paloalto TECHDOCS

PAN-OS 웹 인터페이스 도움말

11.0

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

Last Revised

March 28, 2023

Table of Contents

웹 인터페이스 기본

다음 항목에서는 방화벽에 대한 개요를 제공하고 기본 관리 작업에 대해 설명합니다.

방화벽 개요

Palo Alto Networks® 차세대 방화벽은 모든 트래픽(애플리케이션, 위협, 콘텐츠 포함)을 검사하고 위치나 디바이스 유형에 관계없이 해당 트래픽을 사용자에게 연결합니다. 비즈니스를 실행하는 요소인 사용자, 애플리케이션 및 콘텐츠는 엔터프라이즈 보안 정책의 필수 구성 요소가 됩니다. 이를 통해 보안을 비즈니스 정책에 맞출 수 있을 뿐만 아니라 이해하고 유지 관리하기 쉬운 규칙을 작성할 수 있습니다.

보안 운영 플랫폼의 일부인 차세대 방화벽은 조직에 다음 기능을 제공합니다.

- 포트에 관계없이 모든 트래픽을 분류하여 애플리케이션(Software-as-a-Service 애플리케이션 포함), 사용자 및 콘텐츠를 안전하게 활성화합니다.
- 원하는 모든 애플리케이션을 허용하고 나머지는 모두 차단하여 적극적인 시행 모델을 사용하여 공격의 위험을 줄입니다.
- 보안 정책을 적용하여 알려진 취약점 악용, 바이러스, 랜섬웨어, 스파이웨어, 봇넷 및 지능형 지속 위협과 같은 기타 알려지지 않은 멀웨어를 차단합니다.
- 데이터 및 애플리케이션을 세분화하고 제로 트러스트 원칙을 적용하여 데이터 센터(가상화된 데이터 센터 포함)를 보호하십시오.
- 온프레미스 및 클라우드 환경 전반에 일관된 보안을 적용합니다.
- 사용자와 디바이스가 어디에 있든 보안 운영 플랫폼을 확장하여 보안 모바일 컴퓨팅을 수용합니다.
- 중앙 집중식 가시성을 확보하고 네트워크 보안을 간소화하여 데이터를 실행 가능하게 만들어 성공적인 사이버 공격을 방지할 수 있습니다.
- 불법 웹사이트에 유효한 회사 자격 증명 제출을 중지하고 네트워크 레이어에서 인증 정책을 시행하여 측면 이동 또는 네트워크 손상을 위해 도난당한 자격 증명을 사용하는 공격자의 능력을 무력화하여 자격 증명을 도용하려는 시도를 식별하고 방지합니다.

기능 및 이점

Palo Alto Networks의 차세대 방화벽은 네트워크 액세스가 허용된 트래픽을 세부적으로 제어합니다. 주요 기능 및 이점은 다음과 같습니다.

- 애플리케이션 기반 정책 시행**(App-ID™)** - 애플리케이션 식별이 프로토콜 및 포트 번호 이상을 기반으로 할 때 애플리케이션 유형에 따른 액세스 제어가 훨씬 더 효과적입니다. App-ID 서비스는 파일 공유와 같은 고위험 행위는 물론 고위험 애플리케이션을 차단할 수 있으며 SSL(Secure Sockets Layer) 프로토콜로 암호화된 트래픽을 복호화하고 검사할 수 있습니다.
- 사용자 식별**(User-ID™)** - User-ID 기능을 사용하면 관리자가 네트워크 영역 및 주소 대신 또는 추가로 사용자 및 사용자 그룹을 기반으로 방화벽 정책을 구성하고 시행할 수 있습니다. 방화벽은 Microsoft Active Directory, eDirectory, SunOne, OpenLDAP 및 대부분의 기타 LDAP 기반 디렉토리 서버와 같은 많은 디렉토리 서버와 통신하여 사용자 및 그룹 정보를 방화벽에 제공할 수 있습니다. 그런 다음 사용자 또는 그룹별로 정의할 수 있는 보안 애플리케이션 활성화를 위해 이 정보를 사용할 수 있습니다. 예를 들어, 관리자는 한 조직에서 웹 기반 애플리케이션을 사용하도록 허용하지만 회사의 다른 조직에서는 동일한 애플리케이션을 사용하도록 허용하지 않을 수 있습니다. 사용자 및 그룹을 기반으로 애플리케이션의 특정 구성 요소에 대한 세부적인 제어를 구성할 수도 있습니다(사용자 식별 참조).
- 위협 방지 - 바이러스, 웜, 스파이웨어 및 기타 악성 트래픽으로부터 네트워크를 보호하는 위협 방지 서비스는 애플리케이션 및 트래픽 소스에 따라 다를 수 있습니다(개체 > 보안 프로파일 참조).
- **URL** 필터링 - 아웃바운드 연결을 필터링하여 부적절한 웹사이트에 대한 액세스를 방지할 수 있습니다(개체 > 보안 프로파일 > URL 필터링 참조).
- 트래픽 가시성 - 광범위한 보고서, 로그 및 알림 메커니즘을 통해 네트워크 애플리케이션 트래픽 및 보안 이벤트에 대한 자세한 가시성을 제공합니다. 웹 인터페이스의 ACC(Application Command Center)는 트래픽이 가장 많고 보안 위험이 가장 높은 애플리케이션을 식별합니다(모니터 참조).
- 네트워킹 다양성 및 속도 - Palo Alto Networks 방화벽은 기존 방화벽을 보강하거나 대체할 수 있으며 모든 네트워크에 투명하게 설치하거나 스위치 또는 라우팅 환경을 지원하도록 구성할 수 있습니다. 멀티기가비트 속도와 단일 패스 아키텍처는 네트워크 대기 시간에 거의 또는 전혀 영향을 미치지 않으면서 이러한 서비스를 제공합니다.
- **GlobalProtect** - GlobalProtect™ 소프트웨어는 전 세계 어디에서나 쉽고 안전한 로그인을 허용하여 현장에서 사용되는 랩톱과 같은 클라이언트 시스템에 보안을 제공합니다.
- 페일 세이프 작동 - 고가용성(HA) 지원은 하드웨어 또는 소프트웨어 중단 시 자동 페일오버를 제공합니다(디바이스 > 가상 시스템 참조).
- 멀웨어 분석 및 보고 - WildFire™ 클라우드 기반 분석 서비스는 방화벽을 통과하는 멀웨어에 대한 자세한 분석 및 보고를 제공합니다. AutoFocus™ 위협 인텔리전스 서비스와의 통합을 통해 조직, 산업 및 글로벌 수준에서 네트워크 트래픽과 관련된 위험을 평가할 수 있습니다.
- **VM** 시리즈 방화벽 - VM 시리즈 방화벽은 가상화된 데이터 센터 환경에서 사용하도록 배치된 PAN-OS®의 가상 인스턴스를 제공하며 사설, 공용 및 하이브리드 클라우드 컴퓨팅 환경에 이상적입니다.

- 관리 및 파노라마 - 직관적인 웹 인터페이스 또는 명령줄 인터페이스(CLI)를 통해 각 방화벽을 관리하거나 웹 인터페이스가 있는 Panorama™ 중앙 집중식 관리 시스템을 통해 모든 방화벽을 중앙에서 관리할 수 있으며, 이는 Palo Alto Networks 방화벽의 웹 인터페이스와 매우 유사합니다.

마지막 로그인 시간 및 실패한 로그인 시도

Palo Alto Networks 방화벽 또는 Panorama의 관리 계정과 같은 권한 있는 계정의 오용을 감지하고 악용을 방지하기 위해, 웹 인터페이스 및 명령줄 인터페이스(CLI)는 로그인할 때 사용자 이름에 대한 마지막 로그인 시간과 실패한 로그인 시도를 표시합니다. 이 정보를 통해 누군가가 귀하의 관리 자격 증명을 사용하여 공격을 시작하는지의 여부를 쉽게 식별할 수 있습니다.

웹 인터페이스에 로그인하면 창 왼쪽 하단에 마지막 로그인 시간 정보가 나타납니다. 마지막으로 성공한 로그인 이후에 하나 이상의 로그인 실패가 발생한 경우 마지막 로그인 정보 오른쪽에 주의 아이콘이 나타납니다. 주의 기호 위로 마우스를 가져가면 실패한 로그인 시도 횟수를 보거나 클릭하여 관리 계정 이름, 소스 IP 주소 및 로그인 실패 이유를 나열하는 실패한 로그인 시도 요약 창을 봅니다.

자신의 것으로 인식하지 못하는 로그인 시도가 여러 번 실패한 경우 네트워크 관리자와 협력하여 무차별 대입 공격을 수행하는 시스템을 찾은 다음 사용자와 호스트 컴퓨터를 검토하여 악의적인 활동을 식별하고 근절해야 합니다. 마지막 로그인 날짜 및 시간이 계정 손상을 나타내는 경우 즉시 비밀번호를 변경한 다음 구성 감사를 수행하여 의심스러운 구성 변경이 커밋되었는지 확인해야 합니다. 로그가 지워졌거나 계정을 사용하여 부적절하게 변경되었는지 확인하기 어려운 경우 구성을 알려진 양호한 구성으로 되돌립니다.

오늘의 메시지

사용자나 다른 관리자가 오늘의 메시지를 구성했거나 Palo Alto Networks는 소프트웨어 또는 콘텐츠 릴리스의 일부로 포함된 메시지를 구성한 경우 사용자가 웹 인터페이스에 로그인하면 자동으로 오늘의 메시지 대화 상자가 표시됩니다. 이렇게 하면 사용자가 수행하려는 작업에 영향을 주는 중요한 정보(예: 임박한 시스템 재시작 등)를 볼 수 있습니다.

대화 상자에는 페이지당 하나의 메시지가 표시됩니다. 대화 상자에 다시 표시 안 함을 선택할 수 있는 옵션이 있는 경우 이후 로그인 후 대화 상자를 표시하지 않으려는 각 메시지에 대해 이 옵션을 선택할 수 있습니다.

오늘의 메시지가 변경될 때마다 이전 로그인 시 다시 표시 안 함을 선택했더라도 다음 세션에 메시지가 나타납니다. 이후 세션에서 수정된 메시지가 표시되지 않도록 하려면 이 옵션을 다시 선택해야 합니다.

대화 상자 페이지를 탐색하려면 대화 상자의 측면을 따라 오른쪽( ) 및 왼쪽( ) 화살표를 클릭하거나 대화 상자 아래쪽에 있는 페이지 선택기( )를 클릭합니다. 대화 상자를 닫은 후 웹 인터페이스 하단의 메시지( )를 클릭하여 수동으로 다시 열 수 있습니다.

오늘의 메시지를 구성하려면 디바이스 > 설정 > 관리를 선택한 다음 배너 및 메시지 설정을 편집합니다.

작업 관리자

웹 인터페이스 하단의 작업을 클릭하여 마지막 방화벽 재부팅 이후 시작한 사용자, 다른 관리자 또는 PAN-OS(예: 수동 커밋 또는 자동 FQDN 새로 고침)를 표시합니다. 각 작업에 대해 작업 관리자는 아래 표에 설명된 정보와 작업을 제공합니다.

일부 열은 기본적으로 숨겨져 있습니다. 특정 열을 표시하거나 숨기려면 열 머리글에서 드롭 다운을 열고 열을 선택한 다음 열 이름을 선택(표시)하거나 선택 취소(숨기기)합니다.

필드/버튼	설명
	작업을 필터링하려면 열 중 하나의 값을 기반으로 텍스트 문자열을 입력하고 필터( )를 적용합니다. 예를 들어 **edl**을 입력하면 목록을 필터링하여 EDLFetch(외부 동적 목록 가져오기) 작업만 표시합니다. 필터링을 제거하려면 필터를 제거합니다( ).
유형	로그 요청, 라이선스 새로 고침 또는 커밋과 같은 작업 유형입니다. 작업(예: 경고)과 관련된 정보가 메시지 열에 맞지 않아도 모든 세부 정보를 보려면 형식 값을 클릭할 수 있습니다.
상태	작업이 보류 중(예: 대기 상태의 커밋), 진행 중(예: 활성 상태의 로그 요청), 완료 또는 실패 여부를 나타냅니다. 진행 중인 커밋의 경우 상태는 완료 비율을 나타냅니다.
작업 ID	작업을 식별하는 숫자입니다. CLI에서 작업 ID를 사용하여 작업에 대한 추가 세부 정보를 볼 수 있습니다. 예를 들어 커밋 큐에서 커밋 작업의 위치를 입력하여 볼 수 있습니다. `>## ID ## <job-id>`
시작 시간	작업이 시작된 날짜와 시간입니다. 커밋 작업의 경우 시작 시간은 커밋이 커밋 큐에 추가된 시기를 나타냅니다.
메시지	작업에 대한 세부 정보를 표시합니다. 항목이 메시지가 지나치게 많다는 것을 나타내는 경우 작업 유형을 클릭하여 메시지를 볼 수 있습니다. 커밋 작업의 경우 메시지에는 PAN-OS가 커밋 수행을 시작한 시간을 나타내는 대기열에서 제외된 시간이 포함됩니다. 관리자가 커밋에 대

필드/버튼	설명
	해 입력한 설명을 보려면 커밋 설명을 클릭합니다. 자세한 내용은 커밋 변경 내용을 참조하십시오.
작업	관리자 또는 PAN-OS에서 시작한 보류 중인 커밋을 취소하려면 **x**를 클릭합니다. 이 버튼은 운용 관리자, 디바이스 관리자, 가상 시스템 관리자 또는 Panorama 관리자와 같은 사전 정의된 역할 중 하나를 가진 관리자만 사용할 수 있습니다.
관리자	작업을 시작한 관리자를 표시합니다. #### ## ##과 같은 자동 작업의 경우 관리자는 ###입니다. (Panorama 관리형 방화벽) Panorama 관리자가 작업을 시작한 경우 관리자 이름에 `Panorama`가 추가됩니다. 그러한 예는 `Panorama-`<admin>입니다.
종료 시간	작업이 완료된 날짜와 시간입니다. 이 열은 기본적으로 숨겨져 있습니다.
보기	표시할 작업을 선택합니다. • 모든 작업(기본값) • 특정 유형의 모든, 작업(작업,보고서, 또는 로그 요청) • 모든 실행 중인 작업(진행 중) • 특정 유형의 모든 실행 작업(업무, 보고서, 또는 로그 요청) • (Panorama만 해당) 두 번째 드롭다운을 사용하여 **Panorama**(기본값) 또는 특정 관리 방화벽에 대한 작업을 표시합니다.
커밋 대기열 지우기	관리자 또는 PAN-OS에서 시작한 모든 보류 중인 커밋을 취소합니다. 이 버튼은 운용 관리자, 디바이스 관리자, 가상 시스템 관리자 또는 Panorama 관리자와 같은 사전 정의된 역할 중 하나를 가진 관리자만 사용할 수 있습니다.

언어

기본적으로 방화벽에 로그인하는 데 사용되는 컴퓨터에서 설정된 언어는 관리 웹 인터페이스에 표시되는 언어를 결정합니다. 수동으로 언어를 변경하려면 언어(웹 인터페이스 오른쪽 하단)를 클릭하고 드롭다운에서 원하는 언어를 선택한 다음 확인을 클릭합니다. 웹 인터페이스는 웹 인터페이스를 새로 고치고 선택한 언어로 표시합니다.

지원되는 언어에는 다음이 포함됩니다. 프랑스어, 일본어, 스페인어, 중국어(간체), 중국어(번체)를 단순화하고 중국어를 더합니다.

알람

알람은 특정 유형의 이벤트 수(예: 암호화 및 복호화 오류)가 해당 이벤트 유형에 대해 구성된 임계값을 초과했음을 나타내는 방화벽 생성 메시지입니다(알람 설정 정의참조). 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 경보를 선택한 다음 승인을 클릭하여 알람을 승인된 경보 목록으로 이동합니다.

변경 사항 커밋

웹 인터페이스의 오른쪽 상단에서 커밋을 클릭하고 방화벽 구성에 대한 보류 중인 변경 작업(커밋(활성화), 유효성 검사 또는 미리보기)을 지정합니다. 관리자 또는 위치별로 보류 중인 변경 사항을 필터링한 다음 해당 변경 사항만 미리 보고, 확인하고, 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 마칠 때까지 기다려야 합니다.

작업 관리자를 사용하여 커밋을 취소하거나 보류 중, 진행 중, 완료 또는 실패한 커밋에 대한 세부 정보를 봅니다.

커밋 대화 상자에는 다음 표에 설명된 옵션이 표시됩니다.

필드/버튼	설명
모든 변경 사항 커밋	관리 권한이 있는 모든 변경 사항을 커밋합니다(기본값). 이 옵션을 선택하면 방화벽이 커밋하는 구성 변경 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 커밋 범위가 결정됩니다. • 운용 관리자 역할 - 방화벽은 모든 관리자의 변경 사항을 커밋합니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 커밋 범위가 결정됩니다(디바이스 > 관리자 역할 참조). 프로파일에 **Commit For Other Admins** 권한이 포함되어 있으면 방화벽은 모든 관리자가 구성한 변경 사항을 커밋합니다. 관리자 역할 프로파일에 다른 관리자를 위해 커밋할 권한이 없는 경우 방화벽은 다른 관리자의 변경 사항이 아닌 사용자의 변경 사항만 커밋합니다. 액세스 도메인을 구현한 경우 방화벽은 해당 도메인을 자동으로 적용하여 커밋 범위를 필터링합니다(디바이스 > 액세스 도메인 참조). 관리자 역할에 관계없이 방화벽은 계정에 할당된 액세스 도메인의 구성 변경만 커밋합니다.
변경 사항 커밋	방화벽 커밋의 구성 변경 범위를 필터링합니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링 옵션이 결정됩니다. • 운용 관리자 역할 - 특정 관리자가 수행한 변경 사항과 특정 위치의 변경 사항으로 커밋 범위를 제한할 수 있습니다.

필드/버튼	설명
	• 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 필터링 옵션이 결정됩니다(디바이스 > 관리자 역할 참조). 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 포함되어 있으면 커밋 범위를 특정 관리자가 구성한 변경 사항과 특정 위치의 변경 사항으로 제한할 수 있습니다. 관리자 역할 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 포함되어 있지 않은 경우 커밋 범위를 특정 위치에서 변경한 내용으로만 제한할 수 있습니다. 다음과 같이 커밋 범위를 필터링합니다. • 관리자별 필터링 - 역할이 다른 관리자의 변경 사항을 커밋하도록 허용하더라도 커밋 범위에는 기본적으로 사용자의 변경 사항만 포함됩니다. 커밋 범위에 다른 관리자를 추가하려면 **<usernames>** 링크를 클릭하고 관리자를 선택한 다음 확인을 클릭합니다. • 위치별 필터링 - 커밋에 포함할 변경 사항의 특정 위치를 선택합니다. 액세스 도메인을 구현한 경우 방화벽은 해당 도메인을 기반으로 커밋 범위를 자동으로 필터링합니다(디바이스 > 액세스 도메인 참조). 관리 역할 및 필터링 선택에 관계없이 커밋 범위에는 계정에 할당된 액세스 도메인의 구성 변경 사항만 포함됩니다. 구성을 로드한 후(디바이스 > 설정 > 작업) 모든 변경 사항을 커밋해야 합니다. 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.
커밋 범위	커밋할 변경 사항이 있는 위치를 나열합니다. 목록에 모든 변경 사항이 포함되는지 아니면 변경 사항의 하위 집합이 포함되는지의 여부는 Commit All Changes 및 Commit Changes Made By에 설명된 대로 여러 요인에 따라 달라집니다. 위치는 다음 중 하나일 수 있습니다. • **shared-object** - 공유 위치에 정의된 설정입니다. • 정책 및 개체 - 여러 가상 시스템이 없는 방화벽에 정의된 정책 규칙 또는 개체입니다. • **device-and-network** - 인터페이스 관리 프로파일과 같은 전역적이며 가상 시스템에만 국한되지 않는 네트워크 및 디바이스 설정입니다. 이는 여러 가상 시스템이 없는 방화벽의 네트워크 및 디바이스 설정에도 적용됩니다.

필드/버튼	설명
	• **<virtual-system>** - 여러 가상 시스템이 있는 방화벽에서 정책 규칙 또는 개체가 정의된 가상 시스템의 이름입니다. 여기에는 가상 시스템(예: 영역)과 관련된 네트워크 및 디바이스 설정도 포함됩니다.
위치 유형	이 열은 보류 중인 변경 사항의 위치를 분류합니다. • 가상 시스템 - 특정 가상 시스템에 정의된 설정입니다. • 기타 변경 사항 - 가상 시스템에 고유하지 않은 설정(예: 공유 개체).
커밋에 포함 (부분 커밋만)	커밋할 변경 사항을 선택할 수 있습니다. 기본적으로 커밋 범위 내의 모든 변경 사항이 선택됩니다. 이 열은 특정 관리자가 변경한 사항을 커밋하도록 선택한 후에만 표시됩니다. 커밋에 포함하는 변경 사항에 영향을 미치는 종속성이 있을 수 있습니다. 예를 들어 개체를 추가하고 다른 관리자가 해당 개체를 편집하는 경우 자신의 변경 사항을 커밋하지 않고는 다른 관리자를 위해 변경 사항을 커밋할 수 없습니다.
위치 유형별 그룹화	커밋 범위의 구성 변경 목록을 위치 유형별로 그룹화합니다.
변경 사항 미리보기	커밋 범위에서 선택한 구성을 실행 중인 구성과 비교할 수 있습니다. 미리보기 창은 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)인 변경 사항을 나타냅니다. 웹 인터페이스 섹션에 대한 변경 사항을 일치시키는 데 도움이 되도록 각 변경 전후에 컨텍스트 라인을 표시하도록 미리보기 창을 구성할 수 있습니다. 이 줄은 비교 중인 후보 및 실행 중인 구성의 파일에서 불러온 것입니다. 미리보기 결과가 새 브라우저 창에 표시되기 때문에 브라우저에서 팝업을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 허용 단계를 참조하세요.
변경 요약	변경 사항을 커밋하는 개별 설정을 나열합니다. 변경 요약 목록에는 각 설정에 대한 다음 정보가 표시됩니다. • 개체 이름 - 정책, 개체, 네트워크 설정 또는 디바이스 설정을 식별하는 이름입니다.

필드/버튼	설명
	• 유형 - 설정 유형(예: 주소, 보안 규칙 또는 영역)입니다. • 위치 유형 - 설정이 가상 시스템에 정의되어 있는지의 여부를 나타냅니다. • 위치 - 설정이 정의된 가상 시스템의 이름입니다. 열에는 가상 시스템과 관련이 없는 설정에 대해 공유가 표시됩니다. • 작업 - 마지막 커밋 이후 설정에 대해 수행된 모든 작업(생성, 편집 또는 삭제)을 나타냅니다. • 소유자 - 설정을 마지막으로 변경한 관리자입니다. • 커밋될 예정 - 커밋에 현재 설정이 포함되어 있는지의 여부를 나타냅니다. • 이전 소유자 - 마지막 변경 전에 설정을 변경한 관리자입니다. 선택적으로 열 이름(예: 유형)으로 그룹화할 수 있습니다. 개체 수준 차이를 보려면 변경 목록에서 개체를 선택합니다.
커밋 확인	방화벽 구성이 올바른 구문을 가지고 있고 의미상 완전한지 검증합니다. 출력에는 규칙 섀도잉 및 애플리케이션 종속성 경고를 포함하여 커밋에 표시되는 것과 동일한 오류 및 경고가 포함됩니다. 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.
설명	다른 관리자가 변경 사항을 이해하는 데 도움이 되도록 설명(최대 512자)을 입력할 수 있습니다. 커밋 이벤트에 대한 시스템 로그는 *512*자보다 긴 설명을 자릅니다.
커밋	커밋을 시작하거나 다른 커밋이 보류 중인 경우 커밋을 커밋 대기열에 추가합니다.
커밋 상태	커밋 중 진행 상황을 제공하고 커밋 후 결과를 제공합니다. 커밋 결과에는 성공 또는 실패, 커밋 변경 내용 및 커밋 경고가 포함됩니다. 경고에는 다음이 포함됩니다. • 커밋 - 일반 커밋 경고를 나열합니다. • 앱 종속성 - 기존 규칙에 필요한 앱 종속성을 나열합니다. • 규칙 섀도우 - 섀도우 규칙을 나열합니다.

후보자 구성 저장

방화벽 또는 Panorama 웹 인터페이스의 오른쪽 상단에서 **Config** > **Save Changes**를 선택하여 후보 구성의 새 스냅샷 파일을 저장하거나 기존 구성 파일을 덮어씁니다. 변경 사항을 커밋하기 전에 방화벽이나 Panorama가 재부팅되는 경우 후보 구성을 저장된 스냅샷으로 되돌려 마지막 커밋 이후에 변경한 사항을 복원할 수 있습니다. 스냅샷으로 되돌리려면 디바이스 > 설정 > 작업을 선택한 다음 명명된 구성 스냅샷 로드를 선택합니다. 재부팅 후 스냅샷으로 되돌리지 않으면 후보 구성은 마지막으로 커밋된 구성(실행 중인 구성)과 동일합니다.

관리자 또는 위치에 따라 저장할 구성 변경 사항을 필터링할 수 있습니다. 위치는 특정 가상 시스템, 공유 정책 및 개체 또는 공유 디바이스 및 네트워크 설정일 수 있습니다.

방화벽이나 *Panorama*가 재부팅될 때 변경 사항이 손실되지 않도록 주기적으로 변경 사항을 저장해야 합니다.

후보 구성에 대한 변경 사항을 저장하면 해당 변경 사항이 활성화되지 않습니다. 활성화하려면 변경 사항을 커밋해야 합니다.

변경 사항 저장 대화 상자에는 다음 표에 설명된 옵션이 표시됩니다.

필드/버튼	설명
모든 변경 사항 저장	관리 권한이 있는 모든 변경 사항을 저장합니다(기본값). 이 옵션을 선택하면 방화벽이 저장하는 구성 변경의 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 저장 범위가 결정됩니다. • 운용 관리자 역할 - 방화벽은 모든 관리자의 변경 사항을 저장합니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 저장 범위가 결정됩니다(디바이스 > 관리자 역할 참조). 프로파일에 다른 관리자용으로 저장 권한이 포함된 경우 방화벽은 모든 관리자가 구성한 변경 사항을 저장합니다. 관리자 역할 프로파일에 다른 관리자용으로 저장 권한이 없는 경우 방화벽은 다른 관리자의 변경 사항이 아닌 사용자의 변경 사항만 저장합니다. 액세스 도메인을 구현한 경우 방화벽은 자동으로 해당 도메인을 적용하여 저장 범위를 필터링합니다(디바이스 > 액세스 도메인 참조). 관리자 역할에 관계없이 방화벽은 계정에 할당된 액세스 도메인의 구성 변경 사항만 저장합니다.
변경 사항 저장	방화벽이 저장하는 구성 변경의 범위를 필터링합니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링 옵션이 결정됩니다.

필드/버튼	설명
	• 운용 관리자 역할 - 특정 관리자가 수행한 변경 사항과 특정 위치의 변경 사항으로 저장 범위를 제한할 수 있습니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 필터링 옵션이 결정됩니다(디바이스 > 관리자 역할 참조). 프로파일에 다른 관리자용으로 저장 권한이 포함된 경우 특정 관리자가 구성한 변경 사항과 특정 위치의 변경 사항으로 저장 범위를 제한할 수 있습니다. 관리자 역할 프로파일에 다른 관리자용으로 저장 권한이 없는 경우 특정 위치에서 변경한 내용으로만 저장 범위를 제한할 수 있습니다. 다음과 같이 저장 범위를 필터링합니다. • 관리자별 필터링 - 역할이 다른 관리자의 변경 사항을 저장할 수 있도록 허용하더라도 기본적으로 저장 범위에는 사용자의 변경 사항만 포함됩니다. 저장 범위에 다른 관리자를 추가하려면 **<usernames>** 링크를 클릭하고 관리자를 선택한 다음 확인을 클릭합니다. • 위치별 필터링 - 저장에 포함할 특정 위치의 변경 사항을 선택합니다. 액세스 도메인을 구현한 경우 방화벽은 해당 도메인을 기반으로 저장 범위를 자동으로 필터링합니다(디바이스 > 액세스 도메인 참조). 관리 역할 및 필터링 선택에 관계없이 저장 범위에는 계정에 할당된 액세스 도메인의 구성 변경 사항만 포함됩니다.
범위 저장	저장할 변경 사항이 있는 위치를 나열합니다. 목록에 모든 변경 사항이 포함되는지 아니면 변경 사항의 하위 집합이 포함되는지의 여부는 모든 변경 사항 저장 및 변경 사항 저장 옵션에 대해 설명된 대로 여러 요인에 따라 달라집니다. 위치는 다음 중 하나일 수 있습니다. • **shared-object** - 공유 위치에 정의된 설정입니다. • 정책 및 개체 - (방화벽만 해당) 여러 가상 시스템이 없는 방화벽에 정의된 정책 규칙 또는 개체입니다. • **device-and-network** - (방화벽만 해당) 가상 시스템에 국한되지 않고 전역(예: 인터페이스 관리 프로파일)인 네트워크 및 디바이스 설정입니다. • **<virtual-system>** - (방화벽만) 여러 가상 시스템이 있는 방화벽에서 정책 규칙 또는 개체가 정의된 가상 시스템의 이름입니다. 여기에는 가상 시스템(예: 영역)과 관련된 네트워크 및 디바이스 설정도 포함됩니다.

필드/버튼	설명
	• **<device-group>** - (Panorama 전용) 정책 규칙 또는 개체가 정의된 기기 그룹의 이름입니다. • **<template>** - (Panorama 전용) 설정이 정의된 템플릿 또는 템플릿 스택의 이름입니다. • **<log-collector-group>** - (Panorama 전용) 설정이 정의된 수집기 그룹의 이름입니다. • **<log-collector>** - (Panorama 전용) 설정이 정의된 로그 수집기의 이름입니다.
위치 유형	이 열은 변경된 위치를 분류합니다. • 가상 시스템 - (방화벽만 해당) 특정 가상 시스템에 정의된 설정입니다. • 디바이스 그룹 - (Panorama 전용) 특정 디바이스 그룹에 정의된 설정입니다. • 템플릿 - (Panorama 전용) 특정 템플릿 또는 템플릿 스택(template stack)에 정의된 설정입니다. • 수집기 그룹 - (Panorama 전용) 수집기 그룹 구성과 관련된 설정입니다.
저장에 포함 (부분 저장만)	저장할 변경 사항을 선택할 수 있습니다. 기본적으로 저장 범위 내의 모든 변경 사항이 선택됩니다. 이 열은 특정 관리자가 변경한 내용을 저장하도록 선택한 후에만 표시됩니다. 저장에 포함하는 변경 사항에 영향을 미치는 종속성이 있을 수 있습니다. 예를 들어 개체를 추가하고 다른 관리자가 해당 개체를 편집하는 경우 자신의 변경 사항도 저장하지 않고는 다른 관리자의 변경 사항을 저장할 수 없습니다.
위치 유형별 그룹화	저장 범위의 구성 변경 목록을 위치 유형별로 그룹화합니다.
변경 사항 미리보기	저장 범위에서 선택한 구성을 실행 중인 구성과 비교할 수 있습니다. 미리보기 창은 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)인 변경 사항을 나타냅니다. 웹 인터페이스 섹션에 대한 변경 사항을 일치시키는 데 도움이 되도록 각 변경 전후에 컨텍스트 라인을 표시하도록 미리보기 창을 구성할 수 있습니다. 이 줄은 비교 중인 후보 및 실행 중인 구성의 파일에서 불러온 것입니다.

필드/버튼	설명
	미리보기 결과가 새 창에 표시되기 때문에 브라우저에서 팝업 창을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 창 차단을 해제하는 단계를 참조합니다.
변경 요약	변경 사항을 저장할 개별 설정을 나열합니다. 변경 요약 목록에는 각 설정에 대한 다음 정보가 표시됩니다. • 개체 이름 - 정책, 개체, 네트워크 설정 또는 디바이스 설정을 식별하는 이름입니다. • 유형 - 설정 유형(예: 주소, 보안 규칙 또는 영역)입니다. • 위치 유형 - 설정이 가상 시스템에 정의되어 있는지의 여부를 나타냅니다. • 위치 - 설정이 정의된 가상 시스템의 이름입니다. 열에는 가상 시스템과 관련이 없는 설정에 대해 공유가 표시됩니다. • 작업 - 마지막 커밋 이후 설정에 대해 수행된 모든 작업(생성, 편집 또는 삭제)을 나타냅니다. • 소유자 - 설정을 마지막으로 변경한 관리자입니다. • 저장됨 - 저장 작업에 설정이 포함되는지의 여부를 나타냅니다. • 이전 소유자 - 마지막 변경 전에 설정을 변경한 관리자입니다. 선택적으로 열 이름(예: 유형)으로 그룹화할 수 있습니다.
저장	선택한 변경 사항을 구성 스냅샷 파일에 저장합니다. • 모든 변경 사항 저장을 선택한 경우 방화벽은 기본 구성 스냅샷 파일(.snapshot.xml)을 덮어씁니다. • 변경 사항 저장을 선택한 경우 새 구성 파일 또는 기존 구성 파일의 이름을 지정하고 확인을 클릭합니다.

변경 사항 되돌리기

마지막 커밋 이후 후보 구성에 대한 변경 사항을 취소하려면 방화벽 또는 Panorama 웹 인터페이스의 오른쪽 상단에서 **Config** > **Revert Changes**를 선택합니다. 변경 사항을 되돌리면 설정이 실행 중인 구성 값으로 복원됩니다. 관리자 또는 위치에 따라 되돌릴 구성 변경 사항을 필터링할 수 있습니다. 위치는 특정 가상 시스템, 공유 정책 및 개체 또는 공유 디바이스 및 네트워크 설정일 수 있습니다.

방화벽이나 Panorama가 보류 중이거나 진행 중인 모든 커밋 처리를 마칠 때까지 변경 사항을 되돌릴 수 없습니다. 되돌리기 프로세스를 시작한 후 방화벽 또는 Panorama는 후보 및 실행 중인 구성을 자동으로 잠그므로 다른 관리자가 설정을 편집하거나 변경 사항을 커밋할 수 없습니다. 되돌리기 프로세스가 완료되면 방화벽 또는 Panorama가 자동으로 잠금을 제거합니다.

변경 사항 되돌리기 대화 상자에는 다음 표에 설명된 옵션이 표시됩니다.

필드/버튼	설명
모든 변경 사항 되돌리기	관리 권한이 있는 모든 변경 사항을 되돌립니다(기본값). 이 옵션을 선택하면 방화벽이 되돌리는 구성 변경 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 되돌리기 범위가 결정됩니다. • 운용 관리자 역할 - 방화벽은 모든 관리자의 변경 사항을 되돌립니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 되돌리기 범위가 결정됩니다(디바이스 > 관리자 역할 참조). 프로파일에 **Commit For Other Admins** 권한이 포함되어 있으면 방화벽은 모든 관리자가 구성한 변경 사항을 되돌립니다. 관리자 역할 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 없는 경우 방화벽은 다른 관리자의 변경 사항이 아닌 사용자의 변경 사항만 되돌립니다. 관리자 역할 프로파일에서 커밋 권한은 되돌리기에도 적용됩니다. 액세스 도메인을 구현한 경우 방화벽은 자동으로 해당 도메인을 적용하여 되돌리기 범위를 필터링합니다(디바이스 > 액세스 도메인 참조). 관리자 역할에 관계없이 방화벽은 계정에 할당된 액세스 도메인의 구성 변경 사항만 되돌립니다.
변경 사항 되돌리기	방화벽이 되돌리는 구성 변경 범위를 필터링합니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링 옵션이 결정됩니다. • 운용 관리자 역할 - 특정 관리자가 수행한 변경 사항 및 특정 위치의 변경 사항으로 되돌리기 범위를 제한할 수 있습니다.

필드/버튼	설명
	• 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 필터링 옵션이 결정됩니다(디바이스 > 관리자 역할 참조). 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 포함된 경우 특정 관리자가 구성한 변경 사항과 특정 위치의 변경 사항으로 되돌리는 범위를 제한할 수 있습니다. 관리자 역할 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 없는 경우 특정 위치에서 수행한 변경 사항으로만 되돌리는 범위를 제한할 수 있습니다. 다음과 같이 되돌리기 범위를 필터링합니다. • 관리자별 필터링 - 역할이 다른 관리자의 변경 사항을 되돌릴 수 있도록 허용하더라도 기본적으로 되돌리기 범위에는 사용자의 변경 사항만 포함됩니다. 되돌리기 범위에 다른 관리자를 추가하려면 **<usernames>** 링크를 클릭하고 관리자를 선택한 다음 확인을 클릭합니다. • 위치별 필터링 - 되돌리기에 포함할 특정 위치의 변경 사항을 선택합니다. 액세스 도메인을 구현한 경우 방화벽은 해당 도메인을 기반으로 되돌리기 범위를 자동으로 필터링합니다(디바이스 > 액세스 도메인 참조). 관리 역할 및 필터링 선택에 관계없이 되돌리기 범위에는 계정에 할당된 액세스 도메인의 구성 변경 사항만 포함됩니다.
범위 되돌리기	되돌릴 변경 사항이 있는 위치를 나열합니다. 목록에 모든 변경 사항이 포함되는지 아니면 변경 사항의 하위 집합이 포함되는지의 여부는 모든 변경 사항 되돌리기 및 변경한 내용 되돌리기 옵션에 대해 설명된 대로 여러 요인에 따라 달라집니다. 위치는 다음 중 하나일 수 있습니다. • **shared-object** - 공유 위치에 정의된 설정입니다. • 정책 및 개체 - (방화벽만 해당) 여러 가상 시스템이 없는 방화벽에 정의된 정책 규칙 또는 개체입니다. • **device-and-network** - (방화벽만 해당) 가상 시스템에 국한되지 않고 전역(예: 인터페이스 관리 프로파일)인 네트워크 및 디바이스 설정입니다. • **<virtual-system>** - (방화벽만) 여러 가상 시스템이 있는 방화벽에서 정책 규칙 또는 개체가 정의된 가상 시스템의 이름입니다. 여기에는 가상 시스템(예: 영역)과 관련된 네트워크 및 디바이스 설정도 포함됩니다. • **<device-group>** - (Panorama 전용) 정책 규칙 또는 개체가 정의된 기기 그룹의 이름입니다.

필드/버튼	설명
	• **<template>**—(Panorama 전용) 설정이 정의된 템플릿 또는 템플릿 스택의 이름입니다. • **<log-collector-group>** - (Panorama 전용) 설정이 정의된 수집기 그룹의 이름입니다. • **<log-collector>** - (Panorama 전용) 설정이 정의된 로그 수집기의 이름입니다.
위치 유형	이 열은 변경된 위치를 분류합니다. • 가상 시스템 - (방화벽만 해당) 특정 가상 시스템에 정의된 설정입니다. • 디바이스 그룹 - (Panorama 전용) 특정 디바이스 그룹에 정의된 설정입니다. • 템플릿 - (Panorama 전용) 특정 템플릿 또는 템플릿 스택(template stack)에 정의된 설정입니다. • 로그 수집기 그룹 - (Panorama만 해당) 수집기 그룹 구성과 관련된 설정입니다. • **Log Collector** - (Panorama 전용) Log Collector 구성과 관련된 설정입니다. • 기타 변경 사항 - 이전 구성 영역(예: 공유 개체)과 관련이 없는 설정입니다.
되돌리기에 포함 (부분 복원만 해당)	되돌리려는 변경 사항을 선택할 수 있습니다. 기본적으로 범위 되돌리기 내의 모든 변경 사항이 선택됩니다. 이 열은 특정 관리자가 변경한 사항 되돌리기를 선택한 후에만 표시됩니다. 되돌리기에 포함하는 변경 사항에 영향을 미치는 종속성이 있을 수 있습니다. 예를 들어 개체를 추가하고 다른 관리자가 해당 개체를 편집하는 경우 다른 관리자의 변경 사항도 되돌리지 않고는 변경 사항을 되돌릴 수 없습니다.
위치 유형별 그룹화	위치 유형별 범위 되돌리기의 구성 변경 사항을 나열합니다.
변경 사항 미리보기	범위 되돌리기에서 선택한 구성을 실행 중인 구성과 비교할 수 있습니다. 미리보기 창은 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)인 변경 사항을 나타냅니다. 웹 인터페이스 섹션에 대한 변경 사항을 일치시키는 데 도움이 되도록 각 변경 전후에 컨텍스트 라인을 표시하도록 미리보기 창을 구성할 수

필드/버튼	설명
	있습니다. 이 줄은 비교 중인 후보 및 실행 중인 구성의 파일에서 불러온 것입니다. 미리보기 결과가 새 창에 표시되기 때문에 브라우저에서 팝업 창을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 창 차단을 해제하는 단계를 참조합니다.
변경 요약	변경 사항을 되돌릴 개별 설정을 나열합니다. 변경 요약 목록에는 각 설정에 대한 다음 정보가 표시됩니다. • 개체 이름 - 정책, 개체, 네트워크 설정 또는 디바이스 설정을 식별하는 이름입니다. • 유형 - 설정 유형(예: 주소, 보안 규칙 또는 영역)입니다. • 위치 유형 - 설정이 가상 시스템에 정의되어 있는지의 여부를 나타냅니다. • 위치 - 설정이 정의된 가상 시스템의 이름입니다. 열에는 가상 시스템과 관련이 없는 설정에 대해 공유가 표시됩니다. • 작업 - 마지막 커밋 이후 설정에 대해 수행된 모든 작업(생성, 편집 또는 삭제)을 나타냅니다. • 소유자 - 설정을 마지막으로 변경한 관리자입니다. • 되돌릴 예정 - 되돌리기 작업에 설정이 포함되는지의 여부를 나타냅니다. • 이전 소유자 - 마지막 변경 전에 설정을 변경한 관리자입니다. 선택적으로 열 이름(예: 유형)으로 그룹화할 수 있습니다.
되돌리기	선택한 변경 사항을 되돌립니다.

잠금 구성

동시 로그인 세션 동안 다른 방화벽 관리자와 구성 작업을 조정하는 데 도움이 되도록 웹 인터페이스를 사용하여 구성을 적용하거나 잠금을 커밋할 수 있으므로 다른 관리자는 잠금이 제거될 때까지 구성을 변경하거나 변경 사항을 커밋할 수 없습니다.

웹 인터페이스의 오른쪽 상단에서 잠긴 자물쇠( )는 하나 이상의 자물쇠가 설정되었음을 나타냅니다(괄호 안에 자물쇠 수 포함). 잠금 해제된 자물쇠( )는 자물쇠가 설정되지 않았음을 나타냅니다. 자물쇠 중 하나를 클릭하면 다음 옵션과 필드를 제공하는 잠금 대화 상자가 열립니다.

관리자가 후보 구성을 변경할 때마다 커밋 잠금을 자동으로 설정하도록 방화벽을 구성하려면 ***Device*** > ***Setup*** > ***Management***를 선택한 다음 일반 설정을 편집하고 커밋 잠금 자동 획득을 활성화한 다음 확인 및 커밋을 클릭합니다.

변경 사항을 되돌리면(***Config*** > ***Revert Changes***) 방화벽은 다른 관리자가 설정을 편집하거나 변경 사항을 커밋할 수 없도록 후보 및 실행 중인 구성을 자동으로 잠급니다. 되돌리기 프로세스가 완료되면 방화벽이 자동으로 잠금을 제거합니다.

필드/버튼	설명
관리자	잠금을 설정한 관리자의 사용자명입니다.
위치	둘 이상의 가상 시스템(vsys)이 있는 방화벽에서 잠금 범위는 특정 vsys 또는 공유 위치일 수 있습니다.
유형	잠금 유형은 다음과 같을 수 있습니다. • 구성 잠금 - 다른 관리자가 후보 구성을 변경하지 못하도록 차단합니다. 잠금을 설정한 운용 관리자 또는 관리자만 잠금을 해제할 수 있습니다. • 커밋 잠금 - 다른 관리자가 후보 구성에 대한 변경 사항을 커밋하지 못하도록 차단합니다. 커밋 큐는 모든 잠금이 해제될 때까지 새 커밋을 허용하지 않습니다. 이 잠금은 여러 관리자가 동시 로그인 세션 동안 변경을 수행하고 다른 관리자가 완료되기 전에 한 관리자가 완료하고 커밋을 시작할 때 발생할 수 있는 충돌을 방지합니다. 방화벽은 관리자가 잠금을 설정한 커밋을 완료한 후 자동으로 잠금을 제거합니다. 잠금을 설정한 운용 관리자 또는 관리자도 수동으로 잠금을 제거할 수 있습니다.
코멘트	최대 256자의 텍스트를 입력합니다. 이는 잠금의 이유를 알고자 하는 다른 관리자에게 유용합니다.
생성 시간	관리자가 잠금을 설정한 날짜 및 시간입니다.

필드/버튼	설명
로그인	잠금을 설정한 관리자가 현재 로그인되어 있는지의 여부를 나타냅니다.
잠금 설정	잠금을 설정하려면 잠금을 설정하고 유형을 선택한 다음 위치(다중 가상 시스템 방화벽만 해당)를 선택한 다음 선택적 설명을 입력하고 확인을 클릭한 다음 닫기를 클릭합니다.
잠금 해제	잠금을 해제하려면 잠금을 선택한 다음 잠금 제거를 클릭하고 확인을 클릭한 다음 닫기를 클릭합니다.

전역 찾기

전역 찾기를 사용하면 방화벽이나 Panorama에서 IP 주소, 개체 이름, 정책 이름, 위협 ID, 규칙 UUID 또는 애플리케이션 이름과 같은 특정 문자열에 대한 후보 구성을 검색할 수 있습니다. 검색 결과는 카테고리별로 그룹화되며 웹 인터페이스의 구성 위치에 대한 링크를 제공하므로 문자열이 존재하거나 참조되는 모든 위치를 쉽게 찾을 수 있습니다.

전역 찾기를 시작하려면 웹 인터페이스의 오른쪽 상단에 있는 검색 아이콘 을 클릭합니다. 전역 찾기는 모든 웹 인터페이스 페이지 및 위치에서 사용할 수 있습니다. 다음은 성공적인 검색을 수행하는 데 도움이 되는 전역 찾기 기능 목록입니다.

- 여러 가상 시스템이 활성화된 방화벽에서 검색을 시작하거나 관리 역할이 정의된 경우 전역 찾기는 액세스 권한이 있는 방화벽 영역에 대한 결과만 반환합니다. Panorama 디바이스 그룹에도 동일하게 적용됩니다. 관리 액세스 권한이 있는 디바이스 그룹에 대한 검색 결과만 표시됩니다.
- 검색 텍스트의 공백은 AND 연산으로 처리됩니다. 예를 들어 **`corp policy`**를 검색하는 경우 **corp**와 **policy**가 모두 구성 항목에 있어야 검색 결과에 포함될 수 있습니다.
- 정확한 구를 찾으려면 구를 따옴표로 묶으십시오.
- 이전 검색을 다시 실행하려면 전역 찾기를 클릭하면 최근 20개의 검색 목록이 표시됩니다. 목록에서 항목을 클릭하여 해당 검색을 다시 실행하십시오. 검색 기록 목록은 각 관리 계정에 고유합니다.

검색 가능한 각 필드에 대해 전역 찾기를 사용할 수 있습니다. 예를 들어 보안 정책의 경우 다음 필드에서 검색할 수 있습니다. 이름, 태그, 영역, 주소, 사용자, HIP 프로파일, 애플리케이션, UUID 및 서비스. 검색을 수행하려면 이러한 필드 옆에 있는 드롭다운을 클릭하고 전역 찾기를 클릭합니다. 예를 들어, l3-vlan-trust라는 영역에서 전역 찾기를 클릭하면 전역 찾기가 해당 영역 이름에 대한 전체 구성을 검색하고 영역이 참조되는 각 위치에 대한 결과를 반환합니다. 검색 결과는 카테고리별로 그룹화되며 항목 위로 마우스를 가져가 세부 정보를 보거나 항목을 클릭하여 해당 항목의 구성 페이지로 이동할 수 있습니다.

전역 찾기는 방화벽이 사용자에게 할당하는 동적 콘텐츠(예: 로그, 주소 범위 또는 개별 DHCP 주소)를 검색하지 않습니다. DHCP의 경우 DNS 항목과 같은 DHCP 서버 속성을 검색할 수 있지만 사용자에게 발급된 개별 주소는 검색할 수 없습니다. 또 다른 예로는 User-ID™ 기능을 활성화할 때 방화벽이 수집하는 사용자명이 있습니다. 이 경우 User-ID 데이터베이스에 존재하는 사용자명 또는 사용자 그룹은 사용자 그룹 이름이 정책에 정의된 경우와 같이 구성에 이름 또는 그룹이 존재하는 경우에만 검색할 수 있습니다. 일반적으로 방화벽이 구성에 쓰는 콘텐츠만 검색할 수 있습니다.

더 찾고 계십니까**?**

전역 찾기를 사용하여 방화벽 또는 Panorama 구성을 검색하는 방법에 대해 자세히 알아보세요.

위협 세부 정보

- 모니터링 > 로그 > 위협
- ACC > 위협 활동
- 개체 > 보안 프로파일 > 안티 스파이웨어/취약성 보호

위협 세부 정보 대화 상자를 사용하여 방화벽이 장착된 위협 서명과 해당 서명을 트리거하는 이벤트에 대해 자세히 알아봅니다. 위협 세부 정보는 다음에 대해 제공됩니다.

- 방화벽이 탐지한 위협을 기록하는 위협 로그(**Monitor** > **Logs** > **Threat**)
- 네트워크에서 발견된 상위 위협(**ACC** > 위협 활동)
- 수정하거나 적용에서 제외하려는 위협 서명(**Objects** > **Security Profiles** > **Anti-Spyware/ Vulnerability Protection**)

자세히 알아보려는 위협 서명을 찾으면 위협 이름 또는 위협 **ID** 위로 마우스를 가져간 다음 예외를 클릭하여 위협 세부 정보를 검토합니다. 위협 세부 정보를 통해 위협 서명이 보안 정책의 예외로 구성되었는지의 여부를 쉽게 확인하고 특정 위협에 대한 최신 Threat Vault 정보를 찾을 수 있습니다. Palo Alto Networks Threat Vault 데이터베이스는 방화벽과 통합되어 있어 방화벽 컨텍스트에서 위협 서명에 대한 확장된 세부 정보를 보거나 새 브라우저 창에서 기록된 위협에 대한 Threat Vault 검색을 시작할 수 있습니다.

보고 있는 위협 유형에 따라 세부 정보에는 다음 표에 설명된 위협 세부 정보 전체 또는 일부가 포함됩니다.

위협 세부 정보	설명
이름	위협 서명 이름입니다.
ID	고유한 위협 서명 ID입니다. **Threat Vault**에서 보기를 선택하여 새 브라우저 창에서 Threat Vault 검색을 열고 Palo Alto Networks 위협 데이터베이스가 이 서명에 대해 가지고 있는 최신 정보를 조회합니다. 위협 서명에 대한 Threat Vault 항목에는 서명 업데이트를 포함하는 첫 번째 및 마지막 콘텐츠 릴리스와 서명을 지원하는 데 필요한 최소 PAN-OS 버전을 비롯한 추가 세부 정보가 포함될 수 있습니다.
설명	서명을 트리거하는 위협에 대한 정보입니다.
심각성	위협 심각도 수준: 정보 제공, 낮음, 중간, 높음 또는 위험.
CVE	위협과 관련된 공개적으로 알려진 보안 취약성. CVE(Common Vulnerabilities and Exposures) 식별자는 공급자별 ID가 일반적으로 여러 취약점을 포함하므로 고유한 취약점에 대한 정보를 찾는 데 가장 유용한 식별자입니다.
Bugtraq ID	위협과 관련된 Bugtraq ID입니다.

위협 세부 정보	설명
공급자 ID	취약점에 대한 공급자별 식별자입니다. 예를 들어 MS16-148은 하나 이상의 Microsoft 취약점에 대한 공급자 ID이고 APBSB16-39는 하나 이상의 Adobe 취약점에 대한 공급자 ID입니다.
참조	위협에 대해 자세히 알아보는 데 사용할 수 있는 연구 출처.
면제 프로파일	위협 서명에 대해 기본 서명 작업과 다른 시행 작업을 정의하는 보안 프로파일입니다. 위협 예외는 예외 프로파일이 보안 정책 규칙에 연결된 경우에만 활성화됩니다(예외가 현재 보안 규칙에서 사용됨인지 확인).
현재 보안 규칙에서 사용	활성 위협 예외 - 이 열의 확인 표시는 방화벽이 위협 예외를 적극적으로 시행하고 있음을 나타냅니다(위협 예외를 정의하는 면제 프로파일은 보안 정책 규칙에 첨부됨). 이 열이 선택되지 않은 경우 방화벽은 권장되는 기본 서명 작업만을 기반으로 위협을 시행합니다.
면제 IP 주소	면제 IP 주소 - 위협 예외를 필터링하거나 기존 면제 **IP** 주소를 볼 IP 주소를 추가할 수 있습니다. 이 옵션은 연결된 세션에 예외 IP 주소와 일치하는 소스 또는 대상 IP 주소가 있는 경우에만 위협 예외를 적용합니다. 다른 모든 세션의 경우 기본 서명 작업을 기반으로 위협이 적용됩니다.

위협 세부 정보를 보는 데 문제가 있는 경우 다음 조건을 확인하세요.

- 방화벽 위협 방지 라이선스가 활성 상태입니다(디바이스 > 라이선스).
- 최신 바이러스 백신 및 위협 및 애플리케이션 콘텐츠 업데이트가 설치됩니다.
- *Threat Vault* 액세스가 활성화되었습니다(디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 ***Threat Vault*** 액세스 활성화로 편집).
- 기본(또는 사용자 정의) 안티바이러스, 안티스파이웨어 및 취약성 보호 보안 프로파일이 보안 정책에 적용됩니다.

AutoFocus 인텔리전스 요약

AutoFocus가 컴파일하는 위협 인텔리전스의 그래픽 개요를 확인하여 다음 방화벽 아티팩트의 확산성과 위험을 평가할 수 있습니다.

- IP 주소
- URL
- 도메인
- 사용자 에이전트(데이터 필터링 로그의 사용자 에이전트 열에 있음)
- 위협 이름(아형 바이러스 및 WildFire 바이러스의 위협에만 해당)
- 파일 이름
- SHA-256 해시(WildFire 제출 로그의 파일 다이제스트 열에 있음)

AutoFocus Intelligence Summary 창을 보려면 먼저 활성 AutoFocus 구독이 있어야 하고 AutoFocus 위협 인텔리전스를 활성화해야 합니다(**Device** > **Setup** > **Management**를 선택한 다음 AutoFocus 설정 편집).

AutoFocus 인텔리전스를 활성화한 후 로그 또는 외부 동적 목록 아티팩트 위로 마우스를 가져가서 드롭다운(⌄)을 연 다음 **AutoFocus**를 클릭합니다.

- 트래픽, 위협, URL 필터링, WildFire 제출, 데이터 필터링 및 통합 로그(모니터 > 로그)를 봅니다.
- 외부 동적 목록 항목을 봅니다.

또한 방화벽에서 AutoFocus 검색을 시작하여 발견한 흥미롭거나 의심스러운 아티팩트를 추가로 검토할 수 있습니다.

필드/버튼	설명
AutoFocus 검색...	아티팩트에 대한 AutoFocus 검색을 시작하려면 클릭합니다.
분석 정보 탭	
세션	WildFire가 아티팩트를 감지한 비공개 세션의 수입니다. 비공개 세션은 지원 계정과 연결된 방화벽에서만 실행되는 세션입니다. 세션 표시줄 위로 마우스를 가져가면 월별 세션 수를 볼 수 있습니다.
샘플	아티팩트와 연결되고 WildFire 판정(양성, 그레이웨어, 멀웨어, 피싱)별로 그룹화된 조직 및 글로벌 샘플(파일 및 이메일 링크). 글로벌은 모든 WildFire 제출의 샘플을 참조하는 반면 조직은 조직에서 WildFire에 제출한 샘플만 나타냅니다. WildFire 판정을 클릭하면 범위(조직 또는 글로벌) 및 WildFire 판정으로 필터링된 아티팩트에 대한 AutoFocus 검색을 시작합니다.

필드/버튼	설명
일치하는 태그	아티팩트와 일치하는 AutoFocus 태그: • 비공개 태그 - 지원 계정과 연결된 AutoFocus 사용자에게만 표시됩니다. • 공개 태그 - 모든 AutoFocus 사용자에게 표시됩니다. • **Unit 42** 태그 - 직접적인 보안 위험을 야기하는 위협 및 캠페인을 식별합니다. 이 태그는 Unit 42(Palo Alto Networks 위협 인텔리전스 및 연구 팀)에서 생성합니다. • 정보 태그 - 상품 위협을 식별하는 Unit 42 태그입니다. 태그 위로 마우스를 가져가면 태그 설명 및 기타 태그 세부 정보를 볼 수 있습니다. 태그를 클릭하면 해당 태그에 대한 AutoFocus 검색이 시작됩니다. 이슈에 대해 일치하는 태그를 더 보려면 줄임표(...)를 클릭하여 해당 이슈에 대한 AutoFocus 검색을 시작합니다. AutoFocus 검색 결과의 태그 열에는 아티팩트에 대해 일치하는 태그가 더 많이 표시됩니다.
수동형 DNS 탭 수동형 DNS 탭에는 아티팩트와 연결된 수동형 DNS 기록이 표시됩니다. 이 탭은 아티팩트가 IP 주소, 도메인 또는 URL인 경우에만 일치하는 정보를 표시합니다.	
요청	DNS 요청을 제출한 도메인입니다. 도메인을 클릭하여 AutoFocus 검색을 시작합니다.
유형	DNS 요청 유형(예: A, NS, CNAME).
응답	DNS 요청이 확인된 IP 주소 또는 도메인입니다. IP 주소 또는 도메인을 클릭하여 AutoFocus 검색을 시작합니다. 응답 열에는 개인 *IP* 주소가 표시되지 않습니다.
카운트	요청이 이루어진 횟수입니다.
처음 본	수동형 DNS 기록을 기반으로 요청, 응답 및 유형 조합이 처음 표시된 날짜 및 시간입니다.
마지막으로 본	수동형 DNS 기록을 기반으로 요청, 응답 및 유형 조합이 가장 최근에 확인된 날짜 및 시간입니다.

필드/버튼	설명
일치하는 해시 탭 일치하는 해시 탭에는 WildFire가 아티팩트를 감지한 가장 최근의 비공개 샘플 5개가 표시됩니다. 비공개 샘플은 지원 계정과 연결된 방화벽에서만 감지되는 샘플입니다.	
SHA256	샘플에 대한 SHA-256 해시입니다. 해시를 클릭하여 해당 해시에 대한 AutoFocus 검색을 시작합니다.
파일 형식	샘플의 파일 형식입니다.
날짜 생성	WildFire가 샘플을 분석하고 WildFire 판정을 할당한 날짜와 시간입니다.
업데이트 날짜	WildFire가 샘플에 대한 WildFire 판정을 업데이트한 날짜 및 시간입니다.
평결	샘플에 대한 WildFire 평결: 양성, 그레이웨어, 멀웨어 또는 피싱.

구성 테이블 내보내기

관리 사용자는 정책 규칙 베이스, 개체, 관리되는 장치 및 인터페이스에 대한 데이터를 PDF 파일 또는 CSV 파일의 표 형식으로 내보낼 수 있습니다. 내보내는 데이터는 웹 인터페이스의 가시 데이터입니다. 필터링된 데이터의 경우 필터와 일치하는 데이터만 내보입니다. 필터를 적용하지 않으면 모든 데이터가 내보내집니다.

PDF 파일로 내보내는 경우 영어 설명만 지원됩니다.

암호와 같은 모든 중요한 데이터는 와일드카드(*) 기호로 숨습니다.

성공적인 구성 테이블 내보내기에서 시스템 로그 및 다운로드 링크가 생성됩니다. 다운로드 링크를 사용하여 PDF 또는 CSV 파일을 로컬로 저장합니다. 다운로드 링크가 포함된 창을 닫은 후 해당 특정 내보내기에 대한 다운로드 링크를 더 이상 사용할 수 없습니다.

테이블 데이터를 내보내기하려면 **PDF/CSV**를 클릭하고 다음 설정을 구성합니다.

내보내기 설정	설명
파일 이름	내보낸 데이터를 식별하기 위해 이름(최대 200자)을 입력합니다. 이 이름은 내보내기에서 생성되는 다운로드된 파일의 이름이 됩니다.
파일 유형	생성할 내보내기 출력 유형을 선택합니다. PDF 또는 CSV 형식을 선택할 수 있습니다.
페이지 크기	기본 페이지 크기는 Letter(8.5 x 11.0 인치)입니다. 페이지 크기를 변경할 수 없습니다. 기본적으로 PDF는 세로 방향으로 생성되고 최대 열 수를 수용하기 위해 가로 방향으로 변경됩니다.
설명 (PDF 전용)	설명(최대 255자)을 입력하여 내보내기에 대한 컨텍스트 및 추가 정보를 제공합니다.
테이블 데이터	내보낼 테이블 데이터를 표시합니다. 이전에 설정한 필터링 설정을 지워야 하는 경우 모든 열 표시를 클릭하여 선택한 정책 유형아래에 모든 정책 규칙을 표시합니다. 그런 다음 열을 추가하거나 제거하고 필요에 따라 필터를 적용할 수 있습니다.
모든 열 표시	모든 필터를 제거하고 모든 테이블 열을 표시합니다.

내보내기를 클릭하여 구성 테이블 다운로드 링크를 생성합니다.

부팅 모드 변경

일부 방화벽은 기본적으로 ZTP(Zero Touch Provisioning) 모드로 부팅됩니다. ZTP 구성을 선택하는 경우 시작하는 동안 입력이 필요하지 않습니다. 비 ZTP(표준) 방화벽을 배포하는 경우 CLI에 액세스하여 ZTP 모드를 종료해야 합니다.

ZTP 기능에 액세스하려면 *Panorama* 관리 서버에 *ZTP* 플러그인이 설치되어 있어야 합니다.

STEP 1 | 방화벽의 전원을 켠 후 PuTTY와 같은 터미널 에뮬레이터를 사용하여 다음 CLI 프롬프트를 확인합니다.

```
ZTP ### #### ## ### #### #######(#/###)[###]?
```

#를 입력합니다. 그러면 시스템에서 확인을 요청합니다. 다시 **yes**를 입력하여 방화벽을 표준 모드로 부팅합니다.

STEP 2 | (위의 CLI 프롬프트를 놓친 경우) 웹 인터페이스를 사용하여 부팅 모드를 변경할 수도 있습니다. 시작 프로세스 전이나 도중에 방화벽 로그인 화면으로 이동합니다. ZTP 모드에서 계속 부팅할지 아니면 표준 모드로 전환할지 묻는 메시지가 표시됩니다. ## ##를 선택하면 방화벽이 표준 모드에서 재부팅을 시작합니다.

STEP 3 | 표준 모드를 사용하는 경우 방화벽을 수동으로 설정하십시오. ZTP 모드를 사용하는 경우 Panorama 관리 서버에 정의된 장치 그룹 및 템플릿 구성은 ZTP 서비스에 의해 방화벽에 자동으로 푸시됩니다.

- (표준 모드) 컴퓨터의 IP 주소를 192.168.1.2와 같은 192.168.1.0/24 네트워크의 주소로 변경합니다. 웹 브라우저에서 https://192.168.1.1로 이동합니다. 메시지가 표시되면 기본 사용자 이름과 암호(admin/admin)를 사용하여 웹 인터페이스에 로그인합니다.
- (ZTP 모드) Panorama 관리자가 제공한 지침에 따라 ZTP 방화벽을 등록합니다. 일련번호(S/N으로 식별되는 12자리 숫자)와 청구 키(8자리 숫자)를 입력해야 합니다. 이 번호는 디바이스 뒷면에 부착된 스티커에 있습니다.

대시보드

대시보드 위젯에는 소프트웨어 버전, 각 인터페이스 상태, 리소스 사용률 및 각 여러 로그 유형에 대해 최대 10개의 항목과 같은 일반 방화벽 또는 Panorama™ 정보가 표시됩니다. 로그 위젯은 마지막 시간의 항목을 표시합니다.

대시보드 위젯 항목에서는 대시보드 사용 방법을 설명하고 사용 가능한 위젯을 설명합니다.

대시보드 위젯

기본적으로 대시보드에는 위젯이 **3**개의 열 레이아웃으로 표시되지만 대신 **2**개의 열만 표시하도록 대시보드를 사용자 지정할 수 있습니다.

모니터링하려는 위젯만 표시되도록 표시하거나 숨길 위젯을 결정할 수도 있습니다. 위젯을 표시하려면 위젯 드롭다운에서 위젯 카테고리를 선택한 다음 대시보드에 추가할 위젯을 선택합니다. 흐리게 표시된 텍스트로 표시되는 위젯 이름은 이미 표시되어 있습니다. 위젯을 닫아 위젯(위젯 헤더의 ×)을 숨깁니다(표시 중지). 방화벽과 Panorama는 로그인 시 위젯 디스플레이 설정을 저장합니다(각 관리자마다 별도).

대시보드 데이터가 마지막으로 새로 고쳐진 시점을 확인하려면 마지막으로 업데이트된 타임스탬프를 참조하십시오. 전체 대시보드(대시보드 오른쪽 상단의)를 수동으로 새로 고치거나 개별 위젯(각 위젯 헤더 내의)을 새로 고칠 수 있습니다. 수동 대시보드 새로 고침 옵션( ) 옆에 있는 레이블이 지정되지 않은 드롭다운을 사용하여 전체 대시보드에 대한 자동 새로 고침 인터벌(분)을 선택합니다. **1**분, **2**분 또는 **5**분. 전체 대시보드에 대해 자동 새로 고침을 비활성화하려면 수동을 선택합니다.

대시보드 위젯	설명
애플리케이션 위젯	
상위 애플리케이션	세션이 가장 많은 애플리케이션을 표시합니다. 블록 크기는 세션의 상대적 수를 나타내며(블록 위로 마우스를 가져가면 숫자를 볼 수 있음), 색상은 녹색(가장 낮은)에서 빨간색(가장 높은) 까지의 보안 위험을 나타냅니다. 애플리케이션을 클릭하여 해당 애플리케이션 프로파일을 봅니다.
상위 고위험 애플리케이션	세션이 가장 많은 가장 위험도가 높은 애플리케이션을 표시한다는 점을 제외하면 상위 애플리케이션과 유사합니다.
ACC 위험 요소	지난 주에 처리된 네트워크 트래픽의 평균 위험 요소(1-5)를 표시합니다. 값이 높을수록 위험이 높다는 의미입니다.
시스템 위젯	
일반 정보	방화벽 또는 파노라마 이름 및 모델, 파노라마 CPU 및 RAM, 파노라마 시스템 모드, PAN-OS® 또는 파노라마 소프트웨어 버전, IPv4 및 IPv6 관리 IP 정보, 일련 번호, CPU ID 및 UUID, 애플리케이션, 위협, URL 필터링 정의 버전, 현재 날짜 및 시간, 마지막 재시작 이후 경과된 시간을 나타냅니다.
인터페이스 (방화벽만 해당)	각 인터페이스가 작동(녹색), 작동 중지(빨간색) 또는 알 수 없는 상태(회색)인지의 여부를 나타냅니다. PoE(Power over Ethernet)를 지원하는 인터페이스에는 번개 아이콘이 표시됩니다. 인터페이스 위로 마우스 커서를 가져가면 링크 구성 및 상태 정보가 표시됩니다. 포트 유형에 따라 링크 속도, 링크 듀플렉스 및 PoE 정보와 같은 추가 세부 정보가 표시됩니다.

대시보드 위젯	설명
시스템 리소스	관리 CPU 사용량, 데이터 플레인 사용량 및 세션 수(방화벽 또는 Panorama를 통해 설정된 세션 수)를 표시합니다.
고가용성	HA(고가용성)가 활성화된 경우 로컬 및 피어 방화벽/Panorama의 HA 상태(녹색(활성), 노란색(수동) 또는 검은색(기타)을 나타냅니다. HA에 대한 자세한 내용은 디바이스 > 고가용성 또는 Panorama > 고가용성을 참조하십시오.
HA 클러스터	HA 클러스터가 활성화되면 클러스터 통계와 클러스터의 각 구성원에 대한 HA4 및 HA4_backup 링크의 Keep Alive 값을 나타냅니다.
잠금	관리자가 설정한 구성 잠금을 표시합니다.
로그인한 관리자	현재 로그인한 각 관리자의 소스 IP 주소, 세션 유형(웹 인터페이스 또는 CLI) 및 세션 시작 시간을 표시합니다.
PoE 전력 예산 (지원되는 방화벽만 해당)	PoE(Power over Ethernet)를 사용할 때 구성된 인터페이스의 총 전력 예산 및 총 할당 전력을 표시합니다. 도넛형 차트는 방화벽에서 사용 가능한 전력을 확인하고 PoE 포트에 연결할 전원 장치(PD)를 결정하는 데 도움이 됩니다.
로그 위젯	
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. 지난 60분 동안의 항목만 표시합니다.
URL 필터링 로그	URL 필터링 로그의 최근 60분 동안의 설명과 날짜 및 시간을 표시합니다.
데이터 필터링 로그	데이터 필터링 로그에 지난 60분 동안의 설명과 날짜 및 시간을 표시합니다.
구성 로그	구성 로그의 마지막 10개 항목에 대한 관리자 사용자명, 클라이언트(웹 인터페이스 또는 CLI) 및 날짜와 시간을 표시합니다. 지난 60분 동안의 항목만 표시합니다.
시스템 로그	시스템 로그의 마지막 10개 항목에 대한 설명과 날짜 및 시간을 표시합니다. "구성 설치" 항목은 구성 변경 사항이 성공적으로 커밋되었음을 나타냅니다. 지난 *60*분 동안의 항목만 표시합니다.

ACC

애플리케이션 명령 센터(ACC)는 네트워크 내의 활동에 대한 실행 가능한 인텔리전스를 제공하는 분석 도구입니다. ACC는 방화벽 로그를 사용하여 네트워크의 트래픽 추세를 그래픽으로 묘사합니다. 그래픽 표현을 사용하면 네트워크 사용 패턴, 트래픽 패턴 및 의심스러운 활동 및 변칙을 포함하여 네트워크의 이벤트 간의 관계를 시각화할 수 있습니다.

- ACC 훑어보기
- ACC 탭
- ACC 위젯
- ACC 작업
- 탭 및 위젯 작업
- 필터-로컬 필터 및 전역 필터 작업

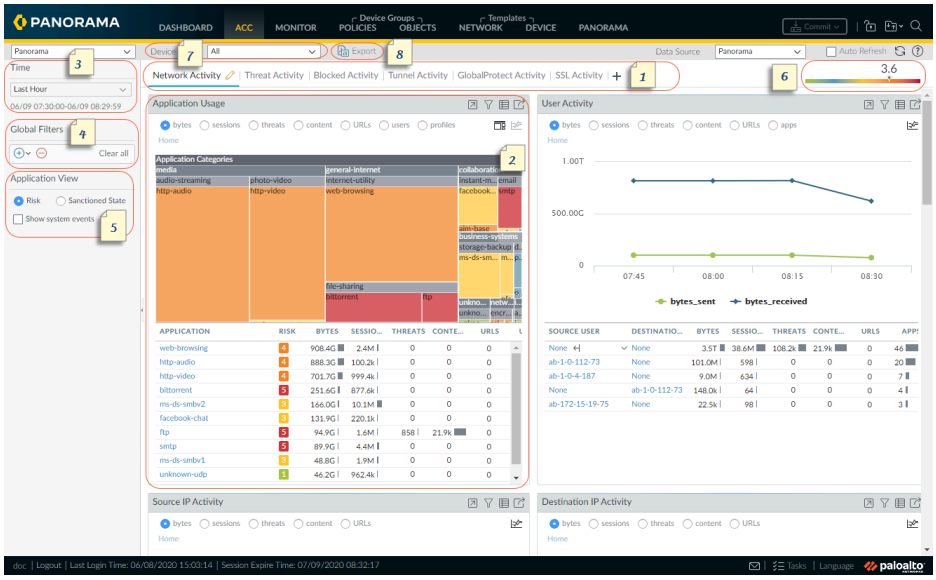
더 찾고 계십니까**?**

애플리케이션 명령 센터 사용 참조.

ACC 훑어보기

다음 표는 ACC 탭을 보여주고 각 구성 요소에 대해 설명합니다.

ACC 훑어보기



1	탭	ACC에는 네트워크 트래픽, 위협 활동, 차단된 활동, 터널 활동 및 모바일 네트워크 활동(GTP 보안이 활성화된 경우)에 대한 가시성을 제공하는 사전 정의된 탭이 포함되어 있습니다. 각 탭에 대한 정보는 ACC 탭을 참조하십시오.
2	위젯	각 탭에는 해당 탭과 관련된 이벤트 및 추세를 가장 잘 나타내는 기본 위젯 세트가 포함되어 있습니다. 위젯을 사용하면 바이트(입력 및 출력), 세션, 콘텐츠(파일 및 데이터), URL 카테고리, 애플리케이션, 사용자, 위협(악성, 양성, 그레이웨어, 피싱) 및 개수와 같은 필터를 사용하여 데이터를 검토할 수 있습니다. 각 위젯에 대한 정보는 ACC 위젯을 참조하세요.
3	시간	각 위젯의 차트와 그래프는 실시간 및 기록 보기를 제공합니다. 사용자 지정 범위를 선택하거나 지난 15분에서 최대 지난 90일 또는 지난 30일까지의 사전 정의된 기간을 사용할 수 있습니다. 기본적으로 데이터를 렌더링하는 데 사용되는 기간은 마지막 시간입니다. 날짜와 시간 인터벌이 화면에 표시됩니다. 예: `11/11 10:30:00-01/12 11:29:59`

ACC 훑어보기		
4	전역 필터	전역 필터를 사용하면 모든 탭에 필터를 설정할 수 있습니다. 차트와 그래프는 데이터를 렌더링하기 전에 선택한 필터를 적용합니다. 필터 사용에 대한 자세한 내용은 ACC 작업을 참조하십시오.
5	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 애플리케이션을 나타내고 노란색은 다른 가상 시스템 또는 디바이스 그룹에서 승인된 상태가 다른 애플리케이션을 나타냅니다.
6	위험 측정기	위험 측정기(1=최저에서 5=최고)는 네트워크의 상대적 보안 위험을 나타냅니다. 위험 측정기는 네트워크에서 볼 수 있는 애플리케이션의 유형 및 애플리케이션과 관련된 위험 수준, 차단된 위협의 수를 통해 볼 수 있는 위협 활동 및 멀웨어, 손상된 호스트 또는 멀웨어 호스트 및 도메인에 대한 트래픽과 같은 다양한 요소를 사용합니다.
7	소스	디스플레이에 사용되는 데이터는 방화벽과 Panorama™ 간에 다릅니다. ACC에서 보기를 생성하는 데 사용할 데이터를 선택하는 옵션은 다음과 같습니다. 가상 시스템: 여러 가상 시스템에 대해 활성화된 방화벽에서 가상 시스템 드롭다운을 사용하여 모든 가상 시스템 또는 선택한 가상 시스템만 포함하도록 ACC 디스플레이를 변경할 수 있습니다. 디바이스 그룹: Panorama에서 디바이스 그룹 드롭다운을 사용하여 모든 디바이스 그룹 또는 선택한 디바이스 그룹의 데이터만 포함하도록 ACC 디스플레이를 변경할 수 있습니다. 데이터 소스: Panorama에서는 **Panorama** 또는 원격 디바이스 데이터(관리되는 방화벽 데이터)를 사용하도록 디스플레이를 변경할 수도 있습니다. 데이터 소스가 **Panorama**인 경우 특정 디바이스 그룹에 대한 디스플레이를 필터링할 수 있습니다.
8	내보내기	현재 탭에 표시된 위젯을 PDF로 내보낼 수 있습니다.

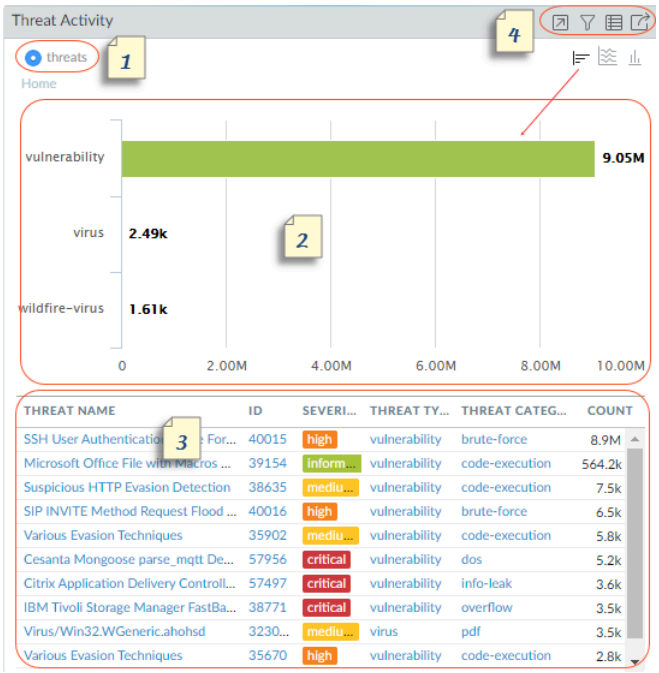
ACC 탭

- 네트워크 활동 - 네트워크의 트래픽 및 사용자 활동에 대한 개요를 표시합니다. 이 보기는 가장 많이 사용되는 애플리케이션, 사용자가 액세스하는 바이트, 콘텐츠, 위협 및 URL에 대한 드릴다운을 통해 트래픽을 생성하는 최상위 사용자 및 트래픽 일치가 발생하는 가장 많이 사용되는 보안 정책 규칙에 중점을 둡니다. 또한 소스 또는 대상 영역, 지역 또는 IP 주소별로 네트워크 활동을 볼 수 있습니다. 인그레스(ingress) 또는 이그레스(Egress) 인터페이스에 의해 네트워크에서 가장 일반적으로 사용되는 디바이스의 운영 체제와 같은 호스트 정보에 따라 다릅니다.
- 위협 활동 - 네트워크의 위협에 대한 개요를 표시합니다. 취약점, 스파이웨어, 바이러스, 악성 도메인 또는 URL을 방문하는 호스트, 파일 유형 및 애플리케이션별 상위 WildFire 제출, 비표준 포트를 사용하는 애플리케이션과 같은 주요 위협에 중점을 둡니다. 손상된 호스트 위젯은 더 나은 시각화 기술로 탐지를 보완합니다. 상관 이벤트 탭(모니터 > 자동 연동 엔진 > 상관 이벤트)의 정보를 사용하여 심각도에 따라 정렬된 소스 사용자 또는 IP 주소별로 네트워크의 손상된 호스트에 대한 통합 보기를 제공합니다.
- 차단된 활동 - 네트워크로 들어오는 것을 차단한 트래픽에 초점을 맞춥니다. 이 탭의 위젯을 사용하면 애플리케이션 이름, 사용자명, 위협 이름, 콘텐츠(파일 및 데이터) 및 트래픽을 차단한 거부 작업이 포함된 최상위 보안 규칙별로 거부된 활동을 볼 수 있습니다.
- 모바일 네트워크 활동 - 보안 정책 규칙 구성에서 생성된 GTP 로그를 사용하여 네트워크의 모바일 트래픽을 시각적으로 표시합니다. 이 보기에는 ACC 필터를 적용하고 드릴다운하여 필요한 정보를 분리할 수 있는 대화형 및 사용자 정의가 가능한 GTP 이벤트, 모바일 가입자 활동 및 GTP 거부 원인 위젯이 포함됩니다. SCTP 보안을 활성화하면 이 탭의 위젯에 방화벽의 SCTP 이벤트 세부 정보와 시각적 표현, SCTP 연결 ID당 보내고 받은 청크 수가 표시됩니다.
- 터널 활동 - 방화벽이 터널 검사 정책에 따라 검사한 터널 트래픽 활동을 표시합니다. 정보에는 터널 ID, 모니터 태그, 사용자 및 GRE(Generic Routing Encapsulation), GTP-U(사용자 데이터용 GPRS) 터널링 프로토콜 및 비암호화 IPSec와 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, 분리된 엔드포인트 수가 포함됩니다.
- **SSL** 활동 - 복호화 정책 및 프로파일에 따라 복호화 및 복호화되지 않은 TLS/SSL 트래픽의 활동을 표시합니다. 비 TLS 활동과 비교한 TLS 활동, 복호화 트래픽 대 복호화되지 않은 트래픽 양, 복호화 실패 이유, 성공적인 TLS 버전 및 키 교환 활동을 볼 수 있습니다. 이 정보를 사용하여 복호화 문제를 일으키는 트래픽을 식별한 다음 복호화 로그 및 사용자 지정 복호화 보고서 템플릿을 사용하여 세부 정보로 드릴다운하고 해당 트래픽에 대한 컨텍스트를 얻어 문제를 정확하게 진단하고 수정할 수 있습니다.

탭 및 위젯 작업에 설명된 대로 탭과 위젯을 사용자 정의할 수도 있습니다.

ACC 위젯

각 탭의 위젯은 대화형입니다. 필터를 설정하고 디스플레이로 드릴다운하여 뷰를 사용자 지정하고 필요한 정보에 집중할 수 있습니다.



각 위젯은 다음 정보를 표시하도록 구성됩니다.

1	보기	바이트, 세션, 위협, 카운트, 사용자, 콘텐츠, 애플리케이션, URL, 악의적인, 양성, 그레이웨어, 피싱, 파일(이름), 데이터, 프로파일, 개체, 포털, 게이트웨이 및 프로파일로 데이터를 정렬할 수 있습니다. 사용 가능한 옵션은 위젯에 따라 다릅니다.
2	그래프	그래픽 표시 옵션은 트리맵, 선 그래프, 수평 막대 그래프, 누적된 영역 그래프, 누적된 막대 그래프, 원형 차트 및 맵입니다. 사용 가능한 옵션은 위젯마다 다르며 상호 작용 환경은 각 그래프 유형에 따라 다릅니다. 예를 들어 비표준 포트를 사용하는 애플리케이션의 위젯을 사용하면 트리맵과 선 그래프 중에서 선택할 수 있습니다. 디스플레이로 드릴다운하려면 그래프를 클릭합니다. 클릭한 영역은 필터가 되고 해당 선택에 대한 자세한 정보를 확대 및 볼 수 있습니다.
3	테이블	그래프를 렌더링하는 데 사용되는 데이터의 자세한 보기는 그래프 아래 표에 표시됩니다. 테이블의 요소에 대한 로컬 필터 또는 전역 필터를 클릭하고 설정할 수 있습니다. 로컬 필터를 사용하면 그래프가 업데이트되고 테이블은 해당 필터로 정렬됩니다.

		전역 필터를 사용하면 ACC 전체의 뷰가 필터에 특정한 정보만 표시합니다.
4	작업	다음은 위젯의 제목 표시줄에서 사용할 수 있는 작업입니다. • 보기 최대화 - 위젯을 확대하여 더 큰 화면 공간에서 볼 수 있습니다. 최대화된 뷰에서 기본 위젯 보기에 표시되는 상위 10개 이상의 항목을 볼 수 있습니다. • 로컬 필터 설정 - 위젯내에서 디스플레이를 구체화하는 필터를 추가할 수 있습니다. 필터 - 로컬 필터 및 전역 필터로 작업을 참조하십시오. • 로그로 이동 - 로그(모니터 > 로그 > **<log-type>**)로 직접 이동할 수 있습니다. 로그는 그래프가 렌더링되는 기간을 사용하여 필터링됩니다. 로컬 및 글로벌 필터를 설정하면 로그 쿼리가 기간과 필터를 연결하고 필터 세트와 일치하는 로그만 표시합니다. • 내보내기 - 그래프를 PDF로 내보낼 수 있습니다.

각 위젯에 대한 설명은 ACC 사용에 대한 세부 정보를 참조하십시오.

ACC 작업

ACC 디스플레이를 사용자 지정하고 구체화하려면 탭을 추가하고 삭제하고 위젯을 추가하고 삭제하고 로컬 및 전역 필터를 설정하고 위젯과 상호 작용할 수 있습니다.

- 탭 및 위젯 작업
- 필터-로컬 필터 및 전역 필터 작업

탭 및 위젯 작업

다음 옵션은 탭 및 위젯을 사용하고 사용자 지정하는 방법을 설명합니다.

- 사용자 지정 탭을 추가합니다.
  1. 탭 목록을 따라 추가(＋)를 선택합니다.
  2. 보기 이름을 추가합니다. 이 이름은 탭의 이름으로 사용됩니다. 최대 10개의 사용자 정의 탭을 추가할 수 있습니다.

- 탭을 편집합니다.

  탭을 선택하고 탭 이름 옆에 편집을 클릭하여 탭을 편집합니다.

  예: Threat Activity.

- 탭을 기본값으로 설정
  1. 탭을 편집합니다.
  2. 현재 탭을 기본값으로 설정하도록 선택합니다. 방화벽에 로그인할 때마다 이 탭이 표시됩니다.

- 탭 상태 저장
  1. 탭을 편집합니다.
  2. 현재 탭의 기본 설정을 기본값으로 저장하려면 을(를) 선택합니다.

     설정할 수 있는 필터를 포함한 탭 상태는 HA 피어 간에 동기화됩니다.

- 탭 내보내기
  1. 탭을 편집합니다.
  2. 을(를) 선택하여 현재 탭을 내보냅니다. 탭은 .txt 파일로 컴퓨터에 다운로드됩니다. 파일을 다운로드하려면 팝업을 활성화해야 합니다.

- 탭 가져오기
  1. 사용자 지정 탭을 추가합니다.
  2. 탭을 가져오려면 을(를) 선택합니다.
  3. 텍스트(.txt) 파일로 찾아본 다음 선택합니다.

- 뷰에 포함된 위젯을 확인합니다.
  1. 보기를 선택하고 편집( )을 클릭합니다.
  2. 선택한 위젯 추가 드롭다운을 선택합니다.

- 위젯 또는 위젯 그룹을 추가합니다.
  1. 새 탭을 추가하거나 미리 정의된 탭을 편집합니다.
  2. 위젯 추가를 선택한 다음 추가할 위젯을 선택합니다. 위젯은 최대 12개까지 선택할 수 있습니다.
  3. (선택사항) 두 열 구성의 레이아웃을 만들려면 위젯 추가 그룹을 선택합니다. 위젯을 두 열 구성의 디스플레이에 드래그하고 드롭할 수 있습니다. 위젯을 레이아웃으로 드래그하면 자리 표시자가 위젯을 삭제할 수 있습니다.

     위젯 그룹의 이름을 지정할 수 없습니다.

- 탭, 위젯 또는 위젯 그룹을 삭제합니다.
  - 사용자 지정 탭을 삭제하려면 탭을 선택하고 삭제(Test)를 클릭합니다.

    미리 정의된 탭은 삭제할 수 없습니다.
  - 위젯 또는 위젯 그룹을 삭제하려면 탭을 편집한 다음 삭제([X])를 클릭합니다. 삭제를 취소할 수 없습니다.

- 기본 보기를 재설정합니다.

  차단된 활동 보기와 같이 미리 정의된 뷰에서는 하나 이상의 위젯을 삭제할 수 있습니다. 탭의 기본 위젯 집합을 포함하도록 레이아웃을 재설정하려면 탭을 편집하고 보기 재설정을 합니다.

필터-로컬 필터 및 전역 필터 작업

세부 정보를 다듬고 ACC가 표시하는 내용을 미세하게 제어하려면 필터를 사용할 수 있습니다.

- 로컬 필터— 로컬 필터는 특정 위젯에 적용됩니다. 로컬 필터를 사용하면 그래프와 상호 작용하고 디스플레이를 사용자 정의할 수 있으므로 세부 정보를 자세히 살펴보고 특정 위젯에서 모니터링하려는 정보에 액세스할 수 있습니다. 로컬 필터를 그래프 또는 테이블의 속성으로 클릭하는 두 가지 방법으로 적용할 수 있습니다. 또는 위젯 내에서 필터 설정을 선택합니다. 필터 설정을 사용하면 재부팅 시 지속되는 로컬 필터를 설정할 수 있습니다.

- 전역 필터-전역 필터는 ACC 전체에 적용됩니다. 전역 필터를 사용하면 가장 관심 있는 세부 정보 주위에 디스플레이를 피벗하고 현재 디스플레이에서 관련없는 정보를 제외할 수 있습니다. 예를 들어 특정 사용자 및 애플리케이션과 관련된 모든 이벤트를 보려면 사용자의 IP 주소를 적용하고 애플리케이션을 지정하여 ACC의 모든 탭 및 위젯을 통해 해당 사용자 및 애플리케이션과 관련된 정보만 표시하는 전역 필터를 만들 수 있습니다. 전역 필터는 로그인 간에 지속되지 않습니다.

  전역 필터는 다음과 같은 세 가지 방법으로 적용할 수 있습니다.

- 테이블에서 전역 필터 설정—모든 위젯의 테이블에서 속성을 선택하고 속성을 전역 필터로 적용합니다.
- 위젯 필터를 전역 필터로 추가합니다—속성 위로 마우스를 가져가고 속성 오른쪽에 있는 화살표 아이콘을 클릭합니다. 이 옵션을 사용하면 위젯에 사용되는 로컬 필터를 높이고 전역으로 속성을 적용하여 ACC의 모든 탭에서 디스플레이를 업데이트할 수 있습니다.
- 전역 필터 정의—ACC의 전역 필터 창을 사용하여 필터를 정의합니다.

- 로컬 필터를 설정합니다.

  그래프 아래 표의 속성을 클릭하여 로컬 필터로 적용할 수도 있습니다.

  1. 위젯을 선택하고 필터( )를 클릭합니다.
  2. 적용할 필터( )를 추가합니다.
  3. 적용을 클릭합니다. 이러한 필터는 재부팅 전반에 걸쳐 지속됩니다.

     위젯 이름 옆에는 위젯에 적용된 로컬 필터 수가 표시됩니다.

- 테이블에서 전역 필터를 설정합니다.

  테이블의 속성 위로 마우스를 가져가고 속성 오른쪽에 나타나는 화살표를 클릭합니다.

- 전역 필터 창을 사용하여 전역 필터를 설정합니다.

  적용할 필터( )를 추가합니다.

- 로컬 필터를 전역 필터로 확장합니다.
  1. 위젯의 테이블에서 속성을 선택합니다. 이렇게 하면 속성이 로컬 필터로 설정됩니다.
  2. 필터를 전역 필터로 승격하려면 속성 위로 마우스를 가져가서 속성 오른쪽에 있는 화살표를 클릭합니다.

- 필터를 제거합니다.

  필터를 제거하려면 제거( )를 클릭합니다.

  - 전역 필터—전역 필터 창에 위치합니다.
  - 로컬 필터—필터를 클릭하여 로컬 필터 설정 대화 상자를 가져온 다음 필터를 선택하고 제거합니다.

- 모든 필터를 지웁니다.

  - 전역 필터—모두 지우기 전역 필터.
  - 로컬 필터—위젯을 선택하고 필터를 클릭합니다( ). 그런 다음 로컬 필터 설정 위젯에서 모두 지우기를 합니다.

- 무효 필터.

  속성 및 무효( ) 필터를 선택합니다.

  - 전역 필터—전역 필터 창에 위치합니다.
  - 로컬 필터—필터를 클릭하여 로컬 필터 설정 대화 상자가 필터를 추가한 다음 무효화합니다.

- 사용 중인 필터를 봅니다.

  - 전역 필터—적용된 전역 필터 수가 전역 필터 아래 왼쪽 창에 표시됩니다.
  - 로컬 필터— 위젯에 적용되는 로컬 필터 수가 위젯 이름 옆에 표시됩니다. 필터를 보려면 로컬 필터 설정을 클릭합니다.

모니터

다음 항목에서는 네트워크 활동을 모니터링하는 데 사용할 수 있는 방화벽 보고서 및 로그에 대해 설명합니다.

모니터 > 로그

다음 항목에서는 모니터링 로그에 대한 추가 정보를 제공합니다.

무엇을 알고 싶습니까?	참조:
다양한 유형의 로그에 대해 알려주세요.	로그 유형
로그를 필터링합니다. 로그를 내보냅니다. 개별 로그 항목에 대한 세부 정보를 봅니다. 로그 표시를 수정합니다.	로그 작업
더 찾고 계십니까?	로그를 모니터링하고 관리합니다.

로그 유형

- 모니터 > 로그

방화벽은 역할 기반 관리 권한이 존중되도록 모든 로그를 표시합니다. 보고 있는 로그 유형에 따라 달라지는 정보만 볼 수 있습니다. 관리자 권한에 대한 자세한 내용은 디바이스 > 관리자 역할을 참조하십시오.

로그 유형	설명
교통	각 세션의 시작과 끝 항목을 표시합니다. 각 항목에는 날짜 및 시간, 소스 및 대상 영역, 주소 및 포트, 애플리케이션 이름, 흐름에 적용된 보안 규칙 이름, 규칙 작업(허용, 거부 또는 삭제), 수신 및 이그레스(egress) 인터페이스, 바이트 수 및 세션 종료 이유가 포함됩니다. 유형 열은 항목이 세션의 시작 또는 끝인지의 여부 또는 세션이 거부 또는 삭제되었는지의 여부를 나타냅니다. "삭제"는 트래픽을 차단한 보안 규칙이 "모든" 애플리케이션을 지정했음을 나타내고 "거부"는 규칙이 특정 애플리케이션을 식별했음을 나타냅니다. 규칙이 특정 서비스에 대한 모든 트래픽을 삭제하는 경우와 같이 애플리케이션이 식별되기 전에 트래픽이 삭제되면 애플리케이션은 "적용 불가"로 표시됩니다. 개별 항목, 아티팩트 및 작업에 대한 자세한 내용은 트래픽 로그에서 드릴다운하십시오.

로그 유형	설명
	• 세부 정보()를 클릭하면 ICMP 항목이 동일한 소스와 대상 간의 여러 세션을 통합하는지의 여부(개수 값이 1보다 큼)와 같은 세션에 대한 추가 세부 정보를 볼 수 있습니다. • 활성 AutoFocus™ 라이선스가 있는 방화벽에서 로그 항목에 포함된 IP 주소, 파일 이름, URL, 사용자 에이전트, 위협 이름 또는 해시 옆에 마우스를 놓고 드롭다운()을 클릭하여 해당 아티팩트에 대한 AutoFocus 인텔리전스 요약을 엽니다. • 검역 목록(디바이스 > 디바이스 검역)에 디바이스를 추가하려면 디바이스의 호스트 **ID** 드롭다운 및 디바이스 차단(팝업 대화상자에서)을 엽니다.
위협	방화벽에서 생성된 각 보안 경보에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 위협 이름 또는 URL, 소스 및 대상 영역, 주소 및 포트, 애플리케이션 이름, 흐름에 적용된 보안 규칙 이름, 경보 작업(허용 또는 차단) 및 심각도가 포함됩니다. 유형 열은 "바이러스" 또는 "스파이웨어"와 같은 위협 유형을 나타내고, 이름 열은 위협 설명 또는 URL입니다. 카테고리 열은 위협 카테고리(예: "키로거") 또는 URL 카테고리입니다. 개별 항목, 아티팩트 및 작업에 대한 자세한 내용은 위협 로그에서 드릴다운하십시오. • 항목이 동일한 소스와 대상 간에 동일한 유형의 여러 위협을 통합하는지의 여부(개수 값은 1보다 큼)와 같은 위협에 대한 추가 세부 정보를 보려면 세부 정보()를 클릭합니다. • 활성 AutoFocus 라이선스가 있는 방화벽에서 로그 항목에 포함된 IP 주소, 파일 이름, URL, 사용자 에이전트, 위협 이름 또는 해시 옆에 마우스를 놓고 드롭다운()을 클릭하여 해당 아티팩트에 대한 AutoFocus 인텔리전스 요약을 엽니다. • 로컬 패킷 캡처가 활성화된 경우 다운로드()를

로그 유형	설명
	클릭하여 캡처된 패킷에 액세스합니다. 로컬 패킷 캡처를 활성화하려면 **Objects** > **Security Profiles**의 하위 섹션을 참조하십시오. • 위협에 대한 자세한 내용을 보거나 위협 로그에서 직접 위협 예외를 신속하게 구성하려면 이름 열에서 위협 이름을 클릭합니다. 면제 프로파일 목록에는 모든 사용자 지정 바이러스 백신, 안티 스파이웨어 및 취약성 보호 프로파일이 표시됩니다. 위협 서명에 대한 면제를 구성하려면 보안 프로파일 이름 왼쪽에 있는 체크박스를 선택한 다음 변경 사항을 저장합니다. IP 주소에 대한 예외를 추가하려면(서명당 최대 100개의 IP 주소) 보안 프로파일을 강조 표시하고 예외 IP 주소 섹션에 IP 주소를 추가한 다음 확인을 클릭하여 저장합니다. 예외를 보거나 수정하려면 연결된 보안 프로파일로 이동하여 예외 탭을 클릭합니다. 예를 들어 위협 유형이 취약성인 경우 개체 > 보안 프로파일 > 취약성 보호를 선택한 다음 연결된 프로파일을 클릭하고 예외 탭을 클릭합니다. • 검역 목록(디바이스 > 디바이스 검역)에 디바이스를 추가하려면 디바이스의 호스트 **ID** 드롭다운 및 디바이스 차단(팝업 대화상자에서)을 엽니다.
URL 필터링	웹사이트에 대한 액세스를 제어하고 사용자가 웹사이트에 자격 증명을 제출할 수 있는지의 여부를 제어하는 URL 필터에 대한 로그를 표시합니다. 개체 > 보안 프로파일 > URL 필터링을 선택하여 차단하거나 허용할 URL 카테고리와 자격 증명 제출을 허용하거나 비활성화할 URL 필터링 설정을 정의합니다. URL에 대한 HTTP 헤더 옵션의 로깅을 활성화할 수도 있습니다. 활성 AutoFocus 라이선스가 있는 방화벽에서 로그 항목에 포함된 IP 주소, 파일 이름, URL, 사용자 에이전트, 위협 이름 또는 해시 옆에 마우스를 놓고 드롭다운( )을 클릭하여 해당 아티팩트에 대한 AutoFocus 인텔리전스 요약을 엽니다.
WildFire Submissions	방화벽이 WildFire™ 분석을 위해 포워딩한 파일 및 이메일 링크에 대한 로그를 표시합니다. WildFire 클라우드는 샘플을 분석하고 샘플에 할당된 WildFire 판정(양성, 멀웨어, 그레이웨어 또는 피싱)을 포함하는 분석 결과를 반환합니다. 작업 열을 보면 방화벽이 보안

로그 유형	설명
	정책 규칙에 따라 파일을 허용 또는 차단했는지 확인할 수 있습니다. 활성 AutoFocus 라이선스가 있는 방화벽에서 로그 항목에 포함된 IP 주소, 파일 이름, URL, 사용자 에이전트, 위협 이름 또는 해시(파일 다이제스트 열) 옆에 마우스를 놓고 드롭다운을 클릭하여 아티팩트에 대한 AutoFocus Intelligence Summary를 엽니다.
데이터 필터링	연결된 데이터 필터링 프로파일과 함께 보안 정책에 대한 로그를 표시하여 신용 카드나 주민등록번호와 같은 민감한 정보가 방화벽으로 보호되는 영역을 벗어나는 것을 방지하고 특정 파일 유형이 업로드 또는 다운로드되는 것을 방지하는 파일 차단 프로파일을 표시합니다. 로그 항목에 대한 세부 정보에 액세스하기 위해 암호 보호를 구성하려면 을 클릭합니다. 암호를 입력하고 확인을 클릭합니다. 데이터 보호 암호 변경 또는 삭제에 대한 지침은 디바이스 > 응답 페이지를 참조하십시오. 시스템은 세션당 한 번만 암호를 입력하라는 메시지를 표시합니다.
HIP 매치	에이전트가 보고한 원시 HIP 데이터를 정의된 HIP 개체 및 HIP 프로파일과 비교할 때 GlobalProtect™ 게이트웨이가 식별하는 모든 HIP 일치 항목을 표시합니다. 다른 로그와 달리 보안 정책과 일치하지 않는 경우에도 HIP 일치가 기록됩니다. 자세한 내용은 네트워크 > GlobalProtect > 포털을 참조하십시오. 격리 목록(**Device** > **Device Quarantine**)에 디바이스를 추가하려면 해당 디바이스의 호스트 **ID** 드롭다운 및 디바이스 차단(팝업 대화 상자에서)을 엽니다.
GlobalProtect	GlobalProtect 연결 로그를 표시합니다. 이 정보를 사용하여 GlobalProtect 사용자 및 해당 클라이언트 OS 버전을 식별하고, 연결 및 성능 문제를 해결하고, 사용자가 연결하는 포털 및 게이트웨이를 식별하십시오. 검역 목록(디바이스 > 디바이스 검역)에 디바이스를 추가하려면 디바이스의 호스트 **ID** 드롭다운 및 디바이스 차단(팝업 대화 상자에서)을 엽니다.

로그 유형	설명
IP 태그	태그가 특정 IP 주소에 적용된 방법과 시기에 대한 정보를 표시합니다. 이 정보를 사용하여 특정 IP 주소가 주소 그룹에 배치된 시기와 이유와 해당 주소에 영향을 주는 정책 규칙을 결정합니다. 로그에는 수신 시간(세션의 첫 번째 및 마지막 패킷이 도착한 날짜 및 시간), 가상 시스템, 소스 IP 주소, 태그, 이벤트, 타임아웃, 소스 이름 및 소스 유형이 포함됩니다.
User-ID™	매핑 정보의 소스, User-ID 에이전트가 매핑을 수행한 시간 및 매핑이 만료되기까지 남은 시간과 같은 IP 주소-사용자명 매핑에 대한 정보를 표시합니다. 이 정보를 사용하여 User-ID 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	GlobalProtect 세션을 포함하여 No Decryption 프로파일이 제어하는 트래픽에 대한 복호화 세션 및 복호화되지 않은 세션에 대한 정보를 표시합니다. 기본적으로 로그에는 실패한 SSL 복호화 핸드쉐이크에 대한 정보가 표시됩니다. 복호화 정책 규칙 옵션에서 성공적인 SSL 복호화 핸드쉐이크에 대한 로깅을 활성화할 수 있습니다. 로그에는 취약한 프로토콜 및 암호 제품군(키 교환, 암호화 및 인증 알고리즘), 우회된 복호화 활동, 복호화 실패 및 그 원인(예: 불완전한 인증서 체인, 클라이언트 인증, 고정된 인증서), 세션 종료 이유 등을 식별할 수 있는 풍부한 정보가 표시됩니다. 예를 들어 정보를 사용하여 약한 프로토콜과 알고리즘을 사용하는 사이트를 허용할지의 여부를 결정합니다. 비즈니스 목적으로 액세스할 필요가 없는 취약한 사이트는 차단하는 것이 좋습니다. 방화벽이 암호를 복호화하지 않고 비복호화 프로파일을 적용한 트래픽의 경우 서버 인증서 확인 문제로 인해 차단된 세션이 로그에 표시됩니다. 기본 복호화 로그 크기는 32MB입니다. 그러나 많은 양의 트래픽을 복호화하거나 성공적인 SSL 복호화 핸드쉐이크 로깅을 활성화한 경우에는 로그 크기를 늘려야 할 수 있습니다(**Device** > **Setup** > **Management** > **Logging** 및 보고 설정 및 로그 저장소 할당량 편집). 할당되지 않은 로그 공간이 없는 경우 복호화 로그 크기와 다른 로그 크기 간의 균형을 고려하십시오. 더 많이 로깅할수록 더 많은 리소스를 사용합니다.

로그 유형	설명
GTP	광범위한 GTP 속성에 대한 정보를 포함하는 이벤트 기반 로그를 표시합니다. 여기에는 GTP 이벤트 유형, GTP 이벤트 메시지 유형, APN, IMSI, IMEI, 최종 사용자 IP 주소와 애플리케이션, 발신지 및 목적지 주소, 타임스탬프와 같이 차세대 방화벽이 식별하는 TCP/IP 정보가 포함됩니다.
터널 검사	검사된 각 터널 세션의 시작 및 끝 항목을 표시합니다. 로그에는 수신 시간(세션의 첫 번째 및 마지막 패킷이 도착한 날짜 및 시간), 터널 ID, 모니터 태그, 세션 ID, 터널 트래픽에 적용된 보안 규칙 등이 포함됩니다. 자세한 내용은 정책 > 터널 검사를 참조하십시오.
SCTP	방화벽이 상태 저장 검사, 프로토콜 유효성 검사 및 SCTP 트래픽 필터링을 수행하는 동안 방화벽에서 생성된 로그를 기반으로 SCTP 이벤트 및 연결을 표시합니다. SCTP 로그에는 SCTP 이벤트 유형, 청크 유형, SCTP 원인 코드, Diameter 애플리케이션 ID, Diameter 명령 코드 및 청크와 같은 광범위한 SCTP 및 페이로드 프로토콜 속성에 대한 정보가 포함됩니다. 이 SCTP 정보는 소스 및 대상 주소, 소스 및 대상 포트, 규칙 및 타임스탬프와 같이 방화벽이 식별하는 일반 정보와 함께 제공됩니다. 자세한 내용은 개체 > 보안 프로파일 > SCTP 보호를 참조하십시오.
구성	각 구성 변경에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 관리자 사용자명, 변경이 이루어진 IP 주소, 클라이언트 유형(웹 인터페이스 또는 CLI), 실행된 명령 유형, 명령 성공 또는 실패 여부, 구성 경로, 변경 전과 후의 값.
체계	각 시스템 이벤트에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 이벤트 심각도 및 이벤트 설명이 포함됩니다.
알람	알람 로그는 시스템에서 생성된 알람에 대한 자세한 정보를 기록합니다. 이 로그의 정보는 경보에도 보고됩니다. 알람 설정 정의를 참조하십시오.
인증	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 대입 공격과 같은 네트워크에서 의심스러운 활동을 식별할 수도 있습니다. 선택적으로 인증 타임아웃을 기록하도록 인증 규칙을 구성할 수 있습니다. 이러한 타임아웃은 사용자가 리소스에 대해 한 번만 인

로그 유형	설명
	증해야 하지만 반복적으로 액세스할 수 있는 기간과 관련됩니다. 타임아웃에 대한 정보를 보면 타임아웃을 조정할지의 여부와 조정 방법을 결정하는 데 도움이 됩니다. 시스템 로그는 *GlobalProtect* 및 웹 인터페이스에 대한 관리자 액세스와 관련된 인증 이벤트를 기록합니다.
통합	최신 트래픽, 위협, URL 필터링, WildFire 제출 및 데이터 필터링 로그 항목을 단일 보기에 표시합니다. 집합적 로그 보기를 사용하면 이러한 서로 다른 유형의 로그를 함께 검토하고 필터링할 수 있습니다(각 로그 세트를 개별적으로 검색하는 대신). 또는 표시할 로그 유형을 선택할 수 있습니다. 필터 필드 왼쪽에 있는 화살표를 클릭하고 트래픽, 위협, **URL**, 데이터 및/또는 **Wildfire**를 선택하여 선택한 로그 유형만 표시합니다. 활성 AutoFocus 라이선스가 있는 방화벽에서 로그 항목에 포함된 IP 주소, 파일 이름, URL, 사용자 에이전트, 위협 이름 또는 해시 옆에 마우스를 놓고 드롭다운( )을 클릭하여 해당 아티팩트에 대한 AutoFocus 인텔리전스 요약을 엽니다. 방화벽은 역할 기반 관리 권한이 존중되도록 모든 로그를 표시합니다. 통합 로그를 볼 때 볼 수 있는 권한이 있는 로그만 표시됩니다. 예를 들어 WildFire 제출 로그를 볼 권한이 없는 관리자는 통합 로그를 볼 때 WildFire 제출 로그 항목을 볼 수 없습니다. 관리자 권한에 대한 자세한 내용은 디바이스 > 관리자 역할을 참조하세요. *AutoFocus* 위협 인텔리전스 포털에서 통합 로그 세트를 사용할 수 있습니다. AutoFocus 검색을 설정하여 *AutoFocus* 검색 필터를 통합 로그 필터 필드에 직접 추가합니다. 검역 목록(**Device** > **Device Quarantine**)에 디바이스를 추가하려면 디바이스의 호스트 **ID** 드롭다운 및 디바이스 차단(팝업 대화 상자에서)을 엽니다.

로그 작업

다음 표는 로그 작업을 설명합니다.

작업	설명
필터 로그	각 로그 페이지에는 페이지 상단에 필터 필드가 있습니다. IP 주소 나 시간 범위와 같은 아티팩트를 필드에 추가하여 일치하는 로그 항목을 찾을 수 있습니다. 필드 오른쪽 아이콘을 사용하면 필터를 적용, 지우기, 생성, 저장 및 로드할 수 있습니다.  • 필터 생성: • 로그 항목에서 아티팩트를 클릭하여 해당 아티팩트를 필터에 추가합니다. • 추 가( )를 클릭하여 새 검색 조건을 정의합니다. 각 기준에 대해 검색 유형(**and** 또는 **or**)을 정의하는 커넥터(또는)를 선택하여 검색을 기반으로 하는 특성, 검색 범위를 정의하는 연산자 및 로그 항목에 대한 평가값을 선택합니다. 각 기준을 필터 필드에추가하고 완료되면 닫습니다. 그런 다음 필터를 적용( )할 수 있습니다. ***Value*** 문자열이 ***Operator****(*예*: **has*** 또는 ***in)***와 일치하는 경우 구문 오류를 방지하기 위해 문자열을 따옴표로 묶습니다. 예를 들어 대상 국가별로 필터링하고 ***IN***을 값으로 사용하여 *INDIA*를 지정하는 경우 필터를 ***(dstloc eq "IN")***로 입력합니다. 로그 필터***(***마지막 ***60***초 ***receive_time)***는 시간이 지남에 따라 표시되는 로그 항목*(*및 로그 페이지*)* 수를 증가시키거나 축소합니다. • 필터 적용- 필터 적용( )을 클릭하여 현재 필터와 일치하는 로그 항목을 표시합니다. • 필터 삭제- 필터 지우기( )를 클릭하여 필터 필드를 지웁니다. • 필터 저장 - 필터 저장( )을 클릭하고 필터 이름을 입력한 다음 확인을 클릭합니다. • 저장된 필터 사용 - 필터 로드( )를 클릭하여 필터 필드에 저장된 필터를 추가합니다.

작업	설명
로그 내보내기	CSV로 내보내기()를 클릭하여 현재 필터와 일치하는 모든 로그를 CSV 형식 보고서로 내보내고 파일 다운로드를 계속합니다. 기본적으로 보고서에는 최대 2,000줄의 로그가 포함되어 있습니다. 생성된 CSV 보고서의 행 제한을 변경하려면, 디바이스 > 설정 > 관리 > 로깅 및 보고 설정 > 로그 내보내기 및 보고를 선택하고, 새 **CSV** 내보내기의 최대 행 수 값을 입력합니다.
정책 작업 강조 표시	작업과 일치하는 로그 항목을 강조 표시하려면 선택합니다. 필터링된 로그는 다음 색상으로 강조 표시됩니다. • 녹색-허용 • 노란색- 계속 또는 재정의 • 빨간색- 거부, 드롭, icmp 드롭, rst-클라이언트, 서버 리셋, 둘 다 리셋, 블록 계속, 재정의 차단, 블록 URL, 전체 드롭, 싱크홀

로그 표시 변경	로그 디스플레이를 사용자 지정하려면 다음을 수행합니다.
	• 자동 새로 고침 인터벌 변경- 인터벌 드롭다운에서 인터벌을 선택합니다(**60**초, **30**초, **10**초 또는 수동).
	• 페이지당 표시되는 항목의 수와 순서를 변경-로그 항목은 10페이지의 블록에서 검색됩니다.
	  • 페이지 하단의 페이징 컨트롤을 사용하여 로그 목록을 탐색합니다.
	  • 페이지당 로그 항목 수를 변경하려면 페이지당 드롭다운에서 행 수를 선택합니다(**20**, **30**, **40**, **50**, **75** 또는 **100**).
	  • 결과를 오름차순 또는 내림차순으로 정렬하려면 **ASC** 또는 **DESC** 드롭다운을 사용하십시오.
	• IP 주소를 도메인 이름으로 해결합니다—호스트네임 확인을 선택하여 외부 IP 주소를 도메인 이름으로 확인하기 시작합니다.
	• 로그가 표시되는 순서 변경-**DESC**를 선택하여 가장 최근 수신 시간으로 로그 항목부터 시작하여 내림차순으로 로그를 표시합니다. **ASC**를 선택하여 가장 오래된 수신 시간으로 로그 항목부터 오름차순으로 로그를 표시합니다.

개별 로그 항목에 대한 세부 정보 보기	개별 로그 항목에 대한 정보를 보려면 다음을 수행합니다. • 추가 세부 정보를 표시하려면 항목의 세부 정보()를 클릭합니다. 소스 또는 대상에 주소 페이지에 정의된 도메인 또는 사용자명 매핑에

작업	설명
	대한 IP 주소가 있는 경우 IP 주소 대신 이름이 표시됩니다. 연결된 IP 주소를 보려면 커서를 이름 위로 이동합니다. • 활성 AutoFocus 라이선스가 있는 방화벽에서 로그 항목에 포함된 IP 주소, 파일 이름, URL, 사용자 에이전트, 위협 이름 또는 해시 옆에 마우스를 가져가서 삭제()를 클릭하여 아티팩트에 대한 AutoFocus 인텔리전스 요약을 엽니다.

모니터 > 외부 로그

이 페이지를 사용하여 Traps™ Endpoint Security Manager(ESM)에서 Panorama™에서 관리하는 로그 수집기로 수집된 로그를 봅니다. Panorama에서 Traps ESM 로그를 보려면 다음을 수행하십시오.

- Traps ESM 서버에서 Panorama를 Syslog 서버로 구성하고 Panorama로 포워딩할 로깅 이벤트를 선택합니다. 이벤트에는 보안 이벤트, 정책 변경, 에이전트 및 ESM 서버 상태 변경, 구성 설정 변경이 포함될 수 있습니다.
- 하나 이상의 관리형 로그 수집기가 있는 Panorama 모드로 배포된 Panorama에서 로그 수집 프로파일(Panorama > 로그 수집 프로파일)을 설정하고 Traps ESM 로그를 저장할 수집기 그룹(Panorama > 수집기 그룹)에 프로파일을 연결합니다.

외부 로그는 디바이스 그룹과 연결되지 않으며 디바이스 그룹을 선택한 경우에만 볼 수 있습니다. 로그가 방화벽에서 포워딩되지 않기 때문에 **All**입니다.

로그 유형	설명
모니터 > 외부 로그 > 트랩 **ESM** > 위협	이러한 위협 이벤트에는 Traps 에이전트가 보고하는 모든 예방, 알림, 임시 및 탐지 후 이벤트가 포함됩니다.
모니터 > 외부 로그 > 트랩 **ESM** > 체계	ESM 서버 시스템 이벤트에는 ESM 상태, 라이선스, ESM 기술 지원 파일 및 WildFire와의 통신과 관련된 변경 사항이 포함됩니다.
모니터 > 외부 로그 > 트랩 **ESM** > 정책	정책 변경 이벤트에는 규칙, 보호 수준, 콘텐츠 업데이트, 해시 제어 로그 및 판정에 대한 변경이 포함됩니다.
모니터 > 외부 로그 > 트랩 **ESM** > 에이전트	에이전트 변경 이벤트는 엔드포인트에서 발생하며 콘텐츠 업데이트, 라이선스, 소프트웨어, 연결 상태, 일회성 작업 규칙, 프로세스 및 서비스, 격리된 파일에 대한 변경을 포함합니다.
모니터 > 외부 로그 > 트랩 **ESM** > 컨피그	ESM 구성 변경 이벤트에는 라이선스, 관리 사용자 및 역할, 프로세스, 제한 설정 및 조건에 대한 시스템 전체 변경이 포함됩니다.

Panorama는 엔드포인트의 개별 보안 이벤트를 네트워크의 이벤트와 연관시켜 엔드포인트와 방화벽 간의 의심스럽거나 악의적인 활동을 추적할 수 있습니다. Panorama가 식별하는 상관 이벤트를 보려면 모니터 > 자동 연동 엔진 > 상관 이벤트을(를) 참조하십시오.

모니터 > 자동 연동 엔진

자동화된 상관 관계 엔진은 네트워크의 패턴을 추적하고 의심스러운 행동의 확대를 나타내는 이벤트 또는 악의적인 활동에 해당하는 이벤트의 상관 관계를 지정합니다. 이 엔진은 방화벽의 여러 로그 집합에서 격리된 이벤트를 검토하고 특정 패턴에 대한 데이터를 쿼리하고 점을 연결하여 실행 가능한 정보를 얻는 개인 보안 분석가의 역할을 합니다.

연동 엔진은 상관 이벤트를 생성하는 상관 개체를 사용합니다. 상관 이벤트는 관련없는 것처럼 보이는 네트워크 이벤트 전반에 걸쳐 공통점을 추적하고 사고 대응에 중점을 두는 데 도움이 되는 증거를 수집합니다.

다음 모델은 자동화된 상관 관계 엔진을 지원합니다.

- Panorama - M-시리즈 어플라이언스 및 가상 어플라이언스
- PA-3200 시리즈 방화벽
- PA-3400 시리즈 방화벽
- PA-5200 시리즈 방화벽
- PA-5400 시리즈 방화벽
- PA-7000 시리즈 방화벽

무엇을 알고 싶습니까?	참조:
상관 개체는 무엇입니까?	모니터 > 자동 연동 엔진 > 상관 개체
상관 이벤트란 무엇입니까? 상관 관계 일치에 대한 일치 증거는 어디에서 볼 수 있습니까?	모니터 > 자동 연동 엔진 > 상관 이벤트
상관 관계 일치의 그래픽 보기를 보려면 어떻게 해야 합니까?	ACC의 손상된 호스트 위젯을 참조하십시오.
더 찾고 계십니까?	자동화된 연동 엔진 사용

모니터 > 자동 연동 엔진 > 상관 개체

익스플로잇 및 멀웨어 배포 방법의 발전에 대응하기 위해 상관 관계 개체는 방화벽에서 서명 기반 멀웨어 탐지 기능을 확장합니다. 다양한 로그 세트에서 의심스러운 행동 패턴을 식별하기 위한 인텔리전스를 제공하고 이벤트를 검토하고 신속하게 대응하는 데 필요한 증거를 수집합니다.

상관 개체는 일치를 위한 패턴, 조회를 수행하는 데 사용할 데이터 소스 및 이러한 패턴을 찾는 기간을 지정하는 정의 파일입니다. 패턴은 데이터 소스를 쿼리하는 조건의 불린(boolean) 구조이며 각 패턴에는 정의된

시간 제한 내에서 패턴 일치가 발생한 횟수인 심각도와 임계값이 할당됩니다. 패턴 일치가 발생하면 상관 이벤트가 기록됩니다.

조회를 수행하는 데 사용되는 데이터 소스에는 애플리케이션 통계, 트래픽, 트래픽 요약, 위협 요약, 위협, 데이터 필터링 및 URL 필터링과 같은 로그가 포함될 수 있습니다. 예를 들어 상관 관계 개체에 대한 정의에는 감염된 호스트의 증거, 멀웨어 패턴의 증거 또는 트래픽, URL 필터링 및 위협 로그에서 멀웨어의 측면 이동에 대해 로그를 쿼리하는 패턴 집합이 포함될 수 있습니다.

상관 개체는 Palo Alto Networks®에 의해 정의되며 콘텐츠 업데이트와 함께 패키지됩니다. 콘텐츠 업데이트를 받으려면 유효한 위협 방지 라이선스가 있어야 합니다.

기본적으로 모든 상관 개체가 활성화됩니다. 개체를 비활성화하려면 개체를 선택한 다음 비활성화합니다.

상관 개체 필드	설명
이름 및 직위	레이블은 상관 관계 개체가 감지하는 활동 유형을 나타냅니다.
ID	고유 번호는 상관 개체를 식별합니다. 이 번호는 6000 시리즈에 있습니다.
카테고리	네트워크, 사용자 또는 호스트에 대한 위협이나 피해의 종류에 대한 요약입니다.
상태	상태는 상관 개체가 활성화(활성) 또는 비활성화(비활성)되었는지의 여부를 나타냅니다.
설명	설명은 방화벽 또는 Panorama가 로그를 분석할 일치 조건을 지정합니다. 악의적인 활동 또는 의심스러운 호스트 동작을 식별하는 데 사용되는 에스컬레이션 패턴 또는 진행 경로를 설명합니다.

모니터 > 자동 연동 엔진 > 상관 이벤트

상관 관계가 있는 이벤트는 방화벽과 Panorama에서 위협 탐지 기능을 확장합니다. 상관 관계가 있는 이벤트는 네트워크의 사용자 또는 호스트의 의심스럽거나 비정상적인 동작에 대한 증거를 수집합니다.

상관 관계 개체를 사용하면 여러 로그 소스에서 특정 조건이나 동작을 피벗하고 공통성을 추적할 수 있습니다. 상관 관계 개체에 지정된 조건 집합이 네트워크에서 관찰되면 각 일치 항목이 상관 관계 이벤트로 기록됩니다.

상관 관계가 있는 이벤트에는 다음 표에 나열된 세부 정보가 포함됩니다.

필드	설명
매치 타임	상관 관계 개체가 일치를 트리거한 시간입니다.
업데이트 시간	경기가 마지막으로 업데이트되었을 타임스탬프입니다.

필드	설명
개체 이름	일치를 트리거한 상관 관계 개체의 이름입니다.
소스 주소	트래픽이 발생한 사용자의 IP 주소
소스 사용자	User-ID를 사용할 수 있는 경우 디렉터리 서버의 사용자 및 사용자 그룹 정보™.
심각도	발생한 피해 정도에 따라 위험을 분류하는 등급입니다.
요약	상관 관계가 있는 이벤트에 수집된 증거를 요약한 설명입니다.
호스트 ID	디바이스의 호스트 ID입니다. 분리 목록(디바이스 > 디바이스 검역)에 디바이스를 추가하려면 디바이스의 호스트 **ID** 옆에 있는 아래쪽 화살표를 클릭하고 표시되는 팝업 창에서 차단 디바이스를 선택합니다.

자세한 로그 보기를 보려면 항목의 세부 정보()를 클릭합니다. 자세한 로그 보기에는 일치에 대한 모든 증거가 포함됩니다.

탭	설명
일치 정보	개체 세부 정보—일치를 트리거한 상관 관계 개체에 대한 정보를 제공합니다. 상관 관계 개체에 대한 자세한 내용은 모니터> 자동화된 상관 관계 엔진 > 상관 관계 개체를 참조하십시오.
	일치 세부 정보—경기 시간, 경기 증거의 마지막 업데이트 시간, 이벤트의 심각도 및 이벤트 요약을 포함하는 경기 세부 정보 요약입니다.
일치 증거	이 탭에는 상관 관계가 있는 이벤트를 확증하는 모든 증거가 포함되어 있습니다. 각 세션에 대해 수집된 증거에 대한 자세한 정보를 나열합니다.

상관 관계 이벤트 탭에서 정보의 그래픽 디스플레이를 참조하고 **ACC** > 위협 활동 탭에서 손상된 호스트 위젯을 참조하십시오. 손상된 호스트 위젯에서 디스플레이는 소스 사용자 및 IP 주소별로 통합되고 심각도에 따라 정렬됩니다.

상관 관계가 있는 이벤트가 기록될 때 알림을 구성하려면 디바이스 > 로그 설정 또는 **Panorama** > 로그 설정 탭으로 이동합니다.

모니터 > 패킷 캡처

모든 Palo Alto Networks 방화벽에는 방화벽의 네트워크 인터페이스를 통과하는 패킷을 캡처하는 데 사용할 수 있는 내장형 패킷 캡처(pcap) 기능이 있습니다. 그런 다음 캡처한 데이터를 문제 해결 목적으로 사용하거나 사용자 지정 애플리케이션 서명을 만들 수 있습니다.

패킷 캡처 기능은 *CPU*를 많이 사용하며 방화벽 성능을 저하시킬 수 있습니다. 필요한 경우에만 이 기능을 사용하고 필요한 패킷을 수집한 후에는 해제해야 합니다.

무엇을 알고 싶습니까?	참조:
방화벽이 패킷을 캡처하는 데 사용할 수 있는 다양한 방법은 무엇입니까?	패킷 캡처 개요
사용자 지정 패킷 캡처를 생성하려면 어떻게 합니까?	맞춤형 패킷 캡처를 위한 빌딩 블록
방화벽이 위협을 탐지할 때 패킷 캡처를 생성하려면 어떻게 합니까?	위협 패킷 캡처 활성화
패킷 캡처는 어디에서 다운로드합니까?	패킷 캡처 개요
더 찾고 계십니까?	
• 보안 프로파일에 대한 확장 패킷 캡처를 켭니다.	기기 > 설정 > 콘텐츠 ID
• 패킷 캡처를 사용하여 사용자 지정 애플리케이션 서명을 작성합니다.	사용자 지정 애플리케이션 및 위협 시그니처를 참조하십시오.
• 방화벽 관리자가 패킷 캡처를 볼 수 없도록 합니다.	웹 인터페이스 관리자 액세스를 정의합니다.
• 예를 참조하십시오.	패킷 캡처 가져오기를 참조하세요.

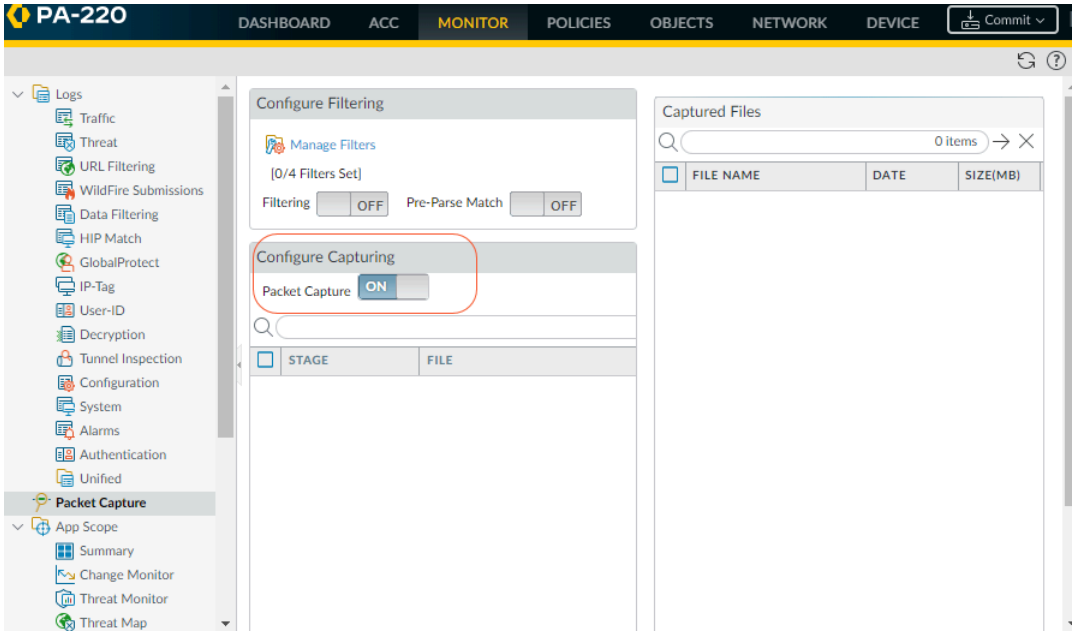
패킷 캡처 개요

사용자 지정 패킷 캡처 또는 위협 패킷 캡처를 수행하도록 Palo Alto Networks 방화벽을 구성할 수 있습니다.

- 사용자 지정 패킷 캡처 - 정의한 필터를 기반으로 모든 트래픽 또는 트래픽에 대한 패킷을 캡처합니다. 예를 들어 특정 소스 및 대상 IP 주소 또는 포트에서 들어오고 나가는 패킷만 캡처하도록 방화벽을 구성할 수 있습니다. 이러한 패킷 캡처를 사용하여 네트워크 트래픽 관련 문제를 해결하거나 애플리케이션 속성을 수집하여 사용자 지정 애플리케이션 서명을 작성합니다(**Monitor** > **Packet Capture**). 단계(삭제, 방화벽, 수신 또는 전송)에 따라 파일 이름을 정의하고 PCAP가 완료된 후 캡처된 파일 섹션에서 PCAP를 다운로드합니다.
- 위협 패킷 캡처 - 방화벽이 바이러스, 스파이웨어 또는 취약성을 감지할 때 패킷을 캡처합니다. 안티바이러스, 안티스파이웨어 및 취약성 보호 보안 프로파일에서 이 기능을 활성화합니다. 이러한 패킷 캡처는 공격의 성공 여부를 확인하거나 공격자가 사용하는 방법에 대해 자세히 알아보는 데 도움이 되는 위협에 대한 컨텍스트를 제공합니다. 위협에 대한 작업은 허용 또는 경고로 설정되어야 합니다. 그렇지 않으면 위협이 차단되고 패킷을 캡처할 수 없습니다. **Objects** > **Security** 프로파일에서 이러한 유형의 패킷 캡처를 구성합니다. (⭳) pcaps를 다운로드하려면 모니터 > 위협을 선택합니다.

맞춤형 패킷 캡처를 위한 빌딩 블록

다음 표에서는 패킷 캡처를 구성하고, 패킷 캡처를 활성화하고, 패킷 캡처 파일을 다운로드하는 데 사용하는 **Monitor** > **Packet Capture** 페이지의 구성 요소에 대해 설명합니다.



맞춤형 패킷 캡처 빌딩 블록	구성 위치	설명
필터 관리	필터링 구성	사용자 지정 패킷 캡처를 활성화할 때 필터와 일치하는 패킷만 캡처되도록 필터를 정의해야 합니다. 이렇게 하면 pcaps에서 필요한 정보를 더 쉽게 찾을 수 있고 방화벽이 패킷 캡처를 수행하는 데 필요한 처리 능력을 줄일 수 있습니다. 추가를 클릭하여 새 필터를 추가하고 다음 필드를 구성합니다. • **Id** - 필터의 식별자를 입력하거나 선택합니다. • 수신 인터페이스 - 트래픽을 캡처할 수신 인터페이스를 선택합니다. • 소스 - 캡처할 트래픽의 소스 IP 주소를 지정합니다. • 대상 - 캡처할 트래픽의 대상 IP 주소를 지정합니다. • **Src** 포트 - 캡처할 트래픽의 소스 포트를 지정합니다. • 대상 포트 - 캡처할 트래픽의 대상 포트를 지정합니다. • **Proto** - 필터링할 프로토콜 번호를 지정합니다(1-255). 예를 들어 ICMP는 프로토콜 번호 1입니다. • 비 **IP** - 비 IP 트래픽을 처리하는 방법을 선택합니다(모든 IP 트래픽 제외, 모든 IP 트래픽 포함, IP 트래픽만 포함 또는 IP 필터 포함 안 함). 브로드캐스트 및 AppleTalk는 비 IP 트래픽의 예입니다. • **IPv6** - 필터에 IPv6 패킷을 포함하려면 이 옵션을 선택합니다.
필터링	필터링 구성	필터를 정의한 후 **Filtering**을 **ON**으로 설정합니다. 필터링이 꺼져 있으면 모든 트래픽이 캡처됩니다.
사전 분석 일치	필터링 구성	이 옵션은 Advanced 문제 해결을 위한 것입니다. 패킷이 수신 포트에 들어간 후 미리 구성된 필터와 일치하는지 구문 분석하기 전에 여러 처리 단계를 거칩니다. 패킷이 실패로 인해 필터링 단계에 도달하지 못할 수 있습니다. 예를 들어, 경로 조회가 실패한 경우에 발생할 수 있습니다.

맞춤형 패킷 캡처 빌딩 블록	구성 위치	설명
		Pre-Parse Match 설정을 **ON**으로 설정하여 시스템에 들어오는 모든 패킷에 대해 긍정적인 일치를 에뮬레이트합니다. 이를 통해 방화벽은 필터링 프로세스에 도달하지 않는 패킷을 캡처할 수 있습니다. 패킷이 필터링 단계에 도달할 수 있으면 필터 구성에 따라 처리되고 필터링 기준을 충족하지 못하면 폐기됩니다.

패킷 캡처	캡처 구성	토글 스위치를 클릭하여 패킷 캡처를 켜거나 끕니다.
		하나 이상의 캡처 단계를 선택해야 합니다. 추가를 클릭하고 다음을 지정합니다.
		• 단계 - 패킷을 캡처할 지점을 나타냅니다.
		  • 드롭 - 패킷 처리에 오류가 발생하여 패킷이 삭제된 경우.
		  • 방화벽 - 패킷에 세션 일치가 있거나 세션이 있는 첫 번째 패킷이 성공적으로 생성된 경우.
		  • 수신 - 데이터플레인 프로세서에서 패킷을 수신한 경우.
		  • 전송 - 패킷이 데이터플레인 프로세서에서 전송되는 경우.
		• 파일 - 캡처 파일 이름을 지정합니다. 파일 이름은 문자로 시작해야 하며 문자, 숫자, 마침표, 밑줄 또는 하이픈을 포함할 수 있습니다.
		• 패킷 수 - 캡처가 중지되는 최대 패킷 수를 지정합니다.
		• 바이트 수 - 캡처가 중지되는 최대 바이트 수를 지정합니다.

캡처된 파일	캡처된 파일	방화벽에서 이전에 생성한 사용자 지정 패킷 캡처 목록을 포함합니다. 파일을 클릭하여 컴퓨터에 다운로드합니다. 패킷 캡처를 삭제하려면 패킷 캡처를 선택한 다음 삭제를 선택합니다. • 파일 이름 - 패킷 캡처 파일을 나열합니다. 파일 이름은 캡처 단계에 대해 지정한 파일 이름을 기반으로 합니다. • 날짜 - 파일이 생성된 날짜입니다. • 크기**(MB)** - 캡처 파일의 크기입니다.

맞춤형 패킷 캡처 빌딩 블록	구성 위치	설명
		패킷 캡처를 켠 다음 이 목록에 새 PCAP 파일이 표시되기 전에 새로 고침( )을 클릭해야 합니다.
모든 설정 지우기	설정	모든 설정 지우기를 클릭하여 패킷 캡처를 끄고 모든 패킷 캡처 설정을 지웁니다. 이것은 보안 프로파일에 설정된 패킷 캡처를 끄지 않습니다. 보안 프로파일에서 패킷 캡처를 활성화하는 방법에 대한 자세한 내용은 위협 패킷 캡처 활성화를 참조하십시오.

위협 패킷 캡처 활성화

- 개체 > 보안 프로파일

방화벽이 위협을 감지할 때 패킷을 캡처하도록 하려면 보안 프로파일에서 패킷 캡처 옵션을 활성화하십시오.

먼저 개체 > 보안 프로파일을 선택한 다음 다음 표에 설명된 대로 원하는 프로파일을 수정합니다.

보안 프로파일의 패킷 캡처 옵션	위치
바이러스 백신	사용자 지정 바이러스 백신 프로파일을 선택한 다음 바이러스 백신 탭에서 패킷 캡처를 선택합니다.
Anti-Spyware	사용자 지정 안티 스파이웨어 프로파일을 선택한 다음 **DNS** 서명 탭을 클릭한 다음 패킷 캡처 드롭다운에서 단일 패킷 또는 확장 캡처를 선택합니다.
취약점 보호	사용자 지정 Vulnerability Protection 프로파일을 선택한 다음 규칙 탭에서 추가를 클릭하여 새 규칙을 추가하거나 기존 규칙을 선택합니다. 그런 다음 패킷 캡처 드롭다운을 선택한 다음 단일 패킷 또는 확장 캡처를 선택합니다.

안티 스파이웨어 및 취약성 보호 프로파일에서 예외 시 패킷 캡처를 활성화할 수도 있습니다. 예외 탭을 클릭하고 서명에 대한 패킷 캡처 열에서 드롭다운을 클릭하고 단일 패킷 또는 확장 캡처를 선택합니다.

(선택 사항) 캡처된 패킷 수(글로벌 설정 기반)를 기반으로 위협 패킷 캡처 길이를 정의하려면 **Device** > **Setup**을 선택합니다. > **Content-ID** 및 Content-ID™ 설정 섹션에서 확장 패킷 캡처 길이**(**패킷**)** 필드(범위는 1-50, 기본값은 5)를 수정합니다.

보안 프로파일에서 패킷 캡처를 활성화한 후 프로파일이 보안 규칙의 일부인지 확인해야 합니다. 보안 규칙에 보안 프로파일을 추가하는 방법에 대한 자세한 내용은 보안 정책 개요를 참조하십시오.

보안 프로파일에 패킷 캡처가 활성화되어 있을 때 방화벽이 위협을 탐지할 때마다 패킷 캡처를 다운로드( )하거나 내보낼 수 있습니다.

모니터 > 앱 범위

다음 주제에서는 앱 범위 기능에 대해 설명합니다.

- 앱 범위 개요
- 앱 범위 요약 보고서
- 앱 범위 변경 모니터링 보고서
- 앱 범위 위협 모니터 보고서
- 앱 범위 위협 맵 보고서
- 앱 범위 네트워크 모니터 보고서
- 앱 범위 트래픽 맵 보고서

앱 범위 개요

앱 범위 보고서는 네트워크의 다음 측면에 대한 그래픽 가시성을 제공합니다.

- 애플리케이션 사용 및 사용자 활동의 변화
- 네트워크 대역폭의 대부분을 차지하는 사용자 및 애플리케이션
- 네트워크 위협

앱 범위 보고서를 사용하면 동작이 비정상적이거나 예기치 않은지 빠르게 확인할 수 있으며 문제가 있는 동작을 정확히 찾아내는 데 도움이 됩니다. 각 보고서는 네트워크에 대한 동적이고 사용자 정의 가능한 창을 제공합니다. 보고서에는 표시할 데이터 및 범위를 선택하는 옵션이 포함됩니다. Panorama에서는 표시되는 정보에 대한 데이터 소스를 선택할 수도 있습니다. 기본 데이터 소스(새 Panorama 설치 시)는 관리되는 방화벽에서 포워딩한 로그를 저장하는 Panorama의 로컬 데이터베이스를 사용합니다. 업그레이드 시 기본 데이터 소스는 원격 디바이스 데이터(관리되는 방화벽 데이터)입니다. 관리되는 방화벽에서 직접 데이터의 통합 보기를 가져와 표시하려면 이제 소스를 **Panorama**에서 원격 디바이스 데이터로 전환해야 합니다.

차트의 선이나 막대를 마우스로 가리키고 클릭하면 ACC로 전환되고 특정 애플리케이션, 애플리케이션 카테고리, 사용자 또는 소스에 대한 자세한 정보를 제공합니다.

애플리케이션 명령 센터 차트	설명
요약	앱 범위 요약 보고서
모니터 변경	앱 범위 변경 모니터링 보고서
위협 모니터	앱 범위 위협 모니터 보고서

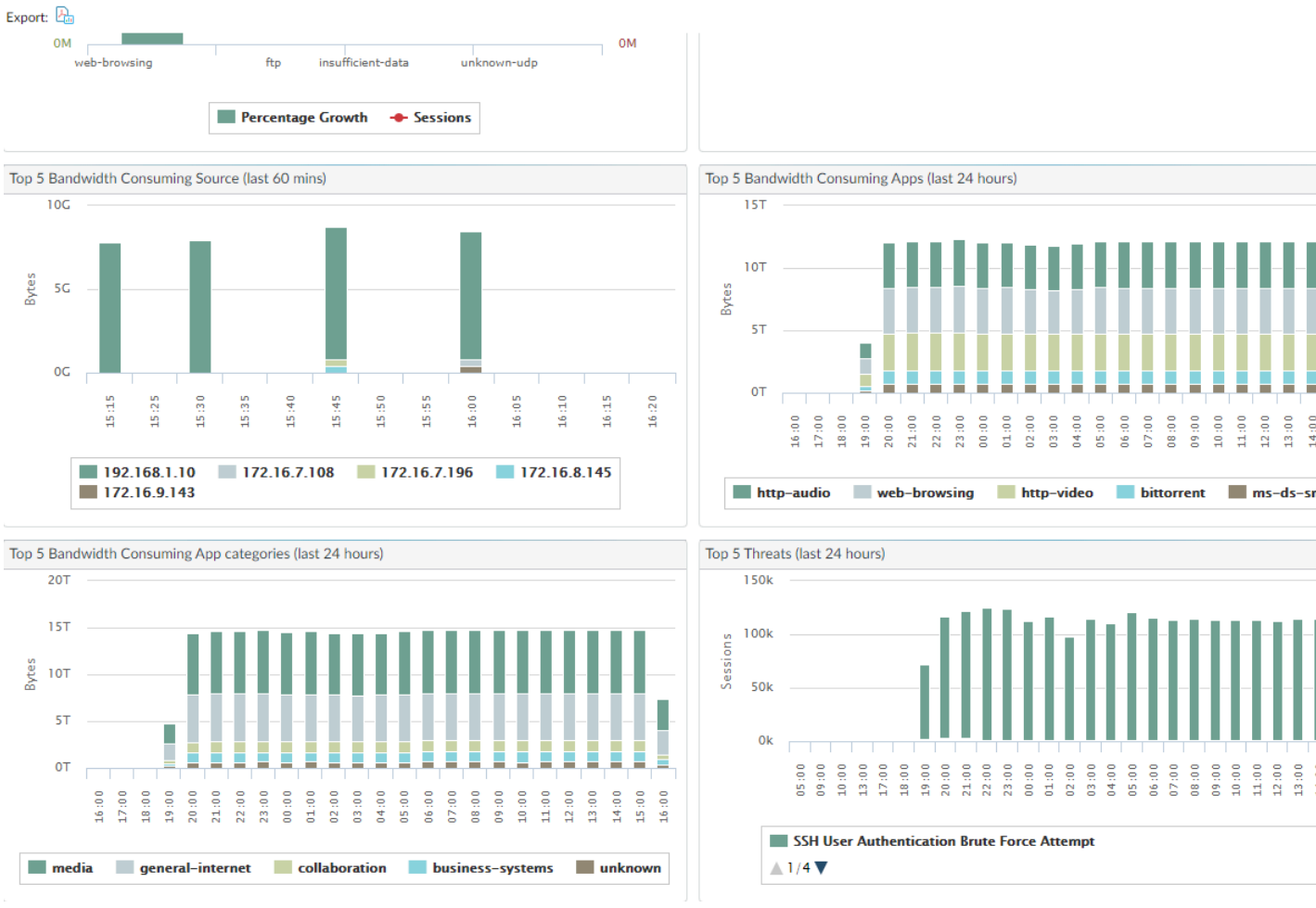
애플리케이션 명령 센터 차트	설명
위협 지도	앱 범위 위협 맵 보고서
네트워크 모니터	앱 범위 네트워크 모니터 보고서
교통 지도	앱 범위 트래픽 맵 보고서

앱 범위 요약 보고서

요약 보고서는 상위 5개 우세자, 열세자 및 대역폭 소비 애플리케이션, 애플리케이션 범주, 사용자 및 소스에 대한 차트를 표시합니다.

요약 보고서의 차트를 PDF로 내보내려면 내보내기( )를 클릭합니다. 각 차트는 PDF 출력의 페이지로 저장됩니다.

앱 범위 요약 보고서



앱 범위 변경 모니터링 보고서

변경 모니터 보고서에 지정된 기간 동안의 변경 내용이 표시됩니다. 예를 들어 아래 그림은 지난 24시간 기간과 비교하여 지난 시간 동안 사용된 상위 애플리케이션을 표시합니다. 상위 애플리케이션은 세션 수에 따라 결정되고 백분율로 정렬됩니다.

앱 범위 변경 모니터링 보고서

이 보고서에는 다음 옵션이 포함되어 있습니다.

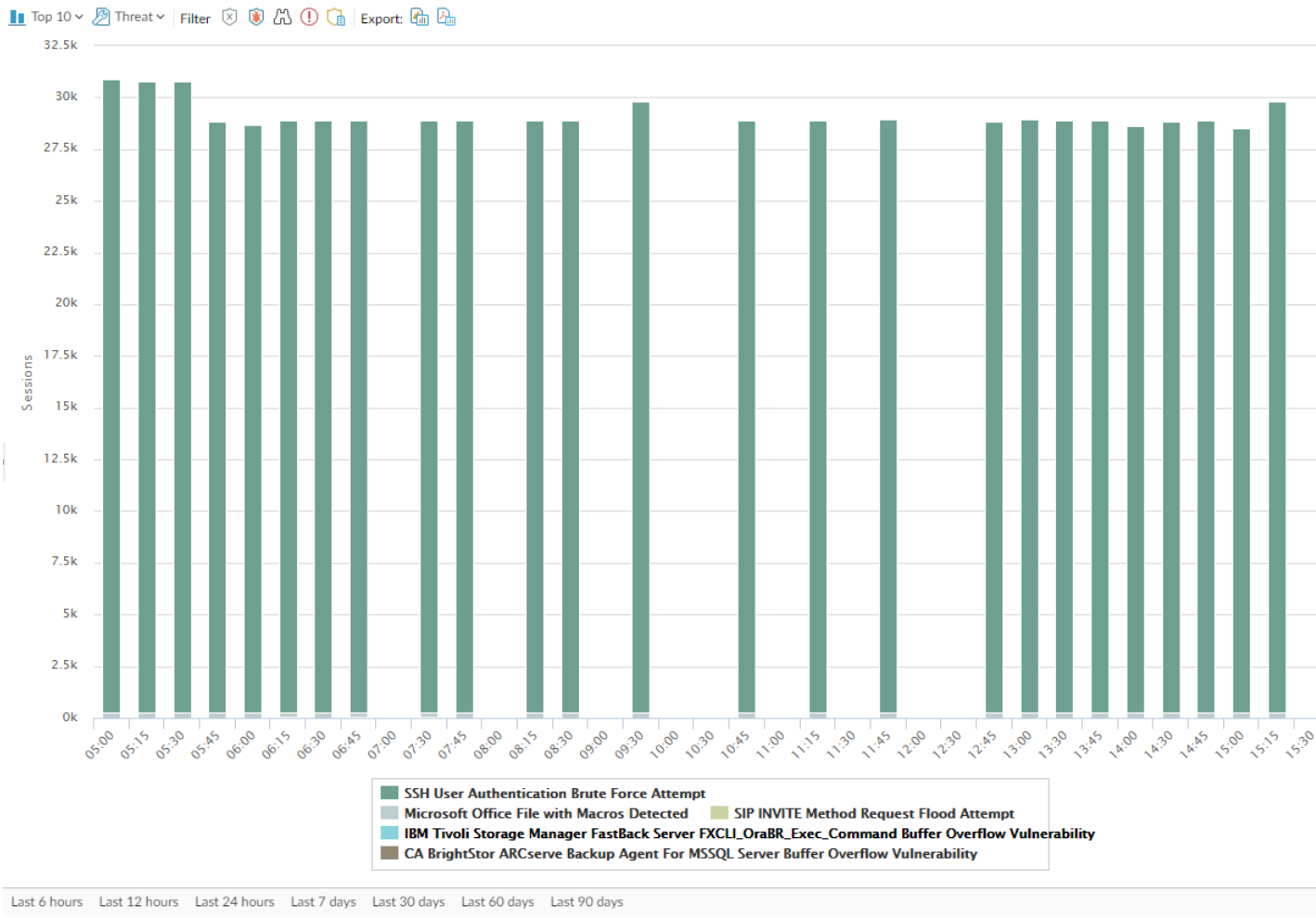
모니터 보고서 옵션 변경	설명
탭 바	
상위 10위	차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다.
애플리케이션	보고된 항목의 유형을 결정합니다. 애플리케이션, 애플리케이션 카테고리, 소스 또는 대상.

모니터 보고서 옵션 변경	설명
우세자	측정된 기간 동안 증가한 품목의 측정을 표시합니다.
열세자	측정된 기간 동안 감소한 품목의 측정값을 표시합니다.
신규	측정 기간 동안 추가된 항목의 측정값을 표시합니다.
드롭	측정 기간 동안 중단된 항목의 측정값을 표시합니다.
필터	선택한 항목만 표시하려면 필터를 적용합니다. 없음은 모든 항목을 표시하지 않습니다.
세션 수 및 바이트 수	세션 또는 바이트 정보를 표시할지의 여부를 결정합니다.
정렬	항목을 백분율 또는 원시 성장별로 정렬할지의 여부를 결정합니다.
내보내기	그래프를 .png 이미지 또는 PDF로 내보합니다.
하단 막대	
비교(인터벌)	변경 측정이 수행되는 기간을 지정합니다.

앱 범위 위협 모니터 보고서

위협 모니터 보고서에는 선택한 기간 동안 상위 위협 수가 표시됩니다. 예를 들어 아래 그림은 지난 6시간 동안의 상위 10개 위협 유형을 보여줍니다.

앱 범위 위협 모니터 보고서



각 위협 유형은 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 이 보고서에는 다음 옵션이 포함되어 있습니다.

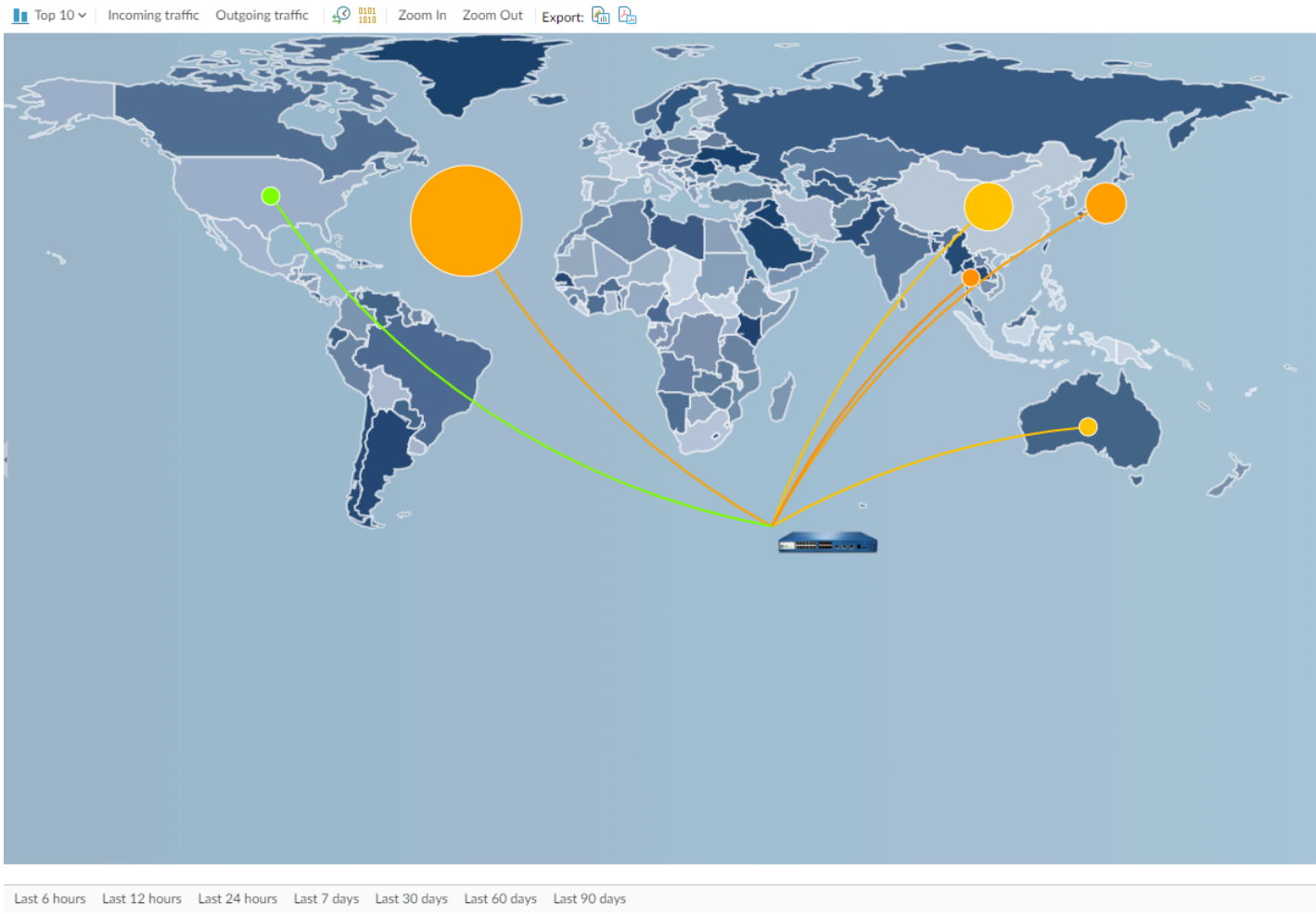
위협 모니터 보고서 옵션	설명
탑 바	
상위 10위	차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다.
위협	측정된 항목의 유형을 결정합니다. 위협, 위협 카테고리, 소스 또는 대상.
필터	선택한 항목만 표시하려면 필터를 적용합니다.
	누적된 열 차트 또는 누적 된 영역 차트에 정보가 표시되는지의 여부를 결정합니다.
내보내기	그래프를 .png 이미지 또는 PDF로 내보합니다.

위협 모니터 보고서 옵션	설명
하단 막대	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	측정이 수행되는 기간을 지정합니다.

앱 범위 위협 맵 보고서

위협 맵 보고서에는 심각도를 포함한 위협에 대한 지리적 보기가 표시됩니다.

앱 범위 위협 맵 보고서



각 위협 유형은 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 맵에서 국가를 클릭하여 확대한 다음 필요에 따라 축소합니다. 이 보고서에는 다음 옵션이 포함되어 있습니다.

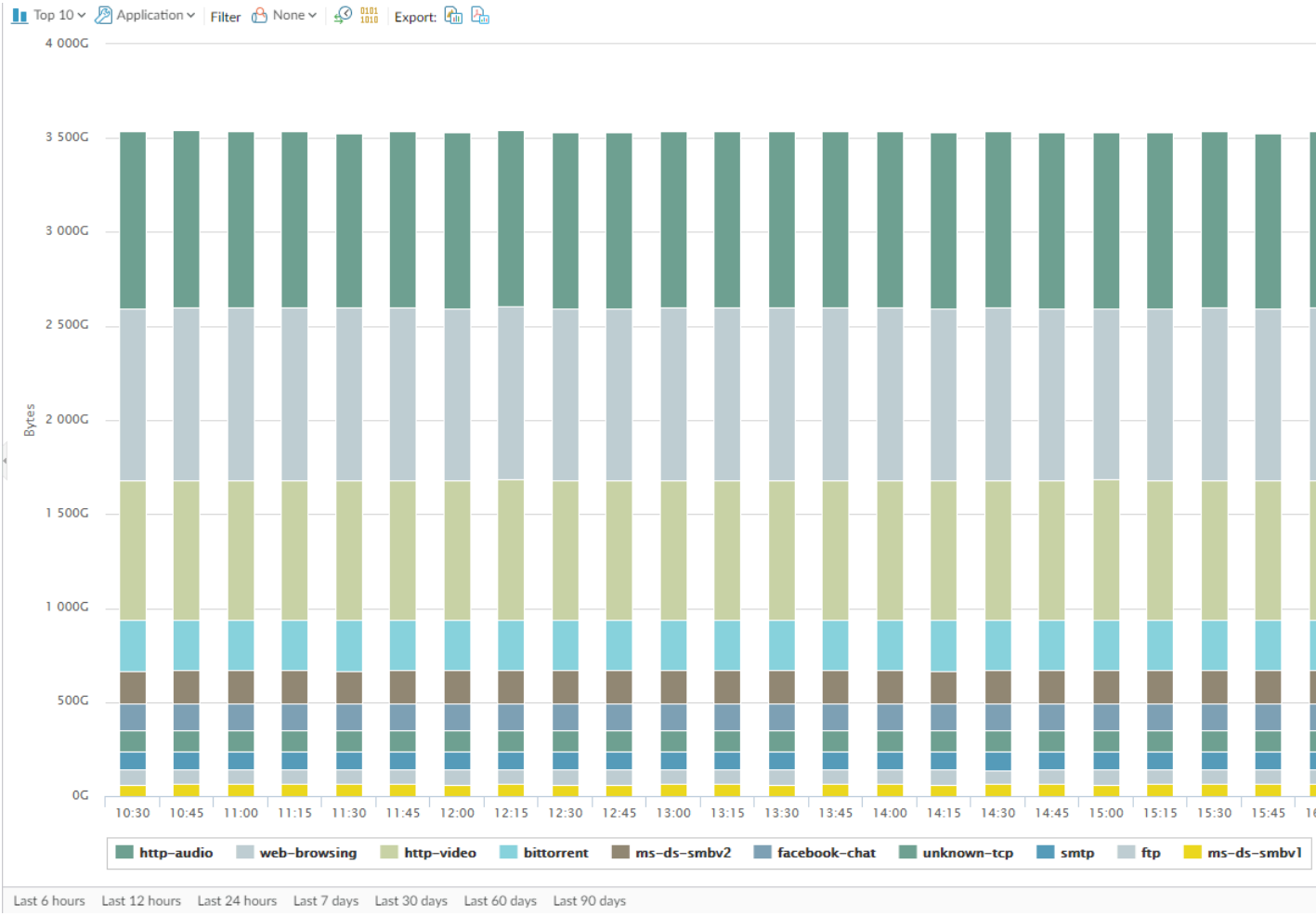
위협 맵 보고서 옵션	설명
탑 바	

위협 맵 보고서 옵션	설명
상위 10위	차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다.
들어오는 위협	들어오는 위협을 표시합니다.
나가는 위협	나가는 위협을 표시합니다.
필터	선택한 항목만 표시하려면 필터를 적용합니다.
확대/축소 및 축소	맵을 확대 및 축소합니다.
내보내기	그래프를 .png 이미지 또는 PDF로 내보합니다.
하단 막대	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last Quarter	측정이 수행되는 기간을 나타냅니다.

앱 범위 네트워크 모니터 보고서

네트워크 모니터 보고서에는 지정된 기간 동안 서로 다른 네트워크 기능에 전념하는 대역폭이 표시됩니다. 각 네트워크 함수는 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 예를 들어 아래 이미지는 세션 정보를 기반으로 지난 7일 동안의 애플리케이션 대역폭을 보여줍니다.

앱 범위 네트워크 모니터 보고서



보고서에는 다음 옵션이 포함되어 있습니다.

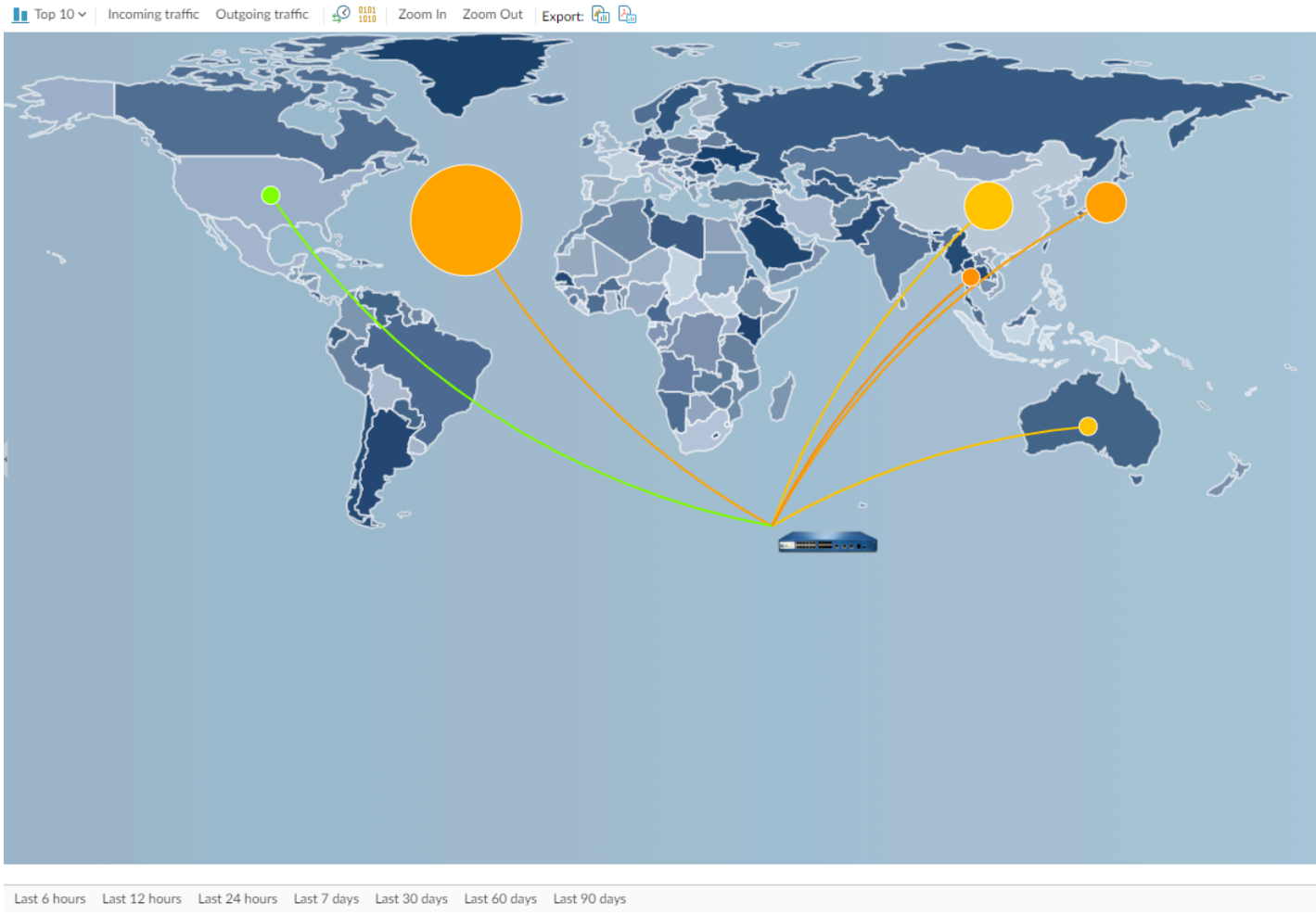
네트워크 모니터 보고서 옵션	설명
탑 바	
상위 10위	차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다.
애플리케이션	보고된 항목의 유형을 결정합니다. 애플리케이션, 애플리케이션 카테고리, 소스 또는 대상.
필터	선택한 항목만 표시하려면 필터를 적용합니다. 없음은 모든 항목을 표시하지 않습니다.
세션 수 및 바이트 수	세션 또는 바이트 정보를 표시할지의 여부를 결정합니다.
	누적된 열 차트 또는 누적 된 영역 차트에 정보가 표시되는지의 여부를 결정합니다.

네트워크 모니터 보고서 옵션	설명
내보내기	그래프를 .png 이미지 또는 PDF로 내보합니다.
하단 막대	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	변경 측정이 수행되는 기간을 나타냅니다.

앱 범위 트래픽 맵 보고서

트래픽 맵 보고서는 세션 또는 흐름에 따른 트래픽 플로우의 지리적 보기를 보여줍니다.

앱 범위 트래픽 맵 보고서



각 트래픽 유형은 차트 아래의 범례에 표시된 대로 색상으로 구분됩니다. 이 보고서에는 다음 옵션이 포함되어 있습니다.

교통 지도 보고서 옵션	설명
탑 바	
상위 10위	차트에 포함된 측정 수가 가장 높은 레코드 수를 결정합니다.
수신 트래픽	수신 트래픽을 표시합니다.
발신 트래픽	발신 트래픽을 표시합니다.
세션 수 및 바이트 수	세션 또는 바이트 정보를 표시할지의 여부를 결정합니다.
확대/축소 및 축소	맵을 확대 및 축소합니다.
내보내기	그래프를 .png 이미지 또는 PDF로 내보냅니다.
하단 막대	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	변경 측정이 수행되는 기간을 나타냅니다.

모니터 > 세션 브라우저

모니터 > 세션 브라우저를 선택하여 방화벽에서 현재 실행 중인 세션을 찾아보고 필터링합니다. 이 페이지의 필터링 옵션에 대한 정보는 로그 작업을 참조하십시오.

모니터 > 차단 IP 목록

다음을 포함하여 여러 가지 방법으로 차단 목록에 IP 주소를 배치하도록 방화벽을 구성할 수 있습니다.

- 보호할 작업으로 DoS 방어 정책 규칙을 구성하고 분류된 DoS 방어 프로파일을 규칙에 적용합니다. 프로파일에는 차단 기간이 포함됩니다.
- **IP** 차단 작업이 포함된 규칙을 사용하는 취약점 보호 프로파일로 보안 정책 규칙을 구성하고 해당 규칙을 영역에 적용합니다.

차단 IP 목록은 PA-3200 시리즈, PA-5200 시리즈 및 PA-7000 시리즈 방화벽에서 지원됩니다.

무엇을 알고 싶습니까?	참조:
차단 IP 목록 필드는 무엇을 나타냅니까?	IP 목록 항목 차단
차단 IP 목록 항목을 필터링, 탐색 또는 삭제하려면 어떻게 합니까?	차단 IP 목록 항목 보기 또는 삭제
더 찾고 계십니까?	바이러스 백신, Palo Alto Networks 및 취약점 보호 설정 신규 세션의 홍수에 대한 DoS 보호 차단된 IP 주소 모니터링

IP 목록 항목 차단

- 모니터 > **BlockIPList**

다음 표는 방화벽이 차단하는 소스 IP 주소에 대한 차단 목록 항목을 설명합니다.

필드	설명
차단 시간	IP 주소가 차단 IP 목록에 올라간 월/일 및 시:분:초.
유형	차단 작업 유형: 하드웨어(hw) 또는 소프트웨어(sw)가 IP 주소를 차단했는지의 여부. 소스 IPv4 주소로부터의 연결을 차단하기 위해 취약점 보호 프로파일을 사용하는 DoS 방어 정책 또는 보안 정책을 구성하면 방화벽은 해당 패킷이 CPU 또는 패킷 버퍼 리소스를 사용하기 전에 하드웨어에서 해당 트래픽을 자동으로 차단합니다. 공격 트래픽이 하드웨어의 차단 용량을 초과하면 방화벽이 소프트웨어를 사용하여 트래픽을 차단합니다.

필드	설명
소스 IP 주소	방화벽이 차단한 패킷의 소스 IP 주소입니다.
인그레스(ingress) 존	패킷이 방화벽에 진입한 인터페이스에 할당된 보안 영역입니다.
남은 시간	IP 주소가 차단 IP 목록에 있을 때까지 남은 시간(초)입니다.
블록 소스	IP 차단 작업을 지정한 분류된 DoS 방어 프로파일의 이름 또는 취약점 보호 개체 이름입니다.
차단된 총 IP 수: x/y(z % 사용)	방화벽이 지원하는 차단된 IP 주소의 수(y) 중 차단된 IP 주소의 수(x)와 사용된 차단된 IP 주소의 해당 비율(z).

차단 IP 목록 항목 보기 또는 삭제

IP 차단 목록 항목을 탐색하고 자세한 정보를 확인하며 원하는 경우 항목을 삭제합니다.

차단 **IP** 목록 항목 보기 또는 삭제	
특정 차단 IP 목록 정보 검색	열에서 값을 선택합니다. 이 값은 필터 필드에 필터를 입력하고 오른쪽 화살표를 클릭하여 해당 값을 가진 항목에 대한 검색을 시작합니다. X를 클릭하여 필터를 제거합니다.
현재 화면 밖에서 차단 IP 목록 보기	페이지 필드에 페이지 번호를 입력하거나 단일 화살표를 클릭하여 항목의 다음 페이지 또는 이전 페이지를 표시합니다. 이중 화살표를 클릭하여 항목의 마지막 페이지 또는 첫 페이지를 봅니다.
차단 IP 목록에서 IP 주소에 대한 자세한 정보 보기	주소에 대한 정보와 함께 네트워크 솔루션 사용자로 연결되는 항목의 소스 IP 주소를 클릭합니다.
차단 IP 목록 항목 삭제	항목을 선택한 다음 [삭제]를 클릭합니다. 웹 인터페이스에서는 하드웨어 항목 삭제만 지원됩니다. 그러나 *CLI*에서는 하드웨어 및 소프트웨어 항목을 모두 삭제할 수 있습니다.
전체 차단 IP 목록 지우기	모든 항목을 영구적으로 삭제하려면 [모두 지우기]를 클릭합니다. 즉, 해당 패킷이 더 이상 차단되지 않습니다.

차단 **IP** 목록 항목 보기 또는 삭제	
	웹 인터페이스에서는 하드웨어 항목의 *IP* 차단 목록만 지울 수 있습니다. 그러나 *CLI*에서는 하드웨어 및 소프트웨어 항목을 모두 지울 수 있습니다.

모니터 > 봇넷

봇넷 보고서를 사용하면 동작 기반 메커니즘을 사용하여 네트워크에서 잠재적인 멀웨어 및 봇넷에 감염된 호스트를 식별할 수 있습니다. 보고서는 봇넷 감염 가능성을 나타내기 위해 각 호스트에 1에서 5까지의 신뢰도 점수를 할당합니다. 여기서 5는 가장 높은 가능성을 나타냅니다. 보고서를 예약하거나 요청 시 실행하기 전에 의심스러운 트래픽 유형을 식별하도록 보고서를 구성해야 합니다. PAN-OS® 관리자 가이드는 봇넷 보고서 출력 해석에 대한 세부 정보를 제공합니다.

- 봇넷 보고서 설정
- 봇넷 구성 설정

봇넷 보고서 설정

- 모니터 > 봇넷 > 보고서 설정

봇넷 보고서를 생성하기 전에 잠재적인 봇넷 활동을 나타내는 트래픽 유형을 지정해야 합니다 (봇넷 보고서 구성 참조). 일일 보고서를 예약하거나 요청 시 실행하려면 보고서 설정을 클릭하고 다음 필드를 작성합니다. 보고서를 내보내려면 보고서를 선택한 다음 **PDF**로 내보내기, **CSV**로 내보내기 또는 **XML**로 내보내기를 선택합니다.

봇넷 보고서 설정	설명
테스트 실행 시간 프레임	보고서의 시간 인터벌(최근 **24**시간 (기본값) 또는 마지막 달력일을 선택합니다.
지금 실행	보고서를 수동으로 즉시 생성하려면 지금 실행을 클릭합니다. 보고서가 봇넷 보고서 대화 상자 내의 새 탭에 표시됩니다.
행 개수	보고서에 표시할 행 수를 지정합니다 (기본값은 100).
예약	보고서를 매일 자동으로 생성하려면 이 옵션을 선택합니다. 기본적으로 이 옵션은 활성화되어 있습니다.
쿼리 빌더	**(**선택 사항**)** 쿼리 작성기에 쿼리를 추가하여 소스/대상 IP 주소, 사용자 또는 영역과 같은 속성별로 보고서 출력을 필터링합니다. 예를 들어 IP 주소 192.0.2.0에서 시작된 트래픽에 잠재적인 봇넷 활동이 포함되어 있지 않은 경우 **`not (192.0.2.0# addr.src)`**를 쿼리로 추가하여 보고서 출력에서 해당 호스트를 제외할 수 있습니다. • 커넥터 - 논리 커넥터(**and** 또는 **or**)를 선택합니다. 무효를 선택하면 보고서에서 쿼리가 지정하는 호스트를 제외합니다. • 속성 —방화벽이 봇넷 활동을 평가하는 호스트와 연결된 영역, 주소 또는 사용자를 선택합니다.

봇넷 보고서 설정	설명
	• 연산자 —속성을 값에 연관시키는 연산자를 선택합니다. • 값 —일치시킬 쿼리 값을 입력합니다.

봇넷 구성 설정

- 모니터 > 봇넷 > 구성

잠재적인 봇넷 활동을 나타내는 트래픽 유형을 지정하려면 봇넷 페이지의 오른쪽에 있는 구성을 클릭하고 다음 필드를 완성하십시오. 보고서를 구성한 후 요청 시 실행하거나 매일 실행하도록 예약할 수 있습니다(모니터 > PDF 보고서 > PDF 요약 관리 참조).

기본 *Botnet* 보고서 구성이 최적입니다. 기본값이 가양성을 식별한다고 생각되면 *Palo Alto Networks*가 값을 재평가할 수 있도록 지원 티켓을 만드십시오.

봇넷 구성 설정	설명
HTTP 트래픽	보고서에 포함될 각 HTTP 트래픽 유형에 대한 개수를 활성화하고 정의합니다. 입력한 개수 값은 보고서에서 더 높은 신뢰도 점수(봇넷 감염 가능성이 높음)로 연결된 호스트를 나열하기 위해 발생해야 하는 각 트래픽 유형의 최소 이벤트 수입니다. 이벤트 수가 개수보다 적으면 보고서에 더 낮은 신뢰도 점수가 표시되거나(특정 트래픽 유형의 경우) 호스트 항목이 표시되지 않습니다. • 멀웨어 **URL** 방문(범위는 2–1000, 기본값은 5) - 멀웨어 및 봇넷 URL 필터링 카테고리를 기반으로 알려진 멀웨어 URL과 통신하는 사용자를 식별합니다. • 동적 **DNS** 사용(범위는 2–1000, 기본값은 5) - 멀웨어, 봇넷 통신 또는 익스플로잇 킷을 나타낼 수 있는 동적 DNS 쿼리 트래픽을 찾습니다. 일반적으로 동적 DNS 도메인을 사용하는 것은 매우 위험합니다. 멀웨어는 종종 동적 DNS를 사용하여 IP 주소 차단 목록을 피합니다. 이러한 트래픽을 차단하려면 URL 필터링을 사용하는 것이 좋습니다. • **IP** 도메인 검색(범위는 2–1000, 기본값은 10) - URL 대신 IP 도메인을 검색하는 사용자를 식별합니다. • 최근에 등록된 도메인 찾아보기(범위는 2–1000, 기본값은 5) - 지난 30일 이내에 등록된 도메인에 대한 트래픽을 찾습니다. 공격자, 멀웨어 및 익스플로잇 킷은 종종 새로 등록된 도메인을 사용합니다. • 알 수 없는 사이트의 실행 파일(범위는 2–1000, 기본값은 5) - 알 수 없는 URL에서 다운로드한 실행 파일을 식별합니다. 실행 파일은 많은 감염

봇넷 구성 설정	설명
	의 일부이며 다른 유형의 의심스러운 트래픽과 결합될 때 호스트 검토의 우선 순위를 지정하는 데 도움이 될 수 있습니다.
알 수 없는 애플리케이션	보고서에 의심스러운 알 수 없는 TCP 또는 알 수 없는 UDP 애플리케이션과 관련된 트래픽이 포함될지의 여부를 결정하는 임계값을 정의합니다. • 시간당 세션 수(범위는 1–3600, 기본값은 10) - 보고서에는 지정된 시간당 애플리케이션 세션 수와 관련된 트래픽이 포함됩니다. • 시간당 대상(범위는 1–3600, 기본값은 10) - 보고서에는 시간당 지정된 수의 애플리케이션 대상과 관련된 트래픽이 포함됩니다. • 최소 바이트(범위는 1–200, 기본값은 50) - 보고서에는 애플리케이션 페이로드가 지정된 크기와 같거나 초과하는 트래픽이 포함됩니다. • 최대 바이트 수(범위는 1–200, 기본값은 100) - 보고서에는 애플리케이션 페이로드가 지정된 크기 이하인 트래픽이 포함됩니다.
IRC	IRC 서버와 관련된 트래픽을 포함하려면 이 옵션을 선택합니다.

모니터 > PDF 보고서

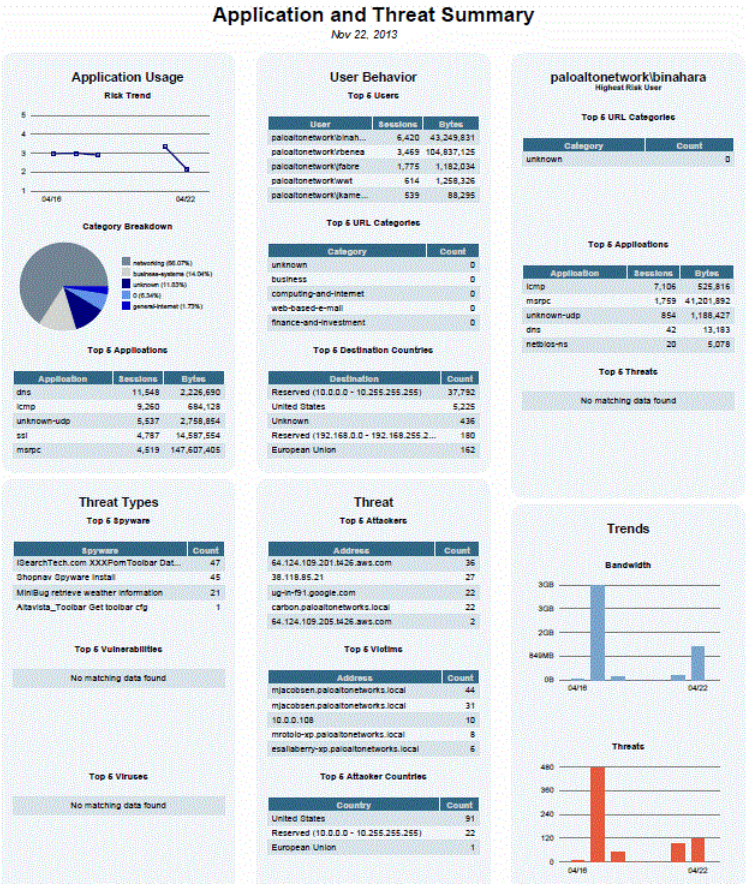
다음 항목은 PDF 보고서를 설명합니다.

- 모니터 > PDF 보고서 > PDF 요약 관리
- 모니터 > PDF 보고서 > 사용자 활동 보고서
- 모니터 > PDF 보고서 > SaaS 애플리케이션 사용
- 모니터 > PDF 보고서 > 보고서 그룹
- 모니터 > PDF 보고서 > 이메일 스케줄러

모니터 > PDF 보고서 > PDF 요약 관리

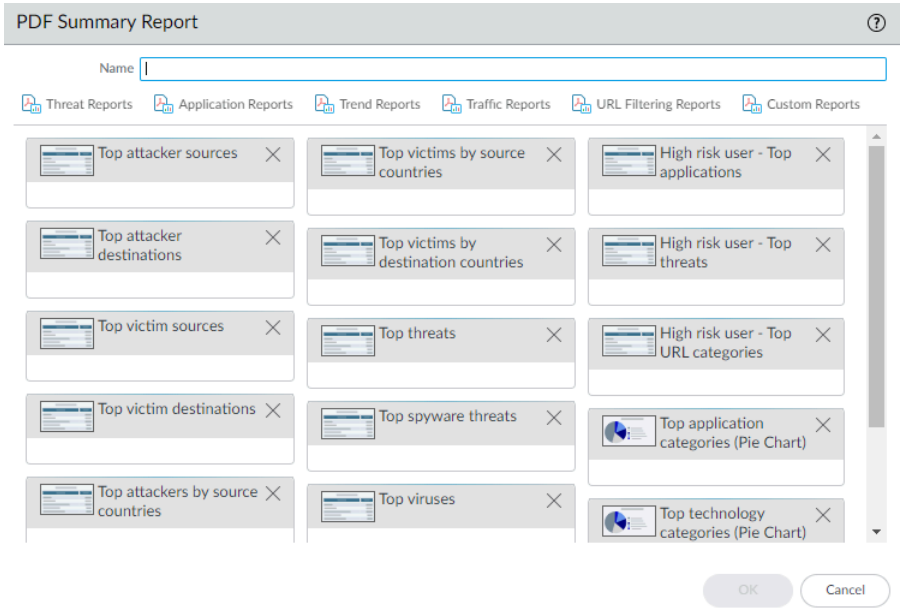
PDF 요약 보고서에는 각 카테고리의 상위 50개(상위 50개 대신)에 대한 데이터를 기반으로 기존 보고서에서 컴파일된 정보가 포함되어 있습니다. 여기에는 다른 보고서에서 사용할 수 없는 추세 차트도 포함됩니다.

PDF 요약 보고서



PDF 요약 보고서를 작성하려면 추가를 클릭하십시오. **PDF** 요약 보고서 페이지가 열리고 사용 가능한 모든 보고서 요소가 표시됩니다.

PDF 보고서 관리



다음 옵션 중 하나 이상을 사용하여 보고서를 디자인합니다.

- 보고서에서 요소를 제거하려면 삭제([X])를 클릭하거나 해당 드롭다운에서 항목을 지웁니다.
- 적절한 드롭다운에서 추가 요소를 선택하여 선택합니다.
- 요소를 끌어서 놓아 보고서의 다른 영역으로 이동합니다.

최대 *18*개의 보고서 요소가 허용됩니다. 이미 *18*개가 있는 경우 새 요소를 추가하기 전에 기존 요소를 삭제해야 합니다.

보고서를 저장하려면 보고서 이름을 입력하고 확인을 클릭합니다.

PDF 보고서를 표시하려면 보고서 > 모니터링을 선택한 다음 **PDF** 요약 보고서를 클릭하여 보고서를 선택한 다음 달력에서 날짜를 클릭하여 해당 날짜의 보고서를 다운로드합니다.

새 *PDF* 요약 보고서는 보고서가 실행될 때까지 나타나지 않습니다. 보고서는 *24*시간마다 오전 *2*시에 자동으로 발생합니다.

모니터 > PDF 보고서 > 사용자 활동 보고서

이 페이지에서는 개별 사용자 또는 사용자 그룹의 작업을 요약하는 보고서를 생성할 수 있습니다. 추가를 클릭하고 다음 정보를 지정합니다.

사용자/그룹 활동 보고서 설정	설명
이름	보고서를 식별하려면 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
유형	사용자 활동 보고서의 경우: 사용자를 선택한 다음 보고서의 제목이 될 사용자의 사용자명 또는 **IP** 주소 (IPv4 또는 IPv6)를 입력합니다.
	그룹 활동 보고서의 경우: 그룹을 선택한 다음 그룹 이름을 입력합니다.
추가 필터	필터 작성기를 선택하여 사용자/그룹 활동 보고서에 대한 필터를 만듭니다.
기간	드롭다운에서 보고서의 기간을 선택합니다.
상세 브라우징 포함	(선택 사항) 보고서에 상세 URL 로그를 포함하려면 이 옵션을 선택합니다. 상세 검색 정보에는 선택한 사용자 또는 사용자 그룹에 대한 대량의 로그(수천 개)가 포함될 수 있으며 이로 인해 보고서 규모가 매우 커질 수 있습니다.

그룹 활동 보고서에는 *URL* 카테고리별 검색 요약이 포함되지 않습니다. 다른 모든 정보는 사용자 작업 보고서 및 그룹 활동 보고서 전체에서 공통적입니다.

요청 시 보고서를 실행하려면 지금 실행을 클릭합니다. 보고서에 표시되는 최대 행 수를 변경하려면 로깅 및 보고 설정을 참조하십시오.

보고서를 저장하려면 확인을 클릭합니다. 그런 다음 보고서를 전자 메일 전달을 예약할 수 있습니다 (모니터 > PDF 보고서 > 전자 메일 스케줄러).

로그 필터 추가

사용자 활동 및 그룹 활동 보고서에 로그 필터를 작성하여 보고서를 사용자 지정합니다. 애플리케이션, 애플리케이션 특성 등을 기준으로 활동 보고서를 필터링할 수 있습니다. 예를 들어 인증이 없는 SaaS 애플리케이션에 관심이 있는 경우 이 애플리케이션 특성을 기반으로 필터를 작성할 수 있습니다.

로그 필터 필드 추가	설명
로그 필터 텍스트 상자	로그에 적용할 필터를 작성합니다. 여러 필터를 작성할 수 있습니다.

로그 필터 필드 추가	설명
커넥터	추가 필터링 옵션을 사용하여 필터를 추가합니다. 작성한 필터에 커넥터를 적용하지 않으려면 무효 상자를 선택합니다.
속성	메뉴에서 추가할 속성을 선택합니다.
운영자	속성이 값과 같아야 하는지 아니면 같지 않은지 선택합니다.
값	속성의 값을 설정합니다. 사용 가능한 경우 가능한 값이 있는 드롭다운 메뉴를 사용할 수 있습니다.

적용을 선택하여 내장된 필터를 사용자 작업 또는 그룹 활동 보고서에 적용합니다.

모니터 > PDF 보고서 > SaaS 애플리케이션 사용

이 페이지를 사용하여 네트워크를 통과하는 SaaS 애플리케이션과 관련된 보안 위험을 요약하는 SaaS 애플리케이션 사용 보고서를 생성합니다. 이 사전 정의된 보고서는 승인된 애플리케이션과 승인되지 않은 애플리케이션을 비교하고, 호스팅 특성이 좋지 않은 위험한 SaaS 애플리케이션을 요약하고, 세부 페이지에 각 카테고리에 대한 상위 애플리케이션을 나열하여 애플리케이션의 활동, 사용 및 규정 준수를 강조합니다. 이 상세 위험 정보를 사용하여 네트워크에서 허용하거나 차단하려는 SaaS 애플리케이션에 대한 정책을 시행할 수 있습니다.

정확하고 유익한 보고서를 생성하려면 네트워크에서 승인된 애플리케이션에 태그를 지정해야 합니다(SaaS 애플리케이션 사용 보고서 생성 참조). 방화벽과 Panorama는 이 사전 정의된 태그가 없는 모든 애플리케이션을 네트워크에서 사용하도록 승인되지 않은 것으로 간주합니다. 승인되지 않은 SaaS 애플리케이션은 정보 보안에 대한 잠재적인 위협이기 때문에 네트워크에 널리 퍼져 있는 승인된 애플리케이션과 승인되지 않은 애플리케이션에 대해 인지하는 것이 중요합니다. 네트워크에서 사용하도록 승인되지 않았으며 위협에 노출되고 개인 및 민감한 데이터가 손실될 수 있습니다.

모든 방화벽 또는 디바이스 그룹에서 일관되게 애플리케이션에 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 반대)) *SaaS* 애플리케이션 사용 보고서는 중복되는 결과를 생성합니다.

ACC에서 애플리케이션 보기를 승인된 상태로 설정하여 가상 시스템 또는 디바이스 그룹에서 승인된 상태가 다른 애플리케이션을 시각적으로 식별합니다. 녹색은 승인된 애플리케이션을 나타내고, 파란색은 승인되지 않은 애플리케이션을 나타내며, 노란색은 다른 가상 시스템 또는 디바이스 그룹에서 승인된 상태가 다른 애플리케이션을 나타냅니다.

보고서를 구성하려면 추가를 클릭하고 다음 정보를 지정합니다.

SaaS 애플리케이션 사용 보고서 설정	설명
이름	보고서를 식별하려면 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
기간	드롭다운에서 보고서의 기간을 선택합니다. 보고서에는 현재 날짜(보고서가 생성된 날짜)의 데이터가 포함됩니다.
다음의 로그 포함	드롭다운에서 선택한 사용자 그룹, 선택한 영역 또는 방화벽이나 Panorama에 구성된 모든 사용자 그룹 및 영역에 대한 보고서를 생성할지의 여부를 선택합니다. • 선택한 사용자 그룹의 경우 - 방화벽 또는 Panorama가 로그를 필터링할 사용자 그룹을 선택합니다. • 선택한 영역의 경우 - 방화벽 또는 Panorama가 로그를 필터링할 영역을 선택합니다. • 모든 사용자 그룹 및 영역의 경우 - 모든 그룹에 대해 보고하거나 가시성을 원하는 최대 25개의 사용자 그룹을 선택할 수 있습니다. 25개 이상의 그룹이 있는 경우 방화벽 또는 Panorama는 보고서에 상위 25개 그룹을 표시하고 나머지 모든 사용자 그룹을 기타 그룹에 할당합니다.
보고서에 사용자 그룹 정보 포함 (선택한 사용자 그룹에 대한 보고서를 생성하도록 선택한 경우에는 사용할 수 없습니다.)	이 옵션은 보고서에 포함할 사용자 그룹에 대한 로그를 필터링합니다. 그룹 관리 또는 선택한 영역 링크에 대한 그룹 관리를 선택하여 표시할 사용자 그룹을 최대 25개까지 선택합니다. 선택한 영역의 특정 사용자 그룹에 대한 보고서를 생성할 때 선택한 그룹의 구성원이 아닌 사용자는 기타라는 사용자 그룹에 할당됩니다.
사용자 그룹	보고서를 생성할 사용자 그룹을 선택합니다. 이 옵션은 다음에서 로그 포함 드롭다운에서 선택한 사용자 그룹을 선택한 경우에만 표시됩니다.
영역	보고서를 생성할 영역을 선택합니다. 이 옵션은 다음에서 로그 포함 드롭다운에서 선택한 영역을 선택한 경우에만 표시됩니다. 그런 다음 보고서에 사용자 그룹 정보 포함을 선택할 수 있습니다.
보고서에 자세한 애플리케이션 카테고리 정보 포함	SaaS 애플리케이션 사용 PDF 보고서는 두 부분으로 구성된 보고서입니다. 기본적으로 보고서의 두 부분이 모두 생성됩니다. 보고서의 첫 번째 부분(10페이지)은 보고 기간 동안 네트워크에서 사용된 SaaS 애플리케이션에 중점을 둡니다.

SaaS 애플리케이션 사용 보고서 설정	설명
	보고서의 첫 번째 부분에 나열된 각 애플리케이션 하위 카테고리에 대한 SaaS 및 비 SaaS 애플리케이션에 대한 자세한 정보를 포함하는 보고서의 두 번째 부분을 원하지 않으면 이 옵션을 선택 취소합니다. 보고서의 두 번째 부분에는 각 하위 카테고리의 상위 애플리케이션 이름과 사용자, 사용자 그룹, 파일, 전송된 바이트 및 이러한 애플리케이션에서 생성된 위협에 대한 정보가 포함됩니다. 자세한 정보가 없으면 보고서 길이는 10페이지입니다.
보고서의 최대 하위 카테고리를 다음으로 제한	SaaS 애플리케이션 사용 보고서의 모든 애플리케이션 하위 카테고리를 사용할지 또는 최대 수를 10, 15, 20 또는 25 하위 카테고리로 제한할지의 여부를 선택합니다. 최대 하위 카테고리 수를 줄이면 보고서에 포함된 SaaS 및 비 SaaS 애플리케이션 활동 정보를 제한하기 때문에 세부 보고서가 더 짧아집니다.

요청 시 보고서를 생성하려면 지금 실행을 클릭합니다.

이 보고서는 요청 시 생성하거나 매일, 매주 또는 매월 실행되도록 예약할 수 있습니다. 보고서를 예약하려면 이메일 전송을 위한 보고서 예약을 참조하세요.

PA-220 및 PA-220R 방화벽에서 SaaS 애플리케이션 사용 보고서는 이메일에 PDF 첨부 파일로 전송되지 않습니다. 대신 이메일에는 웹 브라우저에서 보고서를 여는 데 사용하는 링크가 포함되어 있습니다.

보고서에 대한 자세한 내용은 보고 관리를 참조하십시오.

모니터 > PDF 보고서 > 보고서 그룹

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.

보고서 그룹 설정	설명
이름	보고서 그룹을 식별할 이름을 입력합니다 (최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
제목 페이지	보고서에 제목 페이지를 포함하려면 이 옵션을 선택합니다.
타이틀	보고서 제목으로 표시될 이름을 입력합니다.
보고서 선택/위젯	그룹에 포함할 각 보고서에 대해 왼쪽 열에서 보고서를 선택한 다음 오른쪽 열에 추가합니다. 다음 보고서 유형을 선택할 수 있습니다.

보고서 그룹 설정	설명
	• 사전 정의된 보고서 • 맞춤 리포트 • PDF 요약 보고서 • CSV • 로그 보기 - 맞춤 리포트를 만들 때마다 방화벽이 자동으로 동일한 이름의 Log View 보고서를 만듭니다. Log View 보고서에는 방화벽이 맞춤 리포트의 내용을 작성하는 데 사용한 로그가 표시됩니다. Log View 데이터를 포함하려면 보고서 그룹을 만들 때 맞춤 리포트를 추가한 다음 일치하는 **Log View** 보고서를 추가합니다. 보고서 그룹에 대해 생성된 통합 보고서에는 맞춤 리포트 데이터와 로그 데이터가 표시됩니다. 보고서 그룹을 저장하면 보고서 그룹 페이지의 위젯 열에 그룹에 추가한 보고서가 나열됩니다.

보고서 그룹을 사용하려면 모니터 > PDF 보고서 > 전자 메일 스케줄러를 참조하십시오.

모니터 > PDF 보고서 > 이메일 스케줄러

이메일 스케줄러를 사용하여 이메일로 보고서를 전달하도록 예약합니다. 일정을 추가하기 전에 보고서 그룹과 이메일 프로파일을 정의해야 합니다. 모니터 > PDF 보고서 > 보고서 그룹 및 디바이스 > 서버 프로파일 > 이메일을 참조하세요.

예약된 보고서는 오전 2:00에 실행되기 시작하고 예약된 모든 보고서가 실행 완료된 후에 이메일 포워딩이 발생합니다.

이메일 스케줄러 설정	설명
이름	일정을 식별하려면 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
보고서 그룹	예약할 보고서 그룹(> PDF 보고서> 보고서) 또는 SaaS 애플리케이션 사용 보고서(>PDF 보고서 > SaaS 애플리케이션 사용)를 선택합니다.
이메일 프로파일	전자 메일 설정을 정의하는 프로파일을 선택합니다. 이메일 프로파일 정의에 대한 자세한 내용은 기기 > 서버 프로파일 > 이메일을 참조하세요.
반복	보고서를 생성하고 보낼 빈도를 선택합니다.
이메일 주소 재정의	전자 메일 프로파일에 지정된 받는 사람 대신 사용할 선택적 이메일 주소를 입력합니다.

이메일 스케줄러 설정	설명
테스트 이메일 보내기	선택한 이메일 프로파일에 정의된 이메일 주소로 테스트 이메일을 보내려면 클릭합니다.

모니터 > 사용자 정의 보고서 관리

주문형 또는 일정(매일 밤)에 실행되도록 맞춤 리포트를 만들 수 있습니다. 사전 정의된 보고서의 경우 모니터 > 보고서를 선택합니다.

방화벽이 예약된 맞춤 리포트를 생성한 후 구성을 수정하여 향후 출력을 변경하면 해당 보고서의 과거 결과를 무효화할 위험이 있습니다. 예약된 보고서 구성을 수정해야 하는 경우 모범 사례는 새 보고서를 만드는 것입니다.

맞춤 리포트를 추가하여 새 보고서를 만듭니다. 기존 템플릿에 보고서를 기반으로 하려면 템플릿을 로드하고 템플릿을 선택합니다. 예약된 시간 대신 또는 예약된 시간 이외에 주문형 보고서를 생성하려면 지금 실행을 클릭합니다. 보고서를 정의하기 위해 다음 설정을 지정합니다.

맞춤 리포트 설정	설명
이름	보고서를 식별하려면 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	맞춤 리포트에 대한 설명을 입력합니다.
데이터베이스	보고서의 데이터 소스으로 사용할 데이터베이스를 선택합니다.
예약	매일 밤 보고서를 실행하려면 이 옵션을 선택합니다. 그런 다음 모니터 > 보고서를 선택하여 보고서를 사용할 수 있게 됩니다.
타임 프레임	고정된 타임 프레임을 선택하거나 사용자 지정을 선택한 다음 날짜 및 시간 범위를 지정합니다.
정렬별로	보고서에 포함할 정보의 양을 포함하여 보고서를 구성할 정렬 옵션을 선택합니다. 사용 가능한 옵션은 데이터베이스 선택에 따라 다릅니다.
그룹별	보고서에 포함할 정보의 양을 포함하여 보고서를 구성할 그룹화 옵션을 선택합니다. 사용 가능한 옵션은 데이터베이스 선택에 따라 다릅니다.
열	맞춤 리포트에 포함할 사용 가능한 열을 선택한 다음 ⊕ 선택된 열에 추가합니다. 위쪽, 아래쪽, 위쪽 및 아래쪽을 선택하여 선택한 열을 재정렬합니다. 필요에 따라 이전에 선택한 열을 선택한 다음 제거할 수도 ⊖ 있습니다.

맞춤 리포트 설정	설명
쿼리 빌더	보고서 쿼리를 작성하려면 다음을 지정하고 추가를 클릭합니다. 전체 쿼리를 생성하기 위해 필요에 따라 반복합니다. • 커넥터 —추가하려는 표현식 앞에 올 커넥터(**and** 또는 **or**)를 선택하십시오. • 네게이트—쿼리를 부정으로 해석하려면 이 옵션을 선택합니다. 이전 예제에서 부정 결정 옵션은 지난 24시간이 아니거나 트러스트 영역이 아닌 항목에 대한 일치를 발생시킵니다. • 특성—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.

자세한 내용은 맞춤 리포트 생성을참조하십시오.

모니터 > 보고서

방화벽은 전날 또는 이전 주의 선택한 날짜에 대한 트래픽 통계 관련 다양한 “상위 50개” 보고서를 제공합니다.

보고서를 보려면 페이지 오른쪽에서 보고서 카테고리(예: 맞춤 리포트)를 확장하고 보고서 이름을 선택합니다. 이 페이지에는 섹션으로 보고서가 나열됩니다. 선택한 기간에 대한 각 보고서의 정보를 볼 수 있습니다.

기본적으로 방화벽은 이전 달력 날짜에 대한 모든 보고서를 표시합니다. 다른 날짜에 대한 보고서를 보려면 페이지 오른쪽 하단의 달력에서 보고서 생성 날짜를 선택합니다.

방화벽이 아닌 시스템에 대한 보고서를 보려면 내보내기 옵션을 선택합니다.

- **PDF**로 내보내기
- **CSV**로 내보내기
- **XML**로 내보내기

정책

다음 항목에서는 방화벽 정책 유형, 정책을 이동하거나 복사하는 방법, 정책 설정에 대해 설명합니다.

정책 유형

정책을 사용하면 규칙을 적용하고 작업을 자동화하여 방화벽 작동을 제어할 수 있습니다. 방화벽은 다음 정책 유형을 지원합니다.

- 애플리케이션, 소스 및 대상 영역 및 주소, 및 선택적으로 서비스(포트 및 프로토콜)를 기반으로 네트워크 세션을 차단하거나 허용하는 기본 보안 정책. 영역은 트래픽을 보내거나 받는 물리적 또는 논리적 인터페이스를 식별합니다. 정책 > 보안을 참조하십시오.
- 주소와 포트를 변환하기 위한 NAT(Network Address Translation) 정책. 정책 > NAT를 참조하십시오.
- QoS가 활성화된 인터페이스를 통과할 때 처리를 위해 트래픽이 분류되는 방식을 결정하는 QoS(서비스 품질) 정책. 정책 > QoS를 참조하십시오.
- 라우팅 테이블을 재정의하고 트래픽에 대한 이그레스(egress) 인터페이스를 지정하는 정책 기반 포워딩 정책. 정책 > 정책 기반 포워딩을 참조하십시오.
- 보안 정책에 대한 트래픽 복호화를 지정하는 복호화 정책. 각 정책은 복호화하려는 트래픽의 URL 카테고리를 지정할 수 있습니다. SSH 복호화은 SSH 셸 액세스 외에 SSH 터널링을 식별하고 제어하는 데 사용됩니다. 정책 > 복호화를 참조하십시오.
- 터널링된 트래픽에 보안, DoS 방어 및 QoS 정책을 적용하고 터널 활동을 보기 위한 터널 검사 정책. 정책 > 터널 검사를 참조하십시오.
- 방화벽에서 제공하는 애플리케이션 정의를 재정의하는 재정의 정책. 정책 > 애플리케이션 재정의를 참조하십시오.
- 네트워크 리소스에 액세스하는 최종 사용자에 대한 인증을 정의하는 인증 정책. 정책 > 인증을 참조하십시오.
- DoS(서비스 거부) 정책은 DoS 공격으로부터 보호하고 규칙 일치에 대응하여 보호 조치를 취합니다. 정책 > DoS 방어를 참조하십시오.
- 링크 경로 상태가 승인되고 구성된 상태 메트릭 아래로 저하될 때 소스 및 대상 영역 간의 링크 경로 관리를 결정하는 SD-WAN 정책. 정책 > SD-WAN을 참조하십시오.

방화벽 웹 인터페이스의 Panorama™ 디스플레이에서 푸시된 공유 정책이 주황색으로 표시됩니다. 이러한 공유 정책은 Panorama에서만 편집할 수 있습니다. 방화벽에서 편집할 수 없습니다.

룰베이스(rulebase)에 사용된 모든 태그 그룹을 보려면, 룰베이스(rulebase)를 그룹으로 보기을(를) 합니다. 많은 규칙이 있는 룰베이스(rulebase)에서 룰베이스(rulebase)를 그룹으로 보면 설정된 규칙 레이어를 유지하면서 태그, 색상 코드 및 각 그룹의 규칙 수를 표시하여 표시를 단순화합니다.

정책 규칙 이동 또는 복사

정책을 이동하거나 복사할 때 공유 위치를 포함하여 액세스 권한이 있는 대상(방화벽의 가상 시스템 또는 Panorama의 디바이스 그룹)을 할당할 수 있습니다.

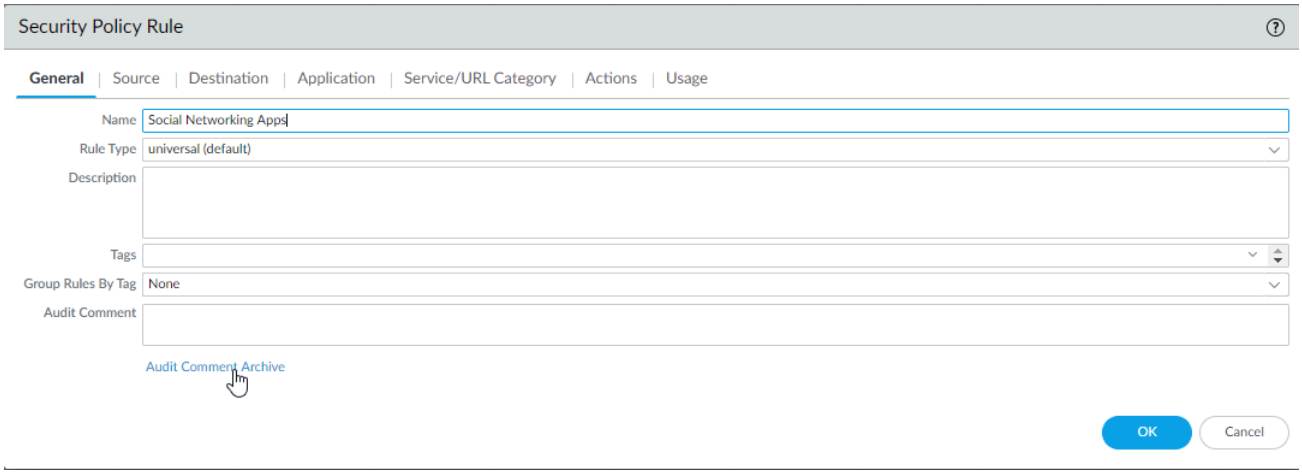
정책 규칙을 이동하려면 정책 탭에서 규칙을 선택하고 이동을 클릭한 다음 다른 **vsys**로 이동을 선택(방화벽만)하거나 다른 룰베이스**(rulebase)** 또는 디바이스 그룹으로 이동(파노라마만)하고 다음 표에서 필드를 지정한 다음 확인을 클릭합니다.

정책 규칙을 복사하려면 정책 탭에서 규칙을 선택한 다음 복사를 클릭하고 다음 표에서 필드를 지정한 후 확인을 클릭합니다.

이동/복사 설정	설명
선택한 규칙	작업에 대해 선택한 정책 규칙의 이름 및 현재 위치(가상 시스템 또는 디바이스 그룹)를 표시합니다.
데스티네이션	정책 또는 개체의 새 위치(가상 시스템, 디바이스 그룹 또는 공유)를 선택합니다. 기본 값은 정책 또는 개체 탭에서 선택한 가상 시스템 또는 디바이스 그룹입니다.
규칙 순서	다른 규칙을 기준으로 규칙 위치를 선택합니다. • 맨 위로 이동 - 해당 규칙이 다른 모든 규칙보다 우선합니다. • 맨 아래로 이동 - 해당 규칙이 다른 모든 규칙을 따릅니다. • 규칙 전 - 인접한 드롭다운에서 후속 규칙을 선택합니다. • 규칙 이후 - 인접한 드롭다운에서 이전 규칙을 선택합니다.
유효성 검사에서 처음 감지된 오류에 대한 오류 발생	이 옵션(기본적으로 선택됨)을 선택하여 방화벽 또는 Panorama가 찾은 첫 번째 오류를 표시하고 추가 오류 확인 작업을 중지합니다. 예를 들어 대상에 이동하는 정책 규칙에 참조되는 개체가 포함되어 있지 않으면 오류가 발생합니다. 이 선택을 취소하면 방화벽이나 Panorama를 표시하기 전에 모든 오류를 찾을 수 있습니다.

코멘트 아카이브 감사

코멘트 감사 아카이브를 선택하여 선택한 규칙의 감사 설명 기록, 구성 로그 및 규칙 변경 기록을 봅니다.



- 감사 코멘트
- 구성 로그(커밋 간)
- 규칙 변경

감사 코멘트

선택한 정책 규칙에 대한 감사 코멘트 기록을 봅니다. 필터를 적용하고 저장하여 특정 감사 주석을 빠르게 식별하고 표시된 감사 코멘트를 CSV 형식으로 내보냅니다.

필드	설명
커밋 시간	감사 코멘트가 커밋된 시간입니다.
감사 의견	감사 코멘트의 내용입니다.
관리자	감사 코멘트를 커밋한 사용자입니다.
구성 버전	구성 개정 버전입니다. 0은 정책 규칙이 처음 생성되어 Panorama에 커밋된 시간을 나타냅니다.

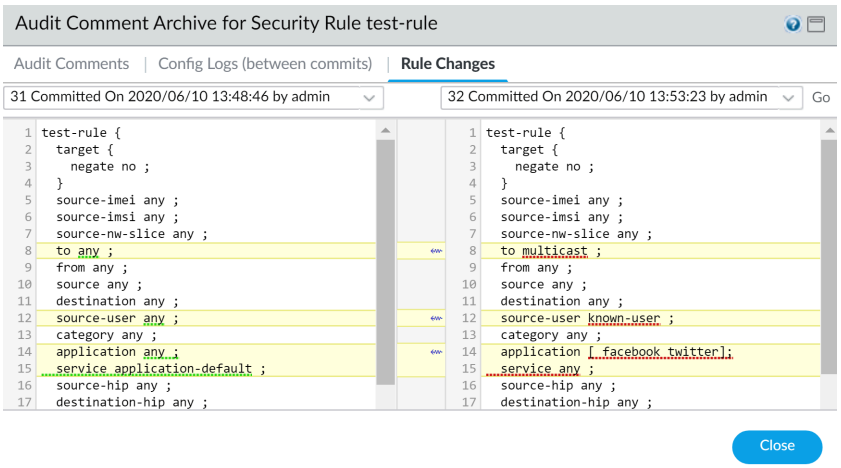
구성 로그(커밋 간)

커밋 간에 선택한 정책 규칙에 의해 생성된 구성 로그를 확인합니다. 필터를 적용하고 저장하여 특정 구성 로그를 빠르게 식별하고 표시된 구성 로그를 CSV 형식으로 내보냅니다.

필드	설명
시간	감사 코멘트가 커밋된 시간입니다.
관리자	감사 코멘트의 내용입니다.
명령	실행된 명령 유형입니다.
변경 전	변경이 발생하기 전의 규칙 정보입니다. 예를 들어 규칙의 이름을 바꾸면 이전 이름이 표시됩니다.
변경 후	변경이 발생한 후의 규칙 정보입니다. 예를 들어 규칙의 이름을 바꾸면 새 이름이 표시됩니다.
디바이스 이름	감사 설명을 변경하기 전의 디바이스 이름입니다.

규칙 변경

선택한 정책 규칙의 구성 버전을 보고 비교하여 발생한 변경 사항을 분석합니다. 드롭다운에서 비교할 두 개의 정책 규칙 구성 버전을 선택합니다.



규칙 사용 적중 수 쿼리

- 선언 > 규칙 사용

규칙 사용 쿼리를 사용하여 지정된 기간 동안 선택한 룰베이스(rulebase)를 필터링합니다. 규칙 사용 쿼리를 사용하면 정책 룰베이스(rulebase)를 빠르게 필터링하여 제거할 사용하지 않는 규칙을 식별하여 공격자에 대한 열린 진입점을 줄일 수 있습니다. **PDF/CSV**를 클릭하여 필터링된 규칙을 PDF 또는 CSV 형식으로 내보냅니다. 규칙 사용 적중 수 쿼리를 사용하려면 정책 규칙 적중 수 설정(디바이스 > 설정 > 관리)을 활성화해야 합니다.

기본적으로 이름, 위치, 생성됨, 수정됨 및 규칙 사용 열은 정책 룰베이스(rulebase)에서 규칙 사용을 쿼리할 때 표시됩니다. 열을 더 추가하여 정책 규칙에 대한 추가 정보를 볼 수 있습니다.

작업	설명
조회수	
기간	선택한 룰베이스(rulebase)를 쿼리할 시간 프레임을 나타냅니다. 미리 결정된 시간 프레임에서 선택하거나 사용자 정의 시간 프레임을 설정합니다.
용법	쿼리할 규칙 사용을 선택합니다. 모두, 사용되지 않음, 사용됨 또는 부분적으로 사용됨(Panorama만 해당).
이후	(Custom Timeframe만 해당) 정책 룰베이스(rulebase)를 쿼리할 날짜와 시간을 선택합니다.
지난 _일 동안 재설정된 제외 규칙	지정된 일 수 내에 사용자가 수동으로 재설정한 모든 규칙을 제외하려면 이 옵션을 선택합니다.
작업	
삭제	하나 이상의 선택한 정책 규칙을 삭제합니다.
활성화	비활성화된 경우 선택한 정책 규칙을 하나 이상 활성화합니다.
비활성화	하나 이상의 선택한 정책 규칙을 비활성화합니다.
PDF/CSV	현재 PDF 또는 CSV 형식으로 표시된 필터링된 정책 규칙을 내보냅니다.
규칙 적중 카운터 재설정	선택한 규칙 또는 필터링되어 현재 표시된 모든 규칙에 대한 규칙 사용 데이터를 재설정합니다.

작업	설명
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.

규칙 적중 수 쿼리에 대한 디바이스 규칙 사용

Panorama 관리 서버에서 정책 규칙에 대한 규칙 사용을 볼 때 디바이스 및 가상 시스템 규칙 사용을 볼 수 있습니다. **Reset Rule Hit Counter**는 적중 횟수, 첫 적중 및 마지막 적중을 재설정합니다.

PDF/CSV를 클릭하여 필터링된 규칙을 PDF 또는 CSV 형식으로 내보냅니다.

필드	설명
디바이스 그룹	디바이스 또는 가상 시스템이 속한 디바이스 그룹입니다.
디바이스 이름/가상 시스템	디바이스 그룹 또는 가상 시스템의 이름입니다.
조회수	정책 규칙에 대한 총 트래픽 일치 수입니다.
마지막 적중	정책 규칙에 대한 최신 트래픽 일치의 날짜 및 시간입니다.
첫 번째 적중	정책 규칙에 대한 첫 번째 트래픽 일치의 날짜 및 시간입니다.
마지막 업데이트 수신	디바이스에서 Panorama 관리 서버로 마지막으로 수신된 규칙 사용 정보의 날짜 및 시간입니다.
생성	정책 규칙이 생성된 날짜 및 시간입니다.
수정	정책 규칙이 마지막으로 수정된 날짜 및 시간입니다. 정책 규칙이 수정되지 않은 경우 열이 비어 있습니다.
상태	디바이스의 연결 상태: ### 또는 ## ###.

정책 > 보안

보안 정책 규칙은 보안 영역을 참조하고 애플리케이션, 사용자 또는 사용자 그룹, 서비스(포트 및 프로토콜)를 기반으로 네트워크의 트래픽을 허용, 제한 및 추적할 수 있도록 합니다. 기본적으로 방화벽에는 트러스트 영역에서 신뢰하지 않는 영역으로의 모든 트래픽을 허용하는 *rule1*이라는 보안 규칙이 포함되어 있습니다.

무엇을 알고 싶습니까?	참조:
보안 정책이란 무엇입니까?	보안 정책 개요 Panorama의 경우 정책 규칙 이동 또는 복사를 참조하십시오.
보안 정책 규칙을 생성하는 데 사용할 수 있는 필드는 무엇입니까?	보안 정책 규칙의 빌딩 블록
웹 인터페이스를 사용하여 보안 정책 규칙을 관리하려면 어떻게 해야 합니까?	정책 생성 및 관리 보안 정책 규칙 재정의 또는 되돌리기 응용 및 사용 보안 정책 최적화
더 찾고 계십니까?	보안 정책

보안 정책 개요

보안 정책을 사용하면 규칙을 적용하고 조치를 취할 수 있으며 필요에 따라 일반적이거나 구체적일 수 있습니다. 정책 규칙은 들어오는 트래픽과 순서대로 비교되며 트래픽과 일치하는 첫 번째 규칙이 적용되기 때문에 보다 구체적인 규칙이 보다 일반적인 규칙보다 우선해야 합니다. 예를 들어, 다른 모든 트래픽 관련 설정이 동일한 경우 단일 애플리케이션에 대한 규칙은 모든 애플리케이션에 대한 규칙보다 우선해야 합니다.

최종 사용자가 네트워크 리소스에 액세스하려고 할 때 인증하도록 하기 위해 방화벽은 보안 정책보다 먼저 인증 정책을 평가합니다. 자세한 내용은 정책 > 인증을 참조하십시오.

사용자 정의 규칙과 일치하지 않는 트래픽에는 기본 규칙이 적용됩니다. 보안 룰베이스(rulebase) 하단에 표시되는 기본 규칙은 모든 영역 내 트래픽(영역 내)을 허용하고 모든 영역 간 트래픽(영역 간)을 거부하도록 사전 정의되어 있습니다. 이러한 규칙은 사전 정의된 구성의 일부이며 기본적으로 읽기 전용이지만 태그, 작업(허용 또는 거부), 로그 설정 및 보안 프로파일을 포함하여 규칙을 재정의하고 제한된 수의 설정을 변경할 수 있습니다.

인터페이스에는 보안 정책 규칙을 정의하기 위한 다음 탭이 있습니다.

- 일반 - 일반 탭을 선택하여 보안 정책 규칙의 이름과 설명을 구성합니다.
- 소스 - 소스 탭을 선택하여 트래픽이 시작되는 소스 영역 또는 소스 주소를 정의합니다.
- 사용자 - 개별 사용자 또는 사용자 그룹에 대한 정책을 시행하려면 사용자 탭을 선택합니다. 호스트 정보 프로파일(HIP)이 활성화된 GlobalProtect™를 사용하는 경우 GlobalProtect에서 수집한 정보를 기반으로 정책을 설정할 수도 있습니다. 예를 들어, 사용자 액세스 수준은 사용자의 로컬 구성에 대해 방화벽에 알리는 HIP를 결정할 수 있습니다. HIP 정보는 호스트에서 실행 중인 보안 프로그램, 레지스트리 값 및 호스트에 바이러스 백신 소프트웨어가 설치되어 있는지의 여부와 같은 기타 여러 검사를 기반으로 하는 세분화된 액세스 제어에 사용할 수 있습니다.
- 대상 - 대상 탭을 선택하여 트래픽의 대상 영역 또는 대상 주소를 정의합니다.
- 애플리케이션 - 애플리케이션 또는 애플리케이션 그룹을 기반으로 정책 작업이 발생하도록 하려면 애플리케이션 탭을 선택합니다. 또한 관리자는 기존 App-ID™ 서명을 사용하고 이를 사용자 정의하여 독점 애플리케이션을 감지하거나 기존 애플리케이션의 특정 속성을 감지할 수도 있습니다. 사용자 지정 애플리케이션은 **Objects** > **Applications**에 정의되어 있습니다.
- 서비스/**URL** 카테고리 - 서비스/**URL** 카테고리 탭을 선택하여 정책의 일치 기준으로 특정 TCP 및/또는 UDP 포트 번호 또는 URL 카테고리를 지정합니다.
- 작업 - 정의된 정책 속성과 일치하는 트래픽을 기반으로 수행할 작업을 결정하려면 작업 탭을 선택합니다.
- 대상 - 보안 정책 규칙에 대한 디바이스 또는 태그를 지정하려면 대상 탭을 선택합니다.
- 사용량 - 규칙에서 본 애플리케이션 수, 규칙에서 마지막으로 새 애플리케이션을 본 시간, 적중 횟수 데이터, 지난 30일 동안의 트래픽 및 규칙이 생성된 시간을 포함하여 규칙의 사용량을 보려면 사용량 탭을 선택합니다. 마지막으로 수정했습니다.

보안 정책 규칙의 빌딩 블록

- 정책 > 보안

다음 섹션에서는 보안 정책 규칙의 각 구성 요소에 대해 설명합니다. 보안 정책 규칙을 생성할 때 여기에 설명된 옵션을 구성할 수 있습니다.

보안 규칙의 빌딩 블록	구성 위치	설명
규칙 번호	해당 사항 없음	방화벽은 각 규칙에 자동으로 번호를 매기고 규칙의 순서는 규칙이 이동함에 따라 변경됩니다. 특정 필터와 일치하도록 규칙을 필터링하면 각 규칙은 규칙 베이스의 전체 규칙 집합 컨텍스트에서 번호와 함께 표시되고 평가 순서에서 해당 위치가 표시됩니다. Panorama는 사전 규칙과 사후 규칙에 독립적으로 번호를 지정합니다. Panorama가 관리 방화벽에 규칙을 푸시할 때 규칙 번호 지정은 규칙 베이스 내의 사전 규칙, 방화벽 규칙 및

보안 규칙의 빌딩 블록	구성 위치	설명
		사후 규칙의 레이어 구조를 통합하고 규칙 순서와 평가 순서를 반영합니다.
이름	일반	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹과 모든 상위 또는 하위 디바이스 그룹 내에서 고유해야 합니다.
규칙 유형		규칙이 영역 내, 영역 간 또는 둘 다에 적용되는지의 여부를 지정합니다. • 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 • 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. • 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.
설명		정책에 대한 설명을 입력합니다(최대 1,024자).
태그		정책에 대한 태그를 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 특정 규칙에 Decrypt 및 No-decrypt와 같은 특정 단어로 태그를 지정하거나 해당 위치와 연결된 정책에 대해 특정 데이터 센터의 이름을 사용할 수 있습니다.

보안 규칙의 빌딩 블록	구성 위치	설명
		기본 규칙에 태그를 추가할 수도 있습니다.
소스 영역	소스	소스 영역을 추가합니다(기본값은 모두). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을 참조하세요. 여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다.
소스 주소	소스	소스 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 **Any**). 드롭다운에서 선택하거나 주소 개체, 주소 그룹 또는 지역(드롭다운 하단)을 선택하여 설정을 지정합니다. 개체>주소 및 개체>주소 그룹은 각각 보안 정책 규칙이 지원하는 주소 개체 및 주소 그룹의 유형을 설명합니다. 무효 옵션을 선택하면 지정된 주소를 제외하고 지정된 영역의 소스 주소에 규칙이 적용됩니다.
소스 사용자	소스	정책에 따라 소스 사용자 또는 사용자 그룹을 추가합니다. • 모두 - 사용자 데이터에 관계없이 모든 트래픽을 포함합니다. • 사전 로그온 - GlobalProtect를 사용하여 네트워크에 연결되었지만 시스템에 로그인하지 않은 원격 사용자를 포함합니다. 사전 로그온 옵션이 GlobalProtect용 포털 엔드포인트에서 구성되면 현재 시스템에 로그인하지 않은 사용자는 사전 로그온 사용자명으로 식별됩니다. 그런 다음 사전 로그온 사용자에 대한 정책을 생성할 수 있으며 사용자가 직접 로그인하지 않더라도 해당 컴퓨터는 완전히 로그인한 것처럼 도메인에서 인증됩니다. • 알려진 사용자 - 모든 인증된 사용자를 포함합니다. 즉, 매핑된 사용자 데이터가 있는 모든 IP 주소를 의미합니다. 이 옵션은 도메인의 도메인 사용자 그룹과 동일합니다. • **unknown** - 인증되지 않은 모든 사용자를 포함합니다. 즉, 사용자에게 매핑되지 않은 IP 주소를 의미합니다. 예를 들어, 게스트 수준 액세스에 대해 **unknown**을 사용할 수 있습니다. 그 이유는 네트워크에 IP 주소가 있지만 도메인에 대해 인증되지 않고 방화벽에 IP 주소-사용자 매핑 정보가 없기 때문입니다.

보안 규칙의 빌딩 블록	구성 위치	설명
		• 선택 - 이 창에서 선택한 항목에 따라 선택한 사용자를 포함합니다. 예를 들어 사용자 한 명, 개인 목록, 일부 그룹을 추가하거나 수동으로 사용자를 추가할 수 있습니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS, TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.
소스 디바이스	소스	정책에 따라 호스트 디바이스를 추가합니다. • 모두 - 모든 디바이스를 포함합니다. • **no-hip** - HIP 정보가 필요하지 않습니다. 이 설정을 사용하면 HIP 정보를 수집하거나 제출할 수 없는 타사 디바이스에서 액세스할 수 있습니다. • 격리 - 격리 목록에 있는 모든 디바이스를 포함합니다(디바이스 > 디바이스 격리). • **select** - 구성에 따라 결정된 선택된 디바이스를 포함합니다. 예를 들어 모델, OS, OS 제품군 또는 공급자를 기반으로 디바이스 개체를 추가할 수 있습니다.
소스 HIP 프로파일	소스	최신 보안 패치 및 바이러스 백신 정의가 설치되어 있는지의 여부와 같은 최종 호스트의 보안 상태에 대한 정보를 수집할 수 있도록 HIP(호스트 정보 프로파일)를 추가합니다. 정책 시행을 위해 호스트 정보 프로파일을 사용하면 중요한 리소스에 액세스하는 원격 호스트가 네트워크 리소스에 액세스하도록 허용되기 전에 보안 표준을 준수하고 적절하게 유지 관리되도록 하는 세분화된 보안이 가능합니다. 다음 소스 HIP 프로파일이 지원됩니다. • **any** - HIP 정보에 관계없이 모든 엔드포인트을 포함합니다. • **select** - 구성에 따라 결정된 선택된 HIP 프로파일을 포함합니다. 예를 들어 HIP 프로파일 하나, HIP 프로파일 목록을 추가하거나 HIP 프로파일을 수동으로 추가할 수 있습니다. • **no-hip** - HIP 정보가 필요하지 않습니다. 이 설정을 사용하면 HIP 정보를 수집하거나 제출할 수 없는 타사 클라이언트에서 액세스할 수 있습니다.

보안 규칙의 빌딩 블록	구성 위치	설명
소스 가입자	소스	다음 형식을 사용하여 5G 또는 4G 네트워크에 하나 이상의 소스 가입자를 추가합니다. • 모두 • (5G만 해당) IMSI를 포함한 5G SUPI(구독 영구 식별자) • IMSI(14 또는 15자리) • 하이픈으로 구분된 11~15자리의 IMSI 값 범위 • 프리픽스 뒤에 와일드카드로 별표(*)가 있는 6자리 IMSI 프리픽스 • IMSI를 지정하는 EDL
소스 장비		다음 형식을 사용하여 5G 또는 4G 네트워크에서 하나 이상의 소스 장비 ID를 추가합니다. • 모두 • (5G만 해당) IMEI(International Mobile Equipment Identity)를 포함한 5G PEI(Permanent Equipment Identifier) • IMEI(11~16자리 길이) • TAC(유형 할당 코드)에 대한 8자리 IMEI 프리픽스 • IMEI를 지정하는 EDL

네트워크 슬라이스	소스	다음과 같이 5G 네트워크에서 네트워크 슬라이스 서비스 유형(SST)을 기반으로 하나 이상의 소스 네트워크 슬라이스를 추가합니다.
		• 표준화된(사전 정의된) **SST**
		  • **eMBB**(enhanced Mobile Broadband) - 비디오 스트리밍과 같은 더 빠른 속도와 높은 데이터 속도용.
		  • **URLLC**(Ultra-Reliable Low-Latency Communications) - 중요한 IoT(의료, 무선 결제, 홈 컨트롤 및 차량 통신)와 같이 지연에 민감한 미션 크리티컬 애플리케이션용.
		  • **MIoT**(대규모 사물 인터넷)—예: 스마트 계량, 스마트 폐기물 관리, 도난 방지, 자산 관리 및 위치 추적.
		• 네트워크 슬라이스 **SST** - 운영자별 - 슬라이스의 이름을 지정하고 지정합니다. 슬라이스 이름의 형식은 텍스트 다

보안 규칙의 빌딩 블록	구성 위치	설명
		음에 쉼표(,) 및 숫자(범위는 128~255)가 오는 형식입니다. 예: 엔터프라이즈 오일2,145.
대상 영역	데스티네이션	대상 영역을 추가합니다(기본값은 모두). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을 참조하세요. 여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다. 영역 내 규칙에서는 이러한 유형의 규칙이 동일한 영역 내의 소스 및 대상이 있는 트래픽만 일치시키기 때문에 대상 영역을 정의할 수 없습니다. 영역 내 규칙과 일치하는 영역을 지정하려면 소스 영역만 지정해야 합니다.
대상 주소		대상 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 **Any**). 드롭다운에서 선택하거나 주소 개체, 주소 그룹 또는 지역(드롭다운 하단)을 클릭하여 주소 설정을 지정합니다. 개체>주소 및 개체>주소 그룹은 각각 보안 정책 규칙이 지원하는 주소 개체 및 주소 그룹의 유형을 설명합니다. 부정 옵션을 선택하면 지정된 주소를 제외하고 지정된 영역의 대상 주소에 규칙이 적용됩니다.
대상 디바이스		정책에 따라 호스트 디바이스를 추가합니다. • 모두 - 모든 디바이스를 포함합니다. • 격리 - 격리 목록에 있는 모든 디바이스를 포함합니다(디바이스 > 디바이스 격리). • **select** - 구성에 따라 결정된 선택된 디바이스를 포함합니다. 예를 들어 모델, OS, OS 제품군 또는 공급자를 기반으로 디바이스 개체를 추가할 수 있습니다.
애플리케이션	애플리케이션	보안 정책 규칙에 대한 특정 애플리케이션을 추가합니다. 애플리케이션에 여러 기능이 있는 경우 전체 애플리케이션 또는 개별 기능을 선택할 수 있습니다. 전체 애플리케이션을 선택하면 모든 기능이 포함되며 향후 기능이 추가되면 애플리케이션 정의가 자동으로 업데이트됩니다.

보안 규칙의 빌딩 블록	구성 위치	설명
		보안 정책 규칙에서 애플리케이션 그룹, 필터 또는 컨테이너를 사용하는 경우 애플리케이션 열의 개체 위로 마우스를 가져간 다음 드롭다운을 열고 값을 선택하여 이러한 개체의 세부 정보를 볼 수 있습니다. 이를 통해 개체 탭으로 이동할 필요 없이 정책에서 직접 애플리케이션 구성원을 볼 수 있습니다. 네트워크에서 원하는 애플리케이션만 허용되도록 항상 하나 이상의 애플리케이션을 지정하십시오. 그러면 공격 면적이 줄어들고 네트워크 트래픽을 더 잘 제어할 수 있습니다. 애플리케이션을 모두로 설정하지 마십시오. 모든 애플리케이션의 트래픽을 허용하고 공격 면적을 증가시킵니다.
서비스	서비스/**URL** 카테고리	특정 TCP 또는 UDP 포트 번호로 제한할 서비스를 선택합니다. 드롭다운에서 다음 중 하나를 선택합니다. • **any** - 선택한 애플리케이션이 모든 프로토콜 또는 포트에서 허용되거나 거부됩니다. • **application-default** - 선택한 애플리케이션은 **Palo Alto Networks®**에서 정의한 기본 포트에서만 허용되거나 거부됩니다. 이 옵션은 의도하지 않은 경우 원치 않는 애플리케이션 동작 및 사용의 신호일 수 있는 비정상적인 포트 및 프로토콜에서 애플리케이션이 실행되는 것을 방지하기 때문에 허용 정책에 권장됩니다. 이 옵션을 사용하면 방화벽은 여전히 모든 포트의 모든 애플리케이션을 확인하지만 애플리케이션은 기본 포트 및 프로토콜에서만 허용됩니다.

보안 규칙의 빌딩 블록	구성 위치	설명
		대부분의 애플리케이션에서 애플리케이션 기본값을 사용하여 애플리케이션이 비표준 포트를 사용하거나 다른 회피 동작을 나타내지 않도록 합니다. 애플리케이션의 기본 포트가 변경되면 방화벽은 자동으로 규칙을 올바른 기본 포트로 업데이트합니다. 내부 사용자 지정 애플리케이션과 같이 비표준 포트를 사용하는 애플리케이션의 경우 애플리케이션을 수정하거나 비표준 포트를 지정하는 규칙을 생성합니다 해당 애플리케이션이 필요한 트래픽에만 규칙을 적용합니다. • 선택 - 기존 서비스를 추가하거나 서비스 또는 서비스 그룹을 선택하여 새 항목을 지정합니다. (또는 개체 > 서비스 및 개체 > 서비스 그룹 선택).
URL 카테고리		보안 규칙에 대한 URL 카테고리를 선택합니다. • URL 카테고리에 관계없이 모든 세션을 허용하거나 거부하려면 모두를 선택합니다. • 카테고리를 지정하려면 드롭다운에서 하나 이상의 특정 카테고리(사용자 지정 카테고리 포함)를 추가합니다. 개체 > 외부 동적 목록을 선택하여 사용자 정의 카테고리를 정의합니다.
액션 설정	작업	규칙에 정의된 속성과 일치하는 트래픽에 대해 방화벽이 수행하는 작업을 선택합니다. • 허용(기본값) - 일치하는 트래픽을 허용합니다. • 거부 - 일치하는 트래픽을 차단하고 거부된 애플리케이션에 대해 정의된 기본 거부 작업을 시행합니다. 애플리케이션에 대해 기본적으로 정의된 거부 작업을 보려면 애플리케이션 세부 정보(개체 > 애플리케이션)를 봅니다. 기본 거부 동작은 애플리케이션에 따라 다르기 때문에 방화벽은 세션을 차단하고 한 애플리케이션에 대한 재설정을 보내는 동안 다른 애플리케이션에 대한 세션을 자동으로 삭제할 수 있습니다. • 삭제 - 애플리케이션을 자동으로 삭제합니다. **Send ICMP Unreachable**을 선택하지 않으면 TCP 재설정이 호스트나 애플리케이션으로 보내지지 않습니다.

보안 규칙의 빌딩 블록	구성 위치	설명
		• 클라이언트 재설정 - TCP 재설정을 클라이언트 측 디바이스로 보냅니다. • 서버 재설정 - TCP 재설정을 서버 측 디바이스로 보냅니다. • 클라이언트와 서버 모두 재설정 - 클라이언트 측 및 서버 측 디바이스 모두에 TCP 재설정을 보냅니다. • **ICMP** 발신 도달 불가 - 레이어 3 인터페이스에만 사용할 수 있습니다. 트래픽을 삭제하거나 연결을 재설정하도록 보안 정책 규칙을 구성하면 트래픽이 대상 호스트에 도달하지 않습니다. 이러한 경우 모든 UDP 트래픽 및 삭제된 TCP 트래픽에 대해 방화벽이 트래픽이 시작된 소스 IP 주소로 ICMP 연결 불가 응답을 보내도록 설정할 수 있습니다. 이 설정을 활성화하면 소스가 세션을 정상적으로 닫거나 지울 수 있으며 애플리케이션이 중단되는 것을 방지할 수 있습니다. 방화벽에 구성된 ICMP 연결할 수 없는 패킷 속도를 보려면 세션 설정(**Device** > **Setup** > **Session**)을 확인하십시오. 사전 정의된 영역 간 및 영역 내 규칙에 정의된 기본 작업을 재정의하려면 보안 정책 규칙 재정의 또는 되돌리기를 참조하십시오.
프로파일 설정	작업	보안 프로파일 규칙과 일치하는 패킷에 대해 방화벽이 수행하는 추가 검사를 지정하려면 개별 바이러스 백신, 취약점 보호, 안티 스파이웨어, URL 필터링, 파일 차단, 데이터 필터링, WildFire 분석, 모바일 네트워크 보호 및 SCTP 보호 프로파일을 선택합니다. 개별 프로파일이 아닌 프로파일 그룹을 지정하려면 프로파일 유형을 그룹으로 선택한 다음 그룹 프로파일을 선택합니다. 새 프로파일 또는 프로파일 그룹을 정의하려면 해당 프로파일 옆에 있는 새로 생성를 클릭하거나 새 그룹 프로파일을 선택합니다. 보안 프로파일(또는 프로파일 그룹)을 기본 규칙에 연결할 수도 있습니다.
로그 설정 및 기타 설정	작업	이 규칙과 일치하는 트래픽에 대한 항목을 로컬 트래픽 로그에 생성하려면 다음 옵션을 선택합니다.

보안 규칙의 빌딩 블록	구성 위치	설명
		• 세션 시작 시 기록(기본적으로 비활성화됨) - 세션 시작에 대한 트래픽 로그 항목을 생성합니다. 문제 해결 목적 또는 터널 세션 로그가 *ACC*에서 활성 *GRE* 터널을 표시하는 경우를 제외하고 세션 시작 시 로그를 활성화하지 마십시오. 세션 끝에서 로깅은 더 적은 리소스를 소비하고 애플리케이션이 몇 패킷 후에 변경되는 경우 정확한 애플리케이션을 식별합니다*(*예*: facebook-base*에서 *facebook-chat*으로*).* • 세션 종료 시 기록(기본적으로 활성화됨) - 세션 종료 시 트래픽 로그 항목을 생성합니다. 세션 시작 또는 종료 항목이 기록되면 삭제 및 거부 항목도 기록됩니다. • 로그 포워딩 프로파일 - 로컬 트래픽 로그 및 위협 로그 항목을 Panorama 및 syslog 서버와 같은 원격 대상으로 포워딩하려면 로그 포워딩 프로파일을 선택합니다. 위협 로그 항목의 생성은 보안 프로파일에 의해 결정됩니다. 필요에 따라 새 로그 프로파일을 정의합니다*(*개체 > 로그 포워딩 참조*).* 전용 외부 저장 디바이스에 로그를 보내기 위해 로그 포워딩 프로파일을 생성하고 활성화합니다. 이렇게 하면 방화벽이 로그 저장 공간을 제한하고 공간이 소모되면 방화벽이 가장 오래된 로그를 제거하기 때문에 로그가 보존됩니다. 기본 규칙에 대한 로그 설정을 수정할 수도 있습니다. 다음 옵션의 조합을 지정합니다. • 일정 - 규칙이 적용되는 날짜와 시간을 제한하려면 드롭다운에서 일정을 선택합니다. 필요에 따라 새 일정을 정의합니다(복호화된 SSL 트래픽 제어 설정 참조). • **QoS** 표시 - 규칙과 일치하는 패킷에 대한 QoS(서비스 품질) 설정을 변경하려면 **IP DSCP** 또는 **IP** 우선 순위를 선택한 다음 QoS 값을 이진 형식으로 입력하거나 드롭다운에서 사전 정의된 값을 선

보안 규칙의 빌딩 블록	구성 위치	설명
		택합니다. QoS에 대한 자세한 내용은 서비스 품질 을 참조하세요. • 서버 응답 검사 비활성화 - 서버에서 클라이언트로 가는 패킷 검사를 비활성화합니다. 이 옵션은 기본적으로 비활성화되어 있습니다. 최상의 보안 상태를 위해 서버 응답 검사 비활성화를 활성화하지 마십시오. 이 옵션을 선택하면 방화벽은 클라이언트에서 서버로의 흐름만 검사합니다. 서버-클라이언트 흐름을 검사하지 않으므로 이러한 트래픽 플로우에 위협이 있는지 식별할 수 없습니다.
기초	규칙 사용	• 생성된 규칙 - 규칙 생성 날짜 및 시간입니다. • 마지막 편집 - 규칙이 마지막으로 편집된 날짜 및 시간입니다.
Activity	규칙 사용	• 적중 횟수 - 트래픽이 규칙과 일치(적중)한 총 횟수입니다. • 첫 번째 적중 - 첫 번째 규칙 일치 시간입니다. • 마지막 적중 - 마지막 규칙 일치 시간입니다.
애플리케이션	규칙 사용	• 본 애플리케이션 - 규칙이 허용하는 애플리케이션 수입니다. • 마지막으로 본 앱 - 마지막 새 애플리케이션(이전에 본 적이 없는 애플리케이션)이 규칙에 표시된 이후의 일 수입니다. • 애플리케이션 및 표시된 애플리케이션 비교 - 규칙에 구성된 애플리케이션을 규칙에 표시된 애플리케이션과 비교하려면 클릭합니다. 이 도구를 사용하여 규칙과 일치하는 애플리케이션을 검색하고 규칙에 애플리케이션을 추가합니다.

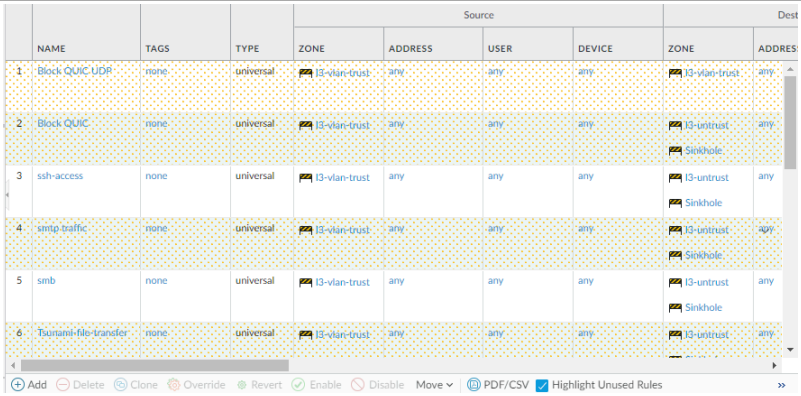
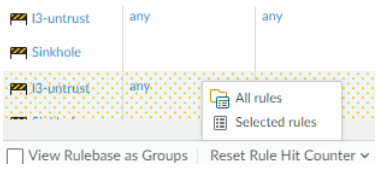
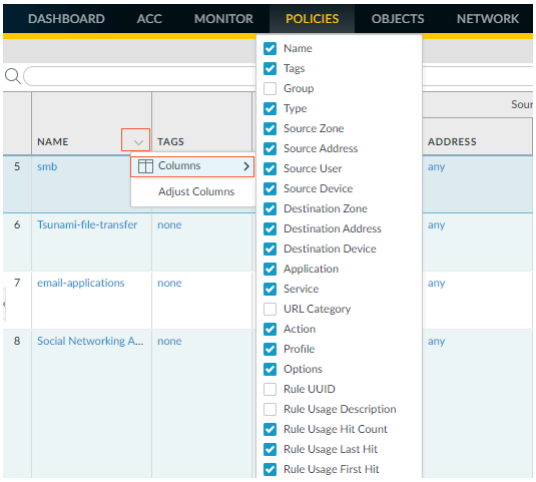
보안 규칙의 빌딩 블록	구성 위치	설명
트래픽(지난 30일)	규칙 사용	• 바이트 - 지난 30일 동안 규칙의 트래픽 양(바이트)입니다. 기간이 *30*일보다 길면 가장 오래된 규칙이 가장 누적된 트래픽을 가질 가능성이 높기 때문에 목록의 맨 위에 남아 있게 됩니다. 이로 인해 새 규칙에서 트래픽이 많이 발생하더라도 새 규칙이 이전 규칙 아래에 나열될 수 있습니다.
모두(모든 디바이스를 대상으로 함) Panorama 전용	대상	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스 Panorama 전용		정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그 Panorama 전용		지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅 Panorama 전용		선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

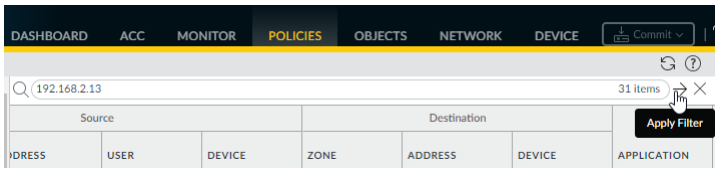
정책 생성 및 관리

정책 > 보안 페이지를 선택하여 보안 정책을 추가, 수정 및 관리합니다.

업무	설명
추가하다	새 정책 규칙을추가하거나 새 규칙 및 복사 규칙을 기반으로 하는 규칙을 선택합니다. 복사된 규칙 "rule*n*"이 선택한 규칙 아래에 삽입됩니다. 여기서 *n*는 규칙 이름을 고유하게 만드는 다음으로 사용 가능한 정수입니다. 복사에 대한 자세한 내용은 정책 규칙 이동 또는 복사를 참조하십시오.
수정	규칙을 선택하여 설정을 수정합니다.

업무	설명
	규칙이 Panorama에서 푸시되는 경우 규칙은 방화벽에서 읽기 전용이며 로컬로 편집할 수 없습니다.
	재정의 및 되돌리기 작업은 보안 규칙 베이스의 맨 아래에 표시되는 기본 규칙에만 적용됩니다. 이러한 사전 정의된 규칙(모든 영역 내 트래픽 허용 및 모든 영역 간 트래픽 거부)은 규칙 베이스의 다른 규칙과 일치하지 않는 트래픽을 처리하는 방법에 대해 방화벽에 지시합니다. 사전 정의된 구성의 일부이므로 정책 설정을 편집하려면 재정의해야 합니다. Panorama를 사용하는 경우 기본 규칙을 재정의한 다음 디바이스 그룹 또는 공유 컨텍스트의 방화벽으로 푸시할 수도 있습니다. 사전 정의된 설정이나 Panorama에서 푸시된 설정을 복원하는 기본 규칙을 되돌릴 수도 있습니다. 자세한 내용은 보안 정책 규칙 재정의 또는 되돌리기를 참조하십시오.
이동	규칙은 위에서 아래로 평가되며 정책 페이지에 내레이션될 때 평가됩니다. 네트워크 트래픽에 대해 규칙이 평가되는 순서를 변경하려면, 규칙, 위로 이동, 아래로 이동, 위로 이동, 아래로 이동 또는 다른 규칙 베이스로 이동 또는 디바이스 그룹을 선택합니다. 자세한 내용은 정책 규칙 이동 또는 복사를 참조하십시오.
UUID 복사	구성 또는 로그를 검색할 때 사용할 수 있도록 규칙의 UUID를 클립보드에 복사합니다.
삭제	기존 규칙을 선택한 다음 삭제합니다.
활성화/비활성화	규칙을 사용하지 않도록 설정하려면 규칙을 선택한 다음 사용하지 않도록 설정합니다.
규칙 사용 모니터	방화벽이 마지막으로 다시 시작된 이후에 사용되지 않은 규칙을 식별하려면 사용하지 않는 규칙을 강조 표시합니다. 사용되지 않는 규칙에는 점선 배경이 있습니다. 그런 다음 규칙을 사용하지 않도록 설정하거나 삭제할지의 여부를 결정할 수 있습니다. 현재 사용되지 않는 규칙은 점선 노란색 배경으로 표시됩니다. 정책 규칙 적중 횟수가 활성화되면 Hit Count 데이터를 사용하여 규칙을 사용하지 않는지의 여부를 결정합니다. 각 방화벽은 일치하는 규칙에 대한 트래픽 플래그를 유지 관리합니다. 리부트 또는 다시 시작할 때 플래그가 재설정되므로 이 목록을 주기적으로 모니터링하여 규칙을 삭제하거나 비활성화하기 전에 마지막 검사 이후 규칙이 일치하는지의 여부를 확인하는 것이 좋습니다.

업무	설명
	
히트 카운트 규칙 재설정	히트 카운트는 정책 규칙의 총 트래픽 조회를 추적합니다. 총 트래픽 적중 횟수는 재부팅, 업그레이드 및 데이터플레인 다시 시작을 통해 유지됩니다. 또는 히트 카운터 룰 재설정(하단 메뉴)을 합니다. 적중 수 통계를 지우려면 모든 규칙을 선택하거나 특정 규칙을 선택한 다음 선택한 규칙에 대해서만 적중 수 통계를 재설정합니다.  첫 번째 히트를 확인하여 보안 정책이 처음 조회된 시기를 확인합니다. 날짜는 날짜 hh:mm:ss 연도로 형식이 지정됩니다. 이 값을 재설정할 수 없습니다. 마지막 히트를 확인하여 보안 정책이 마지막으로 사용된 시기를 확인합니다. 날짜는 날짜 hh:mm:ss 연도로 형식이 지정됩니다. 이 값을 재설정할 수 없습니다.
열 표시/숨기기	정책 아래에 표시되는 열을 표시하거나 숨깁니다. 열을 선택하여 디스플레이를 전환합니다. 

업무	설명
필터 적용	목록에 필터를 적용하려면 필터 규칙 드롭다운 중에서 선택합니다. 필터를 정의하려면 항목 드롭다운에서 필터를 선택합니다. 기본 규칙은 규칙 기준 필터링의 일부가 아니며 항상 필터링된 규칙 목록에 표시됩니다.
	정책에 대해 일치하는 것으로 기록된 네트워크 세션을 보려면 규칙 이름 드롭다운에서 **Log Viewer**를 선택합니다.
	현재 값을 표시하려면 항목 드롭다운에서 값을 선택합니다. 열 메뉴에서 직접 항목을 편집, 필터링 또는 제거할 수도 있습니다. 예를 들어 주소 그룹에 포함된 주소를 보려면 주소 열의 개체 위로 마우스를 가져가고 드롭다운에서 값을 선택합니다. 이렇게 하면 **Object** 탭으로 이동할 필요 없이 주소 그룹의 구성원 및 해당 IP 주소를 빠르게 볼 수 있습니다.
	이름 또는 IP 주소를 기반으로 정책 내에서 사용되는 개체를 찾으려면 필터를 사용합니다. 필터를 적용하면 필터와 일치하는 항목만 표시됩니다. 필터는 임베디드 개체에서도 작동합니다. 예를 들어 10.1.4.8을 필터링할 때 해당 주소가 포함된 정책만 표시됩니다. 
미리보기 규칙(Panorama만 해당)	규칙을 미리 보기 위해 규칙을 관리되는 방화벽으로 푸시하기 전에 규칙 목록을 볼 수 있습니다. 각 규칙 베이스 내에서 규칙 레이어는 각 디바이스 그룹(및 관리방화벽)에 대해 시각적으로 구분되어 많은 수의 규칙을 쉽게 스캔할 수 있습니다.
내보내기 구성 테이블	읽기 전용 액세스 권한이 최소한 관리 역할은 정책 규칙 기준을 **PDF/CSV**로 내보낼 수 있습니다. 필터를 적용하여 감사와 같이 필요에 따라 보다 구체적인 테이블 구성 출력을 만들 수 있습니다. 웹 인터페이스에서 표시되는 열만 내보낼 것입니다. 구성 테이블 내보내기를 참조하십시오.
사용하지 않은 규칙 강조 표시	규칙 사용 열에 트래픽 일치가 없는 정책 규칙을 강조 표시합니다.
그룹	규칙 기준 보기를 그룹 상자로 선택한 경우 태그 그룹을 관리합니다. 다음 작업을 수행할 수 있습니다. • 그룹의 규칙을 다른 규칙 베이스 또는 디바이스 그룹으로 이동 - 선택한 태그 그룹을 다른 디바이스 그룹으로 이동합니다.

업무	설명
	• 모든 규칙의 그룹 변경 - 선택한 태그 그룹의 규칙을 룰베이스(rulebase)의 다른 태그 그룹으로 이동합니다. • 그룹의 모든 규칙을 삭제합니다 - 선택한 태그 그룹의 모든 규칙을 삭제합니다. • 그룹의 모든 규칙을 복사하여 선택한 태그 그룹의 규칙을 디바이스 그룹으로 복사합니다.
룰베이스(rulebase)를 그룹으로 보기	규칙 기준을 그룹으로 보기 위해 태그별 그룹 규칙에 사용된 태그를 사용하여 정책 룰베이스(rulebase)를 볼 수 있습니다. 표시되는 정책 규칙은 선택한 태그 그룹에 속한 규칙입니다.
테스트 정책 일치	선택한 정책 규칙 베이스에 대한 보호 정책을 테스트하여 올바른 트래픽이 거부되고 허용되는지 확인합니다.

보안 정책 규칙 재정의 또는 되돌리기

기본 보안 규칙(interzone-default 및 intrazone-default)에는 방화벽이나 Panorama에서 재정의할 수 있는 사전 정의된 설정이 있습니다. 방화벽이 디바이스 그룹에서 기본 규칙을 수신하는 경우 디바이스 그룹 설정을 재정의할 수도 있습니다. 재정의를 수행하는 방화벽 또는 가상 시스템은 해당 구성에 규칙의 로컬 버전을 저장합니다. 재정의할 수 있는 설정은 전체 집합의 하위 집합입니다(다음 표에는 보안 규칙에 대한 하위 집합이 나열되어 있음). 기본 보안 규칙에 대한 자세한 내용은 정책 > 보안을 참조하십시오.

규칙을 무시하려면 방화벽에서 정책 > 보안을 선택하거나 Panorama에서 정책 > 보안 > 기본 규칙을 선택합니다. 이름 열에는 재정의할 수 있는 규칙에 대한 상속 아이콘( )이 표시됩니다. 규칙을 선택한 다음 재정의를 클릭한 후 다음 표에서 설정을 편집합니다.

재정의된 규칙을 사전 정의된 설정 또는 Panorama 디바이스 그룹에서 푸시된 설정으로 되돌리려면 방화벽에서 **Policies** > **Security**를 선택하거나 Panorama에서 **Policies** > 보안 > 기본 규칙을 선택합니다. 이름 열에는 재정의된 값이 있는 규칙에 대한 재정의 아이콘( )이 표시됩니다. 규칙을 선택한 다음 되돌리기를 클릭한 다음 예를 클릭하여 작업을 확인합니다.

기본 보안 규칙을 재정의하는 필드	설명
일반 탭	
이름	규칙을 식별하는 이름은 읽기 전용입니다. 재정의할 수 없습니다.
규칙 유형	규칙 유형은 읽기 전용입니다. 재정의할 수 없습니다.
설명	설명은 읽기 전용입니다. 재정의할 수 없습니다.

기본 보안 규칙을 재정의하는 필드	설명
태그	드롭다운에서 태그를 선택합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구문입니다. 이는 많은 정책을 정의하고 특정 키워드로 태그가 지정된 정책을 보려는 경우에 유용합니다. 예를 들어 특정 보안 정책에 Inbound to DMZ로 태그를 지정하거나 특정 복호화 정책에 Decrypt 또는 No-decrypt라는 단어로 태그를 지정하거나 해당 위치와 연결된 정책에 대해 특정 데이터 센터의 이름을 사용할 수 있습니다.
작업 탭	
액션 설정	규칙과 일치하는 트래픽에 대해 적절한 작업을 선택합니다. • 허용 - (기본값) 트래픽을 허용합니다. • 거부 - 트래픽을 차단하고 방화벽이 거부하는 애플리케이션에 대해 정의된 기본 거부 작업을 적용합니다. 애플리케이션에 대해 기본적으로 정의된 거부 작업을 보려면 **Objects** > **Applications**에서 애플리케이션 세부 정보를 봅니다. • 삭제 - 애플리케이션을 자동으로 삭제합니다. 방화벽은 호스트나 애플리케이션에 TCP 재설정 메시지를 보내지 않습니다. • 클라이언트 재설정 - 클라이언트 측 디바이스에 TCP 재설정 메시지를 보냅니다. • 서버 재설정 - 서버 측 디바이스에 TCP 재설정 메시지를 보냅니다. • 둘 다 재설정 - 클라이언트 측 디바이스와 서버 측 디바이스 모두에 TCP 재설정 메시지를 보냅니다.
프로파일 설정	프로파일 유형 - 보안 규칙에 프로파일 또는 프로파일 그룹을 할당합니다. • 기본 보안 프로파일이 수행하는 검사를 지정하려면 프로파일을 선택한 다음 개별 안티바이러스, 취약점 보호, 안티스파이웨어, **URL** 필터링, 파일 차단, 데이터 필터링, **WildFire** 분석, **SCTP** 보호 및 모바일 네트워크 보호 프로파일 중 하나 이상을 선택합니다. • 개별 프로파일이 아닌 프로파일 그룹을 할당하려면 그룹을 선택한 다음 드롭다운에서 그룹 프로파일을 선택합니다. • 새 프로파일(개체 > 보안 프로파일) 또는 프로파일 그룹을 정의하려면 해당 프로파일 또는 그룹 프로파일의 드롭다운에서 새로 만들기를 클릭합니다.

기본 보안 규칙을 재정의하는 필드	설명

로그 설정	다음 옵션의 조합을 지정합니다.
	• 로그 포워딩 - 로컬 트래픽 로그 및 위협 로그 항목을 Panorama 및 syslog 서버와 같은 원격 대상으로 포워딩하려면 드롭다운에서 로그 포워딩 프로파일을 선택합니다. 보안 프로파일은 위협 로그 항목의 생성을 결정합니다. 새 로그 포워딩 프로파일을 정의하려면 드롭다운에서 프로파일을 선택합니다(개체 > 로그 포워딩 참조).
	• 이 규칙과 일치하는 트래픽에 대한 항목을 로컬 트래픽 로그에 생성하려면 다음 옵션을 선택합니다.
	  • 세션 시작 시 기록 - 세션 시작에 대한 트래픽 로그 항목을 생성합니다(기본적으로 선택됨).
	  • 세션 종료 시 기록 - 세션 종료에 대한 트래픽 로그 항목을 생성합니다(기본적으로 지워짐).
	  트래픽 로그에 세션 시작 또는 세션 종료 항목을 포함하도록 방화벽을 구성하면 삭제 및 거부 항목도 포함됩니다.

응용 및 사용

- 정책 > **Security** > **Policy Optimizer** > 새 앱 뷰어를 클릭한 다음 표시된 앱에서 숫자를 클릭하거나 비교를 클릭합니다.

  인터페이스에서 새 앱 뷰어를 보려면 *SaaS* 인라인 보안 구독이 있어야 합니다. 새 앱 뷰어에는 콘텐츠 제공 애플리케이션 외에 클라우드 제공 애플리케이션이 포함되어 있으며 *SaaS Inline Security* 구독이 없는 경우 클라우드 제공 애플리케이션을 받을 수 없습니다.

- **Policies** > **Security** > **Policy Optimizer** > **Rules Without App Controls**를 클릭한 다음 **Apps Seen**에서 숫자를 클릭하거나 비교를 클릭합니다.
- 정책 > 보안 > 정책 최적화 프로그램 > 사용하지 않은 앱을 클릭한 다음 표시된 앱에서 숫자를 클릭하거나 비교를 클릭합니다.
- 정책 > 보안를 클릭한 다음 표시된 앱에서 숫자를 클릭합니다.

보안 정책 규칙의 사용 탭에서 포트 기반 보안 정책 규칙에서 애플리케이션 기반 보안 정책 규칙으로 마이그레이션하고 사용하지 않은 애플리케이션 및 사용법의 규칙에서 애플리케이션을 제거하는 데 도움이 되는 도구에 액세스하기 위해 표시된 애플리케이션 및 애플리케이션 비교를 할 수도 있습니다.

필드	설명
기간	신청 기간 정보: • 항상 - 규칙의 수명 동안 표시되는 애플리케이션을 표시합니다. • 지난 **7**일 - 지난 7일 동안 본 애플리케이션만 표시합니다. • 지난 **15**일 - 지난 15일 동안 본 애플리케이션만 표시합니다. • 지난 **30**일 - 지난 30일 동안 본 애플리케이션만 표시합니다.
규칙에 따른 앱	규칙에 구성된 애플리케이션 또는 규칙에 구성된 특정 애플리케이션이 없는 경우 모두. 필요에 따라 애플리케이션을 탐색, 추가 및 삭제할 수 있으며 애플리케이션은 규칙에 따라 구성됩니다. 규칙에 따른 앱 옆의 원으로 표시된 숫자는 수를 나타냅니다. 이 위치에서 애플리케이션을 추가하는 것은 보안 정책 규칙 애플리케이션 탭에서 애플리케이션을 추가하는 것과 동일합니다.
표시된 앱	규칙과 일치하는 방화벽에서 보고 허용된 모든 애플리케이션. 표시된 앱 옆에 있는 숫자는 규칙에서 본 애플리케이션의 수를 나타냅니다. • 애플리케이션 - 규칙에 표시된 애플리케이션입니다. 예를 들어 규칙이 웹 브라우징 트래픽을 허용하는 경우(Apps on Rule에서 볼 수 있음) 웹 브라우징으로 식별된 많은 애플리케이션이 있기 때문에 앱 표시 목록에 많은 애플리케이션이 표시될 수 있습니다. • 하위 카테고리 - 애플리케이션의 하위 카테고리입니다. • 위험 - 애플리케이션의 위험 등급입니다. • 최초 확인 - 애플리케이션이 네트워크에서 처음 본 날입니다. • 최종 확인 - 가장 최근에 애플리케이션이 네트워크에서 본 날짜입니다. 최초 확인 및 최종 확인에 대한 측정 단위는 *1*일이므로 규칙을 정의하는 날에는 첫 번째 날과 마지막 날이 같은 날입니다.

필드	설명
	• 트래픽**(30**일**)** - 지난 30일 동안 발생한 트래픽의 양(바이트)입니다. 기간이 길수록 가장 오래된 규칙이 가장 누적된 트래픽을 가질 가능성이 높기 때문에 목록의 맨 위에 남아 있게 됩니다. 이로 인해 새 규칙에서 트래픽이 많이 발생하더라도 새 규칙이 이전 규칙 아래에 나열될 수 있습니다.
표시된 앱 작업	표시된 앱에서 수행할 수 있는 작업: • 복사된 규칙 생성 - 현재 규칙을 복사합니다. 포트 기반 규칙에서 애플리케이션 기반 규칙으로 마이그레이션할 때 먼저 포트 기반 규칙을 복사한 다음 복사를 편집하여 트래픽을 허용하는 애플리케이션 기반 규칙을 생성하십시오. 복사된 규칙은 정책 목록의 포트 기반 규칙 위에 삽입됩니다. 이 마이그레이션 방법을 사용하여 허용하려는 트래픽을 실수로 거부하지 않도록 합니다. 복사된 규칙이 필요한 모든 애플리케이션을 허용하지 않는 경우 뒤따르는 포트 기반 규칙이 허용합니다. 포트 기반 규칙을 모니터링하고 필요에 따라 (복사된) 애플리케이션 기반 규칙을 조정합니다. 애플리케이션 기반 규칙이 원하는 트래픽을 허용하고 원하지 않는 트래픽만 포트 기반 규칙으로 필터링한다고 확신하면 포트 기반 규칙을 안전하게 제거할 수 있습니다. 복사는 **New App Viewer**에서 볼 수 있는 애플리케이션에 유사한 이점을 제공하며, 이를 통해 콘텐츠 제공 애플리케이션뿐만 아니라 새로 식별된 클라우드 애플리케이션을 애플리케이션 및 액세스를 제어할 수 있는 보안 정책 규칙으로 이동할 수 있습니다. 복사된 규칙에 개별적으로, 애플리케이션 그룹 또는 애플리케이션 필터에 애플리케이션을 추가하도록 선택할 수 있습니다. • 이 규칙에 추가(새 앱 뷰어에는 사용할 수 없음) - 표시되는 앱의 애플리케이션을 규칙에 추가합니다. 규칙에 애플리케이션을 추가하면 모든 애플리케이션(포트 기반 규칙)과 일치하도록 구성된 규칙이 지정한 애플리케이션을 허용하는 애플리케이션 기반 규칙으로 변환됩니다(새 애플리케이션 기반 규칙이 포트 기반 규칙을 대체함). 이 규칙은 다른 애플리케이션 기반 규칙과 마찬가지로 추가하지 않은 애플리케이션을 거부합니다. 실수로 애플리케이션을 거부하지 않도록 허용하려는 모든 애플리케이션을 식별하고 규칙에 추가하십시오.

필드	설명
	• 기존 규칙에 추가 - 표시된 앱의 애플리케이션을 기존 애플리케이션 기반(App-ID) 규칙에 추가합니다. 예를 들어, 이를 통해 포트 기반 규칙에서 App-ID 기반 규칙을 복사한 다음 나중에 포트 기반 규칙에 표시되는 더 많은 애플리케이션을 해당 App-ID 규칙에 추가할 수 있습니다. 새로운 앱 뷰어에 표시되는 애플리케이션의 경우, 새로운 앱이 발견되면 새로 식별된 클라우드 기반 및 콘텐츠 기반 애플리케이션을 합리적인 보안 정책 규칙으로 구성할 수 있습니다. 개별적으로, 애플리케이션 그룹 또는 애플리케이션 필터에서 기존 규칙에 애플리케이션 추가를 선택할 수 있습니다. • 사용 일치(새 앱 뷰어에서는 사용할 수 없음) - 표시되는 모든 앱을 규칙으로 이동합니다(사용 일치 후 규칙의 앱 아래에 나열됨). 규칙이 나열된 모든 애플리케이션을 허용해야 한다고 확신하는 경우 **Match Usage**가 매우 편리합니다. 그러나 나열된 모든 애플리케이션이 네트워크에서 허용하려는 애플리케이션인지 확인해야 합니다. 규칙(예: 웹 브라우징을 허용하는 규칙)에 많은 애플리케이션이 있는 경우 규칙을 복사하고 애플리케이션 기반 규칙으로 전환하는 것이 좋습니다. 사용 일치는 잘 알려진 애플리케이션이 있는 간단한 규칙에 적합합니다. 예를 들어 포트 22에 대한 포트 기반 규칙이 SSH 트래픽만 본 경우(해당 사항이 모두 표시되어야 함) 사용 일치를 사용하는 것이 안전합니다. 복사, 규칙에 추가 및 기존 규칙에 앱 추가 대화 상자는 애플리케이션이 중단되지 않도록 하고 규칙에 복사하거나 추가하는 애플리케이션과 관련된 개별 애플리케이션을 포함하여 규칙을 미래에 대비할 수 있도록 합니다.

복사된 규칙 생성 > 애플리케이션
 	
이 규칙에 추가
 	
기존 규칙에 추가 > 애플리케이션
	애플리케이션을 선택한 다음 개별 애플리케이션을 복사하거나 규칙에 추가합니다.
	• 이름(기존 규칙에 앱 복사 및 추가 대화 상자에만 해당).
	  • 복사: 복사된 새 규칙의 이름을 입력합니다.
	  • 기존 규칙에 앱 추가: 애플리케이션을 추가할 규칙을 선택하거나 규칙 이름을 입력합니다.
	• 애플리케이션:
	  • 컨테이너 앱 추가(기본값): 컨테이너의 모든 앱, 규칙에 표시된 앱 및 규칙에 표시되지 않은 컨테이너 앱을 선택합니

필드	설명
	다. 컨테이너에 대해 표시되는 향후 앱은 규칙과 일치하므로 앱이 변경될 때 미래에 대비할 수 있습니다. • 표시된 특정 앱 추가: 규칙에서 실제로 본 앱만 선택합니다. (컨테이너 앱과 기능 앱을 수동으로 선택할 수도 있습니다.) • 애플리케이션: • 규칙에 표시된 선택된 애플리케이션은 녹색으로 강조 표시됩니다. • 회색으로 강조 표시된 컨테이너 앱과 아래에 나열된 기능적 애플리케이션. • 규칙에 표시되었지만 애플리케이션 및 사용에서 선택되지 않은 컨테이너의 기능성 애플리케이션(강조 표시되지 않음). • 규칙에 표시되지 않은 컨테이너의 기능성 애플리케이션(이탤릭체). • 규칙에서 애플리케이션이 마지막으로 본 날짜입니다. • 종속 애플리케이션: • 선택한 애플리케이션을 실행하는 데 필요한 애플리케이션입니다. • 종속 항목 - 선택한 애플리케이션을 실행하는 데 필요한 종속 애플리케이션입니다. • 필수 - 종속 애플리케이션이 필요한 애플리케이션입니다. (종종 종속 애플리케이션에 종속 애플리케이션이 있는 경우가 있습니다.)
복사된 규칙 생성 > 애플리케이션 그룹 기존 규칙에 추가 > 애플리케이션 그룹	애플리케이션을 선택한 다음 복사된 규칙 생성 또는 기존 규칙에 앱 추가 대화 상자에서 애플리케이션 그룹의 규칙에 애플리케이션을 복사하거나 추가합니다. • 복사된 규칙 이름 또는 이름: • 복사된 규칙 이름: 복사된 새 규칙의 이름을 입력합니다. • 이름: 애플리케이션 그룹을 추가할 규칙을 선택하거나 규칙 이름을 입력합니다. • 정책 작업(복사된 규칙만 해당) - 복사된 규칙의 트래픽을 허용할지 또는 거부할지 선택합니다.

필드	설명

	• 애플리케이션 그룹에 추가 - 기존 그룹을 선택하거나 새 이름을 입력하여 새 애플리케이션 그룹을 생성합니다.
	• 애플리케이션:
	  • 컨테이너 앱 추가(기본값): 컨테이너의 모든 앱, 규칙에 표시된 앱 및 규칙에 표시되지 않은 컨테이너 앱을 선택합니다. 컨테이너에 대해 표시되는 향후 앱은 규칙과 일치하므로 앱이 변경될 때 미래에 대비할 수 있습니다.
	  • 표시된 특정 앱 추가: 규칙에서 실제로 본 앱만 선택합니다. (컨테이너 앱과 기능 앱을 수동으로 선택할 수도 있습니다.)
	• 애플리케이션:
	  • 규칙에 표시된 선택된 애플리케이션은 녹색으로 강조 표시됩니다.
	  • 회색으로 강조 표시된 컨테이너 앱과 아래에 나열된 기능적 애플리케이션.
	  • 규칙에 표시되었지만 애플리케이션 및 사용에서 선택되지 않은 컨테이너의 기능성 애플리케이션(강조 표시되지 않음).
	  • 규칙에 표시되지 않은 컨테이너의 기능성 애플리케이션(이탤릭체).
	  • 규칙에서 애플리케이션이 마지막으로 본 날짜입니다.
	• 종속 애플리케이션:
	  • 선택한 애플리케이션을 실행하는 데 필요한 애플리케이션입니다.
	  • 종속 항목 - 선택한 애플리케이션을 실행하는 데 필요한 종속 애플리케이션입니다.
	  • 필수 - 종속 애플리케이션이 필요한 애플리케이션입니다. (종종 종속 애플리케이션에 종속 애플리케이션이 있는 경우가 있습니다.)

복사된 규칙 생성 > 애플리케이션 필터	애플리케이션을 선택한 다음 복사된 규칙 생성 또는 기존 규칙에 앱 추가 대화 상자의 애플리케이션 필터에서 규칙에 애플리케이션을 복사하거나 추가합니다.

필드	설명

기존 규칙에 추가 > 애플리케이션 필터	• 복사된 규칙 이름 또는 기존 규칙 이름:
	  • 복사된 규칙 이름: 복사된 새 규칙의 이름을 입력합니다.
	  • 기존 규칙 이름: 애플리케이션 필터를 추가할 규칙을 선택하거나 규칙 이름을 입력합니다.
	• 정책 작업(복사된 규칙만 해당) - 복사된 규칙의 트래픽을 허용할지 또는 거부할지 선택합니다.
	• 애플리케이션 필터 이름 - 기존 필터를 선택하거나 새 이름을 입력하여 새 애플리케이션 필터를 생성합니다.
	애플리케이션 필터는 개체 > 애플리케이션 필터와 동일한 방식으로 작동합니다(애플리케이션 필터 생성 참조). 클라우드 기반(SaaS Inline Security 구독 포함) 및 콘텐츠 기반 애플리케이션을 필터링하고 기존 또는 새 필터에 추가할 수 있습니다.

보안 정책 최적화

- 정책 > 보안 > 정책 최적화 프로그램

정책 > **Security** > **Policy Optimizer**는 다음을 표시합니다.

- 새 앱 뷰어 - 방화벽에 SaaS 보안 구독이 있는 경우 Application Control Engine에서 다운로드한 새 클라우드 애플리케이션입니다.
- 앱 제어가 없는 규칙 - 애플리케이션이 **any**로 설정된 규칙이므로 애플리케이션 기반 규칙으로 변환할 포트 기반 규칙을 식별할 수 있습니다.
- 미사용 앱 - 규칙과 일치하지 않는 애플리케이션이 포함된 규칙입니다.
- 보안 서비스를 위한 로그 전달 - 로그 전달 프로파일을 여러 규칙에 일괄적으로 연결하고 분석을 위한 IoT Security 및 저장을 위한 Cortex Data Lake와 같은 서비스에 로그를 보냅니다.

  이 기능을 사용하기 전에 먼저 보안 정책 규칙을 구성하여 로그를 전달하고 향상된 애플리케이션 로깅으로 로깅 서비스를 활성화해야 합니다.
- 규칙 사용 - 여러 기간 동안 사용되지 않은 규칙을 포함하여 여러 기간 동안의 규칙 사용 정보입니다.

필드	설명
이름	보안 정책 규칙의 이름입니다.
서비스	보안 정책 규칙과 연결된 모든 서비스.

필드	설명
트래픽(바이트, 30일)	트래픽**(30일)** - 지난 30일 동안 발생한 트래픽의 양(바이트)입니다. 기간이 길수록 가장 오래된 규칙이 가장 누적된 트래픽을 가질 가능성이 높기 때문에 목록의 맨 위에 남아 있게 됩니다. 이로 인해 새 규칙에서 트래픽이 많이 발생하더라도 새 규칙이 이전 규칙 아래에 나열될 수 있습니다.
허용된 앱	규칙이 허용하는 애플리케이션입니다. 규칙에 대한 애플리케이션을 추가 및 삭제할 수 있는 애플리케이션 대화 상자를 엽니다.
애플리케이션	(새 앱 뷰어만 해당) 규칙이 허용하는 애플리케이션입니다.
표시된 앱	규칙에 표시된 애플리케이션 수입니다. 번호를 클릭하여 규칙에 구성된 애플리케이션을 규칙에 표시된 애플리케이션과 비교하고 애플리케이션을 수정할 수 있는 애플리케이션 및 사용 대화 상자를 엽니다.
신규 앱이 없는 날	규칙에 마지막으로 신규 애플리케이션이 표시된 이후의 일 수입니다.
비교	애플리케이션 및 사용 대화 상자를 열어 규칙에 구성된 애플리케이션을 규칙에 표시된 애플리케이션과 비교하고 규칙을 수정합니다.
(규칙 사용법) 마지막 적중	트래픽이 규칙과 일치한 가장 최근 시간입니다.
(규칙 사용법) 첫 번째 적중	트래픽이 규칙과 처음 일치한 시간입니다.
(규칙 사용법) 적중 횟수	트래픽이 규칙과 일치한 횟수입니다.
수정	규칙이 마지막으로 수정된 날짜 및 시간입니다.
생성	규칙이 생성된 날짜 및 시간입니다.
기간	데이터가 표시되는 기간(일수)입니다.
용법	표시:

필드	설명
	• 트래픽이 규칙과 일치하는지(사용된 규칙) 또는 일치하지 않는지(사용되지 않은 규칙)에 관계없이 지정된 기간 동안 방화벽의 모든(all) 규칙입니다. • 지정된 기간 동안 트래픽이 일치하지 않는 사용되지 않은 규칙입니다. • 지정된 기간 동안 트래픽이 일치하는 사용된 규칙입니다.
지난 *xx*일 동안 재설정된 제외 규칙	지정된 일 수(1-5,000일) 내에 **Reset Rule Hit Counter**에 대한 규칙을 표시하지 않습니다. 예를 들어, 이를 통해 트래픽을 일치시킬 시간이 없었을 수 있는 새로운 규칙을 제외하면서 특정 기간 동안 트래픽과 일치하지 않은 이전 규칙을 검사할 수 있습니다.
재설정 날짜	규칙의 적중 카운터가 재설정된 마지막 날짜입니다.
로그 전달 프로파일(보안 서비스에 대한 로그 전달만 해당)	표시: • 모두 – 로그 전달 프로파일이 연결되어 있는지 여부에 관계없이 방화벽에 대한 규칙입니다. • 없음 – 로그 전달 프로파일이 연결되지 않은 규칙입니다. • **<profile-name>** – 특정 로그 전달 프로파일이 연결된 규칙입니다.
로그 전달 프로파일 첨부(보안 서비스에 대한 로그 전달만 해당)	보안 정책 규칙을 선택한 후 이 화면 하단 옵션을 사용하여 대화상자를 열고 선택한 규칙에 연결할 로그 전달 프로파일을 선택합니다. • 로그 전달 프로파일 - 선택한 규칙에 연결할 로그 전달 프로파일을 선택합니다. • 향상된 **IoT** 로깅 활성화 – 선택한 로그 전달 프로파일이 향상된 애플리케이션 로그(EAL)를 아직 전달하지 않은 경우 선택합니다. 이렇게 하면 선택한 로그 전달 프로파일에서 EAL 전달이 활성화됩니다.

정책 > NAT

방화벽에서 레이어 3 인터페이스를 정의하는 경우 NAT(Network Address Translation) 정책을 구성하여 소스 또는 대상 IP 주소와 포트가 공용 및 개인 주소와 포트 간에 변환되는지의 여부를 지정할 수 있습니다. 예를 들어 개인 소스 주소는 내부 영역(신뢰할 수 있는)에서 공개 영역(신뢰할 수 없는)으로 전송되는 트래픽에서 공용 주소로 변환될 수 있습니다. NAT는 가상 와이어 인터페이스에서도 지원됩니다.

NAT 규칙은 소스 및 대상 영역, 소스 및 대상 주소, 애플리케이션 서비스(예: HTTP)를 기반으로 합니다. 보안 정책과 마찬가지로 NAT 정책 규칙은 들어오는 트래픽에 대해 순서대로 비교되며 트래픽과 일치하는 첫 번째 규칙이 적용됩니다.

필요에 따라 모든 공용 주소에 대한 트래픽이 방화벽으로 라우팅되도록 로컬 라우터에 고정 경로를 추가합니다. 트래픽을 다시 개인 주소로 라우팅하기 위해 방화벽의 수신 인터페이스에 정적 경로를 추가해야 할 수도 있습니다.

다음 표에서는 NAT 및 NPTv6(IPv6-to-IPv6 네트워크 프리픽스 변환) 설정에 대해 설명합니다.

- NAT 정책 일반 탭
- NAT 소스 패킷 탭
- NAT 변환 패킷 탭
- NAT 능동형/능동형 HA 바인딩 탭
- (Panorama만 해당) NAT 대상 탭

더 찾고 계십니까?

NAT 참조

NAT 정책 일반 탭

- 정책 > NAT > 일반

일반 탭을 선택하여 NAT 또는 NPTv6 정책의 이름과 설명을 구성합니다. 많은 정책이 존재할 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수 있습니다. 생성 중인 NAT 정책 유형을 선택합니다. 이는 **Original Packet** 및 **Translated Packet** 탭에서 사용할 수 있는 필드에 영향을 줍니다.

NAT 규칙 - 일반 설정	설명
이름	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	규칙에 대한 설명을 입력합니다(최대 1024자).

NAT 규칙 - 일반 설정	설명
태그	정책에 태그를 지정하려면 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구문입니다. 이는 많은 정책을 정의하고 특정 키워드로 태그가 지정된 정책을 보려는 경우에 유용합니다.
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그를 기반으로 규칙을 그룹화할 수 있습니다.
NAT 유형	번역 유형 지정: • **ipv4** - IPv4 주소 간의 변환. • **nat64** - IPv6과 IPv4 주소 간의 변환. • **nptv6** - IPv6 프리픽스 간의 변환. 단일 NAT 규칙에서 IPv4 및 IPv6 주소 범위를 결합할 수 없습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. 감사 코멘트 아카이브 CSV 형식을 내보낼 수 있습니다.

NAT 소스 패킷 탭

- 정책 > NAT > 소스 패킷

원래 패킷 탭을 선택하여 방화벽이 변환할 패킷의 소스 및 대상 영역을 정의하고 선택적으로 대상 인터페이스와 서비스 유형을 지정합니다. 동일한 유형의 여러 소스 및 대상 영역을 구성할 수 있으며 특정 네트워크 또는 특정 IP 주소에 규칙을 적용할 수 있습니다.

NAT 규칙 - 원래 패킷 설정	설명
소스 영역/대상 영역	소스(비 NAT) 패킷에 대해 하나 이상의 소스 및 대상 영역을 선택합니다(기본값은 모두임). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을 참조하세요.

NAT 규칙 - 원래 패킷 설정	설명
	관리를 단순화하기 위해 여러 영역을 지정할 수 있습니다. 예를 들어 여러 내부 NAT 주소가 동일한 외부 IP 주소로 지정되도록 설정을 구성할 수 있습니다.
대상 인터페이스	방화벽이 변환하는 패킷의 대상 인터페이스를 지정합니다. 네트워크가 IP 주소 풀이 다른 두 ISP에 연결된 경우 대상 인터페이스를 사용하여 IP 주소를 다르게 변환할 수 있습니다.
서비스	방화벽이 소스 또는 대상 주소를 변환하는 서비스를 지정합니다. 새 서비스 그룹을 정의하려면 개체 > 서비스 그룹을 선택합니다.
발신지 주소/목적지 주소	방화벽이 변환할 소스 및 대상 주소 조합을 지정합니다. NPTv6의 경우 소스 주소 및 대상 주소에 대해 구성된 프리픽스는 xxxx:xxxx::/yy 형식이어야 합니다. 주소는 정의된 인터페이스 식별자(호스트) 부분을 가질 수 없습니다. 지원되는 프리픽스 길이의 범위는 /32 ~ /64입니다.

NAT 변환 패킷 탭

- 정책 > NAT > 변환된 패킷

소스 주소 변환의 경우 변환된 패킷 탭을 선택하여 소스, 주소 및 소스가 변환되는 포트에서 수행할 변환 유형을 결정하십시오.

또한 내부 호스트에 대해 대상 주소 변환을 활성화하여 공용 IP 주소에서 액세스할 수 있도록 할 수 있습니다. 이 경우 내부 호스트의 **Original Packet** 탭에서 공개 소스 주소와 목적지 주소를 정의하고 **Translated Packet** 탭에서 **Static IP** 또는 **Dynamic IP(**세션 배포 포함**)**를 구성하고 **Translated Address**를 입력합니다. 그런 다음 공용 주소에 액세스하면 내부 호스트의 내부(목적지) 주소로 변환됩니다.

NAT 규칙 - 변환된 패킷 설정	설명
소스 주소 번역	변환 유형(동적 또는 고정 주소 풀)을 선택한 다음 소스 주소가 변환될 IP 주소 또는 주소 범위(주소1-주소2)(변환된 주소)를 입력합니다. 주소 범위의 크기는 주소 풀 유형에 따라 제한됩니다. • 동적 **IP** 및 포트 - 주소 선택은 소스 IP 주소의 해시를 기반으로 합니다. 주어진 소스 IP 주소에 대해 방화벽은 모든 세션에 대해 동일한 변환된 소스 주소를 사용합니다. DIPP(동적 IP 및 포트) 소스 NAT는 NAT 풀의 각 IP 주소에서 약

NAT 규칙 - 변환된 패킷 설정	설명
	64,000개의 동시 세션을 지원합니다. 일부 모델은 단일 IP가 64,000개 이상의 동시 세션을 호스트할 수 있도록 하는 초과 구독을 지원합니다. Palo Alto Networks® DIPP NAT는 사용 가능한 IP 주소 및 포트 수에서 지원하는 것보다 더 많은 NAT 세션을 지원합니다. 초과 구독을 통해, 대상 IP 주소가 고유한 경우 방화벽은 PA-220, PA-820, PA-850, VM-50, VM-300 및 VM-1000-HV 방화벽에서 IP 주소와 포트 조합을 동시에 두 번 그리고 초과 구독을 통해 방화벽은 PA-5220 방화벽 및 PA-3200 시리즈 방화벽에서 IP 주소 및 포트 조합을 동시에 4번, PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-500, 및 VM-700 방화벽에서 동시에 8번 사용할 수 있습니다. • 동적 **IP** - 지정된 범위에서 사용 가능한 다음 주소로 변환하지만 포트 번호는 변경되지 않습니다. 최대 32,000개의 연속 IP 주소가 지원됩니다. 동적 IP 풀에는 여러 서브넷이 포함될 수 있으므로 내부 네트워크 주소를 두 개 이상의 개별 퍼블릭 서브넷으로 변환할 수 있습니다. • **Advanced(**동적 **IP/**포트 폴백**)** - 이 옵션을 사용하여 IP 및 포트 변환을 수행하고 기본 풀에 주소가 부족한 경우 사용되는 폴백 풀을 생성합니다. 변환된 주소 옵션 또는 인터페이스 주소 옵션을 사용하여 풀에 대한 주소를 정의할 수 있습니다. 후자의 옵션은 IP 주소를 동적으로 수신하는 인터페이스를 위한 것입니다. 대체 풀을 생성할 때 주소가 기본 풀의 주소와 겹치지 않는지 확인하십시오.
소스 주소 번역(계속)	• 고정 **IP** - 변환에 항상 동일한 주소가 사용되며 포트는 변경되지 않습니다. 예를 들어 소스 범위가 192.168.0.1~192.168.0.10이고 변환 범위가 10.0.0.1~10.0.0.10인 경우 주소 192.168.0.2는 항상 10.0.0.2로 변환됩니다. 주소 범위는 사실상 무제한입니다. NPTv6 소스 주소 변환에는 고정 **IP** 변환을 사용해야 합니다. NPTv6의 경우 **Translated Address**에 대해 구성된 프리픽스는 xxxx:xxxx::/yy 형식이어야 하며 주소는 정의된 인터페이스 식별자(호스트) 부분을 가질 수 없습니다. 지원되는 프리픽스 길이의 범위는 /32 ~ /64입니다. • 없음 - 번역이 수행되지 않습니다.
양방향	(선택 사항) 방화벽이 구성한 변환의 반대 방향으로 해당 변환(NAT 또는 NPTv6)을 생성하도록 하려면 고정 **IP** 소스 주소 변환에 대해 양방향 변환을 활성화합니다. 양방향 변환을 활성화하는 경우 양방향 트래픽을 제어하기 위한 보안 정책이 있는지 확인해야 합니다. 이러한 정책이 없으면 양방향 기능을 통해 패킷이 양방향으로 자동 변환될 수 있습니다.

NAT 규칙 - 변환된 패킷 설정	설명
목적지 주소 번역	방화벽이 대상 NAT를 수행하도록 다음 옵션을 구성합니다. 일반적으로 대상 NAT를 사용하여 전자 메일 서버와 같은 내부 서버가 공용 네트워크에서 액세스할 수 있도록 합니다.
번역 유형 및 번역 주소	방화벽이 대상 주소에서 수행하는 변환 유형을 선택하십시오. • 없음(기본값) • 고정 **IP** - 변환된 주소를 IP 주소 또는 IP 주소 범위로 입력하고 원래 대상 주소와 포트 번호가 변환되는 변환된 포트 번호(1 ~ 65535)를 입력합니다. 변환된 포트 필드가 비어 있으면 대상 포트가 변경되지 않습니다. NPTv6의 경우 대상 프리픽스 번역된 주소에 대해 구성된 프리픽스는 xxxx:xxxx::/yy 형식이어야 합니다. 주소는 정의된 인터페이스 식별자(호스트) 부분을 가질 수 없습니다. 지원되는 프리픽스 길이의 범위는 /32 ~ /64입니다. *NPTv6*은 엄격하게 프리픽스 변환이므로 변환된 포트는 *NPTv6*에 대해 지원되지 않습니다. 포트 및 호스트 주소 섹션은 변경되지 않고 단순히 포워딩됩니다. *IPv4*용 고정 *IP* 변환을 사용하면 ***DNS*** 재작성을 활성화할 수도 있습니다*(*아래 설명 참조*)*. • 동적 **IP(**세션 배포 포함**)** - FQDN, 주소 개체 또는 방화벽이 변환된 주소를 선택하는 주소 그룹인 변환된 주소를 선택하거나 입력합니다. DNS 서버가 FQDN에 대해 둘 이상의 주소를 반환하거나 주소 개체 또는 주소 그룹이 둘 이상의 IP 주소로 변환되는 경우 방화벽은 지정된 세션 배포 방법을 사용하여 해당 주소 간에 세션을 배포합니다.
세션 분배 방식	대상 NAT 변환을 동적 **IP(**세션 배포 포함**)**로 선택하면 대상 변환 주소(FQDN, 주소 개체 또는 주소 그룹)가 둘 이상의 주소로 해석될 수 있습니다. 보다 균형 잡힌 세션 배포를 제공하기 위해 방화벽이 이러한 주소 간에 세션을 배포(할당)하는 방법을 선택할 수 있습니다. • 라운드 로빈 - (기본값) 새 세션을 IP 주소에 순환 순서로 할당합니다. 환경에서 다른 배포 방법 중 하나를 선택하도록 지시하지 않는 한 이 방법을 사용하십시오. • 소스 **IP** 해시 - 소스 IP 주소의 해시를 기반으로 새 세션을 할당합니다. 단일 소스 IP 주소에서 들어오는 트래픽이 있는 경우 소스 **IP** 해시가 아닌 다른 방법을 선택하십시오.

NAT 규칙 - 변환된 패킷 설정	설명
	• **IP Modulo** - 방화벽은 들어오는 패킷의 소스 및 대상 IP 주소를 고려합니다. 방화벽은 XOR 연산과 모듈로 연산을 수행합니다. 결과는 방화벽이 새 세션을 할당하는 IP 주소를 결정합니다. • **IP** 해시 - 소스 및 대상 IP 주소의 해시를 사용하여 새 세션을 할당합니다. • 최소 세션 - 동시 세션이 가장 적은 IP 주소에 새 세션을 할당합니다. 단기 세션이 많은 경우 최소 세션을 사용하면 세션을 보다 균형 있게 분배할 수 있습니다.
DNS 재작성 활성화	PAN-OS 9.0.2 이상 9.0 릴리스에서 대상 NAT 정책 규칙 유형이 **ipv4**이고 대상 주소 변환 유형이 고정 **IP**인 경우 **DNS** 재작성 활성화 옵션을 사용할 수 있습니다. 대상 NAT를 사용하고 방화벽의 한 쪽에서 DNS 서비스를 사용하여 방화벽의 다른 쪽에서 클라이언트에 대한 FQDN을 확인하는 경우 DNS 재작성을 활성화할 수 있습니다. DNS 응답이 방화벽을 통과할 때 방화벽은 DNS 응답이 NAT 정책 규칙에서 일치하는 원래 대상 주소 또는 변환된 대상 주소를 기준으로 DNS 응답의 IP 주소를 다시 씁니다. 단일 NAT 정책 규칙은 방화벽이 규칙과 일치하는 패킷에 대해 NAT를 수행하고 규칙과 일치하는 DNS 응답의 IP 주소에 대해 NAT를 수행하도록 합니다. 방화벽이 NAT 규칙(역방향 또는 순방향)과 관련하여 DNS 응답의 IP 주소에 대해 NAT를 수행하는 방법을 지정해야 합니다. • **reverse** - (기본값) 패킷이 규칙의 변환된 대상 주소와 일치하는 DNS 응답인 경우 규칙이 사용하는 역변환을 사용하여 DNS 응답을 변환합니다. 예를 들어 규칙이 1.1.1.10을 192.168.1.10으로 변환하면 방화벽은 192.168.1.10의 DNS 응답을 1.1.1.10으로 다시 씁니다. • **forward** - 패킷이 규칙의 원래 대상 주소와 일치하는 DNS 응답인 경우 규칙에서 사용하는 것과 동일한 변환을 사용하여 DNS 응답을 변환합니다. 예를 들어 규칙이 1.1.1.10을 192.168.1.10으로 변환하면 방화벽은 1.1.1.10의 DNS 응답을 192.168.1.10으로 다시 씁니다.

NAT 능동형/능동형 HA 바인딩 탭

- 정책 > NAT > 능동형/능동형 HA 바인딩

능동형/능동형 HA 바인딩 탭은 방화벽이 고가용성(HA) 능동형/능동형 구성에 있는 경우에만 사용할 수 있습니다. 이 구성에서는 각 소스 NAT 규칙(고정 또는 동적 NAT)을 디바이스 ID 0 또는 디바이스 ID 1에 바인딩해야 합니다. 각 대상 NAT 규칙을 디바이스 ID **0**, 디바이스 ID **1**, 둘 다(디바이스 ID 0 및 디바이스 ID 1) 또는 활성-기본 방화벽에 바인딩해야 합니다.

다음과 같이 NAT 규칙을 HA 방화벽에 바인딩하려면 능동형/능동형 **HA** 바인딩 설정을 선택합니다.

- **0** - HA 디바이스 ID가 0인 방화벽에 NAT 규칙을 바인딩합니다.
- **1** - NAT 규칙을 HA 디바이스 ID가 1인 방화벽에 바인딩합니다.

- 둘 다 - HA 디바이스 ID가 0인 방화벽과 HA 디바이스 ID가 1인 방화벽 모두에 NAT 규칙을 바인딩합니다. 이 설정은 유동 IP 또는 유동 IP 및 포트 NAT를 지원하지 않습니다.
- 기본 - HA 활성-기본 상태에 있는 방화벽에 NAT 규칙을 바인딩합니다. 이 설정은 유동 IP 또는 유동 IP 및 포트 NAT를 지원하지 않습니다.

일반적으로 두 HA 피어에 고유한 NAT IP 주소 풀이 있는 경우 디바이스별 NAT 규칙을 구성합니다.

방화벽이 새 세션을 생성할 때 HA 바인딩은 세션이 일치할 수 있는 NAT 규칙을 결정합니다. 규칙이 일치하려면 바인딩에 세션 소유자가 포함되어야 합니다. 세션 설정 방화벽은 NAT 규칙 일치를 수행하지만 세션은 세션 소유자에게 바인딩되고 규칙 중 하나에 따라 변환되는 NAT 규칙과 비교됩니다. 디바이스별 규칙의 경우 방화벽은 세션 소유자에게 바인딩되지 않은 모든 NAT 규칙을 건너뜁니다. 예를 들어 디바이스 ID가 1인 방화벽이 세션 소유자이고 세션 설정 방화벽이라고 가정합니다. 디바이스 ID 1이 세션을 NAT 규칙과 일치시키려고 할 때 디바이스 ID 0에 바인딩된 모든 규칙을 무시합니다.

한 피어가 실패하면 두 번째 피어는 NAT 변환을 포함하여 실패한 피어에서 동기화된 세션에 대한 트래픽을 계속 처리합니다. Palo Alto Networks는 두 번째 디바이스 ID에 바인딩된 중복 NAT 규칙을 생성할 것을 권장합니다. 따라서 동일한 소스 변환 주소와 동일한 대상 변환 주소를 가진 두 개의 NAT 규칙이 있습니다. 하나의 규칙은 각 디바이스 ID에 바인딩됩니다. 이 구성을 통해 HA 피어는 새 세션 설정 작업을 수행하고 디바이스 ID에 바인딩된 NAT 규칙에 대해 NAT 규칙 일치를 수행할 수 있습니다. 중복 NAT 규칙이 없으면 작동하는 피어가 NAT 정책 일치를 수행하려고 시도하지만 세션은 방화벽의 자체 디바이스별 규칙과 일치하지 않으며 방화벽은 디바이스 ID에 바인딩되지 않은 다른 모든 NAT 규칙을 건너뜁니다.

더 찾고 계십니까**?**

능동형/능동형 HA 모드의 NAT 참조

NAT 대상 탭

- (Panorama 전용) 정책 > **NAT** > **Target**

대상 탭을 선택하여 정책 규칙을 푸시할 디바이스 그룹의 관리 방화벽을 선택합니다. 관리 방화벽을 선택하거나 태그를 지정하여 푸시할 관리 방화벽을 지정할 수 있습니다. 또한 지정된 방화벽을 제외한 모든 관리 방화벽에 푸시하도록 정책 규칙 대상을 구성할 수 있습니다.

NAT 규칙 - 대상 설정	설명
모두(모든 디바이스를 대상으로 함)	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스	정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그	지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.

NAT 규칙 - 대상 설정	설명
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > QoS

QoS 정책 규칙을 추가하여 특정 QoS 처리를 받는 트래픽을 정의하고 할당된 서비스 클래스가 QoS 사용 인터페이스를 종료할 때 연결된 규칙과 일치하는 모든 트래픽에 적용되도록 지정하기 위해 각 QoS 정책 규칙에 대해 QoS 클래스를 할당합니다.

Panorama에서 방화벽으로 푸시된 QoS 정책 규칙은 주황색으로 표시되며 방화벽 수준에서 편집할 수 없습니다.

또한 방화벽이 QoS를 제공하도록 완전히 활성화하려면 다음을 수행하십시오.

- 서비스의 각 QoS 클래스에 대한 대역폭 제한을 설정합니다(QoS 프로파일을 추가하거나 수정하려면 네트워크 > 네트워크 프로파일 > QoS 선택).
- 인터페이스에서 QoS를 활성화합니다(네트워크 > QoS 선택).

전체 QoS 워크플로, 개념 및 사용 사례는 서비스 품질을 참조하십시오.

새 규칙을 추가하거나 기존 규칙을 복사한 후 다음 필드를 정의합니다.

QoS 정책 규칙 설정	
일반 탭	
이름	규칙을 식별할 이름을 입력합니다(최대 63자). 이름은 대/소문자에 민감하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	선택적 설명을 입력합니다.
태그	정책에 태그를 지정해야 하는 경우 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 DMZ에 대한 인바운드와 특정 보안 정책에 태그를 지정하거나, 복호화 및 복호화 금지라는 단어로 정책을 복호화하거나 해당 위치와 관련된 정책에 특정 데이터 센터의 이름을 사용할 수 있습니다.
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화할 수 있습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.

QoS 정책 규칙 설정	
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. 감사 코멘트 아카이브를 CSV 형식으로 내보낼 수 있습니다.
소스 탭	
소스 영역	하나 이상의 소스 영역을 선택합니다(기본값은 **any**). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어).
소스 주소	식별된 애플리케이션을 재정의할 수 있는 소스 IPv4 또는 IPv6 주소 조합을 지정합니다. 특정 주소를 선택하려면 드롭다운에서 선택을 선택한 후 다음 중 하나를 수행합니다. • 사용 가능 열에서 해당 주소  및/또는 주소 그룹  옆에 있는 이 옵션을 선택한 다음 추가를 클릭하여 선택 항목을 선택된 열에 추가합니다. • 검색 필드에 이름의 처음 몇 글자를 입력하면 해당 문자로 시작하는 모든 주소와 주소 그룹이 나열됩니다. 목록에서 항목을 선택하면 사용 가능 열에서 이 옵션이 활성화됩니다. 필요한 만큼 이 프로세스를 반복한 다음 추가를 클릭합니다. • 네트워크 마스크가 있거나 없는 하나 이상의 IP 주소(한 줄에 하나씩)를 입력합니다. 일반적인 형식: <*ip_address*>/<*mask*> • 주소를 제거하려면 주소를 선택한 다음(선택된 열) 삭제를 클릭하거나 모두를 선택하여 모든 주소와 주소 그룹을 지웁니다. 이 정책이나 다른 정책에서 사용할 수 있는 새 주소를 추가하려면 새 주소를 클릭합니다. 새 주소 그룹을 정의하려면 개체 > 주소 그룹을 선택합니다.
소스 사용자	QoS 정책을 적용할 소스 사용자 및 그룹을 지정합니다.
무효	이 탭에 지정된 정보가 일치하지 않는 경우 정책을 적용하려면 이 옵션을 선택합니다.
대상 탭	
목적지 영역	하나 이상의 대상 영역을 선택합니다(기본값은 **any**). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어).

QoS 정책 규칙 설정	
목적지 주소	식별된 애플리케이션을 재정의할 수 있는 소스 IPv4 또는 IPv6 주소 조합을 지정합니다. 특정 주소를 선택하려면 드롭다운에서 선택을 선택한 후 다음 중 하나를 수행합니다. • 사용 가능 열에서 해당 주소  및/또는 주소 그룹  옆에 있는 이 옵션을 선택한 다음 선택 항목을 선택 열에 추가합니다. • 검색 필드에 이름의 처음 몇 글자를 입력하면 해당 문자로 시작하는 모든 주소와 주소 그룹이 나열됩니다. 목록에서 항목을 선택하면 사용 가능 열에서 이 옵션이 활성화됩니다. 필요한 만큼 이 프로세스를 반복한 다음 추가를 클릭합니다. • 네트워크 마스크가 있거나 없는 하나 이상의 IP 주소(한 줄에 하나씩)를 입력합니다. 일반적인 형식은 <*ip_address*>/<*mask*>입니다. • 주소를 제거하려면 주소를 선택한 다음(선택된 열) 삭제를 클릭하거나 모두를 선택하여 모든 주소와 주소 그룹을 지웁니다. 이 정책이나 다른 정책에서 사용할 수 있는 새 주소를 추가하려면 새 주소를 클릭합니다.
무효	이 탭에 지정된 정보가 일치하지 않는 경우 정책을 적용하려면 이 옵션을 선택합니다.
애플리케이션 탭	
애플리케이션	QoS 규칙에 대한 특정 애플리케이션을 선택합니다. 새 애플리케이션 또는 애플리케이션 그룹을 정의하려면 개체 > 애플리케이션을 선택합니다. 애플리케이션에 여러 기능이 있는 경우 전체 애플리케이션 또는 개별 기능을 선택할 수 있습니다. 전체 애플리케이션을 선택하면 모든 기능이 포함되며 향후 기능이 추가되면 애플리케이션 정의가 자동으로 업데이트됩니다. QoS 규칙에서 애플리케이션 그룹, 필터 또는 컨테이너를 사용하는 경우 애플리케이션 열의 개체 위에 마우스를 놓고 아래쪽 화살표를 클릭하고 값을 선택하여 이러한 개체에 대한 세부 정보를 볼 수 있습니다. 이를 통해 개체 탭으로 이동할 필요 없이 정책에서 직접 애플리케이션 구성원을 쉽게 볼 수 있습니다.
서비스/URL 카테고리 탭	

QoS 정책 규칙 설정	
서비스	특정 TCP 및/또는 UDP 포트 번호로 제한할 서비스를 선택합니다. 드롭다운에서 다음 중 하나를 선택합니다. • **any** - 선택한 애플리케이션이 모든 프로토콜 또는 포트에서 허용되거나 거부됩니다. • **application-default** - 선택한 애플리케이션은 **Palo Alto Networks**에서 정의한 기본 포트에서만 허용 또는 거부됩니다. 이 옵션은 허용 정책에 권장됩니다. • 선택 - 추가를 클릭합니다. 기존 서비스를 선택하거나 서비스 또는 서비스 그룹을 선택하여 새 항목을 지정합니다.
URL 카테고리	QoS 규칙에 대한 URL 카테고리를 선택합니다. • URL 카테고리에 관계없이 세션이 이 QoS 규칙과 일치할 수 있도록 하려면 모두를 선택합니다. • 카테고리를 지정하려면 추가를 클릭하고 드롭다운에서 특정 카테고리(사용자 지정 카테고리 포함)를 선택합니다. 여러 카테고리를 추가할 수 있습니다. 사용자 정의 카테고리 정의에 대한 정보는 개체 > 외부 동적 목록을 참조하십시오.
DSCP/TOS 탭	
모두 선택	DSCP(Differentiated Services Code Point) 값이나 트래픽에 대해 정의된 IP 우선 순위/서비스 유형(ToS)에 관계없이 정책이 트래픽과 일치하도록 하려면 모두(기본값)를 선택합니다.
코드포인트	패킷의 IP 헤더에 정의된 DSCP 또는 ToS 값을 기반으로 트래픽이 QoS 처리를 수신할 수 있도록 하려면 **Codepoints**를 선택합니다. DSCP 및 ToS 값은 높은 우선 순위 또는 최선형 전달과 같이 트래픽에 대해 요청된 서비스 수준을 나타내는 데 사용됩니다. QoS 정책에서 일치 기준으로 코드 포인트를 사용하면 세션 시작 시 감지된 코드 포인트를 기반으로 세션이 QoS 처리를 받을 수 있습니다. QoS 정책에 트래픽을 일치시키기 위해 코드 포인트 추가를 계속합니다. • 코드포인트 항목에 설명이 포함된 이름을 지정합니다. • QoS 정책에 대한 일치 기준으로 사용할 코드 포인트 유형을 선택한 다음 특정 코드 포인트 값을 선택하십시오. 코드 포인트 이름과 바이너리 값을 입력하여 사용자 정의 코드 포인트를 생성할 수도 있습니다.
기타 설정 탭	

QoS 정책 규칙 설정	
클래스	규칙에 할당할 QoS 클래스를 선택한 다음 확인을 클릭합니다. 클래스 특성은 QoS 프로파일에 정의됩니다. QoS 클래스에 대한 설정 구성에 대한 정보는 네트워크 > 네트워크 프로파일 > QoS를 참조하십시오.
일정	• 정책 규칙이 항상 활성 상태를 유지하려면 없음을 선택합니다. • 드롭다운에서 일정(달력 아이콘)을 선택하여 규칙이 활성화된 단일 시간 범위 또는 반복 시간 범위를 설정합니다.
대상 탭(Panorama만 해당)	
모두(모든 디바이스를 대상으로 함)	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스	정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그	지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > 정책 기반 포워딩

일반적으로 트래픽이 방화벽에 들어갈 때 수신 인터페이스 가상 라우터는 대상 IP 주소를 기반으로 나가는 인터페이스와 대상 보안 영역을 결정하는 경로를 지시합니다. PBF(정책 기반 포워딩) 규칙을 생성하여 소스 영역, 소스 주소, 소스 사용자, 대상 주소, 대상 애플리케이션 및 대상 서비스를 포함하여 발신 인터페이스를 결정하기 위한 기타 정보를 지정할 수 있습니다. 애플리케이션과 연결된 지정된 대상 IP 주소 및 포트의 초기 세션은 애플리케이션별 규칙과 일치하지 않으며 후속 PBF 규칙(애플리케이션을 지정하지 않음) 또는 가상 라우터의 포워딩 테이블에 따라 포워딩됩니다. 동일한 애플리케이션에 대한 해당 대상 IP 주소 및 포트의 모든 후속 세션은 애플리케이션별 규칙과 일치합니다. PBF 규칙을 통한 포워딩을 보장하기 위해 애플리케이션별 규칙은 권장되지 않습니다.

필요한 경우 PBF 규칙을 사용하여 Forward-to-VSYS 포워딩 작업을 사용하여 추가 가상 시스템을 통해 트래픽을 강제 실행할 수 있습니다. 이 경우 대상 가상 시스템의 패킷을 방화벽의 특정 이그레스(egress) 인터페이스를 통해 포워딩하는 추가 PBF 규칙을 정의해야 합니다.

다음 표에서는 정책 기반 포워딩 설정을 설명합니다.

- 정책 기반 포워딩 일반 탭
- 정책 기반 포워딩 소스 탭
- 정책 기반 포워딩 대상/애플리케이션/서비스 탭
- 정책 기반 포워딩 탭
- (Panorama만 해당) 정책 기반 포워딩 대상 탭

더 찾고 계십니까?

정책 기반 포워딩 참조

정책 기반 포워딩 일반 탭

일반 탭을 선택하여 PBF 정책에 대한 이름과 설명을 구성합니다. 많은 수의 정책이 있을 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수도 있습니다.

필드	설명
이름	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	정책에 대한 설명을 입력합니다(최대 1024자).
태그	정책에 태그를 지정해야 하는 경우 태그를 추가하고 지정합니다.

필드	설명
	정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 DMZ에 대한 인바운드와 특정 보안 정책에 태그를 지정하거나, 복호화 및 복호화 금지라는 단어로 정책을 복호화하거나 해당 위치와 관련된 정책에 특정 데이터 센터의 이름을 사용할 수 있습니다.
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화할 수 있습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. CSV 형식으로 감사 코멘트 아카이브를 내보낼 수 있습니다.

정책 기반 포워딩 소스 탭

소스 탭을 선택하여 포워딩 정책이 적용될 수신 소스 트래픽을 정의하는 소스 영역 또는 소스 주소를 정의합니다.

필드	설명
소스 영역	소스 영역(기본값은 any)을 선택하려면 추가를 클릭하고 드롭다운에서 선택합니다. 새 영역을 정의하려면 네트워크 > 영역을 참조하세요. 여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다. 정책 기반 포워딩에는 *Layer 3* 유형 영역만 지원됩니다.
소스 주소	추가를 클릭하여 소스 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 any). 드롭다운에서 선택하거나 드롭다운 하단에서 주소, 주소 그룹 또는 지역을 클릭하고 설정을 지정합니다.
소스 사용자	추가를 클릭하여 정책이 적용되는 소스 사용자 또는 사용자 그룹을 선택합니다. 다음 소스 사용자 유형이 지원됩니다. • **any** - 사용자 데이터에 관계없이 모든 트래픽을 포함합니다.

필드	설명
	• 사전 로그온 - GlobalProtect™를 사용하여 네트워크에 연결되었지만 시스템에 로그인하지 않은 원격 사용자를 포함합니다. 사전 로그온 옵션이 GlobalProtect 앱용 포털에 구성된 경우 현재 컴퓨터에 로그인하지 않은 사용자는 사전 로그온 사용자명으로 식별됩니다. 그런 다음 사전 로그온 사용자에 대한 정책을 생성할 수 있으며 사용자가 직접 로그인하지 않더라도 해당 컴퓨터는 완전히 로그인한 것처럼 도메인에서 인증됩니다. • 알려진 사용자 - 모든 인증된 사용자를 포함합니다. 즉, 사용자 데이터가 매핑된 모든 IP를 의미합니다. 이 옵션은 도메인의 "도메인 사용자" 그룹과 동일합니다. • **unknown** - 인증되지 않은 모든 사용자를 포함합니다. 즉, 사용자에게 매핑되지 않은 IP 주소를 의미합니다. 예를 들어, 게스트 수준 액세스에 대해 unknown을 사용할 수 있습니다. 그 이유는 네트워크에 IP가 있지만 도메인에 대해 인증되지 않고 방화벽에 IP 주소-사용자 매핑 정보가 없기 때문입니다. • 선택 - 이 창에서 선택한 항목에 따라 선택한 사용자를 포함합니다. 예를 들어 사용자 한 명, 개인 목록, 일부 그룹을 추가하거나 수동으로 사용자를 추가할 수 있습니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS, TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.

정책 기반 포워딩 대상/애플리케이션/서비스 탭

대상/애플리케이션/서비스 탭을 선택하여 포워딩 규칙과 일치하는 트래픽에 적용되는 대상 설정을 정의합니다.

필드	설명
대상 주소	대상 주소 또는 주소 그룹을 추가하려면 추가를 클릭합니다(기본값은 any). 기본적으로 규칙은 모든 IP 주소에 적용됩니다. 드롭다운에서 선택하거나 드롭다운 하단의 주소 또는 주소 그룹을 클릭하고 설정을 지정합니다.
애플리케이션/서비스	PBF 규칙에 대한 특정 애플리케이션 또는 서비스를 선택합니다. 새 애플리케이션을 정의하려면 응용프로그램 정의를 조하십시오. 애플리케이션 그룹을 정의하려면 개체> 애플리케이션 그룹을 참조하세요.

필드	설명
	PBF와 함께 사용하는 경우 애플리케이션별 규칙은 권장되지 않습니다. 가능하면 프로토콜 또는 애플리케이션에서 사용하는 레이어 *4* 포트*(TCP* 또는 *UDP)*인 서비스 개체를 사용합니다. 애플리케이션 열의 개체 위에 마우스를 놓고 아래쪽 화살표를 클릭한 다음 값을 선택하면 이러한 애플리케이션에 대한 세부 정보를 볼 수 있습니다. 이렇게 하면 개체 탭으로 이동하지 않고도 정책에서 직접 애플리케이션 정보를 쉽게 볼 수 있습니다. *PBF* 규칙에서는 사용자 지정 애플리케이션, 애플리케이션 필터 또는 애플리케이션 그룹을 사용할 수 없습니다.

정책 기반 포워딩 탭

포워딩 탭을 선택하여 포워딩 정책과 일치하는 트래픽에 적용할 작업 및 네트워크 정보를 정의합니다. 트래픽은 다음 홉 IP 주소, 가상 시스템으로 포워딩되거나 트래픽이 삭제될 수 있습니다.

필드	설명
작업	다음 옵션 중 하나를 선택합니다. • 포워딩 - 다음 홉 IP 주소 및 이그레스(Egress) 인터페이스(패킷이 지정된 다음 홉에 도달하기 위해 사용하는 인터페이스)를 지정합니다. • **VSYS**로 포워딩 - 드롭다운에서 포워딩할 가상 시스템을 선택합니다. • 삭제 - 패킷을 삭제합니다. • **No PBF** - 패킷이 사용할 경로를 변경하지 마십시오. 이 옵션은 규칙에 정의된 소스/대상/애플리케이션/서비스에 대한 기준과 일치하는 패킷을 제외합니다. 일치하는 패킷은 PBF 대신 경로 테이블을 사용합니다. 방화벽은 경로 테이블을 사용하여 리디렉션된 포트에서 일치하는 트래픽을 제외합니다. 트래픽에 모니터 프로파일을 적용할 수 있도록 작업으로 ***Forward*** 또는 ***Forward to VSYS***를 사용합니다. *(*작업이 트래픽을 포워딩하지 않는 경우 모니터 프로파일을 적용할 수 없습니다.*)* 모니터 프로파일은 *IP* 주소를 모니터링합니다. *IP* 주소에 대한 연결이 실패하면 모니터 프로파일이 작업을 지정합니다.

필드	설명
이그레스(Egress) 인터페이스	패킷을 특정 이그레스(egress) 인터페이스로 보냅니다.
다음 홉	패킷을 특정 인터페이스로 보내는 경우 다음 방법 중 하나로 패킷에 대한 다음 홉을 지정합니다. • **IP** 주소 - IP 주소를 선택한 다음 IPv4 또는 IPv6 주소를 사용하는 주소 개체를 선택하거나 새 주소 개체를 만듭니다. • **FQDN** - FQDN을 선택한 다음 FQDN을 사용하는 주소 개체를 선택하거나 새 주소 개체를 만듭니다. • 없음 - 다음 홉이 없습니다. 패킷이 삭제됩니다.
모니터	모니터링을 활성화하여 대상 **IP** 주소 또는 다음 홉 IP 주소에 대한 연결을 확인합니다. 모니터를 선택한 다음 IP 주소에 연결할 수 없는 경우 작업을 지정하는 모니터링 프로파일(기본 또는 사용자 지정, **Network** > **Network Profiles** > **Monitor**)을 연결합니다. 모니터 프로파일을 구성하고 모니터링을 활성화하여 이그레스*(egress)* 인터페이스가 실패하거나 경로가 다운되는 경우 방화벽이 프로파일에서 조치를 취하고 서비스 중단을 최소화하거나 방지합니다.
대칭 반환 적용	(비대칭 라우팅 환경에 필요) **Enforce Symmetric Return**을 선택한 다음 다음 홉 주소 목록에 하나 이상의 IP 주소를 입력합니다. 대칭 반환을 활성화하면 반환 트래픽(예: LAN의 트러스트 영역에서 인터넷으로)이 인터넷에서 들어오는 트래픽과 동일한 인터페이스를 통해 포워딩됩니다.
일정	규칙이 적용되는 날짜와 시간을 제한하려면 드롭다운에서 일정을 선택합니다. 새 일정을 정의하려면 복호화된 SSL 트래픽 제어 설정을 참조합니다.

정책 기반 포워딩 대상 탭

- (Panorama만 해당) 정책 > 정책 기반 포워딩 > 대상

대상 탭을 선택하여 정책 규칙을 푸시할 디바이스 그룹의 관리 방화벽을 선택합니다. 관리 방화벽을 선택하거나 태그를 지정하여 푸시할 관리 방화벽을 지정할 수 있습니다. 또한 지정된 방화벽을 제외한 모든 관리 방화벽에 푸시하도록 정책 규칙 대상을 구성할 수 있습니다.

NAT 규칙 - 대상 설정	설명
모두(모든 디바이스를 대상으로 함)	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스	정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그	지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > 복호화

가시성, 제어 및 세분화된 보안을 위해 트래픽을 복호화하도록 방화벽을 구성할 수 있습니다. 복호화 정책은 IMAP(S), POP3(S), SMTP(S), FTP(S)와 같은 SSL 캡슐화 프로토콜과 SSH(Secure Shell) 트래픽을 포함한 SSL(Secure Sockets Layer)에 적용될 수 있습니다. SSH 복호화를 사용하여 발신 및 수신 SSH 트래픽을 복호화하여 보안 프로토콜이 허용되지 않는 애플리케이션 및 콘텐츠를 터널링하는 데 사용되지 않도록 할 수 있습니다.

복호화 정책 규칙을 추가하여 암호를 복호화하려는 트래픽을 정의합니다(예: URL 분류를 기반으로 트래픽 암호를 복호화할 수 있음). 복호화 정책 규칙은 트래픽과 순서대로 비교되므로 보다 구체적인 규칙이 보다 일반적인 규칙보다 우선해야 합니다.

SSL 포워딩 프록시 복호화에는 사용자가 연결하는 서버에 방화벽이 신뢰하는 CA에서 서명한 인증서가 있는 경우 사용자에게 제공되는 신뢰할 수 있는 인증서의 구성이 필요합니다. 디바이스 > 인증서 관리 > 인증서 페이지에서 인증서를 만든 다음 인증서 이름을 클릭하고 트러스트 인증서 포워딩을 선택합니다.

방화벽은 예를 들어 고정된 인증서 또는 클라이언트 인증을 사용하기 때문에 기술적으로 복호화를 중단하는 애플리케이션을 복호화하지 않습니다.

SSL 복호화에서 제외된 애플리케이션 목록을 참조하십시오.

다음 표에서는 복호화 정책 설정을 설명합니다.

- 복호화 일반 탭
- 복호화 소스 탭
- 복호화 대상 탭
- 복호화 서비스/URL 카테고리 탭
- 복호화 옵션 탭
- (Panorama만 해당) 복호화 대상 탭

더 찾고 계십니까?

복호화 참조

복호화 일반 탭

일반 탭을 선택하여 복호화 정책에 대한 이름과 설명을 구성합니다. 많은 수의 정책이 있을 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수도 있습니다.

필드	설명
이름	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디

필드	설명
	바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	규칙에 대한 설명을 입력합니다(최대 1024자).
태그	정책에 태그를 지정해야 하는 경우 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 DMZ에 대한 인바운드와 특정 보안 정책에 태그를 지정하거나, 복호화 및 복호화 금지라는 단어로 정책을 복호화하거나 해당 위치와 관련된 정책에 특정 데이터 센터의 이름을 사용할 수 있습니다.
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화할 수 있습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. CSV 형식으로 감사 코멘트 아카이브를 내보낼 수 있습니다.

복호화 소스 탭

소스 탭을 선택하여 복호화 정책이 적용될 수신 소스 트래픽을 정의하는 소스 영역 또는 소스 주소를 정의합니다.

필드	설명
소스 영역	추가를 클릭하여 소스 영역을 선택합니다(기본값은 모두임). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을 참조하세요. 여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다.
소스 주소	추가를 클릭하여 소스 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 any). 드롭다운에서 선택하거나 드롭다운 하단에서 주소, 주소 그룹 또는

필드	설명
	지역을 클릭하고 설정을 지정합니다. 구성된 주소를 제외한 모든 주소를 선택하려면 무효를 선택하십시오.
소스 사용자	추가를 클릭하여 정책이 적용되는 소스 사용자 또는 사용자 그룹을 선택합니다. 다음 소스 사용자 유형이 지원됩니다. • **any** - 사용자 데이터에 관계없이 모든 트래픽을 포함합니다. • 사전 로그온 - GlobalProtect를 사용하여 네트워크에 연결되었지만 시스템에 로그인하지 않은 원격 사용자를 포함합니다. 사전 로그온 옵션이 GlobalProtect 앱용 포털에 구성된 경우 현재 컴퓨터에 로그인하지 않은 사용자는 사전 로그온 사용자명으로 식별됩니다. 그런 다음 사전 로그온 사용자에 대한 정책을 생성할 수 있으며 사용자가 직접 로그인하지 않더라도 해당 컴퓨터는 완전히 로그인한 것처럼 도메인에서 인증됩니다. • 알려진 사용자 - 모든 인증된 사용자를 포함합니다. 즉, 사용자 데이터가 매핑된 모든 IP를 의미합니다. 이 옵션은 도메인의 "도메인 사용자" 그룹과 동일합니다. • **unknown** - 인증되지 않은 모든 사용자를 포함합니다. 즉, 사용자에게 매핑되지 않은 IP 주소를 의미합니다. 예를 들어, 게스트 수준 액세스에 알 수 없음을 사용할 수 있습니다. 그 이유는 네트워크에 IP가 있지만 도메인에 대해 인증되지 않고 방화벽에 IP - 사용자 매핑 정보가 없기 때문입니다. • 선택 - 이 창에서 선택한 항목에 따라 선택한 사용자를 포함합니다. 예를 들어 사용자 한 명, 개인 목록, 일부 그룹을 추가하거나 수동으로 사용자를 추가할 수 있습니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS, TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.

복호화 대상 탭

대상 탭을 선택하여 정책이 적용될 대상 트래픽을 정의하는 대상 영역 또는 대상 주소를 정의합니다.

필드	설명
대상 영역	추가를 클릭하여 대상 영역을 선택합니다(기본값은 모두임). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을(를) 참조하십시오.

필드	설명
	여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다.
대상 주소	추가를 클릭하여 대상 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 모두). 드롭다운에서 선택하거나 드롭다운 하단에서 주소, 주소 그룹 또는 지역을 클릭하고 설정을 지정합니다. 구성된 주소를 제외한 모든 주소를 선택하려면 무효를 선택하십시오.

복호화 서비스/URL 카테고리 탭

서비스/**URL** 카테고리 탭을 선택하여 TCP 포트 번호를 기반으로 하는 트래픽 또는 모든 URL 카테고리(또는 카테고리 목록)에 복호화 정책을 적용합니다.

필드	설명
서비스	특정 TCP 포트 번호를 기반으로 트래픽에 복호화 정책을 적용합니다. 드롭다운에서 다음 중 하나를 선택합니다. • **any** - 선택한 애플리케이션이 모든 프로토콜 또는 포트에서 허용되거나 거부됩니다. • **application-default** - 선택한 애플리케이션은 Palo Alto Networks에서 애플리케이션에 대해 정의한 기본 포트에서만 복호화됩니다(또는 복호화에서 제외됨). • 선택 - 추가를 클릭합니다. 기존 서비스를 선택하거나 새 서비스 또는 서비스 그룹을 지정하십시오. (또는 개체 > 서비스 및 개체 > 서비스 그룹 선택).
URL 카테고리 탭	복호화 규칙에 대한 URL 카테고리를 선택합니다. • URL 카테고리에 관계없이 모든 세션과 일치시키려면 모두를 선택하십시오. • 카테고리를 지정하려면 추가를 클릭하고 드롭다운에서 특정 카테고리(맞춤 카테고리 포함)를 선택합니다. 여러 카테고리를 추가할 수 있습니다. 사용자 정의 범주 정의에 대한 정보를 참조하십시오.

복호화 옵션 탭

옵션 탭을 선택하여 일치하는 트래픽을 복호화할지의 여부를 결정합니다. 복호화가 설정된 경우 복호화 유형을 지정합니다. 암호 해독 프로파일을 구성하거나 선택하여 암호 해독 기능을 추가할 수도 있습니다.

필드	설명
동작	트래픽에 대해 복호화 또는 비복호화를 선택합니다.

유형	드롭다운에서 복호화할 트래픽 유형을 선택합니다.
	• **SSL** 전달 프록시 - 정책이 외부 서버로 향하는 클라이언트 트래픽의 암호를 해독하도록 지정합니다.
	• **SSH** 프록시 - 정책이 SSH 트래픽을 복호화하도록 지정합니다. 이 옵션을 사용하면 ssh-tunnel App-ID를 지정하여 정책에서 SSH 터널링을 제어할 수 있습니다.
	• **SSL** 인바운드 검사 - 정책이 인바운드 SSL 트래픽을 해독하도록 지정합니다.
	  • 인증서 - 인바운드 SSL 트래픽이 대상으로 하는 내부 서버에 대한 인증서를 추가합니다.
	  기존 서버 인증서를 갱신하거나 교체한 후 인증서 번들을 단일 파일로 방화벽으로 가져와 *SSL* 인바운드 검사 암호 해독 정책 규칙에 추가합니다. 정책 규칙을 미리 업데이트하면 결국 웹 서버에 새 인증서를 설치할 때 중단 없이 암호 해독을 계속할 수 있습니다. SSL 인바운드 검사 구성에서는 이 모범 사례를 더 자세히 설명합니다.
	웹 서버에서 호스팅하는 도메인에 대한 인증서를 추가할 수도 있습니다. 정책 규칙당 최대 12개의 인증서가 지원됩니다.

복호화 프로파일	트래픽의 특정 측면을 차단하고 제어하기 위해 정책 규칙에 복호화 프로파일을 연결합니다. 복호화 프로파일 생성에 대한 자세한 내용을 보려면 개체 > 복호화 프로파일을(를) 선택하십시오.
로그 설정	
성공적인 SSL 핸드쉐이크 기록	(선택 사항) 성공적인 SSL 복호화 핸드쉐이크에 대한 자세한 로그를 생성합니다. 기본적으로 비활성화되어 있습니다.

필드	설명
	로그는 저장 공간을 사용합니다. 성공적인 ***SSL*** 핸드쉐이크를 기록하기 전에 로그를 저장하는 데 사용할 수 있는 리소스가 있는지 확인하십시오. ***Device*** > ***Setup*** > ***Management*** > 로깅 및 보고 설정을 편집하여 현재 로그 메모리 할당을 확인하고 로그 유형 간에 로그 메모리를 다시 할당합니다.
SSL 핸드쉐이크 실패 기록	SSL 복호화 핸드쉐이크 실패에 대한 자세한 로그를 생성하여 복호화 문제의 원인을 찾을 수 있습니다. 기본적으로 활성화되어 있습니다. 로그는 저장 공간을 사용합니다. 더 많거나 적은 로그 저장 공간을 복호화 로그에 할당하려면 로그 메모리 할당(***Device*** > ***Setup*** > ***Management*** > ***Logging*** 및 보고 설정)을 편집하십시오.
로그 포워딩	GlobalProtect SSL 핸드쉐이크(복호화) 로그를 포워딩할 방법과 위치를 지정합니다.

복호화 대상 탭

- (Panorama 전용) 정책 > **Decryption** > **Target**

대상 탭을 선택하여 정책 규칙을 푸시할 디바이스 그룹의 관리 방화벽을 선택합니다. 관리 방화벽을 선택하거나 태그를 지정하여 푸시할 관리 방화벽을 지정할 수 있습니다. 또한 지정된 방화벽을 제외한 모든 관리 방화벽에 푸시하도록 정책 규칙 대상을 구성할 수 있습니다.

NAT 규칙 - 대상 설정	설명
모두(모든 디바이스를 대상으로 함)	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스	정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그	지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.

NAT 규칙 - 대상 설정	설명
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > 네트워크 패킷 브로커

네트워크 패킷 브로커 정책 규칙은 애플리케이션, 사용자, 영역, 디바이스 및 IP 주소를 기반으로 타사 보안 어플라이언스의 외부 체인(보안 체인)으로 포워딩할 트래픽을 정의합니다. Network Packet Broker는 복호화된 TLS, 복호화되지 않은 TLS 및 비 TLS 트래픽을 보안 체인으로 포워딩할 수 있습니다. 각 네트워크 패킷 브로커 정책 규칙에 패킷 브로커 프로파일을 연결합니다. 정책 규칙은 보안 체인으로 포워딩할 트래픽을 정의하고 프로파일은 방화벽 포워딩 인터페이스, 상태 모니터링, 여러 체인 간의 세션 분배, 체인 라우팅(레이어 3) 또는 투명 브리지(레이어 1) 여부 선택을 포함하여 해당 트래픽을 포워딩하는 방법을 정의합니다.

다음 표에는 Network Packet Broker에 대한 정책 규칙 설정 및 정책 최적화 옵션이 설명되어 있습니다.

- 네트워크 패킷 브로커 일반 탭
- 네트워크 패킷 브로커 소스 탭
- 네트워크 패킷 브로커 대상 탭
- 네트워크 패킷 브로커 애플리케이션/서비스/트래픽 탭
- 네트워크 패킷 브로커 경로 선택 탭
- 네트워크 패킷 브로커 정책 최적화 프로그램 규칙 사용

네트워크 패킷 브로커 일반 탭

일반 탭을 선택하여 정책에 대한 이름과 설명을 구성합니다. 많은 수의 정책이 있을 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수도 있습니다.

필드	설명
이름	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	정책에 대한 설명을 입력합니다(최대 1024자).
태그	정책에 태그를 지정해야 하는 경우 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구문입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 태그는 네트워크 위치, 레이어 3 보안 체인 또는 레이어 1 보안 체인을 나타낼 수 있습니다.
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력하십시오. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기반 그룹을 볼 수 있습니다.

필드	설명
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. CSV 형식으로 감사 코멘트 아카이브를 내보낼 수 있습니다.

네트워크 패킷 브로커 소스 탭

소스 탭을 선택하여 네트워크 패킷 브로커 보안 체인으로 포워딩할 트래픽의 소스 영역, IP 주소, 사용자 및 디바이스를 정의합니다.

필드	설명
소스 영역	소스 영역(기본값은 any)을 선택하려면 추가를 클릭하고 드롭다운에서 선택합니다. 새 영역을 정의하려면 네트워크 > 영역을 참조하세요. 여러 영역을 추가하여 관리를 단순화할 수 있습니다.
소스 주소	소스 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 **Any**). 드롭다운에서 선택하거나 주소 개체, 주소 그룹 또는 지역(드롭다운 하단)을 선택하여 설정을 지정합니다. 개체 > 주소 및 개체 > 주소 그룹은 각각 정책 규칙이 지원하는 주소 개체 및 주소 그룹의 유형을 설명합니다. 부정 옵션을 선택하면 지정된 주소를 제외하고 지정된 영역의 소스 주소에 규칙이 적용됩니다.
소스 사용자	추가를 클릭하여 정책이 적용되는 소스 사용자 또는 사용자 그룹을 선택합니다. 다음 소스 사용자 유형이 지원됩니다. • **any** - 사용자 데이터에 관계없이 모든 트래픽을 포함합니다. • 사전 로그온 - GlobalProtect™를 사용하여 네트워크에 연결되었지만 시스템에 로그인하지 않은 원격 사용자를 포함합니다. 사전 로그온 옵션이 GlobalProtect 앱용 포털에 구성된 경우 현재 컴퓨터에 로그인하지 않은 사용자는 사전 로그온 사용자명으로 식별됩니다. 그런 다음 사전 로그온 사용자에 대한 정책을 생성할 수 있으며 사용자가 직접 로그인하지 않더라도 해당 컴퓨터는 완전히 로그인한 것처럼 도메인에서 인증됩니다. • 알려진 사용자 - 모든 인증된 사용자를 포함합니다. 즉, 사용자 데이터가 매핑된 모든 IP를 의미합니다. 이 옵션은 도메인의 "도메인 사용자" 그룹과 동일합니다.

필드	설명
	• **unknown** - 인증되지 않은 모든 사용자를 포함합니다. 즉, 사용자에게 매핑되지 않은 IP 주소를 의미합니다. 예를 들어 네트워크에 IP가 있지만 도메인에 대해 인증되지 않고 방화벽에 IP 주소-사용자 매핑 정보가 없기 때문에 게스트 수준 액세스에 대해 unknown을 사용할 수 있습니다. • 선택 - 이 창에서 선택한 항목에 따라 선택한 사용자를 포함합니다. 예를 들어 사용자 한 명, 개인 목록, 일부 그룹을 추가하거나 수동으로 사용자를 추가할 수 있습니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS, TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.
소스 디바이스	정책에 따라 호스트 디바이스를 추가합니다. • 모두 - 모든 디바이스를 포함합니다. • **no-hip** - HIP 정보가 필요하지 않습니다. 이 설정을 사용하면 HIP 정보를 수집하거나 제출할 수 없는 타사 디바이스에서 액세스할 수 있습니다. • 선택 - 구성에 따라 결정된 선택된 디바이스를 포함합니다. 예를 들어 모델, OS, OS 제품군 또는 공급자를 기반으로 디바이스 개체를 추가할 수 있습니다.

네트워크 패킷 브로커 대상 탭

Destination 탭을 선택하여 Network Packet Broker 보안 체인으로 포워딩할 트래픽의 대상 영역, IP 주소 및 디바이스를 정의합니다.

필드	설명
대상 영역	소스 영역(기본값은 any)을 선택하려면 추가를 클릭하고 드롭다운에서 선택합니다. 새 영역을 정의하려면 네트워크 > 영역을 참조하세요. 여러 영역을 추가하여 관리를 단순화할 수 있습니다.
대상 주소	대상 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 **Any**). 드롭다운에서 선택하거나 주소 개체, 주소 그룹 또는 지역(드롭다운 하단)을 클릭하여 주소 설정을 지정합니다. 개체 > 주소 및 개체 > 주소 그룹은 각각 정책 규칙이 지원하는 주소 개체 및 주소 그룹의 유형을 설명합니다.

필드	설명
	무효 옵션을 선택하면 지정된 주소를 제외하고 지정된 영역의 대상 주소에 규칙이 적용됩니다.
대상 디바이스	정책에 따라 호스트 디바이스를 개별적으로 추가하거나 모든 디바이스를 포함하려면 모두를 선택합니다.

네트워크 패킷 브로커 애플리케이션/서비스/트래픽 탭

애플리케이션/서비스/트래픽 탭을 선택하여 네트워크 패킷 브로커 보안 체인으로 포워딩할 트래픽 유형, 애플리케이션 및 서비스를 정의합니다. 복호화된 TLS, 복호화되지 않은 TLS 및 TLS가 아닌 트래픽의 모든 조합을 보안 체인으로 포워딩할 수 있습니다.

필드	설명
트래픽 유형	보안 체인으로 포워딩할 트래픽 유형을 선택합니다. 하나의 규칙에서 트래픽 유형 중 하나, 일부 또는 전체를 선택할 수 있습니다. • **TLS(Decrypted)** 트래픽 포워딩 - (기본값) 복호화된 TLS 트래픽을 네트워크 패킷 브로커 정책에 연결된 패킷 브로커 프로파일에서 지정한 보안 체인으로 포워딩합니다. • **Forward TLS(Non-Decrypted)** 트래픽 - 복호화되지 않은 TLS 트래픽을 Network Packet Broker 정책에 연결된 Packet Broker 프로파일에서 지정한 보안 체인으로 포워딩합니다. • 비 **TLS** 트래픽 포워딩 - 일반 텍스트(비 TLS) 트래픽을 네트워크 패킷 브로커 정책에 연결된 패킷 브로커 프로파일에서 지정한 보안 체인으로 포워딩합니다.
애플리케이션	네트워크 패킷 브로커 정책 규칙에 대한 특정 애플리케이션을 추가합니다. 애플리케이션에 여러 기능이 있는 경우 컨테이너 애플리케이션 또는 개별 기능 애플리케이션을 선택할 수 있습니다. 컨테이너 애플리케이션을 선택하면 모든 기능 애플리케이션이 포함되며 향후 기능 애플리케이션이 컨테이너 애플리케이션에 추가될 때 애플리케이션 정의가 자동으로 업데이트됩니다.
서비스	특정 TCP 또는 UDP 포트 번호로 제한할 서비스를 선택합니다. 드롭다운에서 다음 중 하나를 선택합니다. • **any** - (기본값) 선택한 애플리케이션이 모든 프로토콜 또는 포트에서 포워딩됩니다. • **application-default** - 선택한 애플리케이션이 Palo Alto Networks®에서 정의한 기본 포트에 있는 경우에만 포워딩됩니다. (비표준 포트 및 프

필드	설명
	로토콜에서 실행되는 애플리케이션은 의도하지 않은 경우 원치 않는 애플리케이션 동작 및 사용의 징후가 될 수 있으며 의도적인 경우 악성 동작의 징후가 될 수 있습니다. 그러나 내부 사용자 지정 애플리케이션은 비표준 포트를 사용할 수 있으며 예외가 필요할 수 있습니다.) • 선택 - 기존 서비스를 추가하거나 서비스 또는 서비스 그룹을 선택하여 새 항목을 지정합니다. (또는 개체 > 서비스 및 개체 > 서비스 그룹 선택).

네트워크 패킷 브로커 경로 선택 탭

경로 선택 탭을 선택하여 네트워크 패킷 브로커 정책에 정의된 트래픽에 적용할 패킷 브로커 프로파일을 선택합니다. 정책은 보안 체인으로 전달할 트래픽을 정의하고 프로필은 트래픽을 전달하는 방법(사용할 방화벽 전달 인터페이스, 보안 체인이 라우팅된 레이어 3 체인인지 투명 브리지 레이어 1 체인인지의 여부, 상태 모니터링 방법 등)을 정의합니다.

드롭다운을 사용하여 이전에 구성된 프로파일을 선택하거나 정책 규칙에 대한 새 패킷 브로커 프로파일을 생성합니다.

네트워크 패킷 브로커 정책 최적화 프로그램 규칙 사용

Network Packet Broker 정책 규칙의 경우 Policy Optimizer는 정책이 사용 중인지의 여부를 확인하는 데 사용할 수 있는 규칙 사용 통계를 표시합니다. 다양한 기간 동안의 규칙 사용을 보고 규칙이 예상대로 사용되지 않은 이유를 검토하고 사용하지 않거나 오래된 규칙을 삭제할 수 있습니다.

필드	설명
기간	데이터가 표시되는 기간(일수)입니다.
사용	• 트래픽이 규칙(사용된 규칙)과 일치하는지의 여부(사용되지 않은 규칙)와 관계없이 지정된 기간 동안 방화벽에 대한 임의의 모든 네트워크 패킷 브로커 정책 규칙입니다. • 지정된 기간 동안 트래픽이 일치하지 않는 사용되지 않은 규칙입니다. • 지정된 기간 동안 트래픽이 일치하는 사용된 규칙입니다.
지난 "n"일 동안 재설정된 제외 규칙	지정된 일 수(1-5,000일) 내에 **Reset Rule Hit Counter**에 대한 규칙 표시를 생략합니다. 예를 들어 트래픽을 일치시킬 시간이 없었을 수 있는 최신 규칙을 제외하면서 특정 기간 동안 트래픽과 일치하지 않은 이전 규칙을 검사할 수 있습니다.
이름	네트워크 패킷 브로커 정책 규칙의 이름입니다.

필드	설명
패킷 브로커	• 프로파일 - 정책 규칙과 연결된 패킷 브로커 프로파일의 이름입니다. • 트래픽 유형 - 규칙이 제어하는 트래픽 유형(복호화된 TLS, 복호화되지 않은 TLS 및 비TLS 트래픽 중 하나 이상).
규칙 사용	• 적중 횟수 - 트래픽이 규칙과 일치한 횟수입니다. • 마지막 적중 - 트래픽이 규칙과 일치하는 가장 최근 시간입니다. • 첫 번째 적중 - 트래픽이 규칙과 처음 일치한 시간입니다. • 재설정 날짜 - 규칙의 적중 카운터가 재설정된 마지막 날짜입니다.
수정	규칙이 마지막으로 수정된 날짜 및 시간입니다.
생성	규칙이 생성된 날짜 및 시간입니다.

정책 > 터널 검사

다음 일반 텍스트 터널 프로토콜의 트래픽 콘텐츠를 검사하도록 방화벽을 구성할 수 있습니다.

- 일반 라우팅 캡슐화(GRE)
- GPRS(General Packet Radio Service) 사용자 데이터용 터널링 프로토콜(GTP-U) GTP를 지원하는 방화벽에서만 지원됩니다.
- 암호화되지 않은 IPSec 트래픽(IPSec 및 전송 모드 AH IPSec에 대한 NULL 암호화 알고리즘)
- 가상 확장 LAN(VXLAN)

터널 콘텐츠 검사를 사용하여 이러한 유형의 터널의 트래픽과 다른 일반 텍스트 터널(예: GRE 터널 내부의 Null 암호화 IPSec)에 중첩된 트래픽에 대한 보안, DoS 방어 및 QoS 정책을 시행할 수 있습니다.

들어오는 패킷을 일치시킬 때 방화벽이 검사할 패킷의 터널 프로토콜을 결정하고 방화벽이 패킷을 삭제하거나 계속 처리하는 조건을 지정하는 터널 검사 정책을 만듭니다. ACC에서 터널 검사 로그 및 터널 활동을 보고 터널링된 트래픽이 회사 보안 및 사용 정책을 준수하는지 확인할 수 있습니다.

방화벽은 이더넷 인터페이스 및 서브인터페이스, AE 인터페이스, VLAN 인터페이스, VPN 및 LSVPN 터널에 대한 터널 콘텐츠 검사를 지원합니다. 이 기능은 레이어 3, 레이어 2, 가상 와이어 및 탭 배포에서 지원됩니다. 터널 콘텐츠 검사는 공유 게이트웨이 및 가상 시스템 간 통신에서 작동합니다.

무엇을 알고 싶습니까?	참조:
터널 검사 정책을 만드는 데 사용할 수 있는 필드는 무엇입니까?	터널 검사 정책의 구성 요소
터널 검사 로그는 어떻게 볼 수 있습니까?	로그 유형 및 심각도 수준
더 찾고 계십니까?	터널 콘텐츠 검사

터널 검사 정책의 구성 요소

정책 > 터널 검사를 선택하여 터널 검사 정책 규칙을 추가합니다. 방화벽을 사용하여 일반 텍스트 터널 프로토콜(GRE, GTP-U, 암호화되지 않은 IPSec 및 VXLAN)의 콘텐츠를 검사하고 터널 콘텐츠 검사를 활용하여 이러한 유형의 터널에서 트래픽에 대한 보안, DoS 방어 및 QoS 정책을 시행할 수 있습니다. 모든 방화벽 모델은 GRE 및 암호화되지 않은 IPSec 터널의 터널 콘텐츠 검사를 지원하지만 GTP를 지원하는 방화벽만 GTP-U 터널의 터널 콘텐츠 검사를 지원합니다. 다음 표에서는 터널 검사 정책에 대해 구성하는 필드에 대해 설명합니다.

터널 검사 정책의 구성 요소	구성 위치	설명
이름	일반	영숫자 문자로 시작하고 0개 이상의 영숫자, 밑줄, 하이픈, 마침표 또는 공백 문자를 포함하는 터널 검사 정책의 이름을 입력합니다.
설명		(선택 사항) 터널 검사 정책에 대한 설명을 입력합니다.
태그		(선택 사항) 터널 검사 정책이 적용되는 패킷을 식별하는 보고 및 로깅 목적으로 하나 이상의 태그를 입력합니다.
태그별 그룹 규칙		유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화할 수 있습니다.
감사 코멘트		정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브		정책 규칙에 대한 이전 감사 코멘트를 봅니다. 감사 코멘트 아카이브를 CSV 형식으로 내보낼 수 있습니다.
소스 영역	소스	터널 검사 정책이 적용되는 패킷의 소스 영역을 하나 이상 추가합니다(기본값은 모두임).
소스 주소		(선택 사항) 터널 검사 정책이 적용되는 패킷의 소스 IPv4 또는 IPv6 주소, 주소 그룹 또는 지리적 지역 주소 개체를 추가합니다(기본값은 모두).
소스 사용자		(선택) 터널 검사 정책이 적용되는 패킷의 소스 사용자를 추가합니다(기본값은 모든).
무효		(선택 사항) 지정된 주소를 제외한 모든 주소를 선택하려면 무효를 선택합니다.
대상 영역	데스티네이션	터널 검사 정책이 적용되는 패킷의 대상 영역을 하나 이상 추가합니다(기본값은 모두임).

터널 검사 정책의 구성 요소	구성 위치	설명
대상 주소		(선택 사항) 터널 검사 정책이 적용되는 패킷의 대상 IPv4 또는 IPv6 주소, 주소 그룹 또는 지리적 지역 주소 개체를 추가합니다(기본값은 모두임).
무효		(선택 사항) 지정된 주소를 제외한 모든 주소를 선택하려면 무효를 선택합니다.
터널 프로토콜	점검	방화벽에서 검사할 하나 이상의 터널 프로토콜을 추가합니다. • **GRE** - 방화벽은 터널에서 일반 경로 캡슐화를 사용하는 패킷을 검사합니다. • **GTP-U** - 방화벽은 터널의 사용자 데이터(GTP-U)에 대해 GPRS(일반 패킷 무선 서비스) 터널링 프로토콜을 사용하는 패킷을 검사합니다. • 암호화되지 않은 **IPSec** - 방화벽은 터널에서 암호화되지 않은 IPSec(Null Encrypted IPSec 또는 전송 모드 AH IPSec)을 사용하는 패킷을 검사합니다. • **VXLAN** - 방화벽은 VXLAN 페이로드를 검사하여 터널 내에서 캡슐화된 콘텐츠 또는 애플리케이션을 찾습니다. 목록에서 프로토콜을 제거하려면 프로토콜을 선택한 다음 삭제합니다.
최대 터널 검사 수준	점검 > 검사 옵션	방화벽이 캡슐화의 **One Level**(기본값) 또는 **Two Level**(터널 내 터널)을 검사할지의 여부를 지정합니다. VXLAN의 경우 검사가 외부 레이어에서만 발생하므로 **One Level**을 선택합니다.
최대 터널 검사 수준을 초과하면 패킷 삭제		(선택 사항) 최대 터널 검사 수준에 대해 지정한 것보다 더 많은 캡슐화 수준이 포함된 패킷을 삭제합니다.
터널 프로토콜이 엄격한 헤더 검사에 실패하면 패킷 삭제		(선택 사항) 해당 프로토콜의 RFC와 호환되지 않는 헤더를 사용하는 터널 프로토콜이 포함된 패킷을 삭제합니다. 비준수 헤더는 의심스러운 패킷을 나타냅니다. 이 옵션을 사용하면 방화벽이 RFC 2890에 대해 GRE 헤더를 확인합니다.

터널 검사 정책의 구성 요소	구성 위치	설명
		방화벽이 *RFC 2890*보다 오래된 *GRE* 버전을 구현하는 디바이스로 *GRE*를 터널링하는 경우 이 옵션을 활성화하지 마십시오.
터널 내부의 알 수 없는 프로토콜인 경우 패킷 삭제		(선택 사항) 방화벽이 식별할 수 없는 터널 내부의 프로토콜이 포함된 패킷을 삭제합니다.
스캔한 VXLAN 터널을 소스로 반환		(선택 사항) 트래픽을 원래 VXLAN 터널 엔드포인트(VTEP)으로 반환하려면 이 옵션을 활성화합니다. 예를 들어, 이 옵션을 사용하여 캡슐화된 패킷을 소스 VTEP로 반환합니다. Layer 3, Layer 3 하위 인터페이스, Aggregate-Interface Layer 3 및 VLAN에서만 지원됩니다.
보안 옵션 활성화	점검 > 보안 옵션	(선택 사항) 터널 콘텐츠에 대한 별도의 보안 정책 처리를 위해 보안 영역을 할당하려면 보안 옵션을 활성화합니다. 내부 콘텐츠 소스는 지정한 터널 소스 영역에 속하고 내부 콘텐츠 대상은 지정한 터널 대상 영역에 속합니다. 보안 옵션을 활성화하지 않으면 기본적으로 내부 콘텐츠 소스은 외부 터널 소스과 동일한 영역에 속하고 내부 콘텐츠 대상은 외부 터널 대상과 동일한 영역에 속합니다. 따라서 내부 콘텐츠 소스과 대상 모두 외부 터널의 소스 및 대상 영역에 적용되는 동일한 보안 정책의 적용을 받습니다.
터널 소스 영역		보안 옵션을 활성화한 경우 생성한 터널 영역을 선택하면 내부 콘텐츠가 정책 시행을 위해 이 소스 영역을 사용합니다. 그렇지 않으면 기본적으로 내부 콘텐츠 소스는 외부 터널 소스과 동일한 영역에 속하며 외부 터널 소스 영역의 정책은 내부 콘텐츠 소스 영역에도 적용됩니다.
터널 목적지 구역		보안 옵션을 활성화한 경우 생성한 터널 영역을 선택하면 내부 콘텐츠가 정책 시행을 위해 이 대상 영역을 사용합니다.

터널 검사 정책의 구성 요소	구성 위치	설명
		그렇지 않으면 기본적으로 내부 콘텐츠 대상은 외부 터널 대상과 동일한 영역에 속하며 외부 터널 대상 영역의 정책은 내부 콘텐츠 대상 영역에도 적용됩니다.
모니터 이름	점검 > 모니터 옵션	(선택 사항) 로그 및 보고서의 트래픽을 모니터링하기 위해 유사한 트래픽을 함께 그룹화하려면 모니터 이름을 입력합니다.
모니터 태그(번호)		(선택 사항) 로깅 및 보고를 위해 유사한 트래픽을 함께 그룹화할 수 있는 모니터 태그 번호를 입력합니다(범위는 1~16,777,215). 태그 번호는 전역적으로 정의됩니다. 이 필드는 *VXLAN* 프로토콜에 적용되지 않습니다. *VXLAN* 로그는 *VXLAN* 헤더의 *VNI(VXLAN* 네트워크 식별자*)*를 자동으로 사용합니다.
세션 시작 시 로그인		(선택 사항) 터널 검사 정책과 일치하는 일반 텍스트 터널 세션 시작 시 로그를 생성하려면 이 옵션을 선택합니다. 이 설정은 세션에 적용되는 보안 정책 규칙의 세션 시작 시 기록 설정을 무시합니다. 터널 로그는 트래픽 로그와 별도로 저장됩니다. 외부 터널 세션(GRE, 암호화되지 않은 IPSec 또는 GTP-U) 정보는 터널 로그에 저장되고 내부 트래픽 플로우는 트래픽 로그에 저장됩니다. 이 분리를 통해 ACC 및 보고 기능을 사용하여 터널 활동(내부 콘텐츠 활동과 반대)에 대해 쉽게 보고할 수 있습니다. 터널 로그에 대한 모범 사례는 세션 시작 시 로깅 및 세션 종료 시 로깅입니다. 로깅의 경우 터널의 수명이 매우 길 수 있기 때문입니다. 예를 들어 *GRE* 터널은 라우터가 부팅될 때 나타나며 라우터가 재부팅될 때까지 종료되지 않습니다. 세션 시작 시 로그를 선택하지 않으면 *ACC*에 활성 *GRE* 터널이 있다는 것을 절대 볼 수 없습니다.

터널 검사 정책의 구성 요소	구성 위치	설명
세션 종료 시 로그인		(선택 사항) 터널 검사 정책과 일치하는 일반 텍스트 터널 세션 종료 시 로그를 캡처하려면 이 옵션을 선택합니다. 이 설정은 세션에 적용되는 보안 정책 규칙의 세션 종료 시 로그 설정보다 우선합니다.
로그 포워딩		(선택 사항) 드롭다운에서 로그 포워딩 프로파일을 선택하여 터널 검사 로그를 포워딩할 위치를 지정합니다. (이 설정은 트래픽 로그에 적용되는 보안 정책 규칙의 로그 포워딩 설정과 별개입니다.)
이름	터널 **ID** 기본적으로 VXLAN ID를 구성하지 않으면 모든 트래픽이 검사됩니다.	(선택 사항) 영숫자 문자로 시작하고 0개 이상의 영숫자, 밑줄, 하이픈, 마침표 및 공백 문자를 포함하는 이름입니다. 이름은 그룹화하는 VNI를 설명합니다. 이름은 편의를 위한 것이며 로깅, 모니터링 또는 보고의 요소가 아닙니다.
VXLAN ID(VNI)	VXLAN ID를 구성하면 이를 일치 기준으로 사용하여 특정 VNI에 대한 트래픽 검사를 제한할 수 있습니다.	(선택 사항) 단일 VNI, 쉼표로 구분된 VNI 목록, 최대 1600만 VNI 범위(하이픈을 구분 기호로 사용) 또는 이들의 조합을 입력합니다. 예: 1-54,1024,1677011-1677038,94 정책당 최대 VXLAN ID는 4,096입니다. 구성 메모리를 보존하려면 가능한 범위를 사용하십시오.
모두(모든 디바이스를 대상으로 함) Panorama 전용	대상	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스 Panorama 전용		정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그 Panorama 전용		지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅 Panorama 전용		선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > 애플리케이션 재정의

방화벽이 네트워크 트래픽을 애플리케이션으로 분류하는 방법을 변경하려면 애플리케이션 재정의 정책을 지정할 수 있습니다. 예를 들어 사용자 지정 애플리케이션 중 하나를 제어하려는 경우 애플리케이션 재정의 정책을 사용하여 영역, 소스 및 대상 주소, 포트 및 프로토콜에 따라 해당 애플리케이션의 트래픽을 식별할 수 있습니다. "알 수 없음"으로 분류된 네트워크 애플리케이션이 있는 경우 해당 애플리케이션에 대한 새 애플리케이션 정의를 만들 수 있습니다(애플리케이션 정의 참조).

가능하면 방화벽이 *App-ID*를 사용하여 애플리케이션을 식별하고 위협에 대한 레이어 *7* 검사를 수행하는 것을 방지하기 때문에 애플리케이션 재정의 정책을 사용하지 마십시오. 내부 독점 애플리케이션을 지원하려면 방화벽이 레이어 *7* 검사를 수행하고 애플리케이션 트래픽에서 위협을 검색하도록 애플리케이션 서명을 포함하는 사용자 지정 애플리케이션을 만드는 것이 좋습니다. 상업용 애플리케이션에 *App-ID*가 없는 경우 새 App-ID에 대한 요청을 제출하십시오. 공용 애플리케이션 정의*(*기본 포트 또는 서명*)*가 변경되어 방화벽이 더 이상 애플리케이션을 올바르게 식별하지 못하는 경우 *Palo Alto Networks*가 정의를 업데이트할 수 있도록 지원 티켓을 생성하십시오. 그동안 방화벽이 트래픽에 대한 레이어 *7* 검사를 계속 수행하도록 사용자 지정 애플리케이션을 만듭니다.

보안 정책과 마찬가지로 애플리케이션 재정의 정책은 필요에 따라 일반적이거나 구체적일 수 있습니다. 정책 규칙은 트래픽과 순서대로 비교되므로 보다 구체적인 규칙이 보다 일반적인 규칙보다 우선해야 합니다.

PAN-OS의 App-ID 엔진은 네트워크 트래픽에서 애플리케이션별 콘텐츠를 식별하여 트래픽을 분류하기 때문에 사용자 지정 애플리케이션 정의는 단순히 포트 번호를 사용하여 애플리케이션을 식별할 수 없습니다. 애플리케이션 정의에는 트래픽(소스 영역, 소스 IP 주소, 대상 영역 및 대상 IP 주소로 제한됨)도 포함되어야 합니다.

애플리케이션 재정의를 사용하여 사용자 지정 애플리케이션을 만들려면 다음을 수행합니다.

- 사용자 지정 애플리케이션을 만듭니다(애플리케이션 정의 참조). 애플리케이션이 애플리케이션 재정의 규칙에만 사용되는 경우 애플리케이션에 대한 서명을 지정할 필요가 없습니다.
- 사용자 지정 애플리케이션을 호출해야 하는 시기를 지정하는 애플리케이션 재정의 정책을 정의합니다. 정책에는 일반적으로 사용자 지정 애플리케이션을 실행하는 서버의 IP 주소와 제한된 소스 IP 주소 집합 또는 소스 영역이 포함됩니다.

다음 표를 사용하여 애플리케이션 재정의 규칙을 구성합니다.

- 애플리케이션 재정의 일반 탭
- 애플리케이션 재정의 소스 탭
- 애플리케이션 재정의 대상 탭
- 애플리케이션 재정의 프로토콜/애플리케이션 탭
- (Panorama만 해당) 애플리케이션 재정의 대상 탭

더 찾고 계십니까?

정책에서 애플리케이션 개체 사용을 참조하십시오.

애플리케이션 재정의 일반 탭

일반 탭을 선택하여 애플리케이션 재정의 정책에 대한 이름과 설명을 구성합니다. 많은 수의 정책이 있을 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수도 있습니다.

필드	설명
이름	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	규칙에 대한 설명을 입력합니다(최대 1024자).
태그	정책에 태그를 지정해야 하는 경우 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 DMZ에 대한 인바운드와 특정 보안 정책에 태그를 지정하거나, 복호화 및 복호화 금지라는 단어로 정책을 복호화하거나 해당 위치와 관련된 정책에 특정 데이터 센터의 이름을 사용할 수 있습니다.
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화하도록 선택할 수 있습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 주석을 입력합니다. 감사 댓글은 사례에 민감하며 문자, 숫자, 공간, 하이픈 및 밑줄이 될 수 있는 최대 256자까지 가질 수 있습니다.
코멘트 아카이브 감사	정책 규칙에 대한 이전 감사 코멘트를 봅니다. 감사 코멘트 아카이브는 CSV 형식으로 내보낼 수 있습니다.

애플리케이션 재정의 소스 탭

소스 탭을 선택하여 애플리케이션 재정의 정책이 적용될 수신 소스 트래픽을 정의하는 소스 영역 또는 소스 주소를 정의합니다.

필드	설명
소스 영역	소스 영역을 추가합니다(기본값은 모두). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을(를) 참조하십시오. 여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다.
소스 주소	소스 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 모두). 드롭다운에서 선택하거나 드롭다운 하단에서 주소, 주소 그룹 또는 지역을 클릭하고 설정을 지정합니다. 구성된 주소를 제외한 모든 주소를 선택하려면 무효를 선택하십시오.

애플리케이션 재정의 대상 탭

대상 탭을 선택하여 정책이 적용될 대상 트래픽을 정의하는 대상 영역 또는 대상 주소를 정의합니다.

필드	설명
대상 영역	추가를 클릭하여 대상 영역을 선택합니다(기본값은 모두임). 영역은 동일한 유형이어야 합니다(레이어 2, 레이어 3 또는 가상 와이어). 새 영역을 정의하려면 네트워크 > 영역을(를) 참조하십시오. 여러 영역을 사용하여 관리를 단순화할 수 있습니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다.
대상 주소	추가를 클릭하여 대상 주소, 주소 그룹 또는 지역을 추가합니다(기본값은 모두). 드롭다운에서 선택하거나 드롭다운 하단에서 주소, 주소 그룹 또는 지역을 클릭하고 설정을 지정합니다. 구성된 주소를 제외한 모든 주소를 선택하려면 무효를 선택하십시오.

애플리케이션 재정의 프로토콜/애플리케이션 탭

프로토콜/애플리케이션 탭을 선택하여 프로토콜(TCP 또는 UDP), 포트 및 정책 일치에 대한 애플리케이션의 속성을 추가로 정의하는 애플리케이션을 정의합니다.

필드	설명
프로토콜	애플리케이션 재정의를 허용할 프로토콜(**TCP** 또는 **UDP**)을 선택합니다.
포트	지정된 대상 주소에 대한 포트 번호(0 ~ 65535) 또는 포트 번호 범위(port1-port2)를 입력합니다. 여러 포트 또는 범위는 쉼표로 구분해야 합니다.
애플리케이션	위의 규칙 기준과 일치하는 트래픽 플로우에 대한 재정의 애플리케이션을 선택합니다. 사용자 지정 애플리케이션으로 재정의할 때 수행되는 위협 검사가 없습니다. 이에 대한 예외는 위협 검사를 지원하는 사전 정의된 애플리케이션으로 재정의하는 경우입니다. 새 애플리케이션을 정의하려면 개체 > 애플리케이션을 참조하세요.

애플리케이션 재정의 대상 탭

- (Panorama만 해당) 정책 > 적용 재정의 > 대상

대상 탭을 선택하여 정책 규칙을 푸시할 디바이스 그룹의 관리 방화벽을 선택합니다. 관리 방화벽을 선택하거나 태그를 지정하여 푸시할 관리 방화벽을 지정할 수 있습니다. 또한 지정된 방화벽을 제외한 모든 관리 방화벽에 푸시하도록 정책 규칙 대상을 구성할 수 있습니다.

NAT 규칙 - 대상 설정	설명
모두(모든 디바이스를 대상으로 함)	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스	정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그	지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > 인증

인증 정책을 사용하면 최종 사용자가 네트워크 리소스에 액세스하기 전에 인증할 수 있습니다.

무엇을 알고 싶습니까?	참조:
인증 규칙을 만드는 데 사용할 수 있는 필드는 무엇입니까?	인증 정책 규칙의 빌딩 블록
웹 인터페이스를 사용하여 인증 정책을 관리하려면 어떻게 해야 합니까?	인증 정책 생성 및 관리 Panorama의 경우 정책 규칙 이동 또는 복사를 참조하십시오.
더 찾고 계십니까?	인증 정책

인증 정책 규칙의 빌딩 블록

사용자가 리소스를 요청할 때마다(예: 웹 페이지를 방문할 때) 방화벽은 인증 정책을 평가합니다. 그런 다음 방화벽은 일치 정책 규칙에 따라 로그인 및 암호, 음성, SMS, 푸시 또는 OTP(일회성 암호) 인증과 같은 다양한 요인(유형)의 하나 이상의 챌린지에 응답하도록 사용자에게 프롬프트를 표시합니다. 사용자가 모든 요소에 응답한 후 방화벽은 보안 정책(정책 > 보안 참조)을 평가하여 리소스에 대한 액세스를 허용할지의 여부를 결정합니다.

방화벽은 사용자가 내부 또는 터널 모드에 있는 GlobalProtect™ 게이트웨이를 통해 웹 기반이 아닌 리소스(예: 프린터)에 액세스하는 경우 인증하라는 메시지를 표시하지 않습니다. 대신 사용자에게 연결 실패 메시지가 표시됩니다. 사용자가 이러한 리소스에 액세스할 수 있도록 하려면 인증 포털을 설정하고 연결 실패를 볼 때 방문하도록 사용자를 교육하십시오. 인증 포털을 설정하려면 *IT* 부서에 문의하십시오.

다음 표에서는 인증 정책 규칙의 각 구성 요소 또는 구성 요소에 대해 설명합니다. 규칙을 추가하기 전에 인증 정책 생성 및 관리에 설명된 전제 조건을 완료하십시오.

인증 규칙의 빌딩 블록	구성 위치	설명
규칙 번호	해당 사항 없음	각 규칙에는 자동으로 번호가 매겨지고 규칙이 이동되면 순서가 변경됩니다. 특정 필터와 일치하도록 규칙을 필터링하면 정책 > 인증 페이지에 규칙 베이스의 전체 규칙 집합 컨텍스트에서 번호와 함께 각 규칙이 나열되고 평가 순서에서 해당 위치가

인증 규칙의 빌딩 블록	구성 위치	설명
		표시됩니다. 자세한 내용은 규칙 순서 및 평가 순서 를 참조하세요.
이름	일반	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명		규칙에 대한 설명을 입력합니다(최대 1024자).
태그		규칙을 정렬하고 필터링하기 위한 태그를 선택합니다(개체 > 태그 참조).
태그별 그룹 규칙		유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화할 수 있습니다.
감사 코멘트		정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브		정책 규칙에 대한 이전 감사 코멘트를 봅니다. 감사 코멘트 아카이브를 CSV 형식으로 내보낼 수 있습니다.
소스 영역	소스	지정한 영역의 인터페이스에서 들어오는 트래픽에만 규칙을 적용하려면 영역을 추가합니다(기본값은 **any**). 새 영역을 정의하려면 네트워크 > 영역을 참조하십시오.
소스 주소		지정한 소스에서 발생하는 트래픽에만 규칙을 적용하려면 주소 또는 주소 그룹을 추가합니다(기본값은 모두). 선택한 주소를 제외한 모든 주소를 선택하려면 무효를 선택합니다.

인증 규칙의 빌딩 블록	구성 위치	설명
		새 주소 또는 주소 그룹을 정의하려면 개체 > 주소 및 개체 > 주소 그룹을 참조하십시오.
소스 사용자	사용자	규칙을 적용할 소스 사용자 또는 사용자 그룹을 선택합니다. • 모두 - 소스 사용자에 관계없이 모든 트래픽을 포함합니다. • 사전 로그온 - 클라이언트 시스템에 로그인하지 않았지만 클라이언트 시스템이 GlobalProtect 사전 로그온 기능 을 통해 네트워크에 연결하는 원격 사용자를 포함합니다. • 알려진 사용자 - 규칙이 인증을 유발하기 전에 방화벽에 이미 IP 주소-사용자명 매핑이 있는 모든 사용자가 포함됩니다. • **unknown** - 방화벽에 IP 주소-사용자명 매핑이 없는 모든 사용자가 포함됩니다. 규칙이 인증을 유발한 후 방화벽은 입력한 사용자명을 기반으로 알 수 없는 사용자에 대한 사용자 매핑을 생성합니다. • 선택 - 소스 사용자 목록에 추가한 사용자 및 사용자 그룹만 포함합니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS, TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.
소스 HIP 프로파일		최신 보안 패치 및 바이러스 백신 정의가 있는지의 여부와 같은 최종 호스트의 보안 상태에 대한 정보를 수집할 수 있도록 HIP(호스트 정보 프로파일)를 추가합니다. 자세한 내용과 새 HIP를 정의하려면 개체 > GlobalProtect > HIP 프로파일을 참조하십시오.

인증 규칙의 빌딩 블록	구성 위치	설명
대상 영역	데스티네이션	지정한 영역의 인터페이스로 가는 트래픽에만 규칙을 적용하려면 영역을 추가합니다(기본값은 모두). 새 영역을 정의하려면 네트워크 > 영역을 참조하십시오.
대상 주소		지정한 대상에만 규칙을 적용하려면 주소 또는 주소 그룹을 추가합니다(기본값은 모두). 선택한 주소를 제외한 모든 주소를 선택하려면 무효를 선택합니다. 새 주소 또는 주소 그룹을 정의하려면 개체 > 주소 및 개체 > 주소 그룹을 참조하십시오.
서비스	서비스/**URL** 카테고리	특정 TCP 및 UDP 포트 번호의 서비스에만 규칙을 적용하려면 다음 옵션 중에서 선택합니다. • 모두 - 모든 포트에서 모든 프로토콜을 사용하는 서비스를 지정합니다. • 기본값 - Palo Alto Networks가 정의하는 기본 포트에서만 서비스를 지정합니다. • 선택 - 서비스 또는 서비스 그룹을 추가할 수 있습니다. 새 서비스 및 서비스 그룹을 만들려면 개체 > 서비스 및 개체 > 서비스 그룹을 참조하십시오. 기본 선택은 ***service-http***입니다. 인증 포털에 대한 인증 정책을 사용하는 경우 방화벽이 모든 웹 트래픽에 대한 사용자-*IP*-주소 매핑을 학습하도록 ***service-https***도 활성화합니다.
URL 카테고리		규칙이 적용되는 URL 카테고리를 선택합니다. • URL 카테고리에 관계없이 모든 트래픽을 지정하려면 모두를 선택합니다. • 카테고리를 추가합니다. 사용자 정의 카테고리를 정의하려면 개체 > 사용자 정의 개체 > URL 카테고리를 참조하십시오.
인증 시행	작업	방법(예: 인증 포털 또는 브라우저 챌린지)과 방화벽이 사용자를 인증하는 데 사용하는 인증 프로파일을 지정하는 인증 적용 개체(개체 > 인증)를 선택합니다. 인증

인증 규칙의 빌딩 블록	구성 위치	설명
		프로파일은 사용자가 단일 챌린지에 응답할지 아니면 다단계 인증에 응답할지 정의합니다(디바이스 > 인증 프로파일 참조). 사전 정의된 또는 사용자 지정 인증 적용 개체를 선택할 수 있습니다. 인증 포털 정책에서 호스트 또는 서버를 제외해야 하는 경우 인증 시행으로 ***no-captive-portal***을 지정하는 인증 프로파일에 추가하십시오. 그러나 인증 포털 정책은 방화벽이 사용자-*IP*-주소 매핑을 학습하는 데 도움이 되며 가능한 경우 사용해야 합니다.
타임아웃		사용자 워크플로를 방해하는 인증 문제의 빈도를 줄이려면 방화벽이 리소스에 대한 반복적인 액세스에 대해 한 번만 인증하도록 사용자에게 묻는 인터벌(기본값은 60)을 지정할 수 있습니다. 인증 시행 개체가 다중 요소 인증을 지정하는 경우 사용자는 각 요소에 대해 한 번씩 인증해야 합니다. 방화벽은 타임스탬프를 기록하고 요소에 대한 타임아웃가 만료된 경우에만 챌린지를 다시 발행합니다. 타임스탬프를 다른 방화벽에 재배포 하면 처음에 사용자에 대한 액세스를 허용하는 방화벽이 나중에 해당 사용자에 대한 액세스를 제어하는 방화벽이 아니더라도 타임아웃을 적용할 수 있습니다.

인증 규칙의 빌딩 블록	구성 위치	설명
		타임아웃는 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 경계와 사용자 경험이 핵심인 기업에 올바른 선택입니다. 경계 리소스의 경우 값을 *480*분(*8*시간)으로 설정하고 데이터 센터 리소스 및 중요 시스템의 경우 *60*분과 같이 더 낮은 값을 설정하여 보안을 강화합니다. 필요에 따라 값을 모니터링하고 조정합니다.
로그 인증 타임아웃		인증 요소와 연결된 타임아웃가 만료될 때마다 방화벽이 인증 로그를 생성하도록 하려면 이 옵션(기본적으로 비활성화됨)을 선택합니다. 이 옵션을 활성화하면 액세스 문제를 해결하는 데 더 많은 데이터가 제공됩니다. 상관 관계 개체와 함께 인증 로그를 사용하여 네트워크에서 의심스러운 활동(예: 무차별 대입 공격)을 식별할 수도 있습니다. 이 옵션을 활성화하면 로그 트래픽이 증가합니다.
로그 포워딩		방화벽이 인증 로그를 Panorama 또는 syslog 서버와 같은 외부 서비스로 포워딩하도록 하려면 로그 포워딩 프로파일을 선택하십시오(개체 > 로그 포워딩 참조).
모두(모든 디바이스를 대상으로 함) Panorama 전용	대상	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스		정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.

인증 규칙의 빌딩 블록	구성 위치	설명
Panorama 전용		
태그 Panorama 전용		지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅 Panorama 전용		선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

인증 정책 생성 및 관리

정책 > 인증 페이지를 선택하여 인증 정책 규칙을 만들고 관리합니다.

업무	설명
추가하다	인증 정책 규칙을 생성하기 전에 다음 사전 요구 사항을 수행하십시오. ❑ User-ID™ 인증 포털 설정을 구성합니다(디바이스 > 사용자 식별 > 인증 포털 설정 참조). 방화벽은 인증 포털을 사용하여 인증 규칙에 필요한 첫 번째 인증 요소를 표시합니다. 또한 인증 포털을 사용하면 방화벽이 인증 타임아웃 기간과 관련된 타임스탬프를 기록하고 사용자 매핑을 업데이트할 수 있습니다. ❑ 방화벽이 사용자를 인증할 서비스에 액세스하는 방법을 지정하는 서버 프로파일을 구성합니다(디바이스 > 서버 프로파일 참조). ❑ 인증 설정을 지정하는 인증 프로파일에 서버 프로파일을 할당합니다(디바이스 > 인증 프로파일 참조). ❑ 인증 방법을 지정하는 인증 적용 개체에 인증 프로파일을 할당합니다(개체 > 인증 참조). 규칙을 생성하려면 다음 단계 중 하나를 수행한 후 인증 정책 규칙의 빌딩 블록에 설명된 필드를 완료하십시오. • 추가를 클릭합니다. • 새 규칙의 기반이 될 규칙을 선택한 다음 규칙 복사를 클릭합니다. 방화벽은 선택한 규칙 아래에 <rulename>#이라는 복사된 규칙을 삽입합니다. 여기서 #은 규칙 이름을 고유하게 만드는 다음으로 사용 가능한 정수이고 복제된 규칙에 대한 새 UUID를 생성합니다. 자세한 내용은 정책 규칙 이동 또는 복사를 참조하십시오.

업무	설명
수정	규칙을 수정하려면 규칙 이름을 클릭하고 인증 정책 규칙의 빌딩 블록에 설명된 필드를 편집합니다. 방화벽이 *Panorama*에서 규칙을 수신한 경우 규칙은 읽기 전용입니다. *Panorama*에서만 편집할 수 있습니다.
이동	트래픽을 일치시킬 때 방화벽은 정책 > 인증 페이지에 나열된 순서대로 위에서 아래로 규칙을 평가합니다. 평가 순서를 변경하려면 규칙을 선택한 다음 위로 이동, 아래로 이동, 맨 위로 이동 또는 맨 아래로 이동을 선택합니다. 자세한 내용은 정책 규칙 이동 또는 복사를 참조하십시오.
삭제	기존 규칙을 제거하려면 선택한 다음 삭제합니다.
활성화/비활성화	규칙을 비활성화하려면 규칙을 선택한 다음 비활성화합니다. 비활성화된 규칙을 다시 활성화하려면 해당 규칙을 선택한 다음 활성화합니다.
사용하지 않는 규칙 강조 표시	방화벽이 마지막으로 다시 시작된 이후로 트래픽과 일치하지 않는 규칙을 식별하려면 사용하지 않은 규칙을 강조 표시합니다. 그런 다음 사용하지 않는 규칙을 비활성화할지 삭제할지 결정할 수 있습니다. 페이지는 노란색 점선 배경으로 사용되지 않은 규칙을 강조 표시합니다.
미리보기 규칙(Panorama만 해당)	규칙 미리 보기를 클릭하여 관리되는 방화벽에 규칙을 푸시하기 전에 규칙 목록을 봅니다. 각 규칙 베이스 내에서 페이지는 여러 규칙을 쉽게 검색할 수 있도록 각 디바이스 그룹(및 관리 방화벽)에 대한 규칙 레이어를 시각적으로 구분합니다.

정책 > DoS 방어

DoS 방어 정책을 사용하면 소스 인터페이스, 영역, 주소 또는 사용자 및/또는 대상 인터페이스, 영역 또는 사용자와 일치하는 패킷을 거부하거나 허용할지의 여부를 지정하여 DoS 공격으로부터 개별 중요 리소스를 보호할 수 있습니다.

또는 보호 조치를 선택한 다음 경보를 트리거하는 임계값(초당 세션 또는 패킷)을 설정하고 보호 조치를 활성화하고 모든 새 연결이 삭제되는 최대 속도를 나타내는 DoS 프로파일을 지정할 수 있습니다. 따라서 통합 세션 또는 소스 및/또는 대상 IP 주소를 기반으로 인터페이스, 영역, 주소 및 국가 간의 세션 수를 제어할 수 있습니다. 예를 들어 특정 주소나 주소 그룹, 특정 사용자 및 특정 서비스에 대한 트래픽을 제어할 수 있습니다.

방화벽은 보안 정책 규칙보다 먼저 DoS 방어 정책 규칙을 적용하여 방화벽이 리소스를 가장 효율적인 방식으로 사용하도록 합니다. DoS 방어 정책 규칙이 패킷을 거부하는 경우 해당 패킷은 보안 정책 규칙에 도달하지 않습니다.

다음 표에서는 DoS 방어 정책 설정에 대해 설명합니다.

- DoS 방어 일반 탭
- DoS 방어 소스 탭
- DoS 방어 대상 탭
- DoS 방어 옵션/보호 탭
- (Panorama만 해당) DoS 방어 대상 탭

더 찾고 계십니까?

DoS 방어 프로파일 및 개체 > 보안 프로파일 > DoS 방어를 참조하십시오.

DoS 방어 일반 탭

- 선언 > **DoS** 보호 > 일반

일반 탭을 선택하여 DoS 방어 정책의 이름과 설명을 구성합니다. 정책이 여러 개 있을 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수도 있습니다.

필드	설명
이름	DoS 방어 정책 규칙을 식별할 이름을 입력합니다. 이름은 대소문자를 구분하며 최대 63자를 사용할 수 있으며 문자, 숫자, 공백, 하이픈 및 밑줄로 지정할 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	규칙에 대한 설명을 입력합니다 (최대 1024자).

필드	설명
태그	정책에 태그를 지정하려면 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구문입니다. 태그는 여러 정책을 정의했으며 특정 키워드로 태그가 지정된 정책을 보려는 경우에 유용합니다. 예를 들어 특정 보안 정책에 Inbound to DMZ로 태그를 지정하거나, 복호화 또는 복호화 안 함이라는 단어로 복호화 정책에 태그를 지정하거나, 해당 위치와 연결된 정책에 특정 데이터 센터의 이름을 사용할 수 있습니다.
태그별 규칙 그룹화	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화할 수 있습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. CSV 형식으로 감사 코멘트 아카이브를 내보낼 수 있습니다.

DoS 방어 소스 탭

소스 탭을 선택하여 소스 인터페이스 또는 소스 영역을 정의하고 선택적으로 DoS 정책 규칙이 적용되는 수신 트래픽을 정의하는 소스 주소 및 소스 사용자를 정의합니다.

필드	설명
유형	DoS 방어 정책 규칙이 적용되는 소스 유형을 선택합니다. • 인터페이스 - 지정된 인터페이스 또는 인터페이스 그룹에서 오는 트래픽에 규칙을 적용합니다. • 영역 - 지정된 영역의 인터페이스에서 오는 트래픽에 규칙을 적용합니다. 추가를 클릭하여 여러 인터페이스 또는 영역을 선택합니다.
소스 주소	모두 또는 추가를 선택한 다음 DoS 방어 정책 규칙이 적용되는 하나 이상의 소스 주소를 지정합니다. (선택 사항) 지정된 주소를 제외한 모든 주소에 규칙이 적용되도록 지정하려면 무효를 선택합니다.
소스 사용자	DoS 방어 정책 규칙이 적용되는 하나 이상의 소스 사용자를 지정합니다. • **any** - 소스 사용자에 관계없이 패킷을 포함합니다.

필드	설명
	• 사전 로그온 - GlobalProtect를 사용하여 네트워크에 연결되었지만 시스템에 로그인하지 않은 원격 사용자의 패킷을 포함합니다. GlobalProtect 앱용 포털에서 사전 로그온이 구성되면 현재 컴퓨터에 로그인하지 않은 사용자는 사전 로그온 사용자 명으로 식별됩니다. 그런 다음 사전 로그온 사용자에 대한 정책을 만들 수 있으며 사용자가 직접 로그인하지 않더라도 해당 컴퓨터는 마치 완전히 로그인한 것처럼 도메인에서 인증됩니다. • 알려진 사용자 - 모든 인증된 사용자를 포함합니다. 즉, 매핑된 사용자 데이터가 있는 모든 IP 주소를 의미합니다. 이 옵션은 도메인의 "도메인 사용자" 그룹과 동일합니다. • **unknown** - 인증되지 않은 모든 사용자를 포함합니다. 즉, 사용자에게 매핑되지 않은 IP 주소를 의미합니다. 예를 들어, 게스트 수준 액세스에 대해 **unknown**을 사용할 수 있습니다. 그 이유는 네트워크에 IP 주소가 있지만 도메인에 대해 인증되지 않고 방화벽에 IP 주소-사용자명 매핑 정보가 없기 때문입니다. • 선택 - 이 창에 지정된 사용자를 포함합니다. 예를 들어 사용자 한 명, 개인 목록, 일부 그룹을 선택하거나 수동으로 사용자를 추가할 수 있습니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS, TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.

DoS 방어 대상 탭

대상 탭을 선택하여 정책이 적용되는 대상 트래픽을 정의하는 대상 영역 또는 인터페이스 및 대상 주소를 정의합니다.

필드	설명
유형	DoS 방어 정책 규칙이 적용되는 대상 유형을 선택합니다. • 인터페이스 - 지정된 인터페이스 또는 인터페이스 그룹으로 가는 패킷에 규칙을 적용합니다. 추가를 클릭하고 하나 이상의 인터페이스를 선택합니다. • 영역 - 지정된 영역의 인터페이스로 가는 패킷에 규칙을 적용합니다. 추가를 클릭하고 하나 이상의 영역을 선택합니다.
대상 주소	모두 또는 추가를 선택한 다음 DoS 방어 정책 규칙이 적용되는 하나 이상의 대상 주소를 지정합니다. (선택 사항) 지정된 주소를 제외한 모든 주소에 규칙이 적용되도록 지정하려면 무효를 선택합니다.

DoS 방어 옵션/보호 탭

옵션/보호 탭을 선택하여 규칙이 적용되는 서비스 유형, 규칙과 일치하는 패킷에 대해 수행할 작업 및 일치하는 트래픽에 대해 로그 포워딩을 트리거할지의 여부와 같은 DoS 방어 정책 규칙에 대한 옵션을 구성합니다. 규칙이 활성화되는 일정을 정의할 수 있습니다.

또한 임계값 비율을 결정하는 집계 DoS 보호 프로파일 및/또는 분류된 DoS 보호 프로필을 선택할 수 있습니다. 이 프로파일은 초과 시 방화벽이 경보 트리거와 같은 보호 조치를 취하고 임의 조기 삭제 및 최대 임계값 비율을 초과하는 드롭 패킷과 같은 조치를 활성화하도록 합니다.

필드	설명
서비스	추가를 클릭하고 DoS 방어 정책이 적용되는 서비스를 하나 이상 선택합니다. 기본값은 모든 서비스입니다. 예를 들어 DoS 정책이 웹 서버를 보호하는 경우 웹 애플리케이션에 대해 HTTP, HTTPS 및 기타 적절한 서비스 포트를 지정합니다. 중요 서버의 경우 별도의 *DoS* 방어 규칙을 만들어 사용하지 않는 서비스 포트를 보호하여 표적 공격을 방지하십시오.
동작	DoS 방어 정책 규칙과 일치하는 패킷에 대해 방화벽이 수행하는 작업을 선택합니다. • 거부 - 규칙과 일치하는 모든 패킷을 삭제합니다. • 허용 - 규칙과 일치하는 모든 패킷을 허용합니다. • 보호 - 규칙과 일치하는 패킷에 대해 지정된 DoS 방어 프로파일에 지정된 보호를 적용합니다. 규칙과 일치하는 패킷은 DoS 방어 프로파일의 임계값 비율에 포함되어 차례로 경보를 트리거하고, 다른 작업을 활성화하고, 최대 비율을 초과하면 패킷 삭제를 트리거합니다. *DoS Protection*을 적용하는 목적은 *DoS* 공격으로부터 보호하는 것이므로 일반적으로 ***Protect***를 사용해야 합니다. 거부는 *DoS* 트래픽과 함께 합법적인 트래픽을 삭제하고 허용은 *DoS* 공격을 중지하지 않습니다. 그룹 내에서 예외를 만들려면 거부 및 허용만 사용합니다. 예를 들어 대부분의 그룹에서 오는 트래픽은 거부하지만 해당 트래픽의 하위 집합은 허용하거나 대부분의 그룹에서 오는 트래픽은 허용하지만 해당 트래픽의 하위 집합은 거부할 수 있습니다.
일정	DoS Protection 정책 규칙이 적용되는 일정을 지정합니다. 없음의 기본 설정은 일정이 없음을 나타냅니다. 정책은 항상 유효합니다. 또는 일정을 선택하거나 새 일정을 만들어 DoS 방어 정책 규칙이 적용되는 시기를 제어합니다. 일정의 이름을 입력합니다. 다중 가상 시스템 방화벽의 모든 가상 시스템과 이 일정을 공유하려면 공유를 선택합니다. 매일, 매주 또는 비반복 중 반복을 선택합니다. 24시간제를 기준으로 시작 시간 및 종료 시간을 시:분 단위로 추가합니다.

필드	설명
로그 포워딩	일치하는 트래픽에 대한 위협 로그 항목을 syslog 서버 또는 Panorama와 같은 외부 서비스로 포워딩하도록 트리거하려면 로그 포워딩 프로파일을 선택하거나 프로파일을 클릭하여 새 프로파일을 만듭니다. 방화벽은 규칙의 작업과 일치하는 트래픽만 기록하고 포워딩합니다. 더 쉬운 관리를 위해 *DoS* 로그를 다른 위협 로그와 별도로 이메일을 통해 관리자에게 직접 포워딩하고 로그 서버에 포워딩합니다.
통합	DoS Protection 프로파일 통합은 해당 서버 그룹을 보호하기 위해 DoS Protection 규칙에 지정된 결합된 디바이스 그룹에 적용되는 임계값을 설정합니다. 예를 들어 경보율 임계값이 10,000 CPS인 경우 전체 그룹에 대한 총 신규 CPS가 10,000CPS를 초과하면 방화벽이 경보 메시지를 트리거함을 의미합니다. 초당 들어오는 연결이 경보를 트리거하고, 작업을 활성화하고, 최대 속도를 초과하는 임계값 비율을 지정하는 Aggregate DoS Protection 프로파일을 선택합니다. 들어오는 모든 연결(통합)은 DoS Protection 통합 프로파일에 지정된 임계값에 포함됩니다. 없음의 통합 프로파일 설정은 통합 트래픽에 대한 임계값 설정이 없음을 의미합니다. 개체 > 보안 프로파일 > DoS 방어를 참조하십시오.
분류됨	분류된 DoS 방어 프로파일은 개별 또는 소규모 중요 서버 그룹을 보호하기 위해 DoS 방어 규칙에 지정된 각 개별 디바이스에 적용되는 임계값을 설정합니다. 예를 들어 경보율 임계값이 10,000CPS인 경우 규칙에 지정된 개별 서버에 대한 총 새 CPS가 10,000CPS를 초과하면 방화벽이 경보 메시지를 트리거함을 의미합니다. 이 옵션을 선택한 후 다음을 지정합니다. • 프로파일 - 이 규칙에 적용할 분류된 DoS 방어 프로파일을 선택합니다. • 주소 - 들어오는 연결이 **source-ip-only**, **destination-ip-only** 또는 **src-dest-ip-both**와 일치하는 경우 프로파일의 임계값에 포함되는지의 여부를 선택합니다. 방화벽은 소스 *IP*만 추적하거나 대상 *IP* 카운터만 추적하는 것보다 ***src-dest-ip-both*** 카운터를 추적하는 데 더 많은 리소스를 소비합니다. 분류된 DoS 방어 프로파일을 지정하면 소스 IP 주소, 대상 IP 주소 또는 소스 및 대상 IP 주소 쌍과 일치하는 들어오는 연결만 프로파일에 지정된 임계값에 포함됩니다. 예를 들어 최대 속도가 100cps인 분류된 DoS 방어 프로파일을 지정하고 규칙에서 주소 설정을 **source-ip-only**로 지정할 수 있습니다. 결과는 해당 특정 소스 IP 주소에 대해 초당 100개의 연결 제한이 됩니다.

필드	설명
	방화벽이 가능한 모든 인터넷 *IP* 주소에 대한 카운터를 저장할 수 없기 때문에 인터넷 연결 영역에 대해 ***source-ip-only*** 또는 ***src-dest-ip-both***를 사용하지 마십시오. 경계 영역에서 ***destination-ip-only***를 사용합니다. 개별 중요 디바이스를 보호하려면 ***destination-ip-only***를 사용하십시오. 소스 ***IP*** 전용 및 경보 임계값을 사용하여 인터넷에 연결되지 않은 영역에서 의심스러운 호스트를 모니터링합니다. 개체 > 보안 프로파일 > DoS 방어를 참조하십시오.

DoS 방어 대상 탭

- (Panorama 전용) 정책 > **DoS Protection** > **Target**

대상 탭을 선택하여 정책 규칙을 푸시할 디바이스 그룹의 관리 방화벽을 선택합니다. 관리 방화벽을 선택하거나 태그를 지정하여 푸시할 관리 방화벽을 지정할 수 있습니다. 또한 지정된 방화벽을 제외한 모든 관리 방화벽에 푸시하도록 정책 규칙 대상을 구성할 수 있습니다.

NAT 규칙 - 대상 설정	설명
모두(모든 디바이스를 대상으로 함)	디바이스 그룹의 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(확인)합니다.
디바이스	정책 규칙을 푸시할 디바이스 그룹과 연결된 하나 이상의 관리 방화벽을 선택합니다.
태그	지정된 태그가 있는 디바이스 그룹의 관리 방화벽에 정책 규칙을 푸시하려면 하나 이상의 태그를 추가하십시오.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외하고 디바이스 그룹과 연결된 모든 관리 방화벽에 정책 규칙을 푸시하려면 활성화(선택)합니다.

정책 > SD-WAN

SD-WAN 정책을 추가하여 구성한 상태 지터, 대기 시간 및 패킷 손실 상태 메트릭을 기반으로 애플리케이션별 또는 동일한 링크를 통과하는 애플리케이션 그룹에 대한 링크 경로 관리 설정을 구성합니다. 중요 애플리케이션의 소스와 대상 사이의 특정 경로가 저하되면 SD-WAN 정책 규칙은 민감한 애플리케이션과 중요 애플리케이션이 SD-WAN 정책 규칙에서 할당된 경로 품질 프로파일에 따라 수행하도록 보장하는 새로운 최적 경로를 선택합니다.

- SD-WAN 일반 탭
- SD-WAN 소스 탭
- SD-WAN 대상 탭
- SD-WAN 애플리케이션/서비스 탭
- SD-WAN 경로 선택 탭
- (Panorama만 해당) SD-WAN 대상 탭

SD-WAN 일반 탭

- 선언 > **SD-WAN** > 일반

일반 탭을 선택하여 SD-WAN 정책에 대한 이름과 설명을 구성합니다. 많은 수의 정책이 있을 때 정책을 정렬하거나 필터링할 수 있도록 태그를 구성할 수도 있습니다.

필드	설명
이름	규칙을 식별하기 위해 이름을 입력합니다. 이 이름은 대/소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄이 될 수 있는 최대 63자까지 가질 수 있습니다. 이름은 방화벽에서 고유해야 하며 Panorama에서는 디바이스 그룹 및 모든 조상 요소 또는 후손 요소 디바이스 그룹 내에서 고유해야 합니다.
설명	규칙에 대한 설명을 입력합니다(최대 1,024자).
태그	정책에 태그를 지정해야 하는 경우 태그를 추가하고 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 규칙이 적용되는 특정 허브 또는 브랜치를 식별하는 고유한 태그로 특정 SD-WAN 정책에 태그를 지정할 수 있습니다.

필드	설명
태그별 그룹 규칙	유사한 정책 규칙을 그룹화할 태그를 입력합니다. 그룹 태그를 사용하면 이러한 태그를 기반으로 정책 규칙 기준을 볼 수 있습니다. 태그에 따라 규칙을 그룹화하도록 선택할 수 있습니다.
감사 코멘트	정책 규칙의 생성 또는 편집을 감사하기 위해 코멘트를 입력합니다. 감사 코멘트는 대소문자에 민감하며 문자, 숫자, 공백, 하이픈 및 밑줄을 포함한 최대 256자까지 가질 수 있습니다.
감사 코멘트 아카이브	정책 규칙에 대한 이전 감사 코멘트를 봅니다. 감사 코멘트 아카이브는 CSV 형식으로 내보낼 수 있습니다.

SD-WAN 소스 탭

- 선언 > **SD-WAN** > 소스

SD-WAN 정책이 적용되는 들어오는 패킷을 정의하는 소스 영역, 소스 주소 및 소스 사용자를 정의하려면 소스 탭을 선택합니다.

필드	설명
소스 영역	소스 영역을 지정하려면 하나 이상의 영역을 추가 및 선택 또는 모든 영역을 선택합니다. 여러 영역을 지정하면 관리가 간소화될 수 있습니다. 예를 들어 다른 영역에 세 개의 브랜치가 있고 나머지 일치 조건 및 경로 선택이 세 가지에 대해 동일하게 지정하려면 SD-WAN 규칙 하나를 만들고 세 브랜치를 커버할 세 개의 소스 영역을 지정할 수 있습니다. *SD-WAN* 정책 규칙에 대해서만 레이어 *3* 유형 영역이 지원됩니다.
소스 주소	소스 주소를 지정하려면 소스 주소 또는 EDL(외부 동적 목록)을 추가하거나 드롭다운에서 선택하거나 주소를 선택한 다음 새 주소 개체를 만듭니다. 또는 모든 소스 주소(기본값)를 선택합니다.
소스 사용자	특정 사용자를 지정하려면 추가(그런 다음 유형은 선택을 나타냄)를 선택한 다음 사용자, 사용자 목록 또는 사용자 그룹을 입력합니다. 또는 사용자 유형을 선택합니다. • **any**—사용자 데이터에 관계없이 모든 사용자 포함(기본값).

필드	설명
	• 사전 로그온- GlobalProtect™를 사용하여 네트워크에 연결되어 있지만 시스템에 로그인되지 않은 원격 사용자를 포함합니다. 사전 로그온 옵션이 GlobalProtect 앱용 포털에 구성된 경우 현재 컴퓨터에 로그인하지 않은 사용자는 사전 로그온 사용자명으로 식별됩니다. 그런 다음 사전 로그온 사용자에 대한 정책을 생성할 수 있으며 사용자가 직접 로그인하지 않더라도 해당 컴퓨터는 완전히 로그인한 것처럼 도메인에서 인증됩니다. • 알려진 사용자-사용자 매핑된 모든 IP 주소를 의미하는 인증된 모든 사용자를 포함합니다. 이 옵션은 도메인의 "도메인 사용자" 그룹과 동일합니다. • **unknown** - 인증되지 않은 모든 사용자를 포함합니다. 즉, 사용자에게 매핑되지 않은 IP 주소를 의미합니다. 예를 들어 네트워크에 IP 주소가 있지만 도메인에 인증되지 않으며 방화벽에 IP 주소 간 매핑 정보가 없기 때문에 게스트 수준 액세스에 대해 알 수 없음을 선택할 수 있습니다. 방화벽이 *User-ID™* 에이전트가 아닌 *RADIUS*, *TACACS+* 또는 *SAML ID* 제공자 서버에서 사용자 정보를 수집하는 경우 사용자 목록이 표시되지 않습니다. 사용자 정보를 수동으로 입력해야 합니다.

SD-WAN 대상 탭

- 선언 > **SD-WAN** > 데스티네이션

대상 탭을 선택하여 SD-WAN 정책 규칙이 적용되는 트래픽을 정의하는 대상 영역 또는 대상 주소를 정의합니다.

필드	설명
대상 영역	대상 영역을 추가합니다(기본값은 any). 영역은 레이어 3이어야 합니다. 새 영역을 정의하려면 네트워크 > 영역을 참조합니다. 관리를 단순화하기 위해 여러 영역을 추가합니다. 예를 들어, 모두 신뢰할 수 없는 대상 영역으로 향하는 3개의 서로 다른 내부 영역(마케팅, 영업 및 홍보)이 있는 경우 모든 사례를 다루는 하나의 규칙을 만들 수 있습니다.
대상 주소	대상 주소, 주소 그룹, 외부 동적 목록(EDL) 또는 지역을 추가합니다(기본값은 모두). 드롭다운에서 선택하거나 드롭다운 하단의 주소 또는 주소 그룹을 클릭하고 설정을 지정합니다.

필드	설명
	구성된 주소를 제외한 모든 주소를 선택하려면 부정을 선택하십시오.

SD-WAN 애플리케이션/서비스 탭

- 선언 > **SD-WAN** > 애플리케이션/서비스

애플리케이션/서비스 탭을 선택하여 SD-WAN 정책 규칙이 적용되는 애플리케이션 또는 서비스를 지정하고 애플리케이션 또는 서비스에 적용되는 프로파일(경로 품질, SaaS 품질 및 오류 수정 프로파일)을 지정합니다.

필드	설명
경로 품질 프로파일	지정된 애플리케이션 및 서비스에 적용할 최대 지터, 대기 시간 및 패킷 손실 백분율 임계값을 결정하는 경로 품질 프로파일을 선택합니다. 경로 품질 프로파일이 아직 생성되지 않은 경우 새 **SD-WAN** 경로 품질 프로파일을 생성할 수 있습니다.
SaaS 품질 프로파일	SaaS(Software-as-a-Service) 애플리케이션에 대한 DIA(Direct Internet Access) 링크가 있는 허브 또는 브랜치 방화벽의 대기 시간, 지터 및 패킷 손실에 대한 경로 품질 임계값을 지정하려면 SaaS 품질 프로파일을 선택합니다. SaaS 품질 프로파일이 아직 생성되지 않은 경우 새 **SaaS** 품질 프로파일을 생성할 수 있습니다. 기본값은 없음**(**비활성화**)**입니다.
오류 수정 프로파일	오류 수정 프로파일을 선택하거나 규칙에 지정된 애플리케이션 또는 서비스에 대한 FEC(정방향 오류 수정) 또는 경로 복사를 제어하기 위한 매개변수를 지정하는 새 오류 수정 프로파일을 만듭니다. 이 프로파일은 허브 또는 브랜치 방화벽에서 사용할 수 있습니다. 기본값은 없음**(**비활성화**)**입니다.
애플리케이션	SD-WAN 정책 규칙에 대한 특정 애플리케이션을 추가하거나 모두를 선택합니다. 애플리케이션에 여러 기능이 있는 경우 전체 애플리케이션 또는 개별 기능을 선택합니다. 전체 애플리케이션을 선택하면 모든 기능이 포함되며 향후 기능이 추가되면 애플리케이션 정의가 자동으로 업데이트됩니다. SD-WAN 정책 규칙에서 애플리케이션 그룹, 필터 또는 컨테이너를 사용하는 경우 애플리케이션 열의 개체 위로 마우스를 가져간 다음 드롭다운을 열고 값을 선택하여 이러한 개체의 세부 정보를 봅니다. 이를 통해 개체 탭으로 이동할 필요 없이 정책에서 직접 애플리케이션 구성원을 볼 수 있습니다.

필드	설명
	대기 시간, 지터 또는 패킷 손실의 영향을 받는 비즈니스 크리티컬 애플리케이션만 추가합니다. 애플리케이션 카테고리 또는 하위 카테고리는 너무 광범위하고 애플리케이션별 제어를 허용하지 않으므로 추가하지 마십시오.
서비스	SD-WAN 정책 규칙에 대한 특정 서비스를 추가하고 이러한 서비스의 패킷을 허용 또는 거부할 포트를 선택합니다. • 임의 - 선택한 서비스가 임의의 프로토콜 또는 포트에서 허용되거나 거부됩니다. • **application-default** - 선택한 서비스는 **Palo Alto Networks®**에서 정의한 기본 포트에서만 허용되거나 거부됩니다. 이 옵션은 허용 작업을 지정하는 정책에 권장됩니다. 이 옵션은 의도하지 않은 경우 원치 않는 서비스 동작 및 사용의 징후가 될 수 있는 비정상적인 포트 및 프로토콜에서 서비스가 실행되지 않도록 하기 때문입니다. 이 옵션을 사용하면 기본 포트만 *SD-WAN* 정책과 일치하고 작업이 적용됩니다. 기본 포트에 없는 다른 서비스는 보안 정책 규칙에 따라 허용될 수 있지만 *SD-WAN* 정책과 일치하지 않으며 *SD-WAN* 정책 규칙 작업이 수행되지 않습니다. 대부분의 서비스에서 ***application-default***를 사용하여 서비스가 비표준 포트를 사용하거나 다른 회피 동작을 표시하지 못하도록 합니다. 서비스의 기본 포트가 변경되면 방화벽은 자동으로 규칙을 올바른 기본 포트로 업데이트합니다. 내부 사용자 지정 서비스와 같이 비표준 포트를 사용하는 서비스의 경우 서비스를 수정하거나 비표준 포트를 지정하는 규칙을 만들고 서비스가 필요한 트래픽에만 규칙을 적용합니다. • 선택 - 기존 서비스를 추가하거나 서비스 또는 서비스 그룹을 선택하여 새 항목을 지정합니다. (또는 개체 > 서비스 및 개체 > 서비스 그룹 선택).

SD-WAN 경로 선택 탭

- 선언 > **SD-WAN** > 경로 선택

경로 선택 탭을 선택하여 기본 경로 품질이 경로 품질 프로파일에 구성된 경로 품질 임계값을 초과하는 경우 스왑할 애플리케이션 또는 서비스 트래픽의 경로를 정의합니다.

필드	설명
트래픽 분포 프로파일	드롭다운에서 트래픽 분산 프로파일을 선택합니다. 이 프로파일은 기본 경로에 대한 경로 상태 메트릭 중 하나가 규칙에 대한 경로 품질 프로파일에 구성된 임계값을 초과할 때 방화벽이 애플리케이션 또는 서비스 트래픽에 대한 대체 경로를 선택하는 방법을 결정합니다.

SD-WAN 대상 탭

- 선언 > **SD-WAN** > 대상

대상 탭을 선택하여 SD-WAN 정책 규칙을 푸시할 관리되는 디바이스를 선택합니다. 이 탭은 Panorama 관리 서버에서만 지원됩니다.

필드	설명
모두(모든 디바이스를 대상으로 함)	Panorama 관리 서버에서 SD-WAN 정책 규칙을 모든 디바이스에 푸시하려면 활성화(확인)합니다.
디바이스	SD-WAN 정책 규칙을 푸시할 하나 이상의 디바이스를 선택합니다. 디바이스 상태, 플랫폼, 디바이스 그룹, 템플릿, 태그 또는 HA 상태를 기반으로 디바이스를 필터링할 수 있습니다.
태그	정책에 대한 태그를 지정합니다. 정책 태그는 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구입니다. 이 기능은 많은 정책을 정의하고 특정 키워드로 태그된 정책을 보려는 경우에 유용합니다. 예를 들어 특정 규칙에 Decrypt 및 No-decrypt와 같은 특정 단어로 태그를 지정하거나 해당 위치와 연결된 정책에 대해 특정 데이터 센터의 이름을 사용할 수 있습니다. 기본 규칙에 태그를 추가할 수도 있습니다.
지정된 디바이스 및 태그를 제외한 모든 대상 타겟팅	선택한 디바이스 및 태그를 제외한 모든 디바이스에 정책 규칙을 대상으로 지정하고 푸시하려면 활성화(확인)합니다.

개체

개체는 정책 규칙을 구성, 예약 및 검색할 수 있는 요소이며 보안 프로파일은 정책 규칙에서 위협 보호를 제공합니다.

이 섹션에서는 정책과 함께 사용할 수 있는 보안 프로파일 및 개체를 구성하는 방법에 대해 설명합니다.

- 개체 이동, 복사, 재정의 또는 되돌리기
- 개체>주소
- 개체>주소 그룹
- 개체>영역
- 개체>애플리케이션
- 개체>애플리케이션 그룹
- 개체>애플리케이션 필터
- 개체>서비스
- 개체>서비스그룹
- 개체>태그
- 개체 > 디바이스
- 개체>GlobalProtect> HIP 개체
- 개체>GlobalProtect> HIP 프로파일
- 개체>외부 동적 목록
- 개체>사용자 정의 개체
- 개체>보안 프로파일
- 개체 > 보안 프로파일 > 모바일 네트워크 보호
- 개체 > 보안 프로파일 > SCTP 보호
- 개체>보안 프로파일 그룹
- 개체>로그 포워딩
- 개체>인증
- 개체>복호화 프로파일
- 개체 > SD-WAN 링크 관리
- 개체>일정

개체 이동, 복사, 재정의 또는 되돌리기

기존 개체를 수정하는 옵션에 대한 다음 항목을 참조하십시오.

- 개체 이동 또는 복사
- 개체 재정의 또는 되돌리기

개체 이동 또는 복사

개체를 이동하거나 복제할 때 공유 위치를 포함하여 액세스 권한이 있는 대상(방화벽의 가상 시스템 또는 Panorama™의 장치 그룹)을 할당할 수 있습니다.

개체를 이동하려면 개체 탭에서 개체를 선택하고 이동을 클릭하고 다른 **vsys**로 이동(방화벽만)을 선택하거나 다른 기기 그룹(파노라마만 해당)으로 이동하고 다음 표의 필드를 완성한 다음 확인을 클릭합니다.

개체를 복사하려면 개체 탭에서 개체를 선택한 다음 복사를 클릭하고 다음 표의 필드를 완료한 다음 확인을 클릭합니다.

이동/복사 설정	설명
선택한 개체	작업에 대해 선택한 정책 또는 개체의 이름 및 현재 위치(가상 시스템 또는 디바이스 그룹)를 표시합니다.
데스티네이션	정책 또는 개체의 새 위치(가상 시스템, 디바이스 그룹 또는 공유)를 선택합니다. 기본 값은 정책 또는 개체 탭에서 선택한 가상 시스템 또는 디바이스 그룹입니다.
유효성 검사에서 처음 감지된 오류에 대한 오류 발생	이 옵션(기본적으로 선택됨)을 선택하여 방화벽 또는 Panorama가 찾은 첫 번째 오류를 표시하고 추가 오류 확인 작업을 중지합니다. 예를 들어 대상에 이동하는 정책 규칙에 참조되는 개체가 포함되어 있지 않으면 오류가 발생합니다. 이 선택을 취소하면 방화벽이나 Panorama를 표시하기 전에 모든 오류를 찾을 수 있습니다.

개체 재정의 또는 되돌리기

Panorama에서는 최대 4개 수준의 트리 레이어 구조에서 디바이스 그룹을 중첩할 수 있습니다. 하위 수준에서 디바이스 그룹은 하위 수준 디바이스 그룹이 정책 및 개체를 상속하는 상위 수준(집합적으로 상위라고 함)에 상위, 조부모 요소 및 증조부모 요소 디바이스 그룹을 가질 수 있습니다. 최상위 수준에서 디바이스 그룹에는 자식 요소, 손자 요소 및 증손자 요소 디바이스 그룹(집합적으로 하위 항목이라고 함)이 있을 수 있습니다. 하위 항목의 개체를 재정의하여 해당 값이 상위 항목의 개체와 다르도록 할 수 있습니다. 이 재정의 기능은 기본적으로 활성화되어 있습니다. 그러나 공유 또는 기본(미리 구성된) 개체를 재정의할 수 없습니다. 웹 인터페이스는 개체에 상속된 값이 있음을 나타내는 아이콘을 표시하고 상속된 개체에 재정의된 값이 있음을 나타내는 아이콘을 표시합니다.

- 개체 재정의 - 개체 탭을 선택한 다음 재정의된 버전이 있는 하위 디바이스 그룹을 선택한 다음 개체를 선택한 다음 재정의를 클릭하고 설정을 편집합니다. 개체에 대한 이름 또는 공유 설정을 재정의할 수 없습니다.
- 재정의된 개체를 상속된 값으로 되돌리기 - 개체 탭을 선택한 다음 재정의된 버전이 있는 디바이스 그룹을 선택하고 개체를 선택한 다음 되돌리기를 클릭하고 예를 클릭하여 작업을 확인합니다.
- 개체에 대한 재정의 비활성화 - 개체 탭을 선택한 다음 개체가 있는 디바이스 그룹을 선택한 다음 개체 이름을 클릭하여 편집하고 재정의 비활성화를 선택한 다음 확인을 클릭합니다. 그러면 선택한 디바이스 그룹에서 개체를 상속하는 모든 디바이스 그룹에서 해당 개체에 대한 재정의가 비활성화됩니다.
- **Panorama**의 모든 개체 재정의를 공유 위치 또는 상위 디바이스 그룹에서 상속된 값으로 교체 - **Panorama** > **Setup** > **Management**를 선택한 다음 Panorama 설정을 편집하고 상위 개체가 우선 적용을 선택한 다음 확인을 클릭합니다. 그런 다음 상속된 값을 푸시하려면 Panorama 및 재정의가 포함된 디바이스 그룹에 커밋해야 합니다.

개체 > 주소

주소 개체에는 IPv4 또는 IPv6 주소(단일 IP 주소, 주소 범위 또는 서브넷), FQDN 또는 와일드카드 주소(IPv4 주소 다음에 슬래시 및 와일드카드 마스크)가 포함될 수 있습니다. 주소 개체를 사용하면 각 인스턴스에 대해 수동으로 각 주소를 추가하지 않고도 정책 규칙, 필터 및 기타 방화벽 기능에서 소스 또는 대상 주소로 동일한 주소 또는 주소 그룹을 재사용할 수 있습니다. 웹 인터페이스 또는 CLI를 사용하여 주소 개체를 만듭니다. 변경 사항에는 개체를 구성의 일부로 만들기 위한 커밋 작업이 필요합니다.

먼저 새 주소 개체를 추가하고 다음 값을 지정합니다.

주소 개체 설정	설명
이름	이 개체의 일부로 포함할 주소를 설명하는 이름(최대 63자)을 입력합니다. 이 이름은 보안 정책 규칙을 정의할 때 주소 목록에 나타납니다. 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
공유	이 주소 개체를 다음과 공유하려면 이 옵션을 선택합니다. • 다중 가상 시스템 방화벽의 모든 가상 시스템**(vsys)** - 이 옵션을 선택하지 않으면 개체 탭에서 선택한 가상 시스템에서만 주소 개체를 사용할 수 있습니다. • **Panorama**의 모든 디바이스 그룹 - 이 옵션을 선택하지 않으면 개체 탭에서 선택한 디바이스 그룹에서만 주소 개체를 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 이 개체를 상속하는 디바이스 그룹에서 이 주소 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 기본적으로 이 선택은 비활성화되어 있으며, 이는 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
설명	개체에 대한 설명을 입력합니다(최대 1,023자).

유형	주소 개체 및 항목의 유형을 지정합니다.
	• **IP** 넷마스크 - *ip_address/mask* 또는 *ip_address*의 표기법을 사용하여 IPv4 또는 IPv6 주소 또는 IP 주소 범위를 입력하고, 여기서 마스크는 주소의 네트워크 부분에 사용되는 유효한 2진수의 수입니다. 이상적으로 IPv6 주소의 경우 호스트 부분이 아닌 네트워크 부분만 지정합니다. 예:
	  • **192.168.80.150/32** - 하나의 주소를 나타냅니다.
	  • **192.168.80.0/24** - 192.168.80.0에서 192.168.80.255까지의 모든 주소를 나타냅니다.
	  • **2001:db8::/32**

주소 개체 설정	설명
	• **2001:db8:123:1::/64** • **IP** 범위 - *ip_address*-*ip_address*의 형식을 사용하여 주소 범위를 입력하고, 여기서 범위의 양쪽 끝은 IPv4 주소이거나 둘 다 IPv6 주소입니다. 예: 2001:db8:123:1::1-2001:db8:123:1::22 • **IP** 와일드카드 마스크 - IPv4 주소 뒤에 슬래시와 마스크(0으로 시작해야 함)가 오는 형식으로 IP 와일드카드 주소를 입력합니다(예: 10.182.1.1/0.127.248.0). 와일드카드 마스크에서 0비트는 비교 중인 비트가 0으로 덮인 IP 주소의 비트와 일치해야 함을 나타냅니다. 마스크의 1비트는 와일드카드 비트입니다. 즉, 비교되는 비트가 1로 덮인 IP 주소의 비트와 일치할 필요가 없습니다. IP 주소와 와일드카드 마스크를 바이너리로 변환합니다. 일치를 설명하기 위해 바이너리 스니펫 0011에서 와일드카드 마스크 1010은 4개의 일치(0001, 0011, 1001 및 1011)를 생성합니다. 보안 정책 규칙에서만 *IP* 와일드카드 마스크 유형의 주소 개체를 사용할 수 있습니다. • **FQDN** - 도메인 이름을 입력합니다. FQDN은 처음에 커밋 시 확인됩니다. FQDN 항목은 TTL이 최소 FQDN 새로 고침 시간보다 크거나 같은 경우 FQDN의 TTL을 기반으로 후속적으로 새로 고쳐집니다. 그렇지 않으면 FQDN 항목이 최소 FQDN 새로 고침 시간에 새로 고쳐집니다. FQDN은 프록시가 구성된 경우 시스템 DNS 서버 또는 DNS 프록시 개체에 의해 확인됩니다.
해결	주소 유형을 선택한 다음 IP 주소 또는 FQDN을 입력한 후 확인을 클릭하여 연결된 FQDN 또는 IP 주소를 각각 확인합니다(방화벽 또는 Panorama의 DNS 구성 기반). FQDN에서 IP 넷마스크 또는 그 반대로 주소 개체를 변경할 수 있습니다. FQDN에서 IP 넷마스크로 변경하려면 확인을 클릭하여 FQDN이 확인되는 IP 주소를 확인한 다음 하나를 선택한 다음 이 주소를 사용합니다. 주소 개체 유형이 IP Netmask로 동적으로 변경되고 선택한 IP 주소가 텍스트 필드에 나타납니다. 또는 주소 개체를 IP 넷마스크에서 FQDN으로 변경하려면 확인을 클릭하여 IP 넷마스크가 확인되는 DNS 이름을 확인한 다음 FQDN을 선택한 다음 이 **FQDN** 사용을 선택합니다. 유형이 FQDN으로 변경되고 FQDN이 텍스트 필드에 나타납니다.
태그	이 주소 개체에 적용할 태그를 선택하거나 입력합니다. 여기에서 태그를 정의하거나 개체 > 태그 탭을 사용하여 새 태그를 생성할 수 있습니다.

개체 > 주소 그룹

보안 정책 생성을 단순화하기 위해 동일한 보안 설정이 필요한 주소를 주소 그룹으로 결합할 수 있습니다. 주소 그룹은 정적이거나 동적일 수 있습니다.

- 동적 주소 그룹: 동적 주소 그룹은 태그 및 태그 기반 필터 조회를 사용하여 구성원을 동적으로 채웁니다. 동적 주소 그룹은 가상 머신 위치/IP 주소가 자주 변경되는 광범위한 가상 인프라가 있는 경우 매우 유용합니다. 예를 들어, 정교한 페일오버 설정이 있거나 새 가상 머신을 자주 프로비저닝하고 방화벽의 구성/규칙을 수정하지 않고 새 머신에서 들어오고 나가는 트래픽에 정책을 적용하려고 합니다.

  정책에서 동적 주소 그룹을 사용하려면 다음 작업을 완료해야 합니다.

  - 동적 주소 그룹을 정의하고 정책 규칙에서 참조하십시오.
  - IP 주소와 해당 태그를 방화벽에 알려 동적 주소 그룹의 구성원을 구성할 수 있도록 합니다. 방화벽에서 XML API를 사용하는 외부 스크립트를 사용하여 이 작업을 수행하거나 VMware 기반 환경의 경우 **Device** > **VM** 정보 소스를 선택하여 방화벽에서 설정을 구성할 수 있습니다.

  동적 주소 그룹에는 정적으로 정의된 주소 개체도 포함될 수 있습니다. 주소 개체를 만들고 동적 주소 그룹에 할당한 것과 동일한 태그를 적용하면 해당 동적 주소 그룹에는 태그와 일치하는 모든 정적 및 동적 개체가 포함됩니다. 따라서 태그를 사용하여 동일한 주소 그룹에 있는 동적 개체와 정적 개체를 모두 함께 가져올 수 있습니다.
- 고정 주소 그룹: 정적 주소 그룹은 정적 동적 주소 그룹인 주소 개체를 포함하거나 주소 개체와 동적 주소 그룹의 조합일 수 있습니다.

  주소 그룹을 만들려면 추가를 클릭하고 다음 필드를 채우십시오.

주소 그룹 설정	설명
이름	주소 그룹을 설명하는 이름을 입력합니다(최대 **63**자). 이 이름은 보안 정책을 정의할 때 주소 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유	주소 그룹을 다음에 사용할 수 있게 하려면 이 옵션을 선택하십시오. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 주소 그룹을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에서만 주소 그룹을 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 주소 그룹 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.

주소 그룹 설정	설명
설명	개체에 대한 설명을 입력합니다(최대 1023자).
유형	정적 또는 동적을 선택합니다. 동적 주소 그룹을 만들려면 일치 기준을 사용하여 그룹에 포함할 구성원을 조합합니다. **AND** 또는 **OR** 연산자를 사용하여 일치 기준을 정의합니다. 부정은 지원되지 않습니다. 일치 기준에 대한 속성 목록을 보려면 소스/호스트에서 속성에 액세스하고 검색하도록 방화벽을 구성해야 합니다. 구성된 정보 소스의 각 가상 머신은 방화벽에 등록되고 방화벽은 방화벽을 수정하지 않고도 *IP* 주소 또는 구성의 변경 사항을 검색하기 위해 머신을 폴링할 수 있습니다. 고정 주소 그룹의 경우 추가를 클릭하고 하나 이상의 주소를 선택합니다. 추가를 클릭하여 주소 그룹에 개체 또는 주소 그룹을 추가합니다. 그룹은 주소 개체와 정적 및 동적 주소 그룹을 모두 포함할 수 있습니다.
태그	이 주소 그룹에 적용할 태그를 선택하거나 입력합니다. 태그에 대한 자세한 내용은 개체 > 태그를 참조하십시오.

구성원 수 및 주소	주소 그룹을 추가한 후 개체 > 주소 그룹 페이지의 구성원 수 열은 그룹의 개체가 동적으로 채워질지 아니면 정적으로 채워지는지를 나타냅니다.
	• 고정 주소 그룹의 경우 주소 그룹의 구성원 수를 볼 수 있습니다.
	• 태그를 사용하여 구성원을 동적으로 채우거나 정적 및 동적 구성원이 모두 있는 주소 그룹의 경우 구성원을 보려면 주소 열에서 자세히... 링크를 클릭하십시오. 이제 주소 그룹에 등록된 IP 주소를 볼 수 있습니다.
	  • 유형은 IP 주소가 고정 주소 개체인지 또는 동적으로 등록되는지의 여부를 나타내며 IP 주소를 표시합니다.
	  • 작업을 통해 IP 주소에서 태그 등록을 취소할 수 있습니다. 등록 소스 추가 링크를 클릭하고 등록을 취소할 태그를 지정합니다.

개체 > 영역

방화벽은 지정된 국가 또는 기타 지역에 적용되는 정책 규칙 생성을 지원합니다. 지역은 보안 정책, 복호화 정책, DoS 정책에 대한 소스 및 대상을 지정할 때 옵션으로 사용할 수 있습니다. 표준 국가 목록에서 선택하거나 이 섹션에 설명된 지역 설정을 사용하여 보안 정책 규칙에 대한 옵션으로 포함할 사용자 지정 지역을 정의할 수 있습니다.

다음 표에서는 지역 설정에 대해 설명합니다.

지역 설정	설명
리전	지역을 설명하는 드롭다운 메뉴에서 이름을 선택합니다. 이 이름은 보안 정책을 정의할 때 주소 목록에 나타납니다.
지리적 위치	위도와 경도를 지정하려면 이 옵션을 선택한 다음 값을 지정합니다(xxx.xxxxxx 형식). 이 정보는 App-Scope의 트래픽 및 위협 맵에 사용됩니다. 모니터 > 로그를 참조하세요.
주소	다음 형식 중 하나를 사용하여 지역을 식별할 IP 주소, IP 주소 범위 또는 서브넷을 지정합니다. x.x.x.x x.x.x.x-y.y.y.y x.x.x.x/n

개체 > 동적 사용자 그룹

동적 사용자 그룹을 만들려면 개체 > 동적 사용자 그룹, 새 동적 사용자 그룹 추가를 선택한 후 다음 설정을 구성합니다.

동적 사용자 그룹 설정	설명
이름	동적 사용자 그룹을 설명하는 이름 (최대 63자)을 입력합니다. 이 이름은 보안 정책 규칙을 정의할 때 소스 사용자 목록에 나타납니다. 이름은 고유해야 하며 영숫자, 공백, 하이픈 및 밑줄만 사용해야 합니다.
설명	개체에 대한 설명 (최대 1,023자)을 입력합니다.
공유 (Panorama만 해당)	Panorama의 모든 디바이스 그룹에서 동적 사용자 그룹의 일치 기준을 사용할 수 있도록 하려면 이 옵션을 선택합니다. *Panorama*은 그룹의 구성원을 디바이스 그룹과 공유하지 않습니다. 이 옵션의 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에만 동적 사용자 그룹의 일치 조건을 사용할 수 있습니다.
재정의 비활성화 (Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 동적 사용자 그룹의 설정을 재정의하지 못하도록 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
일치	일치 조건 추가 - **AND** 또는 **OR** 연산자를 사용하여 동적 사용자 그룹의 구성원을 정의하여 여러 태그를 포함합니다. 부정은 지원되지 않습니다. 일치 기준을 추가하면 기존 태그만 표시됩니다. 기존 태그를 선택하거나 새 태그를 만들 수 있습니다.
태그	(선택 사항) 동적 사용자 그룹 개체에 적용할 정적 개체 태그를 선택하거나 입력합니다. 이렇게 하면 그룹의 구성원이 아니라 동적 사용자 그룹 개체 자체에 태그가 지정됩니다. 선택한 태그를 사용하면 관련 항목을 그룹화할 수 있으며 일치 조건과 관련이 없습니다. 태그에 대한 자세한 내용은 개체 > 태그를 참조하십시오.

동적 사용자 그룹을 추가한 후 그룹에 대한 다음 정보를 볼 수 있습니다.

동적 사용자 그룹 열	설명
위치 (Panorama 전용)	동적 사용자 그룹의 일치 조건을 Panorama (공유) 의 모든 디바이스 그룹에 사용할 수 있는지 또는 선택한 디바이스 그룹에서 사용할 수 있는지의 여부를 식별합니다.
사용자	동적 사용자 그룹의 사용자 목록을 보려면 자세히를 선택합니다. • 그룹에 포함할 태그를 사용자에게 추가하려면 [사용자 등록]을 선택한 다음 등록 소스와 사용자에게 적용할 태그를 선택합니다. 사용자의 태그가 그룹의 기준과 일치하면 방화벽이 사용자를 동적 사용자 그룹에 추가합니다. • (선택 사항) 타임아웃(분)(기본값은 0, 범위는 0 - 43,200)를 지정하여 지정된 시간이 만료될 때 그룹에서 사용자를 제거합니다. • (선택 사항) 그룹에 사용자 추가 또는 그룹에서 사용자 삭제 • 사용자에서 태그를 제거하고 그룹의 구성원이 되지 않도록 하려면 사용자를 선택하고 사용자 등록 해제를 선택한 다음 등록 소스 및 태그를 선택합니다. • 동적 사용자 그룹 사용자 목록 검토 또는 수정을 마쳤으면 닫기를 클릭합니다.

개체 > 애플리케이션

다음 항목에서는 [애플리케이션] 페이지에 대해 설명합니다.

무엇을 찾고 계십니까?	참조
[애플리케이션] 페이지에 표시되는 애플리케이션 설정 및 속성을 이해합니다.	애플리케이션 개요 애플리케이션에서 지원되는 작업
새 애플리케이션을 추가하거나 기존 애플리케이션을 수정합니다.	애플리케이션 정의

애플리케이션 개요

애플리케이션 페이지에는 애플리케이션의 상대적 보안 위험(1~5)과 같은 각 애플리케이션 정의의 다양한 속성이 나열됩니다. 위험 값은 애플리케이션이 파일을 공유할 수 있는지, 오용되기 쉬운지 또는 방화벽을 회피하려고 하는지의 여부와 같은 기준을 기반으로 합니다. 더 높은 값은 더 높은 위험을 나타냅니다.

페이지의 상단 애플리케이션 브라우저 영역에는 다음과 같이 디스플레이를 필터링하는 데 사용할 수 있는 속성이 나열됩니다. 각 항목의 왼쪽에 있는 숫자는 해당 속성이 있는 총 애플리케이션 수를 나타냅니다.

주간 콘텐츠 릴리스에는 서명을 개발할 수 있는 새로운 디코더와 컨텍스트가 주기적으로 포함됩니다.

다음 표에서는 애플리케이션 세부 정보를 설명합니다. 사용자 지정 애플리케이션 및 Palo Alto® Networks 애플리케이션은 이러한 필드의 일부 또는 전체를 표시할 수 있습니다.

애플리케이션 내용	설명
이름	애플리케이션의 이름입니다.
설명	애플리케이션에 대한 설명(최대 255자).

애플리케이션 내용	설명
추가 정보	애플리케이션에 대한 추가 정보가 포함된 웹 소스(Wikipedia, Google 및 Yahoo!)에 대한 링크.
표준 포트	애플리케이션이 네트워크와 통신하는 데 사용하는 포트입니다.
의존 대상	이 애플리케이션을 실행하는 데 필요한 다른 애플리케이션 목록입니다. 선택한 애플리케이션을 허용하는 정책 규칙을 만들 때 애플리케이션이 의존하는 다른 애플리케이션도 허용하고 있는지 확인해야 합니다.
암시적으로 사용	선택한 애플리케이션이 종속되지만 해당 애플리케이션이 암시적으로 지원되기 때문에 선택한 애플리케이션을 허용하기 위해 보안 정책 규칙에 추가할 필요가 없는 기타 애플리케이션입니다.
이전에 다음으로 식별됨	새로운 App-ID™ 또는 변경된 App-ID의 경우 애플리케이션이 이전에 식별된 것을 나타냅니다. 이를 통해 애플리케이션의 변경 사항을 기반으로 정책 변경이 필요한지의 여부를 평가할 수 있습니다. App-ID가 비활성화된 경우 해당 애플리케이션과 연결된 세션은 이전에 애플리케이션으로 식별된 정책과 일치합니다. 마찬가지로 비활성화된 App-ID는 이전에 식별된 애플리케이션으로 로그에 나타납니다.
작업 거부	App-ID는 애플리케이션이 거부 작업과 함께 보안 정책 규칙에 포함될 때 방화벽이 응답하는 방식을 지정하는 기본 거부 작업으로 개발됩니다. 기본 거부 작업은 자동 삭제 또는 TCP 재설정을 지정할 수 있습니다. 보안 정책에서 이 기본 작업을 재정의할 수 있습니다.
특성	
회피성	방화벽을 통과할 수 있기를 바라며 원래 의도한 것과 다른 목적으로 포트 또는 프로토콜을 사용합니다.
과도한 대역폭	정상적인 사용을 통해 정기적으로 최소 1Mbps를 소비합니다.
남용하기 쉬움	종종 악의적인 목적으로 사용되거나 사용자가 의도한 것보다 과하게 노출되도록 쉽게 설정됩니다.
SaaS	방화벽에서 SaaS(Software as a Service)는 소프트웨어 및 인프라가 애플리케이션 서비스 공급자에 의해 소유 및 관리되는 서비스이지만 데이터의 생성, 액세스, 공유 및 전송을 할 수 있는 인원을 포함하여 데이터에 대한 모든 권한은 귀하가 보유하는 곳입니다.

애플리케이션 내용	설명
	애플리케이션이 특성화되는 방식의 맥락에서 SaaS 애플리케이션은 웹 서비스와 다릅니다. 웹 서비스는 사용자가 데이터를 소유하지 않거나(예: Pandora) 또는 서비스가 주로 소셜 목적을 위해 많은 가입자가 제공한 데이터 공유로 구성되는 호스팅된 애플리케이션(예: LinkedIn, Twitter 또는 Facebook)입니다.
파일 전송 가능	네트워크를 통해 한 시스템에서 다른 시스템으로 파일을 전송할 수 있는 기능이 있습니다.
기타 애플리케이션 터널	프로토콜 내에서 다른 애플리케이션을 전송할 수 있습니다.
멀웨어에서 사용	멀웨어는 전파, 공격 또는 데이터 도용에 애플리케이션을 사용하는 것으로 알려져 있거나 멀웨어와 함께 배포됩니다.
알려진 취약점이 있음	공개적으로 보고된 취약점이 있습니다.
전파성	1,000,000명 이상의 사용자가 있을 것으로 예상됩니다.
다른 애플리케이션 검색 계속	방화벽이 계속해서 다른 애플리케이션 서명에 대해 일치를 시도하도록 지시합니다. 이 옵션을 선택하지 않으면 방화벽은 일치하는 첫 번째 서명 이후에 추가 애플리케이션 일치 검색을 중지합니다.
SaaS 특성	
데이터 침해	지난 3년 이내에 신뢰할 수 없는 출처에 보안 정보를 공개했을 수 있는 애플리케이션.
부실한 서비스 약관	엔터프라이즈 데이터를 손상시킬 수 있는 서비스 약관이 미흡한 애플리케이션.
인증 없음	SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA 또는 FEDRAMP와 같은 산업 프로그램 또는 인증에 대한 현재 규정 준수가 부족한 애플리케이션.
열악한 재정적 생존력	향후 18~24개월 이내에 중단될 가능성이 있는 애플리케이션.
IP 제한 없음	사용자 액세스에 대한 IP 기반 제한이 없는 애플리케이션.
분류	
카테고리	애플리케이션 카테고리는 다음 중 하나입니다. • business-systems

애플리케이션 내용	설명
	• collaboration • general-internet • media • 네트워킹 • 알려지지 않은
하위 카테고리	애플리케이션이 분류되는 하위 카테고리입니다. 다른 카테고리에는 연관된 다른 하위 카테고리가 있습니다. 예를 들어 협업 카테고리의 하위 카테고리에는 이메일, 파일 공유, 인스턴트 메시징, 인터넷 회의, 소셜 비즈니스, 소셜 네트워킹, VoIP 및 웹 게시가 포함됩니다. 반면 비즈니스 시스템 카테고리의 하위 카테고리에는 인증 서비스, 데이터베이스, erp-crm, 일반 비즈니스, 관리, 사무용 프로그램, 소프트웨어 업데이트 및 스토리지 백업이 포함됩니다.
기술	응용 기술은 다음 중 하나입니다. • client-server: 하나 이상의 클라이언트가 네트워크의 서버와 통신하는 클라이언트-서버 모델을 사용하는 애플리케이션입니다. • 네트워크 프로토콜: 네트워크 작동을 용이하게 하는 시스템 간 통신에 일반적으로 사용되는 애플리케이션입니다. 여기에는 대부분의 IP 프로토콜이 포함됩니다. • 피어 투 피어: 통신을 용이하게 하기 위해 중앙 서버에 의존하는 대신 정보를 전송하기 위해 다른 클라이언트와 직접 통신하는 애플리케이션입니다. • 브라우저 기반: 작동하기 위해 웹 브라우저에 의존하는 애플리케이션입니다.
위험	애플리케이션에 할당된 위험. 이 설정을 사용자 지정하려면 사용자 지정 링크를 클릭하고 값(1-5)을 입력한 다음 확인을 클릭합니다.
태그	애플리케이션에 할당된 태그입니다. 태그를 편집하여 애플리케이션에 대한 태그를 추가하거나 제거합니다.
옵션	
세션 타임아웃	비활성으로 인해 애플리케이션이 타임아웃되는 데 필요한 시간(초)입니다(범위는 1-604800초). 이 타임아웃은 TCP 또는 UDP 이외의 프로

애플리케이션 내용	설명
	토콜에 대한 것입니다. TCP 및 UDP의 경우 이 표의 다음 행을 참조하십시오. 이 설정을 사용자 지정하려면 사용자 지정 링크를 클릭하고 값을 입력한 다음 확인을 클릭합니다.
TCP 타임아웃(초)	TCP 애플리케이션 흐름을 종료하기 위한 타임아웃(초)입니다(범위는 1-604800). 이 설정을 사용자 지정하려면 사용자 지정 링크를 클릭하고 값을 입력한 다음 확인을 클릭합니다. 값 0은 전역 세션 타이머가 사용됨을 나타내며 TCP의 경우 3600초입니다.
UDP 타임아웃(초):	UDP 애플리케이션 흐름을 종료하기 위한 타임아웃(초)입니다(범위는 1-604800초). 이 설정을 사용자 지정하려면 사용자 지정 링크를 클릭하고 값을 입력한 다음 확인을 클릭합니다.
TCP 반 폐쇄(초)	첫 번째 FIN 패킷 수신과 두 번째 FIN 패킷 또는 RST 패킷 수신 사이에 세션이 세션 테이블에 남아 있는 최대 시간(초)입니다. 타이머가 만료되면 세션이 닫힙니다(범위는 1-604800). 기본값: 이 타이머가 애플리케이션 수준에서 구성되지 않은 경우 전역 설정이 사용됩니다. 이 값이 애플리케이션 수준에서 구성된 경우 전역 **TCP Half Closed** 설정을 재정의합니다.
TCP 시간 대기(초)	두 번째 FIN 패킷 또는 RST 패킷을 수신한 후 세션이 세션 테이블에 남아 있는 최대 시간(초)입니다. 타이머가 만료되면 세션이 닫힙니다(범위는 1-600). 기본값: 이 타이머가 애플리케이션 수준에서 구성되지 않은 경우 전역 설정이 사용됩니다. 이 값이 애플리케이션 수준에서 구성된 경우 전역 **TCP** 시간 대기 설정을 재정의합니다.
App-ID 사용	App-ID의 활성화 또는 비활성화 여부를 나타냅니다. App-ID가 비활성화된 경우 해당 애플리케이션의 트래픽은 보안 정책과 로그 모두에서 이전에 **App-ID**로 식별된 것으로 처리됩니다. 콘텐츠 릴리스 버전 490 이후에 추가된 애플리케이션의 경우 새 앱의 정책 영향을 검토하는 동안 해당 애플리케이션을 비활성화할 수 있습니다. 정책을 검토한

애플리케이션 내용	설명
	후 App-ID를 활성화하도록 선택할 수 있습니다. 이전에 활성화한 애플리케이션을 비활성화할 수도 있습니다. Multi-VSYS 방화벽에서는 각 가상 시스템에서 별도로 App-ID를 비활성화할 수 있습니다.

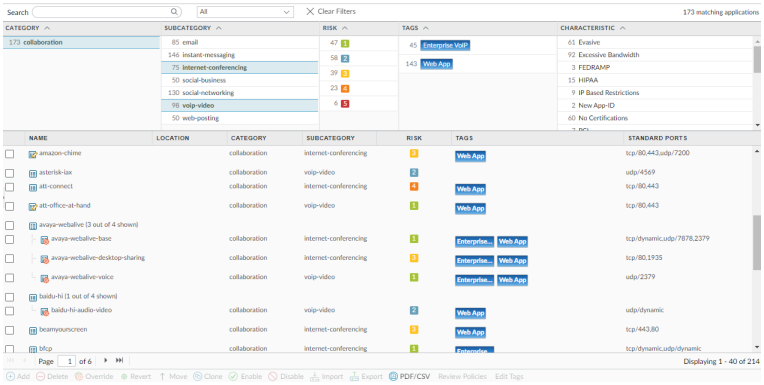
방화벽이 App-ID를 사용하여 애플리케이션을 식별할 수 없는 경우 트래픽은 unknown-tcp 또는 unknown-udp로 분류됩니다. 이 동작은 HTTP를 완전히 에뮬레이트하는 애플리케이션을 제외한 모든 알 수 없는 애플리케이션에 적용됩니다. 자세한 내용은 모니터 > 봇넷을(를) 참조하십시오.

알 수 없는 애플리케이션에 대한 새 정의를 만든 다음 새 애플리케이션 정의에 대한 보안 정책을 정의할 수 있습니다. 또한 동일한 보안 설정이 필요한 애플리케이션을 애플리케이션 그룹으로 결합하여 보안 정책 생성을 단순화할 수 있습니다.

애플리케이션에서 지원되는 작업

이 페이지에서 다음 작업을 수행할 수 있습니다.

애플리케이션에 대해 지원되는 작업	설명
애플리케이션별 필터링	• 특정 애플리케이션을 검색하려면 검색 필드에 애플리케이션 이름 또는 설명을 입력하고 **Enter** 키를 누릅니다. 드롭다운을 사용하면 특정 애플리케이션을 검색 또는 필터링하거나 모든 애플리케이션, 사용자 지정 애플리케이션, 비활성화된 애플리케이션 또는 태그가 지정된 애플리케이션을 볼 수 있습니다. 애플리케이션이 나열되고 필터 열이 업데이트되어 검색과 일치하는 애플리케이션에 대한 통계가 표시됩니다. 검색은 부분 문자열과 일치합니다. 보안 정책을 정의할 때 저장된 필터와 일치하는 모든 애플리케이션에 적용되는 규칙을 작성할 수 있습니다. 이러한 규칙은 필터와 일치하는 콘텐츠 업데이트를 통해 새 애플리케이션이 추가될 때 동적으로 업데이트됩니다. • 페이지에 표시된 애플리케이션 속성으로 필터링하려면 필터링 기준으로 사용할 항목을 클릭합니다. 예를 들어 목록을 협업 카테고리로

애플리케이션에 대해 지원되는 작업	설명
	제한하려면 협업을 클릭하면 이 카테고리의 애플리케이션만 목록에 표시됩니다.  • 추가 열을 필터링하려면 다른 열에서 항목을 선택하십시오. 필터링은 연속적입니다. 카테고리 필터가 먼저 적용된 다음 하위 카테고리 필터, 기술 필터, 위험 필터, 마지막으로 특성 필터가 적용됩니다. 예를 들어 카테고리, 하위 카테고리 및 위험 필터를 적용하면 기술 필터가 명시적으로 적용되지 않더라도 기술 열이 선택한 카테고리 및 하위 카테고리와 일치하는 기술로 자동으로 제한됩니다. 필터를 적용할 때마다 애플리케이션 목록이 자동으로 업데이트됩니다. 새 애플리케이션 필터를 만들려면 개체 > 애플리케이션 필터를 참조하십시오.
새 애플리케이션을 추가합니다.	새 애플리케이션을 추가하려면 애플리케이션 정의를 참조하십시오.
애플리케이션 세부 정보를 보거나 사용자 정의합니다.	애플리케이션 이름 링크를 클릭하면 표준 포트 및 애플리케이션의 특성, 기타 세부 사항 중 위험을 포함한 애플리케이션 설명을 볼 수 있습니다. 애플리케이션 설정에 대한 자세한 내용은 애플리케이션 정의를 참조하십시오. 애플리케이션 이름 왼쪽의 아이콘에 노란색 연필( )이 있으면 해당 애플리케이션은 사용자 지정 애플리케이션입니다.
애플리케이션 비활성화	애플리케이션 서명이 트래픽과 일치하지 않도록 애플리케이션(또는 여러 애플리케이션)을 비활성화할 수 있습니다. 일치하는 애플리케이션을 차단, 허용 또는 시행하도록 정의된 보안 규칙은 앱이 비활성화된 경우 애플리케이션 트래픽에 적용되지 않습니다. 애플리케이션이 고유하게 식별되면 애플리케이션에 대한 정책 시행이 변경될 수 있으므로 새 콘텐츠 릴리스 버전에 포함된 애플리케이션을 비활성화하도록 선택할 수 있습니다. 예를 들어, 웹 브라우징 트래픽으로 식별된 애플리케이션은 새 콘텐

애플리케이션에 대해 지원되는 작업	설명
	츠 버전을 설치하기 전에 방화벽에서 허용합니다. 콘텐츠 업데이트를 설치한 후 고유하게 식별된 애플리케이션은 웹 브라우징 트래픽을 허용하는 보안 규칙과 더 이상 일치하지 않습니다. 이 경우 애플리케이션 서명과 일치하는 트래픽이 계속해서 웹 브라우징 트래픽으로 분류되고 허용되도록 애플리케이션을 비활성화하도록 선택할 수 있습니다.
애플리케이션 활성화	비활성화된 애플리케이션을 선택한 다음 방화벽이 구성된 보안 정책에 따라 애플리케이션을 관리할 수 있도록 활성화합니다.
애플리케이션 가져오기	애플리케이션을 가져오려면 가져오기를 클릭합니다. 파일을 찾아 선택한 다음 대상 드롭다운에서 대상 가상 시스템을 선택합니다.
애플리케이션 내보내기	애플리케이션을 내보내려면 애플리케이션에 대해 이 옵션을 선택한 다음 내보내기를 클릭합니다. 프롬프트에 따라 파일을 저장합니다.
애플리케이션 구성 테이블 내보내기	모든 애플리케이션에 대한 정보를 **PDF/CSV** 형식으로 내보냅니다. 웹 인터페이스에서 보이는 열만 내보내집니다. 구성 테이블 데이터 내보내기를 참조하십시오.
새 콘텐츠 릴리스 설치 후 정책 영향 평가	콘텐츠 릴리스 버전을 설치하기 전후에 애플리케이션에 대한 정책 기반 시행을 평가하려면 정책을 검토하십시오. 정책 검토 대화 상자를 사용하여 다운로드한 콘텐츠 릴리스 버전에 포함된 새 애플리케이션에 대한 정책 영향을 검토합니다. 정책 검토 대화 상자를 사용하면 기존 보안 정책 규칙에서 보류 중인 애플리케이션(콘텐츠 릴리스 버전과 함께 다운로드되지만 방화벽에 설치되지 않은 애플리케이션)을 추가하거나 제거할 수 있습니다. 보류 중인 애플리케이션에 대한 정책 변경 사항은 해당 콘텐츠 릴리스 버전이 설치될 때까지 적용되지 않습니다. **Device** > **Dynamic** 업데이트 페이지에서 콘텐츠 릴리스 버전을 다운로드 및 설치할 때 정책 검토 대화 상자에 액세스할 수도 있습니다.
애플리케이션에 태그 지정	**sanctioned**라는 사전 정의된 태그를 사용하여 SaaS 애플리케이션에 태그를 지정할 수 있습니다. SaaS 애플리케이션은 애플리케이션 특성에 대한 세부 정보에서 **Saas=yes**로 식별되는 애플리케이션이지만 모든 애플리케이션에서 승인된 태그를 사용할 수 있습니다. 예를 들어 *SaaS* 애플리케이션 사용 보고서를 검토하거나 네트워크에서 애플리케이션을 평가할 때 승인된 *SaaS* 애플리케이션 트래픽을 승인되지 않은 *SaaS* 애플리케이션 트래픽과 구별하는 데 도움이 되도록 애플리케이션에 승인된 태그를 지정합니다.

애플리케이션에 대해 지원되는 작업	설명
	애플리케이션을 선택한 다음 태그 편집을 클릭한 다음 드롭다운에서 사전 정의된 승인 태그를 선택하여 네트워크에서 명시적으로 허용하려는 애플리케이션을 식별합니다. 그런 다음 SaaS 애플리케이션 사용 보고서를 생성할 때(모니터 > PDF 보고서 > SaaS 애플리케이션 사용 참조) 승인한 애플리케이션과 네트워크에서 사용 중인 승인되지 않은 SaaS 애플리케이션에 대한 통계를 비교할 수 있습니다. 승인된 애플리케이션으로 태그를 지정하면 다음 제한 사항이 적용됩니다. • 승인된 태그는 애플리케이션 그룹에 적용할 수 없습니다. • 승인된 태그는 공유 수준에서 적용할 수 없습니다. 디바이스 그룹 또는 가상 시스템별로만 애플리케이션에 태그를 지정할 수 있습니다. • sanctioned 태그는 facebook 컨테이너 앱의 일부인 facebook-mail과 같은 컨테이너 앱에 포함된 애플리케이션에 태그를 지정하는 데 사용할 수 없습니다. 태그를 제거하거나 태그를 재정의할 수도 있습니다. 재정의 옵션은 Panorama에서 푸시된 디바이스 그룹의 설정을 상속받은 방화벽에서만 사용할 수 있습니다.

애플리케이션 정의

정책을 적용할 때 평가할 방화벽에 대한 새 사용자 지정 애플리케이션을 추가하려면 개체 > 애플리케이션을 선택합니다.

새 애플리케이션 설정	설명
구성 탭	
이름	애플리케이션 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 애플리케이션 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 마침표, 하이픈 및 밑줄만 사용하십시오. 첫 번째 글자는 문자여야 합니다.
공유	애플리케이션을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 애플리케이션을 사용할 수 있습니다.

새 애플리케이션 설정	설명
	• Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에서만 애플리케이션을 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 애플리케이션 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
설명	일반적인 참조를 위해 애플리케이션에 대한 설명을 입력합니다(최대 255자).
카테고리	이메일 또는 데이터베이스와 같은 애플리케이션 카테고리를 선택합니다. 카테고리는 상위 10개 애플리케이션 카테고리 차트를 생성하는 데 사용되며 필터링에 사용할 수 있습니다(ACC 참조).
하위 카테고리	이메일 또는 데이터베이스와 같은 애플리케이션 하위 카테고리를 선택합니다. 하위 카테고리는 상위 10개 애플리케이션 카테고리 차트를 생성하는 데 사용되며 필터링에 사용할 수 있습니다(ACC 참조).
기술	애플리케이션에 대한 기술을 선택합니다. 기본적으로 기술 열은 표시되지 않습니다. 기술 열을 표시하여 응용 프로그램 필터에 추가할 기술을 선택합니다.
부모 요소 앱	이 애플리케이션의 상위 애플리케이션을 지정하십시오. 이 설정은 세션이 상위 및 사용자 정의 애플리케이션 모두와 일치할 때 적용됩니다. 그러나 사용자 지정 애플리케이션이 더 구체적이기 때문에 보고됩니다.
위험	이 애플리케이션과 관련된 위험 수준을 선택하십시오(1=최저 ~ 5=최고).
특성	애플리케이션을 위험에 빠뜨릴 수 있는 애플리케이션 특성을 선택하십시오. 각 특성에 대한 설명은 특성을 참조하십시오.
Advanced 탭	
포트	애플리케이션에서 사용하는 프로토콜이 TCP 및/또는 UDP인 경우 포트를 선택한 다음 프로토콜과 포트 번호의 조합을 하나 이상 입력합니다(한 줄에 하나의 항목). 일반적인 형식은 다음과 같습니다. *<protocol>/<port>* 여기서 *<port>*은(는) 단일 포트 번호이거나 동적 포트 할당의 경우 동적입니다. 예: TCP/동적 또는 UDP/32.

새 애플리케이션 설정	설명
	이 설정은 보안 규칙의 서비스 열에서 **app-default**를 사용할 때 적용됩니다.
IP 프로토콜	TCP 또는 UDP 이외의 IP 프로토콜을 지정하려면 **IP** 프로토콜을 선택한 다음 프로토콜 번호(1 ~ 255)를 입력합니다.
ICMP 유형	ICMP(Internet Control Message Protocol 버전 4) 유형을 지정하려면 **ICMP** 유형을 선택한 다음 유형 번호를 입력합니다(범위는 0-255).
ICMP6 유형	ICMPv6(Internet Control Message Protocol 버전 6) 유형을 지정하려면 **ICMP6** 유형을 선택한 다음 유형 번호를 입력합니다(범위는 0-255).
없음	프로토콜과 별개로 서명을 지정하려면 없음을 선택합니다.
타임아웃	유휴 애플리케이션 흐름이 종료되기까지의 시간(초)을 입력합니다(범위는 0-604800초). 0은 애플리케이션의 기본 타임아웃이 사용됨을 나타냅니다. 이 값은 모든 경우에 TCP 및 UDP 이외의 프로토콜에 사용되며 TCP 타임아웃 및 UDP 타임아웃이 지정되지 않은 경우 TCP 및 UDP 타임아웃에 사용됩니다.
TCP 타임아웃	유휴 TCP 애플리케이션 흐름이 종료되기 전의 시간(초)을 입력합니다(범위는 0-604800초). 0은 애플리케이션의 기본 타임아웃이 사용됨을 나타냅니다.
UDP 타임아웃	유휴 UDP 애플리케이션 흐름이 종료되기 전의 시간(초)을 입력합니다(범위는 0-604800초). 0은 애플리케이션의 기본 타임아웃이 사용됨을 나타냅니다.
TCP 반 닫힘	첫 번째 FIN 수신과 두 번째 FIN 또는 RST 수신 사이에 세션이 세션 테이블에 남아 있는 최대 시간을 입력하십시오. 타이머가 만료되면 세션이 닫힙니다. 기본: 이 타이머가 애플리케이션 수준에서 구성되지 않은 경우 전역 설정이 사용됩니다(범위는 1-604800초). 이 값이 애플리케이션 수준에서 구성된 경우 전역 TCP Half Closed 설정을 재정의합니다.
TCP 시간 대기	두 번째 FIN 또는 RST를 수신한 후 세션이 세션 테이블에 남아 있는 최대 시간을 입력합니다. 타이머가 만료되면 세션이 닫힙니다. 기본: 이 타이머가 애플리케이션 수준에서 구성되지 않은 경우 전역 설정이 사용됩니다(범위는 1-600초).

새 애플리케이션 설정	설명
	이 값이 애플리케이션 수준에서 구성된 경우 전역 TCP 시간 대기 설정을 재정의합니다.
스캐닝	보안 프로파일(파일 형식, 데이터 패턴 및 바이러스)을 기반으로 허용할 검색 유형을 선택합니다.
서명 탭	
서명	추가를 클릭하여 새 서명을 추가하고 다음 정보를 지정합니다. • 서명 이름 - 서명을 식별할 이름을 입력합니다. • 설명 - 선택적 설명을 입력합니다. • 순서가 지정된 조건 일치 - 서명 조건이 정의된 순서가 중요한 경우 선택합니다. • 범위 - 이 서명을 현재 트랜잭션에만 적용할지 아니면 전체 사용자 세션에 적용할지 선택합니다. 서명을 식별하는 조건을 지정하십시오. 이러한 조건은 방화벽이 애플리케이션 패턴을 일치시키고 트래픽을 제어하는 데 사용하는 서명을 생성하는 데 사용됩니다. • 조건을 추가하려면 **And** 조건 추가 또는 **Or** 조건 추가를 선택합니다. 그룹 내에 조건을 추가하려면 그룹을 선택한 다음 조건 추가를 클릭합니다.

새 애플리케이션 설정	설명
	• 드롭다운에서 연산자를 선택합니다. 옵션은 패턴 일치, 보다 큼, 보다 작음 및 같음이며 다음 옵션을 지정합니다. (패턴 일치에만 해당) • 컨텍스트 - 사용 가능한 컨텍스트에서 선택합니다. 이러한 컨텍스트는 동적 콘텐츠 업데이트를 사용하여 업데이트됩니다. • 패턴 - 사용자 정의 애플리케이션에 적용되는 고유한 문자열 컨텍스트 값을 지정하는 정규식을 지정합니다. 컨텍스트를 식별하기 위해 패킷 캡처를 수행합니다. 정규식에 대한 패턴 규칙은 패턴 규칙 구문을 참조하십시오. (보다 큼, 보다 작음) • 컨텍스트 - 사용 가능한 컨텍스트에서 선택합니다. 이러한 컨텍스트는 동적 콘텐츠 업데이트를 사용하여 업데이트됩니다. • 값 - 일치시킬 값을 지정합니다(범위는 0-4294967295). • 수식어 및 값 - (선택 사항) 수식어/값 쌍을 추가합니다. (같음에만 해당) • 컨텍스트 - TCP 또는 UDP(예: unknown-req-tcp) 또는 동적 콘텐츠 업데이트를 통해 사용할 수 있는 추가 컨텍스트(예: dnp3-req-func-code)에 대한 알 수 없는 요청 및 응답 중에서 선택합니다. TCP 또는 UDP에 대한 알 수 없는 요청 및 응답의 경우 다음을 지정합니다. • 위치 - 페이로드의 처음 4바이트 또는 두 번째 4바이트 중에서 선택합니다. • 마스크 - 4바이트 16진수 값을 지정합니다(예: 0xffffff00). • 값 - 4바이트 16진수 값을 지정합니다(예: 0xaabbccdd). 다른 모든 컨텍스트의 경우 애플리케이션과 관련된 값을 지정하십시오. 그룹 내에서 조건을 이동하려면 조건을 선택한 다음 위로 이동 또는 아래로 이동을 선택합니다. 그룹을 이동하려면 그룹을 선택한 다음 위로 이동 또는 아래로 이동을 선택합니다. 한 그룹에서 다른 그룹으로 조건을 이동할 수 없습니다.

애플리케이션이 애플리케이션 재정의 규칙에만 사용되는 경우 애플리케이션에 대한 서명을 지정할 필요가 없습니다.

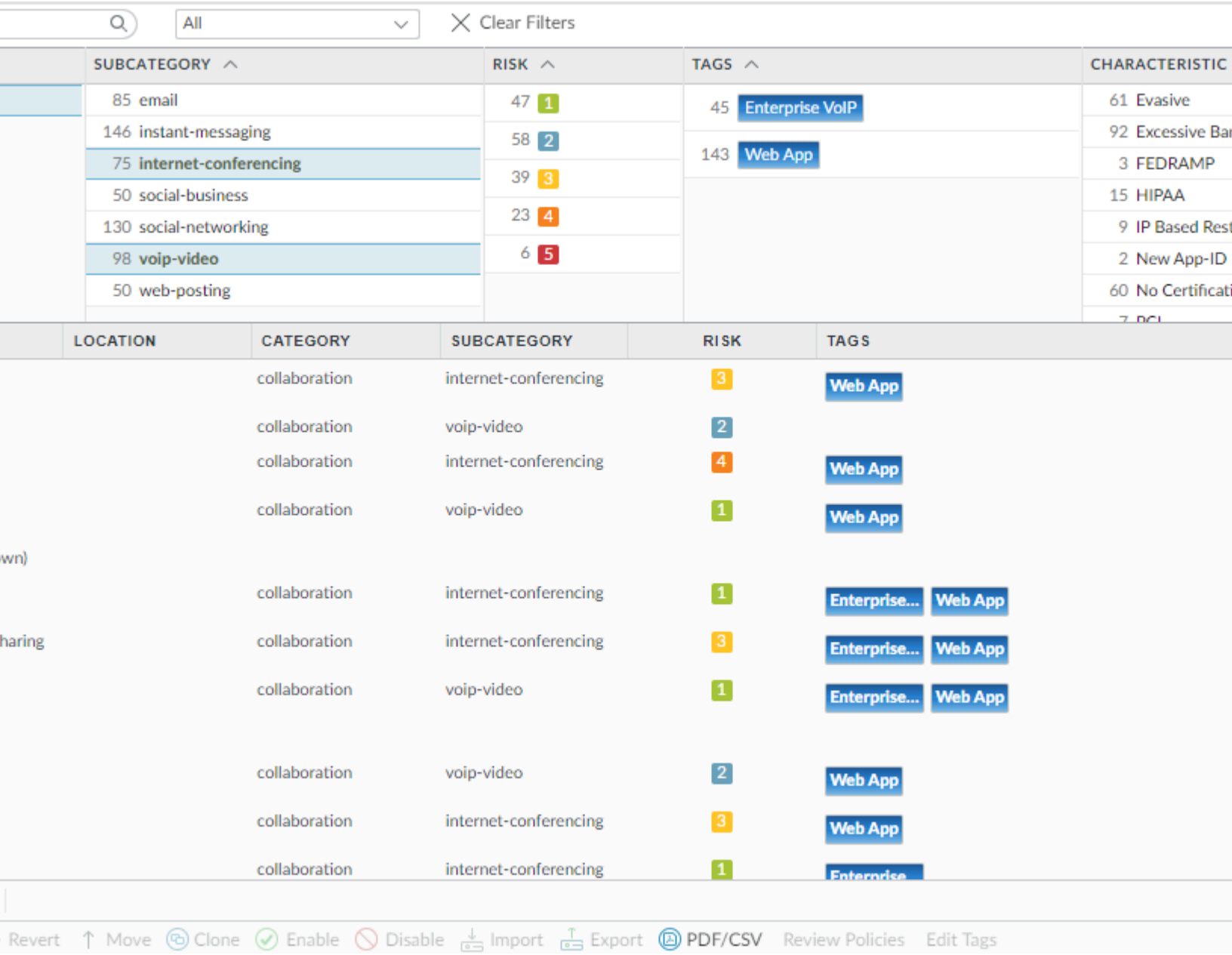
개체 > 애플리케이션 그룹

보안 정책 생성을 단순화하기 위해 애플리케이션 그룹을 생성하여 동일한 보안 설정이 필요한 애플리케이션을 결합할 수 있습니다. (새 애플리케이션을 정의하려면 애플리케이션 정의를 참조하십시오.)

새 애플리케이션 그룹 설정	설명
이름	애플리케이션 그룹을 설명하는 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 애플리케이션 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유	애플리케이션 그룹을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 애플리케이션 그룹을 사용할 수 있습니다. Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에서만 애플리케이션 그룹을 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 애플리케이션 그룹 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
애플리케이션	추가를 클릭하고 이 그룹에 포함할 애플리케이션, 애플리케이션 필터 및/또는 기타 애플리케이션 그룹을 선택합니다.

애플리케이션 필터를 > 개체

애플리케이션 필터는 반복된 검색을 단순화하는 데 도움이 됩니다. 애플리케이션, 필터를 정의하려면 새 필터의 이름을 추가하고 입력합니다. 창의 위쪽 영역에서 필터링의 기준으로 사용할 항목을 클릭합니다. 예를 들어 목록을 공동 작업 카테고리로 제한하려면 공동 작업을 클릭합니다.



추가 열을 필터링하려면 열에서 항목을 선택합니다. 필터링은 연속적입니다. 카테고리 필터는 먼저 하위 카테고리 필터, 기술 필터, 위험 필터, 태그 및 특성 필터 다음에 적용됩니다.

필터를 선택하면 페이지에 표시되는 애플리케이션 목록이 자동으로 업데이트됩니다.

개체 > 서비스

특정 애플리케이션에 대한 보안 정책을 정의할 때 하나 이상의 서비스를 선택하여 애플리케이션이 사용할 수 있는 포트 번호를 제한할 수 있습니다. 기본 서비스는 모든 TCP 및 UDP 포트를 허용하는 **any**입니다. HTTP 및 HTTPS 서비스는 사전 정의되어 있지만 추가 서비스 정의를 추가할 수 있습니다. 종종 함께 할당되는 서비스를 서비스 그룹으로 결합하여 보안 정책 생성을 단순화할 수 있습니다(개체 > 서비스 그룹 참조).

또한 서비스 개체를 사용하여 서비스 기반 세션 타임아웃을 지정할 수 있습니다. 즉, 해당 그룹이 동일한 TCP 또는 UDP 서비스를 사용하는 경우에도 다른 사용자 그룹에 다른 시간 초과를 적용할 수 있습니다. 또는 사용자 지정 애플리케이션이 있는 포트 기반 보안 정책에서 애플리케이션 기반 보안 정책으로 마이그레이션하는 경우 사용자 지정 애플리케이션 시간 초과를 쉽게 유지할 수 있습니다.

다음 표에서는 서비스 설정에 대해 설명합니다.

서비스 설정	설명
이름	서비스 이름을 입력합니다(최대 **63**자). 이 이름은 보안 정책을 정의할 때 서비스 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	서비스에 대한 설명을 입력합니다(최대 1023자).
공유	서비스 개체를 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 서비스 개체는 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 서비스 개체는 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 서비스 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
규약	서비스에서 사용하는 프로토콜(**TCP** 또는 **UDP**)을 선택합니다.
대상 포트	서비스에서 사용하는 대상 포트 번호(0 ~ 65535) 또는 포트 번호 범위(port1-port2)를 입력합니다. 여러 포트 또는 범위는 쉼표로 구분해야 합니다. 대상 포트는 필수 항목입니다.

서비스 설정	설명
소스 포트	서비스에서 사용하는 소스 포트 번호(0 ~ 65535) 또는 포트 번호 범위(port1-port2)를 입력합니다. 여러 포트 또는 범위는 쉼표로 구분해야 합니다. 소스 포트는 선택 사항입니다.
세션 타임 아웃	서비스에 대한 세션 타임아웃을 정의합니다. • 애플리케이션에서 상속(기본값) - 서비스 기반 타임아웃이 적용되지 않습니다. 애플리케이션 타임아웃이 적용됩니다. • 재정의 - 서비스에 대한 사용자 지정 세션 타임아웃을 정의합니다. TCP 타임아웃, TCP Half Closed 및 TCP 대기 시간 필드를 계속 채우십시오.
다음 설정은 애플리케이션 타임아웃을 재정의하고 서비스에 대한 사용자 지정 세션 타임아웃을 생성하도록 선택한 경우에만 표시됩니다.	
TCP 타임아웃	데이터 전송이 시작된 후 TCP 세션이 열린 상태로 남아 있을 수 있는 최대 시간(초)을 설정합니다. 이 시간이 만료되면 세션이 닫힙니다. 범위는 1 - 604800입니다. 기본값은 3600초입니다.
TCP 반 폐쇄	연결의 한쪽에서만 연결을 닫으려고 시도한 경우 세션이 열린 상태로 유지되는 최대 시간(초)을 설정합니다. 이 설정은 다음에 적용됩니다. • 방화벽이 첫 번째 FIN 패킷을 수신한 후(한쪽 연결이 세션을 닫으려는 것을 나타냄) 두 번째 FIN 패킷을 받기 전(연결의 다른 쪽이 세션을 닫고 있음을 나타냄) 기간. • RST 패킷을 수신하기 전의 기간(연결 재설정 시도를 나타냄). 타이머가 만료되면 세션이 닫힙니다. 범위는 1 - 604800입니다. 기본값은 120초입니다.
TCP 대기 시간	세션을 종료하는 데 필요한 두 개의 FIN 패킷 중 두 번째 패킷을 수신한 후 또는 연결을 재설정하기 위해 RST 패킷을 수신한 후 세션이 열려 있는 최대 시간(초)을 설정합니다. 타이머가 만료되면 세션이 닫힙니다. 범위는 1 - 600입니다. 기본값은 15초입니다.

개체 > 서비스 그룹

보안 정책 생성을 단순화하기 위해 보안 설정이 동일한 서비스를 서비스 그룹으로 결합할 수 있습니다. 새 서비스를 정의하려면 개체 > 서비스를 참조하세요.

다음 표에서는 서비스 그룹 설정에 대해 설명합니다.

서비스 그룹 설정	설명
이름	서비스 그룹 이름을 입력합니다(최대 **63**자). 이 이름은 보안 정책을 정의할 때 서비스 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유	서비스 그룹을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 서비스 그룹은 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 서비스 그룹은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 서비스 그룹 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
서비스	추가를 클릭하여 그룹에 서비스를 추가합니다. 드롭다운에서 선택하거나 드롭다운 하단에서 서비스를 클릭하고 설정을 지정합니다. 설정에 대한 설명은 개체 > 서비스를 참조하십시오.

태그> 개체

태그를 사용하면 키워드나 구를 사용하여 개체를 그룹화할 수 있습니다. 개체, 주소 그룹(정적 및 동적), 애플리케이션, 영역, 서비스, 서비스 그룹 및 정책 규칙에 태그를 적용할 수 있습니다. SD-WAN 인터페이스 프로파일을 사용하여 이더넷 인터페이스에 링크 태그를 적용할 수도 있습니다. 태그를 사용하여 개체를 정렬하거나 필터링하고 색상으로 개체를 시각적으로 구별할 수 있습니다. 태그에 색상을 적용하면 정책 탭에 배경색이 있는 개체가 표시됩니다.

해당 태그를 사용하여 규칙을 그룹화하려면 먼저 태그를 만들어야 합니다. 태그별로 그룹화 된 규칙을 할당 한 후 룰베이스**(rulebase)**를 그룹으로 보기 위해 할당 된 태그를 기반으로 정책 규칙 기반의 시각적 표현을 볼 수 있습니다. 규칙 기준을 그룹으로 보는 동안 정책 순서와 우선 순위가 유지됩니다. 이 보기에서 그룹 태그를 선택하여 해당 태그로 그룹화된 모든 규칙을 봅니다.

승인이라는 사전 정의된 태그는 태그 지정 애플리케이션(개체 > 응용프로그램)에 사용할 수 있습니다. 이러한 태그는 정확성에 필요합니다(모니터 > PDF 보고서 > SaaS 애플리케이션 사용).

무엇을 알고 싶습니까**?**	참조**:**
태그를 만들려면 어떻게 해야 합니까?	태그 만들기
룰베이스(rulebase)를 그룹으로 보려면 어떻게 해야 합니까?	룰베이스(rulebase)를 그룹으로 보기
태그가 지정된 규칙을 검색합니다. 태그를 사용하여 규칙을 그룹화합니다. 정책에 사용되는 태그를 봅니다. 정책에 태그를 적용합니다.	태그 관리
더 찾고 계십니까**?**	• 태그를 사용하여 개체를 그룹화하고 시각적으로 구분합니다. • SD-WAN 링크 태그

태그 만들기

- 개체 > 태그

태그를 선택하여 태그를 만들거나, 색상을 할당하거나, 태그를 삭제, 이름 바꾸기 및 복사합니다. 각 개체에는 최대 64개의 태그가 있을 수 있습니다. 개체에 태그가 여러 개 있는 경우 적용된 첫 번째 태그의 색상이 표시됩니다.

방화벽에서 태그 탭에는 방화벽에서 로컬로 정의하거나 Panorama에서 방화벽으로 푸시하는 태그가 표시됩니다. Panorama에서 태그 탭에는 Panorama에서 정의한 태그가 표시됩니다. 이 탭에는 동적 주소 그룹을 형성하기 위해 방화벽에 정의된 VM 정보 소스에서 동적으로 검색된 태그를 표시하지 않으며 XML 또는 REST API를 사용하여 정의된 태그를 표시하지도 않습니다.

새 태그를 생성하면 현재 방화벽이나 Panorama에서 선택된 가상 시스템 또는 디바이스 그룹에 태그가 자동으로 생성됩니다.

태그 설정	설명
이름	고유한 태그 이름(최대 127자)을 입력합니다. 이름은 대/소문자로 구분되지 않습니다.
공유	태그를 사용할 수 있도록 하려면 다음 옵션을 선택합니다. • 멀티 vsys 방화벽의 모든 가상 시스템(vsys)입니다. 이 선택을 취소하면 태그는 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 옵션을 사용하지 않도록 설정하지 않으면 개체 탭에서 선택한 디바이스 그룹에서만 태그를 사용할 수 있습니다.
재정의 비활성화(Panorama 전용)	이 옵션을 선택하여 관리자가 태그를 상속하는 디바이스 그룹에서 이 태그의 설정을 재정의하지 못하도록 합니다. 이 선택은 기본적으로 지워지므로 관리자는 태그를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
색상	드롭다운의 색상 팔레트에서 색상을 선택합니다(기본값은 없음).
코멘트	태그가 사용되는 내용을 설명하기 위해 레이블 또는 설명을 추가합니다.

- 태그 추가: 태그를 추가한 다음 다음 필드를 입력합니다.

  정책 탭에서 정책을 만들거나 편집할 때 새 태그를 만들 수도 있습니다. 태그는 현재 선택된 디바이스 그룹 또는 가상 시스템에서 자동으로 만들어집니다.
- 태그 편집: 태그를 클릭하여 태그를 편집, 이름 바꾸기 또는 태그에 색상을 할당합니다.
- 태그 삭제: 삭제를 클릭하고 태그를 선택합니다. 사전 정의된 태그를 삭제할 수 없습니다.
- 태그를 이동하거나 복사합니다. 태그를 이동하거나 복사하는 옵션을 사용하면 태그를 복사하거나 여러 가상 시스템을 사용하도록 설정한 방화벽의 다른 디바이스 그룹 또는 가상 시스템으로 태그를 이동할 수 있습니다.

  이동 또는 복사하고 태그를 선택합니다. 대상 위치(디바이스 그룹 또는 가상 시스템)를 선택합니다. 유효성 검사 프로세스가 오류를 표시하기 전에 개체에 대한 모든 오류를 검색하려는 경우 유효성 검사에

서 처음 감지된 오류에 오류가 발생하도록 설정(지우기)합니다. 이 옵션은 기본적으로 활성화되며 첫 번째 오류가 감지되고 오류만 표시될 때 유효성 검사 프로세스가 중지됩니다.

- 태그를 재정의하거나 되돌리기(Panorama만): 재정의 옵션은 태그를 만들 때 재정의 설정 옵션을 선택하지 않은 경우에만 사용할 수 있습니다. 재정의 옵션을 사용하면 공유 또는 조상 요소 디바이스 그룹에서 상속된 태그에 할당된 색상을 재정의할 수 있습니다. 위치는 현재 디바이스 그룹입니다. 향후 재정의 시도를 방지하기 위해 재정의를 비활성화할 수도 있습니다.

  변경 내용을되돌리면 태그의 최근 수정을 취소합니다. 태그를 되돌리면 위치 필드에 태그가 상속된 디바이스 그룹 또는 가상 시스템이 표시됩니다.

룰베이스(rulebase)를 그룹으로 보기

- 선언 > **<Rulebase Type>**

룰베이스**(rulebase)**를 그룹 태그로 표시하려면 그룹으로 봅니다. 룰베이스(rulebase)를 그룹으로 보는 동안 정책 순서와 우선 순위가 유지됩니다. 이 보기에서 그룹 태그를 선택하여 해당 태그로 그룹화된 모든 규칙을 봅니다.

룰베이스(rulebase)를 그룹으로 볼 때 그룹을 클릭하여 선택한 태그 그룹의 모든 규칙을 이동, 변경, 삭제 또는 복사합니다. 다음 표는 룰베이스(rulebase)를 그룹으로 볼 때 사용할 수 있는 규칙 관리 옵션에 대해 설명합니다.

선택	설명
그룹의 규칙을 다른 룰베이스(rulebase) 또는 디바이스 그룹으로 이동	선택한 태그 그룹의 모든 정책 규칙을 다른 룰베이스(rulebase) 또는 디바이스 그룹으로 이동합니다.
모든 규칙 그룹 변경	선택한 태그 그룹의 모든 규칙을 다른 태그 그룹으로 이동합니다.
그룹의 모든 규칙 이동	룰베이스(rulebase) 내에서 선택한 태그 그룹의 모든 규칙을 이동합니다.
그룹의 모든 규칙 삭제	선택한 태그 그룹의 모든 규칙을 삭제합니다.
그룹의 모든 규칙 복사	선택한 태그 그룹의 모든 규칙을 복사합니다.

그룹의 규칙을 다른 룰베이스**(rulebase)** 또는 디바이스 그룹으로 이동

규칙 기준을 구성해야 하는 경우 이동할 규칙이 포함된 태그 그룹을 선택한 다음 그룹의 규칙을 다른 룰베이스**(rulebase)** 또는 디바이스 그룹으로 이동하여 각 규칙을 개별적으로 이동하는 대신 다른 룰베이스(rulebase) 또는 디바이스 그룹에 다시 할당합니다. 태그 그룹의 규칙을 다른 디바이스 그룹으로 이동하기 전에 디바이스 그룹이 이미 존재해야 합니다(도중에는 생성할 수 없음). 또한 태그 그룹의 규칙을 동일한 디바이스 그룹 내의 다른 규칙 기반으로 이동할 수 있습니다.

규칙을 다른 규칙 기준 또는 디바이스 그룹으로 이동하려면 다음을 입력합니다.

필드	설명
데스티네이션	정책 규칙을 이동할 대상 디바이스 그룹입니다.
(Panorama만 해당) 대상 유형	규칙을 대상 디바이스 그룹의 사전 규칙 기준 또는 사후 규칙 기반으로 이동할지 선택합니다.
규칙 순서	규칙을 이동할 규칙 기준의 위치를 선택합니다. 다음을 선택할 수 있습니다. • 맨 위로 이동 —대상 장치 그룹의 룰베이스(rulebase) 맨 위로 규칙을 이동합니다. • 맨 아래로 이동 —대상 장치 그룹의 룰베이스(rulebase) 끝으로 규칙을 이동합니다. • 규칙 전 —대상 장치 그룹의 룰베이스(rulebase)에서 선택한 규칙 앞으로 규칙을 이동합니다. • 규칙 이후 —대상 장치 그룹의 룰베이스(rulebase)에서 선택한 규칙 다음으로 규칙을 이동합니다.
유효성 검사에서 처음 감지된 오류에 대한 오류 발생	유효성 검사 중에 오류가 발생할 경우 오류가 표시되는 방식을 결정하려면 이 상자를 선택합니다. 이 옵션을 선택하면 각 오류가 개별적으로 표시됩니다. 이 옵션을 선택하지 않으면 오류가 통합되어 단일 오류로 표시됩니다. 유효성 검사 중 오류가 감지되면 규칙 이동 작업이 실패하고 어떤 규칙도 대상 디바이스 그룹으로 이동되지 않습니다.

모든 규칙 그룹 변경

각 규칙을 편집하는 대신 모든 규칙 그룹을 변경하여 한 태그 그룹에서 다른 기존 태그 그룹으로 설정된 전체 정책 규칙을 이동합니다. 태그 그룹 규칙의 규칙 순서는 새 태그 그룹으로 이동할 때 유지되지만 대상 태그 그룹의 규칙 이전 또는 이후에 새 규칙을 배치할 수 있습니다.

규칙을 다른 태그 그룹으로 이동하려면 대상 태그 그룹을 지정하고 이동된 규칙을 배치합니다.

필드	설명
모양 순서에 대한 그룹 선택	대상 태그 그룹을 선택합니다.
위쪽 이동	위쪽 이동은 대상 태그 그룹의 맨 위에 규칙을 삽입합니다.
아래쪽 이동	아래쪽 이동은 대상 태그 그룹의 맨 아래에 규칙을 삽입합니다.

그룹의 모든 규칙 이동

각 규칙을 개별적으로 재정렬하는 대신 그룹의 모든 규칙 이동을 선택하여 선택한 태그 그룹의 모든 규칙을 규칙 레이어 구조 위나 아래로 이동합니다. 태그 그룹을 이동할 때 태그 그룹 규칙에서 이동된 규칙 순서는 유지되지만 대상 태그 그룹의 규칙 앞에 또는 이후에 규칙을 배치할 수 있습니다.

규칙을 이동하려면 대상 태그 그룹과 이동된 규칙을 배치할 위치를 지정합니다.

필드	설명
모양 순서에 대한 그룹 선택	대상 태그 그룹을 선택합니다.
위쪽 이동	위쪽 이동은 대상 태그 그룹 앞에 규칙을 삽입합니다.
아래쪽 이동	아래쪽 이동은 대상 태그 그룹 이후에 규칙을 삽입합니다.

그룹의 모든 규칙 삭제

규칙 관리를 단순화하기 위해 그룹의 모든 규칙을 삭제하여 보안 위험을 줄이고 선택한 태그 그룹과 연결된 사용되지 않거나 원치 않는 규칙을 삭제하여 정책 규칙 기준을 구성할 수 있습니다.

그룹의 모든 규칙 복사

태그 그룹에서 기존 정책 규칙을 수동으로 다시 생성하는 대신 그룹의 모든 규칙을 복사하여 디바이스 그룹 및 선택한 규칙 베이스에서 선택한 태그 그룹의 규칙을 빠르게 복사합니다. 디바이스 그룹은 태그 그룹의 규칙을 다른 디바이스 그룹으로 복사하기 전에 이미 존재해야 합니다(도중에는 생성할 수 없음). 또한 태그 그룹의 규칙을 동일한 디바이스 그룹 내의 다른 규칙 베이스에 복사할 수 있습니다.

복제된 규칙은 규칙 이름과 `<Rule Name>-1` 형식으로 추가됩니다. 규칙이 복사된 첫 번째 규칙과 동일한 위치에 복사되고 이름이 변경되지 않은 경우 이름이 추가됩니다. 예를 들어,`<Rule Name>-2`, `<Rule Name>-3`등이 있습니다.

규칙을 복사하려면 다음 필드를 구성합니다.

필드	설명
데스티네이션	복사된 정책 규칙의 대상 디바이스 그룹입니다.
(Panorama만 해당) 대상 유형	대상 디바이스 그룹의 사전 규칙 베이스 또는 사후 규칙 베이스에 규칙을 복사할지의 여부를 선택합니다.
규칙 순서	규칙 베이스에서 규칙을 복사할 위치를 선택합니다. 다음을 선택할 수 있습니다.

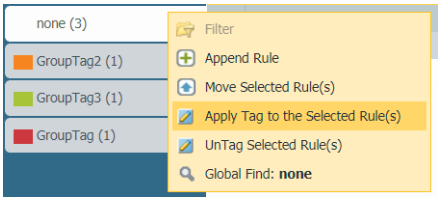
필드	설명
	• 맨 위로 이동 - 대상 디바이스 그룹의 규칙 베이스 맨 위에 복사된 규칙을 삽입합니다. • 맨 아래로 이동 - 대상 디바이스 그룹의 규칙 베이스 끝에 복사된 규칙을 삽입합니다. • 규칙 전 - 대상 디바이스 그룹의 규칙 베이스에서 선택한 규칙 앞에 복사된 규칙을 삽입합니다. • 규칙 이후 - 대상 디바이스 그룹의 규칙 베이스에서 선택한 규칙 뒤에 복사된 규칙을 삽입합니다.
유효성 검사에서 처음 감지된 오류에 대한 오류 출력	유효성 검사 중에 오류가 발생한 경우 오류가 표시되는 방법을 결정하려면 이 옵션을 선택합니다. 활성화하면 각 오류가 개별적으로 표시됩니다. 비활성화(선택 취소)된 경우 오류가 통합되어 단일 오류로 표시됩니다. 유효성 검사 중 오류가 감지되면 규칙 복사 작업이 실패하고 대상 디바이스 그룹에 규칙이 복사되지 않습니다.

태그 관리

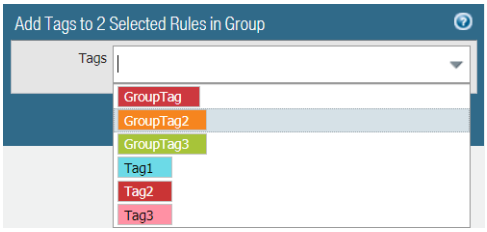
다음 표에는 그룹 태그별로 규칙을 그룹화할 때 수행할 수 있는 작업이 나열됩니다.

◉ 규칙을 태그합니다.

1. 규칙을 그룹으로 보기를 선택합니다.
2. 오른쪽 창에서 하나 이상의 규칙을 선택합니다.
3. 그룹 태그 드롭다운에서 선택한 규칙에 태그를 적용합니다.

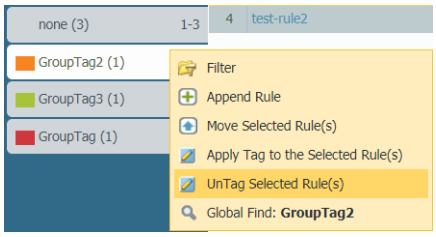


4. 선택한 규칙에 태그를 추가합니다.

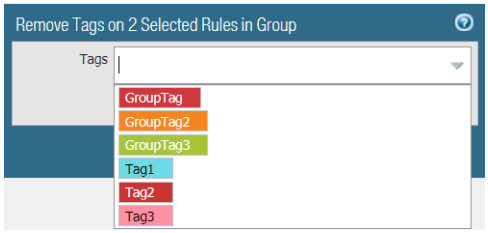


- 그룹 태그가 할당된 규칙을 봅니다.
  1. 규칙이 할당된 그룹 태그를 보려면 룰베이스**(rulebase)**를 그룹으로 봅니다.
  2. 그룹 태그를 표시하려면 오른쪽 창이 업데이트됩니다. 선택한 태그가 있는 규칙입니다.
  3. 그룹에 할당된 규칙을 보려면 그룹 태그를 선택합니다. 그룹 태그가 할당되지 않은 규칙은 없음 그룹에 나열됩니다.

- 규칙의 태그를 취소합니다.
  1. 규칙이 할당된 그룹 태그를 보려면 룰베이스**(rulebase)**를 그룹으로 봅니다.
  2. 오른쪽 창에서 하나 이상의 규칙을 선택합니다.
  3. 그룹 태그 드롭다운에서 선택한 규칙에 태그를 적용합니다.

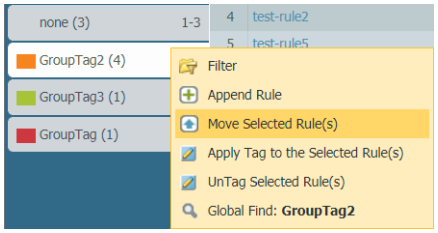


  4. 선택한 규칙에 대한 태그를 제거합니다. 또한 규칙에 할당된 모든 태그를 삭제할 수 있습니다.



- 태그를 사용하여 규칙을 다시 정렬합니다.

  룰베이스**(rulebase)**를 그룹으로 볼때 그룹 태그에서 하나 이상의 규칙을 선택한 다음 규칙 번호 위로 마우스를 가져가서 드롭다운에서 선택한 규칙 이동을 선택합니다. 선택한 그룹 태그의 모든 규칙을 이동하려는 경우 규칙을 선택하지 마십시오.



  이동 규칙 창의 드롭다운에서 그룹 태그를 선택한 다음 드롭다운에서 선택한 태그를 앞으로 이동할지 또는 뒤로 이동할지 선택합니다.

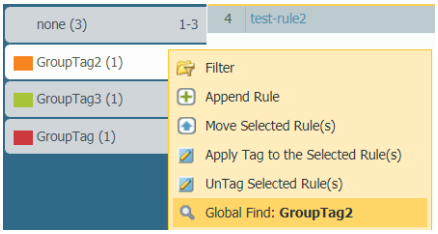
- 선택한 태그를 적용하는 새 규칙을 추가합니다.

  룰베이스**(rulebase)**를 그룹으로, 볼때 그룹 태그 위로 마우스를 가져가서 드롭다운에서 부속 규칙을 선택합니다.

  새 규칙은 그룹 태그에 할당된 규칙 목록의 끝에 추가됩니다.

- 그룹 태그를 검색합니다.

  룰베이스**(rulebase)**를 그룹으로 볼때 그룹 태그 위로 마우스를 가져가고 드롭다운에서 글로벌 찾기를 선택합니다.



- 태그 구성 테이블을 내보냅니다.

  관리 역할은 개체 구성 테이블을 **PDF/CSV** 형식으로 내보낼 수 있으며 필터를 적용하여 테이블 출력을 사용자 지정하여 필요한 열만 포함할 수 있습니다. 내보낸 대화 내보내기에 표시되는 열만 있습니다. 구성 테이블 데이터 내보내기를 참조하십시오.

개체 > 디바이스

디바이스 사전이라고도 하는 이 페이지에는 디바이스 개체에 대한 메타데이터가 포함되어 있습니다. 기존 디바이스 개체에 대한 정보를 검토하거나 새 디바이스 개체를 추가합니다. 디바이스 개체를 보안 정책의 일치 기준으로 사용하면 방화벽이 새 디바이스 및 기존 디바이스에 보안 정책을 동적으로 업데이트하고 적용하는 디바이스 기반 정책을 만들 수 있습니다. Palo Alto Networks는 디바이스 > 동적 업데이트 > 디바이스 **ID** 콘텐츠에서 볼 수 있는 동적 업데이트를 통해 디바이스 사전을 업데이트합니다.

버튼/필드	설명
이름	디바이스 개체의 이름입니다.
위치	디바이스 개체에 대한 디바이스 그룹의 위치입니다.
카테고리	디바이스 개체의 카테고리(예: ### #####)입니다.
프로파일	디바이스 개체의 디바이스 프로파일입니다.
모델	디바이스 개체의 모델입니다.
OS 버전	디바이스 개체의 OS 버전입니다.
OS 제품군	디바이스 개체의 OS 패밀리입니다.
공급자	디바이스 개체에 대한 공급자입니다.
추가	새 디바이스 개체를 추가하려면 추가를 클릭합니다. 이름을 입력하고 선택적으로 설명합니다. 카테고리, **OS** 및 모델과 같은 디바이스에 대한 추가 메타데이터를 선택합니다. 추가하려는 디바이스를 선택하려면 디바이스 목록을 찾아볼 수도 있습니다. 확인을 클릭하여 변경 사항을 확인합니다.
삭제	더 이상 필요하지 않은 디바이스 개체를 선택한 다음 삭제합니다.
이동	이동할 디바이스 개체를 선택한 다음 이동합니다.
복사	새 디바이스 프로파일을 기반으로 하는 디바이스 개체를 선택한 다음 복사합니다.
PDF/CSV	**PDF/CSV** 형식으로 디바이스 목록을 내보냅니다. 필터를 적용하여 필요에 따라 보다 구체적인 출력을 만들 수 있습

버튼/필드	설명
	니다. 웹 인터페이스에서 표시되는 열만 내보낼 것입니다. 구성 테이블 내보내기를 참조하십시오.

개체 > 외부 동적 목록

외부 동적 목록은 트래픽을 차단하거나 허용하는 정책 규칙에서 사용할 수 있는 IP 주소, URL, 도메인 이름, IMEI(International Mobile Equipment Identities) 또는 IMSI(International Mobile Subscriber Identities)의 불러온 목록을 기반으로 하는 주소 개체입니다. 이 목록은 방화벽에서 액세스할 수 있는 웹 서버에 저장된 텍스트 파일이어야 합니다. 기본적으로 방화벽은 관리(MGT) 인터페이스를 사용하여 이 목록을 검색합니다.

활성 위협 예방 라이선스를 통해 Palo Alto Networks는 악성 호스트를 차단하는 데 사용할 수 있는 여러 내장 동적 IP 목록을 제공합니다. 최신 위협 연구를 기반으로 목록을 매일 업데이트합니다.

IP 주소 목록을 정책 규칙의 소스 및 대상에서 주소 개체로 사용할 수 있습니다. URL 필터링 프로필(개체 > 보안 프로파일 > URL 필터링)에서 URL 목록을 사용하거나 보안 정책 규칙의 일치 기준으로 사용할 수 있습니다. 그리고 도메인 목록(개체 > 보안 프로파일 > 안티스파이웨어 프로파일)을 지정된 도메인 이름에 대한 싱크홀로 사용할 수 있습니다.

각 방화벽 모델에서 모든 보안 정책 규칙에 걸쳐 고유한 소스가 있는 최대 30개의 외부 동적 목록을 사용할 수 있습니다. 방화벽이 각 목록 유형에 대해 지원하는 최대 항목 수는 방화벽 모델에 따라 다릅니다(각 외부 동적 목록 유형에 대한 다른 방화벽 제한 참조). 목록 항목은 외부 동적 목록이 정책 규칙에서 사용되는 경우에만 최대값에 포함됩니다. 모델이 지원하는 최대 항목 수를 초과하는 경우 방화벽은 시스템 로그를 생성하고 제한을 초과하는 항목을 건너뜁니다. 현재 정책 규칙에 사용되는 IP 주소, 도메인, URL, IMEI 및 IMSI의 수와 방화벽에서 지원되는 총 수를 확인하려면 목록 용량(방화벽만 해당)을 선택합니다.

외부 동적 목록은 평가되는 순서대로 위에서 아래로 표시됩니다. 목록을 재정렬하려면 페이지 하단의 방향 컨트롤을 사용하십시오. 가장 중요한 항목이 있는 외부 동적 목록을 맨 위로 이동하여 용량 제한에 도달하기 전에 커밋되도록 할 수 있습니다.

유형별 그룹화가 활성화된 경우 외부 동적 목록의 순서를 변경할 수 없습니다.

외부 동적 목록을 호스팅하는 서버에서 최신 버전의 외부 동적 목록을 검색하려면 외부 동적 목록을 선택하고 지금 가져오기를 클릭합니다.

Palo Alto Networks 악성 *IP* 주소 피드의 설정을 삭제, 복사 또는 편집할 수 없습니다.

새 외부 동적 목록을 추가하고 아래 표에 설명된 설정을 구성합니다.

외부 동적 목록 설정	설명
이름	외부 동적 목록을 식별하는 이름을 입력합니다(최대 32자). 이 이름은 정책 규칙 시행 목록을 식별합니다.
공유	외부 동적 목록을 다음에 사용할 수 있도록 하려면 이 옵션을 활성화합니다.

외부 동적 목록 설정	설명
(여러 가상 시스템(multi-vsys) 및 Panorama 전용)	• Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 옵션을 비활성화(선택 취소)하면 외부 동적 목록은 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 옵션을 비활성화(해제)하면 외부 동적 목록은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 외부 동적 목록 개체의 설정을 무시하지 못하게 하려면 이 옵션을 활성화합니다. 이 옵션은 기본적으로 비활성화(선택 취소)되어 있으며, 이는 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
테스트 소스 URL(방화벽만 해당)	소스 **URL**을 테스트하여 방화벽이 외부 동적 목록을 호스팅하는 서버에 연결할 수 있는지 확인합니다. 이 테스트는 서버가 성공적으로 인증되었는지의 여부를 확인하지 않습니다.
목록 탭 만들기	
유형 단일 목록에 *IP* 주소, *URL* 및 도메인 이름을 혼합할 수 없습니다. 각 목록에는 한 가지 유형의 항목만 포함되어야 합니다.	다음 유형의 외부 동적 목록에서 선택합니다. • 사전 정의된 **IP** 목록 - Palo Alto Networks가 불렛프루프 IP 주소, 알려진 악성 IP 주소 또는 고위험 IP 주소로 식별하는 목록을 목록 항목의 소스로 사용합니다(활성 위협 예방 라이선스 필요). • 사전 정의된 **URL** 목록 - Palo Alto Networks가 인증 정책에서 이러한 도메인을 제외하기 위해 신뢰할 수 있는 것으로 식별하는 도메인 목록을 사용합니다. • **IP** 목록(기본값) - 각 목록에는 IPv4 또는 IPv6 주소, 주소 범위 및 서브넷이 포함될 수 있습니다. 목록에는 한 줄에 하나의 IP 주소, 범위 또는 서브넷만 포함되어야 합니다. 예: `192.168.80.150/32 2001:db8:123:1::1 ## 2001:db8:123:1::/64 192.168.80.0/24 2001:db8:123:1::1 - 2001:db8:123:1::22` , 위의 예에서 첫 번째 줄은 192.168.80.0부터 192.168.80.255까지의 모든 주소를 나타냅니다. 서브넷 또는 IP 주소 범위(예:

외부 동적 목록 설정	설명

	92.168.20.0/24 또는 192.168.20.40 – 192.168.20.50)는 여러 IP 주소가 아닌 하나의 IP 주소 항목으로 계산됩니다.
	• 도메인 목록 - 각 목록에는 한 줄에 하나의 도메인 이름 항목만 포함될 수 있습니다. 예:
	`www.p301srv03.paloalonetworks.com ftp.example.co.uk test.domain.net`
	외부 동적 목록에 포함된 도메인 목록에 대해 방화벽은 중간 심각도의 스파이웨어 유형의 사용자 지정 서명 집합을 생성하므로 사용자 지정 도메인 목록에 싱크홀 작업을 사용할 수 있습니다.
	• **URL** 목록 - 각 목록에는 한 줄에 하나의 URL 항목만 있을 수 있습니다. 예:
	`Financialtimes.co.in www.wallaby.au/joey www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx *.example.com/*`
	URL 목록은 허용입니다. 기본 작업을 편집하려면 개체 > 보안 프로파일 > URL 필터링을 참조하십시오.
	IP, 도메인 또는 URL 목록 항목을 생성할 때 외부 동적 목록 형식 지정 지침을 참조하십시오.

유형(계속)	• 가입자 **ID** 목록 - 각 목록에는 3G, 4G 또는 5G 네트워크에 대한 가입자 ID가 포함되어 있습니다. 소스 필드에 목록에 액세스할 방화벽의 URL을 입력합니다. • 장비 **ID** 목록 - 각 목록에는 3G, 4G 또는 5G 네트워크에 대한 장비 ID가 포함되어 있습니다. 소스 필드에 목록에 액세스할 방화벽의 URL을 입력합니다. 외부 동적 목록 및 정적 항목이 지원해야 하는 *3G*, *4G* 및 *5G* 네트워크 식별자의 총 수를 기반으로 구매할 방화벽 모델을 결정합니다.
설명	외부 동적 목록에 대한 설명을 입력합니다(최대 255자).
소스	• 외부 동적 목록이 사전 정의된 IP 목록인 경우 **Palo Alto Networks - Bulletproof IP** 주소, **Palo Alto Networks** - 고위험 **IP** 주소 또는 **Palo Alto Networks** - 알려진 악성 **IP** 주소를 목록 소스로 선택합니다.

외부 동적 목록 설정	설명
	• 외부 동적 목록이 사전 정의된 URL 목록인 경우 기본 설정은 **panw-auth-portal-exclude-list**입니다. • 외부 동적 목록이 IP 목록, 도메인 목록 또는 URL 목록인 경우 텍스트 파일이 포함된 HTTP 또는 HTTPS URL 경로(예: **`http://192.0.2.20/myfile.txt`**)를 입력합니다. • 외부 동적 목록이 도메인 목록인 경우 자동으로 확장하여 하위 도메인을 포함할 수 있습니다. 이 옵션을 사용하면 PAN-OS® 소프트웨어가 외부 동적 목록 파일에 나열된 도메인 이름의 모든 하위 수준 구성 요소를 평가할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다. • 외부 동적 목록이 가입자 식별 목록 또는 장비 식별 목록인 경우 목록이 포함된 URL 경로를 입력하십시오. 외부 동적 목록에 하위 도메인이 포함된 경우 이러한 확장 항목은 어플라이언스 모델 용량 수에 포함됩니다. 하위 도메인을 수동으로 정의하려면 이 기능을 비활성화할 수 있습니다. 그러나 이 기능을 비활성화하면 목록에서 명시적으로 정의하지 않는 한 정책 규칙에 의해 하위 도메인이 평가되지 않습니다.
인증서 프로파일 (IP 목록, 도메인 목록 또는 URL 목록만 해당)	외부 동적 목록에 HTTPS URL이 있는 경우 목록을 호스팅하는 웹 서버를 인증하기 위해 기존 인증서 프로파일(방화벽 및 Panorama)을 선택하거나 새 인증서 프로파일(방화벽만 해당)을 만듭니다. 인증서 프로파일 구성에 대한 자세한 내용은 디바이스 > 인증서 관리 > 인증서 프로파일을 참조하십시오. 기본: 없음(인증서 프로파일 비활성화) 정책을 시행하는 데 사용할 수 있는 외부 동적 목록의 수를 최대화하려면 동일한 인증서 프로파일을 사용하여 동일한 소스 *URL*에서 외부 동적 목록을 인증하십시오. 이러한 목록은 하나의 외부 동적 목록으로만 계산됩니다. 그렇지 않으면 다른 인증서 프로필을 사용하는 동일한 소스 *URL*의 외부 동적 목록이 고유한 외부 동적 목록으로 계산됩니다.
클라이언트 인증	기본 HTTP 인증이 필요한 외부 동적 목록 소스에 액세스할 때 방화벽이 사용할 사용자명과 암호를 추가하려면 이 옵션을 활성화합니다(기본적으로 비활성화됨). 이 설정은 외부 동적 목록에 HTTPS URL이 있는 경우에만 사용할 수 있습니다.

외부 동적 목록 설정	설명
	• 사용자명 - 목록에 액세스하려면 유효한 사용자명을 입력하십시오. • 암호/암호 확인 - 사용자명의 암호를 입력하고 확인합니다.
업데이트 확인	방화벽이 웹 서버에서 목록을 검색하는 빈도를 지정합니다. 간격을 **5**분마다(기본값), 매시간, 매일, 매주 또는 매월로 설정할 수 있습니다. 인터벌은 마지막 커밋을 기준으로 합니다. 예를 들어, 5분 간격을 선택하면 마지막 커밋이 1시간 전이라면 5분 후에 커밋이 발생합니다. 커밋은 목록을 참조하는 모든 정책 규칙을 업데이트합니다. 방화벽은 활성 *Threat Prevention* 라이선스로 콘텐츠 업데이트를 동적으로 수신하므로 미리 정의된 *IP* 목록에 대한 빈도를 지정할 필요가 없습니다.
목록 항목 및 예외 탭	
항목 나열	외부 동적 목록의 항목을 표시합니다. • 항목을 목록 예외로 추가 - 최대 100개의 항목을 선택한 다음 제출(→)합니다. • 항목에 대한 **AutoFocus** 위협 인텔리전스 요약 보기 - 항목 위로 마우스를 가져간 다음 드롭다운에서 **AutoFocus**를 선택합니다. 항목 요약을 보려면 AutoFocus™ 라이선스가 있고 AutoFocus 위협 인텔리전스를 활성화해야 합니다(**Device** > **Setup** > **Management**를 선택한 다음 **AutoFocus** 설정 편집). • **IP** 주소, 도메인 또는 **URL**이 외부 동적 목록에 있는지 확인 - 필터 필드에 값을 입력하고 필터 적용(→). 전체 목록으로 돌아가려면 필터(**[X]**)를 지우십시오.
수동 예외	외부 동적 목록에 대한 예외를 표시합니다. • 예외 편집 - 예외를 선택한 다음 변경합니다. • 수동으로 예외 입력 - 수동으로 새 예외를 추가합니다. • 수동 예외 목록에서 예외 제거 - 예외를 선택한 다음 삭제합니다. • **IP** 주소, 도메인 또는 **URL**이 수동 예외 목록에 있는지 확인 - 필터 필드에 값을 입력하고 필터 적용(→)을 합니다. 전체 목록으로 돌아가려면 필터(**[X]**)를 지우십시오. 수동

외부 동적 목록 설정	설명
	예외 목록에 중복 항목이 있는 경우 변경 사항을 외부 동적 목록에 저장할 수 없습니다.

개체 > 사용자 정의 개체

정책과 함께 사용할 사용자 지정 데이터 패턴, 취약성 및 스파이웨어 서명, URL 카테고리를 생성합니다.

- 개체 > 사용자 정의 개체 > 데이터 패턴
- 개체 > 사용자 정의 개체 > 스파이웨어/취약점
- 개체 > 사용자 정의 개체 > URL 카테고리

개체 > 사용자 정의 개체 > 데이터 패턴

다음 항목에서는 데이터 패턴에 대해 설명합니다.

무엇을 찾고 계십니까?	참조:
데이터 패턴을 생성합니다.	데이터 패턴 설정
정규식 데이터 패턴의 구문에 대해 자세히 알아보고 몇 가지 예를 참조하세요.	정규식 데이터 패턴의 구문 정규식 데이터 패턴 예제

데이터 패턴 설정

개체 > 사용자 정의 개체 > 데이터 패턴을 선택하여 필터링하려는 민감한 정보의 카테고리를 정의합니다. 데이터 필터링 프로파일 정의에 대한 자세한 내용은 개체 > 보안 프로파일 > 데이터 필터링을 선택합니다.

중요한 정보를 검색할 때 방화벽에 사용할 세 가지 유형의 데이터 패턴을 만들 수 있습니다.

- 사전 정의 - 사전 정의된 데이터 패턴을 사용하여 사회 보장 및 신용카드 번호에 대한 파일을 스캔합니다.
- 정규식 - 정규식을 사용하여 사용자 정의 데이터 패턴을 생성합니다.
- 파일 속성 - 특정 파일 속성 및 값에 대해 파일을 스캔합니다.

데이터 패턴 설정	설명
이름	데이터 패턴 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	데이터 패턴에 대한 설명을 입력합니다(최대 255자).
공유	데이터 패턴을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다.

데이터 패턴 설정	설명
	• 멀티 vsys 방화벽의 모든 가상 시스템(vsys)입니다. 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 데이터 패턴을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에서만 데이터 패턴을 사용할 수 있습니다.
재정의 비활성화(Panorama 전용)	관리자가 개체를 상속하는 디바이스 그룹에서 이 데이터 패턴 개체의 설정을 재정의하지 못하도록 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
패턴 유형	생성할 데이터 패턴 유형을 선택합니다. • 사전 정의된 패턴 • 정규식 • 파일 속성
사전 정의된 패턴	Palo Alto Networks는 신용카드 번호 또는 주민등록번호와 같은 파일에서 특정 유형의 정보를 스캔하기 위해 사전 정의된 데이터 패턴을 제공합니다. 사전 정의된 패턴을 기반으로 데이터 필터링을 구성하려면 패턴을 추가하고 다음을 선택합니다. • 이름 - 민감한 데이터를 필터링하는 데 사용할 사전 정의된 패턴을 선택합니다. 사전 정의된 패턴을 선택하면 설명이 자동으로 채워집니다. • 사전 정의된 패턴을 감지할 파일 형식을 선택합니다.
정규식	사용자 정의 데이터 패턴을 추가하십시오. 패턴에 설명이 포함된 이름을 지정하고 데이터 패턴을 검색할 파일 형식을 설정한 다음 데이터 패턴을 정의하는 정규식을 입력합니다. 정규식 데이터 패턴 구문 세부 정보 및 예제는 다음을 참조하세요. • 정규식 데이터 패턴의 구문 • 정규식 데이터 패턴 예제
파일 속성	파일 속성 및 관련 값을 스캔하는 데이터 패턴을 빌드합니다. 예를 들어 문서 제목에 "민감한", "내부" 또는 "기밀"이라는 단어가 포함된 Microsoft Word 문서 및 PDF를 필터링할 데이터 패턴을 추가합니다. • 데이터 패턴에 설명이 포함된 이름을 지정합니다. • 스캔할 파일 형식을 선택합니다. • 특정 값을 검색할 파일 속성을 선택합니다.

데이터 패턴 설정	설명
	• 스캔할 속성 값을 입력합니다.

정규식 데이터 패턴의 구문

데이터 패턴을 생성하기 위한 일반 패턴 요구 사항 및 구문은 사용하는 패턴 일치 엔진(클래식 또는 Advanced(기본값))에 따라 다릅니다.

패턴 요구 사항	전형적	향상된
패턴 길이	마침표(`.`), 별표(*), 더하기 기호(+) 또는 범위(`[a-z]`)를 포함할 수 없는 7개의 리터럴 문자가 필요합니다.	두 개의 리터럴 문자가 필요합니다.
대소문자를 구분하지 않음	용어의 모든 변형과 일치하도록 가능한 모든 문자열에 대한 패턴을 정의해야 합니다. 예시: 기밀로 지정된 문서를 일치시키려면 "confidential", "Confidential" 및 "CONFIDENTIAL"을 포함하는 패턴을 만들어야 합니다.	하위 패턴에서 **`i`** 옵션을 사용할 수 있습니다. 예: **`((?i)\bconfidential\b)`**는 `Confidential`과 일치합니다.

PAN-OS®의 정규식 구문은 기존 정규식 엔진과 유사하지만 모든 엔진이 고유합니다. Classic Syntax 및 Enhanced Syntax 테이블은 PAN-OS 패턴 일치 엔진에서 지원되는 구문을 설명합니다.

전형적 구문

패턴 구문	설명
.	임의의 단일 문자와 일치합니다.
?	선행 문자 또는 표현식을 0~1회 일치시킵니다. 괄호 안에 일반 표현식을 포함해야 합니다. 예: **`(abc)?`**
*	앞의 문자 또는 표현식을 0번 이상 찾습니다. 괄호 안에 일반 표현식을 포함해야 합니다. 예: **`(abc)*`**
+	선행 문자 또는 정규식을 한 번 이상 찾습니다. 괄호 안에 일반 표현식을 포함해야 합니다.

패턴 구문	설명
	예: **(abc)+**
|	하나의 "OR"을 지정하십시오.  괄호 안에 대체 부분 문자열을 포함해야 합니다. 예: **((bif)|(scr)|(exe))**는 bif, scr 또는 exe와 일치합니다.
-	범위를 지정합니다. 예: **[c-z]**는 c와 z(포함) 사이의 모든 문자와 일치합니다.
[ ]	지정된 문자와 일치합니다. 예: **[abz]**는 지정된 문자(a, b 또는 z) 중 하나와 일치합니다.
^	지정된 문자를 제외한 모든 문자를 찾습니다. 예: **[^abz]**는 지정된 문자(a, b 또는 z)를 제외한 모든 문자와 일치합니다.
{ }	최소값과 최대값이 포함된 문자열을 찾습니다. 예: **{10-20}**은 10~20바이트(포함) 사이의 모든 문자열과 일치합니다. 고정 문자열 바로 앞에 지정해야 하며 하이픈(**-**)만 사용할 수 있습니다.
\	임의의 문자에 대해 리터럴 일치를 수행합니다. 지정된 문자 앞에는 백슬래시(****)가 있어야 합니다.
&amp	앰퍼샌드(&)는 특수 문자이므로 문자열에서 &를 찾으려면 **&amp**를 사용해야 합니다.

향상된 구문

향상된 패턴 일치 엔진은 모든 전형적 구문과 다음 구문을 지원합니다.

패턴 구문	설명
속기 문자 클래스	숫자나 공백과 같은 특정 유형의 문자를 나타내는 기호입니다. 대문자를 사용하여 이러한 약식 문자 클래스를 무효화할 수 있습니다.

패턴 구문	설명
\s	모든 공백 문자와 일치합니다. 예: **\s**는 공백, 탭, 줄 바꿈 또는 양식 피드와 일치합니다.
\d	숫자 [0-9]인 문자를 찾습니다. 예: **\d**는 **0**과 일치합니다.
\w	ASCII 문자 [A-Za-z0-9_]와 일치합니다. 예: **\w\w\w**는 **PAN**과 일치합니다.
\v	모든 유니코드 줄 바꿈 문자를 포함하는 세로 공백 문자를 찾습니다. 예: **\v**는 세로 공백 문자와 일치합니다.
\h	탭과 모든 "공백 구분자" 유니코드 문자를 포함하는 가로 공백을 찾습니다. 예: **\h**는 가로 공백 문자와 일치합니다.
제한된 반복 정량자 이전 항목을 반복할 횟수를 지정합니다.	
{n}	정확히 횟수(*n*)를 일치시킵니다. 예: **a{2}**은 **aa**와 일치합니다.
{n,m}	**{n,m}**은 *n*번에서 *m*번까지 일치합니다. 예: **a{2,4}**는 **aa**, **aaa** 및 **aaaa**와 일치합니다.
{n, }	**{n,}**은(는) *n*번 이상 일치합니다. 예: **a{2,}**는 **aaaaab**의 **aaaaa**와 일치합니다..
앵커 캐릭터 표현식을 일치시킬 위치를 지정하십시오.	
^	문자열의 시작 부분에서 일치합니다. 또한 여러 줄 모드(**m**)가 활성화된 경우 줄 바꿈 후에 일치합니다.

패턴 구문	설명
	예시: abc 문자열이 주어지면 **^a**는 a과 일치하지만 b는 문자열의 시작 부분에 발생하지 않기 때문에, **^b**는 아무 것도 일치하지 않습니다.
$	문자열 끝에서 또는 문자열 끝의 개행 문자 앞에서 일치시킵니다. 또한 여러 줄 모드(**m**)가 활성화된 경우 모든 줄 바꿈 전에 일치합니다. 예시: abc 문자열이 주어지면 **c$**는 c과 일치하지만 문자열 끝에 a가 발생하지 않기 때문에 **a$**는 아무 것도 일치하지 않습니다.
\A	문자열의 시작 부분에서 일치합니다. 여러 줄 모드(**m**)가 활성화된 경우에도 줄 바꿈 후에 일치하지 않습니다.
\Z	문자열 끝과 마지막 줄 바꿈 전에 일치합니다. 여러 줄 모드(**m**)가 활성화된 경우에도 다른 줄 바꿈 전에 일치하지 않습니다.
\z	문자열의 절대 끝에서 일치합니다. 줄 바꿈 전에 일치하지 않습니다.
옵션 수정자 하위 패턴의 동작을 변경합니다. 활성화하려면 **(?<option>)**을 입력하고 비활성화하려면 **(?-<option>)**을 입력합니다.	
i	대소문자 구분을 활성화합니다. 예: **((?i)\bconfidential\b)**는 Confidential과 일치합니다.
m	**^**와 **$**가 줄의 시작과 끝에서 일치하도록 합니다.
s	**.**이 줄 바꿈 문자를 포함하여 모든 것과 일치하도록 합니다.
x	정규식 토큰 사이의 공백을 무시합니다.

정규식 데이터 패턴 예제

다음은 유효한 사용자 지정 패턴의 예입니다.

- .*(기밀)| (기밀))
  - 항상 "Confidential" 또는 "CONFIDENTIAL"이라는 단어를 찾습니다.
  - ".*"는 처음에는 스트림의 어느 곳을 볼 수 있도록 지정합니다.
  - 디코더의 케이스 감도 요구 사항에 따라 "confidential"(모든 소문자)과 일치하지 않을 수 있습니다.
- .*((독점 및 기밀) | (독점 및 기밀))
  - "독점 및 기밀" 또는 "독점 및 기밀" 검색
  - "기밀"을 찾는 것보다 더 정밀합니다.
- .*(보도 자료).*(초안)| 드래프트)| (초안))
  - 보도 자료가 회사 외부로 보낼 준비가 되지 않았음을 나타낼 수 있는 다양한 형태의 초안 단어 뒤에 오는 "보도 자료"를 찾습니다.
- .*(Trinidad)
  - "트리니다드"와 같은 프로젝트 코드 이름을 찾습니다.

개체 > 사용자 정의 개체 > 스파이웨어/취약점

방화벽은 방화벽 위협 엔진을 사용하여 사용자 지정 스파이웨어 및 취약성 서명을 만드는 기능을 지원합니다. 사용자 정의 정규식 패턴을 작성하여 스파이웨어 폰 홈(phone home) 또는 취약점 악용을 식별할 수 있습니다. 생성된 스파이웨어 및 취약성 패턴은 모든 사용자 지정 취약성 프로파일에서 사용할 수 있게 됩니다. 방화벽은 네트워크 트래픽에서 사용자 정의 패턴을 찾고 취약점 악용에 대해 지정된 조치를 취합니다.

주간 콘텐츠 릴리스에는 서명을 개발할 수 있는 새로운 디코더와 컨텍스트가 주기적으로 포함됩니다.

공격에 대한 응답으로 가능한 작업을 트리거하기 위해 인터벌당 임계값을 지정하여 사용자 지정 서명을 정의할 때 시간 속성을 선택적으로 포함할 수 있습니다. 임계값에 도달한 후에만 조치가 취해집니다.

사용자 정의 스파이웨어 서명 페이지를 사용하여 안티 스파이웨어 프로파일에 대한 서명을 정의합니다. 사용자 지정 취약점 서명 페이지를 사용하여 취약점 보호 프로파일에 대한 서명을 정의합니다.

사용자 지정 취약점 및 스파이웨어 서명 설정	설명
구성 탭	
위협 ID	구성에 대한 숫자 식별자를 입력합니다(스파이웨어 서명 범위는 15000-18000 및 6900001 - 7000000이고 취약성 서명 범위는 41000-45000 및 6800001-6900000).
이름	위협 이름을 지정합니다.
공유	사용자 정의 서명을 다음에 사용할 수 있게 하려면 이 옵션을 선택하십시오. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 사용자 정의 서명을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에서만 사용자 정의 서명을 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 서명을 상속하는 디바이스 그룹에서 이 서명의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 서명을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
코멘트	선택적 코멘트를 입력합니다.

사용자 지정 취약점 및 스파이웨어 서명 설정	설명
심각성	위협의 심각성을 나타내는 수준을 지정합니다.
기본 작업	위협 조건이 충족되는 경우 수행할 기본 작업을 할당합니다. 작업 목록은 보안 프로파일의 작업을 참조하십시오.
방향	위협이 클라이언트에서 서버로, 서버에서 클라이언트로 또는 둘 다 평가되는지의 여부를 나타냅니다.
영향을 받는 시스템	위협이 클라이언트, 서버 중 하나 또는 둘 다를 포함하는지의 여부를 나타냅니다. 취약점 서명에는 적용되지만 스파이웨어 서명에는 적용되지 않습니다.
CVE	추가 배경 및 분석을 위한 외부 참조로 CVE(공통 취약점 열거)를 지정합니다.
공급자	추가 배경 및 분석을 위한 외부 참조로 취약성에 대한 공급자 식별자를 지정합니다.
버그트랙	추가 배경 및 분석을 위한 외부 참조로 bugtraq(CVE와 유사)를 지정합니다.
참조	추가 분석 또는 배경 정보에 대한 링크를 추가합니다. 사용자가 ACC, 로그 또는 취약점 프로파일에서 위협을 클릭하면 정보가 표시됩니다.
서명 탭	
표준 서명	표준을 선택한 다음 새 서명 추가를 선택합니다. 다음 정보를 지정합니다. • 표준 - 서명을 식별할 이름을 입력합니다. • 설명 - 선택적 설명을 입력합니다. • 순서가 지정된 조건 일치 - 서명 조건이 정의된 순서가 중요한 경우 선택합니다. • 범위 - 이 서명을 현재 트랜잭션에만 적용할지 아니면 전체 사용자 세션에 적용할지 선택합니다. 조건 추가 또는 조건 추가를 클릭하여 조건을 추가합니다. 그룹 내에 조건을 추가하려면 그룹을 선택한 다음 조건 추가를 클릭합니다. 조건에 대해 정의한 매개변수가 true일 때 트래픽에 대해 서명이 생성되도록 서명에 조건을 추가합니다. 드롭다운에서 연산자를 선택합니다. 연산자는 사용자 지정 서명이 트래픽과 일치하기 위해 참이어야 하는 조건 유형을 정의합니다. 더 작음, 같음, 더 큼 또는 패턴 일치 연산자 중에서 선택합니다.

사용자 지정 취약점 및 스파이웨어 서명 설정	설명

	• 패턴 일치 연산자를 선택할 때 서명이 트래픽과 일치하도록 다음을 true로 지정합니다.
	  • 컨텍스트 - 사용 가능한 컨텍스트에서 선택합니다.
	  • 패턴 - 정규식을 지정합니다. 정규식에 대한 패턴 규칙은 패턴 규칙 구문을 참조하십시오.
	  • 수식어 및 값 - 선택적으로 수식어/값 쌍을 추가합니다.
	  • 무효 - 정의된 패턴 일치 조건이 true가 아닌 경우에만 사용자 정의 서명이 트래픽과 일치하도록 무효를 선택합니다. 이를 통해 특정 조건에서 사용자 지정 서명이 트리거되지 않도록 할 수 있습니다.
	  무효 조건만으로 사용자 정의 서명을 생성할 수 없습니다. 무효 조건을 지정하려면 최소한 하나의 긍정 조건이 포함되어야 합니다. 또한 시그니처의 범위가 *Session*으로 설정되어 있으면 무효 조건을 트래픽과 일치시키는 마지막 조건으로 설정할 수 없습니다.
	  트래픽이 서명과 서명에 대한 예외 모두와 일치하는 경우 서명 생성을 무효화하는 새 옵션을 사용하여 사용자 지정 취약성 또는 스파이웨어 서명에 대한 예외를 정의할 수 있습니다. 스파이웨어 또는 취약점 악용으로 분류될 수 있는 네트워크의 특정 트래픽을 허용하려면 이 옵션을 사용합니다. 이 경우 패턴과 일치하는 트래픽에 대해 서명이 생성됩니다. 패턴과 일치하지만 패턴에 대한 예외와도 일치하는 트래픽은 서명 생성 및 관련 정책 작업(예: 차단 또는 삭제)에서 제외됩니다. 예를 들어 리디렉션된 URL에 대해 생성할 서명을 정의할 수 있습니다. 그러나 이제 신뢰할 수 있는 도메인으로 리디렉션되는 URL에 대해 서명이 생성되지 않는 예외를 생성할 수도 있습니다.

	• 같음, 더 작음 또는 더 큼 연산자를 선택할 때 서명이 트래픽과 일치하도록 다음을 true로 지정합니다.
	  • 컨텍스트 - TCP 또는 UDP에 대한 알 수 없는 요청 및 응답 중에서 선택합니다.
	  • 위치 - 페이로드의 처음 4바이트 또는 두 번째 4바이트 중에서 선택합니다.
	  • 마스크 - 4바이트 16진수 값을 지정합니다(예: 0xffffff00).
	  • 값 - 4바이트 16진수 값을 지정합니다(예: 0xaabbccdd).

조합 서명	조합을 선택한 후 다음 정보를 지정합니다.

사용자 지정 취약점 및 스파이웨어 서명 설정	설명
	조합 서명을 선택하여 서명을 정의하는 조건을 지정합니다. • **AND** 조건 추가 또는 **OR** 조건 추가를 클릭하여 조건을 추가합니다. 그룹 내에 조건을 추가하려면 그룹을 선택한 다음 조건 추가를 클릭합니다. • 그룹 내에서 조건을 이동하려면 조건을 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 그룹을 이동하려면 그룹을 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 한 그룹에서 다른 그룹으로 조건을 이동할 수 없습니다. 시간 속성을 선택하여 다음 정보를 지정합니다. • 적중 수 - 정책 기반 작업을 트리거할 임계값을 지정된 시간(1-3600초) 동안 적중 수(1-1000)로 지정합니다. • 통합 기준 - 적중이 소스 IP 주소, 대상 IP 주소 또는 소스 및 대상 IP 주소 조합으로 추적되는지의 여부를 지정합니다. • 그룹 내에서 조건을 이동하려면 조건을 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 그룹을 이동하려면 그룹을 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 한 그룹에서 다른 그룹으로 조건을 이동할 수 없습니다.

개체 > 사용자 정의 개체 > URL 카테고리

사용자 지정 URL 카테고리 페이지를 사용하여 사용자 지정 URL 목록을 만들고 URL 필터링 프로파일 또는 정책 규칙의 일치 기준으로 사용합니다. 사용자 지정 URL 카테고리에서 URL 항목을 개별적으로 추가하거나 URL 목록이 포함된 텍스트 파일을 가져올 수 있습니다.

사용자 지정 카테고리에 추가된 *URL* 항목은 둔감한 경우입니다.

다음 표는 사용자 지정 URL 설정을 설명합니다.

사용자 지정 **URL** 카테고리 설정	설명
이름	이름을 입력하여 사용자 지정 URL 카테고리(최대 31자)를 식별합니다. 이 이름은 URL 필터링 정책을 정의할 때 카테고리 목록과 정책 규칙의 URL 카테고리에 대한 일치 기준에 표시됩니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	URL 카테고리(최대 255자)에 대한 설명을 입력합니다.
유형	카테고리 유형을 선택합니다. • 카테고리 일치— 지정된 URL 카테고리와 일치하는 URL이 포함된 새 사용자 지정 카테고리를 정의하려면 카테고리 일치를 선택합니다(URL은 목록의 모든 카테고리와 일치해야 함). 2-4 카테고리 사이를 지정합니다. • **URL**목록— **URL** 목록을 선택하여 카테고리에 대한 URL 목록을 추가하거나 가져옵니다. 이 카테고리 유형에는 PAN-OS 9.0 이전에 추가된 URL도 포함되어 있습니다.
공유	URL 카테고리를 사용할 수 있도록 하려면 다음 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 옵션을 사용하지 않도록 설정(지우기)하는 경우 URL 카테고리는 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 옵션을 사용하지 않도록 설정(지우기)하는 경우 URL 카테고리는 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.

사용자 지정 **URL** 카테고리 설정	설명
재정의 비활성화(Panorama만 해당)	이 옵션을 선택하여 관리자가 개체를 상속하는 디바이스 그룹에서 이 사용자 지정 URL 개체의 설정을 재정의하지 못하도록 합니다. 이 선택은 기본적으로 비활성화되므로 관리자는 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
사이트	사용자 지정 URL 카테고리에 대한 사이트 관리(추가되거나 불러온 각 URL에 최대 255자)가 있을 수 있습니다. • 추가— URL을 행당 하나만 추가합니다. 각 URL은 "www.example.com" 형식으로 사용되거나 "*example.com"과 같은 와일드카드를 포함할 수 있습니다. 지원되는 형식에 대한 자세한 내용은 개체 > 보안 프로파일 > URL 필터링에서 블록 목록을 참조하십시오. • 가져오기— 가져오기 및 URL 목록이 포함된 텍스트 파일을 찾아 선택합니다. 행당 하나의 URL만 입력합니다. 각 URL은 "www.example.com" 형식으로 사용되거나 "*example.com"과 같은 와일드카드를 포함할 수 있습니다. 지원되는 형식에 대한 자세한 내용은 개체 > 보안 프로파일 > URL 필터링에서 블록 목록을 참조하십시오. • 내보내기— 목록에 포함된 사용자 지정 URL 항목을 내보내기(텍스트 파일로 내보내기). • 삭제— 목록에서 URL을 제거하기 위해 항목을 삭제합니다. *URL* 필터링 프로파일에서 사용한 사용자 지정 카테고리를 삭제하려면 사용자 지정 카테고리를 삭제하기 전에 작업을 ***None***으로 설정해야 합니다. 개체 > 보안 프로파일 > URL 필터링에서 카테고리 작업을 참조하십시오.

개체 > 보안 프로파일

보안 프로파일은 보안 정책에서 위협 보호를 제공합니다. 각 보안 정책 규칙에는 하나 이상의 보안 프로파일이 포함될 수 있습니다. 다음은 사용 가능한 프로파일 유형입니다.

- 웜, 바이러스 및 트로이 목마로부터 보호하고 스파이웨어 다운로드를 차단하기 위한 바이러스 백신 프로파일. 개체 > 보안 프로파일 > 바이러스 백신을 참조하십시오.
- 안티 스파이웨어 프로파일은 외부 명령 및 제어(C2) 서버에 대한 폰-홈(phone-home) 또는 비콘 아웃을 시도하는 손상된 호스트의 스파이웨어 시도를 차단합니다. 개체 > 보안 프로파일 > 안티스파이웨어 프로파일을 참조하십시오.
- 시스템 결함을 악용하거나 시스템에 대한 무단 액세스를 얻으려는 시도를 중지하기 위한 취약성 보호 프로파일. 개체 > 보안 프로파일 > 취약성 보호를 참조하십시오.
- URL 필터링 프로파일은 쇼핑이나 도박과 같은 특정 웹사이트 및/또는 웹사이트 카테고리에 대한 사용자 액세스를 제한합니다. 개체 > 보안 프로파일 > URL 필터링을 참조하십시오.
- 선택한 파일 형식과 지정된 세션 플로우 방향(인바운드/아웃바운드/둘 다)을 차단하는 파일 차단 프로파일. 개체 > 보안 프로파일 > 파일 차단을 참조하십시오.
- WildFire™ 분석 프로파일은 파일 분석이 WildFire 어플라이언스 또는 WildFire 클라우드에서 로컬로 수행되도록 지정합니다. 개체 > 보안 프로파일 > WildFire 분석을 참조하십시오.
- 신용 카드 또는 주민등록번호와 같은 민감한 정보가 보호된 네트워크를 벗어나는 것을 방지하는 데이터 필터링 프로파일. 개체 > 보안 프로파일 > 데이터 필터링을 참조하십시오.
- DoS 방어 프로파일은 대량 단일 세션 및 다중 세션 공격으로부터 방화벽을 보호하기 위해 DoS 방어 정책 규칙과 함께 사용됩니다. 개체 > 보안 프로파일 > DoS 방어를 참조하십시오.
- 모바일 네트워크 보호 프로파일을 사용하면 방화벽이 GTP 트래픽을 검사, 검증 및 필터링할 수 있습니다.

개별 프로파일 외에도 종종 함께 적용되는 프로파일을 결합하고 보안 프로파일 그룹(개체 > 보안 프로파일 그룹)을 만들 수 있습니다.

보안 프로파일의 작업

작업은 방화벽이 위협 이벤트에 대응하는 방법을 지정합니다. Palo Alto Networks에서 정의한 모든 위협 또는 바이러스 서명에는 일반적으로 알림에 대해 활성화한 옵션을 사용하여 알려주는 경고 또는 양쪽 연결을 재설정하는 모두 재설정으로 설정되는 기본 작업이 포함됩니다. 그러나 방화벽에서 작업을 정의하거나 재정의할 수 있습니다. 다음 작업은 바이러스 백신 프로파일, 안티 스파이웨어 프로파일, 취약성 보호 프로파일, 사용자 지정 스파이웨어 개체, 사용자 지정 취약성 개체 또는 DoS 방어 프로파일을 정의할 때 적용할 수 있습니다.

동작	설명	바이러스 백신 프로파일	안티스파이웨어 프로파일	취약점 보호 프로파일	사용자 지정 개체 - 스파이웨어 및 취약성	**DoS** 방어 프로파일
기본	각 위협 서명에 대해 내부적으로 지정된 기본 작업을 수행합니다. 바이러스 백신 프로파일의 경우 바이러스 서명에 대한 기본 작업을 수행합니다.	✓	✓	✓	—	임의의 조기 드롭
허용하다	애플리케이션 트래픽을 허용합니다. 허용 작업은 서명 또는 프로파일과 관련된 로그를 생성하지 않습니다.	✓	✓	✓	✓	—
알리다	각 애플리케이션 트래픽 플로우에 대한 경고를 생성합니다. 경고는 위협 로그에 저장됩니다.	✓	✓	✓	✓	✓ 공격 볼륨(cps)이 프로파일에 설정된 경보 임계값에 도달하면 경고를 생성합니다.

동작	설명	바이러스 백신 프로파일	안티스파이웨어 프로파일	취약점 보호 프로파일	사용자 지정 개체 - 스파이웨어 및 취약성	**DoS** 방어 프로파일
드롭	애플리케이션 트래픽을 삭제합니다.	✓	✓	✓	✓	—
클라이언트 재설정	TCP의 경우 클라이언트 측 연결을 재설정합니다. UDP의 경우 연결이 끊어집니다.	✓	✓	✓	✓	—
서버 재설정	TCP의 경우 서버 측 연결을 재설정합니다. UDP의 경우 연결이 끊어집니다.	✓	✓	✓	✓	—
둘 다 재설정	TCP의 경우 클라이언트와 서버 쪽 모두에서 연결을 재설정합니다. UDP의 경우 연결이 끊어집니다.	✓	✓	✓	✓	—
IP 차단	소스 또는 소스-대상 쌍의 트래픽을 차단합니다. 지정된 시간 동안 구성할 수 있습니다.	—	✓	✓	✓	✓
싱크홀	이 작업은 악의적인 도메인에 대한 DNS 쿼리를 싱크홀 IP 주소로 보냅니다. 이 작업은 Palo Alto Networks DNS 서명 및 개체 > 외부 동적 목록에 포함된 사용자	—	—	—	—	—

동작	설명	바이러스 백신 프로파일	안티스파이웨어 프로파일	취약점 보호 프로파일	사용자 지정 개체 - 스파이웨어 및 취약성	**DoS** 방어 프로파일
	지정 도메인에 사용할 수 있습니다.					
임의의 조기 드롭	DoS 방어 규칙에 적용된 DoS 방어 프로파일에서 초당 연결이 활성화 비율 임계값에 도달하면 방화벽이 패킷을 무작위로 삭제합니다.	—	—	—	—	✓
SYN 쿠키	DoS 방어 규칙에 적용된 DoS 방어 프로파일에서 초당 연결 수가 활성화 속도 임계값에 도달할 때 방화벽이 클라이언트에서 SYN을 인증하기 위해 SYN 쿠키를 생성하도록 합니다.	—	—	—	—	✓

정책 규칙에 사용되는 프로파일은 삭제할 수 없습니다. 먼저 정책 규칙에서 프로파일을 제거해야 합니다.

개체 > 보안 프로파일 > 바이러스 백신

안티바이러스 프로파일 페이지를 사용하여 방화벽이 정의된 트래픽에서 바이러스를 검색하도록 하는 옵션을 구성합니다. 바이러스를 검사해야 하는 애플리케이션과 바이러스가 감지되었을 때 수행할 조치를 설정합니다. 기본 프로파일은 나열된 모든 프로토콜 디코더에서 바이러스를 검사하고 SMTP(Simple Mail Transport Protocol), IMAP(Internet Message Access Protocol) 및 POP3(Post Office Protocol Version 3)에 대한 경고를 생성하고 다른 애플리케이션(경고 또는 거부)에 대한 기본 작업을 수행하며, 이는 탐지된 바이러스 유형에 따라 다릅니다. 그러면 프로파일이 보안 정책 규칙에 연결되어 검사할 특정 영역을 통과하는 트래픽을 결정합니다.

사용자 지정 프로파일을 사용하여 신뢰할 수 있는 보안 영역 간의 트래픽에 대한 바이러스 백신 검사를 최소화하고 인터넷과 같은 신뢰할 수 없는 영역에서 수신한 트래픽과 서버 팜과 같은 매우 민감한 대상으로 보내는 트래픽에 대한 검사를 최대화할 수 있습니다.

새 안티바이러스 프로파일을 추가하려면 추가를 선택한 후 다음 설정을 입력합니다.

필드	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 바이러스 백신 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈, 마침표 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유 (Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 바이러스 백신 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
작업 탭 FTP 및 HTTP와 같은 다양한 유형의 트래픽에 대한 작업을 지정합니다.	
패킷 캡처 활성화	식별된 패킷을 캡처하려면 이 옵션을 선택합니다.
디코더 및 작업	바이러스를 검사할 각 트래픽 유형에 대해 드롭다운에서 작업을 선택합니다. 표준 바이러스 백신 서명(서명 작업 열), WildFire 시스템에서 생성된 서

필드	설명
	명(**WildFire** 서명 작업 열) 및 WildFire 인라인 ML 모델에서 실시간으로 탐지한 악성 위협(**WildFire** 인라인 **ML** 작업 열)에 대해 서로 다른 작업을 정의할 수 있습니다. 일부 환경에서는 안티바이러스 서명에 더 긴 흡수 시간이 요구될 수 있으므로 이 옵션을 사용하면 Palo Alto Networks에서 제공하는 두 가지 안티바이러스 서명 유형에 대해 서로 다른 작업을 설정할 수 있습니다. 예를 들어, 표준 바이러스 백신 서명은 위협이 탐지된 후 15분 이내에 생성 및 해제될 수 있는 WildFire 서명에 비해 릴리스되기 전에 더 긴 대기 기간(24시간)을 거칩니다. 이 때문에 차단 대신 WildFire 서명에 대한 경고 작업을 선택할 수 있습니다. 최상의 보안을 위해 기본 바이러스 백신 프로파일을 복사하고 모든 디코더에 대한 작업 및 *WildFire* 작업을 재설정하고 트래픽을 허용하는 모든 보안 정책 규칙에 프로파일을 연결하도록 설정합니다.
애플리케이션 예외 및 조치	애플리케이션 예외 테이블을 사용하여 검사하지 않을 애플리케이션을 정의할 수 있습니다. 예를 들어 특정 애플리케이션을 제외한 모든 HTTP 트래픽을 차단하려면 해당 애플리케이션이 예외인 바이러스 백신 프로파일을 정의할 수 있습니다. 차단은 HTTP 디코더에 대한 작업이고 허용은 애플리케이션에 대한 예외입니다. 각 애플리케이션 예외에 대해 위협이 탐지될 때 수행할 작업을 선택합니다. 작업 목록은 보안 프로파일의 작업을 참조하십시오. 애플리케이션을 찾으려면 텍스트 상자에 애플리케이션 이름을 입력합니다. 일치하는 애플리케이션 목록이 표시되고 선택할 수 있습니다. 합법적인 애플리케이션이 바이러스를 옮기는 것으로 잘못 식별된 경우(거짓 양성) *TAC*로 지원 사례를 열어 *Palo Alto Networks*에서 잘못 식별된 바이러스를 분석하고 수정할 수 있도록 하십시오. 문제가 해결되면 프로파일에서 예외를 제거합니다.
서명 예외 탭 서명 예외 탭을 사용하여 바이러스 백신 프로파일에서 무시할 위협 목록을 정의합니다. 식별된 바이러스가 위협 요소가 아니라고 확신하는 경우에만 예외를 생성합니다(거짓 양성). 거짓 양성을 발견했다고 생각되면 *TAC*에 지원 사례를 열어 *Palo Alto Networks*가 잘못 식별된 바이러스 서명을 분석하고 수정할 수 있도록 하십시오. 문제가 해결되면 즉시 프로파일에서 예외를 제거하십시오.	

필드	설명
위협 ID	무시할 특정 위협을 추가하려면 위협 ID를 한 번에 하나씩 입력하고 추가를 클릭합니다. 위협 ID는 위협 로그 정보의 일부로 제공됩니다. 모니터 > 로그를 참조하세요.
WildFire 인라인 **ML** 탭 **WildFire** 인라인 **ML** 탭을 사용하여 방화벽 기반 기계 학습 모델을 사용하여 파일에 대한 실시간 WildFire 분석을 활성화하고 구성합니다. *Palo Alto Networks*는 *Wildfire* 인라인 *ML*이 활성화된 경우 *WildFire* 클라우드에 샘플을 포워딩할 것을 권장합니다. 이를 통해 거짓 양성을 유발하는 샘플이 *2*차 분석 시 자동으로 수정될 수 있습니다. 또한 향후 업데이트를 위해 *ML* 모델을 개선하기 위한 데이터를 제공합니다.	
사용 가능한 모델	사용 가능한 각 WildFire 인라인 ML 모델에 대해 다음 작업 설정 중 하나를 선택할 수 있습니다. • 활성화**(**프로토콜별 작업 상속**)** - 작업 탭의 디코더 섹션에 있는 **WildFire** 인라인 **ML** 작업 열에서 선택한 항목에 따라 트래픽이 검사됩니다. • 경고 전용**(**경고에 대한 보다 엄격한 작업 재정의**)** - 작업 탭의 디코더 섹션에 있는 **WildFire** 인라인 **ML** 작업 열에서 선택한 항목에 따라 트래픽이 검사됩니다. 경고보다 심각도 수준이 높은 모든 작업(drop, reset-client, reset-server, reset-both)은 경고로 재정의되어 위협 로그에 경고를 생성하고 저장하는 동안 트래픽이 통과할 수 있습니다. • 비활성화**(**모든 프로토콜에 대해**)** - 정책 작업 없이 트래픽이 전달되도록 허용됩니다.
파일 예외	파일 예외 테이블을 사용하면 거짓 양성과 같이 분석하지 않으려는 특정 파일을 정의할 수 있습니다. 새 파일 예외 항목을 생성하려면 새 항목을 추가하고 시행에서 제외할 파일의 부분 해시, 파일 이름 및 설명을 제공하십시오. 기존 파일 예외를 찾으려면 텍스트 상자에 부분 해시 값, 파일 이름 또는 설명을 입력하기 시작합니다. 해당 값과 일치하는 파일 예외 목록이 표시됩니다. 위협 로그*(*모니터 > 로그 > 위협*)*에서 부분 해시를 찾을 수 있습니다.

개체 > 보안 프로파일 > 안티스파이웨어 프로파일

안티 스파이웨어 프로파일을 보안 정책 규칙에 연결하여 네트워크의 시스템에 설치된 스파이웨어 및 다양한 유형의 명령 및 제어(C2) 멀웨어에 의해 시작된 연결을 탐지할 수 있습니다. 보안 정책 규칙에 연결할 두 개의 사전 정의된 안티 스파이웨어 프로파일 중에서 선택할 수 있습니다. 각 프로파일에는 위협의 심각도별로 구성된 사전 정의된 규칙 집합(위협 서명 포함)이 있습니다. 각 위협 서명에는 Palo Alto Networks에서 지정한 기본 작업이 포함됩니다.

- 기본값 - 기본 프로파일은 서명이 생성될 때 Palo Alto Networks 콘텐츠 패키지에서 지정한 대로 모든 서명에 대한 기본 작업을 사용합니다.
- Strict - Strict 프로파일은 심각도, 높음 및 중간 심각도 위협에 대해 서명 파일에 정의된 작업을 재정의하고 모두 재설정 작업으로 설정합니다. 기본 조치는 심각도가 낮은 정보 제공 위협에 대해 수행됩니다.
- 사용자 정의 프로파일을 만들 수도 있습니다. 예를 들어, 신뢰할 수 있는 보안 영역 간의 트래픽에 대한 안티스파이웨어 검사의 엄격성을 줄이고 인터넷에서 수신된 트래픽 또는 서버 팜과 같은 보호 자산으로 전송된 트래픽의 검사를 최대화할 수 있습니다.

다음 표에서는 안티스파이웨어 프로파일 설정에 대해 설명합니다.

안티스파이웨어 프로파일 설정	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 안티스파이웨어 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈, 마침표 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 안티 스파이웨어 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
서명 정책 탭	

안티스파이웨어 프로파일 설정	설명
안티스파이웨어 규칙을 사용하면 위협, 사용자가 입력한 텍스트가 포함된 특정 위협 이름 및/또는 애드웨어와 같은 위협 카테고리별로 사용자 지정 심각도 및 위협에 대해 수행할 작업을 정의할 수 있습니다. 새 규칙을 추가하거나 기존 규칙을 선택한 다음 일치하는 서명 찾기를 선택하여 해당 규칙을 기반으로 위협 서명을 필터링할 수 있습니다.	
규칙 이름	규칙 이름을 지정합니다.
위협 이름	모든 서명과 일치하도록 모두를 입력하거나 서명 이름의 일부로 입력된 텍스트를 포함하는 서명과 일치하도록 텍스트를 입력합니다.
카테고리	카테고리를 선택하거나 모든 카테고리와 일치하도록 모두를 선택합니다.
작업	각 위협에 대한 작업을 선택하십시오. 작업 목록은 보안 프로파일의 작업을 참조하십시오. 기본 작업은 Palo Alto Networks에서 제공하는 각 서명의 일부인 사전 정의된 작업을 기반으로 합니다. 서명에 대한 기본 작업을 보려면 개체 > 보안 프로파일 > 안티 스파이웨어를 선택한 다음 기존 프로파일을 추가하거나 선택합니다. 예외 탭을 클릭한 다음 모든 서명 표시를 클릭하여 모든 서명 및 관련 작업 목록을 확인합니다. 최상의 보안을 위해 사전 정의된 엄격한 프로파일에서 작업 설정을 사용합니다.
패킷 캡처	식별된 패킷을 캡처하려면 이 옵션을 선택합니다. 단일 패킷을 선택하여 위협이 탐지될 때 하나의 패킷을 캡처하거나 확장 캡처 옵션을 선택하여 1~50개 패킷(기본값은 5개 패킷)을 캡처합니다. 확장 캡처는 위협 로그를 분석할 때 위협에 대한 추가 컨텍스트를 제공합니다. 패킷 캡처를 보려면 **Monitor** > **Logs** > **Threat**를 선택한 다음 관심 있는 로그 항목을 찾은 다음 두 번째 열에서 녹색 아래쪽 화살표를 클릭합니다. 캡처할 패킷 수를 정의하려면 **Device** > **Setup** > **Content-ID**를 선택한 다음 Content-ID™ 설정을 편집합니다. 주어진 위협에 대한 작업이 허용인 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.

안티스파이웨어 프로파일 설정	설명
	중요, 높음 및 중간 심각도 이벤트에 대해 확장 캡처를 활성화합니다. 대부분의 경우 위협을 분석하기에 충분한 정보를 제공하는 기본 확장 캡처 값인 *5*개 패킷을 사용합니다. *(*패킷 캡처 트래픽이 너무 많으면 패킷 캡처가 삭제될 수 있습니다.*)* 정보 제공 및 심각도가 낮은 이벤트에 대해 확장 캡처를 활성화하지 마십시오. 심각도가 높은 이벤트에 대한 정보를 캡처하는 것과 비교하여 그다지 유용하지 않고 상대적으로 많은 양의 낮은 가치의 트래픽을 생성하기 때문입니다.
심각성	심각도 수준**(**위험, 높음, 중간, 낮음 또는 정보 제공)을 선택합니다.

서명 예외 탭

특정 서명에 대한 작업을 변경할 수 있습니다. 예를 들어 특정 서명 집합에 대한 경고를 생성하고 다른 모든 서명과 일치하는 모든 패킷을 차단할 수 있습니다. 위협 예외는 일반적으로 거짓 양성이 발생할 때 구성됩니다. 위협 예외를 더 쉽게 관리하기 위해 **Monitor** > **Logs** > 위협 목록에서 직접 위협 예외를 추가할 수 있습니다. 새로운 위협으로부터 보호하고 거짓 양성에 대한 새 서명을 가질 수 있도록 최신 콘텐츠로 업데이트해야 합니다.

예외	작업을 할당할 각 위협을 활성화하거나 모두를 선택하여 나열된 모든 위협에 대응합니다. 목록은 선택한 호스트, 카테고리 및 심각도에 따라 다릅니다. 목록이 비어 있으면 현재 선택 항목에 대한 위협이 없습니다. IP 주소 예외를 사용하여 위협 예외에 IP 주소 필터를 추가합니다. IP 주소가 위협 예외에 추가되면 해당 서명에 대한 위협 예외 작업은 예외의 IP 주소와 일치하는 소스 또는 대상 IP 주소가 있는 세션에 의해 서명이 트리거되는 경우에만 규칙에 대한 작업을 재정의합니다. 서명당 최대 100개의 IP 주소를 추가할 수 있습니다. 이 옵션을 사용하면 특정 IP 주소에 대한 예외를 만들기 위해 새 정책 규칙과 새 취약성 프로파일을 만들 필요가 없습니다. 스파이웨어로 식별된 서명이 위협이 아니라고 확신하는 경우에만 예외를 생성합니다*(*거짓 양성*)*. 거짓 양성을 발견했다고 생각되면 *TAC*로 지원 사례를 열어 *Palo Alto Networks*가 잘못 식별된 서명을 분석하고 수정할 수 있도록 하십시오. 문제가 해결되는 즉시 프로파일에서 예외를 제거하십시오.

DNS 정책 탭

안티스파이웨어 프로파일 설정	설명
DNS 정책 설정은 네트워크에서 감염된 호스트를 식별하는 추가 방법을 제공합니다. 이러한 서명은 DNS 기반 위협과 연결된 호스트 이름에 대한 특정 DNS 조회를 탐지합니다.	
별도의 정책 작업, 로그 심각도 수준 및 패킷 캡처 설정을 사용하여 특정 DNS 서명 소스를 구성할 수 있습니다. 멀웨어 도메인에 대한 DNS 쿼리를 수행하는 호스트가 봇넷 보고서에 나타납니다. 또한 멀웨어 DNS 쿼리를 싱크홀링하는 경우 **DNS** 싱크홀 설정에서 싱크홀 IP를 지정할 수 있습니다.	
DNS 서명 소스	DNS 쿼리가 발생할 때 작업을 적용할 목록을 선택할 수 있습니다. 두 가지 기본 DNS 서명 정책 옵션이 있습니다. • **Palo Alto Networks** 콘텐츠 - 동적 콘텐츠 업데이트를 통해 업데이트되는 다운로드 가능한 로컬 서명 목록입니다. • **DNS** 보안 - DNS 데이터에 대한 사전 예방적 분석을 수행하고 전체 Palo Alto Networks DNS 서명 데이터베이스에 대한 실시간 액세스를 제공하는 클라우드 기반 DNS 보안 서비스입니다. 이 서비스를 사용하려면 *Threat Prevention* 라이선스와 함께 *DNS Security* 라이선스를 구매하고 활성화해야 합니다. • 외부 동적 목록 - 도메인 목록으로 작동하는 EDL을 사용하여 예를 들어 경고 목록과 같은 도메인 선택에 대한 특정 작업을 시행할 수 있습니다. 기본적으로 도메인 목록에 대한 정책 작업은 허용으로 구성됩니다. *EDL* 허용 목록은 *DNS* 보안에 지정된 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. 기본적으로 로컬에서 액세스되는 Palo Alto Networks 콘텐츠 DNS 서명은 싱크홀이 되어 있는 반면 클라우드 기반 DNS 보안은 허용으로 설정됩니다. DNS 보안을 사용하여 싱크홀링을 활성화하려면 DNS 쿼리에 대한 작업을 싱크홀로 구성해야 합니다. 싱크홀링에 사용되는 기본 주소는 Palo Alto Networks(sinkhole.paloaltonetworks.com)에 속합니다. 이 주소는 고정되어 있지 않으며 방화벽이나 Panorama의 콘텐츠 업데이트를 통해 수정할 수 있습니다.

안티스파이웨어 프로파일 설정	설명
	새 목록을 추가하고 생성한 도메인 유형의 외부 동적 목록을 선택합니다. 새 목록을 만들려면 개체 > 외부 동적 목록을 참조하십시오.
로그 심각도	방화벽이 DNS 서명과 일치하는 도메인을 감지할 때 기록되는 로그 심각도 수준을 지정할 수 있습니다.
정책 조치	알려진 멀웨어 사이트에 대한 DNS 조회가 수행될 때 수행할 작업을 선택합니다. 옵션은 경고, 허용, 차단 또는 싱크홀입니다. Palo Alto Networks DNS 서명의 기본 작업은 싱크홀입니다. DNS 싱크홀 작업은 방화벽이 로컬 DNS 서버의 북쪽에 있는 경우에도(예: 방화벽이 DNS 쿼리의 발신자를 볼 수 없음) DNS 트래픽을 사용하여 네트워크에서 감염된 호스트를 식별하는 방법을 관리자에게 제공합니다. 위협 방지 라이선스가 설치되고 보안 프로파일에서 안티 스파이웨어 프로파일이 활성화되면 DNS 기반 서명은 멀웨어 도메인으로 향하는 DNS 쿼리에서 트리거됩니다. 방화벽이 로컬 DNS 서버의 북쪽에 있는 일반적인 배포에서 위협 로그는 로컬 DNS 확인자를 실제 감염된 호스트가 아닌 트래픽 소스로 식별합니다. 멀웨어 DNS 쿼리를 싱크홀링하면 악의적인 도메인을 대상으로 하는 쿼리에 대한 응답을 위조하여 이러한 가시성 문제를 해결하므로 클라이언트가 악의적인 도메인(예: 명령 및 제어용)에 연결을 시도하는 대신 관리자가 지정한 IP 주소로 연결을 시도합니다. 그러면 싱크홀 IP에 연결을 시도하는 모든 호스트가 멀웨어에 감염될 가능성이 높기 때문에 감염된 호스트를 트래픽 로그에서 쉽게 식별할 수 있습니다. 방화벽이 *DNS* 쿼리의 발신자를 볼 수 없는 경우(일반적으로 방화벽이 로컬 *DNS* 서버의 북쪽에 있는 경우) *DNS* 싱크홀을 활성화하여 감염된 호스트를 식별할 수 있습니다. 트래픽을 싱크홀할 수 없으면 차단하십시오.
패킷 캡처	식별된 패킷을 캡처하려면 지정된 소스에 대해 이 옵션을 선택하십시오. 싱크홀 트래픽에 대한 패킷 캡처를 활성화하여 이를 분석하고 감염된 호스트에 대한 정보를 얻을 수 있습니다.
DNS 싱크홀 설정	DNS 서명 소스에 대해 싱크홀 작업을 정의한 후 싱크홀에 사용할 IPv4 및/또는 IPv6 주소를 지정합니다. 기본적으로 싱크홀 IP 주소는 Palo Alto Networks 서버로 설정됩니다. 그런 다음 트래픽 로그를 사용하거나 싱크홀 IP 주소를 필터링하고 감염된 클라이언트를 식별하는 맞춤 리포트를 작성할 수 있습니다. 다음은 DNS 요청이 싱크홀될 때 발생하는 일련의 이벤트입니다.

안티스파이웨어 프로파일 설정	설명
	감염된 클라이언트 컴퓨터의 악성 소프트웨어는 DNS 쿼리를 전송하여 인터넷의 악성 호스트를 해결합니다. 클라이언트의 DNS 쿼리는 내부 DNS 서버로 보내진 다음 방화벽 반대편에 있는 공용 DNS 서버를 쿼리합니다. DNS 쿼리는 지정된 DNS 서명 데이터베이스 소스의 DNS 항목과 일치하므로 쿼리에 대해 싱크홀 작업이 수행됩니다. 그런 다음 감염된 클라이언트는 호스트와 세션을 시작하려고 시도하지만 대신 위조된 IP 주소를 사용합니다. 위조된 IP 주소는 싱크홀 조치 선택 시 안티스파이웨어 프로파일 DNS 서명 탭에 정의된 주소입니다. 관리자는 위협 로그에서 악성 DNS 쿼리에 대해 경고를 받고 트래픽 로그에서 싱크홀 IP 주소를 검색할 수 있으며 싱크홀 IP 주소로 세션을 시작하려는 클라이언트 IP 주소를 쉽게 찾을 수 있습니다.
블록 DNS 레코드 유형	차단하려는 암호화된 DNS 쿼리에서 사용하는 DNS 리소스 레코드 유형을 선택합니다. 이렇게 하면 클라이언트가 DNS 확인 프로세스 중에 클라이언트 hello를 암호화하지 못하므로 키 정보의 교환이 차단됩니다. 옵션으로는 **SVCB**(유형 64), **HTTPS**(유형 65) 및 **ANY**(유형 255) 등이 있습니다. 방화벽 보안 서비스의 최적 기능을 유지하기 위해 *Palo Alto Networks*는 모든 *ECH* 지원 레코드 유형을 차단할 것을 권장합니다.
DNS 예외 탭 DNS 서명 예외를 사용하면 정책 시행에서 특정 위협 ID를 제외하고 승인된 도메인 소스에 대한 도메인/FQDN 허용 목록을 지정할 수 있습니다. 정책에서 제외할 특정 위협을 추가하려면 위협 **ID**를 선택하거나 검색하고 활성화를 클릭합니다. 각 항목은 위협 **Threat ID**, 이름 및 개체의 **FQDN**을 제공합니다. 도메인 또는 FQDN 허용 목록을 추가하려면 허용 목록의 위치와 적절한 설명을 제공합니다.	
인라인 클라우드 분석 탭 인라인 클라우드 분석을 사용하면 탐지 엔진별로 지능형 C2 위협의 실시간 분석을 위한 설정을 활성화하고 구성할 수 있습니다.	
클라우드 인라인 분석 사용 - 사용 가능한 모든 심층 인라인 클라우드 분석 엔진에서 고급 C2 위협을 실시간으로 분석할 수 있습니다.	

안티스파이웨어 프로파일 설정	설명
사용 가능한 분석 엔진	위협 범주를 나타내는 사용 가능한 각 분석 엔진에 대해 해당 위협이 탐지될 때 방화벽에서 시행할 다음 작업 중 하나를 선택할 수 있습니다. • 허용 - 웹사이트가 허용되며 로그 항목이 생성되지 않습니다. • 경고 - 웹사이트가 허용되고 URL 필터링 로그에 로그 항목이 생성됩니다. • 삭제 - 트래픽을 삭제합니다. TCP 재설정은 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. 모든 분석 엔진에 대한 기본 작업은 경고입니다.
인라인 클라우드 분석에서 제외	인라인 클라우드 분석 엔진을 우회하는 URL 또는 IP 주소 예외 목록을 선택할 수 있습니다. URL 및/또는 IP 주소를 사용하여 예외를 지정할 수 있습니다. URL 예외에는 EDL(외부 동적 목록) 또는 사용자 지정 URL 범주가 포함되고 IP 주소 예외에는 EDL 또는 주소 개체가 포함됩니다. 추가를 클릭하여 사용 가능한 옵션을 보고 선택합니다. 다음 목록 유형을 선택할 수 있습니다. • **EDL URL** - 일련의 URL 또는 사용자 정의 URL 범주가 포함된 외부 동적 목록입니다. • **IP** 주소 - 외부 동적 목록 또는 주소 개체 내에 정의된 IP 주소 목록입니다. 오탐의 경우와 같이 식별된 위협이 위험을 초래하지 않는 경우에만 *IP* 주소 및 *URL* 예외를 생성하십시오.

개체 > 보안 프로파일 > 취약점 보호

보안 정책 규칙에는 버퍼 오버플로, 불법 코드 실행 및 기타 시스템 취약성을 악용하려는 시도에 대한 보호 수준을 결정하는 취약성 보호 프로파일의 사양이 포함될 수 있습니다. Vulnerability Protection 기능에 사용할 수 있는 두 가지 사전 정의된 프로파일이 있습니다.

- 기본 프로파일은 모든 클라이언트 및 서버 심각도, 높음 및 중간 심각도 취약점에 기본 작업을 적용합니다. 낮은 정보 취약성 보호 이벤트는 감지하지 않습니다. 디바이스의 Palo Alto Networks 콘텐츠 패키지에 따라 기본 작업이 결정됩니다.
- 엄격한 프로파일은 모든 클라이언트 및 서버 중요, 높음 및 중간 심각도 스파이웨어 이벤트에 차단 응답을 적용하고 낮음 및 정보용 취약점 보호 이벤트에 대해 기본 작업을 사용합니다.

사용자 지정 프로파일을 사용하면 신뢰할 수 있는 보안 영역 간의 트래픽에 대한 취약성 검사를 최소화하고 인터넷과 같은 신뢰할 수 없는 영역에서 수신되는 트래픽과 서버 팜과 같은 매우 민감한 대상으로 전송되는 트래픽에 대한 보호를 최대화할 수 있습니다. 취약점 보호 프로파일을 보안 정책에 적용하려면 정책 > 보안을 참조합니다.

버퍼 오버플로, 불법 코드 실행, 클라이언트 및 서버 측 취약성을 악용하려는 기타 시도로부터 트래픽을 보호할 수 있는 모든 보안 정책 규칙에 취약성 보호 프로파일을 적용합니다.

규칙 설정은 활성화할 서명 모음과 모음 내 서명이 트리거될 때 수행할 작업을 지정합니다.

예외 설정을 사용하면 특정 서명에 대한 응답을 변경할 수 있습니다. 예를 들어 경고를 생성하는 선택된 패킷을 제외하고 서명과 일치하는 모든 패킷을 차단할 수 있습니다. 예외 탭은 필터링 기능을 지원합니다.

Vulnerability Protection(취약성 보호**)** 페이지에는 기본 열 집합이 표시됩니다. 열 선택기를 사용하여 추가 정보 열을 사용할 수 있습니다. 열 머리글 오른쪽에 있는 화살표를 클릭하고 열 하위 메뉴에서 열을 선택합니다.

다음 표에서는 Vulnerability Protection 프로파일 설정에 대해 설명합니다.

취약점 보호 프로파일 설정	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 Vulnerability Protection 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈, 마침표 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다.

취약점 보호 프로파일 설정	설명
	• Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 취약점 보호 프로파일의 설정을 무시하지 못하도록 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
규칙 탭	
규칙 이름	규칙을 식별할 이름을 지정합니다.
위협 이름	일치시킬 텍스트 문자열을 지정하십시오. 방화벽은 이 텍스트 문자열에 대한 서명 이름을 검색하여 규칙에 서명 컬렉션을 적용합니다.
CVE	서명을 지정된 CVE와도 일치하는 것으로 제한하려면 공통 취약점 및 노출(CVE)을 지정합니다. 각 CVE는 CVE-yyyy-xxxx 형식입니다. 여기서 yyyy는 연도이고 xxxx는 고유 식별자입니다. 이 필드에서 문자열 일치를 수행할 수 있습니다. 예를 들어, 2011년의 취약점을 찾으려면 "2011"을 입력하십시오.
호스트 유형	규칙에 대한 서명을 클라이언트 측, 서버 측 또는 둘 중 하나(임의)로 제한할지의 여부를 지정합니다.
심각성	지정된 심각도와도 일치하는 서명으로 서명을 제한하려면 일치하는 심각도(정보, 낮음, 중간, 높음 또는 위험)를 선택합니다.
작업	규칙이 트리거될 때 수행할 작업을 선택합니다. 작업 목록은 보안 프로파일의 작업을 참조하십시오. 기본 작업은 Palo Alto Networks에서 제공하는 각 서명의 일부인 사전 정의된 작업을 기반으로 합니다. 서명에 대한 기본 작업을 보려면 개체 > 보안 프로파일 > 취약성 보호를 선택한 다음 기존 프로파일을 추가하거나 선택합니다. 예외 탭을 클릭한 다음 모든 서명 표시를 클릭하여 모든 서명 및 관련 작업 목록을 확인합니다. 최상의 보안을 위해 클라이언트 및 서버 위험, 높음 및 중간 심각도 이벤트 모두에 대한 작업을 모두 재설정으로 설정하고 정보 및 낮음 심각도 이벤트에 대한 기본 작업을 사용합니다.

취약점 보호 프로파일 설정	설명
패킷 캡처	식별된 패킷을 캡처하려면 이 옵션을 선택합니다. 단일 패킷을 선택하여 위협이 탐지될 때 하나의 패킷을 캡처하거나 확장 캡처 옵션을 선택하여 1~50개 패킷(기본값은 5개 패킷)을 캡처합니다. 확장 캡처는 위협 로그를 분석할 때 위협에 대한 더 많은 컨텍스트를 제공합니다. 패킷 캡처를 보려면 **Monitor** > **Logs** > **Threat**를 선택한 다음 관심 있는 로그 항목을 찾은 다음 두 번째 열에서 녹색 아래쪽 화살표를 클릭합니다. 캡처해야 하는 패킷 수를 정의하려면 **Device** > **Setup** > **Content-ID**를 선택한 다음 Content-ID 설정을 편집합니다. 주어진 위협에 대한 작업이 허용인 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. 중요, 높음 및 중간 심각도 이벤트에 대해 확장 캡처를 활성화하고 심각도가 낮은 이벤트에 대해 단일 패킷 캡처를 활성화합니다. 대부분의 경우 위협을 분석하기에 충분한 정보를 제공하는 기본 확장 캡처 값인 5개 패킷을 사용합니다. (패킷 캡처 트래픽이 너무 많으면 패킷 캡처가 삭제될 수 있습니다.) 정보 이벤트에 대한 패킷 캡처를 활성화하지 마십시오. 심각도가 높은 이벤트에 대한 정보를 캡처하는 것과 비교하여 그다지 유용하지 않고 상대적으로 많은 양의 낮은 가치의 트래픽을 생성하기 때문입니다. 기록할 트래픽을 결정하는 데 사용하는 것과 동일한 논리를 사용하여 확장 패킷 캡처를 적용합니다. 차단하는 트래픽을 포함하여 기록하는 트래픽의 확장 캡처를 수행합니다.
예외 탭	
사용	작업을 할당하려는 각 위협에 대해 활성화를 선택하거나 나열된 모든 위협에 대응하려면 모두를 선택합니다. 목록은 선택한 호스트, 카테고리 및 심각도에 따라 다릅니다. 목록이 비어 있으면 현재 선택 항목에 대한 위협이 없습니다.
ID	
공급자 ID	지정된 공급자 ID와도 일치하는 서명으로 서명을 제한하려면 공급자 ID를 지정합니다.

취약점 보호 프로파일 설정	설명
	예를 들어 Microsoft 공급자 ID는 MSyy-xxx 형식입니다. 여기서 yy는 2자리 연도이고 xxx는 고유 식별자입니다. 예를 들어, 2009년에 대해 Microsoft와 일치시키려면 검색 필드에 "MS09"를 입력하십시오.
위협 이름	식별된 위협이 위협이 아니라고 확신하는 경우에만 위협 예외를 생성합니다*(*거짓 양성*)*. 거짓 양성을 발견했다고 판단되면 *TAC*에 지원 사례를 열어 *Palo Alto Networks*가 잘못 식별된 위협을 검토할 수 있도록 하십시오. 문제가 해결되면 즉시 프로파일에서 예외를 제거하십시오. 취약점 서명 데이터베이스에는 무차별 대입 공격을 나타내는 서명이 포함되어 있습니다. 예를 들어 위협 ID 40001은 FTP 무차별 대입 공격에서 트리거됩니다. 무차별 대입 서명은 특정 시간 임계값에 조건이 발생할 때 트리거됩니다. 임계값은 무차별 대입 서명에 대해 미리 구성되어 있으며 취약성 탭(사용자 지정 옵션이 선택된 상태)에서 위협 이름 옆에 있는 편집( )을 클릭하여 변경할 수 있습니다. 시간 단위당 적중 수와 임계값이 소스, 대상 또는 소스 및 대상에 적용되는지의 여부를 지정할 수 있습니다. 임계값은 소스 IP, 대상 IP 또는 소스 IP와 대상 IP의 조합에 적용될 수 있습니다. 기본 동작은 괄호 안에 표시됩니다.
IP 주소 면제	**IP** 주소 예외 열을 클릭하여 위협 예외에 IP 주소 필터를 추가합니다. 위협 예외에 IP 주소를 추가하면 해당 서명에 대한 위협 예외 작업은 예외의 IP 주소와 일치하는 소스 또는 대상 IP 주소가 있는 세션에 의해 서명이 트리거되는 경우에만 규칙의 작업보다 우선합니다. 서명당 최대 100개의 IP 주소를 추가할 수 있습니다. 10.1.7.8 또는 2001:db8:123:1::1과 같은 유니캐스트 IP 주소(즉, 넷마스크가 없는 주소)를 입력해야 합니다. IP 주소 예외를 추가하면 특정 IP 주소에 대한 예외를 만들기 위해 새 정책 규칙과 새 취약성 프로파일을 만들 필요가 없습니다.
규칙	
CVE	**CVE** 열에는 CVE(공통 취약점 및 노출)에 대한 식별자가 표시됩니다. 이러한 고유하고 공통적인 식별자는 공개적으로 알려진 정보 보안 취약성에 대한 것입니다.
호스트	

취약점 보호 프로파일 설정	설명
카테고리	해당 카테고리와 일치하는 서명으로 제한하려면 취약성 카테고리를 선택하십시오.
심각성	
작업	드롭다운에서 작업을 선택하거나 목록 상단의 작업 드롭다운에서 선택하여 모든 위협에 동일한 작업을 적용합니다.
패킷 캡처	식별된 패킷을 캡처하려면 패킷 캡처를 선택합니다.
모든 서명 표시	모든 서명을 나열하려면 모든 서명 표시를 활성화합니다. 모든 서명 표시가 비활성화된 경우 예외인 서명만 나열됩니다.
인라인 클라우드 분석 탭 인라인 클라우드 분석을 사용하면 검색 엔진별로 명령 삽입 및 SQL 삽입 취약점의 실시간 분석을 위한 설정을 사용 설정하고 구성할 수 있습니다.	
클라우드 인라인 분석 활성화 - 사용 가능한 모든 인라인 클라우드 분석 엔진에서 명령 삽입 및 SQL 삽입 취약성을 탐지하는 데 사용되는 인라인 딥 러닝 탐지 엔진을 활성화합니다.	
사용 가능한 분석 엔진	취약성 범주를 나타내는 사용 가능한 각 분석 엔진에 대해 해당 취약성이 감지될 때 방화벽이 시행할 다음 작업 중 하나를 선택할 수 있습니다. • **Allow** - 요청이 허용되고 로그 항목이 생성되지 않습니다. • **Alert** - 요청이 허용되고 위협 로그 항목이 생성됩니다. • **Reset-Client** - TCP의 경우 클라이언트 측 연결을 재설정합니다. • **Reset-Server** - 클라이언트 측 연결을 재설정합니다. • **Reset-Both**—클라이언트와 서버 측 모두에서 연결을 재설정합니다. 모든 분석 엔진에 대한 기본 작업은 경고입니다.
인라인 클라우드 분석에서 제외	인라인 클라우드 분석 엔진을 우회하는 URL 또는 IP 주소 예외 목록을 선택할 수 있습니다. URL 및/또는 IP 주소를 사용하여 예외를 지정할 수 있습니다. URL 예외에는 EDL(외부 동적 목록) 또는 사용자 지정 URL 범주가 포함되고 IP 주소 예외에는 EDL 또는 주소 개체가 포함됩니다. 추가를 클릭하여 사용 가능한 옵션을 보고 선택합니다. 다음 목록 유형을 선택할 수 있습니다. • **EDL URL** - 일련의 URL 또는 사용자 정의 URL 범주가 포함된 외부 동적 목록입니다.

취약점 보호 프로파일 설정	설명
	• **IP** 주소 - 외부 동적 목록 또는 주소 개체 내에 정의된 IP 주소 목록입니다. 오탐의 경우와 같이 식별된 위협이 위험을 초래하지 않는 경우에만 *IP* 주소 및 *URL* 예외를 생성하십시오.

개체 > 보안 프로파일 > URL 필터링

URL 필터링 프로파일을 사용하여 웹 콘텐츠에 대한 액세스를 제어할 뿐만 아니라 사용자가 웹 콘텐츠와 상호 작용하는 방식을 제어할 수 있습니다.

무엇을 찾고 계십니까?	참조:
URL 카테고리를 기반으로 웹사이트에 대한 액세스를 제어합니다.	URL 필터링 카테고리
회사 자격 증명 제출을 감지한 다음 사용자가 자격 증명을 제출할 수 있는 URL 카테고리를 결정합니다.	사용자 자격 증명 감지 URL 필터링 카테고리
최종 사용자가 가장 엄격한 안전 검색 설정을 사용하지 않는 경우 검색 결과를 차단합니다.	URL 필터링 설정
HTTP 헤더 로깅을 활성화합니다.	URL 필터링 설정
사용자 정의 HTTP 헤더를 사용하여 웹사이트에 대한 액세스를 제어합니다.	HTTP 헤더 삽입
클라우드 및 로컬 인라인 범주화를 활성화하여 웹 페이지에서 실시간으로 악성 콘텐츠를 분석합니다.	인라인 범주화
더 찾고 계십니까?	• URL 필터링을 구성하는 방법에 대해 자세히 알아보세요. • 자격 증명 피싱을 방지하려면 URL 카테고리를 사용하십시오. • 사용자 지정 URL 카테고리를 만들려면 개체 > 사용자 지정 개체 > URL 카테고리를 선택합니다. • 적용할 URL 목록을 가져오려면 개체 > 외부 동적 목록을(를) 선택하십시오.

URL 필터링 일반 설정

다음 표에서는 일반 URL 필터링 설정에 대해 설명합니다.

일반 설정	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 URL 필터링 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 URL 필터링 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.

URL 필터링 카테고리

개체 > 보안 프로파일 > **URL** 필터링 > 카테고리를 선택하여 URL 카테고리를 기반으로 웹사이트에 대한 액세스를 제어합니다.

카테고리 설정	설명
카테고리	웹 액세스 및 사용 정책을 정의할 수 있는 URL 카테고리 및 목록을 표시합니다. 기본적으로 모든 카테고리에 대한 사이트 액세스 및 사용자 자격 증명 제출 권한은 허용으로 설정됩니다. URL 카테고리 및 목록은 세 가지 드롭다운으로 그룹화됩니다. • 사용자 정의 **URL** 카테고리 - 사용자 정의 URL 카테고리를 정의하려면 개체 > 사용자 정의 개체 > URL 카테고리을(를) 선택합니다. URL 목록이나 사전 정의된 여러 카테고리를 기반으로 사용자 정의 URL 카테고리를 만들 수 있습니다. • 외부 동적 **URL** 목록 - 방화벽이 웹 서버에서 URL 목록을 가져올 수 있도록 하려면 개체 > 외부 동적 목록을(를) 선택합니다.

카테고리 설정	설명
	• 사전 정의된 카테고리 - PAN-DB, Palo Alto Networks URL 및 IP 클라우드 데이터베이스에 의해 정의된 모든 URL 카테고리를 나열합니다. 악용 침입, 악성 코드 다운로드, 명령 및 제어 활동 및 데이터 유출로부터 보호하기 위해 알려진 모든 위험한 ***URL*** 카테고리 차단*:* 명령 및 제어, 저작권 침해, 동적 ***DNS***, 극단주의, 악성 코드, 피싱, 프록시 방지 및 익명화, 알 수 없음, 새로 등록된 도메인, 그레이웨어 및 파킹. 차단 정책을 단계적으로 실행하려면 카테고리를 설정하여 계속하고 사용자 지정 응답 페이지를 만들어 사용자에게 사용 정책에 대해 교육하고 잠재적으로 위협이 될 수 있는 사이트를 방문하고 있음을 알립니다. 적절한 시간이 지나면 이러한 잠재적인 악성 사이트를 차단하는 정책으로 전환합니다.
사이트 액세스	각 URL 카테고리에 대해 사용자가 해당 카테고리의 URL에 액세스하려고 할 때 수행할 작업을 선택합니다. • 경고 - 웹사이트에 대한 액세스를 허용하지만 사용자가 URL에 액세스할 때마다 URL 로그에 경고를 추가합니다. 액세스 시도를 기록하고 트래픽에 대한 가시성을 제공하도록 차단하지 않는 트래픽 카테고리에 대한 작업으로 경고를 설정합니다. • 허용 - 웹사이트에 대한 액세스를 허용합니다. 허용은 차단되지 않은 트래픽을 기록하지 않으므로 액세스 시도를 기록하고 해당 트래픽에 대한 가시성을 제공하려는 경우 차단하지 않는 트래픽 카테고리에 대해 경고를 작업으로 설정합니다. • 차단 - 웹사이트에 대한 액세스를 차단합니다. URL 카테고리에 대한 사이트 액세스가 차단으로 설정된 경우 사용자 자격 증명 제출 권한도 자동으로 차단으로 설정됩니다. • 계속 - 사용자가 웹사이트에 액세스하지 못하도록 경고 페이지를 표시합니다. 그런 다음 사용자는 경고를 무시하기로 결정한 경우 웹사이트에 대해 계속을 선택해야 합니다. 프록시 서버를 사용하도록 구성된 클라이언트 시스템에서는 계속*(*경고*)* 페이지가 제대로 표시되지 않습니다.

카테고리 설정	설명
	• 재정의 - 사이트에 액세스하기 위해 유효한 암호를 입력하라는 응답 페이지를 표시합니다. URL 관리 재정의 설정(**Device** > **Setup** > **Content ID**)을 구성하여 비밀번호 및 기타 재정의 설정을 관리합니다. (디바이스 > 설정 > 콘텐츠 ID의 관리 설정 표도 참조하십시오). 프록시 서버를 사용하도록 구성된 클라이언트 시스템에서는 재정의 페이지가 제대로 표시되지 않습니다. • 없음(사용자 지정 URL 카테고리만 해당) - 사용자 지정 URL 카테고리를 생성한 경우 방화벽이 URL 데이터베이스 공급자로부터 URL 필터링 카테고리 할당을 상속할 수 있도록 작업을 없음으로 설정합니다. 작업을 없음으로 설정하면 정책 규칙(보안, 복호화 및 QoS)의 일치 기준으로 사용자 지정 URL 카테고리를 사용하여 예외를 만들거나 다른 작업을 시행할 수 있도록 허용하면서 URL 필터링 프로파일의 사용자 지정 카테고리를 무시할 수 있는 유연성이 제공됩니다. 사용자 지정 URL 카테고리를 삭제하려면 사용자 지정 카테고리가 사용되는 모든 프로파일에서 작업을 없음으로 설정해야 합니다. 사용자 지정 URL 카테고리에 대한 자세한 내용은 개체 > 사용자 지정 개체 > URL 카테고리를 참조하십시오.
사용자 자격 증명 제출	각 URL 카테고리에 대해 사용자 자격 증명 제출을 선택하여 사용자가 해당 카테고리의 URL에 유효한 회사 자격 증명을 제출하는 것을 허용하거나 허용하지 않습니다. URL 카테고리를 기반으로 사용자 자격 증명 제출을 제어하려면 자격 증명 제출 검색을 활성화해야 합니다(사용자 자격 증명 검색 탭 선택). 사이트 액세스가 차단으로 설정된 URL 카테고리는 사용자 자격 증명 제출도 자동으로 차단하도록 설정됩니다. • 경고 - 사용자가 웹사이트에 자격 증명을 제출할 수 있도록 허용하지만 사용자가 이 카테고리의 사이트에 자격 증명을 제출할 때마다 URL 필터링 로그를 생성합니다. • 허용(기본값) - 사용자가 웹사이트에 자격 증명을 제출할 수 있습니다. • 차단 - 사용자가 웹사이트에 자격 증명을 제출하지 못하도록 차단합니다. 기본 피싱 방지 응답 페이지는 사용자 자격 증명 제출을 차단합니다. • 계속 - 사이트에 자격 증명을 제출하려면 계속을 선택하라는 응답 페이지를 사용자에게 표시합니다. 기본적으로 피싱 방지 계속 페이지는 자격 증명 제출이 권장되지 않는 사이트에 자격 증명을 제출하려고 할 때 사용자에게 경고하기 위해 표시됩니다. 피싱 시도에 대해 사용자에게 경고하거나 다른 웹사이트에서 유효한 회사 자격 증명을 재사용하지 않도록 교육하는 사용자 지정 응답 페이지를 생성하도록 선택할 수 있습니다.

카테고리 설정	설명
URL 카테고리 확인	PAN-DB URL 필터링 데이터베이스에 액세스하려면 클릭합니다. 여기에서 URL 또는 IP 주소를 입력하여 분류 정보를 볼 수 있습니다.
동적 URL 필터링(기본적으로 비활성화됨) (BrightCloud에 대해서만 구성 가능)	URL 분류를 위해 클라우드 조회를 활성화하려면 선택합니다. 이 옵션은 로컬 데이터베이스가 URL을 분류할 수 없는 경우 적용됩니다. 5초 제한 시간 후에 URL이 확인되지 않으면 응답이 #### ## URL로 표시됩니다. *PAN-DB*에서 이 옵션은 기본적으로 활성화되어 있으며 구성할 수 없습니다.

URL 필터링 설정

개체 > 보안 프로파일 > **URL** 필터링 > **URL** 필터링 설정을 선택하여 세이프 서치 설정을 적용하고 HTTP 헤더의 로깅을 활성화합니다.

URL 필터링 설정	설명
로그 컨테이너 페이지만 해당 기본: 활성화됨	지정된 컨텐츠 유형과 일치하는 URL만 기록하려면 이 옵션을 선택하십시오. 방화벽은 세션 중에 광고 및 콘텐츠 링크와 같은 관련 웹 링크를 기록하지 않으므로 관련 URL을 계속 기록하면서 기록 및 메모리 부하를 줄입니다. 소스의 원래 *IP* 주소를 마스킹하는 프록시를 사용하는 경우 HTTP 헤더 로깅 ***X-Forwarded-For*** 옵션을 활성화하여 웹 페이지 요청을 시작한 사용자의 원래 *IP* 주소를 보존하십시오.
세이프서치 기능 활성화 기본: Disabled 이 기능을 사용하기 위해 URL 필터링 라이선스가 필요하지 않습니다.	엄격한 세이프 서치 필터링을 적용하려면 이 옵션을 선택합니다. 많은 검색 엔진에는 검색어 반환 트래픽에서 성인 이미지와 비디오를 필터링하는 세이프 서치 설정이 있습니다. Safe Search Enforcement 사용 설정을 선택하면 최종 사용자가 검색 쿼리에서 가장 엄격한 세이프 서치 설정을 사용하지 않는 경우 방화벽이 검색 결과를 차단합니다. 방화벽은 다음 검색 공급자에 대해 세이프 서치를 시행할 수 있습니다. 구글, 야후, 빙, 얀덱스, 유튜브. 이는 최적화된 설정이며 검색 공급자가 모든 웹사이트에서 작동하도록 보장하지 않습니다. 세이프 서치 기능을 사용하려면 이 설정을 활성화한 다음 URL 필터링 프로파일 보안 정책 규칙을 연결해야 합니다. 그러면 방화벽은 가장 엄격한 세이프 서치 설정을 사용하지 않는 일치하는 검색 쿼리 반환 트래픽을 차단합니다.

URL 필터링 설정	설명
	Yahoo 계정에 로그인한 상태에서 *Yahoo Japan(yahoo.co.jp)*에서 검색을 하는 경우 검색 설정에 대한 잠금 옵션도 활성화해야 합니다. 사용자가 다른 검색 공급자를 통해 이 기능을 우회하지 못하도록 하려면 검색 엔진 카테고리를 차단하도록 *URL* 필터링 프로파일을 구성한 다음 *Bing, Google, Yahoo, Yandex* 및 *YouTube*에 대한 액세스를 허용합니다.
HTTP 헤더 로깅	HTTP 헤더 로깅을 활성화하면 서버로 전송되는 HTTP 요청에 포함된 속성에 대한 가시성을 제공합니다. 활성화되면 다음 속성-값 쌍 중 하나 이상이 URL 필터링 로그에 기록됩니다. • 사용자 에이전트 - 사용자가 URL에 액세스하는 데 사용한 웹 브라우저입니다. 이 정보는 서버에 대한 HTTP 요청으로 전송됩니다. 예를 들어, 사용자 에이전트는 Internet Explorer 또는 Firefox일 수 있습니다. 로그의 User-Agent 값은 최대 1024자를 지원합니다. • 참조자 - 사용자를 다른 웹 페이지에 연결한 웹 페이지의 URL입니다. 사용자를 요청 중인 웹 페이지로 리디렉션(참조)한 소스입니다. 로그의 참조자 값은 최대 256자를 지원합니다. • X-Forwarded-For - 웹 페이지를 요청한 사용자의 IP 주소를 유지하는 헤더 필드 옵션입니다. 이를 통해 사용자의 IP 주소를 식별할 수 있습니다. 이는 네트워크에 프록시 서버가 있거나 모든 요청이 시작되는 것처럼 보이도록 사용자의 IP 주소를 마스킹하는 소스 NAT를 구현한 경우 특히 유용하며, 이는 모든 요청이 프록시 서버의 IP 주소 또는 공통 IP 주소에서 시작된 것처럼 보이도록 사용자의 IP 주소를 마스킹하는 것입니다. 로그의 X-Forwarded-For(XFF) 값은 최대 128자를 지원합니다.

사용자 자격 증명 감지

사용자가 회사 자격 증명을 제출할 때 방화벽이 감지할 수 있도록 하려면 개체 > 보안 프로파일 > **URL** 필터링 > 사용자 자격 증명 검색을 선택합니다.

사용자가 지정된 *URL* 카테고리의 사이트에만 자격 증명을 제출할 수 있도록 사용자 자격 증명 감지를 구성합니다. 이렇게 하면 신뢰할 수 없는 카테고리의 사이트에 대한 자격 증명 제출을 방지하여 공격 면적을 줄일 수 있습니다. 사용자 자격 증명 제출을 위해 *URL* 필터링 프로파일의 모든 *URL* 카테고리를 차단하는 경우 자격 증명을 확인할 필요가 없습니다.

방화벽은 세 가지 방법 중 하나를 사용하여 웹 페이지에 제출된 유효한 자격 증명을 감지합니다. 각 방법에는 방화벽이 웹 페이지에 대한 사용자명 및 암호 제출을 유효한 회사 자격 증명과 비교할 수 있도록 하는

User-ID™가 필요합니다. 다음 방법 중 하나를 선택하여 계속해서 URL 카테고리를 기반으로 자격 증명 피싱을 방지합니다.

사용자 자격 증명을 모니터링할 트래픽을 복호화하도록 방화벽을 구성해야 합니다.

사용자 자격 증명 감지 설정	설명
IP 사용자	이 자격 증명 감지 방법은 유효한 사용자명 제출을 확인합니다. 이 방법을 사용하여 유효한 기업 사용자명이 포함된 자격 증명 제출을 감지할 수 있습니다(수반된 암호와 관계 없음). 방화벽은 사용자명이 세션의 소스 IP 주소에 로그인한 사용자와 일치하는지 확인하여 사용자명 일치를 결정합니다. 이 방법을 사용하기 위해 방화벽은 제출된 사용자명을 IP 주소 - 사용자명 매핑 테이블과 일치시킵니다. 이 방법을 사용하려면 사용자에게 IP 주소 매핑에 설명된 모든 사용자 매핑 방법을 사용할 수 있습니다.
그룹 매핑	방화벽은 사용자가 제한된 사이트에 제출한 사용자명이 유효한 기업 사용자명과 일치하는지 확인합니다. 이를 위해 방화벽은 제출된 사용자명을 사용자 - 그룹 매핑 테이블의 사용자명 목록과 일치시켜 사용자가 제한된 카테고리의 사이트에 기업 사용자명을 제출할 때를 감지합니다. 이 방법은 LDAP 그룹 구성원 자격을 기반으로 기업 사용자명 제출만 확인하므로 구성이 간단하지만 가양성(false positive)이 발생하기 쉽습니다. 이 방법을 사용하려면 그룹 매핑을 활성화 해야 합니다.
도메인 자격 증명	이 자격 증명 감지 방법을 사용하면 방화벽이 유효한 기업 사용자명과 관련 암호를 확인할 수 있습니다. 방화벽은 사용자가 제출한 사용자명 및 암호가 동일한 사용자의 기업 사용자명 및 암호와 일치하는지 확인합니다. 이렇게 하려면 방화벽이 자격 증명 제출을 유효한 기업 사용자명 및 암호와 일치시키고 제출된 사용자명이 로그인한 사용자의 IP 주소에 매핑되는지 확인할 수 있어야 합니다. 이 모드는 Windows 기반 User-ID 에이전트에서만 지원되며 User-ID 에이전트가 RODC(읽기 전용 도메인 컨트롤러)에 설치되고 User-ID 자격 증명 서비스 추가 기능이 갖춰져 있어야 합니다. 이 방법을 사용하려면 인증 정책, 인증 포털 및 GlobalProtect™를 포함하여 지원되는 사용자 매핑 방법을 사용하여 사용자에게 IP 주소를 매핑할 수 있도록 User-ID도 활성화해야 합니다. 방화벽이 유효한 회사 자격 증명 제출을 확인하는 데 사용할 수 있는 각 방법과 피싱 방지를 활성화하는 단계에 대한 자세한 내용은 자격 증명 피싱 방

사용자 자격 증명 감지 설정	설명
	지 를 참조하십시오.
유효한 사용자명이 감지된 로그 심각도	방화벽이 웹사이트에 유효한 사용자명 제출을 감지했음을 나타내는 로그의 심각도를 설정합니다. 이 로그 심각도는 경고, 차단 또는 계속에 대한 자격 증명 제출 권한이 있는 웹사이트에 유효한 사용자명이 제출된 이벤트와 연결됩니다. 자격 증명 제출이 허용되는 웹사이트에 사용자가 유효한 사용자명을 제출할 때 기록하는 로그의 심각도는 정보 제공을 위한 것입니다. 카테고리를 선택하여 자격 증명 제출이 허용 및 차단되는 URL 카테고리를 검토하거나 조정합니다. 로그 심각도를 중간 이상으로 설정합니다.

HTTP 헤더 삽입

HTTP 헤더와 해당 값을 HTTP 요청에 삽입하여 방화벽이 웹 애플리케이션 액세스를 관리할 수 있도록 하려면 개체 > 보안 프로파일 > **URL** 필터링 > **HTTP** 헤더삽입을 선택합니다.

방화벽은 *HTTP/1.x* 트래픽에 대해서만 헤더 삽입을 지원합니다. 방화벽은 *HTTP/2* 트래픽에 대한 헤더 삽입을 지원하지 않습니다.

사전 정의된 HTTP 헤더 삽입 유형에 따라 삽입 항목을 만들거나 사용자 지정 형식을 만들 수 있습니다. 헤더 삽입은 일반적으로 사용자 지정 HTTP 헤더에 대해 수행되지만 표준 HTTP 헤더도 삽입할 수도 있습니다.

헤더 삽입은 다음과 같은 경우에 발생합니다.

1. HTTP 요청은 하나 이상의 구성된 HTTP 헤더 삽입 항목과 보안 정책 규칙과 일치합니다.
2. 지정된 도메인은 HTTP 호스트 헤더에 있는 도메인과 일치합니다.
3. 작업은 ## 이외의 다른 것입니다.

방화벽은 *GET, POST, PUT* 및 *HEAD* 메서드에 대해서만 *HTTP* 헤더 삽입을 수행할 수 있습니다.

HTTP 헤더 삽입을 사용하도록 설정하고 요청에서 식별된 헤더가 없는 경우 방화벽에서 헤더를 삽입합니다. 식별된 헤더가 요청에 이미 있는 경우 방화벽은 지정한 값으로 헤더 값을 덮어씁니다.

삽입 항목을 추가하거나 기존 삽입 항목을 선택하여 수정합니다. 필요한 경우 삽입 항목을 선택한 다음 삭제할 수도 있습니다.

새 *HTTP* 헤더 삽입 항목에 대한 기본 블록 목록 작업은 ##입니다. 다른 작업을 원하면 URL 필터링 카테고리*(으)*로 이동하여 적절한 작업을 선택합니다. 또는 원하는 동작으로 구성된 프로파일에 삽입 항목을 추가합니다.

HTTP 헤더 삽입 설정	설명
이름	이 HTTP 헤더 삽입 항목의 이름입니다.
유형	생성할 항목 유형입니다. 항목은 사전 정의되거나 사용자 지정될 수 있습니다. 방화벽은 콘텐츠 업데이트를 사용하여 사전 정의된 항목을 채우고 유지 관리합니다. HTTP 헤더에 사용자명을 포함하려면 동적 필드를 선택합니다.
도메인	헤더 삽입은 이 목록의 도메인이 HTTP 요청의 호스트 헤더와 일치할 때 발생합니다. 사전 정의된 항목을 만드는 경우 도메인 목록은 콘텐츠 업데이트에서 사전 정의됩니다. 대부분의 사용 사례에 충분하지만 필요에 따라 도메인을 추가하거나 삭제할 수 있습니다. 사용자 지정 항목을 만들려면 이 목록에 하나 이상의 도메인을 추가합니다. 각 도메인 이름은 최대 256자일 수 있으며 각 항목에 대해 최대 50개의 도메인을 식별할 수 있습니다. 별표(*)를 와일드카드 문자로 사용할 수 있으며, 이는 지정된 도메인에 대한 모든 요청(예: *.etrade.com)과 일치합니다.
머리글	사전 정의된 항목을 만들 때 헤더 목록은 콘텐츠 업데이트로 미리 채워집니다. 대부분의 사용 사례에 충분하지만 필요에 따라 헤더를 추가하거나 삭제할 수 있습니다. 사용자 지정 항목을 만들 때 이 목록에 하나 이상의 헤더(최대 5개)를 추가합니다. 헤더 이름에는 최대 100자까지 가질 수 있지만 공백은 포함되지 않습니다. HTTP 헤더에 사용자명을 포함하려면 **X** 인증된 사용자를 선택한 다음 값을 선택하거나 새 헤더를 추가합니다.
값	최대 16K자만 사용하여 값을 구성합니다. 헤더 값은 지정된 도메인의 HTTP 헤더에 포함할 정보에 따라 다릅니다. 예를 들어 사전 정의된 형식을 선택하거나 사용자 지정 항목을사용하여 SaaS 애플리케이션에 대한 사용자 액세스를 관리합니다. HTTP 헤더에 사용자명을 포함하려면 보안 디바이스에 필요한 도메인 및 사용자명 형식을 선택합니다. • **`($domain)\($user)`**

HTTP 헤더 삽입 설정	설명
	• **WinNT://($domain)/($user)** 또는 **($user)** 및 **($domain)** 동적 토큰(예: **$user)@($domain)**을 사용하여 사용자 지정 형식을 입력합니다. 방화벽은 그룹 매핑 프로파일의 기본 사용자명을 사용하여 사용자 및 도메인 동적 토큰을 채웁니다. 각 ***($user)***과 ***($domain)*** 동적 토큰을 값당 한 번만 사용합니다.
로그	이 헤더 삽입 항목의 로깅을 사용하도록 로그를 선택합니다.

인라인 범주화

실시간 웹 페이지 분석을 활성화하고 구성하려면 개체 > 보안 프로파일 > **URL** 필터링 > 인라인 분류를 선택합니다.

필드	설명
인라인 분류 탭을 사용하여 실시간 웹 페이지 분석을 활성화하고 URL 예외를 관리할 수 있습니다.	
실시간 URL 분석은 로컬에서는 방화벽 기반 탐지 메커니즘으로, 클라우드에서는 고급 URL 필터링 서비스의 일부로 사용할 수 있습니다. • 로컬 인라인 분류 사용 - 방화벽 기반 머신 러닝 모델을 사용하여 URL 트래픽을 실시간으로 분석하여 악성 피싱 변종 및 JavaScript 익스플로잇이 네트워크에 침입하는 것을 감지하고 방지합니다. • 클라우드 인라인 분류 사용 - 로컬 인라인 ML에서 사용하는 분석 엔진을 보완하는 기계 학습 기반 감지기를 사용하여 보완 분석을 위해 의심스러운 웹 페이지 콘텐츠를 클라우드로 전달하여 URL의 실시간 분석을 가능하게 합니다.	
예외	인라인 분류를 사용하여 분석하지 않으려는 특정 웹 사이트에 대해 URL 예외를 정의할 수 있습니다. URL 예외를 추가하려면 먼저 유효한 EDL(외부 동적 목록) 또는 사용자 지정 URL 카테고리를 정의해야 합니다. 추가를 클릭하여 사용 가능한 옵션을 보고 선택합니다.

개체 > 보안 프로파일 > 파일 차단

파일 차단 프로파일을 보안 정책 규칙(정책 > 보안)에 연결하여 사용자가 지정된 파일 형식을 업로드 또는 다운로드하지 못하도록 차단하거나 사용자가 지정된 파일 형식을 업로드 또는 다운로드하려고 할 때 경고를 생성할 수 있습니다.

최상의 보안을 위해 사전 정의된 엄격한 프로파일을 적용합니다. 엄격한 프로파일이 차단하는 파일 형식을 사용하는 중요한 애플리케이션을 지원해야 하는 경우 엄격한 프로파일을 복사하고 필요한 파일 형식 예외만 만드십시오. 파일 형식을 사용해야 하는 소스, 대상 및 사용자에게만 예외를 제한하는 보안 정책 규칙에 복사된 프로파일을 적용합니다. 방향을 사용하여 예외를 업로드 또는 다운로드로 제한할 수도 있습니다.

모든 *Windows PE* 파일을 차단하지 않는 경우 분석을 위해 모든 알 수 없는 파일을 *WildFire*로 보냅니다. 사용자 계정의 경우 악성 웹사이트, 이메일 또는 팝업으로 인해 사용자가 의도하지 않게 악성 파일을 다운로드하는 드라이브 바이 다운로드를 계속 방지하도록 작업을 설정합니다. 의도적으로 시작하지 않은 파일 전송에 대한 계속*(Continue)* 프롬프트가 표시되면 악성 다운로드의 대상이 될 수 있음을 사용자에게 교육합니다.

다음 표에서는 파일 차단 프로파일 설정에 대해 설명합니다.

파일 차단 프로파일 설정	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 파일 차단 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 파일 차단 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.

파일 차단 프로파일 설정	설명

규칙	선택한 파일 형식에 대해 수행할 작업(있는 경우)을 지정하는 하나 이상의 규칙을 정의합니다. 규칙을 추가하려면 다음을 지정하고 추가를 클릭합니다.
	• 이름 - 규칙 이름을 입력합니다(최대 31자).
	• 애플리케이션 - 규칙이 적용되는 애플리케이션을 선택하거나 모두를 선택합니다.
	• 파일 형식 - 파일 형식 필드를 클릭한 다음 추가를 클릭하여 지원되는 파일 형식 목록을 봅니다. 파일 형식을 클릭하여 프로파일에 추가하고 필요에 따라 계속해서 추가 파일 형식을 추가합니다. 모두를 선택하면 지원되는 모든 파일 형식에 대해 정의된 작업이 수행됩니다.
	• 방향 - 파일 전송 방향(업로드, 다운로드 또는 둘 다)을 선택합니다.
	• 작업 - 선택한 파일 형식이 감지될 때 수행할 작업을 선택합니다.
	  • 경고 - 위협 로그에 항목이 추가됩니다.
	  • 계속 - 사용자에게 메시지가 다운로드가 요청되었음을 나타내고 계속할지의 여부를 확인하도록 요청합니다. 목적은 사용자에게 알 수 없는 다운로드 가능성(드라이브 바이 다운로드라고도 함)을 경고하고 사용자에게 다운로드를 계속하거나 중지할 수 있는 옵션을 제공하는 것입니다.
	  계속 작업으로 파일 차단 프로파일을 만들 때 애플리케이션 웹 브라우징만 선택할 수 있습니다. 다른 애플리케이션을 선택하면 사용자에게 계속 페이지가 표시되지 않기 때문에 보안 정책 규칙과 일치하는 트래픽이 방화벽을 통과하지 않습니다.
	  • 차단 - 파일이 차단되었습니다.

Objects > Security Profiles > WildFire Analysis

WildFire 분석 프로파일을 사용하여 WildFire 파일 분석이 WildFire 어플라이언스 또는 WildFire 클라우드에서 로컬로 수행되도록 지정합니다. 파일 유형, 애플리케이션 또는 파일의 전송 방향(업로드 또는 다운로드)에 따라 퍼블릭 클라우드 또는 프라이빗 클라우드로 포워딩할 트래픽을 지정할 수 있습니다. WildFire 분석 프로파일을 생성한 후 프로파일을 정책(정책 > 보안)에 추가하면 해당 정책과 일치하는 모든 트래픽(예: 정책에 정의된 URL 카테고리)에 프로파일 설정을 추가로 적용할 수 있습니다.

사전 정의된 기본 프로파일을 사용하여 분석을 위해 모든 알 수 없는 파일을 WildFire로 포워딩합니다. 또한 WildFire 어플라이언스 콘텐츠 업데이트가 매분 다운로드 및 설치되도록 설정하여 항상 최신 지원을 받을 수 있습니다.

WildFire 분석 프로파일 설정	
이름	WildFire 분석 프로파일을 설명하는 이름을 입력합니다(최대 31자). 이 이름은 보안 정책 규칙을 정의할 때 선택할 수 있는 WildFire Analysis 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	선택적으로 프로파일 규칙 또는 프로파일의 용도를 설명합니다(최대 255자).
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 취약점 보호 프로파일의 설정을 무시하지 못하도록 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
규칙	분석을 위해 WildFire 퍼블릭 클라우드 또는 WildFire 어플라이언스(사설 클라우드)로 포워딩할 트래픽을 지정하는 하나 이상의 규칙을 정의합니다. • 프로파일에 추가하는 모든 규칙을 설명하는 이름을 입력합니다(최대 31자). • 모든 애플리케이션 트래픽이 규칙과 일치하고 지정된 분석 대상으로 포워딩되도록 애플리케이션을 추가합니다. • 규칙에 대해 정의된 분석 대상에서 분석할 파일 형식을 선택합니다.

WildFire 분석 프로파일 설정	
	WildFire 프라이빗 클라우드*(WildFire* 어플라이언스에서 호스팅*)*는 *APK, Mac OS X,* 아카이브 및 *Linux* 파일 분석을 지원하지 않습니다. • 전송 방향에 따라 트래픽에 규칙을 적용합니다. 트래픽을 업로드하거나 트래픽을 다운로드하거나 둘 다에 규칙을 적용할 수 있습니다. • 분석을 위해 포워딩할 트래픽의 대상을 선택합니다. 하이브리드 클라우드 배포에서는 프라이빗 클라우드 및 퍼블릭 클라우드 규칙에 모두 일치하는 파일은 예방 조치로 프라이빗 클라우드로만 전달됩니다. • 규칙과 일치하는 모든 트래픽이 분석을 위해 WildFire 퍼블릭 클라우드로 포워딩되도록 public-cloud를 선택합니다. • 규칙과 일치하는 모든 트래픽이 분석을 위해 WildFire 어플라이언스로 포워딩되도록 private-cloud를 선택합니다.

개체 > 보안 프로필 > 데이터 필터링

데이터 필터링을 통해 방화벽은 신용카드 또는 주민등록 번호 또는 내부 회사 문서와 같은 중요한 정보를 감지하고 이 데이터가 보안 네트워크에서 유출되는 것을 방지할 수 있습니다. 데이터 필터링을 활성화하기 전에 개체 > 사용자 정의 개체 > 데이터 패턴을 선택하여 필터링할 데이터 유형(예: "기밀"이라는 단어가 포함된 사회보장 번호 또는 문서 제목)을 정의합니다. 단일 데이터 필터링 프로파일에 여러 데이터 패턴 개체를 추가할 수 있으며 보안 정책 규칙에 연결되면 방화벽 검사에서 각 데이터 패턴에 대한 트래픽이 허용되고 데이터 필터링 프로파일 설정에 따라 트래픽이 일치하는 것을 차단할 수 있습니다.

데이터 필터링 프로파일 설정	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 로그 포워딩 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 데이터 필터링 프로파일의 설정을 재정의하지 못하도록 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
데이터 캡처	이 옵션을 선택하여 필터에 의해 차단된 데이터를 자동으로 수집합니다. 설정 페이지에서 데이터 보호 관리를 위한 암호를 지정하여 캡처된 데이터를 봅니다. 디바이스 > 설정 >관리를 참조하십시오.
데이터 패턴	필터링에 사용할 기존 데이터 패턴을 추가하거나 새로 만들기를 선택하여 새 데이터 패턴 개체를 구성합니다(개체 > 사용자 정의 개체 > 데이터 패턴).
애플리케이션	필터링 규칙에 포함할 애플리케이션을 지정합니다.

데이터 필터링 프로파일 설정	설명
	• 나열된 모든 애플리케이션에 필터를 적용할 필터를 선택합니다. 이 선택은 나열된 애플리케이션만 차단하지는 않습니다. • 개별 애플리케이션을 지정하려면 추가를 클릭합니다.
파일 유형	필터링 규칙에 포함할 파일 형식을 지정합니다. • 나열된 모든 파일 형식에 필터를 적용하려면 모두를 선택합니다. 이 선택으로 나열된 파일 형식만 차단하지는 않습니다. • 개별 파일 형식을 지정하려면 추가를 클릭합니다.
방향	업로드 방향, 다운로드 방향 또는 둘 다에 필터를 적용할지의 여부를 지정합니다.
경고 임계값	경고를 트리거하려면 파일에서 데이터 패턴을 검색해야 하는 횟수를 지정합니다.
블록 임계값	데이터 패턴의 이 많은 인스턴스를 포함하는 파일을 차단합니다.
로그 심각도	이 데이터 필터링 프로파일 규칙과 일치하는 이벤트에 대해 기록된 로그 심각도를 정의합니다.

개체 > 보안 프로파일 > DoS 방어

DoS 방어 프로파일은 고정밀 타겟팅을 위해 설계되었으며 영역 보호 프로파일을 보강합니다. DoS 방어 프로파일은 새 CPS(초당 연결 수)가 경보 및 작업(DoS 방어 정책에 지정됨)을 트리거하는 임계값 비율을 지정합니다. DoS Protection 프로파일은 최대 CPS 속도와 차단된 IP 주소가 차단 IP 목록에 남아 있는 기간도 지정합니다. DoS 방어 정책 규칙에서 DoS 방어 프로파일을 지정합니다. 여기서 규칙과 일치하는 패킷의 기준을 지정하고 정책 규칙은 프로파일이 적용되는 디바이스를 결정합니다.

DoS 방어 프로파일 및 정책을 생성하여 중요한 개별 디바이스 또는 소규모 디바이스 그룹, 특히 웹 서버 및 데이터베이스 서버와 같은 인터넷 연결 디바이스를 보호합니다.

통합 및 분류된 DoS 방어 프로파일을 구성할 수 있습니다. DoS Protection 정책 규칙에 통합 프로파일, 분류된 프로파일 또는 각 유형 중 하나를 적용할 수 있습니다. 규칙에 두 프로파일 유형을 모두 적용하면 방화벽은 먼저 통합 프로파일을 적용한 다음 필요한 경우 분류된 프로파일을 적용합니다.

- 분류된 DoS 방어 프로파일에는 분류됨이 유형으로 선택되어 있습니다. 분류된 DoS 보호 프로파일을 작업이 보호인 DoS 보호 규칙에 적용하면 패킷이 지정된 주소 유형(source-ip-only, destination-ip-only, or src-dest-ip-both)을 충족하는 경우 방화벽이 프로파일의 CPS 임계값에 대한 연결 수를 계산합니다.
- 통합 DoS Protection 프로파일에는 **Aggregate**가 유형으로 선택되어 있습니다. 작업이 보호인 DoS 방어 규칙에 DoS 방어 통합 프로파일을 적용하면 방화벽은 프로파일의 CPS 임계값에 대한 규칙 기준을 충족하는 모든 연결(규칙에 지정된 디바이스 그룹에 대한 결합된 연결 수)을 계산합니다.

DoS 방어 프로파일을 DoS 방어 정책에 적용하려면 정책 > DoS 방어를 참조하십시오.

다중 가상 시스템*(multi-vsys)* 환경이 있고 다음을 구성한 경우*:*

- 가상 시스템 간 통신 및
- 가상 시스템이 외부 통신을 위해 공통 인터페이스와 단일 *IP* 주소를 공유할 수 있도록 하는 공유 게이트웨이

다음 영역 및 *DoS* 방어 메커니즘은 외부 영역에서 비활성화됩니다.

- *SYN* 쿠키
- *IP* 단편화
- *ICMPv6*

IP 조각화 및 *ICMPv6* 보호를 활성화하려면 공유 게이트웨이에 대해 별도의 영역 보호 프로파일을 만듭니다.

공유 게이트웨이에서 *SYN* 플러드로부터 보호하기 위해 *Random Early Drop* 또는 *SYN* 쿠키를 사용하여 *SYN Flood* 보호 프로파일을 적용할 수 있습니다. 외부 영역에서는 *SYN Flood* 보호를 위해 *Random Early Drop*만 사용할 수 있습니다.

DoS 방어 프로파일 설정	
이름	프로파일 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 로그 포워딩 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	프로파일에 대한 설명을 입력합니다(최대 255자).
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 DoS 방어 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.

DoS 방어 프로파일 설정	
유형	다음 프로파일 유형 중 하나를 선택하십시오. • 통합 - 이 프로파일이 적용되는 규칙 기준과 일치하는 모든 연결에 프로파일에 구성된 DoS 임계값을 적용합니다. 예를 들어 SYN 플러드 경보 비율 임계값이 10,000CPS인 통합 규칙은 DoS 규칙과 일치하는 모든 디바이스의 결합된 연결을 계산합니다. 그룹의 총 CPS가 10,000CPS를 초과하면 CPS가 디바이스 전체에 분산되는 방식에 관계없이 경보를 트리거합니다. • 분류됨 - 분류 기준(소스 IP 주소, 대상 IP 주소 또는 소스 및 대상 IP 주소 쌍)과 일치하는 각 개별 연결에 프로파일에 구성된 DoS 임계값을 적용합니다. 예를 들어 SYN 플러드 경보 비율 임계값이 10,000CPS인 분류된 규칙은 디바이스당 최대 10,000CPS를 허용하고 DoS 규칙에 지정된 개별 디바이스가 10,000CPS를 초과하면 경보를 트리거합니다.
플러드 방지 탭	

SYN 플러드 탭
UDP 플러드 탭
ICMP 플러드 탭
ICMPv6 플러드 탭
기타 IP Flood 탭
	탭에 표시된 플러드 방지 유형을 활성화하고 다음 설정을 지정하려면 이 옵션을 선택합니다.
	• 작업 - (**SYN** 서비스 장애만 해당) DoS 방어 정책 작업이 보호이고 수신 CPS가 활성화 비율에 도달하는 경우 방화벽이 수행하는 작업입니다. 다음 중 하나를 선택합니다.
	  • **Random Early Drop** - 초당 연결이 활성화 속도 임계값에 도달하면 패킷을 무작위로 삭제합니다.
	  • **SYN** 쿠키 - SYN 플러드 공격 중에 연결을 끊을 필요가 없도록 SYN 쿠키를 사용하여 승인을 생성합니다.
	  합법적인 트래픽을 공정하게 처리하지만 더 많은 방화벽 리소스를 소비하는 *SYN* 쿠키로 시작하십시오. *CPU* 및 메모리 사용률을 모니터링하고 *SYN* 쿠키가 지나치게 많은 리소스를 소비하는 경우 *RED*로 전환합니다. 대규모 *DoS* 공격으로부터 보호하기 위해 네트워크*(*인터넷*)* 에지에 전용 *DDoS* 방지 디바이스가 없는 경우 항상 *RED*를 사용하십시오.
	• 경보 비율 - DoS 경보를 생성할 임계값 비율(CPS)을 지정합니다(범위는 0 ~ 2,000,000cps, 기본값은 10,000cps).
	분류된 프로파일의 경우 정상 변동을 수용하고 지나치게 많은 경보를 수신하는 경우 임계값을 조정하기 위해 임계값을 디바이스의 평균 CPS 속도보다 15-20% 높게 설정하는 것이 가장 좋습니다. 통합 프로파일의 경

DoS 방어 프로파일 설정	
	우 가장 좋은 방법은 임계값을 그룹의 평균 CPS 비율보다 15-20% 높게 설정하는 것입니다. 필요에 따라 임계값을 모니터링하고 조정합니다. • 활성화 속도 - DoS 응답이 활성화되는 임계값 속도(cps)를 지정합니다. DoS 응답은 DoS 방어 프로파일(임의 조기 삭제 또는 SYN 쿠키)의 작업 필드에서 구성됩니다. 활성화 속도 범위는 0 ~ 2,000,000cps이고, 기본값은 10,000cps입니다. 프로파일 동작이 **Random Early Drop**(RED)인 경우 초당 들어오는 연결이 활성화 속도 임계값에 도달하면 RED가 발생합니다. CPS 비율이 증가하면 알고리즘에 따라 RED 비율이 증가합니다. 방화벽은 CPS 속도가 최대 속도 임계값에 도달할 때까지 빨간색으로 계속됩니다. 분류된 프로파일은 개별 디바이스에 정확한 CPS 제한을 적용하고 보호된 디바이스의 용량을 기준으로 이러한 제한을 설정하므로 CPS를 점진적으로 조절할 필요가 없으며 활성화 속도를 최대 속도와 동일한 임계값으로 설정할 수 있습니다. 최대 속도에 도달하기 전에 개별 서버에 대한 트래픽 삭제를 시작하려는 경우에만 활성화 속도를 최대 속도보다 낮게 설정하십시오. 통합 프로파일의 경우 그룹의 최고 CPS 비율 바로 위의 임계값을 설정합니다. 필요에 따라 임계값을 모니터링하고 조정합니다. • 최대 속도 - 방화벽이 허용하는 초당 들어오는 연결의 임계값 속도를 지정합니다. 최대 속도 임계값에서 방화벽은 새 연결의 100%를 삭제합니다(범위는 2~2,000,000cps, 기본값은 40,000cps). 분류된 프로파일의 경우 최대 속도는 보호하는 디바이스의 용량을 기준으로 하여 넘치지 않도록 합니다. 통합 프로파일의 경우 최대 비율을 그룹 용량의 80-90%로 설정합니다. 필요에 따라 임계값을 모니터링하고 조정합니다. • 차단 기간 - 문제가 되는 IP 주소가 차단 IP 목록에 남아 있고 해당 IP 주소와의 연결이 차단되는 시간(초)을 지정합니다. 방화벽은 경보 비율, 활성화 비율 또는 최대 비율 임계값(범위는 1~21,600초, 기본값은 300초)을 향해 차단 기간 동안 도착하는 패킷을 계산하지 않습니다.
자원 보호 탭	
세션	리소스 보호를 활성화하려면 이 옵션을 선택합니다.
최대 동시 세션	최대 동시 세션 수를 지정합니다. • 통합된 프로파일 유형의 경우 이 제한은 DoS 방어 프로파일이 적용된 DoS 방어 규칙에 도달하는 모든 트래픽에 적용됩니다.

DoS 방어 프로파일 설정	
	• 분류된 프로파일 유형의 경우 이 제한은 DoS 방어 프로파일이 적용되는 DoS 방어 규칙에 도달하는 분류 기반(소스 IP, 대상 IP 또는 소스 및 대상 IP)의 트래픽에 적용됩니다.

개체 > 보안 프로파일 > 모바일 네트워크 보호

모바일 네트워크 보호 프로파일을 사용하면 방화벽이 5G SBA(서비스 기반 아키텍처) 트래픽에서 GTP 및 HTTP/2를 검사할 수 있습니다. 이 프로파일을 보려면 디바이스 > 설정 > 관리에서 GTP 보안을 활성화해야 합니다.

이 프로파일의 옵션을 사용하여 5G HTTP/2, GTP v1-C, GTP v2-C, GTP-U 및 PFCP의 상태 기반 검사를 활성화하고 GTPv1-C, GTP v2-C 및 GTP-에 대한 프로토콜 유효성 검사를 활성화합니다. U 및 GTP-U 터널 내에서 사용자 데이터를 스캔하기 위해 GTP-U 콘텐츠 검사를 활성화합니다. 또한 APN, IMSI/IMSI-Prefix 및 RAT를 기반으로 GTP 세션을 필터링하고 최종 사용자 IP 주소 스푸핑을 방지할 수 있습니다.

GTP 검사 프로파일 설정	
GTP 검사	

GTP-C	• 방화벽이 **GTPv1-C** 또는 **GTPv2-C** 또는 둘 다를 검사하도록 하려면 상태 기반 검사를 선택합니다. 상태 기반 검사를 활성화하면 방화벽은 원본 IP, 원본 포트, 대상 IP, 대상 포트, 프로토콜 및 TEID(Tunnel Endpoint ID)를 사용하여 GTP 세션을 추적합니다. 또한 GTP 터널을 설정하는 데 사용되는 다양한 유형의 GTP 메시지 순서를 확인하고 유효성을 검사합니다. TEID는 GSN 터널 엔드포인트를 고유하게 식별합니다. 업링크와 다운링크에 대한 터널은 별개이며 다른 TEID를 사용합니다.
	• 방화벽이 유효성 검사 실패 시 수행할 작업(차단 또는 경고)을 선택합니다. 경고 작업은 트래픽을 허용하지만 로그를 생성합니다. 차단 작업은 트래픽을 거부하고 로그를 생성합니다.
	• 방화벽이 페이로드의 GTP 헤더 및 IE(정보 요소)에 대해 수행해야 하는 유효성 검사를 지정합니다. 방화벽은 오류 처리를 위해 아래에서 선택한 차단 또는 경고 작업을 사용합니다. 다음을 확인하도록 방화벽 구성 가능:
	  • 예약된 **IE** - 예약된 IE 값을 사용하는 GTPv1-C 또는 GTPv2-C 메시지를 확인합니다.
	  • **IE** 순서(GTPv1-C만 해당) - GTPv1-C 메시지의 IE 순서가 정확한지 확인합니다.
	  • **IE** 길이 - IE 길이가 잘못된 GTPv1-C 또는 GTPv2-C 메시지를 확인합니다.
	  • 헤더의 예약 필드 - 헤더에 잘못된 값이나 예약된 값을 사용하는 잘못된 패킷이 있는지 확인합니다.
	  • 지원되지 않는 메시지 유형 - 알 수 없거나 잘못된 메시지 유형이 있는지 확인합니다.

GTP 검사 프로파일 설정	
GTP-U	GTPv1-C 및/또는 GTPv2-C에 대한 상태 저장 검사를 활성화하면 GTPU-U 상태 저장 검사가 자동으로 활성화됩니다. GTP-U 페이로드에 대해 다음 유효성 검사를 지정할 수 있습니다. • 예약된 **IE** - 페이로드에서 예약된 IE 값을 사용하는 GTP-U 메시지를 확인합니다. • **IE** 순서 - GTP-U 메시지의 IE 순서가 올바른지 확인합니다. • **IE** 길이 - 잘못된 IE 길이가 있는 메시지를 확인합니다. • 헤더의 예비 플래그 - 헤더에 잘못된 값이나 예약된 값을 사용하는 잘못된 패킷이 있는지 확인합니다. • 지원되지 않는 메시지 유형 - 알 수 없거나 잘못된 메시지 유형이 있는지 확인합니다. 또한 다음에 대한 허용, 차단 또는 경고 작업을 구성할 수도 있습니다. • 최종 사용자 **IP** 주소 스푸핑 - 사용자(가입자) 장비의 GTP-U 패킷에 있는 소스 IP 주소가 터널 설정 중에 교환된 해당 GTP-C 메시지의 IP 주소와 같지 않을 때 차단하거나 경고하도록 방화벽을 구성합니다. *PFCP* 상태 저장 검사를 활성화하면 이 옵션을 사용할 수 없습니다. • **GTP-in-GTP** - GTP-in-GTP 메시지를 감지하면 차단하거나 경고하도록 방화벽을 구성할 수 있습니다. 탐지 시 방화벽은 심각도가 심각한 GTP 로그를 생성합니다. • **GTP-U** 세션 시작 시 기록 - GTP-U 세션 시작 시 GTP 로그에 연결된 IP 주소 및 터널 엔드포인트 ID를 기록합니다. • **GTP-U** 세션 종료 시 기록 - GTP-U 세션 종료 시 GTP 로그에 연결된 IP 주소 및 터널 엔드포인트 ID를 기록합니다. • 4G 및 3G의 경우 **GTP-U** 콘텐츠 검사를 활성화하여 GTP-U 패킷 내의 사용자 데이터 페이로드를 검사하고 정책을 적용합니다. GTP-U 콘텐츠를 검사하면 GTP-C 메시지에서 학습한 IMSI 및 IMEI 정보를 GTP-U 패킷에 캡슐화된 IP 트래픽과 연관시킬 수 있습니다.
5G-C	5G의 경우 **5G-HTTP2**를 활성화하여 가입자 ID, 장비 ID 및 네트워크 슬라이스 정보를 포함할 수 있는 5G HTTP/2 제어 패킷의 검사를 활성화합니다. 이를 통해 HTTP/2 메시지에서 학습한 가입자 ID(IMSI), 장비 ID(IMEI) 및 네트워크 슬라이스 ID 정보를 GTP-U 패킷에 캡슐화된 IP 트래픽과 연동시킬 수 있습니다. **5G-HTTP2**를 활성화하면 프로파일에 대해 GTP-C가 비활성화됩니다.

GTP 검사 프로파일 설정	
PFCP	PFCP(패킷 포워딩 제어 프로토콜)의 경우 상태 기반 검사를 활성화하여 PFCP 트래픽을 검사합니다. PFCP 트래픽에 대한 상태 저장 검사를 활성화하면 방화벽이 MEC와 원격 또는 중앙 사이트 간의 트래픽을 검사하여 서비스 거부(DOS) 또는 스푸핑과 같은 공격을 방지하는 데 도움이 됩니다. 이 옵션을 활성화하면 *GTP-U* 최종 사용자 *IP* 주소 스푸핑에 대한 작업을 사용할 수 없습니다. 다음 상태 확인을 지정할 수 있습니다. • 연결 메시지 확인 - 순서가 잘못되었거나 거부된 PFCP 연결 메시지를 확인합니다. • 세션 메시지 확인 - 순서가 잘못되었거나 거부된 PFCP 세션 메시지를 확인합니다. • 시퀀스 번호 확인 - PFCP의 시퀀스 번호가 PFCP 요청 메시지의 시퀀스 번호와 일치하는지 확인합니다. 그런 다음 검사가 실패할 때 방화벽이 수행할 작업(허용, 경고 또는 차단)을 지정할 수 있습니다. 방화벽이 PFCP 연결 또는 세션의 시작 또는 끝에서 로그를 생성하도록 할지의 여부를 선택할 수도 있습니다.
상관 관계	
UEIP 상관관계	GTP-U 콘텐츠 검사를 위해 가입자 ID와 장비 ID를 사용자 장비(UE) IP 기반 트래픽과 연관시킬 수 있습니다.
모드	• 완화 - (기본값) 방화벽이 GTP-U 내부 트래픽을 감지하면 상관 IMEI 또는 IMSI 정보를 찾기 위해 소스 또는 대상 주소를 쿼리합니다. 결과가 없으면 방화벽이 트래픽을 전달합니다. • 엄격 - GTP-U 쿼리가 결과를 반환하지 않는 경우 트래픽을 삭제합니다.
원천	정보를 상호 연관시키는 데 사용할 소스를 선택합니다. *CUPS*를 사용하여 배포하려면 *PFCP*를 선택합니다.
UEIP 시작 시 기록	방화벽이 UE에 IP 주소를 할당할 때 UEIP 상관 관계 이벤트를 기록합니다.
UEIP 종료 시 기록	방화벽이 할당된 IP 주소를 해제할 때 UEIP 상관 관계 이벤트를 기록합니다.

GTP 검사 프로파일 설정	
필터링 옵션	
RAT 필터링	기본적으로 모든 RAT(무선 액세스 기술)가 허용됩니다. GTP-C Create-PDP-Request 및 Create-Session-Request 메시지는 RAT 필터를 기반으로 필터링되거나 허용됩니다. 사용자 장비가 모바일 코어 네트워크에 액세스하는 데 사용하는 다음 RAT에 대해 허용, 차단 또는 경고할지의 여부를 지정할 수 있습니다. • **UTRAN** • **GERAN** • **WLAN** • **GAN** • **HSPA Evolution** • **EUTRAN** • **Virtual** • **EUTRAN-NB-IoT** • **LTE-M** • **NR** **5G-HTTP2**를 활성화할 때 다음 RAT를 사용할 수 있습니다. • **WLAN** • **EUTRAN** • **Virtual** • **NR**
IMSI 필터링	IMSI(International Mobile Subscriber Identity)는 SIM(Subscriber Identity Module) 카드에 제공되는 GSM, UMTS 및 LTE 네트워크의 가입자와 관련된 고유 ID입니다. IMSI는 일반적으로 15자리 숫자(8바이트)로 표시되지만 더 짧을 수도 있습니다. IMSI는 세 부분으로 구성됩니다. • 3자리 숫자로 구성된 모바일 국가 코드(MCC)입니다. MCC는 모바일 가입자의 주소 국가를 고유하게 식별합니다. • 2자리 또는 3자리로 구성된 모바일 네트워크 코드(MNC), 2자리 유럽 표준 또는 3자리 북미 표준. MNC는 모바일 가입자의 홈 PLMN을 식별합니다.

GTP 검사 프로파일 설정	
	• PLMN 내에서 모바일 가입자를 식별하는 MSIN(모바일 가입자 식별 번호). **IMSI** 프리픽스는 MCC와 MNC를 결합하여 특정 PLMN의 GTP 트래픽을 허용, 차단 또는 경고할 수 있습니다. 기본적으로 모든 IMSI가 허용됩니다. IMSI 또는 IMSI 프리픽스가 있는 CSV 파일을 수동으로 입력하거나 방화벽으로 가져올 수 있습니다. IMSI는 와일드카드를 포함할 수 있습니다(예: 310* 또는 240011*). 방화벽은 최대 5,000개의 IMSI 또는 IMSI 프리픽스를 지원합니다.
APN 필터링	APN(액세스 포인트 이름)은 사용자 장비가 인터넷에 연결하는 데 필요한 GGSN/PGW에 대한 참조입니다. 5G에서 데이터 네트워크 이름(DNN)의 한 형식은 APN입니다. APN은 하나 또는 두 개의 식별자로 구성됩니다. • GGSN/PGW가 연결된 외부 네트워크와 선택적으로 이동국에서 요청한 서비스를 정의하는 APN 네트워크 식별자입니다. APN의 이 부분은 필수입니다. • GGSN/PGW가 있는 PLMN GPRS/EPS 백본(backbone)을 정의하는 APN 운영자 식별자입니다. APN의 이 부분은 선택 사항입니다. 모든 APN은 기본적으로 허용됩니다. APN 필터를 사용하면 APN 값을 기반으로 GTP 트래픽을 허용, 차단 또는 경고할 수 있습니다. GTP-C Create-PDP-Request 및 Create-Session-Request 메시지는 APN 필터링에 대해 정의된 규칙에 따라 필터링되거나 허용됩니다. APN 필터링 목록을 방화벽에 수동으로 추가하거나 가져올 수 있습니다. APN의 값에는 네트워크 ID 또는 네트워크의 도메인 이름(예: example.com)이 포함되어야 하며 선택적으로 운영자 ID도 포함되어야 합니다. APN 필터링의 경우 와일드카드 '*'를 사용하면 모든 APN에 대해 일치시킬 수 있습니다. 와일드카드에는 '*' 및 기타 문자 조합이 지원되지 않습니다. 예를 들어 "internet.mnc*"는 일반 APN으로 처리되며 Internet.mnc로 시작하는 모든 항목을 필터링하지 않습니다. 방화벽은 최대 1,000개의 APN 필터를 지원합니다.
GTP 터널 제한	
대상별 허용되는 최대 동시 터널	GTP-U 터널의 최대 수를 대상 IP 주소(예: GGSN)로 제한할 수 있습니다(범위는 0 ~ 100,000,000 터널).

GTP 검사 프로파일 설정	
대상별 최대 동시 터널 경고	대상에 대한 최대 GTP-U 터널 수가 설정되었을 때 방화벽이 경고를 트리거하는 임계값을 지정합니다. 구성된 터널 제한에 도달하면 심각도가 높은 GTP 로그 메시지가 생성됩니다.
로깅 빈도	구성된 GTP 터널 제한이 초과된 경우 방화벽이 로그를 생성하기 전에 계산하는 이벤트 수입니다. 이 설정을 사용하면 기록된 메시지의 볼륨을 줄일 수 있습니다(범위는 0~100,000,000, 기본값은 100).
초과 청구 보호	방화벽에서 Gi/SGi 방화벽 역할을 하는 가상 시스템을 선택합니다. Gi/SGi 방화벽은 Gi/SGi 인터페이스를 통해 PGW/GGSN에서 인터넷과 같은 외부 PDN(패킷 데이터 네트워크)으로 이동하는 모바일 가입자 IP 트래픽을 검사하고 모바일 가입자의 인터넷 액세스를 보호합니다. 초과 청구는 GGSN이 최종 사용자 IP 주소 풀에서 이전에 사용한 IP 주소를 모바일 가입자에게 할당할 때 발생할 수 있습니다. 인터넷의 악의적인 서버가 이전 가입자에 대해 시작된 세션을 닫지 않고 Gi 방화벽에서 세션이 여전히 열려 있기 때문에 이 IP 주소로 패킷을 계속 보낼 때. 데이터 전달을 허용하지 않기 위해 GTP 터널이 삭제되거나(delete-PDP 또는 delete-session 메시지에 의해 감지됨) 시간 초과될 때마다 초과 청구 보호가 활성화된 방화벽이 세션 테이블에서 가입자에게 속한 모든 세션을 삭제하도록 Gi/SGi 방화벽에 알립니다. GTP Security 및 SGi/Gi 방화벽은 동일한 물리적 방화벽에 구성해야 하지만 다른 가상 시스템에 있을 수 있습니다. GTP-C 이벤트를 기반으로 세션을 삭제하려면 방화벽에 모든 관련 세션 정보가 있어야 하며 이는 모바일 코어 네트워크에서 GTPv2용 SGi + S11 또는 S5 인터페이스 및 GTPv1용 Gi + Gn 인터페이스에서 트래픽을 관리하는 경우에만 가능합니다.
기타 로그 설정 기본적으로 방화벽은 허용된 GTP 또는 PFCP 메시지를 기록하지 않습니다. 많은 양의 로그를 생성하므로 필요할 때 문제 해결을 위해 허용된 GTP 및 PFCP 메시지의 로깅을 선택적으로 활성화할 수 있습니다. 허용된 로그 메시지 외에도 이 탭에서는 사용자 위치 정보의 로깅을 선택적으로 활성화할 수 있습니다.	
GTPv1-C 허용 메시지	GTPv1?C에 대한 상태 저장 검사를 활성화한 경우 허용된 GTPv1-C 메시지의 로깅을 선택적으로 활성화할 수 있습니다. 이러한 메시지는 필요에 따라 문제를 해결하는 데 도움이 되는 로그를 생성합니다. 기본적으로 방화벽은 허용된 메시지를 기록하지 않습니다. 허용된 GTPv1-C 메시지에 대한 로깅 옵션은 다음과 같습니다. • 터널 관리 - 이러한 GTPv1-C 메시지는 SGSN 및 GGSN과 같은 주어진 네트워크 노드 쌍 간에 캡슐화된 IP 패킷 및 신호 메시지를 전달하는 GTP-U 터널을 관리하는 데 사용됩니다. 여기에는 Create PDP Context

GTP 검사 프로파일 설정	
	Request, Create PDP Context Response, Update PDP Context Request, Update PDP Context Response, Delete PDP Context Request, Delete PDP Context Response와 같은 메시지가 포함됩니다. • 경로 관리 - 이러한 GTPv1-C 메시지는 일반적으로 GSN 또는 RNC(Radio Network Controller)에서 피어가 활성 상태인지 확인하기 위해 다른 GSN 또는 RNC로 전송됩니다. 여기에는 에코 요청 및 에코 응답과 같은 메시지가 포함됩니다. • 기타 - 이러한 메시지에는 위치 관리, 이동성 관리, RAN 정보 관리 및 MBMS(Multimedia Broadcast Multicast Service) 메시지가 포함됩니다.
사용자 위치 기록	GTP 로그에 지역 번호 및 셀 ID와 같은 사용자 위치 정보를 포함할 수 있습니다.
패킷 캡처	GTP 이벤트를 캡처할 수 있습니다.
GTPv2-C 허용 메시지	GTPv2-C에 대한 상태 저장 검사를 활성화한 경우 허용된 GTPv2-C 메시지의 로깅을 선택적으로 활성화할 수 있습니다. 이러한 메시지는 필요에 따라 문제를 해결하는 데 도움이 되는 로그를 생성합니다. 기본적으로 방화벽은 허용된 메시지를 기록하지 않습니다. 허용된 GTPv2-C 메시지에 대한 로깅 옵션은 다음과 같습니다. • 터널 관리 - 이러한 GTPv2-C 메시지는 SGW 및 PGW와 같은 주어진 네트워크 노드 쌍 간에 캡슐화된 IP 패킷 및 신호 메시지를 전달하는 GTP-U 터널을 관리하는 데 사용됩니다. 여기에는 다음 유형의 메시지가 포함됩니다. 세션 요청 생성, 세션 응답 생성, 베어러 요청 생성, 베어러 응답 생성, 베어러 요청 수정, 베어러 응답 수정, 세션 요청 삭제 및 세션 응답 삭제. • 경로 관리 - 이러한 GTPv2-C 메시지는 일반적으로 SGW 또는 PGW와 같은 네트워크 노드에서 다른 PGW로 전송되어 피어가 살아 있는지 확인합니다. 여기에는 에코 요청 및 에코 응답과 같은 메시지가 포함됩니다. • 기타 - 이러한 메시지에는 이동성 관리 및 비 3GPP 액세스 관련 메시지가 포함됩니다.
GTP-U 허용 메시지	GTPv2-C 또는 GTPv1-C에 대한 상태 저장 검사를 활성화한 경우 허용된 GTP-U 메시지의 로깅을 선택적으로 활성화할 수 있습니다. 이러한 메시지는 필요에 따라 문제를 해결하는 데 도움이 되는 로그를 생성합니다. 허용된 GTP-U 메시지에 대한 로깅 옵션은 다음과 같습니다. • 터널 관리 - 오류 표시와 같은 GTP-U 신호 메시지입니다.

GTP 검사 프로파일 설정	
	• 경로 관리 - 이러한 GTP-U 메시지는 피어가 활성 상태인지 확인하기 위해 네트워크 노드(예: eNodeB)에서 다른 네트워크 노드(예: SGW)로 전송됩니다. 에코 요청/응답과 같은 메시지가 포함됩니다. • **G-PDU** - G-PDU(GTP-U PDU)는 모바일 코어 네트워크의 네트워크 노드 내에서 사용자 데이터 패킷을 운반하는 데 사용됩니다. GTP 헤더와 T-PDU로 구성됩니다.
새 GTP-U 터널당 기록된 G-PDU 패킷	방화벽이 GTP-U PDU를 검사하는지 확인하려면 이 옵션을 활성화합니다. 방화벽은 각각의 새로운 GTP-U 터널에서 지정된 수의 G-PDU 패킷에 대한 로그를 생성합니다(범위는 1~10, 기본값은 1).
5G-C 허용 메시지	허용된 **N11** 메시지의 로깅을 선택적으로 활성화하려면 N11을 선택합니다. N11 메시지는 문제 해결에 도움이 되며 다양한 절차를 위해 N11 인터페이스를 통해 교환되는 HTTP/2 메시지에 대한 더 깊은 가시성을 제공합니다. 이 필드는 모바일 네트워크 보호 프로파일의 **5G-C** 탭에서 **5G-HTTP2**를 활성화한 경우에만 사용할 수 있습니다.
PFCP 허용 메시지	PFCP에 대한 상태 저장 검사를 활성화한 경우 허용된 PFCP 메시지의 로깅을 선택적으로 활성화할 수 있습니다. 이러한 메시지는 필요에 따라 문제를 해결하는 데 도움이 되는 로그를 생성합니다. 허용된 PFCP 메시지에 대한 로깅 옵션은 다음과 같습니다. • 세션 설정 - 이 PFCP 메시지는 GTP-U 터널 설정을 포함하여 세션을 설정합니다. • 세션 수정 - 이러한 PFCP 메시지는 세션 ID 또는 PDR ID가 변경되는 경우(예: 4G에서 5G 네트워크로 이동한 결과) 전송됩니다. 여기에는 PFCP 세션 수정 요청 및 PFCP 세션 수정 응답과 같은 메시지가 포함됩니다. • 세션 삭제 - 이러한 PFCP 메시지는 관련 리소스 해제를 포함하여 PFCP 세션을 종료합니다.

개체 > 보안 프로파일 > SCTP 보호

SCTP(Stream Control Transmission Protocol) 보호 프로파일을 만들어 방화벽이 SCTP 청크를 확인하고 필터링하는 방법을 지정합니다. 보안 프로파일에서 이 프로파일 유형을 보려면 먼저 SCTP 보안(**Device** > **Setup** > **Management** > **General Settings**)을 활성화해야 합니다. 또한 멀티홈 환경에서 SCTP 엔드포인트당 IP 주소 수를 제한할 수 있으며 방화벽이 SCTP 이벤트를 기록하는 시기를 지정할 수 있습니다. SCTP 보호 프로파일을 만든 후 영역에 대한 보안 정책 규칙에 프로파일을 적용해야 합니다.

SCTP 보안을 지원하는 방화벽 모델에는 사전 정의된 SCTP 보호 프로파일(*default-ss7*)이 있어 그대로 사용하거나 default-ss7 프로파일을 새 SCTP 보호 프로파일의 기반으로 복사할 수 있습니다. 개체 > 보안 프로파일 > **SCTP** 보호를 선택한 다음 **default-ss7**을 선택하여 이 사전 정의된 프로파일에 대한 경고를 발생시키는 작업 코드를 확인합니다.

SCTP 보호 프로파일 설정	
이름	SCTP 보호 프로파일의 이름을 입력합니다.
설명	SCTP 보호 프로파일에 대한 설명을 입력합니다.
SCTP 검사	
알 수 없는 청크	알 수 없는 청크가 있는 SCTP 패킷을 수신할 때 방화벽 작업을 선택합니다(청크는 RFC3758, RFC4820, RFC4895, RFC4960, RFC5061 또는 RFC 6525에 정의되어 있지 않음). • 허용(기본값) - 패킷이 수정 없이 전달되도록 허용합니다. • **alert** - 패킷이 수정 없이 전달되고 SCTP 로그를 생성하도록 허용합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정 아래의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리). • 차단 - 패킷을 전달하기 전에 청크를 무효화하고 SCTP 로그를 생성합니다.
청크 플래그	RFC4960과 일치하지 않는 청크 플래그가 있는 SCTP 패킷을 수신할 때 방화벽 작업을 선택합니다. • 허용(기본값) - 패킷이 수정 없이 전달되도록 허용합니다. • **alert** - 패킷이 수정 없이 전달되고 SCTP 로그를 생성하도록 허용합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정 아래의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리). • 차단 - 패킷을 삭제하고 SCTP 로그를 생성합니다.
잘못된 길이	길이가 잘못된 SCTP 청크를 수신할 때 방화벽 작업을 선택합니다.

SCTP 보호 프로파일 설정	
	• 허용(기본값) - 패킷 또는 청크가 수정 없이 전달되도록 허용합니다. • 차단 - 패킷을 삭제하고 SCTP 로그를 생성합니다(이러한 로그에 대한 로그 저장소를 할당해야 합니다. 로그 저장소 탭 참조).
멀티호밍에 대한 IP 주소 제한	방화벽이 경고 메시지를 생성하기 전에 SCTP 엔드포인트에 대해 구성할 수 있는 최대 IP 주소 수를 입력합니다(범위는 1~8, 기본값은 4). SCTP 멀티호밍은 엔드포인트가 피어와의 연결을 위해 둘 이상의 IP 주소를 지원하는 기능입니다. 엔드포인트에 대한 한 경로가 실패하면 SCTP는 해당 연결에 제공된 다른 대상 IP 주소 중 하나를 선택합니다.
로그 설정	허용된 청크, 연결 시작 및 종료, 상태 실패 이벤트에 대한 SCTP 로그를 생성하려면 설정 조합을 선택합니다. • 연결 시작 시 로그인 • 연결 종료 시 로그인 • 허용된 연결 초기화 청크 기록 • 허용된 하트비트 청크 기록 • 허용된 연결 종료 청크 기록 • 모든 제어 청크 기록 • 로그 상태 실패 이벤트 방화벽이 SCTP 로그를 저장하려면 SCTP 로그 저장소를 할당해야 합니다(로깅 및 보고 설정 아래의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리).
필터링 옵션	
SCTP 필터링	
이름	SCTP 필터의 이름을 입력합니다.
PPID	SCTP 필터에 대한 PPID를 지정합니다. • **any** - 방화벽이 PPID를 포함하는 모든 SCTP 데이터 청크에 대해 지정한 작업을 수행합니다. • **3GPP PUA** • **3GPP RNA**

SCTP 보호 프로파일 설정	
	• **LCS-AP** • **M2PA** • **M2UA** • **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • 유효한 PPID 값(드롭다운에 없는 값)을 입력합니다. 예를 들어 H.323의 PPID 값은 13입니다. 각 SCTP 필터는 하나의 PPID만 지정할 수 있지만 SCTP 보호 프로파일에 대해 여러 SCTP 필터를 지정할 수 있습니다.
작업	방화벽이 지정된 PPID를 포함하는 데이터 청크에 대해 수행하는 작업을 지정합니다. • 허용(기본값) - 청크가 수정 없이 전달되도록 허용합니다. • 경고 - 청크가 수정 없이 전달되고 SCTP 로그를 생성하도록 허용합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리). • 차단 - 패킷을 전달하기 전에 청크를 무효화하고 SCTP 로그를 생성합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정 아래의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리).
SCTP 패킷은 위에서 아래로 목록의 필터와 일치합니다. 프로파일에 대해 SCTP 필터를 두 개 이상 만드는 경우 SCTP 필터의 순서가 달라집니다. 필터를 선택한 다음 위로 이동 또는 아래로 이동하여 SCTP 필터링 목록에서 상대적 우선 순위를 변경합니다.	
다이어미터 필터링	
이름	다이어미터 필터의 이름을 입력합니다.
작업	방화벽이 지정된 다이어미터 애플리케이션 ID, 명령 코드 및 AVP를 포함하는 다이어미터 청크에 대해 수행하는 작업을 지정합니다. 검

SCTP 보호 프로파일 설정	
	사된 청크가 지정된 다이어미터 애플리케이션 ID와 지정된 다이어미터 명령 코드 및 지정된 다이어미터 AVP를 포함하는 경우: • 허용(기본값) - 청크가 수정 없이 전달되도록 허용합니다. • 경고 - 청크가 수정 없이 전달되고 SCTP 로그를 생성하도록 허용합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리). • 차단 - 패킷을 전달하기 전에 청크를 무효화하고 SCTP 로그를 생성합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정 아래의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리).
다이어미터 애플리케이션 ID	방화벽이 지정된 작업을 수행하는 청크에 대한 다이어미터 애플리케이션 ID를 지정합니다. • 모두 • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • 다이어미터 기준 회계 • 다이어미터 공통 메시지 • 다이어미터 신용 관리 또는 다이어미터 애플리케이션 ID의 숫자 값을 입력할 수 있습니다(범위는 0에서 4,294,967,295 사이). 다이어미터 필터에는 애플리케이션 ID가 하나만 있을 수 있습니다.
다이어미터 명령 코드	방화벽이 지정된 작업을 수행하는 청크에 대한 다이어미터 명령 코드를 지정합니다. 모두를 선택하거나 드롭다운에서 다이어미터 명령 코드 중 하나를 선택하거나 특정 값을 입력합니다(범위는 0 ~ 16,777,215). 드롭다운에는 선택한 다이어미터 애플리케이션 ID에 적용되는 명령 코드만 포함됩니다. 다이어미터 필터에 여러 다이어미터 명령 코드를 추가할 수 있습니다.

SCTP 보호 프로파일 설정	
다이어미터 AVP	방화벽이 지정된 작업을 수행하는 청크에 대한 AVP(다이어미터 속성-값 쌍) 코드를 지정합니다. 하나 이상의 AVP 코드 또는 값을 입력하십시오(범위는 1에서 16,777,215까지).
프로파일에 대해 둘 이상의 다이어미터 필터를 생성하는 경우 다이어미터 필터의 순서가 달라집니다. 필터를 선택한 다음 위로 이동 또는 아래로 이동하여 다이어미터 필터링 목록에서 상대적 우선 순위를 조정합니다.	
SS7 필터링	
이름	SS7 필터의 이름을 입력합니다.
작업	방화벽이 지정된 SS7 필터 요소를 포함하는 SS7 청크에 대해 수행하는 작업을 지정합니다. 검사 중인 청크에 SCCP 발신자 SSN과 지정된 SCCP 발신자 전체 제목(GT) 값 및 지정된 작업 코드가 포함되어 있으면 다음을 수행합니다. • 허용(기본값) - 청크가 수정 없이 전달되도록 허용합니다. • 경고 - 청크가 수정 없이 전달되고 SCTP 로그를 생성하도록 허용합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리). • 차단 - 패킷을 전달하기 전에 청크를 무효화하고 SCTP 로그를 생성합니다(이러한 로그에 대한 로그 저장소를 할당해야 함 - 로깅 및 보고 설정 아래의 로그 저장소 탭 참조: 디바이스 > 설정 > 관리).
SCCP 발신자 SSN	방화벽이 지정된 작업을 수행하는 청크에 대한 SCCP 발신자 SSN을 지정합니다. 모든 맵을 선택하거나 드롭다운에서 SCCP 발신자 SSN 중 하나를 추가합니다. • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)**

SCTP 보호 프로파일 설정	
	• **CSS(MAP)** • **CAP** • **INAP** • **SCCP** 관리 SS7 필터에는 SCCP 발신자 SSN이 하나만 있을 수 있습니다.
SCCP 발신자 GT	방화벽이 지정된 작업을 수행하는 청크에 대한 SCCP 발신자 GT 값을 지정합니다. 임의 또는 최대 15자리 숫자 값 추가를 선택합니다. 프리픽스를 사용하여 SCCP 발신자 GT 값 그룹을 입력할 수도 있습니다. 예: 876534*. SS7 필터에 여러 SCCP 발신자 GT 값을 추가할 수 있습니다. SCCP 발신자 SSN의 경우: **INAP** 및 **SCCP** 관리, 이 옵션은 비활성화됩니다.
작업 코드	방화벽이 지정된 작업을 수행하는 청크에 대한 작업 코드를 지정합니다. 다음 SCCP 발신자 SSN의 경우 모두를 선택하거나 드롭다운에서 작업 코드를 선택하거나 특정 값을 입력합니다(범위는 1~255). • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** SCCP 발신자 SSN의 경우: **CAP**, 값을 입력합니다(범위는 1~255). SCCP 발신자 SSN의 경우: **INAP** 및 **SCCP** 관리, 이 옵션은 비활성화됩니다. SS7 필터에 여러 작업 코드를 추가할 수 있습니다.

SCTP 보호 프로파일 설정
프로파일에 대해 둘 이상의 SS7 필터를 생성하는 경우 SS7 필터의 순서가 달라집니다. 필터를 선택한 다음 위로 이동 또는 아래로 이동하여 SS7 필터링 목록에서 상대적 우선 순위를 조정합니다.

개체 > 보안 프로파일 그룹

방화벽은 하나의 단위로 처리된 다음 보안 정책에 추가할 수 있는 보안 프로파일 집합을 지정하는 보안 프로파일 그룹을 만드는 기능을 지원합니다. 예를 들어 안티바이러스, 안티스파이웨어 및 취약성 보호에 대한 프로파일을 포함하는 위협 보안 프로파일 그룹을 생성한 다음 위협 프로파일을 포함하는 보안 정책 규칙을 생성할 수 있습니다.

종종 함께 할당되는 바이러스 백신, 안티 스파이웨어, 취약성 보호, URL 필터링 및 파일 차단 프로파일을 프로파일 그룹으로 결합하여 보안 정책 생성을 단순화할 수 있습니다.

새 보안 프로파일을 정의하려면 개체 > 보안 프로파일을 선택합니다.

다음 표에서는 보안 프로파일 설정에 대해 설명합니다.

보안 프로파일 그룹 설정	설명
이름	프로파일 그룹 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의할 때 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유(Panorama만 해당)	프로파일 그룹을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 프로파일 그룹은 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일 그룹은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 보안 프로파일 그룹 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
프로파일	이 그룹에 포함할 바이러스 백신, 안티 스파이웨어, 취약점 보호, URL 필터링 및/또는 파일 차단 프로파일을 선택합니다. 데이터 필터링 프로파일은 보안 프로파일 그룹에서도 지정할 수 있습니다. 개체 > 보안 프로파일 > 데이터 필터링을 참조하십시오.

개체 > 로그 포워딩

기본적으로 방화벽이 생성하는 로그는 로컬 저장소에만 있습니다. 그러나 Panorama™, 로깅 서비스 또는 외부 서비스(예: syslog 서버)를 사용하여 로그 포워딩 프로파일을 정의하고 해당 프로파일을 보안, 인증, DoS 방어 및 터널 검사 정책 규칙에 할당하여 로그 정보를 중앙에서 모니터링할 수 있습니다. 로그 포워딩 프로파일은 다음 로그 유형에 대한 포워딩 대상을 정의합니다. 인증, 데이터 필터링, GTP, SCTP, 위협, 트래픽, 터널, URL 필터링 및 WildFire® 제출 로그.

규정 준수, 중복성, 분석 실행, 중앙 집중식 모니터링, 위협 동작 및 장기 패턴 검토를 비롯한 여러 가지 이유로 로그를 *Panorama* 또는 외부 저장소로 포워딩해야 합니다. 또한 방화벽은 로그 저장 용량이 제한되어 있어 저장 공간이 차면 가장 오래된 로그를 삭제합니다. 위협 로그 및 *WildFire* 로그를 포워딩해야 합니다.

다른 로그 유형을 포워딩하려면 디바이스 > 로그 설정을 참조하십시오.

PA-7000 시리즈 방화벽이 로그를 포워딩하거나 파일을 *WildFire*®로 포워딩하려면 먼저 *PA-7000* 시리즈 방화벽에서 로그 카드 인터페이스를 구성해야 합니다. 이 인터페이스를 구성하면 방화벽이 자동으로 이 포트를 사용하므로 특별한 구성이 필요하지 않습니다. *PA-7000* 시리즈 *NPC(*네트워크 처리 카드*)* 중 하나의 데이터 포트를 로그 카드 인터페이스 유형으로 구성하고 사용하는 네트워크가 로그 서버와 통신할 수 있는지 확인하십시오. *WildFire* 포워딩의 경우 네트워크는 *WildFire* 클라우드 또는 *WildFire* 어플라이언스*(*또는 둘 다*)*와 성공적으로 통신해야 합니다.

다음 표에서는 로그 포워딩 프로파일 설정에 대해 설명합니다.

로그 포워딩 프로파일 설정	설명
이름	프로파일을 식별할 이름(최대 64자)을 입력합니다. 이 이름은 보안 정책 규칙을 정의할 때 로그 포워딩 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • **Multi-VSYS** 방화벽의 모든 가상 시스템**(vsys)** - 이 옵션을 비활성화(선택 취소)하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다. • **Panorama**의 모든 디바이스 그룹 - 이 옵션을 비활성화(선택 취소)하면 개체 탭에서 선택한 디바이스 그룹에서만 프로파일을 사용할 수 있습니다.

로그 포워딩 프로파일 설정	설명
Cortex Data Lake에 대한 향상된 애플리케이션 로깅 활성화(트래픽 및 URL 로그 포함)(Panorama 전용)	Palo Alto Networks Cloud Services의 향상된 애플리케이션 로그는 Cortex Data Lake 구독으로 사용할 수 있습니다. 향상된 애플리케이션 로깅을 통해 방화벽은 Palo Alto Networks Cloud Services 환경에서 실행되는 앱의 네트워크 활동에 대한 가시성을 높이기 위해 특별히 데이터를 수집할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 로그 포워딩 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 비활성화(선택 취소)되어 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
설명	이 로그 포워딩 프로파일의 목적을 설명하는 설명을 입력합니다.
일치 목록(레이블 없음)	포워딩 대상을 지정하는 하나 이상의 일치 목록 프로파일(최대 64개), 방화벽이 포워딩할 로그를 제어하는 로그 속성 기반 필터, 로그에서 수행할 작업(예: 자동 태그 지정)을 추가합니다. 각 일치 목록 프로파일에 대해 다음 두 필드(이름 및 설명)를 완료합니다.
이름(일치 목록 프로파일)	일치 목록 프로파일을 식별할 이름(최대 31자)을 입력합니다.
설명(일치 목록 프로파일)	이 일치 목록 프로파일의 목적을 설명하는 설명(최대 1,023자)을 입력합니다.
로그 유형	이 일치 목록 프로파일이 적용되는 로그 유형(인증(**auth**), 데이터, **gtp**, **sctp**, 위협, 트래픽, 터널, **URL** 또는 **WildFire**)을 선택합니다.
필터	기본적으로 방화벽은 선택한 로그 유형의 모든 로그를 포워딩합니다. 로그의 하위 집합을 포워딩하려면 드롭다운에서 기존 필터를 선택하거나 필터 빌더를 선택하여 새 필터를 추가합니다. 새 필터의 각 쿼리에 대해 다음 필드를 지정하고 쿼리를 추가합니다. • 커넥터 - 쿼리에 대한 커넥터 논리(및/또는)를 선택합니다. 논리에 부정을 적용하려면 부정을 선택합니다. 예를 들어, 신뢰할 수 없는 영역에서 로그를 포워딩하지 않으려면 무효를 선택한 다음 속성으로 영역을 선택하고 연산자로 같음을 선택한 다음 값 열에 신뢰할 수 없는 영역의 이름을 입력합니다. • 속성 - 로그 속성을 선택합니다. 사용 가능한 속성은 로그 유형에 따라 다릅니다. • 연산자 - 속성 적용 여부(예: 같음)를 결정하는 기준을 선택합니다. 사용 가능한 기준은 로그 유형에 따라 다릅니다. • 값 - 일치시킬 속성 값을 지정합니다.

로그 포워딩 프로파일 설정	설명
	필터와 일치하는 로그를 표시하거나 내보내려면 모니터링 탭 페이지와 동일한 옵션(예: **Monitoring** > **Logs** > 트래픽)을 제공하는 **View Filtered Logs**(필터링된 로그 보기)를 참조하십시오.
Panorama Panorama/로깅 서비스(Panorama 전용)	로그를 Log Collectors 또는 Panorama 관리 서버로 포워딩하거나 Logging Service로 로그를 포워딩하려면 **Panorama**를 선택합니다. 이 옵션을 활성화하면 Panorama로의 로그 포워딩을 구성해야 합니다. 로깅 서비스를 사용하려면 디바이스 > 설정 > 관리에서도 로깅 서비스를 활성화해야 합니다.
SNMP	SNMP 트랩으로 로그를 포워딩하려면 하나 이상의 SNMP 트랩 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > SNMP 트랩 참조).
이메일	이메일 알림으로 로그를 포워딩하려면 하나 이상의 이메일 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > 이메일 참조).
Syslog	하나 이상의 Syslog 서버 프로파일을 추가하여 로그를 syslog 메시지로 포워딩합니다(디바이스 > 서버 프로파일 > Syslog 참조).
HTTP	HTTP 요청으로 로그를 포워딩하려면 하나 이상의 HTTP 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > HTTP 참조).
기본 제공 작업	수행할 작업을 추가할 때 두 가지 유형의 기본 제공 작업인 태그 지정 및 통합 중에서 선택할 수 있습니다. • 태깅 - 로그 항목의 소스 또는 대상 IP 주소에 태그를 자동으로 추가하거나 제거하고 방화벽이나 Panorama의 User-ID 에이전트 또는 원격 User-ID 에이전트에 IP 주소 및 태그 매핑을 등록하여 다음을 수행할 수 있습니다. 이벤트에 응답하고 보안 정책을 동적으로 시행할 수 있습니다. IP 주소에 태그를 지정하고 동적 주소 그룹을 사용하여 정책을 동적으로 시행하는 기능은 IP 주소가 네트워크에서 이동하는 위치에 관계없이 보안 정책을 일관되게 시행하기 위해 더 나은 가시성, 컨텍스트 및 제어를 제공합니다. 다음 설정을 구성합니다. • 작업을 추가하고 설명하는 이름을 입력합니다. • 태그를 지정할 대상 IP 주소(소스 주소 또는 대상 주소)를 선택합니다. 로그 항목에 소스 또는 대상 IP 주소를 포함하는 모든 로그 유형에 대해 조치를 취할 수 있습니다. 상관 로그 및 HIP 일치 로그에서 소스 IP 주소에만 태그를 지정할 수 있습니다. 로그 유형에는 로그 항목에 IP 주소가

로그 포워딩 프로파일 설정	설명
	포함되어 있지 않기 때문에 시스템 로그 및 구성 로그에 대한 작업을 구성할 수 없습니다. • 태그 추가 또는 태그 제거 작업을 선택합니다. • 이 방화벽이나 Panorama의 로컬 **User-ID** 에이전트 또는 원격 **User-ID** 에이전트에 IP 주소 및 태그 매핑을 등록할지의 여부를 선택합니다. • 원격 **User-ID** 에이전트에 IP 주소 및 태그 매핑을 등록하려면 포워딩을 활성화할 HTTP 서버 프로파일(디바이스 > 서버 프로파일 > HTTP)을 선택합니다. • IP 주소-태그 매핑이 유지되는 시간을 분 단위로 설정하도록 IP-태그 타임아웃을 구성합니다. 타임아웃을 0으로 설정하면 IP-태그 매핑이 타임아웃되지 않음을 의미합니다(범위는 0 ~ 43200(30일), 기본값은 0). 태그 추가 작업으로만 타임아웃을 구성할 수 있습니다. • 대상 소스 또는 대상 IP 주소에서 적용하거나 제거할 태그를 입력하거나 선택합니다. • 통합 - Azure의 VM 시리즈 방화벽에서만 사용할 수 있습니다. 이 옵션을 사용하면 **Azure-Security-Center-Integration** 작업을 사용하여 선택한 로그를 Azure Security Center로 포워딩할 수 있습니다. 로그 포워딩 프로파일 필터를 기반으로 디바이스를 분리 목록에 추가하려면 분리를 선택합니다.

개체 > 인증

인증 시행 개체는 네트워크 리소스에 액세스하는 최종 사용자를 인증하는 데 사용할 방법과 서비스를 지정합니다. 트래픽이 규칙과 일치할 때 인증 방법 및 서비스를 호출하는 인증 정책 규칙에 개체를 할당합니다(정책 > 인증 참조).

방화벽에는 다음과 같은 사전 정의된 읽기 전용 인증 시행 개체가 있습니다.

- **default-browser-challenge** - 방화벽이 명시적 사용자 인증 자격 증명을 얻습니다. 이 작업을 선택하면 인증 포털을 구성할 때 Kerberos SSO(Single Sign-On) 또는 NTLM(NT LAN Manager) 인증을 활성화해야 합니다. Kerberos SSO 인증이 실패하면 방화벽이 NTLM 인증으로 대체합니다. NTLM을 구성하지 않았거나 NTLM 인증이 실패하면 방화벽은 사전 정의된 **default-web-form** 개체에 지정된 인증 방법으로 대체합니다.
- **default-web-form** - 사용자를 인증하기 위해 방화벽은 인증 포털을 구성할 때 지정한 인증서 프로파일 또는 인증 프로파일을 사용합니다. 인증 프로파일을 지정한 경우 방화벽은 프로파일의 모든 Kerberos SSO 설정을 무시하고 사용자가 인증 자격 증명을 입력할 수 있도록 인증 포털 페이지를 표시합니다.
- **default-no-captive-portal** - 방화벽이 사용자를 인증하지 않고 보안 정책을 평가합니다.

사용자 지정 인증 적용 개체를 만들기 전:

- 인증 서비스에 연결하는 방법을 지정하는 서버 프로파일을 구성합니다(디바이스 > 서버 프로파일 참조).
- 서버 프로파일을 Kerberos Single Sign-On(SSO) 매개변수와 같은 인증 설정을 지정하는 인증 프로파일에 할당합니다(디바이스 > 인증 프로파일 참조).

사용자 지정 인증 적용 개체를 만들려면 추가를 클릭하고 다음 필드를 완성합니다.

인증 시행 설정	설명
이름	인증 규칙을 정의할 때 개체를 식별하는 데 도움이 되도록 설명이 포함된 이름(최대 31자)을 입력합니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유(Panorama만 해당)	개체를 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 개체를 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭에서 선택한 디바이스 그룹에서만 개체를 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	관리자가 개체를 상속하는 디바이스 그룹에서 이 인증 적용 개체의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취

인증 시행 설정	설명
	소되어 있으므로 관리자가 개체를 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
인증 방법	방법 선택: • **browser-challenge** - 방화벽이 명시적 사용자 인증 자격 증명을 얻습니다. 이 작업을 선택하면 선택한 인증 프로파일에 Kerberos SSO가 활성화되어 있어야 합니다. • **web-form** - 방화벽은 사용자를 인증하기 위해 인증 포털 구성 시 지정한 인증서 프로파일 또는 인증 시행 개체에서 선택한 인증 프로파일을 사용합니다. 인증 프로파일을 선택하면 방화벽은 프로파일의 모든 Kerberos SSO 설정을 무시하고 사용자가 인증 자격 증명을 입력할 수 있는 인증 포털 페이지를 표시합니다. • **no-captive-portal** - 방화벽이 사용자를 인증하지 않고 보안 정책을 평가합니다.
인증 프로파일	사용자의 ID를 검증하는 데 사용할 서비스를 지정하는 인증 프로파일을 선택하십시오.
메세지	트래픽이 인증 규칙을 트리거할 때 표시되는 첫 번째 인증 질문에 응답하는 방법을 사용자에게 알려주는 지침을 입력합니다. 메시지가 인증 포털 컴포트 페이지에 표시됩니다. 메시지를 입력하지 않으면 기본 인증 포털 편의 페이지가 표시됩니다(디바이스 > 응답 페이지 참조). 방화벽은 인증 프로파일의 인증 탭에서 정의한 첫 번째 인증 질문(요소)에 대해서만 인증 포털 편의 페이지를 표시합니다(디바이스 > 인증 프로파일 참조). 프로파일의 요소 탭에서 정의한 *MFA*(다단계 인증) 챌린지의 경우 방화벽이 ***MFA*** 로그인 페이지를 표시합니다.

개체 > 복호화 프로파일

복호화 프로파일을 사용하면 복호화를 위해 지정한 SSL 및 SSH 트래픽의 특정 측면과 복호화에서 명시적으로 제외한 트래픽을 차단하고 제어할 수 있습니다. 복호화 프로파일을 만든 후 복호화 정책에 해당 프로파일을 추가할 수 있습니다. 복호화 정책과 일치하는 모든 트래픽은 프로파일 설정에 따라 추가로 시행됩니다.

기본 복호화 프로파일은 방화벽에 구성되며 새 복호화 정책에 자동으로 포함됩니다(기본 복호화 프로파일은 수정할 수 없음). 추가를 클릭하여 새 복호화 프로파일을 생성하거나 기존 프로파일을 선택하여 복사 또는 수정합니다.

무엇을 찾고 계십니까?	참조:
새 복호화 프로파일을 추가합니다. 복호화된 트래픽에 대해 포트 미러링을 활성화합니다.	복호화 프로파일 일반 설정
SSL 복호화 트래픽을 차단하고 제어합니다.	복호화된 SSL 트래픽을 제어하기 위한 설정
복호화에서 제외된 트래픽(예: 건강 및 의료 또는 금융 서비스로 분류된 트래픽)을 차단하고 제어합니다.	복호화되지 않은 트래픽을 제어하기 위한 설정
복호화된 SSH 트래픽을 차단하고 제어합니다.	복호화된 SSH 트래픽을 제어하기 위한 설정

복호화 프로파일 일반 설정

다음 표에서는 복호화 프로파일에 대한 일반 설정을 설명합니다.

복호화 프로파일 - 일반 설정	설명
이름	프로파일 이름을 입력합니다(최대 **31**자). 이 이름은 복호화 정책을 정의할 때 복호화 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유(Panorama만 해당)	프로파일을 다음에 사용할 수 있게 하려면 이 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭에서 선택한 가상 시스템에서만 프로파일을 사용할 수 있습니다.

복호화 프로파일 - 일반 설정	설명
	• Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 프로파일은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama 전용)	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 복호화 프로파일의 설정을 무시하지 못하게 하려면 이 옵션을 선택합니다. 이 선택은 기본적으로 선택 취소되어 있으며, 이는 관리자가 프로파일을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있음을 의미합니다.
복호화 미러링 인터페이스 (AWS, Azure, NSX 에디션 및 Citrix SDX의 VM 시리즈 방화벽을 제외한 모든 모델에서 지원됨)	복호화 포트 미러링에 사용할 인터페이스를 선택합니다. 복호화 포트 미러링을 활성화하려면 먼저 복호화 포트 미러 라이선스를 취득하고 라이선스를 설치하고 방화벽을 재부팅해야 합니다.
포워딩만 해당 (AWS, Azure, NSX 에디션 및 Citrix SDX의 VM 시리즈 방화벽을 제외한 모든 모델에서 지원됨)	보안 정책 시행 후에만 복호화된 트래픽을 미러링하려면 포워딩만 해당을 선택합니다. 이 옵션을 사용하면 방화벽을 통해 포워딩되는 트래픽만 미러링됩니다. 이 옵션은 복호화된 트래픽을 DLP 디바이스 또는 다른 IPS(침입 방지 시스템)와 같은 다른 위협 탐지 디바이스로 포워딩하는 경우에 유용합니다. 이 선택(기본 설정)을 선택 취소하면 방화벽이 보안 정책 조회 전에 인터페이스에 대한 복호화된 모든 트래픽을 미러링하므로 이벤트를 재생하고 위협을 생성하거나 삭제 작업을 트리거하는 트래픽을 분석할 수 있습니다.

복호화된 트래픽을 제어하기 위한 설정

다음 표에서는 방화벽이 정방향 프록시 복호화 또는 인바운드 검사(SSL 프로토콜 설정 탭 포함)를 사용하여 복호화한 트래픽을 제어하는 데 사용할 수 있는 설정을 설명합니다. 이러한 설정을 사용하여 외부 서버 인증서의 상태, 지원되지 않는 암호 제품군 또는 프로토콜 버전의 사용 또는 복호화를 처리하기 위한 시스템 리소스의 가용성을 비롯한 기준에 따라 TLS 세션을 제한하거나 차단할 수 있습니다.

SSL 복호화 탭 설정	설명
SSL 포워딩 프록시 탭 포워딩 프록시를 사용하여 복호화된 TLS 트래픽을 제한하거나 차단하는 옵션을 선택합니다.	
서버 인증서 유효성 검사 - 복호화된 트래픽에 대한 서버 인증서를 제어하는 옵션을 선택합니다.	

SSL 복호화 탭 설정	설명
만료된 인증서가 있는 세션 차단	서버 인증서가 만료되면 TLS 연결을 종료합니다. 이렇게 하면 사용자가 만료된 인증서를 수락하고 TLS 세션을 계속할 수 없습니다. 잠재적으로 안전하지 않은 사이트에 대한 액세스를 방지하기 위해 만료된 인증서가 있는 세션을 차단합니다.
신뢰할 수 없는 발급자와의 세션 차단	서버 인증서 발급자를 신뢰할 수 없는 경우 TLS 세션을 종료합니다. 신뢰할 수 없는 발급자가 중간자 공격, 재전송 공격 또는 다른 공격을 나타낼 수 있으므로 신뢰할 수 없는 발급자와의 세션을 차단합니다.
알 수 없는 인증서 상태의 세션 차단	서버가 "알 수 없음"의 인증서 해지 상태를 반환하는 경우 TLS 세션을 종료합니다. 인증서 해지 상태는 인증서에 대한 신뢰가 취소되었는지의 여부를 나타냅니다. 가장 엄격한 보안을 위해 알 수 없는 인증서 상태의 세션을 차단합니다. 그러나 여러 가지 이유로 인증서 상태를 알 수 없기 때문에 보안이 너무 강화될 수 있습니다. 알 수 없는 인증서 상태를 차단하는 것이 비즈니스에 사용해야 하는 사이트에 영향을 미치는 경우 알 수 없는 인증서 상태의 세션을 차단하지 마십시오.
인증서 상태 확인 타임아웃 시 세션 차단	방화벽이 인증서 상태 서비스의 응답 대기를 중지하도록 구성된 시간 내에 인증서 상태를 검색할 수 없는 경우 TLS 세션을 종료합니다. 인증서 프로파일(**Device** > **Certificate Management** > **Certificate** 프로파일)을 만들거나 수정할 때 인증서 상태 타임아웃 값을 구성할 수 있습니다. 상태 확인 시간이 초과될 때 세션을 차단하는 것은 더 엄격한 보안과 더 나은 사용자 경험 사이의 절충점입니다. 인증서 해지 서버가 느리게 응답하는 경우 제한 시간에 차단하면 유효한 인증서가 있는 사이트가 차단될 수 있습니다. 유효한 인증서 타임아웃이 우려되는 경우 CRL(인증서 해지 확인) 및 OCSP(온라인 인증서 상태 프로토콜)에 대한 타임아웃 값을 늘릴 수 있습니다.
인증서 확장 제한	동적 서버 인증서에 사용되는 인증서 확장을 키 사용 및 확장 키 사용으로 제한합니다. 배포에 다른 인증서 확장이 필요하지 않은 경우 인증서 확장을 제한합니다.

SSL 복호화 탭 설정	설명
인증서의 CN 값을 SAN 확장에 추가	방화벽이 포워드 프록시 복호화의 일부로 클라이언트에 제공하는 가장 인증서에 SAN(주체 대체 이름) 확장을 추가할 수 있도록 합니다. 서버 인증서에 CN(일반 이름) 만 포함된 경우 방화벽은 서버 인증서 CN을 기반으로 가장 인증서에 SAN 확장을 추가합니다. 이 옵션은 브라우저에서 SAN을 사용하기 위해 서버 인증서가 필요하고 더 이상 CN을 기반으로 하는 인증서 일치를 지원하지 않는 경우에 유용합니다. 즉, 최종 사용자가 요청한 웹 리소스에 계속 액세스할 수 있으며 서버가 있더라도 방화벽이 세션을 계속 해독할 수 있도록 합니다.인증서에 CN만 포함되어 있습니다. 요청된 웹 리소스에 대한 액세스를 보장하기 위해 인증서의 *CN* 값을 *SAN* 확장에 추가합니다.
지원되지 않는 모드 확인 - 지원되지 않는 TLS 애플리케이션을 제어하는 옵션을 선택합니다.	
지원되지 않는 버전의 세션 차단	PAN-OS가 "client hello" 메시지를 지원하지 않으면 세션을 종료합니다. PAN-OS는 SSLv3, TLSv1.0, TLSv1.1, TLSv1.2 및 TLSv1.3을 지원합니다. 프로토콜이 약한 사이트에 대한 액세스를 방지하기 위해 항상 지원되지 않는 버전의 세션을 차단하십시오. ***SSL*** 프로토콜 설정 탭에서 최소 프로토콜 버전을 *TLSv1.2*로 설정하여 프로토콜 버전이 취약한 사이트를 차단합니다. 비즈니스 목적으로 액세스해야 하는 사이트가 약한 프로토콜을 사용하는 경우 약한 프로토콜을 허용하는 별도의 복호화 프로파일을 만들고 약한 프로토콜을 허용해야 하는 사이트에만 적용되는 복호화 정책 규칙에 지정합니다.
지원되지 않는 암호 제품군이 있는 세션 차단	PAN-OS에서 지원하지 않는 경우 TLS 핸드쉐이크에 지정된 암호 제품군인 경우 세션을 종료합니다. 지원하지 않는 암호 제품군을 사용하는 세션을 차단합니다. ***SSL*** 프로토콜 설정 탭에서 허용할 암호 그룹*(*암호화 알고리즘*)*을 구성합니다. 사용자가 취약한 암호 제품군을 사용하는 사이트에 연결하는 것을 허용하지 마십시오.
클라이언트 인증으로 세션 차단	포워드 프록시 트래픽에 대한 클라이언트 인증으로 세션을 종료합니다.

SSL 복호화 탭 설정	설명
	중요한 애플리케이션이 요구하지 않는 한 클라이언트 인증으로 세션을 차단합니다. 이 경우 별도의 복호화 프로파일을 만들고 클라이언트 인증이 필요한 트래픽에만 적용해야 합니다.
실패 확인 - 복호화를 처리하는 데 시스템 리소스를 사용할 수 없는 경우 수행할 작업을 선택합니다.	
리소스를 사용할 수 없는 경우 세션 차단	복호화를 처리하는 데 시스템 리소스를 사용할 수 없는 경우 세션을 종료합니다. 리소스를 사용할 수 없을 때 세션을 차단할지의 여부는 더 엄격한 보안과 더 나은 사용자 경험 사이의 절충안입니다. 리소스를 사용할 수 없을 때 세션을 차단하지 않으면 리소스가 영향을 받을 때 복호화하려는 트래픽을 방화벽이 복호화할 수 없습니다. 그러나 리소스를 사용할 수 없을 때 세션을 차단하면 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되기 때문에 사용자 경험에 영향을 줄 수 있습니다.
HSM을 사용할 수 없는 경우 세션 차단	인증서 서명에 하드웨어 보안 모듈(HSM)을 사용할 수 없는 경우 세션을 종료합니다. HSM을 사용할 수 없는 경우 세션을 차단할지의 여부는 개인 키의 출처와 HSM을 사용할 수 없는 경우 암호화된 트래픽을 처리할 방법에 대한 규정 준수 규칙에 따라 다릅니다.
리소스가 없을 때 다운그레이드 차단	TLSv1.2로 다운그레이드하는 대신 TLSv1.3 핸드쉐이크를 처리하는 데 시스템 리소스를 사용할 수 없는 경우 세션을 종료합니다. 리소스를 사용할 수 없을 때 세션을 차단할지의 여부는 더 엄격한 보안과 더 나은 사용자 경험 사이의 절충안입니다. TLSv1.3 리소스를 사용할 수 없을 때 핸드쉐이크를 TLSv1.2로 다운그레이드하는 것을 차단하면 방화벽이 세션을 삭제합니다. 핸드쉐이크 다운그레이드를 차단하지 않으면 TLSv1.3 핸드쉐이크에 리소스를 사용할 수 없는 경우 방화벽이 TLSv1.2로 다운그레이드됩니다.
클라이언트 확장	
스트립 ALPN	방화벽은 기본적으로 HTTP/2 트래픽을 처리하고 검사합니다. 그러나 방화벽이 **ALPN**을 제거하도록 지정하여 HTTP/2 검사를 비활성화할 수 있습니다. 이 옵션을 선택하면 방화벽이 ALPN(Application-Layer Protocol Negotiation) TLS 확장에 포함된 모든 값을 제거합니다.

SSL 복호화 탭 설정	설명
	ALPN은 HTTP/2 연결을 보호하는 데 사용되기 때문에 이 TLS 확장에 대해 지정된 값이 없으면 방화벽은 HTTP/2 트래픽을 HTTP/1.1로 다운그레이드하거나 이를 알 수 없는 TCP 트래픽으로 분류합니다.

지원되지 않는 모드 및 실패 모드의 경우 세션 정보가 *12*시간 동안 캐시되므로 동일한 호스트와 서버 쌍 간의 향후 세션은 복호화되지 않습니다. 대신 해당 세션을 차단하는 옵션을 활성화하십시오.

SSL 인바운드 검사 탭

인바운드 검사를 사용하여 복호화된 트래픽을 제한하거나 차단하는 옵션을 선택합니다.

지원되지 않는 모드 확인 - TLS 트래픽에서 지원되지 않는 모드가 감지되는 경우 세션을 제어하는 옵션을 선택합니다.

지원되지 않는 버전의 세션 차단	PAN-OS가 "client hello" 메시지를 지원하지 않으면 세션을 종료합니다. PAN-OS는 SSLv3, TLSv1.0, TLSv1.1, TLSv1.2 및 TLSv1.3을 지원합니다. 프로토콜이 약한 사이트에 대한 액세스를 방지하기 위해 항상 지원되지 않는 버전의 세션을 차단하십시오. ***SSL*** 프로토콜 설정 탭에서 최소 프로토콜 버전을 *TLSv1.2*로 설정하여 프로토콜 버전이 취약한 사이트를 차단합니다. 비즈니스 목적으로 액세스해야 하는 사이트가 약한 프로토콜을 사용하는 경우 약한 프로토콜을 허용하는 별도의 복호화 프로파일을 만들고 약한 프로토콜을 허용해야 하는 사이트에만 적용되는 복호화 정책 규칙에 지정합니다.
지원되지 않는 암호 제품군이 있는 세션 차단	사용된 암호 제품군이 PAN-OS에서 지원되지 않는 경우 세션을 종료합니다. 지원하지 않는 암호 제품군을 사용하는 세션을 차단합니다. ***SSL*** 프로토콜 설정 탭에서 허용할 암호 그룹*(*암호화 알고리즘*)*을 구성합니다. 사용자가 취약한 암호 제품군을 사용하는 사이트에 연결하는 것을 허용하지 마십시오.

실패 확인 - 시스템 리소스를 사용할 수 없는 경우 수행할 작업을 선택합니다.

리소스를 사용할 수 없는 경우 세션 차단	복호화를 처리하는 데 시스템 리소스를 사용할 수 없는 경우 세션을 종료합니다.

SSL 복호화 탭 설정	설명
	리소스를 사용할 수 없을 때 세션을 차단할지의 여부는 더 엄격한 보안과 더 나은 사용자 경험 사이의 절충안입니다. 리소스를 사용할 수 없을 때 세션을 차단하지 않으면 리소스가 영향을 받을 때 복호화하려는 트래픽을 방화벽이 복호화할 수 없습니다. 그러나 리소스를 사용할 수 없을 때 세션을 차단하면 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되기 때문에 사용자 경험에 영향을 줄 수 있습니다.
HSM을 사용할 수 없는 경우 세션 차단	세션 키를 복호화하는 데 하드웨어 보안 모듈(HSM)을 사용할 수 없는 경우 세션을 종료합니다. HSM을 사용할 수 없는 경우 세션을 차단할지의 여부는 개인 키의 출처와 HSM을 사용할 수 없는 경우 암호화된 트래픽을 처리할 방법에 대한 규정 준수 규칙에 따라 다릅니다.
리소스가 없을 때 다운그레이드 차단	TLSv1.2로 다운그레이드하는 대신 TLSv1.3 핸드쉐이크를 처리하는 데 시스템 리소스를 사용할 수 없는 경우 세션을 종료합니다. 리소스를 사용할 수 없을 때 세션을 차단할지의 여부는 더 엄격한 보안과 더 나은 사용자 경험 사이의 절충안입니다. TLSv1.3 리소스를 사용할 수 없을 때 핸드쉐이크를 TLSv1.2로 다운그레이드하는 것을 차단하면 방화벽이 세션을 삭제합니다. 핸드쉐이크 다운그레이드를 차단하지 않으면 TLSv1.3 핸드쉐이크에 리소스를 사용할 수 없는 경우 방화벽이 TLSv1.2로 다운그레이드됩니다.
SSL 프로토콜 설정 탭 TLS 세션 트래픽에 대해 프로토콜 버전 및 암호 제품군을 적용하려면 다음 설정을 선택합니다.	
프로토콜 버전	TLS 세션에 대해 최소 및 최대 프로토콜 버전 사용을 시행합니다.
최소 버전	TLS 연결을 설정하는 데 사용할 수 있는 최소 프로토콜 버전을 설정합니다. 가장 강력한 보안을 제공하려면 최소 버전을 *TLSv1.2*로 설정하십시오. *TLSv1.2*를 지원하지 않는 사이트를 검토하여 실제로 합법적인 비즈니스 목적이 있는지 확인하십시오. *TLSv1.2*를 지원하지 않는 액세스해야 하는 사이트의 경우 지원하는 가장 강력한 프로토콜 버전을 지정하는 별도의 복호화 프로파일을 만들고 취약한 버전의 사용을 필요한 소스(영역, 주소, 사용자)에서만 필요한 사이트에 한하여 제한하는 복호화 정책 규칙에 적용합니다.

SSL 복호화 탭 설정	설명
최대 버전	TLS 연결을 설정하는 데 사용할 수 있는 최대 프로토콜 버전을 설정합니다. 최대 버전이 지정되지 않도록 최대 옵션을 선택할 수 있습니다. 이 경우 선택한 최소 버전과 동일하거나 이후 버전인 프로토콜 버전이 지원됩니다. 프로토콜이 향상되면 방화벽에서 자동으로 지원하도록 *Max Version*을 ***Max***로 설정합니다. 그러나 복호화 정책이 고정된 인증서를 사용하는 모바일 애플리케이션을 지원하는 경우 최대 버전을 ***TLSv1.2***로 설정하십시오. *TLSv1.3*은 이전 *TLS* 버전에서 암호화되지 않은 인증서 정보를 암호화하기 때문에 방화벽은 인증서 정보를 기반으로 복호화 제외를 자동으로 추가할 수 없으며, 이는 일부 모바일 애플리케이션에 영향을 미칩니다. 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 트래픽에 대해 *TLSv1.3*을 활성화할 수 있도록 해당 애플리케이션에 대한 별도의 복호화 정책 및 프로파일을 만드는 것이 좋습니다.
키 교환 알고리즘	TLS 세션에 대해 선택한 키 교환 알고리즘의 사용을 시행합니다. 세 가지 알고리즘(**RSA**, **DHE** 및 **ECDHE**)은 모두 기본적으로 활성화되어 있습니다. **DHE**(Diffie-Hellman) 및 **ECDHE**(타원 곡선 Diffie-Hellman)는 포워드 프록시 또는 인바운드 검사 복호화를 위해 PFS(완벽한 순방향 비밀성)를 활성화합니다.
암호화 알고리즘	TLS 세션에 대해 선택한 암호화 알고리즘의 사용을 시행합니다. 약한 ***3DES*** 또는 ***RC4*** 암호화 알고리즘을 지원하지 마십시오. *(*방화벽은 *TLSv1.2* 이상을 최소 프로토콜 버전으로 사용하는 경우 이 두 알고리즘을 자동으로 차단합니다.*)* 예외를 만들고 더 약한 프로토콜 버전을 지원해야 하는 경우 복호화 프로파일에서 ***3DES*** 및 ***RC4***를 선택 취소합니다. ***3DES*** 또는 ***RC4*** 암호화 알고리즘을 사용하는 비즈니스 목적으로 액세스해야 하는 사이트가 있는 경우 별도의 복호화 프로파일을 만들어 해당 사이트에 대한 복호화 정책 규칙에 적용합니다.

SSL 복호화 탭 설정	설명
인증 알고리즘	TLS 세션에 대해 선택한 인증 알고리즘을 사용합니다. 기존의 약한 *MD5* 알고리즘을 차단합니다*(*기본적으로 차단됨*). SHA1* 인증을 사용하는 사이트가 없으면 *SHA1*을 차단하십시오. 비즈니스 목적으로 필요한 사이트에서 *SHA1*을 사용하는 경우 별도의 복호화 프로파일을 만들어 해당 사이트에 대한 복호화 정책 규칙에 적용합니다.

복호화되지 않은 트래픽을 제어하기 위한 설정

No Decryption 탭을 사용하여 **No Decrypt** 작업(**Policies** > **Decryption** > **Action**)으로 구성된 복호화 정책과 일치하는 트래픽을 차단하는 설정을 활성화할 수 있습니다. 방화벽이 세션 트래픽의 암호를 복호화하고 검사하지 않지만 이러한 옵션을 사용하여 세션에 대한 서버 인증서를 제어합니다.

복호화 탭 설정 없음	설명
만료된 인증서가 있는 세션 차단	서버 인증서가 만료된 경우 SSL 연결을 종료합니다. 이렇게 하면 사용자가 만료된 인증서를 수락하고 SSL 세션을 계속할 수 없습니다. 잠재적으로 안전하지 않은 사이트에 대한 액세스를 방지하기 위해 만료된 인증서가 있는 세션을 차단합니다.
신뢰할 수 없는 발급자와의 세션 차단	서버 인증서 발급자를 신뢰할 수 없는 경우 SSL 세션을 종료합니다. 신뢰할 수 없는 발급자가 중간자 공격, 재전송 공격 또는 다른 공격을 나타낼 수 있으므로 신뢰할 수 없는 발급자와의 세션을 차단합니다.

복호화된 SSH 트래픽을 제어하기 위한 설정

다음 표에서는 복호화된 인바운드 및 아웃바운드 SSH 트래픽을 제어하는 데 사용할 수 있는 설정을 설명합니다. 이러한 설정을 사용하면 지원되지 않는 알고리즘 사용, SSH 오류 감지 또는 SSH 프록시 복호화를 처리하기 위한 리소스 가용성을 비롯한 기준에 따라 SSH 터널링된 트래픽을 제한하거나 차단할 수 있습니다.

SSH 프록시 탭 설정	설명
지원되지 않는 모드 확인 - SSH 트래픽에서 지원되지 않는 모드가 감지되는 경우 이 옵션을 사용하여 세션을 제어합니다. 지원되는 SSH 버전은 SSH 버전 2입니다.	

SSH 프록시 탭 설정	설명
지원되지 않는 버전의 세션 차단	"client hello" 메시지가 PAN-OS에서 지원되지 않으면 세션을 종료합니다. 프로토콜이 약한 사이트에 대한 액세스를 방지하기 위해 항상 지원되지 않는 버전의 세션을 차단하십시오. ***SSL*** 프로토콜 설정 탭에서 최소 프로토콜 버전을 *TLSv1.2*로 설정하여 프로토콜 버전이 취약한 사이트를 차단합니다. 비즈니스 목적으로 액세스해야 하는 사이트가 약한 프로토콜을 사용하는 경우 약한 프로토콜을 허용하는 별도의 복호화 프로파일을 만들고 약한 프로토콜을 허용해야 하는 사이트에만 적용되는 복호화 정책 규칙에 지정합니다.
지원되지 않는 알고리즘으로 세션 차단	클라이언트 또는 서버에서 지정한 알고리즘이 PAN-OS에서 지원되지 않는 경우 세션을 종료합니다. 약한 알고리즘을 사용하는 사이트에 대한 액세스를 방지하려면 항상 지원되지 않는 알고리즘이 있는 세션을 차단하십시오.
실패 확인 - SSH 애플리케이션 오류가 발생하고 시스템 리소스를 사용할 수 없는 경우 수행할 작업을 선택합니다.	
SSH 오류에 대한 세션 차단	SSH 오류가 발생하면 세션을 종료합니다.
리소스를 사용할 수 없는 경우 세션 차단	복호화를 처리하는 데 시스템 리소스를 사용할 수 없는 경우 세션을 종료합니다. 리소스를 사용할 수 없을 때 세션을 차단할지의 여부는 더 엄격한 보안과 더 나은 사용자 경험 사이의 절충안입니다. 리소스를 사용할 수 없을 때 세션을 차단하지 않으면 리소스가 영향을 받을 때 복호화하려는 트래픽을 방화벽이 복호화할 수 없습니다. 그러나 리소스를 사용할 수 없을 때 세션을 차단하면 일반적으로 연결할 수 있는 사이트에 일시적으로 연결할 수 없게 되기 때문에 사용자 경험에 영향을 줄 수 있습니다.

개체 > 패킷 브로커 프로파일

패킷 브로커 프로파일은 방화벽이 트래픽을 보안 체인으로 포워딩하는 방법을 정의합니다. 보안 체인은 추가 보안 검사 및 시행을 제공하는 인라인 타사 보안 어플라이언스 세트입니다. 프로파일은 보안 체인에 연결하는 데 사용되는 방화벽 인터페이스, 보안 체인 유형(라우팅된 레이어 3 또는 레이어 1 투명 브리지), 레이어 3 보안 체인의 첫 번째 및 마지막 어플라이언스, 여러 레이어 3 체인 간의 세션 배포(로드 밸런싱), 상태 모니터링 및 경로 또는 HTTP 대기 시간 실패 시 수행할 조치를 정의합니다. 패킷 브로커 정책 규칙에 패킷 브로커 프로파일을 연결합니다. 정책 규칙은 보안 체인으로 포워딩할 트래픽을 정의하고 프로파일은 해당 트래픽을 포워딩하는 방법을 정의합니다.

Packet Broker 프로파일을 구성하기 전에 방화벽에서 최소 2개의 Layer 3 인터페이스를 지정하여 트래픽을 보안 체인으로 포워딩해야 합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택합니다.
2. Packet Broker 포워딩에 사용할 인터페이스를 선택합니다.
3. 인터페이스 유형을 **Layer3**으로 설정합니다.
4. **Advanced** > 기타 정보를 선택합니다.
5. 네트워크 패킷 브로커를 선택하여 인터페이스를 활성화합니다.
6. 다른 이더넷 인터페이스로 이 단계를 반복하십시오. 둘 이상의 전용 연결(예: 여러 보안 체인에 연결)을 원하는 경우 각 전용 연결에 대해 이더넷 인터페이스 쌍을 구성하십시오.

패킷 브로커 프로파일 설정	설명
이름	프로파일에 설명이 포함된 이름을 지정합니다.
설명	선택적으로 프로파일 설정 또는 목적을 설명합니다.
일반 탭	
보안 체인 유형	방화벽이 복호화된 트래픽을 포워딩할 보안 체인 유형을 선택합니다. • 라우팅(레이어 3): 이러한 유형의 보안 체인에 있는 디바이스는 레이어 3 인터페이스를 사용하여 보안 체인 네트워크에 연결합니다. 각 인터페이스에는 할당된 IP 주소와 서브넷 마스크가 있어야 합니다. 정적 경로로 보안 체인 디바이스를 구성하거나 동적 라우팅을 사용하여 인바운드 및 아웃바운드 트래픽을 보안 체인의 다음 디바이스로 보낸 다음 다시 방화벽으로 보냅니다. • 투명 브리지: 투명 브리지 보안 체인 네트워크에서 모든 보안 체인 디바이스에는 보안 체인 네트워크에 연결된 두 개의 투명 브리지 모드 인터페이스가 있습니다. 투명 브리지 인터페이스에는 IP 주소, 서브넷 마스크, 기본 게이트웨이 또는 로컬 라우팅 테이블이 없습니다. 보안 체인 어플라이언스는 한 인터페이스에서 트래픽을 수신하고 트래픽을 분석하

패킷 브로커 프로파일 설정	설명
	고 보안을 시행한 다음 트래픽이 다른 인터페이스에서 다음 보안 체인 디바이스로 빠져 나옵니다.
IPv6 활성화	(투명 브리지 모드만 해당) IPv6 트래픽 포워딩을 활성화합니다.
플로우 방향	트래픽이 한 방화벽 인터페이스에서 보안 체인으로 들어가고 다른 방화벽 인터페이스로 보안을 종료할지 또는 트래픽이 두 방화벽 인터페이스에서 보안 체인으로 들어오고 나갈 수 있는지 선택합니다. • 단방향 - 방화벽은 인터페이스 **#1**을 통해 보안 체인으로 모든 트래픽을 포워딩하고 인터페이스 **#2**의 보안 체인에서 트래픽을 다시 수신합니다. 두 인터페이스는 동일한 영역에 있어야 합니다. • 양방향 — 방화벽은 인터페이스 **#1**을 통해 클라이언트-서버 트래픽을 보안 체인으로 포워딩하고 인터페이스 **#2**의 보안 체인에서 트래픽을 다시 수신합니다. 방화벽은 인터페이스 **#2**를 통해 서버-클라이언트 트래픽을 보안 체인으로 포워딩하고 인터페이스 **#1**의 보안 체인에서 트래픽을 다시 수신합니다. 선택하는 흐름 방향은 보안 체인의 어플라이언스 유형에 따라 다릅니다. 예를 들어 보안 체인에 세션의 양쪽을 검사할 수 있는 상태 비저장 디바이스가 있는 경우 단방향 흐름을 선택할 수 있습니다.
인터페이스 #1	방화벽이 보안 체인으로 트래픽을 포워딩하고 보안 체인에서 트래픽을 수신하는 데 사용하는 네트워크 패킷 브로커 인터페이스입니다. 이 도움말 항목의 시작 부분에 설명된 대로 각 인터페이스를 Network Packet Broker 인터페이스로 구성해야 합니다.
인터페이스 #2	

보안 체인 탭

한 쌍의 Network Packet Broker 방화벽 인터페이스에서 하나 이상의 (로드 밸런싱 또는 중복성을 위해) 레이어 3 보안 체인을 구성합니다. 라우팅**(**레이어 **3)** 보안 체인 유형의 경우 트래픽을 포워딩할 위치를 지정하기 위해 하나 이상의 보안 체인을 구성해야 합니다. 다중 보안 체인의 경우 스위치 또는 기타 디바이스가 방화벽과 체인 간의 라우팅을 처리해야 합니다.

이 탭의 옵션은 레이어 *3(*라우팅된*)* 보안 체인에만 사용할 수 있습니다.

활성화	보안 체인을 활성화합니다.

패킷 브로커 프로파일 설정	설명
이름	보안 체인에 설명이 포함된 이름을 지정합니다.
첫 번째 디바이스 마지막 디바이스	보안 체인의 첫 번째 및 마지막 디바이스의 IPv4 주소를 입력하거나 새 주소 개체를 정의하여 디바이스를 쉽게 참조할 수 있습니다.
세션 분배 방식	여러 라우팅(레이어 **3)** 보안 체인에 포워딩할 때 방화벽이 여러 보안 체인 간에 세션을 배포하는 데 사용하는 방법을 선택합니다. • **IP Modulo** - 방화벽은 소스 및 대상 IP 주소의 IP Modulo 해시를 기반으로 세션을 할당합니다. • **IP** 해시 - 방화벽은 소스 및 대상 IP 주소와 포트 번호의 IP 해시를 기반으로 세션을 할당합니다. • 라운드 로빈 - 방화벽이 보안 체인 간에 세션을 균등하게 할당합니다. • 최저 대기 시간 - 방화벽은 대기 시간이 가장 짧은 보안 체인에 더 많은 세션을 할당합니다. 이 방법이 예상대로 작동하려면 상태 모니터 탭에서 대기 시간 모니터링 및 HTTP 모니터링도 활성화해야 합니다.
상태 모니터 탭	
상태 확인 실패 시	상태 확인(경로 모니터링, **HTTP** 모니터링 또는 **HTTP** 모니터링 대기 시간)을 활성화하면 체인(또는 여러 체인이 있는 경우 모든 체인)이 실패할 경우 어떤 일이 발생하는지도 결정합니다. 여러 체인이 있고 하나 이상의 체인이 상태 확인에 실패했지만 하나 이상의 체인이 여전히 정상인 경우 방화벽은 세션 배포 방법을 기반으로 나머지 체인에 트래픽을 분산합니다. 모든 체인이 한 쌍의 방화벽 네트워크 패킷 브로커 인터페이스와 연결된 경우 다음을 수행할 수 있습니다. • 보안 체인 우회 - 방화벽이 트래픽을 실패한 체인 대신 대상으로 포워딩합니다. 방화벽은 구성된 보안 프로파일과 보호 기능을 트래픽에 계속 적용합니다. • 세션 차단 - 방화벽이 세션을 차단합니다.
상태 확인 실패 조건	상태 확인을 두 개 이상 구성하는 경우(체인에서 세 가지 상태 확인을 모두 구성할 수 있음) 방화벽에서 실패를 정의하는 방법을 구성합니다. • **OR** 조건 - 선택한 상태 확인이 실패하면 상태 확인 실패 시 작업이 발생합니다. • **AND** 조건 - 선택한 모든 상태 확인이 실패하면 상태 확인 실패 시 작업이 발생합니다.

패킷 브로커 프로파일 설정	설명
경로 모니터링 지연 모니터링 HTTP 모니터링	경로, HTTP 대기 시간 또는 HTTP 모니터링 또는 세 가지 상태 확인의 조합을 활성화하여 보안 체인에 오류가 발생하는 시기를 식별하고 오류가 발생한 시기를 결정하는 메트릭을 구성합니다. • 경로 모니터링 - 디바이스 연결을 확인합니다. 핑 횟수, 핑 인터벌(초), 복구 보류 시간(초)을 설정합니다. • **HTTP** 모니터링 - 디바이스 가용성 및 응답 시간을 확인합니다. HTTP 수와 HTTP 인터벌을 초 단위로 설정합니다. • **HTTP** 모니터링 대기 시간 - 디바이스 처리 속도와 효율성을 확인합니다. 최대 대기 시간(밀리초), 대기 시간(초) 및 기간을 초과하는 로그 대기 시간을 설정합니다. **HTTP Monitoring Latency**를 선택하면 **HTTP Monitoring**이 자동으로 선택됩니다. 대기 시간 모니터링을 활성화하려면 둘 다 선택해야 합니다.

개체 > SD-WAN 링크 관리

SD-WAN 정책 규칙에 지정된 애플리케이션 및 서비스 세트에 적용할 프로파일을 만듭니다. 각 프로파일 유형은 SD-WAN 링크 관리의 다양한 측면을 제어합니다.

- 개체 > SD-WAN 링크 관리 > 경로 품질 프로파일
- 개체 > SD-WAN 링크 관리 > SaaS 품질 프로파일
- 개체 > SD-WAN 링크 관리 > 트래픽 분산 프로파일
- 개체 > SD-WAN 링크 관리 > 오류 수정 프로파일

개체 > SD-WAN 링크 관리 > 경로 품질 프로파일

SD-WAN을 사용하면 고유한 네트워크 품질 요구 사항이 있고 SD-WAN 정책 규칙에서 프로파일을 참조하는 각 애플리케이션, 애플리케이션 필터, 애플리케이션 그룹, 서비스, 서비스 개체 및 서비스 그룹 개체 집합에 대한 경로 품질 프로파일을 만들 수 있습니다. 프로파일에서 대기 시간, 지터 및 패킷 손실의 세 가지 매개변수에 대한 최대 임계값을 설정합니다. SD-WAN 링크가 임계값 중 하나를 초과하면 방화벽은 이 프로파일을 적용하는 SD-WAN 규칙과 일치하는 패킷에 대해 최상의 새 경로를 선택합니다.

각 경로 품질 매개변수에 대한 민감도 설정을 사용하면 프로파일이 적용되는 애플리케이션에 대해 어떤 매개변수가 더 중요한지(선호됨) 방화벽에 표시할 수 있습니다. 방화벽은 중간 또는 낮은 설정의 매개변수보다 높은 설정의 매개변수를 더 중요하게 생각합니다. 예를 들어 일부 애플리케이션은 지터나 대기 시간보다 패킷 손실에 더 민감하므로 패킷 손실을 높은 감도로 설정하면 방화벽이 패킷 손실을 먼저 검사할 수 있습니다.

대기 시간, 지터 및 패킷 손실에 대한 민감도 설정을 기본 설정(중간)으로 유지하거나 세 가지 매개변수를 모두 동일한 설정으로 설정하는 경우 프로파일의 기본 설정 순서는 패킷 손실, 대기 시간, 지터입니다.

기본적으로 방화벽은 대기 시간과 지터를 200ms마다 측정하고 마지막 세 측정의 평균을 사용하여 슬라이딩 창에서 경로 품질을 측정합니다. SD-WAN 인터페이스 프로파일을 구성할 때 적극적인 또는 완화된 경로 모니터링을 선택하여 이 동작을 수정할 수 있습니다.

	경로 품질 프로파일 설정
이름	최대 31자의 영숫자, 밑줄, 하이픈, 공백 및 마침표를 사용하여 경로 품질 프로파일의 이름을 입력합니다.
공유(Panorama만 해당)	Panorama의 모든 디바이스 그룹과 구성을 푸시하는 다중 vsys 허브 또는 분기의 모든 가상 시스템에서 경로 품질 프로파일을 사용할 수 있도록 하려면 선택합니다.
재정의 비활성화(Panorama만 해당)	관리자가 프로필을 상속하는 디바이스 그룹에서 이 경로 품질 프로필의 설정을 재정의하지 못하도록 하려면 선택합니다. (공유를 선택한 경우 재정의 비활성화를 사용할 수 없습니다.)

	경로 품질 프로파일 설정
대기 시간(밀리초)	임계값 - 패킷이 방화벽을 떠나 SD-WAN 터널의 반대쪽 끝에 도달하고 임계값을 초과하기 전에 응답 패킷이 방화벽으로 돌아가는 데 허용되는 시간(밀리초)을 입력합니다(범위는 10~2,000, 기본값 100)입니다.
	감도 - 높음, 중간 또는 낮음을 선택합니다(기본값은 중간).
지터(밀리초)	임계값 - 밀리초 수를 입력합니다(범위는 10~1,000, 기본값은 100).
	감도 - 높음, 중간 또는 낮음을 선택합니다(기본값은 중간).
패킷 손실 (%)	임계값 - 임계값을 초과하기 전에 링크에서 손실된 패킷의 백분율을 입력합니다(범위는 1~100.0, 기본값은 1).
	감도 - 패킷 손실에 대한 감도 설정은 영향을 미치지 않으므로 기본 설정(중간)을 그대로 둡니다.

개체 > SD-WAN 링크 관리 > SaaS 품질 프로파일

SD-WAN을 사용하면 SaaS(Software-as-a-Service) 품질 프로필을 생성하여 허브 또는 브랜치 방화벽과 서버 측 SaaS 애플리케이션 간의 경로 상태 품질을 측정하여 SaaS 애플리케이션 안정성을 정확하게 모니터링할 수 있으며, 경로 상태 품질이 저하되는 경우 경로를 교체합니다. 이를 통해 방화벽은 다른 DIA(직접 인터넷 액세스) 링크로 페일오버할 시기를 정확하게 결정할 수 있습니다.

SaaS 품질 프로파일을 사용하면 애플리케이션 활동을 모니터링하는 적응형 학습 알고리즘을 사용하거나 애플리케이션 IP 주소, FQDN 또는 URL을 사용하여 SaaS 애플리케이션을 지정하여 모니터링할 SaaS 애플리케이션을 지정할 수 있습니다.

	SaaS 품질 프로파일 설정
이름	영숫자, 밑줄, 하이픈, 공백 및 마침표를 사용하여 경로 품질 프로파일의 이름을 입력합니다.
공유(Panorama만 해당)	모든 디바이스 그룹에서 SaaS 품질 프로파일을 공유하려면 선택(활성화)합니다.
재정의 비활성화(Panorama만 해당)	관리 방화벽에서 로컬로 SaaS 품질 프로파일 설정을 재정의하는 기능을 비활성화하려면 선택(활성화)합니다.
SaaS 모니터링 모드	

	SaaS 품질 프로파일 설정
적응형	SaaS 애플리케이션 세션 활동은 송신 및 수신 활동에 대해 모니터링되며 경로 상태는 SD-WAN 인터페이스에 대한 추가 상태 확인 없이 자동으로 파생됩니다. 이 옵션은 기본적으로 선택되어 있습니다.
고정 IP 주소	**IP** 주소/개체 - 애플리케이션 IP 주소를 사용하여 모니터링할 SaaS 애플리케이션을 지정합니다. • **IP** 주소 - SaaS 애플리케이션의 IP 주소입니다. • 프로브 인터벌(초) - 방화벽이 방화벽과 SaaS 애플리케이션 간의 경로 품질 상태를 프로브하는 인터벌(초)을 지정합니다. 기본값은 3초입니다. 최대 4개의 고정 IP 주소가 지원됩니다.
	FQDN - 애플리케이션 FQDN(정규화된 도메인 이름)을 사용하여 모니터링할 SaaS 애플리케이션을 지정합니다. • **FQDN** - SaaS 애플리케이션의 FQDN입니다. FQDN을 지정하려면 FQDN 주소 개체를 구성해야 합니다. SaaS 애플리케이션을 성공적으로 모니터링하려면 SaaS 애플리케이션 FQDN을 확인할 수 있어야 합니다. • 프로브 인터벌(초) - 방화벽이 분기 방화벽과 SaaS 애플리케이션 간의 경로 품질 상태를 프로브하는 인터벌을 초 단위로 지정합니다. 기본값은 3초입니다.
HTTP/HTTPS	HTTP 또는 HTTPS URL을 사용하여 모니터링할 SaaS 애플리케이션을 지정합니다. • 모니터링된 **URL** - SaaS 애플리케이션의 HTTP 또는 HTTPS URL입니다. • 프로브 인터벌(초) - 방화벽이 방화벽과 SaaS 애플리케이션 간의 경로 품질 상태를 프로브하는 인터벌(초)을 지정합니다. 기본값은 3초입니다.

개체 > SD-WAN 링크 관리 > 트래픽 분산 프로파일

이 트래픽 배포 프로파일의 경우 방화벽이 세션을 배포하고 경로 품질이 저하될 때 더 나은 경로로 페일오버하는 데 사용하는 방법을 선택합니다. 방화벽이 SD-WAN 트래픽을 포워딩하는 링크를 결정할 때 고려하는 링크 태그를 추가합니다. 생성한 각 SD-WAN 정책 규칙에 트래픽 배포 프로파일을 적용합니다.

	트래픽 분포 프로파일
이름	최대 31자의 영숫자, 하이픈, 공백, 밑줄 및 마침표를 사용하여 트래픽 분포 프로파일의 이름을 입력합니다.
공유	모든 디바이스 그룹(허브 및 브랜치 모두) 에서 이 트래픽 분배 프로필을 사용하려면 공유를 선택합니다.
최적의 경로	비용이 요소가 아니고 애플리케이션이 분기 외부의 모든 경로를 사용하도록 허용할 경우 최적의 사용 가능한 경로를 선택하십시오. 방화벽은 트래픽을 분산하고 목록 기반 경로 품질 메트릭의 모든 링크 태그에 속한 링크 중에서 링크로 페일오버하여 사용자에게 최상의 애플리케이션 경험을 제공합니다.
하향식 우선순위	최후의 수단이나 백업 링크로만 사용하려는 비싸거나 용량이 적은 링크가 있는 경우 하향식 우선 순위 방법을 선택한 다음 해당 링크를 포함하는 태그를 이 프로파일의 링크 태그 목록에서 마지막에 배치합니다. 방화벽은 먼저 목록의 최상위 링크 태그를 사용하여 트래픽을 세션 로드하고 페일오버할 링크를 결정합니다. 상위 링크 태그의 링크 중 어느 것도 자격이 없는 경우 방화벽은 목록의 두 번째 링크 태그에서 링크를 선택합니다. 두 번째 링크 태그의 링크 중 어느 것도 규정되지 않은 경우 방화벽이 마지막 링크 태그에서 규정된 링크를 찾을 때까지 프로세스가 필요에 따라 계속됩니다. 연결된 모든 링크가 오버로드되고 품질 임계값을 충족하는 링크가 없는 경우 방화벽은 최상의 사용 가능한 경로 방법을 사용하여 트래픽을 포워딩할 링크를 선택합니다. 애플리케이션의 지터, 대기 시간 또는 패킷 손실이 구성된 임계값을 초과하는 경우 방화벽은 링크 태그의 하향식 목록 맨 위에서 시작하여 페일오버할 링크를 찾습니다.
가중 세션 분포	규칙과 일치하는 트래픽을 ISP 및 WAN 링크에 수동으로 로드하고 절전 상태에서 페일오버가 필요하지 않은 경우 가중치 세션 배포를 선택합니다. 단일 태그로 그룹화된 인터페이스가 가져올 새 세션의 정적 백분율을 적용할 때 링크의 로드를 수동으로 지정합니다. 대기 시간에 민감하지 않고 대규모 분기 백업 및 대용량 파일 전송과 같이 링크의 대역폭 용량이 많이 필요한 애플리케이션에 이 방법을 선택할 수 있습니다. 링크에 브라운아웃이 발생하면 방화벽이 다른 링크에 대한 일치하는 트래픽을 반영하지 않는다는 점에 유의하십시오.
링크 태그	이 프로파일에 대해 선택한 링크 선택 프로세스 중에 방화벽에서 고려할 링크 태그를 추가합니다. 하향식 우선 순위 방법을 선택한 경우 태그 순서가 중요합니다. 위로 이동 또는 아래로 이동을 사용하여 태그 순서를 변경합니다.
무게	가중 세션 배포 방법을 선택한 경우 추가한 각 링크 태그에 대한 백분율을 입력합니다. 백분율 값의 합은 100%와 같아야 합니다.

개체 > SD-WAN 링크 관리 > 오류 수정 프로파일

SD-WAN 트래픽에 오디오, VoIP 또는 화상 회의와 같이 패킷 손실 또는 손상에 민감한 애플리케이션이 포함된 경우 오류 수정 수단으로 FEC(순방향 오류 수정) 또는 패킷 복사를 적용할 수 있습니다. FEC를 사용하면 수신 방화벽(디코더)이 인코더가 애플리케이션 흐름에 포함하는 패리티 비트를 사용하여 손실되거나 손상된 패킷을 복구할 수 있습니다. 패킷 복사는 애플리케이션 세션이 한 터널에서 두 번째 터널로 복사되는 대체 오류 수정 방법입니다. 두 방법 모두 추가 대역폭과 CPU 오버헤드가 필요합니다. 따라서 FEC 또는 패킷 복사는 이러한 방법의 이점을 얻을 수 있는 애플리케이션에만 적용하십시오. 이러한 방법 중 하나를 사용하려면 오류 수정 프로파일을 만들고 특정 애플리케이션에 대한 SD-WAN 정책 규칙에서 참조하십시오.

(또한 SD-WAN 인터페이스 프로파일에 인터페이스가 오류 수정 프로파일 인터페이스 선택에 적합함을 표시하여 방화벽이 오류 수정을 위해 선택할 수 있는 인터페이스를 지정해야 합니다.)

	오류 수정 프로파일 설정
이름	최대 31자의 영숫자를 사용하여 오류 수정 프로파일을 설명하는 이름을 추가합니다.
공유	오류 수정 프로파일을 Panorama의 모든 디바이스 그룹과 구성을 푸시하는 Multi-VSYS 허브 또는 분기의 모든 가상 시스템에서 사용할 수 있도록 하려면 선택합니다.
재정의 비활성화	관리자가 프로파일을 상속하는 디바이스 그룹에서 이 오류 수정 프로파일의 설정을 무시하지 못하도록 하려면 선택합니다. (공유를 선택한 경우 재정의 비활성화를 사용할 수 없습니다.)
활성화 임계값(패킷 손실 %)	패킷 손실이 이 비율을 초과하면 오류 수정 프로파일이 적용되는 SD-WAN 정책 규칙에서 구성된 애플리케이션에 대해 FEC 또는 패킷 복사가 활성화됩니다. 범위는 1~99입니다. 기본값은 2입니다.
순방향 오류 수정/패킷 복사	FEC(순방향 오류 수정) 또는 패킷 복사를 사용할지의 여부를 선택합니다. 패킷 복사에는 FEC보다 훨씬 더 많은 리소스가 필요합니다.
패킷 손실 보정 비율	(순방향 오류 수정만 해당) 데이터 패킷에 대한 패리티 비트의 비율입니다. 인코더가 디코더로 보내는 데이터 패킷에 대한 패리티 비트의 비율이 높을수록 디코더가 패킷 손실을 복구할 수 있는 확률이 높아집니다. 그러나 비율이 높을수록 더 많은 중복성이 필요하고 따라서 더 많은 대역폭 오버헤드가 필요하며 이는 오류 수정을 달성하기 위한 절충안입니다. 사전 정의된 비율 중 하나를 선택합니다. • **10%(20:2)**(기본값) • **20% (20:4)**

	오류 수정 프로파일 설정
	• **30% (20:6)** • **40% (20:8)** • **50% (20:10)** 패리티 비율은 인코딩 방화벽의 나가는 트래픽에 적용됩니다. 예를 들어 허브 패리티 비율이 50%이고 브랜치 패리티 비율이 20%인 경우 허브는 20%의 비율을 받고 브랜치는 50%의 비율을 받습니다.
복구 기간(밀리초)	수신 방화벽(디코더)이 수신한 패리티 패킷을 사용하여 손실된 데이터 패킷에 대한 패킷 복구를 수행하는 데 사용할 수 있는 최대 시간(밀리초)입니다. 범위는 1 ~ 5,000이고, 기본값은 1,000입니다. 방화벽은 수신한 데이터 패킷을 즉시 대상으로 보냅니다. 데이터 블록의 복구 기간 동안 방화벽은 손실된 데이터 패킷에 대해 패킷 복구를 수행합니다. 복구 기간이 만료되면 해당 블록에 대한 관련 패리티 비트가 삭제됩니다. 인코더는 복구 기간 값을 디코더로 보냅니다. 디코더의 복구 기간 설정은 영향을 주지 않습니다.

일정 > 개체

기본적으로 보안 정책 규칙은 항상 적용됩니다(모든 날짜 및 시간). 보안 정책 규칙을 특정 시간으로 제한하려면 일정을 정의한 다음 적절한 정책에 적용할 수 있습니다. 각 일정에 대해 고정된 날짜 및 시간 범위 또는 되풀이되는 일일 또는 주간 일정을 지정할 수 있습니다. 보안 정책에 일정을 적용하려면 정책 >보안 정책을 참조하십시오.

정의된 일정에 의해 보안 정책 규칙이 호출되면 새 세션만 적용된 보안 정책 규칙의 영향을 받습니다. 기존 세션은 예약된 정책의 영향을 받지 않습니다.

일정 설정	설명
이름	일정 이름(최대 31자)을 입력합니다. 이 이름은 보안 정책을 정의할 때 일정 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유(Panorama만 해당)	일정을 사용할 수 있도록 하려면 다음 옵션을 선택합니다. • Multi-VSYS 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 일정은 개체 탭에서 선택한 가상 시스템에서만 사용할 수 있습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 일정은 개체 탭에서 선택한 디바이스 그룹에서만 사용할 수 있습니다.
재정의 비활성화(Panorama만 해당)	이 옵션을 선택하여 관리자가 일정을 상속하는 디바이스 그룹에서 이 일정의 설정을 재정의하지 못하도록 합니다. 이 선택은 기본적으로 지워지므로 관리자는 일정을 상속하는 모든 디바이스 그룹에 대한 설정을 재정의할 수 있습니다.
반복	일정 유형을 선택합니다(일일, 주간 또는 비반복).
매일	추가를 클릭하고 시작 시간 및 종료 시간을 24시간 형식(HH:MM)으로 지정합니다.
매주	추가를 클릭하고 요일을 선택한 다음 시작 시간과 종료 시간을 24시간 형식으로 지정합니다(HH:MM).
비반복	추가를 클릭하고 시작 날짜, 시작 시간, 종료 날짜 및 종료 시간을 지정합니다.

네트워크

다음 항목에서는 방화벽 네트워크 설정에 대해 설명합니다.

- 네트워크 > 인터페이스
- 네트워크 > 영역
- 네트워크 > VLAN
- 네트워크 > 가상 와이어
- 네트워크 > 가상 라우터
- 네트워크 > 라우팅 > 논리적 라우터
- 네트워크 > IPSec 터널
- 네트워크 > GRE 터널
- 네트워크 > DHCP
- 네트워크 > DNS 프록시
- 네트워크 > 프록시
- 네트워크 > QoS
- Network > LLDP
- 네트워크 > 네트워크 프로파일

더 찾고 계십니까?

PAN-OS 네트워킹 관리자 가이드는 네트워크 인터페이스, 다중 가상 라우터 지원, 정적 경로, 동적 라우팅 프로토콜 및 방화벽에서 네트워킹을 지원하는 기타 주요 기능에 대한 정보를 제공합니다.

네트워크 > 인터페이스

방화벽 인터페이스(포트)를 사용하면 방화벽이 다른 네트워크 디바이스 및 방화벽 내의 다른 인터페이스와 연결할 수 있습니다. 다음 항목에서는 인터페이스 유형과 구성 방법에 대해 설명합니다.

무엇을 찾고 계신가요?	참조
방화벽 인터페이스란 무엇입니까?	방화벽 인터페이스 개요
저는 방화벽 인터페이스를 처음 사용합니다. 방화벽 인터페이스의 구성 요소는 무엇입니까?	방화벽 인터페이스의 공통 빌딩 블록 PA-7000 시리즈 방화벽 인터페이스의 공통 빌딩 블록
나는 이미 방화벽 인터페이스를 이해하고 있습니다. 특정 인터페이스 유형 구성에 대한 정보는 어떻게 찾을 수 있습니까?	물리적 인터페이스(이더넷) 탭 인터페이스 HA 인터페이스 가상 와이어 인터페이스 가상 와이어 하위 인터페이스 PA-7000 시리즈 레이어 2 인터페이스 PA-7000 시리즈 레이어 2 하위 인터페이스 PA-7000 시리즈 레이어 3 인터페이스 레이어 3 인터페이스 레이어 3 서브인터페이스 로그 카드 인터페이스 로그 카드 하위 인터페이스 미러 인터페이스 복호화 통합 이더넷(AE) 인터페이스 그룹 통합 이더넷(AE) 인터페이스 논리적 인터페이스 네트워크 > 인터페이스 > VLAN 네트워크 > 인터페이스 > 루프백 네트워크 > 인터페이스 > 터널 네트워크 > 인터페이스 > SD-WAN

무엇을 찾고 계신가요?	참조
	네트워크 > 인터페이스 > PoE
더 찾고 계십니까?	네트워킹

방화벽 인터페이스 개요

방화벽 데이터 포트의 인터페이스 구성을 통해 트래픽이 방화벽에 들어오고 나갈 수 있습니다. Palo Alto Networks® 방화벽은 다양한 배포를 지원하도록 인터페이스를 구성할 수 있기 때문에 다중 배포 시 동시에 작동할 수 있습니다. 예를 들어 가상 와이어, 레이어 2, 레이어 3 및 탭 모드에 대해 방화벽의 이더넷 인터페이스를 구성할 수 있습니다. 방화벽이 지원하는 인터페이스는 다음과 같습니다.

- 물리적 인터페이스 - 방화벽은 서로 다른 전송 속도로 트래픽을 보내고 받을 수 있는 두 가지 유형의 미디어(구리 및 광섬유)를 지원합니다. 이더넷 인터페이스를 탭, 고가용성(HA), 로그 카드(인터페이스 및 하위 인터페이스), 암호 해독 미러, 가상 와이어(인터페이스 및 하위 인터페이스), 레이어 2(인터페이스 및 하위 인터페이스), 레이어 3(인터페이스 및 하위 인터페이스) 및 집계 이더넷과 같은 유형으로 구성할 수 있습니다. 사용 가능한 인터페이스 유형 및 전송 속도는 하드웨어 모델에 따라 다릅니다.
- 논리적 인터페이스 - 여기에는 VLAN(가상 근거리 통신망) 인터페이스, 루프백 인터페이스, 터널 인터페이스 및 SD-WAN 인터페이스가 포함됩니다. VLAN, SD-WAN 또는 터널 인터페이스를 정의하기 전에 물리적 인터페이스를 설정해야 합니다.

방화벽 인터페이스의 공통 빌딩 블록

네트워크 > 인터페이스를 선택하여 대부분의 인터페이스 유형에 공통적인 구성 요소를 표시하고 구성합니다.

PA-7000 시리즈 방화벽에서 인터페이스를 구성할 때 또는 *Panorama*™를 사용하여 방화벽에서 인터페이스를 구성할 때 고유하거나 다른 구성 요소에 대한 설명은 PA-7000 시리즈 방화벽 인터페이스의 공통 빌딩 블록을 참조하십시오.

방화벽 인터페이스 빌딩 블록	설명
인터페이스(인터페이스 이름)	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다. 그러나 하위 인터페이스, 통합 인터페이스, VLAN 인터페이스, 루프백 인터페이스, 터널 인터페이스 및 SD-WAN 인터페이스에 대한 숫자 서픽스를 추가할 수 있습니다.
인터페이스 유형	이더넷 인터페이스(**Network** > **Interfaces** > 이더넷)의 경우 인터페이스 유형을 선택할 수 있습니다. • 탭 • **HA**

방화벽 인터페이스 빌딩 블록	설명
	• 미러 복호화(VM-Series NSX, Citrix SDX, AWS 및 Azure를 제외한 모든 방화벽에서 지원됨) • 가상 와이어 • 레이어 **2** • 레이어 **3** • 로그 카드(PA-7000 시리즈 방화벽만 해당) • 통합 이더넷
관리 프로파일	이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 관리 프로파일(**Network** > **Interfaces** > **<if-config** > **Advanced** > **Other Info**)을 선택합니다.
링크 상태	이더넷 인터페이스의 경우 링크 상태는 인터페이스가 현재 액세스 가능하고 네트워크를 통해 트래픽을 수신할 수 있는지의 여부를 나타냅니다. • 녹색 - 구성되었고 작동 중 • 빨간색 - 구성되었지만 작동 중지 또는 비활성화됨 • 회색 - 구성되지 않음 링크 상태 위로 마우스를 가져가면 해당 인터페이스에 대한 링크 속도 및 이중 설정을 나타내는 도구 설명이 표시됩니다.
IP 주소	(선택 사항) 이더넷, VLAN, 루프백 또는 터널 인터페이스의 IPv4 또는 IPv6 주소를 구성합니다. IPv4 주소의 경우 인터페이스의 주소 지정 모드(유형)를 선택할 수도 있습니다. 정적, **DHCP** 클라이언트 또는 **PPPoE**.
가상 라우터	인터페이스에 가상 라우터를 할당하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
태그(하위 인터페이스만 해당)	하위 인터페이스에 대한 VLAN 태그(1-4,094)를 입력합니다.
VLAN	네트워크 > 인터페이스 > **VLAN**을 선택한 다음 기존 VLAN을 수정하거나 새 **VLAN**을 추가합니다(네트워크 > VLAN 참조). 없음을 선택하여 인터페이스에서 현재 VLAN 할당을 제거합니다. 레이어 2 인터페이스 간 전환을 활성화하거나 VLAN 인터페이스를 통한 라우팅을 활성화하려면 VLAN 개체를 구성해야 합니다.

방화벽 인터페이스 빌딩 블록	설명
가상 시스템	방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역	인터페이스에 대한 보안 영역(**Network** > **Interfaces** > **<if-config** > **Config**)을 선택하거나 영역을 선택하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
특징	이더넷 인터페이스의 경우 이 열은 다음 기능이 활성화되었는지의 여부를 나타냅니다.  DHCP 클라이언트  DNS 프록시  GlobalProtect™ 게이트웨이 활성화됨  LACP(링크 통합 제어 프로토콜)  LLDP(링크 레이어 검색 프로토콜)  NDP 모니터  NetFlow 프로파일  서비스 품질(QoS) 프로파일  SD-WAN
코멘트	인터페이스 기능 또는 목적에 대한 설명입니다.

PA-7000 시리즈 방화벽 인터페이스의 공통 빌딩 블록

다음 표에서는 PA-7000 시리즈 방화벽에서 인터페이스를 구성하거나 Panorama를 사용하여 방화벽에서 인터페이스를 구성할 때 고유하거나 다른 네트워크 > 인터페이스 > 이더넷 페이지의 구성 요소에 대해 설명합니다. 인터페이스 추가를 클릭하여 새 인터페이스를 생성하거나 기존 인터페이스(예: ethernet1/1)를 선택하여 편집합니다.

PA-7000 시리즈 방화벽에서는 하나의 데이터 포트에 로그 카드 인터페이스을(를) 구성해야 합니다.

PA-7000 시리즈 방화벽 인터페이스 빌딩 블록	설명
슬롯	인터페이스의 슬롯 번호(1-12)를 선택합니다. PA-7000 시리즈 방화벽에만 다중 슬롯이 있습니다. Panorama를 사용하여 다른 방화벽 모델에 대한 인터페이스를 구성하는 경우 슬롯 **1**을 선택합니다.
인터페이스(인터페이스 이름)	선택한 슬롯과 연결된 인터페이스의 이름을 선택합니다.

탭 인터페이스

- 네트워크 > 인터페이스 > 이더넷

탭 인터페이스를 사용하여 포트의 트래픽을 모니터링할 수 있습니다.

탭 인터페이스를 구성하려면 구성되지 않은 인터페이스 이름(예: ethernet1/1)을 클릭하고 다음 정보를 지정합니다.

인터페이스 설정 탭	구성 위치	설명
인터페이스 이름	이더넷 인터페이스	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형		탭을 선택합니다.
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 >

인터페이스 설정 탭	구성 위치	설명
		NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
가상 시스템	이더넷 인터페이스 > 컨피그	방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
링크 속도	이더넷 인터페이스 > 고급 > 링크 설정	인터페이스 속도를 Mbps 단위로 선택하거나 자동을 선택하여 방화벽이 속도를 자동으로 결정하도록 합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
PoE Rsvd Pwr	이더넷 인터페이스 > 고급 > **PoE** 설정 (지원되는 방화벽만 해당)	PoE가 활성화된 경우 할당된 전력량(와트)을 선택합니다.
PoE 활성화		이 인터페이스에서 PoE를 활성화하려면 선택합니다.

HA 인터페이스

- 네트워크 > 인터페이스 > 이더넷

각 고가용성(HA) 인터페이스에는 특정 기능이 있습니다. 한 인터페이스는 구성 동기화 및 하트비트용이고 다른 인터페이스는 상태 동기화용입니다. 능동형/능동형 고가용성이 활성화된 경우 방화벽은 세 번째 HA 인터페이스를 사용하여 패킷을 포워딩할 수 있습니다.

일부 *Palo Alto Networks* 방화벽에는 *HA* 배포에 사용할 전용 물리적 포트*(*제어 링크용 포트와 데이터 링크용 포트*)*가 있습니다. 전용 포트가 없는 방화벽의 경우 *HA*에 사용할 데이터 포트를 지정해야 합니다. *HA*에 대한 자세한 내용은 “디바이스 > 가상 시스템”을 참조하십시오.

HA 인터페이스를 구성하려면 구성되지 않은 인터페이스(예: ethernet1/1)의 이름을 클릭하고 다음 정보를 지정합니다.

HA 인터페이스 설정	구성 위치	설명
인터페이스 이름	이더넷 인터페이스	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형		**HA**를 선택합니다.
링크 속도	이더넷 인터페이스 > 고급 > 링크 설정	인터페이스 속도를 Mbps 단위로 선택하거나 자동을 선택하여 방화벽이 속도를 자동으로 결정하도록 합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
PoE Rsvd Pwr	이더넷 인터페이스 > 고급 > **PoE** 설정 (지원되는 방화벽만 해당)	PoE가 활성화된 경우 할당된 전력량(와트)을 선택합니다.
PoE 활성화		이 인터페이스에서 PoE를 활성화하려면 선택합니다.

가상 와이어 인터페이스

- 네트워크 > 인터페이스 > 이더넷

가상 와이어는 두 개의 이더넷 인터페이스를 논리적으로 함께 바인딩하여 모든 트래픽이 인터페이스 간에 포워딩되거나 선택된 VLAN 태그가 있는 트래픽만 허용합니다(다른 스위칭 또는 라우팅 서비스를 사용할 수 없음). 가상 와이어 서브인터페이스를 생성하여 IP 주소, IP 범위 또는 서브넷에 따라 트래픽을 분류할 수 있습니다. 가상 와이어는 인접 네트워크 디바이스를 변경할 필요가 없습니다. 가상 와이어는 동일한 매체의 두 이더넷 인터페이스(동선 또는 광섬유 모두)를 바인딩하거나 구리 인터페이스를 광섬유 인터페이스에 바인딩할 수 있습니다.

가상 와이어를 설정하려면, 바인딩할 두 인터페이스(네트워크 > 인터페이스 > 이더넷)를 결정하고 다음 표에 설명된 대로 해당 설정을 구성합니다.

가상 와이어에 대해 기존 인터페이스를 사용하는 경우 먼저 연결된 보안 영역에서 인터페이스를 제거합니다.

가상 와이어 인터페이스 설정	구성 위치	설명
인터페이스 이름	이더넷 인터페이스	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형		가상 와이어를 선택합니다.
가상 와이어	이더넷 인터페이스 > 컨피그	가상 와이어를 선택하거나 가상 와이어를 클릭하여 새 와이어를 정의합니다(네트워크 > 가상 와이어). 인터페이스에서 현재 가상 와이어 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
링크 속도	이더넷 인터페이스 > 고급 > 링크 설정	인터페이스 속도를 Mbps 단위로 선택하거나 자동을 선택하여 방화벽이 속도를 자동으로 결정하도록 합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다. 가상 와이어의 두 인터페이스는 동일한 전송 모드를 가져야 합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
PoE Rsvd Pwr	이더넷 인터페이스 > 고급 > **PoE** 설정 (지원되는 방화벽만 해당)	PoE가 활성화된 경우 할당된 전력량(와트)을 선택합니다.
PoE 활성화		이 인터페이스에서 PoE를 활성화하려면 선택합니다.
LLDP 활성화	이더넷 인터페이스 > 고급 > **LLDP**	인터페이스에서 LLDP(Link Layer Discovery Protocol)를 활성화하려면 선택합니다. LLDP는 링크 레이어에서 기능하여 인접 디바이스와 해당 기능을 검색합니다.

가상 와이어 인터페이스 설정	구성 위치	설명
프로파일		LLDP가 활성화된 경우 인터페이스에 할당할 LLDP 프로파일을 선택하거나 **LLDP** 프로파일을 클릭하여 새 프로파일을 생성합니다(네트워크 > 네트워크 프로파일 > LLDP 프로파일 참조). 전역 기본값을 사용하도록 방화벽을 구성하려면 없음을 선택합니다.
HA 수동 상태에서 활성화		LLDP가 활성화된 경우 방화벽이 활성화되기 전에 피어와 LLDP를 사전 협상하도록 HA 수동 방화벽을 구성하도록 선택합니다. LLDP가 활성화되지 않은 경우 방화벽을 통해 LLDP 패킷을 단순히 포워딩하도록 HA 수동 방화벽을 구성하도록 선택합니다.

가상 와이어 서브인터페이스

- 네트워크 > 인터페이스 > 이더넷

가상 와이어(vwire) 서브인터페이스를 사용하면 VLAN 태그 또는 VLAN 태그 및 IP 분류자 조합으로 트래픽을 분리하고 태그가 지정된 트래픽을 다른 영역 및 가상 시스템에 할당한 다음 정의된 기준과 일치하는 트래픽에 대한 보안 정책을 시행할 수 있습니다.

가상 와이어 인터페이스을(를) 추가하려면 해당 인터페이스의 행을 선택한 다음 서브인터페이스 추가를 클릭하고 다음 정보를 지정합니다.

가상 와이어 서브인터페이스 설정	설명
인터페이스 이름	읽기 전용 인터페이스 이름은 선택한 vwire 인터페이스의 이름을 표시합니다. 인접한 필드에 숫자 서픽스(1-9,999)를 입력하여 서브인터페이스를 식별합니다.
코멘트	서브인터페이스에 대한 선택적 설명을 입력합니다.
태그	서브인터페이스에 대한 VLAN 태그(0-4,094)를 입력합니다.
넷플로우 프로파일	인그레스(ingress) 서브인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 없음을 선택하면 서브인터페이스에서 현재 NetFlow 서버 할당이 제거됩니다.
IP 분류자	추가를 클릭하고 IP 주소, IP 범위 또는 서브넷을 입력하여 이 vwire 서브인터페이스의 트래픽을 분류합니다.

가상 와이어 서브인터페이스 설정	설명
가상 와이어	가상 와이어를 선택하거나 가상 와이어를 클릭하여 새 와이어를 정의합니다(네트워크 > 가상 와이어 참조). 서브인터페이스에서 현재 가상 와이어 할당을 제거하려면 없음을 선택합니다.
가상 시스템	방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 서브인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역	서브인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 서브인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.

PA-7000 시리즈 레이어 2 인터페이스

- 네트워크 > 인터페이스 > 이더넷

Network > **Interfaces** > 이더넷을 선택하여 레이어 2 인터페이스를 구성합니다. 구성되지 않은 인터페이스(예: ethernet1/1)의 이름을 클릭하고 다음 정보를 지정합니다.

레이어 **2** 인터페이스 설정	구성 위치	설명
인터페이스 이름	이더넷 인터페이스	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형		레이어**2**를 선택합니다.
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
VLAN	이더넷 인터페이스 > 컨피그	레이어 2 인터페이스 간 전환을 활성화하거나 VLAN 인터페이스를 통한 라우팅을 활성화하려면 기존 VLAN을 선택하거나 **VLAN**을

레이어 2 인터페이스 설정	구성 위치	설명
		클릭하여 새 VLAN을 정의합니다(네트워크 > VLAN 참조). 없음을 선택하여 인터페이스에서 현재 VLAN 할당을 제거합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
링크 속도	이더넷 인터페이스 > 고급	인터페이스 속도(Mbps)를 선택하거나 자동을 선택하여 방화벽이 자동으로 속도를 결정하도록 합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
LLDP 활성화	이더넷 인터페이스 > 고급 > **LLDP**	인터페이스에서 LLDP(Link Layer Discovery Protocol)를 활성화하려면 선택합니다. LLDP는 링크 레이어에서 기능하여 인접 디바이스와 해당 기능을 검색합니다.
LLDP 프로파일		LLDP가 활성화된 경우 인터페이스에 할당할 **LLDP** 프로파일을 선택하거나 LLDP 프로파일을 클릭하여 새 프로파일을 생성합니다(네트워크 > 네트워크 프로파일 > LLDP 프로파일 참조). 전역 기본값을 사용하도록 방화벽을 구성하려면 없음을 선택합니다.
HA 수동 상태에서 활성화		LLDP가 활성화된 경우 방화벽이 활성화되기 전에 HA 수동 방화벽이 피어와 LLDP를 미리 협상할 수 있도록 선택합니다.

PA-7000 시리즈 레이어 2 서브인터페이스

- 네트워크 > 인터페이스 > 이더넷

물리적 레이어 2 인터페이스로 구성된 각 이더넷 포트에 대해 포트가 수신하는 트래픽에 할당된 각 VLAN 태그에 대해 추가 논리적 레이어 2 인터페이스(서브인터페이스)를 정의할 수 있습니다. 레이어 2 서브인터페이스 간 전환을 활성화하려면 동일한 VLAN 개체를 서브인터페이스에 할당합니다.

PA-7000 시리즈 레이어 2 인터페이스를 구성하려면 해당 물리적 인터페이스의 행을 선택한 다음 서브인터페이스 추가를 클릭한 후 다음 정보를 지정합니다.

레이어 2 서브인터페이스 설정	설명
인터페이스 이름	읽기 전용 인터페이스 이름은 선택한 물리적 인터페이스의 이름을 표시합니다. 인접한 필드에 숫자 서픽스(1-9,999)를 입력하여 서브인터페이스를 식별합니다.
코멘트	서브인터페이스에 대한 선택적 설명을 입력합니다.
태그	서브인터페이스에 대한 VLAN 태그(1-4,094)를 입력합니다.
넷플로우 프로파일	수신 서브인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 서브인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
VLAN	레이어 2 인터페이스 간 전환을 활성화하거나 VLAN 인터페이스를 통한 라우팅을 활성화하려면 VLAN을 선택하거나 **VLAN**을 클릭하여 새 VLAN을 정의합니다(네트워크 > VLAN 참조). 서브인터페이스에서 현재 VLAN 할당을 제거하려면 없음을 선택합니다.
가상 시스템	방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 서브인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역	서브인터페이스에 대한 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 서브인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.

PA-7000 시리즈 레이어 3 인터페이스

- 네트워크 > 인터페이스 > 이더넷

레이어 3 인터페이스를 구성하려면 인터페이스(예: ethernet1/1)를 선택한 다음 다음 정보를 지정합니다.

레이어 3 인터페이스 설정	구성 위치	설명
인터페이스 이름	이더넷 인터페이스	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형		**Layer3**을 선택합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
가상 라우터	이더넷 인터페이스 > 컨피그	가상 라우터를 선택하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
SD-WAN 활성화	이더넷 인터페이스 > **IPv4**	이더넷 인터페이스에 대한 SD-WAN 기능을 활성화하려면 **SD-WAN** 활성화를 선택합니다.
유형		인터페이스에 IPv4 주소 유형을 할당하는 방법을 선택합니다. • 정적 - IP 주소를 수동으로 지정해야 합니다. • **PPPoE** - 방화벽은 PPPoE(Point-to-Point Protocol over Ethernet)용 인터페이스를 사용합니다. • **DHCP** 클라이언트—인터페이스가 DHCP(동적 호스트 구성 프로토콜) 클라이언트 역할을 하고 동적으로 할당된 IP 주소를 받을 수 있도록 합니다. 고가용성*(HA)* 능동형/능동형 구성에 있는 방화벽은 *PPPoE* 또는 *DHCP* 클라이언트를 지원하지 않습니다. 선택한 IP 주소 방법에 따라 탭에 표시되는 옵션이 달라집니다.
IPv4 주소 유형 = 정적		

레이어 **3** 인터페이스 설정	구성 위치	설명
IP	이더넷 인터페이스 > **IPv4**	추가를 클릭한 후 다음 단계 중 하나를 수행하여 인터페이스에 대한 고정 IP 주소 및 네트워크 마스크를 지정합니다. • CIDR(Classless Inter-domain Routing) 표기법으로 항목을 입력합니다: *ip_address*/*mask*(예: 192.168.2.0/24). • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • 주소를 클릭하여 **IP** 넷마스크 유형의 주소 개체를 만듭니다. 인터페이스에 대해 여러 IP 주소를 입력할 수 있습니다. 방화벽에서 사용하는 FIB(포워딩 정보 기반)에 따라 최대 IP 주소 수가 결정됩니다. IP 주소를 삭제하려면 주소를 선택한 다음 삭제를 클릭합니다.
IPv4 주소 유형 = **PPPoE**		
사용	이더넷 인터페이스 > **IPv4** > **PPPoE** > 일반	PPPoE 종료를 위한 인터페이스를 활성화하려면 선택합니다.
사용자명		지점간 연결에 대한 사용자명을 입력합니다.
비밀번호/비밀번호 확인		사용자명의 암호를 입력한 다음 확인합니다.
PPPoE 클라이언트 런타임 정보 표시		(선택 사항) 방화벽이 인터넷 서비스 공급자(ISP)와 협상하여 연결을 설정한 매개 변수를 표시하는 대화 상자를 엽니다. 특정 정보는 ISP에 따라 다릅니다.
입증	이더넷 인터페이스 > **IPv4** > **PPPoE** > 고급	PPPoE 통신을 위한 인증 프로토콜 선택: **CHAP**(Challenge-Handshake 인증 프로토콜), **PAP**(암호 인증 프로토콜) 또는 기본 **Auto**(방화벽에서 프로토콜 결정). 인터페이스에서 현재 프로토콜 할당을 제거하려면 없음을 선택합니다.
고정 주소		다음 단계 중 하나를 수행하여 인터넷 서비스 공급자가 할당한 IP 주소를 지정합니다(기본값 없음). • CIDR(Classless Inter-Domain Routing) 표기법으로 항목을 입력합니다: *ip_address*/*mask*(예: 192.168.2.0/24). • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • 주소를 클릭하여 **IP** 넷마스크 유형의 주소 개체를 만듭니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
		• 인터페이스에서 현재 주소 할당을 제거하려면 없음을 선택합니다.
피어를 가리키는 기본 경로 자동 생성		연결 시 PPPoE 피어를 가리키는 기본 경로를 자동으로 생성하려면 선택합니다.
기본 경로 측정항목		(선택 사항) 방화벽과 인터넷 서비스 공급자 간의 경로에 대해 기본 경로와 연결하고 경로 선택에 사용할 경로 메트릭(우선 순위 수준)을 입력합니다(범위는 1~65,535). 숫자 값이 감소할수록 우선 순위 수준이 높아집니다.
액세스 집중 디바이스		(선택 사항) 방화벽이 연결되는 인터넷 서비스 공급자 측의 액세스 집중 디바이스 이름을 입력합니다(기본값 없음).
서비스		(선택 사항) 서비스 문자열을 입력합니다(기본값 없음).
수동		수동 모드를 사용하려면 선택합니다. 수동 모드에서 PPPoE 엔드포인트은 액세스 집중 디바이스가 첫 번째 프레임을 보낼 때까지 기다립니다.
IPv4 주소 유형 = **DHCP**		
사용	이더넷 인터페이스 > **IPv4**	인터페이스에서 DHCP 클라이언트를 활성화하려면 선택합니다.
서버에서 제공하는 기본 게이트웨이를 가리키는 기본 경로 자동 생성		DHCP 서버가 제공하는 기본 게이트웨이를 가리키는 기본 경로를 자동으로 생성하려면 선택합니다.
호스트네임 보내기		방화벽(DHCP 클라이언트)이 인터페이스의 호스트네임(옵션 12)을 DHCP 서버로 보내도록 하려면 선택합니다. 호스트 이름을 보내는 경우 방화벽의 호스트 이름은 기본적으로 호스트 이름 필드에서 선택됩니다. 해당 이름을 보내거나 사용자 지정 호스트 이름(대소문자, 숫자, 마침표, 하이픈 및 밑줄을 포함하여 최대 64자)을 입력할 수 있습니다.
기본 경로 측정항목		방화벽과 DHCP 서버 사이의 경로의 경우 선택적으로 기본 경로와 연결하고 경로 선택에 사용할 경로 메트릭(우선 순위 수준)을

레이어 **3** 인터페이스 설정	구성 위치	설명
		입력합니다(범위는 1에서 65,535, 기본값 없음). 숫자 값이 감소할수록 우선 순위 수준이 높아집니다.
DHCP 클라이언트 런타임 정보 표시		DHCP 임대 상태, 동적 IP 주소 할당, 서브넷 마스크, 게이트웨이 및 서버 설정(DNS, NTP, 도메인, WINS, NIS, POP3 및 SMTP)을 포함하여 DHCP 서버에서 수신한 모든 설정을 표시하려면 선택합니다.
인터페이스에서 IPv6 활성화	이더넷 인터페이스 > **IPv6**	이 인터페이스에서 IPv6 주소 지정을 활성화하려면 선택합니다.
인터페이스 ID		64비트 확장 고유 식별자(EUI-64)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 **ID**를 호스트 부분으로 사용 옵션을 활성화하면 방화벽은 인터페이스 ID를 해당 주소의 호스트 부분으로 사용합니다.
주소		추가를 클릭하고 각 IPv6 주소에 대해 다음 매개변수를 구성합니다. • 주소 - IPv6 주소와 프리픽스 길이를 입력합니다(예: 2001:400:f00::1/64). 기존 IPv6 주소 개체를 선택하거나 주소를 클릭하여 주소 개체를 만들 수도 있습니다. • **Enable address on interface** - 인터페이스에서 IPv6 주소를 활성화하려면 선택합니다. • 인터페이스 **ID**를 호스트 부분으로 사용 - 인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다. • **Anycast** - 가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다. • 라우터 알림 보내기 - 이 IP 주소에 대해 라우터 알림(RA)을 활성화하려면 선택합니다. (인터페이스에서 글로벌 **Enable**

레이어 **3** 인터페이스 설정	구성 위치	설명
		Router Advertisement 옵션도 활성화해야 합니다.) RA에 대한 자세한 내용은 라우터 알림 활성화를 참조하십시오. 나머지 필드는 RA를 활성화한 경우에만 적용됩니다. • 유효 시간 - 방화벽이 주소를 유효한 것으로 간주하는 시간(초)입니다. 유효 시간은 기본 유효 시간(기본값: 2,592,000) 이상이어야 합니다. • 선호 유효 시간 - 유효한 주소가 선호되는 시간(초)입니다. 즉, 방화벽이 트래픽을 보내고 받는 데 사용할 수 있습니다. 기본 유효 시간이 만료되면 방화벽은 주소를 사용하여 새 연결을 설정할 수 없지만 기존 연결은 유효 시간이 만료될 때까지 유효합니다(기본값은 604,800). • 온링크 - 프리픽스 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지의 여부를 선택합니다. • **Autonomous**—시스템이 보급된 프리픽스를 인터페이스 ID와 결합하여 IP 주소를 독립적으로 생성할 수 있는지의 여부를 선택합니다.
중복 주소 감지 활성화	이더넷 인터페이스 > **IPv6** > 주소 확인	DAD(중복 주소 감지)를 활성화하도록 선택한 다음 이 섹션의 다른 필드를 구성합니다.
DAD 시도		이웃 식별 시도가 실패하기 전에 이웃 요청 인터벌(**NS** 인터벌) 내에서 DAD 시도 횟수를 지정합니다(범위는 1~10, 기본값은 1).
도달 가능 시간		쿼리 및 응답이 성공한 후 인접 네트워크에 도달할 수 있는 시간을 초 단위로 지정합니다(범위는 10~36,000, 기본값은 30).
NS 인터벌(이웃 모집 인터벌)		실패가 표시되기 전에 DAD 시도에 대한 시간(초)을 지정하십시오(범위는 1 - 10, 기본값은 1).
NDP 모니터링 작동		NDP(Neighbor Discovery Protocol) 모니터링을 활성화하려면 선택합니다. 활성화하면 NDP 모니터(기능 열에서 )를 선택한 다음 IPv6 주소, 해당 MAC 주소 및 User-ID(최상의 경우 기준)와 같이 방화벽이 검색한 이웃에 대한 정보를 볼 수 있습니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
라우터 알림 활성화	이더넷 인터페이스 > **IPv6** > 라우터 알림	IPv6 인터페이스에서 상태 비저장 주소 자동 구성(SLAAC)을 제공하려면 이 섹션의 다른 필드를 선택한 다음 구성합니다. 라우터 알림(RA) 메시지를 수신하는 IPv6 DNS 클라이언트는 이 정보를 사용합니다. RA를 사용하면 방화벽이 정적으로 구성되지 않은 IPv6 호스트의 기본 게이트웨이 역할을 하고 호스트에 주소 구성을 위한 IPv6 프리픽스를 제공할 수 있습니다. 이 기능과 함께 별도의 DHCPv6 서버를 사용하여 클라이언트에 DNS 및 기타 설정을 제공할 수 있습니다. 이것은 인터페이스에 대한 전역 설정입니다. 개별 IP 주소에 대한 RA 옵션을 설정하려면 IP 주소 테이블에서 추가를 클릭하고 주소를 구성합니다. 임의의 IP 주소에 대해 RA 옵션을 설정하는 경우 인터페이스에 대해 **Enable Router Advertisement**(라우터 알림 활성화) 옵션을 선택해야 합니다.
최소 인터벌(초)		방화벽이 보낼 RA 사이의 최소 인터벌(초)을 지정합니다(범위는 3~1,350, 기본값은 200). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
최대 인터벌(초)		방화벽이 보낼 RA 간의 최대 인터벌(초)을 지정합니다(범위는 4~1,800, 기본값은 600). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
홉 제한		나가는 패킷에 대해 클라이언트에 적용할 홉 제한을 지정합니다(범위는 1~255, 기본값은 64). 홉 제한이 없는 경우 0을 입력합니다.
링크 MTU		클라이언트에 적용할 링크 최대 전송 단위(MTU)를 지정합니다. 링크 없음 MTU에 대해 지정되지 않음을 선택합니다(범위는 1,280 ~ 9,192, 기본값은 지정되지 않음).
도달 가능한 시간(ms)		클라이언트가 연결 확인 메시지를 수신한 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능 시간(밀리초)을 지정합니다. 도달할 수 없는 시간 값에 대해 지정되지 않음을 선택합니다(범위는 0 ~ 3,600,000, 기본값은 지정되지 않음).
재전송 시간(ms)		클라이언트가 인접 요청 메시지를 재전송하기 전에 대기하는 시간(밀리초)을 결정하는 재전송 타이머를 지정합니다. 재전

레이어 **3** 인터페이스 설정	구성 위치	설명
		송 시간이 없는 경우 지정되지 않음을 선택합니다(범위는 0 ~ 4,294,967,295, 기본값은 지정되지 않음).
라우터 유효 시간(초)		클라이언트가 방화벽을 기본 게이트웨이로 사용할 기간을 지정합니다(범위는 0~9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.
라우터 기본 설정		네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트는 이 필드를 사용하여 기본 라우터를 선택합니다. RA가 방화벽 라우터를 세그먼트의 다른 라우터에 비해 높음, 중간(기본값) 또는 낮음 우선 순위를 갖는 것으로 광고할지의 여부를 선택합니다.
관리 구성		DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
일관성 확인	이더넷 인터페이스 > **IPv6** > 라우터 알림**(**계속**)**	방화벽이 다른 라우터에서 보낸 RA가 링크에 대한 일관된 정보를 광고하는지 확인하도록 하려면 선택합니다. 방화벽은 시스템 로그에 불일치를 기록합니다. 유형은 **ipv6nd**입니다.
기타 구성		DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
라우터 광고에 DNS 정보 포함	이더넷 인터페이스 > **IPv6** > **DNS** 지원	방화벽이 이 IPv6 이더넷 인터페이스에서 NDP RA(라우터 광고) 메시지의 DNS 정보를 보낼 수 있도록 하려면 선택합니다. 이 표의 다른 DNS 지원 필드는 이 옵션을 선택한 후에만 표시됩니다.
서버		이 IPv6 이더넷 인터페이스에서 NDP 라우터 광고를 보낼 방화벽에 대한 하나 이상의 재귀 DNS(RDNS) 서버 주소를 추가합니다. RDNS 서버는 루트 DNS와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에 대한 NDP 라우터 광고에서 위에서 아래로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있습니다. 그러면 받는 사람은 해당 주소를 같은 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서

레이어 3 인터페이스 설정	구성 위치	설명
		를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다.
유효 기간		IPv6 DNS 클라이언트가 라우터 광고를 수신한 후 클라이언트가 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)에서 최대 인터벌의 두 배, 기본값은 1,200).
서픽스		DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(서픽스)을 추가하고 구성합니다. 최대 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하여 DNS 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "품질"에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 해당 이름에 추가한 다음 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가 "company.com"인 경우 라우터의 결과 DNS 쿼리는 FQDN "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록의 모든 서픽스를 시도할 때까지 DNS 서픽스를 시도합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 해당 주소를 사용하는 수신자에게 보내는 NDP 라우터 광고에서 방화벽이 위에서 아래로 순서대로 보내는 DNS 검색 목록에 대해 최대 8개의 도메인 이름(서픽스)을 구성할 수 있습니다. 서픽스를 선택한 다음 위로 이동 또는 아래로 이동하여 순서를 변경하거나 더 이상 필요하지 않은 경우 서픽스를 삭제합니다.
유효 기간		IPv6 DNS 클라이언트가 DNS 검색 목록의 도메인 이름(서픽스)을 사용할 수 있다는 라우터 광고를 수신한 후 최대 시

레이어 **3** 인터페이스 설정	구성 위치	설명
		간(초)을 입력합니다(범위는 최대 인터벌(초)의 값에서 최대 인터벌의 두 배, 기본값은 1,200입니다).
SD-WAN 인터페이스 상태	이더넷 인터페이스 > **SD-WAN**	**IPv4** 탭에서 **SD-WAN** 활성화를 선택한 경우 방화벽은 SD-WAN ##### ### #####. ####. **SD-WAN**을 활성화하지 않은 경우 #####을 나타냅니다.
SD-WAN 인터페이스 프로파일		SD-WAN 인터페이스 프로파일을 선택하여 이 이더넷 인터페이스에 적용하거나 새 SD-WAN 인터페이스 프로파일을 추가합니다. *SD-WAN* 인터페이스 프로파일을 적용하려면 먼저 인터페이스에 대해 ***SD-WAN***을 활성화해야 합니다.
업스트림 NAT		SD-WAN 허브 또는 분기가 NAT를 수행하는 디바이스 뒤에 있는 경우 허브 또는 분기에 대해 업스트림 NAT를 활성화합니다.
NAT IP 주소 유형		IP 주소 할당 유형을 선택한 다음 해당 NAT 수행 디바이스에서 공용 인터페이스의 FQDN 또는 IP 주소를 지정하거나 DDNS가 주소를 파생하도록 지정합니다. 따라서 Auto VPN은 주소를 허브 또는 분기의 터널 엔드포인트로 사용할 수 있습니다. • 고정 **IP** - 유형을 **IP** 주소 또는 **FQDN**으로 선택한 다음 IPv4 주소 또는 FQDN을 입력합니다. • **DDNS** - DDNS(동적 DNS)는 업스트림 NAT 디바이스의 IP 주소를 파생합니다.
링크 속도	이더넷 인터페이스 > 고급	인터페이스 속도를 Mbps(**10**, **100** 또는 **1000**) 단위로 선택하거나 자동을 선택합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
관리 프로파일	이더넷 인터페이스 > 고급 > 다른 정보	이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 프로파일을 선택

레이어 3 인터페이스 설정	구성 위치	설명
		합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(576~9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방화벽은 패킷이 너무 큼을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.
TCP MSS 조정		인터페이스 MTU 바이트 크기 내의 모든 헤더에 대한 바이트를 수용하도록 최대 세그먼트 크기(MSS)를 조정하려면 선택합니다. MTU 바이트 크기에서 MSS 조정 크기를 뺀 값은 IP 프로토콜에 따라 달라지는 MSS 바이트 크기와 같습니다. • **IPv4 MSS** 조정 크기 - 범위는 40~300이고, 기본값은 40입니다. • **IPv6 MSS** 조정 크기 - 범위는 60~300이고, 기본값은 60입니다. 이 설정을 사용하여 네트워크를 통한 터널에 더 작은 MSS가 필요한 경우를 해결하십시오. 패킷이 조각화 없이 MSS보다 더 많은 바이트를 갖는 경우 이 설정을 사용하면 조정할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로 VLAN 태그가 있는 MPLS 헤더 또는 터널링된 트래픽과 같은 항목에 대해 바이트를 허용하도록 MSS 조정 크기를 구성하는 것이 좋습니다.
태그가 지정되지 않은 서브인터페이스		이 Layer 3 인터페이스에 속하는 모든 서브인터페이스에 태그가 지정되지 않도록 지정합니다. PAN-OS®는 패킷 대상에 따라 태그가 지정되지 않은 서브인터페이스를 수신 인터페이스로 선택합니다. 대상이 태그가 지정되지 않은 서브인터페이스의 IP 주소인 경우 서브인터페이스에 매핑됩니다. 이것은 또한 역방향 패킷의 소스 주소가 태그가 지정되지 않은 서브인터페이스의 IP 주소로 변환되어야 함을 의미합니다. 이 분류 메커니즘의 부산물은 모든 멀티캐스트 및 브로드캐스트 패킷이 서브인터페이스가 아닌 기본 인터페이스에 할당됩니다. OSPF(Open Shortest Path First)는 멀티캐스트를 사용하기 때문에 방화벽은 태그가 지정되지 않은 서브인터페이스에서 멀티캐스트를 지원하지 않습니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
IP 주소 MAC 주소	이더넷 인터페이스 > 고급 > **ARP** 항목	하나 이상의 고정 ARP(Address Resolution Protocol) 항목을 추가하려면 추가를 클릭하고 IP 주소 및 연결된 하드웨어(MAC) 주소를 입력합니다. 항목을 삭제하려면 항목을 선택한 다음 삭제를 클릭합니다. 고정 ARP 항목은 ARP 처리를 줄이고 지정된 주소에 대한 중간자 공격을 방지합니다.
IPv6 주소 MAC 주소	이더넷 인터페이스 > 고급 > **ND** 항목	NDP(Neighbor Discovery Protocol)에 대한 네이버 정보를 제공하려면 추가를 클릭하고 네이버의 IP 주소와 MAC 주소를 입력합니다.
NDP 프록시 사용	이더넷 인터페이스 > 고급 > **NDP** 프록시	인터페이스에 대해 NDP(Neighbor Discovery Protocol) 프록시를 활성화하려면 선택합니다. 방화벽은 이 목록의 IPv6 주소에 대한 MAC 주소를 요청하는 ND 패킷에 응답합니다. ND 응답에서 방화벽은 인터페이스에 대한 자체 MAC 주소를 보내 해당 주소로 향하는 패킷에 응답하여 프록시 역할을 할 것임을 나타냅니다. NPTv6(Network Prefix Translation IPv6)을 사용하는 경우 **NDP** 프록시 사용을 선택하는 것이 좋습니다. **NDP** 프록시 사용을 선택한 경우 검색 문자열을 입력하고 필터 적용(→)을 클릭하여 여러 주소 항목을 필터링할 수 있습니다.
주소		추가를 클릭하여 방화벽이 NDP 프록시로 작동할 IPv6 주소, IP 범위, IPv6 서브넷 또는 주소 개체를 하나 이상 입력합니다. 이상적으로는 이러한 주소 중 하나가 NPTv6의 소스 번역 주소와 동일합니다. 주소의 순서는 중요하지 않습니다. 주소가 하위 네트워크인 경우 방화벽은 서브넷의 모든 주소에 대해 ND 응답을 보내므로 방화벽의 IPv6 이웃도 추가한 다음 무효를 선택하여 방화벽이 이러한 IP 주소에 응답하지 않도록 지시하는 것이 좋습니다.
무효		해당 주소에 대해 NDP 프록시를 방지하려면 주소에 대해 부정을 선택합니다. 지정된 IP 주소 범위 또는 IP 서브넷의 하위 집합을 무효화할 수 있습니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
LLDP 활성화	이더넷 인터페이스 > 고급 > **LLDP**	인터페이스에서 LLDP(Link Layer Discovery Protocol)를 활성화하려면 선택합니다. LLDP는 링크 레이어에서 기능하여 인접 디바이스와 해당 기능을 검색합니다.
LLDP 프로파일		LLDP가 활성화된 경우 인터페이스에 할당할 **LLDP** 프로파일을 선택하거나 LLDP 프로파일을 클릭하여 새 프로파일을 생성합니다(네트워크 > 네트워크 프로파일 > LLDP 프로파일 참조). 전역 기본값을 사용하도록 방화벽을 구성하려면 없음을 선택합니다.
HA 수동 상태에서 활성화		LLDP가 활성화된 경우 방화벽이 HA 수동 방화벽으로서 방화벽이 활성화되기 전에 피어와 LLDP를 미리 협상하도록 허용하려면 선택합니다.
설정	이더넷 인터페이스 > 고급 > **DDNS**	설정을 선택하여 DDNS 필드를 구성할 수 있도록 합니다.
활성화		인터페이스에서 DDNS를 활성화합니다. DDNS를 구성하려면 처음에 활성화해야 합니다. (DDNS 설정이 완료되지 않은 경우 부분 설정을 잃지 않도록 활성화하지 않고 저장할 수 있습니다.)
업데이트 인터벌(일)		FQDN에 매핑된 IP 주소를 업데이트하기 위해 방화벽이 DDNS 서버에 보내는 업데이트 인터벌(일)을 입력합니다(범위는 1~30, 기본값은 1). 또한 방화벽은 *DHCP* 서버에서 인터페이스에 대한 새 *IP* 주소를 수신하면 *DDNS*를 업데이트합니다.
인증서 프로파일		DDNS 서비스를 확인하기 위해 인증서 프로파일을 생성합니다. DDNS 서비스는 인증 기관(CA)이 서명한 인증서를 방화벽에 제공합니다.
호스트네임		DDNS 서버에 등록된 인터페이스의 호스트 이름(예: host123.domain123.com, host123)을 입력합니다. 방화벽은 구문이 도메인 이름에 대해 DNS에서 허용하는 유효한 문자를 사용하는지 확인하는 경우를 제외하고 호스트 이름의 유효성을 검사하지 않습니다.
공급자		이 인터페이스에 DDNS 서비스를 제공하는 DDNS 공급자(및 버전)를 선택하십시오.

레이어 3 인터페이스 설정	구성 위치	설명
		• **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS** - SD-WAN AE 인터페이스 및 SD-WAN Layer 3 서브인터페이스에 사용해야 합니다. 방화벽에서 특정 날짜까지 단계적으로 중단될 것이라고 표시하는 *DDNS* 서비스의 이전 버전을 선택하는 경우 최신 버전으로 이동합니다. 공급자 이름 뒤에 오는 이름 및 값 필드는 공급자별로 다릅니다. 읽기 전용 필드는 방화벽이 DDNS 서비스에 연결하는 데 사용하는 매개변수를 알려줍니다. DDNS 서비스가 사용자에게 제공하는 비밀번호 및 DDNS 서버에서 응답을 수신하지 않는 경우 방화벽이 사용하는 타임아웃와 같은 다른 필드를 구성합니다.
IPv4 탭 - IP		인터페이스에 구성된 IPv4 주소를 추가하고 선택합니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
IPv6 탭 - IPv6		인터페이스에 구성된 IPv6 주소를 추가하고 선택합니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
런타임 정보 표시		DDNS 등록을 표시합니다. DDNS 공급자, 확인된 FQDN 및 기본 IP 주소를 나타내는 별표(*)가 있는 매핑된 IP 주소. 각 DDNS 공급자에는 문제 해결을 위해 호스트 이름 업데이트 상태와 반환 날짜를 나타내는 고유한 반환 코드가 있습니다.

레이어 3 인터페이스

- 네트워크 > 인터페이스 > 이더넷

트래픽을 라우팅할 수 있는 이더넷 레이어 3 인터페이스를 구성합니다.

레이어 3 인터페이스 설정	구성 위치	설명
인터페이스 이름	**Layer3** 인터페이스	읽기 전용 인터페이스 이름 필드에는 선택한 물리적 인터페이스의 이름이 표시됩니다.
코멘트		인터페이스에 대한 사용자 친화적인 설명을 입력합니다.
인터페이스 유형		**Layer3**을 선택합니다.
NetFlow 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 NetFlow 프로파일을 선택하거나 **NetFlow** 프로파일을 선택하여 새 프로파일을 만듭니다(디바이스 > 서버 프로파일 > NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
가상 라우터	**Layer3** 인터페이스 > 구성	인터페이스에 가상 라우터를 할당하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
논리적 라우터		논리적 라우터를 인터페이스에 할당하거나 논리적 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 라우팅 > 논리적 라우터 참조). 인터페이스에서 현재 논리적 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대해 가상 시스템(vsys)을 선택하거나 가상 시스템을 선택하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 선택하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
SD-WAN 활성화	**Layer3** 인터페이스 > **IPv4**	이더넷 인터페이스에 대한 SD-WAN 기능을 활성화하려면 **SD-WAN** 활성화를 선택합니다.
Bonjour 리플렉터 활성화		(PA-220, PA-800 및 PA-3200 시리즈만 해당) 이 옵션을 활성화하면 방화벽은 Bonjour 멀티캐스트 광고와 쿼리를 이 인터페이스에서 수신하고 이 인터페이스로 포워딩하여 이 인터페이스를 활성화한 다른 모든 L3 및 AE 인터페이스와 서브인터페이스로 포워딩합니다. 옵션. 이는 보안 또는 관리 목적으로 트래픽을 라우팅하기 위해 세분화를 사용하는 네트워크 환경에서 사용자 액세스 및 디바이스

레이어 **3** 인터페이스 설정	구성 위치	설명
		검색 가능성을 보장하는 데 도움이 됩니다. 최대 16개의 인터페이스에서 이 옵션을 활성화할 수 있습니다.
IP	**Layer3** 인터페이스 > **IPv4,** 유형 = 정적	인터페이스 또는 AE 인터페이스에 대한 고정 IP 주소 및 네트워크 마스크를 지정하려면 다음 단계 중 하나를 추가하고 수행합니다. • CIDR(Classless Inter-Domain Routing) 표기법으로 항목을 입력합니다: *ip_address*/*mask*(예: 192.168.2.0/24). • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • **IP** 넷마스크 유형의 주소 개체를 만듭니다. 인터페이스에 대해 여러 IP 주소를 입력할 수 있습니다. 시스템에서 사용하는 FIB(포워딩 정보 기반)에 따라 최대 IP 주소 수가 결정됩니다. 더 이상 필요하지 않은 IP 주소는 삭제하십시오.
SD-WAN 게이트웨이		**SD-WAN** 활성화를 선택한 경우 SD-WAN 게이트웨이의 IPv4 주소를 입력합니다.
사용	**Layer3** 인터페이스 > **IPv4** > 일반, 유형 = **PPPoE**	**Enable**을 선택하여 PPPoE(Point-to-Point Protocol over Ethernet) 종료를 위한 인터페이스를 활성화합니다. 인터페이스는 DSL 모뎀이 있지만 연결을 종료할 다른 PPPoE 디바이스가 없는 DSL(디지털 가입자 회선) 환경에서 연결을 지원하기 위한 PPPoE 종료 지점입니다.
사용자명		지점 간 연결을 위해 ISP가 제공한 사용자명을 입력합니다.
비밀번호 및 비밀번호 확인		비밀번호를 입력하고 비밀번호를 확인하세요.
PPPoE 클라이언트 런타임 정보 표시		PPPoE 인터페이스에 대한 정보를 보려면 선택합니다.
인증	**Layer3** 인터페이스 > **IPv4** > 고급, 유형 = **PPPoE**	인증 방법 선택: • 없음 - (기본값) PPPoE 인터페이스에 인증이 없습니다. • **CHAP** - 방화벽은 PPPoE 인터페이스에서 Challenge Handshake 인증 프로토콜(RFC-1994)을 사용합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
		• **PAP** - 방화벽은 PPPoE 인터페이스에서 PAP(암호 인증 프로토콜)를 사용합니다. PAP는 CHAP보다 덜 안전합니다. PAP는 사용자명과 암호를 일반 텍스트로 보냅니다. • **auto** - 방화벽이 PPPoE 서버와 인증 방법(CHAP 또는 PAP)을 협상합니다.
고정 주소		PPPoE 서버에서 원하는 IPv4 주소를 요청합니다. PPPoE 서버는 해당 주소 또는 다른 주소를 할당할 수 있습니다.
피어를 가리키는 기본 경로 자동 생성		PPPoE 서버가 제공하는 기본 게이트웨이를 가리키는 기본 경로를 자동으로 생성하려면 이 옵션을 선택합니다.
기본 경로 측정 항목		PPPoE 연결에 대한 기본 경로 메트릭(우선 순위 수준)을 입력합니다(기본값은 10). 경로 선택 시 번호가 낮은 경로가 우선 순위가 높습니다. 예를 들어 메트릭이 10인 경로는 메트릭이 100인 경로보다 먼저 사용됩니다.
액세스 집중 디바이스		ISP가 액세스 집중 디바이스의 이름을 제공한 경우 입력하십시오. 방화벽은 IPS 측에서 이 액세스 집중 디바이스와 연결됩니다. 0~255자의 문자열 값입니다.
서비스		방화벽(PPPoE 클라이언트)은 PPPoE 서버에 원하는 서비스 요청을 제공할 수 있습니다. 0~255자의 문자열 값입니다.
수동형		방화벽(PPPOE 클라이언트)은 PPPoE 서버가 연결을 시작할 때까지 기다립니다. 이것이 활성화되어 있지 않으면 방화벽이 연결을 시작합니다.
사용	**Layer3** 인터페이스 > **IPv4,** 유형 **= DHCP** 클라이언트	인터페이스가 DHCP(Dynamic Host Configuration Protocol) 클라이언트 역할을 하고 동적으로 할당된 IP 주소를 수신하도록 설정합니다. 고가용성*(HA)* 능동형/능동형 구성에 있는 방화벽은 *DHCP* 클라이언트를 지원하지 않습니다.
서버에서 제공하는 기본 게이트웨이를 가리		방화벽이 기본 게이트웨이에 대한 고정 경로를 생성하도록 하려면 이 옵션을 선택합니다. 기본 게이트웨이는 클라이언트가 방화벽의 라우팅 테이블에서 경로를 유지할 필요가 없는 많은 대상에 액세스하려고 할 때 유용합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
키는 기본 경로 자동 생성		
호스트 이름 보내기		DHCP 클라이언트 인터페이스에 호스트네임을 할당하고 해당 호스트네임(옵션 12)을 DNS 서버에 등록할 수 있는 DHCP 서버로 보내려면 이 옵션을 선택합니다. 그런 다음 DNS 서버는 호스트네임-동적 IP 주소 확인을 자동으로 관리할 수 있습니다. 외부 호스트는 호스트 이름으로 인터페이스를 식별할 수 있습니다. 기본값은 디바이스 > 설정 > 관리 > 일반 설정에서 설정한 방화벽 호스트 이름인 ### #####을 나타냅니다. 또는 인터페이스의 호스트 이름을 입력합니다. 이 이름은 대문자와 소문자, 숫자, 마침표, 하이픈, 밑줄을 포함하여 최대 64자까지 가능합니다.
기본 경로 측정 항목	**Layer3** 인터페이스 > **IPv4,** 유형 **= DHCP** 클라이언트	방화벽과 DHCP 서버 간의 경로에 대한 기본 경로 메트릭(우선 순위 수준)을 입력합니다(범위는 1~65,535이며 기본 메트릭은 없음). 경로 선택 시 번호가 낮은 경로가 우선 순위가 높습니다. 예를 들어 메트릭이 10인 경로는 메트릭이 100인 경로보다 먼저 사용됩니다.
DHCP 클라이언트 런타임 정보 표시		클라이언트가 DHCP 리스 상태, 동적 IP 주소 할당, 서브넷 마스크, 게이트웨이 및 서버 설정(DNS, NTP, 도메인, WINS, NIS, POP3 및 SMTP)을 포함한 DHCP 서버에서 상속한 모든 설정을 보려면 이 옵션을 선택하십시오.
인터페이스에서 IPv6 활성화	**Layer3** 인터페이스 > **IPv6**	인터페이스에서 IPv6 주소 지정을 활성화하려면 선택합니다.
인터페이스 ID		64비트 확장 고유 식별자(**EUI-64**)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 **ID**를 호스트 부분으로 사용 옵션을 활성화하면 방화벽은 인터페이스 ID를 해당 주소의 호스트 부분으로 사용합니다.
주소	**Layer3** 인터페이스 > **IPv6** > 주소 할당**,** 유형 **=** 정적	IPv6 주소 및 프리픽스 길이를 추가합니다(예: 2001:400:f00::1/64). 또는 기존 IPv6 주소 개체를 선택하거나 새 IPv6 주소 개체를 만듭니다.
인터페이스에서 주소 활성화		인터페이스에서 IPv6 주소를 활성화하려면 선택합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
인터페이스 ID를 호스트 부분으로 사용		인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다.
애니캐스트		가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다.
라우터 알림 보내기	**Layer3** 인터페이스 > **IPv6** > 주소 할당, 유형 = 정적	이 IP 주소에 대해 라우터 광고(RA)를 활성화하려면 선택합니다. (인터페이스에서 글로벌 **Enable Router Advertisement** 옵션도 활성화해야 합니다.) RA에 대한 자세한 내용은 이 표에서 라우터 알림 활성화를 참조하십시오. 다음 필드는 라우터 보급을 활성화한 경우에만 적용됩니다. • 유효 시간 - 방화벽이 주소가 유효한 것으로 간주하는 시간(초)입니다. 유효한 유효 시간은 기본 유효 시간과 같거나 초과해야 합니다. 기본값은 2,592,000입니다. • **Preferred Lifetime** - 유효한 주소가 선호되는 시간(초)입니다. 즉, 방화벽이 트래픽을 보내고 받는 데 사용할 수 있습니다. 기본 유효 시간이 만료되면 방화벽은 주소를 사용하여 새 연결을 설정할 수 없지만 기존 연결은 유효 시간이 만료될 때까지 유효합니다. 기본값은 604,800입니다. • 온링크 - 프리픽스 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지의 여부를 선택합니다. • **Autonomous**—시스템이 보급된 프리픽스를 인터페이스 ID와 결합하여 IP 주소를 독립적으로 생성할 수 있는지의 여부를 선택합니다.
라우터 알림 경로 수락	**Layer3** 인터페이스 > **IPv6** > 주소 할당, 유형 **= DHCPv6** 클라이언트	DHCPv6 클라이언트가 DHCPv6 서버에서 RA를 수락하도록 허용하려면 선택합니다.
기본 경로 측정항목		인터페이스에서 ISP까지의 경로에 대한 기본 경로 메트릭을 입력합니다. 범위는 1~65,535입니다. 기본값은 10입니다.
기본 설정		두 개의 인터페이스(각각 중복성을 위해 다른 ISP에 연결됨)가 있는 경우 한 ISP에 대한 인터페이스에 다른 ISP에 대한 인터페이스보다 높은 기본 설정을 할당할 수 있도록 DHCPv6 클라이언트 인터페이스의 기본 설정(낮음, 중간 또는 높음)을 선택합니다. 기본 인터페이스에 연결된 ISP는 호스트 인터페이스에 보낼 위임된 접두사를 제공하는 ISP가 됩니다. 인터페이스의 기본 설정이 동일한 경우 두

레이어 **3** 인터페이스 설정	구성 위치	설명
		ISP는 위임된 접두사를 제공하고 호스트는 사용할 접두사를 결정합니다.
IPv6 주소 활성화	**Layer3** 인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클라이언트 > **DHCPv6** 옵션	이 DHCPv6 클라이언트에 대해 수신된 IPv6 주소를 활성화합니다.
비임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 비임시 주소를 요청합니다. (이 주소 유형은 임시 주소보다 유효 기간이 깁니다). 인터페이스에 대해 비임시 주소 또는 임시 주소를 요청하는지 여부는 사용자의 재량과 *DHCPv6* 서버의 기능에 따라 결정됩니다. 일부 서버는 임시 주소만 제공할 수 있습니다. 가장 좋은 방법은 비임시 주소와 임시 주소를 모두 선택하는 것입니다. 이 경우 방화벽은 비임시 주소를 선호합니다.
임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 임시 주소를 요청합니다. 주소는 짧은 기간 동안 사용하도록 되어 있으므로 더 높은 수준의 보안을 위해 임시 주소를 선택합니다.
신속한 커밋		간청, 광고, 요청 및 응답 메시지 프로세스가 아닌 요청 및 응답 메시지의 DHCP 프로세스를 사용하려면 선택합니다.
접두사 위임 활성화	**Layer3** 인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클라이언트 > 접두사 위임	방화벽이 접두사 위임 기능을 지원할 수 있도록 접두사 위임을 활성화합니다. 즉, 인터페이스는 업스트림 DHCPv6 서버에서 접두사를 수락하고 선택한 접두사 풀에 접두사를 배치합니다. 여기에서 방화벽은 RA를 통해 접두사를 호스트에 위임합니다. 인터페이스에 대한 접두사 위임을 활성화 또는 비활성화하는 기능을 통해 방화벽은 여러 ISP(인터페이스당 하나의 ISP)를 지원할 수 있습니다. 이 인터페이스에서 접두사 위임을 활성화하면 접두사를 제공하는 ISP가 제어됩니다.
DHCP 접두사 길이 힌트		방화벽이 선호하는 DHCPv6 접두사 길이를 DHCPv6 서버로 보내도록 하려면 선택합니다.
DHCP 접두사 길이(비트)		DHCPv6 서버에 힌트로 전송되는 기본 DHCPv6 접두사 길이를 48~64비트 범위로 입력합니다. DHCPv6 서버는 선택한 접두사 길이를 보낼 권한이 있습니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
		예를 들어, 접두사 길이를 *48*로 요청하면 서브넷에 *16*비트*(64-48)*가 남게 되는데, 이는 위임할 접두사의 많은 하위 분할이 필요하다는 것을 의미합니다. 반면에 *63*의 접두사 길이를 요청하면 *2*개의 서브넷만 위임하기 위한 *1*비트가 남습니다. *128*비트 중 호스트 주소용으로 *64*비트가 더 있습니다. 인터페이스는 */48* 접두사를 수신할 수 있지만, 예를 들어 */64* 접두사를 위임하면 방화벽이 위임하는 접두사를 세분화한다는 의미입니다.
접두사 풀 이름		방화벽이 수신된 접두사를 저장하는 접두사 풀의 이름을 입력합니다. 이름은 고유해야 하며 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄을 포함해야 합니다. 쉽게 알아볼 수 있도록 *ISP*를 반영하는 접두사 풀 이름을 사용합니다.
이름	**Layer3** 인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	풀 이름을 입력하여 풀을 추가합니다. 이름은 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄일 수 있습니다.
주소 유형		하나를 고릅니다. • 풀의 **GUA** - 선택한 접두사 풀에서 제공되는 전역 유니캐스트 주소(GUA)입니다. • **ULA** - 고유 로컬 주소는 개인 네트워크 내 연결을 위한 주소 범위 fc00::/7의 개인 주소입니다. DHCPv6 서버가 없는 경우 ULA를 선택합니다.
인터페이스에서 활성화		인터페이스에서 주소를 활성화합니다.
접두사 풀		GUA를 가져올 접두사 풀을 선택합니다.
할당 유형	**Layer3** 인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	할당 유형을 선택합니다. • 동적 - DHCPv6 클라이언트는 상속된 인터페이스를 구성하기 위해 식별자를 선택해야 합니다. • 동적 식별자 - 사용자는 0~4,000 범위의 식별자를 선택하고 DHCPv6 클라이언트에서 고유한 식별자를 유지해야 합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
라우터 알림 보내기		인터페이스에서 LAN 호스트로 라우터 알림(RA)을 보내려면 선택합니다.
온링크		접두사 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지 여부를 선택합니다.
자치		시스템이 광고된 접두사를 인터페이스 ID와 결합하여 IPv6 주소를 독립적으로 생성할 수 있는지 여부를 선택합니다.
중복 주소 감지 활성화	**Layer3** 인터페이스 > **IPv6** > 주소 확인	DAD(중복 주소 감지)를 활성화하도록 선택한 다음 이 섹션의 다른 필드를 구성합니다.
DAD 시도		이웃 식별 시도가 실패하기 전에 이웃 요청 인터벌(**NS** 인터벌) 내에서 DAD 시도 횟수를 지정합니다(범위는 1~10, 기본값은 1).
도달 가능 시간(초)		쿼리 및 응답이 성공한 후 인접 네트워크에 도달할 수 있는 시간을 초 단위로 지정합니다(범위는 1~36,000, 기본값은 30).
NS 인터벌(초)		실패가 표시되기 전에 DAD 시도에 대한 시간(초)을 지정합니다(범위는 1 ~ 3,600, 기본값은 1).
NDP 모니터링 활성화		NDP(Neighbor Discovery Protocol) 모니터링을 활성화하려면 선택합니다. 활성화되면 NDP(기능 열에서의 )를 선택하여 IPv6 주소, 해당 MAC 주소 및 User-ID(최상의 경우 기준)와 같이 검색된 방화벽에 대한 정보를 볼 수 있습니다.
라우터 알림 활성화	**Layer3** 인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 = 상속됨	IPv6 인터페이스에서 Neighbor Discovery를 제공하려면 이 섹션의 다른 필드를 선택한 다음 구성합니다. 라우터 알림(RA) 메시지를 수신하는 IPv6 DNS 클라이언트는 이 정보를 사용합니다. RA를 사용하면 방화벽이 정적으로 구성되지 않은 IPv6 호스트의 기본 게이트웨이 역할을 하고 호스트에 주소 구성을 위한 IPv6 프리픽스를 제공할 수 있습니다. 이 기능과 함께 별도의 DHCPv6 서버를 사용하여 클라이언트에 DNS 및 기타 설정을 제공할 수 있습니다. 이것은 인터페이스에 대한 전역 설정입니다. 개별 IP 주소에 대한 RA 옵션을 설정하려면 IP 주소 테이블에 IPv6 주소를 추가하고 구성합니다. IPv6 주소에 대해 RA 옵션을 설정하는 경우 인터페이스에 대해 라우터 알림을 활성화해야 합니다.

레이어 3 인터페이스 설정	구성 위치	설명
최소 인터벌(초)		방화벽이 보낼 RA 사이의 최소 인터벌(초)을 지정합니다(범위는 3~1,350, 기본값은 200). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
최대 인터벌(초)		방화벽이 보낼 RA 간의 최대 인터벌(초)을 지정합니다(범위는 4~1,800, 기본값은 600). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
홉 제한		나가는 패킷에 대해 클라이언트에 적용할 홉 제한을 지정하거나(범위는 1~255, 기본값은 64) 시스템 기본값에 매핑되는 지정되지 않음을 선택합니다.
링크 MTU	**Layer3** 인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 = 상속됨	클라이언트에 적용할 링크 최대 전송 단위(MTU)를 지정하거나(범위는 1,280 ~ 1,500) 시스템 기본값에 매핑되는 지정되지 않은 기본값을 지정합니다.
도달 가능한 시간(ms)		클라이언트가 연결 가능성 확인 메시지(범위는 0 ~ 3,600,000)를 수신한 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능 시간(밀리초)을 지정하거나 기본값은 시스템 기본값에 매핑되는 지정되지 않음으로 설정됩니다.
재전송 시간(ms)		클라이언트가 이웃 요청 메시지(범위는 0 ~ 4,294,967,295)를 재전송하기 전에 대기하는 시간(밀리초)을 결정하는 재전송 타이머를 지정하거나 시스템 기본값에 매핑되는 지정되지 않음으로 기본값을 지정합니다.
라우터 유효 시간(초)		클라이언트가 방화벽을 기본 게이트웨이로 사용할 시간(초)을 지정합니다(범위는 0~9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.
라우터 기본 설정		네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트는 이 필드를 사용하여 기본 라우터를 선택합니다. RA가 방화벽 라우터를 세그먼트의 다른 라우터에 비해 높음, 중간(기본값) 또는 낮음 우선 순위를 갖는 것으로 광고할지의 여부를 선택합니다.
관리 구성	**Layer3** 인터페이스 > **IPv6** > 라우터 알림,	DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
기타 구성	유형 = 정적 또는 유형 = 상속됨	DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
일관성 확인		방화벽이 다른 라우터에서 보낸 RA가 링크에 대한 일관된 정보를 광고하는지 확인하도록 하려면 선택합니다. 방화벽은 시스템 로그에 불일치를 기록합니다. 유형은 **ipv6nd**입니다.
라우터 광고에 DNS 정보 포함	**Layer3** 인터페이스 > **IPv6** > **DNS** 지원, 유형 = 정적	라우터 알림 탭에서 라우터 알림 사용을 선택하면 DNS 지원을 사용할 수 있습니다. 방화벽이 이 IPv6 이더넷 인터페이스에서 NDP 라우터 광고의 DNS 정보를 보내도록 선택합니다. 다른 DNS 지원 필드(서버, 유효 시간, 서픽스 및 유효 시간)는 이 옵션을 선택한 후에만 표시됩니다.
서버		이 IPv6 이더넷 인터페이스에서 NDP 라우터 광고를 보낼 방화벽에 대한 하나 이상의 재귀 DNS(RDNS) 서버 주소를 추가합니다. RDNS 서버는 루트 DNS와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에 대한 NDP 라우터 광고에서 위쪽에서 아래쪽으로 나열된 순서대로 보내는 최대 8개의 RDNS 서버를 구성할 수 있습니다. 그러면 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다.
유효 시간		IPv6 DNS 클라이언트가 라우터 알림을 수신한 후 클라이언트가 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)에서 최대 인터벌(초)의 두 배, 기본값은 1,200).
도메인 검색 목록	**Layer3** 인터페이스 > **IPv6** > **DNS** 지원, 유형 = 정적 **Layer3** 인터페이스 > **IPv6** > **DNS** 지원	DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(서픽스)을 추가합니다. 최대 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하여 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가하고 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가

레이어 **3** 인터페이스 설정	구성 위치	설명
		"company.com"인 경우 라우터의 결과 쿼리는 정규화된 도메인 이름 "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록에 있는 모든 서픽스를 시도할 때까지 DNS 서픽스를 사용합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 사용하는 NDP 라우터 광고에서 방화벽이 위에서 아래로 나열된 순서대로 보내는 DNS 검색 목록 옵션에 대해 최대 8개의 도메인 이름(서픽스)을 구성할 수 있습니다. 서픽스를 선택한 다음 위로 이동 또는 아래로 이동하여 순서를 변경하거나 더 이상 필요하지 않은 경우 서픽스를 삭제합니다.
유효 시간		IPv6 DNS 클라이언트가 DNS 검색 목록에서 도메인 이름(서픽스)을 사용할 수 있다는 라우터 광고를 수신한 후 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)에서 최대 인터벌(초)의 두 배까지의 값입니다. 기본값 1,200)입니다.
DNS 재귀 네임 서버	**Layer3** 인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 DNS 재귀 네임 서버 정보를 보내도록 합니다. • 수동 - DNS 재귀 네임 서버를 수동으로 구성합니다. 수동을 선택하면, 방화벽이 이 IPv6 VLAN 인터페이스에서 NDP 라우터 알림을 보낼 수 있도록 재귀 DNS(RDNS) 서버의 IPv6 주소(예: 2001:4860:4860:0:0:8888)를 추가합니다. RDNS 서버는 루트 DNS 서버와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에게 보내는 NDP 라우터 광고에서 위에서 아래로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있으며, 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다. 클라이언트가 특정 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간

레이어 **3** 인터페이스 설정	구성 위치	설명
		인 유효 기간명을 초 단위로 입력합니다. 범위는 4~3,600입니다. 기본값은 1,200입니다.
도메인 검색 목록	**Layer3** 인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 도메인 검색 목록 정보를 보내도록 합니다. • 수동 - 도메인 검색 목록을 수동으로 구성합니다. 수동을 선택한 경우 추가하고 DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(접미사)을 구성합니다. 최대 접미사 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 이름을 DNS 쿼리에 입력하기 전에 정규화되지 않은 도메인 이름에 추가(한 번에 하나씩)하여 DNS 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 접미사 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가한 다음 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 접미사가 'company.com'인 경우 라우터의 결과 DNS 쿼리는 정규화된 도메인 이름 'quality.company.com'에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록의 두 번째 DNS 접미사를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 접미사 무시) 또는 라우터가 목록에 있는 모든 접미사를 시도할 때까지 DNS 접미사를 시도합니다. 이웃 검색 DNSSL 옵션에서 DNS 클라이언트 라우터에 제공하려는 접미사로 방화벽을 구성합니다. DNSSL 옵션을 수신하는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에서 접미사를 사용합니다. 클라이언트가 특정 도메인 검색 목록을 사용할 수 있는 최대 시간인 유혀 기간을 초 단위로 입력합니다. 범위는 4~3,600입니다. 기본값은 1,200입니다. 동일한 순서로 해당 주소를 사용하는 받는 사람에 대한 NDP 라우터 알림에서 방화벽이 보내는 DNS 검색 목록에 대해 최대 8개의 도메인 이름(접미사)을 구성할 수 있습니다. 접미사를 선택하고 위로 또는 아래로를 선택하여 순서를 변경하거나 더 이상 필요하지 않은 접미사를 목록에서 삭제합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
SD-WAN 인터페이스 상태	**Layer3** 인터페이스 > **SD-WAN**	**IPv4** 탭에서 **SD-WAN** 활성화를 선택한 경우 방화벽은 SD-WAN ##### ### ##### ####. **SD-WAN**을 활성화하지 않은 경우 ##### #을 나타냅니다.
SD-WAN 인터페이스 프로파일		SD-WAN 인터페이스 프로파일을 선택하여 이 이더넷 인터페이스에 적용하거나 새 SD-WAN 인터페이스 프로파일을 추가합니다. *SD-WAN* 인터페이스 프로파일을 적용하려면 먼저 인터페이스에 대해 ***SD-WAN***을 활성화해야 합니다.
업스트림 NAT		SD-WAN 허브 또는 분기가 NAT를 수행하는 디바이스 뒤에 있는 경우 허브 또는 분기에 대해 업스트림 NAT를 활성화합니다.
NAT IP 주소 유형		IP 주소 할당 유형을 선택한 다음 해당 NAT 수행 디바이스에서 공용 인터페이스의 FQDN 또는 IP 주소를 지정하거나 DDNS가 주소를 파생하도록 지정합니다. 따라서 Auto VPN은 주소를 허브 또는 분기의 터널 엔드포인트로 사용할 수 있습니다. • 고정 **IP** - 유형을 **IP** 주소 또는 **FQDN**으로 선택한 다음 IPv4 주소 또는 FQDN을 입력합니다. • **DDNS** - DDNS(동적 DNS)는 업스트림 NAT 디바이스의 IP 주소를 파생합니다.
링크 속도	이더넷 인터페이스 > 고급 > 링크 설정	인터페이스 속도를 Mbps 단위로 선택하거나 자동을 선택하여 방화벽이 속도를 자동으로 결정하도록 합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
PoE Rsvd Pwr	이더넷 인터페이스 > 고급 > **PoE** 설정 (지원되는 방화벽만 해당)	PoE가 활성화된 경우 할당된 전력량(와트)을 선택합니다.
PoE 활성화		이 인터페이스에서 PoE를 활성화하려면 선택합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
관리 프로파일	**Layer3** 인터페이스 > 고급 > 다른 정보	이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 관리 프로파일을 선택합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방화벽은 패킷이 과다하게 크다는 것을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.
TCP MSS 조정		인터페이스 MTU 바이트 크기 내의 모든 헤더에 대한 바이트를 수용하도록 최대 세그먼트 크기(MSS)를 조정하려면 선택합니다. MTU 바이트 크기에서 MSS 조정 크기를 뺀 값은 IP 프로토콜에 따라 달라지는 MSS 바이트 크기와 같습니다. • **IPv4 MSS** 조정 크기 - 범위는 40~300이고, 기본값은 40입니다. • **IPv6 MSS** 조정 크기 - 범위는 60~300이고, 기본값은 60입니다. 이 설정을 사용하여 네트워크를 통한 터널에 더 작은 MSS가 필요한 경우를 해결하십시오. 패킷이 조각화 없이 MSS보다 더 많은 바이트를 갖는 경우 이 설정을 사용하면 조정할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로 VLAN 태그가 있는 MPLS 헤더 또는 터널링된 트래픽과 같은 항목에 대해 바이트를 허용하도록 MSS 조정 크기를 구성하는 데 도움이 됩니다.
태그가 지정되지 않은 서브인터페이스		이 인터페이스에 대한 해당 서브인터페이스에 태그가 지정되지 않은 경우 이 옵션을 선택합니다.
IP 주소 MAC 주소	**Layer3** 인터페이스 > 고급 > **ARP** 엔트리	하나 이상의 고정 ARP(주소 확인 프로토콜) 항목을 추가하려면 IP 주소 및 관련 하드웨어 [미디어 액세스 제어(MAC)] 주소를 추가합니다. 항목을 삭제하려면 항목을 선택한 다음 삭제를 클릭합니다. 고정 ARP 항목은 ARP 처리를 줄입니다.
IPv6 주소 MAC 주소	**Layer3** 인터페이스 > 고급 > **ND** 항목	NDP(Neighbor Discovery Protocol)에 대한 네이버 정보를 제공하려면 네이버의 IPv6 주소와 MAC 주소를 추가합니다.

레이어 **3** 인터페이스 설정	구성 위치	설명
NDP 프록시 사용	**Layer3** 인터페이스 > 고급 > **NDP** 프록시	인터페이스에 대해 NDP(Neighbor Discovery Protocol) 프록시를 활성화합니다. 방화벽은 이 목록의 IPv6 주소에 대한 MAC 주소를 요청하는 ND 패킷에 응답합니다. ND 응답에서 방화벽은 인터페이스에 대한 자체 MAC 주소를 전송하여 방화벽이 목록의 주소에 대한 패킷을 수신하도록 합니다. NPTv6(Network Prefix Translation IPv6)을 사용하는 경우 NDP 프록시를 활성화하는 것이 좋습니다. **NDP** 프록시 사용을 선택한 경우 필터를 입력하고 필터 적용(회색 화살표)을 클릭하여 수많은 주소 항목을 필터링할 수 있습니다.
주소		방화벽이 NDP 프록시로 작동할 IPv6 주소, IP 범위, IPv6 서브넷 또는 주소 개체를 하나 이상 추가합니다. 이상적으로는 이러한 주소 중 하나가 NPTv6의 소스 번역 주소와 동일합니다. 주소의 순서는 중요하지 않습니다. 주소가 하위 네트워크인 경우 방화벽은 서브넷의 모든 주소에 대해 ND 응답을 보내므로 방화벽의 IPv6 인접 항목도 추가한 다음 무효를 클릭하여 방화벽이 이러한 IP 주소에 응답하지 않도록 지시하는 것이 좋습니다.
무효		해당 주소에 대한 NDP 프록시를 방지하려면 주소를 무효합니다. 지정된 IP 주소 범위 또는 IP 서브넷의 하위 집합을 무효화할 수 있습니다.
LLDP 활성화	**Layer3** 인터페이스 > 고급 > **LLDP**	인터페이스에 대해 LLDP(Link Layer Discovery Protocol)를 활성화합니다. LLDP는 링크 레이어에서 기능하여 LLDP 데이터 단위를 이웃과 주고받아 이웃 디바이스와 해당 기능을 검색합니다.
LLDP 프로파일		LLDP 프로파일을 선택하거나 새 LLDP 프로파일을 만듭니다. 프로파일은 LLDP 모드를 구성하고, syslog 및 SNMP 알림을 활성화하고, LLDP 피어로 전송하려는 선택적 TLV(Type-Length-Values)를 구성하는 방법입니다.
설정	**Layer3** 인터페이스 > 고급 > **DDNS**	설정을 선택하여 DDNS 필드를 구성할 수 있도록 합니다.
활성화		인터페이스에서 DDNS를 활성화합니다. DDNS를 구성하려면 처음에 활성화해야 합니다. (DDNS 설정이 완료되지 않은 경우 부분 설정을 잃지 않도록 활성화하지 않고 저장할 수 있습니다.)

레이어 **3** 인터페이스 설정	구성 위치	설명
업데이트 인터벌(일)		FQDN에 매핑된 IP 주소를 업데이트하기 위해 방화벽이 DDNS 서버에 보내는 업데이트 인터벌(일)을 입력합니다(범위는 1~30, 기본값은 1). 또한 방화벽은 *DHCP* 서버에서 인터페이스에 대한 새 *IP* 주소를 수신하면 *DDNS*를 업데이트합니다.
인증서 프로파일		DDNS 서비스를 확인하기 위해 인증서 프로파일을 생성합니다. DDNS 서비스는 인증 기관(CA)이 서명한 인증서를 방화벽에 제공합니다.
호스트네임		DDNS 서버에 등록된 인터페이스의 호스트 이름(예: host123.domain123.com, host123)을 입력합니다. 방화벽은 구문이 도메인 이름에 대해 DNS에서 허용하는 유효한 문자를 사용하는지 확인하는 경우를 제외하고 호스트 이름의 유효성을 검사하지 않습니다.
공급자	**Layer3** 인터페이스 > 고급 > **DDNS**	이 인터페이스에 DDNS 서비스를 제공하는 DDNS 공급자(및 버전)를 선택하십시오. • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS**(DDNS가 있는 SD-WAN Full Mesh, SD-WAN AE 서브인터페이스 및 SD-WAN Layer 3 서브인터페이스에 적용) 방화벽에서 특정 날짜까지 단계적으로 중단될 것이라고 표시하는 *DDNS* 서비스의 이전 버전을 선택하는 경우 최신 버전으로 이동합니다. 공급자 이름 뒤에 오는 이름 및 값 필드는 공급자별로 다릅니다. 읽기 전용 필드는 방화벽이 DDNS 서비스에 연결하는 데 사용하는 매개변수를 알려줍니다. DDNS 서비스가 사용자에게 제공하는 비밀번호 및 DDNS 서버에서 응답을 수신하지 않는 경우 방화벽이 사용하는 타임아웃과 같은 다른 필드를 구성합니다.

레이어 3 인터페이스 설정	구성 위치	설명
IPv4 탭		인터페이스에 구성된 IPv4 주소를 추가한 다음 선택합니다. DDNS 공급자가 허용하는 만큼만 IPv4 주소를 선택할 수 있습니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
IPv6 탭		인터페이스에 구성된 IPv6 주소를 추가한 다음 선택합니다. DDNS 공급자가 허용하는 만큼만 IPv6 주소를 선택할 수 있습니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
런타임 정보 표시		DDNS 등록을 표시합니다. DDNS 공급자, 확인된 FQDN 및 기본 IP 주소를 나타내는 별표(*)가 있는 매핑된 IP 주소. 각 DDNS 공급자에는 문제 해결을 위해 호스트 이름 업데이트 상태와 반환 날짜를 나타내는 고유한 반환 코드가 있습니다.

레이어 3 서브인터페이스

- 네트워크 > 인터페이스 > 이더넷

물리적 Layer 3 인터페이스로 구성된 각 이더넷 포트에 대해 추가 논리적 Layer 3 인터페이스(서브인터페이스)를 정의할 수 있습니다. ISP가 PPPoE 서브인터페이스에서 802.1Q VLAN 태그를 사용하는 경우 IEEE 802.1Q VLAN용 PPPoE 클라이언트용 레이어 3 서브인터페이스를 생성할 수 있습니다.

SD-WAN AE 인터페이스에 대한 레이어 3 서브인터페이스를 구성할 수도 있습니다. SD WAN AE 인터페이스 그룹을 생성하고 그룹을 선택한 다음 서브인터페이스 추가를 선택하고 다음 정보를 지정합니다.

PA-7000 시리즈 레이어 3 인터페이스를 구성하려면 물리적 인터페이스, 서브인터페이스 추가를 선택한 후 다음 정보를 지정합니다.

레이어 3 서브인터페이스 설정	구성 위치	설명
인터페이스 이름	**Layer3** 서브인터페이스	읽기 전용 인터페이스 이름 필드에는 선택한 물리적 인터페이스의 이름이 표시됩니다. 인접 필드에 숫자 서픽스(1 ~ 9,999)를 입력하여 서브인터페이스를 식별합니다.
코멘트		서브인터페이스에 대한 선택적 설명을 입력합니다.
태그		서브인터페이스에 대한 VLAN 태그(1~4,094)를 입력합니다. 사용의 편의를 위해 인터페이스 이름에 숫자 서픽스와 동일한 숫자를 사용하십시오.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
넷플로우 프로파일		수신 서브인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 서브인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
가상 라우터	**Layer3** 서브인터페이스 > 컨피그	인터페이스에 가상 라우터를 할당하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 서브인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		서브인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 서브인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
SD-WAN 활성화	**Layer3** 서브인터페이스 > **IPv4**	Layer 3 인터페이스 또는 SD-WAN AE 인터페이스 그룹에 대해 Layer3 서브인터페이스에서 SD-WAN을 활성화하려면 선택합니다.
Bonjour 리플렉터 활성화		(PA-220, PA-800 및 PA-3200 시리즈만 해당) 이 옵션을 활성화하면 방화벽은 Bonjour 멀티캐스트 광고와 쿼리를 이 인터페이스에서 수신하고 이 인터페이스로 포워딩하여 이 인터페이스를 활성화한 다른 모든 L3 및 AE 인터페이스와 서브인터페이스로 포워딩합니다. 옵션. 이는 보안 또는 관리 목적으로 트래픽을 라우팅하기 위해 세분화를 사용하는 네트워크 환경에서 사용자 액세스 및 디바이스 검색 가능성을 보장하는 데 도움이 됩니다. 최대 16개의 인터페이스에서 이 옵션을 활성화할 수 있습니다.
유형		서브인터페이스에 IPv4 주소를 할당하는 방법을 선택합니다. • 정적 - **IP** 주소와 서브넷 마스크를 수동으로 추가하고 다음 홉 게이트웨이를 입력해야 합니다. • **PPPoE** - 서브인터페이스가 PPPoE(Point-to-Point Protocol over Ethernet) 클라이언트 역할을 하고 서버의 IP 주소,

레이어 **3** 서브인터페이스 설정	구성 위치	설명
		DNS 정보 및 MTU와 같은 기타 정보와 함께 ISP로부터 IPv4 주소를 받을 수 있도록 합니다. • **DHCP** 클라이언트—서브인터페이스가 DHCP(동적 호스트 구성 프로토콜) 클라이언트 역할을 하고 동적으로 할당된 IP 주소를 받을 수 있도록 합니다. 고가용성*(HA)* 능동형/능동형 구성에 있는 방화벽은 *DHCP* 클라이언트를 지원하지 않습니다. 선택한 IP 주소 방법에 따라 탭에 표시되는 옵션이 달라집니다.
IP	**Layer3** 서브인터페이스 > **IPv4,** 유형 = 정적	다음 단계 중 하나를 추가하고 수행하여 인터페이스에 대한 고정 IP 주소와 네트워크 마스크를 지정합니다. • CIDR(Classless Inter-Domain Routing) 표기법으로 항목을 입력합니다: *ip_address*/*mask*(예: 192.168.2.0/24). • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • **IP** 넷마스크 유형의 주소 개체를 만듭니다. 인터페이스에 대해 여러 IP 주소를 입력할 수 있습니다. 시스템에서 사용하는 FIB(포워딩 정보 기반)에 따라 최대 IP 주소 수가 결정됩니다. 더 이상 필요하지 않은 IP 주소는 삭제하십시오.
사용	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 일반	PPPoE 서브인터페이스를 활성화합니다.
사용자명	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 일반	선택할 인증 유형의 사용자 이름을 입력합니다.
암호	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 일반	선택할 인증 유형의 비밀번호를 입력한 다음비밀번호를 확인합니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
인증	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	PPPoE 서브인터페이스에 대한 인증 유형을 선택합니다. • 없음 - (기본값) 없음을 선택하면 방화벽에서 자동 인증을 사용합니다. • **CHAP** - 방화벽은 챌린지 핸드셰이크 인증 프로토콜(CHAP)을 사용합니다. • **PAP** - 방화벽은 PAP(비밀번호 인증 프로토콜)를 사용합니다. PAP는 CHAP보다 덜 안전합니다. PAP는 사용자 이름과 비밀번호를 일반 텍스트로 보냅니다. • **auto** - 방화벽이 PPPoE 서버와 인증 방법(CHAP 또는 PAP)을 협상합니다.
고정 주소	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	PPPoE 서버가 하위 인터페이스에 해당 IPv4 주소를 할당하도록 요청하려면 정적 주소를 지정합니다. (PPPoE 서버는 요청된 주소 또는 다른 주소를 재량에 따라 할당할 수 있습니다.) 기본값은 없음입니다.
피어를 가리키는 기본 경로 자동 생성	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	PPPoE 서버가 제공하는 기본 게이트웨이를 가리키는 기본 경로를 생성합니다.
기본 경로 측정 항목	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	PPPoE 연결의 기본 경로 메트릭(우선 순위 수준)을 입력합니다. 범위는 1~65,535입니다. 기본값은 10입니다. 경로 선택 시 번호가 낮은 경로가 우선 순위가 높습니다. 예를 들어 메트릭이 10인 경로는 메트릭이 100인 경로보다 먼저 사용됩니다.
액세스 집중 디바이스	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	ISP가 제공한 액세스 집중 디바이스의 이름을 입력합니다(0~255자의 문자열 값). 방화벽은 이 액세스 집중 디바이스와 연결됩니다.
서비스	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	ISP에서 제공한 서비스가 있는 경우 해당 서비스를 입력합니다(문자열 값 0~255자).

레이어 **3** 서브인터페이스 설정	구성 위치	설명
수동	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **PPPoE** > 고급	PPPoE 클라이언트(방화벽)에서 PPPoE 서버가 연결을 시작할 때까지 기다리도록 하려면 수동을 선택합니다. 수동을 선택하지 않으면 방화벽이 연결을 시작할 수 있습니다.
사용	**Layer3** 서브인터페이스 > **IPv4,** 유형 = **DHCP**	인터페이스에서 DHCP 클라이언트를 활성화하려면 선택합니다.
서버에서 제공하는 기본 게이트웨이를 가리키는 기본 경로 자동 생성		DHCP 서버가 제공하는 기본 게이트웨이를 가리키는 기본 경로를 자동으로 생성하려면 선택합니다.
호스트네임 보내기		방화벽(DHCP 클라이언트)이 인터페이스의 호스트네임(옵션 12)을 DHCP 서버로 보내도록 하려면 선택합니다. 기본적으로 호스트네임을 보내면 기본적으로 방화벽의 호스트네임이 호스트 이름 필드에서 선택됩니다. 해당 이름을 보내거나 사용자 지정 호스트네임(대소문자, 숫자, 마침표, 하이픈 및 밑줄을 포함하여 최대 64자)을 입력할 수 있습니다.
기본 경로 측정항목		(선택 사항) 방화벽과 DHCP 서버 간의 경로에 대해 기본 경로와 연결하고 경로 선택에 사용할 경로 메트릭(우선 순위 수준)을 입력할 수 있습니다(범위는 1~65535, 기본값 없음). 숫자 값이 감소할수록 우선 순위 수준이 높아집니다.
DHCP 클라이언트 런타임 정보 표시		**DHCP** 클라이언트 런타임 정보 표시를 선택하여 DHCP 임대 상태, 동적 IP 주소 할당, 서브넷 마스크, 게이트웨이 및 서버 설정(DNS, NTP, 도메인, WINS, NIS, POP3 및 SMTP)을 포함하여 DHCP 서버에서 수신한 모든 설정을 표시합니다.
인터페이스에서 IPv6 활성화	**Layer3** 서브인터페이스 > **IPv6**	이 인터페이스에서 IPv6 주소 지정을 활성화하려면 선택합니다.
인터페이스 ID		64비트 확장 고유 식별자(EUI-64)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 **ID**를 호스트 부분으로 사용 옵션을 활성화하면 방화벽은 인터페이스 ID를 해당 주소의 호스트 부분으로 사용합니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
유형		IPv6 주소 유형을 다음 중에서 선택합니다. 정적, **DHCPv6** 클라이언트 또는 상속됨.
주소	**Layer3** 서브인터페이스 > **IPv6** > 주소 할당, 유형 = 정적	IPv6 주소 및 접두사 길이(예: 2001:400:f00::1/64)를 추가합니다. 또는 IPv6 주소 개체를 선택하거나 새 주소 개체를 생성할 수 있습니다.
인터페이스에서 주소 활성화		인터페이스에서 IPv6 주소를 활성화하려면 선택합니다.
인터페이스 ID를 호스트 부분으로 사용		인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다.
애니캐스트		가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다.
라우터 알림 보내기	**Layer3** 서브인터페이스 > **IPv6** > 주소 할당, 유형 = 정적	이 IP 주소에 대해 라우터 광고(RA)를 활성화하려면 선택합니다. (또한, 인터페이스에서 라우터 알림 활성화를 수행해야 합니다.) RA에 대한 자세한 내용은 이 표에서 라우터 알림 활성화를 참조하십시오. 라우터 알림 보내기인 경우 나머지 필드가 적용됩니다. • 유효 시간**(**초**)** - 방화벽이 주소가 유효한 것으로 간주하는 시간(초)입니다. 유효 시간은 기본 유효 시간과 같거나 초과해야 합니다. 기본값은 2,592,000입니다. • 기본 설정 유효 기간**(**초**)** - 방화벽에서 트래픽 송수신에 사용할 수 있는 유효한 주소가 기본 설정되는 기간(초)입니다. 기본 유효 시간이 만료되면 방화벽은 주소를 사용하여 새 연결을 설정할 수 없지만 기존 연결은 유효 시간이 만료될 때까지 유효합니다. 기본값은 604,800입니다. • 온링크 - 프리픽스 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지의 여부를 선택합니다. • **Autonomous**—시스템이 보급된 프리픽스를 인터페이스 ID와 결합하여 IP 주소를 독립적으로 생성할 수 있는지의 여부를 선택합니다.
라우터 알림 경로 수락	**Layer3** 서브인터페이스 > **IPv6** > 주소 할당, 유형 =	DHCPv6 클라이언트가 DHCPv6 서버에서 RA를 수락하도록 허용하려면 선택합니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
기본 경로 측정 항목	**DHCPv6** 클라이언트	인터페이스에서 ISP까지의 경로에 대한 기본 경로 메트릭을 입력합니다. 범위는 1~65,535입니다. 기본값은 10입니다.
기본 설정		두 개의 인터페이스(각각 중복성을 위해 다른 ISP에 연결됨)가 있는 경우 한 ISP에 대한 인터페이스에 다른 ISP에 대한 인터페이스보다 높은 기본 설정을 할당할 수 있도록 DHCPv6 클라이언트 인터페이스의 기본 설정(낮음, 중간 또는 높음)을 선택합니다. 기본 인터페이스에 연결된 ISP는 호스트 인터페이스에 보낼 위임된 접두사를 제공하는 ISP가 됩니다. 인터페이스의 기본 설정이 동일한 경우 두 ISP는 위임된 접두사를 제공하고 호스트는 사용할 접두사를 결정합니다.
IPv6 주소 활성화	**Layer3** 서브인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클라이언트 > **DHCPv6** 옵션	이 DHCPv6 클라이언트에 대해 수신된 IPv6 주소를 활성화합니다.
비임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 비임시 주소를 요청합니다. 비임시 주소는 임시 주소보다 유효 기간이 깁니다. 비임시 주소는 갱신할 수 있습니다. 인터페이스에 대해 비임시 주소 또는 임시 주소를 요청하는지 여부는 사용자의 재량과 *DHCPv6* 서버의 기능에 따라 결정됩니다. 일부 서버는 임시 주소만 제공할 수 있습니다. 가장 좋은 방법은 비임시 주소와 임시 주소를 모두 선택하는 것입니다. 이 경우 방화벽은 비임시 주소를 선호합니다.
임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 임시 주소를 요청합니다. 주소는 짧은 기간 동안 사용하도록 되어 있으므로 더 높은 수준의 보안을 위해 임시 주소를 선택합니다. 임시 주소는 갱신되거나 갱신되지 않을 수 있습니다.
신속한 커밋		간청, 광고, 요청 및 응답 메시지 프로세스가 아닌 요청 및 응답 메시지의 DHCP 프로세스를 사용하려면 선택합니다.
접두사 위임 활성화	**Layer3** 서브인터페이스 > **IPv6** > 주소	방화벽이 접두사 위임 기능을 지원할 수 있도록 접두사 위임을 활성화합니다. 즉, 인터페이스는 업스트림 DHCPv6 서버에서 접두사를 수락하고 선택한 접두사 풀에 접두사를 배치합니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
	할당, 유형 = **DHCPv6** 클라이언트 > 접두사 위임	여기에서 방화벽은 RA를 통해 접두사를 호스트에 위임합니다. 인터페이스에 대한 접두사 위임을 활성화 또는 비활성화하는 기능을 통해 방화벽은 여러 ISP(인터페이스당 하나의 ISP)를 지원할 수 있습니다. 이 인터페이스에서 접두사 위임을 활성화하면 접두사를 제공하는 ISP가 제어됩니다.
DHCP 접두사 길이 힌트		방화벽이 선호하는 DHCPv6 접두사 길이를 DHCPv6 서버로 보내도록 하려면 선택합니다.
DHCP 접두사 길이(비트)		DHCPv6 서버에 힌트로 전송되는 기본 DHCPv6 접두사 길이를 48~64비트 범위로 입력합니다. 예를 들어, 접두사 길이를 *48*로 요청하면 서브넷에 *16*비트*(64-48)*가 남게 되는데, 이는 위임할 접두사의 많은 하위 분할이 필요하다는 것을 의미합니다. 반면에 *63*의 접두사 길이를 요청하면 *2*개의 서브넷만 위임하기 위한 *1*비트가 남습니다. *128*비트 중 호스트 주소용으로 *64*비트가 더 있습니다.
접두사 풀 이름		방화벽이 수신된 접두사를 저장하는 접두사 풀의 이름을 입력합니다. 이름은 고유해야 하며 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄을 포함해야 합니다. 쉽게 알아볼 수 있도록 *ISP*를 반영하는 접두사 풀 이름을 사용합니다.
이름	**Layer3** 서브인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	풀 이름을 입력하여 풀을 추가합니다. 이름은 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄일 수 있습니다.
주소 유형		하나를 고릅니다. • 풀의 **GUA** - 선택한 접두사 풀에서 제공되는 전역 유니캐스트 주소(GUA)입니다. • **ULA** - 고유 로컬 주소는 개인 네트워크 내 연결을 위한 주소 범위 fc00::/7의 개인 주소입니다. DHCPv6 서버가 없는 경우 ULA를 선택합니다.
인터페이스에서 활성화		인터페이스에서 주소를 활성화합니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
접두사 풀		GUA를 가져올 접두사 풀을 선택합니다.
할당 유형	**Layer3** 서브인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	할당 유형을 선택합니다. • 동적 - DHCPv6 클라이언트는 상속된 인터페이스를 구성하기 위해 식별자를 선택해야 합니다. • 동적 식별자 - 사용자는 0~4,000 범위의 식별자를 선택하고 DHCPv6 클라이언트에서 고유한 식별자를 유지해야 합니다.
라우터 알림 보내기		인터페이스에서 LAN 호스트로 라우터 알림(RA)을 보내려면 선택합니다.
온링크		접두사 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지 여부를 선택합니다.
자치		시스템이 광고된 접두사를 인터페이스 ID와 결합하여 IPv6 주소를 독립적으로 생성할 수 있는지 여부를 선택합니다.
중복 주소 감지 활성화	**Layer3** 서브인터페이스 > **IPv6** > 주소 확인	DAD(중복 주소 감지)를 활성화하도록 선택한 다음 이 섹션의 다른 필드를 구성합니다.
DAD 시도		이웃 식별 시도가 실패하기 전에 이웃 요청 인터벌(**NS** 인터벌) 내에서 DAD 시도 횟수를 지정합니다(범위는 1~10, 기본값은 1).
도달 가능 시간(초)		클라이언트가 도달 가능성 확인 메시지를 받은 후 이웃에 도달할 수 있다고 가정하는 데 사용할 시간(초)을 지정합니다(범위는 10~36,000, 기본값은 30).
NS 인터벌(초)		NS(Neighbor Solicitation) 인터벌을 지정합니다. 이는 장애가 표시되기 전에 DAD 시도에 대한 초 수입니다(범위는 1~3,600, 기본값은 1).
NDP 모니터링 활성화		NDP(Neighbor Discovery Protocol) 모니터링을 활성화하려면 선택합니다. 활성화되면 NDP( ) (기능 열에서)를 선택하여 IPv6 주소, 해당 MAC 주소 및 사용자 ID(최상의 경우 기준)와 같이 방화벽이 검색한 이웃에 대한 정보를 볼 수 있습니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
라우터 알림 활성화	**Layer3** 서브인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 = 상속됨	IPv6 인터페이스에서 Neighbor Discovery를 제공하려면 이 섹션의 다른 필드를 선택한 다음 구성합니다. 라우터 알림(RA) 메시지를 수신하는 IPv6 DNS 클라이언트는 이 정보를 사용합니다. RA를 사용하면 방화벽이 정적으로 구성되지 않은 IPv6 호스트의 기본 게이트웨이 역할을 하고 호스트에 주소 구성을 위한 IPv6 프리픽스를 제공할 수 있습니다. 이 기능과 함께 별도의 DHCPv6 서버를 사용하여 클라이언트에 DNS 및 기타 설정을 제공할 수 있습니다. 이것은 인터페이스에 대한 전역 설정입니다. 개별 IP 주소에 대한 RA 옵션을 설정하려면 IP 주소 테이블에서 주소를 추가 및 구성합니다. IP 주소에 대해 RA 옵션을 설정하는 경우 인터페이스에 대해 라우터 알림을 활성화해야 합니다.
최소 인터벌(초)		방화벽이 보낼 RA 사이의 최소 인터벌(초)을 지정합니다(범위는 3~1,350, 기본값은 200). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
최대 인터벌(초)		방화벽이 보낼 RA 간의 최대 인터벌(초)을 지정합니다(범위는 4~1,800, 기본값은 600). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
홉 제한		나가는 패킷에 대해 클라이언트에 적용할 홉 제한을 지정합니다(범위는 1~255, 기본값은 64). 홉 제한이 없는 경우 0을 입력합니다.
링크 MTU		클라이언트에 적용할 링크 최대 전송 단위(MTU)를 지정합니다. 링크 없음 MTU에 대해 지정되지 않음을 선택합니다(범위는 1,280 ~ 9,192, 기본값은 지정되지 않음).
도달 가능한 시간(ms)		클라이언트가 연결 확인 메시지를 수신한 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능 시간(밀리초)을 지정합니다. 도달할 수 없는 시간 값에 대해 지정되지 않음을 선택합니다(범위는 0 ~ 3,600,000, 기본값은 지정되지 않음).
재전송 시간(ms)		클라이언트가 인접 요청 메시지를 재전송하기 전에 대기하는 시간(밀리초)을 결정하는 재전송 타이머를 지정합니다. 재전송 시간이 없는 경우 지정되지 않음을 선택합니다(범위는 0 ~ 4,294,967,295, 기본값은 지정되지 않음).

레이어 **3** 서브인터페이스 설정	구성 위치	설명
라우터 유효 시간(초)		클라이언트가 방화벽을 기본 게이트웨이로 사용할 시간(초)을 지정합니다(범위는 0~9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.
라우터 기본 설정		네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트는 이 필드를 사용하여 기본 라우터를 선택합니다. RA가 방화벽 라우터를 세그먼트의 다른 라우터에 비해 높음, 중간(기본값) 또는 낮음 우선 순위를 갖는 것으로 광고할지의 여부를 선택합니다.
관리 구성		DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
기타 구성		DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
라우터 기본 설정	**Layer3** 서브인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 = 상속됨	RA를 호스트로 보내는 서로 다른 라우터에 둘 이상의 인터페이스가 있는 경우 라우터 기본 설정을 설정합니다. 높음, 중간 또는 낮음은 상대적 우선 순위를 나타내는 RA가 광고하는 우선 순위이며 호스트는 우선 순위가 더 높은 라우터의 접두사를 사용합니다.
관리 구성		DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
기타 구성		DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
일관성 확인		방화벽이 다른 라우터에서 보낸 RA가 링크에 대한 일관된 정보를 광고하는지 확인하도록 하려면 선택합니다. 방화벽은 시스템 로그에 불일치를 기록합니다. 유형은 **ipv6nd**입니다.
라우터 광고에 DNS 정보 포함	**Layer3** 서브인터페이스 > **IPv6** > **DNS** 지원, 유형 = 정적	방화벽이 이 IPv6 이더넷 서브인터페이스에서 NDP 라우터 광고의 DNS 정보를 보내도록 선택합니다. 이 표의 다른 DNS 지원 필드는 이 옵션을 선택한 후에만 표시됩니다.
서버		이 IPv6 이더넷 인터페이스에서 NDP 라우터 광고를 보낼 방화벽에 대한 하나 이상의 재귀 DNS(RDNS) 서버 주소를 추가합

레이어 **3** 서브인터페이스 설정	구성 위치	설명
		니다. RDNS 서버는 루트 DNS와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에게 보내는 NDP 라우터 광고에서 위에서 아래로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있으며, 그런 다음 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다.
유효 시간		IPv6 DNS 클라이언트가 라우터 광고를 수신한 후 클라이언트가 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간(초)을 입력하십시오(범위는 최대 인터벌(초)에서 최대 인터벌의 두 배, 기본값은 1,200).
도메인 검색 목록	**Layer3** 서브인터페이스 > **IPv6** > **DNS** 지원, 유형 = 정적	DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(서픽스)을 추가합니다. 최대 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하여 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가하고 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가 "company.com"인 경우 라우터의 결과 쿼리는 정규화된 도메인 이름 "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록에 있는 모든 서픽스를 시도할 때까지 DNS 서픽스를 사용합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 사용하는 NDP 라우터 광고에서 방화벽이 보내는 DNS 검색 목록 옵션에 대해 최대 8개의 도메인 이름(서픽

레이어 **3** 서브인터페이스 설정	구성 위치	설명
		스)을 구성할 수 있습니다. 서픽스를 선택한 다음 위로 이동 또는 아래로 이동하여 순서를 변경하거나 더 이상 필요하지 않은 경우 서픽스를 삭제합니다.
유효 기간		IPv6 DNS 클라이언트가 DNS 검색 목록에서 도메인 이름(서픽스)을 사용할 수 있다는 라우터 알림을 수신한 후 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)의 값에서 최대 인터벌의 두 배, 기본값은 1,200입니다.).
DNS 재귀 네임 서버	**Layer3** 서브인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 DNS 재귀 네임 서버 정보를 보내도록 합니다. • 수동 - DNS 재귀 네임 서버를 수동으로 구성합니다. 수동을 선택하는 경우 방화벽이 이 IPv6 VLAN 인터페이스에서 NDP 라우터 알림을 보낼 재귀 DNS(RDNS) 서버의 IPv6 주소를 추가합니다. RDNS 서버는 루트 DNS 서버와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에게 보내는 NDP 라우터 광고에서 위에서 아래로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있으며, 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다. 클라이언트가 특정 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간인 유효 기간명을 초 단위로 입력합니다. 범위는 4~3,600입니다. 기본값은 1,200입니다.
도메인 검색 목록	**Layer3** 서브인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 도메인 검색 목록 정보를 보내도록 합니다. • 수동 - 도메인 검색 목록을 수동으로 구성합니다. 수동을 선택한 경우 추가하고 DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(접미사)을 구성합니다. 최대 접미사 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 이름을 DNS 쿼리에 입력하기 전에 정규화되지 않은 도메인 이름에 추가(한 번에 하나씩)하여 DNS 쿼리에서 정규화된 도메인 이름을 사용하는

레이어 **3** 서브인터페이스 설정	구성 위치	설명
		도메인 접미사 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가한 다음 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 접미사가 'company.com'인 경우 라우터의 결과 DNS 쿼리는 정규화된 도메인 이름 'quality.company.com'에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록의 두 번째 DNS 접미사를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 접미사 무시) 또는 라우터가 목록에 있는 모든 접미사를 시도할 때까지 DNS 접미사를 시도합니다. 이웃 검색 DNSSL 옵션에서 DNS 클라이언트 라우터에 제공하려는 접미사로 방화벽을 구성합니다. DNSSL 옵션을 수신하는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에서 접미사를 사용합니다. 클라이언트가 특정 도메인 검색 목록을 사용할 수 있는 최대 시간인 유효 기간을 초 단위로 입력합니다. 범위는 4~3,600입니다. 기본값은 1,200입니다. 동일한 순서로 해당 주소를 사용하는 받는 사람에 대한 NDP 라우터 알림에서 방화벽이 보내는 DNS 검색 목록에 대해 최대 8개의 도메인 이름(접미사)을 구성할 수 있습니다. 접미사를 선택하고 위로 또는 아래로를 선택하여 순서를 변경하거나 더 이상 필요하지 않은 접미사를 목록에서 삭제합니다.
SD-WAN 인터페이스 프로파일	**Layer3** 서브인터페이스 > **SD-WAN**	이 서브인터페이스에 할당할 SD-WAN 인터페이스 프로파일을 선택하거나 새 프로파일을 만듭니다.
관리 프로파일	**Layer3** 서브인터페이스 > 고급 > 기타 정보	관리 프로파일 - 이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 프로파일을 선택합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방

레이어 **3** 서브인터페이스 설정	구성 위치	설명
		화벽은 패킷이 과다하게 크다는 것을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.
TCP MSS 조정	**Layer3** 서브인터페이스 > 고급 > 기타 정보	인터페이스 MTU 바이트 크기 내의 모든 헤더에 대한 바이트를 수용하도록 최대 세그먼트 크기(MSS)를 조정하려면 선택합니다. MTU 바이트 크기에서 MSS 조정 크기를 뺀 값은 IP 프로토콜에 따라 달라지는 MSS 바이트 크기와 같습니다. • **IPv4 MSS** 조정 크기 - 범위는 40~300이고, 기본값은 40입니다. • **IPv6 MSS** 조정 크기 - 범위는 60~300이고, 기본값은 60입니다. 이 설정을 사용하여 네트워크를 통한 터널에 더 작은 MSS가 필요한 경우를 해결하십시오. 패킷이 조각화 없이 MSS보다 더 많은 바이트를 갖는 경우 이 설정을 사용하면 조정할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로 VLAN 태그가 있는 MPLS 헤더 또는 터널링된 트래픽과 같은 항목에 대해 바이트를 허용하도록 MSS 조정 크기를 구성하는 데 도움이 됩니다.
IP 주소 MAC 주소	**Layer3** 서브인터페이스 > 고급 > **ARP** 엔트리	하나 이상의 고정 ARP(주소 확인 프로토콜) 항목을 추가하려면 IP 주소 및 관련 하드웨어 [미디어 액세스 제어(MAC)] 주소를 추가합니다. 항목을 삭제하려면 항목을 선택한 다음 삭제를 클릭합니다. 고정 ARP 항목은 ARP 처리를 줄입니다.
IPv6 주소 MAC 주소	**Layer3** 서브인터페이스 > 고급 > **ND** 항목	NDP(Neighbor Discovery Protocol)에 대한 네이버 정보를 제공하려면 해당 네이버의 IP 주소와 MAC 주소를 추가합니다.
NDP 프록시 사용	**Layer3** 서브인터페이스 > 고급 > **NDP** 프록시	인터페이스에 대해 NDP(Neighbor Discovery Protocol) 프록시를 활성화합니다. 방화벽은 이 목록의 IPv6 주소에 대한 MAC 주소를 요청하는 ND 패킷에 응답합니다. ND 응답에서 방화벽은 인터페이스에 대한 자체 MAC 주소를 전송하여 방화벽이 목록의 주소에 대한 패킷을 수신하도록 합니다. NPTv6(Network Prefix Translation IPv6)을 사용하는 경우 NDP 프록시를 활성화하는 것이 좋습니다. **NDP** 프록시 사용을 선택한 경우 필터를 입력하고 필터 적용(회색 화살표)을 클릭하여 수많은 주소 항목을 필터링할 수 있습니다.

레이어 3 서브인터페이스 설정	구성 위치	설명
주소		방화벽이 NDP 프록시로 작동할 IPv6 주소, IP 범위, IPv6 서브넷 또는 주소 개체를 하나 이상 추가합니다. 이상적으로는 이러한 주소 중 하나가 NPTv6의 소스 번역 주소와 동일합니다. 주소의 순서는 중요하지 않습니다. 주소가 하위 네트워크인 경우 방화벽은 서브넷의 모든 주소에 대해 ND 응답을 보내므로 방화벽의 IPv6 인접 항목도 추가한 다음 무효를 클릭하여 방화벽이 이러한 IP 주소에 응답하지 않도록 지시하는 것이 좋습니다.
무효		해당 주소에 대한 NDP 프록시를 방지하려면 주소를 무효합니다. 지정된 IP 주소 범위 또는 IP 서브넷의 하위 집합을 무효화할 수 있습니다.
설정	**Layer3** 서브인터페이스 > 고급 > **DDNS**	설정을 선택하여 DDNS 필드를 구성할 수 있도록 합니다.
활성화		인터페이스에서 DDNS를 활성화합니다. DDNS를 구성하려면 처음에 활성화해야 합니다. (DDNS 설정이 완료되지 않은 경우 부분 설정을 잃지 않도록 활성화하지 않고 저장할 수 있습니다.)
업데이트 인터벌(일)	**Layer3** 서브인터페이스 > 고급 > **DDNS**	FQDN에 매핑된 IP 주소를 업데이트하기 위해 방화벽이 DDNS 서버에 보내는 업데이트 인터벌(일)을 입력합니다(범위는 1~30, 기본값은 1). 또한 방화벽은 *DHCP* 서버에서 인터페이스에 대한 새 *IP* 주소를 수신하면 *DDNS*를 업데이트 합니다.
인증서 프로파일		DDNS 서비스를 확인하기 위해 인증서 프로파일을 생성합니다. DDNS 서비스는 인증 기관(CA)이 서명한 인증서를 방화벽에 제공합니다.
호스트네임		DDNS 서버에 등록된 인터페이스의 호스트 이름(예: host123.domain123.com, host123)을 입력합니다. 방화벽은 구문이 도메인 이름에 대해 DNS에서 허용하는 유효한 문자를 사용하는지 확인하는 경우를 제외하고 호스트 이름의 유효성을 검사하지 않습니다.

레이어 **3** 서브인터페이스 설정	구성 위치	설명
공급자	**Layer3** 서브인터페이스 > 고급 > **DDNS**	이 인터페이스에 DDNS 서비스를 제공하는 DDNS 공급자(및 버전)를 선택하십시오. • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS** - SD-WAN AE 서브인터페이스 또는 SD-WAN Layer 3 서브인터페이스에 대해 이 공급자를 선택해야 합니다. 방화벽에서 특정 날짜까지 단계적으로 중단될 것이라고 표시하는 *DDNS* 서비스의 이전 버전을 선택하는 경우 최신 버전으로 이동합니다. 공급자 이름 뒤에 오는 이름 및 값 필드는 공급자별로 다릅니다. 읽기 전용 필드는 방화벽이 DDNS 서비스에 연결하는 데 사용하는 매개변수를 알려줍니다. DDNS 서비스가 사용자에게 제공하는 비밀번호 및 DDNS 서버에서 응답을 수신하지 않는 경우 방화벽이 사용하는 타임아웃와 같은 다른 필드를 구성합니다.
IPv4 탭 - IP		인터페이스에 구성된 IPv4 주소를 추가한 다음 선택합니다. DDNS 공급자가 허용하는 만큼만 IPv4 주소를 선택할 수 있습니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
IPv6 탭 - IPv6		인터페이스에 구성된 IPv6 주소를 추가한 다음 선택합니다. DDNS 공급자가 허용하는 만큼만 IPv6 주소를 선택할 수 있습니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
런타임 정보 표시	**Layer3** 서브인터페이스 > 고급 > **DDNS**	DDNS 등록을 표시합니다. DDNS 공급자, 확인된 FQDN 및 기본 IP 주소를 나타내는 별표(*)가 있는 매핑된 IP 주소. 각 DDNS 공급자에는 문제 해결을 위해 호스트 이름 업데이트 상태와 반환 날짜를 나타내는 고유한 반환 코드가 있습니다.

로그 카드 인터페이스

- 네트워크 > 인터페이스 > 이더넷

로그 처리 카드(LPC)가 있는 PA-7000 시리즈 방화벽에서 로그 포워딩을 구성하는 경우 하나의 데이터 포트를 로그 카드 유형으로 구성해야 합니다. 이는 이 방화벽 모델의 트래픽 및 로깅 기능이 관리(MGT) 인터페이스의 기능을 초과하기 때문입니다. 로그 카드 데이터 포트는 syslog, 이메일, SNMP(Simple Network Management Protocol), Panorama 로그 포워딩 및 WildFire™ 파일 포워딩에 대한 로그 포워딩을 수행합니다.

로그 카드 유형으로 방화벽에서 하나의 포트만 구성할 수 있습니다. 로그 포워딩을 활성화했지만 로그 카드 유형으로 인터페이스를 구성하지 않은 경우 변경 사항을 커밋하려고 할 때 오류가 발생합니다.

이 정보는 *LPC(*로그 처리 카드*)* 구성과 관련이 있습니다. *LFC(*로그 포워딩 카드*)*를 구성하는 방법을 알아보려면 디바이스 > 로그 포워딩 카드을*(*를*)* 참조하십시오.

로그 카드 인터페이스를 구성하려면 구성되지 않은 인터페이스(예: ethernet1/16)를 선택한 다음 다음 표에 설명된 설정을 구성합니다.

로그 카드 인터페이스 설정	구성 위치	설명
슬롯	이더넷 인터페이스	인터페이스의 슬롯 번호(1-12)를 선택합니다.
인터페이스 이름		인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형		로그 카드를 선택합니다.
IPv4	이더넷 인터페이스 > 로그 카드 전달	네트워크에서 IPv4를 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv4 주소입니다. • 넷마스크 - 포트의 IPv4 주소에 대한 네트워크 마스크입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv4 주소입니다.
IPv6		네트워크에서 IPv6을 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv6 주소입니다.

로그 카드 인터페이스 설정	구성 위치	설명
		• 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv6 주소입니다.
링크 속도	이더넷 인터페이스 > 고급	인터페이스 속도를 Mbps(**10**, **100** 또는 **1000**) 단위로 선택하거나 자동(기본값)을 선택하면 방화벽이 연결을 기반으로 속도를 자동으로 결정합니다. 속도를 구성할 수 없는 인터페이스의 경우 **auto**가 유일한 옵션입니다.  연결에 권장되는 최소 속도는 ***1000****(Mbps)*입니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**)인지, 반이중(**half**)인지, 연결에 따라 자동으로 조정되는지(**auto**) 선택합니다. 기본값은 자동입니다.
링크 상태		인터페이스 상태를 활성화(**up**), 비활성화(**down**) 또는 연결에 따라 자동으로 결정(**auto**)할지의 여부를 선택합니다. 기본값은 자동입니다.

로그 카드 서브인터페이스

- 네트워크 > 인터페이스 > 이더넷

로그 카드 인터페이스을(를) 추가하려면 해당 인터페이스의 행인 서브 인터페이스 추가를 선택한 후 다음 정보를 지정합니다.

로그 카드 서브인터페이스 설정	구성 위치	설명
인터페이스 이름	**LPC** 서브인터페이스	인터페이스 이름(읽기 전용)은 선택한 로그 카드 인터페이스의 이름을 표시합니다. 인접한 필드에 숫자 서픽스(1-9,999)를 입력하여 서브인터페이스를 식별합니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
태그		서브인터페이스에 대한 VLAN 태그(0-4,094)를 입력합니다.

로그 카드 서브인터페이스 설정	구성 위치	설명
		사용하기 쉽도록 태그를 서브인터페이스 번호와 동일하게 만드십시오.
가상 시스템	**LPC** 서브인터페이스 > 컨피그	LPC(Log Processing Card) 서브인터페이스가 할당된 가상 시스템(vsys)을 선택합니다. 또는 가상 시스템을 클릭하여 새 vsys를 추가할 수 있습니다. LPC 서브인터페이스가 vsys에 할당되면 해당 인터페이스는 로그 카드에서 로그(syslog, 이메일, SNMP)를 포워딩하는 모든 서비스의 소스 인터페이스로 사용됩니다.
IPv4	이더넷 인터페이스 > 로그 카드 전달	네트워크에서 IPv4를 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv4 주소입니다. • 넷마스크 - 포트의 IPv4 주소에 대한 네트워크 마스크입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv4 주소입니다.
IPv6		네트워크에서 IPv6을 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv6 주소입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv6 주소입니다.

미러 인터페이스 복호화

- 네트워크 > 인터페이스 > 이더넷

Decryption Port Mirror 기능을 사용하려면 **Decrypt Mirror** 인터페이스 유형을 선택해야 합니다. 이 기능을 사용하면 방화벽에서 복호화된 트래픽의 복사본을 만들고 보관 및 분석을 위해 NetWitness 또는 Solera와 같은 원시 패킷 캡처를 수신할 수 있는 트래픽 수집 도구로 보낼 수 있습니다. 포렌식 및 기록 목적 또는 데이터 누출 방지(DLP) 기능을 위해 포괄적인 데이터 캡처가 필요한 조직에는 이 기능이 필요합니다. 이 기능을 활성화하려면 무료 라이선스를 취득하여 설치해야 합니다.

공용 클라우드 플랫폼*(AWS, Azure, Google Cloud Platform), VMware NSX* 및 *Citrix SDX*용 *VM* 시리즈에서는 복호화 포트 미러링을 사용할 수 없습니다.

복호화 인터페이스를 구성하려면 구성되지 않은 인터페이스(예: ethernet1/1)의 이름을 클릭하고 다음 정보를 지정합니다.

미러 인터페이스 설정 복호화	설명
인터페이스 이름	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다.
코멘트	인터페이스에 대한 선택적 설명을 입력합니다.
인터페이스 유형	미러 복호화를 선택합니다.
링크 속도	인터페이스 속도를 Mbps(**10**, **100** 또는 **1000**) 단위로 선택하거나 자동을 선택하여 방화벽이 속도를 자동으로 결정하도록 합니다.
링크 듀플렉스	인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태	인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는 지(**auto**)를 선택합니다.

통합 이더넷(AE) 인터페이스 그룹

- 네트워크 > 인터페이스 > 이더넷 > 통합 그룹 추가

통합 이더넷(AE) 인터페이스 그룹은 IEEE 802.1AX 링크 통합을 사용하여 방화벽을 다른 네트워크 디바이스나 다른 방화벽에 연결하는 단일 가상 인터페이스에 여러 이더넷 인터페이스를 결합합니다. AE 인터페이스 그룹은 결합된 인터페이스에서 트래픽을 로드 밸런싱하여 피어 간의 대역폭을 증가시킵니다. 또한 중복성을 제공합니다. 한 인터페이스에 장애가 발생하면 나머지 인터페이스는 계속해서 트래픽을 지원합니다. SD-WAN은 레이어 3 인터페이스의 AE 인터페이스 그룹을 지원합니다.

AE 인터페이스 그룹을 구성하기 전에 해당 인터페이스를 구성해야 합니다. 특정 집합 그룹에 할당된 인터페이스 중에서 하드웨어 미디어는 다를 수 있지만(예: 광섬유와 구리를 혼합할 수 있음) 대역폭(1Gbps, 10Gbps, 40Gbps 또는 100Gbps) 및 인터페이스 유형(HA3, 가상 와이어, 레이어 2 또는 레이어 3)은 동일해야 합니다.

추가할 수 있는 AE 인터페이스 그룹의 수는 방화벽 모델에 따라 다릅니다. 제품 선택 도구는 각 방화벽 모델이 지원하는 ## ## #####를 나타냅니다. 각 AE 인터페이스 그룹은 최대 8개의 인터페이스를 가질 수 있습니다.

PA-3200 시리즈, PA-5200 시리즈 및 PA-7000 시리즈 방화벽에서 QoS는 처음 8개의 AE 인터페이스 그룹에서만 지원됩니다.

VM 시리즈 모델을 제외한 모든 *Palo Alto Networks* 방화벽은 *AE* 인터페이스 그룹을 지원합니다.

고가용성*(HA)* 능동형/능동형 구성에서 *HA3(*패킷 포워딩*)* 인터페이스를 통합할 수 있지만 다음 방화벽 모델에서만 가능합니다.

- *PA-220*
- *PA-800* 시리즈
- *PA-3200* 시리즈
- *PA-5200* 시리즈

AE 인터페이스 그룹을 구성하려면 통합 그룹을 추가하고, 다음 표에 설명된 설정을 구성한 다음 그룹에 인터페이스를 할당합니다(통합 이더넷(AE) 인터페이스 참조).

인터페이스 그룹 설정 통합	구성 위치	설명
인터페이스 이름	통합 이더넷 인터페이스	읽기 전용 인터페이스 이름은 **ae**로 설정됩니다. 인접한 필드에 AE 인터페이스 그룹을 식별하는 숫자 서픽스를 입력합니다. 숫자 서픽스의 범위는 방화벽 모델이 지원하는 AE 그룹 수에 따라 다릅니다. 제품 선택 도구에서 방화벽 모델별로 지원되는 ## ## #####를 참조하세요.
코멘트		(선택 사항) 인터페이스에 대한 설명을 입력합니다.
인터페이스 유형		나머지 구성 요구 사항 및 옵션을 제어하는 인터페이스 유형을 선택합니다. • **HA** - 인터페이스가 능동형/능동형 배포에서 두 방화벽 간의 HA3 링크인 경우에만 선택합니다. 선택적으로 **NetFlow** 프로파일을 선택한 다음 **LACP** 탭에서 설정을 구성합니다(LACP 활성화 참조). • 가상 와이어 - (선택 사항) 가상 와이어 설정에 설명된 대로 **NetFlow** 프로파일을 선택한 다음 구성 및 **Advanced** 탭에서 설정을 구성합니다. • 레이어 **2** - (선택 사항) **NetFlow** 프로파일을 선택합니다. 레이어 2 인터페이스 설정에 설명된 대로 구성 및 **Advanced** 탭에서 설정을 구성합니다. 선택적으로 **LACP** 탭을 구성합니다(LACP 활성화 참조).

인터페이스 그룹 설정 통합	구성 위치	설명
		• 레이어 **3** - (선택 사항) **NetFlow** 프로파일을 선택합니다. 레이어 3 인터페이스 설정에 설명된 대로 구성 탭, **IPv4** 또는 **IPv6** 탭 및 **Advanced** 탭에서 설정을 구성합니다. 선택적으로 **LACP** 탭을 구성합니다(LACP 활성화 참조). SD-WAN은 레이어 3 인터페이스 및 하위 인터페이스의 AE 인터페이스 그룹을 지원합니다.
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일 또는 **NetFlow** 프로파일을 선택하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). AE 인터페이스 그룹에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
LACP 활성화	통합 이더넷 인터페이스 > **LACP**	AE 인터페이스 그룹에 대해 LACP(Link Aggregation Control Protocol)를 활성화하려면 선택합니다. LACP는 기본적으로 비활성화되어 있습니다. LACP를 활성화하면 방화벽과 해당 LACP 피어가 직접 연결되어 있는지의 여부와 관계없이 물리적 및 데이터 링크 레이어에서 인터페이스 오류 감지가 자동으로 수행됩니다. (LACP가 없으면 인터페이스 장애 감지는 직접 연결된 피어 간의 물리적 레이어에서만 자동으로 수행됩니다.) LACP는 또한 핫 스페어를 구성하는 경우 대기 인터페이스에 대한 자동 페일오버를 활성화합니다(최대 포트 참조).
방법		방화벽의 LACP 모드를 선택합니다. 두 LACP 피어 간에 하나는 활성으로, 다른 하나는 수동으로 구성하는 것이 좋습니다. 두 피어가 모두 수동인 경우 LACP가 작동할 수 없습니다. • 수동(기본값) - 방화벽이 피어 디바이스의 LACP 상태 쿼리에 수동으로 응답합니다. • 활성 - 방화벽이 피어 디바이스의 LACP 상태(사용 가능 또는 응답 없음)를 능동적으로 쿼리합니다.
전송 속도		방화벽이 피어 디바이스와 쿼리 및 응답을 교환하는 속도를 선택합니다. • 빠름 - 매초 • 느림(기본값) - 30초마다
빠른 페일오버		인터페이스가 다운될 때 방화벽이 1초 이내에 작동 인터페이스로 페일오버되도록 하려면 선택합니다. 그렇지 않으면 표준 IEEE 802.1AX 정의 속도(최소 3초)로 페일오버가 발생합니다.

인터페이스 그룹 설정 통합	구성 위치	설명
시스템 우선 순위	통합 이더넷 인터페이스 > **LACP(**계속**)**	방화벽 또는 해당 피어가 포트 우선 순위와 관련하여 다른 것을 무시할지의 여부를 결정하는 숫자입니다(아래 최대 포트 참조). 숫자가 낮을수록 우선 순위가 높아집니다(범위는 *1~65,535*, 기본값은 *32,768*).
최대 인터페이스		LACP 통합 그룹에서 주어진 시간에 활성화될 수 있는 인터페이스 수(1 ~ 8). 이 값은 그룹에 할당한 인터페이스 수를 초과할 수 없습니다. 할당된 인터페이스 수가 활성 인터페이스 수를 초과하는 경우 방화벽은 인터페이스의 LACP 포트 우선 순위를 사용하여 대기 모드에 있는 인터페이스를 결정합니다. 그룹에 대한 개별 인터페이스를 구성할 때 LACP 포트 우선 순위를 설정합니다(통합 이더넷(AE) 인터페이스 참조).
HA 수동 상태에서 활성화		HA 능동형/수동형 구성에 배포된 방화벽의 경우 페일오버가 발생하기 전에 수동 방화벽이 활성 피어와 LACP를 사전 협상할 수 있도록 선택합니다. 사전 협상은 수동 방화벽이 활성 상태가 되기 전에 LACP를 협상할 필요가 없기 때문에 페일오버 속도를 높입니다.
능동형/수동형 HA에 대해 동일한 시스템 MAC 주소	통합 이더넷 인터페이스 > **LACP(**계속**)**	이는 HA 능동형/수동형 구성에 배포된 방화벽에만 적용됩니다. 능동형/능동형 구성의 방화벽에는 고유한 MAC 주소가 필요합니다. HA 방화벽 피어는 동일한 시스템 우선 순위 값을 갖습니다. 그러나 능동형/수동형 배포에서는 동일한 MAC 주소를 할당하는지의 여부에 따라 각각의 시스템 ID가 같을 수도 있고 다를 수도 있습니다. *LACP* 피어*(HA* 모드에서도*)*가 가상화될 때*(*네트워크에 단일 디바이스로 표시됨*)* 방화벽에 대해 동일한 시스템 *MAC* 주소를 사용하면 페일오버 중 대기 시간이 최소화됩니다. *LACP* 피어가 가상화되지 않은 경우 각 방화벽의 고유한 *MAC* 주소를 사용하여 페일오버 대기 시간을 최소화합니다. LACP는 MAC 주소를 사용하여 각 LACP 피어에 대한 시스템 ID를 도출합니다. 방화벽 쌍과 피어 쌍이 동일한 시스템 우선 순위 값을 갖는 경우 LACP는 시스템 ID 값을 사용하여 포트 우선 순위와 관련하여 어느 쪽이 다른 쪽보다 우선하는지 결정합니다. 두 방화벽에 동일한 MAC 주소가 있는 경우 둘 다 동일한 시스템 ID를 갖게 되며 이는 LACP 피어의 시스템 ID보다 높거나 낮습니다. HA 방화벽에 고유한 MAC 주소가 있는 경우 하나는 LACP 피어보다 높은

인터페이스 그룹 설정 통합	구성 위치	설명
		시스템 ID를 갖고 다른 하나는 더 낮은 시스템 ID를 가질 수 있습니다. 후자의 경우 방화벽에서 페일오버가 발생하면 포트 우선 순위가 LACP 피어와 활성화되는 방화벽 간에 전환됩니다.
MAC 주소	통합 이더넷 인터페이스 > **LACP(**계속**)**	동일한 시스템 **MAC** 주소를 사용하는 경우 시스템 생성 MAC 주소를 선택하거나 능동형/수동형 HA 쌍의 두 방화벽에 대해 고유한 MAC 주소를 입력합니다. 주소가 전역적으로 고유한지 확인해야 합니다.
SD-WAN 인터페이스 프로파일	통합 이더넷 인터페이스 > **SD-WAN**	AE 인터페이스 그룹에 적용할 SD-WAN 인터페이스 프로파일을 선택하거나 새 프로파일을 생성합니다.
관리 프로파일	통합 이더넷 인터페이스 > 고급 > 다른 정보	이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 관리 프로파일을 선택합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방화벽은 패킷이 과다하게 크다는 것을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.
TCP MSS 조정		인터페이스 MTU 바이트 크기 내의 모든 헤더에 대한 바이트를 수용하도록 최대 세그먼트 크기(MSS)를 조정하려면 선택합니다. MTU 바이트 크기에서 MSS 조정 크기를 뺀 값은 IP 프로토콜에 따라 달라지는 MSS 바이트 크기와 같습니다. • **IPv4 MSS** 조정 크기 - 범위는 40~300이고, 기본값은 40입니다. • **IPv6 MSS** 조정 크기 - 범위는 60~300이고, 기본값은 60입니다. 이 설정을 사용하여 네트워크를 통한 터널에 더 작은 MSS가 필요한 경우를 해결하십시오. 패킷이 조각화 없이 MSS보다 더 많은 바이트를 갖는 경우 이 설정을 사용하면 조정할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로 VLAN 태그가 있는 MPLS 헤더 또는 터널링된 트래픽과 같은 항목에 대해 바이트를 허용하도록 MSS 조정 크기를 구성하는 데 도움이 됩니다.

인터페이스 그룹 설정 통합	구성 위치	설명
태그가 지정되지 않은 서브인터페이스		이 인터페이스에 대한 해당 서브인터페이스에 태그가 지정되지 않은 경우 이 옵션을 선택합니다.
IP 주소 MAC 주소	통합 이더넷 인터페이스 > 고급 > **ARP** 엔트리	하나 이상의 고정 ARP(주소 확인 프로토콜) 항목을 추가하려면 IP 주소 및 관련 하드웨어 [미디어 액세스 제어(MAC)] 주소를 추가합니다. 항목을 삭제하려면 항목을 선택한 다음 삭제를 클릭합니다. 고정 ARP 항목은 ARP 처리를 줄입니다.
IPv6 주소 MAC 주소	통합 이더넷 인터페이스 > 고급 > **ND** 항목	NDP(Neighbor Discovery Protocol)에 대한 네이버 정보를 제공하려면 네이버의 IPv6 주소와 MAC 주소를 추가합니다.
NDP 프록시 사용	통합 이더넷 인터페이스 > 고급 > **NDP** 프록시	인터페이스에 대해 NDP(Neighbor Discovery Protocol) 프록시를 활성화합니다. 방화벽은 이 목록의 IPv6 주소에 대한 MAC 주소를 요청하는 ND 패킷에 응답합니다. ND 응답에서 방화벽은 인터페이스에 대한 자체 MAC 주소를 전송하여 방화벽이 목록의 주소에 대한 패킷을 수신하도록 합니다. NPTv6(Network Prefix Translation IPv6)을 사용하는 경우 NDP 프록시를 활성화하는 것이 좋습니다. **NDP** 프록시 사용을 선택한 경우 필터를 입력하고 필터 적용(회색 화살표)을 클릭하여 수많은 주소 항목을 필터링할 수 있습니다.
주소		방화벽이 NDP 프록시로 작동할 IPv6 주소, IP 범위, IPv6 서브넷 또는 주소 개체를 하나 이상 추가합니다. 이상적으로는 이러한 주소 중 하나가 NPTv6의 소스 번역 주소와 동일합니다. 주소의 순서는 중요하지 않습니다. 주소가 하위 네트워크인 경우 방화벽은 서브넷의 모든 주소에 대해 ND 응답을 보내므로 방화벽의 IPv6 인접 항목도 추가한 다음 무효를 클릭하여 방화벽이 이러한 IP 주소에 응답하지 않도록 지시하는 것이 좋습니다.
무효		해당 주소에 대한 NDP 프록시를 방지하려면 주소를 무효합니다. 지정된 IP 주소 범위 또는 IP 서브넷의 하위 집합을 무효화할 수 있습니다.

인터페이스 그룹 설정 통합	구성 위치	설명
LLDP 활성화	통합 이더넷 인터페이스 > 고급 > **LLDP**	인터페이스에 대해 LLDP(Link Layer Discovery Protocol)를 활성화합니다. LLDP는 링크 레이어에서 기능하여 LLDP 데이터 단위를 이웃과 주고받아 이웃 디바이스와 해당 기능을 검색합니다.
LLDP 프로파일		LLDP 프로파일을 선택하거나 새 LLDP 프로파일을 만듭니다. 프로파일은 LLDP 모드를 구성하고, syslog 및 SNMP 알림을 활성화하고, LLDP 피어로 전송하려는 선택적 TLV(Type-Length-Values)를 구성하는 방법입니다.
설정	통합 이더넷 인터페이스 > 고급 > **DDNS**	설정을 선택하여 DDNS 필드를 구성할 수 있도록 합니다.
활성화		인터페이스에서 DDNS를 활성화합니다. DDNS를 구성하려면 처음에 활성화해야 합니다. (DDNS 설정이 완료되지 않은 경우 부분 설정을 잃지 않도록 활성화하지 않고 저장할 수 있습니다.)
업데이트 인터벌(일)		FQDN에 매핑된 IP 주소를 업데이트하기 위해 방화벽이 DDNS 서버에 보내는 업데이트 인터벌(일)을 입력합니다(범위는 1~30, 기본값은 1). 또한 방화벽은 *DHCP* 서버에서 인터페이스에 대한 새 *IP* 주소를 수신하면 *DDNS*를 업데이트합니다.
인증서 프로파일		DDNS 서비스를 확인하기 위해 인증서 프로파일을 생성합니다. DDNS 서비스는 인증 기관(CA)이 서명한 인증서를 방화벽에 제공합니다.
호스트네임		DDNS 서버에 등록된 인터페이스의 호스트 이름(예: host123.domain123.com, host123)을 입력합니다. 방화벽은 구문이 도메인 이름에 대해 DNS에서 허용하는 유효한 문자를 사용하는지 확인하는 경우를 제외하고 호스트 이름의 유효성을 검사하지 않습니다.
공급자	통합 이더넷 인터페이스 > 고급 > **DDNS**	이 인터페이스에 DDNS 서비스를 제공하는 DDNS 공급자(및 버전)를 선택하십시오. • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1**

인터페이스 그룹 설정 통합	구성 위치	설명
		• **No-IP v1** • **Palo Alto Networks DDNS**(DDNS가 있는 SD-WAN Full Mesh, SD-WAN AE 서브인터페이스 및 SD-WAN Layer 3 서브인터페이스에 적용) 방화벽에서 특정 날짜까지 단계적으로 중단될 것이라고 표시하는 *DDNS* 서비스의 이전 버전을 선택하는 경우 최신 버전으로 이동합니다. 공급자 이름 뒤에 오는 이름 및 값 필드는 공급자별로 다릅니다. 읽기 전용 필드는 방화벽이 DDNS 서비스에 연결하는 데 사용하는 매개변수를 알려줍니다. DDNS 서비스가 사용자에게 제공하는 비밀번호 및 DDNS 서버에서 응답을 수신하지 않는 경우 방화벽이 사용하는 타임아웃과 같은 다른 필드를 구성합니다.
IPv4 탭		인터페이스에 구성된 IPv4 주소를 추가한 다음 선택합니다. DDNS 공급자가 허용하는 만큼만 IPv4 주소를 선택할 수 있습니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
IPv6 탭		인터페이스에 구성된 IPv6 주소를 추가한 다음 선택합니다. DDNS 공급자가 허용하는 만큼만 IPv6 주소를 선택할 수 있습니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
런타임 정보 표시		DDNS 등록을 표시합니다. DDNS 공급자, 확인된 FQDN 및 기본 IP 주소를 나타내는 별표(*)가 있는 매핑된 IP 주소. 각 DDNS 공급자에는 문제 해결을 위해 호스트 이름 업데이트 상태와 반환 날짜를 나타내는 고유한 반환 코드가 있습니다.

통합 이더넷(AE) 인터페이스

- 네트워크 > 인터페이스 > 이더넷

통합 이더넷(AE) 인터페이스를 구성하려면 먼저 통합 이더넷(AE) 인터페이스 그룹을 추가합니다. 그런 다음 해당 그룹에 할당할 인터페이스의 이름을 클릭합니다. 특정 그룹에 할당하는 인터페이스 중에서 하드웨어 미디어는 다를 수 있지만(예: 광섬유와 구리를 혼합할 수 있음) 대역폭과 인터페이스 유형(예: Layer 3)은 동일해야 합니다. 또한 인터페이스 유형은 AE 인터페이스 그룹에 대해 정의된 것과 동일해야 하지만 각 인터페이스를 구성할 때 유형을 **Aggregate Ethernet**으로 변경합니다. 그룹에 할당하는 각 인터페이스에 대해 다음 정보를 지정합니다.

AE 인터페이스 그룹에 대해 *LACP(Link Aggregation Control Protocol)*를 활성화한 경우 해당 그룹의 모든 인터페이스에 대해 동일한 ***Link Speed*** 및 ***Link Duplex***를 선택합니다. 일치하지 않는 값의 경우 커밋 작업은 경고를 표시하고 *PAN-OS*는 기본적으로 더 높은 속도와 전이중으로 설정됩니다.

통합 인터페이스 설정	구성 위치	설명
인터페이스 이름	통합 이더넷 인터페이스	인터페이스 이름은 사전 정의되어 있으며 변경할 수 없습니다. 인터페이스 이름에서 ae 뒤에 숫자를 입력합니다.
코멘트		(선택 사항) 인터페이스에 대한 설명을 입력합니다.
인터페이스 유형		통합 이더넷을 선택합니다.
통합 그룹		통합 그룹에 인터페이스를 할당합니다.
링크 속도	통합 이더넷 인터페이스 > 고급 > 링크 설정	인터페이스 속도를 Mbps 단위로 선택하거나 자동을 선택하여 방화벽이 속도를 자동으로 결정하도록 합니다.
링크 듀플렉스		인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태		인터페이스 상태가 활성화(**up**), 비활성화(**down**) 또는 자동으로 결정되는지(**auto**)를 선택합니다.
PoE Rsvd Pwr	통합 이더넷 인터페이스 > 고급 > **PoE** 설정 (지원되는 방화벽만 해당)	PoE가 활성화된 경우 할당된 전력량(와트)을 선택합니다.
PoE 활성화		이 인터페이스에서 PoE를 활성화하려면 선택합니다.
LACP 포트 우선 순위		방화벽은 통합 그룹에 대해 LACP(링크 통합 제어 프로토콜)를 활성화한 경우에만 이 필드를 사용합니다. 그룹에 할당한 인터페이스 수가 활성 인터페이스 수(최대 포트 필드)를 초과하는 경우 방화벽은 인터페이스의 LACP 포트 우선 순위를 사용하여 대기 모드에 있는 인터페이스를 결정합니다. 숫자 값이 낮을수록 우선 순위가 높아집니다(범위는 1-65,535, 기본값은 32,768).
가상 라우터	통합 이더넷 인터페이스 > 컨피그	Aggregate Ethernet 인터페이스를 할당할 가상 라우터를 선택합니다.

통합 인터페이스 설정	구성 위치	설명
보안 구역		Aggregate Ethernet 인터페이스를 할당할 보안 영역을 선택합니다.
SD-WAN 활성화	통합 이더넷 인터페이스 > **IPv4**	인터페이스에서 SD-WAN 기능을 활성화하려면 선택합니다.
Bonjour 리플렉터 활성화	통합 이더넷 인터페이스 > **IPv4**	(PA-220, PA-800 및 PA-3200 시리즈만 해당) 이 옵션을 활성화하면 방화벽은 Bonjour 멀티캐스트 광고와 쿼리를 이 인터페이스에서 수신하고 이 인터페이스로 포워딩하여 이 인터페이스를 활성화한 다른 모든 L3 및 AE 인터페이스와 서브인터페이스로 포워딩합니다. 옵션. 이는 보안 또는 관리 목적으로 트래픽을 라우팅하기 위해 세분화를 사용하는 네트워크 환경에서 사용자 액세스 및 디바이스 검색 가능성을 보장하는 데 도움이 됩니다. 최대 16개의 인터페이스에서 이 옵션을 활성화할 수 있습니다.
인터페이스에서 IPv6 활성화	통합 이더넷 인터페이스 > **IPv6**	이 인터페이스에서 IPv6을 활성화하려면 선택합니다.
인터페이스 ID		64비트 확장 고유 식별자(EUI-64)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 ID를 호스트 부분으로 사용하면 방화벽은 인터페이스 **ID**를 해당 주소의 호스트 부분으로 사용합니다.
주소	통합 이더넷 인터페이스 > **IPv6** > 주소 할당, 유형 = 정적	IPv6 주소 및 프리픽스 길이를 추가합니다(예: 2001:400:f00::1/64). 또는 기존 IPv6 주소 개체를 선택하거나 새 IPv6 주소 개체를 만듭니다.
인터페이스에서 주소 활성화		인터페이스에서 IPv6 주소를 활성화하려면 선택합니다.
인터페이스 ID를 호스트 부분으로 사용		인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다.
애니캐스트		가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다.
라우터 알림 보내기	통합 이더넷 인터페이스 >	이 IP 주소에 대해 라우터 광고(RA)를 활성화하려면 선택합니다. (인터페이스에서 글로벌 **Enable Router Advertisement** 옵션도 활

통합 인터페이스 설정	구성 위치	설명
	IPv6 > 주소 할당, 유형 = 정적	성화해야 합니다.) RA에 대한 자세한 내용은 이 표에서 라우터 알림 활성화를 참조하십시오. 다음 필드는 라우터 보급을 활성화한 경우에만 적용됩니다. • 유효 시간 - 방화벽이 주소가 유효한 것으로 간주하는 시간(초)입니다. 유효한 유효 시간은 기본 유효 시간과 같거나 초과해야 합니다. 기본값은 2,592,000입니다. • **Preferred Lifetime** - 유효한 주소가 선호되는 시간(초)입니다. 즉, 방화벽이 트래픽을 보내고 받는 데 사용할 수 있습니다. 기본 유효 시간이 만료되면 방화벽은 주소를 사용하여 새 연결을 설정할 수 없지만 기존 연결은 유효 시간이 만료될 때까지 유효합니다. 기본값은 604,800입니다. • 온링크 - 프리픽스 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지의 여부를 선택합니다. • **Autonomous**—시스템이 보급된 프리픽스를 인터페이스 ID와 결합하여 IP 주소를 독립적으로 생성할 수 있는지의 여부를 선택합니다.
라우터 알림 경로 수락	통합 이더넷 인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클라이언트	DHCPv6 클라이언트가 DHCP 서버에서 RA를 수락하도록 허용하려면 선택합니다.
기본 경로 측정 항목		인터페이스에서 ISP까지의 경로에 대한 기본 경로 메트릭을 입력합니다. 범위는 1~65,535입니다. 기본값은 10입니다.
기본 설정		두 개의 인터페이스(각각 중복성을 위해 다른 ISP에 연결됨)가 있는 경우 한 ISP에 대한 인터페이스에 다른 ISP에 대한 인터페이스보다 높은 기본 설정을 할당할 수 있도록 DHCPv6 클라이언트 인터페이스의 기본 설정(낮음, 중간 또는 높음)을 선택합니다. 기본 인터페이스에 연결된 ISP는 호스트 인터페이스에 보낼 위임된 접두사를 제공하는 ISP가 됩니다. 인터페이스의 기본 설정이 동일한 경우 두 ISP는 위임된 접두사를 제공하고 호스트는 사용할 접두사를 결정합니다.
IPv6 주소 활성화	통합 이더넷 인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클	이 DHCPv6 클라이언트에 대해 수신된 IPv6 주소를 활성화합니다.
비임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 비임시 주소를 요청합니다. 임시 주소보다 긴 유효 기간을 선택합니다.

통합 인터페이스 설정	구성 위치	설명
	라이언트 > **DHCPv6** 옵션	인터페이스에 대해 비임시 주소 또는 임시 주소를 요청하는지 여부는 사용자의 재량과 *DHCPv6* 서버의 기능에 따라 결정됩니다. 일부 서버는 임시 주소만 제공할 수 있습니다. 가장 좋은 방법은 비임시 주소와 임시 주소를 모두 선택하는 것입니다. 이 경우 방화벽은 비임시 주소를 선호합니다.
임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 임시 주소를 요청합니다. 주소는 짧은 기간 동안 사용하도록 되어 있으므로 더 높은 수준의 보안을 위해 임시 주소를 선택합니다.
신속한 커밋		간청, 광고, 요청 및 응답 메시지 프로세스가 아닌 요청 및 응답 메시지의 DHCP 프로세스를 사용하려면 선택합니다.
접두사 위임 활성화	통합 이더넷 인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클라이언트 > 접두사 위임	방화벽이 접두사 위임 기능을 지원할 수 있도록 접두사 위임을 활성화합니다. 즉, 인터페이스는 업스트림 DHCPv6 서버에서 접두사를 수락하고 선택한 접두사 풀에 접두사를 배치합니다. 여기서 방화벽은 SLAAC를 통해 접두사를 호스트에 위임합니다. 인터페이스에 대한 접두사 위임을 활성화 또는 비활성화하는 기능을 통해 방화벽은 여러 ISP(인터페이스당 하나의 ISP)를 지원할 수 있습니다. 이 인터페이스에서 접두사 위임을 활성화하면 접두사를 제공하는 ISP가 제어됩니다. DHCP 서버에서 받은 위임된 접두사는 요청한 인터페이스에서 사용할 수 없습니다.
DHCP 접두사 길이 힌트		방화벽이 선호하는 DHCPv6 접두사 길이를 DHCPv6 서버로 보내도록 하려면 선택합니다.
DHCP 접두사 길이(비트)		DHCPv6 서버에 힌트로 전송되는 기본 DHCPv6 접두사 길이를 48~64비트 범위로 입력합니다. 예를 들어, 접두사 길이를 *48*로 요청하면 서브넷에 *16*비트*(64-48)*가 남게 되는데, 이는 위임할 접두사의 많은 하위 분할이 필요하다는 것을 의미합니다. 반면에 *63*의 접두사 길이를 요청하면 *2*개의 서브넷만 위임하기 위한 *1*비트가 남습니다. *128*비트 중 호스트 주소용으로 *64*비트가 더 있습니다.

통합 인터페이스 설정	구성 위치	설명
접두사 풀 이름		방화벽이 수신된 접두사를 저장하는 접두사 풀의 이름을 입력합니다. 이름은 고유해야 하며 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄을 포함해야 합니다. 쉽게 알아볼 수 있도록 *ISP*를 반영하는 접두사 풀 이름을 사용합니다.
이름	통합 이더넷 인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	풀 이름을 입력하여 풀을 추가합니다. 이름은 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄일 수 있습니다.
주소 유형		하나를 고릅니다. • 풀의 **GUA** - 선택한 접두사 풀에서 제공되는 전역 유니캐스트 주소(GUA)입니다. • **ULA** - 고유 로컬 주소는 개인 네트워크 내 연결을 위한 주소 범위 fc00::/7의 개인 주소입니다. DHCP 서버가 없으면 ULA를 선택합니다. DHCPv6 서버는 선택한 접두사 길이를 보낼 권한이 있습니다.
인터페이스에서 활성화		(GUA) 인터페이스에서 주소를 활성화합니다.
접두사 풀		(GUA) GUA를 가져올 접두사 풀을 선택합니다.
할당 유형	통합 이더넷 인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	(GUA) 할당 유형을 선택합니다. • 동적 - DHCPv6 클라이언트는 상속된 인터페이스를 구성하기 위해 식별자를 선택해야 합니다. • 동적 식별자 - 사용자는 0~4,000 범위의 식별자를 선택하고 DHCPv6 클라이언트에서 고유한 식별자를 유지해야 합니다.
인터페이스에서 주소 활성화		(ULA) 인터페이스에서 주소를 활성화합니다.
주소		(ULA) 주소를 입력합니다.
인터페이스 ID를 호스트 부분으로 사용		(ULA) 인터페이스 ID를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다.

통합 인터페이스 설정	구성 위치	설명
애니캐스트		(선택 사항) IPv6 주소를 애니캐스트 주소로 만들려면 선택합니다. 즉, 여러 위치에서 동일한 접두사를 광고할 수 있으며 IPv6은 라우팅 프로토콜 비용 및 기타 요인을 기반으로 가장 가까운 노드로 애니캐스트 트래픽을 보냅니다.
라우터 알림 보내기		인터페이스에서 LAN 호스트로 라우터 알림(RA)을 보내려면 선택합니다.
온링크		접두사 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지 여부를 선택합니다.
자치		시스템이 광고된 접두사를 인터페이스 ID와 결합하여 IPv6 주소를 독립적으로 생성할 수 있는지 여부를 선택합니다.
중복 주소 감지 활성화	통합 이더넷 인터페이스 > **IPv6** > 주소 확인	DAD(중복 주소 감지)를 활성화하려면 선택합니다. 그러면 **DAD Attempts** 수를 지정할 수 있습니다.
DAD 시도		이웃 식별 시도가 실패하기 전에 이웃 요청 인터벌(**NS** 인터벌) 내에서 DAD 시도 횟수를 지정합니다(범위는 1~10, 기본값은 1).
도달 가능 시간		쿼리 및 응답이 성공한 후 인접 네트워크에 도달할 수 있는 시간을 초 단위로 지정합니다(범위는 1~36,000, 기본값은 30).
NS 인터벌(초)		DAD 시도 실패가 표시되기 전까지의 시간을 초 단위로 지정합니다(범위는 1~3,600, 기본값은 1).
NDP 모니터링 활성화		Neighbor Discovery Protocol 모니터링을 활성화하려면 선택합니다. 활성화되면 NDP(기능 열에서 )를 선택한 다음 방화벽이 검색한 이웃의 IPv6 주소, 해당 MAC 주소 및 User-ID(최상의 경우)와 같은 정보를 볼 수 있습니다.
라우터 알림 활성화	집계된 이더넷 인터페이스 > **IPv6** > 라우터 알림	IPv6 인터페이스에서 Neighbor Discovery를 제공하도록 선택한 다음 이 섹션의 다른 필드를 구성합니다. 라우터 알림(RA) 메시지를 수신하는 IPv6 DNS 클라이언트는 이 정보를 사용합니다. RA를 사용하면 방화벽이 정적으로 구성되지 않은 IPv6 호스트의 기본 게이트웨이 역할을 하고 호스트에 주소 구성을 위한 IPv6 프리픽스를 제공할 수 있습니다. 이 기능과 함께 별도의 DHCPv6 서버

통합 인터페이스 설정	구성 위치	설명
		를 사용하여 클라이언트에 DNS 및 기타 설정을 제공할 수 있습니다. 이것은 인터페이스에 대한 전역 설정입니다. 개별 IP 주소에 대한 RA 옵션을 설정하려면 IP 주소 테이블에 IPv6 주소를 추가하고 구성합니다. IP 주소에 대해 RA 옵션을 설정하는 경우 인터페이스에 대해 라우터 알림을 활성화해야 합니다.
최소 인터벌(초)		방화벽이 보낼 RA 사이의 최소 인터벌(초)을 지정합니다(범위는 3~1,350, 기본값은 200). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
최대 인터벌(초)		방화벽이 보낼 RA 간의 최대 인터벌(초)을 지정합니다(범위는 4~1,800, 기본값은 600). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
홉 제한		나가는 패킷에 대해 클라이언트에 적용할 홉 제한을 지정합니다(범위는 1~255, 기본값은 64). 홉 제한이 없는 경우 **0**을 입력합니다.
링크 MTU		클라이언트에 적용할 링크 최대 전송 단위(MTU)를 지정합니다. 링크 없음 MTU에 대해 지정되지 않음을 선택합니다(범위는 1,280 ~ 9,192, 기본값은 지정되지 않음).
도달 가능한 시간(ms)		클라이언트가 연결 가능성 확인 메시지를 받은 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능한 시간(밀리초)을 지정합니다. 도달할 수 없는 시간 값에 대해 지정되지 않음을 선택합니다(범위는 0 ~ 3,600,000, 기본값은 지정되지 않음).
재전송 시간(ms)		이웃 요청 메시지를 재전송하기 전에 클라이언트가 대기하는 시간(밀리초)을 결정하는 재전송 타이머를 지정합니다. 재전송 시간이 없는 경우 지정되지 않음을 선택합니다(범위는 0 ~ 4,294,967,295, 기본값은 지정되지 않음).
라우터 유효 시간(초)		클라이언트가 방화벽을 기본 게이트웨이로 사용할 시간(초)을 지정합니다(범위는 0~9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.
라우터 기본 설정		네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트는 이 필드를 사용하여 기본 라우터를 선택합니다. RA가 방화벽 라우

통합 인터페이스 설정	구성 위치	설명
		터를 세그먼트의 다른 라우터에 비해 높음, 중간(기본값) 또는 낮음 우선 순위를 갖는 것으로 광고할지의 여부를 선택합니다.
관리 구성		DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
기타 구성		DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
일관성 확인	집계된 이더넷 인터페이스 > **IPv6** > 라우터 알림**(**계속**)**	방화벽이 다른 라우터에서 보낸 RA가 링크에 대한 일관된 정보를 광고하는지 확인하도록 하려면 선택합니다. 방화벽은 시스템 로그에 불일치를 기록합니다. 유형은 **ipv6nd**입니다.
라우터 광고에 DNS 정보 포함	통합 이더넷 인터페이스 > **IPv6** > **DNS** 지원**,** 유형 = 정적	방화벽이 이 IPv6 통합 이더넷 인터페이스에서 NDP RA(라우터 광고) 메시지의 DNS 정보를 보내도록 선택합니다. 이 표의 다른 DNS 지원 필드는 이 옵션을 선택한 후에만 표시됩니다. (**DNS** 지원 탭은 라우터 알림 탭에서 라우터 알림 활성화 후에 사용할 수 있습니다.)
서버		방화벽이 이 IPv6 통합 이더넷 인터페이스에서 NDP 라우터 광고를 보낼 수 있도록 하나 이상의 RDNS(중복 DNS) 서버 주소를 추가합니다. RDNS 서버는 루트 DNS 서버와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에게 보내는 NDP 라우터 광고에서 위쪽에서 아래쪽으로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있습니다. 그러면 받는 사람은 해당 주소를 같은 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버 순서를 변경하거나 더 이상 필요하지 않을 때 서버를 삭제합니다.
라이프타임		IPv6 DNS 클라이언트가 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있다는 라우터 알림을 수신한 후 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초) 값에서 최대 인터벌의 두 배, 기본값은 1,200).
도메인 검색 목록		DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(서픽스)을 추가하고 구성합니다. 최대 서픽스 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩

통합 인터페이스 설정	구성 위치	설명
		추가하여 DNS 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가하고 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가 "company.com"인 경우 라우터의 결과 DNS 쿼리는 정규화된 도메인 이름 "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록에 있는 모든 서픽스를 시도할 때까지 DNS 서픽스를 시도합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 사용하는 NDP 라우터 알림에서 방화벽이 보내는 DNS 검색 목록에 대해 최대 8개의 도메인 이름(서픽스)을 구성할 수 있습니다. 서픽스를 선택한 다음 위로 이동 또는 아래로 이동을 눌러 서픽스 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서픽스를 삭제합니다.
유효 기간	통합 이더넷 인터페이스 > **IPv6** > **DNS** 지원, 유형 = 정적	IPv6 DNS 클라이언트가 DNS 검색 목록에서 도메인 이름(서픽스)을 사용할 수 있다는 라우터 알림을 수신한 후 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)의 값에서 최대 인터벌의 두 배, 기본값은 1,200입니다.).
DNS 재귀 네임 서버	통합 이더넷 인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 DNS 재귀 네임 서버 정보를 보내도록 합니다. • 수동 - DNS 재귀 네임 서버를 수동으로 구성합니다. 수동을 선택하는 경우 방화벽이 이 IPv6 VLAN 인터페이스에서 NDP 라우터 알림을 보낼 재귀 DNS(RDNS) 서버 주소를 추가합니다. RDNS 서버는 루트 DNS 서버와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다.

통합 인터페이스 설정	구성 위치	설명
		방화벽이 받는 사람에게 보내는 NDP 라우터 광고에서 위에서 아래로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있으며, 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다. 클라이언트가 특정 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간인 유효 기간(초)을 입력합니다. 범위는 4~3,600입니다. 기본값은 1,200입니다.
도메인 검색 목록	통합 이더넷 인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 도메인 검색 목록 정보를 보내도록 합니다. • 수동 - 도메인 검색 목록을 수동으로 구성합니다. 수동을 선택한 경우 추가하고 DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(접미사)을 구성합니다. 최대 서픽스 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하여 DNS 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가한 다음 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가 "company.com"인 경우 라우터의 결과 DNS 쿼리는 정규화된 도메인 이름 "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록에 있는 모든 서픽스를 시도할 때까지 DNS 서픽스를 시도합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 해당 주소를 사용하는 받는 사람에 대한 NDP 라우터 알림에서 방화벽이 보내는 DNS 검색 목록에 대해 최대 8개의 도메인 이름(서픽스)을 구성할 수 있습니다. 서픽스를 선택한 다음 위로

통합 인터페이스 설정	구성 위치	설명
		이동 또는 아래로 이동하여 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서픽스를 삭제합니다. 클라이언트가 특정 도메인 검색 목록을 사용할 수 있는 최대 시간인 유효 기간을 초 단위로 입력합니다. 범위는 4~3,600입니다. 기본값은 1,200입니다.

네트워크 > 인터페이스 > VLAN

VLAN 인터페이스는 레이어 3 네트워크(IPv4 및 IPv6)로의 라우팅을 제공할 수 있습니다. 하나 이상의 레이어 2 이더넷 포트(PA-7000 시리즈 레이어 2 인터페이스 참조)를 VLAN 인터페이스에 추가할 수 있습니다.

VLAN 인터페이스 설정	구성 위치	설명
인터페이스 이름	**VLAN** 인터페이스	읽기 전용 인터페이스 이름이 **vlan**으로 설정됩니다. 인접한 필드에 숫자 서픽스(1 ~ 9,999)를 입력하여 인터페이스를 식별합니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
VLAN	**VLAN** 인터페이스 > 컨피그	VLAN을 선택하거나 **VLAN**을 클릭하여 새 VLAN을 정의합니다(네트워크 > VLAN 참조). 없음을 선택하여 인터페이스에서 현재 VLAN 할당을 제거합니다.
가상 라우터		인터페이스에 가상 라우터를 할당하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
IPv4 주소		
유형	**VLAN** 인터페이스 > **IPv4**	인터페이스에 IPv4 주소 유형을 할당하는 방법을 선택합니다. • 정적 - IP 주소를 수동으로 지정해야 합니다.

VLAN 인터페이스 설정	구성 위치	설명
		• **DHCP** 클라이언트—인터페이스가 DHCP(동적 호스트 구성 프로토콜) 클라이언트 역할을 하고 동적으로 할당된 IP 주소를 받을 수 있도록 합니다. 고가용성*(HA)* 능동형/능동형 구성에 있는 방화벽은 *DHCP* 클라이언트를 지원하지 않습니다. 선택한 IP 주소 방법에 따라 탭에 표시되는 옵션이 달라집니다.
IPv4 주소**,** 유형 = 정적		
IP	**VLAN** 인터페이스 > **IPv4**	추가를 클릭한 후 다음 단계 중 하나를 수행하여 인터페이스에 대한 고정 IP 주소 및 네트워크 마스크를 지정합니다. • CIDR(Classless Inter-Domain Routing) 표기법으로 항목을 입력합니다: *ip_address/mask*(예: 192.168.2.0/24). • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • **IP** 넷마스크 유형의 주소 개체를 만듭니다. 인터페이스에 대해 여러 IP 주소를 입력할 수 있습니다. 시스템에서 사용하는 FIB(포워딩 정보 기반)에 따라 최대 IP 주소 수가 결정됩니다. 더 이상 필요하지 않은 IP 주소는 삭제하십시오.
IPv4 주소**,** 유형 = **DHCP** 클라이언트		
사용	**VLAN** 인터페이스 > **IPv4**	인터페이스에서 DHCP 클라이언트를 활성화하려면 선택합니다.
서버에서 제공하는 기본 게이트웨이를 가리키는 기본 경로 자동 생성		DHCP 서버가 제공하는 기본 게이트웨이를 가리키는 기본 경로를 자동으로 생성하려면 선택합니다.
호스트네임 보내기		인터페이스의 호스트 이름(옵션 12)을 DHCP 서버로 보내도록 방화벽(DHCP 클라이언트)을 구성하려면 선택합니다. 호스트네임을 보내면 기본적으로 방화벽의 호스트 이름이 호스트네임 필드에서 선택됩니다. 해당 이름을 보내거나 사용자 지정 호스트 이름(대소문자, 숫자, 마침표, 하이픈 및 밑줄을 포함하여 최대 64자)을 입력할 수 있습니다.

VLAN 인터페이스 설정	구성 위치	설명
기본 경로 측정 항목		방화벽과 DHCP 서버 간의 경로의 경우 선택적으로 기본 경로와 연결하고 경로 선택에 사용할 경로 메트릭(우선 순위 수준)을 입력합니다(범위는 1~65,535이며 기본값은 없음). 숫자 값이 감소할수록 우선 순위 수준이 높아집니다.
DHCP 클라이언트 런타임 정보 표시		DHCP 임대 상태, 동적 IP 주소 할당, 서브넷 마스크, 게이트웨이 및 서버 설정(DNS, NTP, 도메인, WINS, NIS, POP3 및 SMTP)을 포함하여 DHCP 서버에서 수신한 모든 설정을 표시하려면 선택합니다.
IPv6 주소**,** 유형 = 정적		
인터페이스에서 IPv6 활성화	**VLAN** 인터페이스 > **IPv6**	이 인터페이스에서 IPv6 주소 지정을 활성화하려면 선택합니다.
인터페이스 ID		64비트 확장 고유 식별자(EUI-64)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 **ID**를 호스트 부분으로 사용 옵션을 활성화하면 방화벽은 인터페이스 ID를 해당 주소의 호스트 부분으로 사용합니다.
주소	**VLAN** 인터페이스 > **IPv6** > 주소 할당	IPv6 주소 및 프리픽스 길이를 추가합니다(예: 2001:400:f00::1/64). 또는 기존 IPv6 주소 개체를 선택하거나 새로 만듭니다.
인터페이스에서 주소 활성화		인터페이스에서 IPv6 주소를 활성화합니다.
인터페이스 ID를 호스트 부분으로 사용		인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다.
애니캐스트		가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다.
RA 보내기	**VLAN** 인터페이스 > **IPv6** > 주소 할당	이 IPv6 주소에 대해 라우터 알림(RA)을 활성화하려면 선택합니다. 이 옵션을 선택하면 라우터 알림 탭에서 라우터 알림 활성화도 수행해야 합니다. 나머지 필드는 **RA** 보내기를 활성화한 경우에만 적용됩니다.

VLAN 인터페이스 설정	구성 위치	설명
		• 유효 기간 - 방화벽이 주소를 유효한 것으로 간주하는 시간(초)입니다. 유효 시간은 기본 유효 시간과 같거나 초과해야 합니다. 기본값은 2,592,000입니다. • **Preferred Lifetime** - 유효한 주소가 선호되는 시간(초)입니다. 즉, 방화벽이 트래픽을 보내고 받는 데 사용할 수 있습니다. 기본 유효 기간이 만료되면 방화벽은 주소를 사용하여 새 연결을 설정할 수 없지만 기존 연결은 ## ##을 초과할 때까지 유효합니다. 기본값은 604,800입니다. • 온링크 - 보급된 프리픽스 내에 IP 주소가 있는 시스템에 라우터 없이 연결할 수 있는지의 여부를 선택합니다. • **Autonomous**—시스템이 보급된 프리픽스를 인터페이스 ID와 결합하여 IP 주소를 독립적으로 생성할 수 있는지의 여부를 선택합니다.
IPv6 주소**,** 유형 **= DHCPv6** 클라이언트		
라우터 알림 경로 수락	**VLAN** 인터페이스 > **IPv6** > 주소 할당**,** 유형 **= DHCPv6** 클라이언트	DHCPv6 클라이언트가 DHCP 서버에서 RA를 수락하도록 허용하려면 선택합니다.
기본 경로 측정 항목		인터페이스에서 ISP까지의 경로에 대한 기본 경로 메트릭을 입력합니다. 범위는 1~65,535입니다. 기본값은 10입니다.
기본 설정		두 개의 인터페이스(각각 중복성을 위해 다른 ISP에 연결됨)가 있는 경우 한 ISP에 대한 인터페이스에 다른 ISP에 대한 인터페이스보다 높은 기본 설정을 할당할 수 있도록 DHCPv6 클라이언트 인터페이스의 기본 설정(낮음, 중간 또는 높음)을 선택합니다. 기본 인터페이스에 연결된 ISP는 호스트 인터페이스에 보낼 위임된 접두사를 제공하는 ISP가 됩니다. 인터페이스의 기본 설정이 동일한 경우 두 ISP는 위임된 접두사를 제공하고 호스트는 사용할 접두사를 결정합니다.
IPv6 주소 활성화	**VLAN** 인터페이스 > **IPv6** > 주소 할당**,** 유형 **= DHCPv6** 클라이언트 > **DHCPv6** 옵션	이 DHCPv6 클라이언트에 대해 수신된 IPv6 주소를 활성화합니다.
비임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 비임시 주소를 요청합니다. 인터페이스에 더 낮은 수준의 보안이 허용되는 경우(주소의 유효 기간이 더 길기 때문에) 비임시 주소를 선택합니다.

VLAN 인터페이스 설정	구성 위치	설명
		인터페이스에 대해 비임시 주소 또는 임시 주소를 요청하는지 여부는 사용자의 재량과 *DHCPv6* 서버의 기능에 따라 결정됩니다. 일부 서버는 임시 주소만 제공할 수 있습니다. 가장 좋은 방법은 비임시 주소와 임시 주소를 모두 선택하는 것입니다. 이 경우 방화벽은 비임시 주소를 선호합니다.
임시 주소		방화벽이 위임 라우터 및 ISP와 접하는 이 DHCPv6 클라이언트 인터페이스에 할당할 임시 주소를 요청합니다. 주소는 짧은 기간 동안 사용하도록 되어 있으므로 더 높은 수준의 보안을 위해 임시 주소를 선택합니다.
신속한 커밋		간청, 광고, 요청 및 응답 메시지 프로세스가 아닌 요청 및 응답 메시지의 DHCP 프로세스를 사용하려면 선택합니다.
접두사 위임 활성화	**VLAN** 인터페이스 > **IPv6** > 주소 할당, 유형 = **DHCPv6** 클라이언트 > 접두사 위임	방화벽이 접두사 위임 기능을 지원할 수 있도록 접두사 위임을 활성화합니다. 즉, 인터페이스는 업스트림 DHCPv6 서버에서 접두사를 수락하고 선택한 접두사 풀에 접두사를 배치합니다. 여기서 방화벽은 SLAAC를 통해 접두사를 호스트에 위임합니다. 인터페이스에 대한 접두사 위임을 활성화 또는 비활성화하는 기능을 통해 방화벽은 여러 ISP(인터페이스당 하나의 ISP)를 지원할 수 있습니다. 이 인터페이스에서 접두사 위임을 활성화하면 접두사를 제공하는 ISP가 제어됩니다. DHCP 서버에서 받은 위임된 접두사는 요청한 인터페이스에서 사용할 수 없습니다.
DHCP 접두사 길이 힌트		방화벽이 선호하는 DHCPv6 접두사 길이를 DHCPv6 서버로 보내도록 하려면 선택합니다.
DHCP 접두사 길이(비트)		DHCPv6 서버에 힌트로 전송되는 기본 DHCPv6 접두사 길이를 48~64비트 범위로 입력합니다. 예를 들어, 접두사 길이를 *48*로 요청하면 서브넷에 *16*비트*(64-48)*가 남게 되는데, 이는 위임할 접두사의 많은 하위 분할이 필요하다는 것을 의미합니다. 반면에 *63*의 접두사 길이를 요청하면 *2*개의 서브넷만 위임하기 위한 *1*비트가 남습니다. *128*비트 중 호스트 주소용으로 *64*비트가 더 있습니다.

VLAN 인터페이스 설정	구성 위치	설명
접두사 풀 이름		방화벽이 수신된 접두사를 저장하는 접두사 풀의 이름을 입력합니다. 이름은 고유해야 하며 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄을 포함해야 합니다. 쉽게 알아볼 수 있도록 *ISP*를 반영하는 접두사 풀 이름을 사용합니다.
IPv6 주소, 유형 = 상속됨		
이름	**VLAN** 인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	풀 이름을 입력하여 풀을 추가합니다. 이름은 최대 63자의 영숫자 문자, 하이픈, 마침표 및 밑줄일 수 있습니다.
주소 유형		하나를 고릅니다. • 풀의 **GUA** - 선택한 접두사 풀에서 제공되는 전역 유니캐스트 주소(GUA)입니다. 이 GUA를 얻는 것이 접두사 위임을 사용하는 목표입니다. • **ULA** - 고유 로컬 주소는 개인 네트워크 내 연결을 위한 주소 범위 fc00::/7의 개인 주소입니다. DHCP 서버가 없으면 ULA를 선택합니다.
인터페이스에서 활성화		인터페이스에서 주소를 활성화합니다.
접두사 풀		GUA를 가져올 접두사 풀을 선택합니다.
할당 유형	**VLAN** 인터페이스 > **IPv6** > 주소 할당, 유형 = 상속됨	할당 유형을 선택합니다. • 동적 - DHCPv6 클라이언트는 상속된 인터페이스를 구성하기 위해 식별자를 선택해야 합니다. • 동적 식별자 - 사용자는 0~4,000 범위의 식별자를 선택하고 DHCPv6 클라이언트에서 고유한 식별자를 유지해야 합니다.
라우터 알림 보내기		인터페이스에서 LAN 호스트로 라우터 알림(RA)을 보내려면 선택합니다.
온링크		접두사 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는지 여부를 선택합니다.

VLAN 인터페이스 설정	구성 위치	설명
자치		시스템이 광고된 접두사를 인터페이스 ID와 결합하여 IPv6 주소를 독립적으로 생성할 수 있는지 여부를 선택합니다.
중복 주소 감지 활성화	**VLAN** 인터페이스 > **IPv6** > 주소 확인	**DAD** 시도 횟수를 지정할 수 있는 중복 주소 감지(DAD)를 활성화하려면 선택합니다.
DAD 시도		이웃 식별 시도가 실패하기 전에 이웃 요청 인터벌(**NS** 인터벌) 내에서 DAD 시도 횟수를 지정합니다(범위는 1~10, 기본값은 1).
도달 가능 시간		쿼리 및 응답이 성공한 후 인접 네트워크에 도달할 수 있는 시간을 초 단위로 지정합니다(범위는 1~36,000, 기본값은 30).
NS 인터벌(초)		실패가 표시되기 전에 DAD 시도에 대한 시간(초)을 지정하십시오(범위는 1 - 10, 기본값은 1).
NDP 모니터링 작동		Neighbor Discovery Protocol 모니터링을 활성화하려면 선택합니다. 활성화되면 NDP(기능 열에서 )를 선택한 다음 방화벽이 검색한 이웃의 IPv6 주소, 해당 MAC 주소 및 User-ID(최상의 경우)와 같은 정보를 볼 수 있습니다.
IPv6 주소, 유형 = 정적 또는 유형 = 상속됨		
라우터 알림 활성화	**VLAN** 인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 - 상속됨	IPv6 인터페이스에서 Neighbor Discovery를 제공하도록 선택한 다음 이 섹션의 다른 필드를 구성합니다. 라우터 알림(RA) 메시지를 수신하는 IPv6 DNS 클라이언트는 이 정보를 사용합니다. RA를 사용하면 방화벽이 정적으로 구성되지 않은 IPv6 호스트의 기본 게이트웨이 역할을 하고 호스트에 주소 구성을 위한 IPv6 프리픽스를 제공할 수 있습니다. 이 기능과 함께 별도의 DHCPv6 서버를 사용하여 클라이언트에 DNS 및 기타 설정을 제공할 수 있습니다. 이것은 인터페이스에 대한 전역 설정입니다. 개별 IP 주소에 대한 RA 옵션을 설정하려면 IP 주소 테이블에 주소를 추가하고 구성하십시오. IP 주소에 대해 RA 옵션을 설정하는 경우 인터페이스에 대해 라우터 알림을 활성화해야 합니다.
최소 인터벌(초)		방화벽이 보낼 RA 사이의 최소 인터벌(초)을 지정합니다(범위는 3~1,350, 기본값은 200). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.

VLAN 인터페이스 설정	구성 위치	설명
최대 인터벌(초)		방화벽이 보낼 RA 간의 최대 인터벌(초)을 지정합니다(범위는 4~1,800, 기본값은 600). 방화벽은 사용자가 구성한 최소값과 최대값 사이에서 임의의 인터벌로 RA를 보냅니다.
홉 제한		나가는 패킷에 대해 클라이언트에 적용할 홉 제한을 지정합니다(범위는 1~255, 기본값은 64). 홉 제한이 없는 경우 **0**을 입력합니다.
링크 MTU	**VLAN** 인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 = 상속됨	클라이언트에 적용할 링크 최대 전송 단위(MTU)를 지정하거나(범위는 1,280 ~ 1,500) 시스템 기본값에 매핑되는 지정되지 않은 기본값을 지정합니다.
도달 가능한 시간(ms)		클라이언트가 연결 가능성 확인 메시지(범위는 0 ~ 3,600,000)를 수신한 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능 시간(밀리초)을 지정하거나 기본값은 시스템 기본값에 매핑되는 지정되지 않음으로 설정됩니다.
재전송 시간(ms)		클라이언트가 이웃 요청 메시지(범위는 0 ~ 4,294,967,295)를 재전송하기 전에 대기하는 시간(밀리초)을 결정하는 재전송 타이머를 지정하거나 시스템 기본값에 매핑되는 지정되지 않음으로 기본값을 지정합니다.
라우터 유효 시간(초)		클라이언트가 방화벽을 기본 게이트웨이로 사용할 시간(초)을 지정합니다(범위는 0~9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.
라우터 기본 설정		네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트는 이 필드를 사용하여 기본 라우터를 선택합니다. RA가 방화벽 라우터를 세그먼트의 다른 라우터에 비해 높음, 중간(기본값) 또는 낮음 우선 순위를 갖는 것으로 광고할지의 여부를 선택합니다.
도달 가능한 시간(ms)	**VLAN** 인터페이스 > **IPv6** > 라우터 알림, 유형 = 정적 또는 유형 = 상속됨	클라이언트가 연결 가능성 확인 메시지(범위는 0 ~ 3,600,000)를 수신한 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능 시간(밀리초)을 지정하거나 기본값은 시스템 기본값에 매핑되는 지정되지 않음으로 설정됩니다.
재전송 시간(ms)		클라이언트가 이웃 요청 메시지(범위는 0 ~ 4,294,967,295)를 재전송하기 전에 대기하는 시간(밀리초)을 결정하는 재전송 타이머를 지

VLAN 인터페이스 설정	구성 위치	설명
		정하거나 시스템 기본값에 매핑되는 지정되지 않음으로 기본값을 지정합니다.
라우터 유효 시간(초)		클라이언트가 방화벽을 기본 게이트웨이로 사용할 시간(초)을 지정합니다(범위는 0~9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.
라우터 기본 설정		네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트는 이 필드를 사용하여 기본 라우터를 선택합니다. RA가 방화벽 라우터를 세그먼트의 다른 라우터에 비해 높음, 중간(기본값) 또는 낮음 우선 순위를 갖는 것으로 광고할지의 여부를 선택합니다.
관리 구성		DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
기타 구성		DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타내려면 선택합니다.
일관성 확인		방화벽이 다른 라우터에서 보낸 RA가 링크에 대한 일관된 정보를 광고하는지 확인하도록 하려면 선택합니다. 방화벽은 시스템 로그에 불일치를 기록합니다. 유형은 **ipv6nd**입니다.
IPv6 주소**, DNS** 지원**(**유형 = 정적**)**		
라우터 광고에 DNS 정보 포함	**VLAN** 인터페이스 > **IPv6** > **DNS** 지원**,** 유형 = 정적	라우터 알림 탭에서 라우터 알림 사용을 선택하면 DNS 지원을 사용할 수 있습니다. 방화벽이 이 IPv6 이더넷 인터페이스에서 NDP 라우터 광고의 DNS 정보를 보내도록 선택합니다. 다른 DNS 지원 필드(서버, 유효 기간, 도메인 검색 목록 및 유효 기간)는 이 옵션을 선택한 후에만 볼 수 있습니다.
서버		이 IPv6 이더넷 인터페이스에서 NDP 라우터 광고를 보낼 방화벽에 대한 하나 이상의 재귀 DNS(RDNS) 서버 주소를 추가합니다. RDNS 서버는 루트 DNS와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에 대한 NDP 라우터 광고에서 위쪽에서 아래쪽으로 나열된 순서대로 보내는 최대 8개의 RDNS 서버를 구성할 수

VLAN 인터페이스 설정	구성 위치	설명
		있습니다. 그러면 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다.
유효 시간		IPv6 DNS 클라이언트가 라우터 알림을 수신한 후 클라이언트가 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)에서 최대 인터벌(초)의 두 배, 기본값은 1,200).
도메인 검색 목록		DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(서픽스)을 추가합니다. 최대 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하여 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가하고 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가 "company.com"인 경우 라우터의 결과 쿼리는 정규화된 도메인 이름 "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록에 있는 모든 서픽스를 시도할 때까지 DNS 서픽스를 사용합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 사용하는 NDP 라우터 광고에서 방화벽이 위에서 아래로 나열된 순서대로 보내는 DNS 검색 목록 옵션에 대해 최대 8개의 도메인 이름(서픽스)을 구성할 수 있습니다. 서픽스를 선택한 다음 위로 이동 또는 아래로 이동하여 순서를 변경하거나 더 이상 필요하지 않은 경우 서픽스를 삭제합니다.
유효 시간		IPv6 DNS 클라이언트가 DNS 검색 목록에서 도메인 이름(서픽스)을 사용할 수 있다는 라우터 광고를 수신한 후 최대 시간(초)을

VLAN 인터페이스 설정	구성 위치	설명
		입력합니다(범위는 최대 인터벌(초)에서 최대 인터벌(초)의 두 배까지의 값입니다. 기본값 1,200)입니다.
IPv6 주소, **DNS** 지원(유형 = **DHCPv6** 클라이언트 또는 유형 = 상속됨)		
DNS 재귀 네임 서버	**VLAN** 인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 유형 = 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 DNS 재귀 네임 서버 정보를 보내도록 합니다. • 수동 - DNS 재귀 네임 서버를 수동으로 구성합니다. 수동을 선택하는 경우 방화벽이 이 IPv6 VLAN 인터페이스에서 NDP 라우터 알림을 보낼 재귀 DNS(RDNS) 서버 주소를 추가합니다. RDNS 서버는 루트 DNS 서버와 권한 있는 DNS 서버에 일련의 DNS 조회 요청을 보내 궁극적으로 DNS 클라이언트에 IP 주소를 제공합니다. 방화벽이 받는 사람에게 보내는 NDP 라우터 광고에서 위에서 아래로 나열된 순서대로 최대 8개의 RDNS 서버를 구성할 수 있으며, 받는 사람은 이를 동일한 순서로 사용합니다. 서버를 선택한 다음 위로 이동 또는 아래로 이동하여 서버의 순서를 변경하거나 더 이상 필요하지 않은 경우 목록에서 서버를 삭제합니다.
유효 기간		IPv6 DNS 클라이언트가 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있다는 라우터 광고를 수신한 후 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)의 값에서 최대 인터벌의 두 배, 기본값은 1,200).
도메인 검색 목록	**VLAN** 인터페이스 > **IPv6** > **DNS** 지원, 유형 = **DHCPv6** 클라이언트 또는 유형 = 상속됨	활성화 및 선택: • **DHCPv6** - DHCPv6 서버가 도메인 검색 목록을 보내도록 합니다. • 수동 - 도메인 검색 목록을 수동으로 구성합니다. 수동을 선택한 경우 추가하고 DNS 검색 목록(DNSSL)에 대해 하나 이상의 도메인 이름(접미사)을 구성합니다. 최대 서픽스 길이는 255바이트입니다. DNS 검색 목록은 DNS 클라이언트 라우터가 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하여 DNS 쿼리에서 정규화된 도메인 이름을 사용하는 도메인 서픽스 목록입니다. 예를 들어, DNS 클라이언트가 서픽스 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우

VLAN 인터페이스 설정	구성 위치	설명
		터는 마침표와 DNS 검색 목록의 첫 번째 DNS 서픽스를 이름에 추가한 다음 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 서픽스가 "company.com"인 경우 라우터의 결과 DNS 쿼리는 정규화된 도메인 이름 "quality.company.com"에 대한 것입니다. DNS 쿼리가 실패하면 라우터는 목록에서 두 번째 DNS 서픽스를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 라우터는 DNS 조회가 성공할 때까지(나머지 서픽스 무시) 또는 라우터가 목록에 있는 모든 서픽스를 시도할 때까지 DNS 서픽스를 시도합니다. Neighbor Discovery DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 서픽스로 방화벽을 구성합니다. DNSSL 옵션을 받는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에 서픽스를 사용합니다. 동일한 순서로 해당 주소를 사용하는 받는 사람에 대한 NDP 라우터 알림에서 방화벽이 보내는 DNS 검색 목록에 대해 최대 8개의 도메인 이름(서픽스)을 구성할 수 있습니다. 접미사를 선택하고 위로 또는 아래로를 선택하여 순서를 변경하거나 더 이상 필요하지 않은 접미사를 목록에서 삭제합니다.
유효 기간		IPv6 DNS 클라이언트가 DNS 검색 목록에서 도메인 이름(서픽스)을 사용할 수 있다는 라우터 알림을 수신한 후 최대 시간(초)을 입력합니다(범위는 최대 인터벌(초)의 값에서 최대 인터벌의 두 배, 기본값은 1,200입니다.).
고급		
관리 프로파일	**VLAN** 인터페이스 > 고급 > 기타 정보	관리 프로파일 - 이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 프로파일을 선택합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방화벽은 패킷이 과다하게 크다는 것을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.
TCP MSS 조정		인터페이스 MTU 바이트 크기 내의 모든 헤더에 대한 바이트를 수용하도록 최대 세그먼트 크기(MSS)를 조정하려면 선택합니다.

VLAN 인터페이스 설정	구성 위치	설명
		MTU 바이트 크기에서 MSS 조정 크기를 뺀 값은 IP 프로토콜에 따라 달라지는 MSS 바이트 크기와 같습니다. • **IPv4 MSS** 조정 크기 - 범위는 40~300이고, 기본값은 40입니다. • **IPv6 MSS** 조정 크기 - 범위는 60~300이고, 기본값은 60입니다. 이 설정을 사용하여 네트워크를 통한 터널에 더 작은 MSS가 필요한 경우를 해결하십시오. 패킷이 조각화 없이 MSS보다 더 많은 바이트를 갖는 경우 이 설정을 사용하면 조정할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로 MPLS 헤더 또는 VLAN 태그가 있는 터널링된 트래픽과 같은 항목에 대해 바이트를 허용하도록 MSS 조정 크기를 구성하는 데 도움이 됩니다.
IP 주소 MAC 주소 상호 작용	**VLAN** 인터페이스 > 고급 > **ARP** 엔트리	하나 이상의 고정 ARP(Address Resolution Protocol) 항목을 추가하려면 추가를 클릭하고 IP 주소를 입력하고 연결된 하드웨어 [미디어 액세스 제어(MAC)] 주소를 입력하고 하드웨어 주소에 액세스할 수 있는 레이어 3 인터페이스를 선택합니다. 항목을 삭제하려면 항목을 선택한 다음 삭제를 클릭합니다. 고정 ARP 항목은 ARP 처리를 줄이고 지정된 주소에 대한 중간자 공격을 방지합니다.
IPv6 주소 MAC 주소	**VLAN** 인터페이스 > 고급 > **ND** 항목	NDP(Neighbor Discovery Protocol)에 대한 이웃 정보를 제공하려면 추가를 클릭하고 이웃의 IPv6 주소와 MAC 주소를 입력합니다.
NDP 프록시 사용	**VLAN** 인터페이스 > 고급 > **NDP** 프록시	인터페이스에 대해 NDP(Neighbor Discovery Protocol) 프록시를 활성화하려면 선택합니다. 방화벽은 이 목록의 IPv6 주소에 대한 MAC 주소를 요청하는 ND 패킷에 응답합니다. ND 응답에서 방화벽은 인터페이스에 대한 자체 MAC 주소를 보내고 기본적으로 "이 주소에 대한 패킷을 여기로 보내십시오"라고 말합니다. (권장) NPTv6(Network Prefix Translation IPv6)을 사용하는 경우 NDP 프록시를 활성화합니다. **NDP** 프록시를 활성화하면 여러 주소 항목을 필터링할 수 있으며, 먼저 필터를 입력한 다음 적용합니다(녹색 화살표).
주소		방화벽이 NDP 프록시로 작동할 IPv6 주소, IP 범위, IPv6 서브넷 또는 주소 개체를 하나 이상 추가합니다. 이상적으로는 이러한 주소 중 하나가 NPTv6의 소스 번역 주소와 동일합니다. 주소의 순서는 중요하지 않습니다.

VLAN 인터페이스 설정	구성 위치	설명
		주소가 하위 네트워크인 경우 방화벽은 서브넷의 모든 주소에 대해 ND 응답을 보내므로 방화벽의 IPv6 이웃도 추가한 다음 무효를 클릭하여 방화벽이 이러한 IP 주소에 응답하지 않도록 지시하는 것이 좋습니다.
무효		해당 주소에 대해 NDP 프록시를 방지하려면 주소에 대해 부정을 선택합니다. 지정된 IP 주소 범위 또는 IP 서브넷의 하위 집합을 무효화할 수 있습니다.
설정	**VLAN** 인터페이스 > 고급 > **DDNS**	설정을 선택하여 DDNS 필드를 구성할 수 있도록 합니다.
활성화		인터페이스에서 DDNS를 활성화합니다. DDNS를 구성하려면 처음에 활성화해야 합니다. (DDNS 설정이 완료되지 않은 경우 부분 설정을 잃지 않도록 활성화하지 않고 저장할 수 있습니다.)
업데이트 인터벌(일)		FQDN에 매핑된 IP 주소를 업데이트하기 위해 방화벽이 DDNS 서버에 보내는 업데이트 인터벌(일)을 입력합니다(범위는 1~30, 기본값은 1). 또한 방화벽은 *DHCP* 서버에서 인터페이스에 대한 새 *IP* 주소를 수신하면 *DDNS*를 업데이트합니다.
인증서 프로파일		생성한 인증서 프로파일을 선택(또는 새로 생성)하여 DDNS 서비스를 확인합니다. DDNS 서비스는 인증 기관(CA)이 서명한 인증서를 방화벽에 제공합니다.
호스트네임		DDNS 서버에 등록된 인터페이스의 호스트 이름(예: host123.domain123.com, host123)을 입력합니다. 방화벽은 구문이 도메인 이름에 대해 DNS에서 허용하는 유효한 문자를 사용하는지 확인하는 경우를 제외하고 호스트 이름의 유효성을 검사하지 않습니다.
공급자		이 인터페이스에 DDNS 서비스를 제공하는 DDNS 공급자(및 버전 번호)를 선택합니다. • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1**

VLAN 인터페이스 설정	구성 위치	설명
		방화벽에서 특정 날짜까지 단계적으로 중단될 것이라고 표시하는 *DDNS* 서비스의 이전 버전을 선택하는 경우 최신 버전으로 이동합니다. 공급자 이름 뒤에 오는 이름 및 값 필드는 공급자별로 다릅니다. 일부 필드는 방화벽이 DDNS 서비스에 연결하는 데 사용하는 매개변수를 알리기 위해 읽기 전용입니다. DDNS 서비스가 사용자에게 제공하는 비밀번호 및 DDNS 서버로부터 응답을 수신하지 않는 경우 방화벽이 사용하는 타임아웃와 같은 다른 필드를 구성합니다.
IPv4 탭 - IP		인터페이스에 구성된 IPv4 주소를 추가하고 선택합니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
IPv6 탭 - IPv6	**VLAN** 인터페이스 > **Advanced** > **DDNS**(계속)	인터페이스에 구성된 IPv6 주소를 추가하고 선택합니다. 선택된 모든 IP 주소는 DDNS 공급자(Vendor)에 등록됩니다.
런타임 정보 표시		DDNS 등록을 표시합니다. DDNS 공급자, 확인된 FQDN 및 기본 IP 주소를 나타내는 별표(*)가 있는 매핑된 IP 주소. 각 DDNS 공급자에는 문제 해결을 위해 호스트 이름 업데이트 상태와 반환 날짜를 나타내는 고유한 반환 코드가 있습니다.

네트워크 > 인터페이스 > 루프백

다음 필드를 사용하여 루프백 인터페이스를 구성합니다.

루프백 인터페이스 설정	구성 위치	설명
인터페이스 이름	루프백 인터페이스	읽기 전용 인터페이스 이름이 루프백으로 설정됩니다. 인접 필드에 숫자 서픽스(1-9999)를 입력하여 인터페이스를 식별합니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
가상 라우터	루프백 인터페이스 > 컨피그	인터페이스에 가상 라우터를 할당하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
관리 프로파일	터널 인터페이스 > 고급 > 기타 정보	관리 프로파일 - 이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 프로파일을 선택합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(576-9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방화벽은 패킷이 과다하게 크다는 것을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.

루프백 인터페이스 설정	구성 위치	설명
TCP MSS 조정		인터페이스 MTU 바이트 크기 내의 모든 헤더에 대한 바이트를 수용하도록 최대 세그먼트 크기(MSS)를 조정하려면 선택합니다. MTU 바이트 크기에서 MSS 조정 크기를 뺀 값은 IP 프로토콜에 따라 달라지는 MSS 바이트 크기와 같습니다. • **IPv4 MSS** 조정 크기 - 범위는 40-300이고, 기본값은 40입니다. • **IPv6 MSS** 조정 크기 - 범위는 60-300이고, 기본값은 60입니다. 이 설정을 사용하여 네트워크를 통한 터널에 더 작은 MSS가 필요한 경우를 해결하십시오. 패킷이 조각화 없이 MSS보다 더 많은 바이트를 갖는 경우 이 설정을 사용하면 조정할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로 MPLS 헤더 또는 VLAN 태그가 있는 터널링된 트래픽과 같은 항목에 대해 바이트를 허용하도록 MSS 조정 크기를 구성하는 데 도움이 됩니다.
IPv4 주소의 경우		
IP	루프백 인터페이스 > **IPv4**	추가를 클릭한 후 다음 단계 중 하나를 수행하여 인터페이스에 대한 고정 IP 주소 및 네트워크 마스크를 지정합니다. • 서브넷 마스크가 /32인 IPv4 주소를 입력하십시오(예: 192.168.2.1/32). /32 서브넷 마스크만 지원됩니다. • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • 주소를 클릭하여 **IP** 넷마스크 유형의 주소 개체를 만듭니다. 인터페이스에 대해 여러 IP 주소를 입력할 수 있습니다. 시스템에서 사용하는 FIB(포워딩 정보 기반)에 따라 최대 IP 주소 수가 결정됩니다. IP 주소를 삭제하려면 주소를 선택한 다음 삭제를 클릭합니다.
IPv6 주소의 경우		
인터페이스에서 IPv6 활성화	루프백 인터페이스 > **IPv6**	이 인터페이스에서 IPv6 주소 지정을 활성화하려면 선택합니다.
인터페이스 ID		64비트 확장 고유 식별자(EUI-64)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 **ID**를 호스트 부분으로 사용 옵션

루프백 인터페이스 설정	구성 위치	설명
		을 활성화하면 방화벽은 인터페이스 ID를 해당 주소의 호스트 부분으로 사용합니다.
주소		추가를 클릭하고 각 IPv6 주소에 대해 다음 매개변수를 구성합니다. • 주소 - IPv6 주소와 프리픽스 길이를 입력합니다(예: 2001:400:f00::1/64). 기존 IPv6 주소 개체를 선택하거나 주소를 클릭하여 주소 개체를 만들 수도 있습니다. • **Enable address on interface** - 인터페이스에서 IPv6 주소를 활성화하려면 선택합니다. • 인터페이스 **ID**를 호스트 부분으로 사용 - 인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다. • **Anycast** - 가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다.

네트워크 > 인터페이스 > 터널

다음 필드를 사용하여 터널 인터페이스를 구성합니다.

터널 인터페이스 설정	구성 위치	설명
인터페이스 이름	터널 인터페이스	읽기 전용 인터페이스 이름이 터널로 설정됩니다. 인접 필드에 숫자 서픽스(1-9,999)를 입력하여 인터페이스를 식별합니다.
코멘트		인터페이스에 대한 선택적 설명을 입력합니다.
넷플로우 프로파일		수신 인터페이스를 통과하는 단방향 IP 트래픽을 NetFlow 서버로 내보내려면 서버 프로파일을 선택하거나 **Netflow** 프로파일을 클릭하여 새 프로파일을 정의합니다(디바이스 > 서버 프로파일 > NetFlow 참조). 인터페이스에서 현재 NetFlow 서버 할당을 제거하려면 없음을 선택합니다.
가상 라우터	터널 인터페이스 > 컨피그	인터페이스에 가상 라우터를 할당하거나 가상 라우터를 클릭하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템		방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대한 가상 시스템(vsys)을 선택하거나 가상 시스템을 클릭하여 새 vsys를 정의합니다.
보안 구역		인터페이스의 보안 영역을 선택하거나 영역을 클릭하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다.
관리 프로파일	터널 인터페이스 > 고급 > 기타 정보	관리 프로파일 - 이 인터페이스를 통해 방화벽을 관리하는 데 사용할 수 있는 프로토콜(예: SSH, Telnet 및 HTTP)을 정의하는 프로파일을 선택합니다. 인터페이스에서 현재 프로파일 할당을 제거하려면 없음을 선택합니다.
MTU		이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(576-9,192, 기본값은 1,500). 방화벽 양쪽에 있는 시스템이 PMTUD(경로 MTU 검색)를 수행하고 인터페이스가 MTU를 초과하는 패킷을 수신하는 경우 방화벽은 패킷이 과다하게 크다는 것을 나타내는 *ICMP* 조각화 필요 메시지를 소스에 반환합니다.

터널 인터페이스 설정	구성 위치	설명
IPv4 주소의 경우		
IP	터널 인터페이스 > **IPv4**	추가를 클릭한 후 다음 단계 중 하나를 수행하여 인터페이스에 대한 고정 IP 주소 및 네트워크 마스크를 지정합니다. • CIDR(Classless Inter-Domain Routing) 표기법으로 항목을 입력합니다: ip_address/mask(예: 192.168.2.0/24). • **IP** 넷마스크 유형의 기존 주소 개체를 선택합니다. • 주소를 클릭하여 **IP** 넷마스크 유형의 주소 개체를 만듭니다. 인터페이스에 대해 여러 IP 주소를 입력할 수 있습니다. 시스템에서 사용하는 FIB(포워딩 정보 기반)에 따라 최대 IP 주소 수가 결정됩니다. IP 주소를 삭제하려면 주소를 선택한 다음 삭제를 클릭합니다.
IPv6 주소의 경우		
인터페이스에서 IPv6 활성화	터널 인터페이스 > **IPv6**	이 인터페이스에서 IPv6 주소 지정을 활성화하려면 선택합니다.
인터페이스 ID	터널 인터페이스 > **IPv6**	64비트 확장 고유 식별자(EUI-64)를 16진수 형식으로 입력합니다(예: 00:26:08:FF:FE:DE:4E:29). 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 **ID**를 호스트 부분으로 사용 옵션을 활성화하면 방화벽은 인터페이스 ID를 해당 주소의 호스트 부분으로 사용합니다.
주소		추가를 클릭하고 각 IPv6 주소에 대해 다음 매개변수를 구성합니다. • 주소 - IPv6 주소와 프리픽스 길이를 입력합니다(예: 2001:400:f00::1/64). 기존 IPv6 주소 개체를 선택하거나 주소를 클릭하여 주소 개체를 만들 수도 있습니다. • **Enable address on interface** - 인터페이스에서 IPv6 주소를 활성화하려면 선택합니다. • 인터페이스 **ID**를 호스트 부분으로 사용 - 인터페이스 **ID**를 IPv6 주소의 호스트 부분으로 사용하려면 선택합니다. • **Anycast** - 가장 가까운 노드를 통한 라우팅을 포함하려면 선택합니다.

네트워크 > 인터페이스 > SD-WAN

가상 SD-WAN 인터페이스를 생성하고 동일한 대상으로 이동하는 하나 이상의 물리적 이더넷 인터페이스 구성원을 추가합니다.

*Panorama*가 *Multi-VSYS* 방화벽을 관리하는 경우 모든 *SD-WAN* 지원 인터페이스 및 구성을 *vsys1*에서 구성해야 합니다.

*SD-WAN*은 *Multi-VSYS* 방화벽의 다중 가상 시스템에서 *SD-WAN* 구성을 지원하지 않습니다.

SD-WAN 인터페이스 설정	
인터페이스 이름	읽기 전용 인터페이스 이름은 **sdwan**으로 설정됩니다. 인접한 필드에 가상 SD-WAN 인터페이스를 식별하는 숫자 서픽스(1~9,999)를 입력합니다.
코멘트	가장 좋은 방법은 ###이나 ## ## ##와 같은 인터페이스에 대한 사용자 친화적인 설명을 입력하는 것입니다. 귀하의 의견은 로그 및 보고서에서 자동 생성된 이름을 복호화하려고 하는 것보다 인터페이스를 더 쉽게 식별할 수 있도록 합니다.
링크 태그	SD-WAN 링크에 태그 지정 예: 저렴한 광대역 또는 백업.
구성 탭	
가상 라우터	인터페이스에 가상 라우터를 할당하거나 가상 라우터를 선택하여 새 라우터를 정의합니다(네트워크 > 가상 라우터 참조). 인터페이스에서 현재 가상 라우터 할당을 제거하려면 없음을 선택합니다.
가상 시스템	방화벽이 여러 가상 시스템을 지원하고 해당 기능이 활성화된 경우 인터페이스에 대해 **vsys1**을 선택해야 합니다.
보안 구역	인터페이스의 보안 영역을 선택하거나 영역을 선택하여 새 영역을 정의합니다. 인터페이스에서 현재 영역 할당을 제거하려면 없음을 선택합니다. 가상 SD-WAN 인터페이스와 모든 인터페이스 구성원은 동일한 보안 영역에 있어야 하므로 동일한 보안 정책 규칙이 지점에서 동일한 대상까지의 모든 경로에 적용되도록 해야 합니다.
Advanced 탭	
인터페이스	이 가상 SD-WAN 인터페이스를 구성하는 레이어 3 이더넷 인터페이스(다이렉트 인터넷 액세스[DIA]용) 또는 가상 VPN 터널 인터페이스(허브용)를 선택합니다. 방화벽 가상 라우터는 이 가상 SD-WAN 인터페이스를 사용하여 SD-WAN 트래픽을 DIA 또는 허브 위치로 라우팅합니다. 인터페이스는 다른 태그를 가질 수 있습니다.

SD-WAN 인터페이스 설정	
	둘 이상의 인터페이스를 입력하는 경우 모두 동일한 유형(VPN 터널 또는 DIA)이어야 합니다.

네트워크 > 인터페이스 > PoE

지원되는 인터페이스에서 PoE(Power over Ethernet)를 구성하여 방화벽에서 연결된 전원 공급 디바이스(PD)로 전력을 전송할 수 있습니다. 이 화면에는 PoE 설정에서 정의한 전원 예산, 할당 및 사용뿐만 아니라 모든 인터페이스에 대한 PoE 구성 요약이 표시됩니다.

다음 표는 인터페이스 **PoE** 세부 정보 표의 각 열에 대한 개요입니다.

열	설명
상호 작용	인터페이스 이름 및 해당 물리적 포트입니다.
PoE 활성화	인터페이스에서 PoE가 활성화된 경우 예**s**를 나타냅니다.
작동 상태	인터페이스에서 PoE의 현재 상태를 표시합니다. 이 열의 값을 결정하는 데 도움이 되는 범례 표를 참조하십시오.
연결 확인	방화벽과 전원이 켜진 디바이스 사이에 연결이 있는지 여부를 표시합니다.
클래스	전원 출력, 전원 공급 디바이스 유형 및 IEEE 표준을 기반으로 PoE 클래스 정보를 표시합니다.
할당 전력(W)	인터페이스에서 할당한 전력량(와트)입니다.
사용 전력(W)	인터페이스에서 현재 사용 중인 전력량(와트)입니다.
소비 전력(W)	인터페이스에서 소비한 전력량(와트)입니다.
Rsvd 전력/최대 전력(W)	최대 전력 잠재력(와트)에 대해 인터페이스가 예약한 전력량입니다.
결함	PoE 연결에 지정된 포트에서 오류가 발생한 경우 세부 정보를 표시합니다.
블랙리스트 이유	블랙리스트에 추가된 포트에 대한 세부 정보를 표시합니다. 없음은 포트가 블랙리스트에 추가되지 않았음을 나타냅니다.

위의 인터페이스 **PoE** 세부 정보 표의 특정 열은 약어를 사용하여 상태, 오류 또는 기타 상황을 전달합니다. 아래의 범례 표는 각 약어를 설명합니다.

약어	용어
할당	할당됨

약어	용어
Apr	승인됨
구성	구성
Conn-chk	연결 확인
Covc	클래스 과전류
Den	전력 거부됨
Dis	비활성화
디스크	연결 해제
DS	이중 서명
Ena	활성화됨
FLT	Fault
NOFLT	결함 없음
OPR	작동
Pcut	정전
Prgto	전원 양호 시간 초과
Pwr	전원
Rsvd	예약됨
단락	단락
닫기	일시 휴업
Sig	신호 쌍
소프트	소프트웨어
Sp	예비 쌍
SS	단일 서명

약어	용어
너무 높은	예상보다 큰 전기용량
너무 낮은	PD 저항이 너무 낮음
Tstart	허용되는 최대값보다 높은 돌입 전류
UN	알 수 없음
W	와트

네트워크 > 영역

다음 항목에서는 네트워크 보안 영역에 대해 설명합니다.

무엇을 찾고 계신가요?	참조:
보안 영역의 목적은 무엇입니까?	보안 영역 개요
보안 영역을 구성하는 데 사용할 수 있는 필드는 무엇입니까?	보안 영역의 빌딩 블록
더 찾고 계십니까?	인터페이스 및 영역을 사용하여 네트워크 분할

보안 영역 개요

보안 영역은 네트워크의 특정 인터페이스를 통과하는 트래픽을 제어하고 기록하기 위해 방화벽에서 물리적 및 가상 인터페이스를 그룹화하는 논리적 방법입니다. 인터페이스에서 트래픽을 처리하려면 먼저 방화벽의 인터페이스를 보안 영역에 할당해야 합니다. 영역에는 탭, 레이어 2 또는 레이어 3 인터페이스와 같은 동일한 유형의 여러 인터페이스가 할당될 수 있지만 인터페이스는 하나의 영역에만 종속될 수 있습니다.

방화벽의 정책 규칙은 보안 영역을 사용하여 트래픽의 수신지 및 발신지를 식별합니다. 트래픽은 영역 내에서 자유롭게 흐를 수 있지만 허용하는 보안 정책 규칙을 정의할 때까지 트래픽은 다른 영역 간에 플로우될 수 없습니다. 영역 간 트래픽을 허용하거나 거부하려면 보안 정책 규칙이 소스 영역과 대상 영역(인터페이스가 아님)을 참조해야 하며 영역 유형이 동일해야 합니다. 즉, 보안 정책 규칙은 한 레이어 2 영역에서 다른 레이어 2 영역으로의 트래픽만 허용하거나 거부할 수 있습니다.

보안 영역의 빌딩 블록

보안 영역을 정의하려면 추가를 클릭하고 다음 정보를 지정합니다.

보안 영역 설정	설명
이름	영역 이름을 입력합니다(최대 31자). 이 이름은 보안 정책을 정의하고 인터페이스를 구성할 때 영역 목록에 나타납니다. 이름은 대소문자를 구분하며 가상 라우터 내에서 고유해야 합니다. 문자, 숫자, 공백, 하이픈, 마침표 및 밑줄만 사용하십시오.
위치	이 필드는 방화벽이 여러 가상 시스템(vsys)을 지원하고 해당 기능이 활성화된 경우에만 표시됩니다. 이 영역이 적용되는 vsys를 선택하십시오.

보안 영역 설정	설명
유형	영역 유형(**Tap**, **Virtual Wire**, **Layer2**, **Layer3**, **External** 또는 **Tunnel**)을 선택하여 영역에 할당되지 않은 해당 유형의 모든 인터페이스를 봅니다. 레이어 2 및 레이어 3 영역 유형은 해당 유형의 모든 이더넷 인터페이스와 하위 인터페이스를 나열합니다. 영역에 할당할 인터페이스를 추가합니다. 외부 영역은 단일 방화벽에서 여러 가상 시스템 간의 트래픽을 제어하는 데 사용됩니다. 다중 가상 시스템 기능이 활성화된 경우에만 다중 가상 시스템을 지원하는 방화벽에서만 표시됩니다. 외부 영역에 대한 자세한 내용은 방화벽 내에 남아 있는 VSYS 간 트래픽을 참조하십시오. 인터페이스는 하나의 가상 시스템에서 하나의 영역에만 속할 수 있습니다.
인터페이스	이 영역에 하나 이상의 인터페이스를 추가합니다.
영역 보호 프로파일	방화벽이 이 영역의 공격에 대응하는 방법을 지정하는 프로파일을 선택합니다. 새 프로파일을 만들려면 네트워크 > 네트워크 프로파일 > 영역 보호를 참조하세요. 가장 좋은 방법은 영역 보호 프로파일을 사용하여 각 영역을 방어하는 것입니다.
패킷 버퍼 보호 활성화	Packet Buffer Protection(디바이스 > 설정 > 세션)을 전역적으로 구성하고 각 영역에 적용합니다. 방화벽은 패킷 버퍼 보호를 수신 영역에만 적용합니다. 버퍼 사용률을 기반으로 하는 패킷 버퍼 보호는 기본적으로 활성화되어 있습니다. 대안은 대기 시간을 기반으로 패킷 버퍼 보호를 구성하는 것입니다. 방화벽 버퍼를 보호하기 위해 각 영역에서 패킷 버퍼 보호를 활성화하는 것이 가장 좋습니다.
네트워크 검사 활성화	영역 보호 프로필과 연결된 보안 영역에 대한 사용자 지정 규칙을 사용하여 L3 및 L4 헤더 검사를 쉽게 활성화할 수 있습니다. 방화벽(디바이스 > 설정 > 세션)에서도 L3 및 L4 헤더 검사에 대한 전역 설정을 활성화해야 합니다.
로그 설정	영역 보호 로그를 외부 시스템으로 포워딩하기 위한 로그 포워딩 프로파일을 선택합니다. **default**라는 이름의 로그 포워딩 프로파일이 있는 경우 새 보안 영역을 정의할 때 해당 프로파일이 이 드롭다운에 대해 자동으로 선택됩니다. 새 보안 영역을 설정할 때 다른 로그 포워딩 프로파일을 계속 선택하여 언제든지 이 기본 설정을 무시할 수 있습니다. 새 로그 포워딩 프로파일을 정의하거나 추가하려면(그리고 이 드롭다운이 자동으로 채워지도록 프로파일 기본값의 이름을 지정하려면) 새로 생성을 클릭합니다(개체 > 로그 포워딩 참조).

보안 영역 설정	설명
	Panorama 템플릿에서 영역을 구성하는 경우 로그 설정 드롭다운에는 공유 로그 포워딩 프로파일만 나열됩니다. 비공유 프로파일을 지정하려면 해당 이름을 입력해야 합니다.
사용자 식별 활성화	IP 주소 대 사용자명 매핑(검색)을 수행하도록 User-ID™를 구성한 경우 가장 좋은 방법은 사용자 식별을 활성화하여 이 영역의 트래픽에 매핑 정보를 적용하는 것입니다. 이 옵션을 비활성화하면 방화벽 로그, 보고서 및 정책에서 영역 내 트래픽에 대한 사용자 매핑 정보를 제외합니다. 기본적으로 이 옵션을 선택하면 방화벽은 영역에 있는 모든 하위 네트워크의 트래픽에 사용자 매핑 정보를 적용합니다. 정보를 영역 내의 특정 하위 네트워크로 제한하려면 포함 목록 및 제외 목록을 사용하십시오. 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 전송될 수 있으며, 그 결과 사용자 *ID* 에이전트 서비스 계정 이름, 도메인 이름 및 암호화된 암호 해시가 공개되어 공격자가 보호된 리소스에 무단으로 액세스할 수 있습니다. *User-ID*는 *User-ID*가 모니터링하는 네트워크 범위 내에 있는 경우에만 영역에 대한 검색을 수행합니다. 영역이 해당 범위 밖에 있으면 방화벽은 사용자 식별 사용을 선택하더라도 영역 트래픽에 사용자 매핑 정보를 적용하지 않습니다. 자세한 내용은 사용자 매핑을 위한 하위 네트워크 포함 또는 제외를 참조하십시오.
사용자 식별 ACL 포함 목록	기본적으로 이 목록에서 하위 네트워크를 지정하지 않으면 방화벽은 검색한 사용자 매핑 정보를 로그, 보고서 및 정책에서 사용하기 위해 이 영역의 모든 트래픽에 적용합니다. 영역 내의 특정 하위 네트워크에 대한 사용자 매핑 정보의 적용을 제한하려면 각 하위 네트워크에 대해 추가를 클릭하고 주소(또는 주소 그룹) 개체를 선택하거나 IP 주소 범위(예: 10.1.1.1/24)를 입력합니다. 포함 목록이 허용 목록이기 때문에 다른 모든 하위 네트워크의 제외는 암시적이므로 제외 목록에 추가할 필요가 없습니다. 포함 목록의 하위 네트워크 하위 집합에 대한 사용자 매핑 정보를 제외하려면 제외 목록에만 항목을 추가하십시오. 예를 들어 포함 목록에 10.0.0.0/8을 추가하고 제외 목록에 10.2.50.0/22를 추가하면 방화벽은 모든 영역 하위 네트워크에 대한 사용자 매핑 정보를 포함합니다.

보안 영역 설정	설명
	10.2.50.0/22를 제외한 10.0.0.0/8이며 10.0.0.0/8 외부의 모든 영역 하위 네트워크에 대한 정보는 제외됩니다. *User-ID*가 모니터링하는 네트워크 범위에 속하는 하위 네트워크만 포함할 수 있습니다. 자세한 내용은 사용자 매핑을 위한 하위 네트워크 포함 또는 제외를 참조하십시오.
사용자 식별 ACL 제외 목록	포함 목록에서 하위 네트워크의 하위 집합에 대한 사용자 매핑 정보를 제외하려면 주소(또는 주소 그룹) 개체를 추가하거나 제외할 각 하위 네트워크의 IP 주소 범위를 입력합니다. 제외 목록에는 항목을 추가하지만 포함 목록에는 추가하지 않는 경우 방화벽은 추가한 하위 네트워크뿐만 아니라 영역 내의 모든 하위 네트워크에 대한 사용자 매핑 정보를 제외합니다.

네트워크 > VLAN

방화벽은 IEEE 802.1Q 표준을 준수하는 VLAN을 지원합니다. 방화벽에 정의된 각 레이어 2 인터페이스는 VLAN과 연결될 수 있습니다. 동일한 VLAN을 여러 Layer 2 인터페이스에 할당할 수 있지만 각 인터페이스는 하나의 VLAN에만 속할 수 있습니다.

VLAN 설정	설명
이름	VLAN 이름을 입력합니다(최대 31자). 이 이름은 인터페이스를 구성할 때 VLAN 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
VLAN 인터페이스	네트워크 > 인터페이스 > VLAN을 선택하여 트래픽이 VLAN 외부로 라우팅되도록 허용합니다.
인터페이스	VLAN에 대한 방화벽 인터페이스를 지정합니다.
정적 MAC 구성	MAC 주소에 연결할 수 있는 인터페이스를 지정합니다. 이것은 학습된 인터페이스-MAC 매핑을 재정의합니다.

네트워크 > 가상 와이어

방화벽에서 두 개의 가상 와이어 인터페이스를 지정한 후 네트워크 > 가상 와이어를 선택하여 가상 와이어를 정의합니다(네트워크 > 인터페이스).

가상 와이어 설정	설명
가상 와이어 이름	가상 와이어 이름을 입력합니다(최대 **31**자). 이 이름은 인터페이스를 구성할 때 가상 와이어 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
인터페이스	가상 와이어 구성에 대해 표시된 목록에서 두 개의 이더넷 인터페이스를 선택합니다. 인터페이스는 가상 와이어 인터페이스 유형이 있고 다른 가상 와이어에 할당되지 않은 경우에만 여기에 나열됩니다. 가상 와이어 인터페이스에 대한 정보는 가상 와이어 인터페이스를 참조하십시오.
태그 허용	가상 와이어에서 허용되는 트래픽에 대한 태그 번호(0-4094) 또는 태그 번호 범위(tag1-tag2)를 입력합니다. 0(기본값)의 태그 값은 태그가 지정되지 않은 트래픽을 나타냅니다. 여러 태그 또는 범위는 쉼표로 구분해야 합니다. 제외된 태그 값이 있는 트래픽은 삭제됩니다. 태그 값은 수신 또는 발신 패킷에서 변경되지 않습니다. 가상 와이어 서브인터페이스를 사용할 때 태그 허용 목록은 나열된 태그가 있는 모든 트래픽이 상위 가상 와이어로 분류되도록 합니다. 가상 와이어 서브인터페이스는 상위의 태그 허용 목록에 없는 태그를 활용해야 합니다.
멀티캐스트 방화벽	멀티캐스트 트래픽에 보안 규칙을 적용하려면 선택하십시오. 이 설정을 사용하지 않으면 멀티캐스트 트래픽이 가상 와이어를 통해 포워딩됩니다.
링크 상태 통과	다운 링크 상태가 감지될 때 가상 와이어 쌍의 다른 인터페이스를 중단하려면 선택합니다. 이 옵션을 선택하지 않거나 비활성화하면 링크 상태가 가상 와이어를 통해 전파되지 않습니다.

네트워크 > 가상 라우터

방화벽은 수동으로 정의한 고정 경로를 사용하거나 레이어 3 라우팅 프로토콜(동적 경로)에 참여하여 다른 서브넷에 대한 경로를 얻기 위해 가상 라우터가 필요합니다. 방화벽에 정의된 각 Layer 3 인터페이스, 루프백 인터페이스 및 VLAN 인터페이스는 가상 라우터와 연결되어야 합니다. 각 인터페이스는 하나의 가상 라우터에만 속할 수 있습니다.

가상 라우터를 정의하려면 네트워크에서 요구하는 일반 설정과 정적 경로 또는 동적 라우팅 프로토콜의 조합이 필요합니다. 경로 재분배 및 ECMP와 같은 다른 기능을 구성할 수도 있습니다.

무엇을 찾고 계신가요?	참조
가상 라우터의 필수 요소는 무엇입니까?	가상 라우터의 일반 설정
구성:	정적 경로 경로 재분배 RIP OSPF OSPFv3 BGP IP 멀티캐스트 ECMP
가상 라우터에 대한 정보를 봅니다.	가상 라우터에 대한 추가 런타임 통계
더 찾고 계십니까?	네트워킹

가상 라우터의 일반 설정

- 네트워크 > 가상 라우터 > 라우터 설정 > 일반

모든 가상 라우터를 사용하려면 다음 표에 설명된 대로 레이어 3 인터페이스와 관리 거리 메트릭을 할당해야 합니다.

가상 라우터 일반 설정	설명
이름	가상 라우터를 설명하는 이름을 지정합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
인터페이스	가상 라우터에 포함할 인터페이스를 선택합니다. 따라서 가상 라우터의 라우팅 테이블에서 나가는 인터페이스로 사용할 수 있습니다. 인터페이스 유형을 지정하려면 네트워크 > 인터페이스를 참조하세요. 인터페이스를 추가하면 연결된 경로가 자동으로 추가됩니다.
행정 거리	다음 관리 거리를 지정합니다. • 고정 경로 - 범위는 10-240입니다. 기본값은 10입니다. • **OSPF Int** - 범위는 10-240입니다. 기본값은 30입니다. • **OSPF** 확장 - 범위는 10-240입니다. 기본값은 110입니다. • **IBGP** - 범위는 10-240입니다. 기본값은 200입니다. • **EBGP** - 범위는 10-240입니다. 기본값은 20입니다. • **RIP** - 범위는 10-240입니다. 기본값은 120입니다.

정적 경로

- 네트워크 > 가상 라우터 > 고정 경로

선택적으로 하나 이상의 정적 경로를 추가합니다. IPv4 또는 IPv6 주소를 사용하여 경로를 지정하려면 **IP** 또는 **IPv6** 탭을 클릭합니다. 일반적으로 여기에서 기본 경로(0.0.0.0/0)를 구성해야 합니다. 기본 경로는 가상 라우터의 라우팅 테이블에서 찾을 수 없는 대상에 적용됩니다.

정적 경로 설정	설명
이름	고정 경로를 식별하는 이름(최대 63자) 을 입력합니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
데스티네이션	CIDR(Classless Inter-domain Routing) 표기법으로 IP 주소와 네트워크 마스크를 입력합니다: *ip_address*/*mask*(예: IPv4의 경우 192.168.2.0/24 또는 IPv6의 경우 2001:db8::/32). 또는 IP 넷마스크 유형의 주소 개체를 만들 수 있습니다.

정적 경로 설정	설명
상호 작용	패킷을 대상으로 포워딩할 인터페이스를 선택하거나 다음 홉 설정을 구성하거나 둘 다를 구성합니다.
다음 홉	다음 중 하나를 선택합니다. • **IP** 주소 - 다음 홉 라우터의 IP 주소를 입력하려면 선택하거나 IP 넷마스크 유형의 주소 개체를 선택 또는 생성합니다. 주소 개체에는 IPv4의 경우 /32, IPv6의 경우 /128의 넷마스크가 있어야 합니다. • 다음 **VR** - 방화벽의 가상 라우터를 다음 홉으로 선택하려면 선택합니다. 이를 통해 단일 방화벽 내의 가상 라우터 간에 내부적으로 라우팅할 수 있습니다. • **FQDN** - FQDN으로 다음 홉을 식별하려면 선택합니다. 그런 다음 FQDN 유형의 주소 개체를 선택하거나 FQDN 유형의 새 주소 개체를 만듭니다. • 삭제 - 이 대상으로 주소가 지정된 트래픽을 삭제하려면 선택합니다. • 없음 - 경로에 대한 다음 홉이 없는 경우 선택합니다.
AD(Admin Distance)	고정 경로에 대한 관리 거리를 지정합니다(10~240, 기본값은 10).
미터법	정적 경로에 대한 유효한 지표를 지정합니다(1~65535).
라우팅 테이블	방화벽이 고정 경로를 설치하는 경로 테이블을 선택합니다. • 유니캐스트 - 유니캐스트 라우팅 테이블에 경로를 설치합니다. • 멀티캐스트 - 멀티캐스트 라우팅 테이블에 경로를 설치합니다. • 둘 다 - 유니캐스트 및 멀티캐스트 라우팅 테이블에 경로를 설치합니다. • 설치 안 함 - 경로 테이블(RIB)에 경로를 설치하지 않습니다. 방화벽은 사용자가 경로를 삭제할 때까지 나중에 참조할 수 있도록 고정 경로를 유지합니다.
BFD 프로파일	PA-400 시리즈, PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈 또는 VM 시리즈 방화벽의 정적 경로에 대해 BFD(양방향 전달 감지)를 활성화하려면 다음 중 하나를 선택합니다. • 기본값(기본 BFD 설정) • 방화벽에서 생성한 BFD 프로파일 • 새 BFD 프로파일을 만들기 위한 새 **BFD** 프로파일 고정 경로에 대해 BFD를 비활성화하려면 없음**(BFD** 비활성화**)**을 선택합니다.

정적 경로 설정	설명
	고정 경로에서 BFD를 사용하려면: • 방화벽과 정적 경로의 반대쪽에 있는 피어 모두 BFD 세션을 지원해야 합니다. • 고정 경로 다음 홉 유형은 **IP** 주소여야 하며 유효한 IP 주소를 입력해야 합니다. • 인터페이스 설정은 없음일 수 없습니다. DHCP 주소를 사용하는 경우에도 인터페이스를 선택해야 합니다.
경로 모니터링	고정 경로에 대한 경로 모니터링을 활성화하려면 선택합니다.
실패 조건	방화벽에서 모니터링되는 경로가 다운된 것으로 간주하여 정적 경로가 다운되는 조건을 선택합니다. • 임의 - 정적 경로에 대해 모니터링되는 대상 중 하나가 ICMP에 의해 도달할 수 없는 경우 방화벽은 RIB 및 FIB에서 정적 경로를 제거하고 동일한 대상으로 가는 다음으로 가장 낮은 메트릭이 있는 동적 또는 정적 경로를 FIB에 추가합니다. • 모두 - ICMP에서 정적 경로에 대해 모니터링되는 모든 대상에 연결할 수 없는 경우 방화벽은 RIB 및 FIB에서 정적 경로를 제거하고 동일한 대상으로 이동하는 다음으로 낮은 메트릭을 가진 동적 또는 정적 경로를 FIB에 추가합니다. 예를 들어 모니터링되는 대상이 유지 관리를 위해 단순히 오프라인 상태일 때 모니터링되는 단일 대상이 정적 경로 실패를 알리는 것을 방지하려면 모두를 선택합니다.
선점 대기 시간(분)	다운된 경로 모니터가 작동 상태를 유지해야 하는 시간(분)을 입력하십시오. 경로 모니터는 모든 구성원 모니터링 대상을 평가하고 방화벽이 RIB에 고정 경로를 다시 설치하기 전에 작동 상태를 유지해야 합니다. 링크가 다운되거나 플래핑되지 않고 타이머가 만료되면 링크가 안정적인 것으로 간주되고 경로 모니터가 작동 상태를 유지할 수 있으며 방화벽은 정적 경로를 RIB에 다시 추가할 수 있습니다. 보류 시간 동안 링크가 다운되거나 플랩되면 다운된 모니터가 작동 상태로 돌아갈 때 경로 모니터가 실패하고 타이머가 다시 시작됩니다. **Preemptive Hold Time**이 0이면 방화벽은 경로 모니터가 표시되는 즉시 정적 경로를 RIB로 다시 설치합니다. 범위는 0~1,440입니다. 기본값은 2입니다.
이름	모니터링 대상의 이름을 입력합니다(최대 31자).

정적 경로 설정	설명
활성화	고정 경로에 대해 이 특정 대상의 경로 모니터링을 활성화하려면 선택합니다. 방화벽은 ICMP 핑(ping)을 이 대상으로 보냅니다.
소스 IP	모니터링 대상에 대한 ICMP 핑(ping)에서 방화벽이 소스로 사용할 IP 주소를 선택합니다. • 인터페이스에 여러 IP 주소가 있는 경우 하나를 선택합니다. • 인터페이스를 선택하면 방화벽은 기본적으로 인터페이스에 할당된 첫 번째 IP 주소를 사용합니다. • **DHCP(DHCP** 클라이언트 주소 사용**)**를 선택하면 방화벽은 DHCP가 인터페이스에 할당한 주소를 사용합니다. DHCP 주소를 보려면 네트워크 > 인터페이스 > 이더넷을 선택한 다음 이더넷 인터페이스 행에서 동적 **DHCP** 클라이언트를 클릭합니다. IP 주소가 동적 IP 인터페이스 상태 창에 나타납니다.
대상 IP	방화벽이 경로를 모니터링할 강력하고 안정적인 IP 주소 또는 주소 개체를 입력합니다. 모니터링 대상과 고정 경로 대상은 동일한 주소 계열(IPv4 또는 IPv6)을 사용해야 합니다.
핑(ping) 인터벌(초)	ICMP 핑(ping) 인터벌을 초 단위로 지정하여 방화벽이 경로를 모니터링하는 빈도를 결정합니다(모니터링되는 대상에 대한 핑(ping). 범위는 1~60, 기본값은 3).
핑(ping) 카운트	방화벽이 링크 다운을 고려하기 전에 모니터링 대상에서 반환되지 않는 연속 ICMP 핑(ping) 패킷 수를 지정합니다. **Any** 또는 **All** 실패 조건에 따라 경로 모니터링이 실패 상태인 경우 방화벽은 RIB에서 정적 경로를 제거합니다(범위는 3~10, 기본값은 5). 예를 들어, 핑(ping) 인터벌이 3초이고 Ping Count가 5회 누락된 핑(방화벽은 지난 15초 동안 핑을 수신하지 않음)은 경로 모니터링이 링크 오류를 감지했음을 의미합니다. 경로 모니터링이 실패 상태이고 방화벽이 15초 후에 핑(ping)을 수신하면 링크가 작동된 것으로 간주됩니다. **Any** 또는 **All** 장애 조건을 기반으로 **Any** 또는 **All** 모니터링 대상에 대한 경로 모니터링이 수행된 것으로 간주되고 Preemptive Hold Time이 시작됩니다.

경로 재분배

- 네트워크 > 가상 라우터 > 재배포 프로파일

재배포 프로파일은 방화벽이 원하는 네트워크 동작에 따라 필터링하고 우선 순위를 설정하고 작업을 수행하도록 지시합니다. 경로 재분배를 사용하면 다른 프로토콜에서 획득한 고정 경로와 경로가 지정된 라우팅 프로토콜을 통해 보급될 수 있습니다.

재분배 프로파일을 적용하려면 라우팅 프로토콜에 적용해야 합니다. 재배포 규칙이 없으면 각 프로토콜은 별도로 실행되며 해당 범위 외부에서 통신하지 않습니다. 모든 라우팅 프로토콜이 구성되고 결과 네트워크 토폴로지가 설정된 후에 재배포 프로파일을 추가하거나 수정할 수 있습니다.

내보내기 규칙을 정의하여 RIP 및 OSPF 프로토콜에 재배포 프로파일을 적용합니다. 재배포 규칙 탭에서 BGP에 재배포 프로파일을 적용합니다. 다음 표를 참조하십시오.

재배포 프로파일 설정	설명
이름	재배포 프로파일을 추가하고 프로파일 이름을 입력합니다.
우선 사항	이 프로파일의 우선 순위(범위는 1-255)를 입력합니다. 프로파일은 순서대로 일치합니다(가장 낮은 번호 먼저).
재배포	이 창의 설정에 따라 경로 재분배를 수행할지의 여부를 선택합니다. • 재배포 - 일치하는 후보 경로를 재배포하려면 선택합니다. 이 옵션을 선택하는 경우 새 메트릭 값을 입력합니다. 메트릭 값이 낮을수록 더 선호하는 경로를 의미합니다. • 재배포 안 함 - 일치하는 후보 경로를 재배포하지 않으려면 선택합니다.
일반 필터 탭	
유형	후보 경로의 경로 유형을 선택합니다.
상호 작용	인터페이스를 선택하여 후보 경로의 포워딩 인터페이스를 지정합니다.
데스티네이션	후보 경로의 대상을 지정하려면 대상 IP 주소 또는 서브넷(xxxx 또는 xxxx/n 형식)을 입력하고 추가를 클릭합니다. 항목을 제거하려면 제거(⊖)를 클릭합니다.
다음 홉	후보 경로의 게이트웨이를 지정하려면 다음 홉을 나타내는 IP 주소 또는 서브넷(형식 xxxx 또는 xxxx/n)을 입력하고 추가를 클릭합니다. 항목을 제거하려면 제거(⊖)를 클릭합니다.
OSPF 필터 탭	

재배포 프로파일 설정	설명
경로 유형	후보 OSPF 경로의 경로 유형을 선택합니다.
지역	후보 OSPF 경로에 대한 영역 식별자를 지정합니다. **OSPF** 영역 **ID**(형식 xxxx)를 입력하고 추가를 클릭합니다. 항목을 제거하려면 제거(⊖)를 클릭합니다.
태그	OSPF 태그 값을 지정합니다. 숫자 태그 값(1-255)을 입력하고 추가를 클릭합니다. 항목을 제거하려면 제거(⊖)를 클릭합니다.
BGP 필터 탭	
지역 사회	BGP 라우팅 정책에 대한 커뮤니티를 지정합니다.
확장된 커뮤니티	BGP 라우팅 정책에 대한 확장 커뮤니티를 지정합니다.

RIP

- 네트워크 > 가상 라우터 > RIP

RIP(라우팅 정보 프로토콜) 구성에는 다음과 같은 일반 설정이 포함됩니다.

RIP 설정	설명
활성화	RIP를 활성화하려면 선택합니다.
기본 경로 거부	(권장) RIP를 통해 기본 경로를 학습하지 않으려면 선택하십시오.
BFD	PA-400 시리즈, PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈 및 VM 시리즈 방화벽에서 다음 중 하나를 선택합니다. • 기본값(기본 BFD 설정이 있는 프로파일) • 방화벽에서 생성한 BFD 프로파일 • 새 **BFD** 프로파일을 만들기 위한 새 BFD 프로파일

RIP 설정	설명
	가상 라우터의 모든 RIP 인터페이스에 대해 BFD를 비활성화하려면 없음(**BFD** 비활성화)을 선택합니다. 단일 RIP 인터페이스에 대해 BFD를 활성화할 수 없습니다.

또한 다음 탭에서 RIP 설정을 구성해야 합니다.

- 인터페이스: RIP 인터페이스 탭을 참조하십시오.
- 타이머: RIP 타이머 탭을 참조하십시오.
- 인증 프로파일: RIP 인증 프로파일 탭을 참조하십시오.
- 내보내기 규칙: RIP 내보내기 규칙 탭을 참조하십시오.

RIP 인터페이스 탭

- 네트워크 > 가상 라우터 > RIP > 인터페이스

다음 필드를 사용하여 RIP 인터페이스를 구성합니다.

RIP – 인터페이스 설정	설명
상호 작용	RIP 프로토콜을 실행하는 인터페이스를 선택하십시오.
활성화	이 설정을 활성화하려면 선택합니다.
광고	지정된 메트릭 값을 사용하여 RIP 피어에 대한 기본 경로 보급을 활성화하려면 선택합니다.
미터법	라우터 보급에 대한 메트릭 값을 지정합니다. 이 필드는 광고를 활성화한 경우에만 표시됩니다.
인증 프로파일	프로파일을 선택합니다.
방법	일반, 수동 또는 발신 전용을 선택합니다.
BFD	RIP 인터페이스에 대해 BFD를 활성화하려면(이를 통해 가상 라우터 수준에서 RIP에 대해 BFD가 비활성화되지 않는 한 RIP에 대한 BFD 설정을 무시함) 다음 중 하나를 선택합니다. • 기본값(기본 BFD 설정이 있는 프로파일) • 방화벽에서 생성한 BFD 프로파일 • 새 **BFD** 프로파일을 만들기 위한 새 BFD 프로파일

RIP – 인터페이스 설정	설명
	없음**(BFD** 비활성화**)**을 선택하여 RIP 인터페이스에 대해 BFD를 비활성화합니다.

RIP 타이머 탭

- 네트워크 > 가상 라우터 > RIP > 타이머

다음 표에서는 RIP 경로 업데이트 및 만료를 제어하는 타이머에 대해 설명합니다.

RIP – 타이머 설정	설명
RIP 타이밍	
인터벌 초(초)	타이머 인터벌의 길이를 초 단위로 정의합니다. 이 기간은 나머지 RIP 타이밍 필드에 사용됩니다(범위는 1-60).
업데이트 인터벌	경로 업데이트 알림 사이의 인터벌 수를 입력합니다(범위는 1-3,600).
만료 인터벌	경로가 만료될 때까지 마지막으로 업데이트된 시간 사이의 인터벌 수를 입력합니다(범위는 1-3,600).
인터벌 삭제	경로가 삭제될 때까지 만료되는 시간 사이의 인터벌 수를 입력합니다(범위는 1-3,600).

RIP 인증 프로파일 탭

- 네트워크 > 가상 라우터 > RIP > 인증 프로파일

기본적으로 방화벽은 이웃 간의 RIP 메시지를 인증하지 않습니다. 이웃 간의 RIP 메시지를 인증하려면 인증 프로파일을 만들고 가상 라우터에서 RIP를 실행하는 인터페이스에 적용합니다. 다음 표에서는 인증 프로파일 탭에 대한 설정을 설명합니다.

RIP – 인증 프로파일 설정	설명
프로파일 이름	RIP 메시지를 인증하기 위한 인증 프로파일의 이름을 입력합니다.
비밀번호 유형	비밀번호 유형(단순 또는 MD5)을 선택합니다. • **Simple**을 선택하는 경우 간편 비밀번호를 입력한 후 확인합니다. • **MD5**를 선택하는 경우 키 **ID**(0-255), 키 및 선택적 기본 상태를 포함하여 하나 이상의 비밀번호 항목을 입력합니다. 각 항목에 대해 추가를 클

RIP – 인증 프로파일 설정	설명
	릭한 다음 확인을 클릭합니다. 보내는 메시지를 인증하는 데 사용할 키를 지정하려면 기본 옵션을 선택합니다.

RIP 내보내기 규칙 탭

- 네트워크 > 가상 라우터 > RIP > 내보내기 규칙

RIP 내보내기 규칙을 사용하면 가상 라우터가 피어에게 보내는 경로를 제어할 수 있습니다.

RIP – 내보내기 규칙 설정	설명
기본 경로 재배포 허용	방화벽이 기본 경로를 피어에 재배포하도록 허용하려면 선택합니다.
재배포 프로파일	추가를 클릭하고 원하는 네트워크 동작을 기반으로 경로 재배포, 필터, 우선 순위 및 작업을 수정할 수 있는 재배포 프로파일을 선택하거나 생성합니다. 경로 재분배를 참조하십시오.

OSPF

- 네트워크 > 가상 라우터 > OSPF

OSPF(Open Shortest Path First) 프로토콜을 구성하려면 다음 일반 설정을 구성해야 합니다(선택 사항인 BFD 제외).

OSPF 설정	설명
활성화	OSPF 프로토콜을 활성화하려면 선택합니다.
기본 경로 거부	(권장) OSPF를 통해 기본 경로를 학습하지 않으려면 선택하십시오.
라우터 ID	이 가상 라우터의 OSPF 인스턴스와 연결된 라우터 ID를 지정합니다. OSPF 프로토콜은 라우터 ID를 사용하여 OSPF 인스턴스를 고유하게 식별합니다.
BFD	PA-400 시리즈, PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈 또는 VM 시리즈 방화벽의 가상 라우터에 대해 전 세계적으로 OSPF에 대한 양방향 포워딩 탐지(BFD)를 사용하도록 설정하려면 다음 중 하나를 선택합니다. • 기본값(기본 BFD 설정) • 방화벽에서 생성한 BFD 프로파일

OSPF 설정	설명
	• 새 BFD 프로파일을 만들기 위한 새 **BFD** 프로파일 가상 라우터의 모든 OSPF 인터페이스에 대해 BFD를 비활성화하려면 없음**(BFD** 비활성화**)**을 선택합니다. 단일 OSPF 인터페이스에 대해 BFD를 활성화할 수 없습니다.

또한 다음 탭에서 OSPF 설정을 구성해야 합니다.

- 지역: OSPF 영역 탭을 참조하십시오.
- 인증 프로파일: OSPF 인증 프로파일 탭을 참조하십시오.
- 내보내기 규칙: OSPF 내보내기 규칙 탭을 참조하십시오.
- **Advanced**: OSPF Advanced 탭을 참조하십시오.

OSPF 영역 탭

- 네트워크 > 가상 라우터 > OSPF > 영역

다음 필드는 OSPF 영역 설정을 설명합니다.

OSPF – 영역 설정	설명
지역	
지역 ID	OSPF 매개변수를 적용할 수 있는 영역을 구성합니다. 영역에 대한 식별자를 xxxx 형식으로 입력합니다. 이것은 각 이웃이 동일한 영역의 일부로 수락해야 하는 식별자입니다.
유형	다음 옵션 중 하나를 선택합니다. • 일반 - 제한이 없습니다. 이 영역은 모든 유형의 경로를 수행할 수 있습니다. • **Stub** - 해당 영역의 콘센트가 없습니다. 지역 밖의 목적지에 도달하기 위해서는 다른 지역과 연결되는 국경을 통과해야 합니다. 이 옵션을 선택한 경우 다른 영역에서 이러한 LSA(링크 상태 광고) 유형을 수락하려면 요약 수락을 선택합니다. 또한 관련 메트릭 값(범위: 1~255)과 함께 스텁 영역에 대한 광고에 기본 경로 LSA를 포함할지 여부를 지정합니다. 요약 수락 옵션인 경우 스텁 영역에서 ABR(영역 경계 라우터) 인터페이스가 비활성화되면 OSPF 영역은 TSATotally Stubby Area)로 작동하고 ABR은 요약 LSA를 전파하지 않습니다.

OSPF – 영역 설정	설명
	• **NSSA** (Not-So-Stubby Area) - 이 영역을 직접 벗어날 수 있지만 OSPF 경로 이외의 경로를 통해서만 가능합니다. 이 옵션을 선택한 경우 이 유형의 LSA를 수락하려면 요약 수락을 선택합니다. **Advertise Default Route**를 선택하여 관련 메트릭 값(1-255)과 함께 스터브 영역에 대한 광고에 기본 경로 LSA를 포함할지의 여부를 지정합니다. 또한 기본 LSA를 알리는 데 사용되는 경로 유형을 선택합니다. NSSA를 통해 학습된 외부 경로를 다른 영역으로 광고하는 것을 활성화하거나 억제하려면 외부 범위 섹션에서 추가를 클릭하고 범위를 입력합니다.
범위	추가를 클릭하여 해당 영역의 LSA 대상 주소를 서브넷으로 통합합니다. 서브넷과 일치하는 광고 LSA를 활성화하거나 억제하고 확인을 클릭합니다. 추가 범위를 추가하려면 반복합니다.

상호 작용	영역에 포함할 인터페이스를 추가하고 다음 정보를 입력합니다.
	• 인터페이스 - 인터페이스를 선택합니다.
	• 활성화 - OSPF 인터페이스 설정을 적용합니다.
	• 수동 - OSPF 인터페이스에서 OSPF 패킷을 보내거나 받지 않도록 하려면 선택합니다. 이 옵션을 선택하면 OSPF 패킷이 전송되거나 수신되지 않지만 인터페이스는 LSA 데이터베이스에 포함됩니다.
	• 링크 유형 - 인터페이스를 통해 액세스할 수 있는 모든 이웃이 이더넷 인터페이스와 같은 OSPF 헬로 메시지를 멀티캐스팅하여 자동으로 검색되도록 하려면 브로드캐스트를 선택합니다. 이웃을 자동으로 검색하려면 **p2p**(point-to-point)를 선택합니다. 이웃을 수동으로 정의해야 하는 경우 **p2mp**(point-to-multipoint)를 선택합니다. 수동으로 이웃을 정의하는 것은 p2mp 모드에서만 허용됩니다.
	• 메트릭 - 이 인터페이스에 대한 OSPF 메트릭을 입력합니다(0-65,535).
	• 우선 순위 - 이 인터페이스의 OSPF 우선 순위를 입력합니다(0-255). 라우터가 OSPF 프로토콜에 따라 지정 라우터(DR) 또는 백업 DR(BDR)로 선택되는 우선 순위입니다. 값이 0이면 라우터는 DR 또는 BDR로 선택되지 않습니다.
	• 인증 프로파일 - 이전에 정의된 인증 프로파일을 선택합니다.
	• **BFD** - OSPF 피어 인터페이스에 대해 **BFD**(양방향 포워딩 감지)를 활성화하려면(따라서 가상 라우터 수준에서 OSPF에 대해 **BFD**가 비활성화되지 않는 한 OSPF에 대한 BFD 설정을 재정의) 다음 중 하나를 선택합니다.
	  • 기본값(기본 BFD 설정)
	  • 방화벽에서 생성한 BFD 프로파일

OSPF – 영역 설정	설명
	• 새 BFD 프로파일을 만들기 위한 새 **BFD** 프로파일 • OSPF 피어 인터페이스에 대해 BFD를 비활성화하려면 없음**(BFD** 비활성화**)**을 선택합니다. • 헬로 인터벌**(**초**)** - OSPF 프로세스가 직접 연결된 이웃에게 헬로 패킷을 보내는 인터벌(초)입니다(범위는 0-3600, 기본값은 10). • 데드 카운트 - OSPF가 이웃으로부터 헬로 패킷을 수신하지 않는 OSPF가 해당 이웃을 다운으로 간주하기 전에 이웃에 대해 헬로 인터벌이 발생할 수 있는 횟수입니다. 헬로 인터벌에 데드 카운트를 곱하면 데드 타이머 값과 같습니다(범위는 3-20, 기본값은 4). • 재전송 인터벌**(**초**)** - OSPF가 LSA를 재전송하기 전에 OSPF가 이웃으로부터 LSA(링크 상태 광고)를 수신하기 위해 대기하는 시간(초)입니다(범위는 0-3,600, 기본값은 10). • 전송 지연**(**초**)** - LSA가 인터페이스에서 전송되기 전에 지연되는 시간(초)입니다(범위는 0-3,600, 기본값은 1).
인터페이스(계속)	• **Graceful Restart Hello Delay(**초**)** - 능동형/수동형 고가용성이 구성된 경우 OSPF 인터페이스에 적용됩니다. **Graceful Restart Hello Delay**는 방화벽이 1초 인터벌으로 Grace LSA 패킷을 보내는 시간입니다. 이 시간 동안에는 다시 시작하는 방화벽에서 헬로 패킷이 전송되지 않습니다. 다시 시작하는 동안 데드 타이머(헬로 인터벌에 데드 카운트를 곱한 값)도 카운트다운됩니다. 데드 타이머가 너무 짧으면 헬로 지연(hello delay)으로 인해 단계적 재시작 중에 인접성이 낮아집니다. 따라서 데드 타이머는 **Graceful Restart Hello Delay** 값의 4배 이상으로 설정하는 것이 좋습니다. 예를 들어 헬로 인터벌이 10초이고 데드 카운트가 4이면 데드 타이머는 40초가 됩니다. **Graceful Restart Hello Delay**가 10초로 설정된 경우 헬로 패킷의 10초 지연은 40초 데드 타이머 내에서 편안하므로 인접성은 정상적인 재시작 동안 타임아웃되지 않습니다(범위는 1-10, 기본값은 10).
가상 링크	백본 영역 연결을 유지하거나 향상시키기 위해 가상 링크 설정을 구성합니다. 영역 보더 라우터에 대한 설정을 정의해야 하며 백본 영역(0.0.0.0) 내에서 정의해야 합니다. 추가를 클릭하고 백본 영역에 포함될 각 가상 링크에 대해 다음 정보를 입력한 후 확인을 클릭합니다. • 이름 - 가상 링크의 이름을 입력합니다. • 이웃 **ID** - 가상 링크 반대편에 있는 라우터(이웃)의 라우터 ID를 입력합니다. • 대중 교통 영역 - 가상 링크를 물리적으로 포함하는 대중 교통 영역의 영역 ID를 입력합니다.

OSPF – 영역 설정	설명
	• 활성화 - 가상 링크를 활성화하려면 선택합니다. • 타이밍 - 기본 타이밍 설정을 유지하는 것이 좋습니다. • 인증 프로파일 - 이전에 정의된 인증 프로파일을 선택합니다.

OSPF 인증 프로파일 탭

- 네트워크 > 가상 라우터 > OSPF > 인증 프로파일

다음 필드는 OSPF 인증 프로파일 설정을 설명합니다.

OSPF – 인증 프로파일 설정	설명
프로파일 이름	인증 프로파일의 이름을 입력합니다. OSPF 메시지를 인증하려면 먼저 인증 프로파일을 정의한 다음 **OSPF** 탭의 인터페이스에 적용합니다.
비밀번호 유형	비밀번호 유형(단순 또는 MD5)을 선택합니다. • 단순을 선택한 경우 암호를 입력합니다. • **MD5**를 선택하는 경우 키 **ID**(0-255), 키 및 선택적 기본 상태를 포함하여 하나 이상의 비밀번호 항목을 입력하십시오. 각 항목에 대해 추가를 클릭한 다음 확인을 클릭합니다. 보내는 메시지를 인증하는 데 사용할 키를 지정하려면 기본 옵션을 선택합니다.

OSPF 내보내기 규칙 탭

- 네트워크 > 가상 라우터 > OSPF > 내보내기 규칙

다음 표에서는 OSPF 경로를 내보내는 필드에 대해 설명합니다.

OSPF – 내보내기 규칙 설정	설명
기본 경로 재배포 허용	OSPF를 통한 기본 경로 재배포를 허용하려면 선택합니다.
이름	재배포 프로파일의 이름을 선택합니다. 값은 IP 서브넷 또는 유효한 재배포 프로파일 이름이어야 합니다.
새 경로 유형	적용할 측정항목 유형을 선택합니다.
새 태그	32비트 값이 있는 일치하는 경로에 대한 태그를 지정합니다.

OSPF – 내보내기 규칙 설정	설명
미터법	(선택 사항) 내보낸 경로와 연결되고 경로 선택에 사용할 경로 메트릭을 지정합니다(범위는 1-65,535).

OSPF Advanced 탭

- 네트워크 > 가상 라우터 > OSPF > Advanced

다음 필드는 RFC 1583 호환성, OSPF 타이머 및 정상적인 재시작을 설명합니다.

OSPF – **Advanced** 설정	설명
RFC 1583 호환성	RFC 1583(OSPF 버전 2)과의 호환성을 확인하려면 선택합니다.
타이머	• **SPF** 계산 지연**(**초**)** - 새 토폴로지 정보 수신과 SPF 계산 수행 사이의 지연 시간을 조정할 수 있습니다. 값이 낮을수록 OSPF 재수렴 속도가 빨라집니다. 방화벽과 피어링하는 라우터는 수렴 시간을 최적화하기 위해 유사한 방식으로 조정되어야 합니다. • **LSA** 인터벌**(**초**)**—동일한 LSA(동일한 라우터, 동일한 유형, 동일한 LSA ID)의 두 인스턴스 전송 사이의 최소 시간을 지정합니다. 이것은 RFC 2328의 MinLSInterval과 동일합니다. 토폴로지 변경이 발생할 때 더 낮은 값을 사용하여 재수렴 시간을 줄일 수 있습니다.
정상 재시작	• 정상적인 재시작 활성화 - 기본적으로 활성화되어 있는 이 기능에 대해 활성화된 방화벽은 방화벽을 일시적으로 다운시키는 전환이 발생하는 동안 방화벽을 통해 경로를 계속 사용하도록 인접 라우터에 지시합니다. • 도우미 모드 활성화 - 기본적으로 활성화되어 있으며 이 모드에 대해 활성화된 방화벽은 해당 디바이스가 다시 시작될 때 인접 디바이스로 계속 포워딩됩니다. • 엄격한 **LSA** 검사 활성화 - 기본적으로 활성화되어 있는 이 기능은 토폴로지 변경이 발생하는 경우 OSPF 도우미 모드 활성화 방화벽이 도우미 모드를 종료하도록 합니다. • 유예 기간**(**초**)** - 인접 디바이스가 다시 설정되거나 라우터가 다시 시작되는 동안 피어 디바이스가 이 방화벽으로 계속 포워딩해야 하는 시간(초)입니다(범위는 5-1,800, 기본값은 120). • **Max Neighbor Restart Time** - 방화벽이 도움말 모드 라우터로 수락하는 최대 유예 기간(초)입니다. 피어 디바이스가 유예 LSA에서 더 긴 유예 기간을 제공하는 경우 방화벽은 도우미 모드로 전환되지 않습니다(범위는 5-1,800, 기본값은 140).

OSPFv3

- 네트워크 > 가상 라우터 > OSPFv3

OSPFv3(Open Shortest Path First v3) 프로토콜을 구성하려면 다음 표의 처음 세 가지 설정을 구성해야 합니다(BFD는 선택 사항).

OSPFv3 설정	설명
활성화	OSPF 프로토콜을 활성화하려면 선택합니다.
기본 경로 거부	OSPF를 통해 기본 경로를 학습하지 않으려면 선택하십시오.
라우터 ID	이 가상 라우터의 OSPF 인스턴스와 연결된 라우터 ID를 지정합니다. OSPF 프로토콜은 라우터 ID를 사용하여 OSPF 인스턴스를 고유하게 식별합니다.
BFD	PA-400 시리즈, PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈 및 VM 시리즈 방화벽의 가상 라우터에 대해 전 세계적으로 OSPFv3에 대한 양방향 포워딩 탐지(BFD)를 사용하도록 설정하려면 다음 중 하나를 선택합니다. • 기본값(기본 BFD 설정) • 방화벽에서 생성한 BFD 프로파일 • 새 BFD 프로파일을 만들기 위한 새 **BFD** 프로파일 가상 라우터의 모든 OSPFv3 인터페이스에 대해 BFD를 비활성화하려면 없음**(BFD** 비활성화**)**을 선택합니다. 단일 OSPFv3 인터페이스에 대해 BFD를 활성화할 수 없습니다.

또한 다음 탭에서 OSPFv3 설정을 구성합니다.

- 지역: OSPFv3 영역 탭을 참조하십시오.
- 인증 프로파일: OSPFv3 인증 프로파일 탭을 참조하세요.
- 내보내기 규칙: OSPFv3 내보내기 규칙 탭을 참조하십시오.
- **Advanced**: OSPFv3 Advanced 탭을 참조하십시오.

OSPFv3 영역 탭

- 네트워크 > 가상 라우터 > OSPFv3 > 영역

다음 필드를 사용하여 OSPFv3 영역을 구성합니다.

OSPv3 – 영역 설정	설명
인증	이 OSPF 영역에 대해 지정하려는 인증 프로파일의 이름을 선택하십시오.
유형	다음 중 하나를 선택: • 일반 - 제한이 없습니다. 이 영역에는 모든 유형의 경로가 포함될 수 있습니다. • **Stub** - 해당 영역의 콘센트가 없습니다. 지역 밖의 목적지에 도달하기 위해서는 다른 지역과 연결되는 국경을 통과해야 합니다. 이 옵션을 선택한 경우 다른 영역에서 이러한 LSA(링크 상태 광고) 유형을 수락하려면 요약 수락을 선택합니다. 또한 관련 메트릭 값(1~255) 과 함께 스텁 영역에 대한 광고에 기본 경로 LSA를 포함할지 여부를 지정합니다. 스텁 영역 ABR(영역 경계 라우터) 인터페이스에서 요약 수락 옵션이 비활성화된 경우 OSPF 영역은 TSA(Totally Stubby Area) 로 작동하며 ABR은 요약 LSA를 전파하지 않습니다. • **NSSA**(Not-So-Stubby Area - OSPF 경로 이외의 경로를 통해서만 해당 지역을 직접 벗어날 수 있습니다. 이 옵션을 선택한 경우 이 유형의 LSA를 수락하려면 요약 수락을 선택합니다. 연관된 메트릭 값(1-255)과 함께 스터브 영역에 대한 광고에 기본 경로 LSA를 포함할지의 여부를 지정합니다. 또한 기본 LSA를 알리는 데 사용되는 경로 유형을 선택합니다. NSSA를 통해 학습된 외부 경로를 다른 영역으로 광고하는 것을 활성화하거나 억제하려면 외부 범위 섹션에서 추가를 클릭하고 범위를 입력합니다.
범위	추가를 클릭하여 해당 영역의 LSA 대상 IPv6 주소를 서브넷별로 통합합니다. 서브넷과 일치하는 광고 LSA를 활성화하거나 억제하고 확인을 클릭합니다. 추가 범위를 추가하려면 반복합니다.
상호 작용	추가를 클릭하고 영역에 포함될 각 인터페이스에 대해 다음 정보를 입력하고 확인을 클릭합니다. • 인터페이스 - 인터페이스를 선택합니다. • 활성화 - OSPF 인터페이스 설정을 적용합니다. • 인스턴스 **ID** – OSPFv3 인스턴스 ID 번호를 입력합니다. • 수동 - OSPF 인터페이스가 OSPF 패킷을 보내거나 받지 않도록 하려면 선택합니다. 이 옵션을 선택하면 OSPF 패킷이 전송되거나 수신되지 않지만 인터페이스는 LSA 데이터베이스에 포함됩니다.

OSPv3 – 영역 설정	설명

	• 링크 유형 - 인터페이스를 통해 액세스할 수 있는 모든 이웃이 이더넷 인터페이스와 같은 OSPF 헬로 메시지를 멀티캐스팅하여 자동으로 검색되도록 하려면 브로드캐스트를 선택합니다. 이웃을 자동으로 검색하려면 **p2p**(point-to-point)를 선택합니다. 이웃을 수동으로 정의해야 하는 경우 **p2mp**(point-to-multipoint)를 선택합니다. 수동으로 이웃을 정의하는 것은 p2mp 모드에서만 허용됩니다.
	• 메트릭 - 이 인터페이스에 대한 OSPF 메트릭을 입력합니다(0-65,535).
	• 우선 순위 - 이 인터페이스의 OSPF 우선 순위를 입력합니다(0-255). 라우터가 OSPF 프로토콜에 따라 지정 라우터(DR) 또는 백업 DR(BDR)로 선택되는 우선 순위입니다. 값이 0이면 라우터는 DR 또는 BDR로 선택되지 않습니다.
	• 인증 프로파일 - 이전에 정의된 인증 프로파일을 선택합니다.
	• **BFD** - OSPFv3 피어 인터페이스에 대해 **BFD**(양방향 포워딩 감지)를 활성화하려면(결과적으로 가상 라우터 수준에서 OSPFv3에 대해 **BFD**가 비활성화되지 않는 한 OSPFv3에 대한 BFD 설정을 재정의) 다음 중 하나를 선택합니다.
	  • 기본값(기본 BFD 설정)
	  • 방화벽에서 생성한 BFD 프로파일
	  • 새 BFD 프로파일을 만들기 위한 새 **BFD** 프로파일
	  OSPFv3 피어 인터페이스에 대해 BFD를 비활성화하려면 없음**(BFD** 비활성화**)**을 선택합니다.
	• 헬로 인터벌**(**초**)** - OSPF 프로세스가 직접 연결된 이웃에게 헬로 패킷을 보내는 인터벌(초)입니다(범위는 0-3,600, 기본값은 10).
	• 데드 카운트 - OSPF가 이웃으로부터 헬로 패킷을 수신하지 않는 OSPF가 해당 이웃을 다운으로 간주하기 전에 이웃에 대해 헬로 인터벌이 발생할 수 있는 횟수입니다. 헬로 인터벌에 데드 카운트를 곱하면 데드 타이머 값과 같습니다(범위는 3-20, 기본값은 4).
	• 재전송 인터벌**(**초**)** - OSPF가 LSA를 재전송하기 전에 OSPF가 이웃으로부터 LSA(링크 상태 광고)를 수신하기 위해 대기하는 시간(초)입니다(범위는 0-3,600, 기본값은 10).
	• 전송 지연**(**초**)** - 방화벽이 인터페이스에서 LSA를 보내기 전에 LSA가 지연되는 시간(초)입니다(범위는 0-3,600, 기본값은 1).

인터페이스(계속)	• **Graceful Restart Hello Delay(**초**)** - 능동형/수동형 고가용성이 구성된 경우 OSPF 인터페이스에 적용됩니다. **Graceful Restart Hello Delay**는 방화벽이 1초 인터벌으로 Grace LSA 패킷을 보내는

OSPv3 – 영역 설정	설명
	시간입니다. 이 시간 동안에는 다시 시작하는 방화벽에서 헬로 패킷이 전송되지 않습니다. 다시 시작하는 동안 데드 타이머(헬로 인터벌에 데드 카운트를 곱한 값)도 카운트다운됩니다. 데드 타이머가 너무 짧으면 헬로 지연(hello delay)으로 인해 단계적 재시작 중에 인접성이 낮아집니다. 따라서 데드 타이머는 **Graceful Restart Hello Delay** 값의 4배 이상으로 설정하는 것이 좋습니다. 예를 들어 헬로 인터벌이 10초이고 데드 카운트가 4이면 데드 타이머는 40초가 됩니다. **Graceful Restart Hello Delay**가 10초로 설정된 경우 헬로 패킷의 10초 지연은 40초 데드 타이머 내에서 편안하므로 인접성은 정상적인 재시작 동안 타임아웃되지 않습니다(범위는 1-10, 기본값은 10). • 이웃 - p2pmp 인터페이스의 경우 이 인터페이스를 통해 연결할 수 있는 모든 이웃의 이웃 IP 주소를 입력합니다.
가상 링크	백본 영역 연결을 유지하거나 향상시키기 위해 가상 링크 설정을 구성합니다. 영역 경계 라우터에 대한 설정을 정의해야 하며 백본 영역(0.0.0.0) 내에서 정의해야 합니다. 추가를 클릭하고 백본 영역에 포함될 각 가상 링크에 대해 다음 정보를 입력한 후 확인을 클릭합니다. • 이름 - 가상 링크의 이름을 입력합니다. • 인스턴스 **ID** - OSPFv3 인스턴스 ID 번호를 입력합니다. • 이웃 **ID** - 가상 링크 반대편에 있는 라우터(이웃)의 라우터 ID를 입력합니다. • 대중 교통 영역 - 가상 링크를 물리적으로 포함하는 대중 교통 영역의 영역 ID를 입력합니다. • 활성화 - 가상 링크를 활성화하려면 선택합니다. • 타이밍 - 기본 타이밍 설정을 유지하는 것이 좋습니다. • 인증 프로파일 - 이전에 정의된 인증 프로파일을 선택합니다.

OSPFv3 인증 프로파일 탭

- 네트워크 > 가상 라우터 > OSPFv3 > 인증 프로파일

다음 필드를 사용하여 OSPFv3에 대한 인증을 구성합니다.

OSPFv3 – 인증 프로파일 설정	설명
프로파일 이름	인증 프로파일의 이름을 입력합니다. OSPF 메시지를 인증하려면 먼저 인증 프로파일을 정의한 다음 **OSPF** 탭의 인터페이스에 적용합니다.
SPI	원격 방화벽에서 피어로의 패킷 통과를 위한 SPI(보안 매개변수 색인)를 지정합니다.
규약	다음 프로토콜 중 하나를 지정합니다. • **ESP** - 보안 페이로드 프로토콜을 캡슐화합니다. • **AH** - 인증 헤더 프로토콜
암호화 알고리즘	다음 중 하나를 지정하십시오. • **None** - 암호화 알고리즘이 사용되지 않습니다. • **SHA1**(기본값) - 보안 해시 알고리즘 1. • **SHA256** - 보안 해시 알고리즘 2. 256비트 다이제스트가 포함된 4개의 해시 함수 집합입니다. • **SHA384** - 보안 해시 알고리즘 2. 384비트 다이제스트가 있는 4개의 해시 함수 집합입니다. • **SHA512** - 보안 해시 알고리즘 2. 512비트 다이제스트가 있는 4개의 해시 함수 집합입니다. • **MD5** - MD5 메시지 다이제스트 알고리즘.
키/키 확인	인증 키를 입력하고 확인합니다.
암호화(ESP 프로토콜만)	다음 중 하나를 지정합니다. • **3des**(기본값) - 56비트의 세 가지 암호화 키를 사용하여 3DES(Triple Data Encryption Algorithm)를 적용합니다. • **aes-128-cbc** - 128비트의 암호화 키를 사용하여 Advanced 암호화 표준(AES)을 적용합니다. • **aes-192-cbc** - 192비트의 암호화 키를 사용하여 Advanced 암호화 표준(AES)을 적용합니다. • **aes-256-cbc** - 256비트의 암호화 키를 사용하여 Advanced 암호화 표준(AES)을 적용합니다. • **null** - 암호화가 사용되지 않습니다.

OSPFv3 – 인증 프로파일 설정	설명
키/키 확인	암호화 키를 입력하고 확인합니다.

OSPFv3 내보내기 규칙 탭

- 네트워크 > 가상 라우터 > OSPFv3 > 내보내기 규칙

다음 필드를 사용하여 OSPFv3 경로를 내보냅니다.

OSPFv3 – 내보내기 규칙 설정	설명
기본 경로 재배포 허용	OSPF를 통한 기본 경로 재배포를 허용하려면 선택합니다.
이름	재배포 프로파일의 이름을 선택합니다. 값은 IP 서브넷 또는 유효한 재배포 프로파일 이름이어야 합니다.
새 경로 유형	적용할 측정항목 유형을 선택합니다.
새 태그	32비트 값이 있는 일치하는 경로에 대한 태그를 지정합니다.
미터법	(선택 사항) 내보낸 경로와 연결되고 경로 선택에 사용할 경로 메트릭을 지정합니다(범위는 1-65,535).

OSPFv3 Advanced 탭

- 네트워크 > 가상 라우터 > OSPFv3 > Advanced

다음 필드를 사용하여 SPF 계산에 대한 전송 라우팅을 비활성화하고, OSPFv3 타이머를 구성하고, OSPFv3에 대한 단계적 재시작을 구성합니다.

OSPFv3 – Advanced 설정	설명
SPF 계산을 위한 대중교통 라우팅 비활성화	방화벽이 활성 상태가 아님을 나타내기 위해 이 방화벽에서 보낸 라우터 LSA의 R 비트를 설정하려면 선택합니다. 이 상태에서 방화벽은 OSPFv3에 참여하지만 다른 라우터는 전송 트래픽을 보내지 않습니다. 이 상태에서 로컬 트래픽은 여전히 방화벽으로 포워딩됩니다. 트래픽이 방화벽에 도달할 수 있는 동안 방화벽 주위로

OSPFv3 – Advanced 설정	설명
	다시 라우팅될 수 있으므로 이중 홈 네트워크로 유지 관리를 수행하는 동안 유용합니다.
타이머	• **SPF** 계산 지연(초) - 새 토폴로지 정보 수신과 SPF 계산 수행 사이의 지연 시간을 조정할 수 있는 지연 타이머입니다. 값이 낮을수록 OSPF 재수렴 속도가 빨라집니다. 방화벽과 피어링하는 라우터는 수렴 시간을 최적화하기 위해 유사한 방식으로 조정되어야 합니다. • **LSA** 인터벌(초) - 이 옵션은 동일한 LSA(동일한 라우터, 동일한 유형, 동일한 LSA ID)의 두 인스턴스 전송 사이의 최소 시간을 지정합니다. 이것은 RFC 2328의 MinLSInterval과 동일합니다. 토폴로지 변경이 발생할 때 더 낮은 값을 사용하여 재수렴 시간을 줄일 수 있습니다.
정상 재시작	• 정상적인 재시작 활성화 - 기본적으로 활성화되어 있는 이 기능에 대해 활성화된 방화벽은 방화벽을 일시적으로 다운시키는 전환이 발생하는 동안 방화벽을 통해 경로를 계속 사용하도록 인접 라우터에 지시합니다. • 도우미 모드 활성화 - 기본적으로 활성화되어 있으며 이 모드에 대해 활성화된 방화벽은 해당 디바이스가 다시 시작될 때 인접 디바이스로 계속 포워딩됩니다. • 엄격한 **LSA** 검사 활성화 - 기본적으로 활성화되어 있는 이 기능은 토폴로지 변경이 발생하는 경우 OSPF 도우미 모드 활성화 방화벽이 도우미 모드를 종료하도록 합니다. • 유예 기간(초) - 인접 항목이 다시 설정되거나 라우터가 다시 시작되는 동안 피어 디바이스가 이 방화벽으로 계속 포워딩하는 시간(초)입니다(범위는 5-1,800, 기본값은 120). • **Max Neighbor Restart Time** - 방화벽이 도움말 모드 라우터로 수락할 최대 유예 기간(초)입니다. 피어 디바이스가 유예 LSA에서 더 긴 유예 기간을 제공하는 경우 방화벽은 도우미 모드로 전환되지 않습니다(범위는 5-800, 기본값은 140).

BGP

- 네트워크 > 가상 라우터 > BGP

BGP(Border Gateway Protocol)를 구성하려면 다음 표에 설명된 대로 BGP를 활성화하고 라우터 ID 및 AS 번호를 구성하도록 기본 BGP 설정을 구성해야 합니다. 또한 BGP 피어를 BGP 피어 그룹의 일부로 구성해야 합니다.

네트워크에 필요한 대로 다음 탭에서 나머지 BGP 설정을 구성합니다.

- 일반: BGP 일반 탭을 참조하십시오.
- **Advanced**: BGP Advanced 탭을 참조하십시오.
- 피어 그룹: BGP 피어 그룹 탭을 참조하십시오.
- 가져오기: BGP 가져오기 및 내보내기 탭을 참조하십시오.
- 내보내기: BGP 가져오기 및 내보내기 탭을 참조하십시오.
- 조건부 **Adv**: BGP 조건부 Adv 탭을 참조하십시오.
- 통합: BGP 통합 탭을 참조하십시오.
- 재배포 규칙: BGP 재배포 규칙 탭을 참조하십시오.

기본 **BGP** 설정

가상 라우터에서 BGP를 사용하려면 BGP를 활성화하고 라우터 ID와 AS 번호를 구성해야 합니다. BFD 활성화는 선택 사항입니다.

BGP 설정	구성 위치	설명
사용	**BGP**	BGP를 활성화하려면 선택합니다.
라우터 ID		가상 라우터에 할당할 IP 주소를 입력합니다.
AS 번호		라우터 ID(범위: 1~4,294,967,295)를 기준으로 가상 라우터가 속한 AS 번호를 입력합니다.
BFD		PA-400 시리즈, PA-3200 시리즈, PA-3400 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈 또는 VM의 가상 라우터에 대해 전역적으로 BGP용 BFD(Bidirectional Forwarding Detection)를 활성화하려면 시리즈 방화벽에서 다음 중 하나를 선택합니다. • 기본값(기본 BFD 설정) • 방화벽의 기존 BFD 프로파일 • 새 **BFD** 프로파일 생성 가상 라우터의 모든 BGP 인터페이스에 대해 BFD를 비활성화하려면 없음**(BFD** 비활성화**)**을 선택합니다. 단일 BGP 인터페이스에 대해 BFD를 활성화할 수 없습니다.

BGP 설정	구성 위치	설명
		*BFD*를 전역적으로 활성화 또는 비활성화하면 *BGP*를 실행하는 모든 인터페이스가 중단되고 *BFD* 기능으로 다시 시작되어 *BGP* 트래픽을 방해할 수 있습니다. 따라서 재수렴이 프로덕션 트래픽에 영향을 미치지 않는 피크가 아닌 시간에 *BGP* 인터페이스에서 *BFD*를 활성화하십시오.

BGP 일반 탭

- 네트워크 > 가상 라우터 > BGP > 일반

다음 필드를 사용하여 일반 BGP 설정을 구성합니다.

BGP 일반 설정	구성 위치	설명
기본 경로 거부	**BGP** > 일반	BGP 피어에서 보급하는 모든 기본 경로를 무시하려면 선택합니다.
경로 설치		전역 라우팅 테이블에 BGP 경로를 설치하려면 선택합니다.
통합 MED		경로에 다른 MED(Multi-Exit Discriminator) 값이 있는 경우에도 경로 통합을 활성화하려면 선택합니다.
기본 로컬 기본 설정		방화벽이 다른 경로 간의 기본 설정을 결정하는 데 사용할 수 있는 값을 지정합니다.
AS 형식		2바이트(기본값) 또는 4바이트 형식을 선택합니다. 이 설정은 상호 운용성을 위해 구성할 수 있습니다.
항상 MED 비교		다른 자율 시스템에 있는 이웃의 경로에 대해 MED 비교를 활성화합니다.
결정적 MED 비교		MED 비교를 활성화하여 iBGP 피어(동일한 자율 시스템의 BGP 피어)에서 보급하는 경로 중에서 선택합니다.
인증 프로파일		새 인증 프로파일을 추가하고 다음 설정을 구성합니다. • 프로파일 이름 - 프로파일을 식별할 이름을 입력합니다. • **Secret/Confirm Secret** - BGP 피어 통신을 위한 암호를 입력하고 확인합니다.

BGP 일반 설정	구성 위치	설명
		더 이상 필요하지 않은 프로파일은 삭제(⊖)합니다.

BGP Advanced 탭

- 네트워크 > 가상 라우터 > BGP > Advanced

Advanced BGP 설정에는 다양한 기능이 포함됩니다. 여러 BGP 자율 시스템에서 ECMP를 실행할 수 있습니다. eBGP 피어가 자신의 AS를 AS_PATH 속성의 첫 번째 AS로 나열하도록 요구할 수 있습니다(스푸핑된 업데이트 패킷 방지 목적). BGP 정상 재시작을 구성할 수 있습니다. BGP 피어가 BGP 재시작 중에 포워딩 상태를 유지할 수 있는지의 여부를 표시하여 경로 플랩(상승 및 하향)의 결과를 최소화합니다. AS에서 BGP 피어링의 전체 메시를 사용하지 않도록 하는 두 가지 방법인 경로 리플렉터와 AS 컨페더레이션을 구성할 수 있습니다. BGP 네트워크가 불안정하고 경로가 흔들릴 때 불필요한 라우터 수렴을 방지하도록 경로 감쇠를 구성할 수 있습니다.

BGP Advanced 설정	구성 위치	설명
ECMP 다중 AS 지원	**BGP** > 고급	가상 라우터에 대해 ECMP를 활성화하고 여러 BGP 자율 시스템에서 ECMP를 실행하려는 경우 선택합니다.
EBGP에 대한 첫 번째 AS 시행		방화벽이 eBGP 피어의 자체 AS 번호를 AS_PATH 속성의 첫 번째 AS 번호로 나열하지 않는 eBGP 피어에서 들어오는 업데이트 패킷을 삭제하도록 합니다. 이것은 BGP가 이웃 AS가 아닌 다른 AS로부터 도착한 스푸핑되거나 잘못된 업데이트 패킷을 더 이상 처리하는 것을 방지합니다. 기본값은 활성화되어 있습니다.
정상 재시작		단계적 재시작 옵션을 활성화합니다. • **Stale Route Time**—경로가 부실 상태를 유지할 수 있는 시간(초)을 지정합니다(범위는 1-3,600, 기본값은 120). • 로컬 다시 시작 시간 - 방화벽이 다시 시작되는 데 걸리는 시간(초)을 지정합니다. 이 값은 피어에게 보급됩니다(범위는 1-3,600, 기본값은 120). • 최대 피어 다시 시작 시간 - 방화벽이 피어 디바이스에 대한 유예 기간 다시 시작 시간으로 허용하는 최대 시간(초)을 지정합니다(범위는 1-3,600, 기본값은 120).
리플렉터 클러스터 ID		리플렉터 클러스터를 나타내는 IPv4 식별자를 지정합니다. AS의 경로 리플렉터(라우터)는 학습한 경로를 피어에게 다시 알리는 역할을

BGP Advanced 설정	구성 위치	설명
		수행합니다(전체 메시 연결이 필요하고 모든 피어가 서로 경로를 보내는 대신). 경로 반사기는 구성을 단순화합니다.
컨페더레이션 멤버 AS		BGP 컨페더레이션 내에서만 볼 수 있는 자율 시스템 번호 식별자(하위 자율 시스템 번호라고도 함)를 지정합니다. BGP 연합을 사용하여 자율 시스템을 하위 자율 시스템으로 나누고 풀 메시 피어링을 줄입니다.
댐핑 프로파일	**BGP** > 고급**(계속)**	경로 감쇠는 경로가 플래핑되기 때문에 광고되지 않는지의 여부를 결정하는 방법입니다. 경로 감쇠는 경로 플래핑으로 인해 라우터가 강제로 재수렴되는 횟수를 줄일 수 있습니다. 설정에는 다음이 포함됩니다. • 프로파일 이름 - 프로파일을 식별할 이름을 입력합니다. • 활성화 - 프로파일을 활성화합니다. • 컷오프 - 경로 광고가 억제되는 경로 철회 임계값을 지정합니다(범위는 0.0-1,000.0, 기본값은 1.25). • 재사용 - 억제된 경로가 다시 사용되는 경로 철회 임계값을 지정합니다(범위는 0.0-1,000.0, 기본값은 5). • 최대 보류 시간—경로가 얼마나 불안정했는지에 관계없이 경로를 억제할 수 있는 최대 시간(초)을 지정합니다(범위는 0-3,600, 기본값은 900). • **Decay Half Life Reachable** - 방화벽이 경로에 도달할 수 있다고 간주하는 경우 경로의 안정성 메트릭이 반감되는 시간(초 단위)을 지정합니다(범위는 0-3,600, 기본값은 300). • **Decay Half Life Unreachable**—방화벽이 경로에 도달할 수 없다고 간주하는 경우 경로의 안정성 측정 항목이 반감되는 시간을 초 단위로 지정합니다(범위는 0-3,600, 기본값은 300). 더 이상 필요하지 않은 프로파일은 삭제(⊖)합니다.

BGP 피어 그룹 탭

- 네트워크 > 가상 라우터 > BGP > 피어 그룹

BGP 피어 그룹은 피어 그룹 유형(예: EBGP) 또는 가상 라우터가 업데이트 패킷으로 보내는 AS_PATH 목록에서 개인 AS 번호를 제거하는 설정과 같은 설정을 공유하는 BGP 피어 모음입니다. BGP 피어 그룹을

사용하면 동일한 설정으로 여러 피어를 구성할 필요가 없습니다. 그룹에 속한 BGP 피어를 구성하려면 하나 이상의 BGP 피어 그룹을 구성해야 합니다.

BGP 피어 그룹 설정	구성 위치	설명
이름	**BGP** > 피어 그룹	피어 그룹을 식별할 이름을 입력합니다.
활성화		피어 그룹을 활성화하려면 선택합니다.
통합된 Confed AS 경로		구성된 통합 연합 AS에 대한 경로를 포함하려면 선택합니다.
저장된 정보로 소프트 리셋		피어 설정을 업데이트한 후 방화벽의 소프트 리셋을 수행하려면 선택합니다.

유형		피어 또는 그룹의 유형을 지정하고 관련 설정을 구성합니다(다음 홉 가져오기 및 다음 홉 내보내기에 대한 설명은 이 표의 아래 참조).
		• **IBGP** - 다음을 지정합니다.
		  • 다음 홉 내보내기
		• **EBGP Confed** - 다음을 지정합니다.
		  • 다음 홉 내보내기
		• **IBGP Confed** - 다음을 지정합니다.
		  • 다음 홉 내보내기
		• **EBGP** - 다음을 지정합니다.
		  • 다음 홉 가져오기
		  • 다음 홉 내보내기
		  • 개인 **AS** 제거(BGP가 AS_PATH 속성에서 개인 AS 번호를 제거하도록 하려면 선택).

다음 홉 가져오기		다음 홉 가져오기 옵션을 선택합니다. • 소스 - 소스 경로 광고에 제공된 다음 홉 주소를 사용합니다. • 피어 사용 - 피어의 IP 주소를 다음 홉 주소로 사용합니다.
다음 홉 내보내기		다음 홉 내보내기 옵션을 선택합니다. • 확인 - FIB(포워딩 정보 기반)를 사용하여 다음 홉 주소를 확인합니다. • 소스 - 소스 경로 광고에 제공된 다음 홉 주소를 사용합니다.

BGP 피어 그룹 설정	구성 위치	설명
		• 자체 사용 - 다음 홉 주소를 가상 라우터의 IP 주소로 교체하여 포워딩 경로에 있도록 합니다.
비공개 AS 제거		AS_PATH 목록에서 사설 자율 시스템을 제거하려면 선택합니다.
이름	**BGP** > 피어 그룹 > 피어	새 BGP 피어를 추가하고 식별할 이름을 입력합니다.
활성화		피어를 활성화하려면 선택합니다.
피어 AS		피어의 AS(자치 시스템)를 지정합니다.
MP-BGP 확장 사용	**BGP** > 피어 그룹 > 피어 > 주소 지정	방화벽이 IPv4 및 IPv6용 다중 프로토콜 BGP 주소 계열 식별자와 RFC 4760에 따른 후속 주소 계열 식별자 옵션을 지원하도록 합니다.
Address Family 유형		이 피어와의 BGP 세션이 지원할 **IPv4** 또는 **IPv6** Address Family를 선택하십시오.
후속 주소 패밀리		이 피어와의 BGP 세션이 수행할 유니캐스트 또는 멀티캐스트 후속 Address Family 프로토콜을 선택합니다.
로컬 주소 - 인터페이스		방화벽 인터페이스를 선택합니다.
로컬 주소 - IP		로컬 IP 주소를 선택합니다.
피어 주소 - 유형 및 주소		피어를 식별하는 주소 유형을 선택하십시오. • **IP** - IP를 선택한 다음 IP 주소를 사용하는 주소 개체를 선택합니다(또는 IP 주소를 사용하는 새 주소 개체 생성). • **FQDN** - FQDN을 선택한 다음 FQDN을 사용하는 주소 개체를 선택합니다(또는 FQDN을 사용하는 새 주소 개체 생성).
인증 프로파일	**BGP** > 피어 그룹 > 피어 > 연결 옵션	프로파일을 선택하거나 드롭다운에서 새 인증 프로파일을 선택합니다. 프로파일 이름과 비밀을 입력하고 비밀 확인을 합니다.
연결 유지 인터벌		대기 시간 설정에 따라 피어의 경로가 억제되는 인터벌을 지정합니다(범위는 0-1,200초, 기본값은 30초).

BGP 피어 그룹 설정	구성 위치	설명
멀티 홉		IP 헤더에 TTL(Time-to-Live) 값을 설정합니다(범위는 0~255, 기본값은 0). 기본값 0은 eBGP의 경우 1을 의미합니다. 기본값 0은 iBGP의 경우 255를 의미합니다.
오픈 지연 시간		피어 TCP 연결을 열고 첫 번째 BGP 열기 메시지를 보내는 사이의 지연 시간을 지정합니다(범위는 0-240초, 기본값은 0초).
홀드 타임		피어 연결이 닫히기 전에 피어에서 오는 연속적인 KEEPALIVE 또는 UPDATE 메시지 사이에 경과할 수 있는 시간을 지정합니다(범위는 3-3,600초, 기본값은 90초).
유휴 유지 시간		피어에 대한 연결을 재시도하기 전에 유휴 상태에서 대기할 시간을 지정합니다(범위는 1-3,600초, 기본값은 15초).
수신 연결 - 원격 포트		수신 포트 번호를 지정하고 이 포트에 대한 트래픽 허용을 지정합니다.
발신 연결 - 로컬 포트		발신 포트 번호 지정 및 이 포트의 트래픽 허용
리플렉터 클라이언트	**BGP** > 피어 그룹 > 피어 > 고급	리플렉터 클라이언트 유형(비 클라이언트, 클라이언트 또는 메시 클라이언트)을 선택합니다. 리플렉터 클라이언트에서 수신한 경로는 모든 내부 및 외부 BGP 피어와 공유됩니다.
피어링 유형		양방향 피어를 지정하거나 지정되지 않은 상태로 둡니다.
최대 프리픽스		피어에서 가져올 최대 IP 접두사 수(1~100,000 또는 무제한)를 지정합니다.
발신자 측 루프 감지 활성화		피어 AS 번호가 AS_PATH 목록에 없는지 확인하기 위해 업데이트에서 경로를 보내기 전에 방화벽이 FIB에 있는 경로의 AS_PATH 속성을 확인하도록 하려면 활성화합니다. 그렇다면 방화벽은 루프를 방지하기 위해 제거합니다. 일반적으로 수신자는 루프 감지를 수행하지만 이 최적화 기능에는 발신자가 루프 감지를 수행합니다.
BFD		BGP 피어에 대해 BFD(양방향 포워딩 감지)를 활성화하려면(그러므로 가상 라우터 수준에서 BGP에 대해 **BFD**가 비활성화되지 않는 한 BGP에 대한 **BFD** 설정을 재정의), 기본 프로필(기본 BFD 설정), 기존 BFD 프로필, **Inherit-vr-global-setting**(글로벌 BGP BFD 프

BGP 피어 그룹 설정	구성 위치	설명
		로필 상속) 또는 새 **BFD** 프로필(생성 새 BFD 프로필)을 선택합니다. BFD 비활성화는 BGP 피어에 대한 BFD를 비활성화합니다. *BFD*를 전역적으로 활성화 또는 비활성화하면 *BGP*를 실행하는 모든 인터페이스가 중단되고 *BFD* 기능으로 다시 시작됩니다. 이것은 모든 *BGP* 트래픽을 방해할 수 있습니다. 인터페이스에서 *BFD*를 활성화하면 방화벽은 인터페이스에서 *BFD*를 프로그래밍하기 위해 피어에 대한 *BGP* 연결을 중지합니다. 피어 디바이스는 *BGP* 연결이 끊어지는 것을 보게 되며 이로 인해 프로덕션 트래픽에 영향을 미치는 재수렴이 발생할 수 있습니다. 따라서 재수렴이 프로덕션 트래픽에 영향을 미치지 않는 피크가 아닌 시간에 *BGP* 인터페이스에서 *BFD*를 활성화하십시오.

BGP 가져오기 및 내보내기 탭

- 네트워크 > 가상 라우터 > BGP > 가져오기
- 네트워크 > 가상 라우터 > BGP > 내보내기

BGP 경로를 가져오거나 내보내려면 새 가져오기 또는 내보내기 규칙을 추가하십시오.

BGP 가져오기 및 내보내기 설정	구성 위치	설명
규칙	**BGP** > 가져오기 또는 내보내기 > 일반	규칙을 식별할 이름을 지정합니다. 가져오기 규칙은 최대 63자까지 입력할 수 있습니다. 내보내기 규칙은 최대 31자까지 입력할 수 있습니다. 규칙은 영숫자 문자로 시작해야 하며 영숫자 문자, 밑줄(_), 하이픈(-), 점(.) 및 공백의 조합을 포함할 수 있습니다.
사용		규칙을 활성화하려면 선택합니다.
사용자		이 규칙을 사용할 피어 그룹을 선택하십시오.
AS 경로 정규식	**BGP** > 가져오기 또는 내보내기 > 일치	AS 경로 필터링을 위한 정규식을 지정합니다.

BGP 가져오기 및 내보내기 설정	구성 위치	설명
커뮤니티 정규 표현식		커뮤니티 문자열 필터링을 위한 정규식을 지정합니다.
확장 커뮤니티 정규 표현식		확장 커뮤니티 문자열 필터링을 위한 정규식을 지정합니다.
MED		0-4,294,967,295 범위에서 경로 필터링을 위한 Multi-Exit Discriminator 값을 지정합니다.
라우팅 테이블		가져오기 규칙의 경우 일치하는 경로를 가져올 라우팅 테이블(유니캐스트, 멀티캐스트 또는 둘 다)을 지정합니다. 내보내기 규칙의 경우 일치하는 경로를 내보낼 경로 테이블(유니캐스트, 멀티캐스트 또는 둘 다)을 지정합니다.
주소 프리픽스		경로 필터링을 위한 IP 주소 또는 프리픽스를 지정합니다.
다음 홉		경로 필터링을 위한 다음 홉 라우터 또는 서브넷 지정
피어 수신		경로 필터링을 위한 피어 라우터 지정
동작	**BGP** > 가져오기 또는 내보내기 > 동작	일치 조건이 충족될 때 수행할 작업(허용 또는 거부)을 지정합니다.
감쇠		조치가 허용인 경우에만 감쇠 매개변수를 지정합니다.
로컬 선호		작업이 허용인 경우에만 로컬 기본 설정 메트릭을 지정합니다.
MED		작업이 허용(0-65,535)인 경우에만 MED 값을 지정합니다.
무게		작업이 허용(0-65,535)인 경우에만 가중치 값을 지정합니다.
다음 홉		작업이 허용인 경우에만 다음 홉 라우터를 지정합니다.
출처		원래 경로의 경로 유형을 지정합니다. 작업이 허용인 경우에만 IGP, EGP 또는 불완전합니다.
AS 경로 제한		조치가 허용인 경우에만 AS 경로 제한을 지정하십시오.
AS 경로		AS 경로 지정: 없음, 제거, 프리픽스 추가, 제거 및 프리픽스 추가(작업이 허용인 경우에만).

BGP 가져오기 및 내보내기 설정	구성 위치	설명
지역 사회		커뮤니티 옵션 지정: 없음, 모두 제거, 정규식 제거, 추가 또는 덮어쓰기(작업이 허용인 경우에만).
확장된 커뮤니티		커뮤니티 옵션 지정: 없음, 모두 제거, 정규식 제거, 추가 또는 덮어쓰기(작업이 허용인 경우에만).
		더 이상 필요하지 않은 경우 ⊖ 규칙을 삭제하거나 적절한 경우 규칙을 복사합니다. 규칙을 선택한 다음 위로 이동 또는 아래로 이동하여 순서를 변경할 수도 있습니다.

BGP 조건부 Adv 탭

- 네트워크 > 가상 라우터 > BGP > 조건부 Adv

BGP 조건부 광고를 사용하면 선호 경로가 LocRIB(로컬 BGP 라우팅 테이블)에서 사용 가능하지 않아 피어링 또는 연결 실패를 나타내는 경우 광고할 경로를 제어할 수 있습니다. 이것은 여러 ISP를 통한 인터넷 링크가 있고 트래픽이 선호하는 공급자에 대한 연결에 대해 손실된 경우를 제외하고 다른 공급자 대신 한 공급자에게 라우팅되기를 원하는 경우와 같이 다른 AS를 통해 하나의 AS로의 경로를 강제로 시도하려는 경우에 유용합니다.

조건부 광고의 경우 기본 경로(주소 프리픽스)와 기본 경로를 식별하는 기타 특성(예: AS 경로 정규식)을 지정하는 Non Exist(존재하지 않음) 필터를 구성합니다. Non Exist 필터와 일치하는 경로가 로컬 BGP 라우팅 테이블에 없는 경우에만 방화벽은 Advertise 필터에 지정된 대체 경로(선호되지 않는 다른 공급자에 대한 경로)의 보급을 허용합니다.

조건부 광고를 구성하려면 조건부 광고 탭, 조건부 광고 추가를 선택한 다음 다음 표에 설명된 값을 구성합니다.

BGP 조건부 광고 설정	구성 위치	설명
정책	**BGP** > 조건부 진행	이 조건부 광고 정책 규칙의 이름을 지정하십시오.
활성화		이 조건부 광고 정책 규칙을 활성화하려면 선택합니다.
사용자		이 조건부 광고 정책 규칙을 사용할 피어 그룹을 추가합니다.

BGP 조건부 광고 설정	구성 위치	설명
존재하지 않는 필터	**BGP** > 조건부 진행 > 존재하지 않는 필터	이 탭을 사용하여 기본 경로의 프리픽스를 지정합니다. 로컬 BGP 라우팅 테이블에서 사용할 수 있는 경우 보급하려는 경로를 지정합니다. (만약 프리픽스가 광고될 예정이고 존재하지 않는 필터와 일치하면 광고가 억제됩니다.) 존재하지 않는 필터를 추가하고 이 필터를 식별할 이름을 지정하십시오.
활성화		존재하지 않음 필터를 활성화하려면 선택합니다.
AS 경로 정규식		AS 경로 필터링을 위한 정규식을 지정합니다.
커뮤니티 정규 표현식		커뮤니티 문자열 필터링을 위한 정규식을 지정합니다.
확장 커뮤니티 정규 표현식		확장 커뮤니티 문자열을 필터링하기 위한 정규식을 지정합니다.
MED		경로 필터링에 대한 MED 값을 지정합니다(범위는 0-4,294,967,295).
라우팅 테이블		일치하는 경로가 있는지 확인하기 위해 방화벽이 검색할 경로 테이블(유니캐스트, 멀티캐스트 또는 둘 다)을 지정합니다. 일치하는 경로가 해당 경로 테이블에 없는 경우에만 방화벽이 대체 경로의 보급을 허용합니다.
주소 프리픽스		기본 경로에 대한 정확한 NLRI(Network Layer Reachability Information) 프리픽스를 추가합니다.
다음 홉		경로 필터링을 위해 다음 홉 라우터 또는 서브넷을 지정합니다.
피어 수신		경로 필터링을 위한 피어 라우터를 지정합니다.
광고 필터	**BGP** > 조건부 진행 > 광고 필터	이 탭을 사용하여 Non Exist 필터의 경로를 로컬 라우팅 테이블에서 사용할 수 없는 경우 알리기 위해 Local-RIB 라우팅 테이블의 경로 프리픽스를 지정합니다. 프리픽스가 보급되어야 하고 Non Exist(존재하지 않음 필터)와 일치하지 않는 경우 보급이 발생합니다. 광고 필터를 추가하고 이 필터를 식별할 이름을 지정하십시오.

BGP 조건부 광고 설정	구성 위치	설명
활성화		필터를 활성화하려면 선택합니다.
AS 경로 정규식		AS 경로 필터링을 위한 정규식을 지정합니다.
커뮤니티 정규 표현식		커뮤니티 문자열 필터링을 위한 정규식을 지정합니다.
확장 커뮤니티 정규 표현식		확장 커뮤니티 문자열을 필터링하기 위한 정규식을 지정합니다.
MED		경로 필터링에 대한 MED 값을 지정합니다(범위는 0-4,294,967,295).
라우팅 테이블		일치하는 경로가 조건부로 보급될 때 방화벽이 사용하는 경로 테이블(유니캐스트, 멀티캐스트 또는 둘 다)을 지정합니다.
주소 프리픽스		기본 경로를 사용할 수 없는 경우 보급할 경로에 대한 정확한 NLRI(Network Layer Reachability Information) 프리픽스를 추가합니다.
다음 홉		경로 필터링을 위한 다음 홉 라우터 또는 서브넷을 지정합니다.
피어 수신		경로 필터링을 위한 피어 라우터를 지정합니다.

BGP 통합 탭

- 네트워크 > 가상 라우터 > BGP > 통합

경로 통합은 특정 경로(프리픽스 길이가 더 긴 경로)를 단일 경로(프리픽스 길이가 더 짧은 경로)로 결합하여 방화벽이 보내야 하는 라우팅 광고를 줄이고 경로 테이블에 더 적은 수의 경로를 포함하는 작업입니다.

BGP 통합 설정	구성 위치	설명
이름	**BGP** > 통합	통합 규칙의 이름을 입력합니다.
프리픽스		더 긴 프리픽스를 통합하는 데 사용할 요약 프리픽스(IP 주소/프리픽스 길이)를 입력합니다.
활성화		이 경로 통합을 활성화하려면 선택합니다.

BGP 통합 설정	구성 위치	설명
요약		경로를 요약하려면 선택합니다.
AS 세트		이 집합 규칙에 대해 방화벽이 집합 경로의 AS 경로에 AS 번호 집합(AS 집합)을 포함하도록 하려면 선택합니다. AS 세트는 통합되는 개별 경로에서 출발한 AS 번호의 정렬되지 않은 목록입니다.
이름	**BGP** > 통합 > 억제 필터	일치하는 경로가 표시되지 않도록 하는 속성을 정의합니다. 억제 필터의 이름을 추가하고 입력합니다.
활성화		Suppress Filter를 활성화하려면 선택합니다.
AS 경로 정규식		통합될 경로를 필터링하려면 AS_PATH에 대한 정규식을 지정하십시오. 예를 들어 ^5000은 AS 5000에서 학습된 경로를 의미합니다.
커뮤니티 정규 표현식		통합될 경로를 필터링할 커뮤니티에 대한 정규식을 지정합니다. 예를 들어 500:.*는 500:x가 있는 커뮤니티와 일치합니다.
확장 커뮤니티 정규 표현식		통합될 경로를 필터링하려면 확장 커뮤니티에 대한 정규식을 지정하십시오.
MED		통합할 경로를 필터링하는 MED를 지정합니다.
라우팅 테이블		억제해야 하는(공개되지 않음) 통합 경로에 사용할 라우팅 테이블을 유니캐스트, 멀티캐스트 또는 둘 다 지정합니다.
주소 프리픽스		광고에서 제외할 IP 주소를 입력합니다.
다음 홉		억제할 BGP 프리픽스의 다음 홉 주소를 입력합니다.
피어 수신		억제하려는 BGP 프리픽스를 수신한 피어의 IP 주소를 입력하십시오.
이름	**BGP** > 통합 > 광고 필터	방화벽이 필터와 일치하는 모든 경로를 피어에게 알리도록 하는 광고 필터의 속성을 정의합니다. 추가를 클릭하고 광고 필터의 이름을 입력합니다.
활성화		이 광고 필터를 활성화하려면 선택하십시오.
AS 경로 정규식		광고할 경로를 필터링하려면 AS_PATH에 대한 정규식을 지정하십시오.

BGP 통합 설정	구성 위치	설명
커뮤니티 정규 표현식		광고할 경로를 필터링하려면 커뮤니티에 대한 정규식을 지정하십시오.
확장 커뮤니티 정규 표현식		보급될 경로를 필터링하려면 확장 커뮤니티에 대한 정규식을 지정하십시오.
MED		광고할 경로를 필터링하려면 MED 값을 지정하십시오.
라우팅 테이블		유니캐스트, 멀티캐스트 또는 둘 다와 같이 통합 경로의 광고 필터에 사용할 라우팅 테이블을 지정합니다.
주소 프리픽스		BGP가 보급할 IP 주소를 입력합니다.
다음 홉		BGP가 보급할 IP 주소의 다음 홉 주소를 입력합니다.
피어 수신		BGP가 광고할 프리픽스를 수신한 피어의 IP 주소를 입력합니다.
	BGP > 통합 > 라우트 속성 집계	통합 경로에 대한 속성을 정의합니다.
로컬 선호		0-4,294,967,295 범위의 로컬 기본 설정입니다.
MED		0-4,294,967,295 범위의 다중 종료 판별자.
무게		0-65,535 범위의 무게.
다음 홉		다음 홉 IP 주소.
출처		경로의 출처: **igp**, **egp** 또는 불완전.
AS 경로 제한		AS 경로 제한 범위는 1-255입니다.
AS 경로		유형 선택: 없음 또는 추가.
지역 사회		유형 선택: 없음, 모두 제거, 정규식 제거, 추가 또는 덮어쓰기.
확장된 커뮤니티		유형 선택: 없음, 모두 제거, 정규식 제거, 추가 또는 덮어쓰기.

BGP 재배포 규칙 탭

- 네트워크 > 가상 라우터 > BGP > 재배포 규칙

BGP 경로를 재배포하기 위한 규칙을 생성하려면 다음 표에 설명된 설정을 구성합니다.

BGP 재배포 규칙 설정	구성 위치	설명
기본 경로 재배포 허용	**BGP** > 재배포 규칙	방화벽이 기본 경로를 BGP 피어에 재배포하도록 허용합니다.
이름		먼저 IP 서브넷을 추가하거나 재배포 규칙을 생성합니다.
활성화		이 재배포 규칙을 활성화하려면 선택합니다.
라우팅 테이블		경로가 재분배될 경로 테이블을 유니캐스트, 멀티캐스트 또는 둘 다로 지정합니다.
미터법		1-65,535 범위에서 측정 항목을 입력합니다.
원점 설정		재배포된 경로(**igp**, **egp** 또는 **incomplete**)의 원점을 선택합니다. **incomplete** 값은 연결된 경로를 나타냅니다.
MED 설정		0-4,294,967,295 범위에서 재배포된 경로에 대한 MED를 입력합니다.
로컬 기본 설정 지정		0-4,294,967,295 범위에서 재배포된 경로에 대한 로컬 기본 설정을 입력합니다.
AS 경로 제한 설정		1-255 범위에서 재배포 경로에 대한 AS 경로 제한을 입력합니다.
커뮤니티 설정		10진수 또는 16진수 또는 AS:VAL 형식의 32비트 값을 선택하거나 입력합니다. AS 및 VAL은 각각 0-65,535 범위에 있습니다. 최대 10개의 커뮤니티를 입력하세요.
확장 커뮤니티 설정		64비트 값을 16진수 또는 TYPE:AS:VAL 또는 TYPE:IP:VAL 형식으로 입력합니다. 유형은 16비트입니다. AS 또는 IP는 16비트입니다. VAL은 32비트입니다. 최대 5개의 확장 커뮤니티를 입력하세요.

IP 멀티캐스트

- 네트워크 > 가상 라우터 > 멀티캐스트

멀티캐스트 프로토콜을 구성하려면 다음 표준 설정을 구성해야 합니다.

멀티캐스트 설정	설명
활성화	멀티캐스트 라우팅을 활성화하려면 선택합니다.

또한 다음 탭에서 설정을 구성해야 합니다.

- 랑데뷰 포인트: 멀티캐스트 랑데뷰 지점 탭을 참조하십시오.
- 인터페이스: 멀티캐스트 인터페이스 탭을 참조하십시오.
- **SPT** 임계값: 멀티캐스트 SPT 임계값 탭을 참조하십시오.
- 소스 특정 주소 공간: 멀티캐스트 소스 특정 주소 탭을 참조하십시오.
- **Advanced**의: 멀티캐스트 Advanced 탭을 참조하십시오.

멀티캐스트 랑데뷰 포인트 탭

- 네트워크 > 가상 라우터 > 멀티캐스트 > 랑데뷰 포인트

다음 필드를 사용하여 IP 멀티캐스트 랑데뷰 지점을 구성하십시오.

멀티캐스트 설정 – 랑데뷰 포인트	설명

RP 유형	이 가상 라우터에서 실행할 Rendezvous Point(RP) 유형을 선택합니다. 정적 RP는 다른 PIM 라우터에서 명시적으로 구성해야 하는 반면 후보 RP는 자동으로 선택됩니다.
	• 없음 - 이 가상 라우터에서 실행 중인 RP가 없는 경우 선택합니다.
	• 고정 - RP에 대한 고정 IP 주소를 지정하고 드롭다운에서 **RP** 인터페이스 및 **RP** 주소에 대한 옵션을 선택합니다. 이 그룹에 대해 선택된 RP 대신 지정된 RP를 사용하려면 동일한 그룹에 대해 학습된 **RP** 재정의를 선택합니다.
	• 후보 - 이 가상 라우터에서 실행 중인 후보 RP에 대해 다음 정보를 지정합니다.
	  • **RP** 인터페이스 - RP에 대한 인터페이스를 선택합니다. 유효한 인터페이스 유형에는 루프백, L3, VLAN, 통합 이더넷 및 터널이 포함됩니다.
	  • **RP** 주소 - RP의 IP 주소를 선택합니다.
	  • 우선 순위 - 후보 RP 메시지의 우선 순위를 지정합니다(기본값 192).
	  • 알림 인터벌 - 후보 RP 메시지에 대한 알림 인터벌을 지정합니다.
	• 그룹 목록 - 정적 또는 후보를 선택한 경우 추가를 클릭하여 이 후보 RP가 RP로 제안하는 그룹 목록을 지정합니다.

멀티캐스트 설정 – 랑데뷰 포인트	설명
원격 랑데뷰 포인트	추가를 클릭하고 다음을 지정합니다. • **IP** 주소 - RP의 IP 주소를 지정합니다. • 동일한 그룹에 대해 학습된 **RP** 재정의 - 이 그룹에 대해 선택된 RP 대신 지정된 RP를 사용하려면 선택합니다. • 그룹 - 지정된 주소가 RP로 작동할 그룹 목록을 지정합니다.

멀티캐스트 인터페이스 탭

- 네트워크 > 가상 라우터 > 멀티캐스트 > 인터페이스

다음 필드를 사용하여 IGMP, PIM 및 그룹 권한 설정을 공유하는 멀티캐스트 인터페이스를 구성합니다.

멀티캐스트 설정 – 인터페이스	설명
이름	인터페이스 그룹을 식별할 이름을 입력합니다.
설명	선택적 설명을 입력합니다.
상호 작용	인터페이스 그룹에 속하는 하나 이상의 방화벽 인터페이스를 추가하여 멀티캐스트 그룹 권한, IGMP 설정 및 PIM 설정을 공유합니다.
그룹 권한	PIM ASM(Any-Source Multicast) 또는 PIM SSM(Source-Specific Multicast)에 참여하는 멀티캐스트 그룹을 지정합니다. • 모든 소스 - 인터페이스 그룹의 인터페이스에 있는 모든 소스로부터 멀티캐스트 트래픽을 수신할 수 있는 멀티캐스트 그룹을 식별하기 위해 이름을 추가합니다. 기본적으로 그룹은 모든 소스 목록에 포함됩니다. 그룹 구성을 삭제하지 않고 그룹을 쉽게 제외하려면 포함됨을 선택 취소합니다. • 소스 특정 - 인터페이스 그룹의 인터페이스에서 멀티캐스트 트래픽이 허용되는 멀티캐스트 그룹 및 소스 IP 주소 쌍의 이름을 추가합니다. 기본적으로 그룹 및 소스 쌍은 소스 특정 목록에 포함됩니다. 구성을 삭제하지 않고 그룹 및 소스 쌍을 쉽게 제외하려면 포함을 선택 취소합니다.
IGMP	IGMP 트래픽에 대한 설정을 지정합니다. 멀티캐스트 수신기 쪽 인터페이스에 대해 IGMP를 활성화해야 합니다. • 활성화 - IGMP 구성을 활성화하려면 선택합니다.

멀티캐스트 설정 – 인터페이스	설명

	• **IGMP** 버전 - 인터페이스에서 실행할 버전 1, 2 또는 3을 선택합니다.
	• 라우터 경고 **IP** 옵션 적용 - IGMPv2 또는 IGMPv3을 언급할 때 라우터 경고 IP 옵션을 요구하려면 선택합니다. IGMPv1과의 호환성을 위해 비활성화해야 합니다.
	• 항내성 - 네트워크에서 패킷 손실을 설명할 정수 값을 선택합니다(범위는 1~7, 기본값은 2). 패킷 손실이 일반적인 경우 더 높은 값을 선택합니다.
	• 최대 소스 - 인터페이스 그룹에 허용되는 소스별 멤버십의 최대 수를 지정합니다(범위는 1~65,535 또는 무제한).
	• **Max Groups** - 이 인터페이스 그룹에 허용되는 최대 멀티캐스트 그룹 수를 지정합니다(범위는 1 ~ 65,535 또는 무제한).
	• 쿼리 구성 - 다음을 지정합니다.
	  • 쿼리 인터벌 - 일반 쿼리가 모든 수신자에게 전송되는 인터벌을 지정합니다.
	  • 최대 쿼리 응답 시간 - 일반 쿼리와 수신자의 응답 사이의 최대 시간을 지정합니다.
	  • 마지막 구성원 쿼리 인터벌 - 그룹 또는 소스별 쿼리 메시지(그룹 탈퇴 메시지에 대한 응답으로 전송된 메시지 포함) 사이의 인터벌을 지정합니다.
	  • 즉시 탈퇴 - 탈퇴 메시지가 수신되는 즉시 그룹을 탈퇴하려면 선택합니다.

PIM 구성	PIM(프로토콜 독립 멀티캐스트) 설정 지정: • 활성화 - 이 인터페이스가 PIM 메시지를 수신 및/또는 포워딩할 수 있도록 하려면 선택합니다. 멀티캐스트 트래픽을 포워딩하려면 인터페이스를 활성화해야 합니다. • 어설션 인터벌 - PIM 포워딩자를 선택하기 위해 PIM 어설션 메시지 사이의 인터벌을 지정합니다. • 헬로 인터벌 - PIM 헬로 메시지 사이의 인터벌을 지정합니다. • 조인 정리 인터벌 - PIM 조인 메시지(및 PIM 정리 메시지) 사이의 시간(초)을 지정합니다. 기본값은 60입니다. • **DR** 우선 순위 - 이 인터페이스에 대해 지정된 라우터 우선 순위를 지정합니다. • **BSR** 테두리 - 인터페이스를 부트스트랩 테두리로 사용하려면 선택합니다.

멀티캐스트 설정 – 인터페이스	설명
	• **PIM Neighbors** - PIM을 사용하여 통신할 이웃 목록을 추가합니다.

멀티캐스트 SPT 임계값 탭

- 네트워크 > 가상 라우터 > 멀티캐스트 > SPT 임계값

최단 경로 트리(SPT) 임계값은 가상 라우터가 멀티캐스트 그룹 또는 프리픽스에 대한 멀티캐스트 라우팅을 공유 트리 배포(랑데뷰 지점에서 제공)에서 소스 트리(최단 경로 트리 또는 SPT라고도 함) 배포로 전환하는 지점을 정의합니다. 멀티캐스트 그룹 또는 프리픽스에 대한 SPT 임계값을 추가합니다.

SPT 임계값	설명
멀티캐스트 그룹/프리픽스	그룹 또는 프리픽스에 대한 처리량이 임계값 설정에 도달할 때 멀티캐스트 라우팅이 SPT 배포로 전환되는 멀티캐스트 주소 또는 프리픽스를 지정합니다.
임계값(kbps)	멀티캐스트 라우팅이 해당 멀티캐스트 그룹 또는 프리픽스에 대해 SPT 배포로 전환되는 지점을 지정하는 설정을 선택합니다. • **0(**첫 번째 데이터 패킷 켜기**)** - (기본값) 그룹 또는 프리픽스에 대한 멀티캐스트 패킷이 수신되면 가상 라우터가 SPT 배포로 전환합니다. • 부정**(spt**로 전환하지 않음**)**—가상 라우터는 계속해서 멀티캐스트 트래픽을 이 그룹으로 전달하거나 공유 트리의 프리픽스 아래로 전달합니다. • 모든 인터페이스에서 임의의 기간 동안 해당 멀티캐스트 그룹 또는 프리픽스에 도달할 수 있는 멀티캐스트 패킷의 총 킬로비트 수를 입력합니다(범위: 1~4,294,967,295). 처리량이 이 수에 도달하면 가상 라우터가 SPT 배포로 전환됩니다.

멀티캐스트 소스 특정 주소 공간 탭

- 네트워크 > 가상 라우터 > 멀티캐스트 > 소스 특정 주소 공간

특정 소스에서만 멀티캐스트 패킷을 수신할 수 있는 멀티캐스트 그룹을 추가합니다. 이는 멀티캐스트 > 인터페이스 > 그룹 권한 탭에서 소스별로 지정한 것과 동일한 멀티캐스트 그룹 및 이름입니다.

멀티캐스트 설정 – 소스별 주소 공간	설명
이름	방화벽이 SSM(소스별 멀티캐스트) 서비스를 제공하는 멀티캐스트 그룹을 식별합니다.

멀티캐스트 설정 – 소스별 주소 공간	설명
그룹	특정 소스의 멀티캐스트 패킷만 수락할 수 있는 멀티캐스트 그룹 주소를 지정합니다.
포함	SSM 주소 공간에 멀티캐스트 그룹을 포함하려면 선택합니다.

멀티캐스트 **Advanced** 탭

- 네트워크 > 가상 라우터 > 멀티캐스트 > Advanced

세션이 끝난 후 멀티캐스트 경로가 라우팅 테이블에 남아 있는 시간을 구성합니다.

멀티캐스트 **Advanced** 설정	설명
경로 만료 시간(초)	세션이 종료된 후 멀티캐스트 경로가 방화벽의 라우팅 테이블에 남아 있는 기간(초 단위)을 조정할 수 있습니다(범위는 210-7200, 기본값은 210).

ECMP

- 네트워크 > 가상 라우터 > 라우터 설정 > ECMP

ECMP(Equal Cost Multiple Path) 처리는 방화벽이 동일한 대상에 대해 최대 4개의 동일한 비용 경로를 사용할 수 있도록 하는 네트워킹 기능입니다. 이 기능이 없으면 동일한 대상에 대한 동일한 비용 경로가 여러 개 있는 경우 가상 라우터는 라우팅 테이블에서 해당 경로 중 하나를 선택하여 포워딩 테이블에 추가합니다. 선택한 경로에 문제가 발생하지 않는 한 다른 경로를 사용하지 않습니다. 가상 라우터에서 ECMP 기능을 활성화하면 방화벽이 포워딩 테이블의 대상에 대해 최대 4개의 동일한 비용 경로를 가질 수 있으므로 방화벽이 다음을 수행할 수 있습니다.

- 로드 밸런싱 플로우(세션)는 여러 동일한 비용 링크를 통해 동일한 대상으로 이동합니다.
- 일부 링크를 사용하지 않는 상태로 두지 말고 동일한 대상에 대한 모든 링크에서 사용 가능한 대역폭을 사용하십시오.
- 라우팅 프로토콜이나 RIB 테이블이 대체 경로를 선택할 때까지 기다리지 않고 링크가 실패할 경우 다른 ECMP 멤버로의 트래픽을 동일한 대상으로 동적으로 이동하여 링크 실패 시 다운타임을 줄이는 데 도움이 될 수 있습니다.

ECMP 로드 밸런싱은 패킷 수준이 아니라 세션 수준에서 수행됩니다. 이는 방화벽이 패킷을 수신할 때마다가 아니라 새 세션이 시작될 때 동일한 비용 경로를 선택함을 의미합니다.

기존 가상 라우터에서 *ECMP*를 활성화, 비활성화 또는 변경하면 시스템이 가상 라우터를 다시 시작하여 기존 세션이 종료될 수 있습니다.

가상 라우터에 대해 ECMP를 구성하려면 가상 라우터를 선택한 다음 라우터 설정에 대해 **ECMP** 탭을 선택한 다음 설명된 대로 ECMP 설정을 구성합니다.

무엇을 찾고 계신가요?	참조:
ECMP를 구성하는 데 사용할 수 있는 필드는 무엇입니까?	ECMP 설정
더 찾고 계십니까?	ECMP

ECMP 설정

- 네트워크 > 가상 라우터 > 라우터 설정 > ECMP

다음 필드를 사용하여 ECMP(동일 비용 다중 경로) 설정을 구성합니다.

ECMP 설정	설명
활성화	ECMP를 활성화합니다. 기존 가상 라우터에서 *ECMP*를 활성화, 비활성화 또는 변경을 하면 시스템이 가상 라우터를 다시 시작하게 되며 이로 인해 때때로 기존 세션이 종료됩니다.
대칭 반환	(선택 사항) 대칭 반환을 선택하여 반환 패킷이 연결된 수신 패킷이 도착한 동일한 인터페이스로 나가게 합니다. 이렇게 하면 ECMP 인터페이스 대신 반환 패킷을 보낼 때 수신 인터페이스를 사용하도록 방화벽이 구성됩니다. 즉, 대칭 반환 설정이 로드 밸런싱을 재정의합니다. 이 동작은 서버에서 클라이언트로의 트래픽 플로우에 대해서만 발생합니다.
엄격한 소스 경로	기본적으로 방화벽에서 발생하는 IKE 및 IPSec 트래픽은 ECMP 로드 밸런싱 방법이 결정하는 인터페이스를 송신합니다. 방화벽에서 시작되는 IKE 및 IPSec 트래픽이 항상 IPSec 터널의 소스 IP 주소가 속한 물리적 인터페이스를 빠져나가도록 하려면 엄격한 소스 경로를 선택합니다. 방화벽에 동일한 대상에 대해 동일한 비용 경로를 제공하는 둘 이상의 ISP가 있는 경우 엄격한 소스 경로를 활성화하십시오. ISP는 일반적으로 RPF(Reverse Path Forwarding) 검사(또는 IP 주소 스푸핑을 방지하기 위한 다른 검사)를 수행하여 트래픽이 도착한 동일한 인터페이스에서 나가는지 확인합니다. ECMP는 기본적으로 소스 인터페이스를 이그레스(egress) 인터페이스로 선택하는 대신 구성된 ECMP 방법을 기반으로 이그레스(egress) 인터페이스를 선택하기 때문에 ISP가 예상하는 것과 다르며 ISP는 합법적인 반환 트래픽을 차단할 수 있습니다. 이 사용 사례에서는 방화벽이 IPSec 터널의 소스

ECMP 설정	설명
	IP 주소가 속한 인터페이스인 이그레스(egress) 인터페이스를 사용하도록 **Strict Source Path**를 활성화합니다.
최대 경로	동일한 비용 경로의 최대 수를 선택합니다. (2, 3 또는 4) RIB에서 FIB로 복사할 수 있는 대상 네트워크(기본값은 2)입니다.

방법	가상 라우터에서 사용할 다음 ECMP 로드 밸런싱 알고리즘 중 하나를 선택합니다. ECMP 로드 밸런싱은 패킷 수준이 아니라 세션 수준에서 수행됩니다. 즉, 방화벽(ECMP)은 패킷을 수신할 때마다가 아니라 새 세션이 시작될 때 동일한 비용 경로를 선택합니다.
	• **IP Modulo**(기본값) - 가상 라우터는 패킷 헤더에 있는 소스 및 대상 IP 주소의 해시를 사용하여 세션 로드 밸런싱을 수행하여 사용할 ECMP 경로를 결정합니다.
	• **IP** 해시 - 사용할 ECMP 경로를 결정하는 두 가지 IP 해시 방법이 있습니다.
	  • **IP** 해시를 선택하면 기본적으로 방화벽은 소스 및 대상 IP 주소의 해시를 사용합니다.
	  • 소스 주소만 사용(PAN-OS 8.0.3 이상 릴리스에서 사용 가능)을 사용하는 경우 방화벽은 동일한 소스 IP 주소에 속한 모든 세션이 항상 동일한 경로를 사용하도록 합니다.
	  • 소스/대상 포트도 사용하는 경우 방화벽은 해시 계산에 포트를 포함합니다. 또한 해시 시드 값(정수)을 입력하여 로드 밸런싱을 추가로 무작위화할 수 있습니다.
	• 가중 라운드 로빈 - 이 알고리즘을 사용하여 다양한 링크 용량과 속도를 고려할 수 있습니다. 이 알고리즘을 선택하면 인터페이스 대화 상자가 열립니다. 가중치 기반 라운드 로빈 그룹에 포함할 인터페이스를 추가하고 선택합니다. 각 인터페이스에 대해 해당 인터페이스의 가중치를 입력합니다(범위는 1~255, 기본값은 100). 특정 동일 비용 경로에 대한 가중치가 높을수록 새 세션에 대해 동일 비용 경로가 더 자주 선택됩니다. 더 많은 ECMP 트래픽이 더 빠른 링크를 통과하도록 더 높은 속도의 링크에 느린 링크보다 더 높은 가중치를 부여해야 합니다. 그런 다음 다른 인터페이스와 가중치를 추가할 수 있습니다.
	• 균형 라운드 로빈 - 들어오는 ECMP 세션을 링크에 균등하게 분배합니다.

가상 라우터에 대한 추가 런타임 통계

가상 라우터에 대한 고정 경로 또는 라우팅 프로토콜을 구성한 후 네트워크 > 가상 라우터를 선택하고 마지막 항목에서 추가 런타임 통계를 선택합니다. 열에서 라우팅 테이블, 포워딩 테이블, 구성한 라우팅 프로토콜 및 고정 경로와 같은 가상 라우터에 대한 자세한 정보를 볼 수 있습니다. 이 창은 가상 라우터의 단일 화면에 표시할 수 있는 것보다 더 많은 정보를 제공합니다. 창에는 다음 탭이 표시됩니다.

- 라우팅: 라우팅 탭을 참조하십시오.
- **RIP**: RIP 탭을 참조하십시오.
- **BGP**: BGP 탭을 참조하십시오.
- 멀티캐스트: 멀티캐스트 탭을 참조하십시오.
- **BFD** 요약 정보: BFD 요약 정보 탭을 참조하십시오.

라우팅 탭

다음 표는 라우팅 테이블, 포워딩 테이블 및 정적 라우팅 모니터링 테이블에 대한 가상 라우터의 런타임 통계를 설명합니다.

런타임 통계	설명
라우팅 테이블	
라우팅 테이블	유니캐스트 또는 멀티캐스트를 선택하여 유니캐스트 또는 멀티캐스트 라우팅 테이블을 표시합니다.
주소 패밀리 표시	**IPv4** 전용, **IPv6** 전용 또는 **IPv4** 및 **IPv6**(기본값)을 선택하여 테이블에 표시할 주소 그룹을 제어합니다.
데스티네이션	가상 라우터가 도달할 수 있는 네트워크의 IPv4 주소 및 넷마스크 또는 IPv6 주소 및 프리픽스 길이.
다음 홉	대상 네트워크를 향한 다음 홉에 있는 디바이스의 IP 주소입니다. 0.0.0.0의 다음 홉은 기본 경로를 나타냅니다.
미터법	경로에 대한 측정 항목입니다. 라우팅 프로토콜에 동일한 대상 네트워크에 대한 경로가 둘 이상 있는 경우 메트릭 값이 가장 낮은 경로를 선호합니다. 각 라우팅 프로토콜은 다른 유형의 메트릭을 사용합니다. 예를 들어, RIP는 홉 수를 사용합니다.
무게	경로의 가중치입니다. 예를 들어 BGP에 동일한 대상에 대한 경로가 두 개 이상 있는 경우 가중치가 가장 높은 경로를 선호합니다.
플래그	• **A?B** - BGP를 통해 활성 및 학습됨

런타임 통계	설명
	• **AC** - 활성 및 내부 인터페이스의 결과(연결됨) - 대상 = 네트워크 • **AH** - 활성 및 내부 인터페이스의 결과(연결됨) - 대상 = 호스트만 • **AR** - 활성 및 RIP를 통해 학습됨 • **AS** - 활성 및 정적 • **S** - 비활성(이 경로의 메트릭이 더 높기 때문에) 및 정적 • **O1**—OSPF 외부 유형-1 • **O2**—OSPF 외부 유형-2 • **Oi** - OSPF 영역 내 • **Oo** - OSPF 영역 간
기간	라우팅 테이블에 있는 경로 항목의 사용 기간입니다. 정적 경로에는 연령이 없습니다.
상호 작용	다음 홉에 도달하는 데 사용할 가상 라우터의 이그레스(Egress) 인터페이스입니다.
새로 고침	테이블의 런타임 통계를 새로 고치려면 클릭하십시오.

포워딩 테이블

방화벽은 경로 테이블*(RIB)*에서 대상 네트워크로 향하는 최상의 경로를 선택하여 *FIB*에 배치합니다.

주소 패밀리 표시	**IPv4** 전용, **IPv6** 전용 또는 **IPv4** 및 **IPv6**(기본값)을 선택하여 표시할 라우팅 테이블을 제어합니다.
데스티네이션	라우팅 테이블에서 선택한 가상 라우터가 도달할 수 있는 네트워크에 대한 최상의 IPv4 주소 및 넷마스크 또는 IPv6 주소 및 프리픽스 길이.
다음 홉	대상 네트워크를 향한 다음 홉에 있는 디바이스의 IP 주소입니다. 0.0.0.0의 다음 홉은 기본 경로를 나타냅니다.
플래그	• **u** - 경로가 시작되었습니다. • **h** - 경로는 호스트입니다. • **g** - 경로가 게이트웨이입니다. • **e** - 방화벽이 ECMP(Equal Cost Multipath)를 사용하여 이 경로를 선택했습니다.

런타임 통계	설명
	• ***** - 경로는 대상 네트워크에 대한 기본 경로입니다.
상호 작용	가상 라우터가 다음 홉에 도달하는 데 사용할 이그레스(Egress) 인터페이스입니다.
MTU	최대 전송 단위(MTU); 방화벽이 단일 TCP 패킷에서 이 대상으로 전송할 최대 바이트 수입니다.
새로 고침	테이블의 런타임 통계를 새로 고치려면 클릭하십시오.
정적 경로 모니터링	
데스티네이션	가상 라우터가 도달할 수 있는 네트워크의 IPv4 주소 및 넷마스크 또는 IPv6 주소 및 프리픽스 길이.
다음 홉	대상 네트워크를 향한 다음 홉에 있는 디바이스의 IP 주소입니다. 0.0.0.0의 다음 홉은 기본 경로를 나타냅니다.
미터법	경로에 대한 측정 항목입니다. 동일한 대상 네트워크에 대한 정적 경로가 둘 이상 있는 경우 방화벽은 메트릭 값이 가장 낮은 경로를 선호합니다.
무게	경로의 가중치입니다.
플래그	• **A?B** - BGP를 통해 활성 및 학습됨 • **AC** - 활성 및 내부 인터페이스의 결과(연결됨) - 대상 = 네트워크 • **AH** - 활성 및 내부 인터페이스의 결과(연결됨) - 대상 = 호스트만 • **AR** - 활성 및 RIP를 통해 학습됨 • **AS** - 활성 및 정적 • **S** - 비활성(이 경로의 메트릭이 더 높기 때문에) 및 정적 • **O1**—OSPF 외부 유형-1 • **O2**—OSPF 외부 유형-2 • **Oi** - OSPF 영역 내 • **Oo** - OSPF 영역 간
상호 작용	다음 홉에 도달하는 데 사용할 가상 라우터의 이그레스(Egress) 인터페이스입니다.
경로 모니터링(Fail On)	이 고정 경로에 대해 경로 모니터링이 활성화된 경우 Fail On은 다음을 나타냅니다.

런타임 통계	설명
	• 모두 - 방화벽은 정적 경로가 다운된 것으로 간주하고 정적 경로에 대해 모니터링되는 모든 대상이 다운된 경우 페일오버합니다. • 모두 - 방화벽은 고정 경로가 다운된 것으로 간주하고 고정 경로에 대해 모니터링되는 대상 중 하나라도 다운되면 페일오버합니다. 고정 경로 경로 모니터링이 비활성화된 경우 Fail On은 비활성화됨을 나타냅니다.
상태	모니터링 대상에 대한 ICMP ping을 기반으로 하는 정적 경로의 상태: 고정 경로에 대한 **Up**, **Down** 또는 경로 모니터링은 **Disabled**입니다.
새로 고침	테이블의 런타임 통계를 새로 고칩니다.

RIP 탭

다음 표는 가상 라우터의 RIP에 대한 런타임 통계를 설명합니다.

RIP 런타임 통계	설명
요약 탭	
인터벌 초	인터벌의 초 수입니다. RIP는 이 값(시간 길이)을 사용하여 업데이트, 만료 및 삭제 인터벌을 제어합니다.
업데이트 인터벌	가상 라우터가 피어에게 보내는 RIP 경로 알림 업데이트 사이의 인터벌 수입니다.
만료 인터벌	가상 라우터가 피어로부터 수신한 마지막 업데이트 이후 인터벌의 수입니다. 이후 가상 라우터는 피어의 경로를 사용할 수 없는 것으로 표시합니다.
인터벌 삭제	업데이트가 수신되지 않으면 방화벽이 라우팅 테이블에서 경로를 삭제하는 경로를 사용할 수 없는 것으로 표시한 후의 인터벌 수입니다.
인터페이스 탭	
주소	RIP가 활성화된 가상 라우터에 있는 인터페이스의 IP 주소입니다.
인증 유형	인증 유형: 단순 암호, MD5 또는 없음.
발신 허용	확인 표시는 이 인터페이스가 RIP 패킷을 보낼 수 있음을 나타냅니다.

RIP 런타임 통계	설명
수신 허용	확인 표시는 이 인터페이스가 RIP 패킷을 수신할 수 있음을 나타냅니다.
기본 경로 광고	확인 표시는 RIP가 해당 피어에 기본 경로를 알릴 것임을 나타냅니다.
기본 경로 측정 항목	기본 경로에 할당된 메트릭(홉 수)입니다. 메트릭 값이 낮을수록 기본 경로로 선택할 경로 테이블에서 더 높은 우선 순위를 갖습니다.
키 ID	피어와 함께 사용되는 인증 키입니다.
선호	인증을 위한 기본 키입니다.
피어 탭	
피어 주소	가상 라우터의 RIP 인터페이스에 대한 피어의 IP 주소입니다.
마지막 업데이트	이 피어로부터 마지막 업데이트를 받은 날짜 및 시간입니다.
RIP 버전	피어가 실행 중인 RIP 버전입니다.
잘못된 패킷	이 피어에서 수신한 잘못된 패킷 수입니다. 방화벽이 RIP 패킷을 구문 분석할 수 없는 가능한 원인: 경로 경계를 넘는 x 바이트, 패킷에 너무 많은 경로, 잘못된 서브넷, 잘못된 주소, 인증 실패 또는 메모리 부족.
잘못된 경로	이 피어로부터 수신된 잘못된 경로의 수입니다. 가능한 원인: 경로가 잘못되었거나 가져오기가 실패하거나 메모리가 충분하지 않습니다.

BGP 탭

다음 표는 가상 라우터의 BGP에 대한 런타임 통계를 설명합니다.

BGP 런타임 통계	설명
요약 탭	
라우터 ID	BGP 인스턴스에 할당된 라우터 ID입니다.
기본 경로 거부	Reject Default Route 옵션이 구성되어 있는지의 여부를 나타냅니다. 이 옵션으로 인해 VR은 BGP 피어에서 보급한 기본 경로를 무시합니다.
기본 경로 재배포	기본 경로 재배포 허용 옵션이 구성되었는지의 여부를 나타냅니다.

BGP 런타임 통계	설명
경로 설치	VR이 전역 라우팅 테이블에 BGP 경로를 설치하도록 하는 Install Route 옵션이 구성되었는지의 여부를 나타냅니다.
정상 재시작	Graceful Restart가 활성화되었는지의 여부를 나타냅니다(지원).
AS 사이즈	선택한 AS 형식 크기가 2바이트인지 4바이트인지 나타냅니다.
로컬 AS	VR이 속한 AS의 번호입니다.
로컬 멤버 AS	로컬 멤버 AS 번호(VR이 연합에 있는 경우에만 유효). VR이 연합에 없는 경우 필드는 0입니다.
클러스터 ID	구성된 리플렉터 클러스터 ID를 표시합니다.
기본 로컬 기본 설정	VR에 대해 구성된 기본 로컬 기본 설정을 표시합니다.
항상 MED 비교	항상 비교 MED 옵션이 구성되어 있는지의 여부를 나타냅니다. 이 옵션을 사용하면 서로 다른 자율 시스템의 인접 경로 중에서 선택할 수 있습니다.
MED에 관계없이 통합	라우트에 다른 MED 값이 있는 경우에도 라우트 통합를 활성화하는 Aggregate MED 옵션이 구성되었는지의 여부를 나타냅니다.
결정적 MED 처리	결정적 MED 비교 옵션이 구성되어 있는지의 여부를 나타냅니다. 이 옵션을 사용하면 IBGP 피어(동일한 AS의 BGP 피어)가 보급한 경로 간에 비교할 수 있습니다.
현재 RIB 출력 항목	RIB 출력 테이블의 항목 수입니다.
피크 RIB 출력 항목	한 번에 할당된 Adj-RIB-Out 경로의 최대 수입니다.
피어 탭	
이름	피어의 이름입니다.
그룹	이 피어가 속한 피어 그룹의 이름입니다.
로컬 IP	VR에 있는 BGP 인터페이스의 IP 주소입니다.
피어 IP	피어의 IP 주소입니다.
피어 AS	피어가 속한 자율 시스템.

BGP 런타임 통계	설명
비밀번호 설정	예 또는 아니오는 인증 설정 여부를 나타냅니다.
상태	활성, 연결, 설정됨, 유휴, OpenConfirm 또는 OpenSent와 같은 피어의 상태입니다.
상태 지속 시간(초)	피어 상태의 기간입니다.
피어 그룹 탭	
그룹 이름	피어 그룹의 이름입니다.
유형	EBGP 또는 IBGP와 같이 구성된 피어 그룹 유형입니다.
통합 Confed. AS	예 또는 아니오는 Aggregate Confederation AS 옵션이 구성되었는지의 여부를 나타냅니다.
소프트 리셋 지원	예 또는 아니오는 피어 그룹이 소프트 리셋을 지원하는지의 여부를 나타냅니다. BGP 피어 변경으로 정책을 라우팅할 때 라우팅 테이블 업데이트가 영향을 받을 수 있습니다. 소프트 리셋을 사용하면 BGP 세션을 지우지 않고도 라우팅 테이블을 업데이트할 수 있기 때문에 BGP 세션의 소프트 리셋이 하드 리셋보다 선호됩니다.
다음 홉 셀프	예 또는 아니오는 이 옵션이 구성되었는지의 여부를 나타냅니다.
다음 홉 타사	예 또는 아니오는 이 옵션이 구성되었는지의 여부를 나타냅니다.
비공개 AS 제거	업데이트가 전송되기 전에 AS_PATH 속성에서 제거된 개인 AS 번호가 업데이트에 포함되는지의 여부를 나타냅니다.
로컬 RIB 탭	
프리픽스	Local Routing Information Base의 네트워크 프리픽스 및 서브넷 마스크.
깃발	*는 경로가 최상의 BGP 경로로 선택되었음을 나타냅니다.
다음 홉	프리픽스를 향한 다음 홉의 IP 주소입니다.
피어	피어의 이름입니다.
무게	프리픽스에 할당된 가중치 속성입니다. 방화벽에 동일한 프리픽스에 대한 경로가 두 개 이상 있는 경우 가중치가 가장 높은 경로가 IP 라우팅 테이블에 설치됩니다.

BGP 런타임 통계	설명
로컬 선호	여러 출구 지점이 있는 경우 프리픽스를 향한 출구 지점을 선택하는 데 사용되는 경로에 대한 로컬 기본 설정 속성입니다. 높은 지역 선호도가 낮은 지역 선호도보다 선호됩니다.
AS 경로	Prefix 네트워크 경로에 있는 자율 시스템 목록. 목록은 BGP 업데이트에서 알립니다.
출처	프리픽스에 대한 출처 속성. BGP가 경로를 알게 된 방법.
MED	경로의 MED(Multi-Exit Discriminator) 속성입니다. MED는 경로를 광고하는 AS가 외부 AS에 제안하는 경로에 대한 메트릭 속성입니다. 낮은 MED가 높은 MED보다 선호됩니다.
플랩 수	경로의 플랩 수입니다.
RIB 출력 탭	
프리픽스	라우팅 정보 베이스의 네트워크 라우팅 항목입니다.
다음 홉	프리픽스를 향한 다음 홉의 IP 주소입니다.
피어	VR이 이 경로를 광고할 피어입니다.
로컬 선호	프리픽스에 액세스하기 위한 로컬 기본 설정 속성으로, 출구 지점이 여러 개인 경우 프리픽스를 향한 출구 지점을 선택하는 데 사용됩니다. 높은 지역 선호도가 낮은 지역 선호도보다 선호됩니다.
AS 경로	Prefix 네트워크 경로에 있는 자율 시스템 목록입니다.
출처	프리픽스에 대한 출처 속성. BGP가 경로를 알게 된 방법.
MED	프리픽스에 대한 MED(Multi-Exit Discriminator) 속성입니다. MED는 경로를 광고하는 AS가 외부 AS에 제안하는 경로에 대한 메트릭 속성입니다. 낮은 MED가 높은 MED보다 선호됩니다.
Advanced 상태	경로의 공지된 상태입니다.
Aggr. 상태	이 경로가 다른 경로와 통합되는지의 여부를 나타냅니다.

멀티캐스트 탭

다음 표는 IP 멀티캐스트에 대한 가상 라우터의 런타임 통계를 설명합니다.

멀티캐스트 런타임 통계	설명
FIB 탭	
그룹	포워딩 정보 베이스(FIB)의 경로 입력 가상 라우터가 패킷을 포워딩할 멀티캐스트 그룹 주소입니다.
소스	그룹에 대한 멀티캐스트 패킷의 소스 주소입니다.
수신 인터페이스	그룹에 대한 멀티캐스트 패킷이 도착하는 인터페이스입니다.
나가는 인터페이스	가상 라우터가 그룹에 대한 멀티캐스트 패킷을 포워딩하는 인터페이스입니다.
IGMP 인터페이스 탭	
상호 작용	IGMP가 활성화된 인터페이스입니다.
버전	가상 라우터에서 실행되는 IGMP(Internet Group Management Protocol) 버전 1, 2 또는 3.
쿼리어(Querier)	인터페이스에 연결된 다중 액세스 세그먼트에 있는 IGMP 쿼리어(Querier)의 IP 주소입니다.
쿼리어(Querier) 가동 시간	IGMP 쿼리어(Querier)가 가동된 시간(초)입니다.
쿼리어(Querier) 만료 시간	기타 쿼리어(Querier) 존재 타이머가 만료되기 전에 남은 시간(초)입니다.
항내성	IGMP 인터페이스의 항내성 변수입니다.
그룹 제한	IGMP가 동시에 처리할 수 있는 인터페이스당 최대 그룹 수입니다.
소스 제한	IGMP가 동시에 처리할 수 있는 인터페이스당 최대 소스 수입니다.
즉시 중단(Immediate Leave)	예 또는 아니오는 즉시 중단(Immediate Leave)이 구성되었는지의 여부를 나타냅니다. Immediate Leave는 가상 라우터가 인터페이스 IGMP 그룹별 쿼리를 전송하지 않고 포워딩 테이블 항목에서 인터페이스를 제거함을 나타냅니다.
IGMP 멤버십 탭	
상호 작용	그룹에 속한 인터페이스의 이름입니다.

멀티캐스트 런타임 통계	설명
그룹	인터페이스가 속한 멀티캐스트 그룹의 주소입니다.
소스	그룹에 멀티캐스트 패킷을 보내는 소스의 IP 주소입니다.
가동 시간	이 멤버십이 유지된 시간(초)입니다.
만료 시간	멤버십이 만료되기까지 남은 시간(초)입니다.
필터 모드	출처를 포함하거나 제외합니다. 가상 라우터는 모든 트래픽을 포함하거나 이 소스(포함)의 트래픽만 포함하거나 이 소스를 제외한 모든 소스(제외)의 트래픽을 포함하도록 구성됩니다.
만료 제외	인터페이스 제외 상태가 만료되기 전에 남은 시간(초)입니다.
V1 호스트 타이머	로컬 라우터가 인터페이스에 연결된 IP 서브넷에 더 이상 IGMP 버전 1 구성원이 없다고 가정할 때까지 남은 시간입니다.
V2 호스트 타이머	로컬 라우터가 인터페이스에 연결된 IP 서브넷에 더 이상 IGMP 버전 2 구성원이 없다고 가정할 때까지 남은 시간입니다.
PIM 그룹 매핑 탭	
그룹	Rendezvous Point에 매핑된 그룹의 IP 주소입니다.
RP	그룹에 대한 Rendezvous Point의 IP 주소입니다.
원점	가상 라우터가 RP를 알게 된 위치를 나타냅니다.
PIM 모드	ASM 또는 SSM.
비활성	RP에 대한 그룹 매핑이 비활성화되었는지의 여부를 나타냅니다.
PIM 인터페이스 탭	
상호 작용	PIM에 참여하는 인터페이스의 이름입니다.
주소	인터페이스의 IP 주소입니다.
DR	인터페이스에 연결된 다중 액세스 세그먼트에 있는 지정 라우터의 IP 주소입니다.

멀티캐스트 런타임 통계	설명
헬로 인터벌	헬로 인터벌이 구성되었습니다(초).
조인/정리 인터벌	Join 및 Prune 메시지에 대해 구성된 인터벌(초)입니다.
어설션 인터벌	가상 라우터가 Assert 메시지를 보내도록 구성된 PIM Assert 인터벌(초)입니다. PIM은 Assert 메커니즘을 사용하여 다중 액세스 네트워크에 대한 PIM 포워딩자 선택을 시작합니다.
재해 복구 우선 순위	인터페이스에 연결된 다중 액세스 세그먼트의 지정 라우터에 대해 구성된 우선 순위입니다.
BSR 경계	예 또는 아니오는 인터페이스가 엔터프라이즈 LAN 경계에 위치한 부트스트랩 라우터(BSR)인 가상 라우터에 있는지의 여부를 나타냅니다.
PIM 이웃 탭	
상호 작용	가상 라우터의 인터페이스 이름입니다.
주소	인터페이스에서 연결할 수 있는 PIM 인접 항목의 IP 주소입니다.
보조 주소	인터페이스에서 연결할 수 있는 PIM 인접 항목의 보조 IP 주소입니다.
가동 시간	이웃이 가동된 시간입니다.
만료 시간	가상 라우터가 인접 항목에서 헬로 패킷을 수신하지 않기 때문에 인접 항목이 만료되기까지 남은 시간입니다.
세대 ID	인터페이스에서 PIM 포워딩이 시작되거나 다시 시작될 때마다 다시 생성되는 무작위로 생성된 32비트 값(라우터 자체가 다시 시작되는 경우 포함).
재해 복구 우선 순위	가상 라우터가 이 이웃으로부터 마지막 PIM 헬로 메시지에서 수신한 지정된 라우터 우선 순위입니다.

BFD 요약 정보 탭

BFD 요약 정보에는 다음 데이터가 포함됩니다.

BFD 요약 정보 런타임 통계	설명
상호 작용	BFD를 실행하는 인터페이스입니다.
프로토콜	인터페이스에서 BFD를 실행하는 정적 경로(고정 경로의 IP 주소 제품군) 또는 동적 라우팅 프로토콜.
로컬 IP 주소	BFD를 구성한 인터페이스의 IP 주소입니다.
이웃 IP 주소	BFD 이웃의 IP 주소입니다.
상태	로컬 및 원격 BFD 피어의 BFD 상태: **admin down**, **down**, **init** 또는 **up**.
가동 시간	BFD가 작동된 시간(시, 분, 초 및 밀리초)입니다.
판별자(로컬)	로컬 BFD 피어에 대한 판별자. 판별자는 피어가 여러 BFD 세션을 구별하는 데 사용하는 고유한 0이 아닌 값입니다.
판별기(원격)	원격 BFD 피어에 대한 판별자.
오류	BFD 오류 수입니다.
세션 세부 정보	로컬 및 원격 이웃의 IP 주소, 마지막으로 수신한 원격 진단 코드, 송수신된 제어 패킷 수, 오류 수, 상태 변경을 일으키는 마지막 패킷 등에 대한 정보와 같은 세션에 대한 BFD 정보를 보려면 자세히를 클릭합니다.

논리적 라우터에 대한 추가 런타임 통계

논리적 라우터에 대한 고정 경로 또는 라우팅 프로토콜을 구성한 후 네트워크 > 논리적 라우터를 선택하고 마지막 항목에서 **More Runtime Stats**를 선택합니다. 열에서 라우팅 테이블, 전달 테이블, 구성한 라우팅 프로토콜 및 고정 경로와 같은 논리적 라우터에 대한 자세한 정보를 볼 수 있습니다. 이러한 창은 논리적 라우터의 단일 화면에 표시할 수 있는 것보다 더 많은 정보를 제공합니다. 창에는 다음 탭이 표시됩니다.

- 라우팅(논리적 라우터에 대한 통계)
- BGP(논리적 라우터에 대한 통계)

논리적 라우터에 대한 라우팅 통계

- 네트워크 > 라우팅 > 논리적 라우터 > 추가 런타임 통계

다음 표는 라우팅 테이블, 포워딩 테이블 및 정적 라우팅 모니터링 테이블에 대한 논리적 라우터의 런타임 통계를 설명합니다.

런타임 통계	설명
라우팅 테이블	
주소 패밀리 표시	**IPv4** 전용, **IPv6** 전용 또는 **IPv4** 및 **IPv6**(기본값)을 선택하여 테이블에 표시할 주소 그룹을 제어합니다.
데스티네이션	논리적 라우터가 도달할 수 있는 네트워크의 IPv4 주소 및 넷마스크 또는 IPv6 주소 및 프리픽스 길이.
다음 홉	대상 네트워크를 향한 다음 홉에 있는 디바이스의 IP 주소입니다. 0.0.0.0의 다음 홉은 기본 경로를 나타냅니다.
프로토콜	경로가 고정 또는 연결된 경로이거나 BGP를 통해 학습된 경로임을 나타냅니다.
미터법	경로에 대한 측정 항목입니다. 라우팅 프로토콜에 동일한 대상 네트워크에 대한 경로가 둘 이상 있는 경우 메트릭 값이 가장 낮은 경로를 선호합니다. 각 라우팅 프로토콜은 다른 유형의 메트릭을 사용합니다. 예를 들어, RIP는 홉 수를 사용합니다.
선택됨	활성화된 경우 필드가 true입니다. 비활성화된 경우 비어 있습니다.
기간	라우팅 테이블에 있는 경로 항목의 사용 기간입니다.
활동적인	활성화된 경우 필드가 true입니다. 비활성화된 경우 비어 있습니다.
상호 작용	다음 홉에 도달하는 데 사용되는 논리적 라우터의 이그레스(Egress) 인터페이스입니다.
새로 고침	테이블의 런타임 상태를 새로 고치려면 클릭하십시오.
포워딩 테이블	
방화벽은 경로 테이블*(RIB)*에서 대상 네트워크로 향하는 최상의 경로를 선택하여 *FIB*에 배치합니다.	
데스티네이션	라우팅 테이블에서 선택한 논리적 라우터가 도달할 수 있는 네트워크에 대한 최상의 IPv4 주소 및 넷마스크 또는 IPv6 주소 및 프리픽스 길이.

런타임 통계	설명
다음 홉	대상 네트워크를 향한 다음 홉에 있는 디바이스의 IP 주소입니다. 0.0.0.0의 다음 홉은 기본 경로를 나타냅니다.
MTU	최대 전송 단위(MTU); 방화벽이 단일 TCP 패킷에서 이 대상으로 전송할 최대 바이트 수입니다.
플래그	• **u** - 경로가 시작되었습니다. • **h** - 경로는 호스트입니다. • **g** - 경로가 게이트웨이입니다. • **e** - 방화벽이 ECMP(Equal Cost Multipath)를 사용하여 이 경로를 선택했습니다. • ***** - 경로는 대상 네트워크에 대한 기본 경로입니다.
상호 작용	논리적 라우터가 다음 홉에 도달하는 데 사용할 이그레스(Egress) 인터페이스입니다.
정적 경로 모니터링	
데스티네이션	논리적 라우터가 도달할 수 있는 네트워크의 IPv4 주소 및 넷마스크 또는 IPv6 주소 및 프리픽스 길이.
다음 홉	대상 네트워크를 향한 다음 홉에 있는 디바이스의 IP 주소입니다. 0.0.0.0의 다음 홉은 기본 경로를 나타냅니다.
미터법	경로에 대한 측정 항목입니다. 동일한 대상 네트워크에 대한 정적 경로가 둘 이상 있는 경우 방화벽은 메트릭 값이 가장 낮은 경로를 선호합니다.
상호 작용	다음 홉에 도달하는 데 사용되는 논리적 라우터의 이그레스(Egress) 인터페이스입니다.
경로 모니터링(Fail On)	이 고정 경로에 대해 경로 모니터링이 활성화된 경우 Fail On은 다음을 나타냅니다. • 모두 - 방화벽은 정적 경로가 다운된 것으로 간주하고 정적 경로에 대해 모니터링되는 모든 대상이 다운된 경우 페일오버합니다. • 모두 - 방화벽은 고정 경로가 다운된 것으로 간주하고 고정 경로에 대해 모니터링되는 대상 중 하나라도 다운되면 페일오버합니다.

런타임 통계	설명
	고정 경로 경로 모니터링이 비활성화된 경우 Fail On은 비활성화됨을 나타냅니다.
상태	모니터링 대상에 대한 ICMP ping을 기반으로 하는 정적 경로의 상태: 고정 경로에 대한 **Up**, **Down** 또는 경로 모니터링은 **Disabled**입니다.
새로 고침	테이블의 런타임 통계를 새로 고칩니다.

논리적 라우터에 대한 **BGP** 통계

다음 표는 논리적 라우터의 BGP에 대한 런타임 통계를 설명합니다.

BGP 런타임 통계	설명
요약 탭	
활성화됨	BGP 활성화됨: 예 또는 아니오.
라우터 ID	논리적 라우터의 라우터 ID입니다.
로컬 AS	논리적 라우터가 속한 AS.
첫 번째 AS 시행	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
빠른 외부 페일오버	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
기본 로컬 기본 설정	기본 로컬 기본 설정이 구성되었습니다.
정상 재시작	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
최대 피어 재시작 시간(초)	Graceful Restart 최대 피어 다시 시작 시간에 대해 구성된 시간(초)입니다.
오래된 경로 시간(초)	Graceful Restart 오래된 경로 시간에 대해 구성된 시간(초)입니다.

BGP 런타임 통계	설명
항상 MED 비교	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
결정적 MED 비교	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
피어 탭	
이름	피어의 이름입니다.
피어 그룹	이 피어가 속한 피어 그룹의 이름입니다.
로컬 IP	논리적 라우터에 있는 BGP 인터페이스의 IP 주소입니다.
로컬 AS	로컬 BGP 방화벽이 속한 AS입니다.
피어 IP	피어의 IP 주소입니다.
원격 AS	피어가 속한 AS입니다.
위/아래	피어가 위 또는 아래입니다.
상태	이 연결되었습니까?
피어 그룹 탭	
이름	피어 그룹의 이름입니다.
유형	ebgp 또는 ibgp와 같이 구성된 피어 그룹 유형입니다.
연결 유지(초)	연결 유지 시간(초).
유지 시간(초)	시간을 초 단위로 유지합니다.
IP	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
IPv6	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
최소 경로 인터벌(초)	최소 경로 인터벌(초)입니다.

BGP 런타임 통계	설명
유니캐스트	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
경로	
이름	라우팅 테이블의 IPv4 또는 IPv6 경로: IPv4 또는 IPv6 주소 및 프리픽스 길이.
AS 경로	경로의 다음 AS.
최적의 경로	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
MED	0 또는 공백
미터법	0 또는 공백
네트워크	
다음 홉	경로(이름)로 식별된 네트워크에 도달하기 위한 다음 홉의 IP 주소입니다.
출처	경로의 출처: IGP 또는 불완전
경로	경로의 다음 AS입니다.
경로 시작	외부를 나타냅니다.
피어 이름	
프리픽스	
프리픽스 길이	
유효	필드는 활성화된 경우 true이고 활성화되지 않은 경우 비어 있습니다.
무게	경로의 가중치입니다.

네트워크 > 라우팅 > 논리적 라우터

방화벽은 수동으로 정의한 고정 경로를 사용하거나 레이어 3 라우팅 프로토콜(동적 경로)에 참여하여 다른 서브넷에 대한 경로를 얻기 위해 논리적 라우터가 필요합니다. 방화벽에 정의된 각 Layer 3 인터페이스, 루프백 인터페이스 및 VLAN 인터페이스는 논리적 라우터와 연결되어야 합니다. 각 인터페이스는 하나의 논리적 라우터에만 속할 수 있습니다.

논리적 라우터는 **Device** > **Setup** > **Management**의 일반 설정에서 **Advanced** 라우팅을 활성화한 다음 방화벽을 커밋하고 재부팅하면 사용할 수 있습니다.

논리적 라우터를 정의하려면 논리적 라우터에 레이어 3 인터페이스를 추가하고 네트워크에서 요구하는 대로 정적 경로와 동적 라우팅 프로토콜의 조합을 구성해야 합니다. ECMP 및 BFD와 같은 다른 기능을 구성할 수도 있습니다.

무엇을 찾고 계신가요?	참조
논리적 라우터의 필수 요소	논리적 라우터 일반 설정
구성:	정적 경로 필터 OSPF OSPF 라우팅 프로파일 OSPFv3 OSPFv3 라우팅 프로파일 BGP BGP 라우팅 프로파일 멀티캐스트 멀티캐스트 라우팅 프로파일 RIPv2 RIPv2 라우팅 프로파일 BFD 라우팅 프로파일
논리적 라우터에 대한 정보를 봅니다.	논리적 라우터에 대한 추가 런타임 통계

네트워크 > 라우팅 > 논리적 라우터 > 일반

고급 라우팅(디바이스 > 설정 > 관리)을 활성화하면 방화벽은 정적 및 동적 라우팅에 논리적 라우터를 사용합니다. 논리적 라우터를 사용하려면 다음 표에 설명된 대로 이름과 레이어 3 인터페이스를 할당해야 합니다.

논리적 라우터에 대해 ECMP(Equal Cost Multiple Path)를 선택적으로 구성할 수 있습니다. ECMP 처리는 방화벽이 동일한 대상에 대해 최대 4개의 동일한 비용 경로를 사용할 수 있도록 하는 네트워킹 기능입니다. 이 기능이 없으면 동일한 대상에 대한 동일한 비용 경로가 여러 개 있는 경우 가상 라우터는 라우팅 테이블에서 해당 경로 중 하나를 선택하여 포워딩 테이블에 추가합니다. 선택한 경로에 문제가 발생하지 않는 한 다른 경로를 사용하지 않습니다. 가상 라우터에서 ECMP 기능을 활성화하면 방화벽이 포워딩 테이블의 대상에 대해 최대 4개의 동일한 비용 경로를 가질 수 있으므로 방화벽이 다음을 수행할 수 있습니다.

- 로드 밸런싱 플로우(세션)는 여러 동일한 비용 링크를 통해 동일한 대상으로 이동합니다.
- 일부 링크를 사용하지 않는 상태로 두지 말고 동일한 대상에 대한 모든 링크에서 사용 가능한 대역폭을 사용하십시오.
- 라우팅 프로토콜이나 RIB 테이블이 대체 경로를 선택할 때까지 기다리지 않고 링크가 실패할 경우 다른 ECMP 멤버로의 트래픽을 동일한 대상으로 동적으로 이동하여 링크 실패 시 다운타임을 줄이는 데 도움이 될 수 있습니다.

ECMP 로드 밸런싱은 패킷 수준이 아니라 세션 수준에서 수행됩니다. 이는 방화벽이 패킷을 수신할 때마다가 아니라 새 세션이 시작될 때 동일한 비용 경로를 선택함을 의미합니다.

논리적 라우터 일반 설정	설명
이름	논리적 라우터를 설명하는 이름을 지정합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 하이픈 및 밑줄만 사용합니다.
상호 작용	
상호 작용	논리적 라우터에 포함할 레이어 3 인터페이스를 추가합니다. 이러한 인터페이스는 논리적 라우터의 라우팅 테이블에서 나가는 인터페이스로 사용할 수 있습니다. 인터페이스 유형을 지정하려면 네트워크 > 인터페이스를 참조하세요. 논리적 라우터에 인터페이스를 추가하면 연결된 경로가 전역 RIB에 자동으로 추가됩니다.
행정 거리	
고정	범위는 1~255이며, 기본값은 10입니다.

논리적 라우터 일반 설정	설명
정적 IPv6	범위는 1~255이며, 기본값은 10입니다.
OSPF 내부 영역	범위는 1~255이며, 기본값은 110입니다.
OSPF간 영역	범위는 1~255이며, 기본값은 110입니다.
OSPF 외부	범위는 1~255이며, 기본값은 110입니다.
OSPFv3 내부 영역	범위는 1~255이며, 기본값은 110입니다.
OSPFv3 영역 간	범위는 1~255이며, 기본값은 110입니다.
OSPFv3 외부	범위는 1~255이며, 기본값은 110입니다.
BGP AS 내부	범위는 1~255이며, 기본값은 200입니다.
BGP AS 외부	범위는 1~255이며, 기본값은 20입니다.
BGP 로컬 경로	범위는 1~255이며, 기본값은 20입니다.
RIP	범위는 1~255이며, 기본값은 120입니다.
ECMP	
사용	논리적 라우터에 대해 ECMP(Equal-Cost Multiple Path)를 활성화합니다.
대칭 반환	(선택 사항) 대칭 반환을 선택하여 반환 패킷이 연결된 수신 패킷이 도착한 동일한 인터페이스로 나가게 합니다. 즉, 방화벽은 ECMP 인터페이스를 사용하지 않고 반환 패킷을 보낼 수신 인터페이스를 사용하므로 대칭 반환 설정이 로드 밸런싱을 재정의합니다. 이 동작은 서버에서 클라이언트로의 트래픽 플로우에 대해서만 발생합니다.
엄격한 소스 경로	기본적으로 방화벽에서 발생하는 IKE 및 IPSec 트래픽은 ECMP 로드 밸런싱 방법이 결정하는 인터페이스를 송신합니다. 방화벽에서 시작되는 IKE 및 IPSec 트래픽이 항상 IPSec 터널의 소스 IP 주소가 속한 물리적 인터페이스를 빠져나가도록 하려면 엄격한 소스 경로를 선택합니다. 방화벽에 동일한 대상에 대해 동일한 비용 경로를 제공하는 둘 이상의 ISP가 있는 경우 엄격한 소스 경로를 활성화합니다. ISP는 일반적으로 RPF(Reverse Path Forwarding) 검사(또는 IP 주소 스푸핑을 방지하기 위한 다른 검사)를 수행하여 트래픽이 도착한 동일한 인터페이스에서 나가는지 확인합니다. 기본적으로 ECMP는 소스 인터페이스를 이

논리적 라우터 일반 설정	설명
	그레스(egress) 인터페이스로 선택하는 대신 구성된 ECMP 방법을 기반으로 이그레스(egress) 인터페이스를 선택하기 때문에 이는 ISP가 기대하는 것이 아니며 ISP가 합법적인 반환 트래픽을 차단할 수 있습니다. 이 사용 사례에서는 방화벽이 IPSec 터널의 소스 IP 주소가 속한 인터페이스인 이그레스(egress) 인터페이스를 사용하도록 Strict Source Path를 활성화합니다.
최대 경로	동일한 비용 경로의 최대 수를 입력합니다. (2, 3 또는 4) RIB에서 FIB로 복사할 수 있는 대상 네트워크에 연결합니다. 기본값은 2입니다.

로드 밸런싱 방식	가상 라우터에서 사용할 다음 ECMP 로드 밸런싱 알고리즘 중 하나를 선택합니다. ECMP 로드 밸런싱은 패킷 수준이 아니라 세션 수준에서 수행됩니다. 즉, 방화벽(ECMP)은 패킷을 수신할 때마다가 아니라 새 세션이 시작될 때 동일한 비용 경로를 선택합니다.
	• **IP Modulo** - 기본적으로 가상 라우터는 패킷 헤더에 있는 소스 및 대상 IP 주소의 해시를 사용하여 사용할 ECMP 경로를 결정하는 이 옵션을 사용하여 세션 부하를 분산합니다.
	• **IP** 해시 - 사용할 ECMP 경로를 결정하는 두 가지 IP 해시 방법이 있습니다.
	  • **IP** 해시를 선택하면 기본적으로 방화벽은 소스 및 대상 IP 주소의 해시를 사용합니다.
	  • 또는 소스 주소만 사용(PAN-OS 8.0.3 이상 릴리스에서 사용 가능)을 선택할 수 있습니다. 이 IP 해시 방법은 동일한 소스 IP 주소에 속한 모든 세션이 항상 동일한 경로를 사용하도록 합니다.
	  • 선택적으로 소스/대상 포트 사용을 선택하여 해시 계산에 포트를 포함합니다. 또한 해시 시드 값(정수)을 입력하여 로드 밸런싱을 추가로 무작위화할 수 있습니다.
	• 가중 라운드 로빈 - 이 알고리즘은 다양한 링크 용량과 속도를 고려하는 데 사용할 수 있습니다. 이 알고리즘을 선택하면 인터페이스 창이 열립니다. 추가를 클릭하고 가중치 기반 라운드 로빈 그룹에 포함할 인터페이스를 선택합니다. 각 인터페이스에 대해 해당 인터페이스에 사용할 가중치를 입력합니다. 가중치 기본값은 100입니다. 범위는 1-255입니다. 특정 동일 비용 경로에 대한 가중치가 높을수록 새 세션에 대해 동일한 비용 경로가 더 자주 선택됩니다. 더 많은 ECMP 트래픽이 더 빠른 링크를 통과하도록 더 높은 속도의 링크에 느린 링크보다 더 높은 가중치를 부여해야 합니다. 추가를 다시 클릭하여 다른 인터페이스와 가중치를 추가합니다.

논리적 라우터 일반 설정	설명
	• 균형 라운드 로빈 - 들어오는 ECMP 세션을 링크에 균등하게 분배합니다.
RIB 필터	
IPv4 - BGP 경로 맵	재배포 경로 맵을 선택하거나 새 맵을 만들어 전역 RIB에 추가되는 IPv4 BGP 경로를 제어합니다. 기본값은 없음입니다.
IPv4 - OSPFv2 경로 맵	재배포 경로 맵을 선택하거나 전역 RIB에 추가되는 IPv4 OSPFv2 경로를 제어하는 새 맵을 만듭니다. 기본값은 없음입니다.
IPv4 - 정적 경로 맵	재배포 경로 맵을 선택하거나 전역 RIB에 추가되는 IPv4 정적 경로를 제어하는 새 맵을 만듭니다. 기본값은 없음입니다.
IPv4 - RIP 경로 맵	재배포 경로 맵을 선택하거나 전역 RIB에 추가되는 RIP 경로를 제어하는 새 맵을 만듭니다. 기본값은 없음입니다.
IPv6 - BGP 경로 맵	재배포 경로 맵을 선택하거나 새 맵을 만들어 전역 RIB에 추가되는 IPv6 BGP 경로를 제어합니다. 기본값은 없음입니다.
IPv6 - OSPFv3 경로 맵	재배포 경로 맵을 선택하거나 전역 RIB에 추가되는 IPv6 OSPFv3 경로를 제어하는 새 맵을 만듭니다. 기본값은 없음입니다.
IPv6 - 정적 경로 맵	재배포 경로 맵을 선택하거나 새 맵을 만들어 전역 RIB에 추가되는 IPv6 정적 경로를 제어합니다. 기본값은 없음입니다.

네트워크 > 라우팅 > 논리적 라우터 > 정적

선택적으로 Advanced 라우팅 엔진의 논리적 라우터에 대해 하나 이상의 정적 경로를 추가합니다. **IPv4** 또는 **IPv6**을 선택한 다음 IPv4 또는 IPv6 주소를 사용하여 경로를 추가합니다. 일반적으로 기본 경로 구성(0.0.0.0/0)이 필요합니다. 기본 경로는 논리적 라우터의 라우팅 테이블에 없는 대상에 적용됩니다.

정적 경로 설정	설명
이름	고정 경로를 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 하이픈 및 밑줄만 사용합니다.
데스티네이션	CIDR(Classless Inter-domain Routing) 표기법으로 IP 주소와 네트워크 마스크를 입력합니다: *ip_address*/*mask*(예: IPv4의 경우 192.168.2.0/24 또는 IPv6의 경우 2001:db8::/32). 또는 IP 넷마스크 유형의 주소 개체를 만들 수 있습니다.

정적 경로 설정	설명
상호 작용	패킷을 대상으로 전달할 나가는 인터페이스를 선택하거나 다음 홉 설정을 구성하거나 둘 다를 구성합니다. 이 경로의 다음 홉에 대한 경로 테이블의 인터페이스를 사용하는 것보다 방화벽이 사용하는 인터페이스를 보다 엄격하게 제어하려면 인터페이스를 지정하십시오. 기본값은 없음입니다.
다음 홉	다음 중 하나를 선택합니다. • **IP** 주소 또는 **IPv6** 주소 - 다음 홉 라우터의 IP 주소를 입력하거나 / IPv6 넷마스크 유형의 주소 개체를 선택하거나 생성하려면 선택합니다. 주소 개체에는 IPv4의 경우 /32, IPv6의 경우 /128의 넷마스크가 있어야 합니다. IPv6 다음 홉 주소를 사용하려면 인터페이스에서 **IPv6**을 활성화해야 합니다(레이어 3 인터페이스를 구성할 때). • 다음 **LR** - 다음 논리 라우터가 다음 홉이 되도록 선택합니다. • **FQDN** - 다음 홉이 될 정규화된 도메인 이름을 입력합니다. • 삭제 - 이 대상으로 주소가 지정된 트래픽을 삭제하려면 선택합니다. • 없음 - 경로에 대한 다음 홉이 없는 경우 선택합니다. 예를 들어, 지점 간 연결은 패킷이 이동하는 방법이 하나뿐이므로 다음 홉이 필요하지 않습니다.
관리 구역	고정 경로에 대한 관리 거리를 지정합니다(범위는 10~240입니다.
미터법	고정 경로에 대한 유효한 메트릭을 지정하십시오(범위는 1~65,535, 기본값은 10).
BFD 프로파일	BFD 프로파일을 선택하거나 고정 경로에 적용할 새 프로파일을 만듭니다. 기본값은 없음**(BFD** 비활성화**)**입니다.
경로 모니터링	경로 모니터링 구성을 계속하려면 선택합니다.
활성화	고정 경로에 대한 경로 모니터링을 활성화합니다.
실패 조건	방화벽에서 모니터링되는 경로가 다운된 것으로 간주하여 정적 경로가 다운되는 조건을 선택합니다. • 임의 - (기본값) 정적 경로에 대해 모니터링되는 대상 중 하나가 ICMP에 의해 도달할 수 없는 경우 방화벽은 RIB 및 FIB에서 정적 경로를 제거하고 동일한 대상으로 가는 다음으로 가장 낮은 메트릭이 있는 동적 또는 정적 경로를 FIB에 추가합니다. • 모두 - ICMP에서 정적 경로에 대해 모니터링되는 모든 대상에 연결할 수 없는 경우 방화벽은 RIB 및 FIB에서 정적 경로를 제거하고 동일한

정적 경로 설정	설명
	대상으로 이동하는 다음으로 낮은 메트릭을 가진 동적 또는 정적 경로를 FIB에 추가합니다. 예를 들어 모니터링되는 대상이 유지 관리를 위해 단순히 오프라인 상태일 때 모니터링되는 단일 대상이 정적 경로 실패를 알리는 것을 방지하려면 모두를 선택합니다.
선점 대기 시간(분)	다운된 경로 모니터가 작동 상태를 유지해야 하는 시간(분)을 입력하십시오. 경로 모니터는 모든 구성원 모니터링 대상을 평가하고 방화벽이 RIB에 고정 경로를 다시 설치하기 전에 작동 상태를 유지해야 합니다. 링크가 다운되거나 플래핑되지 않고 타이머가 만료되면 링크가 안정적인 것으로 간주되고 경로 모니터가 작동 상태를 유지할 수 있으며 방화벽은 정적 경로를 RIB에 다시 추가할 수 있습니다. 보류 시간 동안 링크가 다운되거나 플랩되면 다운된 모니터가 작동 상태로 돌아갈 때 경로 모니터가 실패하고 타이머가 다시 시작됩니다. **Preemptive Hold Time**이 0이면 방화벽은 경로 모니터가 표시되는 즉시 정적 경로를 RIB로 다시 설치합니다. 범위는 0~1,440입니다. 기본값은 2입니다.
이름	모니터링 대상의 이름을 추가합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 하이픈 및 밑줄만 사용합니다.
사용	고정 경로에 대해 이 특정 대상의 경로 모니터링을 활성화하려면 선택합니다. 방화벽은 ICMP 핑(ping)을 이 대상으로 보냅니다.
소스 IP	모니터링 대상에 대한 ICMP 핑(ping)에서 방화벽이 소스로 사용할 IP 주소를 선택합니다. • 인터페이스에 여러 IP 주소가 있는 경우 하나를 선택합니다. • 인터페이스를 선택하면 방화벽은 기본적으로 인터페이스에 할당된 첫 번째 IP 주소를 사용합니다. • **DHCP(DHCP** 클라이언트 주소 사용**)**를 선택하면 방화벽은 DHCP가 인터페이스에 할당한 주소를 사용합니다. DHCP 주소를 보려면 네트워크 > 인터페이스 > 이더넷을 선택한 다음 이더넷 인터페이스 행에서 동적 **DHCP** 클라이언트를 클릭합니다. IP 주소가 동적 IP 인터페이스 상태 창에 나타납니다. • **PPPOE(PPPoE** 클라이언트 주소 사용**)**
대상 IP	방화벽이 경로를 모니터링할 강력하고 안정적인 IP 주소 또는 주소 개체를 입력합니다. 모니터링되는 대상과 고정 경로 대상은 동일한 주소 패밀리(IPv4 또는 IPv6) 를 사용해야 합니다.

정적 경로 설정	설명
핑(ping) 인터벌(초)	ICMP 핑(ping) 인터벌을 초 단위로 지정하여 방화벽이 경로를 모니터링하는 빈도를 결정합니다(모니터링되는 대상에 대한 핑. 범위는 1~60, 기본값은 3).
핑(ping) 카운트	방화벽이 링크 다운을 고려하기 전에 모니터링 대상에서 반환되지 않는 연속 ICMP 핑(ping) 패킷 수를 지정합니다. **Any** 또는 **All** 실패 조건에 따라 경로 모니터링이 실패 상태인 경우 방화벽은 RIB에서 정적 경로를 제거합니다(범위는 3~10, 기본값은 5). 예를 들어, 핑(ping) 인터벌이 3초이고 Ping Count가 5회 누락된 핑(방화벽은 지난 15초 동안 핑을 수신하지 않음)은 경로 모니터링이 링크 오류를 감지했음을 의미합니다. 경로 모니터링이 실패 상태이고 방화벽이 15초 후에 핑(ping)을 수신하면 링크가 작동된 것으로 간주됩니다. **Any** 또는 **All** 장애 조건을 기반으로 **Any** 또는 **All** 모니터링 대상에 대한 경로 모니터링이 수행된 것으로 간주되고 Preemptive Hold Time이 시작됩니다.

네트워크 > 라우팅 > 논리적 라우터 > OSPF

이 표에서는 고급 라우팅 엔진의 논리적 라우터에 대해 OSPFv2 영역을 구성하는 설정에 대해 설명합니다.

OSPF 설정	설명
사용	논리적 라우터에 대해 OSPF를 사용하도록 설정합니다.
라우터 ID	IPv4 주소 형식으로 라우터 ID를 입력합니다.
BFD 프로파일	OSPF에 양방향 전달 감지를 적용하려면 BFD 프로파일을 선택하거나 새 프로파일을 만듭니다. 기본값은 없음**(BFD** 비활성화**)**입니다.
전역 일반 타이머	전역 타이머 프로파일을 선택하거나 OSPF에 적용할 새 프로파일을 만듭니다.
전역 인터페이스 타이머	OSPF 인터페이스 타이머를 선택하거나 OSPF에 적용할 새 타이머를 만듭니다.
재배포 프로파일	OSPF 재배포 프로파일을 선택하거나 IPv4 정적 경로, 연결된 경로, IPv4 BGP 경로 또는 IPv4 기본 경로를 OSPF 링크 상태 데이터베이스에 재배포할 새 프로파일을 만듭니다.
지역	

OSPF 설정	설명
지역 ID	영역 ID로 식별되는 영역을 x.x.x.x 형식으로 추가합니다. 이것은 각 이웃이 동일한 영역의 일부로 수락해야 하는 식별자입니다.
유형	
입증	인증 프로파일을 선택하거나 새 프로파일을 만듭니다.
유형	OSPF 영역의 유형을 선택합니다. • 일반 - 제한이 없습니다. 이 지역은 모든 유형의 경로를 수행할 수 있습니다. • **Stub** - 해당 지역의 콘센트가 없습니다. 지역 외부의 목적지에 도달하려면 트래픽이 다른 지역에 연결되는 ABR(영역 경계 라우터)을 통과해야 합니다. • **NSSA**(Not-So-Stubby Area) - 트래픽은 OSPF 경로 이외의 경로를 통해서만 해당 영역을 벗어날 수 있습니다.
요약 없음	(스텁 및 NSSA 영역만 해당) 해당 영역이 유형 3 요약 LSA를 수신하지 못하도록 하여 해당 영역의 트래픽을 줄이려면 선택합니다.
기본 정보가 시작됩니다.	(NSSA 영역에만 해당) OSPF가 기본 경로를 시작하도록 하려면 선택합니다.
미터법	(NSSA 영역만 해당) 기본 경로에 대한 메트릭을 입력합니다. 범위는 1~16,777,214이며 기본값은 10입니다.
메트릭 유형	(NSSA 영역에만 해당) 유형 **1** 또는 유형 **2**
ABR	논리적 라우터가 다음 네 개의 필드를 구성할 수 있는 영역 경계 라우터인지 선택합니다.
가져오기 목록	액세스 목록을 선택하거나 새 목록을 만들어 IPv4 원본 주소를 기반으로 영역으로 들어오는 네트워크 경로를 필터링합니다.
내보내기 목록	액세스 목록을 선택하거나 새 목록을 만들어 해당 지역에서 시작된 네트워크 경로를 필터링하여 경로가 다른 영역으로 보급되는 것을 허용하거나 방지합니다.

OSPF 설정	설명
인바운드 필터 목록	접두사 목록을 선택하거나 새 접두사를 만들어 해당 영역으로 들어오는 네트워크 접두사를 필터링합니다.
아웃바운드 필터 목록	접두사 목록을 선택하거나 새 접두사를 만들어 해당 영역에서 시작된 네트워크 접두사를 필터링하여 경로가 다른 영역으로 보급되지 않도록 합니다.
IPv4 접두사	(NSSA 영역에만 해당) **ABR**이 선택되어 있고 영역 유형이 **NSSA**인 경우 IPv4 접두사를 추가하여 외부 서브넷 그룹을 단일 Type-7 LSA로 요약한 다음 광고를 선택할 때 유형-5 LSA로 변환되고 백본에 광고됩니다.
범위	
IP 주소/넷마스크	IP 주소/넷마스크를 추가합니다. 이 범위와 일치하는 라우팅 정보를 갖는 Type-3 요약 LSA(link-state advertisement)는 해당 영역이 이 범위에서 적어도 하나의 영역 내 네트워크(즉, 라우터 또는 네트워크 LSA로 설명됨)를 포함하는 경우 백본 영역으로 공지됩니다.
대체	영역에 지정된 IP 주소/넷마스크에서 하나 이상의 인트라 영역 네트워크가 포함된 경우 이 IP 주소/넷마스크가 있는 유형 3 요약 LSA가 백본에 공지되도록 대체 IPaddress/넷마스크를 입력합니다.
광고	서브넷과 일치하는 LSA를 보내려면 선택합니다.
상호 작용	
상호 작용	영역에 포함할 각 인터페이스를 추가합니다.
사용	인터페이스를 사용하도록 설정합니다.
MTU 무시	인접성을 설정하려고 할 때 MTU(최대 전송 단위) 불일치를 무시하려면 선택합니다(기본값은 사용 안 함). MTU 일치 검사수행). RFC 2328은 인터페이스 MTU를 "조각화 없이 연관된 인터페이스에서 전송할 수 있는 가장 큰 IP 데이터그램의 바이트 크기"로 정의합니다.
수동	인터페이스가 OSPF 패킷을 보내거나 수신하지 못하도록 선택하는 단계입니다. 그러나 인터페이스는 여전히 링크 상태 데이터베이스에 포함되어 있습니다. 예를 들어, 스위치에 연

OSPF 설정	설명
	결하는 경우 라우터가 없는 곳에 Hello 패킷을 보내지 않으려는 경우 인터페이스를 수동으로 만들 수 있습니다.
링크 유형	링크 유형 선택: • 브로드캐스트 - 인터페이스를 통해 액세스할 수 있는 모든 이웃은 이더넷 인터페이스와 같은 OSPF Hello 메시지를 멀티캐스팅하여 자동으로 검색됩니다. • **p2p**(point-to-point) - 자동으로 이웃을 검색합니다. • **p2mp**(point-to-multipoint) - 인접 항목을 수동으로 정의해야 합니다. 이 인터페이스를 통해 연결할 수 있는 모든 인접 이웃에 대한 인접 IP 주소와 각 이웃의 우선 순위를 추가합니다. 범위는 0~255이며 기본값은 1입니다.
우선 사항	인터페이스의 우선 순위를 입력하십시오. 라우터가 지정 라우터(DR) 또는 백업 DR(BDR)로 선택되는 우선 순위 범위는 0~255 사이입니다. 기본값은 1입니다. 0이 구성되면 라우터가 DR 또는 BDR로 선택되지 않습니다.
타이머 프로파일	타이머 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 만듭니다. 이 프로파일은 OSPF에 적용된 전역 인터페이스 타이머 프로파일을 재정의합니다.
입증	인증 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 만듭니다. 이 프로파일은 유형 탭에 적용된 인증 프로파일을 재정의합니다.
BFD 프로파일	BFD 프로필 또는 **Inherit-vr-global-setting**(기본값)을 선택하거나 새 BFD 프로필을 생성하거나 없음**(BFD** 비활성화**)**을 선택합니다. 이 프로파일은 OSPF에 대해 구성된 프로파일을 재정의합니다.
비용	인터페이스에 대한 비용을 지정합니다. 범위는 1~65,535이며 기본값은 10입니다.
가상 링크	
이름	가상 링크의 이름을 입력합니다.
사용	가상 링크를 사용하도록 설정합니다.

OSPF 설정	설명
지역	
라우터 ID	
타이머 프로파일	타이머 프로파일을 선택하거나 가상 링크에 적용할 새 프로파일을 만듭니다. 이 프로파일은 OSPF에 적용된 전역 인터페이스 타이머 프로파일을 재정의합니다.
입증	인증 프로파일을 선택하거나 가상 링크에 적용할 새 프로파일을 만듭니다. 이 프로파일은 유형 탭에 적용된 인증 프로파일을 재정의합니다.
고급	
rfc-1583 호환성	OSPF 라우팅 테이블의 ASBR(자율 시스템 경계 라우터)에 대한 최상의 경로를 허용하는 RFC 1583과의 호환성을 적용하려면 선택합니다. 기본값은 비활성화되며, 이는 OSPF 라우팅 테이블이 라우팅 테이블에서 여러 인트라 AS 경로를 유지할 수 있으므로 라우팅 루프를 방지할 수 있음을 의미합니다.
정상 재시작 - 정상 재시작 사용	논리적 라우터에 대해 정상 재시작을 활성화합니다. 기본값은 활성화되어 있습니다.
도우미 모드 작동	논리적 라우터에 대해 정상 재시작 도우미 모드를 사용하도록 설정합니다. 기본값은 사용입니다.
엄격한 LSA 검사 작동	엄격한 LSA 검사 사용 도우미 라우터가 도우미 모드 수행을 중지하고 링크 상태 알림이 네트워크 토폴로지 변경을 나타내는 경우 정상 재시작 프로세스가 중지되도록 합니다. 기본값은 사용입니다.
유예 기간(초)	방화벽이 다운되거나 사용할 수 없게 될 경우 논리적 라우터가 정상적으로 다시 시작되는 시간(초)을 지정합니다. 범위는 5~1,800이며 기본값은 120입니다.
최대 이웃 재시작 시간(초)	범위는 5~1,800이며 기본값은 140입니다.

네트워크 > 라우팅 > 논리적 라우터 > OSPFv3

이 표에서는 고급 라우팅 엔진의 논리적 라우터에 대해 OSPFv3 영역을 구성하기 위한 설정을 설명합니다.

OSPFv3 설정	설명
사용	논리적 라우터에 대해 OSPFv3을 활성화합니다.
라우터 ID	IPv6 주소 형식으로 라우터 ID를 입력합니다.
BFD 프로파일	OSPF에 양방향 전달 감지를 적용하려면 BFD 프로파일을 선택하거나 새 프로파일을 만듭니다. 기본값은 없음(BFD 비활성화)입니다.
전역 일반 타이머	전역 타이머 프로파일을 선택하거나 OSPFv3에 적용할 새 프로파일을 만듭니다.
전역 인터페이스 타이머	OSPFv3 인터페이스 타이머를 선택하거나 OSPFv3에 적용할 새 타이머를 생성합니다.
재배포 프로파일	OSPFv3 재배포 프로파일을 선택하거나 새로 생성하여 IPv6 고정 경로, 연결된 경로, IPv6 BGP 경로 또는 IPv6 기본 경로를 OSPFv3 링크 상태 데이터베이스에 재배포합니다.
지역	
지역 ID	IPv4 주소 형식의 영역 ID로 식별되는 영역을 추가합니다. 이것은 각 이웃이 동일한 영역의 일부로 수락해야 하는 식별자입니다.
유형	
입증	인증 프로파일을 선택하거나 새 프로파일을 만듭니다.
유형	OSPFv3 영역 유형 선택: • 일반 - 제한이 없습니다. 이 지역은 모든 유형의 경로를 수행할 수 있습니다. • **Stub** - 해당 지역의 콘센트가 없습니다. 지역 외부의 목적지에 도달하려면 트래픽이 다른 지역에 연결되는 ABR(영역 경계 라우터)을 통과해야 합니다. • **NSSA**(Not-So-Stubby-Area) - 트래픽은 OSPFv3 경로 이외의 경로를 통해서만 해당 영역을 벗어날 수 있습니다.

OSPFv3 설정	설명
요약 없음	(스텁 및 NSSA만 해당) 영역이 유형 3 요약 LSA를 수신하지 못하도록 하여 해당 영역의 트래픽을 줄이려면 선택합니다.
기본 정보가 시작됩니다.	(NSSA만 해당) OSPFv3이 기본 경로를 시작하도록 하려면 선택합니다.
미터법	(NSSA만 해당) 기본 경로에 대한 메트릭을 입력합니다. 범위는 1~16,777,214입니다. 기본값은 10입니다.
메트릭 유형	(NSSA만 해당) 유형 **1** 또는 유형 **2**를 선택합니다.
ABR	논리적 라우터가 영역 경계 라우터(영역 0을 포함하여 여러 영역에 인터페이스가 있는 라우터)인 경우 선택하여 다음 4개 필드를 구성할 수 있습니다.
가져오기 목록	액세스 목록을 선택하거나 새로 생성하여 Type-3 LSA를 필터링합니다. Type-3 요약 LSA로 지정된 영역에 발표된 경로에 적용됩니다.
내보내기 목록	액세스 목록을 선택하거나 새로 생성하여 지정된 영역의 영역 내 경로에서 다른 영역에 발표된 Type-3 요약 LSA를 필터링합니다.
인바운드 필터 목록	접두사 목록을 선택하거나 새로 생성하여 해당 영역으로 들어오는 Type-3 요약 LSA를 필터링합니다.
아웃바운드 필터 목록	접두사 목록을 선택하거나 새로 생성하여 영역에서 Type-3 요약 LSA를 필터링합니다.
IPv6 접두사	(NSSA만 해당) **ABR**이 활성화된 경우 IPv6 접두사를 추가하여 외부 서브넷 그룹을 단일 Type-7 LSA로 요약한 다음 광고를 선택할 때 Type-5 LSA로 변환되고 백본에 보급됩니다.
범위	
IPv6 주소/넷마스크	IPv6 주소/넷마스크를 추가합니다. 이 범위와 일치하는 라우팅 정보가 있는 유형 3 요약 LSA는 영역이 이 범위에서 하나 이상의 영역 내 네트워크(즉,

OSPFv3 설정	설명
	라우터 또는 네트워크 LSA로 설명됨)를 포함하는 경우 백본 영역으로 발표됩니다.
광고	LSA에서 일치하는 서브넷을 백본 영역에 알리려면 선택합니다. 광고가 아니요로 설정되면 해당 영역에 있는 일치하는 영역 내 접두사는 백본 영역에서 보급되지 않습니다.
상호 작용	
상호 작용	영역에 포함될 인터페이스를 추가합니다.
사용	인터페이스를 사용하도록 설정합니다.
MTU 무시	인접성을 설정하려고 할 때 MTU(최대 전송 단위) 불일치를 무시하려면 선택합니다(기본값은 사용 안 함). MTU 일치 검사수행).
수동	OSPF Hello 패킷을 이 인터페이스 밖으로 보내는 것을 방지하고 로컬 라우터가 이웃과 OSPF 인접성을 생성하지 못하도록 하려면 선택하십시오. 그러나 인터페이스는 여전히 링크 상태 데이터베이스에 포함됩니다. 예를 들어, 스위치에 연결하는 경우 라우터가 없는 곳에 Hello 패킷을 보내지 않으려는 경우 인터페이스를 수동으로 만들 수 있습니다.
인스턴스 ID	OSPFv3의 인스턴스는 하나만 허용되므로 0으로 유지하십시오. 기본값은 0입니다.
링크 유형	링크 유형 선택: • 브로드캐스트 - 인터페이스를 통해 액세스할 수 있는 모든 이웃은 이더넷 인터페이스와 같은 OSPFv3 Hello 메시지를 멀티캐스팅하여 자동으로 검색됩니다. • **p2p**(point-to-point) - 자동으로 이웃을 검색합니다. • **p2mp**(point-to-multipoint) - 인접 항목을 수동으로 정의해야 합니다. 이 인터페이스를 통해 연결할 수 있는 모든 인접 이웃에 대한 인접

OSPFv3 설정	설명
	IPv6 주소와 각 이웃의 우선 순위를 추가합니다. 범위는 0~255이며 기본값은 1입니다.
우선 사항	인터페이스의 우선 순위를 입력하십시오. 라우터가 지정 라우터(DR) 또는 백업 DR(BDR)로 선택되는 우선 순위 범위는 0~255 사이입니다. 기본값은 1입니다. 0이 구성되면 라우터가 DR 또는 BDR로 선택되지 않습니다.
타이머 프로파일	타이머 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 만듭니다. 이 프로파일은 OSPFv3에 적용된 전역 인터페이스 타이머 프로파일을 재정의합니다.
입증	인증 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 만듭니다. 이 프로파일은 유형 탭에 적용된 인증 프로파일을 재정의합니다.
BFD 프로파일	BFD 프로필 또는 **Inherit-vr-global-setting**(기본값)을 선택하거나 새 BFD 프로필을 생성하거나 없음**(BFD** 비활성화**)**을 선택합니다. 이 프로파일은 OSPFv3에 대해 구성된 프로파일을 재정의합니다.
비용	인터페이스에 대한 비용을 지정합니다. 범위는 1~65,535이며 기본값은 10입니다.
가상 링크	
이름	ABR에 백본 영역에 대한 물리적 링크가 없는 경우 백본 영역에 대한 물리적 링크가 있는 인접 ABR(동일한 영역 내)에 대한 가상 링크를 구성합니다. 가상 링크의 이름을 입력합니다.
사용	가상 링크를 사용하도록 설정합니다.
지역	백본 영역에 대한 물리적 링크가 있는 인접 ABR이 있는 전송 영역을 선택합니다.
라우터 ID	가상 링크의 원격 끝에 인접 ABR의 경로 ID를 입력합니다.

OSPFv3 설정	설명
타이머 프로파일	타이머 프로파일을 선택하거나 가상 링크에 적용할 새 프로파일을 만듭니다. 이 프로파일은 OSPFv3에 적용된 전역 인터페이스 타이머 프로파일과 인터페이스에 적용된 OSPFv3 인터페이스 타이머 프로파일을 재정의합니다.
입증	인증 프로파일을 선택하거나 가상 링크에 적용할 새 프로파일을 만듭니다. 이 프로파일은 유형 탭에 적용된 인증 프로파일과 인터페이스에 적용된 인증 프로파일을 재정의합니다.
고급	
R-Bit 및 v6-Bit 비활성화	방화벽이 활성 상태가 아님을 나타내기 위해 이 논리적 라우터에서 보낸 라우터 LSA의 R-비트 및 V6-비트를 지우려면 선택합니다. 이 상태에서 방화벽은 OSPFv3에 참여하지만 전송 트래픽이나 IPv6 데이터그램을 보내지 않습니다. 이 상태에서는 로컬 트래픽이 여전히 방화벽으로 전달됩니다. 트래픽이 방화벽에 도달할 수 있는 동안 방화벽 주위로 다시 라우팅될 수 있으므로 이중 홈 네트워크로 유지 관리를 수행하는 동안 유용합니다. RFC 5340을 참조하십시오.
정상 재시작 - 정상 재시작 사용	논리적 라우터에 대해 정상 재시작을 활성화합니다. 기본값은 활성화되어 있습니다.
도우미 모드 작동	논리적 라우터에 대해 정상 재시작 도우미 모드를 사용하도록 설정합니다. 기본값은 사용입니다.
엄격한 LSA 검사 작동	연결 상태 광고가 네트워크 토폴로지 변경을 나타내는 경우 도우미 라우터가 도우미 모드 수행을 중지하고 정상적인 재시작 프로세스를 중지하도록 하려면 활성화합니다. 기본값은 활성화되어 있습니다.
유예 기간(초)	방화벽이 다운되거나 사용할 수 없게 된 경우 논리적 라우터가 정상적인 재시작을 수행하는 시간(초)을 입력합니다. 범위는 5~1,800이며 기본값은 120입니다.

OSPFv3 설정	설명
최대 이웃 재시작 시간(초)	논리적 라우터가 도우미 모드에 있을 때 논리적 라우터가 이웃으로부터 수락하는 유예 기간(초)을 입력합니다. 범위는 5~1,800이며 기본값은 140입니다.

RIPv2> 네트워크 > 라우팅 > 논리적 라우터

이 표에서는 고급 라우팅 엔진의 논리적 라우터에 대해 RIPv2 인터페이스를 구성하는 설정에 대해 설명합니다.

RIPv2 설정	설명
사용	논리적 라우터에 대해 RIPv2를 사용하도록 설정합니다.
기본 정보가 시작됩니다.	라우팅 엔진의 RIB에 없는 경우에도 기본 경로를 알립니다.
BFD 프로파일	RIPv2에 BFD(양방향 전달 감지) 프로파일을 적용합니다. 기본값은 없음입니다.
전역 일반 타이머	RIPv2 전역 타이머 프로파일을 선택하여 업데이트 간격, 만료 간격 및 삭제 간격을 설정합니다. 기본값은 없음입니다.
인증 프로파일	RIPv2 인증 프로파일을 선택하여 MD5 또는 단순 암호 인증을 적용합니다. 기본값은 없음입니다.
재배포 프로파일	RIPv2 재배포 프로파일을 선택하여 IPv4 정적 경로, 연결된 경로, BGP AFI IPv4 경로 또는 OSPFv2 경로를 RIPv2에 재배포합니다. 기본값은 없음입니다.
전역 인바운드 배포 목록	허용 경로를 제어하기 위해 배포 목록을 선택합니다. 기본값은 없음입니다.
전역 아웃바운드 배포 목록	배포 목록을 선택하여 RIP 인접 라우터에 광고되는 경로를 제어합니다. 기본값은 없음입니다.

RIPv2 설정	설명
상호 작용	RIPv2 라우팅에 참여할 수 있는 인터페이스를 추가합니다.
사용	인터페이스가 RIPv2를 사용하도록 설정합니다.
수평 분할	다음 중 하나를 선택합니다. • **split-horizon** - 경로가 수신된 동일한 인터페이스에서 경로를 다시 알리지 않습니다. • **no-split-horizon** - 분할 수평선을 사용하지 않도록 설정합니다. • **no-split-horizon-with-poison-reverse** - 광고가 수신된 동일한 인터페이스에서 광고를 다시 허용하고 이러한 경로에 대한 메트릭을 RIP에 허용되는 최대값(16)으로 설정합니다.
모드	인터페이스의 모드를 선택합니다. • **active** - 인터페이스가 네트워크를 광고하고 RIP 업데이트를 보냅니다. • **passive** - 인터페이스가 네트워크를 광고하지만 RIP 업데이트를 전송하지는 않습니다. 네트워크에 RIP 라우터가 없으므로 인터페이스에서 RIP 업데이트를 보낼 이유가 없는 경우에 유용합니다. • **send-only(send-only)** - 방화벽이 끝 노드이고 RIP에만 접두사를 알리고 정적 경로 또는 기본 경로를 사용하여 외부 접두사에 도달하려는 경우에 사용할 수 있습니다.
입증	논리적 라우터 수준에서 적용한 프로파일을 재정의하려면 인증 프로파일을 선택합니다.
BFD 프로파일	기본적으로 인터페이스는 RIPv2의 논리적 라우터에 적용한 BFD 프로파일을 상속합니다. 또는 다른 BFD 프로파일을 선택하거나(논리적 라우터의 RIPv2에 대해 BFD가 비활성화되지 않은 경우) 없음**(BFD** 사용 안 함**)**을 선택하여 인터페이스에 대해 BFD를 사용하지 않도록 설정합니다.

RIPv2 설정	설명
인터페이스 인바운드 배포 목록 - 액세스 목록	액세스 목록을 선택하여 이 인터페이스로 오는 경로를 제어합니다.
인터페이스 인바운드 배포 목록 - 메트릭	들어오는 경로에 적용할 메트릭을 지정합니다. 범위는 1 ~ 16입니다.
인터페이스 아웃바운드 배포 목록 - 액세스 목록	액세스 목록을 선택하여 이 인터페이스에서 RIP 이웃에게 광고된 경로를 제어합니다.
인터페이스 아웃바운드 배포 목록 - 메트릭	광고된 경로에 적용할 메트릭을 지정합니다. 범위는 1 ~ 16입니다.

네트워크 > 라우팅 > 논리 라우터 > BGP

이 표에서는 고급 라우팅 엔진에서 논리 라우터에 대한 BGP, 피어 그룹, 피어, 네트워크, 재배포 정책 및 집계 경로를 구성하는 설정에 대해 설명합니다.

BGP 설정	설명
일반	
사용	논리적 라우터에 대해 BGP를 활성화합니다.
라우터 ID	라우터 ID가 고유한지 확인하기 위해 일반적으로 IPv4 주소인 논리적 라우터의 BGP에 라우터 ID를 할당합니다.
로컬 AS	라우터 ID(2바이트 또는 4바이트 AS 번호의 범위는 1~4,294,967,295)를 기반으로 논리적 라우터가 속한 로컬 AS(Autonomous System)를 할당합니다.
전역 BFD 프로파일	BFD 프로파일을 선택하거나 새 BFD 프로파일을 만들어 BGP에 전역적으로 적용합니다. 기본값은 없음**(BFD** 비활성화**)**입니다.
경로 설치	학습된 BGP 경로를 전역 라우팅 테이블에 설치하려면 선택합니다. 기본값은 비활성화되어 있습니다.
빠른 페일오버	보류 시간이 만료될 때까지 기다리지 않고 해당 피어에 대한 링크가 중단될 경우 BGP가 인접 피어와의 세션을 종료하도록 선택합니다. EBGP의 빠른 페일오버는 기본적으로 활성화되어 있습니다. 방화벽이 BGP 경로를 불필요하게 철회하도록 하는 경우 EBGP 빠른 페일오버를 비활성화합니다.

BGP 설정	설명
정상 종료	BGP가 RFC 8326을 기반으로 대체 경로를 선택하고 전파할 수 있도록 유지 관리 작업 중에 BGP가 eBGP 피어링 링크의 기본 설정을 낮추도록 선택합니다. 기본값은 비활성화되어 있습니다.
ECMP 다중 AS 지원	ECMP를 구성했고 여러 BGP 자율 시스템에서 ECMP를 실행하려는 경우 활성화합니다.
첫 번째 AS 시행	방화벽이 EBGP 피어의 자체 AS 번호를 AS_PATH 속성의 첫 번째 AS 번호로 나열하지 않는 EBGP 피어로부터 들어오는 업데이트 메시지를 삭제하도록 하려면 선택합니다. (기본적으로 활성화되어 있습니다.)
기본 로컬 기본 설정	동일한 대상에 대한 여러 경로 간의 기본 설정을 결정하는 데 사용할 수 있는 기본 로컬 기본 설정을 지정합니다. 범위는 0에서 4,294,967,295입니다. 기본값은 100입니다.
정상 재시작 - 활성화	BGP를 다시 시작하는 동안 패킷 포워딩이 중단되지 않도록 BGP에 대한 단계적 재시작을 활성화합니다(기본값은 활성화임).
오래된 경로 시간(초)	경로가 부실 상태를 유지할 수 있는 시간(초)을 지정합니다(범위는 1~3,600, 기본값은 120).
최대 피어 재시작 시간(초)	로컬 디바이스가 피어 디바이스에 대한 유예 기간 재시작 시간으로 허용하는 최대 시간(초)을 지정합니다(범위는 1 - 3,600, 기본값은 120).
로컬 재시작 시간	로컬 디바이스가 다시 시작하기를 기다리는 시간(초)을 지정하십시오. 범위는 1 - 3,600입니다. 기본값은 120입니다. 이 값은 피어에게 알려집니다.
경로 선택 - 항상 MED 비교	다른 자율 시스템의 이웃에서 경로를 선택하려면 선택하십시오. 기본값은 비활성화되어 있습니다. MED(Multi-Exit Discriminator)는 AS로의 선호 경로를 이웃에게 알려주는 외부 메트릭입니다. 높은 값보다 낮은 값이 선호됩니다.
결정적 MED 비교	IBGP 피어(동일한 AS의 BGP 피어)가 알리는 경로 중에서 선택하려면 선택합니다. 기본값은 활성화되어 있습니다.
피어 그룹	
이름	이름으로 BGP 피어 그룹을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다. 이름은 논리 라우터 내에서 그리고 모든 논리적 라우터에서 고유해야 합니다.

BGP 설정	설명
사용	피어 그룹을 활성화합니다.
유형	피어 그룹 유형을 **IBGP**(내부 BGP, AS 내 피어링) 또는 **EBGP**(외부 BGP - 두 자율 시스템 간 피어링)로 선택합니다.
IPv4 주소 패밀리	AFI IPv4 프로파일을 선택하거나 생성하여 프로파일의 설정을 피어 그룹에 적용합니다. 기본값은 없음입니다.
IPv6 주소 패밀리	AFI IPv6 프로파일을 선택하거나 생성하여 프로파일의 설정을 피어 그룹에 적용합니다. 기본값은 없음입니다.
IPv4 필터링 프로파일	BGP 필터링 프로파일(IPv4 AFI의 경우) 의 요소를 피어 그룹에 적용합니다. 기본값은 없음입니다.
IPv6 필터링 프로파일	BGP 필터링 프로파일(IPv6 AFI의 경우) 의 요소를 피어 그룹에 적용합니다. 기본값은 없음입니다.
인증 프로파일	피어 그룹의 BGP 피어 간에 MD5 인증을 제어하는 인증 프로파일을 선택하거나 생성합니다. 기본값은 없음입니다.
타이머 프로파일	피어 그룹에 적용할 BGP 타이머 프로파일을 선택하거나 생성합니다. 기본값은 없음입니다. 타이머는 경로를 알리는 keepalive 및 업데이트 메시지에 영향을 미칩니다.
멀티 홉	IP 헤더에 TTL(Time-to-Live) 값을 설정합니다. 범위는 0~255입니다. 0으로 설정하면 기본값을 사용합니다. EBGP의 경우 1개; IBGP의 경우 255.
댐핑 프로파일	댐핑 프로파일을 선택하거나 생성하여 안정화될 때까지 플랩 경로가 사용되지 않도록 억제하는 방법을 결정합니다. 기본값은 없음입니다.
피어	
이름	최대 63자를 포함하는 이름으로 BGP 피어를 추가합니다. 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다. 이름은 논리 라우터 내에서 그리고 모든 논리적 라우터에서 고유해야 합니다.
사용	BGP 피어를 활성화합니다.

BGP 설정	설명
수동	피어가 이웃과의 세션을 시작하지 못하도록 하려면 선택합니다. 기본값은 비활성됨입니다.
피어 AS	피어가 속한 AS를 입력하십시오. 범위는 1~4,294,967,295입니다.
피어—어드레싱	
상속	• 예 - (기본값) 피어 그룹에서 AFI 및 후속 AFI(SAFI) 구성을 상속할 피어에 대해 선택합니다. • 아니요 - 피어에 적용할 AFI 및 필터링 프로파일을 작성하여 피어 그룹 설정을 재정의하려면 선택합니다.
로컬 주소 - 인터페이스	BGP를 구성할 레이어 3 인터페이스를 선택합니다. 고정 IP 주소로 구성된 인터페이스와 DHCP 클라이언트로 구성된 인터페이스를 선택할 수 있습니다. DHCP가 주소를 할당하는 인터페이스를 선택하면 **IP** 주소가 없음으로 표시됩니다. DHCP는 나중에 인터페이스에 IP 주소를 할당합니다. 논리적 라우터에 대한 추가 런타임 통계를 볼 때 주소를 볼 수 있습니다.
IP 주소	인터페이스에 둘 이상의 IP 주소가 있는 경우 사용할 IP 주소와 넷마스크를 입력합니다.
피어 주소 - 유형	**IP** 또는 **FQDN**을 선택하고 피어의 IP 주소 또는 FQDN을 입력합니다.
IPv4 주소 패밀리	(상속 아니요인 경우 사용 가능) 기본 프로파일을 선택하거나 AFI IPv4 프로파일을 생성하여 프로파일의 설정을 피어에 적용하거나 상속(피어 그룹에서 상속)을 선택합니다. 기본값은 없음입니다(**IPv4 AFI** 사용 안 함).
IPv6 주소 패밀리	(상속 아니요인 경우 사용 가능) AFI IPv6 프로파일을 선택하거나 생성하여 프로파일의 설정을 피어에 적용하거나 상속(피어 그룹에서 상속)을 선택합니다. 기본값은 없음입니다(**IPv6 AFI** 사용 안 함).
IPv4 필터링 프로파일	(상속 아니요인 경우 사용 가능) 유니캐스트 또는 멀티캐스트 필터링에 대한 **IPv4** AFI를 지정하는 BGP 필터링 프로파일을 선택하거나 생성하여 피어에 적용합니다. 또는 상속(피어 그룹에서 상속)을 선택합니다. 기본값은 없음(**IPv4** 필터링 사용 안 함)입니다.
IPv6 필터링 프로파일	(상속 아니요인 경우 사용 가능) **IPv6** AFI 및 유니캐스트를 지정하는 BGP 필터링 프로파일을 선택하거나 생성하여 피어에 적용합니다. 또는 상속(피어 그룹에서 상속)을 선택합니다. 기본값은 없음(**IPv6** 필터링 사용 안 함)입니다.

BGP 설정	설명
피어 **-** 연결 옵션 이 설정은 피어가 속한 피어 그룹에 대해 설정한 것과 동일한 옵션을 재정의합니다.	
인증 프로파일	인증 프로파일을 선택하거나 생성합니다. 기본값은 상속**(**피어 그룹에서 상속**)**이며, 이 경우 피어는 피어 그룹에 대해 지정된 인증 프로파일을 사용합니다.
타이머 프로파일	타이머 프로파일을 선택하거나 만듭니다. 기본 설정은 상속**(**피어 그룹에서 상속**)**이며, 이로 인해 피어는 피어 그룹에 대해 지정된 타이머 프로파일을 사용합니다.
멀티 홉	IP 헤더에 TTL 값을 지정합니다. 범위는 0 - 255이고 기본값은 상속**(**피어 그룹에서 상속**)**입니다.
댐핑 프로파일	플래핑 루트가 안정화될 때까지 사용되지 않도록 억제하는 방법을 결정하는 댐핑 프로파일을 선택하거나 생성합니다. 기본값은 상속**(**피어 그룹에서 상속**)**이며, 이 경우 피어는 피어 그룹에 대해 지정된 댐핑 프로파일을 사용합니다.
피어 **- Advanced**	
발신자 측 루프 감지 활성화	방화벽이 업데이트에서 경로를 보내기 전에 FIB(포워딩 정보 기반)에서 경로의 AS_PATH 속성을 확인하여 피어 AS 번호가 AS_PATH 목록에 없는지 확인하려면 선택합니다. 그렇다면 방화벽은 루프를 방지하기 위해 제거합니다. 기본값은 활성화되어 있습니다.
BFD 프로파일	피어에 적용할 BFD 프로파일을 선택하거나 생성하거나 피어에 대해 없음**(BFD** 사용 안 함**)**을 선택합니다. 기본값은 **Inherit-vr-global-setting(**프로토콜의 전역 **BFD** 프로파일 상속**)**입니다.
네트워크	
네트워크 라우트 항상 광고	연결 가능 여부에 관계없이 구성된 네트워크 경로를 항상 BGP 피어에 알리려면 선택합니다. 이 옵션을 선택하지 않으면 방화벽은 로컬 라우팅 테이블을 사용하여 확인된 경우에만 네트워크 라우트를 알립니다. 기본값은 활성화되어 있습니다.
IPv4 또는 IPv6	**IPv4** 또는 **IPv6**을 선택하여 네트워크 접두사 유형을 지정합니다.
네트워크	해당 IPv4 또는 IPv6 네트워크 주소를 추가합니다. 네트워크 주소가 일치하는 서브넷은 논리적 라우터의 BGP 피어에 보급됩니다.

BGP 설정	설명
유니캐스트	모든 BGP 피어의 유니캐스트 라우팅 테이블에 일치하는 경로를 설치하려면 선택합니다.
멀티캐스트	(IPv4만 해당)모든 BGP 피어의 멀티캐스트 라우팅 테이블에 일치하는 경로를 설치하려면 선택합니다.
백도어	(IPv4만 해당) iBGP 연결(예: OSPF) 으로 변경될 수 있는 eBGP 연결에 대해 선택하여 BGP가 접두사를 AS 외부에 알리지 못하도록 하고 대신 경로를 AS 내에 유지합니다. 내부적으로 접두사에 대한 관리 거리가 증가하여 접두사가 선호되지 않지만 다른 곳에서 링크 오류가 발생할 경우에도 접두사를 계속 사용할 수 있습니다.
복구	
IPv4 재배포 프로파일	IPv4 AFI를 지정하는 BGP 재배포 프로파일을 선택하거나 생성하여 정적 경로, 연결된 경로 또는 OSPF 경로의 조합을 BGP에 재배포합니다. 기본값은 없음입니다.
IPv6 재배포 프로파일	IPv6 AFI를 지정하는 BGP 재배포 프로파일을 선택하거나 생성하여 정적 경로, 연결된 경로 또는 OSPFv3 경로의 조합을 BGP에 재배포합니다. 기본값은 없음입니다.
집계 경로	
이름	이름을 기준으로 집계 경로 정책을 추가합니다.
설명	집계 경로 정책에 대한 유용한 설명을 입력합니다.
사용	집계 경로 정책을 활성화하려면 선택합니다. 기본적으로 활성화됩니다.
요약 전용	요약된 경로가 아닌 요약 접두사만 이웃에 알리려면 선택합니다. 이렇게 하면 트래픽이 줄어들고 인접 라우팅 테이블의 크기가 불필요하게 증가하는 것을 방지할 수 있습니다(기본값은 비활성화됨). 집계 경로와 집계 경로를 구성하는 개별 경로를 모두 알리려면 선택하지 않은 상태로 둡니다. 요약 전용 및 맵 표시 안 함은 함께 사용할 수 없으며 둘 다 지정할 수 없습니다. 요약 전용를 사용하고 개별 경로도 알리고 싶다면 개별 경로와 일치하는 맵 표시 안 함 경로 맵을 포함하는 *BGP* 필터링 프로파일을 생성합니다.

BGP 설정	설명
AS 세트	집계 경로를 구성하는 AS 번호 목록과 함께 접두사를 알리려면 선택합니다. (기본값은 사용 안 함입니다.)
동일한 MED만 집계	MED(다중 출구 판별자) 값이 동일한 경로만 집계하려면 선택합니다. 기본값은 활성됨입니다.
유형	집계 경로 유형을 선택합니다. **IPv4** 또는 **IPv6**.
요약 접두사	요약할 경로를 계산한 다음 IP 주소/넷마스크 또는 주소 개체를 지정하여 해당 경로를 포괄하는 요약 접두사를 입력합니다.
맵 표시 안 함	경로 맵을 선택하거나 새 경로를 생성하여 개별 경로가 집계되지 않도록 합니다. 기본값은 없음입니다. 경로 맵 표시 안 함의 목적은 특정 경로가 광고에 집계되지 않도록 하는 것입니다. 따라서 경로 맵에서 억제하려는 경로가 집계되지 않도록 허용합니다(억제 중인 경로가 집계되는 것을 거부하지 않음). 요약 전용 및 맵 표시 안 함은 함께 사용할 수 없으며 둘 다 지정할 수 없습니다.
속성 맵	요약 접두사에 대한 속성 정보를 설정하려면 BGP 경로 맵을 선택하거나 새 경로 맵을 생성합니다. 일치 기준을 허용하지 않습니다. 기본값은 없음이며 이 경우 요약 접두사는 기본 속성을 갖습니다.

네트워크 > 라우팅 > 논리적 라우터 > 정적

이 표에서는 고급 라우팅 엔진의 논리적 라우터에 대해 IPv4 멀티캐스트를 구성하는 설정에 대해 설명합니다.

IPv4 멀티캐스트 설정	설명
멀티캐스트 프로토콜 사용	논리적 라우터에 대해 멀티캐스트 프로토콜을 사용하도록 설정하려면 선택합니다.
고정	

IPv4 멀티캐스트 설정	설명
이름	이름으로 mroute를 추가합니다(최대 31자). 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 0개 이상의 영숫자, 밑줄(_) 또는 하이픈(-)을 포함해야 합니다. 점(.) 이나 공백은 사용할 수 없습니다.
데스티네이션	RPF 검사를 수행 중인 멀티캐스트 소스인 대상(IPv4 주소/마스크)을 입력합니다.
상호 작용	멀티캐스트 소스에 대한 유니캐스트 경로에 대한 송신 인터페이스를 선택합니다.
다음 홉	소스에 대한 다음 홉의 IPv4 주소를 입력합니다.
기본 설정	mroute에 대한 기본 설정을 입력하십시오. 범위는 1 ~ 255입니다.
PIM - 일반	
사용	PIM을 사용하도록 설정합니다.
RPF 조회 모드	RPF(역방향 경로 전달) 조회 모드를 선택하면 논리적 라우터가 멀티캐스트 패킷에 포함된 소스 주소에 도달하기 위해 나가는 인터페이스를 찾을 위치를 결정합니다. RIB에 저장된 발신 인터페이스가 멀티캐스트 패킷이 도착한 인터페이스와 일치하면 논리적 라우터는 패킷을 수락하고 전달합니다. 그렇지 않으면 패킷이 삭제됩니다. • **mrib-then-urib** - 멀티캐스트 RIB를 먼저 살펴본 다음 유니캐스트 RIB를 살펴봅니다. • **mrib-only** - 멀티캐스트 RIB만 찾습니다. • **urib** 전용 - 유니캐스트 RIB만 살펴봅니다.
인터페이스 일반 타이머	인터페이스 타이머 프로파일을 선택하거나 새 프로파일을 생성합니다.
경로 만료 시간(초)	멀티캐스트 그룹과 소스 간에 세션이 종료된 후 멀티캐스트 경로가 mRIB에 남아 있는 시간(초)을 지정합니다. 범위는 210~7,200이며, 기본값은 210입니다.
멀티캐스트 SSM 범위	SSM(소스별 멀티캐스트)을 구성하려면 멀티캐스트 트래픽을 수신기에 전달할 수 있는 소스 주소를 지정하는 접두사 목록을 선택합니다. 기본값은 없음(접두사 목록 없음)입니다.

IPv4 멀티캐스트 설정	설명
그룹 주소	멀티캐스트 그룹 또는 접두사에 대한 SPT(최단 경로 트리) 임계값을 구성하려면 접두사 목록을 선택하거나 새 접두사를 만들어 그룹 주소(배포 트리를 지정하는 멀티캐스트 그룹 또는 접두사)를 추가합니다.
임계값	그룹 또는 접두사에 대한 SPT 임계값을 지정합니다. • **0(**첫 번째 데이터 패킷 켜기**)** - (기본값) 논리적 라우터는 논리적 라우터가 그룹/접두사에 대한 첫 번째 데이터 패킷을 수신할 때 공유 트리에서 그룹/접두사에 대한 SPT로 전환합니다. • 논리적 라우터가 해당 멀티캐스트 그룹/접두사에 대한 SPT 배포로 전환되는 모든 인터페이스 및 일정 기간 동안 멀티캐스트 그룹/접두사에 대해 도착할 수 있는 초당 총 킬로비트 수를 입력합니다. 범위는 0~4,294,967,295입니다. • 안 함**(spt**로 전환하지 않음**)** - 가상 라우터는 계속해서 공유 트리를 사용하여 패킷을 그룹 또는 접두사로 전달합니다.
PIM - 그룹 권한	
소스 그룹 목록	특정 소스 및/또는 멀티캐스트 패킷의 멀티캐스트 패킷이 논리적 라우터를 전송하기 위해 특정 대상 멀티캐스트 그룹에 대한 권한을 부여하려면 액세스 목록을 선택합니다. 기본값은 없음**(**액세스 목록 없음**)**이며, 이는 특정 소스 또는 멀티캐스트 그룹에 PIM 그룹 권한이 적용되지 않음을 의미합니다.
PIM - 인터페이스	
이름	인터페이스 이름(최대 31자)을 입력합니다. 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 0개 이상의 영숫자, 밑줄(_) 또는 하이픈(-)을 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
설명	인터페이스에 대한 설명을 입력합니다.
재해 복구 우선 순위	인터페이스의 지정된 라우터 우선 순위를 지정하여 PIM 조인 메시지, PIM 레지스터 메시지 및 프룬 메시지를 RP(Rendezvous Point)로 전달하는 라우터를 제어합니다. 범위는 1~4,294,967,295이며, 기본값은 1입니다. LAN상의 PIM 디바이스들 중에서, DR 우선순위가 구성되면, 가장 높은 우선순위 값을 갖는 디바이스가 DR을 선택합니다.
BSM 보내기	부트스트랩 메시지의 전파를 허용하려면 선택합니다(기본적으로 사용됨).

IPv4 멀티캐스트 설정	설명
타이머 프로파일	인터페이스의 타이머 프로파일은 인터페이스에 대한 타이머 프로파일을 선택하여 재정의하지 않는 한 일반 PIM 섹션에서 상속됩니다. 기본값은 없음입니다.
이웃 필터	액세스 목록을 사용하여 논리적 라우터의 PIM 이웃이 되거나 거부될 수 없는 디바이스의 접두사를 지정합니다. 기본값은 없음(액세스 목록 없음)입니다.
PIM - 랑데뷰 포인트	
RP 유형	정적 RP 및/또는 후보 RP를 구성하며, 상호 배타적이지 않습니다. • 정적 **RP** - 멀티캐스트 그룹에 대한 RP의 정적 매핑을 설정합니다. PIM 도메인의 다른 PIM 라우터에서 동일한 RP를 명시적으로 구성해야 합니다. • 후보 **RP** • 없음
상호 작용	RP가 멀티캐스트 패킷을 수신하고 전송하는 RP 인터페이스를 선택합니다. 유효한 인터페이스 유형은 Layer3 인터페이스(이더넷, 루프백, VLAN, 집계 이더넷(AE), 터널 및 하위 인터페이스 포함)입니다.
주소	인터페이스의 주소/접두사 길이를 선택합니다. 선택한 RP 인터페이스의 IP 주소가 목록을 채웁니다.
동일한 그룹에 대해 학습된 RP 재정의	(정적 RP에만 해당) 이 정적 RP가 그룹 목록의 그룹에 대해 선택된 RP 대신 RP로 작동하도록 선택합니다.
그룹 목록	액세스 목록을 선택하거나 작성하여 정적 RP가 RP 역할을 하는 멀티캐스트 그룹을 지정합니다. 기본값은 없음(액세스 목록 없음)입니다.
우선 사항	(후보 RP에만 해당) 후보 RP의 우선 순위를 지정합니다. 범위는 0~255이며 기본값은 192입니다. 우선 순위 값이 낮을수록 우선 순위가 높음을 나타냅니다.
광고 간격	(후보 RP에만 해당) 후보 RP가 다른 라우터에 알림을 보내는 빈도(초)를 지정합니다. 범위는 1~26,214이며 기본값은 60입니다.
IPv4 주소	인터페이스의 **IPv4** 주소를 선택하여 인터페이스를 추가합니다.

IPv4 멀티캐스트 설정	설명
그룹 목록	후보 RP가 수락하는 그룹을 제어하려면 IPv4 액세스 목록인 그룹 목록을 선택하거나 만듭니다. 기본값은 없음(액세스 목록 없음)입니다. 액세스 목록이 적용되지 않으면 논리적 라우터가 모든 그룹에 대한 RP로 자신을 알리기 시작합니다.
재정의	그룹 목록의 그룹에 대해 동적으로 학습(선택)되는 RP 대신 정적으로 구성한 원격 RP가 RP로 작동하도록 하려면 선택합니다. 기본값은 사용 안 함입니다.
IGMP	
IGMP 활성화	IGMP를 사용하도록 설정합니다.
동적	
상호 작용	인터페이스를 추가합니다.
버전	IGMP 버전 **2** 또는 **3**을 선택합니다.
항내성	견고성 값을 선택합니다. 범위는 1~7이며, 기본값은 2입니다. 이 방화벽이 있는 서브넷에서 패킷이 손실되기 쉬운 경우 값을 늘리십시오. *Robustness * QueryInterval) + MaxQueryResponseTime*은 조인 메시지가 논리적 라우터에서 유효한 기간을 결정합니다. 논리적 라우터가 그룹 나가기 메시지를 수신하는 경우 *Robustness * LastMemberQueryInterval*은 논리적 라우터가 그룹 나가기 항목을 삭제하기 전에 대기하는 시간입니다. 조인 메시지의 경우 *Robustness* 값 *1*이 무시됩니다. 그룹 나가기 메시지의 경우 논리적 라우터는 *Robustness* 값을 마지막 멤버 쿼리 수로도 사용합니다.
그룹 필터	액세스 목록을 선택하거나 작성하여 동적 IGMP를 사용하는 접두사를 제어합니다. 기본값은 없음(액세스 목록 없음)입니다.
최대 그룹	IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 그룹 수를 입력합니다. 범위는 1~65,525이고 기본값은 무제한이며, 이는 범위에서 가장 높은 값을 의미합니다.

IPv4 멀티캐스트 설정	설명
최대 소스	IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 소스 수를 입력합니다. 범위는 1~65,525이고 기본값은 무제한이며, 이는 범위에서 가장 높은 값을 의미합니다.
쿼리 프로파일	만든 IGMP 인터페이스 쿼리 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 작성하십시오.
라우터 경고 옵션없이 IGMP 패킷 삭제	들어오는 IGMPv2 또는 IGMPv3 패킷에 IP 라우터 경고 옵션인 RFC 2113이 있거나 삭제되도록 요구하려면 선택합니다. 기본값은 사용 안 함입니다.
고정	
이름	정적 IGMP 인터페이스를 이름으로 추가합니다(최대 31자). 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 0개 이상의 영숫자, 밑줄(_) 또는 하이픈(-) 을 포함해야 합니다. 점(.) 이나 공백은 사용할 수 없습니다.
상호 작용	정적 IGMP 인터페이스가 될 인터페이스를 선택합니다.
그룹 주소	정적 IGMP 멤버의 멀티캐스트 그룹 주소를 입력합니다.
소스 주소	정적 IGMP 멤버가 멀티캐스트를 수신하는 소스 주소를 입력합니다.
MSDP - 일반	
사용	논리적 라우터에 대해 MSDP(Multicast Source Discovery Protocol)를 활성화합니다.
전역 타이머	전역 MSDP 타이머 프로필을 선택하거나 **default** 프로필을 선택하거나 새 전역 MSDP 타이머 프로필을 만듭니다. 기본 프로필을 선택하면 연결 유지 인터벌이 60으로 설정되고 메시지 시간 초과가 75로 설정되며 연결 재시도 인터벌이 30으로 설정됩니다. 기본값은 없음이며 이는 기본값이 적용됨을 의미합니다.
전역 인증	전역 인증 프로필을 선택하거나 새 프로필을 생성합니다. 기본값은 없음입니다.
발신자 ID - 인터페이스	SA(Source-Active) 메시지에서 논리적 라우터가 RP 인터페이스로 사용하는 인터페이스를 선택합니다. 발신자 ID에 IP 주소를 지정하는 경우 발

IPv4 멀티캐스트 설정	설명
	신자 IP 인터페이스를 구성해야 합니다. 인터페이스가 구성되지 않은 경우 IP 주소를 비워 두어야 합니다.
발신자 ID - IP	논리적 라우터가 SA 메시지에서 RP 주소로 사용하는 IP 주소(접두사 길이 포함)를 선택하거나 입력합니다. 발신자 IP 주소가 구성되지 않은 경우 논리적 라우터는 PIM RP 주소를 사용하여 SA 메시지를 캡슐화합니다.
MSDP - 피어	
피어	피어 이름(최대 63자)을 추가합니다. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
소스 인터페이스	MSDP 피어와 TCP를 통해 MSDP 연결을 설정하는 데 사용되는 소스 인터페이스를 입력합니다.
소스 인터페이스 - IP	소스 인터페이스의 IP 주소를 선택합니다. 기본값은 없음입니다.
피어 주소 유형	피어 주소 유형을 선택합니다. • **IP** - (기본값)이며 주소 개체를 선택하거나 IP 주소를 입력합니다. • **FQDN** - 피어의 정규화된 도메인 이름을 입력합니다. 드롭다운 목록에는 주소 개체로 구성된 모든 FQDN 이름이 표시됩니다.
원격 AS	MSDP 피어가 있는 원격 AS의 BGP 자치 시스템 번호를 입력합니다.
인증	다음 중 하나를 수행합니다. • 이 피어에 적용할 인증 프로필을 선택하면 일반 페이지에서 MSDP에 적용한 전역 인증 프로필을 재정의합니다. • 상속(전역 인증에서 상속) - 전역 인증 프로필(기본값)입니다. • 없음 - 이 피어에 대한 인증을 비활성화하여 전역 인증 프로필을 재정의합니다.
최대 SA	SA 캐시가 이 MSDP 피어에서 수락할 SA(소스-활성) 항목의 최대 수를 입력합니다. 범위는 0~1,024입니다. 기본값은 0입니다. 이 최대값에 도달하면 이 피어의 새 SA 메시지가 삭제됩니다.
피어 인바운드 SA 필터	액세스 목록을 선택하거나 새 액세스 목록을 생성하여 이 피어에서 수신 SA 메시지를 필터링(원치 않는 그룹 차단)합니다. 기본값은 없음입니다.

IPv4 멀티캐스트 설정	설명
	액세스 목록은 필터링할 (S, G)쌍의 원본 주소나 필터링할 (S, G)쌍의 대상(그룹) 주소를 지정하거나 둘 다 지정할 수 있습니다.
피어 아웃바운드 SA 필터	액세스 목록을 선택하거나 새 액세스 목록을 생성하여 이 피어로 전파되는 발신 SA 메시지(원치 않는 그룹 차단)를 필터링합니다. 기본값은 없음입니다. 액세스 목록은 필터링할 (S, G)쌍의 원본 주소나 필터링할 (S, G)쌍의 대상(그룹) 주소를 지정하거나 둘 다 지정할 수 있습니다.

네트워크 > 라우팅 > 라우팅 프로파일

고급 라우팅 엔진에서는 라우팅 프로파일을 생성하여 BGP, BFD, OSPF, OSPFv3, 멀티캐스트, RIPv2 및 필터에 특성을 쉽고 일관되게 적용할 수 있습니다.

네트워크 > 라우팅 > 라우팅 프로파일 > BGP

논리적 라우터의 경우 BGP 라우팅 프로파일을 사용하여 BGP 피어 그룹, 피어 또는 재배포 규칙에 구성을 효율적으로 적용합니다. 예를 들어 타이머 프로파일, 인증 프로파일 및 BGP 필터링 프로파일을 BGP 피어 그룹 또는 피어에 적용할 수 있습니다. IPv4 및 IPv6에 대한 AFI(주소 패밀리) 프로파일을 피어 그룹 또는 피어에 적용할 수 있습니다. IPv4 및 IPv6에 대한 재배포 프로파일을 BGP 재배포에 적용할 수 있습니다.

BGP 라우팅 프로파일	설명
BGP 인증 프로파일	
이름	인증 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다.
비밀	비밀을 입력하고 비밀을 확인하십시오. Secret은 MD5 인증에서 키로 사용됩니다.
BGP 타이머 프로파일	
이름	타이머 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다.
Keep Alive 인터벌(초)	대기 시간 설정(범위는 0~1,200, 기본값은 30)에 따라 피어의 경로가 억제되는 인터벌(초)을 입력합니다.
유지 시간(초)	피어 연결이 닫히기 전에 피어의 연속 Keepalive 또는 업데이트 메시지 사이에 경과할 수 있는 시간(초)을 입력하십시오(범위는 3에서 3,600, 기본값은 90).
재연결 재시도 간격	피어 연결을 다시 시도하기 전에 유휴 상태에서 대기할 시간(초)을 입력합니다(범위는 1~3,600, 기본값은 15).
오픈 지연 시간(초)	피어에 대한 TCP 연결을 열고 BGP 연결을 설정하기 위해 첫 번째 BGP 열기 메시지를 보내는 사이의 지연 시간(초)을 입력합니다(범위는 0~240, 기본값은 0).

BGP 라우팅 프로파일	설명
최소 경로 광고 인터벌(초)	경로를 알리거나 경로를 철회하는 두 개의 연속적인 업데이트 메시지(BGP 스피커 [방화벽]이 BGP 피어로 전송) 사이에 발생해야 하는 최소 시간(초)을 입력하십시오(범위는 1 - 600, 기본값은 30).
BGP 주소 제품군 프로파일	
이름	AFI(Address Family Identifier) 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다.
AFI	AFI 프로파일 유형(**IPv4**또는**IPv6**)을 선택합니다.
유니캐스트/멀티캐스트	SAFI(다음 주소 패밀리 식별자) 유형을 선택합니다.
SAFI 활성화	프로파일에 대해 유니캐스트 및/또는 멀티캐스트 SAFI를 활성화하려면 선택합니다. BGP 프로파일이 유효하려면 하나 이상의 SAFI가 활성화되어야 합니다. 두 SAFI를 모두 활성화할 수 있습니다.
저장된 경로로 피어의 소프트 재구성	BGP 피어의 설정이 업데이트된 후 방화벽이 자체적으로 소프트 재설정을 수행하도록 하려면 선택합니다. 기본값은 활성화되어 있습니다.
피어에 대한 모든 경로 광고	네트워크 내에서 다중 경로 기능을 유지하기 위해 모든 경로를 이웃에 알립니다.
각 인접 AS에 대한 최적 경로를 광고합니다.	BGP가 모든 자율 시스템에 대한 일반 경로가 아니라 각 인접 AS에 대한 최상의 경로를 광고하도록 하려면 활성화합니다. 모든 자율 시스템에 동일한 경로를 알리려면 이 옵션을 비활성화합니다.
AS-Path가 Remote-AS와 동일한 경우 아웃바운드 업데이트에서 ASN 재정의	동일한 AS(예: AS 64512)에 속하는 여러 사이트가 있고 그 사이에 다른 AS가 있는 경우 BGP AS 재정의 기능을 사용할 수 있습니다. 두 사이트 사이의 라우터는 AS 64512에 액세스할 수 있는 경로를 알리는 업데이트를 수신합니다. 업데이트가 AS 64512에도 있기 때문에 두 번째 사이트에서 업데이트를 삭제하지 않도록 중간 라우터는 예를 들어 AS 64512를 자체 ASN인 AS 64522로 바꿉니다.
경로 리플렉터 클라이언트	BGP 피어를 iBGP 네트워크에서 BGP 경로 리플렉터 클라이언트로 만들려면 활성화합니다.
기본 경로 시작	모든 기본 경로를 알리려면 선택합니다. 특정 목적지에 대한 경로만 광고하려면 비활성화하십시오.

BGP 라우팅 프로파일	설명
기본 출발 경로 맵	광고할 기본 경로 유형을 지정할 수 있는 기본 경로 시작 필드에 경로 맵을 적용합니다.
AS 허용	방화벽의 자체 AS(자동 시스템) 번호를 포함하는 경로를 허용할지의 여부를 지정합니다. • 원점 - 방화벽의 자체 AS가 AS_PATH에 있는 경우에도 경로를 수락합니다. • 발생 - 방화벽 자체 AS가 AS_PATH에 있을 수 있는 횟수입니다. • 없음 - (기본 설정) 아무 조치도 취하지 않습니다.
숫자 접두사	피어에서 수락할 최대 접두사 수를 입력합니다. 범위는 1~4,294,967,295입니다. 기본값은 1,000입니다.
임계값(%)	최대 프리픽스 수의 임계값 백분율을 입력하십시오. 피어가 임계값보다 더 많이 알리면 방화벽은 지정된 작업(경고 또는 다시 시작)을 수행합니다. 범위는 1~100입니다.
동작	최대 프리픽스 수를 초과한 후 방화벽이 BGP 연결에 대해 수행하는 작업을 지정합니다. 경고 메시지만 로그 또는 BGP 피어 연결을 다시 시작하십시오.
다음 홉	다음 홉 선택: • 없음 - 원래 다음 홉이 유지됩니다. • 자체 - 다음 홉 계산을 비활성화하고 로컬 다음 홉으로 경로를 알립니다. • **Self Force** - Force는 반영된 경로에 대해 다음 홉을 자체로 설정합니다.
비공개 AS 제거	방화벽이 다른 AS의 피어에 보내는 업데이트의 AS_PATH 속성에서 BGP가 개인 AS 번호를 제거하도록 하려면 다음 중 하나를 선택합니다. • 모두 - 모든 개인 AS 번호를 제거합니다. • **AS** 교체 - 모든 개인 AS 번호를 방화벽의 AS 번호로 교체합니다. • 없음 - (기본 설정) 아무 조치도 취하지 않습니다.
커뮤니티 보내기	아웃바운드 업데이트 메시지로 보낼 BGP 커뮤니티 속성 유형을 선택합니다. • 모두 - 모든 커뮤니티를 보냅니다.

BGP 라우팅 프로파일	설명
	• 둘 다 - 표준 및 확장 커뮤니티를 보냅니다. • 확장 - 확장 커뮤니티를 보냅니다. • 대규모 - 대규모 커뮤니티를 보냅니다. • 표준 - 표준 커뮤니티를 보냅니다. • 없음 - 커뮤니티를 보내지 않습니다.
ORF 목록	피어 그룹 또는 피어가 접두사 목록을 보내고/받거나 접두사 목록을 수신하여 소스에서 아웃바운드 경로 필터링(ORF)을 구현하고 업데이트에서 원치 않는 접두사를 보내거나 받는 것을 최소화할 수 있는 기능을 알립니다. 다음 중 하나를 선택합니다. • 없음 - (기본 설정) 피어 그룹 또는 피어(이 AFI 프로파일이 적용된 경우)에는 ORF 기능이 없습니다. • 둘 다 - 피어 그룹 또는 피어가 ORF를 구현하기 위해 접두사 목록을 보내고 접두사 목록을 수신할 수 있음을 알립니다. • 수신 - 피어 그룹 또는 피어가 ORF를 구현하기 위해 접두사 목록을 수신할 수 있음을 알립니다. 로컬 피어는 원격 피어의 ORF 기능과 접두사 목록을 수신하며 이를 아웃바운드 경로 필터로 구현합니다. • 보내기 - 피어 그룹 또는 피어가 ORF를 구현하기 위해 접두사 목록을 보낼 수 있음을 알립니다. 원격 피어(수신 기능 포함)는 ORF 기능을 수신하고 발신자에게 경로를 알릴 때 수신한 접두사 목록을 아웃바운드 경로 필터로 구현합니다. 다음을 수행하여 ORF를 구현합니다. **1.** 주소 패밀리 프로파일에서 ORF 기능을 지정하십시오. **2.** 피어 그룹 또는 발신자인 피어의 경우 피어 그룹/피어가 수신하려는 접두사 집합을 포함하는 접두사 목록을 만듭니다. **3.** BGP 필터링 프로파일을 만들고 인바운드 접두사 목록에서 생성한 접두사 목록을 선택합니다. **4.** BGP 피어 그룹의 경우 생성한 주소 패밀리 프로파일을 선택하여 피어 그룹에 적용합니다. 발신자의 경우 생성한 필터링 프로파일(접두사 목록을 나타냄)도 선택합니다. 피어 그룹 또는 피어가 ORF 수신기 전용인 경우 필터링 프로파일이 필요하지 않습니다. ORF 수신 기능을 나타내기 위해 주소 패밀리 프로파일만 필요합니다.
BGP 댐핑 프로파일	

BGP 라우팅 프로파일	설명
이름	댐핑 프로필의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다.
설명	댐핑 프로파일에 대한 설명을 입력합니다.
억제 한계	억제 값(플래핑에 대한 패널티의 누적 값)을 입력합니다. 이 지점에서 피어에서 오는 모든 경로가 댐핑됩니다. 범위는 1~20,000입니다. 기본값은 2,000입니다.
재사용 제한	반감기에 대해 설명된 절차에 따라 경로를 재사용할 수 있는 시기를 제어하는 값을 입력하십시오. 범위는 1 ~ 20,000입니다. 기본값은 750입니다.
반감기(분)	플래핑 경로에 적용되는 안정성 메트릭(페널티)을 제어하기 위한 반감기 시간(분)을 입력합니다. 범위는 1~45입니다. 기본값은 15입니다. 안정성 지표는 1,000에서 시작합니다. 페널티가 적용된 경로가 안정화된 후 반감기 타이머는 만료될 때까지 카운트다운합니다. 이 시점에서 라우터에 적용되는 다음 안정성 메트릭은 이전 값(500)의 절반에 불과합니다. 안정성 메트릭이 재사용 제한의 절반 미만이 될 때까지 연속적인 컷이 계속되고 안정성 메트릭이 라우터에서 제거됩니다.
최대 억제 시간(분)	경로가 얼마나 불안정했는지에 관계없이 경로가 억제될 수 있는 최대 시간(분)을 입력하십시오. 범위는 1~255입니다. 기본값은 60입니다.
BGP 재배포 프로파일	
이름	재배포 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다.
IPv4 또는 IPv6	IPv4 또는 IPv6 AFI(Address Family Identifier)를 선택하여 재배포할 경로 유형을 지정합니다.
고정	정적 및 활성화를 선택하여 선택한 AFI와 일치하는 IPv4 또는 IPv6 고정 경로를 BGP에 재배포합니다.
미터법	BGP로 재배포되는 고정 경로에 적용할 측정항목을 입력합니다(범위: 1~65,535).
경로 맵	경로 맵을 선택하여 재배포할 고정 경로를 결정하는 일치 기준을 지정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric

BGP 라우팅 프로파일	설명
	Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
연결됨	연결됨 및 활성화를 선택하여 선택한 AFI와 일치하는 IPv4 또는 IPv6 연결 경로를 BGP에 재배포합니다.
미터법	BGP로 재배포되는 연결된 경로에 적용할 메트릭을 입력합니다(범위는 1~65,535).
경로 맵	경로 맵을 선택하여 재배포할 연결된 경로를 결정하는 일치 기준을 지정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
OSPF	(IPv4만 해당) OSPFv2 경로를 BGP로 재배포하려면**OSPF** 및 활성화를 선택합니다.
미터법	BGP로 재배포되는 OSPF 경로에 적용할 메트릭을 입력합니다(범위는 1~65,535).
경로 맵	경로 맵을 선택하여 재배포할 OSPF 경로를 결정하는 일치 기준을 지정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
RIP	(IPv4 전용) **RIP** 및 활성화를 선택하여 RIP 경로를 BGP로 재배포합니다.
미터법	BGP로 재배포되는 RIP 경로에 적용할 메트릭을 입력하십시오(범위는 1~65,535).
경로 맵	경로 맵을 선택하여 재배포할 RIP 경로를 결정하는 일치 기준을 지정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
OSPFv3	(IPv6만 해당) OSPFv3 경로를 BGP로 재배포하려면**OSPFv3** 및 활성화를 선택합니다.
미터법	BGP로 재배포되는 OSPFv3 경로에 적용할 메트릭을 입력합니다(범위는 1~65,535).
경로 맵	경로 맵을 선택하여 재배포할 OSPFv3 경로를 결정하는 일치 기준을 지정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및

BGP 라우팅 프로파일	설명
	Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
BGP 필터링 프로파일	
이름	BGP 필터링 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_), 하이픈(-) 또는 점(.)으로 시작해야 하며 0개 이상의 영숫자 문자, 밑줄(_) 하이픈(-) 및 점을 포함해야 합니다. 공백은 허용되지 않습니다.
설명	BGP 필터링 프로파일에 대한 설명을 입력합니다.
AFI	**IPv4** 또는 **IPv6** 주소 계열 식별자를 선택하여 필터링할 경로 유형을 지정합니다.
유니캐스트 인바운드 필터 목록	AS 경로 액세스 목록을 선택하거나 새로 생성하여 피어로부터 경로를 수신할 때 동일한 AS 경로가 있는 경로만 피어 그룹 또는 피어에서 가져오도록 지정합니다. 즉, 로컬 BGP RIB에 추가됩니다.
인바운드 배포 목록	BGP가 수신하는 BGP 라우팅 정보를 필터링하려면 액세스 목록(소스 주소만, 대상 주소는 제외)을 사용합니다. 단일 필터링 프로파일의 인바운드 접두사 목록과 상호 배타적입니다.
인바운드 접두사 목록	접두사 목록을 사용하여 네트워크 접두사를 기반으로 BGP가 수신하는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 인바운드 배포 목록과 상호 배타적입니다.
인바운드 노선도	경로 맵을 사용하여 로컬 BGP RIB(기준 일치)에 허용되는 경로를 더욱 세밀하게 제어하고 경로에 대한 속성을 설정합니다(옵션 설정). 예를 들어 경로의 AS 경로 앞에 AS를 추가하여 경로 기본 설정을 제어할 수 있습니다.
아웃바운드 필터 목록	AS Path 액세스 목록을 선택하거나 새 AS Path 액세스 목록을 만들어 동일한 AS Path가 있는 경로만 피어 라우터(피어 그룹 또는 이 필터가 적용되는 피어)에 광고되도록 지정합니다.
아웃바운드 배포 목록	액세스 목록을 사용하여 대상의 IP 주소를 기반으로 BGP가 광고하는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 아웃바운드 접두사 목록과 상호 배타적입니다.

BGP 라우팅 프로파일	설명
아웃바운드 접두사 목록	접두사 목록을 사용하여 네트워크 접두사를 기반으로 BGP가 알리는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 아웃바운드 배포 목록과 상호 배타적입니다.
아웃바운드 노선도	경로 맵을 사용하여 BGP가 광고하는 경로(일치 기준)를 더욱 강력하게 제어하고 광고된 경로에 대한 속성을 설정합니다.
조건부 광고 - 존재 - 존재 맵	조건부 광고에 대한 일치 기준을 지정하려면 경로 맵을 선택하거나 만듭니다. 이러한 경로가 로컬 BGP RIB에 있는 경우 Advertise Map에서 지정한 경로가 광고됩니다. 이 필드에 있는 경로 맵의 일치 부분만 적용됩니다. Set 부분은 무시됩니다.
조건부 광고 - 존재 - 광고 맵	조건이 충족되는 경우 광고할 경로를 지정하려면 경로 맵을 선택하거나 생성하십시오(존재 맵의 경로가 로컬 BGP RIB에 존재함). 이 필드에 있는 경로 맵의 일치 부분만 적용됩니다. Set 부분은 무시됩니다.
조건부 광고 - 존재하지 않음 - 존재하지 않는 맵	조건부 광고에 대한 일치 기준을 지정하려면 경로 맵을 선택하거나 만듭니다. 이러한 경로가 로컬 BGP RIB에 존재하지 않으면 광고 맵에서 지정한 경로가 광고됩니다. 이 필드에 있는 경로 맵의 일치 부분만 적용됩니다. Set 부분은 무시됩니다.
조건부 광고 - 존재하지 않음 - 광고 맵	조건이 충족되는 경우 광고할 경로를 지정하려면 경로 맵을 선택하거나 생성하십시오(존재하지 않는 맵의 경로는 로컬 BGP RIB에 존재하지 않음). 이 필드에 있는 경로 맵의 일치 부분만 적용됩니다. Set 부분은 무시됩니다.
맵 억제 해제	경로 집계 또는 경로 댐핑에서 억제를 해제하고 광고할 경로의 경로 맵을 선택하거나 생성합니다.
멀티캐스트 - 유니캐스트에서 상속	(IPv4 AFI 전용) 멀티캐스트 경로 필터링을 위한 유니캐스트 설정을 상속하려면 선택합니다. 그렇지 않으면 유니캐스트 필터에 대해 이 표에 설명된 대로 멀티캐스트 필터를 구성하십시오.

BFD> 네트워크 > 라우팅 > 라우팅 프로파일

양방향 전달 감지 프로파일을 만듭니다.

BFD 라우팅 프로파일	설명
이름	BFD 프로파일의 이름(최대 63자)을 입력합니다. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
모드	모드 선택: • 활성 - (기본값) BFD가 제어 패킷을 피어로 보내기 시작합니다. BFD 피어 중 하나 이상은 활성 상태여야 합니다. 둘 다 활성일 수 있습니다. • 수동 - BFD는 피어가 제어 패킷을 보낼 때까지 기다렸다가 필요에 따라 응답합니다.
원하는 최소 전송 인터벌(ms)	BFD 프로토콜이 BFD 제어 패킷을 보내기를 원하는 최소 간격(밀리초)입니다. 따라서 피어와 전송 간격을 협상하고 있습니다. PA-7000 시리즈, PA-5200 시리즈, PA-5400 시리즈 및 PA-3400 시리즈의 범위는 50~10,000입니다. PA-3200 시리즈의 범위는 100~10,000입니다. PA-400 시리즈의 범위는 150~10,000입니다. VM 시리즈의 범위는 200~10,000입니다. 기본값은 1,000입니다.
올바른 최소 수신 인터벌(ms)	BFD가 BFD 제어 패킷을 수신할 수 있는 최소 인터벌(밀리초)입니다. PA-7000 시리즈, PA-5200 시리즈, PA-5400 시리즈 및 PA-3400 시리즈의 범위는 50~10,000입니다. PA-3200 시리즈의 범위는 100~10,000입니다. PA-400 시리즈의 범위는 150~10,000입니다. VM 시리즈의 범위는 200~10,000입니다. 기본값은 1,000입니다.
감지 시간 멀티플라이어	범위는 2~255이고 기본값은 3입니다. 로컬 시스템은 원격 시스템에서 수신한 감지 시간 승수에 원격 시스템의 합의된 전송 인터벌을 곱한 값으로 감지 시간을 계산합니다(**Required Minimum Rx Interval**과 마지막으로 수신한 **Desired Minimum Tx Interval** 중 큰 값). BFD가 감지 시간이 만료되기 전에 피어로부터 BFD 제어 패킷을 수신하지 않으면 오류가 발생한 것입니다.

BFD 라우팅 프로파일	설명
유지 시간(ms)	BFD가 BFD 제어 패킷을 전송하기 전에 링크가 발생한 후 지연(밀리초)입니다. 홀드 타임은 BFD **Active** 모드에만 적용됩니다. BFD는 홀드 타임 동안 BFD 제어 패킷을 수신하면 이를 무시합니다. 범위는 0~120,000이고 기본값은 0이며, 이는 전송 홀드 타임이 사용되지 않음을 의미합니다. BFD는 링크가 설정된 직후 BFD 제어 패킷을 보내고 받습니다.
멀티홉 활성화	BGP 멀티홉을 통해 BFD를 사용하도록 설정합니다.
최소 수신 TTL	BGP가 멀티홉 BFD를 지원할 때 BFD가 BFD 제어 패킷에서 수락(수신)할 최소 Time-to-Live(홉 수)를 입력합니다. 범위는 1 내지 254이고; 기본값은 없습니다.

네트워크 > 라우팅 > 라우팅 프로파일 > OSPF

OSPF 라우팅 프로파일을 추가하여 논리적 라우터에 대해 OSPFv2를 효율적으로 구성합니다.

OSPF 라우팅 프로파일	설명
OSPF 전역 타이머 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
LSA 최소 도착	동일한 LSA(동일한 광고 라우터 ID, 동일한 LSA 유형 및 동일한 LSA ID)의 두 인스턴스 전송 사이의 최소 시간(초)을 입력하십시오. 동일한 LSA가 구성된 간격보다 빨리 도착하면 LSA가 삭제됩니다. 범위는 1~10입니다. 기본값은 5입니다. LSA 최소 도착은 RFC 2328의 MinLSInterval과 동일합니다. 토폴로지 변경이 발생할 때 더 낮은 값을 사용하여 재수렴 시간을 줄일 수 있습니다.
SPF - 초기 지연	논리적 라우터가 토폴로지 변경을 수신할 때부터 SPF(최단 경로 우선) 계산을 수행할 때까지의 초기 지연(초)을 입력합니다.

OSPF 라우팅 프로파일	설명
	범위는 0에서 600 사이입니다. 기본값은 5입니다. 값이 낮을수록 OSPF 재수렴 속도가 빨라집니다. 방화벽과 피어링하는 라우터는 수렴 시간을 최적화하기 위해 동일한 지연 값을 사용해야 합니다.
초기 유지 시간	연속 SPF 계산 사이의 초기 유지 시간(초)을 입력합니다. 범위는 0~600입니다. 기본값은 5입니다.
최대 유지 시간	최대 유지 시간(초)을 입력합니다. 이 값은 유지 시간이 안정적으로 유지될 때까지 조절되는 가장 큰 값입니다. 범위는 0~600입니다. 기본값은 5입니다.
OSPF 인터페이스 인증 프로파일	
이름	인증 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
유형	인증 유형 중 하나 선택: • 암호 - 암호(최대 8자) 및 암호 확인을 입력합니다. • **MD5** - **MD5** 키 ID(범위는 0~255) 및 키(최대 16자, 공백을 제외한 모든 문자)를 추가합니다. 다른 MD5 키보다 MD5 키를 선호하려면 선호를 선택합니다.
OSPF 인터페이스 타이머 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
헬로 인터벌	이웃 관계를 유지하기 위해 방화벽이 인터페이스로 보내는 Hello 패킷 사이의 간격(초)을 입력하십시오. 범위는 1 ~ 3600입니다. 기본값은 10입니다.
데드 카운트	OSPF가 이웃으로부터 Hello 패킷을 수신하지 않고 OSPF가 해당 이웃을 다운으로 간주하기 전에 Hello Interval이 이웃에 대해 발생할 수 있는 횟수를 입력하십시오. 범위는 3~20입니다. 기본값은 4입니다.

OSPF 라우팅 프로파일	설명
재전송 간격	인접 라우터로의 LSA 재전송 사이의 시간(초)을 입력하십시오. 범위는 1 ~ 1800입니다. 기본값은 5입니다.
전송 지연	인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 필요한 시간(초)을 입력합니다. 업데이트 패킷의 링크 상태 광고는 전송되기 전에 이 숫자만큼 기간이 증가합니다. 범위는 1 ~ 1800입니다. 기본값은 1입니다.
정상 재시작 Hello 지연(초)	능동/수동 고가용성이 구성될 때 OSPF 인터페이스에 적용되는 정상 재시작 Hello Delay(초)를 입력합니다. 정상 재시작 Hello 지연은 방화벽이 1초 인터벌으로 Grace LSA 패킷을 보내는 시간입니다. 이 시간 동안에는 다시 시작하는 방화벽에서 헬로 패킷이 전송되지 않습니다. 다시 시작하는 동안 데드 타이머(헬로 간격에 데드 카운트를 곱한 값)도 카운트다운됩니다. 데드 타이머가 너무 짧으면 헬로 지연(hello delay)으로 인해 단계적 재시작 중에 인접성이 낮아집니다. 따라서 데드 타이머는 정상 재시작 Hello 지연 값의 4배 이상으로 설정하는 것이 좋습니다. 예를 들어 Hello Interval이 10초이고 Dead Count가 4이면 데드 타이머는 40초입니다. 정상 재시작 Hello 지연이 10초로 설정된 경우 Hello 패킷의 10초 지연은 40초 데드 타이머 내에서 편안하게 이루어지므로 인접성은 정상적인 재시작 동안 시간 초과되지 않습니다. 범위는 1~10입니다. 기본값은 10입니다.
OSPF 재배포 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
IPv4 정적	프로파일의 이 부분을 구성할 수 있도록 선택합니다.
사용	OSPF에 대한 IPv4 정적 경로 재배포를 활성화합니다.
미터법	OSPF로 재배포되는 고정 경로에 적용할 메트릭을 지정합니다(범위는 1~65,535).
메트릭 유형	선택: • 유형 **1**

OSPF 라우팅 프로파일	설명
	• 유형 **2**(기본값)
경로 맵 재배포	재배포 경로 맵을 선택하거나 생성하여 OSPF에 재배포되는 IPv4 고정 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
연결됨	프로파일의 이 부분을 구성할 수 있도록 선택합니다.
사용	OSPF에 연결된 경로 재배포를 활성화합니다.
미터법	OSPF로 재배포되는 연결된 경로에 적용할 메트릭을 지정합니다(범위는 1~65,535).
메트릭 유형	선택: • 유형 **1** • 유형 **2**(기본값)
경로 맵 재배포	재분배 경로 맵을 선택하거나 생성하여 연결된 경로가 OSPF에 재분배되고 속성을 설정하도록 제어합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
RIPv2	프로파일의 이 부분을 구성할 수 있도록 선택합니다.
사용	OSPF에 대한 RIPv2 경로 재배포를 활성화합니다.
미터법	OSPF로 재배포되는 RIPv2 경로에 적용할 지표를 지정합니다(범위는 0~4,294,967,295).
메트릭 유형	선택: • 유형 **1** • 유형 **2**(기본값)

OSPF 라우팅 프로파일	설명
경로 맵 재배포	재배포 경로 맵을 선택하거나 생성하여 OSPF에 재배포되는 RIPv2 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
BGP AFI IPv4	프로파일의 이 부분을 구성할 수 있도록 선택합니다.
사용	OSPF에 대한 BGP IPv4 경로 재배포를 활성화합니다.
미터법	OSPF로 재배포되는 BGP IPv4 경로에 적용할 지표를 지정합니다(범위는 0~4,294,967,295).
메트릭 유형	선택: • 유형 **1** • 유형 **2**(기본값)
경로 맵 재배포	재배포 경로 맵을 선택하거나 생성하여 OSPF에 재배포되는 BGP IPv4 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
IPv4 기본 경로	프로파일의 이 부분을 구성할 수 있도록 선택합니다.
항상	라우터에 기본 경로가 없는 경우에도 항상 IPv4 기본 경로를 생성하고 OSPF에 재배포하려면 선택합니다. 기본값은 활성화되어 있습니다.
사용	OSPF에 대한 IPv4 기본 경로 재배포를 활성화합니다.
미터법	OSPF로 재배포되는 IPv4 기본 경로에 적용할 지표를 지정합니다(범위는 0~4,294,967,295).
메트릭 유형	선택: • 유형 **1**

OSPF 라우팅 프로파일	설명
	• 유형 **2**(기본값)

네트워크 > 라우팅 > 라우팅 프로파일 > OSPFv3

논리적 라우터에 대해 OSPFv3를 효율적으로 구성하려면 OSPFv3 라우팅 프로파일을 추가합니다.

OSPFv3 라우팅 프로파일	설명
OSPFv3 전역 타이머 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
LSA 최소 도착	방화벽이 SPF 트리를 다시 계산하는 가장 작은 간격을 입력합니다. 범위는 1~10이고 기본값은 5입니다. 방화벽은 더 큰 간격(설정보다 덜 빈번함)으로 다시 계산됩니다.
SPF 스로틀 - 초기 지연	논리적 라우터가 토폴로지 변경을 수신할 때부터 SPF(최단 경로 우선) 계산을 수행할 때까지의 초기 지연(초)을 입력합니다. 범위는 0에서 600 사이입니다. 기본값은 5입니다.
초기 유지 시간	처음 두 개의 연속 SPF 계산 사이의 초기 유지 시간(초)을 입력합니다. 범위는 0~600이고 기본값은 5입니다. 각 후속 보류 시간은 보류 시간이 최대 보류 시간에 도달할 때까지 이전 보류 시간의 두 배입니다.
최대 유지 시간	유지 시간이 안정적으로 유지될 때까지 증가하는 가장 큰 값을 입력합니다. 범위는 0~600이고 기본값은 5입니다.
OSPFv3 인증 프로파일	
이름	인증 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
SPI	OSPFv3 인접의 양쪽 끝 간에 일치해야 하는 보안 정책 인덱스를 입력합니다.

OSPFv3 라우팅 프로파일	설명
프로토콜	인증 프로토콜을 선택합니다. **ESP**(보안 페이로드 캡슐화)(권장) 또는 **AH**(인증 헤더)
인증 - 유형	인증 유형 선택: • **SHA1**(기본값) 보안 해시 알고리즘 1. • **SHA256** • **SHA384** • **SHA512** • **MD5** • 없음
열쇠	인증 키를 십진수 형식으로 입력합니다: xxxxxxxx[-xxxxxxxx] ... 총 5 개의 섹션 및 키 확인 사용.
암호화 - 알고리즘	(ESP에만 해당) 암호화 알고리즘을 선택합니다. • **3des**(기본값) • **aes-128-cbc** • **aes-192-cbc** • **aes-256-cbc** • **null**
열쇠	(ESP에만 해당) 암호화 키를 십진수 형식으로 입력합니다. ESP 암호화 유형 및 키 확인에 따라 올바른 섹션 수를 사용합니다. • **3des** - 키에 총 6개의 16진수 섹션을 사용합니다. • **aes-128-cbc** - 키에 총 4개의 16진수 섹션을 사용합니다. • **aes-192-bc** - 키에 총 6개의 16진수 섹션을 사용합니다. • **aes-256-bc**- 키에 총 8개의 16진수 섹션을 사용합니다.
OSPFv3 인터페이스 타이머 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.

OSPFv3 라우팅 프로파일	설명
헬로 인터벌	OSPFv3이 Hello 패킷을 보내는 간격(초)을 입력합니다. 범위는 1~3,600이고 기본값은 10입니다.
데드 카운트	OSPFv3이 이웃을 다운된 것으로 간주하기 전에 OSPFv3이 이웃으로부터 Hello 패킷을 수신하지 않고 이웃으로부터 헬로 간격이 발생할 수 있는 횟수를 입력하십시오. 범위는 3~20이고 기본값은 4입니다.
재전송 간격	OSPFv3이 LSA를 재전송하기 전에 OSPFv3이 이웃으로부터 LSA를 수신하기 위해 대기하는 시간(초)을 입력합니다: 범위는 1~1,800이고 기본값은 5입니다.
전송 지연	인터페이스 밖으로 SLA를 전송하기 전에 OSPFv3이 LSA 전송을 지연시키는 시간(초)을 입력하십시오. 범위는 1~1,800이고 기본값은 1입니다.
정상 재시작 Hello 지연(초)	몇 초 안에 정상 재시작 Hello 지연을 입력하십시오. 범위는 1~10이고 기본값은 10입니다. 이 설정은 활성/수동 HA가 구성된 경우 OSPFv3 인터페이스에 적용됩니다. 정상 재시작 Hello 지연은 방화벽이 1초 간격으로 Grace LSA 패킷을 보내는 시간(초)입니다. 이 시간 동안 다시 시작하는 방화벽에서 Hello 패킷이 전송되지 않습니다. 다시 시작하는 동안 데드 타임(**Hello Interval**에 **Dead Count**를 곱한 값)도 카운트다운됩니다. 데드 타이머가 너무 짧으면 헬로 지연(hello delay)으로 인해 단계적 재시작 중에 인접성이 낮아집니다. 따라서 데드 타이머는 정상 재시작 Hello 지연 값의 4배 이상으로 설정하는 것이 좋습니다.
OSPFv3 재배포 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
IPv6 정적	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
사용	프로파일의 IPv6 정적 부분을 사용하도록 설정합니다.
미터법	OSPFv3으로 재배포되는 고정 경로에 적용할 측정항목을 입력합니다(범위: 1~65,535).

OSPFv3 라우팅 프로파일	설명
메트릭 유형	유형 **1** 또는 유형 **2**를 선택합니다.
경로 맵 재배포	재배포 경로 맵을 선택하거나 만들어 OSPFv3에 재분배되는 IPv6 정적 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
연결됨	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
사용	프로파일의 연결된 부분을 사용하도록 설정합니다.
미터법	OSPFv3(범위는 1~65,535)로 재배포되는 연결된 경로에 적용할 지표를 지정합니다.
메트릭 유형	유형 **1** 또는 유형 **2**를 선택합니다.
경로 맵 재배포	재배포 경로 맵을 선택하거나 생성하여 OSPFv3에 재분배되는 연결된 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
BGP AFI IPv6	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
사용	프로파일의 BGP AFI IPv6 부분을 사용하도록 설정합니다.
미터법	OSPFv3(범위는 0~4,294,967,295)로 재배포되는 BGP IPv6 경로에 적용할 지표를 지정합니다.
메트릭 유형	유형 **1** 또는 유형 **2**를 선택합니다.
경로 맵 재배포	재배포 경로 맵을 선택하거나 만들어 OSPFv3에 재분배되는 BGP IPv6 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에

OSPFv3 라우팅 프로파일	설명
	적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.
IPv6 기본 경로	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
항상	라우터에 기본 경로가 없는 경우에도 항상 IPv6 기본 경로를 생성하고 OSPFv3에 재배포하려면 선택합니다. 기본값은 활성화되어 있습니다.
사용	프로파일의 IPv6 기본 경로 부분을 사용하도록 설정합니다.
미터법	OSPFv3(범위는 0~4,294,967,295)에 재배포되는 IPv6 기본 경로에 적용할 지표를 지정합니다.
메트릭 유형	유형 **1** 또는 유형 **2**를 선택합니다.

네트워크 > 라우팅 > 라우팅 프로파일 > RIPv2

논리적 라우터에 대해 RIPv2를 효율적으로 구성하려면 RIPv2 라우팅 프로파일을 추가합니다.

RIPv2 라우팅 프로파일	설명
RIPv2 전역 타이머 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
업데이트 인터벌	정기적으로 예약된 라우팅 업데이트 메시지 사이의 시간(초) 을 입력합니다. 범위는 5~2,147,483,647이며 기본값은 30입니다.
만료 간격	경로가 업데이트되지 않고 라우팅 테이블에 있을 수 있는 시간(초) 을 입력합니다. 범위는 5~2,147,483,647이며 기본값은 180입니다. 만료 간격에 도달한 후에도 삭제 간격에 도달할 때까지 경로가 업데이트 메시지에 계속 포함됩니다.

RIPv2 라우팅 프로파일	설명
삭제 간격	삭제 간격에 시간(초) 을 입력합니다. 범위는 5 - 2,147,483,647이며 기본값은 120입니다. 라우팅 테이블에서 만료된 라우트가 Delete 간격에 도달하면 라우팅 테이블에서 삭제됩니다.
RIPv2 인증 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
유형	인증 유형 선택: **md5(RIP MD5** 인증 방법 사용**)** 또는 암호**(**단순 암호 인증**)**.
비밀번호	(단순 암호 인증) 암호(최대 16자) 와 암호 확인을 입력합니다.
MD5	(RIP MD5 인증) MD5 키 ID를 입력합니다. 범위는 0~255입니다.
열쇠	(RIP MD5 인증) MD5 키(최대 16자) 및 확인 키를 입력합니다.
패킷을 보낼 때 이 키 사용	(RIP MD5 인증) 이 키를 기본 설정 키로 만들려면 선택합니다.
RIPv2 재배포 프로파일	
이름	프로파일 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
IPv4 정적	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
활성화(기본값) 또는 비활성화	프로파일의 IPv4 정적 부분을 활성화합니다.

RIPv2 라우팅 프로파일	설명
미터법	RIPv2(범위는 1~65,535)로 재배포되는 고정 경로에 적용할 메트릭을 지정합니다.
경로 맵	재배포 경로 맵을 선택하거나 생성하여 RIPv2에 재배포할 IPv4 정적 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
연결됨	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
활성화(기본값) 또는 비활성화	프로파일의 연결된 부분을 사용하도록 설정합니다.
미터법	RIPv2로 재배포되는 연결된 경로에 적용할 메트릭을 지정합니다(범위는 1~65,535).
경로 맵	재배포 경로 맵을 선택하거나 생성하여 RIPv2에 재배포할 연결된 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
BGP AFI IPv4	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
활성화(기본값) 또는 비활성화	프로파일의 BGP AFI IPv4 부분을 활성화합니다.
미터법	RIPv2로 재배포되는 BGP IPv4 경로에 적용할 메트릭을 지정합니다(범위는 0~4,294,967,295).
경로 맵	재배포 경로 맵을 선택하거나 생성하여 RIPv2에 재배포할 BGP IPv4 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면

RIPv2 라우팅 프로파일	설명
	이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
OSPFv2	프로파일의 이 부분의 구성을 허용하려면 선택합니다.
활성화(기본값) 또는 비활성화	프로파일의 OSPFv2 부분을 활성화합니다.
미터법	RIPv2로 재배포되는 OSPFv2 경로에 적용할 지표를 지정합니다(범위는 0~4,294,967,295).
경로 맵	재배포 경로 맵을 선택하거나 생성하여 RIPv2에 재배포할 OSPFv2 경로를 제어하고 해당 속성을 설정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.

네트워크 > 라우팅 > 라우팅 프로파일 > 필터

프로파일에 적용할 필터를 추가하십시오. 예를 들어, RIB로의 경로 승인, 피어에 대한 경로 광고, 조건부 광고, 속성 설정, 경로 집계 및 경로 재분배 등을 제어하는 설정을 쉽고 일관되게 적용하십시오.

필터	설명
필터 액세스 목록	
이름	액세스 목록의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
설명	설명을 입력합니다.
유형	**IPv4** 또는 **IPv6**을 선택합니다.
시퀀스	항목(규칙)을 추가하고 이 액세스 목록에 대한 규칙 목록에 규칙의 순서 번호를 입력합니다. 범위는 1~65,535입니다.

필터	설명
	나중에 추가 규칙을 삽입할 수 있도록 시퀀스 번호 사이에 사용하지 않는 번호를 남겨둡니다.
동작	항목에 대해 거부 또는 허용을 선택합니다. 액세스 목록은 암시적 **Deny Any**로 끝납니다.
소스 주소	(IPv4만 해당) 다음 중 하나를 선택합니다. • 주소 - 다음 주소 필드에 IPv4 주소를 입력하고 와일드카드 마스크를 입력하여 주소 범위를 나타냅니다. 마스크의 영(0)은 비트가 주소의 해당 비트와 일치해야 함을 나타냅니다. 마스크의 일(1)은 "관심 없음" 비트를 나타냅니다. • 모두 선택 • 없음
대상 주소	(IPv4만 해당) 다음 중 하나를 선택합니다. • 주소 - 다음 주소 필드에 IPv4 주소를 입력하고 와일드카드 마스크를 입력하여 주소 범위를 나타냅니다. 마스크의 영(0)은 비트가 주소의 해당 비트와 일치해야 함을 나타냅니다. 마스크의 일(1)은 "관심 없음" 비트를 나타냅니다. • 모두 선택 • 없음
소스 주소	(IPv6만 해당) 다음 중 하나를 선택합니다. • 주소 - 다음 주소 필드에 IPv6 주소를 입력합니다. • 모두 선택 • 없음
이 주소와 정확히 일치	(IPv6 전용) IPv6 소스 주소와 정확히 일치하는 항목만 일치시키려면 선택합니다. 소스 주소가 임의 또는 없음인 경우 사용할 수 없습니다.
필터 접두사 목록	
이름	접두사 목록의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.

필터	설명
설명	설명을 입력합니다.
유형	**IPv4** 또는 **IPv6**을 선택합니다.
시퀀스	항목(규칙)을 추가하고 이 접두사 목록에 대한 규칙 목록에 규칙의 시퀀스 번호를 입력합니다. 범위는 1~65,535입니다. 나중에 추가 규칙을 삽입할 수 있도록 시퀀스 번호 사이에 사용하지 않는 번호를 남겨둡니다.
동작	항목에 대해 거부 또는 허용을 선택합니다. 접두사 목록은 암시적 **Deny Any**로 끝납니다.
프리픽스	다음 중 하나를 선택합니다. • 모든 네트워크 • 항목 - 슬래시 및 접두사 길이를 사용하여 IPv4 또는 IPv6 네트워크를 입력합니다. 선택적으로 접두사가 크거나 같아야 하는 접두사 길이를 입력합니다(범위는 IPv4의 경우 0 ~ 32, IPv6의 경우 0 ~ 128). 선택적으로 접두사가 작거나 같아야 하는 접두사 길이를 입력합니다(범위는 IPv4의 경우 0~32, IPv6의 경우 0~128). 예를 들어, 접두사 길이가 25보다 크거나 같음 접두사 길이가 26보다 작거나 같은 네트워크 192.168.3.0/24를 입력합니다. • 없음
필터 **AS** 경로 액세스 목록	
이름	AS_Path 액세스 목록의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
설명	설명을 입력합니다.
시퀀스	항목(규칙)을 추가하고 이 액세스 목록에 대한 규칙 목록에 규칙의 순서 번호를 입력합니다. 범위는 1~65,535입니다. 나중에 추가 규칙을 삽입할 수 있도록 시퀀스 번호 사이에 사용하지 않는 번호를 남겨둡니다.

필터	설명
동작	항목에 대해 거부 또는 허용을 선택합니다. *AS Path* 액세스 목록은 암시적 ***Permit Any*** 규칙으로 끝납니다. *AS Path* 액세스 목록을 사용하여 자율 시스템을 거부합니다.
Aspath 정규식	AS_PATH에 대한 정규식을 입력하십시오.
필터 커뮤니티 목록	
이름	커뮤니티 목록의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
설명	커뮤니티 목록에 대한 설명을 입력합니다.
유형	일반, 대형 또는 확장 커뮤니티를 선택합니다.
시퀀스	항목(규칙)을 추가하고 이 목록의 규칙 목록에 규칙의 시퀀스 번호를 입력합니다. 범위는 1~65,535입니다. 나중에 추가 규칙을 삽입할 수 있도록 시퀀스 번호 사이에 사용하지 않는 번호를 남겨둡니다.
동작	거부 또는 허용을 선택합니다. 목록은 암시적 **Deny Any**로 끝납니다.
지역 사회	목록에서 잘 알려진 커뮤니티 중 하나를 선택하거나 커뮤니티를 입력합니다.
필터 경로 맵 **BGP**	
이름	BGP 경로 맵의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
설명	경로 맵에 대한 설명을 입력합니다.
입력 탭	

필터	설명
시퀀스	항목(규칙)을 추가하고 이 경로 맵에 대한 규칙 목록에 규칙의 시퀀스 번호를 입력합니다. 범위는 1~65,535입니다.  나중에 추가 규칙을 삽입할 수 있도록 시퀀스 번호 사이에 사용하지 않는 번호를 남겨둡니다.
설명	경로 맵 항목에 대한 설명을 입력합니다.
동작	거부 또는 허용을 선택합니다.
일치 탭	
AS Path 액세스 목록	AS Path 액세스 목록을 선택하십시오.
일반 커뮤니티	일치 기준에 대한 커뮤니티 목록을 선택하십시오.
대규모 커뮤니티	일치 기준에 대한 커뮤니티 목록을 선택하십시오.
확장된 커뮤니티	일치 기준에 대한 커뮤니티 목록을 선택하십시오.
미터법	메트릭을 입력하십시오. 범위는 0~4,294,967,295입니다.
상호 작용	인터페이스를 선택합니다.
원점	**egp**, **igp**, 불완전 또는 없음을 선택합니다.
태그	태그를 입력하십시오. 범위는 1~4,294,967,295입니다.
로컬 선호	로컬 환경 설정을 입력하십시오. 범위는 0~4,294,967,295입니다.
피어	로컬(정적 또는 재분배 경로) 또는 없음을 선택합니다.
IPv4 또는 IPv6	일치시킬 주소 패밀리로 **IPv4** 또는 **IPv6**을 선택합니다.
주소 - 액세스 목록	일치시킬 주소를 지정하는 생성한 액세스 목록을 선택합니다. 기본값은 없음입니다.
주소 - 접두사 목록	일치시킬 접두사를 지정하는 생성한 접두사 목록을 선택합니다. 피어로부터 받았거나 다른 프로토콜에서 재배포된 접두사와 일치합니다. 기본값은 없음입니다.

필터	설명
다음 홉 - 액세스 목록	일치시킬 다음 홉을 지정하는 생성한 액세스 목록을 선택합니다. 기본값은 없음입니다.
다음 홉 - 접두사 목록	일치시킬 다음 홉을 지정하기 위해 생성한 접두사 목록을 선택합니다. 기본값은 없음입니다.
경로 소스 - 액세스 목록	(IPv4만 해당) 일치시킬 경로 소스를 지정하는 생성한 액세스 목록을 선택하십시오. 기본값은 없음입니다.
경로 소스 - 접두사 목록	(IPv4 전용) 일치시킬 경로 소스를 지정하는 접두사 목록을 선택하십시오. 기본값은 없음입니다.
탭 설정	
BGP 원자 집계 사용	경로가 집계되었으므로 덜 구체적인 경로로 표시합니다. ATOMIC_AGGREGATE는 경로를 따라 BGP 스피커에게 경로 집계로 인해 정보가 손실되었음을 알리는 잘 알려진 임의 속성이므로 집계 경로가 대상에 대한 최상의 경로가 아닐 수 있습니다. 일부 라우터가 Aggregator에 의해 집계되면 Aggregator는 해당 Router-ID를 집계된 경로에 AGGREGATOR-ID 속성에 연결하고 집계된 라우터의 AS_PATH 정보가 보존되었는지 여부에 따라 ATOMIC_AGGREGATE 속성을 설정합니다.
집계자 - 집계 AS	Aggregator AS를 입력합니다. Aggregator 속성에는 AS 번호와 집계된 경로를 생성한 라우터의 IP 주소가 포함됩니다. IP 주소는 경로 집계를 수행하는 라우터의 라우터 ID입니다. 범위는 1~4,294,967,295입니다.
애그리게이터 - 라우터 ID	애그리게이터의 라우터 ID(일반적으로 루프백 주소)를 입력합니다.
IPv4 또는 IPv6	설정할 주소 유형을 선택합니다.
IPv6 Nexthop은 전체 주소를 선호합니다.	(IPv6만 해당) IPv6에는 링크 로컬 주소, 전역 유니캐스트 주소, 애니캐스트 주소 및 멀티캐스트 주소의 네 가지 주소 유형이 있습니다. **IPv6 Nexthop** 선호 전역 주소는 방화벽이 전역 유니캐스트 주소를 선호하도록 합니다.
소스 주소	설정할 소스 주소를 /접두어 길이로 선택합니다.

필터	설명
IPv4 넥스트 홉	(IPv4 전용) 없음, 피어 주소(피어 주소 사용) 또는 변경되지 않음을 선택합니다.
IPv6 넥스트 홉	(IPv6 전용) 없음 또는 피어 주소(피어 주소 사용)를 선택합니다.
로컬 선호	로컬 환경 설정을 입력하십시오. 범위는 0~4,294,967,295입니다.
태그	태그를 입력하십시오. 범위는 1~4,294,967,295입니다.
메트릭 작업	없음, 설정, 더하기 또는 빼기를 선택합니다.
메트릭 값	메트릭을 입력하십시오. 범위는 0~4,294,967,295입니다.
무게	가중치를 입력하십시오. 범위는 0~4,294,967,295입니다.
원점	**egp**, **igp**, 불완전 또는 없음을 선택합니다.
발신자 ID	발신자 ID를 설정합니다.
일반 커뮤니티 삭제	삭제할 일반 커뮤니티를 입력하세요.
대규모 커뮤니티 삭제	삭제할 대규모 커뮤니티를 입력하세요.
일반 커뮤니티 - 일반 커뮤니티 덮어쓰기	일반 커뮤니티 필드에 추가된 내용으로 일반 커뮤니티를 덮어쓰려면 선택합니다.
일반 커뮤니티	일반 커뮤니티를 추가합니다.
대규모 커뮤니티 - 일반 커뮤니티 덮어쓰기	대규모 커뮤니티 필드에 추가된 내용으로 대규모 커뮤니티를 덮어쓰려면 선택합니다.
대규모 커뮤니티	대규모 커뮤니티를 추가합니다.
ASPPath 제외	제외할 AS_PATH를 추가합니다.
ASPPath 추가	앞에 추가할 AS_PATH를 추가합니다.
필터 경로 맵 재배포	

필터	설명
이름	재배포 경로 프로파일의 이름을 입력합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
설명	경로 맵에 대한 설명을 입력합니다.
소스 프로토콜	재배포되는 소스 프로토콜을 선택하십시오.
대상 프로토콜	경로를 재배포할 프로토콜을 선택하십시오.
입력	
시퀀스	시퀀스 번호를 입력하십시오. 범위는 1~65,535입니다. 나중에 추가 규칙을 삽입할 수 있도록 시퀀스 번호 사이에 사용하지 않는 번호를 남겨둡니다.
설명	경로 맵 규칙에 대한 설명을 입력합니다.
동작	일치하는 경로가 재배포되는 것을 거부하거나 허용합니다.
일치	
AS Path 액세스 목록	AS Path 액세스 목록을 선택하십시오.
일반 커뮤니티	일반 커뮤니티에 들어가십시오.
대규모 커뮤니티	대규모 커뮤니티에 들어가십시오.
확장된 커뮤니티	확장된 커뮤니티에 참여
미터법	범위는 0~4,294,967,295입니다.
상호 작용	인터페이스를 선택합니다.
원점	**egp**, **igp**, 불완전 또는 없음을 선택합니다.
태그	태그를 입력하십시오. 범위는 1~4,294,967,295입니다.

필터	설명
로컬 선호	로컬 환경 설정을 입력하십시오. 범위는 0~4,294,967,295입니다.
피어	로컬 (정적 또는 재분배 경로) 또는 없음을 선택합니다.
주소 - 액세스 목록	액세스 목록을 선택합니다.
주소 - 접두사 목록	접두사 목록을 선택합니다.
다음 홉 - 액세스 목록	액세스 목록을 선택합니다.
다음 홉 - 접두사 목록	접두사 목록을 선택합니다.
경로 소스 - 액세스 목록	액세스 목록을 선택합니다.
경로 소스 - 접두사 목록	접두사 목록을 선택합니다.
세트	
메트릭 작업	없음, 설정, 더하기 또는 빼기를 선택합니다.
메트릭 값	메트릭 작업에 대한 선택에 따라 메트릭을 설정할 값을 입력하거나 메트릭에 추가하거나 일치하는 경로의 메트릭에서 뺍니다. 범위는 0~4,294,967,295입니다.
메트릭 유형	유형 **1** 또는 유형 **2**를 선택합니다.
태그	범위는 1~4,294,967,295입니다.

네트워크 > 라우팅 > 라우팅 프로파일 > 멀티캐스트

멀티캐스트 라우팅 프로파일을 추가하여 논리적 라우터에 대한 IPv4 멀티캐스트를 효율적으로 구성합니다.

멀티캐스트 라우팅 프로파일	설명
멀티캐스트 **IPv4 PIM** 인터페이스 타이머 프로파일	
이름	프로파일 이름을 입력합니다(최대 31자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는

멀티캐스트 라우팅 프로파일	설명
	하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
어설션 인터벌	논리적 라우터가 PIM 전달자를 선택할 때 다중 액세스 네트워크의 다른 PIM 라우터로 보내는 PIM Assert 메시지 사이의 시간(초)을 입력합니다. 범위는 1~65,534이며 기본값은 177입니다.
헬로 인터벌	논리 라우터가 인터페이스 그룹의 각 인터페이스에서 PIM 이웃으로 보내는 PIM Hello 메시지 사이의 시간(초)을 입력합니다. 범위는 1~180입니다. 기본값은 30입니다.
조인 정리 인터벌	논리 라우터가 멀티캐스트 소스를 향해 업스트림으로 보내는 PIM 조인 메시지 간(및 PIM 정리 메시지 간) 시간(초)을 입력합니다. 범위는 60~600입니다. 기본값은 60입니다.
멀티캐스트 **IPv4 IGMP** 인터페이스 쿼리 프로파일	
이름	프로파일 이름을 입력합니다(최대 31자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-)을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 허용되지 않습니다.
최대 쿼리 응답 시간	논리적 라우터가 수신자가 그룹에 대한 멀티캐스트 패킷을 더 이상 수신하기를 원하지 않는다고 결정하기 전에 수신자가 IGMP 구성원 쿼리 메시지에 응답하는 데 허용되는 최대 시간(초)을 입력합니다. 범위는 1~25입니다. 기본값은 10입니다.
쿼리 간격	수신기가 그룹에 대한 멀티캐스트 패킷을 수신하기를 원하는지 여부를 결정하기 위해 논리적 라우터가 수신기에 보내는 IGMP 멤버십 쿼리 메시지 사이의 시간(초)을 입력합니다. 범위는 1~1,800까지입니다. 기본값은 125입니다.
마지막 멤버 쿼리 간격	수신자가 그룹 탈퇴 메시지를 보낸 후 논리 라우터가 전송하는 그룹별 쿼리에 수신자가 응답할 수 있는 시간(초)을 입력합니다. 범위는 1~25입니다. 기본값은 1입니다.
탈퇴 메시지 수신 즉시 그룹 탈퇴	이 기능을 활성화하면 멀티캐스트 그룹에 구성원이 하나만 있고 논리적 라우터가 해당 그룹에 대한 IGMP Leave 메시지를 수신할 때 이 설정은 논리적 라우터가 mRIB(멀티캐스트 라우팅 정보 기반) 및 마지막 구성원 쿼리 간격이 만료되기를 기다리지 않고 즉시 멀티캐스트 포워딩 정보 베이스(mFIB)에서 해당 그룹과 나가

멀티캐스트 라우팅 프로파일	설명
	는 인터페이스를 제거하도록 합니다. 이 설정을 사용하면 네트워크 리소스가 절약됩니다. 기본값은 비활성화입니다.
멀티캐스트 **MDSP** 인증 프로필	
이름	이름으로 MSDP 인증 프로필을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
비밀	암호를 입력합니다(영숫자 문자, !, @, #, % 및 ^ 허용됨). 암호를 확인합니다.
멀티캐스트 **MDSP** 타이머 프로필	
이름	이름으로 MSDP 타이머 프로필을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
연결 유지 인터벌	값을 초 단위로 입력합니다. 범위는 1~60이고 기본값은 60입니다. MSDP 전송 연결이 피어와 설정된 후 연결의 각 측은 MSDP 세션을 활성 상태로 유지하기 위해 이 인터벌로 Keepalive 메시지를 다른 측에 전송합니다. 타이머가 만료되면 피어는 Keepalive 메시지를 보내고 타이머를 재설정합니다. 메시지 시간 초과 인터벌 동안 Keepalive 또는 SA 메시지가 수신되지 않으면 MSDP 세션이 재설정됩니다.
메시지 시간 초과	값을 초 단위로 입력합니다. 이 인터벌은 MSDP 피어가 다른 피어의 Keepalive 메시지를 기다렸다가 다운을 선언하는 인터벌입니다. 범위는 1~75입니다. 기본값은 75입니다.
연결 재시도 간격	값을 초 단위로 입력합니다. 이 인터벌은 피어링 세션이 재설정된 후 피어가 피어링 세션을 재설정하기 전에 대기하는 인터벌입니다. 범위는 1~60입니다. 기본값은 30입니다.

네트워크 > IPSec 터널

네트워크 > **IPSec** 터널을 선택하여 방화벽 간에 IPSec VPN 터널을 설정하고 관리합니다. 이것은 IKE/IPSec VPN 설정의 2단계 부분입니다.

무엇을 찾고 계신가요?	참조:
IPSec VPN 터널을 관리합니다.	IPSec VPN 터널 관리
IPSec 터널을 구성합니다.	IPSec 터널 일반 탭
	IPSec 터널 프록시 ID 탭
IPSec 터널 상태를 봅니다.	방화벽의 IPSec 터널 상태
IPSec 터널을 다시 시작하거나 새로 고칩니다.	IPSec 터널 다시 시작 또는 새로 고침
더 찾고 계십니까?	IPSec 터널을 설정합니다.

IPSec VPN 터널 관리

- 네트워크 > IPSec 터널

다음 표에서는 IPSec VPN 터널을 관리하는 방법을 설명합니다.

IPSec VPN 터널을 관리하는 필드	
추가하다	새 IPSec VPN 터널을 추가합니다. 새 터널 구성에 대한 지침은 IPSec 터널 일반 탭을 참조하십시오.
삭제	더 이상 필요하지 않은 터널을 삭제합니다.
활성화	비활성화된 터널을 활성화합니다(터널은 기본적으로 활성화되어 있음).
비활성화	사용하고 싶지 않지만 아직 삭제할 준비가 되지 않은 터널을 비활성화합니다.
PDF/CSV	IPSec 터널 구성을 **PDF/CSV** 형식으로 내보냅니다. 필터를 적용하여 테이블 출력을 사용자 정의하고 필요한 열만 포함할 수 있습니다. 내보내기 대화 상자에 표시되는 열만 내보내집니다. 구성 테이블 데이터 내보내기를 참조하십시오.

IPSec 터널 일반 탭

- 네트워크 > IPSec 터널 > 일반

다음 필드를 사용하여 IPSec 터널을 설정합니다.

IPSec 터널 일반 설정	설명
이름	터널을 식별할 이름을 입력합니다(최대 63자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. 이 필드의 63자 제한에는 콜론 문자로 구분된 프록시 ID 외에 터널 이름도 포함됩니다.
터널 인터페이스	기존 터널 인터페이스를 선택하거나 새 터널 인터페이스를 클릭합니다. 터널 인터페이스 생성에 대한 자세한 내용은 네트워크 > 인터페이스 > 터널을 참조하세요.
IPv4 또는 IPv6	**IPv4** 또는 **IPv6**을 선택하여 해당 IP 유형의 주소를 가진 엔드포인트를 갖도록 터널을 구성합니다.
유형	자동 생성된 보안 키를 사용할지 수동으로 입력한 보안 키를 사용할지 선택합니다. 자동 키를 사용하는 것이 좋습니다.
자동 키	자동 키를 선택하는 경우 다음을 지정합니다. • **IKE** 게이트웨이 - IKE 게이트웨이 설정에 대한 설명은 네트워크 > 네트워크 프로파일 > IKE 게이트웨이를 참조하십시오. • **IPSec** 암호화 프로파일 - 기존 프로파일을 선택하거나 기본 프로파일을 유지합니다. 새 프로파일을 정의하려면 새로 만들기를 클릭하고 네트워크 > 네트워크 프로파일 > IPSec 암호화의 지침을 따릅니다. • 나머지 필드에 액세스하려면 **Advanced** 옵션 표시를 클릭합니다. • **Enable Replay Protection(**재전송 보호 활성화**)** - 재전송 공격으로부터 보호하려면 선택합니다. 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 유지

IPSec 터널 일반 설정	설명
	하고, 검증된 수신 패킷의 시퀀스 번호 기록을 유지하며, 슬라이딩 윈도우(너무 오래된 패킷) 또는 슬라이딩 창에 이미 나타나는 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. 재전송 방지를 활성화한 경우 사용할 재전송 방지 윈도우를 선택합니다. 재전송 방지 윈도우 크기를 64, 128, 256, 512, 1024, 2048 또는 4096 중에서 선택할 수 있습니다. 기본값은 1024입니다. • **TOS** 헤더 복사 - 원래 TOS 정보를 보존하기 위해 (서비스 유형) TOS 필드를 내부 IP 헤더에서 캡슐화된 패킷의 외부 IP 헤더로 복사합니다. 이렇게 하면 ECN(명시적 혼잡 알림) 필드도 복사됩니다. • **IPSec** 모드 - IPSec 모드를 지정합니다. 헤더를 포함한 전체 패킷을 암호화하려면 터널 모드를 선택합니다. 암호화 후 패킷에 새 IP 헤더가 추가됩니다. 페이로드만 암호화하고 원래 IP 헤더는 유지하려면 전송 모드를 선택합니다. • **GRE** 캡슐화 추가 - IPSec 터널에 캡슐화된 GRE 헤더를 추가하려면 선택합니다. 방화벽은 다른 공급자 터널 엔드포인트와의 상호 운용성을 위해 IPSec 헤더 뒤에 GRE 헤더를 생성하므로 GRE 터널을 IPSec 터널과 공유합니다. • **Tunnel Monitor(**터널 모니터**)** - 디바이스 관리자에게 터널 오류를 알리고 다른 인터페이스에 대한 자동 페일오버를 제공하려면 선택합니다. 모니터링을 위해 터널 인터페이스에 *IP* 주소를 할당해야 합니다. • 대상 **IP** - 터널 모니터가 터널이 제대로 작동하는지 확인하는 데 사용할 터널 반대쪽의 IP 주소를 지정합니다. • 프로파일 - 터널이 실패할 경우 수행할 작업을 결정할 기존 프로파일을 선택합니다. 모니터 프로파일에 지정된 작업이 대기 복구인 경우 방화벽은 터널이 작동할 때까지 기다리며 경로 테이블을 사용하여 대체 경로를 찾지 않습니다. 페일오버(failover) 작업을 사용하는 경우 방화벽은 경로 테이블을 확인하여 대상에 도달하는 데 사용할 수 있는 대체 경로가 있는지 확인합니다. 자세한 내용은 네트워크 > 네트워크 프로파일 > 모니터를 참조하십시오.
수동 키	수동 키를 선택하는 경우 다음을 지정합니다. • 로컬 **SPI** - 로컬 방화벽에서 피어로의 패킷 통과를 위한 로컬 SPI(보안 매개변수 인덱스)를 지정합니다. SPI는 IPSec 트래픽 플로우를 구분하

IPSec 터널 일반 설정	설명
	는 데 도움이 되도록 IPSec 터널링용 헤더에 추가되는 16진수 인덱스입니다. • 인터페이스 - 터널 엔드포인트인 인터페이스를 선택합니다. • 로컬 주소 - 터널의 엔드포인트인 로컬 인터페이스의 IP 주소를 선택합니다. • 원격 **SPI** - 원격 방화벽에서 피어로의 패킷 통과를 위한 원격 보안 매개변수 인덱스(SPI)를 지정합니다. • 프로토콜 - 터널(**ESP** 또는 **AH**)을 통한 트래픽에 대한 프로토콜을 선택합니다. • 인증 - 터널 액세스에 대한 인증 유형(**SHA1**, **SHA256**, **SHA384**, **SHA512**, **MD5** 또는 없음)을 선택합니다. • 키/키 확인 - 인증 키를 입력하고 확인합니다. • 암호화 - 터널 트래픽에 대한 암호화 옵션을 선택합니다(**3des**, **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **des** 또는 **null**[암호화 없음]). • 키/키 확인 - 암호화 키를 입력하고 확인합니다.
GlobalProtect Satellite	**GlobalProtect Satellite**를 선택하는 경우 다음을 지정합니다. • 이름 - 터널을 식별하는 이름을 입력합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. • 터널 인터페이스 - 기존 터널 인터페이스를 선택하거나 새 터널 인터페이스를 클릭합니다. • 포털 주소 - GlobalProtect™ 포털의 IP 주소를 입력합니다. • 인터페이스 - GlobalProtect 포털에 도달하기 위한 이그레스(egress) 인터페이스인 드롭다운에서 인터페이스를 선택합니다. • 로컬 **IP** 주소 - GlobalProtect 포털에 연결하는 이그레스(egress) 인터페이스의 IP 주소를 입력합니다. • **Advanced** 옵션 • 게이트웨이에 모든 고정 및 연결된 경로 게시 - 새틀라이트에서 이 새틀라이트이 연결된 GlobalProtect 게이트웨이로의 모든 경로를 게시하려면 선택합니다. • 서브넷 - 추가를 클릭하여 새틀라이트 위치에 대한 로컬 서브넷을 수동으로 추가합니다. 다른 새틀라이트이 동일한 서브넷 정보를 사용하는 경우 터널 인터페이스 IP에 대한 모든 트래픽에 대해 NAT를 해야 합니다. 또한 이 경우 새틀라이트은 경로를 공유하지 않아야 하므로 모든 라우팅은 터널 IP를 통해 수행됩니다.

IPSec 터널 일반 설정	설명
	• 외부 인증 기관 - 외부 CA를 사용하여 인증서를 관리할지의 여부를 선택합니다. 인증서가 생성되면 새틀라이트로 가져와서 로컬 인증서와 인증서 프로파일을 선택해야 합니다.

IPSec 터널 프록시 ID 탭

- 네트워크 > IPSec 터널 > 프록시 ID

IPSec 터널 프록시 **ID** 탭은 두 개의 탭으로 구분됩니다. **IPv4** 및 **IPv6**. 도움말은 두 유형 모두 비슷합니다. IPv4와 IPv6의 차이점은 다음 표의 로컬 및 원격 필드에 설명되어 있습니다.

IPSec 터널 프록시 **ID** 탭은 IKEv2에 대한 트래픽 선택기를 지정하는 데도 사용됩니다.

프록시 **ID IPv4** 및 **IPv6** 설정	설명
프록시 ID	추가를 클릭하고 프록시를 식별할 이름을 입력합니다. IKEv2 트래픽 선택기의 경우 이 필드가 이름으로 사용됩니다.
로컬	IPv4의 경우: xxxx/mask 형식(예: 10.1.2.0/24)으로 IP 주소 또는 서브넷을 입력합니다. IPv6의 경우: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length 형식(또는 IPv6 규칙에 따라(예: 2001:DB8:0::/48))으로 IP 주소와 프리픽스 길이를 입력합니다. IPv6 주소 지정에서는 모든 0을 쓸 필요가 없습니다. 선행 0은 생략할 수 있고 연속 0의 그룹 하나는 인접한 두 개의 콜론(::)으로 대체할 수 있습니다. IKEv2 트래픽 선택기의 경우 이 필드는 소스 IP 주소로 변환됩니다.
원격	피어가 요구하는 경우: IPv4의 경우 xxxx/mask 형식으로 IP 주소 또는 서브넷을 입력합니다(예: 10.1.1.0/24). IPv6의 경우 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length 형식으로 IP 주소와 프리픽스 길이를 입력합니다(또는 IPv6 규칙에 따라(예: 2001:DB8:55::/48)). IKEv2 트래픽 선택기의 경우 이 필드는 대상 IP 주소로 변환됩니다.
프로토콜	로컬 및 원격 포트에 대한 프로토콜 및 포트 번호를 지정합니다.

프록시 **ID IPv4** 및 **IPv6** 설정	설명
	번호 - 프로토콜 번호를 지정합니다(타사 디바이스와의 상호 운용성을 위해 사용됨). • 모두 - TCP 및/또는 UDP 트래픽을 허용합니다. • **TCP** - 로컬 및 원격 TCP 포트 번호를 지정합니다. • **UDP** - 로컬 및 원격 UDP 포트 번호를 지정합니다. 구성된 각 프록시 ID는 방화벽의 IPSec VPN 터널 용량에 포함됩니다. 이 필드는 IKEv2 트래픽 선택기로도 사용됩니다.

방화벽의 IPSec 터널 상태

- 네트워크 > IPSec 터널

현재 정의된 IPSec VPN 터널의 상태를 보려면 **IPSec** 터널 페이지를 여십시오. 다음 상태 정보가 페이지에 보고됩니다.

- 터널 상태(첫 번째 상태 열) - 녹색은 IPSec 2단계 SA(보안 연결) 터널을 나타냅니다. 빨간색은 IPSec 2단계 SA를 사용할 수 없거나 만료되었음을 나타냅니다.
- IKE 게이트웨이 상태 - 녹색은 유효한 IKE 1단계 SA 또는 IKEv2 IKE SA를 나타냅니다. 빨간색은 IKE 1단계 SA를 사용할 수 없거나 만료되었음을 나타냅니다.
- 터널 인터페이스 상태 - 녹색은 터널 인터페이스가 작동 중임을 나타냅니다(터널 모니터가 비활성화되었거나 터널 모니터가 작동 상태이고 모니터링 IP 주소에 연결할 수 있기 때문). 빨간색은 터널 모니터가 활성화되어 있고 원격 터널 모니터링 IP 주소에 연결할 수 없기 때문에 터널 인터페이스가 다운되었음을 나타냅니다.

IPSec 터널 다시 시작 또는 새로 고침

- 네트워크 > IPSec 터널

Network > **IPSec Tunnels**를 선택하여 터널의 상태를 표시합니다. 첫 번째 상태 열에는 터널 정보에 대한 링크가 있습니다. 다시 시작하거나 새로 고치려는 터널을 클릭하여 해당 터널에 대한 터널 정보 페이지를 엽니다. 목록에서 항목 중 하나를 클릭하고 다음을 클릭합니다.

- 다시 시작 - 선택한 터널을 다시 시작합니다. 다시 시작하면 터널을 가로질러 가는 트래픽이 중단됩니다.
- 새로 고침 - 현재 IPSec SA 상태를 표시합니다.

네트워크 > GRE 터널

GRE(Generic Routing Encapsulation) 터널 프로토콜은 페이로드 프로토콜을 캡슐화하는 캐리어 프로토콜입니다. GRE 패킷 자체는 전송 프로토콜(IPv4 또는 IPv6)로 캡슐화됩니다. GRE 터널은 방화벽과 라우터(또는 다른 방화벽) 사이의 지점 간 논리적 링크에서 두 엔드포인트를 연결합니다. Palo Alto Networks 방화벽은 GRE 터널 종료를 지원합니다.

무엇을 찾고 계신가요?	참조:
GRE 터널의 빌딩 블록	GRE 터널
다른 공급자의 터널 엔드포인트과 상호 운용성을 제공하는 방법	IPSec 터널을 생성할 때 **GRE** 캡슐화 추가를 선택합니다.
더 찾고 계십니까?	GRE 터널

GRE 터널

- 네트워크 > GRE 터널

먼저 터널 인터페이스를 구성합니다(네트워크 > 인터페이스 > 터널). 그런 다음 일반 라우팅 캡슐화(GRE) 터널을 추가하고 생성한 터널 인터페이스를 참조하여 다음 정보를 제공합니다.

GRE 터널 필드	설명
이름	GRE 터널의 이름.
상호 작용	이더넷 인터페이스 또는 하위 인터페이스, 통합 이더넷(AE) 인터페이스, 루프백 인터페이스 또는 VLAN 인터페이스인 로컬 GRE 터널 엔드포인트(소스 인터페이스)로 사용할 인터페이스를 선택합니다.
지역 주소	터널 인터페이스 주소로 사용할 인터페이스의 로컬 IP 주소를 선택합니다.
피어 주소	GRE 터널의 반대쪽 끝에 있는 IP 주소를 입력합니다.

GRE 터널 필드	설명
터널 인터페이스	구성한 터널 인터페이스를 선택합니다. (이 인터페이스는 라우팅을 위한 다음 홉일 때 터널을 식별합니다.)
TTL	GRE 패킷에 캡슐화된 IP 패킷의 TTL을 입력합니다(범위는 1~255, 기본값은 64).
ERSPAN	방화벽이 GRE 터널을 통해 전송되는 캡슐화된 원격 스위치 포트 분석기(ERSPAN) 데이터를 캡슐화하도록 하려면 선택합니다. ERSPAN을 사용하여 GRE 터널을 통해 미러링된 트래픽을 방화벽으로 전송하여 IoT Security와 같은 보안 서비스에서 사용하도록 네트워크 스위치를 구성할 수 있습니다. 방화벽은 데이터를 캡슐화한 후 TAP 포트에서 수신된 트래픽을 검사하는 방법과 유사하게 데이터를 검사합니다. 그런 다음 향상된 애플리케이션 로그(EAL) 및 트래픽, 위협, WildFire, URL, 데이터, GTP(GTP가 활성화된 경우), SCTP(SCTP가 활성화된 경우), 터널, 인증 및 암호 해독 로그를 만듭니다. 방화벽은 이러한 로그를 IoT Security가 데이터에 액세스하고 분석하는 로깅 서비스로 전달합니다.
ToS 헤더 복사	원래 ToS 정보를 보존하기 위해 캡슐화된 패킷의 내부 IP 헤더에서 외부 IP 헤더로 서비스 유형(ToS) 필드를 복사하려면 선택합니다.
Keep Alive	GRE 터널에 대해 Keep Alive 기능을 활성화하려면 선택합니다(기본적으로 비활성화됨). Keep Alive를 활성화하면 기본적으로 GRE 터널이 작동 중지되는 데 10초 인터벌으로 3회의 미반환 Keepalive 패킷(재시도)이 필요하고 GRE 터널이 다시 작동하는 데 10초 인터벌으로 5회의 Hold Timer 인터벌이 필요합니다.
인터벌(초)	GRE 터널의 로컬 끝이 터널 피어로 보내는 keepalive 패킷 사이의 인터벌과 방화벽이 터널 피어와의 통신을 다시 설정하기 전에 성공적인 keepalive 패킷 후 각 Hold Timer가 대기하는 인

GRE 터널 필드	설명
	터벌을 설정합니다(범위는 1~50입니다. 기본값은 10)입니다.
재시도	방화벽이 터널 피어가 다운된 것으로 간주하기 전에 연결 유지 패킷이 반환되지 않는 인터벌 수를 설정합니다(범위는 1~255, 기본값은 3).
홀드 타이머	방화벽이 터널 피어와의 통신을 다시 설정하기 전에 연결 유지 패킷이 성공하는 인터벌 수를 설정합니다(범위는 1~64, 기본값은 5).

네트워크 > DHCP

DHCP(동적 호스트 구성 프로토콜)는 TCP/IP 네트워크에서 동적으로 구성된 호스트에 TCP/IP 및 링크 레이어 구성 매개변수와 네트워크 주소를 제공하는 표준화된 프로토콜입니다. Palo Alto Networks 방화벽의 인터페이스는 DHCP 서버, 클라이언트 또는 중계 에이전트로 작동할 수 있습니다. 이러한 역할을 다른 인터페이스에 할당하면 방화벽이 여러 역할을 수행할 수 있습니다.

무엇을 찾고 계신가요?	참조:
DHCP란 무엇입니까?	DHCP 개요
DHCP 서버는 어떻게 주소를 할당합니까?	DHCP 주소 지정
방화벽에서 다음과 같이 작동하도록 인터페이스를 구성합니다.	
	DHCP 서버
	DHCP 릴레이
	DNS 프록시
더 찾고 계십니까?	DHCP

DHCP 개요

- 네트워크 > DHCP

DHCP는 클라이언트-서버 통신 모델을 사용합니다. 이 모델은 방화벽이 수행할 수 있는 세 가지 역할로 구성됩니다. DHCP 클라이언트, DHCP 서버 및 DHCP 릴레이 에이전트.

- DHCP 클라이언트(호스트) 역할을 하는 방화벽은 DHCP 서버에서 IP 주소 및 기타 구성 설정을 요청할 수 있습니다. 클라이언트 방화벽의 사용자는 구성 시간과 노력을 절약하고 네트워크의 주소 지정 계획이나 DHCP 서버에서 상속된 기타 네트워크 리소스 및 옵션을 알 필요가 없습니다.
- DHCP 서버 역할을 하는 방화벽은 클라이언트에 서비스를 제공할 수 있습니다. DHCP 주소 지정 메커니즘 중 하나를 사용하여 관리자는 구성 시간을 절약하고 클라이언트가 더 이상 네트워크 연결을 필요로 하지 않는 제한된 수의 IP 주소를 재사용할 수 있는 이점이 있습니다. 서버는 IP 주소 지정 및 DHCP 옵션을 여러 클라이언트에 전달할 수도 있습니다.
- DHCP 릴레이 에이전트 역할을 하는 방화벽은 브로드캐스트 및 유니캐스트 DHCP 메시지를 수신 대기하고 DHCP 클라이언트와 서버 간에 릴레이합니다.

DHCP는 UDP(User Datagram Protocol), RFC 768을 전송 프로토콜로 사용합니다. 클라이언트가 서버로 보내는 DHCP 메시지는 잘 알려진 포트 67(UDP - 부트스트랩 프로토콜 및 DHCP)로 보내집니다. 서버가 클라이언트에 보내는 DHCP 메시지는 포트 68로 전송됩니다.

DHCP 주소 지정

DHCP 서버가 클라이언트에 IP 주소를 할당하거나 보내는 세 가지 방법이 있습니다.

- 자동 할당 - DHCP 서버는 **IP** 풀에서 클라이언트에 영구 IP 주소를 할당합니다. 방화벽에서 무제한으로 지정된 리스는 할당이 영구적임을 의미합니다.
- 동적 할당 - DHCP 서버는 리스라고 하는 최대 기간 동안 주소의 **IP** 풀에서 재사용 가능한 IP 주소를 클라이언트에 할당합니다. 이 주소 할당 방법은 고객에게 제한된 수의 IP 주소가 있는 경우에 유용합니다. 네트워크에 대한 임시 액세스만 필요한 클라이언트에 할당할 수 있습니다.
- 정적 할당 - 네트워크 관리자는 클라이언트에 할당할 IP 주소를 선택한 다음 DHCP 서버는 이를 클라이언트에 보냅니다. 고정 DHCP 할당은 영구적입니다. DHCP 서버를 구성하고 클라이언트 방화벽의 **MAC** 주소에 해당하는 예약 주소를 선택하면 됩니다. DHCP 할당은 클라이언트 연결이 끊긴 경우(로그오프, 재부팅, 정전 등)에도 그대로 유지됩니다.

  IP 주소의 정적 할당은 예를 들어 LAN에 프린터가 있고 DNS를 통해 프린터 이름과 연결되기 때문에 IP 주소가 계속 변경되는 것을 원하지 않는 경우에 유용합니다. 또 다른 예는 클라이언트 방화벽이 중요한 작업에 사용되고 방화벽이 꺼지거나, 연결이 끊어지거나, 재부팅되거나, 정전이 발생하더라도 동일한 IP 주소를 유지해야 하는 경우입니다.

  예약 주소를 구성할 때 다음 사항에 유의하십시오.

  - **IP** 풀의 주소입니다. 여러 예약된 주소를 구성할 수 있습니다.
  - 예약된 주소를 구성하지 않으면 서버의 클라이언트는 리스가 만료되거나 재부팅될 때 풀에서 새 DHCP 할당을 수신합니다(리스를 무제한으로 지정하지 않은 경우).
  - **IP** 풀의 모든 주소를 예약된 주소로 할당하면 주소를 요청하는 다음 DHCP 클라이언트에 할당할 수 있는 동적 주소가 없습니다.
  - **MAC** 주소를 구성하지 않고 예약된 주소를 구성할 수 있습니다. 이 경우 DHCP 서버는 방화벽에 예약된 주소를 할당하지 않습니다. 예를 들어 DHCP를 사용하지 않고 풀에서 몇 개의 주소를 예약하고 팩스와 프린터에 정적으로 할당할 수 있습니다.

DHCP 서버

- 네트워크 > DHCP > DHCP 서버

다음 섹션에서는 DHCP 서버의 각 구성 요소에 대해 설명합니다. DHCP 서버를 구성하기 전에 가상 라우터 및 영역에 할당된 레이어 3 이더넷 또는 레이어 3 VLAN 인터페이스를 미리 구성해야 합니다. 또한 DHCP 서버가 클라이언트에 할당하도록 지정할 수 있는 네트워크 계획의 유효한 IP 주소 풀을 알고 있어야 합니다.

DHCP 서버를 추가할 때 아래 표에 설명된 설정을 구성합니다.

DHCP 서버 설정	구성 위치	설명
상호 작용	**DHCP** 서버	DHCP 서버로 사용할 인터페이스의 이름입니다.
방법		활성화 또는 자동 모드를 선택합니다. 자동 모드는 서버를 활성화하고 네트워크에서 다른 DHCP 서버가 감지되면 비활성화합니다. 비활성화된 설정은 서버를 비활성화합니다.
새 IP 할당 시 Ping IP	**DHCP** 서버 > 리스	새 **IP**를 할당할 때 **Ping IP**를 클릭하면 서버는 해당 주소를 클라이언트에 할당하기 전에 IP 주소를 핑(ping)합니다. ping이 응답을 받으면 다른 방화벽에 이미 해당 주소가 있으므로 할당할 수 없음을 의미합니다. 서버는 대신 풀에서 다음 주소를 할당합니다. 이 옵션을 선택하면 디스플레이의 프로브 IP 열에 확인 표시가 나타납니다.
리스		리스 유형을 지정합니다. • 무제한은 서버가 IP 풀에서 동적으로 IP 주소를 선택한 다음 클라이언트에 영구적으로 할당하도록 합니다. • **Timeout**은 리스가 지속되는 기간을 결정합니다. 일 및 시간 수를 입력하고 선택적으로 분 수를 입력합니다.
IP 풀		DHCP 서버가 주소를 선택한 다음 DHCP 클라이언트에 할당하는 IP 주소의 상태 저장 풀을 지정합니다. 단일 주소, 주소/<mask length>(예: 192.168.1.0/24) 또는 주소 범위(예: 192.168.1.10-192.168.1.20)를 입력할 수 있습니다.
예약된 주소		선택적으로 DHCP 서버에서 동적으로 할당하지 않으려는 IP 풀에서 IP 주소(xxxx 형식)를 지정합니다. **MAC** 주소(xx:xx:xx:xx:xx:xx 형식)도 지정하면 해당 방화벽이 DHCP를 통해 IP 주소를 요청할 때 해당 MAC 주소와 연결된 방화벽에 예약 주소가 할당됩니다.
상속 소스	**DHCP** 서버 > 옵션	없음(기본값)을 선택하거나 소스 DHCP 클라이언트 인터페이스 또는 PPPoE 클라이언트 인터페이스를 선택

DHCP 서버 설정	구성 위치	설명
		하여 다양한 서버 설정을 DHCP 서버에 전파합니다. 상속 소스를 지정하는 경우 이 소스에서 상속할 옵션을 아래에서 하나 이상 선택합니다. 상속 소스를 지정하는 한 가지 이점은 DHCP 옵션이 소스 DHCP 클라이언트의 업스트림에 있는 서버에서 빠르게 전송된다는 것입니다. 또한 상속 소스의 옵션이 변경되는 경우 클라이언트의 옵션을 업데이트된 상태로 유지합니다. 예를 들어, 상속 소스 방화벽이 기본 **NTP** 서버로 식별된 NTP 서버를 대체하는 경우 클라이언트는 자동으로 새 주소를 기본 **NTP** 서버로 상속합니다.
상속 소스 상태 확인		상속 소스를 선택한 경우 상속 소스 상태 확인을 클릭하여 DHCP 클라이언트에서 상속된 옵션을 표시하는 동적 IP 인터페이스 상태 창을 엽니다.
게이트웨이	**DHCP** 서버 > 옵션**(**계속**)**	이 DHCP 서버와 동일한 LAN에 있지 않은 디바이스에 도달하는 데 사용되는 네트워크 게이트웨이(방화벽의 인터페이스)의 IP 주소를 지정하십시오.
서브넷 마스크		**IP** 풀의 주소에 적용되는 네트워크 마스크를 지정합니다.
옵션		다음 필드에 대해 드롭다운을 클릭하고 없음 또는 상속됨을 선택하거나 DHCP 서버가 해당 서비스에 액세스하기 위해 클라이언트에 보낼 원격 서버의 IP 주소를 입력합니다. 상속됨을 선택하면 DHCP 서버는 상속 소스로 지정된 소스 DHCP 클라이언트에서 값을 상속합니다. DHCP 서버는 이러한 설정을 클라이언트에 보냅니다. • 기본 **DNS**, 보조 **DNS** - 기본 및 대체 DNS(Domain Name System) 서버의 IP 주소입니다. • 기본 **WINS**, 보조 **WINS** - 기본 WINS(Windows 인터넷 이름 서비스) 서버의 IP 주소입니다. • 기본 **NIS**, 보조 **NIS** - 기본 및 대체 NIS(네트워크 정보 서비스) 서버의 IP 주소입니다. • 기본 **NTP**, 보조 **NTP** - 사용 가능한 NTP(네트워크 시간 프로토콜) 서버의 IP 주소입니다.

DHCP 서버 설정	구성 위치	설명
		• **POP3** 서버 - POP3(Post Office Protocol version 3) 서버의 IP 주소입니다. • **SMTP** 서버 - SMTP(Simple Mail Transfer Protocol) 서버의 IP 주소입니다. • **DNS** 서픽스 - 클라이언트가 확인할 수 없는 정규화되지 않은 호스트 이름이 입력된 경우 클라이언트가 로컬에서 사용할 서픽스입니다.
사용자 지정 DHCP 옵션		추가를 클릭하고 DHCP 서버가 클라이언트에 보낼 사용자 지정 옵션의 이름을 입력합니다. 옵션 코드를 입력합니다(범위는 1-254). 옵션 코드 **43**을 입력하면 VCI(Vendor Class Identifier) 필드가 나타납니다. 클라이언트의 옵션 60에서 들어오는 VCI와 비교할 일치 기준을 입력합니다. 방화벽은 클라이언트의 옵션 60에서 들어오는 VCI를 보고 자체 DHCP 서버 테이블에서 일치하는 VCI를 찾고 옵션 43에서 해당 값을 클라이언트에 반환합니다. VCI 일치 기준은 문자열 또는 16진수 값입니다. 16진수 값에는 "0x" 프리픽스가 있어야 합니다. 옵션 값을 입력하는 대신 서버가 상속 소스에서 해당 옵션 코드 값을 상속하도록 하려면 **DCHP** 서버 상속 소스에서 상속을 선택합니다. 이 옵션의 대안으로 다음을 진행할 수 있습니다. 옵션 유형: **IP** 주소, **ASCII** 또는 **16**진수를 선택하여 옵션 값에 사용되는 데이터 유형을 지정합니다. 옵션 값에 대해 추가를 클릭하고 사용자 지정 옵션 값을 입력합니다.

DHCP 릴레이

- 네트워크 > DHCP > DHCP 릴레이

방화벽 인터페이스를 DHCP 릴레이 에이전트로 구성하기 전에 Layer 3 이더넷 또는 Layer 3 VLAN 인터페이스를 구성하고 인터페이스를 가상 라우터 및 영역에 할당했는지 확인하십시오. 해당 인터페이스가 클라이언트와 서버 간에 DHCP 메시지를 전달할 수 있기를 원합니다. 각 인터페이스는 최대 8개의 외부 IPv4 DHCP 서버와 8개의 외부 IPv6 DHCP 서버에 메시지를 포워딩할 수 있습니다. 클라이언트는 구성된 모든

서버에 DHCPDISCOVER 메시지를 보내고 방화벽은 요청한 클라이언트에 다시 응답하는 첫 번째 서버의 DHCPOFFER 메시지를 릴레이합니다.

DHCP 릴레이 설정	설명
상호 작용	DHCP 릴레이 에이전트가 될 인터페이스의 이름입니다.
IPv4 / IPv6	지정할 DHCP 서버 유형과 IP 주소를 선택합니다.
DHCP 서버 IP 주소	DHCP 메시지를 릴레이할 DHCP 서버의 IP 주소를 입력합니다.
상호 작용	DHCP 서버의 IP 주소 프로토콜로 IPv6을 선택한 다음 멀티캐스트 주소를 지정한 경우 나가는 인터페이스도 지정해야 합니다.

DHCP 클라이언트

- 네트워크 > 인터페이스 > 이더넷 > IPv4
- 네트워크 > 인터페이스 > VLAN > IPv4

방화벽 인터페이스를 DHCP 클라이언트로 구성하기 전에 레이어 3 이더넷 또는 레이어 3 VLAN 인터페이스를 구성하고 가상 라우터 및 영역에 인터페이스를 할당했는지 확인하십시오. DHCP를 사용하여 방화벽의 인터페이스에 대한 IPv4 주소를 요청해야 하는 경우 이 작업을 수행하십시오.

DHCP 클라이언트 설정	설명
유형	**DHCP** 클라이언트를 선택한 다음 활성화를 선택하여 인터페이스를 DHCP 클라이언트로 구성합니다.
서버에서 제공하는 기본 게이트웨이를 가리키는 기본 경로 자동 생성	클라이언트가 방화벽의 라우팅 테이블에서 경로를 유지할 필요가 없는 많은 대상에 액세스하려고 할 때 유용한 기본 게이트웨이에 대한 정적 경로를 방화벽이 생성하도록 합니다.
기본 경로 측정 항목	선택적으로 방화벽과 DHCP 서버 간의 경로에 대한 기본 경로 지표(우선순위 수준)를 입력합니다. 경로 선택 시 번호가 낮은 경로는 우선 순위가 높습니다. 예를 들어 메트릭이 10인 경로는 메트릭이 100인 경로보다 먼저 사용됩니다(범위는 1-65535, 기본값 없음).
DHCP 클라이언트 런타임 정보 표시	DHCP 리스 상태, 동적 IP 할당, 서브넷 마스크, 게이트웨이 및 서버 설정(DNS, NTP, 도메인, WINS, NIS, POP3 및 SMTP)을 포함하여 DHCP 서버에서 수신한 모든 설정을 표시합니다.

네트워크 > DNS 프록시

DNS 서버는 IP 주소로 도메인 이름을 확인하고 그 반대의 경우도 마찬가지입니다. 방화벽을 DNS 프록시로 구성하면 방화벽은 DNS 캐시에서 쿼리를 해결하거나 쿼리를 다른 DNS 서버로 포워딩하여 클라이언트와 서버 간의 중개자 역할과 DNS 서버 역할을 합니다. 이 페이지를 사용하여 방화벽이 DNS 프록시 역할을 하는 방법을 결정하는 설정을 구성합니다.

무엇을 알고 싶습니까?	참조:
방화벽은 DNS 요청을 어떻게 프록시합니까?	DNS 프록시 개요
DNS 프록시는 어떻게 구성합니까?	DNS 프록시 설정
정적 FQDN-IP 주소 매핑을 구성하려면 어떻게 해야 합니까?	
DNS 프록시를 관리하려면 어떻게 해야 합니까?	추가 DNS 프록시 작업
더 찾고 계십니까?	DNS

DNS 프록시 개요

DNS 서버로 작동하도록 방화벽을 구성할 수 있습니다. 먼저 DNS 프록시를 만들고 프록시가 적용되는 인터페이스를 선택합니다. 그런 다음 방화벽이 DNS 프록시 캐시에서 도메인 이름을 찾지 못한 경우(및 도메인 이름이 프록시 규칙과 일치하지 않는 경우) DNS 쿼리를 보내는 기본 DNS 기본 및 보조 서버를 지정합니다.

DNS 쿼리를 도메인 이름에 따라 다른 DNS 서버로 보내려면 DNS 프록시 규칙을 만듭니다. 여러 DNS 서버를 지정하면 DNS 쿼리의 현지화를 보장하고 효율성을 높일 수 있습니다. 예를 들어 모든 회사 DNS 쿼리를 회사 DNS 서버로 포워딩하고 다른 모든 쿼리를 ISP DNS 서버로 포워딩할 수 있습니다.

다음 탭을 사용하여 DNS 프록시를 정의합니다(기본 DNS 기본 및 보조 서버 외).

- 정적 항목 - 방화벽이 DNS 쿼리에 대한 응답으로 캐시하고 호스트에 보내는 정적 FQDN-IP 주소 매핑을 구성할 수 있습니다.
- **DNS** 프록시 규칙 - 규칙과 일치하는 쿼리를 해결하기 위해 도메인 이름과 해당 기본 및 보조 DNS 서버를 지정할 수 있습니다. 도메인 이름이 DNS 프록시 캐시에 없으면 방화벽은 쿼리가 도착한 인터페이스에서 DNS 프록시에서 일치 항목을 검색하고 일치 결과에 따라 쿼리를 DNS 서버로 포워딩합니다. 일치하는 결과가 없으면 방화벽은 쿼리를 기본 DNS 기본 및 보조 서버로 보냅니다. 규칙과 일치하는 도메인의 캐싱을 활성화할 수 있습니다.

- **Advanced** - DNS 프록시 개체가 방화벽이 생성하는 DNS/FQDN 쿼리를 해결하는 데 사용되는 경우 캐싱(캐시 선택) 및 캐시 **EDNS** 응답을 활성화해야 합니다. Advanced 탭에서는 TCP 쿼리 및 UDP 쿼리 재시도를 제어할 수도 있습니다. 방화벽은 구성된 인터페이스를 통해 TCP 또는 UDP DNS 쿼리를 보냅니다. 단일 UDP 패킷에 대해 DNS 쿼리 응답이 너무 길면 UDP 쿼리가 TCP로 전환됩니다.

DNS 프록시 설정

추가를 클릭하고 방화벽이 DNS 프록시 역할을 하도록 구성합니다. 방화벽에서 최대 256개의 DNS 프록시를 구성할 수 있습니다.

DNS 프록시 설정	구성 위치	설명
사용	**DNS** 프록시	이 DNS 프록시를 활성화하려면 선택합니다.
이름		DNS 프록시 개체를 식별하는 이름을 지정합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치		DNS 프록시 개체가 적용되는 가상 시스템을 지정합니다. • 공유: 프록시는 모든 가상 시스템에 적용됩니다. 공유를 선택하면 서버 프로파일 필드를 사용할 수 없습니다. 대신 기본 및 보조 DNS 서버 IP 주소 또는 주소 개체를 입력합니다. • 이 DNS 프록시를 사용할 가상 시스템을 선택하십시오. 먼저 가상 시스템을 구성해야 합니다. 디바이스 > 가상 시스템을 선택한 다음 가상 시스템을 선택한 다음 **DNS** 프록시를 선택합니다.
상속 소스 (공유 위치만 해당)		기본 DNS 서버 설정을 상속할 소스를 선택합니다. 이것은 방화벽의 WAN 인터페이스가 DHCP 또는 PPPoE에 의해 지정되는 지점 배포에서 일반적으로 사용됩니다.
상속 소스 상태 확인 (공유 위치만 해당)		DHCP 클라이언트 및 PPPoE 클라이언트 인터페이스에 현재 할당된 서버 설정을 보려면 선택합니다. 여기에는 DNS, WINS, NTP, POP3, SMTP 또는 DNS 서픽스가 포함될 수 있습니다.
기본/보조 (공유 위치만 해당)		이 방화벽(DNS 프록시)이 DNS 쿼리를 보내는 기본 기본 및 보조 DNS 서버의 IP 주소를 지정합니다. 기본 DNS 서버를 찾을 수 없으면 방화벽은 보조 DNS 서버를 사용합니다.

DNS 프록시 설정	구성 위치	설명
서버 프로파일 (가상 시스템 위치만 해당)		새 DNS 서버 프로파일을 선택하거나 만듭니다. 가상 시스템의 위치가 공유로 지정된 경우 이 필드가 나타나지 않습니다.
상호 작용		DNS 프록시로 작동하도록 인터페이스를 추가합니다. 여러 인터페이스를 추가할 수 있습니다. 인터페이스에서 DNS 프록시를 제거하려면 선택한 다음 삭제합니다. DNS 프록시가 서비스 경로 기능에만 사용되는 경우 인터페이스가 필요하지 않습니다. 대상 서비스 경로가 소스 IP 주소를 설정하도록 하려면 인터페이스가 없는 DNS 프록시가 있는 대상 서비스 경로를 사용하십시오. 그렇지 않으면 DNS 프록시가 소스로 사용할 인터페이스 IP 주소를 선택합니다(DNS 서비스 경로가 설정되지 않은 경우).
이름	**DNS** 프록시 > **DNS** 프록시 규칙	CLI를 통해 항목을 참조하고 수정할 수 있도록 이름이 필요합니다.
이 매핑으로 확인된 도메인의 캐싱 켜기		이 매핑으로 확인되는 도메인의 캐싱을 활성화하려면 선택합니다.
도메인 이름		방화벽이 들어오는 FQDN을 비교할 도메인 이름을 하나 이상 추가합니다. FQDN이 규칙의 도메인 중 하나와 일치하는 경우 방화벽은 쿼리를 이 프록시에 대해 지정된 기본/보조 DNS 서버로 포워딩합니다. 규칙에서 도메인 이름을 삭제하려면 해당 도메인 이름을 선택한 다음 삭제를 클릭합니다.
DNS 서버 프로필 (공유 위치만 해당)		DNS 서버 프로파일을 선택하거나 추가하여 방화벽이 도메인 이름 쿼리를 보내는 기본 및 보조 DNS 서버를 포함하여 가상 시스템에 대한 DNS 설정을 정의합니다.
기본/보조 (가상 시스템 위치만 해당)		방화벽이 일치하는 도메인 이름 쿼리를 보내는 기본 및 보조 DNS 서버의 호스트 이름 또는 IP 주소를 입력합니다.
이름	**DNS** 프록시 > 정적 항목	정적 항목의 이름을 입력합니다.
FQDN		주소 필드에 정의된 고정 IP 주소에 매핑할 FQDN(정규화된 도메인 이름)을 입력합니다.

DNS 프록시 설정	구성 위치	설명
주소		이 도메인에 매핑되는 하나 이상의 IP 주소를 추가합니다. 방화벽은 DNS 응답에 이러한 모든 주소를 포함하고 클라이언트는 사용할 IP 주소를 선택합니다. 주소를 삭제하려면 주소를 선택한 다음 삭제를 클릭하세요.
TCP 쿼리	**DNS** 프록시 > 고급	TCP를 사용하여 DNS 쿼리를 활성화하려면 선택합니다. 방화벽이 지원할 최대 동시 보류 TCP DNS 요청(최대 보류 요청) 수를 지정합니다(범위는 64~256, 기본값은 64).
UDP 쿼리 재시도	**DNS** 프록시 > 고급	UDP 쿼리 재시도에 대한 설정 지정: • 인터벌 - 응답을 받지 못한 경우 DNS 프록시가 다른 요청을 보내는 시간(초)입니다(범위는 1~30, 기본값은 2). • 시도 - DNSP가 다음 DNS 서버를 시도한 후의 최대 시도 횟수(첫 번째 시도 제외)입니다(범위는 1~30, 기본값은 5).
캐시	**DNS** 프록시 > 고급	이 DNS 프록시 개체가 방화벽이 생성하는 쿼리에 사용되는 경우(즉, **Device** > **Setup** > **Services** > **DNS** 또는 **Device** > **Virtual Systems** 아래에서 가상 시스템 및 일반 > **DNS** 프록시를 선택하는 경우) 캐시를 활성화해야 합니다(기본적으로 활성화됨). 그런 다음 다음을 지정합니다. • **TTL** 활성화 - 방화벽이 프록시 개체에 대한 DNS 항목을 캐시하는 시간을 제한합니다. TTL은 기본적으로 비활성화되어 있습니다. 그런 다음 프록시 개체에 대해 캐시된 모든 항목이 제거되고 새 DNS 요청을 확인하고 다시 캐시해야 하는 시간**(초)**을 입력합니다. 범위는 60~86,400입니다. 기본 TTL은 없습니다. 항목은 방화벽에서 캐시 메모리가 부족해질 때까지 남아 있습니다. • 캐시 **EDNS** 응답 - 이 DNS 프록시 개체가 방화벽이 생성하는 쿼리에 사용되는 경우 DNS(EDNS) 응답에 대한 캐시 확장 메커니즘을 활성화해야 합니다. FQDN 주소 개체에 대한 쿼리가 성공하려면 방화벽이 DNS 응답을 캐시할 수 있어야 합니다.

추가 DNS 프록시 작업

방화벽을 DNS 프록시로 구성한 후 네트워크 > **DNS** 프록시 페이지에서 다음 작업을 수행하여 DNS 프록시 구성을 관리할 수 있습니다.

- 수정 - DNS 프록시를 수정하려면 DNS 프록시 구성의 이름을 클릭합니다.
- 삭제 - DNS 프록시 항목을 선택한 다음 삭제를 클릭하여 DNS 프록시 구성을 제거합니다.
- 비활성화 - DNS 프록시를 비활성화하려면 DNS 프록시 항목의 이름을 클릭하고 활성화 옵션을 지웁니다. 비활성화된 DNS 프록시를 활성화하려면 DNS 프록시 항목의 이름을 클릭하고 활성화를 선택합니다.

네트워크 > 프록시

프록시 구성 옵션의 가용성은 프록시 유형을 기반으로 합니다. 프록시를 구성하려면 먼저 DNS 프록시 개체를 구성해야 합니다.

프록시 필드	설명
프록시 활성화	
프록시 유형	사용할 프록시 유형을 선택합니다. • 없음 - 프록시가 비활성화됩니다. • 명시적 - 요청에 구성된 프록시의 대상 IP 주소가 포함되고 클라이언트 브라우저가 프록시에 직접 요청을 보내도록 프록시를 구성합니다. • 투명 - 요청에 웹 서버의 대상 IP 주소가 포함되고 클라이언트 브라우저가 프록시로 리디렉션되도록 프록시를 구성합니다. 웹 프록시를 성공적으로 구성하려면 투명 프록시에 특정 DNAT(대상 *NAT*) 정책 규칙이 필요합니다. 전체 절차는 PAN-OS 네트워킹 관리자 가이드 문서를 참조하십시오.
프록시 구성	
연결 시간 초과	프록시가 웹 서버의 응답을 기다리는 시간(초)을 지정합니다. 범위는 1~60초이고 기본값은 5초입니다. 지정된 시간이 경과한 후에도 응답이 없으면 프록시가 연결을 닫습니다.
청취 인터페이스 명시적 프록시만 해당	방화벽이 프록시로 다시 라우팅할 트래픽을 확인하는 레이어 3(L3) 인터페이스를 지정합니다.
업스트림 인터페이스	업스트림 인터페이스를 선택합니다. 루프백 인터페이스를 사용하는 경우 해당 인터페이스를 업스트림 인터페이스로 지정합니다.

프록시 필드	설명
프록시 **IP**	방화벽이 프록시(수신 인터페이스)로 다시 라우팅할 트래픽을 확인해야 하는 인터페이스의 IP 주소를 지정합니다.
DNS 프록시	프록시 연결에 사용할 DNS 프록시 개체를 선택합니다.
CONNECT 및 **SNI**의 도메인 확인이 동일함 명시적 프록시만 해당	이 옵션을 활성화하면 CONNECT 요청과 HTTP 헤더의 SNI(서버 이름 표시) 필드 사이에 다른 도메인을 지정하여 발생하는 도메인 프런팅 공격을 방지할 수 있습니다.
인증 서비스 유형 명시적 프록시만 해당	사용자 인증에 사용할 서비스 유형을 선택합니다. • **SAML/CAS** - SAML 2.0 기반 인증 서비스 또는 Cloud Identity Engine에서 사용 가능한 인증 서비스를 사용합니다. 이 옵션에는 *Prisma Access*, 클라우드 서비스 *3.2.1* 플러그인 및 애드온 웹 프록시 라이선스가 필요합니다. • **Kerberos Single Sign On** - Kerberos Single Sign-On 서비스를 사용하여 사용자를 인증합니다. 이 옵션에는 *Panorama*, 웹 프록시 라이선스 및 방화벽에서 Kerberos Single Sign-On 서비스를 사용하는 인증 프로필이 필요합니다.
인증 프로파일 명시적 프록시만 해당	이전 옵션에 대해 선택한 인증 서비스 유형에 사용할 인증 프로필을 선택합니다.

네트워크 > QoS

다음 항목에서는 서비스 품질(QoS)에 대해 설명합니다.

무엇을 찾고 계신가요?	참조:
인터페이스에 대한 대역폭 제한을 설정하고 인터페이스를 나가는 트래픽에 QoS를 적용합니다.	QoS 인터페이스 설정
QoS 지원 인터페이스를 나가는 트래픽을 모니터링합니다.	QoS 인터페이스 통계
더 찾고 계십니까?	전체 QoS 워크플로, 개념 및 사용 사례는 서비스 품질을 참조하십시오.
	정책 > QoS를 선택하여 일치하는 트래픽 QoS 클래스를 할당하거나 네트워크 > 네트워크 프로파일 > QoS를 선택하여 최대 8개의 QoS 클래스에 대한 대역폭 제한 및 우선 순위를 정의합니다.

QoS 인터페이스 설정

인터페이스에서 QoS를 활성화하여 인터페이스에 대한 대역폭 제한을 설정하거나 인터페이스가 이그레스(egress) 트래픽에 대해 QoS를 적용할 수 있도록 합니다. QoS 인터페이스 활성화에는 인터페이스에 QoS 프로파일 연결이 포함됩니다. QoS는 물리적 인터페이스에서 지원되며, 방화벽 모델에 따라 QoS는 서브인터페이스 및 AE(Aggregate Ethernet) 인터페이스에서도 지원됩니다. 방화벽 모델에 대한 QoS 기능 지원을 보려면 Palo Alto Networks 제품 비교 도구를 참조하십시오.

시작하려면 QoS 인터페이스를 추가하거나 수정한 후 다음 표에 설명된 대로 설정을 구성하십시오.

QoS 인터페이스 설정	구성 위치	설명
인터페이스 이름	**QoS** 인터페이스 > 물리적 인터페이스	QoS를 활성화할 방화벽 인터페이스를 선택합니다.
최대 이그레스(egress) (Mbps)		이 인터페이스를 통해 방화벽에서 나가는 트래픽의 최대 처리량(Mbps)을 입력합니다. 이 값은 기본적으로 0이며 방화벽 제한을 지정합니다(PAN-OS 7.1.16 이상 릴리스에서는 60,000Mbps, PAN-OS 7.1.15 및 이전 릴리스에서는 16,000Mbps).

QoS 인터페이스 설정	구성 위치	설명
		필수 필드는 아니지만 *QoS* 인터페이스에 대해 항상 ***Egress Max***를 정의하는 것이 좋습니다.
이 인터페이스에서 QoS 기능 켜기		선택한 인터페이스에서 QoS를 활성화하려면 선택합니다.
명확한 문구 터널 인터페이스	**QoS** 인터페이스 > 물리적 인터페이스 > 기본 프로필	일반 텍스트 및 터널링된 트래픽에 대한 기본 QoS 프로파일을 선택합니다. 각각에 대해 기본 프로파일을 지정해야 합니다. 일반 텍스트 트래픽의 경우 기본 프로파일이 모든 일반 텍스트 트래픽에 통합로 적용됩니다. 터널링된 트래픽의 경우 기본 프로파일은 세부 구성 섹션에서 특정 프로파일 할당이 없는 각 터널에 개별적으로 적용됩니다. QoS 프로파일 정의에 대한 지침은 네트워크 > 네트워크 프로파일 > QoS를 참조하십시오.
터널 인터페이스		
이그레스(egress) 보장(Mbps)	**QoS** 인터페이스 > 텍스트 트래픽 지우기 / 터널링된 트래픽	이 인터페이스에서 일반 텍스트 또는 터널링된 트래픽에 대해 보장되는 대역폭을 입력합니다.
최대 이그레스(egress) (Mbps)		이 인터페이스를 통해 방화벽에서 나가는 일반 텍스트 또는 터널링된 트래픽의 최대 처리량(Mbps)을 입력합니다. 이 값은 기본적으로 0이며 방화벽 제한을 지정합니다(PAN-OS 7.1.16 이상 릴리스에서는 60,000Mbps, PAN-OS 7.1.15 및 이전 릴리스에서는 16,000Mbps). 일반 텍스트 또는 터널링된 트래픽의 **Egress Max**는 물리적 인터페이스의 **Egress Max**보다 작거나 같아야 합니다.

QoS 인터페이스 설정	구성 위치	설명

추가		• 일반 텍스트 트래픽 탭에서 추가를 클릭하여 일반 텍스트 트래픽 처리에 대한 추가 세분성을 정의합니다. 개별 항목을 클릭하여 다음 설정을 구성합니다.
		  • 이름 - 이러한 설정을 식별하는 이름을 입력합니다.
		  • **QoS** 프로파일 - 지정된 인터페이스 및 서브넷에 적용할 QoS 프로파일을 선택합니다. QoS 프로파일 정의에 대한 지침은 네트워크 > 네트워크 프로파일 > QoS를 참조하십시오.
		  • 소스 인터페이스 - 방화벽 인터페이스를 선택합니다.
		  • 대상 인터페이스 - (PA-3200 시리즈, PA-5200 시리즈, PA-5400 시리즈, PA-7000 시리즈만 해당) 트래픽이 의도된 대상 인터페이스를 선택합니다.
		  • 소스 서브넷 - 서브넷을 선택하여 해당 소스에서 오는 트래픽으로 설정을 제한하거나 기본값인 **any**를 유지하여 지정된 인터페이스의 모든 트래픽에 설정을 적용합니다.
		• 터널링된 트래픽 탭에서 추가를 클릭하여 특정 터널에 대한 기본 프로파일 할당을 재정의하고 다음 설정을 구성합니다.
		  • 터널 인터페이스 - 방화벽에서 터널 인터페이스를 선택합니다.
		  • **QoS** 프로파일 - 지정된 터널 인터페이스에 적용할 QoS 프로파일을 선택합니다.
		예를 들어, 하나는 45Mbps 연결이고 다른 하나는 방화벽에 대한 T1 연결이 있는 두 개의 사이트가 있는 구성을 가정합니다. T1 사이트에 제한적인 QoS 설정을 적용하여 연결이 과부하되지 않도록 하는 동시에 45Mbps 연결을 사용하는 사이트에 대해 보다 유연한 설정을 허용할 수 있습니다.
		일반 텍스트 또는 터널링된 트래픽 항목을 제거하려면 항목을 지우고 삭제를 클릭합니다.
		일반 텍스트 또는 터널링된 트래픽 섹션을 비워두면 물리적 인터페이스 탭의 기본 프로파일 섹션에 지정된 값이 사용됩니다.

QoS 인터페이스 통계

- 네트워크 > QoS > 통계

QoS 인터페이스의 경우 통계를 선택하여 구성된 QoS 인터페이스에 대한 대역폭, 세션 및 애플리케이션 정보를 봅니다.

QoS 통계	설명
대역폭	선택한 노드 및 클래스에 대한 실시간 대역폭 차트를 표시합니다. 이 정보는 2초마다 업데이트됩니다. *QoS* 클래스에 대해 구성된 *QoS Egress Max* 및 *Egress Guaranteed* 제한은 *QoS* 통계 화면에서 약간 다른 값으로 표시될 수 있습니다. 이는 정상적인 동작이며 하드웨어 엔진이 대역폭 제한 및 카운터를 요약하는 방식 때문입니다. 대역폭 활용도 그래프가 실시간 값과 수량을 표시하므로 작동 문제가 없습니다.
애플리케이션	선택한 QoS 노드 및/또는 클래스에 대한 모든 활성 애플리케이션을 나열합니다.
소스 사용자	선택한 QoS 노드 및/또는 클래스에 대한 모든 활성 소스 사용자를 나열합니다.
대상 사용자	선택한 QoS 노드 및/또는 클래스에 대한 모든 활성 대상 사용자를 나열합니다.
보안 규칙	선택한 QoS 노드 및/또는 클래스와 일치하고 적용하는 보안 규칙을 나열합니다.
QoS 규칙	선택한 QoS 노드 및/또는 클래스와 일치하고 적용하는 QoS 규칙을 나열합니다.

Network > LLDP

LLDP(Link Layer Discovery Protocol)는 링크 레이어에서 인접 디바이스와 해당 기능을 자동으로 검색하는 방법을 제공합니다.

무엇을 찾고 계신가요?	참조:
LLDP란 무엇입니까?	LLDP 개요
LLDP를 구성합니다.	LLDP의 빌딩 블록
LLDP 프로파일을 구성합니다.	네트워크 > 네트워크 프로파일 > LLDP 프로파일
더 찾고 계십니까?	LLDP

LLDP 개요

LLDP를 사용하면 방화벽이 LLDP 데이터 단위(LLDPDU)를 포함하는 이더넷 프레임을 이웃과 주고받을 수 있습니다. 수신 디바이스는 SNMP(Simple Network Management Protocol)에서 액세스할 수 있는 MIB에 정보를 저장합니다. LLDP를 사용하면 네트워크 디바이스가 네트워크 토폴로지를 매핑하고 연결된 디바이스의 기능을 학습할 수 있으므로 특히 방화벽이 일반적으로 네트워크 토폴로지에서 감지되지 않는 가상 와이어 배포의 경우 문제 해결이 쉬워집니다.

LLDP의 빌딩 블록

방화벽에서 LLDP를 활성화하려면 기본 설정이 사용자 환경에 적합하지 않은 경우 편집, 활성화를 차례로 클릭하고 다음 표에 표시된 네 가지 설정을 선택적으로 구성합니다. 나머지 테이블 항목은 상태 및 피어 통계를 설명합니다.

LLDP 설정	구성 위치	설명
전송 인터벌(초)	**LLDP** 일반	LLDPDU가 전송되는 인터벌(초)을 지정합니다(범위는 1-3,600, 기본값은 30).
전송 지연(초)		TLV(Type-Length-Value) 요소가 변경된 후 전송된 LLDP 전송 사이의 지연 시간(초)을 지정합니다. 지연은 많은 네트워크 변경이 LLDP 변경 수를 급증시키거나 인터페이스가 플랩하는 경우 LLDPDU로 세그먼트 범람을 방지하는 데 도움이 됩니다. 전송 지연은 전송 인터벌보다 작아야 합니다(범위는 1-600, 기본값은 2).

LLDP 설정	구성 위치	설명
홀드 타임 배수		총 TTL 유지 시간을 결정하기 위해 전송 인터벌을 곱한 값을 지정합니다(범위는 1-100, 기본값은 4). TTL 보류 시간은 방화벽이 피어의 정보를 유효한 것으로 유지하는 시간입니다. 최대 TTL 유지 시간은 승수 값에 관계없이 65,535초입니다.
알림 인터벌		MIB 변경이 발생할 때 syslog 및 SNMP 트랩 알림이 전송되는 인터벌을 초 단위로 지정합니다(범위는 1-3,600, 기본값은 5).
망원경 필터	**LLDP** > 상태	선택적으로 필터 행에 데이터 값을 입력하고 회색 화살표를 클릭하면 해당 데이터 값이 포함된 행만 표시됩니다. 필터를 지우려면 빨간색 X를 클릭합니다.
상호 작용		LLDP 프로파일이 할당된 인터페이스의 이름입니다.
유형		LLDP 프로필이 할당된 인터페이스 유형(예: 레이어 2, 레이어 3, 가상 와이어, 탭, HA 또는 통합 이더넷).
LLDP		LLDP 상태: 활성화 또는 비활성화.
HA 사전 협상		HA 사전 협상 상태: 활성화됨 또는 비활성화됨. LLDP 사전 협상을 통해 HA 액티브/패시브 시나리오에서 장애 조치를 더 빠르게 수행할 수 있습니다.
모드		인터페이스의 LLDP 모드: Tx/Rx, Tx 전용 또는 Rx 전용.
프로파일		인터페이스에 할당된 프로파일의 이름입니다.
총 전송		인터페이스 밖으로 전송된 LLDPDU의 수입니다.
전송 중단		오류로 인해 인터페이스 밖으로 전송되지 않은 LLDPDU의 수입니다. 예를 들어, 시스템이 전송을 위해 LLDPDU를 구성할 때 길이 오류가 발생합니다.
총 수령		인터페이스에서 수신된 LLDP 프레임 수입니다.
삭제된 TLV		수신 시 폐기된 LLDP 프레임 수입니다.
오류		인터페이스에서 수신되었고 오류가 포함된 TLV(Time-Length-Value) 요소의 수입니다. TLV 오류 유형에는 하나

LLDP 설정	구성 위치	설명
		이상의 필수 TLV 누락, 순서 오류, 범위를 벗어난 정보 포함 또는 길이 오류가 포함됩니다.
인식할 수 없음		예를 들어, TLV 유형이 예약된 TLV 범위에 있기 때문에 LLDP 로컬 에이전트에서 인식하지 못하는 인터페이스에서 수신된 TLV 수입니다.
에이지 아웃		적절한 TTL 만료로 인해 수신 MIB에서 삭제된 항목 수입니다.
LLDP 통계 지우기		모든 LLDP 통계를 지우려면 선택합니다.
망원경 필터	**LLDP** > 피어	선택적으로 필터 행에 데이터 값을 입력하고 회색 화살표를 클릭하면 해당 데이터 값이 포함된 행만 표시됩니다. 필터를 지우려면 빨간색 X를 클릭합니다.
로컬 인터페이스		인접 디바이스를 감지한 방화벽의 인터페이스입니다.
원격 섀시 ID		피어의 섀시 ID입니다. MAC 주소가 사용됩니다.
포트 ID	**LLDP** > 피어**(**계속**)**	피어의 포트 ID입니다.
이름		피어의 이름입니다.
더 많은 정보		추가 정보를 클릭하면 필수 및 선택적 TLV를 기반으로 하는 원격 피어 세부 정보를 볼 수 있습니다.
섀시 유형		섀시 유형은 MAC 주소입니다.
MAC 주소		피어의 MAC 주소입니다.
시스템 이름		피어의 이름입니다.
시스템 설명		피어에 대한 설명입니다.
포트 설명		피어의 포트 설명입니다.
포트 유형		인터페이스 이름.
포트 ID		방화벽은 인터페이스의 ifname을 사용합니다.

LLDP 설정	구성 위치	설명
시스템 기능		시스템의 기능. O=기타, P=중계기, B=브리지, W=무선 LAN, R=라우터, T=전화기
활성화된 기능		피어에서 활성화된 기능입니다.
관리 주소		피어의 관리 주소입니다.

네트워크 > 네트워크 프로파일

다음 항목에서는 네트워크 프로파일에 대해 설명합니다.

- 네트워크 > 네트워크 프로파일 > GlobalProtect IPSec 암호화
- 네트워크 > 네트워크 프로파일 > IKE 게이트웨이
- 네트워크 > 네트워크 프로파일 > IPSec 암호화
- 네트워크 > 네트워크 프로파일 > IKE 암호화
- 네트워크 > 네트워크 프로파일 > 모니터
- 네트워크 > 네트워크 프로파일 > 인터페이스 관리
- 네트워크 > 네트워크 프로파일 > 영역 보호
- 네트워크 > 네트워크 프로파일 > QoS
- 네트워크 > 네트워크 프로파일 > LLDP 프로파일
- 네트워크 > 네트워크 프로파일 > BFD 프로파일
- 네트워크 > 네트워크 프로파일 > SD-WAN 인터페이스 프로파일

네트워크 > 네트워크 프로파일 > GlobalProtect IPSec 암호화

GlobalProtect IPSec 암호화 프로파일 페이지를 사용하여 GlobalProtect 게이트웨이와 클라이언트 간의 VPN 터널에서 인증 및 암호화 알고리즘을 지정합니다. 알고리즘을 추가하는 순서는 방화벽이 알고리즘을 적용하는 순서이며 터널 보안 및 성능에 영향을 줄 수 있습니다. 순서를 변경하려면 알고리즘을 선택한 다음 위로 이동 또는 아래로 이동합니다.

GlobalProtect 게이트웨이와 새틀라이트*(*방화벽*)* 간의 *VPN* 터널에 대해서는 네트워크 > 네트워크 프로파일 > IPSec 암호화를 참조하십시오.

GlobalProtect IPSec 암호화 프로파일 설정	
이름	프로파일을 식별할 수 있는 이름을 입력합니다. 이름은 대소문자를 구분하고 고유해야 하며 최대 **31**자를 사용할 수 있습니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
암호화	추가를 클릭하고 원하는 암호화 알고리즘을 선택합니다. 최고의 보안을 위해 순서(위에서 아래로)를 **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**로 변경하십시오.
인증	추가를 클릭하고 인증 알고리즘을 선택합니다. 현재 유일한 옵션은 **sha1**입니다.

네트워크 > 네트워크 프로파일 > IKE 게이트웨이

이 페이지에서는 피어 게이트웨이와의 IKE(인터넷 키 교환) 프로토콜 협상을 수행하는 데 필요한 구성 정보를 포함하여 게이트웨이를 관리하거나 정의할 수 있습니다. 이것은 IKE/IPSec VPN 설정의 1단계 부분입니다.

IKE 게이트웨이를 관리, 구성, 다시 시작 또는 새로 고치려면 다음을 참조하십시오.

- IKE 게이트웨이 관리
- IKE 게이트웨이 일반 탭
- IKE 게이트웨이 Advanced 옵션 탭
- IKE 게이트웨이 다시 시작 또는 새로 고침

IKE 게이트웨이 관리

- 네트워크 > 네트워크 프로파일 > IKE 게이트웨이

다음 표에서는 IKE 게이트웨이를 관리하는 방법을 설명합니다.

IKE 게이트웨이 관리	설명
추가하다	새 IKE 게이트웨이를 만들려면 추가를 클릭합니다. 새 게이트웨이 구성에 대한 지침은 IKE 게이트웨이 일반 탭 및 IKE 게이트웨이 Advanced 옵션 탭을 참조하십시오.
삭제	게이트웨이를 삭제하려면 게이트웨이를 선택한 다음 삭제를 클릭합니다.
활성화	비활성화된 게이트웨이를 활성화하려면 게이트웨이를 선택한 다음 게이트웨이의 기본 설정인 활성화를 클릭합니다.
비활성화	게이트웨이를 비활성화하려면 게이트웨이를 선택한 다음 비활성화를 클릭합니다.
PDF/CSV	최소한의 읽기 전용 액세스 권한이 있는 관리 역할은 개체 구성 테이블을 **PDF/CSV**로 내보낼 수 있습니다. 필터를 적용하여 감사와 같은 항목에 대한 보다 구체적인 테이블 구성 출력을 생성할 수 있습니다. 웹 인터페이스에서 보이는 열만 내보내집니다. 구성 테이블 내보내기를 참조하십시오.

IKE 게이트웨이 일반 탭

- 네트워크 > 네트워크 프로파일 > IKE 게이트웨이 > 일반

다음 표에서는 IKE 게이트웨이를 구성하기 위한 시작 설정을 설명합니다. IKE는 IKE/IPSec VPN 프로세스의 1단계입니다. 이러한 설정을 구성한 후 IKE 게이트웨이 Advanced 옵션 탭을 참조하십시오.

IKE 게이트웨이 일반 설정	설명
이름	게이트웨이를 식별할 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
버전	게이트웨이가 지원하고 피어 게이트웨이와 함께 사용하는 데 동의해야 하는 IKE 버전을 선택합니다. **IKEv1** 전용 모드, **IKEv2** 전용 모드 또는 **IKEv2** 기본 모드. IKEv2 기본 모드는 게이트웨이가 IKEv2를 협상하도록 하며 피어가 IKEv2도 지원하는 경우 게이트웨이가 사용하는 모드입니다. 그렇지 않으면 게이트웨이가 IKEv1로 대체됩니다.
주소 유형	게이트웨이가 사용하는 IP 주소 유형 선택: **IPv4** 또는 **IPv6**.
상호 작용	VPN 터널에 대한 나가는 방화벽 인터페이스를 지정합니다.
로컬 IP 주소	터널의 엔드포인트인 로컬 인터페이스의 IP 주소를 선택하거나 입력합니다.

피어 IP 주소
 	
유형
	다음 설정 중 하나를 선택한 다음 피어에 대한 해당 정보를 입력합니다.
	• 동적 - 피어 IP 주소 또는 FQDN 값을 알 수 없는 경우 이 옵션을 선택합니다. 피어 IP 주소 유형이 동적이면 IKE 게이트웨이 협상을 시작하는 것은 피어에 달려 있습니다.
	• **IP** - 피어 주소를 IPv4 또는 IPv6 주소 또는 IPv4 또는 IPv6 주소인 주소 개체로 입력합니다.
	• **FQDN** - 피어 주소를 FQDN 또는 FQDN을 사용하는 주소 개체로 입력합니다.
	둘 이상의 IP 주소로 확인되는 FQDN 또는 FQDN 주소 개체를 입력하면 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.
	  • 주소가 IKE 게이트웨이에서 사용되고 반환된 주소 집합에 있는 경우 해당 주소가 사용됩니다(가장 작은지의 여부와 관계없이).
	  • 주소가 IKE 게이트웨이에서 사용되지만 반환된 주소 집합에 없는 경우 새 주소(집합에서 가장 작은 주소)가 선택됩니다.
	
	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*).*

IKE 게이트웨이 일반 설정	설명
인증	인증 유형 선택: 피어 게이트웨이와 함께 발생할 사전 공유 키 또는 인증서. 선택 항목에 따라 사전 공유 키 필드 또는 인증서 필드를 참조하십시오.
사전 공유 키 필드	
사전 공유 키 / 미리 공유한 키 확인	사전 공유 키를 선택하는 경우 터널 전체에서 대칭 인증에 사용할 단일 보안 키를 입력합니다. 사전 공유 키 값은 관리자가 최대 255개의 ASCII 또는 비 ASCII 문자를 사용하여 생성하는 문자열입니다. 사전 공격으로 복호화하기 어려운 키를 생성하고, 필요한 경우 미리 공유한 키 생성기를 사용합니다.
로컬 식별	IKEv1 단계 1 SA 및 IKEv2 SA 설정 모두에 사전 공유 키와 함께 사용되는 로컬 게이트웨이의 형식 및 ID를 정의합니다. 다음 유형 중 하나를 선택한 다음 값을 입력합니다. **FQDN**(호스트 이름), **IP** 주소, **KEYID**(16진수의 이진 형식 ID 문자열) 또는 사용자 **FQDN**(이메일 주소). 값을 지정하지 않으면 게이트웨이는 로컬 IP 주소를 로컬 **ID** 값으로 사용합니다.
피어 식별	IKEv1 단계 1 SA 및 IKEv2 SA 설정 중에 사전 공유 키와 함께 사용되는 피어 게이트웨이의 유형 및 ID를 정의합니다. 다음 유형 중 하나를 선택한 다음 값을 입력합니다. **FQDN**(호스트 이름), **IP** 주소, **KEYID**(16진수의 이진 형식 ID 문자열) 또는 사용자 **FQDN**(이메일 주소). 값을 지정하지 않으면 게이트웨이는 피어의 IP 주소를 피어 식별 값으로 사용합니다.
인증서 필드	
로컬 인증서	인증서가 인증 유형으로 선택된 경우 드롭다운에서 이미 방화벽에 있는 인증서를 선택합니다. 또는 다음과 같이 인증서를 가져오거나 새 인증서를 생성할 수 있습니다. 가져오기: • 인증서 이름 - 가져올 인증서의 이름을 입력합니다. • **Shared(**공유**)** - 이 인증서를 여러 가상 시스템에서 공유하려면 클릭합니다.

IKE 게이트웨이 일반 설정	설명

	• 인증서 파일 - 찾아보기를 클릭하여 인증서 파일이 있는 위치로 이동합니다. 파일을 클릭하고 열기를 선택합니다.
	• 파일 형식 - 다음 중 하나를 선택합니다.
	  • **Base64** 인코딩된 인증서**(PEM)** - 인증서는 포함하지만 키는 포함하지 않습니다. 평문.
	  • 암호화된 개인 키 및 인증서**(PKCS12)** - 인증서와 키를 모두 포함합니다.
	• 개인 키가 하드웨어 보안 모듈에 있음 - 방화벽이 키가 있는 HSM 서버의 클라이언트인 경우 클릭합니다.
	• 개인 키 가져오기 - 개인 키가 인증서 파일과 다른 파일에 있기 때문에 가져올 경우 클릭합니다.
	  • 개인 키 내보내기 차단 - 개인 키 가져오기를 선택하면 운용 관리자를 포함한 모든 관리자가 개인 키를 내보낼 수 없습니다.
	  • 키 파일 - 가져올 키 파일을 찾아 탐색합니다. 이 항목은 파일 형식으로 PEM을 선택한 경우입니다.
	  • 패스프레이즈 및 패스프레이즈 확인 - 키에 액세스하려면 Enter 키를 누릅니다.

로컬 인증서(계속)	생성: • 인증서 이름 - 생성 중인 인증서의 이름을 입력합니다. • 일반 이름 - 인증서에 표시할 IP 주소 또는 FQDN인 일반 이름을 입력합니다. • **Shared(**공유**)** - 이 인증서를 여러 가상 시스템에서 공유하려면 클릭합니다. • 서명자 - 외부 기관(CSR)을 선택하거나 방화벽 IP 주소를 입력합니다. 이 항목은 CA여야 합니다. • 인증 기관 - 방화벽이 루트 CA인 경우 클릭합니다. • 개인 키 내보내기 차단—운용 관리자를 포함한 모든 관리자가 개인 키를 내보내는 것을 방지합니다. • **OCSP** 응답자 - 인증서가 유효한지 취소되었는지 추적하는 OCSP를 입력합니다. • 알고리즘 - RSA 또는 타원 곡선 DSA를 선택하여 인증서에 대한 키를 생성합니다. • 비트 수 - 키의 비트 수로 512, 1024, 2048 또는 3072를 선택합니다.

IKE 게이트웨이 일반 설정	설명
	• 다이제스트 - 해시에서 문자열을 되돌리는 방법으로 md5, sha1, sha256, sha384 또는 sha512를 선택합니다. • 만료**(**일**)** - 인증서가 유효한 일 수를 입력합니다. • 인증서 속성: 유형 - 선택적으로 드롭다운에서 인증서에 포함될 추가 속성 유형을 선택합니다. • 값 - 속성 값을 입력합니다.
HTTP 인증서 교환	**HTTP** 인증서 교환을 클릭하고 인증서 **URL**을 입력하여 해시 및 URL 방법을 사용하여 피어에게 인증서를 가져올 위치를 알려줍니다. 인증서 URL은 인증서를 저장하는 원격 서버의 URL입니다. 피어가 해시 및 URL도 지원한다고 표시하면 SHA1 해시 및 URL 교환을 통해 인증서가 교환됩니다. 피어가 IKE 인증서 페이로드를 수신하면 HTTP URL을 보고 해당 서버에서 인증서를 가져옵니다. 그런 다음 피어는 인증서 페이로드에 지정된 해시를 사용하여 HTTP 서버에서 다운로드한 인증서를 확인합니다.
로컬 식별	인증서에서 로컬 피어가 식별되는 방법을 식별합니다. 다음 유형 중 하나를 선택한 다음 값을 입력합니다. 고유 이름(제목), **FQDN**(호스트 이름), **IP** 주소 또는 사용자 **FQDN**(이메일 주소).
피어 식별	인증서에서 원격 피어가 식별되는 방법을 식별합니다. 다음 유형 중 하나를 선택한 다음 값을 입력합니다. 고유 이름(제목), **FQDN**(호스트 이름), **IP** 주소 또는 사용자 **FQDN**(이메일 주소).
피어 ID 확인	일치 또는 와일드카드를 선택합니다. 이 설정은 인증서의 유효성을 검사하는 피어 ID에 적용됩니다. 예를 들어 피어 ID가 domain.com과 동일한 이름이고 정확함을 선택한 다음 IKE ID 페이로드의 인증서 이름이 mail.domain2.com인 경우 IKE 협상은 실패합니다. 그러나 와일드카드를 선택한 경우 이름 문자열에서 와일드카드 별표(*) 앞의 문자만 일치해야 하며 와일드카드 뒤의 모든 문자는 다를 수 있습니다.
피어 식별 및 인증서 페이로드 식별 불일치 허용	피어 ID가 인증서 페이로드와 일치하지 않더라도 성공적인 IKE SA를 가질 수 있는 유연성을 원하는 경우 선택합니다.
인증서 프로파일	프로파일을 선택하거나 로컬 게이트웨이가 피어 게이트웨이로 보내는 인증서에 적용되는 인증서 옵션을 구성하는 새 인증서 프로파일을 만듭니다. 디바이스 > 인증서 관리 > 인증서 프로파일을 참조하십시오.

IKE 게이트웨이 일반 설정	설명
피어의 확장 키 사용에 대한 엄격한 유효성 검사 활성화	키 사용 방법을 엄격하게 제어하려면 선택합니다.

IKE 게이트웨이 Advanced 옵션 탭

- 네트워크 > 네트워크 프로파일 > IKE 게이트웨이 > Advanced 옵션

패시브 모드, NAT Traversal과 같은 Advanced IKE 게이트웨이 설정 및 Dead Peer 감지와 같은 IKEv1 설정을 구성합니다.

IKE 게이트웨이 Advanced 옵션	설명
수동 모드 활성화	방화벽이 IKE 연결에만 응답하고 시작하지 않도록 하려면 클릭합니다.
NAT 통과 활성화	IKE 및 UDP 프로토콜에 UDP 캡슐화를 사용하여 중간 NAT 디바이스를 통과하도록 하려면 클릭합니다. NAT(Network Address Translation)가 IPSec VPN 종료 지점 사이의 디바이스에 구성된 경우 NAT Traversal을 활성화합니다.
IKEv1 탭	
교환 모드	자동, 적극적인 또는 기본을 선택합니다. 자동 모드(기본값)에서 디바이스는 기본 모드와 적극적인 모드 협상 요청을 모두 수락할 수 있습니다. 그러나 가능할 때마다 협상을 시작하고 기본 모드에서 교환을 허용합니다. 첫 번째 디바이스에서 시작된 협상 요청을 수락할 수 있도록 피어 디바이스를 동일한 교환 모드로 구성해야 합니다.
IKE 암호화 프로파일	기존 프로파일을 선택하거나 기본 프로파일을 유지하거나 새 프로파일을 만듭니다. IKEv1 및 IKEv2에 대해 선택한 프로파일은 다를 수 있습니다. IKE 암호화 프로파일에 대한 자세한 내용은 네트워크 > 네트워크 프로파일 > IKE 암호화를 참조하십시오.
조각화 활성화	로컬 게이트웨이가 조각난 IKE 패킷을 수신하도록 허용하려면 클릭합니다. 최대 조각화된 패킷 크기는 576바이트입니다.
데드 피어 감지	인터벌(2~100초) 및 재시도 횟수(2~100)를 활성화하고 입력하려면 클릭합니다. 데드 피어 감지는 비활성 또는 사용할 수 없는 IKE 피어를 식별하고

IKE 게이트웨이 Advanced 옵션	설명
	피어를 사용할 수 없을 때 손실된 리소스를 복원하는 데 도움이 될 수 있습니다.
IKEv2 탭	
IKE 암호화 프로파일	기존 프로파일을 선택하거나 기본 프로파일을 유지하거나 새 프로파일을 만듭니다. IKEv1 및 IKEv2에 대해 선택한 프로파일은 다를 수 있습니다. IKE 암호화 프로파일에 대한 자세한 내용은 네트워크 > 네트워크 프로파일 > IKE 암호화를 참조하십시오.
엄격한 쿠키 유효성 검사	IKE 게이트웨이에서 엄격한 쿠키 유효성 검사를 활성화하려면 클릭합니다. • 엄격한 쿠키 유효성 검사를 활성화하면 IKEv2 쿠키 유효성 검사가 항상 시행됩니다. 개시자는 쿠키가 포함된 IKE_SA_INIT를 보내야 합니다. • **Strict Cookie Validation**(기본값)을 비활성화하면 시스템은 VPN 세션 설정인 전역 쿠키 활성화 임계값에 대해 절반만 열린 SA의 수를 확인합니다. 반쯤 열린 SA의 수가 쿠키 활성화 임계값을 초과하는 경우 개시자는 쿠키가 포함된 IKE_SA_INIT를 보내야 합니다.
라이브니스 체크	IKEv2 활성 검사는 항상 켜져 있습니다. 모든 IKEv2 패킷은 활성 검사의 목적으로 사용됩니다. 피어가 지정된 시간(초) 동안 유휴 상태인 후 시스템이 빈 정보 패킷을 보내도록 하려면 이 상자를 클릭합니다. 범위: 2-100. 기본: 5. 필요한 경우 IKEv2 패킷을 보내려는 쪽에서 활성 확인을 최대 10번 시도합니다(모든 IKEv2 패킷은 재전송 설정에 포함됨). 응답이 없으면 발신자는 IKE_SA 및 CHILD_SA를 닫고 삭제합니다. 발신자는 다른 IKE_SA_INIT를 전송하여 다시 시작합니다.

IKE 게이트웨이 다시 시작 또는 새로 고침

- 네트워크 > IPSec 터널

Network > **IPSec Tunnels**를 선택하여 터널의 상태를 표시합니다. 두 번째 상태 열에는 IKE 정보에 대한 링크가 있습니다. 다시 시작하거나 새로 고칠 게이트웨이를 클릭합니다. IKE 정보 페이지가 열립니다. 목록에서 항목 중 하나를 클릭하고 다음을 클릭합니다.

- 다시 시작 - 선택한 게이트웨이를 다시 시작합니다. 다시 시작하면 터널을 가로질러 가는 트래픽이 중단됩니다. IKEv1 및 IKEv2의 다시 시작 동작은 다음과 같이 다릅니다.
  - **IKEv1** - 1단계 SA 또는 2단계 SA를 독립적으로 다시 시작(지우기)할 수 있으며 해당 SA만 영향을 받습니다.
  - **IKEv2** - IKEv2 SA가 다시 시작될 때 모든 하위 SA(IPSec 터널)가 지워지도록 합니다.

    IKEv2 SA를 다시 시작하면 모든 기본 IPSec 터널도 지워집니다.

    IKEv2 SA와 연결된 IPSec 터널(하위 SA)을 다시 시작하면 다시 시작해도 IKEv2 SA에 영향을 주지 않습니다.
- 새로 고침 - 현재 IKE SA 상태를 표시합니다.

네트워크 > 네트워크 프로파일 > IPSec 암호화

네트워크 > 네트워크 프로파일 > **IPSec** 암호화를 선택하여 IPSec SA 협상(2단계)을 기반으로 VPN 터널에서 인증 및 암호화를 위한 프로토콜과 알고리즘을 지정하는 IPSec 암호화 프로파일을 구성합니다.

GlobalProtect 게이트웨이와 클라이언트 간의 *VPN* 터널에 대해서는 네트워크 > 네트워크 프로파일 > GlobalProtect IPSec Crypto를 참조하십시오.

IPSec 암호화 프로파일 설정	설명
이름	프로파일을 식별할 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
IPSec 프로토콜	VPN 터널을 통과하는 데이터를 보호하기 위한 프로토콜 선택: • **ESP** - Encapsulating Security Payload 프로토콜은 데이터를 암호화하고 소스를 인증하며 데이터 무결성을 확인합니다. • **AH** - 인증 헤더 프로토콜은 소스를 인증하고 데이터 무결성을 확인합니다. ***ESP*** 프로토콜은 인증뿐만 아니라 연결 기밀성(암호화)을 제공하기 때문에 사용합니다.
암호화(ESP 프로토콜만 해당)	추가를 클릭하고 원하는 암호화 알고리즘을 선택합니다. 최고의 보안을 위해 위로 이동 및 아래로 이동을 사용하여 순서(위에서 아래로)를 **aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm**(VM 시리즈 방화벽 이 옵션을 지원하지 않음), **aes-128-cbc** 및 **3des**로 변경합니다. **null**(암호화 없음)을 선택할 수도 있습니다.

IPSec 암호화 프로파일 설정	설명
	AES 암호화 형식을 사용합니다. *(3DES*는 약하고 취약한 알고리즘입니다.*)*
입증	추가를 클릭하고 원하는 인증 알고리즘을 선택합니다. 최고의 보안을 위해 위로 이동 및 아래로 이동을 사용하여 순서(위에서 아래로)를 **sha512**, **sha384**, **sha256**, **sha1**, **md5**로 변경합니다. **IPSec** 프로토콜이 **ESP**인 경우 없음(인증 없음)을 선택할 수도 있습니다. ***md5*** 및 ***sha1***은 안전하지 않으므로 ***sha256*** 이상의 인증을 사용하십시오. 단기 세션에는 ***sha256***을 사용하고 금융 거래와 같이 가장 안전한 인증이 필요한 트래픽에는 ***sha384*** 이상을 사용합니다.
DH 그룹	인터넷 키 교환(IKE)용 Diffie-Hellman(DH) 그룹 선택: **group1**, **group2**, **group5**, **group14**, 그룹**15**, 그룹**16**, 그룹**19**, 그룹**20** 또는 그룹**21**. 최고의 보안을 위해 가장 높은 숫자를 가진 그룹을 선택하십시오. 방화벽이 IKE 단계 1 동안 생성하는 키를 갱신하지 않으려면 **no-pfs**(완전한 순방향 비밀성 없음)를 선택합니다. 방화벽은 IPSec SA(보안 연결) 협상을 위해 현재 키를 재사용합니다.
유효 기간	단위를 선택한 다음 협상된 키가 유효하게 유지되는 시간 길이(기본값은 1시간)를 입력합니다.
실제 크기	옵션 단위를 선택한 다음 키가 암호화에 사용할 수 있는 데이터 양을 입력합니다.

네트워크 > 네트워크 프로파일 > IKE 암호화

IKE 암호화 프로파일 페이지를 사용하여 식별, 인증 및 암호화(IKEv1 또는 IKEv2, 1단계)를 위한 프로토콜 및 알고리즘을 지정합니다.

알고리즘 또는 그룹이 나열되는 순서를 변경하려면 항목을 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 원격 피어와 설정을 협상할 때 순서에 따라 첫 번째 선택 항목이 결정됩니다. 목록 맨 위에 있는 설정이 먼저 시도되고 성공할 때까지 목록 아래로 계속됩니다.

IKE 암호화 프로파일 설정	설명
이름	프로파일의 이름을 입력합니다.

IKE 암호화 프로파일 설정	설명
DH 그룹	Diffie-Hellman(DH) 그룹의 우선 순위를 지정합니다. 추가를 클릭하고 그룹(**group1**, **group2**, **group5**, **group14**, **group15**, **group16**, **group19**, **group20** 또는 **group21**)을 선택합니다. 최고의 보안을 위해 항목을 선택한 다음 위로 이동 또는 아래로 이동을 클릭하여 숫자 식별자가 더 높은 그룹을 목록의 맨 위로 이동합니다. 예를 들어 **group14**를 **group2** 위로 이동합니다.
인증	해시 알고리즘의 우선 순위를 지정합니다. 추가를 클릭하고 알고리즘을 선택합니다. 최고의 보안을 위해 항목을 선택한 다음 위로 이동 또는 아래로 이동을 클릭하여 순서(위에서 아래로)를 다음과 같이 변경합니다. • **sha512** • **sha384** • **sha256** • **sha1** • **md5** • 없음 암호화를 위해 *AES-GCM* 알고리즘을 선택하는 경우 인증 설정 없음을 선택해야 합니다. 해시는 선택한 *DH* 그룹에 따라 자동으로 선택됩니다. *DH* 그룹 *19* 이하에서는 ***sha256***을 사용합니다. *DH* 그룹 *20*은 ***sha384***를 사용합니다.
암호화	적절한 ESP(Encapsulating Security Payload) 인증 옵션을 선택합니다. 추가를 클릭하고 알고리즘을 선택합니다. 최고의 보안을 위해 항목을 선택한 다음 위로 이동 또는 아래로 이동을 클릭하여 순서(위에서 아래로)를 다음과 같이 변경합니다. • **aes-256-gcm**(IKEv2 필요, DH 그룹은 **group20**으로 설정해야 함) • **aes-128-gcm**(IKEv2 및 DH 그룹을 **group19**로 설정해야 함) • **aes-256-cbc** • **aes-192-cbc** • **aes-128-cbc** • **3des**

IKE 암호화 프로파일 설정	설명
	aes-256-gcm 및 ***aes-128-gcm*** 알고리즘에는 인증이 내장되어 있습니다. 따라서 이러한 경우에는 인증 설정을 없음으로 선택해야 합니다.
키 유효 시간	시간 단위를 선택한 다음 협상된 IKE 1단계 키가 유효한 시간을 입력합니다(기본값은 8시간). • IKEv2 - 키 유효 시간이 만료되기 전에 SA에 키를 다시 입력해야 합니다. 그렇지 않으면 만료 시 SA가 새로운 1단계 키 협상을 시작해야 합니다. • IKEv1 - 만료되기 전에 1단계 키 다시 입력을 적극적으로 수행하지 않습니다. IKEv1 IPSec SA가 만료된 경우에만 IKEv1 1단계 키 재입력을 트리거합니다.
IKEv2 인증 다중	인증 횟수를 결정하기 위해 키 유효 시간을 곱한 값(범위는 0-50, 기본값은 0)을 지정합니다. 인증 횟수는 게이트웨이가 IKEv2 재인증으로 다시 시작해야 하기 전에 게이트웨이가 IKEv2 IKE SA 키 재입력을 수행할 수 있는 횟수입니다. 값이 0이면 재인증 기능이 비활성화됩니다.

네트워크 > 네트워크 프로파일 > 모니터

모니터 프로파일은 IPSec 터널을 모니터링하고 PBF(정책 기반 포워딩) 규칙에 대한 다음 홉 디바이스를 모니터링하는 데 사용됩니다. 두 경우 모두 모니터 프로파일을 사용하여 리소스(IPSec 터널 또는 다음 홉 디바이스)를 사용할 수 없게 될 때 수행할 작업을 지정합니다. 모니터 프로파일은 선택 사항이지만 사이트 간의 연결을 유지하고 PBF 규칙이 유지되도록 하는 데 매우 유용할 수 있습니다. 다음 설정은 모니터 프로파일을 구성하는 데 사용됩니다.

필드	설명
이름	모니터 프로파일을 식별하는 이름을 입력합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
동작	터널을 사용할 수 없는 경우 수행할 작업을 지정합니다. 임계값 하트비트 수가 손실되면 방화벽은 지정된 작업을 수행합니다. • **wait-recover** - 터널이 복구될 때까지 기다립니다. 추가 조치를 취하지 마십시오. 패킷은 PBF 규칙에 따라 계속 전송됩니다.

필드	설명
	• 페일오버**(failover)** - 사용 가능한 경우 백업 경로로 트래픽이 페일오버 됩니다. 방화벽은 라우팅 테이블 조회를 사용하여 이 세션 기간 동안 라우팅을 결정합니다. 두 경우 모두 방화벽은 복구를 가속화하기 위해 새 IPSec 키를 협상하려고 합니다.
인터벌	하트비트 사이의 시간을 지정합니다(범위는 2~10, 기본값은 3).
임계값	방화벽이 지정된 작업을 수행하기 전에 손실될 하트비트 수를 지정합니다(범위는 2~10, 기본값은 5).

네트워크 > 네트워크 프로파일 > 인터페이스 관리

인터페이스 관리 프로파일은 방화벽 인터페이스가 허용하는 서비스와 IP 주소를 정의하여 무단 액세스로부터 방화벽을 보호합니다. 인터페이스 관리 프로파일을 레이어 3 이더넷 인터페이스(서브인터페이스 포함)와 논리적 인터페이스(통합 그룹, VLAN, 루프백 및 터널 인터페이스)에 할당할 수 있습니다. 인터페이스 관리 프로파일을 할당하려면 네트워크 > 인터페이스를 참조하십시오.

Telnet, SSH, HTTP 또는 *HTTPS*를 허용하는 인터페이스 관리 프로파일을 인터넷이나 엔터프라이즈 보안 경계 내의 다른 신뢰할 수 없는 영역에서 액세스할 수 있는 인터페이스에 연결하지 마십시오. 여기에는 *GlobalProtect* 포털 또는 게이트웨이를 구성한 인터페이스가 포함됩니다. *GlobalProtect*는 포털 또는 게이트웨이에 대한 액세스를 활성화하기 위해 인터페이스 관리 프로파일이 필요하지 않습니다. 방화벽 및 *Panorama*에 대한 액세스를 보호하는 방법에 대한 자세한 내용은 관리 액세스 모범 사례를 참조하십시오.

Telnet, SSH, HTTP 또는 *HTTPS*를 허용하는 인터페이스 관리 프로파일을 *GlobalProtect* 포털 또는 게이트웨이를 구성한 인터페이스에 연결하지 마십시오. 관리 인터페이스가 인터넷에 노출되기 때문입니다.

필드	설명
이름	프로파일 이름을 입력합니다(최대 **31**자). 이 이름은 인터페이스를 구성할 때 인터페이스 관리 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.

필드	설명
행정 관리 서비스	• **Telnet** - 방화벽 CLI에 액세스하는 데 사용합니다. Telnet은 SSH만큼 안전하지 않은 일반 텍스트를 사용합니다. 인터페이스의 관리 트래픽에 대해 *Telnet* 대신 *SSH*를 활성화합니다. • **SSH** - 방화벽 CLI에 대한 보안 액세스에 사용합니다. • **HTTP** - 방화벽 웹 인터페이스에 액세스하는 데 사용합니다. HTTP는 HTTPS만큼 안전하지 않은 일반 텍스트를 사용합니다. 인터페이스의 관리 트래픽에 대해 *HTTP* 대신 ***HTTPS***를 활성화합니다. • **HTTPS** - 방화벽 웹 인터페이스에 대한 보안 액세스에 사용합니다.

네트워크 서비스	• **Ping** - 외부 서비스와의 연결을 테스트하는 데 사용합니다. 예를 들어 인터페이스를 핑(ping)하여 Palo Alto Networks 업데이트 서버에서 PAN-OS 소프트웨어 및 콘텐츠 업데이트를 수신할 수 있는지 확인할 수 있습니다.
	• **HTTP OCSP** - 방화벽을 OCSP(온라인 인증서 상태 프로토콜) 응답자로 구성하는 데 사용합니다. 자세한 내용은 디바이스 > 인증서 관리 > OCSP 응답자를 참조하십시오.
	• **SNMP** - SNMP 관리자에서 방화벽 통계 쿼리를 처리하는 데 사용합니다. 자세한 내용은 SNMP 모니터링 활성화를 참조하십시오.
	• 응답 페이지 - 다음에 대한 응답 페이지를 활성화하는 데 사용합니다.
	  • 인증 포털 - 인증 포털 응답 페이지를 제공하는 데 사용되는 포트는 레이어 3 인터페이스에서 열린 상태로 유지됩니다. NTLM의 경우 포트 6080, SSL/TLS 서버 프로파일이 없는 인증 포털의 경우 6081, SSL/TLS 서버 프로파일이 있는 인증 포털의 경우 6082입니다. 자세한 내용은 디바이스 > 사용자 식별 > 인증 포털 설정을 참조하십시오.
	  • **URL** 관리 재정의 - 자세한 내용은 디바이스 > 설정 > Content-ID를 참조하십시오.
	• **User-ID** - 방화벽 간에 사용자 매핑의 데이터 재배포를 활성화하는 데 사용합니다.
	• **User-ID Syslog** 수신기-**SSL** - PAN-OS 통합 User-ID 에이전트가 SSL을 통해 syslog 메시지를 수집하도록 허용하는 데 사용합니다. 자세한 내용은 모니터링되는 서버에 대한 액세스 구성을 참조하십시오.
	• **User-ID Syslog Listener-UDP** - PAN-OS 통합 User-ID 에이전트가 UDP를 통해 syslog 메시지를 수집하도록 허용하는 데 사용합니다. 자세한 내용은 모니터링되는 서버에 대한 액세스 구성을 참조하십시오.

필드	설명
허용된 IP 주소	인터페이스에서 액세스를 허용하는 IPv4 또는 IPv6 주소 목록을 입력합니다.

네트워크 > 네트워크 프로파일 > 영역 보호

영역에 적용된 영역 보호 프로파일은 가장 일반적인 플러드, 정찰 공격, 기타 패킷 기반 공격, 비 IP 프로토콜 사용, 특정 SGT(보안 그룹 태그)가 있는 802.1Q(Ethertype 0x8909) 헤더에 대한 보호를 제공합니다. 영역 보호 프로파일은 수신 영역(트래픽이 방화벽으로 들어가는 영역)에서 광범위한 보호를 제공하도록 설계되었으며 특정 최종 호스트나 특정 대상 영역으로 가는 트래픽을 보호하도록 설계되지 않았습니다. 하나의 영역 보호 프로파일을 영역에 연결할 수 있습니다.

영역 보호 프로파일을 각 영역에 적용하여 *IP* 플러드, 정찰, 패킷 기반 공격 및 비 *IP* 프로토콜 공격에 대한 추가 보호 레이어를 만듭니다. 방화벽의 영역 보호는 인터넷 경계의 전용 *DDoS* 디바이스에 이어 두 번째 보호 레이어여야 합니다.

방화벽에서 영역 보호 기능을 강화하려면 특정 영역, 인터페이스, IP 주소 또는 사용자와 일치하도록 DoS 방어 정책(정책 > DoS 방어)을 구성합니다.

영역 보호는 *pps(*초당 패킷 수*)*가 아닌 *cps(*초당 새 연결 수*)*를 기반으로 하기 때문에 패킷에 대한 세션 일치가 없을 때만 적용됩니다. 패킷이 기존 세션과 일치하는 경우 영역 보호 설정을 무시합니다.

무엇을 찾고 계신가요?	참조:
영역 보호 프로파일은 어떻게 만듭니까?	영역 보호 프로파일의 빌딩 블록 플러드 방지 정찰 보호 패킷 기반 공격 보호 프로토콜 보호 이더넷 SGT 보호 L3 및 L4 헤더 검사

영역 보호 프로파일의 빌딩 블록

영역 보호 프로파일을 만들려면 프로파일을 추가하고 이름을 지정합니다.

영역 보호 프로파일 설정	구성 위치	설명
이름	네트워크 > 네트워크 프로파일 > 존 보호	프로파일 이름을 입력합니다(최대 31자). 이 이름은 영역을 구성할 때 영역 보호 프로파일 목록에 나타납니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백 및 밑줄만 사용하십시오.
설명		영역 보호 프로파일에 대한 선택적 설명을 입력합니다.

영역에 필요한 보호 유형에 따라 설정 조합을 구성하여 영역 보호 프로파일을 계속 생성합니다.

- 홍수 방지
- 정찰 보호
- 패킷 기반 공격 보호
- 프로토콜 보호
- 이더넷 SGT 보호

다중 가상 시스템 환경이 있고 다음을 활성화한 경우:

- 가상 시스템 간 통신을 가능하게 하는 외부 영역
- 가상 시스템이 외부 통신을 위해 공통 인터페이스와 단일 *IP* 주소를 공유할 수 있도록 하는 공유 게이트웨이

다음 영역 및 *DoS* 방어 메커니즘은 외부 영역에서 비활성화됩니다.

- *SYN* 쿠키
- *IP* 단편화
- *ICMPv6*

공유 게이트웨이에 대해 *IP* 조각화 및 *ICMPv6* 보호를 활성화하려면 공유 게이트웨이에 대해 별도의 영역 보호 프로파일을 생성해야 합니다.

공유 게이트웨이에서 *SYN* 플러드로부터 보호하기 위해 *Random Early Drop* 또는 *SYN* 쿠키를 사용하여 *SYN Flood* 보호 프로파일을 적용할 수 있습니다. 외부 영역에서는 *SYN Flood* 보호를 위해 *Random Early Drop*만 사용할 수 있습니다.

홍수 방지

- 네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호

SYN, ICMP, ICMPv6, SCTP INIT 및 UDP 패킷에 대한 플러드 보호는 물론 다른 유형의 IP 패킷으로부터의 플러딩에 대한 보호를 제공하는 프로파일을 구성합니다. 속도는 초당 연결 수입니다. 예를 들어, 기존 세션과 일치하지 않는 들어오는 SYN 패킷은 새 연결로 간주됩니다.

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
SYN	네트워크 > 네트워크 프로파일 > 존 보호 > 홍수 방지	SYN 플러드에 대한 보호를 활성화하려면 선택합니다.

동작		SYN 플러드 공격에 대응하여 수행할 작업을 선택합니다.
		• **Random Early Drop**—플러드 공격을 완화하기 위해 SYN 패킷을 삭제합니다.
		  • 흐름이 경보 비율 임계값을 초과하면 경보가 생성됩니다.
		  • 흐름이 활성화 속도 임계값을 초과하면 방화벽은 흐름을 제한하기 위해 개별 SYN 패킷을 무작위로 삭제합니다.
		  • 흐름이 최대 속도 임계값을 초과하면 들어오는 SYN 패킷의 100%가 삭제됩니다.
		• **SYN** 쿠키 - 방화벽이 프록시처럼 작동하고, SYN을 가로채고, SYN이 전달된 서버를 대신하여 쿠키를 생성하고, 쿠키와 함께 SYN-ACK를 원래 소스로 보냅니다. 소스가 쿠키가 포함된 ACK를 방화벽에 반환할 때만 방화벽은 소스를 유효한 것으로 간주하고 SYN을 서버에 포워딩합니다. 이것은 기본 동작입니다.
		SYN 쿠키가 활성화되면 방화벽은 SYN/ACK를 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.

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
		서버 경로의 MSS가 방화벽의 기본 MSS 값보다 작은 시나리오에서는 패킷을 조각화해야 합니다. *SYN* 쿠키는 합법적인 트래픽을 공정하게 처리하지만 *RED*보다 더 많은 방화벽 리소스를 소비합니다. *SYN* 쿠키가 너무 많은 리소스를 소비하는 경우 *RED*로 전환하십시오. 방화벽 앞*(*인터넷 경계*)*에 전용 *DDoS* 방지 디바이스가 없는 경우 항상 *RED*를 사용하십시오.
경보율(연결/초)	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	영역이 알람을 트리거하는 초당 수신하는 SYN 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 대시보드 및 위협 로그(모니터 > 패킷 캡처)에서 경보를 볼 수 있습니다. 범위는 0~2,000,000입니다. 기본값은 10,000입니다. 임계값을 평균 구역 *CPS* 비율보다 *15-20%* 높게 설정하여 정상적인 변동을 수용하고 과도한 경보를 수신하는 경우 임계값을 조정하십시오.
활성화(연결/초)		이 영역 보호 프로파일에 지정된 작업을 트리거하는 초당 영역에서 수신하는 SYN 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 방화벽은 공격 속도가 증가함에 따라 속도가 최대 속도에 도달할 때까지 더 많은 패킷을 점진적으로 삭제하는 알고리즘을 사용합니다. 방화벽은 들어오는 속도가 활성화 임계값 아래로 떨어지면 SYN 패킷 삭제를 중지합니다. RED의 경우 범위는 1~2,000,000이고 기본값은 10,000입니다. SYN 쿠키의 경우 범위는 0~2,000,000이고 기본값은 0입니다. 영역의 최고 *CPS* 속도 바로 위에 임계값을 설정하여 합법적인 트래픽을 제한하지 않고 필요에 따라 임계값을 조정합니다.
최대(연결/초)		최대값을 초과하는 패킷이 삭제되기 전에 영역이 초당 수신하는 최대 SYN 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 범위는 1~2,000,000입니다. 기본값은 RED의 경우 40,000입니다. 기본값은 SYN 쿠키의 경우

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
		1,000,000입니다. 이 임계값을 초과하면 CPS 비율이 임계값 아래로 떨어질 때까지 새 연결이 차단됩니다. 방화벽 리소스를 소비하는 다른 기능을 고려하여 임계값을 방화벽 용량의 *80-90%*로 설정합니다.
ICMP	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	ICMP 플러드에 대한 보호를 활성화하려면 선택합니다.
경보율(연결/초)		영역이 공격 경보를 트리거하는 초당 수신 ICMP 에코 요청(기존 세션과 일치하지 않는 핑) 수를 입력합니다. 범위는 0-2,000,000입니다. 기본값은 10,000입니다. 임계값을 평균 구역 *CPS* 비율보다 *15-20%* 높게 설정하여 정상적인 변동을 수용하고 과도한 경보를 수신하는 경우 임계값을 조정하십시오.
활성화(연결/초)		후속 ICMP 패킷이 삭제되기 전에 영역이 초당 수신하는 ICMP 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 방화벽은 공격 속도가 증가함에 따라 속도가 최대 속도에 도달할 때까지 더 많은 패킷을 점진적으로 삭제하는 알고리즘을 사용합니다. 방화벽은 수신 속도가 활성화 임계값 아래로 떨어지면 ICMP 패킷 삭제를 중지합니다. 범위는 1~2,000,000입니다. 기본값은 10,000입니다. 영역의 최고 *CPS* 속도 바로 위에 임계값을 설정하여 합법적인 트래픽을 제한하지 않고 필요에 따라 임계값을 조정합니다.
최대(연결/초)		최대값을 초과하는 패킷이 삭제되기 전에 영역이 초당 수신하는 ICMP 패킷(기존 세션과 일치하지 않음)의 최대 수를 입력합니다. 범위는 1~2,000,000입니다. 기본값은 40,000입니다. 방화벽 리소스를 소비하는 다른 기능을 고려하여 임계값을 방화벽 용량의 *80-90%*로 설정합니다.

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
SCTP INIT	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	INIT(초기화) 청크가 포함된 SCTP(스트림 제어 전송 프로토콜) 패킷의 플러드에 대한 보호를 활성화하려면 선택합니다. INIT 청크는 다른 청크와 번들로 묶일 수 없으므로 SCTP INIT 패킷이라고 합니다.
경보율(연결/초)		영역이 공격 경보를 트리거하는 초당 수신 SCTP INIT 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 범위는 0-2,000,000입니다. 방화벽 모델별 기본값은 다음과 같습니다. • **PA-5280**—10,000 • **PA-5260**—7,000 • **PA-5250**—5,000 • **PA-5220**—3,000 • **VM-700**—1,000 • **VM-500**—500 • **VM-300**—250 • **VM-100**—200 • **VM-50**—100
활성화(연결/초)		후속 SCTP INIT 패킷이 삭제되기 전에 영역이 초당 수신하는 SCTP INIT 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 방화벽은 공격 속도가 증가함에 따라 속도가 최대 속도에 도달할 때까지 더 많은 패킷을 점진적으로 삭제하는 알고리즘을 사용합니다. 방화벽은 들어오는 속도가 활성화 임계값 아래로 떨어지면 SCTP INIT 패킷 삭제를 중지합니다. 범위는 1~2,000,000입니다. 방화벽 모델별 기본값은 경보율과 동일합니다.
최대(연결/초)	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	최대값을 초과하는 패킷이 삭제되기 전에 영역이 초당 수신하는 SCTP INIT 패킷(기존 세션과 일치하지 않음)의 최대 수를 입력합니다. 범위는 1~2,000,000입니다. 방화벽 모델별 기본값은 다음과 같습니다. • **PA-5280**—20,000 • **PA-5260**—14,000 • **PA-5250**—10,000

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
		• **PA-5220**—6,000 • **VM-700**—2,000 • **VM-500**—1,000 • **VM-300**—500 • **VM-100**—400 • **VM-50**—200
UDP	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	UDP 플러드에 대한 보호를 활성화하려면 선택합니다.
경보율(연결/초)		공격 경보를 트리거하는 초당 수신하는 UDP 패킷(기존 세션과 일치하지 않음)의 수를 입력합니다. 범위는 0-2,000,000입니다. 기본값은 10,000입니다. 임계값을 평균 구역 *CPS* 비율보다 *15-20%* 높게 설정하여 정상적인 변동을 수용하고 과도한 경보를 수신하는 경우 임계값을 조정하십시오.
활성화(연결/초)		UDP 패킷의 무작위 삭제를 트리거하는 초당 수신하는 UDP 패킷(기존 세션과 일치하지 않음)의 수를 입력합니다. 방화벽은 공격 속도가 증가함에 따라 속도가 최대 속도에 도달할 때까지 더 많은 패킷을 점진적으로 삭제하는 알고리즘을 사용합니다. 방화벽은 들어오는 속도가 활성화 임계값 아래로 떨어지면 UDP 패킷 삭제를 중지합니다. 범위는 1~2,000,000입니다. 기본값은 10,000입니다. 영역의 최고 *CPS* 속도 바로 위에 임계값을 설정하여 합법적인 트래픽을 제한하지 않고 필요에 따라 임계값을 조정합니다.
최대(연결/초)		최대값을 초과하는 패킷이 삭제되기 전에 영역이 수신하는 초당 최대 UDP 패킷 수(기존 세션과 일치하지 않음)를 입력합니다. 범위는 1~2,000,000입니다. 기본값은 40,000입니다.

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
		방화벽 리소스를 소비하는 다른 기능을 고려하여 임계값을 방화벽 용량의 *80-90%*로 설정합니다.
ICMPv6	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	ICMPv6 플러드에 대한 보호를 활성화하려면 선택합니다.
경보율(연결/초)		영역이 공격 경보를 트리거하는 초당 수신 ICMPv6 에코 요청(기존 세션과 일치하지 않는 핑) 수를 입력합니다. 범위는 0-2,000,000입니다. 기본값은 10,000입니다. 임계값을 평균 구역 *CPS* 비율보다 *15-20%* 높게 설정하여 정상적인 변동을 수용하고 과도한 경보를 수신하는 경우 임계값을 조정하십시오.
활성화(연결/초)		후속 ICMPv6 패킷이 삭제되기 전에 영역이 초당 수신하는 ICMPv6 패킷(기존 세션과 일치하지 않음) 수를 입력합니다. 방화벽은 공격 속도가 증가함에 따라 속도가 최대 속도에 도달할 때까지 더 많은 패킷을 점진적으로 삭제하는 알고리즘을 사용합니다. 방화벽은 수신 속도가 활성화 임계값 아래로 떨어지면 ICMPv6 패킷 삭제를 중지합니다. 범위는 1~2,000,000입니다. 기본값은 10,000입니다. 영역의 최고 *CPS* 속도 바로 위에 임계값을 설정하여 합법적인 트래픽을 제한하지 않고 필요에 따라 임계값을 조정합니다.
최대(연결/초)		최대값을 초과하는 패킷이 삭제되기 전에 영역이 초당 수신하는 ICMPv6 패킷(기존 세션과 일치하지 않음)의 최대 수를 입력합니다. 범위는 1~2,000,000입니다. 기본값은 40,000입니다. 방화벽 리소스를 소비하는 다른 기능을 고려하여 임계값을 방화벽 용량의 *80-90%*로 설정합니다.

영역 보호 프로파일 설정 - 플러드 방지	구성 위치	설명
기타 **IP**	네트워크 > 네트워크 프로파일 > 영역 보호 > 플러드 보호(계속)	다른 IP(비 TCP, 비 ICMP, 비 ICMPv6, 비 SCTP 및 비 UDP) 플러드에 대한 보호를 활성화하려면 선택합니다.
경보율(연결/초)		영역이 공격 경보를 트리거하는 초당 수신하는 기타 IP 패킷(비 TCP, 비 ICMP, 비 ICMPv6, 비 SCTP 및 비 UDP 패킷)(기존 세션과 일치하지 않음)의 수를 입력합니다. 범위는 0-2,000,000입니다. 기본값은 10,000입니다. 임계값을 평균 구역 *CPS* 비율보다 *15-20%* 높게 설정하여 정상적인 변동을 수용하고 과도한 경보를 수신하는 경우 임계값을 조정하십시오.
활성화(연결/초)		다른 IP 패킷의 무작위 삭제를 트리거하는 초당 수신하는 다른 IP 패킷(비 TCP, 비 ICMP, 비 ICMPv6 및 비 UDP 패킷)(기존 세션과 일치하지 않음)의 수를 입력합니다. 방화벽은 공격 속도가 증가함에 따라 속도가 최대 속도에 도달할 때까지 더 많은 패킷을 점진적으로 삭제하는 알고리즘을 사용합니다. 방화벽은 수신 속도가 활성화 임계값 아래로 떨어지면 기타 IP 패킷 삭제를 중지합니다. 범위는 1~2,000,000입니다. 기본값은 10,000입니다. 영역의 최고 *CPS* 속도 바로 위에 임계값을 설정하여 합법적인 트래픽을 제한하지 않고 필요에 따라 임계값을 조정합니다.
최대(연결/초)		최대값을 초과하는 패킷이 삭제되기 전에 영역이 초당 수신하는 다른 IP 패킷(비 TCP, 비 ICMP, 비 ICMPv6 및 비 UDP 패킷)(기존 세션과 일치하지 않음)의 최대 수를 입력합니다. 범위는 1~2,000,000입니다. 기본값은 40,000입니다. 방화벽 리소스를 소비하는 다른 기능을 고려하여 임계값을 방화벽 용량의 *80-90%*로 설정합니다.

정찰 보호

- 네트워크 > 네트워크 프로파일 > 영역 보호 > 정찰 보호

다음 설정은 정찰 보호를 정의합니다.

영역 보호 프로파일 설정 - 정찰 보호	구성 위치	설명
TCP 포트 스캔	네트워크 > 네트워크 프로파일 > 존 보호 > 정찰 보호	활성화는 TCP 포트 스캔에 대한 보호를 활성화하도록 프로파일을 구성합니다.
UDP 포트 스캔		활성화는 UDP 포트 스캔에 대한 보호를 활성화하도록 프로파일을 구성합니다.
호스트 스윕		활성화는 호스트 스윕에 대한 보호를 활성화하도록 프로파일을 구성합니다.
작업		해당 정찰 시도에 대한 응답으로 시스템이 취하는 조치: • 허용 - 포트 스캔 또는 호스트 스윕 정찰을 허용합니다. • 경고 - 지정된 시간 인터벌(기본 작업) 내에서 임계값과 일치하는 각 포트 스캔 또는 호스트 스윕에 대한 경고를 생성합니다. • 차단 - 지정된 시간 인터벌의 나머지 동안 소스에서 대상으로의 모든 후속 패킷을 삭제합니다. • **IP** 차단 - 지정된 기간(초) 동안 모든 후속 패킷을 삭제합니다(범위는 1-3,600). 추적 기준은 소스 또는 소스 및 대상 트래픽을 차단할지의 여부를 결정합니다. 예를 들어, 단일 소스에서 오는 인터벌당 임계값 수를 초과하는 차단 시도(더 엄격함) 또는 소스 및 대상 쌍이 있는 차단 시도(덜 엄격함)가 있습니다. 내부 취약성 테스트 스캔을 제외한 모든 정찰 스캔을 차단합니다.
인터벌(초)		TCP 또는 UDP 포트 스캔 감지를 위한 시간 인터벌(초)입니다(범위는 2-65,535, 기본값은 2). 호스트 스윕 감지를 위한 시간 인터벌(초)입니다(범위는 2-65,535, 기본값은 10).
임계값(이벤트)		작업을 트리거하는 지정된 시간 인터벌 내에서 검색된 포트 이벤트 또는 호스트 스윕 이벤트의 수(범위는 2-65,535, 기본값은 100).

영역 보호 프로파일 설정 - 정찰 보호	구성 위치	설명
		기본 이벤트 임계값을 사용하여 정찰 시도를 차단하기 전에 분석을 위해 몇 가지 패킷을 기록합니다.
소스 주소 제외		정찰 보호에서 제외할 IP 주소입니다. 목록은 최대 20개의 IP 주소 또는 넷마스크 주소 개체를 지원합니다. • 이름 - 제외할 주소를 설명하는 이름을 입력합니다. • 주소 유형 - 드롭다운에서 IPv4 또는 IPv6을 선택합니다. • 주소 - 드롭다운에서 주소 또는 주소 개체를 선택하거나 수동으로 입력합니다. 취약성 테스트를 수행하는 신뢰할 수 있는 내부 그룹의 *IP* 주소만 제외합니다.

패킷 기반 공격 보호

- 네트워크 > 네트워크 프로파일 > 영역 보호 > 패킷 기반 공격 보호

다음 유형의 패킷을 삭제하도록 패킷 기반 공격 보호를 구성할 수 있습니다.

- IP 드롭
- TCP 드롭
- ICMP 드롭
- IPv6 드롭
- ICMPv6 드롭

IP 드롭

영역에서 수신하는 특정 IP 패킷을 어떻게 처리할지 방화벽에 지시하려면 다음 설정을 지정하십시오.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
스푸핑된 IP 주소	네트워크 > 네트워크 프로파일 > 존 보호 >	수신 패킷의 소스 IP 주소가 라우팅 가능하고 라우팅 인터페이스가 수신 인터페이스와 동일한 영역에 있는지 확인하십시오. 두 조건 중 하나라도 참이 아니면 패킷을 버립니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
	패킷 기반 공격 보호 > **IP** 드롭	방화벽은 이 검사 중에 *PBF(*정책 기반 포워딩*)* 규칙을 고려하지 않습니다. 라우팅 테이블*(RIB)*에 나열된 경로, 즉 *### ## ##*에 대한 *CLI* 출력 아래에 나열된 경로만 고려합니다. 내부 영역에서만 스푸핑된 *IP* 주소 패킷을 삭제하여 수신 시 소스 주소가 방화벽 라우팅 테이블과 일치하도록 합니다.
엄격한 IP 주소 확인		두 조건이 모두 참인지 확인합니다. • 소스 IP 주소는 수신 인터페이스의 서브넷 브로드캐스트 IP 주소가 아닙니다. • 소스 IP 주소는 정확한 수신 인터페이스를 통해 라우팅할 수 있습니다. 두 조건 중 하나라도 참이 아니면 패킷을 버립니다. 방화벽은 이 검사 중에 *PBF(*정책 기반 포워딩*)* 규칙을 고려하지 않습니다. 라우팅 테이블*(RIB)*에 나열된 경로, 즉 *### ## ##*에 대한 *CLI* 출력 아래에 나열된 경로만 고려합니다. CC(Common Criteria) 모드의 방화벽의 경우 폐기된 패킷에 대한 로깅을 활성화할 수 있습니다. 방화벽 웹 인터페이스에서 **Device** > **Log** 설정을 선택합니다. 로그 관리 섹션에서 선택적 감사를 선택한 다음 패킷 삭제 로깅을 활성화합니다.
분산 트래픽		분산된 IP 패킷을 버립니다.
IP 옵션 삭제		방화벽이 이러한 IP 옵션을 포함하는 패킷을 삭제할 수 있도록 하려면 이 그룹의 설정을 선택합니다.
Strict Source Routing		Strict Source Routing IP 옵션이 설정된 패킷을 버립니다. Strict Source Routing은 데이터그램의 소스가 게이트웨이나 호스트가 데이터그램을 보내야 하는 라우팅 정보를 제공하는 옵션입니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
		소스 라우팅을 사용하면 공격자가 대상 *IP* 주소를 일치 기준으로 사용하는 보안 정책 규칙을 우회할 수 있으므로 엄격한 소스 라우팅으로 패킷을 삭제합니다.
느슨한 소스 라우팅		느슨한 소스 라우팅 IP 옵션이 설정된 패킷을 버립니다. 느슨한 소스 라우팅은 데이터그램의 소스가 라우팅 정보를 제공하고 게이트웨이 또는 호스트가 경로의 다음 주소로 데이터그램을 가져오기 위해 여러 중간 게이트웨이 중 임의의 경로를 선택할 수 있는 옵션입니다. 소스 라우팅을 사용하면 공격자가 대상 *IP* 주소를 일치 기준으로 사용하는 보안 정책 규칙을 우회할 수 있으므로 느슨한 소스 라우팅으로 패킷을 삭제합니다.
타임스탬프		Timestamp IP 옵션이 설정된 패킷을 버립니다.
경로 기록		Record Route IP 옵션이 설정된 패킷을 버립니다. 데이터그램에 이 옵션이 있으면 데이터그램을 라우팅하는 각 라우터는 헤더에 고유한 IP 주소를 추가하여 수신자에게 경로를 제공합니다.
보안		보안 옵션이 정의된 경우 패킷을 버립니다.
스트림 ID		스트림 ID 옵션이 정의된 경우 패킷을 버립니다.
알 수 없음		클래스와 번호를 알 수 없는 경우 패킷을 버립니다. 알 수 없는 패킷을 버립니다.
변칙		RFC 791, 1108, 1393 및 2113에 따라 클래스, 번호 및 길이의 잘못된 조합이 있는 패킷은 버립니다. 잘못된 패킷을 폐기하십시오.

TCP 드롭

방화벽이 영역에서 수신하는 특정 TCP 패킷에 대해 수행할 작업을 지시하려면 다음 설정을 지정하십시오.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
일치하지 않고 겹치는 TCP 세그먼트	네트워크 > 네트워크 프로파일 > 존 보호 > 패킷 기반 공격 보호 > **TCP** 드롭	공격자는 중복되지만 다른 데이터로 연결을 구성하여 연결을 잘못 해석할 수 있습니다. 공격자는 IP 스푸핑 및 시퀀스 번호 예측을 사용하여 사용자의 연결을 가로채고 자체 데이터를 삽입할 수 있습니다. 다음 시나리오에서 세그먼트 데이터가 일치하지 않을 때 중복 불일치를 보고하고 패킷을 삭제하려면 이 설정을 사용하십시오. • 세그먼트가 다른 세그먼트 내에 있습니다. • 세그먼트가 다른 세그먼트의 일부와 겹칩니다. • 세그먼트는 다른 세그먼트를 포함합니다. 이 보호 메커니즘은 시퀀스 번호를 사용하여 TCP 데이터 스트림 내에서 패킷이 상주하는 위치를 결정합니다. 일치하지 않는 겹치는 *TCP* 세그먼트가 있는 패킷을 삭제합니다.
스플릿 핸드쉐이크		세션 설정 절차가 잘 알려진 3방향 핸드쉐이크를 사용하지 않는 경우 TCP 세션이 설정되지 않도록 합니다. 4방향 또는 5방향 스플릿 핸드쉐이크 또는 동시 개방형 세션 설정 절차는 허용되지 않는 변형의 예입니다. Palo Alto Networks 차세대 방화벽은 스플릿 핸드쉐이크를 구성하지 않고도 스플릿 핸드쉐이크 및 동시 개방형 세션 설정을 위한 세션 및 모든 레이어 7 프로세스를 올바르게 처리합니다. 이것이 영역 보호 프로파일에 대해 구성되고 프로파일이 영역에 적용되는 경우 표준 3방향 핸드쉐이크를 사용하여 해당 영역의 인터페이스에 대한 TCP 세션을 설정해야 합며, 변형은 허용되지 않습니다. 스플릿 핸드쉐이크를 사용하여 패킷을 삭제합니다.
데이터가 있는 TCP SYN		3방향 핸드쉐이크 동안 TCP SYN 패킷에 데이터가 포함된 경우 TCP 세션이 설정되지 않도록 합니다. 기본적으로 활성화되어 있습니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
데이터가 있는 TCP SYNACK		3방향 핸드쉐이크 동안 TCP SYN-ACK 패킷에 데이터가 포함된 경우 TCP 세션이 설정되지 않도록 합니다. 기본적으로 활성화되어 있습니다.
비 SYN TCP 거부		TCP 세션 설정의 첫 번째 패킷이 SYN 패킷이 아닌 경우 패킷을 거부할지의 여부를 결정합니다. • 전역 - CLI를 통해 할당된 시스템 전체 설정을 사용합니다. • **yes** - 비 SYN TCP를 거부합니다. • **no** - SYN이 아닌 TCP를 수락합니다. 비 *SYN TCP* 트래픽을 허용하면 차단이 발생한 후 클라이언트 및/또는 서버 연결이 설정되지 않은 경우 파일 차단 정책이 예상대로 작동하지 않을 수 있습니다. 영역에서 터널 콘텐츠 검사를 구성하고 세션 재일치를 활성화한 경우 해당 영역에 대해서만 ***Reject Non-SYN TCP***를 비활성화하여 터널 콘텐츠 검사 정책을 활성화하거나 편집해도 방화벽이 기존 터널 세션을 삭제하지 않도록 합니다.
비대칭 경로		동기화되지 않은 ACK 또는 윈도우 외 시퀀스 번호가 포함된 패킷을 삭제할지 우회할지 결정합니다. • 전역 - **TCP** 설정 또는 CLI를 통해 할당된 시스템 전체 설정을 사용합니다. • 드롭 - 비대칭 경로가 포함된 패킷을 삭제합니다. • 우회 - 비대칭 경로가 포함된 패킷에 대한 스캔을 우회합니다.
스트립 TCP 옵션		TCP 패킷에서 TCP 타임스탬프 또는 TCP Fast Open 옵션을 제거할지의 여부를 결정합니다.
TCP 타임스탬프	네트워크 > 네트워크 프로파일 > 존 보호 > 패킷 기반 공격	패킷 헤더에 TCP 타임스탬프가 있는지 확인하고 있으면 헤더에서 타임스탬프를 제거합니다. 타임스탬프 *DoS* 공격을 방지하기 위해 패킷에서 *TCP* 타임스탬프를 제거합니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
	보호 > **TCP** 드롭	
TCP 빠른 열기		TCP 3방향 핸드쉐이크가 진행되는 동안 TCP SYN 또는 SYN-ACK 패킷에서 TCP Fast Open 옵션(및 데이터 페이로드가 있는 경우)을 제거합니다. 이 옵션을 선택 취소(비활성화)하면 데이터 포워딩을 포함하여 연결 설정 속도를 유지하는 TCP Fast Open 옵션이 허용됩니다. 이것은 데이터가 있는 TCP SYN 및 데이터가 있는 TCP SYN-ACK와 독립적으로 작동합니다. 기본적으로 비활성화되어 있습니다.
다중 경로 TCP(MPTCP) 옵션		MPTCP는 클라이언트가 여러 경로를 사용하여 동시에 대상 호스트에 연결하여 연결을 유지할 수 있도록 하는 TCP의 확장입니다. 기본적으로 MPTCP 지원은 전역 MPTCP 설정에 따라 비활성화됩니다. 이 프로파일과 연결된 보안 영역에 대한 MPTCP 설정을 검토하거나 조정합니다. • **no** - MPTCP 지원을 활성화합니다(MPTCP 옵션을 제거하지 않음). • **yes** - MPTCP 지원을 비활성화합니다(MPTCP 옵션 제거). 이렇게 구성하면 MPTCP가 TCP와 역호환되기 때문에 MPTCP 연결이 표준 TCP 연결로 변환됩니다. • **(기본값) global** - 전역 MPTCP 설정을 기반으로 MPTCP를 지원합니다. 기본적으로 전역 MPTCP 설정은 yes로 설정되어 MPTCP가 비활성화됩니다(MPTCP 옵션이 패킷에서 제거됨). **TCP** 설정의 **Strip MPTCP** 옵션을 사용하거나 다음 CLI 명령을 통해 전역 MPTCP 설정을 검토하거나 조정할 수 있습니다. `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

ICMP 드롭

영역에서 수신하는 특정 ICMP 패킷을 삭제하도록 방화벽에 지시하려면 다음 설정을 선택하여 활성화합니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
ICMP Ping ID 0	네트워크 > 네트워크 프로파일 > 존 보호 > 패킷 기반 공격 보호 > **ICMP** 드롭	ICMP 핑(ping) 패킷의 식별자 값이 0인 경우 패킷을 버립니다.
ICMP 조각		ICMP 조각으로 구성된 패킷을 버립니다.
ICMP 대형 패킷(>1024)		1024바이트보다 큰 ICMP 패킷을 버립니다.
오류 메시지가 포함된 ICMP 폐기		오류 메시지가 포함된 ICMP 패킷을 버립니다.
ICMP TTL 만료 오류 억제		ICMP TTL 만료된 메시지 전송을 중지합니다.
필요한 ICMP 조각 억제		인터페이스 MTU를 초과하고 조각화 금지(DF) 비트가 설정된 패킷에 대한 응답으로 ICMP 조각화 필요 메시지 전송을 중지합니다. 이 설정은 방화벽 뒤의 호스트가 수행하는 PMTUD 프로세스를 방해합니다.

IPv6 드롭

영역에서 수신하는 특정 IPv6 패킷을 삭제하도록 방화벽에 지시하려면 다음 설정을 선택하여 활성화합니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
유형 0 라우팅 제목	네트워크 > 네트워크 프로파일 > 존 보호 > 패킷 기반 공격 보호 > **IPv6** 드롭	유형 0 라우팅 헤더가 포함된 IPv6 패킷을 삭제합니다. 유형 0 라우팅 헤더 정보는 RFC 5095를 참조하십시오.
IPv4 호환 주소		RFC 4291 IPv4 호환 IPv6 주소로 정의된 IPv6 패킷을 삭제합니다.
애니캐스트 소스 주소		애니캐스트 소스 주소가 포함된 IPv6 패킷을 삭제합니다.
불필요한 조각 헤더		마지막 조각 플래그(M=0)와 오프셋이 0인 IPv6 패킷을 버립니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
ICMP 'Packet Too Big'의 MTU가 1280바이트 미만		MTU(최대 전송 단위)가 1,280바이트 미만인 경우 Packet Too Big ICMPv6 메시지가 포함된 IPv6 패킷을 버립니다.
홉 바이 홉 확장		홉별 옵션 확장 헤더가 포함된 IPv6 패킷을 삭제합니다.
라우팅 확장		목적지로 가는 도중에 하나 이상의 중간 노드로 패킷을 보내는 라우팅 확장 헤더가 포함된 IPv6 패킷을 버립니다.
대상 확장		패킷의 대상에 대해서만 의도된 옵션이 포함된 Destination Options 확장이 포함된 IPv6 패킷을 버리십시오.
확장 헤더의 잘못된 IPv6 옵션		확장 헤더에 잘못된 IPv6 옵션이 포함된 IPv6 패킷을 삭제합니다.
0이 아닌 예약 필드		예약 필드가 0으로 설정되지 않은 헤더가 있는 IPv6 패킷을 버립니다.

ICMPv6 드롭

방화벽이 영역에서 수신하는 특정 ICMPv6 패킷으로 수행할 작업을 지시하려면 다음 설정을 선택하여 활성화합니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
ICMPv6 대상에 연결할 수 없음 - 명시적 보안 규칙 일치 필요	네트워크 > 네트워크 프로파일 > 존 보호 > 패킷 기반 공격 보호 > **ICMPv6** 드롭	메시지가 기존 세션과 연결된 경우에도 Destination Unreachable ICMPv6 메시지에 대해 명시적 보안 정책 일치가 필요합니다.
ICMPv6 패킷이 너무 큼 - 명시적 보안 규칙		메시지가 기존 세션과 연결된 경우에도 Packet Too Big ICMPv6 메시지에 대해 명시적 보안 정책 일치가 필요합니다.

영역 보호 프로파일 설정 - 패킷 기반 공격 보호	구성 위치	설명
일치가 필요합니다.		
ICMPv6 타임 아웃 - 명시적 보안 규칙 일치 필요		메시지가 기존 세션과 연결된 경우에도 Time Exceeded ICMPv6 메시지에 대해 명시적 보안 정책 일치가 필요합니다.
ICMPv6 매개 변수 문제 - 명시적 보안 규칙 일치 필요		메시지가 기존 세션과 연결된 경우에도 매개변수 문제 ICMPv6 메시지에 대해 명시적 보안 정책 일치가 필요합니다.
ICMPv6 리디렉션 - 명시적 보안 규칙 일치 필요		메시지가 기존 세션과 연결된 경우에도 메시지 리디렉션 ICMPv6 메시지에 대해 명시적 보안 정책 일치가 필요합니다.

프로토콜 보호

- 네트워크 > 네트워크 프로파일 > 영역 보호 > 프로토콜 보호

방화벽은 일반적으로 레이어 2 영역과 가상 와이어 영역 사이에 비 IP 프로토콜을 허용합니다. 프로토콜 보호를 사용하면 레이어 2 VLAN 또는 가상 와이어의 보안 영역 사이 또는 내부에서 허용(포함) 또는 거부(제외)되는 비 IP 프로토콜을 제어할 수 있습니다. 비 IP 프로토콜의 예로는 AppleTalk, Banyan VINES, Novell, NetBEUI 및 GOOSE(Generic Object Oriented Substation Event)와 같은 SCADA(Supervisory Control and Data Acquisition) 시스템이 있습니다.

영역 보호 프로파일에서 프로토콜 보호를 구성한 후 레이어 2 VLAN 또는 가상 와이어의 수신 보안 영역에 프로파일을 적용합니다.

인터넷 연결 영역에서 프로토콜 보호를 활성화하여 사용하지 않는 프로토콜의 레이어 *2* 트래픽이 네트워크에 들어오는 것을 방지합니다.

영역 보호 프로파일 설정 - 프로토콜 보호	구성 위치	설명
규칙 유형	네트워크 > 네트워크 프로파	프로토콜 보호를 위해 생성 중인 목록 유형을 지정합니다.

영역 보호 프로파일 설정 - 프로토콜 보호	구성 위치	설명
	일 > 존 보호 > 프로토콜 보호	• 목록 포함 - IPv4(0x0800), IPv6(0x86DD), ARP(0x0806) 및 VLAN 태그 프레임(0x8100) 외에 목록에 있는 프로토콜만 허용됩니다. 다른 모든 프로토콜은 암시적으로 거부(차단)됩니다. • 목록 제외 - 목록에 있는 프로토콜만 거부됩니다. 다른 모든 프로토콜은 암시적으로 허용됩니다. IPv4(0x0800), IPv6(0x86DD), ARP(0x0806) 또는 VLAN 태그 프레임(0x8100)은 제외할 수 없습니다. 포함 목록을 사용하여 사용하는 레이어 *2* 프로토콜만 허용하고 다른 모든 프로토콜은 거부합니다. 이렇게 하면 네트워크에서 사용하지 않는 프로토콜을 거부하여 공격 면적을 줄일 수 있습니다. 방화벽은 제외 목록에 추가한 프로토콜만 거부하고 목록에 없는 다른 모든 프로토콜은 허용합니다. 프로토콜 보호를 구성하지 않으면 모든 레이어 *2* 프로토콜이 허용됩니다.
프로토콜 이름		목록에 추가하려는 Ethertype 코드에 해당하는 프로토콜 이름을 입력합니다. 방화벽은 프로토콜 이름이 Ethertype 코드와 일치하는지 확인하지 않지만 Ethertype 코드는 프로토콜 필터를 결정합니다.
활성화		목록에서 Ethertype 코드를 활성화합니다. 테스트 목적으로 프로토콜을 비활성화하지만 삭제하지 않으려면 대신 비활성화하십시오.
Ethertype(16진수)		16진수를 나타내기 위해 0x가 앞에 오는 Ethertype 코드(프로토콜)를 입력합니다(범위는 0x0000 ~ 0xFFFF). 목록은 최대 64개의 Ethertype을 가질 수 있습니다. Ethertype 코드의 일부 소스는 다음과 같습니다. • IEEE 16진수 Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

이더넷 SGT 보호

- 네트워크 > 네트워크 프로파일 > 영역 보호 > 이더넷 SGT 보호

Cisco TrustSec 네트워크의 방화벽에 대해 제외할 레이어 2 SGT(보안 그룹 태그) 목록이 있는 영역 보호 프로파일을 생성합니다. 영역 보호 프로파일을 레이어 2, 가상 와이어 또는 탭 인터페이스에 적용합니다.

802.1Q(Ethertype 0x8909) 헤더가 있는 수신 패킷에 목록의 SGT와 일치하는 SGT가 있는 경우 방화벽은 패킷을 삭제합니다.

영역 보호 프로파일 설정	구성 위치	설명
레이어 2 SGT 제외 목록	네트워크 > 네트워크 프로파일 > 존 보호 > 이더넷 **SGT** 보호	SGT(보안 그룹 태그) 목록의 이름을 입력합니다.
꼬리표		SGT가 영역에 적용된 영역 보호 프로파일의 이 목록과 일치할 때 제외(삭제)하려는 패킷의 헤더에 레이어 2 SGT를 입력합니다(범위는 0~65,535).
활성화		이더넷 SGT 보호를 위해 이 제외 목록을 활성화(기본값)합니다. 제외 목록을 비활성화하려면 활성화 옵션을 선택 취소합니다.

L3 및 L4 헤더 검사

- 네트워크 > 네트워크 프로필 > 영역 보호 > L3 및 L4 헤더 검사

L3 및 L4 헤더 검사가 전역적으로 활성화되면 방화벽은 지원되는 프로토콜(IP/IPv6, ICMP/ICMPv6, TCP 및 UDP) 내에서 취약성을 탐지 및 방지하고 사용자 정의 사용자 지정 규칙과 일치하는 패킷을 기록 및/또는 차단할 수 있습니다. 또한, 헤더 검사 사용자 정의 규칙을 사용하여 각 보안 영역에 대해 네트워크 검사 활성화(네트워크 > 영역)를 해야 합니다.

기존 규칙을 추가, 삭제 및 복제할 수 있을 뿐만 아니라 영역 보호 프로필에서 평가한 대로 사용자 지정 규칙의 우선 순위 및 작동 상태를 정의할 수 있습니다.

영역 보호 프로필에서 L3 및 L4 헤더 검사를 구성한 후 수신 보안 영역에 프로필을 적용합니다.

*Palo Alto Networks*는 이 기능이 활성화될 때 동시에 작동할 수 있는 영역의 수가 제한되어 있으므로 맞춤형 규칙과 일치하는 패킷을 만나고 처리할 것으로 예상되는 보안 영역에서만 *L3* 및 *L4* 헤더 검사를 구성하고 활성화할 것을 권장합니다.

영역 보호 프로필 설정 - **L3** 및 **L4** 헤더 검사	구성 위치	설명
구성 탭		
일반		

영역 보호 프로필 설정 - **L3** 및 **L4** 헤더 검사	구성 위치	설명
규칙	네트워크 > 네트워크 프로파일 > 존 보호 > **L3** 및 **L4** 헤더 검사	사용자 지정 규칙을 식별할 이름을 입력합니다(최대 31자).
위협 ID		사용자 지정 규칙 구성의 위협 ID 번호를 지정합니다(취약성 서명 범위는 41000~45000 및 6800001~6900000).
코멘트		사용자 지정 규칙을 설명하는 설명(선택 사항)을 입력합니다.
패킷 캡처		사용자 지정 규칙과 일치하는 취약점이 탐지되면 패킷 캡처를 활성화합니다. 드롭다운에서 단일 패킷 또는 확장된 캡처를 선택하거나 방화벽이 패킷 캡처를 기록하지 않도록 하려면 비활성화를 선택합니다. 또한 패킷이 삭제된 경우 **icmp**에 도달할 수 없는 패킷을 전송하여 세션이 허용되지 않음을 클라이언트에 알릴 수 있습니다.
면제 IP		사용자 지정 규칙을 적용하지 않으려는 IP 주소를 입력합니다.
속성		
로그 심각도	네트워크 > 네트워크 프로파일 > 존 보호 > **L3** 및 **L4** 헤더 검사	방화벽이 사용자 지정 규칙과 일치하는 취약점을 탐지할 때 기록되는 로그 심각도 수준을 지정합니다.
로그 인터벌		일치하는 이벤트의 최대 로그 빈도(초)를 지정합니다.
동작		헤더에서 사용자 지정 규칙과 일치하는 취약성이 탐지될 때 취할 정책 조치를 지정합니다. 옵션에는 다음이 포함됩니다. • 허용 • 경고 • drop • reset-client • reset-server • reset-both
참조		
CVE	네트워크 > 네트워크 프로파일 >	위협과 관련된 공개적으로 알려진 보안 취약성 식별자입니다. CVE(Common Vulnerabilities and Exposures) 식별자는

영역 보호 프로필 설정 - **L3** 및 **L4** 헤더 검사	구성 위치	설명
	존 보호 > **L3** 및 **L4** 헤더 검사	공급업체별 ID가 일반적으로 여러 취약점을 포함하므로 고유한 취약점에 대한 정보를 찾는 데 가장 유용한 식별자입니다.
버그트랙		취약점과 관련된 bugtraq 식별자(CVE와 유사)입니다. 추가 배경 및 분석 세부 정보에 대한 외부 참조로 사용할 수 있습니다.
공급자		취약점에 대한 공급자별 식별자입니다.
참조		추가 분석 또는 배경 정보에 대한 링크입니다.
서명 탭		
코멘트	네트워크 > 네트워크 프로파일 > 존 보호 > **L3** 및 **L4** 헤더 검사	사용자 지정 규칙 서명 세부 정보를 설명하는 선택적 설명을 입력합니다.
OR 조건		사용자 지정 서명의 **OR** 조건값을 지정합니다.
AND 조건		다음을 구성하여 맞춤 서명에 대한 **AND** 조건을 추가합니다. • **AND** 조건 - 사용자 지정 서명의 AND 조건 값을 지정합니다. • 연산자 - 사용자 정의 서명이 헤더 콘텐츠와 일치하기 위해 참이어야 하는 조건 유형을 정의합니다. 보다 큼, 보다 작음, 같음, 범위 또는 이벤트 연산자 중에서 선택합니다. • 컨텍스트 - 사용 가능한 컨텍스트 옵션에서 선택합니다. 선택에 따라 조건을 활성화하기 위해 지정해야 하는 컨텍스트 및/또는 연산자와 관련된 다른 필드가 있을 수 있습니다. 추가 조건은 ***OR*** 조건 아래에 두 번째 레벨 항목으로 추가됩니다.

네트워크 > 네트워크 프로파일 > QoS

QoS 프로파일을 추가하여 최대 8개의 서비스 클래스에 대한 대역폭 제한 및 우선 순위를 정의합니다. 개별 클래스와 집합 클래스에 대해 보장된 최대 대역폭 제한을 모두 설정할 수 있습니다. 우선 순위는 경합이 있는 경우 트래픽을 처리하는 방법을 결정합니다.

방화벽이 QoS를 제공하도록 완전히 활성화하려면 다음도 수행하십시오.

- QoS 처리를 받을 트래픽을 정의합니다(QoS 정책을 추가하거나 수정하려면 정책 > QoS 선택).
- 인터페이스에서 QoS를 활성화합니다(네트워크 > QoS 선택).

전체 QoS 워크플로, 개념 및 사용 사례는 서비스 품질을 참조하십시오.

QoS 프로파일 설정	
프로파일 이름	프로파일을 식별할 수 있는 이름을 입력합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
최대 이그레스(Egress)	이 인터페이스를 통해 방화벽에서 나가는 트래픽의 최대 처리량(Mbps)을 입력합니다. 이 값은 기본적으로 0이며 방화벽 제한을 지정합니다(PAN-OS 7.1.16 이상 릴리스에서는 60,000Mbps, PAN-OS 7.1.15 및 이전 릴리스에서는 16,000Mbps). QoS 프로파일에 대한 최대 이그레스**(Egress)**은 QoS가 활성화된 물리적 인터페이스에 대한 최대 이그레스**(Egress)**보다 작거나 같아야 합니다. 네트워크 > QoS를 참조하십시오. 필수 필드는 아니지만 *QoS* 프로파일에 대해 항상 ***Egress Max***를 정의하는 것이 좋습니다.
이그레스(Egress) 보장	이 프로파일에 대해 보장되는 대역폭(Mbps)을 입력합니다. 이그레스(egress) 보장 대역폭이 초과되면 방화벽은 최적화된 방식으로 트래픽을 전달합니다. 이그레스 보장 및 최대 이그레스 값을 Mbps 또는 백분율로 구성할 수 있습니다. 이러한 값을 백분율로 구성할 때는 다음 사항을 고려해야 합니다. • 클래스당 이그레스 보장(%)은 이그레스 보장 값이 아닌 최대 이그레스 값을 사용하여 계산됩니다. • 프로필 이그레스 보장은 최대 이그레스를 곱한 클래스당 이그레스 보장(%)의 합계와 같습니다. 예: 최대 이그레스는 100Mbps로 구성되어 있습니다. 클래스 1에 대해 구성된 보장 비율은 30%, 클래스 2의 경우 20%, 클래스 3의 경우 5%, 클래스 4의 경우 1% 입니다. 이 구성의 총 비율은 56%로 보장됩니다. 이 경우 프로필 이그레스 보장은 56Mbps(최대 이그레스 56%)입니다. 즉, 클래스 1 이그레스 보장은 30Mbps, 클래스 2 이그레스 보장은 20Mbps 등입니다.
클래스	개별 QoS 클래스를 처리하는 방법을 추가하고 지정합니다. 구성할 클래스를 하나 이상 선택 가능:

QoS 프로파일 설정	

	• 클래스 - 클래스를 구성하지 않은 경우에도 QoS 정책에 클래스를 포함할 수 있습니다. 이 경우 트래픽에는 전체 QoS 제한이 적용됩니다. QoS 정책과 일치하지 않는 트래픽은 클래스 4에 할당됩니다.
	• 우선 순위 - 클래스에 할당할 우선 순위를 클릭하고 선택:
	  • 실시간
	  • 높음
	  • 중간
	  • 낮음
	경합이 발생하면 더 낮은 우선 순위가 할당된 트래픽이 삭제됩니다. 실시간 우선 순위는 자체 별도의 대기열을 사용합니다.
	• 최대 송신 - 이 클래스의 최대 처리량(Mbps)을 클릭하고 입력합니다. 이 값은 기본적으로 0이며 방화벽 제한을 지정합니다(PAN-OS 7.1.16 이상 릴리스에서는 60,000Mbps, PAN-OS 7.1.15 및 이전 릴리스에서는 16,000Mbps). QoS 클래스에 대한 최대 이그레스**(Egress)**는 QoS 프로파일에 대한 최대 이그레스**(Egress)** 보다 작거나 같아야 합니다.
	그러나 필수 필드가 아니므로 항상 *QoS* 프로파일에 대해 최대 이그레스***(Egress)*** 값을 정의하는 것이 좋습니다.
	• 이그레스**(Egress)** 보장 - 이 클래스에 대해 보장된 대역폭(Mbps)을 클릭하고 입력합니다. 클래스에 할당된 보장된 대역폭은 해당 클래스에 대해 예약되지 않습니다. 사용되지 않는 대역폭은 모든 트래픽에서 계속 사용할 수 있습니다. 그러나 트래픽 클래스에 대해 송신 보장 대역폭을 초과하면 방화벽은 최적화된 해당 트래픽을 전달합니다.

네트워크 > 네트워크 프로파일 > LLDP 프로파일

LLDP(Link Layer Discovery Protocol) 프로파일은 방화벽의 LLDP 모드를 구성하고, syslog 및 SNMP 알림을 활성화하고, LLDP 피어로 전송하려는 선택적 TLV(Type-Length-Values)를 구성하는 방법입니다. LLDP 프로파일을 구성한 후 프로파일을 하나 이상의 인터페이스에 할당합니다.

LLDP를 구성하고 모니터링하는 방법을 포함하여 LLDP에 대해 자세히 알아보세요.

LLDP 프로파일 설정	설명
이름	LLDP 프로파일의 이름을 지정합니다.
모드	LLDP가 작동할 모드(전송-수신, 전송 전용 또는 수신 전용)를 선택합니다.

LLDP 프로파일 설정	설명
SNMP 시스템 로그 알림	전역 알림 인터벌에서 발생하는 SNMP 트랩 및 syslog 알림을 활성화합니다. 활성화된 경우 방화벽은 디바이스 > 로그 설정 > 시스템 > **SNMP** 트랩 프로파일 및 **Syslog** 프로파일에 구성된 대로 SNMP 트랩과 syslog 이벤트를 모두 보냅니다.
포트 설명	방화벽의 ifAlias 개체가 포트 설명 TLV로 전송되도록 합니다.
시스템 이름	방화벽의 sysName 개체가 시스템 이름 TLV로 전송되도록 합니다.
시스템 설명	방화벽의 sysDescr 개체가 시스템 설명 TLV로 전송되도록 합니다.
시스템 기능	시스템 기능 TLV에서 다음 매핑을 통해 인터페이스의 배포 모드(L3, L2 또는 가상 와이어)를 보낼 수 있습니다. • L3인 경우 방화벽은 라우터(비트 6) 기능과 기타 비트(비트 1)를 알립니다. • L2인 경우 방화벽은 MAC 브리지(비트 3) 기능과 기타 비트(비트 1)를 알립니다. • 가상 와이어인 경우 방화벽은 리피터(비트 2) 기능과 기타 비트(비트 1)를 알립니다. SNMP MIB는 인터페이스에 구성된 기능을 단일 항목으로 결합합니다.
관리 주소	관리 주소 TLV에서 보낼 관리 주소를 활성화합니다. 지정된 순서대로 전송되는 관리 주소를 최대 4개까지 입력할 수 있습니다. 순서를 변경하려면 위로 이동 또는 아래로 이동을 클릭합니다.
이름	관리 주소의 이름을 지정합니다.
상호 작용	IP 주소가 관리 주소가 될 인터페이스를 선택하십시오. 없음을 선택하면 IPv4 또는 IPv6 선택 항목 옆에 있는 필드에 IP 주소를 입력할 수 있습니다.
IP 선택	**IPv4** 또는 **IPv6**을 선택한 다음 인접한 필드에 관리 주소로 전송할 IP 주소를 선택하거나 입력합니다. 관리 주소 TLV가 활성화된 경우 하나 이상의 관리 주소가 필요합니다. 관리 IP 주소가 구성되지 않은 경우 시스템은 전송 인터페이스의 MAC 주소를 전송된 관리 주소로 사용합니다.

네트워크 > 네트워크 프로파일 > BFD 프로파일

BFD(양방향 포워딩 감지)는 링크 장애를 매우 빠르게 감지하여 다른 경로로의 페일오버를 가속화합니다.

무엇을 찾고 계신가요?	참조:
BFD란 무엇입니까?	BFD 개요
BFD 프로파일을 만드는 데 사용할 수 있는 필드는 무엇입니까?	BFD 프로파일의 빌딩 블록
가상 라우터에 대한 BFD 상태를 봅니다.	BFD 요약 및 세부 정보 보기
더 찾고 계십니까?	BFD에 대해 자세히 알아보고 구성하십시오. BFD 구성 정적 경로 BGP OSPF OSPFv3 RIP

BFD 개요

BFD는 인터페이스, 데이터 링크 또는 실제 포워딩 엔진과 같은 두 포워딩 엔진 간의 양방향 경로 장애를 인식하는 프로토콜입니다. PAN-OS 구현에서 포워딩 엔진 중 하나는 방화벽의 인터페이스이고 다른 하나는 인접한 구성된 BFD 피어입니다. 두 엔진 간의 BFD 실패 감지는 매우 빠르며 링크 모니터링 또는 헬로 패킷 또는 하트비트와 같은 빈번한 동적 라우팅 상태 확인으로 달성할 수 있는 것보다 더 빠른 페일오버를 제공합니다.

BFD는 실패를 감지한 후 라우팅 프로토콜에 피어에 대한 대체 경로로 전환하도록 알립니다. BFD가 고정 경로로 구성된 경우 방화벽은 영향을 받는 경로를 RIB 및 FIB 테이블에서 제거합니다.

BFD는 물리적 이더넷, AE, VLAN, 터널(Site-to-Site VPN 및 LSVPN) 및 Layer 3 인터페이스의 하위 인터페이스와 같은 인터페이스 유형에서 지원됩니다. 각 고정 경로 또는 동적 라우팅 프로토콜에 대해 BFD를 활성화 또는 비활성화하고 기본 BFD 프로파일을 선택하거나 BFD 프로파일을 구성할 수 있습니다.

BFD 프로파일의 빌딩 블록

- 네트워크 > 네트워크 프로파일 > BFD 프로파일

기본 BFD 프로파일 또는 생성한 BFD 프로파일을 적용하여 정적 경로 또는 동적 라우팅 프로토콜에 대해 BFD를 활성화할 수 있습니다. 기본 프로파일은 기본 BFD 설정을 사용하며 변경할 수 없습니다. 새 BFD 프로파일을 추가하고 다음 정보를 지정할 수 있습니다.

BFD 프로파일 설정	설명
이름	BFD 프로파일의 이름(최대 31자). 이름은 대소문자를 구분하며 방화벽에서 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
방법	BFD가 작동하는 모드: • 활성 - BFD가 제어 패킷 전송을 시작합니다(기본값). BFD 피어 중 적어도 하나는 활성 상태여야 합니다. 둘 다 활성화될 수 있습니다. • 수동 - BFD는 피어가 제어 패킷을 보낼 때까지 기다렸다가 필요에 따라 응답합니다.
원하는 최소 전송 인터벌(ms)	BFD 프로토콜이 BFD 제어 패킷을 보내는 최소 인터벌(밀리초)입니다. PA-7000 시리즈, PA-5450, PA-5430, PA-5420, PA-5410 및 PA-3400 시리즈의 최소값은 50입니다. PA-3200 시리즈의 최소값은 100입니다. PA-400의 최소값은 150입니다. VM 시리즈의 최소값은 200입니다(최대값은 10,000, 기본값은 1000). 동일한 인터페이스에서 서로 다른 *BFD* 프로파일을 사용하는 여러 프로토콜이 있는 경우 동일한 ***Desired Minimum Tx Interval***로 *BFD* 프로파일을 구성합니다.
필요한 최소 수신 인터벌(ms)	BFD가 BFD 제어 패킷을 수신할 수 있는 최소 인터벌(밀리초)입니다. PA-7000 시리즈, PA-5450, PA-5430, PA-5420, PA-5410 및 PA-3400 시리즈의 최소값은 50입니다. PA-3200 시리즈의 최소값은 100입니다. PA-400의 최소값은 150입니다. VM 시리즈의 최소값은 200입니다(최대값은 10,000, 기본값은 1000).
감지 시간 멀티플라이어	로컬 시스템은 원격 시스템에서 수신한 감지 시간 승수에 원격 시스템의 합의된 전송 인터벌을 곱한 값으로 감지 시간을 계산합니다(**Required Minimum Rx Interval**과 마지막으로 수신한 **Desired Minimum Tx Interval** 중 큰 값). BFD가 탐지 시간이 만료되기 전에 피어로부터 BFD 제어 패킷을 수신하지 않으면 실패가 발생한 것입니다(범위는 2~50, 기본값은 3).
유지 시간(ms)	방화벽이 BFD 제어 패킷을 전송하기 전에 링크가 발생한 후 지연(밀리초)입니다. **Hold Time**은 BFD Active 모드에만 적용됩니다. 방화벽이 **Hold Time** 동안 BFD 제어 패킷을 수신하면 이를 무시합니다(범위는 0-120000, 기본값은 0). 기본 설정 0은 전송 보류 시간이 사용되지 않음을 의미합니다. 방화벽은 링크가 설정된 직후 BFD 제어 패킷을 보내고 받습니다.
멀티홉 활성화	여러 홉에서 BFD를 활성화합니다. BGP 구현에만 적용됩니다.
최소 수신 TTL	최소 Time-to-Live 값(홉 수) BFD는 멀티홉 BFD를 지원할 때 수락(수신)합니다. BGP 구현에만 적용됩니다(범위는 1-254, 기본값 없음).

BFD 요약 및 세부 정보 보기

- 네트워크 > 가상 라우터

다음 표에서는 BFD 요약 정보를 설명합니다.

BFD 정보 보기	
BFD 요약을 봅니다.	네트워크 > 가상 라우터를 선택한 다음 관심 있는 가상 라우터 행에서 추가 런타임 통계를 클릭합니다. **BFD** 요약 정보 탭을 선택합니다.
BFD 세부 정보를 봅니다.	BFD 세부 정보를 보려면 관심 있는 인터페이스 행에서 세부 정보를 선택합니다.

네트워크 > 네트워크 프로파일 > SD-WAN 인터페이스 프로파일

링크 태그별로 물리적 링크를 그룹화하고 링크 속도와 방화벽이 링크를 모니터링하는 빈도를 제어하려면 SD-WAN 인터페이스 프로파일을 만듭니다.

	SD-WAN 인터페이스 프로파일
이름	최대 31자의 영숫자를 사용하여 SD-WAN 인터페이스 프로파일의 이름을 입력합니다. 이름은 영숫자로 시작해야 하며 문자, 숫자, 밑줄(_), 하이픈(-), 마침표(.) 및 공백을 포함할 수 있습니다.
위치	Multi-VSYS 디바이스에 대한 가상 시스템을 선택하십시오.
링크 태그	이 프로파일이 인터페이스에 할당할 링크 태그를 선택하거나 새 태그를 추가합니다. 링크 태그는 경로 선택 및 페일오버 중에 방화벽이 선택할 물리적 링크(다른 ISP)를 묶습니다.
설명	프로파일에 대한 사용자 친화적인 설명을 입력하는 것이 가장 좋습니다.
링크 유형	사전 정의된 목록(**ADSL/DSL**, 케이블 모뎀, 이더넷, 광섬유, **LTE/3G/4G/5G**, **MPLS**, 마이크로웨이브/라디오, 새틀라이트, **WiFi** 또는 기타)에서 물리적 링크 유형을 선택합니다. 방화벽은 종료되고 방화벽에 대한 이더넷 연결로 전달되는 모든 CPE 디바이스를 지원할 수 있습니다. 예를 들어 WiFi 액세스 포인트, LTE 모뎀, 레이저 마이크로파 CPE는 모두 이더넷 핸드오프로 종료될 수 있습니다.

	SD-WAN 인터페이스 프로파일
	*PAN-OS SD-WAN*을 지원하는 데 사용될 인터페이스에 영역이 정의된 기존 *PAN-OS* 배포의 경우, *Panorama*는 다음 조건에서 인터페이스의 영역 이름을 사전 정의된 *SD-WAN* 영역 중 하나로 자동 구성할 수 있습니다. *1. SD-WAN* 인터페이스는 해당 인터페이스 프로필에서 지점 간 프라이빗 링크 유형*(**MPLS**, **Satellite** 또는 **Microwave**)*으로 구성됩니다. *2. SD-WAN* 인터페이스 프로필에서 ***VPN*** 데이터 터널 지원 확인란이 비활성화*(*선택 해제*)*되어 있습니다. 이는 *PAN-OS*가 *SD-WAN VPN* 터널 외부에서 일반 텍스트로 트래픽을 전달하도록 지시합니다. 허브 방화벽에서 영역 이름은 조건 *#1*이 충족되면 *"zone-to-branch"*로 구성됩니다. 지점 방화벽에서 조건 *#1* 및 조건 *#2*가 모두 충족되면 영역 이름이 *"zone-to-hub"*로 구성됩니다. *Panorama*는 이 단계를 자동화하여 구성을 단순화하여 허브와 분기 방화벽 간의 적절한 통신을 보장합니다. 이전 영역 이름을 참조하는 기존 방화벽 정책이 있는 경우 미리 정의된 새 *SD-WAN* 영역 이름을 반영하도록 정책을 업데이트해야 합니다.
최대 다운로드(Mbps)	ISP의 최대 다운로드 속도를 초당 메가비트로 입력합니다. 범위는 1~100,000이며 기본값은 없습니다. ISP에 링크 속도에 대해 문의하거나 speedtest.net과 같은 도구를 사용하여 링크의 최대 속도를 샘플링하고 적절한 시간 동안 최대값의 평균을 구하십시오.
최대 업로드(Mbps)	ISP의 최대 업로드 속도를 초당 메가비트로 입력합니다. 범위는 1~100,000이며 기본값은 없습니다. ISP에 링크 속도에 대해 문의하거나 speedtest.net과 같은 도구를 사용하여 링크의 최대 속도를 샘플링하고 적절한 시간 동안 최대값의 평균을 구하십시오.
오류 수정 프로파일 인터페이스 선택 가능	이 설정을 선택하면 인터페이스(이 프로파일을 적용하는 곳)가 인코딩 방화벽에 적합하여 FEC(Forward Error Correction) 또는 패킷 복사를 위해 선택할 수 있습니다. 프로파일을 적용하는 고가의 링크(인터페이스)에서 고가의 FEC 또는 패킷 복사가 사용되지 않도록 이 설정을 선택 취소할 수 있습니다. 프로파일에 대해 지

	SD-WAN 인터페이스 프로파일
	정된 링크 유형은 기본 설정인 오류 수정 프로파일 인터페이스 선택 가능이 선택되었는지의 여부를 결정합니다. FEC 또는 패킷 복사를 구성하려면 SD-WAN 오류 수정 프로파일을 만듭니다.
VPN 데이터 터널 지원	분기-허브 트래픽 및 반환 트래픽이 추가 보안을 위해 VPN 터널을 통과할지(기본적으로 활성화됨) 또는 암호화 오버헤드를 피하기 위해 VPN 터널 외부로 플로우될지를 결정합니다. • 케이블 모뎀, ADSL 및 기타 인터넷 연결과 같이 직접 인터넷 연결 또는 인터넷 브레이크아웃 기능이 있는 공개 링크 유형에 대해 **VPN** 데이터 터널 지원을 활성화된 상태로 둡니다. • 인터넷 브레이크아웃 기능이 없는 MPLS, 새틀라이트 또는 마이크로웨이브와 같은 개인 링크 유형에 대해 **VPN** 데이터 터널 지원을 비활성화할 수 있습니다. 그러나 먼저 트래픽이 VPN 터널 외부로 전송되기 때문에 가로채지 못하도록 해야 합니다. • 다수의 브랜치(branch)는 허브에 연결하는 개인 MPLS 링크로 페일오버하고 허브에서 인터넷에 도달해야 하는 DIA 트래픽이 있습니다. **VPN** 데이터 터널 지원 설정은 개인 데이터가 VPN 터널을 통해 플로우될지 터널 외부로 플로우될지 결정하고 페일오버된 트래픽이 다른 연결(프라이빗 데이터 흐름이 사용하지 않음)을 사용합니다. 방화벽은 영역을 사용하여 사설 MPLS 트래픽에서 DIA 페일오버 트래픽을 분할합니다.
VPN 페일오버 메트릭	(PAN-OS 10.0.3 이상 릴리스) DIA AnyPath를 구성할 때 DIA가 페일오버되는 허브 가상 인터페이스 또는 분기 가상 인터페이스에 번들로 제공되는 개별 VPN 터널의 페일오버 순서를 지정하는 방법이 필요합니다. VPN 터널(링크)에 대한 VPN 페일오버 메트릭을 지정합니다. 범위는 1 ~ 65,535이고, 기본값은 10입니다. 메트릭 값이 낮을수록 페일오버 중에 선택되는 터널(이 프로파일을 적용하는 링크)의 우선 순위가 높아집니다. 예를 들어, 메트릭을 낮은 값으로 설정하고 프로파일을 광대역 인터페이스에 적용합니다. 그런 다음 광대역이 페일오버된 후에만 사용되도록 고가의 LTE 인터페이스에 적용할 높은 메트릭을 설정하는 다른 프로파일을 만듭니다.

	SD-WAN 인터페이스 프로파일
	허브에 링크가 하나만 있는 경우 해당 링크는 모든 가상 인터페이스와 *DIA* 트래픽을 지원합니다. 링크 유형을 특정 순서로 사용하려면 하향식 우선 순위를 지정하는 허브에 트래픽 분산 프로파일을 적용한 다음 기본 설정 순서를 지정하도록 링크 태그의 순서를 지정해야 합니다. *(*대신 사용 가능한 최적 경로를 지정하는 트래픽 분산 프로파일을 적용하면 방화벽은 비용에 관계없이 링크를 사용하여 분기에 대한 최상의 성능 경로를 선택합니다.*)* 요약하면 트래픽 분산 프로파일의 링크 태그, 허브 가상 인터페이스에 적용된 링크 태그 및 *VPN* 페일오버 메트릭은 트래픽 분산 프로파일이 하향식 우선 순위를 지정하는 경우에만 작동합니다.
경로 모니터링	이 SD-WAN 인터페이스 프로파일을 적용하는 인터페이스를 방화벽이 모니터링하는 경로 모니터링 모드를 선택합니다. • 적극적 - (LTE 및 새틀라이트을 제외한 모든 링크 유형에 대한 기본값) 방화벽은 일정한 빈도로 SD-WAN 링크의 반대쪽 끝으로 프로브 패킷을 보냅니다. 절전 및 정전 상태에 대한 빠른 감지 및 페일오버가 필요한 경우 적극적인 모드를 사용하십시오. • 완화 -(LTE 및 새틀라이트 링크 유형의 기본값) 방화벽은 프로브 패킷 세트를 보내는 사이에 몇 초(프로브 유휴 시간) 동안 대기하므로 경로 모니터링 빈도가 줄어듭니다. 프로브 유휴 시간이 만료되면 방화벽은 구성된 프로브 빈도에서 7초 동안 프로브를 보냅니다. 낮은 대역폭 링크가 있거나 사용량에 따라 요금이 청구되는 링크*(*예*: LTE)*가 있거나 빠른 감지가 비용과 대역폭을 유지하는 것만큼 중요하지 않은 경우 완화 모드를 사용합니다.
프로브 주파수(초당)	방화벽이 SD-WAN 링크의 반대쪽 끝으로 프로브 패킷을 보내는 초당 횟수인 프로브 빈도를 입력합니다(범위는 1~5, 기본값은 5).
프로브 유휴 시간(초)	완화된 경로 모니터링을 선택하면 방화벽이 프로브 패킷 세트 사이에서 대기하는 프로브 유휴 시간(초)을 설정할 수 있습니다(범위는 1~60, 기본값은 60).
장애 복구 보류 시간(초)	복구된 링크가 페일오버된 후 방화벽이 해당 링크를 기본 링크로 복원하기 전에 방화벽이 복구된 링크를 기다리는 시간(초)을 입력합니다(범위는 20~120, 기본값은 120). 장애 복구 보류 시간은 복구된 링크가 너무 빨리 기본 링크로 복원되어 즉시 다시 실패하는 것을 방지합니다.

디바이스

방화벽의 기본 시스템 구성 및 유지 관리 작업에 대한 필드 참조를 위해 다음 섹션을 사용하십시오.

- 디바이스 > 설정
- 디바이스 > 고가용성
- 디바이스 > 로그 포워딩 카드
- 디바이스 > 구성 감사
- 디바이스 > 암호 프로파일
- 디바이스 > 관리자
- 디바이스 > 관리자 역할
- 디바이스 > 액세스 도메인
- 디바이스 > 인증 프로파일
- 디바이스 > 인증 순서
- 디바이스 > 사용자 식별
- 디바이스 > IoT > DHCP 서버
- 디바이스 > 데이터 재배포
- 디바이스 > 디바이스 검역
- 디바이스 > VM 정보 소스
- 디바이스 > 문제 해결
- 디바이스 > 가상 시스템
- 디바이스 > 공유 게이트웨이
- 디바이스 > 인증서 관리
- 디바이스 > 응답 페이지
- 디바이스 > 로그 설정
- 디바이스 > 서버 프로파일
- 디바이스 > 로컬 사용자 데이터베이스 > 사용자
- 디바이스 > 로컬 사용자 데이터베이스 > 사용자 그룹
- 디바이스 > 예약된 로그 내보내기
- 디바이스 > 소프트웨어
- Device > GlobalProtect Client
- 디바이스 > 동적 업데이트

- 디바이스 > 라이선스
- 디바이스 > 지원
- 디바이스 > 마스터 키 및 진단
- 디바이스 > 정책 권장 사항

디바이스 > 설정

- 디바이스 > 설정 > 관리
- 디바이스 > 설정 > 작업
- 디바이스 > 설정 > HSM
- 디바이스 > 설정 > 서비스
- 디바이스 > 설정 > 인터페이스
- 디바이스 > 설정 > 원격 측정
- 디바이스 > 설정 > 콘텐츠 ID
- Device > Setup > WildFire
- 디바이스 > 설정 > 세션
- 디바이스 > 설정 > DLP

디바이스 > 설정 > 관리

- 디바이스 > 설정 > 관리
- **Panorama** > 설정 > 관리

방화벽에서 디바이스 > 설정 > 관리를 선택하여 관리 설정을 구성합니다.

Panorama™에서 **Device** > **Setup** > **Management**를 선택하여 Panorama 템플릿으로 관리하는 방화벽을 구성합니다. Panorama에 대한 관리 설정을 구성하려면 **Panorama** > **Setup** > **Management**를 선택합니다.

다음 관리 설정은 명시된 경우를 제외하고 방화벽과 Panorama 모두에 적용됩니다.

- 일반 설정
- 인증 설정
- 정책 규칙 베이스 설정
- Panorama 설정: 디바이스 > 설정 > 관리(방화벽에서 Panorama에 연결하도록 구성된 설정)
- Panorama 설정: Panorama > 설정 > 관리(방화벽 연결을 위해 Panorama에 구성된 설정)
- 로깅 및 보고 설정
- 로그 인터페이스(PA-5450 전용)
- 배너 및 메시지
- 최소 암호 복잡성
- AutoFocus™
- Cortex Data Lake
- SSH 관리 프로파일 설정
- PAN-OS 엣지 서비스 설정

항목	설명
일반 설정	
호스트네임	호스트 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 마침표, 하이픈 및 밑줄만 포함할 수 있습니다. 값을 입력하지 않으면 PAN-OS®는 방화벽 모델(예: PA-5220_2)을 기본값으로 사용합니다. 선택적으로 DHCP 서버가 제공하는 호스트 이름을 사용하도록 방화벽을 구성할 수 있습니다. DHCP 서버 제공 호스트 이름 수락(방화벽만 해당)을 참조하십시오.

항목	설명
	관리 중인 디바이스를 쉽게 식별할 수 있도록 고유한 호스트 이름을 구성하십시오.
도메인	방화벽의 네트워크 도메인 이름을 입력합니다(최대 31자). 선택적으로 DHCP 서버가 제공하는 도메인을 사용하도록 방화벽과 Panorama를 구성할 수 있습니다. DHCP 서버 제공 도메인 수락(방화벽만 해당)을 참조하십시오.
DHCP 서버 제공 호스트 이름 수락(방화벽만 해당)	(관리 인터페이스 IP 유형이 DHCP 클라이언트인 경우에만 적용됨) 관리 인터페이스가 DHCP 서버에서 수신하는 호스트 이름을 수락하도록 하려면 이 옵션을 선택합니다. 서버의 호스트 이름(유효한 경우)은 호스트 이름 필드에 지정된 값을 덮어씁니다.
DHCP 서버 제공 도메인 수락(방화벽만 해당)	(관리 인터페이스 IP 유형이 DHCP 클라이언트인 경우에만 적용됨) 관리 인터페이스가 DHCP 서버에서 수신하는 도메인(DNS 서픽스)을 수락하도록 하려면 이 옵션을 선택합니다. 서버의 도메인은 도메인 필드에 지정된 값을 덮어씁니다.
로그인 배너	웹 인터페이스 로그인 페이지의 이름 및 비밀번호 필드 아래에 표시할 텍스트(최대 3,200자)를 입력합니다.
관리자가 로그인 배너를 확인하도록 강제 설정	이 옵션을 선택하면 관리자가 로그인하기 전에 메시지 내용을 이해하고 수락했음을 확인하도록 강제하는 아래 설명(로그인 페이지의 로그인 배너 위)을 표시하고 관리자가 선택하도록 강제합니다.
관리 TLS 모드	다음 TLS 모드 중 하나를 선택하여 관리 인터페이스가 협상하는 프로토콜 버전 및 암호화 제품군을 지정합니다. • **tlsv1.3_only** - 관리 인터페이스 액세스를 TLSv1.3 및 관련 암호화 제품군으로 보호되는 연결로 제한합니다. 클라이언트가 TLSv1.3 암호를 협상할 수 없으면 연결이 실패합니다. • 혼합 모드 - 모든 TLS 버전(TLSv1.0-TLSv1.3) 및 관련 암호화 제품군으로 보호되는 연결에 대한 관리 인터페이스 액세스를 허용합니다. *TLSv1.1*은 *FIPS-CC* 모드의 방화벽이 지원하는 가장 초기의 *TLS* 버전입니다.

항목	설명
	• (기본값) **exclude_tlsv1.3** - 관리 인터페이스 액세스를 TLSv1.0, TLSv1.1 또는 TLSv1.2 및 관련 암호화 제품군으로 보호되는 연결로 제한합니다.
인증서	관리 인터페이스에 대한 관리 액세스를 보호하기 위해 관리 서버에서 사용하는 인증서를 선택합니다. 이 설정은 *TLSv1.3* 지원을 제공하는 모드(*tlsv1.3_only* 및 *## ##*)에서만 사용할 수 있습니다. *TLS* 프로토콜 버전, 암호화 제품군을 제한하고 ***exclude_tlsv1.3*** 모드에서 수동으로 인증서를 지정하려면 SSL/TLS 서비스 프로필을 구성합니다.
SSL/TLS 서비스 프로파일	기존 SSL/TLS 서비스 프로필을 할당하거나 새 프로필을 만들어 관리 인터페이스에서 허용되는 인증서 및 SSL/TLS 프로토콜 설정을 지정합니다(디바이스 > 인증서 관리 > SSL/TLS 서비스 프로필 참조). 방화벽 또는 Panorama는 이 인증서를 사용하여 관리(MGT) 인터페이스 또는 HTTP/HTTPS 관리 트래픽을 지원하는 기타 인터페이스를 통해 웹 인터페이스에 액세스하는 관리자를 인증합니다(네트워크 > 네트워크 프로필 > 인터페이스 관리 참조). 없음(기본값)을 선택하면 방화벽 또는 Panorama가 사전 정의된 인증서를 사용합니다. 편의를 위해 사전 정의된 인증서가 제공됩니다. 보안을 강화하려면 *SSL/TLS* 서비스 프로파일을 할당합니다. 신뢰를 보장하려면 클라이언트 시스템의 신뢰할 수 있는 루트 인증서 저장소에 있는 인증 기관*(CA)* 인증서를 통해 인증서에 서명해야 합니다.
시간대	방화벽의 시간대를 선택하십시오.
장소	드롭다운에서 PDF 보고서의 언어를 선택합니다. 모니터 > PDF 보고서 > PDF 요약 관리를 참조하십시오. 웹 인터페이스에 대해 특정 언어 기본 설정을 설정한 경우에도 PDF 보고서는 로케일에 대해 지정된 언어를 사용합니다.
날짜	방화벽에 날짜를 설정하십시오. 현재 날짜(YYYY/MM/DD 형식)를 입력하거나 드롭다운에서 날짜를 선택합니다.

항목	설명
	NTP 서버(***Device*** > ***Setup*** > ***Services***)를 정의할 수도 있습니다.
시간	방화벽에서 시간을 설정하십시오. 현재 시간)을 24시간 형식으로 입력) 또는 드롭다운에서 시간을 선택합니다. *NTP* 서버(***Device*** > ***Setup*** > ***Services***)를 정의할 수도 있습니다.
일련번호 (Panorama 가상 어플라이언스만 해당)	Panorama의 일련번호를 입력합니다. Palo Alto Networks®에서 받은 주문 이행 이메일에서 일련번호를 찾을 수 있습니다.
위도	방화벽의 위도(-90.0 ~ 90.0)를 입력합니다.
경도	방화벽의 경도(-180.0 ~ 180.0)를 입력합니다.
커밋 잠금 자동 획득	후보 구성을 변경할 때 커밋 잠금을 자동으로 적용하려면 이 옵션을 선택합니다. 자세한 내용은 잠금 구성을 참조하십시오. 첫 번째 관리자가 변경 사항을 커밋할 때까지 다른 관리자가 구성을 변경할 수 없도록 자동으로 커밋 잠금 획득을 활성화합니다.
인증서 만료 확인	온박스 인증서가 만료 날짜에 가까워지면 방화벽이 경고 메시지를 생성하도록 지시합니다. 인증서 만료 활성화 온박스 인증서가 만료 날짜에 가까워지면 경고 메시지를 생성하려면 선택합니다.
다중 가상 시스템 기능	이 기능을 지원하는 방화벽에서 여러 가상 시스템을 사용할 수 있습니다(디바이스 > 가상 시스템 참조).

항목	설명
	방화벽에서 여러 가상 시스템을 활성화하려면 방화벽 정책이 *640*개 이하의 개별 사용자 그룹을 참조해야 합니다. 필요한 경우 참조되는 사용자 그룹의 수를 줄이십시오. 그런 다음 여러 가상 시스템을 활성화하고 추가한 후 정책은 각 추가 가상 시스템에 대해 다른 *640*개의 사용자 그룹을 참조할 수 있습니다.
URL 필터링 데이터베이스 (Panorama만 해당)	Panorama와 함께 사용할 URL 필터링 공급자를 하나 선택하세요: **brightcloud** 또는 **paloaltonetworks**(PAN-DB).
하이퍼바이저 할당 MAC 주소 사용 (VM 시리즈 방화벽만 해당)	VM 시리즈 방화벽이 PAN-OS 사용자 지정 스키마를 사용하여 MAC 주소를 생성하는 대신 하이퍼바이저가 할당한 MAC 주소를 사용하도록 하려면 이 옵션을 선택합니다. 이 옵션을 활성화하고 인터페이스에 IPv6 주소를 사용하는 경우 인터페이스 ID는 인터페이스 MAC 주소에서 IPv6 주소를 파생하는 EUI-64 형식을 사용할 수 없습니다. 고가용성(HA) 능동형/수동형 구성에서 EUI-64 형식을 사용하면 커밋 오류가 발생합니다.
GTP 보안	GPRS 터널링 프로토콜(GTP) 트래픽에서 컨트롤 플레인 및 사용자 데이터 플레인 메시지를 검사하는 기능을 활성화하려면 이 옵션을 선택합니다. GTP 트래픽에 대한 정책을 시행할 수 있도록 모바일 네트워크 보호 프로파일을 구성하려면 개체 > 보안 프로파일 > 모바일 네트워크 보호를 참조하십시오.
SCTP 보안	SCTP(Stream Control Transmission Protocol) 패킷 및 청크를 검사 및 필터링하고 SCTP 시작(INIT) 플러드 보호를 적용하려면 이 옵션을 선택합니다. 개체 > 보안 프로파일 > SCTP 보호를 참조하십시오. SCTP INIT 플러드 보호의 경우 SCTP INIT 플러드 보호 구성을 참조하십시오.
Advanced 라우팅	논리 라우터에서 정적 경로, BGP, OSPFv2, OSPFv3, IPv4 멀티캐스트 및 RIPv2를 지원하는 고급 라우팅 엔진을 활성화하려면 이 옵션을 선택합니다. 새 라우팅 엔진에 대한 변경 사항을 적용하려면(또는 레거시 경로 엔진으로 다시 변경하려면) 방화벽을 커밋하고 재부팅해야 합니다.
터널 가속	GRE 터널, VXLAN 터널 및 GTP-U 터널을 통과하는 트래픽의 성능과 처리량을 향상시키려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

항목	설명
	• **GRE** 및 **VXLAN** 터널 가속 - PA-7000-NPC 및 SMC-B가 있는 PA-3200 시리즈 방화벽 및 PA-7000 시리즈 방화벽에서 지원됩니다. • **GTP-U** 터널 가속 - PA-7000-NPC 및 SMC-B가 있는 PA-7000 시리즈 방화벽에서 지원됩니다. GTP-U 터널 트래픽이 터널 가속을 사용하려면 터널 가속을 활성화해야 하고, GTP를 활성화해야 하며, GTP-U 프로토콜에 대한 터널 콘텐츠 검사(TCI) 정책 규칙을 구성할 수 없으며, 모바일 네트워크 보호가 포함된 보안 정책 규칙을 구성해야 합니다. 연결된 프로파일은 GTP 트래픽을 허용해야 합니다. *Tunnel Acceleration* 및 커밋을 비활성화하거나 다시 활성화하는 경우 방화벽을 재부팅해야 합니다.
디바이스 인증서	
인증서 받기	Palo Alto Networks 고객 지원 포털에서 생성된 OTP(일회용 비밀번호)를 클릭하여 입력합니다. CSP로 Panorama를 성공적으로 인증하고 ZTP(제로 터치 프로비저닝), IoT, 디바이스 원격 측정 및 엔터프라이즈 DLP(데이터 손실 방지)와 같은 클라우드 서비스를 활용하려면 디바이스 인증서가 필요합니다. 디바이스 인증서를 성공적으로 설치하면 다음이 표시됩니다. • 현재 디바이스 인증서 상태 - 디바이스 인증서의 현재 상태(##, ## 또는 ###) • 과거에 유효하지 않음 - 디바이스 인증서 유효성이 시작되는 시점을 나타내는 타임스탬프입니다. • 다음 이후 유효하지 않음 - 디바이스 인증서 유효 기간이 만료되고 디바이스 인증서가 #### ### ###을 나타내는 타임스탬프입니다. • 마지막으로 불러온 메시지 - 디바이스 인증서가 성공적으로 설치되었는지 또는 디바이스 인증서 설치가 실패했는지를 표시하는 메시지입니다. • 마지막으로 불러온 상태 - 디바이스 인증서를 가져오는 상태(## 또는 ##)입니다. • 마지막으로 불러온 타임스탬프 - 마지막 디바이스 인증서 설치 시도의 타임스탬프입니다.
인증 설정	

항목	설명
인증 프로파일	방화벽에서 로컬로가 아닌 외부 서버에서 정의하는 관리 계정을 인증하기 위해 방화벽에서 사용하는 인증 프로파일(또는 시퀀스)을 선택합니다(디바이스 > 인증 프로파일 참조). 외부 관리자가 로그인하면 방화벽은 외부 서버에 인증 및 권한 부여 정보(예: 관리 역할)를 요청합니다. 외부 관리자에 대한 인증을 활성화하려면 인증 프로파일이 지정하는 서버 유형에 따라 다음 중 하나여야 하는 추가 단계가 필요합니다. • 반지 름 • TACACS+ • SAML 관리자는 *SAML*을 사용하여 웹 인터페이스에 인증할 수 있지만 *CLI*에는 인증할 수 없습니다. 외부 관리자에 대한 인증을 비활성화하려면 없음을 선택합니다. 로컬로(방화벽에서) 정의하는 관리 계정의 경우 방화벽은 해당 계정에 할당된 인증 프로파일을 사용하여 인증합니다(디바이스 > 관리자 참조).
인증서 프로파일	방화벽 웹 인터페이스에 대한 인증서 기반 액세스를 위해 구성된 관리자의 클라이언트 인증서를 확인하려면 인증서 프로파일을 선택하십시오. 인증서 프로파일 구성에 대한 지침은 디바이스 > 인증서 관리 > 인증서 프로파일을 참조하십시오. 관리자의 호스트 시스템에 인증서 프로파일에 정의된 루트 *CA* 인증서로 인증할 수 있는 올바른 인증서가 있는지 확인하도록 인증서 프로파일을 구성합니다.
유휴 타임아웃	관리자가 자동으로 로그아웃되기 전에 웹 인터페이스 또는 CLI에서 활동이 없는 최대 시간(분)을 입력합니다(범위는 0~1,440, 기본값은 60). 값이 0이면 비활성 상태가 자동 로그아웃을 트리거하지 않음을 의미합니다.

항목	설명
	웹 인터페이스 페이지(예: 대시보드 및 시스템 알람 대화 상자)의 수동 및 자동 새로 고침은 모두 유휴 타임아웃 카운터를 재설정합니다. 자동 새로 고침을 지원하는 페이지에 있을 때 방화벽이 타임아웃을 적용하도록 하려면 새로 고침 인터벌을 수동으로 설정하거나 유휴 타임아웃보다 높은 값으로 설정합니다. ***ACC*** 탭에서 자동 새로 고침을 비활성화할 수도 있습니다. 관리자가 방화벽 세션을 열어 둔 경우 권한이 없는 사용자가 방화벽에 액세스하지 못하도록 하려면 유휴 시간 제한을 *10*분으로 설정합니다.
API 키 수명	API 키가 유효한 시간(분)을 입력합니다(범위는 0~525,600, 기본값은 0). 0 값은 API 키가 만료되지 않음을 의미합니다. 모든 **API** 키를 만료하여 이전에 생성된 모든 API 키를 무효화합니다. 모든 기존 키가 쓸모없게 렌더링되고 현재 해당 API 키를 사용하는 모든 작업이 작동을 중지하므로 이 옵션을 주의해서 사용하십시오. *API* 키를 참조한 현재 구현을 중단하지 않고 키를 교체할 수 있도록 유지 관리 기간 동안 이 작업을 수행합니다.
마지막으로 만료된 API 키	API 키가 마지막으로 만료된 시간의 타임스탬프를 표시합니다. 키를 재설정한 적이 없는 경우 이 필드에는 값이 없습니다.
실패한 시도	관리자 계정을 잠그기 전에 방화벽이 웹 인터페이스 및 CLI에 대해 허용하는 실패한 로그인 시도 횟수(0~10)를 입력합니다. 0 값은 무제한 로그인 시도를 지정합니다. 기본값은 일반 작동 모드의 방화벽의 경우 0이고 FIPS-CC 모드의 방화벽의 경우 10입니다. 로그인 시도를 제한하면 무차별 대입 공격으로부터 방화벽을 보호할 수 있습니다. (Panorama 관리형 방화벽만 해당) Panorama의 템플릿 또는 템플릿 스택 구성에서 실패한 시도 설정을 관리할 때 지원되는 최소값은 1입니다. 실패한 시도 횟수를 *0* 이외의 값으로 설정했지만 잠금 시간을 *0*으로 두면 실패한 시도 횟수가 무시되고 사용자가 잠기지 않습니다.

항목	설명
	악의적인 시스템이 방화벽에 로그인하기 위해 무차별 대입 방법을 시도하는 것을 방지하면서 입력 오류가 발생한 경우 적절한 재시도 횟수를 수용하려면 실패한 시도 횟수를 *5* 이하로 설정하십시오.
잠금 시간	실패한 시도 횟수 제한에 도달한 후 방화벽이 관리자가 웹 인터페이스 및 CLI에 액세스하지 못하도록 잠그는 시간(분)을 입력합니다(범위: 0~60). 값이 0(기본값)이면 다른 관리자가 계정을 수동으로 잠금 해제할 때까지 잠금이 적용됩니다. 실패한 시도 횟수를 *0* 이외의 값으로 설정하고 잠금 시간을 *0*으로 두면 설정된 로그인 시도 실패 횟수 후에 다른 관리자가 수동으로 계정 잠금을 해제할 때까지 사용자가 잠깁니다. 악의적인 행위자의 지속적인 로그인 시도를 방지하려면 잠금 시간을 최소 *30*분으로 설정하십시오.
최대 세션 수	모든 관리자 및 사용자 계정에 허용되는 동시 세션 수를 입력합니다(범위는 0~4). 값 0(기본값)은 무제한의 동시 세션이 허용됨을 의미합니다. *FIPS-CC* 모드에서 범위는 *0*에서 *4*이며 기본값은 *4*입니다. 무제한 동시 세션을 허용하려면 ***0*** 값을 입력하십시오.
최대 세션 시간	유휴 상태가 아닌 활성 관리자가 로그인 상태를 유지할 수 있는 시간(분 범위: 60~1,499)을 입력합니다. 이 최대 세션 시간에 도달하면 세션이 종료되고 다른 세션을 시작하려면 재인증이 필요합니다. 기본값은 0(30일)으로 설정되어 있으며 수동으로 입력할 수 없습니다. 값을 입력하지 않으면 최대 세션 시간의 기본값은 0입니다. *FIPS-CC* 모드에서 범위는 *60~1,499*이고 기본값은 *720*입니다. 값을 입력하지 않으면 최대 세션 시간은 기본적으로 *720*으로 설정됩니다.
정책 규칙 베이스 설정	

항목	설명
정책에 태그 필요	새 정책 규칙을 생성할 때 하나 이상의 태그가 필요합니다. 이 옵션을 활성화할 때 정책 규칙이 이미 있는 경우 다음에 규칙을 편집할 때 하나 이상의 태그를 추가해야 합니다.
정책에 대한 설명 필요	새 정책 규칙을 생성할 때 설명을 추가해야 합니다. 이 옵션을 활성화할 때 정책 규칙이 이미 있는 경우 다음에 규칙을 편집할 때 설명을 추가해야 합니다.
정책에 태그나 설명이 없는 경우 커밋 실패	정책 규칙에 태그나 설명을 추가하지 않으면 커밋이 강제로 실패합니다. 이 옵션을 활성화할 때 정책 규칙이 이미 존재하는 경우 다음에 규칙을 편집할 때 태그나 설명이 추가되지 않으면 커밋이 실패합니다. 커밋에 실패하려면 정책에 대한 태그 필요 또는 정책에 대한 설명 필요를 해야 합니다.
정책에 대한 코멘트 감사 필요	새 정책 규칙을 생성할 때 코멘트 감사가 필요합니다. 이 옵션을 활성화할 때 정책 규칙이 이미 있는 경우 다음에 규칙을 편집할 때 코멘트 감사를 추가해야 합니다.
코멘트 감사 정규식	코멘트 감사에서 코멘트 형식 매개변수에 대한 요구사항을 지정하십시오.
와일드카드 하향식 일치 모드(방화벽만 해당)	(PAN-OS 10.2.1 이상 10.2 릴리스) 와일드카드 하향식 일치 모드가 활성화된 경우 패킷이 와일드카드 마스크가 있는 소스 또는 대상 IP 주소를 사용하는 보안 정책 규칙과 일치하고 마스크가 겹치면 방화벽은 일치하는 규칙 중 마스킹을 기반으로 모든 주소 비트와 일치하는 첫 번째 규칙을 선택합니다(하향식 순서). 기본값은 비활성화되어 있으며, 중첩되는 와일드카드 마스크가 일치하는 경우 방화벽은 와일드카드 마스크에서 가장 긴 접두사를 가진 규칙을 선택합니다.
정책 규칙 적중 수	트래픽이 방화벽에서 구성한 정책 규칙과 일치하는 빈도를 추적합니다. 활성화되면 규칙이 생성, 수정, 첫 번째 적중 및 마지막 적중이었던 날짜 및 시간과 함께 각 규칙에 대한 총 트래픽 일치에 대한 총 적중 수를 볼 수 있습니다.
정책 적용 활용	

Panorama 설정: 디바이스 > 설정 > 관리

항목	설명
방화벽 또는 Panorama의 템플릿에서 다음 설정을 구성합니다. 이러한 설정은 방화벽에서 Panorama로의 연결을 설정합니다. Panorama(Panorama 설정: Panorama > 설정 > 관리). 방화벽은 *AES256* 암호화가 포함된 *SSL* 연결을 사용하여 *Panorama*에 등록합니다. 기본적으로 *Panorama*와 방화벽은 사전 정의된 *2,048*비트 인증서를 사용하여 서로를 인증하고 구성 관리 및 로그 수집을 위해 *SSL* 연결을 사용합니다. *Panorama*, 방화벽 및 로그 수집기 간의 *SSL* 연결을 더욱 안전하게 보호하려면 보안 클라이언트 통신을 참조하여 방화벽과 *Panorama* 또는 로그 수집기 간의 사용자 지정 인증서를 구성하십시오.	
다음으로 관리됨	방화벽이 **Panorama** 또는 클라우드 서비스에서 관리되는지 여부를 지정합니다.
(Panorama 관리형만 해당) Panorama 서버	Panorama 서버의 IP 주소 또는 FQDN을 입력합니다. Panorama가 고가용성(HA) 구성인 경우 두 번째 **Panorama Servers** 필드에 보조 Panorama 서버의 IP 주소 또는 FQDN을 입력합니다.
인증 키	Panorama에서 생성된 디바이스 등록 인증 키를 입력합니다.
Panorama 연결에 대한 수신 타임아웃	Panorama에서 TCP 메시지를 수신하기 위한 타임아웃(초)을 입력합니다(범위는 1~240, 기본값은 240).
Panorama 연결에 대한 타임아웃 보내기	TCP 메시지를 Panorama로 보내는 타임아웃(초)를 입력합니다(범위는 1~240, 기본값은 240).
Panorama로 SSL 전송 재시도 횟수	Panorama에 SSL(Secure Socket Layer) 메시지를 보낼 때 허용되는 재시도 횟수를 입력합니다(범위는 1~64, 기본값은 25).
자동 커밋 복구 활성화	구성이 커밋되고 방화벽에 푸시될 때 그리고 구성이 성공적으로 푸시된 후 구성된 인터벌로 방화벽이 Panorama 관리 서버에 대한 연결을 자동으로 확인하도록 활성화합니다. 활성화된 경우 방화벽이 Panorama 관리 서버에 대한 연결을 확인하지 못하면 방화벽 및 Panorama 관리가 자동으로 구성을 이전 실행 구성으로 되돌려 연결을 복원합니다.
Panorama 연결 확인 시도 횟수	**Enabled Automated Commit Recovery**가 활성화되면 방화벽이 Panorama 관리 서버에 대한 연결을 테스트하는 횟수를 구성합니다.

항목	설명
재시도 인터벌(초)	**Enable Automated Commit Recovery**가 활성화되면 방화벽이 Panorama 관리 서버에 대한 연결을 테스트하는 시도 횟수 사이의 시간을 초 단위로 구성하십시오.

보안 클라이언트 통신	보안 클라이언트 통신을 활성화하여 방화벽이 구성된 사용자 지정 인증서(기본 인증서 대신)를 사용하여 Panorama 또는 로그 수집기와의 SSL 연결을 인증하도록 합니다.
	• 없음(기본값) - 디바이스 인증서가 구성되지 않고 기본 사전 정의 인증서가 사용됩니다.
	• 로컬 - 방화벽은 로컬 디바이스 인증서와 방화벽에서 생성되거나 기존 엔터프라이즈 PKI 서버에서 불러온 해당 개인 키를 사용합니다.
	  • 인증서 - 생성하거나 불러온 로컬 디바이스 인증서를 선택합니다. 이 인증서는 방화벽에 고유할 수도 있고(방화벽 일련번호의 해시를 기반으로 함) Panorama에 연결하는 모든 방화벽에서 사용하는 공통 디바이스 인증서일 수도 있습니다.
	  • 인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다. 인증서 프로파일은 클라이언트 인증서를 확인하기 위한 CA 인증서와 인증서 해지 상태를 확인하는 방법을 정의합니다.
	• **SCEP** - 방화벽은 SCEP(Simple Certificate Enrollment Protocol) 서버에서 생성된 디바이스 인증서와 개인 키를 사용합니다.
	  • **SCEP** 프로파일 - 드롭다운에서 디바이스 > 인증서 관리 > SCEP를 선택합니다. SCEP 프로파일은 Panorama에 엔터프라이즈 PKI의 SCEP 서버에 대해 클라이언트 디바이스를 인증하는 데 필요한 정보를 제공합니다.
	  • 인증서 프로파일 - 드롭다운에서 디바이스 > 인증서 관리 > 인증서 프로파일을 선택합니다. 인증서 프로파일은 클라이언트 인증서를 확인하기 위한 CA 인증서와 인증서 해지 상태를 확인하는 방법을 정의합니다.

항목	설명

	• 통신 사용자 지정 - 방화벽은 구성된 사용자 지정 인증서를 사용하여 선택한 디바이스를 인증합니다.
	  • **Panorama** 통신 - 방화벽은 Panorama와 통신하기 위해 구성된 클라이언트 인증서를 사용합니다.
	  • **PAN-DB** 통신 - 방화벽은 PAN-DB 어플라이언스와의 통신을 위해 구성된 클라이언트 인증서를 사용합니다.
	  • **WildFire** 통신 - 방화벽은 WildFire® 어플라이언스와의 통신을 위해 구성된 클라이언트 인증서를 사용합니다.
	  • 로그 수집기 통신 - 방화벽은 로그 수집기와 통신하기 위해 구성된 클라이언트 인증서를 사용합니다.
	  • 서버 **ID** 확인 - (Panorama 및 로그 수집기 통신만 해당) 방화벽은 CN(일반 이름)을 서버의 IP 주소 또는 FQDN과 일치시켜 서버의 식별을 확인합니다.

Panorama 정책 및 개체 비활성화/능동형화	이 옵션은 방화벽에서 **Panorama** 설정을 편집할 때만 표시됩니다(Panorama의 템플릿이 아님). 디바이스 그룹 정책 및 개체가 방화벽으로 전파되지 않도록 하려면 Panorama 정책 및 개체를 비활성화합니다. 기본적으로 이 작업은 방화벽에서 해당 정책 및 개체도 제거합니다. 디바이스 그룹 정책 및 개체의 로컬 복사본을 방화벽에 보관하려면 이 옵션을 클릭할 때 열리는 대화 상자에서 비활성화하기 전에 **Panorama** 정책 및 개체 가져오기를 선택합니다. 커밋을 수행한 후 이러한 정책 및 개체는 방화벽 구성의 일부가 되고 Panorama는 더 이상 이를 관리하지 않습니다. *Multi-VSYS* 방화벽의 경우 먼저 템플릿 구성을 불러온 다음 디바이스 그룹 구성을 가져와서 *Panorama* 푸시 구성을 성공적으로 비활성화해야 합니다. 정상적인 작동 조건에서는 Panorama 관리를 비활성화할 필요가 없으며 방화벽의 유지 관리 및 구성이 복잡해질 수 있습니다. 이 옵션은 일반적으로 방화벽이 디바이스 그룹에 정의된 것과 다른 규칙 및 개체 값을 요구하는 상황에 적용됩니다. 예를 들어 방화벽을 프로덕션에서 테스트를 위해 실험실 환경으로 이동하는 경우입니다. 방화벽 정책 및 개체 관리를 Panorama로 되돌리려면 **Panorama** 정책 및 개체 활성화를 클릭합니다.

항목	설명
디바이스 및 네트워크 템플릿 비활성화/능동형화	이 옵션은 방화벽에서 **Panorama** 설정을 편집할 때만 표시됩니다(Panorama의 템플릿이 아님). 디바이스 및 네트워크 템플릿을 비활성화하여 템플릿 정보(디바이스 및 네트워크 구성)를 방화벽으로 전파하는 것을 비활성화합니다. 기본적으로 이 작업은 방화벽에서 템플릿 정보도 제거합니다. 템플릿 정보의 로컬 복사본을 방화벽에 유지하려면 이 옵션을 선택할 때 열리는 대화 상자에서 비활성화하기 전에 디바이스 및 네트워크 템플릿 가져오기를 선택합니다. 커밋을 수행한 후 템플릿 정보는 방화벽 구성의 일부가 되고 Panorama는 더 이상 해당 정보를 관리하지 않습니다. *Multi-VSYS* 방화벽의 경우 먼저 템플릿 구성을 불러온 다음 디바이스 그룹 구성을 가져와서 *Panorama* 푸시 구성을 성공적으로 비활성화해야 합니다. 정상적인 작동 조건에서는 *Panorama* 관리를 비활성화할 필요가 없으며 방화벽의 유지 관리 및 구성이 복잡해질 수 있습니다. 이 옵션은 일반적으로 템플릿에 정의된 것과 다른 디바이스 및 네트워크 구성 값이 방화벽에 필요한 상황에 적용됩니다. 예를 들어 방화벽을 프로덕션에서 테스트를 위해 실험실 환경으로 이동하는 경우입니다. 템플릿을 다시 수락하도록 방화벽을 구성하려면 디바이스 및 네트워크 템플릿 활성화를 클릭합니다.

Panorama 설정: Panorama > 설정 > 관리

Panorama를 사용하여 방화벽을 관리하는 경우 Panorama에서 다음 설정을 구성합니다. 이러한 설정은 Panorama에서 관리 방화벽으로의 연결에 대한 타임아웃 및 SSL 메시지 시도와 개체 공유 매개변수를 결정합니다.

또한 방화벽 또는 Panorama의 템플릿에서 Panorama 연결 설정을 구성해야 합니다. Panorama 설정 참조: 디바이스 > 설정 > 관리.

방화벽은 *AES256* 암호화가 포함된 *SSL* 연결을 사용하여 *Panorama*에 등록합니다. 기본적으로 *Panorama*와 방화벽은 사전 정의된 *2,048*비트 인증서를 사용하여 서로를 인증하고 구성 관리 및 로그 수집을 위해 *SSL* 연결을 사용합니다. 이러한 *SSL* 연결을 더욱 안전하게 보호하려면 보안 서버 통신 사용자 지정을 참조하여 *Panorama*와 해당 클라이언트 간의 사용자 지정 인증서를 구성하십시오.

항목	설명
디바이스 연결에 대한 수신 타임아웃	모든 관리 방화벽에서 TCP 메시지를 수신하기 위한 타임아웃(초)을 입력합니다(범위는 1~240, 기본값은 240).
디바이스 연결에 대한 타임아웃 보내기	모든 관리 방화벽에 TCP 메시지를 보내는 타임아웃(초)을 입력합니다(범위는 1~240, 기본값은 240).
디바이스로 SSL 전송 재시도 횟수	관리 방화벽에 SSL(Secure Socket Layer) 메시지를 보낼 때 허용되는 재시도 횟수를 입력합니다(범위는 1~64, 기본값은 25).
사용하지 않는 주소 및 서비스 개체를 디바이스와 공유	모든 Panorama 공유 개체 및 디바이스 그룹별 개체를 관리 방화벽과 공유하려면 이 옵션(기본적으로 활성화됨)을 선택합니다. 이 옵션을 비활성화하면 어플라이언스는 주소, 주소 그룹, 서비스 및 서비스 그룹 개체에 대한 참조에 대한 Panorama 정책을 확인하고 참조되지 않은 개체를 공유하지 않습니다. 이 옵션은 어플라이언스가 관리되는 방화벽에 필요한 개체만 보내도록 하여 총 개체 수를 줄입니다. 디바이스 그룹의 특정 디바이스를 대상으로 하는 정책 규칙이 있는 경우 해당 정책에 사용된 개체는 해당 디바이스 그룹에서 사용된 것으로 간주됩니다.
조상 요소에 정의된 개체가 더 높은 우선 순위를 갖습니다.	이 옵션(기본적으로 비활성화됨)을 선택하면 레이어 구조의 다른 수준에 있는 디바이스 그룹에 유형과 이름은 같지만 값이 다른 개체가 있는 경우 상위 그룹의 개체 값이 하위 그룹의 개체 값보다 우선적으로 적용되도록 지정합니다. 즉, 디바이스 그룹 커밋을 수행할 때 상위 값이 재정의 값을 대체합니다. 마찬가지로 이 옵션을 사용하면 공유 개체의 값이 디바이스 그룹에 있는 동일한 유형 및 이름의 개체 값을 재정의합니다. 이 옵션을 선택하면 재정의된 개체 찾기 링크가 표시됩니다.
재정의된 개체 찾기	그림자가 있는 개체를 나열하려면 이 옵션(Panorama 설정 대화상자 하단)을 선택합니다. 그림자가 있는 개체는 디바이스 그룹에서 이름은 같지만 값이 다른 공유 위치의 개체입니다. 링크는 상위 항목에 정의된 개체가 더 높은 우선 순위를 갖도록 지정한 경우에만 표시됩니다.
그룹에 대한 보고 및 필터링 활성화	이 옵션(기본적으로 비활성화됨)을 선택하면 Panorama가 방화벽에서 수신한 사용자명, 사용자 그룹 이름 및 사용자명-그룹 매핑 정보를 로컬로 저장할 수 있습니다. 이 옵션은 Panorama의 모든 디바이스 그룹에 적용됩니다. 그러나 마스터 디바이스를 지정하고 마스터 디바이스에서 사용자 및 그룹을 저장하도록 방화벽을

항목	설명
	구성하여 각 디바이스 그룹 수준에서 로컬 저장소도 활성화해야 합니다.
통신 보안 설정: Panorama > 설정 > 관리	

보안 서버 통신 사용자 지정	• 사용자 지정 인증서만 - 활성화된 경우 Panorama는 관리되는 방화벽 및 로그 수집기를 사용한 인증을 위해 사용자 지정 인증서만 수락합니다.
	• **SSL/TLS** 서비스 프로파일 - 드롭다운에서 SSL/TLS 서비스 프로파일을 선택합니다. 이 프로파일은 방화벽이 Panorama와 통신하는 데 사용할 수 있는 인증서 및 지원되는 SSL/TLS 버전을 정의합니다.
	• 인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다. 이 인증서 프로파일은 인증서 해지 확인 동작과 클라이언트가 제공하는 인증서 체인을 인증하는 데 사용되는 루트 CA를 정의합니다.
	• 인증 목록 - 다음 필드를 사용하여 새 인증 프로파일을 추가 및 구성하여 Panorama에 연결할 수 있는 클라이언트 디바이스를 인증하는 기준을 설정합니다. 인증 목록은 최대 16개의 프로파일 항목을 지원합니다.
	  • 식별자 - 제목 또는 제목 대체를 선택합니다. 권한 부여 식별자로 이름을 지정합니다.
	  • 유형 - 제목 대체를 선택한 경우. 식별자로 이름을 지정한 다음 식별자 유형으로 **IP**, 호스트 이름 또는 전자 메일을 선택합니다. 제목을 선택한 경우 식별자 유형으로 일반 이름을 사용해야 합니다.
	  • 값 - 식별자 값을 입력합니다.
	• 일련번호를 기반으로 클라이언트 인증 - Panorama는 디바이스 일련번호의 해시를 기반으로 클라이언트 디바이스를 인증합니다.
	• 인증 목록 확인 - Panorama는 인증 목록에 대해 클라이언트 디바이스 ID를 확인합니다. 디바이스는 승인을 받으려면 목록에 있는 하나의 기준과만 일치해야 합니다. 일치하는 항목이 없으면 디바이스가 인증되지 않은 것입니다.
	• 연결 해제 대기 시간(분) - Panorama가 관리 디바이스와의 현재 연결을 종료하기 전에 대기하는 시간(분)입니다. 그런 다음 Panorama는 구성된 보안 서버 통신 설정을 사용하여 관리되는

항목	설명
	디바이스와의 연결을 다시 설정합니다. 보안 서버 통신 구성을 커밋한 후 대기 시간이 시작됩니다.

보안 클라이언트 통신	보안 클라이언트 통신을 사용하면 클라이언트 Panorama가 구성된 사용자 지정 인증서(기본 사전 정의 인증서 대신)를 사용하여 HA 쌍 또는 WildFire 어플라이언스의 다른 Panorama 어플라이언스와의 SSL 연결을 인증합니다.
	• 사전 정의됨(기본값) - 디바이스 인증서가 구성되지 않고 Panorama는 사전 정의된 기본 인증서를 사용합니다.
	• 로컬 - Panorama는 로컬 디바이스 인증서와 방화벽에서 생성되거나 기존 엔터프라이즈 PKI 서버에서 불러온 해당 개인 키를 사용합니다.
	  • 인증서 - 로컬 디바이스 인증서를 선택합니다.
	  • 인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다.
	• **SCEP** - Panorama는 SCEP(Simple Certificate Enrollment Protocol) 서버에서 생성한 디바이스 인증서와 개인 키를 사용합니다.
	  • **SCEP** 프로파일 - 드롭다운에서 SCEP 프로파일을 선택합니다.
	  • 인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다.
	• 커뮤니케이션 사용자 정의
	  • **HA** 통신 - Panorama는 HA 피어와의 HA 통신을 위해 구성된 클라이언트 인증서를 사용합니다.
	  • **WildFire** 통신 - Panorama는 WildFire 어플라이언스와 통신하기 위해 구성된 클라이언트 인증서를 사용합니다.

로깅 및 보고 설정

이 섹션을 사용하여 다음을 수정합니다.

항목	설명
• 보고서 및 다음 로그 유형에 대한 만료 기간 및 저장 할당량. 설정은 고가용성 쌍 간에 동기화됩니다. • 방화벽이 로컬로 생성 및 저장하는 모든 유형의 로그(**Device** > **Setup** > 관리). 설정은 방화벽의 모든 가상 시스템에 적용됩니다. • M-시리즈 어플라이언스 또는 Panorama 모드의 Panorama 가상 어플라이언스가 로컬로 생성 및 저장하는 로그: 시스템, 구성, 애플리케이션 통계 및 User-ID™ 로그(**Panorama** > **Setup** > **Management**). • 레거시 모드의 Panorama 가상 어플라이언스가 로컬에서 생성하거나 방화벽에서 수집하는 모든 유형의 로그(**Panorama** > **Setup** > **Management**). 방화벽이 *Panorama Log Collectors*로 보내는 로그의 경우 각 수집기 그룹에서 스토리지 할당량 및 만료 기간을 설정합니다(Panorama > 수집기 그룹 참조). • 사용자 활동 보고서를 계산하고 내보내기 위한 속성입니다. • 방화벽 또는 Panorama에서 생성된 사전 정의된 보고서.	
로그 저장소 탭 (Panorama 관리 서버 및 PA-5200 시리즈 및 PA-7000 시리즈 방화벽을 제외한 모든 방화벽 모델) 로깅 및 보고 설정(***Panorama*** > 설정 > 관리)을 편집하면 *Panorama*에 이 탭이 표시됩니다. *Panorama* 템플릿을 사용하여 방화벽 설정을 구성하는 경우(***Device*** > ***Setup*** > ***Management***) 단일 디스크 스토리지 및 다중 디스크 스토리지 탭을 참조하십시오.	각 로그 유형에 대해 다음을 지정합니다. • 할당량 - 로그 저장을 위해 하드 디스크에 할당된 할당량(백분율)입니다. 할당량 값을 변경하면 연결된 디스크 할당이 자동으로 변경됩니다. 모든 값의 합계가 100%를 초과하면 빨간색으로 메시지가 나타나고 설정을 저장하려고 하면 오류 메시지가 나타납니다. 이 경우 합계가 100% 한도 이내가 되도록 백분율을 조정하십시오. *VM* 시리즈 방화벽은 기본적으로 ***SCTP*** 로그 저장소, ***SCTP*** 요약, 시간별 ***SCTP*** 요약, 일일 ***SCTP*** 요약 및 주간 ***SCTP*** 요약에 대해 할당량이 *0%*이므로 *SCTP* 정보를 기록하려면 이러한 방화벽에 일정 비율을 할당해야 합니다. • 최대 일수 - 로그 만료 기간의 길이(일)입니다(범위는 1 - 2,000). 방화벽 또는 Panorama 어플라이언스는 지정된 기간을 초과하는 로그를 자동으로 삭제합니다. 기본적으로 만료 기간이 없으므로 로그가 만료되지 않습니다. 방화벽 또는 Panorama 어플라이언스는 로그를 생성하는 동안 로그를 평가한 다음 만료 기간 또는 할당량 크기를 초과하는 로그를 삭제합니다.

항목	설명
	주간 요약 로그는 방화벽이 로그를 삭제하는 시간 사이에 만료 임계값에 도달하면 다음 삭제 전에 임계값을 초과하여 에이징될 수 있습니다. 로그 할당량이 최대 크기에 도달하면 새 로그 항목이 가장 오래된 로그 항목을 덮어쓰기 시작합니다. 로그 할당량 크기를 줄이면 변경 사항을 커밋할 때 방화벽이나 *Panorama*가 가장 오래된 로그를 제거합니다. *HA* 액티브/패시브 구성에서 패시브 피어는 로그를 수신하지 않으므로 페일오버가 발생하고 패시브 피어가 활성화되지 않는 한 로그를 삭제하지 않습니다.

	• 코어 파일 - 방화벽에서 시스템 프로세스 오류가 발생하면 프로세스와 실패한 이유에 대한 세부 정보가 포함된 코어 파일이 생성됩니다. 코어 파일이 기본 코어 파일 저장 위치(`/var/cores` 파티션)에 비해 너무 큰 경우 ### 코어 파일 옵션을 활성화하여 더 큰 대체 저장 위치(`/opt/panlogs/cores`)를 할당할 수 있습니다. Palo Alto Networks 지원 엔지니어는 필요한 경우 할당된 스토리지를 늘릴 수 있습니다.
	## ## 파일 옵션을 활성화하거나 비활성화하려면 컨피그레이션 모드에서 CLI 명령
	`# set deviceconfig setting management large-core [yes|no]`
	를 입력한 다음 컨피그레이션을 ##합니다.
	이 옵션을 비활성화하면 코어 파일이 삭제됩니다.
	코어 파일을 내보내려면 작동 모드에서 SCP를 사용해야 합니다.
	`> scp export core-file large-corefile`
	Palo Alto Networks 지원 엔지니어만 코어 파일의 내용을 해석할 수 있습니다.
	• 기본값 복원 - 기본값으로 되돌리려면 이 옵션을 선택합니다.

항목	설명
세션 로그 저장소 및 관리 로그 저장소 탭 (PA-5200 시리즈 및 PA-7000 시리즈 방화벽만 해당)	PA-5200 시리즈 및 PA-7000 시리즈 방화벽은 관리 로그와 세션 로그를 별도의 디스크에 저장합니다. 각 로그 세트에 대한 탭을 선택한 다음 로그 저장소 탭에 설명된 설정을 구성합니다. • 세션 로그 저장소 - 세션 로그 할당량을 선택한 다음 트래픽, 위협, URL 필터링, HIP 일치, User-ID, GTP/터널, SCTP 및 인증 로그와 확장된 위협 PCAP에 대한 할당량 및 만료 기간을 설정합니다. • 관리 로그 저장소 - HIP 보고서, 데이터 필터링 캡처, 앱 PCAP 및 디버그 필터 PCAP뿐만 아니라 시스템, 구성 및 앱 통계 로그에 대한 할당량 및 만료 기간을 설정합니다.
단일 디스크 저장소 및 다중 디스크 저장소 탭 (Panorama 템플릿만 해당)	Panorama 템플릿을 사용하여 로그 할당량 및 만료 기간을 구성하는 경우 템플릿에 할당된 방화벽에 따라 다음 탭 중 하나 또는 둘 모두에서 설정을 구성합니다. • **PA-5200** 시리즈 및 **PA-7000** 시리즈 방화벽 - 다중 디스크 스토리지를 선택한 다음 세션 로그 스토리지 및 관리 로그 스토리지 탭에서 설정을 구성합니다. *PA-5200* 시리즈 방화벽은 기본적으로 ***SCTP*** 로그 저장소, ***SCTP*** 요약, 시간별 ***SCTP*** 요약, 일일 ***SCTP*** 요약 및 주간 ***SCTP*** 요약에 대해 할당량이 *0%*이므로 *SCTP* 정보를 기록하려면 이러한 방화벽에 일정 비율을 할당해야 합니다. • 기타 모든 방화벽 모델 - 단일 디스크 저장소를 선택한 다음 세션 로그 할당량을 선택하고 로그 저장소 탭에서 설정을 구성합니다.
로그 내보내기 및 보고 탭	필요에 따라 다음 로그 내보내기 및 보고 설정을 구성합니다. • 구성 감사용 버전 수 - 가장 오래된 구성 버전을 삭제하기 전에 저장할 구성 버전 수를 입력합니다(기본값은 100). 이러한 저장된 버전을 사용하여 구성 변경 사항을 감사하고 비교할 수 있습니다. • 구성 백업 버전 수 - (Panorama만 해당) 가장 오래된 구성 백업을 버리기 전에 저장할 구성 백업 수를 입력합니다(기본값은 100). • **CSV** 내보내기의 최대 행 수 - 트래픽 로그 보기에서 **CSV**로 내보낼 때 생성된 CSV 보고서에 나타날 최대 행 수를 입력합니다(범위는 1~1,048,576, 기본값은 65,535).

항목	설명
	• 사용자 활동 보고서의 최대 행 수 - 자세한 사용자 활동 보고서에 지원되는 최대 행 수를 입력합니다(범위는 1~1,048,576, 기본값은 5,000).
로그 내보내기 및 보고 탭(계속)	• 평균 찾아보기 시간(초) - 모니터 > PDF 보고서 > 사용자 활동 보고서(범위는 0~300초, 기본값은 60)에 대해 찾아보기 시간이 초 단위로 계산되는 방식을 조정하려면 이 변수를 구성합니다. 계산 시 웹 광고 및 콘텐츠 전송 네트워크로 분류된 사이트는 무시됩니다. 찾아보기 시간 계산은 URL 필터링 로그에 기록된 컨테이너 페이지를 기반으로 합니다. 많은 사이트에서 고려해서는 안 되는 외부 사이트의 콘텐츠를 로드하기 때문에 컨테이너 페이지가 이 계산의 기초로 사용됩니다. 컨테이너 페이지에 대한 자세한 내용은 컨테이너 페이지를 참조하십시오. 평균 탐색 시간 설정은 관리자가 사용자가 웹 페이지를 탐색하는 데 소요되어야 한다고 생각하는 평균 시간입니다. 평균 탐색 시간이 경과한 후에 이루어진 모든 요청은 새로운 탐색 활동으로 간주됩니다. 계산은 첫 번째 요청 시간(시작 시간)과 평균 탐색 시간 사이에 로드된 모든 새 웹 페이지를 무시합니다. 이 동작은 관심 있는 웹 페이지 내에 로드된 모든 외부 사이트를 제외하도록 설계되었습니다. 예시: 평균 탐색 시간 설정이 2분이고 사용자가 웹 페이지를 열고 5분 동안 해당 페이지를 보는 경우 해당 페이지의 탐색 시간은 여전히 2분입니다. 이것은 사용자가 주어진 페이지를 보는 시간을 결정할 방법이 없기 때문에 수행됩니다. • 페이지 로드 임계값(초) - 페이지 요소가 페이지에 로드되는 데 걸리는 예상 시간(초)을 조정할 수 있습니다(범위는 0~60, 기본값은 20). 첫 번째 페이지 로드와 페이지 로드 임계값 사이에 발생하는 모든 요청은 페이지의 요소로 간주됩니다. 페이지 로드 임계값 외부에서 발생하는 모든 요청은 사용자가 페이지 내에서 링크를 클릭한 것으로 간주됩니다. 페이지 로드 임계값은 모니터 > PDF 보고서 > 사용자 활동 보고서에 대한 계산에도 사용됩니다. • **Syslog HOSTNAME** 형식 - syslog 메시지 헤더에서 FQDN, 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 사용할지의 여부를 선택합니다. 이 헤더는 메시지가 시작된 방화벽 또는 Panorama 관리 서버를 식별합니다.

항목	설명
	• 보고서 런타임 - 방화벽 또는 Panorama 어플라이언스가 매일 예약된 보고서 생성을 시작할 시간(기본값: 오전 2시)을 선택합니다. • 보고서 만료 기간 - 보고서의 만료 기간(일)을 설정합니다(범위는 1 ~ 2,000). 기본적으로 만료 기간이 없으므로 보고서가 만료되지 않습니다. 방화벽 또는 Panorama 어플라이언스는 시스템 시간에 따라 매일 오전 2시에 만료된 보고서를 삭제합니다.
	• **Stop Traffic when LogDb full**(방화벽만 해당, 기본적으로 비활성화됨) - 로그 데이터베이스가 가득 찼을 때 방화벽을 통한 트래픽을 중지하려면 이 옵션을 선택합니다. • **Threat Vault Access** 활성화(기본적으로 활성화됨) - 방화벽이 Threat Vault에 액세스하여 탐지된 위협에 대한 최신 정보를 수집할 수 있도록 합니다. 이 정보는 위협 로그 및 ACC에 차트로 표시된 주요 위협 활동에 대해 사용할 수 있습니다. • 높은 **DP** 로드 시 로그온 활성화(방화벽만 해당, 기본적으로 비활성화됨) - 방화벽의 패킷 처리 로드가 CPU 사용률 100%일 때 시스템 로그 항목이 생성되도록 지정하려면 이 옵션을 선택합니다. 높은 ***DP*** 로드에 로그온 활성화를 통해 관리자는 높은 *CPU* 사용률의 원인을 검토하고 식별할 수 있습니다. *CPU*에 모든 패킷을 처리할 수 있는 충분한 주기가 없기 때문에 *CPU* 로드가 높으면 운영 성능이 저하될 수 있습니다. 시스템 로그는 이 문제에 대해 경고하고*(*로그 항목이 *1*분마다 생성됨*)* 가능한 원인을 검토할 수 있도록 합니다. • 고속 로그 전달 활성화(PA-5200 시리즈, PA-5450 및 PA-7000 시리즈 방화벽만, 기본적으로 PA-5450에서만 활성화됨) - 모범 사례로서 최대 100%까지 Panorama에 로그를 초당 최대 120,000개의 로그 속도로 전달하려면 이 옵션을 선택

항목	설명
	하십시오. 비활성화된 경우 방화벽은 초당 최대 80,000개의 로그만 Panorama에 로그를 포워딩합니다. 이 옵션을 활성화하면 방화벽이 로그를 로컬에 저장하거나 대시보드, **ACC** 또는 모니터 탭에 표시하지 않습니다. 또한 이 옵션을 사용하려면 Panorama로의 로그 포워딩을 구성 해야 합니다. • 로그 수집기 상태 - 방화벽이 분산 로그 수집 아키텍처에 대한 연결을 성공적으로 설정하고 로그를 보내고 있는지의 여부를 표시합니다. 로깅 서비스에 로그를 보내도록 방화벽도 구성된 경우 로깅 서비스 상태를 확인합니다. 로깅 서비스 섹션에서 확인할 수 있습니다.
(Panorama 전용)	• 디바이스에서 버퍼링된 로그 포워딩(기본적으로 활성화됨) - Panorama에 대한 연결이 끊어지면 방화벽이 하드 디스크(로컬 스토리지)의 로그 항목을 버퍼링할 수 있습니다. Panorama에 대한 연결이 복원되면 방화벽이 로그 항목을 Panorama로 포워딩합니다. 버퍼링에 사용할 수 있는 디스크 공간은 방화벽 모델의 로그 저장소 할당량과 롤오버 보류 중인 로그의 양에 따라 다릅니다. 사용 가능한 공간이 소모되면 새 이벤트를 기록할 수 있도록 가장 오래된 항목이 삭제됩니다. *Panorama*에 대한 연결이 끊어진 경우 로그 손실을 방지하려면 디바이스에서 버퍼링된 로그 포워딩을 활성화하십시오. • 기본으로 변환 시 새 로그만 가져오기(기본적으로 비활성화됨) - 이 옵션은 NFS(네트워크 파일 시스템)에 로그를 기록하는 레거시 모드의 Panorama 가상 어플라이언스에만 적용됩니다. NFS 로깅을 사용하면 기본 Panorama만 NFS에 마운트됩니다. 따라서 방화벽은 활성 기본 Panorama에만 로그를 보냅니다. 이 옵션을 사용하면 HA 페일오버가 발생하고 보조 Panorama가 NFS에 대한 로깅을 재개할 때(기본으로 승격된 후) 새로 생성된 로그만 Panorama로 보내도록 방화벽을 구성할 수 있습니다. 이 옵션은 일반적으로 상당한 시간이 지난 후 Panorama에 대한 연결이 복원될 때 방화벽이 버퍼링된 로그를 대량으로 보내는 것을 방지하기 위해 활성화됩니다. • 로컬 디스크에 대한 활성 기본 로그만(기본적으로 비활성화됨) - 이 옵션은 레거시 모드의 Panorama 가상 어플라이언스에

항목	설명
	만 적용됩니다. 이 옵션을 사용하면 활성 Panorama만 구성하여 로그를 로컬 디스크에 저장할 수 있습니다.

	• 사전 정의된 보고서(기본적으로 활성화됨) - 애플리케이션, 트래픽, 위협, URL 필터링 및 SCTP(Stream Control Transmission Protocol)에 대한 사전 정의된 보고서를 방화벽과 Panorama에서 사용할 수 있습니다. SCTP에 대해 사전 정의된 보고서는 **Device** > **Setup** > **Management** > 일반 설정에서 SCTP 보안이 활성화된 후 방화벽 및 Panorama에서 사용할 수 있습니다.
	
	방화벽은 매시간 결과를 생성하는 데 메모리 리소스를 사용하기 때문에(보기를 위해 통합 및 컴파일되는 Panorama로 포워딩) 메모리 사용량을 줄이기 위해 사용자와 관련이 없는 보고서를 비활성화할 수 있습니다. 보고서를 비활성화하려면 보고서에 대해 이 옵션을 비활성화합니다.
	
	사전 정의된 보고서 생성을 완전히 활성화하거나 비활성화하려면 모두 선택 또는 모두 선택 취소를 클릭합니다.
	
	보고서를 비활성화하기 전에 이를 사용하는 그룹 보고서 또는 *PDF* 보고서가 없는지 확인하십시오. 보고서 세트에 할당된 사전 정의된 보고서를 비활성화하면 전체 보고서 세트에 데이터가 없습니다.
	• 관리자 활동 로그(기본적으로 비활성화됨) - 관리자가 방화벽 CLI에서 작동 명령을 실행하거나 웹 인터페이스를 탐색할 때 감사 로그를 생성할지의 여부를 지정합니다. 감사 로그를 생성하고 포워딩하려면 먼저 syslog 서버를 성공적으로 구성해야 합니다.
	  • 작동 명령 - 관리자가 CLI에서 작동 또는 디버그 명령을 실행하거나 웹 인터페이스에서 트리거되는 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 개체 간 탐색이 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.

항목	설명
	• **Syslog** 서버 - 감사 로그를 포워딩할 대상 syslog 서버 프로파일을 선택합니다.
로그 인터페이스(PA-5450 전용)	
IP 주소	로그 인터페이스 포트의 IP 주소를 입력합니다. 로그 인터페이스가 *IP* 주소로 구성되면 특정 서비스에 대해 서비스 경로가 지정되는 경우를 제외하고 모든 로그 전달이 관리 인터페이스*(*기본값*)*에서 처리되는 것에서 로그 인터페이스로 자동 전환됩니다. 특정 서비스 경로는 로그 인터페이스에 의해 우선순위가 지정됩니다.
넷마스크(netmask)	로그 인터페이스의 IP 주소에 대한 네트워크 마스크를 지정합니다.
기본 게이트웨이	발신 로그의 경로를 활성화하려면 기본 게이트웨이의 IP 주소를 입력합니다.
IPv6 주소	네트워크에서 IPv6을 사용하는 경우 다음을 정의합니다. • **IPv6** 주소 - 로그 인터페이스 포트의 IPv6 주소입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv6 주소입니다.
링크 속도	인터페이스 속도를 Mbps 단위로 선택하거나 자동(기본값)을 선택하여 방화벽이 연결을 기반으로 속도를 자동으로 결정하도록 합니다. 속도를 구성할 수 없는 인터페이스의 경우 **auto**가 유일한 옵션입니다.
링크 듀플렉스	인터페이스 전송 모드가 전이중(**full**), 반이중(**half**) 또는 자동 협상(**auto**)인지 선택합니다.
링크 상태	인터페이스 상태를 활성화(**up**), 비활성화(**down**) 또는 연결에 따라 자동으로 결정(**auto**)할지의 여부를 선택합니다. 기본값은 자동입니다.
로그 인터페이스 통계	통계 표시를 선택하여 패킷 통계 및 오류를 봅니다.
배너 및 메시지	

항목	설명
오늘의 메시지 대화 상자에서 모든 메시지를 보려면 오늘의 메시지를 참조하십시오. 오늘의 메시지를 구성하고 확인을 클릭하면 이후에 로그인하는 관리자와 브라우저를 새로 고치는 활성 관리자에게 새 메시지나 업데이트된 메시지가 즉시 표시됩니다. 커밋이 필요하지 않습니다. 이를 통해 커밋을 수행하기 전에 임박한 커밋에 대해 다른 관리자에게 경고할 수 있습니다.	
오늘의 메시지 (체크박스)	관리자가 웹 인터페이스에 로그인할 때 표시할 오늘의 메시지 대화 상자를 활성화하려면 이 옵션을 선택합니다.
오늘의 메시지 (텍스트 입력 필드)	오늘의 메시지 대화 상자에 대한 텍스트(최대 3,200자)를 입력합니다.
다시 표시 안 함 허용	오늘의 메시지 대화 상자에 다시 표시 안 함 옵션을 포함하려면 이 옵션(기본적으로 비활성화됨)을 선택하십시오. 이를 통해 관리자는 후속 로그인에서 동일한 메시지가 표시되지 않도록 할 수 있습니다. 오늘의 메시지 텍스트를 수정하면 다시 표시 안 함을 선택한 관리자에게도 메시지가 표시됩니다. 관리자는 메시지가 다시 수정되지 않는 한 후속 세션에서 수정된 메시지를 보지 않으려면 이 옵션을 다시 선택해야 합니다.
제목	오늘의 메시지 헤더에 텍스트를 입력합니다(기본값은 ### ###).
배경색	오늘의 메시지 대화 상자의 배경색을 선택합니다. 기본값(없음)은 밝은 회색 배경입니다.
아이콘	오늘의 메시지 대화 상자에서 텍스트 위에 표시할 사전 정의된 아이콘을 선택합니다. • 없음(기본값) • 오류 • 도움말 • 정보

항목	설명
	• 경 고 
헤더 배너	헤더 배너에 표시되는 텍스트를 입력합니다(최대 3,200자).
헤더 색상	헤더 배경의 색상을 선택합니다. 기본값(없음)은 투명한 배경입니다.
헤더 텍스트 색상	헤더 텍스트의 색상을 선택합니다. 기본값(없음)은 검정색입니다.
머리글과 바닥글에 동일한 배너	바닥글 배너가 머리글 배너와 동일한 텍스트 및 색상을 갖도록 하려면 이 옵션(기본적으로 활성화됨)을 선택합니다. 활성화되면 바닥글 배너 텍스트 및 색상 필드가 회색으로 표시됩니다.
바닥글 배너	바닥글 배너에 표시되는 텍스트를 입력합니다(최대 3,200자).
바닥글 색상	바닥글 배경 색상을 선택합니다. 기본값(없음)은 투명한 배경입니다.
바닥글 텍스트 색상	바닥글 텍스트의 색상을 선택합니다. 기본값(없음)은 검정색입니다.
최소 암호 복잡성	
활성화됨	로컬 계정에 대한 최소 암호 요구 사항을 활성화합니다. 이 기능을 사용하면 방화벽의 로컬 관리자 계정이 정의된 암호 요구 사항 집합을 준수하도록 할 수 있습니다. 이러한 설정을 재정의하고 특정 계정에 적용할 수 있는 이러한 옵션의 하위 집합으로 암호 프로파일을 만들 수도 있습니다. 자세한 내용은 디바이스 > 암호 프로파일을 참조하고 계정에 사용할 수 있는 유효한 문자에 대한 정보는 사용자명 및 암호 요구 사항을 참조하십시오. 최대 암호 길이는 *64*자입니다. 고가용성(HA)을 구성한 경우 암호 복잡성 옵션을 구성할 때 항상 기본 피어를 사용하고 변경한 후 즉시 커밋합니다. 최소 암호 복잡성 설정은 암호 해시를 지정한 로컬 데이터베이스 계정에 적용되지 않습니다(디바이스 > 로컬 사용자 데이터베이스 > 사용자 참조).

항목	설명
	무차별 대입 네트워크 액세스 공격이 성공하는 것을 방지하려면 강력한 암호가 필요합니다. 최소 길이와 대문자, 소문자, 숫자, 특수 문자 중 하나 이상을 사용해야 합니다. 또한 비밀번호에 문자와 사용자명이 과도하게 반복되는 것을 방지하고 비밀번호를 재사용할 수 있는 빈도에 대한 제한을 설정하고 비밀번호가 너무 오래 사용되지 않도록 정기적인 비밀번호 변경 기간을 설정합니다. 암호 요구 사항이 강할수록 공격자가 암호를 해킹하기가 더 어려워집니다. 엄격한 암호를 보장하기 위해 암호 강도에 대한 모범 사례를 사용하십시오.
최소 길이	최소 암호 길이가 필요합니다(범위는 1~16자). *FIPS-CC* 모드에서 최소 암호 길이의 범위는 *8~16*자입니다.
최소 대문자	최소 대문자 수를 요구합니다(범위는 0~16자).
최소 소문자	최소 소문자 수를 요구합니다(범위는 0~16자).
최소 숫자	최소 숫자의 문자가 필요합니다(범위는 0~16개의 숫자).
최소 특수 문자	최소 특수 문자(영숫자 아님)가 필요합니다(범위는 0~16자).
반복 문자 차단	암호에 허용되는 순차적 중복 문자 수를 지정합니다(범위는 3~16). 값을 3으로 설정하면 동일한 문자를 3번 연속으로 사용할 수 있지만, 동일한 문자를 4번 이상 연속해서 사용하면 암호를 허용하지 않습니다. 예를 들어, 값이 3으로 설정되면 시스템은 비밀번호 test111 또는 111test111을 승인하지만 test1111은 승인하지 않습니다. 숫자 1이 순서대로 4번 나타나기 때문입니다.
사용자명 포함 차단(역방향 포함)	계정 사용자명(또는 이름의 역버전)이 암호에 사용되지 않도록 하려면 이 옵션을 선택합니다.
새 비밀번호는 문자별로 다릅니다.	관리자가 암호를 변경할 때 문자는 지정된 값만큼 달라야 합니다.

항목	설명
첫 로그인 시 비밀번호 변경 필요	관리자가 방화벽에 처음 로그인할 때 암호를 변경하라는 메시지를 표시하려면 이 옵션을 선택합니다.
비밀번호 재사용 제한 방지	지정된 개수에 따라 이전 암호를 재사용하지 않도록 요구합니다. 예를 들어 값이 4로 설정되면 마지막 4개의 비밀번호(범위는 0~50)를 재사용할 수 없습니다.
비밀번호 변경 차단 기간(일)	사용자는 지정된 일 수에 도달할 때까지 암호를 변경할 수 없습니다(범위는 0~365일).
비밀번호 변경 필수 기간(일)	관리자가 정기적으로(일 단위로) 암호를 변경하도록 요구합니다(범위는 0~365). 예를 들어 값을 90으로 설정하면 관리자에게 90일마다 암호를 변경하라는 메시지가 표시됩니다. 만료 경고를 0일에서 30일 사이로 설정하고 유예 기간을 지정할 수도 있습니다.
만료 경고 기간(일)	필수 암호 변경 기간이 설정된 경우 이 만료 경고 기간을 사용하여 필요한 변경 날짜(범위: 0 ~ 30)까지 남은 날짜가 지정된 일 수 미만인 경우 로그인할 때마다 사용자에게 암호를 변경하라는 메시지를 표시할 수 있습니다.
만료 후 관리자 로그인 수(횟수)	관리자가 변경이 필요한 날짜 이후 지정된 횟수만큼 로그인할 수 있도록 허용합니다(범위는 0~3). 예를 들어 이 값을 3으로 설정하고 계정이 만료된 경우 계정이 잠디바이스 전에 암호를 변경하지 않고 3번 더 로그인할 수 있습니다.
만료 후 유예 기간(일)	관리자는 계정이 만료된 후 지정된 일 수 동안 로그인할 수 있습니다(범위는 0~30).
AutoFocus™	
활성화됨	방화벽이 AutoFocus 포털에 연결하여 위협 인텔리전스 데이터를 검색하고 방화벽과 AutoFocus 간의 통합 검색을 활성화할 수 있습니다. AutoFocus에 연결되면 방화벽은 트래픽, 위협, URL 필터링, WildFire 제출 및 데이터 필터링 로그 항목(**Monitor** > **Logs**)과 관련된 AutoFocus 데이터를 표시합니다. 이러한 유형의 로그 항목(예: IP 주소 또는 URL)에서 아티팩트를 클릭하여 해당 아티팩트에 대한 AutoFocus 결과 및 통계 요약을 표시할 수 있습니다. 그런 다음 방화벽에서 직접 아티팩트에 대한 확장된 AutoFocus 검색을 열 수 있습니다.

항목	설명
	AutoFocus 라이선스가 방화벽(***Device*** > ***Licenses***)에서 활성화되어 있는지 확인하십시오. *AutoFocus* 라이선스가 표시되지 않으면 라이선스 관리 옵션 중 하나를 사용하여 라이선스를 활성화하십시오.
AutoFocus URL	AutoFocus URL 입력: **`https://autofocus.paloaltonetworks.com:10443`**
쿼리 타임아웃(초)	방화벽이 위협 인텔리전스 데이터에 대해 AutoFocus 쿼리를 시도하는 시간(초)을 설정합니다. AutoFocus 포털이 지정된 기간이 끝나기 전에 응답하지 않으면 방화벽이 연결을 닫습니다.

Cortex Data Lake

이 섹션을 사용하여 로그를 Cortex Data Lake로 포워딩하도록 VM 시리즈 및 하드웨어 기반 방화벽을 구성합니다. 아래에 설명된 옵션을 구성하는 전체 워크플로는 다음과 같습니다.

- Cortex Data Lake에 로깅 시작(Panorama 제외)
- Cortex Data Lake에 로깅 시작(Panorama 관리 방화벽용)

로깅 서비스는 이제 *Cortex Data Lake*라고 합니다. 그러나 일부 방화벽 기능과 버튼에는 여전히 로깅 서비스 이름이 표시됩니다.

Cortex Data Lake 활성화	방화벽(또는 Panorama를 사용하는 경우 선택한 템플릿에 속한 방화벽) 이 로그를 Cortex Data Lake(이전에는 로깅 서비스라고 함)로 전달하도록 하려면 이 옵션을 선택합니다. 로그 전달을 구성한 후(개체 > 로그 전달) 방화벽은 로그를 Cortex Data Lake로 직접 전달합니다. 이는 Panorama 관리 방화벽의 경우에도 마찬가지입니다.
중복 로깅 활성화(Panorama 관리 방화벽에만 해당)	Cortex Data Lake에 로그를 보내는 것 외에도 Panorama 및 분산 로그 수집기에 계속 로그를 보내려면 중복 로깅을 활성화합니다. 이것은 Cortex Data Lake를 평가할 때 유용한 옵션입니다. 활성화되면 선택한 템플릿에 속한 방화벽이 Cortex Data Lake와 Panorama 또는 Distributed Log Collection 아키텍처에 로그 복사본을 저장합니다.
향상된 애플리케이션 로깅 활성화	방화벽이 Palo Alto Networks 애플리케이션에 대한 네트워크 가시성을 높이는 데이터를 수집하도록 하려면 **Enhanced**

항목	설명
	Application Logging을 활성화하십시오. 예를 들어, 이렇게 향상된 네트워크 가시성을 통해 Palo Alto Networks Cortex XDR 앱은 정상적인 네트워크 활동에 대한 기준을 더 잘 분류하고 설정하여 방화벽이 공격을 나타낼 수 있는 비정상적인 동작을 탐지할 수 있습니다. 향상된 애플리케이션 로깅에는 로깅 서비스(Cortex Data Lake) 라이센스가 필요합니다. 이러한 로그는 볼 수 없으며 Palo Alto Networks 애플리케이션에서만 사용하도록 설계되었습니다.
리전	방화벽이 로그를 포워딩할 Cortex Data Lake(Logging Service) 인스턴스의 지리적 영역을 선택합니다. Cortex 허브에 로그인하여 Cortex Data Lake 인스턴스가 배포된 지역을 확인합니다(허브에서 상단 메뉴 모음 및 앱 관리에서 설정 기어 선택).
PA-7000 시리즈 및 PA-5200 시리즈 방화벽용 Cortex Data Lake에 대한 연결 수	(PA-7000 시리즈 및 PA-5200 시리즈 방화벽만 해당) 방화벽에서 Cortex Data Lake로 로그를 보내기 위한 연결 수를 지정합니다(범위는 1~20, 기본값은 5). 방화벽에서 **`request logging-service-forwarding status`** CLI 명령을 사용하여 방화벽과 Cortex Data Lake 간의 활성 연결 수를 확인할 수 있습니다.
Panorama 없이 온보드 (Panorama에서 관리하지 않는 방화벽의 경우)	Panorama에서 관리하지 않는 방화벽을 활성화하여 Cortex Data Lake에 로그를 보낼 수 있습니다. 이렇게 하려면 먼저 Cortex Data Lake 앱에서 키를 생성해야 합니다. 이 키를 사용하면 방화벽이 Cortex Data Lake를 인증하고 안전하게 연결할 수 있습니다. 키를 생성한 후 키를 입력하고 방화벽이 Cortex Data Lake로 로그 포워딩을 시작하도록 합니다.
로깅 서비스 상태	Cortex Data Lake에 대한 연결 상태를 봅니다. 다음 검사에 대한 세부 정보를 보려면 상태 표시: • 라이선스 - 방화벽에 Cortex Data Lake로 로그를 포워딩할 수 있는 유효한 라이선스가 있는지의 여부를 나타내는 ## 또는 ##입니다. • 인증서 - 방화벽이 Cortex Data Lake에 인증하는 데 필요한 인증서를 성공적으로 가져왔는지의 여부를 나타내는 ## 또는 ##입니다. • 고객 정보 - 방화벽에 Cortex Data Lake를 사용하는 데 필요한 고객 식별 번호가 있는지의 여부를 나타내는 ## 또는 ##입니다. 상태가 ##이면 고객 식별 번호도 볼 수 있습니다.

항목	설명
	• 디바이스 연결 - 방화벽이 Cortex Data Lake에 성공적으로 연결되었는지의 여부를 나타냅니다.
SSH 관리 프로파일 설정	
서버 프로파일	네트워크의 CLI 관리 연결을 위한 SSH 세션에 적용되는 SSH 서비스 프로파일 유형입니다. 기존 서버 프로파일을 적용하려면 프로파일을 선택한 다음 확인을 클릭한 다음 변경 사항을 커밋합니다. 프로파일을 활성화하려면 *CLI*에서 *SSH* 서비스를 다시 시작해야 합니다. 자세한 내용은 디바이스 > 인증서 관리 > SSH 서비스 프로파일을을 참조하십시오.
PAN-OS 엣지 서비스 설정	
타사 디바이스 판정 사용	이 옵션은 향후 릴리스용으로 예약되어 있습니다. 이 옵션을 활성화하면 기능이 없습니다.
연결 상태	방화벽과 에지 서비스 연결 상태(연결됨 또는 연결 끊김) 를 표시합니다.
사용자 컨텍스트 클라우드 서비스 활성화	이 옵션을 선택하면 방화벽을 사용자 컨텍스트 클라우드 서비스에 연결하여 클라우드 ID 엔진을 사용하여 방화벽 및 장치 간의 매핑 및 태그와 같은 정보에 대한 재배포를 보고 관리할 수 있습니다.
연결 상태	방화벽의 사용자 컨텍스트 클라우드 서비스에 대한 연결 상태(연결 또는 연결 해제)를 표시합니다.

디바이스 > 설정 > 작업

다음 작업을 수행하여 방화벽 및 Panorama™의 실행 및 후보 구성을 관리할 수 있습니다. Panorama 가상 어플라이언스를 사용하는 경우 이 페이지의 설정을 사용하여 레거시 모드에서 Panorama 가상 어플라이언스에 대한 로그 스토리지 파티션을 구성할 수도 있습니다.

실행 중인 구성의 일부가 되는 지점에서 변경 사항을 활성화하려면 후보 구성에서 변경 사항을 커밋해야 합니다. 가장 좋은 방법은 후보 구성을 주기적으로 저장하는 것입니다.

CLI에서 SCP(Secure Copy) 명령을 사용하여 구성 파일, 로그, 보고서 및 기타 파일을 *SCP* 서버로 내보내고 파일을 다른 방화벽이나 *Panorama M*-시리즈 또는 가상 어플라이언스로 가져올 수 있습니다. 그러나 로그 데이터베이스가 너무 커서 내보내기 또는 가져오기가 실용적이지 않기 때문에 다음 모델은 전체 로그 데이터베이스의 내보내기 또는 가져오기를 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*).*

기능	설명
구성 관리	
마지막으로 저장된 구성으로 되돌리기	후보 구성의 기본 스냅샷(.snapshot.xml)을 복원합니다(웹 인터페이스의 오른쪽 상단에서 구성 > 저장 변경을 선택할 때 생성하거나 덮어쓰는 스냅샷). (Panorama만 해당) 되돌릴 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 선택하려면 디바이스 그룹 및 템플릿을 선택합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.
실행 중인 구성으로 되돌리기	현재 실행 중인 구성을 복원합니다. 이 작업은 마지막 커밋 이후에 모든 관리자가 후보 구성에 대해 수행한 모든 변경 사항을 취소합니다. 특정 관리자의 변경 사항만 되돌리려면 변경 사항 되돌리기를 참조하십시오. (Panorama만 해당) 되돌릴 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 선택하려면 디바이스 그룹 및 템플릿을 선택합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.

기능	설명
명명된 구성 스냅샷 저장	기본 스냅샷(.snapshot.xml)을 덮어쓰지 않는 후보 구성 스냅샷을 생성합니다. 스냅샷의 이름을 입력하거나 덮어쓸 기존의 명명된 스냅샷을 선택합니다. (Panorama만 해당) 저장할 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 선택하려면 디바이스 그룹 및 템플릿을 선택합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.
후보 구성 저장	현재 후보 구성으로 후보 구성(.snapshot.xml)의 기본 스냅샷을 만들거나 덮어씁니다. 웹 인터페이스의 오른쪽 상단에서 **Config** > **Save Changes**를 선택했을 때와 같은 동작입니다. 특정 관리자의 변경 사항만 저장하려면 후보자 구성 저장을 참조하십시오. (Panorama만 해당) 저장할 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 선택하려면 디바이스 그룹 및 템플릿을 선택합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.
명명된 구성 스냅샷 로드(방화벽) 또는 명명된 Panorama 구성 스냅샷 로드	현재 후보 구성을 다음 중 하나로 덮어씁니다. • 사용자 지정 이름이 지정된 후보 구성 스냅샷(기본 스냅샷 대신). • 불러온 사용자 지정 이름의 실행 구성입니다. • 현재 실행 중인 구성입니다. 구성은 로드 중인 방화벽 또는 Panorama에 있어야 합니다. 구성 이름을 선택한 다음 방화벽 또는 Panorama의 마스터 키인 복호화 키를 입력합니다(디바이스 > 마스터 키 및 진단 참조). 마스터 키는 구성 내의 모든 암호와 개인 키를 복호화하는 데 필요합니다. 불러온 구성을 로드하는 경우 불러온 방화벽 또는 Panorama의 마스터 키를 입력해야 합니다. 로드 작업이 완료되면 구성을 로드한 방화벽 또는 Panorama의 마스터 키가 비밀번호와 개인 키를 다시 암호화합니다. 구성의 모든 규칙에 대해 새 UUID를 생성하려면(예: 다른 방화벽에서 구성을 로드하지만 해당 구성을 로드할 때 고유한 규칙을 유지하려는 경우), 운용 관리자는 모든 규칙에 대한 새 UUID를 생성하기 위해 선택한 명명된 구성에 대한 규칙 **UUID**를 재생성해야 합니다. (Panorama에만 해당) 다음 중에서 선택하여 명명된 구성에서 구성을 부분적으로 로드할 개체, 정책, 디바이스 그룹 또는 템플릿 구성을 지정합니다.

기능	설명
	• 공유 개체 로드 - 모든 디바이스 그룹 및 템플릿 구성과 함께 공유 개체만 로드합니다. • 공유 정책 로드 - 모든 디바이스 그룹 및 템플릿 구성과 함께 공유 정책만 로드합니다. • 디바이스 그룹 및 템플릿 선택 - 로드할 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 지정합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다. • 규칙 **UUID** 유지 - 현재 실행 중인 구성에서 UUID를 유지합니다.
구성 버전 로드(방화벽) 또는 Panorama 구성 버전 로드	현재 후보 구성을 방화벽이나 Panorama에 저장된 실행 중인 구성의 이전 버전으로 덮어씁니다. 구성 이름을 선택한 다음 방화벽 또는 Panorama의 마스터 키인 복호화 키를 입력합니다(디바이스 > 마스터 키 및 진단 참조). 마스터 키는 구성 내의 모든 암호와 개인 키를 복호화하는 데 필요합니다. 로드 작업이 완료되면 마스터 키는 암호와 개인 키를 다시 암호화합니다. (Panorama만 해당) 다음을 선택하여 명명된 구성에서 구성을 부분적으로 로드할 개체, 정책, 디바이스 그룹 또는 템플릿 구성을 지정합니다. • 공유 개체 로드 - 모든 디바이스 그룹 및 템플릿 구성과 함께 공유 개체만 로드합니다. • 공유 정책 로드 - 모든 디바이스 그룹 및 템플릿 구성과 함께 공유 정책만 로드합니다. • 디바이스 그룹 및 템플릿 선택 - 로드할 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 지정합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.
명명된 구성 스냅샷 내보내기	현재 실행 중인 구성, 후보 구성 스냅샷 또는 이전에 불러온 구성(후보 또는 실행 중)을 내보냅니다. 방화벽은 구성을 지정된 이름의 XML 파일로 내보냅니다. 모든 네트워크 위치에 스냅샷을 저장할 수 있습니다. (Panorama만 해당) 내보낼 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 선택하려면 디바이스 그룹 및 템플릿을 선택합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.
구성 버전 내보내기	실행 중인 구성의 버전을 XML 파일로 내보냅니다.

기능	설명
	(Panorama만 해당) 내보낼 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 선택하려면 디바이스 그룹 및 템플릿을 선택합니다. 디바이스 그룹 및 템플릿 관리자는 할당된 액세스 도메인에 지정된 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)만 선택할 수 있습니다.
Panorama 및 디바이스 구성 번들 내보내기 (Panorama만 해당)	구성 백업을 실행하는 Panorama 및 각 관리 방화벽의 최신 버전을 생성하고 내보냅니다. 구성 번들을 만들고 SCP 또는 FTP 서버로 매일 내보내는 프로세스를 자동화하려면 Panorama > 예약된 구성 내보내기를 참조하십시오.
디바이스 구성 번들 내보내기 또는 푸시 (Panorama만 해당)	방화벽을 선택한 다음 Panorama에 저장된 방화벽 구성에 대해 다음 작업 중 하나를 수행하라는 메시지가 표시됩니다. • 구성을 방화벽에 푸시 및 커밋합니다. 이 작업은 방화벽을 정리하고(모든 로컬 구성을 제거함) Panorama에 저장된 방화벽 구성을 푸시합니다. 방화벽 구성을 불러온 후 Panorama를 사용하여 방화벽을 관리할 수 있도록 이 옵션을 사용하여 해당 방화벽을 정리합니다. • 구성을 로드하지 않고 방화벽으로 내보내기를 합니다. 구성을 로드하려면 방화벽 CLI에 액세스하고 구성 모드 명령 **load device-state**를 실행해야 합니다. 이 명령은 푸시 및 커밋 옵션과 동일한 방식으로 방화벽을 정리합니다. • **FW** 마스터 키를 사용하여 관리되는 방화벽에 배포된 마스터 키로 내보낸 디바이스 구성 번들을 암호화합니다. **FW** 마스터 키를 입력한 다음 **FW** 마스터 키를 확인합니다.
디바이스 상태 내보내기 (방화벽만 해당)	방화벽 상태 정보를 번들로 내보냅니다. 실행 중인 구성 외에도 상태 정보에는 Panorama에서 푸시한 디바이스 그룹 및 템플릿 설정이 포함됩니다. 방화벽이 GlobalProtect™ 포털인 경우 번들에는 인증서 정보, 포털이 관리하는 새틀라이트 목록 및 새틀라이트 인증 정보도 포함됩니다. 방화벽이나 포털을 교체하는 경우 상태 번들을 가져와 교체에 대해 내보낸 정보를 복원할 수 있습니다. 방화벽 상태 내보내기를 수동으로 실행하거나 예약된 *XML API* 스크립트를 생성하여 파일을 원격 서버로 내보내야 합니다. 새틀라이트 인증서가 자주 변경되기 때문에 이 작업을 정기적으로 수행해야 합니다. CLI에서 방화벽 상태 파일을 생성하려면 구성 모드에서 **`save device state`** 명령을 실행합니다. 파일 이름은 `device_state_cfg.tgz`이며 `/opt/pancfg/mgmt/device-state`에 저장됩니다. 방화벽 상

기능	설명
	태 파일을 내보내는 작업 명령은 **scp export device-state**입니다(**tftp export device-state**를 사용할 수도 있습니다). XML 또는 REST API 사용에 대한 정보는 PAN-OS 및 Panorama API 가이드 를 참조하십시오.
명명된 구성 스냅샷 가져오기	모든 네트워크 위치에서 실행 중인 구성 또는 후보 구성을 가져옵니다. 찾아보기를 클릭하고 가져올 구성 파일을 선택합니다.
디바이스 상태 가져오기 (방화벽만 해당)	디바이스 상태 내보내기를 선택할 때 방화벽에서 내보낸 상태 정보 번들을 가져옵니다. 실행 중인 구성 외에도 상태 정보에는 Panorama에서 푸시된 디바이스 그룹 및 템플릿 설정이 포함됩니다. 방화벽이 GlobalProtect 포털인 경우 번들에는 인증서 정보, 새틀라이트 목록 및 새틀라이트 인증 정보도 포함됩니다. 방화벽이나 포털을 교체하는 경우 상태 번들을 가져와 교체에 대한 정보를 복원할 수 있습니다.
디바이스 구성을 Panorama로 가져오기 (Panorama만 해당)	방화벽 구성을 Panorama로 가져옵니다. Panorama는 네트워크 및 디바이스 구성을 포함하는 템플릿을 자동으로 생성합니다. 방화벽의 각 가상 시스템(vsys)에 대해 Panorama는 정책 및 개체 구성을 포함할 디바이스 그룹을 자동으로 생성합니다. 디바이스 그룹은 레이어 구조에서 공유 위치보다 한 수준 아래에 있지만 가져오기를 마친 후 다른 상위 디바이스 그룹에 다시 할당할 수 있습니다(Panorama > VMware NSX 참조). *Panorama*의 콘텐츠 버전*(*예*:* 애플리케이션 및 위협 데이터베이스*)*은 구성을 가져올 방화벽의 버전과 같거나 높아야 합니다. 다음 가져오기 옵션을 구성합니다. • 디바이스 - Panorama가 구성을 가져올 방화벽을 선택합니다. 드롭다운에는 Panorama에 연결되어 있고 디바이스 그룹이나 템플릿에 할당되지 않은 방화벽만 포함됩니다. 개별 vsys가 아닌 전체 방화벽만 선택할 수 있습니다. • **FW** 마스터 키 사용 - 관리 방화벽에 배포된 마스터 키를 사용하여 불러온 방화벽 구성을 복호화하려면 이 옵션을 활성화합니다. **FW** 마스터 키를 입력한 다음 **FW** 마스터 키를 확인합니다. 여러 방화벽의 불러온 구성을 복호화하는 경우 방화벽은 모두 동일한 마스터 키를 사용해야 합니다. • 템플릿 이름 - 불러온 디바이스 및 네트워크 설정을 포함할 템플릿의 이름을 입력합니다. Multi-VSYS 방화벽의 경우 필드가 비어 있습니다. 다

기능	설명
	른 방화벽의 경우 기본값은 방화벽 이름입니다. 기존 템플릿의 이름을 사용할 수 없습니다. • 디바이스 그룹 이름 프리픽스(multi-vsys 방화벽만 해당) - 선택적으로 각 디바이스 그룹 이름에 대한 프리픽스로 문자열을 추가합니다. • 디바이스 그룹 이름 - Multi-VSYS 방화벽의 경우 각 디바이스 그룹에는 기본적으로 vsys 이름이 있습니다. 다른 방화벽의 경우 기본값은 방화벽 이름입니다. 기본 이름을 편집할 수 있지만 기존 디바이스 그룹의 이름은 사용할 수 없습니다. • 디바이스의 공유 개체를 **Panorama**의 공유 컨텍스트로 가져오기(기본적으로 활성화됨) - Panorama는 방화벽에서 공유 상태의 개체를 Panorama의 공유 상태로 가져옵니다. *Panorama*는 모든 개체를 여러 가상 시스템 없이 방화벽에서 공유되는 것으로 간주합니다. 이 옵션을 비활성화하면 *Panorama*는 공유 방화벽 개체를 공유 대신 디바이스 그룹에 복사합니다. 이 설정에는 다음과 같은 예외가 있습니다. • 공유 방화벽 개체가 기존 공유 Panorama 개체와 이름 및 값이 동일한 경우 가져오기에서 해당 방화벽 개체를 제외합니다. • 공유 방화벽 개체의 이름이나 값이 공유 Panorama 개체와 다른 경우 Panorama는 방화벽 개체를 각 디바이스 그룹으로 가져옵니다. • 템플릿으로 불러온 구성이 공유 방화벽 개체를 참조하는 경우 Panorama는 이 옵션을 선택하는지의 여부와 관계없이 해당 개체를 공유 상태로 가져옵니다. • 공유 방화벽 개체가 템플릿으로 불러온 구성을 참조하는 경우 Panorama는 이 옵션의 선택 여부와 관계없이 개체를 디바이스 그룹으로 가져옵니다. • 규칙 가져오기 위치 - Panorama에서 정책을 사전 규칙으로 가져올지 사후 규칙으로 가져올지 선택합니다. 선택에 관계없이 Panorama는 기본 보안 규칙(intrazone-default 및 interzone-default)을 사후 규칙 베이스로 가져옵니다. *Panorama*에 가져오는 방화벽 규칙과 이름이 같은 규칙이 있는 경우 *Panorama*는 두 규칙을 모두 표시합니다. 그러나 규칙 이름은 고유해야 합니다. *Panorama*에서 커밋을 수행하기 전에 규칙 중 하나를 삭제하지 않으면 커밋이 실패합니다.

기능	설명
디바이스 작업	
재부팅	방화벽 또는 Panorama를 다시 시작하려면 디바이스를 재부팅하십시오. 방화벽 또는 Panorama는 사용자를 로그아웃하고, 소프트웨어(PAN-OS 또는 Panorama)와 활성 구성을 다시 로드하고, 기존 세션을 닫고 기록하고, 종료를 시작한 관리자의 이름을 보여주는 시스템 로그 항목을 생성합니다. 저장되거나 커밋되지 않은 모든 구성 변경 사항은 손실됩니다(디바이스 > 설정 > 작업 참조). 웹 인터페이스를 사용할 수 없는 경우 다음 작동 *CLI* 명령을 사용하십시오. **### ### ##**
일시 휴업	방화벽 또는 Panorama, **Shutdown Device** 또는 **Shutdown Panorama**를 정상적으로 종료한 다음 메시지가 표시되면 예를 클릭합니다. 저장되거나 커밋되지 않은 구성 변경 사항은 손실됩니다. 모든 관리자가 로그오프되고 다음 프로세스가 발생합니다. • 모든 로그인 세션이 로그오프됩니다. • 인터페이스가 비활성화됩니다. • 모든 시스템 프로세스가 중지됩니다. • 기존 세션이 닫히고 기록됩니다. • 종료를 시작한 관리자 이름을 표시하는 시스템 로그가 생성됩니다. 이 로그 항목을 쓸 수 없으면 경고가 나타나고 시스템이 종료되지 않습니다. • 디스크 드라이브가 완전히 마운트 해제되고 방화벽 또는 Panorama의 전원이 꺼집니다. 방화벽이나 Panorama의 전원을 다시 켜려면 먼저 전원을 뽑았다가 다시 연결해야 합니다. 웹 인터페이스를 사용할 수 없는 경우 다음 *CLI* 명령을 사용하십시오. **### ## ##**
데이터플레인 다시 시작	재부팅하지 않고 방화벽의 데이터 기능을 다시 시작하려면 **Dataplane**을 다시 시작하십시오. 이 옵션은 Panorama 또는 PA-220, PA-800 시리즈 또는 VM 시리즈 방화벽에서는 사용할 수 없습니다.

기능	설명
	웹 인터페이스를 사용할 수 없는 경우 *CLI* 명령 ***request restart dataplane***을 사용합니다. PA-7000 시리즈 방화벽에서 각 NPC에는 데이터플레인이 있으므로 **request ## ## ## ##** 명령을 실행하여 NPC를 다시 시작하여 이 작업을 수행할 수 있습니다.
기타	
사용자 정의 로고	사용자 정의 로고를 사용하여 다음 중 하나를 사용자 정의하십시오. • 로그인 화면 배경 이미지 • 메인 **UI**(웹 인터페이스) 헤더 이미지 • **PDF** 보고서 제목 페이지 이미지. 모니터 > PDF 보고서 > PDF 요약 관리를 참조하세요. • **PDF** 보고서 바닥글 이미지 이미지 파일을 업로드(<image>)여 미리 보거나 이전에 업로드한 이미지를 삭제( )합니다. 기본 로고로 돌아가려면 항목을 제거하고 커밋하십시오. 로그인 화면과 메인 **UI**의 경우 이미지를 표시( )할 수 있습니다. 필요한 경우 방화벽은 이미지에 맞게 자릅니다. PDF 보고서의 경우 방화벽은 자르지 않고 이미지 크기를 자동으로 조정합니다. 모든 경우에 미리보기에 권장 이미지 크기가 표시됩니다. 로고의 최대 이미지 크기는 128KB입니다. 지원되는 파일 형식은 png 및 jpg입니다. 방화벽은 인터레이스된 이미지 파일, 알파 채널이 포함된 이미지 및 gif 파일 형식을 지원하지 않습니다. 이러한 파일은 PDF 보고서 생성을 방해하기 때문입니다. 알파 채널을 제거하거나 사용 중인 그래픽 소프트웨어가 알파 채널 기능이 있는 파일을 저장하지 않는지 확인하려면 이미지를 만든 일러스트레이터에게 문의해야 할 수 있습니다. PDF 보고서 생성에 대한 자세한 내용은 모니터 > PDF 보고서 > PDF 요약 관리를 참조하십시오.

기능	설명
SNMP 설정	SNMP 모니터링을 활성화합니다.
스토리지 파티션 설정(Panorama만 해당)	레거시 모드의 Panorama 가상 어플라이언스에 대한 로그 스토리지 파티션.

SNMP 모니터링 활성화

- 디바이스 > 설정 > 작업

SNMP(Simple Network Management Protocol)는 네트워크의 디바이스를 모니터링하기 위한 표준 프로토콜입니다. 작업을 선택하여 SNMP 관리자가 지원하는 SNMP 버전(SNMPv2c 또는 SNMPv3)을 사용하도록 방화벽을 구성합니다. 방화벽에서 수집한 통계를 해석할 수 있도록 SNMP 관리자에 로드해야 하는 MIB 목록은 지원되는 MIB를 참조하십시오. 방화벽이 네트워크의 SNMP 트랩 대상과 통신할 수 있도록 하는 서버 프로파일을 구성하려면 디바이스 > 서버 프로파일 > SNMP 트랩을 참조하십시오. SNMP MIB는 방화벽이 생성하는 모든 SNMP 트랩을 정의합니다. SNMP 트랩은 고유한 개체 ID(OID)로 이벤트를 식별하고 개별 필드는 변수 바인딩(varbind) 목록으로 정의됩니다. **SNMP** 설정을 클릭하고 다음 설정을 지정하여 SNMP 관리자의 SNMP GET 요청을 허용합니다.

필드	설명
물리적 위치	방화벽의 물리적 위치를 지정합니다. 로그 또는 트랩이 생성되면 이 정보를 통해 알림을 생성한 방화벽을 식별할 수 있습니다(SNMP 관리자에서).
연락	방화벽 유지 관리 책임자의 이름 또는 이메일 주소를 입력합니다. 이 설정은 표준 시스템 정보 MIB에 보고됩니다.
특정 트랩 정의 사용	이 옵션은 기본적으로 선택되어 있습니다. 즉, 방화벽은 이벤트 유형에 따라 각 SNMP 트랩에 대해 고유한 OID를 사용합니다. 이 옵션을 선택 취소하면 모든 트랩이 동일한 OID를 갖습니다.
버전	SNMP 버전 선택: **V2c**(기본값) 또는 **V3**. 선택 항목은 대화 상자에 표시되는 나머지 필드를 제어합니다.
For SNMP V2c	
SNMP 커뮤니티 문자열	SNMP 관리자 및 모니터링되는 디바이스의 SNMP 커뮤니티를 식별하고 SNMP 가져오기(통계 요청) 및 트랩 메시지를 교환할 때 커뮤니티 구성원을 서로 인증하기 위한 암호 역할도 하는 커뮤니티 문자열을 입력하십시오. 문자열은 최대 127자를 포함할 수 있으며 모든 문자를 허용하며 대소문자를 구분합니다.

필드	설명
	기본 커뮤니티 문자열 ***public***을 사용하지 마십시오. *SNMP* 메시지에는 일반 텍스트로 된 커뮤니티 문자열이 포함되어 있으므로 커뮤니티 구성원*(*관리자 액세스*)*을 정의할 때 네트워크의 보안 요구 사항을 고려하십시오.
SNMP V3의 경우	
이름 / 보기	SNMP 관리자의 사용자에게 하나 이상의 보기 그룹을 할당하여 사용자가 방화벽에서 가져올 수 있는 MIB 개체(통계)를 제어할 수 있습니다. 각 보기는 쌍을 이루는 OID와 비트 단위 마스크입니다. OID는 MIB를 지정하고 마스크(16진수 형식)는 해당 MIB 내부(일치 포함) 또는 외부(일치 제외)에 액세스할 수 있는 개체를 지정합니다. 예를 들어, **OID**가 1.3.6.1이고 일치 옵션이 포함으로 설정되고 마스크가 0xf0이면 사용자가 요청하는 개체에는 1.3.6.1의 처음 4개 노드(f = 1111)와 일치하는 OID가 있어야 합니다. 개체는 나머지 노드와 일치할 필요가 없습니다. 이 예에서 1.3.6.1.2는 마스크와 일치하고 1.4.6.1.2는 일치하지 않습니다. 각 보기 그룹에 대해 추가를 클릭하고 그룹의 이름을 입력한 후 그룹에 추가하는 각 보기에 대해 다음을 구성합니다. • 보기 - 보기의 이름을 지정합니다. 이름은 영숫자, 마침표, 밑줄 또는 하이픈으로 최대 31자를 사용할 수 있습니다. • **OID** - MIB의 OID를 지정합니다. • 옵션 - MIB에 적용할 일치 논리를 선택합니다. • 마스크 - 16진수 형식으로 마스크를 지정합니다. 모든 관리 정보에 대한 액세스를 제공하려면 최상위 ***OID*** *1.3.6.1*을 사용하고 마스크를 *0xf0*으로 설정하고 일치 옵션을 포함하도록 설정합니다.
사용자	SNMP 사용자 계정은 방화벽이 트랩을 포워딩하고 SNMP 관리자가 방화벽 통계를 얻을 때 인증, 개인 정보 보호 및 액세스 제어를 제공합니다. 각 사용자에 대해 추가를 클릭하고 다음 설정을 구성합니다. • 사용자 - SNMP 사용자 계정을 식별하기 위한 사용자명을 지정합니다. 방화벽에서 구성한 사용자명은 SNMP 관리자에 구성된 사용자명과 일치해야 합니다. 사용자명은 최대 31자까지 가능합니다. • 보기 - 사용자에게 보기 그룹을 할당합니다.

필드	설명

	• 인증 암호 - 사용자의 인증 암호를 지정합니다. 방화벽은 트랩을 포워딩하고 통계 요청에 응답할 때 암호를 사용하여 SNMP 관리자를 인증합니다. 암호는 8-256자여야 하며 모든 문자가 허용됩니다.
	• 개인 암호 - 사용자의 개인 암호를 지정합니다. 암호는 8-256자여야 하며 모든 문자가 허용됩니다.
	• 인증 프로토콜 - 방화벽은 SHA(Secure Hash Algorithm)를 사용하여 암호를 해시합니다.
	  • **SHA-1**, **SHA-224**, **SHA-256**, **SHA-384**, **SHA-512**
	• 개인 정보 보호 프로토콜 - 방화벽은 암호 및 AES(Advanced Encryption Standard) 알고리즘을 사용하여 SNMP 트랩 및 통계 요청에 대한 응답을 암호화합니다.
	  • **AES-128**, **AES-192**, **AES-256**

디바이스 > 설정 > HSM

HSM(하드웨어 보안 모듈)을 구성하고, 작업을 수행하고, HSM 상태를 보려면 **Device** > **Setup** > **HSM**을 선택합니다.

무엇을 찾고 계신가요?	참조:
HSM(Hardware Security Module)의 목적은 무엇이며 자세한 구성 절차는 어디에서 찾을 수 있습니까?	하드웨어 보안 모듈을 사용한 보안 키
구성:	하드웨어 보안 모듈 공급자 설정
	HSM 인증
하드웨어 보안 작업 수행	하드웨어 보안 작업
HSM 상태를 보려면 어떻게 해야 합니까?	하드웨어 보안 모듈 공급자 구성 및 상태
	하드웨어 보안 모듈 상태

하드웨어 보안 모듈 공급자 설정

방화벽에서 HSM(하드웨어 보안 모듈)을 구성하려면 하드웨어 보안 모듈 공급자 설정을 편집합니다.

하드웨어 보안 모듈 공급자 설정	설명
공급자 구성됨	HSM 공급자를 선택합니다. • 없음(기본값) - 방화벽이 HSM에 연결하지 않습니다. • **SafeNet Network HSM** • **nCipher nShield Connect** *HSM* 서버 버전은 방화벽의 HSM 클라이언트 버전 과 호환되어야 합니다.

하드웨어 보안 모듈 공급자 설정	설명
모듈 이름	HSM의 모듈 이름을 추가합니다. 최대 31자 길이의 ASCII 문자열이 될 수 있습니다. 독립 또는 고가용성 SafeNet HSM 구성을 구성하는 경우 최대 16개의 모듈 이름을 추가하십시오.
서버 주소	구성 중인 HSM 모듈의 IPv4 주소를 지정합니다.
고가용성 (SafeNet 네트워크만 해당)	(선택 사항) 고가용성 구성에서 SafeNet HSM 모듈을 구성하는 경우 이 옵션을 선택합니다. 각 HSM 모듈의 모듈 이름과 서버 주소를 구성해야 합니다.
자동 복구 재시도 (SafeNet 네트워크만 해당)	방화벽이 HSM HA 구성에서 다른 HSM으로 페일오버하기 전에 HSM에 대한 연결 복구를 시도하는 횟수를 지정합니다(범위는 0-500, 기본값은 0).
고가용성 그룹 이름 (SafeNet 네트워크만 해당)	HSM HA 그룹에 사용할 그룹 이름을 지정합니다. 이 이름은 방화벽에서 내부적으로 사용됩니다. 최대 31자 길이의 ASCII 문자열일 수 있습니다.
파일 시스템 주소 제거 (nCipher nShield Connect만 해당)	nShield Connect HSM 구성에 사용되는 원격 파일 시스템의 IPv4 주소를 구성합니다.

HSM 인증

하드웨어 보안 모듈 설정을 선택한 후 다음 설정을 구성하여 HSM에 대한 방화벽을 인증합니다.

HSM 모듈 인증	
서버 이름	드롭다운에서 HSM 서버 이름을 선택한 다음 자동 또는 수동으로 생성된 인증서를 사용하여 인증하고 신뢰를 설정할지의 여부를 선택합니다. • 자동 • 수동 수동을 선택하는 경우 수동으로 생성된 HSM 서버 인증서를 가져와 설치해야 합니다. HSM 서버에 설치할 HSM 클라이언트 인증서를 내보냅니다.
관리자 비밀번호	HSM에 대한 방화벽을 인증하려면 HSM의 관리자 암호를 입력합니다.

하드웨어 보안 작업

HSM(Hardware Security Module) 또는 HSM에 연결된 방화벽에서 작업을 수행하려면 **Device** > **Setup** > **HSM**을 선택한 다음 다음 하드웨어 보안 작업 중 하나를 선택합니다.

하드웨어 보안 작업	
하드웨어 보안 모듈 설정	HSM으로 인증하도록 방화벽을 구성합니다.
자세한 정보 표시	HSM 서버, HSM 고가용성 상태 및 HSM 하드웨어에 대한 정보를 표시합니다.
원격 파일 시스템과 동기화(nCipher nShield Connect만 해당)	nShield Connect 원격 파일 시스템의 키 데이터를 방화벽으로 동기화합니다.
구성 재설정	방화벽에 대한 모든 HSM 연결을 제거합니다. HSM 구성을 재설정한 후 모든 인증 절차를 반복해야 합니다.
HSM 클라이언트 버전 선택(SafeNet 네트워크만 해당)	HSM 클라이언트(방화벽)에서 실행되는 소프트웨어 버전을 선택할 수 있습니다. HSM 클라이언트 버전은 HSM 서버 버전과 호환되어야 합니다. 클라이언트-서버 버전 호환성 매트릭스는 HSM 공급자 설명서를 참조하십시오.

하드웨어 보안 모듈 공급자 구성 및 상태

Hardware Security Module Provider 섹션은 HSM 구성 설정과 HSM의 연결 상태를 보여줍니다.

하드웨어 보안 모듈 공급자 상태	
공급자 구성됨	방화벽에 구성된 HSM 공급자를 선택합니다. • 없음 • **SafeNet Network HSM** • **nCipher nShield Connect**
고가용성	(SafeNet 네트워크만 해당) 체크하면 HSM 고가용성이 구성됩니다.
고가용성 그룹 이름	(SafeNet 네트워크만 해당) HSM 고가용성을 위해 방화벽에 구성된 그룹 이름입니다.
원격 파일 시스템 주소	(nShield Connect만 해당) 원격 파일 시스템의 주소입니다.

하드웨어 보안 모듈 공급자 상태	
방화벽 소스 주소	HSM 서비스에 사용되는 포트의 주소입니다. 기본적으로 이것은 관리 포트 주소입니다. 그러나 **Device** > **Setup** > **Services**의 서비스 경로 구성을 통해 다른 포트로 지정할 수 있습니다.
방화벽의 HSM 클라이언트 버전	설치된 HSM 클라이언트 버전을 표시합니다.
HSM으로 보호되는 마스터 키	선택하면 마스터 키가 HSM에서 보호됩니다.
상태	방화벽이 HSM에 연결 및 인증된 경우 녹색으로 표시되고 방화벽이 인증되지 않았거나 HSM에 대한 네트워크 연결이 중단된 경우 빨간색이 표시됩니다. HSM 연결에 대한 자세한 내용은 하드웨어 보안 모듈 상태에서도 확인할 수 있습니다.

하드웨어 보안 모듈 상태

하드웨어 보안 모듈 상태에는 성공적으로 인증된 HSM에 대한 다음 정보가 포함됩니다. 디스플레이는 구성된 HSM 공급자(SafeNet 또는 nCipher)에 따라 다릅니다.

하드웨어 보안 모듈 상태	
SafeNet Network HSM	• 일련번호 - HSM 파티션이 성공적으로 인증된 경우 HSM 파티션의 일련번호가 표시됩니다. • 파티션 - 방화벽에 할당된 HSM의 파티션 이름입니다. • 모듈 상태 - HSM 연결의 현재 작동 상태입니다. 이 테이블에 HSM이 표시되는 경우 이 필드는 인증됨을 표시합니다.
nCipher nShield Connect HSM	• 이름 - HSM의 서버 이름입니다. • **IP** 주소 - 방화벽에 할당된 HSM의 IP 주소입니다. • 모듈 상태 - HSM 연결의 현재 작동 상태입니다. 이 설정은 방화벽이 HSM에 대해 성공적으로 인증된 경우 인증됨을 표시하고 인증이 실패한 경우 인증되지 않음을 표시합니다.

디바이스 > 설정 > 서비스

다음 항목에서는 방화벽의 전역 및 가상 시스템 서비스 설정에 대해 설명합니다.

- 글로벌 및 가상 시스템에 대한 서비스 구성
- 글로벌 서비스 설정
- 서비스 경로 구성을 위한 IPv4 및 IPv6 지원
- 목적지 서비스 경로

글로벌 및 가상 시스템에 대한 서비스 구성

여러 가상 시스템이 활성화된 방화벽에서 서비스를 선택하여 방화벽 또는 해당 가상 시스템이 각각 효율적으로 작동하는 데 사용하는 서비스를 설정하는 전역 및 가상 시스템 탭을 표시합니다. (방화벽이 단일 가상 시스템이거나 여러 가상 시스템이 비활성화된 경우 가상 시스템 탭이 표시되지 않습니다.)

전체 방화벽에 대한 서비스를 설정하려면 전역을 선택합니다. 이러한 설정은 서비스에 대한 사용자 정의 설정이 없는 가상 시스템의 기본값으로도 사용됩니다.

- 서비스를 편집하여 DNS 서버, 업데이트 서버 및 프록시 서버의 대상 IP 주소를 정의합니다. 전용 **NTP** 탭을 사용하여 네트워크 시간 프로토콜 설정을 구성합니다. 사용 가능한 서비스 옵션에 대한 필드 설명은 표 12를 참조하십시오.
- 서비스 기능에서 서비스 경로 구성을 클릭하여 방화벽이 DNS, 이메일, LDAP, RADIUS, syslog 등과 같은 서비스에 대해 다른 서버/디바이스와 통신하는 방법을 지정합니다. 전역 서비스 경로를 구성하는 방법에는 두 가지가 있습니다.
  - 모두에 대해 관리 인터페이스 사용 옵션은 관리 인터페이스(MGT)를 통해 외부 서버와의 모든 방화벽 서비스 통신을 강제 실행합니다. 이 옵션을 선택하면 방화벽과 서비스를 제공하는 서버/디바이스 간의 통신을 허용하도록 MGT 인터페이스를 구성해야 합니다. MGT 인터페이스를 구성하려면 디바이스 > 설정 > 관리를 선택한 다음 설정을 편집합니다.
  - 사용자 지정 옵션을 사용하면 서비스가 응답에서 대상 인터페이스 및 대상 IP 주소로 사용할 특정 소스 인터페이스 및 IP 주소를 구성하여 서비스 통신을 세부적으로 제어할 수 있습니다. (예를 들어, 방화벽과 이메일 서버 간의 모든 이메일 통신에 대해 특정 소스 IP/인터페이스를 구성하고 Palo Alto Networks Services에 대해 다른 소스 IP/인터페이스를 사용할 수 있습니다.) 동일한 설정을 갖도록 사용자 지정할 서비스를 하나 이상 선택한 다음 선택한 서비스 경로 설정을 클릭합니다. 서비스는 글로벌 방화벽 또는 가상 시스템에 대해 서비스를 구성할 수 있는지의 여부와 서비스가 IPv4 및/또는 IPv6 소스 주소를 지원하는지의 여부를 나타내는 표 13에 나열되어 있습니다.

대상 탭은 사용자 정의할 수 있는 또 다른 글로벌 서비스 경로 기능입니다. 이 탭은 서비스 경로 구성 창에 표시되며 대상 서비스 경로에 설명되어 있습니다.

가상 시스템 탭을 사용하여 단일 가상 시스템에 대한 서비스 경로를 지정합니다. 위치(가상 시스템)를 선택한 다음 서비스 경로 구성을 클릭합니다. 전역 서비스 경로 구성 상속 또는 가상 시스템에 대한 서비스 경로 사용자 지정을 선택합니다. 설정을 사용자 지정하도록 선택한 경우 **IPv4** 또는 **IPv6**을 선택합니다. 동일한

설정을 갖도록 사용자 지정할 서비스를 하나 이상 선택한 다음 선택한 서비스 경로 설정을 클릭합니다. 사용자 정의할 수 있는 서비스는 표 13을 참조하십시오.

공유 및 특정 가상 시스템 간의 DNS 쿼리를 제어하고 리디렉션하기 위해 DNS 프록시와 DNS 서버 프로파일을 사용할 수 있습니다.

글로벌 서비스 설정

- 디바이스 > 설정 > 서비스

공유 및 특정 가상 시스템 간의 DNS 쿼리를 제어하고 리디렉션하기 위해 DNS 프록시와 DNS 서버 프로파일을 사용할 수 있습니다.

글로벌 서비스 설정	설명
서비스	
서버 업데이트	Palo Alto Networks에서 업데이트를 다운로드할 서버의 IP 주소 또는 호스트 이름을 나타냅니다. 현재 값은 **updates.paloaltonetworks.com**입니다. 기술 지원에서 지시하지 않는 한 이 설정을 변경하지 마십시오.
업데이트 서버 ID 확인	이 옵션을 활성화하면 방화벽 또는 Panorama가 소프트웨어 또는 콘텐츠 패키지를 다운로드하는 서버에 신뢰할 수 있는 기관에서 서명한 SSL 인증서가 있는지 확인합니다. 이렇게 하면 방화벽 또는 Panorama 서버와 업데이트 서버 간의 통신에 대한 보안 수준이 추가됩니다. 업데이트 서버 *ID*를 확인하여 서버에 신뢰할 수 있는 기관에서 서명한 *SSL* 인증서가 있는지 확인합니다.
DNS 설정	FQDN 주소 개체, 로깅 및 방화벽 관리를 지원하기 위해 방화벽이 시작하는 모든 DNS 쿼리에 대해 DNS 서비스 유형(서버 또는 **DNS** 프록시 개체)을 선택합니다. 옵션에는 다음이 포함됩니다. • 도메인 이름 확인을 제공하는 기본 및 보조 DNS 서버. • DNS 서버를 구성하는 대신 방화벽에 구성된 DNS 프록시입니다. DNS 프록시를 활성화하는 경우 캐시 및 **EDNS** 캐시 응답(**Network** > **DNS Proxy** > **Advanced**)을 활성화해야 합니다.
기본 DNS 서버	방화벽에서 DNS 쿼리에 대한 기본 DNS 서버의 IP 주소를 입력합니다. 예를 들어 업데이트 서버를 찾거나 로그의 DNS 항목을 확인하거나 FDQN 기반 주소 개체를 확인합니다.

글로벌 서비스 설정	설명
보조 DNS 서버	(선택 사항) 기본 서버를 사용할 수 없는 경우 사용할 보조 DNS 서버의 IP 주소를 입력합니다.
최소 FQDN 새로 고침 시간(초)	방화벽이 DNS에서 수신하는 FQDN을 새로 고치는 속도에 대한 제한을 설정합니다. 방화벽은 TTL이 이 최소 **FQDN** 새로 고침 시간(초)보다 크거나 같으면 FQDN의 TTL을 기반으로 FQDN을 새로 고칩니다. TTL이 이 최소 FQDN 새로 고침 시간보다 짧은 경우 방화벽은 이 최소 FQDN 새로 고침 시간을 기반으로 FQDN을 새로 고칩니다(즉, 방화벽이 이 설정보다 빠른 TTL을 인정하지 않음). 방화벽이 FQDN을 확인하는 DNS 서버 또는 DNS 프록시 개체로부터 DNS 응답을 받으면 타이머가 시작됩니다(범위는 0 ~ 14,400, 기본값은 30). 0으로 설정하면 방화벽이 DNS의 TTL 값을 기반으로 FQDN을 새로 고치고 최소 FQDN 새로 고침 시간을 적용하지 않습니다. *DNS*의 *FQDN*에 대한 *TTL*이 짧지만 *FQDN* 확인이 *TTL* 시간 프레임만큼 자주 변경되지 않으므로 더 빠른 새로 고침이 필요하지 않은 경우 불필요한 *FQDN* 새로 고침 시도를 피하기 위해 최소 *FQDN* 새로 고침 시간을 설정해야 합니다.
FQDN의 오래된 항목 타임아웃(분)	FQDN이 새로 고쳐지지 않을 때(범위는 0 ~ 10,080, 기본값은 1,440) 네트워크 오류 또는 DNS 서버에 연결할 수 없는 경우 방화벽이 오래된 FQDN을 계속 사용하는 시간(분)을 지정합니다. 값 0은 방화벽이 오래된 항목을 계속 사용하지 않음을 의미합니다. 상태 타임아웃이 끝날 때 DNS 서버에 여전히 연결할 수 없으면 FQDN 항목이 확인되지 않습니다(오래된 항목 이슈가 제거됨). ***FQDN Stale Entry Timeout*** 값이 잘못된 트래픽 포워딩(보안 위험을 초래함)을 허용하지 않을 만큼 충분히 짧고 계획되지 않은 네트워크 중단을 일으키지 않고 트래픽 연속성을 허용할 만큼 충분히 긴지 확인합니다.
프록시 서버 섹션	
서버	방화벽이 Palo Alto Networks 업데이트 서비스에 도달하기 위해 프록시 서버를 사용해야 하는 경우 프록시 서버의 IP 주소 또는 호스트 이름을 입력하십시오.
포트	프록시 서버의 포트를 입력합니다.
사용자	프록시 서버에 액세스할 때 관리자가 입력할 사용자명을 입력합니다.

글로벌 서비스 설정	설명
비밀번호/비밀번호 확인	프록시 서버에 액세스할 때 관리자가 입력할 비밀번호를 입력하고 확인합니다.
프록시를 사용하여 Cortex Data Lake에 로그 보내기	프록시 서버를 통해 Cortex Data Lake에 로그를 보내도록 방화벽을 활성화합니다.
NTP	
NTP 서버 주소	방화벽에서 시계를 동기화하는 데 사용할 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다. 선택적으로 기본 서버를 사용할 수 없는 경우 두 번째 NTP 서버의 IP 주소 또는 호스트 이름을 입력하여 방화벽의 시계를 동기화할 수 있습니다. *NTP* 서버가 모든 네트워크 방화벽 시계를 동기화된 상태로 유지하면 예약된 작업이 예상대로 실행되고 타임스탬프는 여러 디바이스와 관련된 문제의 근본 원인을 식별하는 데 도움이 될 수 있습니다. 기본 *NTP* 서버에 연결할 수 없는 경우 기본 및 보조 *NTP* 서버를 구성합니다.

인증 유형	방화벽이 NTP 서버의 시간 업데이트를 인증하도록 설정할 수 있습니다. 각 NTP 서버에 대해 방화벽이 사용할 인증 유형을 선택합니다.
	• 없음(기본값) - NTP 인증을 비활성화하려면 이 옵션을 선택합니다.
	• 대칭 키 - 방화벽이 대칭 키 교환(공유 암호)을 사용하여 NTP 서버의 시간 업데이트를 인증하려면 이 옵션을 선택합니다. 대칭 키를 선택하는 경우 다음 값을 지정하여 계속하십시오.
	  • 키 **ID** - 키 ID(1–65534)를 입력합니다.
	  • 알고리즘 - NTP 인증에 사용할 MD5 또는 SHA1 알고리즘을 선택합니다.
	  • 인증 키/인증 키 확인 - 인증 알고리즘에 대한 인증 키를 입력하고 확인합니다.
	• 자동 키 - 방화벽이 자동 키(공개 키 암호화)를 사용하여 NTP 서버의 시간 업데이트를 인증하려면 이 옵션을 선택합니다.
	
	NTP 서버가 클라이언트를 승인하고 동기화된 업데이트를 제공하도록 *NTP* 서버 인증을 활성화합니다.

서비스 경로 구성을 위한 IPv4 및 IPv6 지원

다음 표는 글로벌 및 가상 시스템에서 서비스 경로 구성에 대한 IPv4 및 IPv6 지원을 보여줍니다.

서비스 경로 구성 설정	글로벌		가상 시스템	
	IPv4	**IPv6**	**IPv4**	**IPv6**
AutoFocus - AutoFocus™ 서버.	✓	—	—	—
CRL 상태 - CRL(인증서 해지 목록) 서버입니다.	✓	✓	—	—
데이터 서비스 - 방화벽 데이터플레인에서 Palo Alto Networks 클라우드 서비스로 데이터를 보냅니다. 더 빠른 데이터 전송을 위해 최적화되고 데이터 손실을 방지합니다. IoT 보안, Enterprise DLP 및 SaaS 보안에 필요합니다.	✓	✓	✓	✓
DDNS - 동적 DNS 서비스.	✓	✓	✓	✓
Panorama 푸시 업데이트 - Panorama™에서 배포된 콘텐츠 및 소프트웨어 업데이트.	✓	✓	—	—
DNS - 도메인 이름 시스템 서버. *가상 시스템의 경우 DNS는 DNS 서버 프로파일에서 수행됩니다.	✓	✓	✓ *	✓ *
외부 동적 목록 - 외부 동적 목록에 대한 업데이트입니다.	✓	✓	—	—
이메일 - 이메일 서버.	✓	✓	✓	✓
HSM - 하드웨어 보안 모듈 서버.	✓	—	—	✓
HTTP - HTTP 포워딩.	✓	✓	✓	✓
Kerberos - Kerberos 인증 서버입니다.	✓	—	✓	✓
LDAP—Lightweight Directory Access Protocol 서버.	✓	✓	✓	✓

서비스 경로 구성 설정	글로벌		가상 시스템	
	IPv4	**IPv6**	**IPv4**	**IPv6**
MDM - 모바일 디바이스 관리 서버.	✓	✓	—	—
다중 요소 인증 - 다중 요소 인증(MFA) 서버입니다.	✓	✓	✓	✓
NetFlow - 네트워크 트래픽 통계를 수집하기 위한 NetFlow 수집기입니다.	✓	✓	✓	✓
NTP - 네트워크 시간 프로토콜 서버.	✓	✓	—	—
Palo Alto Networks 서비스 - Palo Alto Networks® 및 공용 WildFire® 서버의 업데이트. 이는 10.0 이전 원격 측정 데이터를 Palo Alto Networks로 포워딩하기 위한 서비스 경로이기도 합니다. (현재 원격 측정 지원은 데이터를 Cortex Data Lake로 포워딩합니다. 이 경우에는 이 서비스 경로를 사용하지 않습니다.)	✓	—	—	—
Panorama - Panorama 관리 서버.	✓	✓	—	—
Panorama 로그 포워딩(PA-5200 시리즈 방화벽만 해당) - 방화벽에서 로그 수집기로의 로그 포워딩.	✓	✓	—	—
프록시 - 방화벽에 대한 프록시 역할을 하는 서버입니다.	✓	✓	—	—
RADIUS - 원격 인증 전화 접속 사용자 서비스 서버.	✓	✓	✓	✓
SCEP - 클라이언트 인증서를 요청하고 배포하기 위한 단순 인증서 등록 프로토콜입니다.	✓	✓	✓	—
SNMP 트랩 - 단순 네트워크 관리 프로토콜 트랩 서버.	✓	—	✓	—
Syslog - 시스템 메시지 로깅을 위한 서버입니다.	✓	✓	✓	✓

서비스 경로 구성 설정	글로벌		가상 시스템	
	IPv4	**IPv6**	**IPv4**	**IPv6**
TACACS+ - AAA(인증, 권한 부여 및 계정) 서비스를 위한 TACACS+(터미널 액세스 컨트롤러 액세스 제어 시스템 플러스) 서버입니다.	✓	✓	✓	✓
UID 에이전트 - User-ID 에이전트 서버.	✓	✓	—	✓
URL 업데이트 - URL(Uniform Resource Locator)이 서버를 업데이트합니다.	✓	✓	—	—
VM 모니터 - 디바이스 > VM 정보 소스를 활성화한 경우 가상 머신 정보를 모니터링합니다. 가상 머신을 모니터링하는 공용 클라우드 배포의 *VM* 시리즈 방화벽은 *MGT* 인터페이스를 사용해야 합니다. 데이터플레인 인터페이스를 서비스 경로로 사용할 수 없습니다.	✓	✓	✓	✓
WildFire Private—사설 Palo Alto Networks WildFire 서버.	✓	—	—	—

전역 서비스 경로를 사용자 지정할 때 서비스 경로 구성을 선택한 다음 **IPv4** 또는 **IPv6** 탭에서 사용 가능한 서비스 목록에서 서비스를 선택합니다. 여러 서비스를 선택한 다음 선택한 서비스 경로를 설정하여 한 번에 여러 서비스 경로를 구성할 수도 있습니다. 소스 주소 드롭다운에서 선택을 제한하려면 소스 인터페이스를 선택한 다음 소스 주소(해당 인터페이스에서)를 선택합니다. 모두로 설정된 소스 인터페이스를 사용하면 사용 가능한 인터페이스에서 소스 주소를 선택할 수 있습니다. 소스 주소는 선택한 인터페이스에 할당된 IPv4 또는 IPv6 주소를 표시하며 선택한 IP 주소는 서비스 트래픽의 소스가 됩니다. 방화벽이 서비스 경로에 대한 관리 인터페이스를 사용하도록 하려면 기본값 사용을 선택할 수 있습니다. 그러나 패킷 대상 IP 주소가 구성된 대상 IP 주소와 일치하는 경우 소스 IP 주소는 대상에 대해 구성된 소스 주소로 설정됩니다. 각 서비스를 구성할 때 목적지가 설정되기 때문에 목적지 주소를 정의할 필요가 없습니다. 예를 들어, DNS 서버(**Device** > **Setup** > **Services**)를 정의할 때 DNS 쿼리의 대상을 설정합니다. 서비스에 대해 IPv4 및 IPv6 주소를 모두 지정할 수 있습니다.

전역 서비스 경로를 사용자 지정하는 다른 방법은 서비스 경로 구성을 선택한 다음 대상을 선택하는 것입니다. 들어오는 패킷을 비교할 대상 IP 주소를 지정합니다. 패킷 대상 주소가 구성된 대상 IP 주소와 일치하는 경우 소스 IP 주소는 대상에 대해 구성된 소스 주소로 설정됩니다. 소스 주소 드롭다운에서 선택을 제한하려면 소스 인터페이스를 선택한 다음 소스 주소(해당 인터페이스에서)를 선택합니다. 모두로 설정된 소

스 인터페이스를 사용하면 사용 가능한 모든 인터페이스에서 소스 주소를 선택할 수 있습니다. **MGT** 소스 인터페이스는 방화벽이 서비스 경로에 대한 관리 인터페이스를 사용하도록 합니다.

가상 시스템에 대한 서비스 경로를 구성할 때 전역 서비스 경로 구성 상속을 선택하면 가상 시스템의 모든 서비스가 전역 서비스 경로 설정을 상속합니다. 대신 사용자 지정을 선택한 다음 **IPv4** 또는 **IPv6**을 선택한 다음 서비스를 선택할 수 있습니다. 여러 서비스를 선택한 다음 선택한 서비스 경로를 설정할 수도 있습니다. 소스 인터페이스에는 다음 세 가지 선택 사항이 있습니다.

- 전역 설정 상속 - 선택한 서비스가 해당 서비스에 대한 전역 설정을 상속합니다.
- **Any**—사용 가능한 모든 인터페이스(특정 가상 시스템의 인터페이스)에서 소스 주소를 선택할 수 있습니다.
- 드롭다운의 인터페이스 - 소스 주소의 드롭다운을 이 인터페이스의 IP 주소로 제한합니다.

소스 주소의 경우 드롭다운에서 주소를 선택합니다. 선택한 서비스에 대해 서버 응답이 이 소스 주소로 전송됩니다.

대상 서비스 경로

- 디바이스 > 설정 > 서비스 > 글로벌

전역 탭에서 서비스 경로 구성을 클릭한 다음 사용자 지정을 클릭하면 대상 탭이 나타납니다. 대상 서비스 경로는 가상 시스템 탭이 아닌 전역 탭에서만 사용할 수 있으므로 개별 가상 시스템에 대한 서비스 경로는 해당 가상 시스템과 연결되지 않은 경로 테이블 항목을 재정의할 수 없습니다.

대상 서비스 경로를 사용하여 서비스 사용자 지정 목록에서 지원되지 않는 서비스의 사용자 지정 리디렉션을 추가할 수 있습니다. 대상 서비스 경로는 FIB(포워딩 정보 기반) 경로 테이블을 재정의하도록 라우팅을 설정하는 방법입니다. 대상 서비스 경로의 모든 설정은 경로 테이블 항목을 재정의합니다. 서비스와 관련되거나 관련이 없을 수 있습니다.

대상 탭은 다음 사용 사례를 위한 것입니다.

- 서비스에 애플리케이션 서비스 경로가 없는 경우.
- 단일 가상 시스템 내에서 여러 가상 라우터를 사용하거나 가상 라우터와 관리 포트의 조합을 사용하려는 경우.

대상 서비스 경로 설정	설명
데스티네이션	대상 IP 주소를 입력합니다. 목적지 주소가 이 주소와 일치하는 수신 패킷은 이 서비스 경로에 대해 지정한 소스 주소를 소스로 사용합니다.
소스 인터페이스	소스 주소에 대한 드롭다운을 제한하려면 소스 인터페이스를 선택하십시오. 모두를 선택하면 모든 인터페이스의 모든 IP 주소를 소스 주소 드롭다운에서 사용할 수 있습니다. **MGT**를 선택하면 방화벽이 서비스 경로에 대해 MGT 인터페이스를 사용합니다.

대상 서비스 경로 설정	설명
소스 주소	서비스 경로에 대한 소스 주소를 선택하십시오. 이 주소는 목적지에서 돌아오는 패킷에 사용됩니다. 대상 주소에 대한 서브넷을 입력할 필요가 없습니다.

디바이스 > 설정 > 인터페이스

이 페이지를 사용하여 모든 방화벽 모델의 관리(MGT) 인터페이스와 PA-5200 시리즈 방화벽의 보조 인터페이스(AUX-1 및 AUX-2)에 대한 연결 설정, 허용된 서비스 및 관리 액세스를 구성할 수 있습니다.

Palo Alto Networks는 항상 모든 인터페이스에 대해 IP 주소와 넷마스크(IPv4의 경우) 또는 프리픽스 길이(IPv6의 경우) 및 기본 게이트웨이를 지정할 것을 권장합니다. MGT 인터페이스(예: 기본 게이트웨이)에 대해 이러한 설정을 생략하면 향후 구성 변경을 위해 콘솔 포트를 통해서만 방화벽에 액세스할 수 있습니다.

M-500 어플라이언스 또는 *Panorama* 가상 어플라이언스에서 *MGT* 인터페이스를 구성하려면 Panorama > 설정 > 인터페이스를 참조하십시오.

방화벽 관리를 위해 *MGT* 인터페이스 대신 루프백 인터페이스를 사용할 수 있습니다*(*네트워크 > 인터페이스 > 루프백*)*.

항목	설명

유형
 	
(MGT 인터페이스만 해당)
	하나를 고릅니다.
	• 정적 - 이 표에서 자세히 설명하는 IPv4 또는 IPv6 주소(또는 둘 다)와 기본 게이트웨이를 수동으로 입력해야 합니다.
	• **DHCP** 클라이언트 - 방화벽이 DHCP 서버를 찾기 위해 DHCP Discover 또는 Request 메시지를 보낼 수 있도록 MGT 인터페이스를 DHCP 클라이언트로 구성합니다. 서버는 MGT 인터페이스에 대한 IP 주소(IPv4), 넷마스크(IPv4) 및 기본 게이트웨이를 제공하여 응답합니다. MGT 인터페이스의 DHCP는 VM 시리즈 방화벽에 대해 기본적으로 꺼져 있습니다(AWS 및 Azure의 VM 시리즈 방화벽 제외). **DHCP** 클라이언트를 선택하는 경우 선택적으로 다음 클라이언트 옵션 중 하나 또는 둘 다를 선택합니다.
	  • 호스트 이름 보내기 - MGT 인터페이스가 DHCP 옵션 12의 일부로 DHCP 서버에 호스트 이름을 보내도록 합니다.
	  • 클라이언트 **ID** 보내기 - MGT 인터페이스가 DHCP 옵션 61의 일부로 클라이언트 식별자를 보내도록 합니다.
	DHCP 클라이언트를 선택하는 경우 선택적으로 **DHCP** 클라이언트 런타임 정보 표시를 클릭하여 동적 IP 인터페이스 상태를 봅니다.
	• 인터페이스 - MGT 인터페이스를 나타냅니다.
	• IP 주소 - MGT 인터페이스의 IP 주소입니다.
	• 넷마스크 - 어떤 비트가 네트워크 또는 서브네트워크이고 어떤 비트가 호스트인지를 나타내는 IP 주소의 서브넷 마스크입니다.
	• 게이트웨이 - MGT 인터페이스에서 나가는 트래픽의 기본 게이트웨이입니다.

항목	설명
	• 기본/보조 NTP - MGT 인터페이스를 제공하는 최대 2개의 NTP 서버의 IP 주소입니다. DHCP 서버가 NTP 서버 주소를 반환하면 방화벽은 NTP 서버 주소를 수동으로 구성하지 않은 경우에만 해당 주소를 고려합니다. NTP 서버 주소를 수동으로 구성한 경우 방화벽은 DHCP 서버의 주소로 주소를 덮어쓰지 않습니다. • 리스 시간 - DHCP IP 주소가 할당된 일, 시간, 분, 초 수입니다. • 만료 시간 - 년/월/일, 시간/분/초 및 시간대, DHCP 리스가 만료되는 시기를 나타냅니다. • DHCP 서버 - MGT 인터페이스 DHCP 클라이언트에 응답하는 DHCP 서버의 IP 주소입니다. • 도메인 - MGT 인터페이스가 속한 도메인의 이름입니다. • DNS 서버 - MGT 인터페이스를 제공하는 최대 2개의 DNS 서버의 IP 주소입니다. DHCP 서버가 DNS 서버 주소를 반환하면 방화벽은 DNS 서버 주소를 수동으로 구성하지 않은 경우에만 해당 주소를 고려합니다. DNS 서버 주소를 수동으로 구성한 경우 방화벽은 DHCP 서버의 주소로 이를 덮어쓰지 않습니다. 선택적으로 MGT 인터페이스에 할당된 IP 주소에 대한 DHCP 리스를 갱신할 수 있습니다. 그렇지 않으면 창을 닫습니다.
Aux 1 / Aux 2 (PA-5200 시리즈 방화벽만 해당)	보조 인터페이스를 활성화하려면 다음 옵션 중 하나를 선택합니다. 이러한 인터페이스는 다음에 대해 10Gbps(SFP+) 처리량을 제공합니다. • 방화벽 관리 트래픽 - 관리자가 방화벽을 관리하기 위해 웹 인터페이스 및 CLI에 액세스할 때 사용할 네트워크 서비스(프로토콜)를 활성화해야 합니다. 웹 인터페이스에 대해 *HTTP* 대신 *HTTPS*를 활성화하고 *CLI*에 대해 *Telnet* 대신 *SSH*를 활성화합니다. • 방화벽 피어 간의 고가용성(HA) 동기화 - 인터페이스를 구성한 후 이를 HA 제어 링크(**Device** > **High Availability** > 일반)로 선택해야 합니다. • Panorama로의 로그 포워딩 - **Panorama Log Forwarding** 서비스가 활성화된 상태에서 서비스 경로를 구성해야 합니다(디바이스 > 설정 > 서비스).
IP 주소(IPv4)	네트워크에서 IPv4를 사용하는 경우 인터페이스에 IPv4 주소를 할당합니다. 또는 방화벽 관리를 위해 루프백 인터페이스의 IP 주소를 할당할 수 있습니다(네트워크 > 인터페이스 > 루프백 참조). 기본적으로 입력한 IP 주소는 로그 포워딩을 위한 소스 주소입니다.

항목	설명
넷마스크(IPv4)	인터페이스에 IPv4 주소를 할당한 경우 네트워크 마스크도 입력해야 합니다(예: 255.255.255.0).
기본 게이트웨이	인터페이스에 IPv4 주소를 할당한 경우 기본 게이트웨이에도 IPv4 주소를 할당해야 합니다(게이트웨이는 인터페이스와 동일한 서브넷에 있어야 함).
IPv6 주소/프리픽스 길이	네트워크에서 IPv6을 사용하는 경우 인터페이스에 IPv6 주소를 할당합니다. 넷마스크를 나타내려면 IPv6 프리픽스 길이를 입력합니다(예: 2001:db8:300::1/64).
기본 IPv6 게이트웨이	인터페이스에 IPv6 주소를 할당한 경우 기본 게이트웨이(게이트웨이는 인터페이스와 동일한 서브넷에 있어야 함)에도 IPv6 주소를 할당해야 합니다(예: 2001:db8:300::5).
속도	인터페이스에 대한 데이터 속도 및 이중 옵션을 구성합니다. 선택 사항에는 전이중 또는 반이중에서 10Mbps, 100Mbps 및 1Gbps가 포함됩니다. 방화벽이 인터페이스 속도를 결정하도록 하려면 기본 자동 협상 설정을 사용하십시오. 이 설정은 인접 네트워크 장비의 포트 설정과 일치해야 합니다. 설정이 일치하도록 하려면 인접 장비가 해당 옵션을 지원하는 경우 자동 협상을 선택합니다.
MTU	이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~1,500, 기본값은 1,500).
행정 관리 서비스	• **HTTP** - 이 서비스를 사용하여 방화벽 웹 인터페이스에 액세스합니다. *HTTP*는 *HTTPS*만큼 안전하지 않은 일반 텍스트를 사용합니다. 따라서 *Palo Alto Networks*는 인터페이스의 관리 트래픽에 대해 *HTTP* 대신 ***HTTPS***를 활성화할 것을 권장합니다. • **Telnet** - 이 서비스를 사용하여 방화벽 CLI에 액세스합니다. *Telnet*은 *SSH*만큼 안전하지 않은 일반 텍스트를 사용합니다. 따라서 *Palo Alto Networks*는 인터페이스의 관리 트래픽에 대해 *Telnet* 대신 *SSH*를 활성화할 것을 권장합니다. • **HTTPS** - 방화벽 웹 인터페이스에 대한 보안 액세스를 위해 이 서비스를 사용합니다. • **SSH** - 방화벽 CLI에 대한 보안 액세스를 위해 이 서비스를 사용합니다.

항목	설명
네트워크 서비스	인터페이스에서 활성화할 서비스를 선택합니다. • **HTTP OCSP** - 이 서비스를 사용하여 방화벽을 OCSP(온라인 인증서 상태 프로토콜) 응답자로 구성합니다. 자세한 내용은 디바이스 > 인증서 관리 > OCSP 응답자를 참조하십시오. • **Ping** - 이 서비스를 사용하여 외부 서비스와의 연결을 테스트합니다. 예를 들어 인터페이스를 핑(ping)하여 Palo Alto Networks 업데이트 서버에서 PAN-OS 소프트웨어 및 콘텐츠 업데이트를 수신할 수 있는지 확인할 수 있습니다. 고가용성(HA) 배포에서 HA 피어는 핑(ping)을 사용하여 하트비트 백업 정보를 교환합니다. • **SNMP** - 이 서비스를 사용하여 SNMP 관리자의 방화벽 통계 쿼리를 처리합니다. 자세한 내용은 SNMP 모니터링 활성화를 참조하십시오. • **User-ID** - 이 서비스를 사용하여 방화벽 간에 사용자 매핑의 데이터 재배포를 활성화합니다. • **User-ID Syslog Listener-SSL** - 이 서비스를 사용하여 PAN-OS 통합 User-ID™ 에이전트가 SSL을 통해 syslog 메시지를 수집할 수 있도록 합니다. 자세한 내용은 모니터링되는 서버에 대한 액세스 구성을 참조하십시오. • **User-ID Syslog** 수신기-**UDP** - 이 서비스를 사용하여 PAN-OS 통합 User-ID 에이전트가 UDP를 통해 syslog 메시지를 수집할 수 있도록 합니다. 자세한 내용은 모니터링되는 서버에 대한 액세스 구성을 참조하십시오.
허용된 IP 주소	관리자가 인터페이스를 통해 방화벽에 액세스할 수 있는 IP 주소를 입력합니다. 빈 목록(기본값)은 모든 IP 주소에서 액세스할 수 있음을 지정합니다. 목록을 공백으로 두지 마십시오. 무단 액세스를 방지하기 위해 방화벽 관리자의 *IP* 주소만 지정합니다.

디바이스 > 설정 > 원격 측정

원격 측정은 위협 및 지원 분석을 위해 데이터를 수집 및 전송하고 애플리케이션 논리를 활성화하는 프로세스입니다. 원격 측정을 수집하고 Palo Alto Networks로 전송하려면 먼저 대상 지역을 선택해야 합니다. 조직에 현재 Cortex Data Lake 라이선스가 있는 경우 대상 지역은 Cortex Data Lake 인스턴스가 있는 지역으로 제한됩니다.

텔레메트리 데이터는 Palo Alto Networks 제품 및 서비스를 관리하고 구성하는 능력을 향상시키는 애플리케이션을 강화하는 데 사용됩니다. 이러한 앱은 디바이스 상태, 성능, 용량 계획 및 구성에 대한 향상된 가시성을 제공합니다. Palo Alto Networks는 또한 이 데이터를 지속적으로 사용하여 위협 방지를 개선하고 제품 사용 이점을 극대화할 수 있도록 지원합니다.

Device > **Setup** > **Telemetry**를 선택하여 현재 수집된 원격 분석 카테고리를 확인합니다. 이러한 카테고리를 변경하려면 원격 분석 위젯을 편집하십시오. 방화벽에서 수집하지 않을 카테고리를 선택 취소하고 변경 사항을 커밋합니다.

다음 원격 측정 전송 인터벌에서 방화벽이 Palo Alto Networks에 보낼 데이터의 실시간 예를 얻으려면 원격 측정 파일을 생성하십시오.

원격 측정 전송을 완전히 비활성화하려면 원격 측정 활성화가 선택되지 않았는지 확인하고 변경 사항을 커밋합니다.

디바이스 > 설정 > 콘텐츠 ID

Content-ID™ 탭을 사용하여 URL 필터링, 데이터 보호 및 컨테이너 페이지에 대한 설정을 정의합니다.

콘텐츠 **ID** 설정	설명
URL 필터링	
URL 계속 타임아웃	사용자가 동일한 카테고리의 URL에 대해 계속을 다시 누르기 전에 사용자의 계속 작업 후 인터벌을 지정합니다(범위는 1~86,400분, 기본값은 15).
URL 관리자 재정의 타임아웃	사용자가 관리자 무시 암호를 입력한 후 동일한 카테고리의 URL에 대해 해당 암호를 다시 입력해야 하는 인터벌을 지정합니다(범위는 1~86,400분, 기본값은 15).
카테고리 조회에 대한 클라이언트 요청 보류	방화벽이 로컬 캐시에서 URL에 대한 카테고리 정보를 찾을 수 없는 경우 PAN-DB를 쿼리할 때 웹 요청을 보류하도록 지정하려면 이 옵션을 활성화합니다. 이 옵션은 기본적으로 비활성화되어 있습니다. 모범 사례 URL 필터링 프로파일의 일부로 활성화합니다.
후행 슬래시 추가	방화벽이 사용자 지정 URL 범주 및 URL 목록 유형의 외부 동적 목록에서 *END*가 아닌 도메인 항목(예: **paloaltonetworks.com**)에 후행 슬래시 또는 별표 와일드카드(*)를 추가하도록 설정합니다. 후행 슬래시는 방화벽이 항목과 일치하는 것으로 간주하고 URL 필터링 정책 규칙을 적용할 수 있는 URL을 제한합니다. • 와일드카드(* 또는 ^)가 없는 도메인 항목의 경우 후행 슬래시는 일치 항목을 지정된 도메인과 그 하위 디렉터리로 제한합니다. • 와일드카드가 있는 도메인 항목의 경우 후행 슬래시는 지정된 패턴을 준수하는 URL과의 일치를 제한합니다. URL 범주 예외는 후행 슬래시를 자세히 설명하고 URL 목록 형식 가이드라인을 포함합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
카테고리 조회 타임아웃(초)	카테고리가 #### ##을 결정하기 전에 방화벽이 URL에 대한 카테고리 조회를 시도하는 시간을 초 단위로 지정합니다(범위는 1~60초, 기본값은 2).

콘텐츠 **ID** 설정	설명
URL 관리자 잠금 타임아웃	사용자가 세 번 실패한 후 URL 관리자 재정의 암호를 사용하려는 시도에서 잠기는 시간을 지정합니다(범위는 1~86,400분, 기본값은 30).
PAN-DB Server (사설 PAN-DB 서버 접속 시 필요)	네트워크의 개인 PAN-DB 서버에 대한 IPv4 주소, IPv6 주소 또는 FQDN을 지정합니다. 최대 20개의 항목을 추가할 수 있습니다. 방화벽은 기본적으로 공용 PAN-DB 클라우드에 연결됩니다. 프라이빗 PAN-DB 솔루션은 방화벽이 퍼블릭 클라우드의 PAN-DB 서버에 직접 접근하는 것을 허용하지 않는 기업을 위한 솔루션입니다. 방화벽은 URL 데이터베이스, URL 업데이트 및 웹 페이지 분류를 위한 URL 조회를 위해 이 PAN-DB 서버 목록에 포함된 서버에 액세스합니다.
URL 관리자 재정의	
URL 관리자 재정의 설정	URL 관리 재정의에 대해 구성하려는 각 가상 시스템에 대해 URL 필터링 프로파일이 페이지를 차단하고 재정의 작업이 지정될 때 적용되는 설정을 추가하고 지정합니다. 자세한 내용은 객체 > 보안 프로파일 > URL 필터링을 참조하십시오. • 위치 - (multi-vsys 방화벽만 해당) 드롭다운에서 가상 시스템을 선택합니다. • 암호/암호 확인 - 사용자가 차단 페이지를 무시하기 위해 입력해야 하는 암호를 입력합니다. • **SSL/TLS** 서비스 프로파일 - 지정된 서버를 통해 리디렉션할 때 통신 보안을 위해 인증서 및 허용되는 TLS 프로토콜 버전을 지정하려면 SSL/TLS 서비스 프로파일을 선택합니다. 자세한 내용은 디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일을 참조하십시오. • 모드 - 차단 페이지가 투명하게 전달되는지(차단된 웹사이트에서 시작된 것처럼 보임) 사용자를 지정된 서버로 리디렉션할지 결정합니다. 리디렉션을 선택한 경우 리디렉션할 IP 주소를 입력합니다. 항목을 삭제할 수도 있습니다.
HTTP/2 설정	
연결 로깅	방화벽이 HTTP/2 연결 세션을 터널 검사 로그 항목으로 기록하도록 합니다.
콘텐츠 클라우드 설정	
서비스 URL	클라우드 제공 보안 서비스 서버 URL입니다.

콘텐츠 ID 설정	설명
	• **APAC—apac.hawkeye.services-edge.paloaltonetworks.com** • **Europe—eu.hawkeye.services-edge.paloaltonetworks.com** • 영국 - **uk.hawkeye.services-edge.paloaltonetworks.com** • **United States—us.hawkeye.services-edge.paloaltonetworks.com**
URL 인라인 클라우드 분류	
최대 지연 시간(초)	인라인 클라우드 분류가 결과를 반환하는 데 허용되는 최대 처리 시간(초)을 지정합니다.
최대 지연 시간 허용	최대 대기 시간에 도달하면 방화벽이 허용 작업을 수행할 수 있도록 합니다. 이 옵션을 선택 취소하면 방화벽 작업이 차단으로 설정됩니다.
로그 트래픽이 검사되지 않음	방화벽이 특정 고급 웹 페이지 위협의 존재를 나타내지만 인라인 클라우드 분류에 의해 처리되지 않은 URL 분류 요청을 기록할 수 있도록 합니다.
콘텐츠 ID 설정	
복호화된 콘텐츠 포워딩 허용	포트 미러링 또는 분석을 위해 WildFire® 파일을 보낼 때 복호화된 콘텐츠를 외부 서비스로 포워딩하도록 방화벽을 구성하려면 이 옵션을 활성화합니다. 이 옵션을 활성화하고 복호화된 트래픽의 모든 알 수 없는 파일을 분석을 위해 *WildFire*로 보냅니다. 다중 가상 시스템(multi-vsys) 기능이 있는 방화벽의 경우 각 가상 시스템에 대해 이 옵션을 개별적으로 활성화합니다. 디바이스 > 가상 시스템을 선택한 다음 복호화된 콘텐츠의 포워딩을 활성화할 가상 시스템을 선택합니다. 이 옵션은 가상 시스템 대화 상자에서 사용할 수 있습니다.
확장된 패킷 캡처 길이	Anti-Spyware 및 Vulnerability Protection 프로파일에서 확장 캡처 옵션이 활성화된 경우 캡처할 패킷 수를 설정합니다(범위는 1~50, 기본값은 5).
TCP App-ID™ 검사 대기열을 초과하는 포워딩 세그먼트	App-ID 대기열이 64개 세그먼트 제한을 초과할 때 세그먼트를 전달하고 애플리케이션을 `unknown-tcp`로 분류하려면 이 옵션을 활성화하십시오. 이 옵션을 활성화 또는 비활성화했는지 여부에 관계없이 다음 전역 카운터를 사용하여 대기열 제한을 초과하는 세그먼트 수를 확인합니다.

콘텐츠 **ID** 설정	설명
	`appid_exceed_queue_limit` 방화벽이 TCP 세그먼트를 포워딩하고 App-ID 검사 대기열이 가득 찼을 때 App-ID 검사를 건너뛰는 것을 방지하려면 이 옵션을 비활성화합니다. 이 옵션은 기본적으로 비활성화되어 있으며 최대 보안을 위해 비활성화된 상태로 유지해야 합니다. 이 옵션을 비활성화하면 *64*개 이상의 세그먼트가 *App-ID* 처리를 기다리는 스트림에서 지연 시간이 증가할 수 있습니다.

TCP 콘텐츠 검사 대기열을 초과하는 포워딩 세그먼트	TCP 콘텐츠 검사 대기열이 가득찼을 때 TCP 세그먼트를 포워딩하고 콘텐츠 검사를 건너뛰려면 이 옵션을 활성화합니다. 방화벽은 콘텐츠 엔진을 기다리는 동안 최대 64개의 세그먼트를 대기열에 넣을 수 있습니다. 방화벽이 세그먼트를 포워딩하고 전체 콘텐츠 검사 대기열로 인해 콘텐츠 검사를 건너뛰면 다음 전역 카운터가 증가합니다.
	
	`ctd_exceed_queue_limit`
	
	콘텐츠 검사 대기열이 가득 찼을 때 방화벽이 TCP 세그먼트를 포워딩하고 콘텐츠 검사를 건너뛰지 못하도록 하려면 이 옵션을 비활성화합니다. 이 옵션을 비활성화하면 방화벽이 대기열 제한을 초과하는 모든 세그먼트를 삭제하고 다음 전역 카운터를 증가시킵니다.
	
	`ctd_exceed_queue_limit_drop`
	
	이 글로벌 카운터 쌍은 TCP 및 UDP 패킷 모두에 적용됩니다. 전역 카운터를 본 후 설정을 변경하기로 결정한 경우 다음 명령을 사용하여 CLI 내에서 수정할 수 있습니다.
	
	`deviceconfig ## ctd tcp-bypass-exceed-queue ##`
	
	이 옵션은 기본적으로 활성화되어 있지만 최대 보안을 위해 *Palo Alto Networks*는 이 옵션을 비활성화할 것을 권장합니다. 그러나 손실된 트래픽에 대한 *TCP* 재전송으로 인해 이 옵션을 비활성화하면 특히 대용량 트래픽 환경에서 일부 애플리케이션의 성능이 저하되고 기능이 손실될 수 있습니다.

콘텐츠 ID 설정	설명

UDP 콘텐츠 검사 대기열을 초과하는 포워딩 데이터그램	UDP 콘텐츠 검사 대기열이 가득 찬 경우 UDP 데이터그램을 포워딩하고 콘텐츠 검사를 건너뛰려면 이 옵션을 활성화합니다. 방화벽은 콘텐츠 엔진의 응답을 기다리는 동안 최대 64개의 데이터그램을 대기열에 넣을 수 있습니다. 방화벽이 데이터그램을 포워딩하고 UDP 콘텐츠 검사 대기열 오버플로로 인해 콘텐츠 검사를 건너뛰면 다음 전역 카운터가 증가합니다.
	
	`ctd_exceed_queue_limit`
	
	UDP 콘텐츠 검사 대기열이 가득찼을 때 방화벽이 데이터그램을 포워딩하고 콘텐츠 검사를 건너뛰는 것을 방지하려면 이 옵션을 비활성화합니다. 이 옵션이 비활성화되면 방화벽은 대기열 제한을 초과하는 모든 데이터그램을 삭제하고 다음 전역 카운터를 증가시킵니다.
	
	`ctd_exceed_queue_limit_drop`
	
	이 글로벌 카운터 쌍은 TCP 및 UDP 패킷 모두에 적용됩니다. 전역 카운터를 확인한 후 설정을 변경하기로 결정한 경우 다음 명령을 사용하여 CLI 내에서 수정할 수 있습니다.
	
	`#### ## ## ctd udp-bypass-exceed-queue`
	
	이 옵션은 기본적으로 활성화되어 있지만 최대 보안을 위해 *Palo Alto Networks*는 이 옵션을 비활성화할 것을 권장합니다. 그러나 패킷 손실로 인해 이 옵션을 비활성화하면 일부 애플리케이션, 특히 대용량 트래픽 환경에서 성능이 저하되고 기능이 손실될 수 있습니다.

HTTP 부분 응답 허용	클라이언트가 파일의 일부만 가져올 수 있도록 하려면 이 HTTP 부분 응답 옵션을 활성화합니다. 전송 경로에 있는 차세대 방화벽이 악성 파일을 식별하여 삭제하면 RST 패킷으로 TCP 세션을 종료합니다. 웹 브라우저가 HTTP 범위 옵션을 구현하면 새 세션을 시작하여 파일의 나머지 부분만 가져올 수 있습니다. 이렇게 하면 방화벽이 초기 세션에 대한 컨텍스트 부족으로 인해 동일한 서명을 다시 트리거하는 것을 방지하는 동시에 웹 브라우저가 파일을 재구성하고 악성 콘텐츠를 전달할 수 있습니다. 이를 방지하려면 이 옵션을 비활성화해야 합니다.

콘텐츠 **ID** 설정	설명
	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.
실시간 서명 조회	
DNS 서명 조회 타임아웃(ms)	방화벽이 DNS 보안 서비스를 쿼리하는 시간(밀리초)을 지정합니다. 클라우드가 지정된 기간이 끝나기 전에 응답하지 않으면 방화벽은 요청 클라이언트에 연결된 DNS 응답을 해제합니다(범위는 0~60,000, 기본값은 100).
X-Forwarded-For 헤더	
X-Forwarded-For 헤더 사용	*User-ID* 및 보안 정책에 대해 *X-Forwarded-For*를 동시에 활성화할 수 없습니다. • 비활성화됨 - 비활성화되면 방화벽이 클라이언트 요청의 XFF(X-Forwarded-For) 헤더에서 IP 주소를 읽지 않습니다. • **User-ID**에 대해 활성화 - 방화벽이 인터넷과 클라이언트 IP 주소를 숨기는 프록시 서버 사이에 배포될 때 웹 서비스에 대한 클라이언트 요청

콘텐츠 **ID** 설정	설명
	의 XFF(X-Forwarded-For) 헤더에서 IP 주소를 읽도록 지정하려면 이 옵션을 활성화합니다. User-ID는 해당 정책이 연결된 사용자 및 그룹에 대한 액세스를 제어하고 기록할 수 있도록 정책이 참조하는 사용자명과 읽은 IP 주소를 일치시킵니다. 헤더에 여러 IP 주소가 있는 경우 User-ID는 왼쪽에서 첫 번째 항목을 사용합니다. 헤더 값이 IP 주소가 아닌 문자열인 경우가 있습니다. 문자열이 User-ID가 IP 주소에 매핑한 사용자명과 일치하면 방화벽은 정책의 그룹 매핑 참조에 해당 사용자명을 사용합니다. 문자열에 대한 IP 주소 매핑이 없는 경우 방화벽은 소스 사용자가 모두 또는 알 수 없음으로 설정된 정책 규칙을 호출합니다. URL 필터링 로그는 소스 사용자 필드에 일치하는 사용자명을 표시합니다. User-ID가 일치를 수행할 수 없거나 IP 주소와 연결된 영역에 대해 활성화되지 않은 경우 소스 사용자 필드는 **`x-fwd-for`** 프리픽스가 있는 XFF IP 주소를 표시합니다. 문제를 조사하는 데 도움이 되도록 원래 클라이언트 *IP* 주소가 로그에 표시되도록 *User-ID*에서 *XFF* 헤더를 사용하도록 설정합니다. • 보안 정책 활성화 - 프록시 서버 또는 로드 밸런서와 같은 업스트림 디바이스가 클라이언트와 방화벽 사이에 배포될 때 방화벽이 웹 서비스에 대한 클라이언트 요청의 XFF(X-Forwarded-For) 헤더에서 IP 주소를 읽도록 지정하려면 이 옵션을 활성화합니다. 프록시 서버 또는 로드 밸런서 IP 주소는 클라이언트 IP 주소를 요청 소스 IP로 대체합니다. 그러면 방화벽이 XFF 헤더의 IP 주소를 사용하여 정책을 적용할 수 있습니다. 방화벽은 *XFF* 필드에 가장 최근에 추가된 *IP* 주소를 사용합니다. 요청이 여러 업스트림 디바이스를 통과하는 경우 방화벽은 마지막으로 추가된 *IP* 주소를 기반으로 정책을 적용합니다.
Strip-X-Forwarded-For 헤더	인터넷과 프록시 서버 사이에 방화벽이 배포될 때 웹 서비스를 요청하는 클라이언트의 IP 주소를 포함하는 XFF(X-Forwarded-For) 헤더를 제거하려면 이 옵션을 활성화합니다. 방화벽은 요청을 포워딩하기 전에 헤더 값을 0으로 만듭니다. 포워딩된 패킷에는 내부 소스 IP 정보가 포함되어 있지 않습니다. 이 옵션을 활성화해도 정책에서 사용자 속성에 대한 *XFF* 헤더 사용이 비활성화되지 않습니다. 방화벽은 사용자 어트리뷰션에 사용한 후에만 *XFF* 값을 *0*으로 만듭니다.

콘텐츠 **ID** 설정	설명
	*User-ID*에서 *XFF* 헤더 사용을 활성화하면 패킷을 포워딩하기 전에 *XFF* 헤더를 제거하여 사용자를 추적하는 기능을 잃지 않고 사용자 개인 정보를 보호할 수 있습니다. 두 옵션을 모두 활성화하면 원래 사용자 *IP* 주소를 기록 및 추적하는 동시에 원래 *IP* 주소를 포워딩하지 않음으로써 사용자 개인 정보를 보호할 수 있습니다.
콘텐츠 ID 기능	
데이터 보호 관리	신용카드 또는 주민등록번호와 같은 민감한 정보가 포함될 수 있는 로그에 대한 액세스에 관련 추가 보호 기능을 추가합니다. 데이터 보호 관리를 클릭하여 다음 작업을 수행합니다. • 암호 설정 - 구성되지 않은 경우 새 암호를 입력하고 확인합니다. • 암호 변경 - 이전 암호를 입력하고 새 암호를 입력하고 확인합니다. • 비밀번호 삭제 - 비밀번호와 보호된 데이터를 삭제합니다.
컨테이너 페이지	이러한 설정을 사용하여 application/pdf, application/soap+xml, application/xhtml+, text/html, text/plain 및 text/xml과 같은 콘텐츠 유형을 기반으로 방화벽이 추적하거나 기록하는 URL 유형을 지정합니다. 컨테이너 페이지는 위치 드롭다운에서 선택한 가상 시스템별로 설정됩니다. 가상 시스템에 명시적 컨테이너 페이지가 정의되어 있지 않으면 방화벽은 기본 콘텐츠 유형을 사용합니다. 콘텐츠 유형을 추가 및 입력하거나 기존 콘텐츠 유형을 선택합니다. 가상 시스템에 대한 새 콘텐츠 형식을 추가하면 콘텐츠 형식의 기본 목록이 재정의됩니다. 가상 시스템과 연결된 콘텐츠 유형이 없으면 기본 콘텐츠 유형 목록이 사용됩니다.
위협 방지 인라인 클라우드 분석	
최대 지연 시간(초)	지능형 위협 차단 인라인 클라우드 분석에서 결과를 반환하는 데 걸리는 최대 처리 시간(초) 을 지정합니다.
최대 지연 시간 허용	최대 대기 시간에 도달하면 방화벽이 허용 작업을 수행할 수 있도록 합니다. 이 옵션을 선택 취소하면 방화벽 작업이 차단으로 설정됩니다.
로그 트래픽이 검사되지 않음	방화벽이 C2(고급 및 회피 명령 및 제어) 위협의 존재를 나타내는 비정상적인 특성을 나타내지만 위협 방지 인라인 클라우드 분석기에서 처리하지 않은 트래픽 요청을 기록할 수 있도록 합니다.

디바이스 > 설정 > WildFire

디바이스 > 설정 > **WildFire**를 선택하여 방화벽 및 Panorama에서 WildFire 설정을 구성합니다. WildFire 클라우드와 WildFire 어플라이언스를 모두 사용하여 파일 분석을 수행할 수 있습니다. 보고할 파일 크기 제한 및 세션 정보를 설정할 수도 있습니다. WildFire 설정을 채운 후 **WildFire** 분석 프로파일(**Objects** > **Security Profiles** > **WildFire Analysis**)을 만들어 WildFire 클라우드 또는 WildFire 어플라이언스에 포워딩할 파일을 지정할 수 있습니다.

복호화된 콘텐츠를 *WildFire*로 포워딩하려면 WildFire 분석을 위한 복호화된 SSL 트래픽 포워딩을 참조하십시오.

WildFire 설정	설명
일반 설정	
WildFire Public Cloud	**wildfire.paloaltonetworks.com**을 입력하여 분석을 위해 미국에서 호스팅되는 WildFire 글로벌 클라우드(미국)로 파일을 보냅니다. 또는 대신 분석을 위해 WildFire 지역 클라우드로 파일을 보낼 수 있습니다. 지역 클라우드는 위치에 따라 가질 수 있는 데이터 개인 정보 보호 기대치를 준수하도록 설계되었습니다. 샘플을 지역 *WildFire* 클라우드로 포워딩하여 해당 지역의 데이터 개인 정보 보호 및 규정 준수 표준을 준수하도록 합니다. 지역별 클라우드는 다음과 같습니다. • *Europe*—***eu.wildfire.paloaltonetworks.com*** • *Japan*—***jp.wildfire.paloaltonetworks.com*** • *Singapore*—***sg.wildfire.paloaltonetworks.com*** • 영국 - ***uk.wildfire.paloaltonetworks.com*** • 캐나다 - ***ca.wildfire.paloaltonetworks.com*** • 호주 - ***au.wildfire.paloaltonetworks.com*** • 독일 - ***de.wildfire.paloaltonetworks.com*** • 인도 - ***in.wildfire.paloaltonetworks.com***

WildFire 설정	설명
WildFire Private Cloud	WildFire 어플라이언스의 IPv4/IPv6 주소 또는 FQDN을 지정합니다. 방화벽은 분석을 위해 지정된 WildFire 어플라이언스로 파일을 보냅니다. Panorama는 WildFire 어플라이언스에서 위협 ID를 수집하여 디바이스 그룹에서 구성한 Anti-Spyware 프로파일(DNS 서명만 해당) 및 Antivirus 프로파일에 위협 예외를 추가할 수 있도록 합니다. Panorama는 또한 PAN-OS 7.0 이전 버전의 소프트웨어를 실행하는 방화벽에서 수신한 WildFire 제출 로그에서 누락된 필드를 채우기 위해 WildFire 어플라이언스에서 정보를 수집합니다.
파일 크기 제한	WildFire 서버에 포워딩할 최대 파일 크기를 지정합니다. 파일 크기 제한에 대한 모든 모범 사례 권장 사항의 경우 제한이 너무 커서 방화벽이 여러 개의 큰 제로 데이(zero-day) 파일을 동시에 포워딩하지 못하는 경우 사용 가능한 방화벽 버퍼 공간의 양에 따라 최대 제한을 낮추고 조정합니다. 더 많은 버퍼 공간을 사용할 수 있는 경우 모범 사례 권장 사항 이상으로 파일 크기 제한을 늘릴 수 있습니다. 모범 사례 권장 사항은 방화벽 리소스에 무리를 주지 않는 효과적인 제한을 설정하기 위한 좋은 출발점입니다. 사용 가능한 범위는 다음과 같습니다. • **pe**(Portable Executable) - 범위는 1~50MB입니다. 기본값은 16MB입니다. *PE* 파일의 크기를 *16MB*로 설정합니다. • **apk**(Android 애플리케이션) - 범위는 1~50MB입니다. 기본 10MB. *APK* 파일의 크기를 *10MB*로 설정합니다. • **pdf**(Portable Document Format) - 범위는 100KB에서 51,200KB입니다. 기본값은 3,072KB입니다. *PDF* 파일의 크기를 *3,072KB*로 설정합니다. • **ms-office**(Microsoft Office) - 범위는 200KB ~ 51,200KB입니다. 기본값은 16,384KB입니다. *ms-office* 파일의 크기를 *16,384KB*로 설정합니다.

WildFire 설정	설명
	• **jar**(패키지된 Java 클래스 파일) - 범위는 1~20MB입니다. 기본값은 5MB입니다. *jar* 파일의 크기를 *5MB*로 설정합니다. • **flash**(Adobe Flash) - 범위는 1~10MB입니다. 기본값은 5MB입니다. 플래시 파일의 크기를 *5MB*로 설정합니다. • **MacOSX**(DMG/MAC-APP/MACH-O PKG 파일) - 범위는 1~50MB입니다. 기본값은 10MB입니다. *MacOSX* 파일의 크기를 *1MB*로 설정합니다. • 아카이브(RAR 및 7z 파일) - 범위는 1~50MB입니다. 기본값은 50MB입니다. 아카이브 파일의 크기를 *50MB*로 설정합니다. • **linux**(ELF 파일) - 범위는 1~50MB입니다. 기본값은 50MB입니다. *Linux* 파일의 크기를 *50MB*로 설정합니다. • 스크립트(JScript, VBScript, PowerShell 및 Shell 스크립트 파일) - 범위는 10~4096KB입니다. 기본값은 20KB입니다. 스크립트 파일의 크기를 *20KB*로 설정합니다. 위의 값은 *PAN-OS*의 현재 버전 또는 콘텐츠 릴리스에 따라 다를 수 있습니다. 유효한 범위를 보려면 크기 제한 필드를 클릭하십시오. 팝업에 사용 가능한 범위와 기본값이 표시됩니다.
정상 파일 보고	이 옵션이 활성화되면(기본적으로 비활성화되어 있음) WildFire에서 분석하여 정상으로 판단되는 파일이 **Monitor** > **WildFire** 제출 로그에 나타납니다. 방화벽에서 이 옵션이 활성화된 경우에도 처리되는 링크의 잠재적 수량으로 인해 WildFire가 정상이라고 간주하는 이메일 링크는 기록되지 않습니다.
그레이웨어 파일 보고	이 옵션이 활성화되면(기본적으로 비활성화됨) WildFire에서 분석한 그레이웨어로 확인된 파일이 **Monitor** > **WildFire** 제출 로그에 나타납니다.

WildFire 설정	설명
	방화벽에서 이 옵션을 사용하도록 설정한 경우에도 *WildFire*에서 그레이웨어로 판단한 이메일 링크는 처리되는 링크의 잠재적 수량으로 인해 기록되지 않습니다. 보고 그레이웨어 파일을 활성화하여 세션 정보, 네트워크 활동, 호스트 활동 및 분석에 도움이 되는 기타 정보를 기록합니다.
세션 정보 설정	
설정	WildFire 서버에 포워딩할 정보를 지정합니다. 기본적으로 모두 선택되어 있으며 가장 좋은 방법은 모든 세션 정보를 포워딩하여 위협 이벤트를 방지하기 위한 조치를 취할 수 있는 통계 및 기타 메트릭을 제공하는 것입니다. • 소스 **IP** - 의심되는 파일을 보낸 소스 IP 주소입니다. • 소스 포트 - 의심되는 파일을 보낸 소스 포트입니다. • 대상 **IP** - 의심되는 파일의 대상 IP 주소입니다. • 대상 포트 - 의심되는 파일의 대상 포트입니다. • **Vsys** - 가능한 멀웨어를 식별한 방화벽 가상 시스템입니다. • 애플리케이션 - 파일을 전송하는 데 사용된 사용자 애플리케이션입니다. • 사용자 - 대상 사용자. • **URL** - 의심되는 파일과 연결된 URL입니다. • 파일 이름 - 전송된 파일의 이름입니다. • 이메일 발신자 - SMTP 및 POP3 트래픽에서 악성 이메일 링크가 감지되면 WildFire 로그 및 WildFire 세부 보고서에 발신자 이름을 제공합니다. • 이메일 수신자 - SMTP 및 POP3 트래픽에서 악성 이메일 링크가 감지되면 WildFire 로그 및 WildFire 세부 보고서에 수신자 이름을 제공합니다. • 이메일 제목 - SMTP 및 POP3 트래픽에서 악성 이메일 링크가 감지되면 WildFire 로그 및 WildFire 세부 보고서에 이메일 제목을 제공합니다.

디바이스 > 설정 > 세션

Device > **Setup** > **Session**을 선택하여 세션 만료 시간, 복호화 인증서 설정, IPv6 트래픽 방화벽 및 정책 변경 시 보안 정책을 기존 세션과 다시 일치시키는 것과 같은 전역 세션 관련 설정을 구성합니다. 탭에는 다음 섹션이 있습니다.

- 세션 설정
- 세션 타임아웃
- TCP 설정
- 복호화 설정: 인증서 해지 확인
- 복호화 설정: 포워딩 프록시 서버 인증서 설정
- 복호화 설정: SSL 복호화 설정
- VPN 세션 설정

세션 설정

다음 표에서는 세션 설정에 대해 설명합니다.

세션 설정	설명
재일치 세션	편집을 클릭하고 세션 다시 일치를 선택하여 방화벽이 새로 구성된 보안 정책 규칙을 이미 진행 중인 세션에 적용하도록 합니다. 이 기능은 기본적으로 활성화되어 있습니다. 이 설정을 사용하지 않으면 정책 규칙 변경 사항이 변경 사항이 커밋된 후에 시작된 세션에만 적용됩니다. 예를 들어 텔넷을 허용하는 연결된 정책 규칙이 구성되는 동안 텔넷 세션이 시작되었고 이후에 텔넷을 거부하도록 정책 규칙 변경을 커밋한 경우 방화벽은 수정된 정책 규칙을 현재 세션에 적용하고 차단합니다. ***Rematch Sessions***를 활성화하여 현재 활성 세션에 최신 보안 정책 규칙을 적용합니다.
ICMPv6 토큰 버킷 크기	ICMPv6 오류 메시지의 속도 제한을 위한 버킷 크기를 입력합니다. 토큰 버킷 크기는 ICMPv6 오류 패킷의 버스트를 제어하는 토큰 버킷 알고리즘의 매개변수입니다(범위는 10 - 65,535 패킷, 기본값은 100).
ICMPv6 오류 패킷 비율	방화벽을 통해 전역적으로 허용되는 초당 평균 ICMPv6 오류 패킷 수를 입력합니다(범위는 10~65,535, 기본값은 100). 이 값은 모든 인터페이스에 적용됩니다. 방화벽이 ICMPv6 오류 패킷 속도에 도달하면 ICMPv6 토큰 버킷을 사용하여 ICMPv6 오류 메시지의 조절을 활성화합니다.

세션 설정	설명
IPv6 방화벽 활성화	IPv6 트래픽에 대한 방화벽 기능을 활성화하려면 **IPv6** 방화벽을 편집하고 선택합니다. IPv6 방화벽을 활성화하지 않으면 방화벽은 모든 IPv6 기반 구성을 무시합니다. 인터페이스에서 IPv6 트래픽을 활성화하더라도 IPv6 방화벽이 작동하려면 **IPv6** 방화벽 옵션도 활성화해야 합니다.
ERSPAN 지원	방화벽이 GRE(일반 라우팅 캡슐화) 터널을 종료하고 캡슐화된 원격 스위치 포트 분석기(ERSPAN) 데이터를 캡슐화하도록 설정합니다. 이는 IoT 보안과 같은 보안 서비스에 유용합니다. 네트워크 스위치는 네트워크 트래픽을 미러링하고 ERSPAN을 사용하여 GRE 터널을 통해 방화벽으로 전송합니다. 방화벽은 데이터를 캡슐화한 후 TAP 포트에서 수신된 트래픽을 검사하는 방법과 유사하게 데이터를 검사합니다. 그런 다음 향상된 애플리케이션 로그(EAL) 및 트래픽, 위협, WildFire, URL, 데이터, GTP(GTP가 활성화된 경우), SCTP(SCTP가 활성화된 경우), 터널, 인증 및 암호 해독 로그를 만듭니다. 방화벽은 이러한 로그를 IoT Security가 데이터에 액세스하고 분석하는 로깅 서비스로 전달합니다.
점보 프레임 활성화 글로벌 MTU	이더넷 인터페이스에서 점보 프레임 지원을 활성화하려면 선택합니다. 점보 프레임의 최대 전송 단위(MTU)는 9,192바이트이며 특정 모델에서만 사용할 수 있습니다. • 점보 프레임을 활성화하지 않으면 글로벌 **MTU**는 기본적으로 1,500바이트(범위는 576~1,500)로 설정됩니다. • 점보 프레임을 활성화하는 경우 글로벌 **MTU**는 기본적으로 9,192바이트(범위는 9,192~9,216바이트)로 설정됩니다. 점보 프레임은 일반 패킷에 비해 최대 *5*배 더 많은 메모리를 차지할 수 있으며 사용 가능한 패킷 버퍼 수를 *20%*까지 줄일 수 있습니다. 이렇게 하면 비순차적, 애플리케이션 식별 및 기타 패킷 처리 작업 전용 대기열 크기가 줄어듭니다. *PAN-OS 8.1*부터 점보 프레임 글로벌 *MTU* 구성을 활성화하고 방화벽을 재부팅하면 패킷 버퍼가 재분배되어 점보 프레임을 보다 효율적으로 처리합니다. 점보 프레임을 활성화하고 MTU가 특별히 구성되지 않은 인터페이스가 있는 경우 해당 인터페이스는 점보 프레임 크기를 자동으로 상속합니다. 따라서 점보 프레임을 활성화하기 전에 점보 프레임을 허용하지 않으려는 인터페이스가 있는 경우 해당 인터페이스의 MTU를 1,500바이트 또는 다른 값으로 설정해야 합니다. 인터페이스(네트워크 > 인터페이스 > 이더넷)에 대한 MTU를 구성하려면 PA-7000 시리즈 레이어 3 인터페이스를 참조하십시오.

세션 설정	설명
DHCP 브로드캐스트 세션	방화벽이 DHCP 서버로 작동하는 경우 DHCP 브로드캐스트 패킷에 대한 세션 로그를 활성화하려면 이 옵션을 선택합니다. DHCP 브로드캐스트 세션 옵션을 사용하면 IoT 보안 및 기타 서비스에서 사용할 DHCP용 EAL 로그(Enhanced Application Logs)를 생성할 수 있습니다. 이 옵션을 활성화하지 않으면 방화벽은 DHCP 브로드캐스트 패킷에 대한 로그를 생성하지 않고 패킷을 포워딩합니다.
L3 및 L4 헤더 검사	레이어 3 및 레이어 4 헤더 검사를 활성화합니다. 영역 보호 프로필을 통해 L3 및 L4 헤더 필드를 기반으로 사용자 지정 위협 서명을 작성하여 특정 IoT 디바이스에 있는 것과 같이 일반적으로 표준 서명 업데이트를 통해 해결되지 않는 취약성을 방어하려면 이 옵션을 선택합니다. 구성 변경 사항을 적용하려면 방화벽을 재부팅해야 합니다.
NAT64 IPv6 최소 네트워크 MTU	IPv6 변환 트래픽에 대한 글로벌 MTU를 입력합니다. 기본값 1,280바이트는 IPv6 트래픽에 대한 표준 최소 MTU(범위는 1,280~9,216)를 기반으로 합니다.
NAT 초과 가입 비율	방화벽이 동일한 변환된 IP 주소와 포트 쌍을 동시에 사용할 수 있는 횟수인 DIPP NAT 초과 가입 비율을 선택합니다. 초과 구독 비율을 줄이면 소스 디바이스 변환 수가 줄어들지만 더 높은 NAT 규칙 용량을 제공합니다. • 플랫폼 기본값 - 초과 가입 비율의 명시적 구성이 해제되고 모델에 대한 기본 초과 가입 비율이 적용됩니다. (https://www.paloaltonetworks.com/products/product-selection.html에서 방화벽 모델의 기본 속도를 참조하십시오). • **1x**-1회. 이는 초과 구독이 없음을 의미합니다. 방화벽은 동일한 변환된 IP 주소와 포트 쌍을 동시에 두 번 이상 사용할 수 없습니다. • **2**배—2배 • **4**배—4배 • **8x**—8배
ICMP 연결할 수 없는 패킷 속도(초당)	방화벽이 초당 보낼 수 있는 ICMP 연결할 수 없는 응답의 최대 수를 정의합니다. 이 제한은 IPv4 및 IPv6 패킷에서 공유됩니다. 기본값은 초당 200개 메시지입니다(범위는 1~65,535).
가속화된 기간	유휴 세션의 가속화된 유효 시간 만료를 활성화합니다.

세션 설정	설명
	가속화된 기간을 활성화하고 임계값(%) 및 배율 인수를 지정하려면 이 옵션을 선택합니다. 세션 테이블이 **Accelerated Aging Threshold**(% full)에 도달하면 PAN-OS는 **Accelerated Aging Scaling Factor**를 모든 세션의 기간 계산에 적용합니다. 기본 배율 인수는 2입니다. 즉, 구성된 유휴 시간보다 두 배 빠른 속도로 노화가 가속화됩니다. 구성된 유휴 시간을 2로 나누면 타임아웃이 더 빨라집니다(시간의 1/2). 세션의 가속화된 에이징을 계산하기 위해 PAN-OS는 구성된 유휴 시간(해당 세션 유형에 대해)을 배율 인수로 나누어 더 짧은 타임아웃을 결정합니다. 예를 들어 배율 인수가 10인 경우 일반적으로 3,600초 후에 타임아웃되는 세션은 10배 더 빠른 타임아웃(시간의 1/10)인 360초가 됩니다. 가속화된 기간 임계값을 활성화하고 허용 가능한 스케일링 계수를 설정하여 세션 테이블이 가득 차기 시작할 때 세션 테이블 공간을 더 빨리 확보하십시오.
패킷 버퍼 보호	PAN-OS 10.0부터 패킷 버퍼 보호는 기본적으로 전역 및 각 영역에서 활성화됩니다. 모범 사례로 패킷 버퍼 보호를 전역 및 각 영역에서 활성화하여 DoS 공격과 공격적인 세션 및 소스로부터 방화벽 버퍼를 보호하십시오. 이 옵션은 시스템 리소스를 백업하고 합법적인 트래픽을 삭제하는 공격이나 악의적인 트래픽으로부터 방화벽의 수신 버퍼를 보호합니다. 패킷 버퍼 보호는 문제가 되는 세션을 식별하고 RED(Random Early Detection)를 첫 번째 방어선으로 사용하며 남용이 계속되면 세션을 삭제하거나 문제가 되는 IP 주소를 차단합니다. 방화벽이 특정 IP 주소에서 많은 소규모 세션이나 빠른 세션 생성(또는 둘 다)을 감지하면 해당 IP 주소를 차단합니다. 방화벽 패킷 버퍼 사용률의 기준 측정을 수행하여 방화벽 용량을 이해하고 공격만 버퍼 사용을 크게 증가시키도록 방화벽이 적절하게 구성되었는지 확인합니다. • 경고**(%)** - 패킷 버퍼 사용률이 10초 이상 이 임계값을 초과하면 방화벽이 1분마다 로그 이벤트를 생성합니다. 방화벽은 패킷 버퍼 보호가 전역적으로 활성화된 경우 로그 이벤트를 생성합니다(범위는 0% ~ 99%, 기본값은 50%). 값이 0%이면 방화벽이 로그 이벤트를 생성하지 않습니다. 기본 임계값으로 시작하여 필요에 따라 조정합니다. • 활성화**(%)** - 이 임계값에 도달하면 방화벽이 가장 악의적인 세션을 완화하기 시작합니다(범위는 0%~99%, 기본값은 80%). 값이 0%이면 방화벽이 RED를 적용하지 않습니다. 기본 임계값으로 시작하여 필요에 따라 조정합니다.

세션 설정	설명
패킷 버퍼 보호(계속)	• (PAN-OS 10.0 이상 릴리스를 실행하는 하드웨어 방화벽) 사용률(위에 설명됨)을 기반으로 하는 패킷 버퍼 보호의 대안으로, 대신 버퍼링 지연 시간 기반을 활성화하고 다음 설정을 구성하여 CPU 처리 지연 시간을 기반으로 패킷 버퍼 보호를 트리거할 수 있습니다. • 대기 시간 경고(밀리초) - 대기 시간이 이 임계값을 초과하면 방화벽이 1분마다 경고 로그 이벤트를 생성하기 시작합니다(범위는 1~20,000, 기본값은 50). • 대기 시간 활성화(밀리초) - 대기 시간이 이 임계값을 초과하면 방화벽이 수신 패킷에 대해 RED(임의 조기 감지)를 활성화하고 10초마다 활성화 로그를 생성하기 시작합니다(범위는 1 - 20,000, 기본값은 200). • 최대 허용 지연 시간(밀리초) - 지연 시간이 이 임계값과 같거나 초과하는 경우 방화벽은 100% 드롭 확률에 가까운 RED를 사용합니다(범위는 1~20,000ms, 기본값은 500ms). 현재 대기 시간이 활성화 대기 시간 임계값과 최대 허용 대기 시간 임계값 사이의 값이면 방화벽은 (현재 대기 시간 - 활성화 대기 시간 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.
패킷 버퍼 보호(계속)	• 차단 보류 시간(초) - 세션이 삭제되거나 소스 IP 주소가 차단되기 전에 세션을 계속할 수 있는 시간(초)입니다(범위는 0 ~ 65,535, 기본값은 60). 이 타이머는 RED 완화 세션을 모니터링하여 버퍼 사용률이나 대기 시간이 구성된 임계값 이상으로 계속 올라가고 있는지 확인합니다. 블록 보류 시간 이후에도 남용 행위가 계속되면 세션이 삭제됩니다. 값이 0이면 방화벽은 패킷 버퍼 보호를 기반으로 세션을 삭제하지 않습니다. 기본값으로 시작하여 패킷 버퍼 사용률 또는 대기 시간을 모니터링하고 필요에 따라 시간 값을 조정합니다. • 차단 기간(초) - 삭제된 세션이 삭제된 상태로 유지되거나 차단된 IP 주소가 차단된 상태로 유지되는 시간(초)입니다(범위는 1~15,999,999, 기본값은 3,600). 1시간 동안 IP 주소를 차단하는 것이 비즈니스 상황에 지나치게 심각한 불이익이 아닌 경우 기본값을 사용하십시오. 이 경우 기간을 줄일 수 있습니다. 패킷 버퍼 사용률 또는 대기 시간을 모니터링하고 필요에 따라 기간을 조정합니다.

세션 설정	설명
	*NAT(Network Address Translation)*는 패킷 버퍼 활용도를 높일 수 있습니다. 이것이 버퍼 사용에 영향을 미치는 경우 블록 유지 시간을 줄여 개별 세션을 더 빠르게 차단하고 기본 *IP* 주소의 다른 세션이 부당하게 불이익을 받지 않도록 차단 기간을 줄입니다.
멀티캐스트 경로 설정 버퍼링	멀티캐스트 경로 설정 버퍼링을 활성화하려면 이 옵션(기본적으로 비활성화됨)을 선택합니다. 그러면 해당 멀티캐스트 그룹에 대한 멀티캐스트 경로 또는 FIB(Forwarding Information Base) 항목이 아직 존재하지 않을 때 방화벽이 멀티캐스트 세션의 첫 번째 패킷을 보존할 수 있습니다. 기본적으로 방화벽은 새 세션에서 첫 번째 멀티캐스트 패킷을 버퍼링하지 않습니다. 대신 첫 번째 패킷을 사용하여 멀티캐스트 경로를 설정합니다. 이는 멀티캐스트 트래픽에 대해 예상되는 동작입니다. 콘텐츠 서버가 방화벽에 직접 연결되어 있고 사용자 지정 애플리케이션이 세션의 첫 번째 패킷이 삭제되는 것을 견딜 수 없는 경우에만 멀티캐스트 경로 설정 버퍼링을 활성화해야 합니다.
멀티캐스트 경로 설정 버퍼 크기	멀티캐스트 경로 설정 버퍼링을 활성화하면 흐름당 버퍼 크기를 지정하는 버퍼 크기를 조정할 수 있습니다(범위는 1~2,000, 기본값은 1,000). 방화벽은 최대 5,000개의 패킷을 버퍼링할 수 있습니다.

세션 타임아웃

일부 세션 타임아웃은 세션에서 비활성 후 PAN-OS가 방화벽에서 세션을 유지하는 기간을 정의합니다. 기본적으로 프로토콜의 세션 타임아웃이 만료되면 PAN-OS는 세션을 닫습니다. Discard 세션 타임아웃은 PAN-OS가 보안 정책 규칙에 따라 세션을 거부한 후 세션이 열려 있는 최대 시간을 정의합니다.

방화벽에서 특히 TCP, UDP, ICMP 및 SCTP 세션에 대한 타임아웃 수를 정의할 수 있습니다. 기본 타임아웃은 다른 유형의 세션에 적용됩니다. 이러한 모든 타임아웃은 전역적이며, 이는 방화벽에서 해당 유형의 모든 세션에 적용됨을 의미합니다.

전역 설정 외에도 개체 > 애플리케이션 탭에서 개별 애플리케이션에 대한 타임아웃을 유연하게 정의할 수 있습니다. 해당 애플리케이션에 사용할 수 있는 타임아웃이 옵션 창에 나타납니다. 방화벽은 설정됨 상태의 애플리케이션에 애플리케이션 타임아웃을 적용합니다. 구성된 경우 애플리케이션의 타임아웃은 전역 TCP, UDP 또는 SCTP 세션 타임아웃보다 우선합니다.

이 섹션의 옵션을 사용하여 특히 TCP, UDP, ICMP, SCTP 및 기타 모든 유형의 세션에 대한 전역 세션 타임아웃 설정을 구성합니다.

기본값은 최적 값이며 가장 좋은 방법은 기본값을 사용하는 것입니다. 그러나 네트워크 요구 사항에 따라 수정할 수 있습니다. 값을 너무 낮게 설정하면 사소한 네트워크 지연에 민감하게 반응할 수 있으며 방화벽과의 연결 설정에 실패할 수 있습니다. 값을 너무 높게 설정하면 오류 감지가 지연될 수 있습니다.

세션 타임아웃 설정	설명
기본	비 TCP/UDP, 비 SCTP 또는 비 ICMP 세션이 응답 없이 열릴 수 있는 최대 시간(초)입니다(범위는 1~15,999,999, 기본값은 30).
기본값 무시	방화벽에 구성된 보안 정책 규칙에 따라 PAN-OS가 세션을 거부한 후 비 TCP/UDP/SCTP 세션이 열린 상태로 유지되는 최대 시간(초)입니다(범위는 1~15,999,999, 기본값은 60).
TCP 폐기	방화벽에 구성된 보안 정책 규칙에 따라 PAN-OS가 세션을 거부한 후 TCP 세션이 열려 있는 최대 시간(초)입니다(범위는 1~15,999,999, 기본값은 90).
UDP 폐기	PAN-OS가 방화벽에 구성된 보안 정책 규칙에 따라 세션을 거부한 후 UDP 세션이 열려 있는 최대 시간(초)입니다(범위는 1~15,999,999, 기본값은 60).
ICMP	ICMP 응답 없이 ICMP 세션을 열 수 있는 최대 시간(범위는 1~15,999,999, 기본값은 6)입니다.
스캔	방화벽이 세션을 지우고 세션이 사용하고 있던 버퍼 리소스를 복구하기 전에 세션이 비활성화될 수 있는 최대 시간(초)입니다. 비활성 시간은 세션이 패킷 또는 이벤트에 의해 마지막으로 새로 고쳐진 이후 경과된 시간의 길이입니다. 범위는 5~30이고, 기본값은 10입니다.
TCP	TCP 세션이 설정됨 상태(핸드쉐이크가 완료된 후 및/또는 데이터 전송이 시작된 후)에 있은 후 응답 없이 TCP 세션이 열려 있는 최대 시간입니다. (범위는 1~15,999,999, 기본값은 3,600)
TCP 핸드쉐이크	세션을 완전히 설정하기 위해 SYN-ACK 수신과 후속 ACK 사이의 최대 시간(초)입니다(범위는 1~60, 기본값은 10).
TCP 초기화	TCP 핸드쉐이크 타이머를 시작하기 전에 SYN과 SYN-ACK를 수신하는 사이의 최대 시간(초)입니다(범위는 1~60, 기본값은 5).
TCP 반 폐쇄	첫 번째 FIN 수신과 두 번째 FIN 또는 RST 수신 사이의 최대 시간(초)입니다(범위는 1~604,800, 기본값은 120).
TCP 시간 대기	두 번째 FIN 또는 RST(범위는 1~600, 기본값은 15)를 수신한 후의 최대 시간(초)입니다.
확인되지 않은 RST	확인할 수 없는 RST를 수신한 후의 최대 시간(초)(RST가 TCP 창 내에 있지만 예기치 않은 시퀀스 번호가 있거나 RST가 비대칭 경로에 있음, 범위는 1 ~ 600, 기본값은 30).

세션 타임아웃 설정	설명
UDP	UDP 응답 없이 UDP 세션이 열려 있는 최대 시간(초)입니다(범위는 1~1,599,999, 기본값은 30).
인증 포털	인증 포털 웹 양식의 인증 세션 타임아웃(기본값은 30, 범위는 1~1,599,999)입니다. 요청된 콘텐츠에 액세스하려면 사용자가 이 양식에 인증 자격 증명을 입력하고 성공적으로 인증되어야 합니다. 인증 포털 웹 양식의 인증 세션 타임아웃(기본값은 30, 범위는 1~1,599,999)입니다. 요청된 콘텐츠에 액세스하려면 사용자가 이 양식에 인증 자격 증명을 입력하고 성공적으로 인증되어야 합니다.
SCTP INIT	방화벽이 SCTP 연결 시작을 중지하기 전에 방화벽이 INIT ACK 청크를 수신해야 하는 SCTP INIT 청크를 수신한 후부터의 최대 시간(초)입니다(범위는 1~60, 기본값은 5).
SCTP 쿠키	방화벽이 SCTP 연결 시작을 중지하기 전에 방화벽이 쿠키와 함께 COOKIE ECHO 청크를 수신해야 하는 상태 COOKIE 매개변수가 있는 SCTP INIT ACK 청크를 수신한 후의 최대 시간(초)(범위는 1~600, 기본값은 60).
SCTP 폐기	PAN-OS가 방화벽에 구성된 보안 정책 규칙에 따라 세션을 거부한 후 SCTP 연결이 열린 상태로 유지되는 최대 시간(초)입니다(범위는 1~604,800, 기본값은 30).
SCTP	연결의 모든 세션이 타임아웃되기 전에 연결에 대한 SCTP 트래픽 없이 경과할 수 있는 최대 시간(초)입니다(범위는 1 - 604,800, 기본값은 3,600).
SCTP 종료	방화벽이 SHUTDOWN 청크를 무시하기 전에 SCTP SHUTDOWN 청크 이후 SHUTDOWN ACK 청크를 수신하기 위해 방화벽이 대기하는 최대 시간(초)입니다(범위는 1~600, 기본값은 30).

TCP 설정

다음 표에서는 TCP 설정에 대해 설명합니다.

TCP 설정	설명
TCP out-of-order queue를 초과하는 포워딩 세그먼트	방화벽이 세션당 TCP 비순차 대기열 제한인 64를 초과하는 세그먼트를 포워딩하도록 하려면 이 옵션을 선택하십시오. 이 옵션을 비활성화하면 방화벽은 순서가 잘못된 대기열 제한을 초과하는 세그먼트를 삭제합니다. 이 옵션을 활

TCP 설정	설명
	성화한 결과 방화벽이 삭제한 세그먼트 수를 보려면 다음 CLI 명령을 실행하십시오. `show counter global tcp_exceed_flow_seg_limit` 이 옵션은 기본적으로 비활성화되어 있으며 가장 안전한 배포를 위해 이 방식을 유지해야 합니다. 이 옵션을 비활성화하면 잘못된 순서로 *64*개 이상의 세그먼트를 수신한 특정 스트림의 대기 시간이 늘어날 수 있습니다. *TCP* 스택이 누락된 세그먼트 재전송을 처리해야 하므로 연결 손실이 없어야 합니다.
Challenge ACK 허용 / SYN에 대한 응답으로 임의의 ACK 허용	서버가 SYN/ACK 대신 ACK를 사용하여 클라이언트 SYN에 응답하는 경우 인증 확인 ACK(임의 ACK라고도 함) 에 대한 응답을 허용하려면 이 옵션을 활성화합니다. 예를 들어 공격 완화를 위해 서버에서 인증 확인 ACK를 보낼 수 있으며 방화벽에서 이 설정을 사용하도록 설정하면 클라이언트와 서버 간의 통신이 가능하므로 핸드셰이크가 상태를 벗어나거나 순서를 벗어난 경우에도 챌린지 ACK 프로세스를 완료할 수 있습니다.
null 타임스탬프 옵션이 있는 세그먼트 삭제	TCP 타임스탬프는 세그먼트가 전송된 시간을 기록하고 방화벽이 타임스탬프가 해당 세션에 유효한지 확인할 수 있도록 하여 TCP 시퀀스 번호 래핑을 방지합니다. TCP 타임스탬프는 왕복 시간을 계산하는 데도 사용됩니다. 이 옵션이 활성화되면 방화벽은 null 타임스탬프가 있는 패킷을 삭제합니다. 이 옵션을 활성화한 결과 방화벽이 삭제한 세그먼트 수를 보려면 다음 CLI 명령을 실행하십시오. `show counter global tcp_invalid_ts_option` 이 옵션은 기본적으로 활성화되어 있으며 가장 안전한 배포를 위해 이 방식을 유지해야 합니다. 이 옵션을 활성화해도 성능이 저하되지 않아야 합니다. 그러나 네트워크 스택이 *null TCP* 타임스탬프 옵션 값으로 세그먼트를 잘못 생성하는 경우 이 옵션을 활성화하면 연결 문제가 발생할 수 있습니다.
비대칭 경로	동기화되지 않은 ACK 또는 윈도우 외 시퀀스 번호가 포함된 패킷을 삭제할지 아니면 우회할지 전역적으로 설정합니다. • 삭제 - 비대칭 경로가 포함된 패킷을 삭제합니다.

TCP 설정	설명
	• 우회 - 비대칭 경로가 포함된 패킷에 대한 스캔을 우회합니다. 개별 영역 보호 프로파일에 대한 설정을 제어하려면 TCP 드롭에서 비대칭 경로 설정을 변경하십시오.
긴급 데이터 플래그	방화벽이 TCP 헤더에서 긴급 포인터(URG 비트 플래그)를 허용하는지의 여부를 구성하려면 이 옵션을 사용합니다. TCP 헤더의 긴급 포인터는 즉각적인 처리를 위해 패킷을 승격하는 데 사용됩니다. 방화벽은 처리 대기열에서 패킷을 제거하고 호스트의 TCP/IP 스택을 통해 신속하게 처리합니다. 이 프로세스를 대역 외 처리라고 합니다. 긴급 포인터의 구현은 호스트마다 다르기 때문에 이 옵션을 지우기로 설정하면 대역 외 처리를 허용하지 않아 모호성이 제거되어 페이로드의 대역 외 바이트가 페이로드의 일부가 되고, 패킷이 긴급하게 처리되지 않습니다. 또한 지우기 설정은 방화벽이 프로토콜 스택의 정확한 스트림을 패킷의 대상이 되는 호스트로 인식하도록 합니다. 이 옵션이 지우기로 설정된 경우 방화벽이 URG 플래그를 지운 세그먼트 수를 보려면 다음 CLI 명령을 실행하십시오. `show counter global tcp_clear_urg` 기본적으로 이 플래그는 지우기로 설정되며 가장 안전한 배포를 위해 이 상태를 유지해야 합니다. 이로 인해 성능이 저하되어서는 안 됩니다. 텔넷과 같은 애플리케이션이 긴급 데이터 기능을 사용하는 드문 경우지만 *TCP*가 영향을 받을 수 있습니다. 이 플래그를 ***Do Not Modify***로 설정하면 방화벽은 *TCP* 헤더에 *URG* 비트 플래그가 있는 패킷을 허용하고 대역 외 처리를 활성화합니다*(*권장하지 않음*)*.
플래그 없이 세그먼트 삭제	플래그가 설정되지 않은 잘못된 TCP 세그먼트는 콘텐츠 검사를 회피하는 데 사용할 수 있습니다. 이 옵션이 활성화되면(기본값) 방화벽은 TCP 헤더에 플래그가 설정되지 않은 패킷을 삭제합니다. 이 옵션의 결과로 방화벽이 삭제한 세그먼트 수를 보려면 다음 CLI 명령을 실행하십시오. `show counter global tcp_flag_zero`

TCP 설정	설명
	이 옵션은 기본적으로 활성화되어 있으며 가장 안전한 배포를 위해 이 방식을 유지해야 합니다. 이 옵션을 활성화해도 성능이 저하되지 않아야 합니다. 그러나 네트워크 스택이 *TCP* 플래그가 없는 세그먼트를 잘못 생성하는 경우 이 옵션을 활성화하면 연결 문제가 발생할 수 있습니다.
스트립 MPTCP 옵션	(다중 경로 TCP) MPTCP 연결을 표준 TCP 연결로 변환하기 위해 기본적으로 전역적으로 활성화됩니다. *MCTCP*를 허용하려면 TCP 드롭에서 다중 경로 ***TCP(MPTCP)*** 옵션 설정을 변경합니다.
SIP TCP 일반 텍스트	분할된 SIP 헤더가 감지될 때 SIP TCP 세션에 대한 일반 텍스트 프록시 동작을 설정하려면 다음 옵션 중 하나를 선택합니다. • 항상 끄기 - 일반 텍스트 프록시를 비활성화합니다. SIP 메시지 크기가 일반적으로 MSS보다 작고 SIP 메시지가 단일 세그먼트에 맞는 경우 또는 TCP 프록시 리소스가 SSL 포워딩 프록시 또는 HTTP/2로 예약되어 있는지 확인해야 하는 경우 프록시를 비활성화합니다. • 항상 활성화됨 - 기본값입니다. 모든 SIP over TCP 세션에 대해 TCP 프록시를 사용하여 적절한 ALG 작업을 위한 TCP 세그먼트의 올바른 재조립 및 순서를 지원합니다. • 필요시 자동으로 프록시 활성화 - 이 옵션을 선택하면 ALG가 SIP 메시지 조각화를 감지하는 세션에 대해 일반 텍스트 프록시가 자동으로 활성화됩니다. SSL 포워딩 프록시 또는 HTTP/2에도 사용되는 경우 프록시를 최적화하는 데 도움이 됩니다.
TCP 재전송 스캔 (PAN-OS 9.0 이상)	활성화된 경우 재전송된 패킷이 표시될 때 원래 패킷의 검사합이 스캔됩니다. 소스 패킷과 재전송된 패킷의 검사합이 다른 경우 재전송된 패킷은 악성으로 간주되어 삭제됩니다.

복호화 설정: 인증서 해지 확인

세션을 선택한 다음 복호화 설정에서 인증서 해지 확인을 선택하여 다음 표에 설명된 매개변수를 설정합니다.

세션 기능: 인증서 해지 확인 설정	설명
활성화: CRL	CRL(인증서 해지 목록) 방법을 사용하여 인증서 해지 상태를 확인하려면 이 옵션을 선택합니다. OCSP(온라인 인증서 상태 프로토콜)도 활성화하면 방화벽이 먼저 OCSP를 시도합니다. OCSP 서버를 사용할 수 없는 경우 방화벽은 CRL 방법을 시도합니다. 복호화 인증서에 대한 자세한 내용은 복호화를 위한 키 및 인증서를 참조하십시오.
수신 타임아웃: CRL	인증서 해지 상태를 확인하기 위해 CRL 방법을 활성화한 경우 방화벽이 CRL 서비스의 응답을 기다리는 것을 중지하는 인터벌(1~60초, 기본값은 5)을 지정합니다.
활성화: OCSP	OCSP를 사용하여 인증서 해지 상태를 확인하려면 이 옵션을 선택합니다.
수신 타임아웃: OCSP	인증서 해지 상태를 확인하기 위해 OCSP 방법을 활성화한 경우 방화벽이 OCSP 응답자의 응답을 기다리는 것을 중지하는 인터벌(1~60초, 기본값은 5)을 지정합니다.
알 수 없는 인증서 상태의 세션 차단	OCSP 또는 CRL 서비스가 알 수 없는 인증서 해지 상태를 반환할 때 SSL/TLS 세션을 차단하려면 이 옵션을 선택합니다. 그렇지 않으면 방화벽이 세션을 진행합니다.
인증서 상태 확인 타임아웃 시 세션 차단	방화벽이 CRL 또는 OCSP 요청 타임아웃을 등록한 후 SSL/TLS 세션을 차단하려면 이 옵션을 선택합니다. 그렇지 않으면 방화벽이 세션을 진행합니다.
인증서 상태 타임아웃	방화벽이 인증서 상태 서비스의 응답 대기를 중지하고 선택적으로 정의한 세션 차단 로직을 적용하는 인터벌(1~60초, 기본값은 5)을 지정합니다. 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.

세션 기능: 인증서 해지 확인 설정	설명
	• CRL만 활성화하는 경우 - 방화벽은 인증서 상태 타임아웃 값 또는 CRL 수신 타임아웃 값 중 작은 인터벌이 지난 후 요청 타임아웃을 등록합니다.

복호화 설정: 포워딩 프록시 서버 인증서 설정

복호화 설정(세션 탭)에서 **SSL** 포워딩 프록시 설정을 선택하여 SSL/TLS 포워딩 프록시 복호화를 위한 세션을 설정할 때 방화벽이 클라이언트에 제공하는 인증서의 **RSA** 키 크기 또는 **ECDSA** 키 크기 및 해싱 알고리즘을 구성합니다. 다음 표에서는 매개변수에 대해 설명합니다.

세션 기능: 포워딩 프록시 서버 인증서 설정	

RSA 키 크기	다음 중 하나를 선택합니다.
	• 대상 호스트에 의해 정의됨(기본값) - 방화벽이 대상 서버가 사용하는 키를 기반으로 인증서를 생성하도록 하려면 이 옵션을 선택합니다.
	  • 대상 서버가 RSA 1,024비트 키를 사용하는 경우 방화벽은 해당 키 크기와 SHA1 해싱 알고리즘을 사용하여 인증서를 생성합니다.
	  • 대상 서버가 1,024비트보다 큰 키 크기(예: 2,048비트 또는 4,096비트)를 사용하는 경우 방화벽은 2,048비트 키와 SHA-256 알고리즘을 사용하는 인증서를 생성합니다.
	• **1024**비트 **RSA** - 대상 서버가 사용하는 키 크기에 관계없이 방화벽이 RSA 1,024비트 키와 SHA-256 해싱 알고리즘을 사용하는 인증서를 생성하도록 하려면 이 옵션을 선택합니다. 2013년 12월 31일부로 공용 CA(인증 기관) 및 널리 사용되는 브라우저는 2,048비트 미만의 키를 사용하는 X.509 인증서를 제한적으로 지원합니다. 앞으로는 보안 설정에 따라 브라우저가 사용자에게 경고하거나 이러한 키가 제공될 때 SSL/TLS 세션을 완전히 차단할 수 있습니다.
	• **2048**비트 **RSA** - 대상 서버가 사용하는 키 크기에 관계없이 방화벽이 RSA 2,048비트 키와 SHA-256 해싱 알고리즘을 사용하는 인증서를 생성하도록 하려면 이 옵션을 선택합니다. 공용 CA 및 널리 사용되는 브라우저는 1,024비트 키보다 더 나은 보안을 제공하는 2,048비트 키를 지원합니다.

ECDSA 키 크기	다음 중 하나를 선택합니다.

세션 기능: 포워딩 프록시 서버 인증서 설정	

	• 대상 호스트에 의해 정의됨(기본값) - 방화벽이 대상 서버가 사용하는 키를 기반으로 인증서를 생성하도록 하려면 이 옵션을 선택합니다.
	  • 대상 서버가 ECDSA 256비트 또는 384비트 키를 사용하는 경우 방화벽은 해당 키 크기의 인증서를 생성합니다.
	  • 대상 서버가 384비트보다 큰 키 크기를 사용하는 경우 방화벽은 521비트 키를 사용하는 인증서를 생성합니다.
	• **256**비트 **ECDSA** - 대상 서버가 사용하는 키 크기에 관계없이 방화벽이 ECDSA 256비트 키를 사용하는 인증서를 생성하도록 하려면 이 옵션을 선택합니다.
	• **384**비트 **ECDSA** - 대상 서버가 사용하는 키 크기에 관계없이 방화벽이 ECDSA 384비트 키를 사용하는 인증서를 생성하도록 하려면 이 옵션을 선택합니다.

복호화 설정: SSL 복호화 설정

사용자가 복호화된 HTTPS 연결을 통해 웹사이트를 탐색할 때 SSL/TLS 핸드쉐이크 검사를 활성화하려면 **SSL** 복호화 설정을 선택합니다. 방화벽의 CTD(콘텐츠 및 위협 탐지) 엔진은 보안 정책 규칙에 대해 핸드쉐이크의 콘텐츠를 평가하여 방화벽이 세션 초기에 규칙을 시행할 수 있도록 합니다. 이 기능을 사용하려면 URL 필터링 구독이 있어야 하고 SSL 포워딩 프록시 또는 SSL 인바운드 검사를 구성하고 보안 정책 규칙에서 특정 URL 카테고리를 차단해야 합니다.

SSL/TLS 핸드쉐이크 검사 중에 차단된 사이트에 대해서는 *URL* 필터링 응답 페이지가 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.

SSL 복호화 설정	설명
검사를 위해 CTD에 핸드쉐이크 메시지 보내기	복호화된 웹 세션 중에 CTD가 SSL/TLS 핸드쉐이크를 검사하도록 하려면 선택합니다.

VPN 세션 설정

세션을 선택한 다음 VPN 세션 설정에서 VPN 세션을 설정하는 방화벽과 관련된 전역 설정을 구성합니다. 다음 표에서는 설정에 대해 설명합니다.

VPN 세션 설정	설명
쿠키 활성화 임계값	쿠키 유효성 검사가 트리거되는 방화벽당 허용되는 최대 IKEv2 반-개방 IKE SA 수를 지정합니다. 반쯤 열린 IKE SA의 수가 쿠키 활성화 임계값을 초과하면 응답자는 쿠키를 요청하고 이니시에이터는 쿠키가 포함된 IKE_SA_INIT로 응답해야 합니다. 쿠키 유효성 검사에 성공하면 다른 SA 세션을 시작할 수 있습니다. 값 0은 쿠키 유효성 검사가 항상 켜져 있음을 의미합니다. 쿠키 활성화 임계값은 전역 방화벽 설정이며 최대 반-열림 SA 설정보다 낮아야 합니다.
최대 절반 열림 SA	이니시에이터가 응답을 받지 않고 방화벽에 보낼 수 있는 IKEv2 반-개방 IKE SA의 최대 수를 지정합니다. 최대값에 도달하면 방화벽은 새 IKE_SA_INIT 패킷에 응답하지 않습니다(범위는 1~65535, 기본값은 65535).
최대 캐시된 인증서	방화벽이 캐시할 수 있는 HTTP를 통해 검색된 피어 인증 기관(CA) 인증서의 최대 수를 지정합니다. 이 값은 IKEv2 해시 및 URL 기능에서만 사용됩니다(범위는 1~4000, 기본값은 500).

디바이스 > 설정 > ACE

App-ID ACE(Cloud Engine)를 활성화 또는 비활성화합니다. ACE는 기본적으로 비활성화되어 있습니다. ACE를 사용하려면 확인란을 클릭하여 ACE가 비활성화되지 않도록 합니다.

*ACE*를 사용하려면 방화벽에 유효한 *SaaS* 보안 인라인 라이선스가 있어야 합니다. 방화벽에 *SaaS* 보안 인라인 라이선스가 없는 경우 해당 방화벽은 *ACE App-ID*를 설치하거나 보안 정책에서 사용할 수 없습니다. *Panorama*는 *ACE*를 사용하는 방화벽을 관리하기 위해 라이선스가 필요하지 않습니다.

디바이스 > 설정 > DLP

- 디바이스 > 설정 > **DLP**

엔터프라이즈 DLP(데이터 손실 방지) 클라우드 서비스로 스캔한 파일에 대한 네트워크 설정을 구성합니다.

필드	설명
최대 지연 시간(초)	방화벽에서 작업을 수행하기 전에 파일 업로드에 대한 최대 대기 시간(**1**~**240**초)을 지정합니다. 기본값은 **60**입니다.
최대 대기 시간에 대한 조치	파일 업로드 대기 시간이 구성된 최대 대기 시간에 도달할 때 방화벽이 수행하는 작업을 지정합니다. • 허용(기본값) - 방화벽은 최대 지연 시간에 도달했을 때 DLP 클라우드 서비스에 대한 파일 업로드를 계속할 수 있도록 허용합니다. • 차단 - 방화벽은 구성된 최대 지연 시간에 도달하는 DLP 클라우드 서비스로의 파일 업로드를 차단합니다.
최대 파일 크기(MB)	DLP 클라우드 서비스에 업로드할 최대 파일 크기(**1**~**20**)를 적용합니다. 기본값은 **20**입니다.
최대 파일 크기에 대한 조치	파일 업로드가 구성된 최대 파일 크기에 도달할 때 방화벽이 수행하는 작업을 지정합니다. • 허용(기본값) - 방화벽은 파일이 구성된 최대 파일 크기인 경우 DLP 클라우드 서비스에 대한 파일 업로드를 계속하도록 허용합니다. • 차단 - 방화벽은 파일이 구성된 최대 파일 크기인 경우 DLP 클라우드 서비스로의 파일 업로드를 차단합니다.
스캔되지 않은 로그 파일	파일을 DLP 클라우드 서비스에 업로드할 수 없을 때 데이터 필터링 로그에 경고를 생성하려면 선택(활성화)합니다.
모든 오류에 대한 조치	DLP 클라우드 서비스에 파일을 업로드하는 동안 오류가 발생할 때 방화벽이 수행하는 작업을 지정합니다. • 허용(기본값) - 방화벽은 업로드 중에 오류가 발생하는 경우 파일 업로드가 DLP 클라우드 서비스로 계속되도록 허용합니다.

필드	설명
	• 차단 - 방화벽은 업로드 중에 오류가 발생하는 경우 DLP 클라우드 서비스에 대한 파일 업로드를 차단합니다.

디바이스 > 고가용성

- 디바이스 > 고가용성

이중화를 위해 HA 쌍 또는 HA 클러스터의 고가용성 구성에 Palo Alto Networks 차세대 방화벽을 배포하십시오. 2개의 HA 방화벽이 HA 쌍으로 작동하는 경우 2개의 HA 배포가 있습니다.

- 능동형/수동형 - 이 배포에서 활성 피어는 두 개의 전용 인터페이스를 통해 구성 및 세션 정보를 수동 피어와 지속적으로 동기화합니다. 능동형 방화벽에서 하드웨어 또는 소프트웨어 중단이 발생하는 경우 수동 방화벽은 서비스 손실 없이 자동으로 활성 상태가 됩니다. 능동형/수동형 HA 배포는 가상 와이어, 레이어 2 또는 레이어 3과 같은 모든 인터페이스 모드에서 지원됩니다.
- 능동형/능동형 - 이 배포에서는 두 HA 피어가 모두 활성 상태이고 트래픽을 처리합니다. 이러한 배포는 비대칭 라우팅과 관련된 시나리오 또는 동적 라우팅 프로토콜(OSPF, BGP)이 두 피어에서 활성 상태를 유지하도록 허용하려는 경우에 가장 적합합니다. 능동형/능동형 HA는 가상 와이어 및 레이어 3 인터페이스 모드에서만 지원됩니다. HA1 및 HA2 링크 외에도 능동형/능동형 배포에는 전용 HA3 링크가 필요합니다. HA3 링크는 세션 설정 및 비대칭 트래픽 처리를 위한 패킷 포워딩 링크로 사용됩니다.

  HA 쌍에서 두 피어는 모두 동일한 모델이어야 하고 동일한 *PAN-OS* 및 콘텐츠 릴리스 버전을 실행해야 하며 동일한 라이선스 세트를 가지고 있어야 합니다.

  또한 *VM* 시리즈 방화벽의 경우 두 피어가 동일한 하이퍼바이저에 있어야 하며 각 피어에 할당된 *CPU* 코어 수가 동일해야 합니다.

지원되는 방화벽 모델에서 데이터 센터 내부 및 데이터 센터 간의 세션 지속성을 위해 HA 방화벽 클러스터를 생성할 수 있습니다. 링크가 다운되면 세션이 클러스터의 다른 방화벽으로 페일오버됩니다. 이러한 동기화는 HA 피어가 여러 데이터 센터에 분산되어 있거나 활성 데이터 센터와 대기 데이터 센터 간에 분산되어 있는 사용 사례에서 유용합니다. 또 다른 사용 사례는 보안을 확장하고 세션 생존성을 보장하기 위해 HA 클러스터 구성원을 단일 데이터 센터에 추가하는 수평적 확장입니다. HA 쌍은 HA 클러스터에 속할 수 있으며 클러스터에서 두 개의 방화벽으로 계산됩니다. HA 클러스터에서 지원되는 방화벽의 수는 방화벽 모델에 따라 다릅니다.

- HA 구성을 위한 중요 고려 사항
- HA 일반 설정
- HA 커뮤니케이션
- HA 링크 및 경로 모니터링
- HA 능동형/능동형 구성
- 클러스터 구성

HA 구성을 위한 중요 고려 사항

다음은 HA 쌍을 구성하기 위한 중요한 고려 사항입니다.

- 로컬 및 피어 IP에 사용되는 서브넷은 가상 라우터의 다른 곳에서 사용하면 안 됩니다.

- OS 및 콘텐츠 릴리스 버전은 각 방화벽에서 동일해야 합니다. 불일치로 인해 피어 방화벽이 동기화되지 않을 수 있습니다.
- 능동형 방화벽의 경우 HA 포트의 LED는 녹색이고 수동 방화벽의 경우 황색입니다.
- 로컬 및 피어 방화벽의 구성을 비교하려면 왼쪽 선택 상자에서 원하는 로컬 구성을 선택한 다음 오른쪽 선택 상자에서 피어 구성을 선택하여 **Device** 탭의 **Config Audit** 도구를 사용합니다.
- 대시보드의 HA 위젯에서 구성 푸시를 클릭하여 웹 인터페이스에서 방화벽을 동기화합니다. 구성을 푸시하는 방화벽의 구성이 피어 방화벽의 구성을 덮어씁니다. 능동형 방화벽의 CLI에서 방화벽을 동기화하려면 request high-availability sync-to-remote running-config 명령을 사용합니다.

> *10*기가비트 *SFP+* 포트를 사용하는 방화벽이 있는 고가용성*(HA)* 능동형/수동형 구성에서 페일오버가 발생하고 능동형 방화벽이 수동 상태로 변경되면 *10*기가비트 이더넷 포트가 중단되었다가 다시 가져와 새로 고침을 수행합니다. 그러나 방화벽이 다시 활성화될 때까지 전송을 활성화하지 않습니다. 인접 디바이스에 모니터링 소프트웨어가 있는 경우 포트가 내려갔다가 다시 올라가기 때문에 포트가 플래핑되는 것으로 표시됩니다. 이것은 비활성화되어 여전히 전송을 허용하는 *1*기가비트 이더넷 포트와 같은 다른 포트의 동작과 다른 동작이므로 인접 디바이스에서 플래핑이 감지되지 않습니다.

HA 일반 설정

- 디바이스 > 고가용성 > 일반

고가용성(HA) 쌍 또는 HA 클러스터 구성원을 구성하려면 먼저 디바이스 > 고가용성 > 일반을 선택한 다음 일반 설정을 구성합니다.

HA 설정	설명
일반 탭	
HA 쌍 설정 - 설정	**HA** 쌍 기능을 활성화하고 다음 설정에 액세스하려면 HA 쌍을 활성화하십시오. • 그룹 **ID** - HA 쌍을 식별하는 숫자(1 ~ 63)를 입력합니다. 이 필드는 여러 HA 쌍이 동일한 브로드캐스트 도메인에 있는 경우 필수이며 고유해야 합니다. • 설명 - (선택 사항) HA 쌍에 대한 설명을 입력합니다. • 모드 - HA 배포 유형을 설정합니다. 능동형/수동형 또는 능동형/능동형. • 디바이스 **ID** - 능동형/능동형 구성에서 디바이스 ID를 설정하여 능동형-기본 피어(디바이스 **ID**를 **0**으로 설정)와 능동형-보조 피어(디바이스 **ID**를 **1**로 설정)를 결정합니다. • 구성 동기화 활성화 - 피어 간의 구성 설정 동기화를 활성화하려면 이 옵션을 선택합니다.

HA 설정	설명
	두 디바이스가 항상 동일한 구성을 갖고 동일한 방식으로 트래픽을 처리하도록 구성 동기화를 활성화합니다. • **Peer HA1 IP Address(**피어 **HA1 IP** 주소**)** - 피어 방화벽의 HA1 인터페이스 IP 주소를 입력합니다. • 백업 피어 **HA1 IP** 주소 - 피어의 백업 제어 링크에 대한 IP 주소를 입력합니다. 기본 링크가 실패할 경우 백업 링크가 방화벽을 동기화된 최신 상태로 유지하도록 백업 피어 *HA1 IP* 주소를 구성합니다.

능동형/수동형 설정	• 수동 링크 상태 - 다음 옵션 중 하나를 선택하여 수동 방화벽의 데이터 링크가 작동 상태를 유지해야 하는지의 여부를 지정합니다. 이 옵션은 AWS의 VM 시리즈 방화벽에서 사용할 수 없습니다.
	  • **Shutdown**—인터페이스 링크를 강제 종료 상태로 만듭니다. 이것은 네트워크에서 루프가 생성되지 않도록 하는 기본 옵션입니다.
	  • 자동 - 물리적 연결이 있는 링크는 물리적으로 작동 상태를 유지하지만 비활성화된 상태입니다. ARP 학습 또는 패킷 포워딩에 참여하지 않습니다. 이렇게 하면 링크를 불러오는 시간이 절약되므로 페일오버 중 수렴 시간에 도움이 됩니다. 네트워크 루프를 방지하려면 방화벽에 레이어 2 인터페이스가 구성되어 있는 경우 이 옵션을 선택하지 마십시오.
	  방화벽에 레이어 *2* 인터페이스가 구성되어 있지 않으면 수동 링크 상태를 자동으로 설정합니다.
	• **Monitor Fail Hold Down Time(**분**)** - 방화벽이 수동 상태가 되기 전에 작동하지 않는 상태가 되는 시간(분)입니다(범위는 1~60). 이 타이머는 링크 또는 경로 모니터링 실패로 인해 누락된 하트비트 또는 헬로 메시지가 있을 때 사용됩니다.

일렉션(election) 설정	다음 설정을 지정하거나 활성화합니다. • 디바이스 우선 순위 - 능동형 방화벽을 식별하기 위한 우선 순위 값을 입력합니다. 쌍의 두 방화벽에서 선점 기능이 활성화되면 값이 더 낮은(우선 순위가 높은) 방화벽이 능동형 방화벽(범위: 0 ~ 255)이 됩니다. • 선점 - 장애 복구 후 우선 순위가 더 높은 방화벽이 활성(능동형/수동형) 또는 능동형-기본(능동형/능동형) 작업을 재개할 수 있습니다. 장애 후 복구 시 더 높은 우선 순위의 방화벽이 능동형 또는 능동형-기본 작업을 재개하려면 두 방화벽 모두에서 선점 옵션을 활성화해야 합니다. 이 설정을 비활

HA 설정	설명
	성화하면 우선 순위가 더 높은 방화벽이 오류에서 복구된 후에도 우선 순위가 낮은 방화벽이 능동형 또는 능동형-기본으로 유지됩니다. 선점 옵션을 활성화할지의 여부는 비즈니스 요구 사항에 따라 다릅니다. 기본 디바이스가 활성 디바이스가 되어야 하는 경우 오류에서 복구한 후 기본 디바이스가 보조 디바이스를 선점하도록 선점을 활성화합니다. 가장 적은 수의 페일오버 이벤트가 필요한 경우 선점 옵션을 비활성화하여 페일오버 후 *HA* 쌍이 더 높은 우선 순위의 방화벽을 기본 방화벽으로 만들기 위해 다시 페일오버하지 않도록 합니다. • 하트비트 백업 - HA 방화벽의 관리 포트를 사용하여 하트비트 및 헬로 메시지에 대한 백업 경로를 제공합니다. 관리 포트 IP 주소는 HA1 제어 링크를 통해 HA 피어와 공유됩니다. 추가 구성이 필요하지 않습니다. *HA1* 및 *HA1* 백업 링크에 대역 내 포트를 사용하는 경우 하트비트 백업을 활성화합니다. *HA1* 또는 *HA1* 백업 링크에 관리 포트를 사용하는 경우 하트비트 백업을 활성화하지 마십시오.
	• **HA** 타이머 설정 - 사전 설정된 프로파일 중 하나를 선택합니다. • 권장: 일반적인 페일오버 타이머 설정에 사용합니다. 다른 설정이 필요한지 확실하지 않은 경우 권장 설정을 사용하는 것이 가장 좋습니다. • **Aggressive**: 더 빠른 장애 조치 타이머 설정에 사용합니다. 프로파일에 포함된 개별 타이머의 사전 설정 값을 보려면 고급 및 로드 권장 또는 적극적 로드를 선택합니다. 하드웨어 모델에 대한 사전 설정 값이 화면에 표시됩니다. • **Advanced**: 다음 타이머 각각에 대한 네트워크 요구 사항에 맞게 값을 사용자 지정할 수 있습니다. • 승격 보류 시간**(ms)** - 수동 피어(능동형/수동형 모드) 또는 능동형-보조 피어(능동형/능동형 모드)가 HA 피어가 손실되었습니다. 이 보류 시간은 피어 실패 선언 후에만 시작됩니다. • 헬로 인터벌**(ms)** - 다른 방화벽의 HA 프로그램이 작동하는지 확인하기 위해 보낸 헬로 패킷 사이의 시간(밀리초)입니다(범위는 8,000 ~ 60,000, 기본값은 8,000). • 하트비트 인터벌**(ms)** - HA 피어가 ICMP 핑 형식으로 하트비트 메시지를 교환하는 빈도를 지정합니다(범위는 1,000~60,000이며 기본값은 없음).

HA 설정	설명
	• **Flap Max** - 방화벽이 마지막으로 활성 상태를 떠난 후 15분 이내에 활성 상태를 벗어날 때 플랩이 계산됩니다. 방화벽이 일시 중단되고 수동 방화벽이 인계받기 전에 허용되는 최대 플랩 수를 지정합니다(범위는 0~16, 기본값은 3). 값 0은 최대값이 없음을 의미합니다(수동형 방화벽이 인계받기 전에 무한 수의 플랩이 필요함). • 선점 보류 시간**(분)** - 수동형 또는 능동형-보조 피어가 활성 또는 능동형-기본 피어로 인계받기 전에 기다리는 시간(분)입니다(범위는 1~60, 기본값은 1). • **Monitor Fail Hold Up Time(ms)** - 경로 모니터 또는 링크 모니터 실패 후 방화벽이 활성 상태를 유지하는 시간 인터벌(밀리초)입니다. 이 설정은 인접 디바이스의 간헐적인 플래핑으로 인한 HA 페일오버를 방지하기 위해 권장됩니다(범위는 0 ~ 60,000, 기본값은 0). • 추가 마스터 보류 시간**(ms)** - 모니터 장애 보류 시간과 동일한 이벤트에 적용되는 추가 시간(밀리초)입니다(범위는 0 ~ 60,000, 기본값은 500). 추가 시간 인터벌은 능동형/수동형 모드의 능동형 피어에만 적용되고 능동형/능동형 모드의 능동형-기본 피어에만 적용됩니다. 이 타이머는 두 피어 모두 동일한 링크 또는 경로 모니터 오류가 동시에 발생할 때 페일오버를 피하기 위해 권장됩니다.
SSH HA 프로파일 설정	네트워크의 고가용성(HA) 어플라이언스에 대한 SSH 세션에 적용되는 SSH 서비스 프로파일 유형입니다. 기존 HA 프로파일을 적용하려면 프로파일을 선택한 다음 확인을 클릭한 다음 변경 사항을 커밋합니다. 프로파일을 활성화하려면 *CLI*에서 *SSH* 서비스를 다시 시작해야 합니다. 자세한 내용은 디바이스 > 인증서 관리 > SSH 서비스 프로파일를 참조하십시오.
클러스터링 설정	클러스터링 설정에 액세스하려면 클러스터 참여를 활성화하십시오. HA 클러스터링을 지원하는 방화벽은 구성원 방화벽(쌍의 각 방화벽이 총계에 포함되는 개별 또는 HA 쌍)의 클러스터를 허용합니다. 방화벽 모델이 지원하는 클러스터당 구성원 수는 다음과 같습니다. • PA-3200 시리즈: 6명 • PA-5200 시리즈: 16명 • PA-5450: 8명 • PA-7080 시리즈: 4명 • PA-7050 시리즈: 6명

HA 설정	설명
	클러스터를 구성합니다. • 클러스터 **ID** - 모든 구성원이 세션 상태를 공유할 수 있는 HA 클러스터의 고유 숫자 ID입니다(범위는 1에서 99까지이며 기본값은 없습니다). • 클러스터 설명 - 클러스터에 대한 간략한 설명입니다. • 클러스터 동기화 타임아웃(분) - 다른 클러스터 구성원(예: 알 수 없는 상태)이 클러스터의 완전한 동기화를 방해할 때 로컬 방화벽이 활성 상태가 되기 전에 대기하는 최대 시간(분)입니다(범위는 0 - 30, 기본값은 0). • 모니터 장애 보류 시간(분) - 다운 링크가 백업되었는지 확인하기 위해 다운 링크를 다시 테스트하는 시간(분 범위: 1~60, 기본값은 1).
작동 명령	
로컬 디바이스 일시 중지 (또는 로컬 디바이스가 작동하도록 설정)	로컬 HA 피어를 일시 중단된 상태로 만들고 HA 기능을 일시적으로 비활성화하려면 다음 CLI 작동 명령을 사용하십시오. • **`request high-availability state suspend`** 일시 중단된 로컬 HA 피어를 다시 기능 상태로 전환하려면 CLI 작동 명령을 사용합니다. • **`request high-availability state functional`** 페일오버를 테스트하기 위해 능동형(또는 능동형-기본) 방화벽을 비활성화할 수 있습니다.

HA 커뮤니케이션

- 디바이스 > 고가용성 > HA 통신

HA 쌍 또는 HA 클러스터링에 대한 HA 링크를 구성하려면 **Device** > **High Availability** > **HA Communications**를 선택하십시오.

HA 링크	설명
제어 링크 (HA1)/제어 링크(HA1 백업)	HA 쌍의 방화벽은 HA 링크 를 사용하여 데이터를 동기화하고 상태 정보를 유지합니다. 일부 방화벽 모델에는 전용 제어 링크와 전용 백업 제어 링크가 있습니다. 예를 들어 PA-5200 시리즈 방화벽에는 HA1-A 및 HA1-B가 있습니다. 이 경우 일렉션(election) 설정에서 하트비트 백업 옵션을 활성화해야 합니다. Control Link HA 링크에 전용 HA1 포트를 사용하고 Control Link(HA 백업)에 데이터 포트를 사용하는 경우 Heartbeat 백업 옵션을 활성화하는 것이 좋습니다.

HA 링크	설명
	PA-220 방화벽과 같이 전용 HA 포트가 없는 방화벽의 경우 Control Link HA 연결용 관리 포트와 Control Link HA1 백업 연결용 HA 유형으로 구성된 데이터 포트 인터페이스를 구성해야 합니다. 이 경우 관리 포트를 사용하므로 하트비트 백업이 관리 인터페이스 연결을 통해 이미 발생하기 때문에 하트비트 백업 옵션을 활성화할 필요가 없습니다. AWS의 VM 시리즈 방화벽에서 관리 포트는 HA1 링크로 사용됩니다. *HA* 제어 링크에 데이터 포트를 사용할 때 제어 메시지는 데이터 플레인에서 *Management Plane(MP)*으로 통신해야 하므로 데이터플레인에서 장애가 발생하면 피어가 *HA* 제어 링크 정보를 전달할 수 없고 페일오버가 발생한다는 점에 유의하십시오. 전용 *HA* 포트를 사용하는 것이 가장 좋으며, 전용 *HA* 포트가 없는 방화벽에서는 관리 포트를 사용하는 것이 좋습니다.
제어 링크 (HA1)/제어 링크(HA1 백업)	기본 및 백업 HA 제어 링크에 대해 다음 설정을 지정합니다. • 포트 - 기본 및 백업 HA1 인터페이스에 대한 HA 포트를 선택합니다. 백업 설정은 선택 사항입니다. • **IPv4/IPv6** 주소 - 기본 및 백업 HA1 인터페이스에 대한 HA1 인터페이스의 IPv4 또는 IPv6 주소를 입력합니다. 백업 설정은 선택 사항입니다. *PA-3200* 시리즈 방화벽은 백업 *HA1* 인터페이스에 대해 *IPv6* 주소를 지원하지 않으며, *IPv4* 주소를 사용합니다. • 넷마스크 - 기본 및 백업 HA1 인터페이스에 대한 IP 주소(예: 255.255.255.0)의 네트워크 마스크를 입력합니다. 백업 설정은 선택 사항입니다. • 게이트웨이 - 기본 및 백업 HA1 인터페이스에 대한 기본 게이트웨이의 IP 주소를 입력합니다. 백업 설정은 선택 사항입니다. • 링크 속도 - (전용 HA 포트가 있는 모델만 해당) 전용 HA1 포트에 대한 방화벽 간의 제어 링크 속도를 선택합니다. • **Link Duplex**—(전용 HA 포트가 있는 모델만 해당) 전용 HA1 포트에 대한 방화벽 간의 제어 링크에 대해 이중 옵션을 선택합니다. • 암호화 활성화됨 - HA 피어에서 HA 키를 내보내고 이 방화벽으로 불러온 후 암호화를 활성화합니다. 이 방화벽의 HA 키도 이 방화벽에서 내보내고 HA 피어에서 가져와야 합니다. 기본 HA1 인터페이스에 대해 이 설정을 구성합니

HA 링크	설명
	다. 인증서 페이지에서 키 가져오기/내보내기(디바이스 > 인증서 관리 > 인증서 프로파일 참조). 방화벽이 직접 연결되지 않은 경우 암호화를 활성화합니다(*HA1* 연결은 트래픽을 검사, 처리 또는 캡처할 수 있는 네트워크 디바이스를 통과함). • 모니터 보류 시간**(ms)** - 제어 링크 실패로 인해 피어 실패를 선언하기 전에 방화벽이 대기하는 시간(밀리초)을 입력합니다(범위는 1,000 ~ 60,000, 기본값은 3,000). 이 옵션은 HA1 포트의 물리적 링크 상태를 모니터링합니다.
데이터 링크(HA2)	기본 및 백업 데이터 링크에 대해 다음 설정을 지정합니다. • 포트 - HA 포트를 선택합니다. 기본 및 백업 HA2 인터페이스에 대해 이 설정을 구성합니다. 백업 설정은 선택 사항입니다.

HA 링크	설명
HA2 백업 링크가 구성되면 물리적 링크 장애가 발생하면 백업 링크로 페일오버*(failover)*가 발생합니다. *HA2* 연결 유지 옵션을 활성화하면 정의된 임계값에 따라 *HA* 연결 유지 메시지가 실패하는 경우에도 페일오버가 발생합니다.	• **IP** 주소 - 기본 및 백업 HA2 인터페이스에 대한 HA 인터페이스의 IPv4 또는 IPv6 주소를 지정합니다. 백업 설정은 선택 사항입니다. • 넷마스크 - 기본 및 백업 HA2 인터페이스에 대한 HA 인터페이스의 네트워크 마스크를 지정합니다. 백업 설정은 선택 사항입니다. • 게이트웨이 - 기본 및 백업 HA2 인터페이스에 대한 HA 인터페이스의 기본 게이트웨이를 지정합니다. 백업 설정은 선택 사항입니다. 방화벽의 HA2 IP 주소가 동일한 서브넷에 있는 경우 게이트웨이 필드를 비워 두어야 합니다. • 세션 동기화 활성화 - 수동 방화벽과 세션 정보의 동기화를 활성화하고 전송 옵션을 선택합니다. 세션 동기화를 활성화하여 방화벽이 패킷을 동기화된 세션과 일치시키고 패킷을 빠르게 포워딩할 수 있도록 하는 데이터플레인에 세션을 갖도록 하십시오. 세션 동기화를 활성화하지 않으면 방화벽이 세션을 다시 생성해야 하므로 대기 시간이 발생하고 연결이 끊길 수 있습니다.

HA 링크	설명

	• 전송 - 다음 전송 옵션 중 하나를 선택합니다.
	  • 이더넷 - 방화벽이 연속적으로 연결되거나 스위치(Ethertype 0x7261)를 통해 연결될 때 사용합니다.
	  • **IP** - 레이어 3 전송이 필요할 때 사용합니다(IP 프로토콜 번호 99).
	  • **UDP** - 체크섬이 IP 옵션(UDP 포트 29281)에서와 같이 헤더만이 아니라 전체 패킷에 대해 계산된다는 사실을 활용하는 데 사용합니다. UDP 모드 사용의 이점은 세션 동기화 메시지의 무결성을 확인하기 위한 UDP 체크섬이 있다는 것입니다.
	• (전용 HA 포트가 있는 모델만 해당) 링크 속도 - 전용 HA2 포트에 대한 피어 간의 제어 링크 속도를 선택합니다.
	• (전용 HA 포트가 있는 모델만 해당) **Link Duplex** - 전용 HA2 포트에 대한 피어 간의 제어 링크에 대한 이중 옵션을 선택합니다.
	• **HA2** 연결 유지 - HA 피어 간의 HA2 데이터 링크 상태를 모니터링하려면 이 옵션을 선택하는 것이 가장 좋습니다. 이 옵션은 기본적으로 비활성화되어 있으며 한 피어 또는 두 피어에서 활성화할 수 있습니다. 활성화된 경우 피어는 연결 유지 메시지를 사용하여 HA2 연결을 모니터링하여 설정한 임계값(기본값은 10,000ms)에 따라 실패를 감지합니다. HA2 연결 유지를 활성화하면 HA2 연결 유지 복구 작업이 수행됩니다. 작업 선택:
	  • **Log Only(로그만)** - 시스템 로그에 HA2 인터페이스 오류를 중요한 이벤트로 기록합니다. 활성 피어가 유일한 방화벽 포워딩 트래픽이므로 능동형/수동형 배포에 대해 이 옵션을 선택합니다. 수동 피어가 백업 상태이며 트래픽을 포워딩하지 않습니다. 따라서 분할 데이터 경로가 필요하지 않습니다. HA2 백업 링크를 구성하지 않은 경우 상태 동기화가 해제됩니다. HA2 경로가 복구되면 정보 로그가 생성됩니다.
	  • 데이터 경로 분할 - 능동형/능동형 HA 배포에서 이 옵션을 선택하여 HA2 인터페이스 오류를 감지할 때 각 피어가 로컬 상태 및 세션 테이블의 소유권을 갖도록 지시합니다. HA2 연결이 없으면 상태 및 세션 동기화가 발생할 수 없습니다. 이 작업을 통해 세션 테이블을 별도로 관리하여 각 HA 피어가 트래픽을 성공적으로 포워딩할 수 있습니다. 이 상태를 방지하려면 HA2 백업 링크를 구성하십시오.
	• 임계값**(ms)** - 위의 작업 중 하나가 트리거되기 전에 연결 유지 메시지가 실패한 기간이고(범위는 5,000 ~ 60,000), 기본값은 10,000입니다.

클러스터링 링크	클러스터 ID가 동일한 모든 클러스터 구성원 간에 세션 상태를 동기화하는 전용 HA 클러스터 링크인 HA4 링크에 대한 설정을 구성합니다. 클러스터 구성원 간의 HA4 링크는 클러스터 구성원 간의 연결 실패를 감지합니다. • 포트 - HA4 링크가 될 HA 인터페이스를 선택합니다(예: ethernet1/1).

HA 링크	설명
	• **IPv4/IPv6** 주소 - 로컬 HA4 인터페이스의 IP 주소를 입력합니다. • 넷마스크 - 넷마스크를 입력합니다. • **HA4** 연결 유지 임계값**(ms)** - 방화벽이 클러스터 구성원이 작동 중임을 알기 위해 클러스터 구성원으로부터 연결 유지를 수신해야 하는 시간입니다(범위는 5,000 ~ 60,000, 기본값은 10,000). HA4 백업 설정 구성: • 포트 - HA4 백업 링크가 될 HA 인터페이스를 선택합니다. • **IPv4/IPv6** 주소 - 로컬 HA4 백업 링크의 주소를 입력합니다. • 넷마스크 - 넷마스크를 입력합니다.

HA 링크 및 경로 모니터링

- 디바이스 > 고가용성 > 링크 및 경로 모니터링

HA 페일오버 조건을 정의하려면 HA 링크 및 경로 모니터링을 구성하십시오.**Device** > **High Availability** > **Link** 및 경로 모니터링을 선택합니다.

*AWS*의 *VM* 시리즈 방화벽에는 링크 모니터링 및 경로 모니터링을 사용할 수 없습니다.

HA 링크 및 경로 모니터링 설정	설명
링크 모니터링	다음을 지정합니다. • 활성화됨 - 링크 모니터링을 활성화합니다. 링크 모니터링을 사용하면 물리적 링크 또는 물리적 링크 그룹이 실패할 때 페일오버를 트리거할 수 있습니다. • 실패 조건 - 모니터링되는 링크 그룹 중 일부 또는 전체가 실패할 때 페일오버가 발생하는지의 여부를 선택합니다. 경로 또는 링크가 다운될 경우 페일오버를 트리거하는 데 도움이 되도록 경로 모니터링 또는 링크 모니터링을 활성화하고 구성합니다. 경로 모니터링을 위한 하나 이상의 경로 그룹을 구성하고 링크 모니터링을 위한 하나 이상의 링크 그룹을 구성합니다.
링크 그룹	특정 이더넷 링크를 모니터링하려면 하나 이상의 링크 그룹을 정의하십시오. 링크 그룹을 추가하려면 다음을 지정하고 추가를 클릭합니다. • 이름 - 링크 그룹 이름을 입력합니다.

HA 링크 및 경로 모니터링 설정	설명
	• 활성화됨 - 링크 그룹을 활성화합니다. • 실패 조건 - 선택한 링크 중 일부 또는 전체가 실패할 때 실패가 발생하는지의 여부를 선택합니다. • **Interfaces(**인터페이스**)** - 모니터링할 이더넷 인터페이스를 하나 이상 선택합니다.

경로 모니터링	다음을 지정합니다.
	• 활성화됨 - 결합되거나 독립적인 가상 와이어 경로 모니터링, VLAN 경로 모니터링 및 가상 라우터* 경로 모니터링을 기반으로 경로 모니터링을 활성화합니다. 경로 모니터링을 사용하면 방화벽이 ICMP 핑(ping) 메시지를 보내 지정된 대상 IP 주소가 응답하는지 확인하여 모니터링할 수 있습니다. 페일오버에 다른 네트워크 디바이스의 모니터링이 필요하고 링크 모니터링만으로는 충분하지 않은 가상 와이어, 레이어 2 또는 레이어 3 구성에 경로 모니터링을 사용합니다.
	• 실패 조건:
	  • **Any**—(기본값) 방화벽은 가상 와이어, VLAN 또는 가상 라우터*에 대한 경로 모니터링이 실패할 때 HA 페일오버를 트리거합니다.
	  • **All** - 방화벽은 가상 와이어, VLAN 및 가상 라우터*에 대한 경로 모니터링이 실패할 때 HA 페일오버를 트리거합니다(세 가지 중 활성화된 항목).
	* *Advanced* 라우팅이 활성화된 경우 논리적 라우터가 가상 라우터를 대체하고 논리적 라우터 경로 모니터링을 활성화할 수 있습니다.
	경로 또는 링크가 다운될 경우 페일오버를 트리거하는 데 도움이 되도록 경로 모니터링 또는 링크 모니터링을 활성화하고 구성합니다. 경로 모니터링을 위한 하나 이상의 경로 그룹을 구성하고 링크 모니터링을 위한 하나 이상의 링크 그룹을 구성합니다.

경로 그룹	인터페이스 유형에 대한 특정 대상 주소를 모니터링하려면 하나 이상의 경로 그룹을 정의하십시오. 가상 와이어 경로를 추가하고 **VLAN** 경로를 추가하고 가상 라우터 경로를 추가합니다. (Advanced 라우팅을 활성화한 경우 논리적 라우터 경로를 추가할 수 있습니다.) 추가하는 각 경로 모니터링 유형에 대해 다음을 지정합니다. • 이름 - 모니터링할 가상 와이어, VLAN 또는 가상 라우터*를 선택합니다(드롭다운 선택은 추가하는 경로 모니터링 유형을 기반으로 함).

HA 링크 및 경로 모니터링 설정	설명

	• 소스 **IP** - 가상 와이어 및 VLAN 인터페이스의 경우 다음 홉 라우터로 전송되는 핑(ping)에 사용할 소스 IP 주소(대상 IP 주소)를 입력합니다. 로컬 라우터는 주소를 방화벽으로 라우팅할 수 있어야 합니다. (가상 라우터*와 연결된 경로 그룹의 소스 IP 주소는 지정된 대상 IP 주소에 대한 이그레스(egress) 인터페이스로 경로 테이블에 표시된 인터페이스 IP 주소로 자동 구성됩니다.)
	• 활성화됨 - 가상 와이어, VLAN 또는 가상 라우터*의 모니터링을 활성화합니다.
	• 실패 조건:
	  • **Any**(기본값) - 방화벽은 대상 IP 그룹에서 ping 오류가 발생할 때 가상 와이어, VLAN 또는 가상 라우터*가 실패한 것으로 결정합니다.
	  • **All**—방화벽은 모든 대상 IP 그룹에서 핑 실패가 발생할 때 가상 와이어, VLAN 또는 가상 라우터*가 실패했다고 판단합니다.
	실제 *HA* 페일오버는 가상 와이어, *VLAN* 및 가상 라우터* 경로 모니터링*(*활성화한 항목*)*을 고려하는 경로 모니터링에 대해 설정한 오류 조건에 따라 결정됩니다.
	• 핑**(ping)** 인터벌 - 대상 IP 주소로 전송되는 핑(ping) 사이의 인터벌을 지정합니다(범위는 200~60,000ms, 기본값은 200ms).
	• 핑**(ping)** 수—실패를 선언하기 전에 실패한 핑(ping) 수를 지정합니다(범위는 3~10, 기본값은 10).
	* *Advanced* 라우팅이 활성화된 경우 논리적 라우터가 가상 라우터를 대체하고 논리적 라우터 경로 모니터링을 활성화할 수 있습니다.

경로 그룹의 대상 IP	• 대상 **IP** - 경로 그룹을 모니터링할 대상 IP 주소 그룹을 하나 이상 추가합니다.
	  • 대상 **IP** 그룹 - 그룹의 이름을 입력합니다.
	  • 그룹에 대해 모니터링할 대상 **IP** 주소를 하나 이상 추가합니다.
	  • 활성화됨 - 대상 IP 그룹을 활성화하려면 선택합니다.
	  • 실패 조건: **Any**(그룹의 IP 주소에 대해 핑(ping) 실패가 발생하면 대상 그룹이 실패한 것으로 간주하도록 지정) 또는 **All**(핑(ping) 실패가 발생하는 경우 지정 그룹의 모든 IP 주소에 대해 대상 그룹이 실패한 것으로 간주됨)을 선택합니다.

HA 능동형/능동형 구성

- 디바이스 > 고가용성 > 능동형/능동형 구성

능동형/능동형 HA 쌍에 대한 설정을 구성하려면 디바이스 > 고가용성 > 능동형/능동형 구성을 선택합니다.

능동형/능동형 구성 설정	설명
패킷 포워딩	피어가 세션 설정 및 비대칭 라우팅 세션의 레이어 7 검사(App-ID, Content-ID 및 위협 검사)를 위해 HA3 링크를 통해 패킷을 포워딩할 수 있도록 합니다.
HA3 인터페이스	능동형/능동형 HA 피어 간에 패킷을 포워딩하는 데 사용할 데이터 인터페이스를 선택합니다. 사용하는 인터페이스는 Interface Type **HA**로 설정된 전용 Layer 2 인터페이스여야 합니다. *HA3* 링크가 실패하면 활성-보조 피어가 작동하지 않는 상태로 전환됩니다. 이 상태를 방지하려면 *HA3* 링크로 둘 이상의 물리적 인터페이스가 있는 *LAG(*링크 통합 그룹*)* 인터페이스를 구성하십시오. 방화벽은 *HA3* 백업 링크를 지원하지 않습니다. 다중 인터페이스가 있는 통합 인터페이스는 *HA* 피어 간의 패킷 포워딩을 지원하기 위해 추가 용량과 링크 중복성을 제공합니다. *HA3* 인터페이스를 사용할 때 모든 중간 네트워킹 디바이스에서 점보 프레임을 활성화해야 합니다.
VR 동기화	HA 피어에 구성된 모든 가상 라우터를 강제로 동기화합니다. 가상 라우터가 동적 라우팅 프로토콜에 대해 구성되지 않은 경우 이 옵션을 사용합니다. 두 피어는 교환 네트워크를 통해 동일한 다음 홉 라우터에 연결되어야 하며 정적 라우팅만 사용해야 합니다.
QoS 동기화	모든 물리적 인터페이스에서 QoS 프로파일 선택을 동기화합니다. 두 피어의 링크 속도가 비슷하고 모든 물리적 인터페이스에서 동일한 QoS 프로파일이 필요한 경우 이 옵션을 사용합니다. 이 설정은 네트워크 탭의 QoS 설정 동기화에 영향을 줍니다. QoS 정책은 이 설정에 관계없이 동기화됩니다.
임시 유지 시간(초)	HA 능동형/능동형 구성의 방화벽이 실패하면 임시 상태가 됩니다. 임시 상태에서 활성 보조 상태로의 전환은 임시 보류 시간을 트리거하며, 이 시간 동안 방화벽은 패킷을 처리하기 전에 라우팅 인접 항목을 구축하고 경로 테이블을 채우려고 시도합니다. 이 타이머가 없으면 복구 중인 방화벽은 즉시 능동형-보조

능동형/능동형 구성 설정	설명
	상태가 되고 필요한 경로가 없기 때문에 패킷을 자동으로 삭제합니다(기본값은 60초).
세션 소유자 선택	세션 소유자는 세션에 대한 모든 레이어 7 검사(App-ID 및 Content-ID)와 세션에 대한 모든 트래픽 로그 생성을 담당합니다. 패킷의 세션 소유자를 결정하는 방법을 지정하려면 다음 옵션 중 하나를 선택하십시오. • 첫 번째 패킷 - 세션의 첫 번째 패킷을 받는 방화벽을 세션 소유자로 지정하려면 이 옵션을 선택합니다. 이것은 HA3에서 트래픽을 최소화하고 피어 간에 데이터플레인 로드를 분산하기 위한 모범 사례 구성입니다. • 기본 디바이스 - 활성-기본 방화벽이 모든 세션을 소유하도록 하려면 이 옵션을 선택합니다. 이 경우 활성-보조 방화벽이 첫 번째 패킷을 수신하면 레이어 7 검사가 필요한 모든 패킷을 HA3 링크를 통해 능동형-기본 방화벽으로 포워딩합니다.

가상 주소	추가를 클릭하고 **IPv4** 또는 **IPv6** 탭을 선택한 다음 추가를 다시 클릭하여 사용할 HA 가상 주소 유형을 지정하는 옵션을 입력합니다. 플로팅 또는 ARP 로드 공유. 쌍에서 가상 주소 유형의 유형을 혼합할 수도 있습니다. 예를 들어 LAN 인터페이스에서 ARP 로드 공유를 사용하고 WAN 인터페이스에서 유동 IP를 사용할 수 있습니다.
	• **Floating** - 링크 또는 시스템 장애가 발생한 경우 HA 피어 간에 이동할 IP 주소를 입력합니다. 인터페이스에서 두 개의 유동 IP 주소를 구성하여 각 방화벽이 하나씩 소유하고 우선 순위를 설정하도록 합니다. 방화벽 중 하나가 실패하면 유동 IP 주소가 HA 피어로 전환됩니다.
	  • 디바이스 **0** 우선 순위 - 디바이스 ID가 0인 방화벽의 우선 순위를 설정하여 유동 IP 주소를 소유할 방화벽을 결정합니다. 값이 가장 낮은 방화벽이 우선 순위가 가장 높습니다.
	  • 디바이스 **1** 우선 순위 - 디바이스 ID가 1인 방화벽의 우선 순위를 설정하여 유동 IP 주소를 소유할 방화벽을 결정합니다. 값이 가장 낮은 방화벽이 우선 순위가 가장 높습니다.
	  • 링크 상태가 다운된 경우 페일오버 주소 - 인터페이스에서 링크 상태가 다운된 경우 페일오버 주소를 사용합니다.
	  • **Active-Primary HA** 디바이스에 바인딩된 유동 **IP** - 유동 IP 주소를 능동형-기본 피어에 바인딩하려면 이 옵션을 선택합니다. 하나의 피어가 실패하면 실패한 방화벽이 복구되어 능동형-보조 피어가 된 후에도 트래픽이 능동형-기본 피어로 계속 전송됩니다.

능동형/능동형 구성 설정	설명

가상 주소(계속)	• **ARP** 로드 공유 - HA 쌍에서 공유하고 호스트에 게이트웨이 서비스를 제공할 IP 주소를 입력합니다. 이 옵션은 방화벽이 호스트와 동일한 브로드캐스트 도메인에 있는 경우에만 필요합니다. 디바이스 선택 알고리즘 선택:
	  • **IP Modulo** - ARP 요청자 IP 주소의 패리티를 기반으로 ARP 요청에 응답할 방화벽을 선택합니다.
	  • **IP** 해시 - ARP 요청자 IP 주소의 해시를 기반으로 ARP 요청에 응답할 방화벽을 선택합니다.

클러스터 구성

- 디바이스 > 고가용성 > 클러스터 구성

Device > **High Availability** > 클러스터 구성을 선택하여 HA 클러스터에 구성원을 추가합니다.

클러스터 구성	설명
추가하다	클러스터 구성원을 추가하십시오. 로컬 방화벽을 추가해야 하며 HA 쌍을 사용하는 경우 쌍의 두 HA 피어를 클러스터 구성원으로 추가해야 합니다. • (지원되는 방화벽) 디바이스 일련번호 - 클러스터 구성원의 고유한 일련번호를 입력합니다. • (Panorama) 디바이스 - 드롭다운에서 디바이스를 선택한 다음 디바이스 이름을 입력합니다. • **HA4 IP** 주소 - 클러스터 구성원에 대한 HA4 링크의 IP 주소를 입력합니다. • **HA4** 백업 **IP** 주소 - 클러스터 구성원에 대한 백업 HA4 링크의 IP 주소를 입력합니다. • 세션 동기화 - 이 클러스터 구성원과 세션 동기화를 활성화하려면 선택합니다. • 설명 - 유용한 설명을 입력합니다.
삭제	하나 이상의 클러스터 구성원을 선택한 다음 클러스터에서 삭제하십시오.
활성화	(지원되는 방화벽) 클러스터 구성원이 다른 구성원과 세션을 동기화하는지의 여부를 결정할 수 있습니다. 기본적으로 모든 구성원은 세션을 동기화할 수 있습니다. 하나 이상의 구성원에 대해 동기화를 비활성화하는 경우 활성화를 선택하여 하나 이상의 구성원에 대해 동기화를 다시 활성화합니다.

클러스터 구성	설명
비활성화	(지원되는 방화벽) 하나 이상의 구성원을 선택한 다음 다른 구성원과의 동기화를 비활성화합니다.
새로 고침	(Panorama) HA 클러스터의 HA 기기 목록을 새로 고치려면 새로 고침을 선택합니다.

디바이스 > 로그 포워딩 카드

- 디바이스 > 로그 포워딩 카드

LFC(로그 포워딩 카드)는 방화벽에서 Panorama, Firewall Data Lake 또는 syslog 서버와 같은 하나 이상의 외부 로깅 시스템으로 모든 데이터플레인 로그(예: 트래픽 및 위협)를 포워딩하는 고성능 로그 카드입니다. 로컬 방화벽에서 데이터플레인 로그를 더 이상 사용할 수 없으므로 ACC 탭이 관리 웹 인터페이스에서 제거되고 모니터 > 로그에는 관리 로그(구성, 시스템 및 알람)만 포함됩니다.

LFC에 대한 포트를 구성해야 합니다. 브레이크아웃 케이블을 사용하여 LFC 1/1을 구성하면 최대 8개의 10G 브레이크아웃 포트에 액세스할 수 있습니다. 이것은 첫 번째 인터페이스에서 포트 1-4를 자동 구성하고 두 번째 인터페이스에서 포트 5-8을 자동 구성합니다. 하나 또는 두 인터페이스를 모두 사용하여 각각 최대 40G 또는 80G 연결을 제공할 수 있습니다. 연결된 디바이스는 LFC에 연결된 모든 포트에 대해 LAG를 사용하도록 설정해야 합니다.

LFC 1/9를 구성하면 최대 2개의 40G 포트에 접근할 수 있습니다. 이렇게 하면 첫 번째 인터페이스에서 포트 9가 자동 구성되고 두 번째 인터페이스에서 포트 10이 자동으로 구성됩니다. 하나 또는 두 인터페이스를 모두 사용하여 각각 최대 40G 또는 80G 연결을 제공할 수 있습니다. 연결된 디바이스는 LFC에 연결된 모든 포트에 대해 LAG를 사용하도록 설정해야 합니다.

*LFC*는 현재 *LACP*를 지원하지 않습니다.

디바이스 카드 > 로그 포워딩에서 포트를 구성합니다. 방화벽은 이들 포트를 사용하여 모든 데이터 평면 로그를 Panorama 또는 syslog 서버와 같은 외부 시스템으로 전달합니다.

LFC 요구 사항 및 구성 요소에 대한 정보는 PA-7000 시리즈 하드웨어 참조 안내서를 참조하십시오.

LFC 인터페이스의 경우 다음 표에 설명된 설정을 구성합니다.

LFC 인터페이스 설정	설명
이름	인터페이스 이름을 입력합니다. LFC의 경우 드롭다운 메뉴에서 **lfc1/1** 또는 **lfc1/9**를 선택해야 합니다.
코멘트	인터페이스에 대한 선택적 설명을 입력합니다.
IPv4	네트워크에서 IPv4를 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv4 주소입니다. • 넷마스크 - 포트의 IPv4 주소에 대한 네트워크 마스크입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv4 주소입니다.
IPv6	네트워크에서 IPv6을 사용하는 경우 다음을 정의합니다.

LFC 인터페이스 설정	설명
	• **IP** 주소 - 포트의 IPv6 주소입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv6 주소입니다.
링크 속도	인터페이스 속도를 Mbps(**10000** 또는 **40000**) 단위로 선택하거나 자동(기본값)을 선택하여 방화벽이 연결에 따라 속도를 자동으로 결정하도록 합니다. 사용 가능한 인터페이스 속도는 사용된 이름(lfc1/1 또는 lfc1/9)에 따라 다릅니다. 속도를 구성할 수 없는 인터페이스의 경우 **auto**가 유일한 옵션입니다.
링크 상태	인터페이스 상태를 활성화(**up**), 비활성화(**down**) 또는 연결에 따라 자동으로 결정(**auto**)할지의 여부를 선택합니다. 기본값은 자동입니다.
LACP 포트 우선 순위	LACP는 현재 LFC에서 지원되지 않습니다.

Multi-VSYS가 활성화된 경우 하위 인터페이스를 사용할 수 있습니다. LFC 하위 인터페이스를 구성하려면 하위 인터페이스를 추가하고 다음 표에 설명된 설정을 사용하십시오.

외부 서버에 대한 로그 전달은 *LFC* 하위 인터페이스에서 아직 지원되지 않습니다. 로그를 외부 서버로 전달하려면 기본 *LFC* 인터페이스를 사용해야 합니다.

LFC 서브인터페이스 설정	설명
인터페이스 이름	인터페이스 이름(읽기 전용)은 선택한 로그 카드 인터페이스의 이름을 표시합니다. 인접한 필드에 숫자 서픽스(1-9,999)를 입력하여 서브인터페이스를 식별합니다.
코멘트	인터페이스에 대한 선택적 설명을 입력합니다.
태그	서브인터페이스에 대한 VLAN 태그(0-4,094)를 입력합니다. 사용하기 쉽도록 태그를 서브인터페이스 번호와 동일하게 만드십시오.
가상 시스템	LFC(Log Forwarding Card) 하위 인터페이스가 할당된 가상 시스템(vsys)을 선택합니다. 또는 가상 시스템을 클릭하여 새 vsys를 추가할 수 있습니다. LFC 하위 인터페이스가 vsys에 할당되면 해당 인터페이스는 로그 카드에서 로그(syslog, 이메일, SNMP)를 포워딩하는 모든 서비스의 소스 인터페이스로 사용됩니다.

LFC 서브인터페이스 설정	설명
IPv4	네트워크에서 IPv4를 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv4 주소입니다. • 넷마스크 - 포트의 IPv4 주소에 대한 네트워크 마스크입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv4 주소입니다.
IPv6	네트워크에서 IPv6을 사용하는 경우 다음을 정의합니다. • **IP** 주소 - 포트의 IPv6 주소입니다. • 기본 게이트웨이 - 포트에 대한 기본 게이트웨이의 IPv6 주소입니다.

디바이스 > 구성 감사

디바이스 > 구성 감사를 선택하여 구성 파일 간의 차이점을 확인합니다. 이 페이지는 구성을 별도의 창에 나란히 표시하고 추가(녹색), 수정(노란색) 또는 삭제(빨간색)를 나타내는 색상을 사용하여 차이점을 한 줄씩 강조 표시합니다.

Added Modified Deleted

구성 감사 설정	설명
구성 이름 드롭다운(레이블 없음)	(레이블이 지정되지 않은) 구성 이름 드롭다운에서 비교할 두 개의 구성을 선택합니다(기본값은 **Running config** 및 **Candidate config**임). 원하는 구성과 연결된 커밋 작업의 설명 값에서 파생된 텍스트 문자열을 입력하여 드롭다운을 필터링할 수 있습니다(변경 사항 커밋 참조).
컨텍스트 드롭다운	컨텍스트 드롭다운을 사용하여 각 파일에서 강조 표시된 차이점 전후에 표시할 줄 수를 지정합니다. 더 많은 줄을 지정하면 감사 결과를 웹 인터페이스의 설정과 연관시키는 데 도움이 될 수 있습니다. 컨텍스트를 모두로 설정하면 결과에 전체 구성 파일이 포함됩니다.
실행	이동을 클릭하여 감사를 시작합니다.
이전(및 다음 ( )	이러한 탐색 화살표는 구성 이름 드롭다운에서 연속 구성 버전을 선택한 경우 활성화됩니다. 드롭다운에서 이전 구성 쌍을 비교하려면 을 클릭하고 다음 구성 쌍을 비교하려면 을 클릭하십시오.

디바이스 > 암호 프로파일

- 디바이스 > 암호 프로파일
- Panorama > 비밀번호 프로파일

Device > **Password** 프로파일 또는 **Panorama** > 암호 프로파일을 선택하여 개별 로컬 계정에 대한 기본 암호 요구 사항을 설정합니다. 암호 프로파일은 모든 로컬 계정(**Device** > **Setup** > 관리)에 대해 정의한 최소 암호 복잡성 설정보다 우선합니다.

계정에 암호 프로파일을 적용하려면 **Device** > **Administrators**(방화벽) 또는 **Panorama** > **Administrators** (Panorama)를 선택한 다음 계정을 선택한 다음 암호 프로파일을 선택합니다.

로컬 데이터베이스 인증을 사용하는 관리 계정에는 비밀번호 프로파일을 할당할 수 없습니다(디바이스 > 로컬 사용자 데이터베이스 > 사용자 참조).

암호 프로파일을 생성하려면 다음 표에 정보를 추가하고 지정합니다.

비밀번호 프로파일 설정	설명
이름	비밀번호 프로파일을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
비밀번호 변경 필수 기간(일)	관리자가 일 수(범위는 0~365)로 지정된 정기적으로 암호를 변경하도록 요구합니다. 예를 들어 값을 90으로 설정하면 관리자에게 90일마다 암호를 변경하라는 메시지가 표시됩니다. 만료 경고를 0일에서 30일 사이로 설정하고 유예 기간을 지정할 수도 있습니다.
만료 경고 기간(일)	필수 비밀번호 변경 기간이 설정되어 있으면 이 설정을 사용하여 강제 비밀번호 변경 날짜(범위: 0 ~ 30)가 가까워지면 로그인할 때마다 비밀번호를 변경하라는 메시지를 표시할 수 있습니다.
만료 후 관리자 로그인 수	관리자는 계정이 만료된 후 지정된 횟수만큼 로그인할 수 있습니다. 예를 들어 값이 3으로 설정되고 계정이 만료된 경우 계정이 잠기기 전에 3번 더 로그인할 수 있습니다(범위는 0~3).
만료 후 유예 기간(일)	관리자가 계정이 만료된 후 지정된 일 수(0~30일 범위)에 로그인할 수 있도록 허용합니다.

사용자명 및 암호 요구 사항

다음 표에는 PAN-OS 및 Panorama 계정에 대한 사용자명과 암호에 사용할 수 있는 유효한 문자가 나열되어 있습니다.

계정 유형	사용자명 및 암호 제한
암호 문자 집합	암호 필드 문자 집합에는 제한이 없습니다.
원격 관리자, SSL-VPN 또는 인증 포털	사용자명은 다음 문자는 허용되지 않습니다. • 백틱 (') • 꺾쇠 괄호(< and >) • 앰퍼샌드 (&) • 별표 (*) • 기호에서 (@) • 물음표 (?) • 파이프 (|) • 따옴표(') • 세미콜론 (;) • 쌍따옴표 (") • 달러 ($) • 괄호 ('(' 및 ')') • 콜론 (':')
로컬 관리자 계정	다음은 로컬 사용자명에 허용되는 문자입니다. • 소문자(a-z) • 대문자 (A-Z) • 숫자 (0-9) • 밑줄(_) • 마침표(.) • 하이픈 (-) 로그인 이름은 하이픈(-)으로 시작할 수 없습니다. 관리자 사용자 이름은 숫자로만 구성될 수 없습니다. 최소한 하나의 알파벳 문자 또는 하나의 법적 기호 문자를 포함해야 합니다. 예를 들어,

계정 유형	사용자명 및 암호 제한
	1234_567, **1234a789_** 및 **c7897432**는 유효한 사용자 이름입니다. **12345678**은 유효한 사용자 이름이 아닙니다.
로컬 관리자 암호	일반적으로 사용되는 단어와 구는 대문자와 소문자의 조합에 관계없이 암호로 허용되지 않습니다. 일반적으로 사용되는 단어와 구의 예로는 *Admin*, *password*, *PASSWORD*, *letmein*, *pa55word*, *QwErTy* 및 *q1w2e3r4*가 있습니다.

디바이스 > 관리자

관리자 계정은 방화벽 및 Panorama에 대한 액세스를 제어합니다. 방화벽 관리자는 단일 방화벽 또는 단일 방화벽의 가상 시스템에 대한 전체 또는 읽기 전용 액세스 권한을 가질 수 있습니다. 방화벽에는 전체 액세스 권한이 있는 사전 정의된 관리자 계정이 있습니다.

Panorama 관리자를 정의하려면 Panorama > 관리 디바이스 > 요약을 참조하십시오.

다음 인증 옵션이 지원됩니다.

- 비밀번호 인증 - 관리자는 사용자명과 비밀번호를 입력하여 로그인합니다. 이 인증에는 인증서가 필요하지 않습니다. 인증 프로파일과 함께 사용하거나 로컬 데이터베이스 인증에 사용할 수 있습니다.
- 클라이언트 인증서 인증(웹) - 이 인증에는 사용자명이나 암호가 필요하지 않습니다. 인증서는 방화벽에 대한 액세스를 인증하기에 충분합니다.
- 공개 키 인증(SSH) - 관리자는 방화벽에 액세스해야 하는 시스템에서 공개/개인 키 쌍을 생성한 다음 관리자가 사용자명과 암호를 입력하지 않고도 보안 액세스를 허용하도록 공개 키를 방화벽에 업로드합니다.

관리자를 추가하려면 추가를 클릭하고 다음 정보를 입력합니다.

관리자 계정 설정	설명
이름	관리자의 로그인 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 하이픈, 마침표 및 밑줄만 사용하십시오. 로그인 이름은 하이픈(-)으로 시작할 수 없습니다.
인증 프로파일	관리자 인증을 위한 인증 프로파일을 선택합니다. RADIUS, TACACS+, LDAP, Kerberos, SAML 또는 로컬 데이터베이스 인증에 이 설정을 사용할 수 있습니다. 자세한 내용은 디바이스 > 인증 프로파일을 참조하십시오.
클라이언트 인증서 인증만 사용(웹)	웹 액세스에 클라이언트 인증서 인증을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 사용자명과 암호가 필요하지 않습니다. 인증서는 방화벽에 대한 액세스를 인증하기에 충분합니다.
새 비밀번호 새 암호를 확인합니다	관리자의 대소문자를 구분하는 암호를 입력하고 확인합니다(최대 64자). 또한 **Setup** > **Management**를 선택하여 최소 암호 길이를 적용할 수 있습니다.

관리자 계정 설정	설명
	방화벽 관리 인터페이스의 보안을 유지하려면 소문자, 대문자 및 숫자를 혼합하여 관리 암호를 주기적으로 변경하는 것이 좋습니다. 방화벽의 모든 관리자에 대해 최소 암호 복잡성 설정을 구성할 수도 있습니다.
공개 키 인증(SSH) 사용	SSH 공개 키 인증을 사용하려면 이 옵션을 선택하십시오. 키 가져오기를 클릭하고 공개 키 파일을 찾아 선택합니다. 업로드된 키는 읽기 전용 텍스트 영역에 나타납니다. 지원되는 주요 파일 형식은 IETF SECSH 및 OpenSSH입니다. 지원되는 키 알고리즘은 DSA(1,024비트) 및 RSA(768~4,096비트)입니다. 공개 키 인증이 실패하면 방화벽은 관리자에게 사용자명과 암호를 묻는 메시지를 표시합니다.
관리자 유형	이 관리자에게 역할을 할당하십시오. 역할은 관리자가 보고 수정할 수 있는 항목을 결정합니다. 역할 기반을 선택하는 경우 드롭다운에서 사용자 지정 역할 프로파일을 선택합니다. 자세한 내용은 디바이스 > 관리자 역할을 참조하십시오. 동적을 선택하면 다음과 같은 사전 정의된 역할 중 하나를 선택할 수 있습니다. • 운용 관리자 - 방화벽에 대한 전체 액세스 권한이 있으며 새 관리자 계정 및 가상 시스템을 정의할 수 있습니다. 운용 관리자 권한이 있는 관리 사용자를 생성하려면 운용 관리자 권한이 있어야 합니다. • 운용 관리자(읽기 전용) - 방화벽에 대한 읽기 전용 액세스 권한이 있습니다. • 디바이스 관리자 - 새 계정 또는 가상 시스템 정의를 제외한 모든 방화벽 설정에 대한 전체 액세스 권한이 있습니다. • 디바이스 관리자(읽기 전용) - 암호 프로파일(액세스 불가) 및 관리자 계정(로그인한 계정만 볼 수 있음)을 제외한 모든 방화벽 설정에 대한 읽기 전용 액세스 권한이 있습니다. • 가상 시스템 관리자 - 가상 시스템의 특정 측면을 만들고 관리하기 위해 방화벽의 특정 가상 시스템에 액세스할 수 있습니다(다중 가상 시스템 기능이 활성화된 경우). 가상 시스

관리자 계정 설정	설명
	템 관리자는 네트워크 인터페이스, 가상 라우터, IPSec 터널, VLAN, 가상 와이어, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다. • 가상 시스템 관리자(읽기 전용) - 가상 시스템의 특정 측면을 보기 위해 방화벽의 특정 가상 시스템에 대한 읽기 전용 액세스 권한이 있습니다(다중 가상 시스템 기능이 활성화된 경우). 읽기 전용 액세스 권한이 있는 가상 시스템 관리자는 네트워크 인터페이스, 가상 라우터, IPSec 터널, VLAN, 가상 와이어, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다.
가상 시스템 (가상 시스템 관리자 역할만 해당)	추가를 클릭하여 관리자가 관리할 수 있는 가상 시스템을 선택합니다.
비밀번호 프로파일	해당하는 경우 암호 프로파일을 선택합니다. 새 암호 프로파일을 만들려면 디바이스 > 암호 프로파일을 참조하십시오. 구성된 기간 후에 관리자 암호가 만료되도록 관리자용 암호 프로파일을 만듭니다. 관리자 암호를 정기적으로 변경하면 공격자가 저장하거나 도난당한 자격 증명을 사용하는 것을 방지할 수 있습니다.

디바이스 > 관리자 역할

디바이스 > 관리자 역할을 선택하여 관리 사용자의 액세스 권한과 책임을 결정하는 사용자 지정 역할인 관리자 역할 프로파일을 정의합니다. 관리 계정을 생성할 때 관리 역할 프로파일 또는 동적 역할을 할당합니다(디바이스>관리자).

Panorama 관리자에 대한 관리자 역할 프로파일을 정의하려면 Panorama > 관리자 역할을 참조하십시오.

방화벽에는 공통 기준 목적으로 사용할 수 있는 세 가지 사전 정의된 역할이 있습니다. 먼저 초기 방화벽 구성에 운용 관리자 역할을 사용하고 보안 관리자, 감사 관리자 및 암호화 관리자에 대한 관리자 계정을 만듭니다. 이러한 계정을 만들고 적절한 공통 기준인 관리자 역할을 적용한 후 해당 계정을 사용하여 로그인합니다. FIPS(Federal Information Processing Standard)/CC(Common Criteria) FIPS-CC 모드의 기본 운용 관리자 계정은 **admin**이고 기본 암호는 **paloalto**입니다. 표준 작동 모드에서 기본 관리자 암호는 **admin**입니다. 모두가 감사 추적에 대한 읽기 전용 액세스 권한이 있다는 점을 제외하고 기능이 중복되지 않는 사전 정의된 관리자 역할이 생성되었습니다(전체 읽기/삭제 액세스 권한이 있는 감사 관리자 제외). 이러한 관리자 역할은 수정할 수 없으며 다음과 같이 정의됩니다.

- auditadmin - 감사 관리자는 방화벽의 감사 데이터를 정기적으로 검토할 책임이 있습니다.
- cryptoadmin - 암호화 관리자는 방화벽에 대한 보안 연결 설정과 관련된 암호화 요소의 구성 및 유지 관리를 담당합니다.
- securityadmin - 보안 관리자는 다른 두 관리 역할에서 다루지 않는 다른 모든 관리 작업(예: 보안 정책 생성)을 담당합니다.

관리자 역할 프로파일을 추가하려면 추가를 클릭하고 다음 표에 설명된 설정을 지정합니다.

각 유형의 관리자가 필요로 하는 항목으로만 관리자 액세스를 제한하는 사용자 지정 역할을 만듭니다. 각 유형의 관리자에 대해 웹 ***UI***, ***XML API***, 명령줄 및 ***REST API*** 액세스에 대한 읽기 전용 액세스를 활성화, 비활성화 또는 설정합니다.

관리자 역할 설정	
이름	이 관리자 역할을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	(선택 사항) 역할에 대한 설명을 입력합니다(최대 255자).
역할	관리 책임 범위 선택: • 디바이스 - 역할은 가상 시스템(vsys)이 두 개 이상 있는지의 여부와 관계없이 전체 방화벽에 적용됩니다.

관리자 역할 설정	
	• 가상 시스템 - 이 역할 은 방화벽의 특정 가상 시스템과 가상 시스템의 특정 측면에 적용됩니다(다중 가상 시스템 기능이 활성화된 경우). 가상 시스템을 기반으로 하는 관리자 역할 프로파일은 웹 **UI** 탭에서 네트워크 인터페이스, VLAN, 가상 와이어, IPSec 터널, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일에 액세스할 수 없습니다. 관리 계정을 생성할 때 가상 시스템을 선택합니다(디바이스>관리자).
WebUI	특정 웹 인터페이스 기능 에 대한 아이콘을 클릭하여 허용된 액세스 권한을 설정합니다. • 활성화 - 선택한 기능에 대한 읽기/쓰기 액세스 권한입니다. • 읽기 전용 - 선택한 기능에 대한 읽기 전용 액세스입니다. • 비활성화 - 선택한 기능에 액세스할 수 없습니다.
XML API	특정 XML API 기능의 아이콘을 클릭하여 허용된 액세스 권한(활성화 또는 비활성화)을 설정합니다.

명령줄	CLI 액세스에 대한 역할 유형을 선택합니다. 기본값은 없음이며 이는 CLI에 대한 액세스가 허용되지 않음을 의미합니다. 다른 옵션은 역할 범위에 따라 다릅니다.
	• 디바이스
	  • 운용 관리자 - 방화벽에 대한 전체 액세스 권한이 있으며 새 관리자 계정 및 가상 시스템을 정의할 수 있습니다. 운용 관리자 권한이 있는 관리 사용자를 생성하려면 운용 관리자 권한이 있어야 합니다.
	  • **superreader** - 방화벽에 대한 읽기 전용 액세스 권한이 있습니다.
	  • **deviceadmin** - 새 계정 또는 가상 시스템 정의를 제외한 모든 방화벽 설정에 대한 전체 액세스 권한이 있습니다.
	  • **devicereader** - 암호 프로파일(액세스 없음) 및 관리자 계정(로그인한 계정만 표시)을 제외한 모든 방화벽 설정에 대한 읽기 전용 액세스 권한이 있습니다.
	• 가상 시스템
	  • **vsysadmin** - 방화벽의 특정 가상 시스템에 액세스하여 가상 시스템의 특정 측면을 만들고 관리합니다. **vsysadmin** 설정은 방화벽 수준

관리자 역할 설정	
	또는 네트워크 수준 기능(예: 정적 및 동적 라우팅, 인터페이스의 IP 주소, IPSec 터널, VLAN, 가상 와이어, 가상 라우터, 논리적 라우터, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일)을 제어하지 않습니다. • **vsysreader** - 방화벽의 특정 가상 시스템 및 가상 시스템의 특정 측면에 대한 읽기 전용 액세스 권한이 있습니다. **vsysreader** 설정은 방화벽 수준 또는 네트워크 수준 기능(예: 정적 및 동적 라우팅, 인터페이스의 IP 주소, IPSec 터널, VLAN, 가상 와이어, 가상 라우터, 논리적 라우터, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 또는 네트워크 프로파일)에 액세스할 수 없습니다.
REST API	특정 REST API  기능에 대한 아이콘을 클릭하여 허용된 액세스 권한(활성화, 읽기 전용 또는 비활성화)을 설정합니다.

디바이스 > 액세스 도메인

- 디바이스 > 액세스 도메인

방화벽의 특정 가상 시스템에 대한 관리자 액세스를 제한하도록 액세스 도메인을 구성합니다. 방화벽은 RADIUS, TACACS+ 또는 SAML ID 서버(IdP) 서버를 사용하여 관리자 인증 및 권한 부여를 관리하는 경우에만 액세스 도메인을 지원합니다. 액세스 도메인을 활성화하려면 다음을 정의해야 합니다.

- 외부 인증 서버에 대한 서버 프로파일 - 디바이스 > 서버 프로파일 > RADIUS, 디바이스 > 서버 프로파일 > TACACS+ 및 디바이스 > 서버 프로파일 > SAML ID 공급자를 참조하십시오.
- RADIUS VSA(Vendor-Specific Attributes), TACACS+ VSA 또는 SAML 속성.

관리자가 방화벽에 로그인을 시도하면 방화벽은 외부 서버에 관리자의 액세스 도메인을 쿼리합니다. 외부 서버는 연결된 도메인을 반환하고 방화벽은 액세스 도메인에서 지정한 가상 시스템으로 관리자를 제한합니다. 방화벽이 관리자 인증 및 권한 부여를 위해 외부 서버를 사용하지 않는 경우 디바이스 > 액세스 도메인 설정은 무시됩니다.

*Panorama*에서는 로컬에서 또는 *RADIUS VSA*, *TACACS+ VSA* 또는 *SAML* 속성을 사용하여 액세스 도메인을 관리할 수 있습니다*(*Panorama > 액세스 도메인 참조*)*.

도메인 설정에 액세스	설명
이름	액세스 도메인의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 하이픈, 밑줄 및 마침표만 사용하십시오.
가상 시스템	사용 가능한 열에서 가상 시스템을 선택한 다음 추가합니다. 액세스 도메인은 가상 시스템을 지원하는 방화벽에서만 지원됩니다.

디바이스 > 인증 프로파일

이 페이지를 사용하여 관리자 및 최종 사용자를 인증하기 위한 설정을 구성합니다. 방화벽 및 Panorama는 로컬, RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0 및 MFA(다단계 인증) 서비스를 지원합니다.

하나 이상의 인증 프로파일을 만들어 외부 인증을 제공합니다. 이 프로파일은 모든 인증 요청을 한 곳에서 관리하기 쉽게 유지하고 추적과 같은 서비스를 포함하는 표준 인증 프로세스를 사용합니다. 가장 좋은 방법은 인증 실패 시 다른 방법을 사용하여 여러 인증 프로파일을 만들고 우선 순위(디바이스 > 인증 시퀀스)를 지정하고 모든 외부 방법이 실패할 경우 대체할 로컬 로그인 계정을 하나 이상 만드는 것입니다.

이 페이지를 사용하여 SAML ID 공급자(IdP)에 방화벽 또는 Panorama 서비스(예: 웹 인터페이스에 대한 관리 액세스)를 등록할 수도 있습니다. 서비스를 등록하면 방화벽 또는 Panorama가 IdP를 사용하여 서비스를 요청하는 사용자를 인증할 수 있습니다. IdP에 SAML 메타데이터를 입력하여 서비스를 등록합니다. 방화벽과 Panorama는 서비스에 할당한 인증 프로파일을 기반으로 SAML 메타데이터 파일을 자동으로 생성하여 쉽게 등록할 수 있습니다. 이 메타데이터 파일을 IdP로 내보낼 수 있습니다.

- 인증 프로파일
- 인증 프로파일에서 SAML 메타데이터 내보내기

인증 프로파일

- 디바이스 > 인증 프로파일

Device > **Authentication Profile** 또는 **Panorama** > 인증 프로파일을 선택하여 인증 프로파일을 관리합니다. 새 프로파일을 만들려면 프로파일을 하나 추가하고 다음 필드를 완성하세요.

인증 프로파일을 구성한 후 ***### ## CLI*** 명령을 사용하여 방화벽 또는 *Panorama* 관리 서버가 백엔드 인증 서버와 통신할 수 있는지의 여부와 인증 요청이 성공했는지의 여부를 확인합니다. 커밋하기 전에 구성이 올바른지 확인하기 위해 후보 구성에 대한 인증 테스트를 수행할 수 있습니다.

인증 프로파일 설정	설명
이름	프로파일을 식별할 수 있는 이름을 입력합니다. 이름은 대소문자를 구분하며 최대 31자까지 가능하며 문자, 숫자, 공백, 하이픈, 밑줄 및 마침표만 포함할 수 있습니다. 이름은 다른 인증 프로파일 및 인증 시퀀스와 관련하여 현재 위치(방화벽 또는 가상 시스템)에서 고유해야 합니다.

인증 프로파일 설정	설명
	다중 가상 시스템 모드에 있는 방화벽에서 인증 프로파일의 위치가 가상 시스템인 경우 공유 위치에 인증 시퀀스와 동일한 이름을 입력하지 마십시오. 마찬가지로 프로파일 위치가 공유인 경우 가상 시스템의 시퀀스와 동일한 이름을 입력하지 마십시오. 이러한 경우 동일한 이름으로 인증 프로파일과 시퀀스를 커밋할 수 있지만 참조 오류가 발생할 수 있습니다.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
인증 탭 방화벽은 요소 탭에서 추가한 MFA(다단계 인증) 서비스를 호출하기 전에 이 탭에서 구성한 인증 서비스를 호출합니다. 방화벽이 공급자 *API* 대신 *RADIUS*를 통해 *MFA* 공급자와 통합되는 경우 *MFA* 서버 프로파일이 아니라 해당 공급자에 대한 *RADIUS* 서버 프로파일을 구성해야 합니다.	
유형	사용자에게 표시되는 첫 번째(그리고 선택적으로 유일한) 인증 챌린지를 제공하는 서비스 유형을 선택합니다. 선택 사항에 따라 대화 상자에는 서비스에 대해 정의한 다른 설정이 표시됩니다. 옵션은 다음과 같습니다. • 없음 - 인증을 사용하지 않습니다. • 클라우드 인증 서비스 - Cloud Identity Engine에서 제공하는 클라우드 기반 인증 서비스를 사용합니다. • 로컬 데이터베이스 - 방화벽에서 로컬 인증 데이터베이스를 사용합니다. 이 옵션은 Panorama에서 사용할 수 없습니다. • **RADIUS** - RADIUS(원격 인증 전화 접속 사용자 서비스) 서버를 사용합니다. • **TACACS+** - TACACS+(터미널 액세스 컨트롤러 액세스 제어 시스템 플러스) 서버를 사용합니다. • **LDAP** - LDAP(Lightweight Directory Access Protocol) 서버를 사용합니다. • **Kerberos** - Kerberos 서버를 사용합니다. • **SAML** - SAML 2.0(Security Assertion Markup Language 2.0) ID 공급자(IdP)를 사용합니다.

인증 프로파일 설정	설명
	관리자는 *SAML*을 사용하여 방화벽 또는 *Panorama* 웹 인터페이스에 인증할 수 있지만 *CLI*에는 인증할 수 없습니다.
서버 프로파일 (RADIUS, TACACS+, LDAP 또는 Kerberos만 해당)	드롭다운에서 인증 서버 프로파일을 선택합니다. 디바이스 > 서버 프로파일 > RADIUS, 디바이스 > 서버 프로파일 > TACACS+, 디바이스 > 서버 프로파일 > LDAP 또는 디바이스 > 서버 프로파일 > Kerberos를 참조하십시오.
IdP 서버 프로파일 (SAML만 해당)	드롭다운에서 SAML ID 공급자 서버 프로파일을 선택합니다. 디바이스 > 서버 프로파일 > SAML ID 공급자를 참조하십시오.
RADIUS에서 사용자 그룹 검색 (RADIUS만 해당)	RADIUS 서버에 정의된 VSA(Vendor-Specific Attributes)에서 사용자 그룹 정보를 수집하려면 이 옵션을 선택합니다. 방화벽은 이 정보를 사용하여 정책을 시행하거나 보고서를 생성하는 것이 아니라 허용 목록 항목에 대해 인증 사용자를 일치시킵니다.
TACACS+에서 사용자 그룹 검색 (TACACS+ 전용)	TACACS+ 서버에 정의된 VSA(Vendor-Specific Attributes)에서 사용자 그룹 정보를 수집하려면 이 옵션을 선택합니다. 방화벽은 이 정보를 사용하여 정책을 시행하거나 보고서를 생성하는 것이 아니라 허용 목록 항목에 대해 인증 사용자를 일치시킵니다.
로그인 속성 (LDAP만 해당)	사용자를 고유하게 식별하고 해당 사용자의 로그인 ID로 작동하는 LDAP 디렉토리 속성을 입력하십시오.
비밀번호 만료 경고 (LDAP만 해당)	인증 프로파일이 GlobalProtect 사용자를 위한 것이라면 암호 만료 전 일 수를 입력하여 사용자에게 x일 후에 암호가 만료된다는 알림 메시지를 표시하기 시작합니다. 기본적으로 알림 메시지는 암호 만료 7일 전에 표시됩니다(범위는 1~255). 사용자는 암호가 만료되면 VPN에 액세스할 수 없습니다. 사전 로그온 연결 방법 을 사용하도록 *GlobalProtect* 에이전트를 구성하는 것을 고려하십시오. 이렇게 하면 암호가 만료된 후에도 사용자가 도메인에 연결하여 암호를 변경할 수 있습니다. 사용자가 암호 만료를 허용하는 경우 관리자는 사용자가 VPN에 로그인할 수 있도록 임시 LDAP 암호를 할당할 수 있습니다. 이 워크플로에서는 포털 구성의 인증 수정자를 구성 새로 고침을 위한 쿠키 인증으로 설정하는 것이 좋습니다(그렇지 않으면 임시 암호가 포털 인증에 사용되지만 게이트웨이 로그인이 실패하여 VPN 액세스가 차단됨).

인증 프로파일 설정	설명
서명 요청에 대한 인증서 (SAML만 해당)	방화벽이 IdP(ID 공급자)로 보내는 SAML 메시지에 서명하는 데 사용할 인증서를 선택합니다. 이 필드는 **IdP** 서버 프로파일에서 **SAML** 메시지를 **IdP**에 서명 옵션을 활성화한 경우 필요합니다(기기 > 서버 프로파일 > SAML ID 공급자 참조). 그렇지 않으면 SAML 메시지에 서명할 인증서를 선택하는 것은 선택 사항입니다. 인증서 및 관련 개인 키를 생성하거나 가져올 때 인증서에 지정된 키 사용 속성은 키 사용 방법을 제어합니다. • 인증서가 주요 사용 속성을 명시적으로 나열하는 경우 속성 중 하나는 방화벽에서 생성하는 인증서에서 사용할 수 없는 디지털 서명이어야 합니다. 이 경우 엔터프라이즈 CA(인증 기관) 또는 타사 CA에서 인증서와 키를 가져와야 합니다. • 인증서에 키 사용 속성이 지정되지 않은 경우 메시지 서명을 포함하여 모든 용도로 키를 사용할 수 있습니다. 이 경우 모든 방법을 사용하여 SAML 메시지 서명을 위한 인증서와 키를 얻을 수 있습니다. *Palo Alto Networks*는 *IdP*로 전송되는 *SAML* 메시지의 무결성을 보장하기 위해 서명 인증서를 사용할 것을 권장합니다.
싱글 로그아웃 활성화 (SAML만 해당)	사용자가 단일 서비스에서 로그아웃하여 인증된 모든 서비스에서 로그아웃할 수 있도록 하려면 이 옵션을 선택합니다. 싱글 로그아웃(SLO)은 사용자가 SAML 인증을 통해 액세스한 서비스에만 적용됩니다. 서비스는 조직 외부에 있을 수도 있고 내부에 있을 수도 있습니다(예: 방화벽 웹 인터페이스). 이 옵션은 IdP 서버 프로파일에 **IdP SLO URL**을 입력한 경우에만 적용됩니다. 인증 포털 사용자에 대해 SLO를 활성화할 수 없습니다. 사용자를 로그아웃한 후 방화벽은 자동으로 IP 주소와 사용자명 매핑을 제거합니다.
인증서 프로파일 (SAML만 해당)	방화벽이 유효성을 검사하는 데 사용할 인증서 프로파일을 선택합니다. • IdP 서버 프로파일에 지정된 **IdP** 인증서입니다. IdP는 이 인증서를 사용하여 방화벽을 인증합니다. 방화벽은 인증 프로파일 구성을 커밋할 때 인증서의 유효성을 검사합니다.

인증 프로파일 설정	설명
	• IdP가 SSO(Single Sign-On) 및 SLO(Single Logout) 인증을 위해 방화벽으로 보내는 SAML 메시지입니다. IdP는 IdP 서버 프로파일에 지정된 **ID** 공급자 인증서를 사용하여 메시지에 서명합니다. 디바이스 > 인증서 관리 > 인증서 프로파일을 참조하십시오.
사용자 도메인 및 사용자명 수정자 (SAML 및 클라우드 인증 서비스를 제외한 모든 인증 유형)	방화벽은 허용 목록 항목에 대해 인증 사용자를 일치시키고 User-ID 그룹 매핑 을 위해 사용자 도메인을 사용합니다. 사용자명 수정자를 지정하여 사용자가 로그인하는 동안 입력하는 도메인 및 사용자명 형식을 수정할 수 있습니다. 방화벽은 수정된 문자열을 인증에 사용합니다. 다음 옵션 중에서 선택하십시오. • 수정되지 않은 사용자 입력만 보내려면 사용자 도메인을 비워두고(기본값) 사용자명 수정자를 변수 **%USERINPUT%**(기본값)로 설정합니다. • 사용자 입력 앞에 도메인을 추가하려면 사용자 도메인을 입력하고 사용자명 수정자를 **%USERDOMAIN%\%USERINPUT%**로 설정합니다. • 사용자 입력에 도메인을 추가하려면 사용자 도메인을 입력하고 사용자 이름 수정자를 **%USERINPUT%@%USERDOMAIN%**으로 설정합니다. ***Username Modifier***는 *%USERDOMAIN%* 변수를 포함하며, ***User Domain*** 값은 사용자가 입력하는 모든 도메인 문자열을 대체합니다. *%USERDOMAIN%* 변수를 지정하고 사용자 도메인을 비워두면 방화벽은 사용자가 입력한 모든 도메인 문자열을 제거합니다. 방화벽은 도메인 이름을 *User-ID* 그룹 매핑에 적합한 *NetBIOS* 이름으로 확인합니다. 이는 상위 및 하위 도메인 모두에 적용됩니다. 사용자 도메 수정자는 자동으로 파생된 *NetBIOS* 이름보다 우선합니다. • 방화벽이 서버 프로파일 유형을 사용하여 인증 시퀀스에서 사용자 입력 형식을 수정하는 방법과 시기를 결정할 수 있도록 하려면 수동으로 **##**을 사용자명 수정자로 입력합니다. 이 옵션에 대한 자세한 내용은 PAN-OS 관리자 가이드의 인증 프로파일 및 시퀀스 구성을 참조하십시오.
Kerberos 영역 (SAML 및 클라우드 인증 서비스를 제외한 모든 인증 유형)	네트워크에서 Kerberos SSO(Single Sign-On)를 지원하는 경우 **Kerberos** 영역을 입력합니다(최대 127자). 이것은 사용자 로그인 이름의 호스트네임 부분입니다. 예를 들어 사용자 계정 이름 user@EXAMPLE.LOCAL에는 EXAMPLE.LOCAL 영역이 있습니다.
Kerberos 키탭	네트워크에서 Kerberos Single Sign-On(SSO) 을 지원하는 경우, 가져오기를 클릭하고 찾아보기를 클릭하여 keytab 파일을 찾

인증 프로파일 설정	설명
(SAML 및 클라우드 인증 서비스를 제외한 모든 인증 유형)	은 다음 확인을 클릭합니다. keytab에는 SSO 인증에 필요한 방화벽에 대한 Kerberos 계정 정보(기본 이름 및 해시 암호)가 포함되어 있습니다. 각 인증 프로파일에는 하나의 키 탭이 있을 수 있습니다. 인증하는 동안 방화벽은 먼저 keytab을 사용하여 SSO를 설정하려고 시도합니다. 성공하고 액세스를 시도하는 사용자가 허용 목록에 있으면 인증이 즉시 성공합니다. 그렇지 않으면 인증 프로세스가 Kerberos일 필요가 없는 지정된 유형의 수동 인증(사용자명/암호)으로 대체됩니다. 방화벽이 *FIPS/CC* 모드인 경우 알고리즘은 *aes128-cts-hmac-sha1-96* 또는 *aes256-cts-hmac-sha1-96*이어야 합니다. 그렇지 않으면 *des3-cbc-sha1* 또는 *arcfour-hmac*을 사용할 수도 있습니다. 그러나 키 탭의 알고리즘이 티켓 부여 서비스가 *SSO*를 활성화하기 위해 클라이언트에 발급하는 서비스 티켓의 알고리즘과 일치하지 않으면 *SSO* 프로세스가 실패합니다. *Kerberos* 관리자는 서비스 티켓이 사용하는 알고리즘을 결정합니다.
사용자명 속성 (SAML만 해당)	IdP의 메시지에서 인증 사용자의 사용자명을 식별하는 SAML 속성을 입력합니다(기본값은 사용자명). **IdP** 서버 프로파일에 사용자명 속성을 지정하는 메타데이터가 포함된 경우 방화벽은 자동으로 이 필드를 해당 속성으로 채웁니다. 방화벽은 SAML 메시지에서 검색된 사용자명을 인증 프로파일의 허용 목록에 있는 사용자 및 사용자 그룹과 일치시킵니다. 사용자가 SAML 로그인 중에 입력하는 도메인/사용자명 문자열을 수정하도록 방화벽을 구성할 수 없기 때문에 로그인 사용자명은 허용 목록 항목과 정확히 일치해야 합니다. 이것은 필수인 유일한 SAML 속성입니다. *SAML* 메시지는 제목 필드에 사용자명을 표시할 수 있습니다. 사용자명 속성이 사용자명을 표시하지 않으면 방화벽은 자동으로 제목 필드를 확인합니다.
사용자 그룹 속성 (SAML만 해당)	IdP의 메시지에서 인증 사용자의 사용자 그룹을 식별하는 SAML 속성을 입력합니다(기본값은 **usergroup**). **IdP** 서버 프로파일에 사용자 그룹 속성을 지정하는 메타데이터가 포함된 경우 필드에 자동으로 해당 속성이 사용됩니다. 방화벽은 그룹 정보를 사용하여 정책이나 보고서가 아닌 허용 목록 항목에 대해 인증 사용자를 일치시킵니다.
관리자 역할 속성 (SAML만 해당)	IdP의 메시지에서 인증 사용자의 관리자 역할을 식별하는 SAML 속성을 입력합니다(기본값은 **admin-role**). 이 속성은 최종 사용자가 아닌 방화벽 관리자에게만 적용됩니다. **IdP** 서버 프로파일에 admin-role 속성을 지정하는 메타데이터가 포함된 경우 방화벽은 자동으로 이 필드를 해당 속성으로 채웁니다. 방화벽은 사전 정의된(동적) 역할 또는 관리자 역할 프로파일을 SAML 메시지에서 검색된 역할과 일치시켜 역할 기반 액세스 제어를 시행합니다. SAML 메시지

인증 프로파일 설정	설명
	에 역할이 하나만 있는 관리자에 대한 여러 admin-role 값이 있는 경우 일치는 admin-role 속성의 첫 번째(가장 왼쪽) 값에만 적용됩니다. 둘 이상의 역할이 있는 관리자의 경우 일치가 속성의 여러 값에 적용될 수 있습니다.
액세스 도메인 속성 (SAML만 해당)	IdP의 메시지에서 인증 사용자의 액세스 도메인을 식별하는 SAML 속성을 입력합니다(기본값은 **access-domain**). 이 속성은 최종 사용자가 아닌 방화벽 관리자에게만 적용됩니다. **IdP** 서버 프로파일에 액세스 도메인 속성을 지정하는 메타데이터가 포함된 경우 방화벽은 자동으로 이 필드를 해당 속성으로 채웁니다. 방화벽은 로컬로 구성된 액세스 도메인을 SAML 메시지에서 검색된 도메인과 일치시켜 액세스 제어를 시행합니다. SAML 메시지에 액세스 도메인이 하나만 있는 관리자에 대한 여러 액세스 도메인 값이 있는 경우 일치는 access-domain 속성의 첫 번째(가장 왼쪽) 값에만 적용됩니다. 둘 이상의 액세스 도메인이 있는 관리자의 경우 일치가 속성의 여러 값에 적용될 수 있습니다.
리전 (클라우드 인증 서비스만 해당)	Cloud Identity Engine 인스턴스의 리전 엔드포인트를 선택합니다. 선택하는 지역은 *Cloud Identity Engine* 인스턴스를 활성화할 때 선택한 지역과 일치해야 합니다.
인스턴스 (클라우드 인증 서비스만 해당)	인스턴스가 두 개 이상인 경우 사용할 Cloud Identity Engine 인스턴스를 선택합니다.
프로파일 (클라우드 인증 서비스만 해당)	Cloud Identity Engine ID 제공자 프로파일(IdP 프로파일)이 두 개 이상 있는 경우 사용할 Cloud Identity Engine IdP 프로파일을 선택합니다.
최대 클럭 스큐(초) (클라우드 인증 서비스만 해당)	방화벽이 IdP에서 수신한 메시지의 유효성을 검사하는 순간 IdP와 방화벽 시스템 시간 사이의 허용 가능한 최대 시간 차이를 초 단위로 입력합니다(범위는 1~900, 기본값은 60). 시간 차이가 이 값을 초과하면 유효성 검사(및 인증)가 실패합니다.
클라우드에서 다단계 인증 강제 실행 (클라우드 인증 서비스만 해당)	IdP가 사용자가 다단계 인증을 사용하여 로그인하도록 구성한 경우 클라우드에서 강제 다단계 인증을 활성화합니다.
요인 탭	

인증 프로파일 설정	설명
추가 인증 요소 활성화	사용자가 첫 번째 요소(인증 탭의 유형 필드에 지정)에 성공적으로 응답한 후 방화벽이 추가 인증 요소(도전)를 호출하도록 하려면 이 옵션을 선택합니다. 인증 정책을 통한 최종 사용자 인증에 대해서만 추가 인증 요소가 지원됩니다. *GlobalProtect* 포털 및 게이트웨이에 대한 원격 사용자 인증이나 *PAN-OS* 또는 *Panorama* 웹 인터페이스에 대한 관리자 인증에는 추가 요소가 지원되지 않습니다. 추가 요소를 구성할 수 있지만 이러한 사용 사례에는 적용되지 않습니다. 그러나 모든 인증 사용 사례에 대해 *RADIUS* 또는 *SAML*을 사용하여 *MFA* 공급자와 통합할 수 있습니다. MFA(다단계 인증)를 사용하는 인증 프로파일을 구성한 후에는 이를 인증 시행 개체에 할당하고(개체>인증) 네트워크 리소스에 대한 액세스를 제어하는 인증 정책 규칙(정책>인증)에 개체를 할당해야 합니다.
요인	사용자가 첫 번째 요소(인증 탭의 유형 필드에 지정)에 성공적으로 응답한 후 방화벽이 호출할 각 인증 요소에 대해 MFA 서버 프로파일(디바이스>서버 프로파일>다단계 인증)을 추가합니다. 방화벽은 요소를 제공하는 MFA 서비스를 나열하는 위에서 아래로 각 요소를 호출합니다. 순서를 변경하려면 서버 프로파일을 선택한 다음 위로 이동 또는 아래로 이동을 선택합니다. 최대 3개의 추가 요소를 지정할 수 있습니다. 각 MFA 서비스는 하나의 요소를 제공합니다. 일부 MFA 서비스에서는 사용자가 여러 목록에서 하나의 요소를 선택할 수 있습니다. 방화벽은 공급자 API를 통해 이러한 MFA 서비스와 통합됩니다. 추가 MFA 공급자 API 통합은 애플리케이션 또는 애플리케이션 및 위협 콘텐츠 업데이트를 통해 주기적으로 추가됩니다.
Advanced 탭	
허용 목록	추가를 클릭하고 모두 선택하거나 이 프로파일로 인증할 수 있는 특정 사용자 및 그룹을 선택합니다. 사용자가 인증되면 방화벽은 연결된 사용자명 또는 그룹을 이 목록의 항목과 일치시킵니다. 항목을 추가하지 않으면 사용자가 인증할 수 없습니다. 합법적인 비즈니스 액세스 요구 사항이 있는 사용자에게만 인증을 제한하고 공격 면적을 줄이려면 사용자 또는 사용자 그룹을 지정하고 모두 사용하지 마십시오.

인증 프로파일 설정	설명
	사용자 도메인 값을 입력한 경우 허용 목록에서 도메인을 지정할 필요가 없습니다. 예를 들어 사용자 도메인이 ***businessinc***이고 사용자 ***admin1***을 허용 목록에 추가하려는 경우 ***admin1***을 입력하면 ***businessinc\admin1***을 입력하는 것과 동일한 효과가 나타납니다. 디렉토리 서비스에 이미 있는 그룹을 지정하거나 *LDAP* 필터를 기반으로 사용자 정의 그룹을 지정할 수 있습니다.
실패한 시도 (SAML을 제외한 모든 인증 유형)	사용자 계정을 잠그기 전에 방화벽이 허용하는 연속 로그인 시도 실패 횟수(0~10)를 입력합니다. 0 값은 무제한 로그인 시도를 지정합니다. 기본값은 일반 작동 모드의 방화벽의 경우 0이고 FIPS-CC 모드의 방화벽의 경우 10입니다. 악의적인 시스템이 방화벽에 로그인하기 위해 무차별 대입 방법을 시도하는 것을 방지하면서 입력 오류가 발생한 경우 적절한 재시도 횟수를 수용하려면 실패한 시도 횟수를 *5* 이하로 설정하십시오. 실패한 시도 횟수를 *0* 이외의 값으로 설정했지만 잠금 시간을 *0*으로 두면 실패한 시도 횟수가 무시되고 사용자가 잠기지 않습니다.
잠금 시간 (SAML을 제외한 모든 인증 유형)	사용자가 실패한 시도 횟수에 도달한 후 방화벽이 사용자 계정을 잠그는 시간(분 범위는 0~60, 기본값은 0)을 입력합니다. 값이 0이면 관리자가 사용자 계정의 잠금을 수동으로 해제할 때까지 잠금이 적용됩니다. 악의적인 행위자의 지속적인 로그인 시도를 방지하려면 잠금 시간을 *30*분 이상으로 설정하십시오. 잠금 시간을 *0* 이외의 값으로 설정하고 실패한 시도를 *0*으로 두면 잠금 시간이 무시되고 사용자가 잠기지 않습니다.

인증 프로파일에서 SAML 메타데이터 내보내기

- 디바이스 > 인증 프로파일

방화벽 및 Panorama는 SAML ID 공급자(IdP)를 사용하여 서비스를 요청하는 사용자를 인증할 수 있습니다. 관리자의 경우 서비스에서 웹 인터페이스에 액세스할 수 있습니다. 최종 사용자의 경우 서비스는 네트워크 리소스에 대한 액세스를 활성화하는 인증 포털 또는 GlobalProtect일 수 있습니다. 서비스에 대한 SAML 인증을 활성화하려면 SAML 메타데이터 형식으로 IdP에 대한 특정 정보를 입력하여 해당 서비스를 등록해야 합니다. 방화벽 및 Panorama는 서비스에 할당한 인증 프로파일을 기반으로 SAML 메타데이

터 파일을 자동으로 생성하여 등록을 간소화하고 이 메타데이터 파일을 IdP로 내보낼 수 있습니다. 메타데이터 내보내기는 IdP의 각 메타데이터 필드에 대한 값을 입력하는 것보다 더 쉬운 대안입니다.

내보낸 파일의 일부 메타데이터는 인증 프로파일(디바이스 > 서버 프로파일 > SAML ID 공급자)에 할당된 *SAML IdP* 서버 프로파일에서 파생됩니다. 그러나 내보낸 파일은 *SAML IdP* 서버 프로파일에 지정된 방법에 관계없이 항상 *POST*를 *HTTP* 바인딩 방법으로 지정합니다. *IdP*는 *POST* 방법을 사용하여 *SAML* 메시지를 방화벽이나 *Panorama*로 보냅니다.

인증 프로파일에서 SAML 메타데이터를 내보내려면 인증 열에서 SAML 메타데이터 링크를 클릭하고 다음 필드를 완성합니다. 메타데이터 파일을 IdP로 가져오려면 IdP 설명서를 참조하십시오.

SAML 메타데이터 내보내기 설정	설명
명령	SAML 메타데이터를 내보낼 서비스를 선택합니다. • 관리(기본값) - 웹 인터페이스에 대한 관리자 액세스를 제공합니다. • **authentication-portal** - 인증 포털을 통해 네트워크 리소스에 대한 최종 사용자 액세스를 제공합니다. • **global-protect** - GlobalProtect를 통해 네트워크 리소스에 대한 최종 사용자 액세스를 제공합니다. 선택에 따라 대화 상자가 표시되는 다른 필드가 결정됩니다.
[관리 | 인증 포털 | GlobalProtect] 인증 프로파일	메타데이터를 내보내는 인증 프로파일의 이름을 입력합니다. 기본값은 메타데이터 링크를 클릭하여 대화 상자를 연 프로파일입니다.
관리 선택 (관리 전용)	관리 트래픽에 대해 활성화된 인터페이스(예: MGT 인터페이스)를 지정하기 위한 옵션을 선택합니다. • 인터페이스 - 방화벽의 인터페이스 목록에서 인터페이스를 선택합니다. • **IP** 호스트 이름 - 인터페이스의 IP 주소 또는 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우 DNS 서버에는 IP 주소에 매핑되는 주소(A) 레코드가 있어야 합니다.
[인증 포털 | GlobalProtect] 가상 시스템 (인증 포털 또는 GlobalProtect만 해당)	인증 포털 설정 또는 GlobalProtect 포털이 정의된 가상 시스템을 선택하십시오.
IP 호스트 이름	서비스의 IP 주소 또는 호스트 이름을 입력합니다.

SAML 메타데이터 내보내기 설정	설명
(인증 포털 또는 GlobalProtect만 해당)	• 인증 포털 - 리디렉션 호스트 IP 주소 또는 호스트 이름을 입력합니다(디바이스 > 사용자 식별 > 인증 포털 설정). • **GlobalProtect** - GlobalProtect 포털의 호스트 이름 또는 **IP** 주소를 입력합니다. 호스트 이름을 입력하는 경우 DNS 서버에는 IP 주소에 매핑되는 주소(A) 레코드가 있어야 합니다.

디바이스 > 인증 순서

- 디바이스 > 인증 순서
- Panorama > 인증 순서

일부 환경에서는 사용자 계정이 여러 디렉터리(예: LDAP 및 RADIUS)에 있습니다. 인증 시퀀스는 방화벽이 로그인할 때 사용자를 인증하는 데 사용하려고 하는 인증 프로파일 집합입니다. 방화벽은 하나의 프로파일이 사용자를 성공적으로 인증할 때까지 각각에 대해 인증, Kerberos Single Sign-On(SSO), 허용 목록 및 계정 잠금 값을 적용하여 목록의 위쪽에서 아래쪽으로 프로파일을 순차적으로 시도합니다. 방화벽은 시퀀스의 모든 프로파일이 인증에 실패한 경우에만 액세스를 거부합니다. 인증 프로파일에 대한 자세한 내용은 디바이스 > 인증 프로파일을 참조하십시오.

서로 다른 인증 방법을 사용하는 여러 인증 프로파일로 인증 시퀀스를 구성합니다. 연결 문제로 인해 인증이 차단되지 않도록 *2*개 이상의 외부 인증 방법과 *1*개의 로컬*(*내부*)* 방법을 구성하십시오. 모든 외부 인증 방법이 실패한 경우에만 사용되도록 로컬 인증 프로파일을 시퀀스의 마지막 프로파일로 만듭니다. *(*외부 인증은 로깅 및 문제 해결 기능을 포함하여 신뢰할 수 있는 전용 중앙 집중식 인증 서비스를 제공합니다.*)*

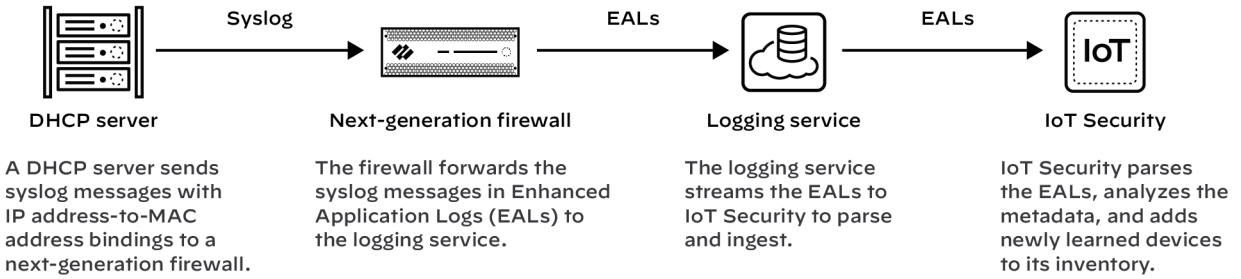
인증 시퀀스 설정	설명
이름	시퀀스를 식별할 이름을 입력합니다. 이름은 대소문자를 구분하며 최대 31자까지 가능하며 문자, 숫자, 공백, 하이픈, 밑줄 및 마침표만 포함할 수 있습니다. 이름은 다른 인증 시퀀스 및 인증 프로파일과 관련하여 현재 위치(방화벽 또는 가상 시스템)에서 고유해야 합니다. 여러 가상 시스템이 있는 방화벽에서 인증 시퀀스의 위치가 가상 시스템*(vsys)*인 경우 공유 위치에 인증 프로파일과 동일한 이름을 입력하지 마십시오. 마찬가지로 시퀀스 위치가 공유인 경우 *vsys*의 프로파일과 동일한 이름을 입력하지 마십시오. 이러한 경우 동일한 이름으로 인증 시퀀스 및 프로파일을 커밋할 수 있지만 레퍼런스 오류가 발생할 수 있습니다.
위치	시퀀스를 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 시퀀스를 저장한 후에는 위치를 변경할 수 없습니다.
도메인을 사용하여 인증 프로파일 결정	다음 옵션은 LDAP 인증 프로필에만 적용되며 기본적으로 활성화됩니다. • 인증 실패 시 시퀀스 종료 - 로그인 중에 사용자가 입력한 도메인 이름이 인증 시퀀스(정규화 유무에 관계없이)의 인증 프로필에 있는 도메인 이름

인증 시퀀스 설정	설명
	과 일치하는 경우 방화벽은 다음과 같은 경우 인증 시퀀스를 중단합니다. 방화벽은 나머지 인증 시퀀스를 위에서 아래 순서로 완료하지 않고 사용자를 성공적으로 인증할 수 없습니다. 이 옵션은 방화벽이 순서대로 인증 프로필이 있는 도메인 이름과 일치하는 경우에만 적용됩니다. • **User-ID** 도메인을 사용하여 인증 프로필 결정 - 도메인 이름을 사용하여 인증 프로필을 순서대로 확인하기 전에 사용자가 로그인할 때 입력하는 도메인 이름을 정규화합니다. 이 옵션을 선택하지 않으면 방화벽은 인증 프로필 시퀀스를 적용하기 전에 사용자가 로그인할 때 입력하는 도메인 이름을 정규화하지 않습니다. 이 옵션을 사용하지 않도록 설정하면 방화벽이 도메인 이름을 정규화하지 않고 인증에 실패하더라도 도메인 이름을 위에서 아래 순서로 인증 프로필과 일치시키려고 시도합니다.
인증 프로파일	추가를 클릭하고 시퀀스에 추가할 각 인증 프로파일의 드롭다운에서 선택합니다. 목록 순서를 변경하려면 프로파일을 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 프로파일을 제거하려면 프로파일을 선택한 다음 삭제를 클릭합니다. *MFA(*다단계 인증*)* 서버 프로파일 또는 *SAML(Security Assertion Markup Language) ID* 공급자 서버 프로파일을 지정하는 인증 프로파일을 추가할 수 없습니다.

디바이스 > IoT > DHCP 서버

IoT 보안은 관찰된 네트워크 동작을 IoT 디바이스에 할당하고 이를 고유하게 추적하기 위해 IP 주소-MAC 주소 바인딩을 활용합니다. IoT 보안은 일반적으로 차세대 방화벽에서 수집한 DHCP 트래픽을 사용하여 IP 주소-MAC 주소 바인딩을 학습하고 IP 주소 변경 사항을 추적합니다. 그러나 DHCP 데이터 경로에 방화벽을 배치할 수 없는 경우 이 방법을 사용하여 DHCP 서버 로그를 수집하고 DHCP 트래픽 가시성을 확장할 수 있습니다.

DHCP 트래픽을 방화벽으로 또는 방화벽을 통해 라우팅하기 어려운 네트워크 영역에서는 서버 로그를 syslog 메시지로 방화벽에 보내도록 DHCP 서버를 구성합니다. 그런 다음 방화벽은 로깅 서비스를 통해 하위 유형이 dhcp-syslog인 EAL(향상된 애플리케이션 로그)로 메시지를 IoT 보안에 전달합니다. IoT 보안은 이를 구문 분석하여 IP 주소-MAC 주소 바인딩을 학습한 다음 새로 학습한 디바이스를 인벤토리에 추가합니다.



전제 조건

- 차세대 방화벽에서 실행되는 syslog 서버에 메시지를 보내도록 구성된 syslog 기능이 있는 DHCP 서버
- 활성 IoT 보안 구독으로 PAN-OS 11.0 이상을 실행하는 차세대 방화벽

차세대 방화벽 설정

하나 이상의 DHCP 서버에서 syslog 메시지를 수신하도록 차세대 방화벽을 설정합니다. 방화벽은 EAL로 수신한 syslog 메시지를 로깅 서비스에 자동으로 전달하고, 로깅 서비스는 구문 분석 및 분석을 위해 이를 IoT 보안으로 스트리밍합니다.

1. 차세대 방화벽에 DHCP 서버를 추가합니다.

   차세대 방화벽에 로그인하고 디바이스 > **IoT** > **+** 추가를 선택하고 다음을 구성한 후 확인을 클릭합니다.

필드	설명
이름	DHCP 서버의 이름을 입력합니다. 공백을 포함하여 최대 32자까지 가능합니다.
설명	나중에 참조할 수 있도록 DHCP 서버에 대한 메모를 입력합니다. 공백을 포함하여 최대 256자까지 입력할 수 있습니다.

필드	설명
활성화됨	방화벽이 DHCP 서버의 연결을 수신 대기하고 연결이 수신될 때 처리하도록 설정하려면 선택합니다.
IP 주소	DHCP 서버가 방화벽에 연결할 IP 주소를 입력합니다. 주소는 IPv4 또는 IPv6 형식일 수 있습니다. FQDN은 허용되지 않습니다.
프로토콜	**TCP**, **UDP** 또는 **SSL**을 선택합니다. 선택할 때 DHCP 서버와 방화벽 간의 연결에 중요한 사항을 고려합니다. TCP는 전송 안정성을 제공하지만 보안은 제공하지 않습니다. UDP는 낮은 처리 오버헤드와 더 빠른 속도를 제공하지만 안정성과 보안이 부족합니다. SSL은 안정성과 보안을 제공하지만 오버헤드가 더 많이 발생합니다. 방화벽은 포트 *10514*에서 *TCP* 및 *UDP*를 사용하는 *DHCP* 서버 연결과 포트 *16514*에서 *SSL*을 사용하는 연결을 수신 대기합니다.

2. 이전 단계를 반복하여 DHCP 서버를 더 추가합니다.

   필요에 따라 DHCP 서버를 추가하여 네트워크 전체에서 DHCP 트래픽에 대한 가시성을 확장할 수 있습니다. 모든 차세대 방화벽은 방화벽당 최대 100개의 DHCP 서버를 지원합니다.

Syslog용 **DHCP** 서버 설정

서버 로그의 syslog 메시지를 차세대 방화벽의 관리 인터페이스로 보내도록 DHCP 서버를 구성합니다. 방화벽에서 구성된 것과 동일한 TCP, UDP 또는 SSL 프로토콜을 사용하도록 DHCP 서버를 구성해야 합니다. 구성 지침은 DHCP 서버 설명서를 참조하십시오.

DHCP 서버 연결 상태 확인

구성된 모든 DHCP 서버를 보려면 디바이스 > **IoT**를 선택합니다.

DHCP 서버 이름 옆의 녹색 원은 해당 서버가 Panorama에서 구성되었으며 로컬 차세대 방화벽의 웹 인터페이스에서 볼 때 읽기 전용임을 의미합니다.

TCP 또는 SSL을 사용하는 DHCP 서버가 현재 방화벽에 연결되어 있으면 상태 열에 "연결됨"이 표시됩니다. UDP를 사용하는 DHCP 서버가 지난 2시간 이내에 연결된 경우에도 "연결됨"이 이 열에 표시됩니다. 다른 시간에는 상태 열이 비어 있어 서버가 현재 방화벽에 연결되어 있지 않음을 나타냅니다.

다음 CLI 명령은 DHCP 서버 설정, 연결 상태 및 IoT 보안에 제공하는 데이터를 확인하는 데에도 유용합니다.

show iot dhcp-server status { all | server <server-name> }	**all**을 입력하면 방화벽에 구성된 모든 DHCP 서버, 연결된 포트 번호 및 현재 연결 상태가 있는 테이블이 표시됩니다. **server <server-name>** 를 입력하면 특정 DHCP 서버 및 해당 서버의 최근 활동에 대한 자세한 정보가 표시됩니다.

show iot eal dhcp-syslog-eal	이 명령은 DHCP 서버 syslog 메시지를 전달하는 EAL과 관련된 정보를 표시합니다.

디바이스 > 데이터 재배포

이러한 설정은 방화벽 또는 Panorama가 데이터를 재배포하는 데 사용하는 방법을 정의합니다.

무엇을 찾고 계신가요?	참조:
데이터 재배포 에이전트를 추가하거나 삭제합니다.	디바이스 > 데이터 재배포 > 에이전트
데이터 재배포 클라이언트에 대한 정보를 봅니다.	디바이스 > 데이터 재배포 > 클라이언트
데이터 재배포 에이전트 수집기 이름 및 사전 공유 키를 구성합니다.	디바이스 > 데이터 재배포 > 수집기 설정
데이터 재배포 에이전트가 데이터를 재배포할 때 포함하거나 제외하는 하위 네트워크를 정의합니다.	디바이스 > 데이터 재배포 > 네트워크 포함/제외

디바이스 > 데이터 재배포 > 에이전트

일련번호 또는 호스트 및 포트 정보를 사용하여 데이터 재배포 에이전트를 추가합니다.

데이터 재배포 에이전트 설정	설명
이름	데이터 재배포 에이전트의 이름을 입력합니다(최대 31자). 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
활성화됨	데이터 재배포 에이전트를 활성화하려면 이 옵션을 선택합니다.
다음을 사용하여 에이전트 추가	데이터 재배포 에이전트를 추가할 방법을 선택합니다. • 일련번호 - 이 옵션을 선택한 다음 일련번호를 선택합니다.

데이터 재배포 에이전트 설정	설명

	• 호스트 및 포트 - 이 옵션을 선택하고 다음 호스트 및 포트 정보를 입력합니다.
	  • 호스트 - 호스트 이름을 입력합니다.
	  • **LDAP** 프록시 - 호스트를 LDAP 프록시로 사용하려면 이 옵션을 선택합니다.
	  • 포트 - 에이전트가 요청을 수신하는 포트 번호를 입력합니다.
	  • 수집기 이 - 방화벽 또는 가상 시스템을 User-ID 에이전트로 식별하는 수집기 이름 및 사전 공유 키를 입력합니다.

데이터 형식	재배포할 데이터 유형(IP 사용자 매핑, IP 태그, 사용자 태그, HIP 또는 격리 목록)을 선택합니다.

데이터 재배포 에이전트를 구성한 후 재배포 에이전트에 대한 다음 정보를 볼 수 있습니다.

데이터 재배포 에이전트 정보	설명
일련 번호	에이전트의 식별 번호입니다.
호스트	호스트에 대한 정보입니다.
수집기 이름	수집기 에이전트의 이름입니다.
HIP	에이전트의 호스트 정보 프로파일입니다.
IP 사용자 매핑	IP 주소-사용자 이름 매핑 정보입니다.
IP 태그	IP 주소-태그 매핑 정보입니다.
격리 목록	검역 중인 기기의 목록을 표시합니다.
동적 사용자 그룹	사용자 이름-태그 매핑 정보입니다.
연결됨	에이전트가 재배포 서비스에 연결되어 있는지 나타냅니다.

디바이스 > 데이터 재배포 > 클라이언트

Device > **Data Redistribution** > **Clients**를 선택하여 각 재배포 클라이언트에 대해 다음 정보를 표시합니다.

재배포 에이전트 정보	설명
호스트 정보	클라이언트에 대한 호스트 정보입니다.
포트	재배포 클라이언트가 사용하는 포트입니다.
Vsys ID	재배포 클라이언트가 연결된 가상 시스템의 ID입니다.
버전	클라이언트의 PAN-OS 버전입니다.
상태	재배포 클라이언트의 상태를 표시합니다.
PDF/CSV	최소한의 읽기 전용 액세스 권한이 있는 관리 역할은 데이터 재배포 정보를 **PDF/CSV**로 내보낼 수 있습니다.
새로고침 연결	연결된 모든 재배포 클라이언트에 대한 정보를 업데이트합니다.

디바이스 > 데이터 재배포 > 수집기 설정

User-ID 재배포 에이전트에 대한 연결을 구성하려면 수집기 이름과 사전 공유 키를 입력합니다.

데이터 재배포 에이전트 설정 설정	설명
수집기 이름	재배포 에이전트를 식별하기 위해 수집기 이름(최대 255자의 영숫자)을 입력합니다.
수집기 사전 공유 키 / 수집기 사전 공유 키 확인	수집기에 대한 사전 공유 키(최대 255자의 영숫자)를 입력하고 확인합니다.

디바이스 > 데이터 재배포 > 네트워크 포함/제외

Include/Exclude Networks 목록을 사용하여 재배포 에이전트가 매핑을 재배포할 때 포함하거나 제외하는 하위 네트워크를 정의합니다.

업무	설명
추가하다	특정 하위 네트워크로 검색을 제한하려면 하위 네트워크 프로파일을 추가하고 다음 필드를 완료하십시오. • 이름 - 하위 네트워크를 식별하는 이름을 입력합니다.

업무	설명
	• 활성화됨 - 서버 모니터링을 위해 하위 네트워크를 포함하거나 제외하려면 이 옵션을 선택합니다. • 검색 - User-ID 에이전트가 하위 네트워크를 포함할지 또는 제외할지 선택합니다. • 네트워크 주소 - 서브네트워크의 IP 주소 범위를 입력합니다. 에이전트는 목록에 모든 암시적 제외 규칙을 적용합니다. 예를 들어 포함 옵션을 사용하여 하위 네트워크 10.0.0.0/8을 추가하면 목록에 추가하지 않더라도 에이전트는 다른 모든 하위 네트워크를 제외합니다. 에이전트가 명시적으로 포함된 하위 네트워크의 하위 집합을 제외하도록 하려는 경우에만 제외 옵션을 사용하여 항목을 추가하십시오. 예를 들어 포함 옵션으로 10.0.0.0/8을 추가하고 제외 옵션으로 10.2.50.0/22를 추가하면 User-ID 에이전트는 10.2.50.0/을 제외한 10.0.0.0/8의 모든 하위 네트워크에서 검색을 수행합니다. 22 및 10.0.0.0/8 외부의 모든 하위 네트워크를 제외합니다. 포함 프로파일을 추가하지 않고 제외 프로파일을 추가하면 에이전트는 추가한 하위 네트워크뿐만 아니라 모든 하위 네트워크를 제외합니다.
삭제	목록에서 하위 네트워크를 제거하려면 선택한 다음 삭제합니다. 팁: 구성을 삭제하지 않고 네트워크 포함/제외 목록에서 하위 네트워크를 제거하려면 하위 네트워크 프로파일을 편집하고 사용을 선택 취소합니다.
사용자 정의 네트워크 포함/제외	기본적으로 에이전트는 하위 네트워크를 추가한 순서대로 위에서부터 맨 아래로까지 평가합니다. 평가 순서를 변경하려면 사용자 지정 네트워크 시퀀스 포함/제외를 클릭합니다. 그런 다음 하위 네트워크를 추가, 삭제, 위로 이동 또는 아래로 이동하여 사용자 지정 평가 순서를 생성할 수 있습니다.

디바이스 > 디바이스 검역

Device > **Device Quarantine**(디바이스 디바이스 검역) 페이지에는 검역 목록에 있는 디바이스가 표시됩니다.

디바이스는 다음 작업의 결과로 검역 목록에 나타납니다.

- 시스템 관리자가 수동으로 이 목록에 디바이스를 추가했습니다.

  디바이스를 수동으로 추가하려면 호스트 **ID**를 입력하고 선택적으로 분리해야 하는 디바이스의 일련번호를 입력합니다.
- 시스템 관리자는 트래픽, GlobalProtect, 위협 로그 또는 통합 로그에서 호스트 ID 열을 선택하고 해당 열에서 디바이스를 선택한 다음 디바이스 차단을 선택했습니다.
- 디바이스가 격리 목록에 자동으로 추가됨:
  - 일치 목록에 기본 제공 작업이 격리로 설정된 보안 정책 규칙과 함께 로그 전달 프로파일을 사용합니다.

    호스트 *ID*는 *GlobalProtect* 로그에 자동으로 표시됩니다. 호스트 *ID*가 트래픽, 위협 또는 통합 로그에 표시되려면 방화벽에 소스 디바이스가 검역소로 설정된 보안 정책 규칙이 하나 이상 있어야 합니다. 보안 정책에 이 설정이 없으면 트래픽, 위협 또는 통합 로그에 호스트 *ID*가 없고 로그 포워딩 프로파일이 적용되지 않습니다.
  - HIP를 사용하여 기본 제공 작업이 격리로 설정된 로그 설정을 일치시킵니다.

    방화벽에는 *GlobalProtect* 디바이스를 수동 또는 자동으로 격리 목록에 추가하고 격리된 디바이스에 대한 로그인을 차단하려면 GlobalProtect 구독 라이선스가필요합니다.
- API를 사용하여 디바이스를 검역 목록에 추가했습니다.
- 방화벽이 재배포 항목의 일부로 검역 목록을 수신했습니다(검역 목록은 다른 Panorama 어플라이언스 또는 방화벽에서 재배포되었습니다).

디바이스 검역소 테이블에는 다음 필드가 포함됩니다.

필드	설명
호스트 ID	차단된 호스트의 호스트 ID입니다.
이유	디바이스가 분리된 이유입니다. **Admin Add**의 이유는 관리자가 테이블에 디바이스를 수동으로 추가했음을 의미합니다.
타임스탬프	관리자 또는 보안 정책 규칙이 디바이스를 검역 목록에 추가한 시간입니다.
소스 디바이스/앱	분리 목록에 디바이스를 추가한 Panorama, 방화벽 또는 타사 앱의 IP 주소입니다.

필드	설명
일련번호	(선택 사항) 분리된 디바이스의 일련번호(사용 가능한 경우).
사용자명	(선택 사항) 디바이스가 분리되었을 때 로그인한 GlobalProtect 클라이언트 사용자의 사용자명입니다.

격리된 디바이스 목록을 pdf 또는 csv 파일로 내보낼 수 있습니다.

디바이스 > VM 정보 소스

이 탭을 사용하여 VMware ESXi 서버, VMware vCenter 서버, Amazon Web Services Virtual Private Cloud(AWS-VPC) 또는 Google Compute Engine(GCE) 소스에 배포된 VM(가상 머신)의 변경 사항을 사전에 추적할 수 있습니다.

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 여러 *NSX* 보안 그룹에 걸쳐 *IP* 주소가 겹치는 경우 정책을 적절하게 시행할 수 있도록 하기 때문에 동적 주소 그룹에서 일치 기준을 정의하기 위한 전체 컨텍스트를 제공합니다.

하나의 *IP* 주소에 최대 *32*개의 태그를 등록할 수 있습니다.

VM 정보 소스를 모니터링하는 방법에는 두 가지가 있습니다.

- 방화벽은 VMware ESXi 서버, VMware vCenter 서버, GCE 인스턴스 또는 AWS-VPC를 모니터링하고 모니터링되는 소스에 구성된 게스트를 프로비저닝하거나 수정할 때 변경 사항을 검색할 수 있습니다. 방화벽에서 최대 10개의 소스(구성된 모든 가상 시스템의 모든 소스의 누적)를 구성할 수 있습니다.

  방화벽이 고가용성(HA) 구성으로 구성된 경우 다음 조건이 적용됩니다.

  - 능동형/수동형 **HA** 구성 - 능동형 방화벽만 VM 정보 소스를 모니터링합니다.
  - 능동형/능동형 **HA** 구성 - ## 우선 순위 값이 있는 방화벽만 VM 정보 소스를 모니터링합니다.

  VM 정보 소스 및 동적 주소 그룹이 어떻게 동기적으로 작동하고 가상 환경의 변경 사항을 모니터링할 수 있는지에 대한 정보는 VM-시리즈 배포 가이드를 참조하십시오.
- IP 주소-사용자명 매핑의 경우 Windows User-ID 에이전트 또는 방화벽에서 VM 정보 소스를 구성하여 VMware ESXi 및 vCenter 서버를 모니터링하고 서버에 구성된 게스트를 프로비저닝하거나 수정할 때 변경 사항을 검색할 수 있습니다. Windows User-ID 에이전트는 최대 100개의 소스를 지원합니다. AWS 및 Google Compute Engine에 대한 지원은 User-ID 에이전트에 사용할 수 없습니다.

  모니터링되는 *ESXi* 또는 *vCenter* 서버의 각 *VM*에는 *VMware Tools*가 설치되어 실행 중이어야 합니다. *VMware Tools*는 각 *VM*에 할당된 *IP* 주소 및 기타 값에 대한 기능을 제공합니다.

모니터링되는 VM에 할당된 값을 수집하기 위해 방화벽은 다음 표의 특성을 모니터링합니다.

VMware 소스에서 모니터링되는 속성
• UUID • 이름

VMware 소스에서 모니터링되는 속성

- 게스트 OS
- 주석
- VM 상태 - 전원 상태는 `powerOff`,`poweredOn`, `StandBy` 또는 `unknown`일 수 있습니다.
- 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 및 호스트 IP 주소.

AWS-VPC에서 모니터링되는 속성

- 건축학
- 게스트 OS
- 이미지 ID
- 인스턴스 ID
- 인스턴스 상태
- 인스턴스 유형
- 키 이름
- 배치 - 테넌시, 그룹 이름 및 가용 영역
- 사설 DNS 이름
- 공개 DNS 이름
- 서브넷 ID
- 태그(키, 값); 인스턴스당 최대 18개의 태그 지원
- VPC ID

Google Compute Engine(GCE)에 대해 모니터링되는 속성

- VM의 호스트 이름
- 머신 유형
- 프로젝트 ID
- 소스(OS 유형)
- 상태
- 서브네트워크

Google Compute Engine(GCE)에 대해 모니터링되는 속성
• VPC 네트워크 • 영역

추가 - VM 모니터링을 위한 새 소스를 추가하고 모니터링 중인 소스를 기반으로 세부 정보를 입력합니다.

- VMware ESXi 또는 vCenter Server의 경우 VMware ESXi 및 vCenter Server에 대한 VM 정보 소스 사용 설정을 참조하십시오.
- AWS-VPC의 경우 AWS VPC에 대한 VM 정보 소스 활성화 설정을 참조하십시오.
- Google Compute Engine(GCE)의 경우 Google Compute Engine용 VM 정보 소스 활성화 설정을 참조하십시오.

연결 새로 고침 - 온스크린 디스플레이에서 연결 상태를 새로 고침합니다. 이것은 방화벽과 모니터링되는 소스 간의 연결을 새로 고침하지 않습니다.

삭제 - 선택한 모든 구성된 VM 정보 소스를 삭제합니다.

PDF/CSV - VM 정보 소스 구성 테이블을 PDF 또는 CSV(쉼표로 구분된 값) 파일로 내보냅니다. 구성 테이블 내보내기를 참조하십시오.

VMware ESXi 및 vCenter Server에 대한 VM 정보 소스 사용 설정

다음 표에서는 VMware ESXi 및 vCenter 서버에 대해 VM 정보 소스를 사용하도록 구성할 수 있는 설정을 설명합니다.

가상 머신에 대한 태그를 검색하려면 방화벽에 *VMware ESXi* 및 *vCenter* 서버에 대한 읽기 전용 액세스 권한이 있는 계정이 필요합니다.

VMware ESXi 또는 **vCenter Server**에 대한 **VM** 정보 소스 사용 설정	
이름	모니터링되는 소스를 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
유형	모니터링 중인 호스트/소스가 **ESXi** 서버인지 또는 **vCenter** 서버인지 선택합니다.
설명	(선택 사항) 레이블을 추가하여 소스의 위치 또는 기능을 식별합니다.
포트	호스트/소스가 수신하는 포트를 지정합니다(기본 포트 443).
활성화됨	기본적으로 방화벽과 구성된 소스 간의 통신은 활성화되어 있습니다.

VMware ESXi 또는 vCenter Server에 대한 VM 정보 소스 사용 설정	
	모니터링되는 소스와 방화벽 간의 연결 상태는 인터페이스에 다음과 같이 표시됩니다. •  연결됨 •  연결 끊김 •  보류 중; 모니터링되는 소스가 비활성화되면 연결 상태도 노란색으로 표시됩니다. 호스트와 방화벽 간의 통신을 비활성화하려면 사용 옵션을 선택 취소합니다.
타임아웃	호스트가 응답하지 않는 경우 모니터링되는 소스에 대한 연결이 닫히는 인터벌을 시간 단위로 입력합니다(범위는 2–10, 기본값은 2). (선택 사항) 기본값을 변경하려면 소스 연결이 끊겼을 때 타임아웃을 활성화하고 값을 지정합니다. 지정된 제한에 도달했을 때 호스트에 액세스할 수 없거나 호스트가 응답하지 않으면 방화벽은 소스에 대한 연결을 닫습니다.
소스	모니터링 중인 호스트/소스의 FQDN 또는 IP 주소를 입력합니다.
사용자명	소스에 인증하는 데 필요한 사용자명을 지정합니다.
비밀번호	비밀번호를 입력하고 입력을 확인합니다.
업데이트 인터벌	방화벽이 소스에서 정보를 검색하는 인터벌(초)을 지정합니다(범위는 5–600, 기본값은 5).

AWS VPC용 VM 정보 소스를 활성화하는 설정

다음 표에서는 AWS VPC에 대한 VM 정보 소스를 사용하도록 구성한 설정에 대해 설명합니다.

AWS VPC용 VM 정보 소스를 활성화하는 설정	
이름	모니터링되는 소스를 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
유형	**AWS VPC**를 선택합니다.

AWS VPC용 VM 정보 소스를 활성화하는 설정	
설명	(선택 사항) 레이블을 추가하여 소스의 위치 또는 기능을 식별합니다.
활성화	기본적으로 방화벽과 구성된 소스 간의 통신은 활성화되어 있습니다. 모니터링되는 소스와 방화벽 간의 연결 상태는 인터페이스에 다음과 같이 표시됩니다. •  연결됨 •  연결 끊김 •  보류 중. 모니터링된 소스를 사용하지 않도록 설정하면 연결 상태가 노란색으로 표시됩니다. 활성화 옵션을 지우면 호스트와 방화벽 간의 통신을 비활성화합니다.
소스	가상 프라이빗 클라우드가 있는 URI를 추가합니다. 예를 들어 ec2.us-west-1.amazonaws.com 구문은 ec2.<*your_AWS_region*>.amazonaws.com이고, AWS 중국의 경우 ec2.<AWS_region>.amazonaws.com.cnn입니다.
키 ID 액세스	AWS 계정을 소유하거나 액세스 권한이 있는 사용자를 고유하게 식별하는 영숫자 텍스트 문자열을 입력합니다. 이 정보는 AWS 보안 자격 증명의 일부입니다. 방화벽에는 AWS 서비스에 대한 API 호출에 디지털 서명하려면 액세스 키 ID와 보안 액세스 키와 같은 자격 증명이 필요합니다.
보안 액세스 키	암호를 입력하고 항목을 확인합니다.
업데이트 인터벌	방화벽이 소스에서 정보를 검색하는 인터벌을 몇 초 만에 지정합니다(범위는 60~1,200개, 기본값은 60개).
타임 아웃	호스트가 응답하지 않는 경우 모니터링된 소스에 대한 연결이 닫힌 후의 인터벌(기본값은 2)입니다. (선택사항) 소스 연결이 끊어지면 타임아웃을 활성화합니다. 지정된 제한에 도달하면 소스에 액세스할 수 없거나 소스가 응답하지 않으면 방화벽이 소스에 대한 연결을 닫습니다.
VPC ID	예를 들어 vpc-1a2b3c4d와 같은 AWS-VPC의 ID를 입력합니다. 이 VPC 내에 배포되는 EC2 인스턴스만 모니터링됩니다.

AWS VPC용 VM 정보 소스를 활성화하는 설정	
	계정이 기본 VPC를 사용하도록 구성된 경우 기본 VPC ID가 AWS 계정 속성 아래에 나열됩니다.

Google Compute Engine에 대한 VM 정보 소스 사용 설정

디바이스 > **VM** 정보 원본 > 추가

다음 표에서는 Google Cloud Platform에서 Google Compute Engine 인스턴스에 대한 VM 정보 소스를 사용 설정하기 위해 구성해야 하는 설정을 설명합니다. 방화벽(실제 또는 가상 온프레미스 또는 Google Cloud에서 실행)이 지정된 프로젝트의 특정 Google Cloud 영역에서 실행 중인 인스턴스에 대한 태그, 라벨 및 기타 메타데이터를 검색할 수 있도록 Google Compute Engine(GCE) 인스턴스 모니터링을 활성화합니다. Google Cloud Platform의 VM 시리즈에 대한 자세한 내용은 VM 시리즈 배포 가이드를 참조합니다.

Google Compute Engine에 대한 VM 정보 소스 사용 설정	
이름	모니터링되는 소스를 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
유형	**Google Compute Engine**을 선택합니다.
설명	(선택 사항) 레이블을 추가하여 소스의 위치 또는 기능을 식별합니다.
활성화됨	방화벽과 구성된 원본 간의 통신은 기본적으로 사용하도록 설정되어 있습니다. 모니터링되는 소스와 방화벽 간의 연결 상태는 인터페이스에 다음과 같이 표시됩니다.—연결됨 - 연결 끊김 - 보류 중 또는 모니터링되는 소스가 비활성화됩니다. • 연결됨 — • - 연결 해제됨 • - 대기 중이거나 모니터링되는 소스가 비활성화되었습니다. 구성된 소스와 방화벽 간의 통신을 비활성화하려면 활성화됨 옵션을 선택 취소합니다.

Google Compute Engine에 대한 **VM** 정보 소스 사용 설정	
	통신을 비활성화하면 등록된 모든 IP 주소와 태그가 연결된 동적 주소 그룹에서 제거됩니다. 즉, 이 GCP 프로젝트의 GCE 인스턴스에는 정책 규칙이 적용되지 않습니다.
서비스 인증 유형	GCE 또는 서비스 계정에서 실행 중인 VM 시리즈를 선택합니다. • **GCE**에서 실행되는 **VM** 시리즈 - VM 모니터링을 사용 설정하는 하드웨어 기반 또는 VM 시리즈 방화벽이 Google Cloud Platform 내에 배포되지 않은 경우 이 옵션을 선택합니다. • 서비스 계정 - Google Cloud Platform에 배포되지 않은 방화벽에서 Google Cloud Engine 인스턴스를 모니터링하는 경우 이 옵션을 선택합니다. 이 옵션을 사용하면 개별 최종 사용자 계정을 사용하는 대신 가상 머신 또는 애플리케이션에 속한 특수 Google 계정을 사용할 수 있습니다. 서비스 계정에는 Google API에 대한 액세스를 승인하고 가상 머신 메타데이터에 대해 Google Cloud 프로젝트의 가상 머신을 쿼리할 수 있는 IAM 정책(**Compute Engine** > **Compute** 뷰어 권한)이 있어야 합니다.
서비스 계정 자격 증명	(서비스 계정만 해당) 서비스 계정에 대한 자격 증명이 포함된 JSON 파일을 업로드합니다. 이 파일을 사용하면 방화벽이 인스턴스를 인증하고 메타데이터에 대한 액세스 권한을 부여할 수 있습니다. Google Cloud 콘솔에서 계정을 만들 수 있습니다(**IAM** 및 관리자 > 서비스 계정). 계정 생성, 계정에 키 추가, 방화벽에 업로드해야 하는 JSON 파일 다운로드 방법에 대한 정보는 Google 문서를 참조하십시오.
프로젝트 ID	모니터링하려는 Google Cloud 프로젝트를 고유하게 식별하는 영숫자 텍스트 문자열을 입력합니다.
영역 이름	영역 정보를 최대 63자 길이의 문자열로 입력합니다. 예: **us-west1-a**.
업데이트 인터벌	방화벽이 소스에서 정보를 검색하는 인터벌(초)을 지정합니다(범위는 60~1,200, 기본값은 60).
타임아웃	호스트가 응답하지 않는 경우 모니터링되는 소스에 대한 연결이 종료되는 인터벌(시간)입니다(기본값은 2). (선택 사항) 소스 연결이 끊겼을 때 타임아웃을 활성화합니다. 지정된 제한에 도달했을 때 소스에 액세스할 수 없거나 응답하지 않으면 방화벽이 소스에 대한 연결을 닫습니다. 소스 연결이 끊어지면 이 프

Google Compute Engine에 대한 VM 정보 소스 사용 설정	
	로젝트에서 등록된 모든 IP 주소와 태그가 동적 주소 그룹에서 제거됩니다.

디바이스 > 문제 해결

- 디바이스 > 문제 해결
- **Panorama** > 관리되는 디바이스 > 문제 해결

디바이스 그룹 또는 템플릿 구성 변경 사항을 커밋하기 전에 웹 인터페이스에서 기능을 테스트하여 변경 사항으로 인해 연결 문제가 실행 중인 구성에 도입되었는지, 정책이 트래픽을 올바르게 허용하거나 거부하는지 확인하십시오.

- 정책 일치 테스트
  - 보안 정책 일치
  - QoS 정책 일치
  - 인증 정책 일치
  - 복호화/SSL 정책 일치
  - NAT 정책 일치
  - 정책 기반 포워딩 정책 일치
  - DoS 정책 일치
- 연결 테스트
  - 라우팅
  - Wildfire 테스트
  - 위협 금고
  - 핑(ping)
  - 경로 추적
  - 로그 수집기 연결
  - 외부 동적 목록
  - 서버 업데이트
  - Cloud Logging 서비스 상태 테스트
  - Cloud GP 서비스 상태 테스트

보안 정책 일치

필드	설명
테스트 구성	

필드	설명
테스트 선택	실행할 정책 일치 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
수신지	트래픽의 대상 영역을 선택합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
대상 포트	트래픽이 의도된 특정 대상 포트를 입력합니다.
소스 사용자	트래픽이 발생한 사용자를 입력합니다.
프로토콜	라우팅에 사용되는 IP 프로토콜을 입력합니다. 0에서 255까지 가능합니다.
첫 번째 허용 규칙까지 모든 잠재적 일치 규칙 표시	첫 번째 일치 규칙 결과까지 모든 잠재적 규칙 일치를 표시하려면 이 옵션을 활성화합니다. 테스트 결과에서 첫 번째로 일치하는 규칙만 반환하려면 비활성화(지우기)합니다.
애플리케이션	테스트할 애플리케이션 트래픽을 선택합니다.
카테고리	테스트할 트래픽 카테고리를 선택합니다.
(방화벽만 해당) HIP 마스크 확인	네트워크에 액세스하는 최종 디바이스의 보안 상태를 확인하려면 선택합니다.
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다. (Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다. • 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.

필드	설명

	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.
	  • ###### ## ## ##### - 디바이스의 Panorama 설정은 Panorama에서 정책을 푸시하는 것을 허용하지 않습니다.

QoS 정책 일치

필드	설명
테스트 구성	
테스트 선택	실행할 정책 일치 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
수신지	트래픽의 대상 영역을 선택합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
대상 포트	트래픽이 의도된 특정 대상 포트를 입력합니다.
소스 사용자	트래픽이 발생한 사용자를 선택합니다.

필드	설명
프로토콜	라우팅에 사용되는 IP 프로토콜을 입력합니다. 0에서 255까지 가능합니다.
애플리케이션	테스트할 애플리케이션 트래픽을 선택합니다.
카테고리	테스트할 트래픽 카테고리를 선택합니다.
코드포인트 유형	테스트할 코드포인트 인코딩 유형을 선택합니다.
코드 포인트 값	코드 포인트 인코딩 값을 지정하십시오. • **DSCP**—0 ~ 63 • **ToS**—0 ~ 7

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.
	  • ###### ## ## ##### - 디바이스의 Panorama 설정은 Panorama에서 정책을 푸시하는 것을 허용하지 않습니다.

인증 정책 일치

필드	설명
테스트 구성	
테스트 선택	실행할 정책 일치 테스트를 선택합니다.

필드	설명
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
수신지	트래픽의 대상 영역을 선택합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
카테고리	테스트할 트래픽 카테고리를 선택합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.
	  • ###### ## ## ##### - 디바이스의 Panorama 설정은 Panorama에서 정책을 푸시하는 것을 허용하지 않습니다.

복호화/SSL 정책 일치

필드	설명
테스트 구성	
테스트 선택	실행할 정책 일치 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
수신지	트래픽의 대상 영역을 선택합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
애플리케이션	테스트할 애플리케이션 트래픽을 선택합니다.
카테고리	테스트할 트래픽 카테고리를 선택합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

NAT 정책 일치

필드	설명
테스트 구성	
테스트 선택	실행할 정책 일치 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
수신지	트래픽의 대상 영역을 선택합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
소스 포트	트래픽이 발생한 특정 포트를 입력합니다.
대상 포트	트래픽이 의도된 특정 대상 포트를 입력합니다.
프로토콜	라우팅에 사용되는 IP 프로토콜을 입력합니다. 0에서 255까지 가능합니다.
인터페이스로	트래픽이 의도된 디바이스의 대상 인터페이스를 입력합니다.
HA 디바이스 ID	HA 디바이스의 ID를 입력하십시오. • **0** - 기본 HA 피어 • **1** - 보조 HA 피어
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다. (Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다. • 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.

필드	설명

	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.
	  • ###### ## ## ##### - 디바이스의 Panorama 설정은 Panorama에서 정책을 푸시하는 것을 허용하지 않습니다.

정책 기반 포워딩 정책 일치

필드	설명
테스트 구성	
테스트 선택	실행할 정책 일치 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
인터페이스에서	트래픽이 시작된 디바이스의 인터페이스를 입력합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
대상 포트	트래픽이 의도된 특정 대상 포트를 입력합니다.
소스 사용자	트래픽이 발생한 사용자를 입력합니다.

필드	설명
프로토콜	라우팅에 사용되는 IP 프로토콜을 입력합니다. 0에서 255까지 가능합니다.
애플리케이션	테스트할 애플리케이션 트래픽을 선택합니다.
HA 디바이스 ID	HA 디바이스의 ID: • **0** - 기본 HA 피어 • **1** - 보조 HA 피어

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.
	  • ###### ## ## ##### - 디바이스의 Panorama 설정은 Panorama에서 정책을 푸시하는 것을 허용하지 않습니다.

DoS 정책 일치

필드	설명
테스트 구성	
테스트 선택	실행할 정책 일치 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.

필드	설명
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
발신지	트래픽이 발생한 영역을 입력합니다.
수신지	트래픽의 대상 영역을 선택합니다.
인터페이스에서	트래픽이 시작된 디바이스의 인터페이스를 입력합니다.
인터페이스로	트래픽이 의도된 디바이스의 대상 인터페이스를 입력합니다.
소스	트래픽이 발생한 IP 주소를 입력합니다.
데스티네이션	트래픽의 대상 IP 주소를 입력합니다.
대상 포트	트래픽이 의도된 특정 대상 포트를 입력합니다.
소스 사용자	트래픽이 발생한 사용자를 입력합니다.
프로토콜	라우팅에 사용되는 IP 프로토콜을 입력합니다. 0에서 255까지 가능합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

라우팅

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
FiB 조회, Mfib 조회	조회에 대해 다음 중 하나를 선택합니다. • **FiB** - 경로 테이블 활성화 내에서 경로 조회 수행 • **Mfib** - 활성 경로 테이블 내에서 멀티캐스트 경로 조회 수행
대상 IP	트래픽이 의도된 IP 주소를 입력합니다.
가상 라우터	라우팅 테스트가 수행되는 특정 가상 라우터입니다. 드롭다운에서 가상 라우터를 선택합니다.
ECMP	
소스 IP	트래픽이 발생한 특정 IP 주소를 입력합니다.
소스 포트	트래픽이 발생한 특정 포트를 입력합니다.
대상 IP	트래픽이 의도된 특정 IP 주소를 입력합니다.
대상 포트	트래픽이 의도된 특정 대상 포트를 입력합니다.
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다. (Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다. • 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다. • 방화벽 - 트래픽을 처리하는 방화벽의 이름 • 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.

필드	설명

	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

Wildfire 테스트

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
채널	Wildfire 채널 선택: ## 또는 ###.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

위협 금고

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

핑(ping)

핑(ping) 문제 해결 테스트는 PAN-OS 9.0 이상의 버전을 실행하는 방화벽에서만 지원됩니다.

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.

필드	설명
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
라우팅 테이블 우회, 지정된 인터페이스 사용	라우팅 테이블을 무시하고 지정된 인터페이스를 사용하려면 이 옵션을 활성화합니다. 구성된 라우팅 테이블을 테스트하려면 이 옵션을 비활성화(지우기)합니다.
카운트	보낼 요청 수를 입력합니다. 기본 개수는 5입니다.
에코 요청 패킷(IPv4)을 조각화하지 마십시오.	테스트에 대한 에코 요청 패킷을 조각화하지 않으려면 이 옵션을 활성화합니다. 비활성화
IPv6 대상으로 강제 실행	IPv6 대상에 대한 테스트를 강제 실행하려면 활성화합니다.
인터벌	요청 사이의 지연을 초 단위로 지정합니다(범위는 1~2,000,000,000).
소스	에코 요청의 소스 주소를 입력합니다.
주소를 기호로 인쇄하지 마십시오.	테스트 결과에 IP 주소를 표시하고 IP 주소 호스트 이름을 확인하지 않으려면 이 옵션을 활성화합니다. IP 주소 호스트 이름을 확인하려면 비활성화(지우기)하십시오.
패턴	16진수 채우기 패턴을 지정합니다.
크기	요청 패킷의 크기를 바이트 단위로 입력합니다(범위는 0~65468).
ToS	IP 서비스 유형 값을 입력합니다(범위는 1~255).
TTL	IP TTL(Time-to-Live) 값을 홉 단위로 입력합니다. IPv6 홉 제한 값(범위는 1~255)입니다.
자세한 출력 표시	테스트 결과의 자세한 출력을 표시하려면 활성화합니다.
호스트	원격 호스트의 호스트 이름 또는 IP 주소를 입력합니다.
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다. (Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다. • 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다. • 방화벽 - 트래픽을 처리하는 방화벽의 이름

필드	설명

	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

경로 추적

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
IPv4 사용	선택한 디바이스의 IPv4 주소를 사용하려면 활성화합니다.
IPv6 사용	선택한 디바이스의 IPv6 주소를 사용하려면 활성화합니다.
첫 번째 TTL	첫 번째 나가는 프로브 패킷에 사용된 TTL(Time-to-Live)을 입력합니다(범위는 1~255).
최대 TTL	최대 TTL(Time-to-Live) 홉을 입력합니다(범위는 1~255).
포트	프로브에 사용된 기본 포트 번호를 입력합니다.
ToS	IP 서비스 유형 값을 입력합니다(범위는 1~255).
대기	응답을 기다리는 시간(초)을 입력합니다(범위: 1~99,999).
정지	프로브 사이에 일시 중지할 시간을 밀리초 단위로 입력합니다(범위는 1~2,000,000,000).

필드	설명
"분할 금지" 비트 설정	경로가 구성된 MTU(최대 전송 단위)를 지원할 수 없는 경우 ICMP 패킷을 여러 패킷으로 분할하지 않으려면 이 옵션을 활성화합니다.
소켓 수준 디버깅 활성화	이 옵션을 활성화하면 소켓 수준에서 디버그할 수 있습니다.
게이트웨이	최대 8개의 느슨한 소스 경로 게이트웨이를 지정합니다.
주소를 기호로 인쇄하지 마십시오.	테스트 결과에 IP 주소를 표시하고 IP 주소 호스트 이름을 확인하지 않으려면 이 옵션을 활성화합니다. IP 주소 호스트 이름을 확인하려면 비활성화(지우기)하십시오.
라우팅 테이블을 우회하고 호스트로 직접 전송	구성된 라우팅 테이블을 무시하고 호스트에서 직접 테스트하려면 이 옵션을 활성화합니다.
소스	나가는 프로브 패킷에 소스 주소를 입력합니다.
호스트	원격 호스트의 호스트 이름 또는 IP 주소를 입력합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

로그 수집기 연결

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.

필드	설명
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택된 디바이스 및 가상 시스템을 나열합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

외부 동적 목록

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
(Panorama만 해당) 디바이스 선택	디바이스/**VSYS**를 선택하여 정책 기능을 테스트할 디바이스 및 가상 시스템을 지정합니다. 관리자 및 디바이스 그룹 및 템플릿 사용자는 액세스 도메인을 기반으로 디바이스 및 가상 시스템이 제공됩니다. 또한 Panorama 관리 서버를 디바이스로 선택할 수 있습니다.
(Panorama 전용) 선택한 디바이스	테스트를 위해 선택한 디바이스 및 가상 시스템을 나열합니다.
URL 테스트	연결 테스트를 위한 URL을 지정합니다.
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.

필드	설명

	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

서버 업데이트

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.

결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다.
	(Panorama만 해당) 여러 관리 디바이스에 대한 테스트를 실행할 때 결과는 테스트된 각 디바이스에 대해 다음 정보를 표시합니다.
	• 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다.
	• 방화벽 - 트래픽을 처리하는 방화벽의 이름
	• 상태 - 테스트 상태를 나타냅니다. ## 또는 ##.
	• 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.
	  • N/A - 테스트가 디바이스에 적용되지 않았습니다.
	  • ##### #### ## - 디바이스 연결이 끊어졌습니다.

Cloud Logging 서비스 상태 테스트

Cloud Logging 서비스에 대한 연결 상태를 테스트합니다. 이 테스트는 설치된 Cloud Services 플러그인 버전 1.3 이상을 실행하는 Panorama 관리 서버에서만 사용할 수 있습니다.

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다. 여러 관리되는 디바이스에 대한 테스트를 실행할 때 결과에는 테스트된 각 디바이스에 대한 다음 정보가 표시됩니다. • 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다. • 방화벽 - 트래픽을 처리하는 방화벽의 이름 • 상태 - 테스트 상태를 나타냅니다. ## 또는 ##. • 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.

Cloud GP 서비스 상태 테스트

GlobalProtect as a Service에 대한 연결 상태를 테스트합니다. 이 테스트는 설치된 Cloud Services 플러그인 버전 1.3 이상을 실행하는 Panorama 관리 서버에서만 사용할 수 있습니다.

필드	설명
테스트 선택	실행할 연결 테스트를 선택합니다.
결과	실행된 테스트의 결과 세부 정보를 보려면 선택합니다. 여러 관리되는 디바이스에 대한 테스트를 실행할 때 결과에는 테스트된 각 디바이스에 대한 다음 정보가 표시됩니다. • 디바이스 그룹 - 트래픽을 처리하는 방화벽이 속한 디바이스 그룹의 이름입니다. • 방화벽 - 트래픽을 처리하는 방화벽의 이름 • 상태 - 테스트 상태를 나타냅니다. ## 또는 ##. • 결과 - 테스트 결과를 표시합니다. 테스트를 수행할 수 없으면 다음 중 하나가 표시됩니다.

디바이스 > 가상 시스템

가상 시스템(vsys)은 물리적 방화벽 내에서 별도로 관리할 수 있는 독립(가상) 방화벽 인스턴스입니다. 각 vsys는 자체 보안 정책, 인터페이스 및 관리자가 있는 독립적인 방화벽이 될 수 있습니다. vsys를 사용하면 방화벽이 제공하는 모든 정책, 보고 및 가시성 기능의 관리를 세분화할 수 있습니다.

예를 들어 재무 부서와 연결된 트래픽에 대한 보안 기능을 사용자 지정하려는 경우 재무 vsys를 정의한 다음 해당 부서에만 관련된 보안 정책을 정의할 수 있습니다. 정책 관리를 최적화하기 위해 개별 vsys에 대한 액세스를 허용하는 vsys 관리자 계정을 만드는 동안 전체 방화벽 및 네트워크 기능에 대해 별도의 관리자 계정을 유지 관리할 수 있습니다. 이렇게 하면 재무 부서의 vsys 관리자가 해당 부서에 대한 보안 정책만 관리할 수 있습니다.

네트워킹 기능(예: 정적 및 동적 라우팅, 인터페이스의 IP 주소, IPSec 터널)은 전체 방화벽과 모든 가상 시스템과 관련이 있습니다. 가상 시스템 구성(기기 > 가상 시스템)은 방화벽 수준 및 네트워크 수준 기능(예: 정적 및 동적 라우팅, 인터페이스의 IP 주소, IPSec 터널, VLAN, 가상 와이어, 가상 라우터, GRE 터널, DHCP, DNS 프록시, QoS, LLDP 및 네트워크 프로필)을 제어하지 않습니다. 각 vsys에 대해 물리적 및 논리적 방화벽 인터페이스(VLAN 및 가상 와이어 포함) 및 보안 영역 모음을 지정할 수 있습니다. 각 vsys에 대한 라우팅 분할이 필요한 경우 추가 가상 라우터를 생성 및 할당하고 필요에 따라 인터페이스, VLAN 및 가상 와이어를 할당해야 합니다.

Panorama 템플릿을 사용하여 가상 시스템을 정의하는 경우 하나의 vsys를 기본값으로 구성할 수 있습니다. 기본 vsys 및 다중 가상 시스템 기능은 템플릿 커밋 중에 방화벽이 vsys 특정 구성을 수락하는지의 여부를 결정합니다.

- 다중 가상 시스템 기능이 활성화된 방화벽은 템플릿에 정의된 모든 vsys에 대한 vsys 관련 구성을 허용합니다.
- 다중 가상 시스템 기능이 활성화되지 않은 방화벽은 기본 vsys에 대해서만 vsys 관련 구성을 허용합니다. 기본 vsys를 구성하지 않으면 이러한 방화벽은 vsys 관련 구성을 허용하지 않습니다.

> *PA-400* 시리즈, *PA-3200* 시리즈, *PA-5200* 시리즈, *PA-5400* 시리즈 및 *PA-7000* 시리즈 방화벽은 여러 가상 시스템을 지원합니다. 그러나 *PA-400* 시리즈 및 *PA-3200* 시리즈 방화벽에는 여러 가상 시스템을 활성화하기 위한 라이선스가 필요합니다. *PA-220* 및 *PA-800* 시리즈 방화벽은 다중 가상 시스템을 지원하지 않습니다.

여러 가상 시스템을 활성화하기 전에 다음을 고려하십시오.

- vsys 관리자는 할당된 가상 시스템별로 보안 정책에 필요한 모든 항목을 생성하고 관리합니다.
- 영역은 vsys 내의 개체입니다. 정책 또는 정책 개체를 정의하기 전에 정책 또는 개체 탭의 드롭다운에서 적절한 가상 시스템을 선택합니다.
- 원격 로깅 대상(SNMP, syslog 및 이메일), 애플리케이션, 서비스 및 프로파일을 모든 가상 시스템(공유) 또는 단일 vsys에서 사용할 수 있도록 설정할 수 있습니다.
- 여러 가상 시스템이 있는 경우 User-ID 허브로 vsys를 선택하여 가상 시스템 간에 IP 주소-사용자명 매핑 정보를 공유할 수 있습니다.

- 전역적으로(방화벽의 모든 가상 시스템에 대해) 또는 vsys 특정 서비스 경로(디바이스 > 설정 > 서비스)를 구성할 수 있습니다.
- 로컬 방화벽에서만 vsys의 이름을 바꿀 수 있습니다. Panorama에서는 vsys 이름 변경이 지원되지 않습니다. Panorama에서 vsys의 이름을 변경하면 결과는 완전히 새로운 vsys가 되거나 새 vsys 이름이 방화벽의 잘못된 vsys에 매핑됩니다.

가상 시스템을 정의하기 전에 먼저 방화벽에서 다중 가상 시스템 기능을 활성화해야 합니다. 디바이스 > 설정 > 관리를 선택한 다음 일반 설정을 편집하고 다중 가상 시스템 기능을 선택한 다음 확인을 클릭합니다. 그러면 **Device** > **Virtual** 시스템 페이지가 추가됩니다. vsys 추가 페이지를 선택한 다음 다음 정보를 지정하십시오.

가상 시스템 설정	설명
ID	vsys에 대한 정수 식별자를 입력합니다. 지원되는 가상 시스템의 수에 대한 정보는 방화벽 모델의 데이터 시트를 참조하십시오. *Panorama* 템플릿을 사용하여 *vsys*를 구성하는 경우 이 필드가 나타나지 않습니다.
이름	vsys를 식별하는 이름(최대 31자)을 입력합니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. *Panorama* 템플릿을 사용하여 *vsys* 구성을 푸시하는 경우 템플릿의 *vsys* 이름은 방화벽의 *vsys* 이름과 일치해야 합니다.
복호화된 콘텐츠 포워딩 허용	포트 미러링 또는 분석을 위해 WildFire 파일을 보낼 때 가상 시스템이 복호화된 콘텐츠를 외부 서비스로 포워딩하도록 하려면 이 옵션을 선택합니다. 복호화 포트 미러링도 참조하십시오.
일반 탭	이 vsys에 DNS 프록시 규칙을 적용하려면 **DNS** 프록시 개체를 선택합니다. (네트워크 > DNS 프록시). 특정 유형의 개체를 포함하려면 해당 유형(인터페이스, VLAN, 가상 와이어, 가상 라우터 또는 가시적 가상 시스템)을 선택한 다음 개체를 추가한 다음 드롭다운에서 개체를 선택합니다. 모든 유형의 개체를 하나 이상 추가할 수 있습니다. 개체를 제거하려면 개체를 선택한 다음 삭제합니다.
리소스 탭	이 vsys에 허용되는 다음 리소스 제한을 지정합니다. 각 필드에는 방화벽 모델에 따라 달라지는 유효한 값 범위가 표시됩니다. 기본 설정은 0이며, 이는 vsys에 대한 제한이 방화벽 모델에 대한 제한임을 의미합니다. 그러나 특정 설정에 대한 제한은 각 vsys에 대해 복사되지 않습니다. 예를 들어 방화벽에 4개의 가상 시스템이 있는 경우 각 가상 시스템은 방화벽당 허용되는 전체 복호화 규칙 수를 가질 수 없습니다.

가상 시스템 설정	설명

	모든 가상 시스템에 대한 전체 복호화 규칙 수가 방화벽 제한에 도달한 후에는 더 이상 추가할 수 없습니다.
	• 세션 제한 - 최대 세션 수입니다.
	  `show session meter` *CLI* 명령을 사용하는 경우 방화벽은 데이터플레인당 허용된 최대 세션 수, 가상 시스템에서 사용 중인 현재 세션 수 및 가상 시스템당 제한된 세션 수를 표시합니다. *PA-5200* 시리즈 및 *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 - 최대 보안 규칙 수입니다.
	• **NAT** 규칙 - 최대 NAT 규칙 수입니다.
	• 복호화 규칙 - 최대 수의 복호화 규칙입니다.
	• **QoS** 규칙 - QoS 규칙의 최대 수입니다.
	• 애플리케이션 재정의 규칙 - 애플리케이션 재정의 규칙의 최대 수입니다.
	• 정책 기반 포워딩 규칙 - PBF(정책 기반 포워딩) 규칙의 최대 수입니다.
	• 인증 규칙 - 최대 인증 규칙 수입니다.
	• **DoS** 방어 규칙 - DoS(서비스 거부) 규칙의 최대 수입니다.
	• 사이트 간 **VPN** 터널 - 사이트 간 VPN 터널의 최대 수입니다.
	• 동시 **GlobalProtect** 터널 - 최대 동시 원격 GlobalProtect 사용자 수입니다.
	• **Inter-Vsys User-ID** 데이터 공유 - User-ID 데이터 허브를 구성하려면 운용 관리자 또는 관리자 권한이 필요합니다.
	  • 이 **vsys**를 **User-ID** 데이터 허브로 만들기 - 방화벽의 다른 모든 가상 시스템이 공유 매핑에 액세스하도록 허용합니다. 이 옵션을 활성화한 후 공유할 매핑 유형을 선택합니다. IP 주소 대 사용자명 매핑**(IP** 사용자 매핑), 그룹 매핑(사용자 그룹 매핑) 또는 둘 다.
	  • 허브 변경 - User-ID 데이터 허브인 vsys를 변경하려면 새 vsys를 선택하여 해당 vsys를 User-ID 데이터 허브로 재할당합니다. vsys를 User-ID 데이터 허브로 사용을 중지하려면 없음을 선택합니다.

디바이스 > 공유 게이트웨이

공유 게이트웨이를 사용하면 여러 가상 시스템이 외부 통신을 위한 단일 인터페이스를 공유할 수 있습니다(일반적으로 인터넷 서비스 공급자와 같은 공통 업스트림 네트워크에 연결됨). 모든 가상 시스템은 단일 IP 주소를 사용하여 물리적 인터페이스를 통해 외부 세계와 통신합니다. 단일 가상 라우터는 공유 게이트웨이를 통해 모든 가상 시스템에 대한 트래픽을 라우팅하는 데 사용됩니다.

공유 게이트웨이는 레이어 3 인터페이스를 사용하며 하나 이상의 레이어 3 인터페이스를 공유 게이트웨이로 구성해야 합니다. 가상 시스템에서 시작하여 공유 게이트웨이를 통해 방화벽을 나가는 통신에는 두 가상 시스템 사이를 통과하는 통신과 유사한 정책이 필요합니다. 가상 시스템에서 보안 규칙을 정의하기 위해 '외부 vsys' 영역을 구성할 수 있습니다.

공유 게이트웨이 설정	설명
ID	게이트웨이의 식별자입니다(방화벽에서 사용하지 않음).
이름	공유 게이트웨이의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. 이름만 필요합니다.
DNS 프록시	(선택 사항) DNS 프록시가 구성된 경우 도메인 이름 쿼리에 사용할 DNS 서버를 선택합니다.
인터페이스	공유 게이트웨이가 사용할 인터페이스를 선택하십시오.

디바이스 > 인증서 관리

- 디바이스 > 인증서 관리 > 인증서
- 디바이스 > 인증서 관리 > 인증서 프로파일
- 디바이스 > 인증서 관리 > OCSP 응답자
- 디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일
- 디바이스 > 인증서 관리 > SCEP
- 디바이스 > 인증서 관리 > SSL 복호화 제외
- 디바이스 > 인증서 관리 > SSH 서비스 프로파일

디바이스 > 인증서 관리 > 인증서

디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서를 선택하여 네트워크를 통한 통신 보안에 사용되는 인증서를 관리(생성, 가져오기, 갱신, 삭제 및 취소)합니다. 네트워크에서 HA 피어 간의 연결을 보호하는 고가용성(HA) 키를 내보내고 가져올 수도 있습니다. **Device** > **Certificate Management** > **Certificates** > 신뢰할 수 있는 인증 기관을 선택하여 방화벽이 신뢰하는 CA(인증 기관)를 확인, 활성화 및 비활성화합니다.

방화벽 및 *Panorama*에서 인증서를 구현하는 방법에 대한 자세한 내용은 인증서 관리를 참조하십시오.

- 방화벽 및 Panorama 인증서 관리
- 기본 신뢰할 수 있는 인증 기관 관리
- 디바이스 > 인증서 관리 > 인증서 프로파일
- 디바이스 > 인증서 관리 > OCSP 응답자
- 디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일
- 디바이스 > 인증서 관리 > SCEP
- 디바이스 > 마스터 키 및 진단

방화벽 및 Panorama 인증서 관리

- 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서
- Panorama > 인증서 관리 > 인증서

Device > **Certificate Management** > **Certificates** > **Device Certificates** 또는 **Panorama** > **Certificate Management** > **Certificates** > **Device Certificates**를 선택하여 방화벽이나 Panorama가 웹 인터페이스, SSL 복호화 또는 LSVPN에 대한 액세스 보안과 같은 작업에 사용하는 인증서를 표시합니다.

다음은 인증서의 일부 용도입니다. 인증서를 생성한 후 사용을 정의합니다(신뢰할 수 있는 기본 인증 기관 관리 참조).

- 포워딩 신뢰 - 방화벽은 이 인증서를 사용하여 서버 인증서에 서명한 인증 기관(CA)이 방화벽의 신뢰할 수 있는 CA 목록에 있는 경우 SSL 포워딩 프록시 복호화 중에 방화벽이 클라이언트에 제공하는 서버 인증서 사본에 서명합니다.
- 포워딩 언트러스트 - 방화벽은 이 인증서를 사용하여 서버 인증서에 서명한 CA가 방화벽의 신뢰할 수 있는 CA 목록에 없을 때 SSL 포워딩 프록시 복호화 중에 방화벽이 클라이언트에 제공하는 서버 인증서 사본에 서명합니다.
- 신뢰할 수 있는 루트 **CA** - 방화벽은 SSL 포워딩 프록시 복호화, GlobalProtect, URL 관리 재정의 및 인증 포털에 대해 이 인증서를 신뢰할 수 있는 CA로 사용합니다. 방화벽에는 기존의 신뢰할 수 있는 CA 목록이 많이 있습니다. 신뢰할 수 있는 루트 CA 인증서는 조직이 신뢰하지만 사전 설치된 신뢰할 수 있는 목록의 일부가 아닌 추가 CA를 위한 것입니다.

- **SSL** 제외 - SSL/TLS 복호화에서 특정 서버를 제외하도록 복호화 예외를 구성한 경우 방화벽이 이 인증서를 사용합니다.
- 보안 **Syslog**용 인증서 - 방화벽은 이 인증서를 사용하여 로그를 syslog 메시지로 syslog 서버에 안전하게 전달합니다.

인증서를 생성하려면 생성을 클릭하고 다음 필드를 지정합니다.

인증서가 생성되면 페이지에 인증서 관리를 위해 지원되는 기타 작업이 표시됩니다.

인증서 생성 설정	설명
인증서 유형	인증서를 생성하는 엔터티를 선택합니다. 로컬 - 방화벽 또는 Panorama가 인증서를 생성합니다. **SCEP** - SCEP(Simple Certificate Enrollment Protocol) 서버가 인증서를 생성하여 방화벽이나 Panorama로 보냅니다.
인증서 이름	(필수) 인증서를 식별할 이름(방화벽의 경우 최대 63자, Panorama의 경우 최대 31자)을 입력합니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
SCEP 프로파일	(SCEP 인증서만 해당) **SCEP** 프로파일을 선택하여 방화벽 또는 Panorama가 SCEP 서버와 통신하는 방법을 정의하고 SCEP 인증서에 대한 설정을 정의합니다. 자세한 내용은 디바이스 > 인증서 관리 > SCEP를 참조하십시오. GlobalProtect 포털 역할을 하는 방화벽을 구성하여 요청 시 SCEP 인증서를 요청하고 인증서를 엔드포인트에 자동으로 배포 할 수 있습니다. 인증서 생성 대화 상자의 나머지 필드는 SCEP 인증서에 적용되지 않습니다. 인증서 이름 및 **SCEP** 프로파일을 지정한 후 생성을 클릭합니다.
일반 이름	(필수) 인증서에 표시할 IP 주소 또는 FQDN을 입력합니다.
공유	둘 이상의 가상 시스템(vsys)이 있는 방화벽에서 모든 vsys에서 인증서를 사용할 수 있도록 하려면 공유를 선택합니다.
서명자	인증서에 서명하기 위해 방화벽으로 불러온 인증 기관(CA) 인증서를 사용할 수 있습니다. 인증서는 자체 서명될 수도 있으며 이 경우 방화벽은 CA입니다. Panorama를 사용하는 경우 Panorama용 자체 서명 인증서를 생성할 수도 있습니다. CA 인증서를 가져오거나 방화벽에서 발급한 경우(자체 서명) 드롭다운에는 생성 중인 인증서에 서명하는 데 사용할 수 있는 CA가 포함됩니다.

인증서 생성 설정	설명
	CSR(인증서 서명 요청)을 생성하려면 **CSR(**외부 기관**)**을 선택합니다. 방화벽이 인증서와 키 쌍을 생성한 후 CSR을 내보내고 서명을 위해 CA로 보낼 수 있습니다.
인증 기관	방화벽에서 인증서를 발급하도록 하려면 이 옵션을 선택합니다. 이 인증서를 CA로 표시하면 이 인증서를 사용하여 방화벽의 다른 인증서에 서명할 수 있습니다.
개인 키 내보내기 차단	인증서를 생성할 때 운용 관리자를 포함한 모든 관리자가 개인 키를 내보내는 것을 차단하려면 이 옵션을 선택하십시오.
OCSP 응답자	드롭다운에서 OCSP 응답자 프로파일을 선택합니다(디바이스 > 인증서 관리 > OCSP 응답자 참조). 해당 호스트 이름이 인증서에 나타납니다.
알고리즘	인증서에 대한 키 생성 알고리즘을 선택합니다. **RSA** 또는 타원 곡선 **DSA**(ECDSA). ECDSA는 RSA 알고리즘보다 작은 키 크기를 사용하므로 SSL/TLS 연결 처리를 위한 성능 향상을 제공합니다. ECDSA는 또한 RSA와 같거나 더 큰 보안을 제공합니다. ECDSA는 이를 지원하는 클라이언트 브라우저 및 운영 체제에 권장되지만 레거시 브라우저 및 운영 체제와의 호환성을 위해 RSA를 선택해야 할 수도 있습니다. *PAN-OS 6.1* 또는 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 포워딩 프록시 또는 인바운드 검사 복호화에 사용되는 개인 ECDSA 키를 저장할 수 없습니다.
비트 수	인증서의 키 길이를 선택하십시오. 방화벽이 FIPS-CC 모드이고 키 생성 알고리즘이 **RSA**인 경우 생성된 RSA 키는 **2048** 또는 **3027**비트여야 합니다. 알고리즘이 타원 곡선 **DSA**인 경우 두 키 길이 옵션**(256** 및 **384)**이 모두 작동합니다.
다이제스트	인증서에 대한 다이제스트 알고리즘을 선택합니다. 사용 가능한 옵션은 키 생성 알고리즘에 따라 다릅니다. • **RSA**—**MD5**, **SHA1**, **SHA256**, **SHA384** 또는 **SHA512** • 타원 곡선 **DSA - SHA256** 또는 **SHA384**

인증서 생성 설정	설명
	방화벽이 FIPS-CC 모드이고 키 생성 알고리즘이 **RSA**인 경우 다이제스트 알고리즘으로 **SHA256**, **SHA384** 또는 **SHA512**를 선택해야 합니다. 알고리즘이 타원 곡선 **DSA**인 경우 다이제스트 알고리즘**(SHA256** 및 **SHA384)**이 모두 작동합니다. *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 하위 다이제스트 알고리즘*(*예*:* ***SHA384****)*을 사용해야 하거나 방화벽 서비스에 대한 *SSL/TLS* 서비스 프로파일을 구성할 때 최대 버전을 ***TLSv1.1***로 제한해야 합니다*(*디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일 참조*).*
만료(일)	인증서가 유효한 일 수(기본값은 365일)를 지정합니다. *GlobalProtect* 새틀라이트 구성에서 유효 기간을 지정하면 해당 값이 이 필드에 입력한 값을 무시합니다.
인증서 속성	인증서를 발급하는 엔터티를 식별하기 위해 추가 인증서 속성을 추가합니다. 다음 속성을 추가할 수 있습니다. 국가, 주, 지역, 조직, 부서 및 이메일. 또한 다음 주체 대체 이름 필드 중 하나를 지정할 수 있습니다. 호스트 이름(SubjectAltName:DNS), **IP**(SubjectAltName:IP) 및 대체 이메일(SubjectAltName:email). 국가를 인증서 속성으로 추가하려면 유형 열에서 국가를 선택한 다음 값 열을 클릭하여 *ISO 6366* 국가 코드를 확인합니다.

*HSM(*하드웨어 보안 모듈*)*을 구성한 경우 개인 키는 방화벽이 아닌 외부 *HSM* 저장소에 저장됩니다.

인증서 관리를 위해 지원되는 기타 작업

인증서를 생성하면 해당 세부 정보가 페이지에 표시되고 다음 작업을 수행할 수 있습니다.

인증서 관리를 위해 지원되는 기타 작업	설명
삭제	인증서를 선택한 다음 삭제합니다. 방화벽에 복호화 정책이 있는 경우 사용이 트러스트 인증서 포워딩 또는 언트러스트 인증서 포워딩으로 설정된 인증서는 삭제할 수 없습니다. 인증서 사용을 변경하려면 트러스트 기본 인증 기관 관리를 참조하십시오.
취소	해지할 인증서를 선택한 다음 해지를 클릭합니다. 인증서는 즉시 취소 상태로 설정됩니다. 커밋이 필요하지 않습니다.
갱신	인증서가 만료되거나 만료되려고 하는 경우 해당 인증서를 선택한 다음 갱신을 클릭합니다. 인증서의 유효 기간(일)을 설정하고 확인을 클릭합니다. 방화벽이 인증서를 발급한 CA인 경우 방화벽은 일련번호는 다르지만 속성은 이전 인증서와 동일한 새 인증서로 교체합니다. 외부 인증 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.
가져오기	인증서를 가져오고 다음과 같이 구성합니다. • 인증서를 식별하기 위해 인증서 이름을 입력합니다. • 인증서 파일을 찾습니다. **PKCS12** 인증서와 개인 키를 가져오면 단일 파일에 둘 다 포함됩니다. **PEM** 인증서를 가져오면 파일에 인증서만 포함됩니다. • 인증서의 파일 형식을 선택합니다. • HSM이 이 인증서에 대한 키를 저장하는 경우 개인 키가 하드웨어 보안 모듈에 상주함을 선택합니다. HSM에 대한 자세한 내용은 디바이스 > 설정 > HSM을 참조하십시오. • 필요에 따라 개인 키를 가져옵니다(PEM 형식만 해당). **PKCS12**를 인증서 파일 형식으로 선택한 경우 선택한 인증서 파일에 키가 포함됩니다. **PEM** 형식을 선택한 경우 암호화된 개인 키 파일(일반적으로 *.key로 명명)을 찾습니다. 두 형식 모두에 대해 암호 및 암호 확인을 입력합니다. 인증서를 가져오고 개인 키 가져오기를 선택할 때 개인 키 내보내기 차단을 선택하여 운용 관리자를 포함한 모든 관리자가 개인 키를 내보내지 못하도록 합니다.

인증서 관리를 위해 지원되는 기타 작업	설명
	FIPS-CC 모드에 있는 *Palo Alto Networks* 방화벽 또는 *Panorama* 서버로 인증서를 가져올 때 인증서를 *Base64* 인코딩 인증서*(PEM)*로 가져와야 하고 *AES*를 사용하여 개인 키를 암호화해야 합니다. 또한 암호문 기반 키 파생 방법으로 *SHA1*을 사용해야 합니다. PKCS12 인증서를 가져오려면 인증서를 PEM 형식으로 변환합니다(OpenSSL과 같은 도구 사용). 변환하는 동안 사용하는 암호 구문이 6자 이상인지 확인하십시오.
내보내기	내보낼 인증서를 선택한 다음 내보내기를 클릭한 다음 파일 형식을 선택합니다. • 암호화된 개인 키 및 인증서(PKCS12) - 내보낸 파일에는 인증서와 개인 키가 모두 포함됩니다. • Base64 인코딩된 인증서(PEM) - 개인 키도 내보내려면 개인 키 내보내기를 선택한 다음 암호 및 암호 확인을 입력합니다. • 바이너리 인코딩 인증서(DER) - 인증서만 내보낼 수 있고 키는 내보낼 수 없습니다. 개인 키 내보내기 및 암호 문구 필드는 무시합니다.
HA 키 가져오기 HA 키 내보내기	HA 키는 두 방화벽 피어에서 교환되어야 합니다. 즉, 방화벽 1의 키를 내보낸 다음 방화벽 2로 가져와야 하며 그 반대의 경우도 마찬가지입니다. 고가용성(HA)을 위한 키를 가져오려면 **HA** 키 가져오기 및 찾아보기를 클릭하여 가져올 키 파일을 지정합니다. HA용 키를 내보내려면 **HA** 키 내보내기를 클릭하고 파일을 저장할 위치를 지정합니다.
인증서 사용 정의	이름 열에서 인증서를 선택한 다음 인증서 사용 계획에 적합한 옵션을 선택합니다.
PDF/CSV	최소한의 읽기 전용 액세스 권한이 있는 관리 역할은 관리되는 인증서 구성 테이블을 **PDF/CSV**로 내보낼 수 있습니다. 필터를 적용하여 감사와 같은 항목에 대한 보다 구체적인 테이블 구성 출력을 생성할 수 있습니다. 웹 인터페이스에서 보이는 열만 내보내집니다. 구성 테이블 내보내기를 참조하십시오.

기본 신뢰할 수 있는 인증 기관 관리

- 디바이스 > 인증서 관리 > 인증서 > 기본 신뢰할 수 있는 인증 기관

이 페이지를 사용하여 방화벽이 신뢰하는 사전 포함된 인증 기관(CA)을 보거나 비활성화하거나 내보낼 수 있습니다. 사전 설치된 CA 목록에는 방화벽이 인터넷 연결을 보호하는 데 필요한 인증서 발급을 담당하는 가장 일반적이고 신뢰할 수 있는 인증서 공급자가 포함되어 있습니다. 각 신뢰할 수 있는 루트 CA에 대해 이름, 주체, 발급자, 만료 날짜 및 유효성 상태가 표시됩니다.

중간 CA는 방화벽과 신뢰할 수 있는 루트 CA 간의 신뢰 체인의 일부가 아니기 때문에 방화벽은 기본적으로 중간 CA를 신뢰하지 않습니다. 조직에 필요한 추가 신뢰할 수 있는 엔터프라이즈 CA와 함께 방화벽이 신뢰하도록 하려는 중간 CA를 수동으로 추가해야 합니다(**Device** > **Certificate Management** > **Certificates** > **Device Certificates**).

신뢰할 수 있는 인증 기관 설정	설명
활성화	CA를 비활성화한 경우 다시 활성화할 수 있습니다.
비활성화	CA를 선택한 다음 비활성화하십시오. 이 옵션을 사용하여 특정 CA만 신뢰하거나 다른 모든 CA를 비활성화하고 로컬 CA만 신뢰할 수 있습니다.
내보내기	CA 인증서를 선택한 다음 내보냅니다. 다른 시스템으로 가져오거나 인증서를 오프라인으로 볼 수 있습니다.

디바이스 > 인증서 관리 > 인증서 프로파일

- 디바이스 > 인증서 관리 > 인증서 프로파일
- **Panorama** > 인증서 관리 > 인증서 프로파일

인증서 프로파일은 클라이언트 인증서를 확인하는 데 사용할 CA(인증 기관) 인증서, 인증서 해지 상태를 확인하는 방법 및 해당 상태가 액세스를 제한하는 방법을 정의합니다. 인증 포털, GlobalProtect, 사이트 간 IPSec VPN, DDNS(동적 DNS), 방화벽 및 Panorama에 대한 웹 인터페이스 액세스에 대한 인증서 인증을 구성할 때 프로파일을 선택합니다. 이러한 각 서비스에 대해 별도의 인증서 프로파일을 구성할 수 있습니다.

인증서 프로파일 설정	설명
이름	(필수) 프로파일을 식별할 수 있는 이름을 입력합니다(방화벽의 경우 최대 63자, Panorama의 경우 최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
사용자명 필드	GlobalProtect가 포털 및 게이트웨이 인증용 인증서만 사용하는 경우 PAN-OS 소프트웨어는 사용자명 필드 드롭다운에서 선택한 인증서 필드를 사용자명으로 사용하고 이를 User-ID 서비스의 IP 주소와 일치시킵니다. • **Subject** - 일반 이름입니다. • **Subject Alt** - 이메일 또는 보안 주체 이름. • 없음 - 일반적으로 GlobalProtect 디바이스 또는 사전 로그인 인증용입니다.
도메인	PAN-OS 소프트웨어가 User-ID를 통해 사용자를 매핑할 수 있도록 NetBIOS 도메인을 입력합니다.
CA 인증서	(필수) 프로파일에 할당할 **CA** 인증서를 추가합니다. 선택적으로 방화벽이 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 해지 상태를 확인하는 경우 다음 필드를 구성하여 기본 동작을 재정의합니다. 대부분의 배포에서는 이러한 필드가 적용되지 않습니다.

인증서 프로파일 설정	설명
	• 기본적으로 방화벽은 인증서의 AIA(Authority Information Access) 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. 또한 템플릿 이름을 입력하여 인증서 서명에 사용된 템플릿을 식별합니다.
CRL 사용	CRL(인증서 해지 목록)을 사용하여 인증서 해지 상태를 확인하려면 이 옵션을 선택합니다.
OCSP 사용	OCSP를 사용하여 인증서 해지 상태를 확인하려면 이 옵션을 선택합니다.  *OCSP*와 *CRL*을 모두 선택하면 방화벽은 먼저 *OCSP*를 시도하고 *OCSP* 응답자를 사용할 수 없는 경우에만 *CRL* 방법으로 대체합니다.
CRL 수신 타임아웃	방화벽이 CRL 서비스의 응답을 기다리는 것을 중지하는 인터벌(1~60초)을 지정합니다.
OCSP 수신 타임아웃	방화벽이 OCSP 응답자의 응답 대기를 중지하는 인터벌(1~60초)을 지정합니다.
인증서 상태 타임아웃	방화벽이 인증서 상태 서비스의 응답 대기를 중지하고 사용자가 정의한 세션 차단 논리를 적용하는 인터벌(1~60초)을 지정합니다.
인증서 상태를 알 수 없는 경우 세션 차단	OCSP 또는 CRL 서비스가 알 수 없는 인증서 해지 상태를 반환할 때 방화벽이 세션을 차단하도록 하려면 이 옵션을 선택합니다. 그렇지 않으면 방화벽이 세션을 진행합니다.
제한 시간 내에 인증서 상태를 검색할 수 없는 경우 세션 차단	방화벽이 OCSP 또는 CRL 요청 타임아웃을 등록한 후 세션을 차단하도록 하려면 이 옵션을 선택합니다. 그렇지 않으면 방화벽이 세션을 진행합니다.
인증 디바이스에 인증서가 발급되지 않은 경우 세션 차단	(GlobalProtect만 해당) 클라이언트 인증서 제목의 일련번호 속성이 GlobalProtect 앱이 엔드포인트에 대해 보고하는 호스트 ID와 일치하지 않을 때 방화벽이 세션을 차단하도록 하려면 이 옵션을 선

인증서 프로파일 설정	설명
	택합니다. 그렇지 않으면 방화벽이 세션을 허용합니다. 이 옵션은 GlobalProtect 인증서 인증에만 적용됩니다.

디바이스 > 인증서 관리 > OCSP 응답자

디바이스 > 인증서 관리 > **OCSP** 응답자를 선택하여 OCSP(온라인 인증서 상태 프로토콜) 응답자(서버)를 정의하여 인증서 해지 상태를 확인합니다.

OCSP 응답자를 추가하는 것 외에도 OCSP를 활성화하려면 다음 작업이 필요합니다.

- 방화벽과 OCSP 서버 간의 통신 활성화: **Device** > **Setup** > 관리를 선택한 다음 관리 인터페이스 설정에서 **HTTP OCSP**를 선택한 다음 확인을 클릭합니다.
- 방화벽이 아웃바운드 SSL/TLS 트래픽을 복호화하는 경우 선택적으로 대상 서버 인증서의 해지 상태를 확인하도록 구성합니다. 디바이스 > 설정 > 세션을 선택합니다. 복호화 인증서 해지 설정을 클릭하고 OCSP 설정에서 활성화를 선택한 다음 수신 타임아웃(방화벽이 OCSP 응답을 기다리지 않는 인터벌)을 클릭하고 확인을 클릭합니다.
- 선택적으로 방화벽을 OCSP 응답자로 구성하려면 OCSP 서비스에 사용되는 인터페이스에 인터페이스 관리 프로파일을 추가합니다. 먼저 네트워크 > 네트워크 프로파일 > 인터페이스 관리를 선택한 다음 추가를 클릭하고 **HTTP OCSP**를 선택한 다음 확인을 클릭합니다. 둘째, **Network** > **Interfaces**를 선택한 다음 방화벽이 OCSP 서비스에 사용할 인터페이스 이름을 클릭하고 **Advanced** > 기타 정보를 선택한 다음 구성한 인터페이스 관리 프로파일을 선택한 다음 확인 및 커밋을 클릭합니다.

인증서가 해지된 경우 알림을 받고 포털 및 게이트웨이에 대한 보안 연결을 설정하기 위해 적절한 조치를 취할 수 있도록 *OCSP* 응답자를 활성화하십시오.

OCSP 응답자 설정	설명
이름	응답자를 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분합니다. 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 사용해야 합니다.
위치	응답자를 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 값은 Shared로 사전 정의됩니다. 응답자를 저장한 후에는 위치를 변경할 수 없습니다.
호스트 이름	OCSP 응답자의 호스트 이름(권장) 또는 IP 주소를 입력합니다. 이 값에서 PAN-OS는 URL을 자동으로 파생하여 확인 중인 인증서에 추가합니다. 방화벽을 OCSP 응답자로 구성하는 경우 호스트 이름은 방화벽이 OCSP 서비스에 사용하는 인터페이스의 IP 주소로 확인되어야 합니다.

디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일

- 디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일
- Panorama > 인증서 관리 > SSL/TLS 서비스 프로파일

SSL/TLS 서비스 프로파일은 SSL/TLS(웹 인터페이스에 대한 관리 액세스 등)를 사용하는 방화벽 또는 Panorama 서비스에 대한 서버 인증서 및 프로토콜 버전 또는 버전 범위를 지정합니다. 프로토콜 버전을 정의하면 프로파일을 사용하여 서비스를 요청하는 클라이언트 시스템과의 통신 보안에 사용할 수 있는 암호 제품군을 제한할 수 있습니다.

방화벽 또는 *Panorama* 서비스를 요청하는 클라이언트 시스템에서 *CTL(*인증서 신뢰 목록*)*에는 *SSL/TLS* 서비스 프로파일에 지정된 인증서를 발급한 *CA(*인증 기관*)* 인증서가 포함되어야 합니다. 그렇지 않으면 사용자가 서비스를 요청할 때 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.

프로파일을 추가하려면 추가를 클릭하고 다음 표의 필드를 완성하십시오.

SSL/TLS 서비스 프로파일 설정	설명
이름	프로파일을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분합니다. 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 사용해야 합니다.
공유	방화벽에 둘 이상의 가상 시스템(vsys)이 있는 경우 이 옵션을 선택하면 모든 가상 시스템에서 프로파일을 사용할 수 있습니다. 기본적으로 이 옵션은 선택 취소되어 있으며 디바이스 탭의 위치 드롭다운에서 선택한 vsys에 대해서만 프로파일을 사용할 수 있습니다.
자격증	프로파일과 연결할 서버 인증서를 선택, 가져오기 또는 생성합니다(방화벽 및 Panorama 인증서 관리 참조). *SSL/TLS* 서비스에 인증 기관*(CA)* 인증서를 사용하지 마십시오. 서명된 인증서만 사용하십시오.
최소 버전	서비스에서 사용할 수 있는 TLS의 가장 오래된(최소 버전) 및 최신(최대 버전) 버전을 선택합니다. **TLSv1.0**, **TLSv1.1**, **TLSv1.2**, **TLSv1.3** 또는 **Max**(사용 가능한 최신 버전).
최대 버전	

SSL/TLS 서비스 프로파일 설정	설명
	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 낮은 다이제스트 알고리즘*(*예*: SHA384)*을 사용하거나 서비스에 대해 최대 버전을 ***TLSv1.1***로 제한해야 합니다. 가장 강력한 버전의 프로토콜을 사용하여 네트워크에 가장 강력한 보안을 제공하십시오. 가능한 경우 최소 버전을 ***TLSv1.2***로 설정하고 최대 버전을 최대로 설정합니다.

디바이스 > 인증서 관리 > SCEP

SCEP(단순 인증서 등록 프로토콜)는 엔드포인트, 게이트웨이 및 새틀라이트 디바이스에 고유한 인증서를 발급하기 위한 메커니즘을 제공합니다. 디바이스 > 인증서 관리 > **SCEP**를 선택하여 SCEP 구성을 만듭니다.

SCEP 프로파일을 만드는 방법에 대한 자세한 내용은 SCEP를 사용하여 인증서 배포를 참조하십시오

.

새 SCEP 구성을 시작하려면 추가를 클릭하고 다음 필드를 완료하십시오.

SCEP 설정	설명
이름	SCEP_*Example*과 같이 이 SCEP 구성을 식별하는 설명적인 이름을 지정합니다. 이 이름은 SCEP 프로파일을 구성 프로파일에 있을 수 있는 다른 인스턴스와 구별합니다.
위치	시스템에 여러 가상 시스템이 있는 경우 프로파일 위치를 선택합니다. 위치는 SCEP 구성을 사용할 수 있는 위치를 식별합니다.
일회용 비밀번호(시도)	
SCEP 챌린지	(선택 사항) SCEP 기반 인증서 생성을 보다 안전하게 만들기 위해 각 인증서 요청에 대해 PKI(공개 키 인프라)와 포털 간에 SCEP 챌린지 응답 메커니즘(OTP(일회성 암호))을 구성할 수 있습니다. 이 메커니즘을 구성한 후에는 해당 작업이 보이지 않으며 사용자의 추가 입력이 필요하지 않습니다. 선택한 챌린지 메커니즘에 따라 OTP 소스가 결정됩니다. 고정을 선택한 경우 SCEP 서버에서 PKI에 대한 등록 챌린지 비밀번호를 복사하고 고정으로 구성될 때 표시되는 포털의 비밀번호 대화 상자에 문자열을 입력합니다. 포털은 인증서를 요청할 때마다 이 비밀번호를 사용하여 PKI로 인증합니다. 동적을 선택하면 선택한 사용자명과 암호(PKI 관리자의 자격 증명일 수 있음) 및 포털 클라이언트가 이러한 자격 증명을 제출하는 SCEP 서버 **URL**을 입력합니다. 이 사용자명과 암호는 동일하게 유지되지만 SCEP 서버는 각 인증서 요청 시 포털에 대한 OTP 암호를 철저하게 생성합니다. (각 인증서 요청 시 "등록 챌린지 비밀번호는" 필드에서 화면 새로 고침 후 이 OTP 변경 사항을 확인할 수 있습니다.) PKI는 각 새 암호를 포털에 철저하게 전달한 다음 인증서 요청에 암호를 사용합니다.

SCEP 설정	설명
	미국 규정 준수 *FIPS(*연방 정보 처리 표준*)*에서 동작을 선택한 다음 *HTTPS*를 사용하는 서버 ***URL***을 지정하고 ***SCEP*** 서버 ***SSL*** 인증을 활성화합니다. *(FIPS-CC* 동작은 방화벽 로그인 페이지와 방화벽 상태 표시줄에 표시됩니다.*)*
구성	
서버 URL	포털이 SCEP 서버에서 클라이언트 인증서를 요청하고 수신하는 URL을 입력하십시오. 예시: `http://<hostname or IP>/certsrv/mscep/.`
CA-IDENT 이름	SCEP 서버를 식별하는 문자열을 입력하십시오. 최대 길이는 255자입니다.
주제	디바이스 및 선택적으로 사용자에 대한 식별 정보를 포함하도록 주제를 구성하고 SCEP 서버에 대한 인증서 서명 요청(CSR)에서 이 정보를 제공합니다. 엔드포인트에 대한 클라이언트 인증서를 요청하는 데 사용되는 경우 엔드포인트는 호스트 ID 값이 포함된 디바이스에 대한 식별 정보를 보냅니다. 호스트 ID 값은 디바이스 유형, 즉 GUID(Windows) 인터페이스의 MAC 주소(Mac), Android ID(Android 디바이스), UDID(iOS 디바이스) 또는 GlobalProtect가 할당하는 고유 이름(Chrome)에 따라 다릅니다. 새틀라이트 디바이스에 대한 인증서를 요청하는 데 사용되는 경우 호스트 ID 값은 디바이스 일련번호입니다. CSR에 추가 정보를 지정하려면 주체 이름을 입력합니다. 제목은 <*attribute*>=<*value*> 형식의 고유 이름이어야 하며 CN(일반 이름) 키를 포함해야 합니다. 예: `O=acme,CN=acmescep` CN을 지정하는 방법에는 두 가지가 있습니다. • (권장) 토큰 기반 **CN** - 지원되는 토큰 **$USERNAME**, **$EMAILADDRESS** 또는 **$HOSTID** 중 하나를 입력합니다. 포털이 특정 사용자에 대한 인증서를 요청하도록 하려면 사용자명 또는 이메일 주소 변수를 사용하십시오. 디바이스에 대한 인증서만 요청하려면 hostid 변수를 지정하십시오. GlobalProtect 포털이 SCEP 설정을 에이전트에 푸시하면 주체 이름의 CN 부분이 인증서 소유자의 실제 값(사용자명, 호스트 ID 또는 이메일 주소)으로 바뀝니다. 예:

SCEP 설정	설명

	`O=acme,CN=$HOSTID`
	• 고정 **CN** - 지정한 CN은 SCEP 서버에서 발급한 모든 인증서의 제목으로 사용됩니다. 예:
	`O=acme,CN=acmescep`

제목 대체 이름 유형	없음 이외의 유형을 선택하면 적절한 값을 입력할 수 있는 대화 상자가 표시됩니다. • **RFC 822** 이름 - 인증서 제목 또는 제목 대체 이름 확장에 이메일 이름을 입력합니다. • **DNS** 이름 - 인증서를 평가하는 데 사용되는 DNS 이름을 입력합니다. • **URI(Uniform Resource Identifier)** - 클라이언트가 인증서를 얻는 URI 리소스의 이름을 입력합니다.
암호화 설정	• 비트 수 - 인증서에 대한 키의 비트 수를 선택합니다. 방화벽이 FIPS-CC 모드인 경우 생성된 키는 최소 2,048비트여야 합니다. (FIPS-CC 동작은 방화벽 로그인 페이지와 방화벽 상태 표시줄에 표시됩니다.) • 다이제스트 - 인증서에 대한 다이제스트 알고리즘을 선택합니다. **SHA1**, **SHA256**, **SHA384** 또는 **SHA512**. 방화벽이 FIPS-CC 모드인 경우 다이제스트 알고리즘으로 **SHA256**, **SHA384** 또는 **SHA512**를 선택해야 합니다.
디지털 서명으로 사용	인증서의 개인 키를 사용하여 디지털 서명의 유효성을 검사하도록 엔드포인트를 구성하려면 이 옵션을 선택합니다.
키 암호화에 사용	SCEP 서버에서 발급한 인증서로 설정된 HTTPS 연결을 통해 교환되는 데이터를 암호화하기 위해 인증서의 개인 키를 사용하도록 클라이언트 엔드포인트를 구성하려면 이 옵션을 선택합니다.
CA 인증서 지문	(선택 사항) 포털이 올바른 SCEP 서버에 연결되도록 하려면 **CA** 인증서 지문을 입력합니다. **Thumbprint** 필드의 SCEP 서버 인터페이스에서 이 지문을 가져옵니다. SCEP 서버의 관리 사용자 인터페이스(예: http://<hostname or IP>/CertSrv/mcep_admin/)에 로그인합니다. 지문을 복사하여 **CA** 인증서 지문에 입력합니다.

SCEP 설정	설명
SCEP 서버 SSL 인증	SSL을 활성화하려면 SCEP 서버에 대한 루트 **CA** 인증서를 선택합니다. 선택적으로 클라이언트 인증서를 선택하여 SCEP 서버와 GlobalProtect 포털 간에 상호 SSL 인증을 활성화할 수 있습니다.

디바이스 > 인증서 관리 > SSL 복호화 제외

SSL 복호화 제외를 보고 관리합니다. 복호화 제외에는 사전 정의된 제외와 사용자 지정 제외의 두 가지 유형이 있습니다.

- 사전 정의된 복호화 제외를 사용하면 방화벽이 암호를 복호화할 때 중단될 수 있는 애플리케이션 및 서비스가 암호화된 상태로 유지됩니다. Palo Alto Networks는 사전 정의된 복호화 제외를 정의하고 애플리케이션 및 위협 콘텐츠 업데이트의 일부로 사전 정의된 제외 목록에 업데이트 및 추가를 정기적으로 제공합니다. 사전 정의된 제외는 기본적으로 활성화되어 있지만 필요에 따라 제외를 비활성화하도록 선택할 수 있습니다.
- 사용자 지정 복호화 제외를 만들어 복호화에서 서버 트래픽을 제외할 수 있습니다. 대상 서버에서 발생하거나 대상 서버로 향하는 모든 트래픽은 암호화된 상태로 유지됩니다.

애플리케이션, 소스, 대상, *URL* 카테고리 및 서비스를 기반으로 트래픽을 복호화에서 제외할 수도 있습니다.

이 페이지의 설정을 사용하여 복호화 제외를 수정 또는 추가하고 복호화 제외를 관리합니다.

SSL 복호화 제외 설정	설명
복호화 제외 수정 또는 추가	
호스트 이름	사용자 정의 복호화 제외를 정의하려면 호스트 이름을 입력하십시오. 방화벽은 호스트 이름을 클라이언트가 요청한 SNI 또는 서버 인증서에 제공된 CN과 비교합니다. 방화벽은 정의된 도메인을 포함하는 CN을 서버가 복호화에서 제공하는 세션을 제외합니다. 별표(*)를 와일드카드로 사용하여 도메인과 연결된 여러 호스트 이름에 대한 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.

SSL 복호화 제외 설정	설명
	• 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.com은 모두 google.com과 일치합니다. 그러나 하나의 레이블(dev)이 와일드카드가 아니기 때문에 *.dev.*.google.com은 google.com과 일치하지 않습니다. 호스트 이름은 각 항목에 대해 고유해야 합니다. 사전 정의된 항목이 기존 사용자 정의 항목과 일치하는 방화벽에 전달되는 경우 사용자 정의 항목이 우선합니다. 사전 정의된 복호화 제외에 대한 호스트 이름을 편집할 수 없습니다.
공유	다중 가상 시스템 방화벽의 모든 가상 시스템에서 복호화 제외를 공유하려면 공유를 선택합니다. 사전 정의된 복호화 제외는 기본적으로 공유되지만 특정 가상 시스템에 대해 사전 정의된 항목과 사용자 정의 항목을 모두 활성화 및 비활성화할 수 있습니다.
설명	(선택 사항) 복호화할 때 애플리케이션이 중단되는 이유를 포함하여 복호화에서 제외할 애플리케이션을 설명합니다.
제외	복호화에서 애플리케이션을 제외합니다. 이전에 복호화에서 제외된 애플리케이션의 복호화를 시작하려면 이 옵션을 비활성화합니다.
복호화 제외 관리	
활성화	복호화에서 제외하려면 하나 이상의 항목을 활성화하십시오.
비활성화	하나 이상의 사전 정의된 복호화 제외를 비활성화합니다. 복호화 제외는 복호화 시 중단되는 애플리케이션을 식별하므로 이러한 항목 중 하나를 비활성화하면 애플리케이션이 지원되지 않습니다. 방화벽이 애플리케이션의 복호화를 시도하고 애플리케이션이 중단됩니다. 특정 암호화된

SSL 복호화 제외 설정	설명
	애플리케이션이 네트워크에 들어가지 않도록 하려면 이 옵션을 사용할 수 있습니다.
사용되지 않는 항목 표시	Palo Alto Networks가 더 이상 복호화 제외로 정의하지 않는 사전 정의된 항목을 보려면 사용되지 않는 항목을 표시합니다. 사용되지 않는 항목에 대한 추가 정보: 사전 정의된 복호화 제외에 대한 업데이트(사전 정의된 항목 제거 포함)는 애플리케이션 및 위협 콘텐츠 업데이트의 일부로 방화벽에 전달됩니다. 복호화에서 제외가 활성화된 사전 정의된 항목은 방화벽이 해당 항목을 더 이상 포함하지 않는 콘텐츠 업데이트를 수신할 때 SSL 복호화 제외 목록에서 자동으로 제거됩니다. 그러나 복호화에서 제외가 비활성화된 사전 정의된 항목은 방화벽이 해당 항목을 더 이상 포함하지 않는 콘텐츠 업데이트를 받은 후에도 SSL 복호화 목록에 남아 있습니다. 더 이상 사용되지 않는 항목을 표시하면 현재 시행되고 있지 않은 비활성화된 사전 정의 항목이 표시됩니다. 필요에 따라 이러한 항목을 수동으로 제거할 수 있습니다.
로컬 제외 캐시 표시	로컬 제외 캐시 표시는 고정된 인증서, 클라이언트 인증 또는 지원되지 않는 암호와 같이 복호화를 방해하는 기술적인 상황으로 인해 방화벽이 복호화에서 자동으로 제외한 사이트를 표시합니다. 로컬 SSL 복호화 캐시는 Palo Alto Networks가 식별한 복호화를 방지하는 사이트가 포함되어 있고 영구 복호화 제외를 추가할 수 있는 SSL 복호화 제외 목록(**Device** > **Certificate Management** > **SSL** 복호화 제외)과 다릅니다. 방화벽은 트래픽을 제어하는 복호화 정책 규칙과 연결된 복호화 프로파일의 설정에 따라 로컬 SSL 복호화 캐시를 로컬에서 검색된 복호화 예외로 채웁니다. 제외된 사이트는 로컬 캐시에 12시간 동안 남아 있다가 만료됩니다. 각 제외 항목에는 애플리케이션, 서버, 방화벽이 사이트를 복호화에서 자동으로 제외한 이유, 트래픽에 적용된 복호화 프로파일 및 Vsys에 대한 정보가 포함됩니다.

디바이스 > 인증서 관리 > SSH 서비스 프로파일

SSH 서비스 프로파일을 사용하면 데이터 무결성을 암호화하고 보호하는 암호, 키 교환 및 메시지 인증 코드 알고리즘을 제한할 수 있습니다. 특히 이러한 프로파일은 명령줄 인터페이스(CLI)와 네트워크의 관리 연결 및 고가용성(HA) 어플라이언스 간의 SSH 세션 동안 데이터 보호를 강화합니다. 새 SSH 호스트 키를 생성하고 SSH 키 재입력을 시작하는 임계값(데이터 볼륨, 시간 인터벌 및 패킷 수)을 지정할 수도 있습니다.

SSH 서비스 프로파일을 구성하려면 HA 또는 관리 - 서버 프로파일 추가를 클릭하고 다음 표의 필드를 적절하게 완성한 다음 확인을 클릭하고 변경 사항을 커밋합니다.

프로파일 적용 프로세스는 프로파일 유형에 따라 다릅니다.

- HA 프로파일을 적용하려면 디바이스 > 고가용성 > 일반을 선택합니다. SSH HA 프로파일 설정에서 기존 프로파일을 선택합니다. 확인을 클릭하고 변경 사항을 커밋합니다.
- 관리 - 서버 프로파일을 적용하려면 디바이스 > 설정 > 관리을(를) 선택합니다. SSH 관리 프로파일 설정에서 기존 프로파일을 선택합니다. 확인을 클릭하고 변경 사항을 커밋합니다.

프로파일을 적용한 후 *CLI*에서 *SSH* 서비스를 다시 시작하여 프로파일을 활성화해야 합니다.

SSH 서비스 프로파일 설정	설명
이름	프로파일 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
암호	서버가 SSH 세션 암호화를 지원할 암호 알고리즘을 선택하십시오.
KEX	SSH 세션 동안 서버가 지원할 키 교환 알고리즘을 선택하십시오.
MAC	SSH 세션 동안 서버가 지원할 메시지 인증 코드 알고리즘을 선택하십시오.
호스트 키	지정된 호스트 키 알고리즘 및 키 길이의 새 키 쌍을 생성하려면 호스트 키 유형 및 키 길이를 선택하십시오. 호스트 키 유형을 선택한 후 키 길이를 입력할 수 있습니다. 기본 키 유형 및 길이는 *RSA 2048*입니다.

SSH 서비스 프로파일 설정	설명
데이터	SSH 키를 다시 입력하기 전에 전송되는 데이터의 최대 볼륨(MB)을 설정합니다(범위는 10~4000, 기본값은 선택한 암호 값).
인터벌	SSH 키 다시 입력 전 최대 시간 인터벌(초)을 설정합니다(범위는 10~3600, 기본값은 시간 기반 키 다시 입력 없음).
패킷	SSH 키를 다시 입력하기 전에 최대 패킷 수(2^n)를 설정합니다. 이 매개변수를 구성하지 않으면 세션은 2^{28} 패킷 후에 키를 다시 지정합니다. 더 자주 키를 다시 입력하려면 *12*에서 *27* 사이의 값을 지정하십시오.

디바이스 > 응답 페이지

사용자 정의 응답 페이지는 사용자가 URL에 액세스하려고 할 때 표시되는 웹 페이지입니다. 요청한 웹 페이지나 파일 대신 다운로드되어 표시되는 사용자 정의 HTML 메시지를 제공할 수 있습니다.

각 가상 시스템에는 고유한 사용자 정의 응답 페이지가 있을 수 있습니다. 다음 표에서는 고객 메시지를 지원하는 사용자 지정 응답 페이지 유형을 설명합니다.

사용자 정의 응답 페이지 유형	설명
안티바이러스 차단 페이지	바이러스 감염으로 인해 접근이 차단되었습니다.
애플리케이션 차단 페이지	애플리케이션이 보안 정책 규칙에 의해 차단되어 액세스가 차단되었습니다.
인증 포털 컴포트 페이지	방화벽은 사용자가 인증 정책 규칙이 적용되는 서비스에 액세스하기 위해 로그인 자격 증명을 입력할 수 있도록 이 페이지를 표시합니다(정책 > 인증 참조). 이 인증 질문에 응답하는 방법을 사용자에게 알려주는 메시지를 입력합니다. 방화벽은 인증 규칙에 할당된 인증 적용 개체에 지정된 인증 프로파일을 기반으로 사용자를 인증합니다(개체 > 인증 참조). 연결된 인증 시행 개체에 메시지를 입력하여 각 인증 규칙에 대한 고유한 인증 지침을 표시할 수 있습니다. 개체에 정의된 메시지는 인증 포털 편의 페이지에 정의된 메시지를 재정의합니다.
데이터 필터링 블록 페이지	민감한 정보가 감지되어 콘텐츠가 데이터 필터링 프로파일과 일치하고 차단되었습니다.
파일 차단 계속 페이지	사용자가 다운로드를 계속해야 하는지 확인하는 페이지입니다. 이 옵션은 보안 프로파일에서 계속 기능이 활성화된 경우에만 사용할 수 있습니다. 개체 > 보안 프로파일 > 파일 차단을 선택합니다.
파일 차단 차단 페이지	파일에 대한 액세스가 차단되어 액세스가 차단되었습니다.
GlobalProtect 앱 도움말 페이지	GlobalProtect 사용자를 위한 사용자 정의 도움말 페이지(GlobalProtect 상태 패널의 설정 메뉴에서 액세스 가능).
GlobalProtect 포털 로그인 페이지	GlobalProtect 포털 웹 페이지에 인증을 시도하는 사용자를 위한 로그인 페이지입니다.

사용자 정의 응답 페이지 유형	설명
GlobalProtect 포털 홈 페이지	GlobalProtect 포털 웹 페이지에 성공적으로 인증한 사용자를 위한 홈 페이지입니다.
GlobalProtect 앱 시작 페이지	GlobalProtect에 성공적으로 연결한 사용자를 위한 시작 페이지입니다.
MFA 로그인 페이지	방화벽은 사용자가 인증 정책 규칙이 적용되는 서비스에 액세스할 때 MFA(다단계 인증) 문제에 응답할 수 있도록 이 페이지를 표시합니다(정책 > 인증 참조). 사용자에게 MFA 챌린지에 응답하는 방법을 알려주는 메시지를 입력합니다.
SAML 인증 내부 오류 페이지	SAML 인증이 실패했음을 사용자에게 알리는 페이지입니다. 이 페이지에는 사용자가 인증을 다시 시도할 수 있는 링크가 포함되어 있습니다.
SSL 인증서 오류 알림 페이지	SSL 인증서가 취소되었음을 알립니다.
SSL 복호화 옵트아웃 페이지	방화벽이 검사를 위해 SSL 세션의 암호를 복호화할 것임을 나타내는 사용자 경고 페이지입니다.
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 차단을 우회할 수 있도록 하는 초기 차단 정책이 있는 페이지입니다. 예를 들어 페이지가 부적절하게 차단되었다고 생각하는 사용자는 계속을 클릭하여 해당 페이지로 이동할 수 있습니다. 재정의 페이지에서 사용자가 이 URL을 차단하는 정책을 재정의하려면 암호가 필요합니다. 재정의 암호 설정에 대한 지침은 URL 관리 재정의 섹션을 참조하십시오.
URL 필터링 Safe Search 시행 차단 페이지	**Safe Search Enforcement** 옵션이 활성화된 URL 필터링 프로파일이 있는 보안 정책 규칙에 의해 액세스가 차단되었습니다. Bing, Google, Yahoo, Yandex 또는 YouTube를 사용하여 검색을 수행하고 Safe Search에 대한 브라우저 또는 검색 엔진 계정 설정이 strict로 설정되지 않은 경우 사용자에게 이 페이지가 표시됩니다. 차단 페이지는 사용자에게 Safe Search 설정을 엄격하게 설정하도록 지시합니다.
안티 피싱 차단 페이지	자격 증명 제출이 차단된 웹 페이지에서 유효한 회사 자격 증명(사용자명 또는 암호)을 입력하려고 할 때 사용자에게 표시됩니다. 사용자

사용자 정의 응답 페이지 유형	설명
	는 계속해서 사이트에 액세스할 수 있지만 연결된 웹 양식에 유효한 회사 자격 증명을 제출할 수는 없습니다. 개체 > 보안 프로파일 > URL 필터링을 선택하여 자격 증명 감지를 활성화하고 URL 카테고리를 기반으로 웹 페이지에 대한 자격 증명 제출을 제어합니다.
안티 피싱 계속 페이지	이 페이지는 회사 자격 증명(사용자명 및 암호)을 웹사이트에 제출하지 않도록 사용자에게 경고합니다. 사용자에게 자격 증명 제출에 대해 경고하면 기업 자격 증명을 재사용하지 못하도록 하고 피싱 시도 가능성에 대해 교육하는 데 도움이 될 수 있습니다. 사용자 자격 증명 제출 권한이 계속되도록 설정된 사이트에 자격 증명을 제출하려고 할 때 사용자에게 이 페이지가 표시됩니다(개체 > 보안 프로파일 > URL 필터링 참조). 사이트에 자격 증명을 입력하려면 계속을 선택해야 합니다.

응답 페이지에 대해 다음 기능을 수행할 수 있습니다.

- 사용자 정의 HTML 응답 페이지를 가져오려면 변경하려는 페이지 유형의 링크를 클릭한 다음 가져오기/내보내기를 클릭하십시오. 찾아보기 페이지를 찾습니다. 가져오기가 성공했는지의 여부를 나타내는 메시지가 표시됩니다. 가져오기가 성공하려면 파일이 HTML 형식이어야 합니다.
- 사용자 정의 HTML 응답 페이지를 내보내려면 페이지 유형에 대해 내보내기를 클릭하십시오. 파일을 열지 디스크에 저장할지 선택한 다음 해당하는 경우 항상 동일한 옵션 사용을 선택합니다.
- 애플리케이션 차단 페이지 또는 **SSL** 복호화 옵트아웃 페이지를 활성화하거나 비활성화하려면 페이지 유형에 대해 활성화를 클릭합니다. 필요에 따라 활성화를 선택하거나 선택 취소합니다.
- 이전에 업로드한 사용자 지정 페이지 대신 기본 응답 페이지를 사용하려면 사용자 지정 차단 페이지를 삭제하고 커밋합니다. 이렇게 하면 기본 차단 페이지가 새 활성 페이지로 설정됩니다.

디바이스 > 로그 설정

디바이스 > 로그 설정을 선택하여 알람을 구성하거나 로그를 지우거나 Panorama, 로깅 서비스 및 기타 외부 서비스에 대한 로그 포워딩을 활성화합니다.

- 로그 포워딩 대상 선택
- 알람 설정 정의
- 로그 지우기

로그 포워딩 대상 선택

디바이스 > 로그 설정

로그 설정 페이지에서 다음으로 로그 포워딩을 구성할 수 있습니다.

- **Panorama, SNMP** 트랩 수신기**,** 이메일 서버**, Syslog** 서버 및 **HTTP** 서버 - 로그 항목의 소스 또는 대상 IP 주소에서 태그를 추가하거나 제거할 수도 있습니다. 시스템 로그 및 구성 로그를 제외한 모든 로그 유형은 태깅을 지원합니다.
- 로깅 서비스 - 로깅 서비스 구독이 있고 로깅 서비스를 활성화한 경우(디바이스 > 설정 > 관리) Panorama/로깅 서비스로의 로그 포워딩을 구성할 때 방화벽이 로깅 서비스로 로그를 보냅니다. Panorama는 로깅 서비스에 쿼리하여 로그에 액세스하고, 로그를 표시하고, 보고서를 생성합니다.
- **Azure Security Center** - Azure Security Center와의 통합은 Azure의 VM 시리즈 방화벽에만 사용할 수 있습니다.
  - Azure Security Center에서 VM 시리즈 방화벽을 시작한 경우 로그 포워딩 프로파일이 포함된 보안 정책 규칙이 자동으로 활성화됩니다.
  - Azure Marketplace에서 또는 사용자 지정 Azure 템플릿을 사용하여 VM 시리즈 방화벽을 시작한 경우 시스템 로그, 사용자 ID 로그 및 HIP 일치 로그를 Azure Security Center로 포워딩하려면 **Azure-Security-Center-Integration**을 수동으로 선택하고, 다른 로그 유형(객체 > 로그 포워딩 참조)에 대해 로그 포워딩 프로파일을 사용해야 합니다.

    *Security Center*의 무료 레이어는 *Azure* 구독에서 자동으로 활성화됩니다.

다음 로그 유형을 포워딩할 수 있습니다. 시스템, 구성, User-ID, HIP 일치 및 상관 관계 로그. 각 로그 유형에 대한 대상을 지정하려면 하나 이상의 일치 목록 프로파일(최대 64개)을 추가하고 다음 표에 설명된 필드를 완성하십시오.

트래픽, 위협, *WildFire* 제출, *URL* 필터링, 데이터 필터링, 터널 검사, *GTP* 및 인증 로그를 포워딩하려면 로그 포워딩 프로파일을 구성해야 합니다*(*개체 > 로그 포워딩 참조*).*

일치 목록 프로파일 설정	설명
이름	일치 목록 프로파일을 식별할 이름(최대 31자)을 입력합니다. 유효한 이름은 영숫자로 시작해야 하며 0, 영숫자, 밑줄, 하이픈, 마침표 또는 공백을 포함할 수 있습니다.
필터	기본적으로 방화벽은 일치 목록 프로파일을 추가한 유형의 모든 로그를 포워딩합니다. 로그의 하위 집합을 포워딩하려면 드롭다운을 열고 기존 필터를 선택하거나 필터 빌더를 선택하여 새 필터를 추가합니다. 새 필터의 각 쿼리에 대해 다음 필드를 지정하고 쿼리를 추가합니다. • 커넥터 - 쿼리에 대한 커넥터 논리(AND/OR)를 선택합니다. 논리에 무효를 적용하려면 무효를 선택합니다. 예를 들어, 신뢰할 수 없는 영역에서 로그를 포워딩하지 않으려면 무효를 선택한 다음 속성으로 영역을 선택하고 연산자로 같음을 선택한 다음 값 열에 신뢰할 수 없는 영역의 이름을 입력합니다. • 속성 - 로그 속성을 선택합니다. 사용 가능한 속성은 로그 유형에 따라 다릅니다. • 연산자 - 속성 적용 여부(예: 같음)를 결정하는 기준을 선택합니다. 사용 가능한 기준은 로그 유형에 따라 다릅니다. • 값 - 일치시킬 속성 값을 지정합니다. 필터와 일치하는 로그를 표시하거나 내보내려면 필터링된 로그 보기를 선택합니다. 이 탭은 모니터링 탭 페이지와 동일한 옵션을 제공합니다(예: 모니터링 > 로그 > 트래픽). 모든 이벤트 심각도 수준에 대한 로그를 포워딩하도록 필터를 설정합니다(기본 필터는 모든 로그임). 다른 심각도 수준에 대해 별도의 로그 포워딩 메서드을 만들려면 필터에서 하나 이상의 심각도 수준을 지정하고 포워딩 메서드를 구성한 다음 나머지 심각도 수준에 대해 프로세스를 반복합니다.
설명	이 일치 목록 프로파일의 목적을 설명하는 설명(최대 1,023자)을 입력합니다.
Panorama/로깅 서비스	로깅 서비스, 로그 수집기 또는 Panorama 관리 서버로 로그를 포워딩하려면 **Panorama**/로깅 서비스를 선택합니다. 이 옵션을 활성화하면 Panorama로의 로그 포워딩을 구성 해야 합니다.

일치 목록 프로파일 설정	설명
	방화벽에서 *Panorama*로 상관 관계 로그를 포워딩할 수 없습니다. *Panorama*는 수신한 방화벽 로그를 기반으로 상관 관계 로그를 생성합니다.
SNMP	SNMP 트랩으로 로그를 포워딩하려면 하나 이상의 SNMP 트랩 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > SNMP 트랩 참조).
이메일	이메일 알림으로 로그를 포워딩하려면 하나 이상의 이메일 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > 이메일 참조).
Syslog	하나 이상의 Syslog 서버 프로파일을 추가하여 로그를 syslog 메시지로 포워딩합니다(디바이스 > 서버 프로파일 > Syslog 참조).
HTTP	HTTP 요청으로 로그를 포워딩하려면 하나 이상의 HTTP 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > HTTP 참조).
기본 제공 작업	수행할 작업을 추가할 때 두 가지 유형의 기본 제공 작업인 태그 지정 및 통합 중에서 선택할 수 있습니다. • 태그 지정 - 필요에 따라 다음 설정을 구성하여 로그 항목에 소스 또는 대상 IP 주소를 포함하는 모든 로그 유형에 대한 작업을 추가할 수 있습니다. 상관 관계 로그 및 *HIP* 일치 로그에서 소스 *IP* 주소에만 태그를 지정할 수 있습니다. 로그 유형에는 로그 항목에 *IP* 주소가 포함되어 있지 않으므로 시스템 로그 및 구성 로그에 대한 작업을 구성할 수 없습니다. • 작업을 추가하고 작업을 설명하는 이름을 입력합니다. • 자동으로 태그를 지정할 IP 주소(소스 주소 또는 대상 주소)를 선택합니다. • 태그 추가 또는 태그 제거 작업을 선택합니다. • 이 방화벽이나 Panorama의 로컬 **User-ID** 에이전트 또는 원격 **User-ID** 에이전트에 IP 주소 및 태그 매핑을 등록할지의 여부를 선택합니다. • 원격 **User-ID** 에이전트에 IP 주소 및 태그 매핑을 등록하려면 포워딩을 활성화할 HTTP 서버 프로파일(디바이스 > 서버 프로파일 > HTTP)을 선택합니다. • IP 주소-태그 매핑이 유지되는 시간을 분 단위로 설정하도록 IP-태그 타임아웃을 구성합니다. 타임아웃을 0으로 설정하면 IP-태그 매핑이

일치 목록 프로파일 설정	설명
	타임아웃되지 않음을 의미합니다(범위는 0 ~ 43200(30일), 기본값은 0). 태그 추가 작업으로만 타임아웃을 구성할 수 있습니다. • 대상 소스 또는 대상 IP 주소에서 적용하거나 제거할 태그를 입력하거나 선택합니다. • 통합 - Azure의 VM 시리즈 방화벽에서만 사용할 수 있습니다. 이름을 추가하고 이 작업을 사용하여 선택한 로그를 Azure Security Center로 포워딩합니다. 이 옵션이 표시되지 않으면 Azure Security Center에 대해 Azure 구독이 활성화되지 않았을 수 있습니다. 로그 포워딩 프로파일 필터를 기반으로 디바이스를 분리 목록에 추가하려면 분리를 선택합니다.

알람 설정 정의

- 디바이스 > 로그 설정

경보 설정을 사용하여 CLI 및 웹 인터페이스에 대한 경보를 구성합니다. 다음 이벤트에 대한 알림을 구성할 수 있습니다.

- 보안 규칙(또는 규칙 그룹)이 지정된 임계값과 지정된 시간 인터벌 내에서 일치했습니다.
- 암호화/복호화 실패 임계값이 충족되었습니다.
- 각 로그 유형에 대한 로그 데이터베이스가 거의 꽉 찼습니다. 기본적으로 할당량은 사용 가능한 디스크 공간의 90%가 사용될 때 알리도록 설정됩니다. 경보를 구성하면 디스크가 가득차고 로그가 제거되기 전에 조치를 취할 수 있습니다.

알람을 활성화하면 웹 인터페이스 하단의 알람(Alarms)을 클릭하여 현재 목록을 볼 수 있습니다.

알람을 추가하려면 다음 표에 설명된 알람 설정을 편집하십시오.

알람 로그 설정	설명
알람 활성화	경보는 경보를 활성화한 경우에만 표시됩니다. 경보를 비활성화하면 방화벽은 조치가 필요한 중요한 이벤트에 대해 경고하지 않습니다. 예를 들어 알람은 마스터 키가 만료될 때를 알려줍니다. 키를 변경하기 전에 키가 만료되면 방화벽이 유지 관리 모드로 재부팅되고 공장 초기화가 필요합니다.

알람 로그 설정	설명
CLI 경보 알림 활성화	알람이 발생할 때마다 CLI 알람 알림을 활성화합니다.
웹 알람 알림 활성화	창을 열어 사용자 세션에 대한 경보(발생 시점 및 확인 시점 포함)를 표시합니다.
가청 경보 활성화	관리자가 웹 인터페이스에 로그인하고 승인되지 않은 경보가 존재하면 관리자의 컴퓨터에서 15초마다 경보음이 재생됩니다. 관리자가 모든 경보를 확인할 때까지 경보음이 재생됩니다. 경보를 보고 승인하려면 경보를 클릭합니다. 이 기능은 방화벽이 FIPS-CC 모드일 때만 사용할 수 있습니다.
암호화/복호화 실패 임계값	경보가 생성된 후의 암호화/복호화 실패 횟수를 지정합니다.
<로그 유형> 로그 DB	로그 데이터베이스가 최대 크기의 표시된 백분율에 도달하면 경보를 생성합니다.
보안 위반 임계값 / 보안 위반 기간	특정 IP 주소 또는 포트가 **Security Violations Time Period** 설정에 지정된 기간(초) 내에서 **Security Violations Threshold** 설정에 지정된 횟수만큼 거부 규칙에 도달하면 경보가 생성됩니다.
위반 임계값 / 위반 기간 / 보안 정책 태그	규칙 모음이 **Violations Time Period** 필드에 지정된 기간 동안 **Violations Threshold** 필드에 지정된 규칙 제한 위반 수에 도달하면 경보가 생성됩니다. 세션이 명시적 거부 정책과 일치하면 위반이 계산됩니다. 보안 정책 태그를 사용하여 규칙 제한 임계값이 경보를 생성할 태그를 지정합니다. 이러한 태그는 보안 정책을 정의할 때 지정할 수 있습니다.
선택적 감사	선택적 감사 옵션은 방화벽이 FIPS-CC 모드에 있는 경우에만 사용할 수 있습니다. 다음 설정을 지정합니다. • **FIPS-CC** 특정 로깅 - CC(Common Criteria) 준수에 필요한 자세한 로깅을 활성화합니다. • 패킷 삭제 로깅 - 방화벽에 의해 삭제된 패킷을 기록합니다. • **Suppress Login Success Logging**—방화벽에 대한 성공적인 관리자 로그인의 로깅을 중지합니다. • **Suppress Login Failure Logging(**로그인 실패 로깅 억제**)** - 방화벽에 대한 실패한 관리자 로그인의 로깅을 중지합니다. • **TLS** 세션 로깅 - TLS 세션 설정을 기록합니다.

알람 로그 설정	설명
	• **CA(OCSP/CRL)** 세션 설정 로깅 - 방화벽이 온라인 인증서 상태 프로토콜 또는 인증서 해지 목록 서버 요청을 사용하여 인증서 해지 상태 확인 요청을 보낼 때 방화벽과 인증 기관 간의 세션 설정을 기록합니다. (기본적으로 비활성화되어 있습니다.) • **IKE** 세션 설정 로깅 - 방화벽의 VPN 게이트웨이가 피어로 인증할 때 IPSec IKE 세션 설정을 기록합니다. 피어는 Palo Alto Networks 방화벽 또는 VPN 연결을 시작하고 종료하는 데 사용되는 다른 보안 디바이스일 수 있습니다. 로그에 지정된 인터페이스 이름은 IKE 게이트웨이에 바인딩된 인터페이스입니다. 해당되는 경우 IKE 게이트웨이 이름도 표시됩니다. 이 옵션을 비활성화하면 모든 IKE 로깅 이벤트의 로깅이 중지됩니다. (기본적으로 활성화되어 있습니다.) • 억제된 관리자 - 나열된 관리자가 방화벽 구성에 대해 수행한 변경 사항의 기록을 중지합니다.

로그 지우기

- 디바이스 > 로그 설정

로그 설정 페이지에서 로그 관리에서 방화벽의 로그를 지울 수 있습니다. 지우려는 로그 유형을 클릭하고 예를 클릭하여 요청을 확인합니다.

로그 및 보고서를 자동으로 삭제하려면 만료 기간을 구성할 수 있습니다. 자세한 내용은 로깅 및 보고 설정을 참조하십시오.

디바이스 > 서버 프로파일

다음 항목에서는 방화벽에서 구성할 수 있는 서버 프로파일 설정에 대해 설명합니다.

- 디바이스 > 서버 프로파일 > SNMP 트랩
- 디바이스 > 서버 프로파일 > Syslog
- 디바이스 > 서버 프로파일 > 이메일
- 디바이스 > 서버 프로파일 > HTTP
- Device > Server Profiles > NetFlow
- 디바이스 > 서버 프로파일 > RADIUS
- 디바이스 > 서버 프로파일 > TACACS+
- 디바이스 > 서버 프로파일 > LDAP
- 디바이스 > 서버 프로파일 > Kerberos
- 디바이스 > 서버 프로파일 > SAML ID 공급자
- 디바이스 > 서버 프로파일 > DNS
- 디바이스 > 서버 프로파일 > 다단계 인증

디바이스 > 서버 프로파일 > SNMP 트랩

SNMP(Simple Network Management Protocol)는 네트워크의 디바이스를 모니터링하기 위한 표준 프로토콜입니다. 네트워크의 시스템 이벤트 또는 위협에 대해 경고하기 위해 모니터링되는 디바이스는 SNMP 트랩을 SNMP 관리자(트랩 서버)로 보냅니다. **Device** > **Server Profiles** > **SNMP Trap** 또는 **Panorama** > **Server Profiles** > **SNMP Trap**을 선택하여 방화벽 또는 Panorama가 SNMP 관리자에게 트랩을 보낼 수 있도록 하는 서버 프로파일을 구성합니다. SNMP GET 메시지(SNMP 관리자의 통계 요청)를 활성화하려면 SNMP 모니터링 활성화를 참조하십시오.

서버 프로파일을 만든 후에는 SNMP 트랩을 보내기 위해 방화벽을 트리거할 로그 유형을 지정해야 합니다(디바이스 > 로그 설정). SNMP 관리자가 트랩을 해석할 수 있도록 로드해야 하는 MIB 목록은 지원되는 MIB를 참조하십시오.

시스템 로그 설정 또는 로깅 프로파일이 사용하는 서버 프로파일을 삭제하지 마십시오.

SNMP 트랩 서버 프로파일 설정	설명
이름	SNMP 프로파일의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
버전	SNMP 버전 선택: **V2c**(기본값) 또는 **V3**. 선택 항목은 대화 상자에 표시되는 나머지 필드를 제어합니다. 두 버전에 대해 최대 4개의 SNMP 관리자를 추가할 수 있습니다. 네트워크 연결을 안전하게 유지하기 위해 인증 및 기타 기능을 제공하는 *SNMPv3*를 사용하십시오.
For SNMP V2c	
이름	SNMP 관리자의 이름을 지정합니다. 이름은 영숫자, 마침표, 밑줄 또는 하이픈으로 최대 31자를 사용할 수 있습니다.
SNMP 관리자	SNMP 관리자의 FQDN 또는 IP 주소를 지정합니다.

SNMP 트랩 서버 프로파일 설정	설명
커뮤니티	SNMP 관리자 및 모니터링되는 디바이스의 SNMP 커뮤니티를 식별하고 트랩 포워딩 중에 커뮤니티 구성원을 서로 인증하기 위한 암호 역할도 하는 커뮤니티 문자열을 입력합니다. 문자열은 최대 127자를 포함할 수 있으며 모든 문자를 허용하며 대소문자를 구분합니다. 기본 커뮤니티 문자열을 사용하지 마십시오*(*커뮤니티 문자열을 공개 또는 비공개로 설정하지 마십시오*)*. 여러 *SNMP* 서비스를 사용하는 경우 충돌을 방지하는 고유한 커뮤니티 문자열을 사용합니다. *SNMP* 메시지에는 일반 텍스트로 된 커뮤니티 문자열이 포함되어 있으므로 커뮤니티 구성원*(*관리자 액세스*)*을 정의할 때 네트워크의 보안 요구 사항을 고려하십시오.
SNMP V3의 경우	
이름	SNMP 관리자의 이름을 지정합니다. 이름은 영숫자, 마침표, 밑줄 또는 하이픈으로 최대 31자를 사용할 수 있습니다.
SNMP 관리자	SNMP 관리자의 FQDN 또는 IP 주소를 지정합니다.
사용자	SNMP 사용자 계정을 식별하기 위한 사용자명을 지정합니다(최대 31자). 방화벽에서 구성한 사용자명은 SNMP 관리자에 구성된 사용자명과 일치해야 합니다.
EngineID	방화벽의 엔진 ID를 지정합니다. SNMP 관리자와 방화벽이 서로를 인증할 때 트랩 메시지는 이 값을 사용하여 방화벽을 고유하게 식별합니다. 필드를 비워 두면 메시지에서 방화벽 일련번호를 **EngineID**로 사용합니다. 값을 입력하는 경우 5-64바이트(바이트당 2자)를 나타내기 위해 0x가 프리픽스로 추가되고 10-128자가 추가로 붙는 16진수 형식이어야 합니다. 고가용성(HA) 구성의 방화벽의 경우 SNMP 관리자가 트랩을 보낸 HA 피어를 식별할 수 있도록 필드를 비워 둡니다. 그렇지 않으면 값이 동기화되고 두 피어 모두 동일한 **EngineID**를 사용합니다.
인증 비밀번호	SNMP 사용자의 인증 암호를 지정합니다. 방화벽은 암호를 사용하여 SNMP 관리자를 인증합니다. 암호는 8-256자여야 하며 모든 문자가 허용됩니다.
개인 비밀번호	SNMP 사용자의 개인 정보 암호를 지정합니다. 암호는 8-256자여야 하며 모든 문자가 허용됩니다.

SNMP 트랩 서버 프로파일 설정	설명
인증 프로토콜	SNMP 관리자 암호에 대해 보안 해시 알고리즘(SHA)을 선택합니다. **SHA-1**, **SHA-224**, **SHA-256**, **SHA-384** 또는 **SHA-512**를 선택할 수 있습니다.
개인 정보 보호 프로토콜	SNMP 트랩 및 통계 요청에 대한 응답에 대해 Advanced 암호화 표준(AES)을 선택합니다. **AES-128**, **AES-192** 또는 **AES-256**을 선택할 수 있습니다.

디바이스 > 서버 프로파일 > Syslog

Device > **Server Profiles** > **Syslog** 또는 **Panorama** > **Server Profiles** > **Syslog**를 선택하여 방화벽, Panorama 및 Log Collector 로그를 syslog 서버에 syslog 메시지로 포워딩하기 위한 서버 프로파일을 구성합니다. syslog 서버 프로파일을 정의하려면 추가를 클릭하고 새 Syslog 서버 필드를 지정합니다.

- 시스템, 구성, *User-ID*, *HIP* 일치 및 상관 관계 로그에 대한 *Syslog* 서버 프로파일을 선택하려면 디바이스 > 로그 설정을 참조하십시오.
- 트래픽, 위협, *Wildfire*, *URL* 필터링, 데이터 필터링, 터널 검사, 인증 및 *GTP* 로그에 대한 *Syslog* 서버 프로파일을 선택하려면 개체 > 로그 포워딩을 참조하십시오.
- 방화벽이 시스템 또는 구성 로그 설정 또는 로그 포워딩 프로파일에서 사용하는 서버 프로파일은 삭제할 수 없습니다.

Syslog 서버 설정	설명
이름	syslog 프로파일의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
서버 탭	
이름	추가를 클릭하고 syslog 서버의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
서버	syslog 서버의 IP 주소 또는 FQDN을 입력합니다.
전송	UDP, TCP 또는 SSL을 통해 syslog 메시지를 전송할지의 여부를 선택합니다. ***SSL***을 사용하여 *syslog* 서버로 전송되는 데이터를 암호화하고 보호합니다. 데이터는 일반 텍스트로 *UDP* 또는 *TCP*를 통해 전송되며 전송 중에 읽을 수 있습니다.

Syslog 서버 설정	설명
포트	syslog 서버의 포트 번호를 입력합니다(UDP의 표준 포트는 514, SSL의 표준 포트는 6514, TCP의 경우 포트 번호를 지정해야 함).
형식	사용할 syslog 형식을 지정합니다. BSD(기본값) 또는 IETF.
시설	Syslog 표준 값 중 하나를 선택합니다. Syslog 서버가 기능 필드를 사용하여 메시지를 관리하는 방법에 매핑되는 값을 선택하십시오. 시설 필드에 대한 자세한 내용은 RFC 3164(BSD 형식) 또는 RFC 5424(IETF 형식)를 참조하십시오.
사용자 정의 로그 형식 탭	
로그 유형	로그 유형을 클릭하여 사용자 정의 로그 형식을 지정할 수 있는 대화 상자를 엽니다. 대화 상자에서 필드를 클릭하여 로그 형식 영역에 추가합니다. 다른 텍스트 문자열은 로그 형식 영역에서 직접 편집할 수 있습니다. 확인을 클릭하여 설정을 저장합니다. 사용자 지정 로그 에 사용할 수 있는 각 필드에 대한 설명을 봅니다. 사용자 정의 로그에 사용할 수 있는 필드에 대한 자세한 내용은 디바이스 > 서버 프로파일 > 이메일을 참조하십시오.
이스케이프	이스케이프 시퀀스를 지정합니다. 이스케이프된 문자는 공백 없이 이스케이프할 모든 문자의 목록입니다.

디바이스 > 서버 프로파일 > 이메일

디바이스 > 서버 프로파일 > 이메일 또는 **Panorama** > **Server** 프로파일 > 이메일을 선택하여 로그를 이메일 알림으로 포워딩하기 위한 서버 프로파일을 구성합니다. 이메일 서버 프로파일을 정의하려면 프로파일을 추가하고 이메일 알림 설정을 지정합니다.

- 시스템, 구성, *User-ID*, *HIP* 일치 및 상관 관계 로그에 대한 이메일 서버 프로파일을 선택하려면 디바이스 > 로그 설정을 참조하십시오.
- 트래픽, 위협, *Wildfire*, *URL* 필터링, 데이터 필터링, 터널 검사, 인증 및 *GTP* 로그에 대한 이메일 서버 프로파일을 선택하려면 개체 > 로그 포워딩을 참조하십시오.
- 이메일 보고서를 예약할 수도 있습니다(모니터 > PDF 보고서 > 이메일 스케줄러).
- 방화벽이 시스템 또는 구성 로그 설정 또는 로그 포워딩 프로파일에서 사용하는 서버 프로파일은 삭제할 수 없습니다.

이메일 알림 설정	설명
이름	서버 프로파일의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치 (가상 시스템에만 해당)	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
서버 탭	
이름	서버를 식별할 수 있는 이름을 입력합니다(최대 31자). 이 필드는 레이블일 뿐이며 기존 이메일 서버의 호스트 이름일 필요는 없습니다.
이메일 표시 이름	이메일의 보낸 사람 필드에 표시된 이름을 입력합니다.
발신자	발신자의 이메일 주소(예: security_alert@company.com)를 입력합니다.
수신자	받는 사람의 이메일 주소를 입력합니다.

이메일 알림 설정	설명
추가 수신자	선택적으로 다른 수신자의 이메일 주소를 입력합니다. 수신자는 한 명만 추가할 수 있습니다. 여러 수신자를 추가하려면 메일 그룹의 이메일 주소를 추가하십시오.
이메일 게이트웨이	이메일을 보내는 서버의 IP 주소 또는 호스트 이름을 입력합니다.
프로토콜	이메일을 보내는 데 사용할 프로토콜을 선택합니다(인증되지 않은 **SMTP** 또는 **TLS**를 통한 **SMTP**).
포트	기본값(SMTP의 경우 25 또는 TLS의 경우 587)과 다른 경우 이메일을 보내는 데 사용할 포트 번호를 입력합니다.
TLS 버전 (TLS를 통한 SMTP만 해당)	사용할 TLS 버전(**1.2** 또는 **1.1**)을 선택합니다. 모범 사례로 최신 *TLS* 버전을 사용하는 것이 좋습니다.
인증 방법 (TLS를 통한 SMTP만 해당)	사용하려는 인증 방법을 선택하십시오. • 자동(기본값) - 클라이언트와 서버가 인증 방법을 결정할 수 있도록 합니다. • 로그인 - 사용자명과 비밀번호에 Base64 인코딩을 사용하고 별도로 전송합니다. • 일반 - 사용자명과 암호에 Base64 인코딩을 사용하고 함께 전송합니다.
인증서 프로파일 (TLS를 통한 SMTP에만 해당)	이메일 서버를 인증하는 데 사용할 방화벽의 인증서 프로파일을 선택합니다.
사용자 이름 (TLS를 통한 SMTP에만 해당)	이메일을 보내는 계정의 사용자명을 입력합니다.
암호 (TLS를 통한 SMTP에만 해당)	이메일을 보내는 계정의 비밀번호를 입력하세요.
암호 확인	이메일을 보내는 계정의 비밀번호를 확인합니다.

이메일 알림 설정	설명
(TLS를 통한 SMTP에만 해당)	
연결 테스트 (TLS를 통한 SMTP에만 해당)	이메일 서버와 방화벽 간의 연결을 확인합니다.
사용자 정의 로그 형식 탭	
로그 유형	로그 유형을 클릭하여 사용자 정의 로그 형식을 지정할 수 있는 대화 상자를 엽니다. 대화 상자에서 필드를 클릭하여 로그 형식 영역에 추가합니다. 확인을 클릭하여 변경 사항을 저장합니다.
이스케이프	공백 없이 이스케이프 문자(문자 그대로 해석되지 않는 모든 문자)를 지정하고 이스케이프 시퀀스에 대한 이스케이프 문자를 지정합니다.

디바이스 > 서버 프로파일 > HTTP

디바이스 > 서버 프로파일 > **HTTP** 또는 **Panorama** > **Server** 프로파일 > **HTTP**를 선택하여 로그 포워딩을 위한 서버 프로파일을 구성합니다. 로그를 HTTP(S) 대상으로 포워딩하거나 API를 노출하는 모든 HTTP 기반 서비스와 통합하도록 방화벽을 구성하고 사용자 요구 사항을 충족하도록 HTTP 요청의 URL, HTTP 헤더, 매개변수 및 페이로드를 필요에 따라 수정할 수 있습니다. 또한 HTTP 서버 프로파일을 사용하여 PAN-OS 통합 User-ID 에이전트를 실행하는 방화벽에 액세스하고 방화벽이 생성한 로그의 소스 또는 대상 IP 주소에 하나 이상의 태그를 등록할 수 있습니다.

HTTP 서버 프로파일을 사용하여 로그를 포워딩하려면*:*

- 시스템, 구성, *User-ID*, *HIP* 일치 및 상관 관계 로그에 대한 디바이스 > 로그 설정을 참조하십시오.
- 트래픽, 위협, *WildFire*, *URL* 필터링, 데이터 필터링, 터널 검사, 인증 및 *GTP* 로그에 대한 개체 > 로그 포워딩을 참조하십시오.

로그를 포워딩하는 데 사용되는 *HTTP* 서버 프로파일은 삭제할 수 없습니다. 방화벽 또는 *Panorama*에서 서버 프로파일을 삭제하려면 디바이스 > 로그 설정또는 개체 > 로그 포워딩 프로파일에서 프로파일에 대한 모든 참조를 삭제해야 합니다.

HTTP 서버 프로파일을 정의하려면 새 프로파일을 추가하고 다음 표에서 설정을 구성합니다.

HTTP 서버 설정	설명
이름	서버 프로파일의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 유효한 이름은 영숫자 문자로 시작해야 하며 0, 영숫자 문자, 밑줄, 하이픈, 점 또는 공백을 포함할 수 있습니다.
위치	서버 프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
태그 등록	태그 등록을 사용하면 로그 항목의 소스 또는 대상 IP 주소에 태그를 추가하거나 제거하고 HTTP(S)를 사용하여 방화벽의 User-ID 에이전트에 IP 주소 및 태그 매핑을 등록할 수 있습니다. 그런 다음 이러한 태그를 필터링 기준으로 사용하여 해당 구성원을 결정하고 태그를 기반으로 IP 주소에 정책 규칙을 적용하는 동적 주소 그룹을 정의할 수 있습니다.

HTTP 서버 설정	설명
	방화벽의 User-ID 에이전트에 대한 HTTP(S) 액세스를 활성화하려면 연결 세부 정보를 추가합니다. Panorama의 User-ID 에이전트에 태그를 등록하려면 서버 프로파일이 필요하지 않습니다. 또한 HTTP 서버 프로파일을 사용하여 Windows 서버에서 실행되는 User-ID 에이전트에 태그를 등록할 수 없습니다.
서버 탭	
이름	HTTP(s) 서버를 추가하고 이름(최대 31자) 또는 원격 User-ID 에이전트를 입력합니다. 유효한 이름은 고유해야 하며 영숫자로 시작해야 합니다. 이름에는 0, 영숫자, 밑줄, 하이픈, 점 또는 공백이 포함될 수 있습니다. 서버 프로파일에는 최대 4개의 서버가 포함될 수 있습니다.
주소	HTTP(S) 서버의 IP 주소를 입력합니다. 태그 등록을 위해 User-ID 에이전트로 구성된 방화벽의 IP 주소를 지정합니다.
프로토콜	프로토콜 선택: HTTP 또는 HTTPS.
포트	서버 또는 방화벽에 액세스할 포트 번호를 입력합니다. HTTP의 기본 포트는 80이고 HTTPS의 기본 포트는 443입니다. 태그 등록을 위해 방화벽은 HTTP 또는 HTTPS를 사용하여 User-ID 에이전트로 구성된 방화벽의 웹 서버에 연결합니다.
TLS 버전	서버의 SSL에 대해 지원되는 TLS 버전을 선택하십시오. 기본값은 **1.2**입니다.
인증서 프로파일	서버와의 TLS 연결에 사용할 인증서 프로파일을 선택합니다. 방화벽은 서버에 대한 보안 연결을 설정할 때 지정된 인증서 프로파일을 사용하여 서버 인증서의 유효성을 검사합니다.
HTTP 메서드	서버가 지원하는 HTTP 메서드를 선택하십시오. 옵션은 GET, PUT, POST(기본값) 및 DELETE입니다. User-ID 에이전트의 경우 GET 방법을 사용합니다.
사용자명	선택한 HTTP 메서드를 완료하기 위해 액세스 권한이 있는 사용자명을 입력합니다.

HTTP 서버 설정	설명
	방화벽의 User-ID 에이전트에 태그를 등록하는 경우 사용자명은 운용 관리자 역할을 가진 관리자의 사용자명이어야 합니다.
비밀번호	서버 또는 방화벽에 인증할 비밀번호를 입력합니다.
테스트 서버 연결	서버와 테스트 서버 연결을 선택하여 서버에 대한 네트워크 연결을 테스트합니다. 이 테스트는 User-ID 에이전트를 실행하는 서버에 대한 연결을 테스트하지 않습니다.
페이로드 형식 탭	
로그 유형	HTTP 포워딩에 사용할 수 있는 로그 유형이 표시됩니다. 로그 유형을 클릭하여 사용자 정의 로그 형식을 지정할 수 있는 대화 상자를 엽니다.
형식	로그 유형이 기본 형식, 사전 정의된 형식 또는 사용자가 정의한 사용자 지정 페이로드 형식을 사용하는지의 여부를 표시합니다.
사전 정의된 형식	로그를 보낼 서비스 또는 공급자의 형식을 선택합니다. 사전 정의된 형식은 콘텐츠 업데이트를 통해 푸시되며 방화벽이나 Panorama에 새 콘텐츠 업데이트를 설치할 때마다 변경될 수 있습니다.
이름	사용자 정의 로그 형식의 이름을 입력하십시오.
URI 형식	HTTP(S)를 사용하여 로그를 보낼 리소스를 지정합니다. 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 공급자에서 요구하는 구문과 일치하는지 확인합니다. HTTP 헤더, 매개변수 및 값 쌍과 요청 페이로드 내에서 선택한 로그 유형에서 지원되는 모든 속성을 사용할 수 있습니다.
HTTP 헤더	헤더 및 해당 값을 추가합니다.
매개변수	선택적 매개변수와 값을 포함합니다.
페이로드	외부 웹 서버에 대한 HTTP 메시지에 페이로드로 포함할 로그 속성을 선택합니다.
테스트 로그 보내기	외부 웹 서버가 올바른 페이로드 형식으로 요청을 수신하는지 확인하려면 이 버튼을 클릭하십시오.

디바이스 > 서버 프로파일 > NetFlow

Palo Alto Networks 방화벽은 인터페이스의 IP 트래픽에 대한 통계를 NetFlow 필드로 NetFlow 수집기에 내보낼 수 있습니다. 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. 집합 이더넷 인터페이스의 경우 집합 그룹에 대한 레코드를 내보낼 수 있지만 그룹 내의 개별 인터페이스에 대해서는 내보낼 수 없습니다. 방화벽은 NetFlow 수집기가 NetFlow 필드를 복호화하는 데 사용하는 표준 및 엔터프라이즈(PAN-OS 전용) NetFlow 템플릿을 지원합니다. 방화벽은 내보낸 데이터 유형에 따라 템플릿을 선택합니다. IPv4 또는 IPv6 트래픽(NAT 포함 또는 미포함, 표준 또는 기업별 필드 포함).

NetFlow 내보내기를 구성하려면 NetFlow 서버 프로파일을 추가하여 내보낸 데이터를 수신할 NetFlow 서버를 지정하고 내보내기 매개변수를 지정합니다. 인터페이스에 프로파일을 할당하면(네트워크 > 인터페이스 참조) 방화벽은 해당 인터페이스의 모든 트래픽에 대한 NetFlow 데이터를 지정된 서버로 내보냅니다.

넷플로우 설정	설명
이름	Netflow 서버 프로파일의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
템플릿 새로 고침 빈도	방화벽은 NetFlow 템플릿을 주기적으로 새로 고쳐 어떤 템플릿을 사용할지(내보낸 데이터 유형이 변경된 경우) 다시 평가하고 선택한 템플릿의 필드에 변경 사항을 적용합니다. NetFlow 수집기의 요구 사항에 따라 방화벽이 NetFlow 템플릿을 새로 고치는 속도를 분(범위: 1~3,600, 기본값: 30) 및 패킷(내보낸 레코드 - 범위: 1~600, 기본값: 20)으로 지정합니다. 방화벽은 임계값 중 하나를 통과한 후 템플릿을 새로 고칩니다. 필요한 새로 고침 빈도는 NetFlow 수집기에 따라 다릅니다. 여러 NetFlow 수집기를 서버 프로파일에 추가하는 경우 새로 고침 빈도가 가장 빠른 수집기의 값을 사용합니다.
활성 타임아웃	방화벽이 각 세션에 대한 데이터 레코드를 내보내는 빈도(분)를 지정합니다(범위는 1~60, 기본값은 5). NetFlow 수집기가 트래픽 통계를 업데이트할 빈도를 기반으로 빈도를 설정합니다.
PAN-OS 필드 유형	Netflow 레코드의 App-ID 및 User-ID 서비스에 대한 PAN-OS 특정 필드를 내보냅니다.
서버	

넷플로우 설정	설명
이름	서버를 식별하는 이름을 지정합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
서버	서버의 호스트 이름 또는 IP 주소를 지정합니다. 프로파일당 최대 2개의 서버를 추가할 수 있습니다.
포트	서버 액세스를 위한 포트 번호를 지정합니다(기본값은 2055).

디바이스 > 서버 프로파일 > RADIUS

디바이스 > 서버 프로파일 > **RADIUS** 또는 **Panorama** > **Server** 프로파일 > **RADIUS**를 선택하여 인증 프로파일이 참조하는 RADIUS(Remote Authentication Dial-In User Service) 서버에 대한 설정을 구성합니다(디바이스 > 인증 프로파일 참조). RADIUS를 사용하여 (GlobalProtect 또는 인증 포털을 통해) 네트워크 리소스에 액세스하는 최종 사용자를 인증하고, 방화벽 또는 Panorama에 로컬로 정의된 관리자를 인증하고, RADIUS 서버에 외부적으로 정의된 관리자를 인증 및 승인할 수 있습니다.

RADIUS 서버 설정	설명
프로파일 이름	서버 프로파일을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대/소문자에 민감하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
관리자 전용	관리자 계정만 인증에 프로파일을 사용할 수 있도록 지정하려면 이 옵션을 선택합니다. 여러 가상 시스템이 있는 방화벽의 경우 이 옵션은 위치가 공유인 경우에만 나타납니다.
타임아웃	인증 요청 시간이 초과되는 인터벌(초)을 입력합니다(범위는 1–120, 기본값은 3). *RADIUS* 서버 프로파일을 사용하여 방화벽을 *MFA* 서비스와 통합하는 경우 사용자에게 인증 질문에 응답할 수 있는 충분한 시간을 제공하는 인터벌을 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.
인증 프로토콜	방화벽이 RADIUS 서버에 대한 연결을 보호하는 데 사용하는 인증 프로토콜을 선택합니다. • **PEAP-MSCHAPv2** - (기본값) Microsoft Challenge-Handshake 인증 프로토콜(MSCHAPv2)을 사용하는 PEAP(보호된 EAP)는 암호화된 터널에서 사용자명과 암호를 모두 전송하여 PAP 또는 CHAP에 대해 향상된 보안을 제공합니다.

RADIUS 서버 설정	설명
	• **PEAP with GTC** - 암호화된 터널에서 일회성 토큰을 사용하려면 일반 토큰 카드(GTC)가 있는 보호된 EAP(PEAP)를 선택합니다. • **PAP**가 포함된 **EAP-TTLS** - 터널링된 전송 레이어 보안(TTLS) 및 PAP가 포함된 EAP를 선택하여 암호화된 터널에서 PAP에 대한 일반 텍스트 자격 증명을 전송합니다. • **CHAP** - RADIUS 서버가 EAP 또는 PAP를 지원하지 않거나 이에 대해 구성되지 않은 경우 CHAP(Challenge-Handshake 인증 프로토콜)를 선택합니다. • **PAP** - RADIUS 서버가 EAP 또는 CHAP를 지원하지 않거나 이에 대해 구성되지 않은 경우 PAP(암호 인증 프로토콜)를 선택합니다.
만료 후 사용자가 비밀번호를 변경할 수 있도록 허용	(GlobalProtect 4.1 이상이 포함된 PEAP-MSCHAPv2) GlobalProtect 사용자가 만료된 암호를 변경할 수 있도록 하려면 이 옵션을 선택합니다.
외부 ID를 익명으로 설정	(PEAP-MSCHAPv2, PEAP with GTC 또는 EAP-TTLS with PAP) 이 옵션은 서버 인증 후 방화벽이 생성하는 외부 터널에서 User-ID를 익명화하기 위해 기본적으로 활성화됩니다. 일부 *RADIUS* 서버 구성은 익명 외부 *ID*를 지원하지 않을 수 있으며 이 옵션을 선택 취소해야 할 수 있습니다. 선택을 취소하면 사용자명이 일반 텍스트로 전송됩니다.
인증서 프로파일	(PEAP-MSCHAPv2, PEAP with GTC 또는 EAP-TTLS with PAP) RADIUS 서버 프로파일과 연결할 인증서 프로파일을 선택하거나 구성합니다. 방화벽은 인증서 프로파일을 사용하여 RADIUS 서버를 인증합니다.
재시도	타임아웃 후 재시도할 횟수를 지정합니다(범위는 1–5, 기본값은 3).
서버	원하는 순서대로 각 서버에 대한 정보를 구성합니다. • 이름 - 서버를 식별하는 이름을 입력합니다. • **RADIUS** 서버 - 서버 IP 주소 또는 FQDN을 입력합니다. • **Secret/Confirm Secret**(비밀/비밀 확인) - 방화벽과 RADIUS 서버 간의 연결을 확인하고 암호화하기 위한 키를 입력하고 확인합니다. • 포트 - 인증 요청을 위한 서버 포트(범위는 1–65,535, 기본값은 1812)를 입력합니다.

디바이스 > 서버 프로파일 > TACACS+

디바이스 > 서버 프로파일 > **TACACS+** 또는 **Panorama** > **Server** 프로파일 > **TACACS+**를 선택하여 방화벽 또는 Panorama가 TACACS+(터미널 액세스 컨트롤러 액세스 제어 시스템 플러스) 서버에 연결하는 방법을 정의하는 설정을 구성합니다(디바이스 > 인증 프로파일 참조). TACACS+를 사용하여 (GlobalProtect 또는 인증 포털을 통해) 네트워크 리소스에 액세스하는 최종 사용자를 인증하고, 방화벽 또는 Panorama에 로컬로 정의된 관리자를 인증하고, TACACS+ 서버에 외부적으로 정의된 관리자를 인증 및 승인할 수 있습니다.

TACACS+ 서버 설정	설명
프로파일 이름	서버 프로파일을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대/소문자에 민감하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
관리자 전용	관리자 계정만 인증에 프로파일을 사용할 수 있도록 지정하려면 이 옵션을 선택합니다. Multi-VSYS 방화벽의 경우 이 옵션은 위치가 공유인 경우에만 나타납니다.
타임아웃	인증 요청 시간이 초과되는 인터벌(초)을 입력합니다(범위는 1–20, 기본값은 3).
인증 프로토콜	방화벽이 TACACS+ 서버에 대한 연결을 보호하는 데 사용하는 인증 프로토콜을 선택합니다. • **CHAP** - CHAP(Challenge-Handshake 인증 프로토콜)는 PAP보다 안전하기 때문에 기본적으로 선호되는 프로토콜입니다. • **PAP** - TACACS+ 서버가 CHAP를 지원하지 않거나 구성되지 않은 경우 PAP(암호 인증 프로토콜)를 선택합니다. • 자동 - 방화벽이 먼저 CHAP를 사용하여 인증을 시도합니다. TACACS+ 서버가 응답하지 않으면 방화벽이 PAP로 대체됩니다.
모든 인증에 단일 연결 사용	모든 인증에 동일한 TCP 세션을 사용하려면 이 옵션을 선택합니다. 이 옵션은 각 인증 이벤트에 대해 별도의 TCP 세션을 시작하고 해제하는 데 필요한 처리를 피함으로써 성능을 향상시킵니다.

TACACS+ 서버 설정	설명
서버	추가를 클릭하고 각 TACACS+ 서버에 대해 다음 설정을 지정합니다. • 이름 - 서버를 식별하는 이름을 입력합니다. • **TACACS+** 서버 - TACACS+ 서버의 IP 주소 또는 FQDN을 입력합니다. • **Secret/Confirm Secret(**비밀/비밀 확인**)** - 방화벽과 TACACS+ 서버 간의 연결을 확인하고 암호화하기 위한 키를 입력하고 확인합니다. • 포트 - 인증 요청을 위한 서버 포트(기본값은 49)를 입력합니다.

디바이스 > 서버 프로파일 > LDAP

- 디바이스 > 서버 프로파일 > **LDAP**
- **Panorama** > 서버 프로파일 > **LDAP**

LDAP 서버 프로파일을 추가하거나 선택하여 인증 프로파일이 참조하는 LDAP(Lightweight Directory Access Protocol) 서버에 대한 설정을 구성합니다(디바이스 > 인증 프로파일 참조). LDAP를 사용하여 네트워크 리소스(GlobalProtect 또는 인증 포털을 통해)에 액세스하는 최종 사용자와 방화벽 또는 Panorama에 로컬로 정의된 관리자를 인증할 수 있습니다.

LDAP 서버 설정	설명
프로파일 이름	프로파일을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
관리자 전용	관리자 계정만 인증에 프로파일을 사용할 수 있도록 지정하려면 이 옵션을 선택합니다. 여러 가상 시스템이 있는 방화벽의 경우 이 옵션은 위치가 공유인 경우에만 나타납니다.
서버 목록	각 LDAP 서버에 대해 호스트 이름, IP 주소 또는 FQDN(**LDAP** 서버) 및 포트(기본값은 389)를 추가합니다. 중복성을 제공하려면 두 개 이상의 *LDAP* 서버를 구성하십시오.
유형	드롭다운에서 서버 유형을 선택합니다.
베이스 DN	사용자 또는 그룹 정보에 대한 검색 범위를 좁히려면 디렉토리 서버에 루트 컨텍스트를 지정하십시오.
바인드 DN	디렉토리 서버의 로그인 이름(고유 이름)을 지정합니다. *Bind DN* 계정에는 *LDAP* 디렉토리를 읽을 수 있는 권한이 있어야 합니다.

LDAP 서버 설정	설명
비밀번호/비밀번호 확인	바인드 계정 비밀번호를 지정하십시오. 에이전트는 암호화된 암호를 구성 파일에 저장합니다.
바인딩 타임아웃	디렉토리 서버에 연결할 때 적용되는 시간 제한(초)을 지정합니다(범위는 1 - 30, 기본값은 30).
검색 타임아웃	디렉토리 검색을 수행할 때 적용되는 시간 제한(초)을 지정합니다(범위는 1 - 30, 기본값은 30).
재시도 인터벌	이전에 시도가 실패한 후 시스템이 LDAP 서버에 연결을 시도할 인터벌(초)을 지정합니다(범위는 1 - 3,600, 기본값은 60).
SSL/TLS 보안 연결 필요	방화벽이 디렉토리 서버와의 통신에 SSL 또는 TLS를 사용하도록 하려면 이 옵션을 선택하십시오. 프로토콜은 서버 포트에 따라 다릅니다. • 389(기본값) - TLS(특히, 방화벽은 초기 일반 텍스트 연결을 TLS로 업그레이드하는 TLS 시작 작업을 사용합니다.) • 636—SSL • 기타 포트 - 방화벽은 먼저 TLS 사용을 시도합니다. 디렉토리 서버가 TLS를 지원하지 않으면 방화벽은 SSL로 대체합니다. 이 옵션은 보안을 강화하고 기본적으로 선택되므로 모범 사례입니다.
SSL 세션에 대한 서버 인증서 확인	디렉터리 서버가 SSL/TLS 연결에 대해 제공하는 인증서를 방화벽이 확인하도록 하려면 이 옵션(기본적으로 선택 취소됨)을 선택합니다. 방화벽은 두 가지 측면에서 인증서를 확인합니다. • 인증서가 신뢰할 수 있고 유효합니다. 방화벽이 인증서를 신뢰하려면 해당 루트 CA(인증 기관) 및 모든 중간 인증서가 디바이스 > 인증서 관리 > 인증서 > 디바이스 인증서 아래의 인증서 저장소에 있어야 합니다. • 인증서 이름은 LDAP 서버의 호스트 이름과 일치해야 합니다. 방화벽은 먼저 인증서 속성 Subject AltName이 일치하는지 확인한 다음 Subject DN 속성을 시도합니다. 인증서가 디렉토리 서버의 FQDN을 사용하는 경우 이름 일치가 성공하려면 **LDAP** 서버 필드에 FQDN을 사용해야 합니다. 확인에 실패하면 연결이 실패합니다. 이 확인을 활성화하려면 **SSL/TLS** 보안 연결 필요도 선택해야 합니다.

LDAP 서버 설정	설명
	보안을 강화하기 위해 ***SSL*** 세션에 대한 서버 인증서를 확인하도록 방화벽을 활성화하십시오.

디바이스 > 서버 프로파일 > Kerberos

디바이스 > 서버 프로파일 > **Kerberos** 또는 **Panorama** > **Server** 프로파일 > **Kerberos**를 선택하여 사용자가 기본적으로 Active Directory 도메인 컨트롤러 또는 Kerberos V5 호환 인증 서버에 인증할 수 있도록 하는 서버 프로파일을 구성합니다. Kerberos 서버 프로파일을 구성한 후 이를 인증 프로파일에 할당할 수 있습니다(디바이스 > 인증 프로파일 참조). Kerberos를 사용하여 네트워크 리소스(GlobalProtect 또는 인증 포털을 통해)에 액세스하는 최종 사용자와 방화벽 또는 Panorama에 로컬로 정의된 관리자를 인증할 수 있습니다.

Kerberos 인증을 사용하려면 *IPv4* 주소를 통해 백엔드 *Kerberos* 서버에 액세스할 수 있어야 합니다. *IPv6* 주소는 지원되지 않습니다.

Kerberos 서버 설정	설명
프로파일 이름	서버를 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
관리자 전용	관리자 계정만 인증에 프로파일을 사용할 수 있도록 지정하려면 이 옵션을 선택합니다. 여러 가상 시스템이 있는 방화벽의 경우 이 옵션은 위치가 공유인 경우에만 나타납니다.
서버	각 Kerberos 서버에 대해 추가를 클릭하고 다음 설정을 지정합니다. • 이름 - 서버의 이름을 입력합니다. • **Kerberos** 서버 - 서버 IPv4 주소 또는 FQDN을 입력합니다. • 포트 - 서버와의 통신을 위한 선택적 포트(범위는 1 ~ 65,535, 기본값은 88)를 입력합니다.

디바이스 > 서버 프로파일 > SAML ID 공급자

이 페이지를 사용하여 SAML(Security Assertion Markup Language) 2.0 IdP(ID 공급자)를 방화벽 또는 Panorama에 등록하십시오. 등록은 방화벽 또는 Panorama가 네트워크 리소스에 대한 액세스를 제어하는 SAML 서비스 공급자로 작동하도록 하는 데 필요한 단계입니다. 관리자와 최종 사용자가 리소스를 요청하면 서비스 공급자는 인증을 위해 사용자를 IdP로 리디렉션합니다. 최종 사용자는 GlobalProtect 또는 인증 포털 사용자일 수 있습니다. 관리자는 방화벽 및 Panorama에서 로컬로 관리하거나 IdP ID 저장소에서 외부적으로 관리할 수 있습니다. 각 사용자가 로그인한 후 여러 리소스에 자동으로 액세스할 수 있도록 SAML SSO(Single Sign-On)를 구성할 수 있습니다. 각 사용자가 단일 서비스에서 로그아웃하여 모든 SSO 사용 서비스에서 동시에 로그아웃할 수 있도록 SAML SLO(단일 로그아웃)를 구성할 수도 있습니다.

인증 시퀀스는 *SAML IdP* 서버 프로파일을 지정하는 인증 프로파일을 지원하지 않습니다.

대부분의 경우 *SSO*를 사용하여 동일한 모바일 디바이스에서 여러 앱에 액세스할 수 없습니다.

인증 포털 사용자에 대해 *SLO*를 활성화할 수 없습니다.

SAML IdP 서버 프로파일을 만드는 가장 쉬운 방법은 IdP에서 등록 정보가 포함된 메타데이터 파일을 가져오는 것입니다. 불러온 값으로 서버 프로파일을 저장한 후 프로파일을 편집하여 값을 수정할 수 있습니다. IdP가 메타데이터 파일을 제공하지 않는 경우 서버 프로파일을 추가하고 정보를 수동으로 입력할 수 있습니다. 서버 프로파일을 만든 후 특정 방화벽 또는 Panorama 서비스에 대한 인증 프로파일(디바이스 > 인증 프로파일 참조)에 할당합니다.

SAML ID 제공자 서버 설정	설명
프로파일 이름	서버를 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	프로파일을 사용할 수 있는 범위를 선택합니다. 여러 가상 시스템이 있는 방화벽 컨텍스트에서 가상 시스템을 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
관리자 전용	관리자 계정만 인증에 프로파일을 사용할 수 있도록 지정하려면 이 옵션을 선택합니다. 여러 가상 시스템이 있는 방화벽의 경우 이 옵션은 위치가 공유인 경우에만 나타납니다.
ID 제공자 ID	IdP의 식별자를 입력합니다. IdP가 이 정보를 제공합니다.
ID 제공자 인증서	IdP가 방화벽으로 보내는 SAML 메시지에 서명하는 데 사용하는 인증서를 선택합니다. IdP가 방화벽으로 보내는 메시지의 무결성을 보장하려면 IdP 인

SAML ID 제공자 서버 설정	설명
	증서를 선택해야 합니다. 발급하는 인증 기관(CA)에 대해 IdP 인증서의 유효성을 검사하려면 IdP 서버 프로파일을 참조하는 인증 프로파일에서 인증서 프로파일을 지정해야 합니다(디바이스 > 인증 프로파일 참조). 인증서 및 관련 개인 키를 생성하거나 가져올 때 인증서에 지정된 키 사용 속성이 키를 사용할 수 있는 대상을 제어한다는 점을 기억하십시오. 인증서가 주요 사용 속성을 명시적으로 나열하는 경우 속성 중 하나는 방화벽에서 생성한 인증서에서 사용할 수 없는 디지털 서명이어야 합니다. 이 경우 엔터프라이즈 CA(인증 기관) 또는 타사 CA에서 인증서와 키를 가져와야 합니다. 인증서에 키 사용 속성이 지정되지 않은 경우 메시지 서명을 포함하여 모든 용도로 키를 사용할 수 있습니다. 이 경우 모든 방법을 사용하여 SAML 메시지 서명을 위한 인증서와 키를 얻을 수 있습니다 IdP 인증서는 다음 알고리즘을 지원합니다. • 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.
ID 제공자 SSO URL	IdP가 Single Sign-On(SSO) 서비스에 대해 광고하는 URL을 입력하십시오. 메타데이터 파일을 가져와서 서버 프로파일을 만들고 파일이 여러 SSO URL을 지정하는 경우 방화벽은 POST 또는 리디렉션 바인딩 방법을 지정하는 첫 번째 URL을 사용합니다. *SAML*도 *HTTP*를 지원하지만 *Palo Alto Networks*는 *HTTPS*에 의존하는 *URL*을 사용할 것을 강력히 권장합니다.
ID 공급자 SLO URL	IdP가 단일 로그아웃(SLO) 서비스에 대해 광고하는 URL을 입력합니다. 메타데이터 파일을 가져와서 서버 프로파일을 만들고 파일이 여러 SLO URL을 지정하는 경우 방화벽은 POST 또는 리디렉션 바인딩 방법을 지정하는 첫 번째 URL을 사용합니다. *SAML*도 *HTTP*를 지원하지만 *Palo Alto Networks*는 *HTTPS*에 의존하는 *URL*을 사용할 것을 강력히 권장합니다.
SSO SAML HTTP 바인딩	**IdP SSO URL**과 연결된 HTTP 바인딩을 선택합니다. 방화벽은 바인딩을 사용하여 SAML 메시지를 IdP에 보냅니다. 옵션은 다음과 같습니다.

SAML ID 제공자 서버 설정	설명
	• **POST** - 방화벽이 base64로 인코딩된 HTML 양식을 사용하여 메시지를 보냅니다. • 리디렉션 - 방화벽은 URL 매개변수 내에서 base64 인코딩 및 URL 인코딩 SSO 메시지를 보냅니다. 여러 *SSO URL*이 있는 *IdP* 메타데이터 파일을 가져오는 경우 방화벽은 *POST* 또는 리디렉션 방법을 사용하는 첫 번째 *URL*의 바인딩을 사용합니다. 방화벽은 다른 바인딩을 사용하는 *URL*을 무시합니다.
SLO SAML HTTP 바인딩	**IdP SLO URL**과 연결된 HTTP 바인딩을 선택합니다. 방화벽은 바인딩을 사용하여 SAML 메시지를 IdP에 보냅니다. 옵션은 다음과 같습니다. • **POST** - 방화벽이 base64로 인코딩된 HTML 양식을 사용하여 메시지를 보냅니다. • 리디렉션 - 방화벽은 URL 매개변수 내에서 base64 인코딩 및 URL 인코딩 SSO 메시지를 보냅니다. 여러 *SLO URL*이 있는 *IdP* 메타데이터 파일을 가져오는 경우 방화벽은 *POST* 또는 리디렉션 방법을 사용하는 첫 번째 *URL*의 바인딩을 사용합니다. 방화벽은 다른 바인딩을 사용하는 *URL*을 무시합니다.
ID 제공자 메타데이터	이 필드는 IdP에서 방화벽으로 업로드한 IdP 메타데이터 파일을 가져오는 경우에만 표시됩니다. 파일은 새 SAML IdP 서버 프로파일에 대한 값과 서명 인증서를 지정합니다. 파일을 찾아 프로파일 이름과 최대 클럭 스큐를 지정한 다음 확인을 클릭하여 프로파일을 만듭니다. 선택적으로 프로파일을 편집하여 불러온 값을 변경할 수 있습니다.
ID 공급자 인증서 확인	신뢰 체인을 확인하고 선택적으로 IdP 서명 인증서의 해지 상태를 확인하려면 이 옵션을 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(디바이스 > 인증 프로파일 참조). IdP 서명 인증서가 자체 서명된 인증서인 경우 트러스트 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. IdP에서 자체 서명 인증서를 제공하는

SAML ID 제공자 서버 설정	설명
	경우, CVE-2020-2021에 대한 노출을 완화하기 위해 PAN-OS 11.0을 사용해야 합니다.
IdP에 SAML 메시지 서명	방화벽이 IdP에 보내는 메시지에 서명하도록 지정하려면 이 옵션을 선택합니다. 방화벽은 인증 프로파일에서 지정한 서명 요청용 인증서를 사용합니다(디바이스 > 인증 프로파일 참조). 서명 인증서를 사용하면 *IdP*에 전송된 메시지의 무결성이 보장됩니다.
최대 클럭 스큐	방화벽이 IdP에서 수신한 메시지의 유효성을 검사하는 순간 IdP와 방화벽 시스템 시간 사이의 허용 가능한 최대 시간 차이를 초 단위로 입력합니다(범위는 1~900, 기본값은 60). 시간 차이가 이 값을 초과하면 유효성 검사(및 인증)가 실패합니다.

디바이스 > 서버 프로파일 > DNS

가상 시스템에 대한 구성을 단순화하기 위해 DNS 서버 프로파일을 사용하여 구성 중인 가상 시스템, DNS 서버의 상속 소스 또는 기본 및 보조 DNS 주소, 소스 인터페이스 및 DNS 서버로 전송되는 패킷에 사용되는 소스 주소(서비스 경로)를 지정할 수 있습니다. 소스 인터페이스와 소스 주소는 DNS 서버의 응답에서 대상 인터페이스 및 대상 주소로 사용됩니다.

DNS 서버 프로파일은 가상 시스템 전용입니다. 전역 공유 위치용이 아닙니다.

DNS 서버 프로파일 설정	설명
이름	DNS 서버 프로파일의 이름을 지정합니다.
위치	프로파일이 적용되는 가상 시스템을 선택하십시오.
상속 소스	DNS 서버 주소가 상속되지 않는 경우 없음을 선택합니다. 그렇지 않으면 프로파일이 설정을 상속해야 하는 DNS 서버를 지정합니다.
상속 소스 상태 확인	클릭하면 상속 소스 정보를 볼 수 있습니다.
기본 DNS	기본 DNS 서버의 IP 주소를 지정합니다.
보조 DNS	보조 DNS 서버의 IP 주소를 지정합니다.
서비스 경로 IPv4	DNS 서버로 가는 패킷의 출처가 IPv4 주소임을 지정하려면 이 옵션을 선택합니다.
소스 인터페이스	DNS 서버로 가는 패킷이 사용할 소스 인터페이스를 지정합니다.
소스 주소	DNS 서버로 가는 패킷이 소싱되는 IPv4 소스 주소를 지정하십시오.
서비스 경로 IPv6	DNS 서버로 가는 패킷의 출처가 IPv6 주소임을 지정하려면 이 옵션을 선택합니다.
소스 인터페이스	DNS 서버로 가는 패킷이 사용할 소스 인터페이스를 지정합니다.
소스 주소	DNS 서버로 가는 패킷이 소싱되는 IPv6 소스 주소를 지정하십시오.

디바이스 > 서버 프로파일 > 다단계 인증

이 페이지를 사용하여 방화벽이 MFA 서버에 연결하는 방법을 정의하는 MFA(다단계 인증) 서버 프로파일을 구성합니다. MFA는 공격자가 단일 인증 요소(예: 로그인 자격 증명 도용)를 손상시켜 네트워크에 액세스하고 네트워크를 통해 측면으로 이동할 수 없도록 하여 가장 민감한 리소스를 보호할 수 있습니다. 서버 프로파일을 구성한 후 인증이 필요한 서비스의 인증 프로파일에 할당합니다(디바이스 > 인증 프로파일 참조).

방화벽이 RADIUS 및 SAML을 사용하는 MFA(다단계 인증) 공급업체와 통합되는 인증 사용 사례:

- GlobalProtect™ 포털 및 게이트웨이를 통한 원격 사용자 인증.
- PAN-OS 및 Panorama™ 웹 인터페이스에서 관리자 인증.
- 인증 정책을 통한 인증.

또한 방화벽은 API를 사용하여 MFA 공급자와 통합하여 최종 사용자 인증만을 위한 인증 정책을 통해 MFA를 시행할 수도 있습니다(GlobalProtect 인증 또는 관리자 인증이 아님).

*MFA*를 구성하는 전체 절차에는 서버 프로파일을 만드는 것 외에 추가 작업이 필요합니다.

인증 시퀀스는 *MFA* 서버 프로파일을 지정하는 인증 프로파일을 지원하지 않습니다.

방화벽이 *RADIUS*를 통해 *MFA* 공급자와 통합되는 경우 *RADIUS* 서버 프로파일을 구성합니다(디바이스 > 서버 프로파일 > RADIUS 참조). 방화벽은 *RADIUS*를 통해 모든 *MFA* 공급자를 지원합니다.

MFA 서버 설정	설명
프로파일 이름	서버를 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	둘 이상의 가상 시스템(vsys)이 있는 방화벽에서 vsys 또는 공유 위치를 선택합니다. 프로파일을 저장한 후에는 위치를 변경할 수 없습니다.
인증서 프로파일	서버에 대한 보안 연결을 설정할 때 방화벽이 MFA 서버 인증서의 유효성을 검사하는 데 사용할 CA(인증 기관) 인증서를 지정하는 인증서 프로파일을 선택합니다. 자세한 내용은 디바이스 > 인증서 관리 > 인증서 프로파일을 참조하십시오.
MFA 공급자/값	**MFA** 공급자 MFA 공급자를 선택한 다음 각 공급자 속성에 대한 값을 입력합니다. 속성은 공급자에 따라 다릅니다. 올바른 값은 공급자 설명서를 참조하십시오.

MFA 서버 설정	설명

	• **Duo v2**:
	  • **API** 호스트 - Duo v2 서버의 호스트 이름입니다.
	  • 통합 키 및 비밀 키 - 방화벽은 이러한 키를 사용하여 Duo v2 서버에 인증하고 서버에 보내는 인증 요청에 서명합니다. 이러한 키를 보호하기 위해 방화벽의 마스터 키는 일반 텍스트 값이 방화벽 저장소의 어디에도 노출되지 않도록 자동으로 암호화합니다. 키를 얻으려면 Duo v2 관리자에게 문의하세요.
	  • 타임아웃 - **API** 호스트와 통신을 시도할 때 방화벽이 타임아웃되는 시간을 초 단위로 입력합니다(범위는 5~600, 기본값은 30). 이 인터벌은 API 호스트와 사용자의 엔드포인트 디바이스 사이의 타임아웃보다 길어야 합니다.
	  • 기본 **URI** - 조직에서 Duo v2 서버용 로컬 인증 프록시 서버를 호스팅하는 경우 프록시 서버 URI(기본값 /auth/v2)를 입력합니다.
	• 옥타 어댑티브:
	  • **API** 호스트 - Okta 서버의 호스트 이름입니다.
	  • 기본 **URI** - 조직에서 Okta 서버에 대한 로컬 인증 프록시 서버를 호스팅하는 경우 프록시 서버 URI(기본값 /api/v1)를 입력합니다.
	  • 토큰 - 방화벽은 이 토큰을 사용하여 Okta 서버를 인증하고 서버로 보내는 인증 요청에 서명합니다. 토큰을 보호하기 위해 방화벽의 마스터 키는 토큰을 자동으로 암호화하여 일반 텍스트 값이 방화벽 저장소의 어디에도 노출되지 않도록 합니다. 토큰을 얻으려면 Okta 관리자에게 문의하십시오.
	  • 조직 - **API** 호스트에 있는 조직의 하위 도메인입니다.
	  • 타임아웃 - **API** 호스트와 통신을 시도할 때 방화벽이 타임아웃되는 시간을 초 단위로 입력합니다(범위는 5~600, 기본값은 30). 이 인터벌은 API 호스트와 사용자의 엔드포인트 디바이스 사이의 타임아웃보다 길어야 합니다.
	• **PingID**:
	  • 기본 **URI** - 조직에서 PingID 서버에 대한 로컬 인증 프록시 서버를 호스팅하는 경우 프록시 서버 URI(기본값 /pingid/rest/4)를 입력합니다.
	  • 호스트 이름 - PingID 서버의 호스트 이름을 입력합니다(기본값 idpxnyl3m.pingidentity.com).
	  • **Base64** 키 및 토큰 사용 - 방화벽은 키와 토큰을 사용하여 PingID 서버를 인증하고 서버로 보내는 인증 요청에 서명합니다. 키와 토큰을 보호하기 위해 방화벽의 마스터 키는 일반 텍스트 값이 방화벽 저장소

MFA 서버 설정	설명
	의 어디에도 노출되지 않도록 자동으로 암호화합니다. 값을 얻으려면 PingID 관리자에게 문의하십시오. • **PingID** 클라이언트 조직 **ID** - 조직의 PingID 식별자입니다. • 타임아웃 - 호스트 이름 필드에 지정된 PingID 서버와 통신을 시도할 때 방화벽이 타임아웃되는 시간을 초 단위로 입력합니다(범위는 5~600, 기본값은 30). 이 인터벌은 PingID 서버와 사용자의 엔드포인트 디바이스 사이의 타임아웃보다 길어야 합니다.

디바이스 > 로컬 사용자 데이터베이스 > 사용자

방화벽에 로컬 데이터베이스를 설정하여 방화벽 관리자, 인증 포털 최종 사용자, GlobalProtect 포털 및 GlobalProtect 게이트웨이에 인증하는 최종 사용자에 대한 인증 정보를 저장할 수 있습니다. 로컬 데이터베이스 인증에는 외부 인증 서비스가 필요하지 않습니다. 방화벽에서 모든 계정 관리를 수행합니다. 로컬 데이터베이스를 생성하고 (선택 사항) 사용자를 그룹에 할당한 후(디바이스 > 로컬 사용자 데이터베이스 > 사용자 그룹 참조), 로컬 데이터베이스를 기반으로 디바이스 > 인증 프로파일을 할 수 있습니다.

로컬 데이터베이스 인증을 사용하는 관리 계정에 대해서는 디바이스 > 암호 프로파일을 구성할 수 없습니다.

데이터베이스에 로컬 사용자를 추가하려면 다음 표에 설명된 설정을 구성합니다.

로컬 사용자 설정	설명
이름	사용자를 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하지 않으며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	사용자 계정을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 사용자 계정을 저장한 후에는 해당 위치를 변경할 수 없습니다.
방법	이 필드를 사용하여 인증 옵션을 지정합니다. • 암호 - 사용자의 암호를 입력하고 확인합니다. • 암호 해시 - 해시된 암호 문자열을 입력합니다. 예를 들어 기존 Unix 계정의 자격 증명을 재사용하려고 하지만 일반 텍스트 암호를 모르고 해시된 암호만 모르는 경우에 유용할 수 있습니다. 방화벽은 해시 값을 생성하는 데 사용된 알고리즘에 관계없이 최대 63자의 모든 문자열을 허용합니다. 작동 CLI 명령 **`request password-hash password`**는 일반 및 CC/FIPS 모드에서 SHA256 알고리즘을 사용합니다. 방화벽(***Device*** > ***Setup*** > ***Management***)에 대해 설정한 최소 암호 복잡성 매개변수는 암호 해시를 사용하는 계정에 적용되지 않습니다.
활성화	사용자 계정을 활성화하려면 이 옵션을 선택합니다.

디바이스 > 로컬 사용자 데이터베이스 > 사용자 그룹

디바이스 > 로컬 사용자 데이터베이스 > 사용자 그룹을 선택하여 사용자 그룹 정보를 로컬 데이터베이스에 추가합니다.

로컬 사용자 그룹 설정	설명
이름	그룹을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하지 않으며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	사용자 그룹을 사용할 수 있는 범위를 선택합니다. 둘 이상의 가상 시스템(vsys)이 있는 방화벽 컨텍스트에서 vsys를 선택하거나 공유(모든 가상 시스템)를 선택합니다. 다른 컨텍스트에서는 위치를 선택할 수 없습니다. 해당 값은 Shared(방화벽) 또는 Panorama로 사전 정의됩니다. 사용자 그룹을 저장한 후에는 위치를 변경할 수 없습니다.
모든 로컬 사용자	추가를 클릭하여 그룹에 추가할 사용자를 선택합니다.

디바이스 > 예약된 로그 내보내기

로그 내보내기를 예약하고 파일 전송 프로토콜(FTP) 서버에 CSV 형식으로 저장하거나 보안 복사(SCP)를 사용하여 방화벽과 원격 호스트 간에 데이터를 안전하게 전송할 수 있습니다. 로그 프로파일에는 일정 및 FTP 서버 정보가 포함됩니다. 예를 들어, 프로파일은 전날의 로그가 매일 오전 3시에 수집되어 특정 FTP 서버에 저장되도록 지정할 수 있습니다.

추가를 클릭하고 다음 세부 정보를 입력합니다.

예약된 로그 내보내기 설정	설명
이름	프로파일을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. 프로파일을 만든 후에는 이름을 변경할 수 없습니다.
설명	선택적 설명을 입력합니다(최대 255자).
활성화	로그 내보내기 예약을 활성화하려면 이 옵션을 선택합니다.
로그 유형	로그 유형(트래픽, 위협, **gtp**, **sctp**, 터널, **User-ID**, 인증, **URL**, 데이터, **hipmatch** 또는 **wildfire**)을 선택합니다. 기본값은 트래픽입니다.
예정된 내보내기 시작 시간(일일)	24시간제(00:00 - 23:59)를 사용하여 내보내기를 시작하려면 시간(hh:mm)을 입력합니다.
프로토콜	방화벽에서 원격 호스트로 로그를 내보내는 데 사용할 프로토콜을 선택하십시오. • **FTP** - 이 프로토콜은 안전하지 않습니다. • **SCP** - 이 프로토콜은 안전합니다. 나머지 필드를 완료한 후 **SCP** 서버 연결 테스트를 클릭하여 방화벽과 SCP 서버 간의 연결을 테스트하고 SCP 서버의 호스트 키를 확인하고 수락해야 합니다.
호스트 이름	내보내기에 사용할 FTP 서버의 호스트 이름 또는 IP 주소를 입력합니다.
포트	FTP 서버가 사용할 포트 번호를 입력합니다. 기본값은 21입니다.
경로	내보낸 정보를 저장하는 데 사용할 FTP 서버에 있는 경로를 지정합니다.

예약된 로그 내보내기 설정	설명
FTP 수동 모드 활성화	내보내기에 수동 모드를 사용하려면 이 옵션을 선택합니다. 기본적으로 이 옵션이 선택되어 있습니다.
사용자명	FTP 서버에 액세스하기 위한 사용자명을 입력합니다. 기본값은 익명입니다.
비밀번호 / 비밀번호 확인	FTP 서버에 액세스하기 위한 암호를 입력합니다. 사용자가 익명인 경우 암호가 필요하지 않습니다.
SCP 서버 연결 테스트 (SCP 프로토콜만 해당)	프로토콜을 **SCP**로 설정한 경우 방화벽과 SCP 서버 간의 연결을 테스트하려면 이 버튼을 클릭해야 합니다. SCP 서버 일반 텍스트 비밀번호를 입력한 다음 비밀번호 확인을 입력하라는 팝업 창이 표시됩니다. *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.

디바이스 > 소프트웨어

디바이스 > 소프트웨어를 선택하여 사용 가능한 소프트웨어 릴리스를 보고, 릴리스를 다운로드 또는 업로드하고, 릴리스를 설치하고(지원 라이선스 필요), 방화벽에서 소프트웨어 이미지를 삭제하거나, 릴리스 정보를 봅니다.

소프트웨어 버전을 업그레이드하거나 다운그레이드하기 전:

- 현재 릴리스 정보를 검토하여 릴리스의 새 기능 및 기본 동작에 대한 변경 사항에 대한 설명을 확인하고 소프트웨어 업그레이드를 위한 마이그레이션 경로를 확인하십시오.
- 업그레이드 및 다운그레이드 고려 사항과 업그레이드 지침은 PAN-OS® 11.0 새 기능 가이드에서 확인할 수 있습니다.
- 방화벽의 날짜 및 시간 설정이 최신인지 확인하십시오. PAN-OS 소프트웨어는 디지털 서명되며 방화벽은 새 버전을 설치하기 전에 서명을 확인합니다. 방화벽의 날짜 및 시간 설정이 최신이 아니고 방화벽이 소프트웨어 서명이 현 시점 이후(오류)인 것으로 인식하면 다음 메시지가 표시됩니다.

```
## ## ##: 0# ## GnuPG ##, ## 171072 ## PAN ##### #### #### #####.
```

다음 표는 소프트웨어 페이지 사용에 대한 도움말을 제공합니다.

소프트웨어 옵션 필드	설명
버전	Palo Alto Networks 업데이트 서버에서 현재 사용할 수 있는 소프트웨어 버전을 나열합니다. Palo Alto Networks에서 새 소프트웨어 릴리스를 사용할 수 있는지 확인하려면 지금 확인을 클릭하십시오. 방화벽은 서비스 경로를 사용하여 업데이트 서버에 연결하고 새 버전을 확인하고 사용 가능한 업데이트가 있는 경우 목록의 맨 위에 표시합니다.
크기	소프트웨어 이미지의 크기를 나타냅니다.
출시일	Palo Alto Networks에서 릴리스를 제공한 날짜와 시간을 나타냅니다.
사용 가능	해당 버전의 소프트웨어 이미지가 방화벽에 업로드 또는 다운로드되었음을 나타냅니다.
현재 설치됨	소프트웨어 이미지의 해당 버전이 활성화되어 있고 현재 방화벽에서 실행 중인지의 여부를 나타냅니다.
작업	다음과 같이 해당 소프트웨어 이미지에 대해 수행할 수 있는 현재 작업을 나타냅니다. • 유효성 검사 - 해당 소프트웨어 버전을 Palo Alto Networks 업데이트 서버에서 사용할 수 있습니다. 업데이트 서버 또는 SCP 서버에서 사용 가

소프트웨어 옵션 필드	설명
	능한 소프트웨어 버전과 해당 소프트웨어 또는 콘텐츠 종속성을 다운로드하려면 클릭합니다. • 설치 - 해당 소프트웨어 버전이 방화벽에 다운로드되거나 업로드되었습니다. 소프트웨어를 설치하려면 클릭하십시오. 업그레이드 프로세스를 완료하려면 재부팅이 필요합니다. • 재설치 - 해당 소프트웨어 버전이 이전에 설치되었습니다. 동일한 버전을 다시 설치하려면 클릭하십시오.
릴리즈 노트	해당 소프트웨어 업데이트에 대한 릴리스 정보에 대한 링크를 제공합니다. 이 링크는 Palo Alto Networks 업데이트 서버에서 다운로드한 업데이트에만 사용할 수 있습니다. 업로드된 업데이트에는 사용할 수 없습니다.
	방화벽에서 이전에 다운로드하거나 업로드한 소프트웨어 이미지를 제거합니다. 업그레이드가 필요하지 않은 이전 릴리스의 기본 이미지만 삭제하려고 합니다. 예를 들어, 10.1을 실행 중인 경우 다운그레이드가 필요하지 않다면 10.0의 기본 이미지를 제거할 수 있습니다.
지금 확인	Palo Alto Networks에서 새 소프트웨어 업데이트를 사용할 수 있는지 확인합니다. 소프트웨어 업데이트를 확인하는 데 어려움이 있습니까? 일반적인 연결 문제에 대한 해결 방법은 이 문서를 참조하십시오.
업로드	방화벽이 액세스할 수 있는 컴퓨터에서 소프트웨어 업데이트 이미지를 가져옵니다. 일반적으로 방화벽에 인터넷 액세스 권한이 없는 경우 이 작업을 수행합니다. 이는 Palo Alto Networks 업데이트 서버에서 업데이트를 다운로드할 때 필요합니다. 업로드의 경우 인터넷에 연결된 컴퓨터를 사용하여 Palo Alto Networks 웹사이트를 방문하고 지원 사이트(소프트웨어 업데이트)에서 소프트웨어 이미지를 다운로드하고 컴퓨터에 업데이트를 다운로드하고 방화벽에서 **Device** > **Software**를 선택한 다음 소프트웨어 이미지를 업로드합니다. 고가용성(HA) 구성에서 **Sync To Peer**를 선택하여 불러온 소프트웨어 이미지를 HA 피어로 푸시할 수 있습니다. 업로드 후 소프트웨어 페이지에는 업로드 및 다운로드된 소프트웨어에 대한 동일한 정보(예: 버전 및 크기)와 설치/재설치 옵션이 표시됩니다. 릴리스 정보 옵션은 업로드된 소프트웨어에 대해 활성화되지 않습니다.

디바이스 > 동적 업데이트

- 디바이스 > 동적 업데이트
- Panorama > 동적 업데이트

Palo Alto Networks는 동적 업데이트를 통해 신규 및 수정된 애플리케이션, 위협 보호, IoT 보안용 장치 사전 파일 및 GlobalProtect 데이터 파일을 포함하는 업데이트를 정기적으로 게시합니다. 방화벽은 이러한 업데이트를 검색하여 구성 변경 없이 정책을 시행하는 데 사용할 수 있습니다. 애플리케이션 및 일부 바이러스 백신 업데이트는 구독 없이 사용할 수 있습니다. 다른 것은 귀하의 구독에 연결과 관련이 있습니다.

최신 업데이트를 보고 각 업데이트의 릴리스 정보를 읽은 다음 다운로드하여 설치할 업데이트를 선택할 수 있습니다. 이전에 설치된 업데이트 버전으로 되돌릴 수도 있습니다.

동적 업데이트 일정을 설정하면 방화벽이 새 업데이트를 확인하고 다운로드하거나 설치하는 빈도를 정의할 수 있습니다. 특히 애플리케이션 및 위협 콘텐츠 업데이트의 경우 위협 업데이트 뒤에 새 애플리케이션 업데이트와 수정된 애플리케이션 업데이트를 시차를 두는 일정을 설정할 수 있습니다. 이렇게 하면 방화벽이 항상 최신 위협 보호 기능을 갖추도록 하는 동시에 신규 및 수정된 애플리케이션이 보안 정책에 미치는 영향을 평가할 시간이 더 많이 주어집니다.

동적 업데이트 옵션	설명
버전	현재 Palo Alto Networks 업데이트 서버에서 사용 가능한 버전을 나열합니다. Palo Alto Networks에서 새 소프트웨어 릴리스를 사용할 수 있는지 확인하려면 지금 확인을 클릭하십시오. 방화벽은 서비스 경로를 사용하여 업데이트 서버에 연결하고 새 콘텐츠 릴리스 버전을 확인하고 사용 가능한 업데이트가 있는 경우 목록 맨 위에 표시합니다.
마지막 확인	방화벽이 업데이트 서버에 마지막으로 연결하고 업데이트가 사용 가능한지 확인한 날짜와 시간을 표시합니다.
일정	업데이트 검색 빈도를 예약할 수 있습니다. 동적 콘텐츠 업데이트가 발생하는 빈도와 시기(반복 및 시간)와 다운로드 전용 또는 예약 업데이트 다운로드 및 설치 여부를 정의할 수 있습니다. 바이러스 백신 및 애플리케이션 및 위협 업데이트의 경우 방화벽이 설치하기 전에 콘텐츠 업데이트를 사용할 수 있어야 하는 최소 임계값을 설정할 수 있는 옵션이 있습니다. 매우 드물게 콘텐츠 업데이트에 오류가 있을 수 있으며 이 임계값은 방화벽이 지정된 시간 동안 고객 환경에서 사용 가능하고 작동하는 콘텐츠 릴리스만 다운로드하도록 합니다. 애플리케이션 및 위협 콘텐츠 업데이트의 경우 신규 및 수정된 애플리케이션의 콘텐츠 업데이트에 특별히 적용되는 임계값을 설정할 수도 있습니다. 확장된 애플리케이션 임계값은 신규 또는 수정된 애플리케이션이

동적 업데이트 옵션	설명
	도입하는 변경 사항을 기반으로 보안 정책을 평가하고 조정할 더 많은 시간을 제공합니다. WildFire 업데이트의 경우 실시간으로 서명을 검색할 수 있는 옵션이 있어 서명이 생성되는 즉시 액세스할 수 있습니다. 샘플 검사 중에 다운로드된 서명은 방화벽 캐시에 저장되며 빠른(로컬) 조회에 사용할 수 있습니다. 또한 적용 범위를 최대화하기 위해 방화벽은 실시간 서명이 활성화된 경우 정기적으로 추가 서명 패키지를 자동으로 다운로드합니다. 이러한 보완 서명은 방화벽 캐시에 추가되며 부실해지고 새로 고쳐지거나 새 서명으로 덮어쓸 때까지 계속 사용할 수 있습니다. 지속적인 애플리케이션 가용성과 최신 위협 보호를 모두 달성하기 위해 애플리케이션 및 위협 콘텐츠 업데이트를 가장 잘 활성화하는 방법에 대한 지침은 애플리케이션 및 위협 업데이트에 대한 모범 사례를 검토하십시오.
파일 이름	파일 이름을 나열하십시오. 콘텐츠 버전 정보가 포함됩니다.
특징	콘텐츠 버전에 포함될 수 있는 서명 유형을 나열합니다. 애플리케이션 및 위협 콘텐츠 릴리스 버전의 경우 이 필드에 앱, 위협을 검토하는 옵션이 표시될 수 있습니다. 방화벽에 설치된 마지막 콘텐츠 릴리스 버전 이후에 사용할 수 있는 새 애플리케이션 서명을 보려면 이 옵션을 클릭합니다. 새 애플리케이션 대화 상자를 사용하여 새 애플리케이션을 활성화/비활성화할 수도 있습니다. 고유하게 식별되는 애플리케이션으로 인한 정책 영향을 방지하려면 콘텐츠 릴리스에 포함된 새 애플리케이션을 비활성화하도록 선택할 수 있습니다(이전에 알려지지 않은 애플리케이션이 식별되고 다르게 분류된 경우 애플리케이션은 콘텐츠 설치 전후에 다르게 처리될 수 있습니다.). 디바이스 사전의 경우 이 필드는 *IoT* 보안의 줄임말인 **IoT**이며, 이는 디바이스 ID에 기반한 보안 정책 규칙의 정확한 시행에서 중요한 구성요소로 디바이스 사전을 사용하는 클라우드 보안 서비스입니다.
유형	다운로드에 전체 데이터베이스 업데이트 또는 증분 업데이트가 포함되는지의 여부를 나타냅니다.
크기	콘텐츠 업데이트 패키지의 크기를 표시합니다.
SHA256	파일의 무결성을 확인하는 데 사용되는 체크섬입니다.
출시일	Palo Alto Networks에서 콘텐츠 릴리스를 제공한 날짜 및 시간입니다.

동적 업데이트 옵션	설명
다운로드됨	이 열의 확인 표시는 해당 콘텐츠 릴리스 버전이 방화벽에 다운로드되었음을 나타냅니다.
현재 설치됨	이 열의 확인 표시는 해당 콘텐츠 릴리스 버전이 현재 방화벽에서 실행되고 있음을 나타냅니다.
동작	다음과 같이 해당 소프트웨어 이미지에 대해 수행할 수 있는 현재 작업을 나타냅니다. • 다운로드 - 해당 콘텐츠 릴리스 버전은 Palo Alto Networks 업데이트 서버에서 사용할 수 있습니다. 콘텐츠 릴리스 버전을 다운로드하려면 클릭하세요. 방화벽이 인터넷에 액세스할 수 없는 경우 인터넷에 연결된 컴퓨터를 사용하여 고객 지원 포털로 이동하고 동적 업데이트를 선택합니다. 원하는 콘텐츠 릴리스 버전을 찾고 다운로드를 클릭하여 업데이트 패키지를 로컬 컴퓨터에 저장합니다. 그런 다음 방화벽에 소프트웨어 이미지를 수동으로 업로드합니다. 또한 애플리케이션 및 위협 콘텐츠 릴리스 버전을 다운로드하면 릴리스에 포함된 새 애플리케이션 서명의 영향을 받는 정책을 검토하는 옵션이 활성화됩니다. • 정책 검토(애플리케이션 및 위협 콘텐츠만 해당) - 콘텐츠 릴리스 버전에 포함된 새 애플리케이션에 대한 정책 영향을 검토합니다. 이 옵션을 사용하여 콘텐츠 업데이트를 설치하기 전후에 애플리케이션이 받는 처리를 평가합니다. 정책 검토 대화 상자를 사용하여 보류 중인 애플리케이션(콘텐츠 릴리스 버전과 함께 다운로드되지만 방화벽에 설치되지 않은 애플리케이션)을 기존 보안 정책 규칙에 추가하거나 제거할 수도 있습니다. 보류 중인 애플리케이션에 대한 정책 변경 사항은 해당 콘텐츠 릴리스 버전이 설치될 때까지 적용되지 않습니다. • 앱 검토(애플리케이션 및 위협 콘텐츠만 해당)—방화벽에 설치된 마지막 콘텐츠 릴리스 버전 이후 사용 가능해진 신규 및 수정된 애플리케이션 서명을 봅니다. 콘텐츠 업데이트가 중요한 애플리케이션의 시행에 영향을 미칠 수 있는 변경 사항을 도입하는 경우 해당 애플리케이션은 정책 검토를 위해 권장되는 것으로 표시됩니다. 정책 검토를 클릭하여 콘텐츠 업데이트가 기존 보안 정책에 미치는 영향을 확인하거나 애플리케이션의 정책 영향을 검토할 시간이 될 때까지 애플리케이션을 비활성화할 수 있습니다. • 설치 - 해당 콘텐츠 릴리스 버전이 방화벽에 다운로드되었습니다. 업데이트를 설치하려면 클릭하십시오. 새 애플리케이션 및 위협 콘텐츠 릴리스 버전을 설치할 때 콘텐츠 업데이트에서 새 앱 비활성화 옵션이 표시됩니다. 이 옵션은 최신 위협으로부터 보호하는 동시에 새로운 애플리케이션 서명의 영향으로 인해 정책 업데이트를 준비한 후 애플리케이션을 활성화할 수 있는 유연성을 제공합니다(이전에 비활성화한

동적 업데이트 옵션	설명
	애플리케이션을 활성화하려면 동적 업데이트 페이지에서 앱, 위협 선택 또는 개체 > 애플리케이션 선택). • 되돌리기 - 해당 콘텐츠 릴리스 버전이 이전에 다운로드되었습니다. 동일한 버전을 다시 설치하려면 되돌리기를 클릭합니다.
문서화	해당 버전의 릴리스 정보에 대한 링크를 제공합니다.
	방화벽에서 이전에 다운로드한 콘텐츠 릴리스 버전을 제거합니다.
업로드	방화벽이 Palo Alto Networks 업데이트 서버에 액세스할 수 없는 경우 동적 업데이트 섹션의 Palo Alto Networks 지원 사이트에서 동적 업데이트를 수동으로 다운로드할 수 있습니다. 컴퓨터에 업데이트를 다운로드한 후 방화벽에 업데이트를 업로드합니다. 그런 다음 파일에서 설치를 선택한 다음 다운로드한 파일을 선택합니다.
파일에서 설치	업데이트 파일을 방화벽에 수동으로 업로드한 후 이 옵션을 사용하여 파일을 설치합니다. 패키지 유형 드롭다운에서 설치할 업데이트 유형(애플리케이션 및 위협 요소, 바이러스 백신 또는 **WildFire**)을 선택한 다음 확인을 클릭하고 설치할 파일을 선택한 다음 확인을 다시 클릭하여 설치를 시작합니다.

디바이스 > 라이선스

모든 방화벽 모델에서 라이선스를 활성화하려면 디바이스 > 라이선스를 선택합니다. Palo Alto Networks에서 구독을 구매하면 하나 이상의 라이선스 키를 활성화하기 위한 인증 코드를 받게 됩니다.

VM 시리즈 방화벽에서 이 페이지에서는 VM(가상 머신)을 비활성화할 수도 있습니다.

라이선스 페이지에서는 다음 작업을 수행할 수 있습니다.

- 라이선스 서버에서 라이선스 키 검색: 인증 코드가 필요하고 지원 포털에서 활성화된 구매한 구독을 활성화하려면 선택합니다.
- 인증 코드를 사용하여 기능 활성화: 인증 코드가 필요하고 지원 포털에서 이전에 활성화된 적이 없는 구매한 구독을 활성화하려면 선택합니다. 그런 다음 인증 코드를 입력하고 확인을 클릭합니다.
- 수동으로 라이선스 키 업로드: 방화벽이 라이선스 서버에 연결되어 있지 않고 라이선스 키를 수동으로 업로드하려는 경우 https://support.paloaltonetworks.com에서 라이선스 키 파일을 다운로드하고 로컬에 저장합니다. 수동으로 라이선스 키 업로드를 클릭하고 찾아보기를 클릭하고 파일을 선택한 다음 확인을 클릭합니다.

  > *URL* 필터링에 대한 라이선스를 활성화하려면 라이선스를 설치하고 데이터베이스를 다운로드한 다음 활성화를 클릭해야 합니다. *URL* 필터링에 *PAN-DB*를 사용하는 경우 초기 시드 데이터베이스를 먼저 다운로드한 다음 활성화해야 합니다.
  >
  > *CLI* 명령 ***request url-filtering download paloaltonetworks region <regionname>***을 실행할 수도 있습니다.

- **VM** 비활성화: 이 옵션은 영구 라이선스 및 기간 기반 라이선스를 지원하는 BYOD(Bring Your Own License) 모델이 있는 VM 시리즈 방화벽에서 사용할 수 있습니다. 주문형 라이선스 모델은 이 기능을 지원하지 않습니다. VM 시리즈 방화벽의 인스턴스가 더 이상 필요하지 않으면 **VM** 비활성화를 클릭합니다. 이 옵션을 사용하면 모든 활성 라이선스(구독 라이선스, VM-Capacity 라이선스 및 지원 권한)를 확보할 수 있습니다. 라이선스는 계정에 다시 적립되며 필요할 때 VM 시리즈 방화벽의 새 인스턴스에 라이선스를 적용할 수 있습니다. 라이선스가 비활성화되면 VM 시리즈 방화벽 기능이 비활성화되고 방화벽은 라이선스가 없는 상태가 됩니다. 그러나 구성은 그대로 유지됩니다.
  - VM 시리즈 방화벽이 인터넷에 직접 액세스할 수 없는 경우 수동으로 계속을 클릭합니다. 방화벽은 토큰 파일을 생성합니다. 라이선스 토큰 내보내기를 클릭하여 토큰 파일을 로컬 컴퓨터에 저장한 다음 방화벽을 재부팅하십시오. Palo Alto Networks 지원 포털에 로그인하고 **Assets** > **Devices**를 선택한 다음 **VM** 비활성화를 선택하여 이 토큰 파일을 사용하고 비활성화 프로세스를 완료합니다.
  - 계속을 클릭하여 VM 시리즈 방화벽에서 라이선스를 비활성화합니다. 지금 재부팅을 클릭하여 라이선스 비활성화 프로세스를 완료합니다.
  - 취소하고 VM 비활성화 창을 닫으려면 취소를 클릭합니다.

- **VM** 용량 업그레이드: 이 옵션을 사용하면 현재 라이선스가 부여된 VM 시리즈 방화벽의 용량을 업그레이드할 수 있습니다. 용량을 업그레이드하면 VM 시리즈 방화벽은 업그레이드 이전의 모든 구성 및 구독을 유지합니다.
  - 방화벽이 라이선스 서버에 연결되어 있는 경우 - 인증 코드를 선택한 다음 인증 코드 필드에 인증 코드를 입력한 다음 계속을 클릭하여 용량 업그레이드를 시작합니다.
  - 방화벽이 라이선스 서버에 연결되어 있지 않은 경우 - 라이선스 키를 선택한 다음 수동으로 완료를 클릭하여 토큰 파일을 생성하고 토큰 파일을 로컬 컴퓨터에 저장합니다. 그런 다음 Palo Alto Networks 지원 포털에 로그인하고 **Assets** > **Devices**를 선택한 다음 **Deactivate License(s)**를 선택하여 토큰 파일을 사용합니다. VM 시리즈 방화벽의 라이선스 키를 로컬 컴퓨터에 다운로드하고 방화벽에 라이선스 키를 추가한 다음 계속을 클릭하여 용량 업그레이드를 완료합니다.
  - 방화벽이 라이선스 서버에 연결되어 있지만 인증 코드가 없는 경우 - 라이선스 서버에서 가져오기를 선택한 다음, 용량 업그레이드를 시도하기 전에 라이선스 서버에서 방화벽의 용량 라이선스를 업그레이드한 다음 라이선스가 다음과 같은지 확인한 후에 라이선스 서버에서 업그레이드한 경우 계속을 클릭하여 용량 업그레이드를 시작합니다.

디바이스 > 지원

- 디바이스 > 지원
- Panorama > 지원

지원 관련 옵션에 액세스하려면 **Device** > **Support** 또는 **Panorama** > **Support**를 선택합니다. 방화벽의 일련번호를 기반으로 Palo Alto Networks 연락처 정보, 지원 만료 날짜, 제품 및 보안 경고를 볼 수 있습니다.

이 페이지에서 다음 기능 중 하나를 수행합니다.

- 지원 - 디바이스의 지원 상태에 대한 정보를 제공하고 인증 코드를 사용하여 지원을 활성화하는 링크를 제공합니다.
- 프로덕션 알림/애플리케이션 및 위협 알림 - 이 알림은 이 페이지에 액세스/새로 고침할 때 Palo Alto Networks 업데이트 서버에서 검색됩니다. 프로덕션 경고 또는 애플리케이션 및 위협 경고의 세부 정보를 보려면 경고 이름을 클릭합니다. 특정 릴리스와 관련된 대규모 리콜 또는 긴급 문제가 있는 경우 생산 경고가 게시됩니다. 중대한 위협이 발견되면 애플리케이션 및 위협 경고가 게시됩니다.
- 링크 - 디바이스를 관리하고 지원 연락처 정보에 액세스하는 데 도움이 되는 공통 지원 링크를 제공합니다.
- 기술 지원 파일 - 기술 지원 파일 생성을 클릭하여 지원 팀이 방화벽에서 발생할 수 있는 문제를 해결하는 데 사용할 수 있는 시스템 파일을 생성합니다. 파일을 생성한 후 기술 지원 파일을 다운로드한 다음 Palo Alto Networks 지원 부서로 보내십시오.

  브라우저가 다운로드 후 파일을 자동으로 열도록 구성된 경우 브라우저가 지원 파일을 열고 압축을 풀지 않고 다운로드하도록 해당 옵션을 꺼야 합니다.
- 통계 덤프 파일 - 통계 덤프 파일 생성을 클릭하여 지난 7일 동안의 네트워크 트래픽을 요약하는 XML 보고서 세트를 생성합니다. 보고서가 생성된 후 통계 덤프 파일을 다운로드할 수 있습니다. Palo Alto Networks 또는 공인 파트너 시스템 엔지니어는 보고서를 사용하여 SLR(보안 수명 주기 검토)을 생성합니다. SLR은 네트워크에서 발견된 사항과 존재할 수 있는 관련 비즈니스 또는 보안 위험을 강조하며 일반적으로 평가 프로세스의 일부로 사용됩니다. SLR에 대한 자세한 내용은 Palo Alto Networks 또는 공인 파트너 시스템 엔지니어에게 문의하십시오.

  Panorama™ 관리 서버에서 관리하는 방화벽의 경우 한 번에 단일 관리 방화벽에 대한 통계 덤프 파일을 생성하거나 Panorama에서 관리하는 모든 방화벽에 대해 단일 통계 덤프 파일을 생성할 수 있습니다.
- 코어 파일 - 방화벽에서 시스템 프로세스 오류가 발생하면 프로세스와 실패한 이유에 대한 세부 정보가 포함된 코어 파일이 생성됩니다. 코어 파일 다운로드 링크를 클릭하여 사용 가능한 코어 파일 목록을 본 다음 코어 파일 이름을 클릭하여 다운로드하십시오. 파일을 다운로드한 후 Palo Alto Networks 지원 사례에 업로드하여 문제 해결에 대한 지원을 받으십시오.

  코어 파일의 내용은 *Palo Alto Networks* 지원 엔지니어만 해석할 수 있습니다.
- 디버그 및 관리 **Pcap** 파일 - 방화벽에서 패킷 캡처 실패가 발생하면 실패한 이유에 대한 디버그 및 관리 세부 정보가 포함된 패킷 캡처(pcap) 파일을 생성합니다. 디버그 및 관리 **Pcap** 파일 다운로드를 클릭하

여 사용 가능한 pcap 파일 목록을 확인한 다음 pcap 파일 이름을 클릭하여 다운로드합니다. 파일을 다운로드한 후 Palo Alto Networks 지원 사례에 업로드하여 문제 해결에 대한 지원을 받으십시오.

디바이스 > 마스터 키 및 진단

- 디바이스 > 마스터 키 및 진단
- **Panorama** > 마스터 키 및 진단

방화벽 또는 Panorama의 모든 비밀번호와 개인 키를 암호화하는 마스터 키(예: CLI에 액세스하는 관리자를 인증하기 위한 RSA 키)를 편집하십시오. 암호 및 키를 암호화하면 일반 텍스트 값이 방화벽이나 Panorama의 어느 곳에서도 노출되지 않도록 하여 보안이 향상됩니다.

기본 마스터 키를 복원하는 유일한 방법은 공장 초기화를 수행하는 것입니다.

Palo Alto Networks는 기본 키를 사용하는 대신 새 마스터 키를 구성하고, 키를 안전한 위치에 저장하고, 주기적으로 변경할 것을 권장합니다. 추가 개인 정보 보호를 위해 하드웨어 보안 모듈을 사용하여 마스터 키를 암호화할 수 있습니다(디바이스 > 설정 > HSM 참조). 각 방화벽 또는 Panorama 관리 서버에서 고유한 마스터 키를 구성하면 한 어플라이언스의 마스터 키를 알게 된 공격자가 다른 어플라이언스의 비밀번호와 개인 키에 액세스할 수 없습니다. 그러나 다음과 같은 경우 여러 어플라이언스에서 동일한 마스터 키를 사용해야 합니다.

- 고가용성**(HA)** 구성 - HA 구성에서 방화벽 또는 Panorama를 배포하는 경우 쌍의 두 방화벽 또는 Panorama 관리 서버에서 동일한 마스터 키를 사용합니다. 그렇지 않으면 HA 동기화가 작동하지 않습니다.
- **WildFire** 어플라이언스 및 로그 수집기를 관리하는 **Panorama** - Panorama, WildFire 어플라이언스 및 관리되는 수집기에서 동일한 마스터 키를 구성해야 합니다. 그렇지 않으면 Panorama에서 푸시 작업이 실패합니다.

마스터 키를 구성하려면 마스터 키 설정을 편집하고 다음 표를 사용하여 적절한 값을 결정하십시오.

마스터 키 및 진단 설정	설명
마스터 키	고유한 마스터 키를 구성하려면 활성화합니다. 기본 마스터 키를 사용하려면 비활성화(지우기)합니다.
현재 마스터 키	방화벽에서 모든 개인 키와 암호를 암호화하는 데 현재 사용되는 키를 지정하십시오.
새 마스터 키 마스터 키 확인	마스터 키를 변경하려면 16자 문자열을 입력하고 새 키를 확인합니다.
수명	마스터 키가 만료되는 날짜 및 시간을 지정합니다. 범위는 1~438,000일(50년)입니다. 현재 키가 만료되기 전에 새 마스터 키를 구성해야 합니다. 마스터 키가 만료되면 방화벽 또는 Panorama가 유지 관

마스터 키 및 진단 설정	설명
	리 모드에서 자동으로 재부팅됩니다. 그런 다음 공장 초기화 를 수행해야 합니다. 디바이스가 수행하는 암호화 수에 따라 수명을 *2*년 이하로 설정합니다. 디바이스가 수행하는 암호화가 많을수록 수명을 짧게 설정해야 합니다. 중요한 고려 사항은 마스터 키를 변경하기 전에 고유한 암호화가 부족하지 않도록 하는 것입니다. 각 마스터 키는 최대 *2^32*개의 고유한 암호화를 제공한 다음 암호화를 반복하므로 보안 위험이 있습니다. 마스터 키에 대한 알림 시간을 설정하고 미리 알림이 발생하면 마스터 키를 변경합니다.
알림 시간	방화벽이 만료 알람을 생성할 때 마스터 키가 만료되기 전의 일 수와 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 대해 미리 알림 값이 만료되면 마스터 키를 변경합니다. 만료 알람이 표시되도록 하려면 ***Device*** > ***Log*** 설정을 선택한 다음 알람 설정을 편집하고 알람을 활성화합니다.
HSM에 저장됨	마스터 키가 HSM(하드웨어 보안 모듈)에서 암호화된 경우에만 이 옵션을 활성화하십시오. DHCP 클라이언트 또는 PPPoE와 같은 동적 인터페이스에서는 HSM을 사용할 수 없습니다. HSM 구성은 HA 모드에서 피어 방화벽 간에 동기화되지 않습니다. 따라서 HA 쌍의 각 피어는 다른 HSM 소스에 연결할 수 있습니다. Panorama를 사용 중이고 두 피어 구성을 동기화 상태로 유지해야 하는 경우 Panorama 템플릿을 사용하여 관리되는 방화벽에서 HSM 소스를 구성하십시오. PA-220은 HSM을 지원하지 않습니다.
자동 갱신 마스터 키	지정된 날짜 및 시간 동안 마스터 키를 자동으로 갱신하려면 활성화합니다. 구성된 키 수명 후에 마스터 키가 만료되도록 하려면 비활성화(지우기)합니다.

마스터 키 및 진단 설정	설명
	마스터 키 암호화를 연장할 날짜 및 시간을 지정하여 동일한 마스터 키로 자동 갱신합니다(범위는 1시간에서 730일까지). 자동 갱신 마스터 키를 활성화하는 경우 총 시간(수명 + 자동 갱신 시간)으로 인해 디바이스의 고유한 암호화가 소진되지 않도록 설정하십시오. 예를 들어 디바이스가 마스터 키의 고유 암호화 수를 2년 반 동안 소비한다고 생각되면 2년 동안 수명을 설정하고 미리 알림 시간을 60일로 설정하고 자동 갱신 마스터 키를 60-90일로 설정하여 수명이 만료되기 전에 새 마스터 키를 구성하는 추가 시간을 제공할 수 있습니다. 그러나 가장 좋은 방법은 디바이스가 암호화를 반복하지 않도록 수명이 만료되기 전에 마스터 키를 변경하는 것입니다.
공통 기준	Common Criteria 모드에서는 암호화 알고리즘 자체 테스트 및 소프트웨어 무결성 자체 테스트를 실행하기 위한 추가 옵션을 사용할 수 있습니다. 두 개의 자체 테스트가 실행되는 시간을 지정하는 스케줄러도 포함되어 있습니다.

마스터 키 배포

Panorama에서 직접 마스터 키를 배포하거나 관리 방화벽, Log Collector 또는 WF-500 어플라이언스의 기존 마스터 키를 업데이트합니다.

필드	설명
마스터 키 배포	
필터	플랫폼, 디바이스 그룹, 템플릿, 태그, HA 상태 또는 소프트웨어 버전을 기반으로 표시할 관리 디바이스를 필터링합니다.
디바이스 이름	관리되는 방화벽의 이름입니다.
소프트웨어 버전	관리되는 디바이스에서 실행 중인 소프트웨어 버전입니다.
상태	관리되는 디바이스의 연결 상태: ###, ## ### 또는 # # ##일 수 있습니다.
마스터 키 작업 상태 배포	

필드	설명
디바이스 이름	관리되는 방화벽의 이름입니다.
상태	마스터 키 배포 작업의 상태입니다.
결과	마스터 키 배포 작업의 결과입니다. OK 또는 FAIL일 수 있습니다.
진행	마스터 키 배포 작업의 진행률(%)입니다.
세부	마스터 키 배포 작업에 대한 세부정보입니다. 작업이 실패한 경우 실패한 이유를 설명하는 세부 정보가 여기에 표시됩니다.
요약	
진행	마스터 키 배포 작업의 진행률을 나타내는 진행률 표시줄을 표시합니다. 다음 정보가 표시됩니다. • 결과 성공 - 마스터 키가 성공적으로 배포된 디바이스의 수입니다. • 결과 보류 중 - 마스터 키 배포 작업이 현재 보류 중인 디바이스의 수입니다. • 결과 실패 - 마스터 키 배포 작업이 실패한 디바이스의 수입니다.

디바이스 > 정책 권장사항 > IoT

IoT 보안의 정책 규칙 권장 사항에 대한 정보를 확인합니다. IoT 보안은 방화벽이 네트워크의 트래픽에서 수집하는 메타데이터를 사용하여 디바이스에 허용할 동작을 결정한 다음 적용할 보안 정책 규칙에 대한 권장 사항을 생성합니다.

버튼/필드	설명
정책 가져오기 세부정보	디바이스 그룹 위치, 규칙 이름, 정책을 불러온 사용자, 정책 규칙 권장 사항이 업데이트되었는지의 여부, 정책 규칙 권장 사항을 불러온 시간 및 정책 규칙 권장 사항이 마지막으로 업데이트된 시간과 같은 정책 규칙 권장 사항에 대한 자세한 정보를 봅니다.
Imported to	차세대 방화벽의 경우 정책 규칙 권장 사항을 가져온 가상 시스템이 표시됩니다. Panorama의 경우 정책 규칙 권장 사항을 가져온 디바이스 그룹이 표시됩니다.
정책 규칙 이름	정책 규칙의 이름으로, 기본적으로 IoT 보안 정책 세트 이름과 애플리케이션 이름을 연결한 것입니다.
제안된 디바이스 그룹	IoT 보안이 차세대 방화벽에서 수신한 로그에서 영역 및 디바이스 그룹을 학습한 후 정책 규칙으로 제안한 디바이스 그룹입니다.
소스 디바이스 프로필	정책 규칙 권장 사항에서 트래픽을 허용하는 디바이스 프로필입니다.
소스 영역	정책 규칙 권장 사항에서 트래픽을 허용하는 소스 영역입니다. 소스 영역은 IoT 보안에서 수동으로 추가할 수 있습니다.
소스 사용자	정책 규칙 권장 사항의 소스 사용자입니다. 이는 사용되지 않으며 항상 비어 있습니다.
소스 디바이스	정책 규칙 권장 사항에 대한 소스 디바이스입니다. 이는 사용되지 않으며 항상 비어 있습니다.
소스 주소	정책 규칙 권장 사항의 소스 주소입니다. 이는 사용되지 않으며 항상 비어 있습니다.

버튼/필드	설명
대상 디바이스 프로파일	정책 규칙 권장 사항에서 트래픽을 허용하는 대상 디바이스 프로필입니다.
대상 디바이스 IP	정책 규칙 권장 사항에서 트래픽을 허용하는 디바이스의 IP 주소입니다.
대상 FQDN	정책 규칙 권장 사항에서 트래픽을 허용하는 FQDN(정규화된 도메인 이름)입니다.
목적지 영역	정책 규칙 권장 사항에서 트래픽을 허용하는 대상 영역입니다. 대상 영역은 IoT 보안에서 수동으로 추가할 수 있습니다.
대상 보안 프로필	정책 규칙 권장 사항에서 허용하는 보안 프로필입니다.
대상 서비스	정책 규칙 권장 사항이 허용하는 서비스(예: `ssl`)입니다.
대상 URL 범주	정책 규칙 권장 사항에서 트래픽을 허용하는 URL 필터링 범주입니다.
대상 애플리케이션	정책 규칙 권장 사항이 허용하는 애플리케이션입니다.
대상 태그	정책 규칙 권장 사항의 정책 규칙을 식별하는 태그입니다. 정책 규칙의 태그를 변경하지 마십시오. 태그를 변경하면 방화벽이 정책 매핑을 재구축할 수 없습니다.
설명	규칙이 속한 정책 세트에 대한 IoT 보안의 설명입니다.
내부 디바이스	디바이스가 네트워크 내부 영역에 속하는지(#) 또는 외부 인터넷 연결 영역에 속하는지(###) 식별합니다.
동작	이 정책 규칙 권장 사항에 대한 작업을 식별하며, 기본값은 항상 ##입니다.

버튼/필드	설명
새 업데이트 사용 가능	# 는 규칙 베이스의 해당 규칙에 사용할 수 있는 정책 규칙 권장 사항에 대한 업데이트가 있음을 나타냅니다. (Panorama) Panorama에서 정책 규칙을 가져오면 현재 규칙 권장 사항과 규칙 베이스에서 이전에 가져온 해당 규칙을 덮어씁니다. 이를 수행하면 새 업데이트 사용 가능 필드가 더 이상 보류 중인 업데이트가 있음을 나타내지 않으며 #에서 ###로 변경됩니다. 디바이스 그룹이 두 개 이상인 경우 모든 디바이스 그룹에 정책 규칙을 가져올 때까지 값은 #로 유지됩니다. (PAN-OS UI) 새 업데이트 사용 가능 열에 #가 있는 정책 규칙 권장 사항의 세부 정보를 기록한 다음 업데이트된 정책 규칙 권장 사항과 일치하도록 정책 페이지에서 가져온 해당 정책 규칙을 편집하고 저장합니다. 그런 다음 정책 규칙 동기화를 통해 수정된 규칙과 규칙 권장 사항 간의 매핑을 새로 고칩니다. 새 업데이트 사용 가능 열의 값이#에서###로 변경됩니다.
이 방화벽만 보기	IoT 보안은 활성화된 모든 정책 세트의 규칙을 Panorama와 모든 차세대 방화벽에 자동으로 푸시합니다. 따라서 방화벽에는 적용되지 않는 일부 규칙이 있을 수 있습니다. 로컬 방화벽에 적용되는 규칙만 표시하려면 이 방화벽만 보기를 선택합니다.
정책 규칙 가져오기	IoT 보안이 정책 규칙 권장 사항을 Panorama 또는 방화벽에 푸시하고 정책 권장 사항 데이터베이스에 있으면 정책 규칙 기반으로 가져올 하나 이상(최대 10개)을 선택한 다음 정책 규칙 가져오기를 클릭할 수 있습니다. 표시되는 정책 규칙 가져오기 대화 상자에서 선택한 정책 규칙을 나중에 가져오려면 규칙 베이스의 정책 규칙 이름을 선택하거나 선택한 규칙을 맨 위로 가져오려면 해당 이름을 비워 둡니다. 정책 규칙 권장 사항을 규칙 베이스로 가져온 다음 나중에 IoT 보안에서 수정하면 Panorama를 사용하여 다시 가져올 수 있습니다. PAN-OS UI에서는 규칙을 다시 가져올 수 없으므로 Panorama를 사용하거나 PAN-OS 규칙 베이스에서 규칙을 편집하여 수정된 권장 사항과 일치하도록 한 다음 정책 규칙 동기화를 수행할 수 있습니다.

버튼/필드	설명
정책 매핑 제거	하나 이상의 정책 규칙 권장 사항이 더 이상 필요하지 않은 경우 한 번에 최대 10개의 권장 사항을 선택한 다음 정책 매핑 제거할 수 있습니다. 그런 다음 규칙 베이스에서 해당 규칙을 수동으로 삭제할 수 있습니다.
동기화 정책 규칙	매핑이 동기화되지 않은 경우(예: 이전 구성을 복원하는 경우) 정책 규칙 동기화를 수행하여 규칙 베이스의 정책 규칙과 정책 규칙 권장 사항 간의 매핑을 복원할 수 있습니다.

디바이스 > 정책 > 추천 SaaS

Prisma SaaS에서 정책 규칙 권장 사항에 대한 정보를 보고 정책을 방화벽으로 가져옵니다.

필드	설명
소스 사용자	정책 규칙 권장 사항을 방화벽에 보낸 관리자입니다.
소스 디바이스	정책 규칙 권장 사항에 대한 소스 디바이스입니다.
위치	이 정책 규칙 권장 사항을 사용할 수 있는 Panorama의 디바이스 그룹입니다.
보안 프로파일	정책 규칙 권장 사항이 허용하는 보안 프로파일입니다.
애플리케이션	정책 규칙 권장 사항이 허용하는 애플리케이션 또는 애플리케이션 그룹입니다. 애플리케이션 그룹 이름을 클릭하면 해당 그룹의 개별 애플리케이션을 볼 수 있습니다.
태그	정책 규칙 권장 사항에 대한 정책 규칙을 식별하는 태그입니다. 정책 규칙의 태그를 변경하지 마십시오. 태그를 변경하면 방화벽이 정책 매핑을 다시 작성할 수 없습니다.
설명	Prisma SaaS 관리자가 정책 규칙 권장 사항에 제공하는 설명입니다.
활성 권장 사항	이 정책 규칙 권장 사항이 적합한지의 여부를 식별합니다. • ## - 현재 Prisma SaaS 보안 정책에서 사용됩니다. • ### - Prisma SaaS 관리자가 정책에서 제거했습니다. 방화벽 관리자는 더 이상 정책 규칙을 가져올 수 없으며 방화벽에서 정책 매핑을 제거한 다음 방화벽 규칙 베이스에서 보안 정책 규칙을 제거해야 합니다. 방화벽 규칙 베이스에 제거된 규칙을 그대로 두지 마십시오.

필드	설명
동작	이 정책 규칙 권장 사항에 대한 작업(## 또는 ##)을 식별합니다.
새로운 업데이트 사용 가능	정책 규칙 권장 사항에 대한 새 업데이트가 있음을 식별합니다. 애플리케이션 변경 사항에 대한 애플리케이션 열을 확인하십시오. 변경 사항에 동의하면 규칙 및 정책 규칙 가져오기를 선택하여 정책을 업데이트합니다. Prisma SaaS에서 가져와야 합니다. 정책 규칙 권장 사항 업데이트를 가져오면 방화벽이 보안 정책 규칙 및 관련 개체를 동적으로 업데이트합니다.
정책 규칙 가져오기	Prisma SaaS에서 선택한 정책 규칙 권장 사항을 가져옵니다.
정책 매핑 제거	디바이스에 대한 정책 규칙 권장 사항이 더 이상 필요하지 않은 경우 해당 디바이스에 대한 정책 매핑을 제거할 수 있습니다. 정책 규칙 권장 사항에 해당하는 정책 규칙도 삭제해야 합니다.
동기화 정책 규칙	SaaS 관리자가 정책 권장 사항을 제거하고 이에 대한 정책 매핑을 제거하고 보안 정책 규칙을 삭제하면 정보가 동기화되지 않은 경우 제거된 규칙이 규칙 권장 사항 목록에 남아 있을 수 있습니다. 동기화 정책 규칙을 사용하여 동기화합니다.

사용자 식별

User-ID(User-ID™)는 다양한 엔터프라이즈 디렉토리 및 터미널 서비스와 원활하게 통합되어 애플리케이션 활동과 정책을 IP 주소가 아닌 사용자명 및 그룹에 연결하는 Palo Alto Networks® 차세대 방화벽 기능입니다. User-ID를 구성하면 ACC(Application Command Center), 앱 범위, 보고서 및 로그에 사용자 IP 주소 외에 사용자명이 포함될 수 있습니다.

- 디바이스 > 사용자 식별 > 사용자 매핑
- 디바이스 > 사용자 식별 > 연결 보안
- 디바이스 > 사용자 식별 > 터미널 서버 에이전트
- 디바이스 > 사용자 식별 > 그룹 매핑 설정
- 디바이스 > 사용자 식별 > 신뢰할 수 있는 소스 주소
- 디바이스 > 사용자 식별 > 인증 포털 설정
- 디바이스 > 사용자 식별 > Cloud Identity Engine

더 찾고 계십니까**?**

User-ID 참조

디바이스 > 사용자 식별 > 사용자 매핑

방화벽에서 실행되는 PAN-OS 통합 User-ID 에이전트를 구성하여 IP 주소를 사용자명에 매핑합니다.

무엇을 찾고 계신가요?	참조:
PAN-OS 통합 User-ID 에이전트를 구성합니다.	Palo Alto Networks User-ID 에이전트 설정
User-ID 에이전트가 사용자 매핑 정보를 모니터링하는 서버에 대한 액세스를 관리합니다.	모니터 서버
IP 주소를 사용자명에 매핑할 때 방화벽이 포함하거나 제외하는 하위 네트워크를 관리합니다.	사용자 매핑을 위한 하위 네트워크 포함 또는 제외
더 찾고 계십니까?	PAN-OS IntegratedUser-IDAgent를 사용하여 사용자 매핑을 구성합니다

Palo Alto Networks User-ID 에이전트 설정

이러한 설정은 User-ID 에이전트가 사용자 매핑을 수행하는 데 사용하는 방법을 정의합니다.

무엇을 찾고 계신가요?	참조:
User-ID 에이전트가 WMI(Windows Management Instrumentation)를 사용하여 클라이언트 시스템을 검토하거나 HTTP 또는 HTTPS를 통한 WinRM(Windows 원격 관리)을 사용하여 사용자 매핑 정보에 대해 서버를 모니터링할 수 있도록 합니다.	서버 모니터 계정
User-ID 에이전트를 사용하여 사용자 매핑 정보에 대한 서버 로그를 모니터링합니다.	서버 모니터링

무엇을 찾고 계신가요?	참조:
사용자 매핑 정보에 대해 클라이언트 시스템을 검토하도록 User-ID 에이전트를 활성화합니다.	클라이언트 프로빙
사용자가 로밍하고 새 IP 주소를 얻을 때 방화벽에 최신 사용자 매핑 정보가 있는지 확인합니다.	캐시
사용자 매핑 정보에 대한 syslog 메시지를 구문 분석하도록 User-ID 에이전트를 구성합니다.	시스템 로그 필터
매핑 프로세스에서 특정 사용자명을 생략하도록 User-ID 에이전트를 구성합니다.	사용자 목록 무시

서버 모니터 계정

- 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 서버 모니터 계정

PAN-OS 통합 User-ID 에이전트가 클라이언트 시스템을 검토하기 위해 WMI(Windows Management Instrumentation)를 사용하거나 HTTP 또는 HTTPS를 통해 Windows 원격 관리(WinRM)를 사용하여 사용자 매핑 정보에 대해 서버를 모니터링하도록 구성하려면 다음 필드를 완료하십시오.

또한 HTTP 또는 HTTPS를 통해 WinRM(Windows 원격 관리)을 사용하여 서버 모니터링을 인증하도록 Kerberos 서버를 구성하여 모니터링되는 서버에 대한 액세스 구성을(를) 할 수 있습니다.

WMI 프로빙은 엔드포인트에서 다시 보고되는 데이터를 신뢰하기 때문에 *Palo Alto Network*는 보안 수준이 높은 네트워크에서 *User-ID* 매핑 정보를 얻기 위해 이 방법을 사용하지 않을 것을 권장합니다. *Active Directory(AD)* 보안 이벤트 로그 또는 *syslog* 메시지를 구문 분석하거나 *XML API*를 사용하여 매핑 정보를 얻도록 *User-ID* 에이전트를 구성하는 경우 *Palo Alto Networks*는 *WMI* 프로빙을 비활성화할 것을 권장합니다.

WMI 검색을 사용하는 경우 외부의 신뢰할 수 없는 인터페이스에서 활성화하지 마십시오. 이렇게 하면 에이전트가 *User-ID* 에이전트 서비스 계정의 사용자명, 도메인 이름 및 암호 해시와 같은 민감한 정보가 포함된 *WMI* 프로브를 네트워크 외부로 보냅니다. 공격자는 잠재적으로 이 정보를 악용하여 네트워크에 침투하여 추가 액세스 권한을 얻을 수 있습니다.

Active Directory 인증 설정	설명
사용자명	방화벽이 Windows 리소스에 액세스하는 데 사용할 계정의 도메인 자격 증명(사용자명 및 암호)을 입력합니다. 계정에는 클라이언트 컴퓨터에서 WMI 쿼리를 수행하고 Microsoft Exchange 서버 및 도메인 컨트롤러를 모니터링할 수 있는 권한이 필요합니다. 사용자명에 domain

Active Directory 인증 설정	설명
	\username 구문을 사용하십시오. 서버 인증에 Kerberos를 사용하는 모니터링되는 서버에 대한 액세스 구성 경우 Kerberos UPN(사용자 계정 이름)을 입력합니다.
도메인의 DNS 이름	모니터링되는 서버의 DNS 이름을 입력합니다. 서버 인증에 Kerberos를 사용하는 경우 모니터링되는 서버에 대한 액세스 구성 Kerberos 영역 도메인을 입력합니다. 모니터링되는 서버에 대한 액세스 구성을(를) 수행할 때 **WinRM-HTTP**를 전송 프로토콜로 사용하는 경우 이 설정을 구성해야 합니다.
비밀번호/비밀번호 확인	방화벽이 Windows 리소스에 액세스하는 데 사용하는 계정의 암호를 입력하고 확인합니다.
Kerberos 서버 프로파일	영역에 대한 액세스를 제어하는 Kerberos 서버에 대한 Kerberos 서버 프로파일을 선택하여 HTTP 또는 HTTPS를 통해 WinRM을 사용하여 모니터링되는 서버에서 보안 로그 및 세션 정보를 검색합니다.

서버 및 프로브 클라이언트를 모니터링하도록 *PAN-OS* 통합 *User-ID* 에이전트를 구성하는 전체 절차에는 *Active Directory* 인증 설정을 정의하는 것 외에 추가 작업이 필요합니다.

서버 모니터링

- 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 서버 모니터

User-ID 에이전트가 서버의 보안 이벤트 로그에서 로그온 이벤트를 검색하여 IP 주소를 사용자명에 매핑할 수 있도록 하려면 다음 표에 설명된 설정을 구성합니다.

Windows 서버 로그, *Windows* 서버 세션 또는 *eDirectory* 서버에 대한 쿼리 로드가 높으면 쿼리 간에 관찰된 지연이 지정된 빈도 또는 인터벌을 크게 초과할 수 있습니다.

서버를 모니터링하도록 *PAN-OS* 통합 *User-ID* 에이전트를 구성하는 전체 절차에는 서버 모니터링 설정을 구성하는 것 외에 추가 작업이 필요합니다.

서버 모니터링 설정	설명
보안 로그 활성화	Windows 서버에서 보안 로그 모니터링을 활성화하려면 이 옵션을 선택합니다.
서버 로그 모니터 빈도(초)	방화벽이 Windows 서버 보안 로그에서 사용자 매핑 정보를 쿼리하는 빈도를 초 단위로 지정합니다(범위는 1-3600, 기본값은 2). 이것은 방화벽이 마지막 쿼리 처리를 완료하고 방화벽이 다음 쿼리를 보내는 시간 사이의 인터벌입니다.

서버 모니터링 설정	설명
	로그 모니터링이 자주 발생하지 않으면 최신 *IP* 주소-사용자 매핑을 사용하지 못할 수 있습니다. 방화벽이 로그를 너무 자주 모니터링하면 도메인 컨트롤러, 메모리, *CPU* 및 *User-ID* 정책 시행에 영향을 줄 수 있습니다. *2-30*초 범위의 값으로 시작한 다음 성능 영향 또는 사용자 매핑이 업데이트되는 빈도에 따라 값을 수정합니다.
세션 활성화	모니터링되는 서버에서 사용자 세션 모니터링을 활성화하려면 이 옵션을 선택합니다. 사용자가 서버에 연결할 때마다 세션이 생성됩니다. 방화벽은 이 정보를 사용하여 사용자 IP 주소를 식별할 수 있습니다. 세션을 활성화하지 마십시오. 이 설정을 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*와 같은 모든 디바이스 유형 및 운영 체제*(Windows* 운영 체제 대신*)*에 대한 로그인 및 로그아웃 이벤트를 캡처하는 소스를 모니터링해야 합니다.
서버 세션 읽기 빈도(초)	방화벽이 Windows 서버 사용자 세션에서 사용자 매핑 정보를 쿼리하는 빈도를 초 단위로 지정합니다(범위는 1-3600, 기본값은 10). 이것은 방화벽이 마지막 쿼리 처리를 완료하고 다음 쿼리를 시작하는 시간 사이의 인터벌입니다.
Novell eDirectory 쿼리 인터벌(초)	방화벽이 Novell eDirectory 서버에 사용자 매핑 정보를 쿼리하는 빈도를 초 단위로 지정합니다(범위는 1-3600, 기본값은 30). 이것은 방화벽이 마지막 쿼리 처리를 완료하고 다음 쿼리를 시작하는 시간 사이의 인터벌입니다.
Syslog 서비스 프로파일	인증서를 지정하는 SSL/TLS 서비스 프로파일을 선택한 다음 방화벽과 User-ID 에이전트가 모니터링하는 모든 syslog 발신자 간의 통신에 허용되는 SSL/TLS 버전을 선택합니다. 자세한 내용은 디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일 및 Syslog 필터를 참조하십시오. 없음을 선택하면 방화벽은 사전 정의된 자체 서명 인증서를 사용합니다.

클라이언트 프로빙

- 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 클라이언트 프로빙

올바르게 구성되지 않으면 보안 위험을 초래할 수 있으므로 높은 수준의 보안 네트워크 또는 외부의 신뢰할 수 없는 인터페이스에서 클라이언트 검색을 활성화하지 마십시오. 외부의 신뢰할 수 없는 영역에서 클라이언트 검토를 활성화하면 공격자가 네트워크 외부로 검토를 보내 *User-ID* 에이전트 서비스 계정 이름, 도메인 이름 및 암호화된 암호 해시가 공개될 수 있습니다.

대신, *Palo Alto Network*는 도메인 컨트롤러 또는 Syslog 또는 XML API와의 통합과 같은 분리되고 신뢰할 수 있는 소스에서 사용자 매핑 정보를 수집하여 모든 디바이스 유형 또는 운영 체제에서 사용자 매핑 정보를 안전하게 캡처할 것을 강력히 권장합니다.

사용자 매핑 프로세스가 식별하는 각 클라이언트 시스템에 대해 WMI(Windows Management Instrumentation) 클라이언트 검색을 수행하도록 PAN-OS 통합 User-ID 에이전트를 구성할 수 있습니다. User-ID 에이전트는 각 학습된 IP 주소를 주기적으로 검토하여 동일한 사용자가 여전히 로그인되어 있는지 확인합니다. 방화벽이 사용자 매핑이 없는 IP 주소를 발견하면 즉각적인 검토를 위해 해당 주소를 User-ID 에이전트에 보냅니다. 클라이언트 검색 설정을 구성하려면 다음 필드를 완료하십시오. 클라이언트를 검토하도록 PAN-OS 통합 User-ID 에이전트를 구성하는 전체 절차에는 WMI 클라이언트 검토 설정을 구성하는 것 외에 추가 작업이 필요합니다.

클라이언트 검토 설정	설명
프로빙 활성화	WMI 프로빙을 활성화하려면 이 옵션을 선택합니다.
프로브 인터벌(분)	프로브 인터벌을 분 단위로 입력합니다(범위는 1-1440, 기본값은 20). 이것은 방화벽이 마지막 요청을 처리하고 다음 요청을 시작할 때 사이의 인터벌입니다. 대규모 배포에서는 사용자 매핑 프로세스가 식별한 각 클라이언트를 검토할 시간을 허용하도록 인터벌을 적절하게 설정하는 것이 중요합니다. 예를 들어 사용자가 6,000명이고 인터벌이 10분이면 각 클라이언트에서 초당 10개의 WMI 요청이 필요합니다. 프로브 요청 로드가 높으면 요청 간에 관찰된 지연이 지정한 인터벌을 크게 초과할 수 있습니다.

캐시

- 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 캐시

사용자가 로밍하고 새 IP 주소를 얻을 때 방화벽에 최신 사용자 매핑 정보가 있는지 확인하려면 방화벽 캐시에서 사용자 매핑을 지우기 위한 타임아웃을 구성하십시오. 이 타임아웃은 인증 포털을 제외한 모든 방법을 통해 학습된 사용자 매핑에 적용됩니다. 인증 포털을 통해 학습된 매핑의 경우 인증 포털 설정(디바이스 > 사용자 식별 > 인증 포털 설정, 타이머 및 유휴 타이머 필드)에서 타임아웃을 설정합니다.

도메인이 포함되지 않은 경우에도 User-ID 소스에서 수집된 사용자명을 일치시키려면 도메인 없이 일치하는 사용자명을 허용하도록 방화벽을 구성하십시오. 조직의 사용자명이 도메인 간에 중복되지 않는 경우에만 이 옵션을 사용해야 합니다.

캐시 설정	설명
사용자 식별 타임아웃 활성화	사용자 매핑 항목에 대한 타임아웃 값을 활성화하려면 이 옵션을 선택합니다. 항목에 대한 타임아웃 값에 도달하면 방화벽이 항목을 지우고 새 매핑을 수집합니다. 이렇게 하면 사용자가 로밍하고 새 IP 주소를 얻을 때 방화벽이 최신 정보를 갖게 됩니다. 방화벽에 최신 사용자 대 *IP* 주소 매핑 정보가 있는지 확인하려면 타임아웃을 활성화하십시오.
사용자 식별 타임아웃(분)	사용자 매핑 항목에 대한 타임아웃 값을 분 단위로 설정합니다(범위는 1 - 3,600, 기본값은 45). 타임아웃 값을 *DHCP* 리스의 반감기 또는 *Kerberos* 티켓 유효 시간으로 설정합니다. 매핑 정보를 재배포하도록 방화벽을 구성하는 경우 각 방화벽은 포워딩 방화벽에 설정된 타임아웃이 아니라 해당 방화벽에 설정한 타임아웃을 기반으로 수신하는 매핑 항목을 지웁니다.
도메인 없이 일치하는 사용자명 허용	도메인이 User-ID 소스에서 제공되지 않은 경우 방화벽이 사용자와 일치하도록 허용하려면 이 옵션을 선택합니다. 사용자가 잘못 식별되는 것을 방지하려면 사용자명이 여러 도메인에서 중복되지 않는 경우에만 이 옵션을 선택하십시오. 이 옵션을 활성화하기 전에 방화벽이 *LDAP* 서버에서 그룹 매핑을 가져왔는지 확인하십시오.

시스템 로그 필터

- 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 시스템 로그 필터

User-ID 에이전트는 Syslog 구문 분석 프로파일을 사용하여 에이전트가 IP 주소-사용자명 매핑 정보에 대해 모니터링하는 syslog 발신자가 보낸 syslog 메시지를 필터링합니다(모니터링되는 서버에 대한 액세스 구성 참조). 각 프로파일은 다음 이벤트 유형 중 하나에 대한 syslog 메시지를 구문 분석할 수 있지만 둘 다 구문 분석할 수는 없습니다.

- 인증(로그인) 이벤트 - 방화벽에 사용자 매핑을 추가하는 데 사용됩니다.
- 로그아웃 이벤트 - 더 이상 최신이 아닌 사용자 매핑을 삭제하는 데 사용됩니다. 오래된 매핑을 삭제하면 IP 주소 할당이 자주 변경되는 환경에서 유용합니다.

Palo Alto Networks는 애플리케이션 콘텐츠 업데이트를 통해 사전 정의된 Syslog Parse 프로파일을 방화벽에 제공합니다. 공급자가 새 필터를 개발할 때 프로파일 목록을 동적으로 업데이트하려면 이러한 동적 콘텐츠 업데이트를 예약하십시오(디바이스 > 동적 업데이트 참조). 사전 정의된 프로파일은 방화벽 전체에 적용되는 반면 구성한 사용자 지정 프로파일은 **Device** > **User Identification** > **User Mapping**에서 선택한 가상 시스템(위치)에만 적용됩니다.

Syslog 메시지는 User-ID 에이전트가 메시지를 구문 분석하려면 다음 기준을 충족해야 합니다.

- 각 메시지는 한 줄의 텍스트 문자열이어야 합니다. 줄 바꿈(\n) 또는 캐리지 리턴과 새 라인(\r\n)은 줄 바꿈의 구분 기호입니다.
- 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.

사용자 지정 프로파일을 구성하려면 추가를 클릭하고 다음 표에 설명된 설정을 지정합니다. 이 표의 필드 설명은 다음 형식의 syslog 메시지의 로그인 이벤트 예를 사용합니다.

```
[Tue July 5 13:15:04 2005 CDT] ### ## ## ###:domain\johndoe_4
 Source:192.168.0.212
```

사용자 매핑 정보에 대해 *syslog* 발신자를 구문 분석하도록 *User-ID* 에이전트를 구성하는 전체 절차에는 *Syslog* 구문 분석 프로파일을 만드는 것 외에 추가 작업이 필요합니다.

필드	설명
Syslog 구문 분석 프로파일	프로파일 이름을 입력합니다(최대 63자의 영숫자).
설명	프로파일에 대한 설명을 입력합니다(최대 255자의 영숫자).
유형	사용자 매핑 정보를 필터링하기 위한 구문 분석 유형을 지정합니다. • 정규식 식별자 - 이벤트 정규식, 사용자명 정규식 및 주소 정규식을 사용하여 syslog 메시지에서 사용자 매핑 정보를 식별하고 추출하기 위한 검색 패턴을 설명하는 정규식(regex)을 지정합니다. 방화벽은 정규식을 사용하여 syslog 메시지의 인증 또는 로그아웃 이벤

필드	설명
	트를 일치시키고 일치하는 메시지 내의 사용자명과 IP 주소를 일치시킵니다. • 필드 식별자 - 이벤트 문자열, 사용자명 프리픽스, 사용자명 구분 기호, 주소 프리픽스, 주소 구분 기호 및 로그당 주소 필드를 사용하여 인증 또는 로그아웃 이벤트를 일치시키고 syslog 메시지에서 사용자 매핑 정보를 식별하기 위한 문자열을 지정합니다. 대화 상자의 나머지 필드는 선택 항목에 따라 다릅니다. 다음 행에 설명된 대로 필드를 구성합니다.
이벤트 정규식	성공적인 인증 또는 로그아웃 이벤트를 식별하기 위한 정규식을 입력합니다. 이 테이블에 사용된 예제 메시지의 경우 정규식 **(authentication\ success) {1}**은 문자열 ## ##의 첫 번째 **{1}** 인스턴스를 추출합니다. 공백 앞의 백슬래시는 공백을 특수 문자로 취급하지 않도록 정규식 엔진에 지시하는 표준 정규식 확장 문자입니다.
사용자명 정규식	인증 성공 또는 로그아웃 메시지에서 사용자명 필드를 식별하기 위한 정규식을 입력합니다. 이 테이블에 사용된 예제 메시지의 경우 정규식 **User:([a-zA-Z0-9\\\._]+)**는 문자열 User:johndoe_4와 일치하고 acme\johndoe1을 사용자명으로 추출합니다.
주소 정규식	인증 성공 또는 로그아웃 메시지의 IP 주소 부분을 식별하는 정규식을 입력합니다. 이 테이블에 사용된 예제 메시지에서 정규식 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\ .[0-9]{1,3})** IPv4 주소 Source:192.168.0.212와 일치하고 사용자명 매핑의 IP 주소로 192.168.0.212를 추가합니다.
이벤트 문자열	인증 성공 또는 로그아웃 메시지를 식별하기 위해 일치하는 문자열을 입력하십시오. 이 테이블과 함께 사용되는 예제 메시지의 경우 **##** **##** 문자열을 입력합니다.
사용자명 프리픽스	인증 또는 로그아웃 syslog 메시지 내에서 사용자명 필드의 시작을 식별하기 위해 일치하는 문자열을 입력합니다. 필드는 **\s**(공백의 경우) 또는 **\t**(탭의 경우)와 같은 정규식을 지원하지 않습니다. 이 테이블에 사용된 예제 메시지에서 **###:**는 사용자명 필드의 시작을 식별합니다.
사용자명 구분 기호	인증 또는 로그아웃 메시지 내에서 사용자명 필드의 끝을 표시하는 구분 기호를 입력하십시오. 독립형 공간을 나타내려면 \s를 사용하고(예제 메시지에서와 같이) 탭을 나타내려면 \t를 사용하십시오.

필드	설명
주소 프리픽스	syslog 메시지에서 IP 주소 필드의 시작을 식별하기 위해 일치하는 문자열을 입력하십시오. 필드는 **\s**(공백의 경우) 또는 **\t**(탭의 경우)와 같은 정규식을 지원하지 않습니다. 이 테이블과 함께 사용된 예제 메시지에서 `Source:`는 주소 필드의 시작을 식별합니다.
주소 구분자	인증 성공 또는 로그아웃 메시지 내에서 IP 주소 필드의 끝을 표시하는 일치하는 문자열을 입력하십시오. 예를 들어 구분 기호가 줄 바꿈임을 나타내려면 **\n**을 입력합니다.
로그당 주소	방화벽이 구문 분석할 최대 IP 주소 수를 입력합니다(기본값은 1, 범위는 1~3).

사용자 목록 무시

- 디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 사용자 목록 무시

사용자 무시 목록은 IP 주소-사용자명 매핑이 필요하지 않은 사용자 계정(예: 키오스크 계정)을 정의합니다. 목록을 구성하려면 추가를 클릭하고 사용자명을 입력합니다. 별표를 와일드카드 문자로 사용하여 여러 사용자명과 일치시킬 수 있지만 항목의 마지막 문자로만 사용할 수 있습니다. 예를 들어, **corpdomain\it-admin***은 사용자명이 **it-admin** 문자열로 시작하는 **corpdomain** 도메인의 모든 관리자와 일치합니다. 사용자 매핑에서 제외할 항목을 최대 5,000개까지 추가할 수 있습니다.

클라이언트가 아닌 *User-ID* 에이전트인 방화벽에 사용자 무시 목록을 정의합니다. 클라이언트 방화벽에서 사용자 무시 목록을 정의하는 경우 목록의 사용자는 재배포 중에 계속 매핑됩니다.

모니터 서버

- 디바이스 > 사용자 식별 > 사용자 매핑

서버 모니터링 섹션을 사용하여 User-ID 에이전트가 로그인 이벤트에 대해 모니터링하는 Microsoft Exchange Server, Active Directory(AD) 도메인 컨트롤러, Novell eDirectory 서버 또는 syslog 발신자를 정의합니다.

- 모니터링되는 서버에 대한 액세스 구성
- 모니터링되는 서버에 대한 액세스 관리
- 사용자 매핑을 위한 하위 네트워크 포함 또는 제외

모니터링되는 서버에 대한 액세스 구성

서버 모니터링 섹션을 사용하여 방화벽이 모니터링할 서버를 지정하는 서버 프로파일을 추가합니다.

서버가 다운되더라도 방화벽이 여전히 *IP* 주소와 사용자 이름 간 매핑을 학습할 수 있도록 최소한 *2*개의 *User-ID* 모니터링 서버를 구성합니다.

서버를 모니터링하도록 *PAN-OS* 통합 *User-ID* 에이전트를 구성하는 전체 절차에는 서버 프로파일 생성 외에 추가 작업이 필요합니다.

서버 모니터링 설정	설명
이름	서버 이름을 입력합니다.
설명	서버에 대한 설명을 입력합니다.
활성화됨	이 서버에 대한 로그 모니터링을 활성화하려면 이 옵션을 선택합니다.
유형	서버 유형을 선택합니다. 선택에 따라 이 대화 상자가 표시할 다른 필드가 결정됩니다. • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • 시스템 로그 발신자
전송 프로토콜(Microsoft Active Directory 및 Microsoft Exchange만 해당)	전송 프로토콜 선택: • **WMI** - (기본값) WMI(Windows Management Instrumentation)를 사용하여 학습된 각 IP 주소를 검토하고 동일한 사용자가 여전히 로그인되어 있는지 확인합니다. • **WinRM-HTTP** - HTTP를 통한 Windows 원격 관리(WinRM)를 사용하여 서버의 보안 로그 및 세션 정보를 모니터링합니다. 방화벽은 Kerberos 세션 키를 사용하여 페이로드를 암호화합니다. • **WinRM-HTTPS** - HTTPS를 통한 WinRM(Windows 원격 관리)을 사용하여 서버의 보안 로그 및 세션 정보를 모니터링합니다. Kerberos 인증을 사용할 때 Windows 서버에서 서버 인증서 유효성 검사를 요구하려면 글로벌 서비스 설정에서 NTP를 구성하고 루트 CA를 인증서 프로파일로 선택해야 합니다(디바이스 > 사용자 식별 > 연결 보안).
네트워크 주소	모니터링되는 서버의 서버 IP 주소 또는 FQDN을 입력합니다. 서버 인증에 Kerberos를 사용하는 경우 FQDN을 입력해야 합니다. 유형이 **Novell eDirectory**인 경우 이 옵션이 지원되지 않습니다.

서버 모니터링 설정	설명
서버 프로파일 (Novell eDirectory만 해당)	Novell eDirectory 서버에 연결할 LDAP 서버 프로파일을 선택합니다(디바이스 > 서버 프로파일 > LDAP).
연결 타입 (Syslog 발신자만 해당)	User-ID 에이전트가 **UDP** 포트(514) 또는 **SSL** 포트(6514)에서 syslog 메시지를 수신할지의 여부를 선택합니다. **SSL**을 선택하면 서버 모니터링을 활성화할 때 선택한 **Syslog** 서비스 프로파일에 따라 허용되는 SSL/TLS 버전과 방화벽이 syslog 발신자에 대한 연결을 보호하는 데 사용하는 인증서가 결정됩니다. 보안 모범 사례로 *PAN-OS* 통합 *User-ID* 에이전트를 사용하여 *IP* 주소를 사용자명에 매핑할 때 ***SSL***을 선택하십시오. ***UDP***를 선택하는 경우 신뢰할 수 없는 호스트가 *UDP* 트래픽을 방화벽으로 보내는 것을 방지하기 위해 *syslog* 발신자와 클라이언트가 모두 안전한 전용 네트워크에 있는지 확인하십시오.
필터 (Syslog 발신자만 해당)	서버 유형이 **Syslog Sender**인 경우 이 서버에서 받은 syslog 메시지에서 사용자명과 IP 주소를 추출하는 데 사용할 하나 이상의 Syslog Parse 프로파일을 추가합니다. 사용자 지정 프로파일(Syslog 필터 참조) 또는 사전 정의된 프로파일을 추가할 수 있습니다. 각 프로파일에 대해 이벤트 유형을 설정합니다. • 로그인 - User-ID 에이전트는 로그인 이벤트에 대한 syslog 메시지를 구문 분석하여 사용자 매핑을 생성합니다. • **logout** - User-ID 에이전트는 더 이상 최신이 아닌 사용자 매핑을 삭제하기 위해 로그아웃 이벤트에 대한 syslog 메시지를 구문 분석합니다. IP 주소 할당이 동적인 네트워크에서 자동 삭제는 에이전트가 현재 연결된 사용자에게만 각 IP 주소를 매핑하도록 하여 사용자 매핑의 정확도를 향상시킵니다. 사전 정의된 *Syslog Parse* 프로파일을 추가하는 경우 해당 이름을 확인하여 로그인 또는 로그아웃 이벤트와 일치하도록 의도되었는지의 여부를 결정하십시오.
기본 도메인 이름 (Syslog 발신자만 해당)	(선택 사항) 서버 유형이 **Syslog Sender**인 경우 도메인 이름을 입력하여 syslog 메시지의 사용자명에서 현재 도메인 이름을 재정의하거나 syslog 메시지에 도메인이 포함되어 있지 않은 경우 도메인을 사용자명 앞에 추가합니다.

모니터링되는 서버에 대한 액세스 관리

서버 모니터링 섹션에서 다음 작업을 수행하여 User-ID 에이전트가 사용자 매핑 정보를 모니터링하는 서버에 대한 액세스를 관리합니다.

작업	설명
서버 정보 표시	모니터링되는 각 서버에 대해 사용자 매핑 페이지는 User-ID 에이전트에서 서버로의 연결 상태를 표시합니다. 서버를 추가하면 방화벽이 서버에 연결을 시도합니다. 연결 시도가 성공하면 서버 모니터링 섹션의 상태 열에 연결됨이 표시됩니다. 방화벽이 연결할 수 없는 경우 상태 열에 ## ## 또는 ## ####와 같은 오류 조건이 표시됩니다. 서버 모니터링 섹션에 표시되는 다른 필드에 대한 자세한 내용은 모니터링되는 서버에 대한 액세스 구성을 참조하십시오.
추가	모니터링되는 서버에 대한 액세스를 구성하려면 사용자 매핑 정보에 대해 User-ID 에이전트가 모니터링할 각 서버를 추가합니다.
삭제	사용자 매핑 프로세스(검색)에서 서버를 제거하려면 서버를 선택한 다음 삭제합니다. 팁: 구성을 삭제하지 않고 검색에서 서버를 제거하려면 서버 항목을 편집하고 사용을 선택 취소합니다.
검색	DNS를 사용하여 Microsoft Active Directory 도메인 컨트롤러를 자동으로 검색할 수 있습니다. 방화벽은 **Device** > **Setup** > 관리 페이지, 일반 설정 섹션, 도메인 필드에 입력한 도메인 이름을 기반으로 도메인 컨트롤러를 검색합니다. 방화벽은 도메인 컨트롤러를 검색한 후 서버 모니터링 목록에 해당 항목을 만듭니다. 그런 다음 모니터링을 위해 서버를 활성화할 수 있습니다. 검색 기능은 *Exchange* 서버나 *eDirectory* 서버가 아닌 도메인 컨트롤러에서만 작동합니다.

사용자 매핑을 위한 하위 네트워크 포함 또는 제외

- 디바이스 > 사용자 식별 > 사용자 매핑

네트워크 포함/제외 목록을 사용하여 IP 주소-사용자명 매핑(검색)을 수행할 때 User-ID 에이전트가 포함하거나 제외할 하위 네트워크를 정의합니다. 기본적으로 목록에 하위 네트워크를 추가하지 않으면 User-ID 에이전트는 공용 IPv4 주소가 있는 클라이언트 시스템에 대해 WMI 검색을 사용하는 경우를 제외하고 모든 하위 네트워크에서 사용자 식별 소스에 대한 검색을 수행합니다. (공개 IPv4 주소는 RFC 1918 및 RFC 3927의 범위를 벗어난 주소입니다.)

공용 IPv4 주소에 대한 WMI 검색을 활성화하려면 해당 하위 네트워크를 목록에 추가하고 검색 옵션을 포함으로 설정해야 합니다. 사용자 매핑 정보를 다른 방화벽에 재배포하도록 방화벽을 구성하는 경우 목록에서 지정한 검색 제한이 재배포된 정보에 적용됩니다.

포함 및 제외 목록을 사용하여 방화벽이 사용자 매핑을 수행하는 서브넷을 정의합니다.

네트워크 포함/제외 목록에서 다음 작업을 수행할 수 있습니다.

작업	설명
추가하다	특정 하위 네트워크로 검색을 제한하려면 하위 네트워크 프로파일을 추가하고 다음 필드를 완료하십시오. • 이름 - 하위 네트워크를 식별하는 이름을 입력합니다. • 활성화됨 - 서버 모니터링을 위해 하위 네트워크를 포함하거나 제외하려면 이 옵션을 선택합니다. • 검색 - User-ID 에이전트가 하위 네트워크를 포함할지 또는 제외할지 선택합니다. • 네트워크 주소 - 서브네트워크의 IP 주소 범위를 입력합니다. User-ID 에이전트는 목록에 모든 암시적 제외 규칙을 적용합니다. 예를 들어 포함 옵션을 사용하여 하위 네트워크 10.0.0.0/8을 추가하는 경우 User-ID 에이전트는 목록에 추가하지 않더라도 다른 모든 하위 네트워크를 제외합니다. User-ID 에이전트가 명시적으로 포함된 하위 네트워크의 하위 집합을 제외하도록 하려는 경우에만 제외 옵션을 사용하여 항목을 추가합니다. 예를 들어, **Include** 옵션으로 10.0.0.0/8을 추가하고 **Exclude** 옵션으로 10.2.50.0/22를 추가하면, User-ID 에이전트는 10.2.50.0/22를 제외한 10.0.0.0/8의 모든 하위 네트워크에서 검색을 수행하고 10.0.0.0/8 외부의 모든 하위 네트워크를 제외합니다. 포함 프로파일을 추가하지 않고 제외 프로파일을 추가하면 User-ID 에이전트는 사용자가 추가한 하위 네트워크뿐만 아니라 모든 하위 네트워크를 제외합니다.
삭제	목록에서 하위 네트워크를 제거하려면 선택한 다음 삭제합니다. 팁: 구성을 삭제하지 않고 네트워크 포함/제외 목록에서 하위 네트워크를 제거하려면 하위 네트워크 프로파일을 편집하고 사용을 선택 취소합니다.
사용자 정의 네트워크 포함/제외	기본적으로 User-ID 에이전트는 하위 네트워크를 추가한 순서대로 위에서부터 아래로까지 평가합니다. 평가 순서를 변경하려면 사용자 지정 네트워크 시퀀스 포함/제외를 클릭합니다. 그런 다음 하위 네트워크를 추가, 삭제, 위로 이동 또는 아래로 이동하여 사용자 지정 평가 순서를 생성할 수 있습니다.

디바이스 > 사용자 식별 > 연결 보안

User-ID 연결 보안 설정을 편집( )하여 방화벽에서 Windows User-ID 에이전트가 제공한 인증서의 유효성을 검사하는 데 사용하는 인증서 프로파일을 선택합니다. 방화벽은 선택한 인증서 프로파일을 사용하여 에이전트가 제공한 서버 인증서의 유효성을 검사하여 User-ID 에이전트의 ID를 확인합니다.

작업	설명
User-ID 인증서 프로파일	드롭다운에서 Windows User-ID 에이전트를 인증할 때 사용할 인증서 프로파일을 선택하거나 새 인증서 프로파일을 선택하여 새 인증서 프로파일을 만듭니다. 없음을 선택하여 인증서 프로파일을 제거하고 대신 기본 인증을 사용합니다. 서버 인증에 Kerberos를 사용하는 모니터링되는 서버에 대한 액세스 구성 때 Windows 서버에서 서버 인증서 유효성 검사를 요구하려면 글로벌 서비스 설정에서 NTP를 구성하고 루트 CA를 인증서 프로파일로 선택해야 합니다.
모두 제거(템플릿 구성만 해당)	선택한 템플릿에 대한 User-ID 연결 보안 구성에 연결된 인증서 프로파일을 제거합니다.

디바이스 > 사용자 식별 > 터미널 서버 에이전트

동일한 IP 주소를 공유하는 여러 사용자를 지원하는 시스템에서 TS(터미널 서버) 에이전트는 각 사용자에게 포트 범위를 할당하여 개별 사용자를 식별합니다. TS 에이전트는 연결된 모든 방화벽에 할당된 포트 범위를 알려 방화벽이 사용자 및 사용자 그룹을 기반으로 정책을 시행할 수 있도록 합니다.

모든 방화벽 모델은 최대 5,000개의 다중 사용자 시스템에서 사용자명-포트 매핑 정보를 수집할 수 있습니다. 방화벽이 매핑 정보를 수집할 수 있는 TS 에이전트의 수는 방화벽 모델에 따라 다릅니다.

액세스를 구성하기 전에 *TS* 에이전트를 설치하고 구성해야 합니다. 터미널 서버 사용자에 대한 사용자 매핑을 구성하는 전체 절차에는 *TS* 에이전트에 대한 연결을 구성하는 것 외에 추가 작업이 필요합니다.

다음 작업을 수행하여 TS 에이전트에 대한 액세스를 관리할 수 있습니다.

작업	설명
정보 표시 / 연결 새로 고침	터미널 서버 에이전트 페이지에서 연결됨 열은 방화벽에서 TS 에이전트로의 연결 상태를 표시합니다. 녹색 아이콘은 성공적인 연결을 나타내고 노란색 아이콘은 비활성화된 연결을 나타내며 빨간색 아이콘은 실패한 연결을 나타냅니다. 페이지를 처음 연 이후 연결 상태가 변경되었다고 생각되면 연결 새로 고침을 클릭하여 상태 표시를 업데이트합니다.
추가	TS 에이전트에 대한 액세스를 구성하려면 에이전트를 추가하고 다음 필드를 구성합니다. • 이름 - TS 에이전트를 식별하기 위한 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. • 호스트 - TS 에이전트가 설치된 터미널 서버의 고정 IP 주소 또는 호스트 이름을 입력합니다. • 포트 - TS 에이전트 서비스가 방화벽과 통신하는 데 사용하는 포트 번호(기본값: 5009)를 입력합니다. • 대체 호스트 - TS 에이전트가 설치된 터미널 서버에 발신 트래픽에 대한 소스 IP 주소로 나타날 수 있는 여러 IP 주소가 있는 경우 최대 8개의 추가 고정 IP 주소 또는 호스트 이름을 추가하고 입력합니다. • 활성화 - 방화벽이 이 TS 에이전트와 통신할 수 있도록 하려면 이 옵션을 선택합니다.
삭제	TS 에이전트에 대한 액세스를 활성화하는 구성을 제거하려면 에이전트를 선택한 다음 삭제를 클릭합니다.

작업	설명
	구성을 삭제하지 않고 *TS* 에이전트에 대한 액세스를 비활성화하려면 에이전트를 편집하고 활성화 옵션을 지웁니다.
PDF/CSV	최소한의 읽기 전용 액세스 권한이 있는 관리 역할은 디바이스 구성 테이블을 **PDF/CSV**로 내보낼 수 있습니다. 필터를 적용하여 감사와 같은 항목에 대한 보다 구체적인 테이블 구성 출력을 생성할 수 있습니다. 웹 인터페이스에서 보이는 열만 내보내집니다. 구성 테이블 내보내기를 참조하십시오.

디바이스 > 사용자 식별 > 그룹 매핑 설정

- 디바이스 > 사용자 식별 > 그룹 매핑 설정

사용자 및 사용자 그룹에 대한 보안 정책 및 보고서를 기반으로 하기 위해 방화벽은 그룹 목록과 디렉터리 서버에서 지정 및 유지 관리되는 해당 구성원 목록을 검색합니다. 방화벽은 Microsoft Active Directory(AD), Novell eDirectory 및 Sun ONE Directory Server를 비롯한 다양한 LDAP 디렉토리 서버를 지원합니다.

각 방화벽 또는 Panorama가 모든 정책에서 참조할 수 있는 고유한 사용자 그룹의 수는 모델에 따라 다릅니다. 그러나 모델에 관계없이 그룹 매핑 구성을 생성하기 전에 LDAP 서버 프로파일을 구성해야 합니다(디바이스 > 서버 프로파일 > LDAP).

사용자명을 그룹에 매핑하는 전체 절차에는 그룹 매핑 구성을 만드는 것 외에 추가 작업이 필요합니다.

그룹 매핑 구성을 생성하기 위해 필요에 따라 다음 필드를 추가하고 구성합니다. 그룹 매핑 구성을 제거하려면 선택한 다음 삭제합니다. 그룹 매핑 구성을 삭제하지 않고 비활성화하려면 구성을 편집하고 사용 옵션을 지웁니다.

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.

그룹 매핑 설정 - 서버 프로파일	구성 위치	설명
이름	디바이스 > 사용자 식별 > 그룹 매핑 설정	그룹 매핑 구성을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
서버 프로파일	디바이스 > 사용자 식별 > 그룹 매핑 설정 > 서버 프로파일	이 방화벽에서 그룹 매핑에 사용할 LDAP 서버 프로파일을 선택합니다.
업데이트 인터벌		방화벽 정책이 사용하는 그룹에 대한 업데이트를 가져오기 위해 방화벽이 LDAP 디렉토리 서버와의 연결을 시작하는 인터벌(초)을 지정합니다(범위는 60 - 86,400).
사용자 도메인		기본적으로 사용자 도메인은 비어 있습니다. 방화벽은 Active Directory 서버의 도메인 이름을 자동으로 감지합니다. 값을 입력하면 방화벽이

그룹 매핑 설정 - 서버 프로파일	구성 위치	설명
		LDAP 소스에서 검색하는 모든 도메인 이름을 무시합니다. 항목은 NetBIOS 이름이어야 합니다. 이 필드는 *LDAP* 소스에서 검색된 사용자명과 그룹 이름에만 영향을 줍니다. 사용자 인증을 위해 사용자명과 연결된 도메인을 재정의하려면 해당 사용자에게 할당한 인증 프로파일에 대해 사용자 도메인 및 사용자명 수정자를 구성합니다*(*디바이스 > 인증 프로파일 참조*)*.
그룹 개체		• 검색 필터 - 검색하고 추적할 그룹을 지정하는 LDAP 쿼리를 입력합니다. • 개체 클래스 - 그룹 정의를 입력합니다. 기본값은 objectClass=group이며, 이는 시스템이 검색 필터 그룹과 일치하고 objectClass=group이 있는 디렉토리의 모든 개체를 검색하도록 지정합니다.
사용자 개체		• 검색 필터 - 검색하고 추적할 사용자를 지정하는 LDAP 쿼리를 입력합니다. • 개체 클래스 - 사용자 개체 정의를 입력합니다. 예를 들어, Active Directory에서 objectClass는 *user*입니다.
활성화됨		그룹 매핑에 대해 서버 프로파일을 활성화하려면 이 옵션을 선택합니다.
관리 디바이스 목록 가져오기		GlobalProtect 배포의 경우 방화벽이 디렉터리 서버(예: Active Directory)에서 일련번호를 검색할 수 있도록 하려면 이 옵션을 선택합니다. 이를 통해 GlobalProtect는 연결 엔드포인트의 상태를 식별하고 엔드포인트 일련번호의 존재를 기반으로 HIP 기반 보안 정책을 시행할 수 있습니다.

그룹 매핑 설정 - 서버 프로파일	구성 위치	설명
사용자 속성	디바이스 > 사용자 식별 > 그룹 매핑 설정 > 사용자 및 그룹 속성	사용자를 식별할 디렉토리 속성을 지정합니다. • 기본 사용자 이름 - 사용자 ID 소스가 사용자 이름에 제공하는 속성을 지정합니다(예: **userPrincipalName** 또는 **sAMAccountName**). 기본 사용자 이름 방화벽은 사용자 *ID* 소스에서 다른 형식을 수신하더라도 방화벽이 로그, 보고서 및 정책 구성에서 사용자를 식별하는 방법입니다. 형식을 지정하지 않으면 방화벽은 기본적으로 *Active Directory*의 경우 *sAMAccountName* 형식을 사용하고 *Novell eDirectory* 및 *Sun ONE Directory Server*의 경우 *uid* 형식을 사용합니다. • 이메일 - 이메일 주소에 대해 User-ID 소스가 제공하는 속성을 지정합니다. 기본값은 ##입니다. • 대체 사용자 이름 1-3 - User-ID 소스가 보낼 수 있는 형식에 해당하는 최대 3개의 추가 속성을 지정합니다. *Active Directory* 서버를 구성하는 경우 대체 사용자 이름 *1*은 기본적으로 *userPrincipalName* 입니다.
그룹 속성		User-ID 소스가 그룹을 식별하는 데 사용하는 속성을 지정합니다. • 그룹 이름 - User-ID 소스가 그룹 이름 속성에 사용하는 속성을 지정합니다. Active Directory의 기본값은 name이고

그룹 매핑 설정 - 서버 프로파일	구성 위치	설명
		Novell eDirectory 또는 Sun ONE Directory Server의 기본값은 cn입니다. • 그룹 구성원 - User-ID 소스가 그룹 구성원에 대해 사용하는 속성을 지정합니다. 기본값은 ##입니다. • 이메일 - User-ID 소스가 이메일 주소에 사용하는 속성을 지정합니다. 기본값은 ##입니다.
사용 가능한 그룹 포함된 그룹	디바이스 > 사용자 식별 > 그룹 매핑 설정 > 그룹 포함 목록	이 필드를 사용하여 보안 규칙을 생성할 때 방화벽이 표시하는 그룹 수를 제한합니다. LDAP 트리를 탐색하여 규칙에 사용할 그룹을 찾습니다. 그룹을 포함하려면 사용 가능한 그룹 목록에서 그룹을 선택한 다음 추가( )합니다. 목록에서 그룹을 제거하려면 포함된 그룹 목록에서 선택하여 삭제( )합니다. 방화벽이 *LDAP* 디렉토리에서 전체 트리가 아니라 필요한 그룹에 대해서만 사용자 그룹 매핑을 검색하도록 필요한 그룹만 포함합니다.
이름 LDAP 필터	디바이스 > 사용자 식별 > 그룹 매핑 설정 > 사용자 지정 그룹	LDAP 디렉토리에 있는 기존 사용자 그룹과 일치하지 않는 사용자 속성을 기반으로 방화벽 정책을 설정할 수 있도록 LDAP 필터를 기반으로 사용자 지정 그룹을 만듭니다. User-ID 서비스는 필터와 일치하는 모든 LDAP 디렉터리 사용자를 사용자 지정 그룹에 매핑합니다. 기존 Active Directory 그룹 도메인 이름과 동일한 DN(고유 이름)으로 사용자 지정 그룹을 만드는 경우 방화벽은 해당 이름에 대한 모든 참조(예: 정책 및 로그)에서 사용자 지정 그룹을 사용합니다. 사용자 지정 그룹을 생성하려면 다음 필드를 추가하고 구성합니다.

그룹 매핑 설정 - 서버 프로파일	구성 위치	설명
		• 이름 - 현재 방화벽 또는 가상 시스템에 대한 그룹 매핑 구성에서 고유한 사용자 지정 그룹 이름을 입력합니다. • **LDAP** 필터 - 최대 2,048자의 필터를 입력합니다. 필터에서 색인화된 속성만 사용하여 *LDAP* 검색을 촉진하고 *LDAP* 디렉토리 서버에 대한 성능 영향을 최소화하십시오. 방화벽은 *LDAP* 필터의 유효성을 검사하지 않습니다. 포함된 그룹 및 사용자 지정 그룹 목록의 최대 결합 수는 640개 항목입니다. 사용자 지정 그룹을 삭제하려면 선택한 다음 삭제합니다. 사용자 지정 그룹의 복사본을 만들려면 선택한 다음 복사한 다음 필드를 적절하게 편집합니다. 사용자 지정 그룹을 추가하거나 복사한 후 정책 및 개체에서 새 사용자 지정 그룹을 사용할 수 있으려면 변경 사항을 커밋해야 합니다.

디바이스 > 사용자 식별> 신뢰할 수 있는 소스 주소

명시적 프록시는 특정 IP 주소의 트래픽만 XAU(X-Authenticated-User) 프로토콜을 사용하여 인증하도록 허용합니다. 주소 개체를 만든 다음 신뢰할 수 있는 소스 주소 구성을 편집하고 주소 개체를 추가하여 XAU가 명시적 프록시 인증에 허용되는 IP 주소를 지정합니다. 자세한 내용은 명시적 프록시로 모바일 사용자 보호를 참조하십시오.

신뢰할 수 있는 소스 주소 필드	설명
활성화됨	신뢰할 수 있는 소스 주소 구성을 활성화하려면 이 옵션을 선택합니다.
신뢰할 수 있는 소스 주소	신뢰할 수 있는 소스 주소를 추가합니다. 이러한 소스 주소에서 들어오는 요청에 포함된 XAU(X-Authenticated-User)는 명시적 프록시에 대해 신뢰됩니다. 신뢰할 수 있는 소스 주소 목록을 검색하거나 필요한 경우 소스 주소를 삭제할 수도 있습니다.

디바이스 > 사용자 식별 > 인증 포털 설정

인증 포털 설정을 편집( )하여 트래픽이 인증 정책 규칙과 일치하는 사용자를 인증하도록 방화벽을 구성합니다.

인증 포털이 *SSL/TLS* 서비스 프로파일(디바이스 > 인증서 관리 > SSL/TLS 서비스 프로필), 인증 프로파일(디바이스 > 인증 프로파일) 또는 인증서 프로파일(디바이스 > 인증서 관리 > 인증서 프로파일)을 선택한 다음 시작하기 전에 프로파일을 구성합니다. 인증 포털을 구성하는 전체 절차에는 이러한 프로파일 구성 외에 추가 작업이 필요합니다.

인증 정책을 시행하려면 인증 포털을 활성화를 해야 합니다(정책 > 인증 참조).

필드	설명
인증 포털 활성화	인증 포털을 활성화하려면 이 옵션을 선택합니다.
유휴 타이머(분)	인증 포털 세션에 대한 사용자 TTL(Time-to-Live) 값을 분 단위로 입력합니다(범위는 1~1,440, 기본값은 15). 이 타이머는 인증 포털 사용자의 활동이 있을 때마다 재설정됩니다. 사용자의 유휴 시간이 유휴 타이머 값을 초과하면 PAN-OS는 인증 포털 사용자 매핑을 제거하고 사용자는 다시 로그인해야 합니다.
타이머(분)	이는 인증 포털 세션이 매핑된 상태로 유지될 수 있는 최대 시간(범위는 1~1,440, 기본값은 60)인 최대 TTL(분)입니다. 이 기간이 경과하면 PAN-OS는 매핑을 제거하고 세션이 활성 상태인 경우에도 사용자는 다시 인증해야 합니다. 이 타이머는 오래된 매핑을 방지하고 유휴 타이머 값을 재정의합니다. 만료 타이머는 항상 유휴 타이머보다 높게 설정해야 합니다.
SSL/TLS 서비스 프로파일	방화벽 서버 인증서와 리디렉션 요청을 보호하기 위해 허용되는 프로토콜을 지정하려면 SSL/TLS 서비스 프로파일(디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일)을 선택합니다. 없음을 선택하면 방화벽은 SSL/TLS 연결에 로컬 기본 인증서를 사용합니다. *SSL/TLS* 서비스 프로파일에서 최소 버전을 ***TLSv1.2***로 설정하고 최대 버전을 최대로 설정하여 *SSL/TLS* 프로토콜 취약성에 대한 가장 강력한 보안을 제공합니다. ***Max Version***을 ***Max***로 설정하면 더 강력한 프로토콜을 사용할 수 있게 되면 방화벽이 항상 최신 버전을 사용합니다. 인증서 오류를 표시하지 않고 사용자를 투명하게 리디렉션하려면 웹 요청을 리디렉션하는 인터페이스의 IP 주소와 일치하는 인증서와 연결된 프로파일을 할당합니다.

필드	설명
인증 프로파일	인증 프로파일(디바이스 > 인증 프로파일)을 선택하여 트래픽이 인증 정책 규칙(정책 > 인증)과 일치할 때 사용자를 인증할 수 있습니다. 그러나 인증 포털 설정에서 선택한 인증 프로파일은 기본 인증 적용 개체(개체 > 인증) 중 하나를 참조하는 규칙에만 적용됩니다. 이는 모든 인증 규칙이 초기에 기본 개체를 참조하기 때문에 일반적으로 PAN-OS 8.0으로 업그레이드한 직후의 경우입니다. 사용자 지정 인증 적용 개체를 참조하는 규칙의 경우 개체를 생성할 때 인증 프로파일을 선택합니다.
인바운드 인증 프롬프트(UDP)용 GlobalProtect 네트워크 포트	GlobalProtect™가 다중 요소(MFA) 게이트웨이로부터 인바운드 인증 프롬프트를 수신하는 데 사용하는 포트를 지정하십시오. (범위는 1 ~ 65,536, 기본값은 4,501). 다단계 인증을 지원하려면 GlobalProtect 엔드포인트가 MFA 게이트웨이에서 인바운드되는 UDP 프롬프트를 수신하고 승인해야 합니다. GlobalProtect 엔드포인트가 지정된 네트워크 포트에서 UDP 메시지를 수신하고 UDP 메시지가 신뢰할 수 있는 방화벽이나 게이트웨이에서 오는 경우 GlobalProtect는 인증 메시지를 표시합니다(GlobalProtect 앱 사용자 지정 참조).
모드	방화벽이 인증을 위해 웹 요청을 캡처하는 방법 선택: • 투명 - 방화벽은 인증 규칙에 따라 웹 요청을 가로채고 원래 대상 URL을 가장하여 HTTP 401 메시지를 발행하여 사용자에게 인증을 요청합니다. 그러나 방화벽에는 대상 URL에 대한 실제 인증서가 없기 때문에 브라우저는 보안 사이트에 액세스하려는 사용자에게 인증서 오류를 표시합니다. 따라서 레이어 2 또는 가상 와이어 배포와 같이 절대적으로 필요한 경우에만 이 모드를 사용하십시오. • 리디렉션 - 방화벽이 인증 규칙에 따라 웹 요청을 가로채서 지정된 리디렉션 호스트로 리디렉션합니다. 방화벽은 HTTP 302 리디렉션을 사용하여 사용자에게 인증을 요청합니다. 가장 좋은 방법은 더 나은 최종 사용자 경험을 제공하기 때문에 리디렉션을 사용하는 것입니다(타임아웃이 만료될 때 리디렉션이 다시 매핑되지 않기 때문에 인증서 오류가 표시되지 않고 원활한 탐색을 가능하게 하는 세션 쿠키 허용). 그러나 인그레스 레이어 3 인터페이스에 할당된 인터페이스 관리 프로파일에서 응답 페이지를 활성화해야 합니다 (자세한 내용은 네트워크 > 네트워크 프로파일 > 인터페이스 관리 및 PA-7000 시리즈 레이어 3 인터페이스 참조). 리디렉션 모드의 또 다른 이점은 세션 쿠키를 허용하여 사용자가 시간 초과가 만료될 때마다 다시 매핑할 필요 없이 인증된 사이트를 계속 탐색할 수 있다는 점입니다. 이것은 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). 브라우저가 신뢰할 수 있는 사이트에만 자격 증명을 제공하기 때문에 인증 포털이 Kerberos SSO를 사용하는 경우

필드	설명
	리디렉션 모드가 필요합니다. 인증 포털이 *MFA(*다단계 인증*)*를 사용하는 경우에도 리디렉 모드가 필요합니다.
세션 쿠키 (리디렉트 모드만 해당)	• 활성화 - 세션 쿠키를 활성화하려면 이 옵션을 선택합니다. • 타임아웃 - 세션 쿠키를 활성화하면 이 타이머는 쿠키가 유효한 시간(분)을 지정합니다(범위는 60–10,080, 기본값은 1,440). 타임아웃 값을 충분히 짧게 설정하여 쿠키의 오래된 사용자 매핑 항목으로 이어지지 않지만 세션 중에 사용자에게 여러 번 로그인하라는 메시지를 표시하지 않아 우수한 사용자 경험을 촉진할 수 있을 만큼 충분히 길게 설정합니다. *480*분*(8*시간*)* 이하의 값으로 시작하고 필요에 따라 값을 조정합니다. • 로밍 - 세션이 활성 상태인 동안(예: 엔드포인트가 유선 네트워크에서 무선 네트워크로 이동하는 경우) IP 주소가 변경되는 경우 쿠키를 유지하려면 이 옵션을 선택합니다. 사용자는 쿠키 시간이 초과되거나 사용자가 브라우저를 닫은 경우에만 재인증해야 합니다.
리디렉션 호스트 (리디렉트 모드만 해당)	방화벽이 웹 요청을 리디렉션하는 레이어 3 인터페이스의 IP 주소로 확인되는 인트라넷 호스트 이름을 지정합니다. 사용자가 *Kerberos SSO(Single Sign-On)*를 통해 인증하는 경우 리디렉션 호스트는 Kerberos 키 탭에 지정된 호스트 이름과 동일해야 합니다.
인증서 프로파일	사용자의 트래픽이 인증 정책 규칙(정책 > 인증)과 일치하는 경우 인증서 프로파일(디바이스 > 인증서 관리 > 인증서 프로파일)을 선택하여 사용자를 인증할 수 있습니다. 이 인증 유형의 경우 인증 포털은 클라이언트 인증서를 제시하도록 사용자의 엔드포인트 브라우저에 프롬프트를 표시합니다. 따라서 각 사용자 시스템에 클라이언트 인증서를 배포해야 합니다. 또한 방화벽에 클라이언트 인증서를 발급한 CA(인증 기관) 인증서를 설치하고 인증서 프로파일에 CA 인증서를 할당해야 합니다. 이것은 macOS 및 Linux 엔드포인트에 대해 투명 인증을 활성화하는 유일한 인증 방법입니다.

디바이스 > 사용자 식별 > Cloud Identity Engine

Cloud Identity Engine을 사용자 식별 정보의 소스로 사용하려면 방화벽에 Cloud Identity Engine 프로파일을 추가하십시오. Cloud Identity Engine 프로파일을 만들 때 Cloud Identity Engine 앱에서 구성한 온프레미스 또는 클라우드 기반 디렉터리의 사용자 및 그룹 정보를 기반으로 사용자 또는 그룹 기반 보안 정책을 시행할 수 있습니다. 프로파일을 삭제하거나 현재 Cloud Identity Engine 프로파일의 **PDF/CSV**를 내보낼 수도 있습니다.

방화벽에서 *Cloud Identity Engine* 프로파일을 구성하려면 먼저 디바이스 인증서를 설치하고 허브에서 *Cloud Identity Engine* 인스턴스를 활성화해야 합니다.

프로파일을 검색하려면 필터(🔍)와 필터 적용(→)으로 키워드를 입력하세요.

Cloud ID 엔진 설정	설명
이름	Cloud Identity Engine 프로파일의 이름(최대 31자)을 입력합니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
인스턴스	Cloud Identity Engine 프로파일을 구성하려면 다음 정보를 입력하세요. • 지역 - Cloud Identity Engine 인스턴스의 지역 엔드포인트를 선택합니다. 선택하는 지역은 *Cloud Identity Engine* 인스턴스를 활성화할 때 선택한 지역과 일치해야 합니다. • **Cloud Identity Engine** 인스턴스 - 인스턴스가 두 개 이상인 경우 사용할 Cloud Identity Engine 인스턴스를 선택합니다. • 도메인 - 사용하려는 디렉토리가 포함된 도메인을 선택합니다. • 업데이트 간격**(분)** - 방화벽이 DS의 업데이트 사이에. 기본값은 60분이고 범위는 5-1440입니다. Cloud Identity Engine 프로파일 구성을 마치면 프로파일이 사용 설정되어 있는지 확인합니다.
사용자 속성	각 사용자 속성 이름에 대해 디렉토리 속성을 선택합니다. 기본 사용자명을 선택해야 합니다. 다른 모든 필드는 선택 사항입니다.

Cloud ID 엔진 설정	설명
그룹 속성	각 그룹 속성 이름에 대해 디렉토리 속성을 선택합니다. 그룹 이름을 선택해야 합니다. 나머지 필드는 선택 사항입니다.
디바이스 속성	(GlobalProtect만 해당) GlobalProtect를 사용 중이고 일련번호 확인을 활성화한 경우 Cloud Identity Engine이 관리되는 엔드포인트에서 일련번호를 수집할 수 있도록 엔드포인트 일련번호를 선택합니다. 이 정보는 GlobalProtect 포털에서 엔드포인트가 GlobalProtect에서 관리되고 있는지 확인하기 위해 디렉터리에 일련번호가 있는지 확인하는 데 사용됩니다.

GlobalProtect

GlobalProtect™는 모바일 인력을 관리하기 위한 완벽한 인프라를 제공하여 사용자가 사용하는 디바이스나 위치에 관계없이 모든 사용자가 안전하게 액세스할 수 있도록 합니다. 다음 방화벽 웹 인터페이스 페이지를 사용하여 GlobalProtect 구성 요소를 구성 및 관리할 수 있습니다.

- 네트워크 > GlobalProtect > 포털
- Network > GlobalProtect > Gateways
- Network > GlobalProtect > MDM
- 네트워크 > 글로벌 > 클라이언트리스 앱
- 네트워크 > GlobalProtect > 클라이언트리스 앱 그룹
- 개체 > GlobalProtect > HIP 개체
- 개체 > GlobalProtect > HIP 프로파일
- Device > GlobalProtect Client

더 찾고 계십니까?

GlobalProtect 인프라 설정에 대한 세부 정보, 정책을 시행하기 위해 호스트 정보를 사용하는 방법, 일반적인 GlobalProtect 배포를 구성하기 위한 단계별 지침을 포함하여 GlobalProtect에 대한 자세한 내용은 GlobalProtect 관리자 가이드를 참조하십시오.

네트워크 > GlobalProtect > 포털

Network > **GlobalProtect** > **Portals**를 선택하여 GlobalProtect™ 포털을 설정하고 관리합니다. 포털은 GlobalProtect 인프라에 대한 관리 기능을 제공합니다. GlobalProtect 네트워크에 참여하는 모든 엔드포인트는 사용 가능한 게이트웨이 및 앱이 게이트웨이에 연결하는 데 필요한 클라이언트 인증서에 대한 정보를 포함하여 포털에서 해당 구성을 수신합니다. 또한 포털은 macOS 및 Windows 엔드포인트에 대한 GlobalProtect 앱 소프트웨어의 동작 및 배포를 제어합니다. Linux 엔드포인트의 경우 지원 사이트에서 소프트웨어를 얻어야 합니다. 모바일 디바이스의 경우 GlobalProtect 앱은 Apple App Store(iOS 디바이스의 경우), Google Play(Android 디바이스의 경우) 및 Microsoft Store(Windows Phone 및 기타 Windows UWP 디바이스의 경우)를 통해 배포되며 Chromebook의 경우, GlobalProtect 앱은 Chromebook 관리 콘솔 또는 Google Play를 통해 배포됩니다.

포털 구성을 추가하려면 추가를 클릭하여 GlobalProtect 포털 대화 상자를 엽니다.

무엇을 찾고 계신가요?	참조:
GlobalProtect 포털에 대해 어떤 일반 설정을 구성해야 합니까?	GlobalProtect 포털 일반 탭
포털 구성에 인증 프로파일을 할당하려면 어떻게 해야 합니까?	GlobalProtect 포털 인증 탭
GlobalProtect 앱이 엔드포인트에서 수집하는 데이터를 어떻게 정의할 수 있습니까?	GlobalProtect 포털 포털 데이터 수집 탭
어떤 클라이언트 인증 옵션을 구성할 수 있습니까?	GlobalProtect Portals 에이전트 인증 탭
운영 체제, 사용자 및/또는 사용자 그룹을 기반으로 특정 디바이스 그룹에 구성을 할당하려면 어떻게 해야 합니까?	GlobalProtect Portals 에이전트 구성 선택 기준 탭
내부 게이트웨이의 설정과 우선 순위를 구성하려면 어떻게 해야 합니까?	GlobalProtect 포털 에이전트 내부 탭
외부 게이트웨이의 설정 및 우선 순위를 구성하려면 어떻게 해야 합니까?	GlobalProtect 포털 에이전트 외부 탭
다양한 유형의 사용자에 대해 별도의 클라이언트 구성을 생성하려면 어떻게 해야 합니까?	GlobalProtect 포털 에이전트 탭

무엇을 찾고 계신가요?	참조:
GlobalProtect 앱의 모양과 동작에 대해 어떤 설정을 사용자 지정할 수 있습니까?	GlobalProtect Portals 에이전트 앱 탭
데이터 수집 옵션을 구성하려면 어떻게 해야 합니까?	GlobalProtect Portals 에이전트 데이터 수집 탭
GlobalProtect 앱을 설치하지 않고 웹 애플리케이션에 대한 액세스를 허용하도록 GlobalProtect 포털을 구성하려면 어떻게 해야 합니까?	GlobalProtect 포털 클라이언트리스 VPN 탭
새틀라이트 역할을 하는 방화벽으로 VPN 연결을 확장하려면 어떻게 해야 합니까?	GlobalProtect 포털 새틀라이트 탭
더 찾고 계십니까?	포털 설정에 대한 자세한 단계별 지침은 *GlobalProtect* 관리자 안내서에서 GlobalProtect 포털 구성을 참조하십시오.

GlobalProtect 포털 일반 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 일반

일반 탭을 선택하여 GlobalProtect 앱이 GlobalProtect 포털에 연결하는 데 사용하는 네트워크 설정을 정의합니다. 선택적으로 로그인 페이지를 비활성화하거나 GlobalProtect에 대한 사용자 정의 포털 로그인 및 도움말 페이지를 지정할 수 있습니다. 사용자 정의 페이지를 만들고 가져오는 방법에 대한 정보는 GlobalProtect 관리자 안내서에서 포털 로그인, 시작 및 도움말 페이지 사용자 정의를 참조하십시오.

GlobalProtect 포털 설정	설명
이름	포털 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	다중 가상 시스템 모드에 있는 방화벽의 경우 위치는 GlobalProtect 포털을 사용할 수 있는 가상 시스템(vsys)입니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 위치 선택을 사용할 수 없습니다. 포털을 저장한 후에는 위치를 변경할 수 없습니다.
네트워크 설정	

GlobalProtect 포털 설정	설명
상호 작용	원격 엔드포인트 및 방화벽으로부터의 통신에 대한 수신이 될 방화벽 인터페이스의 이름을 선택하십시오. 관리 인터페이스가 인터넷에 노출되기 때문에, *Telnet*, *SSH*, *HTTP* 또는 *HTTPS*를 허용하는 인터페이스 관리 프로파일을 *GlobalProtect* 포털 또는 게이트웨이를 구성한 인터페이스에 연결하지 마십시오. 관리 네트워크에 대한 액세스를 보호하는 방법에 대한 자세한 내용은 관리 액세스 모범 사례를 참조하십시오.
IP 주소	GlobalProtect 포털 웹 서비스를 실행할 IP 주소를 지정합니다. **IP** 주소 유형을 선택한 다음 **IP** 주소를 입력합니다. • 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 IPv4의 경우 172.16.1.0 또는 IPv6의 경우 21DA:D3:0:2F3b입니다. • **IPv4** 및 **IPv6**을 선택하는 경우 각각에 대해 적절한 IP 주소 유형을 입력합니다.
로그 설정	
성공적인 SSL 핸드쉐이크 기록	(선택 사항) 성공적인 SSL 복호화 핸드쉐이크에 대한 자세한 로그를 생성합니다. 기본적으로 비활성화되어 있습니다. 로그는 저장 공간을 사용합니다. 성공적인 *SSL* 핸드쉐이크를 기록하기 전에 로그를 저장하는 데 사용할 수 있는 리소스가 있는지 확인하십시오. ***Device*** > ***Setup*** > ***Management*** > 로깅 및 보고 설정을 편집하여 현재 로그 메모리 할당을 확인하고 로그 유형 간에 로그 메모리를 다시 할당합니다.
SSL 핸드쉐이크 실패 기록	SSL 복호화 핸드쉐이크 실패에 대한 자세한 로그를 생성하여 복호화 문제의 원인을 찾을 수 있습니다. 기본적으로 활성화되어 있습니다. 로그는 저장 공간을 사용합니다. 더 많거나 적은 로그 저장 공간을 복호화 로그에 할당하려면 로그 메모리 할당*(*디바이스 > 설정 > 관리 > 로깅 및 보고 설정*)*을 편집하십시오.

GlobalProtect 포털 설정	설명
로그 포워딩	GlobalProtect SSL 핸드쉐이크(복호화) 로그를 포워딩할 방법과 위치를 지정합니다.
형태	
포털 로그인 페이지	(선택 사항) 포털에 대한 사용자 액세스를 위한 사용자 정의 로그인 페이지를 선택합니다. 공장 기본 페이지 또는 사용자 정의 페이지 가져오기를 선택할 수 있습니다. 기본값은 없음입니다. 웹 브라우저에서 이 페이지에 액세스하는 것을 방지하려면 이 페이지를 비활성화하십시오.
포털 랜딩 페이지	(선택 사항) 포털에 대한 사용자 지정 랜딩 페이지를 선택합니다. 공장 기본 페이지 또는 사용자 정의 페이지 가져오기를 선택할 수 있습니다. 기본값은 없음입니다.
앱 도움말 페이지	(선택 사항) 사용자 정의 도움말 페이지를 선택하여 GlobalProtect로 사용자를 지원합니다. 공장 기본 페이지 또는 사용자 정의 페이지 가져오기를 선택할 수 있습니다. 공장 기본값 도움말 페이지는 GlobalProtect 앱 소프트웨어와 함께 제공됩니다. 사용자 정의 도움말 페이지를 선택하는 경우 GlobalProtect 포털은 GlobalProtect 포털 구성이 포함된 도움말 페이지를 제공합니다. 기본값인 없음을 그대로 두면 GlobalProtect 앱이 페이지를 표시하지 않고 메뉴에서 옵션을 제거합니다.

GlobalProtect 포털 인증 구성 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 입증

인증 탭을 선택하여 다양한 GlobalProtect™ 포털 설정을 구성합니다.

- 포털 및 서버가 인증에 사용하는 SSL/TLS 서비스 프로파일입니다. 서비스 프로파일은 인증의 다른 설정과 독립적입니다.
- 주로 사용자 엔드포인트의 운영 체제를 기반으로 하고 두 번째로 선택적 인증 프로파일을 기반으로 하는 고유한 인증 체계입니다.
- (선택 사항) GlobalProtect가 사용자 인증을 위해 특정 인증서 프로파일을 사용할 수 있도록 하는 인증서 프로파일. 클라이언트의 인증서는 인증서 프로파일과 일치해야 합니다(클라이언트 인증서가 보안 체계의 일부인 경우).

GlobalProtect 포털 인증 설정	설명
서버 인증	

GlobalProtect 포털 인증 설정	설명
SSL/TLS 서비스 프로파일	기존 SSL/TLS 서비스 프로파일을 선택합니다. 프로파일은 관리 인터페이스에서 트래픽을 보호하기 위해 인증서와 허용된 프로토콜을 지정합니다. CN(일반 이름) 및 해당하는 경우 프로파일과 연결된 인증서의 SAN(주체 대체 이름) 필드는 일반 탭에서 선택한 인터페이스의 IP 주소 또는 FQDN과 일치해야 합니다. *GlobalProtect VPN* 구성에서 신뢰할 수 있는 타사 *CA*의 인증서 또는 내부 엔터프라이즈 *CA*에서 생성한 인증서와 연결된 프로파일을 사용합니다.
클라이언트 인증	
이름	클라이언트 인증 구성을 식별하는 이름을 입력합니다. (클라이언트 인증 구성은 SSL/TLS 서비스 프로파일과 무관합니다.) 여러 클라이언트 인증 구성을 만들고 운영 체제별로 구분할 수 있습니다. 예를 들어 Windows 엔드포인트에 대해 고유한 인증 프로파일을 하나 추가하고 macOS 엔드포인트에 대해 다른 인증 프로파일을 추가할 수 있습니다. 동일한 *OS*에 대해 여러 클라이언트 인증 구성을 추가할 수 있지만 방화벽은 항상 목록 맨 위에 있는 인증 프로파일을 선택하여 특정 *OS*를 사용하는 모든 사용자를 인증합니다. GlobalProtect가 사전 로그온 모드(사용자가 시스템에 로그인하기 전)에서 앱에 배포하거나 모든 사용자에게 적용하는 구성을 생성할 수도 있습니다. (사전 로그온은 사용자가 GlobalProtect에 로그인하기 전에 GlobalProtect 게이트웨이에 대한 VPN 터널을 설정합니다.)
OS	엔드포인트의 운영 체제(OS)에 특정한 클라이언트 인증 프로파일을 배포하려면 OS(**Any**, **Android**, **Chrome**, **iOS**, **Linux**, **Mac**, **Windows** 또는 **WindowsUWP**)를 추가합니다. OS는 구성 간의 주요 차별화 요소입니다. (추가 차별화는 인증 프로파일을 참조하십시오.) 브라우저 및 새틀라이트의 추가 옵션을 사용하면 특정 시나리오에 사용할 인증 프로파일을 지정할 수 있습니다. 브라우저를 선택하여 GlobalProtect 앱(Windows 및 Mac)을 다운로드할 목적으로 웹 브라우저에서 포털에 액세스하는 사용자를 인증하는 데 사용할 인증 프로파일을 지정합니다. 새틀라이트(LSVPN)을 인증하는 데 사용할 인증 프로파일을 지정하려면 새틀라이트를 선택합니다.

GlobalProtect 포털 인증 설정	설명
인증 프로파일	OS별로 클라이언트 인증 구성을 구분하는 것 외에도 인증 프로파일을 지정하여 추가로 구분할 수 있습니다. (새 인증 프로파일을 생성하거나 기존 프로파일을 선택할 수 있습니다.) OS에 대해 여러 인증 옵션을 구성하기 위해 여러 클라이언트 인증 프로파일을 만들 수 있습니다. 게이트웨이에서 *LSVPN*을 구성하는 경우 여기에서 인증 프로파일을 선택하지 않으면 해당 구성을 저장할 수 없습니다. 또한 일련번호를 사용하여 새틀라이트를 인증하려는 경우 포털에서 방화벽 일련번호를 찾거나 유효성을 검사할 수 없을 때 사용할 수 있는 인증 프로파일이 있어야 합니다. 디바이스 > 인증 프로파일도 참조하십시오.
사용자명 레이블	GlobalProtect 포털 로그인에 대한 사용자 정의 사용자명 레이블을 지정하십시오. 예를 들어 사용자명**(**만**)** 또는 이메일 주소**(username@domain)**입니다.
비밀번호 레이블	GlobalProtect 포털 로그인에 대한 사용자 정의 비밀번호 레이블을 지정하십시오. 예를 들어 암호**(**터키어**)** 또는 암호(2단계 토큰 기반 인증의 경우)가 해당됩니다.
인증 메시지	최종 사용자가 로그인에 필요한 자격 증명 유형을 알 수 있도록 하려면 메시지를 입력하거나 기본 메시지를 유지하십시오. 메시지의 최대 길이는 256자입니다.
사용자 자격 증명 또는 클라이언트 인증서로 인증 허용	아니오를 선택하면 사용자는 사용자 자격 증명과 클라이언트 인증서를 모두 사용하여 게이트웨이에 인증해야 합니다. 예를 선택하면 사용자는 사용자 자격 증명이나 클라이언트 인증서를 사용하여 게이트웨이에 인증할 수 있습니다.
인증서 프로파일	
인증서 프로파일	(선택 사항) 포털이 사용자 엔드포인트에서 오는 클라이언트 인증서를 일치시키는 데 사용하는 인증서 프로파일을 선택합니다. 인증서 프로파일을 사용하면 클라이언트의 인증서가 이 프로파일과 일치하는 경우에만 포털이 사용자를 인증합니다. 사용자 자격 증명 또는 클라이언트 인증서로 인증 허용 옵션을 아니오로 설정한 경우 인증서 프로파일을 선택해야 합니다. 사용자 자격 증명 또는 클라이언트 인증서로 인증 허용 옵션을 예로 설정하면 인증서 프로파일은 선택 사항입니다.

GlobalProtect 포털 인증 설정	설명
	인증서 프로파일은 OS와 독립적입니다. 또한 이 프로파일은 암호화된 쿠키를 사용한 인증을 허용하도록 인증 프로파일을 재정의하는 인증 재정의를 활성화한 경우에도 활성화됩니다.

GlobalProtect 포털 포털 데이터 수집 탭

Network > **GlobalProtect** > **Portals** > **<portal-config>** > **Portal Data Collection**을 선택하여 GlobalProtect 앱이 엔드포인트에서 수집하고 사용자가 포털에 성공적으로 로그인한 후 구성 선택 기준 데이터로 보내는 데이터를 정의합니다.

GlobalProtect 포털 데이터 수집 설정	설명
인증서 프로파일	GlobalProtect 포털이 GlobalProtect 앱에서 보낸 컴퓨터 인증서와 일치시키기 위해 사용하는 인증서 프로파일을 선택합니다.
맞춤 수표	앱에서 수집할 사용자 지정 호스트 정보를 정의합니다. • **Windows** - 특정 레지스트리 키 또는 키 값에 대한 검사를 추가합니다. • **Mac** - 특정 Plist 키 또는 키 값에 대한 검사를 추가합니다.

GlobalProtect 포털 에이전트 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트

에이전트 탭을 선택하여 에이전트 구성 설정을 정의합니다. GlobalProtect 포털은 연결이 처음 설정된 후 디바이스에 구성을 배포합니다.

포털이 신뢰할 수 있는 루트 CA(인증 기관) 인증서 및 중간 인증서를 자동으로 배포하도록 지정할 수도 있습니다. 엔드포인트가 GlobalProtect 게이트웨이 및 GlobalProtect Mobile Security Manager가 사용 중인 서버 인증서를 신뢰하지 않는 경우 엔드포인트는 게이트웨이 또는 Mobile Security Manager에 대한 HTTPS 연결을 설정하기 위해 이러한 인증서가 필요합니다. 포털은 여기에서 지정한 인증서를 클라이언트 구성과 함께 클라이언트로 푸시합니다.

신뢰할 수 있는 루트 CA 인증서를 추가하려면 기존 인증서를 추가하거나 새 인증서를 가져옵니다. 클라이언트의 인증서 저장소에 SSL 포워딩 프록시 복호화에 필요한 신뢰할 수 있는 루트 CA 인증서를 (명확하게) 설치하려면 로컬 루트 인증서 저장소에 설치를 선택합니다.

GlobalProtect 앱이 *GlobalProtect* 포털 및 게이트웨이의 *ID*를 확인하는 데 사용하는 신뢰할 수 있는 루트 *CA* 인증서를 지정하십시오. 포털 또는 게이트웨이가 신뢰할 수 있는 루트 *CA*를 발급한 동일한 인증 기관에서 서명하거나 발급하지 않은 인증서를 제시하는 경우 *GlobalProtect* 앱은 포털 또는 게이트웨이와의 연결을 설정할 수 없습니다.

다른 구성이 필요한 여러 유형의 사용자가 있는 경우 이를 지원하기 위해 별도의 에이전트 구성을 생성할 수 있습니다. 포털은 이후에 클라이언트의 사용자 또는 그룹 이름과 OS를 사용하여 배포할 에이전트 구성을 결정합니다. 보안 규칙 평가와 마찬가지로 포털은 목록의 맨 위에서 시작하여 일치 항목을 찾습니다. 포털에서 일치하는 항목을 찾으면 해당 구성을 앱에 전달합니다. 따라서 에이전트 구성이 여러 개인 경우 보다 구체적인 구성(특정 사용자 또는 운영 체제에 대한 구성)이 보다 일반적인 구성보다 우선하도록 구성하는 것이 중요합니다. 위로 이동 및 아래로 이동을 사용하여 구성을 재정렬합니다. 필요에 따라 새 에이전트 구성을 추가합니다. 포털 구성 및 에이전트 구성 생성에 대한 자세한 내용은 GlobalProtect 관리자 안내서의 GlobalProtect 포털을 참조하십시오. 새 에이전트 구성을 추가하거나 기존 구성을 수정하면 구성 창이 열리고 다음 표에 설명된 5개의 탭이 표시됩니다.

- GlobalProtect Portals 에이전트 인증 탭
- GlobalProtect Portals 에이전트 구성 선택 기준 탭
- GlobalProtect 포털 에이전트 내부 탭
- GlobalProtect 포털 에이전트 외부 탭
- GlobalProtect Portals 에이전트 앱 탭
- GlobalProtect 포털 에이전트 HIP 데이터 수집 탭

GlobalProtect Portals 에이전트 인증 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트 > ***<agent-config>*** > 입증

인증 탭을 선택하여 에이전트 구성에 적용되는 인증 설정을 구성합니다.

GlobalProtect Portal 클라이언트 인증 구성 설정	설명
인증 탭	
이름	클라이언트 인증을 위해 이 구성을 설명하는 이름을 입력합니다.
클라이언트 인증서	(선택 사항) 클라이언트 인증서를 엔드포인트에 배포하는 소스를 선택하면 엔드포인트가 인증서를 게이트웨이에 제공합니다. 상호 SSL 인증을 구성하는 경우 클라이언트 인증서가 필요합니다.

GlobalProtect Portal 클라이언트 인증 구성 설정	설명
	모바일 디바이스용 포털 구성에 클라이언트 인증서를 포함하면 클라이언트 인증서 암호가 포털 구성에 저장되기 때문에 게이트웨이 구성에서만 클라이언트 인증서 인증을 사용할 수 있습니다. 또한 클라이언트 인증서는 포털 구성에서 인증서를 검색한 후에만 사용할 수 있습니다. 포털 클라이언트 구성에서 사전 로그온을 위해 SCEP가 구성된 경우 포털은 게이트웨이 인증 및 연결을 위해 시스템 인증서 저장소에 저장된 컴퓨터 인증서를 생성합니다. **SCEP**를 통해 PKI에서 생성된 인증서 대신 방화벽에 대해 로컬인 인증서를 사용하려면 방화벽에 이미 업로드된 인증서를 선택하십시오. 내부 CA를 사용하여 인증서를 엔드포인트에 배포하는 경우 없음(기본값)을 선택합니다. 없음을 선택하면 포털이 인증서를 엔드포인트로 푸시하지 않습니다.
사용자 자격 증명 저장	예를 선택하여 앱에 사용자명과 암호를 저장하거나 아니오를 선택하여 사용자가 연결할 때마다 엔드포인트을 통해 명확하게 또는 수동으로 입력하여 암호를 제공하도록 합니다. 사용자가 연결할 때마다 사용자명만 저장하려면 사용자명만 저장을 선택합니다. 생체 인식 로그인을 허용하려면 사용자 지문으로만을 선택합니다. 엔드포인트에서 생체 인식 로그인이 활성화되면 GlobalProtect는 지문 스캔이 엔드포인트의 신뢰할 수 있는 지문 템플릿과 일치할 때 저장된 사용자 자격 증명을 사용합니다. 권한이 없는 사용자가 민감한 리소스 및 기밀 정보에 더 쉽게 액세스할 수 있으므로 사용자 자격 증명을 저장하지 마십시오. 사용자는 *GlobalProtect*에 연결할 때마다 자격 증명을 수동으로 입력해야 합니다.
인증 재정의	
인증 재정의를 위한 쿠키 생성	암호화된 엔드포인트별 쿠키를 생성하도록 포털을 구성하려면 이 옵션을 선택하십시오. 포털은 사용자가 포털에서 처음 인증한 후 이 쿠키를 엔드포인트로 보냅니다.

GlobalProtect Portal 클라이언트 인증 구성 설정	설명
인증 재정의를 위해 쿠키 허용	유효하고 암호화된 쿠키를 통해 엔드포인트를 인증하도록 포털을 구성하려면 이 옵션을 선택하십시오. 엔드포인트가 유효한 쿠키를 제공하면 포털은 쿠키가 포털에서 암호화되었는지 확인하고 쿠키를 복호화한 다음 사용자를 인증합니다.
쿠키 유효 시간	쿠키가 유효한 시간, 일 또는 주를 지정하십시오. 일반적인 유효 시간은 24시간입니다. 범위는 1–72시간, 1–52주 또는 1–365일입니다. 쿠키가 만료된 후 사용자는 로그인 자격 증명을 입력해야 하며 포털은 이후에 사용자 엔드포인트에 보낼 새 쿠키를 암호화합니다.
쿠키를 암호화/복호화하기 위한 인증서	쿠키 암호화 및 복호화에 사용할 인증서를 선택합니다. 포털과 게이트웨이가 동일한 인증서를 사용하여 쿠키를 암호화하고 복호화하는지 확인하십시오. *(*게이트웨이 클라이언트 구성의 일부로 인증서를 구성하십시오. 네트워크 > GlobalProtect > 게이트웨이 참조).
동적 암호가 필요한 구성 요소(2단계 인증)	
OTP(일회성 암호)와 같은 동적 암호를 지원하도록 GlobalProtect를 구성하려면 사용자가 동적 암호를 입력해야 하는 포털 또는 게이트웨이 유형을 지정합니다. 이중 요소 인증이 활성화되지 않은 경우 GlobalProtect는 로그인 자격 증명(예: AD) 및 인증서를 사용하여 일반 인증을 사용합니다. 2단계 인증에 대해 포털 또는 게이트웨이 유형을 활성화하면 해당 포털 또는 게이트웨이는 초기 포털 인증 후 사용자에게 자격 증명과 두 번째 OTP(또는 기타 동적 암호)를 제출하라는 메시지를 표시합니다. 그러나 인증 재정의도 활성화하면 암호화된 쿠키가 사용자를 인증하는 데 사용되며(사용자가 새 세션에 대해 처음 인증된 후), 따라서 사용자가 자격 증명을 다시 입력해야 하는 요구 사항을 선점합니다. 쿠키는 유효합니다). 따라서 쿠키가 유효한 한 사용자는 필요할 때마다 투명하게 로그인됩니다. 쿠키의 유효 시간을 지정합니다.	
포털	동적 암호를 사용하여 포털에 연결하려면 이 옵션을 선택하십시오.
내부 게이트웨이 - 모두	동적 암호를 사용하여 내부 게이트웨이에 연결하려면 이 옵션을 선택합니다.
외부 게이트웨이 - 수동 전용	동적 암호를 사용하여 수동 게이트웨이로 구성된 외부 게이트웨이에 연결하려면 이 옵션을 선택하십시오.

GlobalProtect Portal 클라이언트 인증 구성 설정	설명
외부 게이트웨이 - 자동 검색	동적 암호를 사용하여 앱이 자동으로 검색할 수 있는 나머지 외부 게이트웨이(수동으로 구성되지 않은 게이트웨이)에 연결하려면 이 옵션을 선택합니다.

GlobalProtect Portals 에이전트 구성 선택 기준 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트 > ***<agent-config>*** > 구성 선택 기준

구성 선택 기준 탭을 선택하여 관리되는 엔드포인트과 관리되지 않는 엔드포인트가 있는 배포에서 엔드포인트 유형을 식별하는 데 사용되는 일치 기준을 구성합니다. 포털은 엔드포인트 유형에 따라 지정된 구성을 엔드포인트로 푸시할 수 있습니다.

GlobalProtect 포털 구성 선택 기준 설정	설명
사용자/사용자 그룹 탭	
OS	이 구성을 수신하는 엔드포인트를 지정하려면 하나 이상의 엔드포인트 운영 체제(OS)를 추가하십시오. 포털은 엔드포인트의 OS를 자동으로 학습하고 클라이언트 구성에서 해당 OS에 대한 세부 정보를 통합합니다. 모든 OS 또는 특정 OS(**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows** 또는 **WindowsUWP**)를 선택할 수 있습니다.
사용자/사용자 그룹	이 구성이 적용되는 특정 사용자 또는 사용자 그룹을 추가합니다. 사용자 그룹을 선택하려면 먼저 그룹 매핑(디바이스 > 사용자 식별 > 그룹 매핑 설정)을 구성해야 합니다. 이 구성을 모든 사용자에게 배포하려면 사용자/사용자 그룹 드롭다운에서 원하는 항목을 선택합니다. 사전 로그온 모드에서 GlobalProtect 앱이 있는 사용자에게만 이 구성을 배포하려면 사용자/사용자 그룹 드롭다운에서 사전 로그온을 선택합니다.
디바이스 확인	

GlobalProtect 포털 구성 선택 기준 설정	설명
디바이스 일련번호가 있는 컴퓨터 계정이 있습니다.	엔드포인트 일련번호가 Active Directory에 있는지의 여부에 따라 일치 기준을 구성합니다.
인증서 프로파일	GlobalProtect 포털이 GlobalProtect 앱에서 보낸 컴퓨터 인증서와 일치시키기 위해 사용하는 인증서 프로파일을 선택합니다.
맞춤 수표	
사용자 정의 검사	일치시킬 사용자 정의 호스트 정보를 정의하려면 이 옵션을 선택하십시오.
레지스트리 키	특정 레지스트리 키에 대한 Windows 엔드포인트을 확인하려면 일치시킬 레지스트리 키를 추가하십시오. 지정된 레지스트리 키 또는 키 값이 없는 엔드포인트만 일치시키려면 키가 존재하지 않거나 지정된 값 데이터와 일치 옵션을 활성화하십시오. 특정 값을 일치시키려면 레지스트리 값 및 값 데이터를 추가하십시오. 지정된 레지스트리 값이 없는 엔드포인트를 일치시키려면 부정을 선택합니다. 부정 옵션을 선택하는 경우 값 데이터 필드를 비워 두어야 합니다. 지정된 레지스트리 값이 없는 GlobalProtect Portal의 사용자 정의 검사에서 레지스트리 값에 대해 부정 옵션을 선택할 수 있습니다(레지스트리 값 없음과 일치). 부정 옵션으로 레지스트리 값을 구성하고 값 데이터 필드를 비워 두면 부정가 레지스트리 값에서 작동합니다. 부정 옵션 및 값 데이터 일치는 상호 배타적이며 값 데이터 및 부정 옵션을 함께 구성할 수 없습니다.
Plist	속성 목록(plist)의 특정 항목에 대한 macOS 엔드포인트을 확인하려면 **Plist** 이름을 추가합니다. 지정된 plist가 없는 엔드포인트만 일치시키려면 **Plist**가 존재하지 않음 옵션을 활성화하십시오. plist 내의 특정 키-값 쌍을 일치시키려면 키 및 해당 값을 추가하십시오. 지정된 키 또는 값이 명시

GlobalProtect 포털 구성 선택 기준 설정	설명
	적으로 없는 엔드포인트를 일치시키려면 무효를 선택하십시오.

GlobalProtect 포털 에이전트 내부 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트 > ***<agent-config>*** > 내부

내부 탭을 선택하여 에이전트 구성에 대한 내부 게이트웨이 설정을 구성합니다.

GlobalProtect 포털 내부 설정	설명
내부 호스트 감지	
내부 호스트 감지	GlobalProtect 앱이 엔터프라이즈 네트워크 내부에 있는지 확인하려면 이 옵션을 선택합니다. 이는 엔터프라이즈 네트워크에 터널이 필요하지 않거나 엔드포인트가 내부 게이트웨이와 통신하도록 구성된 경우 엔드포인트에 적용됩니다. 내부 호스트 탐지 기능을 선택하는 것은 이러한 엔드포인트에 대한 모범 사례입니다. 그러나 내부 게이트웨이 구성은 선택 사항입니다. 사용자가 로그인을 시도하면 앱은 지정된 **IP** 주소를 사용하여 지정된 호스트 이름에 대해 내부 호스트의 역방향 DNS 조회를 수행합니다. 호스트는 연결 가능하지 않아도 되는 참조 지점 역할을 하지만 역방향 DNS 조회는 엔드포인트가 엔터프라이즈 네트워크 내부에 있는 경우에만 성공해야 합니다. 앱이 호스트를 찾으면 엔드포인트가 네트워크 내부에 있고 앱이 내부 게이트웨이(구성된 경우)에 연결하거나 GlobalProtect 앱이 연결 상태를 내부로 표시합니다. 앱이 내부 호스트를 찾지 못하는 경우 엔드포인트는 네트워크 외부에 있고 앱은 외부 게이트웨이 중 하나에 대한 터널을 설정합니다. • IP 주소 유형은 **IPv4**(IPv4 트래픽만), **IPv6**(IPv6 트래픽만) 또는 둘 다일 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 IPv4의 경우 172.16.1.0 또는 IPv6의 경우 21DA:D3:0:2F3b입니다. • **IPv4** 및 **IPv6**을 선택하는 경우 각각에 대해 적절한 IP 주소 유형을 입력합니다.
호스트네임	내부 네트워크 내에서 IP 주소로 해석되는 호스트네임을 입력합니다.
내부 게이트웨이	

GlobalProtect 포털 내부 설정	설명
앱이 액세스를 요청할 수 있는 내부 게이트웨이를 지정하고 HIP 보고서도 제공할 수 있습니다(GlobalProtect Portals 에이전트 데이터 수집 탭에서 HIP가 활성화된 경우).	각각에 대해 다음 정보가 포함된 내부 게이트웨이를 추가합니다. • 이름 - 게이트웨이를 식별하기 위한 최대 31자의 레이블입니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오. • 주소 - 게이트웨이에 대한 방화벽 인터페이스의 IP 주소 또는 FQDN입니다. 이 값은 게이트웨이 서버 인증서의 CN(일반 이름) 및 SAN(지정된 경우)과 일치해야 합니다. 예를 들어 FQDN을 사용하여 인증서를 생성한 경우 여기에 FQDN을 입력해야 합니다. • 소스 주소 - 엔드포인트의 소스 주소 또는 주소 풀입니다. 사용자가 연결할 때 GlobalProtect는 디바이스의 소스 주소를 인식합니다. 소스 주소 풀에 포함된 IP 주소가 있는 GlobalProtect 앱만 이 게이트웨이로 인증하고 HIP 보고서를 보낼 수 있습니다. • **DHCP** 옵션 **43** 코드(Windows 및 Mac만 해당) - 게이트웨이 선택을 위한 DHCP 하위 옵션 코드입니다. 하나 이상의 하위 옵션 코드(십진수)를 지정합니다. GlobalProtect 앱은 하위 옵션 코드로 정의된 값에서 게이트웨이 주소를 읽습니다.

GlobalProtect 포털 에이전트 외부 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트 > ***<agent-config>*** > 외부

외부 탭을 선택하여 에이전트 구성에 대한 외부 게이트웨이 설정을 구성합니다.

GlobalProtect 포털 외부 설정	설명
컷오프 시간(초)	앱이 최상의 게이트웨이를 선택하기 전에 사용 가능한 모든 게이트웨이가 응답할 때까지 기다리는 시간(초)을 지정합니다. 후속 연결 요청의 경우 앱은 차단 전에 응답한 게이트웨이에만 연결을 시도합니다. 값 0은 앱이 앱 탭의 **AppConfigurations**에서 **TCP** 연결 타임아웃을 사용함을 의미합니다(범위는 0~10, 기본값은 5).
외부 게이트웨이	
회사 네트워크에 없는 동안 터널을 설정할 때 앱이 연결을 시도할 수 있는 방화벽 목록을 지정합니다.	각각에 대해 다음 정보를 포함하는 외부 게이트웨이를 추가합니다. • 이름 - 게이트웨이를 식별하기 위한 최대 31자의 레이블입니다. 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.

GlobalProtect 포털 외부 설정	설명
	• 주소 - 게이트웨이가 구성된 방화벽 인터페이스의 IP 주소 또는 FQDN입니다. 값은 게이트웨이 서버 인증서의 CN(지정된 경우 SAN)과 일치해야 합니다. 예를 들어 FQDN을 사용하여 인증서를 생성한 경우 여기에 FQDN도 입력해야 합니다. • 소스 리전 - 엔드포인트의 소스 리전입니다. 사용자가 연결할 때 GlobalProtect는 엔드포인트 지역을 인식하고 사용자가 해당 지역에 대해 구성된 게이트웨이에만 연결할 수 있도록 허용합니다. 게이트웨이 선택의 경우 소스 지역이 먼저 고려된 다음 게이트웨이 우선순위가 고려됩니다. • 우선 순위 - 앱에서 사용할 게이트웨이를 결정하는 데 도움이 되도록 값(높음, 높음, 중간, 낮음, 가장 낮음 또는 수동만 해당)을 선택합니다. 수동은 엔드포인트에서 자동 검색이 활성화된 경우에만 GlobalProtect 앱이 이 게이트웨이에 연결을 시도하는 것을 방지합니다. 앱은 먼저 가장 높음, 높음 또는 보통 우선 순위로 지정된 모든 게이트웨이에 연결하고 가장 빠른 응답을 제공하는 게이트웨이와 터널을 설정합니다. 우선 순위가 더 높은 게이트웨이에 연결할 수 없는 경우 앱은 다음으로 우선 순위 값이 더 낮은 추가 게이트웨이에 연결합니다(수동 전용 게이트웨이 제외). • 수동 - 사용자가 게이트웨이를 수동으로 선택(또는 전환)할 수 있도록 하려면 이 옵션을 선택합니다. GlobalProtect 앱은 수동으로 구성된 모든 외부 게이트웨이에 연결할 수 있습니다. 앱이 다른 게이트웨이에 연결되면 기존 터널의 연결이 끊어지고 새 터널이 설정됩니다. 수동 게이트웨이는 기본 게이트웨이와 다른 인증 메커니즘을 가질 수도 있습니다. 엔드포인트가 다시 시작되거나 재발견이 수행되면 GlobalProtect 앱이 기본 게이트웨이에 연결됩니다. 이 기능은 사용자 그룹이 네트워크의 보안 세그먼트에 액세스하기 위해 특정 게이트웨이에 일시적으로 연결해야 하는 경우에 유용합니다.
타사 VPN	
타사 VPN	GlobalProtect가 선택한 타사 VPN 클라이언트를 무시하도록 GlobalProtect 앱에 지시하여 GlobalProtect가 해당 VPN 클라이언트와 충돌하지 않도록 하려면 VPN 클라이언트의 이름을 추가합니다. 목록에서 이름을 선택하거나 제공된 필드에 이름을 입력합니다. GlobalProtect는 이 기능을 구성하는 경우 지정된 VPN 클라이언트에 대한 경로 설정을 무시합니다.

GlobalProtect Portals 에이전트 앱 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트 > ***<agent-config>*** > 앱

앱 탭을 선택하여 최종 사용자가 시스템에 설치된 GlobalProtect 앱과 상호 작용하는 방식을 지정합니다. 생성한 다양한 GlobalProtect 에이전트 구성에 대해 다른 앱 설정을 정의할 수 있습니다. GlobalProtect 앱 사용자 정의 설정에 대한 최신 업데이트에 대한 자세한 내용은 GlobalProtect 관리자 안내서를 참조하십시오.

GlobalProtect 앱 구성 설정	설명
환영 페이지	최종 사용자가 GlobalProtect에 연결한 후 표시할 시작 페이지를 선택하십시오. 공장 기본 페이지 또는 사용자 정의 페이지 가져오기를 선택할 수 있습니다. 기본값은 없음입니다.
앱 구성	
연결 방법	• 주문형(수동 사용자 시작 연결) - 사용자는 GlobalProtect 앱을 시작한 다음 포털에 대한 연결을 시작하고 GlobalProtect 자격 증명을 입력해야 합니다. 이 옵션은 주로 원격 액세스 연결에 사용됩니다. • 사용자 로그온(항상 켜짐) - GlobalProtect 앱은 사용자가 엔드포인트에 로그인한 후 자동으로 포털에 대한 연결을 설정합니다. 포털은 앱에 적절한 에이전트 구성을 제공하여 응답합니다. 이후 앱은 포털에서 수신한 에이전트 구성에 지정된 게이트웨이 중 하나로 터널을 설정합니다. • 사전 로그온 - 사전 로그온은 원격 Windows 및 Mac 사용자가 항상 회사 네트워크에 연결되어 있는지 확인하고 사용자가 엔드포인트에 로그인할 때 사용자 로그온 스크립트 및 도메인 정책 적용을 활성화합니다. 엔드포인트는 마치 내부 네트워크인 것처럼 회사 네트워크에 연결할 수 있기 때문에 사용자는 비밀번호가 만료될 때 새 비밀번호로 로그인하거나 비밀번호를 잊어버린 경우 비밀번호 복구에 대한 도움을 받을 수 있습니다. 사전 로그온을 통해 GlobalProtect 앱은 사용자가 엔드포인트에 로그인하기 전에 GlobalProtect 게이트웨이에 대한 VPN 터널을 설정합니다. 엔드포인트는 사전 설치된 컴퓨터 인증서를 게이트웨이에 제출하여 인증을 요청합니다. 그런 다음 Windows 엔드포인트에서 게이트웨이는 사전 로그온 사용자의 VPN 터널을 엔드포인트에 로그인한 사용자명으로 재할당합니다. Mac 엔드포인트에서 앱은 연결을 끊고 사용자를 위한 새 VPN 터널을 만듭니다. 두 가지 사전 로그온 연결 방법이 있으며 둘 중 하나는 사용자가 엔드포인트에 로그인하기 전에 발생하는 동일한 사전 로그온 기능을 활성화합니다. 그러나 사용자가 엔드포인트

GlobalProtect 앱 구성 설정	설명
	에 로그인한 후 사전 로그온 연결 방법은 GlobalProtect 앱 연결이 설정된 시기를 결정합니다. • 사전 로그온**(**항상 켜짐**)** - GlobalProtect a pp가 자동으로 GlobalProtect 게이트웨이 연결 및 재연결을 시도합니다. 모바일 디바이스는 사전 로그온 기능을 지원하지 않으므로 이 연결 방법이 지정된 경우 기본적으로 사용자 로그온**(**항상 켜짐**)** 연결 방법이 사용됩니다. • 사전 로그온 후 **On-demand** - 사용자는 GlobalProtect 앱을 시작한 다음 수동으로 연결을 시작해야 합니다. 모바일 디바이스는 사전 로그온 기능을 지원하지 않으므로 이 연결 방법이 지정된 경우 기본적으로 주문형**(**수동 사용자 시작 연결**)** 연결 방법이 사용됩니다.
GlobalProtect 앱 구성 새로 고침 인터벌(시간)	GlobalProtect 포털이 앱 구성의 다음 새로 고침을 시작하기 전에 대기하는 시간을 지정합니다(범위는 1~168, 기본값은 24).
사용자가 GlobalProtect 앱을 비활성화하도록 허용	사용자가 GlobalProtect 앱을 비활성화할 수 있는지의 여부와 허용되는 경우 앱을 비활성화하기 전에 수행해야 하는 작업(있는 경우)을 지정합니다. • 허용 - 모든 사용자가 필요에 따라 GlobalProtect 앱을 비활성화할 수 있습니다. • 허용 안 함 - 최종 사용자가 GlobalProtect 앱을 비활성화하도록 허용하지 않습니다.

GlobalProtect 앱 구성 설정	설명
	• 댓글로 허용 - 사용자가 엔드포인트에서 GlobalProtect 앱을 비활성화하도록 허용하지만 앱 비활성화 이유를 제출하도록 요구합니다. GlobalProtect 앱은 사용자에게 다음을 묻는 메시지를 표시합니다. • 앱 연결을 끊는 이유를 지정합니다. • 느린 인터넷 속도 또는 대기 시간과 같이 표시되는 목록에서 이유를 선택하십시오. 연결 해제 이유는 ***GlobalProtect*** 연결을 해제하는 다음 이유 표시***(***상시 작동 모드***)***를 구성한 경우에만 표시됩니다. 연결 끊김 이유를 표시하도록 *GlobalProtect* 앱을 구성하지 않은 경우 최종 사용자에게 앱 연결을 끊는 이유를 제공하라는 메시지가 표시됩니다. • 암호로 허용 - 사용자가 암호를 입력하여 GlobalProtect 앱을 비활성화하도록 허용합니다. 이 옵션을 사용하려면 사용자가 암호와 같이 입력할 때 표시되지 않는 암호 값을 입력하고 확인해야 합니다. 일반적으로 관리자는 계획되지 않았거나 예상치 못한 이벤트로 인해 사용자가 GlobalProtect VPN을 사용하여 네트워크에 연결하지 못하도록 방지하기 전에 사용자에게 암호를 제공합니다. 이메일을 통해 또는 조직 웹사이트에 게시하여 암호를 제공할 수 있습니다. • 티켓으로 허용 - 이 옵션은 사용자가 GlobalProtect를 비활성화하려고 시도한 후 엔드포인트가 8자 16진수 티켓 요청 번호를 표시하는 시도-응답 메커니즘을 활성화합니다. 사용자는 이 번호를 제공하기 위해 방화벽 관리자 또는 지원 팀에 연락해야 합니다(보안을 위해 전화를 사용하는 것이 좋습니다). 방화벽(**Network** > **GlobalProtect** > **Portals**)에서 관리자 또는 지원 담당자는 티켓 생성을 클릭하고 티켓 요청 번호를 입력하여 티켓 번호(8자리 16진수도 포함)를 얻을 수 있습니다. 관리자 또는 지원 담당자가 이 티켓 번호를 사용자에게 제공하면 사용자가 이를 챌린지 필드에 입력하여 앱을 비활성화합니다.

GlobalProtect 앱 구성 설정	설명
사용자가 GlobalProtect 앱을 제거하도록 허용(Windows만 해당)	사용자가 GlobalProtect 앱을 제거할 수 있는지의 여부와 허용되는 경우 앱을 제거하기 전에 수행해야 하는 작업(있는 경우)을 지정합니다. • 허용 - 모든 사용자가 필요에 따라 GlobalProtect 앱을 제거하도록 허용합니다. • 허용 안 함 - 최종 사용자가 GlobalProtect 앱을 제거하도록 허용하지 않습니다. • 암호로 허용 - GlobalProtect 앱을 제거하려면 암호를 적용합니다. 이 옵션을 사용하려면 제거를 계속하기 전에 사용자가 암호를 입력하고 확인해야 합니다. 이메일을 통해 또는 조직 웹사이트에 게시하여 비밀번호를 제공할 수 있습니다. 이 옵션을 사용하려면 콘텐츠 릴리스 버전 8196-5685 이상이 필요합니다.
사용자가 GlobalProtect 앱을 업그레이드하도록 허용	최종 사용자가 GlobalProtect 앱 소프트웨어를 업그레이드할 수 있는지의 여부와 업그레이드할 수 있는 경우 업그레이드 시기를 선택할 수 있는지의 여부를 지정합니다. • 허용 안 함 - 사용자가 앱 소프트웨어를 업그레이드하지 못하도록 합니다. • 수동으로 허용 - 사용자가 GlobalProtect 앱에서 버전 확인을 선택하여 수동으로 업그레이드를 확인하고 시작할 수 있도록 허용합니다. • 프롬프트로 허용(기본값) - 방화벽에서 새 버전이 활성화될 때 사용자에게 프롬프트를 표시하고 사용자가 편리할 때 소프트웨어를 업그레이드할 수 있도록 합니다. • 명확하게 허용 - 포털에서 새 버전을 사용할 수 있을 때마다 앱 소프트웨어를 자동으로 업그레이드합니다. • 내부 - 포털에서 새 버전을 사용할 수 있을 때마다 앱 소프트웨어를 자동으로 업그레이드하지만 엔드포인트가 내부적으로 회사 네트워크에 연결될 때까지 기다립니다. 이는 낮은 대역폭 연결을 통한 업그레이드로 인한 지연을 방지합니다.
사용자가 GlobalProtect 앱에서	사용자가 Globalprotect 앱에서 수동으로 로그아웃하도록 허용할지의 여부를 지정합니다.

GlobalProtect 앱 구성 설정	설명
로그아웃할 수 있도록 허용(Windows, macOS, iOS, Android 및 Chrome만 해당)	• 예(기본값) - 필요에 따라 모든 사용자가 GlobalProtect 앱에서 로그아웃하도록 허용합니다. • 아니오 - 최종 사용자가 GlobalProtect 앱에서 로그아웃하도록 허용하지 않습니다. 이 옵션을 사용하려면 콘텐츠 릴리스 버전 8196-5685 이상이 필요합니다.
Single Sign-On(SSO) 사용(Windows)	SSO(Single Sign-On)를 비활성화하려면 아니오를 선택합니다. SSO가 활성화된 경우(기본값) GlobalProtect 앱은 자동으로 Windows 로그인 자격 증명을 사용하여 인증한 다음 GlobalProtect 포털 및 게이트웨이에 연결합니다. GlobalProtect는 타사 자격 증명을 래핑하여 Windows 로그인 자격 증명을 래핑하는 데 타사 자격 증명 공급자를 사용하는 경우에도 Windows 사용자가 인증하고 연결할 수 있도록 합니다.
스마트 카드 PIN에 싱글 사인온 사용(Windows) (Windows 10 이상) 콘텐츠 릴리스 버전 8451-6911 이상 및 GlobalProtect 앱 버전 6.0.0 이상이 필요합니다.	이 설정을 사용하면 스마트 카드를 사용하여 SSO(Single Sign-On)를 통해 인증하는 최종 사용자가 원활한 SSO 환경을 위해 GlobalProtect 앱에 스마트 카드 PIN(개인 식별 번호)을 다시 입력하지 않고도 연결할 수 있습니다. GlobalProtect는 스마트 카드 공급자가 허용하는 경우에만 PIN을 캐시할 수 있습니다. 스마트 카드 PIN에 SSO 사용을 사용하도록 설정하려면 먼저 최종 사용자 엔드포인트에 미리 배포된 설정을 설정해야 합니다. 그런 다음 이 설정을 사용하려면 예를 선택합니다.
Single Sign-On(SSO) 사용(macOS)	SSO(Single Sign-On)를 비활성화하려면 아니오를 선택합니다. SSO를 활성화하면(기본값) GlobalProtect 앱은 자동으로 macOS 로그인 자격 증명을 사용하여 인증한 다음 GlobalProtect 포털 및 게이트웨이에 연결합니다. 이 옵션을 사용하려면 콘텐츠 릴리스 버전 8196-5685 이상이 필요합니다.
로그아웃 시 Single Sign-On(SSO) 자격 증명 지우기 (Windows만 해당)	사용자가 로그아웃할 때 Single Sign-On 자격 증명을 유지하려면 아니오를 선택합니다. 예(기본값)를 선택하여 해당 항목을 지우고 사용자가 다음에 로그인할 때 자격 증명을 입력하도록 합니다.
Kerberos 인증 실패 시 기본 인증 사용	Kerberos 인증만 사용하려면 아니오를 선택합니다. Kerberos 인증에 실패한 후 기본 인증 방법을 사용하여 인증을 다시

GlobalProtect 앱 구성 설정	설명
	시도하려면 예(기본값)를 선택합니다. 이 기능은 Mac 및 Windows 엔드포인트에서만 지원됩니다.
SAML 인증에 기본 브라우저 사용 (콘텐츠 릴리스 버전 8284-6139 이상에서 GlobalProtect 앱 5.2 이상 필요)	SAML(보안 어설션 마크업 언어) 인증을 통해 최종 사용자를 인증하도록 GlobalProtect 포털을 구성한 경우 예를 선택하여 사용자가 Chrome, Firefox 또는 Safari와 같은 기본 시스템 브라우저에서 저장된 사용자 자격 증명을 사용하여 GlobalProtect에 대해 동일한 로그인을 활용하여 SAML 지원 애플리케이션에 연결할 수 있도록 합니다. 클라우드 인증 서비스와 함께 SAML을 사용하는 경우 이 설정을 활성화해야 합니다. 이 설정을 사용하도록 설정하는 경우 SAML 인증에 기본 시스템 브라우저를 사용하도록 Windows, macOS, Linux, Android 및 iOS 엔드포인트에서 기본 브라우저를 사용하도록 배포 전 설정도 변경해야 합니다. 각 연결이 기본 브라우저에서 새 탭을 열지 못하도록 하려면 인증 재정의를 구성합니다.
VPN 연결 타임아웃 자동 복원	0에서 180 사이의 타임아웃 값을 분 단위로 입력하여 네트워크 불안정 또는 엔드포인트 상태 변경으로 인해 터널 연결이 끊어졌을 때 GlobalProtect 앱이 수행하는 작업을 지정합니다. 기본값은 30입니다. • 0 - GlobalProtect가 터널 연결이 끊긴 후 터널 재설정을 시도하지 않도록 이 기능을 비활성화합니다. • 1-180 - 여기에서 지정한 타임아웃 값을 초과하지 않는 기간 동안 터널이 다운된 경우 GlobalProtect가 터널 연결 재설정을 시도하도록 이 기능을 활성화합니다. 예를 들어 제한 시간 값이 30분인 경우 GlobalProtect는 터널 연결이 45분 동안 끊어지면 터널 재설정을 시도하지 않습니다. 그러나 터널의 연결이 15분 동안 끊어지면 시간이 제한 시간

GlobalProtect 앱 구성 설정	설명
	값을 초과하지 않았기 때문에 GlobalProtect가 다시 연결을 시도합니다. *Always-On VPN*을 사용하면 타임아웃 값이 만료되기 전에 사용자가 외부 네트워크에서 내부 네트워크로 전환하면 *GlobalProtect*가 네트워크 검색을 수행하지 않습니다. 결과적으로 *GlobalProtect*는 마지막으로 알려진 외부 게이트웨이에 대한 터널을 재설정합니다. 내부 호스트 탐지를 트리거하려면 사용자가 *GlobalProtect* 콘솔에서 네트워크 재발견을 선택해야 합니다.
VPN 연결 복원 시도 사이의 대기 시간(최소)	**VPN** 연결 타임아웃의 자동 복원을 활성화할 때 GlobalProtect 앱이 마지막으로 연결된 게이트웨이와의 연결 재설정 시도 사이에 대기하는 시간(초)을 입력하십시오. 네트워크 상태에 따라 더 길거나 더 짧은 대기 시간을 지정하십시오. 범위는 1~60초입니다. 기본값은 5입니다.
엔드포인트 트래픽 정책 적용 (Windows 10 이상 및 macOS 11 이상만 해당) 콘텐츠 릴리스 버전 8450-6909 이상 및 GlobalProtect 앱 6.0.0 이상이 필요합니다.	엔드포인트가 GlobalProtect에 연결될 때 물리적 어댑터의 트래픽을 방지하도록 엔드포인트 트래픽 정책 적용을 구성합니다. 이는 악의적인 인바운드 연결, 물리적 어댑터에 바인딩하여 터널을 우회하는 애플리케이션, 라우팅 테이블을 변조하여 GlobalProtect 터널을 우회하는 최종 사용자와 같은 보안을 방해하려는 시도로부터 보호합니다. 다음 옵션 중 하나를 선택하여 엔드포인트 트래픽 정책 적용을 구성합니다. • 아니오 - 엔드포인트 트래픽 정책 적용을 사용하지 않도록 설정합니다. 이것이 기본 설정입니다. • 터널 **IP** 주소 유형을 기반으로 하는 **TCP/UDP** 트래픽 - TCP/UDP 트래픽에 대한 엔드포인트 트래픽 정책 적용을 사용하도록 설정합니다. 이 기능은 터널 IP 주소 유형에 따라 트래픽에 대해 사용하도록 설정됩니다. 터널이 IPv4인 경우 이 기능은 IPv4 트래픽에만 적용됩니다. 터널이 IPv6인 경우 이 기능은 IPv6 트래픽에만 적용됩니다. • 모든 **TCP/UDP** 트래픽 - 터널 IP 주소 유형에 관계없이 모든 TCP/UDP 트래픽에 대해 엔드포인트 트래픽 정책 적용을 사용하도록 설정합니다. 터널 IP 주소 유형이 IPv4인 경우 엔드포인트 트래픽 정책 적용은 모든 TCP/UDP(IPv4 또는 IPv6) 트래픽에 적용됩니다. 터널 IP 주소 유형이 IPv6인

GlobalProtect 앱 구성 설정	설명
	경우 엔드포인트 트래픽 정책 적용은 모든 TCP/UDP(IPv4 또는 IPv6) 트래픽에 적용됩니다. • 모든 트래픽 - 터널 IP 주소 유형에 관계없이 모든 TCP, UDP, ICMP 및 기타 모든 프로토콜에 대해 엔드포인트 트래픽 정책 적용을 사용하도록 설정합니다.
네트워크 액세스를 위해 GlobalProtect 연결 적용	모든 네트워크 트래픽이 GlobalProtect 터널을 통과하도록 하려면 예를 선택합니다. 네트워크 액세스에 GlobalProtect가 필요하지 않고 GlobalProtect가 비활성화되거나 연결이 끊긴 경우에도 사용자가 인터넷에 계속 액세스할 수 있는 경우 아니오(기본값)를 선택합니다. 트래픽이 차단되기 전에 사용자에게 지침을 제공하려면 트래픽 차단 알림 메시지를 구성하고 선택적으로 메시지를 표시할 시기를 지정합니다(트래픽 차단 알림 지연). 종속 포털과의 연결을 설정하는 데 필요한 트래픽을 허용하려면 종속 포털 예외 타임아웃를 지정합니다. 사용자는 제한 시간이 만료되기 전에 포털에서 인증해야 합니다. 추가 지침을 제공하려면 종속 포털 감지 메시지를 구성하고 선택적으로 메시지를 표시할 시기를 지정합니다(캡티브 포털 알림 지연). 대부분의 경우 기본 선택인 ***No***를 사용합니다. 예를 선택하면 앱이 기업 내부의 내부 게이트웨이 또는 기업 네트워크 외부의 외부 게이트웨이에 연결될 때까지 엔드포인트에서 들어오고 나가는 모든 네트워크 트래픽이 차단됩니다.
네트워크 액세스에 대해 GlobalProtect 연결 적용이 활성화되고 GlobalProtect 연결이 설정되지 않은 경우 지정된 호스트/네트워크에 대한 트래픽 허용	원하는 경우 네트워크 액세스에 대해 GlobalProtect를 적용하지만 연결이 설정되지 않은 경우 액세스를 허용하려는 최대 10개의 IP 주소 또는 네트워크 세그먼트를 구성할 수 있습니다. 여러 값을 쉼표로 구분하고 항목 사이에 공백을 추가하지 마십시오. 제외를 사용하면 GlobalProtect 연결이 끊긴 경우 사용자가 로컬 리소스에 액세스할 수 있으므로 사용자 경험이 향상될 수 있습니다. 예를 들어, GlobalProtect가 연결되지 않은 경우 GlobalProtect는 링크 로컬 주소를 제외하여 로컬 네트워크 세그먼트 또는 브로드캐스트 도메인에 대한 액세스를 허용할 수 있습니다.
네트워크 액세스에 대해 GlobalProtect 연결 적용이 활성화되고 GlobalProtect	네트워크 액세스에 GlobalProtect 연결을 적용할 때 액세스를 허용하는 FQDN(정규화된 도메인 이름)을 지정합니

GlobalProtect 앱 구성 설정	설명
연결이 설정되지 않은 경우 지정된 FQDN에 대한 트래픽 허용 (Windows 및 macOS 10.15.4 이상) 콘텐츠 릴리스 버전 8284-6139 이상과 GlobalProtect 앱 5.2 이상이 필요합니다.	다. 네트워크 액세스에 대해 GlobalProtect 연결을 적용하고 GlobalProtect가 연결을 설정할 수 없는 경우 액세스를 허용하려는 최대 40개의 정규화된 도메인 이름을 구성할 수 있습니다. FQDN 제외를 구성하면 GlobalProtect의 연결이 끊어질 때 최종 사용자가 특정 리소스에 액세스할 수 있도록 허용하여 사용자 환경을 개선할 수 있습니다. 예를 들어 엔드포인트은 네트워크 액세스에 대한 GlobalProtect 적용 기능을 사용하도록 설정한 경우에도 인증 목적으로 ldP(클라우드 호스팅 ID 공급자) 또는 원격 디바이스 관리 서버와 통신할 수 있습니다. *macOS*의 최근 변경으로 인해 한 번에 로드되는 여러 네트워크 확장에 대해 *FQDN* 제외를 사용하여 *GlobalProtect* 연결을 적용하면 *DnsClient.Net*, 네트워크 액세스에 대해 ***GlobalProtect*** 연결 적용이 활성화되고 ***GlobalProtect*** 연결이 설정되지 않은 경우 지정된 ***FQDN***에 대한 트래픽 허용 설정이 활성화된 *GlobalProtect, Cortex XDR* 실행 중인 환경과 같이 특정 상황에서 작동하지 않습니다.
종속 포털 예외 타임아웃(초)	네트워크 액세스에 대해 GlobalProtect를 적용하지만 사용자가 종속 포털에 연결할 수 있는 충분한 시간을 허용하는 유예 기간을 제공하려면 타임아웃을 초 단위로 지정합니다(범위는 0~3600). 예를 들어 값 60은 GlobalProtect가 종속 포털을 감지한 후 1분 이내에 사용자가 종속 포털에 로그인해야 함을 의미합니다. 값 0은 GlobalProtect가 사용자가 종속 포털에 연결하는 것을 허용하지 않고 즉시 액세스를 차단함을 의미합니다.
종속 포털 감지 시 기본 브라우저에서 웹 페이지 자동 실행	사용자가 종속 포털에 원활하게 로그인할 수 있도록 종속 포털 감지 시 기본 웹 브라우저를 자동으로 시작하려면 기본 웹 브라우저가 시작될 때 웹 트래픽(최대 길이는 256자)을 실시하는 초기 연결 시도에 사용할 웹사이트의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 입력하십시오. 그러면 종속 포털이 이 웹사이트 연결 시도를 가로채고 기본 웹 브라우저를 종속 포털 로그인 페이지로 리디렉션합니다. 이 필드가 비어 있으면(기본값) GlobalProtect는 종속 포털 감지 시 기본 웹 브라우저를 자동으로 시작하지 않습니다.
트래픽 차단 알림 지연(초)	알림 메시지를 표시할 시기를 결정하려면 값을 초 단위로 지정하십시오. GlobalProtect는 네트워크에 연결할 수 있는 후 알림

GlobalProtect 앱 구성 설정	설명
	을 표시하기 위해 카운트다운을 시작합니다(범위는 5 ~ 120, 기본값은 15).
트래픽 차단 알림 메시지 표시	네트워크 액세스에 GlobalProtect가 필요할 때 메시지를 표시할지의 여부를 지정합니다. 메시지를 비활성화하려면 아니오를 선택합니다. 예를 선택하여 메시지를 활성화합니다(GlobalProtect는 GlobalProtect의 연결이 끊어졌을 때 메시지를 표시하지만 네트워크에 연결할 수 있음을 감지합니다.)
트래픽 차단 알림 메시지	네트워크 액세스에 GlobalProtect가 필요할 때 사용자에게 표시할 알림 메시지를 사용자 정의합니다. GlobalProtect는 GlobalProtect의 연결이 끊겼지만 네트워크에 연결할 수 있음을 감지하면 메시지를 표시합니다. 메시지는 트래픽을 차단하는 이유를 나타내고 연결 방법에 대한 지침을 제공할 수 있습니다. 예: `##### ###### ## GlobalProtect# #####.` 메시지는 512자 이하여야 합니다.
사용자가 트래픽 차단 알림을 닫도록 허용	트래픽 차단 알림을 항상 표시하려면 아니오를 선택합니다. 기본적으로 값은 사용자가 알림을 해제할 수 있음을 의미하는 예로 설정됩니다.
종속 포털 감지 메시지 표시	GlobalProtect가 종속 포털을 감지할 때 메시지를 표시할지의 여부를 지정합니다. 예를 선택하여 메시지를 표시합니다. 메시지를 표시하지 않으려면 아니오(기본값)를 선택합니다(GlobalProtect가 종속 포털을 감지할 때 GlobalProtect는 메시지를 표시하지 않음). 종속 포털 감지 메시지를 활성화하면 종속 포털 예외 타임아웃 *85*초 전에 메시지가 나타납니다. 따라서 *Capture Portal* 예외 타임아웃이 *90*초 이하인 경우 종속 포털이 감지된 후 *5*초 후에 메시지가 나타납니다.
종속 포털 감지 메시지	GlobalProtect가 종속 포털에 연결하기 위한 추가 지침을 제공하는 네트워크를 감지할 때 사용자에게 표시할 알림 메시지를 사용자 정의합니다. 예:

GlobalProtect 앱 구성 설정	설명
	`GlobalProtect# #### ### # ### ##### #### ## ## ######. ### #### ### ####. ## ### #### GlobalProtect# ## ### #### ## ######.` 메시지는 512자 이하여야 합니다.
종속 포털 알림 지연(초)	종속 포털 감지 메시지를 활성화하면 GlobalProtect가 감지 메시지를 표시하는 종속 포털 감지 후 지연 시간(초 단위)을 지정할 수 있습니다(범위는 1~120, 기본값은 5).
클라이언트 인증서 저장소 조회	앱이 개인 인증서 저장소에서 조회하는 인증서 유형을 선택합니다. GlobalProtect 앱은 인증서를 사용하여 포털 또는 게이트웨이에 인증한 다음 GlobalProtect 게이트웨이에 대한 VPN 터널을 설정합니다. • 사용자 - 사용자 계정에 로컬인 인증서를 사용하여 인증합니다. • 머신 - 엔드포인트에 로컬인 인증서를 사용하여 인증합니다. 이 인증서는 엔드포인트을 사용하도록 허용된 모든 사용자 계정에 적용됩니다. • 사용자 및 시스템(기본값) - 사용자 인증서와 시스템 인증서를 사용하여 인증합니다.
SCEP 인증서 갱신 기간(일)	이 메커니즘은 인증서가 실제로 만료되기 전에 SCEP 생성 인증서를 갱신하기 위한 것입니다. 포털이 PKI 시스템의 SCEP 서버에서 새 인증서를 요청할 수 있는 인증서 만료 전 최대 일수를 지정합니다(범위는 0~30, 기본값은 7). 값이 0이면 포털이 클라이언트 구성을 새로 고칠 때 클라이언트 인증서를 자동으로 갱신하지 않습니다. 앱에서 새 인증서를 받으려면 사용자가 갱신 기간 동안 로그인해야 합니다(사용자가 로그인하지 않는 한 포털은 이 갱신 기간 동안 사용자에 대한 새 인증서를 요청하지 않습니다). 예를 들어 클라이언트 인증서의 유효 시간이 90일이고 이 인증서 갱신 기간이 7일이라고 가정합니다. 사용자가 인증서 유효 시간의 마지막 7일 동안 로그인하면 포털에서 인증서를 생성하고 새로 고쳐진 클라이언트 구성과 함께 인증서를 다운로드합니다. GlobalProtect 앱 구성 새로 고침 인터벌(시간)을 참조하십시오.
클라이언트 인증서에 대한 확장 키 사용 OID	이 옵션을 사용하면 macOS 또는 Windows 엔드포인트에 여러 인증서가 설치된 경우 인증서 선택 프로세스를 단순화하

GlobalProtect 앱 구성 설정	설명
(Windows 및 macOS 전용)	고 개선하기 위해 선택할 클라이언트 인증서를 결정하는 데 GlobalProtect에서 사용할 개체 식별자(OID)를 제공할 수 있습니다. 기본적으로 GlobalProtect는 클라이언트 인증 목적(OID 1.3.6.1.5.5.7.3.2)을 지정하는 인증서에 대해 인증서를 자동으로 필터링하므로 클라이언트 인증과 연결된 OID를 지정할 필요가 없습니다. 그러나 GlobalProtect가 선택할 인증서를 구별하기 위해 다른 OID를 사용하려는 경우 인증서를 생성할 때 다른 인증서 사용을 지정한 다음 클라이언트 인증서에 대한 확장 키 사용 **OID**를 해당 OID로 설정할 수 있습니다.. 가장 일반적으로 사용되는 OID 중 일부는 다음과 같습니다. • 1.3.6.1.5.5.7.3.1—서버 인증 • 1.3.6.1.5.5.7.3.3—코드 서명 • 1.3.6.1.5.5.7.3.4—이메일 보호 • 1.3.6.1.5.5.7.3.5—IPSec 엔드 시스템 • 1.3.6.1.5.5.7.3.6 - IPSec 터널 • 1.3.6.1.5.5.7.3.7—IPSec 사용자 • 1.3.6.1.5.5.7.3.8—타임스탬프 • 1.3.6.1.5.5.7.3.9—OCSP 서명
스마트 카드 제거 시 연결 유지 (Windows만 해당)	사용자가 클라이언트 인증서가 포함된 스마트 카드를 제거할 때 연결을 유지하려면 예를 선택합니다. 사용자가 스마트 카드를 제거할 때 연결을 종료하려면 아니오(기본값)를 선택합니다.
Advanced 보기 활성화	앱의 사용자 인터페이스를 기본 최소 보기(기본적으로 활성화됨)로 제한하려면 아니오를 선택합니다.
사용자가 시작 페이지를 닫을 수 있도록 허용	사용자가 연결을 시작할 때마다 시작 페이지가 나타나도록 하려면 아니오를 선택합니다. 이 제한은 사용자가 규정 준수를 유지하기 위해 조직에서 요구할 수 있는 이용 약관과 같은 중요한 정보를 무시하는 것을 방지합니다.
터널을 만들기 전에 사용자가 사용 약관에 동의하도록 설정	예를 선택하여 최종 사용자가 회사 정책을 준수하기 위해 사용 약관에 동의하도록 요구하고 GlobalProtect에 연결하기 전에 회사의 서비스 약관을 검토할 페이지를 보려면 예를 선택합니다.

GlobalProtect 앱 구성 설정	설명
	이 옵션을 예로 설정하기 전에 네트워크 > **GlobalProtect** > 포털 > ***<portal_config*** > **General)**을 통해 GlobalProtect 시작 페이지를 구성해야 합니다.
네트워크 재발견 옵션 활성화	사용자가 네트워크 재검색을 수동으로 시작하지 못하도록 하려면 아니오를 선택합니다.
호스트 프로파일 다시 제출 옵션 활성화	사용자가 최신 HIP의 재제출을 수동으로 트리거하지 못하도록 하려면 아니오를 선택합니다.
사용자가 포털 주소를 변경하도록 허용	GlobalProtect 앱의 홈 탭에서 포털 필드를 비활성화하려면 아니오를 선택합니다. 그러나 사용자는 연결할 포털을 지정할 수 없으므로 Windows 레지스트리 또는 Mac plist에 기본 포털 주소를 제공해야 합니다. • **Windows** 레지스트리 - 키 ##이 있는 `HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` • **Mac plist**—`/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` ## 포함) 포털 주소 사전 배포에 대한 자세한 내용은 GlobalProtect 관리자 안내서에서 사용자 정의 가능한 앱 설정을 참조하십시오.
사용자가 잘못된 Portal Server 인증서를 계속 사용하도록 허용	포털 인증서가 유효하지 않은 경우 앱이 포털과 연결하지 못하도록 하려면 아니오를 선택합니다.
GlobalProtect 아이콘 표시	엔드포인트에서 GlobalProtect 아이콘을 숨기려면 아니오를 선택합니다. 아이콘이 숨겨져 있으면 사용자는 문제 해결 정보 보기, 암호 변경, 네트워크 재발견 또는 주문형 연결 수행과 같은 특정 작업을 수행할 수 없습니다. 그러나 사용자 상호 작용이 필요한 경우 HIP 알림 메시지, 로그인 프롬프트 및 인증서 대화 상자가 표시됩니다.
사용자 스위치 터널 이름 변경 타임아웃(초) (Windows만 해당)	Microsoft의 RDP(원격 데스크톱 프로토콜)를 사용하여 엔드포인트에 로그인한 후 GlobalProtect 게이트웨이에서 원격 사용자를 인증해야 하는 시간(초)을 지정합니다(범위는 0~600, 기본값은 0). 원격 사용자가 제한된 시간 내에 인증하도록 요구하면 보안이 유지됩니다. 새 사용자를 인증하고 터널을 사용자로 전환한 후 게이트웨이는 터널의 이름을 바꿉니다.

GlobalProtect 앱 구성 설정	설명
	값 0은 현재 사용자의 터널 이름이 바뀌지 않고 즉시 종료됨을 의미합니다. 이 경우 원격 사용자는 새 터널을 얻게 되며 게이트웨이 인증을 위한 시간 제한이 없습니다(구성된 TCP 타임아웃 제외).
사전 로그온 터널 이름 변경 타임아웃(초)(Windows만 해당)	이 설정은 GlobalProtect가 엔드포인트를 게이트웨이에 연결하는 사전 로그온 터널을 처리하는 방법을 제어합니다. -1 값은 사용자가 엔드포인트에 로그온한 후 사전 로그온 터널이 타임아웃되지 않음을 의미합니다. GlobalProtect는 터널의 이름을 변경하여 사용자에게 다시 할당합니다. 그러나 이름 변경에 실패하거나 사용자가 GlobalProtect 게이트웨이에 로그인하지 않은 경우에도 터널은 유지됩니다. 값 0은 사용자가 엔드포인트에 로그온할 때 GlobalProtect가 이름을 바꾸는 대신 사전 로그온 터널을 즉시 종료함을 의미합니다. 이 경우 GlobalProtect는 사용자가 사전 로그온 터널을 통해 연결할 수 있도록 허용하는 대신 사용자를 위해 새 터널을 시작합니다. 일반적으로 이 설정은 연결 방법을 사전 로그온 후 주문형으로 설정할 때 가장 유용합니다. 그러면 사용자가 초기 로그온 후 수동으로 연결을 시작해야 합니다. 1에서 7200 사이의 값은 사용자가 엔드포인트에 로그온한 후 사전 로그온 터널이 활성 상태를 유지할 수 있는 시간(초)을 나타냅니다. 이 시간 동안 GlobalProtect는 사전 로그온 터널에서 정책을 시행합니다. 사용자가 제한 시간 내에 GlobalProtect 게이트웨이로 인증하는 경우 GlobalProtect는 사용자에게 터널을 재할당합니다. 사용자가 타임아웃 전에 GlobalProtect 게이트웨이로 인증하지 않으면 GlobalProtect는 사전 로그온 터널을 종료합니다.
사용자 로그오프 타임아웃 시 터널 유지(초)	사용자가 엔드포인트에서 로그아웃한 후 GlobalProtect가 기존 VPN 터널을 보존할 수 있도록 하려면 사용자 로그오프 타임아웃 시 터널 보존 값을 지정하십시오(범위는 0~600초, 기본값은 0초). 기본값 **0**을 수락하면 GlobalProtect는 사용자 로그아웃 후 터널을 보존하지 않습니다.
사용자 정의 비밀번호 만료 메시지 (LDAP 인증만 해당)	암호가 만료될 때 사용자에게 표시할 사용자 지정 메시지를 만듭니다. 최대 메시지 길이는 200자입니다.
IPSec을 신뢰할 수 없는 경우 자동으로 SSL 사용(시간)	GlobalProtect 앱이 **IPSec**이 신뢰할 수 없는 경우 **SSL**을 자동으로 사용하도록 하려는 시간(시간 단위)을 지정합니다(범위는 0-168시간). 이 옵션을 구성하면 GlobalProtect 앱은 지정된

GlobalProtect 앱 구성 설정	설명
	기간 동안 IPSec 터널 설정을 시도하지 않습니다. 이 타이머는 터널 연결 유지 타임아웃로 인해 IPSec 터널이 다운될 때마다 시작됩니다. 기본값 **0**을 수락하면 앱이 IPSec 터널을 성공적으로 설정할 수 있는 경우 SSL 터널 설정으로 대체하지 않습니다. IPSec 터널을 설정할 수 없는 경우에만 SSL 터널 설정으로 대체합니다.
IPSec에서 SSL 대체 알림 표시 콘텐츠 릴리스 버전 8387-6595 이상 및 GlobalProtect 앱 버전 6.0 이상이 필요합니다.	사용자가 IPSec에서 SSL로 연결이 변경되었음을 나타내는 알림 메시지를 못하게 하려면 아니요 를 선택합니다. 기본적으로 사용자에게 알림이 전송됩니다.
SSL로만 연결 GlobalProtect 앱 버전 6.0 이상이 필요합니다.	사용자가 IPSec 대신 SSL을 사용하도록 선택할 수 있게 하려면 예를 선택합니다.
GlobalProtect 연결 MTU(바이트)	GlobalProtect 앱이 게이트웨이에 연결하는 데 사용하는 1000~1420바이트 사이의 GlobalProtect 연결 최대 전송 단위(MTU) 값을 입력합니다. 기본값은 1400바이트입니다. 표준 1500바이트보다 낮은 MTU 값이 필요한 네트워크를 통해 연결하는 최종 사용자의 연결 환경을 최적화할 수 있습니다. MTU 크기를 줄이면 VPN 터널 연결이 MTU가 1500바이트 미만인 여러 ISP(인터넷 서비스 공급자) 및 네트워크 경로를 통과할 때 조각화로 인해 발생하는 성능 및 연결 문제를 제거할 수 있습니다.
최대 내부 게이트웨이 연결 시도	GlobalProtect 에이전트가 첫 번째 시도가 실패한 후 내부 게이트웨이에 대한 연결을 재시도해야 하는 최대 횟수를 입력합니다(범위는 0~100, 기본값은 0으로 GlobalProtect 앱이 연결을 재시도하지 않음). 값을 높이면 앱이 첫 번째 연결 시도 중에 일시적으로 다운되거나 연결할 수 없는 내부 게이트웨이에 자동으로 연결할 수 있지만 지정된 재시도 횟수가 모두 소진되기 전에 다시 돌아옵니다. 값을 늘리면 내부 게이트웨이가 최신 사용자 및 호스트 정보를 수신할 수도 있습니다.
고급 내부 호스트 감지 활성화	GlobalProtect 앱에서 내부 호스트 감지를 수행하는 동안 추가 보안 레이어를 추가합니다. 고급 내부 호스트 감지를 통해 앱은 내부 호스트의 역방향 DNS 조회를 수행하는 것 외에도 내

GlobalProtect 앱 구성 설정	설명
	부 게이트웨이의 서버 인증서를 확인하여 앱이 엔터프라이즈 네트워크 내부에 있는지 확인합니다. 예를 선택하여 GlobalProtect 앱이 내부 호스트 감지 중에 내부 호스트의 역방향 DNS 조회를 수행하는 것 외에도 내부 게이트웨이의 서버 인증서를 검증할 수 있도록 합니다. 내부 게이트웨이의 서버 인증서를 확인하지 않고 내부 호스트 감지를 수행하려면 GlobalProtect 앱에 대해 아니요(기본값)을 선택합니다.
포털 연결 타임아웃(초)	포털의 응답이 없어 포털에 대한 연결 요청 시간이 초과되기 전의 시간(1~600초)입니다. 방화벽이 777-4484 이전 버전의 애플리케이션 및 위협 콘텐츠를 실행 중인 경우 기본값은 30입니다. 콘텐츠 릴리스 버전 777-4484부터 기본값은 5입니다.
TCP 연결 타임아웃(초)	연결의 양쪽 끝에서 응답하지 않아 TCP 연결 요청이 타임아웃되기 전의 시간(1~600초)입니다. 방화벽이 777-4484 이전 버전의 애플리케이션 및 위협 콘텐츠를 실행 중인 경우 기본값은 60입니다. 콘텐츠 릴리스 버전 777-4484부터 기본값은 5입니다.
TCP 수신 타임아웃(초)	TCP 요청의 일부 응답이 없기 때문에 TCP 연결 시간이 초과되기까지의 시간(초)입니다(범위는 1~600, 기본값은 30).
분할 터널 옵션	네트워크 > **GlobalProtect** > 게이트웨이 > 에이전트 > 클라이언트 설정 > **(**클라이언트 구성**)** > 분할 터널 > 도메인 및 애플리케이션에서 GlobalProtect 게이트웨이에 구성된 도메인 제외 또는 포함을 기반으로 트래픽에 대해 분할 터널 도메인 및/또는 분할 DNS 기능을 활성화할지 여부를 지정합니다. 네트워크 트래픽만 - 네트워크 > **GlobalProtect** > 게이트웨이 에이전트 > 클라이언트 설정 >**(**클라이언트 구성**)** > 분할 터널 > 도메인 및 애플리케이션의 GlobalProtect 게이트웨이에 구성된 도메인을 포함하거나 제외하는 >에 따라 트래픽에 대해 분할 터널 도메인만 사용하도록 설정하려면 이 옵션을 선택합니다. 네트워크 트래픽 및 **DNS** 모두 - 네트워크 > **GlobalProtect** > 게이트웨이 > 에이전트 > 클라이언트 설정 > **(**클라이언트 구성**)** > 분할 터널 > 도메인 및 애플리케이션에서 GlobalProtect 게이트웨이에 구성된 포함 또는 제외 도메인에 따라 트래픽에 대해 분할 터널 도메인과 분할 DNS를 모두 활성화하려면 이 옵션을 선택하십시오.

GlobalProtect 앱 구성 설정	설명
	이 옵션을 사용하려면 콘텐츠 릴리스 버전 8284-6139 이상이 필요합니다.
터널에서 할당한 DNS 서버를 사용하여 모든 FQDN 확인(Windows만 해당)	(GlobalProtect 4.0.3 이상 릴리스) GlobalProtect 터널이 Windows 엔드포인트에 연결된 경우 DNS 확인 기본 설정을 구성합니다. • 예(기본값)를 선택하여 엔드포인트가 물리적 어댑터에 설정된 DNS 서버로 일부 DNS 쿼리를 보내는 대신 게이트웨이에서 구성한 DNS 서버로 Windows 엔드포인트가 모든 DNS 쿼리를 해결할 수 있도록 GlobalProtect 앱을 활성화합니다. • 게이트웨이에 구성된 DNS 서버에 대한 초기 쿼리가 확인되지 않은 경우 Windows 엔드포인트에서 DNS 쿼리를 물리적 어댑터에 설정된 DNS 서버로 보낼 수 있도록 하려면 아니오를 선택합니다. 이 옵션은 모든 어댑터의 모든 DNS 서버를 재귀적으로 쿼리하는 기본 Windows 동작을 유지하지만 일부 DNS 쿼리를 해결하는 데 오랜 대기 시간이 발생할 수 있습니다. GlobalProtect 앱 4.0.2 및 이전 릴리스에 대한 DNS 설정을 구성하려면 연결 시 **DNS** 설정 업데이트 옵션을 사용하십시오.
Connect에서 DNS 설정 업데이트 (Windows 전용) (더 이상 사용되지 않음)	(GlobalProtect 4.0.2 및 이전 릴리스) GlobalProtect 터널에 대한 DNS 서버 기본 설정을 구성합니다. • 게이트웨이에 구성된 DNS 서버에 대한 초기 쿼리가 확인되지 않은 경우 Windows 엔드포인트가 물리적 어댑터에 설정된 DNS 서버로 DNS 쿼리를 보낼 수 있도록 하려면 아니오(기본값)를 선택합니다. 이 옵션은 모든 어댑터의 모든 DNS 서버를 재귀적으로 쿼리하는 기본 Windows 동작을 유지하지만 일부 DNS 쿼리를 해결하는 데 오랜 대기 시간이 발생할 수 있습니다. • Windows 엔드포인트가 엔드포인트의 물리적 어댑터에 설정된 DNS 서버 대신 게이트웨이에서 구성한 DNS 서버를 사용하여 모든 DNS 쿼리를 해결할 수 있도록 하려면 예를 선택합니다. 이 옵션을 활성화하면 GlobalProtect가 게이트

GlobalProtect 앱 구성 설정	설명
	웨이 DNS 설정을 엄격하게 적용하고 모든 물리적 어댑터에 대한 정적 설정을 재정의합니다. 이 설정이 활성화되면(***Yes***로 설정) *GlobalProtect*가 이전에 저장된 *DNS* 설정을 복원하지 못할 수 있으며 결과적으로 엔드포인트가 *DNS* 쿼리를 해결하지 못할 수 있습니다. 이 기능은 더 이상 사용되지 않으며 이 시나리오가 발생하지 않도록 개선된 구현으로 대체되었습니다. 이전에 이 기능을 사용하고 있었다면 *GlobalProtect* 앱 *4.0.3* 이상 릴리스로 업그레이드하는 것이 좋습니다. GlobalProtect 앱 4.0.3 이상 릴리스에 대한 DNS 설정을 구성하려면 터널이 할당한 **DNS** 서버를 사용하여 모든 **FQDN** 확인 옵션을 사용하십시오.
프록시 자동 구성(PAC) 파일 URL	예를 선택하여 프록시 자동 구성(PAC) 파일의 URL을 GlobalProtect 앱에서 엔드포인트로 푸시합니다. 프록시 설정을 구성하기 위해 엔드포인트에 푸시할 PAC(Proxy Auto-Configuration) 파일 URL을 지정합니다. 최대 URL 길이는 256자입니다. 다음과 같은 PAC(프록시 자동 구성) 파일 URL 방법이 지원됩니다. • 프록시 자동 구성(PAC) 표준(예: http://pac.<hostname or IP>/proxy.pac). • WPAD(Web Proxy Auto-Discovery Protocol) 표준(예: http://wpad.<hostname or IP>/wpad.dat).
각 연결에 대한 프록시 감지 (Windows만 해당)	포털 연결에 대한 프록시를 자동 감지하고 후속 연결에 해당 프록시를 사용하려면 아니오를 선택합니다. 모든 연결에서 프록시를 자동 감지하려면 예(기본값)를 선택합니다.
프록시를 통한 터널 설정(Windows 및 Mac만 해당)	GlobalProtect가 프록시를 사용하거나 우회해야 하는지의 여부를 지정합니다. GlobalProtect가 프록시를 우회하도록 하려면 아니오를 선택합니다. GlobalProtect가 프록시를 사용하도록 하려면 예를 선택합니다. GlobalProtect 프록시 사용, 엔드포인트 OS 및 터널 유형에 따라 네트워크 트래픽이 다르게 작동합니다.

GlobalProtect 앱 구성 설정	설명
WSC(Windows 보안 센터) 상태가 변경되면 즉시 HIP 보고서 보내기 (Windows만 해당)	WSC(Windows 보안 센터) 상태가 변경될 때 GlobalProtect 앱이 HIP 데이터를 보내지 못하도록 하려면 아니오를 선택합니다. 예(기본값)를 선택하면 WSC 상태가 변경될 때 HIP 데이터를 즉시 전송합니다.
MFA 게이트웨이에서 인바운드 인증 프롬프트 활성화	MFA(다단계 인증)를 지원하려면 GlobalProtect 엔드포인트가 게이트웨이에서 인바운드되는 UDP 프롬프트를 수신하고 승인해야 합니다. 예를 선택하여 GlobalProtect 엔드포인트가 프롬프트를 수신하고 승인할 수 있도록 합니다. 게이트웨이에서 UDP 프롬프트를 차단하려면 GlobalProtect에 대해 아니오(기본값)를 선택합니다.
인바운드 인증 프롬프트(UDP)용 네트워크 포트	GlobalProtect 엔드포인트가 MFA 게이트웨이에서 인바운드 인증 프롬프트를 수신하는 데 사용하는 포트 번호를 지정합니다. 기본 포트는 4501입니다. 포트를 변경하려면 1에서 65535 사이의 숫자를 지정하십시오.
신뢰할 수 있는 MFA 게이트웨이	GlobalProtect 엔드포인트가 다단계 인증을 위해 신뢰하는 방화벽 또는 인증 게이트웨이 목록을 지정합니다. GlobalProtect 엔드포인트가 지정된 네트워크 포트에서 UDP 메시지를 수신하면 GlobalProtect는 UDP 프롬프트가 신뢰할 수 있는 게이트웨이에서 오는 경우에만 인증 메시지를 표시합니다.
인바운드 인증 메시지	사용자가 추가 인증이 필요한 리소스에 액세스하려고 할 때 표시할 알림 메시지를 사용자 지정합니다. 사용자가 추가 인증이 필요한 리소스에 액세스하려고 하면 GlobalProtect는 인바운드 인증 프롬프트가 포함된 UDP 패킷을 수신하고 이 메시지를 표시합니다. UDP 패킷에는 Multi-Factor Authentication을 구성할 때 지정하는 인증 포털 페이지의 URL도 포함되어 있습니다. GlobalProtect는 URL을 메시지에 자동으로 추가합니다. 예: `## ### ### ### #### ###### ####. ### #####.` 메시지는 255자 이하여야 합니다.
IPv6 선호	GlobalProtect 엔드포인트 통신에 대한 기본 프로토콜을 지정합니다. 기본 프로토콜을 IPv4로 변경하려면 아니오를 선택합니다. IPv6을 이중 스택 환경으로 기본 연결하려면 예(기본값)를 선택합니다.

GlobalProtect 앱 구성 설정	설명
비밀번호 변경 메시지	사용자가 AD(Active Directory) 암호를 변경할 때 암호 정책 또는 요구 사항을 지정하도록 메시지를 사용자 지정합니다. 예: `### ## ### ### ### #### #### ###.` 메시지는 중국어 간체와 같은 2바이트 유니코드 언어의 경우 255자 이하여야 합니다. 일본어의 경우 메시지는 128자 이하여야 합니다.
로그 게이트웨이 선택 기준	예를 선택하여 GlobalProtect 앱이 게이트웨이 선택 기준 로그를 방화벽으로 보낼 수 있도록 합니다. 기본값은 아니오입니다. 앱은 게이트웨이 선택 기준에 대한 향상된 로그를 방화벽으로 보내지 않습니다.
문제 해결을 위해 자율 DEM 및 GlobalProtect 앱 로그 수집 사용 콘텐츠 릴리스 버전 8350-14191 이상이 필요합니다. GlobalProtect 앱 5.2.5 이상이 필요합니다.	예를 선택하여 GlobalProtect 앱이 문제 보고 옵션을 표시하여 최종 사용자가 문제 해결 및 진단 로그를 Cortex Data Lake로 직접 보낼 수 있도록 합니다. 포털에서 푸시되는 Cortex Data Lake 인증서를 클라이언트 인증서로 구성하여 문제 보고 옵션을 표시해야 합니다. 이 인증서는 클라이언트가 로그를 보낼 때 Cortex Data Lake에 인증하는 데 사용됩니다. 이 설정을 아니요(기본값)로 설정하면 GlobalProtect 앱에 문제 보고 옵션이 표시되지 않으며 최종 사용자는 문제 해결 및 진단 로그를 Cortex Data Lake로 보낼 수 없습니다.
자율 DEM 업데이트 알림 표시	ADEM 에이전트가 업데이트될 때마다 사용자에게 알림을 표시하려면 예를 선택합니다.
이러한 대상 웹 서버에 대한 진단 테스트 실행 콘텐츠 릴리스 버전 8350-14191 이상이 필요합니다. GlobalProtect 앱 5.2.5 이상이 필요합니다.	최대 열 개의 HTTPS 기반 대상 URL을 입력하여 프로빙에 대한 성능 테스트를 시작합니다. 이러한 진단 테스트는 문제 해결을 위해 자율 **DEM** 및 **GlobalProtect** 앱 로그 수집 사용을 선택한 경우에만 실행됩니다. 입력하는 대상 URL은 IP 주소 또는 정규화된 도메인 이름(예: https://10.10.10.10/resource.html, https://webserver/file.pdf 또는 https://google.com)일 수 있습니다.
Prisma Access용 자율 DEM 엔드포인트 에이전트(Windows & Mac에만 해당) Windows 10 및 macOS에서만 실행되고 콘텐츠 릴리스 버전 8393-6628 이	GlobalProtect 앱을 설치하는 동안 ADEM(자율 DEM) 엔드포인트 에이전트를 설치할지 여부를 지정하고 최종 사용자가 앱에서 사용자 환경 테스트를 사용하거나 사용하지 않도록 설정할 수 있도록 허용합니다.

GlobalProtect 앱 구성 설정	설명
상이며 GlobalProtect 앱 5.2.6 이상이 필요합니다.	• 설치를 선택하고 사용자는 GlobalProtect 앱 설치 중에 ADEM 엔드포인트 에이전트를 설치하기 위해 GlobalProtect에서 에이전트를 활성화/비활성화할 수 있으며 최종 사용자가 GlobalProtect 앱에서 사용자 경험 테스트를 활성화 또는 비활성화할 수 있습니다. • 설치를 선택하고 사용자는 GlobalProtect 앱 설치 중에 ADEM 엔드포인트 에이전트를 설치하기 위해 GlobalProtect에서 에이전트를 활성화/비활성화할 수 없으며 최종 사용자가 GlobalProtect 앱에서 사용자 경험 테스트를 활성화 또는 비활성화하도록 허용할 수 없습니다. • 설치 안 함(기본값)을 선택하여 GlobalProtect 앱 설치 중에 ADEM 엔드포인트 에이전트를 설치하지 않습니다.
격리 메시지에 추가된 디바이스	기본적으로 GlobalProtect는 최종 사용자의 디바이스가 격리될 때 다음 메시지를 표시합니다. `# ###### ##### ## #### ### ## ### ## #######. IT ##### ######.` 이 기본 메시지를 최대 512자의 사용자 지정 메시지로 바꿀 수 있습니다.
격리 메시지에서 제거된 디바이스	기본적으로 GlobalProtect는 최종 사용자의 디바이스가 격리될 때 다음 메시지를 표시합니다. `# ###### ##### ## #### ### ## ### ## #######.` 이 기본 메시지를 최대 512자의 사용자 지정 메시지로 바꿀 수 있습니다.
시작 시 상태 패널 표시(Windows만 해당)	사용자가 처음으로 연결을 설정할 때 GlobalProtect 상태 패널을 자동으로 표시하려면 예를 선택하십시오. 사용자가 처음으로 연결을 설정할 때 GlobalProtect 상태 패널을 표시하지 않으려면 아니오를 선택합니다.
GlobalProtect UI가 사용자 입력에 대해 유지되도록 허용 (Windows 10 이상 및 macOSS)	예를 선택하여 최종 사용자가 자격 증명을 입력할 때 GlobalProtect 앱이 화면에 상태 패널을 계속 표시할 수 있도록 합니다.

GlobalProtect 앱 구성 설정	설명
콘텐츠 릴리스 버전 8450-6909 이상 및 GlobalProtect 앱 6.0.0 이상이 필요합니다.	
GlobalProtect 앱 비활성화	
암호/암호 확인	사용자가 **GlobalProtect** 앱을 비활성화하도록 허용 설정이 암호로 허용인 경우 암호를 입력한 다음 확인합니다. 이 암호를 암호처럼 취급하여 기록하고 안전한 장소에 보관하십시오. 이메일로 새 GlobalProtect 사용자에게 암호를 배포하거나 회사 웹사이트의 지원 영역에 게시할 수 있습니다. 상황으로 인해 엔드포인트에서 VPN 연결을 설정할 수 없고 이 기능이 활성화된 경우 사용자는 앱 인터페이스에 이 암호를 입력하여 GlobalProtect 앱을 비활성화하고 VPN을 사용하지 않고 인터넷에 액세스할 수 있습니다.
사용자가 연결을 끊을 수 있는 최대 시간	사용자가 방화벽에 연결하기 전에 GlobalProtect 연결을 끊을 수 있는 최대 횟수를 지정합니다. 기본값 0은 사용자가 앱 연결을 끊을 수 있는 횟수에 제한이 없음을 의미합니다.
연결 해제 시간 초과(분)	GlobalProtect 앱의 연결을 끊을 수 있는 최대 시간(분)을 지정합니다. 지정된 시간이 지나면 앱이 방화벽에 연결을 시도합니다. 기본값 0은 연결 해제 기간이 무제한임을 나타냅니다. 사용자가 앱을 연결 해제할 수 있는 시간을 제한하려면 연결 해제 제한 시간 값을 설정합니다. 이렇게 하면 제한 시간이 끝나면 *GlobalProtect*가 *VPN*을 다시 시작하고 설정하여 사용자와 리소스에 대한 사용자 액세스를 보호합니다.
모바일 보안 관리자 설정	
모바일 보안 관리자	MDM(모바일 디바이스 관리)을 위해 GlobalProtect Mobile Security Manager를 사용하는 경우 GP-100 어플라이언스에서 디바이스 체크인(등록) 인터페이스의 IP 주소 또는 FQDN을 입력하십시오.
등록 포트	모바일 엔드포인트는 등록을 위해 GlobalProtect Mobile Security Manager에 연결할 때 사용해야 하는 포트 번호입니

GlobalProtect 앱 구성 설정	설명
	다. Mobile Security Manager는 기본적으로 포트 443에서 수신 대기합니다. 모바일 엔드포인트 사용자가 등록 프로세스 동안 클라이언트 인증서를 요구하지 않도록 이 포트 번호를 유지하십시오*(다른 가능한 값은 443, 7443* 및 *8443*임*).*

GlobalProtect 포털 에이전트 HIP 데이터 수집 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트 > ***<agent-config>*** > **HIP** 데이터 수집

HIP 데이터 수집 탭을 선택하여 앱이 HIP 보고서의 엔드포인트에서 수집하는 데이터를 정의합니다.

GlobalProtect HIP 데이터 수집 구성 설정	설명
HIP 데이터 수집	앱이 HIP 데이터를 수집 및 전송하지 못하도록 하려면 이 옵션을 선택 취소합니다. *GlobalProtect*가 *HIP* 기반 정책 시행을 위해 *HIP* 데이터를 수집할 수 있도록 하면 방화벽이 엔드포인트의 *HIP* 데이터를 사용자가 정의한 *HIP* 개체 및/또는 *HIP* 프로파일과 일치시킨 다음 적절한 정책을 적용할 수 있습니다.
최대 대기 시간(초)	사용 가능한 데이터를 제출하기 전에 앱이 HIP 데이터를 검색해야 하는 시간을 지정합니다(범위는 10-60, 기본값은 20).
인증서 프로파일	GlobalProtect 포털이 GlobalProtect 앱에서 보낸 컴퓨터 인증서와 일치시키기 위해 사용하는 인증서 프로파일을 선택합니다.
카테고리 제외	앱에서 HIP 데이터를 수집하지 않도록 하려는 호스트 정보 카테고리를 지정하려면 카테고리 제외를 선택합니다. HIP 수집에서 제외할 카테고리(예: 데이터 손실 방지)를 선택합니다. 카테고리를 선택한 후 특정 공급자를 추가한 다음 공급자의 특정 제품을 추가하여 필요에 따라 제외를 더욱 세분화할 수 있습니다. 확인을 클릭하여 각 대화 상자의 설정을 저장합니다.
맞춤 수표	사용자 지정 검사를 선택하여 앱에서 수집할 사용자 지정 호스트 정보를 정의합니다. 예를 들어, HIP 개체를 생성하기 위한 공급자 또는 제품 목록에 포함되지 않은 필수 애플리케이션이 있는 경우 해당 애플리케이션이 설치

GlobalProtect HIP 데이터 수집 구성 설정	설명
	되어 있거나(해당 Windows 레지스트리 또는 Mac plist 키가 있음) 현재 실행 중입니다(해당 실행 중인 프로세스가 있음): • **Windows** - 특정 레지스트리 키 또는 키 값에 대한 검사를 추가합니다. • **Mac** - 특정 plist 키 또는 키 값에 대한 검사를 추가합니다. • 프로세스 목록 - 사용자 엔드포인트에서 확인하려는 프로세스를 추가하여 실행 중인지 확인합니다. 예를 들어, 소프트웨어 애플리케이션이 실행 중인지 확인하려면 실행 파일의 이름을 프로세스 목록에 추가합니다. **Windows** 탭, **Mac** 탭 또는 둘 다에 프로세스를 추가할 수 있습니다.

GlobalProtect 포털 클라이언트리스 VPN 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > **Clientless VPN**

이제 HTML, HTML5 및 JavaScript 기술을 사용하는 일반 엔터프라이즈 웹 애플리케이션에 대한 보안 원격 액세스를 제공하도록 GlobalProtect 포털을 구성할 수 있습니다. 사용자는 GlobalProtect 소프트웨어를 설치하지 않고도 SSL 지원 웹 브라우저에서 안전하게 액세스할 수 있는 이점이 있습니다. 이는 파트너 또는 계약자가 애플리케이션에 액세스할 수 있도록 해야 하고 개인 디바이스를 포함하여 관리되지 않는 자산을 안전하게 활성화해야 할 때 유용합니다. 이 기능을 사용하려면 GlobalProtect 포털에서 Clientless VPN을 호스팅하는 방화벽에 GlobalProtect 구독을 설치해야 합니다. **Clientless VPN** 탭을 선택하여 다음 표에 설명된 대로 포털에서 GlobalProtect Clientless VPN 설정을 구성합니다.

GlobalProtect Portal Clientless 구성 설정	설명
일반 탭	
Clientless VPN	**Clientless VPN**을 선택하여 Clientless VPN 세션에 대한 일반 정보를 지정합니다.
호스트네임	웹 애플리케이션 랜딩 페이지를 호스팅하는 GlobalProtect 포털의 IP 주소 또는 FQDN입니다. GlobalProtect Clientless VPN은 이 호스트 이름으로 애플리케이션 URL을 다시 작성합니다. *NAT(Network Address Translation)*를 사용하여 *GlobalProtect* 포털에 대한 액세스를 제공하는 경우 입력하는 *IP* 주소 또는 *FQDN*은 *GlobalProtect* 포털의 *NAT IP* 주소*(*공용 *IP* 주소*)*와 일치*(*또는 확인*)*해야 합니다.

GlobalProtect Portal Clientless 구성 설정	설명
보안 구역	Clientless VPN 구성을 위한 영역입니다. 이 영역에 정의된 보안 규칙은 사용자가 액세스할 수 있는 애플리케이션을 제어합니다.
DNS 프록시	애플리케이션 이름을 확인하는 DNS 서버입니다. **DNS** 프록시 서버를 선택하거나 새 **DNS** 프록시를 구성합니다(네트워크 > DNS 프록시).
로그인 유효 시간	Clientless SSL VPN 세션이 유효한 분(범위는 60~1,440) 또는 시간(범위는 1~24, 기본값은 3)입니다. 지정된 시간이 지나면 사용자는 Clientless VPN 세션을 다시 인증하고 시작해야 합니다.
비활성 타임아웃	Clientless SSL VPN 세션이 유휴 상태로 유지될 수 있는 분(범위: 5~1,440, 기본값: 30) 또는 시간(범위: 1~24)입니다. 지정된 시간 동안 사용자 활동이 없으면 사용자는 다시 인증하고 새로운 Clientless VPN 세션을 시작해야 합니다.
최대 사용자	포털에 동시에 로그인할 수 있는 최대 사용자 수(기본값은 10, 범위는 1에서 최대 없음)입니다. 최대 사용자 수에 도달하면 추가 Clientless VPN 사용자가 포털에 로그인할 수 없습니다.
애플리케이션 탭	
사용자 매핑에 대한 애플리케이션	게시된 애플리케이션과 사용자를 일치시키려면 사용자 매핑에 하나 이상의 애플리케이션을 추가하십시오. 이 매핑은 Clientless VPN을 사용하여 애플리케이션에 액세스할 수 있는 사용자 또는 사용자 그룹을 제어합니다. 애플리케이션 및 애플리케이션 그룹을 사용자에게 매핑하기 전에 정의해야 합니다(네트워크 > GlobalProtect > Clientless 앱 및 네트워크 > GlobalProtect > Clientless 앱 그룹). • 이름 - 매핑 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다. • 애플리케이션 **URL** 주소 표시줄 표시 - 사용자가 애플리케이션 랜딩 페이지에 게시되지 않은 애플리케이션을 실행할 수 있는 애플리케이션 URL 주소 표시줄을 표시하려면 이 옵션을 선택합니다. 활성화되면 사용자는 페이지에서 애플리케이션 **URL** 링크를 클릭하고 URL을 지정할 수 있습니다.
사용자/사용자 그룹	현재 애플리케이션 구성이 적용되는 개별 사용자 또는 사용자 그룹을 추가할 수 있습니다. 이러한 사용자는 GlobalProtect Clientless VPN을 사용하여 구성된 애플리케이션을 실행할 수 있는 권한이 있습니다.

GlobalProtect Portal Clientless 구성 설정	설명
	그룹을 선택하려면 먼저 그룹 매핑(***Device*** > ***User*** 식별 > 그룹 매핑 설정)을 구성해야 합니다. 사용자 및 그룹 외에도 이러한 설정이 사용자 또는 그룹에 적용되는 시기를 지정할 수 있습니다. • **any** - 애플리케이션 구성이 모든 사용자에게 적용됩니다(사용자 또는 사용자 그룹을 추가할 필요 없음). • 선택 - 이 목록에 추가한 사용자 및 사용자 그룹에만 애플리케이션 구성이 적용됩니다.
애플리케이션	매핑에 개별 애플리케이션 또는 애플리케이션 그룹을 추가할 수 있습니다. 구성에 포함시킨 소스 사용자는 GlobalProtect Clientless VPN을 사용하여 추가한 애플리케이션을 실행할 수 있습니다.
암호화 설정 탭	
프로토콜 버전	필요한 최소 및 최대 TLS/SSL 버전을 선택합니다. TLS 버전이 높을수록 연결이 더 안전합니다. **SSLv3**, **TLSv1.0**, **TLSv1.1** 또는 **TLSv1.2** 중에서 선택할 수 있습니다.
키 교환 알고리즘	키 교환을 위해 지원되는 알고리즘 유형을 선택하십시오. **RSA**, Diffie-Hellman(**DHE**) 또는 Elliptic Curve Ephemeral Diffie-Hellman(**ECDHE**)을 선택할 수 있습니다.
암호화 알고리즘	지원되는 암호화 알고리즘을 선택합니다. **AES128** 이상을 권장합니다.
인증 알고리즘	지원되는 인증 알고리즘을 선택합니다. 선택 사항은 다음과 같습니다. **MD5**, **SHA1**, **SHA256** 또는 **SHA384**. **SHA256** 이상을 권장합니다.
서버 인증서 확인	애플리케이션이 서버 인증서를 제공할 때 발생할 수 있는 다음 문제에 대해 수행할 작업을 활성화합니다. • 인증서가 만료된 세션 차단 - 서버 인증서가 만료된 경우 애플리케이션에 대한 액세스를 차단합니다. • 신뢰할 수 없는 발급자와의 세션 차단 - 서버 인증서가 신뢰할 수 없는 인증 기관에서 발급된 경우 애플리케이션에 대한 액세스를 차단합니다. • 알 수 없는 인증서 상태의 세션 차단 - OCSP 또는 CRL 서비스가 # # ## 인증서 해지 상태를 반환하는 경우 애플리케이션에 대한 액세스를 차단합니다.

GlobalProtect Portal Clientless 구성 설정	설명
	• 인증서 상태 확인 타임아웃 시 세션 차단 - 인증서 상태 서비스로부터 응답을 받기 전에 인증서 상태 확인 시간이 초과되면 애플리케이션에 대한 액세스를 차단합니다.
프록시 탭	
이름	GlobalProtect 포털이 게시된 애플리케이션에 액세스하는 데 사용하는 프록시 서버를 식별하기 위한 최대 31자의 레이블입니다. 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
도메인	프록시 서버에서 제공하는 도메인을 추가합니다.
프록시 사용	GlobalProtect 포털이 프록시 서버를 사용하여 게시된 애플리케이션에 액세스하도록 허용하려면 선택합니다.
서버 포트	프록시 서버의 호스트 이름(또는 IP 주소)과 포트 번호를 지정합니다.
사용자 비밀번호	프록시 서버에 로그인하는 데 필요한 사용자명과 암호를 지정합니다. 확인을 위해 비밀번호를 다시 입력하세요.
Advanced 설정 탭	
제외 도메인 목록 다시 쓰기	(선택 사항) 도메인 이름, 호스트 이름 또는 IP 주소를 다시 쓰기 제외 도메인 목록에 추가합니다. Clientless VPN은 역방향 프록시 역할을 하며 게시된 애플리케이션에서 반환된 페이지를 수정합니다. 원격 사용자가 URL에 액세스하면 요청이 GlobalProtect 포털을 통해 이동합니다. 경우에 따라 애플리케이션에 포털을 통해 액세스할 필요가 없는 페이지가 있을 수 있습니다. 다시 쓰기 규칙에서 제외해야 하고 다시 쓸 수 없는 도메인을 지정합니다. 경로는 호스트 및 도메인 이름에서 지원되지 않습니다. 호스트 및 도메인 이름의 와일드카드 문자(*)는 이름의 시작 부분에만 나타날 수 있습니다(예: *.etrade.com).

GlobalProtect 포털 새틀라이트 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 위성

새틀라이트는 일반적으로 지사에 있는 Palo Alto Networks® 방화벽으로 GlobalProtect 앱 역할을 하여 새틀라이트가 GlobalProtect 게이트웨이에 대한 VPN 연결을 설정할 수 있도록 합니다. GlobalProtect 앱과 마

찬가지로 새틀라이트는 인증서 및 VPN 구성 라우팅 정보가 포함된 포털에서 초기 구성을 수신하고 새틀라이트가 VPN 연결을 설정하기 위해 구성된 모든 게이트웨이에 연결할 수 있도록 합니다.

지점 방화벽에서 GlobalProtect 새틀라이트 설정을 구성하기 전에 WAN 연결이 있는 인터페이스를 구성하고 지점 LAN이 인터넷과 통신할 수 있도록 보안 영역 및 정책을 설정해야 합니다. 그런 다음 새틀라이트 탭을 선택하여 다음 표에 설명된 대로 포털에서 GlobalProtect 새틀라이트 설정을 구성할 수 있습니다.

GlobalProtect Portal Satellite 구성 설정	설명
일반	• 이름 - GlobalProtect 포털에서 이 새틀라이트 구성의 이름입니다. • 구성 새로 고침 인터벌(시간) - 새틀라이트가 포털에서 구성 업데이트를 확인해야 하는 빈도(범위는 1-48, 기본값은 24)입니다.
디바이스	방화벽 일련번호를 사용하여 새틀라이트를 추가합니다. 포털은 연결을 요청하는 사용자를 식별하기 위해 일련 번호 또는 로그인 자격 증명을 수락할 수 있습니다. Satellite를 처음으로 포털에 인증하려면 Satellite 관리자가 사용자 이름과 비밀번호를 제공해야 합니다. Satellite가 성공적으로 인증되면 **Satellite** 호스트 이름이 자동으로 포털에 추가됩니다.
등록 사용자/사용자 그룹	포털은 일련번호가 있거나 없는 등록 사용자/사용자 그룹 설정을 사용하여 새틀라이트를 이 구성과 일치시킬 수 있습니다. 이 구성으로 제어하려는 사용자 또는 그룹을 추가하십시오. 구성을 특정 그룹으로 제한하려면 먼저 방화벽에서 그룹 매핑을 활성화해야 합니다(디바이스 > 사용자 식별 > 그룹 매핑 설정).
게이트웨이	추가를 클릭하여 이 구성이 IPSec 터널을 설정할 수 있는 게이트웨이 새틀라이트의 IP 주소 또는 호스트 이름을 입력합니다. 게이트웨이 필드에 게이트웨이가 구성된 인터페이스의 FQDN 또는 IP 주소를 입력합니다. IP 주소는 **IPv6**, **IPv4** 또는 둘 다로 지정할 수 있습니다. 이중 스택 환경에서 IPv6 연결의 기본 설정을 지정하려면 **IPv6** 기본을 선택합니다. (선택 사항) 구성에 둘 이상의 게이트웨이를 추가하는 경우 라우팅 우선 순위는 새틀라이트가 선호하는 게이트웨이를 선택하는 데 도움이 됩니다(범위는 1~25). 숫자가 낮을수록 우선 순위가 높습니다(사용 가능한 게이트웨이의 경우). 새틀라이트는 라우팅 메트릭을 결정하기 위해 라우팅 우선 순위에 10을 곱합니다.

GlobalProtect Portal Satellite 구성 설정	설명
	게이트웨이에서 게시한 경로는 새틀라이트에 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 경로보다 더 높은 메트릭을 갖도록 라우팅 우선 순위를 설정해야 합니다. 예를 들어 기본 게이트웨이와 백업 게이트웨이에 대한 라우팅 우선 순위를 각각 *1*과 *10*으로 설정하면 새틀라이트는 기본 게이트웨이에 대한 메트릭으로 *10*을 사용하고 백업 게이트웨이에 대한 메트릭으로 *100*을 사용합니다. 또한 모든 정적 및 연결된 경로를 게이트웨이에 게시하는 경우 새틀라이트는 네트워크 및 라우팅 정보를 게이트웨이와 공유합니다(네트워크 > **IPSec** 터널 > **<tunnel** > **Advanced - <tunnel General**에서 **GlobalProtect Satellite**).
신뢰할 수 있는 루트 CA	추가를 클릭한 다음 게이트웨이 서버 인증서 발급을 위한 CA 인증서를 선택합니다. Satellite Trusted Root CA 인증서는 포털 에이전트 구성과 동시에 엔드포인트에 푸시됩니다. 게이트웨이 서버 인증서를 확인하고 *GlobalProtect* 게이트웨이에 대한 보안 *VPN* 터널 연결을 설정하려면 신뢰할 수 있는 루트 *CA*를 지정하십시오. 모든 게이트웨이는 동일한 발급자를 사용해야 합니다. 포털에 아직 존재하지 않는 경우 게이트웨이 서버 인증서를 발급하기 위해 루트 *CA* 인증서를 가져오거나 생성할 수 있습니다.
클라이언트 인증서	
로컬	• 인증서 발급 - 포털이 성공적으로 인증된 후 새틀라이트에 인증서를 발급하는 데 사용하는 루트 CA 발급 인증서를 선택합니다. 필요한 인증서가 방화벽에 아직 없는 경우 가져오거나 생성할 수 있습니다. 인증서가 방화벽에 아직 없는 경우 발급 인증서를 가져오거나 생성할 수 있습니다. • **OCSP** 응답자 - 새틀라이트가 포털 및 게이트웨이에서 제공하는 인증서의 해지 상태를 확인하는 데 사용하는 OCSP 응답자를 선택합니다. 없

GlobalProtect Portal Satellite 구성 설정	설명
	음을 선택하여 인증서 해지 확인에 OCSP를 사용하지 않도록 지정합니다. 인증서가 취소된 경우 알림을 받고 포털 및 게이트웨이에 대한 보안 연결을 설정하기 위해 적절한 조치를 취할 수 있도록 새틀라이트 *OCSP* 응답자를 활성화하십시오. 새틀라이트 *OCSP* 응답자를 활성화하려면 인증서 해지 확인 설정(***Device*** > ***Setup*** > ***Session*** > ***Decryption Settings***)에서 ***CRL*** 및 ***OCSP***도 활성화해야 합니다. • 유효 기간(일) - GlobalProtect 새틀라이트 인증서 유효 시간을 지정합니다(범위는 7~365, 기본값은 7). • 인증서 갱신 기간(일) - 인증서가 자동으로 갱신될 수 있는 만료 전 일 수를 지정합니다(범위는 3~30, 기본값은 3).
SCEP	• **SCEP** - 클라이언트 인증서 생성을 위한 SCEP 프로파일을 선택합니다. 프로파일이 드롭다운에 없으면 새 프로파일을 만들 수 있습니다. • 인증서 갱신 기간(일) - 인증서가 자동으로 갱신될 수 있는 만료 전 일 수를 지정합니다(범위는 3~30, 기본값은 3).

Network > GlobalProtect > Gateways

Network > **GlobalProtect** > **Gateways**를 선택하여 GlobalProtect 게이트웨이를 구성합니다. 게이트웨이는 GlobalProtect 앱 또는 GlobalProtect 새틀라이트에 대한 VPN 연결을 제공할 수 있습니다.

GlobalProtect Gateway 대화 상자에서 새 게이트웨이 구성을 추가하거나 기존 게이트웨이 구성을 선택하여 수정합니다.

무엇을 찾고 계신가요?	참조:
GlobalProtect 게이트웨이에 대해 어떤 일반 설정을 구성할 수 있습니까?	GlobalProtect 게이트웨이 일반 탭
게이트웨이 클라이언트 인증은 어떻게 구성합니까?	GlobalProtect 게이트웨이 인증 탭
앱이 게이트웨이와 VPN 터널을 설정할 수 있도록 하는 터널 및 네트워크 설정을 구성하려면 어떻게 해야 합니까?	GlobalProtect 게이트웨이 에이전트 탭
새틀라이트이 새틀라이트 역할을 하는 게이트웨이와 VPN 연결을 설정할 수 있도록 터널 및 네트워크 설정을 어떻게 구성합니까?	GlobalProtect 게이트웨이 새틀라이트 탭
더 찾고 계십니까?	포털 설정에 대한 자세한 단계별 지침은 GlobalProtect 관리자 안내서에서 GlobalProtect 게이트웨이 구성을 참조하십시오.

GlobalProtect 게이트웨이 일반 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 일반

일반 탭을 선택하여 앱이 연결할 수 있는 게이트웨이 인터페이스를 정의하고 게이트웨이가 엔드포인트를 인증하는 방법을 지정하십시오.

GlobalProtect 게이트웨이 일반 설정	설명
이름	게이트웨이 이름을 입력합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.

GlobalProtect 게이트웨이 일반 설정	설명
위치	다중 가상 시스템 모드에 있는 방화벽의 경우 위치는 GlobalProtect 게이트웨이를 사용할 수 있는 가상 시스템(vsys)입니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 위치 필드가 GlobalProtect Gateway 대화 상자에 나타나지 않습니다. 게이트웨이 구성을 저장한 후에는 위치를 변경할 수 없습니다.
네트워크 설정 영역	
상호 작용	원격 엔드포인트의 수신 인터페이스 역할을 할 방화벽 인터페이스의 이름을 선택하십시오. (이러한 인터페이스는 이미 존재해야 합니다.) 관리 인터페이스가 인터넷에 노출되기 때문에, *Telnet*, *SSH*, *HTTP* 또는 *HTTPS*를 허용하는 인터페이스 관리 프로파일을 *GlobalProtect* 포털 또는 게이트웨이를 구성한 인터페이스에 연결하지 마십시오. 관리 네트워크에 대한 액세스를 보호하는 방법에 대한 자세한 내용은 관리 액세스 모범 사례를 참조하십시오.
IP 주소	(선택 사항) 게이트웨이 액세스를 위한 IP 주소를 지정합니다. **IP** 주소 유형을 선택한 다음 **IP** 주소를 입력합니다. • IP 주소 유형은 **IPv4**(IPv4 트래픽만), **IPv6**(IPv6 트래픽만) 또는 **IPv4** 및 **IPv6**일 수 있습니다. 네트워크에서 **IPv4** 및 **IPv6**이 동시에 실행되는 이중 스택 구성을 지원하는 경우 IPv4 및 IPv6을 사용합니다. IP 주소는 IP 주소 유형과 호환되어야 합니다. 예를 들어 IPv4의 경우 172.16.1.0 또는 IPv6의 경우 21DA:D3:0:2F3b입니다. **IPv4** 및 **IPv6**을 선택하는 경우 각각에 대해 적절한 주소 유형을 입력합니다.
로그 설정	
성공적인 SSL 핸드쉐이크 기록	(선택 사항) 성공적인 SSL 복호화 핸드쉐이크에 대한 자세한 로그를 생성합니다. 기본적으로 비활성화되어 있습니다.

GlobalProtect 게이트웨이 일반 설정	설명
	로그는 저장 공간을 사용합니다. 성공적인 ***SSL*** 핸드쉐이크를 기록하기 전에 로그를 저장하는 데 사용할 수 있는 리소스가 있는지 확인하십시오. ***Device*** > ***Setup*** > ***Management*** > 로깅 및 보고 설정을 편집하여 현재 로그 메모리 할당을 확인하고 로그 유형 간에 로그 메모리를 다시 할당합니다.
SSL 핸드쉐이크 실패 기록	SSL 복호화 핸드쉐이크 실패에 대한 자세한 로그를 생성하여 복호화 문제의 원인을 찾을 수 있습니다. 기본적으로 활성화되어 있습니다. 로그는 저장 공간을 사용합니다. 더 많거나 적은 로그 저장 공간을 복호화 로그에 할당하려면 로그 메모리 할당*(*디바이스 > 설정 > 관리 > 로깅 및 보고 설정*)*을 편집하십시오.
로그 포워딩	GlobalProtect SSL 핸드쉐이크(복호화) 로그를 포워딩할 방법과 위치를 지정합니다.

GlobalProtect 게이트웨이 인증 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 입증

인증 탭을 선택하여 SSL/TLS 서비스 프로파일을 식별하고 클라이언트 인증의 세부 사항을 구성합니다. 여러 클라이언트 인증 구성을 추가할 수 있습니다.

GlobalProtect 게이트웨이 인증 설정	
SSL/TLS 서비스 프로파일	이 GlobalProtect 게이트웨이를 보호하기 위한 SSL/TLS 서비스 프로파일을 선택하십시오. 서비스 프로파일의 내용에 대한 자세한 내용은 디바이스 > 인증서 관리 > SSL/TLS 서비스 프로파일을 참조하십시오.
클라이언트 인증 영역	
이름	이 구성을 식별하기 위해 고유한 이름을 입력하십시오.
OS	기본적으로 구성은 모든 엔드포인트에 적용됩니다. OS(**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows** 또는 **WindowsUWP**), **Satellite** 디바이스 또는 타사 IPSec VPN 클라이언트(**X-Auth**)별로 엔드포인트 목록을 구체화할 수 있습니다.

GlobalProtect 게이트웨이 인증 설정	
	OS는 여러 구성 간의 주요 차별화 요소입니다. 하나의 OS에 대해 여러 구성이 필요한 경우 인증 프로파일을 선택하여 구성을 더 구분할 수 있습니다. 목록 상단의 가장 구체적인 구성부터 하단의 가장 일반적인 구성까지 순서를 지정하십시오.
인증 프로파일	드롭다운에서 인증 프로파일 또는 시퀀스를 선택하여 게이트웨이에 대한 액세스를 인증합니다. 디바이스 > 인증 프로파일을 참조하세요. 클라이언트 인증의 경우 인증 프로파일이 *2*단계 인증과 함께 *RADIUS* 또는 *SAML*을 사용하는지 확인합니다. *RADIUS* 또는 *SAML*을 사용하지 않는 경우 인증 프로파일 외에 인증서 프로파일을 구성해야 합니다.
사용자명 레이블	GlobalProtect 게이트웨이 로그인에 대한 사용자 정의 사용자명 레이블을 지정하십시오. 예를 들어 사용자명**(**만**)** 또는 이메일 주소**(username@domain)**입니다.
비밀번호 레이블	GlobalProtect 게이트웨이 로그인에 대한 사용자 정의 비밀번호 레이블을 지정하십시오. 예를 들어 암호**(**터키어**)** 또는 암호(2단계 토큰 기반 인증의 경우)가 해당됩니다.
인증 메시지	최종 사용자가 이 게이트웨이에 로그인하는 데 사용해야 하는 자격 증명을 알 수 있도록 메시지를 입력하거나 기본 메시지를 유지할 수 있습니다. 메시지는 최대 256자까지 가능합니다.
사용자 자격 증명 또는 클라이언트 인증서로 인증 허용	아니오를 선택하면 사용자는 사용자 자격 증명과 클라이언트 인증서를 모두 사용하여 게이트웨이에 인증해야 합니다. 예를 선택하면 사용자는 사용자 자격 증명이나 클라이언트 인증서를 사용하여 게이트웨이에 인증할 수 있습니다.
인증서 프로파일	
인증서 프로파일	(선택 사항) 게이트웨이가 사용자 엔드포인트에서 오는 클라이언트 인증서를 일치시키는 데 사용하는 인증서 프로파일을 선택합니다. 인증서 프로파일을 사용하면 게이트웨이는 클라이언트의 인증서가 이 프로파일과 일치하는 경우에만 사용자를 인증합니다.

GlobalProtect 게이트웨이 인증 설정	
	사용자 자격 증명 또는 클라이언트 인증서로 인증 허용 옵션을 아니오로 설정한 경우 인증서 프로파일을 선택해야 합니다. 사용자 자격 증명 또는 클라이언트 인증서로 인증 허용 옵션을 예로 설정하면 인증서 프로파일은 선택 사항입니다. 인증서 프로파일은 OS와 독립적입니다.
격리된 디바이스에 대한 로그인 차단	격리 목록(**Device** > **Device Quarantine**)에 있는 GlobalProtect 클라이언트 디바이스에 대한 게이트웨이 로그인을 차단할지의 여부를 지정합니다.

GlobalProtect 게이트웨이 에이전트 탭

- 네트워크 > **GlobalProtect** > 포털 > ***<portal-config>*** > 에이전트

에이전트 탭을 선택하여 앱이 게이트웨이와 VPN 터널을 설정할 수 있도록 하는 터널 설정을 구성합니다. 또한 이 탭을 사용하면 VPN에 대한 타임아웃, DNS 및 WINS의 네트워크 서비스, 보안 정책 규칙에 연결된 HIP 프로파일이 일치하거나 일치하지 않을 때 최종 사용자에 대한 HIP 알림 메시지를 지정할 수 있습니다.

다음 탭에서 에이전트 설정을 구성합니다.

- 터널 설정 탭
- 클라이언트 설정 탭
- 클라이언트 IP 풀 탭
- 네트워크 서비스 탭
- 연결 설정 탭
- 비디오 트래픽 탭
- HIP 알림 탭

터널 설정 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > 터널 설정

터널 설정 탭을 선택하여 터널링을 활성화하고 터널 매개변수를 구성합니다.

외부 게이트웨이를 설정하는 경우 터널 매개변수가 필요합니다. 내부 게이트웨이를 구성하는 경우 터널 매개변수는 선택 사항입니다.

GlobalProtect Gateway 클라이언트 터널 모드 구성 설정	설명

터널 모드	터널 모드를 선택하여 터널 모드를 활성화한 후 다음 설정을 지정합니다.
	• 터널 인터페이스 - 이 게이트웨이에 액세스할 터널 인터페이스를 선택합니다.
	• 최대 사용자 - 인증, HIP 업데이트 및 GlobalProtect 앱 업데이트를 위해 게이트웨이에 동시에 액세스할 수 있는 최대 사용자 수를 지정합니다. 최대 사용자 수에 도달하면 최대 사용자 수에 도달했음을 나타내는 메시지와 함께 후속 사용자의 액세스가 거부됩니다(범위는 플랫폼에 따라 다르며 필드가 비어 있을 때 표시됨).
	• **IPSec** 활성화 - 엔드포인트 트래픽에 대해 IPSec 모드를 활성화하여 IPSec을 기본 방법으로 만들고 SSL-VPN을 대체 방법으로 만들려면 이 옵션을 선택합니다. 나머지 옵션은 IPSec이 활성화될 때까지 사용할 수 없습니다.
	• **GlobalProtect IPSec Crypto** - VPN 터널에 대한 인증 및 암호화 알고리즘을 지정하는 GlobalProtect IPSec Crypto 프로파일을 선택합니다. 기본 프로파일은 AES-128-CBC 암호화 및 SHA1 인증을 사용합니다. 자세한 내용은 네트워크 > 네트워크 프로파일 > GlobalProtect IPSec 암호화를 참조하십시오.
	• **X-Auth** 지원 활성화 - IPSec이 활성화된 경우 GlobalProtect 게이트웨이에서 확장 인증(X-Auth) 지원을 활성화하려면 이 옵션을 선택합니다. X-Auth 지원을 통해 X-Auth를 지원하는 타사 IPSec VPN 클라이언트(예: Apple iOS 및 Android 디바이스의 IPSec VPN 클라이언트 및 Linux의 VPNC 클라이언트)는 GlobalProtect 게이트웨이를 사용하여 VPN 터널을 설정할 수 있습니다. X-Auth 옵션은 VPN 클라이언트에서 특정 GlobalProtect 게이트웨이로의 원격 액세스를 제공합니다. X-Auth 액세스는 제한된 GlobalProtect 기능을 제공하므로 GlobalProtect가 iOS 및 Android 디바이스에서 제공하는 전체 보안 기능 세트에 대한 단순화된 액세스를 위해 GlobalProtect 앱을 사용하는 것을 고려하십시오.
	X-Auth 지원을 선택하면 그룹 이름 및 그룹 암호 옵션이 활성화됩니다.
	  • 그룹 이름과 그룹 암호가 지정된 경우 첫 번째 인증 단계에서는 양 당사자가 이 자격 증명을 사용하여 인증해야 합니다. 두 번째 단계에서는 인증 섹션에 구성된 인증 프로파일을 통해 확인되는 유효한 사용자명과 암호가 필요합니다.
	  • 그룹 이름과 그룹 암호가 정의되지 않은 경우 첫 번째 인증 단계는 타사 VPN 클라이언트에서 제공하는 유효한 인증서를 기반으로 합니다. 그런 다음 이 인증서는 인증 섹션에 구성된 인증서 프로파일을 통해 검증됩니다.

GlobalProtect Gateway 클라이언트 터널 모드 구성 설정	설명
	• 기본적으로 사용자는 IPSec 터널을 설정하는 데 사용된 키가 만료될 때 다시 인증할 필요가 없습니다. 사용자가 다시 인증하도록 하려면 **IKE** 키 재입력에 대한 인증 건너뛰기 옵션을 선택 취소합니다.

클라이언트 설정 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > 클라이언트 설정

GlobalProtect 앱이 게이트웨이와 터널을 설정할 때 엔드포인트에서 가상 네트워크 어댑터에 대한 설정을 구성하려면 클라이언트 설정 탭을 선택합니다.

일부 클라이언트 설정 옵션은 터널 모드를 활성화하고 터널 설정 탭에서 터널 인터페이스를 정의한 후에만 사용할 수 있습니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
구성 선택 기준 탭	
이름	클라이언트 설정 구성을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
소스 사용자	이 구성이 적용되는 특정 사용자 또는 사용자 그룹을 추가하십시오. 사용자 및 그룹을 선택하려면 먼저 그룹 매핑(디바이스 > 사용자 식별 > 그룹 매핑 설정)을 구성해야 합니다. 이 구성을 모든 사용자에게 배포하려면 소스 사용자 드롭다운에서 아무 항목이나 선택합니다. 사전 로그온 모드에서 GlobalProtect 앱이 있는 사용자에게만 이 구성을 배포하려면 소스 사용자 드롭다운에서 사전 로그온을 선택하십시오. 클라이언트 설정 구성은 사용자가 소스 사용자, ***OS*** 및 소스 주소에 대한 기준과 일치하는 경우에만 사용자에게 배포됩니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
OS	엔드포인트의 운영 체제를 기반으로 이 구성을 배포하려면 OS(**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows**, **WindowsUWP**)를 추가합니다. 또는 구성 배포가 엔드포인트의 운영 체제가 아닌 사용자 또는 사용자 그룹만을 기반으로 하도록 이 값을 **Any**로 설정할 수 있습니다. 클라이언트 설정 구성은 사용자가 소스 사용자, ***OS*** 및 소스 주소에 대한 기준과 일치하는 경우에만 사용자에게 배포됩니다.
소스 주소	사용자 위치를 기반으로 이 구성을 배포하려면 소스 지역 또는 로컬 **IP** 주소(IPv4 및 IPv6)를 추가합니다. 이 구성을 모든 사용자 위치에 배포하려면 지역 또는 **IP** 주소를 지정하지 마십시오. 이 기능은 이전 GlobalProtect 앱 릴리스에서 지원되지 않으므로 사용자가 GlobalProtect 앱 4.0 및 이전 릴리스를 실행하는 경우에도 이 필드를 비워 두어야 합니다. 연결하는 사용자의 위치가 구성한 지역 또는 ***IP*** 주소와 일치하면 소스 주소 일치가 성공한 것입니다. 클라이언트 설정 구성은 사용자가 소스 사용자, ***OS*** 및 소스 주소에 대한 기준과 일치하는 경우에만 사용자에게 배포됩니다.
인증 재정의 탭	
인증 재정의	사용자가 인증 또는 인증서 프로파일에 지정된 인증 체계를 사용하여 처음 인증한 후 게이트웨이가 안전한 디바이스별 암호화 쿠키를 사용하여 사용자를 인증할 수 있도록 합니다. • 인증 재정의를 위한 쿠키 생성 - 쿠키의 수명 동안 에이전트는 사용자가 게이트웨이로 인증할 때마다 이 쿠키를 제공합니다. • 쿠키 수명 - 쿠키가 유효한 시간, 일 또는 주를 지정합니다. 일반적인 수명은 24시간입니다. 범위는 1–72시간, 1–52주 또는 1–365일입니다. 쿠키가 만료된 후 사용자는 로그인 자격 증명을 입력해야 하며 게이트웨이는 이후에 사용자 디바이스로 보낼 새 쿠키를 암호화합니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
	• 인증 재정의를 위해 쿠키 허용 - 암호화된 쿠키를 사용하여 인증을 허용하도록 게이트웨이를 구성하려면 이 옵션을 선택합니다. 에이전트가 쿠키를 제공하면 게이트웨이는 사용자를 인증하기 전에 게이트웨이에서 쿠키를 암호화했는지 확인합니다. • 쿠키를 암호화/복호화할 인증서 - 게이트웨이가 쿠키를 암호화 및 복호화할 때 사용하는 인증서를 선택합니다. 게이트웨이와 포털이 모두 동일한 인증서를 사용하여 쿠키를 암호화하고 복호화하는지 확인합니다.
IP 풀 탭	
인증 서버에서 Framed-IP-Address 속성 검색	GlobalProtect 게이트웨이가 외부 인증 서버를 사용하여 고정 IP 주소를 할당할 수 있도록 하려면 이 옵션을 선택합니다. 이 옵션이 활성화되면 GlobalProtect 게이트웨이는 인증 서버의 Framed-IP-Address 속성을 사용하여 디바이스에 연결하기 위한 IP 주소를 할당합니다.
인증 서버 IP 풀	원격 사용자에게 할당할 서브넷 또는 IP 주소 범위를 추가합니다. 터널이 설정되면 GlobalProtect 게이트웨이는 인증 서버의 Framed-IP-Address 속성을 사용하여 연결 디바이스에 이 범위의 IP 주소를 할당합니다. IPv4 주소(예: 192.168.74.0/24 및 192.168.75.1-192.168.75.100) 또는 IPv6 주소(예: 2001:aa::1-2001:aa::10)를 추가할 수 있습니다. 인증 서버에서 **Framed-IP-Address** 속성 검색을 활성화한 경우에만 인증 서버 **IP** 풀을 활성화 및 구성할 수 있습니다. 인증 서버 *IP* 풀은 모든 동시 연결을 지원할 만큼 충분히 커야 합니다. *IP* 주소 할당은 고정되어 사용자가 연결을 끊은 후에도 유지됩니다. 시스템이 클라이언트의 다른 인터페이스와 충돌하지 않는 *IP* 주소를 클라이언트에 제공할 수 있도록 서로 다른 서브넷의 여러 범위를 구성합니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
	네트워크의 서버와 라우터는 이 IP 풀의 트래픽을 방화벽으로 라우팅해야 합니다. 예를 들어, 192.168.0.0/16 네트워크의 경우 원격 사용자는 192.168.0.10 주소를 수신할 수 있습니다.
IP 풀	원격 사용자에게 할당할 IP 주소 범위를 추가합니다. 터널이 설정되면 이 범위의 주소를 사용하여 원격 사용자의 엔드포인트에 인터페이스가 생성됩니다. IPv4 주소(예: 192.168.74.0/24 및 192.168.75.1-192.168.75.100) 또는 IPv6 주소(예: 2001:aa::1-2001:aa::10)를 추가할 수 있습니다. 충돌을 방지하려면 *IP* 풀이 모든 동시 연결을 지원할 만큼 충분히 커야 합니다. 게이트웨이는 클라이언트와 *IP* 주소의 인덱스를 유지하여 클라이언트가 다음에 연결할 때 동일한 *IP* 주소를 자동으로 수신하도록 합니다. 다른 서브넷에서 여러 범위를 구성하면 시스템에서 클라이언트의 다른 인터페이스와 충돌하지 않는 *IP* 주소를 클라이언트에 제공할 수 있습니다. 네트워크의 서버와 라우터는 이 IP 풀의 트래픽을 방화벽으로 라우팅해야 합니다. 예를 들어, 192.168.0.0/16 네트워크의 경우 원격 사용자에게 주소 192.168.0.10이 할당될 수 있습니다.
분할 터널 탭	
액세스 경로 탭	
로컬 네트워크에 직접 액세스할 수 없음	Windows 및 macOS 엔드포인트에서 로컬 네트워크에 대한 직접 액세스를 포함하여 분할 터널링을 비활성화하려면 이 옵션을 선택합니다. 이 기능은 사용자가 프록시 또는 가정용 프린터와 같은 로컬 리소스로 트래픽을 보내는 것을 방지합니다. 터널이 설정되면 모든 트래픽이 터널을 통해 라우팅되고 방화벽의 정책 적용을 받습니다.
포함 내용	VPN 터널에 포함할 경로를 추가합니다. 이는 게이트웨이가 VPN 연결을 통해 보낼 수 있는 사용자 엔드포인트를 지정하기 위해 원격 사용자의 엔드포인트로 푸시하는 경로입니다. IPv6 또는 IPv4 서브넷을 포함할 수 있습니다. PAN-OS 8.0.2 이상 릴리스에서는 분할 터널 게이트웨이 구성에 트래픽을 포함하기 위해 최대 100개의 액세스 경로를 사용할 수 있습니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
	GlobalProtect 앱 4.1.x 또는 이후 릴리스와 결합하지 않는 한 최대 1,000개의 액세스 경로를 사용할 수 있습니다. 모든 대상 서브넷 또는 주소 개체를 포함하려면 *0.0.0.0/0* 및 *::/0*을 액세스 경로로 포함합니다.
제외 내용	VPN 터널에서 제외할 경로를 추가합니다. 이러한 경로는 가상 어댑터(터널)가 아니라 엔드포인트의 물리적 어댑터를 통해 전송됩니다. VPN 터널을 통해 보내는 경로를 터널에 포함하는 경로, 터널에서 제외하는 경로 또는 둘의 조합으로 정의할 수 있습니다. 예를 들어 원격 사용자가 VPN 터널을 통하지 않고 인터넷에 액세스할 수 있도록 분할 터널링을 설정할 수 있습니다. 제외하려는 경로보다 더 많은 트래픽이 제외되지 않도록 제외된 경로는 포함된 경로보다 더 구체적이어야 합니다. IPv6 또는 IPv4 서브넷을 제외할 수 있습니다. 방화벽은 분할 터널 게이트웨이 구성에서 최대 100개의 제외 액세스 경로를 지원합니다. GlobalProtect 앱 4.1 이상 릴리스와 함께 사용하지 않는 한 최대 200개의 제외 액세스 경로를 사용할 수 있습니다. Chromebook에서 Android를 실행하는 엔드포인트의 액세스 경로는 제외할 수 없습니다. 크롬북에서는 IPv4 라우트만 지원됩니다. 분할 터널링을 활성화하지 않으면 모든 요청이 터널을 통해 라우팅됩니다(분할 터널링 없음). 이 경우 각 인터넷 요청은 방화벽을 통과한 다음 네트워크로 포워딩됩니다. 이 방법은 외부 당사자가 사용자 엔드포인트에 액세스하고 내부 네트워크에 액세스할 가능성을 방지할 수 있습니다(사용자 엔드포인트가 브리지 역할을 함).
도메인 및 애플리케이션 탭	
도메인 포함	대상 도메인 및 포트(선택 사항)를 기반으로 VPN 터널에 포함할 SaaS(Software as a Service) 또는 퍼블릭 클라우드 애플리케이션을 추가합니다. 게이트웨이가 VPN 연결을 통해 보낼 수 있는 사용자 엔드포인트을 지정하기 위해 원격 사용자의 엔드포인트에 푸시하는 애플리케이션입니다. ICMP는 포함되어 있지 않습니다. 목록에 최대 200개의 항목을 추가할 수 있습니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
	예를 들어 모든 Office 365 트래픽이 VPN 터널을 통과하도록 허용하려면 ***.office365.com** 도메인을 추가합니다. 각 도메인에 대한 포트 목록을 구성할 수 있습니다. 구성된 포트가 없으면 지정된 도메인의 모든 포트에 이 정책이 적용됩니다.
도메인 제외	대상 도메인 및 포트(선택 사항)를 기반으로 VPN 터널에서 제외할 SaaS(Software as a Service) 또는 퍼블릭 클라우드 애플리케이션을 추가합니다. 이러한 애플리케이션은 가상 어댑터(터널)가 아닌 엔드포인트의 물리적 어댑터를 통해 전송됩니다. 목록에 최대 200개의 항목을 추가할 수 있습니다. 예를 들어, ***.ringcentral.com** 도메인을 추가하여 VPN 터널에서 모든 링센트럴 트래픽을 제외합니다. 각 도메인에 대한 포트 목록을 구성할 수 있습니다. 구성된 포트가 없으면 지정된 도메인의 모든 포트에 이 정책이 적용됩니다. 분할 터널링을 활성화하지 않으면 모든 요청이 터널을 통해 라우팅됩니다(분할 터널링 없음). 이 경우 각 인터넷 요청은 방화벽을 통해 네트워크로 전달됩니다. 이 방법은 외부 당사자가 사용자 엔드포인트에 액세스하여 내부 네트워크에 액세스하는 것을 방지할 수 있습니다.
클라이언트 애플리케이션 프로세스 이름 포함	VPN 터널에 트래픽을 포함하려는 각 애플리케이션 프로세스의 전체 경로를 추가합니다. 이는 게이트웨이가 원격 사용자의 엔드포인트로 푸시하여 해당 사용자 엔드포인트가 VPN 연결을 통해 보낼 수 있는 항목을 지정하는 애플리케이션입니다. 목록에 최대 200개의 항목을 추가할 수 있습니다. 예를 들어, **/Application/Safari.app/Contents/MacOS/Safari** 기반 트래픽이 macOS 엔드포인트에서 VPN 터널을 통과하도록 허용할 수 있습니다.
클라이언트 애플리케이션 프로세스 이름 제외	VPN 터널에서 트래픽을 제외하려는 각 애플리케이션 프로세스의 전체 경로를 추가합니다. 이러한 애플리케이션은 가상 어댑터(터널)가 아닌 엔드포인트의 물리적 어댑터를 통해 전송됩니다. 목록에 최대 200개의 항목을 추가할 수 있습니다.

GlobalProtect Gateway 클라이언트 설정 및 네트워크 구성	설명
	예를 들어, RingCentral 애플리케이션에서 트래픽을 제외하려면 다음을 수행합니다. • Windows 엔드포인트의 경우 **%AppData%\Local\RingCentral\SoftPhoneApp\Softphone.exe** 및 **%AppData%\Local\RingCentral\SoftPhoneApp\SoftphoneMapiBridge.exe**를 추가합니다. • macOS 엔드포인트의 경우 **/Applications/RignCentral for Mac.app/Contents/MacOS/Softphone**을 추가합니다. 분할 터널링을 활성화하지 않으면 모든 요청이 터널을 통해 라우팅됩니다(분할 터널링 없음). 이 경우 각 인터넷 요청은 방화벽을 통해 네트워크로 전달됩니다. 이 방법을 통해 외부 당사자가 사용자 엔드포인트에 액세스하여 내부 네트워크에 액세스하는 것을 방지할 수 있습니다.
네트워크 서비스 탭	
DNS 서버	이 클라이언트 설정 구성이 있는 GlobalProtect 앱이 DNS 쿼리를 보내는 DNS 서버의 IP 주소를 지정합니다. 각 IP 주소를 쉼표로 구분하여 여러 DNS 서버를 추가할 수 있습니다.
DNS 서픽스	엔드포인트가 확인할 수 없는 정규화되지 않은 호스트 이름이 입력된 경우 엔드포인트가 로컬로 사용해야 하는 DNS 서픽스를 지정합니다. 각 서픽스를 쉼표로 구분하여 여러 DNS 서픽스(최대 100개)를 입력할 수 있습니다.

클라이언트 **IP** 풀 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > 클라이언트 **IP** 풀

클라이언트 **IP** 풀 탭을 선택하여 GlobalProtect™ 게이트웨이에 연결하는 모든 엔드포인트에 IPv4 또는 IPv6 주소를 할당하는 데 사용되는 전역 IP 풀을 구성합니다.

GlobalProtect 게이트웨이 클라이언트 **IP** 풀 구성 설정	설명
IP 풀	원격 사용자에게 할당할 IPv4 또는 IPv6 주소 범위를 추가합니다. 터널을 설정한 후 GlobalProtect 게이트웨이는 이 범위의 IP 주소를 해당 터널을 통해 연결하는 모든 엔드포인트에 할당합니다. 게이트웨이 수준에서 *IP* 풀을 구성하는 경우*(*네트워크 > ***GlobalProtect*** > 게이트웨이 > ***<gateway-config>*** > ***GlobalProtect*** 게이트웨이 구성 > 에이전트 > 클라이언트 ***IP*** 풀*)*, 클라이언트 수준에서 *IP* 풀을 구성하지 마십시오*(*네트워크 > ***GlobalProtect*** > 게이트웨이 > ***<gateway-config>*** > ***GlobalProtect*** 게이트웨이 구성 > 에이전트 > 클라이언트 설정 > ***<client-setting>*** > 구성 > ***IP*** 풀*).*

네트워크 서비스 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > 네트워크 서비스

네트워크 서비스 탭을 선택하여 GlobalProtect 앱이 게이트웨이와 터널을 설정할 때 엔드포인트의 가상 네트워크 어댑터에 할당할 DNS 설정을 구성합니다.

네트워크 서비스 옵션은 터널 모드를 활성화하고 터널 설정 탭에서 터널 인터페이스를 정의한 경우에만 사용할 수 있습니다.

GlobalProtect 게이트웨이 클라이언트 네트워크 서비스 구성 설정	설명
상속 소스	선택한 DHCP 클라이언트 또는 PPPoE 클라이언트 인터페이스에서 GlobalProtect 앱의 구성으로 DNS 서버 및 기타 설정을 전파할 소스를 선택합니다. 이 설정을 사용하면 DNS 서버 및 WINS 서버와 같은 모든 클라이언트 네트워크 구성이 상속 소스에서 선택한 인터페이스 구성에서 상속됩니다.

GlobalProtect 게이트웨이 클라이언트 네트워크 서비스 구성 설정	설명
상속 소스 상태 확인	상속 소스를 클릭하여 현재 클라이언트 인터페이스에 할당된 서버 설정을 확인합니다.
기본 DNS 보조 DNS	클라이언트에 DNS를 제공하는 기본 및 보조 서버의 IP 주소를 입력합니다.
기본 WINS 보조 WINS	엔드포인트에 WINS(Windows Internet Naming Service)를 제공하는 기본 및 보조 서버의 IP 주소를 입력합니다.
DNS 서픽스 상속	상속 소스에서 DNS 서픽스를 상속하려면 이 옵션을 선택합니다.
DNS 서픽스	확인할 수 없는 정규화되지 않은 호스트네임이 입력될 때 엔드포인트가 로컬로 사용해야 하는 서픽스를 추가합니다. 각 서픽스를 쉼표로 구분하여 여러 서픽스(최대 100개)를 입력할 수 있습니다.

연결 설정 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > 연결 설정

연결 설정 탭을 선택하여 GlobalProtect™ 앱에 대한 타임아웃 설정 및 인증 쿠키 사용 제한을 정의합니다.

GlobalProtect Gateway 클라이언트 터널 모드 연결 설정	설명
타임아웃 구성	
로그인 유효 시간	단일 게이트웨이 로그인 세션에 허용되는 일 수, 시간 또는 분을 지정합니다.
로그인 유효 기간이 만료되기 전에 알림	GlobalProtect 앱에서 로그인 유효 기간 만료 알림 표시를 예약하려면 시간을 분 단위로 설정합니다(기본값은 30분). 유효 기간 만료 전 알림은 로그인 유효 기간보다 작아야 합니다.
로그인 유효 기간 만료 메시지	기본 로그인 유효 기간 만료 메시지를 수정하고 로그인 유효 기간 세션이 곧 만료될 때 사용자에게 표시할 사용자 정의 메시지를 생성할 수 있습니다. 최대 메시지 길이는 127자입니다.

GlobalProtect Gateway 클라이언트 터널 모드 연결 설정	설명
비활동 로그아웃	비활성 세션이 자동으로 로그아웃되는 시간(분)을 지정합니다(터널 모드의 범위는 5~43200분, 비터널 모드의 경우 120~43200분, 기본값은 180분). GlobalProtect 앱이 VPN 터널을 통해 트래픽을 라우팅하지 않았거나 게이트웨이가 구성된 기간 내에 엔드포인트로부터 HIP 검사를 받지 못한 경우 사용자는 GlobalProtect에서 로그아웃됩니다.
비활성 로그아웃 전 알림(분)	비활성 로그아웃 시간 전 알림을 분 단위로 설정하여(기본값은 30분) 앱에서 비활성 로그아웃 알림 표시를 예약합니다. 비활성 로그아웃 전 알림 은 비활성 로그아웃 기간보다 짧아야 합니다.
비활성 로그아웃 메시지	기본 메시지를 수정하고 비활성 세션이 만료되려고 할 때 사용자에게 표시할 사용자 정의 메시지를 만들 수 있습니다. 최대 메시지 길이는 127자입니다.
관리자가 시작한 로그아웃 시 사용자에게 알림	관리자가 로그아웃을 시작한 후 앱이 사용자에게 알림을 표시하도록 하려면 이 옵션을 활성화합니다.
관리자 로그아웃 메시지	기본 메시지를 수정하고 관리자가 로그아웃을 시작한 후 사용자에게 표시할 사용자 지정 메시지를 만들 수 있습니다. 최대 메시지 길이는 127자입니다.
인증 쿠키 사용 제한	
SSL VPN 자동 복원 비활성화	SSL VPN 터널의 자동 복원을 방지하려면 이 옵션을 활성화합니다. 이 옵션을 활성화하면 *GlobalProtect*가 *Resilient VPN*을 지원하지 않습니다.
인증 쿠키 사용 제한(VPN 터널 자동 복원 또는 인증 재정의)	다음 조건 중 하나에 따라 인증 쿠키 사용을 제한하려면 이 옵션을 활성화합니다. • 인증 쿠키가 발행된 원래 소스 **IP** - 쿠키가 원래 발행된 엔드포인트와 동일한 공개 소스 IP 주소를 가진 엔드포인트로 인증 쿠키 사용을 제한합니다. • 원래 소스 **IP** 네트워크 범위 - 지정된 네트워크 IP 주소 범위 내에 공용 소스 IP 주소가 있는 엔드포인트로 인증 쿠키 사용을 제한합니다. 소스

GlobalProtect Gateway 클라이언트 터널 모드 연결 설정	설명
	IPv4 넷마스크를 입력하여 IPv4 주소 범위를 지정하거나 소스 **IPv6** 넷마스크를 입력하여 IPv6 주소 범위를 지정합니다. 넷마스크 중 하나를 **0**으로 설정하면 지정된 IP 주소 유형에 대해 이 옵션이 비활성화됩니다. 예를 들어 포털 또는 게이트웨이가 하나의 IP 주소 유형(IPv4 또는 IPv6)만 지원하거나 하나의 IP 주소 유형에 대해서만 이 옵션을 활성화하려는 경우 넷마스크를 **0**으로 설정할 수 있습니다(포털 또는 게이트웨이가 IPv4와 IPv6을 모두 지원하는 경우). 지정된 게이트웨이 구성에서 하나의 넷마스크만 **0**으로 설정할 수 있으며, 두 넷마스크를 동시에 **0**으로 설정할 수는 없습니다. 기본 소스 **IPv4** 넷마스크 값 **32**를 수락하면 인증 쿠키 사용이 쿠키가 원래 발급된 엔드포인트의 동일한 공용 IPv4 주소로 제한됩니다. 기본 소스 **IPv6** 넷마스크 값 **128**을 수락하면 인증 쿠키 사용이 쿠키가 원래 발급된 엔드포인트의 동일한 공용 IPv6 주소로 제한됩니다.

비디오 트래픽 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > 비디오 트래픽

VPN 터널에서 비디오 스트리밍 트래픽을 제외하려면 비디오 트래픽 탭을 선택합니다.

GlobalProtect 게이트웨이 비디오 트래픽 구성 설정	설명
터널에서 비디오 애플리케이션 제외	VPN 터널에서 비디오 스트리밍 트래픽을 제외하려면 이 옵션을 선택합니다.
애플리케이션	VPN 터널에서 제외할 비디오 스트리밍 애플리케이션을 추가하거나 찾아보십시오. 이 비디오 리디렉션은 다음 애플리케이션의 모든 비디오 트래픽 유형에 적용할 수 있습니다. • 유튜브 • 데일리모션 • 넷플릭스 다른 비디오 스트리밍 애플리케이션의 경우 다음 비디오 유형만 리디렉션할 수 있습니다.

GlobalProtect 게이트웨이 비디오 트래픽 구성 설정	설명
	• MP4 • WebM • MPEG 비디오 스트리밍 트래픽은 VPN 터널에서만 제외할 수 있습니다. 비디오 스트리밍 애플리케이션을 제외하지 않으면 모든 요청이 터널을 통해 라우팅 됩니다(스플릿 터널링 없음). 이 경우 각 인터넷 요청은 방화벽을 통해 네트워크로 전달됩니다. 이 방법을 통해 외부 당사자가 사용자 엔드포인트에 액세스하여 내부 네트워크에 액세스하는 것을 방지할 수 있습니다.

HIP 알림 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 에이전트 > ***<agent-config>*** > **HIP** 알림

HIP 알림 탭을 선택하여 최종 사용자가 호스트 정보 프로파일(HIP)이 있는 보안 규칙이 적용되는 시기를 확인하는 알림 메시지를 정의합니다.

이러한 옵션은 HIP 프로파일을 만들고 보안 정책에 추가한 경우에만 사용할 수 있습니다.

GlobalProtect 에이전트 **HIP** 알림 구성 설정	설명
HIP 알림	HIP 알림을추가하고 옵션을 구성합니다. 매치 메시지,일치하지 않는 메시지, 또는 둘 다에 대한 알림을 활성화한 다음 알림을 시스템 트레이 풍선 또는 팝업 메시지로 표시할지의 여부를 지정할 수 있습니다. 그런 다음 일치하거나 일치하지 않을 메시지를 지정합니다. 이러한 설정을 사용하여 호스트 시스템에 필요한 응용 프로그램이 설치되어 있지 않다는 경고 메시지와 같은 시스템 상태에 대해 최종 사용자에게 알립니다. 일치 메시지의 경우 모바일 앱 목록을 포함하여 HIP 일치를 트리거한 애플리케이션을 표시하는 옵션을 사용하도록 설정할 수도 있습니다. 외부 웹사이트 및 리소스에 대한 링크를 포함할 수 있는 풍부한 *HTML*로 *HIP* 알림 메시지를 포맷할 수 있습니다. 서식 있는 텍스트 설정 도구 모음에서 하이퍼링크*(*  *)*를 클릭하여 링크를 추가합니다.

GlobalProtect 게이트웨이 새틀라이트 탭

- 네트워크 > **GlobalProtect** > 게이트웨이 > ***<gateway-config>*** > 위성

새틀라이트는 일반적으로 지사에 있는 Palo Alto Networks 방화벽으로 GlobalProtect 게이트웨이에 VPN 연결을 설정할 수 있도록 하는 GlobalProtect 앱 역할을 합니다. **Satellite** 탭을 선택하여 게이트웨이 터널과 네트워크 설정을 정의하여 Satellite에서 VPN 연결을 설정할 수 있도록 합니다. 새틀라이트에서 보급하는 경로를 구성할 수도 있습니다.

- 터널 설정 탭
- 네트워크 설정 탭
- 경로 필터 탭

GlobalProtect Gateway Satellite 구성 설정	설명
터널 설정 탭	
터널 구성	터널 구성을 선택한 다음 기존 터널 인터페이스를 선택하거나 드롭다운에서 새 터널 인터페이스를 선택합니다. 자세한 내용은 네트워크 > 인터페이스 > 터널을 참조하십시오. • 재생 공격 탐지 - 재생 공격으로부터 보호합니다. 새틀라이트 터널 구성을 활성화한 경우 재생 공격 탐지를 활성화하여 재생 공격으로부터 *GlobalProtect* 새틀라이트를 보호합니다. • **TOS** 복사 - 원래 ToS 정보를 보존하기 위해 내부 IP 헤더에서 캡슐화된 패킷의 외부 IP 헤더로 서비스 유형(ToS) 헤더를 복사합니다. • 구성 새로 고침 인터벌(시간) - 새틀라이트가 포털에서 구성 업데이트를 확인해야 하는 빈도를 지정합니다(범위는 1-48, 기본값은 2).
터널 모니터링	새틀라이트가 게이트웨이 터널 연결을 모니터링할 수 있도록 하려면 터널 모니터링을 선택하여 연결에 실패할 경우 백업 게이트웨이로 페일오버할 수 있습니다. • 대상 주소 - 터널 모니터가 게이트웨이에 대한 연결이 있는지 확인하는 데 사용할 **IPv4** 또는 **IPv6** 주소를 지정합니다(예: 게이트웨이에 의해 보호되는 네트워크의 IP 주소). 또는 터널 인터페이스에 대한 IP 주소를 구성한 경우 이 필드를 비워 둘 수 있으며 터널 모니터는 대신 터널 인터페이스를 사용하여 연결이 활성 상태인지 확인합니다.

GlobalProtect Gateway Satellite 구성 설정	설명
	• 터널 모니터 프로파일 - 다른 게이트웨이로의 페일오버는 LSVPN에서 지원되는 유일한 유형의 터널 모니터링 프로파일입니다. 터널 모니터링을 활성화하고 터널 모니터링 프로파일을 구성하여 새틀라이트 터널 구성을 활성화한 경우 페일오버 작업을 제어합니다.
암호화 프로파일	**IPSec** 암호화 프로파일을 선택하거나 새로 만듭니다. 암호화 프로파일은 VPN 터널의 식별, 인증 및 암호화를 위한 프로토콜과 알고리즘을 결정합니다. LSVPN의 두 터널 엔드포인트는 조직 내에서 신뢰할 수 있는 방화벽이므로 일반적으로 ESP 프로토콜, DH 그룹2, AES 128 CVC 암호화 및 SHA-1 인증을 사용하는 기본 프로파일을 사용합니다. 자세한 내용은 네트워크 > 네트워크 프로파일 > GlobalProtect IPSec 암호화를 참조하십시오.
네트워크 설정 탭	
상속 소스	선택한 DHCP 클라이언트 또는 PPPoE 클라이언트 인터페이스에서 GlobalProtect 새틀라이트 구성으로 DNS 서버 및 기타 설정을 전파할 소스를 선택합니다. 이 설정을 사용하면 DNS 서버와 같은 모든 네트워크 구성이 상속 소스에서 선택한 인터페이스 구성에서 상속됩니다.
기본 DNS 보조 DNS	새틀라이트에 DNS를 제공하는 기본 및 보조 서버의 IP 주소를 입력합니다.
DNS 서픽스	추가를 클릭하여 분석할 수 없는 정규화되지 않은 호스트 이름이 입력될 때 새틀라이트가 로컬로 사용해야 하는 서픽스를 입력하십시오. 여러 서픽스를 쉼표로 구분하여 입력할 수 있습니다.
DNS 서픽스 상속	확인할 수 없는 정규화되지 않은 호스트 이름이 입력될 때 로컬로 사용할 DNS 서픽스를 새틀라이트으로 보내려면 이 옵션을 선택합니다.
IP 풀	VPN 터널 설정 시 새틀라이트의 터널 인터페이스에 할당할 IP 주소 범위를 추가합니다. IPv6 또는 IPv4 주소를 지정할 수 있습니다. *IP* 풀은 모든 동시 연결을 지원할 만큼 충분히 커야 합니다. *IP* 주소 할당은 동적이며 새틀라이트 연결이 끊긴 후에도 유지되지 않습니다. 다른 서브넷에서 여러 범위를 구성하면 시스템에서 새틀라이트의 다른 인터페이스와 충돌하지 않는 *IP* 주소를 새틀라이트에 제공할 수 있습니다.

GlobalProtect Gateway Satellite 구성 설정	설명
	네트워크의 서버와 라우터는 이 IP 풀의 트래픽을 방화벽으로 라우팅해야 합니다. 예를 들어, 192.168.0.0/16 네트워크의 경우 새틀라이트에 주소 192.168.0.10을 할당할 수 있습니다. 동적 라우팅을 사용하는 경우 새틀라이트에 대해 지정한 IP 주소 풀이 게이트웨이 및 새틀라이트의 터널 인터페이스에 수동으로 할당한 IP 주소와 겹치지 않는지 확인하십시오.
액세스 경로	추가를 클릭하고 다음과 같이 경로를 입력합니다. • 터널을 통해 새틀라이트의 모든 트래픽을 라우팅하려면 이 필드를 비워 둡니다. • 게이트웨이를 통해 일부 트래픽만 라우팅하려면(분할 터널링이라고 함) 터널링해야 하는 대상 서브넷을 지정합니다. 이 경우 새틀라이트는 자체 라우팅 테이블을 사용하여 지정된 액세스 경로로 향하지 않는 트래픽을 라우팅합니다. 예를 들어 회사 네트워크로 향하는 트래픽만 터널링하도록 선택한 다음 로컬 새틀라이트를 사용하여 안전한 인터넷 액세스를 활성화할 수 있습니다. • 새틀라이트 간 라우팅을 활성화하려면 각 새틀라이트에서 보호하는 네트워크에 대한 요약 경로를 입력합니다.
경로 필터 탭	
게시된 경로 수락	새틀라이트에서 게이트웨이의 라우팅 테이블에 보급한 경로를 수락하려면 게시된 경로 수락을 활성화합니다. 이 옵션을 선택하지 않으면 게이트웨이는 새틀라이트에서 보급한 경로를 수락하지 않습니다.
허용된 서브넷	새틀라이트에서 보급한 경로를 더 제한적으로 수락하려면 허용된 서브넷을 추가하고 게이트웨이가 경로를 수락할 수 있는 서브넷을 정의하십시오. 목록의 일부가 아닌 새틀라이트에 의해 보급된 서브넷은 필터링됩니다. 예를 들어 모든 새틀라이트가 LAN 측에서 192.168.x.0/24 서브넷으로 구성된 경우 게이트웨이에서 192.168.0.0/16의 허용 경로를 구성할 수 있습니다. 이 구성은 게이트웨이가 새틀라이트가 192.168.0.0/16 서브넷에 있는 경우에만 새틀라이트의 경로를 수락하도록 합니다.

Network > GlobalProtect > MDM

Mobile Security Manager를 사용하여 최종 사용자 모바일 엔드포인트를 관리하고 HIP 지원 정책 시행을 사용하는 경우 관리되는 엔드포인트에 대한 HIP 보고서를 검색하기 위해 Mobile Security Manager와 통신하도록 게이트웨이를 구성해야 합니다.

게이트웨이가 Mobile Security Manager와 통신할 수 있도록 Mobile Security Manager에 대한 MDM 정보를 추가하십시오.

GlobalProtect MDM 설정	설명
이름	Mobile Security Manager의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
	방화벽이 다중 가상 시스템 모드에 있는 경우 MDM 설정은 Mobile Security Manager를 사용할 수 있는 가상 시스템(vsys)을 표시합니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 이 필드는 MDM 대화 상자에 표시되지 않습니다. Mobile Security Manager를 저장한 후에는 위치를 변경할 수 없습니다.
연결 설정	
서버	게이트웨이가 HIP 보고서를 검색하기 위해 연결하는 Mobile Security Manager 인터페이스의 IP 주소 또는 FQDN을 입력합니다. 이 인터페이스에 대한 서비스 경로가 있는지 확인하십시오.
연결 포트	연결 포트는 Mobile Security Manager가 HIP 보고서 요청을 수신하는 곳입니다. 기본 포트는 GlobalProtect Mobile Security Manager가 수신하는 동일한 포트인 5008입니다. 타사 Mobile Security Manager를 사용하는 경우 해당 서버가 HIP 보고서 요청을 수신하는 포트 번호를 입력하십시오.
클라이언트 인증서	게이트웨이가 HTTPS 연결을 설정할 때 Mobile Security Manager에 제공할 클라이언트 인증서를 선택하십시오. 이 인증서는 Mobile Security Manager가 상호 인증을 사용하도록 구성된 경우에만 필요합니다.
신뢰할 수 있는 루트 CA	추가를 클릭한 다음 게이트웨이가 HIP 보고서를 검색하기 위해 연결하는 인터페이스에 대한 인증서를 발급하는 데 사용된 루트 CA 인증서를 선택합니다. (이 서버 인증서는 Mobile Security Manager의 엔드포인트 체크인 인터페이스에 대해 발급된 인증서와 다를 수 있습니다.) 루트 CA 인증서를 가져와서 이 목록에 추가해야 합니다.

네트워크 > 글로벌 > 클라이언트리스 앱

네트워크 > **GlobalProtect** > 클라이언트리스 앱을 선택하여 GlobalProtect 클라이언트리스 VPN을 통해 액세스할 수 있는 애플리케이션을 추가합니다. 개별 클라이언트가 없는 애플리케이션을 추가한 다음 네트워크 > **GlobalProtect** > 클라이언트가 없는 앱 그룹을 선택하여 애플리케이션 그룹을 정의할 수 있습니다.

GlobalProtect Clientless VPN은 HTML, HTML5 및 자바스크립트 기술을 사용하는 공통 엔터프라이즈 웹 애플리케이션에 대한 안전한 원격 액세스를 제공합니다. 사용자는 GlobalProtect 소프트웨어를 설치하지 않고도 SSL 지원 웹 브라우저에서 보안 액세스의 이점을 누릴 수 있습니다. 이 기능은 파트너 또는 계약자가 애플리케이션에 액세스할 수 있도록 하고 개인 디바이스를 포함하여 관리되지 않는 자산을 안전하게 사용하도록 설정해야 하는 경우에 유용합니다.

이 기능을 사용하려면 **GlobalProtect** 클라이언트리스 **VPN** 동적 업데이트가 필요합니다. 또한 이 기능을 사용하려면 GlobalProtect 포털에서 클라이언트리스 VPN을 호스팅하는 방화벽에 GlobalProtect 구독을 설치해야 합니다.

클라이언트리스 앱 설정	설명
이름	애플리케이션에 대한 설명 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
위치	다중 가상 시스템 모드에 있는 방화벽의 경우 위치는 GlobalProtect 게이트웨이를 사용할 수 있는 가상 시스템(vsys)입니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 위치 필드가 GlobalProtect Gateway 대화 상자에 나타나지 않습니다. 게이트웨이 구성을 저장한 후에는 위치를 변경할 수 없습니다.
애플리케이션 홈 URL	애플리케이션이 있는 URL(최대 4095자)을 입력합니다.
애플리케이션 설명	(선택사항)애플리케이션(최대 255자)에 대한 설명을 입력합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
애플리케이션 아이콘	(선택사항)아이콘을 업로드하여 게시된 애플리케이션 페이지에서 애플리케이션을 식별합니다. 아이콘을 업로드하려면 찾아볼 수 있습니다.

네트워크 > GlobalProtect > 클라이언트리스 앱 그룹

Network > **GlobalProtect** > **Clientless** 앱 그룹을 선택하여 GlobalProtect Clientless VPN을 통해 액세스할 수 있는 애플리케이션을 그룹화합니다. 기존 클라이언트리스 애플리케이션을 그룹에 추가하거나 그룹에 대한 새 클라이언트리스 애플리케이션을 구성할 수 있습니다. 그룹은 동시에 여러 애플리케이션으로 작업하는 데 유용합니다. 예를 들어, 클라이언트리스 VPN 액세스에 대해 구성하려는 표준 SaaS 애플리케이션(예: Workday, JIRA 또는 Bugzilla) 세트가 있을 수 있습니다.

클라이언트리스 앱 그룹 설정	설명
이름	애플리케이션 그룹을 설명하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
위치	다중 가상 시스템 모드에 있는 방화벽의 경우 위치는 GlobalProtect 게이트웨이를 사용할 수 있는 가상 시스템(vsys)입니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 위치 필드가 GlobalProtect Gateway 대화 상자에 나타나지 않습니다. 게이트웨이 구성을 저장한 후에는 위치를 변경할 수 없습니다.
애플리케이션	드롭다운에서 애플리케이션을 추가하거나 새 클라이언트리스 애플리케이션을 구성하고 그룹에 추가합니다. 새로운 클라이언트리스 애플리케이션을 구성하려면 네트워크 > GlobalProtect > 클라이언트리스 앱을 참조하십시오.

개체 > GlobalProtect > HIP 개체

개체 > **GlobalProtect** > **HIP** 개체를 선택하여 호스트 정보 프로파일(HIP)에 대한 개체를 정의합니다. HIP 개체는 정책을 시행하는 데 사용하려는 앱에서 보고한 원시 데이터를 필터링하기 위한 일치 기준을 제공합니다. 예를 들어 원시 호스트 데이터에 엔드포인트의 여러 바이러스 백신 패키지에 대한 정보가 포함된 경우 조직에서 해당 패키지가 필요하기 때문에 특정 애플리케이션에 관심이 있을 수 있습니다. 이 시나리오에서는 적용하려는 특정 애플리케이션과 일치하도록 HIP 개체를 생성합니다.

필요한 HIP 개체를 결정하는 가장 좋은 방법은 호스트 정보를 사용하여 정책을 시행하는 방법을 결정하는 것입니다. HIP 개체는 보안 정책에서 사용할 수 있는 HIP 프로파일을 만들 수 있도록 하는 빌딩 블록일 뿐입니다. 따라서 특정 유형의 필수 소프트웨어 존재, 특정 도메인의 구성원 자격 또는 특정 엔드포인트 OS의 존재와 같은 한 가지에 대해 일치하도록 개체를 단순하게 유지하고자 할 수 있습니다. 이 접근 방식을 사용하면 매우 세분화된 HIP 강화 정책을 유연하게 생성할 수 있습니다.

HIP 개체를 생성하려면 추가를 클릭하여 HIP 개체 대화 상자를 엽니다. 특정 필드에 입력할 내용에 대한 설명은 다음 표를 참조하십시오.

- HIP 개체 일반 탭
- HIP 개체 모바일 디바이스 탭
- HIP 개체 패치 관리 탭
- HIP 개체 방화벽 탭
- HIP 개체 안티 멀웨어 탭
- HIP 개체 디스크 백업 탭
- HIP 개체 디스크 암호화 탭
- HIP 개체 데이터 손실 방지 탭
- HIP 개체 인증서 탭
- HIP 개체 사용자 정의 검사 탭

HIP 강화 보안 정책 생성에 대한 자세한 내용은 *GlobalProtect* 관리자 안내서에서 HIP 기반 정책 시행 구성을 참조하십시오.

HIP 개체 일반 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 일반

일반 탭을 선택하여 새 HIP 개체의 이름을 지정하고 도메인, 운영 체제 또는 네트워크 연결 유형과 같은 일반 호스트 정보와 일치하도록 개체를 구성합니다.

HIP 개체 일반 설정	설명
이름	HIP 개체의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
공유	공유를 선택하면 현재 HIP 개체를 다음에 사용할 수 있습니다. 다중 가상 시스템 모드에 있는 방화벽에 로그인한 경우 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭의 가상 시스템 드롭다운에서 선택한 vsys에서만 개체를 사용할 수 있습니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 HIP 개체 대화 상자에서 이 옵션을 사용할 수 없습니다. Panorama™의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭의 디바이스 그룹 드롭다운에서 선택한 디바이스 그룹에서만 개체를 사용할 수 있습니다. 개체를 저장한 후에는 공유 설정을 변경할 수 없습니다. 현재 위치를 보려면 **Objects** > **GlobalProtect** > **HIP Objects**를 선택하십시오.
설명	(선택 사항) 설명을 입력합니다.
호스트 정보	호스트 정보 구성 옵션을 활성화하려면 이 옵션을 선택합니다.
관리	엔드포인트가 관리되는지의 여부에 따라 필터링합니다. 관리되는 엔드포인트를 일치시키려면 예를 선택하십시오. 관리되지 않는 엔드포인트를 일치시키려면 아니오를 선택합니다.
재정의 비활성화(Panorama만 해당)	제어는 개체 탭에서 선택한 디바이스 그룹의 하위 항목인 디바이스 그룹의 HIP 개체에 대한 액세스를 재정의합니다. 관리자가 상속된 값을 재정의하여 하위 디바이스 그룹에 개체의 로컬 복사본을 생성하지 못하도록 하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택 취소되어 있습니다(재정의가 활성화됨).
도메인	도메인 이름을 일치시키려면 드롭다운에서 연산자를 선택한 다음 일치시킬 문자열을 입력하십시오.
OS	호스트 OS에서 일치시키려면 첫 번째 드롭다운에서 포함을 선택한 다음 두 번째 드롭다운에서 공급자를 선택한 다음 세 번째 드롭다운에서 OS 버전을 선택합니다. 또는 선택한 공급자의 모든 OS 버전에서 일치하도록 모두를 선택할 수 있습니다.
클라이언트 버전	특정 버전 번호와 일치시키려면 드롭다운에서 연산자를 선택한 다음 텍스트 상자에 일치(또는 일치하지 않음)할 문자열을 입력합니다.

HIP 개체 일반 설정	설명
호스트 이름	특정 호스트 이름이나 호스트 이름의 일부를 일치시키려면 드롭다운에서 연산자를 선택한 다음 텍스트 상자에 일치(또는 선택한 연산자에 따라 일치하지 않음)시킬 문자열을 입력합니다.
호스트 ID	호스트 ID는 GlobalProtect가 호스트를 식별하기 위해 할당하는 고유 ID입니다. 호스트 ID 값은 디바이스 유형에 따라 다릅니다. • **Windows** - Windows 레지스트리에 저장된 컴퓨터 GUID(HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) • **macOS** - 최초의 내장형 물리 네트워크 인터페이스의 MAC 주소 • 안드로이드—안드로이드 ID • **iOS**—UDID • **Linux** - 시스템 DMI 테이블에서 검색된 제품 UUID • **Chrome** - 길이가 32자인 GlobalProtect 할당 고유 영숫자 문자열 특정 호스트 ID와 일치시키려면 드롭다운에서 연산자를 선택한 다음 텍스트 상자에 일치(또는 선택한 연산자에 따라 일치하지 않음)시킬 문자열을 입력합니다.
일련번호	엔드포인트 일련번호의 전체 또는 일부를 일치시키려면 드롭다운에서 연산자를 선택한 다음 일치시킬 문자열을 입력합니다.
네트워크	이 필드를 사용하여 특정 모바일 디바이스 네트워크 구성에 대한 필터링을 활성화합니다. 이 일치 기준은 모바일 디바이스에만 적용됩니다. 드롭다운에서 운영자를 선택한 다음 두 번째 드롭다운에서 필터링할 네트워크 연결 유형을 선택합니다. **Wi-Fi**, 모바일, 이더넷(**Is Not** 필터에만 사용 가능) 또는 **Unknown**. 네트워크 유형을 선택한 후 모바일 캐리어 또는 Wi-Fi **SSID**와 같이 가능한 경우 일치시킬 추가 문자열을 입력합니다.

HIP 개체 모바일 디바이스 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 휴대용 디바이스

Mobile Device 탭을 선택하여 GlobalProtect 앱을 실행하는 모바일 디바이스에서 수집된 데이터에서 HIP 일치를 활성화합니다.

모바일 디바이스 속성을 수집하고 *HIP* 시행 정책에서 활용하려면 *GlobalProtect*에 *MDM* 서버가 필요합니다. *GlobalProtect*는 현재 *AirWatch MDM* 서버와의 *HIP* 통합을 지원합니다.

HIP 개체 모바일 디바이스 설정	설명
휴대용 디바이스	GlobalProtect 앱을 실행하는 모바일 디바이스에서 수집된 호스트 데이터에 대한 필터링을 활성화하고 디바이스, 설정 및 앱 탭을 활성화하려면 이 옵션을 선택합니다.
디바이스 탭	• 모델 - 특정 디바이스 모델에서 일치시키려면 드롭다운에서 연산자를 선택한 다음 일치시킬 문자열을 입력합니다. • 태그 - GlobalProtect Mobile Security Manager에 정의된 태그 값과 일치시키려면 첫 번째 드롭다운에서 연산자를 선택한 다음 두 번째 드롭다운에서 태그를 선택합니다. • 전화번호 - 디바이스 전화번호의 전체 또는 일부를 일치시키려면 드롭다운에서 교환원을 선택한 다음 일치시킬 문자열을 입력합니다. • **IMEI** - 디바이스 IMEI(International Mobile Equipment Identity) 번호의 전체 또는 일부를 일치시키려면 드롭다운에서 연산자를 선택한 다음 일치시킬 문자열을 입력합니다.
설정 탭	• 암호 - 디바이스에 암호가 설정되어 있는지의 여부를 기준으로 필터링합니다. 암호가 설정된 디바이스를 일치시키려면 예를 선택합니다. 암호가 설정되지 않은 디바이스를 일치시키려면 아니오를 선택하십시오. • 루팅/탈옥 - 디바이스가 루팅되었거나 탈옥되었는지의 여부에 따라 필터링합니다. 루팅되었거나 탈옥된 디바이스를 일치시키려면 예를 선택하십시오. 루팅되지 않았거나 탈옥되지 않은 디바이스를 일치시키려면 아니오를 선택하십시오. • 디스크 암호화 - 디바이스 데이터가 암호화되었는지의 여부를 기준으로 필터링합니다. 디스크 암호화가 활성화된 디바이스를 일치시키려면 예를 선택합니다. 디스크 암호화가 활성화되지 않은 디바이스를 일치시키려면 아니오를 선택하십시오. • 마지막 체크인 이후 시간 - 디바이스가 MDM으로 마지막으로 체크인된 시간을 기준으로 필터링합니다. 드롭다운에서 교환원을 선택한 다음 체크인 기간의 일 수를 지정합니다. 예를 들어, 지난 5일 이내에 체크인하지 않은 디바이스와 일치하도록 개체를 정의할 수 있습니다.
앱 탭	• 앱 - (Android 디바이스만 해당) 디바이스에 설치된 앱과 디바이스에 멀웨어에 감염된 앱이 설치되어 있는지의 여부를 기반으로 필터링을 활성화하려면 이 옵션을 선택합니다. • 기준 탭 • 멀웨어 있음 - 멀웨어에 감염된 앱이 설치된 디바이스를 일치시키려면 예를 선택합니다. 멀웨어에 감염된 앱이 설치되지 않은 디바이스

HIP 개체 모바일 디바이스 설정	설명
	와 일치시키려면 아니오를 선택합니다. 멀웨어 있음을 일치 기준으로 사용하지 않으려면 없음을 선택합니다. • 포함 탭 • 패키지 - 특정 앱이 설치된 디바이스를 일치시키려면 앱을 추가하고 역방향 DNS 형식으로 고유한 앱 이름을 입력합니다. 예를 들어 com.netflix.mediaclient를 입력한 다음 GlobalProtect 앱이 계산하고 디바이스 HIP 보고서와 함께 제출하는 해당 앱 해시를 입력합니다.

HIP 개체 패치 관리 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 패치 관리

패치 관리 탭을 선택하여 GlobalProtect 엔드포인트의 패치 상태에서 HIP 일치를 활성화합니다.

HIP 개체 패치 관리 설정	설명
패치 관리	호스트의 패치 관리 상태에서 일치를 활성화하고 기준 및 공급자 탭을 활성화하려면 이 옵션을 선택합니다.

기준 탭	다음 설정을 지정합니다.
	• 설치됨 - 패치 관리 소프트웨어가 호스트에 설치되어 있는지의 여부와 일치합니다.
	• 활성화됨 - 패치 관리 소프트웨어가 호스트에서 활성화되었는지의 여부와 일치합니다. 설치됨 선택을 취소하면 이 필드는 자동으로 없음으로 설정되고 편집할 수 없습니다.
	• 심각도 - 호스트에 지정된 심각도 값의 누락된 패치가 있는지의 여부를 일치시키기 위해 논리 연산자 목록에서 선택합니다.
	GlobalProtect 심각도 값과 OPSWAT 심각도 등급 간의 다음 매핑을 사용하여 각 값의 의미를 이해하십시오.
	  • **0** - 낮음
	  • **1** - 보통
	  • **2** - 중요
	  • **3** - 중요
	• 확인 - 엔드포인트에 누락된 패치가 있는지의 여부와 일치시킵니다.

HIP 개체 패치 관리 설정	설명
	• 패치 - 호스트에 특정 패치가 있는지의 여부와 일치시킵니다. 추가를 클릭하고 확인할 특정 패치에 대한 KB 문서 ID를 입력합니다. 예를 들어 Microsoft Office 2010(KB3128031) 32비트 버전용 업데이트를 확인하려면 **3128031**을 입력합니다.
공급자 탭	패치 관리 소프트웨어 및 제품의 특정 공급자를 정의하여 일치 여부를 결정하기 위해 엔드포인트에서 찾을 수 있습니다. 추가를 클릭한 다음 드롭다운에서 공급자를 선택합니다. 선택적으로 추가를 클릭하여 특정 제품을 선택합니다. 확인을 클릭하여 설정을 저장합니다.

HIP 개체 방화벽 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 방화벽

방화벽 탭을 선택하여 GlobalProtect 엔드포인트의 방화벽 소프트웨어 상태를 기반으로 HIP 일치를 활성화합니다.

HIP 개체 방화벽 설정
방화벽을 선택하여 호스트의 방화벽 소프트웨어 상태에 대한 일치를 활성화합니다. • 설치됨 - 방화벽 소프트웨어가 호스트에 설치되어 있는지의 여부와 일치합니다. • 활성화됨 - 호스트에서 방화벽 소프트웨어가 활성화되었는지의 여부와 일치합니다. 설치됨 선택을 취소하면 이 필드는 자동으로 없음으로 설정되고 편집할 수 없습니다. • 공급자 및 제품 - 일치 여부를 결정하기 위해 호스트에서 찾을 특정 방화벽 소프트웨어 공급자 및/또는 제품을 정의합니다. 추가를 클릭한 다음 드롭다운에서 공급자를 선택합니다. 선택적으로 추가를 클릭하여 특정 제품을 선택합니다. 확인을 클릭하여 설정을 저장합니다. • 공급자 제외 - 지정된 공급자의 소프트웨어가 없는 호스트를 일치시키려면 이 옵션을 선택합니다.

HIP 개체 안티 멀웨어 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 맬웨어 방지

Anti-Malware 탭을 선택하여 GlobalProtect 엔드포인트에서 안티바이러스 또는 안티스파이웨어 적용 범위를 기반으로 HIP 일치를 활성화합니다.

HIP 개체 멀웨어 방지 설정
호스트의 안티바이러스 또는 안티스파이웨어 적용 범위를 기반으로 일치를 활성화하려면 안티멀웨어를 선택합니다. 다음과 같이 일치에 대한 추가 일치 기준을 정의합니다.

HIP 개체 멀웨어 방지 설정

- 설치됨 - 호스트에 바이러스 백신 또는 안티 스파이웨어 소프트웨어가 설치되어 있는지 일치합니다.
- 실시간 보호 - 호스트에서 실시간 안티바이러스 또는 안티스파이웨어 보호가 활성화되었는지의 여부를 일치시킵니다. 설치됨 선택을 취소하면 이 필드가 자동으로 없음으로 설정되고 편집할 수 없습니다.
- 바이러스 정의 버전 - 바이러스 정의가 지정된 일 수 또는 릴리스 버전 내에 업데이트된 경우 일치합니다.
- 제품 버전 - 바이러스 백신 또는 안티 스파이웨어 소프트웨어의 특정 버전과 일치시킵니다. 버전을 지정하려면 드롭다운에서 연산자를 선택한 다음 제품 버전을 나타내는 문자열을 입력합니다.
- 마지막 검사 시간 - 바이러스 백신 또는 안티 스파이웨어 검사가 마지막으로 실행된 시간을 기준으로 일치 여부를 지정합니다. 드롭다운에서 연산자를 선택한 다음 비교할 일 또는 시간을 지정합니다.
- 공급자 및 제품 - 특정 안티바이러스 또는 안티스파이웨어 소프트웨어 공급자 및/또는 제품을 정의하여 일치 여부를 결정합니다. 추가를 클릭한 다음 드롭다운에서 공급자를 선택합니다. 선택적으로 추가를 클릭하여 특정 제품을 선택합니다. 확인을 클릭하여 설정을 저장합니다.
- 공급자 제외 - 지정된 공급자의 소프트웨어가 없는 호스트를 일치시키려면 이 옵션을 선택합니다.

HIP 개체 디스크 백업 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 디스크 백업

디스크 백업 탭을 선택하여 GlobalProtect 엔드포인트의 디스크 백업 상태를 기반으로 HIP 일치를 활성화합니다.

HIP 개체 디스크 백업 설정

디스크 백업을 선택하여 호스트의 디스크 백업 상태에 대한 일치를 활성화한 다음 일치에 대한 추가 일치 기준을 다음과 같이 정의합니다.

- 설치됨 - 디스크 백업 소프트웨어가 호스트에 설치되어 있는지의 여부와 일치합니다.
- 마지막 백업 시간 - 마지막 디스크 백업이 실행된 시간을 기준으로 일치 여부를 지정합니다. 드롭다운에서 연산자를 선택한 다음 비교할 일 또는 시간을 지정합니다.
- 공급자 및 제품 - 호스트에서 일치시킬 특정 디스크 백업 소프트웨어 공급자 및 제품을 정의합니다. 추가를 클릭한 다음 드롭다운에서 공급자를 선택합니다. 선택적으로 추가를 클릭하여 특정 제품을 선택합니다. 확인을 클릭하여 설정을 저장합니다.
- 공급자 제외 - 지정된 공급자의 소프트웨어가 없는 호스트를 일치시키려면 이 옵션을 선택합니다.

HIP 개체 디스크 암호화 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 디스크 암호화

디스크 암호화 탭을 선택하여 GlobalProtect 엔드포인트의 디스크 암호화 상태를 기반으로 HIP 일치를 활성화합니다.

HIP 개체 디스크 암호화 설정	설명
디스크 암호화	디스크 암호화를 선택하여 호스트의 디스크 암호화 상태에 대한 일치를 활성화합니다.
기준	다음 설정을 지정합니다. • 설치됨 - 디스크 암호화 소프트웨어가 호스트에 설치되어 있는지의 여부와 일치합니다. • 암호화된 위치 - 일치를 결정할 때 디스크 암호화를 확인할 드라이브 또는 경로를 지정하려면 추가를 클릭합니다. • 암호화된 위치 - 호스트에서 암호화를 확인할 특정 위치를 입력합니다. • 상태 - 드롭다운에서 연산자를 선택한 다음 가능한 상태(전체, 없음, 부분, 사용 불가)를 선택하여 암호화된 위치의 상태를 일치시키는 방법을 지정합니다. 확인을 클릭하여 설정을 저장합니다.
공급자	엔드포인트에서 일치시킬 특정 디스크 암호화 소프트웨어 공급자 및 제품을 정의합니다. 추가를 클릭한 다음 드롭다운에서 공급자를 선택합니다. 선택적으로 추가를 클릭하여 특정 제품을 선택합니다. 확인을 클릭하여 설정을 저장하고 디스크 암호화 탭으로 돌아갑니다.

HIP 개체 데이터 손실 방지 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 데이터 손실 방지

Data Loss Prevention 탭을 선택하여 GlobalProtect 엔드포인트가 데이터 손실 방지 소프트웨어를 실행 중인지의 여부를 기반으로 하는 HIP 일치를 구성합니다.

HIP 개체 데이터 손실 방지 설정
데이터 손실 방지를 선택하여 호스트(Windows 호스트만 해당)의 데이터 손실 방지(DLP) 상태에 대한 일치를 활성화한 후 다음과 같이 일치에 대한 추가 일치 기준을 정의합니다. • 설치됨 - DLP 소프트웨어가 호스트에 설치되어 있는지의 여부와 일치합니다. • 활성화됨 - 호스트에서 DLP 소프트웨어가 활성화되었는지의 여부와 일치합니다. 설치됨 선택을 취소하면 이 필드는 자동으로 없음으로 설정되고 편집할 수 없습니다.

HIP 개체 데이터 손실 방지 설정
• 공급자 및 제품 - 특정 DLP 소프트웨어 공급자 및/또는 제품이 일치하는지 확인하기 위해 호스트에서 찾을 제품을 정의합니다. 추가를 클릭한 다음 드롭다운에서 공급자를 선택합니다. 선택적으로 추가를 클릭하여 특정 제품을 선택합니다. 확인을 클릭하여 설정을 저장합니다. • 공급자 제외 - 지정된 공급자의 소프트웨어가 없는 호스트를 일치시키려면 이 옵션을 선택합니다.

HIP 개체 인증서 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 자격증

인증서 프로파일 및 기타 인증서 속성을 기반으로 HIP 일치를 활성화하려면 인증서 탭을 선택합니다.

HIP 개체 인증서 설정
인증서 프로파일 및 인증서 속성을 기반으로 일치를 활성화하려면 인증서 확인을 선택합니다. 그런 다음 다음과 같이 일치 기준을 정의합니다. • 인증서 프로파일 - GlobalProtect 게이트웨이가 HIP 보고서에서 전송된 컴퓨터 인증서의 유효성을 검사하는 데 사용할 인증서 프로파일을 선택합니다. • 인증서 필드 - 컴퓨터 인증서와 일치하는 데 사용되는 인증서 속성을 선택합니다. • 값 - 속성 값을 설정합니다.

HIP 개체 사용자 정의 검사 탭

- 개체 > **GlobalProtect** > **HIP** 오브젝트 > ***<hip-object>*** > 사용자 정의 검사

GlobalProtect 포털에서 정의한 모든 사용자 정의 검사에서 HIP 일치를 활성화하려면 Custom Checks(사용자 정의 검사) 탭을 선택합니다. HIP 컬렉션에 사용자 지정 검사를 추가하는 방법에 대한 자세한 내용은 네트워크 > GlobalProtect > 포털을 참조하십시오.

HIP 개체 사용자 정의 검사 설정	설명
사용자 정의 검사	GlobalProtect 포털에서 정의한 사용자 정의 검사에 대한 일치를 활성화하려면 **Custom Checks**(사용자 정의 검사)를 선택합니다.
프로세스 목록	특정 프로세스에 대한 호스트 시스템을 확인하려면 추가를 클릭한 다음 프로세스 이름을 입력하십시오. 기본적으로 앱은 실행 중인 프로세스를 확인합니다. 특정 프로세스가 실행되고 있지 않은지 확인하려면 실행 중 선택을 취소하십시오. 프로세스는 운영 체제 수준 프로세스 또는 사용자 공간 애플리케이션 프로세스일 수 있습니다.

HIP 개체 사용자 정의 검사 설정	설명
레지스트리 키	Windows 호스트에서 특정 레지스트리 키를 확인하려면 추가를 클릭하고 일치시킬 레지스트리 키를 입력하십시오. 지정된 레지스트리 키 또는 키 값이 없는 호스트만 일치시키려면 키가 존재하지 않거나 지정된 값 데이터 상자와 일치함을 표시하십시오. 특정 값을 일치시키려면 추가를 클릭한 다음 레지스트리 값 및 값 데이터를 입력하십시오. 지정된 값 또는 값 데이터가 명시적으로 없는 호스트를 일치시키려면 무효를 선택하십시오. 확인을 클릭하여 설정을 저장합니다.
Plist	속성 목록(plist)의 특정 항목에 대해 Mac 호스트를 확인하려면 추가를 클릭하고 **Plist** 이름을 입력합니다. 지정된 Plist가 없는 호스트만 일치시키려면 **Plist**가 존재하지 않음을 선택하십시오. Plist 내의 특정 키-값 쌍을 일치시키려면 추가를 클릭한 다음 일치시킬 키와 해당 값을 입력하십시오. 지정된 키 또는 값이 명시적으로 없는 호스트를 일치시키려면 무효를 선택하십시오. 확인을 클릭하여 설정을 저장합니다.

개체 > GlobalProtect > HIP 프로파일

개체 > **GlobalProtect** > **HIP** 프로파일을 선택하여 HIP 지원 보안 정책을 설정하는 데 사용하는 HIP 프로파일(모니터링 또는 보안 정책 시행을 위해 함께 평가할 HIP 개체 모음)을 생성합니다. HIP 프로파일을 만들 때 부울 논리를 사용하여 이전에 만든 HIP 개체(및 다른 HIP 프로파일)를 결합할 수 있으므로 트래픽 플로우가 결과 HIP 프로파일에 대해 평가될 때 일치하거나 일치하지 않습니다. 일치 시 해당 정책 규칙이 적용됩니다. 일치하는 항목이 없으면 흐름이 다음 규칙에 대해 평가됩니다(다른 정책 일치 기준과 동일함).

HIP 프로파일을 만들려면 추가를 클릭합니다. 다음 표는 HIP 프로파일 대화 상자의 필드에 입력할 내용에 대한 정보를 제공합니다. GlobalProtect 설정 및 HIP 강화 보안 정책 생성 워크플로에 대한 자세한 내용은 *GlobalProtect* 관리자 안내서에서 HIP 기반 정책 시행 구성을 참조하십시오.

HIP 프로파일 설정	설명
이름	프로파일 이름을 입력합니다(최대 **31**자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
설명	(선택 사항) 설명을 입력합니다.
공유	현재 HIP 프로파일을 다음에 사용할 수 있도록 하려면 공유를 선택합니다: • 다중 가상 시스템 모드에 있는 방화벽에 로그인한 경우 방화벽의 모든 가상 시스템(vsys). 이 선택을 취소하면 개체 탭의 가상 시스템 드롭다운에서 선택한 vsys에서만 프로파일을 사용할 수 있습니다. 다중 가상 시스템 모드가 아닌 방화벽의 경우 이 옵션은 HIP 프로파일 대화 상자에 표시되지 않습니다. • Panorama의 모든 디바이스 그룹. 이 선택을 취소하면 개체 탭의 디바이스 그룹 드롭다운에서 선택한 디바이스 그룹에서만 프로파일을 사용할 수 있습니다. 프로파일을 저장한 후에는 공유 설정을 변경할 수 없습니다. 현재 위치를 보려면 개체 > **GlobalProtect** > **HIP** 프로파일을 선택합니다.
재정의 비활성화(Panorama만 해당)	제어는 개체 탭에서 선택한 디바이스 그룹의 하위 항목인 디바이스 그룹의 HIP 프로파일에 대한 액세스를 재정의합니다. 관리자가 상속된 값을 재정의하여 하위 디바이스 그룹에서 프로파일의 로컬 복사본을 생성하지 못하도록 하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택 취소되어 있습니다(재정의가 활성화됨).
일치	일치 기준 추가를 클릭하여 HIP 개체/프로파일 작성기를 엽니다. 일치 기준으로 사용할 첫 번째 HIP 개체 또는 프로파일을 선택한 다음 HIP 개체/프로파일 작성기 대화 상자의 일치 텍스트 상자에 추가( )합

HIP 프로파일 설정	설명
	니다. 개체의 기준이 흐름에 대해 참이 아닐 때만 HIP 프로파일이 개체를 일치로 평가하도록 하려면 개체를 추가하기 전에 **NOT**을 선택하십시오. 만들고 있는 프로파일에 맞게 일치 기준을 계속 추가하고 각 추가 사이에 적절한 부울 연산자(**AND** 또는 **OR**)를 선택했는지 확인합니다(해당되는 경우 **NOT** 연산자 사용). 복잡한 부울 표현식을 생성하려면 일치 텍스트 상자의 적절한 위치에 수동으로 괄호를 추가하여 의도한 논리를 사용하여 HIP 프로파일이 평가되도록 해야 합니다. 예를 들어 다음 표현식은 HIP 프로파일이 FileVault 디스크 암호화(Mac OS 시스템) 또는 TrueCrypt 디스크 암호화(Windows 시스템)가 있고 필수 도메인에 속하고 Symantec 바이러스 백신 클라이언트가 설치된 호스트의 트래픽과 일치함을 나타냅니다. `((“MacOS” # “FileVault”) ## (“Windows” # “TrueCrypt”)) # “###” # “SymantecAV”` 개체와 프로파일을 새 HIP 프로파일에 추가했으면 확인을 클릭합니다.

Device > GlobalProtect Client

다음 주제에서는 GlobalProtect 앱을 설정하고 관리하는 방법을 설명합니다.

무엇을 찾고 계신가요?	참조:
GlobalProtect 소프트웨어 릴리스에 대한 자세한 정보를 보십시오.	GlobalProtect 에이전트 소프트웨어 관리
GlobalProtect 소프트웨어를 설치합니다.	GlobalProtect 에이전트 설정
GlobalProtect 소프트웨어를 사용하십시오.	GlobalProtect 에이전트 사용
더 찾고 계십니까?	GlobalProtect 소프트웨어 설정에 대한 자세한 단계별 지침은 GlobalProtect 관리자 안내서에서 GlobalProtect 앱 소프트웨어 배포를 참조하십시오.

GlobalProtect 앱 소프트웨어 관리

디바이스 > **GlobalProtect** 클라이언트(방화벽 전용)를 선택하여 포털을 호스팅하는 방화벽에서 GlobalProtect 앱 소프트웨어를 다운로드하고 활성화합니다. 그런 다음 포털에 연결하는 엔드포인트는 앱 소프트웨어를 다운로드합니다. 포털에서 지정하는 에이전트 구성에서 포털이 엔드포인트에 소프트웨어를 푸시하는 방법과 시기를 정의합니다. 구성에 따라 앱이 연결될 때 자동으로 업그레이드가 수행되는지, 최종 사용자에게 업그레이드하라는 메시지가 표시되는지 또는 모든 사용자 또는 특정 사용자 집합에 대해 업그레이드가 금지되는지의 여부가 결정됩니다. 자세한 내용은 사용자가 GlobalProtect 앱을 업그레이드하도록 허용을 참조하십시오. GlobalProtect 앱 소프트웨어 배포 옵션 및 소프트웨어 배포에 대한 단계별 지침에 대한 자세한 내용은 GlobalProtect 관리자 안내서에서 GlobalProtect 앱 소프트웨어 배포를 참조하십시오.

GlobalProtect 앱의 초기 다운로드 및 설치를 위해 엔드포인트 사용자는 관리자 권한으로 로그인해야 합니다. 후속 업그레이드의 경우 관리자 권한이 필요하지 않습니다.

GlobalProtect 클라이언트 설정	설명
버전	이 버전 번호는 Palo Alto Networks 업데이트 서버에서 사용할 수 있는 GlobalProtect 앱 소프트웨어입니다. Palo Alto Networks에서 새 앱 소프트웨어 릴리스를 사용할 수 있는지 확인하려면 지금 확인을 클릭하십시오. 방

GlobalProtect 클라이언트 설정	설명
	화벽은 서비스 경로를 사용하여 업데이트 서버에 연결하여 사용 가능한 새 버전이 있는지 확인하고 목록의 맨 위에 표시합니다.
크기	앱 소프트웨어 번들의 크기입니다.
출시일	Palo Alto Networks에서 릴리스를 제공한 날짜 및 시간입니다.
다운로드됨	이 열의 확인 표시는 해당 버전의 앱 소프트웨어 패키지가 방화벽에 다운로드되었음을 나타냅니다.
현재 활성화됨	이 열의 확인 표시는 해당 버전의 앱 소프트웨어 패키지가 방화벽에서 활성화되었으며 앱을 연결하여 다운로드할 수 있음을 나타냅니다. 한 번에 하나의 소프트웨어 버전만 활성화할 수 있습니다.
작업	다음과 같이 해당 앱 소프트웨어 패키지에 대해 수행할 수 있는 현재 작업을 나타냅니다. • 다운로드—해당 앱 소프트웨어 버전은 Palo Alto Networks 업데이트 서버에서 사용할 수 있습니다. 다운로드를 클릭하여 다운로드를 시작합니다. 방화벽이 인터넷에 액세스할 수 없는 경우 인터넷에 연결된 컴퓨터를 사용하여 고객 지원 사이트로 이동한 다음 업데이트 > 소프트웨어 업데이트를 선택하여 새 앱 소프트웨어 버전을 찾아 로컬 컴퓨터에 다운로드합니다. 그런 다음 방화벽에 앱 소프트웨어를 수동으로 업로드합니다. • 활성화 - 해당 앱 소프트웨어 버전이 방화벽에 다운로드되었지만 앱에서 아직 다운로드할 수 없습니다. 활성화를 클릭하여 소프트웨어를 활성화하고 앱 업그레이드를 활성화합니다. 방화벽에 수동으로 업로드한 소프트웨어 업데이트를 활성화하려면 파일에서 활성화를 클릭하고 드롭다운에서 활성화하려는 버전을 선택합니다(현재 활성화됨으로 표시하려면 화면을 새로 고쳐야 할 수 있음). • 재활성화 - 해당 앱 소프트웨어가 활성화되었으며 엔드포인트를 다운로드할 준비가 되었습니다. 한 번에 한 버전의 GlobalProtect 앱 소프트웨어만 방화벽에서 활성화될 수 있으므로 최종 사용자가 현재 활성화된 버전과 다른 버전에 액세스해야 하는 경우 다른 버전을 활성화하여 현재 활성화된 버전으로 만들어야 합니다.
릴리스 노트	해당 앱 버전에 대한 GlobalProtect 릴리스 정보에 대한 링크를 제공합니다.
	방화벽에서 이전에 다운로드한 앱 소프트웨어 이미지를 제거합니다.

GlobalProtect 앱 설정

GlobalProtect 앱은 포털 및 게이트웨이와의 GlobalProtect 연결을 지원하기 위해 엔드포인트(일반적으로 랩톱)에 설치되는 애플리케이션입니다. 앱은 GlobalProtect 서비스(PanGP 서비스)에서 지원됩니다.

호스트 운영 체제*(32*비트 또는 *64*비트*)*에 대해 올바른 설치 옵션을 선택했는지 확인하십시오. *64*비트 호스트에 설치하는 경우 초기 설치에 *64*비트 브라우저와 *Java* 조합을 사용하십시오.

앱을 설치하려면 설치 프로그램 파일을 열고 화면의 지시를 따릅니다.

GlobalProtect 앱 사용

GlobalProtect 앱을 실행하고 GlobalProtect 상태 패널의 설정 메뉴에서 설정을 선택할 때 열리는 **GlobalProtect** 설정 패널의 탭에는 상태 및 설정에 대한 유용한 정보가 포함되어 있으며 연결 문제 해결에 도움이 되는 정보를 제공합니다.

- 일반 탭 - GlobalProtect 계정과 연결된 사용자명 및 포털을 표시합니다. 이 탭에서 포털을 추가, 삭제 또는 수정할 수도 있습니다.
- 연결 탭 - GlobalProtect 앱에 대해 구성된 게이트웨이를 표시하고 각 게이트웨이에 대한 다음 정보를 제공합니다.
  - 게이트웨이 이름
  - 터널 상태
  - 인증 상태
  - 연결 타입
  - 게이트웨이 IP 주소 또는 FQDN(외부 모드에서만 사용 가능)

  내부 모드의 경우 연결 탭에 사용 가능한 게이트웨이의 전체 목록이 표시됩니다. 외부 모드의 경우 연결 탭에는 연결된 게이트웨이와 게이트웨이에 대한 추가 세부 정보*(*예*:* 게이트웨이 *IP* 주소 및 가동 시간*)*가 표시됩니다.
- 호스트 프로파일 탭 - GlobalProtect가 HIP(호스트 정보 프로파일)를 통해 보안 정책을 모니터링하고 시행하는 데 사용하는 엔드포인트 데이터를 표시합니다. 게이트웨이에 HIP 데이터를 수동으로 다시 제출하려면 호스트 프로파일 다시 제출을 클릭합니다.

- 문제 해결 탭 - macOS 엔드포인트에서 이 탭을 사용하여 로그를 수집하고 로깅 수준을 설정할 수 있습니다. Windows 엔드포인트에서 이 탭을 사용하면 로그를 수집하고, 로깅 수준을 설정하고, 문제 해결에 도움이 되는 다음 정보를 볼 수 있습니다.
  - 네트워크 구성 - 현재 시스템 구성을 표시합니다.
  - 라우팅 테이블 - GlobalProtect 연결이 현재 라우팅되는 방식에 대한 정보를 표시합니다.
  - 소켓—현재 활성 연결에 대한 소켓 정보를 표시합니다.
  - 로그 - 사용자가 GlobalProtect 앱 및 서비스에 대한 로그를 표시할 수 있습니다. 로그 유형 및 디버깅 수준을 선택합니다. 시작을 클릭하여 로깅을 시작하고 중지를 클릭하여 로깅을 종료합니다.
- 알림 탭 - GlobalProtect 앱에서 트리거된 알림 목록을 표시합니다. 특정 알림에 대한 자세한 내용을 보려면 알림을 두 번 클릭합니다.

Panorama 웹 인터페이스

Panorama™는 Palo Alto Networks® 차세대 방화벽 제품군을 위한 중앙 집중식 관리 시스템입니다. Panorama는 네트워크의 모든 애플리케이션, 사용자 및 콘텐츠를 감독할 수 있는 단일 위치를 제공하고 이 지식을 사용하여 네트워크를 제어하고 보호하는 정책을 생성합니다. 중앙 집중식 정책 및 방화벽 관리에 Panorama를 사용하면 분산 방화벽 네트워크를 관리할 때 운영 효율성이 높아집니다. Panorama는 전용 하드웨어(M-시리즈) 어플라이언스와 VMware 가상 어플라이언스(ESXi 서버 또는 vCloud Air 플랫폼에서 실행)로 사용할 수 있습니다.

많은 Panorama 웹 인터페이스 보기 및 설정이 방화벽 웹 인터페이스에서 볼 수 있는 것과 동일하지만 다음 항목에서는 Panorama, 방화벽 및 로그 수집기를 관리하기 위해 Panorama 웹 인터페이스에서만 사용할 수 있는 옵션에 대해 설명합니다.

- Panorama > 로그 설정
- Panorama > 서버 프로파일 > SCP
- Panorama > 예약된 구성 내보내기
- Panorama > 소프트웨어
- Panorama > 디바이스 배포
- Panorama > 디바이스 등록 인증 키

더 찾고 계십니까**?**

중앙 집중식 관리를 위한 Panorama 설정 및 사용에 대한 자세한 내용은 Panorama 관리자 안내서를 참조하십시오.

Panorama 웹 인터페이스 사용

Panorama와 방화벽의 웹 인터페이스는 모양과 느낌이 동일합니다. 그러나 Panorama 웹 인터페이스에는 Panorama를 관리하고 Panorama를 사용하여 방화벽 및 로그 수집기를 관리하기 위한 추가 옵션과 Panorama 관련 탭이 포함되어 있습니다.

다음과 같은 공통 필드는 여러 Panorama 웹 인터페이스 페이지의 머리글 또는 바닥글에 나타납니다.

공통 필드	설명
컨텍스트	왼쪽 메뉴 위의 컨텍스트 드롭다운을 사용하여 Panorama 웹 인터페이스와 방화벽 웹 인터페이스 간에 전환할 수 있습니다(컨텍스트 전환 참조).
	대시보드 및 모니터 탭에서 탭 헤더의 새로 고침()을 클릭하여 해당 탭의 데이터를 수동으로 새로 고칩니다. 탭 헤더 오른쪽에 있는 레이블이 지정되지 않은 드롭다운을 사용하여 자동 새로 고침 인터벌(**1**분, **2**분 또는 **5**분)을 선택할 수도 있습니다. 자동 새로 고침을 비활성화하려면 수동을 선택합니다.
액세스 도메인	액세스 도메인은 컨텍스트 드롭다운을 통해 특정 디바이스 그룹, 템플릿 및 개별 방화벽에 대한 액세스를 정의합니다. 계정에 여러 액세스 도메인이 할당된 관리자로 로그인하면 대시보드, **ACC** 및 모니터 탭에 웹 인터페이스 바닥글에서 선택한 액세스 도메인에 대한 정보(예: 로그 데이터)만 표시됩니다. 계정에 액세스 도메인이 하나만 할당된 경우 웹 인터페이스에 액세스 도메인 드롭다운이 표시되지 않습니다.
디바이스 그룹	디바이스 그룹은 그룹으로 관리하는 방화벽 및 가상 시스템으로 구성됩니다(Panorama > 디바이스 그룹 참조). 대시보드, **ACC** 및 모니터 탭에는 탭 헤더에서 선택한 디바이스 그룹에 대한 정보(예: 로그 데이터)만 표시됩니다. 정책 및 개체 탭에서 특정 디바이스 그룹 또는 모든 디바이스 그룹(공유 선택)에 대한 설정을 구성할 수 있습니다.
템플릿	템플릿은 공통 네트워크 및 디바이스 설정이 있는 방화벽 그룹이고 템플릿 스택(template stack)은 템플릿의 조합입니다(Panorama > 템플릿 참조). 네트워크 및 디바이스 탭에서 특정 템플릿 또는 템플릿 스택(template stack)에 대한 설정을 구성합니다. 개별 템플릿 내에서만 설정을 편집할 수 있으므로 템플릿 스택(template stack)을 선택하는 경우 이러한 탭의 설정은 읽기 전용입니다.
보기 기준: 디바이스	기본적으로 네트워크 및 디바이스 탭에는 정상 작동 모드에 있고 여러 가상 시스템 및 VPN을 지원하는 방화벽에 사용할 수 있는 설정과 값이 표시됩니

공통 필드	설명
모드	다. 그러나 다음 옵션을 사용하여 편집하려는 모드별 설정만 표시하도록 탭을 필터링할 수 있습니다. • 모드 드롭다운에서 **Multi-VSYS**, 작동 모드 및 **VPN** 모드 옵션을 선택하거나 선택 취소합니다. • 보기 기준에서 선택하여 특정 방화벽의 모드 구성을 반영하도록 모든 모드 옵션을 설정합니다. 디바이스 드롭다운.

Panorama 탭은 Panorama 및 Log Collector를 관리하기 위한 다음 페이지를 제공합니다.

Panorama 페이지	설명
설정	다음 작업에 대해 **Panorama** > 설정을 선택합니다. • 일반 설정(예: Panorama 호스트 이름)과 인증, 로그, 보고서, AutoFocus™, 배너, 오늘의 메시지 및 암호 복잡성에 대한 설정을 지정합니다. 이러한 설정은 방화벽에 대해 구성한 설정과 유사합니다. 디바이스 > 설정 > 관리를 선택합니다. • 구성을 백업 및 복원하고 Panorama를 재부팅한 다음 Panorama를 종료합니다. 이러한 작업은 방화벽에 대해 수행하는 작업과 유사합니다. 디바이스 > 설정 > 작업을 선택합니다. • DNS, NTP 및 Palo Alto Networks 업데이트를 위한 서버 연결을 정의합니다. 이러한 설정은 방화벽에 대해 구성한 설정과 유사합니다. 디바이스 > 설정 > 서비스를 선택합니다. • Panorama 인터페이스에 대한 네트워크 설정을 정의합니다. Panorama > 설정 > 인터페이스를 선택합니다. • WildFire™ 어플라이언스에 대한 설정을 지정합니다. 이러한 설정은 방화벽에 대해 구성한 설정과 유사합니다. 디바이스 > 설정 > WildFire를 선택합니다. • 하드웨어 보안 모듈(HSM) 설정을 관리합니다. 이러한 설정은 방화벽에 대해 구성한 설정과 유사합니다. 디바이스 > 설정 > HSM을 선택합니다.
고가용성	Panorama 관리 서버 쌍에 대해 고가용성(HA)을 구성할 수 있습니다. Panorama > 고가용성을 선택합니다.
구성 감사	구성 파일 간의 차이점을 볼 수 있습니다. 디바이스 > 구성 감사를 선택합니다.
비밀번호 프로파일	Panorama 관리자의 비밀번호 프로파일을 정의할 수 있습니다. 디바이스 > 암호 프로파일을 선택합니다.

Panorama 페이지	설명
관리자	Panorama 관리자 계정을 구성할 수 있습니다. Panorama > 관리자를 선택합니다. 관리자 계정이 잠긴 경우 관리자 페이지의 잠긴 사용자 열에 잠금이 표시됩니다. 잠금을 클릭하여 계정을 잠금 해제할 수 있습니다.
관리자 역할	Panorama에 액세스하는 관리자의 권한과 책임을 제어하는 관리 역할을 정의할 수 있습니다. Panorama > 관리자 역할을 선택합니다.
액세스 도메인	디바이스 그룹, 템플릿, 템플릿 스택(template stack) 및 방화벽의 웹 인터페이스에 대한 관리자 액세스를 제어할 수 있습니다. Panorama > 액세스 도메인을 선택합니다.
인증 프로파일	Panorama에 대한 액세스를 인증하기 위한 프로파일을 지정할 수 있습니다. 디바이스 > 인증 프로파일을 선택합니다.
인증 순서	Panorama에 대한 액세스를 허용하는 데 사용할 일련의 인증 프로파일을 지정할 수 있습니다. 디바이스 > 인증 순서를 선택합니다.
사용자 식별	User-ID 에이전트와의 상호 인증을 위해 사용자 지정 인증서 프로파일을 구성할 수 있습니다. 디바이스 > 사용자 식별 > 연결 보안을 선택합니다.
데이터 재배포	데이터를 다른 방화벽이나 Panorama 관리 시스템에 선택적으로 재배포할 수 있습니다. 디바이스 > 데이터 재배포를 선택합니다.
관리되는 디바이스	Panorama에 관리 디바이스로 방화벽 추가, 방화벽 연결 및 라이선스 상태 표시, 방화벽 태그 지정, 방화벽 소프트웨어 및 콘텐츠 업데이트, 구성 백업 로드를 포함하여 방화벽을 관리할 수 있습니다. Panorama > 관리 디바이스 > 요약을 선택합니다.
템플릿	디바이스 및 네트워크 탭에서 구성 옵션을 관리할 수 있습니다. 템플릿 및 템플릿 스택(template stack)을 사용하면 동일하거나 유사한 구성으로 여러 방화벽을 배포하는 관리 시간을 줄일 수 있습니다. Panorama > 템플릿을 선택합니다.
디바이스 그룹	기능, 네트워크 분할 또는 지리적 위치를 기반으로 방화벽을 그룹화하는 디바이스 그룹을 구성할 수 있습니다. 디바이스 그룹에는 물리적 방화벽, 가상 방화벽 및 가상 시스템이 포함될 수 있습니다. 일반적으로 디바이스 그룹의 방화벽에는 유사한 정책 구성이 필요합니다. Panorama의 정책 및 개체 탭을 사용하여 디바이스 그룹은 관리되는 방화벽 네트워크에서 정책을 관리하기 위한 계층화된 접근 방식을 구현하는 방법을 제공

Panorama 페이지	설명
	합니다. 최대 4개 수준의 트리 계층 구조에서 디바이스 그룹을 중첩할 수 있습니다. 하위 그룹은 상위 그룹 및 공유 위치의 정책 및 개체를 자동으로 상속합니다. Panorama > 디바이스 그룹을 선택합니다.
관리형 수집기	로그 수집기를 관리할 수 있습니다. Panorama를 사용하여 로그 수집기를 구성하기 때문에 관리형 수집기라고도 합니다. 관리형 수집기는 Panorama 관리 서버(Panorama 모드의 M 시리즈 어플라이언스 또는 Panorama 가상 어플라이언스) 또는 전용 로그 수집기(로그 수집기 모드의 M 시리즈 어플라이언스)에 로컬일 수 있습니다. Panorama > 관리 수집기를 선택합니다. 전용 로그 수집기용 소프트웨어 업데이트를 설치할 수도 있습니다. Panorama 관리 서버를 DedicatedLogCollector로 변환할 수 있습니다.
수집기 그룹	수집기 그룹을 관리할 수 있습니다. 수집기 그룹은 동일한 구성 설정을 적용하고 방화벽을 할당할 수 있도록 Log Collector를 논리적으로 그룹화합니다. Panorama는 로그 수집기의 모든 디스크와 수집기 그룹의 모든 구성원에 걸쳐 로그를 균일하게 배포합니다. Panorama > 수집기 그룹을 선택합니다.
플러그인	VMware NSX와 같은 타사 통합을 위한 플러그인을 관리할 수 있습니다. Panorama > VMware NSX를 선택합니다.
VMware NSX	NSX Manager와 Panorama 간의 통신을 활성화하여 VM 시리즈 방화벽 프로비저닝을 자동화할 수 있습니다. Panorama > VMware NSX를 선택합니다.
인증서 관리	인증서, 인증서 프로파일 및 키를 구성하고 관리할 수 있습니다. 방화벽 및 Panorama 인증서 관리를 선택합니다.
로그 설정	SNMP(Simple Network Management Protocol) 트랩 수신기, syslog 서버, 이메일 서버 및 HTTP 서버로 로그를 포워딩할 수 있습니다. 디바이스 > 로그 설정을 선택합니다.
서버 프로파일	Panorama에 서비스를 제공하는 다양한 서버 유형에 대한 프로파일을 구성할 수 있습니다. 다음 중 하나를 선택하여 특정 서버 유형을 구성합니다. • 디바이스 > 서버 프로파일 > 이메일 • 디바이스 > 서버 프로파일 > HTTP • 디바이스 > 서버 프로파일 > SNMP 트랩 • 디바이스 > 서버 프로파일 > Syslog • 디바이스 > 서버 프로파일 > RADIUS

Panorama 페이지	설명
	• 디바이스 > 서버 프로파일 > TACACS+ • 디바이스 > 서버 프로파일 > LDAP • 디바이스 > 서버 프로파일 > Kerberos • 디바이스 > 서버 프로파일 > SAML ID 공급자
예약된 구성 내보내기	Panorama 및 방화벽 구성을 매일 FTP 서버 또는 SCP(Secure Copy) 서버로 내보낼 수 있습니다. Panorama > 예약된 구성 내보내기를 선택합니다.
소프트웨어	Panorama 소프트웨어를 업데이트할 수 있습니다. Panorama > 소프트웨어를 선택합니다.
동적 업데이트	안티바이러스 서명(위협 방지 라이선스 필요)과 같은 새로운 보안 위협에 대한 최신 애플리케이션 정의 및 정보를 본 다음 새 정의로 Panorama를 업데이트할 수 있습니다. 디바이스 > 동적 업데이트를 선택합니다.
지원	Palo Alto Networks의 제품 및 보안 경고에 액세스할 수 있습니다. 디바이스 > 지원을 선택합니다.
디바이스 배포	방화벽 및 로그 수집기에 소프트웨어 및 콘텐츠 업데이트를 배포할 수 있습니다. Panorama > 디바이스 배포를 선택합니다.
마스터 키 및 진단	Panorama에서 개인 키를 암호화하기 위해 마스터 키를 지정할 수 있습니다. 기본적으로 Panorama는 새 마스터 키를 지정하지 않은 경우에도 개인 키를 암호화된 형식으로 저장합니다. 디바이스 > 마스터 키 및 진단을 선택합니다.

컨텍스트 전환

모든 Panorama 웹 인터페이스 페이지의 헤더에서 왼쪽 메뉴 위의 컨텍스트 드롭다운을 사용하여 Panorama 웹 인터페이스와 방화벽 웹 인터페이스 간에 전환할 수 있습니다. 방화벽을 선택하면 웹 인터페이스가 새로 고쳐져 선택한 방화벽에 대한 모든 페이지와 옵션이 표시되므로 로컬에서 관리할 수 있습니다. 드롭다운에는 관리 액세스 권한이 있고(Panorama > 액세스 도메인 참조) Panorama에 연결된 방화벽만 표시됩니다.

필터를 사용하여 플랫폼(모델), 디바이스 그룹, 템플릿, 태그 또는 HA 상태별로 방화벽을 검색할 수 있습니다. 필터 표시줄에 텍스트 문자열을 입력하여 디바이스 이름으로 검색할 수도 있습니다.

고가용성(HA) 모드에 있는 방화벽 아이콘은 HA 상태를 나타내기 위해 배경색이 지정됩니다.

Panorama 커밋 작업

웹 인터페이스의 오른쪽 상단에서 커밋을 클릭하고 Panorama 구성에 대한 보류 중인 변경 사항과 Panorama가 방화벽, 로그 수집기, WildFire 클러스터 및 어플라이언스에 푸시하는 변경 사항에 대한 작업을 선택합니다.

- **Commit** > **Commit to Panorama** - Panorama 관리 서버의 구성에서 변경한 사항을 활성화합니다. 또한 이 작업은 방화벽, 로그 수집기 또는 WildFire 클러스터 및 어플라이언스에 변경 사항을 푸시하지 않고 디바이스 그룹, 템플릿, 수집기 그룹, WildFire 클러스터 및 어플라이언스 변경 사항을 Panorama 구성에 커밋합니다. Panorama 구성만 커밋하면 방화벽, 로그 수집기 또는 WildFire 클러스터 및 어플라이언스에서 활성화할 준비가 되지 않은 변경 사항을 저장할 수 있습니다.

  관리되는 디바이스에 구성을 푸시할 때 *Panorama 8.0* 이상 릴리스는 *Panorama*에 커밋된 구성인 실행 중인 구성을 푸시합니다. *Panorama 7.1* 및 이전 릴리스는 커밋되지 않은 변경 사항을 포함하는 후보 구성을 푸시합니다. 따라서 *Panorama 8.0* 이상 릴리스에서는 먼저 *Panorama*에 변경 사항을 커밋할 때까지 관리 디바이스에 변경 사항을 푸시할 수 없습니다.

- **Commit** > **Push to Devices**- Panorama 실행 구성을 디바이스 그룹, 템플릿, 수집기 그룹, WildFire 클러스터 및 어플라이언스로 푸시합니다.
- 커밋 > 커밋 및 푸시 - 모든 구성 변경 사항을 로컬 Panorama 구성에 커밋한 다음 Panorama 실행 구성을 디바이스 그룹, 템플릿, 수집기 그룹, WildFire 클러스터 및 어플라이언스에 푸시합니다.

관리자 또는 위치별로 보류 중인 변경 사항을 필터링한 다음 해당 변경 사항만 커밋, 푸시, 유효성 검사 또는 미리 볼 수 있습니다. 위치는 특정 디바이스 그룹, 템플릿, 수집기 그룹, 로그 수집기, WildFire 어플라이언스 및 클러스터, 공유 설정 또는 Panorama 관리 서버일 수 있습니다.

변경 사항을 커밋하면 실행 중인 구성의 일부가 됩니다. 커밋하지 않은 변경 사항은 후보 구성의 일부입니다. Panorama는 이전 커밋이 진행 중인 동안 새 커밋을 시작할 수 있도록 커밋 요청을 대기열에 넣습니다. Panorama는 커밋을 시작된 순서대로 수행하지만 Panorama에서 시작한 자동 커밋(예: FQDN 새로 고침)에 우선 순위를 둡니다. 그러나 대기열에 이미 관리자가 시작한 최대 커밋 수가 있는 경우 새 커밋을 시작하기 전에 Panorama가 보류 중인 커밋 처리를 완료할 때까지 기다려야 합니다. 작업 관리자(Tasks)를 사용하여 커밋 대기열을 지우거나 커밋에 대한 세부 정보를 볼 수 있습니다. 구성 변경, 커밋 프로세스, 커밋 유효성 검사 및 커밋 대기열에 대한 자세한 내용은 Panorama 커밋 및 유효성 검사 작업을 참조하십시오. 또한 후보 구성을 저장하고 변경 사항을 되돌리고 구성을 가져오거나 내보내거나 로드할 수 있습니다(디바이스 > 설정 > 작업).

구성 변경 사항을 커밋, 유효성 검사 또는 미리 보기 위해 다음 옵션을 사용할 수 있습니다.

필드/버튼	설명
커밋 > **Panorama**에 커밋 또는 커밋 > 커밋 및 푸시를 선택하여 Panorama에 커밋할 때 다음 옵션이 적용됩니다.	

필드/버튼	설명
모든 변경 사항 커밋	관리 권한이 있는 모든 변경 사항을 커밋합니다(기본값). 이 옵션을 선택할 때 Panorama가 커밋하는 구성 변경의 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 커밋 범위가 결정됩니다. • 운용 관리자 역할 - Panorama는 모든 관리자의 변경 사항을 커밋합니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 커밋 범위가 결정됩니다(Panorama > 관리자 역할 참조). 프로파일에 다른 관리자를 위해 커밋할 권한이 포함된 경우 Panorama는 모든 관리자가 구성한 변경 사항을 커밋합니다. 관리자 역할 프로파일에 다른 관리자를 위해 커밋할 권한이 없는 경우 Panorama는 다른 관리자의 변경 사항이 아닌 사용자의 변경 사항만 커밋합니다. 액세스 도메인을 구현한 경우 Panorama는 해당 도메인을 자동으로 적용하여 커밋 범위를 필터링합니다(Panorama > 액세스 도메인 참조). 관리자 역할에 관계없이 Panorama는 계정에 할당된 액세스 도메인의 구성 변경만 커밋합니다.
변경 사항 커밋	Panorama가 커밋하는 구성 변경의 범위를 필터링합니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링 옵션이 결정됩니다. • 운용 관리자 역할 - 특정 관리자가 수행한 변경 사항과 특정 위치의 변경 사항으로 커밋 범위를 제한할 수 있습니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 필터링 옵션이 결정됩니다(Panorama > 관리자 역할 참조). 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 포함된 경우 커밋 범위를 특정 관리자가 구성한 변경 사항과 특정 위치의 변경 사항으로 제한할 수 있습니다. 관리자 역할 프로파일에 다른 관리자를 위해 커밋할 수 있는 권한이 포함되어 있지 않은 경우 커밋 범위를 특정 위치에서 변경한 내용으로만 제한할 수 있습니다. 다음과 같이 커밋 범위를 필터링합니다. • 관리자별 필터링 - 역할이 다른 관리자의 변경 사항을 커밋하도록 허용하더라도 커밋 범위에는 기본적으로 사용자의 변경 사항만 포함됩니다. 커밋 범위에 다른 관리자를 추가하려면 <*usernames*> 링크를 클릭하고 관리자를 선택한 다음 확인을 클릭합니다. • 위치별 필터링 - 커밋에 포함할 변경 사항의 특정 위치를 선택합니다.

필드/버튼	설명
	액세스 도메인을 구현한 경우 Panorama는 해당 도메인을 기반으로 커밋 범위를 자동으로 필터링합니다(Panorama > 액세스 도메인 참조). 관리 역할 및 필터링 선택에 관계없이 커밋 범위에는 계정에 할당된 액세스 도메인의 구성 변경 사항만 포함됩니다. 구성을 로드한 후(디바이스 > 설정 > 작업) 모든 변경 사항을 커밋해야 합니다. 디바이스 그룹에 대한 변경 사항을 커밋할 때 해당 디바이스 그룹의 동일한 룰베이스(rulebase)에 대한 규칙을 추가, 삭제 또는 재배치한 모든 관리자의 변경 사항을 포함해야 합니다.
커밋 범위	커밋할 변경 사항이 있는 위치를 나열합니다. 목록에 모든 변경 사항이 포함되는지 아니면 변경 사항의 하위 집합이 포함되는지의 여부는 Commit All Changes 및 Commit Changes Made By에 설명된 대로 여러 요인에 따라 달라집니다. 위치는 다음 중 하나일 수 있습니다. • **shared-object** - 공유 위치에 정의된 설정입니다. • ***<device-group>*** - 정책 규칙 또는 개체가 정의된 디바이스 그룹의 이름입니다. • ***<template>*** - 설정이 정의된 템플릿 또는 템플릿 스택의 이름입니다. • ***<log-collector-group>*** - 설정이 정의된 수집기 그룹의 이름입니다. • ***<log-collector>*** - 설정이 정의된 로그 수집기의 이름입니다. • ***<wildfire-appliances>*** - 설정이 정의된 WildFire 어플라이언스의 일련 번호입니다. • ***<wildfire-appliance-clusters>*** - 설정이 정의된 WildFire 클러스터의 이름입니다.
위치 유형	이 열은 보류 중인 변경 사항의 위치를 분류합니다. • **Panorama** - Panorama 관리 서버 구성과 관련된 설정입니다. • 디바이스 그룹 - 특정 디바이스 그룹에 정의된 설정입니다. • 템플릿 - 특정 템플릿 또는 템플릿 스택(template stack)에 정의된 설정입니다. • 로그 수집기 그룹 - 수집기 그룹 구성과 관련된 설정입니다. • 로그 수집기 - 로그 수집기 구성과 관련된 설정입니다. • **WildFire** 어플라이언스 클러스터 - WildFire 어플라이언스 클러스터 구성과 관련된 설정입니다.

필드/버튼	설명
	• **WildFire** 어플라이언스 - WildFire 어플라이언스와 관련된 설정입니다. • 기타 변경 사항 - 이전 구성 영역(예: 공유 개체)과 관련이 없는 설정입니다.
개체 유형	구성 변경의 객체 유형을 표시합니다. 예를 들어 네트워크 프로파일(네트워크 > 네트워크 프로파일)을 구성한 경우 ####이 표시됩니다. 주소 그룹(개체 > 주소 그룹)을 구성하면 ## ##이 표시됩니다.
관리자	구성을 변경한 관리자의 이름입니다.
커밋에 포함 (부분 커밋만)	커밋할 변경 사항을 선택할 수 있습니다. 기본적으로 커밋 범위 내의 모든 변경 사항이 선택됩니다. 이 열은 특정 관리자가 변경한 사항을 커밋하도록 선택한 후에만 표시됩니다. 커밋에 포함하는 변경 사항에 영향을 미치는 종속성이 있을 수 있습니다. 예를 들어 개체를 추가하고 다른 관리자가 해당 개체를 편집하는 경우 자신의 변경 사항을 커밋하지 않고는 다른 관리자를 위해 변경 사항을 커밋할 수 없습니다.
유형별 그룹화	커밋 범위의 구성 변경 목록을 위치 유형별로 그룹화합니다.
변경 사항 미리보기	커밋 범위에서 선택한 구성을 실행 중인 구성과 비교할 수 있습니다. 미리보기 창은 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)인 변경 사항을 나타냅니다. 웹 인터페이스 섹션에 대한 변경 사항을 일치시키는 데 도움이 되도록 각 변경 전후에 컨텍스트 라인을 표시하도록 미리보기 창을 구성할 수 있습니다. 이 줄은 비교 중인 후보 및 실행 중인 구성의 파일에서 불러온 것입니다. 미리보기 결과가 새 브라우저 창에 표시되기 때문에 브라우저에서 팝업을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 허용 단계를 참조하세요.
변경 요약	변경 사항을 커밋하는 개별 설정을 나열합니다. 변경 요약 목록에는 각 설정에 대한 다음 정보가 표시됩니다.

필드/버튼	설명
	• 개체 이름 - 정책, 개체, 네트워크 설정 또는 디바이스 설정을 식별하는 이름입니다. • 유형 - 설정 유형(예: 주소, 보안 규칙 또는 영역)입니다. • 위치 유형 - 설정이 디바이스 그룹, 템플릿, 수집기 그룹, **WildFire** 어플라이언스 또는 **Wildfire** 어플라이언스 클러스터에 정의되어 있는지의 여부를 나타냅니다. • 위치 - 설정이 정의된 디바이스 그룹, 템플릿, 수집기 그룹, WildFire 클러스터 또는 WildFire 어플라이언스의 이름입니다. 열은 이러한 위치에 정의되지 않은 설정에 대해 공유를 표시합니다. • 작업 - 마지막 커밋 이후 설정에 대해 수행된 모든 작업(생성, 편집 또는 삭제)을 나타냅니다. • 소유자 - 설정을 마지막으로 변경한 관리자입니다. • 커밋될 예정 - 커밋에 설정이 포함되는지의 여부를 나타냅니다. • 이전 소유자 - 마지막 변경 전에 설정을 변경한 관리자입니다. 선택적으로 열 이름(예: 유형)으로 그룹화할 수 있습니다.
커밋 확인	Panorama 구성이 올바른 구문을 가지고 있고 의미상 완전한지 확인합니다. 출력에는 규칙 섀도잉 및 애플리케이션 종속성 경고를 포함하여 커밋에 표시되는 것과 동일한 오류 및 경고가 포함됩니다. 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.
다음 옵션은 커밋 > 디바이스에 푸시 또는 커밋 > 커밋 및 푸시를 선택하여 관리되는 디바이스에 구성 변경 사항을 푸시할 때 적용됩니다.	
모든 변경 사항 푸시	관리 권한이 있는 모든 변경 사항을 푸시합니다(기본값). 이 옵션을 선택할 때 Panorama가 푸시하는 구성 변경의 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 푸시 범위가 결정됩니다. • 수퍼유저 역할 - Panorama는 모든 관리자의 변경 사항을 푸시합니다. • 맞춤 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 푸시 범위가 결정됩니다(Panorama > 관리자 역할 참조). 프로파일에 다른 관리자를 위해 커밋 권한이 포함된 경우 Panorama는 모든 관리자가 구성한 변경 사항을 푸시합니다. 관리자 역할 프로파일에 다른 관리자에게 푸시 권한이 없는 경우 Panorama는 다른 관리자의 변경 사항이 아닌 사용자의 변경 사항만 푸시합니다.

필드/버튼	설명
	액세스 도메인을 구현한 경우 Panorama는 푸시 범위를 필터링하기 위해 해당 도메인을 자동으로 적용합니다(Panorama > 액세스 도메인 참조). 관리자 역할에 관계없이 Panorama는 계정에 할당된 액세스 도메인의 구성 변경 사항만 푸시합니다.
푸시 변경 사항	Panorama가 푸시하는 구성 변경의 범위를 필터링합니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링 옵션이 결정됩니다. • 수퍼유저 역할 - 푸시 범위를 특정 관리자가 수행한 변경 사항과 특정 위치의 변경 사항으로 제한할 수 있습니다. • 사용자 지정 역할 - 계정에 할당된 관리자 역할 프로파일의 권한에 따라 필터링 옵션이 결정됩니다(Panorama > 관리자 역할 참조). 프로파일에 다른 관리자에 대한 푸시 권한이 포함된 경우 특정 관리자가 구성한 변경 사항과 특정 위치의 변경 사항으로 푸시 범위를 제한할 수 있습니다. 관리자 역할 프로파일에 다른 관리자에게 푸시 권한이 없는 경우 특정 위치에서 변경한 사항으로만 푸시 범위를 제한할 수 있습니다. 다음과 같이 푸시 범위를 필터링합니다. • 관리자별 필터링 - 내 역할이 다른 관리자의 변경 사항을 푸시하도록 허용하더라도 기본적으로 푸시 범위에는 귀하의 변경 사항만 포함됩니다. 푸시 범위에 다른 관리자를 추가하려면 <*usernames*> 링크를 클릭하고 관리자를 선택한 다음 확인을 클릭합니다. • 위치별 필터링 - 푸시에 포함을 변경할 특정 위치를 선택합니다. 액세스 도메인을 구현한 경우 Panorama는 해당 도메인을 기반으로 푸시 범위를 자동으로 필터링합니다(Panorama > 액세스 도메인 참조). 관리 역할 및 필터링 선택에 관계없이 푸시 범위에는 계정에 할당된 액세스 도메인의 구성 변경 사항만 포함됩니다.
푸시 범위	푸시할 변경 사항이 있는 위치를 나열합니다. 범위에 기본적으로 포함되는 위치는 다음 옵션 중 선택하는 옵션에 따라 다릅니다. • 커밋 > 커밋 및 푸시 - 범위에는 Panorama 커밋이 필요한 변경 사항이 있는 모든 위치가 포함됩니다. • 커밋 > 디바이스에 푸시 - 범위에는 Panorama 실행 구성과 ### ## ##(동기화 상태는 Panorama > 관리형 디바이스 > 요약 및 Panorama > 관리형 수집기 참조). 두 선택 모두에 대해 Panorama는 다음을 기준으로 푸시 범위를 필터링합니다.

필드/버튼	설명
	• 관리자 - Panorama는 커밋 범위와 동일한 필터를 적용합니다(모든 변경 사항 커밋 또는 변경 사항 커밋 참조). • 액세스 도메인 - 액세스 도메인을 구현한 경우 Panorama는 해당 도메인을 기반으로 푸시 범위를 자동으로 필터링합니다(Panorama > 액세스 도메인 참조). 관리 역할 및 필터링 선택에 관계없이 범위에는 계정에 할당된 액세스 도메인의 구성 변경 사항만 포함됩니다. 기본 위치를 수락하는 대신 푸시 범위에 대한 선택을 편집할 수 있습니다. 커밋 > 디바이스에 푸시를 선택하면 구성 푸시를 예약할 수 있습니다.
위치 유형	이 열은 보류 중인 변경 사항의 위치를 분류합니다. • 디바이스 그룹 - 특정 디바이스 그룹에 정의된 설정입니다. • 템플릿 - 특정 템플릿 또는 템플릿 스택(template stack)에 정의된 설정입니다. • 로그 수집기 그룹 - 수집기 그룹 구성과 관련된 설정입니다. • **WildFire** 클러스터 - WildFire 클러스터 구성과 관련된 설정입니다. • **WildFire** 어플라이언스 - WildFire 어플라이언스 구성과 관련된 설정입니다.
개체 유형	구성 변경의 객체 유형을 표시합니다. 예를 들어 네트워크 프로파일(네트워크 > 네트워크 프로파일)을 구성한 경우 ####이 표시됩니다. 주소 그룹(개체 > 주소 그룹)을 구성한 경우 ##-##이 표시됩니다.
엔티티	각 디바이스 그룹 또는 템플릿에 대해 이 열에는 푸시 작업에 포함된 방화벽(디바이스 이름 또는 일련번호별) 또는 가상 시스템(이름별)이 나열됩니다. 영향을 받는 방화벽 또는 가상 시스템 목록을 변경하여 구성 변경 사항을 푸시하려면 선택 사항 편집을 클릭합니다. 수집기 그룹에 변경 사항을 푸시하면 목록에 없는 경우에도 그룹의 구성원인 모든 로그 수집기가 작업에 포함됩니다.
관리자	구성을 변경한 관리자의 이름입니다.

필드/버튼	설명
푸시에 포함	푸시할 변경 사항을 선택할 수 있습니다. 기본적으로 푸시 범위 내의 모든 변경 사항이 선택됩니다. 이 열은 특정 관리자가 변경사항 푸시를 선택한 후에만 표시됩니다.
선택 수정	푸시 작업에 포함할 엔터티를 클릭하여 선택합니다. • 디바이스 그룹 및 템플릿 • 로그 수집기 그룹 • WildFire 어플라이언스 및 클러스터 *Panorama*에서는 *Panorama* 구성에 아직 커밋하지 않은 변경 사항을 푸시할 수 없습니다.
디바이스 그룹 및 템플릿	선택 사항을 편집하고 디바이스 그룹 또는 템플릿을 선택하여 다음 행에 옵션을 표시합니다.
필터	템플릿, 템플릿 스택(template stack) 또는 디바이스 그룹 목록과 연결된 방화벽 및 가상 시스템을 필터링합니다. 커밋 상태, 디바이스 상태, 태그 및 고가용성(HA) 상태에 따라 관리 방화벽을 필터링할 수도 있습니다.
이름	푸시 작업에 포함할 템플릿, 템플릿 스택(template stack), 디바이스 그룹, 방화벽 또는 가상 시스템을 선택합니다.
마지막 커밋 상태	방화벽 및 가상 시스템 구성이 Panorama의 템플릿 또는 디바이스 그룹 구성과 동기화되는지의 여부를 나타냅니다.
HA 상태	나열된 방화벽의 고가용성(HA) 상태를 나타냅니다. • 활성 - 정상적인 트래픽 처리 작동 상태입니다. • 수동 - 일반 백업 상태입니다. • 시작 중 - 방화벽은 부팅 후 최대 60초 동안 이 상태에 있습니다. • 작동하지 않음 - 오류 상태입니다. • 일시 중단됨 - 관리자가 방화벽을 비활성화했습니다. • 임시 - 능동형/능동형 구성의 링크 또는 경로 모니터링 이벤트의 경우.

필드/버튼	설명
보류 중인 변경 사항(Panorama) 커밋	선택한 방화벽 및 가상 시스템에 변경 사항을 푸시하기 전에 Panorama 커밋이 필요한지(#) 아니면 필요하지 않은지(###) 나타냅니다.
변경 사항 미리보기 열	푸시 범위에서 선택한 구성을 Panorama 실행 구성과 비교하려면 변경 사항을 미리 봅니다. Panorama는 디바이스 그룹 또는 템플릿 탭에서 선택한 방화벽 및 가상 시스템에 대한 결과만 표시하도록 출력을 필터링합니다. 미리보기 창은 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)인 변경 사항을 나타냅니다. 미리보기 결과가 새 브라우저 창에 표시되기 때문에 브라우저에서 팝업을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 허용 단계를 참조하세요.
모두 선택	목록의 모든 항목을 선택합니다.
모두 선택 해제	목록의 모든 항목을 선택 취소합니다.
모두 확장	템플릿, 템플릿 스택(template stack) 또는 디바이스 그룹에 할당된 방화벽 및 가상 시스템을 표시합니다.
모두 중단	템플릿, 템플릿 스택(template stack) 또는 디바이스 그룹만 표시하고 할당된 방화벽이나 가상 시스템은 표시하지 않습니다.
그룹 HA 피어	고가용성(HA) 구성에서 피어인 방화벽을 그룹화합니다. 결과 목록에는 능동형 방화벽(또는 능동형/능동형 구성의 능동형-기본 방화벽)이 먼저 표시되고 괄호 안에 수동형 방화벽(또는 능동형/능동형 구성의 능동형-보조 방화벽)이 표시됩니다. 이를 통해 HA 모드에 있는 방화벽을 쉽게 식별할 수 있습니다. 공유 정책을 푸시할 때 개별 피어 대신 그룹화된 쌍으로 푸시할 수 있습니다. 능동형/수동형 구성의 *HA* 피어의 경우 두 피어에 동시에 구성을 푸시할 수 있도록 두 방화벽 또는 가상 시스템을 동일한 디바이스 그룹, 템플릿 또는 템플릿 스택*(template stack)*에 추가하는 것을 고려하십시오.
확인	선택한 방화벽 및 가상 시스템에 푸시하는 구성을 확인하려면 클릭합니다. 작업 관리자가 자동으로 열리고 유효성 검사 상태가 표시됩니다.

필드/버튼	설명
필터 선택	목록에 특정 방화벽이나 가상 시스템만 표시하려면 해당 방화벽이나 가상 시스템을 선택한 다음 선택 항목 필터링을 선택합니다.
후보 구성과 병합	(기본적으로 선택됨) Panorama에서 푸시된 구성 변경 사항을 관리자가 대상 방화벽에서 로컬로 구현한 보류 중인 구성 변경 사항과 병합합니다. 푸시 작업은 PAN-OS®가 병합된 변경 사항을 커밋하도록 트리거합니다. 이 선택을 취소하면 커밋에서 방화벽의 후보 구성을 제외합니다. 방화벽 관리자가 방화벽에서 로컬로 변경 사항을 커밋하도록 허용하고 *Panorama*에서 변경 사항을 커밋할 때 이러한 로컬 변경 사항을 포함하지 않으려면 이 선택을 취소합니다. 또 다른 모범 사례는 방화벽에서 구성 감사를 수행하여 Panorama에서 변경 사항을 푸시하기 전에 로컬 변경 사항을 검토하는 것입니다(디바이스 > 구성 감사 참조).
디바이스 및 네트워크 템플릿 포함 (디바이스 그룹 탭만 해당)	(기본적으로 선택됨) 단일 작업으로 디바이스 그룹 변경 사항과 연결된 템플릿 변경 사항을 모두 선택한 방화벽 및 가상 시스템에 푸시합니다. 이러한 변경 사항을 별도의 작업으로 푸시하려면 이 옵션을 선택 취소합니다.
강제 템플릿 값	템플릿 또는 템플릿 스택(template stack)에 정의된 개체로 모든 로컬 설정을 재정의합니다. 여기에는 로컬로 구성된 개체와 Panorama에서 푸시하여 로컬로 덮어쓴 개체가 포함됩니다. 개체가 방화벽에 로컬로 구성되어 있지만 템플릿이나 템플릿 스택(template stack)에 구성되지 않은 경우 방화벽에서 변경되지 않고 삭제되지 않습니다. 이 설정은 기본적으로 비활성화되어 있으며 Panorama에서 관리 방화벽으로 푸시할 때마다 활성화(선택)해야 합니다. 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 교체하여 발생하는 예기치 않은 네트워크 중단이나 문제가 발생하지 않는지 확인하십시오.
로그 수집기 그룹	선택 사항을 편집하고 푸시 작업에 포함할 로그 수집기 그룹을 선택합니다. 이 탭에는 다음 옵션이 표시됩니다.

필드/버튼	설명
	• 모두 선택 - 목록의 모든 수집기 그룹을 선택합니다. • 모두 선택 취소 - 목록의 모든 수집기 그룹을 선택 취소합니다.
WildFire 어플라이언스 및 클러스터	선택을 편집하고 **WildFire** 어플라이언스 및 클러스터를 선택하여 다음 옵션을 표시합니다.
필터	WildFire 어플라이언스 및 클러스터 목록을 필터링합니다.
이름	Panorama가 변경 사항을 푸시할 WildFire 어플라이언스 및 클러스터를 선택합니다.
마지막 커밋 상태	WildFire 어플라이언스 및 클러스터 구성이 Panorama와 동기화되는지의 여부를 나타냅니다.
기본 선택 없음	기본적으로 선택된 디바이스를 제거하려면 활성화(선택)하여 푸시할 특정 디바이스를 수동으로 선택합니다. Panorama가 푸시하는 기본 디바이스는 영향을 받는 디바이스 그룹 및 템플릿 구성 변경 사항을 기반으로 합니다. 이 설정을 활성화하면 디바이스에 푸시(*커밋 > 푸시 및 커밋 > 및 푸시*)가 지속되며 설정을 활성화한 관리자 계정에만 적용됩니다. 한 번의 푸시에 대해 이 설정을 활성화하면 비활성화될 때까지 모든 후속 푸시에 대해 이 설정이 활성화됩니다.
디바이스 그룹 푸시 확인	푸시 범위 목록에서 디바이스 그룹으로 푸시하는 구성의 유효성을 검사합니다. 작업 관리자가 자동으로 열리고 유효성 검사 상태가 표시됩니다.
템플릿 푸시 검증	푸시 범위 목록의 템플릿에 푸시하는 구성을 검증합니다. 작업 관리자가 자동으로 열리고 유효성 검사 상태가 표시됩니다.
위치 유형별 그룹화	위치 유형을 사용하여 푸시 범위 목록을 그룹화하려면 선택합니다.
Panorama 구성을 커밋하거나 변경 사항을 디바이스에 푸시할 때 다음 옵션이 적용됩니다.	
설명	다른 관리자가 변경 사항을 이해할 수 있도록 설명(최대 512자)을 입력합니다. 커밋 이벤트에 대한 시스템 로그는 *512*자보다 긴 설명을 자릅니다.

필드/버튼	설명
커밋 / 푸시 / 커밋 및 푸시	커밋을 시작하거나 다른 커밋이 보류 중인 경우 커밋 요청을 커밋 큐에 추가합니다.

Panorama 정책 정의

Panorama™의 디바이스 그룹을 사용하면 방화벽 정책을 중앙에서 관리할 수 있습니다. Panorama에서 사전 규칙 또는 사후 규칙으로 정책을 생성합니다. 사전 규칙 및 사후 규칙을 사용하면 정책 구현을 위한 계층적 접근 방식을 만들 수 있습니다.

공유 컨텍스트에서 사전 규칙 및 사후 규칙을 모든 관리되는 방화벽에 대한 공유 정책으로 정의하거나 디바이스 그룹 컨텍스트에서 디바이스 그룹에 특정한 규칙을 만들 수 있습니다. Panorama에서 사전 규칙 및 사후 규칙을 정의한 다음 Panorama에서 관리되는 방화벽으로 푸시하기 때문에 관리되는 방화벽에서 규칙을 볼 수 있지만 Panorama에서만 사전 규칙 및 사후 규칙을 편집할 수 있습니다.

- 사전 규칙 - 규칙 순서의 맨 위에 추가되고 먼저 평가되는 규칙입니다. 사전 규칙을 사용하여 조직에 대한 사용 제한 정책을 시행할 수 있습니다. 예를 들어 특정 URL 카테고리에 대한 액세스를 차단하거나 모든 사용자에 대해 DNS 트래픽을 허용할 수 있습니다.
- 사후 규칙 - 규칙 순서의 맨 아래에 추가되고 사전 규칙 및 방화벽에 로컬로 정의된 규칙 이후에 평가되는 규칙입니다. 사후 규칙에는 일반적으로 App-ID™, User-ID™ 또는 서비스를 기반으로 트래픽에 대한 액세스를 거부하는 규칙이 포함됩니다.
- 기본 규칙 - 방화벽이 사전 규칙, 사후 규칙 또는 로컬 방화벽 규칙과 일치하지 않는 트래픽을 처리하는 방법을 지정하는 규칙입니다. 이러한 규칙은 사전 정의된 Panorama 구성의 일부입니다. 이러한 규칙의 선택 설정을 재정의하고 편집을 활성화하려면 보안 정책 규칙 재정의 또는 되돌리기를 참조하십시오.

관리되는 방화벽에 규칙을 푸시하기 전에 모든 규칙 목록을 보려면 규칙 미리 보기를 클릭합니다. 각 규칙 베이스 내에서 규칙 레이어는 각 디바이스 그룹(및 관리되는 방화벽)에 대해 시각적으로 구분되어 많은 수의 규칙을 쉽게 검색할 수 있습니다.

새 규칙을 추가하면 규칙에 대한 정적 운영 데이터가 표시됩니다. UUID(Universally Unique Identifier) 열에는 규칙에 대한 36자의 UUID가 표시됩니다. 방화벽은 규칙별로 UUID를 생성합니다. 그러나 Panorama에서 규칙을 푸시하는 경우 이러한 규칙에는 동일한 UUID가 있으며 이는 결합된 규칙 미리 보기에도 표시됩니다. **Created** 열에는 규칙이 규칙 베이스에 추가된 시간과 날짜가 표시됩니다. 또한 **Modified** 열에는 규칙이 마지막으로 편집된 시간과 날짜가 표시됩니다. PAN-OS 9.0으로 업그레이드하기 전에 정책 규칙을 만든 경우 **First Hit** 데이터를 사용하여 **Created** 날짜를 설정합니다. 규칙에 사용할 수 있는 **First Hit** 데이터가 없는 경우 방화벽 또는 Panorama 관리 서버가 PAN-OS 9.0으로 업그레이드된 시간 및 날짜를 사용하여 생성 날짜를 설정합니다.

Panorama에서 규칙을 추가하거나 편집하면 대상 탭이 표시됩니다. 이 탭을 사용하여 규칙이 정의된 디바이스 그룹(또는 공유 위치)의 특정 방화벽 또는 하위 디바이스 그룹에 규칙을 적용할 수 있습니다. 대상 탭에서 모두(기본값)를 선택할 수 있습니다. 이는 규칙이 모든 방화벽 및 하위 디바이스 그룹에 적용됨을 의미합니다. 특정 방화벽 또는 디바이스 그룹을 대상으로 하려면 모두의 선택을 취소하고 이름으로 특정 방화벽 또는 디바이스 그룹을 선택합니다. 특정 방화벽 또는 디바이스 그룹을 제외하려면 모두를 선택 취소하고 이름별로 특정 방화벽 및 디바이스 그룹을 선택한 다음 지정된 디바이스를 제외한 모든 디바이스에 대상을 선택합니다. 디바이스 그룹 및 방화벽 목록이 긴 경우 필터를 적용하여 속성(예: 플랫폼) 또는 일치하는 이름에 대한 텍스트 문자열로 항목을 검색할 수 있습니다.

Panorama에서 규칙을 성공적으로 추가하고 푸시한 후 규칙 사용은 규칙이 디바이스 그룹의 모든 디바이스에서 사용됨, 디바이스 그룹의 일부 디바이스에서 부분적으로 사용됨 또는 디바이스 그룹의 디바이스에서 사용되지 않음인지 표시합니다. Panorama는 정책 규칙 적중 횟수(기본적으로 활성화됨)가 있는 관리 방화벽을 기반으로 규칙 사용을 결정합니다. Panorama 컨텍스트에서 모든 디바이스 그룹에서 공유 정책 규칙에 대한 규칙 사용을 볼 수 있습니다. 또한 컨텍스트를 개별 디바이스 그룹으로 변경하고 디바이스 그룹의 모든 디바이스에서 총 정책 규칙 사용량을 볼 수 있습니다. 미리 보기 규칙은 디바이스 그룹에 대한 각 정책 규칙에 대한 적중 수, 마지막 적중 및 첫 적중을 표시합니다. 총 트래픽 적중 횟수와 첫 번째 및 마지막 적중 타임스탬프는 재부팅, 업그레이드 및 데이터플레인 다시 시작 이벤트를 통해 유지됩니다. 정책 규칙 사용 모니터링을 참조하십시오.

태그로 규칙을 그룹화하여 규칙 기능을 더 잘 시각화하고 규칙 베이스 전체에서 정책 규칙을 보다 쉽게 관리할 수 있도록 정책 규칙과 같은 그룹화를 허용하는 태그를 적용합니다. 태그별로 그룹화된 규칙은 태그 그룹 목록을 표시하지만 규칙 우선 순위 목록을 유지합니다. 태그 그룹 끝에 규칙을 추가하고, 규칙을 다른 태그 그룹으로 이동하고, 태그 그룹의 규칙에 추가 태그를 적용하고, 그룹 태그를 사용하여 필터링하거나 검색할 수 있습니다.

정책 규칙의 변경 사항을 추적하려면 코멘트 감사를 추가하여 변경 사항과 규칙이 생성 또는 수정된 이유를 설명합니다. 코멘트 감사를 입력하고 구성 변경이 커밋된 후 코멘트 감사는 선택한 규칙에 대한 모든 이전 코멘트 감사를 볼 수 있는 코멘트 감사 아카이브에 보존됩니다. Global Find에서 코멘트 감사를 검색할 수 있습니다. 코멘트 감사 아카이브는 읽기 전용입니다.

정책 탭에 대한 액세스 권한이 있는 관리 사용자는 웹 인터페이스에 **PDF/CSV**로 표시되는 정책 규칙을 내보낼 수 있습니다. 구성 테이블 데이터 내보내기를 참조하십시오.

정책을 생성하려면 각 규칙 베이스에 대한 관련 섹션을 참조하십시오.

- 정책 > 보안
- 정책 > NAT
- 정책 > QoS
- 정책 > 정책 기반 포워딩
- 정책 > 복호화
- 정책 > 네트워크 패킷 브로커
- 정책 > 터널 검사
- 정책 > 애플리케이션 재정의
- 정책 > 인증
- 정책 > DoS 방어
- 정책 > SD-WAN

레거시 모드의 Panorama 가상 어플라이언스에 대한 로그 스토리지 파티션

- Panorama > 설정 > 작업

기본적으로 레거시 모드의 Panorama 가상 어플라이언스에는 10.89GB가 로그 스토리지에 할당되는 모든 데이터에 대한 단일 디스크 파티션이 있습니다. 디스크 크기를 늘려도 로그 저장 용량은 늘어나지 않습니다. 그러나 다음 옵션을 사용하여 로그 저장 용량을 수정할 수 있습니다.

- **NFS(**네트워크 파일 시스템**)** - NFS 스토리지를 마운트하는 옵션은 레거시 모드에 있고 VMware ESXi 서버에서 실행 중인 Panorama 가상 어플라이언스에만 사용할 수 있습니다. NFS 스토리지를 마운트하려면 기타 섹션에서 스토리지 파티션 설정을 선택한 다음 스토리지 파티션을 **NFS V3**로 설정하고 표에 설명된 대로 설정을 구성합니다. NFS 스토리지 설정.
- 기본 내부 스토리지 - 기본 내부 스토리지 파티션으로 되돌립니다(이전에 다른 가상 로깅 디스크를 구성했거나 NFS에 마운트한 ESXi 서버 또는 vCloud Air 플랫폼의 Panorama에만 적용 가능). 기본 내부 스토리지 파티션으로 되돌리려면 기타 섹션에서 스토리지 파티션 설정을 선택한 다음 스토리지 파티션을 내부로 설정합니다.
- 가상 로깅 디스크 - VMware ESXi 버전 5.5 이상 릴리스에서 실행되는 Panorama 또는 VMware vCloud Air 플랫폼에서 실행되는 Panorama에 대해 다른 가상 디스크(최대 8TB)를 추가할 수 있습니다. 그러나 Panorama는 소스 디스크의 기본 10.89GB 로그 저장소 사용을 중지하고 기존 로그를 새 디스크에 복사합니다. (이전 ESXi 버전은 최대 2TB의 가상 디스크만 지원합니다.)

> 스토리지 파티션 설정을 변경한 후 *Panorama*를 재부팅해야 합니다. ***Panorama*** > ***Setup*** > ***Operations*** 및 ***Reboot Panorama***를 선택합니다.
>
> *NFS* 스토리지는 *Panorama* 모드의 *Panorama* 가상 어플라이언스 또는 *M*-시리즈 어플라이언스에서 사용할 수 없습니다.

표 **1:** 표**: NFS** 스토리지 설정

Panorama 스토리지 파티션 설정 - **NFS V3**	설명
서버	NFS 서버의 FQDN 또는 IP 주소를 지정합니다.
로그 디렉토리	로그가 위치할 디렉토리의 전체 경로 이름을 지정하십시오.
프로토콜	NFS 서버와의 통신을 위한 프로토콜(UDP 또는 TCP)을 지정합니다.
포트	NFS 서버와 통신할 포트를 지정합니다.
읽기 크기	NFS 읽기 작업의 최대 크기를 바이트 단위로 지정합니다(범위는 256~32,768).

Panorama 스토리지 파티션 설정 - **NFS V3**	설명
쓰기 크기	NFS 쓰기 작업의 최대 크기를 바이트 단위로 지정합니다(범위는 256~32,768).
설정 시 복사	Panorama가 부팅될 때 NFS 파티션을 마운트하고 기존 로그를 서버의 대상 디렉토리에 복사하려면 선택합니다.
로깅 파티션 테스트	NFS 파티션을 마운트하고 성공 또는 실패 메시지를 표시하는 테스트를 수행하려면 선택합니다.

Panorama > 설정 > 인터페이스

- Panorama > 설정 > 인터페이스

Panorama > **Setup** > **Interfaces**를 선택하여 Panorama가 방화벽 및 로그 수집기를 관리하고, 방화벽 및 로그 수집기에 소프트웨어 및 콘텐츠 업데이트를 배포하고, 방화벽에서 로그를 수집하고, 수집기 그룹과 통신하는 데 사용하는 인터페이스를 구성합니다. 기본적으로 Panorama는 방화벽 및 로그 수집기와의 모든 통신에 관리(MGT) 인터페이스를 사용합니다.

MGT 인터페이스의 트래픽을 줄이려면 업데이트를 배포하고, 로그를 수집하고, 수집기 그룹과 통신하도록 다른 인터페이스를 구성합니다. 로그 트래픽이 많은 환경에서는 로그 수집을 위해 여러 인터페이스를 구성할 수 있습니다. 또한 관리 트래픽의 보안을 향상시키기 위해 다른 인터페이스의 서브넷보다 더 비공개인 *MGT* 인터페이스에 대해 별도의 서브넷*(IPv4* 넷마스크 또는 *IPv6* 프리픽스 길이*)*을 정의할 수 있습니다.

상호 작용	최대 속도	**M-700** 어플라이언스	**M-600** 어플라이언스	**M-500** 어플라이언스	**M-300** 어플라이언스	**M-200** 어플라이언스	**Panorama** 가상 어플라이언스
관리(MGT)	1Gbps	✓	✓	✓	✓	✓	✓
이더넷1(Eth1)	1Gbps	✓	✓	✓	✓	✓	✓
이더넷2(Eth2)	1Gbps	—	✓	✓	—	✓	✓
이더넷3(Eth3)	1Gbps	—	✓	✓	—	✓	✓
이더넷4(Eth4)	10Gbps	—	✓	✓	—	—	✓
이더넷5(Eth5)	10Gbps	—	✓	✓	—	—	✓

모든 M-시리즈 어플라이언스 모델에 대한 로깅 속도를 검토하십시오. 아래 나열된 로깅 속도를 달성하려면 M-시리즈 어플라이언스가 수집기 그룹의 단일 로그 수집기여야 하며 M-시리즈 모델에 대한 모든 로깅 디스크를 설치해야 합니다. 예를 들어, M-500 어플라이언스에 대해 초당 30,000개의 로그를 달성하려면 1TB 또는 2TB 디스크가 있는 12개의 로깅 디스크를 모두 설치해야 합니다.

모델 용량 및 기능	**M-700** 어플라이언스	**M-600** 어플라이언스	**M-500** 어플라이언스	**M-300** 어플라이언스	**M-200** 어플라이언스
관리 전용 모드에서 Panorama에 대한 최대 로깅 속도	로컬 로그 스토리지는 지원되지 않습니다.				
Panorama 모드에서 Panorama에 대한 최대 로깅 속도	36,500 로그/초	25,000로그/초	20,000로그/초	16,500 로그/초	10,000로그/초
로그 수집기 모드에서 Panorama에 대한 최대 로깅 속도	73,000 로그/초	50,000로그/초	30,000로그/초	33,000 로그/초	28,000로그/초
어플라이언스의 최대 로그 스토리지	48TB(12x8TB RAID 디스크)	48TB(12x8TB RAID 디스크)	• 24TB(24x2TB RAID 디스크) • 12TB(24x1TB RAID 디스크)	16TB(4x8TB RAID 디스크)	16TB(4x8TB RAID 디스크)
어플라이언스의 기본 로그 스토리지	16TB(4x8TB RAID 디스크)	16TB(4x8TB RAID 디스크)	4TB(4x2TB RAID 디스크)	16TB(4x8TB RAID 디스크)	16TB(4x8TB RAID 디스크)
어플라이언스의 SSD 스토리지(M-시리즈 어플라이언스가 생성하는 로그용)	240GB	240GB	240GB	240GB	240GB
NFS 연결 로그 스토리지	사용할 수 없습니다				

인터페이스를 구성하려면 인터페이스 이름을 클릭하고 다음 표에 설명된 설정을 구성합니다.

항상 *IP* 주소, 넷마스크*(IPv4*의 경우*)* 또는 프리픽스 길이*(IPv6*의 경우*)* 및 *MGT* 인터페이스의 기본 게이트웨이를 지정하십시오. 일부 설정*(*예*:* 기본 게이트웨이*)*의 값을 생략하면 향후 구성 변경을 위해 콘솔 포트를 통해서만 *Panorama*에 액세스할 수 있습니다. 세 가지 설정을 모두 지정하지 않으면 다른 인터페이스에 대한 구성을 커밋할 수 없습니다. *DHCP*만 인터페이스를 지원하므로 이 요구 사항은 지원되는 클라우드 하이퍼바이저의 *Panorama* 가상 어플라이언스에는 적용되지 않습니다.

인터페이스 설정	설명
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	구성하려면 인터페이스를 활성화해야 합니다. 예외는 기본적으로 활성화되어 있는 MGT 인터페이스입니다.
IP 주소(IPv4)	네트워크에서 IPv4 주소를 사용하는 경우 인터페이스에 IPv4 주소를 할당합니다.
넷마스크(IPv4)	인터페이스에 IPv4 주소를 할당한 경우 네트워크 마스크(예: 255.255.255.0)도 입력해야 합니다.
기본 게이트웨이(IPv4)	인터페이스에 IPv4 주소를 할당한 경우 기본 게이트웨이에도 IPv4 주소를 할당해야 합니다(게이트웨이는 인터페이스와 동일한 서브넷에 있어야 함).
IPv6 주소/프리픽스 길이	네트워크에서 IPv6 주소를 사용하는 경우 인터페이스에 IPv6 주소를 할당합니다. 넷마스크를 나타내려면 IPv6 프리픽스 길이(예: 2001:400:f00::1/64)를 입력합니다. *IPv6* 주소는 프라이빗 클라우드 환경*(ESXi, vCloud Air, KVM* 또는 *Hyper-V)*에 배포된 모든 *M* 시리즈 어플라이언스 및 *Panorama* 가상 어플라이언스의 *MGT* 인터페이스에 대해 지원됩니다. 퍼블릭 클라우드 환경*(Amazon Web Services(AWS), AWS GovCloud, Microsoft Azure* 또는 *Google Cloud Platform)*에 배포된 *Panorama* 가상 어플라이언스의 *MGT* 인터페이스에는 *IPv6* 주소가 지원되지 않습니다.
기본 IPv6 게이트웨이	인터페이스에 IPv6 주소를 할당한 경우 기본 게이트웨이에도 IPv6 주소를 할당해야 합니다(게이트웨이는 인터페이스와 동일한 서브넷에 있어야 함).

인터페이스 설정	설명
	IPv6 주소는 프라이빗 클라우드 환경*(ESXi, vCloud Air, KVM* 또는 *Hyper-V)*에 배포된 모든 *M* 시리즈 어플라이언스 및 *Panorama* 가상 어플라이언스의 *MGT* 인터페이스에 대해 지원됩니다. 퍼블릭 클라우드 환경*(Amazon Web Services(AWS), AWS GovCloud, Microsoft Azure* 또는 *Google Cloud Platform)*에 배포된 *Panorama* 가상 어플라이언스의 *MGT* 인터페이스에는 *IPv6* 주소가 지원되지 않습니다.
속도	인터페이스 속도를 전이중 또는 반이중에서 10Mbps, 100Mbps, 1Gbps 또는 10Gbps(Eth4 및 Eth5만 해당)로 설정합니다. 기본 자동 협상 설정을 사용하여 Panorama가 인터페이스 속도를 결정하도록 합니다. 이 설정은 인접 네트워크 장비의 인터페이스 설정과 일치해야 합니다. 설정이 일치하도록 하려면 인접 장비가 해당 옵션을 지원하는 경우 자동 협상을 선택합니다.
MTU	이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~1,500, 기본값은 1,500).
디바이스 관리 및 디바이스 로그 수집	방화벽 및 로그 수집기를 관리하고 해당 로그를 수집하기 위해 인터페이스(MGT 인터페이스에서 기본적으로 활성화됨)를 활성화합니다. 여러 인터페이스를 활성화하여 이러한 기능을 수행할 수 있습니다.
수집기 그룹 커뮤니케이션	Collector Group 통신을 위한 인터페이스를 활성화합니다(기본값은 MGT 인터페이스). 하나의 인터페이스만 이 기능을 수행할 수 있습니다.
시스템 로그 포워딩	syslog 포워딩을 위한 인터페이스를 활성화합니다(기본값은 MGT 인터페이스). 하나의 인터페이스만 이 기능을 수행할 수 있습니다.
디바이스 배포	방화벽 및 로그 수집기에 소프트웨어 및 콘텐츠 업데이트를 배포하기 위한 인터페이스를 활성화합니다(기본값은 MGT 인터페이스). 하나의 인터페이스만 이 기능을 수행할 수 있습니다.
행정 관리 서비스	• **HTTP** - Panorama 웹 인터페이스에 액세스할 수 있습니다. HTTP는 HTTPS만큼 안전하지 않은 일반 텍스트를 사용합니다. 인터페이스의 관리 트래픽에 대해 *HTTP* 대신 ***HTTPS***를 활성화합니다. • **Telnet** - Panorama CLI에 액세스할 수 있습니다. Telnet은 SSH만큼 안전하지 않은 일반 텍스트를 사용합니다.

인터페이스 설정	설명
	• **HTTPS** - Panorama 웹 인터페이스에 대한 보안 액세스를 활성화합니다. 인터페이스의 관리 트래픽에 대해 *Telnet* 대신 ***SSH***를 활성화합니다. • **SSH** - Panorama CLI에 대한 보안 액세스를 활성화합니다.
네트워크 연결 서비스	**Ping** 서비스는 모든 인터페이스에서 사용할 수 있습니다. 핑(ping)을 사용하여 Panorama 인터페이스와 외부 서비스 간의 연결을 테스트할 수 있습니다. 고가용성(HA) 배포에서 HA 피어는 핑(ping)을 사용하여 하트비트 백업 정보를 교환합니다. 다음 서비스는 MGT 인터페이스에서만 사용할 수 있습니다. • **SNMP** - Panorama가 SNMP 관리자의 통계 쿼리를 처리할 수 있도록 합니다. 자세한 내용은 SNMP 모니터링 활성화를 참조하십시오. • **User-ID** - Panorama에서 User-ID 에이전트로부터 수신한 사용자 매핑 정보를 재배포할 수 있습니다.
허용된 IP 주소	관리자가 이 인터페이스에서 Panorama에 액세스할 수 있는 IP 주소를 입력합니다. 빈 목록(기본값)은 모든 IP 주소에서 액세스할 수 있음을 지정합니다. 이 목록을 공백으로 두지 마십시오. 무단 액세스를 방지하기 위해 *Panorama* 관리자의 *IP* 주소를 지정합니다*(*전용*)*.

Panorama > 고가용성

Panorama에서 고가용성(HA)을 활성화하려면 다음 표에 설명된 대로 설정을 구성합니다.

Panorama HA 설정	설명
설정 편집()을 클릭하여 다음 설정을 구성합니다.	
HA 활성화	HA를 활성화하려면 선택합니다.
피어 HA IP 주소	피어에 있는 MGT 인터페이스의 IP 주소를 입력합니다.
암호화 활성화	활성화되면 MGT 인터페이스가 HA 피어 간의 통신을 암호화합니다. 암호화를 활성화하기 전에 각 HA 피어에서 HA 키를 내보내고 다른 피어로 키를 가져옵니다. **Panorama** > **Certificate** 관리 > 인증서 페이지에서 HA 키를 가져오고 내보냅니다(방화벽 및 Panorama 인증서 관리 참조). *HA* 연결은 암호화가 활성화된 *TCP* 포트 *28*을 사용하고 암호화가 활성화되지 않은 *TCP* 포트 *28769*를 사용합니다.
모니터 유지 시간(ms)	제어 링크 실패에 대해 조치를 취하기 전에 시스템이 대기할 시간(밀리초)을 입력하십시오(범위는 1,000 ~ 60,000, 기본값은 3,000).
일렉션(election) 설정 편집()을 클릭하여 다음 설정을 구성합니다.	
우선 사항 (Panorama 가상 어플라이언스에 필요)	이 설정은 어떤 피어가 방화벽 로그의 기본 수신자인지 결정합니다. HA 쌍에서 한 피어를 기본으로 할당하고 다른 피어를 보조로 할당합니다. 레거시 모드에서 Panorama 가상 어플라이언스에 대한 로그 스토리지 파티션을 구성할 때 내부 디스크(기본값) 또는 로그 스토리지에 NFS(네트워크 파일 시스템)를 사용할 수 있습니다. NFS를 구성하면 기본 수신자만 방화벽 로그를 수신합니다. 내부 디스크 저장소를 구성하는 경우 방화벽은 기본적으로 기본 피어와 보조 피어 모두에 로그를 보내지만 로깅 및 보고 설정에서 활성 기본 로그만 로컬 디스크로 활성화하여 이를 변경할 수 있습니다.

Panorama HA 설정	설명
선점	기본 Panorama가 장애 복구 후 활성 작업을 재개할 수 있도록 하려면 선택합니다. 비활성화하면 기본 Panorama가 오류에서 복구된 후에도 보조 Panorama가 활성 상태로 유지됩니다.
HA 타이머 설정	선택 항목에 따라 페일오버 속도를 제어하는 나머지 HA 선택 설정 값이 결정됩니다. • 권장 - 일반적인(기본) 페일오버 타이머 설정에 대해 선택합니다. 연결된 값을 보려면 **Advanced** 및 권장 로드를 선택합니다. • **Aggressive** - 더 빠른 페일오버 타이머 설정을 위해 선택합니다. 연결된 값을 보려면 **Advanced** 및 **Aggressive** 로드를 선택합니다. • **Advanced** - 나머지 HA 선택 설정을 표시하고 해당 값을 사용자 지정하려면 선택합니다. 다음 설정에 대한 권장 및 **Aggressive** 값을 참조하십시오.
프로모션 보류 시간(ms)	기본 피어가 다운된 후 인계받기 전에 보조 Panorama 피어가 대기하는 시간(범위: 0~60,000)을 밀리초로 입력합니다. 권장되는(기본값) 값은 2,000입니다. Aggressive 값은 500입니다.
헬로 인터벌(ms)	다른 피어가 작동하는지 확인하기 위해 전송되는 헬로 패킷 사이의 시간(범위: 8,000 ~ 60,000)을 밀리초로 입력합니다. 권장(기본값) 및 Aggressive 값은 8,000입니다.
하트비트 인터벌(ms)	Panorama가 ICMP 핑을 HA 피어로 보내는 빈도를 밀리초 단위(범위: 1,000 ~ 60,000)로 지정합니다. 권장되는(기본값) 값은 2,000입니다. Aggressive 값은 1,000입니다.
선점 보류 시간(분)	이 필드는 선점을 선택한 경우에만 적용됩니다. 패시브 Panorama 피어가 페일오버를 유발한 이벤트에서 복구한 후 활성 상태로 폴백하기 전에 대기할 시간(분 범위: 1~60)을 입력합니다. 권장(기본값) 및 Aggressive 값은 1입니다.
모니터 장애 유지 시간(ms)	밀리초 수를 지정합니다(범위는 0 ~ 60,000). Panorama는 패시브 상태로 다시 들어가기 전에 경로 모니터 실패 후 대기합니다. 이 기간 동안 패시브 피어는 장애 발생 시 액티브 피어를 대신할 수 없습니다. 이 인터벌을 통해 Panorama는 인접 디바이스의 간헐적인 플래핑으로 인한 페일오버를 방지할 수 있습니다. 권장(기본값) 및 Aggressive 값은 0입니다.
추가 마스터 보류 시간(ms)	선점하는 피어가 활성 피어로 인계받기 전에 수동 상태를 유지하는 시간(밀리초: 0~60,000)을 지정합니다. 권장되는(기본값) 값은 7,000입니다. Aggressive 값은 5,000입니다.

Panorama HA 설정	설명
경로 모니터링 편 집()을 클릭하여 HA 경로 모니터링을 구성합니다.	
활성화됨	경로 모니터링을 활성화하려면 선택합니다. 경로 모니터링을 통해 Panorama는 ICMP 핑 메시지를 보내 응답 여부를 확인함으로써 지정된 대상 IP 주소를 모니터링할 수 있습니다.
실패 조건	모니터링되는 경로 그룹의 일부 또는 전체가 응답하지 않을 때 페일오버를 수행할지의 여부를 선택합니다.
경로 그룹 HA 경로 모니터링을 위한 경로 그룹을 생성하려면 추가를 클릭하고 다음 필드를 완성하십시오.	
이름	경로 그룹의 이름을 지정하십시오.
활성화됨	경로 그룹을 활성화하려면 선택합니다.
실패 조건	지정된 대상 주소 중 일부 또는 전체가 응답하지 않을 때 오류가 발생하는지의 여부를 선택합니다.
핑(ping) 인터벌	대상 IP 주소에 대한 경로가 작동 중인지 확인하는 ICMP 에코 메시지 사이의 시간(밀리초)을 지정합니다(범위는 1,000 ~ 60,000, 기본값은 5,000).
핑(ping) 카운트	실패를 선언하기 전에 실패한 핑(ping) 수를 지정하십시오(범위는 3~10, 기본값은 3).
대상 IP	모니터링할 대상 IP 주소를 하나 이상 입력합니다. 쉼표를 사용하여 여러 주소를 구분합니다.

Panorama > 관리형 WildFire 클러스터

- Panorama > 관리형 WildFire 클러스터
- Panorama > 관리형 WildFire 어플라이언스

클러스터에서 또는 Panorama M-시리즈 또는 가상 어플라이언스에서 독립 실행형 어플라이언스로 WildFire 어플라이언스를 관리할 수 있습니다. 클러스터 관리(**Panorama** > **Managed WildFire Clusters**)와 독립 실행형 어플라이언스 관리(**Panorama** > **Managed WildFire Appliances**)는 많은 공통 관리 및 구성 작업을 공유하므로 둘 다 다음 주제에 포함됩니다.

WildFire 어플라이언스를 Panorama에 추가한 후 웹 인터페이스를 사용하여 해당 어플라이언스를 클러스터에 추가하고 클러스터로 관리하거나 독립 실행형 어플라이언스로 관리합니다.

- 관리형 WildFire 클러스터 작업
- 관리되는 WildFire 어플라이언스 작업
- 관리되는 WildFire 정보
- 관리형 WildFire 클러스터 및 어플라이언스 관리

관리형 WildFire 클러스터 작업

Panorama에서 WildFire 어플라이언스 클러스터를 생성 및 제거할 수 있습니다. 또한 한 클러스터에서 다른 클러스터로 구성을 가져올 때 구성 시간을 절약할 수 있습니다.

작업	설명
클러스터 생성	필요에 따라 클러스터 생성, 새 클러스터 이름을 입력한 다음 확인을 클릭합니다. 개별 WildFire 어플라이언스 노드를 추가하여 로컬로 구성하고 Panorama에 추가한 기존 클러스터는 해당 WildFire 노드 및 노드 역할(**Panorama** > **Managed WildFire** 어플라이언스)과 함께 나열됩니다. 클러스터 이름은 소문자 또는 숫자로 시작하는 유효한 하위 도메인 이름이어야 하며 클러스터 이름의 첫 번째 또는 마지막 문자가 아닌 경우에만 하이픈을 포함할 수 있습니다. 공백이나 다른 문자는 허용되지 않습니다. 클러스터 이름의 최대 길이는 63자입니다. 클러스터를 생성한 후 관리되는 WildFire 어플라이언스를 클러스터에 추가하고 Panorama에서 관리할 수 있습니다. WildFire 어플라이언스를 Panorama에 추가하면 Panorama에 어플라이언스가 자동으로 등록됩니다. Panorama에서 최대 10개의 관리형 WildFire 클러스터를 생성할 수 있으며 각 클러스터에는 최대 20개의 WildFire 어플라이언스 노드가 있을 수 있습니다.

작업	설명
	Panorama는 최대 총 200개의 독립 실행형 어플라이언스 및 클러스터 노드를 관리할 수 있습니다.
클러스터 구성 가져오기	클러스터 구성 가져오기 기존 클러스터 구성을 가져옵니다. 클러스터 구성을 가져오기 전에 클러스터를 선택하면 컨트롤러와 클러스터가 선택한 클러스터에 대한 적절한 정보로 자동으로 채워집니다. 클러스터 구성을 가져오기 전에 클러스터를 선택하지 않으면 컨트롤러를 선택해야 하며 클러스터는 선택한 컨트롤러 노드에 따라 자동으로 채워집니다. 구성을 불러온 후 **Panorama**에 커밋하여 불러온 후보 구성을 Panorama 실행 구성에 저장합니다.
Panorama에서 제거	더 이상 Panorama에서 WildFire 클러스터를 관리할 필요가 없으면 **Panorama**에서 제거하고 예를 선택하여 작업을 확인합니다. Panorama 관리에서 클러스터를 제거한 후 컨트롤러 노드에서 로컬로 클러스터를 관리할 수 있습니다. 클러스터를 로컬이 아닌 중앙에서 다시 관리하려는 경우 언제든지 Panorama 어플라이언스에 클러스터를 다시 추가할 수 있습니다.
WildFire 클러스터 어플라이언스 간 통신 암호화	클러스터에 있는 WildFire 어플라이언스 간의 데이터 통신을 암호화하려면 보안 클러스터 통신에서 암호화를 활성화하십시오. WildFire는 사전 정의된 인증서 또는 사용자 지정 인증서를 사용하여 어플라이언스 간에 통신합니다. 사용자 정의 인증서는 보안 서버 통신 사용자 정의 및 사용자 정의 인증서 전용을 활성화한 경우에만 사용됩니다. WildFire 클러스터가 FIPS-CC 모드에서 작동하려면 암호화가 필요합니다. FIPS-CC 모드에서 사용되는 사용자 지정 인증서는 FIPS-CC 요구 사항을 충족해야 합니다. 보안 클러스터 통신을 활성화한 후 클러스터에 관리되는 WildFire 어플라이언스를 추가할 수 있습니다. 새로 추가된 어플라이언스는 보안 클러스터 통신 설정을 자동으로 사용합니다.

관리되는 WildFire 어플라이언스 작업

Panorama 디바이스에서 독립형 WildFire 어플라이언스를 추가, 제거 및 관리할 수 있습니다. 독립 실행형 어플라이언스를 추가한 후 WildFire 어플라이언스 클러스터에 클러스터 노드로 추가하거나 개별 독립 실행형 어플라이언스로 관리할 수 있습니다.

작업	설명
어플라이언스 추가	중앙 집중식 관리를 위해 하나 이상의 WildFire 어플라이언스를 Panorama 어플라이언스에 추가하려면 어플라이언스 추가를 클릭합니다. 별도의 행(새

작업	설명

	줄)에 각 WildFire 어플라이언스의 일련번호를 입력합니다. Panorama는 최대 총 200개의 WildFire 클러스터 노드와 독립 실행형 WildFire 어플라이언스를 관리할 수 있습니다.
	
	Panorama에서 관리하려는 각 WildFire 어플라이언스에서 다음 WildFire 어플라이언스 CLI 명령을 사용하여 Panorama 어플라이언스(Panorama 서버)의 IP 주소 또는 FQDN을 구성하고 선택적으로 백업 Panorama 서버를 구성합니다.
	
	`#### ## ### Panorama-## ## <ip-address | FQDN>`
	`#### ## ### Panorama-##-2 ## <ip-address | FQDN>`

구성 가져오기	WildFire 어플라이언스 및 구성 가져오기를 선택하여 해당 어플라이언스에 대해 실행 중인 구성만 Panorama로 가져옵니다. 구성을 불러온 후 **Panorama**에 커밋하여 불러온 후보 구성을 Panorama 실행 구성에 저장합니다.
제거	더 이상 Panorama에서 WildFire 어플라이언스를 관리할 필요가 없으면 어플라이언스를 제거하고 예를 선택하여 작업을 확인합니다. Panorama 관리에서 어플라이언스를 제거한 후 해당 CLI를 사용하여 로컬에서 어플라이언스를 관리할 수 있습니다. 필요한 경우 어플라이언스를 로컬이 아닌 중앙에서 다시 관리하려는 경우 언제든지 어플라이언스를 Panorama 어플라이언스에 다시 추가할 수 있습니다.

관리되는 WildFire 정보

Panorama > **Managed WildFire Clusters**를 선택하여 각 관리 클러스터에 대한 다음 정보를 표시하거나(이 페이지에서 독립 실행형 어플라이언스를 선택한 다음 해당 정보를 표시할 수 있음) **Panorama** > **Managed WildFire Appliances**를 선택하여 독립형 어플라이언스에 대한 정보를 표시합니다.

별도의 언급이 없는 한 다음 표의 정보는 WildFire 클러스터와 독립 실행형 어플라이언스 모두에 적용됩니다. 클러스터 또는 어플라이언스에 대해 이전에 구성된 정보는 미리 채워져 있습니다.

관리되는 **WildFire** 정보	설명
기구	어플라이언스의 이름입니다. Managed WildFire Clusters 보기는 클러스터별로 그룹화된 어플라이언스를 표시하고 클러스터에 추가할 수 있는 독립 실행형 어플라이언스를 포함하며 어플라이언스 이름과 함께 일련번호(괄호 안)를 포함합니다(일련번호는 이름의 일부가 아님).

관리되는 **WildFire** 정보	설명
일련번호 (관리형 WildFire 어플라이언스 보기 전용)	어플라이언스의 일련번호입니다. 관리형 WildFire 클러스터 보기는 어플라이언스 이름과 동일한 열에 일련번호를 표시합니다(일련번호는 이름의 일부가 아님).
소프트웨어 버전	어플라이언스에 설치되어 실행 중인 소프트웨어 버전입니다.
IP 주소	어플라이언스의 IP 주소입니다.
연결됨	어플라이언스와 Panorama 간의 연결 상태(연결됨 또는 연결 해제됨)입니다.
클러스터 이름	어플라이언스가 노드로 포함된 클러스터의 이름이며, 독립 실행형 어플라이언스에 대해서는 여기에 아무 것도 표시되지 않습니다.
분석 환경	분석 환경(vm1, vm2, vm3, vm4 또는 vm5). 각 분석 환경은 운영 체제 및 애플리케이션 집합을 나타냅니다. • vm-1은 Windows XP, Adobe Reader 9.3.3, Flash 9, PE, PDF 및 Office 2003 및 이전 Office 릴리스를 지원합니다. • vm-2는 Windows XP, Adobe Reader 9.4.0, Flash 10n, PE, PDF, Office 2007 및 이전 Office 릴리스를 지원합니다. • vm-3은 Windows XP, Adobe Reader 11, Flash 11, PE, PDF 및 Office 2010 및 이전 Office 릴리스를 지원합니다. • vm-4는 Windows 7 32비트, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 및 이전 Office 릴리스를 지원합니다. • vm-5는 Windows 7 64비트, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 및 이전 Office 릴리스를 지원합니다.
콘텐츠	콘텐츠 릴리스 버전의 버전 번호입니다.
역할	어플라이언스 역할: • 독립 실행형 - 어플라이언스가 클러스터 노드가 아닙니다. • 컨트롤러 - 어플라이언스는 클러스터 컨트롤러 노드입니다. • 컨트롤러 백업 - 어플라이언스는 클러스터 컨트롤러 백업 노드입니다. • 작업자 - 어플라이언스는 클러스터의 작업자 노드입니다.
구성 상태	어플라이언스의 구성 동기화 상태입니다. Panorama 어플라이언스는 WildFire 어플라이언스 설정을 확인하고 Panorama에서 해당 어플라이언스에 대해 저장된 구성과 어플라이언스 구성 간의 구성 차이를 보고합니다.

관리되는 **WildFire** 정보	설명
	• 동기화 중 - 어플라이언스 구성이 Panorama에 저장된 구성과 동기화됩니다. • 동기화되지 않음 - 어플라이언스 구성이 Panorama에 저장된 구성과 동기화되지 않습니다. 안경 위로 마우스를 가져가면 동기화 실패의 원인을 표시할 수 있습니다.

클러스터 상태
(관리형 WildFire 클러스터 페이지만 해당)
	클러스터 상태는 각 클러스터 노드에 대한 세 가지 유형의 정보를 표시합니다.
	• 사용 가능한 서비스(정상 작동 조건):
	  • **wfpc**(WildFire Private Cloud) - 멀웨어 샘플 분석 및 보고 서비스입니다.
	  • 서명 - 로컬 서명 생성 서비스입니다.
	• 작업 진행 - 작업 이름 뒤에 콜론(:) 및 상태:
	  • 작업 - 해제, 일시 중단 및 재부팅 작업의 상태입니다.
	  • 진행 상태 - 작업 상태 알림은 요청됨, 진행 중, 거부됨, 성공 또는 실패와 같이 각 작업에 대해 동일합니다.
	  예를 들어, 노드를 일시 중단하고 작업이 진행 중인 경우 클러스터 상태는 ## ##:## 중을 표시하거나, 노드를 재부팅하고 작업이 요청되었지만 아직 시작되지 않은 경우 클러스터 상태는 ###:###을 표시합니다.
	• 오류 조건:
	  클러스터 상태는 다음 오류 조건을 표시합니다.
	  • 클러스터 - ####:#### 또는 ####:######.
	  • 서비스 - ###:## ## 또는 ###:##.

마지막 커밋 상태	가장 최근 커밋이 성공하면 ### ##하고 가장 최근 커밋이 실패하면 ### ##합니다. 상태를 선택하여 마지막 커밋에 대한 세부 정보를 봅니다.
활용 > 보기	
보기	클러스터 또는 어플라이언스 활용 통계를 봅니다. 개별 어플라이언스(**Panorama** > **Managed WildFire Appliances**)만 보거나 클러스터 통계(**Panorama** > **Managed WildFire Clusters**)만 볼 수 있습니다. • 어플라이언스 - (독립형 어플라이언스 보기 전용) 어플라이언스 일련번호입니다. • 클러스터 - (클러스터 보기 전용) 클러스터 이름입니다. 다른 클러스터를 선택하여 볼 수도 있습니다.

관리되는 **WildFire** 정보	설명

	• 기간 - 통계가 수집되고 표시되는 기간을 표시합니다. 다른 기간 선택 가능:
	  • **15**분
	  • 마지막 시간 지난 **24**시간
	  • **(**기본값**)**
	  • 지난 **7**일
	  • 모두
	사용률 보기에는 4개의 탭이 있으며, 각 탭에서 구성된 기간에 따라 표시되는 항목을 결정합니다.

일반 탭	일반 탭에는 클러스터 또는 어플라이언스에 대해 통합된 리소스 사용률 통계가 표시됩니다. 다른 탭에는 파일 유형별 리소스 사용률에 대한 보다 세부적인 정보가 표시됩니다.
	• 총 디스크 사용량 - 총 클러스터 또는 어플라이언스 디스크 사용량입니다.
	• 판정 - 총 판정 수, 파일에 할당된 각 판정 유형 수—멀웨어, 그레이웨어, 양성 및 오류 판정이 나온 판정 수입니다.
	• 샘플 통계 - 제출 및 분석된 총 샘플 수와 분석 보류 중인 샘플 수입니다.
	• 분석 환경 및 시스템 활용도:
	  • 분석된 파일 유형 - 분석된 파일 유형(실행 가능, 실행 불가 또는 링크)입니다.
	  • 가상 머신 사용량 - 분석된 각 파일 유형에 사용된 가상 머신의 수와 각 파일 유형을 분석하는 데 사용할 수 있는 가상 머신의 수입니다. 예를 들어 실행 파일의 경우 VM 사용량은 6/10일 수 있습니다(6개의 VM이 사용되고 10개의 VM이 사용 가능).
	  • 분석된 파일 - 분석된 각 유형의 파일 수입니다.

실행 가능, 실행 불가능 및 링크 탭	실행 파일, 비실행 파일 및 링크는 각 파일 유형에 대해 유사한 정보를 표시합니다. • 판정 - 파일 유형별 판정에 대한 세부 정보입니다. 결과를 필터링할 수 있습니다. • 검색 상자 - 판정을 필터링할 검색어를 입력합니다. 검색 상자는 목록의 파일 형식(항목) 수를 나타냅니다. 검색어를 입력한 후 필터를 적용하거나(→ 필터를 지우)

관리되는 **WildFire** 정보	설명
	고(✕) 다른 용어 집합을 입력합니다. • 파일 유형 - 유형별로 파일을 나열합니다. 예를 들어 실행 파일 탭에는 .exe 및 .dll 파일 형식이 표시됩니다. 비실행 탭에는 .pdf, .jar, .doc, .ppt, .xls, .docx, .pptx, .xlsx, .rtf, class 및 .swf 파일 형식이 표시되고, 링크 탭에는 elink 파일 형식 정보가 표시됩니다. • 각 파일 형식에 대해 **Malware**, **Grayware** 및 **Benign** 파일에 대한 총 판정 수, 오류 판정 수 및 총 판정 수가 각 탭에 표시됩니다. • 샘플 통계 - 파일 유형별 샘플 분석에 대한 세부 정보입니다. • 검색 상자 - 판정 검색 상자와 동일합니다. • 파일 형식 - 판정 파일 형식과 동일합니다. • 각 파일 유형에 대해 분석을 위해 제출된 총 파일 수, 분석된 총 파일 수 및 분석 보류 중인 수가 각 탭에 표시됩니다.
연결된 방화벽 > 보기	
보기	클러스터 또는 어플라이언스에 연결된 방화벽에 대한 정보를 봅니다. 개별 어플라이언스(**Panorama** > **Managed WildFire Appliances**)만 보거나 클러스터 통계(**Panorama** > **Managed WildFire** 클러스터)만 볼 수 있습니다. • 어플라이언스 - (독립형 어플라이언스 보기 전용) 어플라이언스 일련번호입니다. • 클러스터 - (클러스터 보기만 해당) 클러스터 이름으로 다른 클러스터를 선택하여 볼 수도 있습니다. • 새로 고침 - 디스플레이를 새로 고칩니다.
샘플 탭 등록 및 제출	등록된 탭에는 방화벽이 샘플을 제출하는지의 여부와 관계없이 클러스터 또는 어플라이언스에 등록된 방화벽에 대한 정보가 표시됩니다. 샘플 제출 탭에는 WildFire 클러스터 또는 어플라이언스에 샘플을 활발하게 제출하는 방화벽에 대한 정보가 표시됩니다. 이러한 탭에 표시되는 정보 유형과 정보를 필터링하는 방법은 다음 두 가지 모두 유사합니다. • 검색 상자 - 방화벽 목록을 필터링할 검색어를 입력합니다. 검색 상자는 목록의 방화벽(항목) 수를 나타냅니다. 검색어를 입력한 후 필터를 적용하거나(→) 필터를 지우 고(✕) 다른 용어 집합을 입력합니다.

관리되는 **WildFire** 정보	설명
	• **S/N** - 방화벽의 일련번호입니다. • **IP** 주소 - 방화벽의 IP 주소입니다. • 모델 - 방화벽의 모델 번호입니다. • 소프트웨어 버전 - 방화벽에 설치되어 실행 중인 소프트웨어 버전입니다.

관리형 WildFire 클러스터 및 어플라이언스 관리

Panorama > **Managed WildFire Clusters**를 선택한 다음 클러스터를 선택하여 관리하거나 WildFire 어플라이언스(**Panorama** > **Managed WildFire** 어플라이언스)를 선택하여 독립 실행형 어플라이언스를 관리합니다. **Panorama** > **Managed WildFire Cluster** 보기에는 클러스터 노드(클러스터의 구성원인 WildFire 어플라이언스)와 독립 실행형 어플라이언스가 나열되어 클러스터에 사용 가능한 어플라이언스를 추가할 수 있습니다. 클러스터가 노드를 관리하기 때문에 클러스터 노드를 선택하면 제한된 관리 기능만 제공됩니다.

별도의 언급이 없는 한 다음 표의 설정 및 설명은 WildFire 클러스터와 WildFire 독립 실행형 어플라이언스 모두에 적용됩니다. 클러스터 또는 어플라이언스에 이전에 구성된 정보가 미리 채워집니다. 먼저 Panorama의 정보에 대한 변경 사항 및 추가 사항을 커밋한 다음 새 구성을 어플라이언스에 푸시해야 합니다.

세팅	설명
일반 탭	
이름	클러스터 또는 어플라이언스 이름 또는 어플라이언스 일련번호입니다.
DNS 활성화 (WildFire 클러스터만 해당)	클러스터에 대해 **DNS** 서비스를 활성화합니다.
방화벽 등록 대상	방화벽을 등록하는 도메인 이름입니다. 형식은 **`wfpc.service.<`**클러스터 이름**`>.<`**도메인**`>`**이어야 합니다. 예를 들어, 기본 도메인 이름은 **`wfpc.service.mycluster.paloaltonetworks.com`**입니다.
콘텐츠 업데이트 서버	**Content Update Server** 위치를 입력하거나 기본 **`wildfire.paloaltonetworks.com`**을 사용하여 클러스터 또는 어플라이언스가 Content Delivery Network 인프라에서 가장 가까운 서버에서 콘텐츠 업데이트를 수신하도록 합니다. 글로벌 클라우드에 연결하면 로컬 위협 분석에만 의존하는 대신 클라우드에 연결된 모든 소스의 위협 분석을 기반으로 서명 및 업데이트에 액세스할 수 있는 이점이 있습니다.

세팅	설명
서버 ID 확인	서버 **ID**를 확인하여 인증서의 CN(일반 이름)을 서버의 IP 주소 또는 FQDN과 일치시켜 업데이트 서버의 ID를 확인합니다.
WildFire Cloud Server	클러스터 또는 어플라이언스가 가장 가까운 서버에 정보를 보낼 수 있도록 전역 **WildFire** 클라우드 서버 위치를 입력하거나 기본 **`wildfire.paloaltonetworks.com`**을 사용하십시오. 정보를 보낼지의 여부와 글로벌 클라우드(**WildFire Cloud Services**)로 보낼 정보 유형을 선택할 수 있습니다.
샘플 분석 이미지	샘플 분석에 사용할 클러스터 또는 어플라이언스의 VM 이미지를 선택합니다(기본값은 vm-5). 악성코드 테스트 파일(WildFire API)을 받아 샘플 분석 결과를 확인할 수 있습니다.
WildFire Cloud Services	클러스터 또는 어플라이언스가 글로벌 WildFire 클라우드 서버에 연결된 경우 분석 데이터 보내기, 악성 샘플 보내기, 글로벌 클라우드에 진단 보내기 또는 이 세 가지의 조합을 선택할 수 있습니다. 글로벌 클라우드에서 판정 조회를 수행할지의 여부를 선택할 수도 있습니다. 정보를 글로벌 클라우드로 보내면 공유 정보가 악성 트래픽을 식별하고 네트워크를 통과하는 것을 방지하는 모든 어플라이언스의 능력이 향상되기 때문에 WildFire 사용자 커뮤니티 전체에 이익이 됩니다.
샘플 데이터 보존	양성 또는 그레이웨어 샘플 및 악성 샘플을 보관하는 기간(일): • 양성/그레이웨어 샘플 - 범위는 1~90입니다. 기본값은 14입니다. • 악성 샘플 - 최소값은 1이고 최대값은 없습니다(무한). 기본값은 미규정입니다.
분석 환경 서비스	환경 네트워킹을 사용하면 가상 머신이 인터넷과 통신할 수 있습니다. 익명 네트워킹을 선택하여 네트워크 통신을 익명으로 만들 수 있지만 익명 네트워킹을 활성화하려면 먼저 환경 네트워킹을 선택해야 합니다. 다른 네트워크 환경은 더 많은 문서를 분석해야 하는지 또는 더 많은 실행 파일을 분석해야 하는지에 따라 다른 유형의 분석 로드를 생성합니다. 환경 요구 사항에 따라 실행 파일 또는 문서에 더 많은 리소스를 할당하도록 선호 분석 환경을 구성할 수 있습니다. 기본 할당은 실행 파일과 문서 간에 균형을 이룹니다. 사용 가능한 리소스의 양은 클러스터에 있는 WildFire 노드 수에 따라 다릅니다.
서명 생성	클러스터 또는 어플라이언스가 AV, DNS, URL 또는 세 가지 조합에 대한 서명을 생성하도록 할지 선택합니다.

세팅	설명
어플라이언스 탭	
호스트네임 (독립형 WildFire 어플라이언스만 해당)	WildFire 어플라이언스의 호스트네임을 입력합니다.
Panorama 서버	어플라이언스 또는 클러스터를 관리하는 기본 Panorama의 IP 주소 또는 FQDN을 입력합니다.
Panorama 서버 2	어플라이언스 또는 클러스터를 관리하는 백업 Panorama의 IP 주소 또는 FQDN을 입력합니다.
도메인	어플라이언스 클러스터 또는 어플라이언스의 도메인 이름을 입력합니다.
기본 DNS 서버	기본 DNS 서버의 IP 주소를 입력합니다.
보조 DNS 서버	보조 DNS 서버의 IP 주소를 입력합니다.
시간대	클러스터 또는 어플라이언스에 사용할 시간대를 선택하십시오.
위도 (독립형 WildFire 어플라이언스만 해당)	WildFire 어플라이언스의 위도를 입력합니다.
경도 (독립형 WildFire 어플라이언스만 해당)	WildFire 어플라이언스의 경도를 입력합니다.
기본 NTP 서버	기본 NTP 서버의 IP 주소를 입력하고 인증 유형을 없음(기본값), 대칭 키 또는 자동 키로 설정합니다. 인증 유형을 대칭 키로 설정하면 4개의 필드가 더 표시됩니다. • 키 **ID** - 인증 키 ID를 입력합니다. • 알고리즘 - 인증 알고리즘을 **SHA1** 또는 **MD5**로 설정합니다. • 인증 키 - 인증 키를 입력합니다. • 인증 키 확인 - 인증 키를 다시 입력하여 확인합니다.
보조 NTP 서버	보조 NTP 서버의 IP 주소를 입력하고 인증 유형을 없음(기본값), 대칭 키 또는 자동 키로 설정합니다.

세팅	설명
	인증 유형을 대칭 키로 설정하면 4개의 필드가 더 표시됩니다. • 키 **ID** - 인증 키 ID를 입력합니다. • 알고리즘 - 인증 알고리즘을 **SHA1** 또는 **MD5**로 설정합니다. • 인증 키 - 인증 키를 입력합니다. • 인증 키 확인 - 인증 키를 다시 입력하여 확인합니다.
로그인 배너	사용자가 클러스터 또는 어플라이언스에 로그인할 때 표시되는 배너 메시지를 입력하십시오.
로깅 탭(시스템 탭 및 구성 탭 포함)	
추가	다음을 포워딩할 로그 포워딩 프로파일(**Panorama** > **Managed WildFire Clusters** > **<*cluster*>** > **Logging** > **System** or **Panorama** > **Managed WildFire Clusters** > **<*cluster*>** > **Logging** > **Configuration**) 추가: • 시스템 또는 구성 로그는 SNMP 트랩 수신기에 대한 SNMP 트랩으로 기록됩니다. • syslog 서버에 대한 syslog 메시지. • 이메일 서버에 이메일 알림. • HTTP 서버에 대한 HTTP 요청. 다른 로그 유형은 지원되지 않습니다(디바이스 > 로그 설정 참조). 로그 포워딩 프로파일은 포워딩할 로그와 대상 서버를 지정합니다. 각 프로파일에 대해 다음을 완료합니다. • 이름 - 영숫자와 밑줄로만 구성된 로그 설정(최대 31자)을 식별하는 이름으로 공백과 특수 문자는 허용되지 않습니다. • 필터 - 기본적으로 Panorama 어플라이언스는 지정된 프로파일의 모든 로그를 포워딩합니다. 로그의 하위 집합을 포워딩하려면 필터(**severity eq critical**, **severity eq high**, **severity eq informational**, **severity eq low**, or **severity eq medium**)를 선택하거나 필터 빌더를 선택하여 새 필터를 만듭니다. • 설명 - 프로파일의 목적을 설명하는 설명(최대 1,023자)을 입력합니다.
추가 > 필터 > 필터 빌더	필터 빌더를 사용하여 새 로그 필터를 만듭니다. 필터 만들기를 선택하여 필터를 구성하고 새 필터의 각 쿼리에 대해 다음 설정을 지정한 다음 쿼리 추가: • 커넥터 - 커넥터 논리(**and** 또는 **or**)를 선택합니다. 무효를 적용하려면 부정을 선택합니다. 예를 들어, 로그 설명의 하위 집합을 포워딩하지 않으려

세팅	설명
	면 특성으로 설명을 선택한 다음 연산자로 포함을 선택하고 값으로 설명 문자열을 입력하여 포워딩하지 않으려는 설명을 식별합니다. • 속성 - 로그 속성을 선택합니다. 옵션은 로그 유형에 따라 다릅니다. • 연산자 - 속성 적용 방법(예: 포함)을 결정하는 기준을 선택합니다. 옵션은 로그 유형에 따라 다릅니다. • 값 - 일치시킬 속성 값을 지정합니다. • 추가 - 새 필터를 추가합니다. 필터와 일치하는 로그를 표시하거나 내보내려면 필터링된 로그 보기를 선택합니다. • 일치하는 로그 항목을 찾기 위해 검색 필드에 IP 주소 또는 시간 범위와 같은 아티팩트를 추가할 수 있습니다. • 로그를 보려는 기간을 선택합니다. 지난 **15**분, 지난 **1**시간, 지난 **6**시간, 지난 **12**시간, 지난 **24**시간, 지난 **7**일, 지난 **30**일 또는 모두(기본값). • 기간 드롭다운 오른쪽에 있는 옵션을 사용하여 필터를 적용, 지우기, 추가, 저장 및 로드합니다. • 필터 적용(→) - 검색 필드의 용어와 일치하는 로그 항목을 표시합니다. • 필터 지우기(×) - 필터 필드를 지웁니다. • 새 필터 추가(⊕) - 새 검색 기준을 정의합니다(필터 생성과 유사한 로그 필터 추가로 이동). • 필터 저장( ) - 필터 이름을 입력한 다음 확인을 클릭합니다. • 저장된 필터 사용( ) - 필터 필드에 저장된 필터를 추가합니다. • **CSV**로 내보내기( ) - 로그를 CSV 형식 보고서로 내보낸 다음 파일을 다운로드합니다. 기본적으로 보고서에는 최대 2,000줄의 로그가 포함됩니다. 생성된 CSV 보고서에 대한 줄 제한을 변경하려면 **Device** > **Setup** > **Management**

세팅	설명

	> 로깅 및 보고 설정 > 로그 내보내기 및 보고를 선택한 다음 **CSV** 내보내기의 새 최대 행 값을 입력합니다.
	
	페이지당 표시되는 항목의 수와 순서를 변경할 수 있으며 페이지 왼쪽 하단에 있는 페이징 컨트롤을 사용하여 로그 목록을 탐색할 수 있습니다. 로그 항목은 10페이지 블록으로 검색됩니다.
	
	• 페이지 기준 - 드롭다운을 사용하여 페이지당 로그 항목 수(**20**, **30**, **40**, **50**, **75** 또는 **100**)를 변경합니다.
	• **ASC** 또는 **DESC** - 결과를 오름차순으로 정렬하려면 **ASC**를 선택한 다음(가장 오래된 로그 항목 먼저), **DESC**를 선택하여 내림차순으로 정렬합니다(최신 로그 항목 먼저). 기본값은 **DESC**입니다.
	• 호스트네임 확인 - 외부 IP 주소를 도메인 이름으로 확인하려면 선택합니다.
	• 정책 작업 강조 표시 - 작업을 지정하고 작업과 일치하는 로그 항목을 강조 표시하도록 선택합니다. 필터링된 로그는 다음 색상으로 강조 표시됩니다.
	  • 녹색 - 허용
	  • 노란색 - 계속 또는 무시
	  • 빨간색 - 거부, 삭제, drop-icmp, rst-client, reset-server, reset-both, block-continue, block-override, block-url, drop-all, 싱크홀

삭제	시스템 또는 구성 로그 목록에서 제거할 로그 포워딩 설정을 선택한 다음 삭제합니다.
인증 탭	
인증 프로파일	구성된 인증 프로파일을 선택하여 WildFire 어플라이언스 또는 Panorama 관리자의 로그인 자격 증명을 확인하는 인증 서비스를 정의합니다.
실패한 시도	WildFire 어플라이언스가 관리자를 잠그기 전에 CLI에서 허용하는 로그인 시도 실패 횟수를 입력합니다(범위는 0~10, 기본값은 10). 로그인 시도를 제한하면 무차별 대입 공격으로부터 WildFire 어플라이언스를 보호하는 데 도움이 됩니다. 0 값은 무제한 로그인 시도를 지정합니다.

세팅	설명
	실패한 시도를 *0* 이외의 값으로 설정하고 잠금 시간을 *0*으로 두면 다른 관리자가 잠긴 관리자의 잠금을 수동으로 해제할 때까지 관리자가 무기한 잠깁니다. 다른 관리자가 생성되지 않은 경우 *Panorama*에서 실패한 시도 및 잠금 시간 설정을 재구성하고 구성 변경 사항을 *WildFire* 어플라이언스에 푸시해야 합니다. 관리자가 잠기지 않도록 하려면 실패한 시도 및 잠금 시간 모두에 대해 기본값(**0**)을 사용하십시오. 입력 오류가 발생한 경우 적절한 재시도 횟수를 수용할 수 있도록 실패한 시도 횟수를 *5* 이하로 설정하고 악성 시스템이 *WildFire* 어플라이언스에 로그인하기 위해 무차별 대입 방식을 시도하는 것을 방지합니다.
잠금 시간(분)	실패한 시도 제한(범위는 0~60, 기본값은 5)에 도달한 후 WildFire 어플라이언스가 관리자의 CLI 액세스를 잠그는 시간(분)을 입력합니다. 0 값은 다른 관리자가 계정을 수동으로 잠금 해제할 때까지 잠금이 적용됨을 의미합니다. 실패한 시도를 *0* 이외의 값으로 설정하고 잠금 시간을 *0*으로 두면 다른 관리자가 잠긴 관리자의 잠금을 수동으로 해제할 때까지 관리자가 무기한 잠깁니다. 다른 관리자가 생성되지 않은 경우 *Panorama*에서 실패한 시도 및 잠금 시간 설정을 재구성하고 구성 변경 사항을 *WildFire* 어플라이언스에 푸시해야 합니다. 관리자가 잠기지 않도록 하려면 실패한 시도 및 잠금 시간 모두에 대해 기본값(**0**)을 사용하십시오. 악의적인 행위자의 지속적인 로그인 시도를 방지하려면 잠금 시간을 최소 *30*분으로 설정하십시오.
유휴 타임아웃(분)	관리자가 자동으로 로그아웃되기 전에 CLI에서 활동이 없는 최대 시간(분)을 입력합니다(범위는 0~1,440, 기본값은 없음). 값이 0이면 비활성 상태가 자동 로그아웃을 트리거하지 않음을 의미합니다. 관리자가 세션을 열어 둔 경우 권한이 없는 사용자가 *WildFire* 어플라이언스에 액세스하지 못하도록 하려면 유휴 시간 제한을 *10*분으로 설정하십시오.
최대 세션 수	관리자가 동시에 열 수 있는 활성 세션 수를 입력합니다. 기본값은 0이며, 이는 WildFire 어플라이언스가 동시에 활성 세션을 무제한으로 가질 수 있음을 의미합니다.

세팅	설명
최대 세션 시간	관리자가 자동으로 로그아웃되기 전까지 로그인할 수 있는 시간(분)을 입력합니다. 기본값은 0이며, 이는 관리자가 유휴 상태에서도 무기한으로 로그인할 수 있음을 의미합니다.
로컬 관리자	WildFire 어플라이언스에 대한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 WildFire 어플라이언스에 고유하며 이 페이지에서 관리됩니다(**Panorama** > **Managed WildFire Appliances** > **Authentication**).
Panorama 관리자	Panorama에 구성된 기존 관리자를 가져옵니다. 이러한 관리자는 Panorama에서 생성되어 WildFire 어플라이언스로 가져옵니다.
클러스터링 탭(관리형 WildFire 클러스터만 해당) 및 인터페이스 탭(관리형 WildFire 어플라이언스만 해당) 인터페이스를 관리하려면 Panorama에 어플라이언스를 추가하고 노드 인터페이스를 관리하려면 클러스터에 어플라이언스를 추가해야 합니다.	
기구 (클러스터링 탭만 해당)	클러스터 노드를 선택하여 해당 노드의 어플라이언스 및 인터페이스 탭에 액세스합니다. 어플라이언스 탭 노드 정보는 미리 채워져 있으며 호스트네임을 제외하고 구성할 수 없습니다. 인터페이스 탭에는 노드 인터페이스가 나열됩니다. 다음에 설명된 대로 관리할 인터페이스를 선택합니다. • 인터페이스 이름 관리 • 인터페이스 이름 분석 환경 네트워크 • 인터페이스 이름 이더넷2 • 인터페이스 이름 이더넷3
인터페이스 이름 관리	관리 인터페이스는 Ethernet0입니다. 관리 인터페이스 설정을 구성하거나 봅니다. • 속도 및 이중 - 자동 협상(기본값), **10Mbps** 반이중, **10Mbps** 전이중, **100Mbps** 반이중, **100Mbps** 전이중, **1Gbps** 반이중 또는 **1Gbps** 전이중을 선택합니다. • **IP** 주소 - 인터페이스 IP 주소를 입력합니다. • 넷마스크 - 인터페이스 넷마스크를 입력합니다. • 기본 게이트웨이 - 기본 게이트웨이의 IP 주소를 입력합니다. • **MTU** - MTU를 바이트 단위로 입력합니다(범위는 576~1,500, 기본값은 1,500). • 관리 서비스 - 지원하려는 관리 서비스를 활성화합니다. **Ping**, **SSH** 및 **SNMP** 서비스를 지원할 수 있습니다.

세팅	설명

	프록시 서버를 사용하여 인터넷에 연결하는 경우 프록시 설정을 구성합니다.
	• 서버 - 프록시 서버의 IP 주소입니다.
	• 포트 - Panorama 디바이스 요청을 수신 대기하도록 프록시 서버에 구성된 포트 번호입니다.
	• 사용자 - 인증을 위해 프록시 서버에 구성된 사용자명입니다.
	• 암호 및 암호 확인 - 인증을 위해 프록시 서버에 구성된 암호입니다.
	• 클러스터링 서비스(클러스터링 탭만 해당) - HA 서비스를 선택합니다.
	  • **HA** - 클러스터에 두 개의 컨트롤러 노드가 있는 경우 두 컨트롤러 노드 모두에서 관리 정보를 사용할 수 있도록 관리 인터페이스를 HA 인터페이스로 구성할 수 있습니다. 구성 중인 클러스터 노드가 기본 컨트롤러 노드인 경우 **HA** 인터페이스로 표시합니다.
	  WildFire 어플라이언스 이더넷 인터페이스를 사용하는 방법에 따라 Etherent2 또는 Ethernet3을 각각 기본 및 백업 컨트롤러 노드에서 HA 및 HA 백업 인터페이스로 구성할 수 있습니다. 예를 들어 이더넷 2를 HA 및 HA 백업 인터페이스로 사용할 수 있습니다. HA 및 HA 백업 인터페이스는 기본 및 백업 컨트롤러 노드에서 동일한 인터페이스(관리, 이더넷2 또는 이더넷3)여야 합니다. Ethernet1을 HA/HA 백업 인터페이스로 사용할 수 없습니다.
	  • **HA** 백업 - 구성 중인 클러스터 노드가 백업 컨트롤러 노드인 경우 **HA** 백업 인터페이스로 표시합니다.
	인터페이스에서 허용되는 IP 주소를 지정합니다.
	• 검색 상자 - 허용된 IP 주소 목록을 필터링할 검색어를 입력합니다. 검색 상자는 목록의 IP 주소(항목) 수를 표시하므로 목록의 길이를 알 수 있습니다. 검색어를 입력한 후 필터를 적용하거나(→)
	필터를 지우고(×)
	다른 용어 집합을 입력합니다.
	• 추가 - 허용된 IP 주소를 추가합니다.
	• 삭제 - 관리 인터페이스 액세스에서 제거할 IP 주소를 선택한 다음 삭제합니다.

인터페이스 이름 분석 환경 네트워크	WildFire 어플라이언스 클러스터 또는 독립형 WildFire 어플라이언스 분석 환경 네트워크 인터페이스(Ethernet1, VM 인터페이스라고도 함)에 대한 설정을 구성합니다.

세팅	설명
	• 속도 및 이중 - 자동 협상(기본값), **10Mbps** 반이중, **10Mbps** 전이중, **100Mbps** 반이중, **100Mbps** 전이중, **1Gbps** 반이중 또는 **1Gbps** 전이중으로 설정합니다. • **IP** 주소 - 인터페이스 IP 주소를 입력합니다. • 넷마스크 - 인터페이스 넷마스크를 입력합니다. • 기본 게이트웨이 - 기본 게이트웨이의 IP 주소를 입력합니다. • **MTU** - MTU를 바이트 단위로 입력합니다(범위는 576~1,500, 기본값은 1,500). • **DNS** 서버 - DNS 서버 IP 주소를 입력합니다. • 링크 상태 - 인터페이스 링크 상태를 **Up** 또는 **Down**으로 설정합니다. • 관리 서비스 - 인터페이스가 핑 서비스를 지원하도록 하려면 **Ping**을 활성화합니다. 인터페이스에서 허용되는 IP 주소를 지정합니다. • 검색 상자 - 허용된 IP 주소 목록을 필터링할 검색어를 입력합니다. 검색 상자는 목록의 IP 주소(항목) 수를 표시하므로 목록의 길이를 알 수 있습니다. 검색어를 입력한 후 필터를 적용하거나(→) 필터를 지우고(×) 다른 용어 집합을 입력합니다. • 추가 - 허용된 IP 주소를 추가합니다. • 삭제 - 관리 인터페이스 액세스에서 제거할 IP 주소를 선택한 다음 삭제를 선택합니다.
인터페이스 이름 Ethernet2 인터페이스 이름 Ethernet3	Ethernet2 및 Ethernet3 인터페이스에 대해 동일한 매개변수를 설정할 수 있습니다. • 속도 및 이중 - 자동 협상(기본값), **10Mbps** 반이중, **10Mbps** 전이중, **100Mbps** 반이중, **100Mbps** 전이중, **1Gbps** 반이중 또는 **1Gbps** 전이중으로 설정합니다. • **IP** 주소 - 인터페이스 IP 주소를 입력합니다. • 넷마스크 - 인터페이스 넷마스크를 입력합니다. • 기본 게이트웨이 - 기본 게이트웨이의 IP 주소를 입력합니다. • **MTU** - MTU를 바이트 단위로 입력합니다(범위는 576~1,500, 기본값은 1,500).

세팅	설명

	• 관리 서비스 - 인터페이스가 핑 서비스를 지원하도록 하려면 **Ping**을 활성화합니다.
	• 클러스터링 서비스 - 클러스터 서비스 선택:
	  • **HA** - 클러스터에 두 개의 컨트롤러 노드가 있는 경우 두 컨트롤러 노드 모두에서 관리 정보를 사용할 수 있도록 이더넷2 또는 이더넷3 인터페이스를 HA 인터페이스로 구성할 수 있습니다. 구성 중인 클러스터 노드가 기본 컨트롤러 노드인 경우 **HA** 인터페이스로 표시합니다.
	  WildFire 어플라이언스 이더넷 인터페이스를 사용하는 방법에 따라 관리 인터페이스(Ethernet1)를 기본 및 백업 컨트롤러 노드에서 각각 HA 및 HA 백업 인터페이스로 구성할 수 있습니다. HA 및 HA 백업 인터페이스는 기본 및 백업 컨트롤러 노드에서 동일한 인터페이스(관리, 이더넷2 또는 이더넷3)여야 합니다. Ethernet1을 HA/HA 백업 인터페이스로 사용할 수 없습니다.
	  • **HA** 백업 - 구성 중인 클러스터 노드가 백업 컨트롤러 노드인 경우 **HA** 백업 인터페이스로 표시합니다.
	  • 클러스터 관리 - 이더넷2 또는 이더넷3 인터페이스를 클러스터 전체 관리 및 통신에 사용되는 인터페이스로 구성합니다.

역할 (클러스터링 탭만 해당)	클러스터에 구성원 어플라이언스가 있는 경우 어플라이언스 역할은 컨트롤러, 컨트롤러 백업 또는 작업자가 될 수 있습니다. 컨트롤러 또는 백업 컨트롤러를 선택하여 클러스터의 어플라이언스에서 각 역할에 사용되는 WildFire 어플라이언스를 변경합니다. 컨트롤러를 변경하면 역할 변경 중에 데이터가 손실됩니다.
검색 (클러스터링 탭만 해당)	클러스터링 탭에는 클러스터의 WildFire 어플라이언스 노드가 나열됩니다. Panorama 디바이스가 이미 관리하고 있는 독립형 WildFire 어플라이언스를 보고 추가하려면 검색을 합니다. • 검색 상자 - 노드 목록을 필터링할 검색어를 입력합니다. 검색 상자는 목록의 어플라이언스(항목) 수를 표시하므로 목록의 길이를 알 수 있습니다. 검색어를 입력한 후 필터를 적용하거나(→) 필터를 지우고(×) 다른 용어 집합을 입력합니다. • 노드 추가 - 클러스터에 (⊕) 노드를 추가합니다.

세팅	설명
	클러스터에 추가하는 첫 번째 WildFire 어플라이언스는 자동으로 컨트롤러 노드가 됩니다. 추가하는 두 번째 WildFire 어플라이언스는 자동으로 컨트롤러 백업 노드가 됩니다. 클러스터에 최대 20개의 WildFire 어플라이언스를 추가할 수 있습니다. 컨트롤러 및 컨트롤러 백업 노드를 추가한 후 추가되는 모든 노드는 작업자 노드입니다.
삭제 (클러스터링 탭만 해당)	어플라이언스 목록에서 어플라이언스를 하나 이상 선택한 다음 클러스터에서 삭제합니다. 클러스터에 두 개의 컨트롤러 노드가 있는 경우에만 컨트롤러 노드를 제거할 수 있습니다.
컨트롤러 관리 (클러스터링 탭만 해당)	컨트롤러 관리를 선택하여 클러스터에 속한 WildFire 어플라이언스 노드에서 컨트롤러 및 컨트롤러 백업을 지정합니다. 현재 컨트롤러 노드와 백업 컨트롤러 노드가 기본적으로 선택됩니다. 백업 컨트롤러 노드는 기본 컨트롤러 노드와 동일한 노드일 수 없습니다.
통신 탭	

보안 서버 통신 사용자 지정	• **SSL/TLS** 서비스 프로파일 - 드롭다운에서 SSL/TLS 서비스 프로파일을 선택합니다. 이 프로파일은 연결된 디바이스가 WildFire와 통신하는 데 사용하는 인증서 및 지원되는 SSL/TLS 버전을 정의합니다.
	• 인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다. 이 인증서 프로파일은 인증서 해지 확인 동작과 클라이언트가 제공하는 인증서 체인을 인증하는 데 사용되는 루트 CA를 정의합니다.
	• 사용자 지정 인증서만 - 활성화된 경우 WildFire는 연결 디바이스와의 인증을 위해 사용자 지정 인증서만 수락합니다.
	• 인증 목록 확인 - WildFire에 연결하는 클라이언트 디바이스가 인증 목록과 비교하여 확인됩니다. 기기는 승인을 받으려면 목록의 한 항목과만 일치해야 합니다. 일치하는 항목이 없으면 디바이스가 인증되지 않은 것입니다.
	• 인증 목록 - 인증 목록을 추가하고 다음 필드를 완성하여 클라이언트 디바이스 인증 기준을 설정합니다. 인증 목록은 최대 16개 항목을 지원합니다.
	  • 식별자 - 제목 또는 제목 대체를 선택합니다. 권한 부여 식별자로 이름을 지정합니다.
	  • 유형 - 제목 대체를 선택한 경우, 이름을 식별자로 지정한 다음 **IP**, 호스트 이름 또는 전자 메일을 식별자 유형으로 선택합니다. 주제를 선택한 경우 공통 이름은 식별자 유형입니다.
	  • 값 - 식별자 값을 입력합니다.

세팅	설명

보안 클라이언트 통신	보안 클라이언트 통신을 사용하면 WildFire가 구성된 사용자 지정 인증서(사전 정의된 기본 인증서 대신)를 사용하여 다른 WildFire 어플라이언스와의 SSL 연결을 인증합니다.
	• 사전 정의됨 - (기본값) 구성된 디바이스 인증서가 없습니다. WildFire는 사전 정의된 기본 인증서를 사용합니다.
	• 로컬 - WildFire는 로컬 디바이스 인증서와 방화벽에서 생성되거나 기존 엔터프라이즈 PKI 서버에서 불러온 해당 개인 키를 사용합니다.
	  • 자격증: 로컬 디바이스 인증서를 선택합니다.
	  • 인증서 프로파일: 드롭다운에서 인증서 프로파일을 선택합니다.
	• **SCEP** - WildFire는 SCEP(Simple Certificate Enrollment Protocol) 서버에서 생성한 디바이스 인증서와 개인 키를 사용합니다.
	  • **SCEP** 프로파일: 드롭다운에서 SCEP 프로파일을 선택합니다.
	  • 인증서 프로파일: 드롭다운에서 인증서 프로파일을 선택합니다.

보안 클러스터 통신	사용을 선택하여 WildFire 어플라이언스 간의 통신을 암호화합니다. 기본 인증서는 사전 정의된 인증서 유형을 사용합니다. 사용자 정의 사용자 정의 인증서를 사용하려면 보안 서버 통신 사용자 정의를 구성하고 사용자 정의 인증서만을 활성화해야 합니다.

Panorama > 방화벽 클러스터

- **Panorama** > 방화벽 클러스터

방화벽 클러스터 아래의 Panorama 웹 인터페이스에서 CN 시리즈 방화벽 클러스터 요약 및 모니터링 정보를 봅니다.

(CN 시리즈 방화벽에서만 사용 가능) **Panorama** > 관리자 역할 > 웹 **UI** 목록에서, 방화벽 클러스터를 선택한 다음 활성화를 클릭하여 방화벽 클러스터에 액세스합니다. Panorama에 방화벽 클러스터를 추가한 후 웹 인터페이스를 사용하여 CN 시리즈 방화벽 클러스터의 세부 정보를 확인합니다.

방화벽 클러스터에서 클러스터 세부 정보를 보려면 디바이스 > 플러그인에서 클러스터링 플러그인을 설치해야 합니다.

요약 보기

지난 5분 동안 방화벽에 의해 캡처된 CN 시리즈 클러스터에 대한 정보를 봅니다. 최신 정보를 로드하려면 새로고침 버튼을 클릭합니다.

필드	설명
클러스터 이름	방화벽 클러스터의 이름입니다.
소프트웨어 버전	PAN-OS 버전입니다.
클러스터에서 사용되는 플러그인	클러스터에서 사용되는 플러그인 목록입니다. *CN* 시리즈 방화벽 플러그인만 지원됩니다.
템플릿 스택(template stack)	클러스터와 연결된 템플릿 스택의 이름입니다.
디바이스 그룹	클러스터와 연결된 디바이스 그룹의 이름입니다.
클러스터 상태	클러스터가 영향을 받았는지 여부를 표시합니다.
클러스터 유형	클러스터 유형입니다.

필드	설명
	CN 시리즈 방화벽 클러스터 유형만 지원됩니다.
영향을 받는 구성원	영향을 받는 클러스터 구성원 수 및 해당 이름입니다.
시스템 로그 세부 정보	시스템 이벤트의 세부 정보를 표시합니다.
특정 오류	클러스터의 특정 오류 목록입니다. 링크를 클릭하면 모니터 > 로그 > 시스템 아래에서 로그 보기를 수행할 수 있는 오류에 대한 자세한 내용을 볼 수 있습니다.
포드 이름	포드의 이름입니다.
CPU 수	사용된 CPU 수입니다.

모니터링

CN 시리즈 방화벽 클러스터 상태 정보를 봅니다.

필드	설명
관리 소프트웨어 클러스터	방화벽 클러스터를 선택합니다. *CN* 시리즈 방화벽 클러스터 유형만 지원됩니다.
영향을 받음	영향을 받는 방화벽 클러스터 목록입니다. • **CN-Clusters** - 영향을 받는 CN 시리즈 방화벽 클러스터의 수입니다. • 영향을 받는 클러스터 - 영향을 받는 클러스터 목록을 표시합니다. 상호 연결 상태 및 클러스터 사용률 대시보드에서 클러스터에 대한 자세한 정보를 보려면 클릭합니다.
OK	영향을 받지 않는 방화벽 클러스터 목록입니다. • **CN** 클러스터 - 영향을 받지 않는 CN 시리즈 방화벽 클러스터의 수입니다. • 영향을 받는 클러스터 - 영향을 받지 않는 클러스터 목록을 표시합니다. 상호 연결 상태 및 클러스터 사용률 대시보드에서 클러스터에 대한 자세한 정보를 보려면 클릭합니다.

필드	설명

상호 연결 상태	선택한 시간 기간에 대한 클러스터 상호 연결 세부 정보를 봅니다.
	다음 세부 정보를 보려면 마지막 **5**분을 선택합니다.
	• 클러스터 이름 - 방화벽 클러스터의 이름입니다.
	• 클러스터 유형 - 클러스터 유형입니다.
	CN 시리즈 방화벽 클러스터 유형만 지원됩니다.
	• 클러스터 생성 시간 - 클러스터 생성 시간입니다.
	• 현재 클러스터 상태 - 클러스터가 영향을 받았는지 여부를 표시합니다.
	  • 현재 클러스터 세부 정보 - 영향을 받는 클러스터에 대한 세부 정보를 보려면 현재 클러스터 상태 링크를 클릭합니다.
	• 클러스터 상호 연결 상태 - 클러스터가 영향을 받았는지 여부를 표시합니다.
	  • 현재 클러스터 세부 정보 - 영향을 받는 클러스터에 대한 세부 정보를 보려면 현재 상호 연결 상태 링크를 클릭합니다.
	• 트래픽 상호 연결 - 트래픽 상호 연결 상태입니다.
	• 외부 연결 - 외부 연결 상태입니다.
	• 영향을 받은 링크 - 영향을 받은 링크의 수입니다.
	• 관리 연결 - 관리 연결 수입니다.
	• 영향을 받는 클러스터 구성원 - 영향을 받는 클러스터 구성원 목록입니다.
	• 타임 스탬프 고해상도 가동 시간-가동 시간 타임스탬프입니다.
	• 타임 스탬프 고해상도 다운타임-다운타임 타임스탬프입니다.
	다른 시간 프레임을 선택하면 다음 정보만 표시됩니다.
	• 클러스터 이름
	• 클러스터 유형
	• 클러스터 생성 시간
	• 현재 클러스터 상태
	• 클러스터 상호 연결 상태
	• 트래픽 상호 연결
	• 외부 연결

클러스터 활용	전체 방화벽 클러스터, 메모리 및 데이터 사용률을 봅니다.

필드	설명
	• 클러스터 이름 - 방화벽 클러스터의 이름입니다. • 클러스터 세부 정보 - 클러스터 이름 링크를 클릭하면 선택한 클러스터의 처리량, 메모리 및 데이터 사용률 세부 정보를 볼 수 있습니다. • 클러스터 유형 - 클러스터 유형입니다.  *CN* 시리즈 방화벽 클러스터 유형만 지원됩니다. • 클러스터 상태 - 클러스터의 상태를 표시합니다. • 클러스터 처리량**(gbps)** - 전체 방화벽 클러스터(Gbps)입니다. • **CPS** - 초당 연결 수입니다. • 세션 수**(**세션**)** - 세션 수입니다. • 상태 임계값 내의 평균 데이터 영역**(%)** - 평균 데이터 영역 임계값(백분율)입니다. • 관리 플레인 **CPU(%)** - 관리 플레인 CPU 사용률(백분율)입니다. • 관리 플레인 메모리**(%)** - 관리 플레인 메모리 사용률(백분율)입니다. • 로깅 속도**(**로그/초**)** - 클러스터에서 로그가 생성되는 속도입니다. • **DP** 자동 크기 조정 상태 - 데이터 플레인 자동 크기 조정 세부 정보입니다.

Panorama > 관리자

Panorama 관리자 계정을 만들고 관리하려면 **Panorama** > 관리자를 선택합니다.

운용 관리자 역할이 있는 관리자로 Panorama에 로그인하면 잠긴 사용자 열에서 잠금 아이콘을 클릭하여 다른 관리자의 계정을 잠금 해제할 수 있습니다. 잠긴 관리자는 Panorama에 액세스할 수 없습니다. Panorama는 계정에 할당된 인증 프로파일에 정의된 대로 Panorama에 액세스하려는 연속 시도 실패 횟수를 초과하는 관리자를 잠급니다(디바이스 > 인증 프로파일 참조).

관리자 계정을 생성하려면 추가를 클릭하고 다음 표에 설명된 대로 설정을 구성합니다.

관리자 계정 설정	설명
이름	관리자의 로그인 사용자명을 입력합니다(최대 15자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 포함할 수 있습니다.
인증 프로파일	이 관리자를 인증할 인증 프로파일 또는 시퀀스를 선택하십시오. 자세한 내용은 디바이스 > 인증 프로파일 또는 디바이스 > 인증 순서를 참조하십시오.
클라이언트 인증서 인증만 사용(웹)	웹 인터페이스 액세스에 클라이언트 인증서 인증을 사용하려면 선택합니다. 이 옵션을 선택하면 사용자명(이름)과 암호가 필요하지 않습니다.
비밀번호/비밀번호 확인	관리자의 대소문자를 구분하는 암호를 입력하고 확인합니다(최대 16자). 보안을 위해 Palo Alto Networks는 관리자가 소문자, 대문자 및 숫자 조합을 사용하여 주기적으로 비밀번호를 변경할 것을 권장합니다. 엄격한 암호를 보장하기 위해 암호 강도에 대한 모범 사례를 사용하십시오. 디바이스 그룹 및 템플릿 관리자는 **Panorama** > **Administrators**에 액세스할 수 없습니다. 로컬 암호를 변경하려면 이 관리자가 사용자명을 클릭합니다(웹 인터페이스 하단의 로그아웃 옆). 이는 **Panorama** > 관리자에 대한 액세스가 비활성화된 사용자 지정 Panorama 역할이 있는 관리자에게도 적용됩니다. 인증 프로파일(또는 시퀀스) 또는 로컬 데이터베이스 인증과 함께 암호 인증을 사용할 수 있습니다. 암호 프로파일을 선택한 다음(디바이스 > 암호 프로파일 참조) 최소 암호 복잡성 매개변수를 설정하여(디바이스 > 설정 > 관리 참조) 암호 만료 매개변수를 설정할 수 있지만 Panorama가 로컬에서 인증하는 관리 계정에 대해서만 해당됩니다.

관리자 계정 설정	설명
공개 키 인증(SSH) 사용	SSH 공개 키 인증 사용 선택: 키 가져오기, 찾아보기를 차례로 클릭하여 공개 키 파일을 선택한 다음 확인을 클릭합니다. 관리자 대화 상자는 읽기 전용 텍스트 영역에 업로드된 키를 표시합니다. 지원되는 주요 파일 형식은 IETF SECSH 및 OpenSSH입니다. 지원되는 키 알고리즘은 DSA(1024비트) 및 RSA(768~4096비트)입니다. 공개 키 인증에 실패하면 *Panorama*는 로그인 및 암호 프롬프트를 표시합니다.
관리자 유형	유형 선택에 따라 관리 역할 옵션이 결정됩니다. • 동적 - Panorama 및 관리 방화벽에 대한 액세스를 제공하는 역할입니다. 새로운 기능이 추가되면 Panorama는 동적 역할의 정의를 자동으로 업데이트합니다. 수동으로 업데이트할 필요가 없습니다. • **Custom Panorama Admin** - 읽기-쓰기 액세스 권한, 읽기 전용 액세스 권한이 있거나 Panorama 기능에 대한 액세스 권한이 없는 구성 가능한 역할입니다. • 디바이스 그룹 및 템플릿 관리자 - 이 관리자에 대해 선택한 액세스 도메인에 할당된 디바이스 그룹 및 템플릿의 기능에 대한 읽기-쓰기 액세스 권한, 읽기 전용 액세스 권한 또는 액세스 권한이 없는 구성 가능한 역할입니다.

관리자 역할
 	
(동적 관리자 유형)
	사전 정의된 역할 선택:
	• 운용 관리자 - Panorama 및 모든 디바이스 그룹, 템플릿 및 관리되는 방화벽에 대한 전체 읽기-쓰기 액세스 권한입니다.
	• 운용 관리자**(**읽기 전용**)** - Panorama 및 모든 디바이스 그룹, 템플릿 및 관리 방화벽에 대한 읽기 전용 액세스 권한입니다.
	• **Panorama** 관리자 - 다음 작업을 제외하고 Panorama에 대한 전체 액세스 권한입니다.
	  • Panorama 또는 방화벽 관리자 및 역할을 생성, 수정 또는 삭제합니다.
	  • 구성 내보내기, 유효성 검사, 되돌리기, 저장, 로드 또는 가져오기(**Device** > **Setup** > **Operations**).
	  • **Panorama** 탭에서 예약된 구성 내보내기를 구성합니다.

프로파일	사용자 지정 Panorama 역할을 선택합니다(Panorama > 관리 디바이스 > 요약 참조).

관리자 계정 설정	설명
(커스텀 Panorama 관리자 유형)	
관리자 역할에 대한 액세스 도메인 (디바이스 그룹 및 템플릿 관리자 관리자 유형)	관리자에게 할당하려는 각 액세스 도메인(최대 25개)에 대해 드롭다운에서 추가 액세스 도메인(Panorama > 액세스 도메인 참조)) 옆에 있는 관리자 역할 셀을 클릭하고 드롭다운에서 사용자 지정 장치 그룹 및 템플릿 관리자 역할을 선택합니다.(Panorama > Managed Devices > 요약 참조). 둘 이상의 도메인에 대한 액세스 권한이 있는 관리자가 Panorama에 로그인하면 웹 인터페이스 바닥글에 액세스 도메인 드롭다운이 나타납니다. 관리자는 할당된 액세스 도메인을 선택하여 Panorama가 표시하는 모니터링 및 구성 데이터를 필터링할 수 있습니다. 액세스 도메인 선택은 컨텍스트 드롭다운에 표시되는 방화벽도 필터링합니다. *RADIUS* 서버를 사용하여 관리자를 인증하는 경우 관리자 역할을 매핑하고 도메인을 RADIUS VSA에 액세스해야 합니다. *VSA* 문자열은 제한된 수의 문자를 지원하므로 관리자에 대한 최대 액세스 도메인/역할 쌍 수*(25)*를 구성하는 경우 각 액세스 도메인 및 각 역할의 이름 값은 평균 *9*자를 초과하지 않아야 합니다.
비밀번호 프로파일	암호 프로파일을 선택합니다(디바이스 > 암호 프로파일 참조).

Panorama > 관리자 역할

관리자 역할 프로파일은 관리자의 액세스 권한과 책임을 정의하는 사용자 지정 역할입니다. 예를 들어, 관리자에게 할당된 역할은 관리자가 생성할 수 있는 보고서와 관리자가 보거나 변경할 수 있는 디바이스 그룹 또는 템플릿 구성을 제어합니다.

디바이스 그룹 및 템플릿 관리자의 경우 관리 계정에 할당된 각 액세스 도메인에 별도의 역할을 할당할 수 있습니다(Panorama > 액세스 도메인 참조). 액세스 도메인에 역할을 매핑하면 관리자가 Panorama에서 액세스할 수 있는 정보를 매우 세부적으로 제어할 수 있습니다. 예를 들어, 데이터 센터의 방화벽에 대한 모든 디바이스 그룹을 포함하는 액세스 도메인을 구성하고 해당 액세스 도메인을 데이터 센터 트래픽 모니터링이 허용되지만 방화벽 구성은 허용되지 않는 관리자에게 할당하는 시나리오를 고려하십시오. 이 경우 액세스 도메인을 모든 모니터링 권한을 활성화하지만 디바이스 그룹 설정에 대한 액세스를 비활성화하는 역할에 매핑합니다.

관리자 역할 프로파일을 생성하려면 프로파일을 추가하고 다음 표에 설명된 대로 설정을 구성합니다.

RADIUS 서버를 사용하여 관리자를 인증하는 경우 관리자 역할 및 액세스 도메인을 RADIUS VSA(Vendor Specific Attributes)에 매핑합니다.

Panorama 관리자 역할 설정	설명
이름	이 관리자 역할을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
설명	(선택 사항) 역할에 대한 설명을 입력합니다.
역할	관리 책임 범위 선택: **Panorama** 또는 디바이스 그룹 및 템플릿.
웹 UI	Panorama 컨텍스트(웹 **UI** 목록) 및 방화벽 컨텍스트(컨텍스트 전환 **UI** 목록)의 특정 기능에 허용되는 액세스 유형을 설정하려면 다음 옵션 중에서 선택하십시오. • 활성화( ) - 읽기 및 쓰기 액세스 • 읽기 전용( ) - 읽기 전용 액세스

Panorama 관리자 역할 설정	설명
	• 비활성화(⊗) - 액세스 권한 없음
XML API (Panorama 역할만 해당)	Panorama 및 관리 방화벽에 대한 XML API 액세스 유형(활성화 또는 비활성화)을 선택합니다. • 보고서 - Panorama 및 방화벽 보고서에 액세스합니다. • 로그 - Panorama 및 방화벽 로그에 액세스합니다. • 구성 - Panorama 및 방화벽 구성을 검색하거나 수정할 수 있는 권한입니다. • 운영 요청 - Panorama 및 방화벽에서 운영 명령을 실행할 수 있는 권한입니다. • 커밋 - Panorama 및 방화벽 구성을 커밋할 수 있는 권한입니다. • **User-ID** 에이전트 - User-ID 에이전트에 액세스합니다. • 내보내기 - Panorama 및 방화벽에서 파일을 내보낼 수 있는 권한(예: 구성, 차단 또는 응답 페이지, 인증서 및 키). • 가져오기 - 파일을 Panorama 및 방화벽으로 가져올 수 있는 권한(예: 소프트웨어 업데이트, 콘텐츠 업데이트, 라이선스, 구성, 인증서, 차단 페이지 및 사용자 지정 로그).

명령줄
(Panorama 역할만 해당)
	CLI 액세스에 대한 역할 유형 선택:
	• 없음 - (기본값) Panorama CLI에 대한 액세스가 허용되지 않습니다.
	• 운용 관리자 - **Panorama**에 대한 전체 액세스 권한입니다.
	• 슈퍼리더 - **Panorama**에 대한 읽기 전용 액세스 권한입니다.
	• **Panorama** 관리자 — 다음 작업을 제외한 **Panorama**에 대한 전체 액세스 권한입니다.
	  • Panorama 관리자 및 역할을 생성, 수정 또는 삭제합니다.
	  • 구성 내보내기, 유효성 검사, 되돌리기, 저장, 로드 또는 가져오기
	  • 구성 내보내기를 예약합니다.

REST API (Panorama 역할만 해당)	Panorama 및 관리 방화벽에 대한 각 REST API 엔드포인트에 적용되는 액세스 유형(활성화, 읽기 전용 또는 비활성화)을 선택합니다. 다음 카테고리의 엔드포인트에 역할 액세스를 할당할 수 있습니다. • 개체

Panorama 관리자 역할 설정	설명
	• 정책 • 네트워크 • 디바이스
컨텍스트 전환	
디바이스 관리자 역할	**Panorama** 관리자가 Panorama와 관리 방화벽 웹 인터페이스 간에 컨텍스트 전환을 수행할 수 있도록 디바이스 관리자 역할 이름을 입력합니다.

Panorama > 액세스 도메인

액세스 도메인은 디바이스 그룹 및 템플릿 관리자가 특정 디바이스 그룹(정책 및 개체 관리), 템플릿(네트워크 및 디바이스 설정 관리), 관리되는 방화벽의 웹 인터페이스(컨텍스트 전환을 통해) 및 관리 방화벽의 REST API에 대한 액세스를 제어합니다. 최대 4,000개의 액세스 도메인을 정의하고 로컬에서 또는 RADIUS VSA(Vendor-Specific Attributes), TACACS+ VSA 또는 SAML 속성을 사용하여 관리할 수 있습니다. 액세스 도메인을 생성하려면 다음 표에 설명된 대로 도메인을 추가하고 설정을 구성합니다.

도메인 설정에 액세스	설명
이름	액세스 도메인의 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 포함할 수 있습니다.
공유 개체	이 액세스 도메인의 디바이스 그룹이 공유 위치에서 상속하는 개체에 대해 다음 액세스 권한 중 하나를 선택합니다. 권한에 관계없이 관리자는 공유 또는 기본(사전 정의된) 개체를 재정의할 수 없습니다. • 읽기 - 관리자는 공유 개체를 표시하고 복사할 수 있지만 다른 작업은 수행할 수 없습니다. 비공유 개체를 추가하거나 공유 개체를 복사할 때 대상은 공유되지 않은 액세스 도메인 내의 디바이스 그룹이어야 합니다. • 쓰기 - 관리자는 공유 개체에 대한 모든 작업을 수행할 수 있습니다. 이것이 기본값입니다. • 공유 전용 - 관리자는 공유에만 개체를 추가할 수 있습니다. 또한 관리자는 공유 개체를 표시, 편집 및 삭제할 수 있지만 이동하거나 복사할 수는 없습니다. 이 선택의 결과로 관리자는 비공유 개체를 표시하는 것 외에 다른 작업을 수행할 수 없습니다.
디바이스 그룹	액세스 도메인의 특정 디바이스 그룹에 대한 읽기-쓰기 액세스를 활성화하거나 비활성화합니다. 모두 활성화 또는 모두 비활성화를 클릭할 수도 있습니다. 디바이스 그룹에 대해 읽기-쓰기 액세스를 활성화하면 자동으로 해당 하위 항목에 대해 동일한 액세스가 활성화됩니다. 하위 항목을 수동으로 비활성화하면 최상위 상위 항목에 대한 액세스가 자동으로 읽기 전용으로 변경됩니다. 기본적으로 모든 디바이스 그룹에 대한 액세스가 비활성화되어 있습니다. 목록에 특정 디바이스 그룹만 표시되도록 하려면 디바이스 그룹 이름과 선택한 필터를 선택합니다.

도메인 설정에 액세스	설명
	공유 개체에 대한 액세스를 공유 전용으로 설정하면 *Panorama*는 읽기-쓰기 액세스를 지정하는 모든 디바이스 그룹에 읽기 전용 액세스를 적용합니다.
템플릿	할당하려는 각 템플릿 또는 템플릿 스택(template stack)에 대해 추가를 클릭하고 드롭다운에서 선택합니다.
디바이스 컨텍스트 (액세스 도메인 페이지의 디바이스/가상 시스템 열에 해당)	관리자가 로컬 구성을 수행하기 위해 컨텍스트를 전환할 수 있는 방화벽을 선택합니다. 목록이 길면 디바이스 상태, 플랫폼, 디바이스 그룹, 템플릿, 태그 및 **HA** 상태별로 필터링할 수 있습니다.
로그 수집기 그룹	할당하려는 각 수집기 그룹에 대해 드롭다운에서 추가하고 선택합니다.

Panorama > 예약된 구성 푸시

관리 방화벽에 구성 변경 사항을 푸시하는 작업 오버헤드를 단순화하려면 지정된 날짜 및 시간에 관리 방화벽에 변경 사항을 자동으로 푸시하도록 예약된 구성 푸시를 생성합니다. 예약된 구성 푸시가 한 번 또는 반복되는 일정으로 발생하도록 구성할 수 있습니다.

다음 주제에서는 예약된 구성 푸시에 대한 추가 정보를 제공합니다.

무엇을 알고 싶습니까?	참조:
예약된 구성 푸시를 추가합니다.	예약된 구성 푸시 스케줄러
예약된 구성 푸시 기록을 봅니다.	예약된 구성 푸시 실행 기록

예약된 구성 푸시 정보	설명
이름	구성 푸시 일정의 이름입니다.
관리 범위	다른 관리자가 변경한 구성을 예약된 구성에 추가합니다. 다른 관리자에 대한 구성 변경을 푸시하는 기능은 Panorama 관리자 역할 프로파일(Panorama > 관리 역할)에서 정의됩니다. <*usernames*>링크를 클릭하여 관리자를 선택하고 확인을 클릭하여 다른 관리자가 수행한 구성 변경 사항을 표시하고 선택합니다. 역할이 다른 관리자의 변경 내용을 푸시하도록 허용하더라도 푸시 범위에는 기본적으로 변경 사항만 포함됩니다.
비활성화	푸시된 예약 구성이 활성화(선택 취소)되었는지 또는 비활성화(선택)되었는지 표시합니다.
날짜	다음 구성 푸시가 발생하도록 예약된 날짜(YYY/MM/DD)입니다.
회귀	예약된 구성 푸시가 일회성 푸시인지 또는 반복 예약 푸시(##, ## 또는 ##)인지의 여부.
시간	반복 일정의 경우 구성 푸시가 발생하도록 예약된 시간(hh:mm) 및 요일입니다. 일회성 일정의 경우 예약된 구성 푸시가 발생하도록 예약된 시간(hh:mm)입니다.
상태	마지막으로 예약된 구성 푸시의 실행 상태입니다. 예약된 구성 푸시와 연결된 모든 관리 방화벽에 대한 전체 실행 기록을 보려면 클릭합니다.

예약된 구성 푸시 정보	설명
디바이스	예약된 구성 푸시의 영향을 받는 관리형 방화벽. 디바이스 그룹 및 템플릿 변경 사항을 기반으로 영향을 받는 방화벽을 표시합니다.

예약된 구성 푸시 스케줄러

푸시가 발생하는 시기와 빈도, 푸시할 디바이스 그룹 및 템플릿 구성, 푸시할 관리되는 방화벽에 대한 일정 매개변수를 설정하여 관리 방화벽에 대한 예약 푸시를 생성합니다. 디바이스 그룹 또는 템플릿의 마지막 커밋 상태가 ##### ## 경우 Panorama는 예약된 디바이스 그룹 및 템플릿 구성 푸시를 관리형 방화벽으로 수행합니다.

예약된 구성 푸시 설정	설명
이름	구성 푸시 일정의 이름입니다.
Disabled	예약된 구성 푸시를 비활성화하려면 선택합니다. 예약된 구성 푸시를 다시 활성화하려면 선택을 취소합니다.
유형	특정 날짜 및 시간에 구성 푸시를 예약하려면 일회성 일정을 선택합니다. 구성 푸시를 예약하려면 반복 일정을 선택하세요.
날짜	다음 구성 푸시가 발생하도록 예약된 날짜입니다.
시간	예약된 구성 푸시 날짜에 구성 푸시가 발생하도록 예약된 시간(`hh:mm:ss`)입니다.
반복	예약된 구성 푸시가 일회성 푸시(없음) 또는 반복 예약 푸시(매월, 매주 또는 매일)인지의 여부. 기본값은 없음입니다.
푸시 스코프 선택	
디바이스 그룹	하나 이상의 디바이스 그룹과 연결된 관리 방화벽을 선택합니다. • 디바이스 후보 구성과 병합(기본적으로 활성화됨) - Panorama에서 푸시된 구성 변경 사항을 대상 방화벽에서 로컬로 구현된 보류 중인 구성 변경 사항과 병합합니다. 푸시는 PAN-OS® 소프트웨어가 병합된 변경 사항을 커밋하도록 트리거합니다. 이 선택을 비활성화하면 커밋에서 방화벽의 후보 구성을 제외합니다. • 디바이스 및 네트워크 템플릿 포함(기본적으로 활성화됨) - 단일 작업으로 디바이스 그룹 변경 사항과 연결된 템플릿 변경 사항을 선택한 방화벽 및 가상 시스

예약된 구성 푸시 설정	설명
	템에 푸시합니다. 이러한 변경 사항을 별도의 작업으로 푸시하려면 이 옵션을 비활성화하십시오.
템플릿	하나 이상의 템플릿 스택(template stack)과 연결된 관리형 방화벽을 선택합니다. • 디바이스 후보 구성과 병합(기본적으로 활성화됨) - Panorama에서 푸시된 구성 변경 사항을 대상 방화벽에서 로컬로 구현된 보류 중인 구성 변경 사항과 병합합니다. 푸시는 PAN-OS 소프트웨어가 병합된 변경 사항을 커밋하도록 트리거합니다. 이 선택을 비활성화하면 커밋에서 방화벽의 후보 구성을 제외합니다.

예약된 구성 푸시 실행 기록

예약된 구성 푸시 실행 기록을 보고 특정 일정에 대한 마지막 푸시가 발생한 시간을 이해하고 영향을 받은 관리되는 방화벽의 수를 확인합니다. 영향을 받는 관리 방화벽의 총 수에서 관리 방화벽에 성공한 구성 푸시 수와 실패한 구성 푸시 수를 볼 수 있습니다. 실패한 푸시 중에서 관리형 방화벽과 Panorama 간의 연결이 끊기거나 중단되어 구성이 자동으로 되돌려진 관리형 방화벽의 총 수를 볼 수 있습니다.

실행 이력 정보	설명
마지막 푸시 시간	예약된 구성 푸시가 발생한 시간입니다(`MM/DD/YYY HH:MM:SS`).
디바이스	예약된 구성 푸시와 연결된 관리되는 방화벽의 총 수입니다.
성공	푸시가 성공한 예약된 구성 푸시와 연결된 관리되는 방화벽의 총 수입니다.
실패	푸시가 실패한 예약된 구성 푸시와 연결된 관리되는 방화벽의 총 수입니다.
되돌리기	예약된 구성 푸시가 실패하고 구성이 되돌려진 관리 방화벽의 총 수입니다.
작업	Panorama 작업 관리자 및 구성 푸시와 연결된 작업을 봅니다.

Panorama > 관리 디바이스 > 요약

Panorama가 관리하는 Palo Alto Networks 방화벽을 관리 디바이스라고 합니다. Panorama는 동일한 주요 릴리스 또는 이전 주요 릴리스를 실행하는 방화벽을 관리할 수 있지만 Panorama는 이후 주요 릴리스를 실행하는 방화벽을 관리할 수 없습니다. 예를 들어, PAN-OS 11.0을 실행하는 Panorama는 PAN-OS 11.0 및 이전 버전을 실행하는 방화벽을 관리할 수 있습니다. 또한 Panorama보다 최신 유지 관리 릴리스를 실행하는 방화벽을 관리하는 것은 기능이 예상대로 작동하지 않을 수 있으므로 관리하지 않는 것이 좋습니다. 예를 들어 Panorama에서 PAN-OS 10.0.0을 실행하는 경우 PAN-OS 10.0.1 이상 유지 관리 릴리스를 실행하는 방화벽을 관리하지 않는 것이 좋습니다. 릴리스 정보에 대한 자세한 내용은 PAN-OS 11.0 릴리스 노트를 참조하십시오. 지원되는 PAN-OS 버전에 대한 자세한 내용은 단종 요약을 참조하십시오.

- 관리 방화벽 관리
- 관리 방화벽 정보
- 방화벽 소프트웨어 및 콘텐츠 업데이트
- 방화벽 백업

관리 방화벽 관리

방화벽에서 다음과 같은 관리 작업을 수행할 수 있습니다.

작업	설명
추가	방화벽을 추가하고 일련번호(행당 하나씩)를 입력하여 관리 디바이스로 추가합니다. 그러면 관리되는 디바이스 창에 연결 상태, 설치된 업데이트 및 초기 구성 중에 설정된 속성을 포함하여 관리되는 방화벽 정보가 표시됩니다. 디바이스 그룹 또는 템플릿 스택(template stack)과 방화벽을 연결하려면 디바이스 연결 체크박스를 선택합니다. Panorama 관리 서버에서 관리할 CSV 형식의 여러 방화벽을 가져옵니다. 샘플 CSV 파일을 다운로드할 수 있습니다. 그런 다음 Panorama가 방화벽을 관리할 수 있도록 각 방화벽에 Panorama 관리 서버의 IP 주소를 입력합니다(디바이스 > 설정 > 관리 참조). 방화벽은 *AES-256* 암호화를 사용하여 *SSL* 연결을 통해 *Panorama*에 등록합니다. *Panorama*와 방화벽은 *2,048*비트 인증서를 사용하여 서로를 인증하고 구성 관리 및 로그 수집을 위해 *SSL* 연결을 사용합니다.
다시 연결	하나 이상의 선택한 방화벽을 다른 디바이스 그룹 또는 템플릿 스택(template stack)에 재할당합니다.

작업	설명
삭제	하나 이상의 방화벽을 선택한 다음 Panorama가 관리하는 방화벽 목록에서 삭제합니다.
태그	하나 이상의 방화벽을 선택한 다음 태그를 클릭한 다음 최대 31자의 텍스트 문자열을 입력하거나 기존 태그를 선택합니다. 빈 공간을 사용하지 마십시오. 웹 인터페이스가 긴 방화벽 목록을 표시할 때마다(예: 소프트웨어 설치 대화 상자에서) 태그는 목록을 필터링하는 하나의 수단을 제공합니다. 예를 들어 지점이라는 태그를 사용하여 네트워크의 모든 지점 방화벽을 필터링할 수 있습니다.
설치	방화벽 소프트웨어 및 콘텐츠 업데이트를 설치합니다.
그룹 HA 피어	관리되는 디바이스 페이지에서 고가용성(HA) 구성의 피어인 방화벽을 그룹화하도록 하려면 그룹 **HA** 피어를 선택하십시오. 그런 다음 두 피어에 대해서만 작업을 수행하거나 각 HA 쌍에서 아무 피어도 수행하지 않도록 선택할 수 있습니다.
관리(백업)	방화벽 백업을 관리합니다.
PDF/CSV	최소한의 읽기 전용 액세스 권한이 있는 관리 역할은 관리되는 방화벽 테이블을 **PDF/CSV**로 내보낼 수 있습니다. 필터를 적용하여 감사와 같은 항목에 대한 보다 구체적인 테이블 구성 출력을 생성할 수 있습니다. 웹 인터페이스에서 보이는 열만 내보내집니다. 구성 테이블 내보내기를 참조하십시오.
마스터 키 배포	새 마스터 키를 배포하거나 하나 이상의 디바이스의 기존 마스터 키를 업데이트합니다.
CSP에서 OTP 요청	관리되는 방화벽에 대한 OTP(일회용 암호)를 생성합니다. • 선택한 사용자 지정 디바이스 - Palo Alto Networks 클라우드 서비스를 활용하기 위해 선택한 관리 방화벽에 대한 OTP를 생성하여 디바이스 인증서를 설치합니다. • 인증서가 없는 모든 디바이스 선택 - Palo Alto Networks 클라우드 서비스를 활용하기 위해 디바이스 인증서가 성공적으로 설치되지 않은 관리 방화벽에 대해 OTP를 생성합니다.
OTP 업로드	고객 지원 포털에서 생성된 OTP를 붙여넣어 모든 관리 방화벽에 대한 디바이스 인증서를 설치합니다.

관리 방화벽 정보

Panorama > **Managed Devices** > **Summary**를 선택하여 각 관리 방화벽에 대한 다음 정보를 표시합니다.

관리 방화벽 정보	설명
디바이스 그룹	방화벽이 속한 디바이스 그룹의 이름을 표시합니다. 기본적으로 이 열은 숨겨져 있지만 열 머리글에서 드롭다운을 선택한 다음 열 > 디바이스 그룹을 선택하여 표시할 수 있습니다. 이 페이지는 디바이스 그룹에 따라 클러스터의 방화벽을 표시합니다. 각 클러스터에는 디바이스 그룹 이름, 할당된 총 방화벽 수, 연결된 방화벽 수 및 레이어의 디바이스 그룹 경로를 표시하는 헤더 행이 있습니다. 예를 들어, 데이터 센터**(2/4** 디바이스 연결**): Shared** > **Europe** > **Data Center**는 **Data Center**라는 디바이스 그룹에 4개의 구성원 방화벽(그 중 2개는 연결됨)이 있고 **Europe**이라는 디바이스 그룹의 하위 요소임을 나타냅니다. 디바이스 그룹을 축소하거나 확장하여 해당 방화벽을 숨기거나 표시할 수 있습니다.
디바이스 이름	방화벽의 호스트 이름 또는 일련번호를 표시합니다. VM 시리즈 NSX 에디션 방화벽의 경우 방화벽 이름에 ESXi 호스트의 호스트 이름이 추가됩니다. 예를 들어 PA-VM: Host-NY5105
가상 시스템	다중 가상 시스템 모드에 있는 방화벽에서 사용 가능한 가상 시스템을 나열합니다.
모델	방화벽 모델을 표시합니다.
태그	각 방화벽/가상 시스템에 대해 정의된 태그를 표시합니다.
일련번호	방화벽의 일련번호를 표시합니다.
작동 모드	방화벽의 작동 모드를 표시합니다. FIPS-CC 또는 일반일 수 있습니다.
IP 주소	방화벽/가상 시스템의 IP 주소를 표시합니다.
	IPv4 - 방화벽/가상 시스템의 IPv4 주소입니다.
	IPv6 - 방화벽/가상 시스템의 IPv6 주소입니다.
변수	템플릿 스택(template stack)의 디바이스에서 복사하여 디바이스별 변수 정의를 생성하거나 기존 변수 정의를 편집하여 디바이스에 대한 고유 변수를 생성합니다. 디바이스가 템플릿 스택(template stack)과 연결되지 않은 경우 이 열은 비어 있습니다. 기본적으로 변수는 템플릿 스택(template stack)에서 상속됩니다. 디바이스에서 변수 정의 생성 또는 편집을 참조하십시오.

관리 방화벽 정보	설명
템플릿	방화벽이 할당된 템플릿 스택(template stack)을 표시합니다.
상태	디바이스 상태 - Panorama와 방화벽 간의 연결 상태를 나타냅니다. 연결됨 또는 연결 해제됨. VM 시리즈 방화벽에는 두 가지 추가 상태가 있을 수 있습니다. • 비활성화됨 - 방화벽에서 직접 또는 **VM** 비활성화(**Panorama** > **Device Deployment** > **Licenses**)를 선택하여 가상 머신을 비활성화하고 방화벽에서 모든 라이선스와 자격을 제거했음을 나타냅니다. 비활성화 프로세스는 VM 시리즈 방화벽의 일련번호를 제거하므로 비활성화된 방화벽은 더 이상 Panorama에 연결되지 않습니다. • 부분적으로 비활성화됨 - Panorama에서 라이선스 비활성화 프로세스를 시작했지만 방화벽이 오프라인이고 Panorama가 방화벽과 통신할 수 없기 때문에 프로세스가 완전히 완료되지 않았음을 나타냅니다.
	HA 상태 - 방화벽이 다음과 같은지의 여부를 나타냅니다. • 활성 - 정상적인 트래픽 처리 작동 상태 • 수동 - 일반 백업 상태 • 시작 중 - 방화벽은 부팅 후 최대 60초 동안 이 상태에 있습니다. • 작동하지 않음 - 오류 상태 • 일시 중단됨 - 관리자가 방화벽을 비활성화함 • 임시 - 능동형/능동형 구성의 링크 또는 경로 모니터링 이벤트의 경우
	공유 정책 - 방화벽의 정책 및 개체 구성이 Panorama와 동기화되는지의 여부를 나타냅니다.
	템플릿 - 방화벽의 네트워크 및 디바이스 구성이 Panorama와 동기화되었는지의 여부를 나타냅니다.
상태(계속)	인증서 - 관리 디바이스의 클라이언트 인증서 상태를 나타냅니다. • 사전 정의됨 - 관리되는 디바이스가 사전 정의된 인증서를 사용하여 Panorama로 인증합니다. • 배포됨 - 사용자 지정 인증서가 관리되는 디바이스에 성공적으로 배포되었습니다.

관리 방화벽 정보	설명
	• **N**일 **N**시간 후 만료 - 현재 설치된 인증서가 30일 이내에 만료됩니다. • **N**분 후 만료 - 현재 설치된 인증서가 하루 이내에 만료됩니다. • 클라이언트 **ID** 확인 통과 - 인증서 일반 이름이 연결 디바이스의 일련번호와 일치합니다. • **OCSP** 상태 알 수 없음 - Panorama가 OCSP 응답자로부터 OCSP 상태를 가져올 수 없습니다. • **OCSP** 상태를 사용할 수 없음 - Panorama가 OCSP 응답자에 연결할 수 없습니다. • **CRL** 상태 알 수 없음 - Panorama가 CRL 데이터베이스에서 해지 상태를 가져올 수 없습니다. • **CRL** 상태를 사용할 수 없음 - Panorama에서 CRL 데이터베이스에 연결할 수 없습니다.
	• **OCSP/CRL** 상태 알 수 없음 - 둘 다 활성화된 경우 Panorama에서 OCSP 또는 해지 상태를 가져올 수 없습니다. • **OCSP/CRL** 상태를 사용할 수 없음 - 둘 다 활성화된 경우 Panorama가 OCSP 또는 CRL 데이터베이스에 연결할 수 없습니다. • 신뢰할 수 없는 발급자 - 관리되는 디바이스에 사용자 지정 인증서가 있지만 서버에서 유효성을 검사하지 않습니다. 마지막 커밋 상태 - 방화벽에서 마지막 커밋이 실패했는지 성공했는지의 여부를 나타냅니다.
소프트웨어 버전 | 앱 및 위협 | 바이러스 백신 | URL 필터링 | GlobalProtect™ 클라이언트 | WildFire	현재 방화벽에 설치된 소프트웨어 및 콘텐츠 버전을 표시합니다. 자세한 내용은 방화벽 소프트웨어 및 콘텐츠 업데이트를 참조하십시오.
백업	각 방화벽 커밋에서 PAN-OS는 자동으로 방화벽 구성 백업을 Panorama로 보냅니다. 사용 가능한 구성 백업을 보고 선택적으로 하나를 로드하려면 관리를 클릭합니다. 자세한 내용은 방화벽 백업을 참조하십시오.
마지막 마스터 키 푸시	Panorama에서 방화벽으로의 마스터 키 배포 상태를 표시합니다.

관리 방화벽 정보	설명
	상태 - 최신 마스터 키 푸시 상태를 표시합니다. ## 또는 ##일 수 있습니다. 마스터 키가 Panorama에서 방화벽으로 푸시되지 않은 경우 # # ##이 표시됩니다.
	타임스탬프 - Panorama에서 가장 최근에 마스터 키를 누른 날짜와 시간을 표시합니다.
컨테이너 - Kubernetes 클러스터에서 컨테이너화된 애플리케이션 워크로드를 보호하기 위해 CN 시리즈 방화벽을 배포한 경우 다음 열을 사용합니다.	
컨테이너 노드 수	Panorama에 등록된 Management Plane(MP)(CN-Mgmt)에 연결된 컨테이너화된 방화벽 데이터 플레인(CN-NGFW)의 수를 표시합니다. 값은 각 CN-Mgmt 포드 쌍에 대해 0~30개의 CN-NGFW 포드일 수 있습니다.
컨테이너 메모	향후 사용

디바이스 변수 정의 생성

디바이스가 템플릿 스택(template stack)에 처음 추가되면 템플릿 스택(template stack)의 디바이스에서 복사한 디바이스별 변수 정의를 생성하거나 **Panorama** > **Managed Devices** > **Summary**를 통해 템플릿 변수 정의를 편집할 수 있습니다. 기본적으로 모든 변수 정의는 템플릿 스택(template stack)에서 상속되며 개별 디바이스에 대한 변수 정의를 무시하고 삭제할 수는 없습니다. 변수를 사용하여 구성의 모든 영역, IKE 게이트웨이 구성(인터페이스) 및 HA 구성(그룹 ID)의 인터페이스에서 IP 주소 개체 및 IP 주소 리터럴(IP 넷마스크, IP 범위, FQDN)을 바꿀 수 있습니다.

디바이스 변수 정의 정보 생성	설명
템플릿 스택(template stack)의 다른 디바이스에서 디바이스 변수 정의를 복사하시겠습니까?	
아니오	기존 변수 정의를 보고 필요에 따라 편집합니다. Panorama > 템플릿 > 템플릿 변수를 참조하십시오.
예	드롭다운에서 변수 정의를 복사할 디바이스를 선택한 다음 복사할 특정 변수 정의를 선택합니다.

방화벽 소프트웨어 및 콘텐츠 업데이트

관리 방화벽에 소프트웨어 또는 콘텐츠 업데이트를 설치하려면 먼저 **Panorama** > 디바이스 배포 페이지를 사용하여 업데이트를 Panorama에 다운로드하거나 업로드하십시오. 그런 다음 **Panorama** > **Managed Devices** 페이지를 선택한 다음 설치를 클릭하고 다음 필드를 완성합니다.

관리*(MGT)* 인터페이스의 트래픽을 줄이기 위해 업데이트 배포에 별도의 인터페이스를 사용하도록 *Panorama*를 구성할 수 있습니다*(*Panorama > 설정 > 인터페이스 참조*)*.

방화벽 소프트웨어/콘텐츠 업데이트 설치 옵션	설명
유형	설치할 업데이트 유형을 선택하십시오. PAN-OS 소프트웨어, **GlobalProtect** 클라이언트 소프트웨어, 앱 및 위협 서명, 안티바이러스 서명, **WildFire** 또는 **URL** 필터링.
파일	업데이트 이미지를 선택합니다. 드롭다운에는 **Panorama** > **Device Deployment** 페이지를 사용하여 Panorama에 다운로드하거나 업로드한 이미지만 포함됩니다.
필터	필터를 선택하여 디바이스 목록을 필터링합니다.
디바이스	이미지를 설치할 방화벽을 선택하십시오.
디바이스 이름	방화벽 이름.
현재 버전	현재 방화벽에 설치된 선택된 유형의 업데이트 버전입니다.
HA 상태	방화벽이 다음과 같은지의 여부를 나타냅니다. • 활성 - 정상적인 트래픽 처리 작동 상태 • 수동 - 일반 백업 상태 • 시작 중 - 방화벽은 부팅 후 최대 60초 동안 이 상태에 있습니다. • 작동하지 않음 - 오류 상태 • 일시 중단됨 - 관리자가 방화벽을 비활성화함 • 임시 - 능동형/능동형 구성의 링크 또는 경로 모니터링 이벤트의 경우
그룹 HA 피어	고가용성(HA) 구성에서 피어인 방화벽을 그룹화하려면 선택합니다.
필터 선택	디바이스 목록에 특정 방화벽만 표시하려면 해당 디바이스 이름과 선택한 필터를 선택하십시오.

방화벽 소프트웨어/콘텐츠 업데이트 설치 옵션	설명
디바이스에만 업로드	방화벽에 이미지를 업로드하지만 방화벽을 자동으로 재부팅하지 않으려면 선택합니다. 방화벽을 수동으로 재부팅하면 이미지가 설치됩니다.
설치 후 디바이스 재부팅(소프트웨어만 해당)	소프트웨어 이미지를 업로드하고 설치하려면 선택합니다. 설치 프로세스가 재부팅을 트리거합니다.
콘텐츠 업데이트에서 새 앱 비활성화(앱 및 위협에만 해당)	마지막으로 설치된 업데이트와 관련하여 새로운 업데이트의 애플리케이션을 비활성화하려면 선택합니다. 이는 최신 위협으로부터 보호하는 동시에 정책 업데이트를 준비한 후 애플리케이션을 활성화할 수 있는 유연성을 제공합니다. 그런 다음 애플리케이션을 활성화하려면 방화벽에 로그인하고 디바이스 > 동적 업데이트를 선택한 다음 기능 열에서 앱을 클릭하여 새 애플리케이션을 표시하고 활성화하려는 각 애플리케이션에 대해 활성화/비활성화를 클릭합니다.

방화벽 백업

- Panorama > 관리 디바이스

Panorama는 관리 방화벽에 커밋한 모든 구성 변경 사항을 자동으로 백업합니다. 방화벽에 대한 백업을 관리하려면 **Panorama** > **Managed Devices**를 선택한 다음 방화벽에 대한 백업 열에서 관리를 클릭한 후 다음 작업 중 하나를 수행합니다.

*Panorama*가 저장하는 방화벽 구성 백업의 수를 구성하려면 ***Panorama*** > ***Setup*** > ***Management***를 선택한 다음, 로깅 및 보고 설정을 편집하고, 로그 내보내기 및 보고를 선택한 다음, 구성 백업의 버전 수*(*기본값은 *100)*를 입력합니다.

작업	설명
저장되거나 커밋된 구성에 대한 세부 정보를 표시합니다.	백업의 버전 열에서 저장된 구성 파일 이름 또는 커밋된 구성 버전 번호를 클릭하여 연결된 XML 파일의 내용을 표시합니다.
저장되거나 커밋된 구성을 후보 구성으로 복원합니다.	백업에 대한 작업 열에서 로드 및 커밋을 클릭합니다. 방화벽 구성을 로드하면 로컬 디바이스 구성이 되돌려지고 Panorama에서 푸시된 구성이 되돌려지지 않습니다. 방화벽 백업을 로드한 후 방화벽 웹 인터페이스로 컨텍스트 전환하거나 방화벽 웹 인터페이스를 실행하여 커밋해야 합니다.

작업	설명
저장된 구성을 제거합니다.	저장된 백업에 대한 작업 열에서 삭제()를 클릭합니다.

Panorama > 디바이스 검역

Panorama > **Device Quarantine**(Panorama 디바이스 검역) 페이지에는 검역 목록에 있는 디바이스가 표시됩니다. 디바이스는 다음 작업의 결과로 이 목록에 나타납니다.

- 시스템 관리자가 수동으로 이 목록에 디바이스를 추가했습니다.

  디바이스를 수동으로 추가하려면 호스트 **ID**를 입력하고 선택적으로 분리해야 하는 디바이스의 일련번호를 입력합니다.
- 시스템 관리자는 트래픽, GlobalProtect 또는 위협 로그에서 호스트 ID 열을 선택한 다음 해당 열에서 디바이스를 선택한 다음 디바이스 차단을 선택했습니다.
- 디바이스는 일치 목록에 검역소로 설정된 기본 제공 작업이 있는 로그 포워딩 프로파일이 있는 보안 정책 규칙과 일치했습니다.

  호스트 *ID*는 *GlobalProtect* 로그에 자동으로 표시됩니다. 호스트 *ID*가 트래픽, 위협 또는 통합 로그에 표시되려면 *Panorama* 어플라이언스에 소스 디바이스가 검역소로 설정된 보안 정책 규칙이 하나 이상 있어야 합니다. 보안 정책에 이 설정이 없으면 트래픽, 위협 또는 통합 로그에 호스트 *ID*가 없고 로그 포워딩 프로파일이 적용되지 않습니다.
- API를 사용하여 디바이스를 검역 목록에 추가했습니다.
- Panorama 어플라이언스가 재배포 항목의 일부로 검역 목록을 수신했습니다(검역 목록이 다른 Panorama 어플라이언스 또는 방화벽에서 재배포됨).

디바이스 검역소 테이블에는 다음 필드가 포함됩니다.

필드	설명
호스트 ID	차단된 호스트의 호스트 ID입니다.
이유	디바이스가 분리된 이유입니다. **Admin Add**의 이유는 관리자가 테이블에 디바이스를 수동으로 추가했음을 의미합니다.
타임스탬프	관리자 또는 보안 정책 규칙이 디바이스를 검역 목록에 추가한 시간입니다.
소스 디바이스/앱	분리 목록에 디바이스를 추가한 Panorama, 방화벽 또는 타사 앱의 IP 주소입니다.

필드	설명
일련번호	(선택 사항) 분리된 디바이스의 일련번호(사용 가능한 경우).
사용자명	(선택 사항) 디바이스가 분리되었을 때 로그인한 GlobalProtect 클라이언트 사용자의 사용자명입니다.

Panorama > 관리 디바이스 > 상태

Panorama™를 사용하면 관리 방화벽의 하드웨어 리소스와 성능을 모니터링할 수 있습니다. Panorama는 시간에 따른 성능 정보(CPU, 메모리, CPS 및 처리량), 로깅 성능, 환경 정보(예: 팬, RAID 상태, 전원 공급 디바이스)를 중앙 집중화하고 커밋, 콘텐츠 설치 및 상태 데이터에 대한 소프트웨어 업그레이드와 같은 이벤트의 상관 관계를 나타냅니다. 방화벽이 계산된 기준에서 벗어나면 Panorama는 이를 이탈 디바이스로 보고하여 하드웨어 문제를 신속하게 식별, 진단 및 해결하는 데 도움을 줍니다.

이 페이지를 사용하여 다음을 수행할 수 있습니다.

자세한 디바이스 상태를 봅니다.	Panorama에서 관리하는 디바이스의 상태 메트릭을 봅니다.
그룹 HA 피어	어떤 방화벽이 함께 그룹화되어 있는지 확인하여 잠재적인 문제를 식별하고 하드웨어 리소스 또는 성능 문제의 영향을 받는 방화벽인지의 여부를 확인합니다.
PDF/CSV	최소한의 읽기 전용 액세스 권한이 있는 관리 역할은 관리되는 방화벽 테이블을 **PDF/CSV** 형식으로 내보낼 수 있습니다. 감사와 같이 필요할 때 필터를 적용하여 보다 구체적인 테이블 구성 출력을 생성할 수 있습니다. 웹 인터페이스에서 보이는 열만 내보내집니다. 구성 테이블 데이터 내보내기를 참조하십시오.

Panorama > 관리 디바이스 > 상태 > 모든 디바이스

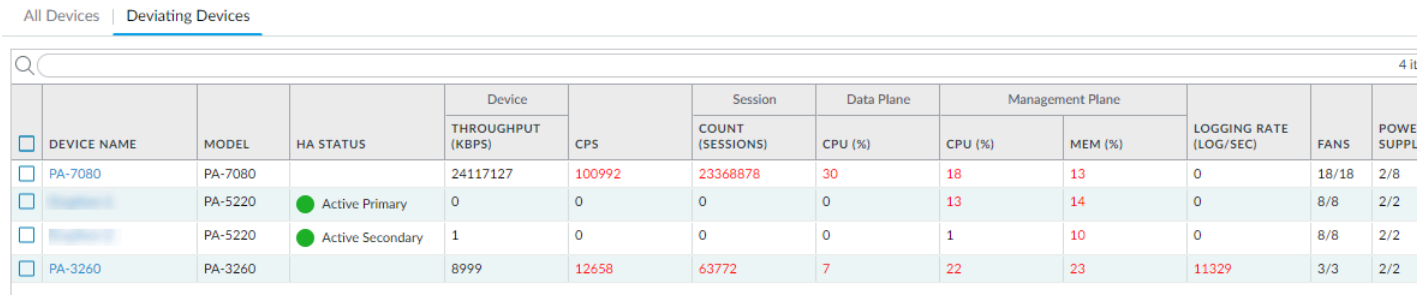
이 페이지에서는 각 방화벽에 대한 다음 정보를 볼 수 있습니다.

상태 정보	설명
디바이스 이름	방화벽의 호스트 이름 또는 일련번호입니다. VM 시리즈 NSX 에디션 방화벽의 경우 방화벽 이름에 ESXi 호스트의 호스트 이름이 추가됩니다. 예를 들어 PA-VM: Host-NY5105

상태 정보	설명
모델	방화벽 모델입니다.
디바이스	
처리량(킬로비트)	초당 킬로비트로 측정된 시간 경과에 따른 데이터 처리량(5분 평균)입니다.
CPS	시간 경과에 따른 방화벽의 초당 총 연결 수(평균 5분).
세션	
카운트(세션)	시간 경과에 따른 총 세션 수(5분 평균).
데이터 플레인	
CPU(%)	데이터 플레인의 총 CPU 사용률입니다.
Management Plane(MP)	
CPU(%)	Management Plane(MP)의 총 CPU 사용률입니다.
MEM (%)	Management Plane(MP)의 총 메모리 사용률입니다.
로깅 속도(초당 로그)	관리형 방화벽의 수신 로그 비율입니다.
팬	각 팬 트레이에 있는 팬의 존재, 현재 상태, RPM 및 마지막 오류를 표시합니다. 팬 상태는 *A*/*B*로 표시됩니다. 여기서 *A*는 정상 작동 중인 팬 수이고 *B*는 방화벽의 총 팬 수입니다. 가상 방화벽은 `N/A`를 표시합니다.
AC 전원 공급 디바이스	존재, 현재 상태 및 마지막 실패 타임스탬프를 표시합니다. 전원 공급 디바이스 상태는 *A*/*B*로 표시됩니다. 여기서 *A*는 정상 작동 중인 전원 공급 디바이스의 수이고 *B*는 디바이스의 총 전원 공급 디바이스 수입니다. 가상 방화벽은 `N/A`를 표시합니다.
포트	방화벽에서 사용 중인 총 포트 수입니다. 포트는 *A*/*B*로 표시됩니다. 여기서 *A*는 실행 중인 양호한 포트의 수이고 *B*는 디바이스의 총 포트 수입니다.

Panorama > 관리 디바이스 > 상태 > 이탈 디바이스

편차 디바이스 탭은 계산된 기준에서 벗어나는 메트릭이 있는 디바이스를 표시하고 이러한 편차 메트릭을 빨간색으로 표시합니다. 메트릭 상태 기준은 표준 편차를 더한 7일 동안 주어진 메트릭에 대한 상태 성능을 평균화하여 결정됩니다.



	DEVICE NAME	MODEL	HA STATUS	Device		Session	Data Plane	Management Plane		LOGGING RATE (LOG/SEC)	FANS	POWE SUPPL
				THROUGHPUT (KBPS)	CPS	COUNT (SESSIONS)	CPU (%)	CPU (%)	MEM (%)			
☐	PA-7080	PA-7080		24117127	100992	23368878	30	18	13	0	18/18	2/8
☐	[redacted]	PA-5220	Active Primary	0	0	0	0	13	14	0	8/8	2/2
☐	[redacted]	PA-5220	Active Secondary	1	0	0	0	1	10	0	8/8	2/2
☐	PA-3260	PA-3260		8999	12658	63772	7	22	23	11329	3/3	2/2

그림 **1:** 이탈 메트릭의 예

Panorama에 대한 자세한 디바이스 상태

모든 디바이스 탭 또는 편차 디바이스 탭에서 디바이스 이름을 클릭하여 개별 방화벽의 자세한 디바이스 상태 기록을 볼 수 있습니다. 상세 디바이스 보기는 시간 필터를 사용하여 상태 기록을 제공하고 디바이스와 연결된 메타데이터를 표시합니다. 디바이스 상태 정보는 시간 추세 데이터의 그래픽 표현을 제공하기 위해 가능한 경우 표 또는 위젯으로 표시됩니다.

세부 디바이스 보기 관리

방화벽과 관련된 설명 메타데이터와 함께 세부 디바이스 보기에는 자세한 방화벽 상태 정보가 표시됩니다. 해당되는 경우 위젯에 대한 추가 옵션에 대해 설정()을 구성하거나 위젯을 확대하려면 패널 최대화()를 구성할 수 있습니다.

필드	설명
행위	
시간 필터	드롭다운에서 디바이스 상태 기록을 보려면 시간 필터를 선택합니다. 지난 **12**시간, **24**시간, **7**일, **15**일, **30**일 또는 **90**일을 선택할 수 있습니다.
평균 표시	모든 시간 추세 위젯에 표시되는 평균 및 표준 분포를 선택합니다. 없음, 지난 **24**시간, **7**일 또는 **15**일을 선택할 수 있습니다.
새로 고침	표시된 정보를 최신 데이터로 새로 고칩니다.
PDF 인쇄	현재 표시된 탭의 PDF를 생성합니다.

필드	설명
	다운로드 위치를 선택한 다음 *PDF*에 액세스하려면 팝업을 활성화해야 합니다.
시스템 정보	
시스템 정보	디바이스와 연결된 메타데이터: IP 주소, 소프트웨어 버전, 바이러스 백신 버전, HA 상태, 일련번호, 앱 및 위협 버전, Wildfire 버전, VSYS 모드, 모델 및 디바이스 모드.

세션

세션 탭에는 방화벽을 통과하는 세션 정보가 표시됩니다. 이 정보는 6개의 개별 그래프로 표시됩니다.

필드	설명
처리량	초당 킬로비트(Kbps)로 측정된 시간 경과에 따른 데이터 처리량(5분 평균)입니다.
세션 수	시간 경과에 따른 총 세션 수(5분 평균).
초당 연결	시간 경과에 따른 디바이스의 총 CPS(평균 5분).
초당 패킷 수	디바이스를 통과한 초당 총 패킷(5분 동안 평균)입니다.
글로벌 세션 테이블 활용(PA-7000 및 PA-5200 어플라이언스만 해당)	글로벌 세션 테이블이 있는 방화벽에 대한 시간 경과에 따른 글로벌 세션 테이블의 백분율(5분 동안 평균).
세션 테이블 활용	시간에 대한 방화벽의 각 데이터플레인에 대한 세션 테이블 사용량의 백분율을 표시합니다(5분 동안 평균).
SSL 복호화 세션 정보	시간 경과에 따른 복호화된 SSL 세션 수를 표시합니다(5분 동안 평균).
SSL 프록시 세션 활용	시간 경과에 따른 프록시 세션의 사용률을 표시합니다(5분 동안 평균).

환경

환경 탭에는 전원 공급 디바이스, 팬 트레이 및 디스크 드라이브와 같은 하드웨어의 존재, 상태 및 작동 조건이 표시됩니다. 이 탭은 하드웨어 기반 방화벽에 대해서만 표시됩니다.

필드	설명
팬 상태	각 팬 트레이에 있는 팬의 존재, 현재 상태, RPM 및 마지막 오류를 표시합니다. 팬 상태는 *A*/*B*로 표시됩니다. 여기서 *A*는 정상 작동 중인 팬 수이고 *B*는 방화벽의 총 팬 수입니다. 가상 방화벽은 `N/A`를 표시합니다.
전원 공급 디바이스	존재, 현재 상태 및 마지막 실패 타임스탬프를 표시합니다. 전원 공급 디바이스 상태는 *A*/*B*로 표시됩니다. 여기서 *A*는 정상 작동 중인 전원 공급 디바이스의 수이고 *B*는 디바이스의 총 전원 공급 디바이스 수입니다. 가상 방화벽은 `N/A`를 표시합니다.
열 상태	디바이스의 각 슬롯과 관련된 열 경보가 있는지의 여부를 표시합니다. 활성 경보가 있는 경우 방화벽은 여기에 정확한 온도 및 위치와 관련된 보다 구체적인 정보도 표시합니다.
시스템 디스크 상태	루트, pancfg, panlogs 및 panrepo 마운트에 대한 사용 가능, 사용 및 활용률을 표시합니다. 시스템 디스크 상태는 RAID가 활성화된 방화벽의 디스크 이름, 크기 및 RAID 상태도 표시합니다.

인터페이스

Interfaces(인터페이스) 탭에는 방화벽의 모든 물리적 인터페이스에 대한 상태 및 통계가 표시됩니다.

필드	설명
인터페이스 이름	인터페이스의 이름입니다. 인터페이스를 선택하여 선택한 인터페이스에 대한 비트 전송률, 초당 패킷 수, 오류 및 삭제 그래프를 봅니다.
상태	인터페이스 상태: `AdminUp`, `Admin Down`, `OperationalUp` 또는 `Operational Down`.
비트 전송률	수신 및 전송된 데이터의 비트 전송률(bps)을 표시합니다.
초당 패킷 수	수신 및 전송된 데이터의 초당 패킷 수를 표시합니다.
오류	수신 및 전송된 데이터의 오류 수를 표시합니다.
드롭	수신 및 전송된 데이터에 대해 끊어진 연결 수를 표시합니다.

로깅

로깅 탭에는 관리 방화벽 간의 로깅 속도와 연결이 표시됩니다.

필드	설명
로깅 속도	디바이스가 Panorama 또는 Log Collector에 로그를 포워딩하는 1분 평균 속도를 표시합니다.
로깅 연결	활성 또는 비활성 상태를 포함하여 사용 가능한 모든 로그 포워딩 연결을 표시합니다.
외부 로그 포워딩	다양한 유형의 외부 로그 포워딩 메서드에 대한 전송, 삭제 및 평균 포워딩 속도(초당 로그)를 표시합니다.

리소스

리소스 탭에는 방화벽에 대한 CPU 및 메모리 통계가 표시됩니다.

필드	설명
Management Plane(MP) 메모리	Management Plane(MP) 메모리의 시간 추세, 5분 평균을 백분율로 표시합니다.
패킷 버퍼	패킷 버퍼 사용률의 시간 추세, 5분 평균을 백분율로 표시합니다. 다중 데이터 플레인 시스템에서 이 디스플레이에는 다양한 데이터 플레인, CPU 및 다양한 색상의 패킷 버퍼가 포함됩니다.
패킷 디스크립터	패킷 디스크립터 사용률의 시간 추세, 5분 평균을 백분율로 표시합니다. 다중 데이터 플레인 시스템에서 이 디스플레이에는 다양한 데이터 플레인, CPU 및 다양한 색상의 패킷 버퍼가 포함됩니다.
CPU Management Plane(MP)	Management Plane(MP) CPU의 시간 추세, 5분 평균을 표시합니다.
CPU 데이터 플레인	데이터플레인 CPU의 시간 추세, 5분 평균 코어당 사용률을 표시합니다. 여러 데이터 플레인이 있는 시스템의 경우 선택기를 볼 데이터플레인을 선택할 수 있습니다.
마운트	디바이스 시스템 파일 정보를 표시합니다. 이 표시에는 마운트 이름, 할당됨(KB), 사용됨(KB) 및 사용 가능(KB) 공간과 활용률이 포함됩니다.

고가용성

고가용성 탭에는 방화벽 및 해당 HA 피어의 HA 상태가 표시됩니다. 상단 위젯은 디바이스 및 해당 피어의 구성 및 콘텐츠 버전을 표시합니다. 하단 위젯은 이전 HA 페일오버에 대한 정보와 장애가 발생한 방화벽을 포함하여 이와 관련된 이유를 제공합니다.

Panorama > 템플릿

디바이스 및 네트워크 탭을 통해 템플릿 또는 템플릿 스택(template stack)(템플릿 조합)을 사용하여 유사한 설정이 필요한 여러 방화벽에 공통 기본 구성을 배포할 수 있습니다. Panorama로 방화벽 구성을 관리할 때 디바이스 그룹(공유 정책 및 개체 관리)과 템플릿(공유 디바이스 및 네트워크 설정 관리)의 조합을 사용합니다.

템플릿 또는 템플릿 스택(template stack)을 만들기 위한 대화 상자에서 사용할 수 있는 설정 외에도 **Panorama** > **Templates**는 다음 열을 표시합니다.

- 유형 - 나열된 항목을 템플릿 또는 템플릿 스택(template stack)으로 식별합니다.
- 스택 - 템플릿 스택(template stack)에 할당된 템플릿을 나열합니다.

무엇을 알고 싶습니까?	참조:
템플릿 추가, 복사, 편집 또는 삭제	템플릿
템플릿 스택 추가, 편집 또는 삭제	템플릿 스택(template stack)
더 찾고 계십니까?	템플릿 및 템플릿 스택(template stack)
	템플릿 및 템플릿 스택(template stack) 관리

템플릿

Panorama는 최대 1,024개의 템플릿을 지원합니다. 다음 표에 설명된 대로 템플릿을 추가하고 설정을 구성할 수 있습니다. 템플릿을 생성한 후 템플릿 스택(template stack)을 구성하고 템플릿과 방화벽을 템플릿 스택(template stack)에 추가해야 방화벽을 관리할 수 있습니다. 템플릿을 구성한 후 Panorama에서 변경 사항을 커밋해야 합니다(Panorama 커밋 작업 참조).

템플릿을 삭제해도 *Panorama*가 방화벽에 푸시한 값은 삭제되지 않습니다.

템플릿 설정	설명
이름	템플릿 이름을 입력합니다(최대 63자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈, 마침표 및 밑줄만 포함할 수 있습니다. 디바이스 및 네트워크 탭에서 이 이름은 템플릿 드롭다운에 나타납니다. 이 탭에서 수정하는 설정은 선택한 템플릿에만 적용됩니다.
설명	템플릿에 대한 설명을 입력합니다.

템플릿 스택(template stack)

템플릿 스택(template stack)을 구성하거나 템플릿 스택(template stack)에 템플릿을 할당할 수 있습니다. 템플릿 스택(template stack)에 방화벽을 할당하면 모든 설정을 모든 템플릿에 개별적으로 추가하는 대신 필요한 모든 설정을 방화벽에 푸시할 수 있습니다. Panorama는 최대 1,024개의 스택을 지원합니다. 스택 추가를 통해 새 템플릿 스택(template stack)을 생성하고 다음 표에 설명된 대로 설정을 구성할 수 있습니다. 템플릿 스택(template stack)을 구성한 후 Panorama에서 변경 사항을 커밋해야 합니다(Panorama 커밋 작업 참조). 또한 스택에 할당된 방화벽의 네트워크 및 디바이스 설정을 구성한 후 템플릿 커밋을 수행하고 설정을 방화벽에 푸시해야 합니다.

템플릿 스택*(template stack)*을 삭제하거나 템플릿 스택*(template stack)*에서 방화벽을 제거해도 *Panorama*가 이전에 해당 방화벽에 푸시한 값은 삭제되지 않습니다. 그러나 템플릿 스택*(template stack)*에서 방화벽을 제거하면 *Panorama*는 더 이상 해당 방화벽에 새 업데이트를 푸시하지 않습니다.

템플릿 스택**(template stack)** 설정	설명
이름	스택 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자로 시작해야 하며 문자, 숫자 및 밑줄만 포함할 수 있습니다. 디바이스 및 네트워크 탭에서 템플릿 드롭다운에는 스택 이름과 할당된 템플릿이 표시됩니다.
설명	스택에 대한 설명을 입력합니다.
소프트웨어 디바이스가 Panorama에 등록되면 자동으로 콘텐츠 푸시	최신 콘텐츠 업데이트를 방화벽에 자동으로 푸시하려면 Panorama에서 VM 시리즈 또는 CN 시리즈 방화벽을 온보딩할 때 이 옵션을 활성화하십시오.
템플릿	스택에 포함할 각 템플릿을 추가합니다(최대 8개). 템플릿에 중복 설정이 있는 경우 Panorama는 할당된 방화벽에 설정을 푸시할 때 목록에서 상위에 있는 템플릿의 설정만 푸시합니다. 예를 들어, Template_A가 목록에서 Template_B 위에 있고 두 템플릿이 모두 ethernet1/1 인터페이스를 정의하는 경우 Panorama는 Template_B가 아니라 Template_A에서 ethernet1/1 정의를 푸시합니다. 목록에서 템플릿의 순서를 변경하려면 템플릿을 선택한 다음 위로 이동 또는 아래로 이동합니다. *Panorama*는 스택의 템플릿 조합을 검증하지 않으므로 잘못된 관계를 방지하기 위해 템플릿 순서를 계획하십시오.
디바이스	스택에 추가할 각 방화벽을 선택합니다.

템플릿 스택(**template stack**) 설정	설명
	방화벽 목록이 길면 플랫폼, 디바이스 그룹, 태그 및 **HA** 상태별로 목록을 필터링할 수 있습니다. 일치하지 않는 모드(*VPN* 모드, 다중 가상 시스템 모드 또는 작동 모드)가 있는 방화벽을 동일한 스택에 할당할 수 있습니다. *Panorama*는 해당 모드를 지원하는 방화벽에만 모드별 설정을 푸시합니다.
모두 선택	목록에서 모든 방화벽을 선택합니다.
모두 선택 해제	목록의 모든 방화벽을 선택 취소합니다.
그룹 HA 피어	고가용성(HA) 피어인 방화벽을 그룹화합니다. 이를 통해 HA 구성이 있는 방화벽을 쉽게 식별할 수 있습니다. 템플릿 스택(template stack)에서 설정을 푸시할 때 각 방화벽에 개별적으로 푸시하는 대신 그룹화된 쌍으로 푸시할 수 있습니다.
필터 선택	특정 방화벽만 표시하려면 방화벽을 선택한 다음 선택된 필터를 선택합니다.
사용자 ID 마스터 디바이스	Panorama를 매핑을 위한 User-ID 마스터 디바이스로 구성합니다.
클라우드 ID 엔진	Cloud Identity Engine에서 구성한 인증 프로파일을 사용하여 사용자를 인증하는 Cloud Identity Engine 인스턴스를 추가합니다.
템플릿	사전 구성된 템플릿을 추가하거나 삭제합니다. 우선 순위를 변경하려면 위로 이동 또는 아래로 이동 템플릿을 사용합니다. 맨 위에 있는 템플릿이 가장 높은 우선 순위를 갖습니다.

Panorama > 템플릿 > 템플릿 변수

- 새 템플릿 변수 생성
- 기존 템플릿 변수 편집
- 디바이스에서 변수 정의 생성 또는 편집

템플릿 및 템플릿 스택(template stack)에 대한 변수(**Panorama** > 템플릿)를 정의하거나 개별 디바이스에 대한 기존 변수를 편집할 수 있습니다(**Panorama** > **Managed Devices** > **Summary**). 변수는 Panorama를 사용하여 방화벽 구성을 관리할 때 유연성과 재사용성을 제공하는 템플릿 또는 템플릿 스택(template stack)에 정의된 구성 구성 요소입니다. 변수를 사용하여 다음을 바꿀 수 있습니다.

- 구성의 모든 영역에 있는 IP 주소(IP 넷마스크, IP 범위 및 FQDN 포함).

- IKE 게이트웨이 구성(인터페이스) 및 HA 구성(그룹 ID)의 인터페이스.
- SD-WAN 구성의 구성 요소(AS 번호, QoS 프로파일, 최대 이그레스(egress), 링크 태그).

템플릿 스택(template stack)에 방화벽을 추가하면 템플릿 또는 템플릿 스택(template stack)에 대해 생성한 변수가 자동으로 상속됩니다.

템플릿 변수 정보	설명
이름	변수 정의의 이름입니다.
템플릿(디바이스 및 템플릿 스택(template stack))	변수 정의가 속한 템플릿의 이름을 표시합니다.
유형	변수 정의 유형을 표시합니다. • **IP** 넷마스크 - 고정 IP 또는 네트워크 주소를 정의합니다. • **IP** 범위 - IP 범위를 정의합니다. 예: 192.168.1.10-192.168.1.20. • **FQDN** - 정규화된 도메인 이름을 정의합니다. • 그룹 **ID** - 고가용성 그룹 ID를 정의합니다. 자세한 내용은 능동형/수동형 HA에 대한 구성 지침을 참조하십시오. • 디바이스 우선 순위 - 디바이스 우선 순위를 정의하여 방화벽이 능동형-수동형 고가용성(HA) 구성에서 능동형 역할을 가정해야 하는 기본 설정을 나타냅니다. • 디바이스 **ID** - 능동형-능동형 고가용성(HA) 구성에서 디바이스 우선 순위 값을 할당하는 데 사용할 디바이스 ID를 정의합니다. • 인터페이스 - 방화벽에서 방화벽 인터페이스를 정의합니다. IKE 게이트웨이 구성에만 사용할 수 있습니다. • **AS** 번호 - BGP 구성에서 사용할 자율 시스템 번호를 정의합니다. • **QoS** 프로파일 - QoS 구성에 사용할 QoS(서비스 품질) 프로파일을 정의합니다. • 최대 이그레스**(egress)** - QoS 프로파일 구성에 사용할 이그레스(egress) 최대 값을 정의합니다. • 링크 태그 - SD-WAN 구성에서 사용할 링크 태그를 정의합니다.
값	변수 정의에 대해 구성된 값을 표시합니다.
추가(템플릿 및 템플릿 스택(template stack))	새 템플릿 변수 정의를 추가합니다.
삭제	기존 템플릿 변수 정의를 삭제합니다.

템플릿 변수 정보	설명
복사	기존 템플릿 변수 정의를 복사합니다.
재정의(템플릿 스택(template stack) 및 디바이스)	템플릿 스택(template stack) 또는 디바이스에서 상속된 기존 템플릿 변수 정의를 재정의합니다. 변수 유형이나 이름을 변경할 수 없으며 디바이스별 변수를 재정의할 수 없습니다.
되돌리기(템플릿 스택(template stack) 및 디바이스)	템플릿 스택(template stack) 또는 디바이스 수준에서 재정의된 값을 지우려면 재정의된 변수를 원래 템플릿 변수 정의로 되돌립니다.
디바이스에서만 사용되는 값 가져오기(디바이스만)	방화벽에서 사용된 값으로 선택한 변수를 채웁니다. Panorama가 값을 검색할 수 있으려면 템플릿 또는 템플릿 스택(template stack) 변수가 이미 정의되어 있고 방화벽으로 푸시되어야 합니다. 방화벽에서 불러온 값은 템플릿 또는 템플릿 스택(template stack) 변수를 재정의하여 디바이스별 변수를 생성합니다. 변수 정의가 방화벽에 푸시되지 않은 경우 Panorama는 해당 변수에 대해 ## ## # ##을 반환합니다.

새 템플릿 변수 생성

새 템플릿 변수 정의를 추가합니다.

새 템플릿 변수 정의 정보	설명
이름	변수 정의의 이름을 지정합니다. 모든 변수 정의 이름은 달러 기호("$") 문자로 시작해야 합니다.
유형	변수 정의 유형 선택: **IP** 넷마스크, **IP** 범위, **FQDN**, 그룹 **ID**, 디바이스 우선 순위, 디바이스 **ID**, 인터페이스, **AS** 번호, **QoS** 프로파일, 최대 이그레스**(egress)** 또는 링크 태그.
값	변수 정의에 대해 원하는 값을 입력합니다.

기존 템플릿 변수 편집

변수가 생성된 후 언제든지 템플릿 또는 템플릿 스택(template stack)에 대한 템플릿 변수 정의를 편집할 수 있습니다(**Panorama** > **Templates**). 템플릿 변수를 관리하여 변수를 선택한 다음 필요에 따라 사용 가능한 값을 편집합니다.

디바이스에서 변수 정의 생성 또는 편집

Panorama > **Managed Devices** > **Summary**로 이동하여 변수 정의를 생성하거나 Panorama 템플릿 또는 템플릿 스택(template stack)에서 푸시된 템플릿 변수를 재정의합니다. 템플릿 변수에는 다음이 포함됩니다.

- 구성의 모든 영역에 있는 IP 주소(IP 넷마스크, IP 범위 또는 FQDN).
- IKE 게이트웨이 구성(인터페이스) 또는 HA 구성(그룹 ID)의 인터페이스.
- SD-WAN 구성의 구성 요소(AS 번호, QoS 프로파일, 최대 이그레스(egress), 링크 태그).

디바이스 변수를 생성하면 개별적으로 다시 생성하는 대신 동일한 템플릿 스택(template stack)의 디바이스에서 재정의된 디바이스별 변수를 복사할 수 있습니다. 기본적으로 모든 변수 정의는 템플릿 또는 템플릿 스택(template stack)에서 상속되며 재정의만 가능합니다. 개별 디바이스에 대한 새 변수 정의를 삭제하거나 생성할 수 없습니다.

템플릿 스택(template stack)의 기존 디바이스에서 변수 정의를 복사하여 디바이스 변수 정의를 생성하거나 기존 디바이스 변수 정의를 편집합니다.

Panorama > 디바이스 그룹

디바이스 그룹은 회사의 지사 그룹이나 개별 부서를 관리하는 방화벽과 같이 그룹으로 관리하려는 가상 시스템과 방화벽으로 구성됩니다. Panorama는 정책을 적용할 때 이러한 그룹을 단일 단위로 취급합니다. 방화벽은 하나의 디바이스 그룹에만 속할 수 있지만 가상 시스템은 Panorama에서 별개의 엔터티이므로 방화벽 내의 가상 시스템을 다른 디바이스 그룹에 할당할 수 있습니다.

공유 위치 아래에 있는 최대 4개 수준의 트리 레이어 구조에서 디바이스 그룹을 중첩하여 방화벽 네트워크 전체에서 정책을 관리하기 위한 계층적 접근 방식을 구현할 수 있습니다. 하위 수준에서 디바이스 그룹은 하위 수준 디바이스 그룹이 정책 및 개체를 상속하는 상위 수준(집합적으로 상위라고 함)에 상위, 조부모 요소 및 증조부모 요소 디바이스 그룹을 가질 수 있습니다. 최상위 수준에서 디바이스 그룹에는 자식 요소, 손자 요소 및 증손자 요소 디바이스 그룹(집합적으로 하위 항목이라고 함)이 있을 수 있습니다. **Panorama** > **Device Groups**를 선택하면 이름 열에 이 디바이스 그룹 레이어가 표시됩니다.

디바이스 그룹을 추가, 편집 또는 삭제한 후 Panorama 커밋 및 디바이스 그룹 커밋을 수행합니다(Panorama 커밋 작업 참조). 그런 다음 Panorama는 구성 변경 사항을 디바이스 그룹에 할당된 방화벽으로 푸시합니다. Panorama는 최대 1,024개의 디바이스 그룹을 지원합니다.

디바이스 그룹을 구성하려면 하나를 추가하고 다음 표에 설명된 대로 설정을 구성합니다.

디바이스 그룹 설정	설명
이름	그룹을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 전체 디바이스 그룹 레이어에서 고유해야 하며 문자, 숫자, 공백, 마침표, 하이픈 및 밑줄만 포함할 수 있습니다.
설명	디바이스 그룹에 대한 설명을 입력합니다.
디바이스	디바이스 그룹에 추가할 각 방화벽을 선택합니다. 방화벽 목록이 길면 디바이스 상태, 플랫폼, 템플릿 또는 태그별로 필터링할 수 있습니다. 필터 섹션에는 이러한 각 카테고리에 대한 관리 방화벽 수가 괄호 안에 표시됩니다. 디바이스 그룹의 목적이 순전히 조직적인 것이라면(즉, 다른 디바이스 그룹을 포함하기 위한) 방화벽을 할당할 필요가 없습니다.
모두 선택	목록에서 모든 방화벽과 가상 시스템을 선택합니다.
모두 선택 해제	목록에서 모든 방화벽 및 가상 시스템을 선택 취소합니다.
그룹 HA 피어	고가용성(HA) 구성에서 피어인 방화벽을 그룹화하려면 선택합니다. 그런 다음 목록에는 활성(또는 능동형/능동형 구성의 능동형-기본) 방화벽이 먼저 표시되고 괄호 안에 수동(또는 능동형/능동형 구성의 능동형-보조) 방화벽이 표시됩니다. 이를 통

디바이스 그룹 설정	설명
	해 HA 모드에 있는 방화벽을 쉽게 식별할 수 있습니다. 공유 정책을 푸시할 때 개별 피어 대신 그룹화된 쌍으로 푸시할 수 있습니다. 능동형/수동형 구성의 *HA* 피어의 경우 두 방화벽 또는 해당 가상 시스템을 동일한 디바이스 그룹에 추가하는 것을 고려하십시오. 이렇게 하면 구성을 두 피어에 동시에 푸시할 수 있습니다.
필터 선택	디바이스 목록에 특정 방화벽만 표시하려면 방화벽을 선택한 다음 선택 필터를 선택합니다.
상위 디바이스 그룹	정의하는 디바이스 그룹과 관련하여 레이어 구조에서 바로 위에 있는 디바이스 그룹(또는 공유 위치)을 선택합니다(기본값은 공유임).
마스터 디바이스	사용자명 및 사용자 그룹을 기반으로 정책 규칙 및 보고서를 구성하려면 마스터 디바이스를 선택해야 합니다. 이것은 Panorama가 사용자명, 사용자 그룹 이름 및 사용자명-그룹 매핑 정보를 수신하는 방화벽입니다. 마스터 디바이스를 변경하거나 없음으로 설정하면 *Panorama*는 해당 방화벽에서 수신한 모든 사용자 및 그룹 정보를 잃게 됩니다.
마스터 디바이스에서 사용자 및 그룹 저장	이 옵션은 마스터 디바이스를 선택한 경우에만 표시됩니다. 이 옵션을 사용하면 Panorama가 마스터 디바이스에서 수신한 사용자명, 사용자 그룹 이름 및 사용자명-그룹 매핑 정보를 로컬로 저장할 수 있습니다. 로컬 스토리지를 활성화하려면 **Panorama** > **Setup** > **Management**를 선택한 다음 Panorama 설정을 편집하고 그룹에 대한 보고 및 필터링 활성화도 선택해야 합니다.
동적으로 추가된 디바이스 속성 - 새 디바이스가 디바이스 그룹에 추가되면 Panorama는 지정된 인증 코드와 PAN-OS 소프트웨어 버전을 새 디바이스에 동적으로 적용합니다. 이는 디바이스 그룹이 Panorama의 NSX 서비스 정의와 연결된 후에만 표시됩니다.	
인증 코드	이 디바이스 그룹에 추가된 디바이스에 적용할 인증 코드를 입력합니다.
SW 버전	이 디바이스 그룹에 추가된 디바이스에 적용할 소프트웨어 버전을 선택합니다.

Panorama > 관리형 수집기

Panorama 관리 서버(M-시리즈 어플라이언스 또는 Panorama 모드의 Panorama 가상 어플라이언스)는 전용 로그 수집기(M-시리즈 어플라이언스 또는 로그 수집기 모드의 Panorama 가상 어플라이언스)를 관리할 수 있습니다. 각 Panorama 관리 서버에는 방화벽에서 직접 수신하는 로그를 처리하기 위해 사전 정의된 로컬 로그 수집기(기본 이름)도 있습니다. (레거시 모드의 Panorama 가상 어플라이언스는 전용 로그 수집기를 사용하지 않고 방화벽에서 직접 수신한 로그를 저장합니다.)

Dedicated Log Collector를 관리하기 위해 Panorama를 사용하려면 Log Collector를 관리되는 수집기로 추가하십시오.

무엇을 알고 싶습니까?	참조:
로그 수집기 정보 표시	로그 수집기 정보
로그 수집기 추가, 편집 또는 삭제	로그 수집기 구성
Log Collector에서 Panorama 소프트웨어 업데이트	전용 로그 수집기를 위한 소프트웨어 업데이트
더 찾고 계십니까?	중앙 집중식 로깅 및 보고
	관리형 수집기 구성

로그 수집기 정보

Panorama > **Managed Collectors**를 선택하여 로그 수집기에 대한 다음 정보를 표시합니다. 추가 매개변수는 로그 수집기 구성 중에 구성할 수 있습니다.

로그 수집기 정보	설명
수집기 이름	이 로그 수집기를 식별하는 이름입니다. 이 이름은 로그 수집기 호스트 이름으로 표시됩니다.
일련번호	Log Collector로 작동하는 Panorama 어플라이언스의 일련번호입니다. Log Collector가 로컬인 경우 Panorama 관리 서버의 일련번호입니다.
소프트웨어 버전	Log Collector에 설치된 Panorama 소프트웨어 릴리스입니다.
IP 주소	Log Collector에 있는 관리 인터페이스의 IP 주소입니다.

로그 수집기 정보	설명
연결됨	Log Collector와 Panorama 간의 연결 상태입니다.
구성 상태/세부 정보	Log Collector의 구성이 Panorama와 동기화되었는지의 여부를 나타냅니다.
실행 시간 상태/세부 정보	이 로그 수집기와 수집기 그룹의 다른 로그 수집기 간의 연결 상태입니다.
로그 재배포 상태	특정 작업(예: 디스크 추가)은 Log Collector가 디스크 쌍 간에 로그를 재배포하도록 합니다. 이 열은 재분배 프로세스의 완료 상태를 백분율로 나타냅니다.
마지막 커밋 상태	로그 수집기에서 수행된 마지막 수집기 그룹 커밋의 실패 또는 성공 여부를 나타냅니다.
상태	로그 수집 프로세스의 상태를 기반으로 한 로그 수집기 상태를 나타냅니다. 로그 수집기가 정상이면  을(를) 표시하고 하나 이상의 로그 수집 프로세스에서 상태가 저하되면  을(를) 표시합니다. • **logd** - 관리되는 방화벽에서 수신한 로그를 수집하고 수집된 로그를 vldmgr로 전송하는 프로세스입니다. • **vldmgr** - vld 프로세스 관리를 담당하는 프로세스입니다. • **vlds** - 개별 로깅 디스크 관리, 로깅 디스크에 로그 쓰기, ElasticSearch에 로그 수집을 담당하는 프로세스입니다. • **es**- Log Collector에서 실행되는 ElasticSearch 프로세스입니다.
통계	로그 수집기 구성을 완료한 후 통계를 클릭하여 디스크 정보, CPU 성능 및 평균 로그 속도(로그/초)를 확인합니다. 검토 중인 로그 범위를 더 잘 이해하기 위해 Log Collector가 수신한 가장 오래된 로그에 대한 정보를 볼 수도 있습니다.  중앙 모니터링을 위해 SNMP 관리자를 사용하는 경우 *panLogCollector MIB*에서 로깅 통계를 볼 수도 있습니다.

로그 수집기 구성

Panorama > **Managed Collectors**를 선택하여 로그 수집기를 관리합니다. 새 Log Collector를 관리형 수집기로 추가할 때 구성하는 설정은 Log Collector의 위치와 Panorama를 고가용성(HA) 구성으로 배포했는지의 여부에 따라 달라집니다.

- 전용 로그 수집기 - 로그 수집기를 추가하면 처음에는 인터페이스 탭이 표시되지 않습니다. 로그 수집기의 일련번호(수집기 **S/N**)를 입력하고 확인을 클릭한 다음 로그 수집기를 편집하여 인터페이스 설정을 표시해야 합니다.
- 단독(비 **HA**) 또는 활성**(HA) Panorama** 관리 서버에 로컬인 기본 로그 수집기 - 파노라마 관리 서버의 일련 번호(**Collector S/N**)를 입력한 후, Collector 대화 상자에는 디스크, 통신 설정 및 일반 설정의 하위 집합만 표시됩니다. Log Collector는 Panorama 관리 서버의 구성에서 다른 모든 설정에 대한 값을 가져옵니다.
- (HA만 해당) 수동 **Panorama** 관리 서버에 로컬인 기본 로그 수집기 - Panorama는 이 로그 수집기를 원격으로 취급하므로 전용 로그 수집기를 구성할 때와 같이 구성해야 합니다.

로그 수집기를 구성하는 전체 절차에는 추가 작업이 필요합니다.

무엇을 찾고 계신가요?	참조:
Log Collector를 식별하고 Panorama 관리 서버 및 외부 서비스에 대한 연결을 정의합니다.	일반 로그 수집기 설정
Log Collector CLI에 대한 액세스를 구성합니다.	로그 수집기 인증 설정
Dedicated Log Collector가 관리 트래픽, Collector Group 통신 및 로그 수집에 사용하는 인터페이스를 구성합니다.	로그 수집기 인터페이스 설정
방화벽에서 수집한 로그를 저장하는 RAID 디스크를 구성합니다.	로그 수집기 RAID 디스크 설정
Windows User-ID 에이전트로 인증하도록 로그 수집기를 구성합니다.	연결 보안
Panorama, 기타 로그 수집기 및 방화벽과의 통신을 위한 보안 설정을 구성합니다.	통신 설정

일반 로그 수집기 설정

- Panorama > 관리형 수집기 > 일반

다음 표에 설명된 대로 설정을 구성하여 Log Collector를 식별하고 Panorama 관리 서버, DNS 서버 및 NTP 서버에 대한 연결을 정의합니다.

로그 수집기 일반 설정	설명
수집기 S/N	(필수) Log Collector로 작동하는 Panorama 어플라이언스의 일련번호를 입력합니다. Log Collector가 로컬인 경우 Panorama 관리 서버의 일련번호를 입력합니다.
수집기 이름	이 로그 수집기를 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다. 이 이름은 로그 수집기 호스트 이름으로 표시됩니다.
Secure Syslog용 인바운드 인증서	관리되는 수집기가 Traps™ ESM 서버에서 로그를 안전하게 수집하는 데 사용해야 하는 인증서를 선택하십시오. Panorama/Managed Collector는 Traps ESM(클라이언트)이 로그를 보내는 서버이기 때문에 이 인증서를 인바운드 인증서라고 합니다. 로그 수집 프로파일의 전송 프로토콜이 **SSL**인 경우 인증서가 필요합니다.
보안 Syslog용 인증서	syslog를 외부 Syslog 서버로 안전하게 포워딩하기 위한 인증서를 선택합니다. 인증서에는 **Secure Syslog**용 인증서 옵션이 선택되어 있어야 합니다(방화벽 및 Panorama 인증서 관리 참조). 이 Log Collector를 포함하는 Collector Group에 Syslog 서버 프로파일을 할당하는 경우(Panorama > Collector Groups, **Panorama** > **Collector Groups** > **Collector** 로그 포워딩 참조), 서버 프로파일의 전송 프로토콜은 **SSL**이어야 합니다(디바이스 > 서버 프로파일 > Syslog 참조).
Panorama 서버 IP	이 Log Collector를 관리하는 Panorama 관리 서버의 IP 주소를 지정하십시오.
Panorama 서버 IP 2	Panorama 관리 서버가 고가용성(HA) 구성으로 배포된 경우 보조 피어의 IP 주소를 지정합니다.
도메인	로그 수집기의 도메인 이름을 입력합니다.
기본 DNS 서버	기본 DNS 서버의 IP 주소를 입력합니다. Log Collector는 DNS 쿼리(예: Panorama 관리 서버 찾기)에 이 서버를 사용합니다.
보조 DNS 서버	(선택 사항) 기본 서버를 사용할 수 없는 경우 사용할 보조 DNS 서버의 IP 주소를 입력합니다.

로그 수집기 일반 설정	설명
기본 NTP 서버	기본 NTP 서버의 IP 주소 또는 호스트 이름(있는 경우)을 입력합니다. NTP 서버를 사용하지 않는 경우 Log Collector 시간을 수동으로 설정할 수 있습니다.
보조 NTP 서버	(선택 사항) 기본 서버를 사용할 수 없는 경우 사용할 보조 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다.
시간대	로그 수집기의 시간대를 선택합니다.
위도	로그 수집기의 위도(-90.0 ~ 90.0)를 입력합니다. 트래픽 및 위협 맵은 앱 범위에 대한 위도를 사용합니다.
경도	Log Collector의 경도(-180.0 ~ 180.0)를 입력합니다. 트래픽 및 위협 맵은 앱 범위에 경도를 사용합니다.

로그 수집기 인증 설정

- Panorama > 관리형 수집기 > 인증

Log Collector 모드(Dedicated Log Collector)의 M 시리즈 어플라이언스 또는 Panorama 가상 어플라이언스에는 웹 인터페이스가 없으며, CLI만 가능합니다. Panorama 관리 서버를 사용하여 Dedicated Log Collector에서 대부분의 설정을 구성할 수 있지만 일부 설정에는 CLI 액세스가 필요합니다. CLI 액세스에 대한 인증 설정을 구성하려면 다음 표에 설명된 대로 설정을 구성하십시오.

로그 수집기 인증 설정	설명
인증 프로파일	Dedicated Log Collector 또는 Panorama 관리자의 로그인 자격 증명을 확인하는 인증 서비스를 정의하려면 구성된 인증 프로파일을 선택합니다.
실패한 시도	Dedicated Log Collector가 관리자를 잠그기 전에 CLI에서 허용하는 로그인 시도 실패 횟수를 입력합니다(범위는 0~10, 기본값은 10). 로그인 시도를 제한하면 무차별 대입 공격으로부터 WildFire 어플라이언스를 보호하는 데 도움이 됩니다. 0 값은 무제한 로그인 시도를 지정합니다.

로그 수집기 인증 설정	설명
	실패한 시도를 *0* 이외의 값으로 설정하고 잠금 시간을 *0*으로 두면 다른 관리자가 잠긴 관리자의 잠금을 수동으로 해제할 때까지 관리자가 무기한 잠깁니다. 다른 관리자가 생성되지 않은 경우 *Panorama*에서 실패한 시도 및 잠금 시간 설정을 재구성하고 구성 변경 사항을 로그 수집기로 푸시해야 합니다. 관리자가 잠기지 않도록 하려면 실패한 시도 및 잠금 시간 모두에 대해 기본값(**0**)을 사용하십시오. 악의적인 시스템이 *Dedicated Log Collector*에 로그인하기 위해 무차별 대입 방식을 시도하는 것을 방지하면서 입력 오류의 경우 적절한 재시도 횟수를 수용하려면 실패한 시도 횟수를 *5* 이하로 설정하십시오.
잠금 시간(분)	실패한 시도 제한(범위는 0~60, 기본값은 5)에 도달한 후 전용 로그 수집기가 CLI에 대한 액세스를 차단하는 시간(분)을 입력하십시오. 0 값은 다른 관리자가 계정을 수동으로 잠금 해제할 때까지 잠금이 적용됨을 의미합니다. 실패한 시도를 *0* 이외의 값으로 설정하고 잠금 시간을 *0*으로 두면 다른 관리자가 잠긴 관리자의 잠금을 수동으로 해제할 때까지 관리자가 무기한 잠깁니다. 다른 관리자가 생성되지 않은 경우 *Panorama*에서 실패한 시도 및 잠금 시간 설정을 재구성하고 구성 변경 사항을 로그 수집기로 푸시해야 합니다. 관리자가 잠기지 않도록 하려면 실패한 시도 및 잠금 시간 모두에 대해 기본값(**0**)을 사용하십시오. 악의적인 행위자의 지속적인 로그인 시도를 방지하려면 잠금 시간을 최소 *30*분으로 설정하십시오.
유휴 타임아웃(분)	관리자가 자동으로 로그아웃되기 전에 CLI에서 활동이 없는 최대 시간(분)을 입력합니다(범위는 0~1,440, 기본값은 없음). 값이 0이면 비활성 상태가 자동 로그아웃을 트리거하지 않음을 의미합니다. 관리자가 세션을 열어 둔 경우 권한이 없는 사용자가 *Dedicated Log Collector*에 액세스하지 못하도록 하려면 유휴 시간 제한을 *10*분으로 설정하십시오.
최대 세션 수	관리자가 동시에 열 수 있는 활성 세션 수를 입력합니다. 기본값은 0이며, 이는 Dedicated Log Collector가 동시에 활성 세션을 무제한으로 가질 수 있음을 의미합니다.

로그 수집기 인증 설정	설명
최대 세션 시간	관리자가 자동으로 로그아웃되기 전까지 로그인할 수 있는 시간(분)을 입력합니다. 기본값은 0이며, 이는 관리자가 유휴 상태에서도 무기한으로 로그인할 수 있음을 의미합니다.
로컬 관리자	Dedicated Log Collector에 대한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 Dedicated Log Collector에 고유하며 이 페이지에서 관리됩니다(**Panorama** > **Managed Collectors** > 인증).
Panorama 관리자	Panorama에 구성된 기존 관리자를 가져옵니다. 이러한 관리자는 Panorama에서 생성되고 Dedicated Log Collector로 가져옵니다.

로그 수집기 인터페이스 설정

- Panorama > 관리형 수집기 > 인터페이스

기본적으로 전용 로그 수집기(로그 수집기 모드의 M-시리즈 어플라이언스)는 관리 트래픽, 로그 수집 및 수집기 그룹 통신을 위해 관리(MGT) 인터페이스를 사용합니다. 그러나 Palo Alto Networks는 MGT 인터페이스의 트래픽을 줄이기 위해 로그 수집 및 Collector Group 통신에 대해 별도의 인터페이스를 할당할 것을 권장합니다. 다른 인터페이스에 대한 서브넷보다 더 프라이빗한 MGT 인터페이스에 대해 별도의 서브넷을 정의하여 보안을 향상시킬 수 있습니다. 별도의 인터페이스를 사용하려면 먼저 Panorama 관리 서버에서 인터페이스를 구성해야 합니다(디바이스 > 설정 > 관리 참조). 로그 수집 및 수집기 그룹 통신에 사용할 수 있는 인터페이스는 Log Collector 어플라이언스 모델에 따라 다릅니다. 예를 들어 M-500 어플라이언스에는 다음과 같은 인터페이스가 있습니다. 이더넷1(1Gbps), 이더넷2(1Gbps), 이더넷3(1Gbps), 이더넷4(10Gbps) 및 이더넷5(10Gbps).

인터페이스를 구성하려면 링크를 선택한 다음 다음 표에 설명된 대로 설정을 구성합니다.

MGT 인터페이스 구성을 완료하려면 *IP* 주소, 넷마스크*(IPv4*의 경우*)* 또는 프리픽스 길이*(IPv6*의 경우*)* 및 기본 게이트웨이를 지정해야 합니다. 부분 구성을 커밋하는 경우*(*예*:* 기본 게이트웨이를 생략할 수 있음*)* 향후 구성 변경을 위해 콘솔 포트를 통해서만 방화벽 또는 *Panorama*에 액세스할 수 있습니다.

항상 완전한 *MGT* 인터페이스 구성을 커밋하십시오. *IP* 주소, 넷마스크*(IPv4*의 경우*)* 또는 프리픽스 길이*(IPv6*의 경우*)* 및 기본 게이트웨이를 지정하지 않으면 다른 인터페이스에 대한 구성을 커밋할 수 없습니다.

로그 수집기 인터페이스 설정	설명
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	구성하려면 인터페이스를 활성화해야 합니다. 예외는 기본적으로 활성화되어 있는 MGT 인터페이스입니다.
속도 및 이중	인터페이스에 대한 데이터 속도 및 이중 옵션을 구성합니다. 선택 사항에는 전이중 또는 반이중에서 10Mbps, 100Mbps, 1Gbps 및 10Gbps(Eth4 및 Eth5만 해당)가 포함됩니다. 기본 자동 협상 설정을 사용하여 로그 수집기가 인터페이스 속도를 결정하도록 합니다. 이 설정은 인접 네트워크 장비의 인터페이스 설정과 일치해야 합니다.
IP 주소(IPv4)	네트워크에서 IPv4 주소를 사용하는 경우 인터페이스에 IPv4 주소를 할당합니다.
넷마스크(IPv4)	인터페이스에 IPv4 주소를 할당한 경우 네트워크 마스크(예: 255.255.255.0)도 입력해야 합니다.
기본 게이트웨이(IPv4)	인터페이스에 IPv4 주소를 할당한 경우 기본 게이트웨이에도 IPv4 주소를 할당해야 합니다(게이트웨이는 MGT 인터페이스와 동일한 서브넷에 있어야 함).
IPv6 주소/프리픽스 길이	네트워크에서 IPv6 주소를 사용하는 경우 인터페이스에 IPv6 주소를 할당합니다. 넷마스크를 나타내려면 IPv6 프리픽스 길이(예: 2001:400:f00::1/64)를 입력합니다.
기본 IPv6 게이트웨이	인터페이스에 IPv6 주소를 할당한 경우 기본 게이트웨이에도 IPv6 주소를 할당해야 합니다(게이트웨이는 인터페이스와 동일한 서브넷에 있어야 함).
MTU	이 인터페이스에서 보낸 패킷의 최대 전송 단위(MTU)를 바이트 단위로 입력합니다(범위는 576~1,500, 기본값은 1,500).
디바이스 로그 수집	방화벽에서 로그를 수집하기 위한 인터페이스를 활성화합니다. 로그 트래픽이 많은 배포의 경우 여러 인터페이스를 활성화하여 이 기능을 수행할 수 있습니다. 이 기능은 MGT 인터페이스에서 기본적으로 활성화되어 있습니다.
수집기 그룹 커뮤니케이션	Collector Group 통신을 위한 인터페이스를 활성화합니다(기본값은 MGT 인터페이스). 하나의 인터페이스만 이 기능을 수행할 수 있습니다.
시스템 로그 포워딩	syslog 포워딩을 위한 인터페이스를 활성화합니다(기본값은 MGT 인터페이스). 하나의 인터페이스만 이 기능을 수행할 수 있습니다.

로그 수집기 인터페이스 설정	설명
네트워크 연결 서비스	**Ping** 서비스는 모든 인터페이스에서 사용할 수 있으며 이를 통해 Log Collector 인터페이스와 외부 서비스 간의 연결을 테스트할 수 있습니다. 다음 서비스는 MGT 인터페이스에서만 사용할 수 있습니다. • **SSH** - Panorama CLI에 대한 보안 액세스를 활성화합니다. • **SNMP** - 인터페이스가 SNMP 관리자로부터 통계 쿼리를 수신할 수 있도록 합니다. 자세한 내용은 SNMP 모니터링 활성화를 참조하십시오. • **User-ID** - Log Collector가 User-ID 에이전트로부터 받은 사용자 매핑 정보를 재배포할 수 있습니다.
허용된 IP 주소	이 인터페이스를 통해 Log Collector에 액세스할 수 있는 클라이언트 시스템의 IP 주소를 입력하십시오. 빈 목록(기본값)은 모든 클라이언트 시스템에서 액세스할 수 있음을 지정합니다. *Palo Alto Networks*는 이 목록을 공백으로 두지 않을 것을 권장합니다. 무단 액세스를 방지하기 위해 *Panorama* 관리자*(*단독*)*의 클라이언트 시스템을 지정합니다.

로그 수집기 **RAID** 디스크 설정

- Panorama > 관리형 수집기 > 디스크

M-Series 어플라이언스 또는 Panorama 가상 어플라이언스에서 로깅 디스크를 구성한 후 Log Collector 구성에 추가할 수 있습니다.

기본적으로 M-시리즈 어플라이언스는 베이 A1 및 A2에 설치된 첫 번째 RAID 1 디스크 쌍과 함께 제공됩니다. 소프트웨어에서 베이 A1 및 A2의 디스크 쌍은 디스크 쌍 A로 명명됩니다. 나머지 베이는 다음과 같이 순차적으로 명명됩니다. 디스크 쌍 B, 디스크 쌍 C 등. 예를 들어, M-500 어플라이언스는 최대 12개의 디스크 쌍을 지원합니다. 동일한 어플라이언스 내에서 2TB 또는 1TB 디스크 쌍을 설치할 수 있습니다. 그러나 디스크 크기는 각 쌍 내의 두 드라이브에 대해 동일해야 합니다.

Panorama 가상 어플라이언스는 24TB의 스토리지 용량을 위해 최대 12개의 가상 로깅 디스크를 지원합니다.

디스크 쌍을 추가한 후 Log Collector는 기존 로그를 모든 디스크에 재배포합니다. 이 작업은 각 테라바이트의 로그에 대해 몇 시간이 걸릴 수 있습니다. 재배포 과정에서 최대 로그 수집 속도가 감소합니다. **Panorama** > **Managed Collectors** 페이지에서 로그 재배포 상태 열은 프로세스의 완료 상태를 백분율로 나타냅니다.

중앙 모니터링을 위해 SNMP 관리자를 사용하는 경우 *panLogCollector MIB*에서 로깅 통계를 볼 수 있습니다.

연결 보안

- 디바이스 > 사용자 식별 > 연결 보안
- **Panorama** > 사용자 식별 > 연결 보안

Windows User-ID 에이전트가 제공한 인증서의 유효성을 검사하기 위해 로그 수집기가 사용하는 인증서 프로파일을 구성합니다. 로그 수집기는 선택한 인증서 프로파일을 사용하여 에이전트가 제공한 서버 인증서의 유효성을 검사하여 User-ID 에이전트의 ID를 확인합니다.

업무	설명
User-ID 인증서 프로파일	드롭다운에서 방화벽 또는 Panorama가 Windows User-ID 에이전트를 인증하는 데 사용하는 인증서 프로파일을 선택하거나 새 인증서 프로파일을 선택하여 생성합니다. 없음을 선택하여 인증서 프로파일을 제거합니다.

통신 설정

- Panorama > 관리형 수집기 > 커뮤니케이션

Log Collector와 Panorama, 방화벽 및 기타 Log Collector 간에 사용자 지정 인증서 기반 인증을 구성하려면 다음 표에 설명된 대로 설정을 구성합니다.

통신 설정	설명
보안 서버 통신 - 보안 서버 통신을 활성화하면 로그 수집기에 연결하는 클라이언트 디바이스의 ID가 검증됩니다.	
SSL/TLS 서비스 프로파일	드롭다운에서 SSL/TLS 서비스 프로파일을 선택합니다. 이 프로파일은 Log Collector에서 제공하는 인증서를 정의하고 Log Collector와의 통신에 허용되는 SSL/TLS 버전 범위를 지정합니다.
인증서 프로파일	드롭다운에서 인증서 프로파일을 선택합니다. 이 인증서 프로파일은 클라이언트가 제공하는 인증서 체인을 인증하는 데 사용되는 인증서 해지 확인 동작과 루트 CA를 정의합니다.
사용자 지정 인증서만	활성화된 경우 로그 수집기는 관리되는 방화벽 및 로그 수집기를 사용한 인증을 위한 사용자 지정 인증서만 수락합니다.

통신 설정	설명
일련번호를 기반으로 클라이언트 인증	Log Collector는 일련번호의 해시를 기반으로 클라이언트 디바이스에 권한을 부여합니다.
승인 목록 확인	이 Log Collector에 연결하는 클라이언트 디바이스 또는 디바이스 그룹은 권한 부여 목록에 대해 확인됩니다.
연결 해제 대기 시간(분)	Log Collector가 관리되는 디바이스와의 현재 연결을 끊기 전에 대기하는 시간입니다. 그런 다음 Log Collector는 구성된 보안 서버 통신 설정을 사용하여 관리되는 디바이스와의 연결을 다시 설정합니다. 보안 서버 통신 구성이 커밋된 후 대기 시간이 시작됩니다.
승인 목록	권한 부여 목록 - 추가를 선택한 다음 다음 필드를 완성하여 기준을 설정합니다. • 식별자 - 제목 또는 제목 대체를 선택합니다. 권한 부여 식별자로 이름 을 지정합니다. • 유형—제목 Alt인 경우. 이름이 식별자로 선택되고 **IP**, 호스트 이름 또는 전자 메일을 식별자 유형으로 선택합니다. 주제를 선택하면 공통 이름이 식별자 유형으로 사용됩니다. • 값 - 식별자 값을 입력합니다.
보안 클라이언트 통신 - 보안 클라이언트 통신을 활성화하면 Panorama, 방화벽 또는 기타 Log Collector와의 SSL 연결을 통해 Log Collector를 인증하는 데 지정된 클라이언트 인증서가 사용됩니다.	
인증서 유형	통신 보안에 사용되는 디바이스 인증서 유형(없음, 로컬 또는 SCEP) 선택
없음	없음을 선택하면 디바이스 인증서가 구성되지 않고 보안 클라이언트 통신이 사용되지 않습니다. 이것이 기본 선택입니다.
로컬	Log Collector는 로컬 디바이스 인증서와 Log Collector에서 생성되거나 기존 엔터프라이즈 PKI 서버에서 불러온 해당 개인 키를 사용합니다.
	인증서 - 로컬 디바이스 인증서를 선택합니다. 이 인증서는 방화벽에 고유한 인증서(Log Collector 일련번호의 해시 기반)이거나 Panorama에 연결하는 모든 Log Collector에서 사용하는 공통 디바이스 인증서일 수 있습니다.
	인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다. 이 인증서 프로파일은 로그 수집기로 서버 인증을 정의하는 데 사용됩니다.
SCEP	로그 수집기는 디바이스 인증서와 개인 키가 생성된 SCEP(Simple Certificate Enrollment Protocol) 서버를 사용합니다.

통신 설정	설명
	SCEP 프로파일 - 드롭다운에서 SCEP 프로파일을 선택합니다.
	인증서 프로파일 - 드롭다운에서 인증서 프로파일을 선택합니다. 이 인증서 프로파일은 로그 수집기로 서버 인증을 정의하는 데 사용됩니다.
서버 ID 확인	클라이언트 디바이스는 공통 이름(CN)을 서버의 IP 주소 또는 FQDN과 일치시켜 서버의 ID를 확인합니다.

전용 로그 수집기를 위한 소프트웨어 업데이트

- Panorama > 관리형 수집기

전용 로그 수집기에 소프트웨어 이미지를 설치하려면 Panorama에 이미지를 다운로드하거나 업로드하고(Panorama > 디바이스 배포 참조) 설치를 클릭하고 다음 필드를 완성합니다.

Panorama 관리 서버는 운영 체제를 로컬 기본 *Log Collector*와 공유하므로 *Panorama* 관리 서버에 소프트웨어 업데이트를 설치할 때 둘 다 업그레이드합니다*(*Panorama > 소프트웨어 참조*)*.

전용 로그 수집기의 경우 ***Panorama*** > ***Device Deployment*** > ***Software***를 선택하여 업데이트를 설치할 수도 있습니다*(*소프트웨어 및 콘텐츠 업데이트 관리 참조*)*.

관리*(MGT)* 인터페이스의 트래픽을 줄이기 위해 업데이트 배포에 별도의 인터페이스를 사용하도록 *Panorama*를 구성할 수 있습니다*(*Panorama > 설정 > 인터페이스 참조*)*.

로그 수집기에 소프트웨어 업데이트를 설치하기 위한 필드	설명
파일	다운로드하거나 업로드한 소프트웨어 이미지를 선택합니다.
디바이스	소프트웨어를 설치할 로그 수집기를 선택합니다. 대화 상자에는 각 로그 수집기에 대한 다음 정보가 표시됩니다. • 디바이스 이름 - 전용 로그 수집기의 이름입니다. • 현재 버전 - 현재 Log Collector에 설치된 Panorama 소프트웨어 릴리스입니다.

로그 수집기에 소프트웨어 업데이트를 설치하기 위한 필드	설명
	• **HA** 상태 - 이 열은 로그 수집기에 적용되지 않습니다. 전용 로그 수집기는 고가용성을 지원하지 않습니다.
필터 선택	특정 로그 수집기만 표시하려면 로그 수집기 및 필터 선택을 선택합니다.
디바이스에만 업로드(설치하지 않음)	소프트웨어를 자동으로 재부팅하지 않고 Log Collector에 업로드하려면 선택합니다. Log Collector CLI에 로그인하고 **`request restart system`** operation 명령을 실행하여 수동으로 재부팅할 때까지 이미지가 설치되지 않습니다.
설치 후 디바이스 재부팅	소프트웨어를 업로드하고 자동으로 설치하려면 선택합니다. 설치 프로세스가 로그 수집기를 재부팅합니다.

Panorama > 수집기 그룹

각 수집기 그룹에는 최대 16개의 로그 수집기가 있을 수 있으며 여기에는 로그를 포워딩하기 위한 방화벽이 할당됩니다. 그런 다음 Panorama를 사용하여 통합된 로그 보기 및 검토를 위해 로그 수집기를 쿼리할 수 있습니다.

*default*라는 사전 정의된 수집기 그룹에는 *Panorama* 관리 서버에 로컬인 사전 정의된 로그 수집기가 포함됩니다.

수집기 그룹 구성

수집기 그룹을 구성하려면 추가를 클릭하고 다음 필드를 완성합니다.

수집기 그룹 설정	구성 위치	설명
이름	**Panorama** > 수집기 그룹 > 일반	이 수집기 그룹을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
로그 스토리지		Collector Group이 수신하는 방화벽 로그의 총 스토리지 할당량과 사용 가능한 공간을 나타냅니다. 스토리지 할당량 링크를 클릭하여 다음 로그 유형에 대한 스토리지 할당량**(%)** 및 만료 기간(최대 일수)을 설정합니다. • 자세한 방화벽 로그 - 트래픽, 위협, HIP 일치, 동적으로 등록된 IP 주소(IP 태그), 확장 PCAP, GTP 및 터널, 앱 통계 등과 같은 디바이스 > 설정 > 로깅 및 보고 설정의 모든 로그 유형을 포함합니다. • 요약 방화벽 로그 - 트래픽 요약, 위협 요약, URL 요약, GTP 및 터널 요약과 같은 디바이스 > 설정 > 로깅 및 보고 설정에 포함된 모든 요약 로그를 포함합니다. • 인프라 및 감사 로그 - 구성, 시스템, User-ID 및 인증 로그를 포함합니다. • **Palo Alto Networks** 플랫폼 로그 - Traps 및 기타 Palo Alto Networks 제품의 로그를 포함합니다.

수집기 그룹 설정	구성 위치	설명
		• 타사 외부 로그 - Palo Alto Networks에서 제공하는 다른 공급자 통합의 로그를 포함합니다. 기본 설정을 사용하려면 기본값 복원을 클릭합니다.
최소 보유 기간(일)		Panorama가 수집기 그룹의 모든 로그 수집기에서 유지 관리하는 최소 로그 보존 기간(1–2,000일)을 입력합니다. 현재 날짜에서 가장 오래된 로그의 날짜를 뺀 날짜가 정의된 최소 보존 기간보다 짧은 경우 Panorama는 경고 위반으로 시스템 로그를 생성합니다.
수집기 그룹 구성원		이 수집기 그룹의 일부가 될 로그 수집기를 추가합니다(최대 16개). **Panorama** > **Managed Collectors** 페이지에서 사용 가능한 모든 로그 수집기를 추가할 수 있습니다. 특정 수집기 그룹에 대한 모든 로그 수집기는 동일한 모델이어야 합니다(예: 모든 M-500 어플라이언스 또는 모든 Panorama 가상 어플라이언스). 기존 수집기 그룹에 로그 수집기를 추가하면 *Panorama*가 모든 로그 수집기에 기존 로그를 재배포합니다. 이 작업에는 각 테라바이트의 로그에 대해 몇 시간이 걸릴 수 있습니다. 재배포 과정에서 최대 로깅 속도가 감소합니다. ***Panorama*** > ***Collector Groups*** 페이지에서 *Log Redistribution State* 열은 프로세스의 완료 상태를 백분율로 나타냅니다.
수집기 간 로그 중복 활성화		이 옵션을 선택하면 수집기 그룹의 각 로그에 두 개의 복사본이 있고 각 복사본은 다른 로그 수집기에 상주합니다. 이 중복성은 하나의 로그 수집기를 사용할 수 없게 되어도 로그가 손실되지 않도록 합니다. 수집기 그룹으로 포워딩된 모든 로그를 보고 모든 로그 데이터에 대한 보고서를 실행할 수 있습니다. 로그 중복성은 수집기 그룹에 여러 개의 로그 수집기가 있고 각 로그 수집기에 동일한 수의 디스크가 있는 경우에만 사용할 수 있습니다. 로그 중복성은 설정이 활성화된 후 새로 수집된 로그에만 적용되며 기존 로그에는 적용되지 않습니다. **Panorama** > **Collector Groups** 그룹 페이지에서 로그 재배포 상태 열은 프로세스의 완료 상태를 백분율로 나

수집기 그룹 설정	구성 위치	설명
		타냅니다. 특정 수집기 그룹에 대한 모든 로그 수집기는 동일한 모델이어야 합니다(예: 모든 M-500 어플라이언스 또는 모든 Panorama 가상 어플라이언스). 중복성을 활성화하면 더 많은 로그가 생성되기 때문에 이 구성에는 더 많은 저장 용량이 필요합니다. 중복을 활성화하면 수집기 그룹에서 로그 처리 트래픽이 두 배로 늘어나 최대 로깅 속도가 절반으로 줄어듭니다. 각 로그 수집기는 수신하는 각 로그의 복사본을 배포해야 하기 때문입니다. *(*컬렉터 그룹의 공간이 부족하면 오래된 로그를 삭제합니다.*)*
기본 설정 목록의 모든 수집기에 포워딩		기본 설정 목록의 모든 로그 수집기에 로그를 보내려면 선택합니다. Panorama는 라운드 로빈 로드 밸런싱을 사용하여 주어진 순간에 로그를 수신하는 Log Collector를 선택합니다. 이것은 기본적으로 비활성화되어 있습니다. 방화벽은 해당 로그 수집기를 사용할 수 없게 되지 않는 한 목록의 첫 번째 로그 수집기에만 로그를 보냅니다(디바이스/수집기 참조).
보안 LC 간 통신 활성화		수집기 그룹의 로그 수집기 간의 상호 SSL 인증을 위해 사용자 지정 인증서를 사용할 수 있습니다.
위치	**Panorama** > 수집기 그룹 > 모니터링	수집기 그룹의 위치를 지정합니다.
연락처		이메일 연락처를 지정하십시오(예: 로그 수집기를 모니터링할 SNMP 관리자의 이메일 주소).
버전		Panorama 관리 서버와 통신하기 위한 SNMP 버전을 지정합니다. **V2c** 또는 **V3**. SNMP를 사용하면 연결 상태, 디스크 드라이브 통계, 소프트웨어 버전, 평균 CPU 사용량, 평균 로그/초 및 로그 유형별 저장 기간을 포함하여 로그 수집기에 대한 정보를 수집할 수 있습니다. SNMP 정보는 수집기 그룹별로 사용할 수 있습니다.
SNMP 커뮤니티 문자		SNMP 관리자 및 모니터링되는 디바이스(이 경우 로그 수집기)의 커뮤니티를 식별하고 커뮤니티 구성원을 서

수집기 그룹 설정	구성 위치	설명
열(V2c만 해당)		로 인증하기 위한 암호 역할을 하는 **SNMP** 커뮤니티 문자열을 입력합니다. 기본 커뮤니티 문자열 *public*을 사용하지 마십시오. 잘 알려져 있으므로 안전하지 않습니다.
보기(V3만 해당)		SNMP 보기 그룹을 추가하고 보기에서 그룹 이름을 입력합니다. 각 보기는 쌍을 이루는 개체 식별자(OID)와 비트 단위 마스크입니다. OID는 MIB(Managed Information Base)를 지정하고 마스크(16진수 형식)는 해당 개체 내(일치 포함) 또는 MIB 외부(일치 제외)에 액세스할 수 있는 SNMP 개체를 지정합니다. 그룹의 각 보기에 대해 다음 설정을 추가합니다. • 보기 - 보기의 이름을 입력합니다. • **OID** - OID를 입력합니다. • 옵션(포함 또는 제외) - 보기에서 OID를 제외할지 또는 포함할지 선택합니다. • 마스크 - OID의 필터에 대한 마스크 값을 지정합니다(예: 0xf0).
사용자(V3만 해당)		각 SNMP 사용자에 대해 다음 설정을 추가합니다. • 사용자 - SNMP 관리자에 대한 사용자 인증을 위한 사용자명을 입력합니다. • 보기 - 사용자에 대한 보기 그룹을 선택합니다. • **Authpwd** - 사용자를 SNMP 관리자에 인증하기 위한 암호를 입력합니다(최소 8자). 비밀번호 암호화에는 SHA(Secure Hash Algorithm)만 지원됩니다. • **Privpwd** - SNMP 관리자에 대한 SNMP 메시지를 암호화하기 위한 개인 정보 암호를 입력합니다(최소 8자). AES(Advanced 암호화 표준)만 지원됩니다.
디바이스/수집기	**Panorama** > 수집기 그룹 > 디바이스 로그 전달	로그 포워딩 기본 설정 목록은 어떤 방화벽이 어떤 로그 수집기로 로그를 포워딩할지 제어합니다. 목록에 추가하는 각 항목에 대해 디바이스 목록을 수정하여 하나

수집기 그룹 설정	구성 위치	설명
		이상의 방화벽을 할당하고 수집기 목록에 하나 이상의 로그 수집기를 추가합니다. 기본적으로 목록 항목에 할당한 방화벽은 사용 가능한 한 기본(첫 번째) Log Collector에만 로그를 보냅니다. 기본 로그 수집기가 실패하면 방화벽이 보조 로그 수집기로 로그를 보냅니다. 2차에 장애가 발생하면 방화벽은 3차 Log Collector 등으로 로그를 보냅니다. 순서를 변경하려면 로그 수집기를 선택한 다음 위로 이동 또는 아래로 이동을 클릭합니다. 일반 탭의 기본 설정 목록에서 모든 수집기로 포워딩을 선택하여 관리 방화벽에 대한 기본 로그 포워딩 동작을 재정의할 수 있습니다.

체계
구성
HIP 매치
트래픽
위협
URL
데이터
WildFire
상관 관계
GTP
SCTP
입증
User-ID
	Panorama > 수집기 그룹 > 수집기 로그 전달	이 수집기 그룹에서 외부 서비스로 포워딩하려는 각 유형의 방화벽 로그에 대해 하나 이상의 일치 목록 프로파일을 추가합니다. 프로파일은 포워딩할 로그와 대상 서버를 지정합니다. 각 프로필에 대해 다음을 수행:
		• 이름 - 일치 목록 프로필을 식별할 수 있는 최대 31자의 이름을 입력합니다.
		• 필터 - 기본적으로 방화벽은 이 일치 목록 프로파일이 적용되는 유형의 모든 로그를 포워딩합니다. 로그의 하위 집합을 포워딩하려면 기존 필터를 선택하거나 필터 빌더를 선택하여 새 필터를 추가합니다. 새 필터의 각 쿼리에 대해 다음 필드를 지정하고
		  • **Connector**—Select the connector logic (and/or) 쿼리를 추가합니다. 무효를 적용하려면 부정을 선택합니다. 예를 들어, 신뢰할 수 없는 영역에서 로그를 포워딩하지 않으려면 무효를 선택한 다음 속성으로 영역을 선택하고 연산자로 같음을 선택한 다음 값 열에 신뢰할 수 없는 영역의 이름을 입력합니다.
		  • 속성 - 로그 속성을 선택합니다. 옵션은 로그 유형에 따라 다릅니다.

수집기 그룹 설정	구성 위치	설명
터널 IP 태그 복호화 GlobalProtect		• 연산자 - 속성이 적용되는 방식을 결정하는 기준을 선택합니다(예: 같음). 옵션은 로그 유형에 따라 다릅니다. • 값 - 일치시킬 속성 값을 지정합니다. 필터와 일치하는 로그를표시하거나 내보내려면 필터링된 로그 보기를 선택합니다. 이 탭은 모니터링 탭 페이지(예: 모니터링 > 로그 > 트래픽)와 동일한 옵션을 제공합니다. • 설명 - 이 일치 목록 프로파일의 목적을 설명하기 위해 최대 1,023자의 설명을 입력합니다. • 대상 서버 - 각 서버 유형에 대해 하나 이상의 서버 프로파일을 추가합니다. 서버 프로파일을 구성하려면 디바이스 > 서버 프로파일 > SNMP 트랩, 디바이스 > 서버 프로파일 > Syslog, 디바이스 > 서버 프로파일 > 이메일 또는 디바이스 > 서버 프로파일 > HTTP를 참조하십시오. • 기본 제공 작업 - 시스템 및 구성 로그를 제외한 모든 로그 유형에 대한 작업을추가할 수 있습니다. • 작업을 설명하는 이름을 입력합니다. • 태그를 지정할 IP 주소(소스 주소 또는 대상 주소)를 선택합니다. 상관 관계 로그 및 HIP 일치 로그에서 소스 IP 주소에만 태그를 지정할 수 있습니다. • 태그 추가 또는 태그 제거 작업을 선택합니다. • 이 Panorama의 로컬 User-ID 에이전트 또는 원격 User-ID 에이전트에 태그를 등록할지 여부를 선택합니다. 원격 디바이스 사용자 **ID** 에이전트에 태그를 등록하려면 전달을 활성화할 HTTP 서버 프로파일을 선택합니다. • IP 주소-태그 매핑이 유지되는 시간을 분 단위로 설정하도록 IP-태그 타임아웃을 구성합니다. 시간 초과를 0으로 설정하면 IP-태그 매핑이

수집기 그룹 설정	구성 위치	설명
		시간 초과되지 않음을 의미합니다(범위는 0 ~ 43200(30일), 기본값은 0). 태그 추가작업으로만 시간 초과를 구성할 수 있습니다. • 대상 소스 또는 대상 IP 주소에서 적용하거나 제거할 태그를 입력하거나 선택합니다.
수집 프로파일	**Panorama** > 수집기 그룹 > 로그 수집	Panorama가 Traps ESM 서버에서 로그를 수신할 수 있도록 하는 하나 이상의 로그 수집 프로파일을 추가합니다. 새 로그 수집 프로파일을 구성하려면 Panorama > 로그 수집 프로파일을 참조하세요.
관리자 활동 기록	**Panorama** > 수집기 그룹 > 감사	관리자 활동의 감사 로그를 생성하고 선택한 syslog 서버로 포워딩하도록 로그 수집기를 구성합니다. • 작동 명령(기본적으로 비활성화됨) - 관리자가 CLI에서 작동 또는 디버그 명령을 실행할 때 감사 로그를 생성합니다. PAN-OS 작동 및 디버그 명령의 전체 목록은 CLI 작동 명령 레이어를 참조하십시오. • **Syslog** 서버 - 감사 로그를 포워딩할 대상 syslog 서버 프로파일을 선택합니다.

수집기 그룹 정보

수집기 그룹에 대한 다음 정보를 표시하려면 **Panorama** > 수집기 그룹을 선택합니다. 로그 수집기 구성을 완료한 후 추가 필드를 구성할 수 있습니다.

수집기 그룹 정보	설명
이름	수집기 그룹을 식별하는 이름입니다.
중복 활성화	수집기 그룹에 대해 로그 중복이 활성화되었는지의 여부를 나타냅니다. 로그 수집기 구성을 완료하거나 수정한 후 수집기 그룹에 대한 로그 중복성을 활성화할 수 있습니다.
수집기	수집기 그룹에 할당된 로그 수집기입니다.

수집기 그룹 정보	설명
로그 재배포 상태	특정 작업(예: 로그 중복 활성화)은 수집기 그룹이 로그 수집기 간에 로그를 재배포하도록 합니다. 이 열은 재분배 프로세스의 완료 상태를 백분율로 나타냅니다.

Panorama > 플러그인

- **Panorama** > 플러그인
- 디바이스 > 플러그인

Panorama에서 타사 통합을 지원하는 플러그인을 설치, 제거 및 관리하려면 **Panorama** > **Plugins**를 선택합니다.

(VM 시리즈 방화벽에서만 사용 가능) VM 시리즈 방화벽용 플러그인을 설치, 제거 및 관리하려면 **Device** > **Plugins**를 선택하십시오.

플러그인	설명
업로드	로컬 디렉토리에서 플러그인 설치 파일을 업로드할 수 있습니다. 이것은 플러그인을 설치하지 않습니다. 설치 파일을 업로드하면 설치 링크가 활성화됩니다.
파일 이름	플러그인 파일 이름입니다. Panorama에 **vm_series** 플러그인을 설치하면 AWS, Azure 및 Google과 같은 퍼블릭 클라우드 환경에 배포된 VM 시리즈 방화벽에서 템플릿 구성을 관리하고 커밋하기 위해 **Device** > **VM** 시리즈 페이지를 사용할 수 있습니다.
버전	플러그인 버전 번호입니다.
플랫폼	플러그인이 지원되는 모델입니다.
출시일	이 버전의 플러그인 릴리스 날짜입니다.
크기	플러그인 파일 크기.
설치됨	Panorama에서 각 플러그인의 현재 설치 상태를 제공합니다.
작업	• 설치—플러그인의 지정된 버전을 설치합니다. 플러그인의 새 버전을 설치하면 이전에 설치된 버전을 덮어씁니다. • 삭제 - 지정된 플러그인 파일을 삭제합니다. • 구성 제거 - 플러그인과 관련된 모든 구성을 제거합니다. Plugin과 관련된 모든 설정을 완전히 제거하기 위해서는 **Remove Config**를 사용한 후 **Uninstall**도 수행해야 합니다. VMware NSX용 Panorama 플러그인에서 구성을 제거할 때 이 작업은 서비스 정의 및 서비스 관리자만 삭제합니다. 영역, 디바이스 그룹 또는 템플릿과 같은 다른 관련 구성은 제거하지 않습니다. 또한 Panorama HA 배포에서 이 작업을 완료

플러그인	설명
	하려면 먼저 활성에서 구성을 제거하고 보조를 활성으로 만들기 위해 페일오버를 시작한 다음 새 활성 피어에서 구성을 제거해야 합니다. • 제거 - 플러그인의 현재 설치를 제거합니다. 이것은 Panorama에서 플러그인 파일을 제거하지 않습니다. 플러그인을 제거하면 해당 플러그인과 관련된 모든 구성이 손실됩니다. 관련 구성을 완전히 제거할 때만 사용하십시오.

Panorama > SD-WAN

Panorama SD-WAN 플러그인을 다운로드 및 설치하여 보고서를 중앙에서 관리, 모니터링 및 생성합니다. 분기를 추가하고 적절한 허브에 연결하여 Panorama에서 SD-WAN 토폴로지를 구성하고 해당 분기 및 허브 디바이스를 적절한 영역에 연결합니다. SD-WAN 토폴로지를 구성한 후 구성된 모든 디바이스 및 경로에서 경로 상태 메트릭을 모니터링하여 애플리케이션 및 링크 문제를 분리하고 시간 경과에 따른 링크 성능을 이해할 수 있습니다. 또한 감사 목적으로 보고서를 생성할 수 있습니다.

무엇을 알고 싶습니까?	참조:
분기 및 허브 디바이스 추가, 편집 또는 삭제	SD-WAN 디바이스
VPN 클러스터 추가, 편집 또는 삭제	SD-WAN VPN 클러스터
경로 상태 모니터링	SD-WAN 모니터링
상태 보고서 생성	SD-WAN 보고서

SD-WAN 디바이스

- **Panorama** > **SD-WAN** > 디바이스

SD-WAN 디바이스는 VPN 클러스터 및 SD-WAN 토폴로지를 구성하는 브랜치 또는 허브입니다.

필드	설명
이름	SD-WAN 디바이스를 식별하는 이름을 입력합니다.
유형	SD-WAN 디바이스 유형 선택: • 허브 - 기본 사무실이나 위치(예: 데이터 센터 또는 비즈니스 본부)에 배포된 중앙 집중식 방화벽으로 모든 브랜치 디바이스가 VPN 연결을 사용하여 연결합니다. 브랜치 간의 트래픽은 대상 브랜치로 계속 이동하기 전에 허브를 통과합니다. 브랜치는 허브에 연결하여 허브 위치의 중앙 집중식 리소스에 액세스할 수 있습니다. 허브 디바이스는 트래픽을 처리하고 정책 규칙을 시행하며 기본 사무실이나 위치에서 링크 스와핑을 관리합니다. • 브랜치 - VPN 연결을 사용하여 허브에 연결하고 브랜치 수준에서 보안을 제공하는 물리적 브랜치 위치에 배포된 방화벽입니다. 지점은 중앙 집중식 리소스에 액세스하기 위해 허브에 연결합니다. 브랜치 디바이스는 트래픽을 처리하고 정책 규칙을 적용하며 브랜치 위치에서 링크 스와핑을 관리합니다.

필드	설명
라우터 이름	SD-WAN 허브와 분기 간의 라우팅에 사용할 가상 또는 논리적 라우터를 선택합니다. 기본적으로 `sdwan-default` 가상 라우터가 생성되고 Panorama가 라우터 구성을 자동으로 푸시할 수 있습니다.
사이트	허브 또는 브랜치를 식별하는 사용자 친화적인 사이트 이름을 입력하십시오. 예를 들어 브랜치 디바이스가 배포된 도시 이름을 입력합니다.
링크 태그	(PAN-OS 10.0.3 이상 릴리스) 허브의 경우 허브가 DIA AnyPath에 참여할 수 있도록 허브 가상 인터페이스에 대해 생성한 링크 태그를 선택합니다. 자동 VPN은 이 링크 태그를 개별 링크가 아닌 전체 허브 가상 인터페이스에 적용합니다. 트래픽 분산 프로파일에서 이 링크 태그를 참조하여 이 허브 가상 인터페이스에 대한 페일오버 순서를 나타냅니다. 브랜치 디바이스에서 Auto VPN은 이 태그를 사용하여 허브 디바이스에서 종료되는 SD-WAN 가상 인터페이스의 링크 태그 필드를 채웁니다.
존(zone) 인터넷	신뢰할 수 없는 소스로 들어오고 나가는 트래픽을 식별하기 위해 하나 이상의 보안 영역을 추가합니다.
존(zone) 허브	SD-WAN 허브 디바이스로 들어오고 나가는 트래픽을 식별하기 위해 하나 이상의 보안 영역을 추가합니다.
존(zone) 브랜치	SD-WAN 브랜치 디바이스로 들어오고 나가는 트래픽을 식별하기 위해 하나 이상의 보안 영역을 추가합니다.
영역 내부	하나 이상의 보안 영역을 추가하여 회사 네트워크의 신뢰할 수 있는 디바이스로 들어오고 나가는 트래픽을 식별합니다.
BGP 탭	
BGP	BGP를 활성화합니다.
라우터 ID	BGP 라우터 ID를 지정합니다. BGP(Border Gateway Protocol) 라우터 ID는 모든 라우터 간에 고유해야 합니다. 루프백 주소를 라우터 *ID*로 사용하십시오.
루프백 주소	BGP 피어링에 대한 정적 루프백 IPv4 주소를 지정합니다.
AS 번호	자치 시스템 번호를 입력하여 인터넷에 일반적으로 정의된 라우팅 정책을 정의합니다. AS 번호는 모든 허브 및 브랜치 위치에 대해 고유해야 합니다.

필드	설명
	공개적으로 라우팅 가능한 *AS* 번호를 방해하지 않으려면 *4*바이트 개인 *BGP AS* 번호를 사용하십시오.
재배포 프로파일 이름	브랜치에서 허브 라우터로 통신되는 로컬 프리픽스를 제어하기 위해 재배포 프로파일을 선택하거나 생성합니다. 기본적으로 로컬로 연결된 모든 인터넷 프리픽스는 허브 위치에 보급됩니다. *Palo Alto Networks*는 *ISP*에서 학습한 지점 기본 경로를 재배포하지 않습니다.
업스트림 **NAT** 탭	
업스트림 NAT	업스트림 NAT를 활성화합니다.
SD-WAN 인터페이스	SD-WAN용으로 구성된 인터페이스를 선택합니다.
NAT IP 주소 유형	다음 중 하나를 선택합니다. • 정적 **IP** - 허브 또는 브랜치에 대해 NAT를 수행하는 장치 뒤에 있는 SD-WAN 허브 또는 브랜치의 경우 Auto VPN 구성에서 해당 주소를 허브 또는 분기의 터널 끝점으로 사용할 수 있도록 업스트림 NAT 수행 디바이스에서 공용 인터페이스의 IP 주소 또는 FQDN을 지정해야 합니다. **IP** 주소를 선택하고 서브넷 마스크 없이 IPv4 주소를 입력하거나 **FQDN**을 선택합니다. • **DDNS** - 분기에 대해 NAT를 수행하는 장치 뒤에 있는 SD-WAN 분기의 경우 NAT 장치의 인터페이스에 대한 IP 주소가 팔로 알토 네트웍스 DDNS 서비스에서 얻어졌음을 나타냅니다.
VPN 터널 탭	
ToS 헤더 복사	(PAN-OS 10.2.1 이상 11.0 릴리스) 원래 ToS 정보를 보존하기 위해(서비스 유형) ToS 필드(ToS 비트 또는 차별화된 서비스 코드 포인트 [DSCP] 표시)를 내부 IPv4 헤더에서 캡슐화된 패킷의 VPN 헤더로 복사합니다. 이렇게 하면 ECN(명시적 혼잡 알림) 필드도 복사됩니다.

SD-WAN VPN 클러스터

- **Panorama** > **SD-WAN** > **VPN** 클러스터

SD-WAN 브랜치 디바이스를 하나 이상의 SD-WAN 허브 디바이스와 연결하여 브랜치와 허브 위치 간의 통신 보안을 허용합니다. SD-WAN VPN 클러스터에서 브랜치 및 허브 디바이스를 연결하면 방화벽은 지정한 VPN 클러스터 유형에 따라 사이트 간에 필요한 IKE 및 IPSec VPN 연결을 생성합니다.

필드	설명
이름	VPN 클러스터를 식별하는 이름을 입력하십시오.
유형	SD-WAN VPN 클러스터 유형 선택: • 허브 스포크 - 기본 사무실 또는 위치의 중앙 집중식 방화벽이 VPN 연결을 사용하여 연결된 브랜치 디바이스 간의 게이트웨이 역할을 하는 SD-WAN 토폴로지입니다. 브랜치 간의 트래픽은 대상 브랜치로 계속 이동하기 전에 허브를 통과합니다.
지점	하나 이상의 허브와 연결할 하나 이상의 브랜치 디바이스를 추가합니다.
허브	하나 이상의 브랜치 디바이스와 연결할 하나 이상의 허브 디바이스를 추가합니다. 여러 허브가 추가된 경우 경로 상태 품질 메트릭을 사용하여 기본 허브와 보조 허브를 제어합니다.

SD-WAN 모니터링

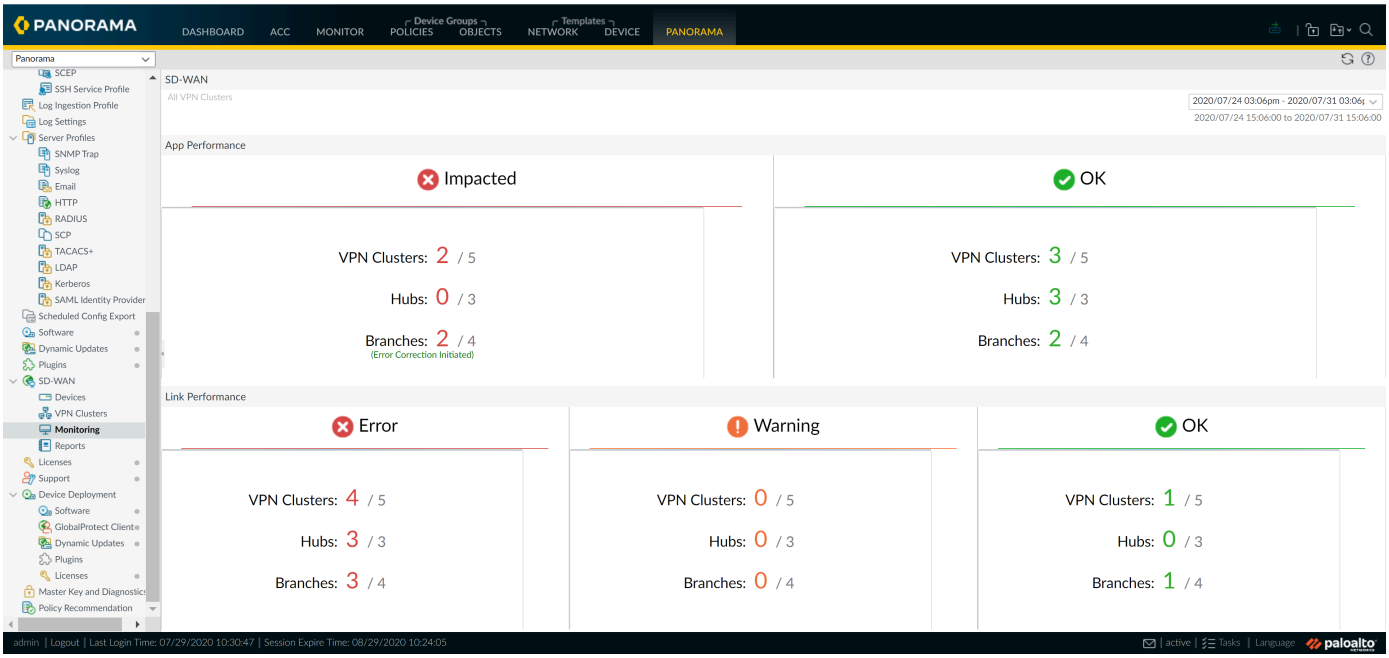
- **Panorama** > **SD-WAN** > 모니터링

모니터링 탭은 모든 SD-WAN 디바이스 상태 메트릭의 요약 위젯을 표시하는 대시보드입니다. 이 도구는 실적 문제가 있는 애플리케이션이나 링크를 빠르게 식별할 수 있도록 하여 SD-WAN 네트워크의 활동에 대한 실행 가능한 인텔리전스를 제공합니다. 지정된 기간 내에 모든 VPN 클러스터 또는 특정 VPN 클러스터에 대한 경로 품질 및 링크 실적을 볼 수 있습니다.

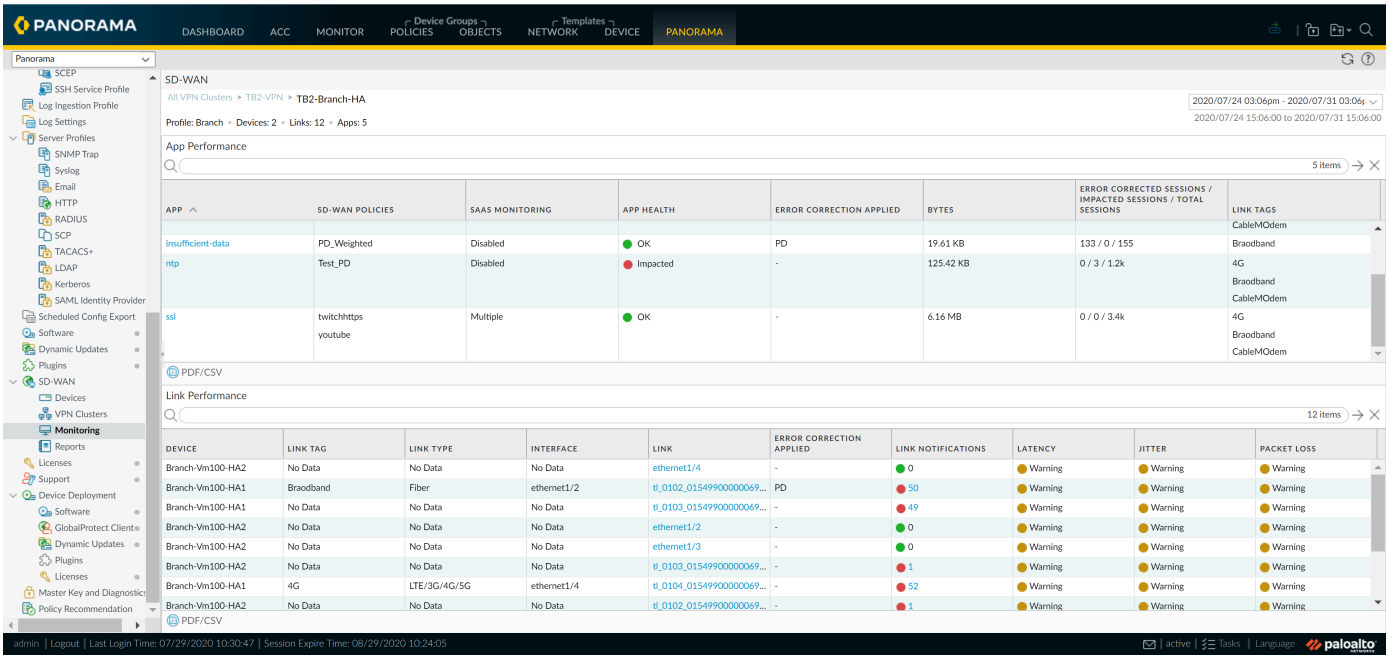
애플리케이션 실적에 영향을 받는 브랜치 또는 허브 방화벽이 있는 VPN 클러스터와 정상 VPN 클러스터의 총 수를 한 눈에 볼 수 있습니다. VPN 클러스터에 대한 다음 애플리케이션 및 링크 상태를 볼 수 있습니다.

- 앱 실적
  - 영향을 받는 경로 - 선택할 수 있는 경로 목록의 경로 품질 프로파일에 지정된 임계값 이하의 경로에 지터, 대기 시간 또는 패킷 손실이 없는 VPN 클러스터의 하나 이상의 애플리케이션입니다.
  - 정상 - VPN 클러스터의 애플리케이션이 정상이며 지터, 대기 시간 또는 패킷 손실이 발생하지 않습니다.

- 링크 실적
  - 오류 - VPN 클러스터에서 선택할 수 있는 경로 목록의 경로 품질 프로파일에 지정된 임계값 이하의 지터, 대기 시간 또는 패킷 손실이 없는 하나 이상의 사이트입니다.
  - 경고 - VPN 클러스터에 있는 하나 이상의 사이트에 지표의 이동하는 7일 평균 값과 비교하여 불리한 지터, 대기 시간 또는 패킷 손실 측정이 있는 링크가 있습니다.
  - **OK** - VPN 클러스터의 링크가 정상이며 지터, 대기 시간 또는 패킷 손실이 발생하지 않습니다.



위젯을 클릭하면 원하는 상태에 대한 모든 VPN 클러스터를 자세히 볼 수 있습니다. 또한 사이트 필터를 사용하여 링크 알림, 대기 시간 편차, 지터 편차, 패킷 손실 편차 또는 영향을 받는 애플리케이션을 기반으로 VPN 클러스터를 볼 수 있습니다.



SD-WAN 보고서

- **Panorama** > **SD-WAN** > 보고서

감사를 위해 지정된 기간 동안 가장 높은 상태 저하를 경험한 상위 애플리케이션 또는 링크에 대한 애플리케이션 또는 링크 실적에 대한 보고서를 생성합니다. 보고서를 구성한 후에는 보고서를 보려면 지금 실행해야 합니다. 보고서는 현재 작동하지 않는 기능을 내보낼 수 있습니다. 어떤 형식으로 보고서를 내보낼 수 있습니까?

필드	설명
이름	보고서의 목적을 식별하는 이름을 입력합니다.
보고서 유형	실행할 보고서 유형을 선택합니다. • 앱 실적— SD-WAN의 모든 애플리케이션 트래픽에 대한 상태 메트릭을 상세히 설명하는 보고서를 생성합니다. • 링크 실적— SD-WAN의 링크 전체 트래픽에 대한 상태 메트릭을 상세히 설명하는 보고서를 생성합니다.
클러스터	드롭다운에서 보고서를 생성할 클러스터를 선택합니다. 기본적으로 모두가 선택됩니다.
사이트	드롭다운에서 보고서를 생성할 사이트를 선택합니다. 기본적으로 모두가 선택됩니다.

필드	설명
	클러스터에 대해 모두 선택된 경우 클러스터에 기인하는 모든 사이트에 대한 보고서를 생성해야 합니다. 특정 클러스터를 선택한 경우 보고서를 생성할 특정 사이트를 선택할 수 있습니다.
애플리케이션(앱 실적 보고서 유형만 해당)	드롭다운에서 보고서를 생성할 애플리케이션을 선택합니다. 기본적으로 모두가 선택됩니다. 사이트에 대해 모두 선택된 경우 사이트에 기인하는 모든 애플리케이션에 대한 보고서를 생성해야 합니다. 특정 사이트를 선택한 경우 보고서를 생성할 특정 애플리케이션을 선택할 수 있습니다.
링크 태그(링크 실적 보고서 유형만)	드롭다운에서 보고서를 생성할 링크 태그를 선택합니다. 기본적으로 모두가 선택됩니다. 사이트에 대해 모두 선택된 경우 사이트에서 만든 모든 링크 태그에 대한 보고서를 생성해야 합니다. 특정 사이트를 선택한 경우 보고서를 생성할 특정 링크 태그를 선택할 수 있습니다.
링크 유형(링크 실적 보고서 유형만 해당)	드롭다운에서 보고서를 생성할 링크 유형을 선택합니다. 기본적으로 모두가 선택됩니다. 링크 태그에 대해 모두 선택된 경우 링크 태그 아래에 생성된 모든 링크 유형에 대한 보고서를 생성해야 합니다. 특정 링크 태그를 선택한 경우 보고서를 생성할 특정 링크 유형을 선택할 수 있습니다.
상위 N개	보고서에 포함할 애플리케이션 또는 링크 수를 지정합니다. 보고서에 상위 5, 10, 25, 50, 100, 250, 500 또는 수행되는 애플리케이션 또는 링크 1000개가 포함됩니다. 기본적으로 **5**가 선택됩니다.
기간	보고서를 실행할 기간을 설정합니다. 기본적으로 없음이 선택되지 않으며 모든 앱을 사용하여 보고서를 생성하고 실적 데이터를 링크합니다.

Panorama > VMware NSX

VM 시리즈 NSX 버전 방화벽 프로비저닝을 자동화하려면 NSX Manager와 Panorama 간의 통신을 활성화해야 합니다. Panorama가 VM 시리즈 방화벽을 NSX Manager의 서비스로 등록하면 NSX Manager에는 클러스터의 각 ESXi 호스트에서 VM 시리즈 방화벽의 하나 이상의 인스턴스를 프로비저닝하는 데 필요한 구성 설정이 있습니다.

무엇을 알고 싶습니까?	참조:
알림 그룹을 구성하려면 어떻게 합니까?	알림 그룹 구성
VM 시리즈 NSX 에디션 방화벽에 대한 구성은 어떻게 정의합니까?	서비스 정의 생성
NSX Manager와 통신하도록 Panorama를 구성하려면 어떻게 해야 합니까?	NSX Manager에 대한 액세스 구성
VM 시리즈 NSX 에디션 방화벽에 대한 스티어링 규칙은 어떻게 정의합니까?	스티어링 규칙 만들기
동적 vSphere 환경에서 정책을 일관되게 적용하도록 방화벽을 구성하려면 어떻게 해야 합니까?	개체 > 주소 그룹 및 정책 > 보안을 선택합니다. Panorama 및 방화벽이 가상 환경의 변경 사항에 대해 학습할 수 있도록 하려면 보안 정책 사전 규칙에서 동적 주소 그룹을 소스 및 대상 주소 개체로 사용하십시오.
더 찾고 계십니까?	VM 시리즈 NSX Edition 방화벽 설정을 참조하십시오.

알림 그룹 구성

- Panorama > 그룹에 알림

다음 표에서는 Panorama 알림 그룹 설정에 대해 설명합니다.

그룹 설정 알림	설명
이름	알림 그룹을 설명하는 이름을 입력합니다.
기기에 알림	네트워크에 배포된 가상 머신에 대한 추가 또는 수정 사항을 알려야 하는 디바이스 그룹의 체크박스를 선택합니다.

그룹 설정 알림	설명
	새 가상 머신이 프로비저닝되거나 기존 머신이 수정되면 가상 네트워크의 변경 사항이 Panorama에 대한 업데이트로 제공됩니다. 그렇게 하도록 구성된 경우 Panorama는 정책 규칙에서 참조하는 동적 주소 개체를 채우고 업데이트하여 지정된 디바이스 그룹의 방화벽이 동적 주소 그룹에 등록된 IP 주소에 대한 변경 사항을 수신하도록 합니다. 알림을 활성화하려면 알림을 활성화할 모든 디바이스 그룹을 선택해야 합니다. 디바이스 그룹을 선택할 수 없는 경우(사용 가능한 체크박스 없음) 디바이스 그룹 레이어 구조에 따라 디바이스 그룹이 자동으로 포함된다는 의미입니다. 이 알림 프로세스는 상황 인식을 생성하고 네트워크에서 애플리케이션 보안을 유지합니다. 예를 들어 새 애플리케이션이나 웹 서버가 배포될 때 알려야 하는 하드웨어 기반 경계 방화벽 그룹이 있는 경우 이 프로세스는 지정된 디바이스 그룹에 대한 동적 주소 그룹의 자동 새로 고침을 시작합니다. 그리고 동적 주소 개체를 참조하는 모든 정책 규칙은 이제 새로 배포되거나 수정된 애플리케이션 또는 웹 서버를 자동으로 포함하며 기준에 따라 안전하게 활성화할 수 있습니다.

서비스 정의 생성

- Panorama > VMware NSX > 서비스 정의

서비스 정의를 사용하면 VM 시리즈 방화벽을 NSX Manager에서 파트너 보안 서비스로 등록할 수 있습니다. Panorama에서 최대 32개의 서비스 정의를 정의하고 NSX Manager에서 동기화할 수 있습니다.

일반적으로 ESXi 클러스터의 각 테넌트에 대해 하나의 서비스 정의를 생성합니다. 각 서비스 정의는 방화벽을 배포하는 데 사용되는 OVF(PAN-OS 버전)를 지정하고 ESXi 클러스터에 설치된 VM 시리즈 방화벽에 대한 구성을 포함합니다. 구성을 지정하려면 서비스 정의에 서비스 정의를 사용하여 배포할 방화벽에 대한 고유한 템플릿, 고유한 디바이스 그룹 및 라이선스 인증 코드가 있어야 합니다. 방화벽이 배포되면 Panorama에 연결되고 방화벽이 보호할 각 테넌트 또는 부서에 대한 영역을 포함한 구성 설정과 서비스 정의에 지정된 디바이스 그룹에서 해당 정책 설정을 모두 수신합니다.

새 서비스 정의를 추가하려면 다음 표에 설명된 대로 설정을 구성하십시오.

필드	설명
이름	NSX Manager에 표시할 서비스의 이름을 입력합니다.
설명	(선택 사항) 이 서비스 정의의 목적 또는 기능을 설명하는 레이블을 입력합니다.
디바이스 그룹	이러한 VM 시리즈 방화벽이 할당될 디바이스 그룹 또는 디바이스 그룹 레이어을 선택하십시오. 자세한 내용은 Panorama > VMware NSX를 참조하십시오.

필드	설명
템플릿	VM 시리즈 방화벽이 할당될 템플릿을 선택합니다. 자세한 내용은 Panorama > 템플릿을 참조하십시오. 각 서비스 정의는 고유한 템플릿 또는 템플릿 스택(template stack)에 할당되어야 합니다. 템플릿에는 연결된 여러 영역(NSX용 NSX 서비스 프로파일 영역)이 있을 수 있습니다. 단일 테넌트 배포의 경우 템플릿에 하나의 영역(NSX 서비스 프로파일 영역)을 생성합니다. 다중 테넌트 배포가 있는 경우 각 하위 테넌트에 대한 영역을 생성합니다. 새 NSX 서비스 프로파일 영역을 생성하면 한 쌍의 가상 와이어 하위 인터페이스에 자동으로 연결됩니다. 자세한 내용은 네트워크 > 영역을 참조하십시오.
VM-Series OVF URL	NSX Manager가 OVF 파일에 액세스하여 새 VM 시리즈 방화벽을 프로비저닝할 수 있는 URL(IP 주소 또는 호스트 이름 및 경로)을 입력합니다.
그룹에 알림	드롭다운에서 알림 그룹을 선택합니다.

NSX Manager에 대한 액세스 구성

- Panorama > VMware NSX > 서비스 관리자

Panorama가 NSX Manager와 통신할 수 있도록 하려면 다음 표에 설명된 대로 설정을 추가하고 구성합니다.

서비스 관리자	설명
서비스 관리자 이름	VM 시리즈 방화벽을 서비스로 식별하는 이름을 입력합니다. 이 이름은 NSX Manager에 표시되며 주문형 VM 시리즈 방화벽을 배포하는 데 사용됩니다. 최대 63자를 지원합니다. 문자, 숫자, 하이픈 및 밑줄만 사용하십시오.
설명	(선택 사항) 이 서비스의 목적 또는 기능을 설명하는 레이블을 입력합니다.
NSX Manager URL	Panorama가 NSX Manager와의 연결을 설정하는 데 사용할 URL을 지정합니다.
NSX 관리자 로그인	NSX Manager에 구성된 인증 자격 증명(사용자명 및 암호)을 입력합니다. Panorama는 이러한 자격 증명을 사용하여 NSX Manager로 인증합니다.
NSX 관리자 암호	

서비스 관리자	설명
NSX Manager 암호 확인	
서비스 정의	이 서비스 관리자와 연관된 서비스 정의를 지정하십시오. 각 서비스 관리자는 최대 32개의 서비스 정의를 지원합니다.

Panorama에 변경 사항을 커밋하면 VMware Service Manager 창에 Panorama와 NSX Manager 간의 연결 상태가 표시됩니다.

동기화 상태	설명
상태	Panorama와 NSX Manager 간의 연결 상태를 표시합니다. 성공적인 연결이 등록됨으로 표시됨 - Panorama와 NSX Manager가 동기화되고 VM 시리즈 방화벽이 NSX Manager에 서비스로 등록됩니다. 연결에 실패한 경우 상태는 다음과 같을 수 있습니다. • 연결 오류 - NSX Manager와 네트워크 연결에 도달/설정할 수 없습니다. • 승인되지 않음 - 액세스 자격 증명(사용자명 및/또는 암호)이 올바르지 않습니다. • 등록되지 않음 - 서비스 관리자, 서비스 정의 또는 서비스 프로파일을 사용할 수 없거나 NSX Manager에서 삭제되었습니다. • 동기화되지 않음 - Panorama에 정의된 구성 설정이 NSX Manager에 정의된 것과 다릅니다. 실패 이유에 대한 자세한 내용을 보려면 동기화되지 않음을 클릭하세요. 예를 들어 NSX Manager에는 Panorama에 정의된 것과 동일한 이름을 가진 서비스 정의가 있을 수 있습니다. 오류를 수정하려면 오류 메시지에 나열된 서비스 정의 이름을 사용하여 NSX Manager에서 서비스 정의를 확인하십시오. Panorama와 NSX Manager의 구성이 동기화될 때까지 Panorama에 새 서비스 정의를 추가할 수 없습니다.
동적 개체 동기화	동적 개체 동기화를 클릭하여 NSX Manager에서 동적 개체 정보를 새로 고칩니다. 동적 개체를 동기화하면 가상 환경의 변경 사항에 대한 컨텍스트를 유지할 수 있고 정책 규칙에 사용되는 동적 주소 그룹을 자동으로 업데이트하여 애플리케이션을 안전하게 활성화할 수 있습니다.

동기화 상태	설명
	*Panorama*에서는 *NSX Manager*에서 동적으로 등록된 *IP* 주소만 볼 수 있습니다. *Panorama*는 방화벽에 직접 등록된 동적 *IP* 주소를 표시하지 않습니다. *VM* 정보 소스*(VM* 시리즈 *NSX* 버전 방화벽에서는 지원되지 않음*)* 또는 *XML API*를 사용하여 *IP* 주소를 방화벽에 동적으로 등록하는 경우 방화벽의 동적 *IP* 주소의 전체 목록*(Panorama*가 푸시한 것과 로컬에 등록된 것 모두*)*을 보려면 각 방화벽에 로그인해야 합니다.
NSX 구성 동기화	**NSX Config-Sync**를 선택하여 Panorama에 구성된 서비스 정의를 NSX Manager와 동기화합니다. Panorama에 보류 중인 커밋이 있는 경우 이 옵션을 사용할 수 없습니다. 동기화에 실패하면 오류 메시지의 세부 정보를 보고 오류가 Panorama에 있는지 NSX Manager에 있는지 확인합니다. 예를 들어 Panorama에서 서비스 정의를 삭제할 때 서비스 정의가 NSX Manager의 규칙에서 참조되는 경우 NSX Manager와의 동기화가 실패합니다. 오류 메시지의 정보를 사용하여 실패 이유와 수정 조치를 취해야 하는 위치(Panorama 또는 NSX Manager)를 확인합니다.

스티어링 규칙 생성

- Panorama > VMware NSX > 스티어링 규칙

스티어링 규칙은 클러스터의 게스트에서 VM 시리즈 방화벽으로 조정되는 트래픽을 결정합니다.

필드	설명
스티어링 규칙 자동 생성	다음과 같이 구성된 보안 규칙을 기반으로 스티어링 규칙을 생성합니다. • NSX Service Manager에 등록된 상위 또는 하위 디바이스 그룹에 속합니다. • 소스 및 대상과 동일한 영역이 있습니다(임의 방향 아님). • 하나의 영역만 있습니다. • 정책에 대해 구성된 고정 주소 그룹, IP 범위 또는 넷마스크가 없습니다. 기본적으로 Panorama를 통해 생성된 스티어링 규칙에는 NSX 서비스가 구성되어 있지 않으며 NSX 트래픽 방향은 inout으로 설정되어 있습니다. 스티어링 규칙을 생성한 후 개별 스티어링 규칙을 업데이트하여 NSX 트래픽 방향을 변경하거나 NSX 서비스를 추가할 수 있습니다. 스티어링 규칙을 자동 생성하면 Panorama가 다음 필드(설명 및 NSX 서비스 제외)를 자동으로 채웁니다.

필드	설명
이름	NSX Manager에 표시할 조정 규칙의 이름을 입력합니다. 자동 생성되면 Panorama는 프리픽스 auto_를 각 스티어링 규칙에 추가하고 보안 정책 규칙 이름의 공백을 밑줄(_)로 바꿉니다.
설명	(선택 사항) 이 서비스 정의의 목적 또는 기능을 설명하는 레이블을 입력합니다.
NSX 트래픽 방향	VM 시리즈 방화벽으로 리디렉션되는 트래픽의 방향을 지정합니다. • **inout** - NSX에서 INOUT 규칙을 생성합니다. 소스과 대상 사이를 이동하는 지정된 유형의 트래픽은 VM 시리즈 방화벽으로 리디렉션됩니다. Panorama는 자동 생성된 조종 규칙에 이 트래픽 방향을 사용합니다. • **in** - NSX에서 IN 규칙을 생성합니다. 대상에서 소스으로 이동하는 지정된 유형의 트래픽은 VM 시리즈 방화벽으로 리디렉션됩니다. • **out** - NSX에서 OUT 규칙을 생성합니다. 소스에서 대상으로 이동하는 지정된 유형의 트래픽은 VM 시리즈 방화벽으로 리디렉션됩니다.
NSX 서비스	VM 시리즈 방화벽으로 리디렉션할 애플리케이션(Active Directory Server, HTTP, DNS 등) 트래픽을 선택합니다.
디바이스 그룹	드롭다운에서 디바이스 그룹을 선택합니다. 선택한 디바이스 그룹에 따라 조정 규칙에 적용되는 보안 정책이 결정됩니다. 디바이스 그룹은 NSX 서비스 정의와 연결되어야 합니다.
보안 정책	자동 생성 조정 규칙의 기반이 되는 보안 정책 규칙입니다.

Panorama > 로그 수집 프로파일

Panorama가 외부 소스에서 로그를 수신할 수 있도록 하려면 로그 수집 프로파일을 사용하십시오. PAN-OS 8.0.0에서 Panorama(Panorama 모드)는 Syslog를 사용하여 Traps ESM 서버에서 로그를 수집할 수 있는 Syslog 수신기 역할을 할 수 있습니다. 새로운 외부 로그 소스에 대한 지원 및 최신 Traps ESM 버전에 대한 업데이트는 콘텐츠 업데이트를 통해 푸시됩니다.

로그 수집을 활성화하려면 Panorama를 Traps ESM 서버에서 Syslog 수신기로 구성하고 Panorama에서 로그 수집 프로파일을 정의하고 로그 수집 프로파일을 Log Collector 그룹에 연결해야 합니다.

새 외부 Syslog 수집 프로파일을 추가하려면 프로파일을 추가하고 다음 표에 설명된 대로 설정을 구성합니다.

필드	설명
이름	외부 Syslog 수집 프로파일의 이름을 입력합니다. 최대 255개의 프로파일을 추가할 수 있습니다.
소스 이름	로그를 보낼 외부 소스의 이름 또는 IP 주소를 입력합니다. 프로파일 내에서 최대 4개의 소스를 추가할 수 있습니다.
포트	네트워크를 통해 Panorama에 액세스할 수 있고 통신 및 수신에 사용할 포트를 입력합니다. Traps ESM의 경우 23000-23999 범위에서 값을 선택합니다. Panorama와 ESM 간의 통신을 활성화하려면 Traps ESM에서 동일한 포트 번호를 구성해야 합니다.
전송	TCP, UDP 또는 SSL을 선택합니다. SSL을 선택하는 경우 Panorama > Managed Collectors > 일반에서 보안 syslog 통신을 위한 인바운드 인증서를 구성해야 합니다.
외부 로그 유형	드롭다운에서 로그 유형을 선택합니다.
버전	드롭다운에서 버전을 선택합니다.

모니터 > 외부 로그를 사용하여 Traps ESM 서버에서 Panorama로 수집된 로그에 대한 정보를 봅니다.

Panorama > 로그 설정

로그 설정 페이지를 사용하여 다음 로그 유형을 외부 서비스로 포워딩합니다.

- Panorama 관리 서버(M-시리즈 어플라이언스 또는 Panorama 모드의 Panorama 가상 어플라이언스)가 로컬로 생성하는 시스템, 구성, User-ID 및 상관 관계 로그.
- 레거시 모드의 Panorama 가상 어플라이언스가 로컬에서 생성하거나 방화벽에서 수집하는 모든 유형의 로그입니다.

방화벽이 로그 수집기로 보내는 로그의 경우 로그 수집기 구성을 완료하여 외부 서비스로 포워딩할 수 있습니다.

시작하기 전에 외부 서비스에 대한 서버 프로파일을 정의해야 합니다(디바이스 > 서버 프로파일 > SNMP 트랩, 디바이스 > 서버 프로파일 > Syslog, 디바이스 > 서버 프로파일 > 이메일 및 디바이스 > 서버 프로파일 > HTTP 참조). 그런 다음 하나 이상의 일치 목록 프로파일을 추가하고 다음 표에 설명된 대로 설정을 구성합니다.

일치 목록 프로파일 설정	설명
이름	일치 목록 프로파일을 식별할 이름(최대 31자)을 입력합니다.
필터	기본적으로 Panorama는 일치 목록 프로파일을 추가하는 유형의 모든 로그를 포워딩합니다. 로그의 하위 집합을 포워딩하려면 드롭다운을 열고 기존 필터를 선택하거나 필터 빌더를 선택하여 새 필터를 추가합니다. 새 필터의 각 쿼리에 대해 다음 필드를 지정하고 쿼리를 추가합니다. • 커넥터 - 쿼리에 대한 커넥터 논리(및/또는)를 선택합니다. 논리에 부정을 적용하려면 부정을 선택합니다. 예를 들어, 신뢰할 수 없는 영역에서 로그를 포워딩하지 않으려면 무효를 선택한 다음 속성으로 영역을 선택하고 연산자로 같음을 선택한 다음 값 열에 신뢰할 수 없는 영역의 이름을 입력합니다. • 속성 - 로그 속성을 선택합니다. 옵션은 로그 유형에 따라 다릅니다. • 연산자 - 속성 적용 여부(예: 같음)를 결정하는 기준을 선택합니다. 사용 가능한 옵션은 로그 유형에 따라 다릅니다. • 값 - 일치시킬 쿼리의 속성 값을 지정합니다. 필터와 일치하는 로그를 표시하거나 내보내려면 필터링된 로그 보기를 선택합니다. 이 탭은 모니터링 탭 페이지(예: **Logs** > **Traffic** > 모니터링)와 동일한 옵션을 제공합니다.
설명	이 일치 목록 프로파일의 목적을 설명하려면 최대 1,024자의 설명을 입력하십시오.

일치 목록 프로파일 설정	설명
SNMP	SNMP 트랩으로 로그를 포워딩하려면 하나 이상의 SNMP 트랩 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > SNMP 트랩 참조).
이메일	이메일 알림으로 로그를 포워딩하려면 하나 이상의 이메일 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > 이메일 참조).
Syslog	하나 이상의 Syslog 서버 프로파일을 추가하여 로그를 syslog 메시지로 포워딩합니다(디바이스 > 서버 프로파일 > Syslog 참조).
HTTP	HTTP 요청으로 로그를 포워딩하려면 하나 이상의 HTTP 서버 프로파일을 추가합니다(디바이스 > 서버 프로파일 > HTTP 참조).
기본 제공 작업	시스템 로그 및 구성 로그를 제외한 모든 로그 유형을 사용하여 작업을 구성할 수 있습니다. • 작업을 추가하고 설명하는 이름을 입력합니다. • 태그를 지정할 IP 주소(소스 주소 또는 대상 주소)를 선택합니다. • 태그 추가 또는 태그 제거 작업을 선택합니다. • 이 디바이스의 로컬 User-ID 에이전트 또는 원격 User-ID 에이전트에 태그를 배포할지의 여부를 선택합니다. • 원격 디바이스 **User-ID** 에이전트에 태그를 배포하려면 포워딩을 활성화할 HTTP 서버 프로파일을 선택합니다. • IP 주소-태그 매핑이 유지되는 시간을 분 단위로 설정하도록 IP-태그 타임아웃를 구성합니다. 타임아웃을 0으로 설정하면 IP-태그 매핑이 타임아웃되지 않음을 의미합니다(범위는 0 ~ 43200(30일), 기본값은 0). 태그 추가 작업으로만 타임아웃을 구성할 수 있습니다. • 대상 소스 또는 대상 IP 주소에서 적용하거나 제거할 태그를 입력하거나 선택합니다. 상관 관계 로그 및 HIP 일치 로그에서 소스 IP 주소에만 태그를 지정할 수 있습니다.

Panorama > 서버 프로파일 > SCP

- Panorama > 서버 프로파일 > SCP

Panorama > 서버 프로파일 > **SCP**를 선택하여 보안 복사 프로토콜(SCP) 서버가 네트워크를 통해 파일을 안전하게 복사 및 전송하도록 설정을 구성합니다. 관리형 방화벽, 로그 수집기 및 Air-gapped Panorama™ 관리 서버에서 관리하는 WildFire® 어플라이언스에서 콘텐츠 업데이트를 자동으로 다운로드하고 설치할 수 있습니다.

SCP 서버 설정	설명
이름	서버 프로파일을 식별할 수 있는 이름을 입력합니다(최대 31자). 이름은 대/소문자에 민감하며 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
서버	서버 IP 주소 또는 FQDN을 입력합니다.
포트	파일 전송을 위한 서버 포트를 입력합니다(범위는 1–65,535, 기본값은 22).
사용자명	SCP 서버에 액세스하는 데 사용되는 사용자명을 입력합니다.
비밀번호 비밀번호 확인	SCP 서버에 액세스하는 데 사용되는 사용자명의 대소문자 구분 암호를 입력하고 확인합니다.

Panorama > 예정된 구성 내보내기

Panorama 및 방화벽에서 실행 중인 모든 구성의 내보내기를 예약하려면 내보내기 작업을 추가하고 다음 표에 설명된 대로 설정을 구성합니다.

*Panorama*가 고가용성*(HA)* 구성을 사용하는 경우 페일오버 후에도 예약된 내보내기가 계속 되도록 각 피어에서 이러한 지침을 수행해야 합니다. *Panorama*는 *HA* 피어 간에 예약된 구성 내보내기를 동기화하지 않습니다.

예약된 구성 내보내기 설정	설명
이름	이름을 입력하여 구성 내보내기 작업(최대 31자)을 식별합니다. 이름은 대/소문자에 민감하며 고유해야 합니다. 문자, 숫자, 하이픈 및 밑줄만 사용합니다.
설명	선택적 설명을 입력합니다.
활성화	내보내기 작업을 사용하도록 선택합니다.
예약된 수출 시작 시간(일일)	내보내기를 시작하는 하루 중 시간을 지정합니다(24시간 시계, 형식 HH:MM).
프로토콜	Panorama에서 원격 호스트로 로그를 내보내는 데 사용할 프로토콜을 선택합니다. 보안복사(**SCP**)는보안 프로토콜입니다. **FTP**는 그렇지 않습니다.
호스트 이름	대상 SCP 또는 FTP 서버의 IP 주소 또는 호스트 이름을 입력합니다.
포트	대상 서버에서 포트 번호를 입력합니다.
경로	내보낸 구성을 저장하는 대상 서버에서 폴더 또는 디렉토리에 대한 경로를 지정합니다. 예를 들어 구성 번들이 Panorama라는 최상위 폴더 내에서 exported_config 라는 폴더에 저장되는 경우 각 서버 유형에 대한 구문은 다음과 같은 것입니다. • SCP 서버: /Panorama/exported_config • FTP 서버: //Panorama/exported_config 다음 문자: **.**(기간), **+**, **{** and **}**, **/**, **-**, **_**, **0**-**9**, **a**-**z** 및 **A**-**Z**. 파일 경로에서 공백이 지원되지 않습니다.

예약된 구성 내보내기 설정	설명
FTP 패시브 모드 사용	FTP 패시브 모드를 사용하도록 선택합니다.
사용자명	대상 시스템에 액세스하는 데 필요한 사용자명을 지정합니다.
암호 / 암호 확인	대상 시스템에 액세스하는 데 필요한 암호를 지정합니다. 최대 길이가 15자인 암호를 사용합니다. 암호가 15자를 초과하는 경우 방화벽이 SCP 서버에 연결하려고 할 때 암호를 암호화하고 암호화된 암호의 길이는 최대 63자일 수 있으므로 테스트 SCP 연결이 오류를 표시합니다.
테스트 SCP 서버 연결	Panorama와 SCP 호스트/서버 간의 통신을 테스트하도록 선택합니다. SCP 서버 연결을 테스트하고 안전한 데이터 전송을 활성화하기 위해 일반 텍스트 비밀번호를 입력한 다음 비밀번호 확인을 입력하라는 팝업 창이 표시됩니다. Panorama에 HA 구성이 있는 경우 각 HA 피어에서 이 단계를 수행하여 각 피어가 SCP 서버의 호스트 키를 수락하도록 합니다. Panorama가 SCP 서버에 성공적으로 연결할 수 있는지 여부입니다.

Panorama > 소프트웨어

이 페이지를 사용하여 Panorama 관리 서버에서 Panorama 소프트웨어 업데이트를 관리하십시오.

- Panorama 소프트웨어 업데이트 관리
- Panorama 소프트웨어 업데이트 정보 표시

Panorama 소프트웨어 업데이트 관리

다음 표에 설명된 작업을 수행하려면 **Panorama** > 소프트웨어를 선택하십시오.

기본적으로 *Panorama* 관리 서버는 최대 *2*개의 소프트웨어 업데이트를 저장합니다. 최신 업데이트를 위한 공간을 확보하기 위해 서버는 가장 오래된 업데이트를 자동으로 삭제합니다. Panorama가 저장하는 소프트웨어 이미지 수를 변경하고 이미지를 수동으로 삭제하여 공간을 확보할 수 있습니다.

버전 호환성에 대한 중요한 정보는 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치를 참조하십시오.

작업	설명
지금 확인	Panorama가 인터넷에 액세스할 수 있는 경우 지금 확인하여 최신 업데이트 정보를 표시하십시오(Panorama 소프트웨어 업데이트 정보 표시 참조). Panorama가 외부 네트워크에 액세스할 수 없는 경우 브라우저를 사용하여 소프트웨어 업데이트 사이트를 방문하여 업데이트 정보를 확인하십시오.
업로드	Panorama가 인터넷에 액세스할 수 없을 때 소프트웨어 이미지를 업로드하려면 브라우저를 사용하여 소프트웨어 업데이트 사이트를 방문하고 원하는 릴리스를 찾은 다음 Panorama가 액세스할 수 있는 컴퓨터에 소프트웨어 이미지를 다운로드하고 **Panorama** > 소프트웨어를 선택한 다음 업로드를 클릭한 다음 찾아보기를 클릭합니다. 소프트웨어 이미지를 선택한 다음 확인을 클릭합니다. 업로드가 완료되면 다운로드됨 열에 확인 표시가 표시되고 작업 열에 설치가 표시됩니다.
확인	Panorama가 인터넷에 액세스할 수 있는 경우 원하는 릴리스를 확인(작업 열)합니다. 업그레이드할 디바이스(배포 열)를 선택하고 업그레이드 소스로 **Panorama**를 선택한 후 다운로드를 클릭합니다. 다운로드가 완료되면 다운로드됨 열에 확인 표시가 표시됩니다. *PAN-OS 10.2.0*에서는 ***SCP*** 서버 및 업데이트 서버를 다운로드 소스로 사용할 수 없습니다.

작업	설명
설치	소프트웨어 이미지를 설치합니다(작업 열). 설치가 완료되면 Panorama가 재부팅되는 동안 로그아웃됩니다. *Panorama*는 정기적으로 *FSCK(*파일 시스템 무결성 검사*)*를 수행하여 *Panorama* 시스템 파일의 손상을 방지합니다. 이 검사는 *8*번의 재부팅 후 또는 마지막 *FSCK* 이후 *90*일간 발생하는 재부팅 시 수행됩니다. *FSCK*가 진행 중이고 완료될 때까지 로그인할 수 없는 경우 웹 인터페이스 및 *SSH* 로그인 화면에 경고가 나타납니다. 이 프로세스를 완료하는 데 걸리는 시간은 스토리지 시스템 크기에 따라 다릅니다. 대규모 시스템의 경우 *Panorama*에 다시 로그인하려면 몇 시간이 걸릴 수 있습니다. 진행 상황을 보려면 *Panorama*에 대한 콘솔 액세스를 설정하세요.
릴리스 노트	Panorama에서 인터넷에 액세스할 수 있는 경우 원하는 소프트웨어 릴리스에 대한 릴리스 정보에 액세스하여 릴리스 변경 사항, 수정 사항, 알려진 문제, 호환성 문제 및 기본 동작에 대한 변경 사항을 검토할 수 있습니다. Panorama에서 인터넷에 액세스할 수 없는 경우 브라우저를 사용하여 소프트웨어 업데이트 사이트를 방문하고 적절한 릴리스를 다운로드하십시오.
	더 이상 필요하지 않거나 더 많은 이미지를 위한 공간을 확보하려는 경우 소프트웨어 이미지를 삭제합니다.

Panorama 소프트웨어 업데이트 정보 표시

Panorama > **Software**를 선택하여 다음 정보를 표시합니다. Palo Alto Networks의 최신 정보를 표시하려면 지금 확인을 클릭하십시오.

소프트웨어 및 콘텐츠 업데이트 정보	설명
버전	Panorama 소프트웨어 버전
크기	소프트웨어 이미지의 크기(MB)입니다.
출시일	Palo Alto Networks에서 업데이트를 제공한 날짜 및 시간입니다.
사용 가능	이미지를 설치할 수 있는지의 여부를 나타냅니다.

소프트웨어 및 콘텐츠 업데이트 정보	설명
현재 설치됨	확인 표시는 설치된 업데이트를 나타냅니다.
작업	이미지에 사용할 수 있는 작업(다운로드, 설치 또는 다시 설치)을 나타냅니다.
릴리즈 노트	릴리스 정보를 클릭하여 원하는 소프트웨어 릴리스에 대한 릴리스 정보에 액세스하고 릴리스 변경 사항, 수정 사항, 알려진 문제, 호환성 문제 및 기본 동작의 변경 사항을 검토하십시오.
	더 이상 필요하지 않거나 추가 다운로드 또는 업로드를 위한 공간을 확보하기 위해 업데이트를 삭제합니다.

Panorama > 디바이스 배포

Panorama를 사용하여 여러 방화벽 및 로그 수집기에 소프트웨어 및 콘텐츠 업데이트를 배포하고 방화벽 라이선스를 관리할 수 있습니다.

무엇을 찾고 계신가요?	참조:
방화벽 및 로그 수집기에 소프트웨어 및 콘텐츠 업데이트를 배포합니다.	소프트웨어 및 콘텐츠 업데이트 관리
어떤 소프트웨어 및 콘텐츠 업데이트가 설치되어 있거나 다운로드 및 설치가 가능한지 확인하십시오.	소프트웨어 및 콘텐츠 업데이트 정보 표시
방화벽 및 로그 수집기에 대한 자동 콘텐츠 업데이트 예약	동적 콘텐츠 업데이트 예약
Panorama에서 하나 이상의 방화벽 콘텐츠 버전을 되돌립니다.	Panorama에서 콘텐츠 버전 되돌리기
라이선스 보기, 활성화, 비활성화 및 새로 고침. 방화벽 라이선스의 상태를 참조하십시오.	방화벽 라이선스 관리
더 찾고 계십니까?	라이선스 및 업데이트를 관리합니다.

소프트웨어 및 콘텐츠 업데이트 관리

- Panorama > 디바이스 배포 > 소프트웨어

Panorama는 소프트웨어 및 콘텐츠 업데이트를 방화벽 및 로그 수집기에 배포하기 위한 다음 옵션을 제공합니다.

관리*(MGT)* 인터페이스의 트래픽을 줄이기 위해 업데이트 배포에 별도의 인터페이스를 사용하도록 *Panorama*를 구성할 수 있습니다*(*Panorama > 설정 > 인터페이스 참조*)*.

Panorama 디바이스 배포 옵션	설명
다운로드	Panorama가 인터넷에 연결되어 있을 때 소프트웨어 또는 콘텐츠 업데이트를 배포하려면 업데이트를 다운로드하십시오. 다운로드가 완료되면 사용 가능 열에 다운로드됨이 표시됩니다. 다음을 수행할 수 있습니다. • PAN-OS/Panorama 소프트웨어 업데이트 또는 콘텐츠 업데이트를 설치합니다. • GlobalProtect™ 앱 또는 SSL VPN 클라이언트 소프트웨어 업데이트를 활성화하십시오.
업그레이드	BrightCloud URL 필터링 콘텐츠 업데이트를 사용할 수 있는 경우 업그레이드를 클릭합니다. 업그레이드에 성공하면 방화벽에 업데이트를 설치할 수 있습니다.
설치	PAN-OS 소프트웨어, Panorama 소프트웨어 또는 콘텐츠 업데이트를 다운로드하거나 업로드한 후 작업 열에서 설치를 클릭하고 다음을 선택합니다. • 디바이스 - 업데이트를 설치할 방화벽 또는 로그 수집기를 선택합니다. 목록이 길면 필터를 사용하십시오. 고가용성(HA) 피어인 방화벽을 그룹화하려면 **Group HA Peers**를 선택합니다. 이를 통해 HA 구성이 있는 방화벽을 쉽게 식별할 수 있습니다. 특정 방화벽 또는 로그 수집기만 표시하려면 해당 방화벽 또는 로그 수집기를 선택한 다음 선택 항목 필터링을 선택합니다. • 디바이스에만 업로드(소프트웨어만) - 소프트웨어를 자동으로 설치하지 않고 로드하려면 선택합니다. 소프트웨어를 수동으로 설치해야 합니다. • 설치 후 디바이스 재부팅(소프트웨어만 해당) - 설치 프로세스가 방화벽 또는 로그 수집기를 자동으로 재부팅하도록 지정하려면 선택합니다. 재부팅할 때까지 설치를 완료할 수 없습니다. • 콘텐츠 업데이트에서 새 앱 비활성화(애플리케이션 및 위협에만 해당) - 마지막으로 설치된 업데이트와 관련하여 새로운 업데이트의 애플리케이션을 비활성화하려면 선택합니다. 이는 최신 위협으로부터 보호하는 동시에 정책 업데이트를 준비한 후 애플리케이션을 활성화할 수 있는 유연성을 제공합니다. 그런 다음 애플리케이션을 활성화하려면 방화벽에 로그인하고 디바이스 > 동적 업데이트를 선택한 다음 기능 열에서 앱을 클릭하여 새 애플리케이션을 표시하고 활성화하려는 각 애플리케이션에 대해 활성화/비활성화를 클릭합니다. ***Panorama*** > 관리 디바이스를 선택하여 방화벽 소프트웨어 및 콘텐츠 업데이트를 설치하거나 ***Panorama*** > 관리 수집기를 선택하여 전용 로그 수집기용 소프트웨어 업데이트를 설치할 수도 있습니다.
활성화	GlobalProtect 앱 소프트웨어 업데이트를 다운로드하거나 업로드한 후 작업 열에서 활성화를 클릭하고 다음과 같이 옵션을 선택합니다.

Panorama 디바이스 배포 옵션	설명
	• 디바이스 - 업데이트를 활성화할 방화벽을 선택합니다. 목록이 길면 필터를 사용하십시오. 고가용성(HA) 피어인 방화벽을 그룹화하려면 **Group HA Peers**를 선택합니다. 이를 통해 HA 구성이 있는 방화벽을 쉽게 식별할 수 있습니다. 특정 방화벽만 표시하려면 방화벽을 선택한 다음 선택 필터를 선택합니다. • 디바이스에만 업로드 - PAN-OS가 업로드된 이미지를 자동으로 활성화하지 않도록 하려면 선택합니다. 방화벽에 로그인하여 활성화해야 합니다.
릴리스 노트	릴리스 정보를 클릭하여 원하는 소프트웨어 릴리스에 대한 릴리스 정보에 액세스하고 릴리스 변경 사항, 수정 사항, 알려진 문제, 호환성 문제 및 기본 동작의 변경 사항을 검토하십시오.
문서	문서를 클릭하여 원하는 콘텐츠 릴리스에 대한 릴리스 정보에 액세스합니다.
☒	더 이상 필요하지 않거나 더 많은 다운로드 또는 업로드를 위한 공간을 확보하려는 경우 소프트웨어 또는 콘텐츠 업데이트를 삭제합니다.
지금 확인	소프트웨어 및 콘텐츠 업데이트 정보를 표시하려면 지금 확인하십시오.
업로드	Panorama가 인터넷에 연결되어 있지 않을 때 소프트웨어 또는 콘텐츠 업데이트를 배포하려면 소프트웨어 업데이트 또는 동적 업데이트 사이트에서 컴퓨터로 업데이트를 다운로드하고 업데이트 유형에 해당하는 **Panorama** > 디바이스 배포 페이지를 선택한 다음 업로드를 클릭하고 업데이트 유형(콘텐츠 업데이트만 해당)을 선택하고, 업로드된 파일을 선택한 다음 확인을 클릭합니다. 그런 다음 업데이트를 설치하거나 활성화하는 단계는 유형에 따라 다릅니다. • **PAN-OS** 또는 **Panorama** 소프트웨어 - 업로드가 완료되면 다운로드됨 열에 확인 표시가 표시되고 작업 열에 설치가 표시될 수 있습니다. • **GlobalProtect** 클라이언트 또는 **SSL VPN** 클라이언트 소프트웨어 - 파일에서 활성화합니다. • 동적 업데이트 - 파일에서 설치합니다.
파일에서 설치	콘텐츠 업데이트를 업로드한 후 파일에서 설치를 클릭하고 콘텐츠 유형을 선택한 다음 업데이트 파일 이름을 선택하고 방화벽 또는 로그 수집기를 선택합니다.
파일에서 활성화	GlobalProtect 앱 소프트웨어 업데이트를 업로드한 후 파일에서 활성화를 클릭하고 업데이트 파일 이름을 선택한 다음 방화벽을 선택합니다.
일정	동적 콘텐츠 업데이트를 예약하려면 선택합니다.

소프트웨어 및 콘텐츠 업데이트 정보 표시

- Panorama > 디바이스 배포 > 소프트웨어

Panorama > **Device Deployment** > **Software**를 선택하여 현재 설치되었거나 다운로드 및 설치가 가능한 PAN-OS 소프트웨어, **GlobalProtect** 클라이언트 소프트웨어 및 동적 업데이트(콘텐츠)를 표시합니다. 동적 업데이트 페이지는 콘텐츠 유형(바이러스 백신, 애플리케이션 및 위협, URL 필터링, WildFire)별로 정보를 구성하고 업데이트된 정보를 마지막으로 확인한 날짜와 시간을 표시합니다. Palo Alto Networks의 최신 소프트웨어 또는 콘텐츠 정보를 표시하려면 지금 확인을 클릭하십시오.

소프트웨어 및 콘텐츠 업데이트 정보	
버전	소프트웨어 또는 콘텐츠 업데이트 버전.
파일 이름	업데이트 파일의 이름입니다.
플랫폼	업데이트에 대해 지정된 방화벽 또는 로그 수집기 모델입니다. 숫자는 하드웨어 방화벽 모델을 나타내고(예: `7000`은 PA-7000 시리즈 방화벽을 나타냄) `vm`은 VM 시리즈 방화벽을 나타내고 `m`은 M 시리즈 어플라이언스를 나타냅니다.
특징	(콘텐츠만 해당) 콘텐츠 버전에 포함될 수 있는 서명 유형을 나열합니다.
유형	(컨텐츠만 해당) 다운로드에 전체 데이터베이스 업데이트 또는 증분 업데이트가 포함되는지의 여부를 나타냅니다.
크기	업데이트 파일의 크기입니다.
출시일	Palo Alto Networks에서 업데이트를 제공한 날짜 및 시간입니다.
사용 가능	(PAN-OS 또는 Panorama 소프트웨어만 해당) 업데이트가 다운로드 또는 업로드되었음을 나타냅니다.
다운로드됨	(SSL VPN 클라이언트 소프트웨어, GlobalProtect 클라이언트 소프트웨어 또는 콘텐츠만 해당) 확인 표시는 업데이트가 다운로드되었음을 나타냅니다.
작업	업데이트에서 수행할 수 있는 작업을 나타냅니다. 다운로드, 업그레이드, 설치 또는 활성화합니다.
문서화	(콘텐츠만 해당) 원하는 콘텐츠 릴리스에 대한 릴리스 정보에 대한 링크를 제공합니다.
릴리즈 노트	(소프트웨어만 해당) 원하는 소프트웨어 릴리스에 대한 릴리스 정보에 대한 링크를 제공합니다.

소프트웨어 및 콘텐츠 업데이트 정보	
	더 이상 필요하지 않거나 더 많은 다운로드 또는 업로드를 위한 공간을 확보하려는 경우 업데이트를 삭제합니다.

동적 콘텐츠 업데이트 예약

- Panorama > 디바이스 배포 > 동적 업데이트

업데이트의 자동 다운로드 및 설치를 예약하려면 일정을 클릭하고 추가를 클릭하고 다음 표에 설명된 대로 설정을 구성합니다.

동적 업데이트 일정 설정	
이름	예약된 작업을 식별하는 이름을 입력합니다(최대 31자). 이름은 대소문자를 구분하고 고유해야 하며 문자, 숫자, 하이픈 및 밑줄만 포함할 수 있습니다.
Disabled	예약된 작업을 비활성화하려면 선택합니다.
소스 다운로드	콘텐츠 업데이트의 다운로드 소스를 선택합니다. Palo Alto Networks 업데이트 서버 또는 **SCP** 서버에서 콘텐츠 업데이트를 다운로드하도록 선택할 수 있습니다.
SCP 프로파일(SCP만 해당)	다운로드할 구성된 SCP 프로파일을 선택합니다.
SCP 경로(SCP 전용)	콘텐츠 업데이트를 다운로드할 SCP 서버의 특정 경로를 입력합니다.
유형	예약할 콘텐츠 업데이트 유형 선택: 앱, 앱 및 위협, 바이러스 백신, **WildFire** 또는 **URL** 데이터베이스.
반복	Panorama가 업데이트 서버에 체크인하는 인터벌을 선택합니다. 반복 옵션은 업데이트 유형에 따라 다릅니다.
시간	매일 업데이트의 경우 24시간제에서 시간을 선택합니다. 주간 업데이트의 경우 24시간제에서 요일 및 시간을 선택합니다.
콘텐츠 업데이트에서 새 앱 비활성화	업데이트 유형을 앱 또는 앱 및 위협으로 설정하고 작업이 다운로드 및 설치로 설정된 경우에만 콘텐츠 업데이트에서 새 앱을 비활성화할 수 있습니다. 마지막으로 설치된 업데이트와 관련하여 새로운 업데이트의 애플리케이션을 비활성화하려면 선택합니다. 이는 최신 위협으로부터 보호하는 동시에 정책 업데이트를 준비한 후 애플리케이션을 활성화할 수 있는 유연성을 제공합니다. 그런 다음 애플

동적 업데이트 일정 설정	
	리케이션을 활성화하려면 방화벽에 로그인하고 디바이스 > 동적 업데이트를 선택한 다음 기능 열에서 앱을 클릭하여 새 애플리케이션을 표시하고 활성화하려는 각 애플리케이션에 대해 활성화/비활성화를 클릭합니다.
작업	• 다운로드 전용 - Panorama™가 예약된 업데이트를 다운로드합니다. 방화벽 및 로그 수집기에 업데이트를 수동으로 설치해야 합니다. • 다운로드 및 설치 - Panorama는 예약된 업데이트를 다운로드하고 자동으로 설치합니다. • 다운로드 및 **SCP** - Panorama는 콘텐츠 업데이트 패키지를 다운로드하여 지정된 SCP 서버로 전송합니다.
디바이스	디바이스를 선택한 다음 예약된 콘텐츠 업데이트를 수신할 방화벽을 선택합니다.
로그 수집기	로그 수집기를 선택한 다음 예약된 콘텐츠 업데이트를 수신할 관리되는 수집기를 선택합니다.

Panorama에서 콘텐츠 버전 되돌리기

- Panorama > 디바이스 배포 > 동적 업데이트

하나 이상의 방화벽에 대한 애플리케이션, 애플리케이션 및 위협, 안티바이러스, WildFire 및 WildFire 콘텐츠 업데이트의 콘텐츠 버전을 Panorama에서 이전에 설치된 콘텐츠 버전으로 신속하게 되돌립니다. 되돌리려는 콘텐츠 버전은 현재 방화벽에 설치된 버전보다 이전 버전이어야 합니다. 콘텐츠 되돌리기는 8.1을 실행하는 Panorama에서 사용할 수 있습니다. 되돌리기 기능이 방화벽에서 로컬로 사용 가능한 한 방화벽의 콘텐츠를 되돌릴 수 있습니다.

필드	설명
필터	콘텐츠를 되돌리려는 디바이스를 필터링합니다. 다음을 기준으로 필터링할 수 있습니다. • 디바이스 상태 • 플랫폼 • 디바이스 그룹 • 템플릿 • 태그 • HA 상태 • 소프트웨어 버전(PAN-OS) • 현재 콘텐츠 버전

필드	설명
디바이스	되돌릴 디바이스를 하나 이상 선택하십시오. 다음 디바이스 정보를 표시합니다. • 디바이스 이름 - 방화벽의 이름입니다. • 현재 버전 - 디바이스에 설치된 현재 콘텐츠 버전입니다. 콘텐츠 버전이 설치되어 있지 않으면 열에 0이 표시됩니다. • 이전 버전(콘텐츠) - PAN 8.1 이상을 실행하는 방화벽에 이전에 설치된 콘텐츠 버전입니다. 콘텐츠 버전이 이전에 설치되지 않았거나 방화벽이 8.1 이전의 PAN-OS 버전을 실행 중인 경우 열이 비어 있습니다. • 소프트웨어 버전 - 디바이스에 설치된 현재 PAN-OS 버전입니다. • HA 상태 - HA 쌍에 있을 때 HA 상태를 표시합니다. 디바이스가 HA 쌍에 없는 경우 열이 비어 있습니다.
그룹 HA 쌍	HA 피어를 그룹화하려면 이 체크박스를 선택합니다.

되돌릴 디바이스를 선택했으면 확인을 클릭합니다.

방화벽 라이선스 관리

- Panorama > 디바이스 배포 > 라이선스

Panorama > **Device Deployment** > **Licenses**를 선택하여 다음 작업을 수행합니다.

- 인터넷에 직접 액세스할 수 없는 방화벽의 라이선스 업데이트 - 새로 고침을 클릭합니다.
- 방화벽에서 라이선스 활성화 - 방화벽에서 라이선스를 활성화하려면 활성화를 클릭하고 방화벽을 선택한 다음 인증 코드 열에 Palo Alto Networks가 방화벽에 제공한 인증 코드를 입력합니다.
- VM 시리즈 방화벽에 설치된 모든 라이선스 및 구독/자격 비활성화 - **VM** 비활성화를 클릭하고 방화벽을 선택한 다음(목록에는 PAN-OS 7.0 이상의 버전을 실행하는 방화벽만 표시됨) 다음을 클릭합니다.
  - 계속 - 라이선스를 비활성화하고 라이선스 서버에 변경 사항을 자동으로 등록합니다. 라이선스는 계정에 다시 적립되어 재사용할 수 있습니다.
  - 수동으로 완료 - 토큰 파일을 생성합니다. Panorama에서 인터넷에 직접 액세스할 수 없는 경우 이 옵션을 사용합니다. 비활성화 프로세스를 완료하려면 지원 포털에 로그인하고 자산을 선택한 다음 라이선스 비활성화를 클릭하고 토큰 파일을 업로드하고 제출을 클릭해야 합니다. 비활성화 프로세스를 완료한 후.

관리되는 방화벽에 대한 현재 라이선스 상태를 볼 수도 있습니다. 인터넷에 직접 액세스할 수 있는 방화벽의 경우 Panorama는 자동으로 라이선스 서버에 일일 체크인을 수행하고 라이선스 업데이트 및 갱신을 검색하여 방화벽으로 푸시합니다. 체크인은 오전 1시에서 2시 사이에 발생하도록 하드 코딩되어 있으며, 이 일정을 변경할 수 없습니다.

방화벽 라이선스 정보	
디바이스	방화벽 이름입니다.
가상 시스템	방화벽이 여러 가상 시스템을 ✓ 지원하는지 ⊗ 지원하지 않는지를 나타냅니다.
위협 예방 URL 지원 GlobalProtect Gateway GlobalProtect 포털 WildFire	라이선스가 활성 ✓ 비활성 ⊗ 또는 만료 ⚠ 되었는지의 여부를 나타냅니다(만료 날짜 포함).
VM 시리즈 용량	이것이 VM 시리즈 방화벽이 ✓ 인지 ⊗ 아닌지를 나타냅니다.

Panorama > 디바이스 등록 인증 키

새 방화벽, 로그 수집기 및 WildFire 어플라이언스를 Panorama™ 관리 서버에 온보딩할 때 보안 태세를 강화하려면 처음 연결할 때 새 디바이스와 Panorama 관리 서버 간의 상호 인증을 위한 디바이스 등록 인증 키를 생성하십시오. 특정 값으로 인증 키를 구성할 수 있습니다. 키 유효 시간, 새 방화벽을 온보딩하기 위해 디바이스 등록 인증 키를 사용할 수 있는 횟수를 결정하는 횟수, 디바이스 등록 인증 키가 있는 하나 이상의 일련번호 목록 유효하고 인증 키가 유효한 디바이스 유형을 지정합니다. Panorama에서 인증 키를 생성한 후에는 Panorama 관리에 온보딩하는 동안 새 방화벽, 로그 수집기 또는 WildFire 어플라이언스에 해당 키를 추가해야 합니다.

디바이스 등록 인증 키 필드	설명
이름	디바이스 등록 인증 키의 이름입니다. 이름은 대소문자를 구분하고 전체 디바이스 그룹 레이어에서 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.
유효 기간	키 유효 시간은 디바이스 등록 인증 키가 새 방화벽, 로그 수집기 및 WildFire 어플라이언스를 온보딩하는 데 유효한 일, 시간 및 분 수를 표시합니다.
카운트	디바이스 등록 인증 키를 사용하여 새 방화벽, 로그 수집기 및 WildFire 어플라이언스를 온보딩할 수 있는 횟수입니다.
시리얼	디바이스 등록 인증 키가 유효한 하나 이상의 새 방화벽, 로그 수집기 및 WildFire 어플라이언스의 일련번호입니다.
유형	인증 키가 유효한 디바이스 유형(##, ### 또는 ## ###).

디바이스 등록 인증 키 추가

새 방화벽, 로그 수집기 및 WildFire 어플라이언스를 Panorama에 온보딩하기 위해 디바이스 등록 인증 키를 추가하고 구성합니다.

디바이스 등록 인증 키 설정	설명
이름	디바이스 등록 인증 키를 식별할 이름을 입력합니다. 이름은 대소문자를 구분하고 전체 디바이스 그룹 레이어에서 고유해야 하며 문자, 숫자, 공백, 하이픈 및 밑줄만 포함할 수 있습니다.

디바이스 등록 인증 키 설정	설명
유효 기간	디바이스 등록 인증 키를 사용하여 새 방화벽, 로그 수집기 및 WildFire 어플라이언스를 온보딩할 수 있는 기간에 대한 키 유효 시간을 지정합니다.
카운트	인증 키를 사용하여 새 방화벽, 로그 수집기 및 WildFire 어플라이언스를 온보딩할 수 있는 횟수를 지정합니다.
디바이스 종류	디바이스 등록 인증 키를 사용할 수 있는 디바이스를 지정합니다. 방화벽, 로그 수집기 또는 모두(기본값).
디바이스	방화벽, 로그 수집기 및 WildFire 어플라이언스 일련번호를 입력하여 디바이스 등록 인증 키가 유효한 방화벽, 로그 수집기 및 WildFire 어플라이언스를 지정합니다.