 Palo Alto Networks, Inc.

규칙을 취약성 보호 프로파일에 추가하고 프로파일을 중요한 애플리케이션과 주고받는 트래픽을 적용하는 보안 정책 규칙에 연결합니다.

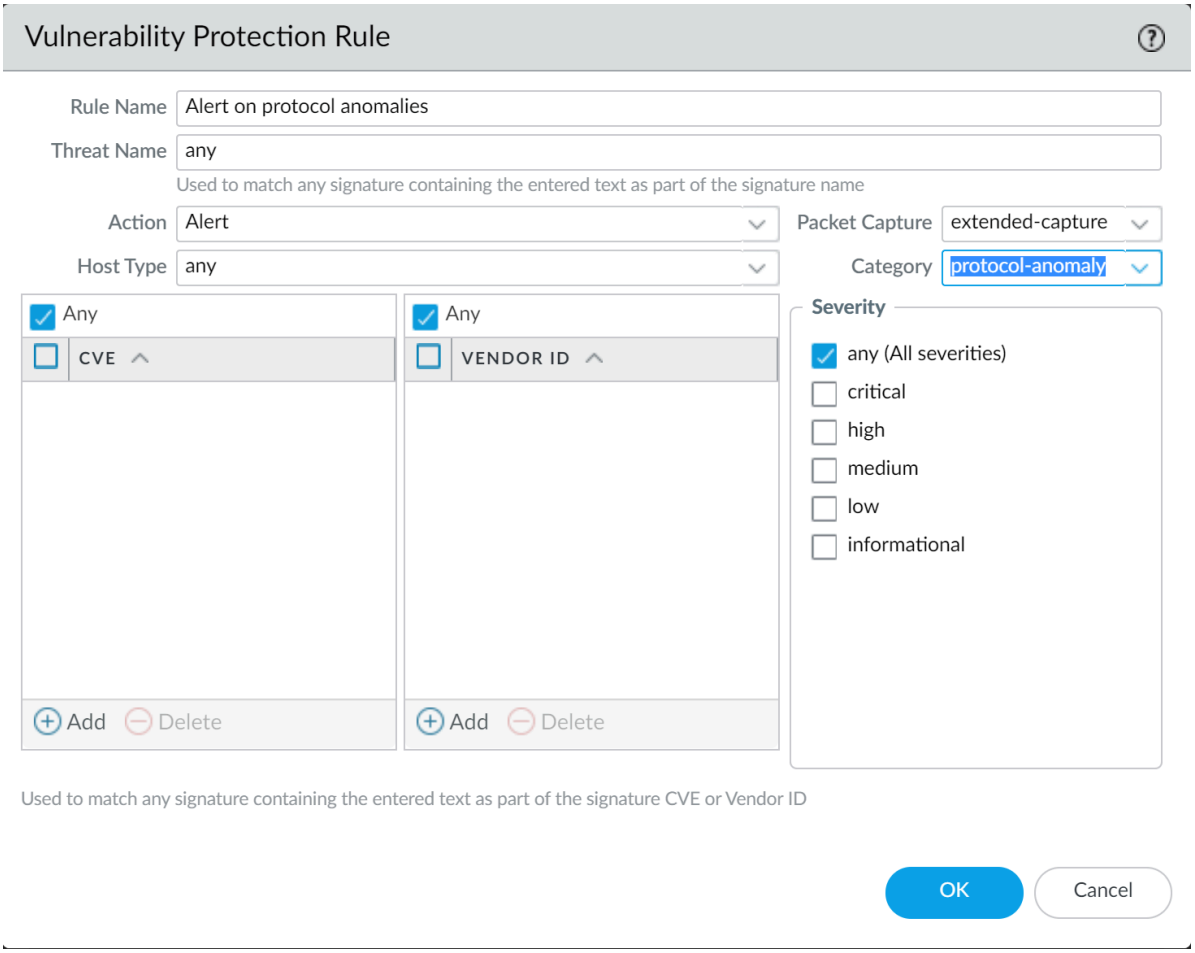
중요한 내부 애플리케이션에 대한 프로토콜 변칙을 허용하는 취약점 보호 프로파일 규칙 및 보안 정책 규칙이 프로토콜 변칙을 차단하는 규칙 위에 나열되어 있는지 확인합니다. 트래픽은 보안 정책 규칙 및 관련 Vulnerability Protection Profiles 규칙에 대해 위에서 아래로 평가되며 첫 번째 일치 규칙을 기반으로 시행됩니다.

- 프로토콜 변칙에 대해 경고하는 것으로 시작하십시오.

  작업은 경고로, 카테고리는 protocol-anomaly로, 심각성은 임의로 설정하여 취약점 보호 프로파일 규칙을 생성합니다. 트래픽을 모니터링하여 중요한 내부 애플리케이션이 비표준 방식으로 확립된

 ©2023 Palo Alto Networks, Inc.

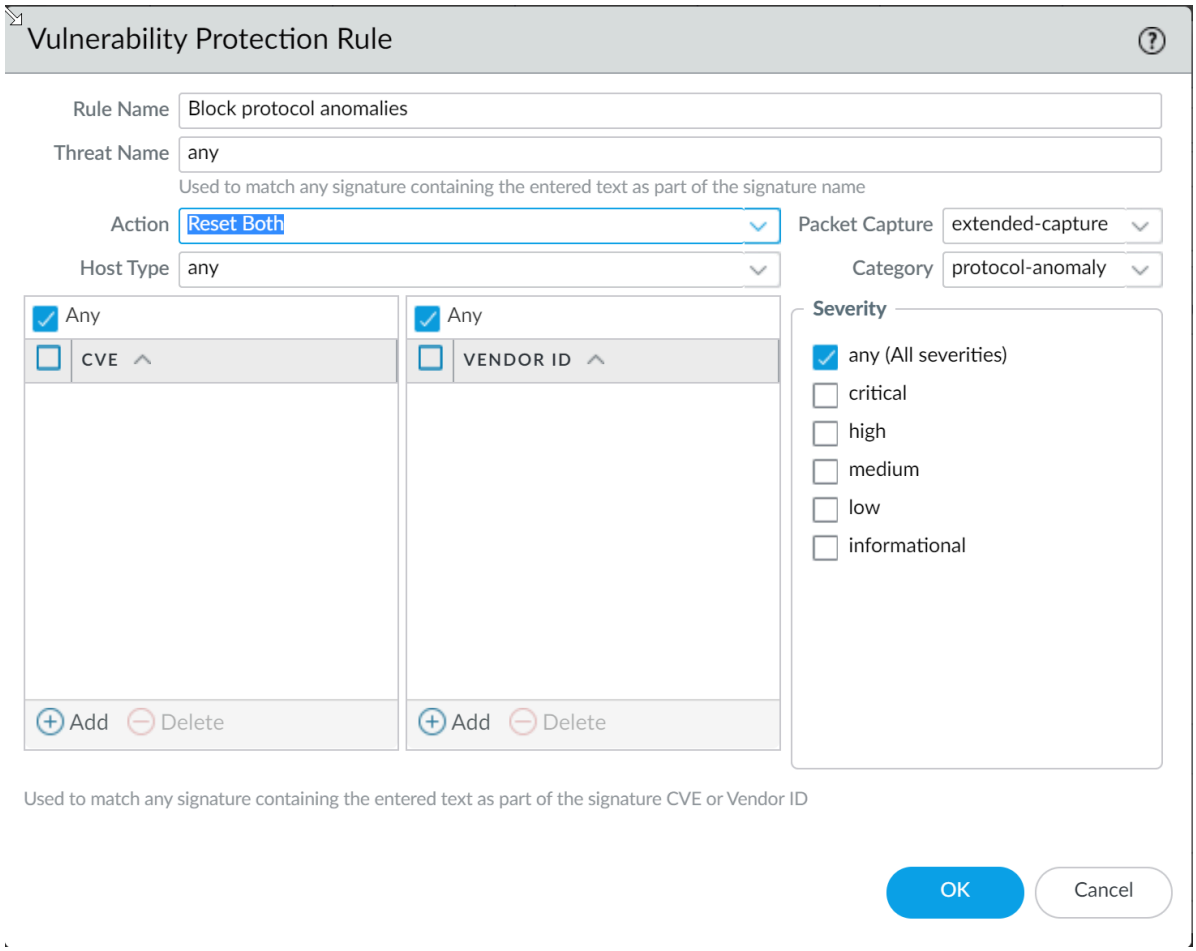
프로토콜을 사용하고 있는지 확인합니다. 이것이 사실인 경우 해당 애플리케이션에 대해 프로토콜 변칙을 계속 허용한 다음 다른 모든 애플리케이션에 대해 프로토콜 변칙을 차단합니다.




- 프로토콜 변칙 차단:

  카테고리가 프로토콜 변칙으로, 작업이 모두 재설정으로, 심각도가 모두로 설정된 취약점 보호 프로파일 규칙을 생성합니다.


©2023 Palo Alto Networks, Inc.

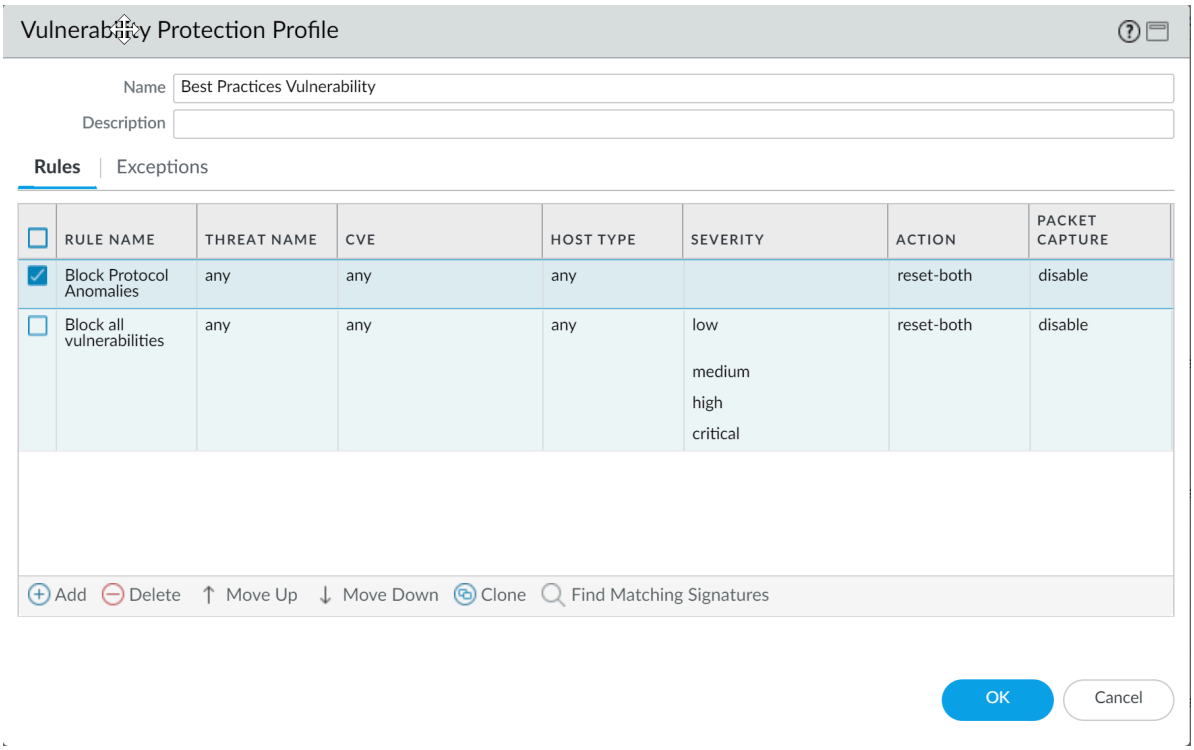



- 선택적으로 비표준 방식으로 확립된 프로토콜을 사용하는 중요한 애플리케이션에 대해 프로토콜 변칙을 허용합니다. 이렇게 하려면 프로토콜 변칙을 허용하는 취약성 보호 프로파일 규칙을 생성합니다. 규칙 작업을 허용으로, 카테고리를 프로토콜 변칙으로, 심각도를 임의로 설정합니다. 취약성


©2023 Palo Alto Networks, Inc.

보호 프로파일 규칙을 중요한 애플리케이션과 주고받는 트래픽을 적용하는 보안 정책 규칙에 연결합니다.

- 취약성 보호 프로파일에 다른 규칙을 추가하여 심각도가 낮거나 높은 모든 취약성을 차단합니다. 이 규칙은 프로토콜 변칙을 차단하는 규칙 뒤에 나열되어야 합니다.




- 서명 기반 보호를 제공하기 위해 보안 정책 규칙에 다음 보안 프로파일을 계속 연결합니다.
  - 심각도가 낮거나 높은 모든 스파이웨어를 차단하는 안티 스파이웨어 프로파일.
  - 바이러스 백신 서명과 일치하는 모든 콘텐츠를 차단하는 바이러스 백신 프로파일.


©2023 Palo Alto Networks, Inc.

# 바이러스 백신, Palo Alto Networks 및 취약점 보호 설정

모든 Palo Alto Networks 차세대 방화벽에는 보안 정책 규칙에 추가할 수 있는 사전 정의된 안티바이러스,, Palo Alto Networks 및 취약점 보호 프로파일이 함께 제공됩니다. 각 프로토콜에 대한 기본 작업(블록, HTTP,FTP 및 SMB 트래픽 및 SMTP, IMAP 및 POP3 트래픽에 대한 경고)을 사용하는 사전 정의된 바이러스 백신 프로파일이 하나 있습니다. 두 개의 사전 정의된 Palo Alto Networks 및 취약점 보호 프로파일이 있습니다.

- 기본값 - 모든 클라이언트 및 서버 심각도, 높음 및 중간 심각도 스파이웨어/취약성 보호 이벤트에 기본 작업을 적용합니다. 저조도 및 정보 이벤트를 감지하지 않습니다.
- 강력 - 모든 클라이언트 및 서버 중요, 높음 및 중간 심각도 스파이웨어/취약점 보호 이벤트에 블록 응답을 적용하고 저정보 이벤트에 기본 작업을 사용합니다.

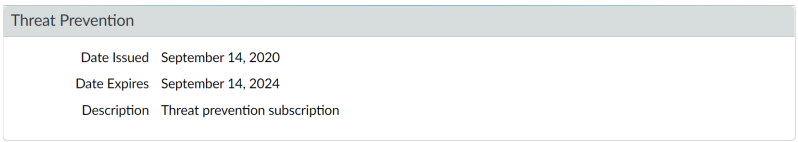
네트워크에 들어오는 트래픽에 위협이 없는지 확인하려면 미리 정의된 프로파일을 기본 웹 액세스 정책에 연결하십시오. 네트워크의 트래픽을 모니터링하고 정책 규칙 기반을 확장하면 특정 보안 요구 사항을 해결하기 위해 보다 세분화된 프로파일을 디자인할 수 있습니다.

다음 워크플로를 사용하여 기본 바이러스 백신, Palo Alto Networks 및 취약점 보호 보안 프로파일을 설정합니다.

*Palo Alto Networks*는 모든 스파이웨어 및 취약점 방지 서명에 대한 기본 작업을 정의합니다. 기본 작업을 보려면 개체 > 보안 프로파일 > 스파이웨어 방지 또는 개체 > 보안 프로파일 > 취약점 보호를 선택한 다음 프로파일을 선택합니다. 예외 탭을 클릭한 다음 모든 서명 표시를 클릭하여 서명 목록과 해당 기본 작업을 봅니다. 기본 작업을 변경하려면 새 프로파일을 생성하고 작업을 지정하거나 프로파일의 예외에 개별 서명 예외를 추가합니다.

**STEP 1 |** 위협 방지 구독이 있는지 확인합니다.

위협 방지 구독은 바이러스 백신, Palo Alto Networks 및 취약점 보호 기능을 하나의 라이선스로 번들로 묶습니다. 활성 위협 방지 구독이 있는지 확인하려면 디바이스 > 라이선스를 선택한 다음 위협 방지 만료 날짜가 향후인지 확인합니다.




**STEP 2 |** 최신 콘텐츠를 다운로드합니다.

1. 디바이스 > 동적 업데이트를 선택하고 페이지 하단의 지금 확인을 클릭하여 최신 서명을 검색합니다.
2. 작업 열에서 다운로드를 클릭하고 최신 바이러스 백신 업데이트를 설치한 다음 최신 애플리케이션 및 위협 업데이트를 다운로드한 다음 설치합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 콘텐츠 업데이트 일정을 조정합니다.

업데이트 배포에 대한 중요한 정보는 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례를 검토합니다.

1. 디바이스 > 동적 업데이트를 선택한 다음 예약을 클릭하여 바이러스 백신 및 애플리케이션 및 위협에 대한 서명 업데이트를 자동으로 검색합니다.
2. 업데이트의 빈도와 타이밍을 지정합니다.
   - 다운로드 전용 - 방화벽은 정의한 일정에 따라 최신 업데이트를 자동으로 다운로드하지만 수동으로 설치해야 합니다.
   - 다운로드 및 설치 - 방화벽은 정의한 일정에 따라 업데이트를 자동으로 다운로드하고 설치합니다.
3. 확인을 클릭하여 업데이트 일정을 저장합니다.
4. (선택 사항) 방화벽이 업데이트를 다운로드하기 전에 업데이트를 사용할 수 있게 된 후 최소 시간을 나타내는 임계값을 정의합니다. 예를 들어임계값을 **10**으로 설정하면 일정에 관계없이 방화벽이 업데이트가 10시간 이상 경과할 때까지 업데이트를 다운로드하지 않습니다.
5. (HA만 해당) 피어가 다운로드 및 설치 후 콘텐츠 업데이트를 동기화할 수 있도록 하는 피어에 동기화할지 여부를 결정합니다(업데이트 일정은 피어 간에 동기화되지 않으며 두 피어 모두에서 일정을 수동으로 구성해야 함).

   HA 배포에 따라 피어로 동기화할지의 여부를 결정하는 방법에 대한 추가 고려 사항이 있습니다.

   - 능동형/수동형 **HA**- 방화벽이 콘텐츠 업데이트에 MGT 포트를 사용하는 경우 두 방화벽을 예약하여 업데이트를 별도로 다운로드하고 설치합니다. 그러나 방화벽이 콘텐츠 업데이트에 데이터 포트를 사용하는 경우 수동 방화벽은 활성화될 때까지 업데이트를 다운로드하거나 설치하지 않습니다. 업데이트에 데이터 포트를 사용할 때 두 방화벽에서 일정을 동기화 상태로 유지하려면 방화벽에서 업데이트를 예약한 다음 피어 동기화를 활성화하여 방화벽이 활성 다운로드및 업데이트를 설치하고 업데이트를 패시브 방화벽으로 푸시합니다.
   - 능동형/능동형 **HA**- 방화벽이 콘텐츠 업데이트에 MGT 인터페이스를 사용하는 경우 두 방화벽 모두에서 다운로드 및 설치를 선택하지만 피어 동기화를 활성화하지는 않습니다. 그러나 방화벽이 데이터 포트를 사용하는 경우 방화벽이 두 방화벽에서 다운로드 및 설치를 선택한 다음 피어 동기화를 활성화하여 하나의 방화벽이 활성 보조 상태로 전환하면 활성 기본 방화벽이 업데이트를 다운로드하여 설치하고 활성 보조 방화벽으로 푸시합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택사항)바이러스 백신, Palo Alto Networks 및 취약점 보호를 위한 사용자 지정 보안 프로파일을 생성합니다.

또는 사전 정의된 기본 또는 엄격한 프로파일을 사용할 수 있습니다.

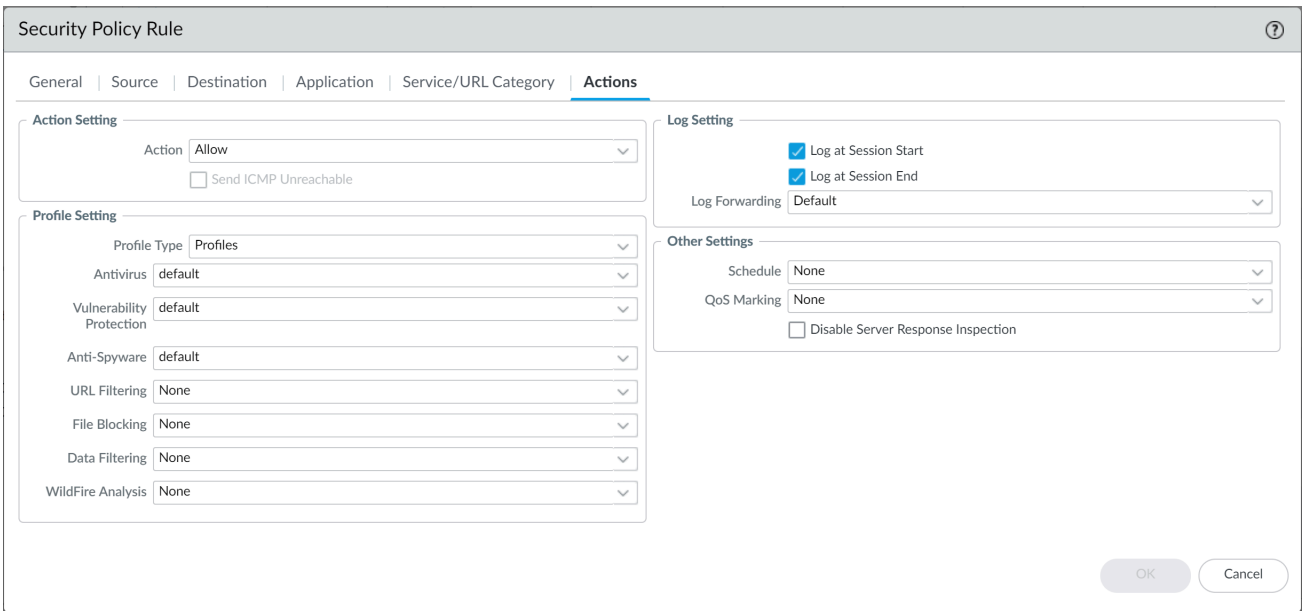
최고 보안 태세를 위해 모범 사례 보안 프로파일로 안전하게 전환합니다.

- 사용자 지정 바이러스 백신, 프로파일을 만들려면 개체 > 보안 프로파일 > 바이러스백신을 선택한 다음 새 프로파일을 추가합니다. 바이러스 백신 프로파일 전환 단계를 사용하여 목표를 안전하게 달성하십시오.
- 맞춤 안티 스파이웨어 프로파일을 만들려면 개체 > 보안 프로파일 > 안티 스파이웨어를 선택한 다음 새 프로파일을 추가합니다. Palo Alto Networks 프로파일 전환 단계를 사용하여 목표를 안전하게 달성하십시오.
- 사용자 지정 취약점 보호, 프로파일을 만들려면 개체 > 보안 프로파일 > 취약점 보호 기능을 선택한 다음 새 프로파일을 추가합니다. 취약성 보호 프로파일 전환 단계를 사용하여 목표를 안전하게 달성하십시오.

**STEP 5 |** 보안 정책 규칙에 보안 프로파일을 첨부합니다.

취약점 보호 프로파일을 사용하여 연결을 차단하는 보안 정책 규칙으로 방화벽을 구성하면 방화벽이 자동으로 하드웨어에서 해당 트래픽을 차단합니다(차단된 IP 주소 참조).

1. 정책 > 보안을 선택하고 수정할 규칙을 선택합니다.
2. 작업 탭에서 프로파일을 프로파일 유형으로 선택합니다.
3. **Antivirus**, **Anti-Spyware** 및 **Vulnerability Protection**에 대해 생성한 보안 프로파일을 선택합니다.




**STEP 6 |** 변경 사항을 커밋합니다.

커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# DNS 보안

DNS 보안은 DNS를 사용하는 지능형 위협으로부터 네트워크를 보호하고 방어하도록 설계된 지속적으로 진화하는 위협 방지 서비스입니다. Advanced 기계 학습 및 예측 분석을 활용하여 이 서비스는 실시간 DNS 요청 분석을 제공하고 C2 및 데이터 도난에 대한 DNS를 사용하여 멀웨어를 방어하도록 특별히 설계된 DNS 서명을 신속하게 생성하고 배포합니다. 확장 가능한 클라우드 아키텍처와 결합하여 확장 가능한 위협 인텔리전스 시스템에 대한 액세스를 제공하여 네트워크 보호를 최신 상태로 유지합니다.

- DNS 보안 정보
- 클라우드 제공 DNS 서명 및 보호
- DNS 보안 분석
- DNS 보안 활성화
- DNS 보안 데이터 수집 및 로깅

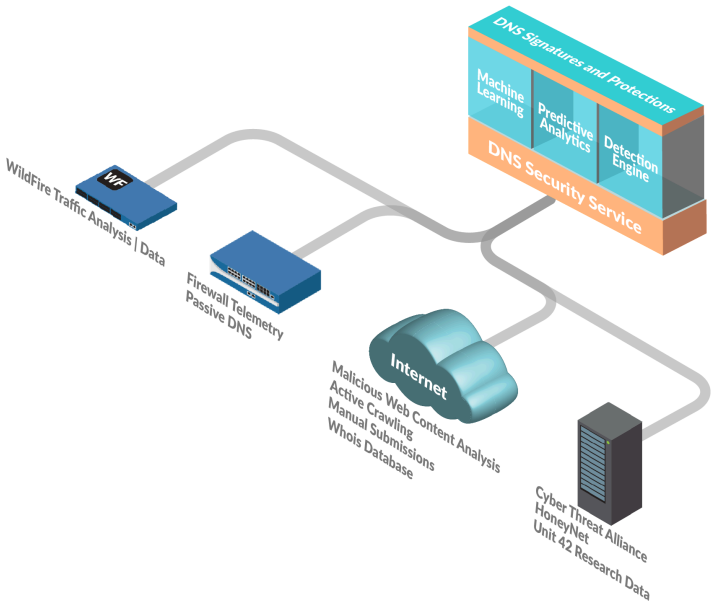
## DNS 보안 정보

활성 위협 예방 라이선스가 있는 고객은 Palo Alto Networks에서 생성한 도메인 목록을 사용하여 DNS 요청을 싱크홀하도록 방화벽을 구성할 수 있습니다. 로컬에서 액세스할 수 있는 사용자 지정 가능한 DNS 서명 목록은 바이러스 백신 및 WildFire 업데이트와 함께 패키지로 제공되며 게시 당시 정책 시행 및 보호에 가장 관련성이 높은 위협을 포함합니다. DNS를 사용하여 위협에 대한 향상된 적용 범위를 위해 DNS 보안 구독을 통해 사용자는 Advanced 예측 분석을 사용하여 실시간 보호에 액세스할 수 있습니다. DGA/DNS 터널링 탐지 및 기계 학습과 같은 기술을 사용하여 DNS 트래픽에 숨겨진 위협을 사전에 식별하고 무한 확장 가능한 클라우드 서비스를 통해 공유할 수 있습니다. DNS 서명 및 보호가 클라우드 기반 아키텍처에 저장되기 때문에 다양한 데이터 소스를 사용하여 생성된 계속 확장되는 서명의 전체 데이터베이스에 액세스할 수 있습니다. 이를 통해 새로 생성된 악성 도메인에 대해 실시간으로 DNS를 사용하여 일련의 위협으로부터 방어할 수 있습니다. 향후 위협에 대처하기 위해 콘텐츠 릴리스를 통해 DNS 보안 서비스의 분석, 탐지 및 방지 기능에 대한 업데이트를 사용할 수 있습니다.

DNS 보안 서비스에 액세스하려면 유효한 위협 예방 및 DNS 보안 라이선스가 있어야 합니다.

다음 워크플로는 DNS 보안 서비스가 다양한 데이터 원본을 사용하여 DNS 서명을 생성하는 방법을 설명합니다.

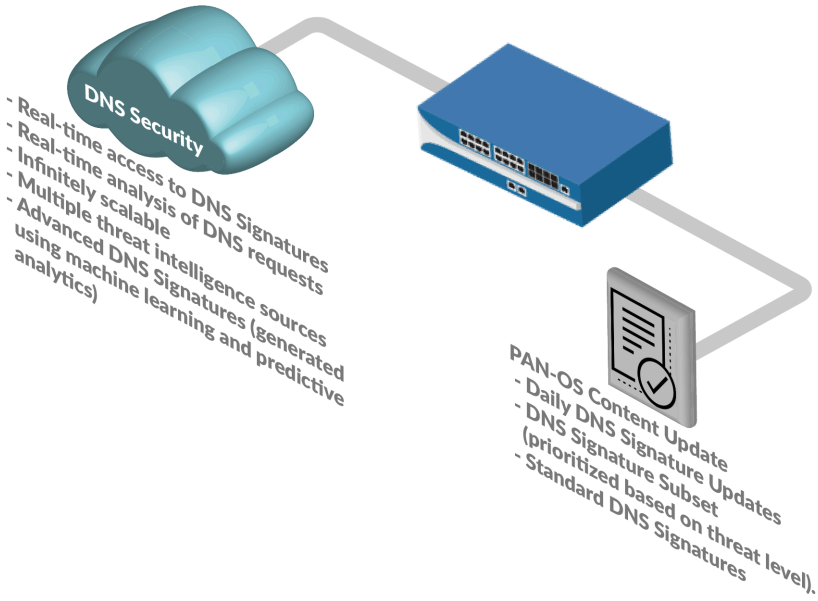

©2023 Palo Alto Networks, Inc.




# 클라우드 제공 DNS 서명 및 보호

클라우드 기반 서비스인 DNS Security를 사용하면 무한히 확장 가능한 DNS 서명 및 보호 소스에 액세스하여 악의적인 도메인으로부터 조직을 보호할 수 있습니다. Palo Alto Networks에서 생성한 도메인 서명 및 보호는 WildFire 트래픽 분석, 수동형 DNS, 능동형 웹 크롤링 및 악성 웹 콘텐츠 분석, URL 샌드박스 분석, Honeynet, DGA 리버스 엔지니어링, 원격 측정 데이터, 후이즈, Unit 42 연구 기관 및 Cyber Threat Alliance와 같은 타사 데이터 소스를 포함한 다양한 소스에서 파생됩니다. 이 온디맨드 클라우드 데이터베이스는 실시간 DNS 요청 분석은 물론 Advanced 분석 기술을 사용하여 생성된 서명을 포함하여 전체 Palo Alto Network의 DNS 서명 세트에 대한 액세스를 사용자에게 제공합니다. 로컬에서 다운로드 가능한 DNS 서명 세트(바이러스 백신 및 WildFire 업데이트와 함께 제공됨)에는 100,000개의 서명으로 하드 코딩된 용량 제한이 있으며 여기에 Advanced 분석을 통해 생성된 서명은 포함되지 않습니다. 하루 단위로 생성되는 신규 DNS 서명의 유입을 더 잘 수용하기 위해 클라우드 기반 서명 데이터베이스는 업데이트를 다운로드할 필요 없이 새로 추가된 DNS 서명에 대한 즉각적인 액세스를 사용자에게 제공합니다. 네트워크 연결이 끊어지거나 사용할 수 없는 경우 방화벽은 온박스 DNS 서명 세트를 사용합니다.


©2023 Palo Alto Networks, Inc.




# DNS 보안 분석

DNS 보안 서비스는 여러 DNS 데이터 소스에 대한 예측 분석 및 머신 러닝을 사용하여 실시간 DNS 요청 분석을 수행합니다. 이는 보안 정책 규칙에 첨부된 안티-스파이웨어 보안 프로파일 구성을 통해 실시간으로 접근할 수 있는 DNS 기반 위협에 대한 보호를 생성하는 데 사용됩니다. 각 DNS 위협 카테고리(DNS 서명 소스)를 사용하면 특정 서명 유형에 대한 로그 심각도 수준과 별도의 정책 작업을 정의할 수 있습니다. 이를 통해 네트워크 보안 프로토콜에 따라 위협의 속성을 기반으로 특정 보안 정책을 생성할 수 있습니다. Palo Alto Networks는 또한 PAN-DB 및 Alexa의 메트릭을 기반으로 명시적으로 허용되는 도메인 목록을 생성하고 유지 관리합니다. 이러한 허용 목록 도메인은 자주 액세스되며 악성 콘텐츠가 없는 것으로 알려져 있습니다. DNS 보안 카테고리 및 허용 목록은 PAN-OS 콘텐츠 릴리스를 통해 업데이트되고 확장 가능합니다.

AutoFocus를 사용하여 DNS Security Cloud 서비스에서 생성된 조직의 DNS 통계 데이터를 볼 수 있습니다. 이는 사용 가능한 DNS 카테고리를 기반으로 네트워크를 통과하는 DNS 요청의 분석을 설명하는 빠르고 시각적인 평가를 제공합니다. 또는 **test dns-proxy dns-signature fqdn <*domain*>** 명령을 사용하여 대기 시간 및 TTL과 같은 트랜잭션 세부 정보와 도메인 정보를 검색할 수 있습니다.

*PAN-OS 10.0* 버전 이상으로 업그레이드하면 *DNS* 보안 소스가 새로운 카테고리로 재정의되어 확장된 세부 제어를 제공합니다. 결과적으로 새 카테고리는 이전에 정의된 작업을 덮어쓰고 기본 설정을 얻습니다. 새로 정의된 *DNS* 보안 카테고리에 적절한 싱크홀, 로그 심각도 및 패킷 캡처 설정을 다시 적용해야 합니다.

DNS 보안 서비스는 현재 다음 DNS 위협 카테고리의 탐지를 지원합니다.

범용 위협 *ID* 번호(위협 로그에 *ID*로 표시됨)는 *DNS* 보안이 도메인을 분류하는 데 사용하는 특정 *DNS* 탐지 메커니즘에 매핑됩니다. 이는 도메인이 속하는 광범위하게 정의된 위협 카테고리와 함께 도메인의 정확한 카테고리화를 보여줍니다.


©2023 Palo Alto Networks, Inc.

- 명령 및 제어 도메인 - C2에는 악성 명령을 수신하거나 데이터를 추출(DNS 터널링 탐지 및 DGA 탐지 포함)하거나 권한 있는 DNS 서버(예: NXNSattack) 대상의 리소스를 고갈시키고 공격자의 원격 서버와 은밀하게 통신하기 위해 악성코드 및/또는 손상된 시스템에서 사용하는 URL 및 도메인이 포함됩니다.
  - **DNS** 터널 감지(UTID: 109001001/109001002) - 공격자는 DNS 터널링을 사용하여 DNS 쿼리 및 응답 내에서 비 DNS 프로그램 및 프로토콜의 데이터를 인코딩할 수 있습니다. 이는 공격자가 파일을 전송하거나 시스템에 원격으로 액세스할 수 있는 오픈 백 채널을 제공합니다. DNS 터널 감지는 기계 학습을 사용하여 도메인의 n-gram 빈도 분석, 엔트로피, 쿼리 속도 및 패턴을 포함하여 DNS 쿼리의 동작 품질을 분석하여 쿼리가 DNS 터널링 기반 공격과 일치하는지 확인합니다. 여기에는 TriFive 및 Snugy와 같이 탐지를 피하기 위해 여러 도메인에서 천천히 데이터를 유출하는 특정 차세대 DNS 터널링 멀웨어가 포함됩니다. 방화벽의 자동화된 정책 작업과 결합하여 DNS 터널에 숨겨진 C2 또는 데이터 도난을 신속하게 감지하고 정의된 정책 규칙에 따라 이를 자동으로 차단할 수 있습니다.
  - **DGA** 도메인 감지(UTID: 109000001) - 도메인 생성 알고리즘(DGA)은 일반적으로 악의적인 명령 및 제어(C2) 통신 채널을 설정하는 컨텍스트 내에서 많은 수의 도메인을 자동으로 생성하는 데 사용됩니다. DGA 기반 멀웨어(예: Pushdo, BankPatch 및 CryptoLocker)는 활성 C2 서버의 위치를 가능한 많은 수의 의심스러운 영역 내에서 숨겨 차단되는 도메인 수를 제한하고, 시간, 암호화 키, 사전 파생 명명 체계 및 기타 고유 값과 같은 요소를 기반으로 알고리즘적으로 생성될 수 있습니다. DGA에 의해 생성된 대부분의 도메인은 유효한 도메인으로 확인되지 않지만 발생한 위협으로부터 완전히 방어하려면 모두 식별되어야 합니다. DGA 분석은 DGA에서 발견되는 자주 사용되는 다른 기술을 리버스 엔지니어링하고 분석하여 도메인이 사람이 아닌 기계에 의해 생성되었을 가능성이 있는지의 여부를 결정합니다. 그런 다음 Palo Alto Networks는 이러한 속성을 사용하여 이전에 알려지지 않은 DGA 기반 위협을 실시간으로 식별하고 차단합니다.
  - **NXNSA**공격(UTID: 109010007) - DNS 프로토콜에 존재하는 NXNSAttack 취약점은 모든 중복 DNS 확인자에 영향을 미치며 악의적인 행위자가 DDos와 유사한 증폭 공격을 시작하여 취약한 권한 있는 DNS 서버의 정상적인 작동을 방해하는 데 사용할 수 있습니다. NXNSAttack은 재귀 DNS 확인자가 서버를 잠재적으로 종료하기 위해 많은 수의 잘못된 요청을 발행하도록 하여 권한 있는 DNS 서버에 대규모 트래픽 스파이크를 유발할 수 있습니다.
  - **DNS** 리바인딩(UTID: 109010009) - DNS 리바인딩 공격은 짧은 TTL 매개변수로 구성된 공격자가 제어하는 도메인으로 사용자를 유인하여 브라우저에서 동일 출처 정책을 악용하고 우회하기 위해 도메인 이름을 확인하는 방법을 조작합니다. 이를 통해 악의적인 행위자는 클라이언트 시스템을 중개자로 사용하여 사설 네트워크에 포함된 리소스를 공격하거나 액세스할 수 있습니다.
  - **DNS** 침입(UTID: 109001003) - DNS 침입에는 악의적인 행위자가 사기성 A(IPv4) 및 AAAA(IPv6) 레코드 요청에 대한 응답을 통해 미세한 페이로드를 숨기고 해결할 수 있도록 하는 DNS 쿼리가 포함됩니다. 클라이언트가 각각 인코딩된 구성 요소가 있는 A/AAAA 레코드를 포함하는 여러 하위 도메인을 확인할 때 그 안에 포함된 데이터를 통합하여 악성 페이로드를 형성한 다음 클라이언트 시스템에서 실행할 수 있습니다. 페이로드를 실행한 후 보조 페이로드를 도입하여 DNS 터널 또는 추가 익스플로잇을 설정할 수 있습니다.
- 동적 **DNS** 호스팅 도메인(UTID: 109020002) - DDNS(동적 DNS) 서비스는 고정 IP를 사용할 수 없을 때 특정 도메인에 연결된 IP 주소를 계속 변경하기 위해 호스트 이름과 IP 주소 간의 매핑을 거의 실시간으로 제공합니다. 이는 공격자가 DDNS 서비스를 사용하여 명령 및 제어 서버를 호스팅하는 IP 주소를 변경하여 네트워크에 침투하는 방법을 제공합니다. 멀웨어 캠페인 및 익스플로잇 킷은 페이로드 배포 전략의 일부로 DDNS 서비스를 활용할 수 있습니다. DDNS 도메인을 호스트 이름 인프라의 일부로 활용함으로써 공격자는 주어진 DNS 레코드와 연결된 IP 주소를 변경하고 탐지를 더 쉽게 피할 수 있습니다. DNS 보안은 다양한 소스의 DNS 데이터를 필터링 및 상호 참조하여 악용적인 DDNS 서비스를 감지하여 후보 목록을 생성한 다음 정확도를 최대화하기 위해 추가로 검증합니다.


©2023 Palo Alto Networks, Inc.

- 멀웨어 도메인 - 악성 도메인은 멀웨어를 호스팅 및 배포하며 다양한 위협(예: 실행 파일, 스크립트, 바이러스, 드라이브 바이 다운로드) 설치를 시도하는 웹사이트를 포함할 수 있습니다. 악성 도메인은 외부 소스를 통해 악성 페이로드를 네트워크에 포워딩한다는 점에서 C2 도메인과 구별되는 반면, C2의 경우 감염된 엔드포인트는 일반적으로 추가 지침이나 기타 악성 콘텐츠를 검색하기 위해 원격 서버에 연결을 시도합니다.
  - 맬웨어로 손상된 **DNS**(UTID: 109003001) - 맬웨어에 감염된 DNS는 겉보기에 진짜처럼 보이는 호스트 이름과 하위 도메인을 생성하는 다양한 기술을 다루며 일부는 합법적입니다. 실제로는 악성입니다. 여기에는 데이터베이스 중심 보안 솔루션을 가장하거나 오도하고 회피하기 위해 기존의 평판이 좋은 호스트 이름을 모방하는 새로 관찰된 호스트 이름이 포함됩니다. 이들은 데이터베이스 목록에 추가되는 것을 선점하기 위해 일괄적으로 신속하게 생성될 수 있습니다. 도메인 섀도잉은 일반적으로 공격자가 보다 일반적인 공격을 통해 도메인 계정에 대한 제어 권한을 얻은 후에 발생합니다. 이는 루트 도메인이 합법적이고 유효한 상태를 유지하더라도 공격을 조정하는 데 사용되는 불법 하위 도메인을 만드는 데 필요한 액세스를 제공하여 네트워크 보안을 우회할 가능성을 높입니다.
- 새로 등록된 도메인(UTID: 109020001) - 새로 등록된 도메인은 TLD 운영자가 최근에 추가했거나 지난 32일 이내에 소유권이 변경된 도메인입니다. 합법적인 목적을 위해 새 도메인을 생성할 수 있지만 대다수는 C2 서버로 작동하는 것과 같은 악의적인 활동을 조장하거나 멀웨어, 스팸, PUP/애드웨어를 배포하는 데 사용되는 경우가 많습니다. Palo Alto Networks는 특정 피드(도메인 레지스트리 및 등록 기관)를 모니터링하고 영역 파일, 수동형 DNS, WHOIS 데이터를 사용하여 등록 캠페인을 감지하여 새로 등록된 도메인을 감지합니다.
- 피싱 도메인(UTID: 109010001) - 피싱 도메인은 피싱 또는 파밍을 통해 합법적인 웹사이트로 가장하여 사용자가 개인 정보 또는 사용자 자격 증명과 같은 민감한 데이터를 제출하도록 유인합니다. 이러한 악의적인 활동은 소셜 엔지니어링 캠페인(신뢰할 수 있는 것처럼 보이는 소스가 사용자를 조작하여 이메일 또는 기타 전자 통신 형태를 통해 개인 정보를 제출하도록 조작) 또는 사용자를 합법적인 것처럼 보이는 사기 사이트로 안내하는 웹 트래픽 리디렉션을 통해 수행될 수 있습니다.
- 그레이웨어 도메인(UTID: 109010002) - (PAN-OS 콘텐츠 릴리스 8290 이상 설치 시 사용 가능). 그레이웨어 도메인은 일반적으로 직접적인 보안 위협을 가하지 않지만 공격 벡터를 촉진하거나 다양한 바람직하지 않은 동작을 생성하거나 단순히 의심스러운/공격적인 콘텐츠를 포함할 수 있습니다.여기에는 다음과 같은 웹사이트가 포함될 수 있습니다.
  - 사용자를 속여 원격 액세스를 허용하도록 시도합니다.
  - 애드웨어 및 기타 원치 않는 애플리케이션(예: 크립토마이너, 하이재커 및 PUP[잠재적 유해 프로그램])을 포함합니다.
  - 빠른 플럭스 기술을 사용하여 도메인 식별 은폐 작업 배포(**fastflux** 감지 - UTID: 109010005).
  - DNS 보안 예측 분석(악성 NRD)을 통해 입증된 대로 악의적인 동작 및 사용을 시연합니다(악의적 **NRD** - UTID: 109010006).
  - 웹 페이지 주소를 입력할 때 사용자 오류를 활용합니다(**typosquatting domains**).
  - 권한이 있는 DNS 서버의 부적절하게 구성되거나 오래된 DNS 레코드가 제거되거나 수정되지 않은 경우(Dangling DNS) 합법적인 소스에서 악성 웹사이트로 트래픽을 리디렉션합니다(**dangling DNS** - UTID: 109010008).
  - 불법 활동이나 사기를 조장합니다.
  - 악성 웹사이트로 트래픽을 라우팅하여 차단 목록을 회피하거나 와일드카드 DNS 공격을 활성화하는 데 사용할 수 있는 와일드카드 DNS 항목을 포함합니다(와일드카드 남용- UTID: 109002001).


©2023 Palo Alto Networks, Inc.

  - 수집된 DNS 데이터에서 구축된 설정된 기준 프로파일과 비교할 때 비정상적인 특성을 가진 DNS 트래픽의 존재를 나타냅니다(이상 탐지).
  - 몇 개월 또는 몇 년 전에 등록되어 활성화될 때 평판 확인을 우회하기 위해 휴면 상태로 남아 있습니다. 여기에는 본 적이 없거나 평가된 적이 없는 새로 관찰된 도메인도 포함됩니다(전략적으로 오래된 도메인- UTID: 109002002).
- 파킹된 도메인(UTID: 109010003) - PAN-OS 콘텐츠 릴리스 8318 이상 버전에서 사용 가능) 파킹된 도메인은 일반적으로 호스트 엔터티에 수익을 창출할 수 있는 클릭형 광고의 형태로 제한된 콘텐츠를 호스팅하는 비활성 웹사이트이지만, 일반적으로 최종 사용자에게 유용한 콘텐츠는 포함하지 않습니다. 이들은 종종 합법적인 플레이스 홀더 역할을 하거나 불편감을 주지만 멀웨어 배포의 가능한 벡터로 사용될 수도 있습니다.
- 프록시 회피 및 익명화(UTID: 109010004) -(PAN-OS 콘텐츠 릴리스 8340 이상 버전에서 사용 가능) 프록시 회피 및 익명화는 콘텐츠 필터링 정책을 우회하는 데 사용되는 서비스에 대한 트래픽입니다. 익명화 프록시 서비스를 통해 조직의 콘텐츠 필터링 정책을 우회하려는 사용자는 DNS 수준에서 차단됩니다.

## DNS 보안 활성화

DNS 보안을 사용하여 도메인 쿼리에 대해 DNS 싱크홀링을 활성화하려면 DNS 보안 구독을 활성화하고, DNS 보안 서비스를 참조하는 안티 스파이웨어 정책을 생성(또는 수정)하고, 각 DNS 서명 카테고리에 대한 로그 심각도 및 정책 설정을 구성하고, 그런 다음 보안 정책 규칙에 프로파일을 연결합니다.

**STEP 1 |** 구독 라이선스 활성화.

**STEP 2 |** 보안 정책의 ***paloalto-dns-security***가 DNS 보안 클라우드 보안 서비스의 트래픽을 활성화하도록 구성되었는지 확인합니다.



방화벽 배포가 ***App-ID*** 보안 정책을 시행하도록 구성된 인터넷 경계 방화벽을 통해 관리 트래픽을 라우팅하는 경우 경계 방화벽에서 ***App-ID***를 허용해야 합니다**.** 그렇게 하지 않으면 ***DNS*** 보안 연결이 차단됩니다**.**


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 정의된 싱크홀에 멀웨어 DNS 쿼리를 보내도록 DNS 보안 서명 정책 설정을 구성합니다.

외부 동적 목록을 도메인 허용 목록으로 사용하는 경우 ***DNS*** 보안 도메인 정책 작업보다 우선하지 않습니다. 결과적으로 ***EDL*** 및 ***DNS*** 보안 도메인 카테고리의 항목과 일치하는 도메인이 있는 경우 ***EDL***이 허용 작업으로 명시적으로 구성된 경우에도 ***DNS*** 보안에 지정된 작업이 계속 적용됩니다. ***DNS*** 도메인 예외를 추가하려면 경고 작업으로 ***EDL***을 구성하거나 ***DNS*** 예외 탭에 있는 ***DNS*** 도메인/***FQDN*** 허용 목록에 추가합니다(8단계).

1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택합니다.
2. 기존 프로파일을 만들거나 수정하거나 기존 기본 프로파일 중 하나를 선택한 다음 복제합니다.
3. 프로파일 이름을 지정하고 선택적으로 설명을 제공합니다.
4. **DNS** 정책 탭을 선택합니다.
5. 서명 원본 열의 DNS 보안 제목 아래에는 개별적으로 구성 가능한 DNS 서명 원본이 있으며 이를 통해 별도의 정책 작업과 로그 심각도 수준을 정의할 수 있습니다.

   *Palo Alto Networks*는 시그니처 소스에 대한 기본 ***DNS*** 정책 설정을 변경하여 최적의 적용 범위를 보장하고 발생 대응 및 치료를 지원할 것을 권장합니다. 레이어 4 및 레이어 7 이베이전(Evasion)으로부터 네트워크를 보호하기 위한 모범 사례에 설명된 대로 ***DNS*** 보안 설정을 구성하는 모범 사례를 따르십시오.

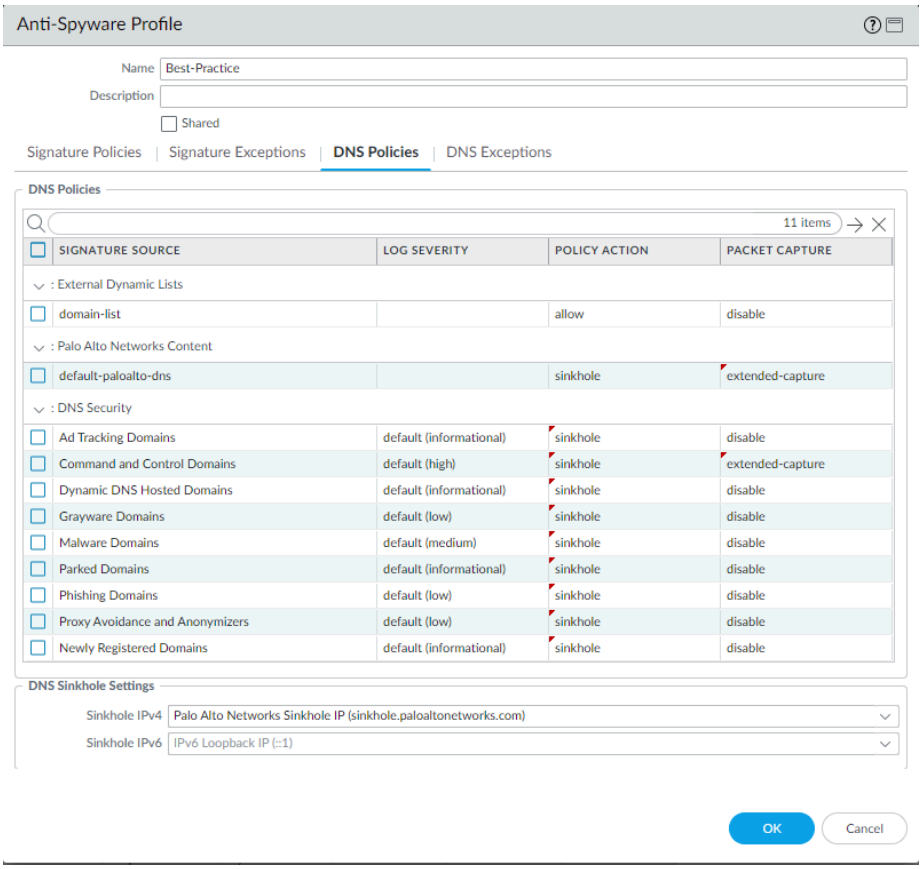
   - 방화벽이 DNS 서명과 일치하는 도메인을 감지할 때 기록되는 로그 심각도 수준을 지정합니다. 다양한 로그 심각도 수준에 대한 자세한 내용은 위협 심각도 수준을 참조하십시오.
   - DNS 보안 서명 소스에 대해 알려진 멀웨어 사이트에 대한 DNS 조회가 수행될 때 수행할 작업을 선택합니다. 옵션은 허용, 블록, 싱크홀 또는 기본값입니다. 작업이 싱크홀로 설정되어 있는지 확인합니다.
   - 각 DNS 서명 소스에 대해 해당 로그 심각도가 없음인 정책 작업을 허용으로 구성하여 DNS 트래픽 검사를 완전히 우회할 수 있습니다.
   - 패킷 캡처 드롭다운에서 단일 패킷을 선택하여 세션의 첫 번째 패킷을 캡처하거나 확장 캡처를 선택하여 1-50개 패킷 사이에서 설정합니다. 그런 다음 추가 분석을 위해 패킷 캡처를 사용할 수 있습니다.
6. **DNS** 싱크홀 설정 섹션에서 싱크홀이 활성화되어 있는지 확인합니다. 사용자의 편의를 위해 기본 싱크홀 주소(sinkhole.paloaltonetworks.com)가 Palo Alto Networks 서버에 액세스하도록

 ©2023 Palo Alto Networks, Inc.

설정되어 있습니다. Palo Alto Networks는 콘텐츠 업데이트를 통해 이 주소를 자동으로 새로 고칠 수 있습니다.

싱크홀 **IPv4** 또는 싱크홀 **IPv6** 주소를 네트워크의 로컬 서버나 루프백 주소로 수정하려면 네트워크의 로컬 서버에 대한 싱크홀 IP 주소 구성을(를) 참조하십시오.

7. 확인을 클릭하여 안티 스파이웨어 프로파일을 저장합니다.




**STEP 4 |** 안티 스파이웨어 프로파일을 보안 정책 규칙에 첨부합니다.

1. 정책 > 보안을 선택합니다.
2. 보안 정책 규칙을 선택하거나 생성합니다.
3. **Actions** 탭에서 **Log at Session End** 체크박스를 선택하여 로깅을 활성화합니다.
4. 프로파일 설정 섹션에서 프로파일 유형 드롭다운을 클릭하여 모든 프로파일을 봅니다. 안티 스파이웨어 드롭다운에서 새 프로파일 또는 수정된 프로파일을 선택합니다.
5. 확인을 클릭하여 정책 규칙을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 정책 작업이 적용되었는지 테스트합니다.

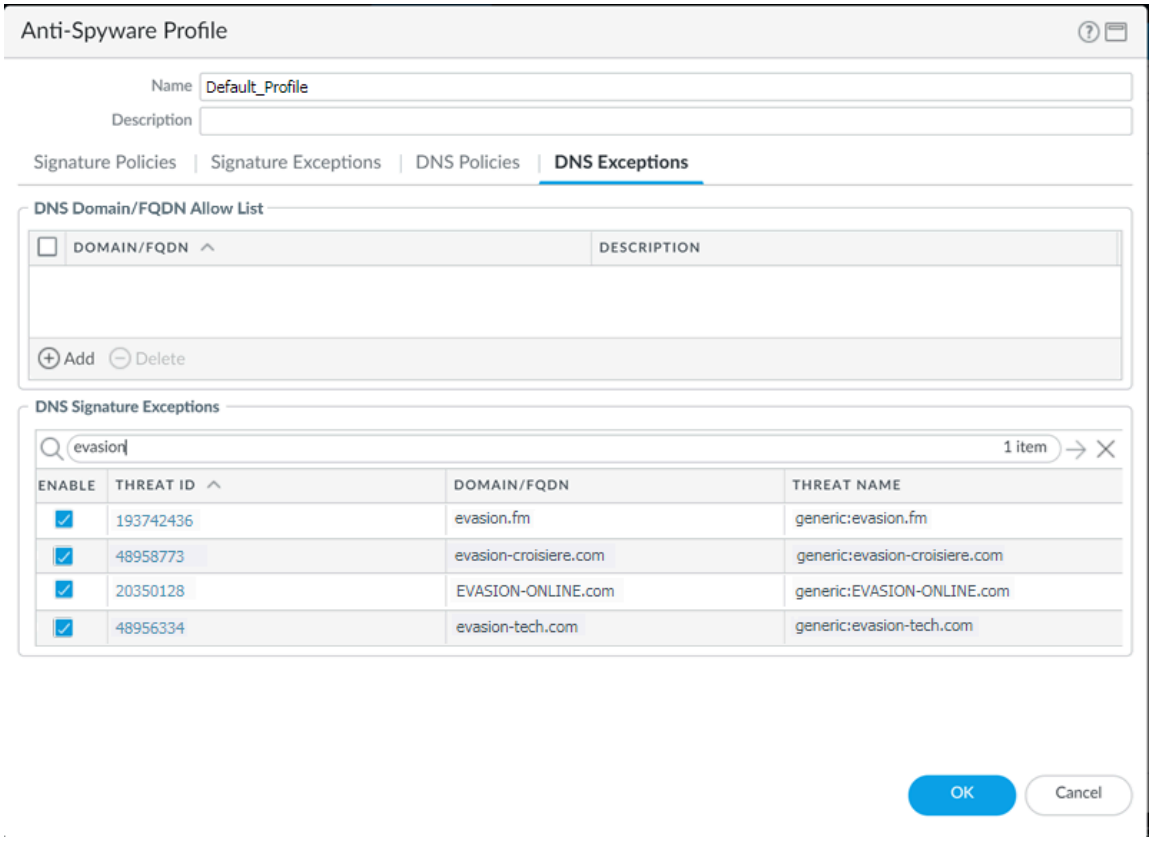
1. 다음 테스트 도메인에 액세스하여 주어진 위협 유형에 대한 정책 조치가 시행되고 있는지 확인하십시오.
   - C2—test-c2.testpanw.com
   - DNS Tunneling—test-dnstun.testpanw.com
   - DGA—test-dga.testpanw.com
   - Dynamic DNS—test-ddns.testpanw.com
   - Malware—test-malware.testpanw.com
   - 새로 등록된 도메인 - test-nrd.testpanw.com
   - 피싱—test-phishing.testpanw.com
   - Grayware—test-grayware.testpanw.com
   - Parked—test-parked.testpanw.com
   - 프록시 회피 및 익명화 - test-proxy.testpanw.com
2. 방화벽에서 활동을 모니터링하려면 다음을 수행합니다.
   1. **ACC**를 선택한 다음 URL 도메인을 전역 필터로 추가하여 액세스한 도메인에 대한 위협 활동 및 차단된 활동을 볼 수 있습니다.
   2. 모니터 > 로그 > 위협및 필터**(작업 eq 싱크홀)**를 선택하여 싱크홀 도메인의 로그를 볼 수 있습니다.

**STEP 6 |** 트래픽 로그에서 감염된 트래픽 호스트 식별

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** (선택 사항) 가양성이 발생하는 경우 도메인 서명 예외를 추가합니다.

1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택합니다.
2. 수정할 프로파일을 선택하세요.
3. 보안 서명을 제외할 안티 스파이웨어 프로파일을 추가하거나 수정하고 **DNS** 예외를 선택합니다.
4. 이름 또는 FQDN을 입력하여 제외할 DNS 서명을 검색합니다.
5. 시행에서 제외할 DNS 서명의 각 위협 **ID**에 대한 체크박스를 선택합니다.
6. 확인을 클릭하여 새 또는 수정된 안티 스파이웨어 프로파일을 저장합니다.




**STEP 8 |** (선택 사항) 명시적으로 허용할 DNS 도메인/FQDN 목록을 지정하려면 허용 목록을 추가합니다.

1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택합니다.
2. 수정할 프로파일을 선택하세요.
3. 보안 서명을 제외할 안티 스파이웨어 프로파일을 추가하거나 수정하고 **DNS** 예외를 선택합니다.
4. 새 **FQDN** 허용 목록을 추가하려면 DNS 도메인 또는 FQDN 위치와 설명을 제공합니다.
5. 확인을 클릭하여 새 또는 수정된 안티 스파이웨어 프로파일을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 9 |** (선택 사항) DNS 보안 서비스에 대한 방화벽의 연결을 확인합니다. 서비스에 연결할 수 없는 경우 dns.service.paloaltonetworks.com 도메인이 차단되지 않았는지 확인하십시오.

방화벽에서 다음 CLI 명령을 사용하여 DNS 보안 서비스에 대한 방화벽의 연결 가용성을 확인합니다.

```
DNS 프록시 DNS 서명 정보 표시
```

예:

```
show dns-proxy dns-signture info Cloud URL:
 dns.service.paloaltonetworks.com:443 Telemetry URL:
 io.dns.service.paloaltonetworks.com:443 Last Result: 없음 마지막 서
버 주소: 매개변수 교환: 간격 300초 목록 새로 고침 허용: 간격 43200 초 요
청 대기 전송 : 0 보류 중인 응답 요청: 0 캐시 크기: 0
```

**STEP 10 |** (선택 사항) 대기 시간, TTL 및 서명 카테고리와 같은 지정된 도메인의 트랜잭션 세부 정보를 검색합니다.

방화벽에서 다음 CLI 명령을 사용하여 목록에 대한 세부 정보를 검토합니다.

```
test dns-proxy dns-signature fqdn
```

예:

```
test dns-proxy dns-signature fqdn www.yahoo.com DNS
 Signature Query [ www.yahoo.com ] Completed in 178 ms DNS
 Signature Response Entries: 2 Domain Category GTID TTL
 ------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

**STEP 11 |** (선택 사항) DNS 서명 조회 시간 제한 설정을 구성합니다. 방화벽이 연결 문제로 인해 할당된 시간 내에 서명 판정을 검색할 수 없는 경우 모든 후속 DNS 응답을 포함한 요청이 통과됩니다. 평균 대기 시간을 확인하여 요청이 구성된 기간 내에 속하는지 확인할 수 있습니다. 평균 대기 시간이 구성된 기간을 초과하는 경우 리퀘스트 타임아웃을 방지하기 위해 평균 대기 시간보다 높은 값으로 설정을 업데이트하는 것이 좋습니다.

1. CLI에서 다음 명령을 실행하여 평균 지연 시간을 확인합니다.

   ```
   show dns-proxy dns-signature counters
   ```

   기본 타임아웃은 100밀리초입니다.
2. 서명 쿼리 API 제목 아래의 대기 시간 섹션으로 출력을 아래로 스크롤하고 평균 대기 시간이 정의된 타임아웃 기간 내에 속하는지 확인합니다. 이 대기 시간은 평균적으로 DNS 보안 서비스에

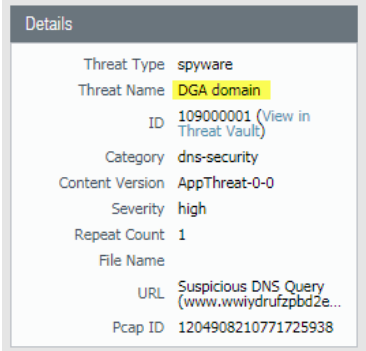
 ©2023 Palo Alto Networks, Inc.

서 서명 판정을 검색하는 데 걸리는 시간을 나타냅니다. 다양한 대기 시간 기간에 대한 추가 대기 시간 통계는 평균 이하에서 찾을 수 있습니다.

```
Signature query API: . . . [latency ] : max 1870 (ms) min
 16(ms) avg 27(ms) 50 or less : 47246 100 이하 : 113 200 이하 :
 25,400 이하 : 15 그 외 : 21
```

3. 평균 대기 시간이 기본 타임아웃 값보다 일관성이 있는 경우 요청이 지정된 기간 내에 포함되도록 설정을 높일 수 있습니다. 디바이스 > 콘텐츠 **ID**를 선택한 다음 실시간 서명 조회 설정을 업데이트합니다.
4. 변경 사항을 커밋합니다.

싱크홀된 DNS 쿼리를 보려면 방화벽 위협 로그를 참조하십시오(모니터 > 로그를 클릭한 다음 목록에서 로그 유형 선택).




## DNS 보안 데이터 수집 및 로깅

DNS 보안 서비스는 도메인 조회를 수행할 때 방화벽 보안 정책 규칙, 관련 작업 및 DNS 쿼리 세부 정보를 기반으로 서버 응답을 수집하고 정보를 요청합니다. 방화벽은 DNS 보안 클라우드 서버에 추가 DNS 데이터를 포워딩하며 Palo Alto Networks 서비스에서 보다 정확한 도메인 정보(예: 공급자 ASN, 호스팅 정보 및 지리적 위치 식별)를 제공하는 데 사용됩니다. DNS 보안 서비스를 운영하는 데 이 추가 데이터는 필요하지 않지만 향상된 분석, DNS 검색 및 예방 기능을 생성하는 리소스를 제공합니다. 이 작업은 수집 및 일괄 처리가 방화벽 성능에 영향을 미치지 않은 상태에서 30초 이내에 발생합니다. 방화벽에 부하가 높은 경우 예상 성능 수준을 유지하기 위해 필요에 따라 DNS 데이터 수집이 축소됩니다.

방화벽은 다음 데이터 필드를 제출할 수 있습니다.

| 필드 | 설명 |
|---|---|
| 동작 | DNS 쿼리에서 수행된 정책 작업을 표시합니다. |
| 유형 | DNS 레코드 유형을 표시합니다. |
| 응답 | DNS 쿼리의 도메인이 해결된 IP 주소입니다. |
| 응답 코드 | DNS 쿼리에 대한 답변으로 수신된 DNS 응답 코드입니다. |
| 소스 IP | DNS 요청을 만든 시스템의 IP 주소입니다. |


©2023 Palo Alto Networks, Inc.

| 필드 | 설명 |
| --- | --- |
| 소스 사용자 | 방화벽 사용자 ID 기능이 활성화되면 DNS 요청자의 ID가 표시됩니다. |
| 소스 영역 | 보안 정책 규칙에서 참조되는 구성된 소스 영역입니다. |

*DNS* 확장된 데이터 수집은 *DNS* 예외의 허용 목록에 추가된 도메인에 대해 우회됩니다.

잠재적으로 사용자(소스 IP, 소스 사용자 및 소스 영역)를 식별하는 데 사용할 수 있는 데이터 필드는 다음 CLI 명령을 사용하여 자동 제출에서 보류할 수 있습니다: **set deviceconfig setting ctd cloud-dns-privacy-mask yes**. 업데이트가 적용되기 위해 변경 내용을 커밋해야 합니다.


©2023 Palo Alto Networks, Inc.

# DNS 쿼리를 사용하여 네트워크에서 감염된 호스트 식별

안티스파이웨어 프로파일의 DNS 싱크홀 작업을 통해 방화벽은 알려진 악성 도메인 또는 사용자 지정 도메인에 대한 DNS 쿼리에 대한 응답을 위조할 수 있으므로 네트워크에서 멀웨어에 감염된 호스트를 식별할 수 있습니다. 손상된 호스트는 C2(명령 및 제어) 서버와 통신을 시작할 수 있습니다. 연결이 설정되면 공격자는 네트워크에 추가로 침투하거나 데이터를 유출하기 위해 감염된 호스트를 원격으로 제어할 수 있습니다.

Palo Alto Networks DNS 서명 목록에 포함된 모든 도메인에 대한 DNS 쿼리는 Palo Alto Networks 서버 IP 주소로 싱크홀됩니다.

방화벽에는 악성 도메인과 C2 도메인을 식별하는 데 사용할 수 있는 두 가지 DNS 서명 소스가 있습니다.

- (위협 예방 필요) 로컬 DNS 서명 - 방화벽이 악성 도메인을 식별하는 데 사용할 수 있는 제한된 온박스 DNS 서명 세트입니다. 방화벽은 일일 바이러스 백신 업데이트의 일부로 새 DNS 서명을 받습니다.
- (DNS 보안 필요) DNS 보안 서명 - 방화벽이 Palo Alto Networks DNS Security 클라우드 서비스에 액세스하여 DNS 서명의 전체 데이터베이스에 대해 악성 도메인을 확인합니다. DNS 보안만 제공하는 특정 서명은 DGA(도메인 생성 알고리즘) 및 DNS 터널링과 같은 기계 학습 기술을 사용하는 C2 공격을 고유하게 감지할 수 있습니다.

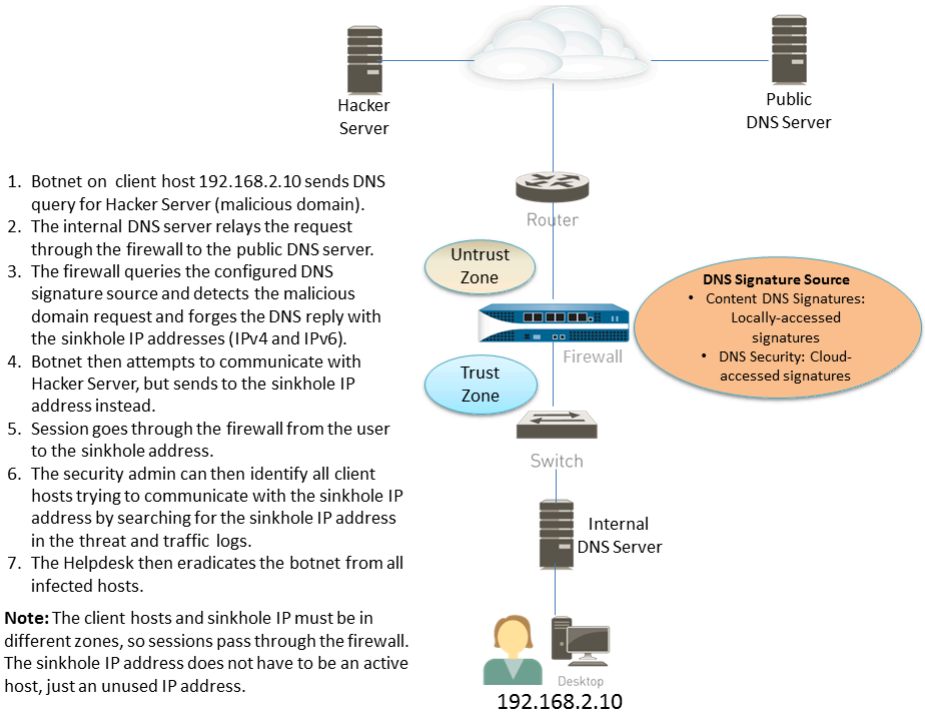
로컬 DNS 서명 세트 또는 DNS 보안 서명 세트의 도메인에 대한 DNS 쿼리는 Palo Alto Networks 서버로 리디렉션되고 호스트는 악성 도메인에 액세스할 수 없습니다. 다음 항목에서는 감염된 호스트를 식별할 수 있도록 DNS 싱크홀을 활성화하는 방법에 대해 자세히 설명합니다.

- DNS 싱크홀링 작동 방식에 대해 알아봅니다.
- DNS 싱크홀링 구성.
- 사용자 지정 도메인 목록에 대한 DNS 싱크홀링을 구성합니다.
- DNS 보안을 활성화하여 C2 도메인을 싱크홀합니다.
- 네트워크의 로컬 서버에 대한 싱크홀 IP 주소를 구성합니다.
- 악의적인 도메인에 연결하려고 시도한 감염된 호스트 보기.

## DNS 싱크홀링 작동 방식

DNS 싱크홀링은 방화벽이 감염된 클라이언트의 DNS 쿼리를 볼 수 없는(즉, 방화벽이 DNS 쿼리의 발신자를 볼 수 없는) 상황에서 DNS 트래픽을 사용하여 보호된 네트워크에서 감염된 호스트를 식별하는 데 도움이 됩니다. 방화벽이 로컬 DNS 서버의 북쪽에 있는 일반적인 배포에서 위협 로그는 실제 감염된 호스트가 아닌 트래픽 소스로 로컬 DNS 확인자를 식별합니다. 멀웨어 DNS 쿼리를 싱크홀링하면 악성 도메인을 대상으로 하는 클라이언트 호스트 쿼리에 대한 응답을 위조하여 이러한 가시성 문제를 해결해서 악성 도메인에 연결을 시도하는 클라이언트(예: 명령 및 제어용)가 대신 기본 Palo Alto Networks 싱크홀 IP 주소(또는 사용자 지정 도메인 목록에 대한 DNS 싱크홀 구성을 선택하는 경우 정의한 IP 주소)에 연결을 시도합니다. 그러면 트래픽 로그에서 감염된 호스트를 쉽게 식별할 수 있습니다.


©2023 Palo Alto Networks, Inc.




1. Botnet on client host 192.168.2.10 sends DNS query for Hacker Server (malicious domain).
2. The internal DNS server relays the request through the firewall to the public DNS server.
3. The firewall queries the configured DNS signature source and detects the malicious domain request and forges the DNS reply with the sinkhole IP addresses (IPv4 and IPv6).
4. Botnet then attempts to communicate with Hacker Server, but sends to the sinkhole IP address instead.
5. Session goes through the firewall from the user to the sinkhole address.
6. The security admin can then identify all client hosts trying to communicate with the sinkhole IP address by searching for the sinkhole IP address in the threat and traffic logs.
7. The Helpdesk then eradicates the botnet from all infected hosts.

**Note:** The client hosts and sinkhole IP must be in different zones, so sessions pass through the firewall. The sinkhole IP address does not have to be an active host, just an unused IP address.

# DNS 싱크홀링 구성

DNS 싱크홀링을 사용하려면 기본 안티 스파이웨어 프로파일을 보안 정책 규칙에 연결합니다(바이러스 백신 설정, 안티 스파이웨어 및 취약점 보호 설정 참조). 지정한 Palo Alto Networks DNS 서명 소스에 포함된 도메인에 대한 DNS 쿼리는 기본 Palo Alto Networks 싱크홀 IP 주소로 해결됩니다. IP 주소는 현재 IPv4-sinkhole.paloaltonetworks.com 루프백 주소인 IPv6 주소(::1)입니다. 이러한 주소는 변경될 수 있으며 콘텐츠 업데이트로 업데이트할 수 있습니다.

**STEP 1 |** 외부 동적 목록에서 사용자 지정 도메인 목록에 DNS 싱크홀링을 사용하도록 설정합니다.

1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택합니다.
2. 기존 프로파일을 수정하거나 기존 기본 프로파일 중 하나를 선택한 다음 복제합니다.
3. 프로파일 이름을 지정하고 **DNS** 정책 탭을 선택합니다.
4. **default-paloalto-dns**가 서명 소스에 있는지 확인합니다.
5. (선택 사항) 패킷 캡처 드롭다운에서 단일 패킷을 선택하여 세션의 첫 번째 패킷을 캡처하거나 확장 캡처를 하여 1-50 패킷 사이를 설정합니다. 그런 다음 추가 분석을 위해 패킷 캡처를 사용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 안티 스파이웨어 프로파일에서 싱크홀링 설정을 확인합니다.

1. **DNS** 정책 탭에서 DNS 쿼리의 정책 조치가 싱크홀인지 확인합니다.
2. DNS 싱크홀 설정 섹션에서 싱크홀이 활성화되어 있는지 확인합니다. 사용자의 편의를 위해 기본 싱크홀 IP 주소가 Palo Alto Networks 서버에 액세스하도록 설정되어 있습니다. Palo Alto Networks는 콘텐츠 업데이트를 통해 이 IP 주소를 자동으로 새로 고칠 수 있습니다.

   싱크홀 **IPv4** 또는 싱크홀 **IPv6** 주소를 네트워크의 로컬 서버나 루프백 주소로 수정하려면 네트워크의 로컬 서버에 대한 싱크홀 IP 주소 구성을(를) 참조하십시오.
3. 확인을 클릭하여 안티 스파이웨어 프로파일을 저장합니다.

**STEP 3 |** 안티 스파이웨어 프로파일을 보안 정책 규칙에 첨부합니다.

1. 정책 > 보안을 선택한 다음 보안 정책 규칙을 선택합니다.
2. 작업 탭에서 세션 시작 시 로그 체크박스를 선택하여 로깅을 사용하도록 설정합니다.
3. 프로파일 설정 섹션에서 프로파일 유형 드롭다운을 클릭하여 모든 프로파일을 봅니다. 안티 스파이웨어 드롭다운에서 새 프로파일을 선택합니다.
4. 확인을 클릭하여 정책 규칙을 저장합니다.

**STEP 4 |** 방화벽에서 활동을 모니터링하여 정책 작업이 적용되는지 테스트합니다.

1. **ACC**를 선택한 다음 URL 도메인을 전역 필터로 추가하여 액세스한 도메인에 대한 위협 활동 및 차단된 활동을 볼 수 있습니다.
2. 모니터 > 로그 > 위협 및 필터(**작업 eq 싱크홀**)를 선택하여 싱크홀 도메인의 로그를 볼 수 있습니다.

## 사용자 지정 도메인 목록에 대한 DNS 싱크홀링 구성

사용자 지정 도메인 목록에 대해 DNS 싱크홀링을 사용하도록 설정하려면 도메인이 포함된 외부 동적 목록을 생성하고 안티 스파이웨어 프로파일에서 싱크홀 작업을 사용하도록 설정한 다음 프로파일을 보안 정책 규칙에 연결해야 합니다. 클라이언트가 목록의 악성 도메인에 액세스하려고 하면 방화벽이 패킷의 대상 IP 주소를 기본 Palo Alto Networks 서버 또는 싱크홀링용 사용자 정의 IP 주소로 위조합니다.

방화벽은 외부 동적 목록에 포함된 각 사용자 지정 도메인에 대해 DNS 기반 스파이웨어 서명을 생성합니다. 이 서명은 사용자 지정 악성 DNS 쿼리 <domain name>(이)라고 하며 심각도가 중간 정도인 스파이웨어 유형입니다. 각 서명은 도메인 이름의 24바이트 해시입니다.

각 방화벽 모델은 하나 이상의 외부 동적 목록에서 총 50,000개의 도메인 이름을 지원하지만 목록 하나에 대해 최대 제한이 적용되지 않습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 외부 동적 목록에서 사용자 지정 도메인 목록에 DNS 싱크홀링을 사용하도록 설정합니다.

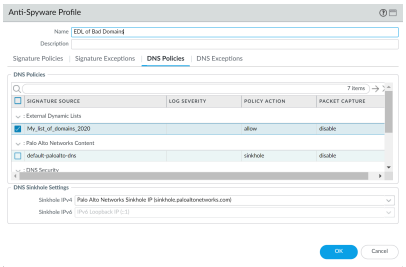
1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택합니다.
2. 기존 프로파일을 수정하거나 기존 기본 프로파일 중 하나를 선택한 다음 복제합니다.
3. 프로파일 이름을 지정하고 **DNS** 정책 탭을 선택합니다.
4. 외부 동적 목록 서명 소스에서 EDL을 선택합니다.

   외부 동적 유형 목록을 이미 만든 경우 다음을 수행합니다. 도메인 목록은 여기에서 선택할 수 있습니다. 이 목록에는 사용자가 만든 ***URL*** 또는 ***IP*** 주소 유형의 외부 동적 목록이 표시되지 않습니다.
5. 안티 스파이웨어 프로파일에서 외부 동적 목록을 구성합니다(외부 동적 목록에 액세스하도록 방화벽 구성 참조). 유형은 도메인 목록으로 미리 설정되어 있습니다.
6. (선택 사항) 패킷 캡처 드롭다운에서 단일 패킷을 선택하여 세션의 첫 번째 패킷을 캡처하거나 확장 캡처를 하여 1-50 패킷 사이를 설정합니다. 그런 다음 추가 분석을 위해 패킷 캡처를 사용할 수 있습니다.

**STEP 2 |** 안티 스파이웨어 프로파일에서 싱크홀링 설정을 확인합니다.

1. **DNS** 정책 탭에서 DNS 쿼리의 정책 조치가 싱크홀인지 확인합니다.
2. DNS 싱크홀 설정 섹션에서 싱크홀이 활성화되어 있는지 확인합니다. 사용자의 편의를 위해 기본 싱크홀 IP 주소가 Palo Alto Networks 서버에 액세스하도록 설정되어 있습니다. Palo Alto Networks는 콘텐츠 업데이트를 통해 이 IP 주소를 자동으로 새로 고칠 수 있습니다.

   싱크홀 **IPv4** 또는 **Sinkhole IPv6** 주소를 네트워크의 로컬 서버 또는 루프백 주소로 수정하려면 네트워크의 로컬 서버에 싱크홀 IP 주소 구성을 참조하십시오.




3. 확인을 클릭하여 안티 스파이웨어 프로파일을 저장합니다.

**STEP 3 |** 안티 스파이웨어 프로파일을 보안 정책 규칙에 첨부합니다.

1. 정책 > 보안을 선택한 다음 보안 정책 규칙을 선택합니다.
2. 작업 탭에서 세션 시작 시 로그 체크박스를 선택하여 로깅을 사용하도록 설정합니다.
3. 프로파일 설정 섹션에서 프로파일 유형 드롭다운을 클릭하여 모든 프로파일을 봅니다. 안티 스파이웨어 드롭다운에서 새 프로파일을 선택합니다.
4. 확인을 클릭하여 정책 규칙을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 정책 작업이 적용되었는지 테스트합니다.

1. 도메인 목록에 속하는 외부 동적 목록 항목을 확인하고 목록에서 도메인에 액세스합니다.
2. 방화벽에서 활동을 모니터링하려면 다음을 수행합니다.
   1. **ACC**를 선택한 다음 URL 도메인을 전역 필터로 추가하여 액세스한 도메인에 대한 위협 활동 및 차단된 활동을 볼 수 있습니다.
   2. 모니터 > 로그 > 위협및 필터**(작업 eq 싱크홀)**를 선택하여 싱크홀 도메인의 로그를 볼 수 있습니다.

**STEP 5 |** 외부 동적 목록의 항목이 무시되는지 또는 건너뛰는지 확인합니다.

방화벽에서 다음 CLI 명령을 사용하여 목록에 대한 세부 정보를 검토합니다.

```
request system external-list show type domain name <list_name>
```

예:

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain: Next update
 at : Thu May 21 10:15:39 2015 Source : https://1.2.3.4/
My_List_of_Domains_2015 Referenced : Yes Valid : Yes Number of
 entries : 3 domains:www.example.com baddomain.com qqq.abcedfg.com
```

**STEP 6 |** (선택 사항) 요청 시 외부 동적 목록을 검색합니다.

방화벽이 다음 새로 고침 간격(외부 동적 목록에 대해 정의한 반복 빈도) 이 아니라 필요에 따라 업데이트된 목록을 검색하도록 하려면 다음 CLI 명령을 사용합니다.

```
요청 시스템 외부 목록 새로 고침 유형 도메인 이름  <list_name>
```



또는 방화벽 인터페이스를 사용하여 웹 서버에서 외부 동적 목록을 검색할 수 있습니다.

## 네트워크의 로컬 서버에 대한 싱크홀 IP 주소 구성

기본적으로 싱크홀링은 모든 Palo Alto Networks DNS 서명에 대해 활성화되며 싱크홀 IP 주소는 Palo Alto Networks 서버에 액세스하도록 설정됩니다. 싱크 홀 IP 주소를 네트워크의 로컬 서버로 설정하려면 이 섹션의 지침을 따르십시오.

악성 소프트웨어가 이러한 프로토콜 중 하나 또는 둘 다를 사용하여 DNS 쿼리를 수행할 수 있으므로 싱크홀 IP 주소로 사용할 IPv4 및 IPv6 주소를 모두 가져와야 합니다. 감염된 호스트가 싱크홀 IP 주소로 세션을 시작하려고 할 때 방화벽을 통해 라우팅되도록 하려면 DNS 싱크홀 주소는 클라이언트 호스트와 다른 영역에 있어야 합니다.


©2023 Palo Alto Networks, Inc.

싱크홀 주소는 이 용도로 예약되어야 하며 물리적 호스트에 할당할 필요가 없습니다. 선택적으로 *Honey-pot* 서버를 물리적 호스트로 사용하여 악성 트래픽을 추가로 분석할 수 있습니다.

다음 구성 단계에서는 다음 예제 *DNS* 싱크홀 주소를 사용합니다.

*IPv4 DNS* 싱크홀 주소 - *10.15.0.20*

*IPv6 DNS* 싱크홀 주소 - *fd97:3dec:4d27:e37c:5:5:5:5*

**STEP 1 |** 싱크홀 인터페이스와 구역을 구성합니다.

클라이언트 호스트가 상주하는 영역의 트래픽은 싱크홀 IP 주소가 정의된 영역으로 라우팅해야 하므로 트래픽이 기록됩니다.

감염된 호스트가 이 영역으로 트래픽을 전송하므로 싱크홀 트래픽에 전용 영역을 사용합니다.

1. 네트워크 > 인터페이스를 선택하고 싱크홀 인터페이스로 구성할 인터페이스를 선택합니다.
2. 인터페이스 유형 드롭다운에서 레이어**3**을 선택합니다.
3. IPv4 주소를 추가하려면 **IPv4** 탭을 선택하고 고정을 선택한 다음 추가를 클릭합니다. 이 예제에서는 IPv4 DNS 싱크홀 주소로 10.15.0.20을 추가합니다.
4. **IPv6** 탭을 선택한 다음 고정을 클릭한 다음 추가를 클릭하고 IPv6 주소 및 서브넷 마스크를 입력합니다. 이 예에서는 IPv6 싱크홀 주소로 fd97:3dec:4d27:e37c::/64를 입력합니다.
5. 확인을 클릭하여 저장합니다.
6. 싱크홀 영역을 추가하려면 네트워크 > 영역을 선택하고 추가를 클릭합니다.
7. 영역 이름을 입력합니다.
8. 유형 드롭다운에서 레이어**3**을 선택합니다.
9. 인터페이스 섹션에서 추가를 클릭하고 방금 구성한 인터페이스를 추가합니다.
10. 확인을 클릭합니다.

**STEP 2 |** DNS 싱크홀링을 사용하도록 설정합니다.

기본적으로 싱크홀링은 모든 Palo Alto Networks DNS 서명에 대해 활성화됩니다. 싱크홀 주소를 로컬 서버로 변경하려면 안티 스파이웨어 프로파일의 싱크홀링 설정 단계 확인을 참조하십시오. 사용자 지정 도메인 목록에 대한 DNS 싱크홀링 구성을 참조하십시오.

**STEP 3 |** 트러스트 영역의 클라이언트 호스트에서 언트러스트 영역으로의 트래픽을 허용하는 보안 정책 규칙을 편집하여 싱크홀 영역을 대상으로 포함하고 안티 스파이웨어 프로파일을 연결합니다.

트러스트 영역의 클라이언트 호스트에서 언트러스트 영역으로의 트래픽을 허용하는 보안 정책 규칙을 편집하면 감염된 호스트의 트래픽을 식별할 수 있습니다. 싱크홀 영역을 규칙의 대상으로 추가하면 감염된 클라이언트가 가짜 DNS 쿼리를 DNS 싱크홀로 보낼 수 있습니다.

1. 정책 > 보안을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

2. 클라이언트 호스트 영역에서 언트러스트 영역으로의 트래픽을 허용하는 기존 규칙을 선택합니다.
3. 대상 탭에서 싱크홀 영역을 추가합니다. 이렇게 하면 클라이언트 호스트 트래픽이 싱크홀 영역으로 흐를 수 있습니다.
4. 작업 탭에서 세션 시작 시 로그 체크박스를 선택하여 로깅을 사용하도록 설정합니다. 이렇게 하면 언트러스트 또는 싱클홀 영역에 액세스할 때 트러스트 영역에 있는 클라이언트 호스트의 트래픽이 기록됩니다.
5. 프로파일 설정 섹션에서 DNS 싱크홀링을 활성화한 안티-스파이웨어 프로파일을 선택합니다.
6. 확인을 클릭하여 보안 정책 규칙을 저장한 다음 커밋을 클릭합니다.

**STEP 4 |** 감염된 호스트를 식별할 수 있는지 확인하려면 트러스트 영역의 클라이언트 호스트에서 새 싱크홀 영역으로 이동하는 트래픽이 기록되는지 확인합니다.

이 예에서 감염된 클라이언트 호스트는 192.168.2.10이고 싱크홀 IPv4 주소는 10.15.0.20입니다.

1. 트러스트 영역의 클라이언트 호스트에서 명령 프롬프트를 열고 다음 명령을 실행합니다.

```
C:\>ping <sinkhole address>
```

다음 예제 출력은 10.15.0.2의 DNS 싱크홀 주소에 대한 핑(ping) 요청과 그 결과를 보여 줍니다. 이 예에서는 싱크홀 IP 주소가 물리적 호스트에 할당되지 않았기 때문에 **타임아웃 요청**이 되었습니다.

```
C:\>ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of data:
 Request timed out. Request timed out. Ping statistics for
 10.15.0.20: Packets: Sent = 4, Received = 0, Lost = 4 (100%
 loss)
```

2. 방화벽에서 모니터 > 로그 > 트래픽을 선택하고 소스가 192.168.2.10이고 대상이 10.15.0.20인 로그 항목을 찾습니다. 이렇게 하면 싱크홀 IP 주소에 대한 트래픽이 방화벽 영역을 통과하고 있음을 확인할 수 있습니다.



로그를 검색 및/또는 필터링할 수 있으며 대상 ***10.15.0.20***의 로그만 표시할 수 있습니다. 이렇게 하려면 *[대상]* 열에서 ***IP*** 주소***(10.15.0.20)***를 클릭합니다. 그러면 검색 필드에 필터***(10.15.0.20***의 ***addr.dst)***가 추가됩니다. 검색 필드 오른쪽에 있는 필터 적용 아이콘을 클릭하여 필터를 적용합니다.

**STEP 5 |** DNS 싱크홀링이 제대로 구성되었는지 테스트합니다.

악성 애플리케이션이 집으로 전화를 걸려고 할 때 감염된 클라이언트 호스트가 수행하는 작업을 시뮬레이션합니다.

1. 방화벽의 현재 안티바이러스 서명 데이터베이스에 포함된 악성 도메인을 찾아 싱크홀링을 테스트합니다.
   1. 디바이스 > 동적 업데이트를 선택한 다음 바이러스 백신 섹션에서 현재 설치된 바이러스 백신 데이터베이스에 대한 릴리스 정보 링크를 클릭합니다. 또한 Palo Alto Networks 지원 사이트의 동적 업데이트에서 서명 업데이트 증가분을 나열하는 바이러스 백신 릴리스 정보를 찾을 수 있습니다.


©2023 Palo Alto Networks, Inc.

**2.** 릴리스 노트의 두 번째 열에서 도메인 확장명이 있는 항목을 찾습니다(예: .com, .edu 또는.net). 왼쪽 열에는 도메인 이름이 표시됩니다. 예를 들어 안티바이러스 릴리스 1117-1560은 왼쪽 열에 “tbsbana”라는 항목을 포함하고 오른쪽 열에는 “net”이 나열됩니다.

다음은 이 행 항목에 대한 릴리스 노트의 내용을 보여 줍니다.

```
conficker:tbsbana 1 variants: net
```

2. 클라이언트 호스트에서 명령 프롬프트를 엽니다.
3. 알려진 악성 도메인으로 식별된 URL에 NSLOOKUP을 수행합니다.

   예를 들어 다음과 같이 URL **track.bidtrk.com:**을 사용할 수 있습니다.

```
C:\>nslookup track.bidtrk.com Server: my-local-
dns.local Address: 10.0.0.222 Non-authoritative
 answer: Name: track.bidtrk.com.org Addresses:
 fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
```

   아웃풋에서 악성 도메인에 대한 NSLOOKUP은 우리가 구성한 싱크홀 IP 주소(10.15.0.20)를 사용하여 위조되었습니다. 도메인이 악성 DNS 서명과 일치했기 때문에 싱크홀 작업이 수행되었습니다.
4. 모니터 > 로그 > 위협을 선택한 다음 해당 위협 로그 항목을 찾아 NSLOOKUP 요청에 대해 올바른 작업이 수행되었는지 확인합니다.
5. **track.bidtrk.com**에 대해 핑을 수행합니다. 그러면 싱크홀 주소로의 네트워크 트래픽이 생성됩니다.

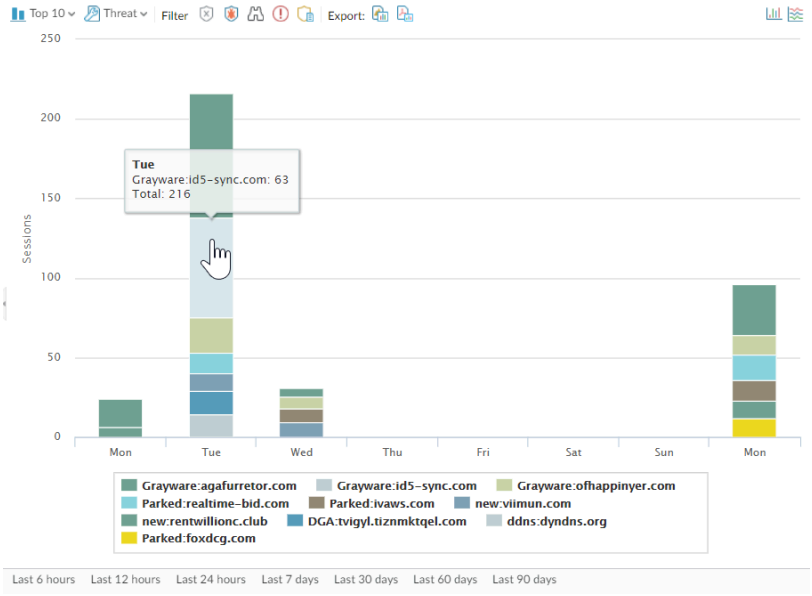
## 악의적인 도메인에 연결하려고 시도한 감염된 호스트 보기

DNS 싱크홀링을 구성하고 악의적인 도메인으로의 트래픽이 싱크홀 주소로 이동한다는 것을 확인한 후에는 감염된 호스트를 추적하고 위협을 제거할 수 있도록 싱크홀 주소로의 트래픽을 정기적으로 모니터링해야 합니다.


©2023 Palo Alto Networks, Inc.

- 앱 범위를 사용하여 감염된 클라이언트 호스트를 식별합니다.
  1. 모니터 > 앱 범위를 선택하고 위협 모니터를 선택합니다.
  2. 표시 페이지 상단의 스파이웨어 표시 단추를 클릭합니다.
  3. 시간 범위를 선택합니다.

     다음 스크린샷에는 테스트 클라이언트 호스트가 알려진 악성 도메인에서 NSLOOKUP을 수행했을 때 생성된 의심스러운 DNS 쿼리의 세 인스턴스가 표시됩니다. 그래프를 클릭하여 이벤트에 대한 자세한 내용을 확인합니다.




- 이 예제에서 10.15.0.20인 싱크홀 IP 주소로 트래픽을 보낸 모든 클라이언트 호스트를 식별하도록 맞춤 보고서를 구성합니다.

  ***SNMP** 관리자, **Syslog** 서버 및/또는 **Panorama**로 포워딩하여 이러한 이벤트에 대한 경고를 활성화합니다.*

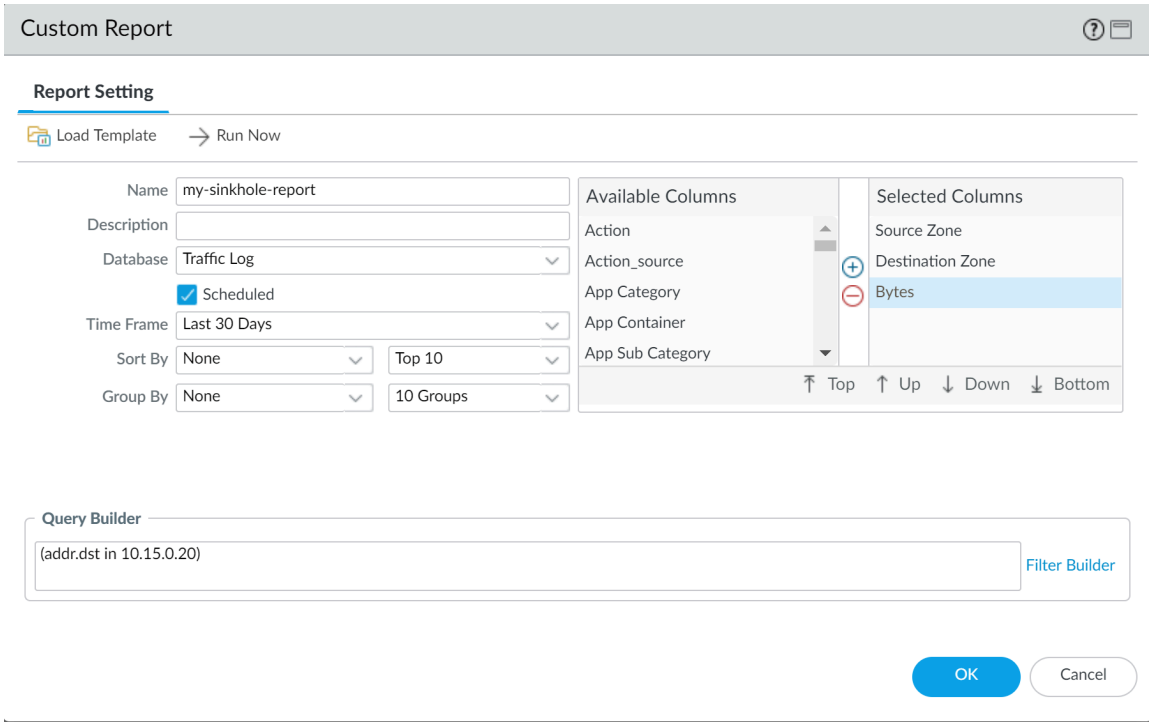
  이 예제에서는 감염된 클라이언트 호스트가 Palo Alto Networks DNS 서명 데이터베이스에 나열된 알려진 악성 도메인에 대한 NSLOOKUP을 수행했습니다. 이 경우 쿼리가 로컬 DNS 서버로 전송된 다음 방화벽을 통해 요청을 외부 DNS 서버로 포워딩했습니다. 구성된 안티 스파이웨어 프로파일의 방화벽 보안 정책은 쿼리를 DNS 서명 데이터베이스와 일치시킨 다음 10.15.0.20 및 fd97:3dec:4d27:e37c:5:5:5:5의 싱크홀 주소를 사용하여 응답을 위조했습니다. 클라이언트는 세션을 시작하려고 시도하고 트래픽 로그는 소스 호스트와 대상 주소로 활동을 기록하며, 이제 위조된 싱크홀 주소로 이동합니다.

  방화벽에서 트래픽 로그를 확인하면 싱크홀 주소로 트래픽을 보내는 클라이언트 호스트를 식별할 수 있습니다. 이 예에서 로그는 소스 주소 192.168.2.10이 악의적인 DNS 쿼리를 전송했음을 보여줍니다. 그런 다음 호스트를 찾아 삭제할 수 있습니다. DNS 싱크홀 옵션이 없으면 관리자는 로컬 DNS 서버만 쿼리를 수행하고 감염된 클라이언트 호스트를 볼 수 없는 시스템으로만 볼 수 있습니다. 작업 "Sinkhole"을 사용하여 위협 로그에 대한 보고서를 실행하려고 하면 로그에 감염된 호스트가 아닌 로컬 DNS 서버가 표시됩니다.

  1. 모니터 > 관리 맞춤 보고서를 선택합니다.


©2023 Palo Alto Networks, Inc.

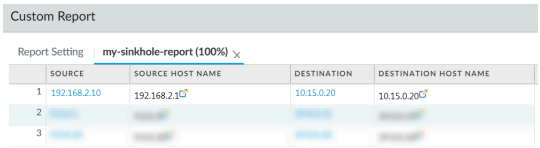
2. 보고서 추가 및 이름을 클릭합니다.
3. 싱크홀 주소로 트래픽을 캡처하는 맞춤 보고서를 다음과 같이 정의합니다.
   - 데이터베이스 - 트래픽 로그를 선택합니다.
   - 예정된 - 예약된 사용 가능과 보고서는 매일 밤 실행됩니다.
   - 시간 프레임 - 30일
   - 선택한 열 - 보고서 및 싱크홀 주소가 되는 대상 주소에서 감염된 클라이언트 호스트를 식별할 소스 주소 또는 소스 사용자(사용자 ID를 구성한 경우)를 선택합니다.
   - 화면 하단의 섹션에서 싱크홀 주소로의 트래픽에 대한 사용자 지정 쿼리를 생성합니다(이 예제에서 10.15.0.20). 쿼리 빌더 창(**10.15.0.20**의 **addr.dst**)에서 대상 주소를 입력하거나 각 열에서 다음을 선택한 다음 추가를 클릭할 수 있습니다. 커넥터 = and, 속성 = Destination Address, 연산자 = in 및 값 = 10.15.0.20. 추가를 클릭하여 쿼리를 추가합니다.





©2023 Palo Alto Networks, Inc.

4. 보고서를 실행하려면 지금 실행을 클릭합니다. 보고서에는 싱크홀 주소로 트래픽을 보낸 모든 클라이언트 호스트가 표시되며, 이는 감염 가능성이 가장 높다는 것을 나타냅니다. 이제 호스트를 추적하고 스파이웨어를 확인할 수 있습니다.




5. 실행된 예약 보고서를 보려면 모니터 > 보고서를 선택합니다.


©2023 Palo Alto Networks, Inc.

# 데이터 필터링

데이터 필터링 프로파일을 사용하여 중요하고 기밀적이며 독점적인 정보가 네트워크에서 유출되지 않도록 합니다. 사전 정의된 패턴, 기본 제공 설정 및 사용자 지정 옵션을 사용하면 특정 파일 속성(예: 문서 제목 또는 작성자), 신용카드 번호, 다른 국가의 규제 정보(예: 사회 보장 번호) 및 타사 데이터 손실 방지(DLP) 라벨이 포함된 파일을 쉽게 보호할 수 있습니다.

- 사전 정의된 데이터 패턴 - 신용카드 번호를 포함한 일반적인 패턴을 쉽게 필터링할 수 있습니다. 사전 정의된 데이터 필터링 패턴은 또한 사회 보장 번호(미국), INSEE 식별 번호(프랑스), 뉴질랜드 국세청 식별 번호와 같은 세계 여러 국가의 특정(규제) 정보를 식별합니다. 사전 정의된 데이터 필터링 패턴의 대부분은 HIPAA, GDPR, Gramm-Leach-Bliley 법과 같은 표준에 대한 준수를 가능하게 합니다.
- **Azure** 정보 보호 및 **Titus** 데이터 분류에 대한 기본 제공 지원 - 사전 정의된 파일 속성을 사용하면 Azure 정보 보호 및 Titus 레이블을 기반으로 콘텐츠를 필터링할 수 있습니다. Azure 정보 보호 레이블은 메타데이터에 저장되므로 방화벽이 필터링하려는 Azure 정보 보호 레이블의 GUID를 알고 있는지 확인합니다.
- **DLP(**데이터 손실 방지**)** 솔루션에 대한 사용자 지정 데이터 패턴-중요한 콘텐츠를 나타내기 위해 파일 속성을 채우는 타사 엔드포인트 DLP 솔루션을 사용하는 경우 사용자 지정 데이터 패턴을 만들어 DLP 솔루션에 태그된 파일 속성 및 값을 식별한 다음 해당 패턴에 따라 데이터 필터링 프로파일이 감지하는 파일을 기록하거나 차단할 수 있습니다.

## 데이터 필터링 프로파일 생성

데이터 필터링 프로파일은 중요한 정보가 네트워크에서 유출되지 못하도록 유지할 수 있습니다.

시작하려면 먼저 방화벽이 필터링할 정보 유형 및 필드를 지정하는 데이터 패턴을 생성합니다. 그런 다음 해당 패턴을 데이터 필터링 프로파일에 첨부하여 방화벽이 필터링하는 콘텐츠를 적용하는 방법을 지정합니다. 데이터 필터링 프로파일을 보안 정책 규칙에 추가하여 규칙과 일치하는 트래픽을 필터링합니다.

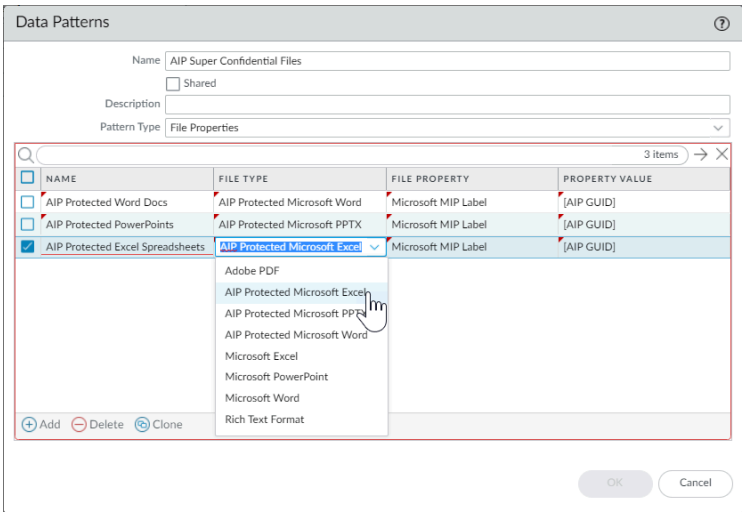

©2023 Palo Alto Networks, Inc.

**STEP 1 |** 필터링할 정보를 검색하려면 새 데이터 패턴 개체를 정의합니다.

1. 개체 > 사용자 정의 개체 > 데이터 패턴을 선택하고 새 개체를 추가합니다.
2. 새 개체에 대한 설명이 포함된 이름을 제공합니다.
3. (선택 사항) 데이터 패턴을 다음에 사용할 수 있도록 하려면 공유를 선택합니다.
   - **Multi-VSYS** 방화벽의 모든 가상 시스템**(vsys)**은 삭제(비활성화)하는 경우 개체 탭에서 선택한 가상 시스템에서만 데이터 패턴을 사용할 수 있습니다.
   - **Panorama**의모든 디바이스 그룹-삭제(비활성화)하는 경우 데이터 패턴은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
4. (선택사항-Panorama 전용) 관리자가 개체를 상속하는 디바이스 그룹에서 이 데이터 패턴 개체의 설정을 재정의하지 못하도록 재정의를 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
5. (선택사항—Panorama 전용)필터에 의해 차단된 데이터를 자동으로 수집하기 위해 데이터 캡처를 선택합니다.

   설정 페이지에서 데이터 보호 관리를 위한 암호를 지정하여 캡처된 데이터를 볼 수 있습니다**(**디바이스 **>** 설정 **>** 콘텐츠***-ID*** **>** 데이터 보호관리**).**
6. 패턴 유형을 다음 중 하나로 설정합니다.
   - 사전 정의된 패턴 - HIPAA, GDPR, Gramm-Leach-Bliley 법을 포함한 여러 규정 준수 표준에 대한 신용카드, 주민등록 번호 및 개인 식별 정보를 필터링합니다.
   - 정규식 - 사용자 지정 데이터 패턴을 필터링합니다.
   - 파일 속성 - 파일 속성 및 관련 값을 기반으로 필터링합니다.
7. 데이터 패턴 개체에 새 규칙을 추가합니다.
8. 이 개체에 대해 선택한 패턴 유형에 따라 데이터 패턴을 지정합니다.
   - 사전 정의된 - 이름을 선택한 다음 필터링할 사전 정의된 데이터 패턴을 선택합니다.
   - 정규식 - 이름을 지정하고, 스캔할 파일 유형(또는 형식)을 선택한 다음 방화벽이 감지할 특정 데이터 패턴을 입력합니다.
   - 파일속성 - 이름을 지정하고, 스캔할 파일 유형 및 파일 속성을 선택한 다음, 방화벽이 검색할 특정 속성 값을 입력합니다.
     - **Titus** 기밀 문서를 필터링하려면: AIP가 보호되지 않는 파일 유형 중 하나를 선택한 다음 파일 속성을 TITUS GUID로 설정합니다. Titus 레이블 GUID를 속성 값으로 입력합니다.
     - **Azure** 정보 보호 레이블이 지정된 문서**:** 텍스트 형식이 풍부한 것을 제외한 파일 유형을 선택합니다. 선택한 파일 형식의 경우 파일 속성을 Microsoft MIP 레이블로 설정하고 Azure Informatin 보호 레이블 GUID를 속성 값으로 입력합니다.


©2023 Palo Alto Networks, Inc.




9. 확인을 클릭하여 데이터 패턴을 저장합니다.

**STEP 2 |** 데이터 패턴 개체를 데이터 필터링 프로파일에 추가합니다.

1. 개체 > 보안 프로파일 > 데이터 필터링 및 추가를 선택하거나 데이터 필터링 프로파일을 수정합니다.
2. 새 프로파일에 대한 설명이 포함된 이름을 제공합니다.
3. 새 프로파일 규칙을 추가하고 해당 단계에서 만든 데이터 패턴을 선택합니다.
4. 데이터 패턴에 따라 필터링할 애플리케이션, 파일 유형 및 트래픽 방향(업로드 또는 다운로드)을 지정합니다.

   선택한 파일 형식은 이전에 데이터 패턴에 대해 정의된 파일 형식이어야 하며 데이터 패턴 파일 형식을 포함하는 파일 유형이어야 합니다. 예를 들어 모든 *Microsoft Office* 문서를 스캔하기 위해 데이터 패턴 개체와 데이터 필터링 프로파일을 모두 정의할 수 있습니다. 또는 데이터 필터링 프로파일이 모든 *Microsoft Office* 문서를 검사하는 동안 *Microsoft PowerPoint* 프레젠테이션과 일치하도록 데이터 패턴 개체를 정의할 수 있습니다.

   데이터 패턴 개체가 데이터 필터링 프로파일에 연결되고 구성된 파일 형식이 둘 사이에 정렬되지 않으면 프로파일이 데이터 패턴 개체와 일치하는 문서를 올바르게 필터링하지 않습니다.
5. 경고를 트리거하기 위해 파일에서 데이터 패턴을 검색해야 하는 횟수를 지정하도록 경고 임계값을 설정합니다.
6. 블록 임계값을 설정하여 데이터 패턴의 많은 해당 인스턴스를 포함하는 파일을 차단합니다.
7. 이 규칙과 일치하는 파일에 대해 기록된 로그 심각도를 설정합니다.
8. 확인을 클릭하여 데이터 필터링 프로파일을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 트래픽에 데이터 필터링 설정을 적용합니다.

1. 정책 > 보안 및 추가를 선택하거나 보안 정책 규칙을 수정합니다.
2. 작업을 선택하고 프로파일 유형을 프로파일로 설정합니다.
3. 2단계에서 만든 데이터 필터링 프로파일을 보안 정책 규칙에 첨부합니다.
4. 확인을 클릭합니다.

**STEP 4 |** (권장) 웹 브라우저가 방화벽이 종료된 세션을 다시 시작하지 못하도록 합니다.



이 옵션을 사용하면 방화벽이 중요한 파일을 감지한 다음 삭제하면 파일을 검색하기 위해 웹 브라우저가 세션을 다시 시작할 수 없습니다.

1. 디바이스 > 설정 > 콘텐츠 **ID**를 선택하고 콘텐츠 ID 설정을 수정합니다.
2. **HTTP** 부분 응답 허용을 선택 취소합니다.
3. 확인을 클릭합니다.

**STEP 5 |** 방화벽이 필터링하는 파일을 모니터링합니다.

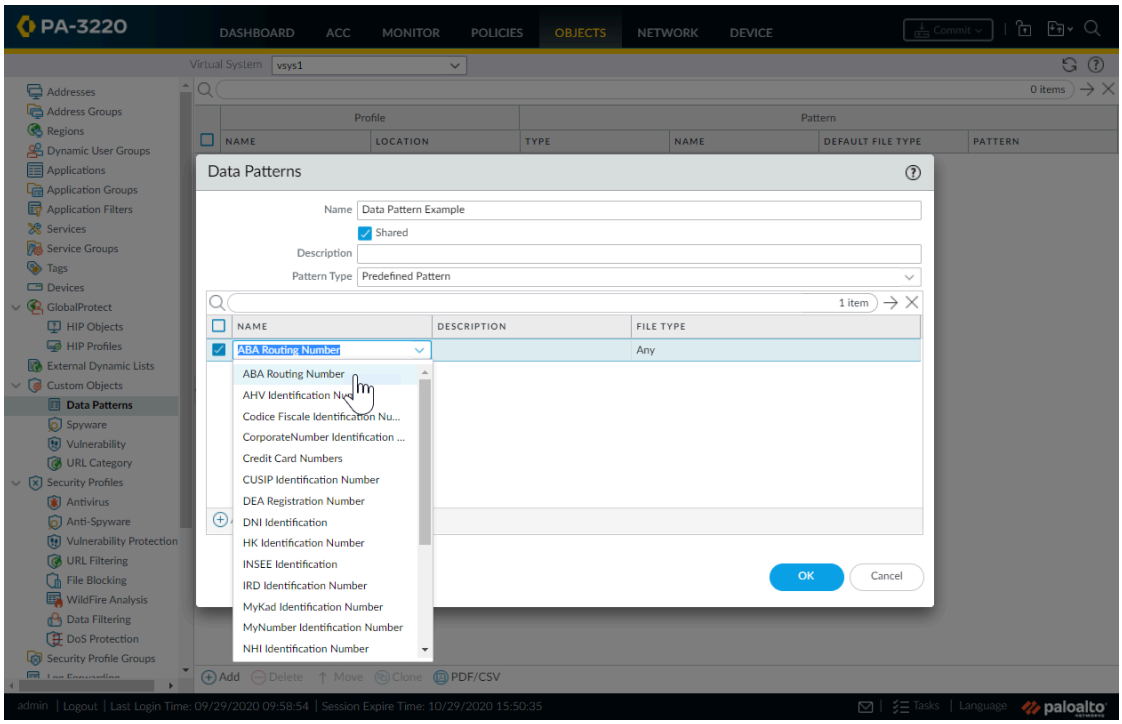
데이터 필터링 > 모니터를 선택하여 데이터 필터링 설정에 따라 방화벽이 감지하고 차단한 파일을 볼 수 있습니다.

## 사전 정의된 데이터 필터링 패턴

HIPAA, GDPR 및 Gramm-Leach-Bliley Act와 같은 표준을 준수하기 위해 방화벽은 사전 정의된 데이터 패턴을 제공합니다. 이러한 패턴을 사용하여 신용카드 및 주민등록번호와 같은 일반적인 유형의 민감한 정보가 유출되는 것을 방지할 수 있습니다.

개체 **>** 사용자 정의 개체 **>** 데이터 패턴을 선택한 다음 새 개체 추가를 클릭하여 사전 정의된 데이터 패턴을 찾을 수 있습니다. 그런 다음 패턴 유형을 사전 정의된 패턴으로 설정하고 데이터 패턴 개체에 새 규칙을 추가합니다. 이름 아래에 나타나는 목록에서 데이터 패턴을 선택합니다.


©2023 Palo Alto Networks, Inc.




보호하려는 정보 유형이 사전 정의된 패턴 목록에 없는 경우 정규식을 사용하여 사용자 정의 패턴을 작성할 수 있습니다.

다음은 사용 가능한 데이터 패턴 목록입니다.

| 패턴 | 설명 |
|---|---|
| 신용카드 번호 | 16자리 신용카드 번호 |
| 사회 보장 번호 | 대시가 있는 9자리 사회 보장 번호 |
| 사회 보장 번호(대시 구분 기호 없음) | 대시가 없는 9자리 사회 보장 번호 |
| ABA 라우팅 번호 | 미국 은행 협회 라우팅 번호 |
| AHV 식별 번호 | Swiss Alters und Hinterlassenenversicherungsnummer |
| Codice Fiscale 식별 번호 | 이탈리아 재정세 코드 카드 식별 번호 |
| 기업 번호 식별 번호 | 일본 국세청 법인번호 |
| CUSIP 식별 번호 | 통일보안식별절차위원회 식별번호 |
| DEA 등록 번호 | 미국 마약단속국 등록번호 |


©2023 Palo Alto Networks, Inc.

| 패턴 | 설명 |
| --- | --- |
| DNI 식별 번호 | 스페인어 Documento nacional de identidad 식별 번호 |
| 홍콩 식별 번호 | 홍콩 거주자 식별 번호 |
| INSEE 식별 번호 | 프랑스 국립 통계 및 경제 연구소 식별 번호 |
| IRD 식별 번호 | 뉴질랜드 국세청 식별 번호 |
| MyKad 식별 번호 | 말레이시아 MyKad 신분증 식별 번호 |
| 마이넘버 식별번호 | 일본 사회 보장 및 세금 번호 시스템 식별 번호 |
| 국민건강보험 식별번호 | 뉴질랜드 국민 건강 지수 번호 |
| NIF 식별 번호 | 스페인 세금 식별 번호 |
| NIN 식별 번호 | 대만 신분증 번호 |
| NRIC 식별 번호 | 싱가포르 국가 등록 신분증 식별 번호 |
| 영구 계정 식별 번호 | 인도 영구 계좌 인도 국민의 수 |
| 중국 식별 번호 | 중화인민공화국 주민등록번호 |
| PRN 식별 번호 | 대한민국 주민등록번호 |
| 대한민국 주민등록 | 대한민국 주민등록번호 |


©2023 Palo Alto Networks, Inc.

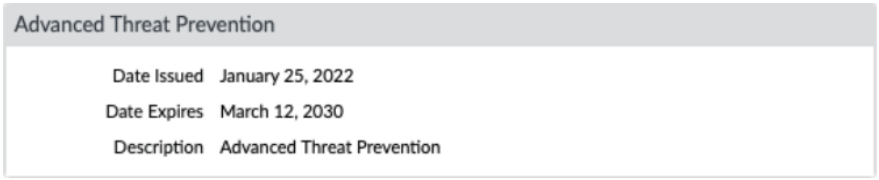
# 인라인 클라우드 분석 구성

고급 위협 방지를 사용하도록 설정하려면 인라인 클라우드 분석 설정으로 구성된 스파이웨어 방지 프로파일을 보안 정책 규칙에 연결합니다(기본 보안 정책 설정 참조).

**STEP 1 |** PAN-OS 웹 인터페이스에 로그인합니다.

**STEP 2 |** 인라인 클라우드 분석을 활용하려면 활성 고급 위협 방지 구독이 있어야 합니다.

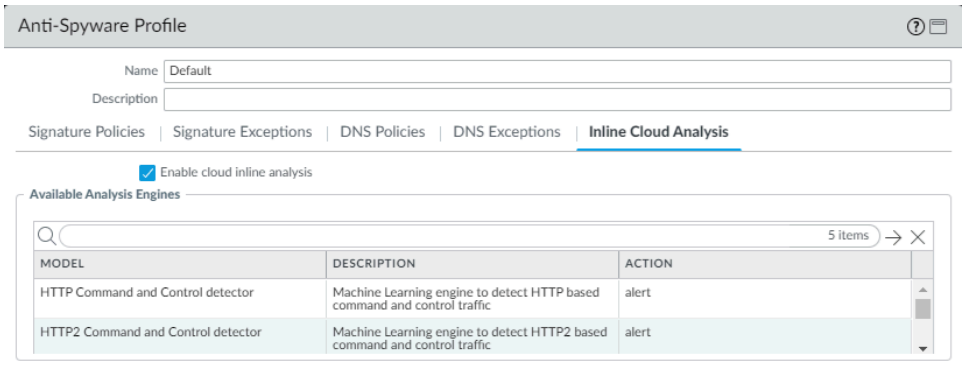
현재 활성화된 라이선스가 있는 구독을 확인하려면 디바이스 > 라이선스를 선택한 다음 적절한 라이선스가 표시되고 만료되지 않았는지 확인합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 새 스파이웨어 방지 보안 프로파일을 업데이트하거나 만들어 인라인 클라우드 분석을 사용하도록 설정합니다.

1. 기존 스파이웨어 방지 프로파일을 선택하거나 새 프로파일을 추가합니다(개체 > 보안 프로파일 > 스파이웨어 방지).
2. 안티스파이웨어 프로파일을 선택한 다음 인라인 클라우드 분석 및 인라인 클라우드 분석 활성화로 이동합니다.




3. 해당 분석 엔진을 사용하여 위협이 감지될 때 수행할 작업을 지정합니다. 다음 옵션을 사용할 수 있습니다.

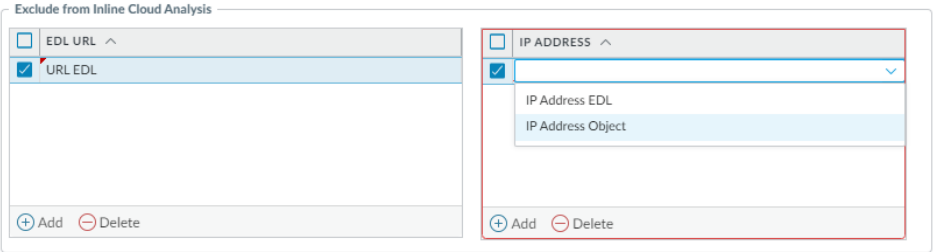
   각 분석 엔진의 기본 작업은 경고이지만, *Palo Alto Networks*는 최상의 보안 상태를 위해 모든 작업을 모두 재설정으로 설정할 것을 권장합니다.

   - **Allow** - 요청이 허용되고 로그 항목이 생성되지 않습니다.
   - **Alert** - 요청이 허용되고 위협 로그 항목이 생성됩니다.
   - **Drop** - 요청을 삭제합니다. 재설정 작업은 호스트/애플리케이션으로 전송되지 않습니다.
   - **Reset-Client** - TCP의 경우 클라이언트 측 연결을 재설정합니다.
   - **Reset-Server** - 클라이언트 측 연결을 재설정합니다.
   - **Reset-Both** - 클라이언트와 서버 측 모두에서 연결을 재설정합니다.
4. 확인을 클릭하여 스파이웨어 방지 프로파일 구성 대화 상자를 종료하고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) 인라인 클라우드 분석이 오탐을 생성하는 경우 안티스파이웨어 프로파일에 URL 및/또는 IP 주소 예외를 추가합니다. 외부 동적 목록(URL 또는 IP 주소 목록 유형) 또는 주소 개체를 지정하여 예외를 추가할 수 있습니다.

1. 외부 동적 목록 또는 [IP] 주소 개체 예외를 추가합니다.
2. 개체 **>** 보안 프로파일 **>** 안티스파이웨어를 선택합니다.
3. 특정 URL 및/또는 IP 주소를 제외할 안티스파이웨어 프로파일을 선택한 다음 인라인 클라우드 분석을 선택합니다.
4. 추가하려는 예외 유형에 따라 **EDL URL** 또는 **IP** 주소를 추가한 다음 기존 URL 또는 IP 주소 외부 동적 목록을 선택합니다. 사용할 수 없는 경우 새 외부 동적 목록을 만듭니다. IP 주소 예외의 경우 선택적으로 주소 개체 목록을 선택할 수 있습니다.




5. 확인을 클릭하여 스파이웨어 방지 프로파일을 저장하고 변경 사항을 커밋합니다.

**STEP 5 |** Advanced Threat Prevention 인라인 클라우드 분석 서비스에 인증하는 데 사용되는 업데이트된 방화벽 기기 인증서를 설치합니다. 인라인 클라우드 분석이 활성화된 모든 방화벽에 대해 반복합니다.

**STEP 6 |** (선택 사항) 인라인 클라우드 분석 서비스 요청을 처리하기 위해 방화벽에서 사용하는 클라우드 콘텐츠 FQDN(정규화된 도메인 이름)을 설정합니다. 기본 FQDN은 hawkeye.services-edge.paloaltonetworks.com에 연결한 다음 가장 가까운 클라우드 서비스 서버로 확인합니다. 데이터 상주 및 성능 요구 사항을 가장 잘 충족하는 지역 클라우드 콘텐츠 서버를 지정하여 자동 서버 선택을 재정의할 수 있습니다.

클라우드 콘텐츠 *FQDN*은 전역적으로 사용되는 리소스이며 이 연결에 의존하는 다른 서비스가 트래픽 페이로드를 보내는 방법에 영향을 줍니다.

방화벽이 올바른 Content Cloud FQDN을 사용하는지 확인합니다(디바이스**e** > 설정 > **Content-ID** > 콘텐츠 클라우드 설정). 필요한 경우 FQDN을 변경하십시오.

- US - **us.hawkeye.services-edge.paloaltonetworks.com**
- EU - **eu.hawkeye.services-edge.paloaltonetworks.com**
- UK - **uk.hawkeye.services-edge.paloaltonetworks.com**

  영국 기반의 클라우드 콘텐츠 *FQDN*은 *EU*에 위치한 백엔드 서비스*(eu.hawkeye.services-edge.paloaltonetworks.com)*에 연결하여 *Advanced Threat Prevention* 인라인 클라우드 분석 서비스 지원을 제공합니다.
- APAC - **apac.hawkeye.services-edge.paloaltonetworks.com**


©2023 Palo Alto Networks, Inc.

**STEP 7 |** (선택 사항) 고급 위협 방지 클라우드 서비스에 대한 방화벽 연결 상태를 확인합니다.

방화벽에서 다음 CLI 명령을 사용하여 연결 상태를 확인합니다.

```
show ctd-agent status security-client
```

예:

```
show ctd-agent status security-client ... Security
 Client AceMlc2(1) 현재 클라우드 서버: hawkeye.services-
edge.paloaltonetworks.com Cloud connection: connected ...
```

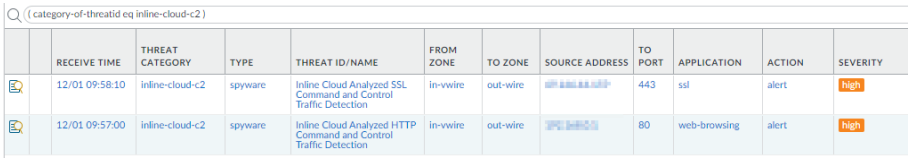
*CLI* 출력은 간결함을 위해 간략하게 표시되었습니다.

Advanced Threat Prevention 클라우드 서비스에 연결할 수 없는 경우 hawkeye.services-edge.paloaltonetworks.com 도메인이 차단되고 있지 않은지 확인합니다.

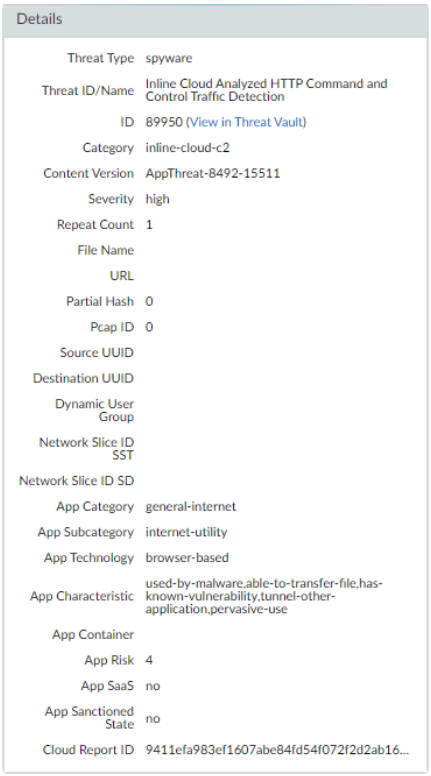

©2023 Palo Alto Networks, Inc.

**STEP 8 |** (선택 사항) 인라인 클라우드 분석을 사용하여 탐지된 C2 위협에 대한 방화벽의 활동을 모니터링합니다.

1. 모니터 > 로그 > 위협을 선택하고 **(category-of-threatid eq inline-cloud-c2)**로 필터링합니다. Advanced Threat Prevention의 인라인 클라우드 분석 메커니즘을 사용하여 분석된 로그를 봅니다.




2. 로그 항목을 선택하여 검색된 C2 위협의 세부 정보를 봅니다.
3. 카테고리 위협은 상세 로그 보기의 세부 정보 창 아래에 표시됩니다. 인라인 클라우드 분석을 사용하여 탐지된 C2 위협에는 inline-cloud-c2의 위협 카테고리가 있습니다.




 ©2023 Palo Alto Networks, Inc.

# WildFire Inline ML

바이러스 백신 프로파일에 있는 WildFire 인라인 ML 옵션을 사용하면 방화벽 데이터플레인이 PE(휴대용 실행 파일), ELF(실행 파일 및 연결된 형식) 및 MS Office 파일, PowerShell 및 셸 스크립트에 기계 학습을 실시간으로 적용할 수 있습니다. 이 바이러스 백신 보호 레이어는 WildFire 기반 서명을 보완하여 서명이 아직 존재하지 않는 파일에 대한 확장된 커버리지를 제공합니다. 각 인라인 ML 모델은 파일의 높은 확률 분류를 공식화하기 위해 디코더 필드 및 패턴을 포함한 파일 세부 정보를 평가하여 특정 유형의 악성 파일을 동적으로 탐지합니다. 이 보호는 Palo Alto Networks가 악의적인 것으로 확인된 특성과 일치하는 위협의 미래 변형뿐만 아니라 현재 알려지지 않은 것으로 확장됩니다. 위협 환경의 최신 변경 사항을 따라잡기 위해 인라인 ML 모델은 콘텐츠 릴리스를 통해 추가 또는 업데이트됩니다. WildFire 인라인 ML을 활성화하려면 활성 WildFire 구독을 보유해야 합니다.

URL 필터링 구성의 일부로 악성 URL을 실시간으로 감지할 수 있는 INline ML 기반 보호 기능을 사용할 수도 있습니다. 자세한 내용은 로컬 인라인 분류을(를) 참조하십시오.

***WildFire*** 인라인 ***ML***은 ***VM-50*** 또는 ***VM50L*** 가상 어플라이언스에서 지원되지 않습니다.

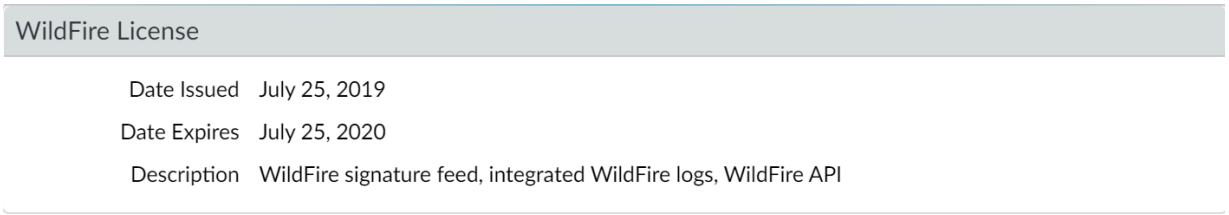
## WildFire Inline ML 구성

WildFire 인라인 ML 구성을 활성화하려면 인라인 ML 설정으로 구성된 바이러스 백신 프로파일을 보안 정책 규칙에 연결합니다(바이러스 백신 설정, 안티 스파이웨어 및 취약점 보호설정 참조).

***WildFire*** 인라인 ***ML***는 현재 ***VM-50*** 또는 ***VM50L*** 가상 어플라이언스에서 지원되지 않습니다.

**STEP 1 |** WildFire 인라인 ML을 활용하려면 Windows 실행 기능을 분석하기 위해 활성 WildFire 구독이 있어야 합니다.

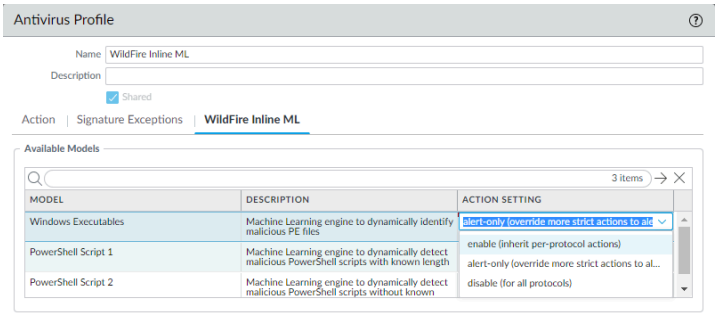
WildFire 구독이 있는지 확인합니다. 현재 라이선스가 있는 구독을 확인하려면 디바이스 > 라이선스를 선택한 다음 적절한 라이선스가 표시되고 만료되지 않았는지 확인합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 실시간 WildFire 인라인 ML 모델을 사용하도록 새 바이러스 백신 보안 프로파일을 만들거나 기존 바이러스 백신 보안 프로파일을 업데이트합니다.

1. 기존 바이러스 백신 프로파일을 선택하거나 새 프로파일을 생성합니다(바이러스 백신 **>** 보안 프로파일에 **>** 개체를 선택한 다음 새 프로파일을 추가합니다.
2. 바이러스 백신 프로파일을 구성합니다.
3. **WildFire** 인라인 **ML** 탭을 선택한 다음 각 WildFire 인라인 ML 모델에 대한 액션 설정을 적용합니다. 이렇게 하면 모델별로 각 프로토콜에 대해 구성된 WildFire 인라인 ML 작업 설정이 적용됩니다. 다음과 같은 분류 엔진을 사용할 수 있습니다.
   - 윈도우 실행 파일
   - PowerShell 스크립트 1
   - PowerShell 스크립트 2
   - 실행 가능한 연결된 형식(PAN-OS 콘텐츠 릴리스 8367 이상 설치와 함께 사용 가능)
   - MSOffice(PAN-OS 콘텐츠 릴리스 8434 이상 설치와 함께 사용 가능)
   - 셸 스크립트(PAN-OS 콘텐츠 릴리스 8543 이상 설치와 함께 사용 가능)




   - 사용**(**프로토콜당 상속**)** - WildFire는 액션 탭의 디코더 섹션의 WildFire 인라인 ML 액션 열에서 선택한 항목에 따라 트래픽을 검사합니다.
   - 경고 전용**(**경고할 더 엄격한 동작을 재정의**)**-WildFire는 액션 탭의 디코더 섹션에서 WildFire 인라인 ML 액션 컬럼의 선택에 따라 트래픽을 검사하고 **경고**보다 높은 심각도 수준으로 모든 작업을 재정의하고(**드롭**, **재설정 클라이언트**, **재설정 서버**, **리셋-둘다 경고**) 위협 로그에 경고를 생성하고 저장하는 동안 트래픽이 통과할 수 있도록 합니다.
   - 비활성화**(**모든 프로토콜에 대해**)** - WildFire를 사용하면 정책 조치 없이 트래픽이 통과할 수 있습니다.
4. 확인을 클릭하여 바이러스 백신 프로파일 구성 창을 종료하고 새 설정을 커밋합니다.

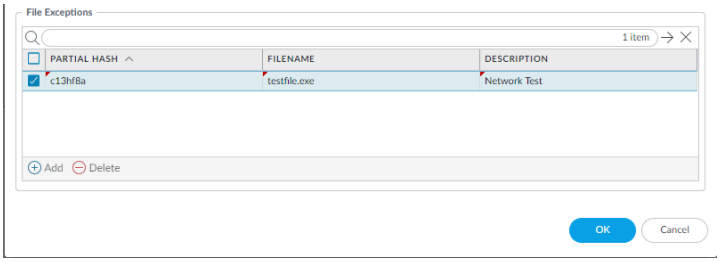
**STEP 3 |** (선택 사항) 오탐(false-positive)이 발생한 경우 바이러스 백신 보안 프로파일에 파일 예외를 추가합니다. 이는 일반적으로 분석을 위해 WildFire에 파일을 포워딩하지 않는 사용자를 위해 수행됩니다.


©2023 Palo Alto Networks, Inc.

예외 목록에 직접 추가하거나 위협 로그에서 파일을 지정하여 파일 예외 세부 정보를 추가할 수 있습니다.

*WildFire* 분석 보안 프로파일이 *WildFire* 인라인 *ML*를 사용하여 분석된 파일 유형을 포워딩하도록 구성된 경우 오탐*(false-positive)*이 수신될 때 자동으로 수정됩니다*. WildFire* 분석에 의해 양성으로 분류된 파일에 대한 *ml* 바이러스 경고를 계속 볼 경우 *Palo Alto Networks* 지원팀에 문의하십시오*.*

- 예외 목록에 직접 파일 예외를 추가합니다.
  1. 개체 보안 프로파일을 선택합니다.
  2. 특정 파일을 제외하려는 바이러스 백신 프로파일을 선택한 다음 **WildFire** 인라인 **ML**을 선택합니다.
  3. 적용에서 제외하려는 파일의 해시, 파일 이름 및 설명을 추가합니다.




  4. 확인을 클릭하여 바이러스 백신 프로파일을 저장한 다음 업데이트를 커밋합니다.
- 위협 로그 항목에서 파일 예외를 추가합니다.
  1. 모니터 **>** 로그 **>** 위협을 선택한 다음 **ml** 바이러스 위협 유형에 대한 로그를 필터링합니다. 파일 예외를 만들려는 파일에 대한 위협 로그를 선택합니다.
  2. 상세 로그 뷰로 이동하여 세부 정보 창으로 스크롤한 다음 예외 생성을 선택합니다.




  3. 설명을 추가하고 확인을 클릭하여 파일 예외를 추가합니다.
  4. 새 파일 예외는 개체 **>** 보안 프로파일 **>** 안티바이러스 **> WildFire Inline ML**에서 파일 예외 목록을 찾을 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) 방화벽이 Inline ML 클라우드 서비스에 연결되었는지 확인합니다.

방화벽에서 다음 CLI 명령을 사용하여 연결 상태를 확인합니다.

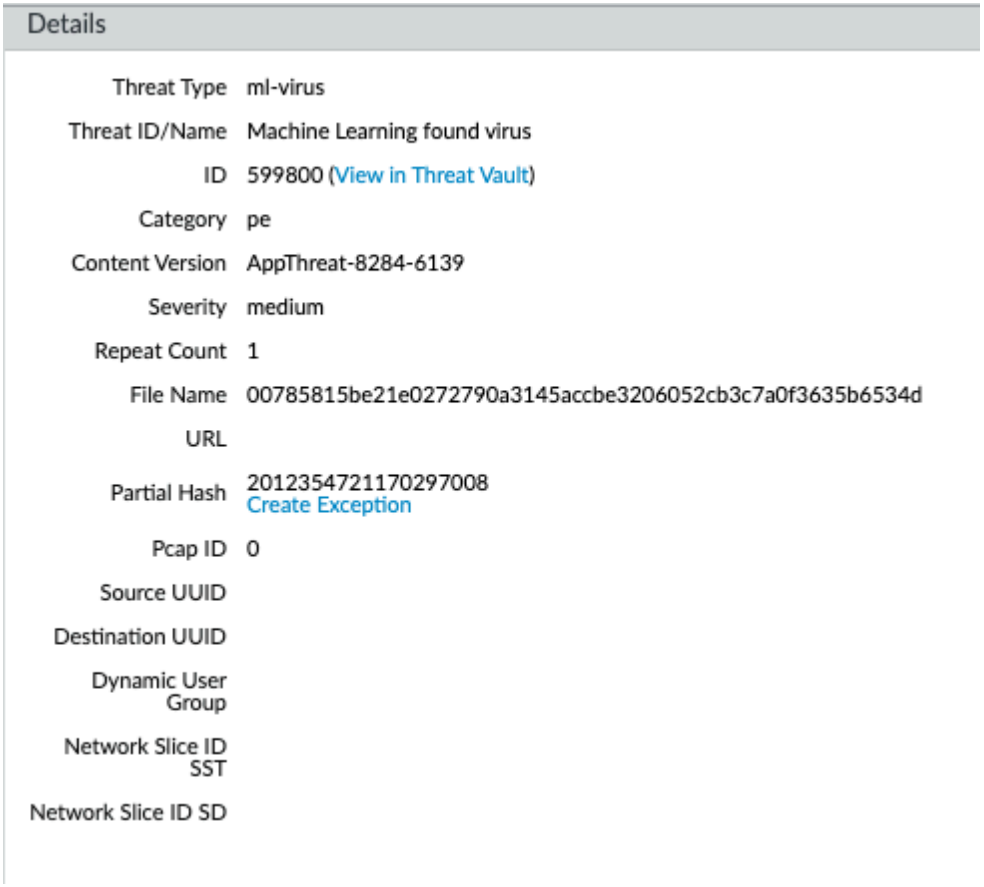
```
mlav 클라우드 상태 보기
```

예:

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

Inline ML 클라우드 서비스에 연결할 수 없는 경우 다음 도메인이 차단되지 않았는지 ml.service.paloaltonetworks.com을 확인합니다.

WildFire Inline ML를 사용하여 검색된 파일에 대한 정보를 보려면 위협 로그를 검사합니다(모니터 **>** 로그 **>** 위협 경로에서 다음 목록의 로그 유형을 선택합니다). WildFire 인라인 ML를 사용하여 분석된 파일은 위협 유형 **ml-virus**:




로 레이블이 지정됩니다.

 ©2023 Palo Alto Networks, Inc.

# 파일 차단 설정

파일 차단 프로파일을 사용하면 차단하거나 모니터링할 특정 파일 형식을 식별할 수 있습니다. 대부분의 트래픽(내부 네트워크의 트래픽 포함)의 경우 위협이 있는 것으로 알려져 있거나 업로드/다운로드에 대한 실제 사용 사례가 없는 파일을 차단합니다. 현재 이러한 파일에는 배치 파일, DLL, Java 클래스 파일, 도움말 파일, Windows 바로 가기(.lnk) 및 BitTorrent 파일이 포함됩니다. 또한 드라이브 바이 다운로드 보호 기능을 제공하려면 실행 파일 및 아카이브 파일(.zip 및.rar)의 다운로드/업로드를 허용하되 사용자가 파일을 전송하고 있음을 확인하여 브라우저가 인식하지 못하는 것을 다운로드하려고 한다는 것을 확인하도록 합니다. 일반적인 웹 브라우징을 허용하는 정책 규칙의 경우 사용자가 모르는 사이에 악성 파일을 다운로드할 위험이 훨씬 높으므로 파일 차단을 더욱 엄격하게 해야 합니다. 이러한 유형의 트래픽의 경우 이동식 실행 파일(PE)도 차단하는 보다 엄격한 파일 차단 프로파일을 추가하십시오.

보안 정책 규칙에 파일 차단을 적용할 때 고유한 사용자 지정 파일 차단 프로파일을 정의하거나 다음과 같은 사전 정의된 프로파일 중 하나를 선택할 수 있습니다. 콘텐츠 릴리스 버전 653 이상에서 사용할 수 있는 사전 정의된 프로파일을 복사 및 편집한 다음 파일 차단 프로파일 안전 전환 단계에 따라 모범 사례 파일 차단 설정으로 전환할 때 애플리케이션 가용성을 유지할 수 있습니다.

- 기본 파일 차단 - 덜 민감한 애플리케이션에서 트래픽이 멀웨어 공격 캠페인에 일반적으로 포함되거나 업로드/다운로드에 대한 실제 사용 사례가 없는 파일을 차단할 수 있도록 하는 보안 정책 규칙에 이 프로파일을 연결합니다. 이 프로파일은 PE 파일(.scr, .cpl, .dll, .ocx, .pif, .exe), 자바 파일(.class, .jar), 도움말 파일(.chm, .hlp) 및 .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat 등 잠재적으로 악의적인 파일 유형의 업로드 및 다운로드를 차단합니다. 또한 암호화된 rar 또는 암호화된 zip 파일을 다운로드하려고 할 때 사용자에게 인증하라는 메시지가 표시됩니다. 이 규칙은 다른 모든 파일 유형에 대해 경고하여 네트워크 안팎으로 들어오는 모든 파일 유형에 대한 완전한 가시성을 제공합니다.
- 엄격한 파일 차단- 가장 중요한 애플리케이션에 액세스할 수 있도록 하는 보안 정책 규칙에 이 엄격한 프로파일을 사용합니다. 이 프로파일은 다른 프로파일과 동일한 파일 형식을 차단하고 플래시, .tar, 다단계 인코딩, .cab, .msi, 암호화된 지퍼 파일 및 암호화된 zip 파일을 추가로 차단합니다.

이러한 사전 정의된 프로파일은 네트워크에 가장 안전한 상태를 제공하도록 설계되었습니다. 그러나 이러한 기본 프로파일에서 차단된 일부 애플리케이션에 의존하는 비즈니스 크리티컬 애플리케이션이 있는 경우 프로파일을 복사하고 필요에 따라 수정할 수 있습니다. 위험한 파일 형식을 업로드 및/또는 다운로드해야 하는 사용자에 대해서만 수정된 프로파일을 사용해야 합니다. 또한 공격 영역을 줄이려면 다른 보안 조치를 사용하여 사용자가 업로드하고 다운로드하는 파일이 조직에 위협이 되지 않도록 해야 합니다. 예를 들어 PE 파일의 다운로드를 허용해야 하는 경우 알 수 없는 모든 PE 파일을 WildFire foranalysis로 보내고 있는지 확인합니다. 또한 사용자가 악성 콘텐츠를 호스팅하는 것으로 알려진 웹사이트에서 콘텐츠를 다운로드할 수 없도록 엄격한 URL 필터링 정책을 유지합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 파일 차단 프로파일을 생성합니다.

1. 개체 > 보안 프로파일 > 파일 차단을 선택하고 프로파일을 추가합니다.
2. 파일 차단 프로파일의 이름(예: **Block_EXE**)을 입력합니다.
3. (선택사항) **사용자가 웹사이트에서 exe 파일을 다운로드하지 못하도록 차단**과 같은 설명을 입력합니다.
4. (선택 사항) 프로파일이 다음과 공유되도록 지정합니다.
   - 다중 가상 시스템 방화벽의 모든 가상 시스템**(vsys)** - 선택을 취소하면(비활성화) 프로파일은 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다.
   - **Panorama**의 모든 디바이스 그룹-삭제(비활성화)하는 경우 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
5. (선택 사항 - Panorama 전용) 관리자가 프로파일을 상속하는 디바이스 그룹에서 이 파일 차단 프로파일의 설정을 무시하지 못하도록 하려면 재정의 비활성화를 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.

**STEP 2 |** 파일 차단 옵션을 구성합니다.

1. 추가하고 프로파일에 대한 규칙을 정의합니다.
2. **BlockEXE**와 같이 규칙의 이름을 입력합니다.
3. 모두를 선택하거나 필터링을 위해 하나 이상의 특정 애플리케이션(예: 웹 브라우징)을 지정합니다.

   웹 브라우저에서만 응답 페이지**(**계속 프롬프트**)**를 표시할 수 있습니다**.** 이 페이지를 통해 다른 애플리케이션을 선택하면 사용자가 계속할 수 있는 프롬프트가 표시되지 않으므로 해당 애플리케이션에 대한 트래픽이 차단됩니다**.**
4. 모두를 선택하거나 하나 이상의 특정 파일 형식(예: **exe**)을 지정합니다.
5. 다운로드와 같은방향을 지정합니다.
6. **Action**(**alert**, **block** 또는 **continue**)을 지정합니다. 예를 들어 실행 파일(.exe)을 다운로드하기 전에 사용자에게 확인 메시지를 표시하려면 계속을 선택합니다. 또는 지정된 파일을 차단하거나 사용자가 실행 파일을 다운로드할 때 단순히 경고를 트리거하도록 방화벽을 구성할 수 있습니다.
7. 확인을 클릭하여 프로파일을 저장합니다.

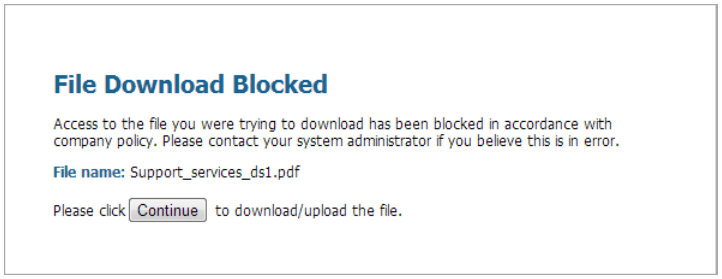
**STEP 3 |** 파일 차단 프로파일을 보안 정책 규칙에 적용합니다.

1. 정책 > 보안을 선택하고 기존 정책 규칙을 선택하거나 기본 보안 정책 설정에 설명된 대로 새 규칙을 추가합니다.
2. 작업 탭에서 이전 단계에서 구성한 파일 차단 프로파일을 선택합니다. 이 예에서 프로파일 이름은**Block_EXE**입니다.
3. 구성을 커밋합니다.

**STEP 4 |** 파일 차단 구성을 테스트하려면 방화벽의 트러스트 영역에 있는 엔드포인트 PC에 액세스하고 언트러스트 영역의 웹사이트에서 실행 파일을 다운로드하려고 하면 응답 페이지가 표시됩니다. 계속을 클릭하여 파일을 다운로드할 수 있는지 확인합니다. 사용자가 다운로드를 계속할 수 있는 옵션을 제

 ©2023 Palo Alto Networks, Inc.

공하지 않는 경고 또는 차단과 같은 다른 작업을 설정할 수도 있습니다. 다음은 파일 차단에 대한 기본 응답 페이지를 보여줍니다.




**STEP 5 |** (선택 사항) 사용자 지정 파일 차단 응답 페이지를 정의합니다(디바이스 > 응답 페이지). 이렇게 하면 사용자가 응답 페이지를 볼 때 더 많은 정보를 제공할 수 있습니다. 헬프데스크에 대한 회사 정책 정보 및 연락처 정보와 같은 정보를 포함할 수 있습니다.

계속 작업을 사용하여 파일 차단 프로파일을 만드는 경우 웹 검색 애플리케이션만 선택할 수 있습니다. 다른 애플리케이션을 선택하면 계속할 수 있는 옵션이 사용자에게 표시되지 않으므로 보안 정책과 일치하는 트래픽이 방화벽을 통과하지 않습니다. 또한 ***HTTPS*** 웹사이트에 대한 복호화 정책을 구성하고 사용하도록 설정해야 합니다.

로그를 확인하여 이 기능을 테스트할 때 사용되는 애플리케이션을 확인하십시오. 예를 들어 ***Microsoft SharePoint***를 사용하여 파일을 다운로드하는 경우 웹 브라우저를 사용하여 사이트에 액세스하는 경우에도 애플리케이션은 실제로 **쉐어 포인트 기반** 또는 **쉐어 포인트 문서**입니다. **(**테스트를 위해 애플리케이션 유형을 ***Any***로 설정하는 데 도움이 될 수 있습니다.**)**

 ©2023 Palo Alto Networks, Inc.

# 무차별 대입 공격 방지

무차별 대입 공격은 동일한 소스 또는 대상 IP 주소에서 대량의 요청/응답을 사용하여 시스템에 침입합니다. 공격자는 시도 또는 요청에 대한 응답을 추측하기 위해 시행 착오 방법을 사용합니다.

방화벽의 취약점 보호 프로파일에는 무차별 대입 공격으로부터 사용자를 보호하는 서명이 포함되어 있습니다. 각 서명에는 ID, 위협 이름 및 심각도가 있으며 패턴이 기록될 때 트리거됩니다. 패턴은 트래픽이 무차별 암호 계수 공격으로 식별되는 조건과 인터벌을 지정합니다. 일부 서명은 심각도가 낮은 다른 자식 서명과 연결되며 일치하는 패턴을 지정합니다. 패턴이 서명 또는 자식 서명과 일치하면 서명의 기본 작업이 트리거됩니다.

보호를 적용하려면 다음을 수행하십시오.

- 취약점 보호 프로파일을 보안 정책 규칙에 첨부합니다. 바이러스 백신 설정, 안티 스파이웨어 및 취약점 보호를 참조하십시오.
- 새로운 위협으로부터 보호하기 위해 새 서명이 포함된 콘텐츠 업데이트를 설치합니다. 콘텐츠 및 소프트웨어 업데이트 설치를 참조하십시오.


©2023 Palo Alto Networks, Inc.

# 무차별 암호 대입 서명에 대한 작업 및 트리거 조건 사용자 지정

방화벽에는 사전 정의된 두 가지 유형의 무차별 서명, 부모 서명 및 자식 서명이 포함됩니다. 자식 서명은 서명과 일치하는 트래픽 패턴의 단일 발생입니다. 부모 서명은 자식 서명과 연결되며 지정된 시간 간격 내에 여러 이벤트가 발생하고 자식 서명에 정의된 트래픽 패턴과 일치할 때 트리거됩니다.

일반적으로 하위 서명의 기본 작업은 단일 이벤트가 공격을 나타내지 않기 때문에 허용됩니다. 이렇게 하면 합법적인 트래픽이 차단되지 않고 주목할 만한 이벤트에 대한 위협 로그를 생성하지 않습니다. Palo Alto Networks는 고려 대상에서 배제하고 기본 작업을 변경하지 않는 것이 좋습니다.

대부분의 경우 무차별 서명은 반복되는 패턴으로 인해 주목할 만한 이벤트입니다. 필요한 경우 다음 중 하나를 수행하여 무차별 서명에 대한 작업을 사용자 지정할 수 있습니다.

- 무차별 암호 카테고리의 모든 서명에 대한 기본 작업을 수정하는 규칙을 생성합니다. 트래픽을 허용, 경고, 차단, 재설정 또는 삭제하도록 선택할 수 있습니다.
- 특정 서명에 대한 예외를 정의합니다. 예를 들어 CVE에 대한 예외를 검색하고 정의할 수 있습니다.

부모 서명의 경우 트리거 조건과 작업을 모두 수정할 수 있습니다. 자식 서명의 경우 작업만 수정할 수 있습니다.



공격을 효과적으로 완화하려면 대부분의 무차별 서명에 대한 드롭 또는 재설정 작업 대신 블록 ***ip*** 주소 작업을 지정합니다**.**

**STEP 1 |** 새 취약점 보호 프로파일을 생성합니다.

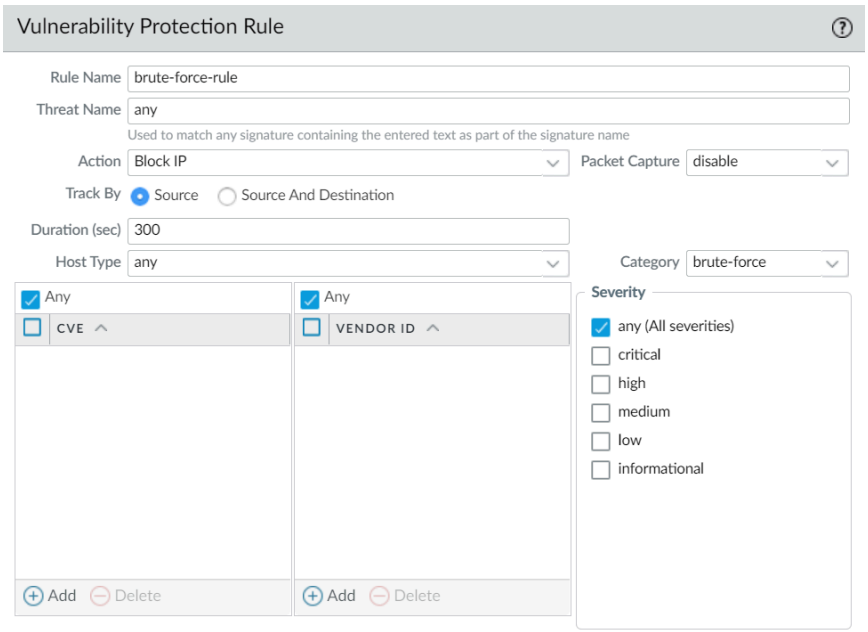
1. 개체 > 보안 프로파일 > 취약점 보호를 선택하고 프로파일을 추가합니다.
2. 취약점 보호 프로파일에 대한 이름을 입력합니다.
3. (선택 사항) 설명을 입력합니다.
4. (선택 사항) 프로파일이 다음과 공유되도록 지정합니다.
   - 다중 가상 시스템 방화벽의 모든 가상 시스템**(vsys)** - 선택을 취소하면(비활성화) 프로파일은 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다.
   - **Panorama**의 모든 디바이스 그룹-삭제(비활성화)하는 경우 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
5. (선택 사항-Panorama 전용) 관리자가 프로파일을 상속하는 디바이스 그룹에서 이 취약점 보호 프로파일의 설정을 재정의 비활성화로 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 카테고리의 모든 서명에 대한 작업을 정의하는 규칙을 생성합니다.

1. 규칙 탭에서 추가하고 새 규칙의 규칙 이름을 입력합니다.
2. (선택 사항) 특정 위협 이름을 지정합니다(기본값은 **any**).
3. 액션을 설정합니다. 이 예제에서는 **IP** 차단으로 설정됩니다.

   *IP* 차단을 위해 취약점 보호 프로파일을 설정한 경우 방화벽은 먼저 하드웨어를 사용하여 *IP* 주소를 차단합니다. 공격 트래픽이 하드웨어의 차단 용량을 초과하는 경우 방화벽은 소프트웨어 차단 메커니즘을 사용하여 나머지 *IP* 주소를 차단합니다.
4. 카테고리를 무차별 대입으로 설정합니다.
5. (선택 사항) 차단하는 경우 차단할 호스트 유형을 지정합니다. 서버 또는 클라이언트(기본값은 모든).
6. 특정 서명에 대한 작업을 사용자 지정하려면 3단계를 참조하십시오.
7. 상위 서명에 대한 트리거 임계값을 사용자 지정하는 4단계를 참조하십시오.




8. 규칙과 프로파일을 저장하려면 확인을 클릭합니다.

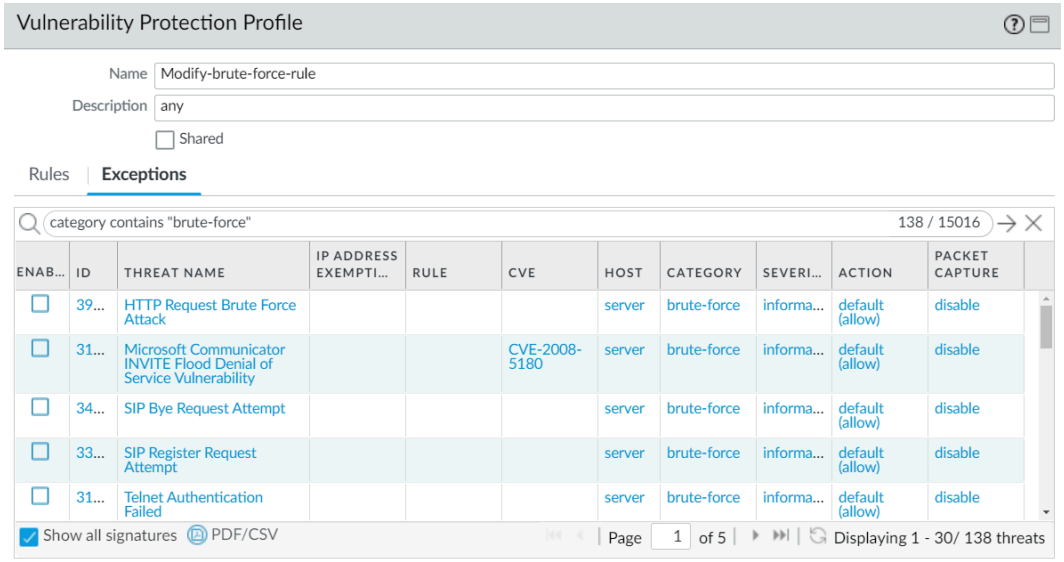

©2023 Palo Alto Networks, Inc.

**STEP 3 |** (선택 사항) 특정 서명에 대한 작업을 사용자 지정합니다.

1. 예외 탭에서 모든 서명을 표시하여 수정할 서명을 찾습니다.

   무차별 암호 대입 카테고리의 모든 서명을 보려면 **'무차별 대입 공격'을 포함한 카테고리**가 포함되어 있습니다.

2. 특정 서명을 편집하려면 작업 열에서 사전 정의된 기본 작업을 클릭합니다.




3. 작업을 설정합니다. 허용, 경고,, 블록 **IP**, 또는 드롭. 블록 **IP**를 선택하면 다음 추가 작업을 완료하십시오.

   **1.** 작업을 트리거할 기간(초)을 지정합니다.

   **2.** **IP** 소스 또는 **IP** 소스 및 대상을 사용하여 IP 주소를 추적 및 차단할지의 여부를 지정합니다.

4. 확인을 클릭합니다.
5. 수정된 각 서명에 대해 활성화 컬럼에서 체크박스를 선택합니다.
6. 확인을 클릭합니다.

**STEP 4 |** 상위 서명에 대한 트리거 조건을 사용자 지정합니다.

편집할 수 있는 부모 서명에는 이 아이콘이 표시됩니다.

이 예제에서는 검색 기준이 무차별 암호 계수 카테고리와 CVE-2008-1447이었습니다.

1. 편집() 서명에 대한 시간 특성 및 집계 기준입니다.
2. 트리거 임계값을 수정하려면 초 단위로 적중 횟수를 지정합니다.
3. 적중 수(집계 기준)를 소스, 대상 또는 소스 및 대상별로 집계할지 여부를 지정합니다.
4. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 이 새 프로파일을 보안 정책 규칙에 첨부합니다.

1. 정책 > 보안 및 추가를 선택하거나 보안 정책 규칙을 수정합니다.
2. 작업 탭에서 프로파일 설정의 프로파일 유형으로 프로파일을 선택합니다.
3. 취약점 보호 프로파일을 선택합니다.
4. 확인을 클릭합니다.

**STEP 6 |** 변경 사항을 커밋합니다.

1. 커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 회피 서명 활성화

Palo Alto Networks 회피 서명은 조작된 HTTP 또는 TLS 요청을 감지하고 클라이언트가 DNS 쿼리에 지정된 도메인이 아닌 다른 도메인에 연결하는 인스턴스에 경고할 수 있습니다. 회피 서명은 방화벽이 DNS 프록시 역할을 하고 도메인 이름 쿼리를 해결하도록 설정된 경우에만 유효합니다. 모범 사례로 다음 단계를 수행하여 회피 서명을 활성화하십시오.

**STEP 1 |** DNS 프록시 역할을 하도록 클라이언트 및 서버에 대한 중간 방화벽을 활성화합니다.

다음을 포함하여 DNS 프록시 개체를 구성합니다.

- 방화벽이 DNS 쿼리를 수신할 인터페이스를 지정합니다.
- 방화벽이 DNS 요청을 해결하기 위해 통신하는 DNS 서버를 정의합니다.
- 방화벽이 DNS 서버에 연결하지 않고 로컬로 확인할 수 있는 정적 FQDN-to-IP 주소 항목을 설정합니다.
- 확인된 호스트 이름-IP 주소 매핑에 대해 캐싱을 활성화합니다.

**STEP 2 |** 최신 애플리케이션 및 위협 콘텐츠 버전(최소 콘텐츠 버전 579 이상)을 받으십시오.

1. 디바이스 > 동적 업데이트를 선택합니다.
2. 최신 애플리케이션 및 위협 콘텐츠 업데이트를 받으려면 지금 확인하십시오.
3. 애플리케이션 및 위협 콘텐츠 버전 579(이상)를 다운로드하고 설치합니다.

**STEP 3 |** 방화벽이 회피 서명과 일치하는 트래픽을 적용하는 방법을 정의합니다.

1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택한 다음 안티 스파이웨어 프로파일을 추가하거나 수정합니다.
2. 예외를 선택한 다음 **Show all signatures**를 선택합니다.
3. 키워드 **회피**를 기반으로 서명을 필터링합니다.
4. 모든 회피 서명에 대해 작업을 허용 또는 기본 작업 이외의 설정으로 설정합니다(회피 서명에 대한 기본 작업은 허용임). 예를 들어 서명 ID 14978 및 14984에 대한 작업을 경고 또는 삭제로 설정합니다.
5. 확인을 클릭하여 업데이트된 안티스파이웨어 프로파일을 저장합니다.
6. 스파이웨어 방지 프로파일을 보안 정책 규칙에 연결합니다. 정책 > 보안을 선택한 다음 수정할 정책을 선택한 다음 작업 탭을 클릭합니다. 프로파일 설정에서 안티스파이웨어 옆에 있는 드롭다운을 클릭하고 방금 수정한 안티스파이웨어 프로파일을 선택하여 회피 서명을 적용합니다.

**STEP 4 |** 변경 사항을 커밋합니다.

커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 차단된 IP 주소 모니터링

방화벽은 차단하는 소스 IP 주소의 차단 목록을 유지합니다. 방화벽이 다음 정책 규칙 중 하나를 구성할 때와 같은 소스 IP 주소를 차단하면 방화벽은 해당 패킷이 CPU 또는 패킷 버퍼 리소스를 사용하기 전에 하드웨어에서 해당 트래픽을 차단합니다.

- 보호 조치와 분류된 DoS 방어 정책 규칙(새 세션 플러딩에 대한 DoS 보호에 설명된 대로, 분류된 DoS 보호 정책은 들어오는 연결이 소스 IP 주소, 대상 IP 주소 또는 소스 및 대상 IP 주소 쌍과 일치하도록 지정하고 분류된 DoS 보호 프로파일과 연결됨).
- 취약점 보호 프로파일을 사용하는 보안 정책 규칙

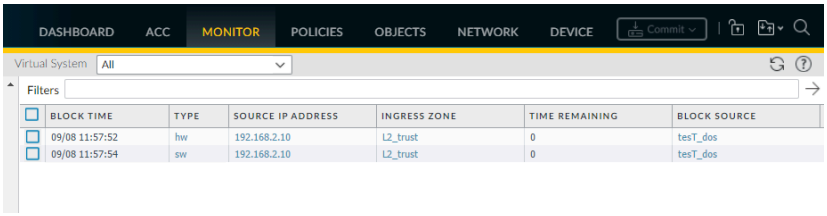
하드웨어 IP 주소 차단은 PA-3200 시리즈, PA-5200 시리즈, PA-5400 시리즈(PA-5450 제외) 및 PA-7000 시리즈 방화벽에서 지원됩니다.

차단 목록을 보거나, 차단 목록에서 IP 주소에 대한 자세한 정보를 얻거나, 하드웨어 및 소프트웨어가 차단하고 있는 주소 수를 볼 수 있습니다. 차단해서는 안 된다고 생각되는 경우 목록에서 IP 주소를 삭제할 수 있습니다. 목록의 주소에 대한 자세한 정보의 출처를 변경할 수 있습니다. 하드웨어가 IP 주소를 차단하는 빈도를 변경할 수도 있습니다.

◉ 보기 차단 목록 항목입니다.

1. 모니터 > 차단 **IP** 목록을 선택합니다.

   차단 목록의 항목은 형식 열에서 하드웨어(hw) 또는 소프트웨어(sw)에 의해 차단되었는지의 여부를 나타냅니다.
2. 화면 하단에서 보기:
   - 차단된 IP 주소 수 중 차단된 총 **IP** 수입니다.
   - 방화벽이 사용한 차단 목록의 백분율입니다.
3. 표시된 항목을 필터링하려면 열(필터 필드에 필터를 만드는 값)과 필터 적용(→)에서 값을 선택합니다. 그렇지 않으면 방화벽에 처음 1,000개의 항목이 표시됩니다.
4. 페이지 번호를 입력하거나 화면 하단의 화살표를 클릭하여 항목 페이지를 진행합니다.
5. 차단 목록에 있는 주소에 대한 세부 정보를 보려면 소스 IP 주소에 마우스를 갖다 대고 아래쪽 화살표 링크를 클릭합니다. **Who Is** 링크를 클릭하면 주소에 대한 Network Solutions Who Is 정보가 표시됩니다.




 ©2023 Palo Alto Networks, Inc.

- 차단 목록 항목을 삭제합니다.

  *IP* 주소를 차단해서는 안 된다고 판단되면 항목을 삭제합니다. 그런 다음 방화벽이 주소를 차단하는 정책 규칙을 수정합니다.

  1. 모니터 > 차단 **IP** 목록을 선택합니다.
  2. 항목을 하나 이상 선택하고삭제를 클릭합니다.
  3. (선택사항)목록에서 모든 항목을 제거하기 위해 모두 지우기를 선택합니다.

- 문제 해결을 위해 하드웨어 IP 주소 차단을 비활성화하거나 다시 활성화합니다.

  하드웨어 *IP* 주소 차단을 사용하지 않도록 설정하지만 방화벽은 구성한 소프트웨어 *IP* 주소를 차단하는 모든 소프트웨어 *IP* 주소를 여전히 수행합니다.

  ```
  > set system setting hardware-acl-blocking [enable | disable]
  ```

  *CPU* 및 패킷 버퍼 리소스를 절약하려면 *Palo Alto Networks*의 기술 지원이 트래픽 플로우를 디버깅하는 경우와 같은 비활성화를 요청하지 않는 한 하드웨어 *IP* 주소 차단을 사용하도록 설정합니다.

- 하드웨어에 의해 차단된 IP 주소가 차단 목록에 남아 있는 초 수를 조정합니다(범위는 1-3,600, 기본값은 1).

  ```
  > set system setting hardware-acl-blocking duration <seconds>
  ```

  하드웨어 차단 용량을 초과할 가능성을 줄이기 위해 소프트웨어 차단 목록 항목보다 하드웨어 차단 목록 항목에 대한 기간이 짧아집니다.

- 기본 웹사이트를 변경하여 네트워크 솔루션의 IP 주소에 대한 자세한 정보를 다른 웹사이트로 변경합니다.

  ```
  # set deviceconfig system ip-address-lookup-url <url>
  ```


©2023 Palo Alto Networks, Inc.

- 예를 들어 공격 속도를 보려면 하드웨어 및 소프트웨어에 의해 차단된 소스 IP 주소 수를 볼 수 있습니다.

  하드웨어 차단 테이블 및 차단 목록(하드웨어 및 소프트웨어에 의해 차단됨)에서 IP 주소 항목의 총 합계를 봅니다.

  ```
  > show counter global name flow_dos_blk_num_entries
  ```

  하드웨어에 의해 차단된 하드웨어 차단 테이블의 IP 주소 항목 수를 확인합니다.

  ```
  > show counter global name flow_dos_blk_hw_entries
  ```

  소프트웨어에 의해 차단된 차단 목록에서 IP 주소 항목 수를 확인합니다.

  ```
  > show counter global name flow_dos_blk_sw_entries
  ```

- PA-7000 시리즈 방화벽에서 슬롯당 차단 목록 정보를 봅니다.

  ```
  > show dos-block-table software filter slot <slot-number>
  ```

 ©2023 Palo Alto Networks, Inc.

# 위협 서명 카테고리

Palo Alto Networks 위협 시그니처에는 세 가지 유형이 있으며, 각 유형은 방화벽이 네트워크 트래픽을 검사할 때 서로 다른 유형의 위협을 탐지하도록 설계되었습니다.

- 바이러스 백신 서명 - 실행 파일 및 파일 형식에서 발견된 바이러스 및 멀웨어를 탐지합니다.
- 안티 스파이웨어 서명 - 감염된 클라이언트의 스파이웨어가 사용자의 동의 없이 데이터를 수집하거나 원격 공격자와 통신하는 C2(Command-and-Control) 활동을 탐지합니다.
- 취약점 시그니처 - 공격자가 악용하려고 시도할 수 있는 시스템 결함을 탐지합니다.

서명의 심각도는 감지된 이벤트의 위험을 나타내며 서명의 기본 동작(예: 차단 또는 경고)은 Palo Alto Networks는 일치하는 트래픽을 적용하도록 권장하는 방식입니다.

위협을 탐지할 때 수행할 조치를 방화벽에 알리려면 안티바이러스, 안티 스파이웨어 및 취약점 방지를 설정해야 하며, 기본 보안 프로파일을 사용하여 Palo Alto Networks 권장 사항에 따라 위협 차단을 쉽게 시작할 수 있습니다. 각 서명 유형, 카테고리 및 특정 서명에 대해 계속해서 수정하거나 새 프로파일을 생성하여 잠재적 위협을 보다 세부적으로 적용할 수 있습니다.

다음 표에는 가능한 모든 서명 카테고리(바이러스 백신, 스파이웨어 및 취약성)가 나열되어 있으며 각 카테고리의 서명을 제공하는 콘텐츠 업데이트(애플리케이션 및 위협, 바이러스 백신 또는 WildFire)가 포함되어 있습니다. Palo Alto Networks 위협 볼트에서 위협 서명에 대해 자세히 알아보기까지 이동할 수도 있습니다.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| 안티바이러스 시그니처 | | |
| apk | 바이러스 백신<br>WildFire | 악성 안드로이드 애플리케이션(APK) 파일. |
| MacOSX | 바이러스 백신<br>WildFire | 악성 MacOSX 파일, 포함:<br>• 애플 디스크 이미지(DMG) 파일.<br>• Mach 개체 파일(Mach-O)은 실행 파일, 라이브러리 및 개체 코드입니다.<br>• Apple 소프트웨어 설치 프로그램 패키지(PKG) |
| 플래시 | 바이러스 백신<br>WildFire 또는 WildFire 프라이빗 | 웹 페이지에 포함된 Adobe Flash 애플릿 및 Flash 콘텐츠 |
| jar | 바이러스 백신 | 자바 애플릿(JAR/클래스 파일 형식). |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| | Wildfire | |
| ms-office | 바이러스 백신<br>WildFire 또는 WildFire 프라이빗 | 문서(DOC, DOCX, RTF), 통합 문서(XLS, XLSX) 및 파워포인트 프레젠테이션(PPT, PPTX)을 포함한 마이크로소프트 오피스 파일. 여기에는 OOXML(Office Open XML) 2007+ 문서도 포함됩니다. |
| pdf | 바이러스 백신<br>WildFire 또는 WildFire 프라이빗 | 휴대용 문서 형식(PDF) 파일. |
| pe | 바이러스 백신<br>WildFire 또는 WildFire 프라이빗 | 이동식 실행 파일(PE) 파일은 Microsoft Windows 시스템에서 자동으로 실행될 수 있으며 권한이 있는 경우에만 허용되어야 합니다. 이러한 파일 유형에는 다음이 포함됩니다.<br>• 개체 코드.<br>• 글꼴(FONS).<br>• 시스템 파일(SYS)<br>• 드라이버 파일(DRV).<br>• CPL(윈도우 제어판 항목).<br>• DLL(동적 연결 라이브러리)<br>• OCX(OLE 사용자 지정 컨트롤용 라이브러리 또는 ActiveX 컨트롤용 라이브러리)<br>• 윈도우 스크린 세이버 파일 (SCR).<br>• EFI(확장 가능 펌웨어 인터페이스) 파일 - 디바이스 업데이트 및 부팅 작업을 용이하게 하기 위해 OS와 펌웨어 간에 실행됩니다.<br>• 프로그램 정보 파일(PIF). |
| 리눅스 | 바이러스 백신<br>Wildfire | 실행 파일 및 ELF(연결 가능한 형식) 파일. |
| 보관 | 바이러스 백신<br>Wildfire | Roshal 아카이브 (RAR) 및 7-Zip (7z) 아카이브 파일. |
| 스파이웨어 서명 | | |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| 애드웨어 | 애플리케이션 및 위협 | 잠재적으로 원치 않는 광고를 표시하는 프로그램을 감지합니다. 일부 애드웨어는 웹 페이지에서 가장 자주 검색되는 키워드를 강조 표시하고 하이퍼 링크하도록 브라우저를 수정합니다. 이러한 링크는 사용자를 광고 웹사이트로 리디렉션합니다. 애드웨어는 C2(Command-and-Control) 서버에서 업데이트를 검색하여 브라우저 또는 클라이언트 시스템에 이러한 업데이트를 설치할 수도 있습니다.<br>이 카테고리에서 새로 출시된 보호 기능은 드뭅니다. |
| autogen | 바이러스 백신 | 이러한 페이로드 기반 서명은 명령 및 제어(C2) 트래픽을 감지하고 자동으로 생성됩니다. 중요한 것은 자동 세대 시그니처가 C2 호스트를 알 수 없거나 빠르게 변경되는 경우에도 C2 트래픽을 감지할 수 있다는 것입니다. |
| 뒷문 | 애플리케이션 및 위협 | 공격자가 시스템에 대한 무단 원격 액세스를 얻을 수 있도록 하는 프로그램을 탐지합니다. |
| 봇넷 | 애플리케이션 및 위협 | 봇넷 활동을 나타냅니다. 봇넷은 공격자가 제어하는 멀웨어에 감염된 컴퓨터("봇") 의 네트워크입니다. 공격자는 중앙에서 봇넷의 모든 컴퓨터에 DoS 공격 실행과 같은 조율된 작업을 동시에 수행하도록 명령할 수 있습니다. |
| 브라우저 하이재킹 | 애플리케이션 및 위협 | 브라우저 설정을 수정하는 플러그인 또는 소프트웨어를 감지합니다. 브라우저 하이재커는 자동 검색을 인수하거나 사용자의 웹 활동을 추적하여이 정보를 C2 서버로 보낼 수 있습니다.<br>이 카테고리에서 새로 출시된 보호 기능은 드뭅니다. |
| 크립토마이너 | 애플리케이션 및 위협 | (크립토재킹 또는 마이너라고도 함) 사용자 모르게 크립토 통화를 마이닝하기 위해 컴퓨팅 리소스를 사용하도록 설계된 악성 프로그램에서 생성된 다운로드 시도 또는 네트워크 트래픽을 감지합니다. Cryptominer 바이너리는 시스템 아키텍처를 결정하고 시스템의 다른 마이너 프로세스를 죽이려고 시도하는 쉘 스크립트 다운로더에 의해 자주 제공됩니다. 일부 마이너는 악의적인 웹 페이지를 렌더링하는 웹 브라우저와 같은 다른 프로세스 내에서 실행됩니다. |
| 데이터 도난 | 애플리케이션 및 위협 | 알려진 C2 서버로 정보를 보내는 시스템을 감지합니다.<br>이 카테고리에서 새로 출시된 보호 기능은 드뭅니다. |
| dns | 바이러스 백신 | 악성 도메인에 연결하기 위한 DNS 요청을 탐지합니다. |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| | | dns 및 dns-wildfire 서명은 동일한 악성 도메인을 탐지합니다. 그러나 DNS 서명은 일일 바이러스 백신 콘텐츠 업데이트에 포함되며 dns-wildfire 서명은 5분마다 보호 기능을 해제하는 WildFire 업데이트에 포함됩니다. |
| dns-security | 바이러스 백신 | 악성 도메인에 연결하기 위한 DNS 요청을 탐지합니다.<br>dns-security에는 DNS 보안 서비스에서 생성된 고유한 서명 외에도 dns 및 dns-wildfire의 서명이 포함됩니다. |
| dns-wildfire | WildFire 또는 WildFire 프라이빗 | 악성 도메인에 연결하기 위한 DNS 요청을 탐지합니다.<br>dns 및 dns-wildfire 서명은 동일한 악성 도메인을 탐지합니다. 그러나 DNS 서명은 일일 바이러스 백신 콘텐츠 업데이트에 포함되며 dns-wildfire 서명은 5분마다 보호 기능을 해제하는 WildFire 업데이트에 포함됩니다. |
| 다운로더 | 애플리케이션 및 위협 | (드롭퍼, 스태거 또는 로더라고도 함) 인터넷 연결을 사용하여 원격 서버에 연결하여 손상된 시스템에서 멀웨어를 다운로드하고 실행하는 프로그램을 검색합니다. 가장 일반적인 사용 사례는 다운로더가 사이버 공격의 ***1***단계의 절정으로 배포되는 것입니다. 여기서 다운로더의 가져온 페이로드 실행은 ***2***단계로 간주됩니다. 쉘 스크립트(Bash, PowerShell 등), 트로이 목마 및 PDF 및 Word 파일과 같은 악성 루어 문서(maldocs라고도 함)는 일반적인 다운로더 유형입니다. |
| 사기 | 애플리케이션 및 위협 | (폼 재킹, 피싱 및 사기 포함) 악성 JavaScript 코드가 삽입된 것으로 확인된 손상된 웹사이트에 대한 액세스를 감지하여 중요한 사용자 정보를 수집합니다.전자 상거래 웹사이트의 결제 페이지에 캡처된 결제 양식의 이름, 주소, 이메일, 신용카드 번호, CVV, 만료 날짜 등. |
| 해킹툴 | 애플리케이션 및 위협 | 악의적인 행위자가 정찰, 공격 또는 취약한 시스템에 액세스하거나, 데이터를 유출하거나, 명령 및 제어 채널을 생성하여 승인 없이 컴퓨터 시스템을 몰래 제어하는 데 사용하는 소프트웨어 도구에 의해 생성된 트래픽을 탐지합니다. 이러한 프로그램은 멀웨어 및 사이버 공격과 밀접한 관련이 있습니다. 해킹 도구는 Red 및 Blue Team 운영, 침투 테스트 및 R&D에서 사용될 때 악성 방식으로 배포될 수 있습니다. 이러한 도구의 사용 또는 소지는 의도에 관계없이 일부 국가에서는 불법일 수 있습니다. |
| keylogger | 애플리케이션 및 위협 | 키 입력을 기록하고 스크린샷을 캡처하여 공격자가 사용자 활동을 비밀리에 추적할 수 있는 프로그램을 탐지합니다. |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| | | 키로거는 다양한 C2 방법을 사용하여 로그 및 보고서를 사전 정의된 전자 메일 주소 또는 C2 서버로 주기적으로 보냅니다. 키로거 감시를 통해 공격자는 네트워크 액세스를 가능하게 하는 자격 증명을 검색할 수 있습니다. |
| 넷웜(Net-worm) | 애플리케이션 및 위협 | 자체 복사 및 시스템 간에 확산되는 프로그램을 감지합니다. 넷웜(Net-worm)은 공유 리소스를 사용하거나 보안 오류를 활용하여 대상 시스템에 액세스할 수 있습니다. |
| 피싱 키트 | 애플리케이션 및 위협 | 사용자가 피싱 키트 랜딩 페이지에 연결을 시도하는 시점을 감지합니다(악성 사이트에 대한 링크가 포함된 이메일을 수신한 후일 수 있음). 피싱 웹사이트는 공격자가 네트워크에 액세스하기 위해 훔칠 수 있는 자격 증명을 제출하도록 사용자를 속입니다.<br><br>피싱 키트 방문 페이지에 대한 액세스를 차단하는 것 외에도 Multi-Factor Authentication 및 자격 증명 피싱 방지를 활성화하여 모든 단계에서 피싱 공격을 방지합니다. |
| 사후 악용(post-exploitation) | 애플리케이션 및 위협 | 공격자가 손상된 시스템의 가치를 평가하려고 시도하는 공격의 사후 악용 단계를 나타내는 활동을 탐지합니다. 여기에는 시스템에 저장된 데이터의 민감도 평가와 네트워크 손상에 대한 시스템의 유용성을 평가하는 것이 포함될 수 있습니다. |
| 웹쉘 | 애플리케이션 및 위협 | 임플란트 감지, 명령 및 제어 상호 작용을 포함하여 웹 셸 및 웹 쉘 트래픽을 감지합니다. 웹 셸은 먼저 악의적인 행위자에 의해 손상된 호스트에 이식되어야 하며, 대부분 웹 서버 또는 프레임워크를 대상으로 합니다. 이후 웹 셸 파일과의 통신은 악의적 인 행위자가 시스템에 발판을 마련하고 웹 서버 사용자의 컨텍스트에서 서비스 및 네트워크 열거, 데이터 유출 및 원격 코드 실행을 수행하는 경우가 많습니다. 가장 일반적인 웹 셸 유형은 PHP, .NET 및 Perl 마크업 스크립트입니다. 공격자는 웹 셸에 감염된 웹 서버(웹 서버는 인터넷에 연결되거나 내부 시스템일 수 있음)를 사용하여 다른 내부 시스템을 대상으로 할 수도 있습니다. |
| 스파이웨어 | 애플리케이션 및 위협 | 아웃바운드 C2 통신을 감지합니다. 이러한 서명은 자동으로 생성되거나 Palo Alto Networks 연구원이 수동으로 생성합니다. |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| | | 스파이웨어와 자동 서명 모두 아웃바운드 *C2* 통신을 감지합니다. 그러나 자동 생산 서명은 페이로드 기반이며 알 수 없거나 빠르게 변경되는 *C2* 호스트와의 *C2* 통신을 고유하게 감지할 수 있습니다. |
| 취약성 시그니처 | | |
| 무차별 대입 | 애플리케이션 및 위협 | 무차별 대입 시그니처는 특정 시간대의 여러 조건 발생을 감지합니다. 고립된 활동은 악성일 수 있지만 무차별 대입 서명은 활동이 발생한 빈도와 비율이 의심스럽다는 것을 나타냅니다. 예를 들어, 단일 FTP 로그인 실패가 악의적인 활동을 나타내는 것은 아닙니다. 그러나 단기간에 실패한 많은 FTP 로그인은 공격자가 FTP 서버에 액세스하기 위해 암호 조합을 시도했음을 나타냅니다.<br>무차별 대입 서명에 대한 동작 및 트리거 조건을 조정할 수 있습니다. |
| 코드 실행 | 애플리케이션 및 위협 | 공격자가 로그인한 사용자의 권한으로 시스템에서 코드를 실행하는 데 활용할 수 있는 코드 실행 취약성을 탐지합니다. |
| code-obfuscation | 애플리케이션 및 위협 | 기능을 유지하면서 특정 데이터를 숨기도록 변환된 코드를 감지합니다. 난독화된 코드는 읽기가 어렵거나 불가능하므로 코드가 어떤 명령을 실행하는지 또는 어떤 프로그램과 상호작용하도록 설계되었는지는 분명하지 않습니다. 대부분의 경우 악의적인 행위자는 코드를 난독화하여 멀웨어를 숨깁니다. 적법한 개발자가 개인 정보 보호, 지적 재산을 보호하거나 사용자 환경을 개선하기 위해 코드를 난독화할 수 있는 경우는 드뭅니다. 예를 들어 특정 유형의 난독화(예: 축소)는 파일 크기를 줄여 웹사이트 로드 시간과 대역폭 사용량을 줄입니다. |
| dos | 애플리케이션 및 위협 | 공격자가 표적 시스템을 사용할 수 없도록 설정하여 시스템 및 종속 애플리케이션 및 서비스를 일시적으로 중단시키는 DoS(서비스 거부) 공격을 탐지합니다. DoS 공격을 수행하기 위해 공격자는 대상 시스템에 트래픽을 넘치거나 실패를 유발하는 정보를 보낼 수 있습니다. DoS 공격은 합법적인 사용자(예: 직원, 회원, 계정 소유자)가 액세스를 기대하는 서비스 또는 리소스를 박탈합니다. |
| exploit-kit | 애플리케이션 및 위협 | 익스플로잇 키트 소개 페이지를 감지합니다. 익스플로잇 키트 랜딩 페이지에는 여러 브라우저 및 플러그인에 대해 하나 |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
|---|---|---|
| | | 이상의 공통 취약점 및 노출(CVE)을 대상으로 하는 여러 익스플로잇이 포함되어 있는 경우가 많습니다. 대상 CVE는 빠르게 변경되므로 익스플로잇 키트 서명은 CVE가 아닌 익스플로잇 키트 랜딩 페이지를 기반으로 트리거됩니다.<br><br>사용자가 익스플로잇 키트가 있는 웹사이트를 방문하면 익스플로잇 키트는 대상 CVE를 검색하고 악의적인 페이로드를 피해자의 컴퓨터에 자동으로 전송하려고 시도합니다. |
| 정보 누출 | 애플리케이션 및 위협 | 공격자가 민감한 정보 또는 독점 정보를 훔치기 위해 악용할 수 있는 소프트웨어 취약점을 탐지합니다. 데이터를 보호하기 위한 포괄적인 검사가 없고 공격자가 조작된 요청을 전송하여 정보 유출을 악용할 수 있기 때문에 정보 유출이 발생할 수 있습니다. |
| insecure-credentials | 애플리케이션 및 위협 | 소프트웨어, 네트워크 어플라이언스 및 IoT 디바이스에 대해 취약하고 손상된 제조업체 기본 암호의 사용을 감지합니다. |
| 오버플로우 | 애플리케이션 및 위협 | 요청에 대한 적절한 검사가 부족하여 공격자가 악용할 수 있는 오버플로우 취약점을 탐지합니다. 공격이 성공하면 애플리케이션, 서버 또는 운영 체제의 권한으로 원격 코드가 실행될 수 있습니다. |
| 피싱 | 애플리케이션 및 위협 | 사용자가 피싱 키트 랜딩 페이지에 연결을 시도하는 시점을 감지합니다(악성 사이트에 대한 링크가 포함된 이메일을 수신한 후일 수 있음). 피싱 웹사이트는 공격자가 네트워크에 액세스하기 위해 훔칠 수 있는 자격 증명을 제출하도록 사용자를 속입니다.<br><br>피싱 키트 방문 페이지에 대한 액세스를 차단하는 것 외에도 Multi-Factor Authentication 및 자격 증명 피싱 방지를 활성화하여 모든 단계에서 피싱 공격을 방지합니다. |
| 프로토콜 변칙 | 애플리케이션 및 위협 | 프로토콜 동작이 표준 및 규정 준수 사용에서 벗어나는 프로토콜 변칙을 감지합니다. 예를 들어 형식이 잘못된 패킷, 잘못 작성된 애플리케이션 또는 비표준 포트에서 실행되는 애플리케이션은 모두 프로토콜 예외로 간주되어 회피 도구로 사용될 수 있습니다. 모든 심각도의 프로토콜 변칙을 차단하는 것이 가장 좋습니다. |
| sql-injection | 애플리케이션 및 위협 | 공격자가 데이터베이스를 읽거나 수정하기 위해 SQL 쿼리를 애플리케이션의 요청에 삽입하는 일반적인 해킹 기술을 탐 |


©2023 Palo Alto Networks, Inc.

| 위협 카테고리 | 이러한 서명을 제공하는 콘텐츠 업데이트 | 설명 |
| --- | --- | --- |
| | | 지합니다. 이러한 유형의 기술은 사용자 입력을 종합적으로 살균하지 않는 웹사이트에서 자주 사용됩니다. |


©2023 Palo Alto Networks, Inc.

# 위협 예외 생성

Palo Alto Networks는 보안 서명에 대해 권장되는 기본 작업(예: 차단 또는 경고)을 정의합니다. 위협 ID를 사용하여 보안 서명을 적용에서 제외하거나 방화벽이 해당 보안 서명에 대해 적용하는 작업을 수정할 수 있습니다. 예를 들어 네트워크에서 가양성을 트리거하는 보안 서명에 대한 작업을 수정할 수 있습니다.

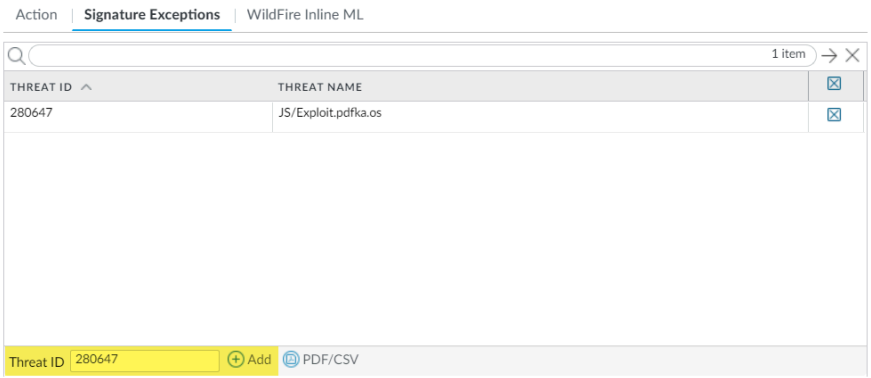
안티바이러스, 취약성, 스파이웨어 및 DNS 서명에 대한 위협 예외를 구성하여 위협에 대한 방화벽 적용을 변경합니다. 그러나 시작하기 전에 방화벽이 기본 서명 설정을 기반으로 위협을 탐지하고 시행하는지 확인하십시오.

- 최신 안티바이러스, 위협 및 애플리케이션, WildFire 서명 업데이트를 받으십시오.
- 안티바이러스, 안티스파이웨어 및 취약성 보호를 설정하고 이러한 보안 프로파일을 보안 정책에 적용합니다.

**STEP 1 |** 시행에서 바이러스 백신 서명을 제외합니다.

바이러스 백신 프로파일을 사용하여 바이러스 백신 서명을 시행에서 제외할 수 있지만 방화벽이 특정 바이러스 백신 서명에 대해 시행하는 작업은 변경할 수 없습니다. 그러나 디코더를 편집하여 다른 유형의 트래픽에서 발견된 바이러스에 대해 방화벽이 적용할 작업을 정의할 수 있습니다(개체 > 보안 프로파일 > 안티바이러스 > ***<antivirus-profile>*** > 안티바이러스).

1. 개체 > 보안 프로파일 > 바이러스 백신을 선택합니다.
2. 보안 서명을 제외할 기존 안티바이러스 프로파일을 추가하거나 수정하고 서명 예외를 선택합니다.
3. 시행에서 제외할 보안 서명에 대한 위협 **ID**를 추가합니다.

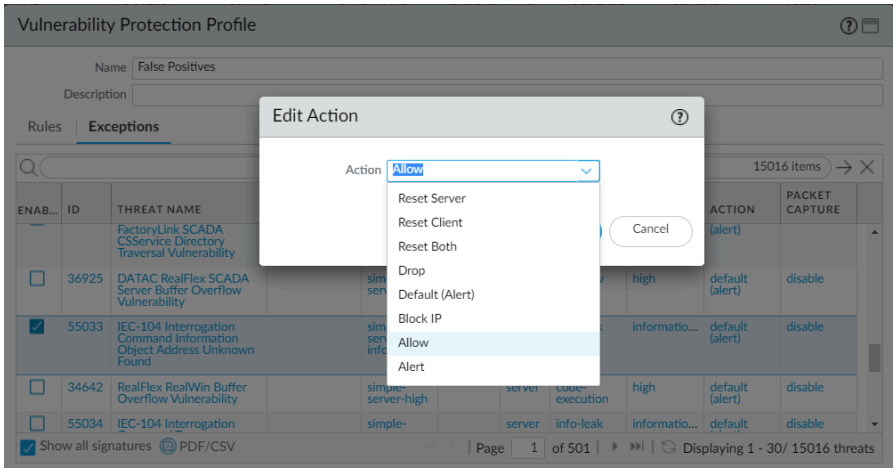



4. 확인을 클릭하여 바이러스 백신 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 취약성 및 스파이웨어 서명에 대한 시행 수정(DNS 서명 제외, 스파이웨어 서명 유형인 DNS 서명에 대한 시행을 수정하려면 다음 옵션으로 건너뛰십시오.)

1. 개체 > 보안 프로파일 > 안티스파이웨어 또는 개체 > 보안 프로파일 > 취약점 보호를 선택합니다.
2. 보안 서명을 제외할 기존 안티 스파이웨어 또는 취약점 보호 프로파일을 추가하거나 수정한 다음 안티 스파이웨어 프로파일에 대한 서명 예외 또는 취약점 보호 프로파일에 대한 예외를 선택합니다.
3. 모든 서명을 표시한 다음 필터링하여 적용 규칙을 수정할 서명을 선택합니다.
4. 적용을 수정하려는 서명의 사용 열 아래에 있는 체크박스를 선택합니다.
5. 방화벽이 이 보안 서명에 적용할 작업을 선택합니다.



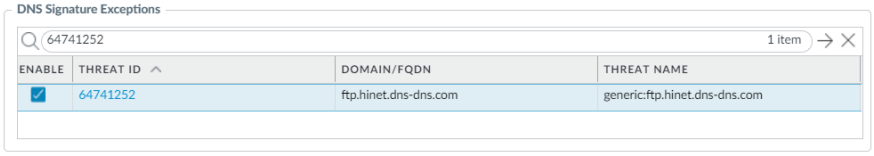

가양성을 트리거하기 때문에 시행에서 제외하려는 서명의 경우 작업을 허용으로 설정합니다.

6. 확인을 클릭하여 새롭거나 수정된 안티스파이웨어 또는 취약점 보호 프로파일을 저장합니다.

**STEP 3 |** DNS 서명에 대한 시행을 수정합니다.

기본적으로 DNS 서명이 감지하는 악성 호스트 이름에 대한 DNS 조회는 싱크홀입니다.

1. 개체 > 보안 프로파일 > 안티 스파이웨어를 선택합니다.
2. 보안 서명을 제외할 안티 스파이웨어 프로파일을 추가하거나 수정하고 **DNS** 예외를 선택합니다.
3. 시행에서 제외할 DNS 서명의 DNS 위협 ID를 검색하고 해당 서명 상자를 선택합니다.




4. 확인을 클릭하여 새 또는 수정된 안티 스파이웨어 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

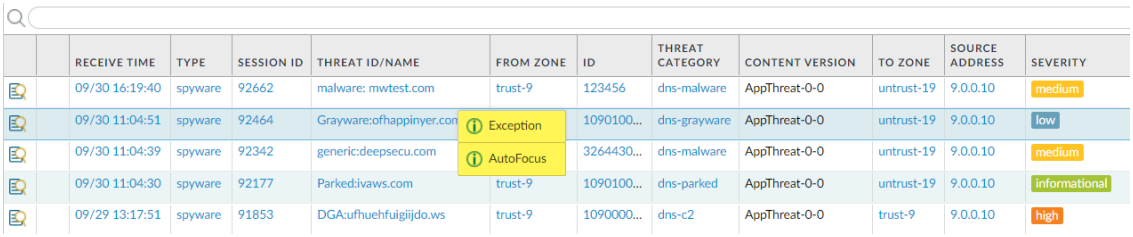
# 사용자 정의 서명

특정 트래픽을 감지하고 차단하기 위해 사용자 지정 보안 서명을 만들 수 있습니다. Panorama 관리 서버에서 방화벽을 관리하면 ThreatID가 방화벽의 해당 사용자 지정 위협에 매핑되어 방화벽이 구성된 사용자 지정 ThreatID로 채워진 위협 로그를 생성할 수 있습니다. 사용자 지정 애플리케이션 및 보안 서명에 대한 가이드를 방문하여 자세히 알아보십시오.


©2023 Palo Alto Networks, Inc.

# 위협 보고서 모니터링 및 Get

Threat Vault 및 AutoFocus의 기능은 방화벽이 감지하는 위협의 특성에 대한 가시성을 제공하고 아티팩트가 조직의 네트워크 트래픽에 어떻게 맞는지 보다 완벽하게 파악할 수 있도록 방화벽에 통합되어 있습니다(아티팩트는 파일, 이메일 링크 또는 세션과 관련된 속성, 활동 또는 동작입니다). 위협에 대한 즉각적인 컨텍스트 정보를 얻거나 방화벽에서 위협 조사를 Threat Vault 및 AutoFocus로 원활하게 전환할 수 있습니다.




또한 위협 이벤트 유형을 분류하는 위협 서명 카테고리을(를) 사용하여 특정 유형의 위협 활동으로 보기 범위를 좁히거나 맞춤 보고서를 작성할 수 있습니다.

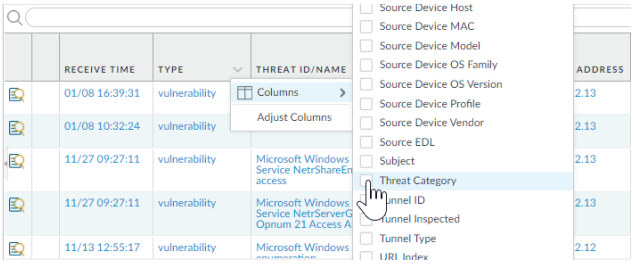
- 위협 카테고리를 기반으로 활동 모니터링 및 맞춤 리포트 생성
- 위협 서명에 대해 자세히 알아보기
- 네트워크 트래픽에 대한 AutoFocus 위협 인텔리전스

## 위협 카테고리를 기반으로 활동 모니터링 및 맞춤 리포트 생성

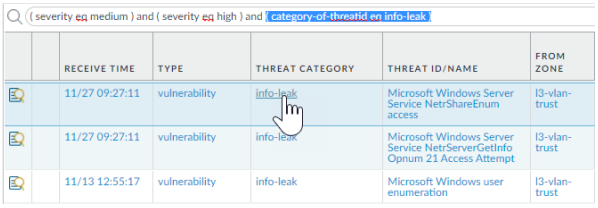
위협 카테고리는 여러 유형의 위협 서명을 분류하여 위협 시그니처가 탐지하는 이벤트를 이해하고 연결을 유도하는 데 도움이 됩니다. 위협 카테고리는 스파이웨어, 취약성, 바이러스 백신 및 DNS 서명과 같은 광범위한 위협 시그니처 유형의 하위 집합입니다. 위협 로그 항목에는 기록된 각 이벤트에 대한 위협 카테고리가 표시됩니다.


©2023 Palo Alto Networks, Inc.

- 위협 카테고리별로 위협 로그를 필터링합니다.
  1. 모니터 > 로그 > 위협을 선택합니다.
  2. 위협 카테고리 열을 추가하여 각 로그 항목에 대한 위협 카테고리를 볼 수 있습니다.

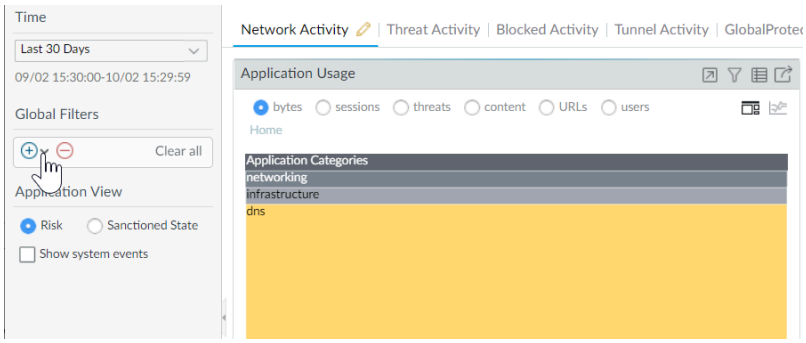



  3. 위협 카테고리를 기준으로 필터링하려면 다음을 수행합니다.
     - 로그 쿼리 빌더를 사용하여 특성 위협 카테고리가 있는 필터를 추가하고 값 필드에 위협 카테고리를 입력합니다.
     - 로그 항목의 위협 카테고리를 선택하여 해당 카테고리를 필터에 추가합니다.

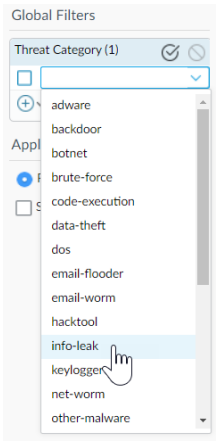



 ©2023 Palo Alto Networks, Inc.

- 위협 카테고리별로 ACC 활동을 필터링합니다.
  1. **ACC**를 선택한 다음 위협 카테고리를 전역 필터로 추가합니다.




  2. 위협 카테고리를 선택하여 모든 ACC 탭을 필터링합니다.




- 위협 카테고리를 기반으로 맞춤 리포트를 만들어 방화벽에서 탐지한 특정 유형의 위협에 대한 정보를 수신합니다.
  1. 모니터 > 사용자 정의 보고서 관리를 선택하여 새 사용자 정의 보고서를 추가하거나 기존 보고서를 수정합니다.
  2. 맞춤 리포트의 원본으로 사용할 데이터베이스를 선택합니다. 이 경우 두 가지 유형의 데이터베이스 소스(요약 데이터베이스 및 세부 로그)에서 위협을 선택합니다. 요약 데이터베이스 데이터는 보고서를 생성할 때 응답 시간을 단축할 수 있도록 압축됩니다. 자세한 로그는 생성하는 데 시간이 오래 걸리지만 각 로그 항목에 대해 항목별 및 전체 데이터 세트를 제공합니다.
  3. 쿼리 빌더에서 속성 위협 카테고리가 있는 보고서 필터를 추가하고 값 필드에서 보고서의 기반으로 사용할 위협 카테고리를 선택합니다.
  4. 새 보고서 설정을 테스트하려면지금 실행을 클릭합니다.
  5. 확인을 클릭하여 보고서를 저장합니다.

## 위협 서명에 대해 자세히 알아보기

방화벽 위협 로그는 위협 시그니처(안티바이러스, 안티스파이웨어 및 취약점 보호 설정)를 기반으로 방화벽이 탐지하는 모든 위협을 기록하며 ACC는 네트워크의 주요 위협에 대한 개요를 표시합니다. 방화벽이 기록하는 각 이벤트에는 연관된 위협 서명을 식별하는 ID가 포함됩니다.

위협 로그 또는 ACC 항목과 함께 발견된 위협 ID를 사용하여 다음을 수행할 수 있습니다.


©2023 Palo Alto Networks, Inc.

- 위협 서명이 보안 정책의 예외로 구성되어 있는지 쉽게 확인할 수 있습니다(위협 예외 생성).
- 특정 위협에 대한 최신 Threat Vault 정보를 찾아보십시오. Threat Vault는 방화벽과 통합되어 있으므로 방화벽 컨텍스트에서 직접 위협 세부 정보를 보거나 방화벽에 기록된 위협에 대해 새 브라우저 창에서 Threat Vault 검색을 시작할 수 있습니다.

서명이 비활성화된 경우 서명 ***UTID***가 새 서명에 재사용될 수 있습니다.

콘텐츠 업데이트 릴리스 노트를 검토하여 새 서명과 비활성화된 서명에 대한 알림을 확인합니다. 서명이 탐지한 활동이 공격자에 의해 사용되지 않거나, 서명이 중대한 오탐지를 생성했거나, 서명이 다른 유사한 서명과 단일 서명으로 통합(서명 최적화)된 경우 서명이 비활성화될 수 있습니다.

**STEP 1 |** 방화벽이 위협 요소 볼트에 연결되어 있는지 확인합니다.

디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 **Threat Vault** 액세스 사용으로 편집합니다. 위협 저장소 액세스는 기본적으로 사용하도록 설정되어 있습니다.

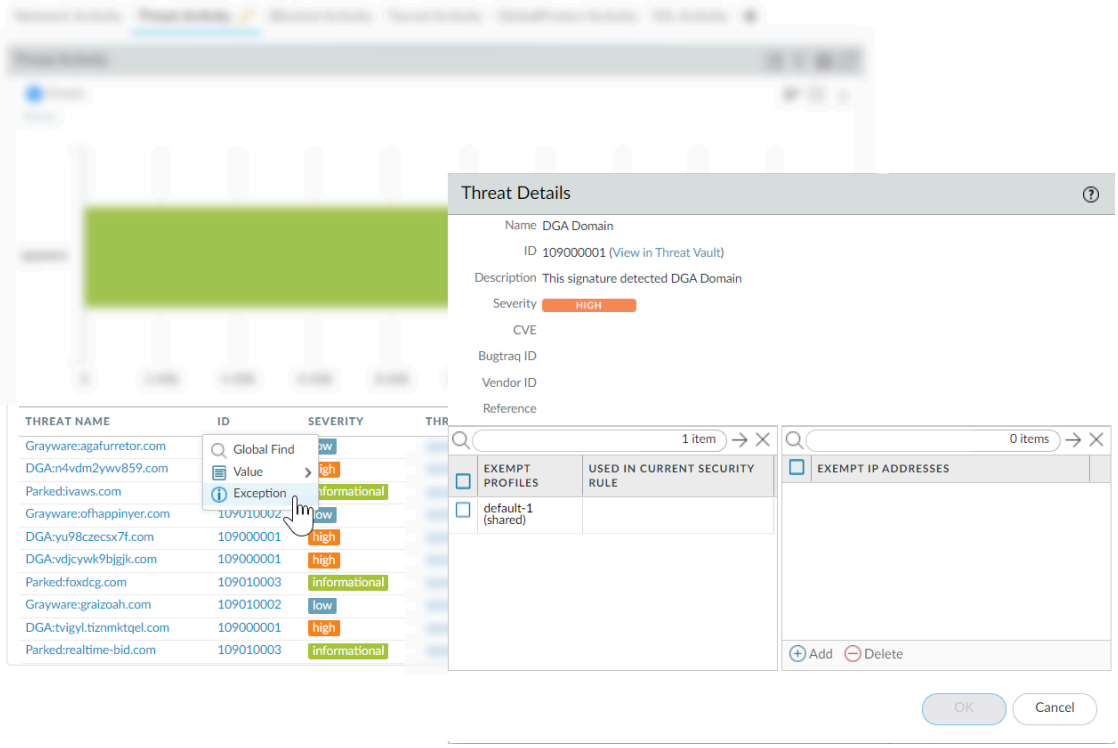
**STEP 2 |** 방화벽이 탐지하는 위협에 대한 위협 ID를 찾습니다.

- 위협 시그니처를 기반으로 방화벽이 탐지하는 각 위협 이벤트를 보려면 로그 > 위협 > 모니터링을 선택합니다. ID 열에 나열된 위협 항목의 ID를 찾거나 로그 항목을 선택하여 위협 ID를 비롯한 로그 세부 정보를 볼 수 있습니다.
- 네트워크의 최상위 위협에 대한 개요를 보려면 **ACC** > 위협 활동을 선택한 다음 위협 활동 위젯을 살펴보십시오. ID 열에는 표시된 각 위협에 대한 위협 ID가 표시됩니다.
- 위협 예외로 구성할 수 있는 위협에 대한 세부정보를 보려면(즉, 방화벽이 위협 서명에 대해 정의된 기본 작업과 다르게 위협을 적용함), 개체 > 보안 프로파일 > 스파이웨어 방지/취약점 보호를 선택합니다.. 프로파일을 추가하거나 수정하고 예외 탭을 클릭하여 구성된 예외를 봅니다. 예외가 구성되지 않은 경우 위협 서명을 필터링하거나 모든 서명 표시를 선택할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 위협 이름 또는 위협 **ID** 위로 마우스를 가져가 드롭다운을 열고 예외를 클릭하여 위협 세부 정보와 방화벽이 위협을 적용하도록 구성된 방법을 모두 검토합니다.

예를 들어, ACC에서 차트로 된 주요 위협에 대해 자세히 알아보십시오.




**STEP 4 |** 위협에 대한 최신 위협 세부 정보를 검토하고 위협 ID를 기반으로 Threat Vault 검색을 시작합니다.

- 표시되는 위협 세부 정보에는 위협에 대한 최신 Threat Vault 정보, 위협에 대해 자세히 알아보는 데 사용할 수 있는 리소스 및 위협과 관련된 CVE가 포함됩니다.
- 새 창에서 Threat Vault 검색을 열고 이 위협 시그니처에 대한 Palo Alto Networks 위협 데이터베이스의 최신 정보를 조회하려면 **Threat Vault**에서 보기를 선택합니다.

**STEP 5 |** 위협 서명이 보안 정책의 예외로 구성되어 있는지 확인합니다.

- 현재 보안 규칙에 사용 열이 명확하지 않은 경우 방화벽은 권장되는 기본 서명 작업(예: 차단 또는 경고)을 기반으로 위협을 적용합니다.
- 현재 보안 규칙에 사용 열의 아무 곳에서나 확인 표시는 보안 정책 규칙이 연결된 예외 프로파일 설정에 따라 위협에 대해 기본이 아닌 동작(예: 허용)을 적용하도록 구성되어 있음을 나타냅니다.

보안 정책 규칙이 위협 예외를 사용하여 구성된 경우에만 보안 정책 규칙이 사용되는지의 여부에는 보안 규칙에 사용됨 열이 표시되지 않습니다. 정책 > 보안을 선택하여 지정된 보안 정책 규칙이 사용으로 설정되어 있는지 확인합니다.

**STEP 6 |** 위협 예외를 필터링하거나 기존 예외 **IP** 주소를 볼 IP 주소를 추가합니다.

연결된 세션에 일치하는 소스 또는 대상 IP 주소가 있는 경우에만 위협 예외를 적용하도록 예외 IP 주소를 구성합니다. 다른 모든 세션에 대해 위협은 기본 서명 작업을 기반으로 시행됩니다.


©2023 Palo Alto Networks, Inc.

# 네트워크 트래픽에 대한 AutoFocus 위협 인텔리전스

유효한 AutoFocus 구독으로 네트워크 활동을 AutoFocus 포털에서 사용 가능한 최신 위협 데이터와 비교할 수 있습니다. 방화벽과 AutoFocus를 연결하면 다음 기능이 잠금 해제됩니다.

- 방화벽 로그에 기록된 세션 아티팩트에 대한 AutoFocus 인텔리전스 요약을 봅니다.
- 방화벽에서 로그 아티팩트에 대한 AutoFocus 검색을 엽니다.

AutoFocus 인텔리전스 요약은 네트워크 및 전 세계적으로 아티팩트가 널리 퍼져 있음을 보여줍니다. 아티팩트에 대해 나열된 WildFire 판정 및 AutoFocus 태그는 아티팩트가 보안 위험을 제기하는지의 여부를 나타냅니다.

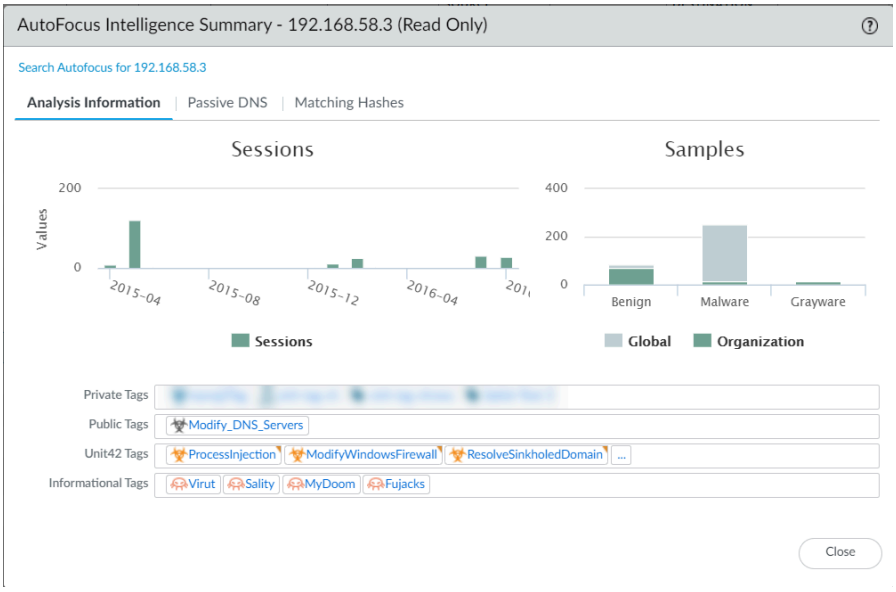
- AutoFocus 인텔리전스 요약
- AutoFocus 위협 인텔리전스 활성화
- AutoFocus 인텔리전스 요약 데이터 보기 및 조치

***AutoFocus* 결과:**

- AutoFocus 아티팩트(IP 주소, URL 및 도메인) 내보내기를 기반으로 정책을 적용하고 외부 동적 목록에서 사용할 수도 있습니다.
- AutoFocus 추출기를 외부 동적 목록 소스로 사용합니다.

## AutoFocus 인텔리전스 요약

AutoFocus 인텔리전스 요약은 다른 AutoFocus 사용자, WildFire, PAN-DB URL 필터링 데이터베이스, Unit 42 및 오픈 소스 인텔리전스에서 수집한 위협 인텔리전스에서 AutoFocus가 추출한 아티팩트에 대한 정보를 중앙 집중식으로 볼 수 있습니다.




| AutoFocus 인텔리전스 요약 | |
|---|---|
| 분석 정보 | 분석 정보 탭에는 다음 정보가 표시됩니다. |


©2023 Palo Alto Networks, Inc.

| **AutoFocus** 인텔리전스 요약 | |
|---|---|
| | • 세션 - 방화벽에서 아티팩트와 연결된 샘플을 감지한 방화벽에 기록된 세션 수입니다.<br>• 샘플 - 개체와 연관되고 WildFire 판결(양성, 맬웨어 또는 그레이웨어)별로 그룹화된 조직 및 글로벌 샘플을 비교합니다. 글로벌은 모든 WildFire 제출물의 샘플을 참조하는 반면, 조직은 조직에서 WildFire에 제출한 샘플만 참조합니다.<br>• 일치하는 태그 - 아티팩트와 일치하는 자동 초점 태그입니다. AutoFocus 태그는 아티팩트가 맬웨어 또는 표적 공격에 연결되어 있는지의 여부를 나타냅니다. |
| 패시브 DNS | 패시브 DNS 탭에는 아티팩트가 포함된 패시브 DNS 기록이 표시됩니다. 이 패시브 DNS 기록은 AutoFocus의 글로벌 DNS 인텔리전스를 기반으로 하며, 네트워크의 DNS 활동에만 국한되지 않습니다. 패시브 DNS 기록은 다음과 같이 구성됩니다.<br>• 도메인 요청<br>• DNS 요청 유형<br>• DNS 요청이 해결된 IP 주소 또는 도메인(프라이빗 IP 주소는 표시되지 않음)<br>• 요청이 이루어진 횟수입니다.<br>• 요청을 최초 및 최종적으로 본 날짜 및 시간 |
| 일치하는 해시 | 일치하는 해시 탭에는 가장 최근에 감지된 5개의 일치하는 샘플이 표시됩니다. 샘플 정보에는 다음이 포함됩니다.<br>• 샘플의 SHA256 해시<br>• 샘플 파일 형식<br>• WildFire가 샘플을 분석하고 샘플에 WildFire 판정을 할당한 날짜 및 시간<br>• 샘플에 대한 WildFire 판정<br>• WildFire가 샘플에 대한 WildFire 판정을 업데이트한 날짜 및 시간(해당하는 경우) |

## **AutoFocus** 위협 인텔리전스 활성화

AutoFocus 라이선스를 활성화하고 방화벽이 AutoFocus와 통신하도록 합니다. 설정이 완료되면 로그 또는 ACC 아티팩트에 대한 AutoFocus 인텔리전스 요약을(를) 확인하고 네트워크 및 관련 위협에 대한 침투성을 평가할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** AutoFocus 라이선스가 방화벽에서 활성화되어 있는지 확인하십시오.

1. AutoFocus Device License가 설치되어 있고 유효한지 확인하려면 디바이스 > 라이선스를 선택하십시오(만료일 확인).
2. 방화벽에 라이선스가 표시되지 않으면 구독 라이선스 활성화을(를) 합니다.

**STEP 2 |** 방화벽을 AutoFocus에 연결합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 AutoFocus 설정을 편집합니다.
2. **AutoFocus URL** 입력:

   **`https://autofocus.paloaltonetworks.com:10443`**
3. **Query Timeout** 필드를 사용하여 방화벽이 위협 인텔리전스 데이터에 대해 AutoFocus에 쿼리를 시도하는 시간을 설정합니다. AutoFocus 포털이 지정된 기간이 끝나기 전에 응답하지 않으면 방화벽이 연결을 닫습니다.

   가장 좋은 방법은 쿼리 제한 시간을 기본값인 ***15***초로 설정하는 것입니다. ***AutoFocus*** 쿼리는 이 기간 내에 완료되도록 최적화됩니다.
4. 방화벽이 AutoFocus에 연결할 수 있도록 하려면 사용을 선택합니다.
5. 확인을 클릭합니다.
6. 재부팅 시 AutoFocus 설정을 유지하려면 변경 사항을 커밋합니다.

**STEP 3 |** AutoFocus를 방화벽에 연결합니다.

1. AutoFocus 포털에 로그인: https://autofocus.paloaltonetworks.com
2. 설정을 선택합니다.
3. 새 원격 시스템을 추가합니다.
4. 방화벽을 식별하는 설명이 포함된 이름을 입력합니다.
5. 시스템 유형으로 **PanOS**를 선택합니다.
6. 방화벽 IP 주소를 입력합니다.
7. 변경 사항 저장을 클릭하여 원격 시스템을 추가합니다.
8. 설정 페이지에서 변경 사항 저장을 다시 클릭하여 방화벽이 성공적으로 추가되었는지 확인합니다.

**STEP 4 |** 방화벽과 AutoFocus 간의 연결을 테스트합니다.

1. 방화벽에서 모니터 > 로그 > 트래픽을 선택합니다.
2. AutoFocus로 방화벽 아티팩트를 평가할 수 있는지 확인하십시오.

## AutoFocus Intelligence 요약 데이터 보기 및 조치

AutoFocus Intelligence Summary와 상호 작용하여 아티팩트(artifact)에 대한 추가 정보를 표시하거나 아티팩트(artifact) 연구를 AutoFocus로 확장하십시오. AutoFocus 태그는 아티팩트가 특정 유형의 멀웨어 또는 악의적인 동작과 관련되어 있는지의 여부를 나타냅니다.

**STEP 1 |** 방화벽이 AutoFocus에 연결되어 있는지 확인합니다.

방화벽에서 AutoFocus 위협 인텔리전스를 활성화합니다(활성 AutoFocus 구독 필요).

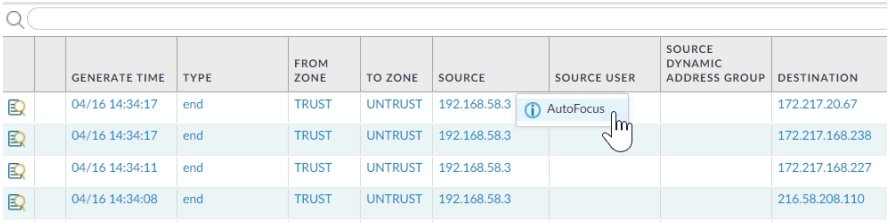
 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 검토할 아티팩트(artifact)를 찾으십시오.

다음과 같은 경우 아티팩트에 대한 AutoFocus 인텔리전스 요약을 볼 수 있습니다.

- 로그 보기(트래픽, 위협, URL 필터링, WildFire 제출, 데이터 필터링 및 통합 로그만 해당).
- 외부 동적 목록 항목을 봅니다.

**STEP 3 |** 아티팩트 위로 마우스를 가져가서 드롭다운을 열고 **AutoFocus**를 클릭합니다.




AutoFocus Intelligence Summary는 다음 유형의 아티팩트에만 사용할 수 있습니다.

IP 주소

URL

도메인

사용자 에이전트

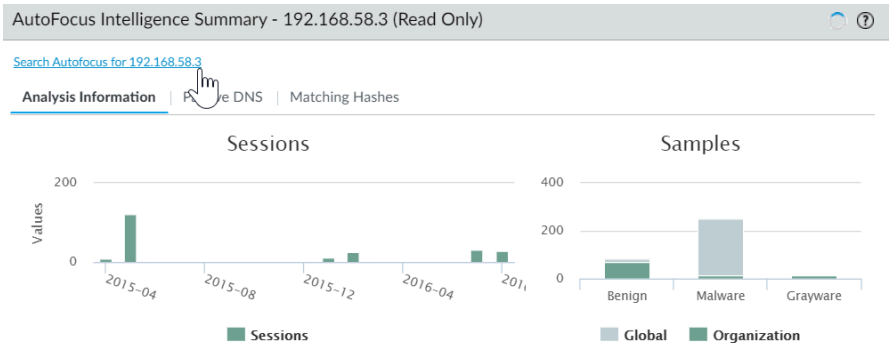
위협 이름(아형 바이러스 및 Wildfire 바이러스의 위협에만 해당)

파일 이름

SHA-256 해시

**STEP 4 |** AutoFocus Intelligence Summary를 연 아티팩트에 대해 AutoFocus 검색을 시작합니다.

AutoFocus Intelligence Summary 창 상단에 있는 **Search AutoFocus for...** 링크를 클릭하십시오. 검색 결과에는 아티팩트와 관련된 모든 샘플이 포함됩니다. 내 샘플과 모든 샘플 탭 간에 전환하고 샘플 수를 비교하여 조직에서 아티팩트의 보급 정도를 확인합니다.




 ©2023 Palo Alto Networks, Inc.

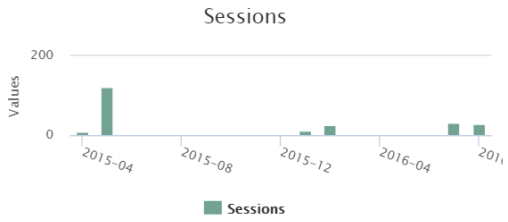
**STEP 5 |** AutoFocus Intelligence Summary에서 다른 아티팩트에 대한 AutoFocus 검색을 시작합니다.

다음 아티팩트를 클릭하여 조직에서의 보급성을 확인하십시오.

- 분석 정보 탭의 WildFire 판정
- 수동 DNS 탭의 URL 및 IP 주소
- 일치하는 해시 탭의 SHA256 해시

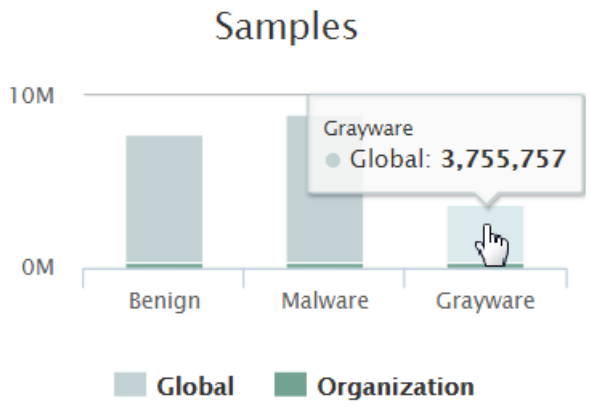
**STEP 6 |** 매월 조직의 아티팩트와 연결된 세션 수를 봅니다.

세션 표시줄 위로 마우스를 가져갑니다.




**STEP 7 |** 범위 및 WildFire 판정에 따라 아티팩트와 연결된 샘플 수를 봅니다.

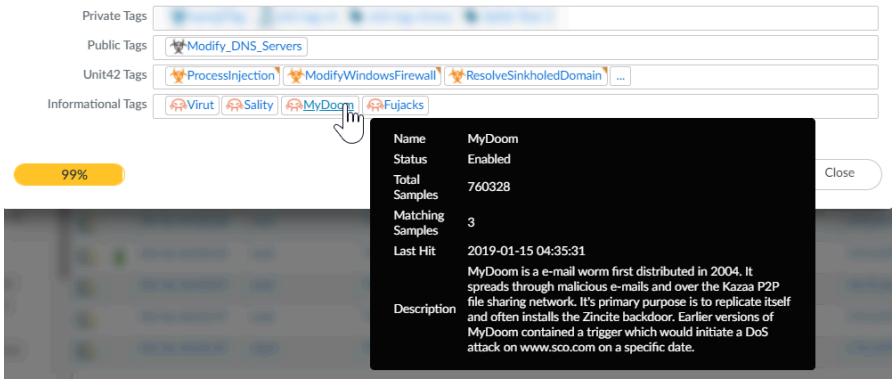
샘플 막대 위로 마우스를 가져갑니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** AutoFocus 일치에 대한 자세한 내용을 확인하십시오. 태그.

태그 설명 및 기타 태그 세부 정보를 보려면 일치하는 태그 위로 마우스를 가져갑니다.




**STEP 9 |** 일치하는 태그와 연결된 다른 샘플을 봅니다.

일치하는 태그를 클릭하면 해당 태그에 대한 AutoFocus 검색이 시작됩니다. 검색 결과에는 태그와 일치하는 모든 샘플이 포함됩니다.

Unit 42 태그는 직접적인 보안 위험을 제기하는 위협 및 캠페인을 식별합니다. 태그가 식별하는 위협과 연결된 네트워크의 샘플 수를 보려면 Unit 42 일치 태그를 클릭하십시오.

**STEP 10 |** 아티팩트에 대해 더 많은 일치하는 태그를 찾으십시오.

아티팩트에 대한 AutoFocus 검색을 시작하려면 줄임표( ... )를 클릭하십시오. 검색 결과의 태그 열에는 아티팩트에 대해 일치하는 태그가 더 많이 표시되어 아티팩트가 일반적으로 탐지되는 다른 멀웨어, 악성 동작, 위협 행위자, 악용 또는 캠페인에 대한 아이디어를 얻을 수 있습니다.




 ©2023 Palo Alto Networks, Inc.

# Palo Alto Networks와 위협 인텔리전스 공유

원격 측정은 분석을 위해 데이터를 수집하고 전송하는 프로세스입니다. 방화벽에서 원격 측정을 활성화하면 방화벽은 애플리케이션, 위협 및 디바이스 상태를 포함하는 정보를 주기적으로 수집하여 Palo Alto Networks로 보냅니다. 위협 인텔리전스를 공유하면 다음과 같은 이점이 있습니다.

- 강화된 취약성 및 스파이웨어 서명이 귀하와 전 세계 다른 고객에게 제공됩니다. 예를 들어 위협 이벤트가 취약성 또는 스파이웨어 서명을 트리거하면 방화벽은 위협과 관련된 URL을 Palo Alto Networks 위협 연구 팀과 공유하므로 URL을 악성으로 적절하게 분류할 수 있습니다.
- 네트워크에 영향을 주지 않고 실험적 위협 서명을 신속하게 테스트하고 평가하여 모든 Palo Alto Networks 고객에게 중요한 위협 방지 서명을 더 빠르게 출시할 수 있습니다.
- PAN-DB URL 필터링, DNS 기반 명령 및 제어(C2) 서명 및 WildFire 내에서 정확도 및 멀웨어 탐지 기능이 향상되었습니다.

Palo Alto Networks는 원격 측정에서 추출한 위협 인텔리전스를 사용하여 귀하와 다른 Palo Alto Networks 사용자에게 이러한 이점을 제공합니다. 모든 Palo Alto Networks 사용자는 각 사용자가 공유하는 원격 측정 데이터의 이점을 활용하여 원격 측정을 위협 방지에 대한 커뮤니티 중심 접근 방식으로 생성합니다. Palo Alto Networks는 귀하의 원격 측정 데이터를 다른 고객이나 제3자 조직과 공유하지 않습니다.

이점, 사용법 및 구성을 포함하여 원격 분석에 대한 자세한 내용은 디바이스 원격 측정을(를) 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# 위협 예방 리소스

위협 방지 모범 사례에 대한 자세한 내용은 다음 소스를 참조하십시오.

- 사용자 지정 위협 서명 만들기
- 레이어 4 및 레이어 7 이베이전으로부터 네트워크를 보호하기 위한 모범 사례
- URL 필터링 모범 사례
- 제로 트러스트 모범 사례
- DoS 및 영역 보호 모범 사례

Palo Alto Networks 제품이 식별할 수 있는 위협 및 애플리케이션 목록을 보려면 다음 링크를 사용하십시오.

- Applipedia - Palo Alto Networks가 식별할 수 있는 애플리케이션에 대한 세부 정보를 제공합니다.
- 위협 볼트 - Palo Alto Networks 제품이 식별할 수 있는 위협을 나열합니다. 취약점, 스파이웨어 또는 바이러스로 검색할 수 있습니다. 위협에 대한 자세한 내용은 ID 번호 옆에 있는 세부 정보 아이콘을 클릭합니다.


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

# 복호화

Palo Alto Networks 방화벽은 트래픽을 해독하고 검사하여 위협에 대한 가시성을 제공하고 프로토콜, 인증서 확인 및 장애 처리를 제어할 수 있습니다. 복호화은 구성된 보안 설정에 따라 방화벽이 암호화된 트래픽을 처리하도록 암호화된 트래픽에 정책을 적용할 수 있습니다. 트래픽을 해독하여 암호화된 악성 콘텐츠가 네트워크에 유입되지 않도록 하고 민감한 콘텐츠가 네트워크를 암호화된 트래픽으로 숨겨져 나가는 것을 방지합니다. 복호화 활성화에는 복호화에 필요한 키 및 인증서 준비, 복호화 프로파일 및 정책 생성, 복호화 포트 미러링 구성이 포함될 수 있습니다.


- 복호화 개요
- 복호화 개념
- 복호화 배포 준비
- 해독할 트래픽 정의
- SSL 포워드 프록시 구성
- SSL 인바운드 검사 구성
- SSH 프록시 구성
- 복호화되지 않은 트래픽에 대한 서버 인증서 확인 구성
- 복호화 제외
- 개인 키 내보내기 차단
- 사용자가 SSL 복호화를 옵트아웃할 수 있도록 설정
- 일시적으로 SSL 복호화 사용 안 함
- 복호화 포트 미러링 구성
- 암호 해독 확인
- 복호화 문제 해결 및 모니터링
- 복호화 기능을 위한 무료 라이선스 활성화

# 복호화 개요

SSL(Secure Sockets Layer) 및 SSH(Secure Shell) 암호화 프로토콜은 웹 서버와 클라이언트와 같은 두 엔터티 간의 트래픽을 보호합니다. SSL 및 SSH는 트래픽을 캡슐화하여 데이터를 암호화하여 데이터를 디코딩하는 키와 디바이스 간의 신뢰를 확인하는 인증서가 있는 클라이언트 및 서버 이외의 엔터티에 의미가 없도록 합니다. SSL 및 SSH 트래픽 복호화:

- 암호화된 트래픽으로 숨겨진 멀웨어가 네트워크에 유입되는 것을 방지합니다. 예를 들어 공격자는 SSL 암호화를 사용하는 웹사이트를 손상시킵니다. 직원이 해당 웹사이트를 방문하여 자신도 모르게 익스플로잇이나 멀웨어를 다운로드합니다. 그런 다음 멀웨어는 감염된 직원 엔드포인트를 사용하여 네트워크를 통해 측면으로 이동하고 다른 시스템을 손상시킵니다.
- 민감한 정보가 네트워크 외부로 이동하는 것을 방지합니다.
- 적절한 애플리케이션이 보안 네트워크에서 실행되고 있는지 확인합니다.
- 트래픽을 선택적으로 복호화합니다. 예를 들어, 금융 또는 의료 사이트에 대한 트래픽을 복호화에서 제외하는 복호화 정책 및 프로파일을 생성합니다.

Palo Alto Networks 방화벽 복호화은 정책 기반이며 인바운드 및 아웃바운드 SSL 및 SSH 연결을 복호화, 검사 및 제어할 수 있습니다. 복호화 정책을 사용하면 대상, 소스, 서비스 또는 URL 카테고리별로 복호화할 트래픽을 지정하고 연결된 복호화 프로파일의 보안 설정에 따라 지정된 트래픽을 차단, 제한 또는 포워딩할 수 있습니다. 복호화 프로파일은 SSL 프로토콜, 인증서 확인 및 실패 검사를 제어하여 약한 알고리즘이나 지원되지 않는 모드를 사용하는 트래픽이 네트워크에 액세스하는 것을 방지합니다. 방화벽은 인증서와 키를 사용하여 일반 텍스트에 대한 트래픽을 복호화한 다음 복호화, 바이러스 백신, 취약점, 안티 스파이웨어, URL 필터링, WildFire 및 파일 차단 프로파일을 포함하여 일반 텍스트 트래픽에 App-ID 및 보안 설정을 적용합니다. 트래픽을 복호화하고 검사한 후 방화벽은 개인 정보 및 보안을 보장하기 위해 방화벽을 나갈 때 일반 텍스트 트래픽을 다시 암호화합니다.

방화벽은 세 가지 유형의 복호화 정책 규칙을 제공합니다. SSL 포워딩 프록시는 아웃바운드 SSL 트래픽을 제어하고 SSL 인바운드 검사는 인바운드 SSL 트래픽을 제어하며 SSH 프록시는 터널링된 SSH 트래픽을 제어합니다. 정책 규칙에 복호화 프로파일을 연결하여 서버 인증서 확인, 지원되지 않는 모드 및 실패와 같은 세분화된 액세스 설정을 트래픽에 적용할 수 있습니다.

SSL 복호화(순방향 프록시 및 인바운드 검사 모두)에는 방화벽을 신뢰할 수 있는 제3자로 설정하고 SSL/TLS 연결을 보호하기 위해 클라이언트와 서버 간에 신뢰를 설정하기 위한 인증서가 필요합니다. 기술적인 이유로 SSL 복호화에서 서버를 제외할 때도 인증서를 사용할 수 있습니다(인증서 고정, 지원되지 않는 암호 또는 상호 인증과 같은 이유로 사이트에서 복호화가 중단됨). SSH 복호화에는 인증서가 필요하지 않습니다.



복호화 모범 사례 체크리스트를 사용하여 복호화 배포를 계획, 구현 및 유지 관리합니다.

하드웨어 보안 모듈(HSM)을 방화벽과 통합하여 SSL 포워딩 프록시 및 SSL 인바운드 검사 복호화에 사용되는 개인 키에 대한 보안을 강화할 수 있습니다. HSM을 사용하여 키를 저장 및 생성하고 HSM을 방화벽과 통합하는 방법에 대해 자세히 알아보려면 하드웨어 보안 모듈이 있는 보안 키를 참조하십시오.

또한 암호 해독 미러링을 사용하여 해독된 트래픽을 일반 텍스트로 타사 솔루션으로 전달하여 추가 분석 및 보관을 수행할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

*Decryption* 미러링을 사용하도록 설정하는 경우 중요한 정보를 포함하여 미러링된 모든 트래픽이 일반 텍스트로 전달되므로 미러링할 수 있는 트래픽과 트래픽을 저장할 수 있는 위치와 방법에 대한 현지 법률 및 규정을 알고 있어야 합니다.


©2023 Palo Alto Networks, Inc.

# 복호화 개념

복호화 기능 및 지원에 대해 자세히 알아보려면 다음 항목을 검토하십시오.

- 복호화 정책용 키 및 인증서
- SSL 포워드 프록시
- SSL 포워드 프록시 복호화 프로파일
- SSL 인바운드 검사
- SSL 인바운드 검사 복호화 프로파일
- SSL 프로토콜 설정 복호화 프로파일
- SSH 프록시
- SSH 프록시 복호화 프로파일
- 비복호화을 위한 SSL 프로파일
- ECC(타원 곡선 암호화) 인증서에 대한 SSL 복호화
- SSL 복호화를 위한 PFS(완전한 순방향 보안) 지원
- SSL 복호화 및 주체 대체 이름(SAN)
- TLSv1.3 복호화
- 복호화된 세션에 대한 고가용성 지원
- 복호화 미러링

## 복호화 정책용 키 및 인증서

키는 일반적으로 난수와 큰 소수를 포함하는 수학 연산을 사용하여 생성된 숫자 문자열입니다. 키는 암호 및 공유 비밀과 같은 문자열을 암호화되지 않은 일반 텍스트에서 암호화된 암호문으로, 암호화된 암호문에서 암호화되지 않은 일반 텍스트로 변환합니다. 키는 대칭(암호화 및 복호화에 동일한 키 사용) 또는 비대칭(하나의 키가 암호화에 사용되고 수학적으로 관련된 키가 복호화에 사용됨)일 수 있습니다. 모든 시스템에서 키를 생성할 수 있습니다.

X.509 인증서는 클라이언트와 서버 간에 신뢰를 설정하여 SSL 연결을 설정합니다. 서버를 인증하려는 클라이언트(또는 클라이언트를 인증하는 서버)는 X.509 인증서의 구조를 알고 있으므로 FQDN 또는 IP 주소(인증서 내에서 공통 이름 또는 ***CN***이라고 함) 또는 인증서가 발급된 조직, 부서 또는 사용자의 이름과 같은 인증서 내의 필드에서 서버에 대한 식별 정보를 추출하는 방법을 알고 있습니다. 인증 기관(CA)은 모든 인증서를 발급해야 합니다. CA가 클라이언트나 서버를 확인한 후 CA는 인증서를 발급하고 개인 키로 서명합니다.

동일한 제목과 키를 가진 두 개의 ***CA*(*Device* > *Certificate*** 관리 **>** 디바이스 인증서***)***가 있고 하나의 ***CA***가 만료되는 경우 만료된 ***CA***를 삭제***(***사용자 지정***)***하거나 비활성화***(***사전 정의***)***하십시오**.** 만료된 ***CA***를 삭제하거나 비활성화하지 않으면 방화벽이 만료된 ***CA***에 대한 체인을 구축할 수 있습니다**.**

트래픽에 복호화 정책을 적용하면 방화벽이 서버 인증서에 서명한 CA를 신뢰하는 경우에만 클라이언트와 서버 간의 세션이 설정됩니다. 신뢰를 설정하려면 방화벽의 인증서 신뢰 목록(CTL)에 서버 루트 CA 인증

 ©2023 Palo Alto Networks, Inc.

서가 있어야 하고 해당 루트 CA 인증서에 포함된 공개 키를 사용하여 서명을 확인해야 합니다. 그런 다음 방화벽은 클라이언트가 인증할 수 있도록 포워드 트러스트 인증서로 서명된 서버 인증서 복사본을 제공합니다. 엔터프라이즈 CA를 SSL 포워딩 프록시에 대한 포워딩 신뢰 인증서로 사용하도록 방화벽을 구성할 수도 있습니다. 방화벽의 CTL에 서버 루트 CA 인증서가 없는 경우 방화벽은 포워드 언트러스트 인증서로 서명된 서버 인증서 복사본을 클라이언트에 제공합니다. 포워드 언트러스트 인증서를 사용하면 신뢰할 수 없는 인증서가 있는 서버에서 호스팅하는 사이트에 액세스하려고 할 때 클라이언트에 인증서 경고 메시지가 표시됩니다.

인증서에 대한 자세한 내용은 인증서 관리를 참조하십시오.

방화벽이 신뢰하는 신뢰할 수 있는 ***CA***를 제어하려면 방화벽 웹 인터페이스에서 ***Device*** > ***Certificate Management*** > ***Certificates*** > ***Default Trusted Certificate Authorities*** 탭을 사용하십시오.

다음 표에서는 Palo Alto Networks 방화벽이 복호화에 사용하는 다양한 인증서를 설명합니다.

| 복호화에 사용되는 인증서 | 설명 |
|---|---|
| 포워드 트러스트(SSL 포워드 프록시 복호화에 사용) | 클라이언트가 연결을 시도하는 사이트에 방화벽이 신뢰하는 CA에서 서명한 인증서가 있는 경우 방화벽이 복호화 중에 클라이언트에 제공하는 인증서입니다. 서버 인증서가 신뢰할 수 있는 CA에 의해 서명될 때 클라이언트에 제공하도록 방화벽에서 포워딩 신뢰 인증서를 구성하려면 SSL 포워딩 프록시 구성을 참조하십시오.<br><br>기본적으로 방화벽은 대상 서버의 키 크기에 따라 클라이언트 인증서에 사용할 키 크기를 결정합니다. 그러나 SSL 프록시 서버 인증서의 키 크기를 구성할 수 있습니다. 보안을 강화하려면 하드웨어 보안 모듈에 포워드 트러스트 인증서와 연결된 개인 키를 저장하는 것이 좋습니다(HSM에 개인 키 저장 참조).<br><br>방화벽에 문제가 발생하는 경우에도 포워드 트러스트 ***CA*** 인증서에 계속 액세스할 수 있도록 보안 리포지토리에 방화벽의 포워드 트러스트 ***CA*** 인증서와 연결된 개인 키(방화벽의 마스터 키 아님)를 백업합니다. 보안을 강화하려면 하드웨어 보안 모듈에 포워드 트러스트 인증서와 연결된 개인 키를 저장하는 것이 좋습니다(HSM에 개인 키 저장 참조). |
| 포워딩 언트러스트(SSL 포워딩 프록시 복호화에 사용) | 클라이언트가 연결을 시도하는 사이트에 방화벽이 신뢰하지 않는 CA에서 서명한 인증서가 있는 경우 방화벽이 복호화 중에 클라이언트에 제공하는 인증서입니다. 방화벽에서 포워딩 언트러스트 인증서를 구성하려면 SSL 포워딩 프록시 구성을 참조하십시오. |
| SSL 인바운드 검사 | 해당 서버로 향하는 트래픽의 SSL 인바운드 검사를 수행하려는 네트워크의 서버 인증서. 서버 인증서를 방화벽으로 가져옵니다. |

 ©2023 Palo Alto Networks, Inc.

| 복호화에 사용되는 인증서 | 설명 |
| --- | --- |
| | *PAN-OS 8.0*부터 방화벽은 *ECDHE(Elliptic-Curve Diffie-Hellman Ephemeral)* 알고리즘을 사용하여 엄격한 인증서 검사를 수행합니다. 즉, 방화벽이 중간 인증서를 사용하는 경우 *PAN-OS 8.0* 또는 이후 릴리스로 업그레이드한 후 웹 서버에서 방화벽으로 인증서를 다시 가져와 서버 인증서를 중간 인증서와 결합해야 합니다*(*체인 인증서 설치*)*. 그렇지 않으면 체인에 중간 인증서가 있는 ***SSL*** 인바운드 검사 세션이 실패합니다. 체인 인증서를 설치하려면 다음을 수행하십시오.<br>**1.** 메모장과 같은 일반 텍스트 편집기에서 각 인증서*(.cer)* 파일을 엽니다.<br>**2.** 아래에 포함된 각 서명자와 함께 맨 위에 서버 인증서가 있는 각 인증서를 양끝에 붙여넣습니다.<br>**3.** 파일을 텍스트*(.txt)* 또는 인증서*(.cer)* 파일로 저장합니다*(*파일 이름에 빈 공백이 포함될 수 없음*)*.<br>**4.** 결합된*(*체인*)* 인증서를 방화벽으로 가져옵니다. |

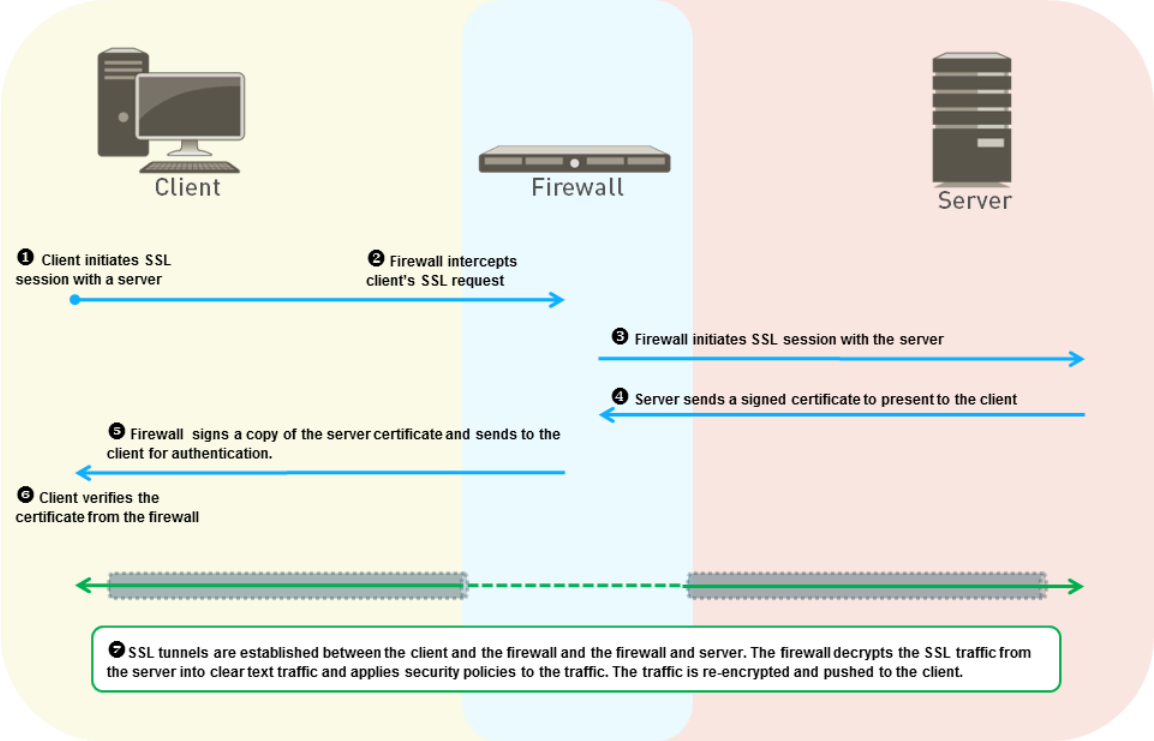
## SSL 포워드 프록시

외부 사이트로 나가는 SSL 트래픽을 복호화하도록 방화벽을 구성하면 SSL 포워딩 프록시로 작동합니다. SSL 포워드 프록시 복호화 정책을 사용하여 내부 사용자에서 웹으로의 SSL/TLS 트래픽을 복호화하고 검사합니다. SSL Forward 프록시 복호화는 방화벽이 복호화 프로파일 및 보안 정책 및 프로파일을 트래픽에 적용할 수 있도록 트래픽을 복호화하여 SSL 암호화 트래픽이 회사 네트워크에 유입되는 것을 방지합니다.

SSL Forward Proxy 복호화에서 방화벽은 내부 클라이언트와 외부 서버 사이의 중간자(man-in-the-middle)입니다. 방화벽은 인증서를 사용하여 클라이언트를 서버에 투명하게 나타내고 서버를 클라이언트에 투명하게 나타내므로 클라이언트가 서버와 직접 통신하고 있다고 판단되고(클라이언트 세션이 방화벽과 함께 있더라도) 서버는 서버 세션이 방화벽과도 통신하고 있다고 판단합니다. 방화벽은 인증서를 사용하여 클라이언트-서버 세션에 대해 신뢰할 수 있는 중간자(man-in-the-middle)로 설정합니다(인증서에 대한 자세한 내용은 복호화 정책을 위한 키 및 인증서 참조).

다음 그림은 이 과정을 자세히 보여줍니다. SSL 포워드 프록시 구성에 대한 자세한 내용은 SSL 포워드 프록시 구성을 참조하십시오.


©2023 Palo Alto Networks, Inc.



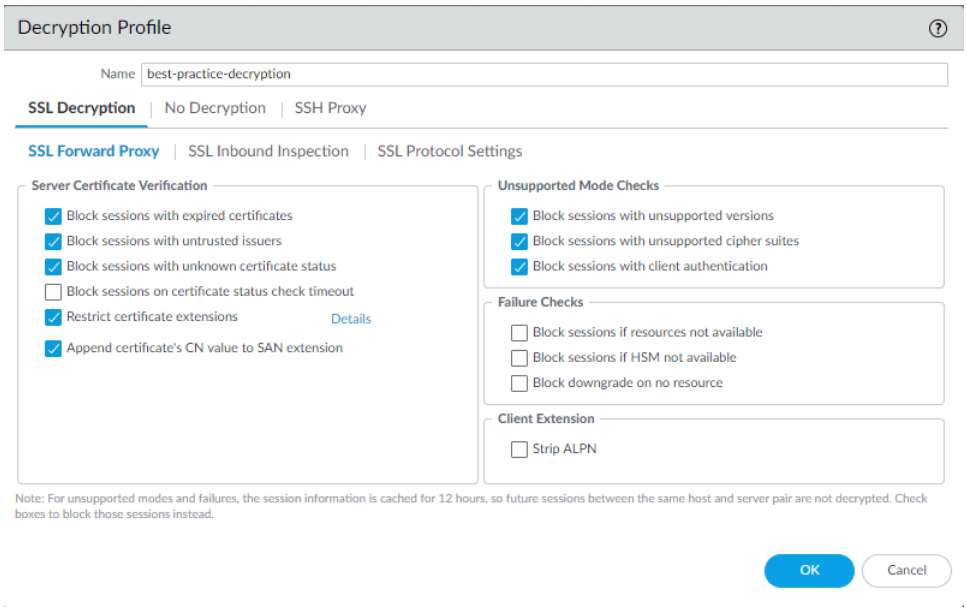

1. 네트워크의 내부 클라이언트가 외부 서버를 사용하여 TLS 세션을 시작하려고 시도합니다.
2. 방화벽은 클라이언트의 SSL 인증서 요청을 가로채지 않습니다. 클라이언트의 경우 방화벽은 설정된 보안 세션이 실제 서버가 아닌 방화벽과 함께 사용되더라도 외부 서버 역할을 합니다.
3. 그런 다음 방화벽은 클라이언트의 SSL 인증서 요청을 서버로 포워딩하여 서버와 별도의 세션을 시작합니다. 서버에게 방화벽은 클라이언트처럼 보이고 서버는 중간자(man-in-the-middle)가 있다는 것을 모르는 상태에서 서버는 인증서를 확인합니다.
4. 서버는 클라이언트를 위해 서명된 인증서를 방화벽으로 보냅니다.
5. 방화벽은 서버 인증서를 분석합니다. 방화벽이 신뢰하고 구성한 정책 및 프로파일을 충족하는 CA에서 서버 인증서에 서명하면 방화벽은 서버 인증서의 SSL Forward Trust 복사본을 생성하고 클라이언트로 보냅니다. 방화벽이 신뢰하지 않는 CA에서 서버 인증서에 서명하면 방화벽은 서버 인증서의 SSL 포워드 트러스트 해제 복사본을 생성하고 클라이언트로 보냅니다. 방화벽이 생성하고 클라이언트로 보내는 인증서를 복사하면 원래 서버 인증서의 확장이 포함되어 있으며 서버의 실제 인증서가 아니기 때문에 가장 인증서라고 합니다. 방화벽이 서버를 신뢰하지 않는 경우 클라이언트는 연결을 시도하는 사이트를 신뢰할 수 없다는 차단 페이지 경고 메시지를 보고 사용자가 SSL 복호화를 옵트아웃할 수 있도록 설정하면 클라이언트는 세션을 계속하거나 종료하도록 선택할 수 있습니다.
6. 클라이언트는 방화벽의 가장 인증서를 확인합니다. 그런 다음 클라이언트는 방화벽이 인증서를 프록시하는 것과 동일한 방식으로 프록시하는 서버와 세션 키 교환을 시작합니다. 방화벽은 클라이언트 키를 서버로 포워딩하고 클라이언트의 서버 키를 가장하여 방화벽이 "보이지 않는" 프록시로 유지되도록 하고 클라이언트와 서버는 세션이 서로 일치한다고 판단하지만 클라이언트와 방화벽 사이에는 여전히 두 개의 별도의 세션이 있습니다. 이제 모든 당사자에게 필요한 인증서와 키가 있고 방화벽은 트래픽을 복호화할 수 있습니다.
7. 사이 모든 SSL 세션 트래픽은 클라이언트와 서버 사이의 방화벽을 문제 없이 통과합니다. 방화벽은 SSL 트래픽을 복호화하고, 보안 정책 및 프로파일 및 복호화 프로파일을 트래픽에 적용하고, 트래픽을 다시 암호화한 다음 포워딩합니다.


©2023 Palo Alto Networks, Inc.

*SSL* 포워드 프록시를 구성할 때, 프록시 트래픽은 *DSCP* 코드 포인트 또는 *QoS*를 지원하지 않습니다.

## SSL 포워드 프록시 복호화 프로파일

SSL 포워드 프록시 복호화 프로파일( **Objects** > **Decryption** 프로파일 > **SSL Decryption** > **SSL** 포워드 프록시)은 프로파일을 연결하는 포워드 프록시 복호화 정책에 정의된 아웃바운드 SSL/TLS 트래픽에 대한 서버 확인, 세션 모드 확인 및 실패 확인을 제어합니다. 다음 그림은 포워드 프록시 복호화 프로파일 설정에 대한 일반적인 모범 사례 권장 사항을 보여주지만 사용하는 설정은 회사의 보안 준수 규칙과 현지 법률 및 규정에 따라 달라집니다. 페리미터 인터넷 게이트웨이 복호화 프로파일 및 데이터 센터 복호화 프로파일에 대한 특정 모범 사례도 있습니다.

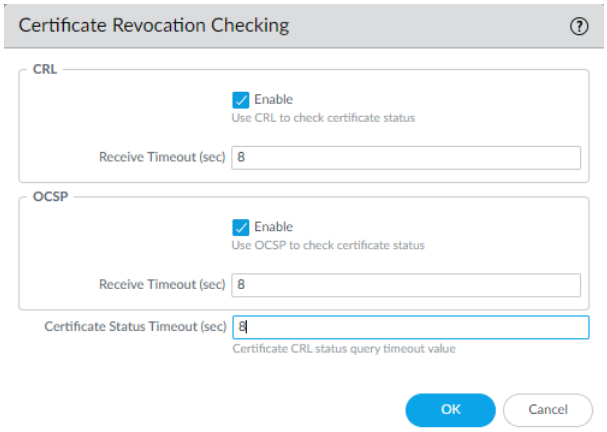



서버 인증서 확인:

- 인증서가 만료된 세션 차단 - 인증서가 만료된 서버와의 세션을 차단하고 잠재적으로 안전하지 않은 사이트에 대한 액세스를 방지하려면 항상 이 체크박스를 선택합니다. 이 체크박스를 선택하지 않으면 사용자는 잠재적으로 악의적인 사이트와 연결하고 거래하고 연결을 시도할 때 경고 메시지를 볼 수 있지만 연결이 방지되지는 않습니다.
- 신뢰할 수 없는 발급자가 있는 세션 차단 - 신뢰할 수 없는 인증서 발급자가 있는 서버와의 세션을 차단하려면 항상 이 체크박스를 선택합니다. 언트러스티드(untrusted) 발급자는 중간자 공격, 재전송 공격 또는 기타 공격을 나타낼 수 있습니다.
- 알 수 없는 인증서 상태의 세션 차단 - 서버의 인증서 해지 상태가 "알 수 없음" 상태로 반환되면 SSL/TLS 세션을 차단합니다. 여러 가지 이유로 인증서 상태를 알 수 없기 때문에 일반적인 복호화 보안을 위해 이 체크박스를 선택하면 일반적으로 보안이 심하게 강화됩니다. 그러나 데이터 센터와 같은 네트워크의 더 높은 보안 영역에서는 이 체크박스를 선택하는 것이 좋습니다.
- 인증서 상태 확인 타임아웃 시 세션 차단 - 상태 확인 타임아웃 시 세션 차단 여부는 회사의 보안 규정 준수 입장에 따라 달라집니다. 이는 엄격한 보안과 더 나은 사용자 경험 간의 절충점이기 때문입니다. 인증서 상태 확인은 해지 서버의 CRL(인증서 해지 목록)을 검사하거나 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 발급 CA가 인증서를 해지했으며 인증서를 신뢰할 수 없는지 확인합니다. 그러나 해지 서버의 응답 속도가 느려 인증서가 유효하더라도 세션 시간이 초과되고 방화벽이 세션을 차단할 수


©2023 Palo Alto Networks, Inc.

있습니다. 인증서 상태 확인 타임아웃 시 세션 차단을 선택하고 해지 서버의 응답이 느린 경우 **Device** > **Setup** > **Session** > 복호화 설정을 사용하고 인증서 해지 확인을 클릭하여 기본 타임아웃 값인 5초를 다른 값으로 변경할 수 있습니다. 예를 들어 다음 그림과 같이 타임아웃 값을 8초로 늘릴 수 있습니다. 서버 인증서에 CRL 배포 지점(CDP) 확장의 CRL URL 또는 AIA(기관 정보 액세스) 인증서 확장의 OCSP URL이 포함될 수 있으므로 CRL 및 OCSP 인증서 해지 확인을 모두 활성화하십시오.




- 인증서 확장 제한 - 이 체크박스를 선택하면 서버 인증서의 인증서 확장이 키 사용 및 확장 키 사용으로 제한되고 다른 확장이 있는 인증서가 차단됩니다. 그러나 특정 배포에서는 다른 인증서 확장이 필요할 수 있으므로 배포에 다른 인증서 확장이 필요하지 않은 경우에만 이 체크박스를 선택합니다.
- 인증서의 **CN** 값을 **SAN** 확장에 추가 - 이 체크박스를 선택하면 브라우저에서 서버 인증서가 SAN(주체 대체 이름)을 사용하도록 요구하고 인증서가 CN(일반 이름)을 기반으로 하는 인증서 일치를 지원하지 않는 경우 SAN 확장이 있는 경우 방화벽이 가장 인증서에 SAN 확장(CN 기반)을 추가하기 때문에 사용자는 요청된 웹 리소스에 계속 액세스할 수 있습니다.

지원되지 않는 모드 확인. 지원되지 않는 모드로 세션을 차단하지 않으면 사용자가 잠재적으로 안전하지 않은 서버에 연결하는 경우 경고 메시지를 수신하고 해당 메시지를 클릭하여 잠재적으로 위험한 사이트에 연결할 수 있습니다. 이러한 세션을 차단하면 취약하고 위험한 프로토콜 버전 및 알고리즘을 사용하는 서버로부터 사용자를 보호할 수 있습니다.

- 지원되지 않는 버전의 세션 차단 - SSL 프로토콜 설정 복호화 프로파일을(를) 구성할 때 네트워크에서 약한 프로토콜을 차단하여 공격 면적을 줄일 수 있도록 SSL 프로토콜의 최소 버전을 지정합니다. 지원하지 않기로 선택한 약한 SSL/TLS 프로토콜 버전의 세션을 차단하려면 항상 이 체크박스를 선택합니다.
- 지원되지 않는 암호화 제품군이 있는 세션 차단 - 방화벽이 핸드쉐이크에 지정된 암호화 제품군을 지원하지 않는 경우 세션을 차단하려면 항상 이 체크박스를 선택합니다. 복호화 프로파일의 **SSL** 프로토콜 설정 탭에서 방화벽이 지원하는 알고리즘을 구성합니다.
- 클라이언트 인증으로 세션 차단 - 클라이언트 인증이 필요한 중요한 애플리케이션이 없는 경우 방화벽이 클라이언트 인증이 필요한 세션의 암호를 복호화할 수 없으므로 차단합니다. 방화벽은 양방향 복호화를 수행하기 위해 클라이언트와 서버 인증서가 모두 필요하지만 클라이언트 인증을 사용하면 방화벽은 서버 인증서만 인지하고 있습니다. 이렇게 하면 클라이언트 인증 세션에 대한 복호화가 중단됩니다.


©2023 Palo Alto Networks, Inc.

이 체크박스를 선택하면 방화벽이 SSL 복호화 제외 목록(**Device** > **Certificate Management** > **SSL** 복호화 제외)에 있는 사이트의 세션을 제외하고 클라이언트 인증이 있는 모든 세션을 차단합니다.

클라이언트 인증으로 세션을 차단하지 않으면 방화벽이 클라이언트 인증을 사용하는 세션의 암호를 해독하려고 할 때 방화벽이 세션을 허용하고 서버 URL/IP 주소, 애플리케이션 및 로컬 복호화 제외 캐시에 대한 암호 해독 프로파일이 포함된 항목을 추가합니다.



클라이언트 인증을 사용하고 ***SSL*** 복호화 제외 목록의 사전 정의된 사이트에 없는 사이트의 네트워크 트래픽을 허용해야 할 수 있습니다. 클라이언트 인증이 있는 세션을 허용하는 복호화 프로파일을 생성합니다. 애플리케이션을 호스팅하는 서버에만 적용되는 복호화 정책 규칙에 추가합니다. 보안을 더욱 강화하려면 사용자 로그인 프로세스를 완료하기 위해 다단계 인증을 요구할 수 있습니다.

실패 확인:

- 리소스를 사용할 수 없는 경우 세션 차단 - 방화벽 처리 리소스를 사용할 수 없을 때 세션을 차단하면 트래픽을 복호화할 리소스가 없을 때 방화벽이 트래픽을 삭제합니다. 방화벽이 리소스 부족으로 인해 복호화를 처리할 수 없을 때 세션을 차단하지 않으면 암호를 복호화하려는 트래픽이 여전히 암호화된 상태로 네트워크에 들어가므로 검사를 받지 않습니다. 그러나 리소스를 사용할 수 없을 때 세션을 차단하면 사용자가 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되어 사용자 경험에 영향을 줄 수 있습니다. 이 실패 검사를 구현할지의 여부는 회사의 보안 규정 준수 입장과 사용자 경험의 중요성에 따라 더 엄격한 보안과 비교하여 결정됩니다. 또는 더 많은 트래픽을 복호화할 수 있도록 처리 능력이 더 높은 방화벽 모델을 사용하는 것이 좋습니다.
- **HSM**을 사용할 수 없는 경우 세션 차단 - HSM(하드웨어 보안 모듈)을 사용하여 비공개 키를 저장하는 경우 사용 여부는 비공개 키의 출처와 원하는 방식에 대한 규정 준수 규칙에 따라 다릅니다. HSM을 사용할 수 없는 경우 암호화된 트래픽을 처리합니다. 예를 들어 회사에서 개인 키 서명에 HSM 사용을 의무화한 경우 HSM을 사용할 수 없는 경우 세션을 차단하십시오. 그러나 회사가 이에 대해 덜 엄격하다면 HSM을 사용할 수 없는 경우 세션을 차단하지 않는 것을 고려할 수 있습니다. (HSM이 다운된 경우 방화벽은 HSM의 응답을 캐시한 사이트에 대한 복호화를 처리할 수 있지만 다른 사이트에 대해서는 처리할 수 없습니다.) 이 경우 모범 사례는 회사 정책에 따라 다릅니다. HSM이 비즈니스에 중요한 경우 고가용성(HA) 쌍에서 HSM을 실행하십시오(PAN-OS 8.1은 HSM HA 쌍에서 두 구성원을 지원함).
- 리소스가 없는 경우 다운그레이드 차단 - 방화벽에 사용 가능한 TLSv1.3 처리 리소스가 없는 경우 방화벽이 TLSv1.3을 TLSv1.2로 다운그레이드하는 것을 방지합니다. 다운그레이드를 차단하면 방화벽에서 TLSv1.3 리소스가 부족할 때 TLSv1.2로 다운그레이드하는 대신 TLSv1.3을 사용하는 트래픽을 삭제합니다. 다운그레이드를 차단하지 않으면 방화벽에 TLSv1.3 리소스가 부족할 때 TLSv1.2로 다운그레이드됩니다. 그러나 리소스를 사용할 수 없을 때 다운그레이드를 차단하면 사용자가 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되어 사용자 경험에 영향을 줄 수 있습니다. 이 실패 검사를 구현할지의 여부는 회사의 보안 규정 준수 입장과 사용자 경험의 중요성에 따라 더 엄격한 보안과 비교하여 결정됩니다. TLS 버전을 다운그레이드하지 않으려는 민감한 트래픽에 대한 복호화를 제어하기 위해 별도의 복호화 정책 및 프로파일을 생성할 수 있습니다.

## SSL 인바운드 검사

SSL 인바운드 검사를 사용하여 클라이언트에서 대상 네트워크 서버(인증서가 있고 방화벽으로 가져올 수 있는 모든 서버)로의 인바운드 SSL/TLS 트래픽을 복호화하고 검사하고 의심스러운 세션을 차단합니다. 예를 들어 악의적인 행위자가 웹 서버의 알려진 취약점을 악용하려고 한다고 가정해 보겠습니다. 인바운드 SSL/TLS 암호 해독은 트래픽에 대한 가시성을 제공하여 방화벽이 위협에 사전 대응할 수 있도록 합니다.


©2023 Palo Alto Networks, Inc.

SSL 인바운드 검사는 방화벽이 내부 클라이언트의 아웃바운드 트래픽을 해독하는 대신 내부 서버에 대한 인바운드 트래픽을 해독한다는 점을 제외하면 SSL 전달 프록시와 유사하게 작동합니다. 방화벽은 외부 클라이언트와 내부 서버 간의 중간자 프록시 역할을 하며 각 보안 세션에 대해 새 세션 키를 생성합니다. 방화벽은 클라이언트와 방화벽 간에 보안 세션을 만들고 방화벽과 서버 간에 트래픽을 해독하고 검사하는 또 다른 보안 세션을 만듭니다.

방화벽에서 SSL 인바운드 검사를 수행하려는 각 서버에 대한 인증서 및 개인 키를 설치해야 합니다. 방화벽은 SSL/TLS 핸드셰이크 중에 대상 서버에서 보낸 인증서가 암호 해독 정책 규칙의 인증서와 일치하는지 확인합니다. 일치하는 항목이 있는 경우 방화벽은 서버 액세스를 요청하는 클라이언트에 서버 인증서를 전달하고 보안 연결을 설정합니다.

웹 서버에서 지원하는 TLS 버전은 방화벽에 서버 인증서 및 키를 설치하는 방법을 결정합니다. 웹 서버가 TLS 1.2 및 Rivest, Shamir, Adleman(RSA) 또는 Perfect Forward Secrecy(PFS) 키 교환 알고리즘을 지원하는 경우 그리고 최종 엔티티(리프) 인증서는 중간 인증서의 경우 방화벽에 인증서 체인을 업로드(단일 파일)하는 것이 좋습니다. 체인을 업로드하면 클라이언트 쪽 서버 인증서 인증 문제가 방지됩니다.

***TLS 1.3***은 ***RSA*** 키 교환 알고리즘에 대한 지원을 제거합니다.

방화벽은 TLS 1.3 연결을 TLS 1.2 연결과 다르게 처리합니다. TLS 1.3 핸드셰이크 중에 방화벽은 서버에서 받은 것과 동일한 인증서 또는 인증서 체인을 클라이언트에 보냅니다. 따라서 웹 서버를 올바르게 설정한 경우 서버 인증서와 개인 키를 방화벽에 업로드하는 것으로 충분합니다. 예를 들어 서버의 리프 인증서가 중간 인증서로 서명된 경우 클라이언트 쪽 서버 인증 문제를 방지하기 위해 인증서 체인을 서버에 설치해야 합니다.


©2023 Palo Alto Networks, Inc.

다중 인증서 지원

*SSL* 인바운드 검사 정책 규칙은 최대 *12*개의 인증서를 지원하므로 가동 중지 시간 없이 보호된 내부 서버에 대한 인증서를 업데이트할 수 있습니다. 지속적인 암호 해독을 위해 정책 규칙과 서버에 유효한 인증서가 항상 있어야 합니다. 서버 인증서가 만료되거나 유효하지 않게 되기 전에 새 인증서를 갱신하거나 얻어야 합니다. 그런 다음 웹 서버에 동일한 인증서를 설치하기 전에 인증서 및 개인 키를 방화벽으로 가져와 *SSL* 인바운드 검사 정책 규칙에 추가합니다. 웹 서버에서 다른 인증서가 활성 상태일 때 정책 규칙을 새 인증서로 업데이트하면 방화벽이 사용 중인 인증서에 관계없이 서버에 대한 트래픽을 해독할 수 있도록 준비됩니다.

새 인증서를 배포할 준비가 되면 웹 서버에 로드하고 올바르게 설치했는지 확인합니다. 새 인증서의 설치는 기존 연결에 영향을 주지 않습니다. 방화벽은 *Server Hello* 메시지의 인증서가 암호 해독 정책 규칙의 새 인증서와 일치하는지 확인합니다. 일치하는 항목이 없으면 세션이 종료됩니다. 해당 암호 해독 로그 항목은 세션 종료 이유를 방화벽과 서버 인증서 간의 불일치로 보고합니다. 성공적인 핸드셰이크를 기록하여 모든 인바운드 검사 세션에 사용된 서버 인증서를 봅니다.

정책 규칙을 만들어 다양한 도메인을 호스팅하는 서버*(*각 도메인마다 자체 인증서가 있는 도메인*)*에 대한 트래픽을 검사할 수도 있습니다.

*(Panorama™) SSL* 인바운드 검사 정책 규칙의 여러 인증서에 대한 지원은 *PAN-OS 10.2* 이전 버전의 *PAN-OS®* 버전에서는 사용할 수 없습니다. *PAN-OS 10.2*를 실행하는 *Panorama* 관리 서버에서 이전 버전을 실행하는 방화벽으로 여러 인증서를 사용하여 *SSL* 인바운드 검사 정책 규칙을 푸시하는 경우 관리되는 방화벽의 정책 규칙은 알파벳순으로 정렬된 인증서 목록에서 첫 번째 인증서만 상속합니다.

*Panorama*에서 암호 해독 정책 규칙을 푸시하기 전에 *PAN-OS 10.1* 이하를 실행하는 방화벽에 대해 다른 템플릿 또는 디바이스 그룹을 설정하여 올바른 정책을 푸시하도록 하는 것이 좋습니다. 규칙 및 인증서를 적절한 방화벽에 연결합니다.

*SSL* 인바운드 검사 트래픽에 대해 SSL 프로토콜 설정 복호화 프로파일을 구성할 때 보안 기능이 서로 다른 서버에 대해 별도의 프로파일을 만듭니다. 예를 들어, 한 서버 세트가 *RSA*만 지원하는 경우 *SSL* 프로토콜 설정은 *RSA*만 지원하면 됩니다. 그러나 *PFS*를 지원하는 서버에 대한 *SSL* 프로토콜 설정은 *PFS*를 지원해야 합니다. 서버가 지원하는 최고 수준의 보안을 위해 *SSL* 프로토콜 설정을 구성하지만 방화벽 리소스가 더 높은 보안 프로토콜 및 알고리즘에 필요한 더 높은 처리 부하를 처리할 수 있는지 확인하려면 성능을 확인하십시오.

*SSL* 인바운드 검사는 세션 재개를 지원하지 않습니다.

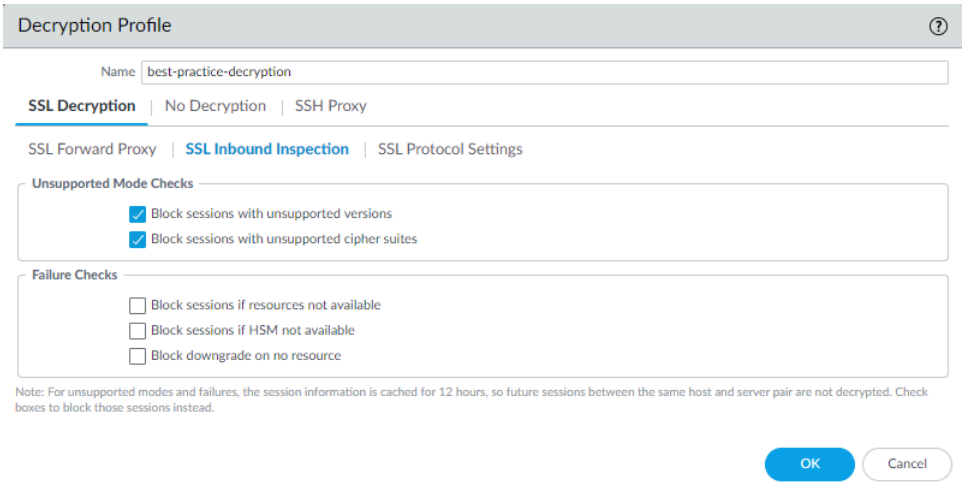
*SSL* 인바운드 검사를 구성할 때 프록시된 트래픽은 *DSCP* 코드 포인트 또는 *QoS*를 지원하지 않습니다.

내부 서버를 보호하려면 SSL 인바운드 검사 구성 정책 규칙 단계를 따르십시오.


©2023 Palo Alto Networks, Inc.

# SSL 인바운드 검사 복호화 프로파일

SSL 인바운드 검사 복호화 프로파일(**Objects** > **Decryption** 프로파일 > **SSL Decryption** > **SSL** 인바운드 검사)은 프로파일을 연결하는 인바운드 검사 복호화 정책에 정의된 인바운드 SSL/TLS 트래픽에 대한 세션 모드 검사 및 실패 검사를 제어합니다. 다음 그림은 Inbound Inspection Decryption 프로파일 설정에 대한 일반적인 모범 사례 권장 사항을 보여주지만 사용하는 설정은 회사의 보안 준수 규칙과 현지 법률 및 규정에 따라 달라집니다.




지원되지 않는 모드 확인. 지원되지 않는 모드로 세션을 차단하지 않으면 사용자가 잠재적으로 안전하지 않은 서버에 연결하는 경우 경고 메시지를 수신하고 해당 메시지를 클릭하여 잠재적으로 위험한 사이트에 연결할 수 있습니다. 이러한 세션을 차단하면 취약하고 위험한 프로토콜 버전 및 알고리즘을 사용하는 서버로부터 사용자를 보호할 수 있습니다.

1. 지원되지 않는 버전의 세션 차단 - SSL 프로토콜 설정 복호화 프로파일을(를) 구성할 때 네트워크에서 약한 프로토콜을 차단하여 공격 면적을 줄일 수 있도록 TLS 프로토콜의 최소 버전을 지정합니다. 지원하지 않기로 선택한 약한 SSL 및 TLS 프로토콜 버전의 세션을 차단하려면 항상 이 체크박스를 선택합니다.
2. 지원되지 않는 암호화 제품군이 있는 세션 차단 - 방화벽이 핸드쉐이크에 지정된 암호화 제품군을 지원하지 않는 경우 세션을 차단하려면 항상 이 체크박스를 선택합니다. 복호화 프로파일의 **SSL** 프로토콜 설정 탭에서 방화벽이 지원하는 알고리즘을 구성합니다.

실패 확인:

- 리소스를 사용할 수 없는 경우 세션 차단 - 방화벽 처리 리소스를 사용할 수 없을 때 세션을 차단하면 트래픽을 복호화할 리소스가 없을 때 방화벽이 트래픽을 삭제합니다. 방화벽이 리소스 부족으로 인해 복호화를 처리할 수 없을 때 세션을 차단하지 않으면 암호를 복호화하려는 트래픽이 여전히 암호화된 상태로 네트워크에 들어가므로 검사를 받지 않습니다. 그러나 리소스를 사용할 수 없을 때 세션을 차단하면 사용자가 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되어 사용자 경험에 영향을 줄 수 있습니다. 이 실패 검사를 구현할지의 여부는 회사의 보안 규정 준수 입장과 사용자 경험의 중요성에 따라 더 엄격한 보안과 비교하여 결정됩니다. 또는 더 많은 트래픽을 복호화할 수 있도록 처리 능력이 더 높은 방화벽 모델을 사용하는 것이 좋습니다.
- **HSM**을 사용할 수 없는 경우 세션 차단 - HSM(하드웨어 보안 모듈)을 사용하여 비공개 키를 저장하는 경우 사용 여부는 비공개 키의 출처와 원하는 방식에 대한 규정 준수 규칙에 따라 다릅니다. HSM을 사용할 수 없는 경우 암호화된 트래픽을 처리합니다. 예를 들어 회사에서 개인 키 서명에 HSM 사용을 의


©2023 Palo Alto Networks, Inc.

무화한 경우 HSM을 사용할 수 없는 경우 세션을 차단하십시오. 그러나 회사가 이에 대해 덜 엄격하다면 HSM을 사용할 수 없는 경우 세션을 차단하지 않는 것을 고려할 수 있습니다. (HSM이 다운된 경우 방화벽은 HSM의 응답을 캐시한 사이트에 대한 복호화를 처리할 수 있지만 다른 사이트에 대해서는 처리할 수 없습니다.) 이 경우 모범 사례는 회사 정책에 따라 다릅니다. HSM이 비즈니스에 중요한 경우 고가용성(HA) 쌍에서 HSM을 실행하십시오(PAN-OS 8.1은 HSM HA 쌍에서 두 구성원을 지원함).

- 리소스가 없는 경우 다운그레이드 차단 - 방화벽에 사용 가능한 TLSv1.3 처리 리소스가 없는 경우 방화벽이 TLSv1.3을 TLSv1.2로 다운그레이드하는 것을 방지합니다. 다운그레이드를 차단하면 방화벽에서 TLSv1.3 리소스가 부족할 때 TLSv1.2로 다운그레이드하는 대신 TLSv1.3을 사용하는 트래픽을 삭제합니다. 다운그레이드를 차단하지 않으면 방화벽에 TLSv1.3 리소스가 부족할 때 TLSv1.2로 다운그레이드됩니다. 그러나 리소스를 사용할 수 없을 때 다운그레이드를 차단하면 사용자가 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되어 사용자 경험에 영향을 줄 수 있습니다. 이 실패 검사를 구현할지의 여부는 회사의 보안 규정 준수 입장과 사용자 경험의 중요성에 따라 더 엄격한 보안과 비교하여 결정됩니다. TLS 버전을 다운그레이드하지 않으려는 민감한 트래픽에 대한 복호화를 제어하기 위해 별도의 복호화 정책 및 프로파일을 생성할 수 있습니다.

## SSL 프로토콜 설정 복호화 프로파일

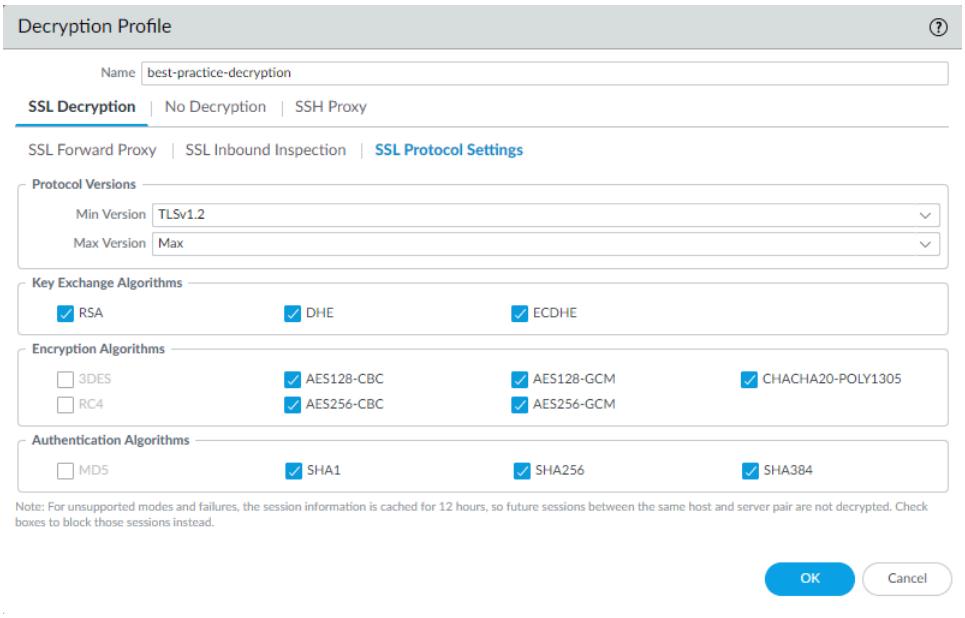
SSL 프로토콜 설정(개체 > 복호화 프로파일 > **SSL** 복호화 > **SSL** 프로토콜 설정)은 취약한 SSL/TLS 프로토콜 버전, 약한 암호화 알고리즘 및 약한 인증 알고리즘을 허용할지의 여부를 제어합니다. SSL 프로토콜 설정은 아웃바운드 SSL 포워드 프록시 및 인바운드 SSL 인바운드 검사 트래픽에 적용됩니다. 이러한 설정은 SSH 프록시 트래픽이나 복호화하지 않는 트래픽에는 적용되지 않습니다.

다음 그림은 SSL 프로토콜 설정에 대한 일반적인 모범 사례 권장 사항을 보여줍니다. 페리미터 인터넷 게이트웨이 복호화 프로파일 및 데이터 센터 복호화 프로파일에 대한 특정 모범 사례도 있습니다.



***SSL*** 인바운드 검사 트래픽에 대한 ***SSL*** 프로토콜 설정을 구성할 때 보안 기능이 다른 서버에 대해 별도의 프로파일을 생성합니다. 예를 들어, 한 서버 세트가 ***RSA***만 지원하는 경우 ***SSL*** 프로토콜 설정은 ***RSA***만 지원하면 됩니다. 그러나 ***PFS***를 지원하는 서버에 대한 ***SSL*** 프로토콜 설정은 ***PFS***를 지원해야 합니다. ***SSL*** 프로토콜 설정을 보호하는 대상 서버가 지원하는 최고 수준의 보안에 대해 구성하지만 성능을 확인하여 방화벽 리소스가 더 높은 보안 프로토콜 및 알고리즘이 요구하는 더 높은 처리 부하를 처리할 수 있는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.




프로토콜 버전:

- 보안 지원 **TLSv1.2**의 가치를 가진 비즈니스 사이트인 가장 강력한 보안을 제공하기 위해 **Min Version**을 TLSv1.2로 설정합니다. 사이트(또는 사이트 카테고리)만 약한 암호만 지원하는 경우 사이트를 검토하고 합법적인 비즈니스 애플리케이션을 호스팅하는지 확인합니다. 이 경우 사이트가 지원하는 가장 강력한 암호와 일치하는 **Min Version**으로 복호화 프로파일을 구성한 다음 약한 암호가 해당 사이트 또는 사이트만 허용하도록 제한하는 복호화 정책 규칙에 프로파일을 적용하여 해당 사이트에 대해서만 예외를 생성합니다. 사이트가 합법적인 비즈니스 애플리케이션을 호스팅하지 않는 경우 공격자가 악용할 수 있는 알려진 취약점이 포함된 취약한 프로토콜(및 암호)과 같은 사이트를 지원하기 위해 보안 수준을 낮추지 마십시오.

  사이트가 비즈니스 목적으로 필요하지 않은 사이트 카테고리에 속하는 경우 URL 필터링을 사용하여 전체 카테고리에 대한 액세스를 차단합니다. 중요한 레거시 사이트를 지원해야 하고 예외를 만들 경우 해당 사이트에 대해 약한 프로토콜을 허용하는 별도의 복호화 프로파일을 만들지 않는 한 약한 암호화 또는 인증 알고리즘을 지원하지 마십시오. 몇 가지 예외를 수용하기 위해 대부분의 사이트에 적용되는 기본 복호화 프로파일을 TLSv1.1로 다운그레이드하지 마십시오.

  *Qualys SSL Labs* SSL Pulse 웹 페이지는 전 세계에서 가장 인기 있는 *150,000*개 사이트에서 사용되는 다양한 암호 및 프로토콜의 백분율에 대한 최신 통계를 제공하므로 추세를 확인하고 전 세계적으로 보다 안전한 암호 및 프로토콜에 대한 광범위한 지원을 이해할 수 있습니다.

- 프로토콜이 개선되면 방화벽이 자동으로 최신 프로토콜을 지원하도록 특정 버전이 아닌 **Max** 버전으로 **Max Version**을 설정합니다. 인바운드(SSL 인바운드 검사) 또는 아웃바운드(SSL Forward Proxy) 트

 ©2023 Palo Alto Networks, Inc.

래픽을 제어하는 복호화 정책 규칙에 복호화 프로파일을 첨부하려는 경우 약한 알고리즘을 허용하지 마십시오.

복호화 정책이 고정된 인증서를 사용하는 모바일 애플리케이션을 지원하는 경우 ***Max Version***을 ***TLSv1.2***로 설정합니다. ***TLSv1.3***은 이전 ***TLS*** 버전에서 암호화되지 않은 인증서 정보를 암호화하므로 방화벽은 일부 모바일 애플리케이션에 영향을 미치는 인증서 정보에 따라 복호화 제외를 자동으로 추가할 수 없습니다. 따라서 ***TLSv1.3***을 사용하도록 설정하면 해당 트래픽에 대한 복호화 정책을 만들지 않는 한 방화벽이 일부 모바일 애플리케이션 트래픽이 떨어질 수 있습니다.

비즈니스에 사용하는 모바일 애플리케이션을 알고 있는 경우 다른 모든 애플리케이션 트래픽에 대해 ***TLSv1.3***을 활성화할 수 있도록 해당 애플리케이션에 대해 별도의 복호화 정책 및 프로파일을 만드는 것이 좋습니다.

키 교환 알고리즘: 최소 버전이 TLSv1.3으로 설정되지 않은 경우 RSA 및 PFS(DHE 및 ECDHE) 키 교환을 모두 지원하려면 세 개의 상자를 모두 선택된 상태로 둡니다(기본값). ECDHE만 지원합니다.

***HTTP/2*** 트래픽을 지원하려면 ***ECDHE*** 확인란을 선택된 상태로 두어야 합니다.

암호화 알고리즘: 최소 프로토콜 버전을 TLSv1.2로 설정하면 이전의 약한 3DES 및 RC4 알고리즘이 자동으로 선택 해제되지 않습니다(차단됨). 최소 프로토콜 버전을 TLSv1.3으로 설정하면 3DES, RC4, AES128-CBC 및 AES256-CBC 알고리즘이 자동으로 차단됩니다. 약한 TLS 프로토콜을 허용해야 하는 트래픽의 경우 별도의 복호화 프로파일을 생성하고 해당 사이트의 트래픽에만 적용하고 알고리즘을 허용하도록 적절한 상자를 선택 해제합니다. 3DES 또는 RC4 알고리즘을 사용하는 트래픽을 허용하면 네트워크가 과도한 위험에 노출됩니다. 3DES 또는 RC4를 차단하면 비즈니스에 사용해야 하는 사이트에 액세스하지 못하도록 하는 경우 해당 사이트에 대해 별도의 복호화 프로파일 및 정책을 생성합니다. 다른 사이트의 복호화 수준을 낮추지 마십시오.

인증 알고리즘: 방화벽은 이전의 약한 MD5 알고리즘을 자동으로 차단합니다. TLSv1.3이 최소 버전인 경우 방화벽은 SHA1을 차단합니다. 네트워크에서 MD5 인증 트래픽을 허용하지 마십시오. SHA1은 허용해야 하는 가장 약한 인증 알고리즘입니다. 필요한 사이트가 SHA1을 사용하지 않으면 SHA1 트래픽을 차단하여 공격 면적을 더욱 줄입니다.

## SSH 프록시

SSH 프록시 구성에서 방화벽은 클라이언트와 서버 사이에 있습니다. SSH 프록시를 사용하면 방화벽이 인바운드 및 아웃바운드 SSH 연결을 복호화할 수 있으며 공격자가 SSH를 사용하여 원치 않는 애플리케이션 및 콘텐츠를 터널링하지 않도록 합니다. SSH 복호화에는 인증서가 필요하지 않으며 방화벽이 부팅될 때 방화벽이 SSH 복호화에 사용되는 키를 자동으로 생성합니다. 부팅 프로세스 중에 방화벽은 기존 키가 있는지 확인합니다. 그렇지 않은 경우 방화벽이 키를 생성합니다. 방화벽은 키를 사용하여 방화벽 및 모든 SSH v2 세션에 구성된 모든 가상 시스템의 SSH 세션을 복호화합니다.

SSH는 터널링을 허용하여 악성 트래픽을 복호화으로부터 숨길 수 있습니다. 방화벽은 SSH 터널 내부의 트래픽을 복호화할 수 없습니다. 작업이 거부로 설정된 애플리케이션 **ssh-tunnel**에 대한 보안 정책 규칙(ssh 애플리케이션의 트래픽을 허용하는 보안 정책 규칙 포함)을 구성하여 모든 **SSH** 터널 트래픽을 차단할 수 있습니다.


©2023 Palo Alto Networks, Inc.

SSH 터널링 세션은 X11 윈도우 패킷과 TCP 패킷을 터널링할 수 있습니다. 하나의 SSH 연결에는 여러 채널이 포함될 수 있습니다. 트래픽에 SSH 복호화 프로파일을 적용하면 방화벽이 트래픽의 앱 ID를 검사하고 채널 유형을 식별합니다. 채널 유형은 다음과 같습니다.

- 세션
- X11
- forwarded-tcpip
- direct-tcpip

채널 유형이 세션인 경우 방화벽은 트래픽을 SFTP 또는 SCP와 같은 허용된 SSH 트래픽으로 식별합니다. 채널 유형이 X11, 포워딩된 tcpip 또는 직접 tcpip인 경우 방화벽은 트래픽을 SSH 터널링 트래픽으로 식별하고 차단합니다.



네트워크 디바이스를 관리하고, 모든 ***SSH*** 트래픽을 기록해야 하는 관리자로 ***SSH*** 사용을 제한하고, 합법적인 사용자만 ***SSH***를 사용하여 디바이스에 액세스할 수 있도록 멀티 팩터 인증을 구성하여 공격 범위를 줄입니다.



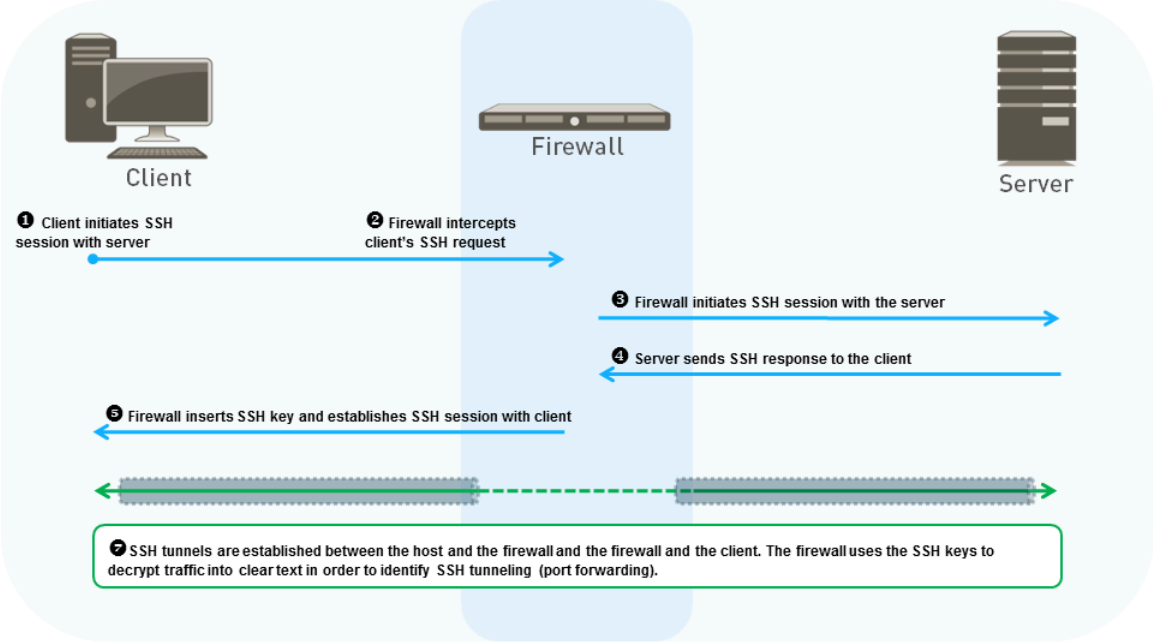
방화벽에서 ***SSH*** 암호 해독을 사용하도록 설정한 후에는 ***SSH*** 클라이언트가 더 이상 공개 키 기반 인증을 사용하지 않으므로 인증서가 있는 호스트에 대한 인증이 실패하므로 서버는 클라이언트가 개인 키로 해독할 수 있는 클라이언트의 공개 키를 사용하여 핸드셰이크를 완료할 수 없습니다. 사용자 이름 및 암호 인증을 사용하여 ***SSH*** 세션을 시작합니다.

키 기반 인증을 사용해야 하는 시스템의 경우 공개 키 인증이 필요한 시스템을 제외하도록 ***SSH*** 암호 해독 정책 규칙을 구성합니다. ***SSH*** 암호 해독 정책 규칙을 편집하려면 다음을 수행합니다.

1. 정책 > 암호 해독으로 이동하여 ***SSH*** 암호 해독을 제어하는 정책 규칙을 선택합니다.
2. 대상 탭을 선택합니다.
3. 규칙에서 제외할 시스템의 ***IP*** 주소를 추가합니다.
4. 부정을 선택합니다.
5. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

다음 그림은 SSH 프록시 복호화의 작동 방식을 보여 줍니다. SSH 프록시 복호화를 사용하도록 설정하는 방법은 SSH 프록시 구성을 참조하십시오.


©2023 Palo Alto Networks, Inc.




1. 클라이언트는 세션을 시작하기 위해 서버에 SSH 요청을 보냅니다.
2. 방화벽은 클라이언트의 SSH 요청 을 가로챕니다.
3. 방화벽은 서버에 요청을 전달하고 서버와의 SSH 세션을 시작합니다. 이렇게 하면 방화벽이 만드는 두 개의 개별 세션 중 첫 번째 세션이 설정됩니다. 각 세션은 별도의 SSH 터널을 설정합니다.
4. 서버는 방화벽이 가로채는 요청에 응답합니다.
5. 방화벽은 SSH 키를 서버의 응답에 삽입하고 클라이언트로 전달합니다. 이렇게 하면 방화벽이 만드는 두 번째 개별 세션(및 별도의 SSH 터널)이 설정됩니다.
6. (다이어그램에서 "7"의 첫 번째 부분) 방화벽이 서버와 클라이언트와 별도의 세션을 설정한 후 방화벽은 이들 사이의 프록시 역할을 합니다.
7. 방화벽은 클라이언트와 서버 간의 트래픽을 검사하여 정상적으로 라우팅되는지 또는 SSH 포트 전달(SSH 터널링)을 사용하는지 확인합니다. 방화벽이 SSH 포트 전달을 식별하면 방화벽은 터널링된 트래픽을 차단하고 구성된 보안 정책에 따라 제한합니다. 방화벽은 SSH 포트 포워딩만 찾고 SSH 터널에서 콘텐츠 및 위협 검사를 수행하지 않습니다.

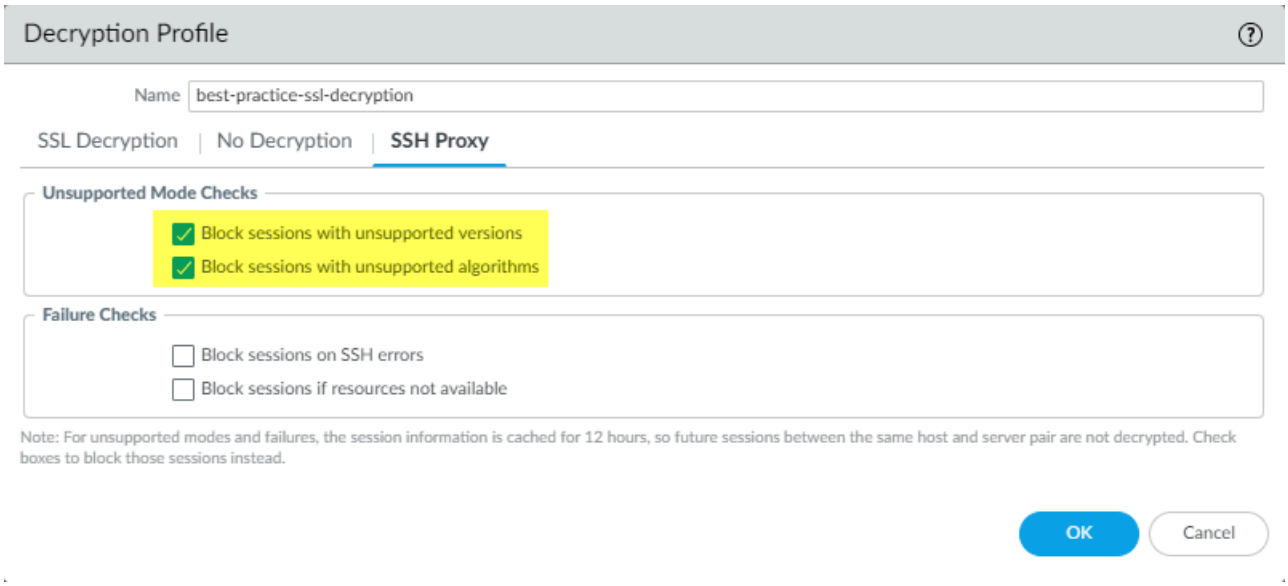
*SSH* 프록시를 구성할 때 프록시된 트래픽은 *DSCP* 코드 포인트 또는 *QoS*를 지원하지 않습니다.

## SSH 프록시 복호화 프로파일

SSH 프록시 복호화 프로파일(**Objects** > **Decryption Profile** > **SSH Proxy**)은 프로파일을 연결하는 SSH 프록시 복호화 정책에 정의된 SSH 트래픽에 대한 세션 모드 검사 및 실패 검사를 제어합니다. 다음 그림은 SSH 프록시 복호화 프로파일 설정에 대한 일반적인 모범 사례 권장 사항을 보여주지만 사용하는 설정은 회사의 보안 규정 준수 규칙과 현지 법률 및 규정에 따라 달라집니다.

방화벽은 *SSH* 터널*(*포트 포워딩*)*에 대한 콘텐츠 및 위협 검사를 수행하지 않습니다*.* 그러나 방화벽은 *SSH* 애플리케이션과 *SSH* 터널 애플리케이션을 구분합니다*.* 방화벽이 *SSH* 터널을 식별하면 *SSH* 터널링된 트래픽을 차단하고 구성된 보안 정책에 따라 트래픽을 제한합니다*.*


©2023 Palo Alto Networks, Inc.




지원되지 않는 모드 확인. 방화벽은 SSHv2를 지원합니다. 지원되지 않는 모드로 세션을 차단하지 않으면 사용자가 잠재적으로 안전하지 않은 서버에 연결하는 경우 경고 메시지를 수신하고 해당 메시지를 클릭하여 잠재적으로 위험한 사이트에 연결할 수 있습니다. 이러한 세션을 차단하면 취약하고 위험한 프로토콜 버전 및 알고리즘을 사용하는 서버로부터 사용자를 보호할 수 있습니다.

1. 지원되지 않는 버전이 있는 세션 차단 - 방화벽에는 사전 정의된 지원 버전 집합이 있습니다. 이 상자를 선택하면 약한 버전의 트래픽을 차단합니다. 공격 면적을 줄이기 위해 약한 프로토콜 버전의 세션을 차단하려면 항상 이 체크박스를 선택하십시오.
2. 지원되지 않는 알고리즘이 있는 세션 차단 - 방화벽에는 사전 정의된 지원되는 알고리즘 집합이 있습니다. 이 체크박스를 선택하면 알고리즘이 약한 트래픽을 차단합니다. 공격 면적을 줄이기 위해 지원되지 않는 알고리즘이 있는 세션을 차단하려면 항상 이 체크박스를 선택합니다.

실패 확인:

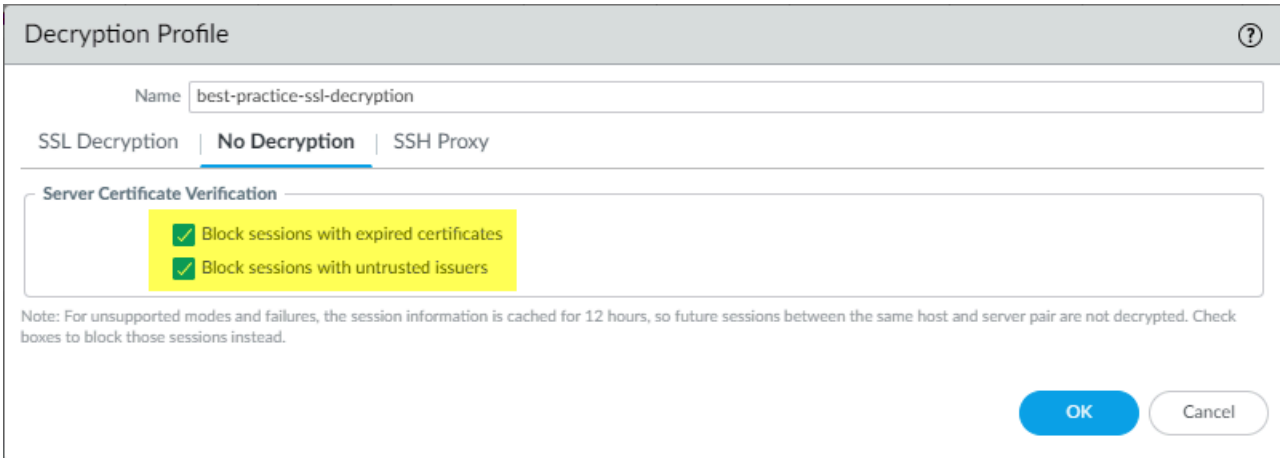
- **SSH** 오류 시 세션 차단 - 이 상자를 선택하면 SSH 오류가 발생할 경우 세션이 종료됩니다.
- 리소스를 사용할 수 없는 경우 세션 차단 - 방화벽 처리 리소스를 사용할 수 없을 때 세션을 차단하지 않으면 암호를 복호화하려는 암호화된 트래픽이 여전히 암호화된 상태로 네트워크에 들어가 잠재적으로 위험한 연결을 허용할 위험이 있습니다. 그러나 방화벽 처리 리소스를 사용할 수 없을 때 세션을 차단하면 사용자가 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되어 사용자 경험에 영향을 줄 수 있습니다. 실패 검사를 구현할지의 여부는 회사의 보안 규정 준수 입장과 비즈니스에 대한 사용자 경험의 중요성, 더 엄격한 보안에 따라 결정됩니다. 또는 더 많은 트래픽을 복호화할 수 있도록 처리 능력이 더 높은 방화벽 모델을 사용하는 것이 좋습니다.

## 비복호화 프로파일

복호화 프로파일 없음(개체 > 복호화 프로파일 > 복호화 없음)은 복호화를 선택하지 않은 트래픽에 대해 서버 확인 검사를 수행합니다. “비복호화" 복호화 정책에 비복호화 프로파일을 첨부하여 복호화에서 제외할 트래픽을 정의합니다. (고정된 인증서 또는 상호 인증과 같은 기술적 이유로 사이트가 복호화를 중단하기 때문에 암호를 복호화할 수 없는 트래픽을 제외하기 위해 정책을 사용하지 마십시오. 대신 암호 복호화 제외 목록에 호스트 이름을 추가합니다. 다음 그림은 복호화 프로파일 설정에 대한 일반적인 모범 사례 권

 ©2023 Palo Alto Networks, Inc.

장 사항을 보여 주지만 사용하는 설정은 회사의 보안 규정 준수 규칙 및 현지 법률 및 규정에 따라 달라집니다.




- 만료된 인증서가 있는 세션 차단 - 이 체크박스를 선택하여 인증서가 만료된 서버가 있는 세션을 차단하고 잠재적으로 안전하지 않은 사이트에 대한 액세스를 방지합니다. 이 체크박스를 선택하지 않으면 사용자는 잠재적으로 악의적인 사이트와 연결하고 거래하고 연결을 시도할 때 경고 메시지를 볼 수 있지만 연결이 방지되지는 않습니다.
- 언트러스티드**(untrusted)** 발급자가 있는 세션 차단 - 이 체크박스를 선택하여 신뢰할 수 없는 인증서 발급자가 있는 서버가 있는 세션을 차단합니다. 언트러스티드(untrusted) 발급자는 중간자 공격, 재전송 공격 또는 기타 공격을 나타낼 수 있습니다.

복호화하지 않는 *TLSv1.3* 트래픽에 대한 복호화 정책에 비복호화 프로파일을 첨부하지 마십시오. 이전 버전과 달리 *TLSv1.3*은 인증서 정보를 암호화하므로 방화벽은 인증서 데이터에 대한 가시성이 없기 때문에 만료된 인증서 또는 언트러스티드*(untrusted)* 발급자가 있는 세션을 차단할 수 없으므로 프로파일에는 아무런 영향을 주지 않습니다. *(*방화벽은 *TLSv1.2*와 함께 인증서 검사를 수행할 수 있으며 이러한 프로토콜은 인증서 정보를 암호화하지 않으며 트래픽에 비복호화 프로파일을 적용해야 하기 때문입니다*.)* 그러나 복호화 정책이 해당 트래픽을 제어하지 않는 한 방화벽이 복호화되지 않은 트래픽을 기록하지 않으므로 복호화하지 않는 *TLSv1.3* 트래픽에 대한 복호화 정책을 만들어야 합니다.

*(TLSv1.2* 이전에도 적용*)* 언트러스티드*(untrusted)* 발급자가 있는 세션을 허용하도록 선택한 다음 만료된 인증서가 있는 세션만 차단하도록 선택한 경우 신뢰할 수 있고 만료된 발급자가 실수로 차단될 수 있는 시나리오가 있습니다. 방화벽의 인증서 저장소에 유효한 자체 서명된 신뢰할 수 있는 *CA*가 포함되어 있고 서버가 인증서 체인에서 만료된 *CA*를 보내면 방화벽이 인증서 저장소를 확인하지 않습니다. 대신 방화벽은 신뢰할 수 있고 유효한 대체 트러스트 앵커를 찾고 신뢰할 수 있는 자체 서명된 인증서를 기반으로 세션을 허용해야 하는 만료된 *CA*를 기반으로 세션을 차단합니다.

이 시나리오를 방지하려면 만료된 인증서가 있는 차단 세션 외에도 신뢰할 수 없는 발급자가 있는 차단 세션을 사용하도록 설정합니다. 이렇게 하면 방화벽이 인증서 저장소를 확인하고 자체 서명된 신뢰할 수 있는 *CA*를 찾고 세션을 허용해야 합니다.


©2023 Palo Alto Networks, Inc.

# ECC(타원 곡선 암호화) 인증서에 대한 SSL 복호화

방화벽은 ECDSA(타원형 곡선 디지털 서명 알고리즘) 인증서를 포함한 ECC 인증서를 사용하여 웹사이트 및 애플리케이션의 SSL 트래픽을 자동으로 복호화합니다. 조직이 강력한 키와 작은 인증서 크기의 혜택을 받기 위해 ECC 인증서를 사용하는 것으로 전환함에 따라 ECC 보안 애플리케이션 및 웹사이트 트래픽에 대한 가시성을 지속적으로 유지하고 안전하게 활성화할 수 있습니다.

***ECC*** 인증서를 사용하는 웹사이트 및 애플리케이션의 복호화는 방화벽에 미러링되는 트래픽에 대해 지원되지 않습니다. ***ECC*** 인증서를 사용하는 암호화된 트래픽이 방화벽을 복호화하려면 방화벽을 직접 통과해야 합니다.

HSM(하드웨어 보안 모듈)을 사용하여 ***ECDSA*** 인증서와 연결된 개인 키를 저장할 수 있습니다. ***TLSv1.3*** 트래픽의 경우 ***PAN-OS***는 ***SSL*** 포워드 프록시에 대해서만 ***HSM***을 지원합니다. ***SSL*** 인바운드 검사용 ***HSM***은 지원하지 않습니다.

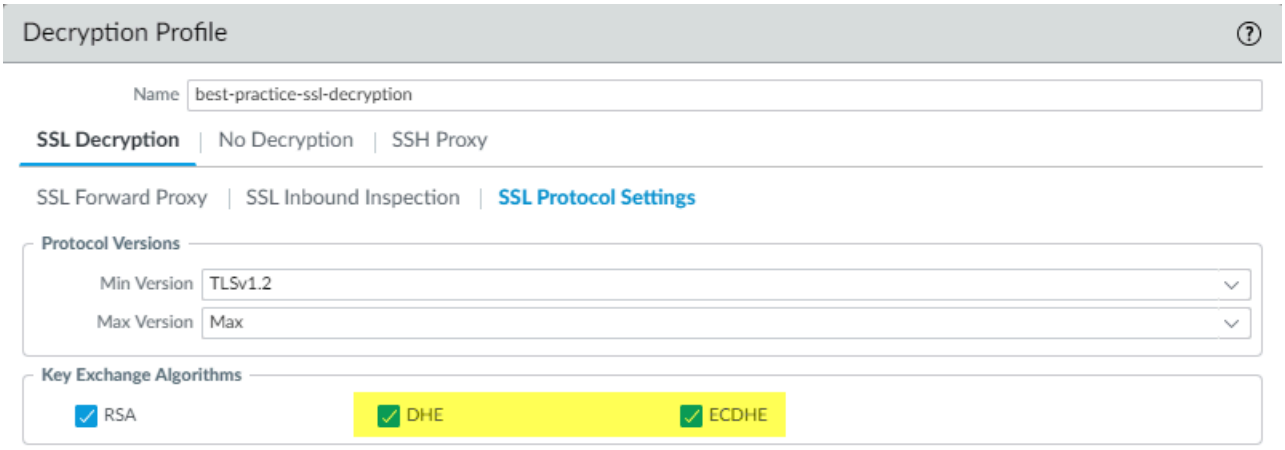
# SSL 복호화를 위한 PFS(완전한 순방향 보안) 지원

PFS는 암호화된 한 세션의 손상이 여러 암호화된 세션의 손상으로 이어지는 것을 방지하는 통신 보안 프로토콜입니다. PFS를 사용하면 서버가 클라이언트와 함께 설정하는 각 보안 세션에 대해 고유한 개인 키를 생성합니다. 서버 개인 키가 손상된 경우 해당 키로 설정된 단일 세션만 취약하므로 서버가 고유하게 생성된 키와 연결된 각 세션을 설정하므로 공격자는 과거 세션과 향후 세션에서 데이터를 검색할 수 없습니다. 방화벽은 PFS 키 교환 알고리즘으로 설정된 SSL 세션을 복호화하고 과거 및 향후 세션에 대한 PFS 보호를 유지합니다.

Diffie-Hellman(DHE)기반 PFS 및 타원형 곡선 Diffie-Hellman(ECDHE) 기반 PFS에 대한 지원은 기본적으로 활성화됩니다(개체 > 복호화 프로파일 > **SSL** 복호화 > **SSL** 프로토콜 설정).

***DHE*** 또는 ***ECDHE*** 키 교환 알고리즘을 사용하여 ***SSL*** 복호화에 대한 ***PFS*** 지원을 사용하는 경우 하드웨어 보안 모듈(HSM)을 사용하여 ***SSL*** 인바운드 검사를 위한 개인 키를 저장할 수 있습니다.

***SSL*** 인바운드 검사를 구성하고 ***PFS*** 암호를 사용하면 세션 재개가 지원되지 않습니다.

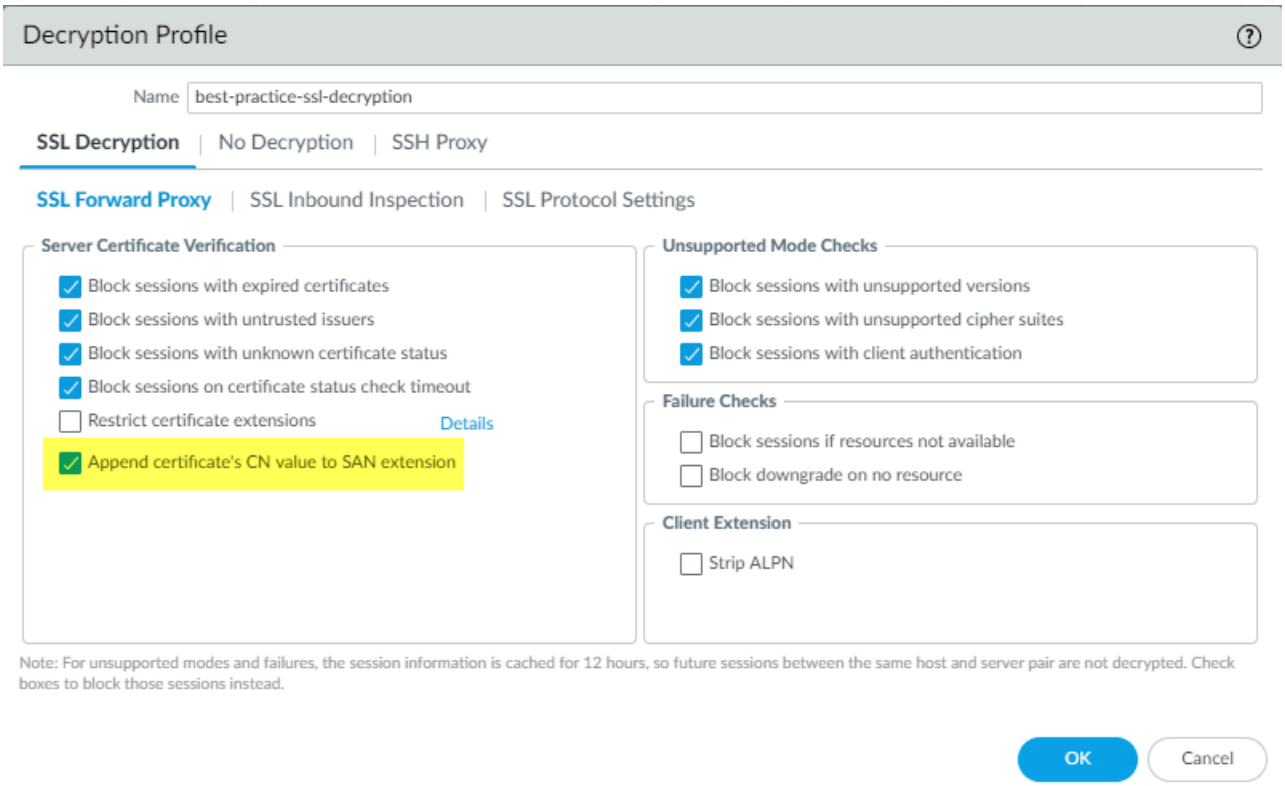



 ©2023 Palo Alto Networks, Inc.

# SSL 복호화 및 주체 대체 이름(SAN)

일부 브라우저에서는 서버 인증서가 SAN(주체 대체 이름)을 사용하여 인증서가 보호하는 도메인을 지정해야 하며 더 이상 서버 인증서 CN(일반 이름)을 기반으로 하는 인증서 일치를 지원하지 않습니다. SAN을 사용하면 단일 서버 인증서가 여러 이름을 보호할 수 있습니다. CN은 SAN보다 미흡하게 정의되어 단일 도메인만 보호하거나 도메인의 모든 첫 번째 수준 하위 도메인을 보호할 수 있습니다. 그러나 서버 인증서에 CN만 포함된 경우 SAN이 필요한 브라우저는 최종 사용자가 요청된 웹 리소스에 연결하는 것을 허용하지 않습니다. 방화벽은 SSL 암호 복호화 중에 자신을 신뢰할 수 있는 타사로 설정하기 위해 생성하는 가장 인증서에 SAN을 추가할 수 있습니다. 서버 인증서에 CN만 포함된 경우 SSL 복호화를 수행하는 방화벽은 서버 인증서 CN을 가상 인증서 SAN에 복사합니다. 방화벽은 SAN과 함께 가장 인증서를 클라이언트에 제공하고 브라우저는 연결을 지원할 수 있습니다. 최종 사용자는 계속해서 필요한 리소스에 액세스할 수 있으며 방화벽은 세션의 암호를 복호화할 수 있습니다.

복호화된 SSL 트래픽에 대한 SAN 지원을 활성화하려면 관련 복호화 정책에 연결된 복호화 프로파일을 업데이트합니다. 개체 > 암호화 프로파일 > **SSL** 복호화 > **SSL** 포워딩 프록시 > 인증서의 **CN** 값을 **SAN** 확장에 추가를 선택합니다.




# TLSv1.3 복호화

TLSv1.3 트래픽에서 알려진 위협과 알려지지 않은 위협을 복호화하고 완전한 가시성을 확보하고 방지할 수 있습니다. TLSv1.3은 애플리케이션 보안 및 성능 개선을 제공하는 TLS 프로토콜의 최신 버전입니다. TLSv1.3 암호 해독을 지원하려면 TLSv1.3이 최소 프로토콜 버전으로 구성되거나 최대 또는 TLSv1.3이 최대 프로토콜 버전으로 구성된 기존 및 새 암호 해독 정책 규칙에 암호 해독 프로파일을 적용해야 합니다. TLSv1.3을 지원하도록 기존 프로파일을 편집할 수 있습니다. 암호 해독 프로파일에서 TLSv1.3 지원을 지정하지 않으면 PAN-OS는 기본적으로 TLSv1.2를 최대 프로토콜 버전으로 지원합니다. 방화벽은 포워


©2023 Palo Alto Networks, Inc.

드 프록시, 인바운드 검사, 복호화된 네트워크 패킷 브로커 트래픽 및 복호화 포트 미러링에 대한 TLSv1.3 복호화를 지원합니다.

TLSv1.3을 사용하려면 클라이언트와 서버가 TLSv1.3 암호를 협상할 수 있어야 합니다. TLSv1.3을 지원하지 않는 웹사이트의 경우 방화벽은 서버가 지원하는 이전 버전의 TLS 프로토콜을 선택합니다.

방화벽은 TLSv1.3에 대해 다음과 같은 복호화 알고리즘을 지원합니다.

- TLS13-AES-128-GCM-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

복호화된 트래픽에 적용하는 복호화 프로파일이 프로토콜의 최대 버전을 **Max**로 지정하는 경우 프로파일은 TLSv1.3을 지원하고 TLSv1.3을 지원하는 사이트에서 TLSv1.3을 자동으로 사용합니다. (TLSv1.3을 지원하기 위해 최대 버전을 **TLSv1.3**으로 설정할 수 있지만, 다음 버전의 TLS가 출시되면 프로파일을 업데이트해야 합니다. 최대 버전을 최대로 설정하면 프로파일이 새로운 TLS 버전이 출시될 때 자동으로 지원하도록 보장합니다.) PAN-OS 10.0으로 업그레이드하면 최대 버전이 최대로 설정된 모든 복호화 프로파일이 **TLSv1.2**로 재설정되어 고정된 인증서를 사용하고 해당 트래픽이 떨어지는 것을 방지하는 모바일 애플리케이션에 대한 자동 지원을 제공합니다.

모든 애플리케이션이 TLSv1.3 프로토콜을 지원하는 것은 아닙니다. 복호화 모범 사례를 따르고 TLS 프로토콜의 최소 버전을 **TLSv1.2**로 설정하고 최대 버전 설정을 최대로 둡니다. 비즈니스 요구 사항에 따라 약한 TLS 프로토콜을 허용해야 하는 경우 약한 프로토콜을 허용하는 최소 버전으로 별도의 SSL 복호화 프로파일을 생성하고 약한 TLS 프로토콜로 허용해야 하는 트래픽을 정의하는 복호화 정책에 연결합니다.

복호화 정책이 고정된 인증서를 사용하는 모바일 애플리케이션을 지원하는 경우 **Max Version**을 **TLSv1.2**로 설정합니다. TLSv1.3은 이전 TLS 버전에서 암호화되지 않은 인증서 정보를 암호화하므로 방화벽은 일부 모바일 애플리케이션에 영향을 미치는 인증서 정보에 따라 복호화 제외를 자동으로 추가할 수 없습니다. 따라서 TLSv1.3을 사용하도록 설정하면 해당 트래픽에 대한 복호화 정책을 만들지 않는 한 방화벽이 일부 모바일 애플리케이션 트래픽이 떨어질 수 있습니다. 비즈니스에 사용하는 모바일 애플리케이션을 알고 있는 경우 다른 모든 트래픽에 대해 TLSv1.3을 활성화할 수 있도록 해당 애플리케이션에 대한 별도의 복호화 정책 및 프로파일을 만드는 것이 좋습니다.



특정 정책이 ***TLSv1.3*** 트래픽만 제어한다는 것을 알고 있는 경우 암호를 복호화하지 않는 ***TLSv1.3*** 트래픽에 대한 복호화 정책에 비복호화 프로파일을 연결하지 마십시오**.** 이전 ***TLS*** 버전에서 변경된 사항은 ***TLSv1.3***이 인증서 정보를 암호화하므로 방화벽이 더 이상 해당 데이터에 대한 가시성을 가지지 않으므로 인증서가 만료되거나 신뢰할 수 없는 발급자가 있는 세션을 차단할 수 없으므로 프로파일이 영향을 받지 않는다는 것입니다**. (**방화벽은 ***TLSv1.2***와 함께 인증서 검사를 수행할 수 있으며 이러한 프로토콜은 인증서 정보를 암호화하지 않으며 트래픽에 비복호화 프로파일을 적용해야 하기 때문입니다**.)** 그러나 복호화 정책에서 성공 및 실패한 ***TLS*** 핸드쉐이크 기록을 활성화하여 모든 유형의 복호화되지 않은 트래픽을 기록할 수 있습니다**(**실패한 ***TLS*** 핸드쉐이크 기록은 기본적으로 활성화됨**).**

SSL 프로토콜 설정 복호화 프로파일에서 지원되지 않는 모드를 허용하면 방화벽이 자동으로 트래픽을 로컬 복호화 제외 캐시에 추가합니다. 방화벽은 여전히 TLSv1.3에서 TLSv1.2로 다운그레이드된 트래픽을 복호화하고 검사하며 캐시에 서버를 추가하기 위해 캐시에 표시된 이유는 TLS13_UNSUPPORTED입니다.

PAN-OS 10.2에서 이전 버전으로 다운그레이드하면 TLSv1.3을 최소 버전 또는 최대 버전으로 지정하는 모든 암호 해독 프로파일이 지원되는 가장 높은 버전으로 변경됩니다. 예를 들어 PAN-OS 10.2에서 PAN-

 ©2023 Palo Alto Networks, Inc.

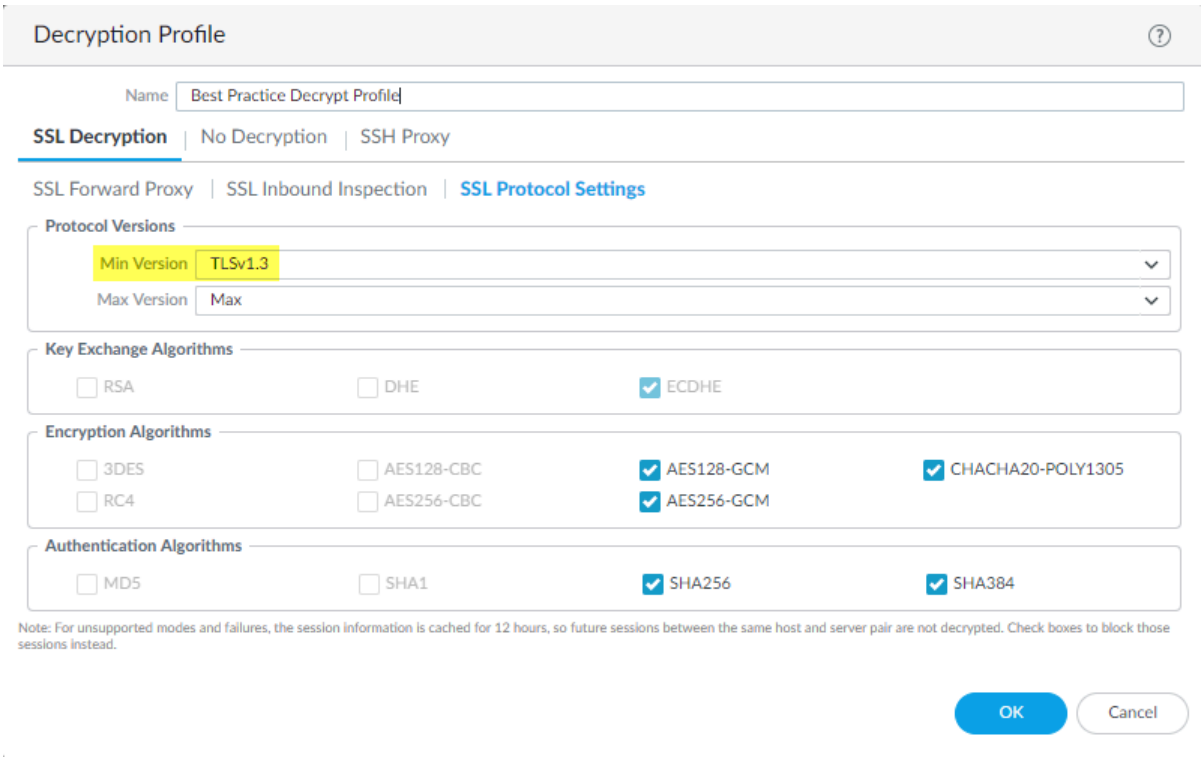
OS 9.1로 다운그레이드하면 TLSv1.3이 TLSv1.2로 바뀝니다. PAN-OS 10.2의 Panorama 디바이스가 이전 버전의 PAN-OS를 실행하는 디바이스에 구성을 푸시하는 경우 TLSv1.3을 최소 버전 또는 최대 버전으로 지정한 모든 복호화 프로파일도 지원되는 가장 높은 버전으로 변경됩니다.

*HSM(*하드웨어 보안 모듈*)*을 사용하는 고객의 경우 *PAN-OS*는 *SSL* 포워딩 프록시에 대해서만 *TLSv1.3*을 지원합니다. *SSL* 인바운드 검사용 *HSM*은 지원하지 않습니다.

가장 엄격한 보안을 달성하기 위해 TLSv1.3을 허용되는 최소 프로토콜 버전으로 설정하는 SSL 복호화 프로파일을 구성할 수 있습니다. 그러나 일부 애플리케이션은 TLSv1.3을 지원하지 않으며 TLSv1.3이 허용되는 최소 프로토콜인 경우 작동하지 않을 수 있습니다. TLSv1.3만 지원하는 애플리케이션 트래픽에만 TLSv1.3을 최소 버전으로 설정하는 프로파일을 적용합니다.

1. 새 SSL 복호화 프로파일을 만들거나 기존 프로파일(**Objects** > **Decryption** > **Decryption** 프로파일)을 편집합니다.

   프로파일이 새 프로파일인 경우 프로파일 이름을 지정합니다.
2. **SSL** 프로토콜 설정을 선택합니다.
3. 최소 버전을 **TLSv1.3**으로 변경합니다.




**Max Version**에 대해 **Max**를 사용하면 프로파일이 제어하는 트래픽이 사용 가능한 가장 강력한 프로토콜 버전을 사용할 수 있습니다. 최소 버전은 트래픽이 사용할 수 있는 프로토콜의 가장 약한 버전을 설정합니다. 최소 버전을 **TLSv1.3**으로 설정하면 트래픽이 TLSv1.3(또는 그 이상)을 사용해야 하고 약한 프로토콜 버전이 차단됩니다. (복호화 정책 규칙은 프로파일이 제어하는 트래픽을 정의합니다.)

TLSv1.3을 최소 버전으로 구성할 때 PFS(Perfect Forward Secrecy)를 사용해야 하며 약한 키 교환, 암호화 및 인증 알고리즘을 사용할 수 없습니다.

4. 설정하거나 변경해야 하는 다른 복호화 프로파일 설정을 구성합니다.


©2023 Palo Alto Networks, Inc.

5. 확인을 클릭하여 프로파일을 저장합니다.
6. 프로파일을 적절한 복호화 정책 규칙에 연결하여 적절한 트래픽에 적용합니다.

## 암호 해독된 세션에 대해 고가용성이 지원되지 않음

장애 조치 후 방화벽은 암호 해독된 SSL 세션에 대해 HA(고가용성) 동기화를 지원하지 않습니다. 방화벽은 암호 해독된 SSL 전달 프록시, SSL 인바운드 검사 또는 SSH 프록시 세션을 다시 시작하지 않습니다. 방화벽은 복호화 정책에 따라 페일오버 후에 시작하는 새 세션을 해독합니다.

## 복호화 미러링

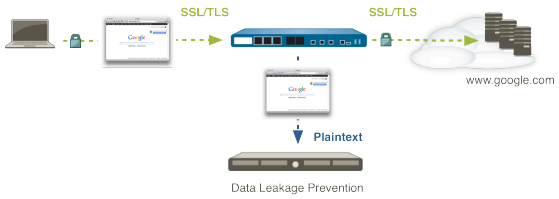
복호화 미러링은 방화벽에서 복호화된 트래픽의 복사본을 만들어 보관 및 분석을 위해 원시 패킷 캡처를 수신할 수 있는 NetWitness 또는 Solera와 같은 트래픽 수집 도구로 보냅니다. 포렌식 및 기록 목적 또는 데이터 유출 방지(DLP)를 위해 포괄적인 데이터 캡처가 필요한 조직은 이 기능을 활성화하기 위해 무료 라이선스를 설치할 수 있습니다.

라이선스를 설치한 후 트래픽 수집 도구를 방화벽의 이더넷 인터페이스에 직접 연결하고 **Interface Type**을 **Decrypt Mirror**로 설정하십시오. 방화벽은 수집 도구를 사용하여 TCP 핸드쉐이크를 시뮬레이션한 다음 복호화된(일반 텍스트로) 해당 인터페이스를 통해 모든 데이터 패킷을 보냅니다.

공용 클라우드 플랫폼*(AWS, Azure, Google Cloud Platform)* 및 *VMware NSX*용 *VM* 시리즈에서는 복호화 포트 미러링을 사용할 수 없습니다.

SSL 트래픽의 복호화, 저장, 검사 및/또는 사용은 특정 국가에서 관리되며 복호화 미러 기능을 사용하려면 사용자 동의가 필요할 수 있습니다. 또한 이 기능을 사용하면 방화벽에 대한 관리 액세스 권한이 있는 악의적인 사용자가 암호화된 채널을 사용하여 제출된 사용자 이름, 암호, 주민등록 번호, 신용카드 번호 또는 기타 중요한 정보를 수집할 수 있습니다. Palo Alto Networks는 프로덕션 환경에서 이 기능을 활성화하고 사용하기 전에 기업 변호사와 상의할 것을 권장합니다.

다음 그래픽은 복호화된 트래픽을 미러링하는 프로세스를 보여주며 복호화 포트 미러링 구성 섹션에서는 이 기능에 라이선스를 부여하고 활성화하는 방법을 설명합니다.




 ©2023 Palo Alto Networks, Inc.

# 복호화 배포 준비

복호화를 배포하는 데 가장 시간이 많이 걸리는 부분은 암호 해독 정책 및 프로필을 구성하는 것이 아니라 이해 관계자와 협력하여 해독할 트래픽과 해독하지 않을 트래픽을 결정하고 웹 사이트 액세스 변경 사항, 개인 키 인프라(PKI) 전략 개발 및 단계적 우선 순위 출시 계획에 대해 사용자 집단을 교육함으로써 배포를 준비하는 것입니다.

복호화 목표를 설정하고 복호화 계획 모범 사례 체크리스트를 검토하여 권장되는 모범 사례를 이해했는지 확인하십시오. 모범 사례 목표는 방화벽 리소스가 허용하는 만큼의 트래픽을 복호화하고 가장 중요한 트래픽을 먼저 복호화하는 것입니다.



복호화 정책 규칙을 생성하고 배포하기 전에 포트 기반에서 애플리케이션 기반 보안 정책 규칙으로 마이그레이션합니다. 포트 기반 보안 정책을 기반으로 복호화 규칙을 만든 다음 애플리케이션 기반 보안 정책으로 마이그레이션하는 경우 보안 정책 규칙이 애플리케이션 트래픽을 방지하기 위해 애플리케이션 기본 포트를 사용할 가능성이 높기 때문에 비표준 포트를 사용하여 복호화 규칙이 허용하려는 트래픽을 차단할 수 있습니다.. 예를 들어 웹 검색 애플리케이션 트래픽(기본 포트 *80*)으로 식별된 트래픽에는 *HTTPS* 트래픽(기본 포트 *443*)과 같이 다른 기본 포트가 있는 기본 애플리케이션이 있을 수 있습니다. 애플리케이션 기본 규칙은 "비표준" 포트(*80*이 아닌 *443*)를 사용하여 복호화된 트래픽을 확인하므로 *HTTPS* 트래픽을 차단합니다. 복호화를 배포하기 전에 *App-ID* 기반 규칙으로 마이그레이션하면 *POC*에서 복호화 배포를 테스트할 때 보안 정책 구성이 잘못되어 일반 사용자로 롤아웃하기 전에 이를 수정하게 됩니다.

복호화 배포를 준비하려면 다음과 같이 하십시오.

- 이해 관계자와 협력하여 복호화 배포 전략 개발
- PKI 롤아웃 계획 개발
- 복호화 방화벽 배포 크기 조정
- 단계적으로 우선 순위가 지정된 배포 계획

## 이해 관계자와 협력하여 복호화 배포 전략 개발

법률, 재무, HR, 임원, 보안 및 IT/지원과 같은 이해 관계자와 협력하여 복호화 배포 전략을 개발합니다. 회사를 보호하기 위해 트래픽을 복호화하는 데 필요한 승인을 받는 것부터 시작하십시오. 트래픽 복호화에는 법적 규정과 비즈니스 요구 사항이 복호화할 수 있는 것과 복호화할 수 없는 것에 미치는 영향을 이해하는 것이 포함됩니다.

복호화하려는 트래픽을 식별하고 우선 순위를 지정합니다. 가장 좋은 방법은 최대한 많은 트래픽을 복호화하여 암호화된 트래픽의 잠재적 위협에 대한 가시성을 확보하고 이러한 위협을 방지하는 것입니다. 잘못된 방화벽 크기 조정으로 인해 암호를 복호화하려는 모든 트래픽의 암호를 복호화할 수 없는 경우 가장 중요한 서버, 가장 위험한 트래픽 카테고리, 신뢰도가 다소 낮은 세그먼트 및 IP 서브넷의 우선 순위를 지정하십시오. 우선 순위를 정하는 데 도움이 되도록 "이 서버가 손상되면 어떻게 됩니까?"와 같은 질문을 스스로에게 하십시오. 및 "내가 달성하고자 하는 성과 수준과 관련하여 얼마나 많은 위험을 감수할 의향이 있습니까?"

다음으로 고정된 인증서, 불완전한 인증서 체인, 지원되지 않는 암호 또는 상호 인증과 같은 기술적인 이유로 트래픽이 복호화를 중단하기 때문에 암호를 복호화할 수 없는 트래픽을 식별합니다. 기술적으로 복호

 ©2023 Palo Alto Networks, Inc.

화를 방해하는 사이트를 복호화하면 해당 트래픽이 차단됩니다. 기술적으로 복호화를 방해하는 웹사이트를 평가하고 비즈니스상의 이유로 해당 사이트에 액세스해야 하는지 자문해 보십시오. 해당 사이트에 대한 액세스가 필요하지 않은 경우 복호화를 허용하여 해당 사이트를 차단합니다. 비즈니스 목적으로 이러한 사이트에 액세스해야 하는 경우 해당 사이트를 SSL 복호화 제외 목록에 추가하여 복호화에서 제외하십시오. SSL 복호화 제외 목록은 기술적으로 복호화를 중단한 사이트 전용입니다.

재정, 건강 또는 정부 트래픽이나 특정 경영진의 트래픽과 같이 법적, 규제적, 개인적 또는 기타 이유로 복호화하지 않기로 선택한 민감한 트래픽을 식별합니다. 이것은 기술적으로 복호화를 중단시키는 트래픽이 아니므로 SSL 복호화 제외 목록을 사용하여 이 트래픽을 복호화에서 제외하지 마십시오. 대신 정책 기반 복호화 제외를 생성하여 암호를 복호화하지 않기로 선택한 트래픽을 식별하고 제어하고 비복호화 - 복호화 프로파일을 정책에 적용하여 인증서 문제가 있는 서버가 네트워크에 액세스하지 못하도록 합니다. 정책 기반 복호화 제외는 복호화를 선택하지 않은 트래픽에만 적용됩니다.

복호화 정책을 계획할 때 회사의 보안 준수 규칙, 컴퓨터 사용 정책 및 비즈니스 목표를 고려하십시오. 매우 엄격한 제어는 사용자가 액세스하는 데 사용했던 비업무 사이트에 대한 액세스를 차단하여 사용자 경험에 영향을 줄 수 있지만 정부 또는 금융 기관의 경우 필요할 수 있습니다. 사용성, 관리 오버헤드 및 보안 간에는 항상 절충점이 있습니다. 복호화 정책이 엄격할수록 웹사이트에 연결할 수 없게 되어 사용자 불만이 발생하고 규칙 베이스가 수정될 가능성이 높아집니다.



엄격한 복호화 정책으로 인해 처음에는 몇 가지 사용자 불만이 발생할 수 있지만 이러한 불만은 취약한 알고리즘을 사용하거나 인증서 문제가 있기 때문에 차단된 승인되지 않았거나 바람직하지 않은 웹사이트에 주의를 끌 수 있습니다. 불만 사항을 네트워크의 트래픽을 더 잘 이해하기 위한 도구로 사용하십시오.

사용자 그룹 및 개별 사용자에 따라 다른 복호화 정책이 필요할 수도 있고 모든 사용자에게 동일한 복호화 정책을 적용할 수도 있습니다. 예를 들어, 임원은 다른 직원에게 적용되는 복호화 정책에서 면제될 수 있습니다. 직원 그룹, 계약, 파트너 및 게스트에 다른 복호화 정책을 적용할 수도 있습니다. 모든 직원, 계약자, 파트너, 게스트 및 기타 네트워크 사용자에게 배포할 업데이트된 법률 및 HR 컴퓨터 사용 정책을 준비하여 복호화를 배포할 때 사용자가 자신의 데이터를 복호화하고 위협을 검색할 수 있다는 것을 이해하도록 합니다.



게스트 사용자를 처리하는 방법은 필요한 액세스 권한에 따라 다릅니다. 게스트를 별도의 ***VLAN***과 무선 액세스를 위한 별도의 ***SSID***에 배치하여 나머지 네트워크로부터 게스트를 격리합니다. 게스트가 회사 네트워크에 액세스할 필요가 없는 경우 허용하지 마십시오. 그러면 트래픽을 복호화할 필요가 없습니다. 게스트가 회사 네트워크에 액세스해야 하는 경우 트래픽을 복호화합니다.

- 기업은 게스트 디바이스를 제어하지 않습니다. 게스트 트래픽을 복호화하고 게스트 보안 정책에 따라 방화벽이 트래픽을 검사하고 위협을 방지할 수 있도록 합니다. 이렇게 하려면 인증 포털을 통해 게스트 사용자를 리디렉션하고 ***CA*** 인증서를 다운로드 및 설치하는 방법을 지시하고 트래픽이 복호화될 것임을 게스트에게 명확하게 알립니다. 회사의 개인 정보 및 컴퓨터 사용 정책에 프로세스를 포함하십시오.
- 게스트가 액세스해야 하는 네트워크 영역에만 액세스할 수 있도록 게스트 액세스를 엄격하게 제어하는 별도의 복호화 정책 규칙 및 보안 정책 규칙을 만듭니다.

다른 사용자 그룹과 마찬가지로 암호를 복호화할 디바이스와 암호를 복호화할 애플리케이션을 결정합니다. 오늘날의 네트워크는 기업 디바이스뿐만 아니라 BYOD, 모바일, 원격 사용자 및 계약자, 파트너 및 게

 ©2023 Palo Alto Networks, Inc.

스트 디바이스를 포함한 기타 디바이스를 지원합니다. 오늘날의 사용자는 승인된 사이트와 승인되지 않은 사이트 모두에 액세스하려고 시도하며 해당 트래픽 중 암호를 복호화할 양을 결정해야 합니다.



기업은 ***BYOD*** 디바이스를 제어하지 않습니다. 네트워크에서 ***BYOD*** 디바이스를 허용하는 경우 트래픽을 복호화하고 다른 네트워크 트래픽에 적용하는 것과 동일한 보안 정책을 적용하여 방화벽이 트래픽을 검사하고 위협을 방지할 수 있도록 합니다. 이렇게 하려면 인증 포털을 통해 ***BYOD*** 사용자를 리디렉션하고 ***CA*** 인증서를 다운로드 및 설치하는 방법을 지시하고 트래픽이 복호화될 것임을 사용자에게 명확하게 알립니다. ***BYOD*** 사용자에게 프로세스에 대해 교육하고 이를 회사의 개인 정보 및 컴퓨터 사용 정책에 포함합니다.

기록할 트래픽을 결정하고 기록할 수 있는 트래픽을 검토하십시오. 기록하고 저장할 수 있는 데이터 유형과 데이터를 기록하고 저장할 수 있는 위치에 관한 현지 법률을 숙지하십시오. 예를 들어, 현지 법률에 따라 건강 및 금융 데이터와 같은 개인 정보의 로깅 및 저장이 금지될 수 있습니다.

잘못된 인증서를 처리하는 방법을 결정합니다. 예를 들어, 인증서 상태를 알 수 없는 세션을 차단하거나 허용하시겠습니까? 잘못된 인증서를 처리하는 방법을 이해하면 서버 인증서 확인 상태를 기반으로 허용하는 세션을 제어하기 위해 복호화 정책에 연결하는 복호화 프로파일을 구성하는 방법이 결정됩니다.

## PKI 롤아웃 계획 개발

공개 키 인프라(PKI)를 배포하는 방법을 계획합니다. 네트워크 디바이스에는 신뢰할 수 있는 사이트에 대한 SSL Forward Trust CA 인증서와 신뢰할 수 없는 사이트에 대한 SSL Forward Untrust CA 인증서가 필요합니다. 별도의 포워드 트러스트 및 포워드 언트러스트 인증서를 생성합니다(언트러스트 인증서가 사용자에게 잠재적으로 안전하지 않은 사이트에 액세스하려고 시도하고 있음을 경고하도록 하려면 엔터프라이즈 루트 CA를 사용하여 포워드 언트러스트 인증서에 서명하지 마십시오.) Palo Alto Networks 차세대 방화벽에는 SSL 복호화를 위한 CA 인증서를 생성하는 두 가지 방법이 있습니다.

- **Enterprise Root CA**에서 하위 인증서로 **SSL CA** 인증서 생성 - 기존 Enterprise PKI가 있는 경우 이것이 모범 사례입니다. 엔터프라이즈 루트 CA에서 하위 인증서를 생성하면 네트워크 디바이스가 이미 엔터프라이즈 루트 CA를 신뢰하므로 배포 단계를 시작할 때 인증서 문제를 피할 수 있으므로 롤아웃이 더 쉽고 원활해집니다. 엔터프라이즈 루트 CA가 없으면 하나 가져오는 것이 좋습니다.
- 방화벽에서 자체 서명된 루트 **CA** 인증서를 생성하고 해당 방화벽에서 하위 **CA** 인증서를 생성합니다. 엔터프라이즈 루트 CA가 없는 경우 이 방법은 자체 서명된 루트 CA 인증서와 하위 순방향 트러스트 및 언트러스트 CA 인증서를 제공합니다. 이 방법을 사용하면 해당 디바이스가 방화벽의 자체 서명된 인증서를 인식할 수 있도록 모든 네트워크 디바이스에 자체 서명된 인증서를 설치해야 합니다. 인증서를 모든 디바이스에 배포해야 하므로 이 메서드는 대규모 배포보다 작은 배포 및 개념 증명(POC) 평가판에 더 적합합니다.



네트워크 디바이스의 인증서 신뢰 목록에 위임되지 않는 인증서를 내보내지 마십시오***!*** 트러스트 목록에 언트러스트 인증서를 설치하면 방화벽이 신뢰할 수 없는 웹사이트를 신뢰하는 디바이스가 생성되므로 매우 중요합니다. 또한 사용자는 신뢰할 수 없는 사이트에 대한 인증서 경고가 표시되지 않으므로 사이트가 신뢰할 수 없다는 것을 알지 못하고 해당 사이트에 액세스할 수 있으므로 네트워크가 위협에 노출될 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

엔터프라이즈 루트 *CA*에서 *Forward Trust* 인증서를 생성하든 방화벽에서 생성된 자체 서명 인증서를 사용하든 각 방화벽에 대해 별도의 하위 종속 상태 트러스트 *CA* 인증서를 생성합니다. 별도의 하위 *CA*를 사용하면 배포의 나머지 부분에 영향을 주지 않고 디바이스(또는 디바이스 쌍)를 해제할 때 하나의 인증서를 해지할 수 있으며 인증서를 해지해야 하는 모든 상황에서 영향을 줄일 수 있습니다. 각 방화벽의 별도 *Forward Trust CA*는 사용자가 보는 *CA* 오류 메시지에 트래픽이 횡단하는 방화벽에 대한 정보가 포함되어 있으므로 문제를 해결하는 데도 도움이 됩니다. 모든 방화벽에서 동일한 *Forward Trust CA*를 사용하는 경우 해당 정보의 세분성을 잃게 됩니다.

서로 다른 방화벽에서 서로 다른 포워드 언트러스트 인증서를 사용하면 이점이 없으므로 모든 방화벽에서 동일한 포워드 언트러스트 인증서를 사용할 수 있습니다. 개인 키에 대한 추가 보안이 필요한 경우 HSM에 저장하는 것이 좋습니다.

게스트 사용자를 위해 특별한 편의를 제공해야 할 수도 있습니다. 게스트 사용자가 회사 네트워크에 액세스할 필요가 없는 경우 액세스를 허용하지 않으면 트래픽을 복호화하거나 게스트 액세스를 지원하기 위한 인프라를 만들 필요가 없습니다. 게스트 사용자를 지원해야 하는 경우 법무 부서와 게스트 트래픽의 암호를 복호화할 수 있는지 논의하십시오.

게스트 트래픽을 복호화할 수 있는 경우 BYOD 디바이스를 취급하는 방식과 유사하게 게스트를 취급하십시오. 게스트 트래픽을 복호화하고 다른 네트워크 트래픽에 적용하는 것과 동일한 보안 정책을 적용합니다. 인증 포털을 통해 게스트 사용자를 리디렉션하여 이를 수행하고 CA 인증서를 다운로드 및 설치하는 방법을 지시하고 트래픽이 복호화될 것임을 사용자에게 명확하게 알립니다. 회사의 개인 정보 및 컴퓨터 사용 정책에 프로세스를 포함하십시오. 또한 게스트가 액세스해야 하는 영역으로만 게스트 트래픽을 제한합니다.

법적 이유로 게스트 트래픽의 암호를 복호화할 수 없는 경우 게스트 트래픽을 독립 운영하고 네트워크에서 측면으로 이동하는 것을 방지합니다.

- 게스트를 위한 별도의 영역을 생성하고 해당 영역에 대한 게스트 액세스를 제한합니다. 측면 이동을 방지하기 위해 게스트가 다른 구역에 접근하는 것을 허용하지 마십시오.
- 승인된 애플리케이션만 허용하고 URL 필터링을 사용하여 위험한 URL 카테고리에 대한 액세스를 방지하고 모범 사례 보안 프로파일을 적용합니다.
- 게스트가 알 수 없거나 만료된 CA가 있는 웹사이트에 액세스하지 못하도록 하려면 비복호화 정책 및 프로파일을 적용합니다.

모든 직원, 계약자, 파트너 및 기타 사용자는 일반적인 회사 인프라를 사용해야 하며 트래픽을 복호화하고 검증해야 합니다.

## 복호화 방화벽 배포 크기 조정

암호화된 트래픽의 암호를 복호화하면 방화벽 CPU 리소스가 소모되고 처리량에 영향을 줄 수 있습니다. 일반적으로 보안이 강화될수록(암호화하는 SSL 트래픽이 많을수록 프로토콜 설정이 더 엄격해짐) 복호화에 더 많은 방화벽 리소스가 사용됩니다. Palo Alto Networks SE/CE와 협력하여 방화벽 배포 규모를 조정하고 크기 조정 실수를 방지하십시오. 복호화 리소스 소비에 영향을 미치므로 방화벽이 복호화할 수 있는 트래픽의 양에는 다음이 포함됩니다.

- 암호를 복호화하려는 SSL 트래픽의 양입니다. 이것은 네트워크마다 다릅니다. 예를 들어, 일부 애플리케이션은 네트워크에 멀웨어 또는 악용이 삽입되거나 무단 데이터 전송을 방지하기 위해 암호를 복호화해야 하고, 일부 애플리케이션은 현지 법률 및 규정 또는 비즈니스 이유로 암호를 복호화할 수 없으


©2023 Palo Alto Networks, Inc.

며, 다른 애플리케이션은 일반 텍스트(암호화되지 않음)이며 복호화할 필요가 없습니다. 복호화하려는 트래픽이 많을수록 더 많은 리소스가 필요합니다.

- TLS 프로토콜 버전입니다. 더 높은 버전은 더 안전하지만 더 많은 리소스를 소비합니다. 보안을 최대화하려면 가능한 가장 높은 TLS 프로토콜 버전을 사용하십시오.
- 키 크기입니다. 키 크기가 클수록 보안이 향상되지만 키 처리에 더 많은 리소스가 사용됩니다.
- 키 교환 알고리즘. DHE(Diffie-Hellman Ephemeral) ECDHE(Elliptic-Curve Diffie-Hellman Exchange)와 같은 PFS(Perfect Forward Secrecy) 임시 키 교환 알고리즘은 RSA(Rivest-Shamir-Adleman) 알고리즘보다 처리 리소스를 더 많이 사용합니다. PFS 키 교환 알고리즘은 방화벽이 각 세션에 대해 새 암호 키를 생성해야 하기 때문에 RSA 키 교환 알고리즘보다 더 강력한 보안을 제공하지만 새 키를 생성하면 더 많은 방화벽 리소스가 소모됩니다. 그러나 공격자가 세션 키를 손상시키는 경우 PFS는 공격자가 이 키를 사용하여 동일한 클라이언트와 서버 간의 다른 세션을 복호화하는 것을 방지하지만 RSA는 그렇지 않습니다.
- 암호화 알고리즘. 키 교환 알고리즘은 암호화 알고리즘이 PFS인지 RSA인지를 결정합니다.
- 인증서 인증 방법입니다. RSA (RSA 키 교환 알고리즘이 아님)는 타원 곡선 디지털 서명 알고리즘(ECDSA)보다 적은 리소스를 소비하지만 ECDSA는 더 안전합니다.

  키 교환 알고리즘과 인증서 인증 방법의 조합은 ***RSA*** 및 ***ECDSA*** 벤치마크 테스트에 표시된 처리량 성능에 영향을 줍니다. ***PFS***의 성능 비용은 ***PFS***가 달성하는 더 높은 보안과 상쇄되지만 모든 유형의 트래픽에 ***PFS***가 필요한 것은 아닙니다. 암호를 복호화하고 위협을 검사하지만 민감하지 않은 트래픽에 대해 ***RSA***를 사용하여 방화벽 ***CPU*** 주기를 절약할 수 있습니다.

- 평균 트랜잭션 크기. 예를 들어 평균 트랜잭션 크기가 작을수록 복호화에 더 많은 처리 능력이 소모됩니다. 모든 트래픽의 평균 트랜잭션 크기를 측정한 다음 포트 443(HTTPS 암호화 트래픽의 기본 포트)에서 트래픽의 평균 트랜잭션 크기를 측정하여 전체 트래픽 및 평균 트랜잭션 크기와 관련하여 방화벽으로 가는 암호화된 트래픽의 비율을 파악합니다. 평균 트랜잭션 크기를 보다 정확하게 측정하려면 비정상적으로 큰 트랜잭션과 같은 비정상적인 이상값을 제거하십시오.
- 방화벽 모델 및 리소스. 최신 방화벽 모델은 이전 모델보다 처리 능력이 더 뛰어납니다.

이러한 요소의 조합은 복호화가 방화벽 처리 리소스를 사용하는 방식을 결정합니다. 방화벽의 리소스를 최대한 활용하려면 보호하는 데이터의 위험을 이해하십시오. 방화벽 리소스가 문제인 경우 우선 순위가 높은 트래픽에 대해 더 강력한 복호화를 사용하고 사용 가능한 리소스를 늘릴 수 있을 때까지 프로세서를 덜 사용하는 복호화를 사용하여 우선 순위가 낮은 트래픽을 복호화하고 검사합니다. 예를 들어 민감하지 않거나 우선 순위가 높지 않은 트래픽에 대해 ECDHE 및 ECDSA 대신 RSA를 사용하여 우선 순위가 높고 민감한 트래픽에 PFS 기반 복호화를 사용하기 위해 방화벽 리소스를 보존할 수 있습니다. (여전히 우선 순위가 낮은 트래픽을 복호화하고 검사하고 있지만 PFS만큼 안전하지 않은 알고리즘을 사용하여 더 적은 계산 리소스를 소비하는 것과 상충합니다.) 핵심은 다양한 트래픽 유형의 위험을 이해하고 그에 따라 처리하는 것입니다.

현재 사용 가능한 리소스를 이해할 수 있도록 방화벽 성능을 측정하면 복호화하려는 트래픽을 복호화하기 위해 더 많은 방화벽 리소스가 필요한지의 여부를 이해하는 데 도움이 됩니다. 방화벽 성능을 측정하면 복호화를 제공한 후 성능 비교를 위한 기준도 설정됩니다.

방화벽 배포의 규모를 결정할 때는 현재 요구 사항뿐만 아니라 미래의 요구 사항도 기반으로 하십시오. Gartner는 2019년까지 기업 웹 트래픽의 80% 이상이 암호화되고 새로운 악성 코드 캠페인의 50% 이상이 다양한 형태의 암호화를 사용할 것으로 예측하기 때문에 복호화 트래픽의 증가에 대한 헤드룸을 포함

 ©2023 Palo Alto Networks, Inc.

합니다. Palo Alto Networks 담당자와 협력하고 방화벽 크기 조정 경험을 활용하여 방화벽 복호화 제공 크기를 조정하십시오.

## 단계적으로 우선 순위가 지정된 배포 계획

제어된 방식으로 복호화를 하나씩 롤아웃(roll out)할 계획입니다. 한 번에 전체 복호화 배포를 롤아웃하지 마십시오. 복호화가 계획대로 작동하고 사용자가 무엇을 하고 있는지, 그 이유를 이해해야 하는지 테스트하고 확인합니다. 이러한 방식으로 복호화를 롤아웃하면 예상대로 작동하지 않고 사용자가 변경 사항에 적응하는 데 도움이 되는 경우에 문제를 쉽게 해결할 수 있습니다.

복호화 설정으로 인해 일부 웹사이트에 액세스하는 기능이 변경될 수 있으므로 이해 관계자, 직원 및 계약자 및 파트너와 같은 다른 사용자를 교육하는 것이 중요합니다. 사용자는 이전에 접속할 수 있었던 웹사이트에 접속할 수 없게 된 상황에 어떻게 대응하고 기술 지원을 제공할 정보가 무엇인지 이해해야 합니다. 지원팀은 문제가 발생한 사용자를 도울 때와 방법을 롤아웃하는 항목과 방법을 이해해야 합니다. 일반 인구에 대한 복호화를 출시하기 전:

- 얼리 어답터(early adopter)를 식별하여 복호화를 돕고 전체 롤아웃 중에 질문이 있는 다른 직원을 도울 수 있는 사람을 식별합니다. 부서 관리자의 도움을 받아 트래픽 복호화의 이점을 이해할 수 있도록 도와줍니다.
- 트래픽 복호화가 중요한 이유를 이해하는 얼리 어답터 및 기타 직원과 함께 각 부서에서 개념 증명(POC) 시험을 설정합니다. POC 참가자에게 문제가 발생하면 변경 사항및 기술 지원팀에 문의하는 방법을 교육합니다. 이러한 방식으로 복호화 POC는 POC에 대한 기술 지원과 협력하여 복호화를 지원하는 방법과 일반 롤아웃을 지원하는 가장 손쉬운 방법을 개발할 수 있는 기회가 됩니다. POC 사용자와 기술 지원 간의 상호 작용을 통해 정책과 사용자와 통신하는 방법도 세부적으로 조정할 수 있습니다.

  POC를 사용하면 먼저 복호화할 내용의 우선 순위를 지정하여 일반 모집단에서 복호화를 단계적으로 수행할 때 POC 환경을 사용하면 다른 URL 카테고리를 복호화하는 단계를 이해하는 데 도움이 됩니다. 복호화가 방화벽 CPU 및 메모리 사용률에 영향을 미치는 방식을 측정하여 방화벽 크기 조정이 올바른지 또는 업그레이드해야 하는지 파악합니다. POC는 또한 기술적으로 암호 해독을 중단하는 응용 프로그램을 공개 할 수 있으며 (암호 해독하면 트래픽이 차단됨) 암호 해독 제외 목록에 추가해야합니다.

  POC를 설정할 때 일반 롤아웃 전에 운영 준비 및 절차를 인증할 수 있는 사용자 그룹도 설정합니다.
- 일반 롤아웃 전에 사용자 집단을 교육하고 가입할 때 신규 사용자를 교육할 계획입니다. 배포는 이전에 방문했지만 안전하지 않은 웹사이트에 영향을 줄 수 있으므로 이러한 사이트에 더 이상 연결할 수 없기 때문에 복호화를 배포하는 중요한 단계입니다. POC 환경은 의사 소통에 가장 중요한 지점을 식별하는 데 도움이 됩니다.
- 복호화 단계. 이 여러 가지 방법을 수행할 수 있습니다. 우선 순위가 가장 높은 트래픽(예: 게임과 같은 악의적인 트래픽이 발생할 가능성이 가장 높은 URL 카테고리)을 복호화한 다음 경험을 쌓을수록 더 많은 암호를 복호화할 수 있습니다. 또는 보다 보수적인 접근 방식을 취하고 비즈니스에 먼저 영향을 미치지 않는 URL 카테고리를 복호화할 수 있습니다(문제가 발생해도 비즈니스에 영향을 미치지 않습니다). 모든 경우에 복호화를 단계적으로 하는 가장 좋은 방법은 몇 가지 URL 카테고리를 복호화하고, 사용자 피드백을 고려하고, 보고서를 실행하여 복호화가 예상대로 작동하는지 확인한 다음, 몇 가지 URL

 ©2023 Palo Alto Networks, Inc.

카테고리를 점진적으로 복호화하고 확인하는 것입니다. 기술적인 이유로 사이트를 복호화할 수 없거나 복호화하지 않기로 선택한 경우 사이트를 복호화에서 제외하려면 복호화 제외를 계획하십시오.

사용자가 SSL을 선택 해제할 수 있도록 하는 경우 복호화(사용자는 사이트로 이동하지 않고 복호화를 선택 해제하고 세션을 종료하거나 사이트로 이동하여 트래픽 복호화에 동의하는 응답 페이지를 보고 그것이 무엇인지에 대해 교육합니다. 그들이 그것을 보는 이유와 그들의 선택권은 무엇입니까?

- 롤아웃의 각 단계를 평가할 시간을 허용하는 실질적인 배포 일정을 생성합니다.



방화벽을 우회하기 때문에 암호화된 트래픽이 실수로 네트워크에 액세스하지 않도록 모든 네트워크 트래픽을 볼 수 있는 위치에 방화벽을 배치합니다.


©2023 Palo Alto Networks, Inc.

# 해독할 트래픽 정의

복호화 정책 규칙을 사용하면 방화벽에서 복호화할 트래픽을 정의하고 트래픽이 개인적이거나 현지 규정 등으로 인해 복호화에서 제외하도록 선택하는 트래픽을 정의할 수 있습니다.

각 복호화 정책 규칙에 복호화 프로파일을 연결하여 프로파일에 따라 인증서 검사, 세션 모드 확인, 실패 확인, 프로토콜 및 알고리즘 검사를 사용하도록 설정합니다. 이러한 검사는 신뢰할 수 없는 인증서 발급자와의 세션, 취약한 프로토콜, 암호 및 알고리즘, 인증서 문제가 있는 서버와 같은 위험한 연결을 방지합니다.



복호화 배포 모범 사례 검사 목록을 검토하여 권장되는 모범 사례를 이해했는지 확인합니다.

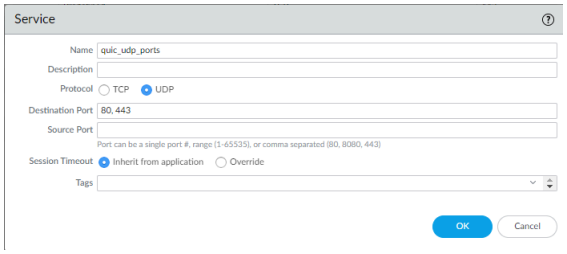
멀웨어, 피싱, 동적 DNS, 알 수 없음, 명령 및 제어, 프록시 회피 및 익명화, 저작권 침해, 극단주의, 새로 등록된 도메인, 그레이웨어 및 파킹과 같은 알려진 위험한 URL 필터링 카테고리를 차단합니다. 비즈니스 이유로 이러한 카테고리 중 하나를 허용해야 하는 경우 암호를 복호화하고 트래픽에 엄격한 보안 프로파일을 적용합니다.

허용할 경우 항상 복호화해야 하는 URL 카테고리에는 온라인 저장소 및 백업, 웹 기반 이메일, 웹 호스팅, 개인 사이트 및 블로그, 콘텐츠 전송 네트워크가 포함됩니다.

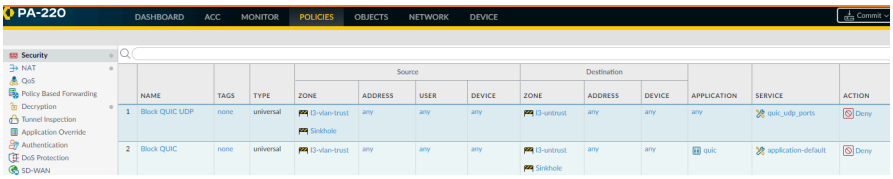

©2023 Palo Alto Networks, Inc.

비즈니스상의 이유로 암호화된 브라우저 트래픽을 허용하려는 경우가 아니면 보안 정책에서 *QUIC(*빠른 *UDP* 인터넷 연결*)* 프로토콜을 차단합니다. *Chrome*과 일부 다른 브라우저는 *TLS* 대신 *QUIC*을 사용하여 세션을 설정하지만 *QUIC*은 방화벽이 복호화할 수 없는 독점 암호화를 사용하므로 잠재적으로 위험한 트래픽이 암호화된 트래픽으로 네트워크에 유입될 수 있습니다. *QUIC*을 차단하면 브라우저가 *TLS*로 폴백되고 방화벽이 트래픽을 복호화할 수 있습니다.

*UDP* 서비스 포트*(80* 및 *443)* 에서 *QUIC*을 차단하는 보안 정책 규칙을 생성하고 *QUIC* 애플리케이션을 차단하는 별도의 규칙을 생성합니다. *UDP* 포트 *80* 및 *443*을 차단하는 규칙의 경우 *UDP* 포트 *80* 및 *443*을 포함하는 서비스*(*개체 > 서비스*)*를 생성합니다.




*QUIC*에서 차단할 *UDP* 포트를 지정하기 위해 서비스를 이용한다. 두 번째 규칙에서 *QUIC* 애플리케이션을 차단하십시오.




- 복호화 프로파일 생성
- 복호화 정책 규칙 생성

## 복호화 프로파일 생성

복호화 프로파일을 사용하면 복호화에서 제외하도록 선택한 복호화된 트래픽과 SSL 트래픽 모두에 대해 검사를 수행할 수 있습니다. (서버가 인증서 고정 또는 기타 이유로 SSL 복호화를 기술적으로 중단하는 경우 서버를 복호화 제외 목록에 추가하십시오.) 필요에 따라 복호화 프로파일을 생성하여 다음을 수행합니다.


©2023 Palo Alto Networks, Inc.

- 만료된 인증서, 신뢰할 수 없는 발급자, 알 수 없는 인증서 상태, 인증서 상태 확인 타임아웃 및 인증서 확장이 있는 차단 세션을 포함하여 인증서 상태를 기반으로 세션을 차단합니다.
- 지원되지 않는 버전 및 암호 제품군이 있고 클라이언트 인증을 사용해야 하는 세션을 차단합니다.
- 복호화를 수행할 리소스를 사용할 수 없거나 인증서 서명에 하드웨어 보안 모듈을 사용할 수 없는 경우 세션을 차단합니다.
- SSL 프로토콜 설정에서 SSL 포워딩 프록시 및 SSL 인바운드 검사 트래픽에 허용되는 프로토콜 버전 및 키 교환, 암호화 및 인증 알고리즘을 정의합니다.

약한 사이트를 수용하기 위해 대부분의 사이트에 적용하는 기본 복호화 프로파일을 약화시키지 마십시오. 대신 지원해야 하지만 강력한 암호 및 알고리즘을 지원하지 않는 사이트에 대해 하나 이상의 개별 복호화 프로파일을 생성합니다. 다른 URL 카테고리에 대해 다른 복호화 프로파일을 만들어 민감한 자료가 포함되지 않은 트래픽의 보안과 성능을 미세 조정할 수도 있습니다. 그러나 항상 가능한 모든 트래픽을 해독하고 검사해야 합니다.

복호화 프로파일을 만든 후 복호화 정책 규칙에 연결합니다. 그런 다음 방화벽은 복호화 정책 규칙과 일치하는 트래픽에 복호화 프로파일 설정을 적용합니다.

Palo Alto Networks 방화벽에는 복호화된 트래픽에 대한 기본 권장 프로토콜 버전 및 암호 제품군을 시행하는 데 사용할 수 있는 기본 복호화 프로파일이 포함되어 있습니다. 그러나 모범 사례는 SSL 포워드 프록시 복호화 프로파일, SSL 인바운드 검사 복호화 프로파일 및 SSL 프로토콜 설정 복호화 프로파일에 설명된 대로 더 엄격한 복호화 제어를 활성화하는 것입니다.



약한 프로토콜이나 알고리즘에는 공격자가 악용할 수 있는 알려진 취약점이 포함되어 있으므로 지원하지 마십시오. 약한 프로토콜이 있는 레거시 시스템을 사용하는 주요 파트너 또는 계약자를 지원하기 위해 취약한 프로토콜이나 알고리즘을 허용해야 하는 경우 예외에 대한 별도의 복호화 프로파일을 생성하고 관련 트래픽에만 프로파일을 적용하는 복호화 정책 규칙에 연결합니다( 예: 파트너의 소스 *IP* 주소). 모든 트래픽에 대해 약한 프로토콜을 허용하지 마십시오.

**STEP 1 |** 새 복호화 프로파일을 생성합니다.

**Objects** > **Decryption Profile**을 선택한 다음, 복호화 프로파일 규칙을 추가 또는 수정하고, 규칙을 설명하는 이름을 지정합니다.

**STEP 2 |** (선택사항) 프로파일 규칙이 방화벽 또는 모든 Panorama 디바이스 그룹의 모든 가상 시스템에서 공유되도록 허용합니다.

**STEP 3 |** (암호 해독 미러링만 해당) 방화벽이 해독된 트래픽을 복사하고 전달하는 데 사용할 이더넷 인터페이스를 사용하도록 설정합니다.

이 작업과 별도로 암호 해독 포트 미러링 구성 단계를 따릅니다. 미러링을 금지하거나 미러링할 수 있는 트래픽 유형을 제어할 수 있는 현지 개인 정보 보호 규정을 숙지하십시오. 복호화 포트 미러링에는 복호화 포트 미러 라이선스가 필요합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) SSL 터널링 및/또는 인바운드 트래픽 차단 및 제어:



복호화된 트래픽에 복호화 프로파일을 적용하는 것은 선택 사항이지만 암호화된 위협으로부터 네트워크를 보호하기 위해 항상 복호화 프로파일을 정책 규칙에 적용하는 것이 가장 좋습니다. 보이지 않는 위협으로부터 자신을 보호할 수 없습니다.

**SSL** 복호화 선택:

- **SSL** 포워딩 프록시를 선택하여 인증서를 확인하고, 프로토콜 버전 및 암호 제품군을 적용하고, SSL 복호화 트래픽에 대한 실패 검사를 수행하도록 설정을 구성합니다. 이 설정은 이 프로파일이 SSL 포워딩 프록시 복호화를 수행하도록 구성된 복호화 정책 규칙에 연결된 경우에만 활성화됩니다.
- **SSL** 인바운드 검사를 선택하여 프로토콜 버전 및 암호 제품군을 적용하고 인바운드 SSL 트래픽에 대한 실패 검사를 수행하도록 설정을 구성합니다. 이 설정은 이 프로파일이 SSL 인바운드 검사를 수행하는 복호화 정책 규칙에 연결된 경우에만 활성화됩니다.
- **SSL** 프로토콜 설정을 선택하여 복호화된 SSL 트래픽에 적용할 최소 및 최대 프로토콜 버전과 키 교환, 암호화 및 인증 알고리즘을 제어하는 설정을 구성합니다. 이 설정은 이 프로파일이 SSL 포워딩 프록시 복호화 또는 SSL 인바운드 검사를 수행하도록 설정된 복호화 정책 규칙에 연결될 때 활성화됩니다.



방화벽이 ***FIPS-CC*** 모드이고 표준 모드의 ***Panorama***™ 관리 서버에서 관리하는 경우 복호화 프로파일을 방화벽에서 로컬로 생성해야 합니다. 표준 모드의 ***Panorama***에서 생성된 복호화 프로파일에는 지원되지 않는 ***3DES*** 및 ***RC4*** 암호화 알고리즘과 ***MD5*** 인증 알고리즘에 대한 참조가 포함되어 있어 관리되는 방화벽에 대한 푸시가 실패합니다.

**STEP 5 |** (선택 사항) 정책 기반 복호화 제외 생성을 선택하는 트래픽(예: URL 카테고리)을 차단 및 제어합니다.



복호화를 선택하지 않은 트래픽에 복호화 프로파일을 적용하는 것은 선택 사항이지만 만료된 인증서나 신뢰할 수 없는 발급자가 있는 세션으로부터 네트워크를 보호하기 위해 항상 복호화 프로파일을 정책 규칙에 적용하는 것이 가장 좋습니다.

암호 해독 없음을 선택하여 비복호화 프로파일를 구성하고 만료된 인증서가 있는 세션 차단 및 신뢰할 수 없는 발급자가 있는 세션 차단 상자를 선택하여 제외된 트래픽에 대한 인증서의 유효성을 검사합니다. 해독하지 않기로 선택한 트래픽에 대해서만 정책 기반 제외를 생성합니다. 서버가 기술적인 이유로 복호화를 중단하는 경우 정책 기반 제외를 만들지 말고 SSL 복호화 제외 목록( **Device** > **Certificate Management** > **SSL** 복호화 제외)에 서버를 추가하십시오.

이러한 설정은 특정 트래픽에 대한 복호화를 비활성화하는 복호화 정책 규칙에 복호화 프로파일이 연결된 경우에만 활성화됩니다.

**STEP 6 |** (선택 사항) 해독된 SSH 트래픽을 차단하고 제어합니다.

**SSH** 프록시를 선택하여 SSH 프록시 복호화 프로파일을(를) 구성하여 지원되는 프로토콜 버전을 적용하고 복호화를 수행하는 데 시스템 리소스를 사용할 수 없는 경우 세션을 차단하도록 설정을 구성 및 구성합니다.

이러한 설정은 복호화 프로파일이 SSH 트래픽을 해독하는 복호화 정책 규칙에 연결된 경우에만 활성화됩니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 복호화 정책 규칙을 생성할 때 복호화 프로파일을 추가합니다.

방화벽은 복호화 정책 규칙과 일치하는 트래픽에 복호화 프로파일을 적용하고 프로파일 설정을 적용합니다.

**STEP 8 |** 구성을 커밋합니다.

## 복호화 정책 규칙 생성

방화벽이 암호를 해독할 트래픽과 방화벽에서 수행할 복호화 유형을 정의하는 복호화 정책 규칙을 생성합니다. SSL 포워딩 프록시, SSL 인바운드 검사 또는 SSH 프록시 복호화. 복호화 정책 규칙을 사용하여 복호화 미러링을 정의할 수도 있습니다.

**STEP 1 |** 새 암호 해독 정책 규칙을 추가합니다.

정책 > 암호 해독, 새 암호 해독 정책 규칙 추가를 선택하고 정책 규칙에 설명적인 이름을 지정합니다.

**STEP 2 |** 네트워크 및 정책 개체를 기반으로 트래픽과 일치하도록 암호 해독 규칙을 구성합니다.

- 방화벽 보안 영역 - 소스 및/또는 대상을 선택한 다음 소스 영역 및/또는 대상 영역을 기반으로 트래픽과 일치시킵니다.
- **IP** 주소, 주소 개체 및/또는 주소 그룹 - 원본 주소 및/또는 대상 주소를 기반으로 트래픽과 일치시킬 원본 및/또는 대상을 선택합니다. 또는 **Negate**를 선택하여 복호화에서 소스 주소 목록을 제외합니다.
- 사용자 - 소스를 선택한 다음 트래픽 암호를 해독할 소스 사용자를 설정합니다. 특정 사용자 또는 그룹 트래픽을 해독하거나 알 수 없는 사용자 또는 사전 로그온 사용자(GlobalProtect에 연결되었지만 아직 로그인하지 않은 사용자)와 같은 특정 유형의 사용자에 대한 트래픽을 해독할 수 있습니다.
- 포트 및 프로토콜 - 서비스/**URL** 카테고리를 선택하여 서비스 기반 트래픽과 일치하도록 규칙을 설정합니다. 기본적으로 정책 규칙은 TCP 및 UDP 포트의 모든 트래픽을 해독하도록 설정됩니다. 서비스 또는 서비스 그룹을 추가하고 선택적으로 규칙을 **application-default**로 설정하여 애플리케이션 기본 포트의 애플리케이션에만 일치하도록 할 수 있습니다.



애플리케이션 기본 설정은 정책 기반 복호화 제외를 생성할 때 유용할 수 있습니다. 기본 포트에서 실행되는 애플리케이션을 복호화에서 제외할 수 있으며, 비표준 포트에서 탐지될 때 동일한 애플리케이션을 계속 복호화할 수 있습니다.

- **URL** 및 **URL** 카테고리 - 서비스/URL 카테고리를 선택한 다음 다음을 기반으로 트래픽 복호화:
  - 방화벽이 정책 시행을 위해 검색하는 외부 호스팅 URL 목록입니다(**Objects** > **External Dynamic Lists** 참조).
  - Palo Alto Networks는 사전 정의된 URL 카테고리를 통해 허용된 트래픽의 전체 카테고리를 쉽게 해독할 수 있습니다. 이 옵션은 민감한 사이트를 개별적으로가 아니라 카테고리별로 제외할 수 있으므로 정책 기반 복호화 제외를 생성할 때도 유용합니다. 예를 들어 복호화를 원하지 않는 그룹 사이트에 대한 사용자 지정 URL 카테고리를 만들 수 있지만 사전 정의된 Palo Alto Networks URL 카테고리를 기반으로 금융 또는 의료 관련 사이트를 복호화에서 제외할 수도 있

 ©2023 Palo Alto Networks, Inc.

습니다. 또한 위험한 URL 카테고리를 차단하고 편안한 페이지를 생성하여 사이트가 차단된 이유를 알리거나 사용자가 SSL 복호화를 선택 해제하도록 할 수 있습니다.

사전 정의된 고위험 및 중간 위험 URL 카테고리를 사용하여 모든 고위험 및 중간 위험 URL 트래픽의 암호를 해독하는 복호화 정책 규칙을 생성할 수 있습니다. 모든 위험한 트래픽을 복호화하고 검사할 수 있도록 안전망으로 규칙을 규칙 베이스의 맨 아래에 배치합니다(모든 복호화 예외는 이 규칙 위에 있어야 민감한 정보를 해독하지 않습니다). 그러나 액세스를 허용한 고위험 또는 중간 위험 사이트에 개인 식별 정보(PII) 또는 복호화를 원하지 않는 기타 민감한 정보가 포함되어 있는 경우 해당 사이트를 차단하여 암호화된 위험한 트래픽을 허용하지 않고 개인 정보 문제를 방지하거나 비복호화 규칙을 만들어 민감한 트래픽을 처리합니다.

- 사용자 정의 URL 카테고리(개체 > 사용자 정의 개체 > **URL** 카테고리 참조). 예를 들어, 사용자 지정 URL 카테고리를 만들어 비즈니스 목적으로 액세스해야 하지만 가장 안전한 프로토콜 및 알고리즘을 지원하지 않는 사이트 그룹을 지정한 다음 해당 사이트에 대해서만 사용자 지정 복호화 프로파일을 적용하여 느슨한 프로토콜 및 알고리즘을 허용할 수 있습니다(이 경우 대부분의 사이트에 사용하는 복호화 프로파일을 다운그레이드하여 보안 성능이 저하되지 않습니다).

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 일치하는 트래픽을 해독하거나 해독에서 일치하는 트래픽을 제외하도록 규칙을 설정합니다.

옵션을 선택한 다음 정책 규칙 작업을 설정합니다.

일치하는 트래픽을 해독하려면:

1. 작업을 복호화로 설정합니다.
2. 방화벽이 일치하는 트래픽에서 수행할 복호화의 유형을 설정합니다.
   - SSL 전달 프록시.
   - SSL 인바운드 검사. 그런 다음 인바운드 SSL 트래픽의 대상 내부 서버에 대해 하나 이상의 인증서를 추가합니다. SSL 인바운드 검사 정책 규칙은 최대 12개의 인증서를 지원합니다.

     각 도메인에 자체 인증서가 있는 여러 도메인을 호스팅하는 내부 서버에 대한 ***SSL/TLS*** 트래픽을 해독하도록 암호 해독 정책 규칙을 구성할 수 있습니다. 방화벽은 요청된 ***URL***에 대해 서버가 제공하는 인증서와 일치하는 정책 규칙의 인증서를 사용하여 ***SSL/TLS*** 연결을 협상합니다.

     가동 중지 시간을 발생시키지 않고 보호된 내부 서버에 대한 인증서를 업데이트하려면 만료되거나 유효하지 않게 되기 전에 새 서버 인증서를 갱신하거나 가져옵니다. 그런 다음 웹 서버에 동일한 인증서를 설치하기 전에 인증서 및 개인 키를 방화벽으로 가져와 ***SSL*** 인바운드 검사 정책 규칙에 추가합니다. 웹 서버에서 다른 인증서가 활성 상태일 때 정책 규칙을 새 인증서로 업데이트하면 방화벽이 사용 중인 인증서에 관계없이 서버에 대한 트래픽을 해독할 수 있도록 준비됩니다. SSL 인바운드 검사 구성에서는 이 프로세스에 대해 자세히 설명합니다.

     (*Panorama*™) ***SSL*** 인바운드 검사 정책 규칙의 여러 인증서에 대한 지원은 ***PAN-OS 10.2*** 이전 버전의 ***PAN-OS***® 버전에서는 사용할 수 없습니다. ***PAN-OS 10.2***를 실행하는 ***Panorama*** 관리 서버에서 이전 버전을 실행하는 방화벽으로 여러 인증서를 사용하여 ***SSL*** 인바운드 검사 정책 규칙을 푸시하는 경우 관리되는 방화벽의 정책 규칙은 알파벳순으로 정렬된 인증서 목록에서 첫 번째 인증서만 상속합니다.

     ***Panorama***에서 암호 해독 정책 규칙을 푸시하기 전에 ***PAN-OS 10.1*** 이하를 실행하는 방화벽에 대해 다른 템플릿 또는 디바이스 그룹을 설정하여 올바른 정책을 푸시하도록 하는 것이 좋습니다. 규칙 및 인증서를 적절한 방화벽에 연결합니다.
   - SSH 프록시.

복호화에서 일치하는 트래픽을 제외하려면:

작업을 비복호화으로 설정합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) 정책 규칙과 일치하는 트래픽에 대한 추가 검사를 수행하려면 암호 해독 프로파일을 선택합니다.



복호화된 트래픽에 복호화 프로파일을 적용하는 것은 선택 사항이지만 암호화된 위협으로부터 네트워크를 보호하기 위해 항상 복호화 프로파일을 정책 규칙에 적용하는 것이 가장 좋습니다. 보이지 않는 위협으로부터 자신을 보호할 수 없습니다.

예를 들어, 정책 규칙에 복호화 프로파일을 연결하여 서버 인증서가 유효한지 확인하고 지원되지 않는 프로토콜이나 암호를 사용하는 세션을 차단합니다. 암호 해독 프로파일을 만들려면 개체 > 암호 해독 프로파일을 선택합니다.

1. 복호화 정책 규칙을 생성하거나 기존 규칙을 열어 수정합니다.
2. 옵션을 선택하고 암호 해독 프로파일을 선택하여 규칙과 일치하는 트래픽의 다양한 측면을 차단하고 제어합니다.

   방화벽이 일치하는 트래픽에 적용하는 프로파일 규칙 설정은 정책 규칙 작업(복호화 또는 비복호화) 및 정책 규칙 유형(SSL 포워딩 프록시, SSL 인바운드 검사 또는 SSH 프록시)에 따라 다릅니다. 이를 통해 다양한 유형의 트래픽 및 사용자에게 적용되는 다양한 유형의 복호화 정책 규칙과 함께 다양한 복호화 프로파일을 사용할 수 있습니다.
3. 확인을 클릭합니다.

**STEP 5 |** 암호 해독 로깅 구성(성공 및 실패한 TLS 핸드셰이크를 모두 기록할지 여부를 구성하고 암호 해독 로그 전달을 구성).

**STEP 6 |** 확인을 클릭하여 정책을 저장합니다.

**STEP 7 |** 방화벽이 트래픽을 해독하도록 완전히 활성화하려면 다음 단계를 선택하십시오...

- SSL 전달 프록시를 구성합니다.
- SSL 인바운드 검사 구성.
- SSH 프록시를 구성합니다.
- 정책 기반의 암호 해독 제외를 생성하여 암호를 해독하지 선택하고 고정된 인증서 또는 상호 인증과 같은 기술적인 이유로 암호 해독을 중단하는 사이트를 SSL 암호 해독 제외 목록에 추가합니다.


©2023 Palo Alto Networks, Inc.

# SSL 포워드 프록시 구성

방화벽이 SSL 포워드 프록시 복호화를 수행할 수 있도록 하려면 방화벽을 신뢰할 수 있는 타사(프록시)로 설정하는 데 필요한 인증서를 클라이언트와 서버 간의 세션에 설정해야 합니다. 방화벽은 엔터프라이즈 인증서 기관(CA)이 서명한 인증서 또는 방화벽에서 생성된 자체 서명 된 인증서를 포워드 신뢰 인증서로 사용하여 클라이언트와 SSL 세션을 인증할 수 있습니다.

- (모범 사례) 엔터프라이즈**CA** 서명 인증서 - 엔터프라이즈 CA는 방화벽이 SSL 복호화가 필요한 사이트에 대한 인증서에 서명하는 데 사용할 수 있는 서명 인증서를 발급할 수 있습니다. 방화벽이 대상 서버의 인증서에 서명한 CA를 신뢰하면 방화벽은 엔터프라이즈 CA가 서명한 클라이언트에 대상 서버 인증서의 복사본을 보낼 수 있습니다. 일반적으로 모든 네트워크 디바이스가 이미 엔터프라이즈 CA(일반적으로 디바이스의 CA Trust 저장소에 이미 설치됨)를 신뢰하므로 엔드포인트에 인증서를 배포할 필요가 없게 되어 롤아웃 프로세스가 더 원활하기 때문입니다.
- 자체 서명된 인증서 - 방화벽은 CA 역할을 하고 방화벽이 SSL 복호화이 필요한 사이트에 대한 인증서에 서명하는 데 사용할 수 있는 자체 서명된 인증서를 생성할 수 있습니다. 방화벽은 서버에 표시하여 클라이언트에 표시하고 SSL 세션을 설정하도록 서버 인증서의 복사본에 서명할 수 있습니다. 이 방법을 사용하면 이러한 디바이스가 방화벽의 자체 서명된 인증서를 인식할 수 있도록 모든 네트워크 디바이스에 자체 서명된 인증서를 설치해야합니다. 인증서를 모든 디바이스에 배포해야 하므로 이 메서드는 대규모 배포보다 작은 배포 및 개념 증명(POC) 평가판에 더 적합합니다.

또한 방화벽이 신뢰하지 않는 CA에서 서버 인증서에 서명할 때 방화벽에 대한 상태 표시 해제 인증서를 클라이언트에 표시하도록 설정합니다. 이렇게 하면 신뢰할 수 없는 인증서가 있는 사이트에 액세스하려고 할 때 클라이언트가 인증서 경고를 표시합니다.

엔터프라이즈 루트 *CA*에서 *Forward Trust* 인증서를 생성하든 방화벽에서 생성된 자체 서명 인증서를 사용하든 각 방화벽에 대해 별도의 하위 종속 상태 트러스트 *CA* 인증서를 생성합니다. 별도의 하위 *CA*를 사용할 수 있는 유연성을 통해 나머지 배포에 영향을 주지 않고 기기(또는 기기 쌍)를 폐기할 때 하나의 인증서를 취소할 수 있으며 취소해야 하는 상황에서 영향을 줄일 수 있습니다. 또한 각 방화벽에서 별도의 전달 신뢰 *CA*는 사용자에게 표시되는 *CA* 오류 메시지에 트래픽이 통과하는 방화벽에 대한 정보가 포함되어 있으므로 문제를 해결하는 데 도움이 됩니다. 모든 방화벽에서 동일한 *Forward Trust CA*를 사용하면 해당 정보의 세분성이 손실됩니다.

SSL 정방향 프록시 암호 해독에 필요한 전달 신뢰 및 전달 불신임 인증서를 설정한 후 방화벽이 복호화할 트래픽을 정의하는 암호 해독 정책 규칙을 만들고 SSL 제어 및 검사를 트래픽에 적용하는 암호 해독 프로파일을 만듭니다. 암호 해독 정책은 규칙과 일치하는 SSL 터널링된 트래픽을 일반 텍스트 트래픽으로 해독합니다. 방화벽은 암호 해독 정책 및 방화벽 보안 정책에 연결된 암호 해독 프로파일을 기반으로 트래픽을 차단하고 제한합니다. 방화벽은 방화벽을 종료할 때 트래픽을 다시 암호화합니다.

*SSL* 전달 프록시를 구성할 때 프록시된 트래픽은 *DSCP* 코드 포인트 또는 *QoS*를 지원하지 않습니다.

**STEP 1 |** 적절한 인터페이스가 가상 와이어, 레이어 2 또는 레이어 3 인터페이스로 구성된지 확인합니다.

**Network** > **Interfaces** > **Ethernet** 탭에서 구성된 인터페이스를 봅니다. 인터페이스 유형 열은 인터페이스가 가상 와이어, 레이어 **2** 또는 레이어 **3** 인터페이스로 구성된 경우 표시됩니다. 인터페이스 유형을 포함하여 구성을 수정할 인터페이스를 선택할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 신뢰할 수 있는 CA가 서버 인증서에 서명한 경우 방화벽이 클라이언트에 표시되도록 정방향 신뢰 인증서를 구성합니다. 엔터프라이즈 CA 서명 인증서 또는 자체 서명된 인증서를 전달 신뢰 인증서로 사용할 수 있습니다.

(권장 모범 사례) 엔터프라이즈 CA 서명 인증서를 전달 신뢰 인증서로 사용합니다. 각 방화벽에 고유하게 명명된 전달 신뢰 인증서를 만듭니다.

1. 엔터프라이즈 CA가 서명하고 검증할 인증서 서명 요청(CSR)을 생성:
   1. 디바이스 > 인증서 관리 > 인증서를 선택하고 생성을 클릭합니다.
   2. 인증서 이름을 입력합니다. 각 방화벽에 고유한 이름을 사용합니다.
   3. 서명자 드롭다운에서 외부 기관**(CSR)**을 선택합니다.
   4. (선택사항) 엔터프라이즈 CA에서 요구하는 경우 인증서 속성을 추가하여 국가 또는 부서와 같은 방화벽 세부정보를 추가로 식별합니다.
   5. CSR을 저장하려면 생성을 클릭합니다. 이제 디바이스 인증서 탭에 보류 중인 인증서가 표시됩니다.
2. CSR 내보내기:
   1. 디바이스 인증서 탭에 표시된 보류 중인 인증서를 선택합니다.
   2. 인증서 파일을 다운로드하고 저장하려면 내보내기를 클릭합니다.

      비공개 키가 방화벽에서 안전하게 유지되도록 비공개 키 내보내기를 선택하지 않은 상태로 둡니다.
   3. 확인을 클릭합니다.
3. 엔터프라이즈 CA에 인증서 파일을 제공합니다. 엔터프라이즈 CA에서 엔터프라이즈 CA 서명 인증서를 받으면 엔터프라이즈 CA 서명 인증서를 저장하여 방화벽으로 가져옵니다.
4. 엔터프라이즈 CA 서명 인증서를 방화벽으로 가져옵니다.
   1. 디바이스 > 인증서 관리 > 인증서를 선택한 다음 가져오기를 클릭합니다.
   2. 보류 중인 인증서 이름을 정확하게 입력합니다. 입력한 인증서 이름은 보류 중인 인증서의 유효성을 검사하려면 보류 중인 인증서 이름과 정확히 일치해야 합니다.
   3. 엔터프라이즈 CA에서 받은 서명된 인증서 파일을 선택합니다.
   4. 확인을 클릭합니다. 인증서는 키 및 CA 체크박스를 선택한 경우 유효한 것으로 표시됩니다.
5. 검증된 인증서를 선택하여 SSL 포워드 프록시 복호화에 사용할 포워딩 신뢰 인증서로 사용하도록 설정합니다.
6. 확인을 클릭하여 엔터프라이즈 CA 서명된 포워드 트러스트 인증서를 저장합니다.

자체 서명된 인증서를 Forward Trust 인증서로 사용합니다.

1. 자체 서명된 루트 CA 인증서를생성합니다.
2. 자체 서명된 루트 CA 인증서(디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서 디바이스 인증서)를 클릭하여 인증서 정보를 열고 신뢰할 수 있는 루트 **CA** 체크박스를 클릭합니다.
3. 확인을 클릭합니다.
4. 각 방화벽에 대해 새로운 하위 CA 인증서를 생성합니다.
   1. 디바이스 > 인증서 관리 > 인증서를 선택합니다.


©2023 Palo Alto Networks, Inc.

2. 창 하단에서 생성을 클릭합니다.
3. 인증서 이름을 입력합니다.
4. 192.168.2.1과 같은 공통 이름을 입력합니다. 인증서에 표시되는 IP 또는 FQDN이어야 합니다. 이 경우 트러스트 인터페이스의 IP를 사용하고 있습니다. 이 필드의 공백을 사용하지 마십시오.
5. 서명 필드에서 만든 자체 서명된 루트 CA 인증서를 선택합니다.
6. 인증서 기관 체크박스를 클릭하여 방화벽이 인증서를 발급할 수 있도록 합니다. 이 체크박스를 선택하면 클라이언트 브라우저로 가져오는 방화벽에 인증서 기관(CA)이 생성되므로 클라이언트는 방화벽을 CA로 신뢰합니다.
7. 인증서를 생성합니다.

5. 새 인증서를 클릭하여 수정하고 포워드 신뢰 인증서 체크박스를 클릭하여 인증서를 포워드 신뢰 인증서로 구성합니다.
6. 확인을 클릭하여 자체 서명된 포워드 트러스트 인증서를 저장합니다.
7. 이 절차를 반복하여 각 방화벽에서 고유한 하위 CA 인증서를 생성합니다.

**STEP 3 |** 클라이언트 시스템 인증서 저장소에 포워딩 신뢰 인증서를 배포합니다.

엔터프라이즈-CA 서명된 인증서를 SSL 포워드 프록시 복호화에 대한 포워딩 신뢰 인증서로 사용하고 클라이언트 시스템에 이미 로컬 신뢰할 수 있는 루트 CA 목록에 엔터프라이즈 CA가 설치된 경우 이 단계를 건너뛸 수 있습니다. 클라이언트 시스템은 엔터프라이즈 신뢰할 수 있는 루트 CA가 서명했기 때문에 방화벽에서 생성하는 하위 CA 인증서를 신뢰합니다.

클라이언트 시스템에 포워딩 신뢰 인증서를 설치하지 않으면 사용자가 방문하는 각 ***SSL*** 사이트에 대한 인증서 경고를 볼 수 있습니다.

GlobalProtect 포털로 구성된 방화벽에서:

이 옵션은 ***Windows*** 및 ***Mac*** 클라이언트 ***OS*** 버전에서 지원되며 ***GlobalProtect*** 에이전트 ***3.0.0*** 이상의 클라이언트 시스템에 설치해야 합니다.

1. 네트워크 > **GlobalProtect** > **Portals**를 선택한 다음 기존 포털 구성을 선택하거나 새 구성을 추가합니다.
2. 에이전트를 선택한 다음 기존 에이전트 구성을 선택하거나 새 구성을 추가합니다.
3. 신뢰할 수 있는 루트 CA 섹션에 자체 서명된 방화벽 신뢰할 수 있는 루트 CA 인증서를 추가합니다. GlobalProtect가 방화벽의 신뢰할 수 있는 루트 CA 인증서를 클라이언트 시스템에 배포한

 ©2023 Palo Alto Networks, Inc.

후 클라이언트 시스템은 방화벽의 루트 CA 인증서를 신뢰하기 때문에 방화벽의 하위 CA 인증서를 신뢰합니다.

4. GlobalProtect 포털이 인증서를 자동으로 배포하고 GlobalProtect 클라이언트 시스템의 인증서 저장소에 설치되도록 로컬 루트 인증서 저장소에 설치합니다.
5. 확인을 두 번 클릭합니다.

GlobalProtect가 없는 경우:

방화벽을 클라이언트 시스템으로 가져올 수 있도록 신뢰할 수 있는 루트 CA 인증서를 내보냅니다. 인증서를 강조 표시하고 창 하단에서 내보내기를 클릭합니다. PEM 형식을 선택합니다.

내보내기 개인 키 체크박스를 선택하지 마십시오! 개인 키는 방화벽에 남아 있어야 하며 클라이언트 시스템으로 내보내야 합니다.

클라이언트가 방화벽의 신뢰할 수 있는 루트 CA 인증서를 클라이언트 시스템의 브라우저 신뢰할 수 있는 루트 CA 목록에 가져와 클라이언트가 신뢰할 수 있도록 합니다. 클라이언트 브라우저로 가져올 때 신뢰할 수 있는 루트 인증 기관 인증서 저장소에 인증서를 추가해야 합니다. Windows 시스템에서 기본 가져오기 위치는 개인 인증서 저장소입니다. 또한 GPO(Active Directory 그룹 정책 개체)와 같은 중앙 집중식 배포 옵션을 사용하여 이 프로세스를 단순화할 수도 있습니다.

**STEP 4 |** 포워드 언트러스트 인증서를 구성합니다(모든 방화벽에 대해 동일한 포워드 언트러스트 인증서를 사용).

1. 인증서 페이지 하단에서 생성을 클릭합니다.
2. 내 my-ssl-fwd-untrust와 같은 인증서 이름을 입력합니다.
3. 예를 들어 공통 이름(예:192.168.2.1)을 설정합니다. 서명자를 비워둡니다.
4. 인증서 기관 체크박스를 클릭하여 방화벽이 인증서를 발급할 수 있도록 합니다.
5. 생성을 클릭하여 인증서를 생성합니다.
6. 확인을 클릭하여 저장합니다.
7. 새 ssl-fwd-언트러스트 인증서를 클릭하여 수정하고 언트러스트 인증서 포워딩 옵션을 활성화합니다.

   네트워크 디바이스의 인증서 신뢰 목록에 위임되지 않는 인증서를 내보내지 마십시오! 클라이언트 시스템에 언트러스트 인증서를 설치하지 마십시오. 트러스트 목록에 언트러스트 인증서를 설치하면 방화벽이 신뢰할 수 없는 웹사이트를 신뢰하는 디바이스가 생성되므로 매우 중요합니다. 또한 사용자는 신뢰할 수 없는 사이트에 대한 인증서 경고가 표시되지 않으므로 사이트가 신뢰할 수 없다는 것을 알지 못하고 해당 사이트에 액세스할 수 있으므로 네트워크가 위협에 노출될 수 있습니다.

8. 확인을 클릭하여 저장합니다.

**STEP 5 |** (선택사항) 방화벽이 클라이언트에 제공하는 SSL 포워드 프록시 서버 인증서의 키 크기를 구성합니다. 기본적으로 방화벽은 대상 서버 인증서의 키 크기에 따라 사용할 키 크기를 결정합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 복호화 정책 규칙을 만들어 방화벽이 해독할 트래픽을 정의하고 복호화 프로파일을 만들어 트래픽에 SSL 컨트롤을 적용합니다.



복호화 프로파일은 선택 사항이지만 각 복호화 정책 규칙에 복호화 프로파일을 포함하여 취약하고 취약한 프로토콜과 알고리즘이 네트워크에서 의심스러운 트래픽을 허용하지 않도록 하는 것이 가장 좋습니다.

1. 정책 > 암호 해독을 선택하고 기존 규칙을 추가 또는 수정하고 복호화할 트래픽을 정의합니다.
2. 옵션을 선택한 다음:
   - 규칙 작업을 일치하는 트래픽 복호화로 설정합니다.
   - 규칙 유형을 **SSL** 포워드 프록시로 설정합니다.
   - (선택사항이지만 모범 사례) 기존 복호화 프로파일을 구성하거나 선택하여 해독된 트래픽의 다양한 측면을 차단하고 제어합니다(예: 복호화 프로파일을 만들어 인증서 검사를 수행하고 강력한 암호 제품군 및 프로토콜 버전을 적용합니다).
3. 확인을 클릭하여 저장합니다.

**STEP 7 |** 방화벽이 WildFire 분석을 위해 복호화된 SSL 트래픽을 전달하도록 설정합니다.



이 옵션은 활성 ***WildFire*** 라이선스가 필요하며 WildFire 모범 사례입니다.

**STEP 8 |** 구성을 커밋합니다.

**STEP 9 |** 다음 단계를 선택합니다.

- 사용자가 SSL 복호화을 옵트아웃할 수 있도록 합니다.
- 특정 유형의 트래픽에 대한 복호화을 비활성화하도록 복호화 제외를 구성합니다.


©2023 Palo Alto Networks, Inc.

# SSL 인바운드 검사 구성

SSL 인바운드 검사를 사용하여 네트워크 서버로 향하는 인바운드 SSL 트래픽을 해독하고 검사합니다(서버 인증서를 방화벽에 로드하면 모든 서버에 대해 SSL 인바운드 검사를 수행할 수 있음). SSL 인바운드 검사 복호화 정책이 활성화되면 방화벽은 정책에서 식별된 모든 SSL 트래픽을 해독하여 텍스트 트래픽을 지우고 검사합니다. 방화벽은 구성된 모든 안티바이러스, 취약성 보호, 안티스파이웨어, URL 필터링 및 파일 차단 프로파일을 포함하여 트래픽에 적용되는 보안 정책 및 정책에 첨부된 복호화 프로파일을 기반으로 트래픽을 차단, 제한 또는 허용합니다. 가장 좋은 방법은 방화벽이 WildFire 분석 및 서명 생성을 위해 해독된 SSL 트래픽을 포워딩할 수 있도록 하는 것입니다.

SSL 인바운드 검사 구성에는 다음이 포함됩니다.

- 방화벽에 대상 서버 인증서를 설치합니다.
- SSL 인바운드 검사 복호화 정책 규칙을 생성합니다.
- 정책 규칙에 암호 해독 프로파일을 적용합니다.

*SSL* 인바운드 검사를 구성할 때 프록시된 트래픽은 *DSCP* 코드 포인트 또는 *QoS*를 지원하지 않습니다.

*SSL* 인바운드 검사는 인증 포털 리디렉션을 지원하지 않습니다. 인증 포털 리디렉션 및 복호화을 사용하려면 SSL 포워드 프록시를 사용해야 합니다.

**STEP 1 |** 적절한 인터페이스가 가상 와이어, 레이어 2 또는 레이어 3 인터페이스로 구성된지 확인합니다.

*SSL* 인바운드 검사에는 탭 모드 인터페이스를 사용할 수 없습니다.

**Network** > **Interfaces** > 이더넷 탭에서 구성된 인터페이스를 봅니다. 인터페이스가 **Virtual Wire**, 레이어 **2** 또는 레이어 **3** 인터페이스로 구성된 경우 인터페이스 유형 열이 표시됩니다. 인터페이스 유형을 포함하여 구성을 수정할 인터페이스를 선택할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 대상 서버 인증서가 방화벽에 설치되어 있는지 확인하십시오.

웹 인터페이스에서 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택하여 방화벽에 설치된 인증서를 확인합니다.

웹 서버에서 지원하는 ***TLS*** 버전은 방화벽에 서버 인증서 및 키를 설치하는 방법을 결정합니다.

최종 엔티티*(*리프*)* 인증서가 하나 이상의 중간 인증서로 서명되고 웹 서버가 ***TLS 1.2*** 및 ***Rivest, Shamir, Adleman(RSA)*** 또는 ***Perfect Forward*** 비밀(PFS*)* 키 교환 알고리즘을 지원하는 경우 인증서 체인*(*단일 파일*)*을 방화벽에 업로드하는 것이 좋습니다. 체인을 업로드하면 클라이언트 쪽 서버 인증서 인증 문제가 방지됩니다. 다음과 같이 파일에 인증서를 정렬해야 합니다.

***1.*** 최종 엔티티*(*리프*)* 인증서

***2.*** 중간 인증서*(*발급 순서대로*)*

***3.*** *(*선택 사항*)* 루트 인증서

웹 서버가 ***TLS 1.3*** 연결을 지원하고 인증서 체인이 서버에 설치된 경우 리프 인증서에 의해 중간 인증서로 서명될 때 서버 인증서 및 개인 키만 방화벽에 업로드할 수 있습니다. SSL 인바운드 검사에서는 각 사례에 대해 자세히 설명합니다.

대상 서버 인증서를 방화벽으로 가져오려면:

1. 디바이스 인증서 탭에서 가져오기를 선택합니다.
2. 설명이 포함된 인증서 이름을 입력합니다.
3. 대상 서버 인증서 파일을 찾아 선택합니다.
4. 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 복호화 정책 규칙을 만들어 방화벽이 해독할 트래픽을 정의하고 복호화 프로파일을 만들어 트래픽에 SSL 컨트롤을 적용합니다.

암호 해독 프로파일은 선택 사항이지만 각 암호 해독 정책 규칙에 암호 해독 프로파일을 포함하여 취약하고 취약한 프로토콜과 알고리즘이 네트워크에서 의심스러운 트래픽을 허용하지 않도록 하는 것이 가장 좋습니다.

1. 정책 > 암호 해독, 추가를 선택하거나 기존 규칙을 수정하고 복호화할 트래픽을 정의합니다.
2. 옵션을 선택한 다음:
   - 트래픽과 일치하는 작업을 복호화로 설정합니다.
   - 유형을 **SSL** 인바운드 검사로 설정합니다.
   - 인바운드 SSL 트래픽의 대상인 내부 서버에 대한 인증서를 추가합니다. SSL 인바운드 검사 정책 규칙은 최대 12개의 인증서를 지원합니다.

     각 도메인에 자체 인증서가 있는 여러 도메인을 호스팅하는 내부 서버에 대한 ***SSL/TLS*** 트래픽을 해독하도록 암호 해독 정책 규칙을 구성할 수 있습니다. 방화벽은 요청된 ***URL***에 대해 서버가 제공하는 인증서와 일치하는 정책 규칙의 인증서를 사용하여 ***SSL/TLS*** 연결을 협상합니다.


©2023 Palo Alto Networks, Inc.

가동 중지 시간을 발생시키지 않고 보호된 내부 서버에 대한 인증서를 업데이트하려면 만료되거나 유효하지 않게 되기 전에 새 서버 인증서를 갱신하거나 가져옵니다. 그런 다음 웹 서버에 동일한 인증서를 설치하기 전에 인증서 및 개인 키를 방화벽으로 가져와 ***SSL*** 인바운드 검사 정책 규칙에 추가합니다. 웹 서버에서 다른 인증서가 활성 상태일 때 정책 규칙을 새 인증서로 업데이트하면 방화벽이 사용 중인 인증서에 관계없이 서버에 대한 트래픽을 해독할 수 있도록 준비됩니다.

새 인증서를 배포할 준비가 되면 웹 서버에 로드하고 올바르게 설치했는지 확인합니다. 새 인증서의 설치는 기존 연결에 영향을 주지 않습니다. 방화벽은 ***Server Hello*** 메시지의 인증서가 암호 해독 정책 규칙의 새 인증서와 일치하는지 확인합니다. 일치하는 항목이 없으면 세션이 종료됩니다. 해당 암호 해독 로그 항목은 세션 종료 이유를 방화벽과 서버 인증서 간의 불일치로 보고합니다. 성공적인 핸드셰이크를 기록하여 모든 인바운드 검사 세션에 사용된 서버 인증서를 봅니다.

*(Panorama™) **SSL*** 인바운드 검사 정책 규칙의 여러 인증서에 대한 지원은 ***PAN-OS 10.2*** 이전 버전의 ***PAN-OS®*** 버전에서는 사용할 수 없습니다. ***PAN-OS 10.2***를 실행하는 ***Panorama*** 관리 서버에서 이전 버전을 실행하는 방화벽으로 여러 인증서를 사용하여 ***SSL*** 인바운드 검사 정책 규칙을 푸시하는 경우 관리되는 방화벽의 정책 규칙은 알파벳순으로 정렬된 인증서 목록에서 첫 번째 인증서만 상속합니다.

***Panorama***에서 암호 해독 정책 규칙을 푸시하기 전에 ***PAN-OS 10.1*** 이하를 실행하는 방화벽에 대해 다른 템플릿 또는 디바이스 그룹을 설정하여 올바른 정책을 푸시하도록 하는 것이 좋습니다. 규칙 및 인증서를 적절한 방화벽에 연결합니다.

- (선택 사항이지만 모범 사례) 기존 복호화 프로파일을 구성하거나 선택하여 복호화된 트래픽의 다양한 측면을 차단하고 제어합니다(예: 지원되지 않는 알고리즘 및 지원되지 않는 암호 제품군이 있는 세션을 종료하는 복호화 프로파일 생성).

  ***SSL*** 인바운드 검사 트래픽에 대해 SSL 프로토콜 설정 복호화 프로파일을 구성할 때 보안 기능이 서로 다른 서버에 대해 별도의 프로파일을 만듭니다. 예를 들어, 한 서버 세트가 ***RSA***만 지원하는 경우 ***SSL*** 프로토콜 설정은 ***RSA***만 지원하면 됩니다. 그러나 ***PFS***를 지원하는 서버에 대한 ***SSL*** 프로토콜 설정은 ***PFS***를 지원해야 합니다. 서버가 지원하는 최고 수준의 보안을 위해 ***SSL*** 프로토콜 설정을 구성하지만 방화벽 리소스가 더 높은 보안 프로토콜 및 알고리즘에 필요한 더 높은 처리 부하를 처리할 수 있는지 확인하려면 성능을 확인하십시오.

3. 확인을 클릭하여 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 방화벽이 WildFire 분석을 위해 복호화된 SSL 트래픽을 전달하도록 설정합니다.



이 옵션은 활성 ***WildFire*** 라이선스가 필요하며 WildFire 모범 사례입니다.

**STEP 5 |** 구성을 커밋합니다.

**STEP 6 |** 다음 단계를 선택하십시오...

- 사용자가 SSL 복호화을 옵트아웃할 수 있도록 합니다.
- 특정 유형의 트래픽에 대한 복호화을 비활성화하도록 복호화 제외를 구성합니다.


©2023 Palo Alto Networks, Inc.

# SSH 프록시 구성

SSH 프록시 구성에는 인증서가 필요하지 않으며 SSH 세션을 해독하는 데 사용되는 키는 부팅하는 동안 방화벽에서 자동으로 생성됩니다. SSH 복호화이 활성화되면 방화벽은 SSH 트래픽을 복호화하고 복호화 정책 및 복호화 프로파일 설정에 따라 SSH 트래픽을 차단하거나 제한합니다. 트래픽은 방화벽을 나갈 때 다시 암호화됩니다.

*SSH* 프록시를 구성할 때 프록시된 트래픽은 *DSCP* 코드 포인트 또는 *QoS*를 지원하지 않습니다.

**STEP 1 |** 적절한 인터페이스가 가상 와이어, 레이어 2 또는 레이어 3 인터페이스로 구성된지 확인합니다. 암호 해독은 가상 와이어, 계층 2 또는 계층 3 인터페이스에서만 수행할 수 있습니다.

**Network** > **Interfaces** > **Ethernet** 탭에서 구성된 인터페이스를 봅니다. 인터페이스 유형 열은 인터페이스가 가상 와이어, 레이어 **2** 또는 레이어 **3** 인터페이스로 구성된 경우 표시됩니다. 인터페이스 유형을 포함하여 구성을 수정할 인터페이스를 선택할 수 있습니다.

**STEP 2 |** 방화벽이 암호를 해독할 트래픽을 정의하는 복호화 정책 규칙을 생성하고 SSH 트래픽에 검사를 적용하려면 복호화 프로파일을 생성합니다.

복호화 프로파일은 선택 사항이지만 각 복호화 정책 규칙에 복호화 프로파일을 포함하여 취약하고 취약한 프로토콜과 알고리즘이 네트워크에서 의심스러운 트래픽을 허용하지 않도록 하는 것이 가장 좋습니다.

1. 정책 > 암호 해독을 선택하고 기존 규칙을 추가 또는 수정하고 복호화할 트래픽을 정의합니다.
2. 옵션을 선택한 다음:
   - 규칙 작업을 일치하는 트래픽 복호화로 설정합니다.
   - 규칙 유형을 **SSH** 프록시로 설정합니다.
   - (선택 사항이지만 모범 사례) 기존 복호화 프로파일을 구성하거나 선택하여 복호화된 트래픽의 다양한 측면을 차단하고 제어합니다(예: 지원되지 않는 버전 및 지원되지 않는 알고리즘이 있는 세션을 종료하는 복호화 프로파일 생성).
3. 확인을 클릭하여 저장합니다.

**STEP 3 |** 구성을 커밋합니다.

**STEP 4 |** (선택 사항) 특정 유형의 트래픽에 대한 복호화를 비활성화하려면 복호화 제외를 계속합니다.


©2023 Palo Alto Networks, Inc.

# 복호화되지 않은 트래픽에 대한 서버 인증서 확인 구성

트래픽이 개인적이고 민감하거나 현지 법률 및 규정의 적용을 받기 때문에 복호화하지 않기로 선택한 트래픽에 대해 복호화 금지 정책을 생성합니다. 예를 들어 특정 임원의 트래픽이나 파이낸스 사용자와 개인 정보가 포함된 파이낸스 서버 간의 트래픽을 해독하지 않도록 선택할 수 있습니다. (고정된 인증서 또는 정책에 의한 상호 인증과 같은 기술적인 이유로 사이트에서 복호화를 중단하여 복호화할 수 없는 트래픽을 제외하지 마십시오. 대신 복호화 제외 목록에 호스트 이름을 추가하십시오.)

그러나 트래픽을 해독하지 않는다고 해서 네트워크에서 해독되지 않은 모든 트래픽을 허용해야 하는 것은 아닙니다. 만료된 인증서 및 신뢰할 수 없는 발급자가 있는 세션을 차단하려면 해독되지 않은 트래픽에 No Decryption 프로파일을 적용하는 것이 가장 좋습니다.

**STEP 1 |** 복호화되지 않은 트래픽을 식별하기 위한 복호화 정책 규칙을 생성하고 잘못된 세션을 차단하기 위해 복호화 프로파일을 생성합니다.

1. 정책 > 복호화를 선택한 다음 기존 규칙을 추가 또는 수정하여 복호화되지 않은 트래픽을 식별합니다.
2. 옵션을 선택한 다음:
   - 방화벽이 규칙과 일치하는 트래픽의 암호를 해독하지 않도록 규칙 작업을 복호화 없음으로 설정합니다.
   - 트래픽이 해독되지 않았기 때문에 규칙 유형을 무시하십시오.
   - (선택 사항이지만 모범 사례) 만료된 인증서 및 신뢰할 수 없는 인증서 발급자가 있는 세션을 차단하려면 기존 복호화되지 않은 트래픽에 대한 복호화 프로파일을 구성하거나 선택합니다.



방화벽이 암호화된 인증서 정보를 읽을 수 없어 인증서 검사를 수행할 수 없기 때문에 암호를 해독하지 않는 ***TLSv1.3*** 트래픽에 대한 복호화 정책에 ***No Decryption*** 프로파일을 연결하지 마십시오**.** 그러나 복호화 정책이 해당 트래픽을 제어하지 않는 한 복호화되지 않은 트래픽이 기록되지 않기 때문에 복호화하지 않는 ***TLSv1.3*** 트래픽에 대한 복호화 정책을 생성해야 합니다**.**

**STEP 2 |** 구성을 커밋합니다.

**STEP 3 |** 다음 단계를 선택합니다.

- 사용자가 SSL 복호화을 옵트아웃할 수 있도록 합니다.
- 특정 유형의 트래픽에 대한 복호화을 비활성화하도록 복호화 제외를 구성합니다.


©2023 Palo Alto Networks, Inc.

# 복호화 제외

복호화에서 두 가지 유형의 트래픽을 제외할 수 있습니다.

- 고정된 인증서, 불완전한 인증서 체인, 지원되지 않는 암호 또는 상호 인증(트래픽 복호화를 시도하면 트래픽이 차단됨)을 사용하는 등 기술적인 이유로 복호화를 중단하는 트래픽입니다. Palo Alto Networks는 다음과 같은 애플리케이션 및 서비스가 있는 호스트를 제외하는 사전 정의된 SSL 암호 해독 제외 목록(디바이스 > 인증서 관리 > **SSL** 암호 해독 제외)을 제공합니다. 기본적으로 SSL 복호화에서 기술적으로 복호화를 중단하는 것으로 알려져 있습니다. 기술적으로 복호화를 중단하고 SSL 복호화 제외 목록에 없는 사이트가 있는 경우 서버 호스트 이름별로 수동으로 목록에 추가할 수 있습니다. 방화벽은 사용자가 SSL 복호화 제외 목록에 추가하지 않는 한 애플리케이션 및 서비스가 기술적으로 복호화를 중단하는 사이트를 차단합니다.

  복호화 프로파일이 지원되지 않는 모드(클라이언트 인증, 지원되지 않는 버전 또는 지원되지 않는 암호 제품군이 있는 세션)를 허용하는 경우 방화벽은 허용되지 않는 모드를 사용하는 서버 및 애플리케이션을 로컬 SSL 복호화 제외 캐시(기기 > 인증서 관리 > **SSL** 복호화 제외 > 로컬 제외 캐시 표시)에 자동으로 추가합니다. 지원되지 않는 모드를 차단하면 보안이 강화되지만 해당 모드를 사용하는 애플리케이션과의 통신도 차단됩니다.
- 비즈니스, 규제, 개인적 또는 기타 이유로 인해 해독하지 않기로 선택한 트래픽(예: 금융 서비스, 의료 및 의료 또는 정부 트래픽). 소스, 대상, URL 카테고리 및 서비스를 기반으로 트래픽을 제외하도록 선택할 수 있습니다.

별표(*)를 와일드카드로 사용하여 도메인과 연결된 여러 호스트 이름에 대해 복호화 제외를 만들 수 있습니다. 별표는 URL 카테고리 예외에 대해 캐럿(^)이 동작하는 것과 동일한 방식으로 작동합니다. 각 별표는 호스트 이름에서 하나의 변수 하위 도메인(레이블)을 제어합니다. 이렇게 하면 매우 구체적이고 매우 일반적인 제외 항목을 모두 만들 수 있습니다. 예:

- mail.*.com은 mail.company.com과 일치하지만 mail.company.sso.com과 일치하지 않습니다.
- *.company.com은 도구.company.com과 일치하지만 일치하지 않습니다.
- *.*.company.com은 eng.tools.company.com과 일치하지만 eng.company.com과 일치하지 않습니다.
- *.*.*.company.com은 corp.exec.mail.company.com과 일치하지만 corp.mail.company.com과 일치하지 않습니다.
- mail.google.*은 mail.google.com과 일치하지만 mail.google.uk.com과 일치하지 않습니다.
- mail.google.*.*는 mail.google.co.uk와 일치하지만 mail.google.com과 일치하지 않습니다.

예를 들어 와일드카드를 사용하여 video-stats.video.google.com을 복호화에서 제외하고 video.google.com을 복호화에서 제외하지 않으려면 *.*.google.com을 제외합니다.



호스트 이름 앞에 있는 별표 와일드카드의 수*(*호스트 이름 앞에 와일드카드가 아닌 레이블 없음*)*에 관계없이 호스트 이름은 항목과 일치합니다*.* 예를 들어 ***.google.com, *.*.google.com*** 및 ***.*.*.google.com***은 모두 ***google.com***과 일치합니다*.* 그러나 하나의 레이블*(dev)*이 와일드카드가 아니기 때문에 ***.dev.*.google.com***은 ***google.com***과 일치하지 않습니다*.*

트래픽에 대한 가시성을 높이고 공격 노출 영역을 최대한 줄이려면 반드시 필요한 경우가 아니면 복호화 예외를 만들지 마십시오.

- Palo Alto Networks / 사전 정의된 복호화 제외


©2023 Palo Alto Networks, Inc.

- 기술적인 이유로 복호화에서 서버 제외
- 로컬 복호화 제외 캐시
- 정책 기반 복호화 제외 생성

## Palo Alto Networks / 사전 정의된 복호화 제외

방화벽은 고정된 인증서 및 상호 인증과 같은 기술적 이유로 인해 복호화를 중단하는 일반적으로 사용되는 사이트 복호화에서 제외할 사전 정의된 SSL 복호화 제외 목록을 제공합니다. 사전 정의된 복호화 제외는 기본적으로 활성화되며 Palo Alto Networks는 애플리케이션 및 위협 콘텐츠 업데이트(또는 위협 방지 라이선스가 없는 경우 애플리케이션 콘텐츠 업데이트)의 일부로 방화벽에 새롭고 업데이트된 사전 정의된 복호화 제외를 제공합니다. 방화벽은 사전 정의된 제외와 일치하는 트래픽을 복호화하지 않으며 해당 트래픽을 제어하는 보안 정책에 따라 암호화된 트래픽을 허용합니다. 그러나 방화벽은 암호화된 트래픽을 검사하거나 보안 정책을 적용할 수 없습니다.

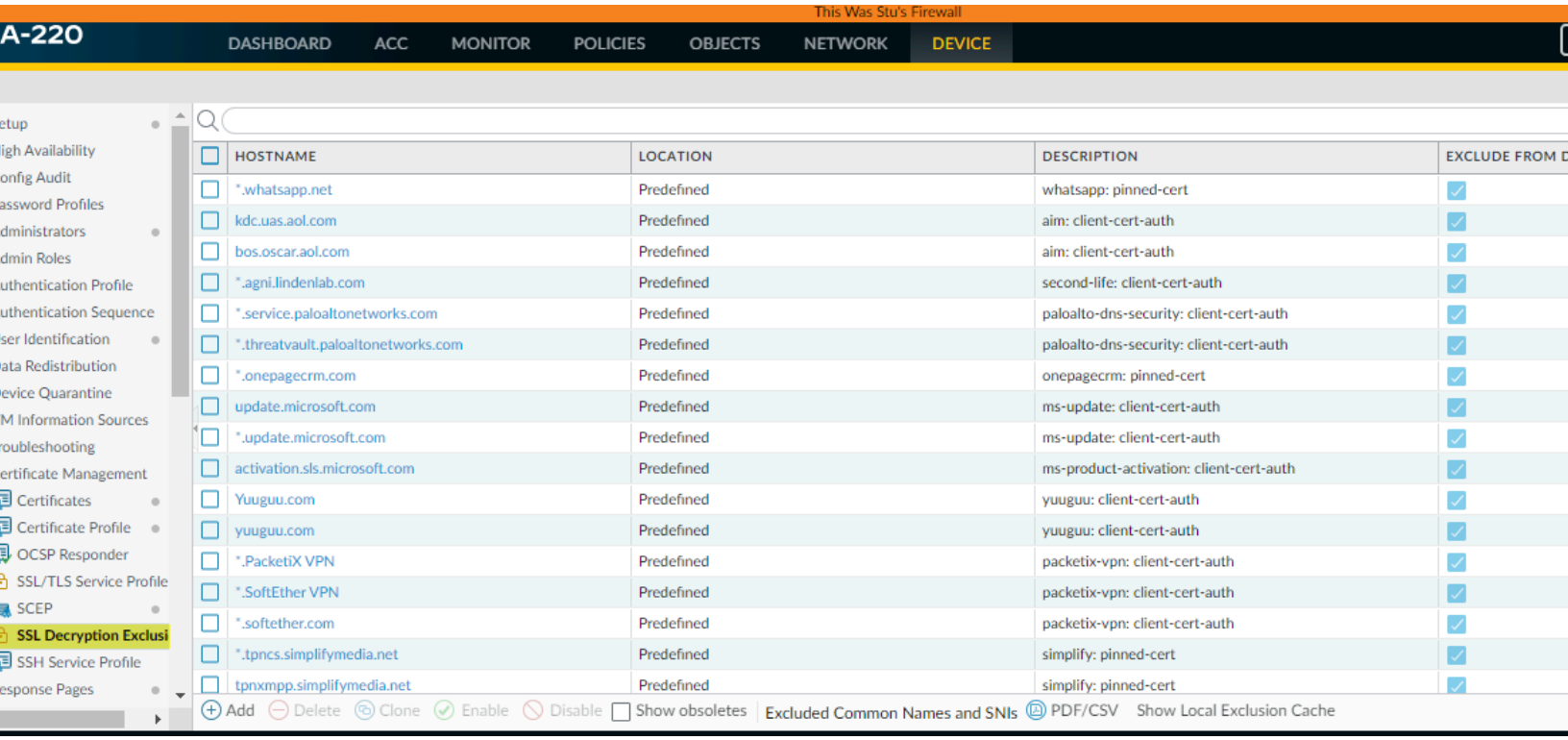


***SSL*** 복호화 제외 목록은 법적, 규제, 비즈니스, 개인정보 보호 또는 기타 임의적 이유로 복호화하지 않기로 선택한 사이트가 아니며 기술적으로 복호화를 중단한 사이트에만 해당됩니다*(*이 사이트의 암호를 복호화하면 트래픽이 차단됨*). IP* 주소, 사용자, *URL* 카테고리, 서비스 및 복호화하지 않기로 선택한 전체 영역과 같은 트래픽의 경우 정책 기반 복호화 제외를 생성합니다.

SSL 복호화 제외 목록의 사이트 트래픽은 암호화된 상태로 유지되므로 방화벽은 트래픽을 검사하거나 추가 보안 적용을 제공하지 않습니다. 사전 정의된 제외를 비활성화할 수 있습니다. 예를 들어 사전 정의된 제외를 비활성화하여 방화벽이 검사할 수 있는 애플리케이션 및 서비스만 허용하고 방화벽이 보안 정책을 적용할 수 있는 엄격한 보안 정책을 적용하도록 선택할 수 있습니다. 그러나 방화벽은 SSL 복호화 제외 목록에서 활성화되지 않은 경우 애플리케이션 및 서비스가 기술적으로 복호화를 중단하는 사이트를 차단합니다.

방화벽에서 직접 모든 Palo Alto Networks 사전 정의된 SSL 복호화 제외(디바이스 > 인증서 관리 > **SSL** 복호화 제외)를 보고 관리할 수 있습니다.


©2023 Palo Alto Networks, Inc.




**Hostname**에는 기술적으로 복호화를 중단하는 애플리케이션 또는 서비스가 있는 호스트의 이름이 표시됩니다. 또한 미리 설명된 목록에 없는 경우 기술적 이유로 서버를 복호화에서 제외하도록 호스트를 추가할 수도 있습니다.

설명은 방화벽이 사이트의 트래픽을 복호화할 수 없는 이유를 표시합니다(예: **pinned-cert**(고정된 인증서) 또는 **client-cert-auth**(클라이언트 인증)).

방화벽은 사용되지 않을 때 사전 정의된 SSL 복호화 제외를 자동으로 제거합니다(방화벽은 애플리케이션이 복호화로 지원될 때 이전에 복호화된 애플리케이션을 제거합니다). 사용하지 않는 항목 표시는 비활성화된 사전 정의된 제외 항목이 목록에 남아 있고 더 이상 필요하지 않은지 확인합니다. 방화벽은 목록에서 사전 정의된 복호화 제외를 자동으로 제거하지는 않지만 사용되지 않는 항목을 선택한 다음 삭제할 수 있습니다.

호스트 이름의 체크박스를 선택한 다음 사용하지 않도록 클릭하여 목록에서 사전 정의된 사이트를 제거할 수 있습니다. SSL 복호화 제외 목록을 기술적 이유로 복호화를 중단하는 사이트에 대해서만 사용하지 말고 복호화하지 않기로 선택한 사이트에 사용하지 마십시오.

## 기술적인 이유로 복호화에서 서버 제외

복호화가 기술적으로 중요한 애플리케이션 또는 서비스를 중단하는 경우(트래픽 복호화로 차단됨), 애플리케이션 또는 서비스를 호스팅하는 사이트의 호스트 이름을 Palo Alto Networks의 사전 정의된 SSL 복호화 제외 목록에 추가하여 맞춤형 복호화 예외를 생성할 수 있습니다. 방화벽은 트래픽이 암호화된 상태로 유지되기 때문에 SSL 복호화 제외 목록이 허용하는 트래픽에 대한 보안 정책을 복호화, 검사 및 시행하지 않습니다. 따라서 목록에 추가하는 사이트가 실제로 비즈니스에 필요한 애플리케이션이나 서비스가 있는 사이트인지 확인하십시오. 예를 들어, 일부 비즈니스 크리티컬 내부 사용자 지정 애플리케이션은 복호화를 중단할 수 있으며 방화벽이 암호화된 사용자 지정 애플리케이션 트래픽을 허용하도록 목록에 추가할 수 있습니다.


©2023 Palo Alto Networks, Inc.

> ***SSL*** 복호화 제외 목록은 법적, 규제, 비즈니스, 개인 정보 보호 또는 기타 임의적인 이유로 복호화를 선택하지 않은 사이트가 아니라 기술적으로 복호화를 중단한 사이트만을 위한 것입니다. 복호화를 선택하지 않은 트래픽(***IP*** 주소, 사용자, ***URL*** 카테고리, 서비스 및 전체 영역)의 경우 정책 기반 복호화 제외를 생성합니다.

사이트가 기술적으로 복호화를 중단하는 이유에는 고정된 인증서, 클라이언트 인증, 불완전한 인증서 체인 및 지원되지 않는 암호가 포함됩니다. HTTP 공개 키 고정(HPKP)의 경우 HPKP를 사용하는 대부분의 브라우저는 클라이언트에 엔터프라이즈 CA 인증서(또는 인증서 체인)를 설치하는 한 포워드 프록시 복호화를 허용합니다.

> 복호화에서 사이트를 제외하는 기술적인 이유가 불완전한 인증서 체인인 경우 차세대 방화벽은 브라우저처럼 체인을 자동으로 수정하지 않습니다. ***SSL*** 복호화 제외 목록에 사이트를 추가해야 하는 경우 사이트를 수동형으로 검토하여 합법적인 비즈니스 사이트인지 확인한 다음 누락된 하위 ***CA*** 인증서를 다운로드하고 방화벽에 로드 및 배포합니다.

SSL 복호화 제외 목록에 서버를 추가한 후 방화벽은 복호화 제외를 정의하는 데 사용하는 서버 호스트 이름을 클라이언트 헬로 메시지의 SNI(서버 이름 표시) 및 서버 인증서의 CN(일반 이름)과 비교합니다. SNI 또는 CN이 SSL 복호화 제외 목록의 항목과 일치하는 경우 방화벽은 복호화에서 트래픽을 제외합니다.

**STEP 1 |** 디바이스 > 인증서 관리 > **SSL** 복호화 제외를 선택합니다.

**STEP 2 |** 새 복호화 제외를 추가하거나 기존 사용자 지정 항목을 선택하여 수정합니다.

**STEP 3 |** 복호화에서 제외하려는 웹사이트 또는 애플리케이션의 호스트 이름을 입력합니다.

> 호스트 이름은 대소문자를 구분합니다.

와일드카드를 사용하여 도메인과 연결된 여러 호스트 이름을 제외할 수 있습니다. 방화벽은 서버가 도메인과 일치하는 CN을 복호화에서 제공하는 모든 세션을 제외합니다.

호스트 이름 필드가 각 사용자 정의 항목에 대해 고유한지 확인하십시오. 사전 정의된 제외가 사용자 정의 항목과 일치하는 경우 사용자 정의 항목이 우선합니다.

**STEP 4 |** (선택 사항) 다중 가상 시스템 방화벽의 모든 가상 시스템에서 제외를 공유하려면 공유를 선택합니다.

**STEP 5 |** 복호화에서 애플리케이션을 제외합니다. 또는 기존 복호화 제외를 수정하는 경우 이 체크박스의 선택을 취소하여 이전에 복호화에서 제외된 항목의 복호화를 시작할 수 있습니다.

**STEP 6 |** 확인을 클릭하여 새 제외 항목을 저장합니다.

## 로컬 복호화 제외 캐시

방화벽은 로컬 복호화 제외 캐시(디바이스 > 인증서 관리 > **SSL** 암호 해독 제외 > 로컬 제외 캐시 표시)에 서버를 추가할 수 있으며, 트래픽이 고정된 인증서 또는 지원되지 않는 인증서와 같은 기술적인 이유로 복호화를 중단하는 경우 해당 트래픽을 12시간 동안 복호화에서 자동으로 제외합니다. 복호화 프로파일에서 지원되지 않는 모드(클라이언트 인증을 사용하는 세션, 지원되지 않는 버전 또는 지원되지 않는 암호 모음)를 허용하고 허용된 트래픽이 지원되지 않는 모드를 사용하는 경우 디바이스는 자동으로 서버를 로컬 제외 캐시에 추가하고 복호화를 무시합니다. 트래픽이 암호화된 상태로 유지되기 때문에 방화벽은 로컬


©2023 Palo Alto Networks, Inc.

복호화 제외 캐시에서 허용하는 트래픽에 대해 보안 정책을 복호화, 검사 및 적용하지 않습니다. 지원되지 않는 모드를 허용하는 복호화 프로파일을 적용하여 복호화에서 제외하는 사이트가 비즈니스에 필요한 애플리케이션이나 서비스가 있는 사이트인지 확인합니다.

지원되지 않는 모드를 차단하면 보안을 강화하기 위해 해당 모드를 사용하는 애플리케이션과의 통신이 차단됩니다. 클라이언트 인증은 애플리케이션을 복호화에서 제외시키는 일반적인 이유입니다. 따라서 지원되지 않는 버전과 지원되지 않는 암호를 차단하고 복호화 프로파일에서 클라이언트 인증을 허용하는 것이 가장 좋습니다. 암호 해독 프로파일이 클라이언트 인증을 허용하는 경우 방화벽이 복호화할 수 없기 때문에 트래픽을 차단하는 대신 클라이언트가 인증을 요구하는 서버와 세션을 시작할 때 방화벽은 애플리케이션과 서버를 로컬 제외 캐시에 추가하고 트래픽을 허용합니다.



클라이언트 인증을 사용하고 SSL 복호화 제외 목록의 사전 정의된 사이트에 없는 사이트의 트래픽을 허용하는 경우 클라이언트 인증을 사용하는 세션을 허용하는 복호화 프로파일을 생성합니다. 애플리케이션을 호스트하는 서버에만 적용되는 복호화 정책 규칙에 프로파일을 추가합니다. 보안을 더욱 강화하려면 사용자 로그인 프로세스를 완료하기 위해 다단계 인증을 요구할 수 있습니다. 또는 명시적 복호화 정책을 사용하지 않고 사이트를 ***SSL*** 복호화 제외 목록에 추가하여 복호화를 건너뛸 수 있습니다.

방화벽은 애플리케이션 트래픽을 제어하는 복호화 정책 및 프로파일을 기반으로 로컬 SSL 복호화 제외 캐시 항목을 추가합니다. 복호화 프로파일에서 지원되지 않는 모드 검사를 차단하지 않으면 방화벽은 다음과 같은 경우에 로컬 SSL 복호화 제외 캐시에 항목을 추가합니다.

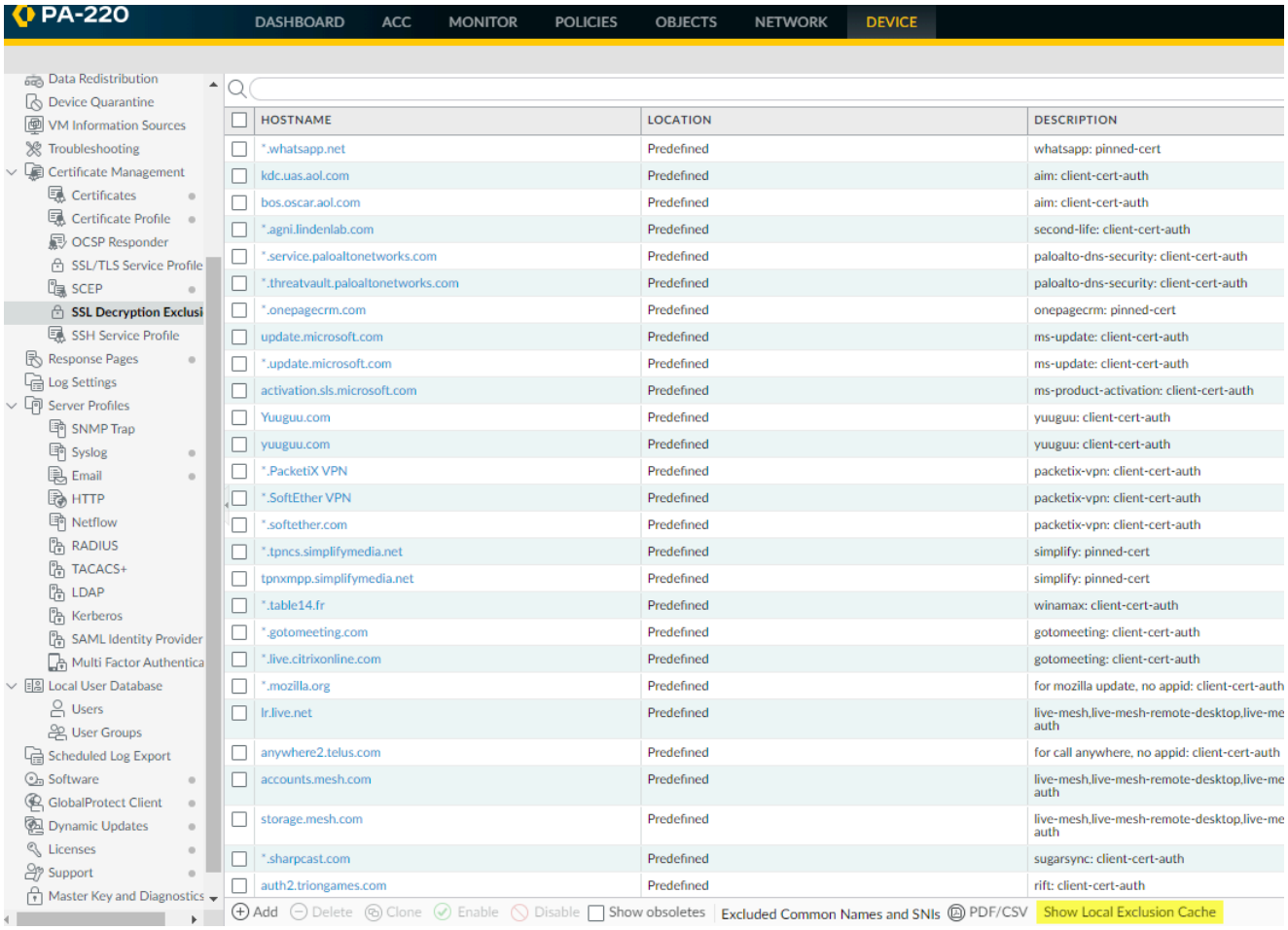
- 클라이언트는 TLSv1.2만 지원하며 서버는 TLSv1.3만 지원합니다. 로컬 캐시에서 이 제외에 대해 표시되는 이유는 SSL_UNSEPORTED입니다.
- 클라이언트는 TLSv1.3 및 TLSv1.2를 지원하며 서버는 TLSv1.2만 지원합니다. 이 경우 이유 열에 TLS13_UNSUPPORTED을 표시합니다.

  로컬 ***SSL*** 복호화 제외 캐시에 서버를 추가하는 이유가 ***TLS13_UNSPORTED***인 경우 방화벽은 프로토콜을 ***TLSv1.2***로 다운그레이드하고 방화벽이 트래픽을 복호화하고 검사합니다.
- 클라이언트는 서버가 지원하지 않는 특정 암호를 알립니다.
- 클라이언트는 서버가 지원하지 않는 특정 커브를 알립니다.

로컬 캐시에는 최대 1,024개의 항목이 포함됩니다. 로컬 SSL 복호화 제외 캐시에 로컬 제외를 수동으로 추가할 수는 없지만 SSL 복호화 제외 목록에 복호화 제외를 수동으로 추가할 수는 있습니다.

로컬 SSL 복호화 제외 캐시를 보려면 운용 관리자 또는 인증서 관리 액세스 권한이 있어야 합니다. 이를 보려면 디바이스 > 인증서 관리 > **SSL** 복호화 제외로 이동한 다음 화면 하단에 있는 로컬 제외 캐시 표시를 클릭합니다. 로컬 제외 캐시는 애플리케이션, 서버, 캐시에 포함되는 이유, 트래픽을 제어하는 복호화 프로파일 등을 각 항목에 대해 표시합니다. 로컬 캐시에서 항목을 수동으로 선택한 다음 삭제할 수 있습니다.


©2023 Palo Alto Networks, Inc.




CLI를 사용하여 캐시된 항목을 삭제할 수도 있습니다.

```
clear ssl-decrypt exclude-cache [server <value>] [application
 <value>]
```

로컬 캐시 항목이 만료되기 전에(12시간) 누군가 동일한 서버에 액세스하려고 하면 방화벽이 세션을 캐시 항목과 일치시키고 복호화를 무시하고 트래픽을 허용합니다. 복호화 정책 또는 프로파일을 변경하면 해당 변경 내용이 세션 분류에 영향을 줄 수 있으므로 방화벽은 로컬 제외 캐시를 플러시합니다. 캐시가 가득차면 새 항목이 도착함에 따라 방화벽이 가장 오래된 항목을 제거합니다.

## 정책 기반 복호화 제외 생성

정책 기반 복호화 제외는 복호화를 선택하지 않은 트래픽을 제외하기 위한 것입니다. 트래픽의 소스, 대상, 서비스 또는 URL 카테고리의 조합을 기반으로 정책 기반 복호화 제외를 생성할 수 있습니다. 해독하지 않도록 선택할 수 있는 트래픽의 예는 다음과 같습니다.

- 개인 식별 정보(PII) 또는 URL 필터링 카테고리 금융 서비스, 의료, 정부와 같은 기타 민감한 정보가 포함되어 있기 때문에 절대 해독해서는 안 되는 트래픽입니다.
- 트래픽이 해독되어서는 안 되는 경영진 또는 기타 사용자를 위해 발생하거나 대상으로 하는 트래픽입니다.
- 금융 서버와 같은 일부 디바이스는 복호화에서 제외해야 할 수 있습니다.


©2023 Palo Alto Networks, Inc.

- 비즈니스에 따라 일부 회사는 일부 애플리케이션의 경우 보안보다 개인 정보 보호 및 사용자 경험을 더 중요하게 생각할 수 있습니다.
- 일부 트래픽의 암호 해독을 금지하는 법률 또는 현지 규정.

  규정 및 법률 준수를 위해 트래픽을 복호화하지 않는 예는 유럽 연합(EU) GDPR(일반 데이터 보호 규정)입니다. EU GDPR은 모든 개인의 모든 개인 데이터를 강력하게 보호해야 합니다. GDPR은 EU 거주자의 개인 데이터를 수집하거나 처리하는 외국 회사를 포함한 모든 회사에 영향을 미칩니다.

  규정 및 규정 준수 규칙이 다르면 국가 또는 지역에 따라 동일한 데이터를 다르게 취급할 수 있습니다. 기업은 일반적으로 기업이 정보를 소유하기 때문에 기업 데이터 센터의 개인 정보를 해독할 수 있습니다. 가장 좋은 방법은 가능한 한 많은 트래픽을 해독하여 볼 수 있고 보안 보호를 적용하는 것입니다.

사전 정의된 URL 카테고리를 사용하여 전체 웹사이트 카테고리를 복호화에서 제외할 수 있으며, 사용자 정의 URL 카테고리를 생성하여 복호화하지 않으려는 URL의 사용자 정의 목록을 정의하거나 외부 동적 목록(EDL)을 만들어 암호 해독을 원하지 않는 맞춤 URL 목록을 정의할 수 있습니다.

IP 주소가 동적으로 변경되는 Office 365와 같은 환경이나 복호화에서 제외하려는 URL 목록을 자주 변경하는 환경에서는 URL 카테고리 대신 EDL을 사용하여 제외된 URL을 지정하는 것이 더 나은 경우가 많습니다. EDL을 편집하면 커밋 없이 URL 카테고리가 동적으로 변경되지만 사용자 지정 URL 카테고리를 편집하려면 커밋이 적용되어야 하기 때문에 EDL을 사용하면 동적 환경에서 덜 방해가 됩니다.

하나의 복호화 정책 규칙이 허용하도록 선택한 암호화된 트래픽을 제어하도록 복호화하지 않기로 선택한 모든 카테고리가 포함된 ***EDL*** 또는 사용자 지정 ***URL*** 카테고리를 생성합니다. 규칙에 비복호화 프로파일을 적용합니다. ***EDL*** 또는 사용자 지정 ***URL*** 카테고리에 카테고리를 추가하는 기능을 사용하면 복호화에서 트래픽을 쉽게 제외할 수 있고 규칙 베이스를 깨끗하게 유지하는 데 도움이 됩니다.

보안 정책 규칙과 유사하게 방화벽은 들어오는 트래픽을 정책 규칙 베이스의 순서에 따라 복호화 정책 규칙과 비교합니다. 규칙 베이스 상단에 복호화 제외 규칙을 배치하여 민감한 트래픽이나 법률 및 규정에서 복호화를 금지하는 트래픽을 실수로 복호화하는 것을 방지합니다.

정책 기반 복호화 제외를 생성하는 경우 다음 제외 규칙을 복호화 규칙 베이스의 맨 위에 다음 순서로 배치하는 것이 가장 좋습니다.

1. 민감한 대상 서버에 대한 IP 주소 기반 예외.
2. 경영진 및 기타 사용자 또는 그룹에 대한 소스 사용자 기반 예외.
3. 도착 URL에 대한 맞춤 URL 또는 EDL 기반 예외
4. 금융 서비스, 건강 및 의료, 정부와 같은 전체 카테고리의 도착 URL에 대해 사전 정의된 민감한 URL 카테고리 기반 예외.

복호화 규칙 베이스에서 이러한 규칙 뒤에 트래픽을 복호화하는 규칙을 배치하십시오.


©2023 Palo Alto Networks, Inc.

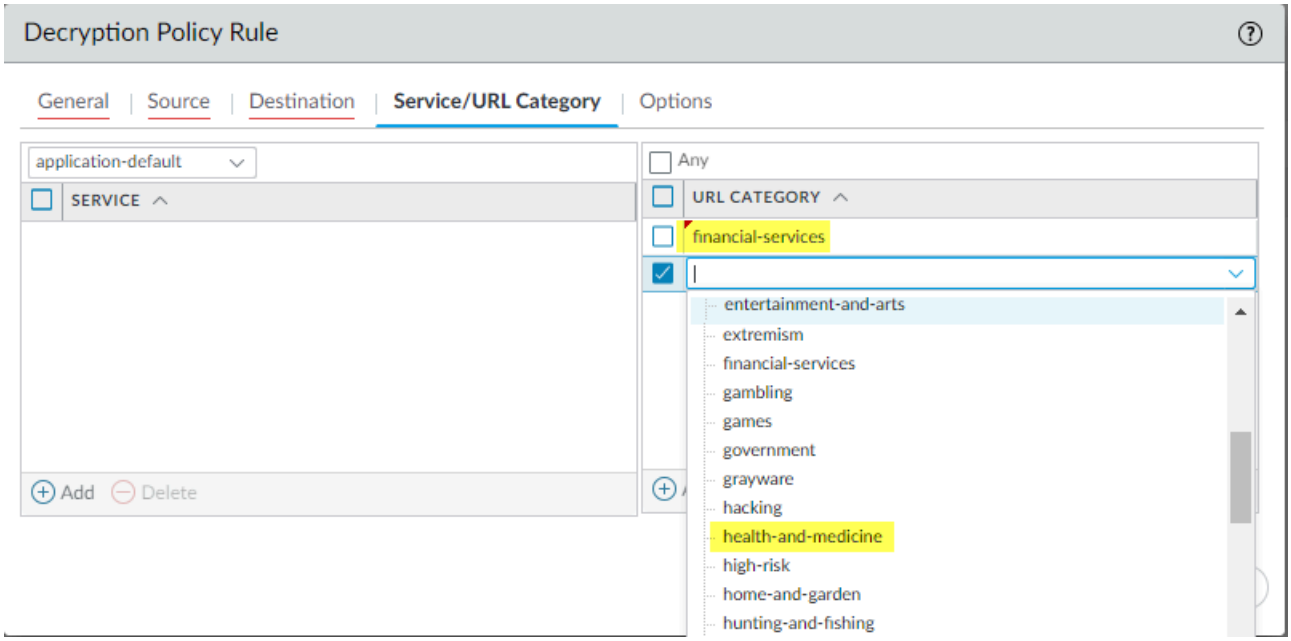
**STEP 1 |** 일치 기준에 따라 복호화에서 트래픽을 제외합니다.

이 예는 SSL Forward Proxy 복호화에서 재무 또는 건강 관련으로 분류된 트래픽을 제외하는 방법을 보여줍니다.

1. 정책 > 암호 해독 및 추가를 선택하거나 암호 해독 정책 규칙을 수정합니다.
2. 복호화에서 제외할 트래픽을 정의합니다.

   이 예에서:

   1. 규칙에 No-Decrypt-Finance-Health와 같은 설명이 포함된 이름을 지정합니다.
   2. 외부 서버로 향하는 모든 SSL 트래픽에 No-Decrypt-Finance-Health 규칙을 적용하려면 **Source** 및 **Destination**을 **Any**로 설정합니다.
   3. **URL** 카테고리를 선택한 다음 URL 카테고리 금융 서비스 및 건강 및 의학을 추가합니다.




3. 옵션을 선택하고 규칙을 복호화 안 함으로 설정합니다.
4. (선택 사항이지만 모범 사례) 방화벽이 암호를 해독하지 않는 세션에 대한 인증서의 유효성을 검사하려면 비복호화 프로파일을 생성하고 규칙에 연결합니다. 프로파일을 만료된 인증서가 있는 세션 차단 및 신뢰할 수 없는 발급자가 있는 세션 차단으로 구성합니다.

   예외: 방화벽이 암호화된 인증서 정보를 읽을 수 없어 인증서 검사를 수행할 수 없기 때문에 암호를 해독하지 않는 *TLSv1.3* 트래픽에 대한 복호화 정책에 *No Decryption* 프로파일을 연결하지 마십시오. 그러나 복호화 정책이 해당 트래픽을 제어하지 않는 한 복호화되지 않은 트래픽이 기록되지 않기 때문에 복호화하지 않는 *TLSv1.3* 트래픽에 대한 복호화 정책을 생성해야 합니다.
5. 확인을 클릭하여 No-Decrypt-Finance-Health 복호화 규칙을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 복호화 정책 규칙 베이스의 맨 위에 복호화 제외 규칙을 배치합니다.

방화벽은 규칙 베이스 시퀀스에서 들어오는 트래픽에 대해 복호화 규칙을 적용하고 트래픽과 일치하는 첫 번째 규칙을 적용합니다.

**No-Decrypt-Finance-Health** 정책(**Decryption** > **Policies**)을 선택한 다음 목록 맨 위에 나타날 때까지 위로 이동을 클릭하거나 규칙을 끌어다 놓습니다.

**STEP 3 |** 구성을 저장합니다.

커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 개인 키 내보내기 차단

PAN-OS 또는 Panorama에서 인증서를 생성하거나 가져올 때 인증서에 대한 개인 키 내보내기를 영구적으로 차단할 수 있습니다. PAN-OS 디바이스에서 개인 키 내보내기를 차단하면 악의적인 관리자나 기타 악의적인 행위자가 키를 오용하는 것을 방지하기 때문에 보안 태세가 강화됩니다. 인증서 관리를 포함하는 역할을 가진 관리자는 개인 키 내보내기를 차단할 수 있습니다. 디바이스에 이미 있는 키는 차단할 수 없습니다. 키를 생성하거나 PAN-OS로 가져올 때만 키를 차단할 수 있습니다.

관리자가 개인 키 내보내기를 차단하면 운용 관리자를 비롯한 어떤 관리자도 해당 키를 내보낼 수 없습니다. PAN-OS 어플라이언스에서 개인 키를 내보내야 하는 경우 개인 키 내보내기를 차단하는 옵션을 선택하지 않고 인증서와 키를 다시 생성하십시오.

이전 버전의 PAN-OS로 다운그레이드하려면 먼저 개인 키가 차단된 인증서를 삭제해야 합니다. 다운그레이드를 시도하기 전에 개인 키가 차단된 인증서를 삭제하지 않으면 해당 인증서를 삭제하라는 오류 메시지가 표시됩니다. 삭제할 때까지 다운그레이드할 수 없습니다. 다운그레이드한 후 필요한 경우 삭제된 인증서를 다시 가져오거나 다시 생성하십시오.

엔터프라이즈 ***PKI***(공개 키 인프라)를 사용하여 인증서 및 개인 키를 생성하는 경우 엔터프라이즈 ***CA***(인증 기관)에서 새 방화벽 및 ***Panorama***에 설치할 수 있으므로 ***PAN-OS***에서 개인 키 내보내기를 차단하여 내보낼 이유가 없습니다.

방화벽 또는 ***Panorama***에서 자체 서명된 인증서를 생성하고 개인 키 내보내기 차단 옵션을 적용하면 인증서와 키를 다른 ***PAN-OS*** 어플라이언스로 내보낼 수 없습니다.

개인 키 내보내기를 차단하더라도 디바이스 상태(디바이스 > 설정 > 작업)를 내보내고 가져올 수 있습니다. 디바이스 상태 가져오기 및 내보내기에 개인 키를 포함하지만 관리자는 이를 읽거나 디코딩할 수 없습니다.

마스터 키가 두 방화벽에서 동일한 경우 다른 방화벽에서 한 방화벽의 구성을 가져오거나 로드할 수 있습니다. 방화벽에서 마스터 키가 다른 경우 구성 가져오기 또는 로드가 작동하지 않고 인증서를 읽는 동안 커밋이 실패합니다.

- 개인 키 생성 및 차단
- 개인 키 가져오기 및 차단
- IKE 게이트웨이에 대한 프라이빗 키 가져오기 및 차단
- 개인 키 차단 확인

## 개인 키 생성 및 차단

인증서를 생성한 후 오용을 방지하기 위해 개인 키의 내보내기를 차단합니다.

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

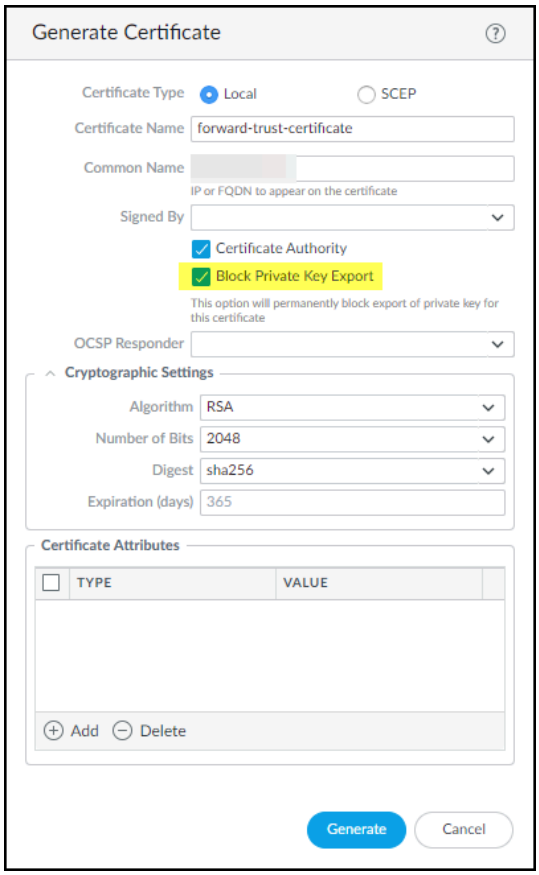
두 개 이상의 가상 시스템이 있는 경우 인증서의 위치 또는 공유를 선택합니다.

**STEP 2 |** 인증서를 생성합니다.

**STEP 3 |** 개인 키 내보내기 차단을 선택하여 사람이 인증서를 내보내지 못하도록 합니다.

 ©2023 Palo Alto Networks, Inc.

다른 인증서 필드에 대한 정보는 인증서 생성을 참조하십시오.




**STEP 4 |** 생성을 클릭하여 새 인증서를 생성합니다.

작동 *CLI* 명령을 사용하여 인증서를 생성하고 개인 키 내보내기를 차단할 수도 있습니다.

```
admin@pa-220> request certificate generate block-private-keys yes
```

앞의 *CLI* 명령에는 표시되지 않은 인증서 및 기타 매개 변수도 포함될 수 있습니다.

## 개인 키 가져오기 및 차단

인증서를 불러온 후 오용되지 않도록 개인 키 내보내기를 차단합니다.

**STEP 1 |** 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.

두 개 이상의 가상 시스템이 있는 경우 인증서의 위치 또는 공유를 선택합니다.

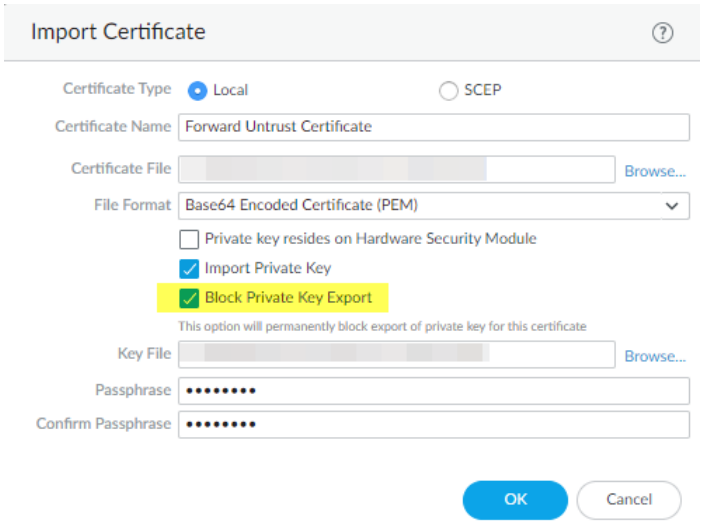
**STEP 2 |** 인증서를 가져옵니다.

**STEP 3 |** 개인 키 가져오기를 선택하여 개인 키 내보내기를 차단하는 옵션을 활성화합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 개인 키 내보내기 차단을 선택하여 사람이 인증서를 내보내지 못하도록 합니다.

다른 인증서 가져오기 필드에 대한 자세한 내용은 인증서 및 개인 키 가져오기를 참조하십시오.




**STEP 5 |** 확인을 클릭하여 인증서를 가져옵니다.

*SCP* 운영 *CLI* 명령을 사용하여 인증서를 가져오거나 인증서에 대한 개인 키를 가져오는 경우에도 개인 키의 내보내기를 차단할 수 있습니다.

- ***admin@pa-220> scp import private-key block-private-key ...***

앞의 각 *CLI* 명령에는 원본, 인증서 이름 및 표시되지 않는 기타 매개 변수를 지정하는 키워드가 포함될 수도 있습니다.

*SCP* 작업 *CLI* 명령을 사용하여 인증서를 내보내고 개인 키를 포함하는 경우(***scp export certificate passphrase <phrase> remote-port <1-65536> to <destination> certificate-name <name> include-key <yes | no>*** 형식 ***<der | pem | pkcs10 | pkcs12>***), 인증서의 개인 키가 차단되면 차단된 개인 키를 내보낼 수 없기 때문에 명령이 실패하고 오류 메시지를 반환합니다.

## IKE 게이트웨이에 대한 프라이빗 키 가져오기 및 차단

IKE 게이트웨이 인증용 인증서를 생성한 후 개인 키의 오용을 방지하기 위해 개인 키 내보내기를 차단합니다.

**STEP 1 |** 네트워크 > 네트워크 프로파일 > **IKE** 게이트웨이를 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 새 IKE 게이트웨이를 추가합니다.

**STEP 3 |** 일반 탭에서 인증에 대해 인증서를 선택합니다.

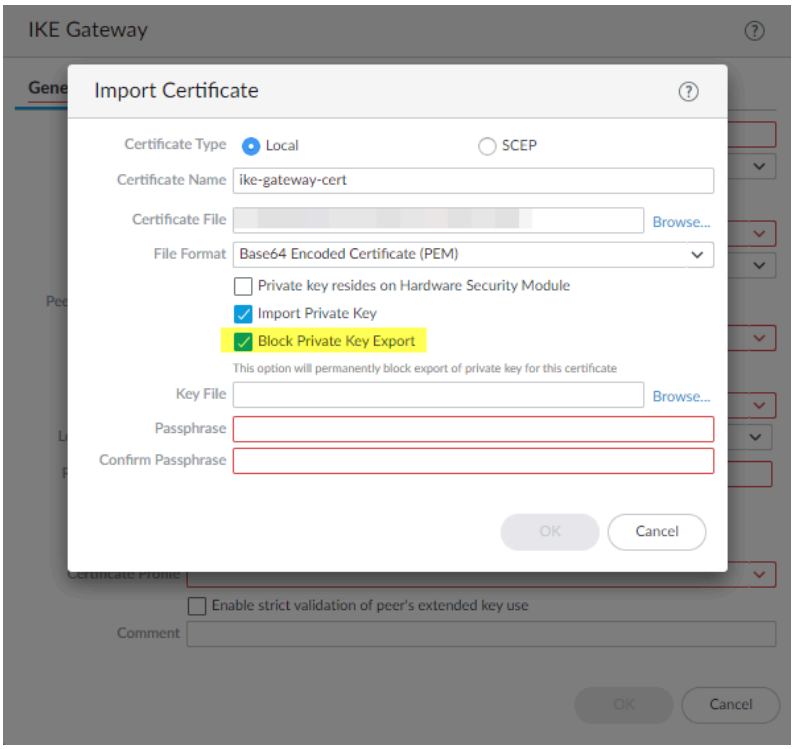
**STEP 4 |** 로컬 인증서의 경우 기존 인증서를 가져오거나 인증서를 생성할지 여부에 따라 가져오기 또는 생성을 선택합니다.

**STEP 5 |** 인증서 정보를 입력합니다. 인증서를 가져오는 경우 개인 키 가져오기를 선택하여 개인 키 내보내기 차단 확인란을 활성화합니다.

 ©2023 Palo Alto Networks, Inc.

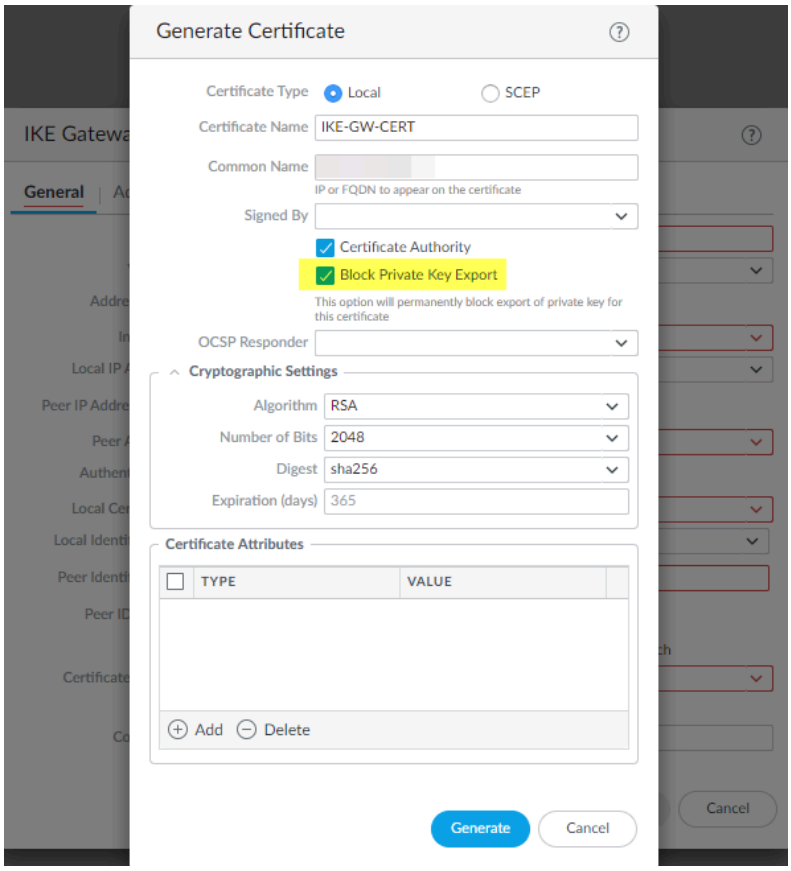
**STEP 6 |** 다른 사람이 키를 내보내지 못하도록 하려면 개인 키 내보내기 차단을 선택합니다.

인증서를 가져오려면 암호를 입력하고 확인한 다음 확인을 클릭합니다.




인증서를 생성하려면 생성을 클릭합니다.


©2023 Palo Alto Networks, Inc.



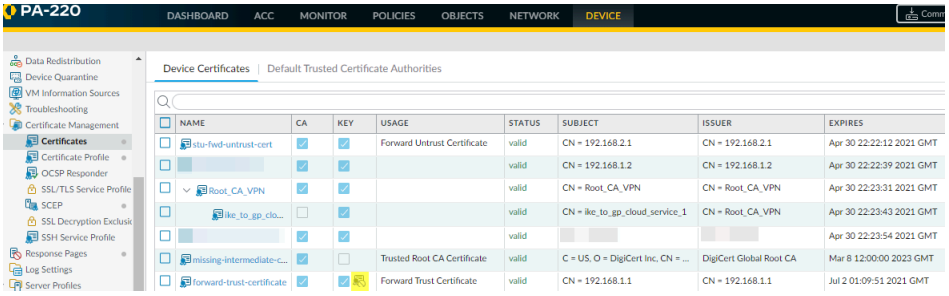

**STEP 7 |** 암호를 입력하고 확인한 다음 확인을 클릭합니다.

## 개인 키 차단 확인

여러 가지 방법으로 개인 키 내보내기가 차단되었는지 확인할 수 있습니다.

- 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서의 키 열을 확인하십시오.

  이 예에서는 forward-trust-certificate가 차단됩니다.




- 개인 키 내보내기가 차단된 인증서를 내보내려고 하면 개인 키 내보내기 확인란을 사용할 수 없으며 키를 내보낼 수 없고 인증서만 내보낼 수 있습니다.


©2023 Palo Alto Networks, Inc.

- 다음 작동 CLI 명령을 사용하여 내보내기가 차단된 개인 키가 있는 디바이스 또는 특정 Vsys의 모든 인증서를 나열합니다.

```
admin@pa-220> request certificate show-blocked <shared | vsys>
```

- 다음 작동 CLI 명령을 사용하여 특정 인증서의 개인 키 내보내기가 차단되었는지 확인하십시오.

```
admin@pa-220> request certificate is-blocked certificate-name
 <name>
```

인증서가 내보내기에서 차단된 경우 명령은 **yes** 를 반환하고 인증서가 차단되지 않으면 명령은 **no**를 반환합니다.


©2023 Palo Alto Networks, Inc.

# 사용자가 SSL 복호화를 옵트아웃할 수 있도록 설정

개인 정보에 민감한 상황에서는 방화벽이 특정 웹 트래픽을 복호화하고 있음을 사용자에게 알리고 트래픽이 복호화되었음을 이해하고 사이트를 계속 방문하도록 허용하거나 세션을 종료하고 웹사이트로 이동하지 못하도록 차단할 수 있습니다. (사이트로 이동하여 복호화를 피할 수 있는 옵션이 없습니다.)

사용자가 복호화 정책과 일치하는 HTTPS 사이트 또는 애플리케이션을 처음 탐색하려고 하면 방화벽에서 세션 암호를 복호화할 것임을 알리는 응답 페이지를 표시합니다. 사용자는 예를 클릭하여 복호화를 허용하고 사이트로 계속 이동하거나 아니오를 클릭하여 복호화를 선택 해제하고 세션을 종료할 수 있습니다. 복호화 허용 선택은 사용자가 다음 24시간 동안 액세스를 시도하는 모든 HTTPS 사이트에 적용되며, 그 후 방화벽은 응답 페이지를 다시 표시합니다. SSL 복호화를 선택 해제한 사용자는 다음 1분 동안 요청한 웹 페이지 또는 다른 HTTPS 사이트에 액세스할 수 없습니다. 1분이 경과한 후 방화벽은 다음에 사용자가 HTTPS 사이트에 액세스를 시도할 때 응답 페이지를 다시 표시합니다.

방화벽에는 활성화할 수 있는 사전 정의된 SSL 복호화 옵트아웃 페이지가 포함되어 있습니다. 선택적으로 본인의 텍스트 및/또는 이미지로 페이지를 사용자 정의할 수 있습니다. 그러나 가장 좋은 방법은 사용자가 복호화를 선택 해제하도록 허용하지 않는 것입니다.



지원되는 최대 크기보다 큰 사용자 지정 응답 페이지는 해독되거나 사용자에게 표시되지 않습니다. *PAN-OS 8.1.2* 및 이전 *PAN-OS 8.1* 릴리스에서 해독된 사이트의 사용자 지정 응답 페이지는 *8,191*바이트를 초과할 수 없습니다. 최대 크기는 *PAN-OS 8.1.3* 및 이후 릴리스에서 *17,999*바이트로 증가합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** (선택 사항) SSL 암호 해독 옵트아웃 페이지를 사용자 지정합니다.

1. 디바이스 > 응답 페이지를 선택합니다.
2. **SSL** 암호 해독 옵트아웃 페이지 링크를 선택합니다.
3. 사전 정의된 페이지를 선택한 다음 내보내기를 클릭합니다.
4. 원하는 HTML 텍스트 편집기를 사용하여 페이지를 편집합니다.
5. 이미지를 추가하려면 최종 사용자 시스템에서 액세스할 수 있는 웹 서버에서 이미지를 호스팅하십시오.
6. 이미지를 가리키도록 HTML에 줄을 추가합니다. 예:

```
<img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?1382722588"/>
```

7. 편집한 페이지를 새 파일 이름으로 저장합니다. 페이지가 UTF-8 인코딩을 유지했는지 확인합니다.
8. 방화벽으로 돌아가 디바이스 > 응답 페이지를 선택합니다.
9. **SSL** 암호 해독 옵트아웃 페이지 링크를 선택합니다.
10. 가져오기를 클릭한 다음 파일 가져오기 필드에 경로와 파일 이름을 입력하거나 파일을 찾아봅니다.
11. (선택사항) 대상 드롭다운에서 이 로그인 페이지가 사용되는 가상 시스템을 선택하거나 공유를 선택하여 모든 가상 시스템에서 사용할 수 있도록 합니다.
12. 확인을 클릭하여 파일을 가져옵니다.
13. 방금 불러온 응답 페이지를 선택한 다음 닫기를 클릭합니다.

**STEP 2 |** SSL 복호화 옵트아웃을 활성화합니다.

1. 디바이스 > 응답 페이지 페이지에서 비활성화됨 링크를 클릭합니다.
2. **SSL** 옵트아웃 페이지 활성화를 선택한 다음 확인을 클릭합니다.
3. 변경 사항을 커밋합니다.

**STEP 3 |** 사이트 탐색을 시도할 때 옵트 아웃 페이지가 표시되는지 확인합니다.

브라우저에서 복호화 정책과 일치하는 암호화된 사이트로 이동합니다.

SSL 복호화 옵트아웃 응답 페이지가 표시되는지 확인합니다.




 ©2023 Palo Alto Networks, Inc.

# 일시적으로 SSL 복호화 사용 안 함

경우에 따라 SSL 복호화를 일시적으로 비활성화할 수 있습니다. 예를 들어 SSL 복호화를 급하게 배포했는데 뭔가 제대로 작동하지 않지만 그것이 무엇인지 확실하지 않고 검사해야 할 규칙이 많은 경우 CLI를 사용하여 일시적으로 복호화를 끄고 스스로 문제를 분석하고 해결하는 시간을 가질 수 있습니다. 문제를 해결한 후 CLI를 사용하여 SSL 복호화를 다시 켤 수 있습니다. CLI를 사용하여 복호화를 일시적으로 비활성화한 다음 다시 활성화하는 데 커밋 작업이 필요하지 않기 때문에 네트워크 트래픽을 방해하지 않고 수행할 수 있습니다.

다음 CLI 명령은 커밋 없이 SSL 복호화를 일시적으로 비활성화하고 커밋 없이 복호화를 다시 활성화합니다.

*SSL* 복호화를 비활성화하는 명령은 재부팅 후 구성에서 지속되지 않습니다. 일시적으로 복호화를 해제한 후 방화벽을 재부팅하면 문제 해결 여부와 상관없이 복호화가 다시 켜집니다.

- SSL 복호화 비활성화

```
시스템 설정 SSL 암호 해독 건너 뛰기-SSL 암호 해독 예
```

- SSL 복호화 재활성화

```
시스템 설정 SSL 암호 해독 건너 뛰기-SSL 암호 해독 예
```


©2023 Palo Alto Networks, Inc.

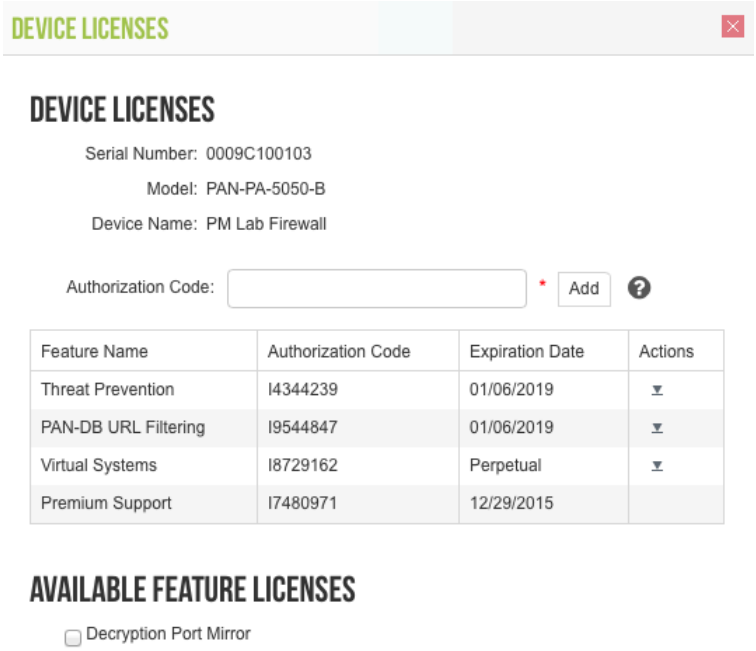
# 복호화 포트 미러링 구성

복호화 미러링을 활성화하려면 먼저 복호화 포트 미러 라이선스를 가져오고 설치해야 합니다. 라이선스는 무료이며 다음 절차에 설명된 대로 지원 포털을 통해 활성화할 수 있습니다. 복호화 포트 미러 라이선스를 설치하고 방화벽을 재부팅한 후 복호화 포트 미러링을 활성화할 수 있습니다.

특정 국가에서 SSL 트래픽의 복호화, 저장, 검사 및/또는 사용이 규제되며 복호화 미러 기능을 사용하기 위해서는 사용자 동의가 필요할 수 있습니다. 또한 이 기능을 사용하면 방화벽에 대한 관리 액세스 권한이 있는 악의적인 사용자가 암호화된 채널을 사용하여 제출된 사용자 이름, 암호, 주민등록 번호, 신용카드 번호 또는 기타 중요한 정보를 수집할 수 있습니다. Palo Alto Networks는 프로덕션 환경에서 이 기능을 활성화하고 사용하기 전에 기업 변호사와 상의할 것을 권장합니다.

**STEP 1 |** 복호화 포트 미러링을 사용하도록 설정하려는 각 방화벽에 대한 라이선스를 요청합니다.

1. Palo Alto Networks 고객 지원 웹 사이트에 로그인하고 자산 탭으로 이동합니다.
2. 라이선스를 부여하고 작업을 선택하려는 방화벽의 항목을 선택합니다.
3. 복호화 포트 미러를 선택합니다. 법적 공지가 표시됩니다.
4. 잠재적인 법적 의미와 요구 사항에 대해 명확 하고 여전히 복호화 포트 미러링을 설정 하려는 경우, 이해했으며**,** 진행하겠습니다를 클릭합니다.
5. 활성화를 클릭합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽에 복호화 포트 미러 라이선스를 설치합니다.

1. 방화벽 웹 인터페이스에서 디바이스 > 라이선스를 선택합니다.
2. 라이선스 서버에서 라이선스 키 검색을 클릭합니다.
3. 방화벽에서 라이선스가 활성화되었는지 확인합니다.




4. 방화벽을 재부팅합니다(디바이스 > 설정 > 작업). 이 기능은 PAN-OS가 다시 로드될 때까지 구성에 사용할 수 없습니다.

**STEP 3 |** 방화벽이 암호 해독된 트래픽을 전달하도록 설정합니다. 이 단계를 수행하려면 수퍼유저 권한이 필요합니다.

단일 가상 시스템이 있는 방화벽의 경우**:**

1. 디바이스 > 설정 > 콘텐츠 **ID**를 선택합니다.
2. 복호화된 콘텐츠 포워딩 허용 체크박스를 선택합니다.
3. 확인을 클릭하여 저장합니다.

여러 가상 시스템이 있는 방화벽의 경우**:**

1. 디바이스 > 가상 시스템을 선택합니다.
2. 추가를 선택하여 가상 시스템을 선택하여 새 가상 시스템을 편집하거나 생성합니다.
3. 복호화된 콘텐츠 포워딩 허용 체크박스를 선택합니다.
4. 확인을 클릭하여 저장합니다.

**STEP 4 |** 복호화 미러링에 이더넷 인터페이스를 사용하도록 설정합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택합니다.
2. 복호화 포트 미러링을 위해 구성할 이더넷 인터페이스를 선택합니다.
3. 인터페이스 유형으로 미러 복호화를 선택합니다.

   이 인터페이스 유형은 복호화 포트 미러 라이선스가 설치된 경우에만 나타납니다.
4. 확인을 클릭하여 저장합니다.

**STEP 5 |** 해독된 트래픽의 미러링을 사용하도록 설정합니다.

1. 개체 > 복호화 프로파일을 선택합니다.
2. 복호화 미러링에 사용할 인터페이스를 선택합니다.

   인터페이스 드롭다운에는 다음과 같은 유형으로 정의된 모든 이더넷 인터페이스가 포함되어 있습니다. 미러를 복호화합니다.
3. 정책 적용 전이나 후에 해독된 트래픽을 미러로 할지의 여부를 지정합니다.

   기본적으로 방화벽은 보안 정책 조회 전에 해독된 모든 트래픽을 인터페이스로 미러로 설정하므로 이벤트를 재생하고 위협을 발생시키거나 드롭 액션을 트리거하는 트래픽을 분석할 수 있습니다. 보안 정책 적용 후 해독된 트래픽만 미러로 표시하려면 포워딩 전용 체크박스를 선택합니다.


©2023 Palo Alto Networks, Inc.

이 옵션을 사용하면 방화벽을 통해 포워딩되는 트래픽만 미러됩니다. 이 옵션은 복호화된 트래픽을 DLP 디바이스 또는 다른 IPS(침입 방지 시스템)와 같은 다른 위협 탐지 디바이스로 포워딩하는 경우에 유용합니다.

4. 확인을 클릭하여 복호화 프로파일을 저장합니다.

**STEP 6 |** 복호화 프로파일 규칙(복호화 포트 미러링이 활성화된)을 복호화 정책 규칙에 첨부합니다. 정책 규칙에 따라 해독된 모든 트래픽은 미러링됩니다.

1. 정책 > 복호화를 선택합니다.
2. 추가를 클릭하여 복호화 정책을 구성하거나 기존 복호화 정책을 선택하여 편집합니다.
3. 옵션 탭에서 복호화 및 4단계에서 만든 복호화 프로파일을 선택합니다.
4. 확인을 클릭하여 정책을 저장합니다.

**STEP 7 |** 구성을 저장합니다.

커밋을 클릭합니다.

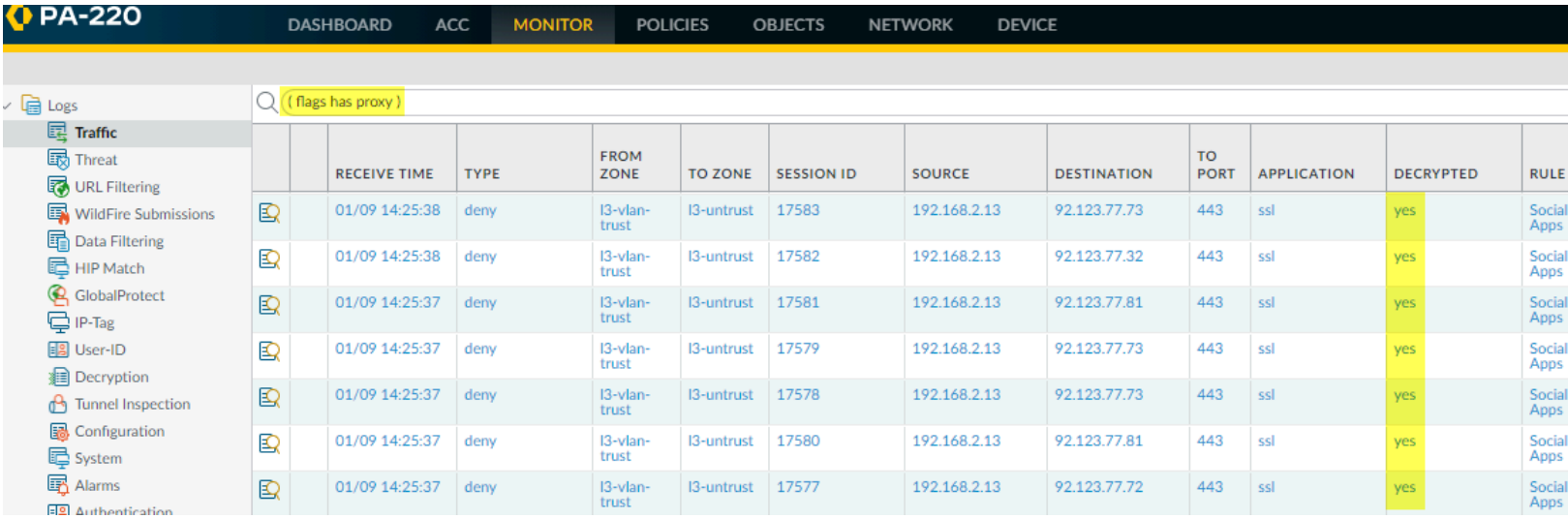
 ©2023 Palo Alto Networks, Inc.

# 복호화 확인

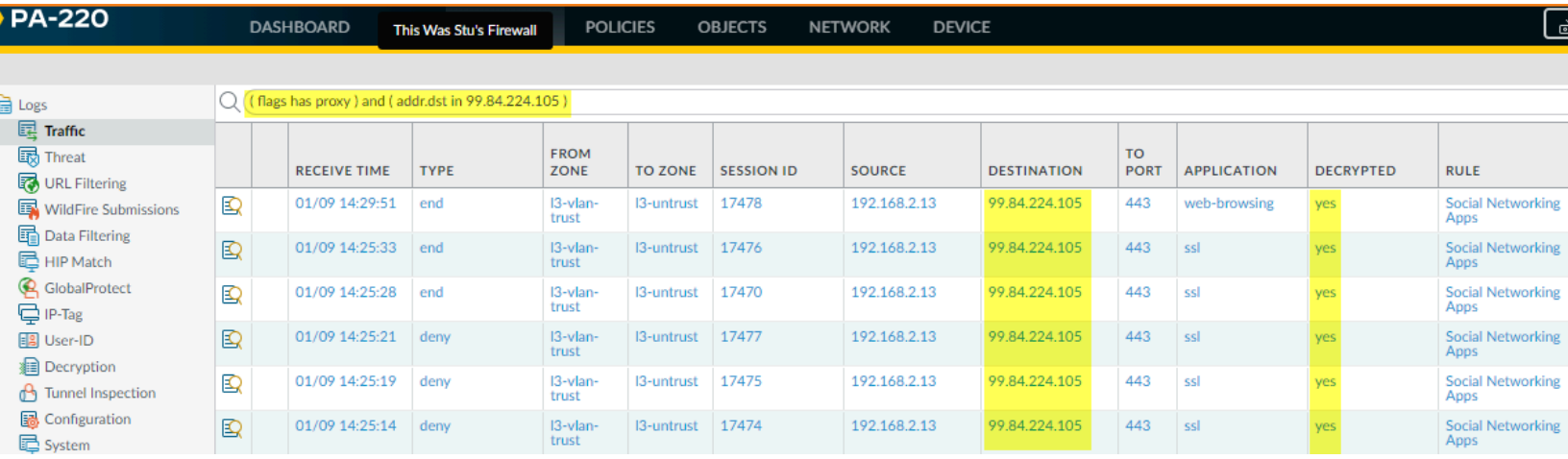
모범 사례 복호화 프로파일을 구성하고 트래픽에 적용한 후에는 암호화 로그(PAN-OS 10.0에서 도입)와 트래픽 로그를 모두 확인하여 방화벽이 트래픽을 복호화하고 있는지 확인할 수 있습니다. 복호화하려고 하며 복호화를 원하지 않는 트래픽은 방화벽이 복호화를 하지 않습니다. 이 항목에서는 트래픽 로그를 사용하여 복호화를 확인하는 방법을 보여 줍니다. 또한 배포 후 복호화 모범 사례에 따라 배포를 유지 관리합니다.

- 복호화된 트래픽 세션 보기 - 필터 를 사용하여 트래픽 로그 필터링(모니터 > 로그 > 트래픽) ( 플래그에 프록시가 있음 ).

  이 필터는 SSL 프록시 플래그가 켜져 있는 로그만 표시합니다. 즉, 복호화된 트래픽만 의미합니다. 모든 로그 항목에는 **Decrypted** 열에 yes 값이 있습니다.



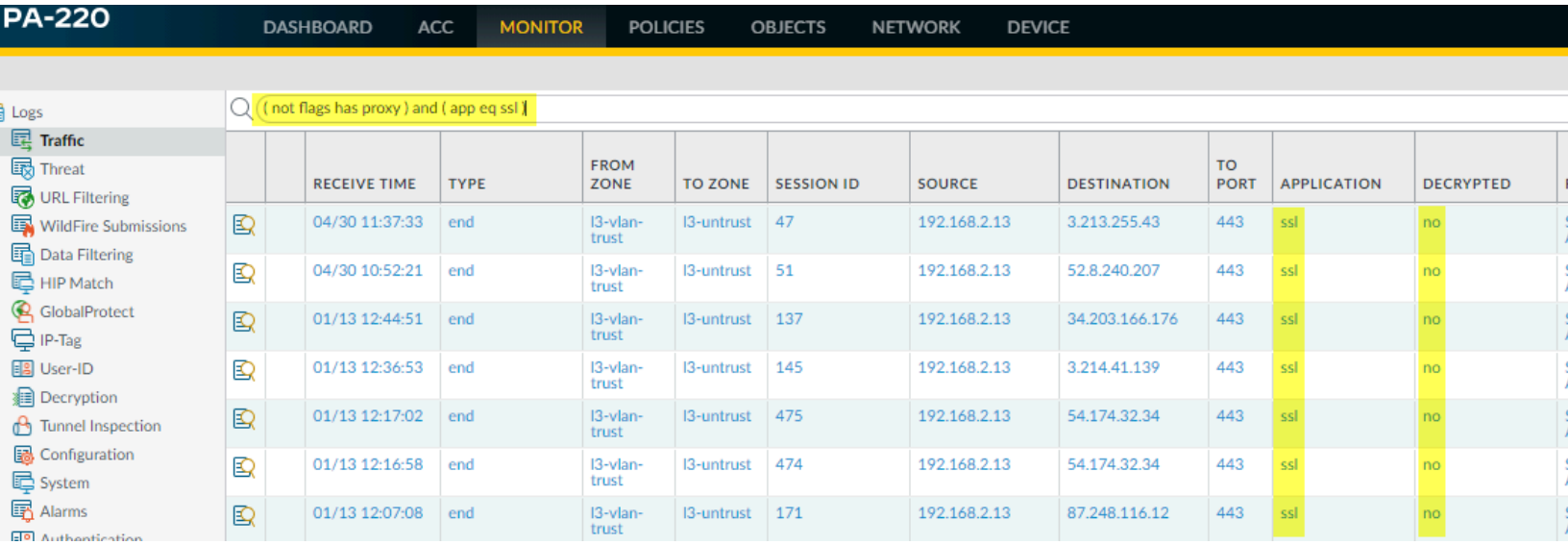

필터에 더 많은 용어를 추가하여 트래픽을 보다 세분화된 방식으로 필터링할 수 있습니다. 예를 들어 필터 (99.84.224.105의 addr.dst)를 추가하여 대상 IP 주소 99.84.224.105로만 이동하는 암호화된 트래픽에 대해 필터링할 수 있습니다.




 ©2023 Palo Alto Networks, Inc.

- 암호 해독되지 않은 **SSL** 트래픽 세션 보기 - 다음을 사용하여 트래픽 로그 필터링(모니터 > 로그 > 트래픽) 필터 ( 플래그에 프록시가 없음) 및 ( app eq ssl ).

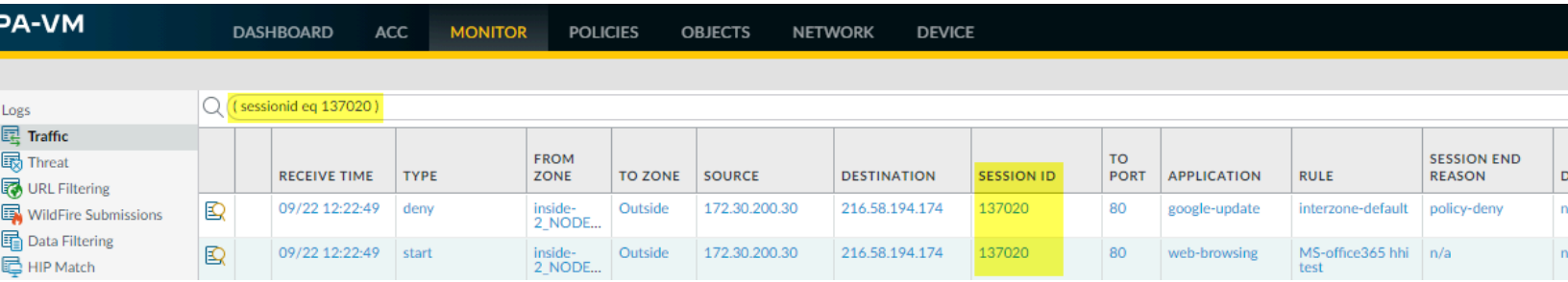
  이 필터는 SSL 프록시 플래그가 꺼져 있고(암호화된 트래픽만 해당) 트래픽이 SSL 트래픽인 로그만 표시합니다. 모든 로그 항목은 복호화됨 열에 값이 **no**이고 애플리케이션 열에 **ssl** 값이 있습니다.




  복호화된 트래픽 로그를 보는 예와 마찬가지로 용어를 추가하여 복호화하지 않는 트래픽을 보다 세부적으로 필터링할 수 있습니다.

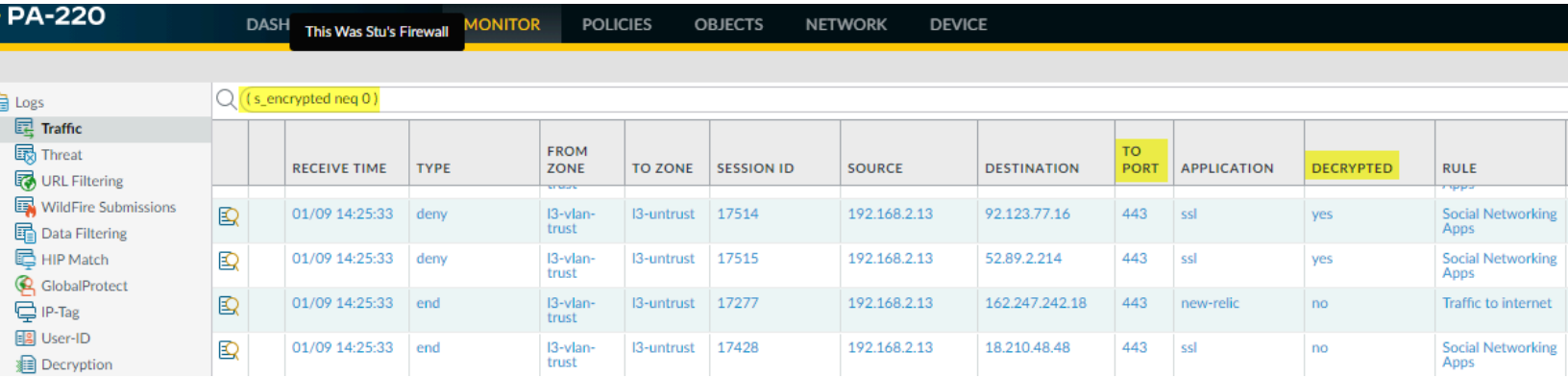
- 특정 세션에 대한 로그 보기 - 특정 세션에 대한 트래픽 로그를 보려면 세션 ID를 필터링합니다.

  예를 들어 ID가 137020인 세션에 대한 로그를 보려면 (sessionid eq 137020) 용어를 사용하여 필터링합니다. 이전 화면과 같이 로그 출력의 세션 ID 열에서 ID 번호를 찾을 수 있습니다. 세션 ID 열이 표시되지 않으면 출력에 열을 추가합니다.



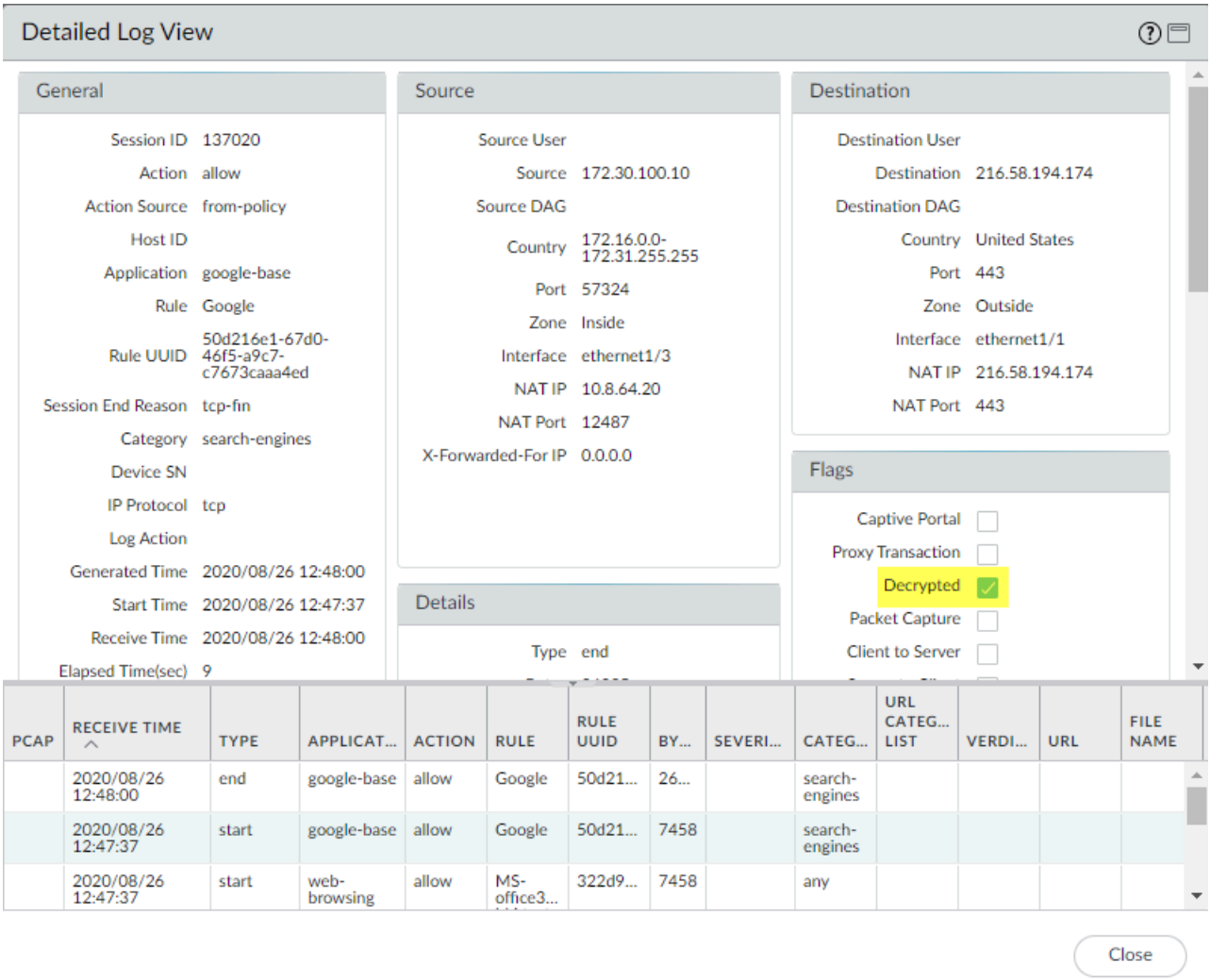

 ©2023 Palo Alto Networks, Inc.

- 모든 **TLS** 및 **SSH** 트래픽 보기 - 트래픽 로그(모니터 > 로그 > 트래픽)를 필터링하여 복호화된 두 가지를 모두 봅니다. 복호화되지 않은 TLS 및 SSH 트래픽의 경우 ( s_encrypted neq 0 ) 필터를 사용합니다.




 ©2023 Palo Alto Networks, Inc.

- 세부정보로 드릴다운 - 특정 로그 항목에 대한 자세한 정보를 보려면 돋보기를 클릭하여 자세한 로그 보기를 봅니다. 예를 들어 세션 ID 137020(이전 글머리 기호 참조) 의 경우 자세한 로그는 다음과 같습니다.




**Decrypted** 플래그 상자는 트래픽의 암호가 복호화되었는지 확인하는 두 번째 방법을 제공합니다.

또한 복호화된 트래픽의 업스트림 및 다운스트림 패킷 캡처를 통해 방화벽이 SSL 트래픽을 처리하고 패킷에 대해 작업을 수행하는 방식을 보거나 심층 패킷 검사를 수행할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

# 복호화 문제 해결 및 모니터링

문제 해결 도구는 TLS 트래픽에 대한 향상된 가시성을 제공하므로 복호화 배포를 모니터링할 수 있습니다. 이 도구를 사용하면 복호화 문제를 빠르고 쉽게 진단 및 해결하고 복호화 배포의 약점을 강화하고 복호화 문제를 수정하여 보안 태세를 개선할 수 있습니다. 예를 들어 다음을 수행할 수 있습니다.

- SNI(Service Name Identification) 및 애플리케이션별로 복호화 실패를 유발하는 트래픽을 식별합니다.
- 약한 프로토콜과 알고리즘을 사용하는 트래픽을 식별합니다.
- 네트워크에서 성공한 복호화 작업과 실패한 복호화 작업을 검사합니다.
- 개별 세션에 대한 자세한 정보를 봅니다.
- 프로파일 복호화 사용 및 패턴.
- 자세한 복호화 통계 및 채택, 실패, 버전, 알고리즘 등에 대한 정보를 모니터링합니다.

다음 도구는 TLS 핸드쉐이크에 대한 완전한 가시성을 제공하고 문제를 해결하고 복호화 배포를 모니터링하는 데 도움이 됩니다.

- **ACC** > **SSL** 활동 - 이 탭의 5개 ACC 위젯(PAN-OS 10.0에 도입됨)은 네트워크에서 복호화 실패, TLS 버전, 키 교환, 복호화 및 복호화되지 않은 트래픽의 양과 유형을 포함하는 성공 및 실패한 암호 해독 활동에 대한 세부 정보를 제공합니다.
- **Monitor** > **Logs** > **Decryption** - 암호 해독 로그(PAN-OS 10.0에 도입됨)는 암호 해독 정책과 일치하는 개별 세션에 대한 포괄적인 정보를 제공하고(암호화하지 않는 트래픽에 대해 암호 해독 없음 정책 사용) GlobalProtect Portal 또는 GlobalProtect Gateway 구성에 로그인하여 복호화를 활성화할 때 GlobalProtect 세션에 대한 포괄적인 정보를 제공합니다. 애플리케이션, SNI, 복호화 정책 이름, 오류 인덱스, TLS 버전, 키 교환 버전, 암호화 알고리즘, 인증서 키 유형 및 기타 여러 특성과 같은 정보를 보려면 표시할 열을 선택하십시오. 열의 정보를 필터링하여 특정 TLS 버전 및 알고리즘, 특정 오류 또는 조사하려는 기타 특성을 사용하는 트래픽을 식별합니다. 기본적으로 복호화 정책은 실패한 TLS 핸드쉐이크만 기록합니다. 사용 가능한 로그 저장소에 따라 성공적인 TLS 핸드쉐이크도 기록하도록 복호화 정책을 구성할 수 있습니다.
- 로컬 복호화 제외 캐시 - 클라이언트 인증 또는 고정된 인증서와 같은 기술적인 이유로 복호화를 중단하여 복호화에서 제외해야 하는 사이트에는 SSL 복호화 제외 목록과 로컬 복호화 제외 캐시의 두 가지 구성이 있습니다. SSL 복호화 제외 목록에는 Palo Alto Networks가 기술적으로 복호화를 방해하는 사이트를 식별한 사이트가 포함되어 있습니다. 콘텐츠 업데이트는 목록을 최신 상태로 유지하며 수동으로 목록에 사이트를 추가할 수 있습니다. 로컬 복호화 제외 캐시는 트래픽에 적용된 복호화 프로파일이 지원되지 않는 모드를 허용하는 경우 기술적인 이유로 복호화를 중단하고 복호화에서 제외하는 로컬 사용자가 만나는 사이트를 자동으로 추가합니다(지원되지 않는 모드가 차단되면 트래픽이 로컬 캐시에 추가되는 대신 차단됩니다).
- 복호화를 위한 맞춤 리포트 템플릿 - 복호화 활동을 요약하는 4개의 사전 정의된 템플릿(PAN-OS 10.0에 도입됨)을 사용하여 맞춤 리포트(**Monitor** > **Manage** 맞춤 리포트)를 생성할 수 있습니다.

일반적인 문제 해결 방법론은 새로운 ACC 위젯을 사용하여 복호화 문제를 일으키는 트래픽을 식별한 다음 새로운 복호화 로그 및 맞춤 리포트 템플릿을 사용하여 세부 정보를 드릴다운하고 해당 트래픽에 대한 컨텍스트를 얻는 것입니다. 이를 통해 과거보다 더 쉽게 문제를 정확하고 많이 진단할 수 있습니다. 복호화 문제와 그 원인을 이해하면 다음과 같이 각 문제를 해결하는 적절한 방법을 선택할 수 있습니다.

- 복호화 정책 규칙 수정(정책 규칙은 규칙이 영향을 미치는 트래픽, 해당 트래픽에 대해 수행되는 작업, 로그 설정 및 트래픽에 적용된 복호화 프로파일을 정의합니다.)


©2023 Palo Alto Networks, Inc.

- 복호화 프로파일 수정(복호화 정책 규칙이 정의하는 트래픽에 대해 허용되는 프로토콜 및 알고리즘, 실패 검사, 지원되지 않는 암호 및 버전과 같은 항목에 대한 지원되지 않는 모드 검사, 인증서 검사 등)
- SSL 복호화 제외 목록에 기술적인 이유로 복호화를 중단하는 사이트 추가
- 직원, 고객 및 파트너가 실제로 액세스해야 하는 사이트와 취약한 복호화 프로토콜 또는 알고리즘을 사용할 때 차단할 수 있는 사이트에 대한 보안 결정을 평가합니다.

목표는 복호화할 수 있는 모든 트래픽을 복호화하여(복호화 모범 사례) 이를 검사하고 복호화하지 않은 트래픽을 적절하게 처리하는 것이어야 합니다.

PAN-OS 10.0으로 업그레이드하면 디바이스가 로그 공간의 1%를 차지하여 복호화 로그에 할당합니다. 복호화 로깅 구성의 에서는 복호화 로그에 더 많은 공간을 제공하기 위해 로그 공간 할당을 수정하는 방법을 보여줍니다.

PAN-OS 10.2 이상에서 PAN-OS 9.1 이하로 다운그레이드하면 PAN-OS 10.2에 도입된 기능(복호화 로그, ACC의 SSL 활동 위젯, 사용자 정의 보고서 복호화 템플릿)이 UI에서 제거됩니다. 복호화 로그에 대한 레퍼런스도 로그 포워딩 프로파일에서 제거됩니다. 또한 Local Decryption Exclusion Cache는 PAN-OS 9.1 및 이전 버전(PAN-OS 10.2는 UI에 로컬 캐시를 추가함)의 CLI를 통해서만 볼 수 있습니다.

PAN-OS 10.2 이상의 Panorama에서 PAN-OS 9.1 이하를 실행하는 디바이스로 구성을 푸시하면 Panorama는 PAN-OS 10.0에 도입된 기능을 제거합니다.

- 복호화 애플리케이션 명령 센터 위젯
- 복호화 로그
- 복호화를 위한 맞춤 리포트 템플릿
- 복호화 문제 해결 워크플로 예제

## 복호화 애플리케이션 명령 센터 위젯

PAN-OS 10.2에 도입된 복호화용 ACC(Application Command Center) 위젯(**ACC** > **SSL** 활동)은 복호화 로그와 함께 작동하여 진단 및 해결을 돕습니다. 암호 해독 문제를 빠르고 쉽게 해결합니다. **SSL** 활동 위젯을 사용하여 복호화 및 비복호화 세션 수, 다양한 TLS 프로토콜 버전을 사용하는 트래픽 양, 가장 일반적인 복호화 실패 이유, 애플리케이션 및 서버 이름과 같은 네트워크 복호화 활동을 보고 분석하고 어떤 애플리케이션과 SNI(서버 이름 식별)가 약한 암호와 알고리즘을 사용하는지 확인합니다. 그런 다음 복호화 로그를 사용하여 세션을 드릴다운하고 정확한 문제를 진단하여 적절한 조치를 취할 수 있습니다.

PAN-OS 10.2에는 5개의 새로운 복호화 위젯이 도입되었습니다. 위젯이 제공하는 정보를 사용하여 잘못 구성된 복호화 정책 및 프로파일을 식별하고 허용할 트래픽과 차단할 트래픽에 대해 정보에 입각한 결정을 내립니다.

- 트래픽 활동 - SSL/TLS 활동을 비 SSL/TLS 활동과 비교하여 총 세션 수 또는 트래픽 양(바이트)별로 표시합니다.

 ©2023 Palo Alto Networks, Inc.

- **SSL/TLS** 트래픽 - 세션 수 또는 트래픽 양(바이트)별로 복호화 및 복호화되지 않은 트래픽의 양을 표시합니다. 트래픽이 해독되지 않는 이유는 다음과 같습니다.
  - 트래픽에 복호화 정책이 적용되지 않습니다.
  - 복호화 정책이 의도적으로 트래픽을 복호화에서 제외했습니다(예: 비복호화 정책).
  - 복호화 정책이 잘못 구성되어 트래픽이 복호화되지 않았습니다.
  - 해당 사이트는 Palo Alto Networks가 식별한 고정된 인증서 또는 클라이언트 인증과 같은 기술적인 이유로 암호 해독을 중단하는 사이트를 포함하는 SSL 복호화 제외 목록(디바이스 > 인증서 관리 > **SSL** 복호화 제외)에 있습니다. 이러한 사이트의 경우 방화벽은 복호화를 우회합니다.
  - 이 사이트는 로컬 사용자가 기술적인 이유로 복호화를 방지하는 사이트를 포함하는 로컬 복호화 제외 캐시에 있습니다.

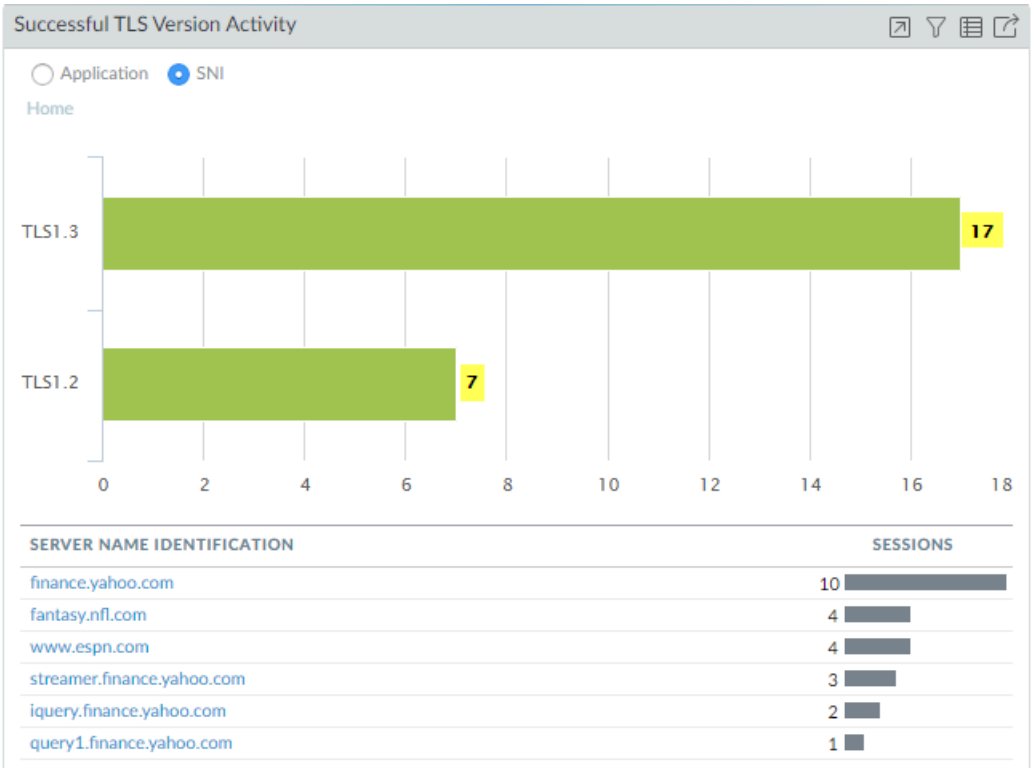
ACC는 복호화 정책이 제어하는 트래픽의 데이터로 다음 세 개의 위젯만 채웁니다. 트래픽에 복호화 정책을 적용하지 않으면 해당 트래픽이 이러한 위젯을 채우지 않습니다.

- 복호화 실패 이유 - SNI별로 프로토콜, 인증서, 버전, 암호, HSM, 리소스, 이력서 또는 기능 문제와 같은 복호화 실패 이유를 표시합니다. 이 정보를 사용하여 복호화 정책 또는 프로파일 구성 오류 또는 지원되지 않는 약한 프로토콜이나 알고리즘을 사용하는 트래픽으로 인해 발생하는 문제를 감지합니다. 실패 이유를 클릭하여 실패를 경험한 SNI당 세션 수를 드릴다운하고 격리하거나 SNI를 클릭하여 해당 SNI에 대한 모든 복호화 실패를 확인합니다.
- 성공적인 **TLS** 버전 활동 - 애플리케이션 또는 SNI에 대한 TLS 버전별 성공적인 TLS 연결을 표시합니다(SNI는 포워드 프록시에서만 사용 가능). 따라서 약한 TLS 프로토콜 버전을 허용함으로써 얼마나 많은 위험을 감수하고 있는지 평가할 수 있습니다. 약한 프로토콜을 사용하는 애플리케이션 및 SNI를 식별하면 각각을 평가하고 비즈니스상의 이유로 액세스를 허용해야 하는지의 여부를 결정할 수 있습니다. 비즈니스 목적으로 애플리케이션이 필요하지 않은 경우, 위험을 줄이기 위해 트래픽을 허용하는 대신 트래픽을 차단할 수 있습니다. TLS 버전을 클릭하여 드릴다운하고 해당 TLS 버전을 사용한 SNI 또는 애플리케이션을 확인합니다. 드릴다운하고 각 TLS 버전을 사용한 애플리케이션 또는 SNI 세션 수를 보려면 애플리케이션 또는 SNI를 클릭하십시오.
- 키 교환 작업 성공 - 애플리케이션 또는 SNI에 대한 알고리즘별 키 교환 작업 성공을 표시합니다(SNI는 포워드 프록시에서만 사용 가능). 키 교환 알고리즘을 클릭하여 해당 알고리즘에 대한 활동을 확인하거나 애플리케이션 또는 SNI를 클릭하여 해당 애플리케이션 또는 SNI에 대한 키 교환 알고리즘 활동을 확인합니다.

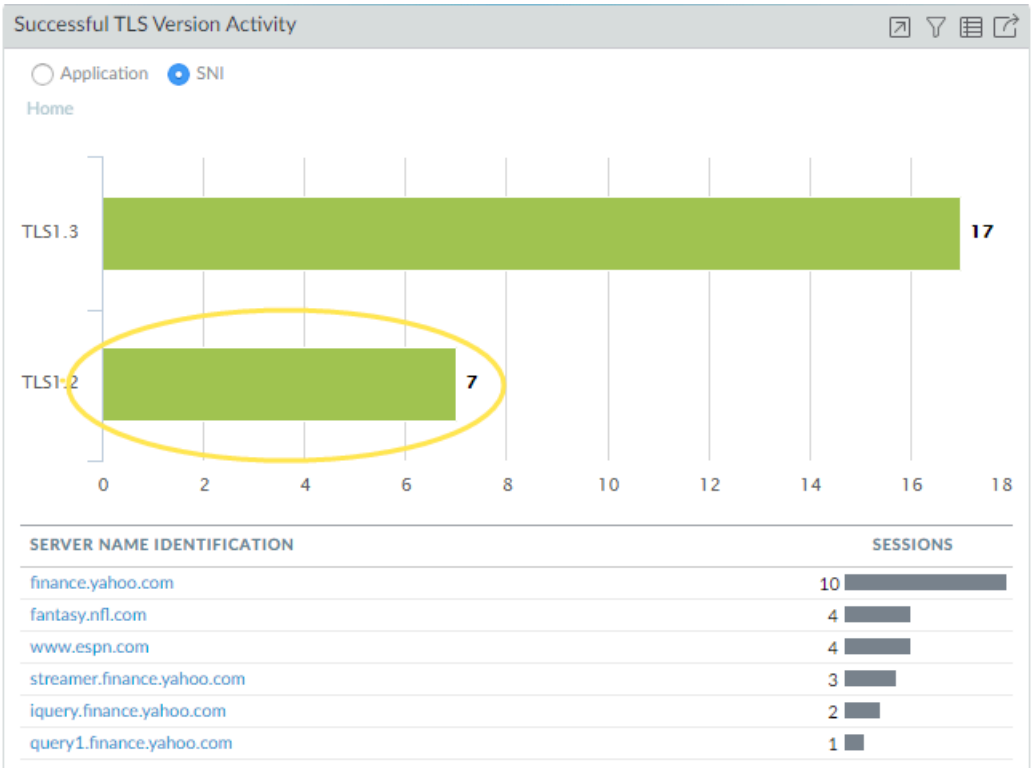
ACC 데이터로 드릴다운하는 다음 예는 성공적인 TLS 버전 활동을 검사하는 방법을 보여줍니다.

 ©2023 Palo Alto Networks, Inc.

1. 성공적인 **TLS** 버전 활동 위젯은 17개의 세션이 TLSv1.3을 사용하고 7개의 세션이 TLSv1.2를 사용했음을 보여줍니다. SNI 목록에는 대상 SNI와 SNI당 세션 수가 표시됩니다.

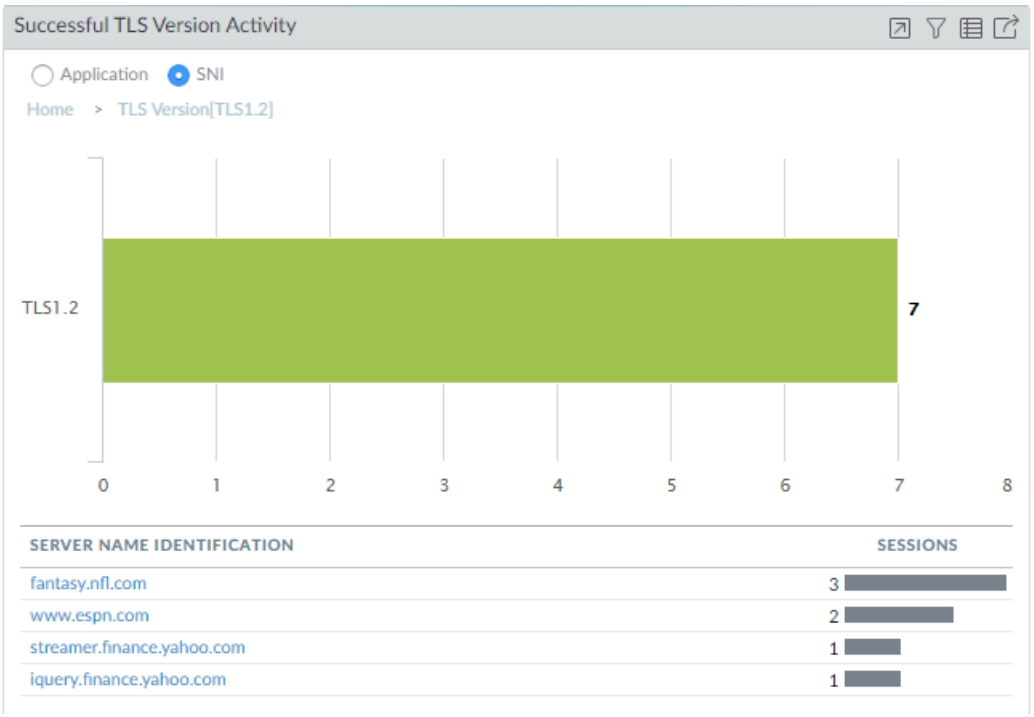



2. 어떤 SNI가 TLSv1.2를 사용했는지 보려면 TLS1.2라고 표시된 녹색 막대를 클릭하십시오.

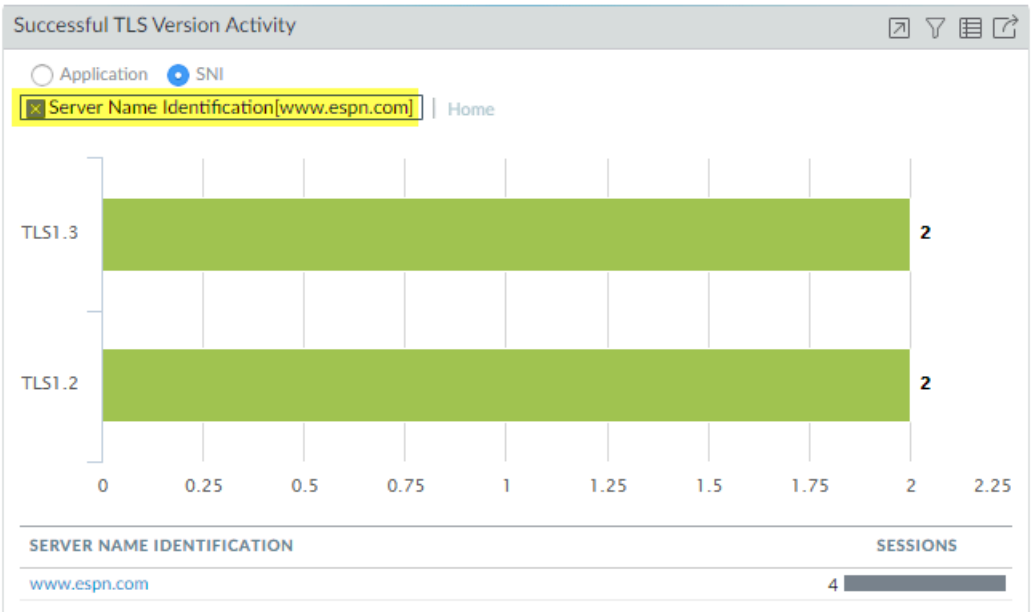



 ©2023 Palo Alto Networks, Inc.

3. 이제 7개의 TLSv1.2 세션이 4개의 서버에 분산된 것을 볼 수 있습니다.




4. 홈을 클릭하면 홈 화면으로 돌아갑니다. 이제 www.espn.com SNI를 클릭하면 사용된 TLS 버전이 표시됩니다. 4개의 세션 중 2개는 TLSv1.3을 사용하고 2개는 TLSv1.2를 사용했음을 알 수 있습니다.




복호화 위젯의 경우 로그로 이동 아이콘을 클릭하여 ACC의 데이터에 해당하는 복호화 로그로 직접 이동합니다.




 ©2023 Palo Alto Networks, Inc.

앞의 예에서 조사의 어느 시점에서나 데이터에 대한 복호화 로그로 이동하여 더 자세히 드릴다운할 수 있습니다. 예를 들어, TLSv1.2를 사용한 개별 세션에 대한 로그를 조사하여 TLSv1.3을 사용하지 않은 이유를 찾을 수 있습니다.

복호화 ACC 위젯은 Palo Alto Networks App-ID를 기반으로 복호화된 애플리케이션의 이름을 표시합니다. ACC를 채우기 위해 방화벽은 Palo Alto Networks App-ID가 있는 애플리케이션만 식별할 수 있습니다. 방화벽은 App-ID가 없는 사용자 지정 애플리케이션이나 애플리케이션으로 ACC를 채울 수 없습니다. 콘텐츠 업데이트는 정기적으로 App-ID를 업데이트합니다. 애플리케이션가 불완전하거나 알 수 없는 것으로 표시될 수 있는 다른 이유는 다음과 같습니다.

- 방화벽이 애플리케이션을 식별하기 전에 세션을 삭제했습니다.
- 복호화 로그는 복호화 로그 애플리케이션 필드를 채우는 트래픽 로그에 의존합니다. 그러나 트래픽 로그가 60초 이내에 완료되지 않으면 트래픽 로그가 복호화 로그의 애플리케이션을 채우지 않고 애플리케이션이 불완전하거나 알 수 없음으로 표시됩니다.

## 복호화 로그

복호화 로그(**Monitor** > **Logs** > **Decryption**)는 복호화 정책과 일치하는 세션에 대한 포괄적인 정보를 제공하여 해당 트래픽에 대한 컨텍스트를 얻는 데 도움이 되므로 복호화 문제를 정확하고 쉽게 진단하고 해결할 수 있습니다. 트래픽이 복호화 정책과 일치하지 않으면 방화벽은 트래픽을 기록하지 않습니다. 암호를 복호화하지 않는 트래픽을 기록하려면 정책 기반 복호화 제외를 생성하고 TLSv1.2 및 이전 트래픽을 제어하는 정책에 대해 비복호화 프로파일을 트래픽에 적용합니다.

PAN-OS는 다음 트래픽 유형에 대한 복호화 로그를 지원합니다.

- 포워드 프록시 - 루트 CA(신뢰할 수 있는 인증서만 해당) 및 SNI(서버 이름 식별)를 포함하여 일부 필드에는 포워드 프록시 트래픽에 대한 정보만 표시됩니다.
- 인바운드 검사.
- 비복호화(복호화 정책에 의해 복호화에서 제외된 트래픽).

  세션이 암호화된 상태로 유지되기 때문에 방화벽은 더 적은 정보를 표시합니다. 복호화되지 않은 ***TLSv1.3*** 트래픽의 경우 ***TLSv1.3***이 인증서 정보를 암호화하기 때문에 인증서 정보가 없습니다.

- GlobalProtect - GlobalProtect Gateway, GlobalProtect Portal 및 GlobalProtect Clientless VPN(클라이언트-방화벽만 해당)을 다룹니다.

  ***GlobalProtect***는 ***TLSv1.3***을 지원하지 않습니다.

- 복호화 미러

모든 유형의 트래픽이 모든 매개변수를 지원하는 것은 아닙니다. 프록시 유형 및 TLS 버전별로 지원되지 않는 매개 변수은(는) 각 유형의 복호화 트래픽에 대해 지원되지 않는 매개변수의 전체 목록을 제공합니다.

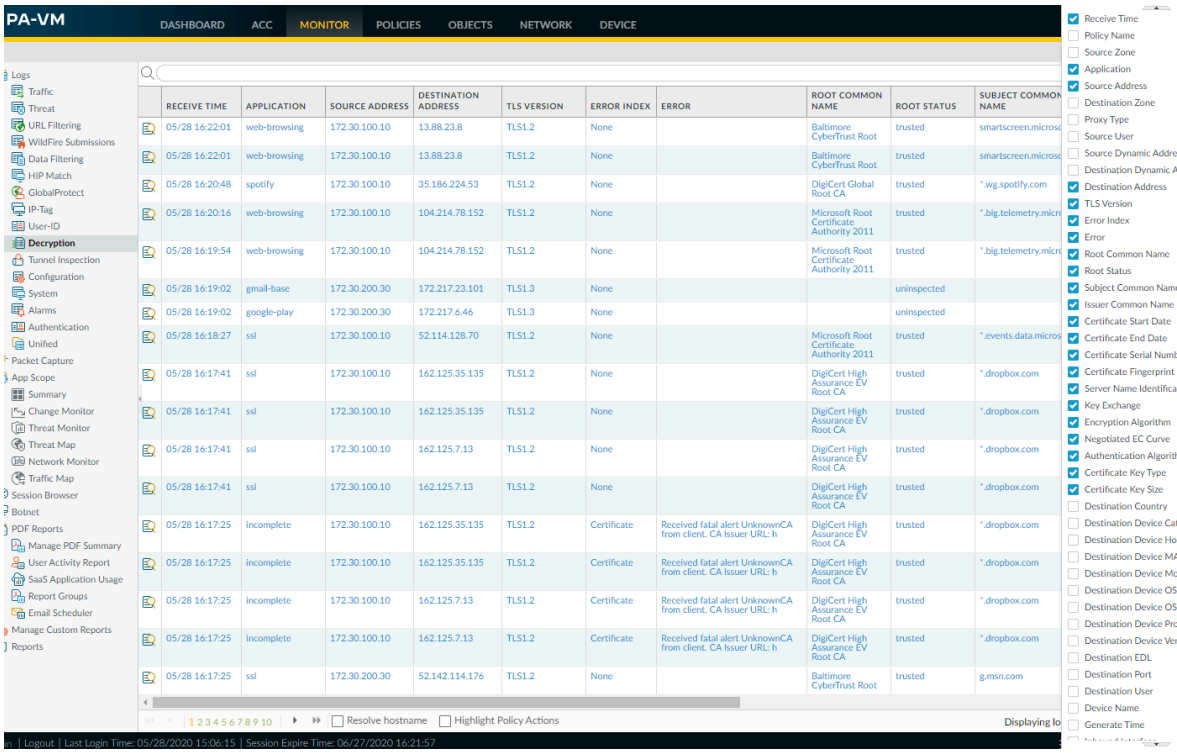
포워드 프록시 트래픽에 대한 데이터는 TLS 핸드쉐이크의 성공 여부를 기반으로 합니다. TLS 핸드쉐이크에 실패한 경우 방화벽은 클라이언트에서 방화벽으로 또는 방화벽에서 서버로 오류를 일으킨 트랜잭션 구간에 대한 오류 데이터를 보냅니다. 성공적인 TLS 핸드쉐이크의 경우 데이터는 일반적으로 클라이언트에서 방화벽으로 성공적으로 먼저 완료된 구간에서 가져옵니다.

 ©2023 Palo Alto Networks, Inc.

방화벽은 SSL/TLS 핸드쉐이크 검사 중에 차단된 웹 트래픽에 대한 복호화 로그 항목을 생성하지 않습니다. 방화벽이 ***SSL/TLS*** 연결을 재설정하여 핸드쉐이크를 종료할 때 복호화를 방지하기 때문에 이러한 세션은 복호화 로그에 나타나지 않습니다. ***URL*** 필터링 로그에서 차단된 세션의 세부 정보를 볼 수 있습니다.

***SSH*** 프록시 트래픽에는 복호화 로그가 지원되지 않습니다. 또한 세션 재개 로그에는 인증서 정보를 사용할 수 없습니다.

기본적으로 방화벽은 실패한 모든 TLS 핸드쉐이크 트래픽을 기록합니다. 원하는 경우 성공적인 TLS 핸드쉐이크 트래픽을 기록할 수도 있습니다. 애플리케이션, SNI, 복호화 정책 이름, 오류 색인, TLS 버전, 키 교환 버전, 암호화 알고리즘, 인증서 키 유형 및 기타 여러 속성과 같은 로그 정보의 최대 62개 열을 볼 수 있습니다.




돋보기 아이콘(🔍)을 클릭하면 세션의 상세 로그 보기를 볼 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

복호화 로그는 트래픽 로그에서 각 세션의 *App-ID*를 학습하므로 복호화 로그에서 *App-ID*를 보려면 트래픽 로그를 활성화해야 합니다. 트래픽 로그가 비활성화되면 *App-ID*가 불완전한 것으로 표시됩니다. 예를 들어, 많은 *GlobalProtect* 트래픽은 영역 내 트래픽(신뢰할 수 없는 영역에서 신뢰하지 않는 영역으로)이지만 기본 영역 내 정책은 트래픽 로그를 활성화하지 않습니다. *GlobalProtect* 영역 내 트래픽에 대한 *App-ID*를 보려면 영역 내 트래픽에 대해 트래픽 로그를 활성화해야 합니다.

*App-ID*가 불완전한 것으로 표시될 수 있는 또 다른 이유는 긴 세션의 경우 방화벽이 트래픽 로그가 완료되기 전에 복호화 로그를 생성할 수 있기 때문입니다(트래픽 로그는 일반적으로 세션 종료 시 생성됨). 이러한 경우 *App-ID*는 복호화 로그에 사용할 수 없습니다. 또한 *TLS* 핸드쉐이크가 실패하고 오류 로그가 생성되면 방화벽이 *App-ID*를 판별하기 전에 실패로 인해 세션이 종료되므로 *App-ID*를 사용할 수 없습니다. 이러한 경우 애플리케이션이 ***ssl*** 또는 불완전한 것으로 표시될 수 있습니다.

문제를 해결하려면 암호 해독 ACC 위젯(**ACC** > **SSL** 활동)을 사용하여 암호 해독 문제를 일으키는 트래픽을 식별한 다음 암호 해독 log 및 복호화를 위한 맞춤 리포트 템플릿를 사용하여 세부정보를 드릴다운합니다.

저장을 위해 복호화 로그를 포워딩할 때 복호화 로그에는 민감한 정보가 포함되어 있으므로 로그 전송 및 저장을 적절하게 보호해야 합니다.

복호화 로그가 활성화된 경우 방화벽은 *HTTP/2* 로그를 터널 검사 로그로 전송하므로(암호화 로그 비활성화 시 *HTTP/2* 로그를 트래픽 로그로 전송) *HTTP/2* 이벤트의 경우 트래픽 로그 대신 터널 검사 로그를 확인해야 합니다. 또한 *HTTP/2* 트래픽에 대한 *App-ID*를 얻으려면 터널 콘텐츠 검사를 활성화해야 합니다.

- 복호화 로깅 구성
- 불완전한 인증서 체인 수리
- 복호화 로그 오류, 오류 색인 및 비트마스크

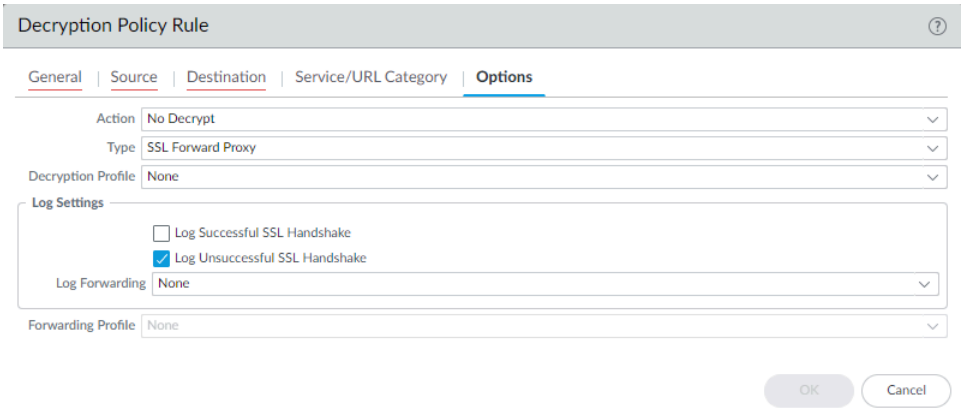
## 복호화 로깅 구성

방화벽은 복호화 정책이 없는 세션을 포함하여 복호화 정책의 적용을 받는 세션에 대한 복호화 로그를 생성합니다. 로그할 트래픽을 제어하는 복호화 정책에서 복호화 로깅을 구성합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 복호화 정책(정책 > 복호화)에 로그인할 복호화 트래픽을 구성합니다.

기본적으로 방화벽은 실패한 TLS 핸드셰이크

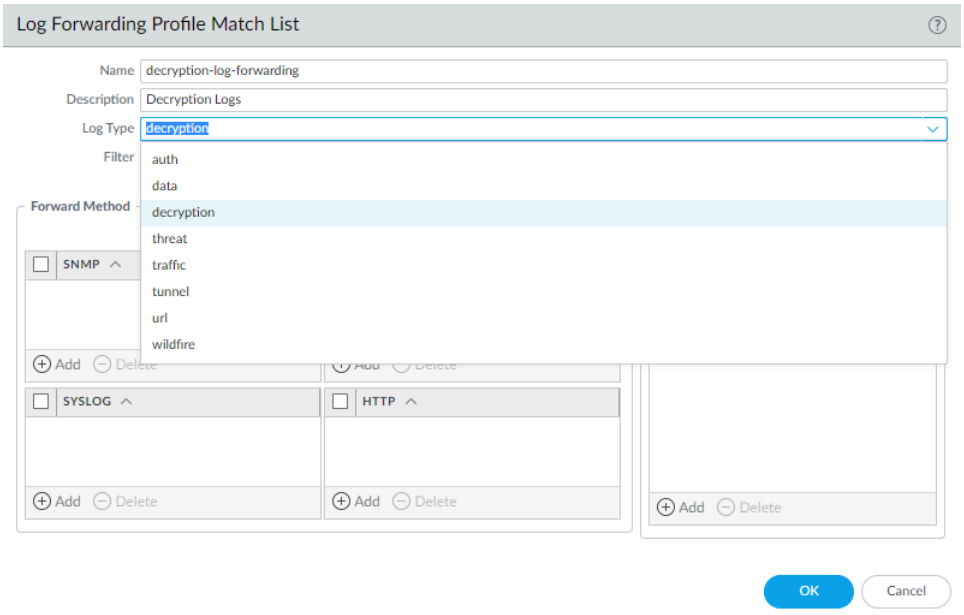



만 기록합니다.

성공적인 핸드셰이크와 실패한 핸드셰이크를 기록하여 디바이스의 사용 가능한 리소스 허용만큼 해독된 트래픽에 대한 가시성을 확보합니다(개인 또는 민감한 트래픽을 해독하지 마십시오. 복호화 모범 사례를 따르고 가능한 한 많은 트래픽을 해독하십시오).

**STEP 2 |** 로그 포워딩 프로파일을 만들어 로그 컬렉터, 다른 저장소 디바이스 또는 특정 관리자에게 복호화 로그를 포워딩한 다음 복호화 정책 옵션 탭의 로그 포워딩 필드에 프로파일을 지정합니다.

복호화 로그를 포워딩하려면 복호화 로그 유형과 로그 포워딩 방법을 지정하려면 로그 포워딩 프로파일(개체 > 로그 포워딩)을 구성해야 합니다.

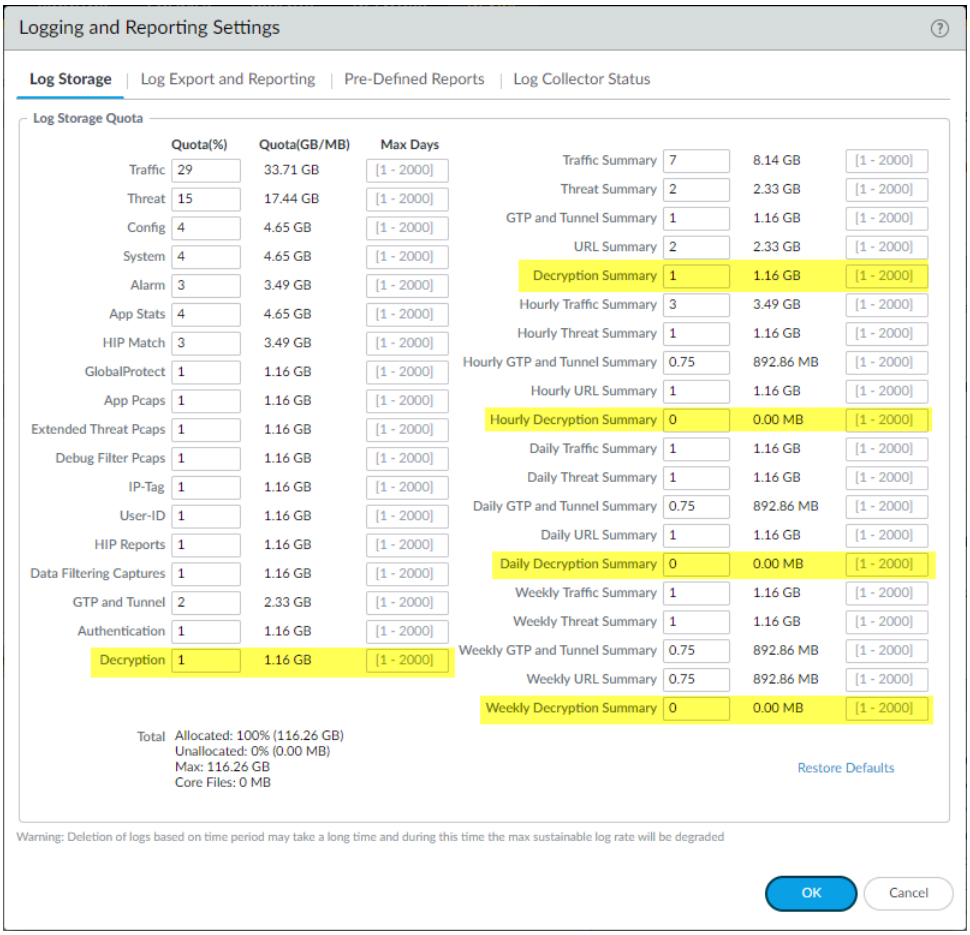



복호화 로그를 포워딩하면 중요한 정보가 포함되어 있으므로 로그가 안전하게 저장되어 있는지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 실패한 TLS 핸드셰이크 외에도 성공적인 TLS 핸드셰이크를 기록하는 경우 방화벽의 복호화 로그에 대해 더 큰 로그 저장 공간 할당량(디바이스 > 설정 > 관리 > 로깅 및 보고 설정 > 로그 저장소)을 구성합니다.

기본 할당량(할당)은 복호화 로그에 대한 디바이스의 로그 저장 용량의 1%와 일반 복호화 요약의 1%입니다. 시간당, 일별 또는 주간 단위의 복호화 요약에 대한 기본 할당은 없습니다.




많은 요인으로 복호화 로그에 필요한 저장소의 양을 결정하고 배포에 따라 달라집니다. 예를 들어 다음 요소를 고려하십시오.

- 방화벽을 통과하는 TLS 트래픽의 양입니다.
- 해독하는 TLS 트래픽의 양입니다.
- 다른 로그를 사용합니다(복호화 로그에 할당할 수 있는 용량을 취해야 하는 로그를 평가).
- 성공 및 실패한 TLS 핸드셰이크를 모두 기록하는 경우, 실패한 TLS 핸드셰이크만 기록하려면 필요한 것보다 훨씬 더 많은 용량이 필요할 수 있습니다. 해독 트래픽의 양에 따라 복호화 로그는 트래픽

 ©2023 Palo Alto Networks, Inc.

로그 또는 위협 로그만큼 많은 용량을 소비할 수 있으며 디바이스의 용량이 이미 완전히 구독된 경우 이러한 트래픽 간에 절충이 필요할 수 있습니다.

로그 할당량의 총 결합 할당은 사용 가능한 방화벽 로그 리소스의 ***100%***를 초과할 수 없습니다.

특정 배포에서 각 로그 카테고리에 대한 적절한 할당량을 찾으려면 테스트가 필요할 수 있습니다. 실패한 핸드셰이크만 기록하면 기본값으로 시작하거나 할당을 2~3%로 늘릴 수 있습니다. 성공적이고 실패한 핸드셰이크를 모두 기록하는 경우 공간의 절반 정도를 트래픽 로그에 할당하는 복호화 로그에 할당하여 시작할 수 있습니다. 공간을 사용하여 복호화 로그에 할당하는 로그는 트래픽, 비즈니스 및 모니터링 요구 사항에 따라 달라집니다.

## 복호화 로그 오류, 오류 색인 및 비트마스크

복호화 로그의 오류 색인 및 오류 열은 각각 복호화 오류 카테고리 및 세부 정보에 대한 정보를 제공합니다. 자세한 로그 보기의 핸드쉐이크 세부 정보 섹션에서 오류 및 오류 색인 정보를 볼 수도 있습니다(로그 항목을 보려면 클릭). 복호화 로그 오류 인덱스는 8가지 오류 카테고리 중 하나를 나타냅니다.

| 오류 인덱스 | 오류(오류 색인에 대해 표시될 수 있는 오류) |
|---|---|
| 인증서 | 유효하지 않은 인증서, 만료된 인증서, 지원되지 않는 클라이언트 인증서, OCSP/CRL 검사 취소 및 실패, 신뢰할 수 없는 발급자 CA(불완전한 인증서 체인을 포함하는 신뢰할 수 없는 루트가 서명한 세션) 및 기타 인증서 오류와 같은 오류.<br><br>사이트에서 전체 인증서 체인을 보내지 않았기 때문에 방화벽에 중간 인증서가 없는 경우 누락된 인증서를 찾아 불완전한 인증서 체인 수리에 설치할 수 있습니다. |
| 암호 | 지원되지 않는 암호 오류:<br>• 클라이언트는 방화벽이 지원하지만 트래픽에 적용된 복호화 프로파일이 지원하지 않는 암호 협상을 시도합니다.<br>• 클라이언트는 방화벽이 지원하지 않는 암호를 협상하려고 합니다.<br>• (특수) 인바운드 검사가 활성화되어 있고 서버의 기능이 복호화 프로파일 설정과 일치하지 않습니다.<br>오류 메시지에는 지원되는 클라이언트 암호 비트마스크 값과 지원되는 복호화 프로파일 암호 비트마스크 값이 포함됩니다. 비트마스크 값을 사용하여 클라이언트가 사용하려고 시도한 암호를 식별하고 이 항목의 뒷부분에 설명된 대로 복호화 프로파일이 지원하는 암호 값을 나열합니다. |
| 기능 | 대형 TLS 핸드쉐이크 또는 알 수 없는 핸드쉐이크, 대형 인증서 체인(5개 이상의 인증서) 및 기타 지원되지 않는 기능과 같은 오류. |
| **HSM** | 알 수 없는 요청, 구성에서 찾을 수 없는 항목, 리퀘스트 타임아웃, 기타 HSM 오류 및 실패와 같은 HSM(하드웨어 스토리지 모듈) 오류. |


©2023 Palo Alto Networks, Inc.

| 오류 인덱스 | 오류(오류 색인에 대해 표시될 수 있는 오류) |
|---|---|
| 프로토콜 | TLS 핸드쉐이크 실패, 개인 및 공개 키 불일치, Heartbleed 오류, TLS 키 교환 실패 및 기타 TLS 프로토콜 오류와 같은 오류. 프로토콜 오류는 서버가 클라이언트가 지원하는 프로토콜을 지원하지 않는 경우, 서버가 방화벽이 지원하지 않는 인증서 유형을 사용하는 경우 및 일반 TLS 프로토콜 오류를 표시합니다. |
| 자원 | 충분한 메모리 부족과 같은 오류. |
| 재개 | 재개 세션 ID 및 티켓과 관련된 세션 재개 오류, 방화벽 캐시의 재개 세션 항목 및 기타 세션 재개 오류. |
| 버전 | 클라이언트 및 복호화 프로파일 버전 불일치 및 클라이언트 및 서버 버전 불일치에 관한 오류입니다.<br>오류 메시지에는 지원되는 클라이언트 및 복호화 프로파일 버전을 식별하는 비트마스크 값이 포함됩니다. 비트마스크 값을 사용하여 클라이언트가 사용하려고 시도한 암호를 식별하고 이 항목의 뒷부분에 설명된 대로 복호화 프로파일이 지원하는 암호 값을 나열합니다. |

오류에 대한 적절한 오류 설명 카테고리가 없는 경우 기본 메시지는 일반 ***TLS*** 프로토콜 오류입니다.

버전 및 암호 로그 오류 정보에는 작동 가능한 CLI 명령을 사용하여 실제 값으로 변환하는 비트마스크 값이 포함됩니다.

- 버전 오류 비트마스크 값은 클라이언트와 서버가 사용하는 TLS 프로토콜 버전 간의 불일치를 식별하고 클라이언트와 트래픽에 적용된 복호화 프로파일 간의 TLS 프로토콜 불일치도 식별합니다. 버전 오류 비트마스크를 변환하는 CLI 명령은 다음과 같습니다.

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-version
   <bitmask-value>
  ```

  이 명령은 비트마스크와 일치하는 TLS 버전을 반환합니다.
- 암호 오류 비트마스크 값은 클라이언트와 트래픽에 적용된 복호화 프로파일 간의 암호화 및 기타 불일치를 식별합니다.

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher <bitmask-
  value>
  ```

  이 명령은 비트 마스크와 일치하는 암호를 반환합니다.

해당 사이트에 대한 액세스를 허용하려는 경우, 복호화 로그를 필터링하여 버전 및 암호 오류를 찾고, 오류가 있는 세션의 비트마스크 값을 적절한 CLI 명령에 연결하고, 오류를 일으킨 프로토콜 버전 또는 암호의 값을 얻고, 정보를 사용하여 복호화 정책 또는 프로파일을 업데이트합니다.

- 버전 오류
- 암호 오류

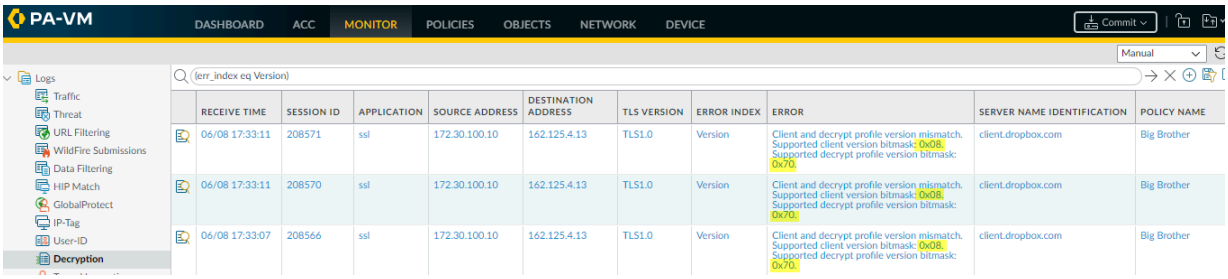

©2023 Palo Alto Networks, Inc.

- 루트 상태 "검사되지 않음"

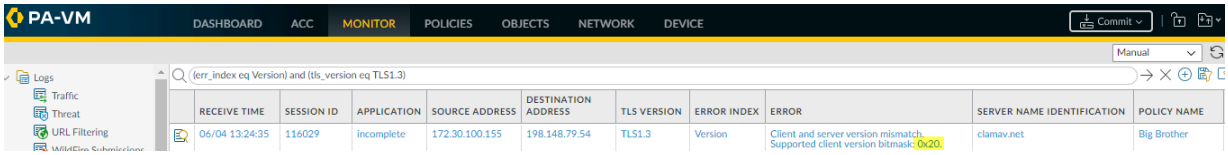
버전 오류

버전 불일치 오류를 식별하고 수정하려면:

1. 복호화 로그를 필터링하여 필터**(err_index eq Version)**를 사용하여 버전 오류를 식별합니다. 강조 표시된 값은 비트마스크 값입니다.




다양한 방법으로 복호화 로그를 필터링할 수 있습니다. 예를 들어 TLSv1.3 버전 오류만 보려면 필터**(err_index eq 버전) 및 (tls_version eq TLS1.3)**을 사용합니다.




2. CLI에 로그인하고 비트마스크 값을 찾습니다. 첫 번째 스크린샷의 버전 오류(세 세션 모두에 동일한 오류)는 클라이언트 및 복호화 프로파일 불일치 문제를 보여줍니다. 지원되는 클라이언트 버전 비트마스크는 0x08이고 지원되는 복호화 프로파일 버전 비트마스크는 0x70입니다.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

이 출력은 클라이언트가 TLSv1.0만 지원하는 것을 보여줍니다.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

이 출력은 복호화 프로파일이 TLSv1.1, TLSv1.2 및 TLSv1.3을 지원하지만 TLSv1.0은 지원하지 않음을 보여줍니다. 이제 문제는 클라이언트가 매우 오래된 버전의 TLS 프로토콜만 지원하고 트래픽을 제

 ©2023 Palo Alto Networks, Inc.

어하는 복호화 정책 규칙에 연결된 복호화 프로파일이 TLSv1.0 트래픽을 허용하지 않는다는 사실을 알고 있습니다.

다음으로 할 일은 취해야 할 조치를 결정하는 것입니다. 더 안전한 TLS 버전을 허용하도록 클라이언트를 업데이트할 수 있습니다. 어떤 이유로 클라이언트에 TLSv1.0이 필요한 경우 방화벽이 계속해서 트래픽을 차단하도록 하거나 모든 TLSv1.0 트래픽을 허용하도록 암호 복호화 프로파일을 업데이트할 수 있습니다(권장하지 않음). 또는 TLSv1.0을 허용하는 암호 복호화 정책 및 프로파일을 만들고 TLSv1.0을 사용해야 하고 더 안전한 프로토콜(트래픽을 허용하는 가장 안전한 옵션)을 지원할 수 없는 클라이언트 디바이스에만 적용할 수 있습니다.

두 번째 스크린샷의 버전 오류는 클라이언트와 서버 버전 불일치라는 다른 문제를 보여줍니다. 오류는 지원되는 클라이언트 비트마스크를 0x20으로 나타냅니다.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x20
```

```
TLSv1.2
```

출력은 클라이언트가 TLSv1.2만 지원함을 보여줍니다. 서버가 TLSv1.2를 지원하지 않기 때문에 TLSv1.3만 지원하거나 TLSv1.1 이하(보안 수준이 낮은 프로토콜)만 지원할 수 있습니다. Wireshark 또는 다른 패킷 분석 도구를 사용하여 서버가 지원하는 TLS 버전을 확인할 수 있습니다. 서버가 지원하는 항목에 따라 다음을 수행할 수 있습니다.

- 서버가 TLSv1.3만 지원하는 경우 TLSv1.3을 지원하도록 복호화 프로파일을 편집할 수 있습니다.
- 서버가 TLSv1.1 이하만 지원하는 경우 비즈니스상의 이유로 해당 서버에 액세스해야 하는지의 여부를 평가하십시오. 그렇지 않은 경우 보안을 강화하기 위해 트래픽을 차단하는 것이 좋습니다. 비즈니스 목적으로 서버에 액세스해야 하는 경우 비즈니스를 위해 액세스해야 하는 서버 및 사이트에만 적용되는 복호화 정책에 서버를 만들거나 추가합니다. 덜 안전한 TLS 버전을 사용하는 모든 서버에 대한 액세스를 허용하지 마십시오.

3. 세션 트래픽을 제어하는 복호화 정책을 찾으려면 로그에서 정책 이름 열을 확인하십시오(또는 복호화 로그 옆에 있는 돋보기 아이콘 을 클릭하여 상세 로그 보기의 일반 섹션에서 정보를 확인하십시오). 위의 예에서 복호화 정책 이름은 Big Brother입니다. 복호화 정책 및 프로파일을 찾으려면 **Policies** > **Decryption**으로 이동하여 Big Brother라는 정책을 선택한 다음 옵션 탭을 선택합니다. 복호화 프로파일에는 복호화 프로파일의 이름이 표시됩니다.

   **Objects** > **Decryption** > **Decryption Profile**로 이동하여 적절한 복호화 프로파일을 선택한 다음 버전 문제를 해결하도록 편집합니다.

암호 오류

암호 오류를 찾기 위해 복호화 로그를 사용하는 것은 버전 오류 찾기와 유사합니다. 로그를 필터링하여 오류를 찾고 오류 비트마스크를 얻습니다. 그런 다음 CLI로 이동하여 비트 마스크를 오류 값으로 변환 한 다음 적절한 조치를 취하여 문제를 해결합니다. 예:

1. 암호 해독 로그를 필터링하여 필터 **(err_index eq 암호)**를 사용하여 암호 오류를 식별합니다. 예를 들어, 지원되지 않는 암호라는 오류 메시지 `가 있는 암호 오류를 조사해 보겠습니다. 지원되는 클라이언트 암호 비트마스크: 0x80000000. 프로파일 암호 비트마스크 0x60f79980 복호화을 지원합니다.`

 ©2023 Palo Alto Networks, Inc.

2. CLI에 로그인하고 비트마스크 값을 찾습니다.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
CHACHA_PLY1305_SHA256
```

이 출력은 클라이언트가 방화벽이 지원하는 암호를 협상하려고 시도했음을 보여줍니다(비트마스크가 모두 0인 경우(`0x0000000`이면 클라이언트가 방화벽이 지원하지 않는 암호 협상을 시도함).

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS13_WITH_AES_256_GCM_SHA384
TLS13_WITH_AES_128_GCM_SHA256
```

이 출력은 트래픽을 제어하는 복호화 프로파일이 많은 암호를 지원하지만 클라이언트가 사용하려는 암호를 지원하지 않음을 보여줍니다.

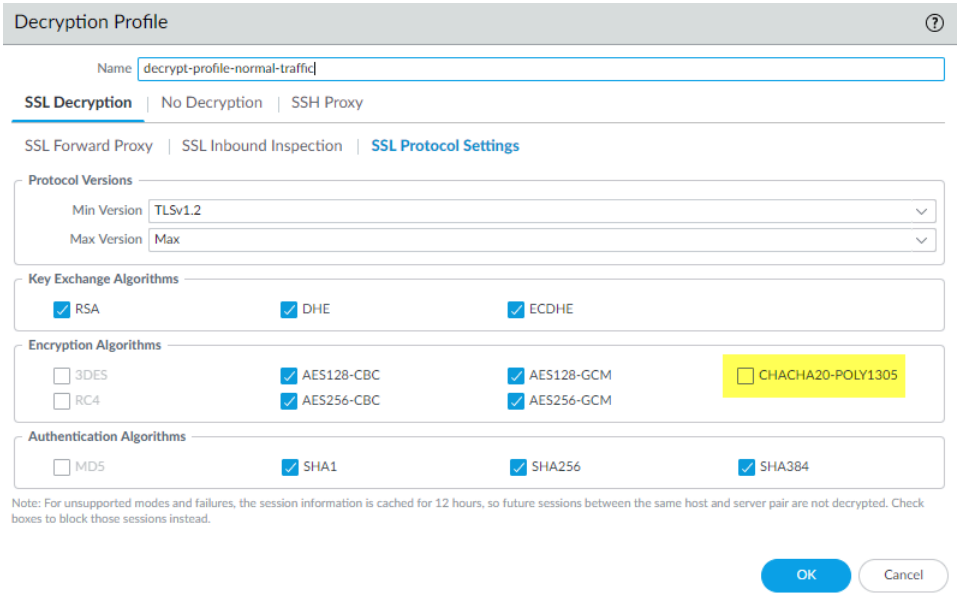
방화벽이 트래픽을 허용하고 복호화하도록 이 문제를 수정하려면 복호화 프로파일에 누락된 암호에 대한 지원을 추가해야 합니다.

3. 복호화 로그 또는 상세 로그 보기 정책 이름을 확인하여 트래픽을 제어하는 복호화 정책의 이름을 가져옵니다. **Policies** > **Decryption**으로 이동하여 정책을 선택합니다. 옵션 탭에서 복호화 프로파일의 이

 ©2023 Palo Alto Networks, Inc.

름을 찾습니다. 그런 다음 **Objects** > **Decryption** > **Decryption Profile**로 이동하여 적절한 복호화 프로파일을 선택한 다음 버전 문제를 해결하도록 편집합니다.

이 예에서 복호화 프로파일은 TLS13_WITH_CHACHA_POLY1305_SHA256 암호를 지원하지 않으므로 클라이언트가 연결할 수 없습니다.




이 문제를 해결하려면 **CHACHA20-POLY1305** 암호화 알고리즘 옵션을 선택하고(**Max**의 **Max** 버전 설정은 프로파일이 이미 TLSv1.3 및 인증을 지원함을 의미합니다. 알고리즘 설정에는 이미 SHA256이 포함되어 있으므로 암호화 알고리즘 지원만 누락됨), 그 다음 구성을 **Commit**합니다. 구성을 커밋하면 복호화 프로파일이 누락된 암호를 지원하고 트래픽에 대한 복호화 세션이 성공합니다.

방화벽이 암호 제품군을 지원하지 않고 비즈니스 목적으로 트래픽을 허용해야 하는 경우 해당 트래픽에만 적용되는 복호화 정책 및 프로파일을 생성합니다. 복호화 프로파일에서 지원되지 않는 암호 그룹이 있는 세션 차단 옵션을 비활성화합니다

.

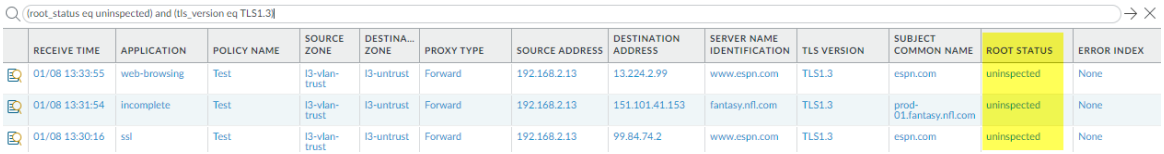
루트 상태 "검사되지 않음"

경우에 따라 루트 상태 열에 검사되지 않은 값이 표시됩니다. 방화벽이 루트 상태를 검사할 수 없는 이유는 다음과 같습니다.

- 세션 재개.
- 비복호화 정책이 트래픽을 제어했기 때문에 트래픽이 복호화되지 않았으므로 방화벽이 트래픽을 복호화하지 않았습니다.
- 방화벽이 서버 인증서를 검사하기 전에 복호화 실패가 발생했습니다.

복호화 로그**(root_status eq uninspected)** 및 **(tls_version eq TLS1.3)**을 필터링하여 루트 상태가 검사되지 않은 복호화 세션을 확인합니다.


©2023 Palo Alto Networks, Inc.


(root_status eq uninspected) and (tls_version eq TLS1.3)

| | RECEIVE TIME | APPLICATION | POLICY NAME | SOURCE ZONE | DESTINA... ZONE | PROXY TYPE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVER NAME IDENTIFICATION | TLS VERSION | SUBJECT COMMON NAME | ROOT STATUS | ERROR INDEX |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 01/08 13:33:55 | web-browsing | Test | l3-vlan-trust | l3-untrust | Forward | 192.168.2.13 | 13.224.2.99 | www.espn.com | TLS1.3 | espn.com | uninspected | None |
| | 01/08 13:31:54 | incomplete | Test | l3-vlan-trust | l3-untrust | Forward | 192.168.2.13 | 151.101.41.153 | fantasy.nfl.com | TLS1.3 | prod-01.fantasy.nfl.com | uninspected | None |
| | 01/08 13:30:16 | ssl | Test | l3-vlan-trust | l3-untrust | Forward | 192.168.2.13 | 99.84.74.2 | www.espn.com | TLS1.3 | espn.com | uninspected | None |

## 불완전한 인증서 체인 수리

RFC 5246 TLSv1.2 표준에 따라 인증된 서버가 유효한 인증서 체인을 제공해야 허용 가능한 인증서 권한을 제공해야 하는 경우에도 모든 웹사이트가 전체 인증서 체인을 보내는 것은 아닙니다. 복호화를 활성화하고 복호화 정책에서 신뢰할 수 없는 발급자를 가진 블록 세션을 가능하게 하는 전방 프록시 복호화 프로파일을 적용하면 웹사이트의 서버가 방화벽에 제공하는 인증서 목록에서 중간 인증서가 없는 경우 방화벽은 인증서 체인을 맨 위(루트) 인증서로 구성할 수 없습니다. 이러한 경우 방화벽은 방화벽이 루트 인증서에 대한 체인을 구성할 수 없고 누락된 중간 인증서 없이는 트러스트를 만들 수 없으므로 클라이언트에 위임 취소 인증서를 제공합니다.

방화벽에는 기본 신뢰할 수 있는 인증서 권한 저장소에 루트 인증서만 있습니다.

비즈니스 목적으로 통신해야 하는 웹사이트에 하나 이상의 누락된 중간 인증서가 있고 복호화 프로파일이 신뢰할 수 없는 발급자와 세션을 차단하면 누락된 중간 인증서를 찾아 다운로드하여 방화벽이 사이트의 서버를 신뢰할 수 있도록 방화벽에 신뢰할 수 있는 루트 CA로 설치할 수 있습니다. (대안은 웹사이트 소유자에게 연락하여 핸드쉐이크 중에 중간 인증서를 보낼 수 있도록 서버를 구성하도록 요청하는 것입니다.)

복호화 프로파일에서 신뢰할 수 없는 발급자가 있는 세션을 허용하는 경우 방화벽은 발급자가 신뢰할 수 없는 경우에도 세션을 설정합니다. 그러나 더 나은 보안을 위해 신뢰할 수 없는 발급자와 세션을 차단하는 것이 좋습니다.

**STEP 1 |** 불완전한 인증서 체인 오류를 일으키는 웹사이트를 찾습니다.

1. 복호화 로그를 필터링하여 불완전한 인증서 체인으로 인해 실패한 복호화 세션을 식별합니다.

   필터 필드에 쿼리 **(err_index eq Certificate)** 및 **(오류에 'http' 포함)**을 입력합니다. 이 쿼리는 CA 발급자 URL(URI라고도 함)이 포함된 모든 오류 항목을 찾는 문자열 "http"가 포함된 인증서 오류에 대한 로그를 필터링합니다. CA 발급자 URL은 CA 발급자의 AIA(기관 정보 액세스) 정보입니다.

2. 오류 열 항목을 클릭하면 "클라이언트로부터 치명적인 경고 UnknownCA를 받았습니다. CA 발급자 URL:" 다음에 URI가 옵니다.

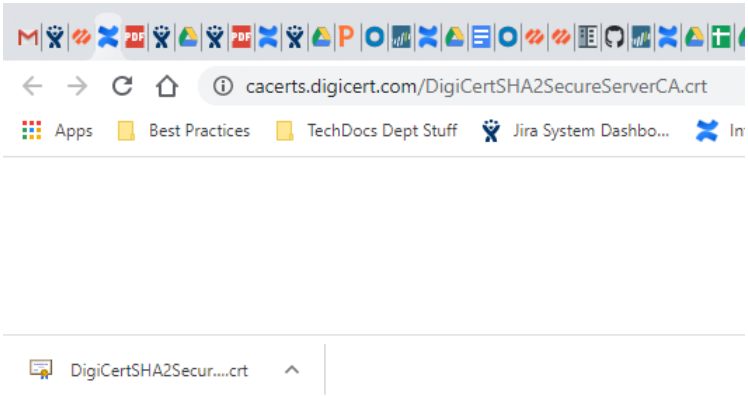
   
   ived fatal alert UnknownCA from client, CA Issuer URL: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt' )

   | ROOT STATUS | SUBJECT COMMON NAME | ISSUER COMMON NAME | CERTIFICATE KEY TYPE | CERTIFICATE KEY SIZE | SERVER NAME IDENTIFICATION | TLS VERSION | KEY EXCHANGE | ENCRYPTION ALGORITHM | NEGOTIATED EC CURVE | AUTHENTICATION ALGORITHM | ERROR | ERROR INDEX |
   |---|---|---|---|---|---|---|---|---|---|---|---|---|
   | untrusted | *.badssl.com | DigiCert SHA2 Secure Server CA | RSA | 2048 | incomplete-chain.badssl.com | TLS1.2 | ECDHE | AES_128_GCM | secp256r1 | SHA256 | Received fatal alert UnknownCA from client, CA Issuer URL: http://cacerts.digicert.... | Certificate |

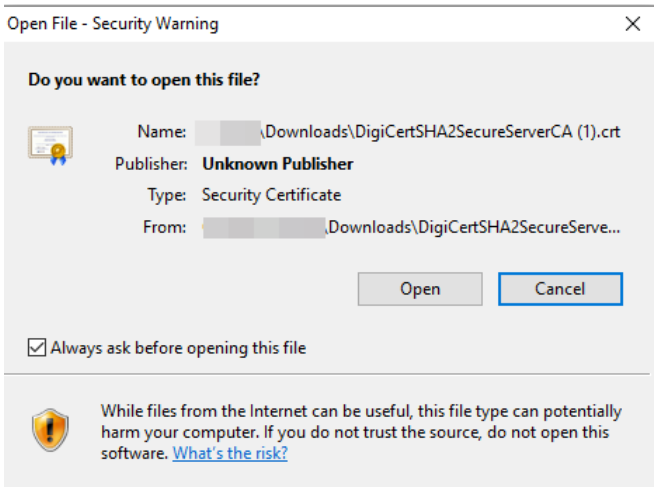
   방화벽은 자동으로 쿼리에 선택한 오류를 추가하고 전체 URI 경로를 표시합니다(전체 URI 경로가 오류 열에서 잘릴 수 있음).


©2023 Palo Alto Networks, Inc.

**STEP 2 |** URI를 브라우저에 복사한 다음 Enter를 눌러 누락된 중간 인증서를 다운로드합니다.

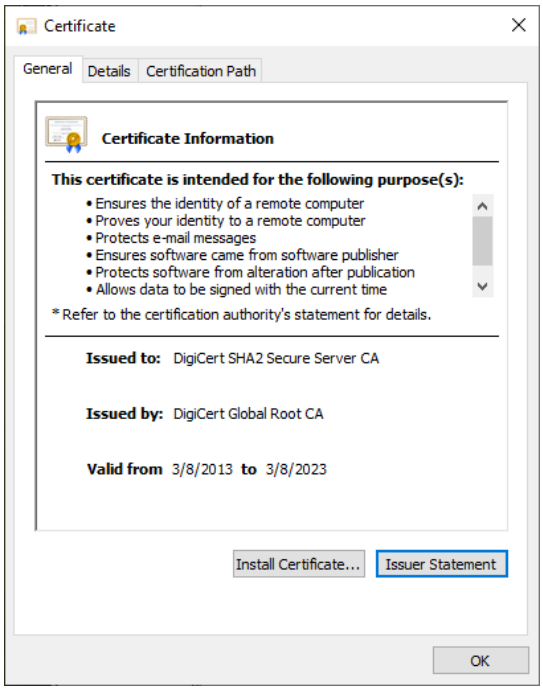



**STEP 3 |** 대화 상자를 열려면 인증서를 클릭합니다.

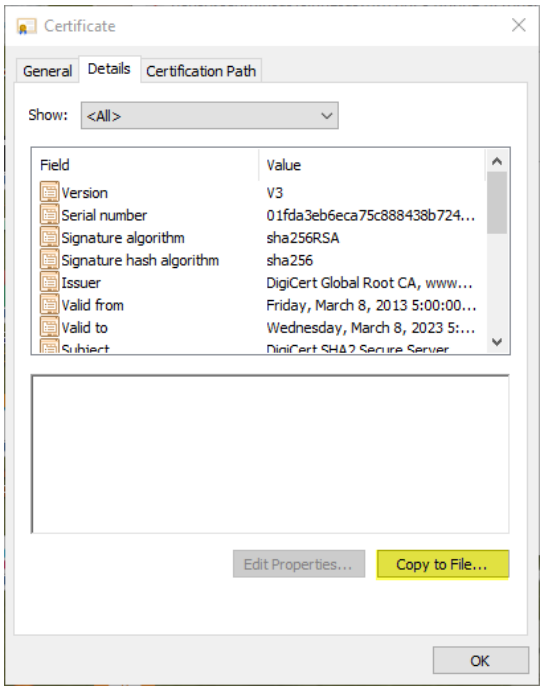



 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 인증서 파일을 열려면 열기를 클릭합니다.




**STEP 5 |** 세부 정보 탭을 선택한 다음 파일로 복사...를 클릭합니다.

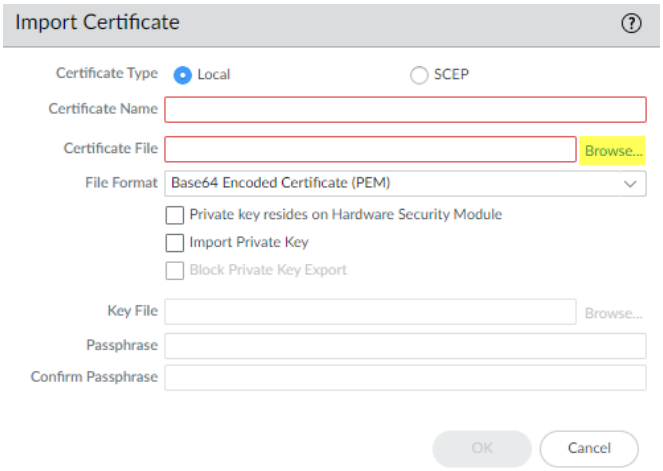



내보내기 지침을 따릅니다. 인증서는 기본 다운로드 폴더로 지정된 폴더에 복사됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 인증서를 방화벽으로 가져옵니다.

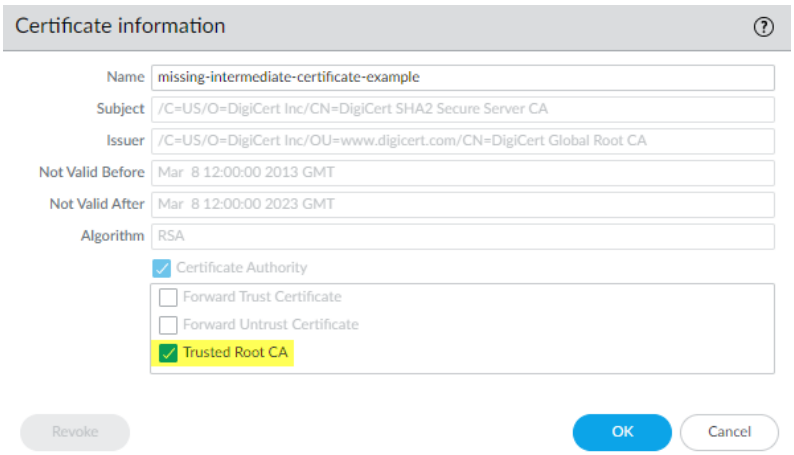
1. 디바이스 > 인증서 관리 > 인증서로 이동한 다음 가져오기를 선택합니다.
2. 누락된 중간 인증서를 저장한 폴더로 찾아보기하여 선택합니다. 파일 형식은 **Base64** 인코딩 인증서**(PEM)**로 그대로 둡니다.




3. 인증서의 이름을 지정하고 사용하려는 다른 옵션을 지정한 다음 확인을 클릭합니다.

**STEP 7 |** 인증서를 불러온 경우 디바이스 인증서 목록에서 인증서를 선택하여 인증서 정보 대화 상자를 엽니다.

**STEP 8 |** 신뢰할 수 있는 루트 **CA**를 선택하여 인증서를 방화벽에서 신뢰할 수 있는 루트 CA로 표시한 다음 확인을 클릭합니다.




디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서 에서 불러온 인증서가 인증서 목록에 나타납니다. 사용 열을 확인하여 상태가 신뢰할 수 있는 루트 **CA** 인증서인지 확인하여 방화벽이 인증서를 신뢰할 수 있는 루트 CA로 간주했는지 확인합니다.

**STEP 9 |** 구성을 커밋합니다.

**STEP 10 |** 이제 깨진 인증서 체인을 복구했습니다.

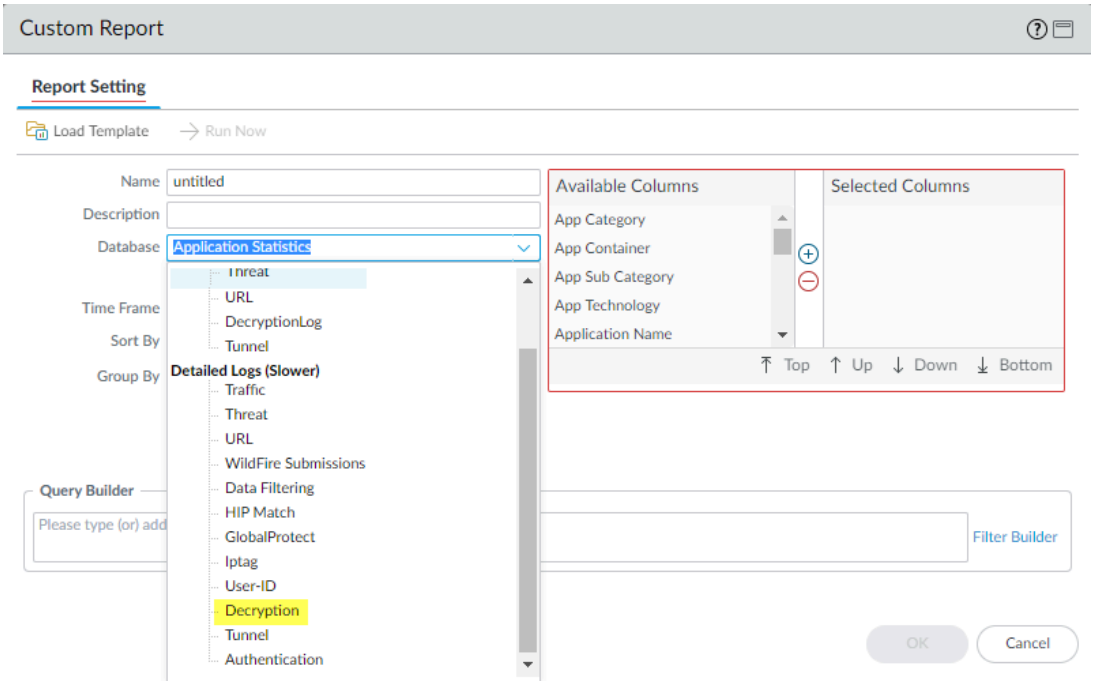
CA 발급자가 더 이상 신뢰할 수 없기 때문에 방화벽이 트래픽을 차단하지 않습니다. 누락된 모든 중간 인증서에 대해 이 프로세스를 반복하여 인증서 체인을 복구합니다.


©2023 Palo Alto Networks, Inc.

# 복호화를 위한 맞춤 리포트 템플릿

맞춤 리포트를 생성하고 복호화 로그 필드 및 사용자 지정 템플릿을 기반으로 복호화 이벤트에 대해 생성할 수 있습니다. 맞춤 리포트에 포함할 로그 필드를 선택한 다음 템플릿을 선택하여 로그 쿼리를 구체화합니다.

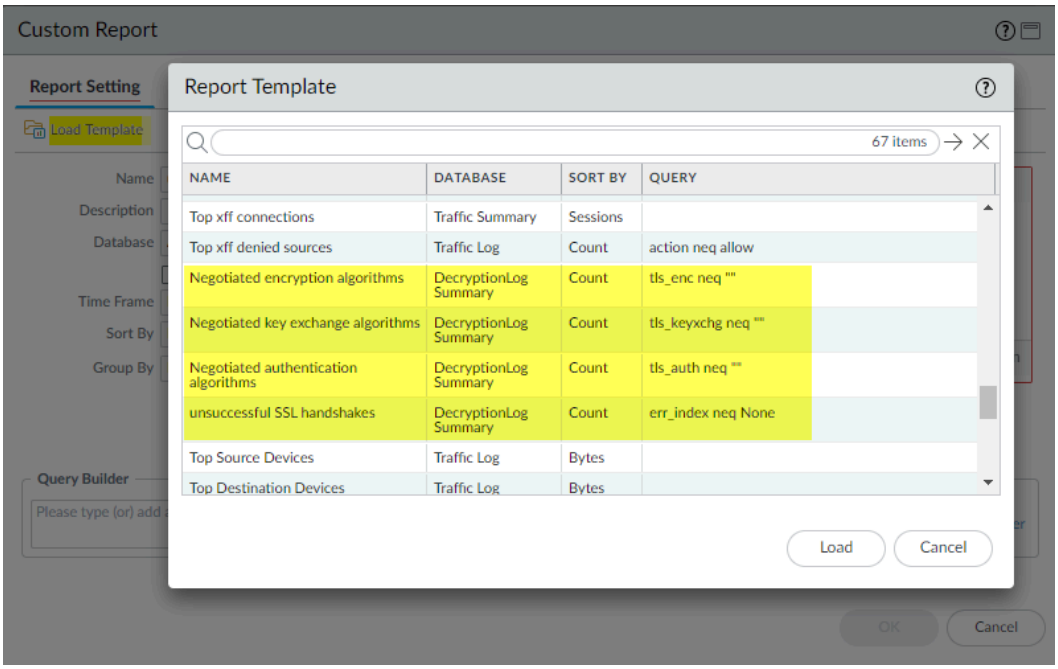
1. 모니터 > 맞춤 보고서 관리.
2. 맞춤 리포트를 추가합니다.
3. 맞춤 리포트에서 사용할 복호화 로그 필드를 구성하려면 복호화를 데이터베이스로 선택합니다.




사용 가능한 열 목록은 복호화 로그에서 사용할 수 있는 열과 일치하도록 변경 사항입니다. 맞춤 리포트에 포함할 열(정보)을 선택한 다음 추가합니다. 맞춤 리포트를 더 자세히 구체화하지 않으려면 확인을 클릭하여 보고서를 생성합니다.


©2023 Palo Alto Networks, Inc.

4. 원하는 경우 쿼리 빌더와 PAN-OS 10.0에 도입된 네 개의 템플릿을 사용하여 사용자 지정 복호화 보고서의 출력을 구체화합니다. 보고서 출력을 필터링하는 템플릿을 선택하려면 템플릿 로드를 클릭하고 네 개의 복호화 템플릿에서 선택합니다.




쿼리 열에는 각 템플릿이 나타내는 필터 쿼리가 표시됩니다. 원하는 쿼리를 로드한 다음 확인을 클릭하여 맞춤 리포트를 생성합니다.

## 프록시 유형 및 TLS 버전별로 지원되지 않는 매개 변수

복호화 로그 필드에는 각 복호화 프록시 유형에 대한 복호화 세션 매개 변수가 표시됩니다. 그러나 버전 지원, TLS 핸드쉐이크의 암호화된 부분, 정보 가용성 등의 이유로 일부 매개 변수는 모든 프록시 유형 또는 TLS 버전에 사용할 수 없습니다. 다음 표에는 프록시 유형 및 TLS 버전별로 지원되지 않는 복호화 로그 매개 변수가 표시됩니다.

| 프록시 유형 | 지원되지 않는 매개 변수 | TLS 버전 |
|---|---|---|
| 포워드 프록시 | 협상된 EC 커브 | TLSv1.3 |
| 인바운드 검사 | 서버 이름 식별<br>루트 공통 이름 | 모두 |
| | 협상된 EC 커브 | TLSv1.3 |
| 비복호화(복호화 정책 규칙에서복호화 작업 없음) | 협상된 EC 커브<br>서버 이름 식별 | TLSv1.2 |
| | 협상된 EC 커브<br>서버 이름 식별 | TLSv1.3 |


©2023 Palo Alto Networks, Inc.

| 프록시 유형 | 지원되지 않는 매개 변수 | TLS 버전 |
|---|---|---|
| | 인증서 정보(예: 인증서 시작 날짜, 인증서 종료 날짜, 인증서 키 유형 등)와 같은 모든 인증서 정보 필드 | |
| 네트워크 패킷 브로커 | 협상된 EC 커브 | TLSv1.3 |
| GlobalProtect 포털 | 서버 이름 식별<br>루트 공통 이름<br>복호화 정책 이름<br>App-ID | 모두 |
| GlobalProtect Gateway | 서버 이름 식별<br>복호화 정책 이름<br>App-ID | 모두 |
| Clientless SSLVPN | 서버 이름 식별 | 모두 |
| SSH | 복호화 로그가 지원되지 않음 | |
| 클리어텍스트 | 복호화 로그가 지원되지 않음 | |

## 복호화 문제 해결 워크플로 예제

복호화 로그 및 ACC(Application Command Center)의 SSL 활동 위젯은 독립적으로 또는 함께 작동하는 강력한 복호화 문제 해결 도구를 제공합니다. 이러한 도구를 사용하는 방법을 이해하면 광범위한 복호화 문제를 조사하고 해결할 수 있습니다.

다음 예에서는 문제 해결 도구를 사용하여 복호화 문제를 식별, 조사 및 해결하는 방법을 보여줍니다. 이러한 방법을 적용하여 복호화 배포에서 발생하는 문제를 해결하십시오.

- 복호화 실패 원인 조사
- 지원되지 않는 암호 제품군 문제 해결
- 약한 프로토콜 및 암호 제품군 식별
- 신뢰할 수 없는 CA 인증서 식별
- 만료된 인증서 문제 해결
- 해지된 인증서 문제 해결
- 고정된 인증서 문제 해결

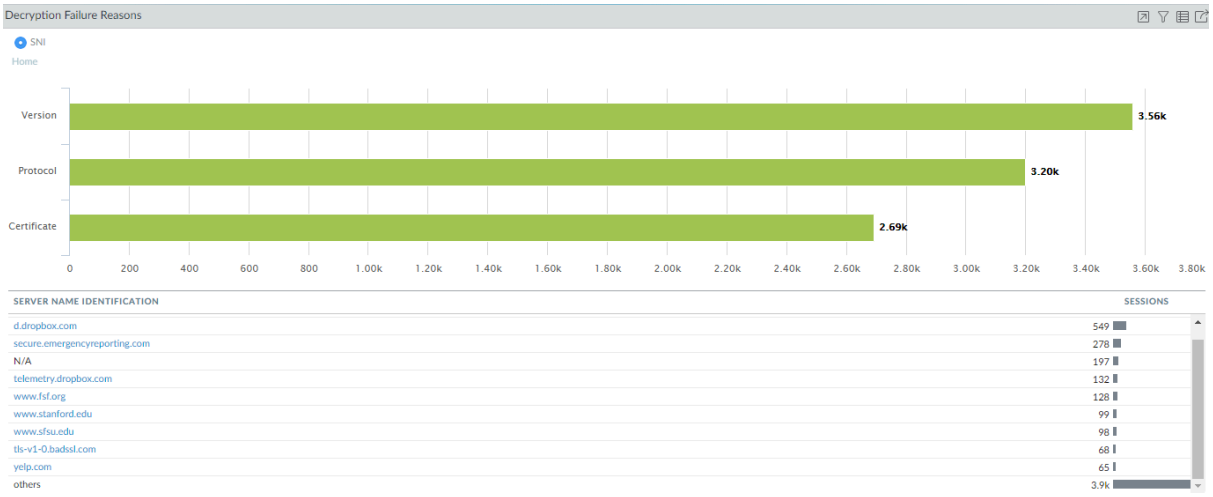
### 복호화 실패 원인 조사

복호화 오류의 가장 일반적인 이유는 TLS 프로토콜 오류, 암호 버전 오류(클라이언트 및 서버 버전 불일치 및 클라이언트 및 복호화 프로파일 버전 불일치) 및 인증서 오류입니다. 복호화 오류를 조사하려면


©2023 Palo Alto Networks, Inc.

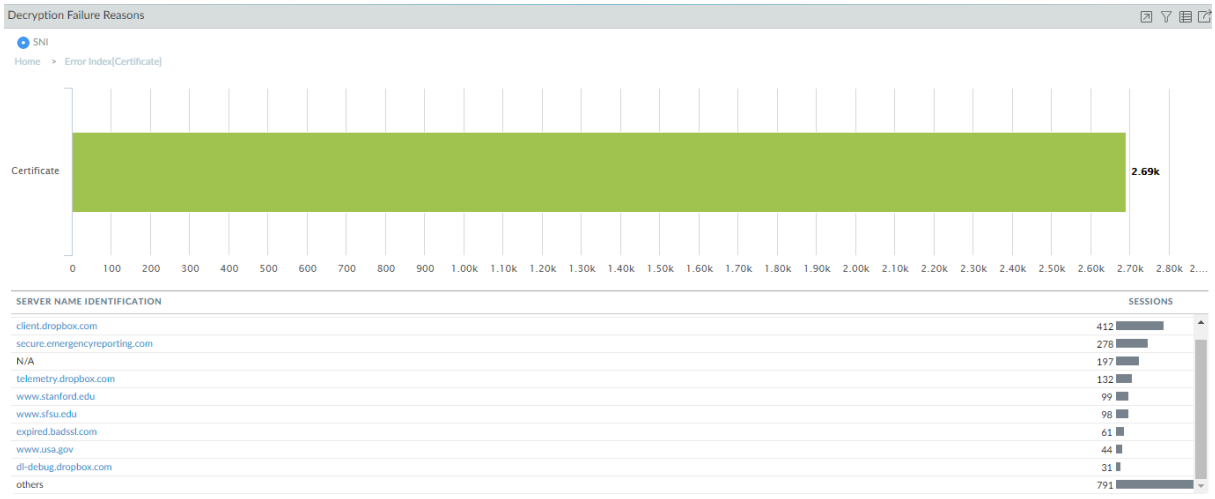
ACC(애플리케이션 명령 센터)로 시작하여 오류를 식별한 다음 복호화 로그로 이동하여 세부 정보로 드릴 다운합니다.

**STEP 1 |** **ACC** > **SSL** 활동에서 조사를 시작하고 복호화 실패 이유 위젯을 살펴보십시오.




이 예제에서는 인증서 오류를 조사합니다. 동일한 프로세스를 사용하여 버전 및 프로토콜 오류를 조사할 수 있습니다.

**STEP 2 |** 인증서 오류가 발생한 호스트(SNI)와 인증서 오류가 가장 많이 발생한 호스트 목록을 보려면 인증서 옆에 있는 녹색 막대를 클릭하십시오.




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 모니터 > 로그 > 암호 해독으로 이동하여 로그를 드릴다운합니다.

쿼리 **(err_index eq 인증서)**를 사용하여 복호화 로그를 필터링하여 인증서 오류가 발생한 모든 복호화 세션을 봅니다.

(err_index eq Certificate)

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 13:22:11 | 205207 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/08 11:17:14 | 203671 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Expired server certificate. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:14 | 203669 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:11 | 203666 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:11 | 203663 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:16:18 | 203598 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:16:18 | 203576 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked |
| 06/08 11:16:18 | 203575 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked |
| 06/04 18:26:34 | 123731 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |

오류 열에는 인증서 오류의 이유가 표시됩니다. 동일한 오류가 있는 모든 복호화 세션을 필터링하려면 오류 메시지를 클릭하여 쿼리에 추가한 다음 쿼리를 실행합니다. 예를 들어, 클라이언트로부터 치명적인 경고 수신을 기반으로 모든 오류를 찾으려면 오류를 클릭하면 쿼리 **(err_index eq Certificate)** 및 **(error eq 'Received fatal alert CertificateUnknown from client')**가 생성됩니다.

(err_index eq Certificate) and ( error eq 'Received fatal alert CertificateUnknown from client' )

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 13:22:11 | 205206 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/08 13:22:11 | 205207 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/04 18:26:34 | 123731 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/04 18:26:34 | 123732 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |

특정 호스트가 받은 인증서 오류를 필터링하려면 오류 메시지 텍스트를 추가하는 대신 쿼리에 SNI를 추가합니다. 예를 들어 expired.badssl.comm에 대한 모든 인증서 오류를 찾으려면 **(err_index eq Certificate)** 및 **(sni eq 'expired.badssl.com')**를 사용합니다.

(err_index eq Certificate) and (sni eq 'expired.badssl.com')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/02 17:17:20 | 12959 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12957 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12955 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12958 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:17:18 | 12956 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:17:18 | 12951 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:11:48 | 12802 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |

오류 열은 expired.badssl.com 연결된 각 인증서 오류에 대한 구체적인 이유를 표시합니다.

복호화 실패를 일으킨 인증서 문제의 원인을 알게 되면 문제를 해결할 수 있습니다. 예를 들어 인증서 체인이 불완전한 경우 불완전한 인증서 체인을 복구할 수 있습니다. 인증서가 만료된 경우 사이트 관리자에게 알리거나 사이트에 액세스해야 하는 경우 정책 기반 예외를 만들 수 있습니다.


©2023 Palo Alto Networks, Inc.

## 지원되지 않는 암호 제품군 문제 해결

복호화 로그에서 지원되지 않는 암호 모음을 식별하고 문제를 해결하는 것은 버전 오류 조사의 한 부분이며 자체적으로 검토할 가치가 있습니다.

**STEP 1 |** 암호 해독 로그(**Monitor** > **Logs** > **Decryption**)에서 쿼리 **(오류에 '클라이언트 및 암호 해독 프로파일 불일치' 포함)**를 **사용합니다.** - 모든 암호 제품군 버전 불일치를 식별합니다.

이러한 불일치에 대한 로그를 필터링하면 클라이언트와 복호화 프로파일 암호 제품군 지원이 일치하지 않는 모든 인스턴스가 식별됩니다.

(error contains 'Client and decrypt profile version mismatch')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|
| 06/16 09:41:22 | 99445 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:22 | 99444 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99441 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99440 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |

동일한 오류가 발생한 모든 복호화 세션을 찾으려면 오류 메시지를 클릭하여 쿼리에 추가하고 원래 쿼리를 제거합니다. 예를 들면 다음과 같습니다.

( error eq 'Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. ')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|
| 06/16 09:41:22 | 99445 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:22 | 99444 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99441 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99440 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:51 | 99251 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:51 | 99250 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:46 | 99249 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:46 | 99248 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 08:41:21 | 98685 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |

16진수 코드는 클라이언트가 지원하는 정확한 버전과 복호화 프로파일이 지원하는 정확한 버전을 식별합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** CLI에 로그인하고 비트마스크 값을 찾습니다.

이 오류는 클라이언트와 복호화 프로파일이 일치하지 않는 것을 나타냅니다. 지원되는 클라이언트 비트마스크는 0x08이고 지원되는 복호화 프로파일 비트마스크는 0x70입니다.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

이 출력은 클라이언트가 TLSv1.0만 지원하는 것을 보여줍니다.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

이 출력은 복호화 프로파일이 TLSv1.1, TLSv1.2 및 TLSv1.3을 지원하지만 TLSv1.0은 지원하지 않음을 보여줍니다. 이제 클라이언트는 이전 버전의 TLS 프로토콜만 지원하며 트래픽을 제어하는 복호화 정책 규칙에 연결된 복호화 프로파일은 해당 버전을 허용하지 않습니다.

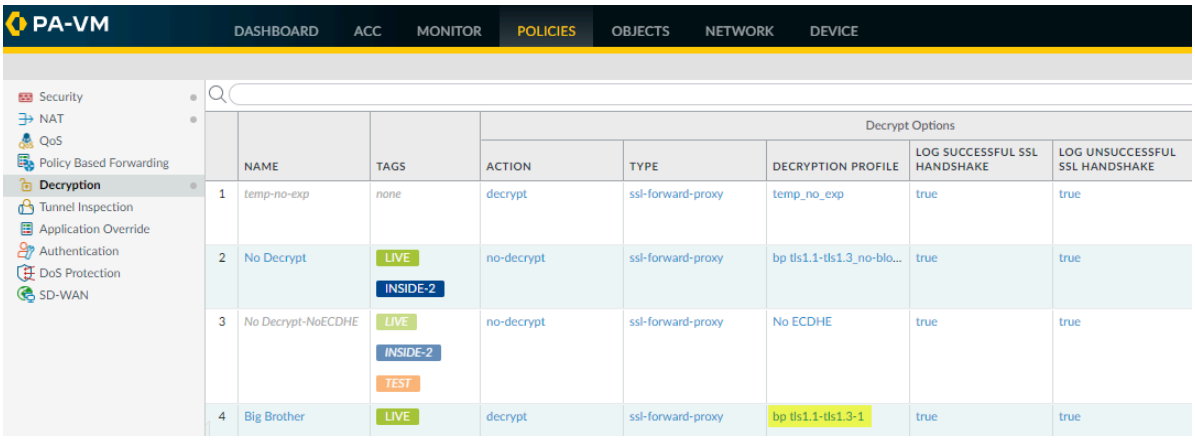
**STEP 3 |** 어떤 조치를 취할지 결정합니다.

더 안전한 TLS 버전을 허용하도록 클라이언트를 업데이트할 수 있습니다. 어떤 이유로 클라이언트에 TLSv1.0이 필요한 경우 방화벽이 계속해서 트래픽을 차단하도록 하거나 모든 TLSv1.0 트래픽을 허용하도록 암호 복호화 프로파일을 업데이트할 수 있습니다(권장하지 않음). 또는 TLSv1.0을 허용하는 암호 복호화 정책 및 프로파일을 만들고 TLSv1.0을 사용해야 하고 더 안전한 프로토콜(트래픽을 허용하는 가장 안전한 옵션)을 지원할 수 없는 클라이언트 디바이스에만 적용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 암호 해독 프로파일을 편집하기로 선택한 경우 세션 트래픽을 제어하는 암호 해독 정책을 찾으려면 로그에서 정책 이름 열을 확인하거나 암호 해독 로그 옆에 있는 돋보기 아이콘 을 클릭하여 자세한 로그 보기의 일반 섹션에 있는 정보를 참조하십시오.

1. 이 예에서 암호 해독 정책 이름은 Big Brother입니다. 암호 해독 프로파일을 찾으려면 정책 > 암호 해독으로 이동하여 암호 해독 프로파일 열을 확인하세요.

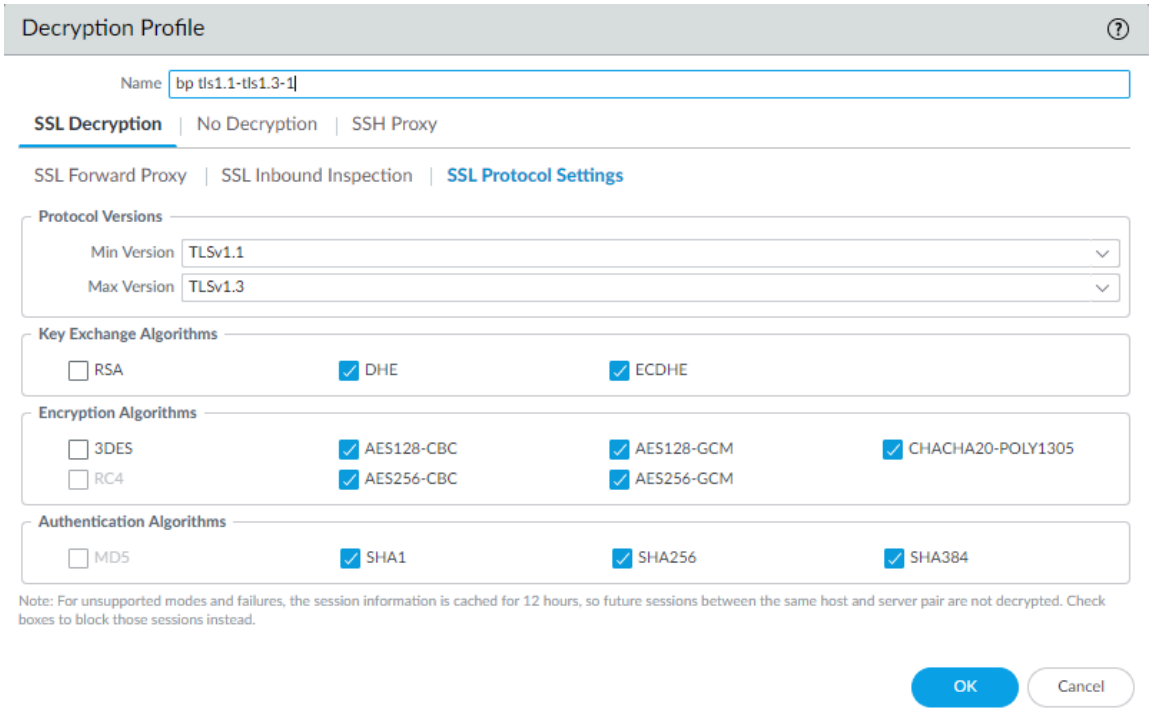



복호화 프로파일의 이름은 **bp tls1.1-tls1.3-1**입니다. Big Brother 정책을 선택한 다음 옵션 탭을 선택하여 복호화 프로파일의 이름을 볼 수도 있습니다.

**Objects** > **Decryption** > **Decryption Profile**로 이동하여 적절한 복호화 프로파일을 선택한 다음 버전 문제를 해결하도록 편집합니다.

2. 개체 > 암호 해독 > 암호 해독 프로파일로 이동합니다.

**bp tls1.1-tls1.3-1** 복호화 프로파일을 선택한 다음 **SSL** 프로토콜 설정 탭을 클릭합니다.




 ©2023 Palo Alto Networks, Inc.

프로파일이 지원하는 최소 TLS 프로토콜 버전(최소 버전)은 TLSv1.1입니다. 버전 불일치가 차단하는 트래픽을 허용하려면 최소 버전을 TLSv1.0으로 변경할 수 있습니다. 그러나 보다 안전한 옵션은 최신 TLS 프로토콜 버전을 사용하도록 클라이언트를 업데이트하는 것입니다. 클라이언트를 업데이트할 수 없는 경우, TLSv1.0 트래픽을 허용하는 일반 암호 해독 정책을 적용하는 대신 해당 사용자, 디바이스 또는 소스 주소(및 하나의 정책과 프로파일이 이 모든 트래픽을 제어할 수 있도록 유사한 사용자, 디바이스 또는 소스 주소에)에만 적용되는 암호 해독 정책 및 프로파일을 만들 수 있습니다.

## 약한 프로토콜 및 암호 제품군 식별

취약한 TLS 프로토콜과 취약한 암호 제품군(암호화 알고리즘, 인증 알고리즘, 키 교환 알고리즘 및 협상된 EC 곡선)은 보안 태세를 약화시키며 강력한 TLS 프로토콜 및 강력한 암호 제품군보다 악성 행위자가 악용하기 쉽습니다.

복호화 로그 항목의 5개 필드는 복호화 세션에 대한 프로토콜 및 암호 제품군을 보여줍니다.

| TLS VERSION | ENCRYPTION ALGORITHM | KEY EXCHANGE | AUTHENTICATI... ALGORITHM | NEGOTIATED EC CURVE |
|---|---|---|---|---|
| TLS1.2 | AES_128_GCM | ECDHE | SHA256 | secp256r1 |
| TLS1.2 | AES_256_GCM | ECDHE | SHA384 | secp256r1 |

오래되고 취약한 TLS 버전 및 암호 제품군을 추적하여 보안 상태를 손상시킬 수 있는 서버 및 애플리케이션과의 연결을 허용할지의 여부에 대해 정보에 입각한 결정을 내릴 수 있습니다.

이 항목의 예는 다음을 수행하는 방법을 보여줍니다.

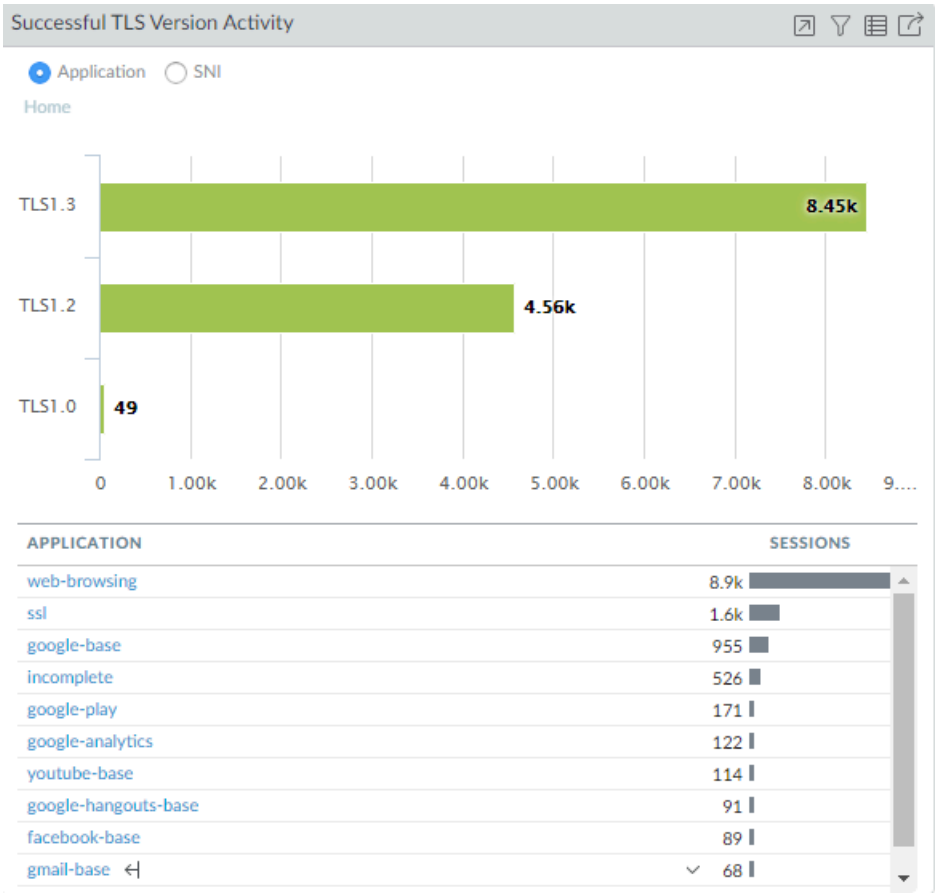
- 덜 안전한 TLS 프로토콜 버전을 사용하는 트래픽을 식별합니다.
- 특정 키 교환 알고리즘을 사용하는 트래픽을 식별합니다.
- 특정 인증 알고리즘을 사용하는 트래픽을 식별합니다.
- 특정 암호화 알고리즘을 사용하는 트래픽을 식별합니다.

이러한 예는 복호화 문제 해결 도구를 다양한 방법으로 사용하여 발생할 수 있는 복호화 문제를 해결하는 데 사용할 수 있는 방법을 보여줍니다.

***Wireshark*** 또는 기타 패킷 분석기를 사용하여 클라이언트 또는 서버가 문제를 일으켰는지의 여부, ***TLS*** 클라이언트 및 서버 버전, 기타 암호 제품군 정보를 다시 확인할 수 있습니다. 이는 버전 불일치 및 기타 문제를 분석하는 데 도움이 될 수 있습니다.

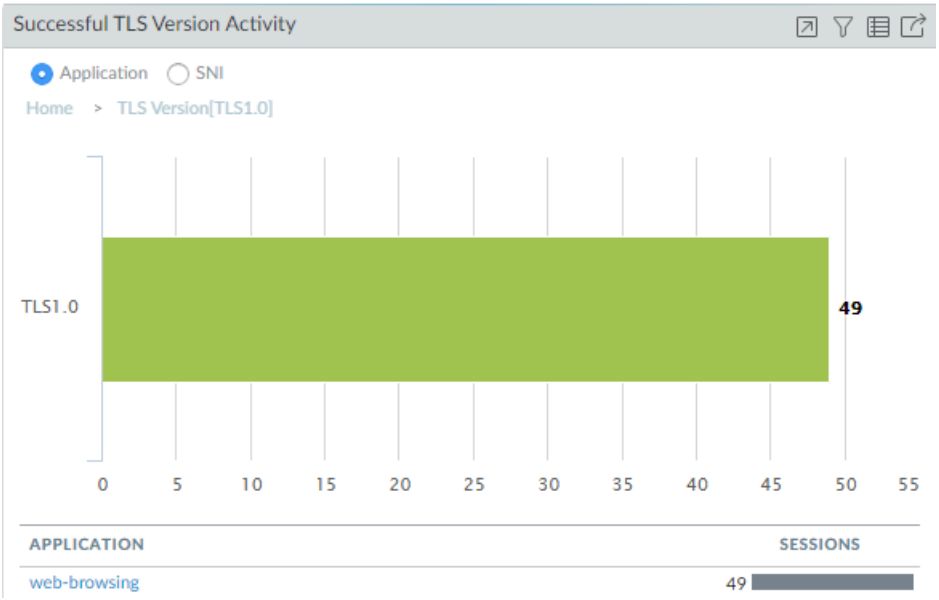

©2023 Palo Alto Networks, Inc.

- **TLS** 프로토콜 - 보안이 취약한 이전 버전의 TLS 프로토콜을 사용하는 트래픽을 식별하여 취약한 프로토콜을 사용하는 서버 및 애플리케이션에 대한 액세스를 허용할지의 여부를 평가할 수 있습니다.
  1. 방화벽이 약한 프로토콜(**ACC** > **SSL** 활동 > 성공적인 **TLS** 버전 활동)을 허용하는지 확인하고 활동에 대한 전반적인 보기를 얻으려면 ACC(애플리케이션 명령 센터)를 확인하여 실시합니다.




이 예에서 성공한 TLS 활동의 대부분은 TLSv1.2 및 TLSv1.3 활동입니다. 그러나 허용되는 TLSv1.0 트래픽의 몇 가지 인스턴스가 있습니다. 숫자 **49**를 클릭하여 TLSv1.0 활동으로 드릴다운하고 어떤 애플리케이션이 TLSv1.0 연결에 성공하는지 확인하겠습니다.


©2023 Palo Alto Networks, Inc.

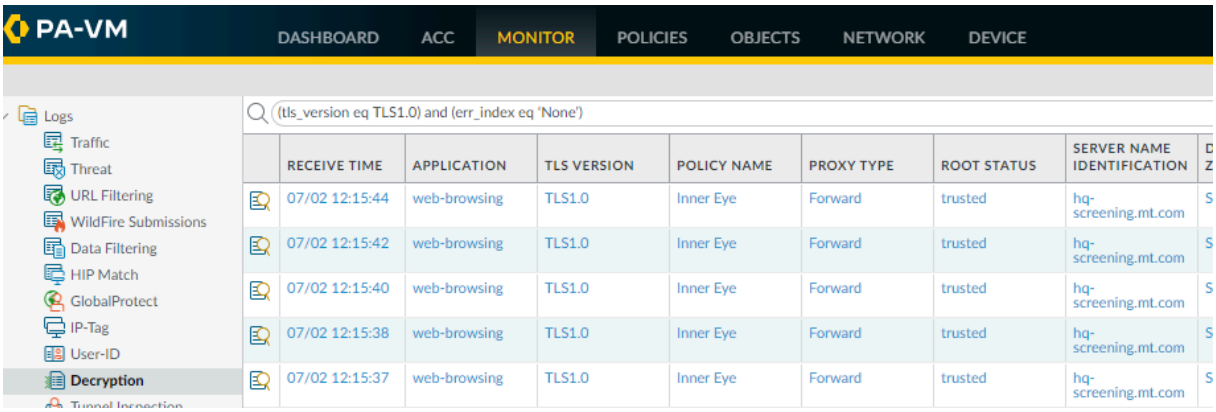



방화벽이 웹 브라우징 트래픽으로 식별된 트래픽을 허용하고 있음을 알 수 있습니다. TLSv1.0 웹 브라우징 트래픽이 무엇이고 왜 허용되는지에 대한 통찰력을 얻기 위해 복호화 로그 다음으로 이동합니다.

2. 복호화 로그를 필터링하여 TLSv1.0 활동 세부 정보를 확인합니다.

   쿼리**(tls_version eq TLS1.0)** 및**(err_index eq 'None')**을 사용하여 성공적인 TLSv1.0 복호화 세션을 표시합니다.

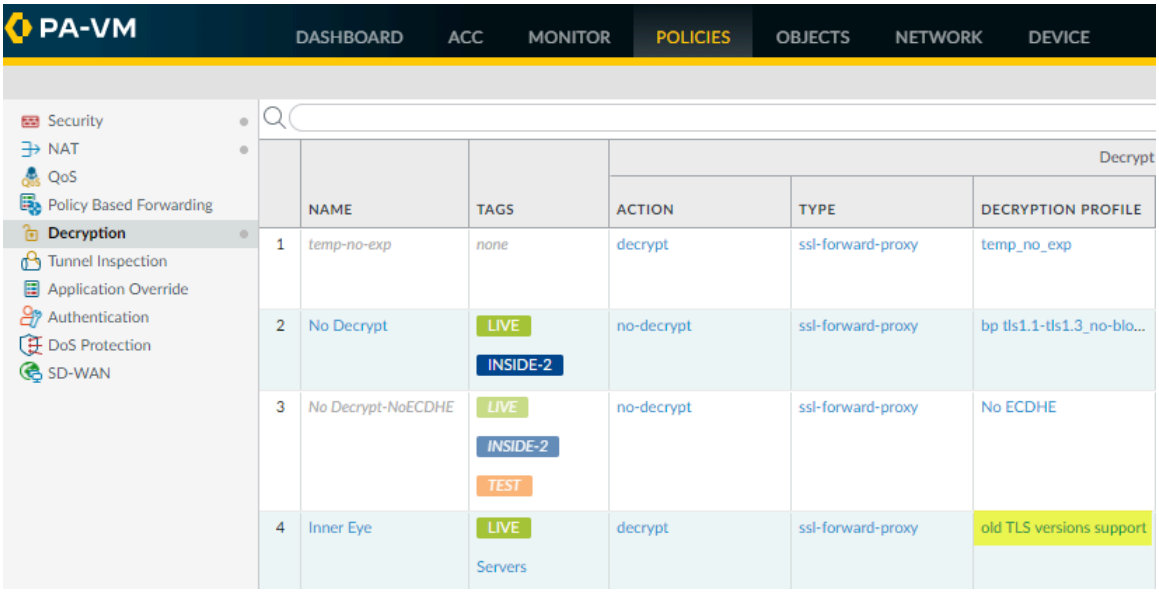
   복호화 로깅 구성일 때 복호화 정책에서 성공적인 ***TLS*** 핸드쉐이크 로깅을 활성화한 경우에만 복호화 로그에 성공적인 ***TLS*** 활동이 표시됩니다. ***TLS*** 핸드쉐이크 성공 로깅이 비활성화된 경우 이 정보를 확인할 수 없습니다.



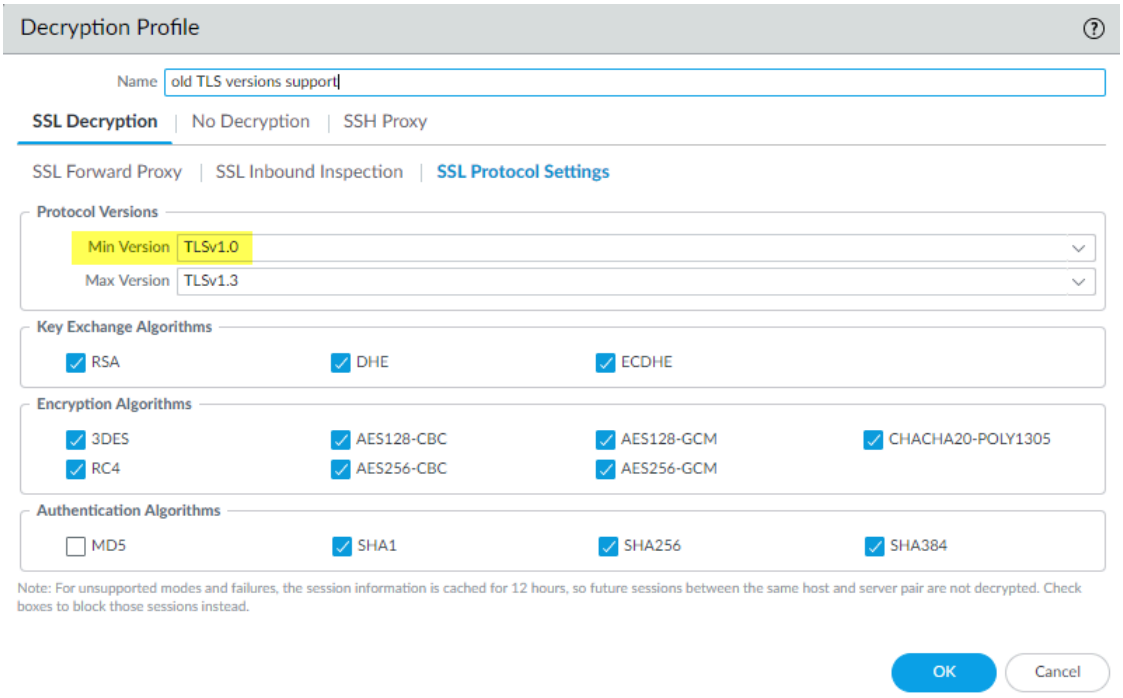

복호화 로그는 트래픽을 제어하는 복호화 정책의 이름이 **Inner Eye**이고 호스트의 이름이 hq-**screening.mt.com**임을 보여줍니다. 이제 우리는 TLSv1.0을 사용하는 사이트를 알고 있으

 ©2023 Palo Alto Networks, Inc.

며 복호화 정책(**Policies** > **Decryption**)을 확인하여 트래픽을 제어하는 복호화 프로파일을 찾고 트래픽이 허용되는 이유를 알 수 있습니다.




정책과 연결된 복호화 프로파일이 이전 **TLS** 버전 지원임을 알 수 있습니다. 프로파일(**Objects** > **Decryption** > **Decryption Profile**)을 확인하고 SSL 프로토콜 설정을 확인하여 프로파일이 허용하는 트래픽을 정확히 알아냅니다.




프로파일은 TLSv1.0 트래픽을 허용합니다. 다음으로 해야 할 일은 사이트에 대한 액세스를 허용할지(비즈니스 목적으로 액세스해야 합니까?) 아니면 차단할지 결정하는 것입니다.

방화벽이 덜 안전한 프로토콜을 사용하는 트래픽을 허용하는 또 다른 일반적인 시나리오는 해당 트래픽이 복호화되지 않은 경우입니다. TLSv1.0 트래픽에 대한 복호화 로그를 필터링할 때


©2023 Palo Alto Networks, Inc.

프록시 유형 열에 **No Decrypt** 값이 포함되어 있으면 No Decryption 정책이 트래픽을 제어하므로 방화벽이 암호를 복호화하거나 검사하지 않습니다. 약한 프로토콜을 허용하지 않으려면 TLSv1.0 트래픽을 차단하도록 복호화 프로파일을 수정하십시오.

복호화 로그를 필터링하여 약한 프로토콜을 사용하는 애플리케이션과 사이트를 찾을 수 있는 방법은 여러 가지가 있습니다. 예를 들면 다음과 같습니다.

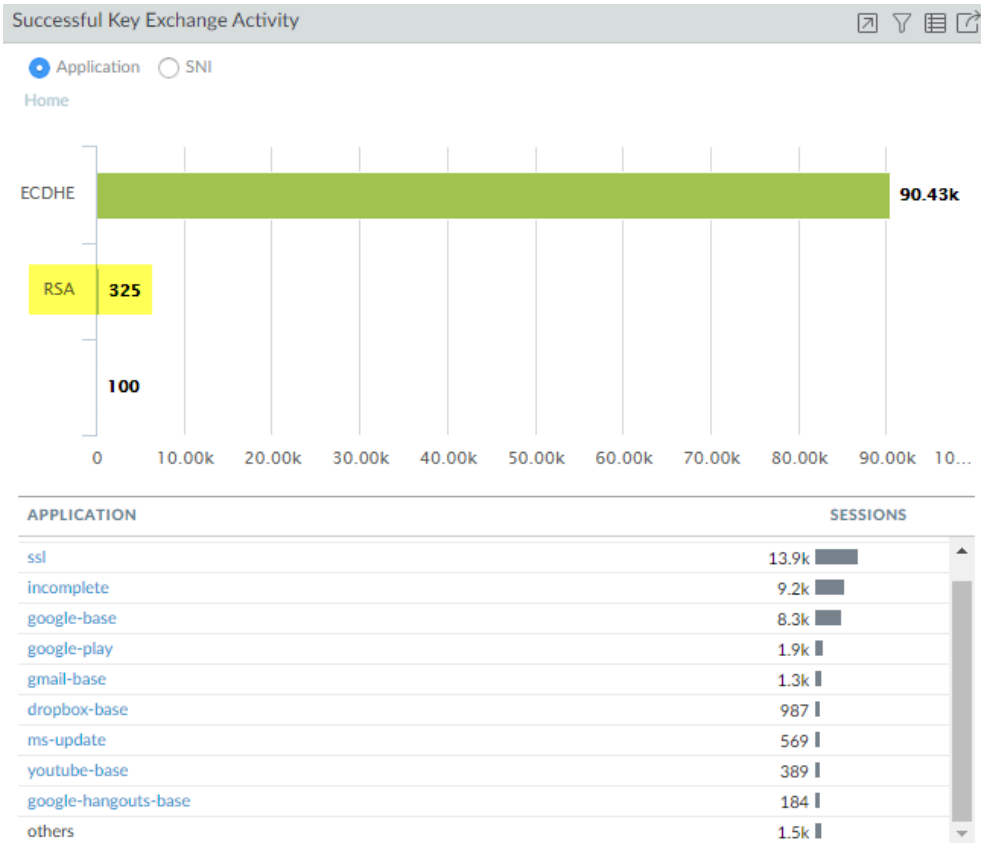
- 성공적인 TLSv1.0 핸드쉐이크에 대해서만 필터링하는 대신 쿼리**(tls_version eq TLS1.0)**를 사용하여 성공한 TLSv1.0 핸드쉐이크와 실패한 TLSv1.0 핸드쉐이크를 모두 필터링합니다.
- 쿼리 **(tls_version eq TLS1.0)** 및**(err_index neq 'None')**을 사용하여 실패한 TLSv1.0 핸드쉐이크만 필터링합니다.
- 쿼리 **(tls_version leq tls1.1)**를 사용하여 보안 수준이 낮은 모든 프로토콜(TLSv1.1 이하)을 필터링합니다.

다른 TLS 버전에 대한 로그를 필터링하려면 **TLS1.0** 또는 **TLS1.1**을 다른 TLS 버전으로 바꾸면 됩니다.

3. 약한 TLS 프로토콜을 사용하는 사이트에 대해 취할 조치를 결정하십시오.
   - 비즈니스 목적으로 사이트에 액세스할 필요가 없는 경우 가장 안전한 조치는 트래픽을 제어하는 복호화 정책 및 복호화 프로파일을 편집하여 사이트에 대한 액세스를 차단하는 것입니다. 복호화 로그 정책 이름 열은 정책 이름을 제공하고 복호화 정책은 첨부된 복호화 프로파일을 표시합니다(옵션 탭).
   - 비즈니스 목적으로 사이트에 액세스해야 하는 경우 해당 사이트(또는 해당 사이트 및 기타 유사한 사이트)에만 적용되는 복호화 정책 및 복호화 프로파일을 생성하고 덜 안전한 프로토콜을 사용하는 다른 모든 트래픽을 차단하는 것이 좋습니다.

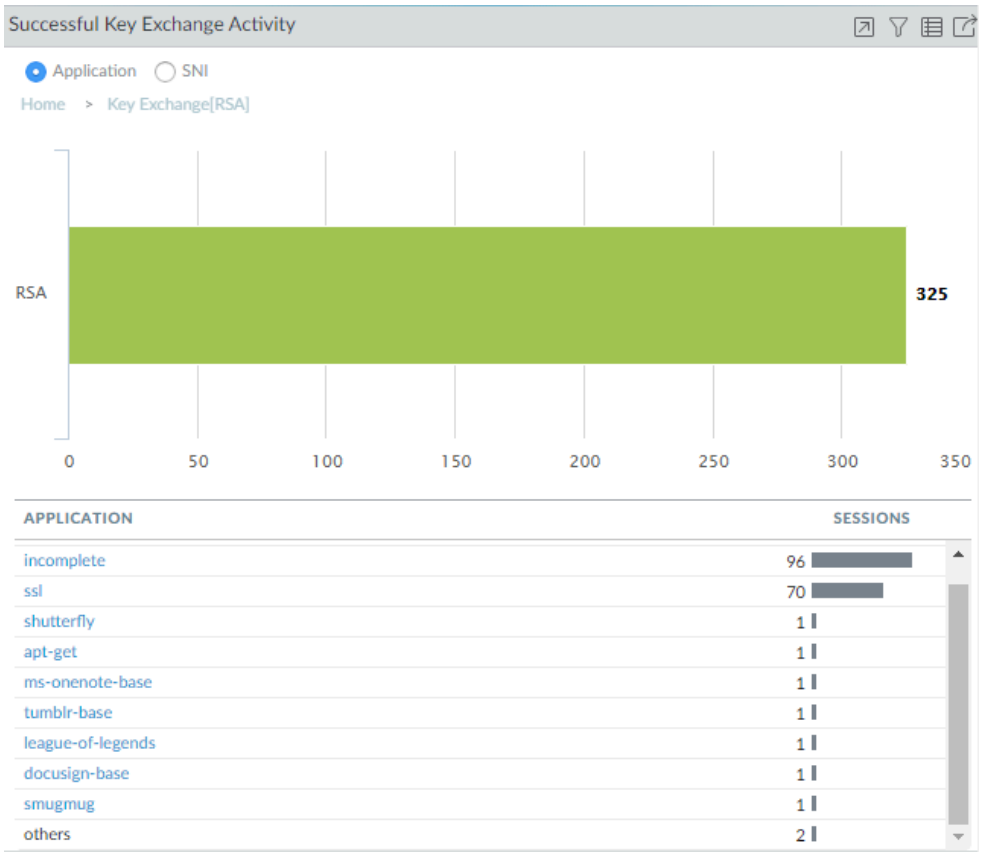
 ©2023 Palo Alto Networks, Inc.

- 키 교환 - 덜 안전한 키 교환 알고리즘을 사용하는 트래픽을 식별합니다.
  1. 먼저 ACC(Application Command Center)에서 방화벽이 허용하는 키 교환 알고리즘(**ACC** > **SSL** 활동 > 성공적인 키 교환 활동) 활동에 대한 전체 보기를 얻을 수 있습니다.



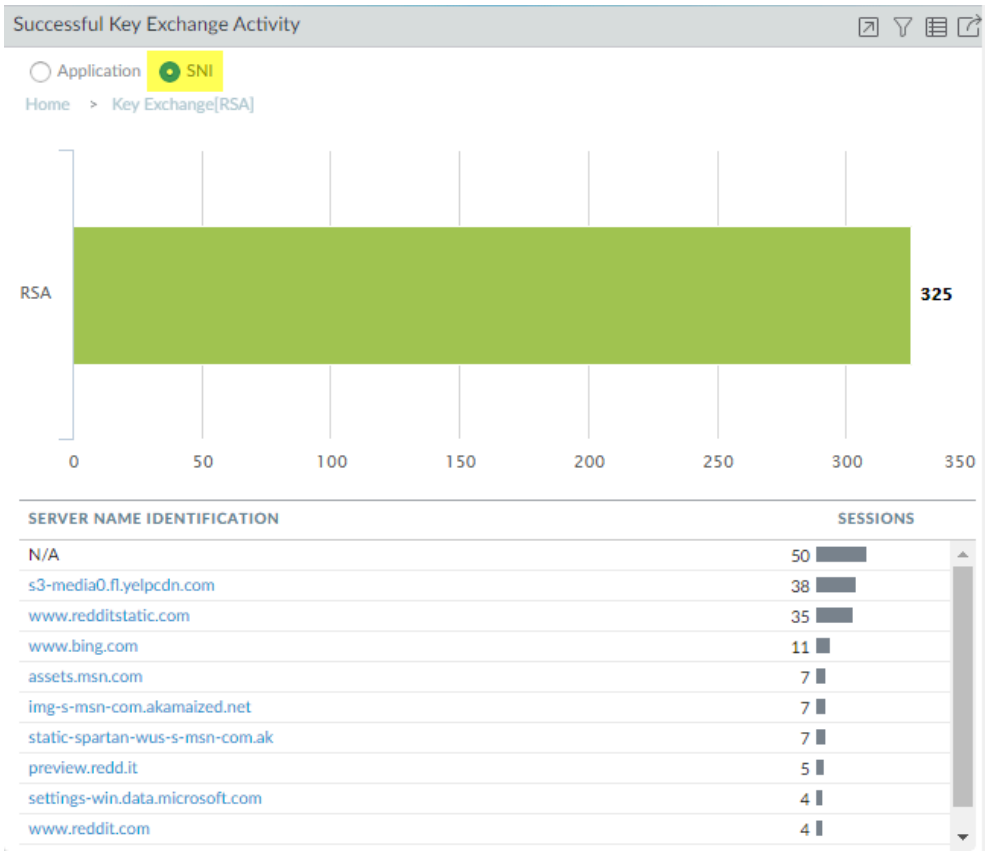

대부분의 키 교환은 보안 ECDHE 키 교환 알고리즘을 사용합니다. 그러나 일부 키 교환 세션은 덜 안전한 RSA 알고리즘을 사용하고 일부는 다른 키 알고리즘을 사용합니다. 예를 들어 RSA 키 교환을 사용하는 트래픽 조사를 시작하려면 숫자 **325**를 클릭하여 데이터를 드릴 다운하십시오.


©2023 Palo Alto Networks, Inc.




드릴 다운은 RSA 키 교환을 사용하는 애플리케이션을 보여줍니다. **SNI** 라디오 버튼을 클릭하여 SNI에 의한 RSA 키 교환을 볼 수도 있습니다.

 ©2023 Palo Alto Networks, Inc.




이 정보를 가지고 로그로 이동하여 RSA 키 교환 사용에 대한 추가 컨텍스트를 얻을 수 있습니다.

2. 암호 해독 로그(모니터 > 로그 > 암호 해독)로 이동하고 쿼리를 사용하여 RSA 키 교환을 사용하는 암호 해독 세션에 대해 필터링합니다. **(tls_keyxchg eq RSA)**:

(tls_keyxchg eq RSA)

| | RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|---|
| | 06/04 09:29:50 | 92884 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:50 | 92887 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:44 | 92998 | ssl | 172.30.200.30 | 74.120.19.22 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:24 | 92882 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:24 | 92880 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:23 | 92874 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:23 | 92873 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/03 22:30:11 | 36522 | vudu | 172.30.100.155 | 208.79.221.210 | TLS1.2 | None | | Big Brother |
| | 06/03 20:08:57 | 16896 | ssl | 172.30.200.30 | 66.117.28.86 | TLS1.2 | None | | No Decrypt |
| | 06/03 20:08:22 | 16947 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |

로그의 정책 이름 열에서 복호화 안 함 복호화 정책이 RSA 키 교환을 사용하는 대부분의 트래픽을 제어하고 방화벽이 트래픽을 복호화하지 않고 검사 없이 허용한다는 것을 유추할 수 있습니다. 트래픽이 복호화되지 않기 때문에 방화벽은 애플리케이션을 식별할 수 없고 **ssl**로 나열합니


©2023 Palo Alto Networks, Inc.

다. RSA 키 교환을 사용하는 트래픽을 허용하지 않으려면 트래픽을 제어하는 복호화 정책에 연결된 복호화 프로파일을 수정하십시오.

쿼리에 추가하여 ACC 또는 첫 번째 복호화 로그 쿼리에서 본 특정 SNI 또는 애플리케이션에 대한 결과를 추가로 필터링할 수 있습니다.

3. 덜 안전한 키 교환 알고리즘을 사용하는 트래픽에 대해 취할 조치를 결정하십시오.

   비즈니스 목적으로 액세스해야 하는 경우가 아니면 보안 수준이 낮은 키 교환 프로토콜을 사용하는 사이트에 대한 액세스를 차단합니다. 이러한 사이트의 경우 해당 사이트(또는 해당 사이트 및 기타 유사한 사이트)에만 적용되는 복호화 정책 및 복호화 프로파일을 생성하고 덜 안전한 키 교환 알고리즘을 사용하는 다른 모든 트래픽을 차단하는 것이 좋습니다.

- 복호화 로그를 사용하여 이전의 덜 안전한 인증 알고리즘을 사용하는 세션을 식별합니다.

  복호화 로그를 필터링하여 이전의 덜 안전한 인증 알고리즘을 식별합니다.

  예를 들어, SHA1 알고리즘을 사용하는 모든 세션을 식별하려면 쿼리 **(tls_auth eq SHA)**를 사용합니다.

  (tls_auth eq SHA)

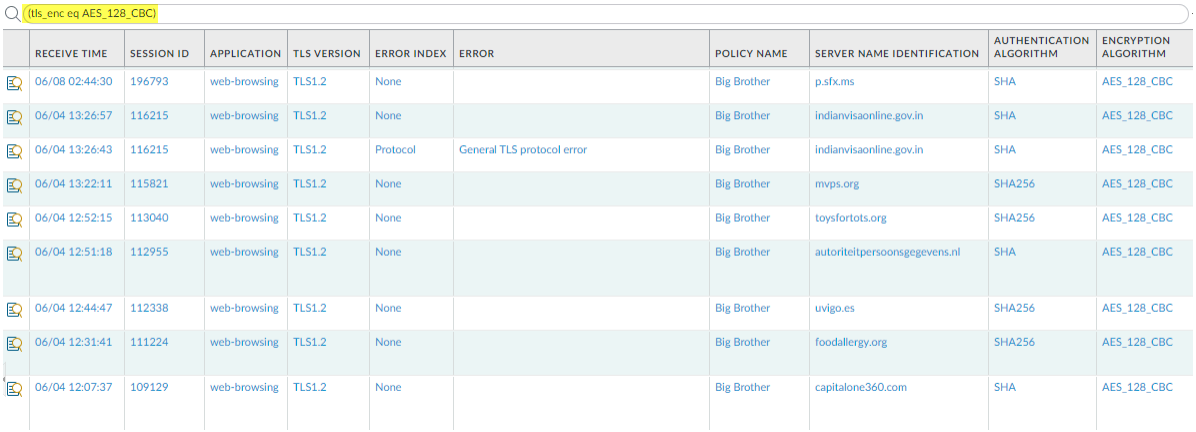
| | RECEIVE TIME | SESSION ID | APPLICATION | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION | AUTHENTICATION ALGORITHM |
|---|---|---|---|---|---|---|---|---|---|
| | 06/08 23:12:02 | 213635 | ssl | TLS1.2 | None | | No Decrypt | | SHA |
| | 06/08 11:16:02 | 203438 | incomplete | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| | 06/08 11:16:02 | 203439 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| | 06/08 11:15:01 | 203437 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| | 06/08 02:45:32 | 196795 | incomplete | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| | 06/08 02:44:30 | 196794 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| | 06/08 02:44:30 | 196793 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| | 06/04 13:38:36 | 117329 | web-browsing | TLS1.2 | None | | Big Brother | inegi.org.mx | SHA |
| | 06/04 13:35:01 | 116980 | web-browsing | TLS1.2 | None | | Big Brother | rupress.org | SHA |

  쿼리에 추가하여 결과를 자세히 드릴 다운할 수 있습니다. 예를 들어 특정 SNI, 키 교환 버전(RSA 키 교환도 사용하는 SHA1 세션에 대한 필터링 등), TLS 버전 또는 복호화 로그 열에 있는 기타 메트릭을 추가할 수 있습니다.


©2023 Palo Alto Networks, Inc.

- 복호화 로그를 사용하여 특정 암호화 알고리즘을 사용하는 세션을 식별합니다.

  예를 들어, AES-128-CBC 암호화 알고리즘을 사용하는 모든 세션을 식별하려면 쿼리 **(tls_enc eq AES_128_CBC)**를 사용하십시오.




| | RECEIVE TIME | SESSION ID | APPLICATION | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION | AUTHENTICATION ALGORITHM | ENCRYPTION ALGORITHM |
|---|---|---|---|---|---|---|---|---|---|---|
| | 06/08 02:44:30 | 196793 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA | AES_128_CBC |
| | 06/04 13:26:57 | 116215 | web-browsing | TLS1.2 | None | | Big Brother | indianvisaonline.gov.in | SHA | AES_128_CBC |
| | 06/04 13:26:43 | 116215 | web-browsing | TLS1.2 | Protocol | General TLS protocol error | Big Brother | indianvisaonline.gov.in | SHA | AES_128_CBC |
| | 06/04 13:22:11 | 115821 | web-browsing | TLS1.2 | None | | Big Brother | mvps.org | SHA256 | AES_128_CBC |
| | 06/04 12:52:15 | 113040 | web-browsing | TLS1.2 | None | | Big Brother | toysfortots.org | SHA256 | AES_128_CBC |
| | 06/04 12:51:18 | 112955 | web-browsing | TLS1.2 | None | | Big Brother | autoriteitpersoonsgegevens.nl | SHA | AES_128_CBC |
| | 06/04 12:44:47 | 112338 | web-browsing | TLS1.2 | None | | Big Brother | uvigo.es | SHA256 | AES_128_CBC |
| | 06/04 12:31:41 | 111224 | web-browsing | TLS1.2 | None | | Big Brother | foodallergy.org | SHA256 | AES_128_CBC |
| | 06/04 12:07:37 | 109129 | web-browsing | TLS1.2 | None | | Big Brother | capitalone360.com | SHA | AES_128_CBC |

  쿼리에 추가하여 결과를 자세히 드릴 다운할 수 있습니다.

  다른 이전 암호화 알고리즘을 찾기 위한 쿼리의 예로는 **(tls_enc eq DES_CBC)**, **(tls_enc eq 3DES_EDE_CBC)** 및 **(tls_enc eq DES40_CBC)**가 있습니다.

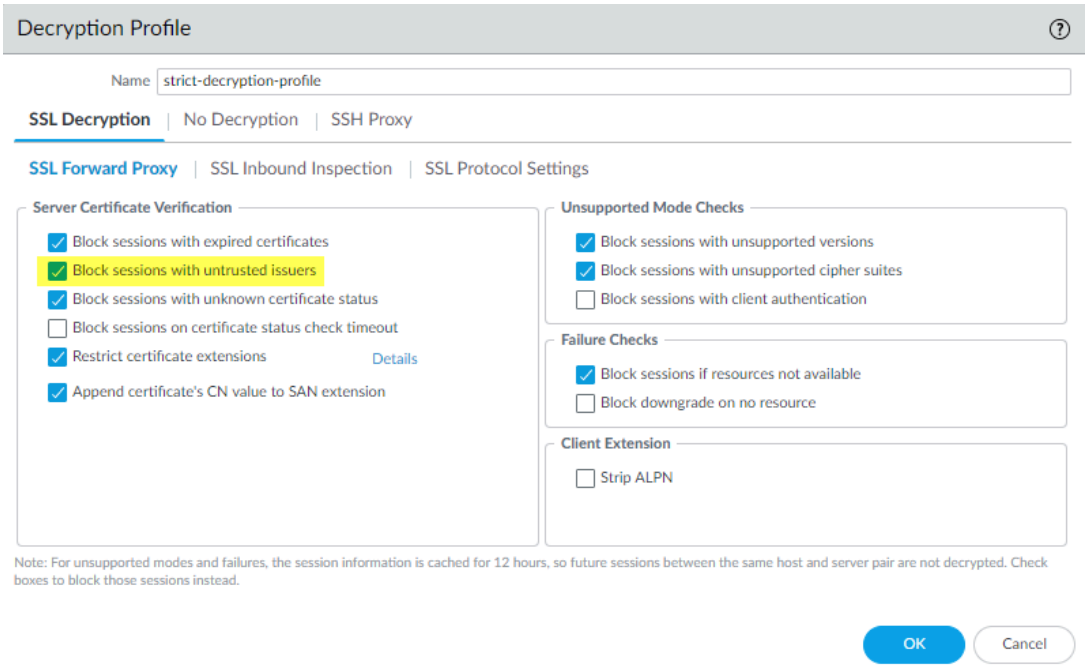
- 이 방법론과 로그 필터 빌더를 사용하여 협상된 ECC 곡선 및 복호화 로그에서 찾은 기타 정보를 조사하기 위한 쿼리를 생성합니다.

## 신뢰할 수 없는 CA 인증서 식별

신뢰할 수 없는 CA 인증서 및 신뢰할 수 없는 루트 CA에서 자체 서명한 인증서가 있는 사이트에 대한 액세스를 차단하는 것은 가장 좋은 방법입니다. 신뢰할 수 없는 CA가 있는 사이트는 중간자 공격, 재전송 공격 또는 기타 악의적인 활동을 나타낼 수 있기 때문입니다.

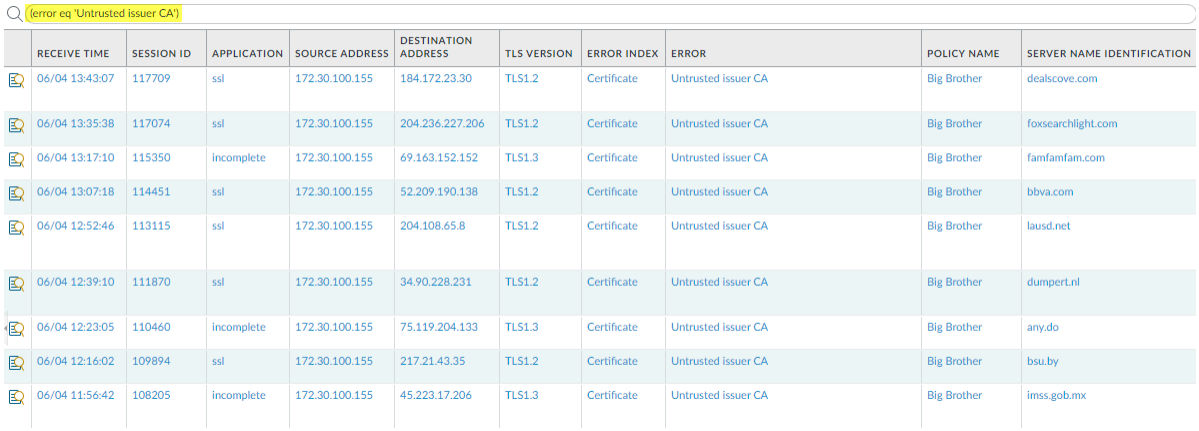

©2023 Palo Alto Networks, Inc.

**STEP 1 |** Forward Proxy Decryption 프로파일(개체 > **Decryption** > **Decryption Profiles**)에서 신뢰할 수 없는 발급자가 있는 세션 차단을 확인합니다. 신뢰할 수 없는 CA가 있는 사이트를 차단합니다.




복호화 프로파일에서 신뢰할 수 없는 발급자가 있는 세션을 차단하면 복호화 로그(**Monitor** > **Logs** > **Decryption**)에 오류가 기록됩니다.

**STEP 2 |** 쿼리를 사용하여 해지된 인증서로 인해 실패한 세션을 식별하도록 로그를 필터링합니다(오류 **eq '신뢰할 수 없는 발급자 CA'**).




**STEP 3 |** (선택사항) Qualys SSL Labs 사이트에서 인증서 만료일을 다시 확인하십시오.

호스트 이름 필드에 서버의 호스트 이름(복호화 로그의 서버 이름 식별 열)을 입력하고 제출하여 호스트에 대한 인증서 정보를 봅니다.

## 만료된 인증서 문제 해결

포워드 프록시 복호화 프로파일 또는 비복호화 프로파일에서 복호화 모범 사례 및 만료된 인증서가 있는 세션 차단을 따르는 경우 서버가 만료된 인증서를 제시하면 방화벽이 세션을 차단합니다. 그러나 업무상

 ©2023 Palo Alto Networks, Inc.

의 이유로 액세스해야 하는 사이트에서 인증서 만료를 허용하는 경우 해당 사이트에 대한 연결이 차단될 수 있으며 이유는 확인 불가할 수 있습니다.

복호화 로그를 사용하여 만료된 인증서를 확인하고 곧 만료될 인증서를 확인하여 상황을 인식하고 적절한 조치를 취할 수 있습니다.

**STEP 1 |** 쿼리 **(오류 eq '만료된 서버 인증서')**를 사용하여 만료된 인증서에 대한 암호 해독 로그를 필터링합니다.


(error eq 'Expired server certificate')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | SERVER NAME IDENTIFICATION | POLICY NAME |
|---|---|---|---|---|---|---|---|---|---|
| 06/04 16:19:49 | 121352 | incomplete | 172.30.100.10 | 34.225.62.221 | TLS1.3 | Certificate | Expired server certificate | www.stanford.edu | Big Brother |
| 06/04 13:43:26 | 117747 | incomplete | 172.30.100.155 | 104.197.149.89 | TLS1.3 | Certificate | Expired server certificate | phone.com | Big Brother |
| 06/04 13:41:03 | 117572 | incomplete | 172.30.100.155 | 208.117.9.16 | TLS1.3 | Certificate | Expired server certificate | netcarshow.com | Big Brother |
| 06/04 13:38:51 | 117379 | ssl | 172.30.100.155 | 69.172.200.184 | TLS1.2 | Certificate | Expired server certificate | royal.gov.uk | Big Brother |
| 06/04 13:36:27 | 117150 | ssl | 172.30.100.155 | 107.21.104.61 | TLS1.2 | Certificate | Expired server certificate | www.uthscsa.edu | Big Brother |
| 06/04 13:34:53 | 117004 | incomplete | 172.30.100.155 | 66.115.56.251 | TLS1.3 | Certificate | Expired server certificate | gunsamerica.com | Big Brother |
| 06/04 13:33:17 | 116853 | incomplete | 172.30.100.155 | 34.107.140.234 | TLS1.3 | Certificate | Expired server certificate | skiplagged.com | Big Brother |
| 06/04 13:32:45 | 116798 | ssl | 172.30.100.155 | 104.236.4.58 | TLS1.2 | Certificate | Expired server certificate | uploading.com | Big Brother |
| 06/04 13:31:28 | 116655 | incomplete | 172.30.100.155 | 35.186.201.59 | TLS1.3 | Certificate | Expired server certificate | shared.com | Big Brother |
| 06/04 13:29:32 | 116507 | ssl | 172.30.100.155 | 147.139.136.53 | TLS1.2 | Certificate | Expired server certificate | beautynesia.id | Big Brother |
| 06/04 13:28:56 | 116426 | incomplete | 172.30.100.155 | 45.55.105.190 | TLS1.3 | Certificate | Expired server certificate | designbundles.net | Big Brother |

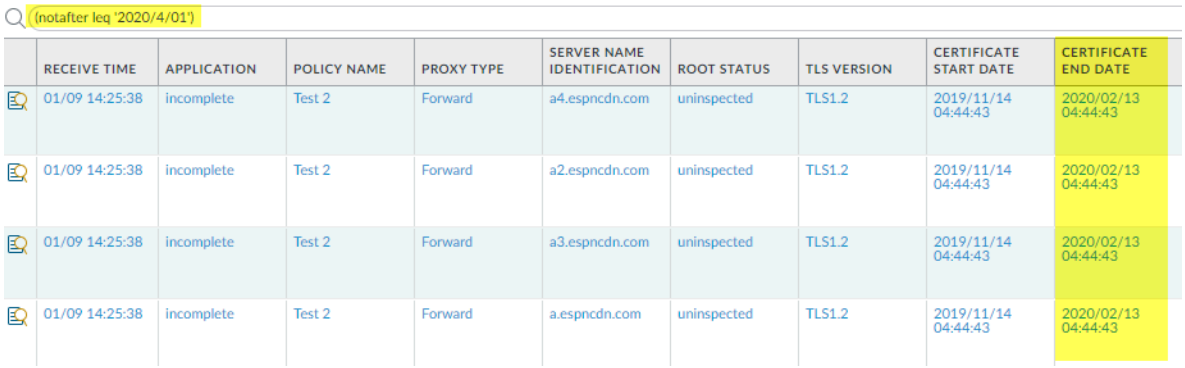
이 쿼리는 **만료된 서버 인증서** 오류를 생성하는 서버를 식별합니다. 방화벽은 만료된 인증서로 인해 이러한 서버에 대한 액세스를 차단합니다.

**STEP 2 |** (선택사항) Qualys SSL Labs 사이트에서 인증서 만료일을 다시 확인하십시오.

호스트 이름 필드에 서버의 호스트 이름(복호화 로그의 서버 이름 식별 열)을 입력하고 제출하여 호스트에 대한 인증서 정보를 봅니다.

**STEP 3 |** 다가오는 인증서 종료 날짜를 식별하는 쿼리를 사용하여 곧 만료되는 인증서의 암호 해독 로그(모니터 > 로그 > 암호 해독)를 필터링합니다.

예를 들어, 오늘 날짜가 2020년 2월 1일이고 사이트에서 인증서를 업데이트하지 않을 경우를 대비하여 평가하고 준비하는 데 2개월의 시간을 부여하려는 경우 암호 해독 로그에서 2020년 4월 1일 또는 그 이전에 만료되는 인증서를 쿼리합니다(**notafter leq '2020/4/01'**):


(notafter leq '2020/4/01')

| RECEIVE TIME | APPLICATION | POLICY NAME | PROXY TYPE | SERVER NAME IDENTIFICATION | ROOT STATUS | TLS VERSION | CERTIFICATE START DATE | CERTIFICATE END DATE |
|---|---|---|---|---|---|---|---|---|
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a4.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a2.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a3.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |

인증서 종료 날짜 열에는 인증서가 만료되는 실제 날짜가 표시됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 만료된 인증서가 있는 사이트에 대해 수행할 작업을 결정합니다.

- 비즈니스 목적으로 사이트에 액세스할 필요가 없는 경우 가장 안전한 조치는 사이트에 대한 액세스를 계속 차단하는 것입니다.
- 비즈니스 목적으로 사이트에 액세스해야 하는 경우 다음 조치 중 하나를 수행하십시오.
  - 만료된 인증서가 있는 사이트 관리자에게 연락하여 인증서를 업데이트하거나 갱신해야 한다고 알립니다.
  - 비즈니스 목적에 필요한 만료된 인증서가 있는 사이트에만 적용되는 복호화 정책과 만료된 인증서가 있는 사이트를 허용하는 복호화 프로파일을 생성합니다. 비즈니스 목적으로 필요하지 않은 사이트에는 정책을 적용하지 마십시오. 사이트에서 인증서를 업데이트하면 정책에서 제거하십시오.

## 해지된 인증서 문제 해결

해지된 인증서는 더 이상 유효하지 않습니다. 사이트에 보안 문제가 있고 인증서가 신뢰할 수 없을 수 있지만 인증서가 해지될 수 있는 악성의 이유도 있습니다.



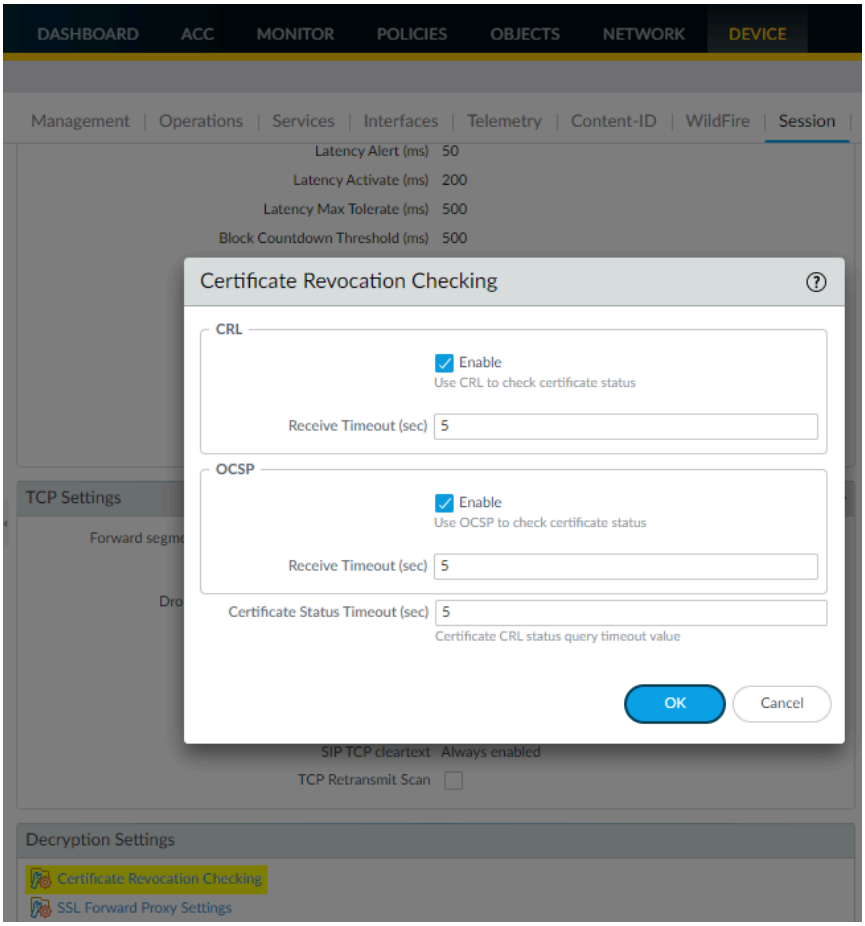
해지된 인증서를 신뢰하지 마십시오. 인증서 해지 검사를 활성화하여 해지된 인증서가 있는 사이트에 대한 액세스를 거부합니다.

해지된 인증서가 있는 세션을 삭제하고 해지된 인증서 문제를 해결하려면 인증서 해지 검사를 사용하도록 설정해야 합니다. 인증서 해지 검사를 사용하도록 설정하지 않으면 방화벽이 해지된 인증서를 확인하지 않으며 사이트에 해지된 인증서가 있는지의 여부를 알 수 없습니다.


©2023 Palo Alto Networks, Inc.

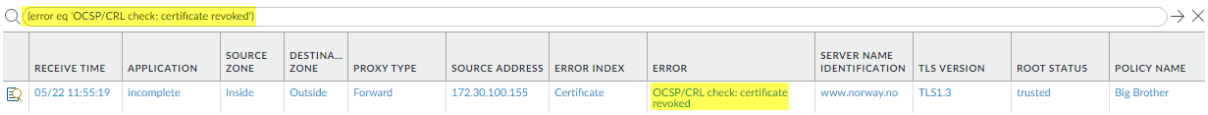
**STEP 1 |** 인증서 해지 검사를 사용하도록 설정하지 않은 경우 인증서 해지 검사를 사용하도록 설정합니다.

1. 디바이스 > 설정 > 세션 > 암호 해독 설정으로 이동합니다.
2. OCSP 및 CRL 인증서 검사를 모두 사용하도록 설정합니다.




포워드 프록시 복호화 프로파일에서 인증서 상태 확인 타임아웃에서 세션 차단이 5초가 충분하지 않아 타임아웃로 인해 너무 많은 세션이 차단될 수 있다고 우려되는 경우 수신 타임아웃**(**초**)**을 더 긴 시간으로 설정합니다.

**STEP 2 |** 암호 해독 로그(**Monitor** > **Logs** > **Decryption**)를 필터링하여 쿼리 **(error eq 'OCSP/ CRL 확인: 인증서가 취소되었습니다')**.




**STEP 3 |** (선택사항) Qualys SSL Labs 사이트에서 인증서 만료일을 다시 확인하십시오.

호스트 이름 필드에 서버의 호스트 이름(복호화 로그의 서버 이름 식별 열)을 입력하고 제출하여 호스트에 대한 인증서 정보를 봅니다.

## 고정된 인증서 문제 해결

인증서 고정은 클라이언트 애플리케이션이 알려진 복사본에 대해 서버 인증서의 유효성을 검사하여 인증서가 실제로 서버에서 오는지 확인하도록 합니다. 고정된 인증서의 목적은 클라이언트와 서버 사이의 디

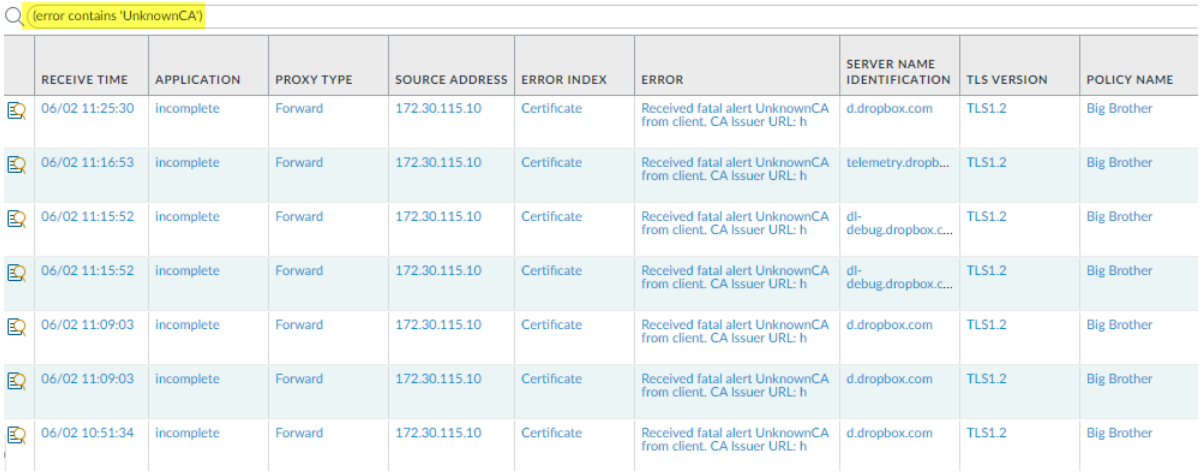

©2023 Palo Alto Networks, Inc.

바이스가 서버 인증서를 다른 인증서로 교체하는 MITM(Man-in-the-Middle) 공격으로부터 보호하는 것입니다.

이렇게 하면 악의적인 행위자가 연결을 가로채고 조작하는 것을 방지할 수 있지만 방화벽이 클라이언트에 제공할 서버 인증서 대신 가장 인증서를 생성하기 때문에 포워드 프록시 복호화도 방지합니다. 클라이언트와 서버를 직접 연결하는 하나의 세션 대신 포워드 프록시는 클라이언트와 방화벽 사이에 하나, 방화벽과 서버 사이에 세션 두 개를 생성합니다. 이렇게 하면 방화벽이 트래픽을 복호화하고 검사할 수 있도록 클라이언트와 신뢰 관계가 설정됩니다.

그러나 인증서가 고정되면 클라이언트가 방화벽의 가장 인증서를 수락하지 않기 때문에 방화벽이 트래픽을 복호화할 수 없습니다. 클라이언트는 애플리케이션에 고정된 인증서만 수락합니다.

**STEP 1 |** 암호 해독 로그(**Monitor** > **Logs** > **Decryption**)를 필터링하여 쿼리 **(오류에 'UnknownCA' 포함)**를 사용하여 고정된 인증서를 찾습니다. .




애플리케이션은 서버의 인증서 확인에 실패하면 TLS 오류 코드(경고)를 생성합니다. 애플리케이션마다 다른 오류 코드를 사용하여 고정된 인증서를 나타낼 수 있습니다. 고정된 인증서에 대한 가장 일반적인 오류 표시기는 UnknownCA 및 BadCertificate입니다. **(오류에 'UnknownCA' 포함)** 쿼리를 실행한 후 쿼리**(오류에 'BadCertificate' 포함)**를 실행하여 고정된 인증서 오류를 더 잡아냅니다.

*Wireshark* 또는 다른 패킷 분석기를 사용하여 오류를 다시 확인할 수 있습니다. 고정된 인증서 문제인지 확인하기 위해 ***TLS*** 핸드쉐이크 직후 연결을 끊는 클라이언트를 찾습니다.

**STEP 2 |** 고정된 인증서에 대해 수행할 작업을 결정합니다.

업무상 액세스가 필요하지 않은 경우 방화벽이 액세스를 계속 차단하도록 할 수 있습니다. 액세스가 필요한 경우 SSL 복호화 제외 목록(디바이스 > 인증서 관리 > **SSL** 복호화 제외)에 추가하여 기술적인 이유로 복호화에서 서버 제외할 수 있습니다.

방화벽은 SSL 복호화 제외 목록에 있는 사이트에 대한 복호화를 우회합니다. 방화벽은 트래픽을 검사할 수 없지만 트래픽은 허용됩니다.


©2023 Palo Alto Networks, Inc.

# 복호화 기능을 위한 무료 라이선스 활성화

SSH 트래픽 및 SSL트래픽(SSL인터넷 트래픽 또는 내부 서버로의SSL 트래픽)복호화에는 라이선스가 필요하지 않습니다. 그러나 복호화 미러링을 활성화하려면 무료 라이선스를 활성화해야 합니다. 무료 라이선스 요구 사항은 승인된 직원이 의도적으로 관련 라이선스를 활성화한 후에만 이 기능을 사용할 수 있도록 합니다.

> ***PAN-OS 10.1***에서는 복호화 브로커 기능과 무료 라이선스가 네트워크 패킷 브로커(네트워킹 관리자 가이드 참조)로 대체되어 브로커의 기능을 해독되지 않은 ***TLS*** 트래픽 및 비 ***TLS*** 트래픽으로 확장합니다. 네트워크 패킷 브로커 라이선스는 고객 지원 포털에서 무료로 다운로드하고 설치할 수 있습니다.

Palo Alto Networks 고객 지원 포털에서 다음 단계를 수행하여 복호화 미러링 기능 라이선스를 활성화합니다.

**STEP 1 |** 고객 지원 포털에 로그인합니다.

**STEP 2 |** 왼쪽 탐색 창에서 자산 > 디바이스를 선택합니다.

**STEP 3 |** 복호화 포트 미러링을 사용하도록 설정하려는 디바이스를 찾아 작업(연필 아이콘)을 선택합니다.

**STEP 4 |** 라이선스 활성화에서 기능 라이선스 활성화를 선택합니다.

**STEP 5 |** 무료 라이선스를 활성화하려는 기능을 선택합니다. 암호 해독 포트 미러.

**STEP 6 |** 동의 및 제출.

**STEP 7 |** 방화벽에 복호화 미러링 라이선스를 설치합니다.

1. 디바이스 > 라이선스를 선택합니다.
2. 라이선스 서버에서 라이선스 키 검색을 클릭합니다.
3. 이제 방화벽에서 복호화 포트 미러 라이선스가 활성화되어 있는지 확인합니다.
4. 방화벽을 다시 시작합니다(디바이스 > 설정 > 작업). 방화벽이 다시 로드될 때까지 암호 해독 포트 미러링을 구성에 사용할 수 없습니다.


©2023 Palo Alto Networks, Inc.

# URL 필터링

Palo Alto Networks URL 필터링을 사용하면 사용자가 액세스할 수 있는 사이트를 모니터링 및 제어하고, 사용자가 유효한 회사 자격 증명을 제출할 수 있는 사이트를 제어하여 피싱 공격을 방지하고, Google 및 Bing과 같은 검색 엔진에 대한 안전한 검색을 시행할 수 있습니다.


- Palo Alto Networks URL 필터링 솔루션 정보
- 고급 URL 필터링 작동 방식
- 로컬 인라인 분류
- URL 필터링 사용 사례
- URL 카테고리
- URL 필터링 배포 계획
- URL 필터링 모범 사례
- 고급 URL 필터링 구독 활성화
- URL 필터링 구성 테스트
- URL 필터링 구성
- 인라인 분류 설정
- 웹 활동 모니터링
- 사용자가 방문한 페이지만 기록
- 사용자 지정 URL 카테고리 생성
- URL 카테고리 예외
- URL 필터링 프로파일에서 외부 동적 목록 사용
- 특정 사이트에 대한 암호 액세스 허용
- 자격 증명 피싱 방지
- 세이프서치 시행
- URL 필터링 응답 페이지
- URL 필터링 응답 페이지 사용자 지정
- HTTP 헤더 로깅
- URL 카테고리 변경 요청
- URL 필터링 문제 해결
- PAN-DB 프라이빗 클라우드
- SSL/TLS 핸드셰이크 검사 활성화

# Palo Alto Networks URL 필터링 솔루션 정보

Palo Alto Networks URL 필터링 솔루션인 Advanced URL Filtering은 사용자가 웹에 안전하게 액세스할 수 있도록 하는 동시에 사용자가 상호 작용하고 온라인 콘텐츠에 액세스하는 방법을 정확하게 정의하는 세분화된 정책 제어를 제공하여 웹 기반 위협으로부터 네트워크를 보호하는 구독 서비스입니다. 고급 URL 필터링 구독은 URL 분류 데이터베이스를 제공하여 레거시 URL 필터링 구독이 제공하는 모든 기능을 제공하는 동시에 인라인 ML 기반 웹 보안 엔진을 사용하여 회피하고 알려지지 않은 웹 위협을 방지하는 전체 웹 콘텐츠 검사의 추가 이점을 제공합니다. .



레거시 ***URL*** 필터링 구독 보유자는 라이선스 기간이 끝날 때까지 ***URL*** 필터링 배포를 계속 사용할 수 있습니다.

URL 카테고리, 사용자 및 그룹을 기준으로 사이트에 대한 액세스를 제한하는 정책 규칙을 생성할 수 있습니다. (보다 URL 필터링 사용 사례다양한 방법으로 고급 URL 필터링 구독을 활용하여 조직의 웹 보안 요구 사항을 충족할 수 있습니다.)

고급 URL 필터링이 활성화된 경우 URL 요청은 다음과 같습니다.

- 분류된 수백만 개의 웹사이트가 포함된 PAN-DB URL 데이터베이스와 비교합니다. 이러한 URL 카테고리를 URL 필터링 프로파일에서 사용하거나 보안 정책을 적용하는 일치 조건으로 사용할 수 있습니다. 또한 URL 필터링을 사용하여 사용자에게 안전 검색 설정을 적용하고 URL 카테고리에 따라 자격 증명 도용을 방지할 수 있습니다.
- 클라우드 기반 고급 URL 필터링 탐지 모듈을 사용하여 실시간으로 분석하여 현재 URL 필터링 데이터베이스에 존재하지 않는 새롭고 알려지지 않은 위협으로부터 보호합니다.
- 알 수 없는 악성 웹페이지를 실시간으로 차단할 수 있는 방화벽 기반 분석 솔루션인 로컬 인라인 분류를 사용하여 피싱 및 악성 자바스크립트를 검사합니다.

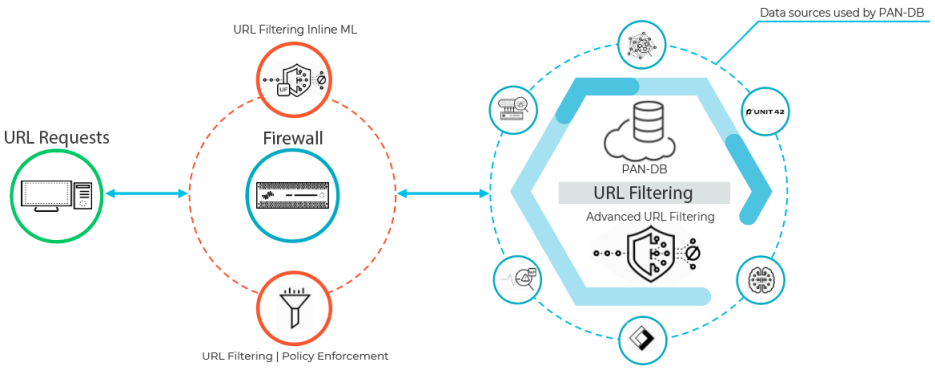
기업의 네트워크 보안 요구 사항이 방화벽이 인터넷에 직접 액세스하는 것을 금지하는 경우 Palo Alto Networks는 ***PAN-DB Private Cloud***와 함께 오프라인 URL 필터링 솔루션을 제공합니다. 이를 통해 네트워크 내에서 PAN-DB 서버로 작동하는 하나 이상의 M-600 어플라이언스에 PAN-DB 사설 클라우드를 배포할 수 있습니다. 그러나 고급 URL 필터링 솔루션에 있는 클라우드 기반 URL 분석 기능은 지원하지 않습니다.


©2023 Palo Alto Networks, Inc.

# 고급 URL 필터링 작동 방식

고급 URL 필터링은 사이트 콘텐츠, 기능 및 안전을 기반으로 웹 사이트를 분류합니다. URL에는 위험 카테고리(높음, 보통, 낮음)를 포함하여 최대 4개의 URL 카테고리가 포함될 수 있으며, 이는 사이트에서 사용자를 위협에 노출할 가능성을 나타냅니다. 고급 URL 필터링 URL 데이터베이스인 PAN-DB는 사이트를 분류하므로 고급 URL 필터링이 활성화된 방화벽은 이러한 지식을 활용하여 조직의 보안 정책을 적용할 수 있습니다. PAN-DB 데이터베이스가 제공하는 보호 기능 외에도 고급 URL 필터링은 기계 학습을 사용하여 실시간 분석을 제공하여 새롭고 알려지지 않은 위협으로부터 방어합니다. 이렇게 하면 URL 필터링 데이터베이스가 콘텐츠를 분석 및 추가하기 전에 업데이트되거나 도입된 악성 URL에 대한 보호 기능을 제공하므로 공격자는 정확한 공격 캠페인을 시작할 수 있는 기간을 공개하게 됩니다. Advanced URL 필터링은 요청별로 실시간 URL 분석을 제공함으로써 데이터베이스 솔루션에 내재된 커버리지 갭을 보완합니다. Advanced URL 필터링에 사용되는 ML 기반 모델은 다양한 악성 URL, 피싱 웹 페이지 및 C2를 탐지하기 위해 학습되고 지속적으로 업데이트됩니다.

특정 지능형 위협의 존재를 나타내는 웹사이트는 고급 URL 필터링에서 사용하는 ML 모델을 보완하는 탐지기와 분석기를 사용하여 클라우드 기반 인라인 딥 러닝 시스템을 통해 추가로 처리됩니다. 딥 러닝 탐지기는 더 큰 데이터 세트를 처리할 수 있으며 다층 신경망을 통해 복잡한 악성 패턴과 행동을 더 잘 식별할 수 있습니다. 의심스러운 웹 요청을 수신하면 고급 URL 필터링이 방화벽으로부터 HTTP 응답 데이터를 수신하면 딥 러닝 탐지기를 통해 데이터를 추가로 분석하고 회피적인 제로 데이 웹 공격에 대한 인라인 보호 기능을 제공합니다. 여기에는 알 수 없는 웹 사이트에서 웹 페이지 콘텐츠를 은밀하게 검색하는 숨겨진 웹 사이트가 포함됩니다. 여기에는 URL 데이터베이스가 설명할 수 없는 악성 콘텐츠, 다단계 공격, CAPTCHA 챌린지 및 이전에는 볼 수 없었던 일회용 URL이 포함될 수 있습니다. 회피 악성 웹 사이트는 지속적으로 유동적이기 때문에 관리자가 업데이트 패키지를 다운로드하지 않고도 Palo Alto Networks의 위협 연구원이 탐지 로직을 개선함에 따라 웹 사이트를 분류하는 데 사용되는 탐지기와 분석기가 자동으로 업데이트되고 배포됩니다.




사용자가 웹 페이지를 요청하면 방화벽은 사이트의 위험 카테고리에 대해 사용자가 추가한 예외 및 PAN-DB를 쿼리합니다. PAN-DB는 유닛 42, 와일드파이어, 수동형 DNS, Palo Alto Networks 텔레메트리 데이터, 사이버 위협 얼라이언스의 데이터 등의 URL 정보를 사용하고 다양한 분석기를 적용하여 카테고리를 결정합니다. URL이 위험하거나 악의적인 특성을 나타내는 경우 웹 페이로드 데이터도 실시간 분석을 위해 클라우드의 고급 URL 필터링에 제출되고 추가 분석 데이터를 생성합니다. 그런 다음 결과 위험 카테고리가 방화벽에 의해 검색되고 정책 구성에 따라 웹 액세스 규칙을 적용하는 데 사용됩니다. 또한 방화벽은 후속 요청을 빠르게 검색할 수 있도록 새 항목에 대한 사이트 분류 정보를 캐시하고 사용자가 최근에 액세스하지 않은 URL을 제거하여 네트워크의 트래픽을 정확하게 반영합니다. 또한 PAN-DB 클라우드 쿼


©2023 Palo Alto Networks, Inc.

리에 내장된 검사를 통해 방화벽이 최신 URL 분류 정보를 수신하는지 확인할 수 있습니다. 인터넷 연결 또는 활성 URL 필터링 라이선스가 없는 경우 PAN-DB를 쿼리하지 않습니다.




방화벽은 1) 사용자 지정 URL 카테고리, 2) 외부 동적 목록(EDL) 및 3) 사전 정의된 URL 카테고리의 항목과 우선 순위에 따라 비교하여 웹사이트의 URL 카테고리를 결정합니다.

데이터플레인에서 머신 러닝을 사용하여 URL을 실시간으로 분석하도록 구성된 방화벽은 피싱 웹사이트 및 JavaScript 악용에 대한 추가 보안 레이어를 제공합니다. 로컬 인라인 분류에 사용되는 ML 모델은 Palo Alto Networks가 악성으로 식별한 특성과 일치하는 URL 기반 위협의 현재 알려지지 않은 변종과 향후 변종을 식별합니다. 위협 환경의 최신 변경 사항을 따라잡기 위해 콘텐츠 릴리스를 통해 로컬 인라인 분류 ML 모델이 추가되거나 업데이트됩니다.

방화벽은 PAN-DB에서 URL을 검사할 때 이전에 양성으로 인증되었지만 현재 악의적인 URL과 같은 중요 업데이트도 찾습니다.

PAN-DB가 사이트를 잘못 분류했다고 생각되는 경우, 브라우저에서 Test A Site 또는 방화벽 로그에서 직접 URL 카테고리 변경 요청을 제출할 수 있습니다.



알고 계셨나요?

기술적으로 방화벽은 *Management Plane(MP)*과 데이터플레인 모두에서 *URL*을 캐시합니다.

- *PAN-OS 9.0* 이상 릴리스는 *PAN-DB* 시드 데이터베이스를 다운로드하지 않습니다. 대신 *URL* 필터링 라이선스가 활성화되면 *URL* 쿼리가 생성될 때 방화벽이 캐시를 채웁니다.
- *Management Plane(MP)*은 더 많은 *URL*을 보유하며 *PAN-DB*와 직접 통신합니다. 방화벽이 캐시에서 *URL*의 카테고리를 찾을 수 없고 *PAN-DB*에서 조회를 수행하면 검색된 카테고리 정보를 *Management Plane(MP)*에 캐시합니다. *Management Plane(MP)*은 해당 정보를 데이터플레인에 포워딩하며 데이터플레인은 데이터를 캐시하고 정책을 적용하는 데 사용합니다.
- 데이터플레인은 더 적은 수의 *URL*을 보유하며 *Management Plane(MP)*으로부터 정보를 수신합니다. 방화벽이 *URL*에 대한 URL 카테고리 예외 목록*(*사용자 지정 *URL* 카테고리 및 외부 동적 목록*)*을 확인한 후 다음 위치는 데이터플레인입니다. 방화벽이 데이터플레인에서 카테고리화된 *URL*을 찾을 수 없는 경우에만 데이터플레인을 확인하고, 카테고리 정보가 없는 경우 *PAN-DB*를 확인합니다.


©2023 Palo Alto Networks, Inc.

# 로컬 인라인 분류

URL 필터링 로컬 인라인 분류(이전의 인라인 ML)를 사용하면 방화벽 데이터 플레인이 웹 페이지에 기계 학습을 적용하여 피싱 변종을 감지할 때 사용자에게 경고하는 동시에 JavaScript 익스플로잇의 악성 변종이 네트워크에 침입하는 것을 방지할 수 있습니다. 로컬 인라인 분류는 일련의 ML 모델을 사용하여 다양한 웹 페이지 세부 정보를 평가하여 악성 콘텐츠를 동적으로 분석하고 탐지합니다. 각 ML 모델은 디코더 필드 및 패턴을 비롯한 파일 세부 정보를 평가하여 악성 콘텐츠를 탐지하여 확률이 높은 분류 및 판결을 공식화한 다음 대규모 웹 보안 정책의 일부로 사용됩니다. 악성으로 분류된 URL은 추가 분석 및 검증을 위해 PAN-DB로 포워딩됩니다. URL 예외를 지정하여 발생할 수 있는 가양성을 제외할 수 있습니다. 이를 통해 특정 보안 요구 사항을 지원하기 위해 프로파일에 대해 보다 세분화된 규칙을 만들 수 있습니다. 위협 환경의 최신 변경 사항을 따라잡기 위해 인라인 ML 모델은 정기적으로 업데이트되고 콘텐츠 릴리스를 통해 추가됩니다. 인라인 분류를 구성하려면 활성 고급 URL 필터링 구독이 필요합니다.

인라인 ML 기반 보호를 사용하여 바이러스 백신 프로파일 구성의 일부로 악성 PE(휴대용 실행 파일), ELF 및 MS Office 파일, PowerShell 및 셸 스크립트를 실시간으로 검색할 수도 있습니다. 자세한 내용은 WildFire Inline ML을(를) 참조하십시오.

로컬 인라인 분류는 ***VM-50*** 또는 ***VM50L*** 가상 어플라이언스에서 지원되지 않습니다.


©2023 Palo Alto Networks, Inc.

# URL 필터링 사용 사례

특정 사이트를 차단하고 허용하는 것 이상으로 웹 페이지 액세스를 적용하는 방법에는 여러 가지가 있습니다. 예를 들어 URL당 여러 카테고리를 사용하여 사용자가 사이트에 액세스하도록 허용하지만 회사 자격 증명 제출 또는 파일 다운로드와 같은 특정 기능은 차단할 수 있습니다. 또한 URL 카테고리를 사용하여 인증, 복호화, QoS 및 보안과 같은 다양한 유형의 정책을 시행할 수 있습니다.

URL 필터링을 배포할 수 있는 다양한 방법에 대해 자세히 알아보세요.

### **URL** 카테고리를 기반으로 웹 액세스 제어

URL 카테고리에 대한 작업을 지정하는 URL 필터링 프로파일을 생성하고 프로파일을 정책 규칙에 연결할 수 있습니다. 방화벽은 프로파일의 설정을 기반으로 트래픽에 대한 정책을 시행합니다. 예를 들어 모든 게임 웹사이트를 차단하려면 URL 필터링 프로파일에서 URL 카테고리 게임에 대한 차단 작업을 설정하고 웹 액세스를 허용하는 보안 정책 규칙에 연결할 수 있습니다.

### 다중 카테고리 **URL** 필터링

모든 URL에는 사이트가 위협에 노출될 가능성을 나타내는 위험 카테고리를 포함하여 최대 4개의 카테고리가 있을 수 있습니다. 보다 세분화된 URL 분류는 웹 액세스에 대한 기본 "차단 또는 허용" 접근 방식 이상으로 이동할 수 있음을 의미합니다. 대신 사용자가 비즈니스에 필요하지만 사이버 공격의 일부로 사용될 가능성이 높은 온라인 콘텐츠와 상호 작용하는 방식을 제어할 수 있습니다.

예를 들어, 특정 URL 카테고리가 조직에 위험하다고 생각할 수 있지만 클라우드 스토리지 서비스 또는 블로그와 같은 귀중한 리소스 또는 서비스를 제공하기 때문에 완전히 차단하는 것을 망설일 수 있습니다. 이제 트래픽을 복호화 및 검사하고 콘텐츠에 대한 읽기 전용 액세스를 적용하여 네트워크를 보호하는 동안 사용자가 이러한 유형의 URL 카테고리에 속하는 사이트를 방문하도록 허용할 수 있습니다.

엄격하게 제어하려는 URL 카테고리의 경우 URL 필터링을 구성하는 단계의 일부로 경고하도록 URL 필터링 프로파일 작업을 설정합니다. 그런 다음 URL 필터링 모범 사례를 계속 따르십시오. URL 카테고리 복호화, 위험한 파일 다운로드 차단, 자격 증명 피싱 방지 켜기.

카테고리 일치를 선택하고 새 카테고리가 구성될 둘 이상의 PAN-DB 카테고리를 지정하여 사용자 정의 URL 카테고리를 정의할 수도 있습니다. 여러 카테고리에서 사용자 지정 카테고리를 만들면 사용자 지정 URL 카테고리 개체에 지정된 모든 카테고리와 일치하는 웹 사이트 또는 페이지에 대한 적용을 대상으로 지정할 수 있습니다.

### **URL** 카테고리에 따라 회사 자격 증명 제출을 차단하거나 허용합니다**.**

방화벽이 사이트에 대한 회사 자격 증명 제출을 감지하도록 설정하여 자격 증명 피싱을 방지한 다음 URL 카테고리를 기반으로 이러한 제출을 제어합니다. 사용자가 악의적이고 신뢰할 수 없는 사이트에 자격 증명을 제출하지 못하도록 차단하고, 알 수 없는 사이트에서 기업 자격 증명을 입력하거나 기업이 아닌 사이트에서 기업 자격 증명을 재사용하지 않도록 사용자에게 경고하고, 사용자가 기업 및 승인된 사이트에 자격 증명을 제출하도록 명시적으로 허용합니다.

### 세이프서치 설정 시행

많은 검색 엔진에는 검색 결과에서 성인 이미지와 비디오를 필터링하는 안전한 검색 설정이 있습니다. 최종 사용자가 가장 엄격한 안전 검색 설정을 사용하지 않는 경우 검색 결과를 차단하도록 방화벽을 활성화할 수 있으며 사용자에 대해 투명하게 안전 검색을 활성화할 수 있습니다. 방화벽은 다음 검색 공급자에


©2023 Palo Alto Networks, Inc.

대한 안전한 검색 시행을 지원합니다. Google, Yahoo, Bing, Yandex 및 YouTube. 세이프서치 시행을(를) 시작하는 방법을 참조하십시오.

특정 사이트에 대한 암호 액세스 시행

특정 사용자가 사이트에 액세스하도록 허용하면서 대부분의 사용자에 대한 사이트 액세스를 차단할 수 있습니다. 특정 사이트에 대한 암호 액세스를 허용하는 방법을 참조하십시오.

특정 **URL** 카테고리에서 고위험 파일 다운로드 차단

파일 차단 프로파일이 첨부된 보안 정책을 생성하여 특정 URL 카테고리에서 고위험 파일 다운로드를 차단할 수 있습니다.

**URL** 카테고리를 기반으로 보안**,** 복호화**,** 인증 및 **QoS** 정책 시행

URL 카테고리를 기반으로 다양한 유형의 방화벽 정책을 시행할 수 있습니다. 예를 들어, 복호화을(를) 활성화했지만 특정 개인 정보가 복호화되지 않도록 제외하려고 한다고 가정합니다. 이 경우 URL 카테고리 금융 서비스 및 의료 및 의료와 일치하는 웹사이트를 복호화에서 제외하는 복호화 정책 규칙을 생성할 수 있습니다. 또 다른 예는 QoS 정책에서 URL 카테고리 스트리밍 미디어를 사용하여 이 카테고리에 속하는 웹사이트에 대역폭 제어를 적용하는 것입니다.

다음 표에서는 URL 카테고리를 일치 기준으로 허용하는 정책을 설명합니다.

| 정책 유형 | 설명 |
|---|---|
| 복호화 | 또한 URL 카테고리를 사용하여 복호화를 단계적으로 수행하고 복호화에서 민감한 개인 정보를 포함할 수 있는 URL 카테고리(예: 금융 서비스 및 의료 및 의료)를 제외할 수 있습니다.<br><br>가장 위험한 트래픽(게임 또는 고위험과 같은 악성 트래픽을 포함할 가능성이 가장 높은 URL 카테고리)을 먼저 복호화한 다음 경험을 쌓으면서 더 많은 암호를 복호화하도록 계획하십시오. 또는 뉴스 피드와 같이 비즈니스에 영향을 주지 않는 URL 카테고리를 먼저 복호화합니다(문제가 발생하더라도 비즈니스에 영향을 미치지 않음). 두 경우 모두 몇 가지 URL 카테고리를 복호화하고 사용자 피드백을 듣고 보고서를 실행하여 복호화가 예상대로 작동하는지 확인한 다음 점차적으로 몇 가지 더 많은 URL 카테고리를 복호화하는 등의 작업을 수행합니다. 기술적인 이유로 사이트를 복호화할 수 없거나 복호화하지 않기로 선택하여 사이트를 복호화에서 제외하도록 복호화 제외를 계획하십시오.<br><br>***URL*** 카테고리를 기반으로 트래픽 암호를 복호화하는 것은 ***URL*** 필터링과 복호화 모두에 대한 모범 사례입니다**.** |
| 인증 | 사용자가 특정 카테고리에 대한 액세스를 허용하기 전에 인증하도록 하려면 인증 정책 규칙에 대한 일치 기준으로 URL 카테고리를 첨부할 수 있습니다. |


©2023 Palo Alto Networks, Inc.

| 정책 유형 | 설명 |
| --- | --- |
| **QoS** | URL 카테고리를 사용하여 특정 웹사이트 카테고리에 대한 처리량 수준을 할당합니다. 예를 들어 스트리밍 미디어 카테고리를 허용하지만 QoS 정책 규칙에 URL 카테고리를 추가하여 처리량을 제한할 수 있습니다. |
| 보안 | 보안 정책 규칙에서 다음 두 가지 방법으로 URL 카테고리를 사용할 수 있습니다.<br>• URL 카테고리를 일치 기준으로 선택하여 해당 카테고리를 기반으로 정책을 시행합니다.<br>• 각 카테고리에 대한 정책 작업을 지정하는 URL 필터링 프로파일을 첨부합니다.<br>예를 들어 회사의 IT 보안 그룹이 해킹 카테고리로 분류되지만 다른 모든 사용자는 카테고리에 대한 액세스가 거부되는 경우 다음 규칙을 만들어야 합니다.<br>• IT 보안 그룹이 해킹으로 분류된 콘텐츠에 액세스할 수 있도록 하는 보안 정책 규칙입니다. 보안 정책 규칙은 서비스/**URL** 카테고리 탭의 해킹 카테고리와 사용자 탭의 IT-보안 그룹 을 참조합니다.<br>• 모든 사용자에게 일반 웹 액세스를 허용하는 또 다른 보안 정책 규칙입니다. 이 규칙에 해킹 카테고리를 차단하는 URL 필터링 프로파일을 첨부합니다.<br>해킹을 차단하는 정책보다 해킹에 대한 접근을 허용하는 정책을 나열해야 합니다. 이는 방화벽이 위에서 아래로 보안 정책 규칙을 평가하기 때문에 보안 그룹에 속한 사용자가 해킹 사이트에 접근을 시도하면 방화벽이 먼저 접근을 허용하는 정책 규칙을 평가하여 사용자에게 접근 권한을 부여하기 때문입니다. 방화벽은 해킹 사이트에 대한 액세스를 차단하는 일반 웹 액세스 규칙에 대해 다른 모든 그룹의 사용자를 평가합니다. |


©2023 Palo Alto Networks, Inc.

# URL 카테고리

PAN-DB는 사이트 콘텐츠, 기능 및 안전에 따라 웹사이트를 분류합니다. URL에는 위험 카테고리(높음, 중간 및 낮음)를 포함하여 최대 4개의 카테고리가 있을 수 있으며, 이는 사이트가 위협에 노출될 가능성을 나타냅니다. 미리 정의된 URL 카테고리의 전체 목록은 PAN-DB URL 필터링 카테고리를 참조하십시오.

Test A Site를 방문하여 PAN-DB가 URL을 분류하는 방법을 확인하고 사용 가능한 모든 URL 카테고리에 대해 알아봅니다. 사이트 테스트를 사용하여 URL 카테고리 변경 요청을 제출하거나 방화벽에서 직접 요청을 제출할 수 있습니다: 모니터 > 로그를 선택한 다음 로그 항목에 대한 세부 정보를 열 수 있습니다. URL 카테고리에 따라 변경 요청을 제출할 수 있는 옵션이 표시됩니다.

URL 카테고리에 대해 자세히 알아보려면 계속 읽어보세요.

- URL 필터링 사용 사례
- 보안 중심 URL 카테고리
- 악성 URL 카테고리
- 확인된 URL 카테고리
- URL 카테고리를 기반으로 수행할 수 있는 정책 작업

## 보안 중심 URL 카테고리

보안 중심 URL 카테고리는 다양한 수준의 위험을 초래하지만 악의적인 것으로 확인되지 않은 사이트에 대한 표적 복호화 및 적용을 제공하여 공격 면적을 줄이는 데 도움이 될 수 있습니다. 웹사이트는 해당 카테고리의 기준을 충족하는 경우에만 보안 관련 카테고리로 분류됩니다. 사이트 콘텐츠가 변경됨에 따라 정책 적용이 동적으로 조정됩니다. 보안 중심 URL 카테고리에 대한 변경 요청을 제출할 수 없습니다.

| 보안 중심 **URL** 카테고리 | |
|---|---|
| 고위험 | 고위험 사이트는 다음과 같습니다.<br>• 이전에 악성 코드, 피싱 또는 C2 사이트로 확인된 사이트. 이러한 사이트는 최소 30일 동안 이 카테고리에 남아 있습니다.<br>• 알 수 없는 도메인은 PAN-DB가 사이트 분석 및 분류를 완료할 때까지 위험도가 높은 도메인으로 분류됩니다.<br>• 확인된 악의적인 활동과 연관된 사이트입니다. 예를 들어 페이지 자체에 악의적인 콘텐츠가 포함되어 있지 않더라도 동일한 도메인에 악의적인 호스트가 있는 경우 페이지가 위험할 수 있습니다.<br>• 방탄 ISP 호스팅 사이트.<br>• 활성 동적 DNS 구성이 존재하여 DDNS로 분류된 도메인입니다.<br>• 악의적인 콘텐츠를 허용하는 것으로 알려진 ASN의 IP에서 호스팅되는 사이트입니다. |


©2023 Palo Alto Networks, Inc.

| 보안 중심 **URL** 카테고리 | |
|---|---|
| | 기본 및 권장 정책 조치**:** 경고 |
| 중간 위험 | 중위험 사이트는 다음과 같습니다.<br>• 모든 클라우드 저장소 사이트(URL 카테고리 온라인 저장소 및 백업).<br>• 이전에 악성 코드, 피싱 또는 C2 사이트로 확인된 사이트로서 최소 30일 동안 무해한 활동만 표시했습니다. 이러한 사이트는 60일 동안 이 카테고리에 남아 있습니다.<br>• PAN-DB가 사이트 분석 및 분류를 완료할 때까지 알 수 없는 IP 주소가 중간 위험으로 분류됩니다.<br>기본 및 권장 정책 조치**:** 경고 |
| 위험도가 낮음 | 중간 또는 위험이 높지 않은 사이트는 위험도가 낮은 것으로 간주됩니다. 이러한 사이트는 최소 90일 동안 양성 활동을 표시했습니다.<br>기본 및 권장 정책 조치**:** 허용하다 |
| 새로 등록된 도메인 | 지난 32일 이내에 등록된 사이트를 식별합니다. 새 도메인은 악의적인 캠페인의 도구로 자주 사용됩니다.<br>기본 정책 작업**:** 경고<br>권장 정책 조치**:** 차단<br>새로 등록된 도메인은 의도적으로 또는 도메인 생성 알고리즘에 의해 생성되며 악의적인 활동에 사용되는 경우가 많습니다. 이 ***URL*** 카테고리를 차단하는 것이 좋습니다**.** |

## 악성 URL 카테고리

악의적이거나 악의적인 콘텐츠를 식별하는 URL 카테고리를 차단하는 것이 좋습니다. 시작하려면 기본적으로 멀웨어, 피싱 및 명령 및 제어 URL 카테고리를 차단하는 기본 URL 필터링 프로파일을 복제할 수 있습니다. 기본 URL 필터링 프로파일은 또한 약물 남용, 성인, 도박, 해킹, 의심스러운 행동 및 무기 URL 카테고리를 차단합니다. 이러한 URL 카테고리를 차단할지의 여부는 비즈니스 요구 사항에 따라 다릅니다. 예를 들어, 대학은 가용성이 중요하기 때문에 이러한 사이트의 대부분에 대한 학생 액세스를 제한하고 싶지 않을 수 있지만 보안을 최우선으로 생각하는 기업은 일부 또는 전체를 차단할 수 있습니다.

- 명령 및 제어 - 악성 명령을 수신하거나 데이터를 추출하기 위해 공격자의 원격 서버와 은밀하게 통신하기 위해 악성코드 및/또는 손상된 시스템에서 사용하는 명령 및 제어 URL 및 도메인입니다.
- 멀웨어 - 멀웨어를 호스팅하거나 명령 및 제어(C2) 트래픽에 사용되는 것으로 알려진 사이트입니다. Exploit Kit도 전시할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

- 피싱 - 자격 증명 피싱 페이지 또는 개인 식별을 위한 피싱을 호스팅하는 것으로 알려져 있습니다. 여기에는 로그인 자격 증명, 신용카드 정보(자발적 또는 비자발적), 계정 번호, PIN 및 소셜 엔지니어링 기술을 통해 피해자로부터 개인 식별 정보(PII)로 간주되는 모든 정보를 포함하여 정보를 수집하기 위해 사용자를 속이려고 은밀하게 시도하는 웹 콘텐츠가 포함됩니다. 기술 지원 스캠 및 스케어웨어도 피싱에 포함됩니다.
- 그레이웨어**(grayware)** - 바이러스의 정의에 부합하지 않거나 직접적인 보안 위협을 제기하지만 눈에 거슬리는 동작을 표시하고 사용자가 원격 액세스 권한을 부여하거나 기타 승인되지 않은 작업을 수행하도록 영향을 미치는 웹사이트 및 서비스입니다. 그레이웨어에는 사기, 불법 활동, 범죄 활동, 겟 리치 퀵 사이트, 애드웨어 및 브라우저 요소를 변경하는 임베디드 크립토 마이너 또는 하이재커와 같은 기타 원치 않거나 원치 않는 애플리케이션이 포함됩니다. 악의를 나타내지 않고 대상 도메인이 소유하지 않은 타이포스쿼팅 도메인은 그레이웨어로 분류됩니다. 콘텐츠 릴리스 버전 8206 이전에는 방화벽이 멀웨어 또는 의심스러운 URL 카테고리에 그레이웨어를 배치했습니다. 그레이웨어를 차단할지의 여부가 확실하지 않은 경우 그레이웨어에 대한 경고부터 시작하여 경고를 검토한 다음 그레이웨어를 차단할지 아니면 그레이웨어에 대한 경고를 계속할지 결정하십시오.
- **dynamic-dns** - 동적으로 할당된 IP 주소가 있고 종종 멀웨어 페이로드 또는 C2 트래픽을 포워딩하는 데 사용되는 시스템의 호스트 및 도메인 이름입니다. 또한 동적 DNS 도메인은 평판이 좋은 도메인 등록 회사에서 등록한 도메인과 동일한 검증 프로세스를 거치지 않으므로 신뢰도가 떨어집니다.
- **unknown** - PAN-DB에 의해 아직 식별되지 않은 사이트입니다. 가용성이 비즈니스에 중요하고 트래픽을 허용해야 하는 경우 알 수 없는 사이트에 경고하고 모범 사례의 보안 프로파일을 트래픽에 적용하고 경고를 검토해야 합니다.

  > *PAN-DB* 실시간 업데이트는 알 수 없는 사이트에 대한 첫 번째 액세스 시도 후 알 수 없는 사이트를 학습하므로 알 수 없는 ***URL***을 빠르게 식별하고 방화벽이 실제 ***URL*** 카테고리를 기반으로 처리할 수 있는 알려진 ***URL***이 됩니다**.**

- 새로 등록된 도메인 - 새로 등록된 도메인은 종종 의도적으로 또는 도메인 생성 알고리즘에 의해 생성되며 악의적인 활동에 사용됩니다.
- 저작권 침해 - 소프트웨어 또는 기타 지적 재산의 불법 다운로드를 허용하는 콘텐츠와 같이 잠재적인 책임 위험이 있는 불법 콘텐츠가 있는 도메인입니다. 이 카테고리는 교육 업계에서 요구하는 아동 보호법과 인터넷 제공자가 서비스를 통해 저작권 자료를 공유하는 것을 방지하도록 요구하는 국가의 법률을 준수할 수 있도록 도입되었습니다.
- 극단주의 - 테러리즘, 인종차별주의, 파시즘 또는 다른 인종적 배경, 종교 또는 기타 신념을 가진 사람이나 그룹을 차별하는 기타 극단주의적 견해를 조장하는 웹사이트입니다. 이 카테고리는 교육 산업에서 요구되는 아동 보호법을 준수할 수 있도록 도입되었습니다. 일부 지역에서는 법률 및 규정에 따라 극단주의 사이트에 대한 액세스 허용이 금지될 수 있으며 액세스를 허용하면 법적 책임이 따를 수 있습니다.
- **proxy-avoidance-and-anonymizers** - 콘텐츠 필터링 제품을 우회하는 데 자주 사용되는 URL 및 서비스입니다.
- 의심스러운 활동 - 개인 또는 그룹의 특정 인구 통계를 대상으로 하는 무미건조한 유머, 불쾌감을 주는 콘텐츠가 포함된 웹사이트입니다.
- 파킹 - 개인이 등록한 도메인으로, 나중에 계정 피싱에 사용되는 경우가 종종 있습니다. 이러한 도메인은 자격 증명 또는 개인 식별 정보에 대한 피싱을 목적으로 하는 합법적인 도메인(예: pal0alto0netw0rks.com)과 유사할 수 있습니다. 또는 panw.net과 같이 언젠가는 가치가 있기를 바라는 마음으로 개인이 권리를 구매하는 도메인일 수도 있습니다.

 ©2023 Palo Alto Networks, Inc.

차단 대신 경고하기로 결정한 카테고리의 경우 사용자가 사이트 콘텐츠와 상호 작용하는 방식을 매우 엄격하게 제어할 수 있습니다. 예를 들어 사용자에게 필요한 리소스(예: 연구 목적의 개발자 블로그 또는 클라우드 스토리지 서비스)에 대한 액세스 권한을 부여하되 웹 기반 위협에 대한 노출을 줄이려면 다음 예방 조치를 취하세요.

- 안티 스파이웨어, 취약점 보호 및 파일 차단 모범 사례를 따르십시오. 보호 조치는 위험한 파일 형식의 다운로드를 차단하고 경고하는 사이트에 대해 난독화된 JavaScript를 차단하는 것입니다.
- URL 카테고리를 기반으로 대상 복호화. 좋은 시작은 고위험 및 중간 위험 사이트의 암호를 복호화하는 것입니다.
- 사용자가 고위험 및 중간 위험 사이트를 방문할 때 응답 페이지를 표시합니다. 액세스하려는 사이트가 잠재적으로 악의적임을 알리고 사이트를 계속 사용하기로 결정한 경우 예방 조치를 취하는 방법에 대해 조언합니다.
- 사용자가 고위험 및 중간 위험 사이트를 포함한 사이트에 회사 자격 증명을 제출하지 못하도록 차단하여 자격 증명 도난을 방지합니다.

## 확인된 URL 카테고리

Palo Alto Networks는 요청된 사이트가 속한 URL 카테고리를 확인합니다. PAN-DB가 URL이 악성 URL 카테고리에 속하는 것으로 판단하면 사이트에 보안 중심 URL 카테고리(고위험, 중간 위험, 저위험 ). 방화벽은 대부분의 환경에서 허용할 수 없는 수준의 위험을 제기하기 때문에 이러한 카테고리의 사이트를 자동으로 차단합니다. 위험 수준은 악성으로 분류되지 않거나 증거 부족으로 인해 악성으로 분류되지 않은 URL에 대해서만 예약됩니다.

다음 표에는 PAN-DB가 **비공개 IP 주소**를 제외하고 악성으로 간주하고 기본적으로 차단하는 카테고리가 나열되어 있습니다. 사설 IP 주소(및 호스트)는 호스트 환경에 고유하며 PAN-DB에는 표시되지 않습니다. 따라서 Palo Alto Networks는 이 카테고리의 사이트에 위험 등급을 할당하지 않습니다.

| 카테고리 | 기본 작업 |
|---|---|
| 멀웨어 | 차단 |
| 피싱 | |
| 명령 및 제어 | |
| 그레이웨어 | |
| 사설 **IP** 주소 | 허용됨(기본 작업 없음) |

현재 ***URL*** 카테고리에 대한 자세한 내용은 다음을 참조하십시오. PAN-DB URL 필터링 카테고리의 전체 목록

## URL 카테고리에 따라 취할 수 있는 정책 조치

방화벽에서 URL 필터링 프로파일을 사용하여 URL 카테고리를 적용할 방법을 지정할 수 있습니다. 기본적으로 모든 URL 카테고리에 대한 사이트 액세스는 새 URL 필터링 프로파일을 만들 때 허용하도록 설정됩니다. 이는 사용자가 모든 사이트를 자유롭게 탐색할 수 있고 트래픽이 기록되지 않음을 의미합니다. 각


©2023 Palo Alto Networks, Inc.

카테고리에 적용할 사이트 액세스 유형을 결정하여 URL 필터링 프로파일을 사용자 지정합니다. 자격 증명 피싱을 방지하기 위해 URL 카테고리에 따라 사용자 자격 증명 제출을 허용하거나 허용하지 않을 수도 있습니다(예: 중간 및 고위험 사이트에 대한 사용자 자격 증명 제출을 차단할 수 있음). 사용자는 이러한 사이트에 계속 액세스할 수 있지만 회사 자격 증명을 제출할 수는 없습니다.

URL 필터링에 정의한 작업을 시행하려면 보안 정책 규칙에 프로파일을 연결해야 합니다. 방화벽은 보안 정책 규칙과 일치하는 트래픽에 대해 프로파일 작업을 시행합니다(자세한 내용은 URL 필터링 구성 참조).



멀웨어 또는 악용 콘텐츠를 호스팅하는 것으로 관찰된 ***URL***에 대한 보호를 보장하기 위해 모범 사례 URL 필터링 프로파일을 구성하는 방법에 대해 자세히 알아보세요.

| 동작 | 설명 |
|---|---|
| 사이트 액세스 | |
| 경고 | 웹사이트가 허용되고 URL 필터링 로그에 로그 항목이 생성됩니다.<br><br>차단하지 않는 트래픽 카테고리에 대해 경고를 작업으로 설정하여 트래픽을 기록하고 가시성을 제공합니다. |
| 허용 | 웹사이트가 허용되며 로그 항목이 생성되지 않습니다.<br><br>기록하지 않는 트래픽에 대한 가시성을 잃게 되므로 차단하지 않는 트래픽 카테고리에 대한 작업으로 허용을 설정하지 마십시오. 대신, 차단하지 않는 트래픽 카테고리에 대한 작업으로 경고를 설정하여 트래픽에 대한 가시성을 기록하고 제공하십시오. |
| 차단 | 웹사이트가 차단되고 사용자에게 응답 페이지가 표시되고 웹사이트를 계속할 수 없습니다. URL 필터링 로그에 로그 항목이 생성됩니다.<br>URL 카테고리에 대한 사이트 액세스를 차단하면 해당 URL 카테고리에 대한 사용자 자격 증명 제출도 차단되도록 설정됩니다. |
| 계속 | 사용자에게 회사 정책으로 인해 사이트가 차단되었음을 나타내는 응답 페이지가 표시되지만 웹사이트를 계속할 것인지 묻는 옵션이 표시됩니다. 계속 작업은 일반적으로 무해한 것으로 간주되는 카테고리에 사용되며 사이트가 잘못 분류되었다고 느끼는 경우 계속할 수 있는 옵션을 제공하여 사용자 경험을 개선하는 데 사용됩니다. 응답 페이지 메시지는 회사에 특정한 세부 정보를 포함하도록 사용자 정의할 수 있습니다. URL 필터링 로그에 로그 항목이 생성됩니다.<br><br>계속 페이지는 프록시 서버를 사용하도록 구성된 클라이언트 시스템에서 제대로 표시되지 않습니다. |


©2023 Palo Alto Networks, Inc.

| 동작 | 설명 |
| --- | --- |
| 재정의 | 사용자는 주어진 카테고리의 웹사이트에 대한 액세스를 허용하려면 암호가 필요하다는 응답 페이지를 보게 됩니다. 이 옵션을 사용하면 보안 관리자 또는 헬프데스크 담당자가 지정된 카테고리의 모든 웹사이트에 대한 임시 액세스 권한을 부여하는 암호를 제공합니다. URL 필터링 로그에 로그 항목이 생성됩니다. 특정 사이트에 대한 암호 액세스 허용을 참조하십시오.<br><br>이전 릴리스 버전에서는 URL 필터링 카테고리 재정의가 사용자 지정 URL 카테고리보다 우선 적용되었습니다. PAN-OS 9.0으로 업그레이드하는 과정에서 URL 카테고리 재정의가 사용자 지정 URL 카테고리로 변환되고 더 이상 다른 사용자 지정 URL 카테고리보다 우선 적용되지 않습니다. 이전 릴리스 버전에서 카테고리 재정의에 대해 정의한 작업 대신 가장 엄격한 URL 필터링 프로파일 작업이 있는 보안 정책 규칙에 의해 새 사용자 지정 URL 카테고리가 적용됩니다. 가장 엄격한 것에서 가장 덜 엄격한 것까지 가능한 URL 필터링 프로파일 작업은 차단, 재정의, 계속, 경고 및 허용입니다.<br><br>즉, 허용 작업으로 URL 카테고리 재정의가 있는 경우 PAN-OS 9.0에서 사용자 지정 URL 카테고리로 변환된 후 재정의가 차단될 가능성이 있습니다.<br><br>재정의 페이지는 프록시 서버를 사용하도록 구성된 클라이언트 시스템에서 제대로 표시되지 않습니다. |
| 없음 | 없음 작업은 사용자 지정 URL 카테고리에만 적용됩니다. 여러 URL 필터링 프로파일이 있는 경우 사용자 지정 카테고리가 다른 프로파일에 영향을 미치지 않도록 하려면 없음을 선택합니다. 예를 들어, 두 개의 URL 필터링 프로파일이 있고 사용자 지정 URL 카테고리가 한 프로파일에서 차단으로 설정된 경우 차단 작업이 다른 프로파일에 적용되지 않도록 하려면 작업을 없음으로 설정해야 합니다.<br><br>또한 사용자 지정 URL 카테고리를 삭제하려면 해당 카테고리가 사용되는 프로파일에서 없음으로 설정해야 합니다. |
| 사용자 자격 증명 권한<br><br>이러한 설정을 사용하려면 먼저 자격 증명 피싱 방지를 설정해야 합니다. | |
| 경고 | 사용자가 이 URL 카테고리에 있는 사이트에 회사 자격 증명을 제출할 수 있도록 허용하지만 이러한 상황이 발생할 때마다 URL 필터링 경고 로그를 생성합니다. |
| 허용(기본값) | 사용자가 이 URL 카테고리의 웹사이트에 회사 자격 증명을 제출하도록 허용합니다. |
| 차단 | 사용자가 이 카테고리의 웹사이트에 회사 자격 증명을 제출하지 못하도록 차단합니다. 사용자가 회사 자격 증명 제출이 차단된 사이트에 액세스하면 기본 |


©2023 Palo Alto Networks, Inc.

| 동작 | 설명 |
| --- | --- |
| | 피싱 방지 응답 페이지가 표시됩니다. 표시할 사용자 정의 블록 페이지를 생성하도록 선택할 수 있습니다. |
| 계속 | 사이트에 액세스하려면 계속 액세스를 선택하라는 응답 페이지를 사용자에게 표시합니다. 기본적으로 사용자가 자격 증명 제출을 권장하지 않는 사이트에 액세스하면 안티 피싱 계속 페이지가 표시됩니다. 예를 들어 사용자에게 피싱 시도에 대해 경고하거나 다른 웹사이트에서 자격 증명을 재사용하려는 경우 표시할 사용자 지정 응답 페이지를 생성하도록 선택할 수도 있습니다. |


©2023 Palo Alto Networks, Inc.

# URL 필터링 배포 계획

네트워크에 URL 필터링을 배포하려면 확인된 악성 콘텐츠를 차단하면서 웹 활동 패턴에 대한 가시성을 제공하는 기본 설정으로 시작하는 것이 좋습니다.

- 대부분의 카테고리에 대해 경고하는(대부분) 수동형 URL 필터링 프로파일로 시작합니다. 이렇게 하면 사용자가 액세스하는 사이트를 볼 수 있으므로 허용, 제한 및 차단할 항목을 결정할 수 있습니다.
- 악성코드, C2, 피싱 등 악성으로 알려진 URL 카테고리를 차단합니다.

모든 웹 활동에 대한 경고는 많은 양의 로그 파일을 생성할 수 있으므로 처음에 URL 필터링을 배포할 때만 이 작업을 수행하기로 결정할 수 있습니다.



이때 ***URL*** 필터링 프로파일에서 컨테이너 페이지만 로그 옵션을 활성화하여 ***URL*** 필터링 로그를 줄일 수도 있습니다**.** 그러면 컨테이너 페이지 내에서 로드될 수 있는 후속 페이지**/**카테고리가 아닌 카테고리와 일치하는 기본 페이지만 기록됩니다**.**

**STEP 1 |** 언제든지 Test A Site를 사용하여 PAN-DB(URL 필터링 클라우드 데이터베이스)가 특정 URL을 분류하는 방법을 확인하고 가능한 모든 URL 카테고리에 대해 알아볼 수 있습니다.

특정 URL이 분류되는 방식에 동의하지 않는 경우 Test A Site를 사용하여 변경 요청을 제출할 수도 있습니다.

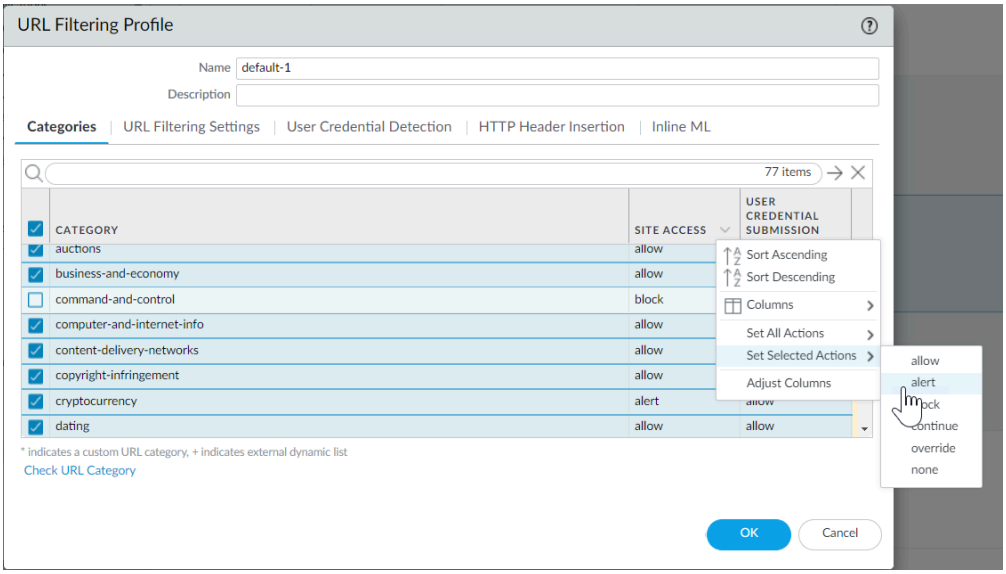
**STEP 2 |** 웹 트래픽을 볼 수 있도록 모든 카테고리에 대해 경고하는 수동형 URL 필터링 프로파일을 생성합니다.

1. 개체 > 보안 프로파일**> URL** 필터링을 선택합니다.
2. 기본 프로파일을 선택한 다음 복제를 클릭합니다. 새 프로파일의 이름은 **default-1**입니다.
3. **default-1** 프로파일을 선택한 다음 이름을 바꿉니다. 예를 들어 URL-Monitoring으로 이름을 바꿉니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 차단된 상태로 유지해야 하는 멀웨어, 명령 및 제어 및 피싱을 제외한 모든 카테고리에 대해 경고할 작업을 구성합니다.

1. 모든 URL 카테고리를 나열하는 섹션에서 모든 카테고리를 선택한 다음 멀웨어, 명령 및 제어 및 피싱을 선택 취소합니다.
2. 작업 열 머리글의 오른쪽에 있는 아래쪽 화살표 위로 마우스를 가져간 다음 선택한 작업 설정을 선택한 다음 경고를 선택합니다.




3. 알려진 위험한 URL 카테고리에 대한 액세스를 차단합니다.

   멀웨어, 피싱, 동적 ***DNS***, 알 수 없음, 명령 및 제어, 극단주의, 저작권 침해, 프록시 회피 및 익명화, 새로 등록된 도메인, 그레이웨어 및 파킹된 ***URL*** 카테고리에 대한 액세스를 차단합니다.

4. 확인을 클릭하여 프로파일을 저장합니다.

**STEP 4 |** URL 필터링 프로파일을 사용자에게 웹 트래픽을 허용하는 보안 정책 규칙에 적용합니다.

1. 정책 > 보안을 선택한 다음 적절한 보안 정책을 선택하여 수정합니다.
2. 작업 탭을 선택한 다음 프로파일 설정 섹션에서 **URL** 필터링 드롭다운을 클릭하고 새 프로파일을 선택합니다.
3. 확인을 클릭하여 저장합니다.

**STEP 5 |** 구성을 저장합니다.

커밋을 클릭합니다.

**STEP 6 |** URL 필터링 로그를 보고 사용자가 액세스하는 모든 웹 사이트 카테고리를 확인합니다. 차단하도록 설정한 카테고리도 기록됩니다.

로그 보기 및 보고서 생성에 대한 자세한 내용은 웹 활동 모니터링을 참조하십시오.

모니터 > 로그 > **URL** 필터링을 선택합니다. 허용 이외의 작업으로 설정된 카테고리에 있는 URL 필터링 데이터베이스에 있는 모든 웹사이트에 대한 로그 항목이 생성됩니다. URL 필터링 보고서는 24시간 동안의 웹 활동에 대한 보기를 제공합니다. (모니터 > 보고서).


©2023 Palo Alto Networks, Inc.

**STEP 7 |** 다음 단계:

- PAN-DB는 모든 URL을 최대 4개의 카테고리로 분류하고 모든 URL에는 위험 카테고리(높음, 중간 및 낮음)가 있습니다. 고위험 및 중간 위험 사이트는 악성으로 확인되지는 않았지만 악성 사이트와 밀접하게 연관되어 있습니다. 예를 들어 악성 사이트와 동일한 도메인에 있거나 아주 최근까지만 해도 악성 콘텐츠를 호스팅했을 수 있습니다. 허용하지 않거나 차단하지 않는 모든 항목에 대해 위험 카테고리를 사용하여 웹사이트 안전을 기반으로 하는 간단한 정책을 작성할 수 있습니다.

  특히 안전 문제가 발생할 수 있는 사이트에 대한 액세스 권한을 사용자에게 부여하려는 경우가 있을 수 있으므로 사용자의 상호 작용이 고위험 사이트를 제한하기 위해 예방 조치를 취할 수 있습니다(예를 들어, 개발자가 연구를 위해 개발자 블로그를 사용하도록 허용할 수 있지만 블로그는 일반적으로 멀웨어를 호스팅하는 것으로 알려진 카테고리입니다.).
- URL 필터링을 User-ID와 페어링하여 조직 또는 부서를 기반으로 웹 액세스를 제어하고 승인되지 않은 사이트에 대한 회사 자격 증명 제출을 차단합니다.
  - URL 필터링은 사이트 카테고리를 기반으로 사이트에 대한 회사 자격 증명 제출을 감지하여 자격 증명 도난을 방지합니다. 사용자가 악의적이고 신뢰할 수 없는 사이트에 자격 증명을 제출하지 못하도록 차단하고, 알 수 없는 사이트에서 기업 자격 증명을 입력하거나 기업이 아닌 사이트에서 기업 자격 증명을 재사용하지 않도록 사용자에게 경고하고, 사용자가 기업 사이트에 자격 증명을 제출하도록 명시적으로 허용합니다.
  - 마케팅 또는 엔지니어링(**Policies** > **Security** > **User**)과 같은 부서 사용자 그룹에 적용되도록 수동형 URL 필터링 프로파일을 사용하여 보안 정책 규칙을 추가하거나 업데이트합니다. 부서 활동을 모니터링하고 부서 구성원의 피드백을 받아 업무에 필수적인 웹 리소스를 이해합니다.
- URL 필터링을 사용하여 공격 표면을 줄이고 웹 사용을 제어할 수 있는 모든 방법을 고려하십시오. 예를 들어 학교인 경우 URL 필터링을 사용하여 검색 엔진이 검색 결과에서 성인 이미지와 비디오를 필터링하는 엄격한 안전 검색 설정을 시행할 수 있습니다. 또는 보안 운영 센터가 있는 경우 연구를 위해 위협 분석가에게 손상되거나 위험한 사이트에 대한 암호 액세스 권한을 부여할 수 있으며, 그렇지 않을 경우 전체 조직이나 팀에 공개하길 원하지 않을 수 있습니다.
- URL 필터링 모범 사례를 따르십시오.

 ©2023 Palo Alto Networks, Inc.

# URL 필터링 모범 사례

Palo Alto Networks URL 필터링은 웹 기반 위협으로부터 사용자를 보호하고 웹 활동을 모니터링하고 제어할 수 있는 간단한 방법을 제공합니다. URL 필터링을 최대한 활용하려면 비즈니스를 수행하는 데 사용하는 애플리케이션에 대한 허용 규칙을 만들어야 합니다. 그런 다음 악성 콘텐츠와 악용적 콘텐츠를 분류하는 URL 카테고리를 검토합니다. 이러한 카테고리를 완전히 차단하는 것이 좋습니다. 그런 다음 다른 모든 경우에 이러한 모범 사례는 필요한 웹 콘텐츠에 대한 사용자의 액세스를 제한하지 않고 웹 기반 위협에 노출되는 것을 줄이는 방법을 안내합니다.

- 시작하기 전에 모범 사례 인터넷 게이트웨이 보안 정책 구축의 일환으로 허용할 애플리케이션을 식별하고 애플리케이션 허용 규칙을 생성하십시오.

  허용되는 애플리케이션에는 비즈니스 및 인프라 목적으로 프로비저닝하고 관리하는 애플리케이션뿐만 아니라 사용자가 작업을 완료하는 데 필요한 애플리케이션과 개인적인 용도로 허용할 수 있는 애플리케이션도 포함됩니다.

  이러한 승인된 애플리케이션을 식별한 후에는 URL 필터링을 사용하여 허용 목록에 없는 모든 웹 활동을 제어하고 보호할 수 있습니다.
- 사용자의 웹 활동에 대한 가시성을 확보하여 조직에 가장 효과적인 URL 필터링 정책을 계획하고 원활하게 배포할 수 있습니다. 여기에는 다음이 포함됩니다.
  - 사이트 테스트를 사용하여 PAN-DB(Palo Alto Networks URL 필터링 클라우드 데이터베이스)가 특정 URL을 분류하는 방법을 확인하고 가능한 모든 URL 카테고리에 대해 알아봅니다.
  - URL 카테고리에 대해 경고하는(대부분) 수동형 URL 필터링 프로파일로 시작합니다. 이렇게 하면 사용자가 액세스하는 사이트를 볼 수 있으므로 허용, 제한 및 차단할 항목을 결정할 수 있습니다.
  - 웹 활동을 모니터링하여 사용자가 액세스하는 사이트를 평가하고 비즈니스 요구 사항에 어떻게 부합하는지 확인합니다.
- 악성 및 악용적 웹 콘텐츠를 분류하는 URL 카테고리를 차단합니다. 이러한 카테고리는 위험하다는 것을 알고 있지만 차단하기로 결정한 URL 카테고리는 비즈니스 요구 사항에 따라 달라질 수 있습니다.
- URL 카테고리를 사용하여 복호화를 단계적으로 처리하고, 민감한 정보 또는 개인 정보(예: 금융 서비스 및 건강 및 의료)를 복호화에서 제외할 수 있습니다.

  가장 위험한 트래픽(게임 또는 고위험과 같은 악성 트래픽을 포함할 가능성이 가장 높은 URL 카테고리)을 먼저 복호화한 다음 경험을 쌓으면서 더 많은 암호를 복호화하도록 계획하십시오. 또는 뉴스 피드와 같이 비즈니스에 영향을 주지 않는 URL 카테고리를 먼저 복호화합니다(문제가 발생하더라도 비즈니스에 영향을 미치지 않음). 두 경우 모두 몇 가지 URL 카테고리를 복호화하고 사용자 피드백을 듣고 보고서를 실행하여 복호화가 예상대로 작동하는지 확인한 다음 점차적으로 몇 가지 더 많은 URL 카테고리를 복호화하는 등의 작업을 수행합니다. 기술적인 이유로 사이트를 복호화할 수 없거나 복호화하지 않기로 선택하여 사이트를 복호화에서 제외하도록 복호화 제외를 계획하십시오.

  ***URL** 카테고리를 기반으로 하는 타깃팅 복호화도 복호화의 모범 사례입니다.*
- 방화벽이 사이트에 대한 기업 자격 증명 제출을 감지하고 URL 카테고리에 따라 제출을 제어하여 자격 증명 도용을 방지할 수 있습니다. 사용자가 악의적이고 신뢰할 수 없는 사이트에 자격 증명을 제출하지 못하도록 차단하고, 알 수 없는 사이트에서 기업 자격 증명을 입력하거나 기업이 아닌 사이트에서 기업 자격 증명을 재사용하지 않도록 사용자에게 경고하고, 사용자가 기업 및 승인된 사이트에 자격 증명을 제출하도록 명시적으로 허용합니다.


©2023 Palo Alto Networks, Inc.

- JavaScript 악용 및 피싱 공격의 악성 변형을 실시간으로 차단합니다. 로컬 인라인 분류을 활성화하면 방화벽에서 기계 학습을 사용하여 웹 페이지를 동적으로 분석할 수 있습니다.
- 고급 URL 필터링 인라인 클라우드 분류 를 활성화하여 인라인 딥 러닝, ML 기반 검색 엔진을 사용하여 의심스러운 웹 페이지 콘텐츠를 분석하고 제로 데이 웹 공격으로부터 사용자를 보호합니다. 클라우드 인라인 분류는 고급 및 표적 피싱 공격, 클로킹, 다단계 공격, CAPTCHA 챌린지 및 이전에는 볼 수 없었던 일회성 URL과 같은 고급 회피 기술을 사용하는 기타 웹 기반 공격을 탐지하고 예방할 수 있습니다.
- 사용자가 고위험 및 중간 위험 콘텐츠와 상호 작용하는 방식을 복호화, 검사 및 엄격하게 제한합니다(비즈니스 이유로 악성 URL 카테고리를 차단하지 않기로 결정한 경우 사용자가 해당 카테고리와 상호 작용하는 방식도 엄격하게 제한해야 함).

  승인하는 웹 콘텐츠와 차단하는 악성 URL 카테고리는 전체 웹 트래픽의 일부에 불과합니다. 사용자가 액세스하는 나머지 콘텐츠는 양성(저위험) 콘텐츠와 위험한 콘텐츠(고위험 및 중간 위험)의 조합입니다. 위험도가 높고 위험도가 중간 정도인 콘텐츠는 악성으로 확인되지는 않지만 악성 사이트와 밀접한 관련이 있습니다. 예를 들어 고위험 URL이 악성 사이트와 동일한 도메인에 있거나 과거에 악성 콘텐츠를 호스팅했을 수 있습니다.

  그러나 조직에 위험을 초래하는 많은 사이트는 사용자에게 귀중한 리소스와 서비스를 제공합니다(클라우드 저장소 서비스가 좋은 예입니다). 이러한 리소스와 서비스는 비즈니스에 필수적이지만 사이버 공격의 일부로 사용될 가능성이 높습니다. 사용자가 위험할 수 있는 콘텐츠와 상호 작용하는 방식을 제어하면서 사용자에게 우수한 사용자 환경을 제공하는 방법은 다음과 같습니다.

  - URL 필터링 프로파일에서 위험 가능성이 높은 사이트를 방문하는 사용자에게 경고하는 응답 페이지를 계속 표시하도록 위험도가 높은 카테고리와 중간 위험 카테고리를 설정합니다. 사이트를 계속 방문하기로 결정한 경우 예방 조치를 취하는 방법을 알려주십시오. 사용자에게 응답 페이지를 표시하지 않으려면 고위험 및 중간 위험 카테고리에 대해 경고하십시오.
  - 고위험 및 중간 위험 사이트를 복호화합니다.
  - 고위험 및 중간 위험 사이트의 경우 안티 스파이웨어, 취약점 보호 및 파일 차단 모범 사례를 따르십시오. 보호 조치는 위험한 파일 형식의 다운로드를 차단하고 난독화된 JavaScript를 차단하는 것입니다.
  - 사용자가 고위험 및 중간 위험 사이트에 회사 자격 증명을 제출하지 못하도록 차단하여 자격 증명 도용을 차단합니다.
- 학교 또는 교육 기관은 검색 엔진이 검색결과에서 성인용 이미지와 동영상을 필터링하도록 하기 위해 안전 검색 정책을 사용해야 합니다. 사용자에 대한 안전한 검색을 명백히 활성화할 수도 있습니다.
- PAN-DB를 사용하여 웹사이트의 URL 카테고리를 조회할 때 초기 웹 요청을 보유하도록 방화벽을 활성화합니다.

  사용자가 웹사이트를 방문하면 URL 필터링이 활성화된 방화벽이 URL 카테고리의 로컬 캐시를 확인하여 사이트를 분류합니다. 방화벽이 캐시에서 URL의 카테고리를 찾지 못하면 PAN-DB인 Palo Alto Networks URL 데이터베이스에서 조회를 수행합니다. 기본적으로 방화벽은 이 클라우드 조회 중에 사용자의 웹 요청을 허용하고 서버가 응답할 때 정책을 적용합니다.

  그러나 웹 요청을 보류하도록 선택하면 방화벽이 URL 카테고리를 찾거나 타임아웃될 때까지 요청을 차단합니다. 조회 시간이 초과되면 방화벽은 URL 카테고리가 해결되지 않은 것으로 간주합니다.

  1. 디바이스 > 설정 > 콘텐츠**-ID**에서

     카테고리 조회를 위한 클라이언트 요청 보류 확인란을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

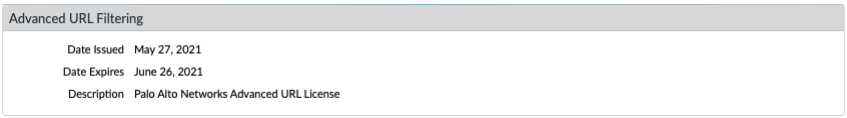
# 고급 URL 필터링 구독 활성화

Palo Alto Networks URL 필터링 솔루션인 고급 URL 필터링 구독은 실시간 URL 분석 및 맬웨어 방지 기능을 제공합니다. Palo Alto Networks가 개발한 고성능 URL 조회를 위한 URL 필터링 데이터베이스인 PAN-DB 액세스 외에도 악성 URL 및 IP 주소에 대한 적용 범위도 제공합니다. 이 다계층 보호 솔루션은 URL 필터링 프로파일을 통해 구성됩니다.

**STEP 1 |** 고급 URL 필터링 라이선스를 가져와 설치하고 설치되었는지 확인합니다.

*Advanced URL* 필터링 라이선스에는 *PAN-DB*에 대한 액세스가 포함됩니다. 라이선스가 만료되면 방화벽은 모든 *URL* 필터링 기능, *URL* 카테고리 적용 및 *URL* 클라우드 조회를 수행하지 않습니다. 또한 유효한 라이선스를 설치하기 전까지는 다른 모든 클라우드 기반 업데이트가 작동하지 않습니다.

1. 디바이스 > 라이선스를 선택한 다음 라이선스 관리 섹션에서 라이선스 설치 방법을 선택합니다.
   - 라이선스 서버에서 라이선스 키 검색
   - 권한 부여 코드를 사용하여 기능 활성화
2. 라이선스를 설치한 후 고급 URL 필터링 섹션의 만료 날짜 필드에 유효한 날짜가 표시되는지 확인합니다.




*Advanced URL* 필터링 라이선스를 활성화하면 *PAN-DB* 및 *Advanced URL* 필터링에 대한 라이선스 자격은 방화벽에 올바르게 표시되지 않을 수 있습니다. 방화벽의 라이선스를 업데이트하여 다음 *CLI* 명령인 **요청 라이선스 가져오기**를 사용하여 디스플레이 문제를 해결할 수 있습니다.

**STEP 2 |** 최신 PAN-OS 콘텐츠 릴리스를 다운로드하고 설치합니다. PAN-OS 애플리케이션 및 위협 콘텐츠는 8390-6607을 릴리스하고 나중에 PAN-OS 9.x를 운영하는 방화벽을 통해 새로운 실시간 검색 카테고리를 사용하여 분류된 URL을 식별하여 Advanced URL 필터링으로 분류되는 URL을 식별할 수 있습니다. 업데이트에 대한 자세한 내용은 애플리케이션 및 위협 콘텐츠 릴리스 노트를 참조하십시오. Palo Alto Networks 지원 포털이나 방화벽 웹 인터페이스에서 직접 앱 및 위협에 대한 콘텐츠 출시 정보를 검토할 수도 있습니다. 디바이스 > 동적 업데이트를 선택하고 특정 콘텐츠 릴리스 버전에 대한 릴리스 노트를 엽니다.

최신 콘텐츠 릴리스 버전으로 업데이트할 때는 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례를 따르십시오.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 방화벽을 예약하여 애플리케이션 및 위협에 대한 동적 업데이트를 다운로드합니다.

바이러스 백신 및 애플리케이션 및 위협을 다루는 콘텐츠 업데이트를 수신하려면 위협 방지 라이선스가 필요합니다.

1. 디바이스 > 동적 업데이트를 선택합니다.
2. 애플리케이션 및 위협 섹션의 일정 필드에서 **None** 링크를 클릭하여 정기적인 업데이트를 예약합니다.

   방화벽에 직접 인터넷에 액세스할 수 있는 경우에만 동적 업데이트를 예약할 수 있습니다. 섹션에 업데이트가 이미 예약된 경우 링크 텍스트에 일정 설정이 표시됩니다.

   애플리케이션 및 위협 업데이트에는 안전 검색 적용과 관련된 URL 필터링에 대한 업데이트가 포함되는 경우가 있습니다.

다음 단계:

1. 조직의 웹 사용 정책을 정의하도록URL 필터링 프로파일을 구성합니다.
2. Advanced URL 필터링 확인


©2023 Palo Alto Networks, Inc.

# URL 필터링 구성

URL 필터링 정책 요구 사항을 결정한 후에는 사용자가 액세스하는 웹사이트 유형 및 웹사이트 카테고리에 대한 기본적인 이해가 있어야 합니다. 이 정보를 사용하여 사용자 지정 URL 필터링 프로파일을 생성하고 웹 액세스를 허용하는 보안 정책 규칙에 연결합니다. URL 필터링 프로파일로 웹 액세스를 관리하는 것 외에도 User-ID™를 구성하면 사용자가 회사 자격 증명을 제출할 수 있는 사이트를 관리할 수 있습니다.

**STEP 1 |** URL 필터링 프로파일을 생성합니다.



아직 구성하지 않았다면 모범 사례 URL 필터링 프로파일을 구성하여 맬웨어 또는 악의적인 콘텐츠를 호스팅하는 ***URL***로부터 보호하십시오.

개체 > 보안 프로파일 > **URL** 필터링을 선택한 다음 URL 필터링 프로파일을 추가하거나 수정합니다.

**STEP 2 |** 각 URL 카테고리에 대한 사이트 액세스를 정의합니다.

카테고리를 선택한 다음 각 URL 카테고리에 대한 사이트 액세스를 설정합니다.

- 해당 URL 카테고리로 향하는 트래픽을 허용합니다. 허용된 트래픽은 기록되지 않습니다.
- 사용자가 액세스하는 사이트에 대한 가시성을 갖도록 경고를 선택합니다. 해당 카테고리와 일치하는 트래픽은 허용되지만 사용자가 해당 카테고리의 사이트에 액세스할 때 기록하기 위해 URL 필터링 로그가 생성됩니다.
- 해당 카테고리와 일치하는 트래픽에 대한 액세스를 거부하고 차단된 트래픽의 로깅을 활성화하려면 차단을 선택합니다.
- 사용자에게 경고와 함께 페이지를 표시하려면 계속을 선택한 다음 해당 카테고리의 사이트로 이동하려면 계속을 클릭하도록 요구합니다.
- 사용자가 구성된 암호를 제공하는 경우에만 액세스를 허용하려면 무시를 선택합니다. 자세한 내용은 특정 사이트에 대한 암호 액세스 허용을 참조하십시오.

**STEP 3 |** 허용된 URL 카테고리에 있는 웹사이트에 대한 회사 자격 증명 제출을 감지하도록 URL 필터링 프로파일을 구성합니다.



최상의 성능과 낮은 오탐지율을 보장하기 위해 방화벽은 악성코드나 피싱 콘텐츠를 호스팅하는 것이 발견되지 않은 사이트와 연결된 모든 ***App-ID***™에 대한 자격 증명 제출 확인을 자동으로 건너뜁니다. 이는 해당 카테고리에서 검사를 활성화한 경우에도 마찬가지입니다. 방화벽이 자격 증명 확인을 건너뛰는 사이트 목록은 애플리케이션 및 위협 콘텐츠 업데이트를 통해 자동으로 업데이트됩니다.

1. 사용자 자격 증명 감지를 선택합니다.
2. 사용자 자격 증명 감지 드롭다운에서 웹페이지에 대한 회사 자격 증명 제출 확인 방법 중 하나를 선택합니다.
   - **IP** 사용자 매핑 사용 - 유효한 회사 사용자 이름 제출을 확인하고 사용자 이름이 세션의 소스 IP 주소에 로그인한 사용자와 일치하는지 확인합니다. 방화벽은 제출된 사용자 이름을 IP 주소-사용자 이름 매핑 테이블과 일치시킵니다. 사용자에게 IP 주소 매핑에 설명된 모든 사용자 매핑 방법을 사용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

- 도메인 자격 증명 필터 사용 - 유효한 회사 사용자 이름과 암호 제출을 확인하고 사용자 이름이 로그인한 사용자의 IP 주소에 매핑되는지 확인합니다. 이 방법을 활성화하기 위해 사용자 ID를 설정하는 방법에 대한 지침은 Windows User-ID 에이전트를 사용하여 사용자 매핑 구성을 참조하십시오.
- 그룹 매핑 사용 - 사용자를 그룹에 매핑하도록 방화벽을 구성할 때 채워진 사용자-그룹 매핑 테이블을 기반으로 유효한 사용자 이름 제출을 확인합니다.

  그룹 매핑을 사용하면 디렉터리의 모든 부분 또는 가장 민감한 애플리케이션에 액세스할 수 있는 IT와 같은 특정 그룹에 자격 증명 감지를 적용할 수 있습니다.

  이 방법은 고유하게 구조화된 사용자 이름이 없는 환경에서 허위양성(***false positive***)이 되기 쉬우므로 이 방법을 사용하여 고가치 사용자 계정을 보호해야 합니다.

3. 방화벽이 회사 자격 증명 제출 감지를 기록하는 데 사용하는 유효한 사용자 이름 감지 로그 심각도를 설정합니다(기본값은 중간).

**STEP 4 |** 로컬 인라인 분류을(를) 사용하여 실시간으로 피싱 및 악성 자바스크립트를 탐지하도록 URL 필터링 프로파일을 구성합니다.

**STEP 5 |** 사용자가 자격 증명 피싱을 방지하기 위해 URL 카테고리를 기반으로 사이트에 회사 자격 증명을 제출하는 것을 허용하거나 차단합니다.

최고의 성능과 낮은 오탐지율을 보장하기 위해 방화벽은 악성코드나 피싱 콘텐츠를 호스팅하는 것이 관찰된 적이 없는 사이트와 연결된 모든 ***App-ID***에 대한 자격 증명 제출 확인을 자동으로 건너뜁니다. 이는 해당 카테고리에서 검사를 활성화한 경우에도 마찬가지입니다. 방화벽이 자격 증명 확인을 건너뛰는 사이트 목록은 애플리케이션 및 위협 콘텐츠 업데이트를 통해 자동으로 업데이트됩니다.

1. 사이트 액세스를 허용하는 각 URL 카테고리에 대해 사용자 자격 증명 제출을 처리할 방법을 선택합니다.
   - 경고 - 사용자가 웹사이트에 자격 증명을 제출하도록 허용하지만 사용자가 이 URL 카테고리의 사이트에 자격 증명을 제출할 때마다 URL 필터링 경고 로그를 생성합니다.
   - 허용(기본값) - 사용자가 웹사이트에 자격 증명을 제출하도록 허용합니다.
   - 차단 - 사용자가 웹사이트에 자격 증명을 제출하지 못하도록 차단하는 안티 피싱 차단 페이지를 표시합니다.
   - 계속 - 피싱 방지 계속 페이지를 표시하여 사용자가 사이트에 액세스하려면 계속을 클릭하도록 요구합니다.
2. 허용된 URL 카테고리에 있는 웹사이트에 대한 회사 자격 증명 제출을 감지하도록 URL 필터링 프로파일을 구성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** URL 카테고리 예외 목록을 정의하여 URL 카테고리에 관계없이 항상 차단하거나 허용해야 하는 웹 사이트를 지정합니다.

예를 들어 URL 필터링 로그를 줄이기 위해 회사 웹사이트를 허용 목록에 추가하여 해당 사이트에 대한 로그가 생성되지 않도록 할 수 있습니다. 차단 목록에 해당 사이트를 추가할 수 있습니다.

사용자 지정 URL 카테고리에 대해 구성된 정책 작업은 외부 동적 목록에서 일치하는 URL보다 우선적으로 적용됩니다.

차단 목록에 있는 웹사이트에 대한 트래픽은 연결된 카테고리에 대한 작업과 관계없이 항상 차단되며 허용 목록에 있는 URL에 대한 트래픽은 항상 허용됩니다.

적절한 형식 및 와일드카드 사용에 대한 자세한 내용은 URL 카테고리 예외 목록 지침을 검토하십시오.

**STEP 7 |** 세이프서치 기능 활성화.

**STEP 8 |** URL 필터링 이벤트에 대한 컨테이너 페이지만 기록합니다.

1. **URL** 필터링 설정을 선택합니다. 방화벽이 컨테이너 페이지 내에서 로드된 후속 페이지 또는 카테고리가 아닌 카테고리와 일치하는 기본 페이지만 기록하도록 컨테이너 페이지만 로그(기본값)를 활성화합니다.
2. 모든 페이지 및 카테고리에 대한 로깅을 활성화하려면 로그 컨테이너 페이지만 옵션을 비활성화합니다.

**STEP 9 |** 지원되는 HTTP 헤더 필드 중 하나 이상에 대해 HTTP 헤더 로깅을 활성화합니다.

**URL** 필터링 설정을 선택한 후 다음 필드 중 하나 이상을 선택하여 기록합니다.

- 사용자 에이전트
- 추천인
- **X-Forwarded-For**

**STEP 10 |** URL 필터링 프로파일을 저장하고 변경 사항을 커밋합니다.

1. 확인을 클릭합니다.
2. 커밋을 클릭합니다.

**STEP 11 |** URL 필터링 정책 구성을 테스트합니다.

1. 원하는 URL 카테고리의 웹사이트에 접속하여 방화벽의 동작을 관찰합니다.

   사이트에 직접 액세스하지 않으려면 Palo Alto Networks URL 필터링 테스트 페이지(urlfiltering.paloaltonetworks.com/test-***<url-category>***)를 사용하십시오. Palo Alto Networks에는 양성 및 악성 URL 카테고리에 대한 테스트 URL이 있습니다. 예를 들어 맬웨어에 대한 차단 정책을 테스트하려면 https://urlfiltering.paloaltonetworks.com/test-malware를 방문하십시오.
2. 트래픽 및 URL 필터링 로그(모니터 > 로그)를 검토하여 올바른 정책 규칙이 기록되었는지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 12 |** 방화벽이 URL 카테고리 조회를 수행하는 동안 클라이언트 요청을 차단하려면 카테고리 조회에 대한 클라이언트 요청 보류를 활성화하십시오.

1. 디바이스 > 설정 > 콘텐츠**-ID**를 선택합니다.
2. 카테고리 조회를 위한 클라이언트 요청 보류를 선택합니다.
3. 변경 사항을 커밋합니다.



URL 필터링 모범 사례로 이 기능을 활성화하십시오.

**STEP 13 |** URL 카테고리 조회 시간이 초과되기까지의 시간(초)을 설정합니다.

1. 디바이스 > 설정 > 콘텐츠**-ID** > 톱니바퀴 아이콘을 선택합니다.
2. 카테고리 조회 시간 초과**(**초**)**에 숫자를 입력합니다.
3. **확인**을 클릭합니다.
4. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# URL 필터링 구성 테스트

URL 필터링 및 고급 URL 필터링 정책 구성을 테스트하려면 Palo Alto Networks URL 필터링 테스트 페이지를 사용하십시오. Advanced URL 필터링을 실행하는 방화벽에만 적용되는 실시간 탐지 카테고리를 포함하여 사전 정의된 모든 URL 카테고리의 안전한 테스트를 위해 테스트 페이지가 생성되었습니다.

테스트 페이지가 ***HTTPS*** 연결을 통해 작동하려면 ***SSL*** 암호 해독을 활성화해야 합니다.

고급 ***URL*** 필터링 테스트 페이지에는 ***URL***에 '실시간 감지'가 포함되어 있고 방화벽이 올바르게 분류하고 있는지 확인합니다. 악성 ***URL***을 실시간으로 분석합니다. 다른 카테고리에 대한 방화벽 동작은 확인하지 않습니다.

***Palo Alto Networks URL*** 카테고리 조회 도구인 Test A Site를 이용하여 특정 웹사이트의 분류를 확인할 수 있습니다.

URL 필터링 구독에 해당하는 절차를 따르십시오.

- URL 필터링 확인
- Advanced URL 필터링 확인

## URL 필터링 확인

레거시 URL 필터링 구독이 있는 경우 방화벽이 사용자가 액세스하는 카테고리의 URL을 올바르게 분류, 적용 및 기록하는지 테스트하고 확인하십시오.

**STEP 1 |** 관심 있는 URL 카테고리의 웹사이트에 액세스합니다.

차단된 URL 카테고리에서 사이트를 테스트하는 것을 고려하십시오. 테스트 페이지(urlfiltering.paloaltonetworks.com/test-***<url-category>***)를 사용하여 사이트에 직접 액세스하지 않도록 할 수 있습니다. 예를 들어 맬웨어에 대한 차단 정책을 테스트하려면 https://urlfiltering.paloaltonetworks.com/test-malware를 방문하십시오.

**STEP 2 |** 트래픽 및 URL 필터링 로그(모니터 > 로그)를 검토하여 방화벽이 사이트를 올바르게 처리하는지 확인합니다.

예를 들어 누군가가 조직의 정책을 위반하는 사이트에 액세스할 때 표시되도록 차단 페이지를 구성한 경우 테스트 사이트를 방문할 때 해당 페이지가 표시되는지 확인합니다.

## Advanced URL 필터링 확인

고급 URL 필터링 구독이 있는 경우 실시간 URL 분석이 발생하는지 테스트하고 확인하십시오.


©2023 Palo Alto Networks, Inc.

*Palo Alto Networks*는 활성 ***URL*** 필터링 프로파일에 대해 경고하도록 실시간 감지 작업 설정을 설정할 것을 권장합니다. 이는 실시간으로 분석된 ***URL***에 대한 가시성을 제공하고 특정 웹 위협에 대해 구성된 카테고리 설정을 기반으로 차단(또는 정책 설정에 따라 허용)합니다.

방화벽은 지정된 ***URL***의 감지된 ***URL*** 카테고리에 대해 구성된 작업 중 가장 심각한 작업을 시행합니다. 예를 들어 ***example.com***이 실시간 감지, 명령 및 제어 및 쇼핑으로 분류되어 각각 경고, 차단 및 허용 작업이 구성된 카테고리라고 가정합니다. 차단은 탐지된 카테고리에서 가장 심각한 작업이기 때문에 방화벽은 ***URL***을 차단합니다.

**STEP 1 |** 다음 각 테스트 URL을 방문하여 Advanced URL 필터링 서비스가 URL을 올바르게 분류하는지 확인하십시오.

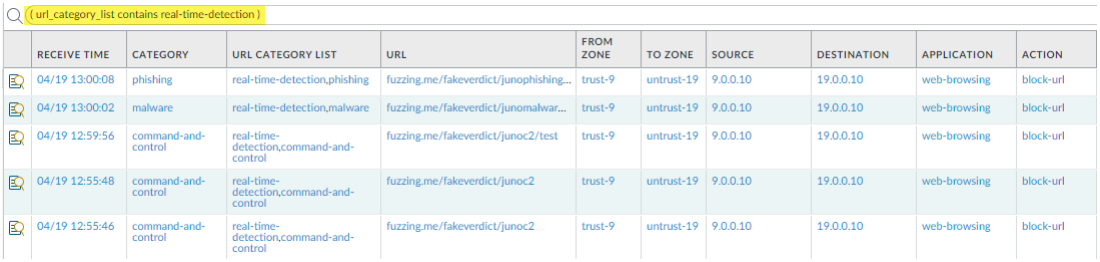
- **Malware** - urlfiltering.paloaltonetworks.com/test-real-time-detection-malware
- **Phishing** - urlfiltering.paloaltonetworks.com/test-real-time-detection-phishing
- **C2** - urlfiltering.paloaltonetworks.com/test-real-time-detection-command-and-control
- **Grayware** - urlfiltering.paloaltonetworks.com/test-real-time-detection-grayware
- **Benign (unknown)** - urlfiltering.paloaltonetworks.com/test-real-time-detection

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽에서 활동을 모니터링하여 테스트된 URL이 실시간 탐지로 적절하게 분류되었는지 확인합니다.

1. 모니터 > 로그 > **URL** 필터링을 선택하고 **(url_category_list가 실시간 감지 포함)**로 필터링하여 로그 보기 고급 URL 필터링을 사용하여 분석되었습니다.

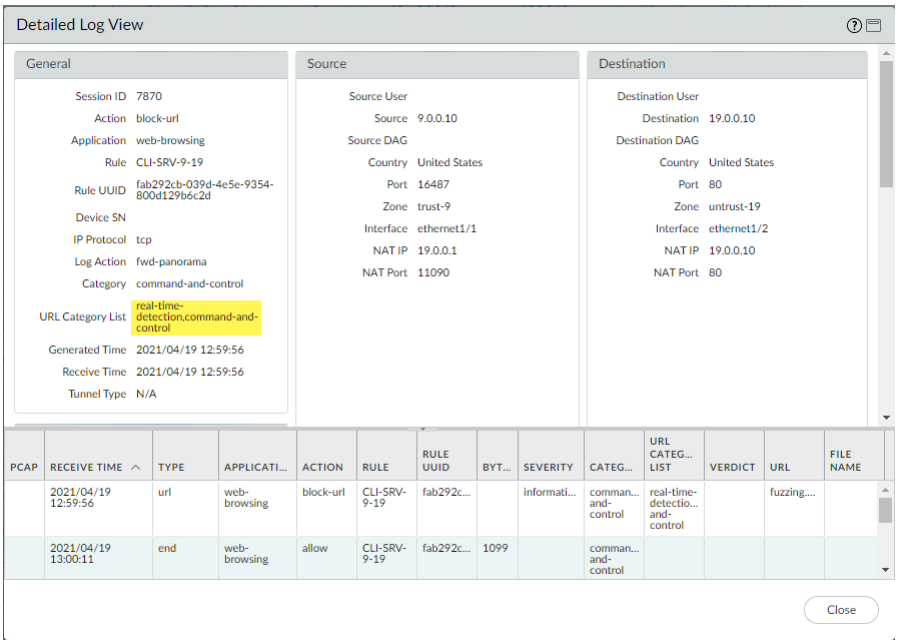
   추가 웹 페이지 카테고리 일치도 표시되며 PAN-DB에서 정의한 카테고리에 해당합니다.




| | RECEIVE TIME | CATEGORY | URL CATEGORY LIST | URL | FROM ZONE | TO ZONE | SOURCE | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|
| | 04/19 13:00:08 | phishing | real-time-detection,phishing | fuzzing.me/fakeverdict/junophishing... | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| | 04/19 13:00:02 | malware | real-time-detection,malware | fuzzing.me/fakeverdict/junomalwar... | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| | 04/19 12:59:56 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2/test | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| | 04/19 12:55:48 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2 | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| | 04/19 12:55:46 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2 | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |

2. 로그를 자세히 살펴보고 각 유형의 웹 위협이 올바르게 분석되고 분류되었는지 확인하십시오.

   다음 예에서 URL은 실시간으로 분석되었으며 이를 명령 및 제어(C2)로 정의하는 품질을 보유한 것으로 분류됩니다. C2 카테고리에는 실시간 감지(경고와 반대되는 차단)보다 더 심각한 관련 작업이 있기 때문에 URL은 명령 및 제어로 분류되고 차단됩니다.




 ©2023 Palo Alto Networks, Inc.

# 인라인 분류 설정

URL 필터링 인라인 분류 구성을 활성화하려면 인라인 분류 설정으로 구성된 URL 필터링 프로파일을 보안 정책 규칙에 연결합니다(기본 보안 정책 설정 참조).

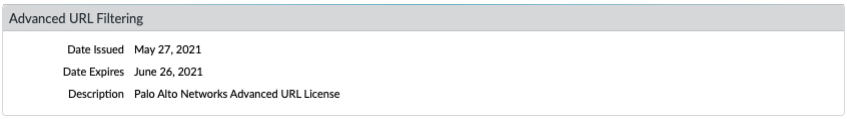
*URL* 필터링 로컬 인라인 분류는 현재 *VM-50* 또는 *VM50L* 가상 어플라이언스에서 지원되지 않습니다.

**STEP 1 |** PAN-OS 웹 인터페이스에 로그인합니다.

**STEP 2 |** 인라인 분류를 활용하려면 고급 URL 필터링이 활성화되어 있어야 합니다.

기존 *URL* 필터링 구독의 기존 보유자인 경우 로컬 인라인 분류를 활성화할 수 있습니다.

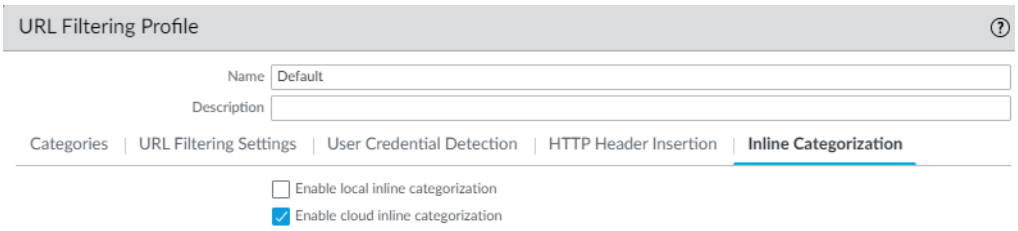
고급 URL 필터링 구독이 있는지 확인하십시오. 현재 활성화된 라이선스가 있는 구독을 확인하려면 디바이스 > 라이선스를 선택한 다음 적절한 라이선스가 표시되고 만료되지 않았는지 확인합니다.




**STEP 3 |** 새 URL 필터링 보안 프로파일을 업데이트하거나 생성하여 클라우드 인라인 분류를 활성화합니다.

로컬 및 클라우드 인라인 분류에 사용되는 정책 조치는 카테고리 탭에서 구성된 설정에 따라 달라집니다.

1. 기존 **URL** 필터링 프로파일을 선택하거나 새 프로파일을 추가합니다(개체 > 보안 프로파일 > **URL** 필터링).
2. URL 필터링 프로파일을 선택한 다음 인라인 분류로 이동하여 배포하려는 인라인 분류 방법을 활성화합니다.
   - 클라우드 인라인 분류 지원 - 의심스러운 웹 페이지 콘텐츠를 실시간으로 분석하여 표적 피싱 공격 및 고급 회피 기술을 사용하는 기타 웹 기반 공격을 비롯한 제로데이 웹 공격으로부터 사용자를 보호하는 클라우드 기반 인라인 딥 러닝 엔진입니다.
   - 로컬 인라인 분류 활성화 - 기계 학습 기술을 사용하는 방화벽 기반 탐지 엔진으로 웹 페이지에 포함된 JavaScript 익스플로이트 및 피싱 공격의 악의적인 변종을 방지합니다.




3. 확인을 클릭하여 URL 필터링 프로파일 구성 대화 상자를 종료하고 변경 사항을 커밋합니다.

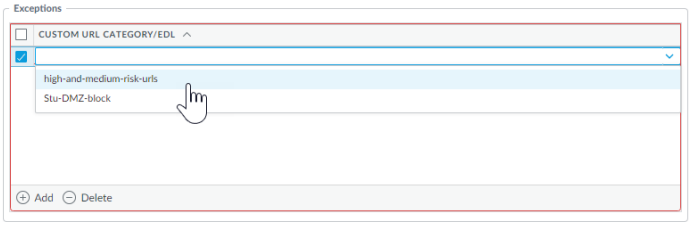

©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) 위양성(false-positive)이 발생하는 경우 URL 필터링 보안 프로파일에 URL 예외를 추가합니다. URL 필터링 프로파일에서 외부 동적 목록 또는 사용자 지정 URL 카테고리 목록을 지정하여 예외를 추가할 수 있습니다. 지정된 예외는 클라우드 및 로컬 인라인 분류에 모두 적용됩니다.

사용자 정의 ***URL*** 카테고리(개체 > 사용자 정의 개체 > ***URL*** 카테고리)에 항목을 추가하는 다른 메커니즘을 통해 생성된 ***URL*** 예외

인라인 분류에 대한 예외로 사용할 수도 있습니다.

1. 개체 > 보안 프로파일 > **URL** 필터링을 선택합니다.
2. 특정 URL을 제외할 URL 필터링 프로파일을 선택한 다음 인라인 분류를 선택합니다.
3. 기존 URL 기반 외부 동적 목록 또는 사용자 정의 URL 카테고리를 선택하려면 추가를 클릭하십시오. 사용할 수 있는 항목이 없으면 각각 새 외부 동적 목록 또는 맞춤 URL 카테고리를 만듭니다.




4. 확인을 클릭하여 URL 필터링 프로파일을 저장하고 변경 사항을 커밋합니다.

**STEP 5 |** (선택 사항) 인라인 분류 서비스 요청을 처리하기 위해 방화벽에서 사용하는 클라우드 콘텐츠 FQDN(정규화된 도메인 이름)을 설정합니다. 기본 FQDN은 hawkeye.services-edge.paloaltonetworks.com에 연결한 다음 가장 가까운 클라우드 서비스 서버로 확인합니다. 데이터 상주 및 성능 요구 사항을 가장 잘 충족하는 지역 클라우드 콘텐츠 서버를 지정하여 자동 서버 선택을 재정의할 수 있습니다.

클라우드 콘텐츠 ***FQDN***은 전역적으로 사용되는 리소스이며 이 연결에 의존하는 다른 서비스가 트래픽 페이로드를 보내는 방법에 영향을 줍니다.

방화벽이 올바른 Content Cloud FQDN을 사용하는지 확인합니다(디바이스**e** > 설정 > **Content-ID** > 콘텐츠 클라우드 설정). 필요한 경우 FQDN을 변경하십시오.

- US - **us.hawkeye.services-edge.paloaltonetworks.com**
- EU - **eu.hawkeye.services-edge.paloaltonetworks.com**
- UK - **uk.hawkeye.services-edge.paloaltonetworks.com**

  영국 기반의 클라우드 콘텐츠 ***FQDN***은 ***EU***에 위치한 백엔드 서비스*(eu.hawkeye.services-edge.paloaltonetworks.com)*에 연결하여 고급 *Threat Prevention* 인라인 클라우드 분석 서비스 지원을 제공합니다.
- APAC - **apac.hawkeye.services-edge.paloaltonetworks.com**


©2023 Palo Alto Networks, Inc.

**STEP 6 |** (선택 사항) 인라인 분류 서버에 대한 방화벽 연결 상태를 확인합니다.

1. ml.service.paloaltonetworks.com 서버는 클라우드 운영 및 로컬 인라인 분류와 관련된 방화벽 기반 구성 요소에 대한 주기적 업데이트를 제공합니다.

   방화벽에서 다음 CLI 명령을 사용하여 연결 상태를 확인합니다.

   ```
   mlav 클라우드 상태 보기
   ```

   예:

   ```
   show mlav cloud-status MLAV cloud Current cloud server:
    ml.service.paloaltonetworks.com Cloud connection: connected
   ```

   인라인 ML 클라우드 서비스에 연결할 수 없는 경우 ml.service.paloaltonetworks.com 도메인이 차단되지 않았는지 확인하십시오.

2. hawkeye.services-edge.paloaltonetworks.com 서버는 클라우드 인라인 분류에서 서비스 요청을 처리하는 데 사용됩니다.

   방화벽에서 다음 CLI 명령을 사용하여 연결 상태를 확인합니다.

   ```
   show ctd-agent status security-client
   ```

   예:

   ```
   show ctd-agent status security-client ... Security
    Client AceMlc2(1) 현재 클라우드 서버: hawkeye.services-
   edge.paloaltonetworks.com Cloud connection: connected ...
   ```

   *CLI* 출력은 간결함을 위해 간략하게 표시되었습니다.

   고급 URL 필터링 클라우드 서비스에 연결할 수 없는 경우 hawkeye.services-edge.paloaltonetworks.com 도메인이 차단되지 않았는지 확인하십시오.

**STEP 7 |** 고급 URL 필터링 클라우드 서비스에 인증하는 데 사용되는 업데이트된 방화벽 디바이스 인증서를 설치합니다. 클라우드 인라인 분류가 활성화된 모든 방화벽에 대해 이 과정을 반복합니다.

**STEP 8 |** (선택 사항 - 클라우드 분류만 해당) 다음 테스트 URL을 방문하여 고급 URL 필터링 서비스가 클라우드 인라인 분류로 감지된 URL을 올바르게 분류하고 있는지 확인하십시오.

- **Malware** - urlfiltering.paloaltonetworks.com/query-real-time-content-detection-malware
- **Phishing** - urlfiltering.paloaltonetworks.com/query-real-time-content-detection-phishing
- **C2** - urlfiltering.paloaltonetworks.com/query-real-time-content-detection-command-and-control
- **Grayware** - urlfiltering.paloaltonetworks.com/query-real-time-content-detection-grayware

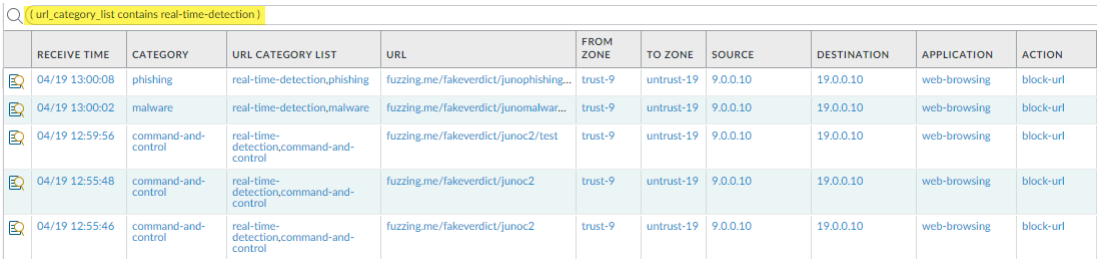

©2023 Palo Alto Networks, Inc.

**STEP 9 |** (선택 사항) 방화벽에서 활동을 모니터링하여 테스트된 URL이 실시간 탐지로 적절하게 분류되었는지 확인합니다.

실시간 감지로 분류된 ***URL***에는 로컬 인라인 분류 ***(URL*** 필터링 인라인 ***ML)*** 와 클라우드 인라인 분류로 분석된 콘텐츠가 포함됩니다.

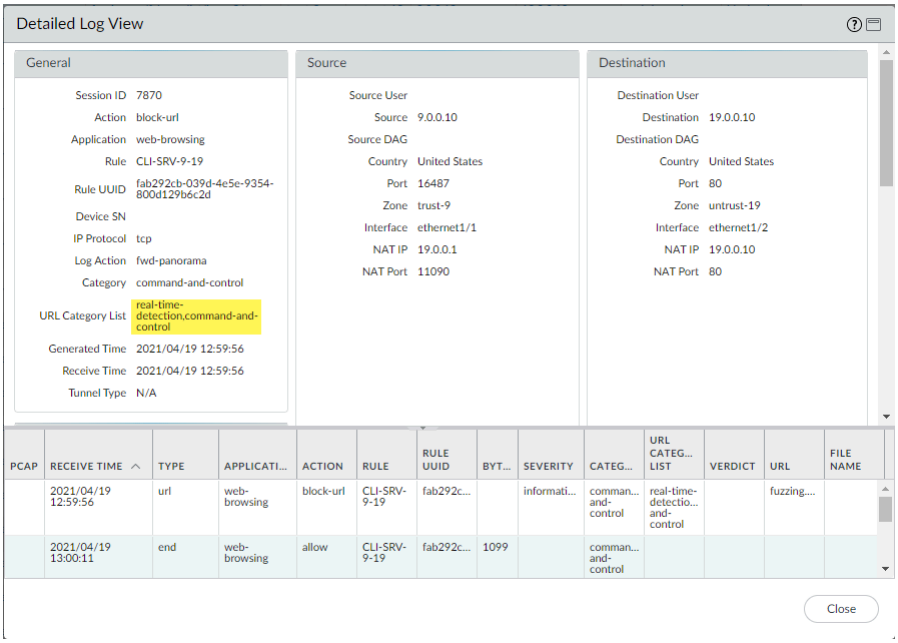
1. 모니터 > 로그 > **URL** 필터링을 선택하고 **(url_category_list가 실시간 감지 포함)**로 필터링하여 로그 보기 고급 URL 필터링을 사용하여 분석되었습니다.

   추가 웹 페이지 카테고리 일치도 표시되며 PAN-DB에서 정의한 카테고리에 해당합니다.



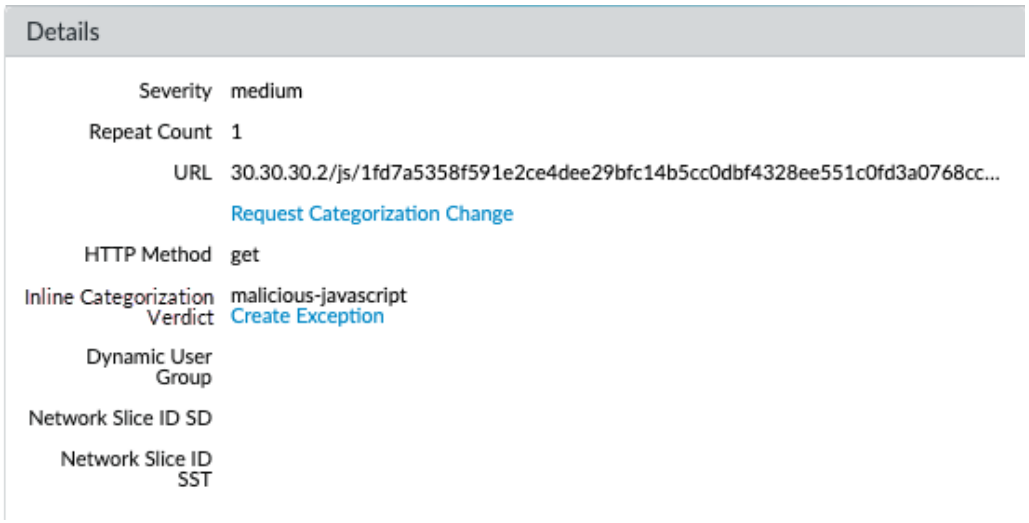

2. 로그를 자세히 살펴보고 각 유형의 웹 위협이 올바르게 분석되고 분류되었는지 확인하십시오.

   다음 예에서 URL은 실시간으로 분석되었으며 이를 명령 및 제어(C2)로 정의하는 품질을 보유한 것으로 분류됩니다. C2 카테고리에는 실시간 감지(경고와 반대되는 차단)보다 더 심각한 관련 작업이 있기 때문에 URL은 명령 및 제어로 분류되고 차단됩니다.




3. **Inline Categorization Verdict**은 상세 로그 보기의 **Details** 창 아래에 표시됩니다. 로컬 인라인 분류에 의해 위협을 포함하는 것으로 결정된 웹 페이지는 피싱 또는 **malicious-javascript** 판정으로 분류됩니다. 클라우드 인라인 분류 판정은 **cloud**로 표시됩니다.


©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

# 웹 활동 모니터링

ACC, URL 필터링 로그 및 보고서는 경고, 차단, 계속 또는 재정의로 설정된 URL 카테고리에 대한 모든 사용자 웹 활동을 표시합니다. 로그를 모니터링하면 사용자 기반의 웹 활동을 더 잘 이해하여 웹 액세스 정책을 결정할 수 있습니다.

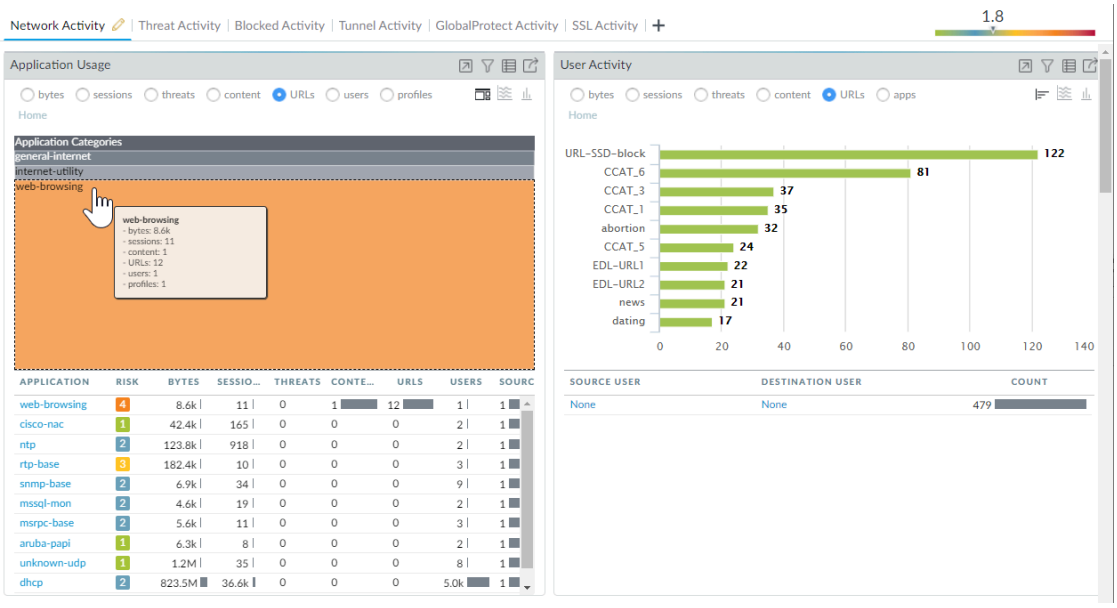
다음 항목에서는 웹 활동을 모니터링하는 방법에 대해 설명합니다.

- 네트워크 사용자의 웹 활동 모니터링
- 사용자 활동 보고서 보기
- 사용자 지정 URL 필터링 보고서 구성

## 네트워크 사용자의 웹 활동 모니터링

방화벽에서 생성된 ACC(애플리케이션 명령 센터), URL 필터링 보고서 및 로그를 사용하여 사용자 활동을 추적할 수 있습니다.

- 사용자 환경에서 사용자가 액세스하는 가장 일반적인 카테고리의 빠른 보기를 보려면 **ACC** 위젯을 확인하십시오. 대부분의 네트워크 활동 위젯을 사용하면 URL을 정렬할 수 있습니다. 예를 들어 애플리케이션 사용량 위젯에서 네트워킹 카테고리가 가장 많이 액세스되는 카테고리이고 그 뒤에는 암호화된 터널과 ssl이 차례로 표시됩니다. URL을 기준으로 정렬된 위협 활동 및 차단된 활동 목록을 볼 수도 있습니다.




로그 보기 및 로그 옵션 구성:


©2023 Palo Alto Networks, Inc.

- ACC에서 로그로 바로 이동하거나( ) 모니터 > 로그 > **URL** 필터링을 선택할 수 있습니다.

  각 항목에 대한 로그 작업은 해당 카테고리에 대해 정의한 사이트 액세스 설정에 따라 다릅니다.

  - 경고 로그 - 이 예에서는 컴퓨터 및 인터넷 정보 카테고리가 경보로 설정되어 있습니다.

| | RECEIVE TIME | CATEGORY | URL | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2020/04/16 14:10:53 | computer-and-internet-info | outlook.office36... | pm wifi | UNTRUST | [redacted] | [redacted] | [redacted] | outlook-web-online | alert |

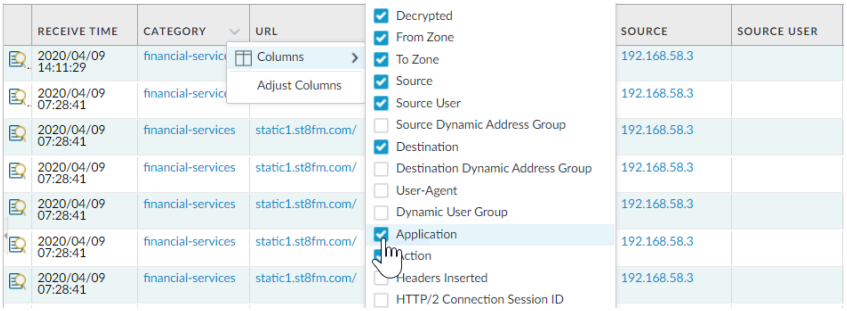
  - 로그 차단 - 이 예에서는 불충분한 컨텐츠 카테고리가 계속되도록 설정되어 있습니다. 카테고리가 대신 차단으로 설정된 경우 로그 작업은 차단 URL이 됩니다.

| | RECEIVE TIME | CATEGORY | URL | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2020/04/08 18:47:49 | insufficient-content | munchkin.mark... | pm wifi | UNTRUST | [redacted] | [redacted] | [redacted] | ssl | block-continue |

  - 암호화된 웹사이트의 경보 로그 - 이 예에서 카테고리는 private-ip-address이고 애플리케이션은 웹 브라우징입니다. 또한 이 로그는 방화벽이 이 트래픽의 암호를 복호화했음을 나타냅니다.

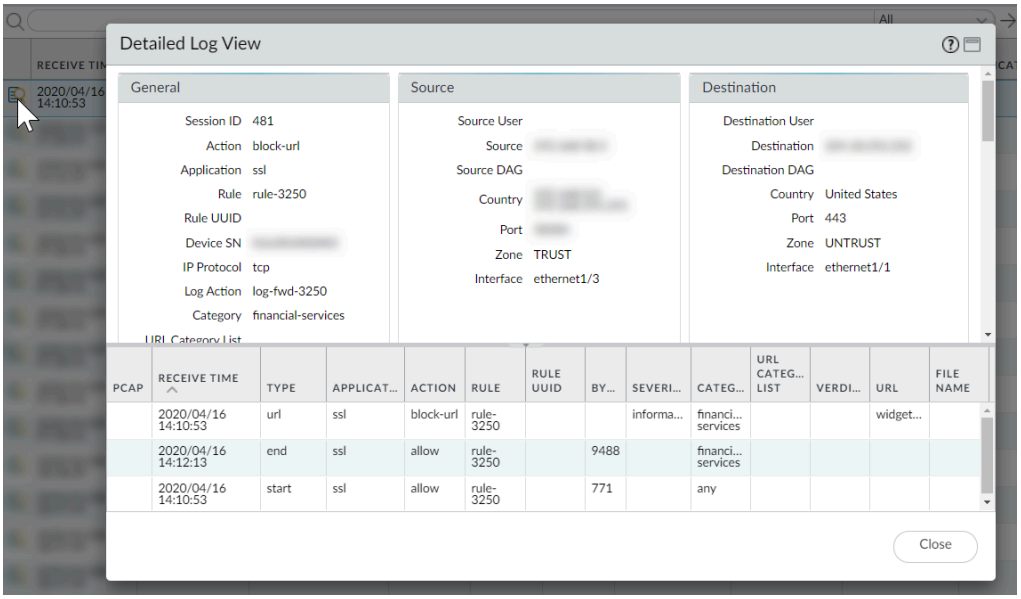
| | RECEIVE TIME | CATEGORY | URL | DECRYPTED | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2020/04/09 14:11:29 | private-ip-addresses | [redacted]/Updates/Updat... | yes | TRUST | UNTRUST | 192.168.58.3 | [redacted] | [redacted] | web-browsing | alert |

- URL 필터링 로그 보기에 영역 간 및 보낸 사람, 콘텐츠 유형, 패킷 캡처 수행 여부 등 여러 열을 추가할 수도 있습니다. 표시할 열을 수정하려면 열에서 아래쪽 화살표를 클릭하고 표시할 속성을 선택합니다.



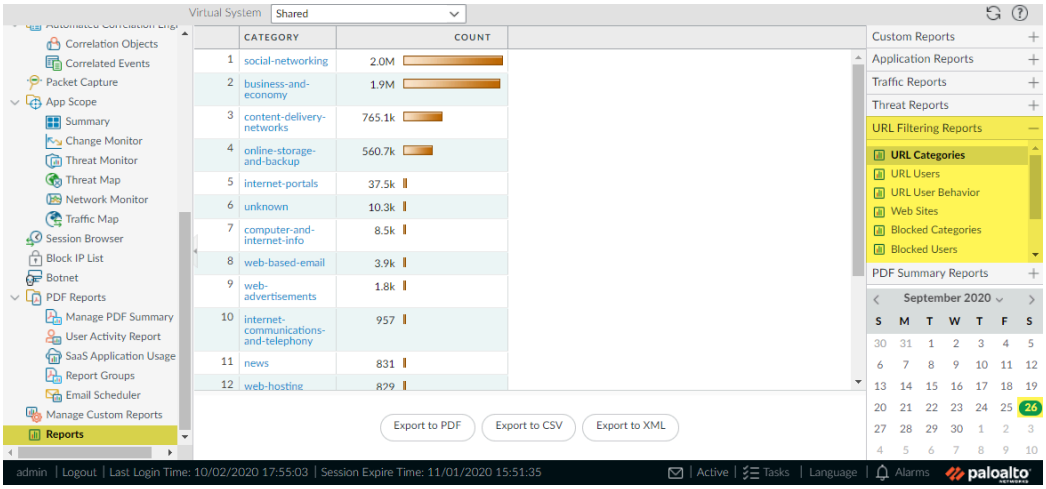

 ©2023 Palo Alto Networks, Inc.

- 전체 로그 세부 정보를 보거나 액세스한 URL에 대한 카테고리 변경을 요청하려면 로그의 첫 번째 열에 있는 로그 세부 정보 아이콘을 클릭합니다.




- URL 카테고리, URL 사용자, 액세스한 웹사이트, 차단된 카테고리 등에 대한 사전 정의된 URL 필터링 보고서를 생성합니다.

  보고서 > 모니터링을 선택한 다음 **URL** 필터링 보고서 섹션에서 보고서 중 하나를 선택합니다. 보고서는 달력에서 선택한 날짜의 24시간 기간을 다룹니다. 보고서를 PDF, CSV 또는 XML로 내보낼 수도 있습니다.




# 사용자 활동 보고서 보기

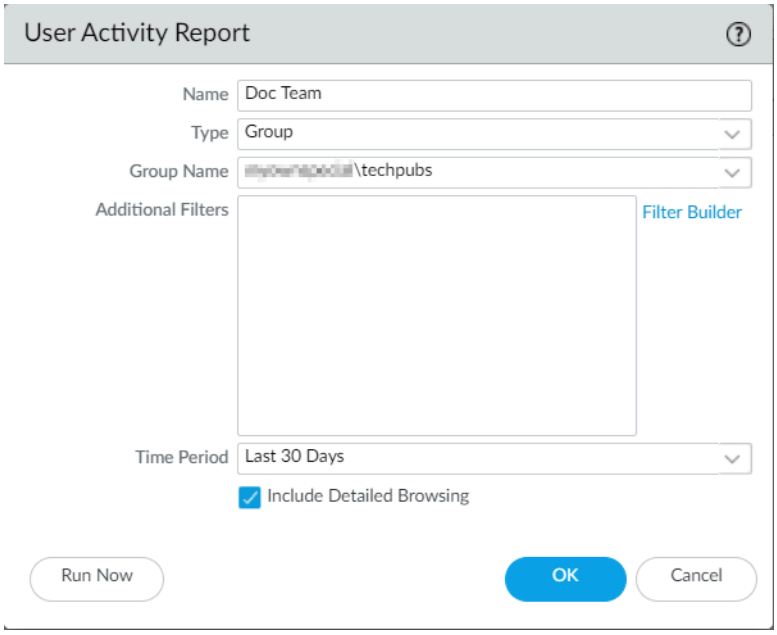
이 보고서는 사용자 또는 그룹 활동을 빠르게 보는 방법을 제공하며 검색 시간 활동을 볼 수 있는 옵션도 제공합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 사용자 활동 보고서를 구성합니다.

1. 모니터 > **PDF** 보고서 > 사용자 활동 보고서를 선택합니다.
2. 보고서를 추가하고 이름을 입력합니다.
3. 보고서 유형을 선택합니다.
   - 사용자를 선택하여 한 사람에 대한 보고서를 생성합니다.
   - 사용자 그룹에 대한 그룹을 선택합니다.

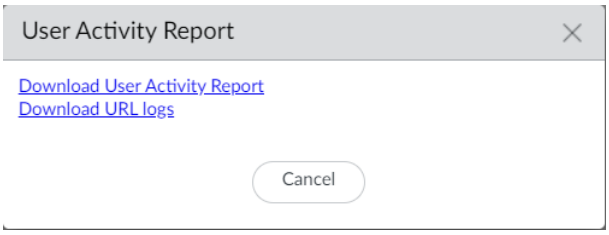
   사용자 또는 그룹 이름을 선택할 수 있도록 User-ID를 사용하도록 설정해야 합니다. ***User-ID***가 구성되지 않은 경우 사용자 유형을 선택한 다음 사용자 컴퓨터의 ***IP*** 주소를 입력할 수 있습니다.
4. 사용자 보고서에 대한 사용자 이름**/IP** 주소를 입력하거나 사용자 그룹 보고서에 대한 그룹 이름을 입력합니다.
5. 기간을 선택합니다. 기존 기간을 선택하거나사용자 지정을 선택할 수 있습니다.
6. 자세한 브라우징 포함 체크박스를 선택하므로 브라우징 정보가 보고서에 포함되어 있습니다.




 ©2023 Palo Alto Networks, Inc.

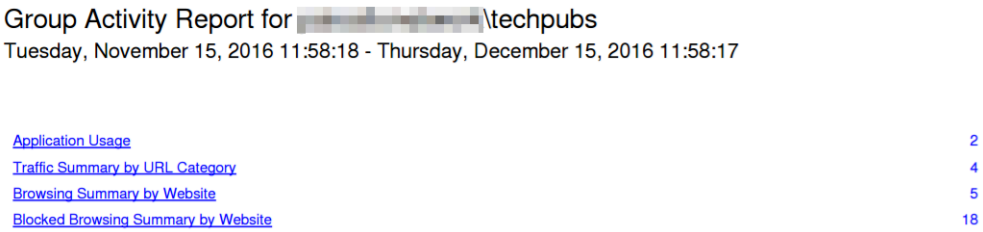
**STEP 2 |** 보고서를 실행합니다.

1. 지금 실행을 클릭합니다.
2. 방화벽이 보고서 생성을 완료하면 링크 중 하나를 클릭하여 다운로드합니다.
   - 사용자 활동 보고서 다운로드를 클릭하여 보고서의 PDF 버전을 다운로드합니다.
   - **URL** 로그 다운로드를 클릭하여 해당 로그 항목의 CSV 파일을 다운로드합니다.

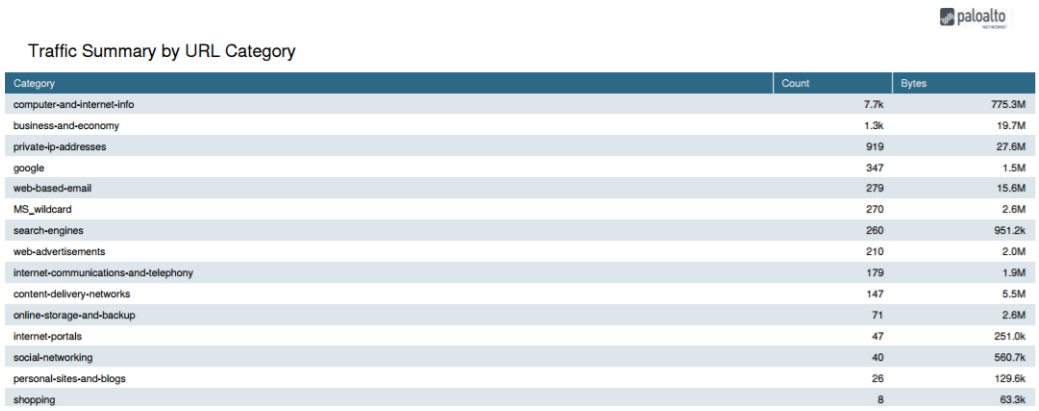



3. 보고서를 다운로드한 후취소를 클릭합니다.
4. 나중에 동일한 보고서를 다시 실행할 수 있도록 사용자 활동 보고서 설정을 저장하려면 확인을 클릭하십시오. 그렇지 않으면 취소를 클릭합니다.

**STEP 3 |** 다운로드한 파일을 열어 사용자 활동 보고서를 봅니다. 보고서의 PDF 버전에는 보고서를 기반으로 하는 사용자 또는 그룹, 보고서 시간 프레임 및 콘텐츠 테이블이 표시됩니다.




**STEP 4 |** 내용 표의 항목을 클릭하여 보고서 세부 정보를 봅니다. 예를 들어 **URL** 카테고리별로 트래픽 요약을 클릭하여 선택한 사용자 또는 그룹에 대한 통계를 봅니다.




| Category | Count | Bytes |
|---|---|---|
| computer-and-internet-info | 7.7k | 775.3M |
| business-and-economy | 1.3k | 19.7M |
| private-ip-addresses | 919 | 27.6M |
| google | 347 | 1.5M |
| web-based-email | 279 | 15.6M |
| MS_wildcard | 270 | 2.6M |
| search-engines | 260 | 951.2k |
| web-advertisements | 210 | 2.0M |
| internet-communications-and-telephony | 179 | 1.9M |
| content-delivery-networks | 147 | 5.5M |
| online-storage-and-backup | 71 | 2.6M |
| internet-portals | 47 | 251.0k |
| social-networking | 40 | 560.7k |
| personal-sites-and-blogs | 26 | 129.6k |
| shopping | 8 | 63.3k |

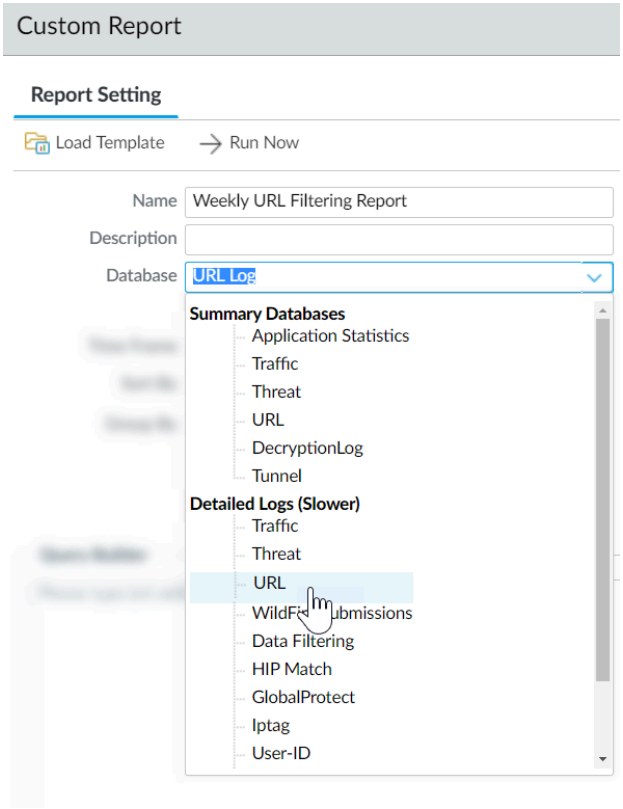
## 사용자 지정 URL 필터링 보고서 구성

정기적으로 실행하도록 예약할 수 있는 자세한 보고서를 생성하려면 사용자 지정 URL 필터링 보고서를 구성합니다. 보고서를 기반으로 하는 URL 필터링 로그 필드의 조합을 선택할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 새 맞춤 리포트를 추가합니다.

1. 모니터 > 맞춤 리포트 관리를 선택한 다음 보고서를 추가합니다.
2. 보고서에 고유한 이름을 지정하고 선택적으로 설명을 제공합니다.
3. 보고서를 생성하는 데 사용할 데이터베이스를 선택합니다. 상세 URL 필터링 보고서를 생성하려면 상세 로그 섹션에서 **URL**을 선택합니다.

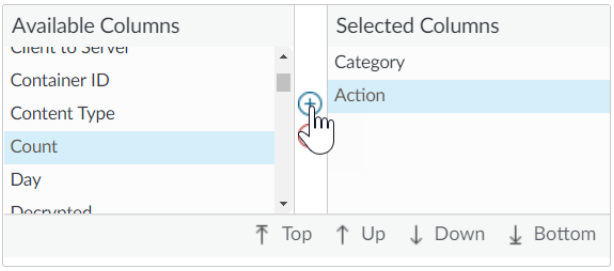




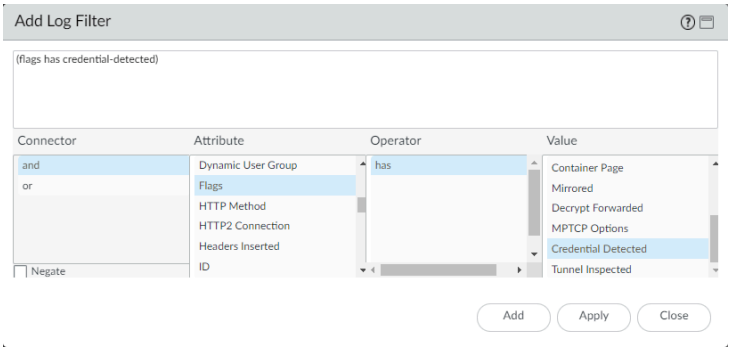
©2023 Palo Alto Networks, Inc.

**STEP 2 |** 보고서 옵션을 구성합니다.

1. 미리 정의된 시간 프레임을 선택하거나 사용자 지정을 선택합니다.
2. 사용 가능한 열 목록에서 보고서에 포함할 로그 열을 선택하여 선택한 열에(⊕) 추가합니다. 예를 들어 URL 필터링 보고서의 경우 다음을 선택할 수 있습니다.
   - 동작
   - 앱 카테고리
   - 카테고리
   - 대상 국가
   - 소스 사용자
   - URL



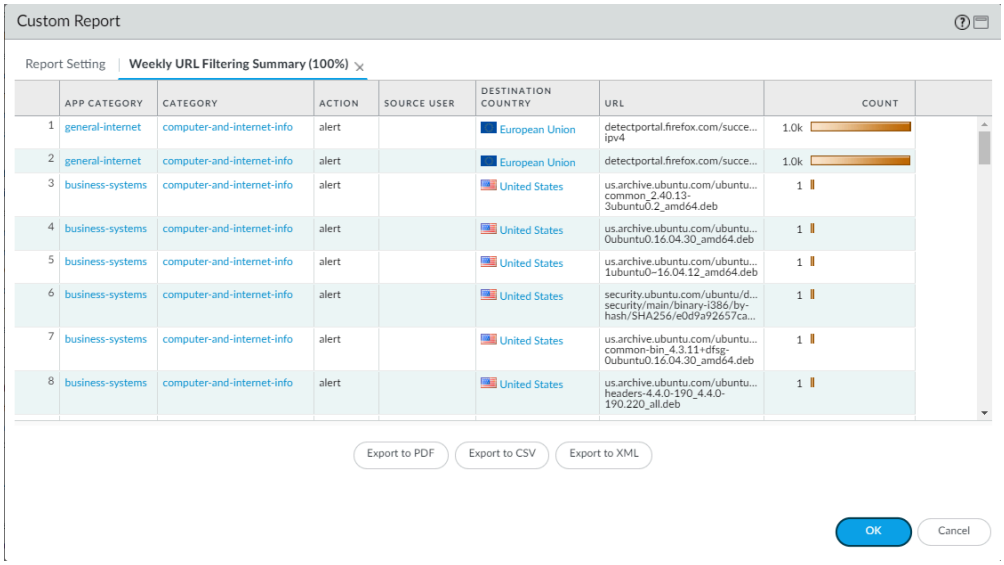

3. 방화벽이 자격 증명 피싱을 방지하도록 설정되어 있는 경우, 사용자가 사이트에 유효한 회사 자격 증명을 제출할 때 기록되는 이벤트에 포함하도록 속성 플래그, 운영자가 있는 속성 플래그 및 값 자격 증명을 선택합니다.




4. (선택 사항) 보고서 세부 정보를 집계하는 데 사용할 특성을 설정하는 정렬별 옵션을 선택합니다. 정렬할 특성을 선택하지 않으면 보고서는 집계 없이 첫 번째 N 결과 수를 반환합니다. 그룹


©2023 Palo Alto Networks, Inc.

별 특성을 선택하여 데이터 그룹화의 앵커로 사용합니다. 다음 예는 그룹화 기준이 앱 카테고리로 설정되고 정렬 기준이 상위 **5**개의 개수로 설정된 보고서를 보여줍니다.




**STEP 3 |** 보고서를 실행합니다.

1. 지금 실행 아이콘을 클릭하여 새 탭에서 열리는 보고서를 즉시 생성합니다.
2. 보고서 검토를 완료하면 보고서 설정 탭으로 돌아가 설정을 조정하고 보고서를 다시 실행하거나 다음 단계로 계속 하여 보고서를 예약합니다.
3. 스케줄 체크박스를 선택하여 하루에 한 번 보고서를 실행합니다. 이렇게 하면 지난 24시간 동안 웹 활동에 대해 자세히 설명하는 일일 보고서가 생성됩니다.

**STEP 4 |** 구성을 커밋합니다.

**STEP 5 |** 맞춤 리포트를 봅니다.

1. 모니터 > 보고서를 선택합니다.
2. 올바른 열에서 맞춤 리포트 창을 확장하고 보고 싶은 보고서를 선택합니다. 최신 보고서가 자동으로 표시됩니다.
3. 이전 날짜에 대한 보고서를 보려면 달력에서 날짜를 선택합니다. 보고서를 PDF, CSV 또는 XML로 내보낼 수도 있습니다.


©2023 Palo Alto Networks, Inc.

# 사용자가 방문한 페이지만 기록

컨테이너 페이지는 사용자가 웹사이트를 방문할 때 액세스하는 기본 페이지이지만 추가 페이지는 기본 페이지와 함께 로드될 수 있습니다. URL 필터링 프로파일(개체 > 보안 프로파일 > **URL** 필터링)에서 로그 컨테이너 페이지만 옵션이 활성화된 경우, 기본 컨테이너 페이지만 기록되고 컨테이너 페이지 내에서 로드될 수 있는 후속 페이지는 기록되지 않습니다. URL 필터링은 잠재적으로 많은 로그 항목을 생성할 수 있으므로 요청된 페이지 파일 이름이 특정 MIME 유형과 일치하는 URI만 로그 항목에 포함되도록 이 옵션을 설정할 수 있습니다. 기본 세트에는 다음과 같은 mime-유형이 포함됩니다.

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml



컨테이너 페이지만 기록 옵션을 사용하도록 설정하는 경우 바이러스 백신 또는 취약점 보호에서 탐지된 위협에 대한 상호 연관된 ***URL*** 로그 항목이 항상 있는 것은 아닙니다.


©2023 Palo Alto Networks, Inc.

# 사용자 지정 URL 카테고리 생성

사용자 지정 URL 필터링 개체를 만들어 URL 카테고리 적용에 대한 예외를 지정하고 여러 URL 카테고리에 따라 사용자 지정 URL 카테고리를 만들 수 있습니다.

- **URL** 카테고리 적용에 대한 예외 정의 - 보안 정책 규칙에서 일치 기준으로 사용할 URL의 사용자 지정 목록 생성입니다. 이는 URL 카테고리에 예외를 지정하는 좋은 방법입니다. 예를 들어, **소셜 네트워킹** 카테고리를 차단하지만 LinkedIn에 대한 액세스는 허용하고 싶을 수 있습니다.
- 여러 **PAN-DB** 카테고리를 기반으로 사용자지정 URL 카테고리를 정의합니다.이경우 카테고리 집합과 일치하는 웹사이트에 대한 적용을 타겟팅할 수 있습니다. 웹사이트 또는 페이지는 사용자 지정 카테고리의 일부로 정의된 모든 카테고리와 일치해야 합니다.

  예를 들어, PAN-DB는 엔지니어가 연구에 사용하는 개발자 블로그를**개인 사이트 및 블로그**,**컴퓨터 및 인터넷 정보**및**고위험** 으로분류할 수 있습니다. 엔지니어가 블로그 및 유사한 웹 사이트에 액세스하고 이러한 웹 사이트에 대한 가시성을 확보할 수 있도록 세 가지 카테고리를 기반으로 사용자 지정 URL 카테고리를 만들고 URL 필터링 프로파일에서 경고하도록 카테고리에 대한 사이트 액세스를 설정할 수 있습니다.

다음 단계를 수행하여 사용자 지정 URL 카테고리를 생성하고 방화벽을 사용하여 사용자 지정 URL 카테고리를 적용하는 방법을 정의합니다.

**STEP 1 |** 개체 > 사용자 정의 개체 > **URL** 카테고리를 선택합니다.

**STEP 2 |** 맞춤 URL 카테고리를 추가하거나 수정하고 카테고리에 설명이 포함된 이름을 지정합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 카테고리 유형을 카테고리 일치 또는 **URL** 목록으로 설정합니다.

- **URL** 목록 - 적용할 URL 카테고리와 다르게 적용할 URL을 추가합니다. 이 목록 유형을 사용하여 URL 카테고리 적용에 대한 예외를 정의하거나 URL 목록을 사용자 지정 카테고리에 속하는 것으로 정의합니다. URL 목록 항목 생성에 대한 지침은 URL 카테고리 예외를 참조하십시오.

  기본적으로 방화벽은 후행 슬래시 또는 별표(*)로 끝나지 않는 도메인 항목(***example.com***)에 후행 슬래시(/)를 자동으로 추가합니다. 후행 슬래시는 방화벽이 도메인 오른쪽에 암시적 별표를 가정하는 것을 방지합니다. 와일드카드가 아닌 도메인 항목에서 후행 슬래시 제한은 지정된 도메인 및 해당 하위 디렉터리와 일치합니다. 예를 들어, ***example.com***(처리 후 ***example.com/***)은 자체 및 ***example.com/search***와 일치합니다.

  와일드카드 도메인 항목(별표 또는 캐럿이 있는 항목)에서 후행 슬래시 제한은 지정된 패턴을 준수하는 *URL*과 일치합니다. 예를 들어, ***.example.com**항목과 일치시키려면 *URL*이 하나 이상의 하위 도메인으로 엄격하게 시작하고 루트 도메인인 ***example.com***으로 끝나야 합니다. ***news.example.com***은 일치하지만 ***example.com***은 하위 도메인이 없기 때문에 일치하지 않습니다.

  *URL* 목록을 검사하는 모든 사람을 위해 항목의 의도된 일치 동작을 명확히 하기 위해 후행 슬래시를 수동으로 추가하는 것이 좋습니다. 후행 슬래시는 방화벽에 의해 추가되면 보이지 않습니다. URL 카테고리 예외에서는 후행 슬래시 및 일치 동작에 대해 자세히 설명합니다.

  이 기능을 비활성화하려면 디바이스 > 설정 > 콘텐츠-***ID*** > ***URL*** 필터링으로 이동합니다. 그런 다음 종료 토큰 추가를 선택 취소합니다. 이 기능을 비활성화하면 의도한 것보다 더 많은 *URL*에 대한 액세스를 차단하거나 허용할 수 있습니다. URL 카테고리 예외(*PAN-OS 10.1* 이하)는 이 기능이 비활성화되었을 때의 방화벽 동작을 설명합니다.

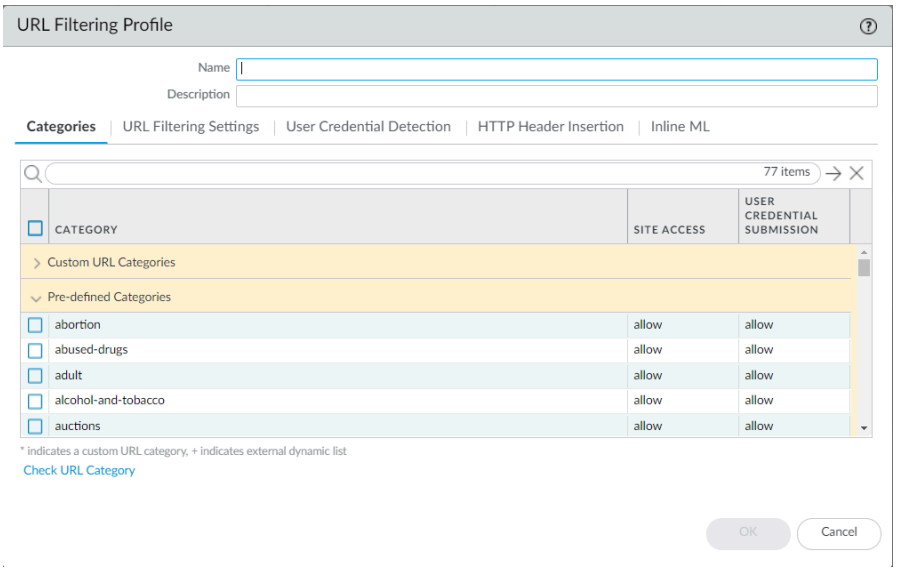
- 카테고리 일치 - 카테고리 집합과 일치하는 웹사이트에 대한 타겟 적용을 제공합니다. 웹사이트 또는 페이지는 맞춤 카테고리에 정의된 모든 카테고리와 일치해야 합니다.

**STEP 4 |** 확인을 선택하여 사용자 지정 URL 카테고리를 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 개체 > 보안 프로파일 > **URL** 필터링 및 추가를 선택하거나 URL 필터링 프로파일을 수정합니다.

사용자 정의 **URL** 카테고리 아래에 새 사용자 정의 카테고리가 표시됩니다.




**STEP 6 |** 맞춤 URL 카테고리에 대해 사이트 액세스 및 사용자 자격 증명 제출을 적용할 방법을 결정합니다. (사용자가 회사 자격 증명을 제출할 수 있는 사이트를 제어하려면 자격 증명 피싱 방지를 참조하십시오.)

**STEP 7 |** URL 필터링 프로파일을 보안 정책 규칙에 연결하여 해당 규칙과 일치하는 트래픽을 적용합니다.

정책 > 보안 > 작업을 선택한 다음 방금 업데이트한 URL 필터링 프로파일을 기반으로 트래픽을 적용하려면 보안 정책 규칙을 지정합니다. 변경 사항을 커밋해야 합니다.

사용자 지정 ***URL*** 카테고리를 보안 정책 규칙 일치 기준으로 사용할 수도 있습니다. 이 경우 ***URL*** 필터링 프로파일에서 ***URL*** 카테고리에 대한 사이트 액세스를 정의하지 않습니다. 사용자 지정 카테고리를 만든 후 사용자 지정 ***URL*** 카테고리를 추가할 보안 정책 규칙(정책 > 보안)으로 이동합니다. 서비스/***URL*** 카테고리를 선택하여 사용자 지정 ***URL*** 카테고리를 규칙의 일치 기준으로 사용합니다.


©2023 Palo Alto Networks, Inc.

# URL 카테고리 예외

URL 카테고리 시행에서 특정 웹사이트를 제외하여 해당 URL 카테고리와 관련된 정책 작업에 관계없이 이러한 웹사이트가 차단되거나 허용되도록 할 수 있습니다. 예를 들어 소셜 네트워킹 URL 카테고리는 차단하지만 LinkedIn에 대한 액세스는 허용할 수 있습니다. URL 카테고리 정책 시행에 대한 예외를 생성하려면 다음을 따릅니다.

- 차단하거나 허용하려는 사이트의 IP 주소 또는 URL을 맞춤 URL 카테고리 유형의 **URL** 목록(개체 > 맞춤 개체 > **URL** 카테고리). 그런 다음 URL 필터링 프로파일에서 카테고리에 대한 사이트 액세스를 정의합니다. 마지막으로 프로파일을 보안 정책 규칙에 연결합니다.

  맞춤 ***URL*** 카테고리를 보안 정책 규칙의 일치 기준으로 사용할 수도 있습니다**.(**정책 **>** 보안을 선택하고 서비스***/URL*** 카테고리 선택**).** ***URL*** 예외가 속한 카테고리를 차단하거나 허용하는 규칙 위에 예외 규칙을 배치해야 합니다**.**

- 차단하거나 허용하려는 사이트의 URL을 **URL** 목록 유형의 외부 동적 목록에 추가합니다.(개체 > 외부 동적 목록). 그런 다음 URL 필터링 프로파일의 외부 동적 목록을 사용하거나 보안 정책 규칙의 일치 기준으로 사용합니다. 외부 동적 목록을 사용할 때의 이점은 방화벽에서 구성 변경 또는 커밋을 수행하지 않고 목록을 업데이트할 수 있다는 것입니다.

  ***URL*** 목록 유형의 외부 동적 목록을 도메인 목록 또는 IP 주소 유형의 외부 동적 목록과 혼동해서는 안 됩니다**.** ***URL***의 외부 동적 목록은 도메인 및 ***IP*** 주소를 허용하지만 그 반대는 사실이 아니며 잘못된 항목이 생성됩니다**.**

다음 지침에서는 URL 카테고리 예외 목록(사용자 지정 URL 카테고리 또는 외부 동적 URL 목록)을 채우는 방법에 대해 설명합니다.

- URL 카테고리 예외 목록에 대한 기본 지침
- URL 카테고리 예외 목록에 대한 와일드카드 지침
- URL 카테고리 예외 목록 - 예시

## URL 카테고리 예외 목록에 대한 기본 지침

URL 카테고리 예외 목록에 항목을 추가하기 전에 항목이 가질 수 있는 잠재적인 일치 항목을 고려하십시오. 다음 지침에서는 의도한 웹 사이트 및 페이지를 차단하거나 허용하는 항목을 만드는 방법을 지정합니다.


©2023 Palo Alto Networks, Inc.

기본적으로 방화벽은 후행 슬래시(/) 또는 별표(*)로 끝나지 않는 도메인 항목에 후행 슬래시(/)를 자동으로 추가합니다. 후행 슬래시를 추가하면 방화벽이 일치 항목으로 간주하고 정책을 적용하는 URL이 변경됩니다. 와일드카드가 아닌 도메인 항목에서 후행 슬래시 제한은 지정된 도메인 및 해당 하위 디렉터리와 일치합니다. 예를 들어, **example.com**(처리 후 **example.com/**)은 자체 및 **example.com/search**와 일치합니다.

와일드카드 도메인 항목(별표 또는 캐럿이 있는 항목)에서 후행 슬래시 제한은 지정된 패턴을 준수하는 URL과 일치합니다. 예를 들어, ***.example.com** 항목과 일치시키려면 URL에 하나 이상의 하위 도메인이 포함되어야 하고 루트 도메인인 **example.com**으로 끝나야 합니다. 패턴: **<subdomain>.example.com**; **news.example.com**은 일치하지만 **example.com**은 하위 도메인이 없기 때문에 일치하지 않습니다.

후행 슬래시를 수동으로 추가하여 항목을 검사하는 모든 사용자가 항목의 의도된 일치 동작을 명확히 하는 것이 좋습니다. 후행 슬래시는 방화벽에 의해 추가될 때 보이지 않습니다.

PAN-OS® 10.2를 실행하는 Panorama™ 관리 서버는 동일한 소프트웨어 버전의 방화벽에 대해서만 이 기능을 활성화할 수 있습니다. PAN-OS 10.1 이하를 실행하는 방화벽에 대해 이 기능을 활성화하려면 각 방화벽에서

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA-850# commit
```

CLI 명령을 사용하십시오.

이 기능을 비활성화하려면 디바이스 > 설정 > 콘텐츠-ID > URL 필터링을 선택합니다. 그런 다음 종료 토큰 추가를 선택 취소합니다. 그러나 이 기능을 사용하지 않도록 설정하면 예상보다 많은 URL에 대한 액세스를 차단하거나 허용할 수 있습니다. 방화벽은 / 또는 *로 끝나지 않는 도메인 항목의 끝에 암시적 별표를 추가합니다. 예를 들어 허용된 웹사이트의 URL 목록에 **example.com**을 추가하면 방화벽은 해당 항목을 **example.com.***로 해석합니다. 결과적으로 방화벽은 **example.com.domain.xyz**와 같은 사이트에 대한 액세스를 허용합니다. URL 카테고리 예외(PAN-OS 10.1 이하)는 이 기능을 비활성화할 때 방화벽의 동작을 설명합니다.

- 목록 항목은 대/소문자를 구분하지 않습니다.


©2023 Palo Alto Networks, Inc.

- URL 항목에서 **http** 및 **https**를 생략합니다.
- 각 URL 항목의 길이는 최대 255자입니다.
- 차단하거나 허용하려는 IP 주소 또는 URL에 정확히 일치를 입력하거나 와일드 카드를 사용하여 패턴 일치를 생성합니다.

  항목이 다르면 정확히 일치하는 항목이 다릅니다. 특정 웹페이지의 *URL*(***example.com/contact***)을 입력하면 방화벽 제한이 해당 페이지에만 적용됩니다. 도메인에 대한 완전 일치는 일치를 도메인 자체 및 해당 하위 디렉터리로 제한합니다.
- URL 이상에서 원래 항목에 액세스할 수 있는 경우 웹 사이트 또는 페이지에 액세스하는 데 가장 일반적으로 사용되는 URL을 예외 목록(예 **: blog.paloaltonetworks.com** 및 **paloaltonetworks.com/blog**)에 추가하는 것이 좋습니다.
- **example.com** 항목은 **www.example.com**과 다릅니다. 도메인 이름은 동일하지만 두 번째 항목에는 *www* 하위 도메인이 포함됩니다.

*Palo Alto Networks*는 사용자 지정 *URL* 카테고리 또는 외부 동적 목록 항목에서 정규식 사용을 지원하지 않습니다. 특정 *URL*을 알고 있거나 와일드카드와 **. / ? & = ; +** 문자를 사용하여 일치시키려는 *URL* 패턴을 구성해야 합니다.

## URL 카테고리 예외 목록에 대한 와일드카드 지침

URL 카테고리 예외 목록에서 별표(*) 및 캐럿(^)을 사용하여 정확한 URL을 지정하지 않고 여러 하위 도메인, 도메인, 최상위 도메인(TLD) 또는 페이지와 일치하도록 단일 항목을 구성할 수 있습니다.

별표**(*)** 및 캐럿**(^)** 와일드카드를 사용하는 방법

토큰 구분 기호는 **. / ? & = ; +**입니다. 이러한 문자 중 하나 또는 두 개로 구분된 모든 문자열은 토큰입니다. 와일드카드 문자를 토큰 자리 표시자로 사용하여 특정 토큰에 모든 값이 포함될 수 있음을 나타냅니다. **docs.paloaltonetworks.com** 항목에서 토큰은 "docs", "paloaltonetworks" 및 "com"입니다.

다음 표에서는 별표와 캐럿의 작동 방식을 설명하고 예시를 제공합니다.

| * | ^ |
|---|---|
| 하나 이상의 가변 하위 도메인, 도메인, TLD 또는 하위 디렉터리를 나타냅니다.<br>후행 슬래시 뒤에 별표를 사용할 수 있습니다(예 **: example.com/***).<br>예: ***.domain.com**은 **docs.domain.com** 및 **abc.xyz.domain.com**과 일치합니다. | 하나의 변수 하위 도메인, 루트 도메인 또는 TLD를 나타냅니다.<br>후행 슬래시 후에는 캐럿을 사용할 수 없습니다. 유효하지 않은 항목: **example.com/^**.<br>예: **^.domain.com**은 **docs.domain.com** 및 **blog.domain.com**과 일치합니다. |

요점**:** 별표는 캐럿보다 더 넓은 범위의 URL과 일치합니다. 별표는 임의의 수의 연속 토큰에 해당하며, 캐럿은 정확히 하나의 토큰에 해당합니다.


©2023 Palo Alto Networks, Inc.

| * | ^ |
|---|---|
| **xyz.*.com**과 같은 항목은 **xyz.^.^.com**보다 많은 수의 사이트와 일치하고, **xyz.*.com**은 문자열 사이에 임의의 수의 토큰이 있는 사이트와 일치하며, **xyz.^.^.com**은 정확히 두 개의 토큰이 있는 사이트와 일치합니다. | |

- 와일드카드는 토큰 내의 유일한 문자여야 합니다. 예를 들어, **example*.com**은 **example** 및 ***가 동일한 토큰에 있기 때문에 잘못된 항목입니다. 그러나 항목에는 둘 이상의 토큰에 와일드카드가 포함될 수 있습니다.
- 동일한 항목에서 별표와 캐럿을 사용할 수 있습니다(예: ***.example.^**).

연속 별표***(*)*** 또는 아홉 개 이상의 연속 캐럿***(^)***이 있는 항목을 만들지 마십시오**.** 이와 같은 항목은 방화벽 성능에 영향을 줄 수 있습니다**.**

예를 들어 ***mail.*.*.com***과 같은 항목을 추가하지 마십시오. 대신 액세스를 제어하려는 웹 사이트의 범위에 따라 ***mail.*.com*** 또는 ***mail.^.^.com***을 입력합니다.

## URL 카테고리 예외 목록 - 예시

다음 표에는 예시 URL 목록 항목, 일치하는 사이트 및 방화벽이 후행 슬래시를 자동으로 추가할 때 일치하는 동작에 대한 설명이 나와 있습니다.

이 테이블의 항목에는 방화벽이 백그라운드의 적용 가능한 항목에 하나를 추가한다는 것을 반영하는 후행 슬래시가 포함되어 있지 않습니다**.** 또한 예외 목록에는 후행 슬래시 지침 앞에 추가된 항목이 포함될 수 있습니다. URL 카테고리 예외 목록 - 예시*(PAN-OS 10.1)*에서는 방화벽이 기본적으로 후행 슬래시를 추가하지 않을 때 일치하는 동작을 보여 줍니다**.**

후행 슬래시를 수동으로 추가하여 항목을 검사하는 모든 사용자가 항목의 의도된 일치 동작을 명확히 하는 것이 좋습니다**.** 후행 슬래시는 방화벽에 의해 추가되면 보이지 않습니다**.**

| **URL** 예외 목록 항목 | 일치하는 사이트 | 설명 |
|---|---|---|
| 예시 세트 **1** | | |
| paloaltonetworks.com | paloaltonetworks.com<br>paloaltonetworks.com/network-security/security-subscriptions | 방화벽은 항목에 후행 슬래시를 추가하여 정확한 도메인 및 하위 디렉터리에 대한 일치 항목을 제한합니다. |
| paloaltonetworks.com/example | paloaltonetworks.com/example | 방화벽은 하위 디렉터리 예시가 도메인을 따르기 때문에 이 항목에 후행 슬래시를 추가하지 않습니다. 특정 웹 페이지의 URL을 입력하면 방화벽이 지정된 웹 페이지에 예외 작업을 적용합니다. |


©2023 Palo Alto Networks, Inc.

| URL 예외 목록 항목 | 일치하는 사이트 | 설명 |
|---|---|---|
| 예시 세트 **2** - 별표 | | |
| *.example.com | www.example.com<br>docs.example.com<br>support.tools.example.com | 별표는 일치 항목을 모든 **example.com** 하위 도메인으로 확장합니다.<br>방화벽은 루트 도메인인 **example.com**의 오른쪽과 일치하는 항목을 제외하고 항목에 후행 슬래시를 추가합니다. |
| mail.example.*<br>이 항목은 후행 슬래시 기능이 활성화되어 있거나 사용되지 않는 동일한 일치 항목을 생성합니다. | mail.example.com<br>mail.example.co.uk<br>mail.example.com/#inbox | 별표는 일치 항목을 **mail.example.<*TLD*>** 패턴을 따르는 모든 URL로 확장합니다. |
| example.*.com | example.yoursite.com<br>example.es.domain.com<br>example.abc.xyz.com | 별표는 맨 왼쪽 하위 도메인이 **example**이고 최상위 도메인이 **com**인 URL로 일치를 확장합니다. 후행 슬래시는 TLD의 오른쪽에 있는 일치 항목을 제외합니다. |
| example.com/* | example.com/photos<br>example.com/blog/latest<br>example.com 하위 디렉터리 | 도메인 뒤에는 / 및 별표가 표시되며 이는 하위 디렉터리가 있어야 함을 나타냅니다. 별표는 모든 **example.com** 하위 디렉터리에 대한 토큰 자리 표시자 역할을 합니다.<br>방화벽은 항목이 별표로 끝나기 때문에 후행 슬래시를 추가하지 않습니다. |
| 예시 세트 **3** - 캐럿 | | |
| google.^ | google.com<br>google.info | 캐럿은 일치 항목을 **google**로 시작하고 단일 TLD로 끝나는 URL로 확장합니다. 후행 슬래시 |


©2023 Palo Alto Networks, Inc.

| URL 예외 목록 항목 | 일치하는 사이트 | 설명 |
|---|---|---|
| *example.co.^*과 같은 패턴은 일반적으로 ***example.co.jp***와 같은 국가별 도메인을 일치시키는 데 사용됩니다. 그러나 일반 최상위 도메인*(gTLD)*을 사용하면 *example.co.^*가 *example.co.info* 또는 *example.co.amzn*과 일치하는 것과 같은 패턴이 생성되며 이러한 패턴은 동일한 조직에 속하지 않을 수 있습니다. | google.com/search?q=paloaltonetworks | 는 마지막 토큰의 오른쪽과 일치하는 항목을 제외합니다. |
| ^.google.com | www.google.com<br>news.google.com | 캐럿은 일치 항목을 **google.com**의 단일 수준 하위 도메인으로 확장합니다. 방화벽은 루트 도메인의 오른쪽에 있는 일치 항목을 제외하고 항목에 후행 슬래시를 추가합니다. |
| ^.^.google.com | www.maps.google.com<br>support.tools.google.com | 두 개의 캐럿은 일치 항목을 **google.com** 앞에 두 개의 연속 하위 도메인을 포함하는 URL로 확장합니다. 방화벽은 루트 도메인 오른쪽에 일치하는 항목을 제외하고 항목에 후행 슬래시를 추가합니다. |
| google.^.com | google.example.com<br>google.company.com | 캐럿은 **google**이 맨 왼쪽 하위 도메인이고 그 뒤에 하나의 토큰과 **.com**이 오는 URL로 일치 항목을 확장합니다.<br>방화벽은 TLD 오른쪽에 있는 일치 항목을 제외하고 항목에 후행 슬래시를 추가합니다. |


©2023 Palo Alto Networks, Inc.

# URL 필터링 프로파일에서 외부 동적 목록 사용

새로 발견된 위협 및 멀웨어로부터 네트워크를 보호하기 위해 URL 필터링 프로파일에서 외부 동적 목록을 사용할 수 있습니다. 외부 동적 목록을 사용하면 방화벽에서 구성을 변경하거나 커밋하지 않고도 목록을 업데이트할 수 있습니다. 외부 동적 목록은 외부 웹 서버에서 호스팅되는 텍스트 파일입니다. 이 목록을 사용하여 URL을 가져오고 이러한 URL에 대한 정책을 시행할 수 있습니다. 웹 서버에서 목록이 업데이트되면 방화벽은 변경 사항을 검색하고 방화벽에서 커밋할 필요 없이 수정된 목록에 정책을 적용합니다.

방화벽은 구성된 인터벌로 목록을 동적으로 가져오고 목록의 URL(IP 주소 또는 도메인은 무시됨)에 대한 정책을 시행합니다. URL 형식 지정 지침은 URL 카테고리 예외을(를) 참조하십시오.

자세한 내용은 외부 동적 목록을 참조하십시오.

**STEP 1 |** 외부 동적 목록에 액세스하도록 방화벽을 구성합니다.

- 목록에 IP 주소나 도메인 이름이 포함되어 있지 않은지 확인하십시오. 방화벽은 URL이 아닌 항목을 건너뜁니다.
- 사용자 정의 URL 목록 지침을 사용하여 목록의 형식을 확인하십시오.
- 유형 드롭다운에서 **URL** 목록을 선택합니다.

**STEP 2 |** URL 필터링 프로파일에서 외부 동적 목록을 사용합니다.

1. 개체 > 보안 프로파일 > **URL** 필터링을 선택합니다.
2. 기존 URL 필터링 프로파일을 추가하거나 수정합니다.
3. 프로파일을 이름으로 지정하고 카테고리 탭의 카테고리 목록에서 외부 동적 목록을 선택합니다.
4. 외부 동적 목록의 URL에 대해 보다 세부적인 작업을 선택하려면 작업을 클릭합니다.

   외부 동적 목록에 포함된 ***URL***이 사용자 지정 ***URL*** 카테고리 또는 차단 및 허용 목록에도 포함된 경우 사용자 지정 카테고리 또는 차단 및 허용 목록에 지정된 작업이 외부 동적 목록보다 우선합니다.
5. 확인을 클릭합니다.
6. URL 필터링 프로파일을 보안 정책 규칙에 연결합니다.
   1. 정책 > 보안을 선택합니다.
   2. 작업 탭을 선택한 다음 프로파일 설정 섹션의 **URL** 필터링 드롭다운에서 새 프로파일을 선택합니다.
   3. 확인 및 커밋을 클릭합니다.

**STEP 3 |** 정책 작업이 적용되었는지 테스트합니다.

1. 외부 동적 목록 항목을 보고 목록에서 URL에 액세스해 봅니다.
2. 정의한 조치가 브라우저에서 시행되는지 확인하십시오.
3. 방화벽에서 활동을 모니터링하려면 다음을 수행합니다.
   1. **ACC**를 선택한 다음 URL 도메인을 전역 필터로 추가하여 액세스한 URL에 대한 네트워크 활동 및 차단된 활동을 봅니다.
   2. 자세한 로그 보기에 액세스하려면 **Monitor** > **Logs** > **URL** 필터링을 선택하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 외부 동적 목록의 항목이 무시되거나 건너뛰었는지 확인합니다.

URL 유형 목록에서 방화벽은 URL이 아닌 항목을 유효하지 않은 항목으로 건너뛰고 방화벽 모델의 최대 제한을 초과하는 항목을 무시합니다.



외부 동적 목록 유형에 대한 제한에 도달했는지 확인하려면 개체 > 외부 동적 목록을 선택한 다음 목록 용량을 클릭합니다.

방화벽에서 다음 CLI 명령을 사용하여 목록에 대한 세부 정보를 검토합니다.

```
request system external-list show type url name <list_name>
```

예:

```
request system external-list show type url name My_URL_List vsys5/
My_URL_List: Next update at : Tue Jan 3 14:00:00 2017 Source:
 http://example.com/My_URL_List.txt Referenced: Yes Valid: Yes
 Auth-Valid: Yes Total valid entries: 3 Total invalid entries: 0
 Valid urls: www.URL1.com www.URL2.com www.URL3.com
```

 ©2023 Palo Alto Networks, Inc.

# 특정 사이트에 대한 암호 액세스 허용

경우에 따라 차단하고 싶지만 특정 개인이 때때로 액세스하도록 허용하는 URL 카테고리가 있을 수 있습니다. 이 경우 방화벽 Content-ID 구성에서 URL 관리자 재정의 암호를 재정의하고 정의하도록 카테고리 작업을 설정합니다. 사용자는 이러한 카테고리의 사이트에 액세스하기 전에 재정의 암호를 제공해야 합니다. URL 관리자 재정의를 구성하려면 다음 절차를 따르십시오.

**STEP 1 |** URL 관리자 재정의 암호를 설정합니다.

1. 디바이스 > 설정 > 콘텐츠 **ID**를 선택합니다.
2. **URL** 관리 재정의 섹션에서 추가를 클릭합니다.
3. 위치 필드에서 이 암호가 적용되는 가상 시스템을 선택합니다.
4. 비밀번호 및 비밀번호 확인을 입력합니다.
5. **SSL/TLS** 서비스 프로파일을 선택합니다. 프로파일은 재정의가 있는 사이트가 HTTPS 사이트인 경우 방화벽이 사용자에게 제공하는 인증서를 지정합니다. 자세한 내용은 SSL/TLS 서비스 프로파일 구성을 참조하십시오.
6. 사용자에게 비밀번호를 묻는 메시지를 표시하려면 모드를 선택합니다.
   - 투명 - 방화벽은 원래 대상 URL을 재정의하고 가장하도록 설정한 URL 카테고리의 사이트로 향하는 브라우저 트래픽을 가로채 HTTP 302를 실행하여 vsys 수준에 적용되는 암호를 묻는 메시지를 표시합니다.

     클라이언트 브라우저는 인증서를 신뢰하지 않는 경우 인증서 오류를 표시합니다.
   - 리디렉션 - 방화벽은 재정의하도록 설정된 URL 카테고리에 대한 HTTP 또는 HTTPS 트래픽을 가로채고 재정의 암호를 묻는 메시지를 표시하기 위해 HTTP 302 리디렉션을 사용하여 방화벽의 레이어 3 인터페이스로 요청을 리디렉션합니다. 이 옵션을 선택하는 경우 트래픽을 리디렉션할 주소(IP 주소 또는 DNS 호스트 이름)를 제공해야 합니다.
7. 확인을 클릭합니다.

**STEP 2 |** (선택 사항) 사용자 지정 재정의 기간을 설정합니다.

1. URL 필터링 섹션을 편집합니다.
2. 사용자가 재정의 암호를 성공적으로 입력한 카테고리의 사이트를 탐색할 수 있는 시간을 변경하려면 **URL** 관리자 재정의 타임아웃 필드에 새 값을 입력합니다. 기본적으로 사용자는 암호를 다시 입력하지 않고 15분 동안 카테고리 내 사이트에 액세스할 수 있습니다.
3. 재정의 암호를 입력하려는 시도가 세 번 실패한 후 재정의하도록 설정된 사이트에 대한 사용자 액세스 차단 시간을 변경하려면 **URL** 관리자 잠금 타임아웃 필드에 새 값을 입력합니다. 기본적으로 사용자는 30분 동안 차단됩니다.
4. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** (리디렉션 모드만 해당) 웹 요청을 재정의하도록 구성된 카테고리의 사이트로 리디렉션할 레이어 3 인터페이스를 생성합니다.

1. 인터페이스에서 URL 필터링 계속 및 재정의 페이지 응답 페이지를 표시할 수 있도록 관리 프로파일을 생성합니다.

   **1.** 네트워크 > 인터페이스 관리를 선택한 다음 추가를 클릭합니다.

   **2.** 프로파일의 이름을 입력하고 응답 페이지를 선택한 다음 확인을 클릭합니다.

2. 레이어 3 인터페이스를 만듭니다. 방금 생성한 관리 프로파일을 첨부해야 합니다(이더넷 인터페이스 대화 상자의 고급 > 기타 정보 탭에서).

**STEP 4 |** (리디렉트 모드만 해당) 인증서 오류를 표시하지 않고 사용자를 투명하게 리디렉션하려면 재정의하도록 구성된 URL 카테고리의 사이트로 웹 요청을 리디렉션하는 인터페이스의 IP 주소와 일치하는 인증서를 설치합니다. 서명된 인증서를 가져오거나 외부 CA에서 서명한 인증서를 가져옵니다.

자체 서명된 인증서를 사용하려면 먼저 루트 CA 인증서를 만든 다음 해당 CA를 사용하여 다음과 같이 URL 관리 재정의에 사용할 인증서에 서명해야 합니다.

1. 루트 CA 인증서를 만들려면 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 생성을 클릭합니다. RootCA와 같은 인증서 이름을 입력합니다. 서명자 필드에서 값을 선택하지 마십시오(자체 서명되었음을 나타냄). 인증 기관 체크박스를 선택했는지 확인한 다음 인증서 생성을 클릭합니다.
2. URL 관리 재정의에 사용할 인증서를 만들려면 생성을 클릭합니다. 인증서 이름을 입력하고 인터페이스의 DNS 호스트 이름 또는 IP 주소를 일반 이름으로 입력합니다. 서명자 필드에서 이전 단계에서 생성한 CA를 선택합니다. IP 주소 속성을 추가하고 웹 요청을 재정의 작업이 있는 URL 카테고리로 리디렉션할 레이어 3 인터페이스의 IP 주소를 지정합니다.
3. 인증서를 생성합니다.
4. 클라이언트가 인증서를 신뢰하도록 구성하려면 디바이스 인증서 탭에서 CA 인증서를 선택한 다음 내보내기를 클릭합니다. 그런 다음 브라우저를 수동으로 구성하거나 Active Directory GPO(그룹 정책 개체)의 신뢰할 수 있는 루트에 인증서를 추가하여 모든 클라이언트 브라우저에 신뢰할 수 있는 루트 CA로 인증서를 가져와야 합니다.

**STEP 5 |** 액세스를 활성화하기 위해 재정의 암호가 필요한 URL 카테고리를 지정합니다.

1. 개체 > **URL** 필터링을 선택한 다음 기존 URL 필터링 프로파일을 선택하거나 새 프로파일을 추가합니다.
2. 카테고리 탭에서 암호가 필요한 각 카테고리에 대해 재정의할 작업을 설정합니다.
3. URL 필터링 프로파일의 나머지 섹션을 완료한 다음 확인을 클릭하여 프로파일을 저장합니다.

**STEP 6 |** 액세스를 위해 암호 재정의가 필요한 사이트에 대한 액세스를 허용하는 보안 정책 규칙에 URL 필터링 프로파일을 적용합니다.

1. 정책 > 보안을 선택한 다음 적절한 보안 정책을 선택하여 수정합니다.
2. 작업 탭을 선택한 다음 프로파일 설정 섹션에서 **URL** 필터링 드롭다운을 클릭하고 프로파일을 선택합니다.
3. 확인을 클릭하여 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** 구성을 저장합니다.

커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 자격 증명 피싱 방지

피싱 사이트는 공격자가 사용자 정보, 특히 네트워크에 대한 액세스를 제공하는 자격 증명을 훔칠 의도로 합법적인 웹사이트로 가장하는 사이트입니다. 피싱 이메일이 네트워크에 침입하면 단 한 명의 사용자만 링크를 클릭하고 자격 증명을 입력하여 위반을 실행합니다. 사이트의 URL 카테고리에 따라 사용자가 회사 자격 증명을 제출할 수 있는 사이트를 제어하여 진행 중인 피싱 공격을 감지 및 방지하여 자격 증명 유출을 방지할 수 있습니다. 이를 통해 사용자가 신뢰할 수 없는 사이트에 자격 증명을 제출하지 못하도록 차단하고 기업 및 승인된 사이트에 대한 자격 증명 제출을 허용할 수 있습니다.

자격 증명 피싱 방지는 웹사이트에 제출된 사용자명 및 암호를 스캔하고 이러한 제출을 유효한 회사 자격 증명과 비교하여 작동합니다. 웹사이트의 URL 카테고리를 기반으로 회사 자격 증명 제출을 허용하거나 차단할 웹사이트를 선택할 수 있습니다. 방화벽이 제한된 카테고리의 사이트에 자격 증명을 제출하려는 사용자를 감지하면 사용자가 자격 증명을 제출하지 못하도록 차단 응답 페이지를 표시하거나 특정 URL의 사이트에 자격 증명을 제출하지 못하도록 사용자에게 경고하는 페이지를 계속 표시하며, 카테고리이지만 여전히 제출을 계속할 수 있습니다. 이러한 차단 페이지를 사용자 지정하여 피싱이 아닌 합법적인 사이트에서도 회사 자격 증명을 재사용하지 못하도록 사용자를 교육할 수 있습니다.

자격 증명 피싱 방지를 활성화하려면 사용자가 개인 자격 증명과 반대되는 유효한 회사 자격 증명을 사이트에 제출할 때 감지하도록 User-ID를 구성하고 사용자가 회사 자격 증명을 입력하지 못하도록 하려는 경우 URL 범주를 지정하기 위한 URL 필터링을 구성해야 합니다. 다음 항목에서는 자격 증명 제출을 검색하는 데 사용할 수 있는 다양한 방법에 대해 설명하고 자격 증명 피싱 보호를 구성하기 위한 지침을 제공합니다.

- 회사 자격 증명 제출 확인 방법
- Windows 기반 User-ID 에이전트로 자격 증명 감지 구성
- 자격 증명 피싱 방지 설정

## 회사 자격 증명 제출 확인 방법

자격 증명 피싱 방지를 설정하기 전에 방화벽에서 유효한 회사 자격 증명이 웹 페이지에 제출되었는지 확인하는 데 사용할 방법을 결정합니다.

| 제출된 자격 증명을 확인하는 방법 | 사용자 **ID** 구성 요구 사항 | 이 매서드는 사용자가 웹사이트에 제출하는 회사 사용자 이름 및/또는 암호를 어떻게 검색합니까**?** |
|---|---|---|
| 그룹 매핑 | 방화벽의그룹 매핑 구성 | 방화벽은 사용자가 제한된 사이트에 제출하는 사용자 이름이 유효한 회사 사용자 이름과 일치하는지 확인합니다.<br>이렇게 하려면 방화벽은 제출된 사용자 이름을 사용자 간 매핑 테이블의 사용자 이름 목록과 일치하여 사용자가 제한된 카테고리의 사이트에 회사 사용자 이름을 제출할 시기를 감지합니다.<br>이 메서드는 LDAP 그룹 구성원 자격에 따라 회사 사용자 이름 제출만 검사하므로 구성이 간단하지만 잘못된 긍정을 더 쉽게 만드는 경향이 있습니다. |


©2023 Palo Alto Networks, Inc.

| 제출된 자격 증명을 확인하는 방법 | 사용자 **ID** 구성 요구 사항 | 이 매서드는 사용자가 웹사이트에 제출하는 회사 사용자 이름 및/또는 암호를 어떻게 검색합니까**?** |
|---|---|---|
| IP 사용자 매핑 | 사용자 매핑., GlobalProtect 또는 인증 정책 및 인증 포털을 통해 식별된 IP 주소-사용자 이름 매핑. | 방화벽은 사용자가 제한된 사이트 맵에 제출하는 사용자 이름이 로그인 사용자 이름의 IP 주소로 제출하는지 확인합니다.<br><br>이렇게 하려면 방화벽은 로그인 사용자 이름의 IP 주소와 웹 사이트에 제출된 사용자 이름을 IP 주소 - 사용자 매핑 테이블과 일치하여 사용자가 제한된 카테고리의 사이트에 회사 사용자 이름을 제출할 시기를 감지합니다.<br><br>이 매서드는 세션과 연결된 로그인 사용자 이름의 IP 주소를 IP 주소-사용자 이름 매핑 테이블과 일치시키기 때문에 회사 사용자 이름 제출을 감지하는 효과적인 방법이지만 회사 암호 제출은 감지하지 못합니다. 회사 사용자 이름과 암호 제출을 검색하려면 도메인 자격 증명 필터 메서드를 사용해야 합니다. |
| 도메인 자격 증명 필터 | 사용자 ID 자격 증명 서비스 추가 기능으로 구성된 Windows User-ID 에이전트<br><br>- 그리고 -<br><br>사용자 매핑., GlobalProtect 또는 인증 정책 및 인증 포털을 통해 식별된 IP 주소-사용자 이름 매핑. | 방화벽은 사용자가 제출하는 사용자 이름과 암호가 동일한 사용자의 회사 사용자 이름과 암호와 일치하는지 확인합니다.<br><br>이렇게 하려면 방화벽은 자격 증명 제출을 유효한 회사 사용자 이름과 암호와 일치시키고 사용자 이름이 로그인 사용자 이름의 IP 주소에 맵을 제출했는지 확인할 수 있어야 합니다.<br><br>• 회사 사용자 이름과 암호를 검색하려면 방화벽은 사용자 ID 자격 증명 서비스 추가 기능이 장착된 Windows User-ID 에이전트에서 블룸 필터라고 하는 보안 비트 마스크를 검색합니다. 이 추가 기능 서비스는 사용자 이름과 암호 해시에 대한 디렉터리를 검사하고 보안 비트 마스크(블룸 필터)로 분해하여 Windows User-ID 에이전트에 제공합니다. 방화벽은 Windows User-ID 에이전트에서 정기적으로 꽃 필터를 검색합니다. 제한된 카테고리에 자격 증명을 제출하는 사용자를 감지할 때마다 블룸 필터를 재구성하고 일치하는 사용자 이름과 암호 해시를 찾습니다. 방화벽은 사용자 ID 자격 증명 서비스 추가 기능을 실행하는 하나의 Windows User-ID 에이전트에만 연결할 수 있습니다.<br>• 자격 증명이 로그인 사용자 이름에 속하는지 확인하려면 - 방화벽은 로그인 사용자 이름의 IP 주소와 IP 주소 간 사용자 이름 매핑 테이블에서 감지된 사용자 이름 간의 매핑을 찾습니다.<br><br>도메인 자격 증명 메서드의 작동 방식과 이러한 유형의 검색을 사용하도록 설정하기 위한 요구 사항을 자세히 알아보 |


©2023 Palo Alto Networks, Inc.

| 제출된 자격 증명을 확인하는 방법 | 사용자 **ID** 구성 요구 사항 | 이 매서드는 사용자가 웹사이트에 제출하는 회사 사용자 이름 및/또는 암호를 어떻게 검색합니까**?** |
|---|---|---|
| | | 려면 Windows 기반 User-ID 에이전트를 사용하여 자격 증명 검색 구성을참조하세요. |

## Windows User-ID 에이전트로 자격 증명 감지 구성

도메인 자격 증명 필터 감지를 사용하면 방화벽이 웹 페이지에 제출된 암호를 감지할 수 있습니다. 이 자격 증명 감지 방법을 사용하려면 Windows User-ID 에이전트와 User-ID 에이전트에 대한 추가 기능인 User-ID 자격 증명 서비스가 RODC(읽기 전용 도메인 컨트롤러)에 설치되어 있어야 합니다.

도메인 자격 증명 필터 검색 방법은 ***Windows User-ID*** 에이전트에서만 지원됩니다**.** ***PAN-OS*** 통합 ***User-ID*** 에이전트를 사용하여 이 자격 증명 감지 방법을 구성할 수 없습니다**.**

RODC는 도메인 컨트롤러가 호스팅하는 Active Directory 데이터베이스의 읽기 전용 복사본을 유지 관리하는 Microsoft Windows 서버입니다. 예를 들어 도메인 컨트롤러가 회사 본사에 있는 경우 RODC를 원격 네트워크 위치에 배포하여 로컬 인증 서비스를 제공할 수 있습니다. RODC에 User-ID 에이전트를 설치하는 것은 몇 가지 이유로 유용할 수 있습니다. 자격 증명 검색을 활성화하기 위해 도메인 컨트롤러 디렉터리에 대한 액세스가 필요하지 않으며 제한된 사용자 또는 대상 사용자 집합에 대한 자격 증명 검색을 지원할 수 있습니다. RODC 호스트 디렉터리는 읽기 전용이므로 디렉터리 내용은 도메인 컨트롤러에서 안전하게 유지됩니다.

자격 증명 검색을 위해 ***RODC***에 ***Windows User-ID*** 에이전트를 설치해야 하므로 모범 사례로 이 목적을 위해 별도의 에이전트를 배포합니다**.** ***RODC***에 설치된 ***User-ID*** 에이전트를 사용하여 ***IP*** 주소를 사용자에게 매핑하지 마십시오**.**

RODC에 User-ID 에이전트를 설치하면 User-ID 자격 증명 서비스가 백그라운드에서 실행되고 디렉터리에서 RODC PRP(암호 복제 정책)에 나열된 그룹 구성원의 사용자 이름 및 암호 해시를 검색합니다. 이 목록에 포함시키고자 하는 사용자를 명시할 수 있습니다. 그런 다음 사용자 ID 자격 증명 서비스는 수집된 사용자 이름과 암호 해시를 가져와 데이터를 블룸 필터라고 하는 비트 마스크 유형으로 분해합니다. 블룸 필터는 요소(사용자 이름 또는 암호 해시)가 요소 집합(RODC에 복제하도록 승인한 자격 증명 집합)의 구성원인지 확인하는 안전한 방법을 제공하는 압축 데이터 구조입니다. 사용자 ID 자격 증명 서비스는 블룸 필터를 Windows User-ID 에이전트에 포워딩합니다. 방화벽은 정기적으로 User-ID 에이전트에서 최신 블룸 필터를 검색하고 이를 사용하여 사용자 이름 및 암호 해시 제출을 감지합니다. 설정에 따라 방화벽은 웹 페이지에 유효한 암호 제출을 차단, 경고 또는 허용하거나 사용자에게 피싱의 위험을 경고하지만 제출을 계속할 수 있는 응답 페이지를 표시합니다.

이 프로세스 동안 User-ID 에이전트는 암호 해시를 저장하거나 노출하지 않으며 암호 해시를 방화벽으로 포워딩하지도 않습니다. 암호 해시가 블룸 필터로 분해되면 복구할 방법이 없습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** Windows 사용자 ID 에이전트를 사용하여 사용자 매핑을 구성합니다.

> 자격 증명 검색을 활성화하려면 ***RODC***에 ***Windows User-ID*** 에이전트를 설치해야 합니다. 지원되는 서버 목록은 호환성 매트릭스를 참조하십시오. 이를 위해 별도의 ***User-ID*** 에이전트를 설치하십시오.

도메인 자격 증명 필터 감지를 활성화하기 위해 사용자 ID를 설정할 때 기억해야 할 중요 항목은 아래와 같습니다.

- 자격 증명 피싱 탐지의 효율성은 RODC 설정에 따라 달라지므로 RODC 관리에 대한 모범 사례 및 권장 사항도 검토해야 합니다.
- User-ID 소프트웨어 업데이트 다운로드:
  - User-ID 에이전트 Windows 설치 프로그램 - UaInstall-xxx-x.msi.
  - User-ID 에이전트 자격 증명 서비스 Windows 설치 프로그램 - UaCredInstall64-xxx-x.msi.
- LDAP를 통해 Active Directory를 읽을 수 있는 권한이 있는 계정을 사용하여 RODC에 User-ID 에이전트 및 사용자 에이전트 자격 증명 서비스를 설치합니다(User-ID 에이전트에도 이 권한이 필요함).
  - User-ID 에이전트 자격 증명 서비스에는 로컬 시스템 계정으로 로그온할 수 있는 권한이 필요합니다. 자세한 내용은 User-ID 에이전트 전용 서비스 계정 생성을 참조하십시오.
  - 서비스 계정은 RODC에서 로컬 관리자 그룹의 구성원이어야 합니다. 자세한 내용은 다음 링크를 참조하십시오.

**STEP 2 |** User-ID 에이전트와 사용자 에이전트 자격 증명 서비스(허용된 자격 증명을 스캔하기 위해 백그라운드에서 실행)를 활성화하여 정보를 공유합니다.

1. RODC 서버에서 User-ID 에이전트를 시작합니다.
2. 설정을 선택한 다음 설정 섹션을 편집합니다.
3. 자격 증명 탭을 선택합니다. 이 탭은 사용자 ID 에이전트 자격 증명 서비스를 이미 설치한 경우에만 표시됩니다.
4. 사용자 **ID** 자격 증명 에이전트에서 가져오기를 선택합니다. 이를 통해 User-ID 에이전트는 사용자 및 해당 암호 해시를 나타내기 위해 User-ID 자격 증명 에이전트가 생성하는 블룸 필터를 가져올 수 있습니다.
5. 확인, 설정 저장, 커밋을 차례로 클릭합니다.

**STEP 3 |** RODC 디렉터리에서 자격 증명 제출 검색을 지원하려는 사용자 그룹을 정의합니다.

- 자격 증명 제출 적용을 받아야 하는 그룹이 허용된 RODC 암호 복제 그룹에 추가되었는지 확인합니다.
- 허용된 RODC 암호 복제 그룹의 그룹이 기본적으로 거부된 RODC 암호 복제 그룹에도 없는지 확인합니다. 둘 다에 나열된 그룹은 자격 증명 피싱 실시 대상이 아닙니다.

**STEP 4 |** 다음 작업을 계속합니다.

방화벽에서 자격 증명 피싱 방지를 설정합니다.

 ©2023 Palo Alto Networks, Inc.

# 자격 증명 피싱 방지 설정

사용할 회사 자격 증명 제출을 감지하는 방법을 결정했으면 다음 단계를 수행하여 사용자가 웹 페이지에 회사 자격 증명을 제출할 때 방화벽이 감지하도록 하고 이 작업에 대해 경고하거나 자격 증명 제출을 차단하거나 사용자는 제출을 계속하기 전에 피싱의 위험을 인지해야 합니다.



자격 증명 피싱 방지를 활성화하기 전에 방화벽에서 구성하는 기본 사용자명이 ***sAMAccountName*** 속성을 사용하는지 확인하십시오**.** 자격 증명 피싱 방지는 대체 속성을 지원하지 않습니다**.**

**STEP 1 |** 아직 수행하지 않았다면 User-ID를 활성화하십시오.

회사 자격 증명 제출을 확인하는 각 방법에는 서로 다른 사용자 ID 구성이 필요합니다.

- 사용자가 유효한 회사 사용자명을 제출하는지의 여부를 감지하는 그룹 매핑 방법을 사용하려는 경우 사용자를 그룹에 매핑합니다.
- 사용자가 유효한 회사 사용자명을 제출하고 해당 사용자명이 로그인 사용자명과 동일한지 감지하는 IP 사용자 매핑 방법을 사용하려는 경우 IP 주소를 사용자에게 매핑합니다.
- 사용자가 유효한 사용자명과 암호를 제출하고 해당 자격 증명이 로그인한 사용자에게 속하는지의 여부를 감지하는 도메인 자격 증명 필터 방법을 사용하려는 경우 Windows 기반 User-ID 에이전트 및 사용자에 대한 맵 IP 주소를 사용하여 자격 증명 검색을 구성합니다.

**STEP 2 |** 아직 수행하지 않은 경우 모범 사례 URL 필터링 프로파일을 구성하여 멀웨어 또는 악용 콘텐츠를 호스팅하는 것으로 파악된 URL에 대한 보호를 보장합니다.

1. 개체 > 보안 프로파일 > **URL** 필터링 및 추가를 선택하거나 URL 필터링 프로파일을 수정합니다.
2. 알려진 모든 위험한 URL 카테고리(멀웨어, 피싱, 동적 DNS, 알 수 없음, 명령 및 제어, 극단주의, 저작권 침해, 프록시 회피 및 익명화, 새로 등록된 도메인, 그레이웨어 및 파킹)에 대한 액세스를 차단합니다.

**STEP 3 |** 사용자 자격 증명 제출에 대해 모니터링하려는 트래픽을 복호화하는 복호화 정책 규칙을 추가합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 허용된 URL 카테고리에 있는 웹사이트에 대한 회사 자격 증명 제출을 감지하도록 URL 필터링 프로파일을 구성합니다.

방화벽은 최상의 성능을 제공하기 위해 신뢰할 수 있는 사이트에 대한 ***URL*** 카테고리 확인을 활성화하더라도 신뢰할 수 있는 사이트에 대한 자격 증명 제출을 확인하지 않습니다. 신뢰할 수 있는 사이트는 ***Palo Alto Networks***가 악성 또는 피싱 공격을 관찰하지 않은 사이트를 나타냅니다. 이 신뢰할 수 있는 사이트 목록에 대한 업데이트는 애플리케이션 및 위협 콘텐츠 업데이트를 통해 제공됩니다. 자격 증명 감지에서 제외되는 ***App-ID*** 목록은 live.paloaltonetworks.com에서 자격 증명 제출 감지를 건너뛰는 신뢰할 수 있는 App-ID를 참조하십시오.

1. 사용자 자격 증명 감지를 선택합니다.
2. 사용자 자격 증명 감지 드롭다운에서 웹페이지에 대한 사용자 자격 증명 감지 방법 중 하나를 선택합니다.

   기본 사용자명의 형식이 ***User-ID*** 소스가 제공하는 사용자명 형식과 동일한지 확인합니다.

   - **IP** 사용자 매핑 사용 - 유효한 회사 사용자명 제출을 확인하고 로그인 사용자명이 세션의 소스 IP 주소에 매핑되는지 확인합니다. 이를 위해 방화벽은 제출된 사용자명과 세션의 소스 IP 주소를 해당 IP 주소 대 사용자명 매핑 테이블과 일치시킵니다. 이 방법을 사용하려면 IP 주소를 사용자에 매핑에 설명된 모든 사용자 매핑 방법을 사용할 수 있습니다.
   - 도메인 자격 증명 필터 사용 - 유효한 회사 사용자명과 암호 제출을 확인하고 사용자명이 로그인한 사용자의 IP 주소에 매핑되는지 확인합니다. 이 방법을 활성화하기 위해 사용자 ID를 설정하는 방법에 대한 지침은 Windows 기반 User-ID 에이전트로 자격 증명 감지 구성을 참조하십시오.
   - 그룹 매핑 사용 - 사용자를 그룹에 매핑하도록 방화벽을 구성할 때 채워진 사용자-그룹 매핑 테이블을 기반으로 유효한 사용자 이름 제출을 확인합니다.

     그룹 매핑을 사용하면 디렉터리의 모든 부분 또는 IT와 같이 가장 민감한 애플리케이션에 액세스할 수 있는 특정 그룹에 자격 증명 검색을 적용할 수 있습니다.

     이 방법은 고유하게 구조화된 사용자명이 없는 환경에서 거짓양성***(false positive)***이 되기 쉽습니다. 따라서 이 방법은 가치가 높은 사용자 계정을 보호하는 데만 사용해야 합니다.
3. 방화벽이 회사 자격 증명 제출의 탐지를 기록하는 데 사용하는 유효한 사용자명 탐지 로그 심각도를 설정합니다. 기본적으로 방화벽은 이러한 이벤트를 중간 심각도로 기록합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 허용된 사이트에 대한 자격 증명 제출을 차단(또는 경고)합니다.

1. 카테고리를 선택합니다.
2. 사이트 액세스가 허용되는 각 카테고리에 대해 사용자 자격 증명 제출을 처리할 방법을 선택하십시오.
   - 경고 - 사용자가 웹사이트에 자격 증명을 제출하도록 허용하지만 사용자가 이 URL 카테고리의 사이트에 자격 증명을 제출할 때마다 URL 필터링 로그를 생성합니다.
   - 허용 -(기본값) 사용자가 웹사이트에 자격 증명을 제출하도록 허용합니다.
   - 차단 - 사용자가 웹사이트에 자격 증명을 제출하지 못하도록 차단합니다. 사용자가 자격 증명을 제출하려고 하면 방화벽이 Anti-Phishing Block Page를 표시하여 자격 증명 제출을 방지합니다.
   - 계속 - 사용자가 자격 증명을 제출하려고 할 때 안티 피싱 계속 페이지 응답 페이지를 표시합니다. 제출을 계속하려면 사용자가 응답 페이지에서 계속을 선택해야 합니다.
3. 확인을 선택하여 URL 필터링 프로파일을 저장합니다.

**STEP 6 |** 자격 증명 검색 설정이 있는 URL 필터링 프로파일을 보안 정책 규칙에 적용합니다.

1. 정책 > 보안 및 추가를 선택하거나 보안 정책 규칙을 수정합니다.
2. 작업 탭에서 프로파일 유형을 프로파일으로 설정합니다.
3. 새 프로파일 또는 업데이트된 **URL** 필터링 프로파일을 선택하여 보안 정책 규칙에 연결합니다.
4. 확인을 선택하여 보안 정책 규칙을 저장합니다.

**STEP 7 |** 구성을 커밋합니다.

**STEP 8 |** 방화벽이 감지하는 자격 증명 제출을 모니터링합니다.



멀웨어 및 피싱 사이트를 방문한 사용자 수를 보려면 ***ACC*** **>** 악성 ***URL***을 방문하는 호스트를 선택합니다.

**Monitor** > **Logs** > **URL** 필터링을 선택합니다.

새로운 **Credential Detected** 열은 방화벽이 유효한 자격 증명이 포함된 HTTP 게시 요청을 감지한 이벤트를 나타냅니다.

이 열을 표시하려면 열 머리글 위로 마우스를 가져간 다음 화살표를 클릭하여 표시할 열을 선택합니다.

로그 항목 세부정보는 자격 증명 제출도 나타냅니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** 자격 증명 제출 감지를 확인하고 문제를 해결합니다.

- 자격 증명 감지 통계를 보려면 다음 CLI 명령을 사용하십시오.

```
> show user credential-filter statistics
```

이 명령의 출력은 자격 증명 제출을 감지하도록 방화벽에 구성된 방법에 따라 다릅니다. 예를 들어 도메인 자격 증명 필터 방법이 URL 필터링 프로파일에 구성된 경우 블룸 필터를 방화벽에 포워딩한 User-ID 에이전트 목록이 블룸 필터에 포함된 자격 증명 수와 함께 표시됩니다.

- (그룹 매핑 메서드만) 다음 CLI 명령을 사용하여 그룹 매핑 자격 증명 감지가 활성화된 URL 필터링 프로파일의 수와 제한된 사이트에 자격 증명을 제출하려고 했습니다.

```
> show user group-mapping statistics
```

- (도메인 자격 증명 필터 메서드 전용) 다음 CLI 명령을 사용하여 방화벽에 매핑을 보내는 모든 Windows 기반 사용자 ID 에이전트를 확인합니다.

```
> show user user-id-agent state all
```

이제 명령 출력은 방화벽이 각 에이전트로부터 수신한 블룸 필터 업데이트 수, 블룸 필터 업데이트 처리에 실패한 경우, 마지막 블룸 필터 업데이트 이후 경과한 시간(초)을 포함하는 블룸 필터 수를 표시합니다.

- (도메인 자격 증명 필터 방법만 해당) Windows 기반 User-ID 에이전트는 방화벽에 대한 BF(블룸 필터) 푸시를 참조하는 로그 메시지를 표시합니다. User-ID 에이전트 인터페이스에서 **Monitoring** > **Logs**를 선택합니다.


©2023 Palo Alto Networks, Inc.

# 세이프서치 시행

많은 검색 엔진에는 검색어 반환 트래픽에서 성인 이미지 및 비디오를 필터링하는 안전한 검색 설정이 있습니다. 최종 사용자가 가장 엄격한 안전 검색 설정을 사용하지 않는 경우 방화벽에서 검색 결과를 차단하도록 설정할 수 있으며 사용자에 대해 안전 검색을 투명하게 사용하도록 설정할 수도 있습니다. 방화벽은 다음 검색 공급자에 대한 안전한 검색 시행을 지원합니다. Google, Yahoo, Bing, Yandex 및 YouTube. 안전 검색은 최선의 노력의 설정이며 서비스 공급자는 모든 웹사이트에서 작동한다고 보장하지 않으며 검색 공급자는 사이트를 안전 또는 안전하지 않은 것으로 분류합니다(Palo Alto Networks가 아님).

이 기능을 사용하려면 URL 필터링 프로파일에서 안전 검색 적용 옵션을 사용하도록 설정하고 보안 정책 규칙에 연결해야 합니다. 그런 다음 방화벽은 가장 엄격한 안전 검색 설정을 사용하지 않는 일치하는 검색 쿼리 반환 트래픽을 차단합니다. 안전 검색을 적용하는 방법에는 두 가지가 있습니다.

- 엄격한 안전 검색을 사용하지 않을 때 검색 결과 차단 - 최종 사용자가 먼저 가장 엄격한 안전 검색 설정을 사용하도록 설정하지 않고 검색을 수행하려고 하면 방화벽이 검색 쿼리 결과를 차단하고 URL 필터링 안전 검색 차단 페이지를 표시합니다. 기본적으로 이 페이지는 안전 검색을 구성하기 위한 검색 공급자 설정에 대한 URL을 제공합니다.
- 투명하게 사용자를 위한 안전 검색 사용 - 일반 사용자가 엄격한 안전 검색 설정을 먼저 사용하지 않고 검색을 수행하려고 하면 방화벽은 HTTP 503 상태 코드를 사용하여 검색 결과를 차단하고 검색 쿼리를 안전 검색 매개 변수가 포함된 URL로 리디렉션합니다. 엄격한 안전 검색 매개 변수를 포함하도록 검색 URL을 다시 작성하기 위해 JavaScript가 포함된 새 URL 필터링 안전 검색 블록 페이지를 가져와서 이 기능을 활성화합니다. 이 구성에서는 사용자에게 차단 페이지가 표시되지 않지만 대신 가장 엄격한 안전 검색 옵션을 적용하는 검색 쿼리로 자동으로 리디렉션됩니다. 이 안전 검색 적용 방법은 Google, Yahoo 및 Bing 검색에서 지원됩니다.

안전 검색 설정은 검색 공급자마다 다르므로 여러 안전 검색 구현을 검토하여 시작하십시오. 그런 다음 안전 검색이 비활성화된 경우 검색 결과 차단 또는 사용자를 위해 안전 검색을 투명하게 사용 설정하는 두 가지 방법 중 하나를 사용하여 안전 검색을 적용합니다.

- 검색 공급자를 위한 안전 검색 설정
- 엄격한 안전 검색이 활성화되지 않은 경우 검색 결과 차단
- 투명하게 사용자를 위한 세이프서치 활성화

## 검색 공급자를 위한 안전 검색 설정

안전 검색 설정은 검색 공급자마다 다릅니다. 자세히 알아보려면 다음 설정을 검토하십시오.

| 검색 공급자 | 세이프서치 설정 설명 |
| --- | --- |
| Google/YouTube | Google의 안전한 검색 가상 IP 주소를 통해 개별 컴퓨터 또는 네트워크 전체에서 안전한 검색을 제공합니다.<br>개별 컴퓨터에서 **Google** 검색을 위한 세이프서치 시행<br>Google 검색 설정에서 음란물 필터링 설정은 안전한 검색 기능을 활성화합니다. 활성화하면 설정이 브라우저 쿠키에 |


©2023 Palo Alto Networks, Inc.

| 검색 공급자 | 세이프서치 설정 설명 |
| --- | --- |
| | **FF=**로 저장되고 사용자가 Google 검색을 수행할 때마다 서버에 포워딩됩니다.<br><br>Google 검색어 URL에 **safe=active**를 추가하면 가장 엄격한 안전 검색 설정도 가능합니다.<br><br>가상 **IP** 주소를 사용한 **Google** 및 **YouTube** 검색에 대한 세이프 서치 시행<br><br>Google은 모든 Google 및 YouTube 검색에서 SafeSearch(forcesafesearch.google.com) 설정을 잠그는 서버를 제공합니다. DNS 서버 구성에 대한 **forcesafesearch.google.com**을 가리키는 CNAME 레코드가 포함된 **www.google.com** 및 **www.youtube.com**(및 기타 관련 Google 및 YouTube 국가 하위 도메인)에 대한 DNS 항목을 추가함으로써, 네트워크의 모든 사용자가 Google 또는 YouTube 검색을 수행할 때마다 엄격한 안전 검색 설정을 사용하도록 할 수 있습니다. 그러나 이 솔루션은 방화벽의 Safe Search Enforcement와 호환되지 않습니다. 따라서 이 옵션을 사용하여 Google에서 안전 검색을 강제 실행하는 경우 사용자 지정 URL 카테고리를 생성하고 URL 필터링 프로파일의 차단 목록에 추가하여 방화벽에서 다른 검색 엔진에 대한 액세스를 차단하는 것이 가장 좋습니다. |


©2023 Palo Alto Networks, Inc.

| 검색 공급자 | 세이프서치 설정 설명 |
| --- | --- |
| | • *PAN-OS*는 *HTTP* 헤더 삽입을 통해 *YouTube*에 대한 안전한 검색 시행을 지원합니다. *HTTP* 헤더 삽입은 현재 *HTTP/2*에 대해 지원되지 않습니다. *YouTube*에 대한 안전한 검색을 시행하려면 앱 ID 및 HTTP/2 검사 적절한 복호화 프로파일에서 ***ALPN*** 제거 기능을 사용하여 *HTTP/2* 연결을 *HTTP/1.1*로 다운그레이드합니다.<br>• *Google Lock SafeSearch* 솔루션을 사용하려는 경우 *DNS* 프록시(네트워크 > ***DNS*** 프록시)를 구성하고 상속 소스를 *Layer 3* 인터페이스로 설정하여 방화벽이 *DHCP*를 통해 서비스 제공업체로부터 *DNS* 설정을 수신하는 것을 고려하십시오. *forcesafesearch.google.com* 서버의 로컬 *IP* 주소를 사용하여 *www.google.com* 및 *www.youtube.com*에 대한 정적 항목으로 *DNS* 프록시를 구성합니다. |
| Yahoo | 개별 컴퓨터에서만 안전한 검색을 제공합니다. Yahoo 검색 기본 설정에는 세 가지 SafeSearch 설정이 포함되어 있습니다. 강력, 보통 또는 끄기. 활성화하면 설정이 브라우저 쿠키에 `vm=`으로 저장되고 사용자가 Yahoo 검색을 수행할 때마다 서버에 포워딩됩니다.<br>Yahoo 검색 쿼리 URL에 `vm=r`을 추가하면 가장 엄격한 안전 검색 설정도 가능합니다.<br>*Yahoo* 계정에 로그인한 상태에서 *Yahoo Japan*(***`yahoo.co.jp`***)에서 검색을 수행할 때 최종 사용자는 ***SafeSearch Lock*** 옵션도 활성화해야 합니다. |


©2023 Palo Alto Networks, Inc.

| 검색 공급자 | 세이프서치 설정 설명 |
| --- | --- |
| Bing | 개별 컴퓨터에서 또는 Bing in the Classroom 프로그램을 통해 안전한 검색을 제공합니다. Bing 설정에는 세 가지 SafeSearch 설정이 포함됩니다. 강력, 보통 또는 끄기. 활성화하면 설정이 브라우저 쿠키에 **adtl=**로 저장되고 사용자가 Bing 검색을 수행할 때마다 서버에 포워딩됩니다.<br><br>Bing 검색 쿼리 URL에 **adlt=strict**를 추가하면 가장 엄격한 안전 검색 설정도 활성화됩니다.<br><br>Bing SSL 검색 엔진은 안전 검색 URL 매개변수를 적용하지 않으므로 완전한 안전 검색 적용을 위해 SSL을 통한 Bing 차단을 고려해야 합니다. |

## 엄격한 안전 검색이 활성화되지 않은 경우 검색 결과 차단

기본적으로 안전 검색 시행을 활성화하고 사용자가 가장 엄격한 설정 없이 검색하는 경우 방화벽은 검색 쿼리 결과를 차단하고 브라우저에 URL 필터링 안전 검색 차단 페이지를 표시합니다. 응답 페이지는 최종 사용자가 설정을 조정할 수 있도록 해당 검색 공급자에 대한 검색 설정 페이지에 대한 링크를 제공합니다. 조직의 특정 요구 사항에 맞게 URL 필터링 응답 페이지를 사용자 지정할 수 있습니다. 이 기본 방법을 사용하여 안전 검색을 적용하려는 경우 정책을 구현하기 전에 최종 사용자에게 해당 정책을 전달해야 합니다. 또는 사용자에 대한 안전 검색을 투명하게 활성화하여 수동으로 설정을 구성할 필요가 없도록 할 수 있습니다.

검색 공급자를 위한 안전 검색 설정에는 각 검색 공급자가 안전한 검색을 구현하는 방법이 요약되어 있습니다.

**STEP 1 |** URL 필터링 프로파일에서 안전한 검색 적용을 사용하도록 설정합니다.

1. 개체 > 보안 프로파일 > **URL** 필터링을 선택합니다.
2. 기존 프로파일을 선택하여 수정하거나 기본 프로파일을 복제하여 새 프로파일을 생성합니다.
3. 설정탭에서안전 검색 실행 옵션을 선택합니다.
4. (선택 사항) 사용자를 특정 검색 엔진으로 제한:
   1. 카테고리 탭에서 검색 엔진 카테고리를 설정하여 차단합니다.
   2. 최종 사용자가 액세스할 수 있도록 하려는 각 검색 엔진에 대해 목록 허용 텍스트 상자에 웹 주소를 입력합니다. 예를 들어 사용자가 Google 및 Bing 검색에만 액세스할 수 있도록 하려면 다음을 입력합니다.

      **www.google.com**

      **www.bing.com**
5. 필요에 따라 다른 설정을 구성합니다.
   - 2
   - 차단을 정의하고 URL 카테고리에 관계없이 항상 차단되거나 허용되어야 하는 웹사이트를 목록으로 지정할 수 있도록 합니다.
6. 확인을 클릭하여 프로파일을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 신뢰 영역의 클라이언트에서 인터넷에 트래픽을 허용하는 보안 정책 규칙에 URL 필터링 프로파일을 추가합니다.

1. 정책 > 보안을 선택한 다음 보안 검색 적용을 위해 방금 활성화한 URL 필터링 프로파일을 적용할 규칙을 선택합니다.
2. 작업 탭에서 **URL** 필터링 프로파일을 선택합니다.
3. 확인을 클릭하여 보안 정책 규칙을 저장합니다.

**STEP 3 |** SSL 포워드 프록시 복호화를 사용하도록 설정합니다.

대부분의 검색 엔진은 검색 결과를 암호화하므로 방화벽이 검색 트래픽을 검사하고 안전한 검색 설정을 감지할 수 있도록 SSL 포워드 프록시 복호화를 사용하도록 설정해야 합니다.

1. 검색 사이트에 대한 사용자 지정 URL 카테고리를 추가합니다.
   1. 개체 > 사용자 지정 개체 > **URL** 카테고리를 선택한 다음 사용자 지정 카테고리를 추가합니다.
   2. SearchEngineDecryption과 같은 카테고리에 대한 이름을 입력합니다.
   3. 사이트 목록에 다음을 추가합니다.

      **www.bing.***

      **www.google.***

      **search.yahoo.***
   4. 사용자 지정 URL 카테고리 개체를 저장하려면 확인을 클릭합니다.
2. 단계에 따라 SSL 전달 프록시를 구성합니다..
3. 복호화 정책 규칙의 서비스/**URL** 카테고리 탭에서 방금 생성한 사용자 지정 URL 카테고리를 추가한 다음 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (권장) SSL을 통해 실행되는 Bing 검색 트래픽을 차단합니다.

Bing SSL 검색 엔진은 안전한 검색 설정을 준수하지 않으므로 전체 안전한 검색 적용을 위해 SSL을 통해 실행되는 모든 Bing 세션을 거부해야 합니다.

1. Bing에 대한 사용자 지정 URL 카테고리 추가:
   1. 개체 > 사용자 지정 개체 > **URL** 카테고리를 선택한 다음 사용자 지정 카테고리를 추가합니다.
   2. EnableBingSafeSearch와 같은 카테고리에 대한 이름을 입력합니다.
   3. 사이트 목록에 다음을 추가합니다.

      **www.bing.com/images/***

      **www.bing.com/videos/***
   4. 사용자 지정 URL 카테고리 개체를 저장하려면 확인을 클릭합니다.
2. 방금 만든 사용자 지정 카테고리를 차단하기 위해 다른 URL 필터링 프로파일을 생성합니다.
   1. 개체 > 보안 프로파일 > **URL** 필터링을 선택합니다.
   2. 새 프로파일을 추가하고 설명할 이름을 지정합니다.
   3. 카테고리 목록에서 사용자 지정 카테고리를 찾아 차단하도록 설정합니다.
   4. URL 필터링 프로파일을 저장하려면 확인을 클릭합니다.
3. Bing SSL 트래픽을 차단하려면 보안 정책 규칙을 추가합니다.
   1. 정책 > 보안을 선택한 다음 신뢰 영역에서 인터넷으로의 트래픽을 허용하는 정책 규칙을 추가합니다.
   2. 작업 탭에서 사용자 지정 Bing 카테고리를 차단하기 위해 방금 만든 URL 필터링 프로파일을 첨부합니다.
   3. 서비스/**URL** 카테고리 탭에서 새 서비스를 추가하고 bingssl과 같은 설명 이름을 지정합니다.
   4. **TCP**를 프로토콜로 선택한 다음 대상 포트를 **443**으로 설정합니다.
   5. 규칙을 저장하려면 확인을 클릭합니다.
   6. 이동 옵션을 사용하여 이 규칙이 암전 검색 실행이 활성화된 URL 필터링 프로파일이 있는 규칙 아래에 있도록 합니다.

**STEP 5 |** 구성을 저장합니다.

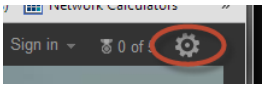
커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

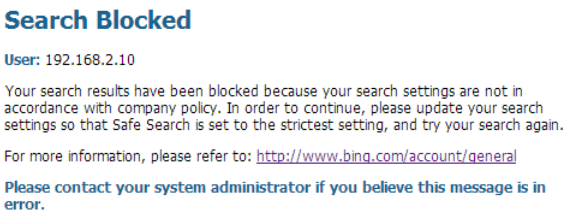
**STEP 6 |** 안전 검색 실행 구성을 확인합니다.

이 확인 단계는 안전한 검색을 적용하기 위해 블록 페이지를 사용하는 경우에만 작동합니다. 투명한 안전 검색 적용을 사용하는 경우 방화벽 블록 페이지에 쿼리 문자열의 안전한 검색 매개변수가 있는 URL 다시 쓰기가 호출됩니다.

1. 방화벽 뒤에 있는 컴퓨터에서 지원되는 검색 공급자 중 하나에 대한 엄격한 검색 설정을 사용하지 않도록 설정합니다. 예를 들어, bing.com에서 Bing 메뉴 모음의 기본 설정 아이콘을 클릭합니다.




2. **SafeSearch** 옵션을 보통 또는 끄기로 설정하고 저장을 클릭합니다.
3. Bing 검색을 수행하고 URL 필터링 안전 검색 블록 페이지가 검색 결과 대신 표시되는지 확인합니다.




4. 차단 페이지의 링크를 사용하여 검색 공급자의 검색 설정으로 이동하고 안전 검색 설정을 다시 가장 엄격한 설정(Bing의 경우 **Strict**)으로 설정한 다음 저장을 클릭합니다.
5. Bing에서 다시 검색을 수행하고 필터링된 검색 결과가 블록 페이지 대신 표시되는지 확인합니다.

## 투명하게 사용자를 위한 세이프서치 활성화

가장 엄격한 안전한 검색 필터로 검색 결과의 필터링을 적용하려는 경우 최종 사용자가 수동으로 설정을 구성하지 않도록 하려면 다음과 같이 투명한 안전한 검색 적용을 활성화할 수 있습니다. 이 기능은 Google, Yahoo 및 Bing 검색 엔진에서만 지원되며 콘텐츠 릴리스 버전 475 이상이 필요합니다.

**STEP 1 |** 방화벽이 콘텐츠 릴리스 버전 475 이상을 실행하고 있는지 확인합니다.

1. 디바이스 > 동적 업데이트를 선택합니다.
2. 애플리케이션 및 위협 섹션을 확인하여 현재 실행 중인 업데이트를 확인합니다.
3. 방화벽이 필요한 업데이트 또는 그 이후에 실행되지 않는 경우 지금 확인을 클릭하여 사용 가능한 업데이트 목록을 검색합니다.
4. 필요한 업데이트를 찾고 다운로드를 클릭합니다.
5. 다운로드가 완료되면 설치를 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** URL 필터링 프로파일에서 안전한 검색 적용을 사용하도록 설정합니다.

1. 개체 > 보안 프로파일 > **URL** 필터링을 선택합니다.
2. 기존 프로파일을 선택하여 수정하거나 기본 프로파일을 복사하여 새 프로파일을 생성합니다.
3. 설정 탭에서 안전 검색 실행 체크박스를 선택하여 활성화합니다.
4. (선택 사항) 특정 검색 엔진에만 액세스 허용:
   1. 카테고리 탭에서 검색 엔진 카테고리를 설정하여 차단합니다.
   2. 최종 사용자가 액세스할 수 있도록 하려는 각 검색 엔진에 대해 목록 허용 텍스트 상자에 웹 주소를 입력합니다. 예를 들어 사용자가 Google 및 Bing 검색에만 액세스할 수 있도록 하려면 다음을 입력합니다.

      **www.google.com**

      **www.bing.com**
5. 필요에 따라 다른 설정을 구성합니다.
   - 각 URL 카테고리에 대한 사이트 액세스를 정의합니다.
   - 차단을 정의하고 URL 카테고리에 관계없이 항상 차단되거나 허용되어야 하는 웹사이트를 목록으로 지정할 수 있도록 합니다.
6. 확인을 클릭하여 프로파일을 저장합니다.

**STEP 3 |** 신뢰 영역의 클라이언트에서 인터넷에 트래픽을 허용하는 보안 정책 규칙에 URL 필터링 프로파일을 추가합니다.

1. 정책 > 보안을 선택한 다음 보안 검색 적용을 위해 방금 활성화한 URL 필터링 프로파일을 적용할 규칙을 선택합니다.
2. 작업 탭에서 **URL** 필터링 프로파일을 선택합니다.
3. 확인을 클릭하여 보안 정책 규칙을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** (권장) SSL을 통해 실행되는 Bing 검색 트래픽을 차단합니다.

Bing SSL 검색 엔진은 안전한 검색 설정을 준수하지 않으므로 전체 안전한 검색 적용을 위해 SSL을 통해 실행되는 모든 Bing 세션을 거부해야 합니다.

1. Bing에 대한 사용자 지정 URL 카테고리 추가:
   1. 개체 > 사용자 지정 개체 > **URL** 카테고리를 선택한 다음 사용자 지정 카테고리를 추가합니다.
   2. EnableBingSafeSearch와 같은 카테고리에 대한 이름을 입력합니다.
   3. 사이트 목록에 다음을 추가합니다.

      **www.bing.com/images/***

      **www.bing.com/videos/***
   4. 사용자 지정 URL 카테고리 개체를 저장하려면 확인을 클릭합니다.
2. 방금 만든 사용자 지정 카테고리를 차단하기 위해 다른 URL 필터링 프로파일을 생성합니다.
   1. 개체 > 보안 프로파일 > **URL** 필터링을 선택합니다.
   2. 새 프로파일을추가하고 설명할 이름을 지정합니다.
   3. 카테고리 목록에서 방금 만든 사용자 지정 카테고리를 찾아 차단하도록 설정합니다.
   4. URL 필터링 프로파일을 저장하려면 확인을 클릭합니다.
3. Bing SSL 트래픽을 차단하려면 보안 정책 규칙을 추가합니다.
   1. 정책 > 보안을 선택한 다음 신뢰 영역에서 인터넷으로의 트래픽을 허용하는 정책 규칙을 추가합니다.
   2. 작업 탭에서 사용자 지정 Bing 카테고리를 차단하기 위해 방금 만든 URL 필터링 프로파일을 첨부합니다.
   3. 서비스/**URL** 카테고리 탭에서 새 서비스를 추가하고 bingssl과 같은 설명 이름을 지정합니다.
   4. **TCP**를 프로토콜로 선택한 다음 대상 포트를 **443**으로 설정합니다.
   5. 규칙을 저장하려면 확인을 클릭합니다.
   6. **Move** 옵션을 사용하여 이 규칙이 안전한 검색 적용을 사용하도록 설정한 URL 필터링 프로파일이 있는 규칙 아래에 있는지 확인합니다.

**STEP 5 |** URL 필터링 안전 검색 블록 페이지를 편집하고 기존 코드를 JavaScript로 교체하여 검색 쿼리 URL을 다시 작성하여 안전한 검색을 투명하게 적용합니다.

1. 디바이스 > 응답 페이지 > **URL** 필터링 세이프 서치 차단 페이지를 선택합니다.
2. 미리 정의됨을 선택한 다음 내보내기를 클릭하여 파일을 로컬에 저장합니다.
3. HTML 편집기를 사용하고 기존 블록 페이지 텍스트를 모두 다음 텍스트로 교체한 다음 파일을 저장합니다.

```
<html> <head> <title>Search Blocked</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
```


©2023 Palo Alto Networks, Inc.

```
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>Search Blocked</h1> <p> <b>User:</b> <user/> </p>
 <p>검색 설정이 회사 정책에 맞지 않아 검색 결과가 차단되었습니
다. 계속하려면 안전 검색이 가장 엄격한 설정으로 설정되도록 검색 설
정을 업데이트하십시오. 현재 계정에 로그인되어 있는 경우 안전 검색
을 잠그고 검색을 다시 시도하십시오.</p> <p> 자세한 내용은 다음
을 참조하세요. <a href="<ssurl/>"> <ssurl/> </a> </p> <p
 id="java_off"> 브라우저에서 JavaScript를 활성화하세요.<br></p>
 <p><b>이 메시지가 오류라고 생각되면 시스템 관리자에게 문의하세요.</
b></p> </div> </body> <script> // 브라우저에 있는 URL을 가져
옵니다. var s_u = 위치.href; //bing // 시작 부분의 슬래시와 일
치하고 그 다음 ".bing"과 일치합니다. 그런 다음 욕심이 없는 슬래
시가 뒤따릅니다. Hopefully the first forward slash. var b_a
 = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a) { s_u
 = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'You are
 being redirected to a safer search!'; } //google // 시
작 부분의 슬래시와 일치하고 그 다음 ".google"과 일치합니다. 그
런 다음 욕심 없는 슬래시가 뒤따릅니다. 바라건대 첫 번째 슬래
시. var g_a = /^.*\/\/(.+\.google\..+?)\//.exec(s_u);
 if (g_a) { s_u = s_u.replace(/&safe=off/ig,""); s_u
 = s_u + "&safe=활성"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 '더 안전한 검색으로 리디렉션됩니다!'; } //yahoo // 시작 부
분의 슬래시와 일치하고, 그 다음 ".yahoo."" 그 다음에는 욕심
이 없는 슬래시가 오는 모든 항목과 일치합니다. Hopefully the
 first forward slash. var y_a = /^.*\/\/(.+\.yahoo\..
+?)\//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

**STEP 6 |** 편집된 URL 필터링 안전 검색 블록 페이지를 방화벽에 가져옵니다.

1. 편집된 차단 페이지를 가져오려면 디바이스 > 응답 페이지 > **URL** 필터링 세이프 서치 차단 페이지를 선택합니다.
2. 가져오기를 클릭한 다음 파일 가져오기 필드에 경로와 파일 이름을 입력하거나 파일을 찾아봅니다.
3. (선택 사항) 대상 드롭다운에서 이 로그인 페이지를 사용할 가상 시스템을 선택하거나 모든 가상 시스템에서 사용할 수 있도록 공유를 선택합니다.
4. 확인을 클릭하여 파일을 가져옵니다.


©2023 Palo Alto Networks, Inc.

**STEP 7 |** SSL 포워드 프록시 복호화를 사용하도록 설정합니다.

대부분의 검색 엔진은 검색 결과를 암호화하므로 방화벽이 검색 트래픽을 검사하고 안전한 검색 설정을 감지할 수 있도록 SSL 포워드 프록시 복호화를 사용하도록 설정해야 합니다.

1. 검색 사이트에 대한 사용자 지정 URL 카테고리를 추가합니다.
   1. 개체 > 사용자 지정 개체 > **URL** 카테고리를 선택한 다음 사용자 지정 카테고리를 추가합니다.
   2. SearchEngineDecryption과 같은 카테고리에 대한 이름을 입력합니다.
   3. 사이트 목록에 다음을 추가합니다.

      **www.bing.***

      **www.google.***

      **search.yahoo.***
   4. 사용자 지정 URL 카테고리 개체를 저장하려면 확인을 클릭합니다.
2. 단계에 따라 SSL 전달 프록시를 구성합니다..
3. 복호화 정책 규칙의 서비스/**URL** 카테고리 탭에서 방금 생성한 사용자 지정 URL 카테고리를 추가한 다음 확인을 클릭합니다.

**STEP 8 |** 구성을 저장합니다.

커밋을 클릭합니다.

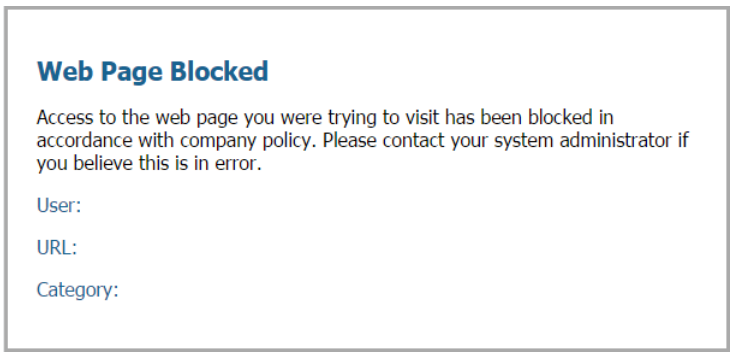

©2023 Palo Alto Networks, Inc.

# URL 필터링 응답 페이지

방화벽은 사용자가 URL 필터링 프로파일(차단, 계속 또는 재정의)의 차단 작업 중 하나로 구성된 범주의 사이트를 탐색하거나 컨테이너 페이지가 활성화된 경우, 기본적으로 표시되는 3개의 미리 정의된 응답 페이지를 제공합니다.

- **URL** 필터링 및 카테고리 일치 차단 페이지

  URL 필터링 프로파일에 의해 또는 URL 카테고리가 보안 정책 규칙에 의해 차단되어 액세스가 차단되었습니다.




- **URL** 필터링 계속 및 재정의 페이지

  사용자가 계속을 클릭하여 차단을 우회할 수 있도록 하는 초기 차단 정책이 있는 페이지입니다. URL 관리 무시가 활성화된 상태에서(특정 사이트에 대한 암호 액세스 허용) 계속을 클릭한 후 사용자는 URL을 차단하는 정책을 무시하기 위해 암호를 제공해야 합니다.

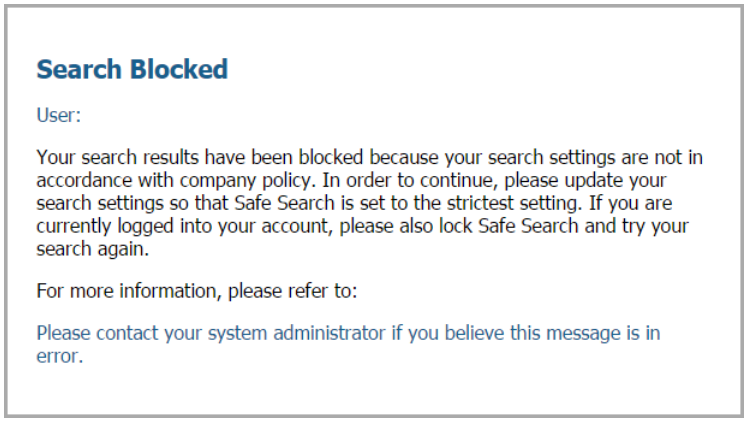



- **URL** 필터링 안전 검색 차단 페이지

  Safe Search Enforcement 옵션이 활성화된 URL 필터링 프로파일이 있는 보안 정책 규칙에 의해 액세스가 차단되었습니다(Safe Search Enforcement 참조). Google, Bing, Yahoo 또는 Yandex를 사용하여

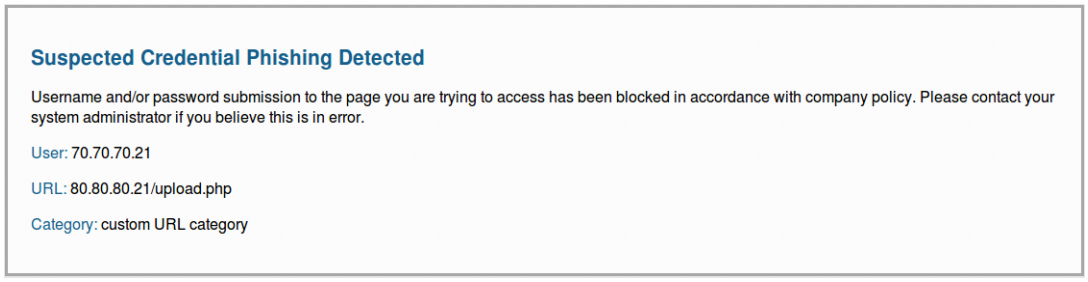

©2023 Palo Alto Networks, Inc.

검색을 수행하고 Safe Search에 대한 브라우저 또는 검색 엔진 계정 설정이 엄격함으로 설정되지 않은 경우 사용자에게 이 페이지가 표시됩니다.




- 안티 피싱 차단 페이지

  이 페이지는 사용자가 자격 증명 제출이 차단된 카테고리의 웹 페이지에 회사 자격 증명(사용자명 또는 암호)을 입력하려고 할 때 표시됩니다. 사용자는 계속해서 사이트에 액세스할 수 있지만 연결된 웹 양식에 유효한 회사 자격 증명을 제출할 수는 없습니다. 사용자가 회사 자격 증명을 제출할 수 있는 사이트를 제어하려면 URL 카테고리를 기반으로 자격 증명 피싱을 방지하도록 방화벽을 User-ID로 구성하고 활성화해야 합니다.




- 안티 피싱 계속 페이지

  이 페이지는 웹사이트에 자격 증명(사용자명 및 암호)을 제출하지 않도록 사용자에게 경고합니다. 자격 증명 제출에 대해 사용자에게 경고하면 기업 자격 증명을 재사용하지 못하도록 하고 피싱 시도 가능성에 대해 교육할 수 있습니다. 사이트의 자격 증명으로 진행하려면 계속을 선택해야 합니다. 사용자가 회사 자격 증명을 제출할 수 있는 사이트를 제어하려면 URL 카테고리를 기반으로 자격 증명 피싱을 방지하도록 방화벽을 User-ID로 구성하고 활성화해야 합니다.




 ©2023 Palo Alto Networks, Inc.

라이선스된 페이지를 사용하거나 URL 필터링 응답 페이지를 사용자 정의하여 특정 사용 정책 및/또는 기업 브랜딩을 포워딩할 수 있습니다. 또한 차단 이벤트 시 URL 필터링 응답 페이지 변수를 대체용으로 사용하거나 지원되는 응답 페이지 참조 중 하나를 외부 이미지, 사운드 또는 스타일 시트에 추가할 수 있습니다.

방화벽이 SSL/TLS 핸드쉐이크를 검사하도록 설정한 경우 브라우저는 응답 페이지를 표시하지 않습니다.

표 **2: URL** 필터링 응답 페이지 변수

| 가변성 | 용법 |
|---|---|
| <user/> | 방화벽은 응답 페이지를 표시할 때 변수를 사용자명(User-ID를 통해 사용 가능한 경우) 또는 사용자의 IP 주소로 바꿉니다. |
| <url/> | 방화벽은 응답 페이지를 표시할 때 변수를 요청된 URL로 바꿉니다. |
| <category/> | 방화벽은 변수를 차단된 요청의 URL 필터링 카테고리로 바꿉니다. |
| <pan_form/> | URL 필터링 계속 및 재정의 페이지에 계속 버튼을 표시하기 위한 HTML 코드입니다. |

사용자가 액세스하려는 URL 카테고리에 따라 다른 메시지를 표시하도록 방화벽을 트리거하는 코드를 추가할 수도 있습니다. 예를 들어 응답 페이지의 다음 코드 조각은 URL 카테고리가 게임인 경우 메시지 1, 카테고리가 여행인 경우 메시지 2, 어린이 카테고리인 경우 메시지 3을 표시하도록 지정합니다.

```
var cat = "<category/>"; switch(cat) { case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break; case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break; case 'kids': document.getElementById("warningText").innerHTML
 = "Message 3"; break; }
```

각 블록 페이지 유형에 대해 각 가상 시스템에 하나의 HTML 페이지만 로드할 수 있습니다. 그러나 이미지, 사운드 및 CSS 파일(Cascading Style Sheet)과 같은 다른 리소스는 브라우저에 응답 페이지가 표시될 때 다른 서버에서 로드될 수 있습니다. 모든 참조에는 정규화된 URL이 포함되어야 합니다.

표 **3:** 응답 페이지 참조

| 참조 유형 | **HTML** 코드 예 |
|---|---|
| 영상 | `<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">` |


©2023 Palo Alto Networks, Inc.

| 참조 유형 | **HTML** 코드 예 |
| --- | --- |
| 소리 | `<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">` |
| 스타일 시트 | `<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />` |
| 하이퍼링크 | `<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">기업 정책 보기</a>` |


©2023 Palo Alto Networks, Inc.

# URL 필터링 응답 페이지 사용자 지정

방화벽은 다음과 같은 경우에 기본적으로 표시되는 사전 정의된 URL 필터링 응답 페이지를 제공합니다.

- 사용자가 액세스가 제한된 카테고리의 사이트를 탐색하려고 시도합니다.
- 사용자는 자격 증명 검색이 활성화된 사이트에 유효한 회사의 자격 증명을 제출합니다(URL 카테고리 기준 자격 증명 피싱 방지).
- 사용자가 방문한 페이지만 기록이(가) 검색 시도를 차단합니다.

그러나 회사 브랜딩, 허용 가능한 사용 정책 및 내부 리소스에 대한 링크로 사용자 지정 응답 페이지를 만들 수 있습니다.

지원되는 최대 크기보다 큰 사용자 지정 응답 페이지는 해독되거나 사용자에게 표시되지 않습니다. *PAN-OS 8.1.2* 및 이전 *PAN-OS 8.1* 릴리스에서 해독된 사이트의 사용자 지정 응답 페이지는 *8,191*바이트를 초과할 수 없습니다. 최대 크기는 *PAN-OS 8.1.3* 및 이후 릴리스에서 *17,999*바이트로 증가합니다.

**STEP 1 |** 기본 응답 페이지를 내보냅니다.

1. 디바이스 > 응답 페이지를 선택합니다.
2. 수정할 URL 필터링 응답 페이지의 링크를 선택합니다.
3. 응답 페이지(사전 정의 또는 공유)를 클릭한 다음 내보내기 링크를 클릭하고 파일을 바탕 화면에 저장합니다.

**STEP 2 |** 내보낸 페이지를 편집합니다.

1. 선택한 HTML 텍스트 편집기에서 페이지를 편집합니다.
   - 응답 페이지가 차단된 특정 사용자, URL 또는 카테고리에 대한 사용자 지정 정보를 표시하려면 지원되는 응답 페이지 변수 중 하나 이상을 추가합니다.
   - 사용자 지정 이미지(예: 회사 로고), 사운드 또는 스타일 시트 또는 다른 URL에 대한 링크(예: 허용 가능한 웹 사용 정책이 상술된 문서)를 포함하려면 지원되는 응답 페이지 참조 중 하나 이상을 포함합니다.
2. 편집한 페이지를 새 파일 이름으로 저장합니다. 페이지가 UTF-8 인코딩을 유지했는지 확인합니다. 예를 들어 메모장에서 다른 이름으로 저장 대화 상자의 인코딩 드롭다운에서 **UTF-8**을 선택합니다.

**STEP 3 |** 사용자 지정된 응답 페이지를 가져옵니다.

1. 디바이스 > 응답 페이지를 선택합니다.
2. 편집한 URL 필터링 응답 페이지에 해당하는 링크를 선택합니다.
3. 가져오기를 클릭한 다음 파일 가져오기 필드에 경로와 파일 이름을 입력하거나 파일을 찾아봅니다.
4. (선택 사항) 대상 드롭다운에서 이 로그인 페이지를 사용할 가상 시스템을 선택하거나 모든 가상 시스템에서 사용할 수 있도록 공유를 선택합니다.
5. 확인을 클릭하여 파일을 가져옵니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 새 응답 페이지를 저장합니다.

변경 사항을 커밋합니다.

**STEP 5 |** 새 응답 페이지가 표시되는지 확인합니다.

브라우저에서 응답 페이지를 트리거하는 URL로 이동합니다. 예를 들어 수정된 URL 필터링 및 카테고리 일치 응답 페이지를 보려면 URL 필터링 정책이 차단하도록 설정된 URL로 이동합니다.

방화벽은 다음 포트를 사용하여 URL 필터링 응답 페이지를 표시합니다.

- **HTTP** - 6080
- 방화벽 인증서가 있는 기본 **TLS** - 6081
- 사용자 지정 **SSL/TLS** 프로파일 - 6082


©2023 Palo Alto Networks, Inc.

# HTTP 헤더 로깅

URL 필터링을 통해 네트워크의 웹 트래픽을 가시성과 제어할 수 있습니다. 웹 콘텐츠에 대한 가시성을 향상시키기 위해 URL 필터링 프로파일을 구성하여 웹 요청에 포함된 HTTP 헤더 특성을 기록할 수 있습니다. 클라이언트가 웹 페이지를 요청하면 HTTP 헤더에는 사용자 에이전트, 참조자 및 x-forward-for 필드가 속성 값 쌍으로 포함되어 웹 서버로 포워딩됩니다. HTTP 헤더로 로깅할 수 있도록 활성화하면 방화벽은 URL 필터링 로그에서 다음 특성 값 쌍을 기록합니다.

***HTTP*** 헤더를 사용하여 ***SaaS*** 애플리케이션에 대한 액세스를 관리할 수도 있습니다**.** 이렇게 하려면 ***URL*** 필터링 라이선스가 필요하지 않지만 ***URL*** 필터링 프로파일을 사용하여 이 기능을 켜야 합니다**.**

| 속성 | 설명 |
|---|---|
| 사용자 에이전트 | 사용자가 URL에 액세스하는 데 사용한 웹 브라우저(예: Internet Explorer)입니다. 이 정보는 서버에 대한 HTTP 요청으로 전송됩니다.<br>HTTP 헤더에는 사용자 에이전트의 전체 문자열이 포함되지 않습니다. 헤더 엔드가 포함된 패킷 앞에 있는 패킷의 최대 로깅 바이트는 36바이트입니다. |
| 추천인 | 사용자를 다른 웹 페이지에 연결한 웹 페이지의 URL; 요청 중인 웹 페이지로 사용자를 리디렉션(참조)하는 소스입니다. |
| X-Forward-For(XFF) | 웹 페이지를 요청한 사용자의 IP 주소를 보존하는 HTTP 요청 헤더 필드의 옵션입니다. 네트워크에 프록시 서버가 있는 경우 XFF를 사용하면 프록시 서버의 IP 주소를 웹 페이지를 요청한 소스 IP 주소로만 기록하는 대신 콘텐츠를 요청한 사용자의 IP 주소를 식별할 수 있습니다. |
| 헤더 삽입 | 방화벽이 삽입하는 헤더 유형과 헤더 텍스트입니다. |


©2023 Palo Alto Networks, Inc.

# URL 카테고리 변경 요청

URL이 정확하게 분류되지 않았다고 생각되면 다른 분류를 요청할 수 있습니다. 방화벽에서 직접 변경 요청을 제출하거나 Test A Site를 사용하십시오. 변경 요청은 URL 필터링 클라우드인 PAN-DB를 트리거하여 카테고리 변경을 제안하는 URL을 즉시 분석합니다. PAN-DB가 새 카테고리 제안이 정확한지 확인하면 변경 요청이 승인됩니다. PAN-DB가 새로운 카테고리 제안이 정확하지 않다고 판단되면 Palo Alto Networks 위협 연구 및 데이터 사이언스 팀의 편집자가 변경 요청을 검토합니다.

변경 요청을 제출하면 요청이 접수되었음을 확인하는 이메일을 받게 됩니다. 검토가 완료되면 결과를 확인하는 두 번째 이메일을 받게 됩니다.

URL이 받는 위험 카테고리(높은 위험, 중간 위험 또는 낮은 위험) 또는 콘텐츠가 불충분하거나 새로 등록된 도메인으로 분류된 URL에 대해서는 변경을 요청할 수 없습니다.

- 온라인으로 변경 요청하기
- 일괄 변경 요청하기
- 방화벽에서 변경 요청하기

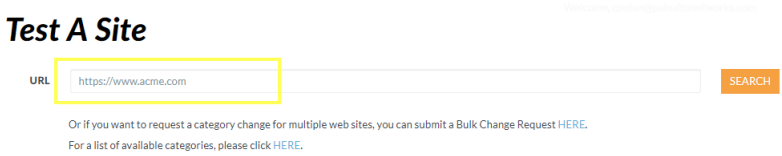
## 온라인으로 변경 요청하기

온라인으로 변경 요청을 하려면 Palo Alto Networks URL Filtering Test A Site를 방문하십시오.

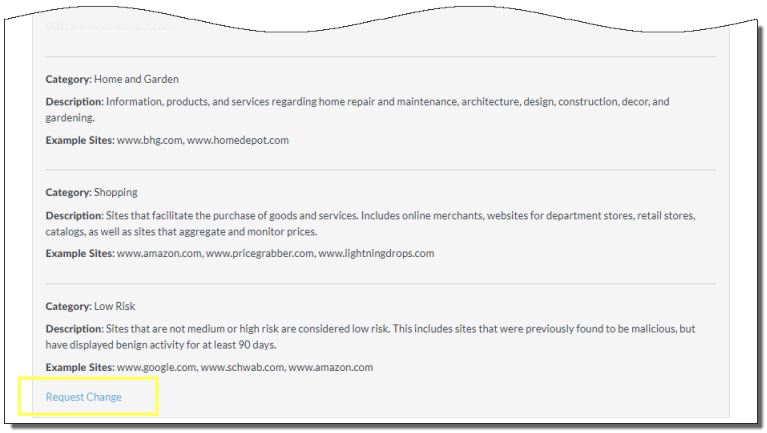
**STEP 1 |** Test A Site로 이동합니다.

변경 요청을 제출하기 위해 로그인할 필요는 없지만 변경 요청 양식의 일부로 이메일을 제공해야 합니다. 로그인하지 않기로 결정한 경우 CAPTCHA 테스트를 수행하여 기계가 아님을 확인해야 합니다(CAPTCHA 테스트를 피하기 위해 로그인).

**STEP 2 |** 카테고리를 확인하려면 URL을 입력하세요.



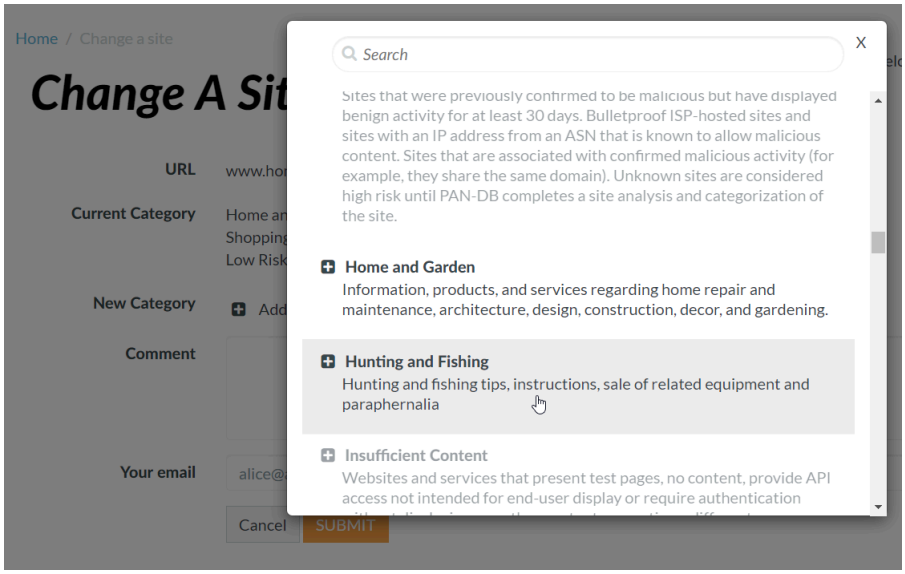

**STEP 3 |** URL 카테고리를 검토하고 정확하지 않다고 생각되면 변경 요청을 선택합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 계속해서 변경 요청 양식을 채우고 제출합니다.

최소 하나(최대 2개)의 새 카테고리 제안을 포함하고 제안에 대해 자세히 알려주려면 댓글(선택 사항)을 남겨주세요.



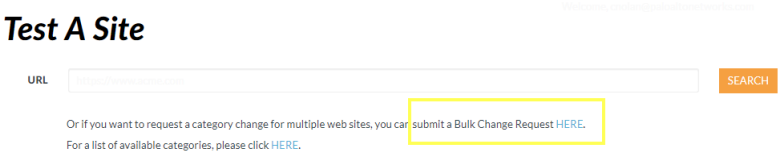

## 일괄 변경 요청하기

Test A Site를 사용하여 한 번에 여러 URL에 대한 변경 요청을 제출하려는 일괄 변경 요청을 만들 수도 있습니다.

**STEP 1 |** Test A Site로 이동합니다.

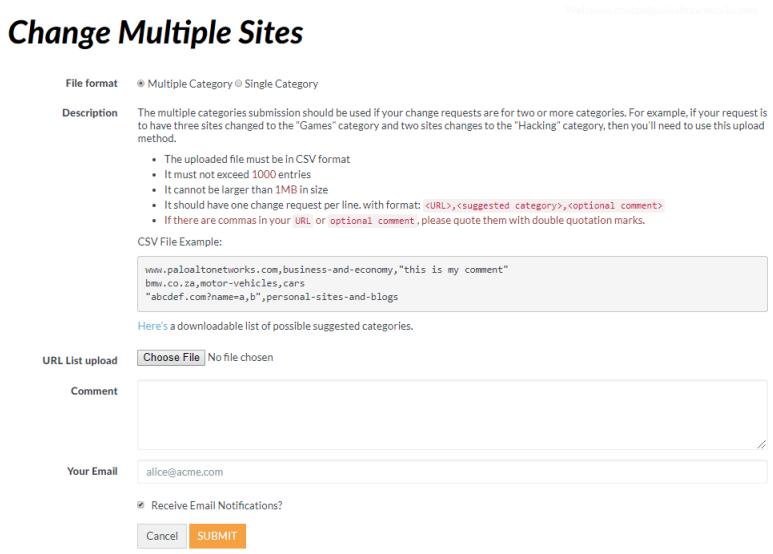
변경 요청을 하기 위해 로그인할 필요가 없습니다. 그러나 변경 요청 양식을 작성할 때 이메일을 제공해야 합니다. 로그인하지 않기로 결정한 경우 CAPTCHA 테스트를 수행하여 기계가 아님을 확인해야 합니다(CAPTCHA 테스트를 피하기 위해 로그인).

**STEP 2 |** 일괄 변경 요청을 제출하는 옵션을 선택합니다.



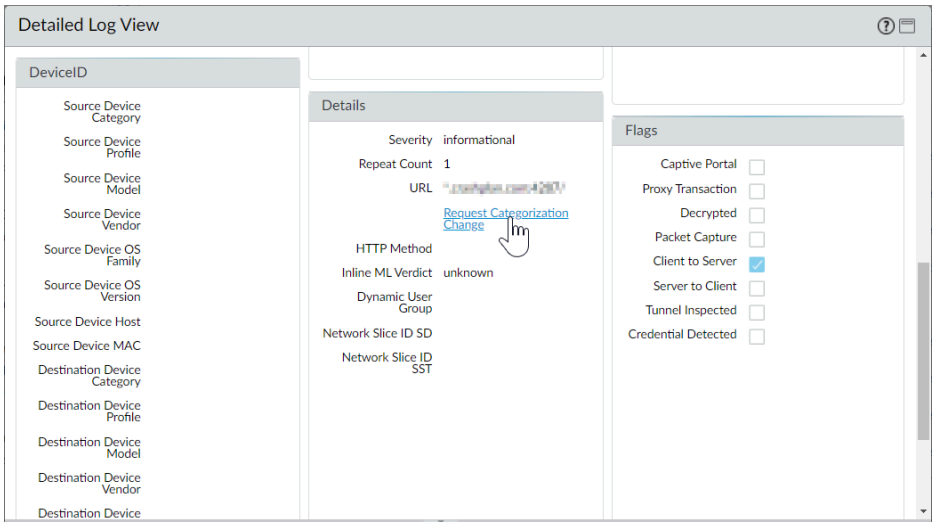

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 일괄 변경 요청 양식을 작성하여 제출합니다.



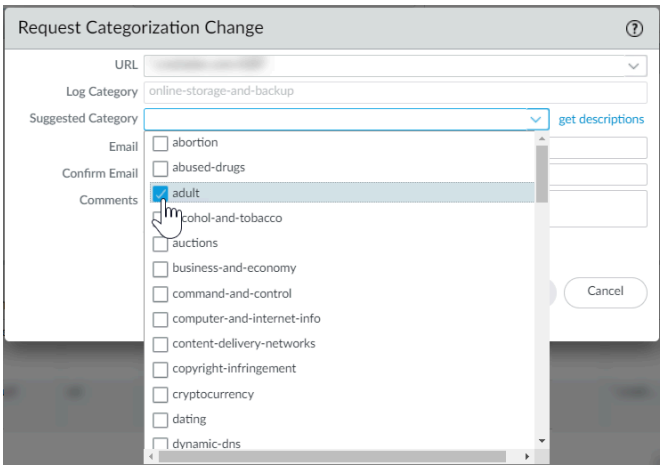

## 방화벽에서 변경 요청하기

방화벽에서 직접 URL 카테고리 변경 요청을 제출할 수도 있습니다. URL 필터링 로그에서 각 로그 항목에 대한 세부 정보에는 분류 변경 요청(**Logs** > **URL** 필터링 > 모니터링) 옵션이 포함됩니다.




여기에서 요청 양식을 작성하고 제출할 수 있습니다.


©2023 Palo Alto Networks, Inc.





©2023 Palo Alto Networks, Inc.

# URL 필터링 문제 해결

다음 항목에서는 일반적인 URL 필터링 문제를 진단하고 해결하기 위한 문제 해결 지침을 제공합니다.

- 고급 URL 필터링 활성화 문제
- PAN-DB 클라우드 연결 문제
- 미해결로 분류된 URL
- 잘못된 분류

## 고급 URL 필터링 활성화 문제

다음 워크플로를 사용하여 고급 URL 필터링 활성화 문제를 해결합니다.

**STEP 1 |** PAN-OS CLI에 액세스합니다.

**STEP 2 |** 다음 명령을 실행하여 고급 URL 필터링이 활성화되었는지 확인합니다.

```
show system setting url-database
```

응답이 **paloaltonetworks**인 경우 Palo Alto Networks URL 필터링 데이터베이스인 PAN-DB가 활성 공급업체입니다.

**STEP 3 |** 다음 명령을 실행하여 방화벽에 유효한 고급 URL 필터링 라이선스가 있는지 확인합니다.

```
request license info
```

라이선스 항목 **기능이 표시됩니다. 고급 URL 필터링**. 라이선스가 설치되지 않은 경우 라이선스를 가져오고 설치해야 합니다. URL 필터링 구성을(를) 참조하십시오.

**STEP 4 |** PAN-DB 클라우드 연결 상태를 확인합니다.

## PAN-DB 클라우드 연결 문제

*PAN-DB* 클라우드에 대한 연결을 보장하려면 모든 *Palo Alto Management Service* 트래픽을 허용하는 전용 보안 정책 규칙을 생성하세요. 이렇게 하면 관리 트래픽이 **확인되지 않음**으로 분류되는 것을 방지하고 데이터플레인을 통해 라우팅될 때 트래픽이 차단되는 것을 방지할 수 있습니다.

방화벽과 PAN-DB 클라우드 간의 연결을 확인하려면 다음 단계를 따르세요.

```
URL 클라우드 상태 표시
```

클라우드에 액세스할 수 있는 경우 예상 응답은 다음과 유사합니다.

```
show url-cloud status PAN-DB URL Filtering License : valid
 Current cloud server : serverlist.urlcloud.paloaltonetworks.com
 Cloud connection : connected Cloud mode : public URL database
 version - device : 20200624.20296 URL database version - cloud :
```


©2023 Palo Alto Networks, Inc.

```
20200624.20296 ( last update time 2020/06/24 12:39:19 ) URL
database status : good URL protocol version - device : pan/2.0.0 URL
protocol version - cloud : pan/2.0.0 Protocol compatibility status :
compatible
```

클라우드에 액세스할 수 없는 경우 예상 응답은 다음과 유사합니다.

```
show url-cloud status PAN-DB URL Filtering License : valid Cloud
connection : not connected URL database version - device :
0000.00.00.000 URL protocol version - device : pan/0.0.2
```

다음 체크리스트를 사용하여 연결 문제를 식별하고 해결합니다.

- PAN-DB URL 필터링 라이선스 필드가 유효하지 않은 것으로 표시됩니까? 유효한 PAN-DB 라이선스를 획득하고 설치합니다.
- URL 프로토콜 버전이 호환되지 않는 것으로 표시됩니까? PAN-OS를 최신 버전으로 업그레이드합니다.
- 방화벽에서 PAN-DB 클라우드 서버를 핑(ping)할 수 있습니까? 다음 명령을 실행하여 확인합니다.

  ```
  ping source <ip-address> host
  serverlist.urlcloud.paloaltonetworks.com <
  ```

  예를 들어 관리 인터페이스 IP 주소가 10.1.1.5인 경우 다음 명령을 실행합니다.

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- 방화벽이 HA 구성에 있습니까? 방화벽의 HA 상태가 능동형, 능동형-기본 또는 능동형-보조 상태에 있는지 확인합니다. 방화벽이 다른 상태에 있는 경우 PAN-DB 클라우드에 대한 액세스가 차단됩니다. 쌍의 각 방화벽에서 다음 명령을 실행하여 상태를 확인합니다.

  ```
  show high-availability state
  ```

방화벽과 PAN-DB 클라우드 간의 연결에 문제가 있는 경우에도 Palo Alto Networks 지원팀에 문의하십시오.

## 미해결로 분류된 URL

URL은 PAN-DB URL 필터링 클라우드 서비스에 대한 연결이 중단되어 URL 조회에 실패한 경우 해결되지 않은 것으로 분류됩니다. 클라우드 연결 상태 및 URL 분류는 만료된 구독 라이선스 또는 라이선스가 없는 사용자에게는 적용되지 않습니다.

다음 워크플로를 사용하여 PAN-DB에 의해 식별되는 일부 또는 전체 URL이 해결되지 않은 것으로 분류되는 이유를 해결하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 다음 명령을 실행하여 PAN-DB 클라우드 연결을 확인하십시오.

**URL 클라우드 상태 표시**

클라우드 연결: 필드에 **연결됨**이 표시되어야 합니다. **연결된** 것 외에 다른 것이 표시되면 Management Plane(MP) 캐시에 존재하지 않는 모든 URL은 **확인되지 않은 것**으로 분류됩니다. 이 문제를 해결하려면 PAN-DB 클라우드 연결 문제를 참조하십시오.

**STEP 2 |** 클라우드 연결 상태가 **연결됨**으로 표시되면 현재 방화벽 사용률을 확인하세요. 방화벽 사용률이 급증하는 경우 URL 요청이 삭제될 수 있으며(Management Plane(MP)에 도달하지 못할 수 있음) **미해결**로 분류됩니다.

시스템 리소스를 보려면 다음 명령을 실행하고 **%CPU** 및 **%MEM** 열을 봅니다.

**시스템 리소스 표시**

웹 인터페이스의 대시보드에 있는 시스템 리소스 위젯에서 시스템 리소스를 볼 수도 있습니다.

**STEP 3 |** 문제가 지속되면 Palo Alto Networks 지원에 문의하십시오.

## 잘못된 분류

때로는 잘못 분류되었다고 생각되는 URL을 발견할 수 있습니다. 다음 워크플로를 사용하여 사이트의 URL 분류를 결정하고 해당하는 경우 카테고리 변경을 요청합니다.

**STEP 1 |** 다음 명령을 실행하여 데이터플레인에서 카테고리를 확인합니다.

```
show running url <URL>
```

예를 들어 Palo Alto Networks 웹사이트의 카테고리를 보려면 다음 명령을 실행합니다.

```
show running url paloaltonetworks.com
```

데이터플레인 캐시에 저장된 URL에 올바른 카테고리(이 예에서는 컴퓨터 및 인터넷 정보)가 있는 경우 카테고리화가 적절하며 추가 작업이 필요하지 않습니다. 카테고리가 올바르지 않으면 다음 단계를 계속합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 다음 명령을 실행하여 Management Plane(MP)의 카테고리인지 확인합니다.

```
test url-info-host <URL>
```

예:

```
test url-info-host paloaltonetworks.com
```

Management Plane(MP) 캐시에 저장된 URL에 올바른 카테고리가 있는 경우 다음 명령을 실행하여 데이터플레인 캐시에서 URL을 제거합니다.

```
clear url-cache url <URL>
```

다음에 방화벽이 이 URL에 대한 카테고리를 요청할 때 요청은 Management Plane(MP)으로 포워딩됩니다. 이렇게 하면 문제가 해결되며 추가 조치가 필요하지 않습니다. 그래도 문제가 해결되지 않으면 다음 단계로 이동하여 클라우드 시스템에서 URL 카테고리를 확인하십시오.

**STEP 3 |** 다음 명령을 실행하여 클라우드에서 카테고리를 확인합니다.

```
test url-info-cloud <URL>
```

**STEP 4 |** 클라우드에 저장된 URL에 올바른 카테고리가 있는 경우 데이터플레인 및 Management Plane(MP) 캐시에서 URL을 제거합니다.

다음 명령을 실행하여 데이터플레인 캐시에서 URL을 삭제합니다.

```
clear url-cache url <URL>
```

다음 명령을 실행하여 Management Plane(MP) 캐시에서 URL을 삭제합니다.

```
delete url-database url <URL>
```

다음에 방화벽이 지정된 URL의 카테고리를 쿼리할 때 요청은 Management Plane(MP)으로 포워딩된 다음 클라우드로 포워딩됩니다. 이렇게 하면 카테고리 조회 문제가 해결됩니다. 문제가 지속되면 다음 단계를 참조하여 분류 변경 요청을 제출하십시오.

**STEP 5 |** 웹 인터페이스에서 변경 요청을 제출하려면 URL 로그로 이동하여 변경하려는 URL에 대한 로그 항목을 선택합니다.

**STEP 6 |** 분류 요청 변경 링크를 클릭하고 지침을 따릅니다. URL을 검색한 다음 변경 요청 아이콘을 클릭하여 Palo Alto Networks Test A Site 웹사이트에서 카테고리 변경을 요청할 수도 있

 ©2023 Palo Alto Networks, Inc.

습니다. 각 카테고리에 대한 설명과 함께 사용 가능한 모든 카테고리 목록을 보려면 https://urlfiltering.paloaltonetworks.com/CategoryList.aspx를 참조하십시오.

변경 요청이 승인되면 이메일 알림을 받게 됩니다. 그런 다음 방화벽에서 URL 카테고리가 업데이트되도록 하는 두 가지 옵션이 있습니다.

- 캐시의 URL이 만료될 때까지 기다렸다가 다음에 사용자가 URL에 액세스할 때 새 분류 업데이트가 캐시에 저장됩니다.
- 다음 명령을 실행하여 캐시에서 업데이트를 강제 실행합니다.

```
request url-filtering update url <URL>
```


©2023 Palo Alto Networks, Inc.

# PAN-DB 프라이빗 클라우드

PAN-DB 프라이빗 클라우드는 클라우드 서비스 사용을 제한하는 조직을 위한 온프레미스 솔루션입니다. 이 온프레미스 솔루션을 사용하면 네트워크 또는 데이터 센터 내에 하나 이상의 M-600 어플라이언스를 PAN-DB 서버로 배포할 수 있습니다. 방화벽은 PAN-DB 퍼블릭 클라우드에 액세스하는 대신 PAN-DB 프라이빗 클라우드를 쿼리하여 URL 조회를 수행합니다.

프라이빗 클라우드와 퍼블릭 클라우드 모두에서 URL 조회를 수행하는 프로세스는 네트워크의 방화벽에 대해 동일합니다. 기본적으로 방화벽은 퍼블릭 PAN-DB 클라우드에 액세스하도록 구성됩니다. PAN-DB 프라이빗 클라우드를 배포하는 경우 프라이빗 클라우드의 서버에 액세스하려면 IP 주소 또는 FQDN 목록을 사용하여 방화벽을 구성해야 합니다.

***PAN-OS 5.0*** 이상의 버전을 실행하는 방화벽은 ***PAN-DB*** 프라이빗 클라우드와 통신할 수 있습니다.

PAN-DB 프라이빗 클라우드를 설정할 때 직접 인터넷에 액세스할 수 있도록 M-600 어플라이언스를 구성하거나 완전히 오프라인 상태로 유지할 수 있습니다. M-600 장비는 URL 조회를 수행하기 위해 데이터베이스 및 콘텐츠 업데이트가 필요하므로 어플라이언스에 활성 인터넷 연결이 없는 경우 수동으로 네트워크의 서버에 업데이트를 다운로드한 다음 SCP를 사용하여 PAN-DB 사설 클라우드의 각 M-600 디바이스로 업데이트를 가져와야 합니다. 또한 어플라이언스는 시드 데이터베이스 및 서비스가 제공하는 방화벽에 대한 기타 일반 또는 중요 콘텐츠 업데이트를 가져올 수 있어야 합니다.

PAN-DB 사설 클라우드에 연결하는 방화벽을 인증하기 위해 기본 서버 인증서 집합이 장비와 함께 패키징됩니다. 방화벽 인증을 위해 다른 서버 인증서를 가져오거나 사용할 수 없습니다. M-600 디바이스에서 호스트 이름을 변경하면 디바이스가 자동으로 새 인증서 집합을 생성하여 방화벽을 인증합니다.

- PAN-DB 프라이빗 클라우드용 M-600 어플라이언스
- PAN-DB 사설 클라우드 설정

## PAN-DB 프라이빗 클라우드용 M-600 어플라이언스

PAN-DB 프라이빗 클라우드를 배포하려면 하나 이상의 M-600 어플라이언스가 필요합니다. M-600 어플라이언스는 Panorama 모드로 배송되며 PAN-DB 프라이빗 클라우드로 배포하려면 PAN-URL-DB 모드에서 작동하도록 설정해야 합니다. PAN-URL-DB 모드에서 어플라이언스는 PAN-DB 퍼블릭 클라우드를 사용하지 않으려는 기업을 위해 URL 분류 서비스를 제공합니다.

PAN-DB 프라이빗 클라우드로 배포된 M-600 어플라이언스는 MGT(Eth0) 및 Eth1의 두 포트를 사용합니다. Eth2는 사용할 수 없습니다. 관리 포트는 어플라이언스에 대한 관리 액세스 및 PAN-DB 공용 클라우드 또는 네트워크의 서버에서 최신 콘텐츠 업데이트를 얻는 데 사용됩니다. PAN-DB 프라이빗 클라우드와 네트워크의 방화벽 간의 통신을 위해 MGT 포트 또는 Eth1을 사용할 수 있습니다.

***M-200*** 어플라이언스는 ***PAN-DB*** 프라이빗 클라우드로 배포할 수 없습니다.

PAN-URL-DB 모드의 M-600 어플라이언스:

- 웹 인터페이스가 없으며 명령줄 인터페이스(CLI)만 지원합니다.
- Panorama로 관리할 수 없습니다.


©2023 Palo Alto Networks, Inc.

- 고가용성 쌍으로 배포할 수 없습니다.
- URL 필터링 라이선스가 필요하지 않습니다. 방화벽에는 PAN-DB 사설 클라우드에 연결하고 쿼리하려면 유효한 PAN-DB URL 필터링 라이선스가 있어야 합니다.
- PAN-DB 프라이빗 클라우드에 연결하는 방화벽을 인증하는 데 사용되는 기본 서버 인증서 세트와 함께 제공됩니다. 방화벽 인증을 위해 다른 서버 인증서를 가져오거나 사용할 수 없습니다. M-600 어플라이언스에서 호스트 이름을 변경하면 어플라이언스가 서비스하는 방화벽을 인증하기 위해 새로운 인증서 세트를 자동으로 생성합니다.
- Panorama 모드로만 재설정할 수 있습니다. 어플라이언스를 전용 Log Collector로 배포하려면 Panorama 모드로 전환한 다음 Log Collector 모드로 설정하십시오.

표 **4: PAN-DB** 퍼블릭 클라우드와 **PAN-DB** 프라이빗 클라우드의 차이점

| 차이점 | **PAN-DB** 퍼블릭 클라우드 | **PAN-DB** 프라이빗 클라우드 |
|---|---|---|
| 콘텐츠 및 데이터베이스 업데이트 | 콘텐츠(정기 및 중요) 업데이트 및 전체 데이터베이스 업데이트는 하루 동안 여러 번 게시됩니다. PAN-DB 퍼블릭 클라우드는 5분마다 악성코드 및 피싱 URL 카테고리를 업데이트합니다. 방화벽은 URL 조회를 위해 클라우드 서버에 쿼리할 때마다 중요한 업데이트를 확인합니다. | 콘텐츠 업데이트 및 전체 URL 데이터베이스 업데이트는 작업 주중 하루에 한 번 사용할 수 있습니다. |
| **URL** 분류 요청 | 다음 옵션을 사용하여 URL 분류 변경 요청을 제출합니다.<br>• Palo Alto Networks Test A Site 웹사이트.<br>• 방화벽의 URL 필터링 프로파일 설정 페이지입니다.<br>• 방화벽의 URL 필터링 로그. | Palo Alto Networks Test A Site 웹사이트를 통해서만 URL 분류 변경 요청을 제출하십시오. |
| 해결되지 않은 **URL** 쿼리 | 방화벽이 URL 쿼리를 해결할 수 없는 경우 요청은 공용 클라우드의 서버로 전송됩니다. | 방화벽이 쿼리를 해결할 수 없는 경우 요청이 PAN-DB 프라이빗 클라우드의 M-600 어플라이언스로 전송됩니다. 일치하는 URL이 없으면 PAN-DB 프라이빗 클라우드는 카테고리 알 수 없는 응답을 방화벽에 보냅니다. PAN-DB 퍼블릭 클라우드에 액세스하도록 M-600 어플라이언스를 구성하지 않는 한 요청은 퍼블릭 클라우드로 전송되지 않습니다.<br>PAN-DB 프라이빗 클라우드를 구성하는 M-600 어플라이언스가 완전히 오프라 |


©2023 Palo Alto Networks, Inc.

| 차이점 | **PAN-DB** 퍼블릭 클라우드 | **PAN-DB** 프라이빗 클라우드 |
|---|---|---|
| | | 인으로 구성된 경우 데이터 또는 분석을 퍼블릭 클라우드로 보내지 않습니다. |

## PAN-DB 사설 클라우드 설정

네트워크 또는 데이터 센터 내에서 하나 이상의 M-600 어플라이언스를 PAN-DB 사설 클라우드로 배포하려면 다음 작업을 완료해야 합니다.

- PAN-DB 프라이빗 클라우드 구성
- PAN-DB 사설 클라우드에 액세스하도록 방화벽 구성
- PAN-DB 사설 클라우드에서 사용자 지정 인증서로 인증 구성

### **PAN-DB** 프라이빗 클라우드 구성

**STEP 1 |** M-600 어플라이언스를 랙에 장착합니다.

지침은 M-600 하드웨어 참조 안내서를 참조하십시오.

**STEP 2 |** M-600 어플라이언스를 등록합니다.

M-600 어플라이언스 등록에 대한 지침은 방화벽 등록을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** M-600 어플라이언스의 초기 구성을 수행합니다.

*PAN-DB* 모드의 *M-600* 어플라이언스는 *MGT(Eth0)* 및 *Eth1*의 두 포트를 사용합니다. *Eth2*는 *PAN-DB* 모드에서 사용되지 않습니다. 관리 포트는 어플라이언스에 대한 관리 액세스 및 *PAN-DB* 공용 클라우드에서 최신 콘텐츠 업데이트를 얻는 데 사용됩니다. 어플라이언스*(PAN-DB* 서버*)*와 네트워크의 방화벽 간의 통신을 위해 *MGT* 포트 또는 *Eth1*을 사용할 수 있습니다.

1. 다음 방법 중 하나로 M-600 어플라이언스에 연결합니다.
   - 컴퓨터의 직렬 케이블을 M-600 어플라이언스의 콘솔 포트에 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 연결합니다.
   - 컴퓨터의 RJ-45 이더넷 케이블을 M-600 어플라이언스의 MGT 포트에 연결합니다. 브라우저에서 https://192.168.1.1로 이동합니다. 이 URL에 대한 액세스를 활성화하려면 컴퓨터의 IP 주소를 192.168.1.0 네트워크의 주소(예: 192.168.1.2)로 변경해야 할 수 있습니다.
2. 메시지가 표시되면 어플라이언스에 로그인합니다. 기본 사용자 이름과 암호(admin/admin)를 사용하여 로그인합니다. 어플라이언스가 초기화되기 시작합니다.
3. MGT 인터페이스의 IP 주소를 포함한 네트워크 액세스 설정을 구성합니다.

   ```
   set deviceconfig system ip-address  <server-IP>
    netmask <netmask> default-gateway <gateway-IP> dns-setting
    servers primary <DNS-IP>
   ```

   여기서 *<server-IP>*은 서버의 관리 인터페이스에 할당하려는 IP 주소이고, *<netmask>*은 서브넷 마스크이고, *<gateway-IP>*는 네트워크 게이트웨이의 IP 주소이고 *<DNS-IP>*은 기본 DNS 서버의 IP 주소입니다.
4. Eth1 인터페이스의 IP 주소를 포함한 네트워크 액세스 설정을 구성합니다.

   ```
   set deviceconfig system eth1 ip-address  <server-IP>
    netmask <netmask> default-gateway <gateway-IP> dns-setting
    servers primary <DNS-IP>
   ```

   여기서 *<server-IP>*은(는) 서버의 데이터 인터페이스에 할당하려는 IP 주소이고, *<netmask>*은 서브넷 마스크이고, *<gateway-IP>*은(는) 네트워크 게이트웨이의 IP 주소이고 *<DNS-IP>*은(는) DNS 서버의 IP 주소입니다.
5. 변경 사항을 PAN-DB 서버에 저장합니다.

   **commit**


©2023 Palo Alto Networks, Inc.

**STEP 4 |** PAN-DB 프라이빗 클라우드 모드로 전환합니다.

1. PAN-DB 모드로 전환하려면 CLI 명령을 사용하십시오.

```
request system system-mode pan-url-db
```

> *Panorama* 모드에서 *PAN-DB* 모드로 전환했다가 다시 전환할 수 있습니다. Panorama 모드 - 로그 수집기 모드 양방향으로 전환 가능합니다. *PAN-DB* 모드 - *Log Collector* 모드 간에는 양방향 전환이 지원되지 않습니다. 작동 모드를 전환하면 데이터 재설정이 트리거됩니다. 관리 접근 설정을 제외한 모든 기존 구성 및 로그는 재시작 시 삭제됩니다.

2. 다음 명령을 사용하여 모드가 변경되었는지 확인합니다.

```
show pan-url-cloud-status hostname: M-600 ip-address: 1.2.3.4
 netmask: 255.255.255.0 default-gateway: 1.2.3.1 ipv6-address:
 unknown ipv6-link-local-address: fe80:00/64 ipv6-default-
gateway: mac-address: 00:56:90:e7:f6:8e time: Mon Apr 27
 13:43:59 2015 uptime: 10 days, 1:51:28 family: m model:
 M-600 serial: 0073010000xxx sw-version: 7.0.0 app-version:
 492-2638 app-release-date: 2015/03/19 20:05:33 av-version:
 0 av-release-date: unknown wf-private-version: 0 wf-private-
release-date: unknown logdb-version: 7.0.9 platform-family: m
 pan-url-db: 20150417-220 system-mode: Pan-URL-DB operational-
mode: normal
```

3. 다음 명령을 사용하여 어플라이언스의 클라우드 데이터베이스 버전을 확인하십시오.

```
show pan-url-cloud-status Cloud status: 최대 URL 데이터베이스 버전
 : 20150417-220
```


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 콘텐츠 및 데이터베이스 업데이트를 설치합니다.

어플라이언스는 현재 실행 중인 콘텐츠 버전과 하나의 이전 버전만 저장합니다.

콘텐츠 및 데이터베이스 업데이트를 설치하는 다음 방법 중 하나를 선택합니다.

- PAN-DB 서버가 인터넷에 직접 액세스할 수 있는 경우 다음 명령을 사용합니다.
  1. 새 버전이 게시되었는지 확인하려면 다음을 사용하십시오.

     **request pan-url-db upgrade check**
  2. 현재 서버에 설치된 버전을 확인하려면 다음을 사용하십시오.

     **request pan-url-db upgrade info**
  3. 최신 버전을 다운로드하고 설치하려면:
     - **request pan-url-db upgrade download latest**
     - **request pan-url-db upgrade install** *<version latest | file>*
  4. 업데이트를 자동으로 확인하도록 M-600 어플라이언스를 예약하려면:

     ```
     set deviceconfig system update-schedule pan-url-db recurring
      weekly action download-and-install day-of-week  <day of week>
      at <hr:min>
     ```
- PAN-DB 서버가 오프라인인 경우 Palo Alto Networks 고객 지원 웹사이트에 액세스하여 네트워크의 SCP 서버에 콘텐츠 업데이트를 다운로드하고 저장합니다. 그런 후 다음 명령을 사용하여 업데이트를 가져오고 설치할 수 있습니다.
  - **scp import pan-url-db remote-port** *<port-number>* from username@host:path
  - **request pan-url-db upgrade install file** *<filename>*


©2023 Palo Alto Networks, Inc.

**STEP 6 |** PAN-DB 프라이빗 클라우드에 대한 관리 액세스를 설정합니다.

어플라이언스에는 기본 **관리자** 계정이 있습니다. 생성하는 추가 관리 사용자는 운용 관리자(전체 액세스 권한) 또는 읽기 전용 액세스 권한이 있는 운용 관리자일 수 있습니다.

PAN-DB 프라이빗 클라우드는 RADIUS VSA 사용을 지원하지 않습니다. 방화벽 또는 Panorama에서 사용되는 VSA를 사용하여 PAN-DB 프라이빗 클라우드에 대한 액세스를 활성화하는 경우 인증 실패가 발생합니다.

- PAN-DB 서버에서 로컬 관리자를 설정하려면:
  1. **configure**
  2. ```
     set mgt-config users  <username> permissions role-based
      <superreader | superuser> yes
     ```
  3. ```
     set mgt-config users <username> password
     ```
  4. **Enter password:xxxxx**
  5. **Confirm password:xxxxx**
  6. **commit**
- RADIUS 인증으로 관리 사용자를 설정하려면:
  1. RADIUS 서버 프로파일을 생성합니다.

     ```
     set shared server-profile radius  <server_profile_name>
      server <server_name> ip-address <ip_address> port <port_no>
      secret <shared_password>
     ```
  2. 인증 프로파일을 생성합니다.

     ```
     set shared authentication-profile  <auth_profile_name> user-
     domain <domain_name_for_authentication> allow-list <all> method
      radius server-profile <server_profile_name>
     ```
  3. 사용자에게 인증 프로파일을 첨부합니다.

     ```
     set mgt-config users  <username> authentication-
     profile <auth_profile_name>
     ```
  4. 변경 사항을 커밋합니다.

     **commit**
- 사용자 목록을 보려면:.

```
show mgt-config users users { admin { phash fnRL/G5lXVMug;
 permissions { role-based { superuser yes; } } } admin_user_2
 { permissions { role-based { superreader yes; } }
 authentication-profile RADIUS; } }
```

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** PAN-DB 프라이빗 클라우드에 액세스하도록 방화벽을 구성합니다.

## PAN-DB 사설 클라우드에 액세스하도록 방화벽 구성

PAN-DB 퍼블릭 클라우드를 사용할 때 각 방화벽은 AWS 클라우드의 PAN-DB 서버에 액세스하여 URL 조회를 위해 연결할 수 있는 적격 서버 목록을 다운로드합니다. PAN-DB 사설 클라우드를 사용하는 경우 URL 조회에 사용할 PAN-DB 사설 클라우드 서버의(정적) 목록으로 방화벽을 구성해야 합니다. 목록에는 최대 20개의 항목이 포함될 수 있습니다. IPv4 주소, IPv6 주소 및 FQDN이 지원됩니다. 목록의 각 항목(IP 주소 또는 FQDN)은 PAN-DB 서버의 관리 포트 및/또는 eth1에 할당되어야 합니다.

**STEP 1 |** PAN-OS CLI에서 URL 조회에 사용되는 정적 PAN-DB 프라이빗 클라우드 서버 목록을 추가합니다.

- 다음 CLI 명령을 사용하여 개인 PAN-DB 서버 IP 주소를 추가합니다.

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

또는 각 방화벽의 웹 인터페이스에서 **Device** > **Setup** > **Content-ID**를 선택한 다음 URL 필터링 섹션을 편집한 다음 **PAN-DB** 서버 IP 주소 또는 FQDN을 입력합니다. 목록은 쉼표로 구분해야 합니다.

- 개인 PAN-DB 서버에 대한 항목을 삭제하려면 다음 명령을 사용하십시오.

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

사설 PAN-DB 서버 목록을 삭제하면 방화벽에서 재선 프로세스가 트리거됩니다. 방화벽은 먼저 PAN-DB 사설 클라우드 서버 목록을 확인하고 찾을 수 없으면 방화벽이 AWS 클라우드의 PAN-DB 서버에 액세스하여 연결할 수 있는 적격 서버 목록을 다운로드합니다.

**STEP 2 |** **#** 커밋을 입력하여 변경 사항을 저장합니다.

**STEP 3 |** 변경 사항이 유효한지 확인하려면 방화벽에서 다음 CLI 명령을 사용하십시오.

```
> show url-cloud status Cloud status: 최대 URL 데이터베이스 버전 : 20150417-220
```

## PAN-DB 사설 클라우드에서 사용자 지정 인증서로 인증 구성

기본적으로 PAN-DB 서버는 상호 인증에 사전 정의된 인증서를 사용하여 관리 액세스 및 디바이스 간 통신에 사용되는 SSL 연결을 설정합니다. 하지만 대신 사용자 지정 인증서를 사용하여 인증을 구성할 수 있습니다. 사용자 지정 인증서를 사용하면 고유한 신뢰 체인을 설정하여 PAN-DB 서버와 방화벽 간의 상호 인증을 보장할 수 있습니다. PAN-DB 사설 클라우드의 경우 방화벽이 클라이언트 역할을 하고 PAN-DB 서버가 서버 역할을 합니다.

**STEP 1 |** PAN-DB 서버 및 방화벽에 대한 키 쌍 및 CA(인증 기관) 인증서를 얻습니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** CA 인증서를 가져와 방화벽에서 인증서의 유효성을 검사합니다.

1. PAN-DB 서버의 CLI에 로그인하고 구성 모드로 들어갑니다.

```
admin@M-600> configure
```

2. TFTP 또는 SCP를 사용하여 CA 인증서를 가져옵니다.

```
admin@M-600# {tftp | scp} import certificate from <value>
 file <value> remote-port <1-65535> source-ip <ip/netmask>
 certificate-name <value> passphrase <value> format {pkcs12 |
 pem}
```

**STEP 3 |** TFTP 또는 SCP를 사용하여 PAN-DB M-600 어플라이언스의 서버 인증서와 개인 키가 포함된 키 쌍을 가져옵니다.

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

**STEP 4 |** 루트 CA 및 중간 CA를 포함하는 인증서 프로파일을 구성합니다. 이 인증서 프로파일은 PAN-DB 서버와 방화벽 간의 디바이스 인증을 정의합니다.

1. PAN-DB 서버의 CLI에서 구성 모드로 들어갑니다.

```
admin@M-600> configure
```

2. 인증서 프로파일의 이름을 지정합니다.

```
admin@M-600# set shared certificate-profile <name>
```

3. (선택 사항) 사용자 도메인을 설정합니다.

```
admin@M-600# set shared certificate-profile <name>
 domain <value>
```

4. CA를 구성합니다.

   기본 ***OCSP-URL***과 ***ocsp-verify-cert***은 선택적 매개 변수입니다.

admin@M-600# **set shared certificate-profile <name> CA <name>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```


©2023 Palo Alto Networks, Inc.

**STEP 5 |** PAN-DB M-600 어플라이언스에 대한 SSL/TLS 프로파일을 구성합니다. 이 프로파일은 PAN-DB 및 클라이언트 디바이스가 SSL/TLS 서비스에 사용하는 인증서 및 프로토콜 범위를 정의합니다.

1. SSL/TLS 프로파일을 식별합니다.

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. 인증서를 선택합니다.

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. SSL/TLS 범위를 정의합니다.

   *PAN-OS 8.0* 이상 릴리스는 ***TLS 1.2*** 이상의 ***TLS*** 버전만 지원합니다. 최대 버전을 ***TLS 1.2*** 또는 최대로 설정해야 합니다.

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

**STEP 6 |** PAN-DB에서 보안 서버 통신을 구성합니다.

1. SSL/TLS 프로파일을 설정합니다. 이 SSL/TLS 서비스 프로파일은 PAN-DB와 방화벽 간의 모든 SSL 연결에 적용됩니다.

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 인증서 프로파일을 설정합니다.

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. PAN-DB가 방화벽과의 연결을 끊고 다시 설정하기 전에 대기해야 하는 연결 해제 대기 시간(분)을 설정합니다(범위는 0 ~ 44,640).

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

**STEP 7 |** CA 인증서를 가져와 PAN-DB M-600 어플라이언스에 대한 인증서의 유효성을 검사합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. CA 인증서를 가져옵니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 방화벽에 대한 로컬 또는 SCEP 인증서를 구성합니다.

1. 로컬 인증서인 경우 방화벽의 키 쌍을 가져옵니다.
2. 방화벽에 대한 SCEP 인증서가 인 경우 SCEP 프로파일을 구성합니다.

**STEP 9 |** 방화벽에 대한 인증서 프로파일을 구성합니다. 각 방화벽에서 개별적으로 구성하거나 템플릿의 일부로 Panoramora의 구성을 방화벽으로 푸시할 수 있습니다.

1. 방화벽의 경우 디바이스 > 인증서 관리 > 인증서 프로파일을 선택한 다음 Panorama의 경우 **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

**STEP 10 |** 각 방화벽에 사용자 지정 인증서를 배포합니다. Panorama의 중앙에서 인증서를 배포하거나 각 방화벽에서 수동으로 인증서를 구성할 수 있습니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 방화벽의 경우 디바이스 > 설정 > 관리 또는 **Panorama** > 설정 > 관리를 선택하고 보안 통신을(를) 편집합니다.
3. 각 드롭다운에서 인증서 유형, 인증서 및 인증서 프로파일을 선택합니다.
4. 통신 설정 사용자 지정에서 **PAN-DB** 통신을 선택합니다.
5. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

변경 사항을 커밋한 후 방화벽은 연결 해제 대기 시간이 끝날 때까지 PAN-DB 서버와의 현재 세션을 종료하지 않습니다. 다음 단계에서 사용자 지정 인증서 사용을 적용한 후 연결 해제 대기 시간 카운트다운이 시작됩니다.

**STEP 11 |** 모든 방화벽에 사용자 지정 인증서를 배포한 후 사용자 지정 인증서 인증을 적용합니다.

1. PAN-DB 서버의 CLI에 로그인하고 구성 모드로 들어갑니다.

```
admin@M-600> configure
```

2. 사용자 지정 인증서 사용을 강제합니다.

```
admin@M-600# set deviceconfig setting management secure-conn-
server disable-pre-defined-cert yes
```

이 변경 사항을 커밋한 후 연결 해제 대기 시간이 카운트다운되기 시작합니다(PAN-DB에서 설정을 구성한 경우). 대기 시간이 끝나면 PAN-DB와 방화벽이 구성된 인증서만 사용하여 연결됩니다.

**STEP 12 |** PAN-DB 프라이빗 클라우드 배포에 새 방화벽 또는 Panorama를 추가할 때 두 가지 옵션을 선택할 수 있습니다.

- 사용자 지정 인증서만 사용하도록 설정하지 않은 경우 PAN-DB 사설 클라우드에 새 방화벽을 추가한 다음 위에서 설명한 대로 사용자 지정 인증서를 배포할 수 있습니다.
- PAN-DB 사설 클라우드에서만 사용자 지정 인증서를 활성화한 경우 PAN-DB 사설 클라우드에 연결하기 전에 방화벽에 사용자 지정 인증서를 배포해야 합니다.


©2023 Palo Alto Networks, Inc.

# SSL/TLS 핸드셰이크 검사 활성화

SSL/TLS 핸드쉐이크 검사는 복호화로 표시된 SSL/TLS 웹 트래픽에 대한 위협 탐지의 격차를 좁힙니다. 활성화되면 방화벽의 CTD(콘텐츠 및 위협 탐지) 엔진이 HTTPS 트래픽을 검사하여 SSL/TLS 핸드쉐이크 중에 잠재적인 위협을 확인합니다. 방화벽은 핸드쉐이크의 데이터를 사용하여 트래픽을 식별하고 해당 보안 정책 규칙을 적용합니다. 핸드쉐이크를 검사하면 네트워크 보안을 개선하고 위협을 방지하고 웹 트래픽에 대한 보안 정책 조치를 가능한 한 빨리 적용하여 URL 필터링 솔루션을 최적화합니다.

특히 방화벽은 요청된 웹사이트의 호스트 이름을 포함하는 SSL/TLS 프로토콜의 확장인 ***SNI(***서버 이름 표시**)** 필드에 대한 클라이언트 헬로 메시지를 검사합니다. 호스트 이름에서 방화벽은 트래픽의 URL 카테고리 및 서버 대상을 파생할 수 있습니다. 그런 다음 보안 정책 규칙일치의 URL 필터링 프로파일에 대해 URL 카테고리를 평가하여 적용할 작업을 결정합니다. 방화벽이 SNI 필드의 악성 웹 서버와 같은 위협을 감지하거나 정책이 웹사이트를 차단하라는 지시가 있는 경우 핸드쉐이크를 종료하고 웹 세션을 즉시 종료합니다. 위협이 감지되지 않고 정책당 트래픽이 허용되면 클라이언트와 서버는 보안 연결을 통해 SSL/TLS 핸드쉐이크를 완료하고 애플리케이션 데이터를 교환할 수 있습니다.

***URL*** 필터링 응답 페이지는 ***SSL/TLS*** 핸드쉐이크 검사 중에 방화벽에 의해 차단된 사이트에 대해 표시되지 않습니다**.** 차단된 카테고리에서 트래픽을 감지한 후 방화벽은 ***HTTPS*** 연결을 재설정하여 핸드쉐이크를 종료하고 응답 페이지를 통한 사용자 알림을 방지합니다**.** 대신 브라우저에 표준 연결 오류 메시지가 표시됩니다**.**

성공적인 ***SSL/TLS*** 핸드셰이크 및 세션에 대한 세부 정보는 트래픽 및 암호 해독 로그에 있습니다**.** 방화벽이 ***SSL/TLS*** 핸드쉐이크 중에 웹 세션을 차단하는 경우 복호화 로그를 생성하지 않습니다**.** 그러나 ***URL*** 필터링 로그에서 실패한 세션의 세부 정보를 찾을 수 있습니다**.**

다음 절차는 SSL/TLS 핸드쉐이크 검사를 지원하는 데 필요한 요구 사항 및 단계를 자세히 설명합니다.

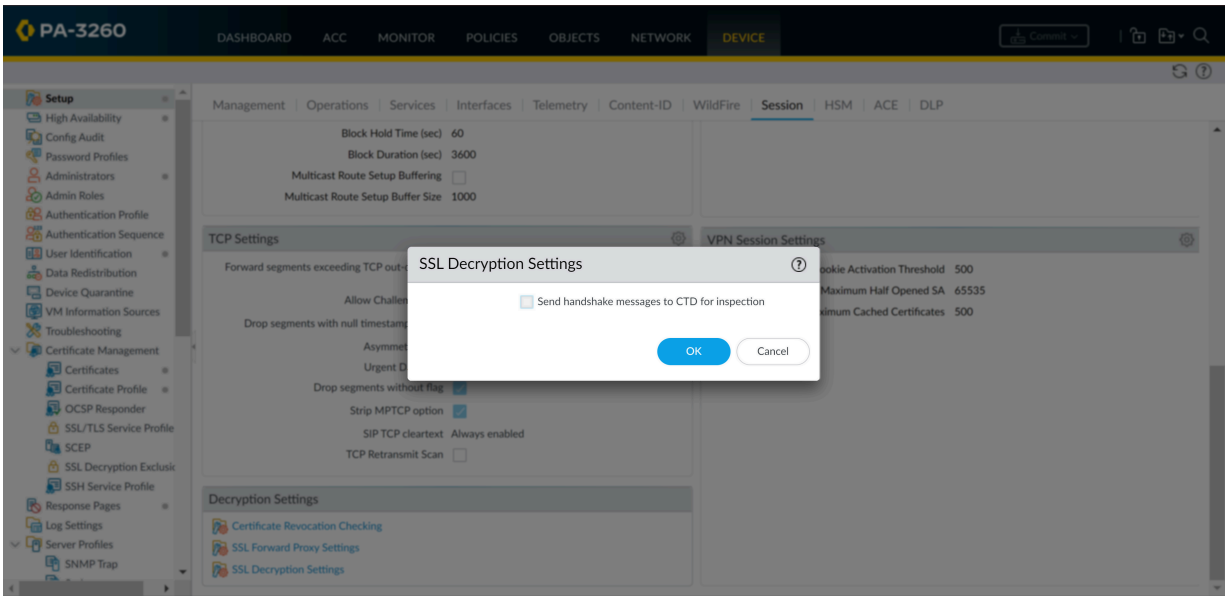
**STEP 1 |** 디바이스 **>** 라이선스를 선택하여 활성 고급 URL 필터링 또는 레거시 URL 필터링 라이선스가 있는지 확인합니다.

**STEP 2 |** SSL 포워드 프록시 또는 SSL 인바운드 검사를 통해 SSL/TLS트래픽을 복호화했는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** CTD에 의한 SSL/TLS 핸드쉐이크를 검사할 수 있습니다. 기본적으로 옵션은 비활성화됩니다.


©2023 Palo Alto Networks, Inc.




 ©2023 Palo Alto Networks, Inc.

1. 디바이스 > 설정 > 세션 > 암호 해독 설정 > **SSL** 암호 해독 설정을 선택합니다.
2. 검사를 위해 **CTD**로 핸드쉐이크 메시지 보내기를 선택합니다.

   또는 **set deviceconfig setting ssl-decrypt scan-handshake *<yes|no>*** CLI 명령을 사용할 수 있습니다.
3. 확인을 클릭합니다.

**STEP 4 |** 구성 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

# 서비스 품질

QoS(서비스 품질)는 제한된 네트워크 용량에서 우선 순위가 높은 애플리케이션과 트래픽을 안정적으로 실행할 수 있는 기능을 보장하기 위해 네트워크에서 작동하는 기술 집합입니다. QoS 기술은 네트워크 트래픽의 특정 흐름에 차별화된 처리 및 용량 할당을 제공함으로써 이러한 목표를 달성합니다. 이를 통해 네트워크 관리자는 트래픽이 처리되는 순서와 트래픽에 제공되는 대역폭의 양을 할당할 수 있습니다.

Palo Alto Networks 애플리케이션 서비스 품질(QoS)은 네트워크에 적용되는 기본 QoS를 제공하고 이를 확장하여 애플리케이션과 사용자에게 QoS를 제공합니다.

Palo Alto Networks 애플리케이션 기반 QoS에 대해 알아보고 구성하려면 다음 항목을 참조하십시오.

- QoS 개요
- QoS 개념
- QoS 구성
- 가상 시스템에 대한 QoS 구성
- DSCP 분류를 기반으로 QoS 적용
- QoS 사용 사례

Palo Alto Networks 제품 비교 도구를 사용하여 방화벽 모델에서 지원되는 QoS 기능을 확인할 수 있습니다. 두 개 이상의 제품 모델을 선택한 다음 지금 비교를 클릭하여 각 모델에 대한 QoS 기능 지원을 확인합니다. 예를 들어 방화벽 모델이 하위 인터페이스에서 QoS를 지원하는지의 여부나 QoS를 활성화할 수 있는 최대 하위 인터페이스 수를 확인할 수 있습니다.

통합 이더넷(AE) 인터페이스의 QoS는 PAN-OS 7.0 이상 릴리스를 실행하는 PA-7000 시리즈, PA-5400 시리즈, PA-5200 시리즈, PA-3400 시리즈, PA-3200 시리즈 및 PA-400 시리즈 방화벽에서 지원됩니다.

# QoS 개요

QoS를 사용하여 네트워크 트래픽의 품질 측면에 우선 순위를 지정하고 조정합니다. 패킷이 처리되는 순서를 지정하고 대역폭을 할당하여 선택한 트래픽, 애플리케이션 및 사용자에 대해 우선적으로 처리되고 최적의 성능 수준을 제공할 수 있습니다.

QoS 구현의 대상이 되는 서비스 품질 측정은 대역폭(최대 전송 속도), 처리량(실제 전송 속도), 대기 시간(지연) 및 지터(대기 시간 차이)입니다. 이러한 서비스 품질 측정을 구성하고 제어하는 기능은 대기 시간 및 지터에 대한 민감도가 높은 VoIP(Voice over IP), 화상 회의 및 주문형 비디오와 같은 QoS를 고대역폭 실시간 트래픽에 특히 중요하게 만듭니다. 또한 QoS를 사용하여 다음과 같은 결과를 얻을 수 있습니다.

- 네트워크 및 애플리케이션 트래픽의 우선 순위를 지정하여 중요한 트래픽에 높은 우선 순위를 보장하거나 필수적이지 않은 트래픽을 제한합니다.
- 네트워크의 다른 서브넷, 클래스 또는 사용자 간에 동일한 대역폭 공유를 달성합니다.
- 대역폭을 외부 또는 내부 또는 둘 다에 할당하여 업로드 및 다운로드 트래픽 모두에 QoS를 적용하거나 트래픽만 업로드 또는 다운로드하도록 적용합니다.
- 엔터프라이즈 환경에서 고객 및 수익 창출 트래픽에 대한 짧은 대기 시간을 보장합니다.
- 대역폭 사용을 보장하기 위해 애플리케이션의 트래픽 프로파일링을 수행합니다.

Palo Alto Networks 방화벽에서 QoS 구현은 전체 QoS 솔루션을 지원하는 세 가지 기본 구성 구성요소(QoS 프로파일, QoS 정책 및 QoS Egress Interface 설정)로 시작됩니다. QoS 구성 작업의 이러한 각 옵션은 트래픽 플로우를 최적화하고 우선 순위를 지정하고 구성 가능한 매개변수에 따라 대역폭을 할당 및 보장하는 광범위한 프로세스를 용이하게 합니다.

그림 QoS 트래픽 플로우는 트래픽이 소스에서 플로우되고 QoS가 활성화된 방화벽에 의해 형성되며 궁극적으로 우선 순위가 지정되어 대상으로 포워딩되는 트래픽을 보여줍니다.

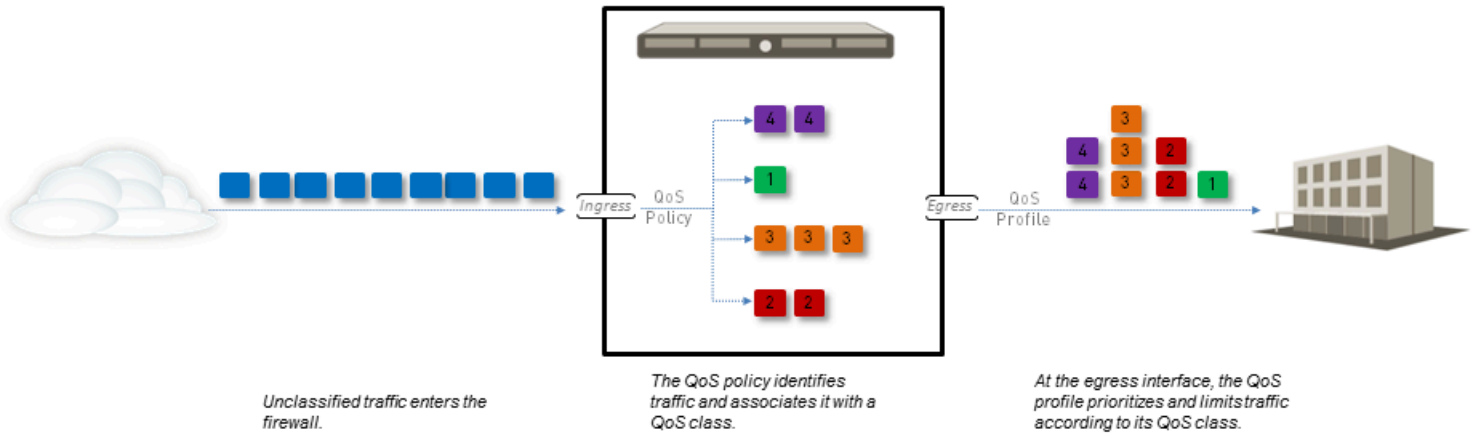



그림 **6: QoS** 트래픽 플로우

QoS 구성 옵션을 사용하면 트래픽 플로우을 제어하고 흐름의 다른 지점에서 정의할 수 있습니다. QoS 트래픽 플로우 그림은 구성 가능한 옵션이 트래픽 플로우를 정의하는 위치를 나타냅니다. QoS 정책 규칙을 사용하면 QoS 처리를 받을 트래픽을 정의하고 해당 트래픽에 QoS 클래스를 할당할 수 있습니다. 그러면 일치하는 트래픽이 물리적 인터페이스를 나갈 때 QoS 프로파일 클래스 설정을 기반으로 형성됩니다.


©2023 Palo Alto Networks, Inc.

각 QoS 구성 요소는 서로 영향을 미치며 QoS 구성 옵션을 사용하여 완전하고 세분화된 QoS 구현을 생성하거나 최소한의 관리자 작업으로 드물게 사용할 수 있습니다.

각 방화벽 모델은 QoS로 구성할 수 있는 최대 포트 수를 지원합니다. 방화벽 모델의 사양 시트를 참조하거나 제품 비교 도구를 사용하여 단일 페이지에서 둘 이상의 방화벽에 대한 QoS 기능 지원을 확인하십시오.


©2023 Palo Alto Networks, Inc.

# QoS 개념

다음 주제를 사용하여 Palo Alto Networks 방화벽에서 QoS 구성의 다양한 구성 요소와 메커니즘에 대해 알아보세요.

- 애플리케이션 및 사용자를 위한 QoS
- QoS 정책
- QoS 프로파일
- QoS 클래스
- QoS 우선 순위 큐
- QoS 대역폭 관리
- QoS 송신 인터페이스
- 일반 텍스트 및 터널링된 트래픽을 위한 QoS

## 애플리케이션 및 사용자를 위한 QoS

Palo Alto Networks 방화벽은 네트워크 또는 서브넷에 따라 방화벽을 나가는 트래픽을 제어하는 기본 QoS를 제공하고 QoS의 기능을 확장하여 애플리케이션 및 사용자에 따라 트래픽을 분류하고 형성합니다. Palo Alto Networks 방화벽은 App-ID 및 User-ID 기능을 QoS 구성과 통합하여 이 기능을 제공합니다. 네트워크의 특정 애플리케이션 및 사용자를 식별하기 위해 존재하는 App-ID 및 User-ID 항목은 QoS 구성에서 사용할 수 있으므로 대역폭을 관리 및/또는 보장하려는 애플리케이션 및 사용자를 쉽게 지정할 수 있습니다.

## QoS 정책

QoS 정책 규칙을 사용하여 QoS 처리(우대 처리 또는 대역폭 제한)를 받을 트래픽을 정의하고 이러한 트래픽에 QoS 서비스 클래스를 할당합니다.

다음을 기반으로 트래픽과 일치하도록 QoS 정책 규칙을 정의합니다.

- 애플리케이션 및 애플리케이션 그룹.
- 소스 영역, 소스 주소 및 소스 사용자.
- 대상 영역 및 대상 주소.
- 특정 TCP 및/또는 UDP 포트 번호로 제한된 서비스 및 서비스 그룹.
- 사용자 정의 URL 카테고리를 포함한 URL 카테고리.
- DSCP(Differentiated Services Code Point) 및 ToS(Type of Service) 값은 높은 우선 순위 또는 최적화된 전달과 같이 트래픽에 대해 요청된 서비스 수준을 나타내는 데 사용됩니다.

> ***SSL*** 포워딩 프록시, ***SSL*** 인바운드 검사 및 ***SSH*** 프록시 트래픽에는 ***DSCP*** 코드 포인트 또는 ***QoS***를 적용할 수 없습니다.

여러 QoS 정책 규칙(정책 > **QoS**)을 설정하여 다양한 유형의 트래픽을 다양한 QoS 클래스 서비스와 연결합니다.

 ©2023 Palo Alto Networks, Inc.

QoS는 방화벽을 나갈 때 트래픽에 적용되므로 방화벽이 NAT(Network Address Translation) 규칙을 비롯한 다른 모든 보안 정책 규칙을 적용한 후에 QoS 정책 규칙이 트래픽에 적용됩니다. 소스를 기반으로 트래픽에 QoS 처리를 적용하려면 QoS 정책 규칙에서 사후 NAT 소스 주소를 지정해야 합니다(사전 NAT 소스 주소를 사용하지 마십시오).

## QoS 프로파일

QoS 프로파일 규칙을 사용하여 해당 단일 프로파일 규칙에 포함된 최대 8개의 QoS 클래스 값을 정의합니다.

QoS 프로파일 규칙을 사용하여 QoS 클래스에 대한 QoS 우선 순위 큐잉(Queuing) 및 QoS 대역폭 관리를 정의할 수 있습니다. 각 QoS 프로파일 규칙을 통해 최대 8개의 QoS 클래스에 대한 개별 대역폭 및 우선 순위 설정과 결합된 8개 클래스에 할당된 총 대역폭을 구성할 수 있습니다. QoS 프로파일 규칙(또는 여러 QoS 프로파일 규칙)을 물리적 인터페이스에 연결하여 정의된 우선 순위 및 대역폭 설정을 해당 인터페이스에서 나가는 트래픽에 적용합니다.

방화벽에서 기본 QoS 프로파일 규칙을 사용할 수 있습니다. 기본 프로파일 규칙 및 프로파일에 정의된 클래스에는 사전 정의된 최대 또는 보장된 대역폭 제한이 없습니다.

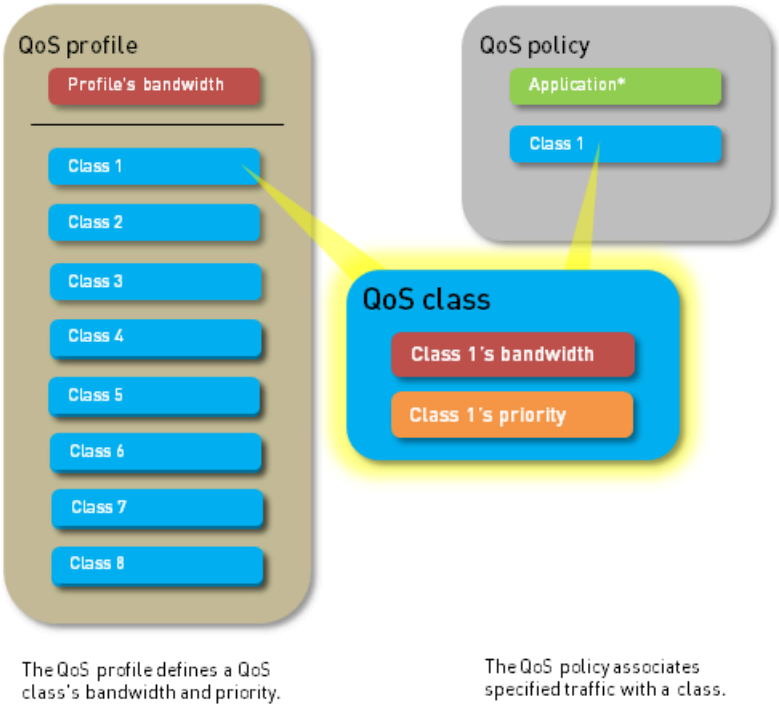
QoS 클래스에 대한 우선 순위 및 대역폭 설정을 정의하려면 QoS 프로파일 규칙 추가 단계를 참조하십시오.

## QoS 클래스

QoS 클래스는 QoS 정책 규칙과 일치하는 트래픽의 우선 순위와 대역폭을 결정합니다. QoS 프로파일 규칙을 사용하여 QoS 클래스를 정의할 수 있습니다. 하나의 QoS 프로파일에는 최대 8개의 정의 가능한 QoS 클래스가 있습니다. 달리 구성되지 않는 한 QoS 클래스와 일치하지 않는 트래픽에는 4 클래스가 할당됩니다.

QoS 구성의 기본 메커니즘인 QoS Priority Queuing 및 QoS Bandwidth Management는 QoS 클래스 정의 내에서 구성됩니다(단계 4 참조). 각 QoS 클래스에 대해 우선 순위(실시간, 높음, 중간 및 낮음)와 일치하는 트래픽에 대한 최대 및 보장 대역폭을 설정할 수 있습니다. QoS 우선 대기열 및 대역폭 관리는 트래픽 순서와 네트워크에 들어오거나 떠날 때 트래픽이 처리되는 방식을 결정합니다.


©2023 Palo Alto Networks, Inc.




## QoS 우선 순위 큐

QoS 클래스에 대해 실시간, 높음, 중간, 낮음 등 네 가지 우선 순위 중 하나를 적용할 수 있습니다. QoS 정책 규칙과 일치하는 트래픽에는 해당 규칙과 연결된 QoS 클래스가 할당되고 방화벽은 QoS 클래스 우선 순위에 따라 일치하는 트래픽을 처리합니다. 나가는 트래픽 플로우의 패킷은 네트워크가 패킷을 처리할 준비가 될 때까지 우선 순위에 따라 대기됩니다. 우선 순위 큐를 사용하면 중요한 트래픽, 애플리케이션 및 사용자가 우선 순위를 갖도록 할 수 있습니다. 실시간 우선 순위는 일반적으로 음성 및 비디오 애플리케이션과 같이 지연 시간에 특히 민감한 애플리케이션에 사용됩니다.

## QoS 대역폭 관리

QoS 대역폭 관리를 사용하면 트래픽이 네트워크 용량을 초과하지 않도록 네트워크의 트래픽 플로우를 제어할 수 있으며(네트워크 정체로 이어짐) 특정 유형의 트래픽과 애플리케이션 및 사용자에 대해 대역폭을 할당할 수도 있습니다. QoS를 사용하면 좁거나 광범위한 트래픽에 대한 대역폭을 적용할 수 있습니다. QoS 프로파일 규칙을 사용하면 개별 QoS 클래스에 대한 대역폭 제한과 8개 QoS 클래스 모두에 대한 총 결합 대역폭을 설정할 수 있습니다. QoS 구성 단계의 일부로 QoS 프로파일 규칙을 물리적 인터페이스에 연결하여 해당 인터페이스를 나가는 트래픽에 대역폭 설정을 적용할 수 있습니다. 개별 QoS 클래스 설정은 해당 QoS 클래스와 일치하는 트래픽에 적용되며(QoS 클래스는 QoS 정책 규칙과 일치하는 트래픽), 프로파일의 전체 대역폭 제한은 모든 일반 텍스트 트래픽, 소스 인터페이스 및 소스 서브넷에서 발생하는 특정 일반 텍스트 트래픽, 모든 터널링된 트래픽 및 개별 터널 인터페이스에 적용될 수 있습니다. 단일 QoS 인터페이스에 여러 프로파일 규칙을 추가하여 해당 인터페이스를 나가는 트래픽에 다양한 대역폭 설정을 적용할 수 있습니다.

다음 필드는 QoS 대역폭 설정을 지원합니다.

 ©2023 Palo Alto Networks, Inc.

- 이그레스**(egress)** 보장 - 일치하는 트래픽에 대해 보장된 대역폭의 양입니다. 이그레스(egress) 보장 대역폭이 초과되면 방화벽은 최선의 방식으로 트래픽을 포워딩합니다. 보장되지만 사용되지 않는 대역폭은 모든 트래픽에 계속 사용할 수 있습니다. QoS 구성에 따라 단일 QoS 클래스, 전체 또는 일부 일반 텍스트 트래픽, 전체 또는 일부 터널링된 트래픽에 대한 대역폭을 보장할 수 있습니다.

  예시:

  클래스 1 트래픽에는 5Gbps의 송신 보장 대역폭이 있습니다. 즉, 5Gbps를 사용할 수 있지만 클래스 1 트래픽용으로 예약되어 있지는 않습니다. 클래스 1 트래픽이 보장된 대역폭을 사용하지 않거나 부분적으로만 사용하는 경우 나머지 대역폭은 다른 클래스의 트래픽에서 사용할 수 있습니다. 그러나 트래픽이 많은 기간 동안에는 클래스 1 트래픽에 대해 5Gbps의 대역폭을 절대적으로 사용할 수 있습니다. 이러한 혼잡 기간 동안 5Gbps를 초과하는 모든 클래스 1 트래픽이 최선의 방법입니다.

- **Egress Max** - 일치하는 트래픽에 대한 전체 대역폭 할당입니다. 방화벽은 사용자가 설정한 최대 이그레스(egress) 제한을 초과하는 트래픽을 삭제합니다. QoS 구성에 따라 QoS 클래스, 전체 또는 일부 일반 텍스트 트래픽, 전체 또는 일부 터널링된 트래픽 및 QoS 인터페이스를 나가는 모든 트래픽에 대해 최대 대역폭 제한을 설정할 수 있습니다.

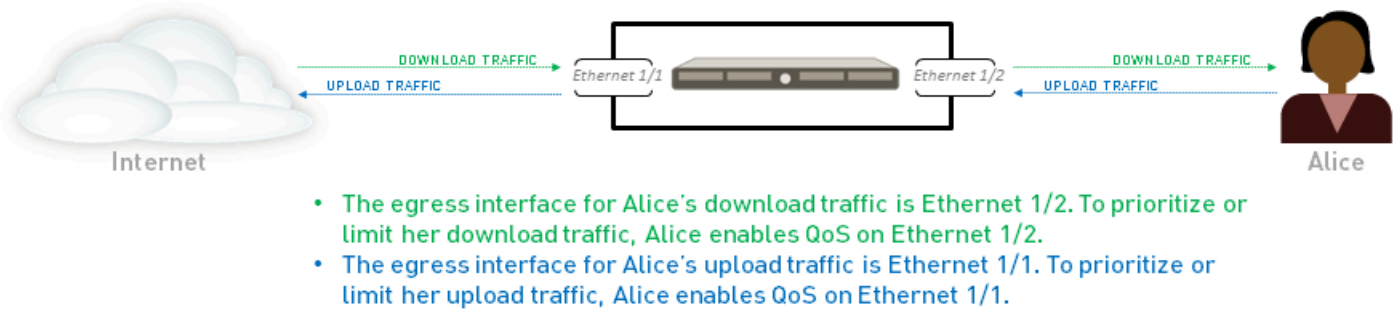
  인터페이스에 연결된 ***QoS*** 프로파일 규칙에 대한 누적 보장 대역폭은 인터페이스에 할당된 총 대역폭을 초과해서는 안 됩니다.

QoS 클래스에 대한 대역폭 설정을 정의하려면 QoS 프로파일 규칙 추가 단계를 참조하십시오. 그런 다음 이러한 대역폭 설정을 일반 텍스트 및 터널링된 트래픽에 적용하고 QoS 인터페이스에 대한 전체 대역폭 제한을 설정하려면 물리적 인터페이스에서 QoS 활성화 단계를 참조하십시오.

## QoS 송신 인터페이스

QoS 처리를 위해 식별된 트래픽의 이그레스(egress) 인터페이스에서 QoS 프로파일 규칙을 사용하도록 설정하면 QoS 구성이 완료됩니다. QoS 트래픽에 대한 인그레스(ingress) 인터페이스는 트래픽이 방화벽으로 들어오는 인터페이스입니다. QoS 트래픽에 대한 이그레스(egress) 인터페이스는 트래픽이 방화벽을 나가는 인터페이스입니다. QoS는 트래픽 플로우에 대한 이그레스(egress) 인터페이스에서 항상 활성화되고 적용됩니다. QoS 구성의 이그레스(egress) 인터페이스는 QoS 처리를 수신하는 트래픽의 흐름에 따라 방화벽의 외부 또는 내부 인터페이스가 될 수 있습니다.

예를 들어 엔터프라이즈 네트워크에서 특정 웹사이트로부터의 직원의 다운로드 트래픽을 제한하는 경우 트래픽 플로우는 인터넷에서 방화벽을 거쳐 회사 네트워크로 포워딩되므로 QoS 구성의 이그레스(egress) 인터페이스는 방화벽의 내부 인터페이스입니다. 또는 직원의 업로드 트래픽을 동일한 웹사이트로 제한하는 경우 제한하는 트래픽이 회사 네트워크에서 방화벽을 거쳐 인터넷으로 흐르기 때문에 QoS 구성의 이그레스(egress) 인터페이스가 방화벽의 외부 인터페이스입니다.




 ©2023 Palo Alto Networks, Inc.

QoS는 방화벽을 나갈 때 트래픽에 적용되므로 방화벽이 NAT(Network Address Translation) 규칙을 비롯한 다른 모든 보안 정책 규칙을 적용한 후에 QoS 정책 규칙이 트래픽에 적용됩니다. 소스를 기반으로 트래픽에 QoS 처리를 적용하려면 QoS 정책 규칙에서 사후 NAT 소스 주소를 지정해야 합니다(사전 NAT 소스 주소를 사용하지 않음).

QoS 처리가 필요한 애플리케이션의 이그레스(egress) 인터페이스를 식별하는 방법에 대해 자세히 알아보십시오.

## 일반 텍스트 및 터널링된 트래픽을 위한 QoS

최소한 QoS 인터페이스를 활성화하려면 인터페이스에서 나가는 일반 텍스트 트래픽에 대한 대역폭 및 우선 순위 설정을 정의하는 기본 QoS 프로파일 규칙을 선택해야 합니다. 그러나 QoS 인터페이스를 설정하거나 수정할 때 나가는 일반 텍스트 트래픽 및 터널링된 트래픽에 세분화된 QoS 설정을 적용할 수 있습니다. QoS 우선 처리 및 대역폭 제한은 터널링된 트래픽, 개별 터널 인터페이스 및/또는 다른 소스 인터페이스 및 소스 서브넷에서 발생하는 일반 텍스트 트래픽에 적용할 수 있습니다. Palo Alto Networks 방화벽에서 터널링된 트래픽은 터널 인터페이스 트래픽, 특히 터널 모드의 IPSec 트래픽을 나타냅니다.

 ©2023 Palo Alto Networks, Inc.

# QoS 구성

다음 단계에 따라 QoS 프로파일 생성, QoS 정책 생성 및 인터페이스에서 QoS 활성화를 포함하는 QoS(서비스 품질)를 구성하십시오.

**STEP 1 |** QoS로 관리할 트래픽을 식별합니다.

이 예는 QoS를 사용하여 웹 브라우징을 제한하는 방법을 보여줍니다.

**ACC**를 선택하여 **Application Command Center** 페이지를 봅니다. **ACC** 페이지의 설정 및 차트를 사용하여 애플리케이션, URL 필터링, 위협 예방, 데이터 필터링 및 HIP 일치와 관련된 트렌드 및 트래픽을 봅니다.

애플리케이션 이름을 클릭하면 자세한 애플리케이션 정보가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** QoS 처리를 받을 애플리케이션의 이그레스(egress) 인터페이스를 식별합니다.



트래픽에 대한 이그레스*(egress)* 인터페이스는 트래픽 플로우에 따라 다릅니다. 수신 트래픽을 형성하는 경우 이그레스*(egress)* 인터페이스는 내부 인터페이스입니다. 나가는 트래픽을 구성하는 경우 이그레스*(egress)* 인터페이스는 외부 인터페이스입니다.

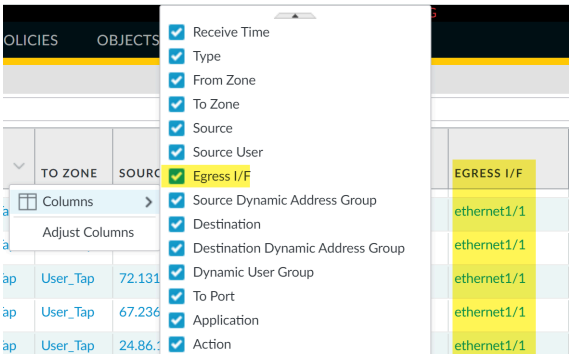
**Monitor** > **Logs** > **Traffic**을 선택하여 트래픽 로그를 봅니다.

특정 애플리케이션에 대한 로그만 필터링하고 표시하려면:

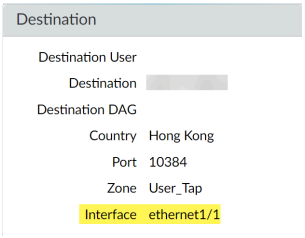
- 애플리케이션에 대한 항목이 표시되면 애플리케이션 열에서 밑줄이 그어진 링크를 클릭한 다음 제출 아이콘을 클릭하십시오.
- 애플리케이션에 대한 항목이 표시되지 않으면 로그 추가 아이콘을 클릭하고 애플리케이션을 검색합니다.

트래픽 로그의 송신 **I/F**는 각 애플리케이션의 이그레스(egress) 인터페이스를 표시합니다. 기본적으로 표시되지 않는 경우 **Egress I/F** 열을 표시하려면:

- 열 헤더를 클릭하여 로그에 열을 추가합니다.




- 항목 왼쪽에 있는 망원경 아이콘을 클릭하면 대상 섹션에 나열된 애플리케이션의 이그레스(egress) 인터페이스가 포함된 자세한 로그가 표시됩니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** QoS 정책 규칙을 추가합니다.

QoS 정책 규칙은 QoS 처리를 받을 트래픽을 정의합니다. 방화벽은 정책 규칙과 일치하는 트래픽에 QoS 서비스 클래스를 할당합니다.

*QoS*는 방화벽을 나갈 때 트래픽에 적용되므로 방화벽이 *NAT(Network Address Translation)* 규칙을 비롯한 다른 모든 보안 정책 규칙을 적용한 후에 *QoS* 정책 규칙이 트래픽에 적용됩니다. 소스를 기반으로 트래픽에 *QoS* 처리를 적용하려면 *QoS* 정책 규칙에서 사후 *NAT* 소스 주소를 지정해야 합니다(사전 *NAT* 소스 주소를 사용하지 않음).

1. 정책 > **QoS**를 선택하고 새 정책 규칙을 추가합니다.
2. 일반 탭에서 QoS 정책 규칙에 설명적인 이름을 지정합니다.
3. 소스, 대상, 애플리케이션, 서비스/**URL** 카테고리 및 **DSCP/ToS** 값을 기반으로 QoS 처리를 수신할 트래픽을 지정합니다(**DSCP/ToS** 설정을 사용하면 DSCP 분류 기반 QoS를 적용할 수 있음).

   예를 들어, 애플리케이션을 선택한 다음 추가를 클릭한 후 웹 브라우징을 선택하여 웹 브라우징 트래픽에 QoS를 적용합니다.
4. (선택 사항) 계속해서 추가 매개변수를 정의합니다. 예를 들어, 특정 사용자의 웹 트래픽에 QoS를 제공하려면 소스 및 추가를 소스 사용자로 선택합니다.
5. 기타 설정을 선택하고 정책 규칙과 일치하는 트래픽에 **QoS** 클래스를 할당합니다. 예를 들어, 클래스 2를 user1의 웹 트래픽에 할당합니다.
6. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** QoS 프로파일 규칙을 추가합니다.

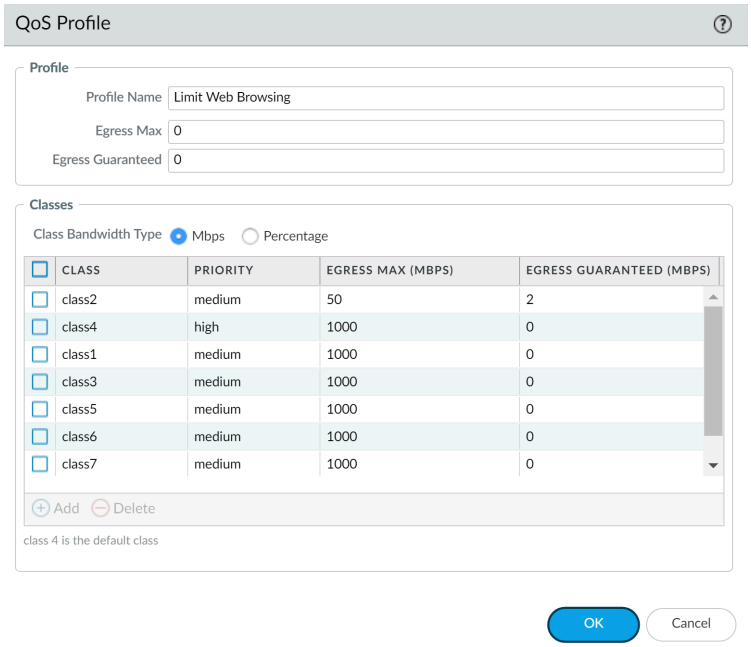
QoS 프로파일 규칙을 사용하면 우선 순위를 포함하여 트래픽이 수신할 수 있는 8가지 서비스 클래스를 정의하고 QoS 대역폭 관리를 활성화할 수 있습니다.

QoS 프로파일 이름을 클릭하여 기본값을 포함하여 기존 QoS 프로파일을 편집할 수 있습니다.

1. 네트워크 > 네트워크 프로파일 > **QoS** 프로파일을 선택하고 새 프로파일을 추가합니다.
2. 설명이 포함된프로파일 이름을 입력합니다.
3. QoS 프로파일 규칙에 대한 전체 대역폭 제한을 설정합니다.
   - QoS 프로파일 규칙에 대한 전체 대역폭 할당을 설정하려면 **Egress Max** 값을 입력합니다.
   - QoS 프로파일에 대해 보장된 대역폭을 설정하려면 **Egress Guaranteed** 값을 입력합니다.

   *Egress Guaranteed* 값을 초과하는 모든 트래픽은 최선의 값이며 보장되지 않습니다. 보장되지만 사용되지 않는 대역폭은 모든 트래픽에 계속 사용할 수 있습니다.
4. 클래스 섹션에서 최대 8개의 개별 QoS 클래스를 처리하는 방법을 지정합니다.
   1. QoS 프로파일에 클래스를 추가합니다.
   2. 실시간, 높음, 중간 또는 낮음 중에서 클래스의 우선 순위를 선택합니다.
   3. 각 QoS 클래스에 할당된 트래픽에 대한 **Egress Max** 및 **Egress Guaranteed** 대역폭을 입력합니다.
5. 확인을 클릭합니다.

다음 예에서 QoS 프로파일 규칙 웹 브라우징 제한은 클래스 2 트래픽을 최대 대역폭 50Mbps 및 보장된 대역폭 2Mbps로 제한합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 물리적 인터페이스에서 QoS를 활성화합니다.

이 단계의 일부에는 고유한 QoS 처리를 위해 일반 텍스트 및 터널링된 트래픽을 선택하는 옵션이 포함됩니다.

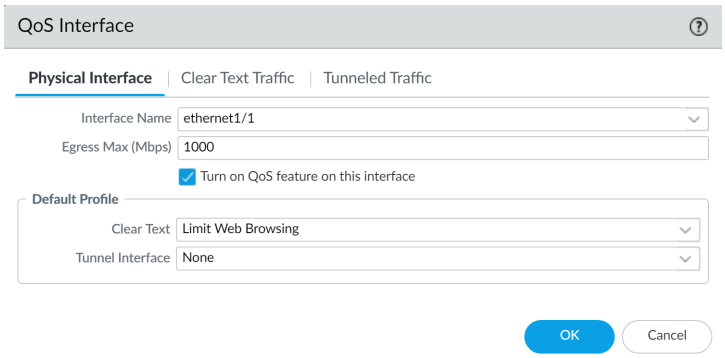
제품 사양 요약을 검토하여 사용 중인 방화벽 모델이 하위 인터페이스에서 ***QoS*** 활성화를 지원하는지 확인하십시오.

1. 네트워크 > **QoS**를 선택하고 QoS 인터페이스를 추가합니다.
2. 물리적 인터페이스를 선택하고 QoS를 활성화할 인터페이스의 인터페이스 이름을 선택합니다.

   이 예에서 이더넷 1/1은 웹 브라우징 트래픽의 이그레스(egress) 인터페이스입니다(2단계 참조).
3. 이 인터페이스를 나가는 모든 트래픽에 대해 **Egress Max** 대역폭을 설정합니다.

   ***QoS*** 인터페이스에 대해 항상 ***Egress Max*** 값을 정의하는 것이 가장 좋습니다. 인터페이스에 연결된 ***QoS*** 프로파일 규칙에 대한 누적 보장 대역폭이 인터페이스에 할당된 총 대역폭을 초과하지 않는지 확인합니다.
4. 이 인터페이스에서 **QoS** 기능 켜기를 선택합니다.
5. 기본 프로파일 섹션에서 물리적 인터페이스를 나가는 모든 일반 텍스트 트래픽에 적용할 QoS 프로파일 규칙을 선택합니다.
6. (선택 사항) 인터페이스를 나가는 모든 터널링된 트래픽에 적용할 기본 QoS 프로파일 규칙을 선택합니다.

예를 들어 이더넷 1/1에서 QoS를 활성화하고 일반 텍스트 송신 트래픽에 대한 기본 설정으로 사용할 QoS 프로파일 규칙 웹 브라우징 제한(4단계)에 대해 정의한 대역폭 및 우선 순위 설정을 적용합니다.




1. (선택 사항) 일반 텍스트 및 터널링된 트래픽에 대한 QoS를 제공하기 위해 더 세분화된 설정을 계속 정의합니다. 일반 텍스트 트래픽 탭 및 터널링된 트래픽 탭에서 구성된 설정은 물리적 인터

 ©2023 Palo Alto Networks, Inc.

페이스 탭의 일반 텍스트 및 터널링된 트래픽에 대한 기본 프로파일 설정을 자동으로 무시합니다.

- 일반 텍스트 트래픽을 선택한 다음:
  - 일반 텍스트 트래픽에 대해 **Egress Guaranteed** 및 **Egress Max** 대역폭을 설정합니다.
  - 추가를 클릭하고 QoS 프로파일 규칙을 적용하여 원본 인터페이스 및 원본 서브넷을 기반으로 일반 텍스트 트래픽을 적용합니다.

    *(PA-3200 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈만 해당)* 특정 하위 인터페이스에 규칙이 적용되는 경우 *QoS* 정책 규칙을 구성할 때 대상 인터페이스도 선택해야 합니다.
- 터널링된 트래픽을 선택한 다음:
  - 터널링된 트래픽에 대해 **Egress Guaranteed** 및 **Egress Max** 대역폭을 설정합니다.
  - 추가를 클릭하고 QoS 프로파일 규칙을 단일 터널 인터페이스에 연결합니다.

2. 확인을 클릭합니다.

**STEP 6 |** 변경 사항을 커밋합니다.

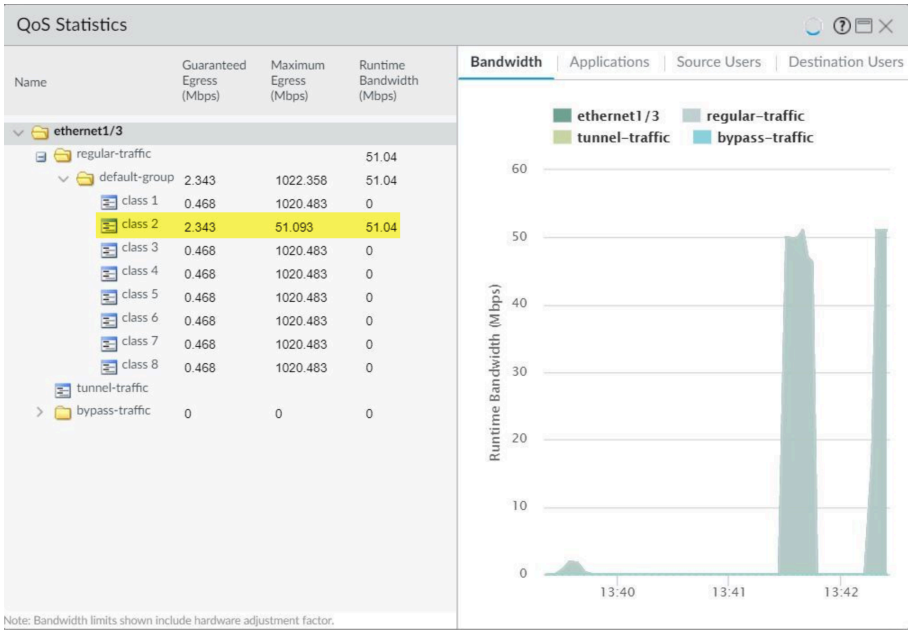
커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** QoS 구성을 확인합니다.

**Network** > **QoS**를 선택한 다음 통계를 선택하여 QoS 대역폭, 선택한 QoS 클래스의 활성 세션 및 선택한 QoS 클래스에 대한 활성 애플리케이션을 봅니다.

예를 들어 QoS가 활성화된 이더넷 1/3에 대한 통계를 참조하십시오.




클래스 2 트래픽은 2.343Mbps의 보장된 대역폭과 51.093Mbps의 최대 대역폭으로 제한됩니다.

탭을 계속 클릭하여 애플리케이션, 소스 사용자, 대상 사용자, 보안 규칙 및 QoS 규칙에 대한 추가 정보를 표시합니다.

***QoS*** 통계 창에 표시된 대역폭 제한에는 하드웨어 조정 요소가 포함됩니다.

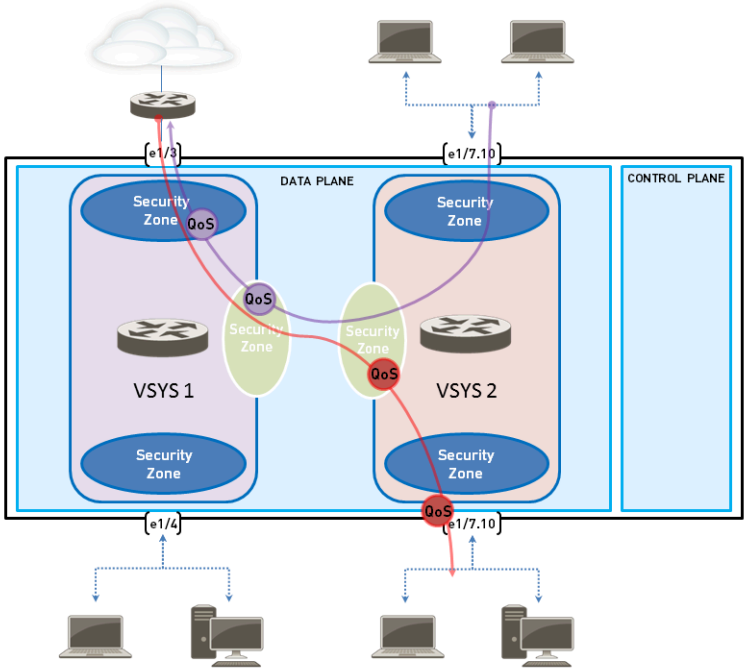

©2023 Palo Alto Networks, Inc.

# 가상 시스템에 대한 QoS 구성

QoS는 Palo Alto Networks 방화벽에 구성된 단일 또는 여러 가상 시스템에 대해 구성할 수 있습니다. 가상 시스템은 독립적인 방화벽이므로 단일 가상 시스템에 대해 QoS를 독립적으로 구성해야 합니다.

가상 시스템에 대한 QoS 구성은 물리적 방화벽에서 QoS를 구성하는 것과 유사하지만 가상 시스템에 대한 QoS를 구성하려면 트래픽의 소스 및 대상을 지정해야 합니다. 가상 시스템은 물리적 경계를 설정하지 않고 존재하고 가상 환경의 트래픽은 둘 이상의 가상 시스템에 걸쳐 있기 때문에 트래픽에 대한 소스 및 대상 영역과 인터페이스를 지정하는 것은 단일 가상 시스템에 대한 트래픽을 제어하고 형성하는 데 필요합니다.

아래 예는 방화벽에 구성된 두 개의 가상 시스템을 보여줍니다. VSYS 1(보라색) 및 VSYS 2(빨간색)에는 각각 해당 보라색(VSYS 1) 및 빨간색(VSYS 2) 라인으로 표시된 두 개의 고유한 트래픽 플로우의 우선 순위를 지정하거나 제한하도록 QoS가 구성되어 있습니다. QoS 노드는 트래픽의 지점이 QoS 정책과 일치하고 QoS 서비스 클래스가 할당되었음을 나타내며 나중에 트래픽이 방화벽을 벗어날 때 형성되는 지점을 나타냅니다.




가상 시스템 및 구성 방법에 대한 정보는 가상 시스템을 참조하십시오.

**STEP 1 |** 적절한 인터페이스, 가상 라우터 및 보안 영역이 각 가상 시스템과 연결되어 있는지 확인합니다.

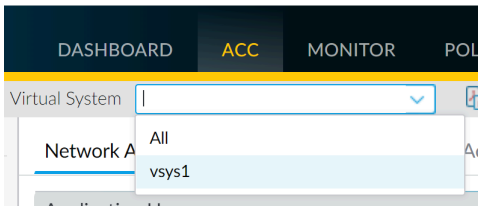
- 구성된 인터페이스를 보려면 **Network** > **Interface**를 선택하십시오.
- 구성된 영역을 보려면 네트워크 > 영역을 선택합니다.
- 정의된 가상 라우터에 대한 정보를 보려면 **Network** > **Virtual** 라우터를 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** QoS를 적용할 트래픽을 식별합니다.

**ACC**를 선택하여 **Application Command Center** 페이지를 봅니다. **ACC** 페이지의 설정 및 차트를 사용하여 애플리케이션, URL 필터링, 위협 예방, 데이터 필터링 및 HIP 일치와 관련된 트렌드 및 트래픽을 봅니다.

특정 가상 시스템에 대한 정보를 보려면 가상 시스템 드롭다운에서 가상 시스템을 선택합니다.




애플리케이션 이름을 클릭하면 자세한 애플리케이션 정보가 표시됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** QoS 처리가 필요한 것으로 식별한 애플리케이션의 이그레스(egress) 인터페이스를 식별하십시오.

가상 시스템 환경에서 QoS는 가상 시스템의 트래픽 송신 지점에 있는 트래픽에 적용됩니다. 가상 시스템에 대한 구성 및 QoS 정책에 따라 QoS 트래픽의 출구 지점은 물리적 인터페이스와 연결되거나 영역이 될 수 있습니다.

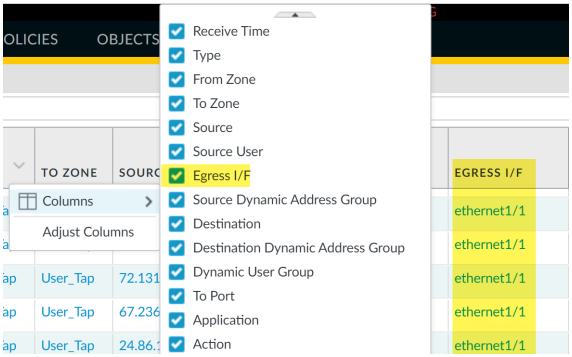
이 예는 vsys 1에서 웹 브라우징 트래픽을 제한하는 방법을 보여줍니다.

트래픽 로그를 보려면 **Monitor** > **Logs** > **Traffic**을 선택합니다. 각 항목에는 가상 시스템 환경에서 QoS를 구성하는 데 필요한 정보가 있는 열을 표시하는 옵션이 있습니다.

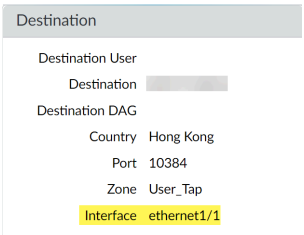
- 가상 시스템
- 출구 인터페이스
- 인그레스(ingress) 인터페이스
- 소스 영역
- 목적지 영역

기본적으로 표시되지 않는 열을 표시하려면 다음을 수행합니다.

- 열 헤더를 클릭하여 로그에 열을 추가합니다.




- 항목 왼쪽에 있는 망원경 아이콘을 클릭하면 소스 및 대상 섹션에 애플리케이션의 이그레스(egress) 인터페이스와 소스 및 대상 영역이 포함된 자세한 로그가 표시됩니다.




예를 들어, VSYS 1의 웹 브라우징 트래픽의 경우 수신 인터페이스는 이더넷 1/2, 이그레스(egress) 인터페이스는 이더넷 1/1, 소스 영역은 트러스트, 대상 영역은 비신뢰입니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** QoS 프로파일을 생성합니다.

프로파일 이름을 클릭하여 기본값을 포함하여 기존 QoS 프로파일을 편집할 수 있습니다.

1. 네트워크 > 네트워크 프로파일 > **QoS** 프로파일을 선택하고 추가를 클릭하여 QoS 프로파일 대화 상자를 엽니다.
2. 설명이 포함된프로파일 이름을 입력합니다.
3. QoS 프로파일에 대한 전체 대역폭 할당을 설정하려면 **Egress Max**를 입력하십시오.
4. QoS 프로파일에 대해 보장된 대역폭을 설정하려면 **Egress Guaranteed**를 입력합니다.

   *QoS* 프로파일의 송신 보장 제한을 초과하는 모든 트래픽은 최선의 노력이지만 보장되지는 않습니다.
5. **QoS** 프로파일의 클래스 섹션에서 최대 8개의 개별 QoS 클래스를 처리하는 방법을 지정합니다.
   1. 추가를 클릭하여 QoS 프로파일에 클래스를 추가합니다.
   2. 클래스의 우선 순위를 선택합니다.
   3. 클래스의 **Egress Max**를 입력하여 해당 개별 클래스에 대한 전체 대역폭 제한을 설정합니다.
   4. 해당 개별 클래스에 대해 보장된 대역폭을 설정하려면 클래스에 대해 **Egress Guaranteed**를 입력합니다.
6. 확인을 클릭하여 QoS 프로파일을 저장합니다.

**STEP 5 |** QoS 정책을 생성합니다.

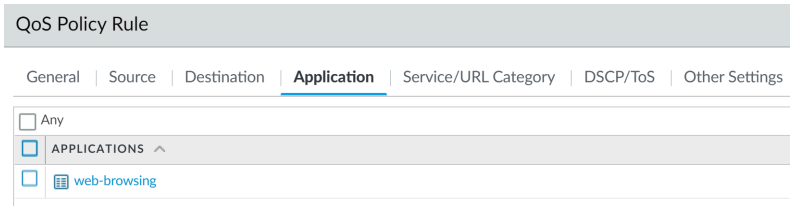
여러 가상 시스템이 있는 환경에서 트래픽은 둘 이상의 가상 시스템에 걸쳐 있습니다. 이 때문에 가상 시스템에 대해 QoS를 활성화할 때 소스 및 대상 영역을 기반으로 QoS 처리를 수신하도록 트래픽을 정

 ©2023 Palo Alto Networks, Inc.

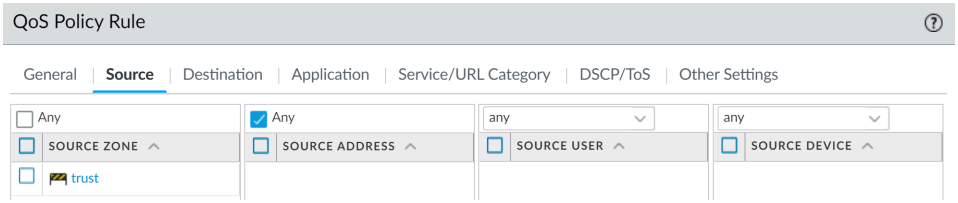
의해야 합니다. 이렇게 하면 트래픽이 해당 가상 시스템에 대해서만 우선 순위가 지정되고 모양이 지정됩니다(트래픽이 플로우될 수 있는 다른 가상 시스템에는 적용되지 않음).

1. 정책 > **QoS**를 선택하고 QoS 정책 규칙을 추가합니다.
2. 일반을 선택하고 QoS 정책 규칙에 설명적인 이름을 지정합니다.
3. QoS 정책 규칙을 적용할 트래픽을 지정합니다. 소스, 대상, 애플리케이션 및 서비스**/URL** 카테고리 탭을 사용하여 트래픽 식별을 위한 일치 매개변수를 정의합니다.

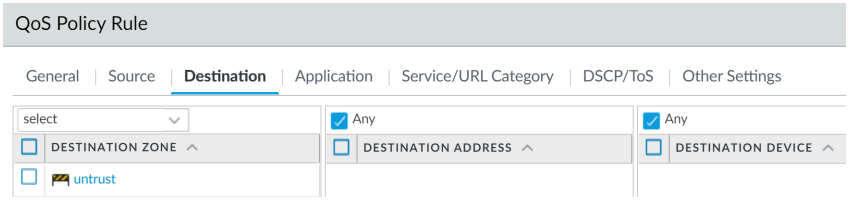
   예를 들어 애플리케이션 및 웹 탐색 추가를 선택하여 QoS 정책 규칙을 해당 애플리케이션에 적용합니다.



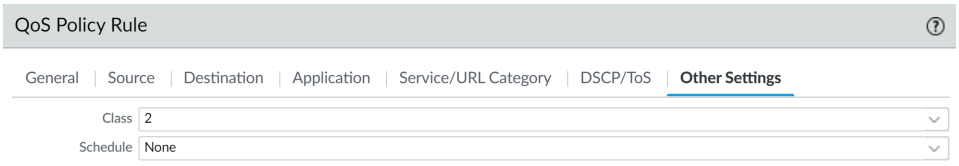

4. vsys 1 웹 브라우징 트래픽의 소스 영역 소스 및 추가를 선택합니다.




5. vsys 1 웹 브라우징 트래픽의 대상 영역 대상 및 추가를 선택합니다.




6. 기타 설정을 선택한 다음 QoS 정책 규칙에 할당할 **QoS** 클래스를 선택합니다. 예를 들어 vsys 1의 웹 브라우징 트래픽에 클래스 2를 할당합니다.




7. 확인을 클릭하여 QoS 정책 규칙을 저장합니다.

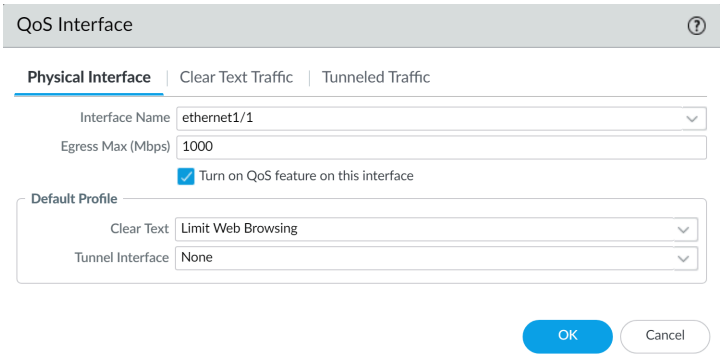

©2023 Palo Alto Networks, Inc.

**STEP 6 |** 물리적 인터페이스에서 QoS 프로파일을 활성화합니다.

*QoS* 인터페이스에 대해 항상 ***Egress Max*** 값을 정의하는 것이 가장 좋습니다.

1. 네트워크 > **QoS**를 선택하고 추가를 클릭하여 QoS 인터페이스 대화 상자를 엽니다.
2. 물리적 인터페이스에서 QoS 활성화:
   1. 물리적 인터페이스 탭에서 QoS 프로파일을 적용할 인터페이스의 인터페이스 이름을 선택합니다.

      이 예에서 이더넷 1/1은 vsys 1의 웹 브라우징 트래픽에 대한 이그레스(egress) 인터페이스입니다(2단계 참조).




   2. 이 인터페이스에서 **QoS** 기능 켜기를 선택합니다.
3. 물리적 인터페이스 탭에서 모든 일반 텍스트 트래픽에 적용할 기본 QoS 프로파일을 선택합니다.

   (선택 사항) 터널 인터페이스 필드를 사용하여 모든 터널링된 트래픽에 기본 QoS 프로파일을 적용합니다.
4. (선택 사항) 일반 텍스트 트래픽 탭에서 일반 텍스트 트래픽에 대한 추가 QoS 설정을 구성합니다.
   - 일반 텍스트 트래픽에 대해 **Egress Guaranteed** 및 **Egress Max** 대역폭을 설정합니다.
   - 추가를 클릭하여 선택한 일반 텍스트 트래픽에 QoS 프로파일을 적용하고 소스 인터페이스 및 소스 서브넷(QoS 노드 생성)에 따라 QoS 처리를 위한 트래픽을 추가로 선택합니다.
5. (선택 사항) 터널링된 트래픽 탭에서 터널 인터페이스에 대한 추가 QoS 설정을 구성합니다.
   - 터널링된 트래픽에 대해 **Egress Guaranteed** 및 **Egress Max** 대역폭을 설정합니다.
   - 선택한 터널 인터페이스를 QoS 프로파일과 연결하려면 추가를 클릭합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.
7. 변경 사항을 커밋합니다.

**STEP 7 |** QoS 구성을 확인합니다.

- QoS 정책 페이지를 보려면 네트워크 > **QoS**를 선택하십시오. **QoS** 정책 페이지는 QoS가 활성화되어 있고 통계 링크를 포함하는지 확인합니다. 통계 링크를 클릭하면 QoS 대역폭, 선택한 QoS 노드


©2023 Palo Alto Networks, Inc.

또는 클래스의 활성 세션, 선택한 QoS 노드 또는 클래스에 대한 활성 애플리케이션을 볼 수 있습니다.

- Multi-VSYS 환경에서 세션은 여러 시스템에 걸쳐 있을 수 없습니다. 트래픽이 둘 이상의 가상 시스템을 통과하는 경우 하나의 트래픽 플로우에 대해 여러 세션이 생성됩니다. 방화벽에서 실행 중인 세션을 탐색하고 적용된 QoS 규칙 및 QoS 클래스를 보려면 **Monitor** > **Session Browser**를 선택합니다.


©2023 Palo Alto Networks, Inc.

# DSCP 분류를 기반으로 QoS 적용

DSCP(Differentiated Services Code Point)는 트래픽에 대해 높은 우선 순위 또는 최선의 포워딩을 요청하는 데 사용할 수 있는 패킷 헤더 값입니다. 세션 기반 DSCP 분류를 사용하면 수신 트래픽에 대한 DSCP 값을 존중하고 세션 트래픽이 방화벽을 나갈 때 DSCP 값으로 세션을 표시할 수 있습니다. 이렇게 하면 세션에 대한 모든 인바운드 및 아웃바운드 트래픽이 네트워크를 통해 흐를 때 지속적인 QoS 처리를 받을 수 있습니다. 예를 들어, 외부 서버로부터의 인바운드 리턴 트래픽은 이제 방화벽이 세션 시작 시 감지한 DSCP 값을 기반으로 아웃바운드 흐름에 대해 방화벽이 처음에 적용한 것과 동일한 QoS 우선 순위로 처리될 수 있습니다. 그러면 방화벽과 최종 사용자 사이의 네트워크 디바이스도 반환 트래픽(및 세션에 대한 다른 모든 아웃바운드 또는 인바운드 트래픽)에 대해 동일한 우선 순위를 적용합니다.

***SSL*** 포워딩 프록시, ***SSL*** 인바운드 검사 및 ***SSH*** 프록시 트래픽에는 ***DSCP*** 코드 포인트 또는 ***QoS***를 적용할 수 없습니다.

다양한 유형의 DSCP 표시는 다양한 서비스 수준을 나타냅니다.

이 단계를 완료하면 방화벽이 세션 시작 시 감지된 동일한 DSCP 값으로 트래픽을 표시할 수 있습니다(이 예에서 방화벽은 DSCP AF11 값으로 반환 트래픽을 표시함). QoS를 구성하면 트래픽이 방화벽을 나갈 때 트래픽을 형성할 수 있지만 보안 규칙에서 이 옵션을 활성화하면 방화벽과 클라이언트의 중간에 있는 다른 네트워크 디바이스가 DSCP로 표시된 트래픽에 대해 우선 순위를 계속 적용할 수 있습니다.

- 신속 포워딩**(EF)**: 트래픽에 대해 낮은 손실, 낮은 대기 시간 및 보장된 대역폭을 요청하는 데 사용할 수 있습니다. EF 코드포인트 값이 있는 패킷은 일반적으로 가장 높은 우선 순위 포워딩이 보장됩니다.
- 확실한 포워딩**(AF)**: 애플리케이션에 대한 안정적인 포워딩을 제공하는 데 사용할 수 있습니다. AF 코드포인트가 있는 패킷은 트래픽이 최선의 서비스가 제공하는 것보다 더 높은 우선순위 처리를 받기 위한 요청을 나타냅니다(EF 코드포인트가 있는 패킷은 AF 코드포인트가 있는 패킷보다 계속 우선권을 가짐).
- 클래스 선택기**(CS)**: IP 우선 순위 필드를 사용하여 우선 순위 트래픽을 표시하는 네트워크 디바이스와의 역호환성을 제공하는 데 사용할 수 있습니다.
- **IP** 우선 순위**(ToS)**: 레거시 네트워크 디바이스에서 우선 순위 트래픽을 표시하는 데 사용할 수 있습니다(IP Precedence 헤더 필드는 DSCP 분류가 도입되기 전에 패킷의 우선 순위를 나타내는 데 사용되었습니다).
- 사용자 지정 코드포인트: 코드 포인트 이름 및 바이너리 값을 입력하여 트래픽과 일치하도록 사용자 정의 코드 포인트를 생성합니다.

예를 들어 **AF(Assured Forwarding)**를 선택하여 AF 코드포인트 값으로 표시된 트래픽이 더 낮은 우선순위를 수신하도록 표시된 애플리케이션보다 안정적인 포워딩을 위해 더 높은 우선순위를 갖도록 합니다. 다음 단계를 사용하여 세션 기반 DSCP 분류를 활성화하십시오. 세션 시작 시 감지된 DSCP 표시를 기반으로 QoS를 구성하여 시작합니다. 그런 다음 초기 아웃바운드 흐름에 대해 QoS를 적용하는 데 사용된 것과 동일한 DSCP 값을 사용하여 세션에 대한 반환 흐름을 표시하도록 방화벽을 계속 활성화할 수 있습니다.

**STEP 1 |** QoS를 구성하기 위한 예비 단계를 수행합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** DSCP 값을 기반으로 QoS 처리를 받을 트래픽을 정의합니다.

1. 정책 > **QoS**를 선택한 다음 기존 QoS 규칙을 추가 또는 수정하고 필수 필드를 채웁니다.
2. **DSCP/ToS**를 선택한 다음 코드포인트를 선택합니다.
3. QoS를 적용할 DSCP/ToS 코드포인트를 추가합니다.
4. 트래픽과 일치시킬 QoS 규칙에 대한 DSCP/ToS 표시 유형을 선택합니다.

   단일 ***DSCP*** 유형을 사용하여 네트워크 트래픽을 관리하고 우선 순위를 지정하는 것이 가장 좋습니다.

5. **Codepoint** 값을 지정하여 QoS 정책을 보다 세분화된 규모의 트래픽과 일치시킵니다. 예를 들어 일치할 정책의 DSCP 값 유형으로 AF(Assured Forwarding)를 선택한 경우 AF11과 같은 AF 코드포인트 값을 추가로 지정합니다.

   ***EF(Expedited Forwarding)***가 ***DSCP*** 표시 유형으로 선택되면 세분화된 ***Codepoint*** 값을 지정할 수 없습니다. ***QoS*** 정책 규칙은 ***EF*** 코드 포인트 값으로 표시된 트래픽과 일치합니다.

6. 기타 설정을 선택한 다음 QoS 규칙과 일치하는 트래픽에 **QoS** 클래스를 할당합니다. 이 예에서는 세션의 첫 번째 패킷에 대해 AF11의 DSCP 표시가 감지된 세션에 클래스 1을 할당합니다.
7. 확인을 클릭하여 QoS 규칙을 저장합니다.

**STEP 3 |** 세션 시작 시 감지된 DSCP 표시를 기반으로 QoS 규칙과 일치할 때 수신할 트래픽의 QoS 우선 순위를 정의합니다.

1. 네트워크 > 네트워크 프로파일 > **QoS** 프로파일을 선택한 다음 기존 QoS 프로파일을 추가하거나 수정합니다. 트래픽에 대한 우선 순위 및 대역폭을 설정하는 프로파일 옵션에 대한 자세한 내용은 QoS 개념 및 QoS 구성을 참조하십시오.
2. 프로파일 클래스를 추가하거나 수정합니다. 예를 들어, 2단계는 AF11 트래픽을 클래스 1 트래픽으로 분류하는 단계를 보여 주었으므로 클래스**1** 항목을 추가하거나 수정할 수 있습니다.
3. 높음과 같은 트래픽 클래스에 대한 우선 순위를 선택합니다.
4. 확인을 클릭하여 QoS 프로파일을 저장합니다.

**STEP 4 |** 인터페이스에서 QoS를 활성화합니다.

**Network** > **QoS**를 선택한 다음 기존 인터페이스를 추가 또는 수정하고 이 인터페이스에서 **QoS** 기능을 켭니다.

이 예에서 AF11 DSCP 표시가 있는 트래픽은 QoS 규칙과 일치하고 클래스 1이 할당됩니다. 인터페이스에서 활성화된 QoS 프로파일은 클래스 1 트래픽이 방화벽을 나갈 때 높은 우선 순위 처리를 적용합니다(세션 아웃바운드 트래픽).

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** DSCP 표시를 활성화합니다.

반환 트래픽을 DSCP 값으로 표시하여 세션의 인바운드 흐름이 아웃바운드 흐름에 대해 감지된 동일한 DSCP 값으로 표시되도록 합니다.

1. 정책 > 보안을 선택한 다음 보안 정책을 추가 또는 수정합니다.
2. 작업을 선택한 다음 **QoS** 표시 드롭다운에서 클라이언트-서버 흐름 따르기를 선택합니다
3. 확인을 클릭하여 변경 사항을 저장합니다.

이 단계를 완료하면 방화벽이 세션 시작 시 감지된 동일한 DSCP 값으로 트래픽을 표시할 수 있습니다(이 예에서 방화벽은 DSCP AF11 값으로 반환 트래픽을 표시함). QoS를 구성하면 트래픽이 방화벽을 나갈 때 트래픽을 형성할 수 있지만 보안 규칙에서 이 옵션을 활성화하면 방화벽과 클라이언트의 중간에 있는 다른 네트워크 디바이스가 DSCP로 표시된 트래픽에 대해 우선 순위를 계속 적용할 수 있습니다.

**STEP 6 |** 구성을 커밋합니다.

변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

# QoS 사용 사례

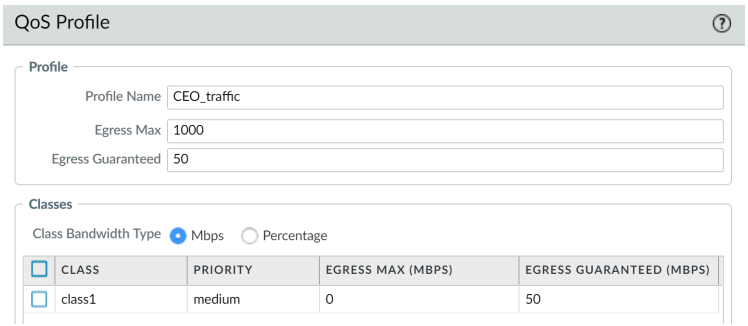
다음 사용 사례는 일반적인 시나리오에서 QoS를 사용하는 방법을 보여줍니다.

- 사용 사례: 단일 사용자를 위한 QoS
- 사용 사례: 음성 및 비디오 애플리케이션을 위한 QoS

## 사용 사례: 단일 사용자를 위한 QoS

한 CEO는 네트워크 사용량이 높은 시기에 엔터프라이즈 애플리케이션에 액세스하여 중요한 비즈니스 커뮤니케이션에 효과적으로 대응할 수 없다는 사실을 발견했습니다. IT 관리자는 CEO와 주고받는 모든 트래픽이 다른 직원 트래픽보다 우선적으로 처리되어 중요한 네트워크 리소스에 대한 액세스는 물론 고성능도 보장되기를 원합니다.

**STEP 1 |** 관리자는 QoS 프로파일 ***CEO_traffic***을 생성하여 CEO로부터 발생하는 트래픽이 회사 네트워크에서 유출될 때 처리되고 형성되는 방식을 정의합니다.




관리자는 네트워크 혼잡에 관계없이 CEO가 항상 자신에게 보장된 대역폭(필요 사용량 이상)을 보장하기 위해 50Mbps의 보장된 대역폭(이그레스**(egress)** 보장)을 할당합니다.

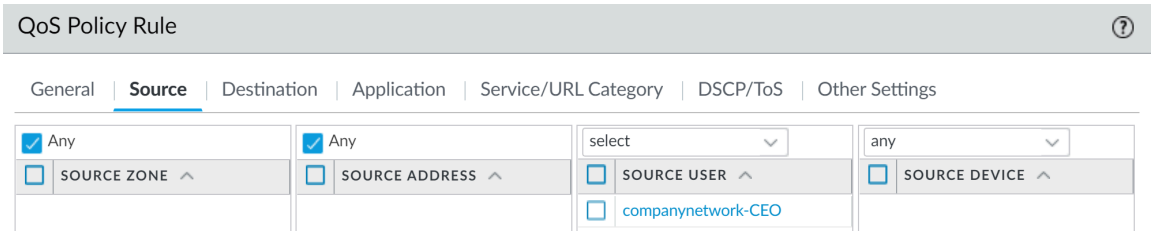
관리자는 계속해서 클래스 1 트래픽을 높은 우선순위로 지정하고 프로파일의 최대 대역폭 사용량(**Egress Max**)을 관리자가 QoS를 활성화할 인터페이스의 최대 대역폭과 동일한 1000Mbps로 설정합니다. 관리자는 CEO의 대역폭 사용량을 어떤 식으로든 제한하지 않기로 결정했습니다.

프로파일의 최대 대역폭이 인터페이스의 최대 대역폭과 일치하더라도 ***QoS*** 프로파일에 대한 ***Egress Max*** 필드를 채우는 것이 좋습니다. ***QoS*** 프로파일의 최대 대역폭은 ***QoS***를 사용하도록 계획하는 인터페이스의 최대 대역폭을 초과해서는 안 됩니다.

**STEP 2 |** 관리자는 QoS 정책을 만들어 CEO의 트래픽**Policies** > **QoS**)을 식별하고 QoS 프로파일에 정의한 클래스를 할당합니다(참조 이전 단계). 사용자 ID가 구성되므로 관리자는 QoS 정책의 소스 탭을 사


©2023 Palo Alto Networks, Inc.

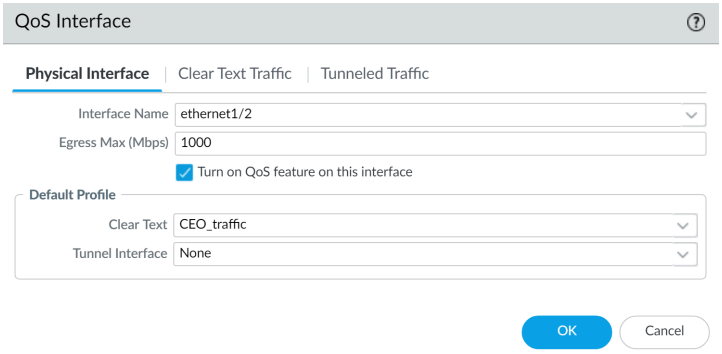
용하여 회사 네트워크 사용자명으로 CEO의 트래픽을 단독으로 식별합니다. 사용자 ID가 구성되지 않은 경우 관리자는 소스 주소 아래에 CEO의 IP 주소를 추가할 수 있습니다. User-ID 참조):




관리자는 CEO의 트래픽을 클래스1(기타 설정 탭)과 연결한 다음 나머지 필수 정책 필드를 계속 채웁니다. 관리자는 정책에 설명 이름(일반 탭)을 제공하고 소스 영역(소스 탭) 및 대상 영역(대상 탭)에 대해 모두를 선택합니다.

| | NAME | TAGS | Source | | | | Destination | | | APPLICATION | SERVICE | DSCP/TOS | CLASS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | | |
| 1 | HTTPS | none | trust | any | any | any | untrust | any | any | web-browsing | any | any | 2 |
| 2 | Voice-Video | none | any | any | any | any | any | any | any | voip-video-l... | any | any | 1 |
| 3 | Guarantee CEO bandwidth | none | any | any | companynet... | any | any | any | any | any | any | any | 1 |

**STEP 3 |** 이제 클래스 1이 CEO의 트래픽과 연결되었으므로 관리자는 인터페이스에서 **QoS** 기능 켜기를 선택하고 트래픽 흐름의 송신 인터페이스를 선택하여 QoS를 활성화합니다. CEO의 트래픽 흐름을 위한 이그레스 인터페이스는 외부 인터페이스이며 이 경우 이더넷 1/2입니다.



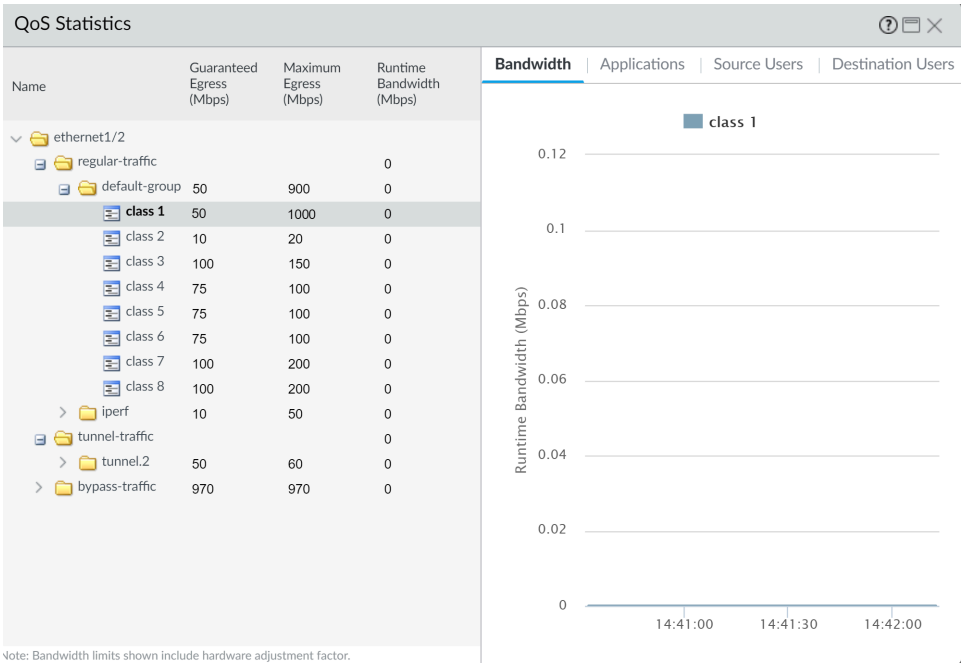

관리자는 CEO 측에서 발생하는 모든 트래픽이 그가 만든 QoS 프로파일 및 관련 QoS 정책에 의해 보장되도록 하기를 원하기 때문에, 이더넷 1/2에서 흐르는 **Clear Text** 트래픽에 적용할 ***CEO_traffic***을 선택합니다.

**STEP 4 |** QoS 구성을 커밋한 후 관리자는 네트워크 > **QoS** 페이지로 이동하여 QoS 프로파일 CEO_traffic이 외부 인터페이스, 이더넷 1/2에서 활성화되어 있는지 확인합니다.

| NAME | GUARANTEED EGRESS (MBPS) | MAXIMUM EGRESS (MBPS) | PROFILE | ENABLED | |
|---|---|---|---|---|---|
| ethernet1/2 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 50.000 | | CEO_traffic | | |


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 그는 통계를 클릭하여 이더넷 1/2에서 유입될 때 CEO(클래스 1) 측에서 발생하는 트래픽이 어떻게 형성되는지 확인합니다.




이 경우 단일 소스 사용자에서 발생하는 트래픽에 ***QoS***를 적용하는 방법을 보여 줍니다. 그러나 대상 사용자에게 트래픽을 보장하거나 형성하려는 경우에도 유사한 ***QoS*** 설정을 구성할 수 있습니다. 이 워크플로 대신 또는 이에 추가하여 사용자의 ***IP*** 주소를 정책 > ***QoS*** 페이지(사용자의 소스 정보를 지정하는 대신)의 대상 주소로 지정하는 ***QoS*** 정책을 만들고, ***Network*** > ***QoS*** 페이지(외부 인터페이스 대신)의 네트워크 내부 인터페이스에서 ***QoS***를 활성화합니다.

## 사용 사례: 음성 및 비디오 애플리케이션을 위한 QoS

음성 및 비디오 트래픽은 QoS 기능이 형성하고 제어하는 측정, 특히 대기 시간 및 지터에 특히 민감합니다. 음성 및 비디오 전송을 들을 수 있고 명확하게 하려면 음성 및 비디오 패킷이 삭제되거나 지연되거나 일관되지 않게 포워딩될 수 없습니다. 대역폭을 보장하는 것 외에도 음성 및 비디오 애플리케이션에 대한 모범 사례는 음성 및 비디오 트래픽에 대한 우선 순위를 보장하는 것입니다.

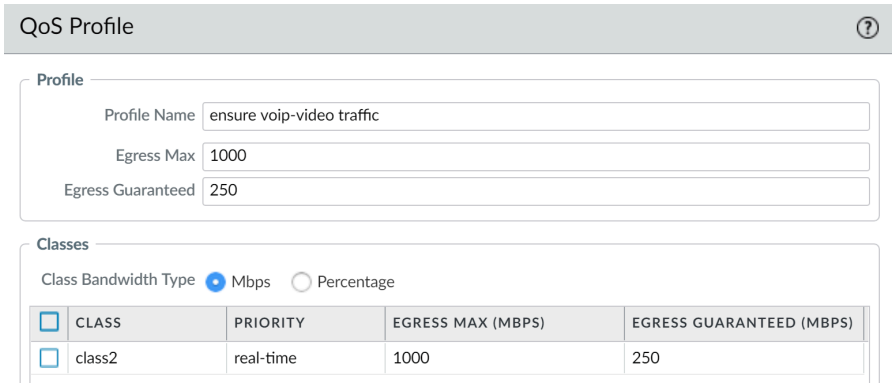
이 예에서 회사 지점의 직원은 화상 회의 및 VoIP(Voice over IP) 기술을 사용하여 다른 지점, 파트너 및 고객과 비즈니스 커뮤니케이션을 수행하는 데 어려움과 불안정성을 경험하고 있습니다. IT 관리자는 이러한 문제를 해결하고 지점 직원을 위한 효과적이고 안정적인 비즈니스 커뮤니케이션을 보장하기 위해 QoS를 구현하려고 합니다. 관리자는 들어오고 나가는 네트워크 트래픽 모두에 QoS를 보장하기를 원하기 때문에 방화벽의 내부 및 외부 인터페이스 모두에서 QoS를 활성화합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 관리자는 클래스 2 트래픽이 실시간 우선 순위를 수신하고 최대 대역폭이 1000Mbps인 인터페이스에서 네트워크 사용 피크 기간을 포함하여 항상 250Mbps의 대역폭을 보장하도록 클래스 2를 정의하는 QoS 프로파일을 생성합니다.

실시간 우선 순위는 일반적으로 대기 시간의 영향을 받는 애플리케이션에 권장되며 특히 음성 및 비디오 애플리케이션의 성능과 품질을 보장하는 데 유용합니다.

방화벽 웹 인터페이스에서 관리자는 네트워크 > 네트워크 프로파일 > **Qos** 프로파일 페이지를 선택한 다음 추가를 클릭하고 프로파일 이름을 입력하여 VoIP 트래픽을 보장하고 클래스 2 트래픽을 정의합니다.

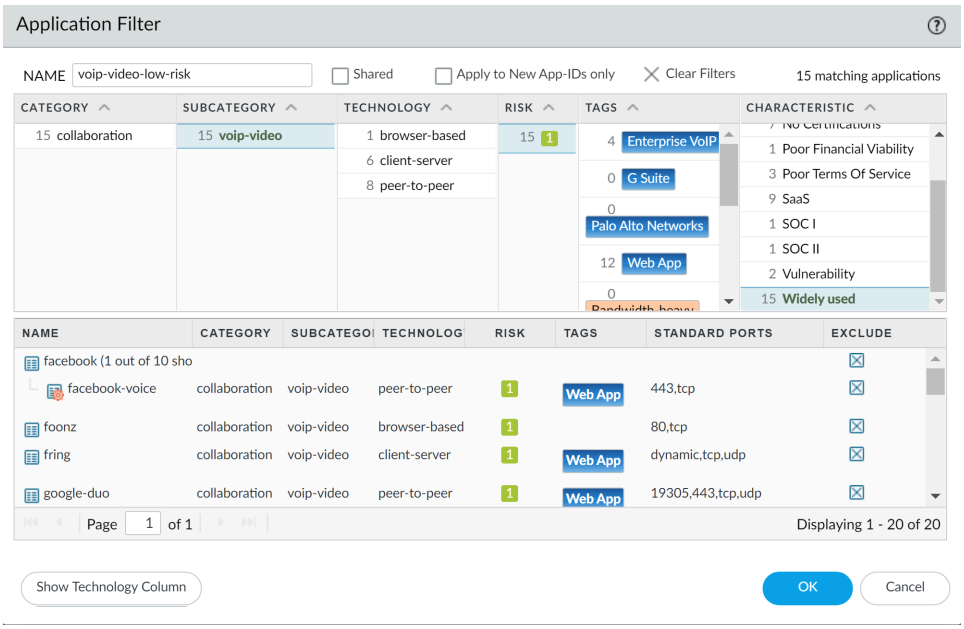



**STEP 2 |** 관리자는 음성 및 비디오 트래픽을 식별하는 QoS 정책을 만듭니다. 회사에는 하나의 표준 음성 및 비디오 애플리케이션이 없기 때문에 관리자는 직원이 다른 사무실, 파트너 및 고객과 통신하는 데 광범위하고 정기적으로 사용하는 몇 가지 애플리케이션에 QoS를 적용하려고 합니다. **Policies** > **QoS** > **QoS** 정책 규칙 > 애플리케이션 탭에서 관리자는 추가를 클릭하고 애플리케이션 필터 창을 엽니다. 관리자는 계속해서 QoS를 적용할 애플리케이션을 필터링할 기준을 선택한 다음 하위 카테고리

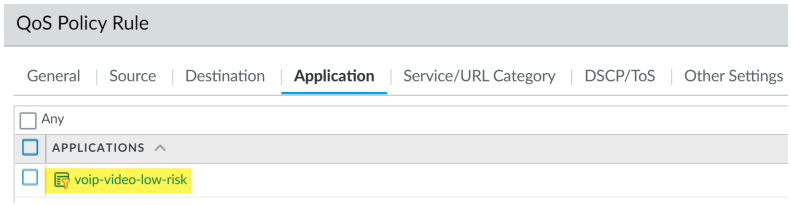

©2023 Palo Alto Networks, Inc.

voip-video를 선택한 다음 위험이 낮고 널리 사용되는 voip-video 애플리케이션만 지정하여 범위를 좁힙니다.

애플리케이션 필터는 QoS 정책에서 애플리케이션을 필터링하는 데 사용되는 동적 도구로, VoIP-비디오, 낮은 위험 및 주어진 시간에 널리 사용되는 기준을 충족하는 모든 애플리케이션에 QoS를 적용할 수 있습니다.




관리자는 애플리케이션 필터의 이름을 voip-video-low-risk로 지정하고 QoS 정책에 포함합니다.



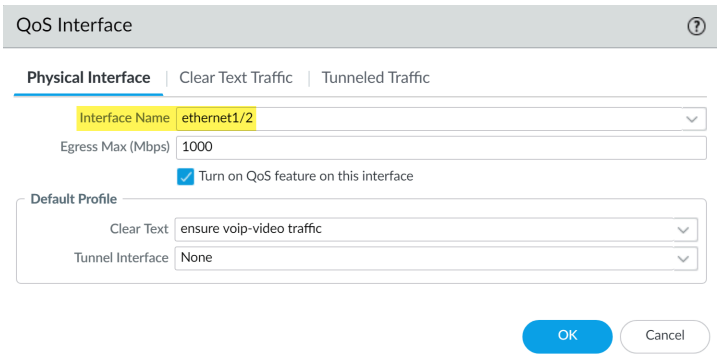

관리자는 QoS 정책의 이름을 음성-비디오로 지정하고 기타 설정을 선택하여 정책 클래스 2와 일치하는 모든 트래픽을 할당합니다. 그는 들어오는 QoS 트래픽과 나가는 QoS 트래픽 모두에 대해 음성-비디오 QoS 정책을 사용할 것이므로 소스 및 대상 정보를 모두로 설정합니다.

| | | | Source | | | | Destination | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | DSCP/TOS | CLASS |
| 1 | HTTPS | none | trust | any | any | any | untrust | any | any | web-browsing | any | any | 2 |
| 2 | Voice-Video | none | any | any | any | any | any | any | any | voip-video-l... | any | any | 1 |

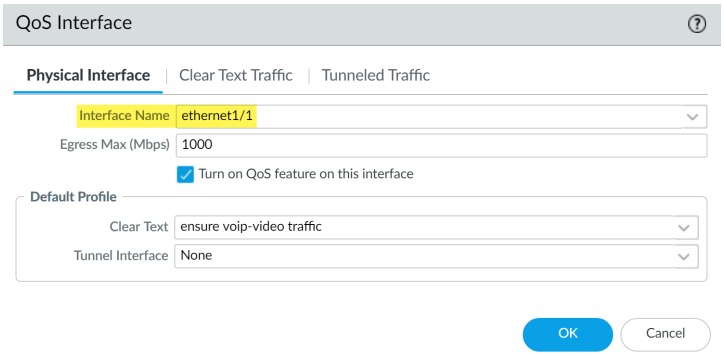

©2023 Palo Alto Networks, Inc.

**STEP 3 |** 관리자는 수신 및 발신 음성 및 화상 통신 모두에 대해 QoS를 보장하기를 원하기 때문에 네트워크의 외부 인터페이스(발신 통신에 QoS 적용) 및 내부 인터페이스(수신 통신에 QoS 적용)에서 QoS를 활성화합니다.

관리자는 먼저 생성한 QoS 프로파일을 활성화하고 외부 인터페이스(이 경우 이더넷 1/2)에서 음성-비디오 트래픽(이 프로파일의 클래스 2는 정책, 음성-비디오와 연결됨)을 확인합니다.




그런 다음 동일한 QoS 프로파일을 활성화하여 두 번째 인터페이스인 내부 인터페이스(이 경우 이더넷 1/1)에서 VoIP-비디오 트래픽을 보장합니다.




**STEP 4 |** 관리자는 네트워크 > **QoS**를 선택하여 수신 및 발신 음성 및 비디오 트래픽 모두에 대해 QoS가 활성화되어 있는지 확인합니다.

| NAME | GUARANTEED EGRESS (MBPS) | MAXIMUM EGRESS (MBPS) | PROFILE | ENABLED | |
|---|---|---|---|---|---|
| ethernet1/1 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 250.000 | | ensure voip-video traffic | | |
| ethernet1/2 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 250.000 | | ensure voip-video traffic | | |

관리자가 네트워크의 내부 및 외부 인터페이스 모두에서 QoS를 성공적으로 활성화했습니다. 이제 음성 및 비디오 애플리케이션 트래픽이 네트워크 안팎으로 흐를 때 실시간 우선 순위가 보장되어 특히 대기 시간과 지터에 민감한 이러한 통신을 안정적이고 효과적으로 사용하여 내부 및 외부 비즈니스 커뮤니케이션 모두를 수행할 수 있습니다.


©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

# VPN

VPN(가상 사설망)은 사용자/시스템이 LAN(Local Area Network)을 통해 연결하는 것처럼 공용 네트워크를 통해 안전하게 연결할 수 있도록 하는 터널을 생성합니다. VPN 터널을 설정하려면 서로를 인증하고 이들 간의 정보 흐름을 암호화할 수 있는 한 쌍의 디바이스가 필요합니다. 디바이스는 한 쌍의 Palo Alto Networks 방화벽이거나 다른 공급자의 VPN 지원 디바이스와 함께 Palo Alto Networks 방화벽일 수 있습니다.


- VPN 배포
- 사이트 간 VPN 개요
- 사이트 간 VPN 개념
- 사이트 간 VPN 설정
- 사이트 간 VPN 빠른 구성

# VPN 배포

Palo Alto Networks 방화벽은 다음과 같은 VPN 배포를 지원합니다.

- 사이트 간 **VPN** - 중앙 사이트와 원격 사이트를 연결하는 간단한 VPN 또는 중앙 사이트를 여러 원격 사이트와 연결하는 허브 및 스포크 VPN입니다. 방화벽은 IPsec(IP 보안) 프로토콜 집합을 사용하여 두 사이트 간 트래픽에 대한 보안 터널을 설정합니다. 사이트 간 VPN 개요를 참조하십시오.
- 원격 사용자 간 **VPN** - GlobalProtect 에이전트를 사용하여 원격 사용자가 방화벽을 통해 보안 연결을 설정할 수 있도록 하는 솔루션입니다. 이 솔루션은 SSL 및 IPsec을 사용하여 사용자와 사이트 간에 보안 연결을 설정합니다. GlobalProtect 관리자 안내서를 참조하십시오.
- 대규모 **VPN** - Palo Alto Networks GlobalProtect 대규모 VPN(LSVPN)은 최대 1,024개의 새틀라이트 사무실과 함께 확장 가능한 허브 및 스포크 VPN을 구축할 수 있는 간소화된 메커니즘을 제공합니다. 이 솔루션을 사용하려면 허브와 모든 스포크에 Palo Alto Networks 방화벽을 배치해야 합니다. 디바이스 인증에 인증서를 사용하고, 모든 구성 요소 간의 통신 보안을 위해 SSL을 사용하고, 데이터를 보호하기 위해 IPsec을 사용합니다. 대규모 VPN(LSVPN)을 참조하십시오.

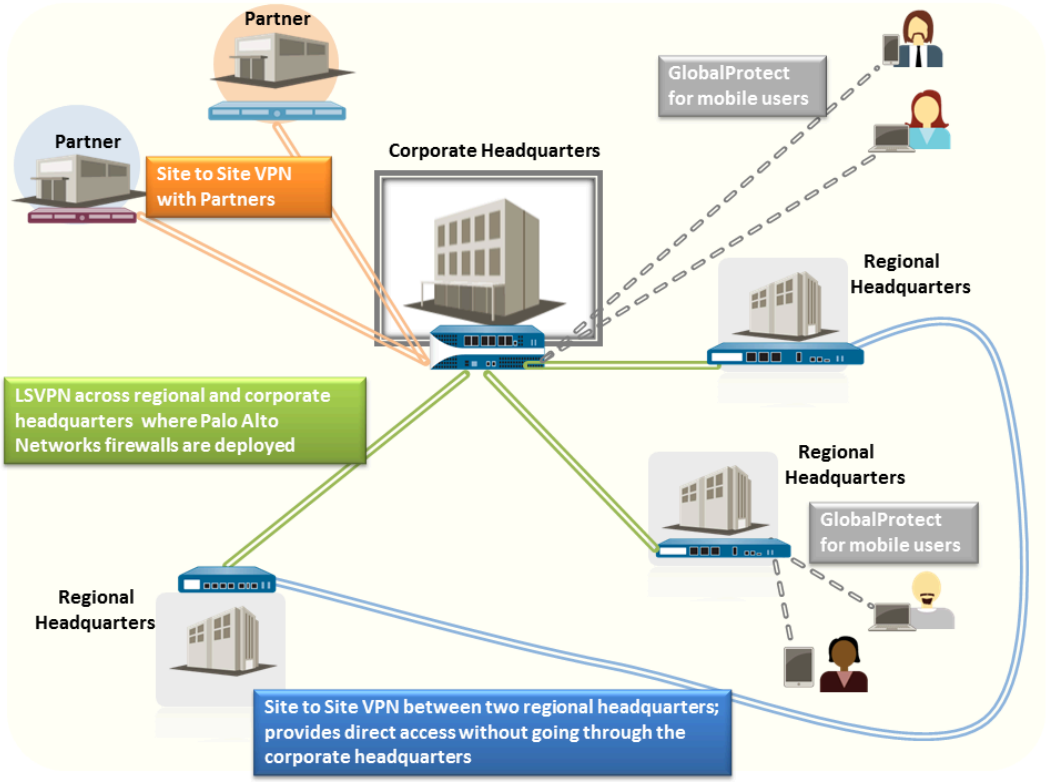



그림 **7: VPN** 배포


©2023 Palo Alto Networks, Inc.

# 사이트 간 VPN 개요

두 개의 LAN(근거리 통신망)을 연결할 수 있는 VPN 연결을 사이트 간 VPN이라고 합니다. 두 사이트에 있는 Palo Alto Networks 방화벽을 연결하거나 Palo Alto Networks 방화벽을 다른 위치에 있는 타사 보안 디바이스와 연결하도록 라우팅 기반 VPN을 구성할 수 있습니다. 방화벽은 타사 정책 기반 VPN 디바이스와도 상호 운용할 수 있습니다. Palo Alto Networks 방화벽은 경로 기반 VPN을 지원합니다.

Palo Alto Networks 방화벽은 경로 기반 VPN을 설정합니다. 이 VPN에서는 방화벽이 대상 IP 주소를 기반으로 라우팅을 결정합니다. 트래픽이 VPN 터널을 통해 특정 대상으로 라우팅되면 VPN 트래픽으로 처리됩니다.

IP 보안(IPsec) 프로토콜 집합은 VPN 트래픽에 대한 보안 터널을 설정하는 데 사용되며 TCP/IP 패킷의 정보는 보안됩니다(터널 유형이 ESP인 경우 암호화). IP 패킷(헤더 및 페이로드) 이 다른 IP 페이로드에 내장되고 새 헤더가 적용된 다음 IPsec 터널을 통해 전송됩니다. 새 헤더의 소스 IP 주소는 로컬 VPN 피어의 소스 IP 주소이고 대상 IP 주소는 터널의 맨 끝에 있는 VPN 피어의 IP 주소입니다. 패킷이 원격 VPN 피어(터널의 맨 끝에 있는 방화벽)에 도달하면 외부 헤더가 제거되고 원래 패킷이 대상으로 전송됩니다.

VPN 터널을 설정하려면 먼저 피어에 대한 인증을 받아야 합니다. 인증에 성공하면 피어는 암호화 메커니즘과 알고리즘을 협상하여 통신을 보호합니다. IKE(인터넷 키 교환) 프로세스는 VPN 피어를 인증하는 데 사용되며 VPN 통신을 보호하기 위해 터널의 각 끝에 IPsec 보안 연결(SA)이 정의되어 있습니다. IKE는 디지털 인증서 또는 사전 공유한 키와 디피 헬먼 키를 사용하여 IPsec 터널용 SA를 설정합니다. SA는 보안 매개 변수 인덱스(SPI), 보안 프로토콜, 암호화 키 및 대상 IP 주소(암호화, 데이터 인증, 데이터 무결성 및 엔드포인트 인증)를 포함하여 보안 전송에 필요한 모든 매개 변수를 지정합니다.

다음 그림은 두 사이트 간의 VPN 터널을 보여줍니다. VPN 피어 A에 의해 보호되는 클라이언트에 다른 사이트에 있는 서버의 콘텐츠가 필요한 경우 VPN 피어 A는 VPN 피어 B에 대한 연결 요청을 시작합니다. 보안 정책에서 연결을 허용하는 경우 VPN 피어 A는 IKE 암호화 프로파일 매개 변수(IKE 단계 1)를 사용하여 보안 연결을 설정하고VPN 피어 B를 인증합니다. 그런 다음 VPN 피어 A는 IKE 2단계 매개 변수를 정의하는 IPsec 암호화 프로파일을 사용하여 VPN 터널을 설정하여 두 사이트 간에 데이터를 안전하게 전송할 수 있도록 합니다.

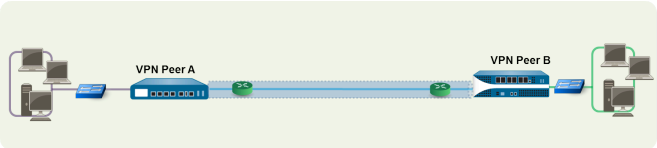



그림 **8:** 사이트 간 **VPN**

 ©2023 Palo Alto Networks, Inc.

# 사이트 간 VPN 개념

VPN 연결은 둘 이상의 사이트 간의 정보에 대한 보안 액세스를 제공합니다. 리소스에 대한 보안 액세스와 안정적인 연결을 제공하기 위해 VPN 연결에는 다음 구성 요소가 필요합니다.

- IKE 게이트웨이
- 터널 인터페이스
- 터널 모니터링
- VPN용 인터넷 키 교환 (IKE)
- IKEv2

## IKE 게이트웨이

두 네트워크에서 VPN 연결을 시작하고 종료하는 Palo Alto Networks 방화벽 또는 방화벽과 다른 보안 디바이스를 IKE 게이트웨이라고 합니다. VPN 터널을 설정하고 IKE 게이트웨이 간에 트래픽을 보내려면 각 피어에 IP 주소(고정 또는 동적) 또는 FQDN이 있어야 합니다. VPN 피어는 미리 공유한 키 또는 인증서를 사용하여 서로를 인증합니다.

피어는 또한 IKE 단계 1에서 VPN 터널 및 SA 수명을 설정하기 위한 모드(기본 또는 어그레시브)를 협상해야 합니다. 기본 모드는 피어의 ID를 보호하고 터널을 설정할 때 더 많은 패킷이 교환되기 때문에 더 안전합니다. 기본 모드는 두 피어가 모두 지원하는 경우 IKE 협상에 권장되는 모드입니다. 공격적 모드는 VPN 터널을 설정하는 데 더 적은 패킷을 사용하므로 VPN 터널을 설정하는 데 더 빠르지만 덜 안전한 옵션입니다.

구성에 대한 자세한 내용은 IKE 게이트웨이 설정을(를) 참조하십시오.

## 터널 인터페이스

VPN 터널을 설정하려면 각 끝에 있는 레이어 3 인터페이스에 방화벽이 VPN 터널에 연결하고 설정하기 위한 로지컬 터널 인터페이스가 있어야 합니다. 터널 인터페이스는 두 엔드포인트 간의 트래픽을 포워딩하는 데 사용되는 로지컬(가상) 인터페이스입니다. 프록시 ID를 구성하면 프록시 ID가 모든 IPSec 터널 용량에 포함됩니다.

터널 인터페이스는 정책을 적용하려면 보안 영역에 속해야 하며 기존 라우팅 인프라를 사용하려면 가상 라우터에 할당해야 합니다. 방화벽이 경로 조회를 수행하고 사용할 적절한 터널을 결정할 수 있도록 터널 인터페이스와 물리적 인터페이스가 동일한 가상 라우터에 할당되었는지 확인합니다.

일반적으로 터널 인터페이스가 연결된 레이어 3 인터페이스는 외부 영역(예: 비신뢰 영역)에 속합니다. 터널 인터페이스는 물리적 인터페이스와 동일한 보안 영역에 있을 수 있지만 보안이 향상되고 가시성이 향상되면 터널 인터페이스에 대한 별도의 영역을 만들 수 있습니다. VPN 영역을 말하는 터널 인터페이스에 대해 별도의 영역을 만들면 트래픽이 VPN 영역과 트러스트 영역 사이로 플로우되도록 보안 정책을 만들어야 합니다.

사이트 간의 트래픽을 라우팅하려면 터널 인터페이스에 IP 주소가 필요하지 않습니다. IP 주소는 터널 모니터링을 활성화하려는 경우 또는 터널을 통해 트래픽을 라우팅하기 위해 동적 라우팅 프로토콜을 사용하는 경우에만 필요합니다. 동적 라우팅에서 터널 IP 주소는 VPN 터널로 트래픽을 라우팅하기 위한 다음 홉 IP 주소 역할을 합니다.

 ©2023 Palo Alto Networks, Inc.

정책 기반 VPN을 수행하는 VPN 피어로 Palo Alto Networks 방화벽을 구성하는 경우 IPSec 터널을 설정할 때 로컬 및 원격 프록시 ID를 구성해야 합니다. 각 피어는 성공적인 IKE 2단계 협상을 허용하기 위해 구성된 프록시 ID를 패킷에서 실제로 수신된 것과 비교합니다. 여러 터널이 필요한 경우 각 터널 인터페이스에 대해 고유한 프록시 ID를 구성합니다. 터널 인터페이스에는 최대 250개의 프록시 ID가 있을 수 있습니다. 각 프록시 ID는 방화벽의 IPSec VPN 터널 용량에 계산되며 터널 용량은 방화벽 모델에 따라 다릅니다.

구성에 대한 자세한 내용은 IPsec 터널 설정을(를) 참조하십시오.

# 터널 모니터링

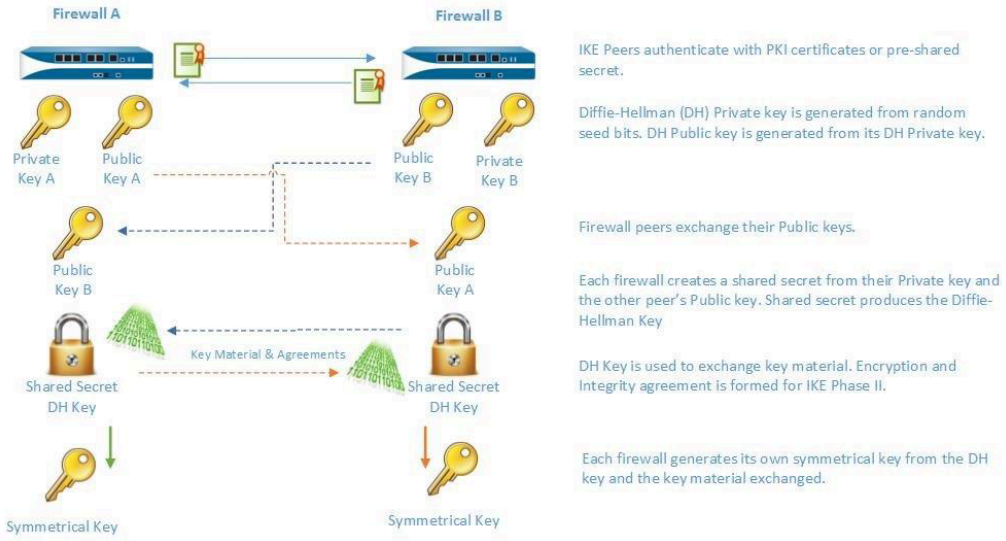
VPN 터널의 경우 터널을 통해 대상 IP 주소에 대한 연결을 확인할 수 있습니다. 방화벽의 네트워크 모니터링 프로파일을 사용하면 지정된 폴링 인터벌로 대상 IP 주소 또는 다음 홉에 대한 연결(ICMP 사용)을 확인하고 모니터링되는 IP 주소에 대한 액세스 실패 시 조치를 지정할 수 있습니다.

대상 IP에 연결할 수 없는 경우 터널이 복구될 때까지 기다리도록 방화벽을 구성하거나 다른 터널에 대한 자동 페일오버를 구성합니다. 두 경우 모두 방화벽은 터널 장애를 경고하는 시스템 로그를 생성하고 IPsec 키를 재협상하여 복구 속도를 높입니다.

구성에 대한 자세한 내용은 터널 모니터링 설정을(를) 참조하십시오.

# VPN용 인터넷 키 교환 (IKE)

IKE 프로세스를 사용하면 터널 양쪽 끝에 있는 VPN 피어가 상호 동의한 키 또는 인증서 및 암호화 방법을 사용하여 패킷을 암호화하고 복호화할 수 있습니다. IKE 프로세스는 다음 두 단계로 진행됩니다. IKE 1단계 및 IKE 2단계. 이러한 각 단계에서는 암호화 프로파일(IKE 암호화 프로파일 및 IPSec 암호화 프로파일)을 사용하여 정의된 키와 암호화 알고리즘을 사용하며 IKE 협상의 결과는 SA(보안 연결)입니다. SA는 VPN 터널을 통한 데이터 흐름을 허용하기 위해 두 VPN 피어에서 사용하는 상호 합의된 키 및 알고리즘 세트입니다. 다음 그림은 VPN 터널 설정을 위한 키 교환 프로세스를 보여줍니다.




## IKE Phase 1

이 단계에서 방화벽은 IKE 게이트웨이 구성 및 IKE 암호화 프로파일에 정의된 매개변수를 사용하여 서로를 인증하고 보안 제어 채널을 설정합니다. IKE 단계는 VPN 피어의 상호 인증을 위해 사전 공유 키 또는

 ©2023 Palo Alto Networks, Inc.

디지털 인증서(공개 키 인프라, PKI 사용)의 사용을 지원합니다. 사전 공유 키는 PKI 인프라의 지원이 필요하지 않기 때문에 소규모 네트워크를 보호하기 위한 간단한 솔루션입니다. 디지털 인증서는 더 강력한 인증 보안이 필요한 대규모 네트워크 또는 구현에 더 편리할 수 있습니다.

인증서를 사용할 때 인증서를 발급하는 CA가 두 게이트웨이 피어 모두에서 신뢰할 수 있고 인증서 체인의 최대 인증서 길이가 5개 이하인지 확인하십시오. IKE 조각화가 활성화되면 방화벽은 인증서 체인에서 최대 5개의 인증서로 IKE 메시지를 재조립하고 VPN 터널을 성공적으로 설정할 수 있습니다.

IKE 암호화 프로파일은 IKE SA 협상에 사용되는 다음 옵션을 정의합니다.

- IKE에 대한 대칭 키를 생성하기 위한 Diffie-Hellman(DH) 그룹입니다.

  Diffie-Hellman 알고리즘은 한 당사자의 개인 키와 다른 당사자의 공개 키를 사용하여 두 VPN 터널 피어가 공유하는 암호화된 키인 공유 비밀을 생성합니다. 방화벽에서 지원되는 DH 그룹은 다음과 같습니다.

| 그룹 번호 | 비트 수 |
|---|---|
| 그룹 1 | 768비트 |
| 그룹 2 | 1024비트(기본값) |
| 그룹 5 | 1536비트 |
| 그룹 14 | 2048비트 |
| 그룹 15 | 3072비트 모듈식 지수 그룹 |
| 그룹 16 | 4096비트 모듈식 지수 그룹 |
| 그룹 19 | 256비트 타원 곡선 그룹 |
| 그룹 20 | 384비트 타원 곡선 그룹 |
| 그룹 21 | 512비트 임의 타원 곡선 그룹 |

- 인증 알고리즘 - sha1, sha 256, sha 384, sha 512 또는 md5
- 암호화 알고리즘 - aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc 또는 aes-256-cbc

## IKE Phase 2

터널이 보안되고 인증된 후 2단계에서 네트워크 간의 데이터 전송을 위해 채널이 추가로 보호됩니다. IKE 2단계에서는 프로세스의 1단계에서 설정된 키와 IKE 2단계에서 SA에 사용되는 IPSec 프로토콜 및 키를 정의하는 IPSec 암호화 프로파일을 사용합니다.

IPSEC는 다음 프로토콜을 사용하여 통신 보안을 활성화합니다.

- ESP(Encapsulating Security Payload) - 전체 IP 패킷을 암호화하고 소스를 인증하며 데이터 무결성을 확인할 수 있습니다. ESP에서는 패킷을 암호화하고 인증해야 하지만 암호화 옵션을 Null로 설정하여 암호화만 또는 인증만 선택할 수 있습니다. 인증 없이 암호화를 사용하는 것은 권장되지 않습니다.


©2023 Palo Alto Networks, Inc.

- 인증 헤더(AH) - 패킷 소스를 인증하고 데이터 무결성을 확인합니다. AH는 데이터 페이로드를 암호화하지 않으며 데이터 개인 정보 보호가 중요한 배포에 적합하지 않습니다. AH는 주요 관심사가 피어의 정당성을 확인하는 것이고 데이터 프라이버시가 필요하지 않을 때 일반적으로 사용됩니다.

표 **5: IPSEC** 인증 및 암호화에 지원되는 알고리즘

| ESP | AH |
|---|---|
| Diffie Hellman(DH) 교환 옵션 지원 | |
| • 그룹 1 - 768비트<br>• 그룹 2 - 1024비트(기본값)<br>• 그룹 5 - 1536비트<br>• 그룹 14 - 2048비트.<br>• 그룹 15 - 3072비트 모듈식 지수 그룹<br>• 그룹 16 - 4096비트 모듈식 지수 그룹<br>• 그룹 19 - 256비트 타원 곡선 그룹<br>• 그룹 20 - 384비트 타원 곡선 그룹<br>• 그룹 21 - 512비트 랜덤 타원 곡선 그룹<br>• no-pfs - 기본적으로 PFS(완벽한 순방향 보안)가 활성화되어 있습니다. 즉, 위에 나열된 그룹 중 하나를 사용하여 IKE 단계 2에서 새 DH 키가 생성됩니다. 이 키는 IKE 단계 1에서 교환된 키와 독립적이며 더 나은 데이터 전송 보안을 제공합니다. no-pfs를 선택하면 1단계에서 생성된 DH 키가 갱신되지 않고 IPSec SA 협상에 단일 키가 사용됩니다. 두 VPN 피어 모두 PFS에 대해 활성화 또는 비활성화되어야 합니다. | |
| 지원되는 암호화 알고리즘 | |
| • 3des | 112비트 보안 강도의 3DES(Triple Data Encryption Standard) |
| • aes-128-cbc | 보안 강도가 128비트인 CBC(암호 블록 체인)를 사용하는 AES(Advanced 암호화 표준) |
| • aes-192-cbc | 보안 강도가 192비트인 CBC를 사용하는 AES |
| • aes-256-cbc | 보안 강도가 256비트인 CBC를 사용하는 AES |
| • aes-128-ccm | 보안 강도가 128비트인 CBC-MAC(CCM)와 함께 카운터를 사용하는 AES |
| • aes-128-gcm | 보안 강도가 128비트인 Galois/Counter Mode(GCM)를 사용하는 AES |
| • aes-256-gcm | 보안 강도가 256비트인 GCM을 사용하는 AES |


©2023 Palo Alto Networks, Inc.

| ESP | AH |
|---|---|
| 지원되는 인증 알고리즘 | |
| • md5 | • md5 |
| • sha 1 | • sha 1 |
| • sha 256 | • sha 256 |
| • sha 384 | • sha 384 |
| • sha512 | • sha 512 |

### IPsec VPN 터널을 보호하는 방법 (IKE 2단계)

IPsec VPN 터널은 수동 키 또는 자동 키를 사용하여 보호할 수 있습니다. 또한 IPsec 구성 옵션에는 키 계약을 위한 Diffie-Hellman 그룹 및/또는 메시지 인증을 위한 암호화 알고리즘 및 해시가 포함됩니다.

- 수동 키 - 수동 키는 일반적으로 Palo Alto Networks 방화벽이 레거시 디바이스를 사용하여 VPN 터널을 설정하거나 세션 키 생성으로 인한 오버헤드를 줄이려는 경우에 사용됩니다. 수동 키를 사용하는 경우 두 피어에 동일한 키를 구성해야 합니다.

  피어 간에 키 정보를 릴레이할 때 세션 키가 손상될 수 있으므로 VPN 터널을 설정할 때는 수동 키를 사용하지 않는 것이 좋습니다. 키가 손상되면 데이터 전송이 더 이상 안전하지 않습니다.
- 자동 키 - 자동 키를 사용하면 IPsec 암호화 프로파일에 정의된 알고리즘을 기반으로 IPsec 터널을 설정하고 유지 관리하기 위한 키를 자동으로 생성할 수 있습니다.

## IKEv2

IPSec VPN 게이트웨이는 IKEv1 또는 IKEv2를 사용하여 IKE SA(보안 연결) 및 IPSec 터널을 협상합니다. IKEv2는 RFC 5996에 정의되어 있습니다.

1단계 SA 및 2단계 SA를 사용하는 IKEv1과 달리 IKEv2는 IKE SA로 설정된 ESP(Encapsulating Security Payload) 또는 AH(인증 헤더)에 하위 SA를 사용합니다.

NAT 통과(NAT-T)는 두 게이트웨이 사이에 있는 디바이스에서 발생하는 NAT가 있는 경우 두 게이트웨이 모두에서 활성화되어야 합니다. 게이트웨이는 NAT 디바이스의 공용(전역적으로 라우팅 가능한) IP 주소만 볼 수 있습니다.

IKEv2는 IKEv1에 비해 다음과 같은 이점을 제공합니다.

- 터널 엔드포인트은 터널을 설정하기 위해 더 적은 수의 메시지를 교환합니다. IKEv2는 4개의 메시지를 사용합니다. IKEv1은 9개의 메시지(메인 모드) 또는 6개의 메시지(어그레시브 모드)를 사용합니다.
- 내장된 NAT-T 기능은 공급업체 간의 호환성을 향상시킵니다.
- 기본 상태 확인 기능은 터널이 다운되면 자동으로 다시 설정합니다. 활성 검사는 IKEv1에서 사용되는 Dead Peer Detection을 대체합니다.


©2023 Palo Alto Networks, Inc.

- 트래픽 선택기를 지원합니다(익스체인지당 1개). 트래픽 선택기는 IKE 협상에서 터널에 액세스할 수 있는 트래픽을 제어하는 데 사용됩니다.
- 단편화를 줄이기 위해 해시 및 URL 인증서 교환을 지원합니다.
- 향상된 피어 검증으로 DoS 공격에 대한 복원력. 절반만 열린 SA가 너무 많으면 쿠키 유효성 검사가 트리거될 수 있습니다.

IKEv2를 구성하기 전에 다음 개념을 숙지해야 합니다.

- 라이브니스 검사
- 쿠키 활성화 임계값 및 엄격한 쿠키 유효성 검사
- 트래픽 선택기
- 해시 및 URL 인증서 교환
- SA 키 수명 및 재인증 간격

IKE 게이트웨이 설정 후에 IKEv2를 선택한 경우 환경에서 요구하는 대로 IKEv2와 관련된 다음 선택적 작업을 수행합니다.

- 해시 및 URL을 사용하여 액세스할 피어에 대한 인증서 내보내기
- IKEv2 게이트웨이 인증을 위한 인증서 가져오기
- IKEv2의 키 수명 또는 인증 간격 변경
- IKEv2에 대한 쿠키 활성화 임계값 변경
- IKEv2 트래픽 선택기 구성

## 라이브니스 검사

IKEv2의 라이브니스 검사는 IKEv1이 피어를 계속 사용할 수 있는지의 여부를 결정하는 방법으로 사용하는 데드 피어 감지(DPD)와 유사합니다.

IKEv2에서 라이브니스 검사는 기본적으로 5초 동안 게이트웨이가 구성 가능한 인터벌로 피어에게 보내는 모든 IKEv2 패킷 전송 또는 빈 정보 메시지에 의해 수행됩니다. 필요한 경우 보낸 사람은 최대 10회까지 재전송을 시도합니다. 응답을 받지 못하면 보낸 사람이 IKE_SA 및 해당 CHILD_SAs 닫고 삭제합니다. 보낸 사람은 다른 IKE_SA_INIT 메시지를 보내 다시 시작합니다.

## 쿠키 활성화 임계값 및 엄격한 쿠키 유효성 검사

쿠키 유효성 검사는 IKEv2에 대해 항상 활성화되며 하프 SA DoS 공격으로부터 보호하는 데 도움이 됩니다. 쿠키 유효성 검사를 트리거하는 반쯤 열린 SA의 전역 임계값 수를 구성할 수 있습니다. 또한 모든 새로운 IKE2 SA에 대해 쿠키 유효성 검사를 시행하도록 개별 IKE 게이트웨이를 구성할 수 있습니다.

- 쿠키 활성화 임계값은 동시에 반쯤 열린 IKE SA(기본값은 500)의 수를 제한하는 글로벌 VPN 세션 설정입니다. 반쯤 열린 IKE SA 수가 쿠키 활성화 임계값을 초과하면 응답자가 쿠키를 요청하고 개시자는

 ©2023 Palo Alto Networks, Inc.

연결을 검증하기 위해 쿠키가 포함된 IKE_SA_INIT로 응답해야 합니다. 쿠키 유효성 검사가 성공하면 다른 SA를 시작할 수 있습니다. 값이 0이면 쿠키 유효성 검사가 항상 켜져 있음을 의미합니다.

응답자는 개시자가 쿠키를 반환할 때까지 초기자의 상태를 유지하거나 Diffie-Hellman 키 교환을 수행하지도 않습니다. IKEv2 쿠키 유효성 검사는 수많은 연결을 절반 열어 두려고 하는 DoS 공격을 완화합니다.

쿠키 활성화 임계값은 최대 절반 개방 **SA** 설정보다 낮아야 합니다. 매우 높은 숫자(예: 65534)로 IKEv2에 대한 쿠키 활성화 임계값 변경을(를) 하고 최대 절반 열린 **SA** 설정이 기본값인 65535로 유지되면 쿠키 유효성 검사가 기본적으로 비활성화됩니다.

- 전역 임계값에 관계없이 게이트웨이가 수신하는 모든 새 IKEv2 SA에 대해 쿠키 유효성 검사를 수행하려는 경우 엄격한 쿠키 유효성 검사를 활성화할 수 있습니다. 엄격한 쿠키 유효성 검사는 구성 중인 IKE 게이트웨이에만 영향을 미치며 기본적으로 비활성화되어 있습니다. 엄격한 쿠키 유효성 검사를 비활성화하면 시스템은 쿠키 활성화 임계값을 사용하여 쿠키가 필요한지의 여부를 결정합니다.

## 트래픽 선택기

IKEv1에서 경로 기반 VPN이 있는 방화벽은 IPSec 터널을 설정하려면 로컬 및 원격 프록시 ID를 사용해야 합니다. 각 피어는 IKE 2단계를 성공적으로 협상하기 위해 프록시 ID를 패킷에서 받은 것과 비교합니다. IKE 2단계는 IPSec 터널을 설정하기 위해 SA를 협상하는 것입니다. (프록시 ID에 대한 자세한 내용은 터널 인터페이스을(를) 참조하십시오.)

IKEv2에서는 IKE 협상 중에 사용되는 네트워크 트래픽의 구성 요소인 IKEv2 트래픽 선택기 구성을(를) 할 수 있습니다. 트래픽 셀렉터는 터널을 설정하고 터널을 통해 허용되는 트래픽을 결정하는 CHILD_SA(터널 생성) 2단계에서 사용됩니다. 두 IKE 게이트웨이 피어는 트래픽 셀렉터와 협상하고 상호 동의해야 합니다. 그렇지 않으면 한쪽은 합의에 도달하기 위해 주소 범위를 좁히지 않습니다. 하나의 IKE 연결에는 여러 터널이 있을 수 있습니다. 예를 들어 각 부서에 다른 터널을 할당하여 트래픽을 격리할 수 있습니다. 트래픽 분리를 통해 QoS와 같은 기능을 구현할 수 있습니다.

IPv4 및 IPv6 트래픽 셀렉터는 다음과 같습니다.

- 소스 **IP** 주소 - 네트워크 프리픽스, 주소 범위, 특정 호스트 또는 와일드카드입니다.
- 대상 **IP** 주소 - 네트워크 프리픽스, 주소 범위, 특정 호스트 또는 와일드카드입니다.
- 프로토콜 - TCP 또는 UDP와 같은 전송 프로토콜입니다.
- 소스 포트 - 패킷이 시작된 포트입니다.
- 대상 포트 - 패킷이 향하는 포트입니다.

IKE 협상 중에 서로 다른 네트워크 및 프로토콜에 대해 여러 트래픽 선택자가 있을 수 있습니다. 예를 들어, 이니시에이터(Initiator)는 터널을 통해 172.168.0.0/16에서 198.5.0.0/16으로 향하는 피어로 TCP 패킷을 보내려고 할 수 있습니다. 또한 동일한 터널을 통해 172.17.0.0/16에서 0.0.0.0(모든 네트워크)으로 향하는 동일한 게이트웨이로 UDP 패킷을 보내려고 합니다. 피어 게이트웨이는 예상할 것을 알 수 있도록 이러한 트래픽 선택기와 동의해야 합니다.

한 게이트웨이가 다른 게이트웨이의 IP 주소보다 더 구체적인 IP 주소인 트래픽 선택기에서 협상을 시작할 수 있습니다.

- 예를 들어 게이트웨이 A는 172.16.0.0/16의 소스 IP 주소와 192.16.0.0/16의 대상 IP 주소를 제공합니다. 그러나 게이트웨이 B는 소스 IP 주소로 0.0.0.0(모든 소스), 대상 IP 주소로 0.0.0.0(모든 대상)으로 구성됩니다. 따라서 게이트웨이 B는 소스 IP 주소를 192.16.0.0/16으로, 대상 주소를

 ©2023 Palo Alto Networks, Inc.

172.16.0.0/16으로 좁힙니다. 따라서 좁혀지는 게이트웨이 A의 주소를 수용하고 두 게이트웨이의 트래픽 선택기가 일치합니다.

- 게이트웨이 B(소스 IP 주소 0.0.0.0으로 구성)가 응답자 대신 이니시에이터(Initiator)인 경우 게이트웨이 A는 보다 구체적인 IP 주소로 응답하고 게이트웨이 B는 주소 범위를 좁혀 합의에 도달합니다.

## 해시 및 URL 인증서 교환

IKEv2는 SA의 IKEv2 협상 중에 사용되는 해시 및 URL 인증서 교환을 지원합니다. URL로 지정된 HTTP 서버에 인증서를 저장합니다. 피어는 서버에 대한 URL 수신을 기반으로 서버에서 인증서를 가져옵니다. 해시는 인증서의 내용이 유효한지의 여부를 확인하는 데 사용됩니다. 따라서 두 피어는 서로가 아니라 HTTP CA와 인증서를 교환합니다.

해시와 URL의 해시 부분은 메시지 크기를 줄여주므로 해시와 URL은 IKE 협상 중 패킷 분할 가능성을 줄이는 방법입니다. 피어는 예상한 인증서와 해시를 수신하므로 IKE 1단계에서 피어의 유효성을 검사했습니다. 분할 발생을 줄이면 DoS 공격으로부터 보호하는 데 도움이 됩니다.

**HTTP** 인증서 교환을 선택한 다음 인증서 **URL**을 입력하여 IKE 게이트웨이를 구성할 때 해시 및 URL 인증서 교환을 활성화할 수 있습니다. 교환이 성공하려면 피어도 해시 및 URL 인증서 교환을 사용해야 합니다. 피어가 해시 및 URL을 사용할 수 없는 경우 X.509 인증서는 IKEv1에서 교환되는 방식과 유사하게 교환됩니다.

해시 및 URL 인증서 교환을 활성화한 경우 인증서가 아직 없는 경우 인증서를 인증서 서버로 내보내야 합니다. 인증서를 내보낼 때 파일 형식은 **DER(Binary Encoded Certificate)**이어야 합니다. 해시 및 URL을 사용하여 액세스할 피어에 대한 인증서 내보내기을(를) 참조하십시오.

## SA 키 수명 및 재인증 간격

IKEv2에서 두 개의 IKE 암호화 프로파일 값인 **Key Lifetime** 및 **IKEv2 Authentication Multiple**은 IKEv2 IKE SA의 설정을 제어합니다. 키 수명은 협상된 IKE SA 키가 유효한 시간입니다. 키 수명이 만료되기 전에 SA를 다시 입력해야 합니다. 그렇지 않으면 만료 시 SA가 새로운 IKEv2 IKE SA 키 재입력을 시작해야 합니다. 기본값은 8시간입니다.

재인증 인터벌은 키 수명에 **IKEv2** 인증 배수를 곱하여 구합니다. 인증 배수의 기본값은 0이며 재인증 기능을 비활성화합니다.

인증 배수의 범위는 0-50입니다. 따라서 예를 들어 인증 배수를 20으로 구성하는 경우 시스템은 160시간 주기로 20번의 키 재입력(re-key)을 할 때마다 재인증을 수행합니다. 이는 게이트웨이가 IKE SA를 처음부터 다시 생성하기 위해 IKE로 다시 인증해야 하기 전에 게이트웨이가 160시간 동안 하위 SA 생성을 수행할 수 있음을 의미합니다.

IKEv2에서 초기자 및 응답자 게이트웨이는 고유한 키 수명 값을 가지며 키 수명이 더 짧은 게이트웨이는 SA에 키 재입력(re-keyed)을 요청하는 게이트웨이입니다.

 ©2023 Palo Alto Networks, Inc.

# 사이트 간 VPN 설정

사이트 간 VPN을 설정하려면 다음을 수행하십시오.

- 이더넷 인터페이스, 가상 라우터 및 영역이 제대로 구성된지 확인합니다. 자세한 내용은 인터페이스 및 영역 구성을 참조하십시오.
- 터널 인터페이스를 생성합니다. 터널 인터페이스를 별도의 영역에 배치하여 터널 트래픽이 서로 다른 정책을 사용할 수 있도록 하는 것이 좋습니다.
- 정적 경로를 설정하거나 라우팅 프로토콜을 할당하여 트래픽을 VPN 터널로 리디렉션합니다. 동적 라우팅(OSPF, BGP, RIP이 지원됨)을 지원하려면 터널 인터페이스에 IP 주소를 할당해야 합니다.
- VPN 터널의 각 끝에 걸쳐 피어 간의 통신을 구축하기 위한 IKE 게이트웨이를 정의합니다. 또한 IKEv1 1단계에서 VPN 터널을 설정하는 데 사용할 식별, 인증 및 암호화를 위한 프로토콜 및 알고리즘을 지정하는 암호화 프로파일을 정의합니다. IKE 게이트웨이 설정 및 IKE 암호화 프로파일 정의 참조.
- VPN 터널 전체에서 데이터 전송을 위해 IPSec 연결을 설정하는 데 필요한 매개 변수를 구성합니다. IPSec 터널 설정을 참조하십시오. IKEv1 2단계의 경우 IPSec 암호화 프로파일 정의를 참조하십시오.
- (선택사항) 방화벽이 IPSec 터널을 모니터링하는 방법을 지정합니다. 터널 모니터링 설정을 참조하십시오.
- 트래픽을 필터링하고 검사하는 보안 정책을 정의합니다.

  보안 규칙의 끝에 거부 규칙이 있는 경우 달리 허용하지 않는 한 영역 내 트래픽이 차단됩니다. ***IKE*** 및 ***IPSec*** 애플리케이션을 허용하는 규칙은 거부 규칙 위에 명시적으로 포함되어야 합니다.

  ***VPN*** 트래픽이 ***PA-7000*** 시리즈 또는 ***PA-5200*** 시리즈 방화벽을 통과하거나 종료하지 않는 경우 양방향 보안 정책 규칙을 구성하여 ***ESP*** 또는 ***AH*** 트래픽을 양방향으로 허용합니다.

이러한 작업이 완료되면 터널을 사용할 준비가 되었습니다. 정책에 정의된 영역/주소로 향하는 트래픽은 라우팅 테이블의 대상 경로에 따라 자동으로 올바르게 라우팅되고 VPN 트래픽으로 처리됩니다. 사이트 간 VPN의 몇 가지 예는 사이트 간 VPN 빠른 구성(Quick Configs)을 참조하십시오.

문제 해결을 위해 IKE 게이트웨이 또는 IPSec 터널을 활성화/비활성화, 새로 고침 또는 다시 시작할 수 있습니다.

## IKE 게이트웨이 설정

VPN 터널을 설정하려면 VPN 피어 또는 게이트웨이는 사전 공유 키 또는 디지털 인증서를 사용하여 서로를 인증하고 각 측의 호스트 간의 트래픽을 보호하는 데 사용되는 IPSec 보안 협회(SA)를 협상하는 보안 채널을 설정해야 합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** IKE 게이트웨이를 정의합니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 게이트웨이를 선택하고 게이트웨이를 추가하고 게이트웨이 이름(일반 탭)을 입력합니다.
2. 버전을 **IKEv1** 전용 모드, **IKEv2** 전용 모드 또는 **IKEv2** 기본 모드로 설정합니다. IKE 게이트웨이는 여기에서 지정한 모드에서 피어와의 협상을 시작합니다. **IKEv2** 기본 모드를 선택하면 원격 피어가 지원하는 경우 두 피어가 IKEv2를 사용합니다. 그렇지 않으면 IKEv1을 사용합니다.

   선택한 버전은 고급 옵션 탭에서 구성할 수 있는 옵션도 결정합니다.

**STEP 2 |** 터널(게이트웨이)의 로컬 엔드포인트을 설정합니다.

1. 주소 유형을 선택합니다. **IPv4** 또는 **IPv6**입니다.
2. 로컬 게이트웨이가 있는 방화벽에서 물리적인 나가는 인터페이스를 선택합니다.
3. 로컬 **IP** 주소 목록에서 VPN 연결이 끝점으로 사용할 IP 주소를 선택합니다. 이것은 방화벽에서 공개적으로 라우팅 가능한 IP 주소가 있는 외부 인터페이스입니다.

**STEP 3 |** 터널(게이트웨이)의 맨 끝에 피어를 설정합니다.

피어 **IP** 주소**,** 유형의 경우 다음 중 하나를 선택한 다음 피어에 대한 해당 정보를 입력합니다.

- **IP** - IPv4 또는 IPv6 주소인 피어 주소를 입력하거나 IPv4 또는 IPv6 주소인 주소 개체를 입력합니다.
- **FQDN** - FQDN 문자열 또는 FQDN 문자열을 사용하는 주소 개체인 피어 주소를 입력합니다. FQDN 또는 FQDN 주소 개체가 둘 이상의 IP 주소로 확인되는 경우 방화벽은 다음과 같이 IKE 게이트웨이의 주소 유형(IPv4 또는 IPv6)과 일치하는 주소 집합에서 기본 주소를 선택합니다.
  - IKE SA(보안 연결)가 협상되지 않은 경우 기본 주소는 값이 가장 작은 IP 주소입니다.
  - IKE 게이트웨이에서 반환된 주소 집합에 있는 주소를 사용하는 경우 방화벽은 해당 주소(집합에서 가장 작은 주소인지의 여부)를 선택합니다.
  - IKE 게이트웨이에서 반환된 주소 집합에 없는 주소를 사용하는 경우 방화벽은 새 주소를 선택한 다음 집합에서 가장 작은 주소입니다.
- 동적 - 피어가 협상을 시작하도록 피어 IP 주소 또는 FQDN 값을 알 수 없는 경우 동적을 선택합니다.



*FQDN* 또는 *FQDN* 주소 개체를 사용하면 피어가 동적 *IP* 주소 변경의 대상이 되는 환경에서 문제가 줄어듭니다*(*그렇지 않으면 이 *IKE* 게이트웨이 피어 주소를 재구성해야 함*).*

**STEP 4 |** 피어 인증 방법을 지정합니다.

인증 방법을 선택합니다. 사전 공유된 키 또는 인증서**.** 사전 공유된 키를 선택하면 다음 단계로 진행합니다. 인증서를 선택하면 6단계로 건너뛰고 인증서 기반 인증 구성을 합니다.


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 사전 공유된 키를 구성합니다.

1. 터널 전체에서 인증의 보안 키인 사전 공유 키를 입력합니다. 사전 공유된 키 확인을 위해 값을 다시 입력합니다. 최대 255개의 ASCII 또는 ASCII가 아닌 문자를 사용합니다.

   사전 공격으로 복호화하기 어려운 키를 생성하고, 필요한 경우 미리 공유한 키 생성기를 사용합니다.

2. 로컬 식별의 경우 다음 형식 중에서 선택한 후 다음 유형을 결정하는 값을 입력합니다. **FQDN(**호스트**,** 이름**)**,**IP** 주소,, **KEYID(HEX**에서 이진 포맷 **ID** 문자열**)** 및 사용자 **FQDN(**이메일 주소**)**. 로컬 식별은 로컬 게이트웨이의 형식과 식별을 정의합니다. 값을 지정하지 않으면 로컬 IP 주소가 로컬 식별 값으로 사용됩니다.
3. 피어 식별의 경우 다음 형식 중에서 선택한 후 다음 유형을 입력합니다. **FQDN(**호스트**,** 이름**)**,**IP** 주소,, **KEYID(HEX**에서 이진 포맷 **ID** 문자열**)** 및 사용자 **FQDN(**이메일 주소**)**. 피어 식별은 피어 게이트웨이의 형식과 식별을 정의합니다. 값을 지정하지 않으면 피어 IP 주소가 피어 식별 값으로 사용됩니다.
4. 7단계로 진행합니다(게이트웨이에 대한 고급 옵션 구성).

**STEP 6 |** 인증서 기반 인증을 구성합니다.

터널의 반대쪽 끝에 있는 피어 게이트웨이를 인증하는 방법으로 인증서를 선택한 경우 이 절차의 나머지 단계를 수행합니다.

1. 이미 방화벽에 있는 로컬 인증서, 인증서를 가져오기 또는 새 인증서 생성을 선택합니다.
   - 인증서를 가져와야 하는 경우 먼저 IKEv2 게이트웨이 인증에 대한 인증서를 불러온 다음 이 작업으로 돌아갑니다.
   - 새 인증서를 생성하려면 먼저 방화벽에서 인증서를 생성한 다음 이 작업으로 돌아갑니다.
2. (선택 사항) **HTTP** 인증서 교환 을 사용하도록 설정(선택)하여 해시 및 URL을 구성합니다(IKEv2만 해당). HTTP 인증서 교환의 경우 인증서 **URL**을 입력합니다. 자세한 내용은 해시 및 URL 인증서 교환을 참조하십시오.
3. 로컬 **ID** 유형 선택 - 고유 이름**(**제목**), FQDN(**호스트 이름**)**, **IP** 주소 또는 사용자 **FQDN(**이메일 주소**)** - 그런 다음 값을 입력합니다. 로컬 식별은 로컬 게이트웨이의 형식과 식별을 정의합니다.
4. 피어 식별 유형 선택 - 고유 이름**(**제목**), FQDN(**호스트 이름**)**, **IP** 주소 또는 사용자 **FQDN(**이메일 주소**)** - 그런 다음 값을 입력합니다. 피어 식별은 피어 게이트웨이의 형식과 식별을 정의합니다.
5. 피어 **ID** 확인 유형 지정:
   - 정확성 - 로컬 설정 및 피어 IKE ID 페이로드가 정확히 일치하는지 확인합니다.
   - 와일드카드 - 와일드카드(*) 앞의 모든 문자가 일치하는 한 피어 식별이 일치하도록 허용합니다. 와일드카드 후의 문자는 일치할 필요가 없습니다.
6. (선택사항) 피어 식별 및 인증서 페이로드 식별 불일치를 허용하여 동료 식별이 인증서의 피어 식별과 일치하지 않는 경우에도 성공적인 IKE SA를 허용합니다.
7. 인증서 프로파일을 선택합니다. 인증서 프로파일에는 피어 게이트웨이를 인증하는 방법에 대한 정보가 포함되어 있습니다.
8. (선택 사항) 피어의 확장 키 사용에 대한 엄격한 유효성 검사를 활성화하여 키 사용 방법을 엄격하게 제어합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** 게이트웨이에 대한 고급 옵션을 구성합니다.

1. (선택 사항) 공통 옵션(고급 옵션)에서 수동 모드를 사용하도록 설정하여 방화벽이 IKE 연결 요청에만 응답하고 시작하지 않도록 지정합니다.
2. 게이트웨이 간에 NAT를 수행하는 디바이스가 있는 경우 **NAT Traversal**이 IKE 및 UDP 프로토콜에서 UDP 캡슐화를 사용하도록 설정하여 중간 NAT 디바이스를 통과할 수 있습니다.
3. 1단계에서 **IKEv1** 전용 모드를 구성한 경우 IKEv1 탭에서 다음 단계를 수행합니다.
   - 교환 모드: 자동, 공격적 또는 기본을 선택합니다. 자동 교환 모드를 사용하도록 방화벽을 설정하면 메인 모드와 공격적인 모드의 협상 요청을 모두 수락할 수 있지만 가능하면 메인 모드에서 교환이 시작됩니다.

     교환 모드를 자동으로 설정하지 않으면 각 피어가 협상 요청을 수락할 수 있도록 동일한 교환 모드로 두 피어를 구성해야 합니다.
   - 기존 프로파일을 선택하거나 **IKE** 암호화 프로파일 목록에서 기본 프로파일을 유지합니다. 필요한 경우 IKE 암호화 프로파일을 정의할 수 있습니다.
   - (인증서 기반 인증을 사용하고 교환 모드가 공격적인 모드로 설정되지 않은 경우에만) 방화벽이 IKE 조각화로 작동할 수 있도록 조각화 활성화를 클릭합니다.
   - 소멸 피어 감지를 클릭하고 인터벌을 입력합니다(범위는 2~100초입니다). 다시 시도의 경우 가용성을 다시 확인하기 전에 지연 시간(범위는 2~100초)을 정의합니다. 죽은 피어 감지는 IKE 1 단계 알림 페이로드를 피어에게 보내고 승인을 기다리면 비활성 또는 사용할 수 없는 IKE 피어를 식별합니다.
4. 1단계에서 **IKEv2** 전용 모드 또는 **IKEv2** 기본 모드를 구성한 경우 IKEv2 탭에서:
   - DH 그룹, 해시 알고리즘 및 ESP 인증과 같은 IKE 1 단계 옵션을 구성하는 **IKE** 암호화 프로파일을 선택합니다. IKE 암호화 프로파일에 대한 자세한 내용은 IKE 1단계를 참조하십시오.
   - (선택 사항) 엄격한 쿠키 유효성 검사 쿠키 활성화 임계값 및 엄격한 쿠키 유효성 검사를 활성화합니다.
   - (선택사항)게이트웨이가 게이트웨이 피어에 메시지 요청을 보내 응답을 요청하도록 하려는 경우 **Liveness Check**를 활성화하고 인터벌**(**초**)**(기본값은 5)을 입력합니다. 필요한 경우 이니시에이터(Initiator)는 라이브니스 확인을 최대 10번 시도합니다. 응답을 받지 못하면 이니시에이터(Initiator)는 IKE_SA 및 CHILD_SA를 닫고 삭제합니다. 이 이니시에이터(Initiator)는 다른 IKE_SA_INIT 발송하여 다시 시작됩니다.

**STEP 8 |** 확인을 클릭하고 변경 사항을 커밋합니다.

## 해시 및 **URL**을 사용하여 액세스할 피어에 대한 인증서 내보내기

IKEv2는 터널의 원격 끝에 있는 피어가 인증서를 내보낸 서버에서 인증서를 가져오도록 하는 방법으로 해시 및 URL 인증서 교환을(를) 지원합니다. 이 작업을 수행하여 인증서를 해당 서버로 내보냅니다. 디바이스 > 인증서 관리를 사용하여 인증서를 이미 만들었어야 합니다.

**STEP 1 |** 디바이스 > 인증서를 선택한 다음 플랫폼이 위치에 대한 여러 가상 시스템을 지원하는 경우 적절한 가상 시스템을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 디바이스 인증서 탭에서 서버에 내보낼 인증서를 선택합니다.

> 인증서의 상태가 만료되지 않고 유효해야 합니다. 방화벽이 잘못된 인증서를 내보내는 것을 막지 않습니다.

**STEP 3 |** 파일 형식에 대해 이진 인코딩 인증서**(DER)**를 선택합니다.

**STEP 4 |** 내보내기 비공개 키는 비워둡니다. 개인 키를 내보내는 것은 해시 및 URL에 필요하지 않습니다.

**STEP 5 |** 확인을 클릭합니다.

## IKEv2 게이트웨이 인증을 위한 인증서 가져오기

IKEv2 게이트웨이에 대한 피어를 인증하고 이미 방화벽에 있는 로컬 인증서를 사용하지 않은 경우 이 작업을 수행하십시오. 다른 곳에서 인증서를 가져오려고 합니다.

이 작업은 네트워크 > **IKE** 게이트웨이를 선택한 다음 게이트웨이를 추가했으며 로컬 인증서에 대해 가져오기를 클릭했다고 가정합니다.

**STEP 1 |** 인증서를 가져옵니다.

1. 네트워크 > **IKE** 게이트웨이를 선택한 후, 게이트웨이를 추가하고, 일반 탭의 인증에서 인증서를 선택합니다. 로컬 인증서의 경우 가져오기를 클릭합니다.
2. 인증서 가져오기 창에서 가져올 인증서의 인증서 이름을 입력합니다.
3. 이 인증서를 여러 가상 시스템에서 공유하려면 공유를 선택합니다.
4. 인증서 파일의 경우 인증서 파일을 찾아보기합니다. 파일 이름을 클릭하고 열기를 클릭하면 인증서 파일 필드가 채워집니다.
5. 파일 형식에 대해 다음 중 하나를 선택합니다.
   - **Base64** 인코딩된 인증서**(PEM)** - 인증서는 포함하지만 키는 포함하지 않습니다. 클리어텍스트입니다.
   - 암호화된 개인 키 및 인증서**(PKCS12)** - 인증서와 키를 모두 포함합니다.
6. 키가 인증서 파일과 다른 파일에 있는 경우 개인 키 가져오기를 선택합니다. 키는 선택 사항이며 다음 예외는 예외입니다.
   - 파일 형식을 **PEM**으로 설정한 경우 키를 가져와야 합니다. 찾아보기를 클릭하고 가져올 키 파일로 이동하여 키 파일을 입력합니다.
   - 암호를 입력하고 암호를 확인합니다.
7. 확인을 클릭합니다.

**STEP 2 |** 다음 작업을 계속합니다.

인증서 기반 인증을 구성 단계.

## IKEv2의 키 수명 또는 인증 간격 변경

이 작업은 선택 사항입니다. IKEv2 IKE SA 키 재지정 수명의 기본 설정은 8시간입니다. IKEv2 인증 다중의 기본 설정은 0이며, 이는 재인증 기능이 비활성화되어 있음을 의미합니다. 자세한 내용은 SA 키 수명 및 재인증 간격 단원을 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

기본값을 변경하려면 다음 작업을 수행하십시오. 전제 조건은 IKE 암호화 프로파일이 이미 존재한다는 것입니다.

**STEP 1 |** IKE 암호화 프로파일에 대한 SA 키 수명 또는 인증 간격을 변경합니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 암호화를 선택한 다음 로컬 게이트웨이에 적용되는 IKE 암호화 프로파일을 선택합니다.
2. 키 수명에서 단위(초, 분, 시간 또는 일)를 선택하고 값을 입력합니다. 최소값은 3분입니다.
3. **IKE** 인증 배수에 재인증 간격을 결정하는 수명을 곱한 값을 입력합니다.

**STEP 2 |** 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

## IKEv2에 대한 쿠키 활성화 임계값 변경

쿠키 유효성 검사가 필요하기 전에 방화벽에 기본 설정인 500개의 반쯤 열린 SA 세션과 다른 임계값을 지정하려면 다음 작업을 수행합니다. 쿠키 유효성 검사에 대한 자세한 내용은 쿠키 활성화 임계값 및 엄격한 쿠키 유효성 검사를 참조하십시오.

**STEP 1 |** 쿠키 활성화 임계값을 변경합니다.

1. 디바이스 > 설정 > 세션을 선택한 다음 VPN 세션 설정을 편집합니다. 쿠키 활성화 임계값에 응답자가 개시자로부터 쿠키를 요청하기 전에 허용되는 반쯤 열린 SA의 최대 수를 입력합니다(범위는 0-65,535, 기본값은 500).
2. 확인을 클릭합니다.

**STEP 2 |** 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

## IKEv2 트래픽 선택기 구성

IKEv2에서는 IKE 협상 중에 사용되는 네트워크 트래픽의 요소인 트래픽 선택기을(를) 구성할 수 있습니다. 트래픽 셀렉터는 터널을 설정하고 터널을 통해 허용되는 트래픽을 결정하는 CHILD_SA(터널 생성) 2단계에서 사용됩니다. 두 IKE 게이트웨이 피어는 트래픽 셀렉터와 협상하고 상호 동의해야 합니다. 그렇지 않으면 한쪽은 합의에 도달하기 위해 주소 범위를 좁히지 않습니다. 하나의 IKE 연결에는 여러 터널이 있을 수 있습니다. 예를 들어 각 부서에 다른 터널을 할당하여 트래픽을 격리할 수 있습니다. 트래픽 분리를 통해 QoS와 같은 기능을 구현할 수 있습니다. 다음 워크플로를 사용하여 트래픽 선택기를 구성합니다.

**STEP 1 |** 네트워크 > **IPSec** 터널 > 프록시 **ID**를 선택합니다.

**STEP 2 |** **IPv4** 또는 **IPv6** 탭을 선택합니다.

**STEP 3 |** 추가를 클릭하고 프록시 **ID** 필드에 이름을 입력합니다.

**STEP 4 |** 로컬필드에소스 **IP** 주소를 입력합니다.

**STEP 5 |** 원격필드에대상 **IP** 주소를 입력합니다.

**STEP 6 |** 프로토콜 필드에서 전송 프로토콜(**TCP** 또는 **UDP**)을 선택합니다.

**STEP 7 |** 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 암호화 프로파일 정의

암호화 프로파일은 두 IKE 피어 간의 인증 및/또는 암호화에 사용되는 암호와 키의 수명을 지정합니다. 각 재협상 사이의 기간을 수명이라고 합니다. 지정된 시간이 만료되면 방화벽이 새 키 집합을 재협상합니다.

VPN 터널을 통한 통신을 보호하기 위해 방화벽에는 IKE 1단계 및 2단계 협상을 각각 완료하기 위해 IKE 및 IPsec 암호화 프로파일이 필요합니다. 방화벽에는 사용할 준비가 된 기본 IKE 암호화 프로파일과 기본 IPsec 암호화 프로파일이 포함되어 있습니다.

- IKE 암호화 프로파일 정의
- IPsec 암호화 프로파일 정의

## IKE 암호화 프로파일 정의

IKE 암호화 프로파일은 IKE 1단계에서 키 교환 프로세스에 사용되는 암호화 및 인증 알고리즘과 키의 유효 기간을 지정하는 키의 수명을 설정하는 데 사용됩니다. 프로파일을 호출하려면 IKE 게이트웨이 구성에 연결해야 합니다.

동일한 인터페이스 또는 로컬 ***IP*** 주소에 구성된 모든 ***IKE*** 게이트웨이는 ***IKE*** 게이트웨이의 피어 ***IP*** 주소 유형이 동적으로 구성되고 ***IKEv1*** 기본 모드 또는 ***IKEv2***가 적용되는 경우 동일한 암호화 프로파일을 사용해야 합니다.

**STEP 1 |** 새 IKE 프로파일을 생성합니다.

1. 네트워크 네트워크 > 프로파일 > **IKE** 암호화를 선택하고 추가를 선택합니다.
2. 새 프로파일의 이름을 입력합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 키 교환과 인증 및 암호화 알고리즘을 위한 DH(Diffie–Hellman) 그룹을 지정합니다.

해당 섹션(DH 그룹, 인증 및 암호화)에서 추가를 클릭하고 메뉴에서 선택합니다.

VPN 피어가 무엇을 지원하는지 확실하지 않은 경우 보안이 가장 높은 순서대로 여러 그룹 또는 알고리즘을 추가합니다. 피어는 터널을 설정하기 위해 가장 강력한 지원 그룹 또는 알고리즘을 협상합니다.

- DH 그룹—
  - 그룹**21**
  - 그룹**20**
  - 그룹**16**
  - 그룹**15**
  - 그룹**19**
  - 그룹**14**
  - 그룹**5**
  - 그룹**2**
  - 그룹**1**
- 인증—
  - **sha512**
  - **sha384**
  - **sha256**
  - **sha1**
  - **md5**
  - 없음

  암호화를 위해 ***AES-GCM*** 알고리즘을 선택하는 경우 인증 설정을 없음으로 선택해야 합니다. 그렇지 않으면 커밋이 실패합니다. 해시는 선택한 ***DH*** 그룹에 따라 자동으로 선택됩니다. ***DH*** 그룹 *19* 이하에서는 ***sha256***을 사용합니다. ***DH*** 그룹 *20*은 ***sha384***를 사용합니다.
- 암호화 - aes-256-gcm
  - **aes-256-gcm**(IKEv2 필요, DH 그룹은 그룹**20**으로 설정해야 함)
  - **aes-128-gcm**(IKEv2 및 DH 그룹 집합 필요 그룹**19**)
  - **aes-256-cbc**
  - **aes-192-cbc**
  - **aes-128-cbc**
  - **3des**

 ©2023 Palo Alto Networks, Inc.

피어가 지원할 수 있는 가장 강력한 인증 및 암호화 알고리즘을 선택하십시오. 인증 알고리즘의 경우 ***SHA-256*** 이상을 사용합니다(장기 트랜잭션의 경우 ***SHA-384*** 이상 선호). ***SHA-1*** 또는 ***MD5***를 사용하지 마십시오. 암호화 알고리즘의 경우 ***AES***를 사용합니다. ***DES***와 ***3DES***는 약하고 취약합니다. ***Galois/Counter Mode(AES-GCM)***를 사용하는 ***AES***는 가장 강력한 보안을 제공하고 인증이 내장되어 있으므로 ***aes-256-gcm*** 또는 ***aes-128-gcm*** 암호화를 선택하는 경우 인증을 없음으로 설정해야 합니다.

**STEP 3 |** 키가 유효한 기간과 재인증 인터벌을 지정합니다.

자세한 내용은 SA 키 수명 및 재인증 인터벌을 참조하십시오.

1. 키 수명 필드에서 키가 유효한 기간(초, 분, 시간 또는 일 단위)을 지정합니다(범위는 3분에서 365일 사이, 기본값은 8시간). 키가 만료되면 방화벽이 새 키를 재협상합니다. 수명은 각 재협상 사이의 기간입니다.
2. **IKEv2** 인증 다중의 경우 인증 수를 결정하기 위해 키 수명을 곱한 값(범위는 0-50, 기본값은 0)을 지정합니다. 기본값 0은 재인증 기능을 사용하지 않도록 설정합니다.

**STEP 4 |** IKE 암호화 프로파일을 커밋합니다.

확인을 클릭하고 커밋을 클릭합니다.

**STEP 5 |** IKE 게이트웨이 구성에 IKE 암호화 프로파일을 연결합니다.

게이트웨이에 대한 Advanced 옵션 구성을 참조하십시오.

## IPsec 암호화 프로파일 정의

IKE 2단계에서 IPsec 암호화 프로파일이 호출됩니다. 자동 키 IKE를 사용하여 IKE SA에 대한 키를 자동으로 생성할 때 터널 내에서 데이터가 보호되는 방법을 지정합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 새 IPsec 프로파일을 생성합니다.

1. 네트워크 > 네트워크 프로파일 > **IPsec** 암호화를 선택한 다음 추가를 선택합니다.
2. 새 프로파일의 이름을 입력합니다.
3. 데이터가 터널을 통과할 때 데이터를 보호하기 위해 적용할 **IPsec** 프로토콜(ESP 또는 AH)을 선택합니다.

   *ESP*는 연결에 대한 기밀성과 인증을 모두 제공하는 반면 *AH*는 인증만 제공하므로 *AH*(인증 헤더)를 통해 *ESP*(보안 페이로드 캡슐화)를 선택하는 것이 가장 좋습니다.
4. 추가를 클릭하고 ESP에 대한 인증 및 암호화 알고리즘과 AH에 대한 인증 알고리즘을 선택합니다. 그러면 IKE 피어는 터널을 통해 데이터를 안전하게 전송하기 위해 키를 협상할 수 있습니다.

   IKE 피어가 지원하는 것이 확실하지 않은 경우 다음과 같이 보안 수준이 가장 낮은 순서로 여러 알고리즘을 추가합니다. 피어는 지원되는 가장 강력한 알고리즘을 협상하여 터널을 설정합니다.

   - 암호화—**aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm**(VM 시리즈 방화벽은 이 옵션을 지원하지 않음), **aes-128-cbc**, **3des**.

     피어가 지원할 수 있는 가장 강력한 인증 및 암호화 알고리즘을 선택하는 것이 가장 좋습니다. 인증 알고리즘의 경우 *SHA-256* 이상을 사용합니다(장기 트랜잭션의 경우 *SHA-384* 이상 선호). *SHA-1*, *MD5* 또는 아무 것도 사용하지 마십시오. 암호화 알고리즘의 경우 *AES*를 사용하십시오. *3DES*는 약하고 취약합니다.
   - 인증—**sha512**, **sha384**, **sha256**, **sha1**, **md5**.

**STEP 2 |** IKE 단계 2에서 IPsec SA 협상에 사용할 DH 그룹을 선택합니다.

**DH** 그룹에서 사용하려는 키 강도를 선택합니다. 그룹**1**, 그룹**2**, 그룹**5**, 그룹**14** , 그룹**15**, 그룹**16**, 그룹**19**, 그룹**20** 또는 그룹**21**. 최고의 보안을 위해 가장 높은 숫자를 가진 그룹을 선택하십시오.

IKE 단계 1 상태에서 방화벽이 만드는 키를 갱신하지 않으려면 **no-pfs**(완벽한 포워딩 보안 없음)를 선택합니다. 방화벽은 IPsec SA(보안 연결) 협상에 현재 키를 재사용합니다.

**STEP 3 |** 키 지속 시간(트래픽 시간 및 볼륨)을 지정합니다.

시간과 교통량을 함께 사용하면 데이터의 안전을 보장할 수 있습니다.

키가 유효한 수명 또는 기간을 초, 분, 시간 또는 일 단위로 선택합니다(범위는 3분에서 365일까지입니다). 지정된 시간이 만료되면 방화벽이 새 키 집합을 재협상합니다.

키를 재협상해야 하는 **Lifesize** 또는 데이터 볼륨을 선택합니다.

**STEP 4 |** IPsec 프로파일을 커밋합니다.

확인을 클릭하고 커밋을 클릭합니다.

**STEP 5 |** IPsec 프로파일을 IPsec 터널 구성에 연결합니다.

키 교환 설정을 참조하십시오.

## IPsec 터널 설정

IPSec 터널 구성을 사용하면 터널을 통과할 때 데이터(IP 패킷)를 인증 및/또는 암호화할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

정책 기반 VPN을 지원하는 피어와 함께 작동하도록 방화벽을 설정하는 경우 프록시 ID를 정의해야 합니다. 정책 기반 VPN을 지원하는 디바이스는 IPSec 터널을 통한 관심 트래픽을 허용하기 위해 특정 보안 규칙/정책 또는 액세스 목록(소스 주소, 대상 주소 및 포트)을 사용합니다. 이러한 규칙은 빠른 모드/IKE 단계 2 협상 중에 참조되며 프로세스의 첫 번째 또는 두 번째 메시지에서 Proxy-ID로 교환됩니다. 따라서 정책 기반 VPN 피어와 함께 작동하도록 방화벽을 구성하는 경우 성공적인 2단계 협상을 위해 두 피어의 설정이 동일하도록 Proxy-ID를 정의해야 합니다. 방화벽이 경로 기반 VPN을 지원하기 때문에 Proxy-ID가 구성되지 않은 경우 Proxy-ID로 사용되는 기본값은 소스 IP입니다. 0.0.0.0/0, 대상 IP: 0.0.0.0/0 및 애플리케이션: 모두 이 값이 피어와 교환되면 VPN 연결 설정에 실패합니다.

**STEP 1 |** 네트워크 > **IPSec** 터널을 선택한 다음 새 터널 구성을 추가합니다.

**STEP 2 |** 일반 탭에서 터널의 이름을 입력합니다.

**STEP 3 |** IPSec 터널을 설정할 터널 인터페이스를 선택합니다.

새 터널 인터페이스를 생성하려면:

1. 터널 인터페이스 > 새 터널 인터페이스를 선택합니다. (네트워크 > 인터페이스 > 터널을 선택하고 추가를 클릭할 수도 있습니다.)
2. 인터페이스 이름 필드에 숫자 접미사(예: **.2**)를 지정합니다.
3. 구성 탭에서 보안 영역 목록을 선택하여 다음과 같이 영역을 정의합니다.

트러스트 영역을 터널의 종료 지점으로 사용 **-** 영역을 선택합니다**.** 패킷이 방화벽에 들어가는 외부 인터페이스와 동일한 영역(및 가상 라우터)과 터널 인터페이스를 연결하면 영역 간 라우팅을 생성할 필요성이 줄어듭니다.

또는:

**VPN** 터널 종료를 위한 별도 영역 생성(권장) - 새 영역을 선택한 다음 새 영역의 이름(예: vpn-corp)을 정의한 다음 확인을 클릭합니다.

1. 가상 라우터의 경우 기본값을 선택합니다.
2. (선택 사항) IPv4 주소를 터널 인터페이스에 할당하려면 **IPv4** 탭을 선택하고 IP 주소와 네트워크 마스크를 추가합니다. 예: 10.31.32.1/32.
3. 확인을 클릭합니다.

**STEP 4 |** (선택 사항) 터널 인터페이스에서 IPv6을 사용하도록 설정합니다.

1. 네트워크 > 인터페이스 > 터널 > **IPv6**에서 IPv6 탭을 선택합니다.
2. 인터페이스에서 **IPv6** 사용을 선택합니다.

   이 옵션을 사용하면 IPv4 IPSec 터널을 통해 IPv6 트래픽을 라우팅할 수 있으며 IPv6 네트워크 간에 기밀성을 제공합니다. IPv6 트래픽은 IPv4에 의해 캡슐화된 다음 ESP에 의해 캡슐화됩니

 ©2023 Palo Alto Networks, Inc.

다. IPv6 트래픽을 터널로 라우팅하려면 터널에 대한 정적 경로를 사용하거나 OSPFv3을 사용하거나 PBF(정책 기반 포워딩) 규칙을 사용할 수 있습니다.

3. 64비트 확장 고유 인터페이스 **ID**를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 기본적으로 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다.
4. 터널 인터페이스에 IPv6 주소를 할당하려면 IPv6 주소와 프리픽스 길이를 추가합니다(예: 2001:400:f00::1/64). 접두사를 선택하지 않으면 인터페이스에 할당된 IPv6 주소가 주소 텍스트 상자에 완전히 지정됩니다.
   1. 인터페이스 **ID**를 호스트 부분으로 사용을 선택하여 인터페이스 ID를 주소의 호스트 부분으로 사용할 인터페이스에 IPv6 주소를 할당합니다.
   2. 가장 가까운 노드를 통한 라우팅을 포함하려면 **Anycast**를 선택합니다.

**STEP 5 |** 키 교환을 설정합니다.

일반 탭에서 다음 유형의 키 교환 중 하나를 구성합니다.

자동 키 교환 설정

1. IKE 게이트웨이를 선택합니다. IKE 게이트웨이를 설정하려면 IKE 게이트웨이 설정을 참조하십시오.
2. (선택 사항) 기본 IPSec 암호화 프로파일을 선택합니다. 새 IPSec 프로파일을 만들려면 IPSec 암호화 프로파일 정의를 참조하십시오.

수동 키 교환 설정

1. 로컬 방화벽에 대한 로컬 **SPI**를 지정합니다. SPI는 IPSec 트래픽 플로우를 구분하는 데 도움이 되도록 IPSec 터널링을 위해 헤더에 추가되는 32비트 16진수 인덱스입니다. VPN 터널을 설정하는 데 필요한 SA를 만드는 데 사용됩니다.
2. 터널 엔드포인트이 될 인터페이스를 선택한 다음 선택적으로 터널의 엔드포인트이 되는 로컬 인터페이스의 IP 주소를 선택합니다.
3. 사용할 프로토콜(**AH** 또는 **ESP**)을 선택합니다.
4. AH의 경우 인증 방법을 선택하고 키를 입력한 다음 키 확인을 입력합니다.
5. ESP의 경우 인증 방법을 선택하고 키를 입력한 다음 키 확인을 입력합니다. 그런 다음 암호화 방법을 선택하고 필요한 경우 키를 입력한 다음 키 확인을 입력합니다.
6. 원격 피어에 대한 원격 **SPI**를 지정합니다.
7. 원격 주소, 원격 피어의 IP 주소를 입력합니다.

**STEP 6 |** 재생 공격으로부터 보호합니다.

재전송 방지는 IPSec의 하위 프로토콜이며 IETF(Internet Engineering Task Force) RFC(Request for Comments) 6479의 일부입니다. 재생 방지 프로토콜은 해커가 소스에서 대상으로 이동하는 패킷을 삽입하거나 변경하는 것을 방지하는 데 사용되며 네트워크의 두 노드 간에 보안 연결을 설정하기 위해 단방향 보안 연결을 사용합니다.

보안 연결이 설정된 후 재생 방지 프로토콜은 패킷 시퀀스 번호를 사용하여 재생 공격을 물리칩니다. 소스가 메시지를 보낼 때 패킷에 시퀀스 번호를 추가합니다. 시퀀스 번호는 0에서 시작하고 각 후속 패킷에 대해 1씩 증가합니다. 목적지는 슬라이딩 윈도우 형식의 숫자 시퀀스를 유지하고, 검증된 수신 패킷의 시퀀스 번호 기록을 유지하며, 슬라이딩 윈도우(너무 오래된 패킷) 또는 슬라이딩 창에 이미 나타

 ©2023 Palo Alto Networks, Inc.

나는 패킷(중복 또는 재생된 패킷)에서 가장 낮은 시퀀스 번호보다 낮은 시퀀스 번호를 가진 모든 패킷을 거부합니다. 승인된 패킷은 유효성이 검사된 후 슬라이딩 윈도우를 업데이트하여 이미 가득 찬 경우 윈도우 밖으로 가장 낮은 시퀀스 번호를 대체합니다.

1. 일반 탭에서 고급 옵션 표시를 선택한 다음 재생 보호 사용을 선택하여 재생 공격을 탐지하고 무력화합니다.
2. 사용할 재전송 방지 윈도우를 선택합니다. 재전송 방지 윈도우 크기를 64, 128, 256, 512, 1024, 2048 또는 4096 중에서 선택할 수 있습니다. 기본값은 1024입니다.

**STEP 7 |** (선택 사항) IP 패킷의 우선 순위 또는 처리를 위해 서비스 유형 헤더를 보존합니다.

고급 옵션 표시 섹션에서 **TOS** 헤더 복사를 선택합니다. 이것은 원래 TOS 정보를 보존하기 위해 내부 IP 헤더에서 캡슐화된 패킷의 외부 IP 헤더로 서비스 유형(TOS) 헤더를 복사합니다.

터널 내부에 여러 세션이 있는 경우*(*각각 다른 *TOS* 값을 가짐*) TOS* 헤더를 복사하면 *IPSec* 패킷이 순서 없이 도착할 수 있습니다*.*

**STEP 8 |** (선택 사항) **GRE** 캡슐화 추가를 선택하여 IPSec을 통한 GRE를 활성화합니다.

IPSec이 트래픽을 암호화하기 전에 원격 엔드포인트이 GRE 터널 내에서 트래픽을 캡슐화해야 하는 경우 GRE 캡슐화를 추가합니다. 예를 들어, 일부 구현에서는 IPSec이 암호화하기 전에 멀티캐스트 트래픽을 캡슐화해야 합니다. IPSec에 캡슐화된 GRE 패킷이 캡슐화하는 IPSec 터널과 동일한 소스 IP 주소 및 대상 IP 주소를 가질 때 GRE 캡슐화를 추가합니다.

**STEP 9 |** 터널 모니터링을 활성화합니다.

모니터링을 위해 터널 인터페이스에 *IP* 주소를 할당해야 합니다*.*

디바이스 관리자에게 터널 실패에 대해 경고하고 다른 터널 인터페이스에 대한 자동 페일오버를 제공하려면:

1. 터널 모니터를 선택합니다.
2. 터널이 제대로 작동하는지 확인하려면 터널 반대쪽에 대상 **IP** 주소를 지정합니다.
3. 프로파일을 선택하여 터널 실패 시 조치를 결정하십시오. 새 프로파일을 생성하려면 터널 모니터링 프로파일 정의를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 10 |** VPN 피어를 식별하는 프록시 ID를 생성합니다.

이 단계는 VPN 피어가 정책 기반 VPN을 사용하는 경우에만 필요합니다.

1. 네트워크 > **IPSec** 터널을 선택하고 추가를 클릭합니다.
2. 프록시 **ID** 탭을 선택합니다.
3. **IPv4** 또는 **IPv6** 탭을 선택합니다.
4. 추가를 클릭하고 프록시 **ID** 이름을 입력합니다.
5. VPN 게이트웨이의 로컬 IP 주소 또는 서브넷을 입력합니다.
6. VPN 게이트웨이의 원격 주소를 입력합니다.
7. 프로토콜을 선택합니다.
   - 번호 - 프로토콜 번호를 지정합니다(타사 디바이스와의 상호 운용성을 위해 사용됨).
   - 모두 - TCP 및/또는 UDP 트래픽을 허용합니다.
   - **TCP** - 로컬 포트 및 원격 포트 번호를 지정합니다.
   - **UDP** - 로컬 포트 및 원격 포트 번호를 지정합니다.
8. 확인을 클릭합니다.

**STEP 11 |** 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

## 터널 모니터링 설정

중단 없는 VPN 서비스를 제공하기 위해 방화벽의 터널 모니터링 기능과 함께 Dead Peer Detection 기능을 사용할 수 있습니다. 터널의 상태를 모니터링할 수도 있습니다. 이러한 모니터링 작업은 다음 섹션에서 설명합니다.

- 터널 모니터링 프로파일 정의
- 터널 상태 보기

### 터널 모니터링 프로파일 정의

터널 모니터링 프로파일을 사용하면 VPN 피어 간의 연결을 확인할 수 있습니다. 지정된 인터벌로 대상 IP 주소를 핑(ping)하도록 터널 인터페이스를 구성하고 터널을 가로지르는 통신이 끊어지면 작업을 지정할 수 있습니다.

**STEP 1 |** 네트워크 > 네트워크 프로파일 > 모니터를 선택합니다. 기본 터널 모니터링 프로파일을 사용할 수 있습니다.

**STEP 2 |** 추가를 클릭하고 프로파일 이름을 입력합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 대상 IP 주소에 연결할 수 없는 경우 취할 작업을 선택합니다.

- 복구 대기—방화벽이 터널이 복구되기를 기다립니다. 터널이 여전히 활성화된 것처럼 라우팅 결정에 터널 인터페이스를 계속 사용합니다.
- 페일오버—트래픽을 사용할 수 있는 경우 백업 경로로 강제로 이동합니다. 방화벽은 터널 인터페이스를 비활성화하여 인터페이스를 사용하는 라우팅 테이블의 모든 경로를 비활성화합니다.

두 경우 모두 방화벽은 새 IPSec 키를 협상하여 복구를 가속화하려고 시도합니다.

**STEP 4 |** 지정된 작업을 트리거하려면 인터벌**(**초**)** 및 임계값을 지정합니다.

- 임계값은 지정된 작업을 수행하기 전에 기다릴 하트비트 수를 지정합니다(범위는 2-100, 기본값은 5).
- 인터벌**(**초**)**은 하트비트 사이의 시간(초)을 지정합니다(범위는 2-10; 기본값은 3).

**STEP 5 |** 모니터링 프로파일을 IPsec 터널 구성에 연결합니다. 터널 모니터링 사용을 참조하십시오.

## 터널 상태 보기

터널 상태는 유효한 IKE 1단계 및 2단계 SA가 설정되었는지 여부와 터널 인터페이스가 작동 중이고 트래픽을 전달할 수 있는지 여부를 알려줍니다.

터널 인터페이스는 논리 인터페이스이므로 물리적 링크 상태를 나타낼 수 없습니다. 따라서 터널 인터페이스가 IP 주소에 대한 연결을 확인하고 경로를 여전히 사용할 수 있는지 확인할 수 있도록 터널 모니터링을 활성화해야 합니다. IP 주소에 연결할 수 없는 경우 방화벽은 터널이 복구되거나 페일오버될 때까지 기다립니다. 페일오버가 발생하면 기존 터널이 철거되고 라우팅 변경이 트리거되어 새 터널을 설정하고 트래픽을 리디렉션합니다.

**STEP 1 |** 네트워크 > **IPSec** 터널을 선택합니다.

**STEP 2 |** 터널 상태를 봅니다.

- 녹색은 유효한 IPSec SA 터널을 나타냅니다.
- 빨간색은 IPSec SA를 사용할 수 없거나 만료되었음을 나타냅니다.

**STEP 3 |** **IKE** 게이트웨이 상태를 봅니다.

- 녹색은 유효한 IKE 위상-1 SA를 나타냅니다.
- 빨간색은 IKE 1단계 SA를 사용할 수 없거나 만료되었음을 나타냅니다.

**STEP 4 |** 터널 인터페이스 상태를 봅니다.

- 녹색은 터널 인터페이스가 작동 중임을 나타냅니다.
- 빨간색은 터널 모니터링이 활성화되고 상태가 다운되어 터널 인터페이스가 다운됨을 나타냅니다.

아직 작동하지 않는 VPN 터널 문제를 해결하려면 VPN 오류 메시지 해석을(를) 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

# IKE 게이트웨이 또는 IPSec 터널 활성화/비활성화, 새로 고침 또는 다시 시작

문제 해결을 더 쉽게 하기 위해 IKE 게이트웨이 또는 VPN 터널을 활성화, 비활성화, 새로 고침 또는 다시 시작할 수 있습니다.

- IKE 게이트웨이 또는 IPsec 터널 사용 또는 사용 안 함
- 새로 고침 및 재시작 동작
- IKE 게이트웨이 또는 IPsec 터널 새로 고침 또는 다시 시작

## **IKE** 게이트웨이 또는 **IPsec** 터널 사용 또는 사용 안 함

문제 해결을 더 쉽게 하려면 IKE 게이트웨이 또는 IPSec 터널을 활성화하거나 비활성화합니다.

- IKE 게이트웨이를 활성화하거나 비활성화합니다.
  1. 네트워크 > 네트워크 프로파일 > **IKE** 게이트웨이를 선택한 다음 활성화 또는 비활성화하려는 게이트웨이를 선택합니다.
  2. 화면 하단에서 활성화 또는 비활성화를 클릭합니다.

- IPSec 터널을 활성화하거나 비활성화합니다.
  1. 네트워크 > **IPSec** 터널을 선택한 다음 활성화하거나 비활성화할 터널을 선택합니다.
  2. 화면 하단에서 활성화 또는 비활성화를 클릭합니다.

## 새로 고침 및 재시작 동작

IKE 게이트웨이 또는 IPSec 터널을 새로 고치거나 다시 시작할 수 있습니다. IKE 게이트웨이 및 IPSec 터널에 대한 새로 고침 및 다시 시작 동작은 다음과 같습니다.

| 단계 | 새로고침 | 재시작 |
|---|---|---|
| IKE 게이트웨이(IKE 1단계) | 선택한 IKE 게이트웨이에 대한 화면 통계를 업데이트합니다.<br>CLI에서 두 번째 **show** 명령을 실행하는 것과 동일합니다(초기 **show** 명령 후). | 선택한 IKE 게이트웨이를 다시 시작합니다.<br>**IKEv2**: 또한 연결된 모든 하위 IPSec SA(보안 연결)를 다시 시작합니다.<br>**IKEv1**: 연결된 IPSec SA를 다시 시작하지 않습니다.<br>다시 시작하면 모든 기존 세션이 중단됩니다.<br>CLI에서 **clear**, **test**, **show** 명령 시퀀스를 실행하는 것과 동일합니다. |
| IPSec 터널(IKE 2단계) | 선택한 IPSec 터널에 대한 화면 통계를 업데이트합니다.<br>CLI에서 두 번째 **show** 명령을 실행하는 것과 동일합니다(초기 **show** 명령 후). | IPSec 터널을 다시 시작합니다.<br>다시 시작하면 모든 기존 세션이 중단됩니다. |


©2023 Palo Alto Networks, Inc.

| 단계 | 새로고침 | 재시작 |
|---|---|---|
| | | CLI에서 **clear**, **test**, **show** 명령 시퀀스를 실행하는 것과 동일합니다. |

### IKE 게이트웨이 또는 IPsec 터널 새로 고침 또는 다시 시작

IKE 게이트웨이를 다시 시작한 결과는 IKEv1인지 IKEv2인지에 따라 다릅니다. IKE 게이트웨이(IKEv1 및 IKEv2) 및 IPsec 터널에 대한 새로 고침 및 작동 재시작을 참조하십시오.

- IKE 게이트웨이를 새로 고치거나 다시 시작합니다
  1. 네트워크 > **IPSec** 터널을 선택하고 새로 고치거나 다시 시작할 게이트웨이의 터널을 선택합니다.
  2. 해당 터널에 대한 행의 상태 열에서 **IKE** 정보를 클릭합니다.
  3. IKE 정보 화면 하단에서 원하는 작업을 클릭합니다.
     - 새로 고침 —화면에서 통계를 업데이트합니다.
     - 다시 시작 - SA를 지우므로 IKE 협상이 다시 시작되고 터널이 다시 생성될 때까지 트래픽이 삭제됩니다.

- IPsec 터널을 새로 고치거나 다시 시작합니다.

  터널 모니터를 사용하여 터널 상태를 모니터링하거나 외부 네트워크 모니터를 사용하여 IPsec 터널을 통한 네트워크 연결을 모니터링하기 때문에 터널을 새로 고치거나 다시 시작해야 할 수 있습니다.
  1. 네트워크 > **IPSec** 터널을 선택하고 새로 고치거나 다시 시작할 터널을 선택합니다.
  2. 해당 터널에 대한 행의 상태 열에서 터널 정보를 클릭합니다.
  3. 터널 정보 화면 하단에서 원하는 작업을 클릭합니다.
     - 새로 고침 —화면상의 통계를 업데이트합니다.
     - 다시 시작 - SA를 지우므로 IKE 협상이 다시 시작되고 터널이 다시 생성될 때까지 트래픽이 삭제됩니다.

## VPN 연결 테스트

VPN 연결을 테스트하려면 이 작업을 수행하십시오.

**STEP 1 |** 터널을 통해 호스트를 핑(ping)하거나 다음 CLI 명령을 사용하여 IKE 단계 1을 시작합니다.

```
test vpn ike-sa gateway <gateway_name>
```

**STEP 2 |** 다음 명령을 입력하여 IKE 단계 1이 설정되었는지 테스트합니다.

```
show vpn ike-sa gateway <gateway_name>
```

출력에서 보안 연결이 표시되는지 확인합니다. 그렇지 않은 경우 시스템 로그 메시지를 검토하여 실패 이유를 해석하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 터널을 통해 호스트를 ping하거나 다음 CLI 명령을 사용하여 IKE 단계 2를 시작합니다.

```
test vpn ipsec-sa tunnel <tunnel_name>
```

**STEP 4 |** 다음 명령을 입력하여 IKE 단계 2가 설정되었는지 테스트합니다.

```
show vpn ipsec-sa tunnel <tunnel_name>
```

출력에서 보안 연결이 표시되는지 확인합니다. 그렇지 않은 경우 시스템 로그 메시지를 검토하여 실패 이유를 해석하십시오.

**STEP 5 |** VPN 트래픽 플로우 정보를 보려면 다음 명령을 사용하십시오.

```
show vpn flow total tunnels configured:              1 filter - type
 IPSec, state any total IPSec tunnel configured:         1 total
 IPSec tunnel shown:                  1 name                      id
      state       local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------------
 vpn-to-siteB        5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

## VPN 오류 메시지 해석

다음 표에는 시스템 로그에 로그인한 몇 가지 일반적인 VPN 오류 메시지가 나열됩니다.

표 **6: VPN** 문제에 대한 **Syslog** 오류 메시지

| 오류가 있는 경우 다음을 수행합니다. | 다음을 시도해 보십시오. |
|---|---|
| `IKE 단계-1 협상은 개시자, 메인 모드로 실패합니다. Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`<br>또는<br>`IKE 1단계 협상이 실패했습니다. 피어 IP x.x.x.x[1929] IKE 위상-1 요청에 대한 구성을 찾을 수 없습니다.` | • IKE 게이트웨이 구성에서 각 VPN 피어의 공용 IP 주소가 정확한지 확인합니다.<br>• IP 주소를 핑(ping)할 수 있는지의 여부와 라우팅 문제가 연결 실패를 일으키지 않는지 확인합니다. |
| `Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...`<br>또는<br>`IKE 1단계 협상이 실패했습니다. 피어의 SA 페이로드를 처리할 수 없습니다.` | IKE 암호화 프로파일 구성을 확인하여 양측의 제안서에 공통 암호화, 인증 및 DH 그룹 제안이 있는지 확인합니다. |

 ©2023 Palo Alto Networks, Inc.

| 오류가 있는 경우 다음을 수행합니다. | 다음을 시도해 보십시오. |
| --- | --- |
| `pfs group mismatched:my: 2peer: 0`<br>또는<br>`SA 페이로드를 처리할 때 IKE 단계-2 협상이 실패했습니다. 피어의 SA 페이로드에서 찾을 수있는 적절한 제안이 없습니다.` | IPSec 암호화 프로파일 구성을 확인하여 다음을 확인합니다.<br>• pfs는 두 VPN 피어 모두에서 사용 가능하거나 비활성화됩니다.<br>• 각 피어에서 제안한 DH 그룹에는 공통이 하나 이상 있습니다. |
| `프록시 ID를 처리할 때 IKE 단계-2 협상이 실패했습니다. Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.` | 한쪽 끝에 VPN 피어는 정책 기반 VPN을 사용하고 있습니다. Palo Alto Networks 방화벽에서 프록시 ID를 구성해야 합니다. VPN 피어를 식별하는 프록시 ID 생성을 참조하세요. |


©2023 Palo Alto Networks, Inc.

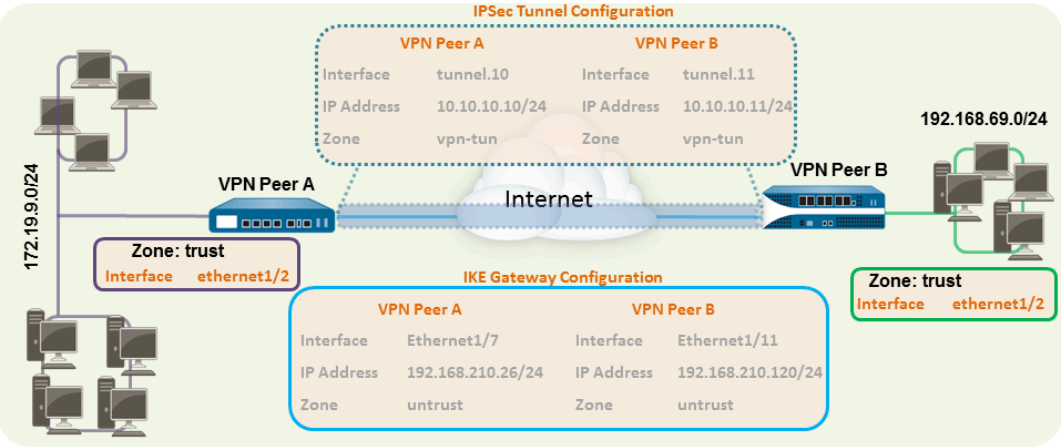
# 사이트 간 VPN 빠른 구성

다음 섹션에서는 몇 가지 일반적인 VPN 배포를 구성하는 지침을 제공합니다.

- 정적 라우팅을 사용하는 사이트 간 VPN
- OSPF를 사용하는 사이트 간 VPN
- 정적 및 동적 라우팅을 사용하는 사이트 간 VPN

## 정적 라우팅을 사용하는 사이트 간 VPN

다음 예는 고정 경로를 사용하는 두 사이트 간의 VPN 연결을 보여줍니다. 동적 라우팅이 없으면 방화벽이 터널 인터페이스를 사이트 간에 트래픽을 라우팅하기 위한 다음 홉으로 자동 사용하기 때문에 VPN 피어 A 및 VPN 피어 B의 터널 인터페이스에는 IP 주소가 필요하지 않습니다. 그러나 터널 모니터링을 활성화하기 위해 각 터널 인터페이스에 고정 IP 주소가 할당되었습니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 레이어 3 인터페이스를 구성합니다.

이 인터페이스는 IKE 단계 1 터널에 사용됩니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택한 다음 VPN에 대해 구성할 인터페이스를 선택합니다.
2. 인터페이스 유형에서 레이어 **3**을 선택합니다.
3. 구성 탭에서 인터페이스가 속한 보안 영역을 선택합니다.
   - 인터페이스는 신뢰 네트워크 외부의 영역에서 액세스할 수 있어야 합니다. VPN 트래픽에 대한 가시성과 제어를 위해 전용 VPN 영역을 만드는 것이 좋습니다.
   - 아직 영역을 만들지 않은 경우 보안**,** 영역에서새 영역을 선택한 다음 새 영역에 대한 이름을 정의한 다음 확인을 클릭합니다.
4. 사용할 가상 라우터를 선택합니다.
5. 인터페이스에 IP 주소를 할당하려면 **IPv4** 탭을 선택하고 IP 섹션에서 추가를 클릭한 다음 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 192.168.210.26/24).
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/7
   - 보안 영역 - 신뢰하지 않음
   - 가상 라우터 - 기본값
   - **IPv4** - 192.168.210.26/24

   VPN 피어 B의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/11
   - 보안 영역 - 신뢰하지 않음
   - 가상 라우터 - 기본값
   - **IPv4** - 192.168.210.120/24


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 터널 인터페이스를 생성하여 가상 라우터 및 보안 영역에 연결합니다.

1. 네트워크 > 인터페이스 > 터널을 선택하고 추가를 클릭합니다.
2. 인터페이스 이름 필드에 숫자 접미사(예: **.1**)를 지정합니다.
3. 구성 탭에서 보안 영역을 확장하여 다음과 같이 영역을 정의합니다.
   - 트러스트 영역을 터널의 종료 지점으로 사용하려면 영역을 선택합니다.
   - (권장) VPN 터널 종료를 위한 별도의 영역을 생성하려면 새 영역을 클릭합니다. 영역 대화 상자에서 새 영역에 대한 이름(예: ***vpn-tun***)을 정의한 다음 확인을 클릭합니다.
4. 가상 라우터를 선택합니다.
5. (선택 사항) 터널 인터페이스에 IP 주소를 할당하고 **IPv4** 또는 **IPv6** 탭을 선택한 다음 IP 섹션에서 추가를 클릭합니다. 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다.

   고정 경로를 사용하면 터널 인터페이스에 IP 주소가 필요하지 않습니다. 지정된 서브넷/IP 주소로 향하는 트래픽의 경우 터널 인터페이스가 자동으로 다음 홉이 됩니다. 터널 모니터링을 활성화하려면 IP 주소를 추가하는 것이 좋습니다.
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.
   - 인터페이스 - tunnel.10
   - **Security Zone** - vpn_tun
   - 가상 라우터 - 기본값
   - **IPv4** - 172.19.9.2/24

   VPN 피어 B의 구성은 다음과 같습니다.
   - 인터페이스 - tunnel.11
   - **Security Zone** - vpn_tun
   - 가상 라우터 - 기본값
   - **IPv4** - 192.168.69.2/24

**STEP 3 |** 가상 라우터에서 대상 서브넷에 대한 고정 경로를 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 이전 단계에서 정의한 라우터를 클릭합니다.
2. 고정 경로를 선택하고 추가를 클릭한 다음 새 경로를 입력하여 터널의 다른 쪽 끝에 있는 서브넷에 액세스합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.
   - 목적지 - 192.168.69.0/24
   - 인터페이스 - tunnel.10

   VPN 피어 B의 구성은 다음과 같습니다.
   - 목적지 - 172.19.9.0/24
   - 인터페이스 - tunnel.11

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 암호화 프로파일을 설정합니다(1단계의 경우 IKE 암호화 프로파일 및 2단계의 경우 IPSec 암호화 프로파일).

두 피어 모두에서 이 작업을 완료하고 동일한 값을 설정해야 합니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 암호화를 선택합니다. 이 예제에서는 기본 프로파일을 사용합니다.
2. 네트워크 > 네트워크 프로파일 > **IPSec** 암호화를 선택합니다. 이 예제에서는 기본 프로파일을 사용합니다.

**STEP 5 |** IKE 게이트웨이를 설정합니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 게이트웨이를 선택합니다.
2. 추가를 클릭하고 일반 탭에서 옵션을 구성합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/7
   - 로컬 **IP** 주소 - 192.168.210.26/24
   - 피어 **IP** 유형/주소 - 고정/192.168.210.120
   - 사전 공유 키 - 값 입력
   - 로컬 식별 - 없음. 이는 로컬 IP 주소가 로컬 식별 값으로 사용됨을 의미합니다.
   - VPN 피어 B의 구성은 다음과 같습니다.
   - **Interface** - ethernet1/11
   - 로컬 **IP** 주소 - 192.168.210.120/24
   - 피어 **IP** 유형/주소 - 고정/192.168.210.26
   - 사전 공유 키 - 피어 A와 동일한 값 입력
   - 로컬 **ID** - 없음
3. 고급 단계 **1** 옵션을 선택하고 IKE 단계 1에 사용할 이전에 생성한 IKE 암호화 프로파일을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** IPSec 터널을 설정합니다.

1. 네트워크 > **IPSec** 터널을 선택합니다.
2. 추가를 클릭하고 일반 탭에서 옵션을 구성합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - 터널 인터페이스 - tunnel.10
   - 유형 - 자동 키
   - **IKE** 게이트웨이 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
   - **IPSec** 암호화 프로파일 - 4단계에서 정의한 IPSec 암호화 프로파일을 선택합니다.

   VPN 피어 B의 구성은 다음과 같습니다.

   - 터널 인터페이스 - tunnel.11
   - 유형 - 자동 키
   - **IKE** 게이트웨이 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
   - **IPSec** 암호화 프로파일 - 4단계에서 정의한 IPSec 암호화를 선택합니다.
3. (선택 사항) 고급 옵션 표시를 선택하고 터널 모니터를 선택한 다음 연결 확인을 위해 ping할 대상 IP 주소를 지정합니다. 일반적으로 VPN 피어의 터널 인터페이스 IP 주소가 사용됩니다.
4. (선택 사항) 연결 설정 실패 시 작업을 정의하려면 터널 모니터링 프로파일 정의를 참조하십시오.

**STEP 7 |** 사이트(서브넷) 간의 트래픽을 허용하는 정책을 생성합니다.

1. 정책 > 보안을 선택합니다.
2. 지정된 소스 및 대상 IP 주소에서 발생하는 트래픽에 대해 untrust 및 vpn-tun 영역과 vpn-tun 및 언트러스트 영역 간의 트래픽을 허용하는 규칙을 생성합니다.

**STEP 8 |** 보류 중인 구성 변경 사항을 커밋합니다.

커밋을 클릭합니다.

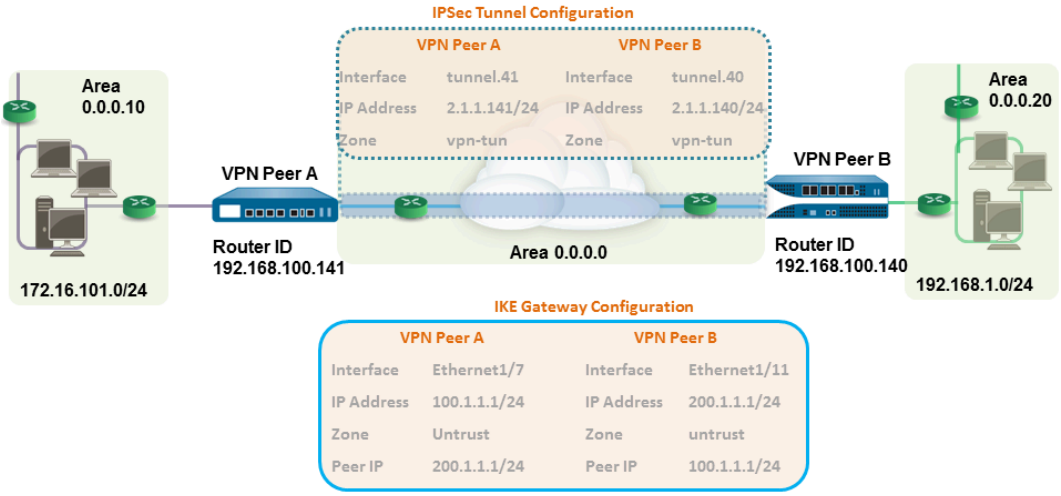
**STEP 9 |** VPN 연결 테스트.

터널 상태 보기도 참조하십시오.

## OSPF를 사용하는 사이트 간 VPN

이 예에서 각 사이트는 트래픽의 동적 라우팅을 위해 OSPF를 사용합니다. 각 VPN 피어의 터널 IP 주소는 정적으로 할당되며 두 사이트 간의 트래픽 라우팅을 위한 다음 홉 역할을 합니다.


©2023 Palo Alto Networks, Inc.




**STEP 1 |** 각 방화벽에서 레이어 3 인터페이스를 구성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택한 다음 VPN에 대해 구성할 인터페이스를 선택합니다.
2. 인터페이스 유형 목록에서 레이어**3**을 선택합니다.
3. 구성 탭에서 인터페이스가 속한 보안 영역을 선택합니다.
   - 인터페이스는 신뢰 네트워크 외부의 영역에서 액세스할 수 있어야 합니다. VPN 트래픽에 대한 가시성과 제어를 위해 전용 VPN 영역을 만드는 것이 좋습니다.
   - 영역을 아직 생성하지 않은 경우 보안 영역 목록에서 새 영역을 선택한 다음 새 영역의 이름을 정의한 다음 확인을 클릭합니다.
4. 사용할 가상 라우터를 선택합니다.
5. 인터페이스에 IP 주소를 할당하려면 **IPv4** 탭을 선택하고 IP 섹션에서 추가를 클릭한 다음 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 192.168.210.26/24).
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/7
   - 보안 영역 - 신뢰하지 않음
   - 가상 라우터 - 기본값
   - **IPv4** - 100.1.1.1/24

   VPN 피어 B의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/11
   - 보안 영역 - 신뢰하지 않음
   - 가상 라우터 - 기본값
   - **IPv4** - 200.1.1.1/24


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 터널 인터페이스를 생성하여 가상 라우터 및 보안 영역에 연결합니다.

1. 네트워크 > 인터페이스 > 터널을 선택하고 추가를 클릭합니다.
2. 인터페이스 이름 필드에 숫자 접미사(예: **.11**)를 지정합니다.
3. 구성 탭에서 보안 영역을 확장하여 다음과 같이 영역을 정의합니다.
   - 트러스트 영역을 터널의 종료 지점으로 사용하려면 영역을 선택합니다.
   - (권장) VPN 터널 종료를 위한 별도의 영역을 생성하려면 새 영역을 클릭합니다. 영역 대화 상자에서 새 영역의 이름(예: vpn-tun)을 정의한 다음 확인을 클릭합니다.
4. 가상 라우터를 선택합니다.
5. 터널 인터페이스에 IP 주소를 할당하고 **IPv4** 또는 **IPv6** 탭을 선택하고 IP 섹션에서 추가를 클릭하고 IP 주소와 네트워크 마스크/를 입력합니다. 인터페이스에 할당할 접두사(예: 172.19.9.2/24).

   이 IP 주소는 트래픽을 터널로 라우팅하는 다음 홉 IP 주소로 사용되며 터널 상태를 모니터링하는 데에도 사용할 수 있습니다.
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.
   - 인터페이스 - tunnel.41
   - **Security Zone** - vpn_tun
   - 가상 라우터 - 기본값
   - **IPv4** - 2.1.1.141/24

   VPN 피어 B의 구성은 다음과 같습니다.
   - 인터페이스 - tunnel.40
   - **Security Zone** - vpn_tun
   - 가상 라우터 - 기본값
   - **IPv4** - 2.1.1.140/24

**STEP 3 |** 암호화 프로파일을 설정합니다(1단계의 경우 IKE 암호화 프로파일 및 2단계의 경우 IPSec 암호화 프로파일).

두 피어 모두에서 이 작업을 완료하고 동일한 값을 설정해야 합니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 암호화를 선택합니다. 이 예제에서는 기본 프로파일을 사용합니다.
2. 네트워크 > 네트워크 프로파일 > **IPSec** 암호화를 선택합니다. 이 예제에서는 기본 프로파일을 사용합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 가상 라우터에서 OSPF 구성을 설정하고 방화벽의 적절한 인터페이스를 사용하여 OSPF 영역을 연결합니다.

방화벽에서 사용할 수 있는 OSPF 옵션에 대한 자세한 내용은 OSPF 구성을 참조하십시오.

라우팅 정보를 교환해야 하는 두 개 이상의 OSPF 라우터가 있는 경우 링크 유형으로 브로드캐스트를 사용합니다.

1. 네트워크 > 가상 라우터를 선택하고 기본 라우터를 선택하거나 새 라우터를 추가합니다.
2. **OSPF**(IPv4의 경우) 또는 **OSPFv3**(IPv6의 경우)를 선택하고 활성화를 선택합니다.
3. 이 예에서 VPN 피어 A에 대한 OSPF 구성은 다음과 같습니다.
   - 라우터 **ID**: 192.168.100.141
   - 지역 **ID**: 링크 유형이 p2p인 tunnel.1 인터페이스에 할당된 0.0.0.0
   - 지역 **ID**: 인터페이스 Ethernet1/1 및 링크 유형에 할당된 0.0.0.10: 브로드캐스트

   VPN 피어 B에 대한 OSPF 구성은 다음과 같습니다.
   - 라우터 **ID**: 192.168.100.140
   - 지역 **ID**: 링크 유형이 p2p인 tunnel.1 인터페이스에 할당된 0.0.0.0
   - 지역 **ID**: 인터페이스 Ethernet1/15 및 링크 유형에 할당된 0.0.0.20: 브로드캐스트

**STEP 5 |** IKE 게이트웨이를 설정합니다.

이 예에서는 두 VPN 피어 모두에 대해 고정 IP 주소를 사용합니다. 일반적으로 본사는 정적으로 구성된 IP 주소를 사용하며 지점은 동적 IP 주소일 수 있습니다. 동적 IP 주소는 VPN과 같은 안정적인 서비스를 구성하는 데 가장 적합하지 않습니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 게이트웨이를 선택합니다.
2. 추가를 클릭하고 일반 탭에서 옵션을 구성합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.
   - **Interface** - ethernet1/7
   - 로컬 **IP** 주소 - 100.1.1.1/24
   - 피어 **IP** 주소 - 200.1.1.1/24
   - 사전 공유 키 - 값 입력

   VPN 피어 B의 구성은 다음과 같습니다.
   - **Interface** - ethernet1/11
   - 로컬 **IP** 주소 - 200.1.1.1/24
   - 피어 **IP** 주소 - 100.1.1.1/24
   - 사전 공유 키 - 피어 A와 동일한 값 입력
3. IKE 1단계에 사용할 이전에 생성한 IKE 암호화 프로파일을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** IPSec 터널을 설정합니다.

1. 네트워크 > **IPSec** 터널을 선택합니다.
2. 추가를 클릭하고 일반 탭에서 옵션을 구성합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - 터널 인터페이스 - tunnel.41
   - 유형 - 자동 키
   - **IKE** 게이트웨이 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
   - **IPSec** 암호화 프로파일 - 위에서 정의한 IKE 게이트웨이를 선택합니다.

   VPN 피어 B의 구성은 다음과 같습니다.

   - 터널 인터페이스 - tunnel.40
   - 유형 - 자동 키
   - **IKE** 게이트웨이 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
   - **IPSec** 암호화 프로파일 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
3. 고급 옵션 표시를 선택하고 터널 모니터를 선택한 다음 연결 확인을 위해 ping할 대상 IP 주소를 지정합니다.
4. 연결 설정 실패 시 작업을 정의하려면 터널 모니터링 프로파일 정의를 참조하십시오.

**STEP 7 |** 사이트(서브넷) 간의 트래픽을 허용하는 정책을 생성합니다.

1. 정책 > 보안을 선택합니다.
2. 지정된 소스 및 대상 IP 주소에서 발생하는 트래픽에 대해 untrust 및 vpn-tun 영역과 vpn-tun 및 언트러스트 영역 간의 트래픽을 허용하는 규칙을 생성합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** CLI에서 OSPF 인접성과 경로를 확인합니다.

두 방화벽이 서로를 전체 상태의 이웃으로 볼 수 있는지 확인합니다. 또한 VPN 피어의 터널 인터페이스 IP 주소와 OSPF 라우터 ID를 확인합니다. 각 VPN 피어에서 다음 CLI 명령을 사용합니다.

- 라우팅 프로토콜 **ospf** 이웃 표시

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- 라우팅 경로 유형 **ospf** 표시

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface
2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
total routes shown: 3
```

 ©2023 Palo Alto Networks, Inc.

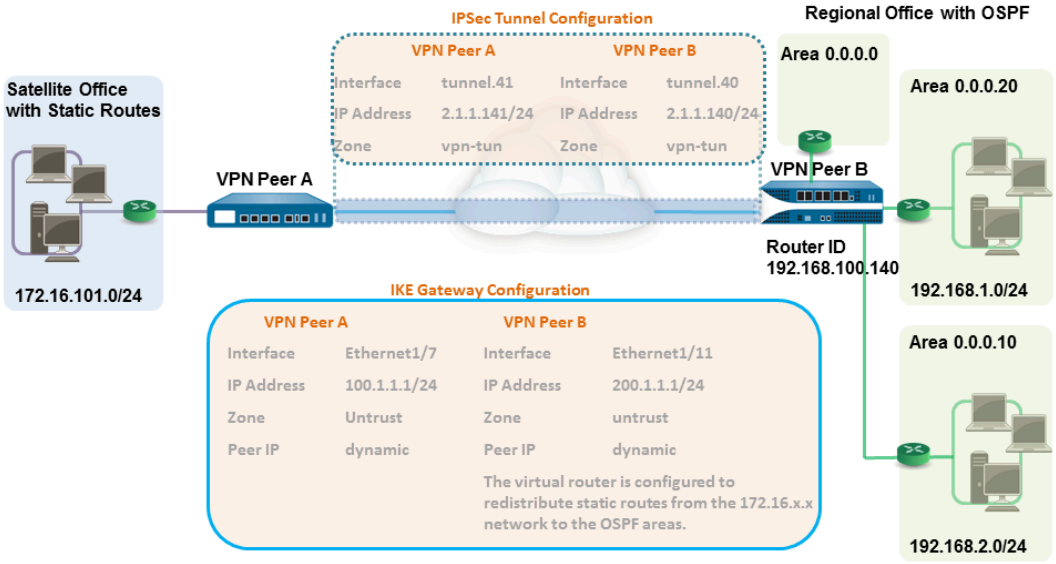
**STEP 9 |** VPN 연결 테스트.

터널 모니터링 설정 및 터널 상태 보기를 참조하십시오.

## 정적 및 동적 라우팅을 사용하는 사이트 간 VPN

이 예제에서는 한 사이트가 정적 경로를 사용하고 다른 사이트는 OSPF를 사용합니다. 라우팅 프로토콜이 위치 간에 동일하지 않은 경우 각 방화벽의 터널 인터페이스를 정적 IP 주소로 구성해야 합니다. 그런 다음 라우팅 정보를 교환하려면 정적 및 동적 라우팅 프로세스에 모두 참여하는 방화벽을 재배포 프로파일로 구성해야 합니다. 재배포 프로파일을 구성하면 가상 라우터가 정적 자율 시스템에서 OSPF 자율 시스템에 이르기까지 정적 경로, 연결된 경로 및 호스트와 같은 프로토콜 간에 경로를 재배포하고 필터링할 수 있습니다. 이 재배포 프로파일이 없으면 각 프로토콜은 자체적으로 작동하며 동일한 가상 라우터에서 실행되는 다른 프로토콜과 경로 정보를 교환하지 않습니다.

이 예제에서는 새틀라이트 사무실에 정적 경로가 있으며 192.168.x.x 네트워크로 향하는 모든 트래픽이 tunnel.41로 라우팅됩니다. VPN Peer B의 가상 라우터는 정적 라우팅 프로세스와 동적 라우팅 프로세스에 모두 참여하고 정적 경로를 OSPF 자율 시스템에 전파(내보내기)하기 위해 재분배 프로파일로 구성됩니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 각 방화벽에서 레이어 3 인터페이스를 구성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택한 다음 VPN에 대해 구성할 인터페이스를 선택합니다.
2. 인터페이스 유형에서 레이어 **3**을 선택합니다.
3. 구성 탭에서 인터페이스가 속한 보안 영역을 선택합니다.
   - 인터페이스는 신뢰 네트워크 외부의 영역에서 액세스할 수 있어야 합니다. VPN 트래픽에 대한 가시성과 제어를 위해 전용 VPN 영역을 만드는 것이 좋습니다.
   - 아직 영역을 만들지 않은 경우 보안**,** 영역에서새 영역을 선택한 다음 새 영역에 대한 이름을 정의한 다음 확인을 클릭합니다.
4. 사용할 가상 라우터를 선택합니다.
5. 인터페이스에 IP 주소를 할당하려면 **IPv4** 탭을 선택하고 IP 섹션에서 추가를 클릭한 다음 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 192.168.210.26/24).
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/7
   - 보안 영역 - 신뢰하지 않음
   - 가상 라우터 - 기본값
   - **IPv4** - 100.1.1.1/24

   VPN 피어 B의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/11
   - 보안 영역 - 신뢰하지 않음
   - 가상 라우터 - 기본값
   - **IPv4** - 200.1.1.1/24

**STEP 2 |** 암호화 프로파일을 설정합니다(1단계의 경우 IKE 암호화 프로파일 및 2단계의 경우 IPSec 암호화 프로파일).

두 피어 모두에서 이 작업을 완료하고 동일한 값을 설정해야 합니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 암호화를 선택합니다. 이 예제에서는 기본 프로파일을 사용합니다.
2. 네트워크 > 네트워크 프로파일 > **IPSec** 암호화를 선택합니다. 이 예제에서는 기본 프로파일을 사용합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** IKE 게이트웨이를 설정합니다.

IKE 단계-1 터널을 설정할 때 인증 조사를 추가하려면 미리 공유된 키를 사용하여 로컬 및 피어 식별 특성과 IKE 협상 프로세스에서 일치하는 해당 값을 설정할 수 있습니다.

1. 네트워크 > 네트워크 프로파일 > **IKE** 게이트웨이를 선택합니다.
2. 추가를 클릭하고 일반 탭에서 옵션을 구성합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/7
   - 로컬 **IP** 주소 - 100.1.1.1/24
   - 피어 **IP** 유형 - 동적
   - 사전 공유 키 - 값 입력
   - 로컬식별 - **FQDN(**호스트 이름**)**을 선택한 다음 VPN 피어 A의 값을 입력합니다.
   - 피어식별 - **FQDN(**호스트 이름**)**을 선택한 다음 VPN 피어 B의 값을 입력합니다.

   VPN 피어 B의 구성은 다음과 같습니다.

   - **Interface** - ethernet1/11
   - 로컬 **IP** 주소 - 200.1.1.1/24
   - 피어 **IP** 주소 - 동적
   - 사전 공유 키 - 피어 A와 동일한 값 입력
   - 로컬 식별 - **FQDN(**호스트 이름**)**을 선택한 다음 VPN 피어 B의 값을 입력합니다.
   - 피어 식별 - **FQDN(**호스트 이름**)**을 선택한 다음 VPN 피어 A의 값을 입력합니다.
3. IKE 1단계에 사용할 이전에 생성한 IKE 암호화 프로파일을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 터널 인터페이스를 생성하여 가상 라우터 및 보안 영역에 연결합니다.

1. 네트워크 > 인터페이스 > 터널을 선택하고 추가를 클릭합니다.
2. 인터페이스 이름 필드에 숫자 접미사(예: **.41**)를 지정합니다.
3. 구성 탭에서 보안 영역을 확장하여 다음과 같이 영역을 정의합니다.
   - 트러스트 영역을 터널의 종료 지점으로 사용하려면 영역을 선택합니다.
   - (권장) VPN 터널 종료를 위한 별도의 영역을 생성하려면 새 영역을 클릭합니다. 영역 대화 상자에서 새 영역에 대한 이름(예: ***vpn-tun***)을 정의한 다음 확인을 클릭합니다.
4. 가상 라우터를 선택합니다.
5. 터널 인터페이스에 IP 주소를 할당하고 **IPv4** 또는 **IPv6** 탭을 선택하고 IP 섹션에서 추가를 클릭하고 IP 주소와 네트워크 마스크/를 입력합니다. 인터페이스에 할당할 접두사(예: 172.19.9.2/24).

   이 IP 주소는 트래픽을 터널로 라우팅하고 터널 상태를 모니터링하는 데 사용됩니다.
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.
   - 인터페이스 - tunnel.41
   - **Security Zone** - vpn_tun
   - 가상 라우터 - 기본값
   - **IPv4** - 2.1.1.141/24

   VPN 피어 B의 구성은 다음과 같습니다.
   - 인터페이스 - 터널.42
   - **Security Zone** - vpn_tun
   - 가상 라우터 - 기본값
   - **IPv4** - 2.1.1.140/24

**STEP 5 |** 192.168.x.x 네트워크의 대상으로 트래픽을 라우팅하도록 인터페이스를 지정합니다.

1. VPN 피어 A에서 가상 라우터를 선택합니다.
2. 고정 경로를 선택하고 192.168.x.x 네트워크에서 대상으로 트래픽을 라우팅하기 위한 인터페이스로 **Add** tunnel.41을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** 가상 라우터에서 정적 경로와 OSPF 구성을 설정하고 방화벽에 적절한 인터페이스를 사용하여 OSPF 영역을 연결합니다.

1. VPN 피어 B에서 네트워크 > 가상 라우터를 선택하고 기본 라우터를 선택하거나 새 라우터를 추가합니다.
2. 고정 경로를 선택하고 172.168.x.x에서 트래픽의 다음 홉으로 터널 IP 주소를 추가합니다.

   원하는 경로 메트릭을 할당합니다. 값이 낮을수록 포운딩 테이블에서 경로 선택을 우선 순위가 높아집니다.
3. **OSPF**(IPv4의 경우) 또는 **OSPFv3**(IPv6의 경우)를 선택하고 활성화를 선택합니다.
4. 이 예제에서는 VPN 피어 B의 OSPF 구성은 다음과 같은 것입니다.
   - 라우터 ID: 192.168.100.140
   - 지역 ID: 0.0.0.0은 인터페이스 이더넷 1/12 링크 유형에 할당됩니다. 브로드캐스트
   - 지역 ID: 인터페이스 Ethernet1/1 및 링크 유형에 할당된 0.0.0.10: 브로드캐스트
   - 지역 ID: 0.0.0.20은 인터페이스 이더넷1/15 및 링크 유형에 할당됩니다. 브로드캐스트

**STEP 7 |** 재분배 프로파일을 만들어 정적 경로를 OSPF 자율 시스템에 삽입합니다.

1. VPN 피어 B에서 재배포 프로파일을 생성합니다.
   1. 네트워크 > 가상 라우터를 선택한 다음 위에서 사용한 라우터를 선택합니다.
   2. 재분배 프로파일을 선택한 다음 추가를 클릭합니다.
   3. 프로파일 이름을 입력하고 **Redist**를 선택한 다음 우선 순위 값을 할당합니다. 여러 프로파일을 구성한 경우 우선 순위가 가장 낮은 프로파일이 먼저 일치합니다.
   4. 소스 유형을 정적으로 설정하고 확인을 클릭합니다. 6단계에서 정의한 정적 경로는 재배포에 사용됩니다.
2. 정적 경로를 OSPF 시스템에 삽입합니다.
   1. **OSPF** > 내보내기 규칙(IPv4용) 또는 **OSPFv3** > 내보내기 규칙(IPv6용)을 선택합니다.
   2. 추가를 클릭하고 방금 만든 재배포 프로파일을 선택합니다.
   3. 외부 경로가 OSPF 시스템에 어떻게 유입되는지 선택합니다. 기본 옵션인 **Ext2**는 외부 메트릭만 사용하여 경로의 총 비용을 계산합니다. 내부 및 외부 OSPF 메트릭을 모두 사용하려면 **Ext1**을 사용합니다.
   4. OSPF 시스템에 주입된 경로에 대해 메트릭(비용 값)을 할당합니다. 이 옵션을 사용하면 OSPF 시스템에 들어오는 주입된 경로에 대한 메트릭을 변경할 수 있습니다.
   5. 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** IPSec 터널을 설정합니다.

1. 네트워크 > **IPSec** 터널을 선택합니다.
2. 추가를 클릭하고 일반 탭에서 옵션을 구성합니다.

   이 예에서 VPN 피어 A의 구성은 다음과 같습니다.

   - 터널 인터페이스 - tunnel.41
   - 유형 - 자동 키
   - **IKE** 게이트웨이 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
   - **IPSec** 암호화 프로파일 - 위에서 정의한 IKE 게이트웨이를 선택합니다.

   VPN 피어 B의 구성은 다음과 같습니다.

   - 터널 인터페이스 - tunnel.40
   - 유형 - 자동 키
   - **IKE** 게이트웨이 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
   - **IPSec** 암호화 프로파일 - 위에서 정의한 IKE 게이트웨이를 선택합니다.
3. 고급 옵션 표시를 선택하고 터널 모니터를 선택한 다음 연결 확인을 위해 ping할 대상 IP 주소를 지정합니다.
4. 연결 설정 실패 시 작업을 정의하려면 터널 모니터링 프로파일 정의를 참조하십시오.

**STEP 9 |** 사이트(서브넷) 간의 트래픽을 허용하는 정책을 생성합니다.

1. 정책 > 보안을 선택합니다.
2. 지정된 소스 및 대상 IP 주소에서 발생하는 트래픽에 대해 untrust 및 vpn-tun 영역과 vpn-tun 및 언트러스트 영역 간의 트래픽을 허용하는 규칙을 생성합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 10 |** CLI에서 OSPF 인접성과 경로를 확인합니다.

두 방화벽이 서로를 전체 상태의 이웃으로 볼 수 있는지 확인합니다. 또한 VPN 피어의 터널 인터페이스 IP 주소와 OSPF 라우터 ID를 확인합니다. 각 VPN 피어에서 다음 CLI 명령을 사용합니다.

- 라우팅 프로토콜 **ospf** 이웃 표시

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

다음은 각 VPN 피어의 출력의 예입니다.

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

**STEP 11 |** VPN 연결 테스트.

터널 모니터링 설정 및 터널 상태 보기를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

# 대규모 VPN(LSVPN)

Palo Alto Networks 차세대 방화벽의 GlobalProtect 대규모 VPN(LSVPN) 기능은 기존 허브 및 스포크 VPN의 배포를 간소화하여 원격 위성에 필요한 최소한의 구성으로 여러 지사를 통해 엔터프라이즈 네트워크를 신속하게 배포할 수 있습니다. 이 솔루션은 방화벽 인증 및 IPSec용 인증서를 사용하여 데이터를 보호합니다.

LSVPN을 사용하면 Palo Alto Networks 방화벽 간에 사이트 간 VPN을 사용할 수 있습니다. Palo Alto Networks 방화벽과 다른 디바이스 간에 사이트 간 VPN을 설정하려면 VPN을 참조하십시오.

다음 항목에서는 LSVPN 구성 요소와 Palo Alto Networks 방화벽 간의 사이트 간 VPN 서비스를 사용하도록 설정하는 방법에 대해 설명합니다.

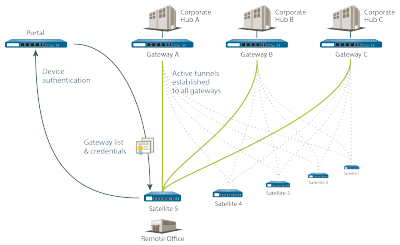

- LSVPN 개요
- LSVPN용 인터페이스 및 영역 생성
- GlobalProtect LSVPN 구성 요소 간에 SSL 활성화
- 위성 인증을 위해 포털 구성
- LSVPN을 위한 글로벌 보호 게이트웨이 구성
- LSVPN을 위한 글로벌 보호 포털 구성
- LSVPN에 가입할 위성 준비
- LSVPN 구성 확인
- LSVPN 빠른 구성

# LSVPN 개요

GlobalProtect는 원격 사이트에서 기업 리소스에 대한 보안 액세스를 관리하기 위한 완벽한 인프라를 제공합니다. 이 인프라에는 다음 구성 요소가 포함됩니다.

- **GlobalProtect** 포털 - GlobalProtect LSVPN 인프라에 대한 관리 기능을 제공합니다. GlobalProtect LSVPN에 참여하는 모든 위성은 위성(스포크)이 게이트웨이(허브)에 연결할 수 있도록 하는 구성 정보를 포함하여 포털에서 구성 정보를 수신합니다. 모든 Palo Alto Networks 차세대 방화벽의 인터페이스에서 포털을 구성합니다.
- **GlobalProtect** 게이트웨이 - 위성 연결을 위한 터널 엔드포인트를 제공하는 Palo Alto Networks 방화벽입니다. 위성이 액세스하는 리소스는 게이트웨이의 보안 정책에 의해 보호됩니다. 별도의 포털과 게이트웨이가 필요하지 않습니다. 단일 방화벽은 포털과 게이트웨이로 모두 작동할 수 있습니다.
- **GlobalProtect** 위성 - 중앙 리소스에 대한 보안 액세스를 위해 회사 사무실의 게이트웨이와 IPSec 터널을 설정하는 원격 사이트의 Palo Alto Networks 방화벽입니다. 위성 방화벽의 구성이 최소화되어 새 사이트를 추가할 때 VPN을 빠르고 쉽게 확장할 수 있습니다.

다음 다이어그램은 GlobalProtect LSVPN 구성 요소가 함께 작동하는 방식을 보여줍니다.




 ©2023 Palo Alto Networks, Inc.

# LSVPN용 인터페이스 및 영역 생성

LSVPN 인프라에 대해 다음 인터페이스 및 영역을 구성해야 합니다.

- **GlobalProtect** 포털 - GlobalProtect 위성이 연결할 레이어 3 인터페이스가 필요합니다. 포털과 게이트웨이가 동일한 방화벽에 있는 경우 동일한 인터페이스를 사용할 수 있습니다. 포털은 지점에서 액세스할 수 있는 영역에 있어야 합니다.
- **GlobalProtect** 게이트웨이 - 원격 위성이 도달할 수 있는 영역의 레이어 3 인터페이스, 보호된 리소스에 연결하는 트러스트 영역의 내부 인터페이스, 위성에서 VPN 터널을 종료하기 위한 논리적 터널 인터페이스의 세 가지 인터페이스가 필요합니다. 다른 사이트 간 VPN 솔루션과 달리 GlobalProtect 게이트웨이는 단일 터널 인터페이스만 필요하며 모든 원격 위성(지점 간)과의 터널 연결에 사용됩니다. 동적 라우팅을 사용하려는 경우 터널 인터페이스에 IP 주소를 할당해야 합니다. GlobalProtect는 터널 인터페이스에 대해 IPv6 및 IPv4 주소 지정을 모두 지원합니다.
- **GlobalProtect** 위성 - 원격 게이트웨이(최대 25개 게이트웨이)와 VPN을 설정하기 위해 단일 터널 인터페이스가 필요합니다. 동적 라우팅을 사용하려는 경우 터널 인터페이스에 IP 주소를 할당해야 합니다. GlobalProtect는 터널 인터페이스에 대해 IPv6 및 IPv4 주소 지정을 모두 지원합니다.

포털, 게이트웨이 및 위성에 대한 자세한 내용은 LSVPN 개요를 참조하십시오.

**STEP 1 |** 레이어 3 인터페이스를 구성합니다.

포털, 각 게이트웨이 및 위성에는 모두 사이트 간에 트래픽을 라우팅할 수 있도록 하는 레이어 3 인터페이스가 필요합니다.

게이트웨이와 포털이 동일한 방화벽에 있는 경우 두 구성 요소에 대해 단일 인터페이스를 사용할 수 있습니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택한 다음 GlobalProtect LSVPN에 대해 구성할 인터페이스를 선택합니다.
2. 인터페이스 유형 드롭다운에서 **Layer3**을 선택합니다.
3. 구성 탭에서 인터페이스가 속한 보안 영역을 선택합니다.
   - 인터페이스는 신뢰 네트워크 외부의 영역에서 액세스할 수 있어야 합니다. VPN 트래픽에 대한 가시성과 제어를 위해 전용 VPN 영역을 만드는 것이 좋습니다.
   - 영역을 아직 생성하지 않은 경우 보안 영역 드롭다운에서 새 영역을 선택한 다음 새 영역의 이름을 정의한 다음 확인을 클릭합니다.
4. 사용할 가상 라우터를 선택합니다.
5. 인터페이스에 IP 주소 할당:
   - IPv4 주소의 경우 **IPv4**를 선택한 다음 인터페이스에 할당할 IP 주소 및 네트워크 마스크 추가(예: 203.0.11.100/24)를 선택합니다.
   - IPv6 주소의 경우 **IPv6**, 인터페이스에서 **IPv6** 활성화를 선택하고 인터페이스에 할당할 IP 주소 및 네트워크 마스크를 추가합니다(예: 2001:1890:12f2:11::10.1.8.160/80).
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** GlobalProtect 게이트웨이를 호스팅하는 방화벽에서 GlobalProtect 위성에 의해 설정된 VPN 터널을 종료할 로지컬 터널 인터페이스를 구성합니다.

동적 라우팅을 사용하려는 경우가 아니면 터널 인터페이스에 ***IP*** 주소가 필요하지 않습니다. 그러나 터널 인터페이스에 ***IP*** 주소를 할당하면 연결 문제를 해결하는 데 유용할 수 있습니다.

***VPN*** 터널이 종료되는 영역에서 사용자 ***ID***를 활성화해야 합니다.

1. 네트워크 > 인터페이스 > 터널을 선택하고 추가를 클릭합니다.
2. 인터페이스 이름 필드에 숫자 접미사(예: **.2**)를 지정합니다.
3. 구성 탭에서 보안 영역 드롭다운을 확장하여 다음과 같이 영역을 정의합니다.
   - 트러스트 영역을 터널의 종료 지점으로 사용하려면 드롭다운에서 영역을 선택합니다.
   - (권장) VPN 터널 종료를 위한 별도의 영역을 생성하려면 새 영역을 클릭합니다. 영역 대화 상자에서 새 영역의 이름(예: ***lsvpn-tun***)을 정의하고 사용자 식별 사용 체크박스를 선택한 다음 확인을 클릭합니다.
4. 가상 라우터를 선택합니다.
5. (선택 사항) 터널 인터페이스에 IP 주소를 할당하려면:
   - IPv4 주소의 경우 **IPv4**를 선택한 다음 인터페이스에 할당할 IP 주소 및 네트워크 마스크 추가(예: 203.0.11.100/24)를 선택합니다.
   - IPv6 주소의 경우 **IPv6**, 인터페이스에서 **IPv6** 활성화를 선택하고 인터페이스에 할당할 IP 주소 및 네트워크 마스크를 추가합니다(예: 2001:1890:12f2:11::10.1.8.160/80).
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

**STEP 3 |** VPN 연결의 터널 종료를 위한 별도의 영역을 생성한 경우 VPN 영역과 트러스트 영역 간의 트래픽 플로우를 활성화하는 보안 정책을 생성합니다.

예를 들어 정책 규칙은 ***lsvpn-tun*** 영역과 ***L3-Trust*** 영역 간의 트래픽을 활성화합니다.

**STEP 4 |** 변경 사항을 커밋합니다.

커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# GlobalProtect LSVPN 구성 요소 간에 SSL 활성화

GlobalProtect 구성 요소 간의 모든 상호 작용은 SSL/TLS 연결을 통해 발생합니다. 따라서 각 구성 요소에 대한 구성에서 적절한 인증서 및/또는 인증서 프로파일을 참조할 수 있도록 각 구성 요소를 구성하기 전에 필요한 인증서를 생성 및/또는 설치해야 합니다. 다음 섹션에서는 지원되는 인증서 배포 방법, 다양한 GlobalProtect 인증서에 대한 설명 및 모범 사례 지침에 대해 설명하고 필요한 인증서를 생성 및 배포하기 위한 지침을 제공합니다.

- 인증서 배포 에 대해
- GlobalProtect LSVPN 구성 요소에 서버 인증서 배포
- SCEP를 사용하여 GlobalProtect Satellite에 클라이언트 인증서 배포

## 인증서 배포 에 대해

GlobalProtect LSVPN용 인증서를 배포하는 데에는 두 가지 기본 접근 방식이 있습니다.

- 엔터프라이즈 인증 기관 - 이미 자체 엔터프라이즈 인증 기관이 있는 경우 이 내부 CA를 사용하여 GlobalProtect 포털에 대한 중간 CA 인증서를 발급하여 GlobalProtect 게이트웨이 및 위성에 인증서를 발급할 수 있습니다. 또한 클라이언트 인증서를 GlobalProtect 위성에 발급하는 SCEP(단순 인증서 등록 프로토콜) 클라이언트 역할을 하도록 GlobalProtect 포털을 구성할 수도 있습니다.
- 자체 서명된 인증서 - 방화벽에서 자체 서명된 루트 CA 인증서를 생성하여 포털, 게이트웨이 및 위성에 대한 서버 인증서를 발급하는 데 사용할 수 있습니다. 자체 서명된 루트 CA 인증서를 사용하는 경우 포털에서 자체 서명된 루트 CA 인증서를 생성하고 이를 사용하여 게이트웨이 및 위성에 대한 서버 인증서를 발급하는 것이 좋습니다. 이렇게 하면 인증서 서명에 사용되는 개인 키가 포털에 유지됩니다.

## GlobalProtect LSVPN 구성 요소에 서버 인증서 배포

GlobalProtect LSVPN 구성 요소는 SSL/TLS를 사용하여 상호 인증합니다. LSVPN을 배포하기 전에 각 포털 및 게이트웨이에 SSL/TLS 서비스 프로파일을 할당해야 합니다. 프로파일은 위성과의 통신을 위해 서버 인증서와 허용되는 TLS 버전을 지정합니다. 포털은 위성 등록 프로세스의 일부로 첫 번째 연결 중에 각 위성에 대한 서버 인증서를 발급하므로 위성에 대한 SSL/TLS 서비스 프로파일을 생성할 필요가 없습니다.

또한 게이트웨이 또는 위성으로 호스팅할 각 방화벽에 서버 인증서를 발급하는 데 사용되는 루트 CA(인증 기관) 인증서를 가져와야 합니다. 마지막으로 LSVPN에 참여하는 각 게이트웨이 및 위성에서 상호 인증을 사용하여 SSL/TLS 연결을 설정할 수 있도록 하는 인증서 프로파일을 구성해야 합니다.

다음 워크플로는 SSL 인증서를 GlobalProtect LSVPN 구성 요소에 배포하기 위한 모범 사례 단계를 보여줍니다.

**STEP 1 |** GlobalProtect 포털을 호스팅하는 방화벽에서 GlobalProtect 구성 요소의 인증서에 서명하기 위한 루트 CA 인증서를 생성합니다.

자체 서명된 루트 CA 인증서 생성:

1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 생성을 클릭합니다.
2. **LSVPN_CA**와 같은 인증서 이름을 입력합니다.
3. 서명자 필드에서 값을 선택하지 마십시오(자체 서명되었음을 나타냄).
4. 인증 기관 체크박스를 선택한 다음 확인을 클릭하여 인증서를 생성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** GlobalProtect 포털 및 게이트웨이에 대한 SSL/TLS 서비스 프로파일을 생성합니다.

포털 및 각 게이트웨이에 대해 고유한 자체 서명된 서버 인증서를 참조하는 SSL/TLS 서비스 프로파일을 할당해야 합니다.



가장 좋은 방법은 포털에서 필요한 모든 인증서를 발급하여 서명 인증서(개인 키 포함)를 내보낼 필요가 없도록 하는 것입니다.



*GlobalProtect* 포털과 게이트웨이가 동일한 방화벽 인터페이스에 있는 경우 두 구성 요소에 대해 동일한 서버 인증서를 사용할 수 있습니다.

1. 포털의 루트 CA를 사용하여 배포할 각 게이트웨이에 대한 인증서를 생성합니다.
   1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 생성을 클릭합니다.
   2. 인증서 이름을 입력합니다.
   3. 공통 이름 필드에 게이트웨이를 구성할 인터페이스의 FQDN(권장) 또는 IP 주소를 입력합니다.
   4. 서명 필드에서 방금 생성한 **LSVPN_CA** 인증서를 선택합니다.
   5. 인증서 속성 섹션에서 추가를 클릭하고 게이트웨이를 고유하게 식별하는 속성을 정의하십시오. 호스트 이름 속성(인증서의 SAN 필드를 채움)을 추가하는 경우 일반 이름에 대해 정의한 값과 정확히 일치해야 합니다.
   6. 인증서를 생성합니다.
2. 포털 및 각 게이트웨이에 대한 SSL/TLS 서비스 프로파일을 구성합니다.
   1. 디바이스 > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택한 다음 추가를 클릭합니다.
   2. 프로파일을 식별할 이름을 입력하고 포털 또는 게이트웨이에 대해 방금 생성한 서버 인증서를 선택합니다.
   3. 위성과 통신할 수 있는 TLS 버전 범위(최소 버전에서 최대 버전까지)를 정의하고 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 자체 서명된 서버 인증서를 게이트웨이에 배포합니다.



모범 사례**:**

- 포털에서 루트 CA에서 발급한 자체 서명된 서버 인증서를 내보내고 게이트웨이로 가져옵니다.
- 각 게이트웨이에 대해 고유한 서버 인증서를 발급해야 합니다.
- CN(일반 이름) 및 해당하는 경우 인증서의 SAN(주체 대체 이름) 필드는 게이트웨이를 구성하는 인터페이스의 IP 주소 또는 FQDN(정규화된 도메인 이름)과 일치해야 합니다.

1. 포털에서 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 배포할 게이트웨이 인증서를 선택한 다음 내보내기를 클릭합니다.
2. 파일 형식 드롭다운에서 암호화된 개인 키 및 인증서**(PKCS12)**를 선택합니다.
3. 인증서와 연결된 개인 키를 암호화하는 암호를 입력(및 다시 입력)한 다음 확인을 클릭하여 PKCS12 파일을 컴퓨터에 다운로드합니다.
4. 게이트웨이에서 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 가져오기를 클릭합니다.
5. 인증서 이름을 입력합니다.
6. 포털에서 방금 다운로드한 인증서 파일의 경로와 이름을 입력하거나 찾아보기를 통해 파일을 찾습니다.
7. 파일 형식으로 암호화된 개인 키 및 인증서**(PKCS12)**를 선택합니다.
8. 키 파일 필드에 PKCS12 파일의 경로와 이름을 입력하거나 찾아보기를 사용하여 파일을 찾습니다.
9. 포털에서 개인 키를 내보낼 때 암호화하는 데 사용한 암호를 입력하고 다시 입력한 다음 확인을 클릭하여 인증서와 키를 가져옵니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** LSVPN 구성 요소에 대한 서버 인증서를 발급하는 데 사용되는 루트 CA 인증서를 가져옵니다.

루트 CA 인증서를 모든 게이트웨이 및 위성으로 가져와야 합니다. 보안상의 이유로 연결된 개인 키가 아닌 인증서만 내보내야 합니다.

1. 포털에서 루트 CA 인증서를 다운로드합니다.
   1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.
   2. LSVPN 구성 요소에 대한 인증서를 발급하는 데 사용되는 루트 CA 인증서를 선택한 다음 내보내기를 클릭합니다.
   3. 파일 형식 드롭다운에서 **Base64** 인코딩된 인증서**(PEM)**를 선택한 다음 확인을 클릭하여 인증서를 다운로드합니다. (프라이빗 키를 내보내지 마십시오.)
2. 게이트웨이 및 위성을 호스팅하는 방화벽에서 루트 CA 인증서를 가져옵니다.
   1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 가져오기를 클릭합니다.
   2. 인증서를 클라이언트 CA 인증서로 식별하는 인증서 이름을 입력합니다.
   3. CA에서 다운로드한 인증서 파일을 찾습니다.
   4. 파일 형식으로 **Base64** 인코딩된 인증서**(PEM)**를 선택한 다음 확인을 클릭합니다.
   5. 디바이스 인증서 탭에서 방금 불러온 인증서를 선택하여 엽니다.
   6. 신뢰할 수 있는 루트 **CA**를 선택한 다음 확인을 클릭합니다.
   7. 변경 사항을 커밋합니다.

**STEP 5 |** 인증서 프로파일을 생성합니다.

GlobalProtect LSVPN 포털 및 각 게이트웨이에는 위성을 인증하는 데 사용할 인증서를 지정하는 인증서 프로파일이 필요합니다.

1. 디바이스 > 인증서 관리 > 인증서 프로파일을 선택한 다음 추가를 클릭하고 프로파일 이름을 입력합니다.
2. 사용자 이름 필드가 없음으로 설정되어 있는지 확인하십시오.
3. **CA** 인증서 필드에서 추가를 클릭하고 이전 단계에서 불러온 신뢰할 수 있는 루트 CA 인증서를 선택합니다.
4. (권장) CRL 및/또는 OCSP를 사용하여 인증서 상태 확인을 사용하도록 설정합니다.
5. 확인을 클릭하여 프로파일을 저장합니다.

**STEP 6 |** 변경 사항을 커밋합니다.

커밋을 클릭합니다.

## SCEP를 사용하여 GlobalProtect Satellite에 클라이언트 인증서 배포

클라이언트 인증서를 위성에 배포하는 다른 방법으로 GlobalProtect 포털이 엔터프라이즈 PKI의 SCEP 서버에 대한 SCEP(Simple Certificate Enrollment Protocol) 클라이언트 역할을 하도록 구성할 수 있습니다. SCEP 작업은 포털이 요청할 때 엔터프라이즈 PKI가 인증서를 생성하고 인증서를 포털로 보내는 점에서 동적입니다.

위성 디바이스가 포털 또는 게이트웨이에 대한 연결을 요청할 때 연결 요청과 함께 일련번호도 포함됩니다. 포털은 SCEP 프로파일의 설정을 사용하여 SCEP 서버에 CSR을 제출하고 클라이언트 인증서 제목에

 ©2023 Palo Alto Networks, Inc.

디바이스의 일련번호를 자동으로 포함합니다. 엔터프라이즈 PKI에서 클라이언트 인증서를 수신한 후 포털은 클라이언트 인증서를 위성 디바이스에 투명하게 배포합니다. 그런 다음 위성 디바이스는 인증을 위해 포털 또는 게이트웨이에 클라이언트 인증서를 제공합니다.

**STEP 1 |** SCEP 프로파일을 생성합니다.

1. 디바이스 > 인증서 관리 > **SCEP**를 선택한 다음 새 프로파일을 추가합니다.
2. 이름을 입력하여 SCEP 프로파일을 식별합니다.
3. 이 프로파일이 여러 가상 시스템 기능을 갖춘 방화벽용인 경우 가상 시스템 또는 공유를 프로파일을 사용할 수 있는 위치로 선택합니다.

**STEP 2 |** (선택 사항) SCEP 기반 인증서 생성을 보다 안전하게 만들려면 각 인증서 요청에 대해 PKI와 포털 간에 SCEP 챌린지-응답 메커니즘을 구성합니다.

이 메커니즘을 구성한 후에는 해당 작업이 보이지 않으며 사용자의 추가 입력이 필요하지 않습니다.

미국 표준 준수 FIPS(연방 정보 처리 표준), 동적 SCEP 챌린지를 사용하고 HTTPS를 사용하는 서버 **URL**을 지정합니다(7단계 참조).

다음 옵션 중 하나를 선택합니다.

- 없음 - (기본값) SCEP 서버는 인증서를 발급하기 전에 포털에 시도하지 않습니다.
- 수정됨 - PKI 인프라의 SCEP 서버에서 등록 시도 암호(예: **http://10.200.101.1/CertSrv/mscep_admin/**)를 얻은 다음 암호 필드에 암호를 복사하거나 입력합니다.
- 동적 - 포털 클라이언트가 이러한 자격 증명을 제출하는 SCEP 서버 **URL**(예: **http://10.200.101.1/CertSrv/mscep_admin/)**과 선택한 사용자 이름 및 OTP를 입력합니다. 사용자 이름과 암호는 PKI 관리자의 자격 증명일 수 있습니다.

**STEP 3 |** 포털이 클라이언트 인증서를 요청하고 받을 수 있도록 SCEP 서버와 포털 간의 연결 설정을 지정합니다.

위성을 식별하기 위해 포털은 SCEP 서버에 대한 CSR 요청에 디바이스 일련번호를 자동으로 포함합니다. SCEP 프로파일에는 제목 필드에 값이 필요하므로 LSVPN에 대한 클라이언트 인증서에서 값이 사용되지 않더라도 기본 **$USERNAME** 토큰을 그대로 둘 수 있습니다.

1. 포털이 PKI의 SCEP 서버에 연결하는 데 사용하는 서버 **URL**을 구성합니다(예: **http://10.200.101.1/certsrv/mscep/**).
2. **CA-IDENT** 이름 필드에 문자열(최대 255자)을 입력하여 SCEP 서버를 식별합니다.
3. 제목 대체 이름 유형을 선택합니다.
   - **RFC 822**이름—인증서의 제목 또는 제목 대체 이름 확장에 이메일 이름을 입력합니다.
   - **DNS** 이름—인증서를 평가하는 데 사용되는 DNS 이름을 입력합니다.
   - 균일한 리소스 식별자—클라이언트가 인증서를 가져오는 리소스의 이름을 입력합니다.
   - 없음—인증서에 대한 속성을 지정하지 마십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** (선택 사항) 인증서에 대한 암호화 설정을 구성합니다.

- 인증서의 키 길이(비트수)를 선택합니다. 방화벽이 FIPS-CC 모드이고 키 생성 알고리즘이 RSA인 경우. RSA 키는 2048비트 이상이어야 합니다.
- CSR(인증서 서명 요청)에 대한 다이제스트 알고리즘을 나타내는 **CSR**용 다이제스트를 선택합니다. SHA1, SHA256, SHA384 또는 SHA512.

**STEP 5 |** (선택 사항) 서명 또는 암호화에 대해 인증서의 허용된 사용을 구성합니다.

- 이 인증서를 서명에 사용하려면 디지털 서명 체크박스로 사용하십시오. 이렇게 하면 엔드포인트이 인증서의 개인 키를 사용하여 디지털 서명의 유효성을 검사할 수 있습니다.
- 이 인증서를 암호화에 사용하려면 키 암호화 체크박스 사용을 선택합니다. 이렇게 하면 클라이언트가 인증서의 개인 키를 사용하여 SCEP 서버에서 발급한 인증서와 함께 설정된 HTTPS 연결을 통해 교환된 데이터를 암호화할 수 있습니다.

**STEP 6 |** (선택 사항) 포털이 올바른 SCEP 서버에 연결되어 있는지 확인하려면 **CA** 인증서 지문을 입력합니다. 지문 필드의 SCEP 서버 인터페이스에서 이 지문을 가져옵니다.

1. SCEP 서버의 관리 UI에 대한 URL을 입력합니다(예 **: http://<hostname or IP>/CertSrv/mscep_admin/**).
2. 지문을 복사하여 **CA** 인증서 지문 필드에 입력합니다.

**STEP 7 |** SCEP 서버와 GlobalProtect 포털 간에 상호 SSL 인증을 사용하도록 설정합니다. 미국 규정을 준수해야 합니다. 연방 정보 처리 표준(FIPS).

*FIPS-CC* 작업은 방화벽 로그인 페이지와 상태 표시줄에 표시됩니다.

SCEP 서버의 루트 **CA** 인증서를 선택합니다. 선택적으로 클라이언트 인증서를 선택하여 SCEP 서버와 GlobalProtect 포털 간에 상호 SSL 인증을 활성화할 수 있습니다.

**STEP 8 |** 구성을 저장하고 커밋합니다.

1. 설정을 저장하고 SCEP 구성을 닫도록 확인을 클릭합니다.
2. 구성을 커밋합니다.

포털은 SCEP 프로파일의 설정을 사용하여 CA 인증서를 요청하려고 시도하고 포털을 호스팅하는 방화벽에 저장합니다. 성공하면 CA 인증서가 디바이스 > 인증서 관리 > 인증서에 표시됩니다.

**STEP 9 |** (선택 사항) SCEP 프로파일을 저장한 후 포털에서 인증서를 얻지 못하면 포털에서 수동형으로 인증서 서명 요청(CSR)을 생성할 수 있습니다.

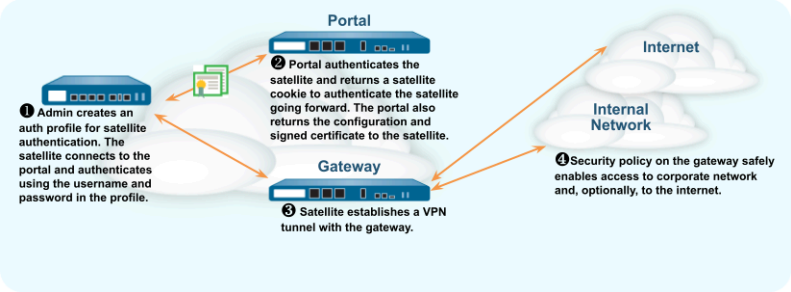
1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 생성을 클릭합니다.
2. 인증서 이름을 입력합니다. 이 이름은 공백을 포함할 수 없습니다.
3. 회사 PKI에 CSR을 제출하는 데 사용할 **SCEP** 프로파일을 선택합니다.
4. 확인을 클릭하여 요청을 제출하고 인증서를 생성합니다.


©2023 Palo Alto Networks, Inc.

# 위성 인증을 위해 포털 구성

LSVPN에 등록하려면 각 위성이 포털과 SSL/TLS 연결을 설정해야 합니다. 연결을 설정한 후 포털은 LSVPN에 가입할 권한이 있는지 확인하기 위해 위성을 인증합니다. 위성을 성공적으로 인증한 후 포털은 위성에 대한 서버 인증서를 발급하고 위성이 연결할 수 있는 게이트웨이와 게이트웨이와의 SSL 연결을 설정하는 데 필요한 루트 CA 인증서를 지정하는 LSVPN 구성을 푸시합니다.

위성이 초기 연결 중에 포털에 인증하려면 포털 LSVPN 구성에 대한 인증 프로파일을 생성해야 합니다. 위성 관리자는 첫 번째 연결을 설정하기 위해 포털에 대한 위성을 수동으로 인증해야 합니다. 인증에 성공하면 포털은 후속 연결에서 위성을 인증하기 위해 위성 쿠키를 반환합니다. 포털에서 발행하는 위성 쿠키의 수명은 180일입니다. 쿠키가 만료되면 위성 관리자는 수동으로 다시 인증해야 합니다. 이때 포털은 새 쿠키를 발행합니다.




다음 워크플로는 기존 인증 서비스에 대해 위성을 인증하도록 포털을 설정하는 방법을 설명합니다. 포털에 대한 위성 인증을 위해 GlobalProtect LSVPN은 로컬 데이터베이스 인증만 지원합니다.

**STEP 1 |** 위성 관리자가 포털에 대해 위성을 인증할 수 있도록 로컬 데이터베이스 인증을 설정하십시오.

1. 디바이스 > 로컬 사용자 데이터베이스 > 사용자를 선택하고 사용자 계정을 로컬 데이터베이스에 추가합니다.
2. 로컬 데이터베이스에 사용자 계정을 추가합니다.

**STEP 2 |** 인증 프로파일을 구성합니다.

1. 디바이스 > 인증 프로파일 > 추가를 선택합니다.
2. 프로파일의 이름을 입력한 다음 유형을 로컬 데이터베이스로 설정합니다.
3. 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 3 |** 위성을 인증합니다.

위성을 포털에 인증하려면 위성 관리자가 로컬 데이터베이스에 구성된 사용자 이름과 암호를 제공해야 합니다.

1. 네트워크 > **IPSec** 터널을 선택하고 LSVPN에 대해 생성한 터널 구성의 상태 열에서 게이트웨이 정보 링크를 클릭합니다.
2. 포털 상태 필드에서 자격 증명 입력 링크를 클릭하고 포털에 위성을 인증하는 데 필요한 사용자 이름과 암호를 클릭합니다.

   포털이 처음으로 포털에 대해 성공적으로 인증한 후 포털은 후속 세션에서 위성을 인증하는 데 사용하는 위성 쿠키를 생성합니다.


©2023 Palo Alto Networks, Inc.

# LSVPN을 위한 글로벌 보호 게이트웨이 구성

포털이 위성에 포워딩하는 GlobalProtect 구성에는 위성이 연결할 수 있는 게이트웨이 목록이 포함되어 있으므로 포털을 구성하기 전에 게이트웨이를 구성하는 것이 좋습니다.

GlobalProtect 게이트웨이를 구성하기 전에 다음 작업을 완료해야 합니다.

- 각 게이트웨이를 구성할 인터페이스에서 LSVPN용 인터페이스 및 영역 생성. 물리적 인터페이스와 가상 터널 인터페이스를 모두 구성해야 합니다.
- GlobalProtect LSVPN 구성 요소 간에 SSL 활성화 GlobalProtect 위성에서 게이트웨이로 상호 SSL/TLS 연결을 설정하는 데 필요한 게이트웨이 서버 인증서, SSL/TLS 서비스 프로파일 및 인증서 프로파일을 구성합니다.

다음과 같이 LSVPN에 참여하도록 각 GlobalProtect 게이트웨이를 구성합니다.

**STEP 1 |** 게이트웨이를 추가합니다.

1. 네트워크 > **GlobalProtect** > 게이트웨이를 선택한 다음 추가를 클릭합니다.
2. 일반 화면에서 게이트웨이의 이름을 입력합니다. 게이트웨이 이름에는 공백이 없어야 하며 사용자와 관리자가 게이트웨이를 식별하는 데 도움이 되도록 위치 또는 기타 설명 정보를 포함하는 것이 가장 좋습니다.
3. (선택 사항) 위치 필드에서 이 게이트웨이가 속한 가상 시스템을 선택합니다.

**STEP 2 |** 위성 디바이스가 게이트웨이에 연결할 수 있도록 하는 네트워크 정보를 지정합니다.

게이트웨이에 대한 네트워크 인터페이스를 생성하지 않은 경우 지침은 LSVPN용 인터페이스 및 영역 생성을(를) 참조하십시오.

1. 게이트웨이에 대한 인그레스 액세스에 위성이 사용할 인터페이스를 선택합니다.
2. 게이트웨이 액세스를 위한 **IP** 주소 유형 및 **IP** 주소를 지정합니다.
   - IP 주소 유형은 **IPv4**(전용), **IPv6**(전용) 또는 **IPv4** 및 **IPv6**일 수 있습니다. 네트워크가 IPv4 및 IPv6이 동시에 실행되는 이중 스택 구성을 지원하는 경우 **IPv4** 및 **IPv6**을 사용하십시오.
   - IP 주소는 IP 주소 유형과 호환되어야 합니다. 예를 들어 IPv4 주소의 경우 **172.16.1/0**, IPv6 주소의 경우 **21DA:D3:0:2F3B**입니다. 이중 스택 구성의 경우 IPv4 및 IPv6 주소를 모두 입력합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 게이트웨이가 터널 설정을 시도하는 위성을 인증하는 방법을 지정합니다. 게이트웨이에 대한 SSL/TLS 서비스 프로파일을 아직 생성하지 않은 경우 GlobalProtect LSVPN 구성 요소에 서버 인증서 배포을(를) 참조하십시오.

인증 프로파일 또는 인증서 프로파일을 설정하지 않은 경우 지침을 위성 인증을 위해 포털 구성 참조하십시오.

아직 인증서 프로파일을 설정하지 않은 경우 지침은 GlobalProtect LSVPN 구성 요소 간에 SSL 활성화을(를) 참조하십시오.

GlobalProtect Gateway 구성 대화 상자에서 인증을 선택한 후 다음 중 하나를 구성합니다.

- 게이트웨이와 위성 간의 통신을 보호하려면 게이트웨이에 대한 **SSL/TLS** 서비스 프로파일을 선택합니다.
- 위성을 인증하는 데 사용할 인증 프로파일을 지정하려면 클라이언트 인증을 추가합니다. 그런 다음 이름을 입력하여 구성을 식별하고 **OS**를 선택합니다. **Satellite**는 모든 위성에 구성을 적용하고 위성을 인증하는 데 사용할 인증 프로파일을 지정합니다. 터널을 설정하려는 위성 디바이스를 인증하는 데 사용할 게이트웨이의 인증서 프로파일을 선택할 수도 있습니다.

**STEP 4 |** 터널 매개변수를 구성하고 터널링을 활성화합니다.

1. GlobalProtect 게이트웨이 구성 대화 상자에서 위성 > 터널 설정을 선택합니다.
2. 터널 구성 확인란을 선택하여 터널링을 활성화합니다.
3. 사용자가 LSVPN용 인터페이스 및 영역 생성에 대한 작업을 수행할 때 GlobalProtect 위성에 의해 설정된 VPN 터널을 종료하기 위해 정의한 터널 인터페이스를 선택합니다.
4. (선택 사항) 캡슐화된 패킷의 서비스 유형(ToS) 정보를 유지하려면 **TOS** 복사를 선택합니다.

   터널 내부에 여러 세션이 있는 경우*(*각각 다른 *TOS* 값을 가짐*) TOS* 헤더를 복사하면 *IPSec* 패킷이 순서 없이 도착할 수 있습니다*.*

**STEP 5 |** (선택 사항) 터널 모니터링을 활성화합니다.

터널 모니터링을 통해 위성은 게이트웨이 터널 연결을 모니터링할 수 있으므로 연결이 실패할 경우 백업 게이트웨이로 페일오버할 수 있습니다. 다른 게이트웨이로의 페일오버는 LSVPN에서 지원되는 유일한 유형의 터널 모니터링 프로파일입니다.

1. 터널 모니터링 확인란을 선택합니다.
2. 게이트웨이가 활성 상태인지 확인하기 위해 위성이 사용해야 하는 대상 **IP** 주소를 지정합니다. **IPv4** 주소와 **IPv6** 주소 또는 둘 다를 지정할 수 있습니다. 또는 터널 인터페이스에 대한 IP 주소를 구성한 경우 이 필드를 비워 둘 수 있으며 터널 모니터는 대신 터널 인터페이스를 사용하여 연결이 활성 상태인지 확인합니다.
3. 터널 모니터 프로파일 드롭다운에서 페일오버를 선택합니다(LSVPN에 대해 지원되는 유일한 터널 모니터 프로파일).

**STEP 6 |** 터널 연결을 설정할 때 사용할 IPsec 암호화 프로파일을 선택합니다.

프로파일은 터널을 통과할 데이터를 보호하기 위한 IPSec 암호화 유형과 인증 방법을 지정합니다. LSVPN의 두 터널의 엔드포인트는 조직 내에서 신뢰할 수 있는 방화벽이므로 일반적으로 ESP를 IPSec

 ©2023 Palo Alto Networks, Inc.

프로토콜로 사용하는 기본(사전 정의된) 프로파일, DH 그룹용 group2, 암호화용 AES-128-CBC 및 인증용 SHA-1입니다.

**IPSec** 암호화 프로파일 드롭다운에서 기본값을 선택하여 사전 정의된 프로파일을 사용하거나 새 **IPSec** 암호화 프로파일을 선택하여 새 프로파일을 정의합니다. 인증 및 암호화 옵션에 대한 자세한 내용은 IPsec 암호화 프로파일 정의을(를) 참조하십시오.

**STEP 7 |** IPSec 터널을 설정하는 동안 위성을 할당하도록 네트워크 설정을 구성합니다.



위성을 호스팅하는 방화벽에서 ***DHCP*** 서버를 구성하여 ***DNS*** 설정을 로컬 클라이언트에 푸시하도록 위성을 구성할 수도 있습니다. 이 구성에서 위성은 게이트웨이에서 배운 ***DNS*** 설정을 ***DHCP*** 클라이언트로 푸시합니다.

1. GlobalProtect 게이트웨이 구성 대화 상자에서 위성 > 네트워크 설정을 선택합니다.
2. (선택 사항) 위성에 로컬인 클라이언트가 회사 네트워크에서 FQDN을 확인해야 하는 경우 다음 방법 중 하나로 DNS 설정을 위성에 푸시하도록 게이트웨이를 구성합니다.
   - 게이트웨이에 DHCP 클라이언트로 구성된 인터페이스가 있는 경우 상속 소스를 해당 인터페이스로 설정하고 DHCP 클라이언트가 수신한 동일한 설정을 GlobalProtect 위성에 할당할 수 있습니다. 동일한 소스에서 DNS 접미사를 상속할 수도 있습니다.
   - 기본 **DNS**, 보조 **DNS** 및 **DNS** 서픽스 설정을 수동으로 정의하여 위성에 푸시합니다.
3. VPN이 설정될 때 위성에 터널 인터페이스를 할당할 주소의 **IP** 풀을 지정하려면 추가를 클릭한 다음 사용할 IP 주소 범위를 지정하십시오.
4. 터널을 통해 라우팅할 대상 서브넷을 정의하려면 액세스 경로 영역에서 추가를 클릭하고 다음과 같이 경로를 입력합니다.
   - 터널을 통해 새틀라이트의 모든 트래픽을 라우팅하려면 이 필드를 비워 둡니다.

     이 경우 로컬 서브넷으로 향하는 트래픽을 제외한 모든 트래픽은 게이트웨이로 터널링됩니다.

   - 게이트웨이를 통해 일부 트래픽만 라우팅하려면(분할 터널링이라고 함) 터널링해야 하는 대상 서브넷을 지정합니다. 이 경우 위성은 자체 라우팅 테이블을 사용하여 지정된 액세스 경로로 향하지 않는 트래픽을 라우팅합니다. 예를 들어, 회사 네트워크로 향하는 트래픽만 터널링하도록 선택한 다음 로컬 위성을 사용하여 인터넷 액세스를 안전하게 활성화할 수 있습니다.
   - 새틀라이트 간 라우팅을 활성화하려면 각 새틀라이트에서 보호하는 네트워크에 대한 요약 경로를 입력합니다.

**STEP 8 |** (선택 사항) 게이트웨이가 위성에서 수락할 경로(있는 경우)를 정의합니다.

기본적으로 게이트웨이는 위성이 라우팅 테이블에 광고하는 경로를 추가하지 않습니다. 게이트웨이가 위성의 경로를 수락하지 않도록 하려면 이 단계를 완료할 필요가 없습니다.

1. 게이트웨이가 위성에서 보급한 경로를 수락하도록 하려면 위성 > 경로 필터를 선택합니다.
2. 게시된 경로 수락 체크박스를 선택합니다.
3. 게이트웨이 라우팅 테이블에 추가할 위성에 의해 보급된 경로를 필터링하려면 추가를 클릭한 다음 포함할 서브넷을 정의합니다. 예를 들어 모든 위성이 LAN 측에서 서브넷 192.168.x.0/24로

 ©2023 Palo Alto Networks, Inc.

구성된 경우, 게이트웨이가 192.168.0.0/16 서브넷에 있으면 위성의 경로만 수락하도록 허용된 경로 192.168.0.0/16을 구성합니다.

**STEP 9 |** 게이트웨이 구성을 저장합니다.

1. 확인을 클릭하여 설정을 저장하고 GlobalProtect Gateway 구성 대화 상자를 닫습니다.
2. 구성을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

# LSVPN을 위한 글로벌 보호 포털 구성

GlobalProtect 포털은 GlobalProtect LSVPN에 대한 관리 기능을 제공합니다. LSVPN에 참여하는 모든 위성 시스템은 사용 가능한 게이트웨이에 대한 정보와 게이트웨이에 연결하는 데 필요한 인증서를 포함하여 포털에서 구성 정보를 받습니다.

다음 섹션에서는 포털 설정 절차를 제공합니다.

- LSVPN 전제 조건 작업에 대한 글로벌 보호 포털
- 포털 구성
- 위성 구성 정의

## LSVPN 전제 조건 작업에 대한 글로벌 보호 포털

GlobalProtect 포털을 구성하기 전에 다음 작업을 완료해야 합니다.

- 포털을 구성할 인터페이스에서의 LSVPN용 인터페이스 및 영역 생성.
- 포털 서버 인증서에 대한 SSL/TLS 서비스 프로파일을 생성하고 게이트웨이 서버 인증서를 발급하고 GlobalProtect 위성에 대한 서버 인증서를 발급하도록 포털을 구성하여 GlobalProtect LSVPN 구성 요소 간에 SSL 활성화.
- 위성 인증을 위해 포털 구성 로컬 데이터베이스 인증을 설정하고 포털에서 위성을 인증하는 데 사용할 인증 프로파일을 정의합니다.
- LSVPN을 위한 글로벌 보호 게이트웨이 구성.

## 포털 구성

LSVPN 전제 조건 작업에 대한 GlobalProtect 포털을 완료한 후 다음과 같이 GlobalProtect 포털을 구성합니다.

**STEP 1 |** 포털을 추가합니다.

1. 네트워크 > **GlobalProtect** > 포털을 선택한 다음 추가를 클릭합니다.
2. 일반 탭에서 포털의 이름을 입력합니다. 포털 이름에는 공백이 없어야 합니다.
3. (선택 사항) 위치 필드에서 이 포털이 속한 가상 시스템을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 위성이 포털에 연결할 수 있도록 네트워크 정보를 지정하십시오.

포털에 대한 네트워크 인터페이스를 아직 생성하지 않은 경우 지침은 LSVPN에 대한 인터페이스 및 영역 생성을 참조하십시오.

1. 위성이 포털에 대한 인그레스(ingress) 액세스에 사용할 인터페이스를 선택합니다.
2. 포털에 대한 위성 액세스를 위해 **IP** 주소 유형 및 **IP** 주소를 지정합니다.
   - IP 주소 유형은 **IPv4**(IPv4 트래픽 전용), **IPv6**(IPv6 트래픽 전용) 또는 **IPv4** 및 **IPv6**일 수 있습니다. 네트워크가 IPv4 및 IPv6이 동시에 실행되는 이중 스택 구성을 지원하는 경우 **IPv4** 및 **IPv6**을 사용하십시오.
   - IP 주소는 IP 주소 유형과 호환되어야 합니다. 예를 들어 IPv4 주소의 경우 **172.16.1/0**, IPv6 주소의 경우 **21DA:D3:0:2F3B**입니다. 이중 스택 구성의 경우 IPv4 및 IPv6 주소를 모두 입력합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

**STEP 3 |** 위성이 포털에 대한 SSL/TLS 연결을 설정하도록 하는 데 사용할 SSL/TLS 서비스 프로파일을 지정하십시오.

포털에 대한 SSL/TLS 서비스 프로파일을 생성하고 게이트웨이 인증서를 발급하지 않은 경우 GlobalProtect LSVPN 구성 요소에 서버 인증서 배포를 참조하십시오.

1. GlobalProtect 포털 구성 대화 상자에서 인증을 선택하십시오.
2. **SSL/TLS** 서비스 프로파일을 선택합니다.

**STEP 4 |** 위성 인증을 위한 인증 프로파일 및 선택적 인증서 프로파일을 지정합니다.

위성이 포털에 처음 연결할 때는 로컬 데이터베이스 인증을 사용하여 인증해야 합니다**(**후속 세션에서는 포털에서 발급한 위성 쿠키를 사용함**).** 따라서 확인을 클릭하여 포털 구성을 저장하려면 먼저 인증 프로파일을 구성해야 합니다**.**

클라이언트 인증을 추가한 다음 이름을 입력하여 구성을 식별하고 **OS**를 선택합니다. 모든 Satellite에 구성을 적용하려면 **Satellite**를 선택한 다음 Satellite 디바이스를 인증하는 데 사용할 인증 프로파일을 지정하십시오. 포털이 위성 디바이스를 인증하는 데 사용할 인증서 프로파일을 지정할 수도 있습니다.

**STEP 5 |** 위성에 푸시할 구성을 계속 정의하거나 위성 구성을 이미 생성한 경우 포털 구성을 저장합니다.

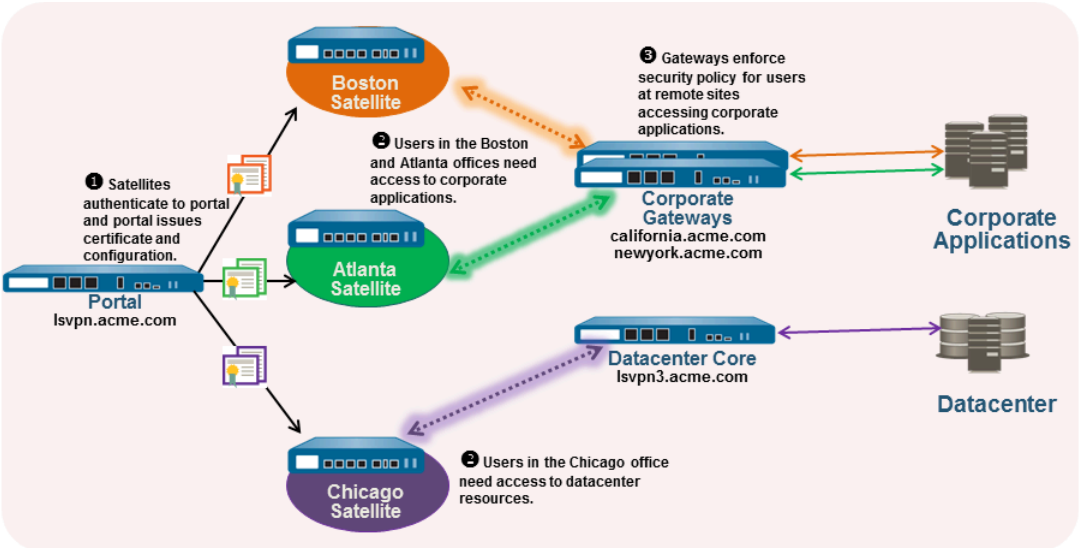
확인을 클릭하여 포털 구성을 저장하거나 Satellite 구성 정의를 계속하십시오.

## 위성 구성 정의

GlobalProtect 위성이 GlobalProtect 포털에 연결되고 성공적으로 인증되면 포털은 위성이 연결할 수 있는 게이트웨이를 지정하는 위성 구성을 제공합니다. 모든 위성이 동일한 게이트웨이 및 인증서 구성을 사용하는 경우 단일 위성 구성을 만들어 인증에 성공하면 모든 위성에 포워딩할 수 있습니다. 그러나 다른 위성 구성이 필요한 경우(예: 한 위성 그룹을 한 게이트웨이에 연결하고 다른 위성 그룹을 다른 게이트웨이에 연결하려는 경우) 각각에 대해 별도의 위성 구성을 생성할 수 있습니다. 그런 다음 포털은 등록 사용자 이름/그룹 이름 또는 위성의 일련번호를 사용하여 배포할 위성 구성을 결정합니다. 보안 규칙 평가와 마찬가지로 포털은 목록의 맨 위에서 시작하여 일치 항목을 찾습니다. 일치하는 항목을 찾으면 해당 구성을 위성에 포워딩합니다.

 ©2023 Palo Alto Networks, Inc.

예를 들어 다음 그림은 일부 지사에서 주변 방화벽으로 보호되는 기업 애플리케이션에 대한 VPN 액세스를 요구하고 다른 사이트는 데이터 센터에 대한 VPN 액세스를 필요로 하는 네트워크를 보여줍니다.




다음 절차를 사용하여 하나 이상의 위성 구성을 생성합니다.

**STEP 1 |** 위성 구성을 추가합니다.

위성 구성은 연결하는 위성에 배포할 GlobalProtect LSVPN 구성 설정을 지정합니다. 하나 이상의 위성 구성을 정의해야 합니다.

1. 네트워크 > **GlobalProtect** > 포털을 선택한 다음 위성 구성을 추가하려는 포털 구성을 선택한 후 위성 탭을 선택합니다.
2. 위성 섹션에서 추가를 클릭합니다.
3. 구성의 이름을 입력합니다.

   여러 구성을 만들 계획이라면 각각에 대해 정의하는 이름이 구성을 구분할 수 있을 만큼 충분히 설명적인지 확인하십시오.
4. 위성이 구성 업데이트를 위해 포털을 확인해야 하는 빈도를 변경하려면 구성 새로 고침 인터벌**(**시간**)** 필드에 값을 지정하십시오(범위는 1-48, 기본값은 24).

**STEP 2 |** 이 구성을 사용할 위성을 지정합니다.

포털은 등록 사용자**/**사용자 그룹 설정 및/또는 디바이스 일련번호를 사용하여 위성을 구성과 일치시킵니다. 따라서 구성이 여러 개인 경우 올바르게 주문해야 합니다. 포털은 일치하는 항목을 찾는 즉시

 ©2023 Palo Alto Networks, Inc.

구성을 제공합니다. 따라서 보다 구체적인 구성이 보다 일반적인 구성보다 우선해야 합니다. 위성 구성 목록 주문에 대한 지침은 5단계를 참조하십시오.

다음과 같이 위성 구성에 대한 일치 기준을 지정합니다.

- 이 구성을 특정 일련번호가 있는 위성으로 제한하려면 디바이스 탭을 선택한 다음 추가를 클릭한 다음 일련번호를 입력합니다(위성 호스트 이름을 입력할 필요가 없으며 위성이 연결될 때 자동으로 추가됨). 이 구성을 수신하려는 각 위성에 대해 이 단계를 반복하십시오.
- 등록 사용자/사용자 그룹 탭을 선택한 다음 추가를 클릭한 다음 이 구성을 받을 사용자 또는 그룹을 선택합니다. 일련번호가 일치하지 않는 Satellite는 여기에 지정된 사용자(개별 사용자 또는 그룹 구성원)로 인증해야 합니다.



구성을 특정 그룹으로 제한하려면 먼저 사용자를 그룹에 매핑해야 합니다.

**STEP 3 |** 이 구성의 위성이 VPN 터널을 설정할 수 있는 게이트웨이를 지정하십시오.



게이트웨이에서 게시한 경로는 위성에 고정 경로로 설치됩니다. 고정 경로에 대한 메트릭은 라우팅 우선 순위의 *10*배입니다. 게이트웨이가 두 개 이상인 경우 백업 게이트웨이에서 보급한 경로가 기본 게이트웨이에서 보급한 동일한 경로와 비교하여 더 높은 메트릭을 갖도록 라우팅 우선 순위도 설정해야 합니다. 예를 들어 기본 게이트웨이와 백업 게이트웨이에 대한 라우팅 우선 순위를 각각 *1*과 *10*으로 설정하면 위성는 기본 게이트웨이에 대한 메트릭으로 *10*을 사용하고 백업 게이트웨이에 대한 메트릭으로 *100*을 사용합니다.

1. 게이트웨이 탭에서 추가를 클릭합니다.
2. 게이트웨이에 대한 설명이 포함된 이름을 입력합니다. 여기에 입력하는 이름은 게이트웨이를 구성할 때 정의한 이름과 일치해야 하며 게이트웨이의 위치를 식별할 수 있을 만큼 충분히 설명적이어야 합니다.
3. 게이트웨이 필드에 게이트웨이가 구성된 인터페이스의 FQDN 또는 IP 주소를 입력합니다. 지정하는 주소는 게이트웨이 서버 인증서의 CN(일반 이름)과 정확히 일치해야 합니다.
4. (선택 사항) 구성에 둘 이상의 게이트웨이를 추가하는 경우 라우팅 우선 순위는 위성이 선호하는 게이트웨이를 선택하는 데 도움이 됩니다. 1-25 범위의 값을 입력하고 숫자가 낮을수록 우선 순위가 높습니다(즉, 모든 게이트웨이가 사용 가능한 경우 위성이 연결할 게이트웨이). 위성은 라우팅 메트릭을 결정하기 위해 라우팅 우선 순위에 10을 곱합니다.

**STEP 4 |** 위성 구성을 저장합니다.

1. 확인을 클릭하여 위성 구성을 저장합니다.
2. 다른 위성 구성을 추가하려면 이전 단계를 반복하십시오.

**STEP 5 |** 각 위성에 적절한 구성이 배포되도록 위성 구성을 정렬합니다.

- 구성 목록에서 위성 구성을 위로 이동하려면 구성을 선택한 다음 위로 이동을 클릭하십시오.
- 구성 목록에서 위성 구성을 아래로 이동하려면 구성을 선택한 다음 아래로 이동을 클릭하십시오.

**STEP 6 |** 위성이 LSVPN에 참여할 수 있도록 하는 데 필요한 인증서를 지정합니다.

1. 신뢰할 수 있는 루트 **CA** 필드에서 추가를 클릭한 다음 게이트웨이 서버 인증서를 발급하는 데 사용되는 CA 인증서를 선택합니다. 포털은 사용자가 여기에 추가한 루트 CA 인증서를 구성의


©2023 Palo Alto Networks, Inc.

일부로 모든 위성에 배포하여 위성이 게이트웨이와 SSL 연결을 설정할 수 있도록 합니다. 가장 좋은 방법은 모든 게이트웨이가 동일한 발급자를 사용하는 것입니다.

2. 클라이언트 인증서 배포 방법 선택:

   - 포털에 클라이언트 인증서를 저장하려면 로컬을 선택한 다음 인증서 발급 드롭다운에서 성공적으로 인증되면 포털이 위성에 클라이언트 인증서를 발급하는 데 사용할 루트 CA 인증서를 선택합니다.

     게이트웨이 서버 인증서를 발급하는 데 사용된 루트 ***CA*** 인증서가 포털에 없으면 지금 가져올 수 있습니다. 루트 ***CA*** 인증서를 가져오는 방법에 대한 자세한 내용은 GlobalProtect LSVPN 구성 요소 간 SSL 활성화를 참조하십시오.

   - 포털이 클라이언트 인증서를 동적으로 요청하고 발급하기 위해 **SCEP** 클라이언트로 작동하도록 하려면 **SCEP**를 선택한 다음 SCEP 서버에 대한 CSR을 생성하는 데 사용되는 **SCEP** 프로파일을 선택합니다.

     ***SCEP*** 클라이언트 역할을 하도록 포털을 아직 설정하지 않은 경우 지금 새 ***SCEP*** 프로파일을 추가할 수 있습니다. 자세한 내용은 SCEP를 사용하여 GlobalProtect Satellite에 클라이언트 인증서 배포를 참조하십시오.

**STEP 7 |** 포털 구성을 저장합니다.

1. 확인을 클릭하여 설정을 저장하고 GlobalProtect 포털 구성 대화 상자를 닫습니다.
2. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# LSVPN에 가입할 위성 준비

LSVPN에 참여하려면 새틀라이트에 최소한의 구성이 필요합니다. 필요한 구성이 최소이므로 설치를 위해 지사에 새틀라이트를 배송하기 전에 새틀라이트를 미리 구성할 수 있습니다.

**STEP 1 |** 레이어 3 인터페이스를 구성합니다.

이것은 새틀라이트가 포털 및 게이트웨이에 연결하는 데 사용할 물리적 인터페이스입니다. 이 인터페이스는 로컬 신뢰 네트워크 외부의 액세스를 허용하는 영역에 있어야 합니다. 가장 좋은 방법은 회사 게이트웨이를 대상으로 하는 트래픽에 대한 가시성과 제어를 위해 VPN 연결 전용 영역을 만드는 것입니다.

**STEP 2 |** GlobalProtect 게이트웨이와 VPN 터널을 설정하는 데 사용할 터널의 로지컬 터널 인터페이스를 구성합니다.



동적 라우팅을 사용하려는 경우가 아니면 터널 인터페이스에 ***IP*** 주소가 필요하지 않습니다**.** 그러나 터널 인터페이스에 ***IP*** 주소를 할당하면 연결 문제를 해결하는 데 유용할 수 있습니다**.**

1. 네트워크 > 인터페이스 > 터널을 선택하고 추가를 클릭합니다.
2. 인터페이스 이름 필드에 숫자 접미사(예: **.2**)를 지정합니다.
3. 구성 탭에서 보안 영역 드롭다운을 확장하고 기존 영역을 선택하거나 새 영역을 클릭하고 다음을 정의하여 VPN 터널 트래픽에 대한 별도의 영역을 만듭니다. 새 영역의 이름(예: ***lsvpnsat***).
4. 가상 라우터드롭다운에서기본값을 선택합니다.
5. (선택 사항) 터널 인터페이스에 IP 주소를 할당하려면:
   - IPv4 주소의 경우 **IPv4**를 선택한 다음 인터페이스에 할당할 IP 주소 및 네트워크 마스크 추가(예: 203.0.11.100/24)를 선택합니다.
   - IPv6 주소의 경우 **IPv6**, 인터페이스에서 **IPv6** 활성화를 선택하고 인터페이스에 할당할 IP 주소 및 네트워크 마스크를 추가합니다(예: 2001:1890:12f2:11::10.1.8.160/80).
6. 인터페이스 구성을 저장하려면 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 새틀라이트에서 신뢰하지 않는 루트 CA를 사용하여 포털 서버 인증서를 생성한 경우(예: 자체 서명된 인증서를 사용한 경우) 포털 서버 인증서를 발행하는 데 사용된 루트 CA 인증서를 가져오십시오.

루트 CA 인증서는 새틀라이트가 포털과의 초기 연결을 설정하여 LSVPN 구성을 가져오도록 하는 데 필요합니다.

1. 포털 서버 인증서를 생성하는 데 사용된 CA 인증서를 다운로드합니다. 자체 서명된 인증서를 사용하는 경우 다음과 같이 포털에서 루트 CA 인증서를 내보냅니다.
   1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택합니다.
   2. CA 인증서를 선택한 다음 내보내기를 클릭합니다.
   3. 파일 형식 드롭다운에서 **Base64** 인코딩된 인증서**(PEM)**를 선택한 다음 확인을 클릭하여 인증서를 다운로드합니다. (프라이빗 키를 내보낼 필요는 없습니다.)
2. 다음과 같이 방금 내보낸 루트 CA 인증서를 각 새틀라이트로 가져옵니다.
   1. 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택한 다음 가져오기를 클릭합니다.
   2. 인증서를 클라이언트 CA 인증서로 식별하는 인증서 이름을 입력합니다.
   3. CA에서 다운로드한 인증서 파일을 찾습니다.
   4. 파일 형식으로 **Base64** 인코딩된 인증서**(PEM)**를 선택한 다음 확인을 클릭합니다.
   5. 디바이스 인증서 탭에서 방금 불러온 인증서를 선택하여 엽니다.
   6. 신뢰할 수 있는 루트 **CA**를 선택한 다음 확인을 클릭합니다.

**STEP 4 |** IPSec 터널 구성을 구성합니다.

1. 네트워크 > **IPSec** 터널을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 IPSec 구성에 대한 설명이 포함된 이름을 입력합니다.
3. 위성에 대해 생성한 터널 인터페이스를 선택합니다.
4. **GlobalProtect Satellite**를 유형으로 선택합니다.
5. 포털의 IP 주소 또는 FQDN을 포털 주소로 입력합니다.
6. 위성에 대해 구성한 레이어 3 인터페이스를 선택합니다.
7. 선택한 인터페이스에서 사용할 **IP** 주소를 선택합니다. **IPv4** 주소, **IPv6** 주소 또는 둘 다를 선택할 수 있습니다. 포털 등록에 **IPv6**을 선호할지 여부를 지정합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** (선택 사항) 게이트웨이에 로컬 경로를 게시하도록 새틀라이트를 구성합니다.

게이트웨이로 경로를 푸시하면 게이트웨이를 통해 새틀라이트에 로컬인 서브넷으로의 트래픽이 활성화됩니다. 그러나 LSVPN용 GlobalProtect 게이트웨이 구성에 설명된 대로 경로를 수락하도록 게이트웨이도 구성해야 합니다.

1. 위성이 게이트웨이로 경로를 푸시할 수 있도록 하려면 고급 탭에서 게이트웨이에 모든 고정 및 연결된 경로 게시를 선택합니다.

   이 체크박스를 선택하면 방화벽이 새틀라이트에서 게이트웨이로 모든 고정 및 연결된 경로를 포워딩합니다. 그러나 라우팅 루프 생성을 방지하기 위해 방화벽은 다음과 같은 일부 경로 필터를 적용합니다.

   - 기본 경로
   - 터널 인터페이스와 연결된 가상 라우터가 아닌 가상 라우터 내의 경로
   - 터널 인터페이스를 사용하는 경로
   - 터널 인터페이스와 연결된 물리적 인터페이스를 사용하는 경로
2. (선택 사항) 모든 경로가 아닌 특정 서브넷에 대한 경로만 푸시하려면 서브넷 섹션에서 추가를 클릭하고 게시할 서브넷 경로를 지정합니다.

**STEP 6 |** 위성 구성을 저장합니다.

1. 확인을 클릭하여 IPSec 터널 설정을 저장합니다.
2. 커밋을 클릭합니다.

**STEP 7 |** 필요한 경우 새틀라이트가 포털에 인증할 수 있도록 자격 증명을 제공합니다.

처음으로 포털에 인증하려면 위성 관리자가 로컬 데이터베이스의 위성 관리자 계정과 연결된 사용자 이름과 비밀번호를 제공해야 합니다.

1. 네트워크 > **IPSec** 터널을 선택하고 LSVPN에 대해 생성한 터널 구성의 상태 열에서 게이트웨이 정보 링크를 클릭합니다.
2. 포털 상태 필드에서 자격 증명 입력 링크를 클릭하고 포털에 위성을 인증하는 데 필요한 사용자 이름과 암호를 클릭합니다.

   포털이 포털에 성공적으로 인증되면 게이트웨이에 연결하는 데 사용할 서명된 인증서 및 구성을 받게 됩니다. 터널이 설정되고 상태가 활성으로 변경되는 것을 확인해야 합니다.


©2023 Palo Alto Networks, Inc.

# LSVPN 구성 확인

포털, 게이트웨이 및 새틀라이트를 구성한 후 새틀라이트가 포털 및 게이트웨이에 연결할 수 있는지 확인하고 게이트웨이와 VPN 터널을 설정할 수 있습니다.

**STEP 1 |** 포털과 새틀라이트 연결을 확인합니다.

포털을 호스팅하는 방화벽에서 **Network** > **GlobalProtect** > **Portal**을 선택한 다음 포털 구성 항목의 정보 열에서 새틀라이트 정보를 클릭하여 새틀라이트가 성공적으로 연결되고 있는지 확인합니다.

**STEP 2 |** 게이트웨이와의 새틀라이트 연결을 확인합니다.

게이트웨이를 호스팅하는 각 방화벽에서 **Network** > **GlobalProtect** > **Gateways**를 선택한 다음 게이트웨이 구성 항목의 정보 열에서 새틀라이트 정보를 클릭하여 새틀라이트가 VPN 터널을 설정할 수 있는지 확인하십시오. 게이트웨이와 성공적으로 터널을 구축한 Satellite는 **Active Satellites** 탭에 표시됩니다.

**STEP 3 |** 새틀라이트에서 LSVPN 터널 상태를 확인합니다.

새틀라이트를 호스팅하는 각 방화벽에서 네트워크 > **IPSec** 터널을 선택하여 터널 상태를 확인하고 녹색 아이콘으로 표시된 활성 상태를 확인합니다.


©2023 Palo Alto Networks, Inc.

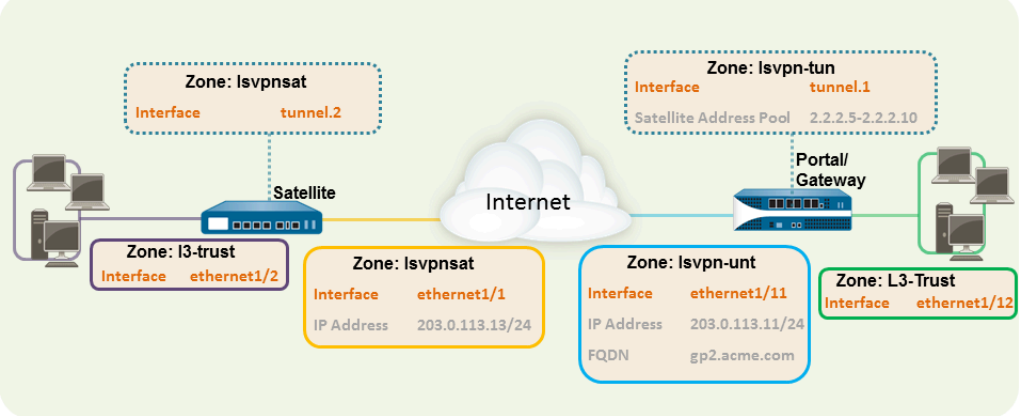
# LSVPN 빠른 구성

다음 섹션에서는 몇 가지 일반적인 GlobalProtect LSVPN 배포를 구성하기 위한 단계별 지침을 제공합니다.

- 정적 라우팅을 갖춘 기본 LSVPN 구성
- 동적 라우팅을 갖춘 Advanced LSVPN 구성
- iBGP를 갖춘 Advanced LSVPN 구성

## 정적 라우팅을 갖춘 기본 LSVPN 구성

이 빠른 구성은 LSVPN을 시작하고 실행하는 가장 빠른 방법을 보여줍니다. 이 예에서 회사 본사 사이트의 단일 방화벽은 포털과 게이트웨이 모두로 구성됩니다. 최적화된 확장성을 위해 최소한의 구성으로 위성을 빠르고 쉽게 배포할 수 있습니다.




다음 워크플로는 이 기본 구성을 설정하는 단계를 보여줍니다.

**STEP 1 |** 레이어 3 인터페이스를 구성합니다.

이 예에서 포털/게이트웨이의 레이어 3 인터페이스에는 다음 구성이 필요합니다.

- 인터페이스 - ethernet1/11
- 보안 영역 - lsvpn-tun
- **IPv4** - 203.0.113.11/24

**STEP 2 |** GlobalProtect 게이트웨이를 호스팅하는 방화벽에서 GlobalProtect 위성에 의해 설정된 VPN 터널을 종료할 로지컬 터널 인터페이스를 구성합니다.

*VPN*을 통해 연결하는 사용자 및 그룹에 대한 가시성을 활성화하려면 *VPN* 터널이 종료되는 영역에서 사용자 *ID*를 활성화하십시오.

이 예에서 포털/게이트웨이의 터널 인터페이스에는 다음 구성이 필요합니다.

- 인터페이스 - tunnel.1
- 보안 영역 - lsvpn-tun


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 터널이 종료되는 VPN 영역(lsvpn-tun)과 기업 애플리케이션이 상주하는 신뢰 영역(L3-Trust) 간의 트래픽 플로우를 활성화하는 보안 정책 규칙을 생성합니다.

보안 정책 규칙 생성을 참조하십시오.

**STEP 4 |** SSL/TLS 서비스 프로파일을 포털/게이트웨이에 할당합니다. 프로파일은 자체 서명된 서버 인증서를 참조해야 합니다.

인증서 주체 이름은 포털/게이트웨이에 대해 생성한 레이어 3 인터페이스의 FQDN 또는 IP 주소와 일치해야 합니다.

1. GlobalProtect 포털을 호스팅하는 방화벽에서 GlobalProtect 구성 요소의 인증서에 서명하기 위한 루트 CA 인증서를 생성합니다. 이 예에서 루트 CA 인증서인 **lsvpn-CA**는 포털/게이트웨이에 대한 서버 인증서를 발급하는 데 사용됩니다. 또한 포털은 이 루트 CA 인증서를 사용하여 위성의 CSR에 서명합니다.
2. GlobalProtect 포털 및 게이트웨이에 대한 SSL/TLS 서비스 프로파일을 생성합니다.

   이 예에서 포털과 게이트웨이는 동일한 인터페이스에 있으므로 동일한 서버 인증서를 사용하는 SSL/TLS 서비스 프로파일을 공유할 수 있습니다. 이 예에서 프로파일의 이름은 **lsvpnserver**입니다.

**STEP 5 |** 인증서 프로파일을 생성합니다.

이 예에서 인증서 프로파일 **lsvpn-profile**은 루트 CA 인증서 **lsvpn-CA**를 참조합니다. 게이트웨이는 이 인증서 프로파일을 사용하여 VPN 터널을 설정하려는 위성을 인증합니다.

**STEP 6 |** 로컬 데이터베이스 인증을 사용하여 위성을 인증하도록 포털을 구성합니다.

**STEP 7 |** LSVPN을 위한 글로벌 보호 게이트웨이 구성.

네트워크 > **GlobalProtect** > 게이트웨이를 선택한 다음 구성을 추가합니다. 이 예에는 다음 게이트웨이 구성이 필요합니다.

- 인터페이스 - ethernet1/11
- **IP** 주소 - 203.0.113.11/24
- **SSL/TLS** 서버 프로파일 - lsvpnserver
- 인증서 프로파일 - lsvpn-profile
- 터널 인터페이스 - tunnel.1
- 기본 **DNS**/보조 **DNS** - 4.2.2.1/4.2.2.2
- **IP** 풀 - 2.2.2.111-2.2.2.120
- 액세스 경로 - 10.2.10.0/24

 ©2023 Palo Alto Networks, Inc.

**STEP 8 |** 포털을 구성합니다.

네트워크 > **GlobalProtect** > 포털을 선택한 다음 구성을 추가합니다. 이 예에는 다음 포털 구성이 필요합니다.

- 인터페이스 - ethernet1/11
- **IP** 주소 - 203.0.113.11/24
- **SSL/TLS** 서버 프로파일 - lsvpnserver
- 인증 프로파일 - lsvpn-sat

**STEP 9 |** 위성 구성 정의.

포털 구성의 위성 탭에서 위성 구성 및 신뢰할 수 있는 루트 CA를 추가하고 포털이 위성에 대한 인증서를 발급하는 데 사용할 CA를 지정합니다. 이 예에서 필요한 설정은 다음과 같습니다.

- 게이트웨이 - 203.0.113.11
- 인증서 발급 - lsvpn-CA
- 신뢰할 수 있는 루트 **CA** - lsvpn-CA

**STEP 10 |** LSVPN에 가입할 위성 준비.

이 예의 위성 구성에는 다음 설정이 필요합니다.

인터페이스 구성

- 레이어 3 인터페이스 - ethernet1/1, 203.0.113.13/24
- 터널 인터페이스 - tunnel.2
- 영역 - lsvpnsat

포털의 루트 CA 인증서

- lsvpn-CA

IPSec 터널 구성

- 터널 인터페이스 - tunnel.2
- 포털 주소 - 203.0.113.11
- 인터페이스 - ethernet1/1
- 로컬 **IP** 주소 - 203.0.113.13/24
- 모든 정적 및 연결된 경로를 게이트웨이에 게시 - 활성화됨

## 동적 라우팅을 갖춘 Advanced LSVPN 구성

여러 게이트웨이와 다수의 위성이 있는 대규모 LSVPN 배포에서 동적 라우팅을 설정하는 초기 구성에 약간의 시간을 투자하면 액세스 경로가 동적으로 업데이트되므로 게이트웨이 구성의 유지 관리가 간소화됩니다. 다음 예제 구성에서는 기본 LSVPN 구성을 확장하여 OSPF를 동적 라우팅 프로토콜로 구성하는 방법을 보여 줍니다.

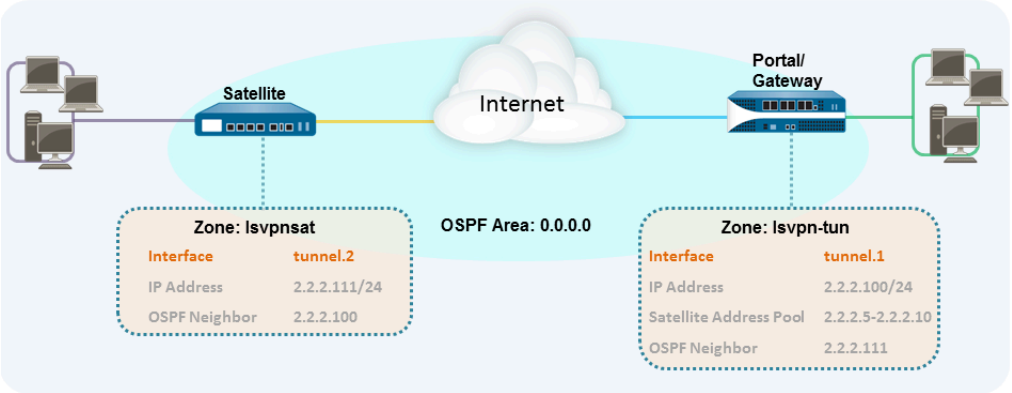
동적 라우팅을 위해 OSPF를 사용하도록 LSVPN을 설정하려면 게이트웨이 및 위성에 대한 다음 추가 단계가 필요합니다.

 ©2023 Palo Alto Networks, Inc.

- 모든 게이트웨이 및 위성의 터널 인터페이스에 IP 주소를 수동으로 할당합니다.
- 모든 게이트웨이 및 위성의 가상 라우터에서 OSPF 지점 간 다중점(P2MP) 구성. 또한 각 게이트웨이의 OSPF 구성의 일부로 각 위성의 터널 IP 주소를 OSPF 이웃으로 수동으로 정의해야 합니다. 마찬가지로 각 위성에서 각 게이트웨이의 터널 IP 주소를 OSPF 이웃으로 수동으로 정의해야 합니다.

동적 라우팅은 LSVPN의 초기 구성 중에 추가 설정이 필요하지만 네트워크에서 토폴로지 변경이 발생할 때 경로를 최신 상태로 유지하는 것과 관련된 유지 관리 작업을 줄입니다.

다음 그림에는 LSVPN 동적 라우팅 구성이 표시됩니다. 이 예제에서는 OSPF를 VPN의 동적 라우팅 프로토콜로 구성하는 방법을 보여 드립니다.




LSVPN의 기본 설정은 정적 라우팅을 통해 기본 LSVPN 구성의 단계를 따르십시오. 그런 다음 워크플로에서 단계를 완료하여 정적 라우팅이 아닌 동적 라우팅을 사용하도록 구성을 확장할 수 있습니다.

**STEP 1 |** 각 게이트웨이와 각 위성의 터널 인터페이스 구성에 IP 주소를 추가합니다.

각 게이트웨이 및 각 위성에서 다음 단계를 완료합니다.

1. 네트워크 > 인터페이스 > 터널을 선택한 다음LSVPN에 대해 만든 터널 구성을 선택하여 터널 인터페이스 대화 상자를 엽니다.

   아직 터널 인터페이스를 만들지 않은 경우 LSVPN에 대한 인터페이스 생성 및 영역의 2단계를 참조하십시오.
2. **IPv4** 탭에서 추가를 클릭한 다음 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 게이트웨이 터널 인터페이스의 IP 주소를 추가하려면 2.2.2.100/24를 입력합니다.
3. 확인을 클릭하여 구성을 저장합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 게이트웨이에서 동적 라우팅 프로토콜을 구성합니다.

게이트웨이에서 OSPF를 구성하려면 다음을 수행합니다.

1. 네트워크 > 가상 라우터를 선택한 다음 VPN 인터페이스와 연결된 가상 라우터를 선택합니다.
2. 영역 탭에서 추가를 클릭하여 백본 영역을 만들거나 이미 구성된 경우 영역 ID를 클릭하여 편집합니다.
3. 새 영역을 만드는 경우 유형 탭에서 영역 **ID**를 입력합니다.
4. 인터페이스 탭에서 추가를 클릭하고 LSVPN용으로 만든 터널 인터페이스를 선택합니다.
5. **p2mp**를 링크 유형으로 선택합니다.
6. 이웃 섹션에 추가를 클릭하고 각 위성의 터널 인터페이스의 IP 주소(예: 2.2.2.111)를 입력합니다.
7. 확인을 두 번 클릭하여 가상 라우터 구성을 저장한 다음 게이트웨이에서 변경 내용을 커밋합니다.
8. LSVPN에 새 위성을 추가할 때마다 이 단계를 반복합니다.

**STEP 3 |** 위성에서 동적 라우팅 프로토콜을 구성합니다.

위성에서 OSPF를 구성하려면 다음을 수행합니다.

1. 네트워크 > 가상 라우터를 선택한 다음 VPN 인터페이스와 연결된 가상 라우터를 선택합니다.
2. 영역 탭에서 추가를 클릭하여 백본 영역을 만들거나 이미 구성된 경우 영역 ID를 클릭하여 편집합니다.
3. 새 영역을 만드는 경우 유형 탭에서 영역 **ID**를 입력합니다.
4. 인터페이스 탭에서 추가를 클릭하고 LSVPN용으로 만든 터널 인터페이스를 선택합니다.
5. **p2mp**를 링크 유형으로 선택합니다.
6. 이웃 섹션에 추가를 클릭하고 각 GlobalProtect 게이트웨이의 터널 인터페이스의 IP 주소를 입력합니다(예: 2.2.2.100).
7. 확인을 두 번 클릭하여 가상 라우터 구성을 저장한 다음 게이트웨이에서 변경 내용을 커밋합니다.
8. 새 게이트웨이를 추가할 때마다 이 단계를 반복합니다.

**STEP 4 |** 게이트웨이와 위성이 라우터 접면을 형성할 수 있는지 확인합니다.

- 각 위성과 각 게이트웨이에서 피어 어셈블러가 형성되고 피어를 위해 라우팅 테이블 항목이 만들어졌는지 확인합니다(즉, 위성에는 게이트웨이에 대한 경로가 있고 게이트웨이에는 위성에 대한 경로가 있음). 네트워크 > 가상 라우터를 선택한 다음 LSVPN에 사용하는 가상 라우터에 대한 더 많은 런타임 통계 링크를 클릭합니다. 라우팅 탭에서 LSVPN 피어에 경로가 있는지 확인합니다.
- **OSPF** > 인터페이스탭에서 형식이 **p2mp**인지 확인합니다.
- **OSPF** > 이웃탭에서 게이트웨이를 호스팅하는 방화벽이 위성을 호스팅하는 방화벽과 라우터 관계를 설정했는지 확인하며 그 반대의 경우도 동일합니다. 또한 상태가 전체인지, 확인하여 전체 거주지가 설정되었음을 나타냅니다.


©2023 Palo Alto Networks, Inc.

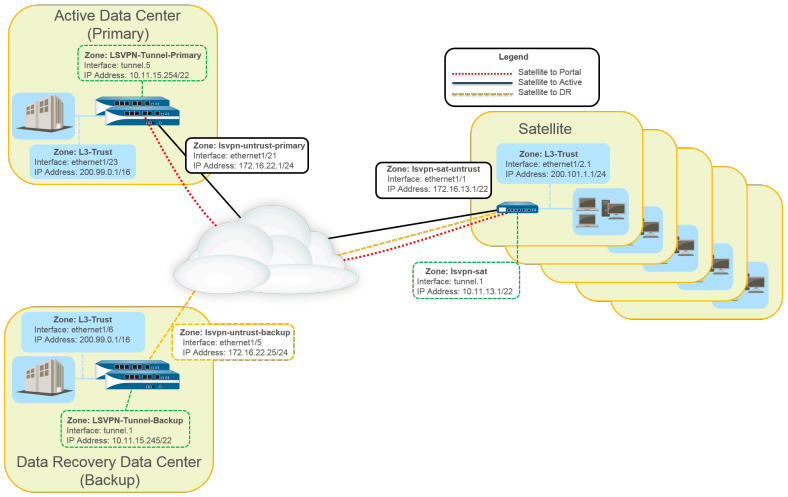
# iBGP를 갖춘 Advanced LSVPN 구성

이 사용 사례는 GlobalProtect LSVPN이 분산된 사무실 위치를 사용자를 위한 중요한 애플리케이션을 수용하는 기본 및 재해 복구 데이터 센터와 안전하게 연결하는 방법과 내부 국경 게이트웨이 프로토콜(iBGP)이 배포 및 유지 보수를 완화하는 방법을 보여 줍니다. 이 방법을 사용하면 단일 게이트웨이에 연결하는 최대 500개의 위성 사무소를 확장할 수 있습니다.

BGP는 LSVPN과 같은 허브 및 스포크 배포에 이상적인 확장성이 뛰어난 동적 라우팅 프로토콜입니다. 동적 라우팅 프로토콜은 추가 위성 방화벽을 비교적 쉽게 배포할 수 있도록 하여 액세스 경로(정적 경로)와 관련된 오버헤드의 대부분을 제거합니다. 경로 필터링 기능 및 여러 튜닝 타이머, 경로 감쇠 및 경로 새로 고침과 같은 기능으로 인해 BGP는 RIP 및 OSPF와 같은 다른 라우팅 프로토콜보다 안정성이 큰 라우팅 프리픽스 수가 훨씬 더 많은 것으로 확장됩니다. LSVPN 배포의 모든 위성과 게이트웨이를 포함하는 피어 그룹인 iBGP의 경우 터널 엔드포인트에 대한 유면이 설정됩니다. 그런 다음 프로토콜은 경로 광고, 업데이트 및 수렴을 암시적으로 제어합니다.

이 예제 구성에서는 활성/수동 HA 쌍의 PA-5200 방화벽이 기본(활성) 데이터 센터에 배포되고 포털 및 기본 게이트웨이 역할을 합니다. 재해 복구 데이터 센터에는 백업 LSVPN 게이트웨이 역할을 하는 활성/패시브 HA 쌍에 두 개의 PA-5200s가 있습니다. 포털 및 게이트웨이는 지사에 LSVPN 위성으로 배포된 500대의 PA-220을 제공합니다.

두 데이터 센터 사이트 모두 경로를 광고하지만 메트릭이 다릅니다. 따라서 위성은 활성 데이터 센터의 경로를 선호하고 설치합니다. 그러나 백업 경로는 로컬 라우팅 정보 베이스(RIB)에도 존재합니다. 활성 데이터 센터가 실패하면 해당 데이터 센터에서 광고하는 경로가 제거되고 재해 복구 데이터 센터의 경로의 경로로 대체됩니다. 페일오버 시간은 iBGP 시간 선택 및 iBGP와 관련된 라우팅 수렴에 따라 달라집니다.




다음 워크플로는 이 배포를 구성하는 단계를 보여줍니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** LSVPN용 인터페이스 및 영역 생성.

포털 및 기본 게이트웨이:

- 영역: LSVPN-Untrust-Primary
- 인터페이스: 이더넷1/21
- IPv4: 172.16.22.1/24
- 영역: L3-Trust
- 인터페이스: 이더넷1/23
- **IPv4**: 200.99.0.1/16

백업 게이트웨이:

- 영역: LSVPN-Untrust-Primary
- 인터페이스: 이더넷1/5
- **IPv4**: 172.16.22.25/24
- 영역: L3-Trust
- 인터페이스: 이더넷1/6
- **IPv4**: 200.99.0.1/16

위성:

- 영역: LSVPN-Sat-불신
- 인터페이스: 이더넷1/1
- **IPv4**: 172.16.13.1/22
- 영역: L3-Trust
- 인터페이스: 이더넷1/2.1
- **IPv4**: 200.101.1.1/24



각 위성의 영역, 인터페이스 및 *IP* 주소를 구성합니다. 인터페이스와 로컬 *IP* 주소는 각 위성마다 다릅니다. 이 인터페이스는 포털 및 게이트웨이에 대한 *VPN* 연결에 사용됩니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** GlobalProtect 게이트웨이를 호스팅하는 방화벽에서 GlobalProtect 위성에 의해 설정된 VPN 터널을 종료할 로지컬 터널 인터페이스를 구성합니다.

기본 게이트웨이:

- 인터페이스: 터널.5
- **IPv4**: 10.11.15.254/22
- 영역: LSVPN-Tunnel-Primary

백업 게이트웨이:

- 인터페이스: 터널.1
- **IPv4**: 10.11.15.245/22
- 영역: LSVPN-Tunnel-Backup

**STEP 3 |** 글로벌 보호 LSVPN 구성 요소 간에 SSL 활성화.

게이트웨이는 자체 서명된 루트 인증서 기관(CA)을 사용하여 GlobalProtect LSVPN에서 위성에 대한 인증서를 발급합니다. 하나의 방화벽에는 포털과 기본 게이트웨이가 있으므로 단일 인증서가 위성에 인증하는 데 사용됩니다. 동일한 CA는 백업 게이트웨이에 대한 인증서를 생성하는 데 사용됩니다. CA는 포털에서 위성으로 밀어붙인 다음 위성에서 게이트웨이로 인증하는 데 사용되는 인증서를 생성합니다.

또한 백업 게이트웨이에 대해 동일한 CA에서 인증서를 생성하여 위성으로 인증할 수 있어야 합니다.

1. GlobalProtect 포털을 호스팅하는 방화벽에서 GlobalProtect 구성 요소의 인증서에 서명하기 위한 루트 CA 인증서를 생성합니다. 이 예에서 루트 CA 인증서를 CA-인증서라고 합니다.
2. GlobalProtect 포털 및 게이트웨이에 대한 SSL/TLS 서비스 프로파일을 생성합니다. GlobalProtect 포털과 기본 게이트웨이는 동일한 방화벽 인터페이스이므로 두 구성 요소에 대해 동일한 서버 인증서를 사용할 수 있습니다.
   - 루트 **CA** 인증서: CA-Cert
   - 인증서 이름: LSVPN 스케일
3. 자체 서명된 서버 인증서를 게이트웨이에 배포합니다.
4. LSVPN 구성 요소에 대한 서버 인증서를 발급하는 데 사용되는 루트 CA 인증서를 가져옵니다.
5. 인증서 프로파일을 생성합니다.
6. 다음 설정으로 백업 게이트웨이에서 2-5단계를 반복합니다.
   - 루트 **CA** 인증서: CA-cert
   - 인증서 이름: LSVPN-back-GW-cert

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** LSVPN을 위한 글로벌 보호 게이트웨이 구성.

1. 네트워크 > **GlobalProtect** > 게이트웨이를 선택한 다음 추가를 클릭합니다.
2. 일반 탭에서 기본 게이트웨이 **LSVPN-Scale** 이름을 지정합니다.
3. 네트워크 설정에서 **ethernet1/21**을 기본 게이트웨이 인터페이스로 선택한 다음 **172.16.22.1/24**를 IP 주소로 입력합니다.
4. 인증 탭에서 3에서 만든 LSVPN 규모 인증서를 선택합니다.
5. 위성 > 터널 설정을 선택한 다음 터널 구성을 선택합니다. 터널 인터페이스를 터널.5로 설정합니다. 이 사용 사례의 모든 위성은 단일 게이트웨이에 연결되므로 단일 위성 구성이 필요합니다. 위성은 일련번호에 따라 일치하므로 사용자로 인증할 필요가 없습니다.
6. 위성 > 네트워크 설정에서 VPN 연결이 설정되면 위성의 터널 인터페이스에 할당할 IP 주소 풀을 정의합니다. 이 사용 사례는 동적 라우팅을 사용하므로 액세스 경로 설정은 비어 있습니다.
7. 다음 설정으로 백업 게이트웨이에서 1-5단계를 반복합니다.
   - 이름: LSVPN 백업
   - 게이트웨이 인터페이스: 이더넷1/5
   - 게이트웨이 **IP**: 172.16.22.25/24
   - 서버 인증서: LSVPN-backup-GW-cert
   - 터널 인터페이스: 터널.1

 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 기본 게이트웨이 및 백업 게이트웨이에서 iBGP를 구성하고 재분배 프로파일을 추가하여 위성이 게이트웨이로 로컬 경로를 다시 삽입할 수 있도록 합니다.

각 위성 사무소는 자체 네트워크 와 방화벽을 관리하므로 ToAllSat라는 재분배 프로파일은 로컬 경로를 GlobalProtect 게이트웨이로 다시 재배포하도록 구성됩니다.

1. 네트워크 > 가상 라우터를 선택한 다음 가상 라우터를 추가합니다.
2. 라우터 설정에서 가상 라우터의 이름 및 인터페이스를 추가합니다.
3. 재배포 프로파일에서 추가를 선택합니다.
   1. 재배포 프로파일의 이름을 **ToAllSat**로 지정하고 **Priority**를 1로 설정합니다.
   2. 재배포를 **Redist**로 설정합니다.
   3. 인터페이스 드롭다운에서**이더넷1/23**을 추가합니다.
   4. 확인을 클릭합니다.
4. 가상 라우터에서 **BGP**를 선택하여 BGP를 구성합니다.
   1. **BGP** > 일반에서 활성화를 선택합니다.
   2. 게이트웨이 IP 주소를 라우터 **ID**(**172.16.22.1**)로, **1000**을 **AS** 번호로 입력합니다.
   3. 옵션 섹션에서 설치 경로를 선택합니다.
   4. **BGP** > 피어 그룹에서, 게이트웨이에 연결되는 모든 위성이 있는 피어 그룹 추가를 클릭합니다.
   5. **BGP** > 레디스트 규칙에서, 이전에 만든 **ToAllSat** 재배포 프로파일을 추가합니다.
5. 확인을 클릭합니다.
6. 재분배 프로파일에 대한 **ethernet1/6**을 사용하여 백업 게이트웨이에서 1~5단계를 반복합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** LSVPN에 가입할 위성 준비.

표시된 구성은 단일 위성의 샘플입니다.

LSVPN 배포에 새 위성을 추가할 때마다 이 구성을 반복합니다.

1. 게이트웨이에 대한 VPN 연결의 터널 엔드포인트로 터널 인터페이스를 구성합니다.
2. IPSec 터널 유형을 GlobalProtect 위성으로 설정하고 GlobalProtect 포털의 IP 주소를 입력합니다.
3. 네트워크 > 가상 라우터를 선택한 다음 가상 라우터를 추가합니다.
4. 라우터 설정에서 가상 라우터의 이름 및 인터페이스를 추가합니다.
5. 가상 라우터 > 재분배 프로파일을 선택한 다음 설정으로 프로파일을 추가합니다.
   1. 재배포 프로파일 **ToLSVPNGW**의 이름을 지정하고 우선 순위를 1로 설정합니다.
   2. 인터페이스 **이더넷1/2.1**을 추가합니다.
   3. 확인을 클릭합니다.
6. **BGP** > 일반, **BGP** 활성화를 선택하고 프로토콜을 다음과 같이 구성합니다.
   1. 게이트웨이 IP 주소를 라우터 **ID**(**172.16.22.1**)로, **1000**을 **AS** 번호로 입력합니다.
   2. 옵션 섹션에서 설치 경로를 선택합니다.
   3. **BGP** > 피어 그룹에서, 게이트웨이에 연결되는 모든 위성이 포함된 피어 그룹을 추가합니다.
   4. **BGP** > 레디스트 규칙에서, 이전에 만든 **ToLSVPNGW** 재배포 프로파일을 추가합니다.
7. 확인을 클릭합니다.

**STEP 7 |** LSVPN을 위한 글로벌 보호 포털 구성.

두 데이터 센터 모두 경로를 광고하지만 활성 데이터 센터가 선호하는 게이트웨이인지 확인하기 위해 라우팅 우선 순위가 다릅니다.

1. 네트워크 > **GlobalProtect** > 포털을 선택한 다음 추가를 클릭합니다.
2. 일반에서 포털 이름으로 **LSVPN-Portal**을 입력합니다.
3. 네트워크 설정에서 **ethernet1/21**을 인터페이스로 선택하고 **172.16.22.1/24**를 **IP** 주소로 선택합니다.
4. 인증 탭의 **SSL/TLS** 서비스 프로파일 드롭다운 메뉴에서 이전에 만든 기본 게이트웨이 SSL/TLS 프로파일 **LSVPN-Scale**을 선택합니다.
5. 위성 탭에서 위성을 추가하고 이름을 **sat-config-1**로 지정합니다.
6. 구성 새로 고침 간격을 **12**로 설정합니다.
7. **GlobalProtect** 위성 > 디바이스에서 LSVPN의 각 위성 디바이스의 일련번호와 호스트 이름을 추가합니다.
8. **GlobalProtect** 위성 > 게이트웨이에서 각 게이트웨이의 이름과 IP 주소를 추가합니다. 활성 데이터 센터가 기본 게이트웨이인지 확인하기 위해 기본 게이트웨이의 라우팅 우선 순위를 1로 설정하고 백업 게이트웨이를 10으로 설정합니다.

**STEP 8 |** LSVPN 구성 확인.

 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** (선택 사항) LSVPN 배포에 새 사이트를 추가합니다.

1. 네트워크 > **GlobalProtect** > 포털 > **GlobalProtect** 포털 > 위성 구성 > **GlobalProtect** 위성 > 디바이스를 선택하여 신규 위성의 일련번호를 GlobalProtect 포털에 추가합니다.
2. GlobalProtect 포털 IP 주소로 위성의 IPSec 터널을 구성합니다.
3. 네트워크 > 가상 라우터 > **BGP** > 피어 그룹을 선택하여 각 게이트웨이의 BGP 피어 그룹 구성에 위성을 추가합니다.
4. 네트워크 > 가상 라우터 > **BGP** > 피어 그룹을 선택하여 새 위성의 BGP 피어 그룹 구성에 게이트웨이를 추가합니다.


©2023 Palo Alto Networks, Inc.

# 정책

정책을 통해 규칙을 시행하고 조치를 취할 수 있습니다. 방화벽에서 만들 수 있는 다양한 유형의 정책 규칙은 다음과 같습니다. 보안, NAT, QoS(서비스 품질), PBF(정책 기반 포워딩), 복호화, 애플리케이션 재정의, 인증, 서비스 거부(DoS) 및 영역 보호 정책. 이러한 모든 정책은 네트워크 보안을 위해 필요에 따라 허용, 거부, 우선 순위 지정, 포워딩, 암호화, 복호화, 예외 설정, 액세스 인증 및 연결 재설정을 위해 함께 작동합니다. 다음 항목에서는 정책 작업 방법에 대해 설명합니다.


- 정책 유형
- 보안 정책
- 정책 개체
- 보안 프로파일
- 규칙 베이스 내에서 규칙 추적
- 정책 규칙 설명, 태그 및 감사 설명 적용
- 정책 규칙 또는 개체를 다른 가상 시스템으로 이동 또는 복제
- 주소 개체를 사용하여 IP 주소 표시
- 태그를 사용하여 개체를 그룹화하고 시각적으로 구분합니다.
- 정책에서 외부 동적 목록 사용
- 동적으로 IP 주소 및 태그 등록
- 정책에서 동적 사용자 그룹 사용
- 자동 태그 지정을 사용하여 보안 작업 자동화
- 가상 환경의 변화 모니터링
- 동적 IP 주소 및 태그에 대한 CLI 명령
- 프록시 서버를 통해 연결된 사용자 식별
- 정책 기반 포워딩
- 테스트 정책 규칙

# 정책 유형

Palo Alto Networks 차세대 방화벽은 네트워크에서 애플리케이션을 안전하게 활성화하기 위해 함께 작동하는 다양한 정책 유형을 지원합니다.

모든 정책 유형에 대해 정책 규칙 설명, 태그 및 감사 설명 적용인 경우 감사 설명 아카이브를 사용하여 시간 경과에 따른 정책 규칙 변경 방법을 볼 수 있습니다. 감사 설명 기록 및 구성 로그가 포함된 아카이브를 사용하면 구성 버전을 비교하고 누가 생성 또는 수정했는지, 그 이유를 검토할 수 있습니다.

| 정책 유형 | 설명 |
|---|---|
| 보안 | 소스 및 대상 보안 영역, 소스 및 대상 IP 주소, 애플리케이션, 사용자 및 서비스와 같은 트래픽 속성을 기반으로 세션을 차단할지 또는 허용할지 결정합니다. 자세한 내용은 보안 정책을 참조하십시오. |
| NAT | 번역이 필요한 패킷과 번역 방법을 방화벽에 지시합니다. 방화벽은 소스 주소 및/또는 포트 변환과 데스티네이션 주소 및/또는 포트 변환을 모두 지원합니다. 자세한 내용은 NAT를 참조하십시오. |
| QoS | 정의된 매개변수 또는 여러 매개변수를 사용하여 QoS 처리(우대 처리 또는 대역폭 제한)가 필요한 트래픽을 식별하고 클래스를 할당합니다. 자세한 내용은 서비스 품질을 참조하십시오. |
| 정책 기반 포워딩 | 라우팅 테이블을 기반으로 일반적으로 사용되는 것과 다른 이그레스(egress) 인터페이스를 사용해야 하는 트래픽을 식별합니다. 자세한 내용은 정책 기반 포워딩을 참조하십시오. |
| 복호화 | 가시성, 제어 및 세분화된 보안을 위해 검사하려는 암호화된 트래픽을 식별합니다. 자세한 내용은 복호화를 참조하십시오. |
| 애플리케이션 재정의 | Layer-7 검사인 App-ID 엔진에서 처리하지 않으려는 세션을 식별합니다. 애플리케이션 재정의 정책과 일치하는 트래픽은 방화벽이 세션을 Layer-4에서 정기적인 상태 분석형 방화벽으로 처리하도록 합니다. 자세한 내용은 사용자 지정 또는 알 수 없는 애플리케이션 관리를 참조하십시오. |
| 인증 | 사용자가 인증해야 하는 트래픽을 식별합니다. 자세한 내용은 인증 정책을 참조하십시오. |
| DoS 보호 | 잠재적인 서비스 거부(DoS) 공격을 식별하고 규칙 일치에 대응하여 보호 조치를 취합니다. 자세한 내용은 DoS 방어 프로파일을 참조하세요. |


©2023 Palo Alto Networks, Inc.

# 보안 정책

보안 정책은 네트워크 자산을 위협 및 중단으로부터 보호하고 비즈니스 프로세스의 생산성과 효율성을 향상시키기 위해 네트워크 리소스를 최적으로 할당하는 데 도움이 됩니다. Palo Alto Networks 방화벽에서 개별 보안 정책 규칙은 소스 및 대상 보안 영역, 소스 및 대상 IP 주소, 애플리케이션, 사용자 및 서비스와 같은 트래픽 특성에 따라 세션을 차단하거나 허용할지의 여부를 결정합니다.

최종 사용자가 네트워크 리소스에 액세스하려고 할 때 인증되도록 방화벽은 보안 정책 전에 인증 정책을 평가합니다.

방화벽을 통과하는 모든 트래픽은 세션과 일치하며 각 세션은 보안 정책 규칙과 일치합니다. 세션 일치가 발생하면 방화벽은 해당 세션의 양방향 트래픽(클라이언트 대 서버 및 서버 대 클라이언트)에 일치하는 보안 정책 규칙을 적용합니다. 정의된 규칙과 일치하지 않는 트래픽의 경우 기본 규칙이 적용됩니다. 보안 규칙 베이스의 맨 아래에 표시되는 기본 규칙은 모든 영역 내 트래픽(영역 내)을 허용하고 모든 영역 간 트래픽(영역 간)을 거부하도록 미리 정의되어 있습니다. 이러한 규칙은 사전 정의된 구성의 일부이며 기본적으로 읽기 전용이지만 태그, 작업(허용 또는 차단), 로그 설정 및 보안 프로파일을 비롯한 제한된 수의 설정을 재정의하고 변경할 수 있습니다.

보안 정책 규칙은 왼쪽에서 오른쪽으로, 위에서 아래로 평가됩니다. 패킷은 정의된 기준을 충족하는 첫 번째 규칙과 일치하며 일치가 트리거된 후 사후 규칙이 평가되지 않습니다. 따라서 최상의 일치 조건을 적용하려면 보다 구체적인 규칙이 더 많은 일반 규칙을 선행해야 합니다. 규칙과 일치하는 트래픽은 해당 규칙에 대한 로깅을 활성화하면 트래픽 로그의 세션 끝에 로그 항목을 생성합니다. 로깅 옵션은 각 규칙에 대해 구성할 수 있으며, 예를 들어 세션 종료 시 로깅 대신 또는 추가로 세션 시작 시 로깅하도록 구성할 수 있습니다.

관리자가 규칙을 구성한 후 정책 규칙 사용을 확인하여 트래픽이 보안 정책 규칙과 일치하는 시기와 횟수를 결정하여 효율성을 결정할 수 있습니다. 규칙 기반이 발전함에 따라 규칙이 생성또는 수정될 때 이 정보를 보관하지 않는 한 시간이 지남에 따라 변경 및 감사 정보가 손실됩니다. 모든 관리자가 감사 주석을 입력하도록 정책 규칙 설명, 태그 및 감사 설명 적용을(를) 할 수 있으므로 감사 주석 아카이브를 보고 주석 및 구성 로그 기록을 검토하고 선택한 규칙에 대한 규칙 구성 버전을 비교할 수 있습니다. 이제 규칙베이스에 대한 가시성과 제어가 더 많아졌습니다.

- 보안 정책 규칙의 구성 요소
- 보안 정책 조치
- 보안 정책 규칙 생성

## 보안 정책 규칙의 구성 요소

보안 정책 규칙 구성은 다음 표에 자세히 설명된 대로 필수 필드와 선택적 필드의 조합을 허용합니다. 원본 또는 대상 주소에서 와일드카드 주소 개체를 사용하는 방법에 대한 자세한 내용은 다음 표에 나와 있습니다.

| 필수/선택 | 필드 | 설명 |
|---|---|---|
| 필수 | 이름 | 규칙을 식별하는 레이블(최대 63자)입니다. |


©2023 Palo Alto Networks, Inc.

| 필수/선택 | 필드 | 설명 |
|---|---|---|
| | **UUID** | UUID(Universally Unique Identifier)는 이름과 같은 변경 사항에 관계없이 규칙을 추적할 수 있도록 규칙을 영구적으로 식별하는 고유한 32자 문자열입니다. |
| | 규칙 유형 | 규칙이 영역 내, 영역 간 또는 둘 다에 적용되는지의 여부를 지정합니다.<br>• 범용(기본값) - 지정된 소스 및 대상 영역에서 일치하는 모든 영역 간 및 영역 내 트래픽에 규칙을 적용합니다. 예를 들어 소스 영역 A와 B, 대상 영역 A와 B가 있는 범용 규칙을 생성하는 경우 규칙은 영역 A 내의 모든 트래픽, 영역 B 내의 모든 트래픽, 영역 A에서 영역 B로의 모든 트래픽 및 모든 영역 B에서 영역 A로의 트래픽<br>• 인트라존**(intrazone)** - 지정된 소스 영역 내에서 일치하는 모든 트래픽에 규칙을 적용합니다(인트라존(intrazone) 규칙에 대해 대상 영역을 지정할 수 없음). 예를 들어 소스 영역을 A와 B로 설정하면 규칙은 영역 A 내의 모든 트래픽과 영역 B 내의 모든 트래픽에 적용되지만 영역 A와 B 사이의 트래픽에는 적용되지 않습니다.<br>• 인터존**(interzone)** - 지정된 소스 영역과 대상 영역 간에 일치하는 모든 트래픽에 규칙을 적용합니다. 예를 들어 소스 영역을 A, B, C로 설정하고 대상 영역을 A와 B로 설정하면 규칙이 영역 A에서 영역 B로, 영역 B에서 영역 A로, 영역 C에서 영역으로의 트래픽에 적용됩니다. A, 영역 C에서 영역 B로 이동하지만 영역 A, B 또는 C 내 트래픽은 허용되지 않습니다. |
| | 소스 영역 | 트래픽이 시작된 영역입니다. |
| | 대상 영역 | 트래픽이 종료되는 영역입니다. NAT를 사용하는 경우 항상 post-NAT 영역을 참조해야 합니다. |
| | 애플리케이션 | 제어하려는 애플리케이션입니다. 방화벽은 트래픽 분류 기술인 App-ID를 사용하여 네트워크의 트래픽을 식별합니다. App-ID는 알려지지 않은 애플리케이션을 차단하는 보안 정책을 생성할 때 애플리케이션 제어 및 가시성을 제공하는 동시에 허용되는 애플리케이션을 활성화, 검사 및 형성합니다. |
| | 동작 | 규칙에 정의한 기준에 따라 트래픽에 대한 허용 또는 거부 작업을 지정합니다. 트래픽을 거부하도록 방화벽을 구성하면 연결이 재설정되거나 패킷이 자동으로 삭제됩니다. 더 나은 사용자 경험을 제공하기 위해 패킷을 자동으로 삭제하는 대신 트래픽을 거부하도록 세분화된 옵션을 구성할 수 있습니다. 그러면 일부 애플리케이션이 중단되고 사용자에게 응답하지 않는 것처럼 보일 수 있습니다. 자세한 내용은 보안 정책 작업을 참조하십시오. |


©2023 Palo Alto Networks, Inc.

| 필수/선택 | 필드 | 설명 |
|---|---|---|
| 선택 사항 | 태그 | 보안 규칙을 필터링할 수 있는 키워드 또는 구문입니다. 이는 많은 규칙을 정의한 다음 *IT* 승인 애플리케이션 또는 고위험 애플리케이션과 같은 키워드로 태그가 지정된 규칙을 검토하려는 경우에 유용합니다. |
| | 설명 | 규칙을 설명하는 데 사용되는 최대 1024자의 텍스트 필드입니다. |
| | 소스 주소 | 호스트 IP 주소, 서브넷, 주소 개체(IP 넷마스크, IP 범위, FQDN 또는 IP 와일드카드 마스크 유형), 주소 그룹 또는 국가 기반 시행을 정의합니다. NAT를 사용하는 경우 항상 패킷의 원래 IP 주소(즉, pre-NAT IP 주소)를 참조해야 합니다. IP 와일드카드 마스크에 대한 자세한 내용은 다음 표를 참조하십시오. |
| | 대상 주소 | 패킷의 위치 또는 대상입니다. IP 주소, 서브넷, 주소 개체(IP 넷마스크, IP 범위, FQDN 또는 IP 와일드카드 마스크 유형), 주소 그룹 또는 국가 기반 시행을 정의합니다. NAT를 사용하는 경우 항상 패킷의 원래 IP 주소(즉, pre-NAT IP 주소)를 참조해야 합니다. IP 와일드카드 마스크에 대한 자세한 내용은 다음 표를 참조하십시오. |
| | 사용자 | 정책이 적용되는 사용자 또는 사용자 그룹입니다. 영역에서 사용자 ID를 활성화해야 합니다. User-ID를 활성화하려면 User-ID 개요를 참조하십시오. |
| | **URL** 카테고리 | URL 카테고리를 일치 기준으로 사용하면 URL 카테고리별로 보안 프로파일(안티바이러스, 안티스파이웨어, 취약성, 파일 차단, 데이터 필터링 및 DoS)을 사용자 지정할 수 있습니다. 예를 들어, 더 높은 위험을 나타내는 URL 카테고리에 대해서는 prevent.exe 파일 다운로드/업로드를 허용하고 다른 카테고리에는 허용할 수 있습니다. 이 기능을 사용하면 특정 URL 카테고리에 일정을 첨부하고(점심 시간 및 근무 시간 이후에 소셜 미디어 웹사이트 허용), 특정 URL 카테고리에 QoS(금융, 의료 및 비즈니스)를 표시하고, per-URL-category-basis에서 다른 로그 포워딩 프로파일을 선택합니다.<br><br>방화벽에서 URL 카테고리를 수동으로 구성할 수 있지만 Palo Alto Networks 방화벽에서 사용할 수 있는 동적 URL 카테고리화 업데이트를 활용하려면 URL 필터링 라이선스를 구매해야 합니다.<br><br>*URL* 카테고리에 따라 트래픽을 차단하거나 허용하려면 보안 정책 규칙에 *URL* 필터링 프로파일을 적용해야 합니다. *URL* 카테고리를 *Any*로 정의하고 *URL* 필터링 프로파일을 보안 정책에 연결합니다. 보안 정책의 기본 프로파일 사용에 대한 자세한 내용은 기본 보안 정책 설정을 참조하십시오. |

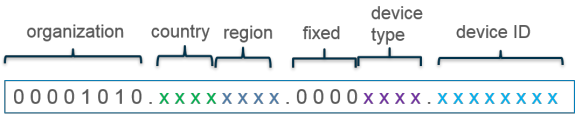

©2023 Palo Alto Networks, Inc.

| 필수/선택 | 필드 | 설명 |
|---|---|---|
| | 서비스 | 애플리케이션에 대한 레이어 4(TCP 또는 UDP) 포트를 선택할 수 있습니다. 임의를 선택하거나, 포트를 지정하거나, ***application-default***를 사용하여 애플리케이션에 대한 표준 기반 포트의 사용을 허용할 수 있습니다. 예를 들어 DNS와 같이 포트 번호가 잘 알려진 애플리케이션의 경우 애플리케이션 기본 옵션은 TCP 포트 53에서만 DNS 트래픽과 일치합니다. 사용자 지정 애플리케이션을 추가하고 애플리케이션이 사용할 수 있는 포트를 정의할 수도 있습니다.<br><br>인바운드 허용 규칙(예: 신뢰하지 않음에서 신뢰로)의 경우 ***application-default***를 사용하면 애플리케이션이 비정상적인 포트 및 프로토콜에서 실행되지 않습니다. ***Application-default***는 기본 옵션입니다. 방화벽은 여전히 모든 포트의 모든 애플리케이션을 확인하지만 이 구성을 사용하면 애플리케이션은 표준 포트/프로토콜에서만 허용됩니다. |
| | 보안 프로파일 | 위협, 취약성 및 데이터 유출로부터 추가 보호를 제공합니다. 보안 프로파일은 허용 작업이 있는 규칙에 대해서만 평가됩니다. |
| | **HIP** 프로파일(GlobalProtect용) | HIP(호스트 정보 프로파일)로 클라이언트를 식별한 다음 액세스 권한을 적용할 수 있습니다. |
| | 옵션 | 세션에 대한 로깅, 로그 포워딩 설정을 정의하고, 규칙과 일치하는 패킷에 대한 QoS(서비스 품질) 표시를 변경하고, 보안 규칙이 적용되어야 하는 시간(요일 및 시간)을 예약할 수 있습니다. |

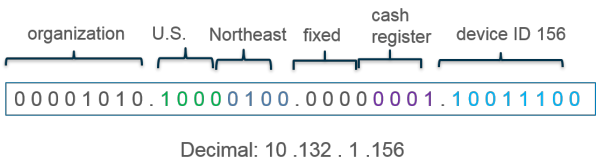
이 섹션에서는 보안 정책 규칙의 원본 주소 또는 대상 주소에서 와일드카드 주소 개체를 사용하는 방법에 대해 설명합니다. 개인 IPv4 주소를 내부 디바이스에 할당할 때 주소의 특정 비트에 의미를 할당하는 IP 주소 지정 구조를 사용할 수 있습니다. 예를 들어 IP 주소의 세 번째 옥텟에 있는 처음 세 비트는 디바이스 유형을 나타냅니다. 이 구조는 디바이스의 IP 주소를 기반으로 디바이스 유형 또는 위치와 같은 디바이스에 대한 세부 정보를 쉽게 식별하는 데 도움이 됩니다. 보안 정책 규칙에서 동일한 IP 주소 지정 구조를 사용하여 보다 쉽게 배포할 수 있습니다. 와일드카드 주소(10.1.2.3/0.127.248.0과 같이 슬래시로 구분된 IP 주소와 와일드카드 마스크)를 사용하는 주소 개체를 만듭니다. 와일드카드 주소는 단일 보안 정책 규칙에서 여러 원본 또는 대상 주소를 식별할 수 있으며, 이는 많은 디바이스를 지원하는 데이터 센터 방화벽에 특히 유용합니다. 일치하는 모든 IP 주소를 커버하거나 IP 주소 용량 제약으로 인해 필요한 것보다 덜 제한적인 보안 정책 규칙을 사용하기 위해 불필요하게 많은 수의 주소 개체를 관리할 필요가 없습니다.

예를 들어, 첫 번째 옥텟이 조직을 나타내는 다음 그림에 표시된 IPv4 주소 지정 체계를 사용한다고 가정해 보겠습니다(00001010 비트는 고정되어 있음). 두 번째 옥텟에서 처음 네 비트는 네트워크 디바이스가 위치한 국가를 지정하고(1000은 미국을 나타냄) 마지막 네 비트는 지역을 나타냅니다(0100은 북동쪽을 나타냄). 세 번째 옥텟에서 처음 네 비트는 0이고 마지막 네 비트는 디바이스 유형을 나타냅니다(0001은 금전 등록기를 나타내고 0011은 프린터를 나타냅니다). 마지막 옥텟은 네트워킹 디바이스의 ID 번호를 나타냅니다.


©2023 Palo Alto Networks, Inc.




이 구조에 따라 미국 북동부의 금전 등록기 번호 156의 IP 주소는 10.132.1.156입니다.




**IP** 와일드카드 마스크 유형의 주소 개체를 사용하여 보안 정책 규칙에서 이러한 주소 지정 구조를 지원할 수 있습니다. IPv4 원본 또는 대상 주소에 와일드카드 마스크를 적용하여 규칙이 적용되는 주소를 지정합니다. Palo Alto Networks 와일드카드 마스크에서 제로 비트는 비교되는 비트가 0으로 커버되는 IP 주소의 비트와 일치해야 함을 나타냅니다. 마스크의 한 비트는 와일드카드 또는 "무시" 비트이며, 이는 비교되는 비트가 IP 주소의 비트와 일치하지 않아도 됨을 의미합니다. 예를 들어 IP 주소 및 와일드카드 마스크의 다음 코드 조각은 네 개의 일치 항목을 생성하는 방법을 보여 줍니다.

```
0011    binary snippet
1010    wildcard mask
--------
0001    yields four matches
0011
1001
1011
```

모든 공급 업체가 와일드 카드 비트로 하나를 사용하고 *0*을 일치하는 비트로 사용하는 것은 아닙니다.

이 예에서 금전 등록기에는 세 번째 옥텟 00000001의 IPv4 주소가 있고 프린터에는 세 번째 옥텟이 00000011 IPv4 주소가 있습니다. 0에서 255 사이의 ID 번호를 가진 모든 금전 등록기 및 프린터에 보안 정책 규칙을 적용하려고 한다고 가정해 보겠습니다. 이 결과를 얻으려면 와일드 카드 마스크가 필요합니다. 와일드카드 마스크의 세 번째 옥텟은 2여야 하고 디바이스 ID(네 번째 옥텟)는 255여야 합니다. 미국 북동부의 모든 금전 등록기 및 프린터를 지정하는 주소 개체는 와일드카드 주소 10.132.1.2/0.0.2.255를 사용합니다.

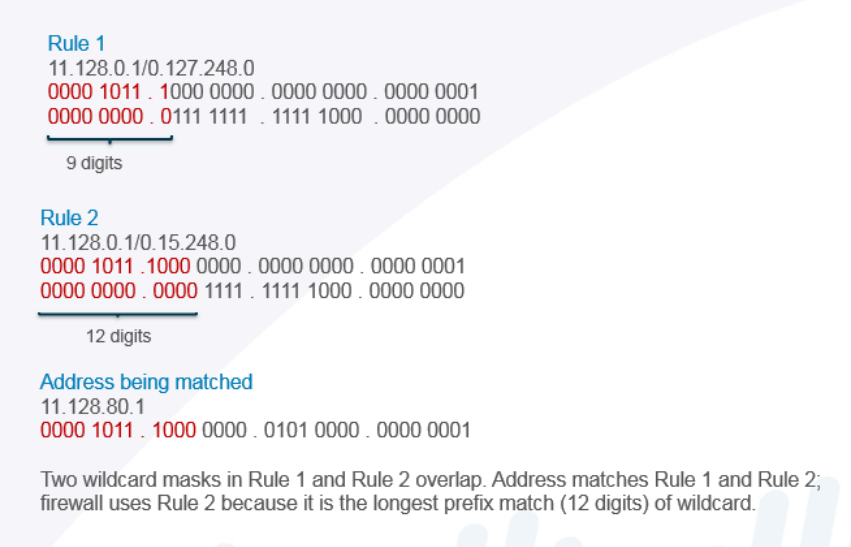
```
0000 1010.1000 0100.0000 0001.0000 0010 (IP address 10.132.1.2)
0000 0000.0000 0000.0000 0010.1111 1111 (wildcard mask 0.0.2.255)
--------------------------------------------------------------------------------
yields these matches:
0000 1010.1000 0100.0000 0001.0000 0000
0000 1010.1000 0100.0000 0001.0000 0001
0000 1010.1000 0100.0000 0001.0000 0010
0000 1010.1000 0100.0000 0001.0000 0011
   ... and so on (fourth octet yields every number from 0 to 255)
and
0000 1010.1000 0100.0000 0011.0000 0000
0000 1010.1000 0100.0000 0011.0000 0001
0000 1010.1000 0100.0000 0011.0000 0010
0000 1010.1000 0100.0000 0011.0000 0011
   ... and so on (fourth octet yields every number from 0 to 255)
```


©2023 Palo Alto Networks, Inc.

따라서 와일드카드 주소가 10.132.1.2/0.0.2.255인 주소 개체를 대상 주소로 사용하는 단일 보안 정책 규칙은 512개 디바이스(금전 등록기 256개 + 프린터 256개)의 주소와 일치하므로 여러 디바이스에 규칙을 적용하는 효율적인 방법입니다. 와일드카드 마스크는 0.0.2.255와 같이 하나 이상의 영(0)으로 시작해야 합니다.

보안 정책 규칙에서 **IP** 와일드카드 마스크 유형의 주소 개체를 사용할 때 다음을 고려하십시오.

- **IP** 와일드카드 마스크 유형의 주소 개체를 사용하는 원본 또는 대상 주소는 **Negate** 옵션을 지원하지 않습니다.
- 방화벽은 섀도 일치를 수행할 때 와일드카드 주소를 고려하지 않으므로 **IP** 와일드카드 마스크 유형의 주소 개체를 사용하는 보안 정책 규칙이 후속 규칙과 겹치거나 목록의 상위 규칙에 의해 겹치는 경우 경고가 표시되지 않습니다.
- 주소가 와일드카드 마스크가 겹치는 규칙과 일치하는 경우 방화벽은 다음 그림과 같이 와일드카드 마스크에서 가장 긴 접두사와 일치하는 항목을 선택합니다.




앞의 글머리 기호는 기본 동작을 설명합니다. 그러나 일부 소스가 일반 애플리케이션(예: Ping, Traceroute 및 웹 브라우징)에 액세스할 수 있도록 허용하는 광범위한 규칙을 사용하지만, 이러한 소스의 하위 집합이 일반 애플리케이션 외에도 다른 애플리케이션(예: SSH, SCP)에 액세스할 수 있도록 허용하는 더 좁은 규칙을 사용하려는 경우가 있습니다. 이전 릴리스에서는 와일드카드 마스크에서 접두사가 가장 긴 규칙과의 일치만 처리되고 다른 규칙은 고려되지 않았기 때문에 이러한 배포가 작동하지 않았습니다.

PAN-OS 10.2.1부터는 와일드카드 하향식 일치 모드를 사용하도록 설정하여 IP 주소가 있는 패킷이 와일드카드 마스크가 겹치는 보안 정책 규칙의 접두사와 일치하는 경우 방화벽이 와일드카드 마스크에서 가장 긴 접두사를 가진 일치하는 규칙을 선택하는 대신 하향식 순서로 첫 번째 완전히 일치하는 규칙을 선택하도록 할 수 있습니다. 겹치는 와일드카드 마스크를 사용하는 규칙의 접두사와 일치하는 패킷이 발견되었습니다. 그런 다음 방화벽은 마스킹을 기반으로 모든 주소 비트와 완전히 일치하는 규칙을 선택합니다. 마스크의 규칙은 와일드카드 또는 "무시" 비트를 나타냅니다. 그런 다음 애플리케이션 및 영역과 같은 다른 규칙 기준을 검토합니다. 다른 규칙 기준을 검사하는 동안 방화벽은 기준과 일치하는 첫 번째 규칙(하향식 순서)을 선택합니다. 다른 규칙은 평가되지 않습니다.

와일드카드 하향식 매치 모드는 둘 이상의 규칙이 서로 다른 패킷에 적용될 가능성이 있음을 의미합니다(일치하는 접두사가 가장 긴 규칙 포함). 보다 구체적인 규칙을 목록의 맨 위에 배치합니다. 예를 들어 더 작은 범위의 일치하는 주소(더 긴 와일드카드 마스크)가 특정 애플리케이션에 액세스하도록 허용할 수 있

 ©2023 Palo Alto Networks, Inc.

으며, 후속 규칙에서는 더 큰 범위의 IP 주소(더 짧은 와일드카드 마스크)가 다른(더 일반적인) 애플리케이션 집합에 액세스하도록 허용할 수 있습니다. 디바이스 > 설정 > 관리를 선택하고 정책 규칙 베이스 설정을 편집하여 와일드카드 하향식 일치 모드를 활성화할 수 있습니다.

다음 예제에서는 와일드카드 하향식 일치 모드를 사용하도록 설정하고 세 가지 보안 정책 규칙을 사용하며, 각각 와일드카드 마스크 주소 개체를 사용하여 원본 IP 주소를 지정하고 와일드카드 마스크가 겹칩니다.

Rule 1: 10.128.0.1/0.127.248.0

0000 1010 1000 0000 0000 0000 0000 0001 IP address
0000 0000 0111 1111 1111 1000 0000 0000 Wildcard Mask
Resulting prefix that matches Rule 1: 10.128.0.1/9

Rule 2: 10.128.0.1/0.15.248.0

0000 1010 1000 0000 0000 0000 0000 0001 IP address
0000 0000 0000 1111 1111 1000 0000 0000 Wildcard Mask
Resulting prefix that matches Rule 2: 10.128.0.1/12

Rule 3: 10.128.0.1/0.127.255.0

0000 1010 1000 0000 0000 0000 0000 0001 IP address
0000 0000 0111 1111 1111 1111 0000 0000 Wildcard Mask
Resulting prefix that matches Rule 3: 10.128.0.1/9

이 예에서 원본 IP 주소가 10.143.8.1(0000 1010 1000 1111 0000 1000 0000 0001)인 클라이언트 A는 규칙 1, 규칙 2 및 규칙 3과 완전히 일치합니다. 첫 번째 일치는 규칙 1(하향식 순서)입니다. 다른 규칙 기준이 일치한다고 가정하면 클라이언트 A의 패킷에는 규칙 1 작업이 적용됩니다.

원본 IP 주소가 10.160 2.1인 클라이언트 B(0000 1010 1010 0000 0000 0010 0000 0001)가 규칙 1의 주소와 완전히 일치하지 않으며 규칙 2의 접두사와 일치하지 않습니다. 클라이언트 B의 주소는 하향식 순서의 첫 번째 일치 규칙인 규칙 3과 완전히 일치합니다. 다른 규칙 기준이 일치한다고 가정하면 클라이언트 B의 패킷에는 규칙 3 작업이 적용됩니다. 따라서 와일드카드 하향식 매치 모드의 이점을 볼 수 있는데, 규칙 1과 규칙 3 모두 서로 다른 패킷에 적용될 수 있습니다.

## 보안 정책 조치

보안 정책에 정의된 특성과 일치하는 트래픽의 경우 다음 작업을 적용할 수 있습니다.

| 동작 | 설명 |
|---|---|
| 허용(기본값) | 트래픽을 허용합니다. |


©2023 Palo Alto Networks, Inc.

| 동작 | 설명 |
| --- | --- |
| 거절 | 트래픽을 차단하고 거부되는 애플리케이션에 대해 정의된 기본 거부 작업을 적용합니다. 애플리케이션에 대해 기본적으로 정의된 거부 작업을 보려면 **Objects** > **Applications**에서 애플리케이션 세부정보를 보거나 Applipedia에서 애플리케이션 세부정보를 확인하십시오. |
| 드롭 | 자동으로 트래픽을 삭제; 애플리케이션의 경우 기본 거부 작업을 재정의합니다. TCP 재설정은 호스트/애플리케이션으로 전송되지 않습니다.<br>레이어 3 인터페이스의 경우 선택적으로 ICMP에 연결할 수 없는 응답을 클라이언트에 보내려면 작업을 설정합니다. 삭제하고 **ICMP Unreachable** 전송 체크박스를 활성화합니다. 사용하도록 설정하면 방화벽이 관리상 금지된 대상과의 통신을 위한 ICMP 코드를 보냅니다. - ICMPv4: 유형 3, 코드 13; ICMPv6: 유형 1, 코드 1. |
| 클라이언트 재설정 | TCP 재설정을 클라이언트 측 디바이스로 보냅니다. |
| 서버 재설정 | 서버 측 디바이스에 TCP 재설정을 보냅니다. |
| 둘 다 재설정 | 클라이언트 측 및 서버 측 디바이스 모두에 TCP 재설정을 보냅니다. |

재설정은 세션이 형성된 후에만 전송됩니다. *3*방향 악수를 완료하기 전에 세션이 차단되면 방화벽이 리셋을 보내지 않습니다.

재설정 작업이 있는 TCP 세션의 경우 방화벽은 ICMP 연결 불가 응답을 보내지 않습니다.

드롭 또는 재설정 작업이 있는 UDP 세션의 경우 **ICMP** 연결 불가 체크박스를 선택한 경우 방화벽은 클라이언트에 ICMP 메시지를 보냅니다.

## 보안 정책 규칙 생성

**STEP 1 |** (선택 사항) 기본 보안 정책 규칙을 삭제합니다.

기본적으로 방화벽에는 트러스트 영역에서 신뢰하지 않는 영역으로의 모든 트래픽을 허용하는 ***rule1***이라는 보안 규칙이 포함되어 있습니다. 규칙을 삭제하거나 영역 명명 규칙을 반영하도록 규칙을 수정할 수 있습니다.

**STEP 2 |** 규칙을 추가합니다.

1. 정책 > 보안을 선택하고 새 규칙을 추가합니다.
2. 일반 탭에서 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. 규칙 유형을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 패킷의 소스 필드에 대한 일치 기준을 정의합니다.

1. 소스 탭에서 소스 영역을 선택합니다.
2. 소스 **IP** 주소를 지정하거나 값을 임의로 설정된 상태로 둡니다.

   지역을 원본 주소로 무효화하기로 결정한 경우 사설 ***IP*** 주소를 포함하는 모든 지역이 원본 주소에 추가되어 해당 사설 ***IP*** 주소 간의 연결 손실을 방지해야 합니다.
3. 소스 사용자를 지정하거나 값을 임의로 설정된 상태로 두십시오.

**STEP 4 |** 패킷의 대상 필드에 대한 일치 기준을 정의합니다.

1. 대상 탭에서 대상 영역을 설정합니다.
2. 대상 **IP** 주소를 지정하거나 임의로 설정된 값을 그대로 둡니다.

   지역을 대상 주소로 무효화하기로 결정한 경우 개인 ***IP*** 주소를 포함하는 모든 지역이 대상 주소에 추가되어 해당 개인 ***IP*** 주소 간의 연결 손실을 방지해야 합니다.

   가장 좋은 방법은 주소 개체를 대상 주소로 사용하여 특히 ***DNS*** 및 ***SMTP***와 같이 일반적으로 악용되는 서비스에 대해 특정 서버 또는 특정 서버 그룹에만 액세스할 수 있도록 하는 것입니다. 사용자를 특정 대상 서버 주소로 제한하여 데이터 유출 및 명령 및 제어 트래픽이 ***DNS*** 터널링과 같은 기술을 통해 통신을 설정하는 것을 방지할 수 있습니다.

**STEP 5 |** 규칙이 허용하거나 차단할 애플리케이션을 지정합니다.

모범 사례로 항상 포트 기반 규칙 대신 애플리케이션 기반 보안 정책 규칙을 사용하고 애플리케이션에 대한 표준 포트보다 더 제한적인 포트 목록을 사용하지 않는 한 항상 서비스를 애플리케이션 기본값으로 설정하십시오.

1. 애플리케이션 탭에서 안전하게 활성화할 애플리케이션 애플리케이션을 추가합니다. 여러 애플리케이션을 선택하거나 애플리케이션 그룹 또는 애플리케이션 필터를 사용할 수 있습니다.
2. 서비스**/URL** 카테고리 탭에서 서비스를 **application-default**로 설정하여 규칙이 허용하는 모든 애플리케이션이 해당 표준 포트에서만 허용되도록 합니다.

**STEP 6 |** (선택 사항) URL 카테고리를 규칙의 일치 기준으로 지정합니다.

서비스**/URL** 카테고리 탭에서 **URL** 카테고리를 선택합니다.

URL 카테고리를 선택하면 웹 트래픽만 규칙과 일치하며 트래픽이 지정된 카테고리로 향하는 경우에만 일치합니다.

**STEP 7 |** 규칙과 일치하는 트래픽에 대해 방화벽이 수행할 작업을 정의합니다.

작업 탭에서 작업을 선택합니다. 각 작업에 대한 설명은 보안 정책 작업을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 로그 설정을 구성합니다.

- 기본적으로 규칙은 세션 종료 시 기록으로 설정됩니다. 트래픽이 이 규칙과 일치할 때 로그가 생성되지 않도록 하려면 이 설정을 비활성화하거나 자세한 로깅을 위해 세션 시작 시 로그를 선택할 수 있습니다.
- 로그 포워딩 프로파일을 선택합니다.



가장 좋은 방법은 ***DSRI(***서버 응답 검사***)*** 비활성화 체크박스를 선택하지 않는 것입니다. 이 옵션을 선택하면 방화벽이 서버에서 클라이언트로 가는 패킷을 검사하지 못합니다. 최상의 보안 상태를 위해 방화벽은 클라이언트에서 서버로의 흐름과 서버에서 클라이언트로의 흐름을 모두 검사하여 위협을 감지하고 방지해야 합니다.

**STEP 9 |** 방화벽이 허용된 모든 트래픽에서 위협을 검색할 수 있도록 보안 프로파일을 연결합니다.



알려진 위협과 알려지지 않은 위협 모두로부터 네트워크를 보호하는 데 도움이 되는 모범 사례 보안 프로파일을 만들어야 합니다.

작업 탭의 프로파일 유형 드롭다운에서 프로파일을 선택한 다음 규칙에 연결할 개별 보안 프로파일을 선택합니다.

또는 프로파일 유형 드롭다운에서 그룹을 선택한 다음 연결할 보안 그룹 프로파일을 선택합니다.

**STEP 10 |** 커밋을 클릭하여 방화벽에서 실행 중인 구성에 정책 규칙을 저장합니다.

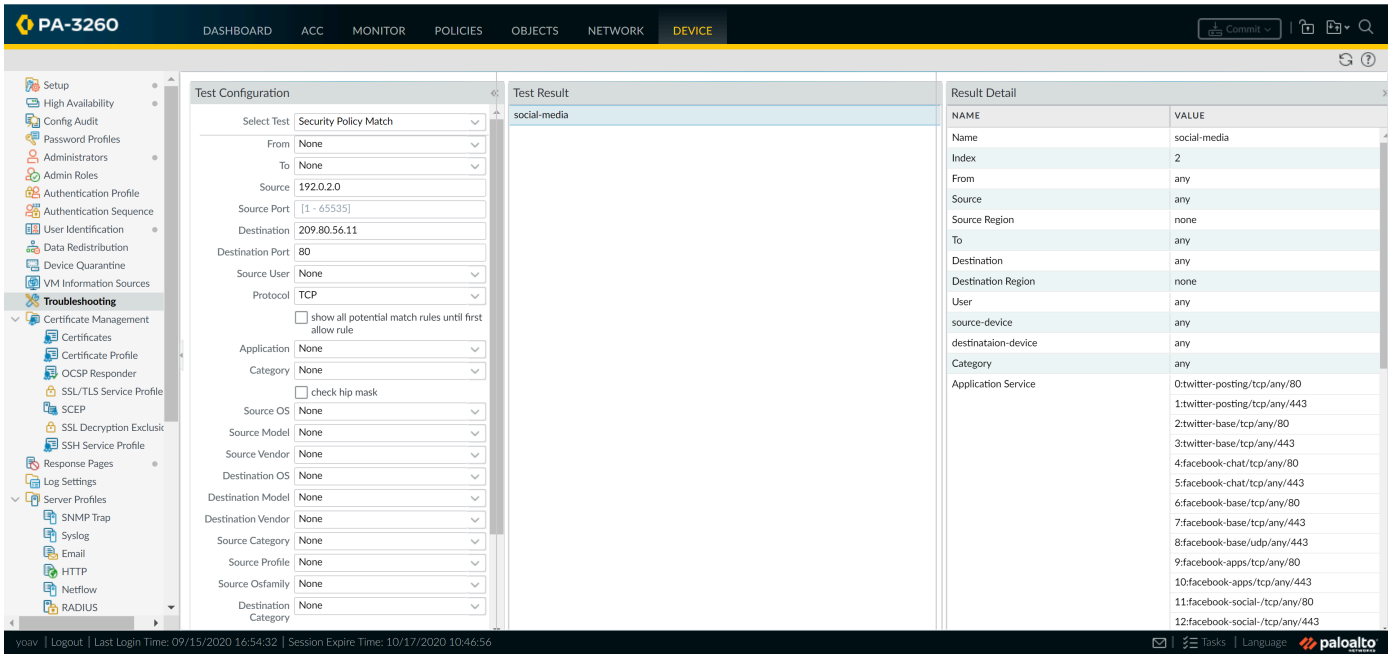

©2023 Palo Alto Networks, Inc.

**STEP 11 |** 기본 보안 정책을 효과적으로 설정했는지 확인하려면 보안 정책 규칙이 평가되고 있는지 테스트하고 트래픽 플로우에 적용되는 보안 정책 규칙을 결정하십시오.

출력은 CLI 명령에 지정된 소스 및 대상 IP 주소와 일치하는 최상의 규칙을 표시합니다.

예를 들어, Microsoft 업데이트 서버에 액세스할 때 IP 주소가 208.90.56.11인 데이터 센터의 서버에 적용될 정책 규칙을 확인하려면:

1. 디바이스 > 문제 해결을 선택하고 테스트 선택 드롭다운에서 보안 정책 일치를 선택합니다.
2. 소스 및 대상 IP 주소를 입력합니다.
3. 프로토콜을 입력합니다.
4. 보안 정책 일치 테스트를 실행합니다.




**STEP 12 |** 트래픽이 방화벽을 통과할 수 있도록 충분히 기다린 후 정책 규칙 사용을 확인하여 정책 규칙 사용 상태를 모니터링하고 정책 규칙의 효과를 확인합니다.


©2023 Palo Alto Networks, Inc.

# 정책 개체

정책 개체는 IP 주소, URL, 애플리케이션 또는 사용자와 같은 개별 ID를 그룹화하는 단일 개체 또는 집합 단위입니다. 집단 단위인 정책 개체를 사용하면 한 번에 여러 개체를 수동으로 선택하는 대신 보안 정책의 개체를 참조할 수 있습니다. 일반적으로 정책 개체를 만들 때 정책에 유사한 권한이 필요한 개체를 그룹화합니다. 예를 들어 조직에서 사용자를 인증하기 위해 서버 IP 주소 집합을 사용하는 경우 서버 IP 주소 집합을 주소 그룹 정책 개체로 그룹화하고 보안 정책의 주소 그룹을 참조할 수 있습니다. 개체를 그룹화하면 정책을 만드는 관리 오버헤드를 크게 줄일 수 있습니다.

내부 검토 또는 감사를 위해 구성의 특정 부분을 내보내야 하는 경우 구성 테이블 데이터를 ***PDF*** 또는 ***CSV*** 파일로 내보낼 수 있습니다.

방화벽에서 다음 정책 개체를 만들 수 있습니다.

| 정책 개체 | 설명 |
|---|---|
| 주소/주소 그룹, 지역 | 동일한 정책 적용이 필요한 특정 소스 또는 대상 주소를 그룹화할 수 있습니다. 주소 개체에는 IPv4 또는 IPv6 주소(단일 IP, 범위, 서브넷), IP 와일드카드 주소(IPv4 주소/와일드카드 마스크) 또는 FQDN이 포함될 수 있습니다. 또는 위도 및 경도 좌표에 의해 영역을 정의하거나 국가를 선택한 다음 IP 주소 또는 IP 범위를 정의할 수 있습니다. 그런 다음 주소 개체의 컬렉션을 그룹화하여 주소 그룹 개체를 만들 수 있습니다.<br><br>동적 주소 그룹을 사용하여 호스트 IP 주소가 자주 변경되는 환경에서 IP 주소를 동적으로 업데이트할 수도 있습니다.<br><br>방화벽의 사전 정의된 외부 동적 목록***(EDL)***은 방화벽 모델이 지원하는 최대 주소 개체 수에 해당합니다. |
| 사용자/사용자 그룹 | 로컬 데이터베이스, 외부 데이터베이스 또는 일치 기준에서 사용자 목록을 생성하고 그룹화할 수 있습니다. |
| 애플리케이션 그룹 및 애플리케이션 필터 | 애플리케이션 필터를 사용하면 애플리케이션을 동적으로 필터링할 수 있습니다. 방화벽의 애플리케이션 데이터베이스에 정의된 특성을 사용하여 애플리케이션 그룹을 필터링하고 저장할 수 있습니다. 예를 들어 카테고리, 하위 카테고리, 기술, 위험, 속성과 같은 하나 이상의 특성으로 애플리케이션 필터를 생성할 수 있습니다. 애플리케이션 필터를 사용하면 콘텐츠 업데이트가 발생할 경우 필터 기준과 일치하는 새 애플리케이션이 저장된 애플리케이션 필터에 자동으로 추가됩니다.<br><br>애플리케이션 그룹을 사용하면 사용자 그룹 또는 특정 서비스에 대해 함께 그룹화하거나 특정 정책 목표를 달성하려는 특정 애플리케이션의 정적 그룹을 만들 수 있습니다. 애플리케이션 그룹 생성을 참조하십시오. |
| 서비스/서비스 그룹 | 서비스가 사용할 수 있는 소스 및 대상 포트 및 프로토콜을 지정할 수 있습니다. 방화벽에는 HTTP에 대해 TCP 포트 80 및 8080을 사용하고 HTTPS에 |


©2023 Palo Alto Networks, Inc.

| 정책 개체 | 설명 |
| --- | --- |
| | 대해 TCP 포트 443을 사용하는 두 개의 사전 정의된 서비스(service-http 및 service-https)가 포함되어 있습니다. 그러나 선택한 TCP/UDP 포트에 있는 사용자 지정 서비스를 만들어 애플리케이션 사용을 네트워크의 특정 포트로 제한할 수 있습니다(즉, 애플리케이션의 기본 포트를 정의할 수 있음).<br> 애플리케이션에서 사용하는 표준 포트를 보려면 개체 > 애플리케이션에서 애플리케이션을 검색하고 링크를 클릭합니다. 간결한 설명이 표시됩니다. |


©2023 Palo Alto Networks, Inc.

# 보안 프로파일

보안 정책 규칙을 사용하면 네트워크의 트래픽을 허용하거나 차단할 수 있지만 보안 프로파일은 허용 하지만 검색 규칙을 정의하는 데 도움이 되며, 이 규칙은 바이러스, 멀웨어, 스파이웨어 및 DDOS 공격과 같은 위협에 대한 애플리케이션을 허용하도록 허용했습니다. 트래픽이 보안 정책에 정의된 허용 규칙과 일치하면 규칙에 연결된 보안 프로파일이 바이러스 백신 검사 및 데이터 필터링과 같은 추가 콘텐츠 검사 규칙에 적용됩니다.



보안 프로파일은 트래픽 플로우의 일치 기준에 사용되지 않습니다. 보안 프로파일은 보안 정책에 의해 애플리케이션 또는 카테고리가 허용된 후 트래픽을 검색하는 데 적용됩니다.

방화벽은 위협으로부터 네트워크를 보호하기 위해 즉시 사용할 수 있는 기본 보안 프로파일을 제공합니다. 보안 정책의 기본 프로파일 사용에 대한 자세한 내용은 기본 보안 정책 설정을 참조하십시오. 네트워크의 보안 요구 사항에 대해 더 잘 이해하려면 인터넷 게이트웨이에 대한 모범 사례 보안 프로파일 생성를 참조하여 사용자 지정 프로파일을 만드는 방법을 알아봅니다.



보안 프로파일에 대한 모범 사례 설정에 대한 권장 사항은 인터넷 게이트웨이에 대한 모범 사례 보안 프로파일 생성을 참조하십시오.

일반적으로 보안 프로파일 그룹 생성에 함께 적용되는 보안 프로파일을 추가할 수 있습니다. 이 프로파일 집합은 하나의 단위로 취급하고 보안 정책에 추가할 수 있습니다(또는 기본 보안 프로파일 그룹을 설정하도록 선택한 경우 기본적으로 보안 정책에 포함).

| 프로파일 유형 | 설명 |
| --- | --- |
| 바이러스 백신 프로파일 | 바이러스 백신 프로파일은 바이러스, 웜 및 트로이 목마뿐만 아니라 스파이웨어 다운로드로부터 보호합니다. Palo Alto Networks 바이러스 백신 솔루션은 첫 번째 패킷이 수신되는 순간 트래픽을 검사하는 스트림 기반 멀웨어 방지 엔진을 사용하여 방화벽 성능에 큰 영향을 주지 않으면서 클라이언트를 보호할 수 있습니다. 이 프로파일은 압축된 파일 내부 스캔 지원 및 데이터 인코딩 구성표를 포함하여 실행 파일, PDF 파일, HTML 및 JavaScript 바이러스에서 다양한 멀웨어를 검사합니다. 방화벽에서 복호화를 사용하도록 설정한 경우 프로파일에서 복호화된 콘텐츠를 검색할 수도 있습니다.<br><br>기본 프로파일은 나열된 모든 프로토콜 디코더를 검사하여 FTP, HTTP 및 SMB 프로토콜을 차단하는 동안 SMTP, IMAP 및 POP3 프로토콜에 대한 경고를 생성합니다. 디코더 또는 바이러스 백신 서명에 대한 작업을 구성하고 방화벽이 위협 이벤트에 어떻게 반응하는지 지정할 수 있습니다.<br><br>• 기본값- Palo Alto Networks가 정의한 각 위협 서명 및 바이러스 백신 서명에 대해 기본 작업이 내부적으로 지정됩니다. 일반적으로 기본 작업은 경고 또는 재설정 둘 다입니다. 기본 작업은 위협 또는 바이러스 백신 서명의 기본값(경고)과 같은 괄호 안에 표시됩니다. |


©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| | • 허용 - 애플리케이션 트래픽을 허용합니다.<br><br>허용 작업은 서명 또는 프로파일과 관련된 로그를 생성하지 않습니다.<br>• 경고 - 각 애플리케이션 트래픽 플로우에 대한 경고를 생성합니다. 경고는 위협 로그에 저장됩니다.<br>• 드롭 - 애플리케이션 트래픽을 삭제합니다.<br>• 클라이언트 재설정 - TCP의 경우 클라이언트 측 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>• 서버 재설정 - TCP의 경우 서버 측 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>• 둘 다 재설정합니다 - TCP의 경우 클라이언트와 서버 끝 모두에서 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br><br>사용자 지정 프로파일을 사용하여 신뢰할 수 있는 보안 영역 간의 트래픽에 대한 안티바이러스 검사를 최소화하고 인터넷과 같은 신뢰할 수 없는 영역에서 수신된 트래픽과 서버 팜(server farm)과 같은 매우 민감한 대상으로 전송된 트래픽의 검사를 최대화할 수 있습니다.<br><br>Palo Alto Networks WildFire 시스템은 또한 다른 안티바이러스 솔루션에서 아직 발견하지 못한 더 회피적이고 지속적인 위협에 대한 서명을 제공합니다. WildFire에서 위협을 발견하면 서명이 빠르게 생성된 다음 Threat Prevention 가입자가 매일(WildFire 가입자의 경우 시간당) 다운로드할 수 있는 표준 바이러스 백신 서명에 통합됩니다. |
| 안티 스파이웨어 프로파일 | 안티 스파이웨어 프로파일은 손상된 호스트의 스파이웨어를 전화 집이나 비콘에서 외부 명령 및 제어(C2) 서버로 차단하여 감염된 클라이언트에서 네트워크를 떠나는 악의적인 트래픽을 감지할 수 있습니다. 영역 간에 다양한 수준의 보호를 적용할 수 있습니다. 예를 들어 신뢰할 수 있는 영역 간의 검사를 최소화하는 사용자 지정 안티 스파이웨어 프로파일을 가지고 인터넷을 향한 영역과 같이 신뢰할 수 없는 영역에서 수신된 트래픽에 대한 검사를 극대화할 수 있습니다. Panorama 관리 서버에서 방화벽을 관리하면 ThreatID가 방화벽의 해당 사용자 지정 위협에 매핑되어 방화벽이 구성된 사용자 지정 ThreatID로 채워진 위협 로그를 생성할 수 있습니다.<br><br>사용자 지정 안티 스파이웨어 프로파일을 정의하거나 보안 정책 규칙에 안티 스파이웨어를 적용할 때 사전 정의된 프로파일 중 하나를 선택할 수 있습니다.<br><br>• 기본값 - 서명이 생성될 때 Palo Alto Networks가 지정한 모든 서명에 대한 기본 작업을 사용합니다.<br>• 강력 - 서명 파일에 정의된 작업에 관계없이 차단 작업에 대한 위험, 높음 및 중간 심각도 위협의 기본 작업을 재정의합니다. 이 프로파일은 여전히 낮은 및 정보 심각도 서명에 대한 기본 작업을 사용합니다. |


©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| | 방화벽이 위협 이벤트를 감지하면 안티 스파이웨어 프로파일에서 다음 작업을 구성할 수 있습니다.<br>• 기본값- Palo Alto Networks가 정의한 각 위협 서명 및 안티 스파이웨어 서명에 대해 기본 작업이 내부적으로 지정됩니다. 일반적으로 기본 작업은 경고 또는 재설정 둘 다입니다. 기본 작업은 위협 또는 바이러스 백신 서명의 기본값(경고)과 같은 괄호 안에 표시됩니다.<br>• 허용 - 애플리케이션 트래픽 허용<br>허용 작업은 서명 또는 프로파일과 관련된 로그를 생성하지 않습니다.<br>• 경고 - 각 애플리케이션 트래픽 플로우에 대한 경고를 생성합니다. 경고는 위협 로그에 저장됩니다.<br>• 드롭 - 애플리케이션 트래픽을 삭제합니다.<br>• 클라이언트 재설정 - TCP의 경우 클라이언트 측 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>• 서버 재설정 - TCP의 경우 서버 측 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>• 둘 다 재설정합니다 - TCP의 경우 클라이언트와 서버 끝 모두에서 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>경우에 따라 프로파일 작업이 ***reset-both***로 설정되면 연결된 위협 로그에 작업이 ***reset-server***로 표시될 수 있습니다. 이 문제는 방화벽이 세션 시작 시 위협을 감지하고 클라이언트에 ***503*** 블록 페이지로 제공될 때 발생합니다. 블록 페이지가 연결을 허용하지 않으므로 클라이언트 측을 재설정할 필요가 없으며 서버 측 연결만 재설정됩니다.<br>• **IP** 차단 - 이 작업은 소스 또는 소스 대상 쌍의 트래픽을 차단합니다. 지정된 기간 동안 구성할 수 있습니다.<br>또한 안티 스파이웨어 프로파일의 DNS 싱홀링 작업을 사용하도록 설정하여 방화벽이 알려진 악성 도메인에 대한 DNS 쿼리에 대한 응답을 위조할 수 있으므로 악의적인 도메인 이름이 정의한 IP 주소로 해결될 수 있습니다. 이 기능은 DNS 트래픽을 사용하여 보호된 네트워크에서 감염된 호스트를 식별하는 데 도움이 됩니다. 그런 다음 싱크홀 IP 주소에 연결하려는 호스트가 멀웨어에 감염될 가능성이 가장 높기 때문에 감염된 호스트는 트래픽 및 위협 로그에서 쉽게 식별할 수 있습니다.<br>안티 스파이웨어 및 취약점 보호 프로파일도 마찬가지로 구성됩니다. |
| 취약점 보호 프로파일 | 취약점 보호 프로파일은 시스템 결함을 악용하거나 시스템에 대한 무단 액세스를 얻으려는 시도를 중지합니다. 안티 스파이웨어 프로파일은 트래픽이 네트워크를 떠날 때 감염된 호스트를 식별하는 데 도움이 되지만 취약점 보호 프로파일은 네트워크에 들어오는 위협으로부터 보호합니다. 예를 들어 취 |


©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| | 약점 보호 프로파일은 버퍼 오버플로, 불법 코드 실행 및 시스템 취약점을 악용하려는 기타 시도로부터 보호하는 데 도움이 됩니다. 기본 Vulnerability Protection 프로파일은 알려진 모든 중요, 높음 및 중간 심각도 위협으로부터 클라이언트와 서버를 보호합니다. 특정 서명에 대한 응답을 변경할 수 있는 예외를 만들 수도 있습니다. Panorama 관리 서버에서 방화벽을 관리하면 ThreatID가 방화벽의 해당 사용자 지정 위협에 매핑되어 방화벽이 구성된 사용자 지정 ThreatID로 채워진 위협 로그를 생성할 수 있습니다.<br><br>방화벽이 위협 이벤트를 감지하면 안티 스파이웨어 프로파일에서 다음 작업을 구성할 수 있습니다.<br>• 기본값- Palo Alto Networks가 정의한 각 위협 서명 및 안티 스파이웨어 서명에 대해 기본 작업이 내부적으로 지정됩니다. 일반적으로 기본 작업은 경고 또는 재설정 둘 다입니다. 기본 작업은 위협 또는 바이러스 백신 서명의 기본값(경고)과 같은 괄호 안에 표시됩니다.<br>• 허용 - 애플리케이션 트래픽 허용<br><br>허용 작업은 서명 또는 프로파일과 관련된 로그를 생성하지 않습니다.<br>• 경고 - 각 애플리케이션 트래픽 플로우에 대한 경고를 생성합니다. 경고는 위협 로그에 저장됩니다.<br>• 드롭 - 애플리케이션 트래픽을 삭제합니다.<br>• 클라이언트 재설정 - TCP의 경우 클라이언트 측 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>• 서버 재설정 - TCP의 경우 서버 측 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br>• 둘 다 재설정합니다 - TCP의 경우 클라이언트와 서버 끝 모두에서 연결을 재설정합니다. UDP의 경우 연결을 삭제합니다.<br><br>경우에 따라 프로파일 작업이 ***reset-both***로 설정되면 연결된 위협 로그에 작업이 ***reset-server***로 표시될 수 있습니다. 이 문제는 방화벽이 세션 시작 시 위협을 감지하고 클라이언트에 ***503*** 블록 페이지로 제공될 때 발생합니다. 블록 페이지가 연결을 허용하지 않으므로 클라이언트 측을 재설정할 필요가 없으며 서버 측 연결만 재설정됩니다.<br>• **IP** 차단 - 이 작업은 소스 또는 소스 대상 쌍의 트래픽을 차단합니다. 지정된 기간 동안 구성할 수 있습니다. |
| URL 필터링 프로파일 | URL 필터링 프로파일을 사용하면 사용자가 HTTP 및 HTTPS를 통해 웹에 액세스하는 방식을 모니터링하고 제어할 수 있습니다. 방화벽에는 알려진 멀웨어 사이트, 피싱 사이트 및 성인 콘텐츠 사이트와 같은 웹사이트를 차단하도록 구성된 기본 프로파일이 함께 제공됩니다. 보안 정책의 기본 프로파일을 사용하거나, 새 URL 필터링 프로파일의 시작점으로 사용할 복사하거나, 네트워크의 트래픽에 대한 가시성을 허용하도록 설정된 모든 카테고리가 설 |

 ©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| | 정된 새 URL 프로파일을 추가할 수 있습니다. 그런 다음 새로 추가된 URL 프로파일을 사용자 지정하고 항상 차단하거나 허용해야 하는 특정 웹사이트 목록을 추가하여 URL 카테고리에 대한 보다 세분화된 제어를 제공합니다. |
| 데이터 필터링 프로파일 | 데이터 필터링 프로파일은 신용카드 또는 주민등록번호와 같은 중요한 정보가 보호된 네트워크로부터 유출되는 것을 방지합니다. 데이터 필터링 프로파일을 사용하면 중요한 프로젝트 이름이나 기밀 단어와 같은 키워드를 필터링할 수도 있습니다. 잘못된 긍정을 줄이기 위해 원하는 파일 유형에 프로파일을 집중하는 것이 중요합니다. 예를 들어 Word 문서 또는 Excel 스프레드시트만 검색할 수 있습니다. 웹 브라우징 트래픽 또는 FTP만 검색할 수도 있습니다.<br><br>사용자 지정 데이터 패턴 개체를 생성하고 데이터 필터링 프로파일에 첨부하여 필터링할 정보 유형을 정의할 수 있습니다. 다음을 기반으로 데이터 패턴 개체 생성<br>• 사전 정의된 패턴 - 사전 정의된 패턴을 사용하여 신용카드 및 주민등록번호(대시 포함 또는 제외)를 필터링합니다.<br>• 정규 식 - 문자열을 필터링합니다.<br>• 파일 속성 - 파일 유형에 따라 파일 속성 및 값을 필터링합니다.<br><br>타사 엔드포인트 데이터 손실 방지(***DLP***) 솔루션을 사용하여 파일 속성을 채우고 중요한 콘텐츠를 표시하는 경우 이 옵션을 사용하면 방화벽이 ***DLP*** 정책을 적용할 수 있습니다.<br><br>시작하려면 데이터 필터링을 설정합니다. |
| 파일 차단 프로파일 | 방화벽은 파일 차단 프로파일을 사용하여 지정된 애플리케이션과 지정된 세션 흐름 방향(인바운드/아웃바운드/둘 다)에서 지정된 파일 형식을 차단합니다. 프로파일을 업로드 및/또는 다운로드에 경고하거나 차단하도록 설정할 수 있으며 파일 차단 프로파일의 적용을 받는 애플리케이션을 지정할 수 있습니다. 사용자가 지정된 파일 유형을 다운로드하려고 할 때 표시되는 사용자 지정 블록 페이지를 구성할 수도 있습니다. 이렇게 하면 사용자가 파일을 다운로드할지의 여부를 고려하는 데 시간이 걸릴 수 있습니다.<br><br>사용자 지정 파일 차단 프로파일을 정의하거나 보안 정책 규칙에 파일 차단을 적용할 때 사전 정의된 프로파일 중 하나를 선택할 수 있습니다. 콘텐츠 릴리스 버전 653 이상에서 사용할 수 있는 사전 정의된 프로파일을 사용하면 모범 사례 파일 차단 설정을 신속하게 활성화할 수 있습니다.<br>• 기본 파일 차단 - 덜 민감한 애플리케이션에서 트래픽이 멀웨어 공격 캠페인에 일반적으로 포함되거나 업로드/다운로드에 대한 실제 사용 사례가 없는 파일을 차단할 수 있도록 하는 보안 정책 규칙에 이 프로파일을 연결합니다. 이 프로파일은 PE 파일(.scr, .cpl, .dll, .ocx, .pif, .exe), 자바 파일(.class, .jar), 도움말 파일(.chm, .hlp) 및 .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat 등 잠재적으로 악 |

 ©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| | 의적인 파일 유형의 업로드 및 다운로드를 차단합니다. 또한 암호화된 rar 또는 암호화된 zip 파일을 다운로드하려고 할 때 사용자에게 인증하라는 메시지가 표시됩니다. 이 규칙은 다른 모든 파일 유형에 대해 경고하여 네트워크 안팎으로 들어오는 모든 파일 유형에 대한 완전한 가시성을 제공합니다.<br>• 엄격한 파일 차단- 가장 중요한 애플리케이션에 액세스할 수 있도록 하는 보안 정책 규칙에 이 엄격한 프로파일을 사용합니다. 이 프로파일은 다른 프로파일과 동일한 파일 형식을 차단하고 플래시, .tar, 다단계 인코딩, .cab, .msi, 암호화된 지퍼 파일 및 암호화된 zip 파일을 추가로 차단합니다.<br>다음 작업으로 파일 차단 프로파일을 구성합니다.<br>• 경고 - 지정된 파일 유형이 감지되면 데이터 필터링 로그에서 로그가 생성됩니다.<br>• 블록 - 지정된 파일 유형이 감지되면 파일이 차단되고 사용자 지정 가능한 블록 페이지가 사용자에게 표시됩니다. 데이터 필터링 로그에서도 로그가 생성됩니다.<br>• 계속 - 지정된 파일 유형이 검색되면 사용자 지정 가능한 응답 페이지가 사용자에게 표시됩니다. 사용자는 페이지를 클릭하여 파일을 다운로드할 수 있습니다. 데이터 필터링 로그에서도 로그가 생성됩니다. 이러한 유형의 포워딩 작업은 사용자 상호 작용이 필요하므로 웹 트래픽에만 적용할 수 있습니다.<br>시작하려면 파일 차단을 설정합니다. |
| WildFire Analysis Profiles | WildFire 분석 프로파일을 사용하여 방화벽이 WildFire 분석을 위해 알 수 없는 파일 또는 이메일 링크를 포워딩할 수있도록 합니다. 애플리케이션, 파일 유형 및 전송 방향(업로드 또는 다운로드)을 기반으로 분석을 위해 포워딩할 파일을 지정합니다. 프로파일 규칙과 일치하는 파일 또는 이메일 링크는 규칙에 정의된 분석 위치에 따라 WildFire 퍼블릭 클라우드 또는 WildFire 프라이빗 클라우드(WF-500 어플라이언스로 호스팅됨)를 포워딩합니다. 프로파일 규칙이 WildFire 퍼블릭 클라우드로 파일을 포워딩하도록 설정된 경우 방화벽은 알 수 없는 파일 외에도 기존 바이러스 백신 서명과 일치하는 파일도 포워딩합니다.<br>WildFire 분석 프로파일을 사용하여 WildFire 하이브리드 클라우드 배포를 설정할 수도 있습니다. WildFire 어플라이언스를 사용하여 중요한 파일(예: PDF)을 로컬로 분석하는 경우 WildFire 어플라이언스 분석(예: APK)에 대해 지원되지 않는 덜 민감한 파일 유형(예: APK)을 대상으로 WildFire 퍼블릭 클라우드에서 분석하도록 지정할 수 있습니다. WildFire 어플라이언스와 WildFire 클라우드를 모두 사용하여 분석을 위해 클라우드에서 이미 처리된 파일과 어플라이언스 분석을 위해 지원되지 않는 파일에 대한 신속한 판정을 받을 수 있으며 중요한 콘텐츠를 처리할 수 있는 어플라이언스 용량을 확보할 수 있습니다. |

 ©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| DoS 보호 프로파일 | DoS 방어 프로파일은 DoS(서비스 거부) 보호 정책에 대한 자세한 제어를 제공합니다. DoS 정책을 사용하면 집계 세션 또는 소스 및/또는 대상 IP 주소를 기반으로 인터페이스, 영역, 주소 및 국가 간의 세션 수를 제어할 수 있습니다. Palo Alto Networks 방화벽이 지원하는 두 가지 DoS 방어 메커니즘이 있습니다.<br>• 플러드 보호 - 네트워크가 패킷으로 넘쳐나는 공격을 감지하고 방지하여 반쯤 열려 있는 세션 및/또는 서비스가 각 요청에 응답할 수 없게 됩니다. 이 경우 공격의 소스 주소는 일반적으로 스푸핑됩니다. 새로운 세션의 플러드에 대한 DoS 방어를 참조하십시오.<br>• 리소스 보호 - 세션 소모 공격을 감지하고 방지합니다. 이러한 유형의 공격에서는 시스템의 모든 리소스를 소비하기 위해 가능한 한 많은 완전히 설정된 세션을 설정하는 데 많은 수의 호스트(봇)가 사용됩니다.<br>단일 DoS 방어 프로파일에서 두 가지 유형의 보호 메커니즘을 모두 활성화할 수 있습니다.<br>DoS 프로파일은 수행할 작업 유형과 DoS 정책의 일치 기준에 대한 세부 정보를 지정하는 데 사용됩니다. DoS 프로파일은 SYN, UDP 및 ICMP 플러드에 대한 설정을 정의하여 리소스를 보호하고 최대 동시 연결 수를 정의할 수 있습니다. DoS 방어 프로파일을 구성한 후 DoS 정책에 첨부합니다.<br>DoS 방어를 구성할 때 올바른 임계값을 설정하기 위해 환경을 분석하는 것이 중요하며 DoS 방어 정책을 정의하는 몇 가지 복잡성으로 인해 이 가이드는 자세한 예제로 이동하지 않습니다. |
| 영역 보호 프로파일 | 영역 보호 프로파일은 공격으로부터 영역을 보호하기 위해 특정 네트워크 영역 간에 추가적인 보호를 제공합니다. 프로파일은 전체 영역에 적용해야 하므로 영역을 통과하는 일반 트래픽으로 발생할 수 있는 문제를 방지하기 위해 프로파일을 신중하게 테스트하는 것이 중요합니다. 초당 패킷(pps) 임계값 제한을 영역 보호 프로파일에 정의할 때 임계값은 이전에 설정된 세션과 일치하지 않는 초당 패킷을 기반으로 합니다. |
| 보안 프로파일 그룹 | 보안 프로파일 그룹은 디바이스로 처리한 다음 보안 정책에 쉽게 추가할 수 있는 보안 프로파일 집합입니다. 종종 함께 할당되는 프로파일을 프로파일 그룹에 추가하여 보안 정책 생성을 간소화할 수 있습니다. 기본 보안 프로파일 그룹을 설정할 수도 있습니다 - 새 보안 정책은 기본 프로파일 그룹에 정의된 설정을 사용하여 보안 정책과 일치하는 트래픽을 확인하고 제어합니다. 기본적으로 해당 그룹의 프로파일을 새 보안 정책에 추가할 수 있도록 보안 프로파일 그룹 기본값의 이름을 지정합니다. 이렇게 하면 새 규칙을 만들 때마다 보안 프로파일을 수동으로 추가할 필요 없이 조직의 기본 프로파일 설정을 새 정책에 자동으로 포함할 수 있습니다.<br>보안 프로파일 그룹 생성 및 기본 보안 프로파일 그룹을 설정하거나 재정의할 수 있습니다. |


©2023 Palo Alto Networks, Inc.

| 프로파일 유형 | 설명 |
| --- | --- |
| | 보안 프로파일에 대한 모범 사례 설정에 대한 권장 사항은 인터넷 게이트웨이에 대한 모범 사례 보안 프로파일 생성을 참조하십시오. |

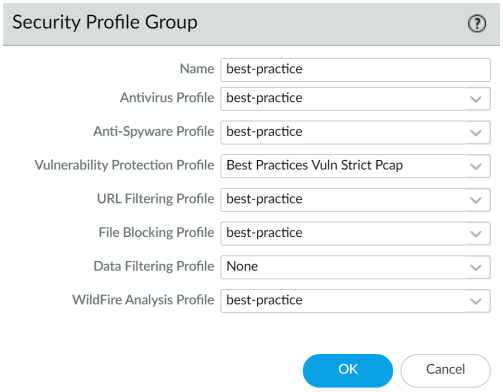
## 보안 프로파일 그룹 생성

다음 단계를 사용하여 보안 프로파일 그룹을 생성하고 보안 정책에 추가합니다.

**STEP 1 |** 보안 프로파일 그룹을 생성합니다.

그룹의 이름을 **기본값**으로 지정하면 방화벽이 사용자가 생성하는 모든 새 규칙에 자동으로 연결합니다. 이것은 모든 새 규칙에 연결되도록 하려는 기본 보안 프로파일 집합이 있는 경우 시간을 절약해 줍니다.

1. 개체 > 보안 프로파일 그룹을 선택하고 새 보안 프로파일 그룹을 추가합니다.
2. 프로파일 그룹에 설명이 포함된 이름을 지정합니다(예: Threats).
3. 방화벽이 다중 가상 시스템 모드인 경우 프로파일이 모든 가상 시스템에서 공유되도록 설정합니다.
4. 그룹에 기존 프로파일을 추가합니다.




5. 확인을 클릭하여 프로파일 그룹을 저장합니다.

**STEP 2 |** 보안 정책에 보안 프로파일 그룹을 추가합니다.

1. 정책 > 보안 및 추가를 선택하거나 보안 정책 규칙을 수정합니다.
2. 작업 탭을 선택합니다.
3. 프로파일 설정 섹션에서 프로파일 유형으로 그룹을 선택합니다.
4. 그룹 프로파일 드롭다운에서 생성한 그룹을 선택합니다(예: 모범 사례 그룹 선택).




5. 확인을 클릭하여 정책을 저장하고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 변경 사항을 저장합니다.

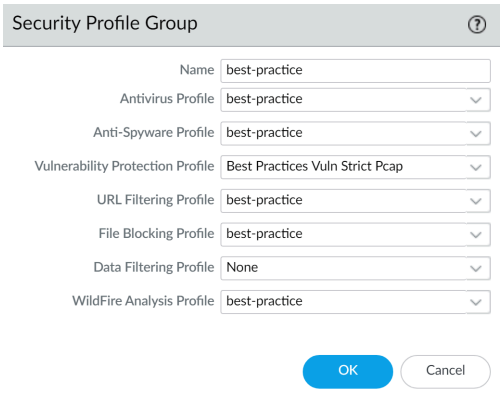
커밋을 클릭합니다.

## 기본 보안 프로파일 그룹 설정 또는 재정의

다음 옵션을 사용하여 새 보안 정책에 사용할 기본 보안 프로파일 그룹을 설정하거나 기존 기본 그룹을 재정의합니다. 관리자가 새 보안 정책을 생성하면 기본 프로파일 그룹이 정책의 프로파일 설정으로 자동 선택되고 프로파일 그룹에 정의된 설정에 따라 정책과 일치하는 트래픽이 확인됩니다(관리자는 원하는 경우 다른 프로파일 설정을 수동으로 선택할 수 있음). 다음 옵션을 사용하여 기본 보안 프로파일 그룹을 설정하거나 기본 설정을 재정의합니다.

기본 보안 프로파일이 없는 경우 새 보안 정책에 대한 프로파일 설정은 기본적으로 없음으로 설정됩니다.

- 보안 프로파일 그룹을 생성합니다.
  1. 개체 > 보안 프로파일 그룹을 선택하고 새 보안 프로파일 그룹을 추가합니다.
  2. 프로파일 그룹에 설명이 포함된 이름을 지정합니다(예: Threats).
  3. 방화벽이 다중 가상 시스템 모드인 경우 프로파일이 모든 가상 시스템에서 공유되도록 설정합니다.
  4. 그룹에 기존 프로파일을 추가합니다. 프로파일 생성에 대한 자세한 내용은 보안 프로파일을 참조하십시오.



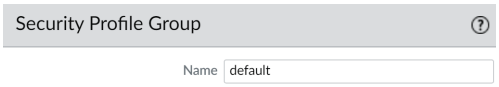

  5. 확인을 클릭하여 프로파일 그룹을 저장합니다.
  6. 보안 정책에 보안 프로파일 그룹을 추가합니다.
  7. 보안 정책 규칙을 추가하거나 수정하고 작업 탭을 선택합니다.
  8. 프로파일 유형으로 그룹을 선택합니다.
  9. 그룹 프로파일 드롭다운에서 생성한 그룹을 선택합니다(예: 위협 그룹 선택).




  10. 확인을 클릭하여 정책을 저장하고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

- 기본 보안 프로파일 그룹을 설정합니다.
  1. 개체 > 보안 프로파일 그룹을 선택하고 새 보안 프로파일 그룹을 추가하거나 기존 보안 프로파일 그룹을 수정합니다.
  2. 이름 보안 프로파일 그룹 기본:

  3. 확인 및 커밋을 클릭합니다.
  4. 기본 보안 프로파일 그룹이 기본적으로 새 보안 정책에 포함되어 있는지 확인합니다.
     1. 정책 > 보안을 선택한 다음 새 보안 정책 추가를 선택합니다.
     2. 작업 탭을 선택한 다음 프로파일 설정 필드를 봅니다.

        기본적으로 새 보안 정책에는 그룹으로 설정된 프로파일 유형이 올바르게 표시되고 기본 그룹 프로파일이 선택됩니다.

- 기본 보안 프로파일 그룹을 재정의합니다.

  기존 기본 보안 프로파일 그룹이 있고 해당 프로파일 집합을 새 보안 정책에 연결하지 않으려는 경우 기본 설정에 따라 프로파일 설정 필드를 계속 수정할 수 있습니다. 먼저 정책에 대해 다른 프로파일 유형을 선택합니다(정책 > 보안 > 보안 정책 규칙 > 작업).

 ©2023 Palo Alto Networks, Inc.

# 규칙 베이스 내에서 규칙 추적

규칙 베이스 내에서 규칙을 추적하려면 규칙베이스의 규칙, 순서에 따라 변경되는 규칙 번호를 참조할 수 있습니다. 규칙 번호는 방화벽이 규칙을 적용하는 순서를 결정합니다.

규칙 이름을 변경할 때와 같이 규칙을 수정하더라도 규칙의 보편적으로 고유 식별자(*UUID*)는 변경되지 않습니다. UUID를 사용하면 규칙을 삭제한 후에도 규칙 베이스에서 규칙을 추적할 수 있습니다.

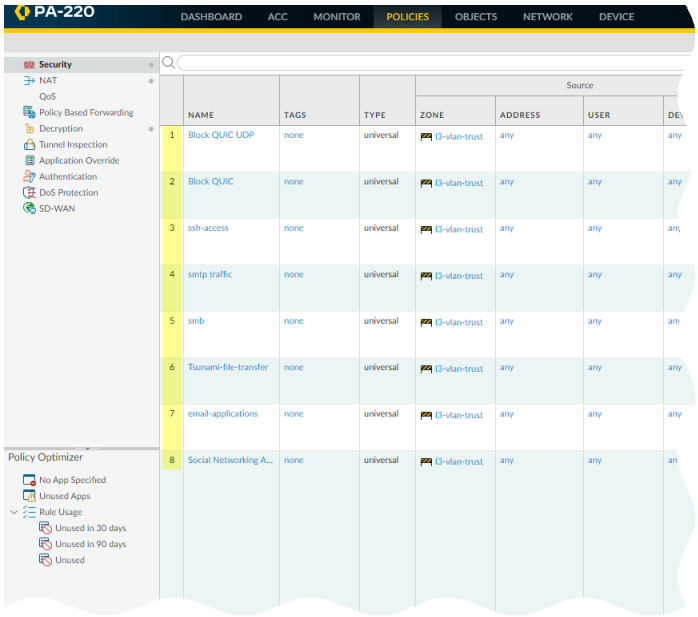
## 규칙 번호

방화벽은 규칙 기준 내에서 각 규칙의 번호를 자동으로 번호로 연결합니다. 규칙을 이동하거나 다시 정렬하면 새 순서에 따라 숫자가 변경됩니다. 규칙 목록을 필터링하여 특정 기준과 일치하는 규칙을 찾을 때 방화벽은 규칙베이스의 전체 규칙 집합과 평가 순서의 해당 위치에 대한 컨텍스트에서 각 규칙을 숫자로 표시합니다.

Panorama는 사전 규칙, 사후-규칙(post-rule) 및 기본 규칙을 독립적으로 번호로 선택합니다. Panorama가 규칙을 방화벽에 푸시할 때 규칙 번호는 공유 규칙, 디바이스 그룹 사전 규칙, 방화벽 규칙, 디바이스 그룹 사후 규칙 및 기본 규칙의 계층 및 평가 순서를 반영합니다. Panorama에서 규칙을 미리 보고 방화벽의 총 규칙 수의 정렬된 목록을 표시할 수 있습니다.

- 방화벽에서 번호가 매겨진 규칙 목록을 봅니다.

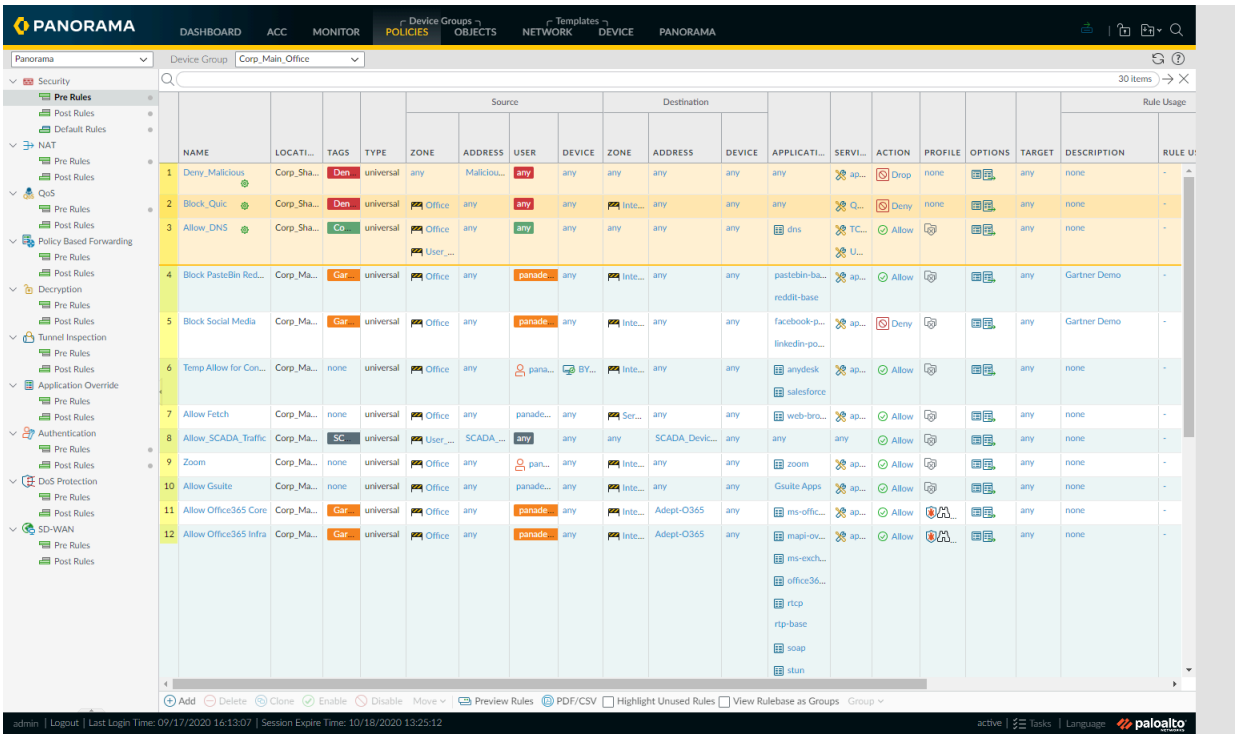
  정책 및 해당 아래에 있는 규칙 기준을 선택합니다. 예를 들어 정책 > 보안이 있습니다. 표의 왼쪽 대부분 열에는 규칙 번호가 표시됩니다.




 ©2023 Palo Alto Networks, Inc.

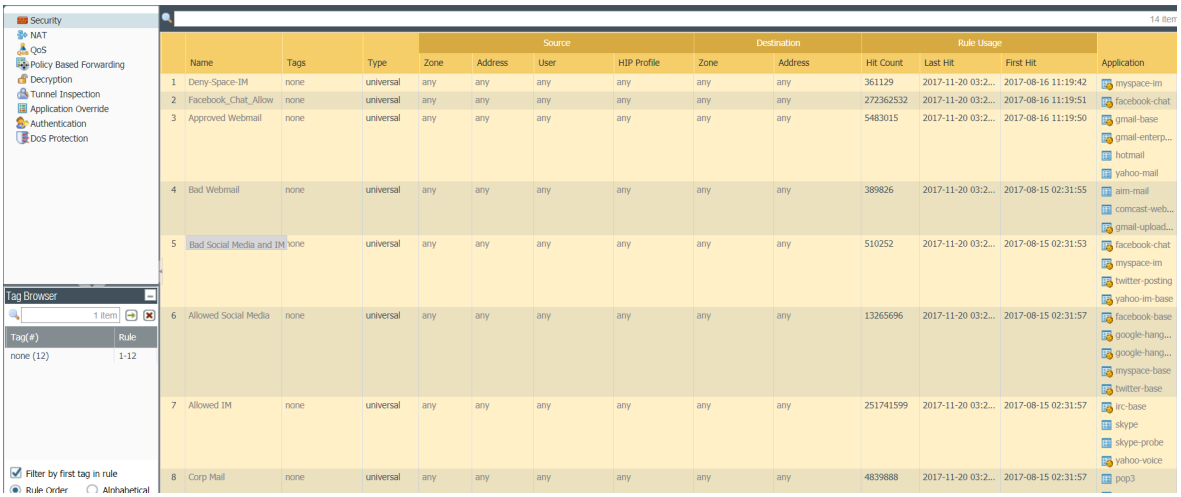
- Panorama에 있는 규칙의 번호가 매겨진 목록을 봅니다.

  정책 및 해당 아래에 있는 규칙 기준을 선택합니다. 예: 정책 > 보안 > 사전 규칙.




- Panorama에서 규칙을 푸시한 후 방화벽에 숫자가 있는 규칙의 전체 목록을 봅니다.

  방화벽의 웹 인터페이스에서 정책을 선택한 다음 그 아래에 있는 규칙 기준을 선택합니다. 예를 들어 정책 > 보안을 선택한 다음 방화벽이 평가할 번호가 매겨진 규칙의 전체 집합을 봅니다.




# 규칙 UUID

규칙에 대한 보편적으로 고유 식별자(UUID)는 방화벽 또는 Panorama가 규칙에 할당하는 32자 문자열(네트워크 주소 및 생성 타임스탬프와 같은 데이터를 기반으로)입니다. UUID는 8-4-4-4-12 형식(8, 4 및 12이 하이픈으로 구분된 고유 문자 수를 나타내는 경우)을 사용합니다. UUID는 모든 정책 규칙 기반에 대


©2023 Palo Alto Networks, Inc.

한 규칙을 식별합니다. UUID를 사용하여 다음 로그 유형에서 적용 가능한 규칙을 식별할 수도 있습니다. 트래픽, 위협, URL 필터링, WildFire 제출, 데이터 필터링, GTP, SCTP, 터널 검사, 구성 및 통합.

UUID를 사용하여 규칙을 검색하면 유사하거나 동일한 이름을 가질 수 있는 수천 개의 규칙 중에서 찾으려는 특정 규칙을 찾을 수 있습니다. 또한 UUID는 이름을 지원하지 않는 타사 시스템(예: 발권 또는 오케스트레이션)의 규칙에 대한 자동화 및 통합을 단순화합니다.

경우에 따라 기존 규칙베이스에 대해 새 UUID를 생성해야 할 수 있습니다. 예를 들어 구성을 다른 방화벽으로 내보내려면 구성을 가져올 때 규칙의 ***UUID***를 재생하여 중복 UUID가 없는지 확인해야 합니다. UUID를 다시 생성하는 경우 이전 UUID를 사용하여 해당 규칙을 더 이상 추적할 수 없으며 해당 규칙에 대한 적중 데이터 및 앱 사용 데이터가 재설정됩니다.

방화벽 또는 Panorama는 다음과 같은 경우 UUID를 할당합니다.

- 새 규칙 생성
- 기존 규칙 복제
- 기본 보안 규칙 재정의
- 명명된 구성로드 및 UUID 재생
- 실행 중인 구성에 없는 새 규칙이 포함된 명명된 구성 로드
- 방화벽 또는 Panorama를 PAN-OS 9.0 릴리스로 업그레이드

UUID와 규칙이 포함된 구성을 로드할 때 방화벽은 규칙 이름, 규칙 기반 및 가상 시스템이 모두 일치하는 경우 규칙을 동일하게 간주합니다. Panorama는 규칙 이름, 규칙 기반 및 디바이스 그룹이 모두 일치하는 경우 규칙을 동일하게 간주합니다.

UUID에 대한 다음 중요한 점을 염두에 두십시오.

- Panorama에서 방화벽 정책을 관리하는 경우 UUID가 Panorama에서 생성되므로 Panorama에서 푸시해야 합니다. 방화벽을 PAN-OS 9.0으로 업그레이드하기 전에 Panorama에서 구성을 푸시하지 않으면 UUID가 없기 때문에 방화벽 업그레이드가 성공하지 못합니다.
- 또한 HA 쌍을 업그레이드하는 경우 PAN-OS 9.0으로 업그레이드하면 각 피어는 각 정책 규칙에 대해 독립적으로 UUID를 할당합니다. 이 때문에 구성(대시보드 > 위젯 > 시스템 > 고가용성 > 동기화)을 동기화할 때까지 피어가 동기화되지 않아 표시됩니다.
- PAN-OS 9.0으로 업그레이드한 후 기존 고가용성(HA) 구성을 제거하는 경우 피어 중 하나에서 UUID를 다시 생성해야 하고(기기 > 설정 > 작업 > 이름이 지정된 구성 스냅샷 로드 > 선택한 이름이 지정된 구성에 대한 **UUID** 재생성), UUID 복제를 방지하기 위해 변경 사항을 커밋합니다.
- Panorama에서 푸시된 모든 규칙은 동일한 UUID를 공유합니다. 방화벽에 로컬되는 모든 규칙에는 다른 UUID가 있습니다. Panorama에서 방화벽으로 규칙을 푸시한 후 방화벽에서 로컬로 규칙을 만들면 로컬로 만든 규칙에는 자체 UUID가 있습니다.
- RMA Panorama를 교체하려면 명명된 Panorama 구성 스냅숏을 로드할 때 규칙 **UUID**를 유지해야 합니다. 이 옵션을 선택하지 않으면 Panorama는 구성 스냅숏에서 이전 규칙 UUID를 모두 제거하고 Panorama의 규칙에 새 UUID를 할당하므로 정책 규칙 적중 수와 같은 이전 UUID와 관련된 정보를 유지하지 않습니다.

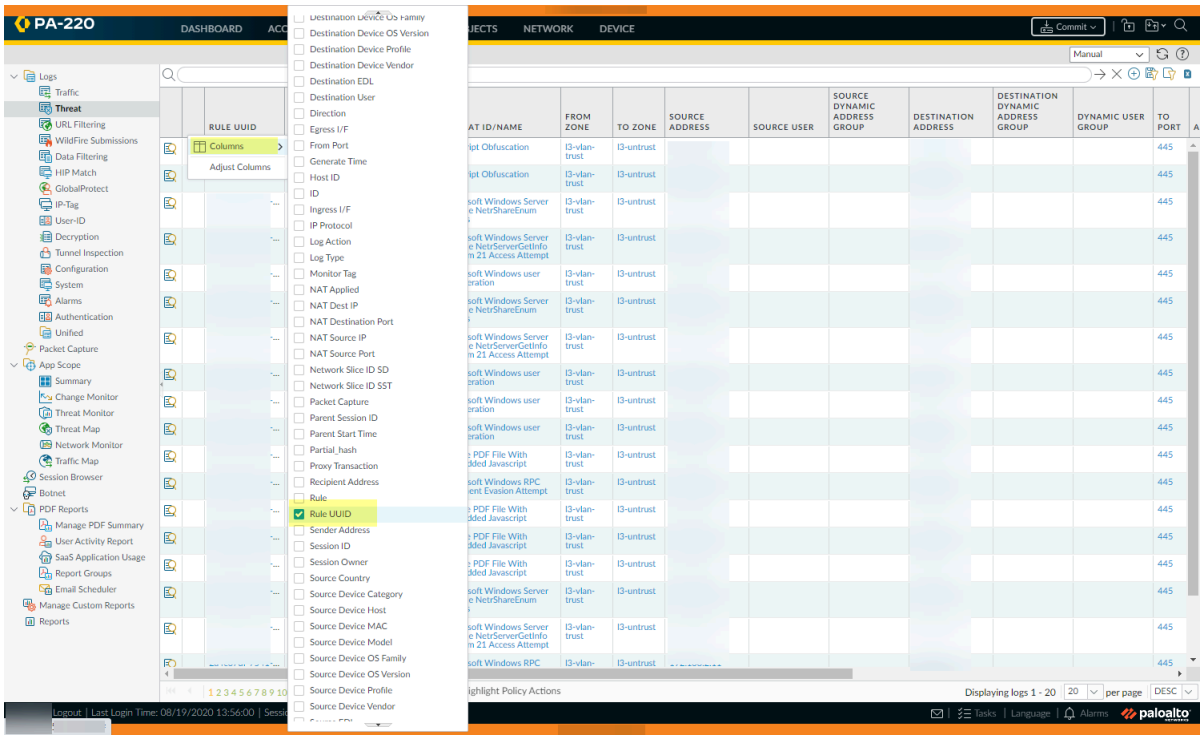
 ©2023 Palo Alto Networks, Inc.

- 로그에 대한 규칙 UUID 열과 정책 규칙에 대한 UUID 열을 표시합니다.

  UUID를 보려면 기본적으로 표시되지 않는 열을 표시해야 합니다.

  - 로그에 UUID를 표시하려면 다음을 수행합니다.

    1. 모니터를 선택한 다음 열 헤더(⌄)를 확장합니다.
    2. 열을 선택합니다.
    3. 규칙 **UUID**를 활성화합니다.

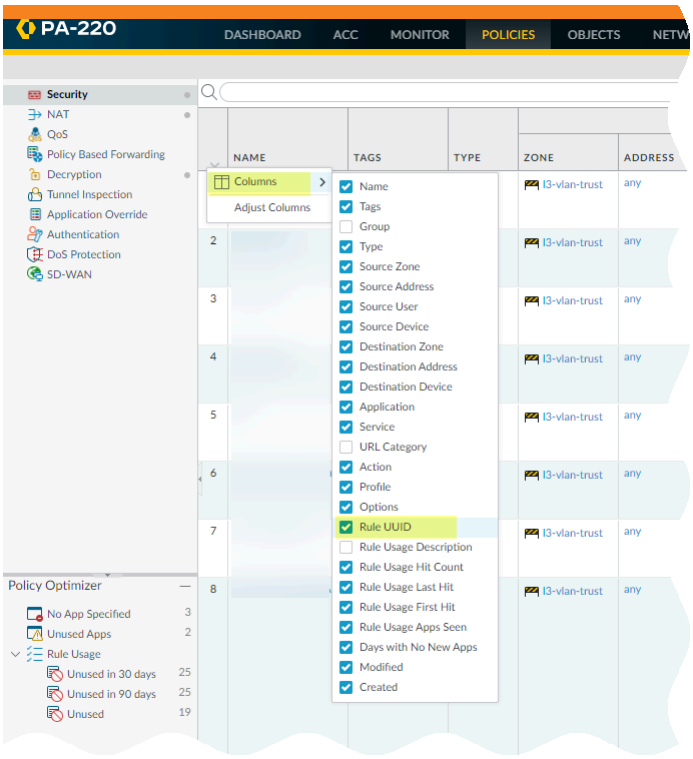



  - 정책 규칙 베이스에 UUID를 표시하려면 다음을 수행하십시오.

    1. 정책을 선택한 다음 열 헤더(⌄)를 확장합니다.
    2. 열을 선택합니다.
    3. 규칙 **UUID**를 활성화합니다.

       UUID는 모든 정책 규칙 베이스에 사용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

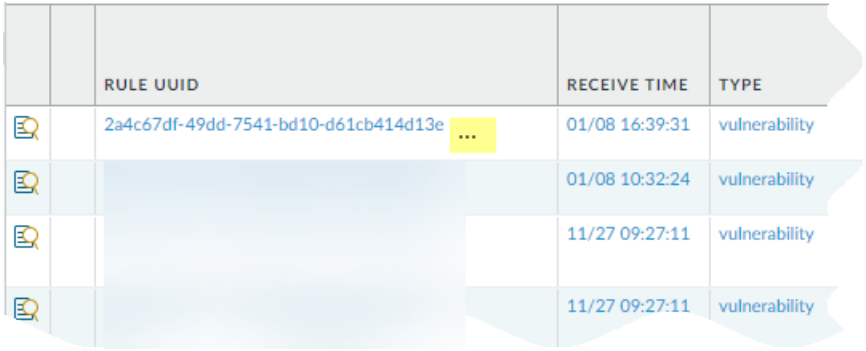



 ©2023 Palo Alto Networks, Inc.

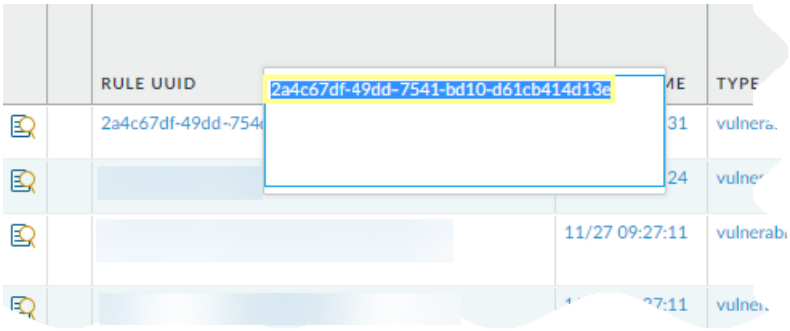
- 로그 또는 정책 규칙에 대한 UUID를 복사합니다.

  UUID를 복사하면 UUID를 검색, ACC, 맞춤 리포트, 필터 및 해당 UUID에서 식별한 규칙을 찾으려는 다른 곳에 붙여넣기할 수 있습니다.

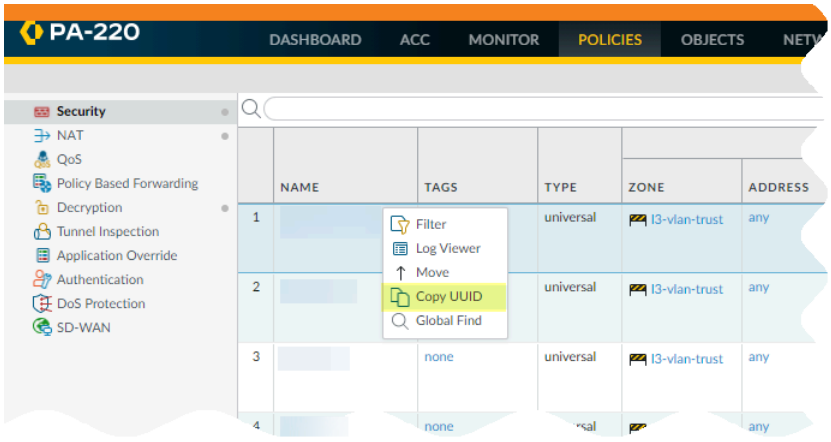
  1. 규칙 UUID 열의 항목 위로 커서를 이동할 때 표시되는 타원을 선택합니다.




  2. 팝업에서 UUID를 복사합니다.




  정책 탭으로 이동하여 규칙 이름 오른쪽에 있는 화살표를 클릭하고 **UUID**를 복사할 수도 있습니다.




- 구성 로그를 확인하여 UUID를 확인하여 삭제된 규칙에 대해 확인합니다.

  삭제된 규칙에 대한 UUID를 보려면 로그 > 구성 > 모니터를 선택합니다.


©2023 Palo Alto Networks, Inc.

# 정책 규칙 설명, 태그 및 감사 설명 적용

규칙을 만들거나 수정할 때 정책 규칙 기반이 올바르게 구성되고 그룹화되었는지 확인하고 감사 목적으로 중요한 규칙 기록을 보존하기 위해 규칙 설명, 태그 및 감사 주석이 필요할 수 있습니다. 규칙 설명, 태그 및 감사 주석을 요구함으로써 규칙이 적절하게 그룹화되고 규칙을 만들거나 수정할 때 규칙 변경 기록을 추적하여 정책 규칙 기준 검토를 간소화할 수 있습니다. 균일성을 위해 감사 주석에 포함할 수 있는 사항에 대한 특정 요구 사항을 설정할 수 있습니다.

기본적으로 설명, 태그 및 감사 주석의 적용이 활성화되지 않습니다. 설명을 지정할 수 있습니다. 태그, 감사 코멘트, 또는 이 세 가지의 조합이 규칙을 성공적으로 추가 하거나 수정 하는 데 필요한지의 여부를 지정할 수 있습니다. 감사 주석 아카이브를 사용하면 선택한 규칙에 대해 입력된 감사 주석을 보고 구성 로그 기록을 검토하고 규칙 구성 버전을 비교할 수 있습니다.

**STEP 1 |** 웹 인터페이스 실행.

**STEP 2 |** 디바이스 > 설정 > 관리를 선택한 다음 정책 규칙 기준 설정을 편집합니다.

**STEP 3 |** 적용할 설정을 구성합니다. 이 예제에서는 모든 정책에 태그 및 감사 주석이 필요합니다.



관리자가 규칙을 만들거나 수정한 이유를 캡처하려면 정책 규칙에 대한 감사 주석을 적용합니다. 정책 규칙에 대한 감사 의견이 필요하면 감사 목적으로 정확한 규칙 기록을 유지하는 데 도움이 됩니다.

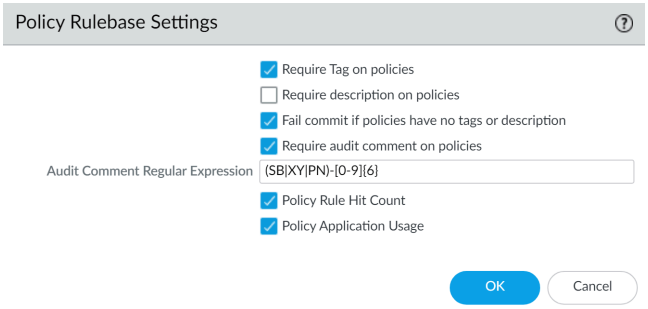
**STEP 4 |** 감사 주석 정규식을 구성하여 감사 주석 형식을 지정합니다.

관리자가 규칙을 만들거나 수정할 때 문자 및 번호 식을 지정하여 해당 감사 주석이 비즈니스에 맞는 특정 형식에 맞는 특정 형식을 준수하는 주석을 입력하도록 요구할 수 있습니다. 예를 들어 이 설정을 사용하여 발권 번호 형식과 일치하는 정규식을 지정할 수 있습니다.

- **[0-9]{<Number of digits>}**—감사 주석에 0에서 9까지의 최소 숫자 수를 포함해야 합니다. 예를 들어 **[0-9]{6}** 숫자 0에서 9까지 숫자 표현식에서 최소 6자리가 필요합니다.
- <문자 식>—감사 주석에 문자 표현 식이 포함되어야 합니다. 예를 들어 **변경 이유**-관리자가 이 문자 표현 식으로 감사 주석을 시작해야 합니다.
- <문자 식>-**[0-9]{<Number of digits>}**—감사주석에 소정의 문자를 포함해야 하며 0에서 9까지의 최소 숫자 수가 필요합니다. 예를 들어 **SB-[0-9]{6}** 감사 주석 형식이 **SB-**로 시작하여 0에서 9까지의 값이 있는 숫자 표현식에서 최소 6자리 숫자가 필요합니다. 예를 들어, **SB-012345**.
- **(**<문자 식>**)|(**<문자 식>**)|(**<문자 식>**)|-[0-9]{<Number of digits>}**-감사 주석에 0에서 9까지의 최소 숫자 수의 미리 정해진 문자 표현식 중 하나를 사용하여 프리픽스를 포함해야 합니다. 예를 들어 **(SB| XY| PN)-[0-9]{6}** 감사 주석 형식이 **SB-**, **XY-**, 또는 **PN-**으로 시작하여 값이 0에서 9까지의 숫자 표현 식에서 최소 6자리 숫자로 시작해야 합니다. 예를 들어, **SB-012345,**, **XY-654321**, 또는 **PN-012543**.

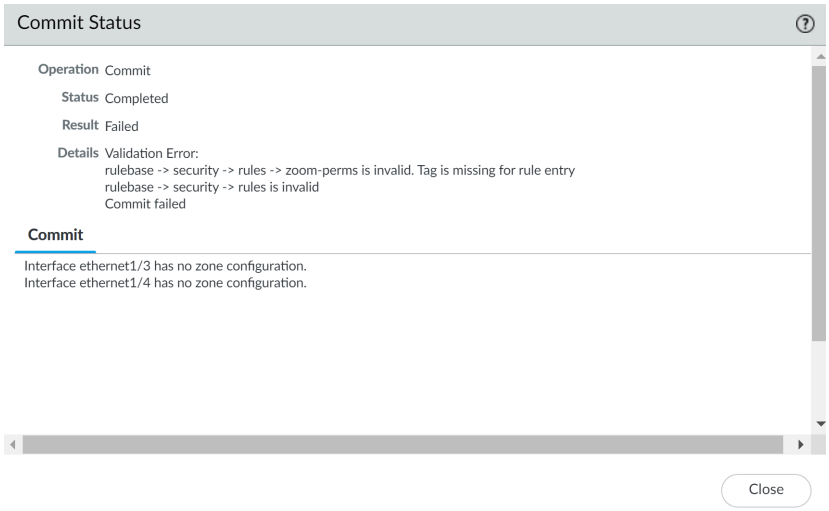
 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 확인을 클릭하여 새 정책 규칙 베이스 설정을 적용합니다.



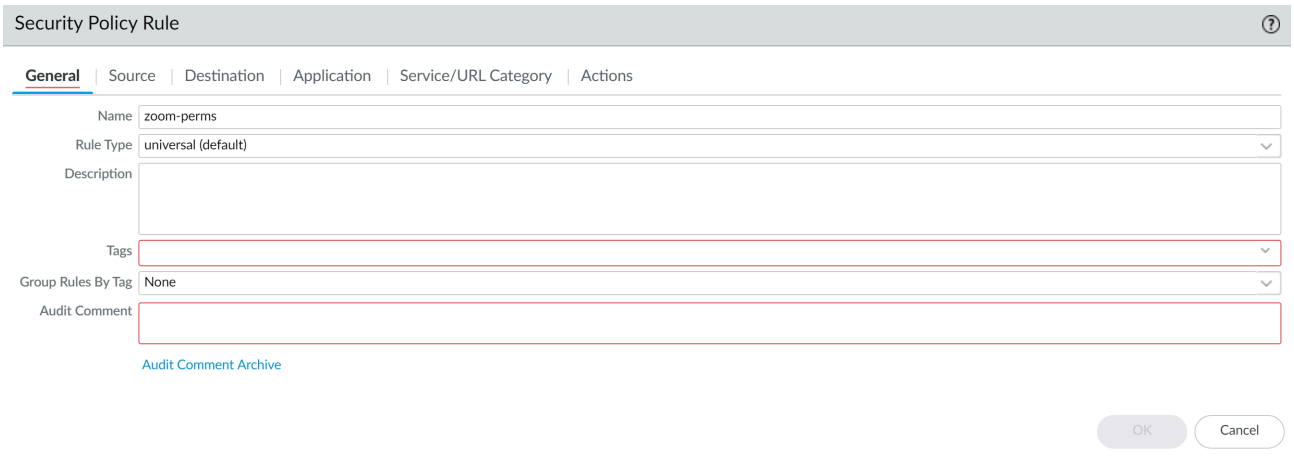

**STEP 6 |** 변경 사항을 커밋합니다.

정책 규칙 기준 설정 변경 내용을 커밋한 후 적용하기로 결정한 규칙 기준 설정에 따라 기존 정책 규칙을 수정합니다.




**STEP 7 |** 방화벽이 새 정책 규칙 기준 설정을 적용하고 있는지 확인합니다.

1. 정책을 선택한 다음 새 규칙을 추가합니다.
2. 태그를 추가하고 감사 댓글 클릭 확인을 입력해야 하는지 확인합니다.





©2023 Palo Alto Networks, Inc.

# 정책 규칙 또는 개체를 다른 가상 시스템으로 이동 또는 복제

둘 이상의 가상 시스템(vsys)이 있는 방화벽에서 정책 규칙 및 개체를 다른 vsys 또는 공유 위치로 이동하거나 복사할 수 있습니다. 이동 및 복사를 수행하면 규칙 및 개체를 삭제, 다시 작성하거나 이름을 바꾸는 수고를 덜 수 있습니다. 가상 시스템에서 이동하거나 복사할 정책 규칙 또는 개체에 해당 가상 시스템의 개체에 대한 참조가 있는 경우 참조된 개체도 이동하거나 복사합니다. 레퍼런스가 공유 개체에 대한 것이라면 이동 또는 복사할 때 레퍼런스를 포함할 필요가 없습니다. 전역 찾기를 사용하여 방화벽 또는 Panorama Management Server에서 레퍼런스를 검색할 수 있습니다.

여러 정책 규칙을 복사할 때 규칙을 선택하는 순서에 따라 디바이스 그룹에 복사되는 순서가 결정됩니다. 예를 들어, 규칙 *1-4*가 있고 선택 순서가 *2-1-4-3*인 경우 이러한 규칙이 복사될 디바이스 그룹은 선택한 것과 동일한 순서로 규칙을 표시합니다. 그러나 성공적으로 복사되면 규칙을 적절하게 재구성할 수 있습니다.

**STEP 1 |** 정책 유형(예: 정책 > 보안) 또는 개체 유형(예: 개체 > 주소)을 선택합니다.).

**STEP 2 |** 가상 시스템을 선택한 다음 하나 이상의 정책 규칙 또는 개체를 선택합니다.

**STEP 3 |** 다음 단계 중 하나를 수행합니다.

- 이동 > 다른 **vsys**로 이동을 선택합니다(정책 규칙의 경우).
- 이동(개체의 경우)을 클릭합니다.
- 복사(정책 규칙 또는 개체의 경우)를 클릭합니다.

**STEP 4 |** 대상 드롭다운에서 새 가상 시스템 또는 공유를 선택합니다.

**STEP 5 |** (정책 규칙만) 규칙 순서를 선택합니다.

- 맨 위로 이동(기본값) - 규칙이 다른 모든 규칙보다 먼저 표시됩니다.
- 맨 아래로 이동 - 규칙이 다른 모든 규칙 다음에 옵니다.
- 사전 규칙 - 인접한 드롭다운에서 선택한 규칙 다음에 오는 규칙을 선택합니다.
- 사후 규칙 - 인접한 드롭다운에서 선택한 규칙 앞에 오는 규칙을 선택합니다.

**STEP 6 |** 유효성 검사에서 처음 감지된 오류 시 오류 출력 체크박스가 기본적으로 선택되어 있습니다. 방화벽은 첫 번째 오류를 발견하면 이동 또는 복사 작업에 대한 검사 수행을 중지하고 이 오류만 표시합니다. 예를 들어 대상 가상 시스템에 이동 중인 정책 규칙이 참조하는 개체가 없을 때 오류가 발생하면 방화벽은 오류를 표시하고 추가 유효성 검사를 중지합니다. 한 번에 여러 항목을 이동하거나 복사할 때 이 체크박스를 선택하면 한 번에 하나의 오류를 찾아 해결할 수 있습니다. 체크박스의 선택을 취소하면 방화벽이 오류 목록을 수집하고 표시합니다. 유효성 검사에 오류가 있으면 모든 오류를 수정할 때까지 개체가 이동되거나 복제되지 않습니다.

**STEP 7 |** 확인을 클릭하여 오류 유효성 검사를 시작합니다. 방화벽에 오류가 표시되면 오류를 수정하고 이동 또는 복사 작업을 다시 시도하십시오. 방화벽이 오류를 찾지 못하면 개체가 성공적으로 이동되거나 복사됩니다. 작업이 완료되면 커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 주소 개체를 사용하여 IP 주소 표시

방화벽에서 주소 개체를 만들어 IP 주소를 그룹화하거나 FQDN을 지정한 다음 방화벽 정책 규칙, 필터 또는 기타 기능에서 주소 개체를 참조하여 규칙, 필터 또는 기타 기능에서 여러 IP 주소를 개별적으로 지정하지 않아도 됩니다.

또한 사용할 때마다 동일한 개별 주소를 지정할 필요 없이 여러 정책 규칙, 필터 또는 기타 기능에서 동일한 주소 개체를 참조할 수 있습니다. 예를 들어 IPv4 주소 범위를 지정하는 주소 개체를 만든 다음 보안 정책 규칙, NAT 정책 규칙 및 맞춤 리포트 로그 필터에서 주소 개체를 참조할 수 있습니다.

- 주소 개체
- 주소 개체 생성

## 주소 개체

주소 개체는 한 곳에서 관리하고 여러 방화벽 정책 규칙, 필터 및 기타 기능에 사용할 수 있는 IP 주소 집합입니다. 주소 객체에는 네 가지 유형이 있습니다. **IP** 넷마스크, **IP** 범위, **IP** 와일드카드 마스크 및 **FQDN**

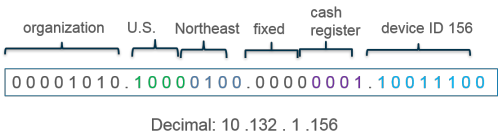
**IP** 넷마스크**, IP** 범위 또는 **FQDN** 유형의 주소 객체는 IPv4 또는 IPv6 주소를 지정할 수 있습니다. **IP** 와일드카드 마스크 유형의 주소 객체는 IPv4 주소만 지정할 수 있습니다.

**IP** 넷마스크 유형의 주소 객체에서는 슬래시 표기법을 사용하여 IPv4 네트워크 또는 IPv6 프리픽스 길이를 나타내는 IP 주소 또는 네트워크를 입력해야 합니다. 192.168.18.0/24 또는 2001:DB 8:123:1#/64를 예로 들 수 있습니다.

**IP** 범위 유형의 주소 개체에서는 하이픈으로 구분된 IPv4 또는 IPv6 주소 범위를 입력해야 합니다.

**FQDN** 유형의 주소 개체 (예: paloaltonetworks.com)는 사용자가 IP 주소를 알고 FQDN이 새 IP 주소로 확인될 때마다 수동으로 업데이트해야 하는 대신 IP 주소에 대한 FQDN 확인을 제공하므로 사용 편의성이 더욱 강화됩니다.

**IP** 와일드카드 마스크 유형의 주소 객체는 내부 디바이스에 프라이빗 IPv4 주소를 정의하고 주소 지정 구조가 주소의 특정 비트에 의미를 할당하는 경우에 유용합니다. 예를 들어, 미국 북동부에 있는 금전 등록기 156의 IP 주소는 다음과 같은 비트 할당을 기준으로 10.132.1.156이 될 수 있습니다.




**IP** 와일드카드 마스크 유형의 주소 객체는 보안 정책 규칙이 적용되는 소스 또는 대상 주소를 지정합니다. 예: 마스크의 **0** 비트는 비교되는 비트가 0으로 처리되는 IP 주소의 비트와 일치해야 함을 나타냅니다. 마스크의 **1**비트 (와일드카드 비트)는 비교되는 비트가 IP 주소의 비트와 일치하지 않아도 됨을 나타냅니다. 다음 IP 주소 및 와일드카드 마스크 스니펫은 네 가지 일치 항목을 산출하는 방법을 보여 줍니다.




 ©2023 Palo Alto Networks, Inc.

주소 개체 생성 이후:

- 보안, 인증, NAT, NAT64, 복호화, DoS 보호, PBF (정책 기반 포워딩), QoS, 애플리케이션 재정의 또는 터널 검사에 대한 정책 규칙에서 또는 NAT 주소 풀, VPN 터널, 경로 모니터링, 외부 동적 목록, 정찰 보호, ACC 전역 필터, 로그 필터 또는 맞춤 리포트 로그 필터에서 **IP** 넷마스크, **IP** 범위 또는 **FQDN** 유형의 주소 개체를 참조할 수 있습니다.
- 보안 정책 규칙에서만 **IP** 와일드카드 마스크 유형의 주소 객체를 참조할 수 있습니다.

## 주소 개체 생성

하나 이상의 IP 주소를 나타내도록 주소 개체을(를) 생성하고, 다음 하나 이상의 정책 규칙, 필터 또는 기타 방화벽 함수의 주소 개체를 참조합니다. 주소 집합을 변경하려면 여러 정책 규칙이나 필터를 변경하지 않고 주소 개체를 한 번 변경하여 운영 오버헤드가 줄어듭니다.

**STEP 1 |** 주소 개체를 생성합니다.

1. 개체 > 주소를 선택하고 이름으로 주소 개체를 추가합니다. 이름은 케이스에 민감하며 고유해야 하며 최대 63자(문자, 숫자, 공간, 하이픈 및 밑줄)일 수 있습니다.
2. 주소 개체 유형을 선택합니다.
   - **IP Netmask** - 단일 IPv4 또는 IPv6 주소, 슬래시 표기표가 있는 IPv4 네트워크 또는 IPv6 주소 및 프리픽스를 지정합니다. 예를 들어 192.168.80.0/24 또는 2001:db8:123:1:1:/64. 선택적으로 **Resolve**를 클릭하여 방화벽 또는 Panorama의 DNS 구성에 따라 연결된 FQDN을 확인합니다. **IP Netmask**에서 **FQDN**으로, 주소 개체 유형을 변경하려면 FQDN을 선택한 다음 이 **FQDN** 사용을 클릭합니다. **FQDN** 및 선택한 FQDN의 형식 변경 내용이 텍스트 필드에 나타납니다.
   - **IP** 범위 - 하이픈으로 구분된 IPv4 주소 또는 IPv6 주소의 범위를 지정합니다. 예를 들어, 192.168.40.1-192.168.40.255 또는 2001:db8:123:1:1:2001:db8:123:1:22.
   - **IP** 와일드카드 마스크 - IP 와일드카드 주소 지정(IPv4 주소 다음에 슬래시와 마스크가 0으로 시작해야 함). 예: 10.5.1.1/0.127.248.2. 마스크의 0(**0**)은 비교되는 비트가 0으로 덮여 있는 IP 주소의 비트와 일치해야 한다는 것을 나타냅니다. 마스크(와일드카드 비트)의 1(**1**)은 비교되는 비트가 IP 주소의 비트와 일치할 필요가 있음을 나타낸다.
   - **FQDN** - 도메인 이름을 지정합니다. FQDN은 커밋 시점에 처음에 해결됩니다. 이후 방화벽은 TTL이 구성한 **최소 FQDN 새로 고침 시간**(또는 기본값 30초)보다 크거나 같을 때 DNS에서 FQDN의 실시간 시간(TTL)을 기반으로 FQDN을 새로 고칩니다. FQDN은 프록시가 구성된 경우 시스템 DNS 서버 또는 DNS 프록시 개체에 의해 해결됩니다. 방화벽 또는 Panorama의 DNS 구성에 따라 연결된 IP 주소를 보려면 확인을 클릭합니다. 주소 개체 유형을 FQDN에서 IP Netmask로 변경하려면 IP Netmask를 선택한 다음 이 주소 사용(사용)을 클릭합니다. IP Netmask의 형식 변경 내용과 선택한 **IP** 주소가 텍스트 필드에 나타납니다.
3. (선택사항)주소 개체에 적용하려면 하나 이상의 태그를 사용하여 개체를 그룹화하고 시각적으로 구별하기을(를) 입력합니다.
4. 확인을 클릭합니다.

**STEP 2 |** 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 주소 개체, 주소 그룹 또는 와일드카드 주소로 필터링된 로그를 봅니다.

1. 예를 들어 모니터 > 로그 > 트래픽을 선택하여 트래픽 로그를 봅니다.
2. 로그 필터를 추가하려면 **+**을(를) 선택합니다.
3. **Address** 속성, **in** 연산자를 선택하고 로그를 보려는 주소 개체의 이름을 입력합니다. 또는 주소 그룹 이름 또는 와일드카드 주소(예: 10.155.3.4/0.0.240.255)를 입력합니다.
4. 적용을 클릭합니다.

**STEP 4 |** 주소 개체를 기반으로 맞춤 보고서를 봅니다.

1. 모니터 > 맞춤 보고서 관리를 선택하고 트래픽 로그와 같은 데이터베이스를 사용하는 보고서를 선택합니다.
2. 필터 빌더를 선택합니다.
3. 주소, 대상 주소 또는 원본 주소와 같은 특성을 선택한 다음 연산자를 선택한 후 보고서를 확인할 주소 개체의 이름을 입력합니다.

**STEP 5 |** ACC의 필터를 사용하여 주소 개체를 사용하는 소스 IP 주소 또는 대상 IP 주소를 기반으로 네트워크 활동을 볼 수 있습니다.

1. **ACC** > 네트워크 활동을 선택합니다.
2. 소스 **IP** 활동 보기 **-** 전역 필터의 경우, **+**를 클릭하여 필터를 추가하고 다음 중 하나를 선택합니다. 주소 또는 원본 > 원본 주소 또는 대상 > 대상 주소 주소 개체를 선택합니다.
3. 대상 **IP** 활동 보기 **-** 전역 필터의 경우, **+**를 클릭하여 필터를 추가하고 다음 중 하나를 선택합니다. 주소 또는 원본 > 원본 주소 또는 대상 > 대상 주소 주소 개체를 선택합니다.


©2023 Palo Alto Networks, Inc.

# 태그를 사용하여 개체를 그룹화하고 시각적으로 구별하기

개체에 태그를 지정하여 관련 항목을 그룹화하고 태그에 색상을 추가하여 쉽게 스캔할 수 있도록 시각적으로 구분할 수 있습니다. 주소 개체, 주소 그룹, 사용자 그룹, 영역, 서비스 그룹 및 정책 규칙과 같은 개체에 대한 태그를 생성할 수 있습니다.

방화벽과 Panorama는 정적 태그와 동적 태그를 모두 지원합니다. 동적 태그는 다양한 소스에서 등록되며 동적 태그는 방화벽 또는 Panorama 구성의 일부가 아니기 때문에 정적 태그와 함께 표시되지 않습니다. 동적으로 태그를 등록하는 방법에 대한 정보는 동적으로 IP 주소 및 태그 등록을(를) 참조하십시오. 이 섹션에서 설명하는 태그는 정적으로 추가되며 구성의 일부입니다.

하나 이상의 태그를 개체 및 정책 규칙에 적용할 수 있으며 개체당 최대 64개의 태그를 적용할 수 있습니다. Panorama는 최대 10,000개의 태그를 지원하며, 이를 Panorama(공유 및 디바이스 그룹)와 관리 방화벽(여러 가상 시스템이 있는 방화벽 포함)에 할당할 수 있습니다.

- 태그 생성 및 적용
- 태그 수정
- 태그 그룹별 규칙 보기

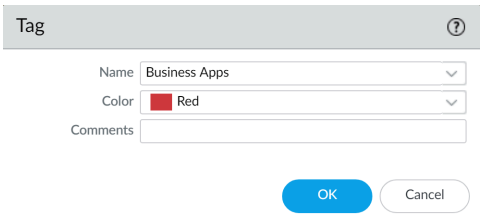
## 태그 생성 및 적용

태그를 사용하여 규칙 또는 구성 개체의 목적을 식별하고 규칙 베이스를 더 잘 구성하는 데 도움이 됩니다. 정책 규칙이 적절하게 태그되었는지 확인하려면 정책 규칙 설명, 태그 및 감사 설명 적용 방법을 참조합니다. 또한 먼저 태그를 생성한 다음 그룹 태그로 설정하여 태그 그룹별 규칙 보기을(를) 할 수 있습니다.

**STEP 1 |** 태그를 생성합니다.

영역에 태그를 지정하려면 영역과 이름이 같은 태그를 만들어야 합니다. 영역이 정책 규칙에 연결되면 태그 색상이 영역 이름에 대한 배경 색으로 자동으로 표시됩니다.

1. 개체 > 태그를 선택합니다.
2. Panorama 또는 다중 가상 시스템 방화벽에서 디바이스 그룹 또는 가상 시스템을 선택하여 태그를 사용할 수 있도록 합니다.
3. 태그를 추가하고 이름을 입력하여 태그를 식별하거나 영역 이름을 선택하여 영역에 대한 태그를 생성합니다. 최대 길이는 127자입니다.
4. (선택 사항) Panorama에서 공유 개체로 액세스하거나 다중 가상 시스템 방화벽의 모든 가상 시스템에서 사용하기 위해 공유 위치에 개체를 생성하려면 공유를 선택합니다.
5. (선택사항) 17개의 사전 정의된 색상에서 색상을 할당합니다. 기본적으로 색상은 없음입니다.




6. 확인 및 커밋을 클릭하여 변경 사항을 저장합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 정책에 태그를 적용합니다.

1. 정책 및 해당 아래에 있는 규칙 기준을 선택합니다.
2. 정책 규칙을 추가하고 1단계에서 만든 태그가 지정된 개체를 사용합니다.
3. 태그가 사용 중인지 확인합니다.

| | | | | Source | | | | Destination | |
|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 1 | General Business Apps | Business Apps | universal | any | any | known-user | any | any | any |

**STEP 3 |** 주소 개체, 주소 그룹, 서비스 또는 서비스 그룹에 태그를 적용합니다.

1. 개체를 생성합니다.

   예를 들어 서비스 그룹을 만들려면 개체 > 서비스 그룹 > 추가를 선택합니다.
2. 태그(태그)를 선택하거나 필드에 이름을 입력하여 새 태그를 생성합니다.

   태그를 편집하거나 태그에 색상을 추가하려면 태그 수정을 참조하십시오.

## 태그 수정

- 개체 > 태그를 선택하여 태그로 다음 작업을 수행합니다.
  - 이름(Name)을 클릭하여 태그의 속성을 편집합니다.
  - 표에서 태그를 선택한 다음 방화벽에서 태그를 삭제합니다.
  - 태그를 복제하여 동일한 속성으로 복제합니다. 태그 이름에 숫자 서픽스가 추가됩니다(예: FTP-1).

  태그 생성에 대한 자세한 내용은 태그 생성 및 적용을(를) 참조하십시오. 태그 작업에 대한 자세한 내용은 태그 그룹별 규칙 보기을(를) 참고하십시오.

## 태그 그룹별 규칙 보기

정책 규칙 기준을 태그 그룹으로 보고 만든 태그 구조에 따라 규칙을 시각적으로 그룹화합니다. 이 보기에서는 선택한 태그 그룹의 규칙을 추가, 삭제 및 이동하는 등의 운영 절차를 보다 쉽게 수행할 수 있습니다. 태그 그룹이 규칙 평가 순서를 유지하며 규칙 레이어을 시각적으로 보존하기 위해 규칙 기반 전체에 단일 태그가 여러 번 나타날 수 있습니다.

규칙의 그룹 태그로 할당하려면 먼저 태그를 만들어야 합니다. PAN-OS 9.0으로 업그레이드할 때 이미 태그가 지정된 정책 규칙에는 첫 번째 태그가 그룹 태그로 자동으로 할당됩니다. PAN-OS 9.0으로 업그레이드하기 전에 규칙베이스에 태그된 규칙을 검토하여 규칙이 올바르게 그룹화되었는지 확인합니다. PAN-OS 9.0으로 업그레이드한 후 규칙이 잘못 그룹화된 경우 각 태그 규칙을 수동으로 편집하고 올바른 그룹 태그를 구성해야 합니다.



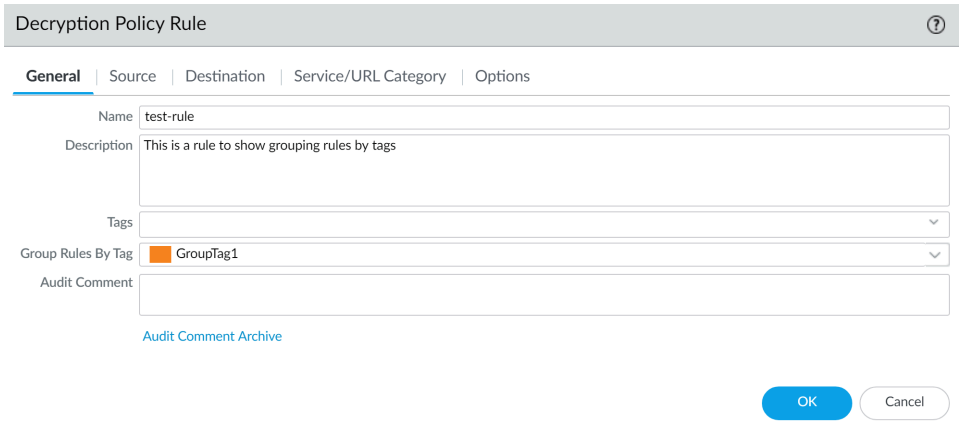

**STEP 1 |** 웹 인터페이스 실행.

**STEP 2 |** 태그 생성 및 적용 규칙 그룹화에 사용하려고 합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 태그 그룹에 정책 규칙을 할당합니다.

1. 정책 규칙을 만듭니다. 정책 규칙 생성에 대한 자세한 내용은 정책을(를) 참조하십시오.
2. 태그별 그룹 규칙 필드의 드롭다운에서 태그를 선택하고 확인을 클릭합니다.

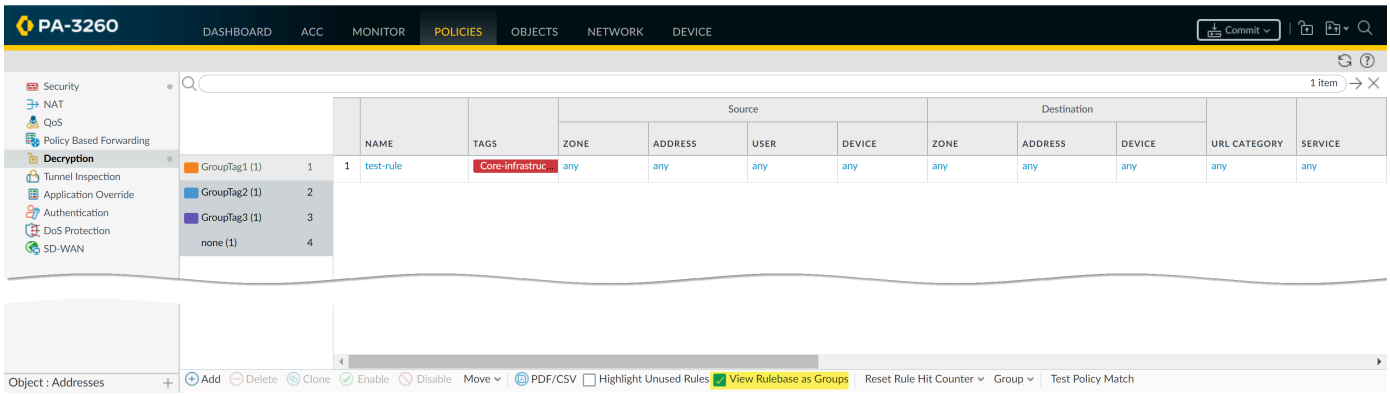



3. 변경 사항을 커밋합니다.

**STEP 4 |** 정책 규칙 기준을 그룹으로 봅니다.

1. (Panorama 전용) 디바이스 그룹에서 디바이스 그룹 규칙 베이스를 선택하여 모든 공유 규칙을 보거나 봅니다.
2. 정책을 클릭하고 2단계에서 규칙을 생성한 규칙 베이스를 선택합니다.
3. 하단에서 규칙 베이스를 그룹으로 보기 옵션을 선택합니다.

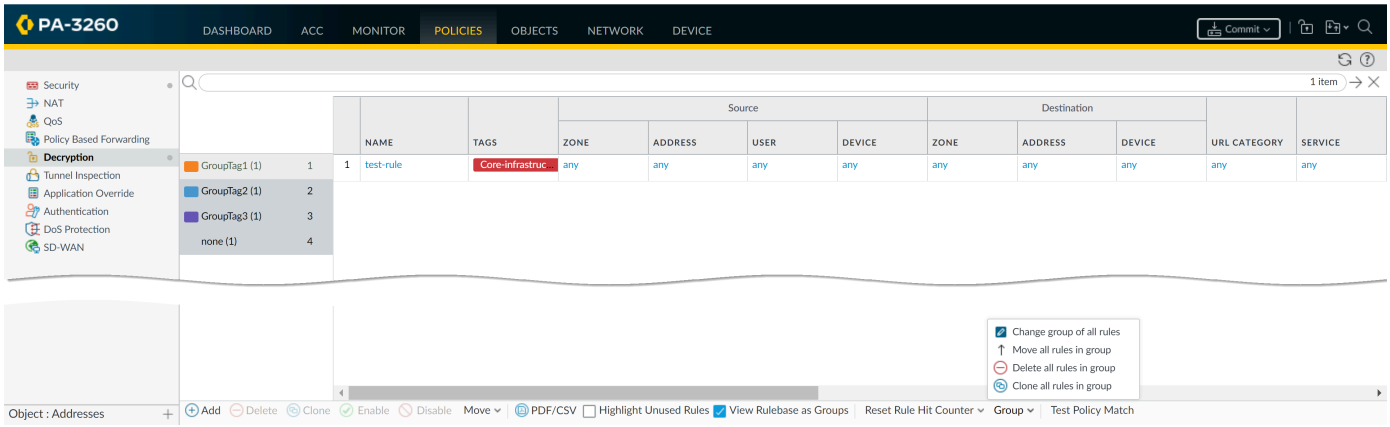
태그 그룹 디스플레이를 없음으로 할당되지 않은 규칙입니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** 필요에 따라 그룹 작업을 수행합니다.

1. 그룹을 클릭하여 선택한 태그 그룹의 규칙에 대한 그룹 작업을 수행합니다.
   - (Panorama만) 그룹의 규칙을 다른 규칙 기반 또는 디바이스 그룹으로 이동-선택한 태그 그룹의 모든 정책 규칙을 규칙 전 또는 규칙 후 베이스로 이동하거나 다른 디바이스 그룹으로 이동합니다.
   - 모든 규칙의 그룹 변경 - 선택한 태그 그룹의 모든 규칙을 다른 태그 그룹으로 이동합니다.
   - 그룹의 모든 규칙을 이동 - 선택한 태그 그룹의 모든 규칙을 이동하여 규칙 우선 순위 순서를 변경합니다.
   - 그룹의 모든 규칙을 삭제합니다 - 선택한 태그 그룹의 모든 규칙을 삭제합니다.
   - 그룹의 모든 규칙을 복사하여 선택한 태그 그룹의 모든 규칙을 복사합니다.




2. 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

# 정책에서 외부 동적 목록 사용

외부 동적 목록(이전의 동적 차단 목록)은 방화벽이 목록의 항목에 대한 정책을 시행하기 위해 IP 주소, URL, 도메인 등의 개체를 가져올 수 있도록 사용자 또는 다른 소스가 외부 웹 서버에서 호스팅하는 텍스트 파일입니다. 목록이 업데이트되면 방화벽은 구성된 인터벌로 목록을 동적으로 가져오고 방화벽에서 구성을 변경하거나 커밋할 필요 없이 정책을 시행합니다.

- 외부 동적 목록
- 외부 동적 목록에 대한 형식 지정 지침
- 내장 외부 동적 목록
- 외부 동적 목록에 액세스하도록 방화벽 구성
- EDL 호스팅 서비스에서 외부 동적 목록에 액세스하도록 방화벽 구성
- 웹 서버에서 외부 동적 목록 검색
- 외부 동적 목록 항목 보기
- 외부 동적 목록에서 항목 제외
- 외부 동적 목록에 대한 정책 시행
- 인증에 실패한 외부 동적 목록 찾기
- 외부 동적 목록에 대한 인증 비활성화

## 외부 동적 목록

외부 동적 목록은 방화벽이 IP 주소, URL, 도메인, 국제 모바일 장비 ID(IMEIs), 국제 모바일 가입자 ID(IMSI) 등 개체를 가져올 수 있도록 외부 웹 서버에서 호스팅되는 텍스트 파일입니다. 외부 동적 목록에 포함된 항목에 대한 보안 정책을 적용하려면 지원되는 정책 규칙 또는 프로파일에서 목록을 참조해야 합니다. 여러 목록을 참조하면 평가 순서의 우선 순위를 지정하여 용량 한도에 도달하기 전에 가장 중요한 EdL이 커밋되었는지 확인할 수 있습니다. 목록을 수정할 때 방화벽은 구성된 인터벌으로 목록을 동적으로 가져오고 구성 변경이나 방화벽의 커밋 없이 정책을 적용합니다. 웹 서버에 연결할 수 없는 경우 방화벽은 웹 서버와의 연결이 복원될 때까지 정책을 실행하기 위해 마지막으로 성공적으로 검색된 목록을 사용합니다. EDL에 대한 인증이 실패하는 경우 보안 정책이 EDL 적용을 중지합니다. 외부 동적 목록을 검색하기 위해 방화벽은 **Palo Alto Networks** 서비스 서비스 경로로 구성된 인터페이스를 사용합니다.

방화벽은 마지막으로 성공적으로 검색된 EDL을 유지하고 다음과 같은 경우 EDL을 호스팅하는 서버와의 연결이 복원될 때까지 최신 EDL 정보로 계속 작동합니다.

- 방화벽을 업그레이드하거나 다운그레이드하는 경우
- 방화벽, 관리부 또는 데이터 평면을 재부팅합니다.
- EDL을 호스팅하는 서버에 연결할 수 없게 됩니다.

방화벽이 연결할 수 없거나 서버에서 최신 EDL 정보를 가져올 수 없는 경우 다음 경고가 표시됩니다.

```
외부 목록을 가져올 수 없습니다. 새로 고침을 위해 이전 복사본 사용.
```

방화벽은 다음과 같은 유형의 외부 동적 목록을 지원합니다.


©2023 Palo Alto Networks, Inc.

- 사전 정의된 **IP** 주소 - 사전 정의된 IP 주소 목록은 고정 또는 "사전 정의된" 내용이 있는 기본 제공 동적 IP 목록을 참조하는 IP 주소 목록의 유형입니다. 활성 위협 방지 라이선스가 있는 경우 방탄 호스팅 제공업체, 알려진 악성 및 고위험 IP 주소를 위한 이러한 내장 외부 동적 목록이 방화벽에 자동으로 추가됩니다. 사전 정의된 IP 주소 목록은 기본 제공 목록 중 하나를 원본으로 사용하는 EDL을 참조할 수도 있습니다. 사전 정의된 목록의 내용을 수정할 수 없으므로 사전 정의된 목록을 목록 항목을 추가하거나 제외하려는 경우 다른 EDL의 원본으로 사용할 수 있습니다.
- 사전 정의된 **URL** 목록 - 이 유형의 외부 동적 목록에는 업데이트 또는 CRL(인증서 해지 목록) 검사와 같은 백그라운드 서비스에 애플리케이션이 사용하는 미리 채워진 URL이 포함되어 있어 방화벽이 인증 정책에서 안전하게 제외될 수 있습니다. Palo Alto Networks는 콘텐츠 업데이트를 통해 인증 포털 제외 목록이라고도 하는 이러한 유형의 외부 동적 목록을 수정하고 유지 관리합니다.
- **IP** 주소 - 방화벽은 일반적으로 방화벽의 정적 개체로 정의된 원본 또는 대상 IP 주소에 대한 정책을 시행합니다(외부 동적 목록의 정책 적용 참조). 임시로 등장하는 소스 또는 대상 IP 주소 목록에 대한 정책을 시행하는 데 민첩성이 필요한 경우 정책 규칙의 원본 또는 대상 주소 개체로 IP 주소의 외부 동적 목록을 사용할 수 있습니다. 목록에 포함된 IP 주소(IPv4 및 IPv6 주소, IP 범위 및 IP 서브넷)에 대한 액세스를 거부하거나 허용하도록 방화벽을 구성합니다. SD-WAN 정책 규칙의 원본 또는 대상에서 IP 주소 EDL을 사용할 수도 있습니다. 방화벽은 IP 주소 유형의 외부 동적 목록을 주소 개체로 처리합니다. 목록에 포함된 모든 IP 주소는 하나의 주소 개체로 처리됩니다.
- 도메인 - 이 유형의 외부 동적 목록을 사용하면 방화벽에 사용자 지정 도메인 이름을 가져와 안티 스파이웨어 프로파일 또는 SD-WAN 정책 규칙을 사용하여 정책을 적용할 수 있습니다. 안티 스파이웨어 프로파일의 EDL은 타사 위협 인텔리전스 피드를 구독하고 악의적인 도메인을 알게 되는 즉시 새로운 위협 또는 멀웨어 소스로부터 네트워크를 보호하려는 경우에 매우 유용합니다. 외부 동적 목록에 포함된 각 도메인에 대해 방화벽은 DNS 싱크홀링을 사용하도록 설정할 수 있도록 사용자 지정 DNS 기반 스파이웨어 서명을 생성합니다. DNS 기반 스파이웨어 서명은 심각도가 중간인 스파이웨어 유형이며 각 서명의 이름은 **사용자 지정 악성 DNS 쿼리<*domain name*>**입니다. 지정된 도메인의 하위 도메인을 포함하도록 방화벽을 지정할 수도 있습니다. 예를 들어, 도메인 목록에 paloaltonetworks.com이 포함된 경우 도메인 이름의 모든 하위 구성 요소(예: *.paloaltonetworks.com)도 목록의 일부로 포함됩니다. 이 설정을 사용하도록 설정하면 지정된 목록의 각 도메인에 추가 항목이 필요하며 목록에서 사용하는 항목 수를 효과적으로 두 배로 늘릴 수 있습니다. 도메인 목록 구성에 대한 자세한 내용은 사용자 지정 도메인 목록에 대한 DNS 싱크홀링 구성을 참조하십시오.
- **URL**-이 유형의 외부 동적 목록은 새로운 위협 또는 멀웨어로부터 네트워크를 보호할 수 있는 민첩성을 제공합니다. 방화벽은 사용자 지정 URL 카테고리와 같은 URL로 외부 동적 목록을 처리하며 이 목록을 두 가지 방법으로 사용할 수 있습니다.
  - 보안 정책 규칙의 일치 기준으로서 복호화 정책 규칙 및 QoS 정책 규칙은 사용자 지정 카테고리의 URL에 대한 대역폭을 허용, 거부, 복호화, 비복호화 또는 할당할 수 있도록 합니다.
  - 보안 정책 규칙에 프로파일을 연결하기 전에 계속, 경고 또는 재정의와 같은 보다 세분화된 작업을 정의할 수 있는 URL 필터링 프로파일의 경우(URL 필터링 프로파일에서 외부 동적 목록 사용 참조).
- 장비 **ID** - 5G 또는 4G 네트워크에 연결된 장비의 트래픽을 제어하는 보안 정책 규칙에서 국제 모바일 장비 ID(IMEI)에 의해 정의된 IoT 디바이스의 외부 동적 목록을 참조할 수 있습니다. 지원되는 방화벽 모델에서 장비 ID 보안 구성에 대한 정보는 모바일 네트워크 인프라 시작에 대한 정보를 참조하십시오.
- 구독자 **ID** - 5G 또는 4G 네트워크에 연결된 구독자의 트래픽을 제어하는 보안 정책 규칙에서 국제 모바일 가입자 ID(IMSI)의 외부 동적 목록을 참조할 수 있습니다. 지원되는 방화벽 모델에서 구독자 ID 보안 구성에 대한 정보는 모바일 네트워크 인프라 시작 시작에 대한 정보를 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

각 방화벽 모델에서 정책을 시행하는 데 사용할 수 있는 고유한 소스가 있는 사용자 지정 EDL을 최대 30개까지 추가할 수 있습니다. 외부 동적 목록 제한은 Panorama에 적용되지 않습니다. Panorama를 사용하여 여러 가상 시스템에 대해 활성화된 방화벽을 관리하는 경우 방화벽의 제한을 초과하면 커밋 오류가 Panorama에 표시됩니다. 소스는 IP 주소 또는 호스트 이름, 경로 및 외부 동적 목록의 파일 이름을 포함하는 URL입니다. 방화벽은 URL(전체 문자열)과 일치하여 원본이 고유한지의 여부를 결정합니다.

방화벽은 특정 형식의 목록 수에 제한을 두지 않지만 다음 제한은 적용됩니다.

- IP 주소-PA-5200 시리즈 및 PA-7000 시리즈 방화벽은 최대 150,000개의 총 IP 주소를 지원합니다. 다른 모든 모델은 총 IP 주소 50,000개를 지원합니다. 목록당 IP 주소 수에 대한 제한은 적용되지 않습니다. 방화벽에서 지원되는 최대 IP 주소 제한에 도달하면 방화벽은 syslog 메시지를 생성합니다. 사전 정의된 IP 주소 목록의 IP 주소는 제한에 포함되지 않습니다.
- URL 및 도메인- 지원되는 URL 및 도메인의 최대 수는 모델에 따라 다릅니다. 목록당 URL 또는 도메인 항목 수에 대한 제한은 적용되지 않습니다. 모델의 세부 사항은 다음 표를 참조하십시오.

| 모델 | **URL** 목록 항목 제한 | 도메인 목록 항목 제한 |
|---|---|---|
| PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈(PA-7000 20GXM NPC, PA-7000 20GQXM NPC 또는 PA-7000 100G NPC로 업그레이드).<br><br>*PA-7000* 어플라이언스 혼합 *NPC*는 표준 용량만 지원합니다. | 250,000 | 4,000,000 |
| VM-500, VM-700 | 100,000 | 2,000,000 |
| PA-400 시리즈(PA-410 제외), PA-850, PA-820, PA-3200 시리즈, PA-3400 시리즈 | 100,000 | 1,000,000 |
| PA-7000 시리즈(PA-7000 20GQ NPC 또는 PA-7000 20G NPC로 업그레이드된 가전 제품), VM-300 | 100,000 | 500,000 |
| PA-220, PA-410, VM-50, VM-50 (Lite), VM-100, VM-1000-HV | 50,000 | 50,000 |

목록 항목은 정책에서 참조되는 외부 동적 목록에 속하는 경우에만 방화벽 제한에 포함됩니다.

 ©2023 Palo Alto Networks, Inc.

- 목록을 구문 분석할 때 방화벽은 목록 형식과 일치하지 않는 항목을 건너뛰고 모델에 대해 지원되는 최대 수를 초과하는 항목을 무시합니다. 항목이 제한을 초과하지 않도록 하려면 현재 정책에 사용되는 항목 수를 확인합니다. 개체 > 외부 동적 목록을 선택한 다음 목록 용량을 클릭합니다.
- 외부 동적 목록에 항목이 포함되어야 합니다. 목록 사용을 중지하려면 정책 규칙 또는 프로파일에서 참조를 제거한 다음 목록을 비워 둡니까? 목록에 항목이 포함되어 있지 않으면 방화벽이 목록을 새로 고치지 못하고 마지막으로 검색한 정보를 계속 사용합니다.
- 가장 좋은 방법으로 *Palo Alto Networks*는 여러 가상 시스템을 사용할 때 공유 *EDL*을 사용할 것을 권장합니다. 각 가상 시스템에 대해 중복된 항목이 있는 개별 *EDL*을 사용하면 방화벽 리소스를 과도하게 활용할 수 있는 메모리가 더 많이 사용됩니다.
- *EDL* 항목은 다중 가상 시스템을 운영하는 방화벽에 대한 카운트를 고려하여 추가 요소(예: *DAG*, 가상 시스템 수, 규칙 기반)를 고려하여 보다 정확한 용량 소비 목록을 생성합니다. 이로 인해 *PAN-OS 8.x* 릴리스에서 업그레이드한 후 용량 사용량이 다를 수 있습니다.
- 방화벽에서 활성화된 기능에 따라 메모리 할당 업데이트로 인해 *EDL* 용량 제한을 충족하기 전에 메모리 사용 제한을 초과할 수 있습니다. *Palo Alto Networks*는 *EDL* 용량을 검토하고 필요한 경우 *EDL*을 공유 목록에 제거하거나 통합하여 메모리 사용을 최소화하는 것이 좋습니다.

## 외부 동적 목록에 대한 형식 지정 지침

IP 주소, URL 또는 도메인과 같은 한 가지 유형의 외부 동적 목록에는 해당 유형의 항목만 포함되어야 합니다. 사전 정의된 IP 주소 목록의 항목은 IP 주소 목록에 대한 서식 지침을 준수합니다.

- IP 주소 목록
- 도메인 목록
- URL 목록

### IP 주소 목록

외부 동적 목록에는 개별 IP 주소, 서브넷 주소(주소/마스크) 또는 IP 주소 범위가 포함될 수 있습니다. 또한 차단 목록에는 주석 및 *****, **:**, **;**, **#** 또는 **/** 등의 특수 문자가 포함될 수 있습니다. 목록의 각 줄에 대한 구문은 **[IP address, IP/Mask, or IP start range-IP end range] [space] [comment]**입니다.


©2023 Palo Alto Networks, Inc.

새 줄에 각 IP 주소/범위/서브넷을 입력합니다. URL 또는 도메인은 이 목록에서 지원되지 않습니다. 서브넷 또는 IP 주소 범위(예: 92.168.20.0/24 또는 192.168.20.40-192.168.20.50)는 여러 IP 주소가 아닌 하나의 IP 주소 항목으로 계산됩니다. 주석을 추가하는 경우 주석은 IP 주소/범위/서브넷과 같은 줄에 있어야 합니다. IP 주소 끝에 있는 공백은 IP 주소와 주석을 구분하는 구분 기호입니다.

IP 주소 목록의 예:

```
192.168.20.10/32 2001:db8:123:1::1 #test IPv6 address
 192.168.20.0/24 ; test internal subnet 2001:db8:123:1::/64 test
 internal IPv6 range 192.168.20.40-192.168.20.50
```

차단된 ***IP*** 주소의 경우 프로토콜이 ***HTTP***인 경우에만 알림 페이지를 표시할 수 있습니다.

## 도메인 목록

도메인 목록의 자리 표시자 문자를 사용하여 단일 항목이 여러 웹사이트 하위 도메인, 전체 최상위 도메인을 포함한 페이지 및 특정 웹 페이지와 일치하도록 구성할 수 있습니다.

도메인 목록 항목을 생성할 때 다음 지침을 따르십시오.

- 새 줄에 각 도메인 이름을 입력합니다. URL 또는 IP 주소는 이 목록에서 지원되지 않습니다.
- 도메인 이름 앞에 프로토콜 http:// 또는 https://를 붙이지 마십시오.
- 별표(*)를 사용하여 와일드카드 값을 나타낼 수 있습니다.
- 캐럿(^)을 사용하여 정확히 일치하는 값을 나타낼 수 있습니다.
- 다음 문자는 토큰 구분자로 간주됩니다: . / ? & = ; +

  이러한 문자 중 하나 또는 두 개로 구분된 모든 문자열은 토큰입니다. 와일드카드 문자를 토큰 자리 표시자로 사용하여 특정 토큰에 모든 값이 포함될 수 있음을 나타냅니다.
- 와일드카드 문자는 토큰 내에서 유일한 문자여야 합니다. 그러나 항목에는 여러 와일드카드가 포함될 수 있습니다.
- 각 도메인 항목의 길이는 최대 255자입니다.

별표**(*)** 와일드카드를 사용하는 경우**:**

별표(*) 와일드카드를 사용하여 하나 이상의 가변 하위 도메인을 나타냅니다. 예를 들어, 사용된 도메인 확장자(위치에 따라 하나 또는 두 개의 하위 도메인이 될 수 있음)에 관계없이 Palo Alto Network의 웹사이트에 대한 시행을 지정하려면 ***.paloaltonetworks.com** 항목을 추가합니다. 이 항목은 docs.paloaltonetworks.com 및 support.paloaltonetworks.com과 일치합니다.

이 와일드카드를 사용하여 전체 최상위 도메인을 나타낼 수도 있습니다. 예를 들어, .work라는 TLD의 시행을 지정하려면 ***.work** 항목을 추가합니다. 이것은 .work로 끝나는 모든 웹사이트와 일치합니다.

***(*)*** 와일드카드는 도메인 항목 앞에만 추가할 수 있습니다**.**

별표**(*)** 예

 ©2023 Palo Alto Networks, Inc.

| EDL 도메인 목록 항목 | 일치하는 사이트 |
|---|---|
| ***.company.com** | eng.tools.company.com<br>support.tools.company.com<br>tools.company.com<br>docs.company.com |
| ***.click** | .click의 최상위 도메인으로 끝나는 모든 웹사이트. |

캐럿**(^)** 문자를 사용하는 경우**:**

하위 도메인의 정확한 일치를 나타내려면 캐럿(^)을 사용합니다. 예를 들어 **^paloaltonetworks.com**은 paloaltonetworks.com과만 일치합니다. 이 항목은 다른 사이트와 일치하지 않습니다.

캐럿**(^)** 예

| EDL 도메인 목록 항목 | 매칭 사이트 |
|---|---|
| **^company.com** | company.com |
| **^eng.company.com** | eng.company.com |

### URL 목록

URL 카테고리 예외을(를) 참조하십시오.

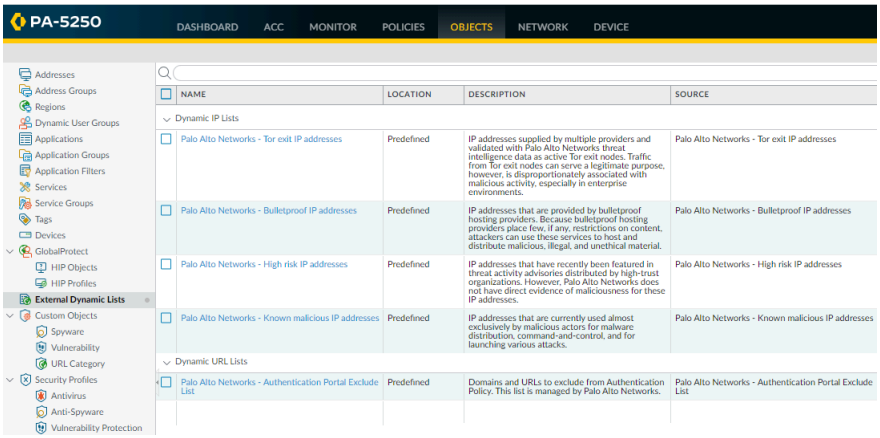
## 내장 외부 동적 목록

활성 위협 방지 라이선스를 통해 Palo Alto Networks는 악성 호스트로부터 보호하는 데 사용할 수 있는 내장 IP 주소 EDL을 제공합니다.

- **Palo Alto Networks Bulletproof IP** 주소 - 방탄 호스팅 제공업체에서 제공한 IP 주소가 포함되어 있습니다. 방탄 호스팅 제공업체는 콘텐츠에 대한 제한이 거의 없기 때문에 공격자는 이러한 서비스를 사용하여 악의적이고 불법적이며 비윤리적인 자료를 호스팅하고 배포하는 경우가 많습니다.
- **Palo Alto Networks** 고위험 **IP** 주소 - 신뢰할 수 있는 타사 조직에서 발행한 위협 권고의 악성 IP 주소가 포함되어 있습니다. Palo Alto Networks는 위협 권고 목록을 컴파일하지만 IP 주소의 악성에 대한 직접적인 증거는 없습니다.
- **Palo Alto Networks** 알려진 악성 **IP** 주소 - WildFire 분석, Unit 42 연구 및 원격 측정에서 수집한 데이터를 기반으로 악성으로 확인된 IP 주소가 포함되어 있습니다(Palo Alto Networks와 위협 인텔리전스 공유). 공격자는 이러한 IP 주소를 거의 독점적으로 사용하여 맬웨어를 배포하고 명령 및 제어 활동을 시작하며 공격을 시작합니다.
- **Palo Alto Networks Tor Exit IP** 주소 - 여러 공급자가 제공하고 활성 Tor 출구 노드로 Palo Alto Networks 위협 인텔리전스 데이터로 검증된 IP 주소를 포함합니다. Tor 출구 노드의 트래픽은 합법적인 목적으로 사용될 수 있지만 특히 기업 환경에서 악의적인 활동과 불균형적으로 연관됩니다.


©2023 Palo Alto Networks, Inc.

방화벽은 콘텐츠 업데이트에서 이러한 피드에 대한 업데이트를 수신하여 방화벽이 Palo Alto Networks의 최신 위협 인텔리전스를 기반으로 정책을 자동으로 시행할 수 있도록 합니다. 기본 제공 목록의 내용은 수정할 수 없습니다. 있는 그대로 사용하거나(외부 동적 목록에 대한 정책 시행 참조) 목록 중 하나를 소스로 사용하는 사용자 지정 외부 동적 목록을 생성하고(외부 동적 목록에 액세스하도록 방화벽 구성 참조) 필요에 따라 목록에서 항목을 제외합니다.




# 외부 동적 목록에 액세스하도록 방화벽 구성

외부 동적 목록에 대한 정책을 시행하기 전에 방화벽과 외부 동적 목록을 호스팅하는 소스 간에 연결을 설정해야 합니다.

**STEP 1 |** (선택 사항) 방화벽이 외부 동적 목록을 검색하는 데 사용하는 서비스 경로를 사용자 지정합니다.

**Device** > **Setup** > **Services** > **Service** 경로 구성 > 사용자 지정을 선택한 다음 외부 동적 목록 서비스 경로를 수정합니다.

방화벽은 외부 동적 목록 서비스 경로를 사용하여 내장 외부 동적 목록을(를) 검색하지 않습니다. 콘텐츠 업데이트는 해당 목록의 콘텐츠를 수정하거나 업데이트합니다(활성 *Threat Prevention* 라이선스 필요).

**STEP 2 |** 방화벽과 함께 사용할 외부 동적 목록을 찾습니다.

- 외부 동적 목록을 생성하고 웹 서버에서 호스팅합니다. 빈 텍스트 파일에 IP 주소, 도메인 또는 URL을 입력합니다. 각 목록 항목은 별도의 줄에 있어야 합니다. 예:

  **financialtimes.co.in**

  **www.wallaby.au/joey**

  **www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx**

  방화벽이 목록 항목을 건너뛰지 않도록 하려면 외부 동적 목록에 대한 형식 지정 지침을 참조하십시오. 커밋 오류 및 잘못된 항목을 방지하려면 항목 앞에 http:// 또는 https://를 프리픽스로 사용하지 마십시오.
- 다른 소스에서 호스팅하는 외부 동적 목록을 사용하고 외부 동적 목록에 대한 형식 지정 지침을 따르는지 확인합니다.

**STEP 3 |** 개체 > 외부 동적 목록을 선택합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** 추가를 클릭하고 목록을 설명하는 이름을 입력합니다.

**STEP 5 |** (선택 사항) 여러 가상 시스템에 대해 활성화된 디바이스의 모든 가상 시스템과 목록을 공유하려면 공유를 선택합니다. 기본적으로 개체는 가상 시스템 드롭다운에서 현재 선택된 가상 시스템에 생성됩니다.



가장 좋은 방법으로 ***Palo Alto Networks***는 여러 가상 시스템을 사용할 때 공유 ***EDL***을 사용할 것을 권장합니다. 각 ***vsys***에 대해 중복 항목이 있는 개별 ***EDL***을 사용하면 더 많은 메모리를 사용하여 방화벽 리소스를 과도하게 사용할 수 있습니다.

**STEP 6 |** (Panorama 전용) 방화벽 관리자가 Panorama의 디바이스 그룹 커밋을 통해 이 구성을 상속하는 방화벽의 설정을 로컬로 재정의할 수 없도록 하려면 재정의 비활성화를 선택합니다.

**STEP 7 |** 목록 유형(예: **URL** 목록)을 선택합니다.

목록에 목록 유형에 대한 항목만 포함되어 있는지 확인하십시오. 외부 동적 목록의 항목이 무시되거나 건너뛰었는지 확인을 참조하십시오.

도메인 목록을 사용하는 경우 선택적으로 하위 도메인을 포함하도록 자동 확장을 활성화하여 지정된 도메인의 하위 도메인도 포함할 수 있습니다. 예를 들어, 도메인 목록에 paloaltonetworks.com이 포함된 경우 도메인 이름의 모든 하위 구성 요소(예: *.paloaltonetworks.com)도 목록의 일부로 포함됩니다. 이 설정이 활성화되면 지정된 목록의 각 도메인에 추가 항목이 필요하므로 소비되는 항목 수가 효과적으로 두 배로 늘어납니다.

**STEP 8 |** 웹 서버에서 방금 생성한 목록의 소스를 입력합니다. 목록에 액세스하려면 소스에 전체 경로가 포함되어야 합니다. 예: **`https://1.2.3.4/EDL_IP_2015`**.

- 사전 정의된 IP 외부 동적 목록을 생성하는 경우 소스로 사용할 Palo Alto Networks 악성 IP 주소 피드를 선택하십시오.
- 사전 정의된 URL 외부 동적 목록을 생성하는 경우 **panw-auth-portal-exclude-list**를 소스로 선택합니다.

**STEP 9 |** 목록 소스가 SSL로 보호되는 경우(예: HTTPS URL이 있는 목록) 서버 인증을 활성화하십시오. 목록을 호스팅하는 서버를 인증하기 위해 인증서 프로파일을 선택하거나 새 인증서 프로파일을 생성합니다. 선택한 인증서 프로파일에는 인증 중인 서버에 설치된 인증서와 일치하는 루트 CA(인증 기관) 및 중간 CA 인증서가 있어야 합니다.

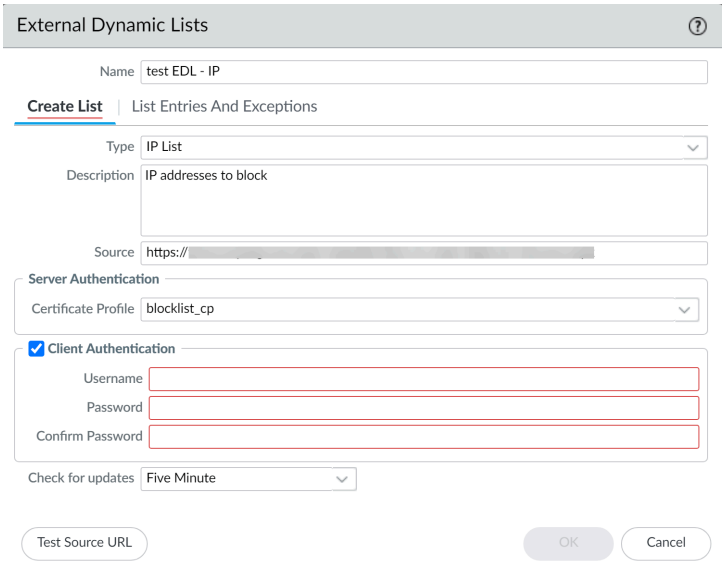


정책을 시행하는 데 사용할 수 있는 외부 동적 목록의 수를 최대화합니다. 동일한 인증서 프로파일을 사용하여 동일한 소스 ***URL***에서 외부 동적 목록을 인증합니다. 동일한 소스 ***URL***의 외부 동적 목록에 다른 인증서 프로파일을 할당하면 방화벽은 각 목록을 고유한 외부 동적 목록으로 계산합니다.


©2023 Palo Alto Networks, Inc.

**STEP 10 |** 목록 소스에 HTTPS URL이 있고 목록 액세스를 위해 기본 HTTP 인증이 필요한 경우 클라이언트 인증을 활성화합니다.

1. 클라이언트 인증을 선택합니다.
2. 목록에 액세스하려면 유효한 사용자 이름을 입력하십시오.
3. 암호 및 암호 확인을 입력합니다.




**STEP 11 |** (Panorama 또는 사전 정의된 URL EDL에서는 사용할 수 없음) 테스트 소스 **URL**을 클릭하여 방화벽이 웹 서버에 연결할 수 있는지 확인합니다.

*EDL* 액세스에 인증을 사용하는 경우 테스트 소스 ***URL*** 기능을 사용할 수 없습니다.

**STEP 12 |** (선택 사항) 방화벽이 목록에 대한 업데이트를 확인해야 하는 빈도를 지정합니다. 기본적으로 방화벽은 1시간에 한 번씩 목록을 검색하고 변경 사항을 커밋합니다.

인터벌은 마지막 커밋을 기준으로 합니다. 따라서 *5*분 간격 동안 마지막 커밋이 *1*시간 전이라면 커밋은 *5*분 후에 발생합니다. 목록을 즉시 검색하려면 웹 서버에서 외부 동적 목록 검색을 참조하십시오.

**STEP 13 |** 확인을 클릭하고 변경 사항을 커밋합니다.

**STEP 14 |** (선택 사항) EDL은 평가 순서대로 위에서 아래로 표시됩니다. 페이지 하단의 방향 컨트롤을 사용하여 목록 순서를 변경합니다. 이를 통해 용량 제한에 도달하기 전에 가장 중요한 EDL이 커밋되도록 목록을 주문하거나 주문할 수 있습니다.

***Group By Type***이 선택 해제된 경우에만 ***EDL*** 순서를 변경할 수 있습니다.


©2023 Palo Alto Networks, Inc.

**STEP 15 |** 외부 동적 목록에 대한 정책 시행.

서버 또는 클라이언트 인증이 실패하면 방화벽은 마지막으로 성공적으로 검색된 외부 동적 목록을 기반으로 정책 시행을 중단합니다. 인증에 실패한 외부 동적 목록을 찾아 인증 실패 이유를 봅니다.

# EDL 호스팅 서비스에서 외부 동적 목록에 액세스하도록 방화벽 구성

SaaS(Software-as-a-Service) 애플리케이션용 EDL 호스팅 서비스에서 외부 동적 목록(EDL)에 액세스하도록 방화벽 구성

- EDL 호스팅 서비스를 사용하여 외부 동적 목록 생성
- GlobalSign 루트 R1 인증서를 PEM 형식으로 변환

## EDL 호스팅 서비스를 사용하여 외부 동적 목록 생성

일부 SaaS(Software-as-a-Service) 공급자는 IP 주소 및 URL 목록을 SaaS 애플리케이션의 대상 엔드포인트로 게시합니다. SaaS 공급자는 지원이 증가하고 서비스가 확장됨에 따라 SaaS 애플리케이션 대상 엔드포인트 목록을 자주 업데이트합니다. 이를 위해서는 SaaS 애플리케이션 엔드포인트의 변경 사항을 수동으로 모니터링하고 정책 구성을 수동으로 업데이트하여 이러한 중요한 SaaS 애플리케이션에 대한 연결을 보장하거나 EDL을 모니터링하고 업데이트하기 위한 외부 도구를 설정해야 합니다.

Palo Alto Networks가 유지 관리하는 EDL 호스팅 서비스를 사용하여 EDL을 구성하여 SaaS 애플리케이션의 EDL을 유지 관리하는 운영 부담을 덜어줍니다. EDL 호스팅 서비스는 SaaS 애플리케이션 공급자가 게시한 SaaS 애플리케이션 엔드포인트에 대해 공개적으로 사용 가능한 피드 URL을 제공합니다. EDL에서 피드 URL을 소스로 활용하면 자체 EDL 소스를 호스팅하고 유지 관리할 필요 없이 SaaS 애플리케이션 트래픽을 동적으로 적용할 수 있습니다.

Palo Alto Networks는 매일 SaaS 공급자가 게시한 애플리케이션 피드 URL을 확인합니다. IP 기반 피드의 경우 Palo Alto Networks는 연속 넷마스크의 항목을 결합하는 최적화를 수행하고 엔드포인트가 여러 영역에 걸쳐 겹치는 경우 중복 제거가 수행됩니다. 또한 Microsoft 365 공통 및 Office 온라인 SaaS 애플리케이션의 엔드포인트는 항상 EDL 호스팅 서비스의 모든 피드 URL에 추가됩니다.

Microsoft는 매월 말에 모든 Microsoft 365 피드 URL을 업데이트하고 업데이트 30일 전에 미리 알림을 제공합니다. 자세한 내용은 공식 Microsoft 365 웹 서비스 페이지를 참조하십시오. EDL 호스팅 서비스 가용성 상태 및 업데이트는 Palo Alto Networks 클라우드 서비스 상태 페이지에 게시됩니다.

**STEP 1 |** EDL 호스팅 서비스를 방문하여 SaaS 애플리케이션의 피드 URL을 확인합니다.

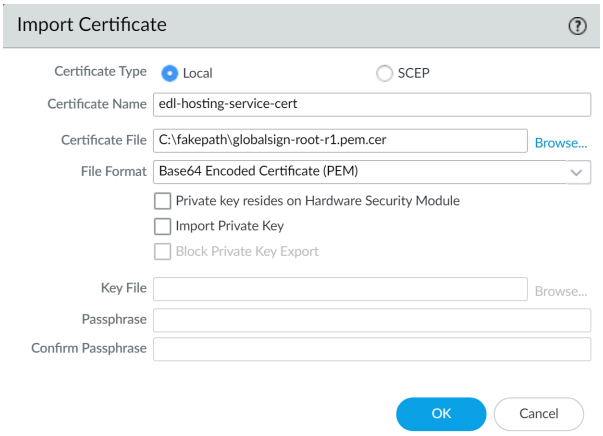
사용 사례에 가장 적합한 피드 URL에 대한 자세한 내용은 Microsoft 365 설명서를 참조하십시오. 또한 에 대한 피드 URL을 식별할 때 SaaS 애플리케이션과 SaaS 애플리케이션에 액세스하는 사용자의 위치를 고려하십시오. 예를 들어 독일에 Exchange Online에만 액세스하면 되는 지사가 있는 경우 서비스 영역에서 피드 URL을 선택합니다. 독일 온라인 교환.

정책 기반 포워딩 정책 규칙의 경우 ***IP*** 기반 피드 ***URL***을 사용합니다.


©2023 Palo Alto Networks, Inc.

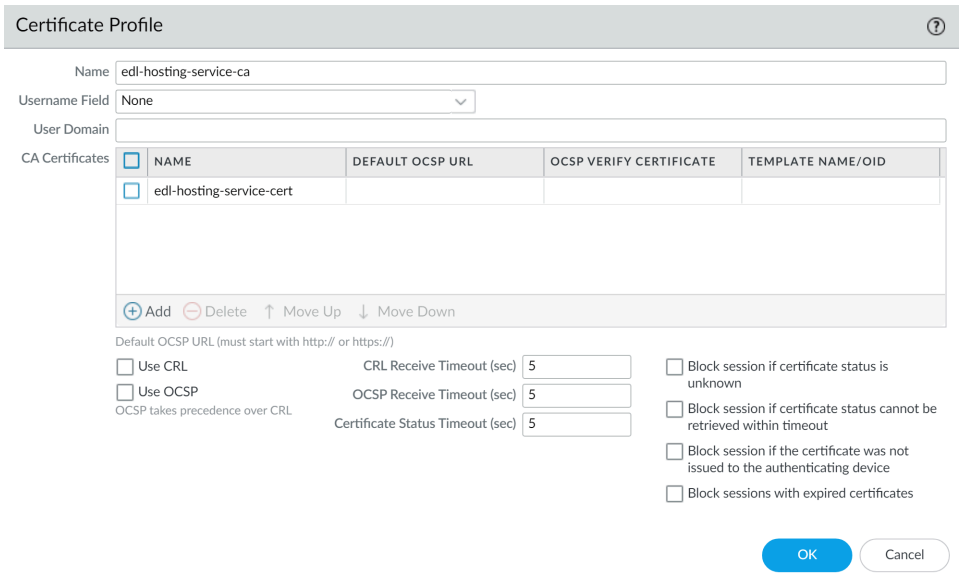
**STEP 2 |** (모범 사례) EDL 호스팅 서비스를 인증하기 위한 인증서 프로파일을 만듭니다.

1. GlobalSign Root R1 인증서를 다운로드합니다.
2. GlobalSign 루트 R1 인증서를 PEM 형식으로 변환.
3. 방화벽 웹 인터페이스를 시작합니다.
4. GlobalSign 루트 R1 인증서를 가져옵니다.
   1. 디바이스 인증서 관리인증서 및 새 인증서 가져오기를 선택합니다.
   2. 인증서 유형에 대해 로컬을 선택합니다.
   3. 설명이 포함된 인증서 이름을 입력합니다.
   4. 인증서 파일의 경우 찾아보기를 선택한 다음 이전 단계에서 변환한 인증서를 선택합니다.
   5. 파일 형식에 대해 Base64 인코딩 인증서(PEM)를 선택합니다.
   6. 확인을 클릭합니다.




5. CA(인증 기관) 인증서 프로파일을 생성합니다.
   1. 디바이스 인증서 관리 인증서 프로파일 및 새 인증서 프로파일 추가를 선택합니다.
   2. 설명이 포함된 이름을 입력합니다.
   3. CA 인증서의 경우 이전 단계에서 불러온 인증서를 추가합니다.
   4. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.




6. 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

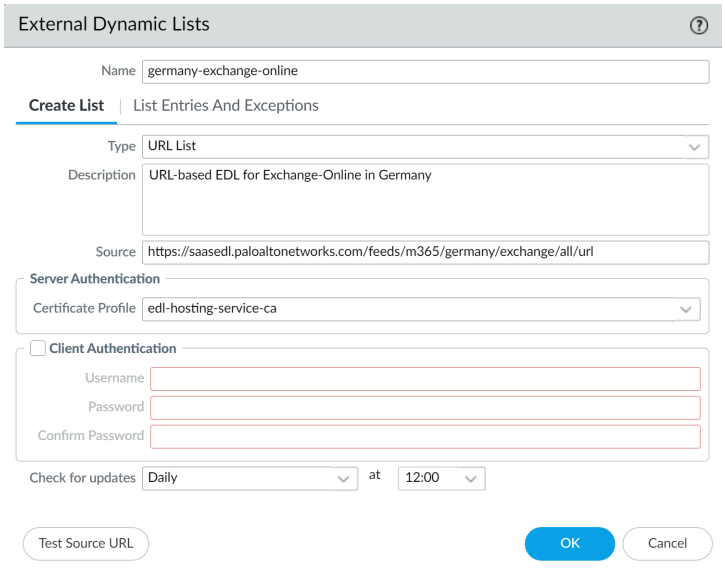
**STEP 3 |** EDL 호스팅 서비스의 피드 URL을 사용하여 EDL을 생성합니다.

1. 개체 외부 동적 목록을 선택하고 새 EDL을 추가합니다.
2. EDL에 대한 설명이 포함된 이름을 입력합니다.
3. EDL 유형을 선택합니다.
   - IP 기반 EDL의 경우 IP 목록을 선택합니다.
   - URL 기반 EDL의 경우 URL 목록을 선택합니다.
4. (선택 사항) EDL에 대한 설명을 입력합니다.
5. 피드 URL을 EDL 소스로 입력합니다.

   특정 피드 ***URL*** 내에 모든 엔드포인트를 적용합니다. 피드 ***URL***에서 특정 엔드포인트를 제외하면 ***SaaS*** 애플리케이션에 연결 문제가 발생할 수 있습니다.
6. (모범 사례) 이전 단계에서 생성한 인증서 프로파일을 선택합니다.
7. 방화벽이 피드 URL의 업데이트 빈도와 일치하도록 업데이트를 확인해야 하는 빈도를 지정합니다.

   예를 들어 피드 URL이 Palo Alto Networks에 의해 매일 업데이트되는 경우 일 단위 업데이트를 확인하도록 EDL을 구성합니다.

   Palo Alto Networks는 EDL 호스팅 서비스의 각 피드 URL에 대한 업데이트 빈도를 표시합니다. 피드 URL은 새 엔드포인트로 자동 업데이트됩니다.
8. 소스 URL 테스트를 클릭하여 방화벽이 EDL 호스팅 서비스의 피드 URL에 액세스할 수 있는지 확인합니다.
9. 확인을 클릭합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 외부 동적 목록에 대한 정책 시행.

EDL이 소스인 EDL 호스팅 서비스에서 EDL에 정책을 적용하는 경우 애플리케이션에 대한 과잉 프로비저닝 액세스를 방지하기 위해 SaaS 애플리케이션에 액세스할 수 있는 사용자를 구성할 때 구체적으로 지정해야 합니다.



정책 규칙에서 ***EDL***과 함께 App-ID를 활용하여 ***SaaS*** 애플리케이션 트래픽을 더욱 엄격하게 적용합니다.

## GlobalSign 루트 R1 인증서를 PEM 형식으로 변환

EDL 호스팅 서비스를 인증하기 위한 인증서 프로파일을 생성하려면 GlobalSign Root R1 인증서를 **PEM** 형식으로 변환해야 합니다. 할 때 EDL 호스팅 서비스를 활용할 때 EDL 호스팅 서비스를 인증하기 위해 인증서 프로파일을 만드는 것이 가장 좋습니다.

GlobalSign Root R1 인증서를 다운로드한 디바이스의 운영 체제에 따라 적절한 절차를 참조하십시오.

**STEP 1 |** 아직 인증서를 다운로드하지 않은 경우 GlobalSign Root R1 인증서를 다운로드합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 인증서를 변환합니다.

- **Mac** 및 **Linux** 운영 체제

1. 터미널을 열고 다운로드한 GlobalSign Root R1 인증서를 변환합니다.

```
관리자:  openssl x509 -in <certificate-path>.crt -inform DER -out
 <target-export-path>.pem -outform PEM
```

```
admin-1@admin-1:~$ openssl x509 -in /home/admin-1/Downloads/Root-R1.crt -inform
DER -out /home/admin-1/Downloads/globalsign-root-r1.pem -outform PEM
```

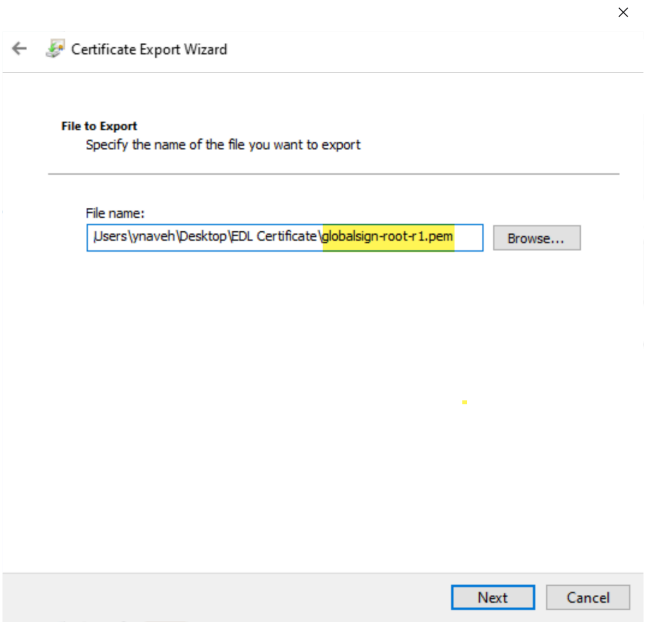
대상 내보내기 경로를 지정하지 않으면 변환된 인증서가 디바이스 바탕 화면에 생성됩니다.

- **Windows** 운영 체제

1. GlobalSign Root1 인증서를 다운로드한 위치로 이동합니다.
2. 두 번 클릭하고 인증서를 엽니다.
3. 세부 정보 및 파일에 복사를 클릭합니다.

   계속할지 묻는 메시지가 표시되면 다음을 클릭합니다.
4. **Base-64**로 인코딩된 **x.509(.CER)**를 선택한 다음 다음을 클릭합니다.
5. 찾아보기를 클릭하여 인증서를 복사할 위치로 이동하고 파일 이름 끝에 **.pem**이 추가된 인증서 이름을 입력합니다. 예: **globalsign-root-r1.pem**

   인증서를 저장합니다. 표시된 파일 이름에는 대상 내보내기 경로와 `.cer`이 추가된 입력한 인증서 이름이 표시됩니다. appended`.cer`을 삭제합니다.




6. 다음을 클릭하고 인증서 내보내기를 마칩니다.

 ©2023 Palo Alto Networks, Inc.

## 웹 서버에서 외부 동적 목록 검색

외부 동적 목록에 액세스하도록 방화벽을 구성할 때 매시간(기본값) 5분, 매일, 매주 또는 매월 웹 서버에서 목록을 검색하도록 방화벽을 구성할 수 있습니다. 목록에서 IP 주소를 추가하거나 삭제했고 즉시 새로 고침을 트리거해야 하는 경우 다음 프로세스를 사용하여 업데이트된 목록을 가져옵니다.

**STEP 1 |** 요청 시 목록을 검색하려면 개체 > 외부 동적 목록을 선택합니다.

**STEP 2 |** 새로 고칠 목록을 선택한 다음 지금 가져오기를 클릭합니다. 목록을 가져올 작업이 큐에 대기됩니다.

**STEP 3 |** 작업 관리자에서 작업 상태를 보려면 관리 작업 관리 및 모니터링을 참조하십시오.

**STEP 4 |** (선택 사항) 방화벽이 목록을 검색한 후 외부 동적 목록 항목 보기.

## 외부 동적 목록 항목 보기

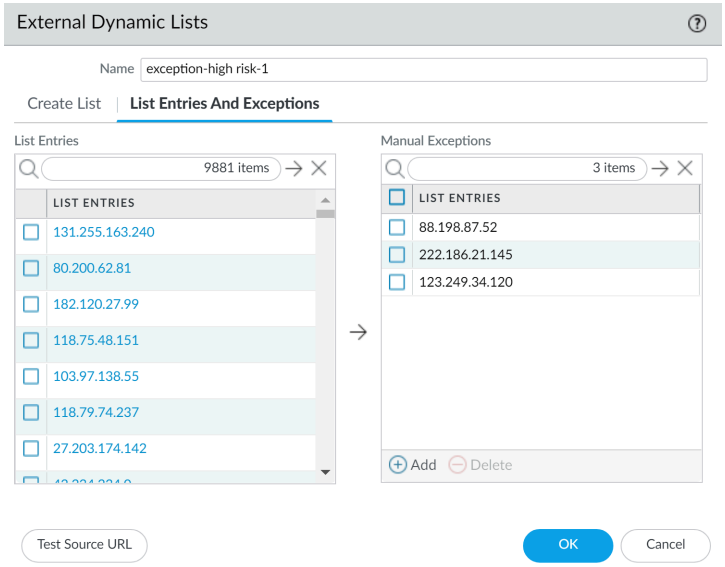
외부 동적 목록에서, 정책을 적용하기 전에 방화벽에서 직접 외부 동적 목록의 내용을 보고 특정 IP 주소, 도메인 또는 URL이 포함되어 있는지 확인할 수 있습니다. 표시된 항목은 방화벽이 가장 최근에 검색한 외부 동적 목록의 버전을 기반으로 합니다.

**STEP 1 |** 개체 > 외부 동적 목록을 선택합니다.

**STEP 2 |** 보려는 외부 동적 목록을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 목록 항목 및 예외를 클릭하고 방화벽이 목록에서 검색한 개체를 봅니다.




다음과 같은 경우 목록이 비어 있을 수 있습니다.

- EDL은 보안 정책 규칙에 아직 적용되지 않았습니다. 보안 정책 규칙에 EDL을 적용하고 EDL을 채우려면 외부 동적 목록에 대한 정책 시행을(를) 참조하십시오.
- 방화벽은 아직 외부 동적 목록을 검색하지 않았습니다. 방화벽이 외부 동적 목록을 즉시 검색하도록 하려면 웹 서버에서 외부 동적 목록을 검색합니다.
- 방화벽은 외부 동적 목록을 호스팅하는 서버에 액세스할 수 없습니다. 테스트 소스 **URL**을 클릭하여 방화벽이 서버에 연결할 수 있는지 확인합니다.

**STEP 4 |** 필터 필드에 IP 주소, 도메인 또는 URL(목록 유형에 따라 다름)을 입력하고 필터 적용(→)을 사용하여 목록에 있는지 확인합니다. 차단하거나 허용해야 하는 IP 주소, 도메인 및 URL을 기반으로 외부 동적 목록에서 항목을 제외합니다.

**STEP 5 |** (선택 사항) 목록 항목에 대한 AutoFocus Intelligence Summary를 봅니다. 항목 위로 마우스를 가져가서 드롭다운을 연 다음 **AutoFocus**를 클릭합니다.

## 외부 동적 목록에서 항목 제외

외부 동적 목록의 항목을 볼 때 목록에서 최대 100개의 항목을 제외할 수 있습니다. 외부 동적 목록에서 항목을 제외할 수 있으므로 목록의 항목 중 일부(전부는 아님)에 대한 정책을 적용할 수 있습니다. 타사 소스에서 제공되므로 외부 동적 목록(예: Palo Alto Networks 고위험 IP 주소 피드)의 내용을 편집할 수 없는 경우에 유용합니다.

**STEP 1 |** 외부 동적 목록 항목을 봅니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 목록에서 제외하려면 최대 100개의 항목을 선택한 다음 제출(→) 또는 수동형으로 목록 예외 추가를 클릭합니다.

- 수동 예외 목록에 중복 항목이 있는 경우 변경 사항을 외부 동적 목록에 저장할 수 없습니다. 중복 항목을 식별하려면 빨간색 밑줄이 있는 항목을 찾습니다.
- 수동형 예외는 목록 항목과 정확히 일치해야 합니다. 또한 IP 주소 범위 내에서 특정 IP 주소를 제외할 수 없습니다. IP 주소 범위에서 특정 IP 주소를 제외하려면 범위의 각 IP 주소를 목록 항목으로 추가한 다음 원하는 IP 주소를 제외해야 합니다.

  방화벽은 IP 주소 범위에서 개별 IP 주소를 제외하는 것을 지원하지 않습니다.

**STEP 3 |** 확인 및 커밋을 클릭하여 변경 사항을 저장합니다.

**STEP 4 |** (선택 사항) 외부 동적목록에서 정책을 적용합니다.

## 외부 동적 목록에 대한 정책 시행

외부 동적 목록의 IP 주소 또는 URL을 기반으로 트래픽을 차단 또는 허용하거나 DNS 싱크홀이 있는 동적 도메인 목록을 사용하여 악성 도메인에 대한 액세스를 방지합니다.

외부 동적 목록을 사용하여 방화벽에서 정책을 시행하기 위한 팁:

- 방화벽에서 외부 동적 목록(개체 > 외부 동적 목록)을 볼 때 목록 수용량을 클릭하여 방화벽이 각 목록 유형에 대해 지원하는 총 항목 수와 현재 정책에서 사용되는 ***IP*** 주소, 도메인 및 ***URL*** 수를 비교합니다.
- 전역 찾기를 사용하여 방화벽 또는 Panorama Management Server에서 도메인, ***IP*** 주소 또는 하나 이상의 외부 동적 목록에 속하는 ***URL*** 검색이 정책에 사용됩니다. 이는 방화벽이 특정 도메인, ***IP*** 주소 또는 ***URL***을 차단하거나 허용하도록 하는 외부 동적 목록(보안 정책 규칙에서 참조)을 결정하는 데 유용합니다.
- 페이지 하단의 방향 컨트롤을 사용하여 ***EDL***의 평가 순서를 변경합니다. 이를 통해 용량 제한에 도달하기 전에 ***EDL***에서 가장 중요한 항목이 커밋되도록 목록을 정렬하거나 주문할 수 있습니다.

  ***Group By Type***이 선택 해제된 경우에만 ***EDL*** 순서를 변경할 수 있습니다.

- 사용자 지정 도메인 목록에 대한 DNS 싱크홀링을 구성합니다.
- URL 필터링 프로파일에서 외부 동적 목록 사용.


©2023 Palo Alto Networks, Inc.

- 보안 정책 규칙에서 **URL** 유형의 외부 동적 목록을 일치 조건으로 사용합니다**.**
  1. 정책 > 보안을 선택합니다.
  2. 추가를 클릭하고 규칙에 대한 설명이 포함된 이름을 입력합니다.
  3. 소스 탭에서 소스 영역을 선택합니다.
  4. 대상 탭에서 대상 영역을 선택합니다.
  5. 서비스**/URL** 카테고리 탭에서 추가를 클릭하여 URL 카테고리 목록에서 적절한 외부 동적 목록을 선택합니다.
  6. 작업 탭에서 작업 설정을 허용 또는 거부로 설정합니다.
  7. 확인 및 커밋을 클릭합니다.
  8. 외부 동적 목록의 항목이 무시되거나 건너뛰었는지 확인합니다.

     방화벽에서 다음 CLI 명령을 사용하여 목록에 대한 세부 정보를 검토합니다.

     ```
     request system external-list show type <domain | ip | url>
      name_of_list
     ```

     예:

     ```
     request system external-list show type url EBL_ISAC_Alert_List
     ```

  9. 정책 작업이 적용되었는지 테스트합니다.

     **1.** URL 목록에 대한 외부 동적 목록 항목을 보고 목록에서 URL에 액세스를 시도합니다.

     **2.** 정의한 조치가 시행되었는지 확인하십시오.

     **3.** 방화벽에서 활동을 모니터링하려면 다음을 수행합니다.

     - **ACC**를 선택한 다음 URL 도메인을 전역 필터로 추가하여 액세스한 URL에 대한 네트워크 활동 및 차단된 활동을 봅니다.
     - 자세한 로그 보기에 액세스하려면 **Monitor** > **Logs** > **URL** 필터링을 선택하십시오.


©2023 Palo Alto Networks, Inc.

- 보안 정책 규칙에서 **IP** 외부 동적 목록 또는 미리 정의된 **IP** 외부 동적 목록을 소스 또는 대상 주소 개체로 사용합니다**.**

  이 기능은 새 서버를 배포하고 방화벽 커밋 없이 새로 배포된 서버에 대한 액세스를 허용하려는 경우에 유용합니다.

  1. 정책 > 보안을 선택합니다.
  2. 추가를 클릭하고 규칙에 설명이 포함된 이름을 지정합니다.
  3. 소스/대상 탭에서 소스/대상 주소로 사용할 외부 동적 목록을 설정합니다.
  4. 서비스/URL 카테고리 탭에서 서비스가 **application-default**로 설정되어 있는지 확인합니다.
  5. 작업 탭에서 작업 설정을 허용 또는 거부로 설정합니다.

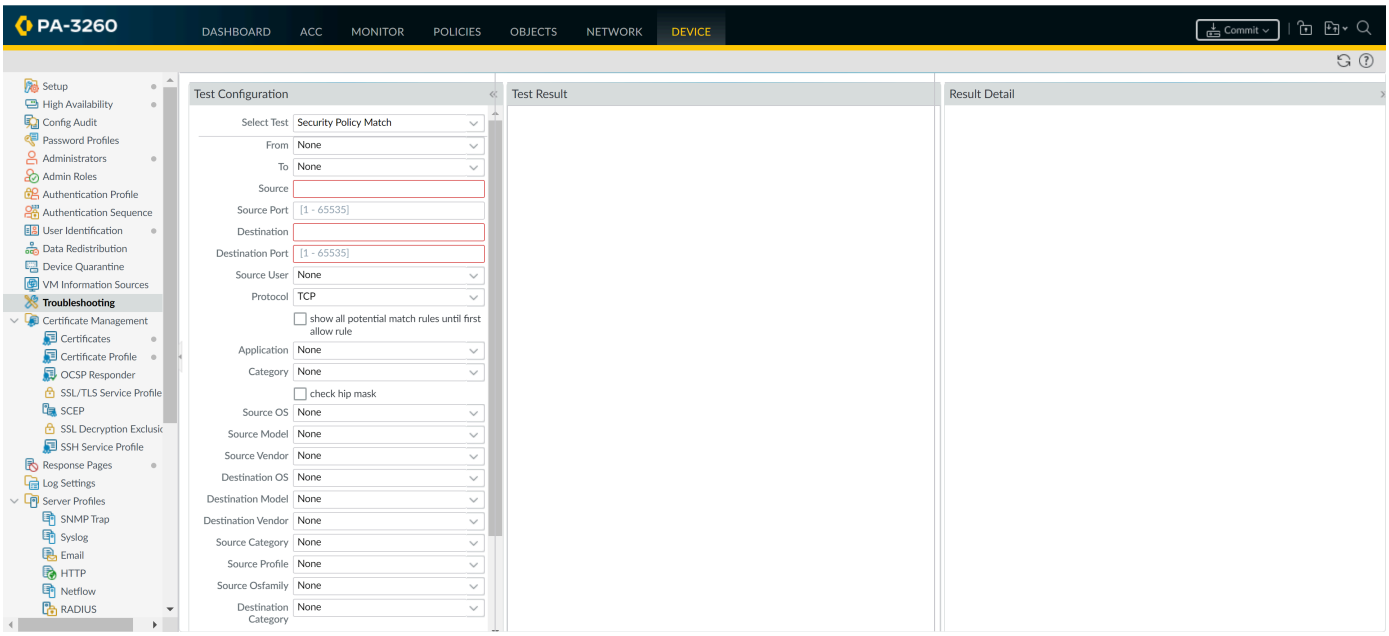
     특정 *IP* 주소에 대한 허용 및 거부 작업을 지정하려면 별도의 외부 동적 목록을 생성합니다**.**
  6. 다른 모든 옵션은 기본값으로 둡니다.
  7. 확인을 클릭하여 변경 사항을 저장합니다.
  8. 변경 사항을 커밋합니다.
  9. 정책 작업이 적용되었는지 테스트합니다.

     **1.** 외부 동적 목록에 대한 외부 동적 목록 항목을 보고 목록에서 IP 주소에 액세스를 시도합니다.

     **2.** 정의한 조치가 시행되었는지 확인하십시오.

     **3.** 모니터 > 로그 > 트래픽을 선택한 다음 세션에 대한 로그 항목을 봅니다.

     **4.** 흐름과 일치하는 정책 규칙을 확인하려면 디바이스 > 문제 해결을 선택한 다음 보안 정책 일치 테스트를 실행합니다.




 ©2023 Palo Alto Networks, Inc.

- 사전 정의된 **URL** 외부 동적 목록을 사용하여 인증 정책에서 애플리케이션이 백그라운드 트래픽에 사용하는 무해한 도메인을 제외합니다**.**

  **panw-auth-portal-exclude-list** EDL 유형을 선택하면 많은 애플리케이션이 업데이트 및 기타 신뢰할 수 있는 서비스와 같은 백그라운드 트래픽에 사용하는 도메인을 인증 정책 시행에서 쉽게 제외할 수 있습니다. 이렇게 하면 방화벽이 이러한 서비스에 필요한 트래픽을 차단하지 않고 애플리케이션 유지 관리가 중단되지 않습니다.

  1. 정책 > 인증을 선택합니다.
  2. 서비스**/URL** 카테고리 탭에서 사전 정의된 URL EDL을 **URL** 카테고리로 선택합니다.
  3. 작업 탭에서 인증 시행으로 **default-no-captive-portal**을 선택합니다.
  4. 확인을 클릭합니다.
  5. 정책의 첫 번째 규칙이 되도록 규칙을 맨 위로 이동합니다.
  6. 변경 사항을 커밋합니다.

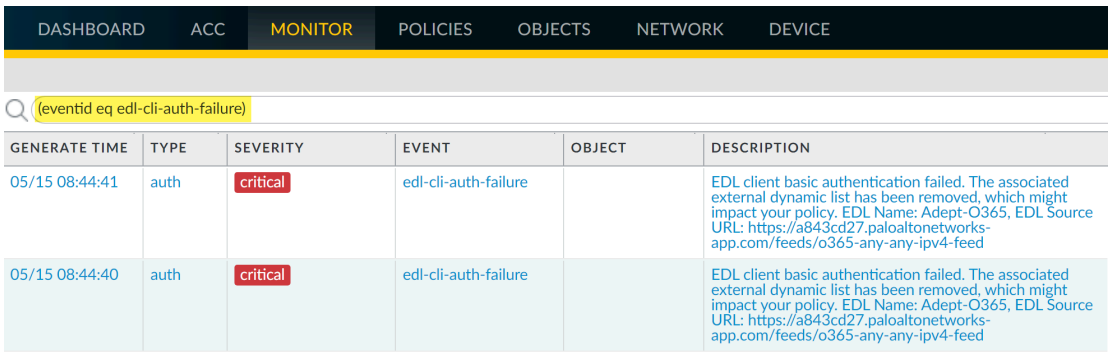
## 인증에 실패한 외부 동적 목록 찾기

SSL이 필요한 외부 동적 목록이 클라이언트 또는 서버 인증에 실패하면 방화벽이 심각한 심각도의 시스템 로그를 생성합니다. 방화벽이 최신 버전을 사용하는 대신 인증에 실패한 후 마지막으로 성공한 외부 동적 목록을 기반으로 정책을 계속 적용하기 때문에 로그가 중요합니다. 다음 프로세스를 사용하여 외부 동적 목록과 관련된 인증 실패를 알리는 중요한 시스템 로그 메시지를 봅니다.

**STEP 1 |** 모니터 > 로그 > 시스템을 선택합니다.

**STEP 2 |** 다음 필터를 구성하여 인증 실패와 관련된 모든 메시지를 보고 필터를 적용합니다. 자세한 내용은 로그 필터링에 대한 전체 워크플로를 검토하십시오.

- 서버 인증 실패 - **(eventid eq tls-edl-auth-failure)**
- 클라이언트 인증 실패 - **(eventid eq edl-cli-auth-failure)**




 ©2023 Palo Alto Networks, Inc.

**STEP 3 |** 시스템 로그 메시지를 검토합니다. 메시지 설명에는 외부 동적 목록의 이름, 목록의 원본 URL 및 인증 실패 이유가 포함됩니다.

인증서가 만료되면 외부 동적 목록을 호스트하는 서버가 인증에 실패합니다. CRL(인증서 해지 목록) 또는 OCSP(온라인 인증서 상태 프로토콜)를 통해 인증서 해지 상태를 확인하도록 인증서 프로파일을 구성한 경우 다음과 같은 경우에도 서버가 인증에 실패할 수 있습니다.

- 인증서가 해지됩니다.
- 인증서의 해지 상태를 알 수 없습니다.
- 방화벽이 CRL/OCSP 서비스에 연결을 시도할 때 연결 시간이 초과되었습니다.

인증서 프로파일 설정에 대한 자세한 내용은 인증서 프로파일 구성 단계를 참조하십시오.

외부 동적 목록으로 구성된 인증서 프로파일에 서버의 루트 *CA* 및 중간 *CA*를 추가했는지 확인합니다. 그렇지 않으면 방화벽이 목록을 제대로 인증하지 않습니다.

외부 동적 목록에 대해 잘못된 사용자 이름과 암호 조합을 입력한 경우 클라이언트 인증이 실패합니다.

**STEP 4 |** (선택 사항) 목록 소유자가 목록을 호스팅하는 서버의 인증서를 갱신할 때까지 중지 인터벌 조치로 인증에 실패한 외부 동적 목록에 대한 인증을 비활성화합니다.

## 외부 동적 목록에 대한 인증 비활성화

Palo Alto Networks는 방화벽에 구성된 외부 동적 목록을 호스트하는 서버에 대해 인증을 사용하도록 설정하는 것이 좋습니다. 그러나 인증에 실패한 외부 동적 목록을 찾고 해당 목록에 대한 서버 인증을 사용하지 않으려면 CLI를 통해 수행할 수 있습니다. 아래 절차는 SSL로 보안이 설정된 외부 동적 목록(즉, HTTPS URL이 있는 목록)에만 적용됩니다. 방화벽은 HTTP URL이 있는 목록에 서버 인증을 적용하지 않습니다.

외부 동적 목록에 대한 서버 인증을 사용하지 않도록 설정하면 클라이언트 인증도 비활성화됩니다. 클라이언트 인증을 사용하지 않도록 설정하면 방화벽을 액세스하기 위해 사용자 이름과 암호가 필요한 외부 동적 목록에 연결할 수 없습니다.

**STEP 1 |** CLI를 실행하고 다음과 같이 구성 모드로 전환합니다.

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

>에서 # 기호로 변경되면 현재 구성 모드에 있음을 나타냅니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 목록 유형에 해당하는 CLI 명령을 입력합니다.

- IP 주소

```
외부 목록 <external dynamic list name> 유형 IP 인증서 프로파일 설정 없음
```

- 도메인

```
외부 목록 <external dynamic list name> 유형 도메인 인증서 프로파일 설정 없음
```

- URL

```
외부 목록 <external dynamic list name> 형식 설정 URL 인증서 프로파일 없음
```

**STEP 3 |** 외부 동적 목록에 대해 인증이 비활성화되어 있는지 확인합니다.

목록에 대한 새로 고침을 트리거합니다(웹 서버에서 외부 동적 목록 검색 참조). 방화벽이 목록을 성공적으로 검색하면 서버 인증이 비활성화됩니다.


©2023 Palo Alto Networks, Inc.

# 동적으로 IP 주소 및 태그 등록

오늘날 네트워크 아키텍처에서는 확장, 유연성 부족 및 성능 문제를 완화하기 위해 필요에 따라 가상 머신(VM) 과 애플리케이션을 프로비저닝, 변경 및 삭제할 수 있습니다. 그러나 이러한 민첩성은 동적으로 프로비저닝된 VM의 IP 주소와 이러한 가상 리소스에서 활성화할 수 있는 수많은 애플리케이션에 대한 가시성이 제한되어 있기 때문에 보안 관리자에게 어려운 과제입니다.

방화벽(하드웨어 기반 및 VM 시리즈 모델)은 IP 주소, IP 세트(IP 범위 및 서브넷) 및 태그를 동적으로 등록하는 기능을 지원합니다. IP 주소와 태그는 방화벽에 직접 등록하거나 Panorama에서 등록할 수 있습니다. 방화벽 로그에 포함된 소스 및 대상 IP 주소의 태그를 자동으로 제거할 수도 있습니다.

*PAN-OS*는 동적 주소 그룹의 ***IPv4 IP*** 서브넷과 범위만 지원합니다**.**

다음 옵션 중 하나를 사용하여 동적 등록 프로세스를 활성화할 수 있습니다.

- **Windows**용 사용자**-ID** 에이전트 - User-ID 에이전트를 배포한 환경에서 User-ID 에이전트를 사용하도록 설정하여 최대 100개의 VMware ESXi 서버, vCenter 서버 또는 이 둘의 조합을 모니터링할 수 있습니다. 이러한 VMware 서버에서 가상 시스템을 프로비저닝하거나 수정하면 에이전트가 IP 주소 변경 사항을 검색하여 방화벽과 공유할 수 있습니다.
- **VM** 정보 소스 - 방화벽에서 VMware ESXi, vCenter Server, AWS-VPC 및 Google 컴퓨트 엔진을 기본적으로 모니터링하고 이러한 소스에서 가상 시스템을 프로비저닝하거나 수정할 때 IP 주소 변경 내용을 검색할 수 있습니다. VM 정보 소스 옵션은 사전 정의된 특성 집합을 폴링하며 XML API를 통해 IP 주소를 등록하기 위해 외부 스크립트가 필요하지 않습니다. 가상 환경의 변화 모니터링을(를) 참조하십시오.
- **Panorama** 플러그인 - Panorama™ M 시리즈 또는 가상 어플라이언스를 사용하여 Azure 또는 AWS 퍼블릭 클라우드 환경에 연결하고 구독 또는 VPC 내에 배포된 가상 머신에 대한 정보를 검색할 수 있습니다. 그런 다음 Panorama가 알림을 위해 구성한 관리되는 Palo Alto Networks 방화벽에 VM 정보를 등록한 다음 이러한 특성을 사용하여 동적 주소 그룹을 정의하고 보안 정책 규칙에 연결하여 이러한 VM을 주고받는 트래픽을 허용하거나 거부할 수 있습니다.
- **VMware Service Manager**(통합 NSX 솔루션만 해당) —통합 NSX 솔루션은 Palo Alto Networks Next-Generation Security Operating Platform®의 자동화된 프로비저닝 및 배포와 Panorama를 사용한 동적 컨텍스트 기반 보안 정책 전달을 위해 설계되었습니다. NSX Manager는 이 통합 솔루션에 배포된 가상 시스템과 관련된 IP 주소, IP 세트 및 태그에 대한 최신 정보로 Panorama를 업데이트합니다. 이 솔루션에 대한 자세한 내용은 VM 시리즈 NSX Edition 방화벽 설정을 참조하십시오.
- **XML API** - 방화벽 및 Panorama는 표준 HTTP 요청을 사용하여 데이터를 송수신하는 XML API를 지원합니다. 이 API를 사용하여 IP 주소와 태그를 방화벽 또는 Panorama에 등록할 수 있습니다. cURL과 같은 명령줄 유틸리티에서 직접 API를 호출하거나 REST 기반 서비스를 지원하는 스크립팅 또는 애플리케이션 프레임워크를 사용하여 API를 호출할 수 있습니다. 자세한 내용은 PAN-OS XML API 사용 안내서를 참조하십시오.
- 자동 태그 - 방화벽에서 로그가 생성될 때 소스 또는 대상 IP 주소에 자동으로 태그를 지정하고 IP 주소 및 태그 매핑을 방화벽이나 Panorama의 User-ID 에이전트 또는 HTTP 서버 프로파일을 사용하여 원격 User-ID 에이전트에 등록합니다. 예를 들어 방화벽이 위협 로그를 생성할 때마다 위협 로그의 소스

 ©2023 Palo Alto Networks, Inc.

IP 주소에 특정 태그 이름을 지정하도록 방화벽을 구성할 수 있습니다. 자세한 내용은 자동 태그 지정을 사용하여 보안 작업 자동화을(를) 참조하십시오.

또한 타임아웃을 사용하여 구성된 시간이 지나면 태그를 동적으로 등록 취소하도록 방화벽을 구성할 수 있습니다. 예를 들어 제한 시간을 IP 주소에 대한 DHCP 리스 타임아웃과 동일하게 구성할 수 있습니다. 이렇게 하면 IP 주소와 태그 간 매핑이 DHCP 리스로 동시에 만료되어 IP 주소가 재할당될 때 의도치 않게 정책을 적용하지 않도록 할 수 있습니다.

HTTP(S) 대상으로 로그 포워딩을 참조하십시오.

동적 주소 그룹 생성 및 사용에 대한 정보는 정책에서 동적 주소 그룹 사용을(를) 참조하십시오.

동적으로 태그를 등록하기 위한 CLI 명령은 동적 IP 주소 및 태그에 대한 CLI 명령을(를) 참조하십시오.


©2023 Palo Alto Networks, Inc.

# 정책에서 동적 사용자 그룹 사용

동적 사용자 그룹을 사용하면 사용자 가시성을 유지하면서 비정상적인 사용자 동작 및 악의적인 활동에 대한 자동 수정을 제공하는 정책을 만들 수 있습니다. 그룹을 생성하고 변경 내용을 커밋한 후 방화벽은 사용자와 연결된 태그를 등록한 다음 동적 사용자 그룹의 구성원을 자동으로 업데이트합니다. 동적 사용자 그룹 구성원에 대한 업데이트는 자동이므로 정적 그룹 개체 대신 동적 사용자 그룹을 사용하면 수동 정책 변경 없이 사용자 동작 또는 잠재적 위협에 대응할 수 있습니다.

구성원으로 포함할 사용자를 결정하기 위해 동적 사용자 그룹은 태그를 필터링 기준으로 사용합니다. 사용자가 필터링 기준과 일치하는 즉시 해당 사용자는 동적 사용자 그룹의 구성원이 됩니다. 태그 기반 필터는 논리적 ***and*** 및 ***or*** 연산자를 사용합니다. 각 태그는 소스에 정적으로 또는 동적으로 등록하는 메타데이터 요소 또는 속성-값 쌍입니다. 정적 태그는 방화벽 구성의 일부이며 동적 태그는 런타임 구성의 일부입니다. 따라서 방화벽에서 커밋한 정책과 이미 연결된 경우 동적 태그에 대한 업데이트를 커밋할 필요가 없습니다.

태그를 동적으로 등록하려면 다음을 사용할 수 있습니다.

- XML API
- User-ID 에이전트
- Panorama
- 방화벽의 웹 인터페이스

방화벽은 동적 사용자 그룹에 대한 태그를 다른 방화벽, Panorama 또는 전용 로그 수집기와 Cortex 애플리케이션을 포함하는 수신 재배포 에이전트에 재배포합니다.

동적 사용자 그룹 태그에 대한 재배포를 지원하려면 모든 방화벽이 ***PAN-OS 9.1***을 사용하여 등록 소스에서 태그를 수신해야 합니다.

방화벽은 동적 사용자 그룹에 대한 태그를 다음 홉에서 특정 서버로 로그를 보내도록 로그 전달을 구성할 수 있습니다. 또한 로그 포싱을 사용하면 자동 태그 지정을 사용하여 로그의 이벤트에 따라 동적 사용자 그룹의 구성원을 자동으로 추가하거나 제거할 수 있습니다.

**STEP 1 |** 개체 > 동적 사용자 그룹을 선택하고 새 동적 사용자 그룹을 추가합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 동적 사용자 그룹의 구성원을 정의합니다.

1. 그룹의 이름을 입력합니다.
2. (선택 사항) 그룹에 대한 설명을 입력합니다.
3. 동적 태그를 사용하여 일치 기준을 추가하여 동적 사용자 그룹의 구성원을 정의합니다.
4. (선택 사항) 필터링하거나 일치시킬 태그와 함께 **And** 또는 **Or** 연산자를 사용합니다.
5. 확인을 클릭합니다.
6. (선택 사항) 그룹 자체에 할당하려는 태그를 선택합니다.

   이 태그는 동적 사용자 그룹 목록의 태그 열에 표시되며 그룹의 구성원이 아닌 동적 그룹 개체를 정의합니다.
7. 확인을 클릭하고 변경 사항을 커밋합니다.

   사용자 그룹 개체 필터를 업데이트하는 경우 구성을 업데이트하려면 변경 내용을 커밋해야 합니다.

**STEP 3 |** 일치 기준으로 사용하려는 로그 정보에 따라 로그 전달 프로파일을 생성하거나 로그 설정을 구성하여 자동 태그 지정을 구성합니다.

- 인증, 데이터, 위협, 트래픽, 터널 검사, URL 및 WildFire 로그를 위해 로그 포워딩 프로파일을 생성합니다.
- User-ID, GlobalProtect 및 IP 태그 로그의 경우 로그 설정을 구성합니다.

**STEP 4 |** (선택 사항) 특정 기간 후에 동적 사용자 그룹 구성원을 원래 그룹으로 되돌리려면 시간 초과 값을 분 단위로 입력합니다(기본값은 0, 범위는 0-43200).

**STEP 5 |** 정책에서 동적 사용자 그룹을 사용하여 그룹 구성원의 트래픽을 규제합니다.

최소한 두 개의 규칙을 만들어야 합니다. 하나는 동적 사용자 그룹을 채우는 초기 트래픽을 허용하고 다른 하나는 방지하려는 활동에 대한 트래픽을 거부합니다. 사용자를 태그하려면 트래픽을 허용하는 규칙은 트래픽을 거부하는 규칙보다 규칙 베이스에 더 높은 규칙 번호를 가져야 합니다.

1. 1단계의 동적 사용자 그룹을 소스 사용자로 선택합니다.
2. 작업이 동적 사용자 그룹 구성원에 대한 트래픽을 거부하는 규칙을 만듭니다.
3. 트래픽이 동적 사용자 그룹 구성원을 채울 수 있도록 하는 규칙을 생성합니다.
4. 3단계에서 로그 포워딩 프로파일을 구성한 경우 정책에 추가할 프로파일을 선택합니다.
5. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 6 |** (선택 사항) 그룹의 구성원을 구체화하고 사용자 태그 매핑 업데이트에 대한 등록 소스를 정의합니다.

초기 사용자 - 태그 매핑이 구성원이 아니어야 하는 사용자를 검색하거나 있어야 하는 사용자를 포함하지 않는 경우 그룹의 구성원을 수정하여 정책을 적용하려는 사용자를 포함하도록 수정하고 매핑의 소스를 지정합니다.

1. 사용자 열에서 더보기를 선택합니다.
2. 사용자를 등록하여 그룹에 추가하고 태그 및 사용자-태그 매핑에 대한 등록 소스를 선택합니다.
   - 로컬(기본값) - 방화벽에서 동적 사용자 그룹 구성원에 대한 태그 및 매핑을 등록합니다.
   - **Panorama User-ID** 에이전트 - Panorama에 연결된 User-ID 에이전트에 동적 사용자 그룹 구성원에 대한 태그 및 매핑을 등록합니다. 동적 사용자 그룹이 Panorama에서 유래하는 경우 행이 노란색으로 표시되고 그룹 이름, 설명, 일치 기준 및 태그는 읽기 전용입니다. 그러나 그룹에서 사용자를 등록하거나 등록 취소할 수 있습니다.
   - 원격 디바이스 **User-ID** 에이전트 - 원격 User-ID 에이전트에서 동적 사용자 그룹 구성원에 대한 태그 및 매핑을 등록합니다. 이 옵션을 선택하려면 먼저 HTTP 서버 프로파일을 구성해야 합니다.
3. 그룹을 구성하는 데 사용한 태그를 사용하여 소스에 등록하려는 태그를 선택합니다.
4. (선택 사항) 특정 기간 후에 동적 사용자 그룹 구성원을 원래 그룹으로 되돌리려면 시간 초과 값을 분 단위로 입력합니다(기본값은 0, 범위는 0-43200).
5. 필요에 따라 사용자를 추가 또는 삭제합니다.
6. (선택 사항) 사용자 등록을 취소하여 태그 및 사용자-태그 매핑을 제거합니다.

**STEP 7 |** 방화벽이 동적 사용자 그룹의 사용자를 올바르게 채우는지 확인합니다.

1. 트래픽, 위협, URL 필터링, WildFire 제출, 데이터 필터링 및 터널 검사 로그에서 동적 사용자 그룹 열이 동적 사용자 그룹을 올바르게 표시하도록 확인합니다.
2. **show user group list dynamic** 명령을 사용하여 모든 동적 사용자 그룹의 목록과 동적 사용자 그룹의 총 수를 표시합니다.
3. 동적 사용자 그룹의 등록된 구성원인 사용자 목록을 표시하려면 **show object registered-user all** 명령을 사용하십시오.
4. **show user group name *group-name*** 명령을 사용하여 소스 유형과 같은 동적 사용자 그룹에 대한 정보를 표시합니다.


©2023 Palo Alto Networks, Inc.

# 자동 태그 지정을 사용하여 보안 작업 자동화

자동 태그 지정을 사용하면 방화벽이나 Panorama가 특정 기준과 일치하는 로그를 수신하고 IP 주소와 태그 간 매핑 또는 사용자 대 태그 매핑을 설정할 때 정책 개체에 태그를 지정할 수 있습니다. 예를 들어 방화벽에서 위협 로그를 생성할 때 위협 로그의 소스 IP 주소 또는 소스 사용자에게 특정 태그 이름을 지정하도록 방화벽을 구성할 수 있습니다. 그런 다음 이러한 태그를 사용하여 동적 사용자 그룹 또는 동적 주소 그룹과 같은 정책 개체를 자동으로 채운 다음 보안, 인증 또는 복호화 정책의 보안 작업을 자동화하는 데 사용할 수 있습니다. 예를 들어 자격 증명 검색됨 열에서 **'예'**에 대한 URL 로그에 대해 필터를 생성할 때 사용자가 멀티 팩터 인증(MFA)을 사용하여 인증하도록 요구하는 인증 정책을 적용하는 태그를 사용자에게 적용할 수 있습니다.

동적 사용자 그룹은 ***HIP*** 일치 로그의 자동 태그 지정을 지원하지 않습니다**.**

방화벽 또는 Panorama의 PAN-OS 통합 User-ID 에이전트 또는 HTTP 서버 프로파일을 사용하여 원격 User-ID 에이전트에 IP 주소-태그 및 사용자 - 태그 매핑을 등록하여 네트워크 전체에 매핑을 재배포합니다. 로그 포워딩 프로파일에 대한 기본 제공 작업의 일부로 타임아웃을 구성하거나 로그 포워딩 설정의 일부로 방화벽은 IP 주소 또는 사용자와 연결된 태그를 자동으로 제거(등록 취소)할 수 있습니다. 예를 들어 방화벽이 사용자의 자격 증명이 손상되었을 가능성이 있음을 감지하면 지정된 기간 동안 해당 사용자에 대해 MFA 인증을 요구하도록 방화벽을 구성한 다음 제한 시간을 구성하여 MFA 요구 사항 그룹에서 사용자를 제거할 수 있습니다.

**STEP 1 |** 태그 지정에 사용할 로그 유형에 따라 로그 포워딩 프로파일을 만들거나 로그 설정을 구성하여 방화벽 또는 Panorama에서 로그를 처리하는 방법을 정의합니다.

- 인증, 데이터, 위협, 트래픽, 터널 검사, URL 및 WildFire 로그의 경우 로그 포워딩 프로파일을 생성합니다.
- 사용자 ID, GlobalProtect 및 IP 태그 로그의 경우 로그 설정을 구성합니다.

**STEP 2 |** 방화벽 또는 Panorama가 정책 개체에 태그를 추가하는 시기를 결정하는 일치 목록 조건을 정의합니다.

예를 들어 필터를 사용하여 임계값을 구성하거나 값을 정의할 수 있습니다(예: 방화벽이 아직 매핑되지 않은 사용자를 식별하는 **user eq "unknown"**). 방화벽이 해당 임계값에 도달하거나 해당 값을 찾으면 방화벽이 태그를 추가합니다.

- 로그 포워딩 프로파일을 만들려면 프로파일을 추가하고 일치 목록 조건을 모니터링할 로그 유형(개체 > 로그 포워딩)을 선택합니다.
- 로그 설정을 구성하려면 일치 목록 기준에 대해 모니터링할 로그 유형에 대한 로그 설정을 추가합니다(디바이스 > 로그 설정).

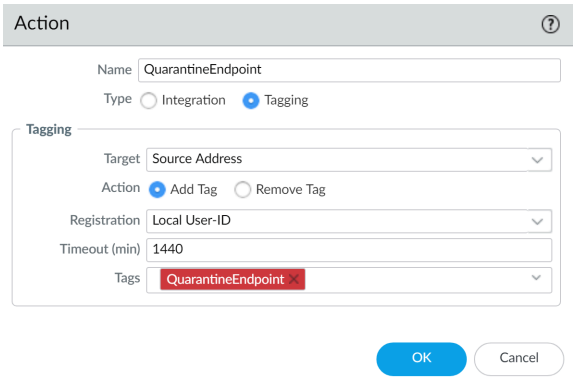
**STEP 3 |** 필터 값을 복사하여 붙여넣거나 필터 빌더를 사용하여 태그의 일치 기준을 정의합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 기본 제공 작업을 추가하여 정책 개체에 태그를 지정합니다.

1. 로그에 일치 목록 기준을 충족하는 항목이 포함되어 있을 때 방화벽 또는 Panorama에서 수행할 기본 제공 동작을 추가합니다.
2. 작업 이름을 지정합니다.
3. 태그를 지정할 **Target** 유형을 선택합니다(**Destination Address**, **Source Address**, **User** 또는 **X-Forwarded -**주소).
4. 태그 추가가 액션인지 확인합니다.
5. 태그의 등록 소스를 선택하여 방화벽 또는 Panorama가 IP 주소-태그 매핑을 재배포하는 방법을 결정합니다.
   - 로컬 **User-ID** - 방화벽 또는 Panorama의 User-ID 에이전트에서 IP 주소와 태그 매핑을 재배포합니다.
   - **Panorama User-ID** - Panorama에서 IP 주소와 태그 매핑을 재배포합니다.
   - 원격 **User-ID** - HTTP 서버 프로파일을 사용하여 IP 주소와 태그 매핑을 다른 User-ID 에이전트에 재배포합니다. 이 옵션을 선택하는 경우 HTTP 서버 프로파일을 구성해야 합니다(5단계 참조).
6. 정책 개체에 추가할 태그를 입력하거나 선택합니다.

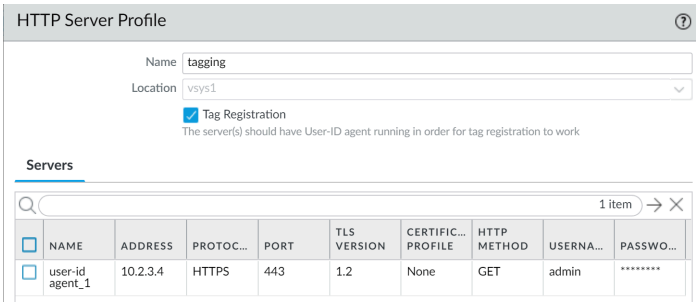
   필드 외부를 클릭하거나 Enter 키를 눌러 확인 버튼을 활성화해야 할 수 있습니다.
7. 확인을 클릭합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 5 |** (원격 User-ID만 해당) 로그를 원격 User-ID 에이전트에 포워딩하도록 HTTP 서버 프로파일을 구성합니다.

1. 디바이스 > 서버 프로파일 > **HTTP**를 선택합니다.
2. 프로파일을 추가하고 서버 프로파일의 이름을 지정합니다.
3. (가상 시스템만) 위치를 선택합니다. 프로파일은 모든 가상 시스템에서 공유되거나 특정 가상 시스템에 속할 수 있습니다.
4. 방화벽이 원격 방화벽의 User-ID 에이전트에 IP 주소 및 태그 매핑을 등록할 수 있도록 하려면 태그 등록을 선택합니다. 태그 등록이 활성화되면 페이로드 형식을 지정할 수 없습니다.
5. 원격 User-ID 에이전트에 액세스하기 위한 서버 연결 세부 정보를 추가하고 확인을 클릭합니다.




6. 만든 로그 포워딩 프로파일을 선택한 다음 이 서버 프로파일을 원격 **User-ID** 태그 등록에 대한 HTTP 서버 프로파일로 선택합니다.

**STEP 6 |** 태그를 적용할 정책 개체를 정의합니다.

1. 동적 주소 그룹, 정책에서 동적 사용자 그룹 사용, 주소, 주소 그룹, 영역, 정책 규칙, 서비스 또는 서비스 그룹 중 하나를 만들거나 선택합니다.
2. 일치 조건으로 개체에 적용할 태그를 입력합니다.

   태그가 4단계의 태그와 동일한지 확인합니다.

**STEP 7 |** 태그가 지정된 정책 개체를 정책에 추가합니다.

이 워크플로에서는 보안 정책을 예로 들지만 인증 정책에서 태그가 지정된 정책 개체를 사용할 수도 있습니다.

1. 정책 > 보안을 선택합니다.
2. 추가를 클릭하고 정책에 대한 이름 및 선택적으로 설명을 입력합니다.
3. 트래픽이 발생하는 소스 영역을 추가합니다.
4. 트래픽이 종료되는 대상 영역을 추가합니다.
5. 5.1단계에서 생성한 **Source** 개체를 선택합니다.
6. 규칙에서 트래픽을 허용할지 아니면 거부할지를 선택합니다.

**STEP 8 |** 로그 전달 프로파일을 구성한 경우 보안 정책에 할당합니다.

각 정책에 대해 하나의 로그 포워딩 프로파일을 할당할 수 있지만 프로파일당 여러 메서드와 작업을 할당할 수 있습니다. 예제는 정책에서 동적 주소 그룹 사용을(를) 참조하십시오.

**STEP 9 |** 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

**STEP 10 |** (선택 사항) 지정된 시간이 경과한 후 정책 개체에서 태그를 제거하도록 제한 시간을 구성합니다.

방화벽이 정책 개체에서 태그를 제거하기 전까지 경과하는 시간(분)을 지정합니다. 범위는 0에서 43,200 사이입니다. 시간 제한을 0으로 설정하면 IP 주소와 태그 간 매핑이 타임아웃되지 않으므로 명시적 작업으로 제거해야 합니다. 제한 시간을 최대 43,200분으로 설정하면 방화벽이 30일 후에 태그를 제거합니다.



태그 제거 작업을 사용하여 타임아웃을 구성할 수 없습니다.

1. 로그 전달 프로파일을 선택합니다.
2. 기본 제공 동작 중 하나를 추가하거나 편집합니다.
3. 타임아웃(분)를 지정합니다. 지정된 시간이 경과하면 방화벽 또는 Panorama가 태그를 제거합니다.

   ***IP*** 태그 타임아웃을 해당 ***IP*** 주소에 대한 ***DHCP*** 리스 타임아웃와 동일한 시간으로 설정합니다. 이렇게 하면 ***IP*** 주소와 태그 간 매핑이 ***DHCP*** 임대로 동시에 만료되어 ***IP*** 주소가 재할당될 때 의도치 않게 정책을 적용하지 않도록 할 수 있습니다.
4. 확인을 클릭하고 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 가상 환경의 변화 모니터링

새로운 사용자와 서버가 지속적으로 등장하는 환경에서 애플리케이션을 보호하고 위협을 방지하려면 보안 정책이 신속해야 합니다. 신속하게 대응하려면 방화벽이 새 IP 주소나 수정된 IP 주소를 파악하고 방화벽의 구성을 변경하지 않고도 정책을 일관되게 적용할 수 있어야 합니다.

이 기능은 **VM** 정보 소스와 방화벽의 동적 주소 그룹 기능 간의 조정을 통해 제공됩니다. 방화벽 및 Panorama는 모니터링되는 각 소스의 가상 시스템(또는 게스트) 인벤토리에 대한 정보를 수집하고 네트워크의 동적 변경 내용과 동기화된 정책 개체를 만드는 자동화된 방법을 제공합니다.

- 가상 네트워크에서 변경 사항을 추적하기 위해 VM 모니터링 사용
- Cloud Platforms의 가상 머신에서 모니터링되는 속성
- 정책에서 동적 주소 그룹 사용

## 가상 네트워크에서 변경 사항을 추적하기 위해 VM 모니터링 사용

VM 정보 소스는 모니터링되는 각 소스(호스트)의 가상 머신(VM) 인벤토리에 대한 정보를 수집하는 자동화된 방법을 제공합니다. 방화벽은 VMware ESXi, vCenter Server, AWS-VPC, Microsoft Azure VNet 및 Google Cloud를 모니터링할 수 있습니다. 가상 머신(게스트)이 배포되거나 이동되면 방화벽은 사전 정의된 속성(또는 메타데이터 요소) 집합을 태그로 수집합니다. 그런 다음 이러한 태그를 사용하여 동적 주소 그룹을 정의하고(정책에서 동적 주소 그룹 사용 참조) 정책에서 일치시킬 수 있습니다.

방화벽을 직접 구성하거나 Panorama 템플릿을 사용하여 최대 10개의 VM 정보 소스를 모니터링할 수 있습니다. **VM** 정보 소스는 손쉬운 구성을 제공하고 사전 정의된 16개의 메타데이터 요소 또는 속성 집합을 모니터링할 수 있도록 합니다. 목록은 Cloud Platforms의 가상 머신에서 모니터링되는 속성을 참조하세요. 기본적으로 방화벽과 모니터링되는 소스 간의 트래픽은 방화벽의 관리(MGT) 포트를 사용합니다.

- VM 시리즈 NSX 에디션 솔루션의 일부인 *ESXi* 호스트를 모니터링할 때 *VM* 정보 소스를 사용하는 대신 동적 주소 그룹을 사용하여 가상 환경의 변경 사항에 대해 알아보십시오. *VM* 시리즈 *NSX* 에디션 솔루션의 경우 *NSX Manager*는 *Panorama*에 *IP* 주소가 속한 *NSX* 보안 그룹에 대한 정보를 제공합니다. *NSX Manager*의 정보는 서비스 프로파일 *ID*를 구별 속성으로 사용하고 서로 다른 *NSX* 보안 그룹에 중복되는 *IP* 주소가 있을 때 정책을 적절히 적용할 수 있기 때문에 동적 주소 그룹에서 일치 조건을 정의하기 위한 전체 컨텍스트를 제공합니다. *IP* 주소에 등록할 수 있는 최대 *32*개의 태그*(vCenter* 서버 및 *NSX Manager*에서*).*
- *Azure* 배포 내에서 가상 머신을 모니터링하려면 *VM* 모니터링 소스 대신 *Azure* 퍼블릭 클라우드 내의 가상 머신에서 실행되는 VM 모니터링 스크립트를 배포해야 합니다. 이 스크립트는 *Azure* 자산에 대한 *IP* 주소-태그 매핑 정보를 수집하고 스크립트에서 지정한 방화벽 및 해당 가상 시스템에 게시합니다.
- *Panorama* 버전 *8.1.3* 이상의 경우 *AWS* 또는 *Azure*용 *Panorama* 플러그인을 사용하여 *VM* 정보를 검색하고 관리되는 방화벽에 등록할 수도 있습니다. 자세한 내용은 Cloud Platforms의 가상 머신에서 모니터링되는 속성을 참조하세요.

**STEP 1 |** VM 모니터링을 활성화합니다.

각 방화벽 또는 여러 가상 시스템 지원 방화벽의 각 가상 시스템에 대해 최대 *10*개의 *VM* 정보 소스를 구성할 수 있습니다.

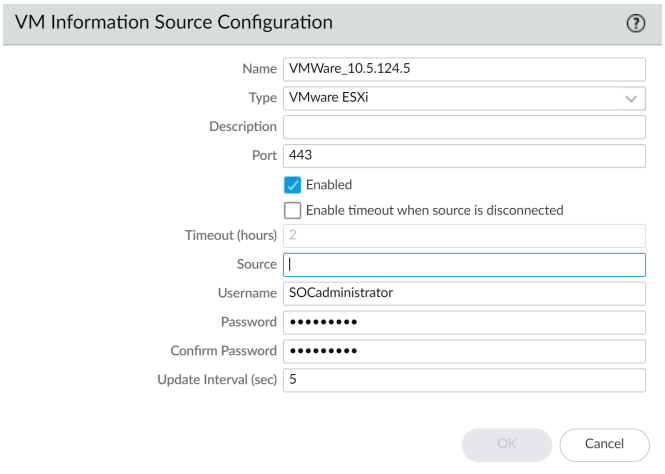

©2023 Palo Alto Networks, Inc.

방화벽이 고가용성 구성으로 구성된 경우:

- 능동형/수동형 설정에서는 능동형 방화벽만 VM 소스를 모니터링합니다.
- 능동형/능동형 설정에서는 우선 순위 값이 기본인 방화벽만 VM 소스를 모니터링합니다.

1. 디바이스 > **VM** 정보 소스를 선택합니다. 이 예에서는 VMware ESX (i) 또는 vCenter 서버를 추가하는 방법을 보여 줍니다.
2. 추가를 클릭하고 다음 정보를 입력합니다.
   - 모니터링할 소스를 식별하는 이름입니다.
   - 유형을 선택하여 소스가 **AWS VPC**, **Google Compute Engine** 인스턴스, **VMware ESX(i)** 서버 또는 **VMware vCenter** Server인지의 여부를 나타냅니다.

     선택한 유형에 따라 표시되는 필드가 결정됩니다.
   - 소스가 수신하는 포트를 입력하십시오.
   - 기본값을 변경하려면 소스 연결이 끊겼을 때 타임아웃 활성화 체크박스를 선택한 다음 값을 지정합니다. 지정된 제한에 도달하거나 호스트에 액세스할 수 없거나 응답하지 않으면 방화벽이 소스에 대한 연결을 닫습니다.
   - 위에서 지정한 서버에 인증할 자격 증명(사용자 이름 및 암호)을 추가합니다.
   - 소스(호스트 이름 또는 IP 주소)를 정의합니다.
   - (선택 사항) 업데이트 인터벌을 5-600초 사이의 값으로 수정합니다. 기본적으로 방화벽은 5초마다 폴링합니다. API 호출은 큐에 대기되고 60초마다 검색되므로 업데이트에는 구성된 폴링 인터벌을 더한 시간이 최대 60초까지 걸릴 수 있습니다.

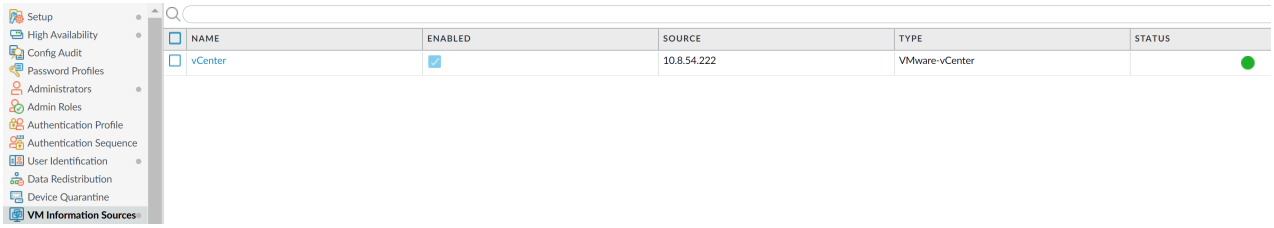



   - 확인을 클릭하고 변경 사항을 커밋합니다.
   - 연결 상태가 연결됨으로 표시되는지 확인합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 연결 상태를 확인하십시오.

연결 상태가 연결됨으로 표시되는지 확인합니다.




연결 상태가 보류 중이거나 연결이 끊긴 경우 소스가 작동 중이고 방화벽이 소스에 액세스할 수 있는지 확인하십시오. 모니터링되는 소스와 통신하기 위해 MGT 포트 이외의 포트를 사용하는 경우 서비스 경로를 변경해야 합니다( **Device** > **Setup** > **Services**, 서비스 경로 구성 링크를 클릭하고 **VM** 모니터 서비스에 대한 소스 인터페이스 수정).

# Cloud Platforms의 가상 머신에서 모니터링되는 속성

프라이빗 또는 퍼블릭 클라우드에서 가상 컴퓨터를 프로비저닝하거나 제거할 때 차세대 방화벽의 Panorama 플러그인, VM 모니터링 스크립트 또는 VM 정보 소스를 사용하여 가상 환경에 배포된 가상 머신(VM)의 변경 사항을 모니터링할 수 있습니다.

**VM** 정보 소스 - 하드웨어 또는 VM 시리즈 방화벽에서 가상 시스템 인스턴스를 모니터링하고 모니터링되는 소스(AWS, ESXi 또는 vCenter Server 또는 AWS)에 구성된 게스트를 프로비저닝하거나 수정하면서 변경 사항을 검색할 수 있습니다. 각 방화벽(및/또는 방화벽에 여러 가상 시스템 기능이 있는 경우, 가상 시스템)에 대해 최대 10개의 소스를 구성할 수 있습니다. VM 정보 소스 및 동적 주소 그룹이 동시에 작동하고 가상 환경의 변경 사항을 모니터링하는 방법에 대한 자세한 내용은 VM 시리즈 배포 가이드를 참조하십시오. 방화벽이 고가용성 구성으로 구성된 경우:

- 능동/수동 설정에서는 활성 방화벽만 VM 정보 소스를 모니터링합니다.
- 활성/활성 설정에서는 기본 방화벽만 VM 정보 소스를 모니터링합니다.

**Panorama** 플러그인 - Panorama(하드웨어 어플라이언스 또는 버전 8.1.3을 실행하는 가상 어플라이언스)에서 Microsoft Azure 및 AWS용 플러그인을 설치할 수 있습니다. 플러그인을 사용하면 Panorama를 Azure 퍼블릭 클라우드 구독 또는 AWS VPC에 연결하고 가상 머신의 IP 주소 대 태그 매핑을 검색할 수 있습니다. 그런 다음 Panorama는 알림을 위해 구성한 관리되는 Palo Alto Networks® 방화벽에 VM 정보를 등록합니다.

다음 섹션을 사용하여 각 클라우드 공급업체에서 지원되는 옵션과 동적 주소 그룹을 생성하기 위해 모니터링할 수 있는 가상 컴퓨터 특성을 검토합니다.

- VMware ESXi
- Amazon Web Services(AWS)
- Microsoft Azure
- Google

## VMware ESXi

모니터링되는 ESXi 또는 vCenter 서버의 각 VM에는 VMware Tools가 설치되어 실행 중이어야 합니다. VMware Tools는 각 VM에 할당된 IP 주소와 기타 값을 수집할 수 있는 기능을 제공합니다.

 ©2023 Palo Alto Networks, Inc.

*VM* 시리즈 *NSX* 에디션 솔루션의 일부인 *ESXi* 호스트를 모니터링할 때는 *VM* 정보 소스를 사용하는 대신 동적 주소 그룹을 사용하여 가상 환경의 변경 사항에 대해 알아봅니다. *VM* 시리즈 *NSX* 에디션 솔루션의 경우 *NSX Manager*는 *Panorama*에 *IP* 주소가 속한 *NSX* 보안 그룹에 대한 정보를 제공합니다. *NSX Manager*의 정보는 서비스 프로파일 *ID*를 구별 속성으로 사용하고 서로 다른 *NSX* 보안 그룹에 중복되는 *IP* 주소가 있을 때 정책을 적절히 적용할 수 있기 때문에 동적 주소 그룹에서 일치 조건을 정의하기 위한 전체 컨텍스트를 제공합니다.

최대 *32*개의 태그*(vCenter* 서버 및 *NSX* 관리자의 경우*)*를 *IP* 주소에 등록할 수 있습니다.

모니터링되는 VM에 할당된 값을 수집하려면 방화벽의 VM 정보 소스를 사용하여 다음과 같은 사전 정의된 ESXi 특성 집합을 모니터링합니다.

| **VMware** 소스에서 모니터링되는 특성 |
| --- |
| UUID |
| 이름 |
| 게스트 OS |
| VM 상태 - 전원 상태는 PowereOff, PowerOn, 대기 상태 및 알 수 없음일 수 있습니다. |
| 주석 |
| 버전 |
| 네트워크 - 가상 스위치 이름, 포트 그룹 이름 및 VLAN ID |
| 컨테이너 이름 - vCenter 이름, 데이터 센터 개체 이름, 리소스 풀 이름, 클러스터 이름, 호스트, 호스트 IP 주소 |

## Amazon Web Services(AWS)

AWS VPC에서 가상 머신을 프로비저닝하거나 수정할 때 이러한 인스턴스를 모니터링하고 동적 주소 그룹에서 일치 기준으로 사용할 태그를 검색하는 두 가지 방법이 있습니다.

- **VM** 정보 소스 - 차세대 방화벽에서는 사전 정의된 14개의 태그 및 18개의 사용자 정의 키-값 페어(태그) 등 총 32개의 태그를 모니터링할 수 있습니다. 동적 주소 그룹에 대한 일치 조건으로 다음 특성(또는 태그 이름)을 사용할 수 있습니다.
- **Panorama**의 **AWS** 플러그인 - AWS용 Panorama 플러그인을 사용하면 Panorama를 AWS VPC에 연결하고 AWS 가상 머신의 IP 주소 대 태그 매핑을 검색할 수 있습니다. 그런 다음 Panorama는 알림을 위해 구성한 관리되는 Palo Alto Networks® 방화벽에 VM 정보를 등록합니다. Panorama는 플러그인을 사용하여 각 가상 머신에 대해 총 32개의 태그, 11개의 사전 정의된 태그 및 최대 21개의 사용자 정의 태그를 검색할 수 있습니다.


©2023 Palo Alto Networks, Inc.

| AWS-VPC에서 모니터링되는 특성 | 방화벽의 VM 정보 소스 | Panorama의 AWS 플러그인 |
|---|---|---|
| 아키텍처 | 예 | 아니요 |
| 게스트 OS | 예 | 아니요 |
| AMI ID | 예 | 예 |
| IAM 인스턴스 프로파일 | 아니요 | 예 |
| 인스턴스 ID | 예 | 아니요 |
| 인스턴스 상태 | 예 | 아니요 |
| 인스턴스 유형 | 예 | 아니요 |
| 키 이름 | 예 | 예 |
| 소유자 ID | 아니요 | 예 |
| 배치 - 테넌시 | 예 | 예 |
| 배치 - 그룹 이름 | 예 | 예 |
| 배치 - 가용 영역 | 예 | 예 |
| 프라이빗 DNS 이름 | 예 | 아니요 |
| 퍼블릭 DNS 이름 | 예 | 예 |
| 서브넷 ID | 예 | 예 |
| 보안 그룹 ID | 아니요 | 예 |
| 보안 그룹 이름 | 아니요 | 예 |
| VPC ID | 예 | 예 |
| 태그(키, 값) | 예.<br>최대 18개의 사용자 정의 태그가 지원됩니다. 사용자 정의 태그는 알파벳순으로 정렬되며 처음 18개 태그는 방화벽에서 사용할 수 있습니다. | 예.<br>최대 21개의 사용자 정의 태그가 지원됩니다. 사용자 정의 태그는 알파벳순으로 정렬되며, 처음 21개의 태그는 Panorama 및 방화벽에서 사용할 수 있습니다. |


©2023 Palo Alto Networks, Inc.

## Microsoft Azure

Azure에서 VM 모니터링의 경우 Azure VM에 대한 IP 주소-태그 매핑을 검색하고 동적 주소 그룹에서 일치 조건으로 사용할 수 있도록 해야 합니다. Microsoft Azure용 Panorama 플러그인을 사용하면 Panorama를 Azure 공용 클라우드 구독에 연결하고 Azure 가상 컴퓨터에 대한 IP 주소-태그 매핑을 검색할 수 있습니다. Panorama는 각 가상 머신에 대해 총 26개의 태그, 11개의 사전 정의된 태그 및 최대 15개의 사용자 정의 태그를 검색하고 알림을 위해 구성한 관리형 Palo Alto Networks® 방화벽에 VM 정보를 등록할 수 있습니다.

Azure용 Panorama 플러그인을 사용하면 Microsoft Azure 배포 내에서 다음과 같은 가상 컴퓨터 특성 집합을 모니터링할 수 있습니다.

| **Microsoft Azure**에서 모니터링되는 특성 | **Panorama**의 **Azure** 플러그인 |
|---|---|
| VM 이름 | 예 |
| VM 크기 | 아니요 |
| 네트워크 보안 그룹 이름 | 예 |
| OS 유형 | 예 |
| OS 퍼블리셔 | 예 |
| OS 오퍼 | 예 |
| OS SKU | 예 |
| 서브넷 | 예 |
| VNet | 예 |
| Azure 리전 | 예 |
| 리소스 그룹 이름 | 예 |
| 구독 ID | 예 |
| 사용자 정의 태그 | 예.<br>최대 15개의 사용자 정의 태그가 지원됩니다. 사용자 정의 태그는 알파벳순으로 정렬되어 있으며, 처음 15개 태그는 Panorama 및 방화벽에서 사용할 수 있습니다. |


©2023 Palo Alto Networks, Inc.

### Google

차세대 방화벽에서 VM 정보 소스를 사용하여 다음과 같은 사전 정의된 Google 컴퓨팅 엔진(GCE) 속성 집합을 모니터링할 수 있습니다.

방화벽에서는 고가용성이 지원되지 않습니다.

| Google 컴퓨트 엔진에서 모니터링되는 속성 |
| --- |
| VM의 호스트 이름 |
| 머신 유형 |
| 프로젝트 ID |
| 소스(OS 유형) |
| 상태 |
| 서브네트워크 |
| VPC 네트워크 |

## 정책에서 동적 주소 그룹 사용

동적 주소 그룹은 정책에 사용됩니다. 이를 통해 서버의 추가, 이동 또는 삭제와 같은 변경 사항에 자동으로 적응하는 정책을 만들 수 있습니다. 또한 네트워크, 운영 체제 또는 프로세스의 다양한 종류의 트래픽에서 해당 역할을 정의하는 태그를 기반으로 동일한 서버에 서로 다른 규칙을 적용할 수 있습니다.

동적 주소 그룹은 태그를 필터링 기준으로 사용하여 멤버를 결정합니다. 필터는 로지컬 ***and*** 및 ***or*** 연산자를 사용합니다. 필터링 기준과 일치하는 모든 IP 주소 또는 주소 그룹은 동적 주소 그룹의 구성원이 됩니다. 태그는 방화벽에서 정적으로 정의되거나 방화벽에 (동적으로) 등록될 수 있습니다. 정적 태그와 동적 태그의 차이점은 정적 태그는 방화벽 구성의 일부이고 동적 태그는 런타임 구성의 일부라는 것입니다. 이는 동적 태그를 업데이트하기 위해 커밋이 필요하지 않음을 의미합니다. 그러나 코드는 정책에서 참조되는 동적 주소 그룹에서 사용해야 하며 정책은 방화벽에서 커밋되어야 합니다.

태그를 동적으로 등록하려면 방화벽 또는 User-ID 에이전트에서 XML API 또는 VM 모니터링 에이전트를 사용할 수 있습니다. 각 태그는 방화벽 또는 Panorama에 등록된 메타데이터 요소 또는 특성 값 쌍입니다. 예를 들어, IP1 {tag1, tag2,.....tag32}가 있으며 여기서 IP 주소 및 관련 태그는 목록으로 유지됩니다. 등록된 각 IP 주소는 운영 체제, 데이터 센터 또는 해당 주소가 속한 가상 스위치와 같이 최대 32개의 태그를 가질 수 있습니다. API 호출을 받은 후 방화벽은 IP 주소와 관련 태그를 등록하고 동적 주소 그룹의 구성원 정보를 자동으로 업데이트합니다.

각 모델에 대해 등록할 수 있는 IP 주소의 최대 수는 다릅니다. 모델의 세부 사항에 대해 다음 표를 사용합니다.

 ©2023 Palo Alto Networks, Inc.

| 모델 | 동적으로 등록된 **IP** 주소의 최대 수 |
|---|---|
| M 시리즈 및 Panorama 가상 가전 제품 | 500,000 |
| PA-5400 시리즈(PA-5450 제외), PA-5200 시리즈, VM-7000 SMC-B 시리즈 | 500,000 |
| VM-500, VM-700 | 300,000 |
| PA-3430, PA-3440, PA-3200 시리즈, VM-300 | 200,000 |
| PA-3410, PA-3420 | 150,000 |
| PA-7000 시리즈, PA-5450, PA-450, PA-460 | 100,000 |
| PA-440 | 50,000 |
| PA-850, VM-100 | 2,500 |
| PA-820, PA-410, PA-220, VM-50 | 1,000 |

***IP*** 범위 또는 서브넷과 같은 ***IP*** 집합은 각 방화벽 모델에서 지원하는 등록된 ***IP*** 주소의 최대 수로 계산될 때 등록된 단일 ***IP*** 주소로 간주됩니다.

다음 예는 동적 주소 그룹이 네트워크 보안 시행을 단순화할 수 있는 방법을 보여줍니다. 예제 워크플로는 다음을 수행하는 방법을 보여줍니다.

- 방화벽에서 VM 모니터링 에이전트를 활성화하고 VMware ESX(i) 호스트 또는 vCenter Server를 모니터링하고 VM IP 주소와 관련 태그를 등록합니다.
- 동적 주소 그룹을 생성하고 필터링할 태그를 정의합니다. 이 예제에서는 두 개의 주소 그룹이 만들어집니다. 하나는 동적 태그만 필터링하고 다른 하나는 정적 및 동적 태그를 모두 필터링하여 그룹 구성원을 채웁니다.
- 동적 주소 그룹의 구성원이 방화벽에 채워져 있는지 확인합니다.
- 정책에 동적 주소 그룹을 사용합니다. 이 예제에서는 두 가지 다른 보안 정책을 사용합니다.
  - FTP 서버로 배포되는 모든 Linux 서버에 대한 보안 정책입니다. 이 규칙은 동적으로 등록된 태그와 일치합니다.
  - 웹 서버로 배포되는 모든 Linux 서버에 대한 보안 정책입니다. 이 규칙은 정적 및 동적 태그를 사용하는 동적 주소 그룹과 일치합니다.
- 동적 주소 그룹의 구성원이 새 FTP 또는 웹 서버를 배포할 때 업데이트되어 있는지 확인합니다. 이렇게 하면 이러한 새 가상 시스템에도 보안 규칙이 적용됩니다.

**STEP 1 |** VM 소스 모니터링을 활성화합니다.

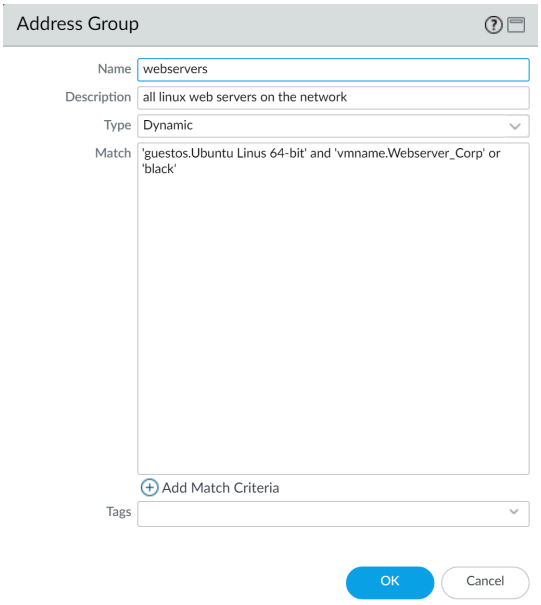
가상 네트워크의 변경 내용을 추적하려면 VM 모니터링을 활성화하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 방화벽에서 동적 주소 그룹을 생성합니다.

이 기능을 보려면 튜토리얼을 참조하십시오.

1. 방화벽의 웹 인터페이스에 로그인합니다.
2. 개체 > 주소 그룹을 선택합니다.
3. 추가를 클릭하고 주소 그룹에 대한 이름 및 설명을 입력합니다.
4. 유형을 동적으로 선택합니다.
5. 일치 기준을 정의합니다. 동적 태그와 정적 태그를 일치 기준으로 선택하여 그룹의 구성원을 채울 수 있습니다. 일치 기준 추가를 클릭하고 **And** 또는 **Or** 연산자를 선택하고 필터링하거나 일치시킬 속성을 선택합니다. 그런 다음 확인을 클릭합니다.




6. 커밋을 클릭합니다.

**STEP 3 |** 이 예제의 각 동적 주소 그룹의 일치 조건은 다음과 같습니다.

ftp_server: 게스트 운영 체제 "Linux 64비트"에서 일치하고 "ftp"로 주석이 지정됩니다('guestos.Ubuntu Linux 64비트' 및 'annotation.ftp').

web-servers: 태그 검정 또는 게스트 운영 체제가 Linux 64비트이고 서버 이름이 Web_server_Corp인 경우의 두 가지 기준과 일치합니다. ('guestos.Ubuntu Linux 64비트' 및 'vmname.WebServer_Corp' 또는 '검정색')




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 정책에 동적 주소 그룹을 사용합니다.

튜토리얼을 볼 수 있습니다.

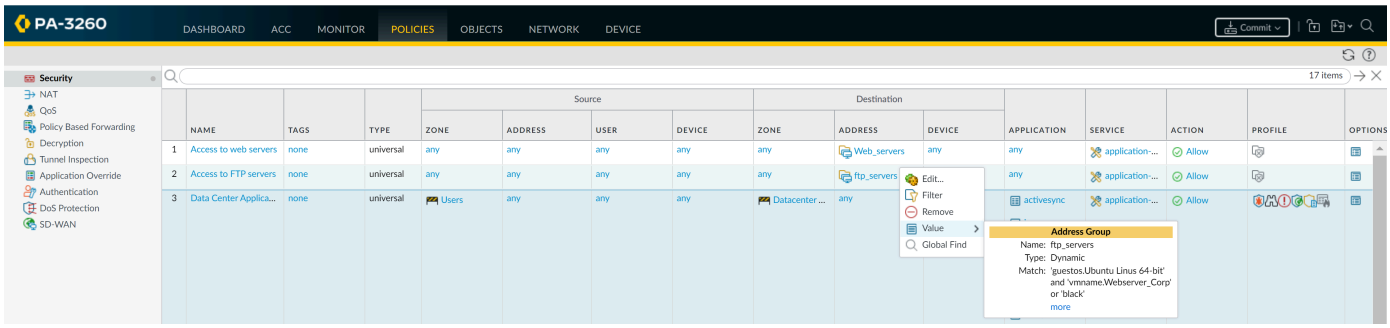
1. 정책 > 보안을 선택합니다.
2. 추가를 클릭하고 정책에 대한 이름 및 설명을 입력합니다.
3. 소스 영역을 추가하여 트래픽이 시작되는 영역을 지정합니다.
4. 트래픽이 종료되는 대상 영역을 추가합니다.
5. 대상 주소에 대해 방금 생성한 동적 주소 그룹을 선택합니다.
6. 트래픽에 대한 작업(허용 또는 거부)을 지정하고 선택적으로 기본 보안 프로파일을 규칙에 연결합니다.
7. 1단계부터 6단계를 반복하여 다른 정책 규칙을 생성합니다.
8. 커밋을 클릭합니다.

**STEP 5 |** 이 예는 FTP 서버에 대한 모든 액세스에 대한 정책과 웹 서버에 대한 액세스에 대한 두 가지 정책을 만드는 방법을 보여줍니다.

| | NAME | TAGS | TYPE | Source ZONE | Source ADDRESS | Source USER | Source DEVICE | Destination ZONE | Destination ADDRESS | Destination DEVICE | APPLICATION | SERVICE | ACTION | PROFILE | OPTI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Access to web servers | none | universal | any | any | any | any | any | Web_servers | any | any | application-... | Allow | | |
| 2 | Access to FTP servers | none | universal | any | any | any | any | any | ftp_servers | any | any | application-... | Allow | | |

**STEP 6 |** 동적 주소 그룹의 구성원이 방화벽에 채워져 있는지 확인합니다.

1. 정책 > 보안을 선택하고 규칙을 선택합니다.
2. 주소 그룹 링크 옆에 있는 드롭다운 화살표를 선택한 다음 값을 선택합니다. 일치 조건이 정확한지 확인할 수도 있습니다.




3. 더 많은 링크를 클릭하고 등록된 IP 주소 목록이 표시되는지 확인합니다.

   이 주소 그룹에 속한 모든 IP 주소에 대해 정책이 적용되고 여기에 표시됩니다.

등록된 모든 *IP* 주소를 삭제하려면 ***CLI*** 명령 디버그 개체를 등록한 다음 태그를 삭제한 후 방화벽을 재부팅합니다.


©2023 Palo Alto Networks, Inc.

# 동적 IP 주소 및 태그에 대한 CLI 명령

방화벽 및 Panorama의 명령줄 인터페이스는 태그와 IP 주소가 동적으로 등록되는 다양한 소스에 대한 자세한 보기를 제공합니다. 또한 등록 및 미등록 태그를 감사할 수 있습니다. 다음 예는 CLI의 기능을 보여줍니다.

| 예시 | CLI 명령 |
| --- | --- |
| `state.poweredOn` 태그와 일치하거나 `vSwitch0`으로 태그가 지정되지 않은 등록된 모든 IP 주소를 봅니다. | **`show log iptag tag_name equal state.poweredOn`**<br>**`show log iptag tag_name not-equal switch.vSwitch0`** |
| VM 정보 소스에서 이름이 `vmware1`이고 `poweredOn`으로 태그가 지정된 동적으로 등록된 모든 IP 주소를 봅니다. | **`show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all`** `registered IP Tags ---------- ---------- --------------- fe80::20c:29ff:fe69:2f76 "state.poweredOn" 10.1.22.100 "state.poweredOn" 2001:1890:12f2:11:20c:29ff:fe69:2f76"state.poweredOn" fe80::20c:29ff:fe69:2f80 "state.poweredOn" 192.168.1.102 "state.poweredOn" 10.1.22.105 "state.poweredOn" 2001:1890:12f2:11:2cf8:77a9:5435:c0d"state.poweredOn" fe80::2cf8:77a9:5435:c0d "state.poweredOn"` |
| 소스 연결을 끊지 않고 특정 VM 모니터링 소스에서 학습한 모든 IP 주소 및 태그를 지웁니다. | **`debug vm-monitor clear source-name <name>`** |
| 모든 소스에서 등록된 IP 주소를 표시합니다. | **`show object registered-ip all`** |
| 모든 소스에서 등록된 IP 주소의 개수를 표시합니다. | **`show object registered-ip all option count`** |
| 모든 소스에서 등록된 IP 주소 지우기 | **`debug object registered-ip clear all`** |


©2023 Palo Alto Networks, Inc.

| 예시 | CLI 명령 |
| --- | --- |
| XML API를 사용하여 등록된 지정된 IP 주소에 대한 태그를 추가하거나 삭제합니다. | **debug object registered-ip test [<register/unregister>] <ip/netmask><tag>** |
| 특정 정보 소스에서 등록된 모든 태그를 봅니다. | **show vm-monitor source source-name vmware1 tag all** vlanId.4095 vswitch.vSwitch1 host-ip.10.1.5.22 portgroup.TOBEUSED hostname.panserver22 portgroup.VM Network 2 datacenter.ha-datacenter vlanId.0 state.poweredOn vswitch.vSwitch0 vmname.Ubuntu22-100 vmname.win2k8-22-105 resource-pool.Resources vswitch.vSwitch2 guestos.Ubuntu Linux 32-bit guestos.Microsoft Windows Server 2008 32-bit annotation. version.vmx-08 portgroup.VM Network vm-info-source.vmware1 uuid.564d362c-11cd-b27f-271f-c361604dfad7 uuid.564dd337-677a-eb8d-47db-293bd6692f76 Total: 22 |
| 방화벽의 VM 모니터링 에이전트, XML API, Windows 사용자 ID 에이전트 또는 CLI와 같은 특정 데이터 소스에서 등록된 모든 태그를 봅니다. | • CLI에서 등록된 태그를 보려면:<br>**show log iptag datasource_type equal unknown**<br>• XML API에서 등록된 태그를 보려면:<br>**show log iptag datasource_type equal xml-api**<br>• VM 정보 소스에서 등록된 태그를 보려면:<br>**show log iptag datasource_type equal vm-monitor**<br>• Windows User-ID 에이전트에서 등록된 태그를 보려면:<br>**show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent** |
| 특정 IP 주소에 대해 등록된 모든 태그를 봅니다(모든 소스에서). | **debug object registered-ip show tag-source ip ip_address tag all** |


©2023 Palo Alto Networks, Inc.

# 업스트림 디바이스 뒤에 있는 엔드포인트 및 사용자에 대한 정책 시행

명시적 프록시 서버 또는 로드 밸런싱과 같은 업스트림 디바이스가 네트워크의 사용자와 방화벽 사이에 배포된 경우, 콘텐츠를 요청한 클라이언트의 IP 주소가 아니라 프록시가 전달하는 HTTP/HTTPS 트래픽의 소스 IP 주소와 같이 방화벽에서 업스트림 디바이스 IP 주소를 볼 수 있습니다. 대부분의 경우 업스트림 디바이스는 콘텐츠를 요청했거나 요청이 시작된 클라이언트의 실제 IPv4 또는 IPv6 주소를 포함하는 HTTP 요청에 XFF(X-Forwarded-For) 헤더를 추가합니다.

이러한 경우 XFF 필드에서 IP 주소를 추출하여 사용자 ID가 있는 사용자에게 매핑하거나 IP 주소를 기반으로 보안 정책을 적용하도록 방화벽을 구성할 수 있습니다.

- **User-ID**에 **X-Forwarded-For** 헤더 사용 - 프록시 서버 뒤에 있는 사용자가 웹 기반 애플리케이션에 안전하게 액세스할 수 있도록 사용자 기반 정책을 시행할 수 있습니다. 또한 User-ID가 XFF IP 주소를 사용자 이름에 매핑할 수 있는 경우 방화벽은 트래픽, 위협, WildFire 제출 및 URL 필터링 로그에서 해당 사용자 이름을 소스 사용자로 표시하여 프록시에서 사용자의 웹 활동에 대한 가시성을 제공합니다.
- 보안 정책에서 **X-Forwarded-For** 헤더 사용 - HTTP 헤더의 XFF 필드에 있는 IP 주소를 사용하여 소스 IP 주소를 기반으로 보안 정책을 시행할 수 있습니다. 또한 XFF 필드에 IP 주소가 포함된 트래픽에 정책이 적용될 때 문제 해결 및 수정을 지원하도록 트래픽, 위협, 데이터 필터링 및 Wildfire 제출 로그를 구성할 수 있습니다.

공격자가 외부 서버에서 콘텐츠를 검색하기 위해 방화벽을 나가는 웹 요청 패킷의 XFF 값을 읽고 악용할 수 없도록 하려면 나가는 패킷에서 XFF 값을 제거하도록 방화벽을 구성할 수도 있습니다. 사용자 ID 또는 정책에서 XFF IP 주소를 사용하고 XFF 값을 제거하는 것은 상호 배타적이지 않습니다. 둘 다 구성하면 방화벽은 정책 시행 및 로깅에서 사용한 후에만 XFF 값을 0으로 생성합니다.

사용자 ***ID***의 ***XFF*** 필드에 있는 ***IP*** 주소와 보안 정책을 동시에 사용하도록 방화벽을 구성할 수 없습니다.

- 정책 및 로깅 소스 사용자에 대해 XFF 값 사용
- 보안 정책 및 로깅에서 XFF IP 주소 값 사용
- XFF 헤더의 IP 주소를 사용하여 이벤트 문제 해결

## 소스 사용자 기반 정책에 XFF 값 사용

XFF 헤더의 IP 주소를 User-ID를 사용하여 사용자명에 매핑하는 방화벽을 구성할 수 있으므로 달리 식별할 수 없는 프록시 서버 뒤에 있는 사용자의 웹 트래픽에 대한 가시성과 사용자 기반 정책 제어를 가질 수 있습니다. XFF 헤더의 IP 주소를 사용자명으로 매핑하려면 먼저 User-ID를 활성화해야 합니다.

이 옵션이 활성화되면 방화벽은 사용자 매핑 목적으로만 XFF 헤더의 IP 주소를 사용합니다. 방화벽 로그의 소스 IP 주소는 소스 사용자가 아닌 프록시 서버의 주소입니다. 방화벽이 매핑한 사용자의 로그 이벤트와 XFF 헤더에서 추출한 IP 주소가 표시되면 이벤트와 관련된 특정 디바이스를 추적하기 어려울 수 있습니다. 프록시 서버 뒤의 사용자에 기인한 이벤트의 디버깅 및 문제 해결을 단순화하려면 URL 필터링 로그의 X-Forwarded-For 열을 XFF 헤더의 IP 주소로 채우도록 방화벽도 구성해야 URL 필터링 로그 항목과 관련된 로그 이벤트와 연결된 특정 사용자 및 디바이스를 추적할 수 있습니다.


©2023 Palo Alto Networks, Inc.

프록시 서버가 추가하는 XFF 헤더에는 요청을 보낸 최종 사용자의 소스 IP 주소가 포함되어야 합니다. 헤더에 여러 IP 주소가 포함된 경우 방화벽은 첫 번째 IP 주소만 사용합니다. 헤더에 IP 주소 이외의 정보가 포함되어 있으면 방화벽이 사용자 매핑을 수행할 수 없습니다.

방화벽이 ***X-Forwarded-For*** 헤더를 사용하여 사용자 매핑을 수행하도록 하면 방화벽이 ***XFF*** 헤더의 클라이언트 ***IP*** 주소를 로그의 소스 주소로 사용할 수 없습니다**.** 로그는 여전히 프록시 서버 ***IP*** 주소를 소스 주소로 표시합니다**.** 그러나 디버깅 및 문제 해결 프로세스를 단순화하기 위해 URL 필터링 로그에 XFF 값 추가로 방화벽을 구성하여 ***URL*** 필터링 로그의 ***XFF*** 헤더에서 클라이언트 ***IP*** 주소를 표시할 수 있습니다**.**

**STEP 1 |** 방화벽이 정책 및 로그의 소스 사용자 필드에서 XFF 값을 사용하도록 설정합니다.

1. 디바이스 > 설정 > 콘텐츠 **ID**를 선택하고 X-Forwarded-For Headers 설정을 수정합니다.
2. **Use X-Forwarded-For Header in User-ID**을 선택합니다.

**STEP 2 |** 나가는 웹 요청에서 XFF 값을 제거합니다.

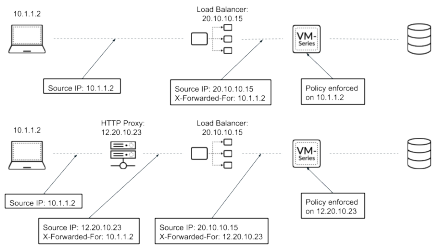
1. **Strip X-Forwarded-For Header**를 선택합니다.
2. 확인 및 커밋을 클릭합니다.

**STEP 3 |** 방화벽이 로그의 소스 사용자 필드를 채우고 있는지 확인합니다.

1. 소스 사용자 필드가 있는 로그 유형을 선택합니다(예: 모니터 > 로그 > 트래픽).
2. 소스 사용자 열에 웹 애플리케이션에 액세스하는 사용자의 사용자 이름이 표시되는지 확인합니다.

## 보안 정책 및 로깅에서 XFF IP 주소 값 사용

X-Forwarded-For(XFF) HTTP 헤더 필드에서 소스 IP 주소를 사용하여 보안 정책을 시행하도록 방화벽을 구성할 수 있습니다. 패킷이 방화벽에 도달하기 전에 단일 프록시 서버를 통과할 때 XFF 필드에는 발신 엔드포인트의 IP 주소가 포함됩니다. 그러나 패킷이 여러 업스트림 디바이스를 통과하는 경우 방화벽은 가장 최근에 추가된 IP 주소를 사용하여 정책을 적용하거나 IP 정보에 의존하는 다른 기능을 사용합니다.




- 정책에서 XFF 값 사용
- 로그에 XFF 값 표시
- 보고서에 XFF 값 표시

### 정책에서 **XFF** 값 사용

XFF 헤더의 클라이언트 IP 주소를 사용하여 보안 정책을 시행하려면 다음 절차를 완료하십시오.


©2023 Palo Alto Networks, Inc.

*Microsoft Azure*에서 기본적으로 애플리케이션 게이트웨이는 원래 소스 *IP* 주소와 포트를 *XFF* 헤더에 삽입합니다. 방화벽의 정책에서 *XFF* 헤더를 사용하려면 *XFF* 헤더에서 포트를 생략하도록 애플리케이션 게이트웨이를 구성해야 합니다. 자세한 내용은 Azure 설명서를 참조하십시오.

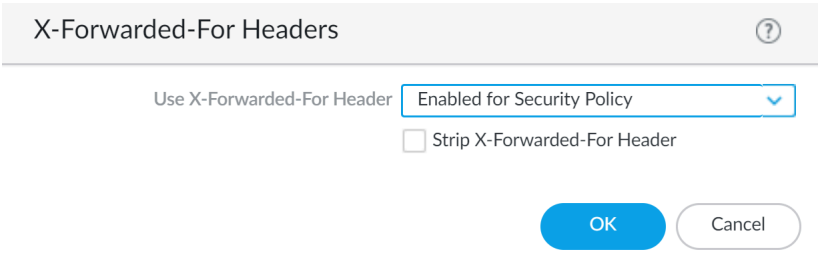
**STEP 1 |** 방화벽에 로그인합니다.

**STEP 2 |** 디바이스 > 설정 > 콘텐츠 **ID** > **X-Forwarded-For Headers**를 선택합니다.

**STEP 3 |** 편집 아이콘을 클릭합니다.

**STEP 4 |** **X-Forwarded-For Header** 사용 드롭다운에서 보안 정책 사용을 선택합니다.

보안 정책 및 *User-ID*에 대해 *X-Forwarded-Ffor* 헤더 사용을 동시에 활성화할 수 없습니다.




**STEP 5 |** (선택 사항) **Strip X-Forwarded-For Header**를 선택하여 발신 HTTP 요청에서 XFF 필드를 제거합니다.

이 옵션을 선택해도 XFF 헤더 사용이 비활성화되지 않습니다. 방화벽은 정책을 시행하고 IP 주소를 기록하기 위해 사용 후 클라이언트 요청에서 XFF 필드를 제거합니다.

**STEP 6 |** 확인을 클릭합니다.

**STEP 7 |** 변경 사항을 커밋합니다.

## 로그에 **XFF** 값 표시

보안 정책의 XFF 헤더 사용 외에도 다양한 로그, 보고서 및 ACC(Application Command Center)에서 XFF IP 주소를 확인하여 모니터링 및 문제 해결을 지원할 수 있습니다. 트래픽, 위협, 데이터 필터링 및 Wildfire 제출 로그에 X-Forwarded-Ford-Ford 열을 추가할 수 있습니다.

*URL*이 아닌 필터링 로그의 경우 *XFF IP* 로깅은 패킷 캡처를 사용할 수 없는 경우에만 지원됩니다.

*X-Forwarded-For IP* 열은 방화벽이 재설정 작업(***reset-client***, ***reset-server*** 또는 ***reset-both***)이 필요한 위협을 감지하고 마지막으로 검사한 패킷에 *XFF* 헤더가 포함되어 있지 않은 경우 값을 표시하지 않습니다.

로그에서 XFF IP 주소를 보려면 다음 단계를 완료하십시오.


©2023 Palo Alto Networks, Inc.

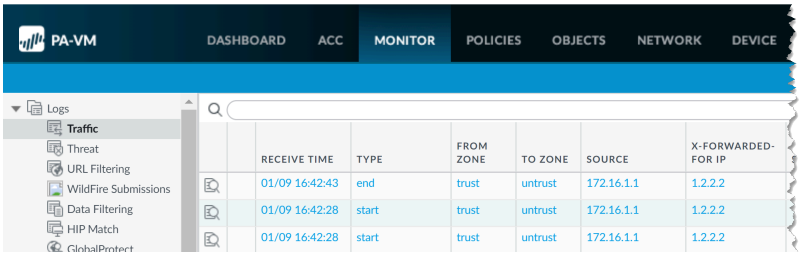
**STEP 1 |** 방화벽에 로그인합니다.

**STEP 2 |** 모니터링 > 로그를 선택합니다.

**STEP 3 |** 교통, 위협, 데이터 필터링 또는 **Wildfire** 제출을 선택합니다.

**STEP 4 |** 열 머리글 오른쪽에 있는 화살표를 클릭하고 열을 선택합니다.

**STEP 5 |** 로그에 XFF IP를 표시하려면 **X-Forwarded-For IP**를 선택합니다.




## 보고서에 **XFF** 값 표시

방화벽에서 생성된 사전 정의된 보고서에는 XFF 값이 포함되어 있지 않습니다. 그러나 방화벽에는 XFF 정보를 포함하는 기본 제공 보고서 템플릿이 있습니다. 보고서에서 XFF IP 주소를 보려면 단계에 따라 기본 제공 템플릿으로 보고서를 생성합니다.

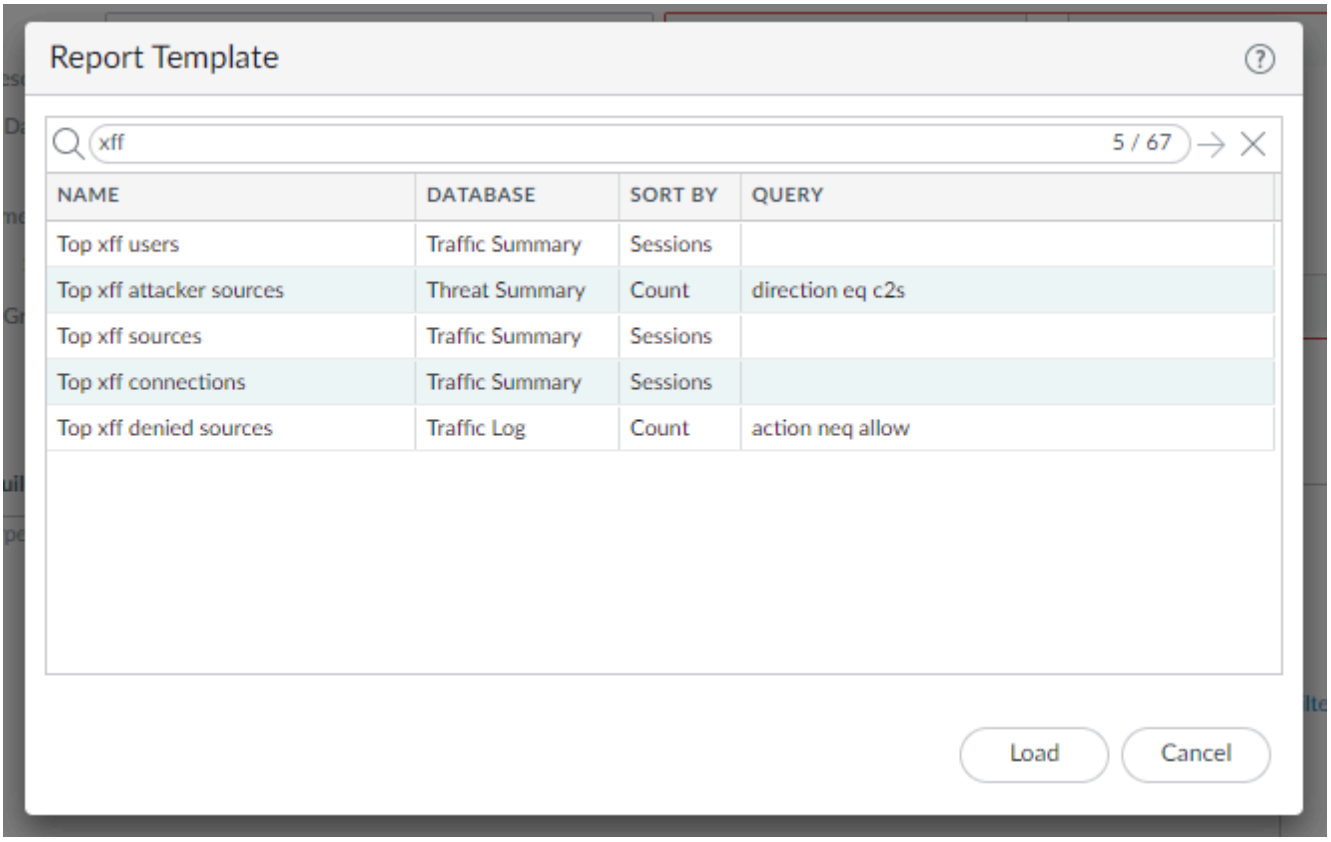
**STEP 1 |** 방화벽에 로그인합니다.

**STEP 2 |** 모니터 > 맞춤 보고서 관리 > 추가를 선택합니다.

**STEP 3 |** 템플릿 로드를 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 검색 창에 XFF를 입력하고 검색 버튼을 클릭하여 내장된 XFF 보고서 템플릿을 찾습니다.




**STEP 5 |** 로드를 클릭합니다.

**STEP 6 |** 맞춤 보고서를 구성합니다. 시간 프레임, 정렬 기준 및 그룹화 기준을 클릭하여 필요에 가장 적합한 방식으로 XFF 정보를 표시합니다.

**STEP 7 |** (선택 사항) 지금 실행을 클릭하면 예약 시간 대신 또는 추가로 요청 시 보고서를 생성할 수 있습니다.

## XFF 헤더의 IP 주소를 사용하여 이벤트 문제 해결

기본적으로 방화벽은 사용자 매핑을 위해 XFF(X-Forwarded-For) 헤더에서 이 주소를 사용하는 경우에도 프록시 서버 뒤에 있는 클라이언트의 소스 주소를 기록하지 않습니다. 따라서 로그 이벤트와 관련된 특정 사용자를 식별할 수 있지만 로그 이벤트를 발생시킨 소스 디바이스는 쉽게 식별할 수 없습니다. 프록시 서버 뒤의 사용자에 대한 이벤트 디버깅 및 문제 해결을 단순화하려면 웹 기반 애플리케이션에 대한 액세스를 허용하는 보안 정책 규칙에 첨부하는 URL 필터링 프로파일에서 X-Forwarded-For 옵션을 활성화합니다. 이 옵션이 활성화되면 방화벽은 규칙과 일치하는 모든 트래픽의 소스 주소로 XFF 헤더의 IP 주소를 기록합니다.

***URL*** 필터링 로그에는 ***X***-전달된 ***IP*** 필드 필드가 표시되지 않습니다. ***X-Forwarded-For IP*** 로그 이벤트를 보려면 로그를 ***CSV*** 형식으로 내보내야 합니다.

방화벽이 ***URL*** 필터링 로그의 소스 주소로 ***XFF*** 헤더를 사용하도록 설정해도 소스 주소의 사용자 매핑이 활성화되지 않습니다. 소스 사용자 필드를 채우려면 정책에 XFF 값 사용 및 소스 사용자 로깅을 참조하십시오.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** URL 필터링 프로파일에서 X-Forwarded-For 옵션을 사용하도록 설정합니다.

1. 개체 > 보안 프로파일 > **URL** 필터링을 선택한 다음 구성하려는 URL 필터링 프로파일을 선택하거나 새 프로파일을 추가합니다.

   기본 ***URL*** 필터링 프로파일에서는 ***XFF*** 로깅을 활성화할 수 없습니다.

2. **URL** 필터링 설정 탭을 선택하고 **X-Forwarded-For**를 사용하도록 설정합니다.
3. 확인을 클릭하여 프로파일을 저장합니다.

**STEP 2 |** 웹 애플리케이션에 대한 액세스를 가능하게 하는 보안 정책 규칙에 URL 필터링 프로파일을 연결합니다.

1. 정책 > 보안을 선택한 다음 규칙을 클릭합니다.
2. 작업 탭을 선택한 다음 프로파일 유형을 프로파일로 설정한 다음 방금 X-Forwarded-For HTTP 헤더 로깅에 대해 구성한 **URL** 필터링 프로파일을 선택합니다.
3. 확인 및 커밋을 클릭합니다.

**STEP 3 |** 방화벽이 XFF 값을 기록하는지 확인하십시오.

***XFF*** 열은 방화벽의 ***URL*** 필터링 로그에 표시되지 않습니다.

1. 모니터 > **Logs** > **URL** 필터링을 선택합니다.
2. 다음 방법 중 하나로 XFF 값을 봅니다.
   - CSV()로 내보내기를 클릭하여 URL 필터링 로그를 쉼표로 구분된 값 파일로 내보냅니다. 다운로드가 완료되면 파일 다운로드를 클릭하여 로컬 폴더에 로그 복사본을 저장합니다.
   - **`show log url csv-output equal yes`** CLI 명령을 사용합니다.

**STEP 4 |** URL 필터링 로그의 XFF 필드를 사용하여 다른 로그 유형의 로그 이벤트 문제를 해결하십시오.

HTTP/HTTPS 트래픽과 연결된 이벤트를 발견했지만 프록시 서버의 주소이기 때문에 원본 IP 주소를 식별할 수 없는 경우 상관 관계가 있는 URL 필터링 로그에서 X-Forwarded-For 값을 사용하여 로그 이벤트와 연결된 원본 주소를 쉽게 식별할 수 있습니다. 다음 절차를 따릅니다.

1. 프록시 서버의 IP 주소를 소스 주소로 표시하는 트래픽, 위협 또는 WildFire 제출 로그에서 조사할 이벤트를 찾습니다.
2. 로그에 대한 망원경 아이콘을 클릭하여 세부 정보를 표시하고 세부 로그 뷰어 창 하단에서 연결된 URL 필터링 로그를 찾습니다.
3. 연결된 URL 필터링 로그를 CSV 파일로 내보내고 X-Forwarded For IP 열을 찾습니다. 이 열의 IP 주소는 프록시 서버 뒤에 있는 원본 사용자의 IP 주소를 나타냅니다. 이 IP 주소를 사용하여 조사 중인 이벤트를 트리거한 디바이스를 추적합니다.


©2023 Palo Alto Networks, Inc.

# 정책 기반 포워딩

일반적으로 방화벽은 패킷의 대상 IP 주소를 사용하여 나가는 인터페이스를 결정합니다. 방화벽은 인터페이스가 연결된 가상 라우터와 연결된 라우팅 테이블을 사용하여 경로 조회를 수행합니다. 정책 기반 포워딩(PBF)을 사용하면 라우팅 테이블을 재정의하고 소스 또는 대상 IP 주소 또는 트래픽 유형과 같은 특정 매개 변수를 기반으로 아웃고잉(outgoing) 또는 이그레스***(egress)*** 인터페이스를 지정할 수 있습니다.

- PBF
- 정책 기반 포워딩 규칙 생성
- 사용 사례: 이중 ISP를 통한 아웃바운드 액세스를 위한 PBF

## PBF

PBF 규칙은 트래픽이 라우팅 테이블에 지정된 다음 홉에서 대체 경로를 사용하도록 허용하며 일반적으로 보안 또는 성능상의 이유로 이그레스(egress) 인터페이스를 지정하는 데 사용됩니다. 회사에 본사와 지점 사이에 더 저렴한 인터넷 링크와 더 비싼 전용 회선이라는 두 개의 링크가 있다고 가정해 보겠습니다. 전용 회선은 고대역폭, 저지연 링크입니다. 보안 강화를 위해 PBF를 사용하여 FTP 트래픽과 같은 암호화되지 않은 트래픽을 전용선을 통해 전송하고 인터넷 링크를 통해 기타 모든 트래픽을 전송할 수 있습니다. 또는 성능을 위해 웹 브라우징과 같은 다른 모든 트래픽을 저렴한 링크를 통해 보내는 동안 전용 회선을 통해 비즈니스 크리티컬 애플리케이션을 라우팅하도록 선택할 수 있습니다.

- 이그레스(Egress) 경로 및 대칭 반환
- PBF에 대한 경로 모니터링
- PBF의 서비스 대 애플리케이션

### 이그레스**(Egress)** 경로 및 대칭 반환

PBF를 사용하여 트래픽을 방화벽의 특정 인터페이스로 보내거나 트래픽을 삭제하거나 다른 가상 시스템(여러 가상 시스템이 활성화된 시스템에서)으로 트래픽을 보낼 수 있습니다.

이중 ISP 환경과 같이 비대칭 경로가 있는 네트워크에서는 트래픽이 방화벽의 한 인터페이스에 도착하고 다른 인터페이스에서 나갈 때 연결 문제가 발생합니다. 포워딩(SYN 패킷) 경로와 반환(SYN/ACK) 경로가 다른 비대칭 경로인 경우 방화벽은 전체 세션의 상태를 추적할 수 없으며 이로 인해 연결 실패가 발생합니다. 트래픽이 대칭 경로를 사용하도록 하려면, 즉 트래픽이 세션이 생성된 동일한 인터페이스에 도착하고 나가는 것을 의미하며 대칭 반환 옵션을 활성화할 수 있습니다.

대칭 반환을 사용하는 경우 가상 라우터는 반환 트래픽에 대한 라우팅 조회를 무시하고 대신 SYN 패킷(또는 첫 번째 패킷)을 수신한 MAC 주소로 흐름을 다시 보냅니다. 그러나 대상 IP 주소가 Ingress/Egress 인터페이스의 IP 주소와 동일한 서브넷에 있는 경우 경로 조회가 수행되고 대칭 반환이 적용되지 않습니다. 이 동작은 트래픽이 자동으로 삭제되는 것을 방지합니다.

대칭 반환에 대한 다음 홉을 결정하기 위해 방화벽은 ***ARP(***주소 확인 프로토콜***)*** 테이블을 사용합니다. 이 ***ARP*** 테이블이 지원하는 최대 항목 수는 방화벽 모델에 의해 제한되며 값은 사용자가 구성할 수 없습니다. 모델에 대한 제한을 결정하려면 *CLI* 명령 ***show pbf return-mac all***을 사용합니다.


©2023 Palo Alto Networks, Inc.

## PBF에 대한 경로 모니터링

경로 모니터링을 사용하면 방화벽이 필요할 때 대체 경로를 통해 트래픽을 보낼 수 있도록 IP 주소에 대한 연결을 확인할 수 있습니다. 방화벽은 ICMP 핑을 하트비트로 사용하여 지정된 IP 주소에 연결할 수 있는지 확인합니다.

모니터링 프로파일을 사용하면 하트비트의 임계값 수를 지정하여 IP 주소에 연결할 수 있는지의 여부를 결정할 수 있습니다. 모니터링되는 IP 주소에 연결할 수 없는 경우 PBF 규칙을 비활성화하거나 페일오버 또는 대기 복구 작업을 지정할 수 있습니다. PBF 규칙을 비활성화하면 가상 라우터가 라우팅 결정을 인계받을 수 있습니다. 페일오버 또는 대기 복구 작업이 수행되면 모니터링 프로파일은 대상 IP 주소에 도달할 수 있는지의 여부를 계속 모니터링하고, 다시 연결되면 방화벽은 원래 경로를 사용하도록 되돌아갑니다.

다음 표는 새 세션과 설정된 세션에서 경로 모니터링 실패에 대한 동작의 차이점을 나열합니다.

| 모니터링 실패 시 세션 동작 | 모니터링되는 **IP** 주소에 연결할 수 없을 때 규칙이 활성화된 상태로 유지되는 경우 | 모니터링되는 **IP** 주소에 연결할 수 없을 때 규칙이 비활성화된 경우 |
|---|---|---|
| 설정된 세션의 경우 | 대기 복구 - PBF 규칙에 지정된 이그레스(egress) 인터페이스를 계속 사용합니다. | 대기 복구 - PBF 규칙에 지정된 이그레스(egress) 인터페이스를 계속 사용합니다. |
| | 페일오버 - 라우팅 테이블에 의해 결정된 경로 사용(PBF 없음) | 페일오버 - 라우팅 테이블에 의해 결정된 경로 사용(PBF 없음) |
| 새 세션의 경우 | 대기 복구 - 라우팅 테이블에 의해 결정된 경로 사용(PBF 없음) | 대기 복구 - 나머지 PBF 규칙을 확인합니다. 일치하지 않으면 라우팅 테이블을 사용하십시오. |
| | 페일오버 - 라우팅 테이블에 의해 결정된 경로 사용(PBF 없음) | 페일오버 - 나머지 PBF 규칙을 확인합니다. 일치하지 않으면 라우팅 테이블을 사용하십시오. |

## PBF의 서비스 대 애플리케이션

PBF 규칙은 첫 번째 패킷(SYN) 또는 첫 번째 패킷(SYN/ACK)에 대한 첫 번째 응답에 적용됩니다. 이는 방화벽이 애플리케이션을 결정하기에 충분한 정보를 갖기 전에 PBF 규칙이 적용될 수 있음을 의미합니다. 따라서 애플리케이션별 규칙은 PBF와 함께 사용하지 않는 것이 좋습니다. 가능하면 프로토콜이나 애플리케이션에서 사용하는 레이어 4 포트(TCP 또는 UDP)인 서비스 개체를 사용하십시오.

그러나 PBF 규칙에 애플리케이션을 지정하면 방화벽이 ***App-ID*** 캐싱을 수행합니다. 애플리케이션이 처음으로 방화벽을 통과할 때 방화벽에는 애플리케이션을 식별할 수 있는 정보가 충분하지 않으므로 PBF 규칙을 적용할 수 없습니다. 더 많은 패킷이 도착할수록 방화벽은 애플리케이션을 결정하고 App-ID 캐시에 항목을 생성하고 세션에 대해 이 App-ID를 유지합니다. 동일한 대상 IP 주소, 대상 포트 및 프로토콜 ID로 새 세션이 생성되면, 방화벽은 애플리케이션을 초기 세션(App-ID 캐시 기반)과 동일하게 식별하고 PBF 규칙을 적용할 수 있습니다. 따라서 정확히 일치하지 않고 동일한 애플리케이션이 아닌 세션은 PBF 규칙에 따라 포워딩할 수 있습니다.


©2023 Palo Alto Networks, Inc.

또한 애플리케이션에는 종속성이 있으며 방화벽이 더 많은 패킷을 수신함에 따라 애플리케이션의 ID가 변경될 수 있습니다. PBF는 세션 시작 시 라우팅 결정을 내리기 때문에 방화벽은 애플리케이션 ID를 변경할 수 없습니다. 예를 들어 YouTube는 웹 브라우징으로 시작하지만 페이지에 포함된 다양한 링크와 비디오를 기반으로 Flash, RTSP 또는 YouTube로 변경됩니다. 그러나 PBF에서는 방화벽이 세션 시작 시 애플리케이션을 웹 브라우징으로 식별하므로 이후 애플리케이션의 변경 사항을 인식하지 못합니다.

***PBF** 규칙에서 사용자 지정 애플리케이션, 애플리케이션 필터 또는 애플리케이션 그룹을 사용할 수 없습니다.*

## 정책 기반 포워딩 규칙 생성

PBF 규칙을 사용하여 트래픽을 방화벽의 특정 이그레스(egress) 인터페이스로 보내고 트래픽의 기본 경로를 재정의합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** PBF(정책 기반 포워딩) 규칙을 생성합니다.

PBF 규칙을 생성할 때 규칙의 이름, 소스 영역 또는 인터페이스, 이그레스(egress) 인터페이스를 지정해야 합니다. 다른 모든 구성 요소는 선택 사항이거나 기본값이 있습니다.



*IP* 주소, 주소 개체 또는 *FQDN*을 사용하여 소스 및 대상 주소를 지정할 수 있습니다.

1. 정책 > 정책 기반 전달을 선택하고 PBF 정책 규칙을 추가합니다.
2. 규칙에 설명이 포함된 이름을 지정합니다(일반).
3. 소스를 선택하고 다음을 구성합니다.
   1. 포워딩 정책을 적용할 유형(영역 또는 인터페이스)을 선택한 다음 관련 영역 또는 인터페이스를 지정합니다. 대칭 반환을 적용하려면 소스 인터페이스를 선택해야 합니다.

      *Layer 3* 인터페이스만 *PBF*를 지원합니다. 루프백 인터페이스는 *PBF*를 지원하지 않습니다.
   2. (선택 사항) PBF 규칙이 적용되는 소스 주소를 지정합니다. 예를 들어 이 규칙에 지정된 인터페이스 또는 영역으로 트래픽을 포워딩하려는 특정 IP 주소 또는 서브넷 IP 주소입니다.

      *PBF* 규칙에서 하나 이상의 소스 주소를 제외하려면 부정을 클릭합니다. 예를 들어, *PBF* 규칙이 지정된 영역의 모든 트래픽을 인터넷으로 보내는 경우 ***Negate***를 사용하면 *PBF* 규칙에서 내부 *IP* 주소를 제외할 수 있습니다.

      평가 순서는 하향식입니다. 패킷은 정의된 기준을 충족하는 첫 번째 규칙과 일치합니다. 일치가 트리거된 후 후속 규칙은 평가되지 않습니다.
   3. (선택 사항) 정책이 적용되는 소스 사용자 또는 사용자 그룹을 추가하고 선택합니다.
4. 대상/애플리케이션/서비스를 선택하고 다음을 구성합니다.
   1. 대상 주소 - 기본적으로 규칙은 모든 IP 주소에 적용됩니다. PBF 규칙에서 하나 이상의 대상 IP 주소를 제외하려면 부정을 클릭합니다.
   2. PBF를 사용하여 제어하려는 애플리케이션 및 서비스를 추가합니다.

      *PBF* 규칙은 방화벽에 애플리케이션을 결정할 수 있는 충분한 정보가 있기 전에 적용될 수 있으므로 *PBF*와 함께 사용하는 애플리케이션별 규칙은 권장하지 않습니다. 가능하면 프로토콜 또는 애플리케이션에서 사용하는 레이어 *4* 포트*(TCP* 또는 *UDP)*인 서비스 개체를 사용합니다. 자세한 내용은 PBF의 서비스 대 애플리케이션을(를) 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 규칙과 일치하는 패킷을 포워딩하는 방법을 지정합니다.

Multi-VSYS 환경에서 PBF를 구성하는 경우 각 가상 시스템에 대해 별도의 ***PBF*** 규칙을 생성해야 합니다***(***이후 트래픽을 활성화하기 위한 적절한 보안 정책 규칙 생성***).***

1. 포워딩을 선택합니다.
2. 패킷 일치 시 수행할 작업을 설정합니다.
   - **Forward** - 패킷을 지정된 **Egress Interface**로 보냅니다.
   - **VSYS**로 포워딩(여러 가상 시스템에 대해 활성화된 방화벽에서) - 패킷을 포워딩할 가상 시스템을 선택합니다.
   - 폐기 - 패킷을 삭제합니다.
   - **No PBF** - 규칙에 정의된 소스, 대상, 애플리케이션 또는 서비스에 대한 기준과 일치하는 패킷을 제외합니다. 일치하는 패킷은 PBF 대신 경로 테이블을 사용합니다. 방화벽은 경로 테이블을 사용하여 리디렉션된 포트에서 일치하는 트래픽을 제외합니다.
3. 매일, 매주 또는 비반복적인 빈도로 지정된 **Action**을 트리거하려면 **Schedule**을 생성하고 첨부합니다.
4. 다음 홉에서 다음 중 하나를 선택합니다.
   - **IP** 주소 - IP 주소를 입력하거나 방화벽이 일치하는 패킷을 포워딩할 IP 넷마스크 유형의 주소 개체를 선택합니다. IPv4 주소 개체에는 /32 넷마스크가 있어야 하고 IPv6 주소 개체에는 /128 넷마스크가 있어야 합니다.
   - **FQDN** - 방화벽이 일치하는 패킷을 포워딩할 FQDN을 입력하거나 FQDN 유형의 주소 개체를 선택하거나 생성합니다. FQDN은 IPv4 주소, IPv6 주소 또는 둘 다로 확인할 수 있습니다. FQDN이 IPv4 및 IPv6 주소 모두로 확인되는 경우 PBF 규칙에는 IPv4 주소와 IPv6 주소라는 두 개의 다음 홉이 있습니다. IPv4 및 IPv6 트래픽 모두에 동일한 PBF 규칙을 사용할 수


©2023 Palo Alto Networks, Inc.

있습니다. IPv4 트래픽은 IPv4 다음 홉으로 전달됩니다. IPv6 트래픽은 IPv6 다음 홉으로 전달됩니다.

이 ***FQDN***은 ***PBF***에 대해 구성한 인터페이스와 동일한 서브넷에 속하는 ***IP*** 주소로 확인되어야 합니다. 그렇지 않으면 방화벽이 확인을 거부하고 ***FQDN***이 확인되지 않은 상태로 유지됩니다.

방화벽은 ***FQDN***의 ***DNS*** 확인에서 하나의 ***IP*** 주소(각 ***IPv4*** 또는 ***IPv6*** 제품군 유형)만 사용합니다. ***DNS*** 확인이 둘 이상의 주소를 반환하는 경우 방화벽은 다음 홉에 대해 구성된 ***IP*** 제품군 유형(***IPv4*** 또는 ***IPv6***)과 일치하는 기본 ***IP*** 주소를 사용합니다. 기본 ***IP*** 주소는 ***DNS*** 서버가 초기 응답에서 반환하는 첫 번째 주소입니다. 방화벽은 순서에 관계없이 후속 응답에 주소가 표시되는 한 이 주소를 선호하는 대로 유지합니다.

- 없음 - 다음 홉이 없음은 패킷의 대상 IP 주소가 다음 홉으로 사용됨을 의미합니다. 대상 IP 주소가 이그레스(egress) 인터페이스와 동일한 서브넷에 있지 않으면 포워딩이 실패합니다.

5. (선택 사항) 모니터링을 활성화하여 대상 IP 주소 또는 IP 주소가 지정되지 않은 경우 다음 홉 IP 주소에 대한 연결을 확인합니다. 모니터링을 선택한 다음 모니터링된 주소에 연결할 수 없는 경우 작업을 지정하는 모니터링 프로파일(기본 또는 사용자 지정)을 연결합니다.
   - **nexthop/monitor ip**에 연결할 수 없는 경우 이 규칙을 비활성화할 수 있습니다.
   - 모니터링할 대상 **IP** 주소를 입력합니다.

   이그레스**(egress)** 인터페이스는 IPv4 및 IPv6 주소를 모두 가질 수 있으며 다음 홉 FQDN은 IPv4 및 IPv6 주소로 확인할 수 있습니다. 이 경우:

   1. 이그레스(egress) 인터페이스에 IPv4 및 IPv6 주소가 모두 있고 다음 홉 FQDN이 하나의 주소 계열 유형으로만 확인되는 경우 방화벽은 확인된 IP 주소를 모니터링합니다. FQDN이 IPv4 및 IPv6 주소로 확인되지만 이그레스(egress) 인터페이스에 주소 계열 유형 주소가 하나만 있는 경우 방화벽은 이그레스(egress) 인터페이스의 주소 계열과 일치하는 확인된 다음 홉 주소를 모니터링합니다.
   2. 이그레스(egress) 인터페이스와 다음 홉 FQDN에 IPv4 및 IPv6 주소가 모두 있는 경우 방화벽은 IPv4 다음 홉 주소를 모니터링합니다.
   3. 이그레스(egress) 인터페이스에 하나의 주소 계열 주소가 있고 다음 홉 FQDN이 다른 주소 계열 주소로 확인되는 경우 방화벽은 아무것도 모니터링하지 않습니다.

6. (비대칭 라우팅 환경에 필수, 그렇지 않으면 선택) 대칭 반환 적용 및 다음 홉 주소 목록에 하나 이상의 IP 주소를 추가합니다. 최대 8개의 다음 홉 IP 주소를 추가할 수 있습니다. 터널 및 PPoE 인터페이스는 다음 홉 IP 주소로 사용할 수 없습니다.

   대칭 반환을 활성화하면 반환 트래픽(예: LAN의 트러스트 영역에서 인터넷으로)이 인터넷에서 들어오는 트래픽과 동일한 인터페이스를 통해 포워딩됩니다.

**STEP 3 |** 변경 사항을 커밋합니다. PBF 규칙이 적용됩니다.

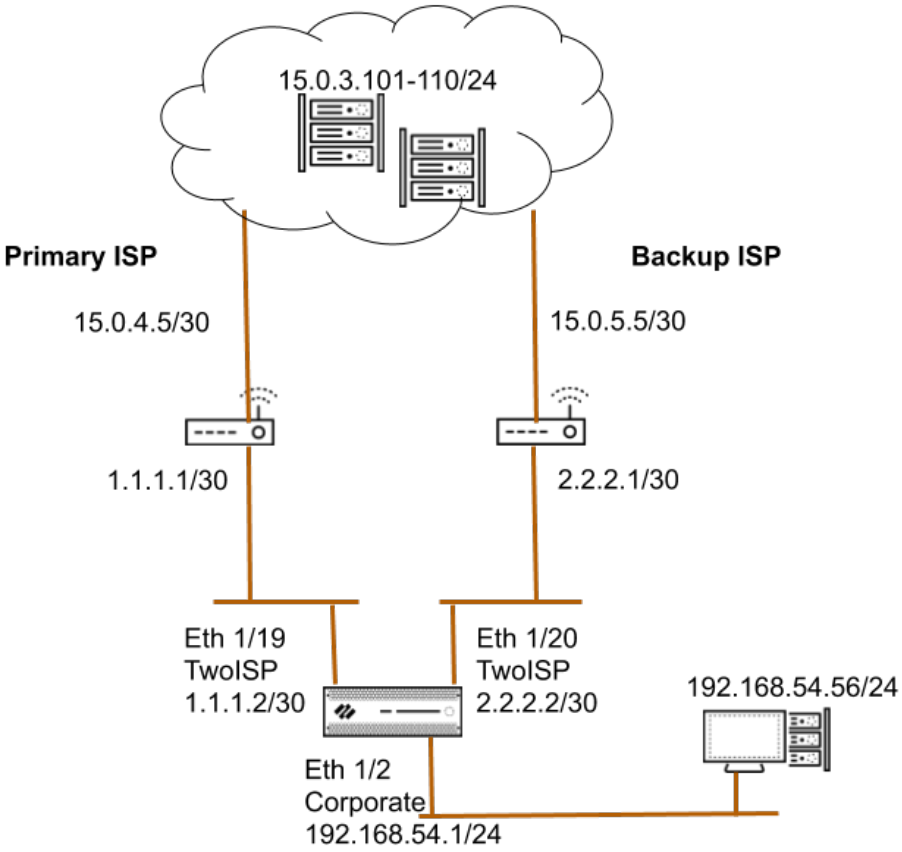
| | Source | | | Destination | | | Forwarding | | | Monitoring | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| NAME | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | DISABLE IF UNREACHABL |
| pdf2 | ethernet1/3 | any | any | HQ-subnet | service-http | forward | ethernet1/1.100 | 192.168.100.2 | false | none | false |


©2023 Palo Alto Networks, Inc.

# 사용 사례: 이중 ISP를 통한 아웃바운드 액세스를 위한 PBF

이 사용 사례에서 지점은 이중 ISP 구성을 가지고 있으며 중복 인터넷 액세스를 위해 PBF를 구현합니다. 백업 ISP는 클라이언트에서 웹 서버로의 트래픽에 대한 기본 경로입니다. BGP와 같은 인터네트워크 프로토콜을 사용하지 않고 중복 인터넷 접속을 가능하게 하기 위해 목적지 인터페이스 기반 소스 NAT와 고정 경로와 함께 PBF를 사용하고 다음과 같이 방화벽을 구성합니다.

- 기본 ISP를 통해 트래픽을 라우팅하는 PBF 규칙을 활성화하고 모니터링 프로파일을 규칙에 연결합니다. 모니터링 프로파일은 기본 ISP를 사용할 수 없을 때 백업 ISP를 통해 기본 경로를 사용하도록 방화벽을 트리거합니다.
- 방화벽이 해당 ISP의 이그레스(egress) 인터페이스와 연결된 소스 IP 주소를 사용하도록 지시하는 기본 및 백업 ISP 모두에 대한 소스 NAT 규칙을 정의합니다. 이렇게 하면 아웃바운드 트래픽이 올바른 소스 IP 주소를 갖게 됩니다.
- 기본 ISP를 사용할 수 없을 때 기본 경로가 적용되고 트래픽이 백업 ISP를 통해 포워딩되도록 백업 ISP에 고정 경로를 추가합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 방화벽에서 수신 및 이그레스(egress) 인터페이스를 구성하십시오.

이그레스(egress) 인터페이스는 동일한 영역에 있을 수 있습니다.

1. 네트워크 > 인터페이스를 선택한 다음 구성할 인터페이스를 선택합니다.

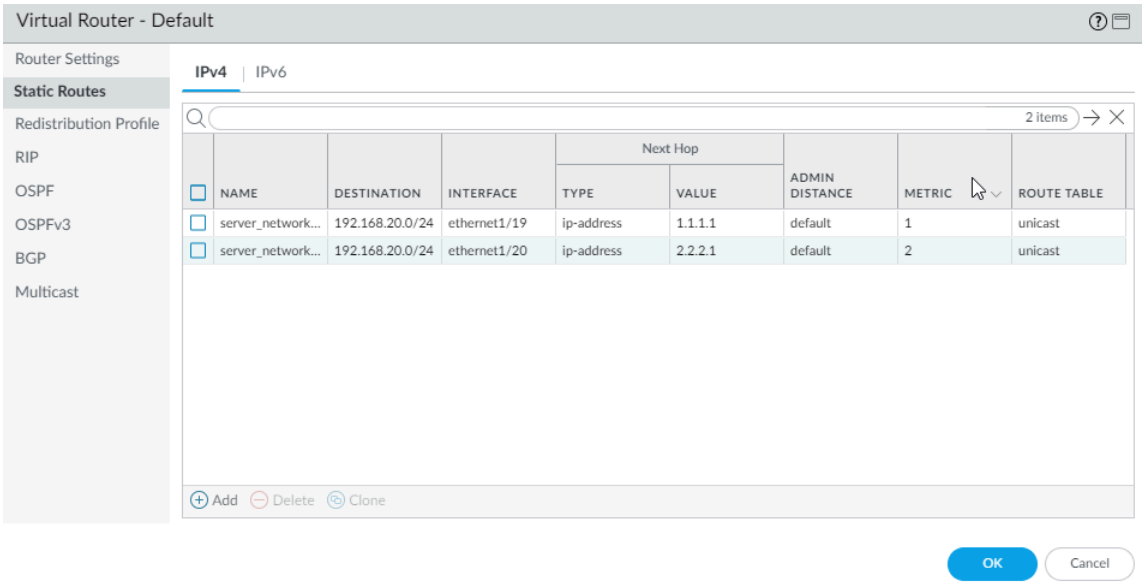
   이 예에서 사용된 방화벽의 인터페이스 구성은 다음과 같습니다.

   - 기본 ISP에 연결된 이더넷 1/19:
     - 영역: TwoISP
     - IP 주소: 1.1.1.2/30
     - 가상 라우터: 기본
   - 백업 ISP에 연결된 이더넷 1/20:
     - 영역: TwoISP
     - IP 주소: 2.2.2.2/30
     - 가상 라우터: 기본
   - 이더넷 1/2는 네트워크 클라이언트가 인터넷에 연결하는 데 사용하는 수신 인터페이스입니다.
     - 영역: Corporate
     - IP 주소: 192.168. 54.1/24
     - 가상 라우터: 기본
2. 인터페이스 구성을 저장하려면 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 가상 라우터에서 백업 ISP에 고정 경로를 추가합니다.

1. 네트워크 > 가상 라우터를 선택하고 기본 링크를 선택하여 가상 라우터 대화 상자를 엽니다.
2. 고정 경로를 선택하고 추가를 클릭합니다. 경로의 이름을 입력하고 고정 경로를 정의할 대상 IP 주소를 지정합니다. 이 예제에서는 모든 트래픽에 0.0.0.0/0을 사용합니다.
3. **IP** 주소 라디오 버튼을 선택하고 백업 인터넷 게이트웨이에 연결하는 라우터의 다음 홉 IP 주소를 설정합니다(다음 홉에 도메인 이름을 사용할 수 없음). 이 예제에서는 2.2.2.1입니다.
4. 경로에 대한 비용 메트릭을 지정합니다.




5. 확인을 두 번 클릭하여 가상 라우터 구성을 저장합니다.

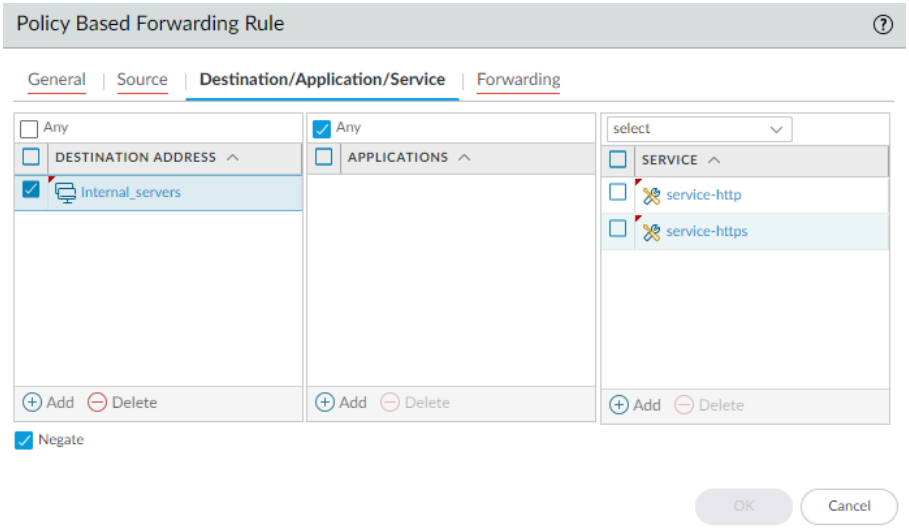

©2023 Palo Alto Networks, Inc.

**STEP 3 |** 기본 ISP에 연결된 인터페이스로 트래픽을 포워딩하는 PBF 규칙을 생성합니다.

PBF에서 내부 서버/IP 주소로 향하는 트래픽을 제외해야 합니다. 내부 IP 주소로 향하는 트래픽이 PBF 규칙에 정의된 이그레스(egress) 인터페이스를 통해 라우팅되지 않도록 무효 규칙을 정의합니다.

1. 정책 > 정책 기반 전달을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 규칙을 설명하는 이름을 지정합니다.
3. 소스 탭에서 소스 영역을 설정합니다. 이 예에서 영역은 Corporate입니다.
4. 대상/애플리케이션/서비스 탭에서 다음을 설정합니다.
   1. 대상 주소 섹션에서 내부 네트워크의 서버에 대한 IP 주소 또는 주소 범위를 추가하거나 내부 서버에 대한 주소 개체를 생성합니다. 이 규칙을 사용하지 않도록 위에 나열된 IP 주소 또는 주소 개체를 제외하려면 무효를 선택합니다.
   2. 서비스 섹션에서 HTTP 및 HTTPS 트래픽이 기본 포트를 사용할 수 있도록 **service-http** 및 **service-https** 서비스를 추가합니다. 보안 정책에서 허용하는 다른 모든 트래픽에는 기본 경로가 사용됩니다.

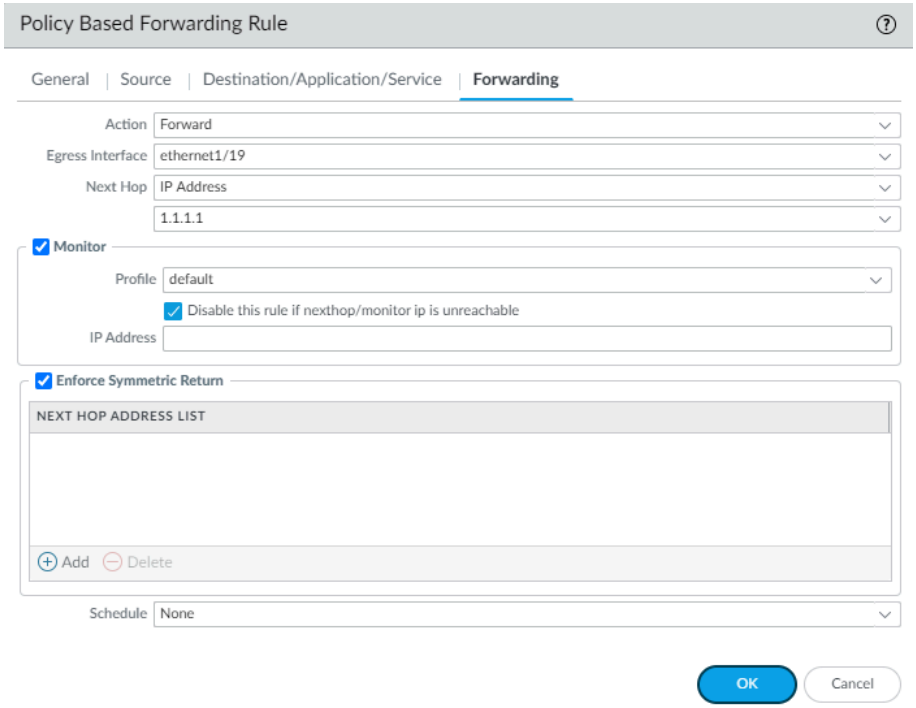
   *PBF*를 사용하여 모든 트래픽을 포워딩하려면 서비스를 모두로 설정합니다.




 ©2023 Palo Alto Networks, Inc.

**STEP 4 |** 트래픽을 포워딩할 위치를 지정합니다.

1. 포워딩 탭에서 트래픽을 포워딩할 인터페이스를 지정하고 경로 모니터링을 활성화합니다.
2. 트래픽을 전달하려면 **Action**을 **Forward**로 설정하고 **Egress Interface**를 선택하고 **Next Hop**을 지정합니다. 이 예에서 이그레스(egress) 인터페이스는 ethernet1/19이고 다음 홉 IP 주소는 1.1.1.1입니다(다음 홉에 FQDN을 사용할 수 없음).




3. 모니터를 활성화하고 기본 모니터링 프로파일을 연결하여 백업 ISP에 대한 페일오버를 트리거합니다. 이 예에서는 모니터링할 대상 IP 주소를 지정하지 않습니다. 방화벽은 다음 홉 IP 주소를 모니터링합니다. 이 IP 주소에 연결할 수 없는 경우 방화벽은 트래픽을 가상 라우터에 지정된 기본 경로로 보냅니다.
4. (비대칭 경로가 있는 경우 필수) Corporate 영역에서 인터넷으로의 반환 트래픽이 인터넷에서 수신된 트래픽과 동일한 인터페이스에서 포워딩되도록 하려면 대칭 반환 적용을 선택합니다.
5. NAT는 인터넷의 트래픽이 방화벽의 올바른 인터페이스/IP 주소로 반환되도록 합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

| | | Source | | | Destination | | | | Forwarding | | | Monitoring | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | APPLICATION | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | TARGET | DISABLE IF UNR |
| 1 | pbf_rule_source_zone | Corporate | 192.168.10.2 | any | any | any | service-http<br>service-https | forward | ethernet1/19 | 1.1.1.1 | true | default | none | true |


©2023 Palo Alto Networks, Inc.

**STEP 5 |** 송신 인터페이스 및 ISP를 기반으로 NAT 규칙을 만듭니다. 이러한 규칙은 아웃바운드 연결에 올바른 원본 IP 주소가 사용되도록 합니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 이 예에서 각 ISP에 대해 생성한 NAT 규칙은 다음과 같습니다.

   기본 **ISP**용 **NAT**

   소스 패킷 탭의 경우,

   소스 영역: Corporate

   목적지 영역: TwoISP

   변환된 패킷 탭의 소스 주소 변환 아래

   변환 유형: 동적 IP 및 포트

   주소 유형: 인터페이스 주소

   인터페이스: 이더넷1/19

   **IP** 주소: 1.1.1.2/30

   백업 **ISP**용 **NAT**

   소스 패킷 탭의 경우,

   소스 영역: Corporate

   목적지 영역: TwoISP

   변환된 패킷 탭의 소스 주소 변환 아래

   변환 유형: 동적 IP 및 포트

   주소 유형: 인터페이스 주소

   인터페이스: 이더넷1/20

   **IP** 주소: 2.2.2.2/30

| | | | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSL |
| 1 | NAT for Primary ISP | none | Corporate | TwoISP | any | any | any | any | dynamic-ip-and-port<br>ethernet1/19<br>1.1.1.2/30 | none |
| 2 | NAT for Backup ISP | none | Corporate | TwoISP | any | any | any | any | dynamic-ip-and-port<br>ethernet1/20<br>2.2.2.2/30 | none |


©2023 Palo Alto Networks, Inc.

**STEP 6 |** 인터넷에 대한 아웃바운드 액세스를 허용하는 보안 정책을 생성합니다.

애플리케이션을 안전하게 활성화하려면 인터넷 액세스를 허용하는 간단한 규칙을 생성하고 방화벽에서 사용할 수 있는 보안 프로파일을 연결하십시오.

1. 정책 > 보안을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 규칙을 설명하는 이름을 지정합니다.
3. 소스 탭에서 소스 영역을 Corporate로 설정합니다.
4. 대상 탭에서 대상 영역을 TwoISP로 설정합니다.
5. 서비스/**URL** 카테고리 탭에서 기본값인 **application-default**를 그대로 둡니다.
6. 작업 탭에서 다음 작업을 완료합니다.
   1. 동작 설정을 허용으로 설정합니다.
   2. 프로파일 설정에서 안티바이러스, 안티스파이웨어, 취약점 보호 및 URL 필터링에 대한 기본 프로파일을 첨부합니다.
7. 옵션에서 세션 종료 시 로깅이 활성화되어 있는지 확인합니다. 보안 규칙과 일치하는 트래픽만 기록됩니다.

| | NAME | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| 1 | Copr2ISP | none | universal | Corporate | any | any | any | TwoISP | any | any | any | any | Allow |

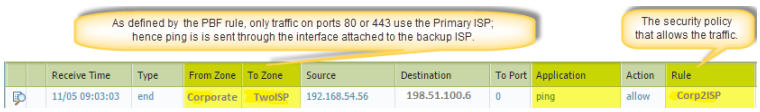
**STEP 7 |** 방화벽에서 실행 중인 구성에 정책을 저장합니다.

커밋을 클릭합니다.

**STEP 8 |** PBF 규칙이 활성화되어 있고 기본 ISP가 인터넷 액세스에 사용되는지 확인합니다.

1. 웹 브라우저를 실행하고 웹 서버에 액세스합니다. 방화벽에서 트래픽 로그에서 웹 브라우징 활동을 확인합니다.
2. 네트워크의 클라이언트에서 핑(ping) 유틸리티를 사용하여 인터넷의 웹 서버에 대한 연결을 확인하고 방화벽의 트래픽 로그를 확인합니다.

```
C:\Users\pm-user1>ping 198.51.100.6 Pinging 198.51.100.6 with
 32 bytes of data: Reply from 198.51.100.6: bytes=32 time=34ms
 TTL=117 Reply from 198.51.100.6: bytes=32 time=13ms TTL=117
 Reply from 198.51.100.6: bytes=32 time=25ms TTL=117 Reply
 from 198.51.100.6: bytes=32 time=3ms TTL=117 Ping statistics
 for 198.51.100.6: 패킷: 전송 = 4, 수신 = 4, 손실 = 0(0% 손실), 대
략적인 왕복 시간(밀리초): 최소 = 3ms, 최대 = 34ms, 평균 = 18ms
```




3. PBF 규칙이 활성 상태인지 확인하려면 다음 CLI 명령을 사용하십시오.

```
admin@PA-NGFW> show pbf rule all Rule ID Rule State Action Egress
 IF/VSYS NextHop ========== === ========== ====== ==============
 Use ISP-Pr 1 Active Forward ethernet1/1 1.1.1.1
```

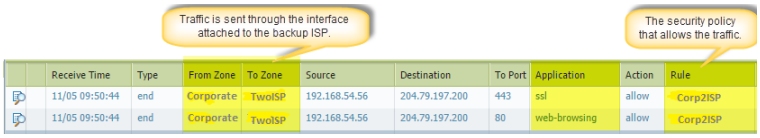
 ©2023 Palo Alto Networks, Inc.

**STEP 9 |** 백업 ISP로의 페일오버가 발생하고 소스 NAT가 올바르게 적용되었는지 확인하십시오.

1. 기본 ISP에 대한 연결을 뽑습니다.
2. 다음 CLI 명령을 사용하여 PBF 규칙이 비활성화되었는지 확인합니다.

```
admin@PA-NGFW> show pbf rule all Rule ID Rule State Action
 Egress IF/VSYS NextHop ========== === ========== ======
 ============== === Use ISP-Pr 1 Disabled Forward ethernet1/19
 1.1.1.1
```

3. 웹 서버에 접속하여 트래픽 로그를 확인하여 트래픽이 백업 ISP를 통해 포워딩되고 있는지 확인합니다.




4. 세션 세부 정보를 보고 NAT 규칙이 제대로 작동하는지 확인합니다.

```
admin@PA-NGFW> show session all
 -------------------------------------------------------------- ID
 Application State Type Flag Src[Sport]/Zone/Proto (translated
 IP[Port]) Vsys Dst[Dport]/Zone (translated IP[Port])
 ------------------------------------------------------------------
 87212 ssl ACTIVE FLOW NS 192.168.54.56[53236]/Corporate/6
 (2.2.2.2[12896]) vsys1 204.79.197.200[443]/TwoISP
 (204.79.197.200[443])
```

5. 출력에서 세션 식별 번호를 얻고 세션 세부 정보를 봅니다.

   *PBF* 규칙은 사용되지 않으므로 출력에 나열되지 않습니다.

```
admin@PA-NGFW> show session id 87212 Session 87212 c2s flow:
 source: 192.168.54.56 [Corporate] dst: 204.79.197.200 proto:
 6 sport: 53236 dport: 443 state: ACTIVE type: FLOW src user:
 unknown dst user: unknown s2c flow: source: 204.79.197.200
 [TwoISP] dst: 2.2.2.2 proto: 6 sport: 443 dport: 12896 state:
 ACTIVE type: FLOW src user: unknown dst user: unknown start
 time : Wed Nov5 11:16:10 2014 timeout : 1800 sec time to
 live : 1757 sec total byte count(c2s) : 1918 total byte
 count(s2c) : 4333 layer7 packet count(c2s) : 10 layer7 packet
 count(s2c) : 7 vsys : vsys1 application : ssl rule : Corp2ISP
 session to be logged at end : True session in session
 ager : True session synced from HA peer : False address/
port translation : source  nat-rule : NAT-Backup ISP(vsys1)
 layer7 processing : enabled URL filtering enabled : True
 URL category : search-engines session via syn-cookies :
 False session terminated on host : False session traverses
 tunnel : False authentication portal session : False ingress
 interface : ethernet1/2  egress interface : ethernet1/20
 session QoS rule : N/A (class 4)
```


©2023 Palo Alto Networks, Inc.

# 테스트 정책 규칙

실행 중인 구성에서 정책 규칙을 테스트하여 정책이 비즈니스 요구 사항 및 요구 사항에 따라 애플리케이션 및 웹사이트에 대한 액세스와 트래픽을 적절하게 허용 및 거부하는지 확인하십시오. 웹 인터페이스에서 방화벽에 대한 정책 일치 테스트를 실행하여 정책 규칙이 올바른 트래픽을 허용하고 거부하는지 테스트하고 확인할 수 있습니다.

**STEP 1 |** 웹 인터페이스 실행.

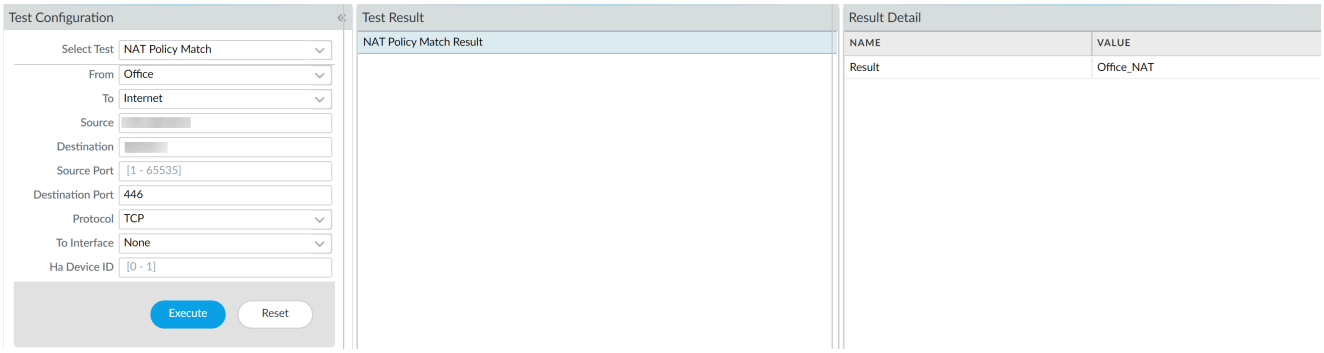
**STEP 2 |** 디바이스 > 문제 해결을 선택하여 정책 일치 또는 연결 테스트를 수행합니다.

**STEP 3 |** 정책 일치 테스트를 수행하는 데 필요한 정보를 입력합니다. 이 예제에서는 NAT 정책 일치 테스트를 실행합니다.

1. 테스트 선택 - **NAT** 정책 일치를 선택합니다.
2. **From** - 트래픽이 시작되는 영역을 선택합니다.
3. **To** - 트래픽의 대상 영역을 선택합니다.
4. 소스 - 트래픽이 발생한 IP 주소를 입력합니다.
5. 대상 - 트래픽에 대한 대상 디바이스의 IP 주소를 입력합니다.
6. 대상 포트 - 트래픽에 사용되는 포트를 입력합니다. 이 포트는 다음 단계에서 사용되는 IP 프로토콜에 따라 다릅니다.
7. 프로토콜 - 트래픽에 사용되는 IP 프로토콜을 입력합니다.
8. 필요한 경우 NAT 정책 규칙 테스트와 관련된 추가 정보를 입력합니다.

**STEP 4 |** NAT 정책 일치 테스트를 실행합니다.

**STEP 5 |** **NAT** 정책 일치 결과를 검토하여 테스트 기준과 일치하는 정책 규칙을 확인합니다.




 ©2023 Palo Alto Networks, Inc.

# 가상 시스템

이 항목에서는 가상 시스템, 그 이점, 일반적인 사용 사례 및 구성 방법에 대해 설명합니다. 또한 가상 시스템이 다른 기능과 함께 작동할 때 문서화된 다른 주제에 대한 링크도 제공합니다.


- 가상 시스템 개요
- 가상 시스템 간의 통신
- 공유 게이트웨이
- 가상 시스템 구성
- 방화벽 내에서 가상 시스템 간 통신 구성
- 공유 게이트웨이 구성
- 가상 시스템에 대한 서비스 경로 사용자 지정
- 다른 기능을 가진 가상 시스템 기능

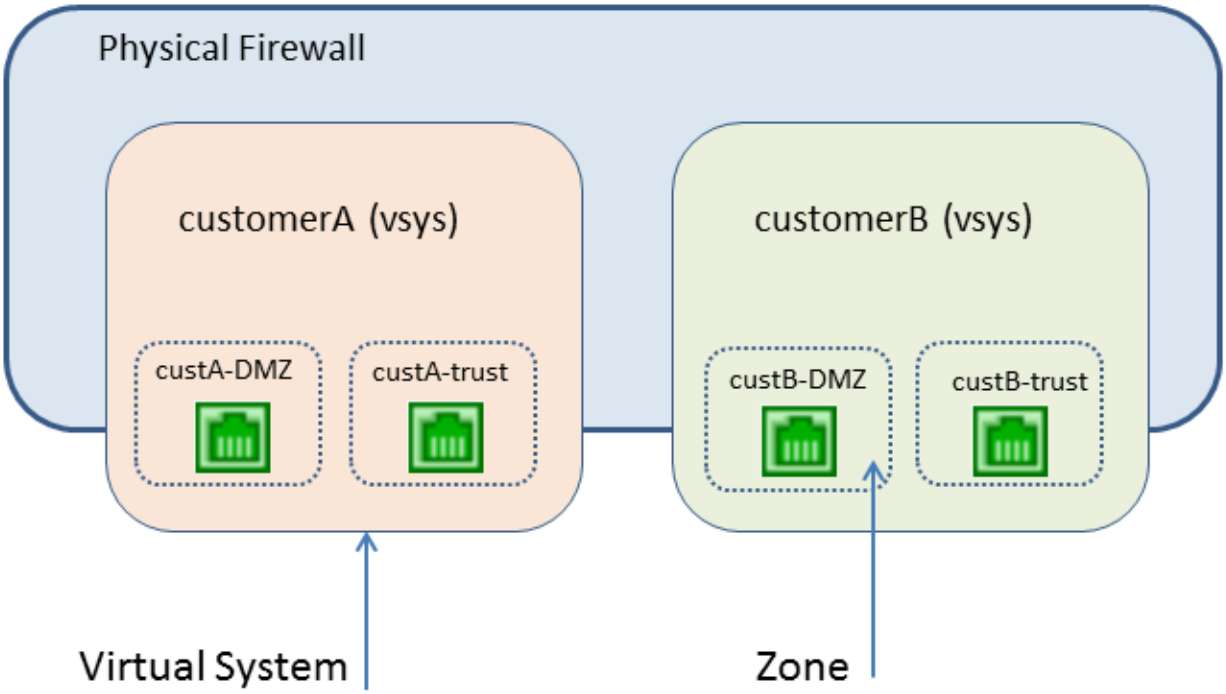
# 가상 시스템 개요

가상 시스템은 단일 물리적 Palo Alto Networks 방화벽 내의 별도의 논리적 방화벽 인스턴스입니다. 관리 서비스 공급자와 기업은 여러 방화벽을 사용하는 대신 한 쌍의 방화벽(고가용성을 위해)을 사용하고 방화벽에서 가상 시스템을 사용할 수 있습니다. 각 가상 시스템(vsys)은 트래픽이 다른 가상 시스템의 트래픽과 별도로 유지되는 독립적이고 별도로 관리되는 방화벽입니다.

- 가상 시스템 구성 요소 및 세분화
- 가상 시스템의 이점
- 가상 시스템에 대한 사례 사용
- 가상 시스템에 대한 플랫폼 지원 및 라이선스
- 가상 시스템에 대한 관리 역할
- 가상 시스템을 위한 공유 개체

## 가상 시스템 구성 요소 및 세분화

가상 시스템은 다음 그림과 같이 관리 경계를 만드는 개체입니다.




가상 시스템은 물리적 및 논리 인터페이스 및 하위 인터페이스(VLAN 및 가상 와이어 포함), 가상 라우터 및 보안 영역으로 구성됩니다. 각 가상 시스템의 배포 모드(가상 와이어, 레이어 2 또는 레이어 3의 조합)를 선택합니다. 가상 시스템을 사용하여 다음 중 일부를 분할할 수 있습니다.

- 관리 액세스
- 모든 정책(Security, NAT, QoS, Policy-based Forwarding, Decryption, Application Override, 터널 검사, 인증, DoS 보호) 관리


©2023 Palo Alto Networks, Inc.

- 모든 개체(주소 개체, 애플리케이션 그룹 및 필터, 외부 동적 목록, 보안 프로파일, 복호화 프로파일, 사용자 지정 개체 등).
- User-ID
- 인증서 관리
- 서버 프로파일
- 로깅, 보고 및 가시성 기능

가상 시스템은 방화벽의 보안 기능에 영향을 미치지만 가상 시스템만으로는 정적 및 동적 라우팅과 같은 네트워킹 기능에는 영향을 주지 않습니다. 다음 사용 사례와 같이 각 가상 시스템에 대해 하나 이상의 가상 라우터를 만들어 각 가상 시스템에 대한 라우팅을 분할할 수 있습니다.

- 한 조직의 부서에 대한 가상 시스템이 있고 모든 부서의 네트워크 트래픽이 공통 네트워크 내에 있는 경우 여러 가상 시스템에 대한 단일 가상 라우터를 만들 수 있습니다.
- 라우팅 세분화를 원하고 각 가상 시스템의 트래픽을 다른 가상 시스템에서 격리해야 하는 경우 각 가상 시스템에 대해 하나 이상의 가상 라우터를 만들 수 있습니다.
- 모든 매핑이 가상 시스템에서 공유되지 않도록 사용자 매핑을 분할하려는 경우 User-ID 허브가 아닌 가상 시스템에서 User-ID 소스를 구성할 수 있습니다. 가상 시스템 전체에서 사용자 ID 매핑 공유을(를) 참조하십시오.

## 가상 시스템의 이점

가상 시스템은 물리적 방화벽과 동일한 기본 기능을 제공하며 다음과 같은 추가 이점을 제공합니다.

- 세분화된 관리—다른 조직(또는 고객 또는 사업부)은 동일한 물리적 방화벽에서 다른 방화벽 인스턴스의 트래픽이나 정책을 방해하지 않고 자체 트래픽을 제어할 수 있도록 별도의 방화벽 인스턴스를 제어(및 모니터링)할 수 있습니다.
- 확장성—물리적 방화벽이 구성된 후에는 고객 또는 사업부를 효율적으로 추가하거나 제거할 수 있습니다. ISP, 관리되는 보안 서비스 공급자 또는 기업은 각 고객에게 서로 다른 보안 서비스를 제공할 수 있습니다.
- 자본 및 운영 비용 절감 - 가상 시스템은 가상 시스템이 하나의 방화벽에 공존하기 때문에 한 위치에 여러 물리적 방화벽을 가질 필요가 없습니다. 여러 방화벽을 구입하지 않아도 조직은 하드웨어 비용, 전기 요금 및 랙 공간을 절약할 수 있으며 유지 관리 및 관리 비용을 절감할 수 있습니다.
- **IP** 주소**-**사용자 이름 매핑을 공유할 수 있는 기능 - (가상 시스템을 사용자 ID 허브로 할당하면 가상 시스템 간에 IP 주소-사용자 이름 매핑을 공유하여 방화벽의 전체 사용자 ID 용량을 활용하고 운영 복잡성을 줄일 수 있습니다.

## 가상 시스템에 대한 사례 사용

네트워크에서 가상 시스템을 사용하는 방법에는 여러 가지가 있습니다. 한 가지 일반적인 사용 사례는 ISP 또는 MSSP(Managed Security Service Provider)가 단일 방화벽으로 여러 고객에게 서비스를 제공하는 것입니다. 고객은 쉽게 활성화 또는 비활성화할 수 있는 다양한 서비스 중에서 선택할 수 있습니다. 방화벽의 역할 기반 관리를 통해 ISP 또는 MSSP는 다른 기능에 대한 읽기 전용 기능을 숨기거나 제공하면서 기능(예: 로깅 및 보고)에 대한 각 고객의 액세스를 제어할 수 있습니다.

또 다른 일반적인 사용 사례는 여러 부서 간에 기술 또는 기밀 요구 사항이 다르기 때문에 다른 방화벽 인스턴스가 필요한 대기업의 경우입니다. 위의 경우와 마찬가지로 IT 부서가 방화벽 자체를 관리하는 동안

 ©2023 Palo Alto Networks, Inc.

그룹마다 액세스 수준이 다를 수 있습니다. 서비스를 추적 및/또는 부서에 다시 청구하여 조직 내에서 별도의 재정적 책임을 수행할 수 있습니다.

## 가상 시스템에 대한 플랫폼 지원 및 라이선스

가상 시스템은 PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈 및 PA-7000 시리즈 방화벽에서 지원됩니다. 각 방화벽 계열은 가상 시스템의 기본 번호를 지원합니다. 숫자는 플랫폼에 따라 다릅니다. PA-3200 시리즈 및 PA-3400 시리즈 방화벽에서 여러 가상 시스템을 지원하고 플랫폼에서 지원되는 가상 시스템의 기본 수 이상을 생성하려면 가상 시스템 라이선스가 필요합니다.

라이선스 정보는 구독을(를) 참조하십시오. 지원되는 가상 시스템의 기본 및 최대 수의 경우 방화벽 비교 도구를 참조하십시오.

PA-220, PA-400 시리즈, PA-800 시리즈 또는 VM 시리즈 방화벽에서는 여러 가상 시스템이 지원되지 않습니다.

기본값은 ***vsys1***입니다. *vsys1*은 방화벽의 내부 레이어와 관련이 있으므로 삭제할 수 없습니다. *vsys1*은 여러 가상 시스템을 지원하지 않는 방화벽 모델에도 나타납니다.

가상 시스템에 허용되는 세션, 규칙 및 VPN 터널에 대한 리소스 할당을 제한하여 방화벽 리소스를 제어할 수 있습니다. 각 리소스 설정에는 방화벽 모델에 따라 달라지는 유효한 값 범위가 표시됩니다. 기본 설정은 0이며, 이는 가상 시스템에 대한 제한이 방화벽 모델에 대한 제한임을 의미합니다. 그러나 특정 설정에 대한 제한은 각 가상 시스템에 대해 복제되지 않습니다. 예를 들어 방화벽에 4개의 가상 시스템이 있는 경우 각 가상 시스템은 방화벽당 허용되는 전체 복호화 규칙 수를 가질 수 없습니다. 모든 가상 시스템에 대한 복호화 규칙의 총 수가 방화벽 한도에 도달하면 더 추가할 수 없습니다.

## 가상 시스템에 대한 관리 역할

운용 관리자는 가상 시스템을 생성하고 디바이스 관리자, **vsysadmin** 또는 **vsysreader**를 추가할 수 있습니다. 디바이스 관리자는 모든 가상 시스템에 액세스할 수 있지만 관리자를 추가할 수는 없습니다. 관리자 역할 프로파일을 생성하고 역할을 가상 시스템으로 선택하면 역할이 방화벽의 특정 가상 시스템에 적용됩니다. 명령줄 탭에서 두 가지 유형의 가상 시스템 관리 역할은 다음과 같습니다.

- **vsysadmin** - 가상 시스템의 특정 측면을 생성하고 관리하기 위해 방화벽의 특정 가상 시스템에 액세스할 수 있습니다. vsysadmin은 네트워크 인터페이스, VLAN, 가상 와이어, 가상 라우터, IPSec 터널, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다. vsysadmin 권한이 있는 사람은 자신에게 할당된 가상 시스템에 대해서만 구성을 커밋할 수 있습니다.
- **vsysreader** - 방화벽의 특정 가상 시스템 및 가상 시스템의 특정 측면에 대한 읽기 전용 액세스 권한이 있습니다. vsysreader는 네트워크 인터페이스, VLAN, 가상 와이어, 가상 라우터, IPSec 터널, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다.

가상 시스템 관리자는 해당 관리자에게 할당된 가상 시스템의 로그만 볼 수 있습니다. 운용 관리자 또는 디바이스 관리자는 모든 로그를 보고, 볼 가상 시스템을 선택하거나, 가상 시스템을 User-ID 허브로 구성할 수 있습니다.


©2023 Palo Alto Networks, Inc.

# 가상 시스템을 위한 공유 개체

관리자 계정이 여러 가상 시스템으로 확장되는 경우 특정 가상 시스템 또는 방화벽의 모든 가상 시스템에 적용되는 공유 개체에 대한 개체(예: 주소 개체) 및 정책을 구성하도록 선택할 수 있습니다. 가상 시스템의 기존 개체와 동일한 이름의 공유 개체를 생성하고 입력하려고 하면 가상 시스템 개체가 사용됩니다.


©2023 Palo Alto Networks, Inc.

# 가상 시스템 간의 통신

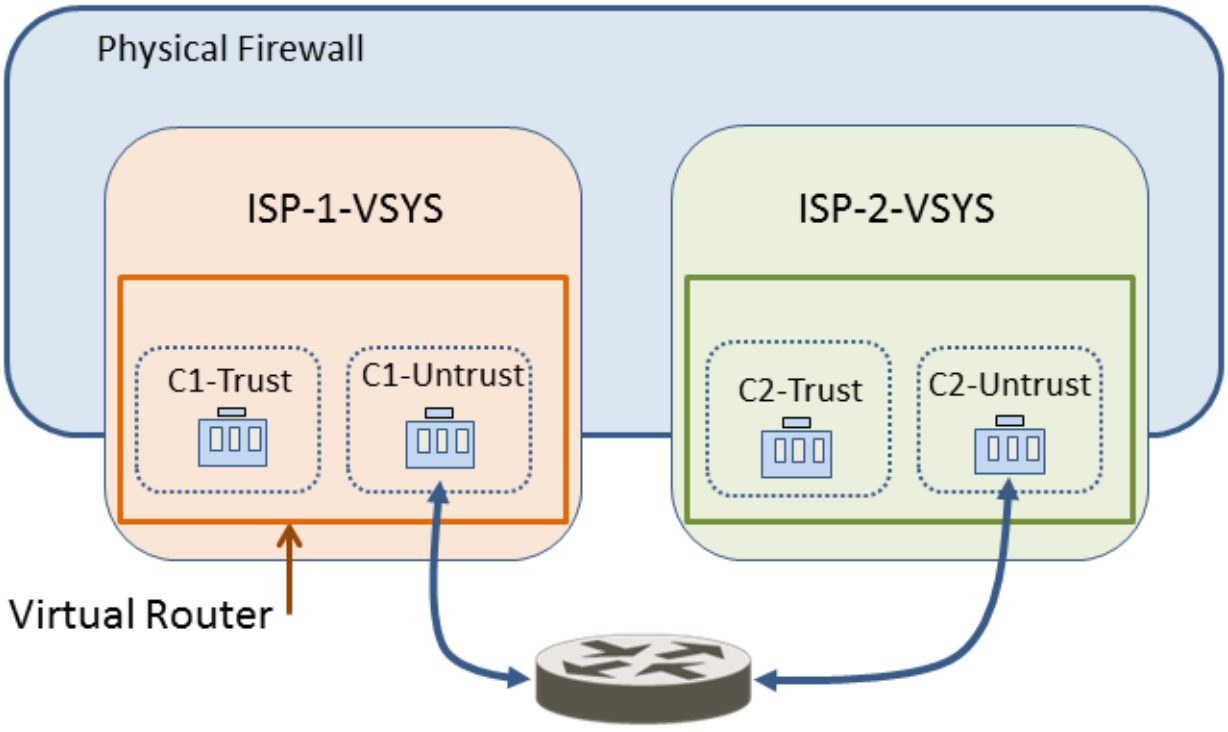
가상 시스템 간의 통신(vsys 간 트래픽)이 바람직한 두 가지 일반적인 시나리오가 있습니다. 다중 테넌시 환경에서 가상 시스템 간의 통신은 트래픽이 방화벽을 벗어나 인터넷을 통해 방화벽에 다시 들어가도록 함으로써 발생할 수 있습니다. 단일 조직 환경에서 가상 시스템 간의 통신은 방화벽 내에서 유지될 수 있습니다. 이 섹션에서는 두 시나리오에 대해 설명합니다.

- 방화벽을 떠나야 하는 VSYS 간 트래픽
- 방화벽 내에 남아 있는 VSYS 간 트래픽
- VSYS 간 통신은 두 세션을 사용합니다.

## 방화벽을 떠나야 하는 VSYS 간 트래픽

방화벽에 여러 고객이 있는 ISP(멀티 테넌시라고 함)는 각 고객에 대한 가상 시스템을 사용하여 각 고객의 가상 시스템 구성에 대한 제어를 제공할 수 있습니다. ISP는 고객에게 **vsysadmin** 권한을 부여합니다. 각 고객의 트래픽과 관리는 다른 고객으로부터 격리됩니다. 트래픽과 인터넷에 대한 자체 연결을 관리하려면 각 가상 시스템은 자체 IP 주소와 하나 이상의 가상 라우터로 구성되어야 합니다.

가상 시스템이 서로 통신해야 하는 경우 해당 트래픽은 다음 그림과 같이 가상 시스템이 동일한 물리적 방화벽에 존재하더라도 방화벽을 다른 Layer 3 라우팅 디바이스로 이동하고 방화벽으로 돌아갑니다.




## 방화벽 내에 남아 있는 VSYS 간 트래픽

위의 멀티 테넌시 시나리오와 달리 방화벽의 가상 시스템은 단일 조직에서 제어할 수 있습니다. 이 조직은 가상 시스템 간의 트래픽을 격리하고 가상 시스템 간의 통신을 허용하려고 합니다. 이러한 일반적인 사용


©2023 Palo Alto Networks, Inc.

사례는 조직에서 부서별 분리를 제공하고 해당 부서가 서로 통신하거나 동일한 네트워크에 연결할 수 있도록 하려는 경우에 발생합니다. 이 시나리오에서는 다음 항목에 설명된 대로 vsys 간 트래픽이 방화벽 내에 남아 있습니다.

- 외부 영역
- 방화벽 내 트래픽에 대한 외부 영역 및 보안 정책

## 외부 영역

위의 사용 사례에서 원하는 통신은 외부 영역을 가리키는 보안 정책을 구성하여 이루어집니다. 외부 영역은 연결할 수 있는 특정 가상 시스템과 연결된 보안 개체이며 영역은 가상 시스템의 외부에 있습니다. 가상 시스템 내에 있는 보안 영역의 수에 관계없이 가상 시스템에는 외부 영역이 하나만 있을 수 있습니다. 트래픽이 방화벽을 벗어나지 않고 서로 다른 가상 시스템의 영역 간 트래픽을 허용하려면 외부 영역이 필요합니다.

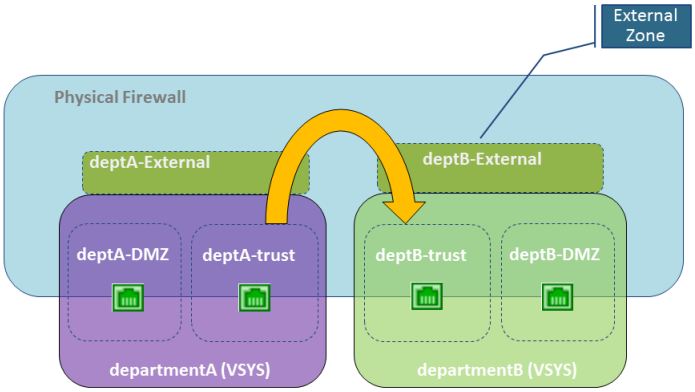
가상 시스템 관리자는 두 가상 시스템 간의 트래픽을 허용하는 데 필요한 보안 정책을 구성합니다. 보안 영역과 달리 외부 영역은 인터페이스와 연결되지 않으며 가상 시스템과 연결됩니다. 보안 정책은 보안(내부) 영역과 외부 영역 간의 트래픽을 허용하거나 거부합니다.

외부 영역에는 인터페이스나 IP 주소가 연결되어 있지 않으므로 일부 영역 보호 프로파일은 외부 영역에서 지원되지 않습니다.

각 가상 시스템은 방화벽의 개별 인스턴스이므로 가상 시스템 간에 이동하는 각 패킷의 보안 정책 및 앱 ID 평가를 검사합니다.

## 방화벽 내 트래픽에 대한 외부 영역 및 보안 정책

다음 예에서 기업에는 두 개의 별도 관리 그룹(departmentA 및 departmentB 가상 시스템)이 있습니다. 다음 그림은 각 가상 시스템과 연결된 외부 영역과 한 트러스트 영역에서 외부 영역으로, 다른 가상 시스템의 외부 영역으로, 그리고 해당 트러스트 영역의 트래픽 플로우를 보여줍니다.




외부 영역을 생성하려면 방화벽 관리자가 가상 시스템이 서로 볼 수 있도록 구성해야 합니다. 외부 영역에는 가상 시스템이 서로 볼 수 있기 때문에 보안 정책이 없습니다.

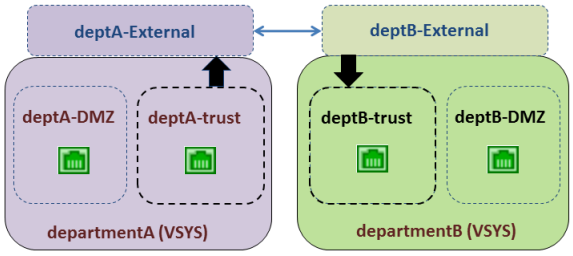
가상 시스템 간의 통신을 위해 방화벽의 수신 및 이그레스(egress) 인터페이스는 단일 가상 라우터에 할당되거나 가상 라우터 간 정적 경로를 사용하여 연결됩니다. 이 두 가지 접근 방식 중 더 간단한 방법은 서로 통신해야 하는 모든 가상 시스템을 단일 가상 라우터에 할당하는 것입니다.


©2023 Palo Alto Networks, Inc.

가상 시스템이 겹치는 IP 주소 범위를 사용하는 경우와 같이 가상 시스템에 자체 가상 라우터가 있어야 하는 이유가 있을 수 있습니다. 트래픽은 가상 시스템 간에 라우팅될 수 있지만 각 가상 라우터에는 다른 가상 라우터를 다음 홉으로 가리키는 정적 경로가 있어야 합니다.

위 그림의 시나리오를 참조하면 departmentA와 departmentB라는 두 개의 관리 그룹이 있는 엔터프라이즈가 있습니다. DepartmentA 그룹은 로컬 네트워크와 DMZ 리소스를 관리합니다. DepartmentB 그룹은 네트워크의 판매 세그먼트 안팎으로 트래픽을 관리합니다. 모든 트래픽은 로컬 네트워크에 있으므로 단일 가상 라우터가 사용됩니다. 두 가상 시스템 간의 통신을 위해 구성된 두 개의 외부 영역이 있습니다. DepartmentA 가상 시스템에는 보안 정책에 사용되는 3개의 영역(deptA-DMZ, deptA-trust 및 deptA-External)이 있습니다. DepartmentB 가상 시스템에는 deptB-DMZ, deptB-trust 및 deptB-External의 세 가지 영역도 있습니다. 두 그룹 모두 가상 시스템을 통과하는 트래픽을 제어할 수 있습니다.

deptA-trust에서 deptB-trust로의 트래픽을 허용하려면 두 가지 보안 정책이 필요합니다. 다음 그림에서 두 개의 수직 화살표는 보안 정책(그림 아래 설명)이 트래픽을 제어하는 위치를 나타냅니다.




- 보안 정책 1: 앞의 그림에서 트래픽은 deptB-trust 영역으로 향합니다. 트래픽은 deptA-trust 영역을 떠나 deptA-External 영역으로 이동합니다. 보안 정책은 소스 영역(deptA-trust)에서 대상 영역(deptA-External)으로의 트래픽을 허용해야 합니다. 가상 시스템에서는 NAT를 포함하여 이 트래픽에 대해 모든 정책 유형을 사용할 수 있습니다.

  외부 영역으로 전송된 트래픽이 원래 외부 영역에 표시되는 다른 외부 영역에 나타나고 자동으로 액세스하므로 외부 영역 간에 정책이 필요하지 않습니다.
- 보안 정책 2: 앞의 그림에서 deptB-External의 트래픽은 여전히 deptB-trust 영역으로 향하고 있으며 이를 허용하도록 보안 정책을 구성해야 합니다. 정책은 원본 영역(deptB-External)에서 대상 영역(deptB-trust)으로의 트래픽을 허용해야 합니다.

DepartmentB 가상 시스템은 DepartmentA 가상 시스템의 트래픽을 차단하도록 구성할 수 있으며 그 반대의 경우도 마찬가지입니다. 다른 영역의 트래픽과 마찬가지로 외부 영역의 트래픽은 정책에 의해 가상 시스템의 다른 영역에 도달하도록 명시적으로 허용되어야 합니다.

방화벽을 벗어나지 않는 가상 시스템 간 트래픽에 외부 영역이 필요한 것 외에도 공유 게이트웨이를 구성하는 경우 외부 영역도 필요합니다. 이 경우 트래픽이 방화벽을 떠나도록 되어 있습니다.

## VSYS 간 통신은 두 세션을 사용합니다.

단일 가상 시스템에 하나의 세션이 사용되는 것과 달리 두 가상 시스템 간의 통신은 두 개의 세션을 사용한다는 것을 이해하면 도움이 됩니다. 시나리오를 비교해 보겠습니다.

시나리오 1 - Vsys1에는 trust1 및 untrust1의 두 영역이 있습니다. trust1 영역의 호스트는 untrust1 영역의 디바이스와 통신해야 할 때 트래픽을 시작합니다. 호스트는 트래픽을 방화벽으로 보내고 방화벽은 원

 ©2023 Palo Alto Networks, Inc.

본 영역 trust1에 대한 새 세션을 대상 영역 untrust1에 생성합니다. 이 트래픽에는 하나의 세션만 필요합니다.

시나리오 2-vsys1의 호스트가 vsys2의 서버에 액세스해야 합니다. trust1 영역의 호스트는 방화벽에 대한 트래픽을 시작하고 방화벽은 첫 번째 세션인 소스 영역 trust1에서 대상 영역 untrust1까지 생성합니다. 트래픽은 내부 또는 외부에서 vsys2로 라우팅됩니다. 그런 다음 방화벽은 원본 영역 untrust2에서 대상 영역 trust2로의 두 번째 세션을 생성합니다. 이 vsys 간 트래픽에는 두 개의 세션이 필요합니다.


©2023 Palo Alto Networks, Inc.

# 공유 게이트웨이

이 주제에는 공유 게이트웨이에 대한 다음 정보가 포함되어 있습니다.

- 외부 영역 및 공유 게이트웨이
- 공유 게이트웨이에 대한 네트워킹 고려 사항

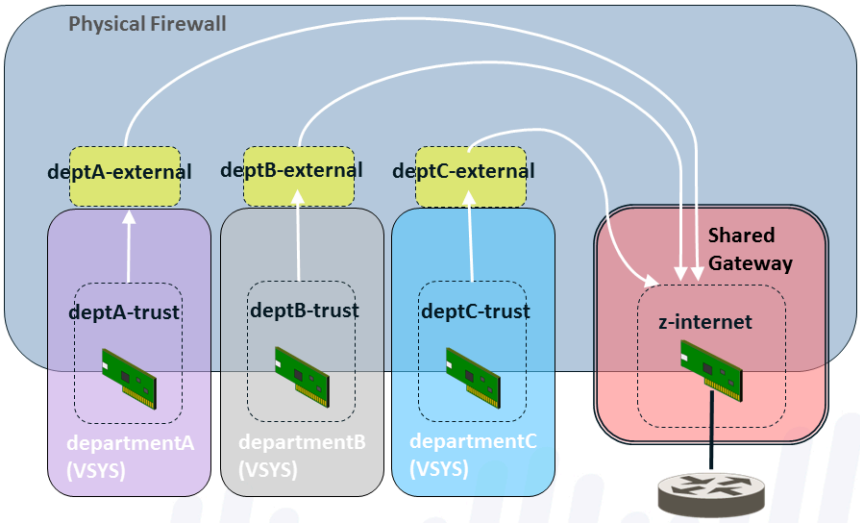
## 외부 영역 및 공유 게이트웨이

공유 게이트웨이는 인터넷을 통해 통신하기 위해 여러 가상 시스템이 공유하는 인터페이스입니다. 각 가상 시스템에는 가상 시스템의 내부 영역에서 공유 게이트웨이로의 트래픽을 허용하거나 거부하는 보안 정책을 구성하기 위해 중개자 역할을 하는 외부 영역이(가) 필요합니다.

공유 게이트웨이는 단일 가상 라우터를 사용하여 모든 가상 시스템에 대한 트래픽을 라우팅합니다. 공유 게이트웨이는 인터페이스 주변에 전체 관리 경계가 필요하지 않거나 여러 가상 시스템이 단일 인터넷 연결을 공유해야 하는 경우에 사용됩니다. 이 두 번째 경우는 ISP가 조직에 하나의 IP 주소(인터페이스)만 제공하지만 여러 가상 시스템에 외부 통신이 필요한 경우에 발생합니다.

가상 시스템 간의 동작과 달리 가상 시스템과 공유 게이트웨이 간에는 보안 정책 및 App-ID 평가가 수행되지 않습니다. 이것이 공유 게이트웨이를 사용하여 인터넷에 액세스하는 것이 다른 가상 시스템을 만드는 것보다 오버헤드가 적은 이유입니다.

다음 그림에서 세 고객은 방화벽을 공유하지만 인터넷에 액세스할 수 있는 인터페이스는 하나뿐입니다. 다른 가상 시스템을 생성하면 추가된 가상 시스템을 통해 인터페이스로 전송되는 트래픽에 대한 App-ID 및 보안 정책 평가의 오버헤드가 추가됩니다. 다른 가상 시스템을 추가하지 않으려면 솔루션은 다음 다이어그램과 같이 공유 게이트웨이를 구성하는 것입니다.




공유 게이트웨이에는 외부 세계와 통신하는 데 사용되는 전역적으로 라우팅 가능한 IP 주소가 하나 있습니다. 가상 시스템의 인터페이스에도 IP 주소가 있지만 라우팅할 수 없는 개인 IP 주소일 수 있습니다.

관리자는 가상 시스템을 다른 가상 시스템에서 볼 수 있는지의 여부를 지정해야 합니다. 가상 시스템과 달리 공유 게이트웨이는 방화벽의 모든 가상 시스템에서 항상 볼 수 있습니다.


©2023 Palo Alto Networks, Inc.

공유 게이트웨이 ID 번호는 웹 인터페이스에서 **sg<ID>**로 나타납니다. ID 번호가 포함된 이름으로 공유 게이트웨이의 이름을 지정하는 것이 좋습니다.

영역 또는 인터페이스와 같은 개체를 공유 게이트웨이에 추가하면 공유 게이트웨이가 vsys 메뉴에서 사용 가능한 가상 시스템으로 나타납니다.

공유 게이트웨이는 가상 시스템의 제한된 버전입니다. NAT 및 PBF(정책 기반 포워딩)를 지원하지만 보안, DoS 정책, QoS, 복호화, 애플리케이션 재정의 또는 인증 정책은 지원하지 않습니다.

## 공유 게이트웨이에 대한 네트워킹 고려 사항

공유 게이트웨이를 구성하는 동안 다음을 염두에 두십시오.

- 공유 게이트웨이 시나리오의 가상 시스템은 단일 IP 주소를 사용하여 공유 게이트웨이의 물리적 인터페이스를 통해 인터넷에 액세스합니다. 가상 시스템의 IP 주소를 전역적으로 라우팅할 수 없는 경우 해당 주소를 전역적으로 라우팅 가능한 IP 주소로 변환하도록 소스 NAT를 구성합니다.
- 가상 라우터는 공유 게이트웨이를 통해 모든 가상 시스템의 트래픽을 라우팅합니다.
- 가상 시스템의 기본 경로는 공유 게이트웨이를 가리켜야 합니다.
- 공유 게이트웨이에 표시되는 내부 영역과 외부 영역 사이의 트래픽을 허용하려면 각 가상 시스템에 대한 보안 정책을 구성해야 합니다.
- 방화벽 관리자는 가상 시스템의 구성원이 다른 가상 시스템의 트래픽에 영향을 줄 수 없도록 가상 라우터를 제어해야 합니다.
- Palo Alto Networks 방화벽 내에서 패킷은 한 가상 시스템에서 다른 가상 시스템 또는 공유 게이트웨이로 도약할 수 있습니다. 패킷은 두 개 이상의 가상 시스템 또는 공유 게이트웨이를 통과하지 못할 수 있습니다. 예를 들어 패킷은 vsys1에서 vsys2에서 vsys3으로 이동하거나 vsys1에서 vsys2에서 공유 gateway1로 이동할 수 없습니다. 두 예제 모두 허용되지 않는 두 개 이상의 가상 시스템을 포함합니다.

구성 시간과 노력을 절약하려면 공유 게이트웨이의 다음 이점을 고려하십시오.

- 공유 게이트웨이와 연결된 여러 가상 시스템에 대해 NAT를 구성하는 대신 공유 게이트웨이에 대해 NAT를 구성할 수 있습니다.
- 공유 게이트웨이와 연결된 여러 가상 시스템에 대해 PBR(정책 기반 라우팅)을 구성하는 대신 공유 게이트웨이에 대해 PBR을 구성할 수 있습니다.


©2023 Palo Alto Networks, Inc.

# 가상 시스템 구성

가상 시스템을 생성하려면 다음이 필요합니다.

- 운용 관리자 관리 역할.
- 구성된 인터페이스입니다.
- 플랫폼에서 지원되는 가상 시스템의 기본 수 이상을 생성하는 경우 가상 시스템 라이선스. 가상 시스템에 대한 플랫폼 지원 및 라이선스를 참조하십시오.

**STEP 1 |** 가상 시스템을 활성화합니다.

1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 수정합니다.
2. 다중 가상 시스템 기능 확인란을 선택하고 확인을 클릭합니다. 이 작업은 커밋을 승인하는 경우 커밋을 트리거합니다.

   가상 시스템을 활성화한 후에만 디바이스 탭에 가상 시스템 및 공유 게이트웨이 옵션이 표시됩니다.

**STEP 2 |** 가상 시스템을 생성합니다.

1. 디바이스 > 가상 시스템을 선택하고 추가를 클릭한 다음 "vsys"에 추가되는 가상 시스템 **ID**를 입력합니다. "(범위는 1-255).

   기본값은 ***vsys1***입니다. *vsys1*은 방화벽의 내부 레이어와 관련이 있으므로 삭제할 수 없습니다. *vsys1*은 여러 가상 시스템을 지원하지 않는 방화벽 모델에도 나타납니다.

2. 방화벽이 해독된 콘텐츠를 외부 서비스로 포워딩하도록 허용하려면 해독된 콘텐츠 포워딩 허용을 선택합니다. 예를 들어, 방화벽이 분석을 위해 해독된 콘텐츠를 WildFire로 보낼 수 있도록 하려면 이 옵션을 활성화해야 합니다.
3. 가상 시스템을 설명하는 이름을 입력합니다. 최대 31자의 영숫자, 공백 및 밑줄 문자가 허용됩니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 가상 시스템에 인터페이스를 할당합니다.

가상 라우터, 가상 와이어 또는 VLAN은 이미 구성되어 있거나 나중에 구성할 수 있습니다. 이때 각각과 연결된 가상 시스템을 지정합니다.

1. 인터페이스에 DNS 프록시 규칙을 적용하려면 일반 탭에서 **DNS** 프록시 개체를 선택합니다.
2. 인터페이스 필드에서 추가를 클릭하여 가상 시스템에 할당할 인터페이스 또는 하위 인터페이스를 입력합니다. 인터페이스는 하나의 가상 시스템에만 속할 수 있습니다.
3. 가상 시스템에 필요한 배포 유형에 따라 다음 중 하나를 수행합니다.
   - vsys에 할당할 **VLAN**을 추가합니다.
   - vsys에 할당할 가상 와이어를 추가합니다.
   - vsys에 할당할 가상 라우터를 추가합니다.
   - 방화벽이 고급 라우팅을 활성화한 경우 vsys에 할당할 논리적 라우터를 추가합니다.
4. **Visible Virtual System** 필드에서 구성 중인 가상 시스템에 표시되어야 하는 모든 가상 시스템을 선택합니다. 이것은 서로 통신해야 하는 가상 시스템에 필요합니다.

   엄격한 관리 경계가 필요한 다중 테넌시 시나리오에서는 가상 시스템을 검사하지 않습니다.
5. 확인을 클릭합니다.

**STEP 4 |** (Panorama 관리 방화벽에 필요) Panorama 웹 인터페이스에 로그인하고 **Commit** > **Push to Devices**를 선택합니다. 그리고 전체 Panorama 관리 구성을 다중 가상 시스템 방화벽의 각 가상 시스템에 푸시합니다.

이는 Panorama에서 관리하는 다중 vsys 방화벽에 대한 공유 구성 개체를 활용하는 데 필요합니다.

**STEP 5 |** (선택 사항) 가상 시스템에 허용되는 세션, 규칙 및 VPN 터널에 대한 리소스 할당을 제한합니다. 가상 시스템당 제한을 할당할 수 있는 유연성으로 방화벽 리소스를 효과적으로 제어할 수 있습니다.

1. 리소스 탭에서 선택적으로 가상 시스템에 대한 제한을 설정합니다. 각 필드에는 방화벽 모델에 따라 달라지는 유효한 값 범위가 표시됩니다. 기본 설정은 0이며, 이는 가상 시스템에 대한 제한이 방화벽 모델에 대한 제한임을 의미합니다. 그러나 특정 설정에 대한 제한은 각 가상 시스템에 대해 복제되지 않습니다. 예를 들어 방화벽에 4개의 가상 시스템이 있는 경우 각 가상 시스템은 방화벽당 허용되는 전체 복호화 규칙 수를 가질 수 없습니다. 모든 가상 시스템에 대한 전체 복호화 규칙 수가 방화벽 제한에 도달한 후에는 더 이상 추가할 수 없습니다.
   - 세션 제한

     *show session meter CLI* 명령을 사용하면 데이터플레인당 허용된 최대 세션 수, 가상 시스템에서 사용 중인 현재 세션 수 및 가상 시스템당 제한된 세션 수가 표시됩니다. *PA-5200* 또는 *PA-7000* 시리즈 방화벽에서 가상 시스템당 여러 데이터플레인이 있기 때문에 현재 사용 중인 세션 수가 세션 제한에 대해 구성된 최대값보다 클 수 있습니다. *PA-5200* 시리즈 또는 *PA-7000* 시리즈 방화벽에서 구성하는 세션 제한은 데이터플레인별로 적용되며 가상 시스템당 최대값이 더 높아집니다.
   - 보안 규칙
   - **NAT** 규칙
   - 복호화 규칙

 ©2023 Palo Alto Networks, Inc.

- **QoS** 규칙
- 애플리케이션 재정의 규칙
- 정책 기반 포워딩 규칙
- 인증 규칙
- **DoS** 보호 규칙
- 사이트 간 **VPN** 터널
- 동시 **SSL VPN** 터널

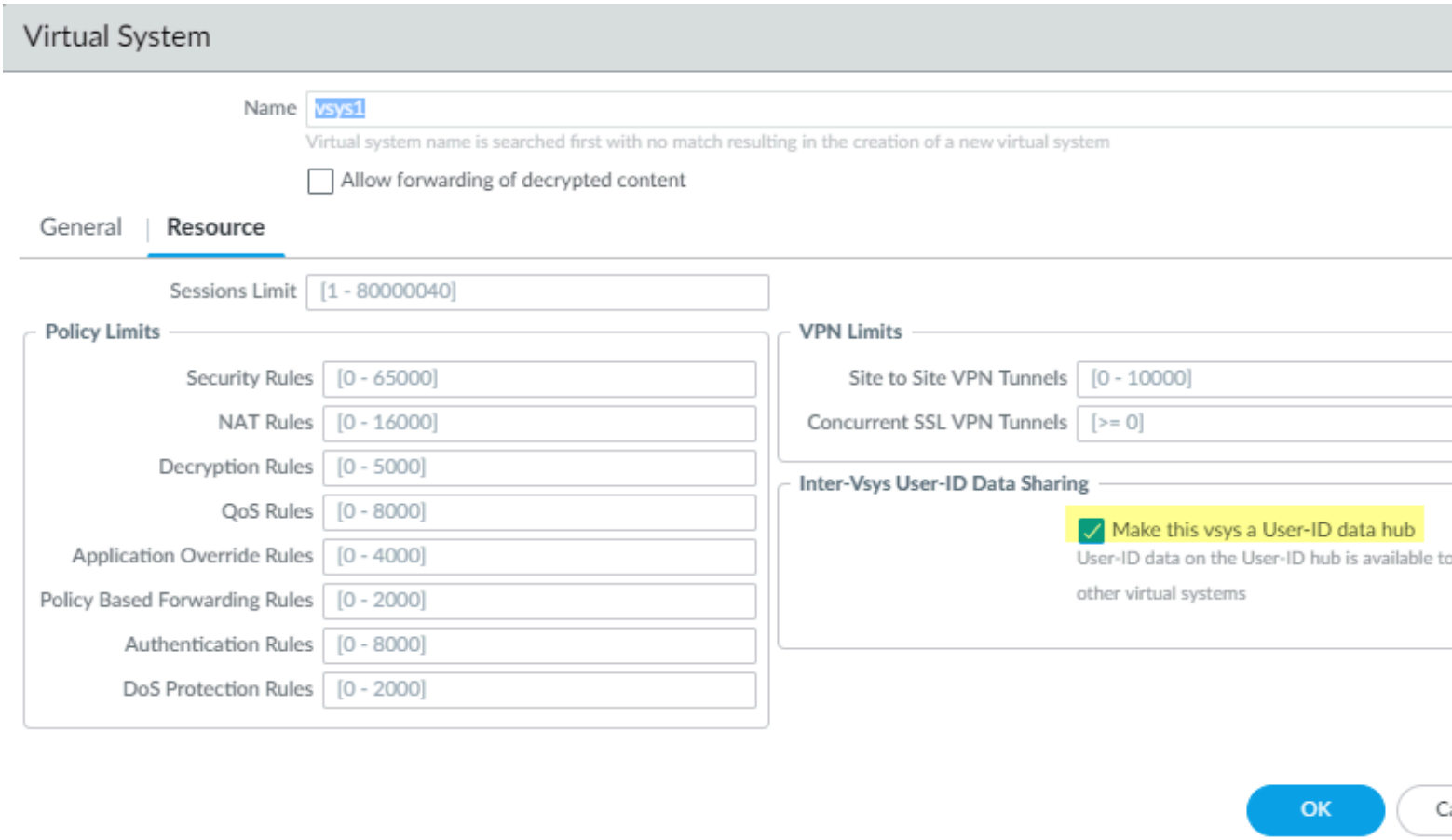
2. 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 6 |** (선택사항) 가상 시스템을 가상 시스템 전체에서 사용자 ID 매핑 공유에 대한 사용자 ID 허브로 구성합니다.

터미널 서버 에이전트의 ***IP*** 주소 및 포트와 사용자 이름 매핑 정보 및 그룹 매핑 데이터는 가상 시스템 허브와 연결된 가상 시스템 간에 공유되지 않습니다.

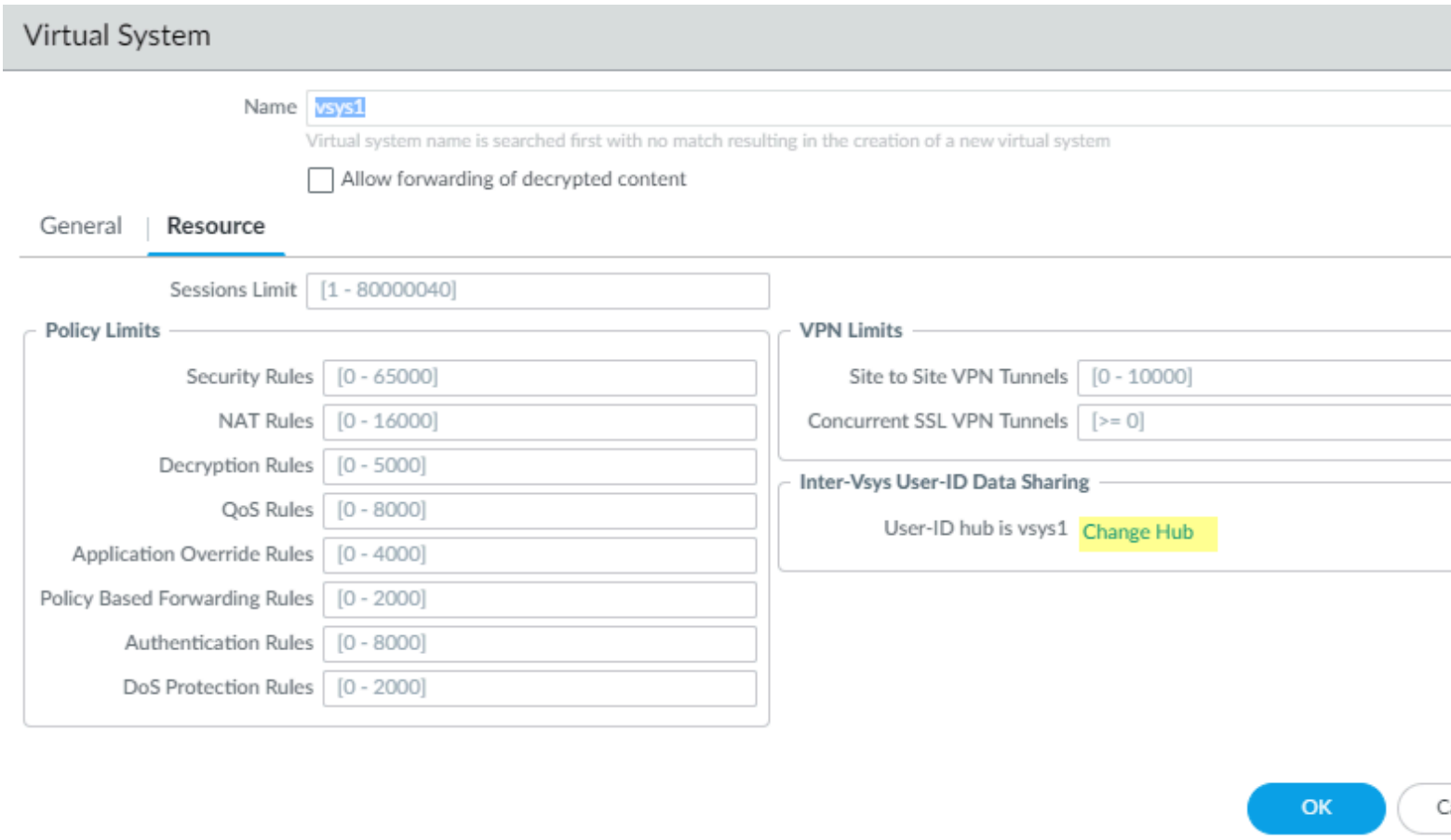
1. 기존 가상 시스템의 경우 공유하려는 User-ID 소스(예: 모니터링되는 서버 및 User-ID 에이전트)에 대한 구성을 허브로 사용할 가상 시스템으로 전송합니다.
2. 리소스 탭에서 이 **vsys**를 **User-ID** 데이터 허브로 설정을 선택합니다.



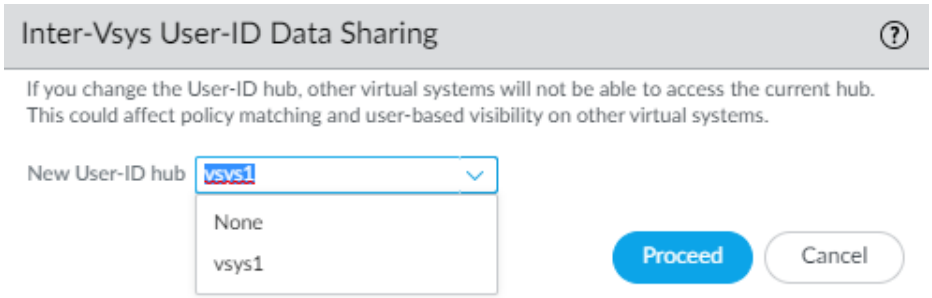

3. 예를 클릭하여 확인한 다음 확인을 클릭합니다.

   User-ID 허브를 다른 가상 시스템으로 변경하거나 비활성화하려면 현재 User-ID 허브로 구성된 가상 시스템을 선택한 다음 리소스 > 변경 허브를 선택합니다.


©2023 Palo Alto Networks, Inc.




목록에서 새 **User-ID** 허브를 선택하거나 없음을 선택하여 User-ID 허브를 비활성화하고 가상 시스템 간의 매핑 공유를 중지합니다.




계속을 클릭하여 변경 사항을 확인하고 커밋합니다.

**STEP 7 |** 구성을 커밋합니다.

커밋을 클릭합니다. 이제 가상 시스템은 개체 탭에서 액세스할 수 있는 개체입니다.


©2023 Palo Alto Networks, Inc.

**STEP 8 |** 가상 시스템이 정적 및 동적 라우팅과 같은 네트워킹 기능을 수행할 수 있도록 하려면 가상 시스템에 대해 하나 이상의 가상 라우터를 생성합니다.

또는 가상 시스템은 배포에 따라 VLAN 또는 가상 와이어를 사용할 수 있습니다.

1. 네트워크 > 가상 라우터를 선택하고 이름으로 가상 라우터를 추가합니다.
2. 인터페이스의 경우 추가를 클릭하고 가상 라우터에 속한 인터페이스를 선택합니다.
3. 확인을 클릭합니다.

**STEP 9 |** 가상 시스템의 각 인터페이스에 대한 보안 영역을 구성합니다.

하나 이상의 인터페이스에 대해 레이어 3 보안 영역을 생성합니다. 인터페이스 및 영역 구성을 참조하십시오.

**STEP 10 |** 가상 시스템의 영역으로 들어오고 나가는 트래픽을 허용하거나 거부하는 보안 정책 규칙을 구성합니다.

보안 정책 규칙 생성을 참조하십시오.

**STEP 11 |** 구성을 커밋합니다.

커밋을 클릭합니다.



가상 시스템을 생성한 후 ***CLI***를 사용하여 특정 가상 시스템에 대한 구성만 커밋할 수 있습니다.

부분적 **vsys** 커밋 ***<vsys-id>***

**STEP 12 |** (선택 사항) 가상 시스템에 대해 구성된 보안 정책을 봅니다.

CLI를 사용하려면 SSH 세션을 엽니다. 가상 시스템에 대한 보안 정책을 보려면 작동 모드에서 다음 명령을 사용하십시오.

```
set system setting target-vsys <vsys-id>
show running security-policy
```


©2023 Palo Alto Networks, Inc.

# 방화벽 내에서 가상 시스템 간 통신 구성

가상 시스템이 방화벽 내에서 서로 통신할 수 있도록 하려는 단일 엔터프라이즈 내에서 사용 사례가 있는 경우 이 작업을 수행합니다. 이러한 시나리오는 방화벽 내에 남아 있는 VSYS 간 트래픽에 설명되어 있습니다. 이 작업은 다음을 가정합니다.

- 작업을 완료하고 가상 시스템구성을 완료했습니다.
- 가상 시스템을 구성할 때 비저블 가상 시스템 필드에서 서로 통신해야 하는 모든 가상 시스템의 상자를 선택하여 서로 볼 수 있습니다.

**STEP 1 |** 각 가상 시스템에 대한 외부 영역을 구성합니다.

1. 네트워크 > 영역을 선택한 다음 이름으로 새 영역을 추가합니다.
2. 위치에서 외부 영역을 생성할 가상 시스템을 선택합니다.
3. 유형에 대해 외부를 선택합니다.
4. 가상 시스템의 경우 추가를 클릭하고 외부 영역이 연결할 수 있는 가상 시스템을 입력합니다.
5. (선택 사항) 플러드, 정찰 또는 패킷 기반 공격 보호를 제공하는 영역 보호 프로파일을 선택하거나 나중에 구성합니다.
6. (선택 사항) 로그 설정에서 영역 보호 로그를 외부 시스템으로 포워딩하기 위한 로그 포워딩 프로파일을 선택합니다.
7. (선택 사항) 사용자 식별 활성화를 선택하여 외부 영역에 대한 사용자 ID를 활성화합니다.
8. 확인을 클릭합니다.

**STEP 2 |** 보안 정책 규칙을 구성하여 내부 영역에서 가상 시스템의 외부 영역으로의 트래픽을 허용하거나 거부하며 그 반대의 경우도 마찬가지입니다.

- 보안 정책 규칙 생성을 참조하십시오.
- 방화벽 내에 남아 있는 VSYS 간 트래픽을 참조하십시오.

**STEP 3 |** 변경 사항을 커밋합니다.

커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 공유 게이트웨이 구성

인터페이스(공유 게이트웨이)를 인터넷에 공유하기 위해 여러 가상 시스템이 필요한 경우 이 작업을 수행하십시오. 이 작업은 다음을 가정합니다.

- 공유 게이트웨이가 될 전역적으로 라우팅 가능한 IP 주소로 인터페이스를 구성했습니다.
- 이전 작업인 가상 시스템 구성을 완료했습니다. 인터페이스의 경우 전역적으로 라우팅 가능한 IP 주소가 있는 외부 연결 인터페이스를 선택했습니다.
- 가상 시스템을 구성할 때 **Visible Virtual System** 필드에서 서로 볼 수 있도록 통신해야 하는 모든 가상 시스템의 상자를 선택했습니다.

**STEP 1 |** 공유 게이트웨이를 구성합니다.

1. 디바이스 > 공유 게이트웨이를 선택한 다음 추가를 클릭한 후 **ID**를 입력합니다.
2. 게이트웨이의 **ID**를 포함하여 유용한 이름을 입력하십시오.
3. **DNS** 프록시 규칙을 인터페이스에 적용하려면 DNS 프록시 필드에서 DNS 프록시 개체를 선택합니다.
4. 외부 세계와 연결되는 인터페이스를 추가합니다.
5. 확인을 클릭합니다.

**STEP 2 |** 공유 게이트웨이에 대한 영역을 구성합니다.

영역 또는 인터페이스와 같은 개체를 공유 게이트웨이에 추가할 때 공유 게이트웨이 자체가 ***VSYS*** 메뉴에서 사용 가능한 *vsys*로 나열됩니다.

1. 네트워크 > 영역을 선택한 다음 이름으로 새 영역을 추가합니다.
2. 위치에서 영역을 생성할 공유 게이트웨이를 선택합니다.
3. 유형에 대해 **Layer3**을 선택합니다.
4. (선택 사항) 플러드, 정찰 또는 패킷 기반 공격 보호를 제공하는 영역 보호 프로파일을 선택하거나 나중에 구성합니다.
5. (선택 사항) 로그 설정에서 영역 보호 로그를 외부 시스템으로 포워딩하기 위한 로그 포워딩 프로파일을 선택합니다.
6. (선택 사항) 사용자 식별 활성화를 선택하여 공유 게이트웨이에 대한 사용자 ID를 활성화합니다.
7. 확인을 클릭합니다.

**STEP 3 |** 변경 사항을 커밋합니다.

커밋을 클릭합니다.


©2023 Palo Alto Networks, Inc.

# 가상 시스템에 대한 서비스 경로 사용자 지정

여러 가상 시스템에 대해 방화벽을 사용하도록 설정하면 가상 시스템은 전역 서비스 및 서비스 경로 설정을 상속합니다. 예를 들어 방화벽은 공유 이메일 서버를 사용하여 모든 가상 시스템에 대한 이메일 경고를 생성할 수 있습니다. 일부 시나리오에서는 각 가상 시스템에 대해 서로 다른 서비스 경로를 만들 려고 합니다.

가상 시스템 수준에서 서비스 경로를 구성하는 한 가지 사용 사례는 단일 Palo Alto Networks 방화벽에서 여러 개별 테넌트를 지원해야 하는 ISP인 경우입니다. 각 테넌트는 DNS, Kerberos, LDAP, NetFlow, RADIUS, TACACS+, 다단계 인증, 이메일, SNMP 트랩, syslog, HTTP, User-ID 에이전트, VM 모니터 및 Panorama(콘텐츠 및 소프트웨어 업데이트 배포)와 같은 서비스에 액세스하기 위해 사용자 지정 서비스 경로가 필요합니다. 또 다른 사용 사례는 서비스에 대한 서버를 설정하는 그룹에 완전한 자율성을 제공하려는 IT 조직입니다. 각 그룹은 가상 시스템을 가지고 자체 서비스 경로를 정의할 수 있습니다.

가상 시스템에서 서비스 경로에 대한 가상 라우터를 선택할 수 있습니다. 이그레스*(egress)* 인터페이스를 선택할 수 없습니다. 가상 라우터를 선택한 다음 방화벽이 가상 라우터에서 패킷을 전송하면 방화벽은 대상 *IP* 주소를 기반으로 이그레스*(egress)* 인터페이스를 선택합니다. 따라서 가상 시스템에 여러 가상 라우터가 있는 경우 서비스에 대한 모든 서버에 대한 패킷은 하나의 가상 라우터에서만 이그레스*(egress)*해야 합니다. 인터페이스 소스 주소가 있는 패킷은 다른 인터페이스를 생성할 수 있지만 반환 트래픽은 원본 *IP* 주소가 있는 인터페이스에 있어 비대칭 트래픽을 생성합니다.

- 가상 시스템을 위한 서비스 경로 사용자 지정
- 가상 시스템당 로깅을 위한 PA-7000 시리즈 방화벽 구성
- 가상 시스템 또는 방화벽별로 관리 액세스 구성

## 가상 시스템을 위한 서비스 경로 사용자 지정

다중 가상 시스템 기능을 활성화하면 특정 서비스 경로가 구성되지 않은 모든 가상 시스템이 방화벽에 대한 전역 서비스 및 서비스 경로 설정을 상속합니다. 대신 다음 워크플로에 설명된 대로 다른 서비스 경로를 사용하도록 가상 시스템을 구성할 수 있습니다.

여러 가상 시스템이 있는 방화벽에는 겹치지 않는 IP 주소가 있는 인터페이스와 하위 인터페이스가 있어야 합니다. SNMP 트랩 또는 Kerberos에 대한 가상 시스템별 서비스 경로는 IPv4 전용입니다.

서비스에 대한 서비스 경로는 서비스에 대한 서버 프로파일을 구성한 방법을 엄격히 따릅니다.

- 공유 위치에 대한 서버 프로파일(**Device** > **Server** 프로파일)을 정의하는 경우 방화벽은 해당 서비스에 대한 전역 서비스 경로를 사용합니다.
- 특정 가상 시스템에 대한 서버 프로파일을 정의하는 경우 방화벽은 해당 서비스에 대해 가상 시스템별 서비스 경로를 사용합니다.
- 특정 가상 시스템에 대한 서버 프로파일을 정의했지만 해당 서비스에 대한 가상 시스템별 서비스 경로가 구성되지 않은 경우 방화벽은 해당 서비스에 대한 전역 서비스 경로를 사용합니다.

방화벽은 가상 시스템 기반의 *syslog* 포워딩을 지원합니다. 방화벽의 여러 가상 시스템이 *SSL* 전송을 사용하여 *syslog* 서버에 연결하는 경우 방화벽은 통신 보안을 위해 인증서를 하나만 생성할 수 있습니다. 방화벽은 자체 인증서가 있는 각 가상 시스템을 지원하지 않습니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** 가상 시스템에 대한 서비스 경로를 사용자 지정합니다.

1. 디바이스 > 설정 > 서비스 > 가상 시스템을 선택하고 구성할 가상 시스템을 선택합니다.
2. 서비스 경로 구성 링크를 클릭합니다.
3. 하나를 고릅니다.
   - 전역 서비스 경로 구성 상속 - 가상 시스템이 가상 시스템과 관련된 전역 서비스 경로 설정을 상속하도록 합니다. 이 옵션을 선택하는 경우 사용자 지정 단계를 건너뜁니다.
   - 사용자 정의 - 각 서비스에 대한 소스 주소를 지정할 수 있습니다.
4. 사용자 지정을 선택한 경우 서비스를 제공하는 서버에서 사용하는 주소 지정 유형에 따라 **IPv4** 또는 **IPv6** 탭을 선택합니다. 서비스에 대해 IPv4 및 IPv6 주소를 모두 지정할 수 있습니다. 서비스를 클릭합니다. (가상 시스템과 관련된 서비스만 사용할 수 있습니다.)

   여러 서비스에 대해 동일한 소스 주소를 쉽게 사용하려면 서비스에 대한 체크박스를 선택한 다음 선택한 경로 설정을 클릭한 다음 계속합니다.

   - 소스 주소 목록을 제한하려면 소스 인터페이스를 선택한 다음 소스 주소(해당 인터페이스에서)를 서비스 경로로 선택하십시오. 모든 소스 인터페이스를 선택하면 가상 시스템의 모든 인터페이스에 있는 모든 IP 주소를 선택한 소스 주소 목록에서 사용할 수 있습니다. 전역 설정 상속을 선택할 수 있습니다.
   - 소스 인터페이스에 대해 전역 설정 상속을 선택한 경우 소스 주소는 상속됨을 나타내거나 선택한 소스 주소를 나타냅니다. 소스 인터페이스에 대해 모두를 선택한 경우 IP 주소를 선택하거나 IP 주소를 입력하여(선택한 탭과 일치하는 IPv4 또는 IPv6 형식 사용) 외부 서비스로 전송되는 패킷에 사용됩니다.
   - 주소 개체를 수정하고 IP 패밀리 유형(IPv4/IPv6)이 변경되면 사용할 서비스 경로 패밀리를 업데이트하기 위해 커밋이 필요합니다.
5. 확인을 클릭합니다.
6. 다른 외부 서비스에 대한 소스 주소를 구성하려면 이전 단계를 반복하십시오.
7. 확인을 클릭합니다.

**STEP 2 |** 변경 사항을 커밋합니다.

커밋 및 확인을 클릭합니다.

PA-7000 시리즈 방화벽에 대한 로깅 서비스에 대한 가상 시스템별 서비스 경로를 구성하는 경우 가상 시스템별 로깅을 위한 PA-7000 시리즈 방화벽 구성 작업을 계속하십시오.

## 가상 시스템당 로깅을 위한 PA-7000 시리즈 방화벽 구성

트래픽, HIP 일치, 위협 및 WildFire 로그 유형의 경우 PA-7000 시리즈 방화벽은 SNMP 트랩, Syslog 및 전자 메일 서비스에 대한 서비스 경로를 사용하지 않습니다. 대신 PA-7000 시리즈 방화벽은 로깅 카드를 사용하여 지원합니다.

방화벽 구성에 따라 다음 카드 유형 중 하나가 있을 수 있습니다.

- 로그 처리 카드**(LPC)** - LPC 하위 인터페이스에서 서버의 각 서비스로의 온프레미스 스위치에 이르는 가상 시스템별 경로를 지원합니다. 시스템 및 구성 로그의 경우 PA-7000 시리즈 방화벽은 LPC가 아닌 전역 서비스 경로를 사용합니다. 방화벽에 LPC가 설치된 경우 로그 카드 포트를 구성해야 합니다.


©2023 Palo Alto Networks, Inc.

- 로그 포워딩 카드**(LFC)** - 모든 데이터플레인 로그를 외부 로그 수집기(예: Panorama 및 syslog 서버)로 포워딩하는 고속 로그 포워딩을 지원합니다. 방화벽에 LFC가 설치된 경우 로그 카드 포트를 구성할 필요가 없습니다.

  ***PAN-OS 10.1*** 이상을 실행하는 ***PA-7000*** 시리즈 방화벽에서 시스템 로그를 전달하는 유일한 방법은 ***LFC***를 구성하는 것입니다.

  외부 서버에 대한 로그 전달은 ***LFC*** 하위 인터페이스에서 아직 지원되지 않습니다.

다른 Palo Alto Networks 모델에서는 데이터 플레인이 로깅 서비스 경로 트래픽을 Management Plane(MP)으로 전송하여 트래픽을 로깅 서버로 전송합니다. PA-7000 시리즈 방화벽에서 LPC 또는 LFC에는 하나의 인터페이스만 있으며 여러 가상 시스템의 데이터플레인은 로깅 서버 트래픽(위에서 언급한 유형)을 PA-7000 시리즈 방화벽 로깅 카드로 보냅니다. 로깅 카드는 여러 하위 인터페이스로 구성되며, 플랫폼은 로깅 서비스 트래픽을 고객의 스위치로 전송하여 여러 로깅 서버에 연결할 수 있습니다.

각 하위 인터페이스는 하위 인터페이스 이름과 점선 하위 인터페이스 번호로 구성할 수 있습니다. 하위 인터페이스는 로깅 서비스를 위해 구성된 가상 시스템에 할당됩니다. PA-7000 시리즈 방화벽의 다른 서비스 경로는 다른 Palo Alto Networks 플랫폼의 서비스 경로와 유사하게 작동합니다. LPC 또는 LFC에 대한 자세한 내용은 PA-7000 시리즈 하드웨어 참조 가이드를 참조하십시오.

- 가상 시스템당 로깅을 위한 PA-7000 시리즈 LPC 구성
- 가상 시스템당 로깅을 위한 PA-7000 시리즈 LFC 구성

## 가상 시스템당 로깅을 위한 **PA-7000** 시리즈 **LPC** 구성

로그 처리 카드(LPC)가 설치된 PA-7000 시리즈 방화벽에서 다중 가상 시스템 기능을 활성화한 경우 다음 워크플로에 설명된 대로 다양한 가상 시스템에 대한 로깅을 구성할 수 있습니다.

**STEP 1 |** 로그 카드 하위 인터페이스를 생성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택한 다음 로그 카드 인터페이스가 될 인터페이스를 선택합니다.
2. 인터페이스 이름을 입력합니다.
3. 인터페이스 유형에서 로그 카드를 선택합니다.
4. 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** LPC 물리적 인터페이스의 각 테넌트에 대한 하위 인터페이스를 추가합니다.

1. 로그 카드 인터페이스 유형인 이더넷 인터페이스를 강조 표시하고 하위 인터페이스 추가를 클릭합니다.
2. 인터페이스 이름에 마침표 뒤에 테넌트의 가상 시스템에 할당된 하위 인터페이스를 입력합니다.
3. 태그에 VLAN 태그 값을 입력합니다.

   사용하기 쉽도록 태그를 하위 인터페이스 번호와 동일하게 만들지만 다른 번호일 수 있습니다.
4. (선택 사항) 설명을 입력합니다.
5. 구성 탭의 가상 시스템에 인터페이스 할당 필드에서 LPC 하위 인터페이스가 할당된 가상 시스템을 선택합니다. 또는 가상 시스템을 클릭하여 새 가상 시스템을 추가할 수 있습니다.
6. 확인을 클릭합니다.

**STEP 3 |** 하위 인터페이스에 할당된 주소를 입력하고 기본 게이트웨이를 구성합니다.

1. 로그 카드 포워딩 탭을 선택한 후 다음 중 하나 또는 둘 다를 수행합니다.
   - IPv4 섹션의 경우 하위 인터페이스에 할당된 **IP** 주소 및 넷마스크를 입력합니다. 기본 게이트웨이(Routing Information Base[RIB]에 알려진 다음 홉 주소가 없는 패킷이 전송될 다음 홉)를 입력합니다.
   - IPv6 섹션에 하위 인터페이스에 할당된 **IPv6** 주소를 입력합니다. **IPv6** 기본 게이트웨이를 입력합니다.
2. 확인을 클릭합니다.

**STEP 4 |** 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

**STEP 5 |** 아직 수행하지 않은 경우 가상 시스템에 대한 나머지 서비스 경로를 구성합니다.

가상 시스템에 대한 서비스 경로를 사용자 지정합니다.

## 가상 시스템당 로깅을 위한 PA-7000 시리즈 LFC 구성

LFC(로그 포워딩 카드)가 설치된 PA-7000 시리즈 방화벽에서 다중 가상 시스템(multi-vsys) 기능을 활성화한 경우 다른 가상 시스템에 대한 로깅을 구성할 수 있습니다. 그런 다음 LFC는 로그를 Panorama 로그 수집기 또는 syslog 서버로 전달할 수 있습니다.

물리적 인터페이스만 구성하도록 선택할 수 있습니다. 하위 인터페이스를 통한 ***syslog*** 전달은 ***LFC***에서 아직 지원되지 않으므로 각 가상 시스템은 태그가 지정되지 않은 단일 물리적 인터페이스를 사용합니다.

로그를 외부로 전달하도록 ***LFC*** 하위 인터페이스를 구성하면 인터페이스가 더 이상 예상대로 작동하지 않습니다.

각 가상 시스템에 대해 별도의 하위 인터페이스를 구성하려면 물리적 인터페이스에 하위 인터페이스를 추가하고 하위 인터페이스 트래픽을 분할하는 데 필요한 태그를 할당합니다.


©2023 Palo Alto Networks, Inc.

*Panorama* 관리 서버에서 관리하는 *PA-7000* 시리즈 방화벽의 경우 *LFC* 구성이 *Panorama*에서 푸시되는 경우 방화벽에서 로컬로 *LFC* 구성을 무시하거나 되돌릴 수 없습니다. *Panorama*에서 푸시된 *LFC* 구성을 재정의하려면 방화벽 CLI에 로그인하고 *Panorama* 푸시된 구성을 삭제해야 합니다.

```
admin> configure
```

```
admin# delete deviceconfig log-fwd-card
```

```
admin# commit
```

## 가상 시스템 또는 방화벽별로 관리 액세스 구성

운용 관리자 관리 계정이 있는 경우 vsysadmin 또는 디바이스 관리자 역할에 대한 세분화된 권한을 생성하고 구성할 수 있습니다.

**STEP 1 |** 웹 인터페이스의 다양한 영역을 구성하거나 읽기 전용으로 구성할 수 있는 권한을 관리자에게 부여하거나 비활성화하는 관리자 역할 프로파일을 생성합니다.

1. 디바이스 > 관리자 역할을 선택한 다음 관리자 역할 프로파일을 추가합니다.
2. 프로파일의 이름과 설명(선택 사항)을 입력합니다.
3. 역할에 프로파일이 영향을 미치는 제어 수준을 지정합니다.
   - 디바이스 - 프로파일을 통해 전역 설정 및 모든 가상 시스템을 관리할 수 있습니다.
   - 가상 시스템 - 이 프로파일을 사용하면 이 프로파일이 있는 관리자에게 할당된 가상 시스템만 관리할 수 있습니다. (관리자는 디바이스 > 설정 > 서비스 > 가상 시스템에 액세스할 수 있지만 글로벌 탭에는 액세스할 수 없습니다.)
4. 관리자 역할 프로파일의 웹 **UI** 탭에서 디바이스까지 아래로 스크롤하고 녹색 확인 표시(활성화)를 그대로 둡니다.
   - 디바이스에서 설정을 활성화합니다. 설정에서 아래와 같이 이 프로파일이 관리자에게 구성 권한을 부여할 영역을 활성화합니다. (해당 설정에 대해 읽기 전용이 허용된 경우 읽기 전용 잠금 아이콘이 활성화/비활성화 로테이션에 나타납니다.)
     - 관리 - 이 프로파일이 있는 관리자가 관리 탭에서 설정을 구성할 수 있습니다.
     - 작업 - 이 프로파일이 있는 관리자가 작업 탭에서 설정을 구성할 수 있습니다.
     - 서비스 - 이 프로파일이 있는 관리자가 서비스 탭에서 설정을 구성할 수 있습니다. 디바이스 > 설정 서비스 > 가상 시스템 탭에 액세스하려면 관리자가 서비스를 활성화해야 합니다. 이전 단계에서 역할이 가상 시스템으로 지정된 경우 서비스는 디바이스 > 설정에서 활성화할 수 있는 유일한 설정입니다.
     - **Content-ID** - 이 프로파일이 있는 관리자가 **Content-ID** 탭에서 설정을 구성할 수 있습니다.
     - **WildFire** - 이 프로파일이 있는 관리자가 **WildFire** 탭에서 설정을 구성할 수 있습니다.
     - 세션 - 이 프로파일이 있는 관리자가 세션 탭에서 설정을 구성할 수 있습니다.


©2023 Palo Alto Networks, Inc.

- **HSM** - 이 프로파일이 있는 관리자가 **HSM** 탭에서 설정을 구성할 수 있습니다.

5. 확인을 클릭합니다.
6. (선택 사항) 필요에 따라 전체 단계를 반복하여 다른 권한을 가진 다른 관리자 역할 프로파일을 생성합니다.

**STEP 2 |** 관리자에게 관리자 역할 프로파일을 적용합니다.

1. 디바이스 > 관리자를 선택한 다음 추가를 클릭한 다음 이름을 입력하여 관리자를 추가 합니다.
2. (선택 사항) 인증 프로파일을 선택합니다.
3. (선택 사항) 양방향 인증을 사용하려면 클라이언트 인증서 인증**(**웹**)**만 사용을 선택합니다. 서버가 클라이언트를 인증하도록 합니다.
4. 암호를 입력하고 암호를 확인합니다.
5. (선택 사항) 암호 대신 SSH 공개 키를 사용하여 훨씬 더 강력한 키 기반 인증 방법을 사용하려면 공개 키 인증**(SSH)** 사용을 선택합니다.
6. 관리자 유형에서 역할 기반을 선택합니다.
7. 프로파일에서 방금 생성한 프로파일을 선택합니다.
8. (선택 사항) 암호 프로파일을 선택합니다.
9. 확인을 클릭합니다.

**STEP 3 |** 구성을 커밋합니다.

커밋을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

# 다른 기능을 가진 가상 시스템 기능

많은 방화벽 기능을 가상 시스템별로 구성, 확인, 기록 또는 보고할 수 있습니다. 따라서 가상 시스템은 설명서의 다른 관련 위치에 언급되어 있으며 해당 정보는 여기에서 반복되지 않습니다. 일부 특정 장은 다음과 같습니다.

- 능동형/수동형 HA를 구성하는 경우 두 방화벽에는 동일한 가상 시스템 기능(단일 또는 다중 가상 시스템 기능)이 있어야 합니다. 고가용성을(를) 참조하십시오.
- 가상 시스템에 대한 QoS를 구성하려면 가상 시스템에 대한 QoS 구성을(를) 참조하십시오.
- 하위 인터페이스(및 VLAN 태그)를 사용하는 가상 와이어 배포에서 가상 시스템으로 방화벽을 구성하는 방법에 대한 자세한 내용은 가상 와이어 인터페이스를 참조하십시오.
- User-ID와 여러 가상 시스템을 구성한 경우 가상 시스템에서 사용자 매핑을 공유할 수 있습니다. 가상 시스템 전체에서 사용자 ID 매핑 공유을(를) 참조하십시오.


©2023 Palo Alto Networks, Inc.

# 영역 보호 및 **DoS** 보호

네트워크를 기능 및 조직 영역으로 분할하면 네트워크의 공격 면적(잠재적 공격자에 노출된 네트워크 부분)이 줄어듭니다. 영역 보호는 비 IP 프로토콜을 사용하는 플러드 공격, 정찰 시도, 패킷 기반 공격 및 공격에 대해 네트워크 영역을 방어합니다. 각 영역을 보호하기 위해 영역 보호 프로파일을 조정합니다(유사한 영역에 동일한 프로파일을 적용할 수 있음). DoS(서비스 거부) 보호는 플러드 공격, 특히 사용자가 웹 서버 및 데이터베이스 서버와 같은 인터넷에서 액세스하는 디바이스로부터 특정 중요한 시스템을 방어하고 세션 플러드로부터 리소스를 보호합니다. DoS 방어 프로파일 및 정책 규칙을 조정하여 각 중요한 디바이스 집합을 보호합니다. 모범 사례 문서 포털을 방문하여 영역 보호 및 DoS 방어 모범 사례에 대한 체크리스트를 확인하십시오.

> 방화벽 데이터플레인 ***CPU*** 소비를 확인하고 모니터링하여 각 방화벽이 복호화와 같이 ***CPU*** 사이클을 소비하는 다른 기능과 함께 ***DoS*** 및 영역 보호를 지원하도록 적절한 크기인지 확인합니다. ***Panorama***를 사용하여 방화벽을 관리하는 경우 디바이스모니터***(Panorama*** > 관리 디바이스 > 상태***)***를 사용하여 관리되는 모든 방화벽의 ***CPU*** 소비를 한 번에 확인하고 모니터링합니다.

- 영역을 사용한 네트워크 세그멘테이션
- 영역은 네트워크를 어떻게 보호합니까?
- 존 디펜스
- 영역 보호를 구성하여 네트워크 보안 강화
- 신규 세션의 홍수에 대한 DoS 보호

# 영역을 사용한 네트워크 세그멘테이션

네트워크가 클수록 보호하기가 더 어렵습니다. 분할되지 않은 대규모 네트워크는 관리 및 보호가 어려울 수 있는 큰 공격 면적을 나타냅니다. 트래픽과 애플리케이션이 전체 네트워크에 액세스할 수 있으므로 공격자가 네트워크에 진입하면 공격자는 네트워크를 통해 측면으로 이동하여 중요한 데이터에 액세스할 수 있습니다. 또한 대규모 네트워크는 모니터링 및 제어하기가 더 어렵습니다. 네트워크를 분할하면 영역 간의 측면 이동을 방지하여 네트워크를 통해 이동할 수 있는 공격자의 능력이 제한됩니다.

보안 영역은 하나 이상의 물리적 또는 가상 방화벽 인터페이스와 영역의 인터페이스에 연결된 네트워크 세그먼트의 그룹입니다. 각 영역이 필요한 특정 보호를 받도록 각 영역에 대한 보호를 개별적으로 제어합니다. 예를 들어 재무 부서의 영역은 IT 영역에서 허용하는 모든 애플리케이션을 허용할 필요가 없습니다.

네트워크를 완전히 보호하려면 모든 트래픽이 방화벽을 통과해야 합니다. 인터페이스 및 영역을 구성하여 인터넷 게이트웨이, 민감한 데이터 스토리지 및 비즈니스 애플리케이션과 같은 다양한 기능 영역과 재무, IT, 마케팅 및 엔지니어링과 같은 다양한 조직 그룹에 대해 별도의 영역을 생성합니다. 기능, 애플리케이션 사용 또는 사용자 액세스 권한이 논리적으로 구분되는 곳마다 해당 영역을 격리 및 보호하기 위해 별도의 영역을 생성하고 적절한 보안 정책 규칙을 적용하여 하나 또는 일부 그룹에서만 액세스가 필요한 데이터 및 애플리케이션에 대한 불필요한 액세스를 방지할 수 있습니다. 영역이 세분화될수록 네트워크 트래픽에 대한 가시성과 제어가 향상됩니다. 네트워크를 영역으로 나누면 사용자, 디바이스, 애플리케이션 또는 패킷을 신뢰하지 않고 모든 것을 확인하는 보안 규칙을 실행하는 제로 트러스트 아키텍처를 만드는 데 도움이 됩니다. 최종 목표는 합법적인 비즈니스 요구 사항이 있는 사용자, 디바이스 및 애플리케이션에만 액세스할 수 있는 네트워크를 생성하고 다른 모든 트래픽은 거부하는 것입니다.

영역에 대한 액세스를 적절하게 제한하고 허용하는 방법은 네트워크 환경에 따라 다릅니다. 예를 들어, 워크스테이션이 민감한 제조 장비를 제어하는 반도체 제조 현장 또는 로봇 조립 공장과 같은 환경 또는 매우 제한된 액세스 영역에서는 외부 디바이스로부터의 액세스를 허용하지 않는 물리적 분할이 필요할 수 있습니다(모바일 디바이스 액세스 불가).

액세스 권한이 특정 영역의 디바이스가 아닌 사용자 또는 사용자 그룹에 연결되기 때문에, 사용자가 네트워크에 액세스하는 위치에 관계없이 적절한 액세스 권한을 받을 수 있도록 사용자가 모바일 디바이스로 네트워크에 액세스할 수 있는 환경으로 네트워크를 영역으로 분할하는 것과 함께 User-ID 및 App-ID를 활성화합니다.

다른 기능 영역 및 그룹에 대한 보호 요구 사항도 다를 수 있습니다. 예를 들어, 많은 양의 트래픽을 처리하는 영역에는 일반적으로 적은 양의 트래픽을 처리하는 영역과 다른 플러드 방지 임계값이 필요할 수 있습니다. 각 영역에 대한 적절한 보호를 정의하는 기능은 네트워크를 분할하는 또 다른 이유입니다. 적절한 보호는 네트워크 아키텍처, 보호하려는 대상, 허용 및 거부하려는 트래픽에 따라 다릅니다.

 ©2023 Palo Alto Networks, Inc.

# 영역은 네트워크를 어떻게 보호합니까?

영역은 네트워크를 더 작고 관리하기 쉬운 영역으로 분할하여 네트워크를 보호할 뿐만 아니라 영역에 대한 액세스와 영역 간의 트래픽 이동을 제어할 수 있기 때문에 영역도 네트워크를 보호합니다.

영역은 방화벽 인터페이스가 영역에 할당할 때까지 트래픽을 처리할 수 없기 때문에 제어되지 않은 트래픽이 방화벽 인터페이스를 통해 네트워크로 흐르는 것을 방지합니다. 방화벽은 트래픽이 영역에 들어가기 전에 트래픽을 필터링하기 위해 원래 클라이언트에서 응답 서버(c2s)로의 흐름 방향으로 트래픽이 방화벽에 들어가는 인그레스(ingress) 인터페이스에 영역 보호를 적용합니다.

방화벽 인터페이스 유형과 영역 유형(Tap, virtual wire, L2, L3, Tunnel 또는 External)이 일치해야 영역에 속하지 않는 트래픽을 허용하지 않도록 네트워크를 보호하는 데 도움이 됩니다. 예를 들어 L2 인터페이스를 L2 영역에 할당하거나 L3 인터페이스를 L3 영역에 할당할 수 있지만 L2 인터페이스를 L3 영역에 할당할 수는 없습니다.

또한 방화벽 인터페이스는 하나의 영역에만 속할 수 있습니다. 다른 영역으로 향하는 트래픽은 동일한 인터페이스를 사용할 수 없으므로 부적절한 트래픽이 영역에 들어가는 것을 방지하고 각 개별 영역에 적절한 보호를 구성할 수 있습니다. 둘 이상의 방화벽 인터페이스를 영역에 연결하여 대역폭을 늘릴 수 있지만 각 인터페이스는 하나의 영역에만 연결할 수 있습니다.

방화벽이 영역에 대한 트래픽을 허용한 후 트래픽은 해당 영역 내에서 자유롭게 흐르고 기록되지 않습니다. 각 영역을 더 세분화할수록 각 영역에 액세스하는 트래픽에 대한 제어가 강화되고 멀웨어가 영역 간에 네트워크를 통해 이동하기가 더 어려워집니다. 보안 정책 규칙이 허용하고 영역이 동일한 영역 유형(Tap, virtual wire, L2, L3, Tunnel 또는 External)인 경우가 아니면 트래픽은 영역 간에 흐를 수 없습니다. 예를 들어 보안 정책 규칙은 두 L3 영역 간의 트래픽을 허용할 수 있지만 L3 영역과 L2 영역 간의 트래픽은 허용하지 않습니다. 방화벽은 보안 정책 규칙이 영역 간 트래픽을 허용할 때 영역 간에 이동하는 트래픽 플로우를 기록합니다.

기본적으로 보안 정책 규칙은 영역 간 트래픽의 측면 이동을 방지하므로 멀웨어가 한 영역에 액세스한 다음 네트워크를 통해 다른 대상으로 자유롭게 이동할 수 없습니다.



터널 영역은 암호화되지 않은 터널을 위한 것입니다. 터널 콘텐츠 검사 개요에 설명된 대로 터널 콘텐츠와 외부 터널 영역에 다른 보안 정책 규칙을 적용할 수 있습니다.


©2023 Palo Alto Networks, Inc.

# 존 디펜스

영역 보호 프로파일은 플러드, 정찰, 패킷 기반 및 비 IP 프로토콜 기반 공격으로부터 영역을 보호합니다. DoS 방어 정책 규칙에 사용되는 DoS 방어 프로파일은 표적 플러드 및 리소스 기반 공격으로부터 특정 중요 디바이스를 방어합니다. DoS 공격은 원치 않는 트래픽이 많은 네트워크 또는 대상 중요 시스템에 과부하를 주어 네트워크 서비스를 중단시키려고 시도합니다.

다양한 유형의 DoS 공격으로부터 네트워크를 보호할 계획:

- 애플리케이션 기반 공격 - 특정 애플리케이션의 약점을 표적으로 삼고 리소스를 고갈시켜 합법적인 사용자가 사용할 수 없도록 합니다. 슬로로리스(Slowloris) 공격이 그 예입니다.
- 프로토콜 기반 공격 - 상태 소진 공격이라고도 하는 이러한 공격은 프로토콜 약점을 대상으로 합니다. 일반적인 예는 SYN 플러드 공격입니다.
- 볼류메트릭 공격 - 사용 가능한 네트워크 리소스, 특히 대역폭을 압도하고 적법한 사용자가 해당 리소스에 액세스하지 못하도록 대상을 다운시키려는 대규모 공격입니다. 이에 대한 예는 UDP 플러드 공격입니다.

기본 영역 보호 프로파일이나 DoS 방어 프로파일 및 DoS 방어 정책 규칙은 없습니다. 각 영역의 트래픽 특성을 기반으로 영역 보호를 구성 및 적용하고 각 영역에서 보호하려는 개별 중요 시스템을 기반으로 DoS 방어를 구성합니다.

- 존 디펜스 툴
- 구역 방어 도구는 어떻게 작동합니까?
- DoS 보호를 위한 방화벽 배치
- 영역 보호 프로파일
- 패킷 버퍼 보호
- DoS 보호 프로파일 및 정책 규칙

## 존 디펜스 툴

DoS 공격에 대한 효과적인 방어에는 계층화된 접근 방식이 필요합니다. 첫 번째 방어 계층은 인터넷 연결 네트워크 경계에 있는 전용 대용량 DDoS 보호 디바이스여야 하며, 세션 기반 방화벽은 처리하도록 설계되지 않은 상태로 경계 라우터, 스위치 또는 볼륨 측정 공격의 방어를 위한 적절한 ACL(액세스 제어 목록)이 있는 기타 하드웨어 기반 패킷 드롭 디바이스여야 합니다. 방화벽은 더 세분화된 DoS 공격 방어 계층과 전용 DDoS 디바이스가 제공하지 않는 애플리케이션 트래픽에 대한 가시성을 추가합니다.

Palo Alto Networks 방화벽은 네트워크 영역 및 중요한 디바이스에 대한 DoS 방어에 계층화할 수 있는 네 가지 보완 도구를 제공합니다.

- 영역 보호 프로파일은 IP 플러드 공격, 정찰 포트 스캔 및 호스트 스윕, IP 패킷 기반 공격 및 비 IP 프로토콜 공격에 대해 인그레스(ingress) 영역 가장자리를 방어합니다. 수신 영역은 트래픽이 클라이언트에서 서버(c2s)로의 플로우 방향으로 방화벽에 들어가는 곳입니다. 여기서 클라이언트는 플로우의 발신자이고 서버는 응답자입니다. 영역 보호 프로파일은 영역으로 의 새로운 연결(CPS)을 제한하여 영역으로 들어오는 집계 트래픽을 기반으로 DoS 공격에 대한 두 번째 방어 레이어를 제공합니다. 영역 보호 프

 ©2023 Palo Alto Networks, Inc.

로파일은 프로파일이 영역으로 들어오는 집계 트래픽에 적용되므로 개별 디바이스(IP 주소)를 고려하지 않습니다.

영역 보호 프로파일은 방화벽이 DoS Protection 정책 및 보안 정책 규칙 조회를 수행하기 전에 세션이 형성될 때 네트워크를 방어하고 DoS Protection 정책 또는 보안 정책 규칙 조회보다 적은 CPU 주기를 사용합니다. 영역 보호 프로파일이 트래픽을 거부하는 경우 방화벽은 정책 규칙 조회에 CPU 주기를 사용하지 않습니다.

인터넷을 향한 및 내부 모두 모든 영역에 영역 보호 프로파일을 적용합니다.

- **DoS** 보호 프로파일 및 정책 규칙은 플러드 공격, 특히 사용자가 인터넷에서 액세스하는 고가치 대상으로부터 특정 개별 엔드포인트 및 리소스를 보호합니다. 영역 보호 프로파일은 홍수 공격으로부터 영역을 보호하는 반면, 적절한 DoS 보호 프로파일이 있는 DoS 보호 정책 규칙은 대상 홍수 공격으로부터 구역의 중요한 개별 시스템을 보호하여 DoS 공격에 대한 세분화된 세 번째 방어 계층을 제공합니다.

  ***DoS*** 방어의 목적은 중요한 디바이스를 방어하는 것이고 리소스를 소비하기 때문에 ***DoS*** 방어는 ***DoS*** 방어 정책 규칙에 지정한 디바이스만 방어합니다**.** 다른 디바이스는 보호되지 않습니다**.**

  DoS 방어 프로파일은 개별 디바이스 또는 디바이스 그룹, 리소스 보호 임계값(지정된 엔드포인트 및 리소스에 대한 세션 제한) 및 프로파일이 집계 또는 분류된 트래픽에 적용되는지의 여부에 대한 플러드 보호 임계값(새 CPS 제한)을 설정합니다. DoS 방어 정책 규칙은 일치 기준(소스, 대상, 서비스 포트), 트래픽이 규칙과 일치할 때 수행할 작업 및 각 규칙과 연결된 집계 및 분류된 DoS 방어 프로파일을 지정합니다.

  집계 DoS 방어 정책 규칙은 DoS 방어 정책 규칙 일치 기준을 충족하는 모든 디바이스의 결합된 트래픽에 총 DoS 방어 프로파일에서 정의된 CPS 임계값을 적용합니다. 예를 들어 CPS 비율을 20,000으로 제한하도록 집계 DoS 방어 프로파일을 구성하면 전체 그룹의 총 연결 수에 20,000CPS 제한이 적용됩니다. 이 경우 한 디바이스는 허용된 연결의 대부분을 받을 수 있습니다.

  분류된 DoS 방어 정책 규칙은 정책 규칙과 일치하는 각 개별 디바이스에 분류된 DoS 방어 프로파일에 정의된 CPS 임계값을 적용합니다. 예를 들어 CPS 속도를 4,000으로 제한하도록 분류된 DoS 방어 프로파일을 구성하면 그룹의 어떤 디바이스도 4,000개 이상의 CPS를 수락할 수 없습니다. DoS 방어 정책에는 하나의 집계 프로파일과 하나의 분류된 프로파일이 있을 수 있습니다.

  분류된 프로파일은 소스 ***IP,*** 대상 ***IP*** 또는 둘 다로 연결을 분류할 수 있습니다**.** 인터넷을 향한 영역의 경우 방화벽이 인터넷 라우팅 테이블을 보유하도록 확장할 수 없기 때문에 대상 ***IP***별로 분류합니다**.**

  중요한 디바이스, 특히 사용자가 웹 서버 및 데이터베이스 서버와 같이 인터넷에서 액세스하는 인기 있는 공격 대상에만 DoS 방어를 적용합니다.

- 기존 세션의 경우 패킷 버퍼 보호는 임계값 및 타이머를 사용하여 악성 세션을 완화하기 위해 방화벽의 패킷 버퍼를 압도하려는 단일 세션 DoS 공격으로부터 방화벽(및 영역)을 보호합니다. 패킷 버퍼 보호 설정을 전역으로 구성하고 영역별로 적용합니다.
- 보안 정책 규칙은 세션의 인그레스(ingress) 및 이그레스(egress) 플로우 모두에 영향을 미칩니다. 세션을 설정하려면 들어오는 트래픽이 기존 보안 정책 규칙과 일치해야 합니다. 일치하지 않으면 방화벽이

 ©2023 Palo Alto Networks, Inc.

패킷을 삭제합니다. 보안 정책은 영역, IP 주소, 사용자, 애플리케이션, 서비스 및 URL 카테고리를 포함한 기준을 사용하여 영역 간(interzone) 및 영역 내(intrazone) 트래픽을 허용하거나 거부합니다.



***DoS*** 공격을 방어하는 데 도움이 되는 경우 각 보안 정책 규칙에 모범 사례 취약성 보호 프로파일을 적용합니다.

기본 보안 정책 규칙은 트래픽이 영역 간 이동을 허용하지 않으므로 인터존(interzone) 트래픽을 허용하려면 보안 정책 규칙을 구성해야 합니다. 기본적으로 모든 인트라존(intrazone) 트래픽이 허용됩니다. 인트라존, 인터존 또는 범용(인트라존 및 인터존) 트래픽과 일치하고 제어하도록 보안 정책 규칙을 구성할 수 있습니다.



영역 보호 프로파일, ***DoS Protection*** 프로파일 및 정책 규칙 및 보안 정책 규칙은 방화벽의 데이터플레인 트래픽에만 영향을 줍니다. 방화벽 관리 인터페이스에서 발생하는 트래픽은 데이터플레인을 교차하지 않으므로 방화벽은 이러한 프로파일 또는 정책 규칙과 관리 트래픽과 일치하지 않습니다.

- 또한 해시, CVE, 서명 ID, 도메인 이름, URL 또는 IP 주소로 위협에 대해 Palo Alto Networks Threat Vault(유효한 지원 계정 및 로그인 필요)를 검색할 수도 있습니다.

## 구역 방어 도구는 어떻게 작동합니까?

패킷이 방화벽에 도착하면 방화벽은 패킷 헤더에서 파생된 ingress 영역, 송신 영역, 소스 IP 주소, 대상 IP 주소, 프로토콜 및 애플리케이션을 기반으로 패킷을 기존 세션과 일치시키려 합니다. 방화벽이 일치를 찾은 경우 패킷은 세션을 이미 제어하는 보안 정책 규칙을 사용합니다. 패킷이 기존 세션과 일치하지 않는 경우 방화벽은 영역 보호 프로파일, DoS 방어 프로파일 및 정책 규칙 및 보안 정책 규칙을 사용하여 세션을 설정할지 아니면 패킷을 삭제할지의 여부와 패킷이 받는 액세스 수준을 결정합니다.

트래픽이 인터넷을 향한 네트워크 가장자리에서 전용 DDoS 디바이스를 통과한 후 방화벽이 적용되는 첫 번째 보호는 해당 영역에 연결된 경우 영역 보호 프로파일의 광범위한 방어입니다. 방화벽은 패킷이 도착하는 인터페이스에서 영역을 결정합니다(각 인터페이스는 하나의 영역에만 할당되고 트래픽을 포워딩하는 모든 인터페이스는 영역에 속해야 합니다). 영역 보호 프로파일이 패킷을 거부하면 방화벽은 패킷을 삭제하고 DoS 방어 정책 또는 보안 정책을 조회할 필요가 없으므로 리소스를 저장합니다. 방화벽은 새 세션(기존 세션과 일치하지 않는 패킷)에만 영역 보호 프로파일을 적용합니다. 방화벽이 세션을 설정한 후 방화벽은 해당 세션에서 패킷을 성공하기 위해 영역 보호 프로파일 조회를 우회합니다.

영역 보호 프로파일이 패킷을 삭제하지 않으면 방화벽이 적용되는 두 번째 보호는 DoS 방어 정책 규칙입니다. 영역 보호 프로파일이 영역으로 가는 총 트래픽량에 따라 패킷을 허용하는 경우 DoS 방어 정책 규칙은 특정 대상으로 이동하거나 규칙의 DoS 방어 프로파일에서 플러드 보호 또는 리소스 보호 설정을 초과한 특정 소스에서 오는 경우 패킷을 거부할 수 있습니다. 패킷이 DoS 방어 정책 규칙과 일치하는 경우 방화벽은 패킷에 규칙을 적용합니다. 규칙이 액세스를 거부하면 방화벽은 패킷을 삭제하고 보안 정책 조회를 수행하지 않습니다. 규칙이 액세스를 허용하는 경우 방화벽은 보안 정책 조회를 수행합니다. 영역 보호 프로파일과 마찬가지로 방화벽은 새 세션에서만 DoS 방어 정책을 적용합니다.

방화벽이 적용되는 세 번째 보호는 보안 정책 조회이며, 이는 영역 보호 프로파일 및 DoS 방어 정책 규칙이 패킷을 허용하는 경우에만 발생합니다. 방화벽이 패킷에 대한 보안 정책 규칙 일치가 없는 경우 방화벽은 패킷을 삭제합니다. 방화벽에서 일치하는 보안 정책 규칙을 찾은 경우 방화벽은 패킷에 규칙을 적용합니다. 방화벽은 세션 수명 동안 양방향(c2 및 s2c)의 트래픽에 대한 보안 정책 규칙을 적용합니다. DoS 공격을 방어하기 위해 모든 보안 정책 규칙에 모범 사례 취약성 보호 프로파일을 적용합니다.


©2023 Palo Alto Networks, Inc.

방화벽이 적용하는 네 번째 보호는 디바이스를 보호하기 위해 전체적으로 적용되고 방화벽의 패킷 버퍼를 압도하려는 단일 세션 DoS 공격을 방지하기 위해 영역에 개별적으로 적용할 수 있는 패킷 버퍼 보호입니다. 전역 보호를 위해 방화벽은 트래픽 수준이 보호 임계값을 초과할 때 세션이 아닌 패킷을 삭제하기 위해 RED(Random Early Drop)를 사용했습니다. 영역별 보호의 경우 방화벽은 패킷 버퍼 임계값을 위반하는 경우 소스 IP 주소를 차단합니다. 영역 및 DoS 방어와 달리 패킷 버퍼 보호는 기존 세션에 적용됩니다.

# DoS 보호를 위한 방화벽 배치

방화벽은 대규모 DoS 공격을 방어하기 위해 초당 수백만 개의 연결(CPS)로 확장하도록 설계되지 않은 세션 기반 디바이스입니다. 방화벽은 각 고유 흐름을 세션으로 처리하며, 포트 및 IP 수준에서 패킷 검사에 CPU 주기를 보내 애플리케이션 트래픽에 대한 가시성을 제공하며, 플러드 임계값 카운터에 대한 각 세션을 계산해야 하므로 방화벽 배치는 방화벽 배치가 방화벽을 범람하지 않도록 하는 것이 중요합니다.

최상의 DoS 방어를 위해 방화벽을 보호하는 리소스에 최대한 가깝게 배치합니다. 이렇게 하면 방화벽이 처리하는 데 필요한 세션 수가 줄어들므로 DoS 방어를 제공하는 데 필요한 방화벽 리소스의 양이 줄어듭니다.

인터넷 페이싱 경계에서 전용 DDoS 디바이스 및 경계 라우터 및 스위치 앞에 DoS 방어 또는 영역 보호에 사용하는 방화벽을 배치하지 마십시오. 대량의 디바이스를 대량 플러드 공격을 완화하기 위해 DoS 방어의 첫 번째 줄로 확인합니다. 경계의 영역 및 DoS 방어의 경우 대용량 방화벽을 사용하여 대용량 디바이스 뒤에 배치합니다. 일반적으로 방화벽이 둘레에 가까울수록 트래픽 볼륨을 처리해야 하는 더 높은 용량이 있어야 합니다.

네트워크를 영역으로 분할하는 방식은 내부 DoS 공격을 완화하는 데 도움이 될 수 있습니다. 작은 영역은 더 많은 트래픽이 영역을 교차해야 하기 때문에 트래픽에 대한 가시성을 높이고 멀웨어의 측면 이동을 더 잘 방지하고 인터존 트래픽을 허용하려면 특정 보안 정책 규칙을 만들어야 합니다(기본적으로 모든 인트라존 트래픽이 허용됨). 네트워크가 상대적으로 분할되지 않은 경우 세분화 방법을 다시 방문하는 것이 좋습니다.

# 플러드 임계값 설정을 위한 기준 CPS 측정

플러드 보호 임계값은 잠재적인 플러드 공격을 완화하기 위해 새 연결을 제한할 때와 모든 새 연결을 끊을 때, 영역(영역 보호 프로파일), 영역의 디바이스 그룹(집계 DoS 보호 정책) 또는 영역의 개별 디바이스(분류된 DoS 보호 정책)에 대해 허용할 새 CPS(초당 연결 수)를 결정합니다. 기본 영역 보호 프로파일 및 DoS 방어 프로파일 플러드 방지 임계값은 각 네트워크가 고유하기 때문에 대부분의 네트워크에 적합하지 않습니다. 효과적인 영역 보호 프로파일 임계값을 설정하려면 각 영역에 대한 총 일반 및 최대 CPS를 이해해야 하며 효과적인 DoS 보호 프로파일 임계값을 설정하려면 실수로 임계값을 너무 높게 설정하지 않고 플러드 공격을 허용하거나 임계값을 너무 낮게 설정하여 트래픽을 조절하지 않도록 방어하려는 개별 중요 시스템에 대해 이해해야 합니다.

- 측정해야 할 CPS 측정
- CPS 측정 방법

## 측정해야 할 **CPS** 측정

최소 5일(영업일 기준) 동안 또는 측정값이 네트워크의 일반적인 트래픽 패턴을 반영한다고 확신할 때까지 평균 및 피크 CPS 트래픽을 측정합니다. 측정 기간이 길수록 측정 정확도가 높아집니다. 특별 이벤트, 분기별 이벤트 및 연례 이벤트를 고려하여 지원해야 하는 CPS 수가 급증할 수 있습니다. 방화벽에 추가 트래픽을 처리할 수 있는 용량이 있는 경우 영역 보호 프로파일을 조정하고 조정된 DoS 보호 정책 규칙을 예약하여 이러한 유형의 이벤트를 수용해야 할 수 있습니다. 다음과 같은 기준선 측정을 수행합니다.

 ©2023 Palo Alto Networks, Inc.

- 영역 보호 프로파일의 경우 각 영역에 진입하는 평균 및 피크 CPS를 측정합니다.
- 총계 DoS 보호 프로파일의 경우 보호하려는 각 디바이스 그룹에 대해 결합된 평균 및 피크 CPS를 측정합니다.
- 분류된 DoS 보호 프로파일의 경우 보호하려는 개별 디바이스의 평균 및 최대 CPS를 측정합니다.

또한 방화벽의 용량과 복호화과 같은 리소스를 많이 사용하는 다른 기능이 각 방화벽에서 제어할 수 있는 연결 수에 어떤 영향을 미치는지 이해합니다. 일반적으로 방화벽이 경계에 가까울수록 더 많은 트래픽을 처리하기 때문에 용량이 커져야 합니다. 각 방화벽 모델의 데이터시트에는 방화벽이 지원하는 총 새 CPS(초당 세션 수)가 포함되어 있으며, 방화벽 비교 도구를 사용하여 여러 방화벽 모델의 CPS(및 기타 지표)를 비교할 수 있습니다.

## CPS 측정 방법

CPS를 측정하는 방법에는 여러 가지가 있습니다.

- Panorama를 사용하여 방화벽을 관리하는 경우 Device Monitoring을 사용하여 방화벽으로 들어오는 CPS를 측정합니다(**Panorama** > **Managed Devices** > **Health** > 모든 디바이스). 디바이스 모니터링은 또한 각 방화벽의 일반적인 사용 가능한 용량을 이해하는 데 도움이 되도록 CPU 평균 및 최대 사용에 따른 90일 추세선을 표시할 수 있습니다.
- 운영 CLI 명령 **show session info**를 실행합니다.

  작동 *CLI* 명령 ***show counter interface***는 실제 *CPS* 값의 두 배를 표시합니다. 이 명령을 사용할 경우 *CPS* 값을 *2*로 나누어 실제 *CPS* 값을 도출합니다.
- 적절한 DoS 방어 프로파일 임계값을 설정하려면 애플리케이션 팀과 협력하여 해당 서버에 대한 정상 및 최대 CPS와 해당 서버가 지원할 수 있는 최대 CPS를 이해하십시오.

  또한 보호하려는 중요 디바이스의 대상 IP 주소에 대한 방화벽 트래픽 로그 및 위협 로그를 필터링하여 정상 및 최대 세션 활동 정보를 얻을 수 있습니다.
- Wireshark 또는 NetFlow와 같은 타사 도구를 사용하여 네트워크 트래픽을 수집하고 분석합니다.
- 스크립트를 사용하여 CPS 정보 수집 및 지속적인 모니터링을 자동화하고 로그에서 정보를 마이닝합니다.
- 세션 종료 시 기록을 하도록 방화벽의 모든 보안 정책 규칙을 구성합니다. NetFlow 또는 Wireshark와 같은 모니터링 도구가 없고 자동화된 스크립트를 얻거나 개발할 수 없는 경우 세션 종료 시 기록은 세션 종료 시 연결 수를 캡처합니다. 이것은 CPS 정보를 제공하지 않지만 선택한 기간에 종료되는 세션 수를 표시하며 해당 정보에서 대략적인 초당 세션 수를 계산할 수 있습니다.

  리소스를 절약하기 위해 방화벽은 *10*초 인터벌으로 총 *CPS*를 측정합니다. 이러한 이유로 방화벽에 표시되는 측정값은 *10*초 인터벌 내에서 버스트*(burst)*를 포착하지 못할 수 있습니다. 평균 *CPS* 측정값은 영향을 받지 않지만 최대 *CPS* 측정값은 정확하지 않을 수 있습니다. 예를 들어 방화벽 로그가 *10*초 인터벌으로 평균 *5,000CPS*를 보고하는 경우 *4,000CPS*가 *1*초 버스트에서 발생하고 나머지 *1,000CPS*가 나머지 *9*초 동안 분산되었을 수 있습니다.

시간 경과에 따른 기록 CPS 데이터를 수집하기 위해 SNMP 서버를 사용하는 경우 자체 관리 도구를 사용하여 SNMP MIB를 폴링할 수 있습니다. 그러나 MIB의 CPS 측정값이 실제 CPS 값의 두 배를 표시한다는 점을 이해하는 것이 중요합니다(예: 실제 CPS 측정값이 10,000인 경우 MIB는 값으로 20,000을 표시함). 여전히 MIB의 추세를 볼 수 있으며 CPS 값을 2로 나누어 실제 값을 얻을 수 있습니다. SNMP MIB

 ©2023 Palo Alto Networks, Inc.

OID는 다음과 같습니다. PanZoneActiveTcpCps, PanZoneActiveUdpCps 및 PanZoneOtherIpCps. 방화벽은 10초마다 SNMP 서버를 측정하고 업데이트하기만 하므로 10초마다 폴링합니다.

또한, 적절한 관리자가 플러드(잠재적 DoS 공격) 이벤트만 포함하는 이메일을 수신할 수 있도록 플러드 이벤트에 대한 별도의 로그 포워딩 프로파일을 생성합니다. 영역 보호 및 DoS 방어 임계값 이벤트 모두에 대해 로그 포워딩을 설정합니다.

영역 및 ***DoS*** 방어를 구현한 후 이러한 방법을 사용하여 배포를 모니터링하여 네트워크가 발전하고 트래픽 패턴이 변경됨에 따라 플러드 방지 임계값을 조정할 수 있습니다.

## 영역 보호 프로파일

각 영역에 영역 보호 프로파일을 적용하여 수신 영역으로 들어오는 집계 트래픽을 기반으로 방어합니다.

영역 보호 및 ***DoS*** 방어를 구성하는 것 외에도 모범 사례 Vulnerability Protection 프로파일을 각 보안 정책 규칙에 적용하여 ***DoS*** 공격을 방어할 수 있습니다.

- 플러드 방지
- 정찰 보호
- 패킷 기반 공격 보호
- 프로토콜 보호
- 이더넷 SGT 보호

### 플러드 방지

플러드 보호가 구성된 영역 보호 프로파일은 SYN, ICMP, ICMPv6, UDP 및 기타 IP 플러드 공격으로부터 전체 수신 영역을 방어합니다. 방화벽은 새 CPS(초당 연결 수)로 영역에 들어가는 각 플러드 유형의 총량을 측정하고 합계를 영역 보호 프로파일에서 구성한 임계값과 비교합니다. (DoS 방어 프로파일 및 정책 규칙을 사용하여 영역 내에서 중요한 개별 디바이스를 보호합니다.)

방화벽 데이터플레인 ***CPU*** 사용량을 측정하고 모니터링하여 각 방화벽이 ***DoS*** 및 ***Zone Protection*** 및 복호화와 같이 ***CPU*** 주기를 소비하는 기타 기능을 지원할 수 있도록 크기가 적절한지 확인합니다. ***Panorama***를 사용하여 방화벽을 관리하는 경우 디바이스 모니터링(***Panorama*** > 관리 디바이스 > 상태 > 모든 디바이스)에 관리되는 각 방화벽의 ***CPU*** 및 메모리 사용량이 표시됩니다. 또한 ***CPU*** 평균 및 피크 사용량에 대한 ***90***일 추세선을 보여 주어 각 방화벽의 일반적인 가용 용량을 파악할 수 있습니다.

각 플러드 유형에 대해 영역에 진입하는 새 CPS에 대해 세 가지 임계값을 설정하고 SYN 플러드에 대한 삭제 작업을 설정할 수 있습니다. 영역에 대한 기준 CPS 비율을 알고 있는 경우 이 지침을 사용하여 초기 임계값을 설정한 다음 필요에 따라 임계값을 모니터링하고 조정합니다.

- 경보 비율 - 경보를 트리거할 새 CPS 임계값입니다. 경보 비율을 영역의 평균 CPS 비율보다 15-20% 높게 설정하여 정상적인 변동으로 인해 경고가 발생하지 않도록 하는 것을 목표로 합니다.
- 활성화 - 플러드 방지 메커니즘을 활성화하고 새 연결을 끊기 시작하는 새 CPS 임계값입니다. ICMP, ICMPv6, UDP 및 기타 IP 플러드의 경우 보호 메커니즘은 Random Early Drop(RED, Random Early Detection이라고도 함)입니다. SYN 플러드의 경우에만 삭제 작업을 SYN 쿠키 또는 RED로 설정할 수


©2023 Palo Alto Networks, Inc.

있습니다. 잠재적 플러드 완화를 시작하기 위해 영역에 대한 최고 CPS 속도 바로 위에 활성화 속도를 설정하는 대상입니다.

- 최대 - RED가 보호 메커니즘일 때 수신 패킷을 삭제하는 초당 연결 수입니다. 방화벽 리소스를 소비하는 다른 기능을 고려하여 최대 속도를 방화벽 용량의 약 80-90%로 설정하는 것을 목표로 합니다.

영역에 대한 기준 CPS 비율을 모르는 경우 최대 CPS 비율을 방화벽 용량의 약 80-90%로 설정하고 이를 사용하여 합리적인 플러드 완화 경보 및 활성화 비율을 도출합니다. 최대 비율을 기준으로 경보 비율과 활성화 비율을 설정합니다. 예를 들어 경보 비율을 최대 비율의 절반으로 설정하고 수신한 경보 수와 사용 중인 방화벽 리소스에 따라 조정할 수 있습니다. 연결을 끊기 시작하므로 활성화 속도를 신중하게 설정하십시오. 정상적인 트래픽 부하에는 약간의 변동이 발생하므로 연결을 너무 적극적으로 끊지 않는 것이 가장 좋습니다. 높은 편에서 오류를 범하고 방화벽 리소스가 영향을 받는 경우 속도를 조정하십시오.

*SYN* 플러드 프로텍션은 드롭 액션을 설정하는 유일한 유형입니다. 먼저 작업을 ***SYN*** 쿠키로 설정합니다. *SYN* 쿠키는 합법적인 트래픽을 공정하게 처리하고 *SYN* 핸드쉐이크에 실패한 트래픽만 삭제합니다. 반면 *Random Early Drop*을 사용하면 트래픽이 무작위로 삭제되므로 *RED*가 합법적인 트래픽에 영향을 줄 수 있습니다. 그러나 *SYN* 쿠키는 방화벽이 대상 서버에 대한 프록시 역할을 하고 서버에 대한 *3*방향 핸드쉐이크를 처리하기 때문에 리소스를 많이 사용합니다. 합법적인 트래픽*(SYN* 쿠키*)*을 삭제하지 않고 방화벽 리소스를 보존하는 것*(RED)*이 절충되는 것이 아닙니다. 방화벽을 모니터링하고 *SYN* 쿠키가 너무 많은 리소스를 사용하는 경우 *RED*로 전환합니다. 방화벽 앞에 전용 *DDoS* 방지 디바이스가 없는 경우 항상 *RED*를 드롭 메커니즘으로 사용하십시오.

***SYN*** 쿠키가 활성화되면 방화벽은 *SYN/ACK*를 프록시할 때 이러한 값을 알지 못하기 때문에 서버가 보내는 *TCP* 옵션을 고려하지 않습니다. 따라서 *TCP* 핸드쉐이크 중에는 *TCP* 서버의 창 크기 및 *MSS* 값과 같은 값을 협상할 수 없으며 방화벽은 자체 기본값을 사용합니다. 서버 경로의 *MSS*가 방화벽의 기본 *MSS* 값보다 작은 시나리오에서는 패킷을 조각화해야 합니다.

영역 보호 프로파일을 활성화해도 정상적인 트래픽이 예기치 않게 삭제되지 않도록 기본 임계값이 높습니다. 네트워크 트래픽에 적절한 값으로 임계값을 조정합니다. 합리적인 플러드 임계값을 설정하는 방법을 이해하는 가장 좋은 방법은 각 플러드 유형에 대한 평균 및 최대 CPS의 기준 측정을 수행하여 각 영역의 정상적인 트래픽 조건을 결정하고 복호화 기능 등 다른 리소스의 영향을 포함하여 방화벽의 용량을 이해하는 것입니다. 필요에 따라 그리고 네트워크가 발전함에 따라 플러드 임계값을 모니터링하고 조정합니다.

여러 *DP(*데이터플레인 프로세서*)*가 있는 방화벽은 *DP* 간에 연결을 분산합니다. 일반적으로 방화벽은 *CPS* 임계값 설정을 *DP* 간에 균등하게 나눕니다. 예를 들어 방화벽에 *5*개의 *DP*가 있고 경보 속도를 *20,000CPS*로 설정한 경우 각 *DP*의 경보 속도는 *4,000CPS(20,000/ 5 = 4,000)*이므로 *DP*의 새 세션이 *4,000*을 초과하면 해당 *DP*에 대한 경보 비율 임계값이 트리거됩니다.

## 정찰 보호

정찰의 군사 정의와 마찬가지로, 정찰의 네트워크 보안 정의는 공격자가 비밀리에 약점을 찾기 위해 네트워크를 조사하여 네트워크의 취약점에 대한 정보를 얻으려고 할 때입니다. 정찰 활동은 종종 네트워크 공격의 예고입니다. 모든 구역에서 정찰 보호를 활성화하여 포트 스캔 및 호스트 스윕을 방어합니다.

 ©2023 Palo Alto Networks, Inc.

- 포트 스캔은 네트워크에서 열린 포트를 발견합니다. 포트 검색 도구는 클라이언트 요청을 호스트의 포트 번호 범위로 전송하며 공격에서 악용할 활성 포트를 찾는 것을 목표로 합니다. 영역 보호 프로파일은 TCP 및 UDP 포트 스캔을 방어합니다.
- 호스트 스윕은 여러 호스트를 검사하여 특정 포트가 열려 있고 취약한지 확인합니다.

네트워크 보안의 펜 테스트 또는 방화벽의 강도와 같은 합법적인 목적을 위해 정찰 도구를 사용할 수 있습니다. 내부 IT 부서에서 네트워크 취약점을 찾아 수정하기 위해 펜 테스트를 수행할 수 있도록 최대 20개의 IP 주소 또는 넷마스크(netmask) 주소 개체를 정찰 보호에서 제외하도록 지정할 수 있습니다.

정찰 보호 구성을(를) 할 때 정찰 트래픽(펜 테스트 트래픽 제외)이 구성된 임계값을 초과할 때 수행할 작업을 설정할 수 있습니다. 정찰 작업을 차단하기 전에 분석을 위해 몇 패킷을 기록하려면 기본 인터벌 및 임계값을 유지합니다.

## 패킷 기반 공격 보호

패킷 기반 공격은 다양한 형태를 취합니다. 영역 보호 프로파일은 IP, TCP, ICMP, IPv6 및 ICMPv6 패킷 헤더를 확인하고 다음을 통해 영역을 보호합니다.

- 바람직하지 않은 특성을 가진 패킷 삭제.
- 패킷을 영역에 허용하기 전에 패킷에서 바람직하지 않은 옵션을 제거합니다.

패킷 기반 공격 보호 구성일 때 각 패킷 유형에 대한 드롭 특성을 선택합니다. 각 IP 프로토콜에 대한 모범 사례는 다음과 같습니다.

- **IP** 삭제 - 알 수 없고 형식이 잘못된 패킷을 삭제합니다. 또한 **Strict Source Routing** 및 **Loose Source Routing**을 삭제하십시오. 이러한 옵션을 허용하면 공격자가 대상 IP 주소를 일치 기준으로 사용하는 보안 정책 규칙을 우회할 수 있기 때문입니다. 내부 영역의 경우에만 방화벽 라우팅 테이블과 일치하는 소스 주소를 가진 트래픽만 영역에 액세스할 수 있도록 스푸핑된 **IP** 주소를 선택합니다.
- **TCP** 삭제 - 데이터가 있는 기본 **TCP SYN** 및 데이터가 있는 **TCP SYNACK**을 유지하고 일치하지 않는 중복 **TCP** 세그먼트 및 분할 핸드쉐이크 패킷을 삭제하고 패킷에서 **TCP** 타임스탬프를 제거합니다.

  세션 재일치(디바이스 > 설정 > 세션 > 세션 설정)를 활성화하는 것은 커밋된 새로 구성되거나 편집된 보안 정책 규칙을 기존 세션에 적용하는 모범 사례입니다. 그러나 영역에서 터널 콘텐츠 검사를 구성하고 세션 재매칭이 활성화된 경우 ***Non-SYN TCP*** 거부도 비활성화해야 합니다(선택 항목을 전역에서 아니오로 변경). 그렇지 않으면 터널 콘텐츠 검사 정책을 활성화하거나 편집할 때 방화벽은 모든 기존 터널 세션을 삭제합니다. *Tunnel Content Inspection* 정책이 있는 영역에서만 ***Rematch Sessions***를 활성화한 경우에만 ***Reject Non-SYN TCP***를 비활성화하려면 별도의 *Zone Protection* 프로파일을 만듭니다.
- **ICMP** 삭제 - ICMP 패킷 삭제는 ICMP 사용 방식(또는 ICMP 사용 여부)에 따라 달라지므로 표준 모범 사례 설정이 없습니다. 예를 들어 핑(ping) 활동을 차단하려는 경우 **ICMP Ping ID 0**을 차단할 수 있습니다.
- **IPv6** 삭제 - 규정 준수가 중요한 경우 방화벽이 비준수 라우팅 헤더, 확장 등이 있는 패킷을 삭제하는지 확인합니다.
- **ICMPv6** 삭제 - 규정 준수가 중요한 경우 패킷이 보안 정책 규칙과 일치하지 않으면 방화벽이 특정 패킷을 삭제하도록 합니다.


©2023 Palo Alto Networks, Inc.

## 프로토콜 보호

영역 보호 프로파일에서 프로토콜 보호는 비 IP 프로토콜 기반 공격을 방어합니다. 프로토콜 보호를 활성화하여 레이어 2 VLAN 또는 가상 와이어의 보안 영역 간 또는 레이어 2 VLAN의 단일 영역 내 인터페이스 간에 비 IP 프로토콜을 차단하거나 허용합니다(레이어 3 인터페이스 및 영역이 비IP 프로토콜을 삭제하므로 비 IP 프로토콜 보호가 적용되지 않음). 프로토콜 보호 구성 보안 수준이 낮은 프로토콜이 영역 또는 영역의 인터페이스에 들어가는 것을 방지하여 보안 위험을 줄이고 규정 준수를 촉진합니다.

동일한 영역에 있는 비 ***IP*** 프로토콜이 한 레이어 ***2*** 인터페이스에서 다른 레이어으로 이동하는 것을 방지하는 영역 보호 프로파일을 구성하지 않으면 기본 영역 내 허용 보안 정책 규칙으로 인해 방화벽이 트래픽을 허용합니다. 다른 영역 인터페이스를 통해 연결할 수 있는 네트워크 검색을 방지하기 위해 영역 내에서 LLDP와 같은 프로토콜을 차단하는 영역 보호 프로파일을 만들 수 있습니다.

네트워크에서 실행 중인 비IP 프로토콜을 검색해야 하는 경우 NetFlow, Wireshark 또는 기타 타사 도구와 같은 모니터링 도구를 사용하여 네트워크에서 비 IP 프로토콜을 검색합니다. 차단하거나 허용할 수 있는 비 IP 프로토콜의 예로는 LLDP, NetBEUI, 스패닝 트리, GOOSE(Generic Object Oriented Substation Event)와 같은 SCADA(Supervisory Control and Data Acquisition) 시스템 등이 있습니다.

영역에 대한 프로토콜 보호를 구성하려면 제외 목록 또는 포함 목록을 만드십시오. 제외 목록은 차단 목록입니다. 방화벽은 제외 목록에 있는 모든 프로토콜을 차단하고 다른 모든 프로토콜을 허용합니다. 포함 목록은 허용 목록입니다. 방화벽은 목록에서 지정한 프로토콜만 허용하고 다른 모든 프로토콜은 차단합니다.

제외 목록 대신 프로토콜 보호에 포함 목록을 사용하십시오. 포함 목록은 허용하려는 프로토콜만 승인하고 필요하지 않거나 네트워크에 있는지 몰랐던 프로토콜을 차단하여 공격 면적을 줄이고 알 수 없는 트래픽을 차단합니다.

목록은 최대 64개의 Ethertype 항목을 지원하며 각각은 IEEE 16진수 Ethertype 코드로 식별됩니다. Ethertype 코드의 다른 소스는 standard.ieee.org/develop/regauth/ethertype/eth.txt 및 http://www.cavebear.com/archive/cavebear/Ethernet/type.html입니다. AE(Aggregated Ethernet) 인터페이스가 있는 영역에서 비 IP 프로토콜에 대한 영역 보호를 구성할 때 AE 인터페이스 구성원은 그룹으로 취급되기 때문에 하나의 AE 인터페이스 구성원에서만 비 IP 프로토콜을 차단하거나 허용할 수 없습니다.

프로토콜 보호는 ***IPv4(Ethertype 0x0800), IPv6(0x86DD), ARP(0x0806)*** 또는 ***VLAN*** 태그가 지정된 프레임***(0x8100)*** 차단을 허용하지 않습니다. 방화벽은 명시적으로 나열하지 않고 제외 목록에 추가하는 것을 허용하지 않는 경우에도 포함 목록에서 이러한 네 가지 ***Ethertype***을 항상 암시적으로 허용합니다.

## 이더넷 **SGT** 보호

Cisco TrustSec 네트워크에서 ISE(Cisco ID 서비스 엔진)는 사용자 또는 엔드포인트 세션에 16비트의 레이어 2 보안 그룹 태그(SGT)를 할당합니다. 방화벽이 Cisco TrustSec 네트워크의 일부인 경우 이더넷 SGT 보호를 사용하여 영역 보호 프로파일을 만들 수 있습니다. 방화벽은 802.1Q(이더타입 0x8909)가 있는 헤더를 검사하여 특정 Layer 2 보안 그룹 태그(SGT) 값에 대해 검사하고, SGT가 인터페이스에 연결된 영역 보호 프로파일에 대해 구성한 목록과 일치하는 경우 패킷을 삭제할 수 있습니다. 영역에 대한 액세스를 거부할 SGT 값을 결정합니다.

 ©2023 Palo Alto Networks, Inc.

# 패킷 버퍼 보호

패킷 버퍼 보호는 방화벽의 패킷 버퍼를 압도하여 합법적인 트래픽이 손실될 수 있는 단일 세션 DoS 공격으로부터 방화벽과 네트워크를 보호합니다. 영역 보호 프로파일이나 DoS 방어 프로파일 또는 정책 규칙에서 패킷 버퍼 보호를 구성하지는 않지만 패킷 버퍼 보호는 수신 영역을 보호합니다. 영역 및 DoS 방어는 새 세션(연결)에 적용되고 세분화되지만 패킷 버퍼 보호는 기존 세션에 적용되며 전역적입니다.

전체 방화벽을 보호하기 위해 전역적으로 패킷 버퍼 보호 구성을(를) 하고 각 영역에서 패킷 버퍼 보호를 활성화하여 영역을 보호합니다.

- 글로벌 패킷 버퍼 보호 - 방화벽은 패킷 버퍼 보호가 영역에서 사용되는지의 여부와 관계없이 모든 영역의 세션과 해당 세션이 패킷 버퍼를 사용하는 방법을 모니터링합니다. 방화벽을 보호하고 개별 영역에서 방화벽을 사용하도록 설정하려면 패킷 버퍼 보호를 전역적으로 구성(디바이스 > 설정 > 세션 설정) 해야 합니다. 패킷 버퍼 소비가 구성된 활성화 비율에 도달하면 방화벽은 Random Eararly Drop(RED)을 사용하여 문제가 있는 세션에서 패킷을 삭제합니다(방화벽이 전역 수준에서 전체 세션을 삭제하지 않음).
- 영역별 패킷 버퍼 보호 - 각 영역(네트워크 > 영역)에서 패킷 버퍼 보호를 두 번째 보호 수준으로 계층화하도록 설정합니다. 패킷 버퍼 소비가 활성화 임계값을 초과하고 전역 보호가 세션 트래픽에 RED가 적용되기 시작하면 차단 대기 시간 타이머가 시작됩니다. 차단 대기 시간은 방화벽이 전체 세션을 차단하기 전에 문제가 있는 세션이 계속될 수 있는 시간(초)입니다. 위반 세션은 차단 기간이 만료될 때까지 차단된 상태로 유지됩니다.

> 패킷 버퍼 보호를 영역에서 활성화하려면 패킷 버퍼 보호를 전역적으로 활성화해야 합니다.

패킷 버퍼 보호에는 두 가지 유형이 있습니다.

- 버퍼 사용률에 따른 패킷 버퍼 보호
- 대기 시간 기반 패킷 버퍼 보호

### 버퍼 사용률에 따른 패킷 버퍼 보호

버퍼 사용률을 기반으로 하는 패킷 버퍼 보호는 기본적으로 사용하도록 설정되어 있습니다. 일정 기간(영업일 기준 1주 이상) 동안 방화벽 패킷 버퍼 사용률을 기준으로 측정하지만 측정 기간이 길수록 기준선이 향상되어 일반적인 사용량을 파악할 수 있습니다.

지정된 기간 동안의 패킷 버퍼 사용률을 보려면(또는 패킷 버퍼의 2% 이상을 사용하는 상위 5개 세션을 보려면) 운영 CLI 명령을 사용하십시오.

```
admin1138@thxvm1>show running resource-monitor [ 하루 | 시간 | 수신 백로그 | 분 | 두 번째 | 주]
```

CLI 명령은 지정된 기간 동안의 버퍼 사용률에 대한 스냅샷을 제공하지만 자동화되거나 연속적이지 않습니다. 동작 및 비정상적인 이벤트의 변화를 모니터링할 수 있도록 연속 패킷 버퍼 사용률 측정을 자동화하려면 스크립트를 사용합니다. Palo Alto Networks 계정 팀은 자체 스크립트를 개발하기 위해 수정할 수 있는 샘플 스크립트를 제공할 수 있습니다. 하지만 스크립트는 공식적으로 지원되지 않으며 스크립트 사용 또는 수정에 대한 기술 지원이 제공되지 않습니다.

기준선 측정에 비정상적으로 높은 패킷 버퍼 사용률이 일관되게 나타나는 경우 방화벽의 용량은 일반적인 트래픽 로드에 비해 크기가 작아질 수 있습니다. 이 경우 방화벽 배포의 크기를 조정하는 것이 좋습니다.


©2023 Palo Alto Networks, Inc.

그렇지 않으면 패킷 버퍼 보호 임계값을 신중하게 조정하여 영향을 받는 버퍼가 넘치지 않도록 하고 합법적인 트래픽이 손실되는 것을 방지해야 합니다. 방화벽 크기가 배포에 적합한 경우 공격만 버퍼 사용량이 급증할 수 있습니다.

방화벽 패킷 버퍼를 초과하면 방화벽의 패킷 포워딩 기능에 부정적인 영향을 미칩니다. 버퍼가 가득 차면 공격이 발생한 인터페이스뿐만 아니라 어떤 인터페이스에서도 패킷이 방화벽에 들어갈 수 없습니다.

임계값을 설정하는 모범 사례는 다음과 같습니다.

- 경고 및 활성화 - 기본 임계값으로 시작하고, 패킷 버퍼 사용률을 모니터링하고, 필요에 따라 임계값을 조정합니다. 경고 임계값은 기본적으로 50%입니다. 패킷 버퍼 사용률이 10초 이상 임계값을 초과하면 방화벽이 1분마다 시스템 로그에 경고 항목을 생성합니다. 활성화 임계값은 기본적으로 80% 입니다. 임계값에 도달하면 방화벽이 가장 악의적인 세션을 완화하기 시작합니다. 방화벽의 크기가 올바르면 버퍼 사용률이 50% 미만이어야 합니다.
- 차단 대기 시간 - 패킷 버퍼 사용률이 활성화 임계값을 트리거할 때 차단 대기 시간은 방화벽이 세션을 차단하기 전에 문제가 있는 세션이 계속될 수 있는 시간을 설정합니다. 차단 대기 시간 동안 방화벽은 문제가 있는 세션의 패킷에 계속해서 RED가 적용됩니다. 기본 차단 보류 시간 임계값(60초)으로 시작하여 패킷 버퍼 사용률을 모니터링하고 필요에 따라 임계값을 조정합니다. 차단 대기 시간이 만료되기 전에 패킷 버퍼 사용률이 활성화 임계값 아래로 떨어지면 활성화 임계값을 다시 초과할 때까지 타이머가 재설정되고 시작되지 않습니다. 차단 대기 시간을 늘리면 위반 세션에 더 큰 페널티를 부과하고 위반 세션에 더 적은 페널티를 부과합니다.
- 차단 기간 - 차단 대기 시간이 만료되면 방화벽은 차단 기간으로 정의된 기간 동안 문제가 되는 세션을 차단합니다. 기본 임계값(3600초)으로 시작하고 패킷 버퍼 사용률을 모니터링한 다음 필요에 따라 임계값을 조정합니다. 영역에서 패킷 버퍼 보호를 사용하도록 설정하면 IP 주소의 세션 하나만 패킷 버퍼를 과도하게 사용하더라도 차단 기간은 IP 주소의 모든 세션에 영향을 줍니다. 한 시간(3600초) 동안 IP 주소를 차단하는 것이 과도한 페널티라고 생각되면 차단 기간을 허용 가능한 값으로 줄입니다.

패킷 버퍼 보호는 개별 세션의 버퍼 사용률을 모니터링하는 것 외에도 특정 조건이 충족되면 IP 주소를 차단할 수도 있습니다. 방화벽이 패킷 버퍼를 모니터링하는 동안 개별적으로는 공격으로 간주되지 않는 세션을 빠르게 생성하는 소스 IP 주소를 감지하면 구성된 차단 기간 동안 해당 IP 주소를 차단합니다.

NAT(네트워크 주소 변환)(소스 *NAT*를 사용하여 인터넷 바운드 트래픽을 변환한 외부 소스)는 *IP* 주소 변환 작업으로 인해 패킷 버퍼 사용률이 높아질 수 있습니다. 이 경우 개별 세션에 불이익을 주지만 기본 *IP* 주소에 불이익을 주지 않는 방식으로 임계값을 조정하십시오(동일한 *IP* 주소의 다른 세션에는 영향을 주지 않음). 이렇게 하려면 차단 대기 시간을 줄여 방화벽이 버퍼를 과도하게 사용하는 개별 세션을 더 빠르게 차단하고 기본 *IP* 주소에 과도한 불이익이 발생하지 않도록 차단 지속 시간을 줄입니다.

### 대기 시간 기반 패킷 버퍼 보호

사용률을 기반으로 하는 패킷 버퍼 보호 대신 데이터플레인 패킷 버퍼링으로 인한 패킷 지연 시간을 기반으로 패킷 버퍼 보호를 트리거할 수 있으며 이는 방화벽의 혼잡을 나타냅니다. 이러한 패킷 버퍼 보호는 혼잡에 대해 경고하고 패킷에서 임의 조기 삭제(RED)를 수행하여 Head-of-Line 차단을 완화합니다. 지연 시간에 따른 패킷 버퍼 보호는 지연 시간에 민감한 프로토콜이나 애플리케이션이 영향을 받기 전에 보호를 트리거할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

트래픽에 지연 시간에 민감한 프로토콜이나 애플리케이션이 포함되어 있는 경우 지연 시간을 기반으로 하는 패킷 버퍼 보호가 버퍼 사용률을 기반으로 하는 패킷 버퍼 보호보다 유용합니다.

대기 시간을 기준으로 한 패킷 버퍼 보호에는 방화벽이 경보 로그 이벤트를 생성하기 시작하는 지연 시간 경고 임계값(밀리초)을 설정하는 것이 포함됩니다. 지연 시간 활성화 임계값은 방화벽이 들어오는 패킷에서 RED를 활성화하고 활성화 로그 생성을 시작하는 시기를 나타냅니다. 지연 시간 최대 허용 임계값은 방화벽이 거의 100%의 드롭 확률로 RED와 함께 사용하는 경우를 나타냅니다.

차단 보류 시간 및 차단 지속 시간 설정은 사용률에 기반한 패킷 버퍼 보호와 동일한 방식으로 대기 시간을 기준으로 패킷 버퍼 보호를 위해 작동합니다.

# DoS 보호 프로파일 및 정책 규칙

DoS 방어 프로파일과 DoS 방어 정책 규칙이 결합되어 세션 플러드로부터 중요 리소스 및 개별 중요 리소스의 특정 그룹을 보호합니다. 플러드 공격으로부터 전체 영역을 보호하는 Zone Protection 프로파일과 비교할 때 DoS 방어는 특정 시스템, 특히 사용자가 인터넷에서 액세스하는 중요한 시스템을 세부적으로 방어하며 웹 서버 및 데이터베이스 서버와 같은 공격 대상인 경우가 많습니다. 영역 보호 프로파일만 적용하는 경우 총 CPS(초당 연결 수)가 영역의 활성화 및 최대 속도를 초과하지 않으면 영역의 특정 시스템을 대상으로 하는 DoS 공격이 성공할 수 있기 때문에 두 가지 보호 유형을 모두 적용합니다.

DoS 방어는 리소스를 많이 사용하므로 중요한 시스템에만 사용하십시오. 영역 보호 프로파일과 마찬가지로 DoS 방어 프로파일은 플러드 임계값을 지정합니다. DoS 방어 정책 규칙은 DoS 프로파일이 적용되는 디바이스, 사용자, 영역 및 서비스를 결정합니다.

***DoS*** 방어 및 영역 보호를 구성하는 것 외에도 각 보안 정책 규칙에 모범 사례 취약점 보호 프로파일을 적용하여 ***DoS*** 공격을 방어합니다**.**

- 분류 및 종합 DoS 보호
- DoS 보호 프로파일
- DoS 보호 정책 규칙

## 분류 및 종합 **DoS** 보호

DoS 보호를 구성할 때 집계 및 분류 DoS 보호 프로파일를 구성하고 하나의 프로파일 또는 각 프로파일 유형 중 하나를 DoS 보호 정책 규칙에 적용할 수 있습니다.

- 집계 - 각 개별 디바이스 대신 DoS 보호 정책 규칙에 지정된 전체 디바이스 그룹에 적용되는 임계값을 설정하여 한 디바이스가 허용된 연결 트래픽의 대부분을 수신할 수 있도록 합니다. 예를 들어 최대 속도가 20,000CPS이면 그룹의 총 CPS가 20,000개이고 다른 디바이스에 연결되어 있지 않으면 개별 디바이스는 최대 20,000CPS를 수신할 수 있습니다. 집계 DoS 보호 정책은 특정 서브넷, 사용자 또는 서비스에 추가 제약 조건을 적용하고자 할 때 특정 중요 디바이스 그룹에 대해 또 다른 광범위한 보호 레이어를 제공합니다(인터넷 경계에 있는 전용 DDoS 디바이스 및 영역 보호 프로파일 이후).
- 분류됨 - DoS 보호 정책 규칙에 지정된 각 개별 디바이스에 적용되는 플러드 임계값을 설정합니다. 예를 들어 최대 속도를 5,000CPS로 설정한 경우 규칙에 지정된 각 디바이스는 새 연결을 끊기 전에 최대 5,000CPS를 허용할 수 있습니다. 분류된 DoS 보호 정책 규칙을 둘 이상의 디바이스에 적용하는 경우

 ©2023 Palo Alto Networks, Inc.

분류된 임계값이 각 개별 디바이스에 적용되므로 규칙이 적용되는 디바이스는 용량 및 CPS 비율을 제어하는 방식과 유사해야 합니다. 분류된 프로파일은 중요한 개별 리소스를 보호합니다.

분류된 DoS 보호 프로파일(옵션/보호 > 분류 > 주소)로 DoS 보호 정책 규칙을 구성할 때 주소 필드는 수신 연결이 **source-ip-only**, **destination-ip-only** 또는 **scr- dest-ip-both**(방화벽은 소스 및 대상 IP 주소가 임계값과 일치하는 것으로 계산함). 카운터는 리소스를 소비하므로 주소 일치 횟수를 계산하는 방식이 방화벽 리소스 소비에 영향을 줍니다. 분류된 DoS 보호를 사용하여 다음을 수행할 수 있습니다

- 중요한 개별 디바이스, 특히 사용자가 인터넷에서 액세스하며 웹 서버, 데이터베이스 서버 및 DNS 서버와 같은 공격 대상인 서버를 보호합니다. 분류된 DoS 보호 프로파일에서 적절한 플러드 및 리소스 보호 임계값을 설정합니다. IP 주소를 규칙의 대상 조건으로 추가하여 프로파일을 각 서버의 IP 주소에 적용하는 DoS 보호 정책 규칙을 생성하고 주소를 대상-**IP**전용으로 설정합니다.

  분류된 ***DoS*** 보호 정책 규칙에서 인터넷 연결 영역에 대해 소스 ***IP*** 전용 또는 ***src-dest-ip-both*** 분류를 사용하지 마십시오. 방화벽에는 인터넷에서 가능한 모든 ***IP*** 주소에 대한 카운터를 저장할 수 있는 용량이 없기 때문입니다. 내부 영역 또는 동일 영역 규칙에 대해서만 소스 ***IP***에 대한 임계값 카운터를 증가시킵니다. 경계 영역에서는 ***destination-ip-only***를 사용합니다.

- 의심되는 호스트 또는 호스트 그룹(호스트가 포함된 영역은 인터넷에 연결할 수 없음)에 대한 CPS 속도를 모니터링합니다. 분류된 DoS 보호 프로파일에 적절한 경보 임계값을 설정하여 호스트가 비정상적으로 많은 수의 연결을 시작하는 경우 이를 알립니다. 개별 원본 또는 원본 주소 그룹에 프로파일을 적용하는 DoS 보호 정책 규칙을 생성하고 주소를 **source-ip-only**로 설정합니다. 경보를 설정하기에 충분한 새 연결을 시작하는 호스트를 조사합니다.

분류된 프로파일에 대한 주소(**source-ip-only**, **destination-ip-only** 또는 **src-dest-ip-both**)를 구성하는 방법은 DoS 보호 목표, 보호 대상 및 보호된 디바이스가 인터넷 연결 상태인지의 여부에 따라 다릅니다.

카운터가 소스 ***IP*** 주소와 대상 ***IP*** 주소 두 가지 중 하나가 아닌 모두에 대한 리소스를 소비하기 때문에 방화벽은 ***source-IP-only*** 또는 ***destination-ip-only***을 추적하는 것보다 ***src-dest-ip-both***를 주소로 추적하기 위해 더 많은 리소스를 사용합니다.

집계 프로파일과 분류된 DoS 보호 프로파일을 모두 동일한 DoS 보호 정책 규칙에 적용하면 방화벽이 집계 프로파일을 먼저 적용한 다음 필요한 경우 분류된 프로파일을 적용합니다. 예를 들어 DoS 보호 정책 규칙에서 두 가지 유형의 프로파일을 모두 사용하여 다섯 개의 웹 서버 그룹을 보호합니다. 그룹에 대한 합계가 최대 속도 25,000CPS에 도달하면 집계 프로파일 구성에서 새 연결을 끊습니다. 분류된 프로파일 구성은 최대 속도 6,000CPS에 도달하면 그룹의 개별 웹 서버에 대한 새 연결을 끊습니다. 새 연결 트래픽이 최대 속도 임계값을 초과하는 세 가지 시나리오가 있습니다.

- 새 CPS 비율이 총 최대 속도를 초과하지만 분류된 최대 속도를 초과하지 않습니다. 이 시나리오에서는 방화벽이 집계 프로파일을 적용하고 구성된 차단 기간 동안 모든 새 연결을 차단합니다.
- 새 CPS 속도는 총 최대 속도를 초과하지 않지만 웹 서버 중 하나에 대한 CPS가 분류된 최대 속도를 초과합니다. 이 시나리오에서 방화벽은 집계 프로파일을 확인하고 그룹의 속도가 25,000 CPS 미만임을 확인하므로 방화벽은 이를 기반으로 새 연결을 차단하지 않습니다. 그런 다음 방화벽은 분류된 프로파일을 확인하고 특정 서버의 속도가 6,000CPS를 초과하는지 확인합니다. 방화벽은 분류된 프로파일을 적용하고 구성된 차단 기간 동안 해당 특정 서버에 대한 새 연결을 차단합니다. 그룹의 다른 서버는 분류된 프로파일의 최대 속도 내에 있으므로 트래픽에는 영향을 주지 않습니다.
- 새 CPS 속도는 총 최대 속도를 초과하며 웹 서버 중 하나에 대해 분류된 최대 속도를 초과합니다. 이 시나리오에서 방화벽은 집계 프로파일을 확인하고 그룹의 속도가 25,000CPS를 초과한다는 것을 확인


©2023 Palo Alto Networks, Inc.

하므로 방화벽이 새 연결을 차단하여 그룹의 총 CPS를 제한합니다. 그런 다음 방화벽은 분류된 프로파일을 확인하고 특정 서버에 대한 속도가 6,000CPS를 초과하는지 확인합니다. 따라서 집계 프로파일은 그룹의 결합 제한을 적용했지만 이 특정 서버를 보호하기에는 충분하지 않았습니다. 방화벽은 분류된 프로파일을 적용하고 구성된 차단 기간 동안 해당 특정 서버에 대한 새 연결을 차단합니다. 그룹의 다른 서버는 분류된 프로파일의 최대 속도 내에 있으므로 트래픽에는 영향을 주지 않습니다.

집계 및 분류된 ***DoS*** 보호 프로파일을 모두 동일한 트래픽에 적용하려면 두 프로파일을 모두 동일한 ***DoS*** 보호 정책 규칙에 적용해야 합니다. 집계 프로파일을 하나의 규칙에 적용하고 분류된 프로파일을 다른 규칙에 적용하면 정확히 동일한 트래픽을 지정하더라도 트래픽이 첫 번째 ***DoS*** 보호 정책 규칙과 일치할 때 방화벽이 실행되기 때문에 방화벽은 하나의 프로파일만 적용할 수 있습니다. 해당 규칙에 지정된 작업 및 후속 규칙에 대한 트래픽과 비교하지 않으므로 트래픽이 두 번째 규칙과 일치하지 않으며 방화벽이 해당 작업을 적용할 수 없습니다. *(*이는 보안 정책 규칙이 작동하는 방식과 동일합니다.*)*

## DoS 보호 프로파일

DoS 방어 프로파일은 새로운 세션 IP 플러드 공격으로부터 보호하고 리소스 보호(지정된 엔드포인트 및 리소스에 대한 최대 동시 세션 제한)를 제공하는 임계값을 설정합니다. DoS 방어 프로파일은 SYN, UDP, ICMP, ICMPv6 및 기타 IP 플러드 공격으로부터 특정 디바이스(분류된 프로파일) 및 디바이스 그룹(집계 프로파일)을 보호합니다. DoS 방어 프로파일에서 플러드 방지 임계값을 구성하는 것은 영역 보호 프로파일에서 플러드 방지을(를) 구성하는 것과 유사하지만 영역 보호 프로파일은 전체 수신 영역을 보호하는 반면 DoS 방어 프로파일과 정책 규칙은 세분화되고 대상이 지정되며 단일 디바이스(IP 주소)로 분류됩니다. 방화벽은 디바이스 그룹(집계 프로파일)에 대한 총 CPS(초당 연결 수)를 측정하거나 개별 디바이스(분류된 프로파일)에 대한 CPS를 측정합니다.

방화벽 데이터플레인 ***CPU*** 사용량을 측정하고 모니터링하여 각 방화벽이 ***DoS*** 및 ***Zone Protection*** 및 복호화와 같이 ***CPU*** 주기를 소비하는 기타 기능을 지원할 수 있도록 크기가 적절한지 확인합니다. ***Panorama***를 사용하여 방화벽을 관리하는 경우 디바이스 모니터링(***Panorama*** > 관리 디바이스 > 상태 > 모든 디바이스)에 관리되는 각 방화벽의 ***CPU*** 및 메모리 사용량이 표시됩니다. 또한 ***CPU*** 평균 및 피크 사용량에 대한 ***90***일 추세선을 보여 주어 각 방화벽의 일반적인 가용 용량을 파악할 수 있습니다.

각 플러드 유형에 대해 새 CPS에 대한 세 가지 임계값을 디바이스 그룹(집계) 또는 개별 디바이스(분류됨) 및 차단 기간으로 설정하고 SYN 플러드에 대한 삭제 작업을 설정할 수 있습니다.

- 경보 속도 —새 CPS가 이 임계값을 초과하면 방화벽이 DoS 경보를 생성합니다. 분류된 프로파일의 경우 정상적인 변동으로 인해 경고가 발생하지 않도록 디바이스의 평균 CPS 속도보다 15-20% 높은 비율을 설정합니다. 집계 프로파일의 경우 그룹 평균 CPS 비율보다 15-20% 높은 비율을 설정합니다.
- 활성화 속도 - 새 CPS가 이 임계값을 초과하면 CPS 속도가 임계값 아래로 떨어질 때까지 방화벽이 플러드를 완화하기 위해 새 연결을 끊기 시작합니다. 분류된 프로파일의 경우 최대 속도는 보호 중인 기기에 대해 허용 가능한 CPS 속도여야 합니다(최대 속도는 중요한 디바이스를 플러딩하지 않습니다). 활성화 속도를 최대 속도와 동일한 임계값으로 설정하여 방화벽이 RED 또는 SYN 쿠키를 사용하여 최대 속도에 도달하기 전에 트래픽을 삭제하지 않도록 할 수 있습니다. 최대 속도에 도달하기 전에 트래픽을 삭제하려는 경우에만 활성화 속도를 최대 속도보다 낮게 설정합니다. 집계 프로파일의 경우 RED(또는 SYN 플러드의 경우 SYN 쿠키)를 사용하여 플러드를 완화하기 시작할 그룹의 평균 피크 CPS 속도 바로 위에 임계값을 설정합니다.

 ©2023 Palo Alto Networks, Inc.

- 최대 속도 - 새 CPS가 이 임계값을 초과하면 방화벽은 지정된 차단 기간 동안 문제가 되는 IP 주소에서 모든 새 연결을 차단(삭제)합니다. 분류된 프로파일의 경우 CPS 속도가 넘치지 않도록 보호하고 있는 디바이스의 용량을 기준으로 **Max Rate** 임계값을 지정합니다. 집계 프로파일의 경우 그룹 용량의 80-90%로 설정합니다.
- 차단 기간 - 새 CPS가 최대 속도를 초과하면 방화벽이 문제가 되는 IP 주소에서 새 연결을 차단합니다. 차단 기간은 방화벽이 IP 주소의 새 연결을 계속 차단하는 시간을 지정합니다. 방화벽은 새 연결을 차단하지만 들어오는 연결을 계산하지 않으며 임계값 카운터를 증가시키지 않습니다. 분류 및 집계 프로파일의 경우 기본값(300초)을 사용하여 너무 오랜 시간 동안 소스의 합법적인 세션에 불이익을 주지 않고 공격 세션을 차단합니다.



*SYN* 플러드 프로텍션은 드롭 액션을 설정하는 유일한 유형입니다. 먼저 작업을 ***SYN*** 쿠키로 설정합니다. *SYN* 쿠키는 합법적인 트래픽을 공정하게 처리하고 *SYN* 핸드쉐이크에 실패한 트래픽만 삭제합니다. 반면 *Random Early Drop*을 사용하면 트래픽이 무작위로 삭제되므로 *RED*가 합법적인 트래픽에 영향을 줄 수 있습니다. 그러나 *SYN* 쿠키는 방화벽이 대상 서버에 대한 프록시 역할을 하고 서버에 대한 *3*방향 핸드쉐이크를 처리하기 때문에 리소스를 많이 사용합니다. 합법적인 트래픽*(SYN* 쿠키*)*을 삭제하지 않고 방화벽 리소스를 보존하는 것*(RED)*이 절충되는 것이 아닙니다. 방화벽을 모니터링하고 *SYN* 쿠키가 너무 많은 리소스를 사용하는 경우 *RED*로 전환합니다. 방화벽 앞에 전용 *DDoS* 방지 디바이스가 없는 경우 항상 *RED*를 드롭 메커니즘으로 사용하십시오.

DoS 방어 프로파일이 정상 트래픽을 예기치 않게 삭제하지 않도록 기본 임계값이 높습니다. 연결 트래픽을 모니터링하고 네트워크에 적합한 값으로 임계값을 조정합니다. 먼저 각 플러드 유형에 대한 평균 및 피크 CPS의 기준 측정을 수행하여 보호하려는 중요 디바이스의 정상적인 교통 상황을 파악합니다. 정상적인 트래픽 부하에는 약간의 변동이 발생하므로 연결을 너무 적극적으로 끊지 않는 것이 가장 좋습니다. 필요에 따라 그리고 네트워크가 발전함에 따라 플러드 임계값을 모니터링하고 조정합니다.

플러드 임계값을 설정하는 또 다른 방법은 기준선 측정을 사용하여 허용할 최대 CPS를 설정하고 거기에서 다시 작업하여 적절한 플러드 완화 경보 및 활성화 비율을 도출하는 것입니다.



여러 *DP(*데이터플레인 프로세서*)*가 있는 방화벽은 *DP* 간에 연결을 분산합니다. 일반적으로 방화벽은 *CPS* 임계값 설정을 *DP* 간에 균등하게 나눕니다. 예를 들어 방화벽에 *5*개의 *DP*가 있고 경보 속도를 *20,000CPS*로 설정한 경우 각 *DP*의 경보 속도는 *4,000CPS(20,000/ 5 = 4,000)*이므로 *DP*의 새 세션이 *4,000*을 초과하면 해당 *DP*에 대한 경보 비율 임계값이 트리거됩니다.

IP 플러드 임계값을 설정하는 것 외에도 DoS 방어 프로파일을 사용하여 많은 수의 호스트(봇)가 대상의 리소스를 소비하기 위해 가능한 한 많은 세션을 설정하는 세션 소모 공격을 탐지하고 방지할 수 있습니다. 프로파일의 리소스 보호 탭에서 프로파일을 적용하는 DoS 방어 정책 규칙에 정의된 디바이스가 수신할 수 있는 최대 동시 세션 수를 설정할 수 있습니다. 동시 세션 수가 최대 제한에 도달하면 새 세션이 삭제됩니다.

설정할 최대 동시 세션 수는 네트워크 컨텍스트에 따라 다릅니다. 프로파일을 연결하는 DoS 방어 정책 규칙에 정의된 보호 중인 리소스가 처리할 수 있는 동시 세션 수를 파악합니다. 임계값을 리소스 용량의 약 80%로 설정한 다음 필요에 따라 임계값을 모니터링하고 조정합니다.

집계 프로파일의 경우 리소스 보호 임계값은 정책 규칙(소스 및 대상)에 정의된 디바이스의 모든 트래픽에 적용됩니다. 분류된 프로파일의 경우 리소스 보호 임계값은 분류된 정책 규칙이 소스 IP에만 적용되는지, 대상 IP에만 적용되는지, 소스 및 대상 IP에 모두 적용되는지에 따라 트래픽에 적용됩니다.

 ©2023 Palo Alto Networks, Inc.

## DoS 보호 정책 규칙

DoS 방어 정책 규칙은 방화벽이 DoS 방어를 적용하는 시스템(DoS 방어 정책 규칙에 연결하는 DoS 방어 프로파일에 구성된 플러드 임계값), 트래픽이 규칙에 정의된 기준과 일치할 때 수행할 조치 및 DoS 트래픽을 로깅하는 방법을 제어합니다. DoS 방어는 방화벽 리소스를 사용하므로 세션 플러드에 대한 특정 중요 리소스, 특히 사용자가 인터넷에서 액세스하는 일반적인 대상(예: 웹 서버 및 데이터베이스 서버)을 방어하는 데만 사용하십시오. 영역 보호 프로파일을 사용하여 플러드 및 기타 공격으로부터 전체 영역을 보호합니다. DoS 방어 정책 규칙은 세분화된 일치 기준을 제공하므로 보호하려는 대상을 유연하게 정의할 수 있습니다.

- 소스 영역, 인터페이스, IP 주소(전체 리전 포함) 및 사용자
- 대상 영역, 인터페이스 및 IP 주소(전체 리전 포함)
- 서비스(포트 및 프로토콜별). DoS 방어는 지정한 서비스에만 적용됩니다. 그러나 서비스를 지정하면 서비스가 허용되지 않으며 다른 모든 서비스는 암시적으로 차단됩니다. 서비스를 지정하면 DoS 방어가 해당 서비스로 제한되지만 다른 서비스는 차단되지 않습니다.

> 중요한 서버에서 사용 중인 서비스 포트를 보호하는 것 외에도 해당 서버의 사용되지 않는 서비스 포트에 대한 ***DoS*** 공격으로부터 보호할 수 있습니다**.** 중요한 시스템의 경우 서비스가 실행 중인 포트를 보호하는 하나의 ***DoS*** 방어 정책 규칙 및 프로파일을 생성하고**,** 서비스가 실행되지 않은 상태에서 포트를 보호하는 다른 ***DoS*** 방어 정책 규칙 및 프로파일을 만들어 이를 수행할 수 있습니다**.** 예를 들어 하나의 정책/프로파일로 웹 서버의 일반 서비스 포트**(**예**:** ***80*** 및 ***443)***를 보호하고 다른 정책/프로파일로 다른 모든 서비스 포트를 보호할 수 있습니다**.** ***DoS*** 카운터 서비스가 성능에 영향을 미치지 않도록 방화벽의 용량에 유의하십시오**.**

트래픽이 DoS 방어 정책 규칙과 일치하면 방화벽은 다음 세 가지 작업 중 하나를 수행합니다.

- 거부 - 방화벽이 액세스를 거부하고 DoS 방어 프로파일을 적용하지 않습니다. 규칙과 일치하는 트래픽이 차단됩니다.
- 허용 —방화벽이 액세스를 허용하고 DoS 방어 프로파일을 적용하지 않습니다. 규칙과 일치하는 트래픽이 허용됩니다.
- 보호 - 방화벽은 지정된 DoS 방어 프로파일 또는 프로파일 임계값을 규칙과 일치하는 트래픽에 적용하여 DoS 방어 정책 규칙에 정의된 디바이스를 보호합니다. 규칙에는 하나의 집계 DoS 방어 프로파일과 하나의 분류된 DoS 방어 프로파일이 있을 수 있으며, 분류된 프로파일의 경우 분류된 DoS 방어와 집계 DoS 방어의 설명에 따라 소스 IP, 대상 IP 또는 둘 다를 사용하여 플러드 임계값 카운터를 증가시킬 수 있습니다. 들어오는 패킷은 규칙과 일치하는 경우 두 DoS 방어 프로파일 임계값에 대해 계산됩니다.

작업이 보호인 경우에만 방화벽이 DoS 방어 프로파일을 적용합니다. DoS 방어 정책 규칙의 작업이 보호인 경우 방화벽이 규칙과 일치하는 트래픽에 DoS 방어 프로파일의 임계값을 적용하도록 규칙에 적절한 집계 및/또는 분류된 DoS 방어 프로파일을 지정합니다. 대부분의 규칙은 보호 규칙입니다.

**Allow** 및 **Deny** 작업을 사용하면 더 큰 그룹 내에서 예외를 만들 수 있지만 트래픽에 DoS 방어를 적용하지는 않습니다. 예를 들어 대부분의 그룹에서 오는 트래픽은 거부하지만 해당 트래픽의 하위 집합은 허용할 수 있습니다. 반대로 대부분의 그룹에서 오는 트래픽을 허용하고 해당 트래픽의 하위 집합을 거부할 수 있습니다.

DoS 방어 정책 규칙이 활성 상태일 때(시작 및 종료 시간, 되풀이 기간) 예약할 수 있습니다. 일정에 대한 한 가지 사용 사례는 하루 또는 주중 다른 시간에 서로 다른 플러드 임계값을 적용하는 것입니다. 예를 들

 ©2023 Palo Alto Networks, Inc.

어 야간에 트래픽이 낮보다 훨씬 적은 경우 밤보다 낮에는 더 높은 플러드 임계값을 적용할 수 있습니다. 또 다른 사용 사례는 방화벽이 CPS 속도를 지원하는 경우 특별 이벤트에 대한 특별 임계값을 예약하는 것입니다.

보다 쉬운 관리와 세분화된 보고를 위해 DoS 방어 로그를 다른 위협 로그와 분리하도록 로그 포워딩을 구성합니다. 로그를 SNMP 또는 syslog 서버와 같은 서버로 포워딩할 뿐만 아니라 이메일을 통해 DoS 임계값 위반 이벤트를 관리자에게 직접 포워딩합니다. 방화벽의 크기가 적절하다고 할 경우 임계값 위반은 빈번하지 않아야 하며 이는 공격 시도를 나타내는 강력한 지표가 될 것입니다.


©2023 Palo Alto Networks, Inc.

# 영역 보호를 구성하여 네트워크 보안 강화

다음 항목에서는 영역 보호 구성 예를 제공합니다.

- 정찰 보호 구성
- 패킷 기반 공격 보호 구성
- 프로토콜 보호 구성
- 패킷 버퍼 보호 구성
- 대기 시간을 기준으로 패킷 버퍼 보호 구성
- 이더넷 SGT 보호 구성

## 정찰 보호 구성

해당 정찰 시도에 대한 응답으로 방화벽이 수행할 다음 정찰 보호 작업 중 하나를 구성합니다.

- 허용 - 방화벽에서 포트 스캔 또는 호스트 스윕 정찰을 계속할 수 있습니다.
- 알림 - 방화벽은 지정된 시간 간격 내에서 구성된 임계값과 일치하는 각 포트 스캔 또는 호스트 스윕에 대한 알림을 생성합니다. 알림은 기본 설정입니다.
- 차단 - 방화벽은 지정된 시간 간격의 나머지 동안 소스에서 대상으로의 모든 후속 패킷을 삭제합니다.
- **IP** 차단 - 방화벽은 지정된 기간(초) 동안 모든 후속 패킷을 삭제합니다(범위는 1-3,600). 추적 기준은 방화벽이 원본 또는 원본 및 대상 트래픽을 차단할지의 여부를 결정합니다.

**STEP 1 |** 정찰 보호를 구성합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택합니다.
2. 영역 보호 프로파일을 선택하거나 새 프로파일을 추가하고 이름을 입력합니다.
3. 정찰 보호 탭에서 보호할 검사 유형을 선택합니다.
4. 각 스캔에 대한 작업을 선택합니다. IP 차단을 선택하는 경우 추적 기준(소스 또는 소스 및 대상) 및 기간도 구성해야 합니다.
5. 간격을 초 단위로 설정합니다. 이 옵션은 포트 스캔 및 호스트 스윕 감지를 위한 시간 간격을 정의합니다.
6. 임계값을 설정합니다. 임계값은 작업을 트리거하도록 위에 구성된 간격 내에서 발생하는 포트 스캔 이벤트 또는 호스트 스윕의 수를 정의합니다.

**STEP 2 |** (선택 사항) 원본 주소 제외를 구성합니다.

1. 정찰 보호 탭에서 원본 주소 제외를 추가합니다.
   1. 제외할 주소를 설명하는 이름을 입력합니다.
   2. 주소 유형을 **IPv4** 또는 **IPv6**으로 설정한 다음 주소 개체를 선택하거나 IP 주소를 입력합니다.
   3. 확인을 클릭합니다.
2. 확인을 클릭하여 영역 보호 프로파일을 저장합니다.
3. 변경 사항을 커밋합니다.


©2023 Palo Alto Networks, Inc.

# 패킷 기반 공격 보호 구성

영역에 대한 보안을 강화하기 위해 패킷 기반 공격 보호은(는) 방화벽이 특정 특성을 가지고 있거나 패킷에서 특정 옵션을 제거하는 IP, IPv6, TCP, ICMP 또는 ICMPv6 패킷을 삭제하는지의 여부를 지정할 수 있습니다.

예를 들어 TCP 3방향 핸드셰이크 중에 페이로드에 데이터가 포함된 TCP SYN 및 SYN-ACK 패킷을 삭제할 수 있습니다. 기본적으로 영역 보호 프로파일은 데이터가 있는 SYN 및 SYN-ACK 패킷을 삭제하도록 설정되어 있습니다(영역에 프로파일을 적용해야 합니다).

TCP 빠른 열기 옵션(RFC 7413)은 SYN 및 SYN-ACK 패킷의 페이로드에 데이터를 포함시켜 연결 설정 속도를 유지합니다. 영역 보호 프로파일은 TCP Fast Open 옵션을 다른 SYN 및 SYN-ACK 패킷과 별도로 사용하는 핸드셰이크를 취급합니다. 프로파일은 기본적으로 유효한 Fast Open 쿠키가 포함된 경우 핸드셰이크 패킷을 허용하도록 설정됩니다.

*PAN-OS 8.0*으로 업그레이드할 때 기존 영역 보호 프로파일이 있는 경우 세 가지 기본 설정이 각 프로파일에 적용되고 방화벽이 그에 따라 작동합니다.

PAN-OS 8.1.2 이후 릴리스를 시작으로 CLI 명령(이 작업의 4단계)을 사용하여 방화벽이 다음 유형의 패킷을 수신하고 삭제할 때 방화벽이 위협 로그를 생성할 수 있도록 하여 이러한 발생을 보다 쉽게 분석하고 감사 및 규정 준수 요구 사항을 충족할 수 있습니다.

- 티어드롭 공격
- 과부하(ping of death)를 통한 DoS 공격

또한 동일한 CLI 명령을 사용하면 해당 패킷 기반 공격 보호를 사용하도록 설정하면 방화벽이 다음 유형의 패킷에 대한 위협 로그를 생성할 수 있습니다.

- 단편화된 IP 패킷
- IP 주소 스푸핑
- 1024바이트보다 큰 ICMP 패킷
- ICMP 조각이 포함된 패킷
- 오류 메시지와 함께 포함된 ICMP 패킷
- SYN 패킷이 아닌 TCP 세션의 첫 번째 패킷

**STEP 1 |** 영역 보호 프로파일을 생성하고 패킷 기반 공격 보호 설정을 구성합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택하고 새 프로파일을 추가합니다.
2. 프로파일의 이름과 선택 사항인 설명을 입력합니다.
3. 패킷 기반 공격 보호를 선택합니다.
4. 각 탭에서(**IP Drop**, **TCP Drop**, **ICMP Drop**, **IPv6 Drop** 및 **ICMPv6 Drop**) , 영역을 보호하기 위해 시행하려는 패킷 기반 공격 보호 설정을 선택합니다.
5. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 2 |** 보호하려는 인터페이스에 할당된 보안 영역에 영역 보호 프로파일을 적용합니다.

1. 네트워크 > 영역을 선택하고 영역 보호 프로파일을 할당할 영역을 선택합니다.
2. 영역에 속한 인터페이스를 추가합니다.
3. 영역 보호 프로파일에서 방금 생성한 프로파일을 선택합니다.
4. 확인을 클릭합니다.

**STEP 3 |** 변경 사항을 커밋합니다.

**STEP 4 |** (PAN-OS 8.1.2 이상 릴리스) 방화벽이 Teardrop 공격 및 죽음의 핑을 사용하는 DoS 공격에 대한 위협 로그를 생성하도록 설정하고 다음과 같은 경우 위에 나열된 패킷 유형에 대한 위협 로그를 생성합니다. 해당 패킷 기반 공격 보호를 활성화합니다(1단계에서). 예를 들어 스푸프된 **IP** 주소에 대한 패킷 기반 공격 보호를 사용하도록 설정하면 다음 CLI를 사용하면 방화벽이 스푸프된 IP 주소가 있는 패킷을 수신하고 삭제할 때 방화벽이 위협 로그를 생성합니다.

1. CLI에 액세스합니다.
2. 운영 CLI 명령 **set system setting additional-threat-log on**을 사용합니다. 기본값은 꺼짐 상태입니다.

## 프로토콜 보호 구성

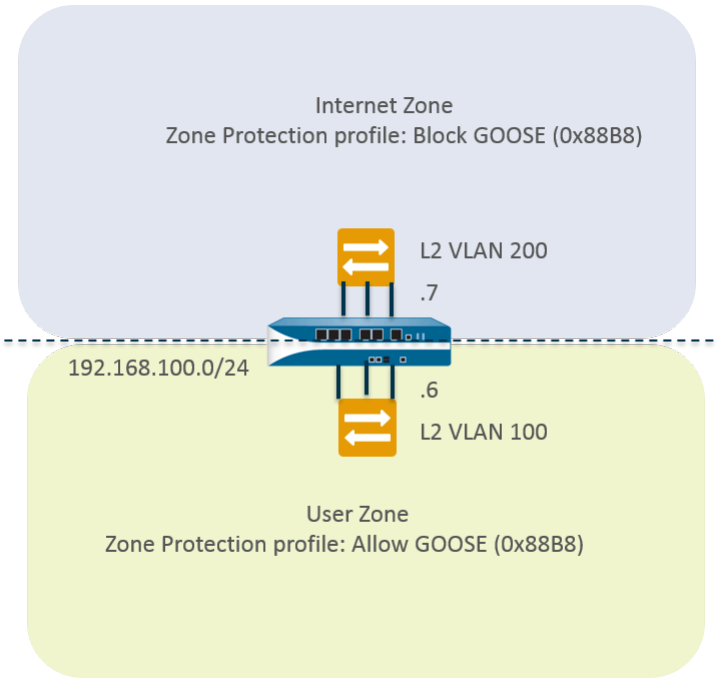
프로토콜 보호을(를) 사용하여 비IP 프로토콜 패킷으로부터 가상 와이어 또는 레이어 2 보안 영역을 보호합니다.

- 사용 사례: 레이어 2 인터페이스의 보안 영역 간 비 IP 프로토콜 보호
- 사용 사례: 레이어 2 인터페이스의 보안 영역 내에서 비 IP 프로토콜 보호

### 사용 사례: 레이어 2 인터페이스의 보안 영역 간 비 IP 프로토콜 보호

이 사용의 경우 방화벽은 두 개의 하위 인터페이스로 나눈 레이어 2 VLAN에 있습니다. VLAN 100은 192.168.100.1/24, 하위 인터페이스 .6입니다. VLAN 200은 192.168.100.1/24, 하위 인터페이스 .7입니다. 비 IP 프로토콜 보호는 인레스 영역에 적용됩니다. 이 사용의 경우 인터넷 영역이 인그레스 영역인 경우 방화벽은 GOOSE(Generic Object Oriented Substation Event) 프로토콜을 차단합니다. 사용자 영역이 인그레스(ingress) 영역인 경우 방화벽을 통해 GOOSE 프로토콜을 허용합니다. 방화벽을 암시적으로 허용하면 두 영역에서 IPv4, IPv6, ARP 및 VLAN 태그 프레임이 모두 허용됩니다.


©2023 Palo Alto Networks, Inc.




**STEP 1 |** 두 개의 VLAN 하위 인터페이스를 구성합니다.

1. 네트워크 > 인터페이스 > **VLAN**을 선택하고 인터페이스를 추가합니다.
2. 인터페이스 이름의 기본값은 vlan입니다. 마침표 뒤에 7을 입력합니다.
3. 구성 탭에서 **VLAN** 200에 인터페이스를 할당합니다.
4. 확인을 클릭합니다.
5. 네트워크 > 인터페이스 > **VLAN**을 선택하고 인터페이스를 추가합니다.
6. 인터페이스 이름의 기본값은 vlan입니다. 마침표 뒤에 6을 입력합니다.
7. 구성 탭에서 **VLAN** 100에 인터페이스를 할당합니다.
8. 확인을 클릭합니다.

**STEP 2 |** 영역 보호 프로파일에서 프로토콜 보호를 구성하여 GOOSE 프로토콜 패킷을 차단합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택하고 프로파일 추가를 선택합니다.
2. 이름 블록 GOOSE를 입력합니다.
3. 프로토콜 보호를 선택합니다.
4. 제외 목록의 규칙 유형을 선택합니다.
5. 목록에서 Ethertype을 쉽게 식별할 수 있도록 프로토콜 이름, GOOSE를 입력합니다. 방화벽은 입력한 이름이 Ethertype 코드와 일치하는지 확인하지 않습니다. Ethertype 코드만 사용하여 필터링합니다.
6. **Ethertype** 코드 0x88B8을 입력합니다. 16진수 값을 나타내려면 Ethertype 앞에 0x가 와야 합니다. 범위는 0xFFFF~0x0000입니다.
7. 프로토콜 보호를 적용하려면 사용 설정을 선택합니다. 예를 들어 테스트용으로 목록에서 프로토콜을 비활성화할 수 있습니다.
8. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** 영역 보호 프로파일을 인터넷 영역에 적용합니다.

1. 네트워크 > 영역을 선택하고 영역을 추가합니다.
2. 영역의 이름을 인터넷으로 입력합니다.
3. 위치에서 영역이 적용되는 가상 시스템을 선택합니다.
4. 유형에 대해 레이어**2**를 선택합니다.
5. 영역 vlan.7에 속한 인터페이스를 추가합니다.
6. 영역 보호 프로파일에 대해 Block GOOSE 프로파일을 선택합니다.
7. 확인을 클릭합니다.

**STEP 4 |** GOOSE 프로토콜 패킷을 허용하도록 프로토콜 보호를 구성합니다.

Allow GOOSE라는 다른 영역 보호 프로파일을 생성하고 포함 목록의 규칙 유형을 선택합니다.

포함 목록을 구성할 때 필요한 모든 비 ***IP*** 프로토콜을 포함합니다**.** 목록이 불완전하면 합법적인 비 ***IP*** 트래픽이 차단될 수 있습니다**.**

**STEP 5 |** 사용자 영역에 영역 보호 프로파일을 적용합니다.

1. 네트워크 > 영역을 선택하고 영역을 추가합니다.
2. 사용자 영역의 이름을 입력합니다.
3. 위치에서 영역이 적용되는 가상 시스템을 선택합니다.
4. 유형에 대해 레이어**2**를 선택합니다.
5. 영역 vlan.6에 속한 인터페이스를 추가합니다.
6. 영역 보호 프로파일에서 GOOSE 허용 프로파일을 선택합니다.
7. 확인을 클릭합니다.

**STEP 6 |** 커밋합니다.

커밋을 클릭합니다.

**STEP 7 |** 프로토콜 보호에 따라 방화벽이 삭제한 비 IP 패킷 수를 봅니다.

CLI에 액세스합니다.

```
> show counter global name pkt_nonip_pkt_drop > show counter global
 name pkt_nonip_pkt_drop delta yes
```

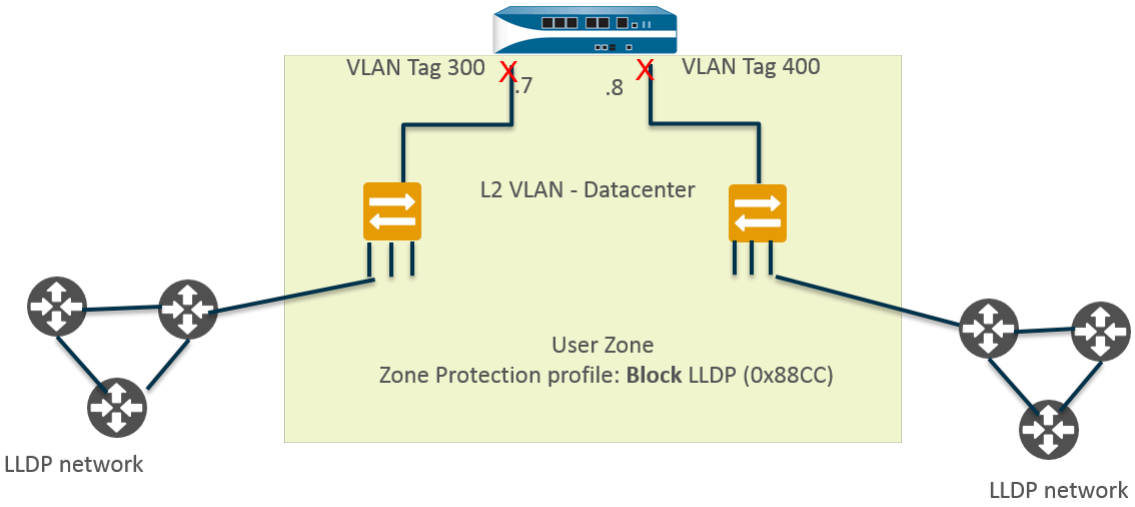
## 사용 사례**:** 레이어 **2** 인터페이스의 보안 영역 내에서 비 **IP** 프로토콜 보호

IP가 아닌 프로토콜 보호를 통해 영역 보호 프로파일을 구현하지 않으면 방화벽을 사용하면 단일 영역의 비 IP 프로토콜이 한 레이어 2 인터페이스에서 다른 레이어로 이동하도록 허용합니다. 이 사용의 경우 LLDP 패킷을 차단하면 한 네트워크에 대해 LLDP가 영역의 다른 인터페이스를 통해 연결할 수 있는 네트워크를 발견하지 못하도록 합니다.

다음 그림에서 데이터 센터라는 레이어 2 VLAN은 두 개의 하위 인터페이스로 나뉩니다. 192.168.1.1/24, 하위 인터페이스 .7 및 192.168.1.2/24, 하위 인터페이스 .8. VLAN은 사용자 영역에 속합니다. 사용자 영역에 LLDP를 차단하는 영역 보호 프로파일을 적용하여 다음을 수행합니다.

 ©2023 Palo Alto Networks, Inc.

- 하위 인터페이스 .7은 왼쪽의 빨간색 X에 있는 방화벽으로의 스위치에서 LLDP를 차단하여 해당 트래픽이 하위 인터페이스 .8에 도달하는 것을 방지합니다.
- 하위 인터페이스 .8은 오른쪽의 빨간색 X에 있는 방화벽으로의 스위치에서 LLDP를 차단하여 해당 트래픽이 하위 인터페이스 .7에 도달하는 것을 방지합니다.




**STEP 1 |** 이더넷 인터페이스에 대한 하위 인터페이스를 생성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 레이어 2 인터페이스(이 예에서는 ethernet1/1)를 선택합니다.
2. 하위 인터페이스 추가를 선택합니다.
3. 인터페이스 이름은 인터페이스(이더넷 1/1)를 기본값으로 설정합니다. 마침표 뒤에 7을 입력합니다.
4. 태그의 경우 300을 입력합니다.
5. 보안 영역에서 사용자를 선택합니다.
6. 확인을 클릭합니다.

**STEP 2 |** 이더넷 인터페이스에 대한 두 번째 하위 인터페이스를 생성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 레이어 2 인터페이스(ethernet1/1)를 선택합니다.
2. 하위 인터페이스 추가를 선택합니다.
3. 인터페이스 이름은 인터페이스(이더넷 1/1)를 기본값으로 설정합니다. 마침표 뒤에 8을 입력합니다.
4. 태그의 경우 400을 입력합니다.
5. 보안 영역에서 사용자를 선택합니다.
6. 확인을 클릭합니다.


©2023 Palo Alto Networks, Inc.

**STEP 3 |** Layer2 인터페이스와 두 개의 하위 인터페이스에 대한 VLAN을 생성합니다.

1. 네트워크 > **VLAN**을 선택하고 VLAN을 추가합니다.
2. VLAN의 이름을 입력합니다. 이 예에서는 Datacenter를 입력합니다.
3. **VLAN** 인터페이스에 대해 없음을 선택합니다.
4. 인터페이스에 대해 추가를 클릭하고 Layer 2 인터페이스인 ethernet1/1과 2개의 하위 인터페이스인 ethernet1/1.7 및 ethernet1/1.8을 선택합니다.
5. 확인을 클릭합니다.

**STEP 4 |** 영역 보호 프로파일에서 비 IP 프로토콜 패킷을 차단합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택하고 프로파일 추가를 선택합니다.
2. 이름(이 예에서는 Block LLDP)을 입력합니다.
3. 프로파일 입력 설명 - LLDP 네트워크에서 영역(영역 내)의 다른 인터페이스로 가는 LLDP 패킷을 차단합니다.
4. 프로토콜 보호를 선택합니다.
5. 제외 목록의 규칙 유형을 선택합니다.
6. 프로토콜 이름 LLDP를 입력합니다.
7. **Ethertype** 코드 0x88cc를 입력합니다. 16진수 값을 나타내려면 Ethertype 앞에 0x가 와야 합니다.
8. 활성화를 선택합니다.
9. 확인을 클릭합니다.

**STEP 5 |** 레이어 2 VLAN이 속한 보안 영역에 영역 보호 프로파일을 적용합니다.

1. 네트워크 > 영역을 선택합니다.
2. 영역을 추가합니다.
3. 사용자 영역의 이름을 입력합니다.
4. 위치에서 영역이 적용되는 가상 시스템을 선택합니다.
5. 유형에 대해 레이어**2**를 선택합니다.
6. ethernet1/1.7 영역에 속한 인터페이스를 추가합니다.
7. ethernet1/1.8 영역에 속한 인터페이스를 추가합니다.
8. 영역 보호 프로파일에 대해 LLDP 차단 프로파일을 선택합니다.
9. 확인을 클릭합니다.

**STEP 6 |** 커밋합니다.

커밋을 클릭합니다.

**STEP 7 |** 프로토콜 보호에 따라 방화벽이 삭제한 비 IP 패킷 수를 봅니다.

CLI에 액세스합니다.

```
> show counter global name pkt_nonip_pkt_drop > show counter global
 name pkt_nonip_pkt_drop delta yes
```


©2023 Palo Alto Networks, Inc.

# 패킷 버퍼 보호 구성

패킷 버퍼 보호는 디바이스 수준(전역)의 두 가지 수준에서 구성할 수 있으며 전역적으로 활성화된 경우 영역 수준에서도 활성화할 수 있습니다. 전역 패킷 버퍼 보호(**Device** > **Setup** > **Session**)는 방화벽 리소스를 보호하고 악성 트래픽으로 인해 방화벽이 응답하지 않도록 하는 것입니다.

수신 영역(네트워크 > 영역)당 패킷 버퍼 보호는 패킷 버퍼 보호 임계값을 계속 초과하는 경우 문제가 되는 IP 주소를 차단하기 시작하는 두 번째 보호 레이어입니다. 방화벽은 문제가 되는 소스 IP 주소의 모든 트래픽을 차단할 수 있습니다. 소스 IP 주소가 변환된 NAT IP 주소인 경우 많은 사용자가 동일한 IP 주소를 사용할 수 있습니다. 한 명의 악의적인 사용자가 패킷 버퍼 보호를 트리거하고 수신 영역에 패킷 버퍼 보호가 활성화되어 있으면 방화벽이 해당 IP 주소를 차단 목록에 넣을 때 문제를 일으키는 소스 IP 주소의 모든 트래픽(비남용적인 사용자의 경우 포함)이 차단될 수 있습니다.

방화벽 뒤의 서비스에 대한 DoS 공격을 차단하는 가장 효과적인 방법은 패킷 버퍼 보호를 전역 및 수신 영역별로 구성하는 것입니다.

영역에 대해 패킷 버퍼 보호를 활성화할 수 있지만 패킷 버퍼 보호를 전역적으로 활성화하고 설정을 지정할 때까지는 활성화되지 않습니다.

**STEP 1 |** 패킷 버퍼 보호를 전역적으로 활성화합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. 패킷 버퍼 보호를 선택합니다.
3. 패킷 버퍼 보호 동작을 정의합니다.
   - 경고**(%)** - 패킷 버퍼 사용률이 10초 이상 이 임계값을 초과하면 방화벽이 1분마다 로그 이벤트를 생성합니다. 범위 s 0% ~ 99%; 기본값은 50%입니다. 값이 0%이면 방화벽이 로그 이벤트를 생성하지 않습니다.
   - 활성화**(%)** - 패킷 버퍼 사용률이 이 임계값에 도달하면 방화벽이 RED(임의 조기 삭제)를 적용하여 가장 악의적인 세션을 완화하기 시작합니다. 범위는 0% ~ 99%입니다. 기본값은 50%입니다. 값이 0%이면 방화벽이 RED를 적용하지 않습니다. 어뷰저가 패킷 버퍼 보호가 활성화된 영역을 침입하는 경우 방화벽은 남용된 세션을 삭제하거나 문제가 되는 소스 IP 주소를 차단할 수도 있습니다. 기본 임계값으로 시작하고 필요한 경우 조정합니다.

     방화벽은 시스템 로그에 경고 이벤트를 기록하고 위협 로그에 삭제된 트래픽, 폐기된 세션 및 차단된 ***IP*** 주소에 대한 이벤트를 기록합니다.
   - **Block Hold Time(초)** - 방화벽에서 세션을 삭제하기 전에 RED 완화 세션을 계속할 수 있는 시간(초)입니다. 범위는 0 ~ 65,535입니다. 기본값은 60입니다. 값이 0이면 방화벽은 패킷 버퍼 보호를 기반으로 세션을 삭제하지 않습니다.
   - 차단 기간**(초)** - 세션이 삭제된 상태로 유지되거나 IP 주소가 차단된 상태로 유지되는 시간(초)입니다. 범위는 1~15,999,999입니다. 기본값은 3,600입니다.
4. 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 수신 영역에서 추가 패킷 버퍼 보호를 활성화합니다.

1. 네트워크 > 영역을 선택합니다.
2. 수신 영역을 선택한 다음 해당 이름을 클릭합니다.
3. 영역 보호 섹션에서 패킷 버퍼 보호를 활성화합니다.
4. 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

## 대기 시간을 기준으로 패킷 버퍼 보호 구성

대기 시간을 기반으로 패킷 버퍼 보호를 구성하고 대기 시간에 민감한 애플리케이션과 프로토콜로 구성된 트래픽이 있는 영역에 적용합니다.

**STEP 1 |** 디바이스 > 설정 > 세션을 선택합니다.

**STEP 2 |** 세션 설정 섹션을 편집하고 패킷 버퍼 보호를 활성화합니다.

**STEP 3 |** 버퍼링 지연 시간 기반을 활성화합니다.

**STEP 4 |** 방화벽이 매분 경고 로그 이벤트를 생성하기 시작하는 대기 시간 경고**(**밀리초**)** 임계값을 입력합니다. 범위는 1 ~ 20,000이고 기본값은 50입니다.

**STEP 5 |** 방화벽이 들어오는 패킷에 대해 임의 조기 삭제(RED)를 활성화하고 10초마다 활성화 로그 생성을 시작하는 지연 활성화**(**밀리초**)** 임계값을 입력합니다. 범위는 1~20,000ms이고 기본값은 200ms입니다.

**STEP 6 |** 방화벽이 100%에 가까운 드롭 확률로 RED를 사용하는 최대 허용 지연 시간**(**밀리초**)** 임계값을 입력합니다. 범위는 1~20,000ms이고 기본값은 500ms입니다.

현재 대기 시간이 지연 활성화 임계값과 대기 시간 최대 허용 임계값 사이의 값이면 방화벽은(현재 대기 시간 - 대기 시간 활성화 임계값) /(대기 시간 최대 허용 임계값 - 대기 시간 활성화 임계값)과 같이 RED 드롭 확률을 계산합니다. 예를 들어 현재 대기 시간이 300이고 활성화 대기 시간이 200이고 최대 허용 대기 시간이 500이면(300-200)/(500-200) = 1/3이며, 이는 방화벽이 약 33%의 RED 드롭 확률을 사용함을 의미합니다.

**STEP 7 |** 활용도를 기반으로 패킷 버퍼 보호에 대해 블록 유지 시간 및 블록 지속 시간을 구성합니다.

**STEP 8 |** 확인을 클릭합니다.

**STEP 9 |** 대기 시간을 기반으로 패킷 버퍼 보호를 원하는 각 영역에 대해 두 번째 보호 레이어을 활성화합니다.

1. 네트워크 > 영역을 선택하고 영역을 선택합니다.
2. 패킷 버퍼 보호를 활성화합니다.

**STEP 10 |** 커밋합니다.

## 이더넷 SGT 보호 구성

다음 작업을 사용하여 이더넷 SGT 보호 프로파일을 구성합니다.

 ©2023 Palo Alto Networks, Inc.

**STEP 1 |** 이더넷 SGT 보호를 제공하는 영역 보호 프로파일을 생성합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택합니다.
2. 이름으로 영역 보호 프로파일을 추가합니다.
3. 이더넷 **SGT** 보호를 선택합니다.
4. 이름으로 **Layer 2 SGT** 제외 목록을 추가합니다.
5. 목록에 대한 하나 이상의 태그 값을 입력하십시오(범위는 0~65,535입니다). 태그 값의 연속 범위인 개별 항목을 입력할 수 있습니다(예: 100-500). 제외 목록에 최대 100개(개별 또는 범위) 태그 항목을 추가할 수 있습니다.
6. 레이어 2 SGT 제외 목록을 활성화합니다. 언제든지 목록을 비활성화할 수 있습니다.
7. 확인을 클릭합니다.

**STEP 2 |** 레이어 2, 가상 와이어 또는 탭 인터페이스가 속한 보안 영역에 영역 보호 프로파일을 적용합니다.

1. 네트워크 > 영역을 선택합니다.
2. 영역을 추가합니다.
3. 영역의 이름을 입력합니다.
4. 위치에서 영역이 적용되는 가상 시스템을 선택합니다.
5. 유형으로 **Layer2**, **Virtual Wire** 또는 **Tap**을 선택합니다.
6. 영역에 속하는 인터페이스를 추가합니다.
7. 영역 보호 프로파일에 대해 생성한 프로파일을 선택합니다.
8. 확인을 클릭합니다.

**STEP 3 |** 커밋합니다.

**STEP 4 |** 이더넷 SGT 보호를 사용하는 모든 영역 보호 프로파일의 결과로 방화벽이 삭제한 패킷의 전역 카운터를 봅니다.

1. CLI에 액세스합니다.
2. **`> show counter global name pan_flow_dos_l2_sec_tag_drop`**


©2023 Palo Alto Networks, Inc.

# 신규 세션의 홍수에 대한 DoS 보호

새 세션의 플러드에 대한 DoS 방어는 대량 단일 세션 및 다중 세션 공격에 유용합니다. 단일 세션 공격에서 공격자는 단일 세션을 사용하여 방화벽 뒤에 있는 디바이스를 대상으로 합니다. 보안 규칙이 트래픽을 허용하는 경우 세션이 설정되고 공격자는 동일한 소스 IP 주소와 포트 번호, 대상 IP 주소 및 포트 번호 및 프로토콜을 사용하여 매우 높은 속도로 패킷을 전송하여 공격을 시작합니다. 다중 세션 공격에서 공격자는 단일 호스트의 여러 세션(또는 초당 연결[cps]을 사용하여 DoS 공격을 시작합니다.

이 기능은 새 세션의 ***DoS*** 공격, 즉 하드웨어로 오프로드되지 않은 트래픽에 대해서만 방어합니다. 오프로드된 공격은 이 기능에 의해 보호되지 않습니다. 그러나 이 항목에서는 클라이언트를 재설정하기 위해 보안 정책 규칙을 만드는 방법에 대해 설명합니다. 공격자는 초당 다양한 패턴으로 공격을 계속하며 이 주제에서 다루는 방어 방법에 의해 차단됩니다.

DoS 보호 프로파일 및 정책 규칙 다수의 들어오는 SYN, UDP, ICMP 및 ICMPv6 패킷 및 기타 유형의 IP 패킷의 플러딩 방지를 위해 협업합니다. 플러드를 구성하는 임계값을 결정합니다. 일반적으로 DoS 방어 프로파일은 방화벽이 DoS 경보를 생성하고, 임의 조기 드롭과 같은 작업을 수행하며, 추가 수신 연결을 삭제하는 임계값을 설정합니다. 패킷을 허용하거나 거부하는 대신 보호하기 위해 구성된 DoS 방어 정책 규칙은 임계값에 계산하기 위해 패킷과 일치하는 패킷(예: 소스 주소)에 대한 기준을 결정합니다. 이러한 유연성을 통해 특정 트래픽을 차단하거나 특정 트래픽을 허용하고 다른 트래픽을 DoS 트래픽으로 취급할 수 있습니다. 들어오는 속도가 최대 임계값을 초과하면 방화벽은 소스 주소에서 들어오는 트래픽을 차단합니다.

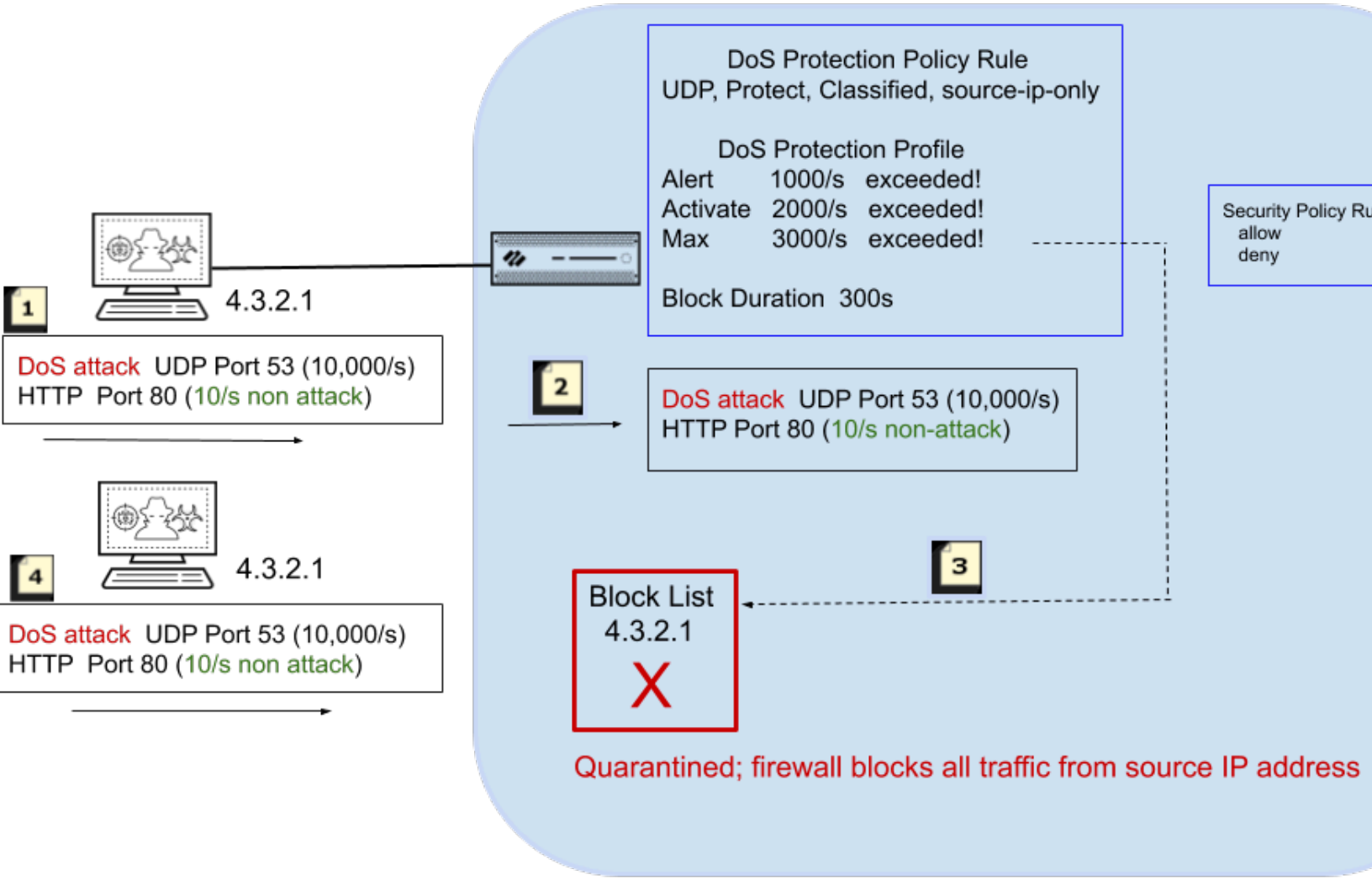
- 다중 세션 DoS 공격
- 단일 세션 DoS 공격
- 신규 세션의 범람으로부터 DoS 보호 구성
- 단일 세션 DoS 공격 종료
- 온칩 패킷 디스크립터를 과하게 사용하는 세션 식별
- 커밋 없이 세션 삭제

## 다중 세션 DoS 공격

수신 패킷과 일치할 때 보호 동작을 트리거하는 기준을 결정하는 DoS 방어 정책 규칙을 구성하여 새 세션의 범람에 대한 DoS 방어를 구성합니다. DoS 방어 프로파일은 각각의 새 연결을 알람 속도, 활성화 속도 및 최대 속도 임계값으로 계산합니다. 초당 들어오는 새 연결이 활성화 속도를 초과하면 방화벽은 DoS 방어 프로파일에 지정된 작업을 수행합니다.

다음 그림과 표에서는 보안 정책 규칙, DoS 방어 정책 규칙 및 프로파일이 함께 작동하는 방식을 예로 들어 설명합니다.


©2023 Palo Alto Networks, Inc.



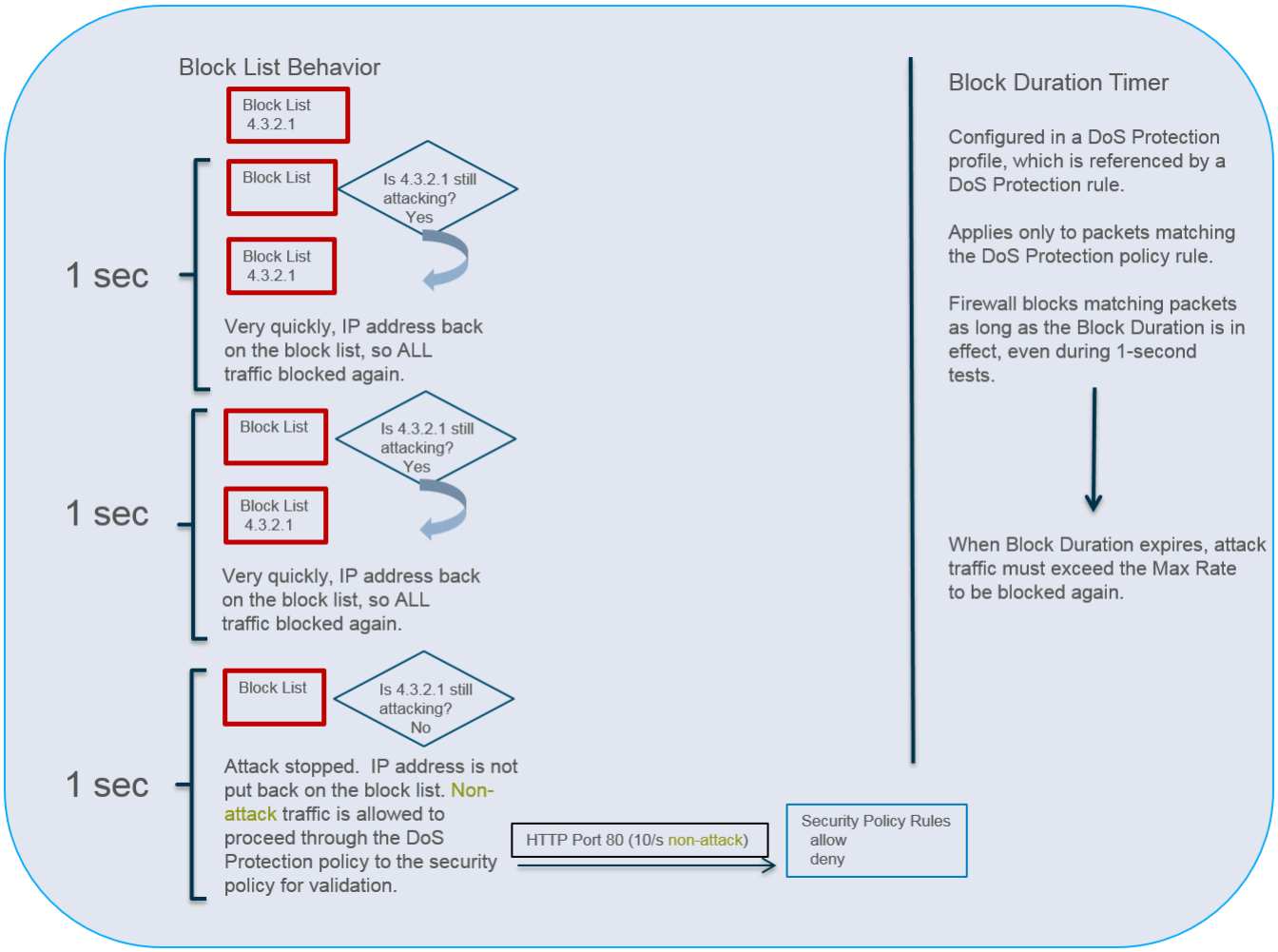

| 방화벽이 **IP** 주소를 격리하는 이벤트 시퀀스 | |
|---|---|
| 1 | 이 예에서 공격자는 UDP 포트 53에 대해 초당 10,000개의 새로운 연결 속도로 DoS 공격을 시작합니다. 또한 공격자는 초당 10개의 새 연결을 HTTP 포트 80으로 보냅니다. |
| 2 | 새 연결은 소스 영역 또는 인터페이스, 소스 IP 주소, 대상 영역 또는 인터페이스, 대상 IP 주소 또는 서비스와 같은 DoS 방어 정책 규칙의 조건과 다른 설정과 일치합니다. 이 예에서는 정책 규칙이 UDP를 지정합니다.<br><br>또한 DoS 방어 정책 규칙은 DoS 보호 프로파일 설정을 동적으로 적용하는 두 가지 설정인 보호 작업과 분류됨을 지정합니다. DoS 방어 프로파일은 초당 3000패킷의 최대 속도를 허용하도록 지정합니다. 수신 패킷이 DoS 방어 정책 규칙과 일치하면 초당 새 연결이 경고, 활성화 및 최대 속도 임계값으로 계산됩니다. |


©2023 Palo Alto Networks, Inc.

| 방화벽이 **IP** 주소를 격리하는 이벤트 시퀀스 | |
|---|---|
| | 또한 보안 정책 규칙을 사용하여 소스 ***IP*** 주소에서 오는 모든 트래픽을 차단할 수 있습니다. |
| 3 | 초당 10,000개의 새 연결이 최대 속도 임계값을 초과합니다. 다음 사항이 모두 발생하는 경우<br>• 임계값을 초과했습니다.<br>• 차단 지속 시간이 지정되고<br>• 분류됨 은 소스 IP 주소를 포함하도록 설정되고<br>방화벽은 문제가 있는 소스 IP 주소를 차단 목록에 추가합니다. |
| 4 | 차단 목록의 IP 주소가 격리되어 해당 IP 주소의 모든 트래픽이 차단됩니다. 방화벽은 추가 공격 패킷이 보안 정책에 도달하기 전에 문제가 있는 소스 IP 주소를 차단합니다. |

다음 그림에서는 DoS 방어 정책 규칙과 일치하는 IP 주소가 차단 목록에 추가되면 어떤 일이 발생하는지 자세히 설명합니다. 또한 차단 지속 시간 타이머에 대해서도 설명합니다.


©2023 Palo Alto Networks, Inc.




방화벽은 1초마다 IP 주소가 차단 목록에서 벗어나도록 허용하므로 방화벽이 트래픽 패턴을 테스트하고 공격이 진행 중인지 확인할 수 있습니다. 방화벽은 다음 작업을 수행합니다.

- 이 1초의 테스트 기간 동안 방화벽은 DoS 방어 정책 규칙을 통해 DoS 방어 정책 기준(이 예에서는 HTTP 트래픽)과 일치하지 않는 패킷을 유효성 검사를 위해 보안 정책으로 허용합니다. IP 주소가 차단 목록에서 제외된 후 방화벽이 받는 첫 번째 공격 패킷이 DoS 방어 정책 기준과 일치하므로 통과할 시간이 있는 패킷은 거의 없습니다. 그러면 IP 주소가 차단 목록에 1초 동안 다시 배치됩니다. 방화벽은 공격이 중지될 때까지 매초마다 이 테스트를 반복합니다.
- 방화벽은 차단 기간이 만료될 때까지 모든 공격 트래픽이 DoS 방어 정책 규칙(주소가 차단 목록에 남아 있음)을 통과하지 못하도록 차단합니다.

앞의 그림에 나와 있는 *1*초간의 검사는 여러 데이터플레인 *CPU*와 하드웨어 네트워크 프로세서가 있는 방화벽 모델에서 수행됩니다. 모든 단일 데이터플레인 시스템 또는 하드웨어 네트워크 프로세서가 없는 시스템은 소프트웨어에서 이 완화 기능을 수행하며 *5*초 인터벌으로 사용합니다.

공격이 중지되면 방화벽은 IP 주소를 차단 목록에 다시 넣지 않습니다. 방화벽은 공격이 아닌 트래픽이 DoS 방어 정책 규칙을 거쳐 평가를 위해 보안 정책 규칙으로 진행되도록 허용합니다. 트래픽을 허용하거나 거부하도록 보안 정책 규칙을 구성해야 합니다. 이 규칙이 없으면 암시적 거부 규칙이 모든 트래픽을 거부하기 때문입니다.


©2023 Palo Alto Networks, Inc.

차단 목록은 소스 영역과 소스 주소 조합을 기반으로 합니다. 이 동작을 사용하면 별도의 가상 라우터에 속하는 서로 다른 영역에 있는 한 중복 IP 주소가 존재할 수 있습니다.

DoS 보호 프로파일의 차단 기간 설정은 방화벽이 DoS 보호 정책 규칙과 일치하는 [공격] 패킷을 차단하는 기간을 지정합니다. 공격 트래픽은 차단 기간이 만료될 때까지 차단된 상태로 유지되며, 이 기간이 지나면 공격 트래픽이 다시 차단될 Max Rate 임계값을 초과해야 합니다.

공격자가 여러 공격 세션을 시작하는 여러 세션 또는 봇을 사용하는 경우 해당 세션은 보안 정책 거부 또는 삭제 규칙이 적용되지 않은 ***DoS*** 방어 프로파일의 임계값에 포함됩니다. 따라서 단일 세션 공격의 경우 각 패킷이 임계값에 포함되도록 보안 정책 거부 또는 삭제 규칙이 필요합니다. 다중 세션 공격은 그렇지 않습니다.

따라서 새 세션의 플러드에 대한 DoS 방어 기능을 통해 공격 트래픽이 진행 중인 동안 방화벽이 소스 IP 주소를 효율적으로 방어하고 공격이 중지되는 즉시 비공격 트래픽이 포워딩되도록 할 수 있습니다. 잘못된 IP 주소를 차단 목록에 넣으면 DoS 방어 기능이 차단 목록을 활용할 수 있습니다. 차단 목록은 다른 애플리케이션의 패킷과 같이 해당 소스 IP 주소의 모든 활동을 분리하도록 설계되었습니다. 모든 활동에서 IP 주소를 분리하면 공격자가 단순히 애플리케이션을 변경하여 새로운 공격을 시작하거나 하이브리드 DoS 공격에서 서로 다른 공격을 조합하여 사용하는 순환 애플리케이션 공격을 시도하는 최신 공격자로부터 보호할 수 있습니다. 차단된 IP 주소를 모니터링하여 차단 목록을 보고, 목록에서 항목을 제거하고, 차단 목록의 IP 주소에 대한 추가 정보를 얻을 수 있습니다.

***PAN-OS 7.0.2***부터는 방화벽이 공격 소스 ***IP*** 주소를 차단 목록에 배치하는 동작의 변화입니다. 공격이 중지되면 공격이 아닌 트래픽이 보안 정책 적용으로 진행될 수 있습니다. ***DoS*** 방어 프로파일 및 ***DoS*** 방어 정책 규칙과 일치하는 공격 트래픽은 차단 기간이 만료될 때까지 차단된 상태로 유지됩니다.

## 단일 세션 DoS 공격

단일 세션 DoS 공격은 일반적으로 세션이 생성된 후에 형성되는 공격이기 때문에 영역 또는 DoS 방어 프로파일을 트리거하지 않습니다. 이러한 공격은 세션 생성을 허용하기 때문에 보안 정책에 의해 허용되며, 세션 생성 후 공격은 패킷 볼륨을 높이고 대상 디바이스를 다운시킵니다.

신규 세션의 범람으로부터 DoS 보호 구성을(를) 하여, 새 세션의 플러딩(단일 세션 및 다중 세션 플러딩)으로부터 보호합니다. 진행 중인 단일 세션 공격의 경우, 추가로 단일 세션 DoS 공격 종료을(를) 합니다.

## 신규 세션의 범람으로부터 DoS 보호 구성

**STEP 1 |** 공격자의 IP 주소에서 오는 트래픽을 거부하고 네트워크 요구 사항에 따라 다른 트래픽을 허용하도록 보안 정책 규칙을 구성합니다. 소스 IP 주소와 같은 보안 정책 규칙에서 일치 기준을 지정할 수 있습니다. (단일 세션 공격 완화 또는 DoS 보호 정책 임계값을 트리거하지 않은 공격의 경우 필수, 다중 세션 공격 완화의 경우 선택 사항).

이 단계는 기존 공격을 중지하기 위해 일반적으로 수행되는 단계 중 하나입니다. 단일 세션 DoS 공격 종료을(를) 참조하십시오.

- 보안 정책 규칙 생성

 ©2023 Palo Alto Networks, Inc.

**STEP 2 |** 플러드 방지를 위한 DoS 보호 프로파일을 구성합니다.



플러드 공격은 여러 프로토콜에서 발생할 수 있으므로 모범 사례로 ***DoS*** 보호 프로파일의 모든 플러드 유형에 대한 보호를 활성화하십시오.

1. 개체 > 보안 프로파일 > **DoS** 보호를 선택한 다음 프로파일 이름 추가를 선택합니다.
2. 유형으로 분류됨을 선택합니다.
3. 플러드 방지에 대해 모든 유형의 플러드 방지를 선택합니다.
   - **SYN** 플러드
   - **UDP** 플러드
   - **ICMP** 플러드
   - **ICMPv6** 플러드
   - 기타 **IP** 플러드
4. **SYN Flood**를 활성화할 때 cps(초당 연결 수)가 활성화 속도 임계값을 초과할 때 발생하는 작업을 선택합니다.
   1. 임의 조기 삭제 - 방화벽은 알고리즘을 사용하여 해당 유형의 패킷 삭제를 점진적으로 시작합니다. 공격이 계속되면 들어오는 cps 속도(활성화 속도 이상)가 높을수록 방화벽이 더 많은 패킷을 삭제합니다. 방화벽은 들어오는 cps 속도가 최대 속도에 도달할 때까지 패킷을 삭제하고 이 지점에서 방화벽은 들어오는 모든 연결을 삭제합니다. RED(**Random Early Drop**)는 **SYN Flood**에 대한 기본 작업이며 **UDP Flood**, **ICMP Flood**, **ICMPv6 Flood** 및 기타 **IP Flood**에 대한 유일한 작업입니다. RED는 SYN 쿠키보다 더 효율적이고 더 큰 공격을 처리할 수 있지만 좋은 트래픽과 나쁜 트래픽을 구분하지 못합니다.
   2. **SYN** 쿠키 - 서버에 SYN을 즉시 보내는 대신 방화벽은 SYN-ACK를 클라이언트에 보낼 쿠키(서버 대체)를 생성합니다. 클라이언트는 ACK와 쿠키로 응답하며 이 유효성 검사 시 방화벽은 SYN을 서버로 보냅니다. **SYN** 쿠키 작업에는 **Random Early Drop**보다 더 많은 방화벽 리소스가 필요하며 이는 부정적인 트래픽에 영향을 미치기 때문에 더 분별력이 있습니다.
5. (선택 사항) 각 플러드 탭에서 환경에 맞게 다음 임계값을 변경합니다.
   - 경보 비율**(연결/초)** - DoS 경보가 생성되는 임계값 비율(cps)을 지정합니다. (범위는 0-2,000,000이고 기본값은 10,000입니다.)
   - 활성화 속도**(connections/s)** - DoS 응답이 활성화되는 임계값 속도(cps)를 지정합니다. **Activate Rate** 임계값에 도달하면 **Random Early Drop**이 발생합니다. 범위는

 ©2023 Palo Alto Networks, Inc.

0-2,000,000입니다. 기본값은 10,000입니다. (SYN Flood의 경우 발생하는 작업을 선택할 수 있습니다.)

- **Max Rate(connections/s)** - 방화벽이 허용하는 초당 들어오는 연결의 임계값 속도를 지정합니다. 임계값을 초과하면 도착하는 새 연결이 삭제됩니다. (범위는 2-2,000,000이고 기본값은 40,000입니다.)



이 단계의 기본 임계값은 시작점일 뿐이며 네트워크에 적합하지 않을 수 있습니다. 초기 임계값을 적절하게 설정하려면 네트워크의 동작을 분석해야 합니다.

6. 각 플러드 탭에서 방화벽이 이 프로파일을 참조하는 DoS 보호 정책 규칙과 일치하는 패킷을 차단하는 시간인 차단 기간(초)을 지정합니다. 0보다 큰 값을 지정하십시오. 범위는 1-21,600입니다. 기본값은 300입니다.



공격 트래픽으로 잘못 식별한 패킷이 불필요하게 차단될 염려가 있는 경우 낮은 차단 기간 값을 설정하십시오.

공격의 일부가 아닌 패킷을 잘못 차단하는 것보다 볼류메트릭 공격을 차단하는 것이 더 우려되는 경우 차단 기간 값을 높게 설정하십시오.

7. 확인을 클릭합니다.

**STEP 3 |** 들어오는 트래픽을 일치시키기 위한 기준을 지정하는 DoS 보호 정책 규칙을 구성합니다.



방화벽 리소스는 유한하므로 ***DoS*** 보호 정책 규칙과 일치하는 고유한 ***IP*** 주소가 현저히 많을 수 있기 때문에 인터넷 연결 영역에서 원본 주소를 사용하여 분류하고 싶지 않을 것입니다. 많은 카운터가 필요하고 방화벽에서 추적 리소스가 부족합니다. 대신 대상 주소(보호 중인 서버 대상)를 사용하여 분류하는 ***DoS*** 보호 정책 규칙을 정의하십시오.

1. 일반 탭에서 정책 > **DoS** 보호를 선택한 다음 이름 추가를 선택합니다. 이름은 대소문자를 구분하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함하여 최대 31자까지 가능합니다.
2. 소스 탭에서 유형을 영역 또는 인터페이스로 선택한 다음 영역 또는 인터페이스를 추가합니다. 배포 및 보호하려는 대상에 따라 영역 또는 인터페이스를 선택합니다. 예를 들어 방화벽에 들어오는 인터페이스가 하나만 있는 경우 인터페이스를 선택합니다.
3. (선택 사항) 소스 주소에서 규칙과 일치하는 들어오는 IP 주소에 대해 모두를 선택하거나 지리적 지역과 같은 주소 개체 추가를 선택합니다.
4. (선택 사항) 소스 사용자에 대해 임의를 선택하거나 사용자를 지정합니다.
5. (선택 사항) 지정한 소스를 제외한 모든 소스와 일치시키려면 부정을 선택합니다.
6. (선택 사항) 대상 탭에서 유형을 영역 또는 인터페이스로 선택한 다음 대상 영역 또는 인터페이스를 추가합니다. 예를 들어 보호할 보안 영역을 입력합니다.
7. (선택 사항) 대상 주소에서 모두를 선택하거나 보호할 디바이스의 IP 주소를 입력합니다.
8. (선택 사항) 옵션/보호 탭에서 서비스를 추가합니다. 서비스를 선택하거나 서비스를 클릭하고 이름을 입력합니다. **TCP** 또는 **UDP**를 선택합니다. 대상 포트를 입력합니다. 특정 서비스를 지정하


©2023 Palo Alto Networks, Inc.

지 않으면 규칙이 애플리케이션별 포트에 관계없이 모든 프로토콜 유형의 플러드와 일치하도록 허용합니다.

9. 옵션/보호 탭에서 작업에 대해 보호를 선택합니다.
10. 분류됨을 선택합니다.
11. 프로파일에서 생성한 **DoS** 보호 프로파일의 이름을 선택합니다.
12. 주소에 대해 규칙이 적용되는 IP 주소 유형을 결정하는 **source-ip-only** 또는 **src-dest-ip-both**를 선택합니다. 방화벽에서 문제가 되는 트래픽을 식별하는 방법에 따라 설정을 선택합니다.
    - 방화벽이 소스 IP 주소에 대해서만 분류하도록 하려면 **source-ip-only**를 지정하십시오. 공격자는 호스트가 공격할 수 있도록 전체 네트워크를 테스트하는 경우가 많기 때문에 보다 광범위한 검사를 위한 일반적인 설정은 **source-ip-only**입니다.
    - 특정 대상 주소가 있는 서버에서만 DoS 공격으로부터 보호하고 모든 소스 IP 주소가 해당 서버에 대한 특정 cps 임계값을 초과하지 않도록 하려면 **src-dest-ip-both**를 지정하십시오.
13. 확인을 클릭합니다.

**STEP 4 |** 커밋합니다.

커밋을 클릭합니다.

## 단일 세션 DoS 공격 종료

단일 세션 DoS 공격을 완화하려면 새 세션 플러딩에 대한 DoS 방어를 미리 구성해야 합니다. 기능을 구성한 후 어느 시점에서 DoS 공격(해당 세션의 IP 주소에서)이 진행 중임을 인지하기 전에 세션이 설정될 수 있습니다. 단일 세션 DoS 공격이 보이면 다음 작업을 수행하여 세션을 종료하십시오. 그러면 해당 IP 주소에서의 후속 연결 시도가 새 세션 플러딩에 대한 DoS 방어를 트리거합니다.

**STEP 1 |** 공격을 일으키는 소스 IP 주소를 식별합니다.

예를 들어 대상 필터와 함께 방화벽 패킷 캡처 기능을 사용하여 대상 IP 주소로 가는 트래픽의 샘플을 수집합니다. 또는 ACC를 사용하여 대상 주소를 필터링하여 공격 대상 호스트에 대한 활동을 확인합니다.

**STEP 2 |** 공격 임계값을 초과한 후 공격자의 IP 주소를 차단하는 DoS 방어 정책 규칙을 생성합니다.

**STEP 3 |** 소스 IP 주소와 공격 트래픽을 거부하는 보안 정책 규칙을 생성합니다.


©2023 Palo Alto Networks, Inc.

**STEP 4 |** **clear session all filter source <*ip-address*>** 운영 명령을 실행하여 공격하는 소스 IP 주소의 기존 공격을 종료합니다.

또는 세션 ID를 알고 있는 경우 **clear session id <*value*>** 명령을 실행하여 해당 세션만 종료할 수 있습니다.

> ***clear session all filter source <ip-address>*** 명령을 사용하면 원본 *IP* 주소와 일치하는 모든 세션이 삭제되며 여기에는 양호한 세션과 나쁜 세션이 모두 포함될 수 있습니다.

기존 공격 세션을 종료한 후 공격 세션을 형성하려는 모든 후속 시도는 보안 정책에 의해 차단됩니다. DoS 방어 정책은 모든 연결 시도를 임계값으로 계산합니다. 최대 속도 임계값을 초과하면 다중 세션 DoS 공격에 설명된 대로 차단 기간 동안 소스 IP 주소가 차단됩니다.

## 온칩 패킷 디스크립터를 과하게 사용하는 세션 식별

방화벽이 리소스 고갈의 징후를 보이는 경우 압도적인 수의 패킷을 보내는 공격이 발생할 수 있습니다. 이러한 이벤트에서 방화벽은 인바운드 패킷을 버퍼링하기 시작합니다. 온칩 패킷 디스크립터의 과도한 백분율을 사용하는 세션을 신속하게 식별하고 이를 삭제하여 영향을 완화할 수 있습니다.

하드웨어 기반 방화벽 모델(VM-Series 방화벽이 아님)에서 다음 작업을 수행하여 각 슬롯 및 데이터플레인, 사용된 온칩 패킷 디스크립터 비율, 온칩 패킷 디스크립터의 2% 이상을 사용하는 상위 5개 세션 및 해당 세션과 연결된 소스 IP 주소를 식별합니다. 해당 정보를 사용하면 적절한 조치를 취할 수 있습니다.

**STEP 1 |** 방화벽 리소스 사용량, 상위 세션 및 세션 세부 정보를 봅니다. CLI에서 다음 운영 명령을 실행합니다(명령의 샘플 출력은 다음과 같습니다).

```
admin@PA-7050> show running resource-monitor ingress-
backlogs -- SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 92% TOTAL:
 93% TOP SESSIONS:SESS-ID      PCT   GRP-ID   COUNT
 6            92%   1        156                 7        1732
 SESSION DETAILS SESS-
ID PROTO SZONESRC       SPORT  DST       DPORT  IGR-IF    EGR-
IF       APP
 6    6     trust 192.168.2.35 55653  10.1.8.89 80  ethernet1/21
 ethernet1/22 undecided
```

명령은 각각 온칩 패킷 디스크립터의 2% 이상을 사용하는 상위 5개 세션의 최대를 표시합니다.

위의 샘플 출력은 세션 6이 소스 IP 주소 192.168.2.35에서 오는 TCP 패킷(프로토콜 6)을 사용하여 온칩 패킷 디스크립터의 92%를 사용하고 있음을 나타냅니다.

- **SESS-ID** - 다른 모든 **show session** 명령에 사용되는 전역 세션 ID를 나타냅니다. 전역 세션 ID는 방화벽 내에서 고유합니다.
- **GRP-ID** - 패킷 처리의 내부 단계를 나타냅니다.
- **COUNT** - 해당 세션의 GRP ID에 있는 패킷 수를 나타냅니다.
- **APP** - 세션 정보에서 추출한 앱 ID를 나타내므로 트래픽이 합법적인지의 여부를 결정하는 데 도움이 될 수 있습니다. 예를 들어 패킷이 일반적인 TCP 또는 UDP 포트를 사용하지만 CLI 출력이 **미정**의 앱을 나타내는 경우 패킷이 트래픽을 공격할 수 있습니다. 애플리케이션 IP 디코더가 애플리케이션을 결정하기에 충분한 정보를 얻을 수 없을 때 APP은 **미정**입니다. APP가 **unknown**이면 애플

 ©2023 Palo Alto Networks, Inc.

리케이션 IP 디코더가 애플리케이션을 결정할 수 없음을 나타냅니다. 이 경우, 높은 비율의 온칩 패킷 설명자를 사용하는 **unknown** APP 세션도 의심스럽습니다.

디스플레이 출력을 제한하려면 다음을 수행합니다.

PA-7000 시리즈 모델에서만 출력을 슬롯, 데이터플레인 또는 둘 다로 제한할 수 있습니다. 예:

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot
 s1 admin@PA-7050> show running resource-monitor ingress-backlogs
 slot s1 dp dp1
```

PA-5200 시리즈 및 PA-7000 시리즈 모델에서만 출력을 데이터플레인으로 제한할 수 있습니다. 예:

```
admin@PA-5260> show running resource-monitor ingress-backlogs dp
 dp1
```

**STEP 2 |** 명령 출력을 사용하여 온칩 패킷 디스크립터의 높은 백분율을 사용하여 소스 IP 주소의 소스가 합법적인 트래픽을 전송하는지 또는 공격 트래픽을 전송하는지의 여부를 결정합니다.

위의 샘플 출력에서 단일 세션 공격이 발생할 수 있습니다. 단일 세션(세션 ID 6)은 슬롯 1, DP 1에 대해 온칩 패킷 설명자의 92%를 사용하고 있으며 해당 시점의 애플리케이션은 미정입니다.

- 단일 사용자가 공격을 보내고 있고 트래픽이 오프로드되지 않은 경우 단일 세션 DoS 공격을 종료할 수 있습니다. 최소한 새 세션의 플러드에 대해 DoS 방어를 구성할 수 있습니다.
- 필드 프로그래밍이 가능한 게이트 어레이(FPGA)가 있는 하드웨어 모델에서 방화벽은 가능한 경우 FPGA로 트래픽을 오프로드하여 성능을 향상시킵니다. 트래픽이 하드웨어로 오프로드되는 경우 패

 ©2023 Palo Alto Networks, Inc.

킷의 공세를 처리해야 하는 소프트웨어이기 때문에 세션을 지우는 것은 도움이 되지 않습니다. 대신 커밋 없이 세션을 폐기해야 합니다.

세션이 오프로드되었는지 여부를 확인하려면 다음 예와 같이 CLI에서 **show session id *<session-id>*** 작업 명령을 사용합니다. layer7processing 값은 오프로드된 세션에 대해 **완료**되었거나 오프로드되지 않은 세션에 대해 **활성화됨**을 나타냅니다.

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```

**show session id *<session-id>*** 명령 출력이 다음과 유사한 정보를 표시하는 경우 출력은 세션이 아직 PAN-OS 방화벽에 설치되지 않았음을 의미합니다. 이러한 일이 발생할 수 있는 이유 중 하나는 구성된 보안 정책 규칙으로 인해 트래픽이 거부되기 때문입니다.

```
> show session id xxxxxxxxxx

Session xxxxxxxxxx

Bad Key: c2s:  'c2s'

Bad Key: s2c:  's2c'
```

 ©2023 Palo Alto Networks, Inc.

```
index(local): : yyyyyyy
```

## 커밋 없이 세션 삭제

이 작업을 수행하면 패킷 버퍼 또는 온칩 패킷 디스크립터에 과부하가 걸리는 세션과 같은 세션을 영구적으로 삭제합니다. 커밋이 필요하지 않습니다. 세션은 명령을 실행한 직후에 삭제됩니다. 명령은 오프로드된 세션과 오프로드되지 않은 세션 모두에 적용됩니다.

**STEP 1 |** CLI에서 하드웨어 모델에 대해 다음 작업 명령을 실행합니다.

```
admin@PA-7050> request session-discard [timeout <seconds>]
 [reason <reason-string>] id <session-id>
```

기본 타임아웃는 3,600초입니다.

**STEP 2 |** 세션이 삭제되었는지 확인합니다.

```
admin@PA-7050> show session all filter state discard
```


©2023 Palo Alto Networks, Inc.

# 인증

다음 항목에서는 표준 보안 보장 및 기능 집합을 보장하는 보안 인증인 일반 기준 및 연방 정보 처리 표준 140-2(FIPS 140-2)를 지원하도록 Palo Alto Networks® 방화벽 및 어플라이언스를 구성하는 방법에 대해 설명합니다. 이러한 인증은 민간 미국 정부 기관 및 정부 계약 업체에서 요구하는 경우가 많습니다.

제품 인증 및 타사 유효성 검사에 대한 자세한 내용은 인증 페이지를 참조하십시오.

- FIPS 및 공통 기준 지원 활성화
- FIPS-CC 보안 기능
- FIPS-CC 모드에서 방화벽 또는 어플라이언스의 스왑 메모리 스크럽

# FIPS 및 공통 기준 지원 활성화

다음 절차를 사용하여 공통 기준 및 연방 정보 처리 표준 140-2(FIPS 140-2)를 지원하는 소프트웨어 버전에서 FIPS-CC 모드를 사용하도록 설정합니다. FIPS-CC 모드를 사용하도록 설정하면 모든 FIPS 및 CC 기능이 포함됩니다.

FIPS-CC 모드는 VM 시리즈 방화벽을 포함한 모든 Palo Alto Networks 차세대 방화벽 및 어플라이언스에서 지원됩니다. FIPS-CC 모드를 활성화하려면 먼저 방화벽을 MRT(유지 관리 복구 도구)로 부팅한 다음 작동 모드를 일반 모드에서 FIPS-CC 모드로 변경합니다. 작동 모드를 변경하는 절차는 모든 방화벽 및 어플라이언스마다 동일하지만 MRT에 액세스하는 절차는 다릅니다.

***FIPS-CC*** 모드를 사용하도록 설정하면 방화벽이 공장 기본 설정으로 재설정되고 모든 구성이 제거됩니다.

- 유지 보수 복구 도구(MRT)에 액세스
- 작동 모드를 FIPS-CC 모드로 변경

## 유지 보수 복구 도구(MRT)에 액세스

MRT(유지 관리 복구 도구)를 사용하면 Palo Alto Networks 방화벽 및 어플라이언스에서 여러 작업을 수행할 수 있습니다. 예를 들어, 방화벽 또는 어플라이언스를 공장 기본 설정으로 되돌리고, PAN-OS 또는 콘텐츠 업데이트를 이전 버전으로 되돌리며, 파일 시스템에서 진단을 실행하고, 시스템 정보를 수집하고, 로그를 추출할 수 있습니다. 또한 MRT를 사용하여 작동 모드를 FIPS-CC 모드로 또는 FIPS-CC 모드에서 일반 모드로 변경할 수 있습니다.

다음 절차에서는 다양한 Palo Alto Networks 제품에서 유지 관리 복구 도구(MRT)에 액세스하는 방법을 설명합니다.


©2023 Palo Alto Networks, Inc.

- 하드웨어 방화벽 및 어플라이언스(예: PA-220 방화벽, PA-7000 시리즈 방화벽 또는 M-시리즈 어플라이언스)에서 MRT에 액세스합니다.
  1. 방화벽 또는 어플라이언스에 대한 직렬 콘솔 세션을 설정합니다.
     1. 컴퓨터의 직렬 포트에서 방화벽이나 어플라이언스의 콘솔 포트로 직렬 케이블을 연결합니다.

        컴퓨터에 *9*핀 직렬 포트가 없지만 *USB* 포트가 있는 경우 직렬-*USB* 변환기를 사용하여 연결을 설정합니다. 방화벽에 마이크로 USB 콘솔 포트가 있는 경우 표준 *Type-A USB*-마이크로 *USB* 케이블을 사용하여 포트에 연결합니다.
     2. 컴퓨터에서 터미널 에뮬레이션 소프트웨어를 열고 9600-8-N-1로 설정한 다음 적절한 COM 포트에 연결합니다.

        *Windows* 시스템에서 제어판으로 이동하여 디바이스 및 프린터에 대한 *COM* 포트 설정을 보고 콘솔에 할당된 *COM* 포트를 확인할 수 있습니다.
     3. 관리자 계정을 사용하여 로그인합니다. (기본 사용자 이름/비밀번호는 admin/admin입니다.)
  2. 다음 CLI 명령을 입력하고 **y**를 눌러 확인합니다.

     ```
     디버그 시스템 유지 관리 모드
     ```
  3. 방화벽이나 어플라이언스가 MRT 시작 화면으로 부팅된 후(약 2~3분) MRT 기본 메뉴에 액세스하려면 **계속**에서 Enter 키를 누릅니다.

     방화벽이나 어플라이언스를 재부팅하고 유지 관리 모드 프롬프트에서 ***maint***를 입력하여 *MRT*에 액세스할 수도 있습니다. 직접 직렬 콘솔 연결이 필요합니다.

     방화벽 또는 어플라이언스가 MRT로 부팅된 후 관리(MGT) 인터페이스 IP 주소에 대한 SSH 연결을 설정하여 MRT에 원격으로 액세스할 수 있습니다. 로그인 프롬프트에서 사용자 이름으로 **maint**를 입력하고 암호로 방화벽 또는 어플라이언스 일련번호를 입력합니다.

- 프라이빗 클라우드(예: VMware ESXi 또는 KVM 하이퍼바이저)에 배포된 VM 시리즈 방화벽의 MRT에 액세스합니다.
  1. 방화벽의 관리 IP 주소에 SSH 세션을 설정하고 관리자 계정으로 로그인합니다.
  2. 다음 CLI 명령을 입력하고 **y**를 눌러 확인합니다.

     ```
     디버그 시스템 유지 관리 모드
     ```

     방화벽이 *MRT*로 부팅하는 데 약 *2~3*분이 소요됩니다. 이 시간 동안 *SSH* 세션의 연결이 끊어집니다.
  3. 방화벽이 MRT 시작 화면으로 부팅된 후 작동 모드에 따라 로그인합니다.
     - 일반 모드 - 방화벽의 관리 IP 주소에 대한 SSH 세션을 설정하고 **maint**를 사용자 이름으로 사용하고 방화벽 또는 어플라이언스 일련번호를 암호로 사용하여 로그인합니다.
     - **FIPS-CC** 모드 - 가상 머신 관리 유틸리티(예: vSphere 클라이언트)에 액세스하고 가상 머신 콘솔에 연결합니다.
  4. MRT 시작 화면의 **계속**에서 Enter를 눌러 MRT 기본 메뉴에 액세스합니다.


©2023 Palo Alto Networks, Inc.

- 퍼블릭 클라우드(예: AWS 또는 Azure)에 배포된 VM 시리즈 방화벽의 MRT에 액세스합니다.
  1. 방화벽의 관리 IP 주소에 SSH 세션을 설정하고 관리자 계정으로 로그인합니다.
  2. 다음 CLI 명령을 입력하고 **y**를 눌러 확인합니다.

     ```
     디버그 시스템 유지 관리 모드
     ```

     방화벽이 *MRT*로 부팅하는 데 약 *2~3*분이 소요됩니다. 이 시간 동안 *SSH* 세션의 연결이 끊어집니다.
  3. 방화벽이 MRT 시작 화면으로 부팅된 후 가상 머신 유형에 따라 로그인합니다.
     - **AWS** - **ec2-user**로 로그인하고 가상 머신을 배포할 때 연결된 SSH 퍼블릭 키를 선택합니다.
     - **Azure** - VM 시리즈 방화벽을 배포할 때 생성한 자격 증명을 입력합니다.
     - **GCP** - **gcp-user**로 로그인하고 가상 머신을 배포할 때 연결된 SSH 공개 키를 선택합니다.
  4. MRT 시작 화면의 **계속**에서 Enter를 눌러 MRT 기본 메뉴에 액세스합니다.

## 작동 모드를 FIPS-CC 모드로 변경

다음 절차는 Palo Alto Networks 제품의 작동 모드를 일반 모드에서 FIPS-CC 모드로 변경하는 방법을 설명합니다.

어플라이언스가 *FIPS-CC* 모드에 있으면 관리 인터페이스 설정을 포함하여 콘솔을 통해 설정을 구성할 수 없습니다. *FIPS-CC* 모드를 사용하도록 설정하기 전에 *SSH* 또는 웹 인터페이스를 통해 관리 인터페이스에 액세스할 수 있도록 네트워크가 설정되어 있는지 확인합니다. 관리 인터페이스는 *PA* 시리즈 방화벽을 사용하는 경우 *192.168.1.1*의 정적 주소또는 *VM*-시리즈 방화벽인 경우 *DHCP*를 통해 검색된 주소로 기본값으로 유지됩니다. 와일드 파이어, 가상 *Panorama* 및 *M* 시리즈 *Panorama* 어플라이언스가 기본값으로 *192.168.1.1*의 정적 주소로 표시됩니다.

*FIPS-CC* 모드를 사용하도록 설정하면 모든 구성 및 설정이 지워집니다. 관리자가 *FIPS-CC* 모드를 사용하도록 설정한 후 다시 사용하려는 구성이나 설정이 있는 경우 관리자는 *FIPS-CC* 모드로 변경하기 전에 구성을 저장하고 내보낼 수 있습니다. 그런 다음 운영 모드 변경이 완료되면 구성을 가져올 수 있습니다. 불러온 구성은 가져오기 프로세스에 따라 FIPS-CC 보안 기능 단위로 편집되거나 가져오기 프로세스가 실패하게 됩니다.

키, 암호 및 기타 중요한 보안 매개변수는 모드에서 공유할 수 없습니다.

*Panorama* 관리 서버에서 관리하는 방화벽 또는 전용 로그 수집기의 작동 모드를 *FIPS-CC* 모드로 변경하는 경우 *Panorama*의 운영 모드를 *FIPS-CC* 모드로 변경해야 합니다. *Panorama*에서 푸시된 로컬 관리자 암호에 대한 암호 해시를 보호하는 데 필요합니다.


©2023 Palo Alto Networks, Inc.

**STEP 1 |** (기존 HA 구성에만 해당) 고가용성(HA) 구성을 사용하지 않도록 설정합니다.

이는 HA 구성에 이미 있는 방화벽에 대해 작동 모드를 FIPS-CC 모드로 성공적으로 변경하는 데 필요합니다.

1. 기본 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 일반을 선택하고 HA 쌍 설정 설정을 편집합니다.
3. **HA** 활성화를 선택 취소(비활성화)하고 확인을 클릭합니다.
4. 커밋합니다.

**STEP 2 |** (퍼블릭 클라우드 VM 시리즈 방화벽 또는 퍼블릭 클라우드 Panorama 가상 어플라이언스만 해당) SSH 키를 만들고 방화벽 또는 Panorama에 로그인합니다.

Microsoft Azure와 같은 일부 공용 클라우드 플랫폼에서는 FIPS-CC 모드로 변경한 후 인증 오류를 방지하기 위해 SSH 키가 있어야 합니다. SSH 키를 사용하여 인증하기 위해 방화벽을 배포했는지 확인합니다. Azure에서는 VM-시리즈 방화벽 또는 Panorama를 배포하고 사용자 이름과 암호를 사용하여 로그인할 수 있지만 운영 모드를 FIPS-CC로 변경한 후 사용자 이름과 암호를 사용하여 인증할 수 없습니다. FIPS-CC 모드로 재설정한 후 로그인하려면 SSH 키를 사용해야 하며 이후에 방화벽 웹 인터페이스에 로그인하는 데 사용할 수 있는 사용자 이름과 암호를 구성할 수 있습니다.

**STEP 3 |** 방화벽 또는 어플라이언스 및 유지 보수 복구 도구(MRT)에 액세스에 연결.

**STEP 4 |** 메뉴에서 **FIPS-CC 모드** 설정을 선택합니다.

**STEP 5 |** **FIPS-CC 모드 활성화**를 선택합니다. 모드 변경 작업은 전체 공장 재설정을 시작하고 상태 표시기가 진행률을 표시합니다. 모드 변경이 완료되면 상태가 **Success**로 표시됩니다.



모든 구성 및 설정이 지워지고 모드 변경이 완료되면 검색할 수 없습니다.

**STEP 6 |** 메시지가 표시되면 **재부팅**을 선택합니다.



퍼블릭 클라우드에 배포된 *VM* 시리즈 방화벽의 작동 모드를 변경하고 **재부팅**할 수 있기 전에 *MRT*에 대한 *SSH* 연결이 끊긴 경우 모드 변경을 위해 *10-15*분을 기다려야 합니다. 완료하려면 *MRT*에 다시 로그인한 다음 방화벽을 재부팅하여 작업을 완료하십시오. *FIPS-CC* 모드로 재설정한 후 일부 가상 폼 팩터*(Panorama* 또는 *VM-Series)*에서 *SSH* 키만 사용하여 로그인할 수 있으며 *SSH* 키를 사용하여 인증을 설정하지 않은 경우 재부팅 시 방화벽에 더 이상 로그인할 수 없습니다.

FIPS-CC 모드로 전환하면 다음 상태가 표시됩니다. **FIPS-CC mode enabled successfully**.

또한 다음과 같은 변경 사항은 다음과 같습니다.

- FIPS-CC는 웹 인터페이스 하단의 상태 표시줄에서 항상 표시됩니다.
- 기본 관리자 로그인 자격 증명은 admin/paloalto로 변경됩니다.

FIPS-CC 모드에서 시행되는 보안 기능에 대한 자세한 내용은 FIPS-CC 보안 기능을(를) 참조하십시오.

 ©2023 Palo Alto Networks, Inc.

**STEP 7 |** (기존 HA에만 해당) HA를 다시 사용하도록 설정합니다.

이 단계는 FIPS-CC 모드로 변경하기 전에 HA에서 구성된 방화벽에 필요합니다.

HA를 처음 설정하는 방법에 대한 자세한 내용은 고가용성을 참조하십시오.

1. 기본 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 일반을 선택하고 HA 쌍 설정 설정을 편집합니다.
3. **HA** 활성화를 선택(활성화)하고 확인을 클릭합니다.
4. 커밋합니다.

**STEP 8 |** HA1 제어 링크에 대한 암호화를 활성화합니다.

이는 HA 구성에서 FIPS-CC 모드의 모든 방화벽에 필요합니다.

FIPS-CC 모드에서 방화벽에 HA를 성공적으로 활용하려면 자동 키 재지정 매개변수를 설정해야 하며 데이터 매개변수를 1000MB를 넘지 않는 값으로 설정해야 합니다. 키를 기본값으로 설정할 수 없으며 시간 간격을 설정해야 합니다(사용하지 않도록 설정할 수 없음).


©2023 Palo Alto Networks, Inc.

# FIPS-CC 보안 기능

FIPS-CC 모드가 활성화되면 모든 방화벽 및 어플라이언스에 다음 보안 기능이 적용됩니다.

- 로그인하려면 브라우저가 TLS 1.2(또는 그 이상)과 호환되어야 합니다. WF-500 어플라이언스에서는 CLI를 통해서만 어플라이언스를 관리하고 SSHv2 호환 클라이언트 애플리케이션을 사용하여 연결해야 합니다.
- 모든 암호는 8자 이상이어야 합니다.
- 인증 설정에서 실패한 시도 및 잠금 시간**(분)**이 0보다 큰지 확인해야 합니다. 관리자가 실패한 시도 임계값에 도달하면 관리자는 잠금 시간**(분)** 필드에 정의된 기간 동안 잠깁니다.
- 인증 설정에서 **Idle Timeout**이 0보다 큰지 확인해야 합니다. 로그인 세션이 지정된 시간 이상 유휴 상태인 경우 관리자는 자동으로 로그아웃됩니다.
- 절대 세션 길이를 구성하여 사용자가 로그인할 수 있는 최대 시간(분)을 설정할 수 있습니다. 설정할 수 있는 최소 길이는 60분입니다. 타임아웃 5분 전에 세션 종료 경고를 받게 됩니다. 이 기능은 FIPS-CC 모드에서 비활성화할 수 없으며 30일 세션에서 기본값이 설정됩니다.
- 최대 세션 수를 구성하여 동일한 관리자 계정에 동시에 로그인할 수 있는 사용자 수를 설정할 수 있습니다.
- 방화벽 또는 어플라이언스는 적절한 수준의 자체 테스트를 자동으로 결정하고 암호화 알고리즘 및 암호 제품군에서 적절한 수준의 강도를 적용합니다.
- 승인되지 않은 FIPS-CC 알고리즘은 복호화되지 않으며 복호화 중에 무시됩니다.
- MS-CHAPv2는 FIPS-CC 모드와 호환되지 않습니다. TLS와 함께 RADIUS를 사용하는 것이 좋습니다.
- IPSec VPN을 구성할 때 관리자는 IPSec 설정 중에 제공되는 암호 제품군 옵션을 선택해야 합니다.
- (Panorama 및 WildFire만 해당) 관리 인터페이스에서 IPSec을 활성화하여 NTP, RADIUS, TACACS 및 DNS와 같은 프로토콜을 보호할 수 있습니다.
- 자체 생성 및 가져온 인증서에는 RSA 2,048비트(또는 그 이상) 또는 ECDSA 256비트(또는 그 이상)인 공개 키가 포함되어야 합니다. 또한 SHA256 이상의 다이제스트를 사용해야 합니다.
- Telnet, TFTP 및 HTTP 관리 연결은 사용할 수 없습니다.
- (새 HA 배포) FIPS-CC 모드에서 방화벽에 대한 고가용성(HA)을 설정할 때 HA1 제어 링크에 대한 암호화를 활성화해야 합니다. 자동 재입력 매개변수를 설정해야 합니다. 데이터 매개변수를 1000MB 이하의 값으로 설정해야 하고(기본값으로 둘 수 없음) 시간 인터벌을 설정해야 합니다(비활성화 상태로 둘 수 없음).
- (기존 HA 배포) 고가용성(HA) 구성의 방화벽에 대해 작동 모드를 FIPS-CC 모드로 변경하기 전에, 작동 모드를 FIPS-CC 모드로 변경하기 전 먼저 HA(디바이스 > 고가용성 > 일반)를 비활성화해야 합니다.

  두 HA 피어 모두에 대해 작동 모드를 FIPS-CC 모드로 변경한 후 위에서 설명한 대로 HA를 다시 활성화하고 HA1 제어 링크에 대한 암호화를 활성화합니다.
- FIPS-CC 모드의 직렬 콘솔 포트는 제한된 상태 출력 포트로만 기능합니다. CLI 액세스를 사용할 수 없습니다.
- MRT로 부팅된 하드웨어 및 프라이빗 클라우드 VM 시리즈 방화벽의 직렬 콘솔 포트는 MRT에 대한 대화형 액세스를 제공합니다.


©2023 Palo Alto Networks, Inc.

- MRT로 부팅된 하이퍼바이저 환경 프라이빗 클라우드 VM 시리즈 방화벽에서는 대화형 콘솔 액세스가 지원되지 않습니다. SSH를 통해서만 MRT에 액세스할 수 있습니다.
- 이전 마스터 키가 만료되기 전에 새 마스터 키를 수동형으로 구성해야 합니다. 자동 갱신 마스터 키는 FIPS-CC 모드에서 지원되지 않습니다.

  마스터 키가 만료되면 방화벽 또는 Panorama가 유지 관리 모드에서 자동으로 재부팅됩니다. 그런 다음 방화벽을 공장 기본 설정으로 재설정해야합니다.
- FIPS-CC 모드가 활성화된 경우 팔로 알토 네트워크 방화벽에서 ZTP(제로 터치 프로비저닝) 모드가 비활성화됩니다.
- (Panorama 관리 디바이스) FIPS-CC를 사용하도록 설정한 경우 방화벽 및 로그 수집기의 Panorama 지원을 검토합니다.

| Panorama | 방화벽 | | 로그 수집기 | |
|---|---|---|---|---|
| FIPS-CC 사용 가능 | FIPS-CC 사용 가능 | FIPS-CC 비활성화 | FIPS-CC 사용 가능 | FIPS-CC 비활성화 |
| | 지원됨 | 지원됨 | 지원됨 | 지원됨 |
| FIPS-CC 비활성화 | 지원되지 않음 | 지원됨 | 지원되지 않음 | 지원됨 |

- (Panorama 관리형 디바이스) FIPS-CC 모드에서 Panorama 및 관리되는 기기를 PAN-OS 10.2 이상 릴리스로 업그레이드하려면 PAN-OS 10.2 릴리스를 실행하는 동안 Panorama 관리에 추가된 경우 FIPS-CC 모드에서 기기의 보안 연결 상태를 재설정해야 합니다.

  자세한 내용은 FIPS-CC 모드에서 Panorama 및 관리 기기 업그레이드를 참조하십시오.
- (PA-7000 시리즈 방화벽만 해당) Palo Alto Networks 하드웨어 단종 날짜 및 호환성 매트릭스를 검토하여 지원되는 라인 카드가 있는지 확인하십시오. 수명 종료에 도달했거나 지원되지 않는 PAN-OS 릴리스를 실행 중인 라인 카드로 인해 PA-7000 시리즈 방화벽이 유지 보수 모드로 전환될 수 있습니다.


©2023 Palo Alto Networks, Inc.

# FIPS-CC 모드에서 실행되는 방화벽 또는 어플라이언스에서 스왑 메모리 스크럽

방화벽이나 어플라이언스를 폐기하기 전(FIPS-CC 모드에서)이나 수리를 위해 보내기 전에 스왑 메모리에서 민감한 정보가 제거되었는지 확인해야 합니다. 다음 절차에 따라 스왑 파티션에서 모든 CSP(암호화 보안 매개 변수) 정보를 제거하십시오.

복구를 위해 *Panorama*가 관리하는 방화벽을 보내는 경우 RMA 방화벽 교체를 시작하기 전을 참조하십시오.

**STEP 1 |** 방화벽 또는 어플라이언스에 대한 SSH 관리 세션을 엽니다.

**STEP 2 |** 다음 운영 명령을 실행합니다.

```
request [restart | shutdown] system with-swap-scrub [dod | nnsa]
```

예를 들어 방화벽 또는 어플라이언스를 종료하고 DoD(Department of Defense) 스크럽을 수행하려면 다음 명령을 실행합니다.

```
request shutdown system with-swap-scrub dod
```

**STEP 3 |** 경고 프롬프트에서 **Y**를 눌러 스크럽을 시작합니다.

**STEP 4 |** 스크럽이 성공적으로 완료되었는지 확인합니다. swap이라는 단어에 대한 시스템 로그 및 필터를 봅니다. 시스템 로그는 각 스왑 파티션(모델에 따라 하나 또는 두 개의 파티션)의 스크럽 상태를 나타내며 전체 스크럽 상태를 나타내는 로그 항목도 표시합니다. 모든 스왑 파티션에서 스크럽이 성공적으로 완료되면 시스템 로그에 `스왑 공간 스크럽이 성공`했음을 표시합니다.

하나 이상의 스왑 파티션에서 스크럽이 실패하면 시스템 로그에 `스왑 공간 스크럽이 실패`했음을 표시합니다. 다음 화면 캡처는 두 개의 파티션이 있는 방화벽에 대한 로그 결과를 보여 줍니다.

| | | | | | |
|---|---|---|---|---|---|
| 06/08 10:24:02 | general | medium | general | | Swap space scrub was successful |
| 06/08 10:24:02 | general | medium | general | | Scrub performed on swap space /opt/panlogs /.secondary_swapfile |
| 06/08 10:24:02 | general | medium | general | | Scrub performed on swap space /dev/sda7 |

*CLI*를 사용하여 스크럽 로그를 보려면 `로그 시스템 표시 | 일치 스왑` 명령을 실행합니다.

셧다운 명령을 사용하여 스크럽을 시작하면 스크럽이 완료된 후 방화벽 또는 어플라이언스의 전원이 꺼집니다. 방화벽이나 어플라이언스의 전원을 켜려면 먼저 전원을 분리했다가 다시 연결해야 합니다.


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.