paloalto NETWORKS TECHDOCS

PAN-OS® 네트워킹 관리자 가이드

Version 10.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

June 6, 2022

Table of Contents

네트워킹

모든 Palo Alto Networks® 차세대 방화벽은 동적 라우팅, 스위칭 및 VPN 연결을 지원하는 유연한 네트워킹 아키텍처를 제공하며, 이를 통해 거의 모든 네트워킹 환경에 방화벽을 배치할 수 있습니다.

- 네트워킹 소개

네트워킹 소개

네트워킹은 데이터를 수신하고 처리하고 전달할 수 있어야 하기 때문에 방화벽의 기본 빌딩 블록입니다. 방화벽에서 이더넷 포트를 구성할 때 탭, 가상 와이어, 레이어 2, 레이어 3 또는 AE 인터페이스 배포 중에서 선택할 수 있습니다. 또한 다양한 네트워크 세그먼트에 통합할 수 있도록 다양한 포트에서 다양한 유형의 인터페이스를 구성할 수 있습니다.

네트워킹을 시작하려면 먼저 PAN-OS® 관리자 가이드의 시작하기 항목에 액세스해야 합니다. 여기에서 네트워크 분할에 대해 배우고 인터페이스 및 존을 구성합니다. 이 초기 작업은 인터넷, 내부 네트워크 및 데이터 센터 애플리케이션에 연결하도록 레이어 3 인터페이스를 구성하는 방법을 보여줍니다.

이 PAN-OS 네트워킹 관리자 가이드는 탭, 가상 와이어, 레이어 2, 레이어 3 및 AE 인터페이스를 구성하는 방법에 대한 주제와 함께 해당 정보에 대해 자세히 설명합니다. 네트워크 인터페이스가 구성된 후 내부 검토 또는 감사를 위해 PDF 또는 CSV로 구성 테이블 데이터를 내보내기할 수 있습니다.

이 가이드는 또한 방화벽이 여러 가상 라우터를 지원하여 다른 서브넷에 대한 레이어 3 경로를 확보하고 별도의 경로 집합을 유지 관리하는 방법에 대해서도 설명합니다. 나머지 장에서는 정적 경로, 동적 라우팅 프로토콜 및 방화벽에서 네트워킹을 지원하는 주요 기능에 대해 설명합니다.

활성화하기로 결정할 수Advanced 라우팅 있습니다. 고급 라우팅 엔진은 가상 라우터 대신 논리적 라우터를 사용합니다.

- 인터페이스 구성
- 가상 라우터
- 서비스 경로
- 정적 경로
- RIP
- OSPF
- BGP
- IP 멀티캐스트
- 경로 재분배
- GRE 터널
- DHCP
- DNS
- DDNS
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP
- BFD

- 세션 설정 및 시간 초과
- 터널 콘텐츠 검사
- 네트워크 패킷 브로커

인터페이스 구성

Palo Alto Networks® 차세대 방화벽은 인터페이스 수준에서 전개가 발생하기 때문에 한 번에 여러 전개에서 작동할 수 있습니다. 예를 들어 레이어 3 인터페이스에 대한 일부 인터페이스를 구성하여 방화벽을 동적 라우팅 환경에 통합하고 다른 인터페이스를 레이어 2 스위칭 네트워크에 통합하도록 구성할 수 있습니다. 다음 주제에서는 각 유형의 인터페이스 전개 및 구성 방법, 봉쥬르 리플렉터 구성 방법 및 인터페이스 관리 프로파일 사용 방법에 대해 설명합니다.

- 탭 인터페이스
- 가상 와이어 인터페이스
- 레이어 2 인터페이스
- 레이어 3 인터페이스
- 집계 인터페이스 그룹 구성
- 네트워크 분할을 위한 봉쥬르 리플렉터 구성
- 인터페이스 관리 프로파일을 사용하여 액세스 제한

탭 인터페이스

네트워크 탭은 컴퓨터 네트워크를 통해 흐르는 데이터에 액세스하는 방법을 제공하는 디바이스입니다. 탭 모드 배포를 사용하면 스위치 SPAN 또는 미러 포트를 통해 네트워크의 트래픽 흐름을 수동으로 모니터링할 수 있습니다.

SPAN 또는 미러 포트는 스위치에 있는 다른 포트의 트래픽 복사를 허용합니다. 방화벽의 인터페이스를 탭 모드 인터페이스로 지정하고 스위치 SPAN 포트와 연결하면 스위치 SPAN 포트가 방화벽에 미러링된 트래픽을 제공합니다. 이것은 네트워크 트래픽의 흐름에 얽매이지 않으면서 네트워크 내에서 애플리케이션 가시성을 제공합니다.

탭 모드에서 방화벽을 배포하면 네트워크 설계를 변경하지 않고도 네트워크에서 실행 중인 애플리케이션에 대한 가시성을 얻을 수 있습니다. 또한 탭 모드에서 방화벽은 네트워크의 위협도 식별할 수 있습니다. 그러나 탭 모드에서는 트래픽이 방화벽을 통해 실행되고 있지 않기 때문에 위협으로 트래픽을 차단하거나 QoS 트래픽 제어를 적용하는 등 트래픽에 대한 조치를 취할 수 없습니다.

탭 인터페이스를 구성하고 네트워크의 애플리케이션 및 위협 모니터링을 시작하려면:

STEP 1 | 탭 인터페이스로 사용할 포트를 결정하고 SPAN/RSPAN 또는 포트 미러링으로 구성된 스위치에 연결합니다.

방화벽을 통해 SPAN 대상 포트에서 네트워크 트래픽을 보내 네트워크의 애플리케이션과 위협에 대한 가시성을 확보할 수 있습니다.

STEP 2 | 방화벽 웹 인터페이스에서 네트워크 탭으로 사용할 인터페이스를 구성합니다.

1. 네트워크 > 인터페이스를 선택하고 방금 케이블로 연결한 포트에 해당하는 인터페이스를 선택합니다.
2. 인터페이스 유형으로 탭을 선택합니다.
3. 구성 탭에서 보안 영역을 확장하고 새 영역을 선택합니다.
4. 영역 대화 상자에서 새 영역의 이름(예: TapZone)을 입력한 다음 확인을 클릭합니다.

STEP 3 | (선택 사항) 사용할 전달 프로파일을 만듭니다.

- 로그 포워딩을 구성합니다.
- Syslog 모니터링을 구성합니다.

STEP 4 | 보안 프로파일을 생성하여 네트워크 트래픽에서 위협을 검사합니다.

1. 개체 > 보안 프로파일을 선택합니다.
2. 각 보안 프로파일 유형에 대해 새 프로파일을 추가하고 작업을 경고로 설정합니다.

   방화벽이 트래픽과 인라인되지 않기 때문에 차단 또는 재설정 작업을 사용할 수 없습니다. 작업을 경고로 설정하면 방화벽이 로그 및 ACC에서 탐지한 모든 위협을 볼 수 있습니다.

STEP 5 | 탭 인터페이스를 통한 트래픽을 허용하는 보안 정책 규칙을 만듭니다.

탭 모드에 대한 보안 정책 규칙을 생성할 때 원본 영역과 대상 영역이 모두 같아야 합니다.

1. 정책 > 보안을 선택하고 추가를 클릭합니다.
2. 소스 탭에서 소스 영역을 방금 생성한 TapZone으로 설정합니다.
3. 대상 탭에서 대상 존도 TapZone으로 설정합니다.
4. 모든 규칙 일치 기준(애플리케이션, 사용자, 서비스, 주소)을 임의로 설정합니다.
5. 작업 탭에서 작업 설정을 허용으로 설정합니다.
6. 프로파일 유형을 프로파일로 설정하고 위협에 대해 경고하기 위해 생성한 각 보안 프로파일을 선택합니다.
7. 세션 종료 시 로그가 활성화되어 있는지 확인합니다.
8. 확인을 클릭합니다.
9. 룰베이스의 맨 위에 규칙을 배치합니다.

STEP 6 | 구성을 커밋합니다.

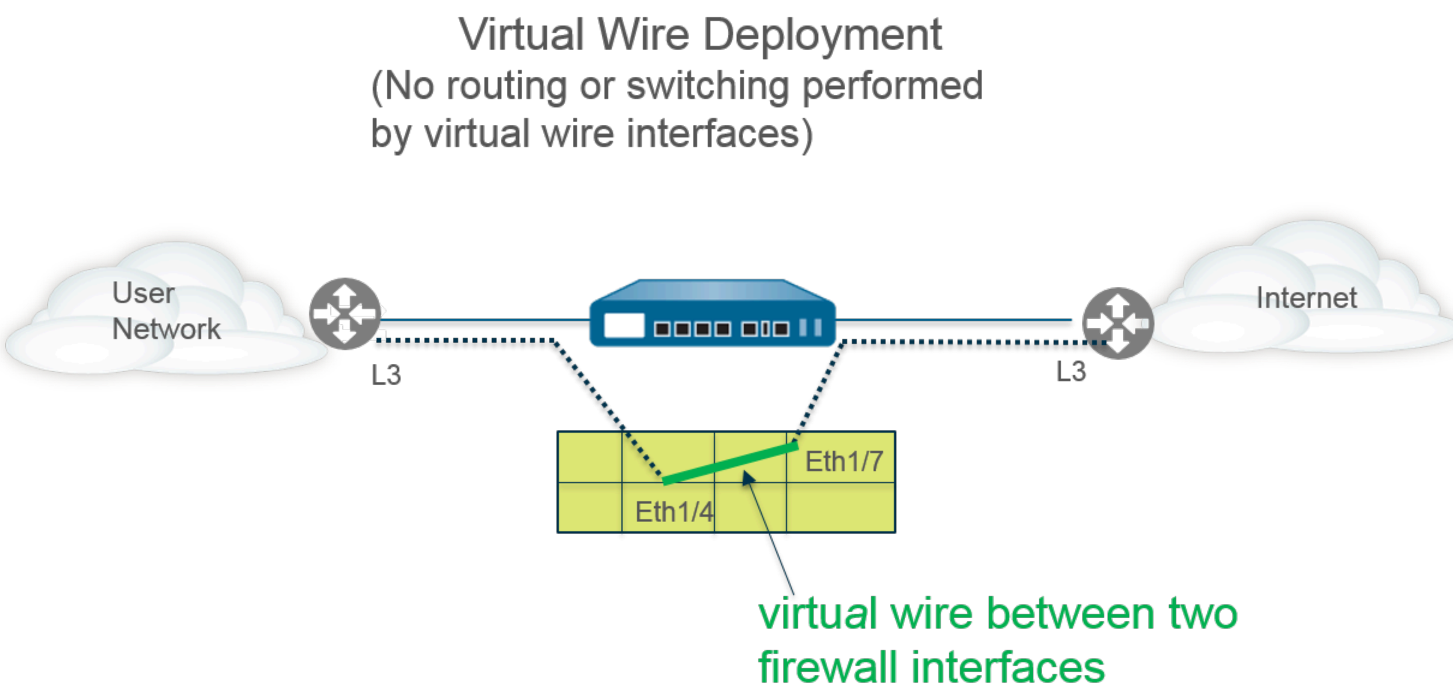
STEP 7 | 방화벽 로그(모니터 > 로그) 및 **ACC**를 모니터링하여 네트워크의 애플리케이션 및 위협에 대한 통찰력을 확보합니다.

가상 와이어 인터페이스

가상 와이어 배포에서 두 개의 방화벽 포트(인터페이스)를 함께 바인딩하여 네트워크 세그먼트에 방화벽을 트랜스페어런트하게 설치합니다. 가상 와이어는 논리적으로 두 인터페이스를 연결합니다. 따라서 가상 와이어는 방화벽 내부로 향합니다.

방화벽을 토폴로지에 원활하게 통합하려는 경우에만 가상 와이어 배포를 사용하며 방화벽의 연결된 두 인터페이스는 스위칭이나 라우팅을 수행할 필요가 없습니다. 이 두 인터페이스의 경우 방화벽은 와이어의 범프로 간주됩니다.

가상 와이어 배포는 인터페이스에 MAC 또는 IP 주소를 할당하거나 네트워크를 다시 설계하거나 주변 네트워크 디바이스를 재구성하지 않고도 방화벽을 기존 토폴로지에 삽입할 수 있으므로 방화벽 설치 및 구성을 간소화합니다. 가상 와이어는 보안 정책 규칙, 앱 ID, 콘텐츠 ID, 사용자 ID, 복호화, LLDP, 활성/수동 및 활성/활성 HA, QoS, 존 보호(일부 예외), 비 IP 프로토콜 보호, DoS 보호, 패킷 버퍼 보호, 터널 콘텐츠 검사 및 NAT를 지원하는 것 외에도 가상 LAN(VLAN) 태그를 기반으로 트래픽을 차단하거나 허용하는 것을 지원합니다.



각 가상 와이어 인터페이스는 레이어 2 또는 레이어 3 네트워킹 디바이스 또는 호스트에 직접 연결됩니다. 가상 와이어 인터페이스에는 레이어 2 또는 레이어 3 주소가 없습니다. 가상 와이어 인터페이스 중 하나가 프레임 또는 패킷을 수신하면 스위칭 또는 라우팅을 위해 레이어 2 또는 레이어 3 주소를 무시하지만 허용된 프레임 또는 패킷을 가상 와이어를 통해 두 번째 인터페이스에 전달하기 전에 보안 또는 NAT 정책 규칙을 적용하고 연결된 네트워크 디바이스에 적용합니다.

레이어 2 또는 레이어 3 주소가 필요하기 때문에 전환, VPN 터널 또는 라우팅을 지원해야 하는 인터페이스에서는 가상 와이어 배포를 사용하지 않습니다. 가상 와이어 인터페이스는 HTTP 및 핑(ping)과 같은 서비스를 제어하는 인터페이스 관리 프로파일을 사용하지 않으므로 인터페이스에 IP 주소가 필요합니다.

공장에서 출하되는 모든 방화벽에는 가상 와이어 인터페이스로 미리 구성된 두 개의 이더넷 포트(포트 1 및 2)가 있으며 이러한 인터페이스는 태그가 지정되지 않은 모든 트래픽을 허용합니다.

Cisco TrustSec 네트워크에서 보안 그룹 태그*(SGT)*를 사용하는 경우 레이어 *2* 또는 가상 와이어 모드에 인라인 방화벽을 배포하는 것이 좋습니다. 레이어 *2* 또는 가상 와이어 모드의 방화벽은 태그가 지정된 트래픽에 대한 위협 방지를 검사하고 제공할 수 있습니다.

미리 구성된 가상 와이어를 사용하지 않으려면 방화벽에서 구성한 다른 설정을 방해하지 않도록 해당 구성을 삭제해야 합니다. 외부 서비스에 대한 네트워크 액세스 설정을 참조하십시오.

가상 와이어를 통한 레이어 2 및 레이어 3 패킷

가상 유선 인터페이스를 사용하면 영역 또는 인터페이스에 적용된 정책이 트래픽을 허용하는 한 연결된 디바이스의 레이어 2 및 레이어 3 패킷이 트랜스페이런트하게 통과할 수 있습니다. 가상 와이어 인터페이스 자체는 라우팅 또는 스위칭에 참여하지 않습니다.

예를 들어, 링크가 투명하고 홉으로 계산되지 않기 때문에 방화벽은 가상 링크를 통과하는 경로 추적 패킷의 TTL을 감소시키지 않습니다. 예를 들어 OAM(운영, 관리 및 유지 관리) 프로토콜 PDU(데이터 단위)와 같은 패킷은 방화벽에서 종료되지 않습니다. 따라서 가상 와이어를 사용하면 방화벽이 통과 링크 역할을 하는 트랜스페어런트한 상태를 유지하면서 보안, NAT 및 QoS 서비스를 계속 제공할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 및 기타 레이어 2 제어 패킷(일반적으로 태그가 지정되지 않음)이 가상 와이어를 통과하려면 태그가 지정되지 않은 트래픽을 허용하는 가상 와이어 개체에 인터페이스를 연결해야 하며 이 방법이 디폴트입니다. 가상 와이어 개체 태그 허용 필드가 비어 있는 경우 가상 와이어는 태그가 지정되지 않은 트래픽을 허용합니다. (보안 정책 규칙은 레이어 2 패킷에 적용되지 않습니다.)

라우팅(레이어 3) 제어 패킷이 가상 회선을 통과하려면 트래픽 통과를 허용하는 보안 정책 규칙을 적용해야 합니다. 예를 들어 BGP 또는 OSPF처럼 애플리케이션을 허용하는 보안 정책 규칙을 적용합니다.

방화벽의 가상 와이어 인터페이스에 도착하는 IPv6 트래픽에 대한 영역에 보안 정책 규칙을 적용할 수 있도록 하려면 IPv6 방화벽을 활성화하십시오. 그렇지 않으면 IPv6 트래픽이 유선을 통해 트랜스페어런트하게 포워드됩니다.

가상 와이어 개체에 대해 멀티캐스트 방화벽을 활성화하고 이를 가상 와이어 인터페이스에 적용하면 방화벽이 멀티캐스트 트래픽을 검사하고 보안 정책 규칙에 따라 전달 여부를 결정합니다. 멀티캐스트 방화벽을 활성화하지 않으면 방화벽은 단순히 멀티캐스트 트래픽을 트랜스페어런트하게 전달합니다.

가상 와이어의 조각화는 다른 인터페이스 배포 모드와 동일하게 발생합니다.

가상 와이어 인터페이스의 포트 속도

서로 다른 방화벽 모델은 서로 다른 속도로 작동하는 다양한 수의 구리 및 광섬유 포트를 제공합니다. 가상 와이어는 동일한 유형의 이더넷 포트 2개(동선 또는 광섬유 모두)를 바인딩하거나 구리 포트를 광섬유 포트로 바인딩할 수 있습니다. 기본적으로 방화벽에 있는 구리 포트의 링크 속도는 자동으로 설정됩니다. 이는 방화벽이 속도와 전송 모드(링크 듀플렉스)를 자동으로 협상함을 의미합니다. 가상 와이어를 구성할 때 특정 링크 속도 및 링크 듀플렉스도 선택할 수 있지만 이러한 설정의 값은 단일 가상 와이어의 두 포트에 대해 동일해야 합니다.

가상 와이어를 통한 LLDP

가상 유선 인터페이스는 LLDP를 사용하여 인접 디바이스 및 해당 기능을 검색할 수 있으며 LLDP를 사용하면 인접 디바이스가 네트워크에서 방화벽의 존재를 감지할 수 있습니다. LLDP를 사용하면 방화벽이 일반적으로 가상 와이어를 통과하는 핑 또는 추적 루트에 의해 감지되지 않는 가상 와이어에서 특히 문제를 더 쉽게 해결할 수 있습니다. LLDP는 다른 디바이스가 네트워크의 방화벽을 감지할 수 있는 방법을 제공합니다. LLDP가 없으면 네트워크 관리 시스템이 가상 링크를 통해 방화벽의 존재를 감지하는 것이 사실상 불가능합니다.

가상 와이어용 통합 인터페이스

가상 와이어 인터페이스의 집계 인터페이스 그룹을 구성할 수 있지만 가상 와이어는 LACP를 사용하지 않습니다. 방화벽을 다른 네트워크에 연결하는 디바이스에서 LACP를 구성하는 경우 가상 와이어는 LACP 기능을 수행하지 않고 LACP 패킷을 투명하게 포워딩합니다.

집계 인터페이스 그룹이 제대로 작동하려면 가상 와이어의 동일한 측면에 있는 동일한 ***LACP*** 그룹에 속한 모든 링크가 동일한 영역에 할당되었는지 확인합니다**.**

고가용성 가상 와이어 지원

가상 회선 경로 그룹을 사용하여 고가용성을 위한 경로 모니터링을 수행하도록 방화벽을 구성하면, 방화벽은 두 가상 회선 인터페이스 모두에서 ARP 패킷을 전송하여 구성된 대상 IP 주소에 대한 ARP 확인을 시도합니다. 모니터링 중인 대상 IP 주소는 가상 와이어를 둘러싼 장치 중 하나와 동일한 서브네트워크에 있어야 합니다.

가상 와이어 인터페이스는 능동/수동 및 능동/능동 HA를 모두 지원합니다. 가상 와이어가 있는 활성/활성 HA 배포의 경우 스캔된 패킷은 전달 경로를 유지하기 위해 수신 방화벽으로 반환되어야 합니다. 따라서 방화벽이 피어 HA 방화벽이 소유한 세션에 속한 패킷을 수신하면 HA3 링크를 통해 피어로 패킷을 보냅니다.

HA 장애 조치가 발생하기 전에 방화벽 양쪽에 있는 피어 장치가 가상 와이어를 통해 LLDP 및 LACP를 사전 협상할 수 있도록 HA 쌍에서 수동 방화벽을 구성할 수 있습니다. 능동/수동 HA를 위한 LACP 및 LLDP 사전 협상에 대한 이러한 구성은 HA 장애 조치 속도를 높입니다.

가상 와이어 인터페이스에 대한 영역 보호

가상 와이어 인터페이스에 영역 보호를 적용할 수 있지만, 가상 와이어 인터페이스는 라우팅을 수행하지 않으므로, 스푸핑된 IP 주소와 함께 오는 패킷에 패킷 기반 공격 보호를 적용할 수 없으며, ICMP TTL 만료 오류 패킷 또는 ICMP 조각 필요 패킷을 억제할 수도 없습니다.

기본 설정으로, 가상 유선 인터페이스는 수신하는 모든 비 IP 트래픽을 전달합니다. 그러나 프로토콜 보호와 함께 영역 보호 프로필을 적용하여 가상 회선의 보안 영역 간에 특정 비 IP 프로토콜 패킷을 차단하거나 허용할 수 있습니다.

VLAN 태그가 지정된 트래픽

가상 와이어 인터페이스는 기본적으로 태그가 지정되지 않은 모든 트래픽을 허용합니다. 그러나 가상 와이어를 사용하여 두 인터페이스를 연결하고 가상 LAN(VLAN) 태그를 기반으로 트래픽을 차단하거나 허용하도록 인터페이스를 구성할 수 있습니다. VLAN 태그 0은 태그가 지정되지 않은 트래픽을 나타냅니다.

또한 여러 하위 인터페이스를 생성하고 다른 영역에 추가한 다음 VLAN 태그 또는 VLAN 태그와 IP 분류자(주소, 범위 또는 서브넷)의 조합에 따라 트래픽을 분류하여 특정 VLAN 태그에 대한 세분화된 정책 제어를 적용하거나 특정 소스 IP 주소, 범위 또는 서브넷에서 VLAN 태그 용도로 적용할 수 있습니다.

가상 와이어 하위 인터페이스

가상 와이어 배포는 가상 와이어 하위 인터페이스를 사용하여 트래픽을 영역으로 분리할 수 있습니다. 가상 와이어 하위 인터페이스는 여러 고객 네트워크의 트래픽을 관리해야 할 때 고유한 정책을 적용할 수 있는 유연성을 제공합니다. 하위 인터페이스를 사용하면 다음 기준을 사용하여 트래픽을 다른 영역으로 분리하고 분류하도록 허용할 수 있습니다(필요한 경우 영역은 별도의 가상 시스템에 속할 수 있음).

- **VLAN** 태그, 즉 하위 인터페이스가 있는 가상 와이어 배포(VLAN 태그만 해당)의 예는 VLAN 태그가 있는 가상 와이어 하위 인터페이스를 사용하여 서로 다른 두 고객의 트래픽을 분리하는 ISP를 보여줍니다.
- **IP** 분류자**(**주소**,** 범위 또는 서브넷**)**와 함께 사용하는 **VLAN** 태그는 다음 예에서 두 개의 서로 다른 고객의 트래픽을 관리하는 방화벽에 두 개의 개별 가상 시스템이 있는 ISP를 보여줍니다. 각 가상 시스템에서 이 예는 VLAN 태그 및 IP 분류자가 있는 가상 와이어 하위 인터페이스를 사용하여 트래픽을 별도의 영역으로 분류하고 각 네트워크의 고객에게 관련 정책을 적용하는 방법을 보여줍니다.

가상 와이어 하위 인터페이스 워크플로우
• 두 개의 이더넷 인터페이스를 가상 와이어 유형으로 구성하고 이러한 인터페이스를 가상 와이어에 할당합니다.
• CustomerA 및 CustomerB 트래픽을 분리하기 위해 상위 가상 와이어에 하위 인터페이스를 생성합니다. 가상 와이어로 구성된 각 하위 인터페이스 쌍에 정의된 VLAN 태그가 동일한지 확인하십시오. 이것은 가상 와이어가 VLAN 태그를 전환하지 않기 때문에 필수적입니다.
• 새 하위 인터페이스를 만들고 IP 분류자를 정의합니다. 이 작업은 선택 사항이며 VLAN 태그와 특정 소스 IP 주소, 범위 또는 서브넷의 조합을 기반으로 고객의 트래픽을 추가로 관리하기 위해 IP 분류자가 있는 추가 하위 인터페이스를 추가하려는 경우에만 필요합니다.

가상 와이어 하위 인터페이스 워크플로우
태그가 지정되지 않은 트래픽을 관리하기 위해 IP 분류자를 사용할 수도 있습니다. 이렇게 하려면 vlan 태그 "0"이 있는 하위 인터페이스를 만들고, IP 분류자를 사용하여 태그가 지정되지 않은 트래픽을 관리하기 위해 IP 분류자로 하위 인터페이스를 정의해야 합니다.

***IP* 분류는 가상 와이어의 한 면과 연결된 하위 인터페이스에서만 사용할 수 있습니다. 가상 와이어의 해당 쪽에 정의된 하위 인터페이스는 동일한 *VLAN* 태그를 사용해야 하지만 *IP* 분류자를 포함해서는 안 됩니다.**

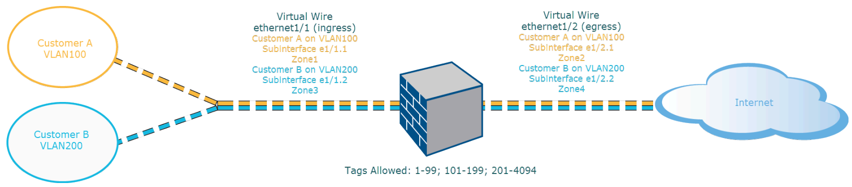


그림 **1:** 하위 인터페이스가 있는 가상 와이어 배포**(VLAN** 태그만 해당**)**

하위 인터페이스가 있는 가상 와이어 배포(VLAN 태그만 해당)는 가상 와이어로 구성된 하나의 물리적 인터페이스인 ethernet1/1을 통해 방화벽에 연결된 CustomerA와 CustomerB를 나타냅니다. 인그레스 인터페이스입니다. 두 번째 물리적 인터페이스인 ethernet1/2도 Virtual Wire의 일부입니다. 인터넷에 대한 액세스를 제공하는 것은 이그레스 인터페이스입니다.

CustomerA의 경우 ethernet1/1.1(ingress) 및 ethernet1/2.1(egress) 하위 인터페이스도 있습니다. CustomerB의 경우 ethernet1/1.2(ingress) 및 ethernet1/2.2(egress) 하위 인터페이스가 있습니다. 하위 인터페이스를 구성할 때 각 고객에 대한 정책을 적용하려면 적절한 VLAN 태그 및 영역을 할당해야 합니다. 이 예에서 CustomerA에 대한 정책은 Zone1과 Zone2 사이에 생성되고 CustomerB에 대한 정책은 Zone3과 Zone4 사이에 생성됩니다.

트래픽이 CustomerA 또는 CustomerB에서 방화벽으로 들어오면 수신 패킷의 VLAN 태그가 먼저 인그레스 하위 인터페이스에 정의된 VLAN 태그와 일치됩니다. 이 예에서 단일 하위 인터페이스는 수신 패킷의 VLAN 태그와 일치하므로 해당 하위 인터페이스가 선택됩니다. 영역에 대해 정의된 정책은 패킷이 해당 하위 인터페이스에서 종료되기 전에 평가되고 적용됩니다.

상위 가상 와이어 인터페이스 및 하위 인터페이스에 동일한 *VLAN* 태그를 정의하면 안 됩니다. 상위 가상 와이어 인터페이스*(Network > Virtual Wires)*의 태그 허용 목록에 정의된 *VLAN* 태그가 하위 인터페이스에 포함되어 있지 않은지 확인합니다.

하위 인터페이스(VLAN 태그 및 IP 분류자)가 있는 가상 와이어 배포는 기본 가상 시스템(vsys1) 외에 두 개의 가상 시스템(vsys)이 있는 하나의 물리적 방화벽에 연결된 CustomerA와 CustomerB를 나타냅니다. 각 가상 시스템은 각 고객에 대해 별도로 관리되는 독립적인 가상 방화벽입니다. 각 vsys에는 독립적으로 관리되는 연결된 인터페이스/하위 인터페이스 및 보안 영역이 있습니다.

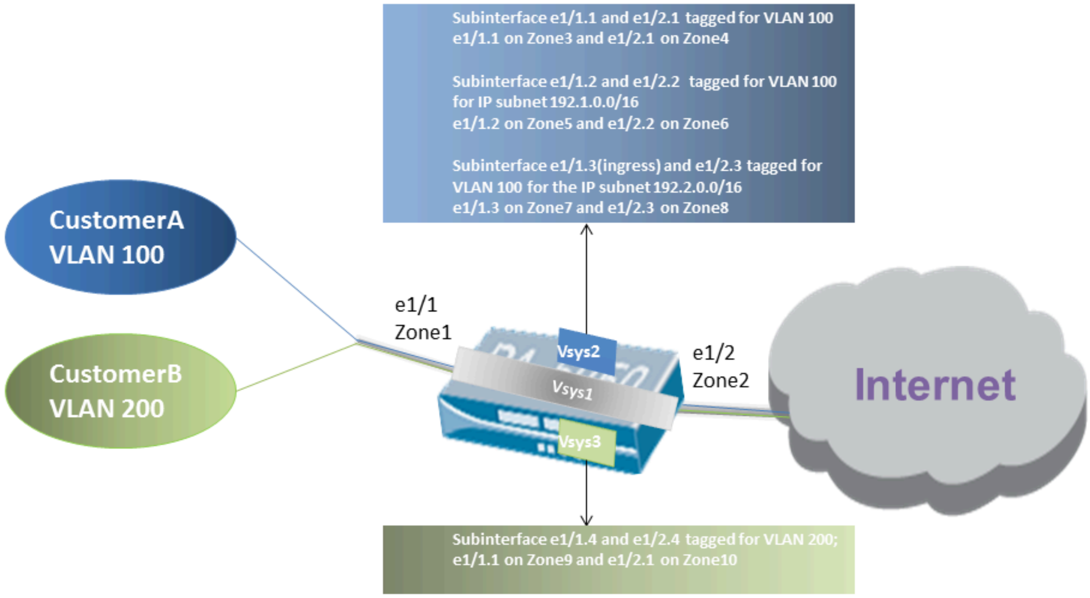


그림 **2:** 하위 인터페이스**(VLAN** 태그 및 **IP** 분류자**)**를 사용한 가상 와이어 배포

Vsys1은 물리적 인터페이스 ethernet1/1 및 ethernet1/2를 가상 와이어로 사용하도록 설정됩니다. ethernet1/1은 수신 인터페이스이고 ethernet1/2는 인터넷에 대한 액세스를 제공하는 송신 인터페이스입니다. 이 가상 와이어는 하위 인터페이스에 할당된 VLAN 태그 100 및 200을 제외하고 모든 태그가 지정된 트래픽과 태그가 지정되지 않은 트래픽을 허용하도록 구성됩니다.

CustomerA는 vsys2에서 관리되고 CustomerB는 vsys3에서 관리됩니다. vsys2 및 vsys3에서는 정책 조치를 시행하기 위해 적절한 VLAN 태그 및 영역을 사용하여 다음 vwire 하위 인터페이스가 생성됩니다.

고객	**Vsys**	**Vwire** 하위 인터페이스	존	**VLAN** 태그	**IP** 분류기
A	2	e1/1.1(인그레스) e1/2.1(이그레스)	존 3 존 4	100 100	없음
	2	e1/1.2(인그레스) e1/2.2(이그레스)	존 5 존 6	100 100	IP 서브넷 192.1.0.0/16
	2	e1/1.3(인그레스) e1/2.3(이그레스)	존 7 존 8	100 100	IP 서브넷 192.2.0.0/16

고객	Vsys	Vwire 하위 인터페이스	존	VLAN 태그	IP 분류기
B	3	e1/1.4(인그레스) e1/2.4(이그레스)	존 9 존 10	200 200	없음

트래픽이 CustomerA 또는 CustomerB에서 방화벽으로 들어오면 수신 패킷의 VLAN 태그가 먼저 인그레스 하위 인터페이스에 정의된 VLAN 태그와 일치됩니다. 이 경우 CustomerA의 경우 동일한 VLAN 태그를 사용하는 여러 하위 인터페이스가 있습니다. 따라서 방화벽은 먼저 패킷의 소스 IP 주소를 기반으로 하위 인터페이스로 분류를 좁힙니다. 영역에 대해 정의된 정책은 패킷이 해당 하위 인터페이스에서 종료되기 전에 평가되고 적용됩니다.

반환 경로 트래픽의 경우 방화벽은 고객 대면 하위 인터페이스의 IP 분류자에 의해 정의된 데스티네이션 IP 주소를 비교하고 정확한 하위 인터페이스를 통해 트래픽을 라우팅하기 위해 적절한 가상 와이어를 선택합니다.

상위 가상 와이어 인터페이스 및 하위 인터페이스에 동일한 *VLAN* 태그를 정의하면 안 됩니다. 상위 가상 와이어 인터페이스(***Network > Virtual Wires***)의 태그 허용 목록에 정의된 *VLAN* 태그가 하위 인터페이스에 포함되어 있지 않은지 확인합니다.

가상 와이어 구성

다음 작업은 가상 와이어를 생성하기 위해 2개 가상 와이어 인터페이스(이 예에서는 이더넷 1/3 및 이더넷 1/4)를 구성하는 방법을 보여줍니다. 두 인터페이스는 링크 속도와 전송 모드(**Link Duplex**)가 같아야 합니다. 예를 들어 전이중 1000Mbps 구리 포트는 전이중 1Gbps 광섬유 포트와 일치합니다.

STEP 1 | 첫 번째 가상 와이어 인터페이스를 생성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 케이블로 연결된 인터페이스를 선택합니다(이 예에서는 이더넷**1/3**).
2. 인터페이스 유형을 가상 와이어로 설정합니다.

STEP 2 | 가상 와이어 개체에 인터페이스를 연결합니다.

1. 동일한 이더넷 인터페이스에 있는 동안 구성 탭에서 가상 와이어를 선택하고 새 가상 와이어를 클릭합니다.
2. 가상 와이어의 이름을 입력합니다.
3. 인터페이스**1**에서 방금 구성한 인터페이스(이더넷**1/3**)를 선택합니다. (가상 와이어 인터페이스로 구성된 인터페이스만 목록에 나타납니다.)
4. 태그 허용에 **0**을 입력 하여 태그가 지정되지 않은 트래픽(예: BPDU 및 기타 레이어 2 제어 트래픽)이 허용됨을 나타냅니다. 태그가 없으면 태그 0을 의미합니다. 추가로 허용되는 태그 정수 또는 태그 범위를 쉼표로 구분하여 입력합니다(기본값은 0, 범위는 0~4,094).
5. 가상 와이어를 통과하는 멀티캐스트 트래픽에 보안 정책 규칙을 적용할 수 있게 하려면 멀티캐스트 방화벽을 선택합니다. 그렇지 않으면 멀티캐스트 트래픽이 가상 와이어를 통해 투명하게 전달됩니다.
6. 방화벽이 투명하게 작동할 수 있도록 링크 상태 통과를 선택합니다. 방화벽이 가상 와이어의 링크에 대한 링크 다운 상태를 감지하면 가상 와이어 쌍의 다른 인터페이스를 다운시킵니다. 따라

서 방화벽 양쪽에 있는 디바이스는 마치 그들 사이에 방화벽이 없는 것처럼 일관된 링크 상태를 봅니다. 이 옵션을 선택하지 않으면 링크 상태가 가상 와이어를 통해 전파되지 않습니다.

7. 확인을 클릭하여 가상 와이어 개체를 저장합니다.

STEP 3 | 가상 와이어 인터페이스의 링크 속도를 결정합니다.

1. 동일한 이더넷 인터페이스를 계속 사용하는 동안 고급을 선택하고 링크 속도를 기록하거나 변경합니다. 포트 유형은 목록에서 사용 가능한 속도 설정을 결정합니다. 기본적으로 구리 포트는 링크 속도를 자동으로 협상하도록 설정됩니다. 두 가상 와이어 인터페이스 모두 링크 속도가 동일해야 합니다.
2. 확인을 클릭하여 이더넷 인터페이스를 저장합니다.

STEP 4 | 앞의 단계를 반복하여 두 번째 가상 와이어 인터페이스(이 예에서는 이더넷**1/4**)를 구성합니다.

생성한 가상 와이어 개체를 선택하면 방화벽이 자동으로 두 번째 가상 와이어 인터페이스를 **Interface2**로 추가합니다.

STEP 5 | 각 가상 와이어 인터페이스에 대해 별도의 보안 영역을 만듭니다.

1. 네트워크 > 영역을 선택하고 영역을 추가합니다.
2. 영역의 이름을 입력합니다(예: **인터넷**).
3. 위치에서 영역이 적용되는 가상 시스템을 선택합니다.
4. 유형에 대해 가상 와이어를 선택합니다.
5. 영역에 속한 인터페이스를 추가합니다.
6. 확인을 클릭합니다.

STEP 6 | (선택 사항) 레이어 3 트래픽이 통과할 수 있도록 하는 보안 정책 규칙을 만듭니다.

가상 회선을 통해 레이어 3 트래픽을 허용하려면 사용자 영역에서 인터넷 영역으로의 트래픽을 허용하는 보안 정책 규칙을 생성하고 인터넷 영역에서 사용자 영역으로의 트래픽을 허용하는 또 다른 규칙을 생성하여 BGP 또는 OSPF와 같은 허용할 애플리케이션을 선택합니다.

STEP 7 | (선택 사항) IPv6 방화벽을 사용하도록 설정합니다.

가상 와이어 인터페이스에 도착하는 IPv6 트래픽에 보안 정책 규칙을 적용하려면 IPv6 방화벽을 활성화하십시오. 그렇지 않으면 IPv6 트래픽이 투명하게 전달됩니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. **IPv6** 방화벽 사용을 선택합니다.
3. 확인을 클릭합니다.

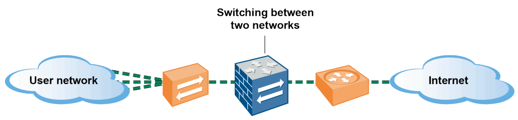
STEP 8 | 변경 사항을 커밋합니다.

STEP 9 | (선택 사항) LLDP 프로파일을 구성하고 가상 와이어 인터페이스에 적용합니다(LLDP 구성 참조).

STEP 10 | (선택 사항) 가상 와이어 영역에 비 IP 프로토콜 제어를 적용합니다(프로토콜 보호 구성). 그렇지 않으면 모든 비 IP 트래픽이 가상 와이어를 통해 전달됩니다.

레이어 2 인터페이스

레이어 2 배포에서 방화벽은 둘 이상의 네트워크 간의 전환을 제공합니다. 디바이스는 레이어 2 세그먼트에 연결됩니다. 방화벽은 프레임에서 식별된 MAC 주소와 연결된 적절한 포트로 프레임을 전달합니다. 전환이 필요한 경우 레이어 2 인터페이스를 구성합니다.



Cisco TrustSec 네트워크에서 ***SGT(**보안 그룹 태그**)**를 사용하는 경우 인라인 방화벽을 레이어 ***2*** 또는 가상 와이어 모드로 배포하는 것이 가장 좋습니다**.** 레이어 ***2*** 또는 가상 와이어 모드의 방화벽은 태그가 지정된 트래픽을 검사하고 위협 방지를 제공할 수 있습니다**.**

다음 항목에서는 트래픽에 VLAN(가상 LAN) 사용 및 그룹 간의 정책 분리에 대한 세부 정보를 포함하여 필요한 각 배포 유형에 대해 구성할 수 있는 다양한 유형의 레이어 2 인터페이스에 대해 설명합니다. 또 다른 주제에서는 방화벽이 Cisco PVST+(VLAN 별 스패닝 트리) 또는 Rapid PVST+ BPDU(Bridge Protocol Data Unit)에서 인바운드 포트 VLAN ID 번호를 다시 쓰는 방법에 대해 설명합니다.

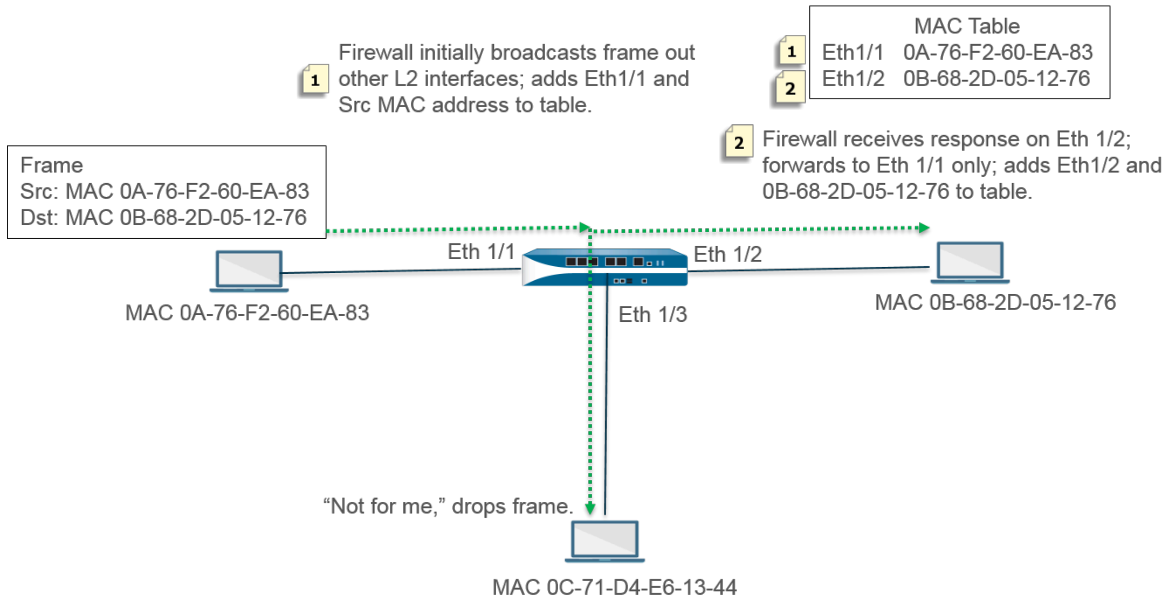
- VLAN이 없는 레이어 2 인터페이스
- VLAN이 있는 레이어 2 인터페이스
- 레이어 2 인터페이스 구성
- 레이어 2 인터페이스, 하위 인터페이스 및 VLAN 구성
- VLAN별 스패닝 트리(PVST+) BPDU 재작성 관리

VLAN이 없는 레이어 2 인터페이스

방화벽에서 레이어 2 인터페이스를 구성하여 계층 2 네트워크(네트워크 경계가 아님)에서 스위치 역할을 할 수 있습니다. 레이어 2 호스트는 지리적으로 서로 가깝고 단일 브로드캐스트 도메인에 속할 수 있습니다. 방화벽은 보안 영역에 인터페이스를 할당하고 영역에 보안 규칙을 적용할 때 레이어 2 호스트 간에 보안을 제공합니다.

호스트는 프레임을 교환하여 OSI 모델의 레이어 2에서 방화벽과 통신 및 서로 통신합니다. 프레임에는 물리적 하드웨어 주소인 소스 및 대상 MAC(Media Access Control) 주소가 포함된 이더넷 헤더가 포함되어 있습니다. MAC 주소는 콜론이나 하이픈으로 구분된 6개의 옥텟으로 형식화된 48비트 16진수입니다(예: 00-85-7E-46-F1-B2).

다음 그림에는 각각 일대일 매핑으로 레이어 2 호스트에 연결되는 3개의 레이어 2 인터페이스가 있는 방화벽이 있습니다.



방화벽은 빈 MAC 테이블로 시작합니다. 소스 주소가 0A-76-F2-60-EA-83인 호스트가 방화벽에 프레임을 보낼 때 방화벽의 MAC 테이블에는 대상 주소 0B-68-2D-05-12-76이 없으므로 프레임을 전달할 인터페이스를 모릅니다. 모든 레이어 2 인터페이스에 프레임을 브로드캐스트합니다. 방화벽은 소스 주소 0A-76-F2-60-EA-83 및 연결된 Eth1/1을 MAC 테이블에 넣습니다.

0C-71-D4-E6-13-44에 있는 호스트는 브로드캐스트를 수신하지만 대상 MAC 주소는 자체 MAC 주소가 아니므로 프레임을 삭제합니다.

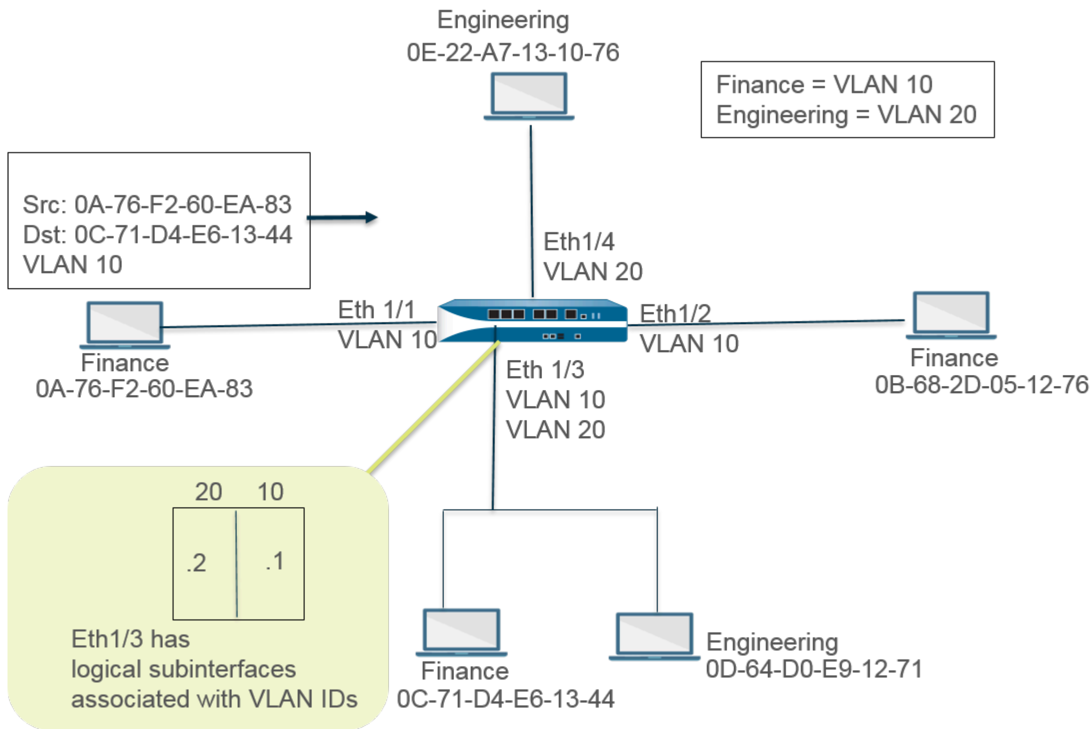
수신 인터페이스 이더넷 1/2는 프레임을 호스트로 전달합니다. 호스트 0B-68-2D-05-12-76이 응답하면 대상 주소 0A-76-F2-60-EA-83을 사용하고 방화벽은 0B-68-2D-05-12-76에 도달하기 위한 인터페이스로 이더넷 1/2를 MAC 테이블에 추가합니다.

VLAN이 있는 레이어 2 인터페이스

조직에서 LAN을 별도의 VLAN(가상 LAN)으로 분할하여 다른 부서의 트래픽과 정책을 별도로 유지하려는 경우 논리적으로 레이어 2 호스트를 VLAN으로 그룹화하여 레이어 2 네트워크 세그먼트를 브로드캐스트 도메인으로 나눌 수 있습니다. 예를 들어 재무 및 엔지니어링 부서에 대한 VLAN을 생성할 수 있습니다. 이렇게 하려면 레이어 2 인터페이스, 하위 인터페이스 및 VLAN을 구성합니다.

방화벽은 VLAN ID가 포함된 이더넷 헤더가 있는 프레임을 전달하는 스위치 역할을 하며 데스티네이션 인터페이스에는 해당 프레임을 수신하고 호스트로 전달하기 위해 해당 VLAN ID가 있는 하위 인터페이스가 있어야 합니다. 방화벽에서 레이어 2 인터페이스를 구성하고 인터페이스에 대해 각각 VLAN 태그(ID)가 있는 하나 이상의 논리적 하위 인터페이스를 구성합니다.

다음 그림에서 방화벽에는 조직 내 서로 다른 부서에 속한 레이어 2 호스트에 연결하는 4개의 레이어 2 인터페이스가 있습니다. 이더넷 인터페이스 1/3은 하위 인터페이스 .1(VLAN 10로 태그 지정됨) 및 하위 인터페이스 .2(VLAN 20으로 태그 지정됨)로 구성되므로 해당 세그먼트에 두 개의 브로드캐스트 도메인이 있습니다. VLAN 10의 호스트는 재무에 속합니다. VLAN 20의 호스트는 Engineering에 속합니다.



이 예에서 MAC 주소 0A-76-F2-60-EA-83의 호스트는 VLAN ID가 10인 프레임을 방화벽으로 보내고 방화벽은 이 프레임을 다른 L2 인터페이스로 브로드캐스트합니다. 이더넷 인터페이스 1/3은 대상이 0C-71-D4-E6-13-44인 호스트에 연결되어 있고 해당 하위 인터페이스 .1에 VLAN 10이 할당되어 있으므로 프레임을 수락합니다. 이더넷 인터페이스 1/3은 프레임을 재무 호스트로 전달합니다.

레이어 2 인터페이스 구성

레이어 2 전환을 원하고 VLAN 간에 트래픽을 분리할 필요가 없는 경우 VLAN이 없는 레이어 2 인터페이스를 구성합니다.

STEP 1 | 레이어 2 인터페이스 구성하기.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 인터페이스를 선택합니다. 인터페이스 이름은 이더넷1/1과 같이 고정되어 있습니다.
2. 인터페이스 유형으로 레이어**2**를 선택합니다.
3. 구성 탭을 선택하고 인터페이스를 보안 영역에 할당하거나 또는 새 영역을 생성합니다.
4. 다른 레이어 2 호스트에 연결하는 방화벽에 추가 레이어 2 인터페이스를 구성합니다.

STEP 2 | 커밋합니다.

확인 및 커밋을 클릭합니다.

레이어 2 인터페이스, 하위 인터페이스 및 VLAN 구성

VLAN 간의 레이어 2 스위칭 및 트래픽 분리를 원할 때 VLAN으로 레이어 2 인터페이스를 구성합니다. 레이어 2 인터페이스의 보안 영역 간 또는 레이어 2 VLAN의 단일 영역 내 인터페이스 간 비IP 프로토콜을 선택적으로 제어할 수 있습니다.

STEP 1 | 레이어 2 인터페이스 및 하위 인터페이스를 구성하고 VLAN ID를 할당합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 인터페이스를 선택합니다. 인터페이스 이름은 이더넷1/1과 같이 고정되어 있습니다.
2. 인터페이스 유형으로 레이어**2**를 선택합니다.
3. 구성 탭을 선택합니다.
4. **VLAN**의 경우 설정 없음을 유지합니다.
5. 보안 영역에 인터페이스를 할당하거나 또는 새 영역을 생성합니다.
6. 확인을 클릭합니다.
7. 이더넷 인터페이스가 강조 표시된 상태에서 하위 인터페이스 추가를 클릭합니다.
8. 인터페이스 이름은 고정된 상태로 유지됩니다. 마침표 뒤에 1에서 9,999 사이의 하위 인터페이스 번호를 입력합니다.
9. 1에서 4,094 사이의 VLAN 태그 ID를 입력합니다.
10. 보안 영역에 하위 인터페이스를 할당합니다.
11. 확인을 클릭합니다.

STEP 2 | 커밋합니다.

커밋을 클릭합니다.

STEP 3 | (선택 사항) 프로토콜 보호가 포함된 영역 보호 프로파일을 적용하여 레이어 2 영역 간(또는 레이어 2 영역 내의 인터페이스 간) 비IP 프로토콜 패킷을 제어합니다.

프로토콜 보호를 구성합니다.

VLAN별 스패닝 트리(PVST+) BPDU 재작성 관리

방화벽의 인터페이스가 레이어 2 배포용으로 구성된 경우 방화벽은 Cisco PVST+(per-VLAN spanning tree) 또는 Rapid PVST+ 브리지 프로토콜 데이터 단위(BPDU)의 인바운드 PVID(Port VLAN ID) 번호를 적절한 아웃바운드 VLAN ID 번호로 다시 쓰고 BPDU를 외부로 포워딩합니다. PAN-OS 7.1에서 시작되는 이 기본 동작을 통해 방화벽은 방화벽 양쪽에 있는 VLAN의 Cisco 스위치 간에 Cisco 독점 PVST+ 및 Rapid PVST+ 프레임에 올바르게 태그를 지정하여 Cisco PVST+ 및 Rapid PVST+를 사용하는 스패닝 트리 루프 감지가 제대로 작동할 수 있습니다. 방화벽은 STP(Spanning Tree Protocol) 선택 프로세스에 참여하지 않으며 다른 유형의 스패닝 트리에 대한 동작 변경 사항이 없습니다.

Cisco 스위치는 ***PVST+*** 또는 ***Rapid PVST+ BPDU*** 재작성이 방화벽에서 제대로 작동하도록 루프가드를 비활성화해야 합니다*.*

이 기능은 레이어 2 이더넷 및 통합 이더넷(AE) 인터페이스에서만 지원됩니다. 방화벽은 Cisco 기본 VLAN 구현과 호환되도록 기본 VLAN ID가 1인 PVID 범위 1~4,094를 지원합니다.

PVST+ BPDU 재작성 기능을 지원하기 위해 PAN-OS는 PVST+ 기본 VLAN의 개념을 지원합니다. 기본 VLAN으로 보내고 받은 프레임은 기본 VLAN과 동일한 PVID로 태그가 지정되지 않습니다. 동일한 레이어 2 배포의 모든 스위치와 방화벽에는 PVST+가 제대로 작동하려면 동일한 기본 VLAN이 있어야 합니다. Cisco 기본 VLAN의 기본값은 vlan1이지만 VLAN ID는 1이 아닌 숫자일 수 있습니다.

예를 들어 방화벽은 스위치 또는 브로드캐스트 도메인에 속하는 인터페이스와 하위 인터페이스를 설명하는 VLAN 개체(VLAN_BRIDGE)로 구성됩니다. 이 예에서 VLAN에는 100으로 태그가 지정

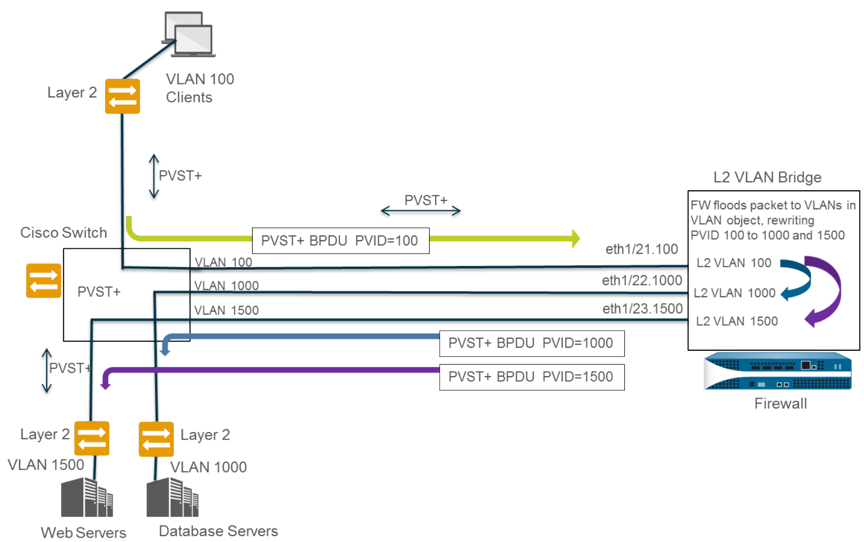
된 ethernet1/21.100, 1000으로 태그가 지정된 ethernet1/22.1000 및 1500으로 태그가 지정된 ethernet1/23.1500의 세 가지 하위 인터페이스가 포함되어 있습니다.

VLAN_BRIDGE에 속하는 하위 인터페이스는 다음과 같습니다.

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	LINK STATE	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/21	Layer2		Untagged	none	none		Disabled
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust		Disabled
ethernet1/22	Layer2		Untagged	none	none		Disabled
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust		Disabled
ethernet1/23	Layer2		Untagged	none	none		Disabled
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management		Disabled

방화벽이 PVST+ BPDU를 자동으로 다시 쓰는 순서는 다음 그림과 설명에 나와 있습니다.



1. VLAN 100에 속한 Cisco 스위치 포트는 PVID 및 802.1Q VLAN 태그가 100으로 설정된 PVST+ BPDU를 방화벽으로 보냅니다.
2. 방화벽 인터페이스 및 하위 인터페이스는 레이어 2 인터페이스 유형으로 구성됩니다. 방화벽의 인그레스 서브인터페이스는 들어오는 BPDU의 PVID 및 VLAN 태그와 일치하는 VLAN 100으로 태그가 지정되어 방화벽이 BPDU를 수락합니다. 방화벽은 동일한 VLAN 개체(이 예에서는 ethernet1/22.1000 및 ethernet1/23.1500)에 속하는 다른 모든 인터페이스로 PVST+ BPDU를 플러딩합니다. VLAN 태그가 일치하지 않으면 방화벽은 대신 BPDU를 삭제합니다.
3. 방화벽이 다른 인터페이스(동일한 VLAN 개체에 속함)를 통해 BPDU를 플러딩하면 방화벽은 PVID 및 802.1Q VLAN 태그를 다시 작성하여 이그레스(egress) 인터페이스의 VLAN 태그와 일치시킵니다. 이 예에서 방화벽은 BPDU가 방화벽의 레이어 2 브리지를 통과할 때 한 하위 인터페이스에 대해 BPDU PVID를 100에서 1000으로, 두 번째 하위 인터페이스에 대해 100에서 1500으로 다시 씁니다.
4. 각 Cisco 스위치는 들어오는 BPDU에서 올바른 PVID 및 VLAN 태그를 수신하고 PVST+ 패킷을 처리하여 네트워크에서 가능한 루프를 감지합니다.

다음 CLI 작동 명령을 사용하여 PVST+ 및 Rapid PVST+ BPDU를 관리할 수 있습니다.

- PVID의 PVST+ 및 Rapid PVST+ BPDU 재작성을 전역적으로 비활성화하거나 다시 활성화합니다(기본값은 활성화됨).

  set session rewrite-pvst-pvid <yes|no>

- 방화벽의 기본 VLAN ID를 설정합니다(범위는 1~4,094, 기본값은 1).

  스위치의 기본 *VLAN ID*가 *1*이 아닌 값이면 방화벽의 기본 *VLAN ID*를 동일한 번호로 설정해야 합니다. 그렇지 않으면 방화벽이 해당 *VLAN ID*를 가진 패킷을 삭제합니다. 이것은 트렁킹된 인터페이스와 트렁킹되지 않은 인터페이스에 적용됩니다.

  set session pvst-native-vlan-id <*vid*>

- Drop all STP BPDU packets.

  set session drop-stp-packet <yes|no>

  모든 STP BPDU 패킷을 삭제하려는 이유의 예:

  - 방화벽 양쪽에 하나의 스위치만 있고 루프를 유발할 수 있는 스위치 간에 다른 연결이 없는 경우 STP가 필요하지 않으며 스위치에서 비활성화하거나 방화벽에 의해 차단될 수 있습니다.
  - BPDU를 부적절하게 플러딩하는 오작동 STP 스위치가 있는 경우 방화벽에서 STP 패킷을 중지하여 BPDU 플러딩을 중지할 수 있습니다.

- PVST+BPDU 재작성이 활성화되었는지 확인하고 PVST 기본 VLAN ID를 보고 방화벽이 모든 STP BPDU 패킷을 삭제하는지 확인합니다.

  show vlan all

```
pvst+ tag rewrite: disabled
pvst native vlan id:     5
drop stp:                disabled
total vlans shown:       1
name      interface          virtual interface
bridge    ethernet1/1
          ethernet1/2
          ethernet1/1.1
          ethernet1/2.1
```

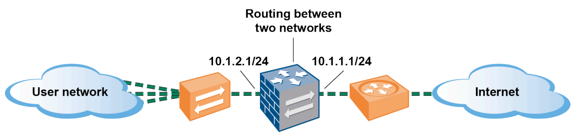
- PVST+ BPDU 오류 문제를 해결합니다.

  show counter global

  PVST+ BPDU 패킷 내부의 802.1Q 태그와 PVID 필드가 일치하지 않는 횟수를 계산하는 `flow_pvid_inconsistent` 카운터를 살펴보십시오.

레이어 3 인터페이스

레이어 3 배포에서 방화벽은 여러 포트 간에 트래픽을 라우팅합니다. 레이어 3 인터페이스를 구성하기 전에 방화벽이 각 레이어 3 인터페이스의 트래픽을 라우팅하는 데 사용할 가상 라우터를 구성해야 합니다.



Cisco TrustSec 네트워크에서 *SGT(*보안 그룹 태그*)*를 사용하는 경우 인라인 방화벽을 레이어 *2* 또는 가상 와이어 모드로 배포하는 것이 가장 좋습니다*.* 그러나 *Cisco TrustSec* 네트워크에서 레이어 *3* 방화벽을 사용해야 하는 경우 두 *SXP(SGT* 교환 프로토콜*)* 피어 간에 레이어 *3* 방화벽을 배포하고 *SXP* 피어 간에 트래픽을 허용하도록 방화벽을 구성해야 합니다*.*

다음 주제에서는 계층 3 인터페이스를 구성하는 방법과 NDP(Neighbor Discovery Protocol)를 사용하여 IPv6 호스트를 프로비저닝하고 링크 로컬 네트워크에서 디바이스의 IPv6 주소를 확인하여 디바이스를 빠르게 찾는 방법에 대해 설명합니다.

- 계층 3 인터페이스 구성
- NDP를 사용하여 IPv6 호스트 관리

레이어 3 인터페이스 구성

방화벽이 이러한 인터페이스에서 라우팅을 수행할 수 있도록 IPv4 또는 IPv6 주소로 레이어 3 인터페이스(이더넷, VLAN, 루프백 및 터널 인터페이스)를 구성하려면 다음 절차가 필요합니다. 터널이 라우팅에 사용되거나 터널 모니터링이 켜져 있는 경우 터널에 IP 주소가 필요합니다. 다음 작업을 수행하기 전에 레거시 라우팅 엔진의 하나 이상의 가상 라우터 또는 고급 라우팅 엔진의 논리적 라우터를 정의합니다.

일반적으로 다음 절차를 사용하여 인터넷에 연결하는 외부 인터페이스와 내부 네트워크용 인터페이스를 구성합니다. 단일 인터페이스에서 IPv4 및 IPv6 주소를 모두 구성할 수 있습니다.

PAN-OS 방화벽 모델은 물리적 또는 가상 레이어 *3* 인터페이스에 할당된 최대 *16,000*개의 *IP* 주소를 지원합니다*.* 이 최대값에는 *IPv4* 및 *IPv6* 주소가 모두 포함됩니다*.*

IPv6 경로를 사용하는 경우 DNS 구성을 위한 IPv6 라우터 알림을 제공하도록 방화벽을 구성할 수 있습니다. 방화벽은 클라이언트가 IPv6 DNS 요청을 해결할 수 있도록 IPv6 DNS 클라이언트에 RDNS(재귀 DNS 서버) 주소 및 DNS 검색 목록을 제공합니다. 따라서 방화벽은 DHCPv6 서버처럼 작동합니다.

STEP 1 | 인터페이스를 선택하고 보안 영역으로 구성합니다.

1. 네트워크 > 인터페이스를 선택하고 이더넷, **VLAN**, 루프백 또는 터널, 원하는 인터페이스 유형에 따라 다릅니다.
2. 구성할 인터페이스를 선택합니다.
3. 인터페이스 유형 - **Layer3**를 선택합니다.
4. 구성 탭에서 가상 라우터에 대해 구성하려는 가상 라우터(예: 기본)를 선택합니다.
5. 가상 시스템의 경우 다중 가상 시스템 방화벽에 있는 경우 구성할 가상 시스템을 선택합니다.
6. 보안 영역에서 인터페이스가 속한 영역을 선택하거나 새 영역을 만듭니다.
7. 확인을 클릭합니다.

STEP 2 | IPv4 주소로 인터페이스를 구성합니다.

다음 세 가지 방법 중 하나로 레이어 3 인터페이스에 IPv4 주소를 할당할 수 있습니다.

- 정적
- DHCP 클라이언트 - 방화벽 인터페이스는 DHCP 클라이언트 역할을 하며 동적으로 할당된 IP 주소를 받습니다. 방화벽은 DHCP 클라이언트 인터페이스에서 받은 설정을 방화벽에서 작동하는 DHCP 서버로 전파하는 기능도 제공합니다. 이는 인터넷 서비스 공급자의 DNS 서버 설정을 방화벽으로 보호되는 네트워크에서 작동하는 클라이언트 컴퓨터로 전파하는 데 가장 일반적으로 사용됩니다.
- PPPoE - DSL 모뎀이 있지만 연결을 종료할 다른 PPPoE 디바이스가 없는 DSL(디지털 가입자 회선) 환경에서 연결을 지원하도록 인터페이스를 이더넷을 통한 지점 간 프로토콜(PPPoE) 종료 지점으로 구성합니다.

1. 네트워크 > 인터페이스를 선택하고 이더넷, **VLAN**, 루프백 또는 터널, 원하는 인터페이스 유형에 따라 다릅니다.
2. 구성할 인터페이스를 선택합니다.
3. 정적 IPv4 주소를 사용하여 인터페이스를 구성하려면 **IPv4** 탭에서 유형을 정적으로 설정합니다.
4. 주소에 대한 이름 및 선택적 설명을 추가합니다.
5. 유형에 대해 다음 중 하나를 선택합니다.
   - **IP** 넷마스크 - 인터페이스에 할당할 IP 주소와 네트워크 마스크를 입력합니다(예: 208.80.56.100/24).

     레이어 *3* 인터페이스 주소에 */31* 서브넷 마스크를 사용하는 경우 *ping*과 같은 유틸리티가 제대로 작동하려면 인터페이스가 *.1/31* 주소로 구성되어야 합니다.

     IPv4 주소로 루프백 인터페이스를 구성하는 경우 */32* 서브넷 마스크가 있어야 합니다. 예: *192.168.2.1/32.*
   - **IP** 범위 - 192.168.2.1-192.168.2.4와 같은 IP 주소 범위를 입력합니다.
   - **FQDN** - 정규화된 도메인 이름을 입력합니다.
6. 주소를 적용할 태그를 선택합니다.
7. 확인을 클릭합니다.

STEP 3 | 이더넷을 통한 지점간 프로토콜(PPPoE)을 사용하여 인터페이스를 구성합니다. 레이어 3 인터페이스를 참조하십시오.

*PPPoE*는 *HA* 활성/활성 모드에서 지원되지 않습니다.

1. 네트워크 > 인터페이스를 선택하고 이더넷, **VLAN**, 루프백 또는 터널 중 하나를 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv4** 탭에서 유형을 **PPPoE**로 설정합니다.
4. 일반 탭에서 활성화를 선택하여 PPPoE 종료를 위한 인터페이스를 활성화합니다.
5. 지점 간 연결에 대한 사용자 이름을 입력합니다.
6. 사용자 이름에 암호를 입력하고 암호 확인을 입력합니다.
7. 확인을 클릭합니다.

STEP 4 | 인터페이스를 DHCP 클라이언트로 구성 따라서 동적으로 할당된 IPv4 주소를 수신합니다.

DHCP 클라이언트는 *HA* 활성/활성 모드에서 지원되지 않습니다.

STEP 5 | 정적 IPv6 주소를 사용하여 인터페이스를 구성합니다.

1. 네트워크 > 인터페이스를 선택하고 이더넷, **VLAN**, 루프백 또는 터널 중 하나를 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv6** 탭에서 인터페이스에서 IPv6 사용을 선택하여 인터페이스에서 IPv6 주소 지정을 사용하도록 설정합니다.
4. 인터페이스 **ID**에 64비트 확장 고유 식별자(EUI-64)를 16진수 형식(예: 00:26:08:FF:FE:DE:4E:29)으로 입력합니다. 이 필드를 비워 두면 방화벽은 물리적 인터페이스의 MAC 주소에서 생성된 EUI-64를 사용합니다. 주소를 추가할 때 인터페이스 ID를 호스트 부분으로 사용 옵션을 사용하도록 설정하면 방화벽은 인터페이스 **ID**를 해당 주소의 호스트 부분으로 사용합니다.
5. IPv6 주소를 추가하거나 주소 그룹을 선택합니다.
6. 인터페이스에서 이 IPv6 주소를 활성화하려면 인터페이스에서 주소 활성화를 선택합니다.
7. 인터페이스 ID를 호스트 부분으로 사용을 선택하여 인터페이스 **ID**를 **IPv6** 주소의 호스트 부분으로 사용합니다.
8. (선택 사항) 애니캐스트를 선택하여 IPv6 주소(경로)를 애니캐스트 주소(경로)로 만들면 여러 위치가 동일한 접두사를 알릴 수 있으며, IPv6은 라우팅 프로토콜 비용 및 기타 요인에 따라 애니캐스트 트래픽을 가장 가까운 노드로 보냅니다.
9. (이더넷 인터페이스만 해당) 방화벽이 라우터 알림에서 이 주소를 보낼 수 있도록 하려면 라우터 알림**(RA)** 보내기를 선택합니다. 이 경우 인터페이스에서 전역 라우터 알림 사용 옵션도 활성화해야 합니다(다음 단계).
10. (이더넷 인터페이스만 해당) 방화벽이 주소가 유효한 것으로 간주하는 유효 수명**(**초**)(**초**)**을 초 단위로 입력합니다. 유효 수명은 기본 수명**(**초**)**(기본값은 2,592,000)과 같거나 초과해야 합니다.
11. (이더넷 인터페이스만 해당) 유효한 주소가 선호되는 기본 설정 수명**(**초**)**을 입력합니다. 즉, 방화벽이 이 주소를 사용하여 트래픽을 보내고 받을 수 있습니다. 기본 설정 수명이 만료된 후 방화

벽은 주소를 사용하여 새 연결을 설정할 수 없지만 유효 수명이 만료될 때까지 기존 연결은 유효합니다(기본값은 604,800).

12. (이더넷 인터페이스만 해당) 접두사 내에 주소가 있는 시스템에 라우터 없이 연결할 수 있는 경우 온링크를 선택합니다.
13. (이더넷 인터페이스에만 해당) 시스템이 광고된 접두사와 인터페이스 ID를 결합하여 IP 주소를 독립적으로 생성할 수 있는 경우 자율성을 선택합니다.
14. 확인을 클릭합니다.

STEP 6 | (IPv6 주소만 사용하는 이더넷 또는 VLAN 인터페이스) 방화벽이 인터페이스에서 IPv6 라우터 알림(RA)을 전송하도록 설정하고 선택적으로 RA 매개 변수를 조정합니다.

> 다음 이유 중 하나로 *RA* 매개 변수를 조정합니다*.* 다른 값을 사용하는 라우터*/*호스트와 상호 운용합니다*.* 여러 게이트웨이가 있을 때 빠른 수렴을 달성하기 위해*.* 예를 들어 기본 게이트웨이가 실패한 후 *IPv6* 클라이언트*/*호스트가 기본 게이트웨이를 빠르게 변경하고 네트워크의 다른 기본 게이트웨이로 전달을 시작할 수 있도록 최소 간격*,* 최대 간격 및 라우터 수명 값을 더 낮게 설정합니다*.*

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv6**을 선택합니다.
4. 인터페이스에서 **IPv6** 사용을 선택합니다.
5. 라우터 알림 탭에서 라우터 알림 사용(기본값은 비활성화됨)을 선택합니다.
6. (선택 사항) 방화벽이 보내는 RA 사이의 최소 간격**(**초**)**인 최소 간격(초)을 설정합니다. (범위는 3-1,350, 기본값은 200). 방화벽은 사용자가 설정한 최소값과 최대값 사이의 임의의 간격으로 RA를 보냅니다.
7. (선택 사항) 방화벽이 보내는 RA 사이의 최대 간격**(**초**)**을 설정합니다. (범위는 4-1,800, 기본값은 600). 방화벽은 사용자가 설정한 최소값과 최대값 사이의 임의의 간격으로 RA를 보냅니다.
8. (선택 사항) 나가는 패킷에 대해 클라이언트에 적용하도록 홉 제한을 설정합니다(범위는 1-255, 기본값은 64). 홉 제한이 없는 경우 0을 입력합니다.
9. (선택 사항) 클라이언트에 적용할 링크 최대 전송 단위(MTU)인 링크 **MTU**를 설정합니다(범위는 1,280-9,192, 기본값은 지정되지 않음). 링크 MTU가 없는 경우 지정 되지 않음을 선택합니다.
10. (선택 사항) 연결 가능 시간**(ms)**을 설정합니다. 연결 가능 시간은 클라이언트가 연결 가능 확인 메시지를 수신한 후 이웃에 연결할 수 있다고 가정하는 데 사용할 연결 가능 시간(밀리초)입니다. 도달 가능한 시간 값이 없는 경우 지정되지 않음을 선택합니다(범위는 0-3,600,000, 기본값은 지정되지 않음).
11. (선택 사항) 이웃 요청 메시지를 다시 전송하기 전에 클라이언트가 대기할 시간을 밀리초 단위로 결정하는 재전송 타이머인 재전송 시간**(ms)**을 설정합니다. 재전송 시간 없이 지정되지 않음을 선택합니다(범위는 0-4,294,967,295, 기본값은 지정되지 않음).
12. (선택 사항) 라우터 수명**(**초**)**을 설정하여 클라이언트가 방화벽을 기본 게이트웨이로 사용하는 시간(초)을 지정합니다(범위는 0-9,000, 기본값은 1,800). 0은 방화벽이 기본 게이트웨이가 아님

을 지정합니다. 유효 시간이 만료되면 클라이언트는 기본 라우터 목록에서 방화벽 항목을 제거하고 다른 라우터를 기본 게이트웨이로 사용합니다.

13. 네트워크 세그먼트에 여러 IPv6 라우터가 있는 경우 클라이언트가 기본 설정 라우터를 선택하는데 사용하는 라우터 기본 설정을 지정합니다. 높음, 중간(기본값) 또는 낮음은 RA가 세그먼트의 다른 라우터에 비해 방화벽 가상 라우터의 상대적 우선 순위를 나타내는 우선 순위입니다.
14. 관리되는 구성을 선택하여 DHCPv6을 통해 주소를 사용할 수 있음을 클라이언트에 나타냅니다.
15. 기타 구성을 선택하여 DHCPv6을 통해 다른 주소 정보(예: DNS 관련 설정)를 사용할 수 있음을 클라이언트에 나타냅니다.
16. 일관성 확인을 선택하여 방화벽이 다른 라우터에서 보낸 RA가 링크에 일관된 정보를 알리고 있는지 확인하도록 합니다. 방화벽은 불일치를 기록합니다.
17. 확인을 클릭합니다.

STEP 7 | (IPv6 주소만 사용하는 이더넷 또는 VLAN 인터페이스) 방화벽이 이 인터페이스의 ND 라우터 알림에 알릴 재귀 DNS 서버 주소 및 DNS 검색 목록을 지정합니다.

RDNS 서버 및 DNS 검색 목록은 클라이언트가 IPv6 DNS 요청을 확인할 수 있도록 DNS 클라이언트에 대한 DNS 구성의 일부입니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv6** > **DNS** 지원을 선택합니다.
4. 라우터 알림에 DNS 정보를 포함시켜 방화벽이 IPv6 DNS 정보를 보낼 수 있도록 합니다.
5. DNS 서버의 경우 재귀 DNS 서버의 IPv6 주소를 추가합니다. 최대 8개의 재귀 DNS 서버를 추가합니다. 방화벽은 ICMPv6 라우터 알림의 서버 주소를 위에서 아래로 순서대로 보냅니다.
6. 클라이언트가 특정 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간(초)인 수명을 지정합니다.
   - 수명 범위는 최대 간격(라우터 알림 탭에서 구성)과 최대 간격의 두 배와 같거나 그 사이의 값입니다. 예를 들어 최대 간격이 600초인 경우 수명 범위는 600-1,200초입니다.
   - 기본 수명은 1,200초입니다.
7. DNS 접미사의 경우 **DNS** 접미사(최대 255바이트의 도메인 이름)를 추가합니다. 최대 8개의 DNS 접미사를 추가합니다. 방화벽은 ICMPv6 라우터 알림에서 접미사를 위에서 아래로 순서대로 보냅니다.
8. 클라이언트가 접미사를 사용할 수 있는 최대 시간인 수명(초)을 지정합니다. 수명은 서버와 동일한 범위와 기본값을 갖습니다.
9. 확인을 클릭합니다.

STEP 8 | (이더넷 또는 VLAN 인터페이스) 정적 ARP 항목을 지정합니다. 정적 ARP 항목은 ARP 처리를 줄입니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. 고급 > **ARP** 항목을 선택합니다.
4. **IP** 주소 및 해당 **MAC** 주소(하드웨어 또는 미디어 액세스 제어 주소)를 추가합니다. VLAN 인터페이스의 경우 인터페이스도 선택해야 합니다.

   정적 *ARP* 항목은 시간 초과되지 않습니다*.* 캐시의 자동 학습된 *ARP* 항목은 기본적으로 *1,800*초 후에 시간 초과됩니다*. ARP* 캐시 시간 초과를 사용자 지정할 수 있습니다*.* 세션 시간 초과 구성을 참조하십시오*.*

5. 확인을 클릭합니다.

STEP 9 | (이더넷 또는 VLAN 인터페이스) 정적 이웃 검색 프로토콜(NDP) 항목을 지정합니다. IPv6용 NDP는 IPv4용 ARP에서 제공하는 것과 유사한 기능을 수행합니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. 고급 > **ND** 항목을 선택합니다.
4. **IPv6** 주소 및 해당 **MAC** 주소를 추가합니다.
5. 확인을 클릭합니다.

STEP 10 | (선택 사항) 인터페이스에서 서비스를 사용하도록 설정합니다.

1. 인터페이스에서 서비스를 활성화하려면 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. 고급 > 기타 정보를 선택합니다.
4. 관리 프로파일 목록을 확장하고 프로파일 또는 새 관리 프로파일을 선택합니다.
5. 프로파일의 이름을 입력합니다.
6. 허용되는 서비스에 대해 **Ping**과 같은 서비스를 선택하고 확인을 클릭합니다.

STEP 11 | 변경 사항을 커밋합니다.

STEP 12 | 인터페이스를 케이블로 연결합니다.

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

STEP 13 | 인터페이스가 활성 상태인지 확인합니다.

웹 인터페이스에서 네트워크 > 인터페이스를 선택하고 링크 상태 열의 아이콘이 녹색인지 확인합니다. 대시보드의 인터페이스 위젯에서 링크 상태를 모니터링할 수도 있습니다.

STEP 14 | 가상 라우터 또는 논리적 라우터가 트래픽을 라우팅할 수 있도록 정적 경로 및/또는 동적 라우팅 프로토콜을 구성합니다.

STEP 15 | 기본 경로를 구성합니다.

정적 경로 또는 정적 경로 만들기 논리적 라우터를 구성하고 기본값으로 설정합니다.

NDP를 사용하여 IPv6 호스트 관리

이 항목에서는 NDP를 사용하여 IPv6 호스트를 프로비저닝하는 방법에 대해 설명합니다. 따라서 이를 위해 별도의 DHCPv6 서버가 필요하지 않습니다. 또한 NDP를 사용하여 IPv6 주소를 모니터링하는 방법을 설명하므로 보안 규칙을 위반한 디바이스 및 관련 사용자의 IPv6 주소와 MAC 주소를 빠르게 추적할 수 있습니다.

- DNS 구성을 위한 IPv6 라우터 알림
- IPv6 라우터 알림용 RDNS 서버 및 DNS 검색 목록 구성
- NDP 모니터링
- NDP 모니터링 활성화

DNS 구성을 위한 **IPv6** 라우터 알림

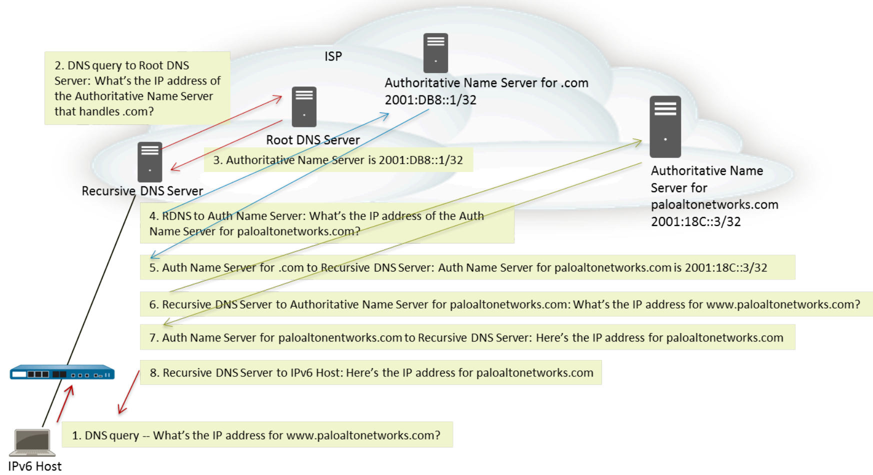
ND(Neighbor Discovery)의 방화벽 구현이 향상되어 RFC 6106, DNS 구성을 위한 IPv6 라우터 보급 옵션에 따라 RDNSS(Recursive DNS Server) 옵션 및 DNSSL(DNS 검색 목록) 옵션을 사용하여 IPv6 호스트를 프로비저닝할 수 있습니다. 레이어 3 인터페이스를 구성할 때 방화벽이 IPv6 호스트를 프로비저닝할 수 있도록 방화벽에서 이러한 DNS 옵션을 구성합니다. 따라서 호스트를 프로비저닝하기 위해 별도의 DHCPv6 서버가 필요하지 않습니다. 방화벽은 이러한 옵션이 포함된 IPv6 라우터 광고(RA)를 DNS 구성의 일부로 IPv6 호스트에 전송하여 인터넷 서비스에 도달하도록 완전히 프로비저닝합니다. 따라서 IPv6 호스트는 다음으로 구성됩니다.

- DNS 쿼리를 해결할 수 있는 RDNS 서버의 주소입니다.
- DNS 쿼리에 도메인 이름을 입력하기 전에 DNS 클라이언트가 정규화되지 않은 도메인 이름에 한 번에 하나씩 추가하는 도메인 이름(접미사) 목록입니다.

DNS 구성을 위한 IPv6 라우터 광고는 모든 PAN-OS 플랫폼에서 이더넷 인터페이스, 하위 인터페이스, 통합 이더넷 인터페이스 및 레이어 3 VLAN 인터페이스에 대해 지원됩니다.

DNS 구성을 위해 ***IPv6 RA***를 보내는 방화벽의 기능은 방화벽이 ***DHCP***와 유사한 역할을 수행할 수 있도록 하며 방화벽이 ***DNS*** 프록시, ***DNS*** 클라이언트 또는 ***DNS*** 서버인 것과 관련이 없습니다.

RDNS 서버 주소로 방화벽을 구성하면 방화벽이 해당 주소로 IPv6 호스트(DNS 클라이언트)를 프로비저닝합니다. IPv6 호스트는 이러한 주소 중 하나 이상을 사용하여 RDNS 서버에 도달합니다. 재귀 DNS는 다음 그림에서 세 쌍의 쿼리 및 응답과 함께 표시된 것처럼 RDNS 서버에 의한 일련의 DNS 요청을 나타냅니다. 예를 들어, 사용자가 www.paloaltonetworks.com에 액세스하려고 하면 로컬 브라우저는 캐시에 해당 도메인 이름에 대한 IP 주소가 없고 클라이언트의 운영 체제에도 IP 주소가 없음을 확인합니다. 클라이언트의 운영 체제는 로컬 ISP에 속한 재귀 DNS 서버에 대한 DNS 쿼리를 시작합니다.



IPv6 라우터 광고에는 각각 수명이 같거나 다른 여러 DNS 재귀 서버 주소 옵션이 포함될 수 있습니다. 단일 DNS 재귀 DNS 서버 주소 옵션은 주소의 수명이 동일한 한 여러 재귀 DNS 서버 주소를 포함할 수 있습니다.

DNS 검색 목록은 방화벽이 DNS 클라이언트에 알리는 도메인 이름(접미사) 목록입니다. 따라서 방화벽은 정규화되지 않은 DNS 쿼리에서 접미사를 사용하도록 DNS 클라이언트를 프로비저닝합니다. DNS 클라이언트는 DNS 쿼리에 이름을 입력하기 전에 정규화되지 않은 도메인 이름에 한 번에 하나씩 접미사를 추가하여 DNS 쿼리에 FQDN(정규화된 도메인 이름)을 사용합니다. 예를 들어, 사용자(구성 중인 DNS 클라이언트의)가 접미사 없이 "quality"라는 이름에 대한 DNS 쿼리를 제출하려고 하면 라우터는 마침표와 DNS 검색 목록의 첫 번째 DNS 접미사를 이름에 추가하고 DNS 쿼리를 전송합니다. 목록의 첫 번째 DNS 접미사가 "company.com"인 경우 라우터의 DNS 쿼리 결과는 FQDN "quality.company.com"에 대한 것입니다.

DNS 쿼리가 실패하면 클라이언트는 목록에서 두 번째 DNS 접미사를 정규화되지 않은 이름에 추가하고 새 DNS 쿼리를 전송합니다. 클라이언트는 DNS 조회가 성공하거나(나머지 접미사 무시) 라우터가 목록의 모든 접미사를 시도할 때까지 DNS 접미사를 순서대로 사용합니다.

ND DNSSL 옵션에서 DNS 클라이언트 라우터에 제공할 접미사로 방화벽을 구성합니다. DNS 검색 목록 옵션을 수신하는 DNS 클라이언트는 정규화되지 않은 DNS 쿼리에서 접미사를 사용하도록 프로비저닝됩니다.

RDNS 서버 및 DNS 검색 목록을 지정하려면 IPv6 라우터 광고에 대한 RDNS 서버 및 DNS 검색 목록을 구성합니다.

IPv6 라우터 알림에 대한 **RDNS** 서버 및 **DNS** 검색 목록 구성

IPv6 호스트의 DNS 구성에 대한 IPv6 라우터 알림을 구성하려면 이 작업을 수행하십시오.

STEP 1 | 인터페이스에서 IPv6 라우터 광고를 보내도록 방화벽을 활성화합니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv6** 탭에서 인터페이스에서 **IPv6** 사용을 선택합니다.
4. 라우터 알림 탭에서 라우터 알림 사용을 선택합니다.
5. 확인을 클릭합니다.

STEP 2 | 방화벽이 이 인터페이스의 ND 라우터 광고에서 광고할 재귀 DNS 서버 주소 및 DNS 검색 목록을 지정합니다.

RDNS 서버 및 DNS 검색 목록은 클라이언트가 IPv6 DNS 요청을 확인할 수 있도록 DNS 클라이언트에 대한 DNS 구성의 일부입니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv6** > **DNS** 지원을 선택합니다.
4. 라우터 알림에 DNS 정보를 포함시켜 방화벽이 IPv6 DNS 정보를 보낼 수 있도록 합니다.
5. DNS 서버의 경우 재귀 DNS 서버의 IPv6 주소를 추가합니다. 최대 8개의 재귀 DNS 서버를 추가합니다. 방화벽은 ICMPv6 라우터 알림의 서버 주소를 위에서 아래로 순서대로 보냅니다.
6. 클라이언트가 특정 RDNS 서버를 사용하여 도메인 이름을 확인할 수 있는 최대 시간(초)인 수명을 지정합니다.
   - 수명 범위는 최대 간격(라우터 알림 탭에서 구성)과 최대 간격의 두 배와 같거나 그 사이의 값입니다. 예를 들어 최대 간격이 600초인 경우 수명 범위는 600-1,200초입니다.
   - 기본 수명은 1,200초입니다.
7. DNS 접미사의 경우 **DNS** 접미사(최대 255바이트의 도메인 이름)를 추가합니다. 최대 8개의 DNS 접미사를 추가합니다. 방화벽은 ICMPv6 라우터 알림에서 접미사를 위에서 아래로 순서대로 보냅니다.
8. 클라이언트가 접미사를 사용할 수 있는 최대 시간인 수명(초)을 지정합니다. 수명은 서버와 동일한 범위와 기본값을 갖습니다.
9. 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

NDP 모니터링

IPv6용 NDP(Neighbor Discovery Protocol)(RFC 4861)는 IPv4용 ARP 기능과 유사한 기능을 수행합니다. 방화벽은 기본적으로 ICMPv6 패킷을 사용하여 연결된 링크에서 링크 계층 주소와 이웃의 상태를 검색하고 추적하는 NDP를 실행합니다.

NDP 모니터링 활성화, 링크 로컬 네트워크에 있는 디바이스의 IPv6 주소, 해당 MAC 주소, User-ID의 관련 사용자 이름(해당 디바이스의 사용자가 디렉토리 서비스를 사용하여 로그인한 경우), 주소의 연결 가능성 상태 및 NDP 모니터가 이 IPv6 주소에서 라우터 알림을 수신한 마지막으로 보고된 날짜 및 시간을 볼 수 있습니다. 사용자 이름은 최상의 경우를 기준으로 합니다. 프린터, 팩스, 서버 등과 같이 사용자 이름이 없는 많은 IPv6 디바이스가 네트워크에 있을 수 있습니다.

보안 규칙을 위반한 디바이스 및 사용자를 빠르게 추적하려면 IPv6 주소, MAC 주소 및 사용자 이름을 한 곳에 모두 표시하는 것이 매우 유용합니다. MAC 주소를 물리적 스위치 또는 액세스 포인트로 다시 추적하려면 IPv6 주소에 해당하는 MAC 주소가 필요합니다.

NDP 모니터링은 방화벽과 클라이언트 사이에 *NDP* 또는 *DAD(*중복 주소 감지*)* 메시지를 필터링하는 다른 네트워킹 디바이스가 있을 수 있으므로 모든 디바이스를 검색한다고 보장할 수 없습니다*.* 방화벽은 인터페이스에서 학습한 디바이스만 모니터링할 수 있습니다*.*

NDP 모니터링은 클라이언트와 이웃에서 보내는 DAD(중복 주소 감지) 패킷도 모니터링합니다. 또한 문제 해결을 더 쉽게 하기 위해 IPv6 ND 로그를 모니터링할 수도 있습니다.

NDP 모니터링은 모든 PAN-OS 모델에서 이더넷 인터페이스, 하위 인터페이스, 통합 이더넷 인터페이스 및 VLAN 인터페이스에 대해 지원됩니다.

NDP 모니터링 활성화

인터페이스에 대해 NDP 모니터링을 활성화하려면 이 작업을 수행합니다.

STEP 1 | NDP 모니터링을 활성화합니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. 구성할 인터페이스를 선택합니다.
3. **IPv6**을 선택합니다.
4. 주소 확인을 선택합니다.
5. **NDP** 모니터링 활성화를 선택합니다.

   NDP 모니터링을 활성화 또는 비활성화한 후 *NDP* 모니터링을 시작하거나 중지하려면 먼저 커밋해야 합니다.
6. 확인을 클릭합니다.

STEP 2 | 변경 사항을 커밋합니다.

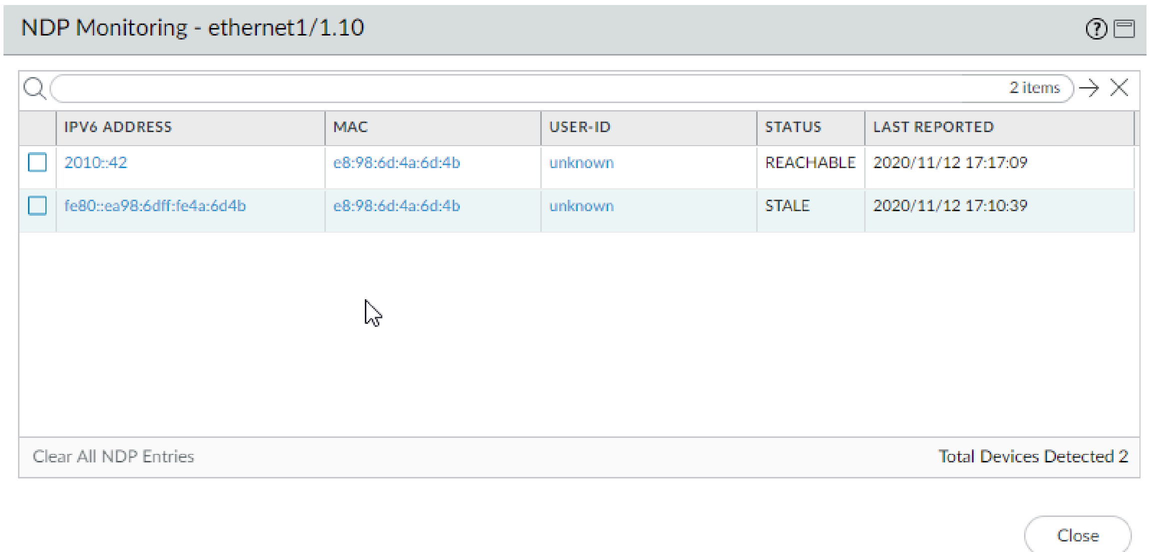
커밋을 클릭합니다.

STEP 3 | 클라이언트와 인접한 NDP 및 DAD 패킷을 모니터링합니다.

1. 네트워크 > 인터페이스 및 이더넷 또는 **VLAN**을 선택합니다.
2. NDP 모니터링을 활성화한 인터페이스의 경우 기능 열에서 NDP 모니터링 아이콘 위로 마우스를 가져갑니다.

   인터페이스에 대한 NDP 모니터링 요약은 RA가 활성화된 경우 이 인터페이스가 라우터 광고(RA)에서 보낼 IPv6 접두사 목록을 표시합니다(인터페이스 자체의 IPv6 접두사임).

   요약은 또한 DAD, 라우터 보급 및 DNS 지원이 활성화되었는지 여부를 나타냅니다. 즉, 구성된 모든 재귀 DNS 서버의 IP 주소 및 DNS 검색 목록에 구성된 모든 DNS 접미사를 뜻합니다.
3. NDP 모니터링 아이콘을 클릭하면 자세한 정보가 표시됩니다.



인터페이스에 대한 세부 NDP 모니터링 테이블의 각 행에는 방화벽이 발견한 인접 네트워크의 IPv6 주소, 해당 MAC 주소, 해당 사용자 ID(최상의 경우), 도달 가능성 주소 상태 및 마지막 보고 날짜가 표시됩니다. 이 NDP 모니터가 이 IP 주소에서 RA를 수신한 시간입니다. 프린터 또는 기타 사용자 기반 호스트가 아닌 경우 사용자 ID가 표시되지 않습니다. IP 주소의 상태가 Stale이면 이웃은 RFC 4861에 따라 연결할 수 없는 것으로 알려져 있습니다.

오른쪽 하단에는 링크 로컬 네트워크에서 감지된 총 디바이스 수가 표시됩니다.

- 필터 필드에 IPv6 주소를 입력하여 표시할 주소를 검색합니다.
- IPv6 주소를 표시하거나 표시하지 않으려면 확인란을 선택합니다.
- 숫자, 오른쪽 또는 왼쪽 화살표 또는 세로 스크롤 막대를 클릭하여 많은 항목을 탐색합니다.
- 전체 테이블을 지우려면 모든 **NDP** 항목 지우기를 클릭합니다.

STEP 4 | 보고 목적으로 ND 로그를 모니터링합니다.

1. 모니터 > 로그 > 시스템을 선택합니다.
2. 유형 열에서**ipv6nd** 로그 및 해당 설명을 봅니다.

   예를 들어, 일치하지 않는 라우터 알림 수신은 방화벽이 전송하려는 RA와 다른 RA를 수신했음을 나타냅니다.

집계 인터페이스 그룹 구성

집계 인터페이스 그룹은 IEEE 802.1AX 링크 집계를 사용하여 여러 이더넷 인터페이스를 방화벽을 다른 네트워크 장치 또는 방화벽에 연결하는 단일 가상 인터페이스로 결합합니다. 집계 그룹은 결합된 인터페이스에서 트래픽의 부하 균형을 조정하여 피어 간의 대역폭을 증가시킵니다. 또한 중복성을 제공합니다. 하나의 인터페이스가 실패하면 나머지 인터페이스는 트래픽을 계속 지원합니다.

기본적으로 인터페이스 오류 감지는 직접 연결된 피어 간의 물리적 계층에서만 자동으로 수행됩니다. 그러나 링크 집계 제어 프로토콜(LACP)을 사용하도록 설정하면 피어가 직접 연결되어 있는지 여부에 관계없이 물리적 및 데이터 링크 계층에서 오류 감지가 자동으로 수행됩니다. 또한 LACP를 사용하면 핫 스페어를 구성하면 자동 장애 조치로 대기 인터페이스를 대기할 수 있습니다. VM 시리즈 모델을 제외한 모든 팔로 알토 네트웍스®는 방화벽을 집계 그룹을 지원합니다. 제품 선택 도구는 각 방화벽이 지원하는 집계 그룹 수를 나타냅니다. 각 집계 그룹에는 최대 8개의 인터페이스가 있을 수 있습니다.

> *PAN-OS®* 방화벽 모델은 물리적 또는 가상 레이어 *3* 인터페이스에 할당된 최대 *16,000*개의 *IP* 주소를 지원하며, 이 최대값에는 *IPv4* 및 *IPv6* 주소가 모두 포함됩니다.

QoS는 처음 8개의 집계 그룹에서만 지원됩니다.

집계 그룹을 구성하기 전에 해당 인터페이스를 구성해야 합니다. 특정 집계 그룹에 할당된 인터페이스 중 하드웨어 미디어는 다를 수 있지만(예: 광섬유와 구리를 혼합할 수 있음) 대역폭 및 인터페이스 유형은 동일해야 합니다. 대역폭 및 인터페이스 유형 옵션은 다음과 같습니다.

- 대역폭—1Gbps, 10Gbps, 40Gbps 또는 100Gbps.
- 인터페이스 유형-HA3, 가상 와이어, 레이어 2 또는 레이어 3.

> 이 절차는 팔로 알토 네트웍스 방화벽의 구성 단계에 대해서만 설명합니다. 피어 장치에서 집계 그룹을 구성해야 합니다. 해당 디바이스의 설명서를 참조하여 지침을 참조하십시오.

STEP 1 | 일반 인터페이스 그룹 매개 변수를 구성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 집계 그룹을 추가합니다.
2. 읽기 전용 인터페이스 이름에 인접한 필드에서 숫자(1-8)를 입력하여 집계 그룹을 식별합니다. 범위는 1에서 방화벽이 지원하는 최대 집계 인터페이스 그룹 수입니다.
3. 인터페이스 유형의 경우 **HA**, 가상 와이어, 레이어**2** 또는 레이어**3**을 선택합니다.
4. 선택한 인터페이스 유형에 대한 나머지 매개 변수를 구성합니다.

STEP 2 | LACP 설정을 구성합니다.

집계 그룹에 대한 LACP를 사용하도록 설정하려는 경우에만 이 단계를 수행합니다.

가상 와이어 인터페이스에 대해 *LACP*를 활성화할 수 없습니다.

1. **LACP** 탭을 선택하고 **LACP**를 활성화합니다.
2. LACP 상태 쿼리 모드를 패시브(방화벽이 기본값으로 응답하기만 하면) 또는 활성(방화벽 쿼리 피어 디바이스)으로 설정합니다.

   모범 사례로 한 *LACP* 피어를 활성으로 설정하고 다른 한 피어를 수동으로 설정합니다. 두 피어가 수동적인 경우 *LACP*가 작동할 수 없습니다. 방화벽은 피어 장치의 모드를 감지할 수 없습니다.
3. LACP 쿼리 및 응답 교환의 전송 속도를 느리게(30초마다 - 기본값) 또는 빠르게(초당)로 설정합니다. 네트워크가 지원하는 LACP 처리량과 LACP 피어가 인터페이스 오류를 감지하고 해결해야 하는 빈도에 따라 선택을 기반으로 합니다.
4. 1초 이내에 대기 인터페이스에 장애 조치 기능을 사용하도록 설정하려면 빠른 장애 조치를 선택합니다. 기본적으로 이 옵션은 비활성화되고 방화벽은 장애 조치 처리에 IEEE 802.1ax 표준을 사용하며, 이 표준은 3초 이상 걸립니다.

   모범 사례로 표준 장애 조치 조치 간격 동안 중요한 데이터가 손실될 수 있는 배포에서 빠른 장애 조치 방법을 사용합니다.
5. 집계 그룹에서 활성(1~8)인 최대 포트(인터페이스 수)를 입력합니다. 그룹에 할당한 인터페이스 수가 **Max** 포트를 초과하면 나머지 인터페이스는 대기 모드에 있습니다. 방화벽은 할당한 각 인터페이스(3단계)의 **LACP** 포트 우선 순위를 사용하여 처음에 활성화된 인터페이스를 결정하고 장애 조치 시 대기 인터페이스가 활성화되는 순서를 결정합니다. LACP 피어에 일치하지 않는 포트 우선 순위 값이 있는 경우 시스템 우선 순위가 낮은 피어값(기본값은 32,768개, 범위는 1~65,535개)이 다른 피어를 재정의합니다.
6. (선택 사항)활성/수동 방화벽의 경우 패시브 방화벽에 대한 LACP 사전 협상을 활성화하려면 **HA** 패시브 상태에서만 사용하도록 설정합니다. LACP 사전 협상을 통해 패시브 방화벽에 대한 더 빠른 장애 조치(자세한 내용은 활성/패시브 HA에 대한 LACP 및 LLDP 사전 협상 참조)를 빠르게 사용할 수 있습니다.

   이 옵션을 선택하면 활성 수동 *HA*에 대해 동일한 시스템 *MAC* 주소를선택할 수 없습니다. 사전 협상하려면 각 *HA* 방화벽에 고유한 인터페이스 *MAC* 주소가 필요합니다.
7. (선택 사항)활성/수동 방화벽의 경우 활성 수동 **HA**에 대해 동일한 시스템 **MAC** 주소를 선택하고 두 HA 방화벽에 대해 단일 **MAC** 주소를 지정합니다. 이 옵션은 LACP 피어가 가상화된 경우 장애 조치 지연 시간을 최소화합니다(네트워크에 단일 장치로 표시됨). 기본적으로 옵션은 비활성화되며, HA 쌍의 각 방화벽에는 고유한 MAC 주소가 있습니다.

   LACP 피어가 가상화되지 않은 경우 고유한 *MAC* 주소를 사용하여 장애 조치 지연 시간을 최소화합니다.

STEP 3 | 확인을 클릭합니다.

STEP 4 | 집계 그룹에 인터페이스를 할당합니다.

집계 그룹의 구성원이 될 각 인터페이스(1-8)에 대해 다음 단계를 수행합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 인터페이스 이름을 클릭하여 편집합니다.
2. 인터페이스 유형을 집계 이더넷으로 설정합니다.
3. 방금 정의한 집계 그룹을 선택합니다.
4. 링크 속도, 링크 듀플렉스 및 링크 상태를 선택합니다.

   모범 사례로 그룹의 모든 인터페이스에 대해 동일한 링크 속도와 이중 값을 설정합니다. 일치하지 않는 값의 경우 방화벽은 더 높은 속도와 전체 듀플렉스로 기본값입니다.

5. (선택 사항)집계 그룹에 대한 LACP를 활성화하는 경우 **LACP** 포트 우선 순위를 입력합니다(기본값은 32,768; 범위는 1~65,535). 할당할 인터페이스 수가 그룹의 최대 포트 값을 초과하는 경우 포트 우선 순위에 따라 활성 또는 대기 중인 인터페이스가 결정됩니다. 숫자가 낮은 인터페이스(높은 우선 순위)가 활성화됩니다.
6. 확인을 클릭합니다.

STEP 5 | 방화벽에 활성/활성 구성이 있고 HA3 인터페이스를 집계하는 경우 집계 그룹에 대한 패킷 전달을 사용하도록 설정합니다.

1. 디바이스 > 고가용성 > 활성/활성 구성을 선택하고 패킷 전달 섹션을 편집합니다.
2. **HA3** 인터페이스에 대해 구성된 집계 그룹을 선택하고 확인을 클릭합니다.

STEP 6 | 변경 사항을 커밋합니다.

STEP 7 | 집계 그룹 상태를 확인합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택합니다.
2. Link 상태 열에 집계 그룹에 대한 녹색 아이콘이 표시되어 있는지 확인하여 모든 멤버 인터페이스가 최대 상태임을 나타냅니다. 아이콘이 노란색인 경우 적어도 하나의 멤버가 다운되었지만 전부는 아닙니다. 아이콘이 빨간색이면 모든 멤버가 다운됩니다.
3. LACP를 구성한 경우 피처 열에 집계 그룹에 대한 LACP 지원 아이콘 이 표시되는지 확인합니다.

STEP 8 | (PA-7050 및 PA-7080 방화벽만)서로 다른 라인 카드에 인터페이스가 있는 집계 인터페이스 그룹이 있는 경우 방화벽을 활성화하여 여러 카드에 분산되는 AE 그룹의 여러 인터페이스에서 수신하는 조각난 IP 패킷을 처리할 수 있도록 하는 것이 좋습니다. 이렇게 하려면 **해시** 키워드와 함께 다음 CLI 운영 명령을 사용합니다. (다른 두 키워드도 완전성을 위해 표시됩니다.)

1. CLI에 액세스합니다.
2. 다음 작동 CLI 명령 사용: **`set ae-frag redistribution-policy`** <**`self`** | **`fixed sXdpX`** | **`hash`**>

   - **자체**—(기본값)이 키워드는 레거시 동작을 위한 것입니다. 방화벽이 AE 인터페이스 그룹의 여러 인터페이스에서 받은 조각난 패킷을 처리할 수 없습니다.
   - **고정** **s**<*slot-number*>**dp**<*dataplane-cpu-number*>— 슬롯 번호 변수를 교체하고 모든 AE 인터페이스의 모든 구성원이 받은 모든 IP 조각을 처리하는 데이터 평면 번호로 데이터 평면-

CPU 번호 변수를 대체합니다. 고정 키워드는 주로 문제 해결을 위한 것이며 프로덕션 환경에서 사용해서는 안 됩니다.

- 해시—방화벽이 둘 이상의 라인 카드에 있는 AE 인터페이스 그룹의 여러 인터페이스에서 수신하는 조각난 패킷을 처리할 수 있도록 하는 데 사용합니다.

네트워크 분할을 위한 봉쥬르 리플렉터 구성

애플 봉쥬르(제로 구성 네트워킹이라고도 함)를 사용하면 로컬 네트워크에서 디바이스 및 서비스를 자동으로 검색할 수 있습니다. 예를 들어, 봉쥬르를 사용하면 프린터의 IP 주소를 수동으로 구성하지 않고도 프린터에 연결할 수 있습니다. 이름을 로컬 네트워크의 주소로 변환하기 위해, 봉쥬르는 mDNS(멀티캐스트 DNS)를 사용합니다. 봉쥬르는 트래픽 라우팅을 허용하지 않는, 개인 멀티캐스트 범위를 트래픽에 사용하므로, 보안 또는 관리 목적으로 네트워크 분할을 사용하는 환경(예: 서버와 클라이언트가 서로 다른 서브넷에 있는 경우)에서 사용할 수 없습니다.

세분화를 사용하여 트래픽을 라우팅하는 네트워크 환경에서 애플 봉쥬르를 지원하기 위해, 지정한 레이어 3 인터페이스(L3) 이더넷 또는 통합 이더넷(AE) 인터페이스 또는 하위 인터페이스 간에 봉쥬르 IPv4 트래픽을 전달할 수 있습니다. 봉쥬르 리플렉터 옵션을 사용하면 멀티캐스트 봉쥬르 알림 및 쿼리를 L3 이더넷 및 AE 인터페이스 또는 하위 인터페이스로 전달할 수 있으므로, TTL(Time To Live) 값이나 홉 제한에 관계없이 서비스 및 디바이스 검색 가능성에 대한 사용자 접속을 보장할 수 있습니다.

봉쥬르 트래픽 포워딩은 *PA-220, PA-400, PA-800* 및 *PA-3200* 시리즈에서 지원됩니다.

이 옵션을 작동시키면, 방화벽이 봉쥬르 트래픽을 이 옵션을 작동시킨 L3 및 AE 인터페이스와 하위 인터페이스로 리디렉션합니다. 봉쥬르 트래픽을 관리하려는 지원되는 모든 인터페이스에서 이 옵션을 작동시켜야 합니다. 예를 들어, 특정 L3 인터페이스가 봉쥬르 트래픽을 AE 인터페이스로 전달하도록 하려면 두 인터페이스 모두에서 이 옵션을 작동시켜야 합니다. 최대 16개의 인터페이스에서 이 옵션을 작동시킬 수 있습니다.

루프를 방지하기 위해 방화벽은 소스 *MAC* 주소를 방화벽의 송신 인터페이스 *MAC* 주소로 수정합니다. 플러딩 공격을 방지하기 위해 방화벽이 다음 표에 지정된 초당 패킷 수 이상을 수신하는 경우, 방화벽은 패킷을 삭제하여 방화벽과 네트워크를 보호합니다.

시리즈	속도 제한(초당)
PA-220	*100*
PA-400	*N/A*
PA-800	*200*
PA-3200	*500*

의 대역폭을 거의 차지하지 않아야 합니다.

STEP 1 | 네트워크 > 인터페이스를 선택합니다.

STEP 2 | L3 이더넷, 하위 인터페이스 또는 AE 인터페이스를 선택하거나 추가합니다.

> 하위 인터페이스를 추가하는 경우 *0*이 아닌 태그를 사용해야 합니다.

STEP 3 | **IPv4**를 선택한 다음 봉쥬르 리플렉터 활성화 옵션을 선택합니다.

STEP 4 | 확인을 클릭합니다.

STEP 5 | 봉쥬르 트래픽을 전달할 모든 L3 또는 AE 인터페이스 및 하위 인터페이스에 대해 1-4단계를 반복합니다.

> 최대 *16*개의 다른 인터페이스 또는 하위 인터페이스에서 이 옵션을 작동시킬 수 있습니다.

STEP 6 | 변경 사항을 커밋합니다.

STEP 7 | 봉쥬르 리플렉터 옵션을 활성화한 인터페이스의 특징 열에 봉쥬르 **리플렉터: 예**( )가 표시되는지 확인합니다.

STEP 8 | `show bonjour interface` CLI 명령을 사용하여 방화벽이 봉쥬르 트래픽을 전달하는 모든 인터페이스와 카운터 목록을 표시합니다. `rx`는 인터페이스가 수신하는 총 봉쥬르 패킷 수를 나타내고, `tx`는 인터페이스가 전송하는 총 봉쥬르 패킷 수를 나타내며, `drop`은 인터페이스가 삭제하는 패킷 수를 나타냅니다.

```
admin> show bonjour interface name rx tx drop
 ----------------------------------------------------------
 ethernet1/4 1 1 0 ethernet1/7 0 0 0 ethernet1/7.10 0 0 0
 ethernet1/7.20 4 4 0 ae15 0 0 0 ae16 0 0 0 ae16.30 0 2 0 ae16.40 0
 0 0
```

인터페이스 관리 프로파일을 사용하여 액세스 제한

인터페이스 관리 프로파일은 방화벽 인터페이스가 관리 트래픽에 대해 허용하는 프로토콜, 서비스 및 IP 주소를 정의하여 무단 액세스로부터 방화벽을 보호합니다. 예를 들어, 사용자가 ethernet1/1 인터페이스를 통해 방화벽 웹 인터페이스에 액세스하는 것을 방지하고 해당 인터페이스가 네트워크 모니터링 시스템에서 SNMP 쿼리를 수신하도록 허용할 수 있습니다. 이 경우 인터페이스 관리 프로파일에서 SNMP를 활성화하고 HTTP/HTTPS를 비활성화하고 프로파일을 ethernet1/1에 할당합니다.

인터페이스 관리 프로파일을 레이어 3 이더넷 인터페이스(하위 인터페이스 포함)와 논리적 인터페이스(집계 그룹, VLAN, 루프백 및 터널 인터페이스)에 할당할 수 있습니다. 인터페이스 관리 프로파일을 인터페이스에 할당하지 않으면 기본적으로 모든 IP 주소, 프로토콜 및 서비스에 대한 액세스가 거부됩니다.

관리*(MGT)* 인터페이스에는 인터페이스 관리 프로파일이 필요하지 않습니다*.* 방화벽의 초기 구성을 수행할 때 *MGT* 인터페이스에 대한 프로토콜*,* 서비스 및 *IP* 주소를 제한합니다*. MGT* 인터페이스가 다운된 경우 다른 인터페이스를 통한 관리 액세스를 허용하면 방화벽 관리를 계속할 수 있습니다*.*

인터페이스 관리 프로파일을 사용하여 방화벽 인터페이스에 대한 액세스를 활성화할 때 인터넷이나 엔터프라이즈 보안 경계 내의 다른 신뢰할 수 없는 영역에서 관리 액세스*(HTTP, HTTPS, SSH* 또는 *Telnet)*를 활성화하지 마십시오*.* 이러한 프로토콜은 일반 텍스트로 전송합니다*.* 관리 액세스 보안을 위한 모범 사례를 따라 방화벽에 대한 관리 액세스를 적절하게 보호하고 있는지 확인하십시오*.*

STEP 1 | 인터페이스 관리 프로파일을 구성합니다.

1. 네트워크 > 네트워크 프로파일 > 인터페이스 관리를 선택하고 추가를 클릭합니다.
2. 인터페이스에서 관리 트래픽에 대해 허용하는 프로토콜을 선택합니다. **ping**, **Telnet**, **SSH**, **HTTP**, **HTTP OCSP**, **HTTPS** 또는 **SNMP**.

   HTTP 또는 ***Telnet***은 일반 텍스트로 전송하므로 안전하지 않기에 활성화하지 마십시오*.*
3. 인터페이스가 관리 트래픽에 대해 허용하는 서비스를 선택합니다.
   - 응답 페이지 - 다음에 대한 응답 페이지를 활성화하는 데 사용합니다.
     - 캡티브 포털 - 캡티브 포털 응답 페이지를 제공하기 위해 방화벽은 레이어 3 인터페이스에서 포트를 열어 둡니다. 트랜스페이런트 모드의 캡티브 포털의 경우 6081, 리디렉션 모드의 캡티브 포털의 경우 6082입니다. 자세한 내용은 인증 정책 및 인증 포털을 참조하십시오.
     - **URL** 관리자 무시 - 자세한 내용은 특정 사이트에 대한 암호 액세스 허용을 참조하십시오.
   - 사용자 **ID** - 데이터 및 인증 타임스탬프를 재배포하는 데 사용합니다.
   - 사용자 **ID Syslog** 수신기**-SSL** 또는 사용자 **ID Syslog** 수신기**-UDP** - SSL 또는 UDP를 통한 사용자 매핑에 대해 Syslog 발신자를 모니터링하도록 사용자 ID를 구성하는 데 사용합니다.
4. (선택 사항) 인터페이스에 액세스할 수 있는 허용된 IP 주소를 추가합니다. 목록에 항목을 추가하지 않으면 인터페이스에 IP 주소 제한이 없습니다.
5. 확인을 클릭합니다.

STEP 2 | 인터페이스 관리 프로파일을 인터페이스에 할당합니다.

1. 네트워크 > 인터페이스를 선택하고 인터페이스 유형 (이더넷, **VLAN**, 루프백 또는 터널)을 선택한 다음 인터페이스를 선택합니다.
2. 고급 > 기타 정보를 선택하고 방금 추가한 인터페이스 관리 프로파일을 선택합니다.
3. 확인 및 커밋을 클릭합니다.

가상 라우터

방화벽의 가상 라우터가 레이어 3 라우팅에 참여하고 가상 라우터를 구성하는 방법에 대해 알아봅니다.

- 가상 라우터 개요
- 가상 라우터 구성

가상 라우터 개요

방화벽은 가상 라우터를 사용하여 수동으로 정적 경로를 정의하거나 하나 이상의 레이어 3 라우팅 프로토콜(동적 경로)에 참여하여 다른 서브넷에 대한 레이어 3 경로를 얻습니다. 방화벽이 이러한 방법을 통해 얻은 경로는 방화벽의 IP RIB(라우팅 정보 기반)를 채웁니다. 패킷이 도착한 서브넷과 다른 서브넷으로 향하는 경우 가상 라우터는 RIB에서 최상의 경로를 얻어 FIB(Forwarding Information Base)에 배치하고 패킷을 FIB에서 정의된 다음 홉 라우터에 포워드합니다. 방화벽은 이더넷 스위칭을 사용하여 동일한 IP 서브넷에 있는 다른 디바이스에 도달합니다. (ECMP을(를) 사용하는 경우 FIB로 가는 하나의 최상의 경로에 대한 예외가 발생합니다. 이 경우 모든 동일 비용 경로는 FIB로 이동합니다.)

방화벽에 정의된 이더넷, VLAN 및 터널 인터페이스는 레이어 3 패킷을 수신 및 포워드합니다. 대상 존은 포워드 기준에 따라 나가는 인터페이스에서 파생되며 방화벽은 정책 규칙을 참조하여 각 패킷에 적용되는 보안 정책을 식별합니다. 다른 네트워크 디바이스로 라우팅하는 것 외에도 가상 라우터는 다음 홉이 다른 가상 라우터를 가리키도록 지정된 경우 동일한 방화벽 내의 다른 가상 라우터로 라우팅할 수 있습니다.

동적 라우팅 프로토콜(BGP, OSPF, OSPFv3 또는 RIP)에 참여하고 정적 경로를 추가하도록 가상 라우터의 레이어 3 인터페이스를 구성할 수 있습니다. 또한 가상 라우터 간에 공유되지 않는 별도의 경로 집합을 유지 관리하는 여러 가상 라우터를 생성할 수 있으므로 서로 다른 인터페이스에 대해 서로 다른 라우팅 동작을 구성할 수 있습니다.

각 가상 라우터에서 루프백 인터페이스를 구성하고 두 루프백 인터페이스 사이에 정적 경로를 생성한 다음 이 두 인터페이스 간에 피어링하도록 동적 라우팅 프로토콜을 구성하여 한 가상 라우터에서 다른 가상 라우터로의 동적 라우팅을 구성할 수 있습니다.

방화벽에 정의된 각 레이어 3 이더넷, 루프백, VLAN 및 터널 인터페이스는 가상 라우터와 연결되어야 합니다. 각 인터페이스는 하나의 가상 라우터에만 속할 수 있지만 가상 라우터에 대해 여러 라우팅 프로토콜과 정적 경로를 구성할 수 있습니다. 가상 라우터에 대해 구성하는 정적 경로 및 동적 라우팅 프로토콜에 관계없이 하나의 일반 구성이 필요합니다.

가상 라우터 구성

방화벽에 가상 라우터를 생성하여 레이어 3 라우팅에 참여합니다.

STEP 1 | 네트워크 관리자로부터 필요한 정보를 수집합니다.

- 라우팅을 수행하려는 방화벽의 인터페이스입니다.
- 정적, OSPF 내부, OSPF 외부, IBGP, EBGP 및 RIP에 대한 관리 거리.

STEP 2 | 가상 라우터를 생성하고 여기에 인터페이스를 적용합니다.

방화벽은 기본 설정이라고 명명된 가상 라우터와 함께 제공됩니다. 기본 설정 가상 라우터를 편집하거나 또는 새 가상 라우터를 추가할 수 있습니다.

1. 네트워크 > 가상 라우터를 선택합니다.
2. 가상 라우터(이름이 **default**인 라우터 또는 다른 가상 라우터)를 선택하거나 새 가상 라우터의 이름을 추가합니다.
3. 라우터 설정 > 일반을 선택합니다.
4. 인터페이스 상자에서 추가를 클릭하고 이미 정의된 인터페이스를 선택합니다.

   가상 라우터에 추가하려는 모든 인터페이스에 대해 이 단계를 반복합니다.
5. 확인을 클릭합니다.

STEP 3 | 정적 및 동적 라우팅에 대한 관리 거리를 설정합니다.

네트워크에 필요한 경로 유형에 대해 관리 거리를 설정합니다. 가상 라우터에 동일한 대상에 대한 두 개 이상의 다른 경로가 있는 경우, 관리 거리를 사용하여 다른 라우팅 프로토콜과 정적 경로로부터, 더 낮은 거리를 선호하여 최상의 경로를 선택합니다.

- 정적-범위는 10~240입니다. 기본값은 10입니다.
- **OSPF** 내부-범위는 10~240입니다. 기본값은 30입니다.
- **OSPF** 외부-범위는 10~240입니다. 기본값은 110입니다.
- **IBGP**-범위는 10~240입니다. 기본값은 200입니다.
- **EBGP**-범위는 10~240입니다. 기본값은 20입니다.
- **RIP**-범위는 10~240입니다. 기본값은 120입니다.

전달을 위해 동일한 비용의 여러 경로를 활용하려면 ECMP를 참조하십시오.

STEP 4 | 가상 라우터 일반 설정을 커밋합니다.

확인 및 커밋을 클릭합니다.

STEP 5 | 필요에 따라 이더넷, VLAN, 루프백 및 터널 인터페이스를 구성합니다.

레이어 3 인터페이스를 구성합니다.

서비스 경로

방화벽이 서비스 경로를 사용하여 외부 서비스에 요청을 보내고 서비스 경로를 구성하는 방법에 대해 알아봅니다.

- 서비스 경로 개요
- 서비스 경로 구성

서비스 경로 개요

방화벽은 기본적으로 관리(MGT) 인터페이스를 사용하여 DNS 서버, 외부 인증 서버와 같은 외부 서비스, 소프트웨어, URL 업데이트, 라이선스 및 AutoFocus와 같은 Palo Alto Networks® 서비스에 액세스합니다. MGT 인터페이스 사용에 대한 대안은 이러한 서비스에 액세스하도록 데이터 포트(일반 인터페이스)를 구성하는 것입니다. 인터페이스에서 서버의 서비스까지의 경로를 서비스 경로라고 합니다. 서비스 패킷은 외부 서비스에 할당된 포트의 방화벽을 빠져나가고 서버는 구성된 소스 인터페이스와 소스 IP 주소로 응답을 보냅니다.

서비스 경로 구성방화벽에 대해 전역적으로 또는 여러 가상 시스템에 대해 활성화된 방화벽에서 가상 시스템에 대한 서비스 경로를 사용자 지정할 수 있으므로 가상 시스템과 연결된 인터페이스를 유연하게 사용할 수 있습니다. 특정 서비스에 대해 구성된 서비스 경로가 없는 가상 시스템은 해당 서비스에 대해 전역적으로 설정된 인터페이스와 IP 주소를 상속합니다.

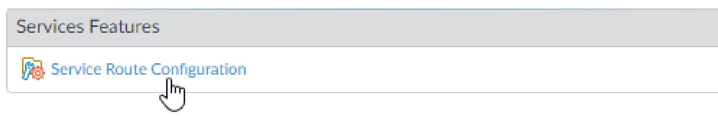
서비스 경로 구성

다음 절차를 통해 방화벽이 Palo Alto Network 클라우드 서비스와 같은 외부 서비스에 요청을 보내거나 로그 전달에 사용하는 인터페이스를 변경하도록 서비스 경로를 구성할 수 있습니다. 고가용성(HA) 구성의 방화벽의 경우 서비스 경로 구성이 HA 피어 간에 동기화됩니다.

활성/수동 HA(고가용성)에 있는 방화벽의 경우 외부 서비스를 활용하거나 로그 전달을 위해 구성한 서비스 경로는 **활성** HA 피어에서만 활동을 보고 **수동** HA 피어는 이더넷 인터페이스를 소스 인터페이스로 구성한 경우 활동을 보지 않습니다. 예를 들어 이더넷 1/3을 소스 인터페이스로 사용하여 서비스 경로를 구성하여 Cortex Data Lake에 로그를 전달합니다. 이 시나리오에서 모든 로그는 **활성** HA 피어에서 전달되지만 시스템 및 구성 로그를 포함한 로그는 **수동** HA 피어에서 전달되지 않습니다. 그러나 MGT 인터페이스를 서비스 경로 소스 인터페이스로 구성하면 **활성** 및 **수동** HA 피어 모두에서 활동이 발생합니다.

STEP 1 | 서비스 경로를 사용자 지정합니다.

1. 디바이스 > 설정 > 서비스 > 전역(다중 가상 시스템 기능이 없는 방화벽에서는 전역 생략)을 선택하고 서비스 기능 섹션에서서비스 경로 구성을 클릭합니다.



2. 사용자 지정을 선택하고 다음 중 하나를 수행하여 서비스 경로를 생성합니다.
   - 사전 정의된 서비스의 경우:
     - **IPv4** 또는 **IPv6**을 선택하고 서비스 경로를 사용자 지정하려는 서비스에 대한 링크를 클릭합니다.

       여러 서비스에 동일한 소스 주소를 쉽게 사용하려면 서비스에 대한 확인란을 선택하고 선택한 경로 설정을 클릭한 후 다음 단계로 진행합니다.
     - 소스 주소 목록을 제한하려면 소스 인터페이스를 선택합니다. 그런 다음 서비스 경로로 소스 주소(해당 인터페이스에서)를 선택합니다. 선택한 인터페이스에 이미 구성된 경우 주소 개체를 소스 주소로 참조할 수도 있습니다. 모든 소스 인터페이스를 선택하면 주소를 선택한 소스 주소 목록에서 모든 인터페이스의 모든 IP 주소를 사용할 수 있습니다. 기본값 사용을 선택하면 패킷 대상 IP 주소가 구성된 대상 IP 주소와 일치하지 않는 한 방화벽이 서비스 경로에 대한 관리 인터페이스를 사용합니다. 이 경우 원본 IP 주소는 대상에 대해 구성된 원본 주소로 설정됩니다. **MGT**를 선택하면 대상 서비스 경로에 관계없이 방화벽이 서비스 경로에 대해 MGT 인터페이스를 사용합니다.

       서비스 경로 소스 주소는 참조된 인터페이스에서 구성 변경 사항을 상속하지 않으며 그 반대의 경우도 마찬가지입니다. 인터페이스 *IP* 주소를 다른 *IP* 주소 또는 주소 객체로 수정하면 해당 서비스 경로 소스 주소가 업데이트되지 않습니다. 이로 인해 커밋이 실패할 수 있으며 서비스 경로를 유효한 소스 주소값으로 업데이트해야 합니다.
     - 확인을 클릭하여 설정을 저장합니다.
     - 서비스에 대해 IPv4 및 IPv6 주소를 모두 지정하려면 이 단계를 반복합니다.

- 대상 서비스 경로의 경우:
    - 대상을 선택하고 대상 IP 주소를 추가합니다. 이 경우 구성된 대상 주소와 일치하는 대상 IP 주소로 패킷이 도착하면, 패킷의 소스 IP 주소는 다음 단계에서 구성된 소스 주소로 설정됩니다.
    - 소스 주소 목록을 제한하려면 소스 인터페이스를 선택합니다. 그런 다음 서비스 경로로 소스 주소(해당 인터페이스에서)를 선택합니다. 모든 소스 인터페이스를 선택하면 주소를 선택한 소스 주소 목록에서 모든 인터페이스의 모든 IP 주소를 사용할 수 있습니다. **MGT**를 선택하면 방화벽이 서비스 경로에 대해 MGT 인터페이스를 사용합니다.
    - 확인을 클릭하여 설정을 저장합니다.

3. 사용자 지정하려는 각 서비스 경로에 대해 이전 단계를 반복합니다.
4. 확인을 클릭하여 서비스 경로 구성을 저장합니다.

STEP 2 | 커밋합니다.

정적 경로

정적 경로는 일반적으로 동적 라우팅 프로토콜과 함께 사용됩니다. 동적 라우팅 프로토콜이 도달할 수 없는 위치에 대해 정적 경로를 구성할 수 있습니다. 정적 경로를 사용하려면 방화벽이 경로 테이블에 동적 경로를 입력하는 대신 네트워크의 모든 라우터에서 수동 구성이 필요합니다. 정적 경로를 사용하려면 모든 라우터에서 해당 구성이 필요하지만 소규모 네트워크에서는 라우팅 프로토콜을 구성하는 것보다 바람직할 수 있습니다.

- 정적 경로 개요
- 경로 모니터링 기반 정적 경로 제거
- 정적 경로 구성
- 정적 경로에 대한 경로 모니터링 구성

정적 경로 개요

IP 라우팅 프로토콜에 참여하지 않고 특정 레이어 3 트래픽이 특정 경로를 선택하도록 결정한 경우 정적 경로 구성 IPv4 및 IPv6 경로를 사용할 수 있습니다.

기본 경로는 특정 정적 경로입니다. 동적 라우팅을 사용하여 가상 라우터의 기본 경로를 가져오지 않는 경우 정적 기본 경로를 구성해야 합니다. 가상 라우터에 들어오는 패킷이 있고 경로 테이블에서 패킷의 대상에 일치하지 않는 경우 가상 라우터는 패킷을 디폴트 경로로 보냅니다. 디폴트 IPv4 경로는 0.0.0.0/0입니다. 디폴트 IPv6 경로는 ::/0입니다. IPv4 및 IPv6 디폴트 경로를 모두 구성할 수 있습니다.

정적 경로 자체는 네트워크 환경의 변경 내용을 변경하거나 조정하지 않으므로 일반적으로 경로를 따라 정적으로 정의된 엔드포인트에 오류가 발생하면 트래픽이 다시 라우팅되지 않습니다. 그러나 문제가 발생할 경우 정적 경로를 백업할 수 있는 옵션이 있습니다.

- 방화벽과 BFD 피어 간의 BFD 세션이 실패하면 방화벽이 RIB 및 FIB 테이블에서 실패한 정적 경로를 제거하고 우선 순위가 낮은 대체 경로를 사용할 수 있도록 양방향 전달 감지(BFD) 프로파일을 사용하여 정적 경로를 구성할 수 있습니다.
- 방화벽이 다른 경로를 사용할 수 있도록 정적 경로에 대한 경로 모니터링 구성할 수 있습니다.

기본적으로 정적 경로의 관리 거리가 10입니다. 방화벽에 동일한 대상으로 두 개 이상의 경로가 있는 경우 관리 거리가 가장 낮은 경로를 사용합니다. 정적 경로의 관리 거리를 동적 경로보다 높은 값으로 늘이면 동적 경로를 사용할 수 없는 경우 정적 경로를 백업 경로로 사용할 수 있습니다.

정적 경로를 구성하는 동안 방화벽이 유니캐스트 또는 멀티캐스트 경로 테이블(RIB)에 IPv4 정적 경로를 설치할지 또는 두 테이블에 설치할지 또는 경로를 전혀 설치하지 않는지 지정할 수 있습니다. 예를 들어 멀티캐스트 경로 테이블에만 IPv4 정적 경로를 설치할 수 있습니다. 이 옵션을 사용하면 트래픽이 소요되는 경로를 더 제어할 수 있습니다. 방화벽이 유니캐스트 경로 테이블에 IPv6 정적 경로를 설치하는지 여부를 지정할 수 있습니다.

경로 모니터링 기반 정적 경로 제거

정적 경로에 대한 경로 모니터링을 구성할 때 방화벽은 경로 모니터링을 사용하여 하나 이상의 모니터링 대상으로 가는 경로가 다운된 시기를 감지합니다. 그런 다음 방화벽은 대체 경로를 사용하여 트래픽의 경로를 변경할 수 있습니다. 방화벽은 HA 또는 정책 기반 전달(PBF)에 대한 경로 모니터링과 마찬가지로 정적 경로에 대한 경로 모니터링을 다음과 같이 사용합니다.

- 방화벽은 ICMP ping 메시지(하트비트 메시지)를 강력하며 정적 경로의 가용성을 반영한다고 판단되는 하나 이상의 모니터링 대상으로 전송합니다.
- 모니터링 대상에 대한 ping이 실패하면 방화벽은 정적 경로를 고려하여 RIB(라우팅 정보 베이스) 및 정보 전달 자료(FIB)에서 제거합니다. RIB는 방화벽이 구성된 정적 경로의 테이블이며 라우팅 프로토콜에서 학습한 동적 경로입니다. FIB는 방화벽이 패킷 전달에 사용하는 경로의 전달 테이블입니다. 방화벽은 RIB에서 동일한 대상에 대한 대체 정적 경로(가장 낮은 메트릭이 있는 경로를 기반으로 함)를 선택하고 FIB에 배치합니다.
- 방화벽은 실패한 경로를 계속 모니터링합니다. 경로가 다시 나타나고(임의 또는 모든 실패 조건에 기반해) 경로 모니터가 Up 상태로 돌아오면 선제 보류 타이머가 시작됩니다. 경로 모니터는 홀드 타이머의 기간 동안 유지되어야 합니다. 그런 다음 방화벽은 정적 경로를 안정적으로 간주하고 RIB로 다시 연결합니다. 그런 다음 방화벽은 경로 메트릭을 동일한 대상과 비교하여 FIB에서 가는 경로를 결정합니다.

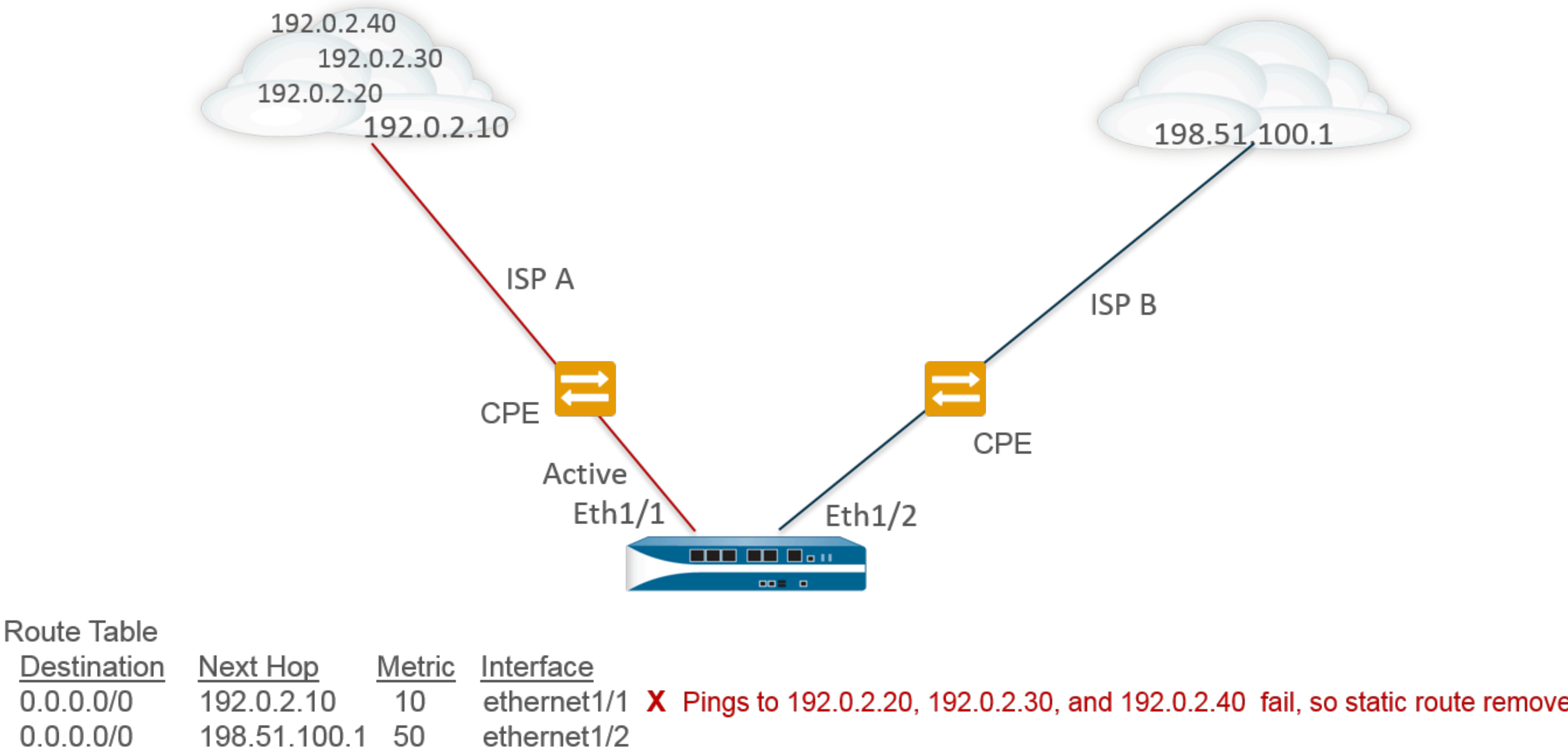
경로 모니터링은 다음을 위해 트래픽을 자동으로 삭제하지 않도록 하는 바람직한 메커니즘입니다.

- 정적 또는 기본 경로입니다.
- 라우팅 프로토콜에 재배포된 정적 또는 기본 경로입니다.
- 한 피어가 BFD를 지원하지 않는 정적 또는 기본 경로입니다. (모범 사례는 단일 인터페이스에서 BFD 및 경로 모니터링을 모두 활성화하지 않는 것입니다.)
- RIB, FIB 또는 재배포 정책에서 실패한 정적 경로를 제거하지 않는 PBF 경로 모니터링을 사용하는 대신 정적 또는 기본 경로를 사용합니다.

경로 모니터링은 가상 라우터 간에 구성된 정적 경로에는 적용되지 않습니다.

다음 그림에서 방화벽은 두 개의 ISP에 연결되어 인터넷에 대한 경로 중복성을 위해 연결됩니다. 기본 디폴트 경로 0.0.0.0(메트릭 10)은 다음 홉 192.0.2.10을 사용합니다. 보조 기본 경로 0.0.0.0(메트릭 50)은 다음 홉 198.51.100.1을 사용합니다. ISP A의 고객 구내 장비(CPE)는 인터넷 연결이 중단된 후에도 기본 물리적 링크를 활성 상태로 유지합니다. 링크가 인위적으로 활성화되어 있으면 방화벽에서 링크가 다운되어 있고 실패한 경로를 RIB의 보조 경로로 교체해야 한다는 것을 감지할 수 없습니다.

실패한 링크로의 트래픽을 자동으로 삭제하지 않으려면 경로 모니터링을 192.0.2.20, 192.0.2.30 및 192.0.2.40 및 이러한 대상으로 향하는 모든 경로가(또는 어떤) 실패하는 경우, 방화벽은 다음 홉 192.0.2.10으로가는 경로도 다운되었다고 추정해, RIB에서 정적 경로 0.0.0.0(Next Hop 192.0.2.10을 사용함)을 제거하고 동일한 대상 0.0.0.0으로 가는 보조 경로로 대체하며(다음 홉 198.51.100.1을 사용함), 또한 인터넷에 액세스할 수 있습니다.



정적 경로를 구성할 때 필요한 필드 중 하나는 해당 대상을 향한 다음 홉입니다. 구성한 다음 홉 유형은 다음과 같이 경로 모니터링 중에 방화벽이 사용하는 작업을 결정합니다.

정적 경로의 다음 홉 유형이 다음과 같은 경우:	ICMP Ping을 위한 방화벽 작업
IP 주소	방화벽은 정적 경로의 소스 IP 주소와 이그레스 인터페이스를 ICMP ping에서 소스 주소와 이그레스 인터페이스로 사용합니다. 모니터링 대상의 구성된 대상 IP 주소를 ping의 대상 주소로 사용합니다. 정적 경로의 다음 홉 주소를 ping의 다음 홉 주소로 사용합니다.
다음 **VR**	방화벽은 정적 경로의 소스 IP 주소를 ICMP ping의 소스 주소로 사용합니다. 송신 인터페이스는 다음 홉의 가상 라우터의 조회 결과를 기반으로 합니다. 모니터링 대상의 구성된 대상 IP 주소는 ping의 대상 주소입니다.
없음	방화벽은 경로 모니터의 대상 IP 주소를 다음 홉으로 사용하고 ICMP ping을 정적 경로에 지정된 인터페이스로 보냅니다.

정적 또는 기본 경로에 대한 경로 모니터링이 실패하면 방화벽은 중요한 이벤트(경로 모니터 실패)로 기록됩니다. 정적 또는 기본 경로가 복구되면 방화벽은 또 다른 중요한 이벤트(경로 모니터 복구)로 로그인합니다.

방화벽은 활성/수동 HA 배포를 위해 경로 모니터링 구성을 동기화하지만 방화벽은 트래픽을 적극적으로 처리하지 않기 때문에 수동 HA 피어에서 ICMP ping 패킷을 생성합니다. 방화벽은 활성/활성 HA 배포를 위해 경로 모니터링 구성을 동기화하지 않습니다.

정적 경로 구성

방화벽에서 가상 라우터에 대한 정적 경로 또는 기본 경로를 구성하려면 다음 작업을 수행합니다.

STEP 1 | 정적 경로를 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 구성하려는 가상 라우터를 선택합니다(예: 기본).
2. 정적 경로 탭을 선택합니다.
3. 구성하려는 정적 경로 유형에 따라 **IPv4** 또는 **IPv6**를 선택합니다.
4. 경로에 대한 이름(최대 63자)을 추가합니다. 이름은 영숫자 문자로 시작해야 하며 영숫자 문자, 밑줄(_), 하이픈(-), 점(.) 및 공백의 조합을 포함할 수 있습니다.
5. 대상에 경로 및 넷마스크를 입력합니다(예: IPv4 주소의 경우 192.168.2.2/24, IPv6 주소의 경우 2001:db8:123:1::1/64). 기본 경로를 생성하는 경우 기본 경로(IPv4 주소의 경우 0.0.0.0/0 또는 IPv6 주소의 경우 ::/0)를 입력합니다. 또는 IP 넷마스크 유형의 주소 개체를 만들 수 있습니다.
6. (선택 사항) 인터페이스의 경우 패킷이 다음 홉으로 이동하는 데 사용할 나가는 인터페이스를 지정합니다. 이 경로의 다음 홉에 대한 경로 테이블의 인터페이스 대신 방화벽이 사용하는 인터페이스를 더 엄격하게 제어하려면 이 옵션을 사용합니다.
7. 다음 홉에서 다음 중 하나를 선택합니다.
   - **IP** 주소 - 특정 다음 홉으로 라우팅하려는 경우 IP 주소(예: 192.168.56.1 또는 2001:db8:49e:1::1)를 입력합니다. IPv6 다음 홉 주소를 사용하려면 인터페이스에서 **IPv6**을 활성화(레이어 3 인터페이스 구성할 때)해야 합니다. 기본 경로를 생성하는 경우 다음 홉에 대해 **IP** 주소를 선택하고 인터넷 게이트웨이의 IP 주소를 입력해야 합니다(예: 192.168.56.1 또는 2001:db8:49e:1::1). 또는 IP 넷마스크 유형의 주소 개체를 만들 수 있습니다. 주소 개체에는 IPv4의 경우 /32 또는 IPv6의 경우 /128의 넷마스크가 있어야 합니다.
   - 다음 **VR** - 방화벽의 다른 가상 라우터에 내부적으로 라우팅하려면 이 옵션을 선택한 다음 가상 라우터를 선택합니다.
   - **FQDN** - FQDN을 입력하거나 FQDN을 사용하는 주소 개체를 선택하거나 FQDN 유형의 새 주소 개체를 만듭니다.

     FQDN을 정적 경로 다음 홉으로 사용하는 경우 해당 FQDN은 정적 경로에 대해 구성한 인터페이스와 동일한 서브넷에 속하는 IP 주소로 확인되어야 합니다. 그렇지 않으면 방화벽이 확인을 거부하고 FQDN이 확인되지 않은 상태로 유지됩니다.

     방화벽은 FQDN의 DNS 확인에서 하나의 IP 주소(각 IPv4 또는 IPv6 제품군 유형에서)만 사용합니다. DNS 확인이 둘 이상의 주소를 반환하는 경우 방화벽은 다음 홉에 대해 구성된 IP 제품군 유형(IPv4 또는 IPv6)과 일치하는 기본 IP 주소를 사용합니다. 기본 IP 주소는 DNS 서버가 초기 응답에서 반환하는 첫 번째 주소입니다. 방화벽은 주소가 순서에 관계없이 후속 응답에 나타나는 한 이 주소를 선호하는 대로 유지합니다.
   - 폐기 - 이 대상으로 지정된 패킷을 삭제하려면 선택합니다.

- 없음 - 경로에 대한 다음 홉이 없는 경우 선택합니다. 예를 들어, 지점간 연결은 패킷이 이동하는 방법이 한가지 뿐이므로 다음 홉이 필요하지 않습니다.

8. 이 가상 라우터의 정적 경로에 대해 설정된 기본 관리 거리를 재정의할 경로의 관리 거리를 입력합니다(범위는 10~240, 기본값은 10임).
9. 경로에 대한 메트릭 을 입력합니다(범위는 1~65,535).

STEP 2 | 경로를 설치할 위치를 선택합니다.

방화벽이 정적 경로를 설치할 경로 테이블(RIB)을 선택합니다.

- 유니캐스트 - 유니캐스트 라우팅 테이블에 경로를 설치합니다. 유니캐스트 트래픽에만 경로를 사용하려면 이 옵션을 선택합니다.
- 멀티캐스트 - 멀티캐스트 경로 테이블에 경로를 설치합니다(IPv4 경로에만 사용 가능). 멀티캐스트 트래픽에만 경로를 사용하려면 이 옵션을 선택합니다.
- 둘 다 - 유니캐스트 및 멀티캐스트 라우팅 테이블에 경로를 설치합니다(IPv4 경로에만 사용 가능). 유니캐스트 또는 멀티캐스트 트래픽이 경로를 사용하도록 하려면 이 옵션을 선택합니다.
- 설치 안 함 - 두 경로 테이블에 경로를 설치하지 마십시오.

STEP 3 | (선택 사항) 방화벽 모델이 BFD을(를) 지원하는 경우 **BFD** 프로파일을 정적 경로에 적용하여 정적 경로가 실패할 경우 방화벽이 RIB 및 FIB에서 경로를 제거하고 대체 경로를 사용하도록 할 수 있습니다. 기본값은 없음입니다.

STEP 4 | 확인을 두 번 클릭합니다.

STEP 5 | 구성을 커밋합니다.

정적 경로에 대한 경로 모니터링 구성

다음 절차를 사용하여 경로 모니터링 기반 정적 경로 제거를 구성합니다.

STEP 1 | 정적 경로에 대한 경로 모니터링을 활성화합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. 정적 경로를 선택하고 **IPv4** 또는 **IPv6**을 선택한 다음 모니터링할 정적 경로를 선택합니다. 최대 128개의 정적 경로를 모니터링할 수 있습니다.
3. 경로 모니터링을 선택하여 경로에 대한 경로 모니터링을 활성화합니다.

STEP 2 | 정적 경로에 대해 모니터링되는 대상을 구성합니다.

1. 이름으로 모니터링되는 대상을 추가합니다. 정적 경로당 모니터링되는 대상을 최대 8개까지 추가할 수 있습니다.
2. 사용을 선택하여 대상을 모니터링합니다.
3. 소스 **IP**의 경우 모니터링되는 대상에 대한 ICMP ping에서 방화벽이 사용하는 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 선택하고 이더넷 인터페이스 행에서 동적 **DHCP** 클라이언트를 클릭합니다. IP 주소는 동적 IP 인터페이스 상태 창에 표시됩니다.
4. 대상 **IP**에 방화벽이 경로를 모니터링할 IP 주소 또는 주소 개체를 입력합니다. 모니터링되는 대상과 정적 경로 대상은 동일한 주소 패밀리(IPv4 또는 IPv6)를 사용해야 합니다.

   대상 ***IP*** 주소는 신뢰할 수 있는 엔드포인트에 속해야 합니다**.** 즉**,** 불안정하거나 신뢰할 수 없는 디바이스를 기반으로 경로 모니터링을 수행하지 않는 것이 좋습니다**.**
5. (선택 사항) ICMP **ping** 간격**(**초**)**을 초 단위로 지정하여 방화벽이 경로를 모니터링하는 빈도를 결정합니다(범위는 1-60, 기본값은 3).
6. (선택 사항) 방화벽이 정적 경로 다운을 고려하여 RIB 및 FIB에서 제거하기 전에 대상에서 반환되지 않는 패킷의 ICMP **ping** 수를 지정합니다(범위는 3-10, 기본값은 5).
7. 확인을 클릭합니다.

STEP 3 | 정적 경로에 대한 경로 모니터링이 모니터링되는 대상 중 하나 또는 전체를 기반으로 하는지 여부를 결정하고 선점 대기 시간을 설정합니다.

1. 방화벽이 RIB 및 FIB에서 정적 경로를 제거하고 다음으로 낮은 메트릭이 있는 정적 경로를 추가하려면 ICMP에서 정적 경로에 대해 모니터링되는 대상 중 임의 또는 모두에 연결할 수 없는지 여부에 관계없이 실패 조건을 선택합니다.FIB와 동일한 목적지로 이동합니다.

   예를 들어 대상이 유지 관리를 위해 단순히 오프라인일 때 단일 모니터링 대상이 경로 실패를 알리는 가능성을 방지하려면 모두를 선택합니다**.**

2. (선택 사항) 방화벽이 정적 경로를 RIB에 다시 설치하기 전에 다운된 경로 모니터가 작동 상태로 유지되어야 하는 시간(분)인 선제 유지 시간**(**분**)**을 지정합니다. 경로 모니터는 정적 경로에 대해 모니터링되는 모든 대상을 평가하고 일부 또는 모두 실패 조건에 따라 나타납니다. 일시 중단 시간 동안 링크가 다운되거나 펄럭이는 경우 링크가 다시 작동할 때 경로 모니터가 다시 작동할 수 있습니다. 경로 모니터가 작동 상태로 돌아가면 타이머가 다시 시작됩니다.

   Preemptive Hold Time이 0이면 방화벽이 경로 모니터가 표시되는 즉시 RIB로 경로를 다시 설치합니다. 범위는 0-1,440입니다. 기본값은 2입니다.

3. 확인을 클릭합니다.

STEP 4 | 커밋합니다.

커밋을 클릭합니다.

STEP 5 | 정적 경로에 대한 경로 모니터링을 확인합니다.

1. 네트워크 > 가상 라우터를 선택하고 관심 있는 가상 라우터 행에서 추가 런타임 통계를 선택합니다.
2. 라우팅 탭에서 정적 경로 모니터링을 선택합니다.
3. 정적 경로(대상)의 경우 경로 모니터링이 사용 또는 사용 안 함으로 설정되어 있는지 확인합니다. 상태 열은 경로가 작동, 작동 중지 또는 사용 안 함인지 여부를 나타냅니다. 정적 경로의 플래그는 다음과 같습니다. A - 활성, S - 정적, E - ECMP.
4. 경로 모니터링의 최신 상태(상태 확인) 를 보려면 주기적으로 새로 고침을 선택합니다.
5. 경로의 상태를 마우스오버하면 모니터링되는 IP 주소와 해당 경로에 대해 모니터링되는 대상으로 전송된 ping 결과를 볼 수 있습니다. 예를 들어, 3/5는 3초의 ping 간격과 5번의 연속 누락된 ping(방화벽이 지난 15초 동안 ping을 수신하지 않음)의 ping 수가 경로 모니터링에서 링크 오류를 감지했음을 의미합니다. 임의 또는 모두 실패 조건에 따라 경로 모니터링이 실패 상태이고 방화벽이 15초 후에 ping을 수신하면 경로가 작동 중인 것으로 간주되어 선제 대기 시간이 시작됩니다.

   상태는 마지막으로 모니터링된 ping 결과(성공 또는 실패)를 나타냅니다. 실패는 일련의 ping 패킷(ping 간격에 ping 수를 곱한 값)이 성공하지 못했음을 나타냅니다. 단일 ping 패킷 실패는 실패한 ping 상태를 반영하지 않습니다.

STEP 6 | RIB 및 FIB를 보고 정적 경로가 제거되었는지 확인합니다.

1. 네트워크 > 가상 라우터를 선택하고 관심 있는 가상 라우터 행에서 추가 런타임 통계를 선택합니다.
2. 라우팅 탭에서 라우팅 테이블(RIB)을 선택한 다음 전달 테이블(FIB)을 선택하여 각각을 봅니다.
3. 적절한 라우팅 테이블을 보려면 유니캐스트 또는 멀티캐스트를 선택합니다.
4. 디스플레이 주소 패밀리에 대해 **IPv4** 및 **IPv6**, **IPv4**만 또는 **IPv6** 전용을 선택합니다.
5. (선택 사항) 필터 필드에 검색 중인 경로를 입력하고 화살표를 선택하거나 스크롤 막대를 사용하여 경로 페이지를 이동합니다.
6. 경로가 제거되었는지 또는 존재하는지 확인합니다.
7. 경로 모니터링의 최신 상태(상태 확인) 를 보려면 주기적으로 새로 고침을 선택합니다.

경로 모니터링에 대해 기록된 이벤트를 보려면 모니터 **>** 로그 **>** 시스템을 선택합니다**.** 정적 경로 대상에 대한 경로 모니터링이 실패하여 경로가 제거되었음을 나타내는 ***path-monitor-failure***에 대한 항목을 봅니다**.** 경로가 복원되었으므로 복구된 정적 경로 대상에 대한 경로 모니터링을 나타내는 ***path-monitor-recovery***에 대한 항목을 봅니다**.**

RIP

RIP가 네트워크에 적합한 라우팅 프로토콜인지 고려하고 적합하다면 RIP를 구성하십시오.

- RIP 개요
- RIP 구성

RIP 개요

RIP(Routing Information Protocol)는 소규모 IP 네트워크용으로 설계된 IGP(내부 게이트웨이 프로토콜)입니다. RIP는 경로를 결정하기 위해 홉 수에 의존합니다. 최상의 경로는 홉 수가 가장 적습니다. RIP는 UDP를 기반으로 하며 경로 업데이트에 포트 520을 사용합니다. 경로를 최대 15개 홉으로 제한함으로써 프로토콜은 라우팅 루프의 개발을 방지하는 데 도움이 되지만 지원되는 네트워크 크기도 제한합니다. RIP를 구성하기 전에 15개 이상의 홉이 필요한 경우 트래픽이 라우팅되지 않는다는 점을 고려하십시오. RIP는 또한 OSPF 및 기타 라우팅 프로토콜보다 수렴하는 데 더 오래 걸릴 수 있습니다.

방화벽은 RIP v2를 지원합니다.

RIP 구성

다음 절차를 수행하여 RIP을 구성합니다.

STEP 1 | 일반 가상 라우터 설정을 구성합니다.

STEP 2 | 일반 RIP 구성 설정을 구성합니다.

1. 가상 라우터(네트워크 > 가상 라우터)를 선택하고 가상 라우터에 대해 **RIP**를 선택합니다.
2. 사용을 선택하여 RIP 프로토콜을 사용하도록 설정합니다.
3. RIP를 통해 기본 경로를 학습하지 않으려면 기본 경로 거부를 선택합니다 . 권장되는 기본 설정입니다.

   RIP를 통한 기본 경로 재배포를 허용하려면 기본 경로 거부를 선택 취소합니다.

STEP 3 | RIP에 대한 인터페이스를 구성합니다.

1. 인터페이스 탭의 인터페이스 구성 섹션에서 인터페이스를 선택합니다.
2. 이미 정의된 인터페이스를 선택합니다.
3. 활성화를 선택합니다.
4. 기본 경로 광고를 선택하여 지정된 메트릭 값을 가진 RIP 피어에 대한 기본 경로를 알립니다.
5. (선택 사항) 인증 프로파일 목록에서 프로파일을 선택합니다.
6. 모드 목록에서 일반, 수동 또는 전송 전용을 선택합니다.
7. (선택 사항) 가상 라우터에 대해 전역적으로 RIP에 대해 BFD을(를) 활성화하려면 **BFD** 프로파일을 선택합니다.
8. 확인을 클릭합니다.

STEP 4 | RIP 타이머를 구성합니다.

1. 타이머 탭에서 간격 초**(**초**)**에 대한 값을 입력합니다. 이 설정은 다음 RIP 타이머 간격의 길이를 초 단위로 정의합니다(범위는 1~60, 기본값은 1임).
2. 업데이트 간격을 지정하여 경로 업데이트 알림 사이의 간격 수를 정의합니다(범위는 1~3,600, 기본값은 30임).
3. 만료 간격을 지정하여 경로가 만료됨으로 마지막으로 업데이트된 시간 사이의 간격 수를 정의합니다(범위는 1~3600, 기본값은 120임).
4. 삭제 간격을 지정하여 경로가 만료되는 시간부터 삭제까지의 간격 수를 정의합니다(범위는 1~3,600, 기본값은 180임).

STEP 5 | (선택 사항) 인증 프로파일을 구성합니다.

기본적으로 방화벽은 RIP 이웃 간의 교환에 RIP 인증을 사용하지 않습니다. 선택적으로, 단순 암호 또는 MD5 인증 중 하나를 사용하여 RIP 이웃 간에 RIP 인증을 구성할 수 있습니다. MD5 인증을 권장합니다. 단순한 암호보다 더 안전합니다.

단순 암호 **RIP** 인증

1. 인증 프로파일을 선택하고 인증 프로파일의 이름을 추가하여 RIP 메시지를 인증합니다.
2. 암호 유형으로 단순 암호를 선택합니다.
3. 간단한 암호를 입력한 후 확인합니다.

MD5 RIP 인증

1. 인증 프로파일을 선택하고 인증 프로파일의 이름을 추가하여 RIP 메시지를 인증합니다.
2. **MD5**를 암호 유형으로 선택합니다.
3. 다음을 포함하여 하나 이상의 암호 항목을 추가합니다.
   - 키 ID(범위는 0 ~ 255)
   - 키
4. (선택 사항) 기본 설정 상태를 선택합니다.
5. 확인을 클릭하여 보내는 메시지를 인증하는 데 사용할 키를 지정합니다.
6. 가상 라우터 - RIP 인증 프로파일 대화 상자에서 확인을 다시 클릭합니다.

STEP 6 | 변경 사항을 커밋합니다.

OSPF

OSPF(Open Shortest Path First)는 대규모 엔터프라이즈 네트워크에서 네트워크 경로를 동적으로 관리하는 데 가장 자주 사용되는 내부 게이트웨이 프로토콜(IGP)입니다. 다른 라우터에서 정보를 얻고 LSA(Link State Advertisements)를 통해 다른 라우터로 경로를 알림으로써 경로를 동적으로 결정합니다. LSA에서 수집된 정보는 네트워크의 토폴로지 맵을 구성하는 데 사용됩니다. 이 토폴로지 맵은 네트워크의 라우터 간에 공유되며 사용 가능한 경로로 IP 라우팅 테이블을 채우는 데 사용됩니다.

네트워크 토폴로지의 변경 사항은 동적으로 감지되고 몇 초 안에 새 토폴로지 맵을 생성하는 데 사용됩니다. 최단 경로 트리는 각 경로에 대해 계산됩니다. 각 라우팅 인터페이스와 관련된 메트릭은 최적의 경로를 계산하는 데 사용됩니다. 여기에는 거리, 네트워크 처리량, 링크 가용성 등이 포함될 수 있습니다. 또한 이러한 메트릭을 정적으로 구성하여 OSPF 토폴로지 맵의 결과를 지시할 수 있습니다.

OSPF의 Palo Alto Networks® 구현은 다음 RFC를 완벽하게 지원합니다.

- RFC 2328(IPv4용)
- RFC 5340(IPv6용)

다음 항목에서는 OSPF 및 방화벽에서 OSPF를 구성하는 절차에 대한 자세한 정보를 제공합니다.

- OSPF 컨셉
- OSPF 구성
- OSPFv3 구성
- OSPF 정상 재시작 구성
- OSPF 작업 확인

OSPF 컨셉

OSPF는 다른 라우터에서 정보를 얻고 LSA(Link State Advertisements)를 통해 다른 라우터로 경로를 알림으로써 경로를 동적으로 결정합니다. 라우터는 라우터와 대상 간의 링크에 대한 정보를 유지하고 매우 효율적인 라우팅 결정을 내릴 수 있습니다. 각각의 라우터 인터페이스에 비용을 할당하고, 발생하는 모든 아웃바운드 라우터 인터페이스와 LSA를 수신하는 인터페이스를 합산하여 가장 비용이 적게 드는 경로를 가장 좋은 경로로 결정합니다.

계층적 기술은 보급해야 하는 경로 수와 관련 LSA를 제한하는 데 사용됩니다. OSPF는 상당한 양의 경로 정보를 동적으로 처리하기 때문에 RIP보다 프로세서 및 메모리 요구 사항이 더 많습니다.

다음 항목에서는 OSPF 네트워크에 참여하도록 방화벽을 구성하기 위해 이해해야 하는 OSPF 개념을 소개합니다.

- OSPFv3
- OSPF 이웃
- OSPF 영역
- OSPF 라우터 유형

OSPFv3

OSPFv3은 IPv6 네트워크 내에서 OSPF 라우팅 프로토콜을 지원합니다. 따라서 IPv6 주소 및 접두사에 대한 지원을 제공합니다. 약간의 변경 사항이 있지만 OSPFv2(IPv4용)의 구조와 기능 대부분을 유지합니다. 다음은 OSPFv3에 대한 몇 가지 추가 및 변경 사항입니다.

- 링크당 여러 인스턴스 지원 - OSPFv3을 사용하면 단일 링크를 통해 OSPF 프로토콜의 여러 인스턴스를 실행할 수 있습니다. 이것은 OSPFv3 인스턴스 ID 번호를 할당하여 수행됩니다. 인스턴스 ID에 할당된 인터페이스는 다른 ID를 포함하는 패킷을 삭제합니다.
- 링크당 프로토콜 처리 - OSPFv3은 OSPFv2에서와 같이 IP 서브넷 대신 링크별로 작동합니다.
- 주소 지정 변경 - 링크 상태 업데이트 패킷 내의 LSA 페이로드를 제외하고 IPv6 주소는 OSPFv3 패킷에 없습니다. 인접 라우터는 라우터 ID로 식별됩니다.
- 인증 변경 - OSPFv3에는 인증 기능이 포함되어 있지 않습니다. 방화벽에서 OSPFv3을 구성하려면 ESP(Encapsulating Security Payload) 또는 IPv6 AH(인증 헤더)를 지정하는 인증 프로파일이 필요합니다. RFC 4552에 지정된 키 다시 지정 절차는 이 릴리스에서 지원되지 않습니다.
- 링크당 여러 인스턴스 지원 - 각 인스턴스는 OSPFv3 패킷 헤더에 포함된 인스턴스 ID에 해당합니다.
- 새로운 **LSA** 유형 - OSPFv3는 두 가지 새로운 LSA 유형을 지원합니다. LSA와 Intra Area Prefix LSA를 연결합니다.

모든 추가 변경 사항은 RFC 5340에 자세히 설명되어 있습니다.

OSPF 이웃

공통 네트워크로 연결되고 관계를 형성하는 동일한 OSPF 영역에 있는 두 개의 OSPF 지원 라우터는 OSPF 인접 라우터입니다. 이러한 라우터 간의 연결은 공통 브로드캐스트 도메인을 통하거나 지점 간 연결을 통해 이루어질 수 있습니다. 이 연결은 hello OSPF 프로토콜 패킷의 교환을 통해 이루어집니다. 이러한 인접 관계는 라우터 간에 라우팅 업데이트를 교환하는 데 사용됩니다.

OSPF 영역

OSPF는 단일 자율 시스템(AS) 내에서 작동합니다. 그러나 이 단일 AS 내의 네트워크는 여러 영역으로 나눌 수 있습니다. 기본적으로 영역 0이 생성됩니다. 영역 0은 단독으로 작동하거나 더 많은 영역에 대해 OSPF 백본으로 작동할 수 있습니다. 각 OSPF 영역은 대부분의 경우 IP4 주소와 동일한 점분리 10진수 표기법으로 작성되는 32비트 식별자를 사용하여 이름이 지정됩니다. 예를 들어 영역 0은 일반적으로 0.0.0.0으로 작성됩니다.

영역의 토폴로지는 자체 링크 상태 데이터베이스에서 유지 관리되고 다른 영역에서 숨겨져 OSPF에 필요한 트래픽 라우팅의 양을 줄입니다. 그런 다음 토폴로지는 연결 라우터에 의해 영역 간에 요약된 형태로 공유됩니다.

OSPF 영역 유형	설명
백본 영역	백본 영역(Area 0)은 OSPF 네트워크의 핵심입니다. 다른 모든 영역은 여기에 연결되어 있으며 영역 간의 모든 트래픽은 해당 영역을 통과해야 합니다. 영역 간의 모든 라우팅은 백본 영역을 통해 분산됩니다. 다른 모든 OSPF 영역은 백본 영역에 연결해야 하지만 이 연결은 직접 연결될 필요가 없으며 가상 링크를 통해 만들 수 있습니다.
일반 OSPF 영역	일반 OSPF 영역에는 제한이 없습니다. 이 지역은 모든 유형의 경로를 수행할 수 있습니다.
스텁 OSPF 영역	스텁 영역은 다른 자율 시스템에서 경로를 수신하지 않습니다. 스텁 영역에서 라우팅은 기본 경로를 통해 백본 영역으로 수행됩니다.
NSSA 영역	NSSA(Not So Stubby Area)는 일부 제한된 예외를 제외하고 외부 경로를 가져올 수 있는 일종의 스텁 영역입니다.

OSPF 라우터 유형

OSPF 영역 내에서 라우터는 다음 범주로 나뉩니다.

- 내부 라우터 - 동일한 영역에 있는 디바이스와만 OSPF 인접 관계가 있는 라우터입니다.
- **ABR(Area Border Router)** - 여러 OSPF 영역에 있는 디바이스와 OSPF 인접 관계가 있는 라우터입니다. ABR은 연결된 영역에서 토폴로지 정보를 수집하여 백본 영역에 배포합니다.
- 백본 라우터 - 백본 라우터는 OSPF를 실행하고 OSPF 백본 영역에 연결된 인터페이스가 하나 이상 있는 라우터입니다. ABR은 항상 백본에 연결되어 있으므로 항상 백본 라우터로 분류됩니다.
- **ASBR(Autonomous System Boundary Router)** - ASBR은 둘 이상의 라우팅 프로토콜에 연결하고 이들 사이에서 라우팅 정보를 교환하는 라우터입니다.

OSPF 구성

OSPF 컨셉을(를) 이해한 후 다음 절차를 수행하여 OSPF를 구성합니다.

STEP 1 | 일반 가상 라우터 설정을 구성합니다.

STEP 2 | OSPF를 활성화합니다.

1. **OSPF** 탭을 선택합니다.
2. OSPF 프로토콜을 활성화하려면 활성화를 선택합니다.
3. 라우터 **ID**를 입력합니다.
4. OSPF를 통해 기본 경로를 학습하지 않으려면 기본 경로 거부를 선택합니다. 권장되는 기본 설정입니다.

   OSPF를 통한 기본 경로 재배포를 허용하려면 기본 경로 거부를 선택 취소합니다.

STEP 3 | 영역 구성 - OSPF 프로토콜에 대한 유형입니다.

1. 영역 탭에서*xxxx* 형식으로 영역에 대한 영역 **ID**를 추가합니다. 이것은 각 이웃이 동일한 영역의 일부로 수락해야 하는 식별자입니다.
2. 유형 탭의유형 목록 영역에서 다음 중 하나를 선택합니다.
   - 일반 - 제한이 없습니다. 이 지역은 모든 유형의 경로를 수행할 수 있습니다.
   - **Stub** - 해당 지역의 콘센트가 없습니다. 영역 밖의 대상에 도달하려면 다른 영역으로 연결되는 경계를 통과해야 합니다. 이 옵션을 선택하는 경우 다음을 구성합니다.
     - 요약 수락 - 다른 영역에서 LSA(링크 상태 광고)를 수락합니다. 스텁 영역 ABR(영역 경계 라우터) 인터페이스에서 이 옵션이 비활성화된 경우 OSPF 영역은 TSA(완전히 스텁 영역)로 작동하고 ABR은 요약 LSA를 전파하지 않습니다.
     - 기본 경로 광고 - 기본 경로 LSA는 구성된 범위 1-255에서 구성된 메트릭 값과 함께 스텁 영역에 대한 광고에 포함됩니다.
   - **NSSA**(Not-So-Stubby Area) - 방화벽은 OSPF 경로 이외의 경로를 통해서만 영역을 떠날 수 있습니다. NSSA를 선택하는 경우 스텁에 대해 설명된 대로 요약 수락 및 기본 경로 광고를 선택합니다. 이 옵션을 선택하는 경우 다음을 구성합니다.
     - 유형 - 기본 LSA를 알리려면 **Ext 1** 또는 **Ext 2** 경로 유형을 선택합니다.
     - 확장 범위 - 광고하거나 광고를 억제하려는 외부 경로의 범위를 추가합니다.
3. 확인을 클릭합니다.

STEP 4 | 영역 구성 - OSPF 프로토콜 범위

1. 범위 탭에서 해당 영역의 집계 LSA 대상 주소를 서브넷에 추가합니다.
2. 서브넷과 일치하는 **LSA**를 광고하거나 표시하지 않고 확인을 클릭합니다. 추가 범위를 추가하려면 반복합니다.

STEP 5 | 영역 구성 - OSPF 프로토콜용 인터페이스

1. 인터페이스 탭에서 영역에 포함될 각 인터페이스에 대해 다음 정보를 추가합니다.
   - 인터페이스 - 인터페이스를 선택합니다.
   - 활성화 - 이 옵션을 선택하면 OSPF 인터페이스 설정이 적용됩니다.
   - 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**(지점 간)를 선택합니다. 이웃을 수동으로 정의해야 하는 경우 **p2mp**(point-to-multipoint)를 선택하고 이 인터페이스를 통해 연결할 수 있는 모든 이웃에 대해 이웃 IP 주소를 추가합니다.
   - 메트릭 - 이 인터페이스에 대한 OSPF 메트릭을 입력합니다(범위는 0-65,535, 기본값은 10).
   - 우선 순위 - 이 인터페이스에 대한 OSPF 우선 순위를 입력합니다. 라우터가 지정 라우터(DR) 또는 백업 DR(BDR)로 선택되는 우선 순위입니다(범위는 0-255, 기본값은 1). 0이 구성되면 라우터는 DR 또는 BDR로 선택되지 않습니다.
   - 인증 프로파일 - 이전에 정의된 인증 프로파일을 선택합니다.
   - 타이밍 - 원하는 경우 타이밍 설정을 수정합니다(권장하지 않음). 이러한 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
2. 확인을 클릭합니다.

STEP 6 | 영역 구성 - 가상 링크.

1. 가상 링크 탭에서 백본 영역에 포함될 각 가상 링크에 대해 다음 정보를 추가합니다.
   - 이름 - 가상 링크의 이름을 입력합니다.
   - 활성화 - 가상 링크를 활성화하려면 선택합니다.
   - **Neighbor ID** - 가상 링크 반대편에 있는 라우터(이웃)의 라우터 ID를 입력합니다.
   - 대중 교통 영역 - 가상 링크를 물리적으로 포함하는 대중 교통 영역의 영역 ID를 입력합니다.
   - 타이밍 - 기본 타이밍 설정을 유지하는 것이 좋습니다.
   - 인증 프로파일 - 이전에 정의된 인증 프로파일을 선택합니다.
2. 확인을 클릭하여 가상 링크를 저장합니다.
3. 확인을 클릭하여 영역을 저장합니다.

STEP 7 | (선택 사항) 인증 프로파일을 구성합니다.

기본적으로 방화벽은 OSPF 이웃 간의 교환에 OSPF 인증을 사용하지 않습니다. 선택적으로 간단한 암호나 MD5 인증을 사용하여 OSPF 이웃 간에 OSPF 인증을 구성할 수 있습니다. MD5 인증을 권장합니다. 단순한 암호보다 더 안전합니다.

단순 암호 **OSPF** 인증

1. 인증 프로파일 탭을 선택하고 인증 프로파일의 이름을 추가하여 OSPF 메시지를 인증합니다.
2. 암호 유형으로 단순 암호를 선택합니다.
3. 간단한 암호를 입력한 후 확인합니다.

MD5 OSPF 인증

1. 인증 프로파일 탭을 선택하고 인증 프로파일의 이름을 추가하여 OSPF 메시지를 인증합니다.
2. 암호 유형으로 **MD5**를 선택하고 다음을 포함하여 하나 이상의 암호 항목을 추가합니다.
   - 키-ID(범위: 0-255)
   - 키
   - 보내는 메시지를 인증하는 데 키를 사용하도록 지정하려면 기본 설정 옵션을 선택합니다.
3. 확인을 클릭합니다.

STEP 8 | 고급 OSPF 옵션을 구성합니다.

1. 고급 탭에서 RFC 1583 호환성을 선택하여 **RFC 1583**과의 호환성을 확인합니다.
2. **SPF** 계산 지연**(**초**)** 타이머 값을 지정하여 새 토폴로지 정보 수신과 SPF 계산 수행 사이의 지연 시간(초)을 조정할 수 있습니다. 값이 낮을수록 OSPF 재수렴 속도가 빨라집니다. 방화벽과 피어링하는 라우터는 수렴 시간을 최적화하기 위해 동일한 지연 값을 사용해야 합니다.
3. 동일한 LSA(동일한 라우터, 동일한 유형, 동일한 LSA ID)의 두 인스턴스 전송 사이의 최소 시간인 **LSA** 간격**(**초**)** 타이머 값을 지정하십시오. 이것은 RFC 2328의 MinLSInterval과 동일합니다. 토폴로지 변경이 발생할 때 더 낮은 값을 사용하여 재수렴 시간을 줄일 수 있습니다.
4. 확인을 클릭합니다.

STEP 9 | 변경 사항을 커밋합니다.

OSPFv3 구성

OSPF는 IPv4와 IPv6를 모두 지원합니다. IPv6을 사용하는 경우 OSPFv3을(를) 사용해야 합니다.

STEP 1 | 일반 가상 라우터 설정을 구성합니다.

STEP 2 | 일반 OSPFv3 구성 설정을 구성합니다.

1. **OSPFv3** 탭을 선택합니다.
2. OSPF 프로토콜을 활성화하려면 활성화를 선택합니다.
3. 라우터 **ID**를 입력합니다.
4. OSPFv3를 통해 기본 경로를 배우지 않으려면 기본 경로 거부를 선택합니다. 권장되는 기본 설정입니다.

   OSPFv3을 통한 기본 경로 재배포를 허용하려면 기본 경로 거부를 선택 취소합니다.

STEP 3 | OSPFv3 프로토콜에 대한 인증 프로파일을 구성합니다.

OSPFv3에는 자체 인증 기능이 포함되어 있지 않지만 이웃 간의 통신을 보호하기 위해 전적으로 IPSec에 의존합니다.

인증 프로파일을 구성할 때 ESP(Encapsulating Security Payload)(권장) 또는 IPv6 인증 헤더(AH)를 사용해야 합니다.

ESP OSPFv3 인증

1. 인증 프로파일 탭에서 OSPFv3 메시지를 인증할 인증 프로파일의 이름을 추가합니다.
2. **SPI**(보안 정책 인덱스)(00000000에서 FFFFFFFFF 사이의 16진수 값)를 지정합니다. OSPFv3 인접성의 두 끝에는 일치하는 SPI 값이 있어야 합니다.
3. 프로토콜로 **ESP**를 선택합니다.
4. 암호화 알고리즘을 선택합니다.

   없음 또는 다음 알고리즘 중 하나를 선택할 수 있습니다. **SHA1**, **SHA256**, **SHA384**, **SHA512** 또는 **MD5**를 사용할 수 있습니다.
5. 없음 이외의 암호화 알고리즘을 선택한 경우 키에 값을 입력한 다음 확인합니다.

AH OSPFv3 인증

1. 인증 프로파일 탭에서 OSPFv3 메시지를 인증할 인증 프로파일의 이름을 추가합니다.
2. **SPI**(보안 정책 인덱스)를 지정합니다. SPI는 OSPFv3 인접성의 양쪽 끝 사이에서 일치해야 합니다. SPI 번호는 00000000에서 FFFFFFFF 사이의 16진수 값이어야 합니다.
3. 프로토콜로 **AH**를 선택합니다.
4. 암호화 알고리즘을 선택합니다.

   다음 알고리즘 중 하나를 입력해야 합니다. **SHA1**, **SHA256**, **SHA384**, **SHA512** 또는 **MD5**를 사용할 수 있습니다.
5. 키에 값을 입력한 다음 확인합니다.
6. 확인을 클릭합니다.
7. 가상 라우터 - OSPF 인증 프로파일 대화 상자에서 확인을 다시 클릭합니다.

STEP 4 | 영역 구성 - OSPFv3 프로토콜의 유형입니다.

1. 영역 탭에서 영역 **ID**를 추가합니다. 이것은 각 이웃이 동일한 영역의 일부로 수락해야 하는 식별자입니다.
2. 일반 탭의 영역 유형 목록에서 다음 중 하나를 선택합니다.
   - 일반 - 제한이 없습니다. 이 지역은 모든 유형의 경로를 수행할 수 있습니다.
   - **Stub** - 해당 지역의 콘센트가 없습니다. 영역 밖의 대상에 도달하려면 다른 영역으로 연결되는 경계를 통과해야 합니다. 이 옵션을 선택하는 경우 다음을 구성합니다.
     - 요약 수락 - 다른 영역에서 LSA(링크 상태 광고)를 수락합니다. 스텁 영역 ABR(영역 경계 라우터) 인터페이스에서 이 옵션이 비활성화된 경우 OSPF 영역은 TSA(완전히 스텁 영역)로 작동하고 ABR은 요약 LSA를 전파하지 않습니다.
     - 기본 경로 광고 - 기본 경로 LSA는 구성된 범위 1-255에서 구성된 메트릭 값과 함께 스텁 영역에 대한 광고에 포함됩니다.
   - **NSSA**(Not-So-Stubby Area) - 방화벽은 OSPF 경로 이외의 경로를 통해서만 영역을 떠날 수 있습니다. 선택한 경우 스텁에 대해 설명된 대로 요약 수락 및 기본 경로 광고를 구성합니다. 이 옵션을 선택하는 경우 다음을 구성합니다.
     - 유형 - 기본 LSA를 알리려면 **Ext 1** 또는 **Ext 2** 경로 유형을 선택합니다.
     - 확장 범위 - 광고를 활성화하거나 억제할 외부 경로 범위를 추가합니다.

STEP 5 | OSPFv3 인증 프로파일을 영역 또는 인터페이스에 연결합니다.

영역으로

1. 영역 탭의 테이블에서 기존 영역을 선택합니다.
2. 일반 탭의 인증 목록에서 이전에 정의한 인증 프로파일을 선택합니다.
3. 확인을 클릭합니다.

인터페이스로

1. 영역 탭의 테이블에서 기존 영역을 선택합니다.
2. 인터페이스 탭을 선택하고 인증 프로파일 목록에서 OSPF 인터페이스와 연결할 인증 프로파일을 추가합니다.
3. 확인을 클릭합니다.

STEP 6 | 확인을 다시 클릭하여 영역 설정을 저장합니다.

STEP 7 | (선택 사항) 내보내기 규칙을 구성합니다.

1. 내보내기 규칙 탭에서 기본 경로 재배포 허용을 선택하여 OSPFv3를 통한 기본 경로 재배포를 허용합니다.
2. 추가를 클릭합니다.
3. 이름을 입력합니다. 값은 유효한 IPv6 서브넷 또는 유효한 재배포 프로파일 이름이어야 합니다.
4. 새 경로 유형, **Ext 1** 또는 **Ext 2**를 선택합니다.
5. 일치하는 경로에 대해 새 태그를 지정합니다. 점으로 구분된 10진수 표기법으로 32비트 값을 사용합니다.
6. 새 규칙에 지표를 할당합니다(범위는 1-16,777,215임).
7. 확인을 클릭합니다.

STEP 8 | 고급 OSPFv3 옵션을 구성합니다.

1. 방화벽이 전송 트래픽을 전달하는 데 사용되지 않고 OSPF 토폴로지 배포에 참여하도록 하려면 고급 탭에서 **SPF** 계산을 위한 전송 라우팅 비활성화를 선택합니다.
2. **SPF** 계산 지연**(**초**)** 타이머 값을 지정하여 새 토폴로지 정보 수신과 SPF 계산 수행 사이의 지연 시간(초)을 조정할 수 있습니다. 값이 낮을수록 OSPF 재수렴 속도가 빨라집니다. 방화벽과 피어링하는 라우터는 수렴 시간을 최적화하기 위해 동일한 지연 값을 사용해야 합니다.
3. **LSA** 간격**(**초**)** 타이머 값을 지정합니다. 이 값은 동일한 LSA(동일한 라우터, 동일한 유형, 동일한 LSA ID)의 두 인스턴스가 전송되는 최소 시간(초)입니다. 이것은 RFC 2328의 MinLSInterval과 동일합니다. 토폴로지 변경이 발생할 때 더 낮은 값을 사용하여 재수렴 시간을 줄일 수 있습니다.
4. (선택 사항) OSPF 정상 재시작을 구성합니다.
5. 확인을 클릭합니다.

STEP 9 | 변경 사항을 커밋합니다.

OSPF 정상 재시작 구성

OSPF 정상 재시작은 OSPF 이웃이 서비스가 중단된 짧은 전환 동안 방화벽을 통해 경로를 계속 사용하도록 지시합니다. 이 동작은 짧은 주기적인 다운 시간 동안 발생할 수 있는 라우팅 테이블 재구성 및 관련 경로 플래ping 빈도를 줄여 네트워크 안정성을 높입니다.

Palo Alto Networks® 방화벽의 경우, OSPF 정상 재시작에는 다음 작업이 포함됩니다.

- 재시작 디바이스로서의 방화벽 - 방화벽이 짧은 시간 동안 다운되거나 짧은 시간 동안 사용할 수 없는 경우, 정상 LSA를 OSPF 이웃에 보냅니다. 이웃은 정상 재시작 도우미 모드에서 실행되도록 구성되어야 합니다. 도우미 모드에서, 이웃은 유예 기간으로 정의된 지정된 기간 내에 방화벽이 정상적인 재시작을 수행할 것임을 알리는 정상 LSA를 수신합니다. 유예 기간 동안, 이웃은 계속해서 방화벽을 통해 경로를 전달하고 방화벽을 통해 경로를 알리는 LSA를 보냅니다. 유예 기간이 만료되기 전에 방화벽이 작동을 재개하면 네트워크 중단 없이 트래픽 전달이 이전과 같이 계속됩니다. 유예 기간이 만료된 후 방화벽이 작동을 재개하지 않으면, 이웃은 도우미 모드를 종료하고 방화벽을 우회하도록 라우팅 테이블을 재구성하는 정상 작동을 재개합니다.
- 정상 재시작 도우미로서의 방화벽 - 인접 라우터가 짧은 시간 동안 다운될 수 있는 경우, 방화벽은 정상 재시작 도우미 모드에서 작동하도록 구성할 수 있습니다. 이 경우 방화벽은 최대 이웃 재시작 시간을 사용합니다. 방화벽이 OSPF 이웃 항목에서 정상 LSA를 수신하면, 유예 기간 또는 최대 인접 항목 재시작 시간이 만료될 때까지 인접 항목으로 트래픽을 계속 라우팅하고 인접 항목을 통해 경로를 알립니다. 인접 항목이 서비스로 돌아오기 전에 둘 다 만료되지 않으면, 네트워크 중단 없이 트래픽 전달이 이전과 같이 계속됩니다. 인접 항목이 서비스로 돌아오기 전에 두 기간이 만료되면 방화벽은 도우미 모드를 종료하고 인접 항목을 우회하도록 라우팅 테이블을 재구성하는 정상 작동을 재개합니다.

STEP 1 | 네트워크 > 가상 라우터를 선택하고 구성할 가상 라우터를 선택합니다.

STEP 2 | **OSPF** > 고급 또는 **OSPFv3** > 고급을 선택합니다.

STEP 3 | 다음이 선택되어 있는지 확인합니다(기본 설정으로 작동되어 있음).

- 정상 재시작 활성화
- 도우미 모드 활성화
- 엄격한 **LSA** 검사 활성화

토폴로지에서 요구하지 않는 한 선택된 상태로 유지해야 합니다.

STEP 4 | 유예 기간을 초 단위로 구성합니다.

STEP 5 | 최대 이웃 재시작 시간(초 단위)을 구성합니다.

OSPF 작업 확인

OSPF 구성이 커밋되면, 다음 작업 중 하나를 사용하여 OSPF가 작동하는지 확인할 수 있습니다.

- 라우팅 테이블 보기
- OSPF 인접성 확인
- OSPF 연결이 설정되었는지 확인

라우팅 테이블 보기

라우팅 테이블을 보면 OSPF 경로가 설정되었는지 확인할 수 있습니다. 라우팅 테이블은 웹 인터페이스 또는 CLI에서 액세스할 수 있습니다. CLI를 사용하는 경우 다음 명령을 사용하십시오.

- **`show routing route`**
- **`show routing fib`**

웹 인터페이스를 사용하여 라우팅 테이블을 보는 경우 다음 워크플로를 사용합니다.

STEP 1 | 네트워크 > 가상 라우터를 선택하고 관심 있는 가상 라우터와 같은 행에서 추가 런타임 통계 링크를 클릭합니다.

STEP 2 | 라우팅 > 라우팅 테이블을 선택하고 OSPF에서 학습한 라우팅에 대한 라우팅 테이블의 플래그 열을 검사합니다.

OSPF 인접성 확인

다음 워크플로를 사용하여 OSPF 인접성이 설정되었는지 확인합니다.

STEP 1 | 네트워크 > 가상 라우터를 선택하고 관심 있는 가상 라우터와 같은 행에서 추가 런타임 통계 링크를 클릭합니다.

STEP 2 | **OSPF** > 이웃을 선택하고 상태 열을 검사하여 OSPF 인접성이 설정되었는지 확인합니다.

OSPF 연결이 설정되었는지 확인

시스템 로그를 보고 방화벽이 OSPF 연결을 설정했는지 확인하십시오.

STEP 1 | 모니터 > 시스템을 선택하고 OSPF 인접 항목이 설정되었음을 확인하는 메시지를 찾습니다.

STEP 2 | **OSPF** > 이웃을 선택하고 상태 열을 검사하여 OSPF 인접 항목이 설정되었는지(가득 찬지) 확인합니다.

BGP

BGP(Border Gateway Protocol, 보더 게이트웨이 프로토콜)는 기본 인터넷 라우팅 프로토콜입니다. BGP는 AS(자율 시스템) 내에서 사용할 수 있는 IP 접두사를 기반으로 네트워크 연결 가능성을 결정합니다. 여기서 AS는 네트워크 공급자가 단일 라우팅 정책의 일부로 지정한 IP 접두사 집합입니다.

BGP 개요

BGP는 자율 시스템(외부 BGP 또는 eBGP) 또는 AS(내부 BGP 또는 iBGP) 내에서 기능하여 BGP 스피커로 라우팅 및 도달 가능성 정보를 교환합니다. 방화벽은 다음 기능을 포함하는, 완전한 BGP 구현을 제공합니다.

- 가상 라우터당 하나의 BGP 라우팅 인스턴스 사양.
- 로컬 라우트 ID 및 로컬 AS와 같은 기본 매개변수와, 경로 선택, 라우트 리플렉터, BGP 연합, 라우트 플랩 감쇠 및 정상적인 재시작과 같은 고급 옵션을 포함하는, 가상 라우터당 BGP 설정.
- 이웃 주소 및 원격 AS를 포함하는, 피어 그룹 및 이웃 설정과 이웃 속성 및 연결과 같은 고급 옵션.
- 경로 가져오기, 내보내기 및 광고를 제어하기 위한 경로 정책; 접두사 기반 필터링; 및 주소 집계.
- 재배포 프로필을 사용하여 BGP에 경로를 주입하기 위한 IGP-BGP 상호 작용.
- BGP 연결을 위한 MD5 인증 키를 지정하는, 인증 프로필. 인증은 경로 누출 및 성공적인 DoS 공격을 방지하는 데 도움이 됩니다.
- 멀티프로토콜 BGP(MP-BGP)를 사용하면 BGP 피어가 업데이트 패킷에서 IPv6 유니캐스트 경로와 IPv4 멀티캐스트 경로를 전달할 수 있고 방화벽과 BGP 피어가 IPv6 주소를 사용하여 서로 통신할 수 있습니다.
- BGP는 접두사에 대해 AS_PATH 목록에서 최대 255개의 AS 번호를 지원합니다.

MP-BGP

BGP는 IPv4 유니캐스트 접두사를 지원하지만 IPv4 멀티캐스트 경로 또는 IPv6 유니캐스트 접두사를 사용하는 BGP 네트워크는 IPv4 유니캐스트 이외의 주소 유형 경로를 교환하기 위해 MP-BGP(멀티프로토콜 BGP)가 필요합니다. MP-BGP를 사용하면 BGP 피어가 MP-BGP를 사용하지 않고 전달할 수 있는 IPv4 유니캐스트 경로 외에도 업데이트 패킷에서 IPv4 멀티캐스트 경로 및 IPv6 유니캐스트 경로를 전달할 수 있습니다.

이러한 방식으로 MP-BGP는 기본 IPv6 또는 이중 스택 IPv4 및 IPv6을 사용하는 BGP 네트워크에 대한 IPv6 연결을 제공합니다. 서비스 제공자는 고객에게 IPv6 서비스를 제공할 수 있고 기업은 서비스 제공자의 IPv6 서비스를 사용할 수 있습니다. 방화벽과 BGP 피어는 IPv6 주소를 사용하여 서로 통신할 수 있습니다.

BGP가 다중 네트워크 계층 프로토콜(IPv4용 BGP 제외)을 지원하기 위해 BGP-4용 다중 프로토콜 확장(RFC 4760)은 방화벽이 BGP 업데이트 패킷에서 송수신하는 다중 프로토콜 도달 가능 NLRI 속성에서 NLRI(네트워크 계층 도달 가능성 정보)를 사용합니다. 이 속성에는 다음 두 식별자를 포함하여 대상 접두사에 대한 정보가 포함됩니다.

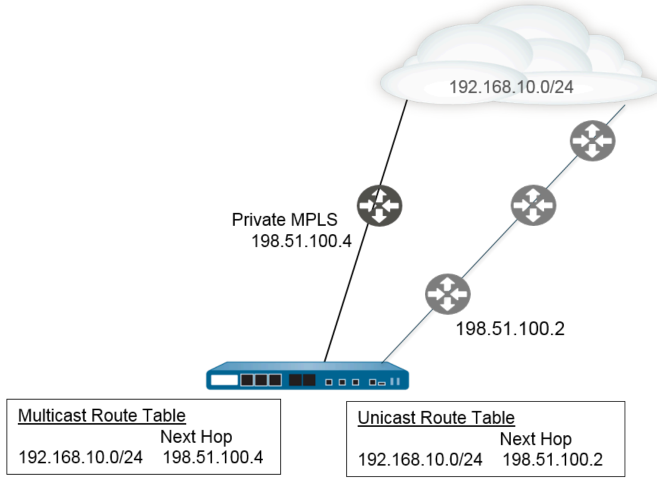
- 주소 패밀리 번호에서 IANA에 의해 정의된 AFI(주소 패밀리 식별자)는 대상 접두사가 IPv4 또는 IPv6 주소임을 나타냅니다. (PAN-OS는 IPv4 및 IPv6 AFI를 지원합니다.)
- PAN-OS의 SAFI(다음 주소 패밀리 식별자)는 대상 접두사가 유니캐스트 또는 멀티캐스트 주소(AFI가 IPv4인 경우)이거나 대상 접두사가 유니캐스트 주소(AFI가 IPv6인 경우)임을 나타냅니다. PAN-OS는 IPv6 멀티캐스트를 지원하지 않습니다.

IPv4 멀티캐스트에 대해 MP-BGP를 활성화하거나 멀티캐스트 고정 경로를 구성하는 경우 방화벽은 고정 경로에 대해 별도의 유니캐스트 및 멀티캐스트 경로 테이블을 지원합니다. 동일한 데스티네이션으로 가는 유니캐스트 트래픽과 멀티캐스트 트래픽을 분리할 수 있습니다. 멀티캐스트 트래픽은 유니캐스트 트래픽과 다른 경로를 취할 수 있습니다. 예를 들어 멀티캐스트 트래픽은 매우 중요하므로 홉을 더 적게 사용하거나 대기 시간을 줄임으로써 더 효율적이어야 하기 때문입니다.

또한 BGP가 경로를 가져오거나 내보낼 때 유니캐스트 또는 멀티캐스트 경로 테이블(또는 둘 다)의 경로만 사용하도록 BGP를 구성하거나 조건부 광고를 보내거나 경로 재분배 또는 경로 집계를 수행하도록 구성하여 BGP가 작동하는 방식을 더 많이 제어할 수 있습니다.

MP-BGP를 활성화하고 IPv4의 주소 계열 및 멀티캐스트의 후속 주소 계열을 선택하거나 멀티캐스트 경로 테이블에 IPv4 고정 경로를 설치하여 전용 멀티캐스트 RIB(경로 테이블)를 사용하도록 결정할 수 있습니다. 이러한 방법 중 하나를 수행하여 멀티캐스트 RIB를 사용하면 방화벽은 모든 멀티캐스트 라우팅 및 RPF(역방향 경로 전달)에 멀티캐스트 RIB를 사용합니다. 모든 라우팅(유니캐스트 및 멀티캐스트)에 유니캐스트 RIB를 사용하려는 경우 두 가지 방법으로 멀티캐스트 RIB를 활성화하면 안 됩니다.

다음 그림에서는 192.168.10.0/24에 대한 고정 경로가 유니캐스트 경로 테이블에 설치되어 있으며 다음 홉은 198.51.100.2입니다. 그러나 멀티캐스트 트래픽은 사설 MPLS 클라우드로 가는 다른 경로를 취할 수 있습니다. 동일한 정적 경로가 다른 다음 홉(198.51.100.4)으로 멀티캐스트 경로 테이블에 설치되어 경로가 다릅니다.



별도의 유니캐스트 및 멀티캐스트 라우팅 테이블을 사용하면 다음과 같은 BGP 기능을 구성할 때 보다 유연하게 제어할 수 있습니다.

- 이전 예에서 설명한 대로 IPv4 고정 경로를 유니캐스트 또는 멀티캐스트 경로 테이블 또는 둘 다에 설치합니다. (IPv6 고정 경로는 유니캐스트 경로 테이블에만 설치할 수 있습니다.)
- 기준과 일치하는 모든 접두사를 유니캐스트 또는 멀티캐스트 라우팅 테이블 또는 둘 다로 가져오도록 가져오기 규칙을 생성합니다.
- 기준과 일치하는 접두사를 유니캐스트 또는 멀티캐스트 라우팅 테이블 또는 둘 다에서 내보내도록(피어에 보내도록) 내보내기 규칙을 생성합니다.
- 방화벽이 유니캐스트 또는 멀티캐스트 라우팅 테이블(또는 둘 다)을 검색하여 해당 테이블에 경로가 존재하지 않는지 확인하고 방화벽이 다른 경로를 알릴 수 있도록 Non Exist 필터로 조건부 광고를 구성합니다.
- 방화벽이 유니캐스트 또는 멀티캐스트 라우팅 테이블 또는 둘 다의 기준과 일치하는 경로를 알리도록 광고 필터를 사용하여 조건부 광고를 구성합니다.
- 유니캐스트 또는 멀티캐스트 라우팅 테이블 또는 둘 다에 나타나는 경로를 재배포합니다.
- 보급할 집계된 경로가 유니캐스트 또는 멀티캐스트 라우팅 테이블 또는 둘 다에서 나오도록 보급 필터를 사용하여 경로 집계를 구성합니다.
- 반대로 억제해야 하는(알리지 않음) 집계된 경로가 유니캐스트 또는 멀티캐스트 라우팅 테이블 또는 둘 다에서 나오도록 억제 필터를 사용하여 경로 집계를 구성합니다.

IPv6의 주소 패밀리를 사용하여 MP-BGP로 피어를 구성할 때 가져오기 규칙, 내보내기 규칙, 조건부 광고(광고 필터 및 존재하지 않는 필터) 및 집계 규칙(Advertise Filter, Suppress Filter 및 Aggregate Route Attribute)의 주소 접두어 및 다음 홉 필드에서 IPv6 주소를 사용할 수 있습니다.

BGP 구성

다음 작업을 수행하여 BGP를 구성합니다.

STEP 1 | 일반 가상 라우터 설정을 구성합니다.

STEP 2 | 가상 라우터에 BGP를 사용하도록 설정하고, 라우터 ID를 할당하고, 가상 라우터를 AS에 할당합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP**를 선택합니다.
3. 이 가상 라우터에 대해 BGP를 사용하도록 설정합니다.
4. 라우터 **ID**가 고유한지 확인하기 위해 일반적으로 IPv4 주소인 가상 라우터의 BGP에 라우터 ID를 할당합니다.
5. 라우터 ID를 기반으로 가상 라우터가 속한 AS의 번호인 **AS** 번호를 할당합니다(범위는 1 - 4,294,967,295).
6. 확인을 클릭합니다.

STEP 3 | 일반 BGP 구성 설정을 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 일반을 선택합니다.
3. 기본 경로 거부를 선택하여 BGP 피어가 광고하는 기본 경로를 무시합니다.
4. 경로 설치를 선택하여 BGP 경로를 전역 라우팅 테이블에 설치합니다.
5. 집계 **MED**를 선택하여 경로에 MED(다중 종료 판별기) 값이 다른 경우에도 경로 집계를 사용하도록 설정합니다.
6. 서로 다른 경로 간의 기본 설정을 결정하는 데 사용할 수 있는 기본 로컬 기본 설정을 지정합니다.
7. 상호 운용성을 위해 **AS** 형식을 선택합니다.
   - **2**바이트(기본값)
   - **4**바이트

   런타임 통계는 RFC 5396에 따라 아스플레인 표기법을 사용하여 ***BGP 4***바이트 ***AS*** 번호를 표시합니다**.**
8. 경로 선택에 대해 다음 각 설정을 사용하거나 사용하지 않도록 설정합니다.
   - 항상 **MED** 비교 - 이 비교를 활성화하여 다른 자율 시스템의 이웃에서 경로를 선택합니다.
   - 결정적 **MED** 비교 - 이 비교를 활성화하여 IBGP 피어(동일한 자율 시스템의 BGP 피어)가 광고하는 경로 중에서 선택합니다.
9. 인증 프로파일의 경우 인증 프로파일을 추가합니다.
   - 프로파일 이름 - 프로파일을 식별할 이름을 입력합니다.
   - 암호**/**암호 확인 - BGP 피어 통신을 위한 암호를 입력하고 확인합니다. 암호는 MD5 인증에서 키로 사용됩니다.
10. 확인을 두 번 클릭합니다.

STEP 4 | (선택 사항) BGP 설정을 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 고급을 선택합니다.
3. ECMP를 구성하고 여러 BGP 자율 시스템에서 ECMP를 실행하려는 경우 **ECMP** 다중 **AS** 지원을 선택합니다.
4. **EBGP**에 대해 첫 번째 **AS**를 적용(기본적으로 사용됨)을 적용하여 방화벽이 eBGP 피어의 자체 AS 번호를 AS_PATH 특성의 첫 번째 AS 번호로 나열하지 않는 eBGP 피어에서 들어오는 업데이트 패킷을 삭제하도록 합니다.
5. 정상 다시 시작 을 선택하고 다음 타이머를 구성합니다.
   - 부실 라우트 시간**(**초**)** - 라우트가 부실 상태를 유지할 수 있는 시간(초)을 지정합니다(범위는 1 ~ 3,600, 기본값은 120).
   - 로컬 다시 시작 시간**(**초**)** -로컬 디바이스가 다시 시작하기를 기다리는 시간(초)을 지정합니다. 이 값은 피어에게 광고됩니다(범위는 1~3,600, 기본값은 120).
   - 최대 피어 다시 시작 시간**(**초**)** - 로컬 디바이스가 피어 디바이스에 대한 유예 기간 다시 시작 시간으로 허용하는 최대 시간(초)을 지정합니다(범위는 1~3,600, 기본값은 120).
6. 리플렉터 클러스터 **ID**에 대해 리플렉터 클러스터를 나타내는 IPv4 식별자를 지정합니다.
7. 연합 멤버 **AS**의 경우 BGP 연합 내에서만 볼 수 있는 자율 시스템 번호 식별자(하위 AS 번호라고도 함)를 지정합니다. 자세한 내용은 BGP 연합을(를) 참조하십시오.
8. 구성하려는 각 댐핑 프로파일에 대해 다음 정보를 추가하고 활성화를 선택한 다음 확인을 클릭합니다.
   - 프로파일 이름 - 프로파일을 식별할 이름을 입력합니다.
   - 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 유지 시간**(**초**)** - 경로가 얼마나 불안정했는지에 관계없이 경로가 억제될 수 있는 최대 시간(초)을 지정합니다(범위는 0 ~ 3,600, 기본값은 900).
   - **Decay Half Life Reachable(**초**)**- 경로가 도달 가능한 것으로 간주되는 경우 경로의 안정성 메트릭이 반감되는 시간(초)을 지정합니다(범위는 0~3,600, 기본값은 300).
   - **Decay Half Life Unreachable(**초**)** - 경로가 도달할 수 없는 것으로 간주되는 경우 경로의 안정성 메트릭이 반으로 줄어들기까지의 시간(초)을 지정합니다(범위는 0 ~ 3,600, 기본값은 300).
9. 확인을 두 번 클릭합니다.

STEP 5 | BGP 피어 그룹을 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 피어 그룹을 선택하고 피어 그룹의 이름을 추가하고 활성화합니다.
3. 집계된 연결된 **AS** 경로를 선택하여 구성된 집계된 연합 AS에 대한 경로를 포함합니다.
4. 저장된 정보가 있는 소프트 재설정을 선택하여 피어 설정을 업데이트한 후 방화벽의 소프트 재설정을 수행합니다.
5. 피어 그룹 유형을 선택합니다.
   - **IBGP** - 다음 홉 내보내기: 원본 또는 자체 사용을 선택합니다.
   - **EBGP Confed** - 다음 홉 내보내기: 원본 또는 자체 사용을 선택합니다.
   - **EBGP Confed** - 다음 홉 내보내기: 원본 또는 자체 사용을 선택합니다.
   - **EBGP** - 다음 홉 가져오기: 원본 또는 자체 사용을 선택하십시오. 다음 홉 내보내기: 해결 또는 자체 사용을 지정합니다. 방화벽이 다른 AS의 피어에게 보내는 업데이트의 AS_PATH 속성에서 BGP가 개인 AS 번호를 강제로 제거하도록 하려면 개인 **AS** 제거를 선택하십시오.
6. 확인을 클릭합니다.

STEP 6 | 피어 그룹에 속하는 BGP 피어를 구성하고 해당 주소를 지정합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 피어 그룹을 선택하고 만든 피어 그룹을 선택합니다.
3. 피어의 경우 이름별로 피어를 추가합니다 .
4. 피어를 사용하도록 설정합니다.
5. 피어가 속한 피어 **AS**를 입력합니다.
6. 주소 지정을 선택합니다.
7. 로컬 주소에서 BGP를 구성할 인터페이스를 선택합니다. 인터페이스에 둘 이상의 **IP** 주소가 있는 경우 해당 인터페이스의 IP 주소를 BGP 피어로 입력합니다.
8. 피어 주소에서 **IP**를 선택하고 IP 주소를 입력하거나 주소 개체를 선택 또는 만들거나 **FQDN**을 선택하고 FQDN을 입력한 FQDN 또는 주소 개체를 입력합니다.

   방화벽은 FQDN의 DNS 확인에서 하나의 IP 주소(각 IPv4 또는 IPv6 제품군 유형에서)만 사용합니다. DNS 확인이 둘 이상의 주소를 반환하는 경우 방화벽은 BGP 피어에 대해 구성된 IP 제품군 유형(IPv4 또는 IPv6)과 일치하는 기본 IP 주소를 사용합니다. 기본 IP 주소는 DNS 서버가 초기 응답에서 반환하는 첫 번째 주소입니다. 방화벽은 주소가 순서에 관계없이 후속 응답에 표시되는 한 이 주소를 선호하는 대로 유지합니다.
9. 확인을 클릭합니다.

STEP 7 | BGP 피어에 대한 연결 설정을 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 피어 그룹을 선택하고 만든 피어 그룹을 선택합니다.
3. 구성한 피어를 선택합니다.
4. 연결 옵션을 선택합니다.
5. 피어에 대한 인증 프로파일을 선택합니다.
6. 연결 유지 간격**(**초**)** 설정 - 보류 시간 설정에 따라 피어의 경로가 억제되는 간격(초)입니다(범위는 0~1,200, 기본값은 30).
7. 다중 홉 설정 - IP 헤더의 TTL(Time-to-Live) 값입니다(범위는 0~255, 기본값은 0). 기본값 0은 eBGP의 경우 1을 의미합니다. 기본값 0은 iBGP의 경우 255를 의미합니다.
8. 열기 지연 시간**(**초**)** 설정 - BGP 연결을 설정하기 위해 TCP 핸드셰이크와 첫 번째 BGP 열기 메시지를 보내는 방화벽 간의 지연(초)입니다(범위는 0~240, 기본값은 0).
9. 보류 시간**(**초**)** 설정 - 피어 연결이 닫히기 전에 피어의 연속적인 Keepalive 또는 업데이트 메시지 사이에 경과할 수 있는 시간(초)입니다(범위는 3~3,600, 기본값은 90).
10. 유휴 대기 시간**(**초**)** 설정 - 피어에 다시 연결하기 전에 대기할 시간(초)입니다(범위는 1~3,600, 기본값은 15).
11. 최소 경로 알림 간격**(**초**)** 설정 - BGP 스피커(방화벽)가 경로를 알리거나 경로를 철회하는 BGP 피어에 보내는 두 개의 연속 업데이트 메시지 사이의 최소 시간(초)입니다(범위는 1~600, 기본값은 30).
12. 들어오는 연결에 원격 포트를 입력하고 허용을 선택하여 이 포트로 들어오는 트래픽을 허용합니다.
13. 나가는 연결에 로컬 포트를 입력하고 허용을 선택하여 이 포트에서 나가는 트래픽을 허용합니다.
14. 확인을 클릭합니다.

STEP 8 | 경로 리플렉터 클라이언트, 피어링 유형, 최대 접두사 및 BFD(양방향 전달 감지)에 대한 설정으로 BGP 피어를 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 피어 그룹을 선택하고 만든 피어 그룹을 선택합니다.
3. 구성한 피어를 선택합니다.
4. 고급을 선택합니다.
5. 리플렉터 클라이언트에서 다음 중 하나를 선택합니다.
   - 비 클라이언트(기본값) - 피어는 경로 리플렉터 클라이언트가 아닙니다.
   - 클라이언트 - 피어는 경로 리플렉터 클라이언트입니다.
   - **meshed-client**
6. 피어링 유형에서 다음 중 하나를 선택합니다.
   - 양방향 - 두 BGP 피어가 피어 연결을 설정합니다.
   - 지정되지 않음(기본값).
7. 최대 접두사에 지원되는 최대 IP 접두사 수(범위는 1~100,000)를 입력하거나 무제한을 선택합니다.
8. 피어에 대해 **BFD**를 사용하도록 설정하려면(따라서 가상 라우터 수준에서 BGP에 대해 BFD가 비활성화되지 않은 한 BGP에 대한 BFD 설정을 재정의하려면) 다음 중 하나를 선택합니다.
   - 기본값 - 피어는 기본 BFD 설정만 사용합니다.
   - **Inherit-vr-global-setting**(기본값) - 피어는 가상 라우터의 BGP에 대해 전역적으로 선택한 BFD 프로파일을 상속합니다.
   - 구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.

   *BGP 피어에 대해 **BFD**를 비활성화하려면 **BFD** 비활성화를 선택합니다.*
9. 확인을 클릭합니다.

STEP 9 | 가져오기 및 내보내기 규칙을 구성합니다.

가져오기 및 내보내기 규칙은 다른 라우터에서 경로를 가져오고 내보내는 데 사용됩니다(예: 인터넷 서비스 공급자로부터 기본 경로 가져오기).

1. 가져오기를 선택하고 규칙 필드에 이름(최대 63자)을 추가합니다. 이름은 영숫자 문자로 시작해야 하며 영숫자 문자, 밑줄(_), 하이픈(-), 점(.) 및 공백의 조합을 포함할 수 있습니다.
2. 규칙을 활성화합니다.
3. 경로를 가져올 피어 그룹을 추가합니다.
4. 일치를 선택하고 라우팅 정보를 필터링하는 데 사용되는 옵션을 정의합니다. 또한 경로 필터링을 위해 MED(Multi-Exit Discriminator) 값과 라우터 또는 서브넷에 대한 다음 홉 값을 정의할

수 있습니다. MED 옵션은 AS로의 선호 경로를 이웃에게 알려주는 외부 메트릭입니다. 높은 값보다 낮은 값이 선호됩니다.

5. 작업을 선택하고 일치 탭에 정의된 필터링 옵션을 기반으로 발생해야 하는 작업(허용 또는 거부)을 정의합니다. 거부를 선택하면 추가 옵션을 정의할 필요가 없습니다. 허용을 선택한 경우 다른 속성을 정의합니다.
6. 확인을 클릭합니다.
7. 내보내기를 선택하고 내보내기 속성을 정의합니다. 이 속성은 가져오기 설정과 유사하지만 방화벽에서 이웃으로 내보내는 경로 정보를 제어하는 데 사용됩니다. 내보내기 규칙의 이름은 최대 31자일 수 있습니다.

STEP 10 | 피어링 또는 연결 실패를 나타내는 로컬 BGP 라우팅 테이블(LocRIB)에서 다른 경로를 사용할 수 없는 경우 광고할 경로를 제어할 수 있는 조건부 광고를 구성합니다.

이는 여러 ISP를 통해 인터넷에 연결되어 있고 트래픽이 다른 공급자 대신 한 공급자에게 라우팅되기를 원하는 경우와 같이, 기본 제공자에 대한 연결 손실이 있을 때 다른 AS를 통해 한 AS로의 경로를 강제하려는 경우에 유용합니다.

1. 조건부 고급을 선택하고 정책 이름을 추가합니다.
2. 조건부 광고를 활성화합니다.
3. 사용자 섹션에서 조건부 광고 정책을 사용할 피어 그룹을 추가합니다.
4. 존재하지 않는 필터를 선택하고 기본 경로의 네트워크 접두사를 정의합니다. 로컬 BGP 라우팅 테이블에서 사용할 수 있을 때 광고하려는 경로를 지정합니다. 접두사가 광고될 예정이고 존재하지 않음 필터와 일치하면 광고가 억제됩니다.
5. 필터 광고을 선택하고 존재하지 않는 필터의 경로를 로컬 라우팅 테이블에서 사용할 수 없는 경우 광고해야 하는 Local-RIB 라우팅 테이블에서 경로의 접두사를 정의합니다. 접두사가 광고될 예정이고 존재하지 않음 필터와 일치하지 않으면 광고가 발생합니다.
6. 확인을 클릭합니다.

STEP 11 | BGP 구성에서 경로를 요약하도록 집계 옵션을 구성합니다.

BGP 경로 집계는 BGP가 주소를 집계하는 방법을 제어하는 데 사용됩니다. 테이블의 각 항목은 하나의 집계 주소를 생성합니다. 지정된 주소와 일치하는 특정 경로가 하나 이상 학습되면 라우팅 테이블에 집계 항목이 생성됩니다.

1. 집계 및 추가를 선택하여 통합 주소 이름을 지정합니다.
2. 집계된 접두사의 기본 접두사가 될 네트워크 접두사를 입력합니다.
3. 필터 억제를 선택하고 일치하는 경로가 표시되지 않도록 하는 속성을 정의합니다.
4. 광고 필터를 선택하고 일치하는 경로가 항상 피어에게 광고되도록 하는 속성을 정의합니다.
5. 확인을 클릭합니다.

STEP 12 | 재배포 규칙을 구성합니다.

이 규칙은 로컬 RIB에 없는 호스트 경로와 알 수 없는 경로를 피어 라우터에 재배포하는 데 사용됩니다.

1. 재배포 규칙 및 새 재배포 규칙 추가를 선택합니다.
2. IP 서브넷의 이름을 입력하거나 재배포 프로파일을 선택합니다. 필요한 경우 새 재배포 프로파일을 구성할 수도 있습니다.
3. 규칙을 활성화합니다.
4. 규칙에 사용할 경로 메트릭을 입력합니다.
5. 원점 설정 목록에서 불완전, **igp** 또는 **egp**를 선택합니다.
6. (선택 사항) MED, 로컬 기본 설정, AS 경로 제한 및 커뮤니티 값을 설정합니다.
7. 확인을 클릭합니다.

STEP 13 | 변경 사항을 커밋합니다.

IPv4 또는 IPv6 유니캐스트용 MP-BGP를 갖춘 BGP 피어 구성

BGP를, 구성한 후, 다음 이유 중 하나에 대해 IPv4 또는 IPv6 유니캐스트에 대한 MP-BGP를 갖춘 BGP 피어를 구성합니다.

- BGP 피어가 IPv6 유니캐스트 경로를 수행하도록 하려면, MP-BGP를 **IPv6**의 주소 패밀리 유형과 유니캐스트의 후속 주소 패밀리로 구성하여 피어가 IPv6 유니캐스트 경로를 포함하는 BGP 업데이트를 보낼 수 있도록 합니다. BGP 피어링(로컬 주소 및 피어 주소)은 여전히 IPv4 주소이거나, 또는 모두 IPv6 주소일 수 있습니다.
- IPv6 주소를 통해 BGP 피어링을 수행하려면 (로컬 주소 및 피어 주소는 IPv6 주소를 사용합니다).

다음 작업은 MP-BGP를 사용하여 BGP 피어를 작동시켜 IPv6 유니캐스트 경로를 수행할 수 있도록 하고, IPv6 주소를 사용하여 피어를 사용할 수 있도록 하는 방법을 보여줍니다.

또한 이 작업은 유니캐스트 또는 멀티캐스트 경로 테이블을 보는 방법과, 유니캐스트 또는 멀티캐스트 경로 테이블 또는 특정 주소 패밀리(IPv4 또는 IPv6)로부터 경로를 보려면 전달 테이블, BGP 로컬 RIB 및 BGP RIB 아웃(이웃으로 전송된 경로)을 보는 방법을 보여줍니다.

STEP 1 | 피어에 대한 MP-BGP 확장을 작동시킵니다.

BGP 피어가 업데이트 패킷에서 IPv4 또는 IPv6 유니캐스트 경로를 수행할 수 있고 방화벽이 IPv4 또는 IPv6 주소를 사용하여 피어와 통신할 수 있도록 다음을 구성합니다.

1. 네트워크 > 가상 라우터를 선택하고 구성 중인 가상 라우터를 선택합니다.
2. **BGP**를 선택합니다.
3. 피어 그룹을 선택하고 피어 그룹을 선택합니다.
4. BGP 피어(라우터)를 선택합니다.
5. 주소 지정을 선택합니다.
6. 피어에 대한 **MP-BGP** 확장 활성화를 선택합니다.
7. 주소 패밀리 유형의 경우 **IPv4** 또는 **IPv6**를 선택합니다. 예를 들어, IPv6을 선택합니다.
8. 후속 주소 패밀리의 경우 유니캐스트가 선택됩니다. 주소 패밀리에 대해 **IPv4**를 선택한 경우 멀티캐스트도 선택할 수 있습니다.
9. 로컬 주소의 경우 인터페이스를 선택하고 선택 사항으로 **IP** 주소를 선택합니다(예: 2001:DB8:55::/32).
10. 피어 주소의 경우 2001:DB8:58::/32와 같은 주소 패밀리(IPv4 또는 IPv6)를 사용하여 피어의 **IP** 주소를 입력합니다.
11. 고급을 선택합니다.
12. (선택 사항) 발신자 측 루프 감지를 활성화합니다. 전송자 측 루프 감지를 사용하도록 설정하면, 방화벽은 피어 AS 번호가 AS_PATH 목록에 없는지 확인하기 위해 업데이트에서 경로를 보내기 전에 FIB의 경로의 AS_PATH 특성을 확인합니다. 그러한 경우 방화벽은 루프를 방지하기 위해 제거합니다.
13. 확인을 클릭합니다.

STEP 2 | (선택 사항) 정적 경로를 만들고 유니캐스트 경로 테이블에 설치합니다.

1. 네트워크 > 가상 라우터를 선택하고 구성 중인 가상 라우터를 선택합니다.
2. 정적 경로를 선택하고 **IPv4** 또는 **IPv6**를 선택한 후 경로를 추가합니다.
3. 정적 경로에 대한 이름을 입력합니다.
4. IPv4 또는 IPv6을 선택했는지 여부에 따라, IPv4 또는 IPv6 대상 접두사와 넷마스크를 입력합니다.
5. 송신 인터페이스를 선택합니다.
6. 다음 홉을 **IPv6** 주소(또는 IPv4를 선택한 경우 **IP** 주소)로 선택하고 이 정적 경로에 대한 유니캐스트 트래픽을 직접 입력하려는 다음 홉의 주소를 입력합니다.
7. 관리자 거리를 입력합니다.
8. 메트릭을 입력합니다.
9. 경로 테이블의 경우 유니캐스트를 선택합니다.
10. 확인을 클릭합니다.

STEP 3 | 구성을 커밋합니다.

커밋을 클릭합니다.

STEP 4 | 유니캐스트 또는 멀티캐스트 경로 테이블을 봅니다.

1. 네트워크 > 가상 라우터를 선택합니다**.**
2. 가상 라우터의 행에서 더 많은 런타임통계를 클릭합니다.
3. 라우팅 > 경로 테이블을 선택합니다.
4. 경로 테이블의 경우, 유니캐스트 또는 멀티캐스트를 선택하여 해당 경로만 표시합니다.
5. 디스플레이 주소 패밀리의 경우, **IPv4** 전용, **IPv6** 전용, 또는 **IPv4** 및 **IPv6**를 선택하여 해당 주소 패밀리에 대한 경로만 표시합니다.

*IPv6*만으로 멀티캐스트를 선택하는 것은 지원되지 않습니다*.*

STEP 5 | 전달 테이블을 봅니다.

1. 네트워크 > 가상 라우터를 선택합니다**.**
2. 가상 라우터의 행에서 더 많은 런타임통계를 클릭합니다.
3. 라우팅 > 전달 테이블을 선택합니다.
4. 디스플레이 주소 패밀리의 경우, **IPv4** 전용, **IPv6** 전용, 또는 **IPv4** 및 **IPv6**를 선택하여 해당 주소 패밀리에 대한 경로만 표시합니다.

STEP 6 | BGP RIB 테이블을 봅니다.

1. 방화벽이 BGP 패킷을 라우팅하는 데 사용하는 BGP 경로를 보여 주는 BGP 로컬 RIB를 봅니다.
    1. 네트워크 > 가상 라우터를 선택합니다**.**
    2. 가상 라우터의 행에서 더 많은 런타임통계를 클릭합니다.
    3. **BGP** > 로컬 **RIB**를선택합니다.
    4. 경로 테이블의 경우, 유니캐스트 또는 멀티캐스트를 선택하여 해당 경로만 표시합니다.
    5. 디스플레이 주소 패밀리의 경우, **IPv4** 전용, **IPv6** 전용, 또는 **IPv4** 및 **IPv6**를 선택하여 해당 주소 패밀리에 대한 경로만 표시합니다.

    IPv6만으로 멀티캐스트를 선택하는 것은 지원되지 않습니다**.**

2. 방화벽이 BGP 이웃에게 보내는 경로를 보여 주는, BGP RIB 아웃 테이블을 봅니다.
    1. 네트워크 > 가상 라우터를 선택합니다**.**
    2. 가상 라우터의 행에서 더 많은 런타임통계를 클릭합니다.
    3. **BGP** > **RIB** 아웃을 선택합니다.
    4. 경로 테이블의 경우, 유니캐스트 또는 멀티캐스트를 선택하여 해당 경로만 표시합니다.
    5. 디스플레이 주소 패밀리의 경우, **IPv4** 전용, **IPv6** 전용, 또는 **IPv4** 및 **IPv6**를 선택하여 해당 주소 패밀리에 대한 경로만 표시합니다.

    IPv6만으로 멀티캐스트를 선택하는 것은 지원되지 않습니다**.**

IPv4 멀티캐스트용 MP-BGP를 갖춘 BGP 피어 구성

BGP를 구성한 후, BGP 피어가 BGP 업데이트에서 IPv4 멀티캐스트 경로를 학습하고 전달할 수 있도록 하려면 IPv4 멀티캐스트용 MP-BGP로 BGP 피어를 구성합니다. 유니캐스트를 멀티캐스트 트래픽과 분리하거나, 또는 MP-BGP에 나열된 기능을 사용하여 유니캐스트 또는 멀티캐스트 경로 테이블의 경로, 또는 두 테이블의 경로만 사용할 수 있습니다.

멀티캐스트 트래픽만 지원하려면, 필터를 사용하여 유니캐스트 트래픽을 제거해야 합니다.

방화벽은 멀티캐스트 트래픽에 대한 ECMP를 지원하지 않습니다.

STEP 1 | BGP 피어가 IPv4 멀티캐스트 경로를 교환할 수 있도록 MP-BGP 확장을 작동합니다.

1. 네트워크 > 가상 라우터를 선택하고 구성 중인 가상 라우터를 선택합니다.
2. **BGP**를 선택합니다.
3. 피어 그룹을 선택하고, 피어 그룹과 BGP 피어를 선택합니다.
4. 주소 지정을 선택합니다.
5. **MP-BGP** 확장 활성화를 선택합니다.
6. 주소 패밀리 유형의 경우 **IPv4**를 선택합니다.
7. 후속 주소 패밀리의 경우 유니캐스트를 선택한 다음 멀티캐스트를 선택합니다.
8. 확인을 클릭합니다.

STEP 2 | (선택 사항) IPv4 정적 경로를 생성하고 멀티캐스트 경로 테이블에만 설치합니다.

MP-BGP의 토폴로지에 표시된 대로, BGP 피어용 멀티캐스트 트래픽을 특정 다음 홉으로 유도하기 위해 이 작업을 수행합니다.

1. 네트워크 > 가상 라우터를 선택하고 구성 중인 가상 라우터를 선택합니다.
2. 정적 경로 > **IPv4**를 선택하고 경로에 대한 이름을 추가합니다.
3. IPv4 대상 접두사와 넷 마스크를 입력합니다.
4. 송신 인터페이스를 선택합니다.
5. 다음 홉을 **IP** 주소로 선택하고 이 정적 경로에 대해 멀티캐스트 트래픽을 안내하려는 다음 홉의 IP 주소를 입력합니다.
6. 관리자 거리를 입력합니다.
7. 메트릭을 입력합니다.
8. 경로 테이블의 경우 멀티캐스트를 선택합니다.
9. 확인을 클릭합니다.

STEP 3 | 구성을 커밋합니다.

커밋을 클릭합니다.

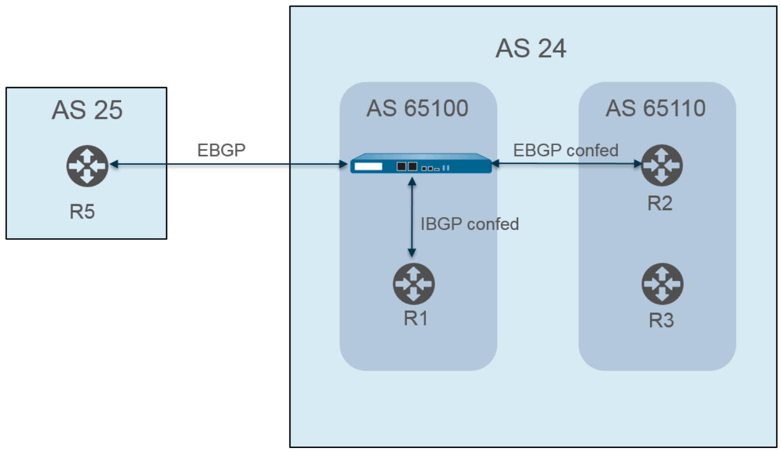
STEP 4 | 경로 테이블을 봅니다.

1. 네트워크 > 가상 라우터를 선택합니다**.**
2. 가상 라우터의 행에서 더 많은 런타임통계를 클릭합니다.
3. 라우팅 > 경로 테이블을 선택합니다.
4. 경로 테이블의 경우, 유니캐스트 또는 멀티캐스트를 선택하여 해당 경로만 표시합니다.
5. 디스플레이 주소 패밀리의 경우, **IPv4** 전용, **IPv6** 전용, 또는 **IPv4** 및 **IPv6**를 선택하여 해당 주소 패밀리에 대한 경로만 표시합니다.

STEP 5 | 포워딩 테이블, BGP 로컬 립 또는 BGP 립 아웃 테이블을 보려면, IPv4 또는 IPv6 유니캐스트용 MP-BGP로 BGP 피어 구성을 참조하십시오.

BGP 연합

BGP 연합은 IBGP에 대한 전체 메시 요구 사항이 야기하는 부담을 줄이기 위해 자율 시스템(AS)을 두 개 이상의 하위 자율 시스템(sub-AS)으로 나누는 방법을 제공합니다. 하위 AS 내의 방화벽(또는 기타 라우팅 장치)에는 동일한 하위 AS의 다른 방화벽과 함께 전체 iBGP 메시가 있어야 합니다. 주 AS 내에서 완전한 연결을 위해서는 하위 자율 시스템 간의 BGP 피어링이 필요합니다. 하위 AS 내에서 서로 피어링하는 방화벽은 IBGP 연합 피어링을 형성합니다. 한 하위 AS의 방화벽이 다른 하위 AS의 방화벽과 피어링하여 EBGP 연합 피어링을 형성합니다. 연결하는 서로 다른 자율 시스템의 두 방화벽은 EBGP 피어입니다.

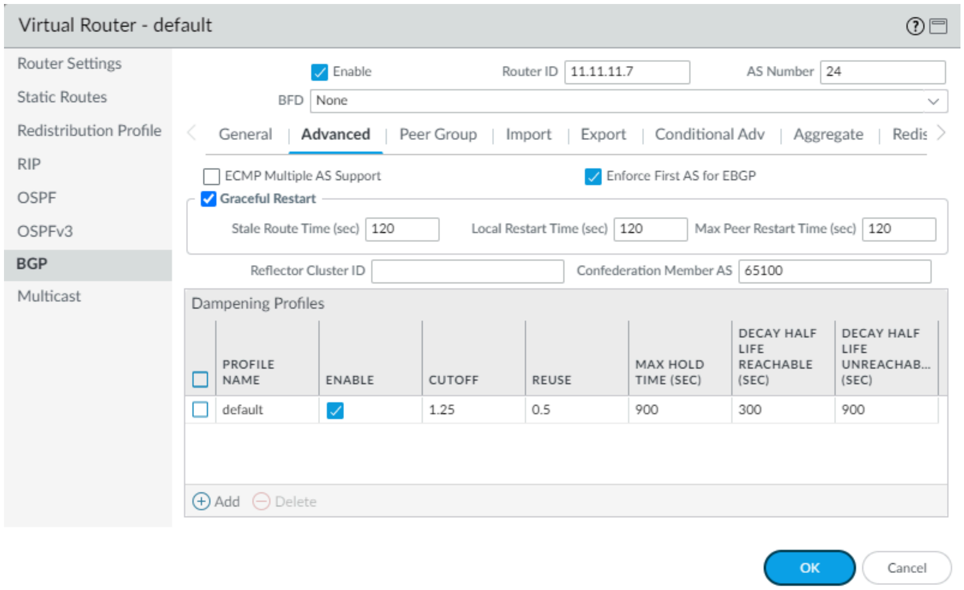


자율 시스템은 앞의 그림에서 AS 24 및 AS 25와 같은, 공개(전역적으로 할당된) AS 번호로 식별됩니다. PAN-OS 환경에서는, 각 하위 AS에 고유한 연합 회원 AS 번호를 할당합니다. 이 번호는 AS 내에서만 볼 수 있는 개인 번호입니다. 이 그림에서, 연합은 AS 65100 및 AS 65110입니다. (RFC6996, 사설 사용을 위한 자율 시스템(AS) 예약은 IANA가 사설 사용을 위해 AS 번호 64512-65534를 예약함을 나타냅니다.)

하위 AS 연합은 AS 내에서 서로에게 완전한 자율 시스템처럼 보입니다. 그러나, 방화벽이 EBGP 피어에 AS 경로를 보낼 때, AS 경로에는 공용 AS 번호만 나타납니다. 비공개 하위 AS(연맹 회원 AS) 번호는 포함되지 않습니다.

BGP 피어링은 방화벽과 R2 사이에서 발생합니다. 그림의 방화벽에는 다음과 같은 관련 구성 설정이 있습니다.

- AS 번호 - 24
- 연합 회원 AS—65100
- 피어링 유형 - EBGP confed
- 피어 AS—65110



AS 65110의 라우터 2(R2)는 다음과 같이 구성됩니다.

- AS 번호 - 24
- 연합 회원 AS - 65110
- 피어링 유형 - EBGP confed
- 피어 AS—65100

BGP 피어링은 방화벽과 R1 사이에서도 발생합니다. 방화벽에는 다음과 같은 추가 구성이 있습니다.

- AS 번호 - 24
- 연합 회원 AS—65100
- 피어링 유형 - IBGP confed
- 피어 AS—65110

R1은 다음과 같이 구성됩니다.

- AS 번호 - 24
- 연합 회원 AS - 65110
- 피어링 유형 - IBGP confed
- 피어 AS—65100

BGP 피어링은 방화벽과 R5 사이에서 발생합니다. 방화벽에는 다음과 같은 추가 구성이 있습니다.

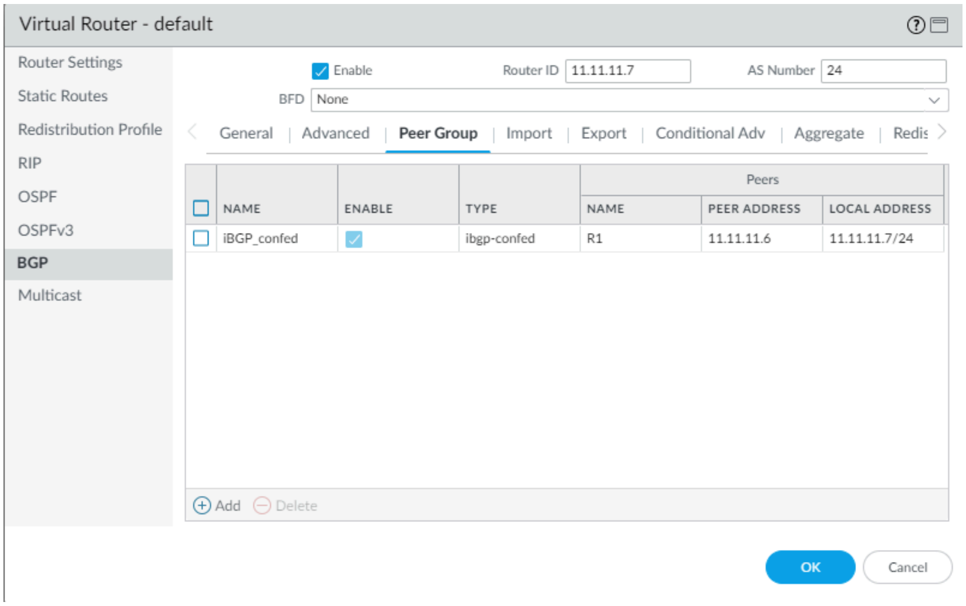
- AS 번호 - 24
- 연합 회원 AS—65100
- 피어링 유형 - EBGP
- 피어 AS—25

R5는 다음과 같이 구성됩니다.

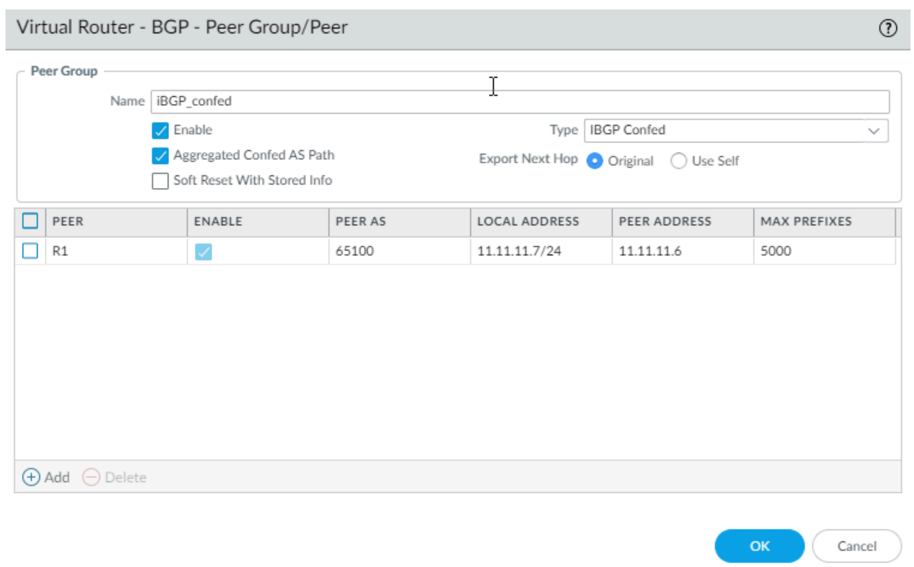
- AS—25

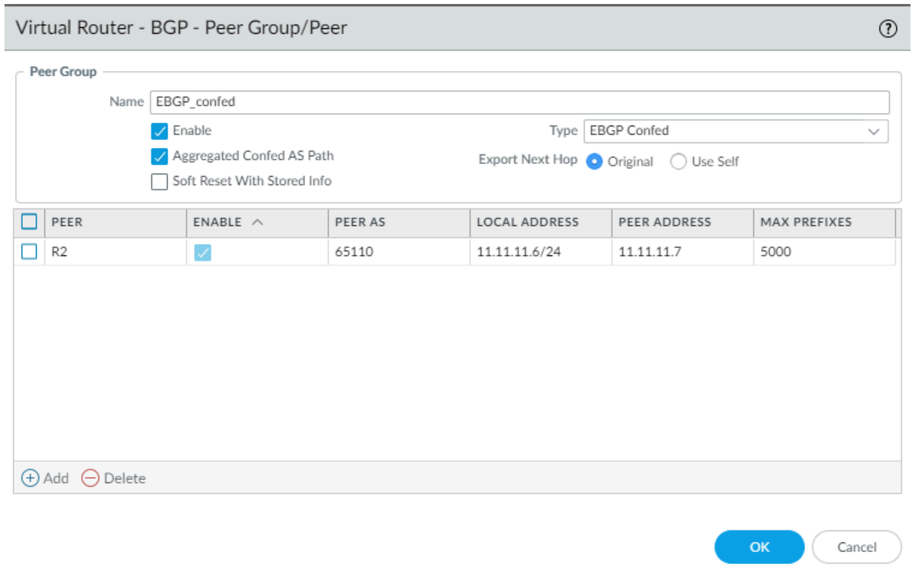
- 피어링 유형 - EBGP
- 피어 AS—24

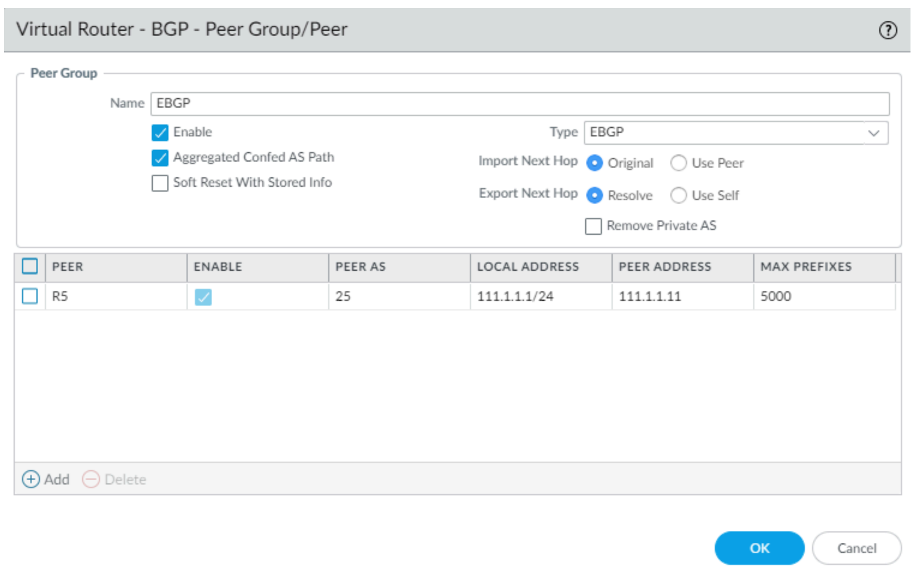
방화벽이 R1, R2 및 R5와 피어링하도록 구성되면 피어 그룹 탭에서 해당 피어를 볼 수 있습니다.



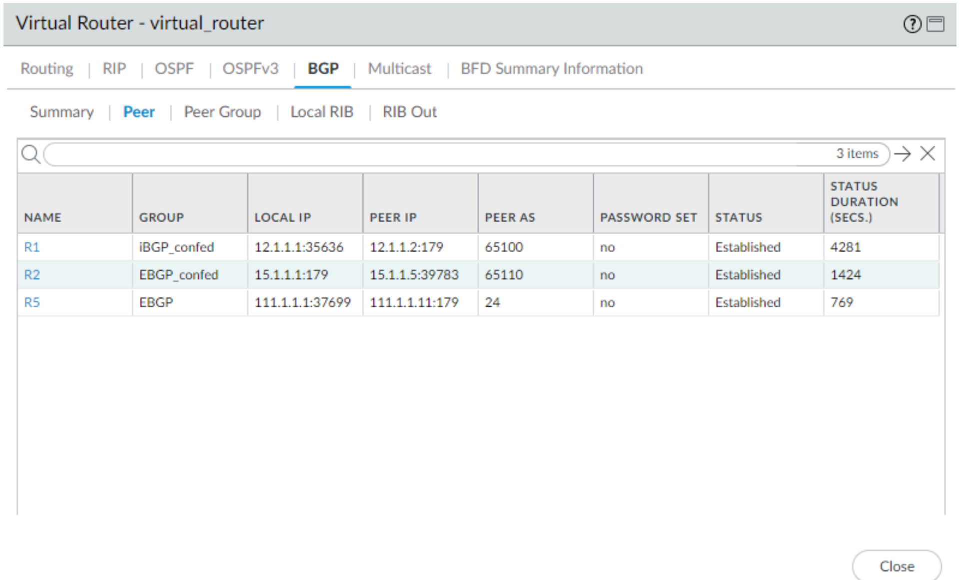
방화벽은 R1, R2 및 R5 피어를 표시합니다.





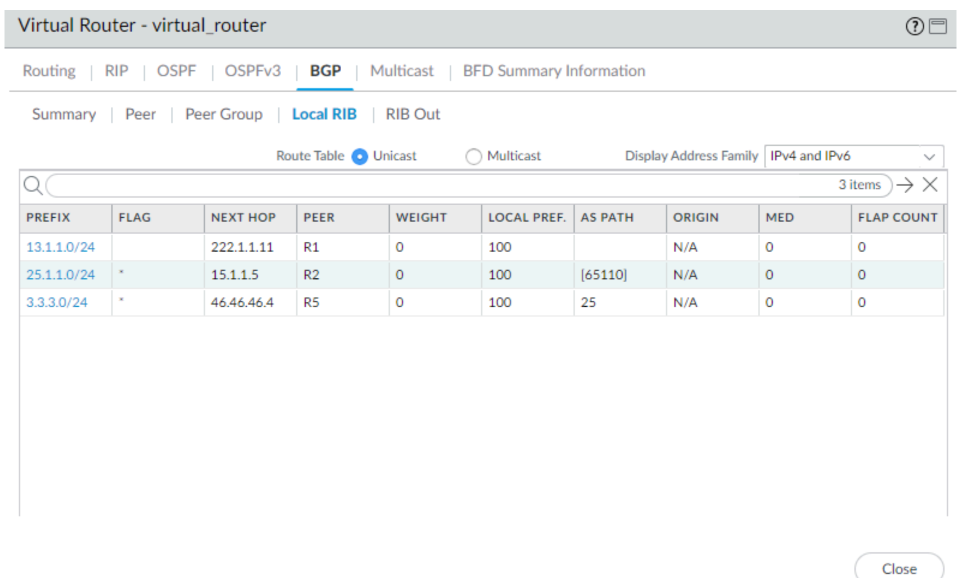


방화벽에서 피어로의 경로가 설정되었는지 확인하려면 가상 라우터 화면에서 추가 런타임 통계를 선택하고 피어 탭을 선택합니다.



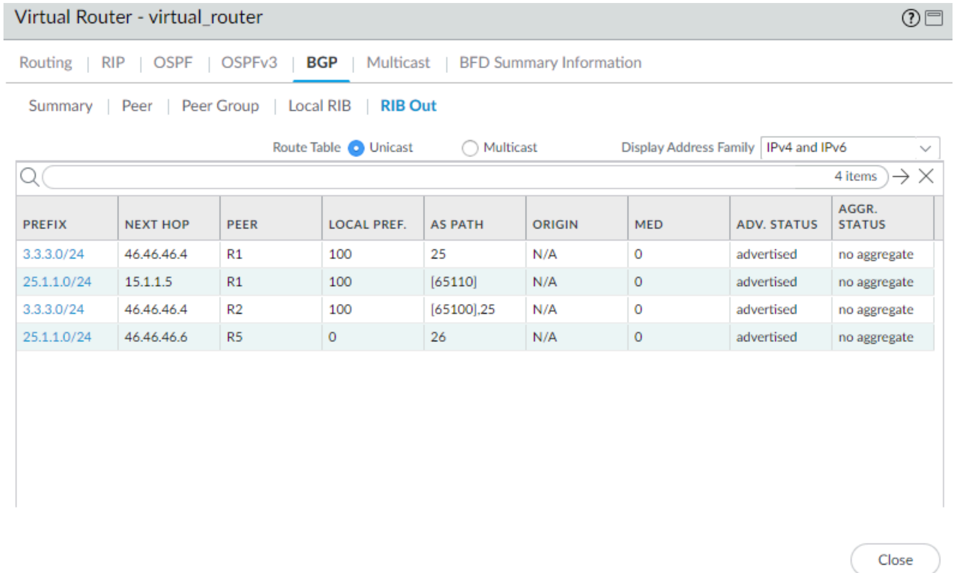
NAME	GROUP	LOCAL IP	PEER IP	PEER AS	PASSWORD SET	STATUS	STATUS DURATION (SECS.)
R1	iBGP_confed	12.1.1.1:35636	12.1.1.2:179	65100	no	Established	4281
R2	EBGP_confed	15.1.1.1:179	15.1.1.5:39783	65110	no	Established	1424
R5	EBGP	111.1.1.1:37699	111.1.1.11:179	24	no	Established	769

RIB(Routing Information Base, 라우팅 정보 베이스)에 저장된 경로에 대한 정보를 보려면 로컬 **RIB** 탭을 선택합니다.



PREFIX	FLAG	NEXT HOP	PEER	WEIGHT	LOCAL PREF.	AS PATH	ORIGIN	MED	FLAP COUNT
13.1.1.0/24		222.1.1.11	R1	0	100		N/A	0	0
25.1.1.0/24	*	15.1.1.5	R2	0	100	[65110]	N/A	0	0
3.3.3.0/24	*	46.46.46.4	R5	0	100	25	N/A	0	0

그런 다음 **RIB** 출력 탭을 선택합니다.


Virtual Router - virtual_router
Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information
Summary | Peer | Peer Group | Local RIB | RIB Out
Route Table Unicast Multicast Display Address Family IPv4 and IPv6
4 items
PREFIX NEXT HOP PEER LOCAL PREF. AS PATH ORIGIN MED ADV. STATUS AGGR. STATUS
3.3.3.0/24 46.46.46.4 R1 100 25 N/A 0 advertised no aggregate
25.1.1.0/24 15.1.1.5 R1 100 [65110] N/A 0 advertised no aggregate
3.3.3.0/24 46.46.46.4 R2 100 [65100],25 N/A 0 advertised no aggregate
25.1.1.0/24 46.46.46.6 R5 0 26 N/A 0 advertised no aggregate
Close

IP 멀티캐스트

IP 멀티캐스트는 네트워크 어플라이언스가 트래픽을 여러 수신기에 유니캐스트하는 대신 단일 전송을 사용하여 관심 있는 수신기 그룹에 멀티캐스트 IP 데이터그램을 전송하여 대역폭을 절약하는 데 사용하는 프로토콜 집합입니다. IP 멀티캐스트는 오디오 또는 비디오 스트리밍, IPTV, 화상 회의 및 뉴스 및 금융 데이터와 같은 기타 통신의 배포와 같은 하나의 소스(또는 여러 소스)에서 많은 수신기로의 통신에 적합합니다.

멀티캐스트 주소는 해당 주소로 가는 트래픽을 수신하려는 수신기 그룹을 식별합니다. 224.0.0.0 ~ 224.0.0.255 또는 239.0.0.0 ~ 239.255.255.255와 같이 특별한 용도로 예약된 멀티캐스트 주소는 사용하지 마십시오. 멀티캐스트 트래픽은 누락된 패킷을 다시 보내지 않는 UDP를 사용합니다.

Palo Alto Networks® 방화벽은 방화벽의 가상 라우터에 대해 구성한 레이어 3 인터페이스에서 IP 멀티캐스트 및 PIM(Protocol Independent Multicast)을 지원합니다.

멀티캐스트 라우팅의 경우 레이어 3 인터페이스 유형은 이더넷, 통합 이더넷(AE), VLAN, 루프백 또는 터널일 수 있습니다. 인터페이스 그룹을 사용하면 동일한 IGMP(Internet Group Management Protocol) 및 PIM 매개변수와 동일한 그룹 권한으로 한 번에 둘 이상의 방화벽 인터페이스를 구성할 수 있습니다(멀티캐스트 그룹은 모든 소스 또는 특정 소스의 트래픽만 허용). 인터페이스는 하나의 인터페이스 그룹에만 속할 수 있습니다.

방화벽은 IPv4 멀티캐스트를 지원하지만 IPv6 멀티캐스트는 지원하지 않습니다. 방화벽은 또한 레이어 2 또는 가상 와이어 인터페이스 유형에서 PIM-DM(PIM Dense Mode), IGMP 프록시, IGMP 정적 조인, Anycast RP, GRE 또는 멀티캐스트 구성을 지원하지 않습니다. 그러나 가상 유선 인터페이스는 멀티캐스트 패킷을 전달할 수 있습니다. 또한 레이어 2 인터페이스는 서로 다른 VLAN 간에 레이어 3 IPv4 멀티캐스트 패킷을 전환할 수 있으며 방화벽은 이그레스 인터페이스의 VLAN ID를 사용하여 VLAN ID에 태그를 다시 지정합니다.

인터페이스가 멀티캐스트 패킷을 수신하거나 전달하려면 가상 라우터에 대해 멀티캐스트를 활성화하고 수신 및 송신 인터페이스에 대해 PIM을 활성화해야 합니다. PIM 외에도 수신기를 향하는 이그레스 인터페이스에서 IGMP도 활성화해야 합니다. IP 멀티캐스트 트래픽을 멀티캐스트라는 미리 정의된 레이어 3 대상 영역 또는 모든 대상 영역으로 허용하도록 보안 정책 규칙을 구성해야 합니다.

- IGMP
- PIM
- IP 멀티캐스트 구성
- IP 멀티캐스트 정보 보기

IGMP

IGMP(Internet Group Management Protocol)는 멀티캐스트 수신기가 Palo Alto Networks® 방화벽의 인터페이스와 통신하는 데 사용하고 방화벽이 멀티캐스트 그룹의 구성원을 추적하는 데 사용하는 IPv4 프로토콜입니다. 호스트가 멀티캐스트 트래픽을 수신하려고 할 때 IGMP 구현은 IGMP Membership 보고 메시지를 보내고 수신 라우터는 차례로 호스트가 가입하려는 그룹의 멀티캐스트 그룹 주소로 PIM Join 메시지를 보냅니다. 동일한 물리적 네트워크(이더넷 세그먼트와 같이)에 있는 IGMP 지원 라우터는 PIM을 사용하여 다른 PIM 지원 라우터와 통신하여 소스에서 관심 있는 수신기까지의 경로를 결정합니다.

멀티캐스트 수신기와 마주하는 인터페이스에서만 IGMP를 활성화합니다. 수신기는 가상 라우터에서 단 하나의 레이어 3 홉 거리에 있을 수 있습니다. IGMP 메시지는 TTL 값이 1인 레이어 2 메시지이므로 LAN 외부로 나갈 수 없습니다.

IP 멀티캐스트를 구성할 때 인터페이스가 IGMP 버전 1, IGMP 버전 2 또는 IGMP 버전 3을 사용할지 지정합니다. IGMPv2 또는 IGMPv3을 사용하는 수신 IGMP 패킷에 IP 라우터 경고 옵션이 있도록 IP 라우터 경고 옵션인 RFC 2113을 적용할 수 있습니다.

기본적으로 인터페이스는 모든 멀티캐스트 그룹에 대한 IGMP 구성원 보고서를 수락합니다. 가상 라우터가 기본적으로 PIM-SM(PIM Sparse Mode)인 모든 소스(모든 소스 멀티캐스트 또는 ASM)의 구성원 보고서를 수락하는 그룹을 제어하기 위해 멀티캐스트 그룹 권한을 구성할 수 있습니다. 가상 라우터가 특정 소스(PIM Source-Specific Multicast[PIM-SSM])의 구성원 보고서를 수락하는 그룹을 지정할 수도 있습니다. ASM 또는 SSM 그룹에 대한 권한을 지정하면 가상 라우터는 다른 그룹의 구성원 보고서를 거부합니다. 인터페이스는 IGMPv3을 사용하여 PIM-SSM 트래픽을 전달해야 합니다.

IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 소스 수와 최대 멀티캐스트 그룹 수를 지정할 수 있습니다.

가상 라우터는 멀티캐스트 그룹의 모든 수신자에게 IGMP 쿼리를 일정한 간격으로 멀티캐스트합니다. 수신기는 수신기가 여전히 해당 그룹에 대한 멀티캐스트 트래픽을 수신하기를 원하는지 확인하는 IGMP 멤버십 보고서로 IGMP 쿼리에 응답합니다. 가상 라우터는 수신기가 있는 멀티캐스트 그룹의 테이블을 유지 관리합니다. 가상 라우터는 그룹에 가입된 해당 멀티캐스트 배포 트리 아래에 수신기가 있는 경우에만 인터페이스에서 다음 홉으로 멀티캐스트 패킷을 전달합니다. 가상 라우터는 그룹에 가입된 수신기를 정확히 추적하지 않습니다. 서브넷의 하나의 라우터만 IGMP 쿼리에 응답하며 이것이 IGMP 쿼리어(IP 주소가 가장 낮은 라우터)입니다.

IGMP 쿼리 간격과 수신기가 쿼리에 응답할 수 있는 시간(최대 쿼리 응답 시간)으로 인터페이스를 구성할 수 있습니다. 가상 라우터는 수신자로부터 IGMP Leave 메시지를 수신하여 그룹을 탈퇴할 때, 가상 라우터는 Leave 메시지를 수신한 인터페이스가 Immediate Leave 옵션으로 구성되지 않았는지 확인합니다. Immediate Leave 옵션이 없는 경우 가상 라우터는 그룹의 수신자 구성원이 아직 있는지 확인하기 위해 쿼리를 보냅니다. 마지막 구성원 쿼리 간격은 해당 그룹의 나머지 수신자가 응답하고 해당 그룹에 대한 멀티캐스트 트래픽을 여전히 원하는지 확인하는 데 허용되는 시간(초)을 지정합니다.

인터페이스는 IGMP 견고성 변수를 지원하므로 방화벽이 그룹 구성원 간격, 기타 쿼리 존재 간격, 시작 쿼리 수 및 마지막 구성원 쿼리 수를 조정하도록 조정할 수 있습니다. 더 높은 견고성 변수는 패킷을 삭제할 가능성이 있는 서브넷을 수용할 수 있습니다.

IP 멀티캐스트 정보 보기에서 IGMP 지원 인터페이스, IGMP 버전, 쿼리어 주소, 견고성 설정, 멀티캐스트 그룹 및 소스 수에 대한 제한, 인터페이스가 즉시 떠나도록 구성되었는지 여부를 확인할 수 있습니다. 인터페이스가 속한 멀티캐스트 그룹 및 기타 IGMP 구성원 정보도 볼 수 있습니다.

PIM

IP 멀티캐스트는 라우터 간의 PIM(Protocol Independent Multicast) 라우팅 프로토콜을 사용하여 멀티캐스트 패킷이 소스에서 수신자(멀티캐스트 그룹 구성원)로 이동하는 배포 트리의 경로를 결정합니다. 가상 라우터(레거시 라우팅 엔진)와 논리적 라우터(고급 라우팅 엔진)는 모두 PIM을 지원합니다.

Palo Alto Networks® 방화벽은 PIM-SM(PIM Sparse Mode)(RFC 4601), PIM ASM(Any-Source Multicast)(PIM Sparse 모드라고도 함) 및 PIM SSM(Source-Specific Multicast)을 지원합니다. PIM-SM에서 소스는 멀티캐스트 그룹에 속한 수신자(사용자)가 소스에 트래픽 전송을 요청할 때까지 멀티캐스트 트래픽을 전달하지 않습니다. 호스트가 멀티캐스트 트래픽을 수신하고자 할 때 IGMP 구현은 IGMP Membership 보고 메시지를 보내고, 수신 라우터는 가입하려는 그룹의 멀티캐스트 그룹 주소로 PIM Join 메시지를 보냅니다.

- **ASM**에서 수신자는 IGMP를 사용하여 멀티캐스트 그룹 주소에 대한 트래픽을 요청합니다. 모든 소스가 해당 트래픽을 발생시켰을 수 있습니다. 결과적으로 수신자가 발신자를 반드시 알 필요는 없으며 수신자는 관심이 없는 멀티캐스트 트래픽을 수신할 수 있습니다.
- **SSM**(RFC 4607)에서 수신기는 IGMP를 사용하여 하나 이상의 특정 소스에서 멀티캐스트 그룹 주소로 트래픽을 요청합니다. 수신자는 발신자의 IP 주소를 알고 원하는 멀티캐스트 트래픽만 수신합니다. SSM에는 IGMPv3가 필요합니다. 기본 SSM 주소 공간(232.0.0.0/8)은 소스별 주소 공간을 조정하여 재정의할 수 있습니다. 그룹 권한도 조정해야 합니다.

Palo Alto Networks 방화벽에서 IP 멀티캐스트를 구성할 때 수신기 쪽 인터페이스에서도 멀티캐스트 트래픽을 전달하는 인터페이스에 대해 PIM을 활성화해야 합니다. 이것은 수신기 쪽 인터페이스에서만 활성화되는 IGMP와 다릅니다.

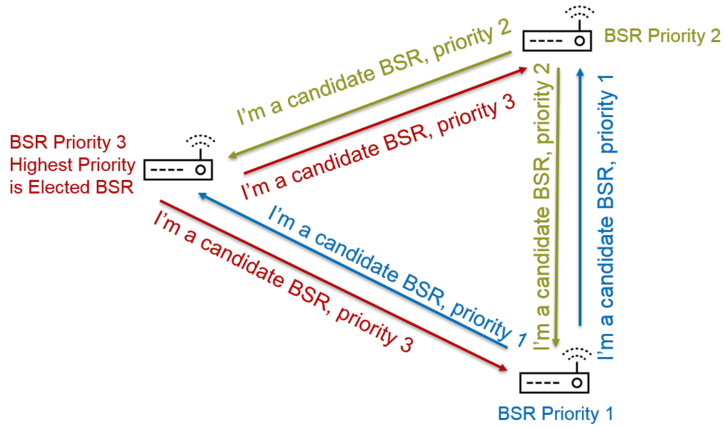
ASM에는 공유 배포 트리의 연결 지점이나 루트에 위치한 라우터인 ***RP***(Rendezvous Point)가 필요합니다. 멀티캐스트 도메인에 대한 RP는 모든 멀티캐스트 그룹 구성원이 가입 메시지를 보내는 단일 지점 역할을 합니다. 이 동작은 그룹 구성원이 여러 라우터에 참여 메시지를 보낸 경우 발생할 수 있는 라우팅 루프의 가능성을 줄입니다. (SSM은 소스별 멀티캐스트가 최단 경로 트리를 사용하므로 RP가 필요하지 않기 때문에 RP가 필요하지 않습니다.)

ASM 환경에서 가상 라우터가 멀티캐스트 그룹의 RP인 라우터를 결정하는 두 가지 방법이 있습니다.

- 정적 **RP-**그룹 매핑 - 방화벽의 가상 라우터가 멀티캐스트 그룹의 RP 역할을 하도록 구성합니다. 정적 RP 주소를 구성하거나 로컬 RP가 후보 RP이고 RP가 동적으로 선택되도록 지정하여 로컬 RP를 구성합니다(최저 우선 순위 값 기반). 또한 로컬 RP에서 다루지 않는 여러 그룹 주소 범위에 대해 하나 이상의 외부 RP를 정적으로 구성할 수 있습니다. 이렇게 하면 하나의 RP가 과부하되지 않도록 멀티캐스트 트래픽의 부하를 분산하는 데 도움이 됩니다.

- 부트스트랩 라우터**(Bootstrap Router, BSR)** - (RFC 5059)은 BSR의 역할을 정의합니다. 먼저 BSR 후보는 서로에게 우선순위를 알리고 다음 그림과 같이 우선순위가 가장 높은 후보가 BSR로 선출됩니다.

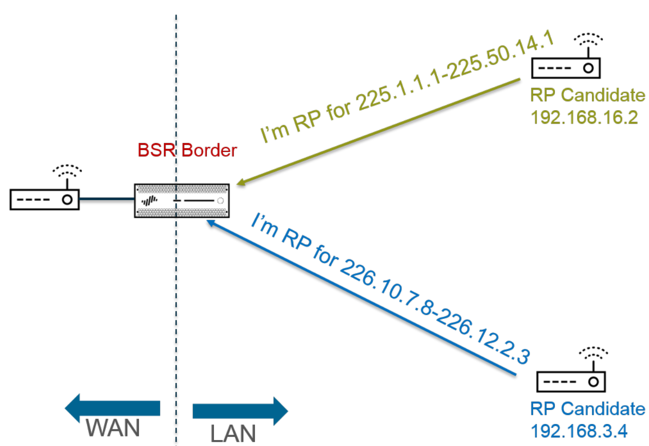
RPs Advertise Their BSR Candidacy; Highest Priority Wins



다음으로, BSR은 후보 RP가 자신의 IP 주소와 RP로 작동할 멀티캐스트 그룹 범위를 포함하는 BSR 메시지를 BSR에 주기적으로 유니캐스트할 때 RP를 발견합니다. 로컬 가상 라우터를 후보 RP로 구성할 수 있습니다. 이 경우 가상 라우터는 특정 멀티캐스트 그룹에 대한 RP 후보를 발표합니다. BSR은 RP 정보를 PIM 도메인의 다른 RP로 보냅니다.

인터페이스에 대해 PIM을 구성할 때 방화벽의 인터페이스가 엔터프라이즈 네트워크에서 반대쪽을 향하는 엔터프라이즈 경계에 있는 경우 BSR 경계를 선택할 수 있습니다. BSR 경계 설정은 방화벽이 LAN 외부에서 RP 후보 BSR 메시지를 보내는 것을 방지합니다. 다음 그림에서 BSR 경계는 LAN과 마주하는 인터페이스에 대해 활성화되어 있으며 해당 인터페이스의 우선순위가 가장 높습니다. 가상 라우터에 정적 RP와 동적 RP(BSR에서 학습)가 모두 있는 경우 로컬 정적 RP를 구성할 때 정적 RP가 그룹에 대해 학습된 RP를 재정의해야 하는지 여부를 지정할 수 있습니다.

BSR Border Router Discovers RPs;
Keeps PIM RP Candidacy Messages Within LAN



PIM 스파스 모드가 공유 트리를 보낼 트래픽이 있음을 RP에 알리려면 RP가 소스를 알고 있어야 합니다. 호스트는 지정된 라우터(DR)가 호스트의 첫 번째 패킷을 PIM 레지스터 메시지로 캡슐화하고 패킷을 로컬 네트워크의 RP로 유니캐스트할 때 멀티캐스트 그룹 주소로 트래픽을 보내고 있음을 RP에 알립니다.

DR은 또한 수신기에서 RP로 Prune 메시지를 전달합니다. RP는 멀티캐스트 그룹으로 보내는 소스의 IP 주소 목록을 유지 관리하고 RP는 소스에서 멀티캐스트 패킷을 전달할 수 있습니다.

PIM 도메인의 라우터에 DR이 필요한 이유는 무엇입니까? 라우터가 스위치에 PIM Join 메시지를 보내면 두 라우터가 이를 수신하여 동일한 RP로 전달할 수 있어 트래픽이 중복되고 대역폭이 낭비됩니다. 불필요한 트래픽을 방지하기 위해 PIM 라우터는 DR(IP 주소가 가장 높은 라우터)을 선택하고 DR만 RP에 Join 메시지를 전달합니다. 또는 IP 주소 비교보다 우선하는 인터페이스 그룹에 DR 우선 순위를 할당할 수 있습니다. 참고로 DR은 PIM 메시지를 전달(유니캐스팅)하고 있습니다. IP 멀티캐스트 패킷을 멀티캐스팅하지 않습니다.

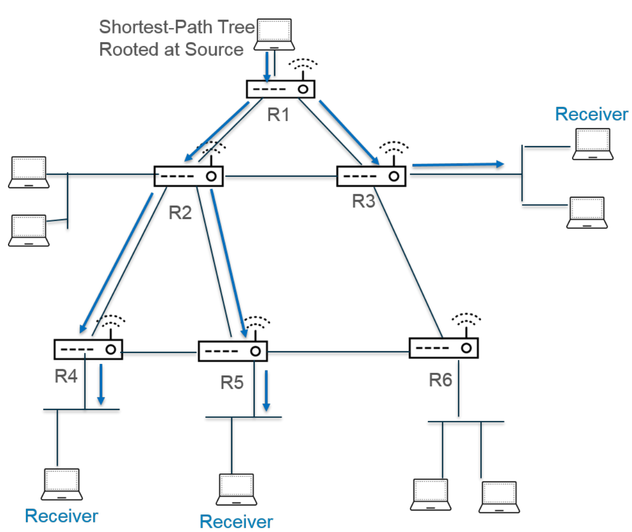
인터페이스 그룹이 가상 라우터와 피어링하도록 허용할 PIM 이웃(라우터)의 IP 주소를 지정할 수 있습니다. 기본적으로 모든 PIM 지원 라우터는 PIM 인접 라우터가 될 수 있지만 인접 라우터를 제한하는 옵션은 PIM 환경에서 가상 라우터를 보호하는 단계를 제공합니다.

- 최단 경로 트리(SPT) 및 공유 트리
- PIM 어설션 메커니즘
- 역방향 경로 전달

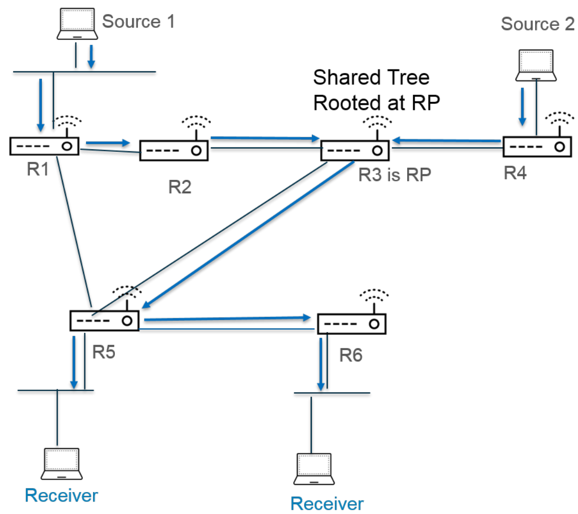
최단 경로 트리(SPT) 및 공유 트리

수신기가 멀티캐스트 그룹에 가입한 후 다중 액세스 네트워크의 라우터는 그룹의 각 수신자에게 데이터를 보내는 데 필요한 라우팅 경로를 작성합니다. 멀티캐스트 그룹으로 전송된 각 IP 데이터그램은 모든 구성원에게 배포(포워딩)됩니다. 라우팅 경로는 멀티캐스트 패킷에 대한 배포 트리 유형을 구성합니다. 멀티캐스트 배포 트리의 목표는 패킷이 경로의 분기에 도달하고 라우터가 모든 그룹 구성원에 도달하기 위해 여러 경로로 패킷을 보내야 할 때 라우터가 멀티캐스트 패킷을 복제하는 것이지만, 배포 트리는 관심 있는 수신기가 없는 경로로 패킷을 보내지 않아야 합니다. 배포 트리는 다음 중 하나입니다.

- 소스 트리 - 멀티캐스트 소스(트리의 루트)에서 네트워크를 거쳐 멀티캐스트 그룹의 수신기까지의 경로입니다. 소스 트리는 멀티캐스트 패킷이 소스에서 수신기로 가져갈 수 있는 최단 경로이므로 **SPT(**최단 경로 트리**)**라고도 합니다. 발신자와 수신자는 소스 및 멀티캐스트 그룹 쌍으로 주석이 추가되며 (S, G)로 단축됩니다(예: (192.168.1.1, 225.9.2.6). 다음 그림은 소스에서 세 개의 수신기에 이르는 세 개의 최단 경로 트리를 보여 줍니다.



- 공유 트리 - 멀티캐스트 소스가 아닌 RP에 루팅된 경로입니다. 공유 트리는 RP 트리 또는 RPT라고도 합니다. 라우터는 다양한 소스의 멀티캐스트 패킷을 RP로 포워딩하고 RP는 패킷을 공유 트리로 포워딩합니다. 멀티캐스트 그룹에 속하는 모든 소스가 RP와 동일한 배포 트리를 공유하므로 공유 트리는 와일드카드를 소스로 사용하여 (*, G)로 주석이 표시됩니다. 공유 트리 주석의 예는 (*, 226.3.1.5)입니다. 다음 그림은 RP의 루트에서 수신기까지의 공유 트리를 보여 줍니다.



소스별 멀티캐스트(SSM)는 소스 트리 배포를 사용합니다. ASM(모든 소스 멀티캐스트)을 사용하도록 IP 멀티캐스트를 구성하는 경우 그룹에 대한 SPT 임계값을 설정하여 Palo Alto Networks® 방화벽의 가상 라우터가 멀티캐스트 패킷을 그룹에 포워딩하는 데 사용하는 배포 트리를 지정할 수 있습니다.

- 기본적으로 가상 라우터는 그룹이나 접두사(**SPT** 임계값이 0으로 설정됨)에 대한 첫 번째 멀티캐스트 패킷을 수신할 때 멀티캐스트 라우팅을 공유 트리에서 SPT로 전환합니다.
- 임의의 시간 동안 인터페이스에서 지정된 멀티캐스트 그룹 또는 접두사에 도달하는 패킷의 총 킬로비트 수가 구성된 수에 도달하면 가상 라우터를 SPT로 전환하도록 구성할 수 있습니다.
- 그룹 또는 접두사(공유 트리를 계속 사용)에 대해 SPT로 전환하지 않도록 가상 라우터를 구성할 수 있습니다.

SPT에는 더 많은 메모리가 필요하므로 그룹에 대한 멀티캐스트 트래픽 수준에 따라 설정을 선택합니다. 가상 라우터가 SPT로 전환되면 패킷은 RP가 아닌 소스에서 도착하고 가상 라우터는 RP에 Prune 메시지를 보냅니다. 소스는 해당 그룹에 대한 후속 멀티캐스트 패킷을 최단 경로 트리로 보냅니다.

PIM 어설션 메커니즘

다중 액세스 네트워크의 라우터가 동일한 멀티캐스트 트래픽을 동일한 다음 홉으로 전달하는 것을 방지하기 위해(이 경우 중복 트래픽 및 대역폭 낭비가 발생함) PIM은 Assert 메커니즘을 사용하여 다중 액세스 네트워크에 대해 단일 PIM 포워더를 선택합니다.

가상 라우터가 패킷에서 식별된 동일한(S,G) 쌍에 대한 OI(outgoing interface)로 가상 라우터가 이미 연결한 인터페이스의 소스에서 멀티캐스트 패킷을 수신하는 경우 이는 중복 패킷임을 의미합니다. 결과적으로 가상 라우터는 메트릭이 포함된 Assert 메시지를 다중 액세스 네트워크의 다른 라우터로 보냅니다. 그런 다음 라우터는 다음과 같은 방식으로 PIM 포워더를 선택합니다.

1. PIM 포워더는 멀티캐스트 소스에 대한 관리 거리(administrative distance)가 가장 낮은 라우터입니다.

2. 관리 거리가 가장 낮은 경우 PIM 포워더가 소스에 대한 최상의 유니캐스트 라우팅 메트릭을 가진 라우터입니다.
3. 최상의 메트릭이 동점인 경우 PIM 포워더가 가장 높은 IP 주소를 가진 라우터입니다.

PIM 포워더로 선택되지 않은 라우터는(S,G) 쌍에서 식별된 멀티캐스트 그룹으로 트래픽 포워딩을 중지합니다.

IP 멀티캐스트를 구성할 때 가상 라우터가 PIM Assert 메시지를 인터페이스로 보내는 인터벌(Assert interval)을 구성할 수 있습니다. IP 멀티캐스트 정보를 볼 때 **PIM** 인터페이스 탭에 인터페이스에 대한 Assert 인터벌이 표시됩니다.

역방향 경로 전달

PIM은 역방향 경로 포워딩(RPF)을 사용하여 가상 라우터의 유니캐스트 라우팅 테이블을 활용하여 멀티캐스트 라우팅 루프를 방지합니다. 가상 라우터가 멀티캐스트 패킷을 받으면 해당 소스 IP 주소와 연결된 나가는 인터페이스가 해당 패킷이 도착한 인터페이스인지 확인하기 위해 유니캐스트 라우팅 테이블에서 멀티캐스트 패킷의 소스를 찾습니다. 인터페이스가 일치하면 가상 라우터는 패킷을 복사하고 그룹의 멀티캐스트 수신기쪽으로 인터페이스를 포워딩합니다. 인터페이스가 일치하지 않으면 가상 라우터가 패킷을 삭제합니다. 유니캐스트 라우팅 테이블은 OSPF와 같이 네트워크에서 사용하는 기본 정적 경로 또는 IGP(내부 게이트웨이 프로토콜)를 기반으로 합니다.

PIM은 또한 RPF를 사용하여 한 번에 하나의 PIM 라우터 홉을 소스로 가장 짧은 경로 트리를 구축합니다. 가상 라우터는 멀티캐스트 소스의 주소를 가지고 있으므로 가상 라우터는 가상 라우터가 유니캐스트 패킷을 소스로 포워딩하는 데 사용할 업스트림 PIM 이웃 소스로 다시 홉으로 선택합니다. 다음 홉 라우터도 동일한 작업을 수행합니다.

RPF가 성공하고 가상 라우터가 mRIB(멀티캐스트 라우팅 정보 기반)에 경로 항목을 갖고 나면 가상 라우터는 멀티캐스트 포워딩 정보 기반(멀티캐스트 포워딩 테이블 또는 mFIB)에서 소스 기반 트리 항목(S,G)과 공유 트리 항목 (*,G)을 유지 관리합니다. 각 항목에는 소스 IP 주소, 멀티캐스트 그룹, 들어오는 인터페이스(RPF 인터페이스) 및 나가는 인터페이스 목록이 포함됩니다. 최단 경로 트리는 라우터에서 분기할 수 있고 라우터는 다른 경로 아래에 있는 그룹의 수신기에 도달하기 위해 패킷을 여러 인터페이스로 전달해야 하기 때문에 항목에 대해 나가는 인터페이스가 여러 개 있을 수 있습니다. 가상 라우터가 mFIB를 사용하여 멀티캐스트 패킷을 포워딩하면 (*,G) 항목을 일치시키려고 시도하기 전에 (S, G) 항목과 일치합니다.

멀티캐스트 소스 접두사를 BGP에 광고하는 경우(IPv4 주소 패밀리 및 멀티캐스트 후속 주소 패밀리로 MP-BGP를 구성) 방화벽은 항상 멀티캐스트 후속 주소 패밀리에서 받은 방화벽이 BGP 경로에서 RPF 검사를 수행합니다.

IP 멀티캐스트 정보를 확인하여 mFIB 및 mRIB 항목을 보는 방법을 확인합니다. 멀티캐스트 경로 테이블(mRIB)은 유니캐스트 경로 테이블(RIB)과 별도의 테이블입니다.

IP 멀티캐스트 구성

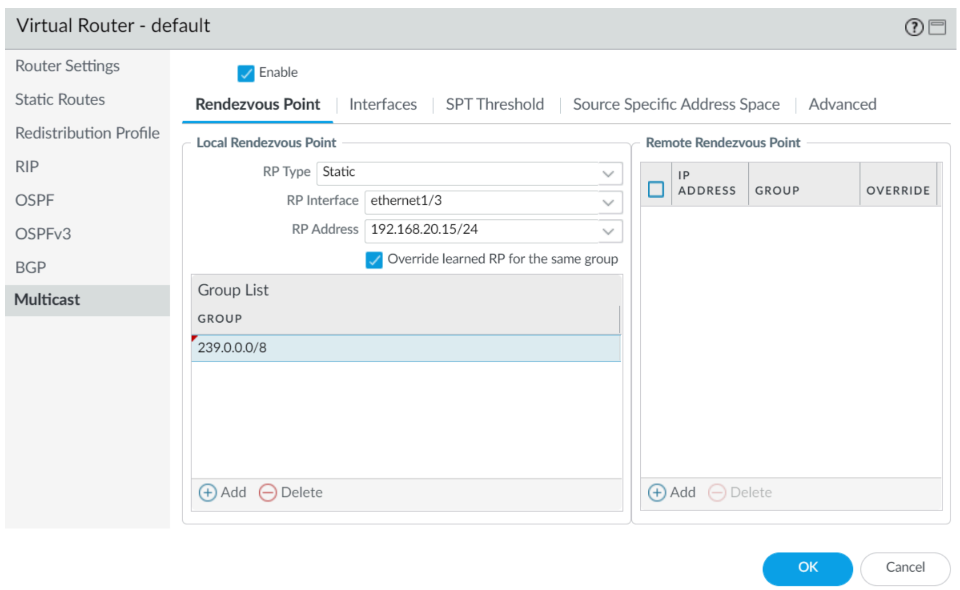
Palo Alto Networks® 방화벽의 가상 라우터에서 인터페이스를 구성하여 IP 멀티캐스트 패킷을 수신하고 전달합니다. 가상 라우터에 대해 IP 멀티캐스트를 활성화하고 수신 및 송신 인터페이스에서 PIM(Protocol Independent Multicast)을 구성하고 수신기 측 인터페이스에서 IGMP(Internet Group Management Protocol)를 구성해야 합니다.

STEP 1 | 가상 라우터에 대해 IP 멀티캐스트를 활성화합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. 멀티캐스트 및 IP 멀티캐스트 활성화를 선택합니다.

STEP 2 | (ASM에만 해당) 가상 라우터가 있는 멀티캐스트 도메인에서 ASM(모든 소스 멀티캐스트)을 사용하는 경우 멀티캐스트 그룹에 대한 로컬 및 원격 랑데부 지점(RP)을 식별하고 구성합니다.

1. 랑데부 포인트를 선택합니다.
2. **RP** 선택 방법을 결정하는 로컬 **RP** 유형을 선택합니다(옵션은 정적, 후보 또는 없음).
   - 정적 - 멀티캐스트 그룹에 대한 RP의 정적 매ping을 설정합니다. 정적 RP를 구성하려면 PIM 도메인의 다른 PIM 라우터에서 동일한 RP를 명시적으로 구성해야 합니다.
     - **RP** 인터페이스를 선택합니다. 유효한 인터페이스 유형은 Layer3, 가상 와이어, 루프백, VLAN, 집계 이더넷(AE) 및 터널입니다.
     - **RP** 주소를 선택합니다. 선택한 RP 인터페이스의 IP 주소가 목록을 채웁니다.
     - 이 정적 RP가 그룹 목록의 그룹에 대해 선택된 RP 대신 RP 역할을 하도록 동일한 그룹에 대해 학습된 **RP** 재정의를 선택합니다.
     - RP가 RP 역할을 하는 하나 이상의 멀티캐스트 그룹을 추가합니다.



   - 후보 - 우선 순위를 기반으로 멀티캐스트 그룹에 대한 RP의 동적 매ping을 설정하여 PIM 도메인의 각 라우터가 자동으로 동일한 RP를 선택하도록 합니다.
     - 후보 RP의 **RP** 인터페이스를 선택합니다. 유효한 인터페이스 유형은 레이어 3, 루프백, VLAN, 통합 이더넷(AE) 및 터널입니다.
     - 후보 RP의 **RP** 주소를 선택합니다. 선택한 RP 인터페이스의 IP 주소가 목록을 채웁니다.
     - (선택 사항) 후보 RP의 우선 순위를 변경합니다. 방화벽은 후보 RP의 우선 순위를 다른 후보 RP의 우선 순위와 비교하여 지정된 그룹에 대한 RP 역할을 결정합니다. 방화벽은 우선 순위 값이 가장 낮은 후보 RP를 선택합니다(범위는 0~255, 기본값은 192).
     - (선택 사항) 광고 간격**(**초**)**을 변경합니다(범위는 1~26,214, 기본값은 60).
     - RP와 통신하는 멀티캐스트 그룹의 그룹 목록을 입력합니다.
   - 없음 - 이 가상 라우터가 RP가 아닌 경우 선택합니다.
3. 원격 랑데부 지점을 추가하고 해당 원격(외부) RP의 **IP** 주소를 입력합니다.
4. 지정된 원격 RP 주소가 RP 역할을 하는 멀티캐스트 그룹 주소를 추가합니다.

5. 그룹 주소 목록의 그룹에 대해 동적으로 학습(선택) 되는 RP 대신 구성한 외부 RP가 정적으로 RP 역할을 하도록 동일한 그룹에 대해 학습한 **RP** 재정의를 선택합니다.
6. 확인을 클릭합니다.

STEP 3 | 멀티캐스트 구성(IGMP, PIM 및 그룹 권한)을 공유하는 인터페이스 그룹을 지정합니다.

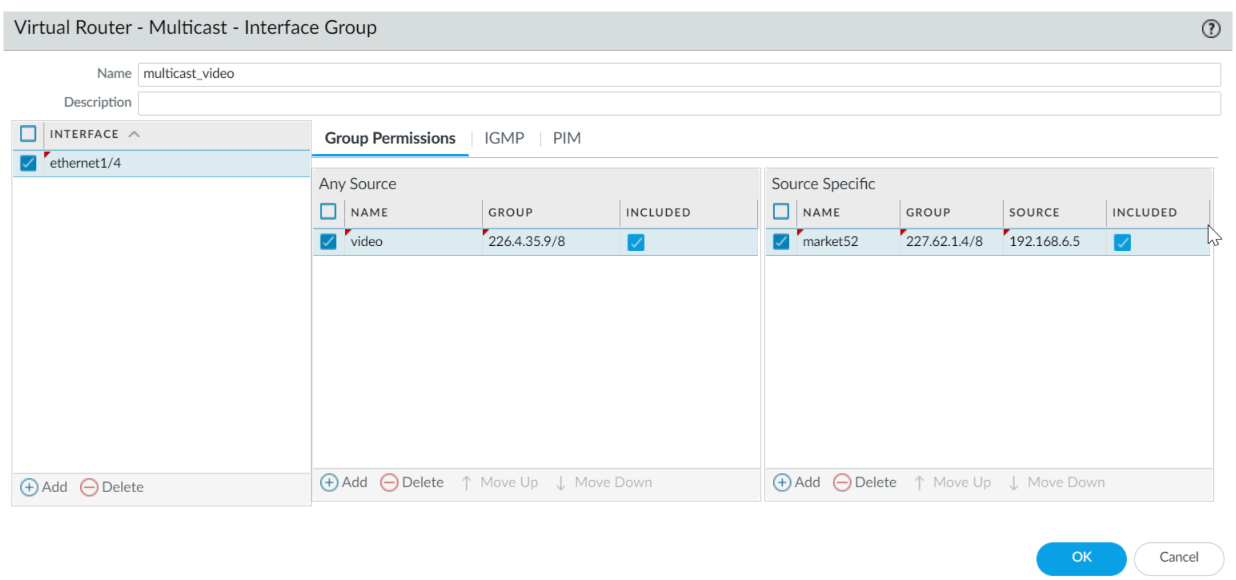
1. 인터페이스 탭에서 인터페이스 그룹의 이름을 추가합니다.
2. 설명을 입력합니다.
3. 인터페이스를 추가하고 인터페이스 그룹에 속한 레이어 3 인터페이스를 하나 이상 선택합니다.

STEP 4 | (선택 사항) 인터페이스 그룹에 대한 멀티캐스트 그룹 권한을 구성합니다. 기본적으로 인터페이스 그룹은 모든 그룹의 IGMP 멤버 자격 보고서와 PIM 조인 메시지를 수락합니다.

1. 그룹 권한을 선택합니다.
2. 이 인터페이스 그룹에 대한 모든 소스 멀티캐스트(ASM) 그룹을 구성하려면 모든 소스 창에서 이름 추가를 선택하여 소스의 IGMP 멤버 자격 보고서 및 PIM 조인 메시지를 수락하는 멀티캐스트 그룹을 식별합니다.
3. 이러한 인터페이스의 모든 소스에서 멀티캐스트 패킷을 수신할 수 있는 멀티캐스트 그룹 주소 또는 그룹 주소 및 /prefix를 입력합니다.
4. 인터페이스 그룹에 ASM 그룹 주소를 포함하려면 포함됨을 선택합니다(기본값). 테스트 중과 같이 인터페이스 그룹에서 ASM 그룹을 쉽게 제외하려면 포함됨을 선택 취소합니다.
5. 모든 소스에서 멀티캐스트 패킷을 수신하려는 추가 멀티캐스트 그룹(인터페이스 그룹의 경우)을 추가합니다.
6. 이 인터페이스 그룹에서 소스 특정 멀티캐스트(SSM) 그룹을 구성하려면 소스 특정 창에서 멀티캐스트 그룹과 소스 주소 쌍을 식별하기 위해 추가 이름을 입력합니다. 모든 소스 멀티캐스트에 사용한 이름을 사용하지 마십시오. (SSM을 구성하려면 IGMPv3를 사용해야 합니다.)
7. 지정된 소스에서만 멀티캐스트 패킷을 수신하고 이러한 인터페이스에서 패킷을 수신할 수 있는 그룹의 멀티캐스트 그룹 주소 또는 그룹 주소 및 /prefix를 입력합니다.

   권한을 지정하는 소스 특정 그룹은 가상 라우터가 소스 특정으로 처리해야 하는 그룹입니다. 권한을 구성한 소스별 그룹을 포함하는 소스 특정 주소 공간(단계9)을 구성합니다.

8. 이 멀티캐스트 그룹이 멀티캐스트 패킷을 수신할 수 있는 소스 IP 주소를 입력합니다.
9. 인터페이스 그룹에 SSM 그룹과 소스 주소 쌍을 포함하려면 포함됨을 선택합니다(기본값). 테스트 중과 같이 인터페이스 그룹에서 페어를 쉽게 제외하려면 포함됨을 선택 취소합니다.
10. 특정 소스에서만 멀티캐스트 패킷을 수신하는 추가 멀티캐스트 그룹(인터페이스 그룹용)을 추가합니다.



STEP 5 | 인터페이스가 그룹에 가입하기 위해 IGMP를 사용해야 하는 멀티캐스트 수신기에 직면하는 경우 인터페이스 그룹에 대해 IGMP를 구성합니다.

1. **IGMP** 탭에서 IGMP 활성화(기본값)를 선택합니다.
2. 인터페이스 그룹의 인터페이스에 대한 IGMP 매개변수를 지정합니다.

   - **IGMP** 버전 - **1**, **2** 또는 **3**(기본값).
   - 라우터 경고 **IP** 옵션 적용(기본적으로 비활성화됨) - IGMPv2 또는 IGMPv3을 사용하는 수신 IGMP 패킷에 IP 라우터 경고 옵션, RFC 2113이 있어야 하는 경우 이 옵션을 선택합니다.
   - 견고성 - 방화벽이 그룹 구성원 간격, 기타 쿼리 존재 간격, 시작 쿼리 수 및 마지막 구성원 쿼리 수를 조정하는 데 사용하는 변수입니다(범위는 1~7, 기본값은 2). 이 방화벽이 있는 서브넷에서 패킷이 손실되기 쉬운 경우 값을 늘리십시오.
   - **Max Sources** - IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 소스 수입니다(범위는 1~65,535, 기본값은 무제한).
   - **Max Groups** - IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 그룹 수입니다(범위는 1~65,535, 기본값은 무제한).
   - 쿼리 간격 - 수신기가 그룹에 대한 멀티캐스트 패킷을 수신하기를 원하는지 여부를 결정하기 위해 가상 라우터가 수신기에 보내는 IGMP 멤버십 쿼리 메시지 사이의 시간(초)입니다(범위는 1~31,744, 기본값은 125).
   - **Max Query Response Time(**초**)** - 가상 라우터가 수신기가 그룹에 대한 멀티캐스트 패킷을 더 이상 수신하기를 원하지 않는다고 결정하기 전에 수신기가 IGMP 구성원 쿼리 메시지에 응답하는 데 허용되는 최대 시간(초)(범위는 0 ~ 3,174.4, 기본값 10)이다.
   - 마지막 구성원 쿼리 간격**(**초**)** - 수신기가 그룹 탈퇴 메시지를 보낸 후 가상 라우터가 보내는 그룹별 쿼리에 수신기가 응답하는 데 허용되는 시간(초)입니다(범위는 0.1~3,174.4, 기본값은 1).
   - **Immediate Leave**(기본적으로 비활성화됨) - 멀티캐스트 그룹에 구성원이 하나만 있고 가상 라우터가 해당 그룹에 대한 IGMP Leave 메시지를 수신하는 경우 Immediate Leave 설정은 가상 라우터가 멀티캐스트 라우팅에서 해당 그룹과 나가는 인터페이스를 제거하도록 합니다. 마지막 구성원 쿼리 간격이 만료될 때까지 기다리지 않고 즉시 정보 기반(mRIB) 및 멀티캐스트 전달 정보 기반(mFIB)을 사용할 수 있습니다. 즉시 나가기 설정은 네트워크 리소스를 절약합니다. 인터페이스 그룹이 IGMPv1을 사용하는 경우 즉시 나가기를 선택할 수 없습니다.

STEP 6 | 인터페이스 그룹에 대해 PIM-SM(PIM Sparse Mode)을 구성합니다.

1. **PIM** 탭에서 PIM 활성화(기본적으로 활성화됨)를 선택합니다.
2. 인터페이스 그룹에 대한 PIM 매개변수를 지정합니다.
   - **Assert Interval** - 가상 라우터가 PIM 전달자를 선택할 때 다중 액세스 네트워크의 다른 PIM 라우터에 보내는 PIM Assert 메시지 사이의 시간(초)입니다(범위는 0 ~ 65,534, 기본값은 177).
   - **Hello** 간격 - 가상 라우터가 인터페이스 그룹의 각 인터페이스에서 PIM 이웃으로 보내는 PIM Hello 메시지 사이의 시간(초)입니다(범위는 0 ~ 18,000, 기본값은 30).
   - 조인 정리 간격 - 가상 라우터가 멀티캐스트 소스를 향해 업스트림으로 보내는 PIM 조인 메시지 간(및 PIM 정리 메시지 간) 시간(범위는 0~18,000, 기본값은 60)입니다.
   - **DR** 우선 순위 - 다중 액세스 네트워크에서 PIM 결합 및 정리 메시지를 RP로 전달하는 라우터를 제어하는 DR(지정된 라우터) 우선 순위(범위는 0~429,467,295, 기본값은 1)입니다. DR 우선 순위는 DR을 선택하기 위해 IP 주소 비교보다 우선합니다.
   - **BSR** 경계 - 인터페이스 그룹의 인터페이스가 엔터프라이즈 LAN 경계에 있는 BSR인 가상 라우터에 있는 경우 이 옵션을 선택합니다. 이는 RP 후보 BSR 메시지가 LAN을 떠나는 것을 방지합니다.
3. 가상 라우터가 멀티캐스트 패킷을 수락하는 각 라우터의 **IP** 주소를 지정하여 하나 이상의 허용된 **PIM** 이웃을 추가합니다.

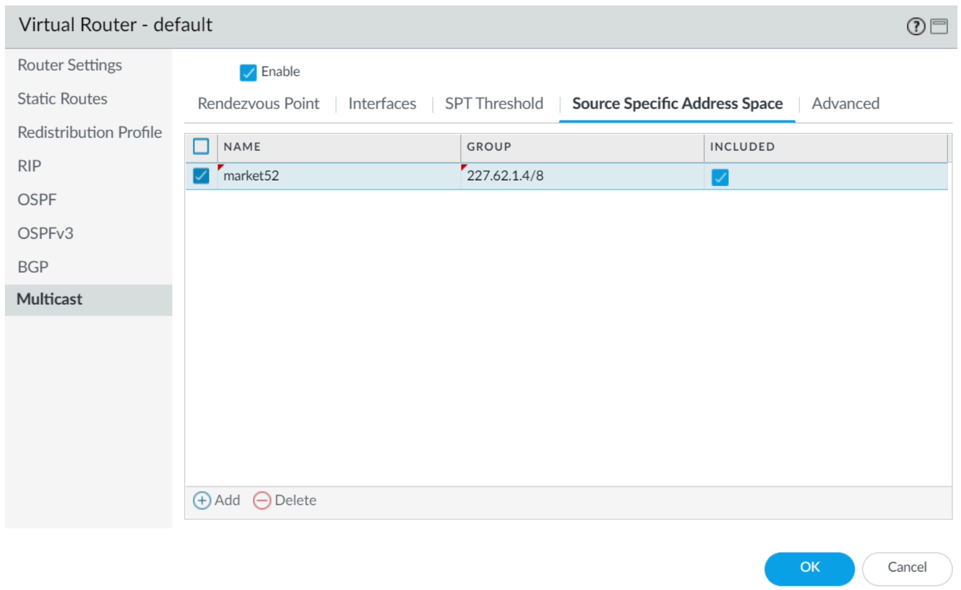
STEP 7 | 확인을 클릭하여 인터페이스 그룹 설정을 저장합니다.

STEP 8 | (선택 사항) 최단 경로 트리(SPT) 및 공유 트리에 설명된 대로 최단 경로 트리(SPT) 임계값을 변경합니다.

1. **SPT** 임계값을 선택하고 배포 트리를 지정할 멀티캐스트 그룹 또는 접두사인 멀티캐스트 그룹**/**접두사를 추가합니다.
2. 임계값**(kb)** 지정 - 지정된 멀티캐스트 그룹 또는 접두사로의 라우팅이 공유 트리(RP에서 제공됨)에서 SPT 배포로 전환되는 지점:
   - **0(**첫 번째 데이터 패킷 켜기**)**(기본값) - 가상 라우터가 그룹 또는 접두사에 대한 첫 번째 데이터 패킷을 수신하면 가상 라우터가 공유 트리에서 그룹 또는 접두사에 대한 SPT로 전환합니다.
   - 안 함**(spt**로 전환하지 않음**)** - 가상 라우터는 계속해서 공유 트리를 사용하여 패킷을 그룹 또는 접두사로 전달합니다.
   - 가상 라우터가 해당 멀티캐스트 그룹 또는 접두사에 대한 SPT 배포로 변경되는 모든 인터페이스에서 임의의 기간 동안 멀티캐스트 그룹 또는 접두사에 도달할 수 있는 멀티캐스트 패킷의 총 킬로비트 수를 입력합니다.

STEP 9 | 특정 소스의 멀티캐스트 패킷만 허용하는 멀티캐스트 그룹 또는 그룹 및 접두사를 식별합니다.

1. 소스별 주소 공간을 선택하고 스페이스의 이름을 추가합니다.
2. 특정 소스에서 멀티캐스트 패킷을 수신하는 주소 공간을 식별하려면 접두사 길이와 함께 멀티캐스트 그룹 주소를 입력합니다. 가상 라우터가 SSM 그룹에 대한 멀티캐스트 패킷을 수신하지만 그룹이 소스 특정 주소 공간에 포함되지 않는 경우 가상 라우터는 패킷을 삭제합니다.
3. 가상 라우터가 허용된 특정 소스에서 시작된 멀티캐스트 패킷을 수락할 멀티캐스트 그룹 주소 범위로 소스별 주소 공간을 포함하려면 포함됨을 선택합니다. 테스트를 위해 그룹 주소 공간을 쉽게 제외하려면 포함됨을 선택 취소합니다.
4. SSM 그룹 권한을 지정한 모든 그룹을 포함하도록 다른 소스별 주소 공간을 추가합니다.



STEP 10 | (선택 사항) 멀티캐스트 그룹과 소스 간에 세션이 종료된 후 멀티캐스트 경로가 MRib에 남아 있는 시간을 변경합니다.

1. 고급 탭을 선택합니다.
2. 멀티캐스트 경로 만료 시간**(**초**)**을 지정합니다(범위는 210~7,200, 기본값은 210).

STEP 11 | 확인을 클릭하여 멀티캐스트 구성을 저장합니다.

STEP 12 | 대상 영역에 대한 멀티캐스트 트래픽을 허용하는 보안 정책 규칙을 만듭니다.

1. 보안 정책 규칙을 만들고 대상 탭에서 대상 영역에 대해 멀티캐스트 또는 임의를 선택합니다. 멀티캐스트 영역은 모든 멀티캐스트 트래픽과 일치하는 미리 정의된 레이어 3 영역입니다. 대상 주소는 멀티캐스트 그룹 주소일 수 있습니다.
2. 나머지 보안 정책 규칙을 구성합니다.

STEP 13 | (선택 사항) 경로를 설정하기 전에 멀티캐스트 패킷의 버퍼링을 활성화합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. 멀티캐스트 경로 설정 버퍼링을 활성화합니다(기본적으로 비활성화됨). 방화벽은 해당 멀티캐스트 그룹에 대한 항목이 mFIB(멀티캐스트 전달 테이블)에 아직 존재하지 않는 경우 멀티캐스트 흐름의 첫 번째 패킷을 보존할 수 있습니다. 버퍼 크기는 방화벽이 흐름에서 버퍼링하는 패킷 수

를 제어합니다. mFIB에 경로가 설치된 후 방화벽은 버퍼링된 첫 번째 패킷을 수신기에 자동으로 전달합니다. (콘텐츠 서버가 방화벽에 직접 연결되어 있고 멀티캐스트 애플리케이션이 삭제되는 흐름의 첫 번째 패킷을 견딜 수 없는 경우에만 멀티캐스트 경로 설정 버퍼링을 활성화해야 합니다.)

3. (선택 사항) 버퍼 크기를 변경합니다. 버퍼 크기는 mFIB 항목이 설정될 때까지 방화벽이 버퍼링할 수 있는 멀티캐스트 흐름당 패킷 수입니다(범위는 1~2,000, 기본값은 1,000). 방화벽은 총 5,000개의 패킷을 버퍼링할 수 있습니다(모든 흐름에 대해).
4. 확인을 클릭합니다.

STEP 14 | 변경 사항을 커밋합니다.

STEP 15 | IP 멀티캐스트 정보를 확인하여 MRib 및 MFIB 항목, IGMP 인터페이스 설정, IGMP 그룹 구성원 자격, PIM ASM 및 SSM 모드, RP에 대한 그룹 매ping, DR 주소, PIM 설정, PIM 이웃 등을 볼 수 있습니다.

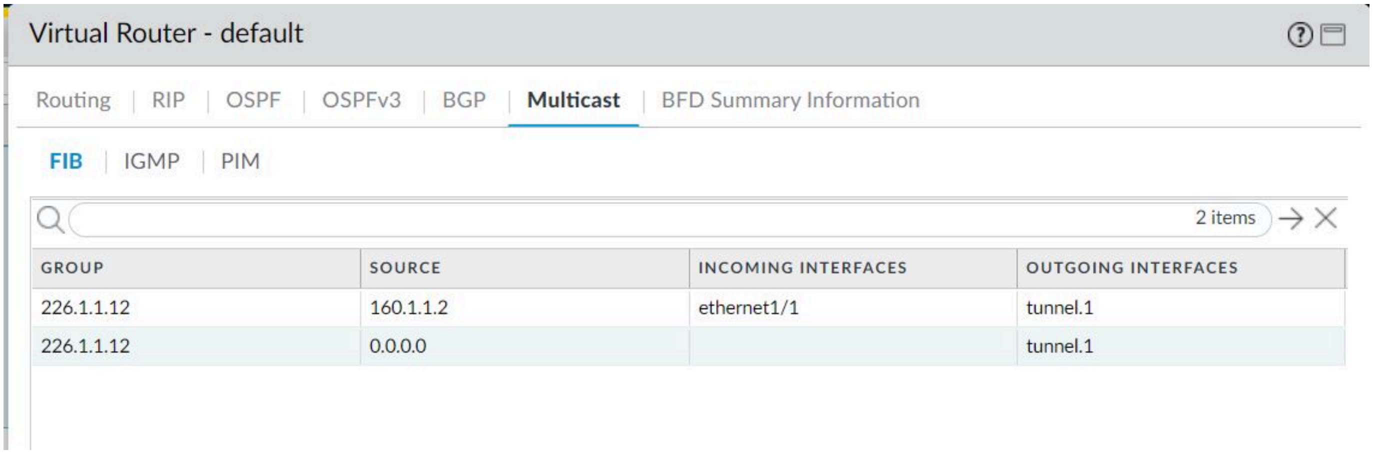
STEP 16 | 멀티캐스트 트래픽에 대해 정적 경로를 구성하는 경우 멀티캐스트 라우팅 테이블(유니캐스트 라우팅 테이블이 아님)에만 경로를 설치하여 멀티캐스트 트래픽에만 경로를 사용할 수 있습니다.

STEP 17 | IP 멀티캐스트를 사용하도록 설정하는 경우 논리적 유니캐스트 토폴로지와 별도의 논리적 멀티캐스트 토폴로지가 없는 한 IPv4 멀티캐스트용 MP-BGP를 사용하여 BGP를 구성할 필요가 없습니다. 멀티캐스트 후속 주소 패밀리에서 멀티캐스트 소스 접두사를 BGP에 보급하려는 경우에만 IPv4 주소 패밀리 및 멀티캐스트 후속 주소 패밀리로 MP-BGP 확장을 구성합니다.

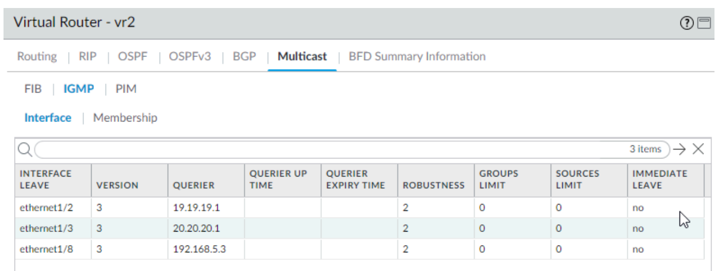
IP 멀티캐스트 정보 보기

IP 멀티캐스트 라우팅을 구성한 후 멀티캐스트 경로, 전달 항목 및 IGMP 및 PIM 인터페이스에 대한 정보를 확인합니다.

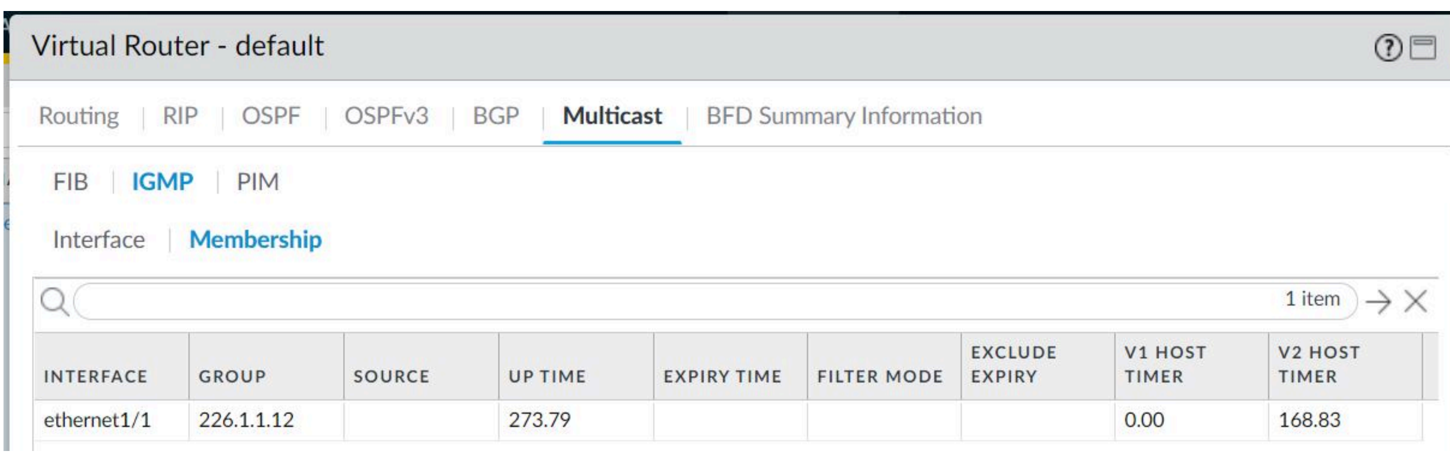
- 네트워크 > 가상 라우터를 선택하고 구성한 가상 라우터의 행에서 추가 런타임 통계를 클릭합니다.
  1. 라우팅 > 라우팅 테이블을 선택한 다음 멀티캐스트 라디오 버튼을 선택하여 멀티캐스트 경로만(대상 IP 멀티캐스트 그룹, 해당 그룹에 대한 다음 홉 및 발신 인터페이스) 표시합니다. 이 정보는 MRib에서 가져온 것입니다.
  2. 멀티캐스트 > **FIB**를 선택하여 MFIB의 멀티캐스트 경로 정보(가상 라우터가 속한 멀티캐스트 그룹, 해당 소스, 수신 인터페이스 및 수신기에 대한 발신 인터페이스)를 봅니다.



  3. 멀티캐스트 > **IGMP** > 인터페이스를 선택하여 IGMP 지원 인터페이스, 관련 IGMP 버전, IGMP 쿼리자의 IP 주소, 쿼리자 가동 시간 및 만료 시간, 견고성 설정, 멀티캐스트 그룹 및 소스 수 제한, 인터페이스가 즉시 사용 가능하도록 구성되었는지 여부를 확인합니다.

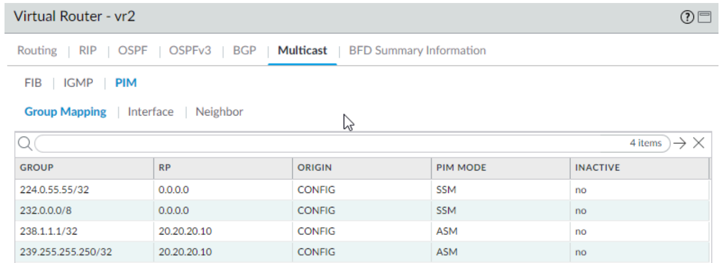


  4. 멀티캐스트 > **IGMP** > 멤버십을 선택하여 IGMP 지원 인터페이스와 인터페이스가 속한 멀티캐스트 그룹, 소스 및 기타 IGMP 정보를 살펴봅니다.

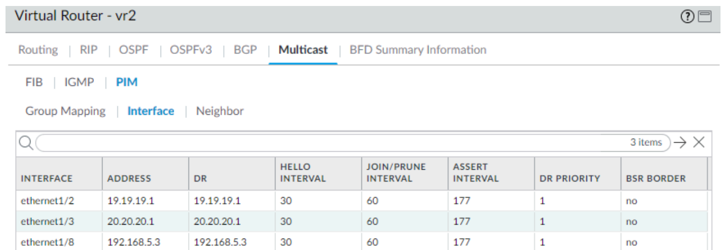


  5. 멀티캐스트 > **PIM** > 그룹 매핑을 선택하여 RP에 매핑된 멀티캐스트 그룹, RP 매핑의 출처, 그룹의 PIM 모드(ASM 또는 SSM) 및 그룹이 비활성 상태인지 여부를 확인합니다. SSM 모

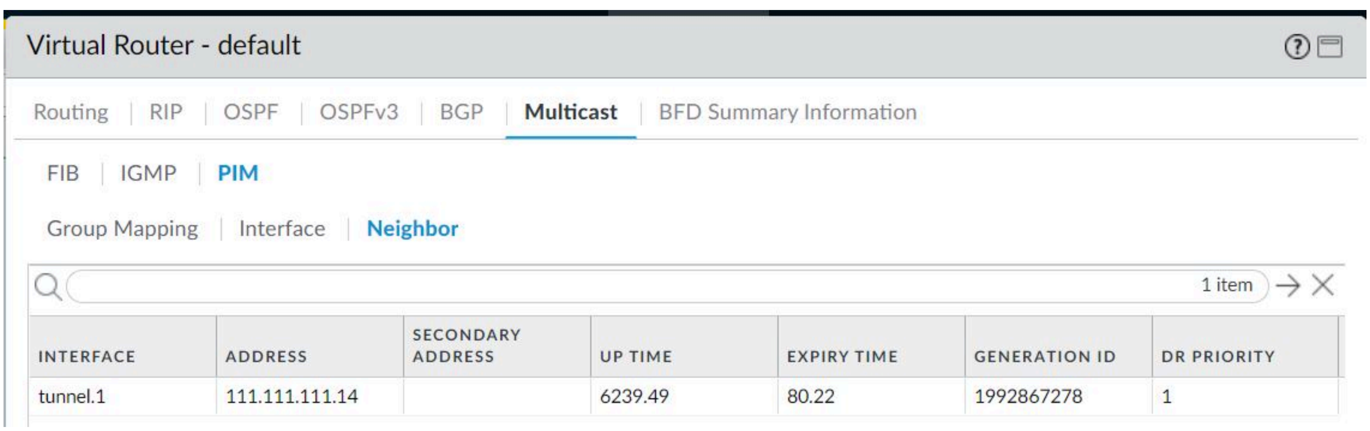
드의 그룹은 RP를 사용하지 않으므로 표시되는 RP 주소는 0.0.0.0입니다. 기본 SSM 그룹은 232.0.0.0/8입니다.



6. 멀티캐스트 > **PIM** > 인터페이스를 선택하여 인터페이스에 대한 DR의 IP 주소, DR 우선 순위, Hello, Join/Prune 및 Assert 간격, 인터페이스가 부트스트랩 라우터(BSR)인지 여부를 확인합니다.



7. 멀티캐스트 > **PIM** > **Neighbor**를 선택하여 가상 라우터에 대한 PIM 인접 라우터에 대한 정보를 봅니다.



경로 재분배

네트워크 트래픽의 접근성을 높이기 위해 경로 재분배에 대해 알아보고 구성합니다.

- 경로 재분배 개요
- 경로 재분배 구성

경로 재분배 개요

방화벽에서 경로 재분배란 방화벽이 하나의 라우팅 프로토콜(또는 정적 또는 연결된 경로)에서 학습한 경로를 다른 라우팅 프로토콜에서 사용할 수 있도록 하여 네트워크 트래픽의 액세스 가능성을 높이는 프로세스입니다. 경로 재분배가 없으면 라우터 또는 가상 라우터는 동일한 라우팅 프로토콜을 실행하는 다른 라우터와만 경로를 알리고 공유합니다. IPv4 또는 IPv6 BGP, 연결 또는 정적 경로를 OSPF RIB에 재배포하고 OSPFv3, 연결 또는 정적 경로를 BGP RIB에 재배포할 수 있습니다.

예를 들어, BGP 자율 시스템 또는 OSPF 영역에서 사용할 수 있는 특정 라우터의 수동 정적 경로 구성을 통해서만 한 번만 사용할 수 있었던 특정 네트워크를 만들 수 있습니다. 또한 프라이빗 랩 네트워크에 대한 경로와 같이 로컬로 연결된 경로를 BGP 자율 시스템 또는 OSPF 영역에 알릴 수도 있습니다.

내부 OSPFv3 네트워크의 사용자에게 BGP에 대한 액세스 권한을 부여하여 인터넷의 디바이스에 액세스할 수 있도록 할 수 있습니다. 이 경우 BGP 경로를 OSPFv3 RIB로 재배포합니다.

반대로 외부 사용자에게 내부 네트워크의 일부에 대한 액세스 권한을 부여할 수 있으므로 OSPFv3 경로를 BGP RIB에 재배포하여 BGP를 통해 내부 OSPFv3 네트워크를 사용할 수 있습니다.

경로 재분배 구성을(를) 하려면 재배포 프로파일을 만들어 시작합니다.

경로 재분배 구성

경로 재분배를 구성하려면 다음 절차를 수행하십시오.

STEP 1 | 재배포 프로파일을 생성합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. 재배포 프로파일 및 **IPv4** 또는 **IPv6**을 선택하고 프로파일을 추가합니다.
3. 프로파일의 이름을 입력합니다. 이 이름은 영숫자로 시작해야 하며 0개 이상의 밑줄(_), 하이픈(-), 점(.) 또는 공백(최대 16자)을 포함할 수 있습니다.
4. 프로파일의 우선순위를 1~255 범위에서 입력합니다. 방화벽은 우선 순위가 가장 높은(우선 순위 값이 가장 낮은) 프로파일을 먼저 사용하여 프로파일에 대한 경로를 일치시킵니다. 높은 우선 순위 규칙이 낮은 우선 순위 규칙보다 우선합니다.
5. 재배포에서 다음 중 하나를 선택합니다.
   - 재배포 - 이 필터와 일치하는 경로를 재배포하려면 선택합니다.
   - 재배포 없음 - 이 필터와 일치하는 경로를 제외하고 재배포 프로파일과 일치하는 재배포 경로에 대해 선택합니다. 이 선택은 프로파일을 재배포를 위해 선택하지 않을 경로를 지정하는 차단 목록으로 취급합니다. 예를 들어 BGP에 대한 재배포 프로파일이 여러 개 있는 경우 여러 접두사를 제외하는 재배포 없음 프로파일을 만든 다음 그 뒤에 우선 순위가 낮은(우선 순위 값이 더 높은) 일반 재배포 프로파일을 만들 수 있습니다. 두 프로파일이 결합되고 우선 순위가 더 높은 프로파일이 우선합니다. **No Redist** 프로파일만 가질 수는 없습니다. 경로를 재배포하려면 항상 하나 이상의 **Redist** 프로파일이 필요합니다.
6. 일반 필터 탭에서 소스 유형에 대해 재배포할 경로 유형을 하나 이상 선택합니다.
   - **bgp** - 프로파일과 일치하는 BGP 경로를 재배포합니다.
   - 연결 - 프로파일과 일치하는 연결된 경로를 재배포합니다.
   - **ospf**(IPv4만 해당) - 프로파일과 일치하는 OSPF 경로를 재배포합니다.
   - **rip**(IPv4만 해당) - 프로파일과 일치하는 RIP 경로를 재배포합니다.
   - **ospfv3**(IPv6만 해당) - 프로파일과 일치하는 OSPFv3 경로를 재배포합니다.
   - 정적 - 프로파일과 일치하는 정적 경로를 재배포합니다.
7. (선택 사항) 인터페이스의 경우 재배포에 맞게 연결된 경로의 송신 인터페이스를 하나 이상 추가합니다. 항목을 제거하려면 삭제를 클릭합니다.
8. (선택 사항) 대상의 경우 재배포를 위해 일치시킬 경로의 IPv4 또는 IPv6 대상을 하나 이상 추가합니다. 항목을 제거하려면 삭제를 클릭합니다.
9. (선택 사항) 다음 홉의 경우 재배포를 위해 일치시킬 경로의 다음 홉 IPv4 또는 IPv6 주소를 하나 이상 추가합니다. 항목을 제거하려면 삭제를 클릭합니다.
10. 확인을 클릭합니다.

STEP 2 | (선택 사항 - 일반 필터에 ospf 또는 ospfv3이 포함된 경우) OSPF 필터를 만들어 재배포할 OSPF 또는 OSPFv3 경로를 추가로 지정합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. 재배포 프로파일 및 **IPv4** 또는 **IPv6**을 선택하고 생성한 프로파일을 선택합니다.
3. **OSPF** 필터를 선택합니다.
4. 경로 유형에서 재배포할 OSPF 경로 유형(**ext-1**, **ext-2**, **inter-area** 또는 **intra-area**) 중 하나 이상을 선택합니다.
5. OSPF 또는 OSPFv3 경로를 재배포할 영역을 지정하려면 IP 주소 형식으로 영역을 추가합니다.
6. 태그를 지정하려면 IP 주소 형식의 태그를 추가합니다.
7. 확인을 클릭합니다.

STEP 3 | (선택 사항 - 일반 필터에 bgp가 포함된 경우) BGP 필터를 만들어 재배포할 BGP 경로를 추가로 지정합니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. 재배포 프로파일 및 **IPv4** 또는 **IPv6**을 선택하고 생성한 프로파일을 선택합니다.
3. **BGP** 필터를 선택합니다.
4. 커뮤니티의 경우 **local-as**, **no-advertise**, **no-export** 또는 **nopeer**와 같은 커뮤니티 목록에서 선택하려면 추가합니다. 10진수 또는 16진수 또는 AS:VAL 형식으로 32비트 값을 입력할 수도 있습니다. 여기서 AS 및 VAL은 각각 0에서 65,535 사이입니다. 최대 10개 항목을 입력합니다.
5. 확장 커뮤니티의 경우 확장 커뮤니티를 16진수 또는 TYPE:AS:VAL 또는 TYPE:IP:VAL 형식의 64비트 값으로 추가합니다. TYPE은 16비트입니다. AS 또는 IP는 16비트입니다. VAL은 32비트입니다. 최대 다섯 개의 항목을 입력합니다.
6. 확인을 클릭합니다.

STEP 4 | 경로를 재배포할 프로토콜을 선택하고 해당 경로의 속성을 설정합니다.

이 작업은 BGP로 경로를 재배포하는 방법을 보여 줍니다.

1. 네트워크 > 가상 라우터를 선택하고 가상 라우터를 선택합니다.
2. **BGP** > 재배포 규칙을 선택합니다.
3. 기본 경로 재배포 허용을 선택하여 방화벽이 기본 경로를 재배포할 수 있도록 허용합니다.
4. 추가를 클릭합니다.
5. 주소 패밀리 유형 선택: **IPv4** 또는 **IPv6**를 사용하여 재분배된 경로를 배치할 경로 테이블을 지정합니다.
6. 재배포할 경로를 선택하는 재배포 프로파일의 이름을 선택합니다.
7. 재배포 규칙을 사용하도록 설정합니다.
8. (선택 사항) 방화벽이 재배포 중인 경로에 적용되는 다음 값 중 하나를 입력합니다.
   - 1에서 65,535 사이의 메트릭입니다.
   - 원점 설정 - 경로의 원점: **igp**, **egp** 또는 불완전.
   - **MED** 설정 - MED 값을 0에서 4,294,967,295 범위로 설정합니다.
   - 로컬 기본 설정 - 0에서 4,294,967,295 범위의 로컬 기본 설정 값을 설정합니다.
   - **AS** 경로 제한 설정 - 1에서 255 사이의 AS_PATH에 있는 최대 자율 시스템 수입니다.
   - 커뮤니티 설정 - 32비트 값을 10진수 또는 16진수로 선택 또는 입력하거나 AS:VAL 형식으로 값을 입력합니다. 여기서 AS 및 VAL은 각각 0~65,525 범위에 있습니다. 최대 10개 항목을 입력합니다.
   - 확장 커뮤니티 설정 - 확장 커뮤니티를 16진수 또는 TYPE:AS:VAL 또는 TYPE:IP:VAL 형식의 64비트 값으로 선택하거나 입력합니다. TYPE은 16비트입니다. AS 또는 IP는 16비트입니다. VAL은 32비트입니다. 최대 다섯 개의 항목을 입력합니다.
9. 확인을 클릭합니다.

STEP 5 | 변경 사항을 커밋합니다.

GRE 터널

GRE(Generic Routing Encapsulation) 터널 프로토콜은 페이로드 프로토콜을 캡슐화하는 캐리어 프로토콜입니다. GRE 패킷 자체는 전송 프로토콜(IPv4 또는 IPv6)로 캡슐화됩니다.

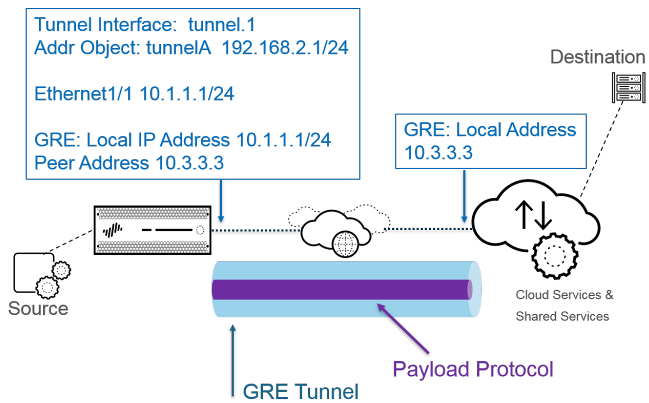
- GRE 터널 개요
- GRE 터널 생성

GRE 터널 개요

GRE(Generic Routing Encapsulation) 터널은 지점간 논리적 링크에서 두 엔드포인트(방화벽 및 다른 어플라이언스)를 연결합니다. 방화벽은 GRE 터널을 종료할 수 있습니다. 패킷을 GRE 터널로 라우팅하거나 전달할 수 있습니다. GRE 터널은 사용이 간편하고 특히 클라우드 또는 파트너 네트워크의 서비스에 대한 지점 간 연결을 위해 선택되는 터널링 프로토콜인 경우가 많습니다.

IP 주소로 향하는 패킷을 특정 지점 간 경로(예: 클라우드 기반 프록시 또는 파트너 네트워크)로 지정하려는 경우 GRE 터널을 생성합니다. 패킷은 대상 주소로 이동하는 동안 GRE 터널(인터넷과 같은 전송 네트워크를 통해)을 통해 클라우드 서비스로 이동합니다. 이를 통해 클라우드 서비스는 패킷에 대한 서비스 또는 정책을 시행할 수 있습니다.

다음 그림은 인터넷을 통해 방화벽을 클라우드 서비스에 연결하는 GRE 터널의 예입니다.



성능 향상과 단일 실패 지점을 방지하려면 단일 터널을 사용하는 대신 여러 ***GRE*** 터널 간에 방화벽에 대한 다중 연결을 분할하십시오. 각 ***GRE*** 터널에는 터널 인터페이스가 필요합니다.

방화벽이 패킷의 통과를 허용하고(정책 일치 기반) 패킷이 GRE 터널 인터페이스로 나갈 때 방화벽은 GRE 캡슐화를 추가하며, 세션을 생성하지 않습니다. 방화벽은 GRE 캡슐화 트래픽에 대한 보안 정책 규칙 조회를 수행하지 않으므로 방화벽이 캡슐화하는 GRE 트래픽에 대한 보안 정책 규칙이 필요하지 않습니다. 그러나 방화벽이 GRE 트래픽을 수신하면 세션을 생성하고 캡슐화된 트래픽 외에 모든 정책을 GRE IP 헤더에 적용합니다. 방화벽은 수신된 GRE 패킷을 다른 패킷과 같이 취급합니다. 그러므로:

- 방화벽이 GRE 터널과 연결된 터널 인터페이스와 동일한 영역(예: tunnel.1)에 있는 인터페이스에서 GRE 패킷을 수신하는 경우 소스 영역은 대상 영역과 동일합니다. 기본적으로 트래픽은 영역(영역 내 트래픽) 내에서 허용되므로 수신 GRE 트래픽은 기본적으로 허용됩니다.
- 그러나 이러한 트래픽을 거부하도록 자체 영역 내 보안 정책 규칙을 구성한 경우 GRE 트래픽을 명시적으로 허용해야 합니다.
- 마찬가지로 GRE 터널과 연결된 터널 인터페이스의 영역(예: tunnel.1)이 수신 인터페이스의 영역과 다른 경우 GRE 트래픽을 허용하도록 보안 정책 규칙을 구성해야 합니다.

방화벽은 터널링된 패킷을 GRE 패킷으로 캡슐화하기 때문에 GRE 헤더의 추가 24바이트는 자동으로 최대 세그먼트 크기(MSS) 최대 전송 단위(MTU)가 작아집니다. 인터페이스의 IPv4 MSS 조정 크기를 변경하지 않으면 방화벽은 기본적으로 MTU를 64바이트(40바이트의 IP 헤더 + 24바이트의 GRE 헤더)만큼 줄입니다. 즉, 기본 MTU가 1,500바이트인 경우 MSS는 1,436바이트(1,500 - 40 - 24 = 1,436)가 됩니다.

예를 들어 MSS 조정 크기를 300바이트로 구성하면 MSS는 1,176바이트(1,500 - 300 - 24 = 1,176)만 됩니다.

방화벽은 GRE 또는 IPSec 터널을 GRE 터널로 라우팅하는 것을 지원하지 않지만 GRE 터널을 IPSec 터널로 라우팅할 수 있습니다. 추가로:

- GRE 터널은 QoS를 지원하지 않습니다.
- 방화벽은 GRE 터널 끝점과 암호 해독 브로커 역할을 하는 단일 인터페이스를 지원하지 않습니다.
- GRE 터널링은 GRE 터널 엔드포인트 간의 NAT를 지원하지 않습니다.

다른 공급업체의 네트워크에 연결해야 하는 경우 ***GRE*** 터널이 아닌 IPSec 터널을 설정하는 것이 좋습니다. 공급업체가 지원하는 유일한 지점간 터널 메커니즘인 경우에만 ***GRE*** 터널을 사용해야 합니다. 원격 엔드포인트에 필요한 경우 ***IPSec***을 통한 ***GRE***를 활성화할 수도 있습니다(***GRE*** 캡슐화 추가). ***IPSec***이 트래픽을 암호화하기 전에 원격 끝점이 ***GRE*** 터널 내에서 트래픽을 캡슐화해야 하는 경우 ***GRE*** 캡슐화를 추가합니다. 예를 들어, 일부 구현에서는 ***IPSec***이 암호화하기 전에 멀티캐스트 트래픽을 캡슐화해야 합니다. 이것이 사용자 환경에 대한 요구 사항이고 ***GRE*** 터널과 ***IPSec*** 터널이 동일한 ***IP*** 주소를 공유하는 경우 ***IPSec*** 터널을 설정할 때 ***GRE*** 캡슐화를 추가합니다.

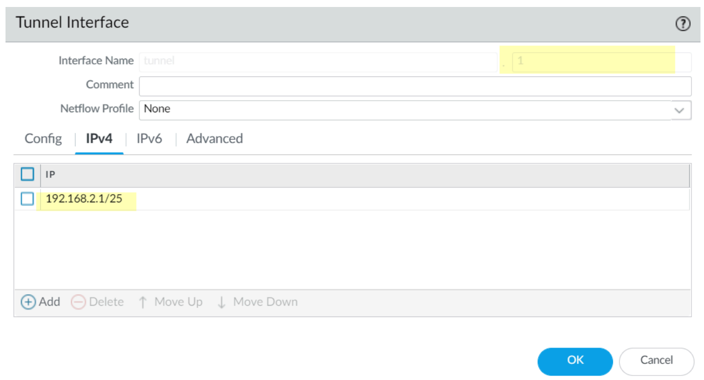
방화벽에서 ***GRE*** 터널을 종료할 계획이 없지만 ***GRE*** 터널 내부에서 방화벽을 통과하는 트래픽을 검사하고 제어하는 기능을 원하는 경우 ***GRE*** 터널을 만들지 마십시오. 대신 ***GRE*** 트래픽을 터널 콘텐츠 검사을(를) 수행하십시오. 터널 콘텐츠 검사를 사용하면 트래픽을 지시할 목적으로 지점 간 논리적 링크를 생성하지 않고 방화벽을 통과하는 ***GRE*** 트래픽에 대한 정책을 검사하고 시행합니다.

GRE 터널 생성

GRE(Generic Routing Encapsulation) 터널을 만들어 지점 간 논리적 링크에서 두 엔드포인트를 연결합니다.

STEP 1 | 터널 인터페이스를 생성합니다.

1. 네트워크 > 인터페이스 > 터널을 선택합니다.
2. 터널을 추가하고 터널 인터페이스 이름 뒤에 마침표와 숫자를 입력합니다(범위: 1~9,999). 예를 들어, **`tunnel.1`**입니다.
3. 구성 탭에서 터널 인터페이스를 가상 라우터에 할당합니다.
4. 방화벽이 여러 가상 시스템을 지원하는 경우 터널 인터페이스를 가상 시스템에 할당합니다.
5. 터널 인터페이스를 보안 영역에 할당합니다.



6. 터널 인터페이스에 IP 주소를 할당합니다. (이 터널로 라우팅하거나 터널 엔드포인트를 모니터링하려면 IP 주소를 할당해야 합니다.) **IPv4** 또는 **IPv6**을 선택하거나 둘 다 구성합니다.

   이 주소와 피어 터널 인터페이스의 해당 주소는 지점간 논리적 링크이므로 동일한 서브넷에 있어야 합니다.

   - (IPv4만 해당) **IPv4** 탭에서 IPv4 주소 추가, 주소 개체를 선택하거나 새 주소를 클릭하고 주소 유형을 지정하고 입력합니다. 예를 들어 **`192.168.2.1`**을 입력합니다.
   - (IPv6에만 해당) **IPv6** 탭 에서 인터페이스에서 **IPv6**을 사용하도록 설정합니다.
     1. 인터페이스 **ID**에서 **EUI-64(**기본 **64**비트 확장 고유 식별자**)**를 선택합니다.
     2. 새 주소를 추가하거나 IPv6 주소 개체를 선택하거나 새 주소를 클릭하고 주소 이름을 지정합니다. 인터페이스에서 주소를 활성화하고 확인을 클릭합니다.
     3. 주소의 유형을 선택하고 IPv6 주소 또는 FQDN을 입력하고 확인을 클릭하여 새 주소를 저장합니다.
     4. 인터페이스에서 주소 사용을 선택하고 확인을 클릭합니다.
7. 확인을 클릭합니다.

STEP 2 | 패킷이 특정 지점 간 경로를 통과하도록 GRE 터널을 만듭니다.

1. 네트워크 > **GRE** 터널을 선택하고 이름으로 터널을 추가합니다.
2. 이더넷 인터페이스 또는 하위 인터페이스, AE(집계 이더넷) 인터페이스, 루프백 인터페이스 또는 VLAN 인터페이스인 로컬 GRE 터널 엔드포인트(소스 인터페이스)로 사용할 인터페이스를 선택합니다.
3. 로컬 주소를 **IP**로 선택하고 방금 선택한 인터페이스의 IP 주소를 선택합니다.
4. GRE 터널의 반대쪽 엔드포인트 IP 주소인 피어 주소를 입력합니다.
5. 1단계에서 생성한 터널 인터페이스를 선택합니다. (라우팅을 위한 송신 인터페이스일 때 터널을 식별합니다.)
6. GRE 패킷에 캡슐화된 IP 패킷의 **TTL**을 입력합니다(범위는 1~255, 기본값은 64).
7. **ToS** 헤더 복사를 선택하여 내부 IP 헤더에서 캡슐화된 패킷의 외부 IP 헤더로 ToS(서비스 유형) 필드를 복사하여 원래 ToS 정보를 보존합니다. 네트워크에서 QoS를 사용하고 QoS 정책을 적용하기 위해 ToS 비트에 의존하는 경우 이 옵션을 선택합니다.

STEP 3 | (모범 사례) GRE 터널에 대해 연결 유지 기능을 사용하도록 설정합니다.

*Keep Alive*가 활성화된 경우 기본적으로 *GRE* 터널이 작동 중지되려면 *10*초 간격으로 *3*개의 미반환 *Keepalive* 패킷*(*재시도*)*이 필요하고 *GRE* 터널이 다시 작동하려면 *10*초 간격으로 *5*개의 *Hold Timer* 간격이 필요합니다.

1. 연결 유지를 선택하여 GRE 터널에 대한 keepalive 기능을 활성화합니다(기본값은 비활성화됨).
2. (선택 사항) GRE 터널의 로컬 끝이 터널 피어로 보내는 연결 유지 패킷 사이의 간격**(**초**)**(초)을 설정합니다. 이것은 또한 **Hold Timer**를 곱할 때 GRE 터널이 다시 작동하기 전에 방화벽이 성공적인 keepalive 패킷을 확인해야 하는 시간의 길이입니다(범위는 1~50, 기본값은 10). 간격을 너무 작게 설정하면 환경에서 불필요할 수 있고 추가 대역폭 및 처리가 필요할 수 있는 연결 유지 패킷이 많이 발생합니다. 간격을 너무 크게 설정하면 오류 조건이 즉시 식별되지 않을 수 있으므로 장애 조치가 지연될 수 있습니다.
3. (선택 사항) 방화벽이 터널 피어 다운을 고려하기 전에 연결 유지 패킷이 반환되지 않는 간격 수인 재시도 설정을 입력합니다(범위는 1~255, 기본값은 3). 터널이 다운되면 방화벽은 전달 테이블에서 터널과 연결된 경로를 제거합니다. 재시도 설정을 구성하면 실제로 다운되지 않은 터널에서 조치를 취하지 않도록 하는 데 도움이 됩니다.
4. (선택 사항) Keepalive 패킷이 성공한 **Intervals**의 수인 **Hold Timer**를 설정합니다. 그 후 방화벽은 터널 피어와 통신을 다시 설정합니다(범위는 1~64, 기본값은 5).

STEP 4 | 확인을 클릭합니다.

STEP 5 | GRE 터널을 통해 트래픽을 대상으로 라우팅하도록 라우팅 프로토콜 또는 정적 경로를 구성합니다. 예를 들어 대상 서버의 네트워크에 정적 경로 구성을 지정하고 송신 인터페이스를 로컬 터널 엔드포인트(tunnel.1)로 지정합니다. 다음 홉을 반대쪽 끝에 있는 터널의 IP 주소로 구성합니다. 예: 192.168.2.3.

STEP 6 | 변경 사항을 커밋합니다.

STEP 7 | 공용 IP 주소, 로컬 및 피어 IP 주소(방화벽에 있는 GRE 터널의 피어 및 로컬 IP 주소에 각각 해당), 라우팅 프로토콜 또는 정적 경로로 터널의 반대쪽 끝을 구성합니다.

STEP 8 | 방화벽이 GRE 터널을 통해 터널 피어와 통신할 수 있는지 확인합니다.

1. CLI에 액세스합니다.
2. > **`ping source 192.168.2.1 host 192.168.2.3`**

DHCP

이 섹션에서는 DHCP(Dynamic Host Configuration Protocol, 동적 호스트 구성 프로토콜)와 Palo Alto Networks® 방화벽에서 DHCP 서버, 클라이언트, 또는 릴레이 에이전트로 역할하도록 인터페이스를 구성하는 데 필요한 작업에 대해 설명합니다. 이러한 역할을 다른 인터페이스에 할당함으로써, 방화벽은 여러 역할을 수행할 수 있습니다.

DHCP 개요

DHCP는 RFC 2131, Dynamic Host Configuration Protocol에 정의된 표준화된 프로토콜입니다. DHCP는 TCP/IP 및 링크 계층 구성 매개변수를 제공하고 TCP/IP 네트워크에서 동적으로 구성된 호스트에 네트워크 주소를 제공하는 두 가지 주요 목적이 있습니다.

DHCP는 클라이언트-서버 통신 모델을 사용합니다. 이 모델은 디바이스가 수행할 수 있는 세 가지 역할로 구성됩니다. DHCP 클라이언트, DHCP 서버 및 DHCP 릴레이 에이전트.

- DHCP 클라이언트(호스트) 역할을 하는 디바이스는 DHCP 서버에서 IP 주소 및 기타 구성 설정을 요청할 수 있습니다. 클라이언트 디바이스의 사용자는 구성 시간과 노력을 절약하고 네트워크의 주소 지정 계획이나 DHCP 서버에서 상속되는 기타 리소스 및 옵션을 알 필요가 없습니다.
- DHCP 서버 역할을 하는 디바이스는 클라이언트에 서비스를 제공할 수 있습니다. 세 가지 DHCP 주소 지정 메커니즘 중 하나를 사용하여 네트워크 관리자는 구성 시간을 절약하고 클라이언트가 더 이상 네트워크 연결을 필요로 하지 않을 때 제한된 수의 IP 주소를 재사용할 수 있는 이점이 있습니다. 서버는 IP 주소 지정과 많은 DHCP 옵션을 많은 클라이언트에 전달할 수 있습니다.
- DHCP 중계 에이전트 역할을 하는 디바이스는 DHCP 클라이언트와 서버 간에 DHCP 메시지를 전송합니다.

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 클라이언트에게 보내는 DHCP 메시지은(는) 포트 68로 보내집니다.

Palo Alto Networks® 방화벽의 인터페이스는 DHCP 서버, 클라이언트 또는 중계 에이전트의 역할을 수행할 수 있습니다. DHCP 서버 또는 중계 에이전트의 인터페이스는 레이어 3 이더넷, 통합 이더넷 또는 레이어 3 VLAN 인터페이스여야 합니다. 역할 조합에 대한 적절한 설정으로 방화벽 인터페이스를 구성합니다. 각 역할의 동작은 DHCP 서버 및 클라이언트로서의 방화벽에 요약되어 있습니다.

방화벽은 DHCPv4 서버 및 DHCPv6 릴레이를 지원합니다.

DHCP 서버 및 DHCP 클라이언트의 Palo Alto Networks 구현은 IPv4 주소만 지원합니다. DHCP 릴레이 구현은 IPv4 및 IPv6을 지원합니다. DHCP 클라이언트는 고가용성 활성/활성 모드에서 지원되지 않습니다.

DHCP 서버 및 클라이언트로서의 방화벽

방화벽은 DHCP 서버 및 DHCP 클라이언트로 작동할 수 있습니다. 동적 호스트 구성 프로토콜, RFC 2131은 IPv4 및 IPv6 주소를 지원하도록 설계되었습니다. DHCP 서버의 Palo Alto Networks® 구현은 IPv4 주소만 지원합니다.

방화벽 DHCP 서버는 다음과 같은 방식으로 작동합니다.

- DHCP 서버가 클라이언트로부터 DHCPDISCOVER 메시지를 수신하면 서버는 구성에 나타나는 순서대로 사전 정의 및 사용자 정의 옵션을 모두 포함하는 DHCPOFFER 메시지로 응답합니다. 클라이언트는 필요한 옵션을 선택하고 DHCPREQUEST 메시지로 응답합니다.
- 서버가 클라이언트로부터 DHCPREQUEST 메시지를 받으면 서버는 요청에 지정된 옵션만 포함하는 DHCPACK 메시지로 응답합니다.

방화벽 DHCP 클라이언트는 다음과 같은 방식으로 작동합니다.

- DHCP 클라이언트가 서버로부터 DHCPOFFER를 받으면 클라이언트는 DHCPREQUEST에서 보낸 옵션에 관계없이 향후 사용을 위해 제공되는 모든 옵션을 자동으로 캐시합니다.
- 기본적으로 그리고 메모리 소비를 줄이기 위해 클라이언트는 코드에 대해 여러 값을 수신하는 경우 각 옵션 코드의 첫 번째 값만 캐시합니다.
- DHCP 클라이언트가 DHCPDISCOVER 또는 DHCPREQUEST 메시지의 옵션 57에서 최대값을 지정하지 않는 한 DHCP 메시지의 최대 길이는 없습니다.

DHCP 메시지

DHCP는 DHCP 메시지의 옵션 유형 번호로 식별되는 8개의 표준 메시지 유형을 사용합니다. 예를 들어 클라이언트가 DHCP 서버를 찾으려면 로컬 물리적 하위 네트워크에서 DHCPDISCOVER 메시지를 브로드캐스트합니다. 서브넷에 DHCP 서버가 없고 DHCP 도우미 또는 DHCP 릴레이가 올바르게 구성되어 있으면 메시지가 다른 물리적 서브넷의 DHCP 서버로 전달됩니다. 그렇지 않으면 메시지는 메시지가 시작된 서브넷 이상으로 이동하지 않습니다. 하나 이상의 DHCP 서버가 사용 가능한 네트워크 주소 및 기타 구성 매개변수가 포함된 DHCPOFFER 메시지로 응답합니다.

클라이언트가 IP 주소를 필요로 하면 DHCPREQUEST를 하나 이상의 서버에 보냅니다. 물론 클라이언트가 IP 주소를 요청하는 경우 아직 IP 주소가 없으므로 RFC 2131에서는 클라이언트가 보내는 브로드캐스트 메시지의 IP 헤더에 0의 소스 주소가 있어야 합니다.

클라이언트가 서버에서 구성 매개변수를 요청하면 둘 이상의 서버에서 응답을 받을 수 있습니다. 클라이언트가 IP 주소를 수신하면 클라이언트에 최소한 IP 주소와 바인딩된 다른 구성 매개변수가 있다고 합니다. DHCP 서버는 클라이언트에 대한 구성 매개변수의 이러한 바인딩을 관리합니다.

다음 표에는 DHCP 메시지가 나열되어 있습니다.

DHCP 메시지	설명
DHCPDISCOVER	사용 가능한 DHCP 서버를 찾기 위한 클라이언트 브로드캐스트.
DHCP 제안	구성 매개변수를 제공하는 클라이언트의 DHCPDISCOVER에 대한 서버 응답입니다.
DHCPREQUEST	다음 중 하나를 수행하기 위해 하나 이상의 서버에 클라이언트 메시지: • 한 서버에서 매개변수를 요청하고 다른 서버에서 제안을 암시적으로 거부합니다. • 예를 들면 시스템 재부팅 후 이전에 할당된 주소가 올바른지 확인합니다. • 네트워크 주소 임대를 연장합니다.
DHCPACK	확인된 네트워크 주소를 포함하여 구성 매개변수가 포함된 서버에서 클라이언트에게 가는 승인 메시지입니다.
DHCPNAK	네트워크 주소에 대한 클라이언트의 이해가 잘못되었음을 나타내는 서버에서 클라이언트로 보내는 부정 승인(예: 클라이언트가 새 서브넷으로 이동한 경우) 또는 클라이언트 임대가 만료되었음을 알리는 메시지입니다.
DHCPDECLINE	네트워크 주소가 이미 사용 중임을 나타내는 클라이언트 대 서버 메시지입니다.

DHCP 메시지	설명
DHCPRELEASE	네트워크 주소의 사용자를 포기하고 임대의 남은 시간을 취소하는 클라이언트에서 서버로 가는 메시지.
DHCPINFORM	로컬 구성 매개변수만 요청하는 클라이언트 대 서버 메시지. 클라이언트에 외부에서 구성된 네트워크 주소가 있습니다.

DHCP 주소 지정

- DHCP 주소 할당 방법
- DHCP 임대

DHCP 주소 할당 방법

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 접속만 필요한 클라이언트에 할당할 수 있습니다. DHCP 임대 섹션을 참조하십시오.
- 정적 할당 - 네트워크 관리자는 클라이언트에 할당할 IP 주소를 선택하고 DHCP 서버는 이를 클라이언트에 보냅니다. 고정 DHCP 할당은 영구적입니다. DHCP 서버를 구성하고 클라이언트 디바이스의 **MAC** 주소에 해당하는 예약 주소를 선택하면 됩니다. 클라이언트가 로그오프하거나, 재부팅하거나, 정전이 발생하더라도 DHCP 할당은 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 디바이스가 중요한 용도로 사용되고 디바이스가 꺼지거나, 연결이 해제되거나, 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 임대가 만료되거나 재부팅될 때, 풀에서 새 DHCP 할당을 수신합니다(임대를 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 예약된 주소를 디바이스에 할당하지 않습니다. 예를 들어 DHCP를 사용하지 않고 풀에서 몇 개의 주소를 예약하고 팩스와 프린터에 정적으로 할당할 수 있습니다.

DHCP 임대

임대는 DHCP 서버가 클라이언트에 네트워크 주소를 할당하는 기간으로 정의됩니다. 임대는 후속 요청시 연장(갱신)될 수 있습니다. 클라이언트가 더 이상 주소를 필요로 하지 않는 경우, 임대가 만료되기 전에 서버에 주소를 다시 공개할 수 있습니다. 그러면 서버는 할당되지 않은 주소가 부족한 경우 해당 주소를 다른 클라이언트에 자유롭게 할당할 수 있습니다.

DHCP 서버에 대해 구성된 임대 기간은 단일 DHCP 서버(인터페이스)가 클라이언트에 동적으로 할당하는 모든 주소에 적용됩니다. 즉, 동적으로 할당된 해당 인터페이스의 모든 주소는 기간이 무제한이거나 또

는 동일한 시간 초과 값을 갖습니다. 방화벽에 구성된 다른 DHCP 서버는 클라이언트에 대해 다른 임대 기간을 가질 수 있습니다. 예약 주소는 고정 주소 할당이며 임대 조건이 적용되지 않습니다.

DHCP 표준인 RFC 2131에 따라, DHCP 클라이언트는 새 주소가 할당될 위험이 있기 때문에 임대가 만료될 때까지 기다리지 않습니다. 대신, DHCP 클라이언트가 임대 기간의 중간 지점에 도달하면, 동일한 IP 주소를 유지하도록 임대 연장을 시도합니다. 따라서, 임대 기간은 슬라이딩 윈도우와 같습니다.

일반적으로 IP 주소가 디바이스에 할당되고, 디바이스가 네트워크에서 분리되고 임대가 연장되지 않은 경우, DHCP 서버는 해당 임대가 만료되도록 합니다. 클라이언트가 네트워크에서 사라지고 더 이상 주소가 필요하지 않기 때문에, 서버의 임대 기간에 도달하고 임대는 "만료됨" 상태입니다.

방화벽에는 만료된 IP 주소가 즉시 재할당되는 것을 방지하는 보류 타이머가 있습니다. 이 동작은 디바이스가 네트워크에 다시 들어올 경우에 대비하여 디바이스의 주소를 임시로 예약합니다. 그러나 주소 풀에 주소가 부족하면 서버는 보류 타이머가 만료되기 전에 만료된 주소를 다시 할당합니다. 만료된 주소는 시스템이 더 많은 주소를 필요로 하거나 보류 타이머가 주소를 해제할 때 자동으로 지워집니다.

CLI에서 **show dhcp server lease**는 운영 명령을 사용하여 할당된 IP 주소에 대한 임대 정보를 봅니다. 만료된 임대가 자동으로 해제될 때까지 기다리지 않으려면, **clear dhcp lease interface <*interface*> expired-only** 명령을 사용하여 만료된 임대를 해제하고, 풀에서 해당 주소를 다시 사용할 수 있습니다. **clear dhcp lease interface <*interface*> ip <*ip_address*>** 명령을 사용하여 특정 IP 주소를 해제할 수 있습니다. **clear dhcp lease interface <*interface*> mac <*mac_address*>** 명령을 사용하여 특정 MAC 주소를 해제합니다.

DHCP 옵션

DHCP 및 DHCP 옵션의 역사는 BOOTP(Bootstrap Protocol)로 거슬러 올라갑니다. BOOTP는 호스트에서 부팅 절차 중에 동적으로 구성하는 데 사용되었습니다. 호스트는 서버 주소 및 인터넷 게이트웨이 주소와 함께 서버에서 부트 프로그램을 다운로드할 IP 주소 및 파일을 수신할 수 있습니다.

BOOTP 패킷에 포함된 벤더 정보 필드에는 서브넷 마스크, BOOTP 파일 크기 및 기타 여러 값과 같은 다양한 유형의 정보를 포함하는 여러 태그 필드가 포함될 수 있습니다. RFC 1497은 BOOTP 공급업체 정보 확장에 대해 설명합니다. DHCP는 BOOTP를 대체합니다. BOOTP는 방화벽에서 지원되지 않습니다.

이러한 확장은 결국 옵션이라고도 하는 DHCP 및 DHCP 호스트 구성 매개변수를 사용하여 확장되었습니다. 공급업체 확장과 유사하게 DHCP 옵션은 DHCP 클라이언트에 정보를 제공하는 태그가 지정된 데이터 항목입니다. 옵션은 DHCP 메시지 끝에 가변 길이 필드로 전송됩니다. 예를 들어, DHCP 메시지 유형은 옵션 53이고 값 1은 DHCPDISCOVER 메시지를 나타냅니다. DHCP 옵션은 RFC 2132, DHCP 옵션 및 BOOTP 공급업체 확장에 정의되어 있습니다.

DHCP 클라이언트는 서버와 협상하여 클라이언트가 요청한 옵션만 보내도록 서버를 제한할 수 있습니다.

- 사전 정의된 DHCP 옵션
- DHCP 옵션에 대한 다중 값
- DHCP 옵션 43, 55, 60 및 기타 사용자 지정 옵션

사전 정의된 DHCP 옵션

Palo Alto Networks® 방화벽은 DHCP 서버 구현에서 사용자 정의 및 사전 정의된 DHCP 옵션을 지원합니다. 이러한 옵션은 DHCP 서버에서 구성되고 서버에 DHCPREQUEST를 보낸 클라이언트로 보내집니다. 클라이언트는 수락하도록 프로그래밍된 옵션을 상속하고 구현한다고 합니다.

방화벽은 DHCP 서버 구성 화면에 나타나는 순서대로 **DHCP** 서버에서 다음과 같은 사전 정의된 옵션을 지원합니다.

DHCP 옵션	**DHCP** 옵션 이름
51	임대 기간
3	게이트웨이
1	IP 풀 서브넷(마스크)
6	도메인 네임 시스템(DNS)(DNS) 서버 주소(기본 및 보조)
44	WINS(Windows Internet Name Service) 서버 주소(기본 및 보조)
41	Network Information Service(NIS) 서버 주소(기본 및 보조)
42	NTP(Network Time Protocol) 서버 주소(기본 및 보조)

DHCP 옵션	**DHCP** 옵션 이름
70	POP3(Post Office Protocol Version 3) 서버 주소
69	SMTP(Simple Mail Transfer Protocol) 서버 주소
15	DNS 접미사

언급한 바와 같이 IP 전화 및 무선 인프라 디바이스와 같은 다양한 사무 장비를 지원하는 공급업체별 및 맞춤형 옵션을 구성할 수도 있습니다. 각 옵션 코드는 IP 주소, ASCII 또는 16진수 형식일 수 있는 여러 값을 지원합니다. 방화벽이 강화된 DCHP 옵션 지원을 통해 지점은 DHCP 클라이언트에 공급업체별 및 사용자 지정 옵션을 제공하기 위해 자체 DHCP 서버를 구입하고 관리할 필요가 없습니다.

DHCP 옵션에 대한 다중 값

옵션 코드가 동일한 옵션 이름에 대해 여러 옵션 값을 입력할 수 있지만 특정 코드와 이름 조합의 모든 값은 동일한 유형(IP 주소, ASCII 또는 16진수) 이어야 합니다. 한 유형이 상속되거나 입력되고 나중에 동일한 코드 및 이름 조합에 대해 다른 유형을 입력하면 두 번째 유형이 첫 번째 유형을 덮어씁니다.

다른 옵션 이름을 사용하여 옵션 코드를 두 번 이상 입력할 수 있습니다. 이 경우 옵션 코드의 옵션 유형은 여러 옵션 이름 간에 다를 수 있습니다. 예를 들어 옵션 해안 서버(옵션 코드 6) 가 IP 주소 유형으로 구성된 경우 ASCII 유형의 옵션 서버 XYZ(옵션 코드 6)도 허용됩니다.

방화벽은 여러 옵션 값(함께 묶음) 을 위에서 아래로 순서대로 클라이언트로 보냅니다. 따라서 옵션에 대해 여러 값을 입력할 때 기본 설정 순서로 값을 입력하거나 옵션을 이동하여 목록에서 원하는 순서를 얻습니다. 방화벽 구성의 옵션 순서에 따라 옵션이 DHCPOFFER 및 DHCPACK 메시지에 표시되는 순서가 결정됩니다.

이미 존재하는 옵션 코드를 미리 정의된 옵션 코드로 입력할 수 있으며, 사용자 정의된 옵션 코드가 미리 정의된 DHCP 옵션보다 우선하며, 방화벽이 경고를 표시합니다.

DHCP 옵션 43, 55, 60 및 기타 사용자 지정 옵션

다음 표에서는 RFC 2132에 설명된 여러 옵션에 대한 옵션 동작을 설명합니다.

옵션 코드	옵션 이름	옵션 설명/동작
43	공급업체별 정보	서버에서 클라이언트로 전송됩니다. DHCP 서버가 클라이언트에 제공하도록 구성된 공급업체별 정보입니다. 서버의 테이블에 클라이언트의 DHCPREQUEST에 있는 VCI와 일치하는 VCI(Vendor Class Identifier)가 있는 경우에만 정보가 클라이언트에 전송됩니다. 옵션 43 패킷에는 여러 공급업체별 정보가 포함될 수 있습니다. 여기에는 캡슐화된 공급업체별 데이터 확장도 포함될 수 있습니다.

옵션 코드	옵션 이름	옵션 설명/동작
55	매개변수 요청 목록	클라이언트에서 서버로 전송됩니다. DHCP 클라이언트가 요청하는 구성 매개변수(옵션 코드) 목록(가능한 경우 클라이언트의 기본 설정 순서). 서버는 동일한 순서로 옵션으로 응답을 시도합니다.
60	공급업체 클래스 식별자(VCI)	클라이언트에서 서버로 전송됩니다. DHCP 클라이언트의 공급업체 유형 및 구성입니다. DHCP 클라이언트는 DHCPREQUEST의 옵션 코드 60을 DHCP 서버로 보냅니다. 서버가 옵션 60을 수신하면 VCI를 보고 자체 테이블에서 일치하는 VCI를 찾은 다음 값(VCI에 해당)과 함께 옵션 43을 반환하여 공급업체별 정보를 올바른 클라이언트에 전달합니다. 클라이언트와 서버 모두 VCI에 대해 알고 있습니다.

RFC 2132에 정의되지 않은 사용자 지정 공급업체별 옵션 코드를 보낼 수 있습니다. 옵션 코드의 범위는 1-254이고 고정 또는 가변 길이일 수 있습니다.

사용자 정의 ***DHCP*** 옵션은 ***DHCP*** 서버에서 검증되지 않습니다. 생성한 옵션에 대해 올바른 값을 입력했는지 확인해야 합니다.

ASCII 및 16진법 DHCP 옵션 유형의 경우 옵션 값은 최대 255옥텟일 수 있습니다.

인터페이스를 DHCP 서버로 구성

이 작업의 전제 조건은 다음과 같습니다.

- 레이어 3 이더넷 또는 레이어 3 VLAN 인터페이스를 구성합니다.
- 가상 라우터 및 영역에 인터페이스를 할당합니다.
- DHCP 서버가 클라이언트에 할당하도록 지정할 수 있는 네트워크 계획에서 유효한 IP 주소 풀을 결정합니다.
- 구성하려는 DHCP 옵션, 값 및 공급업체 클래스 식별자를 수집합니다.

용량은 다음과 같습니다.

- PA-5200 시리즈 및 PA-7000 시리즈 방화벽 이외의 방화벽 모델에 대해서는 제품 선택 도구를 참조하십시오.
- PA-5220 방화벽에서는 구성된 DHCP 서버 수를 뺀 최대 500개의 DHCP 서버와 최대 2,048개의 DHCP 릴레이 에이전트를 구성할 수 있습니다. 예를 들어 500개의 DHCP 서버를 구성하는 경우 1,548개의 DHCP 릴레이 에이전트를 구성할 수 있습니다.
- PA-5250, PA-5260 및 PA-7000 시리즈 방화벽에서 최대 500개의 DHCP 서버와 최대 4,096개의 DHCP 릴레이 에이전트에서 구성된 DHCP 서버 수를 뺀 값을 구성할 수 있습니다. 예를 들어, 500개의 DHCP 서버를 구성하는 경우 3,596개의 DHCP 릴레이 에이전트를 구성할 수 있습니다.

DHCP 서버로 작동하도록 방화벽의 인터페이스를 구성하려면 다음 작업을 수행합니다.

STEP 1 | DHCP 서버가 될 인터페이스를 선택합니다.

1. 네트워크 > **DHCP** > **DHCP** 서버를 선택하고 인터페이스 이름을 추가하거나 하나를 선택합니다.
2. 모드에서 사용 또는 자동 모드를 선택합니다. 자동 모드는 서버를 활성화하고 네트워크에서 다른 DHCP 서버가 감지되면 비활성화합니다. 비활성화됨 설정은 서버를 비활성화합니다.
3. (선택 사항) 서버에서 IP 주소를 클라이언트에 할당하기 전에 IP 주소를 ping하도록 하려면 새 **IP**를 할당할 때 **Ping IP**를 선택합니다.

   *ping*이 응답을 수신하면 다른 디바이스에 이미 해당 주소가 있으므로 사용할 수 없음을 의미합니다. 서버가 대신 풀에서 다음 주소를 할당합니다. 이 동작은 IPv6, RFC 4429에 대한 낙관적 중복 주소 감지(DAD)와 유사합니다.

   옵션을 설정하고 *DHCP* 서버 탭으로 돌아가면 인터페이스의 프로브 ***IP*** 열에 새 ***IP*** 할당 시 ***Ping IP***가 선택되었는지 여부가 표시됩니다.

STEP 2 | 서버가 클라이언트에 전송하는 미리 정의된 DHCP 옵션을 구성합니다.

- 옵션 섹션에서 임대 유형을 선택합니다.
- 무제한은 서버가 **IP** 풀에서 동적으로 IP 주소를 선택하고 클라이언트에 영구적으로 할당하도록 합니다.
- **Timeout**은 임대가 지속되는 기간을 결정합니다. 일 및 시간 수를 입력하고 선택적으로 분 수를 입력합니다.
- 상속 소스 - 없음으로 두거나 소스 DHCP 클라이언트 인터페이스 또는 PPPoE 클라이언트 인터페이스를 선택하여 다양한 서버 설정을 DHCP 서버로 전파합니다. 상속 소스를 지정하는 경우 이 소스에서 상속할 옵션을 아래에서 하나 이상 선택합니다.

상속 소스를 지정하면 방화벽이 DHCP 클라이언트가 수신한 업스트림 서버에서 DHCP 옵션을 빠르게 추가할 수 있습니다. 또한 소스가 옵션을 변경하는 경우 클라이언트 옵션을 업데이트된 상태로 유지합니다. 예를 들어 소스가 기본 **NTP** 서버로 식별된 NTP 서버를 교체하는 경우 클라이언트는 자동으로 새 주소를 기본 **NTP** 서버로 상속합니다.

여러 *IP* 주소가 포함된 *DHCP* 옵션을 상속할 때 방화벽은 캐시 메모리를 절약하기 위해 옵션에 포함된 첫 번째 *IP* 주소만 사용합니다**.** 단일 옵션에 대해 여러 *IP* 주소가 필요한 경우 상속을 구성하는 대신 해당 방화벽에서 직접 *DHCP* 옵션을 구성합니다**.**

- 상속 소스 상태 확인 - 상속 소스를 선택한 경우 이 링크를 클릭하면 DHCP 클라이언트에서 상속된 옵션을 표시하는 동적 **IP** 인터페이스 상태 창이 열립니다.
- 게이트웨이 - 이 DHCP 서버와 동일한 LAN에 있지 않은 디바이스에 연결하는 데 사용되는 네트워크 게이트웨이(방화벽의 인터페이스)의 IP 주소입니다.
- 서브넷 마스크 - **IP** 풀의 주소와 함께 사용되는 네트워크 마스크입니다.

다음 필드에 대해 아래쪽 화살표를 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.

- 기본 **DNS**, 보조 **DNS** - 기본 및 대체 DNS(Domain Name System) 서버의 IP 주소입니다.
- 기본 **WINS**, 보조 **WINS** - 기본 WINS(Windows Internet Naming Service) 서버의 IP 주소입니다.
- 기본 **NIS**, 보조 **NIS** - 기본 및 대체 NIS(네트워크 정보 서비스) 서버의 IP 주소입니다.
- 기본 **NTP**, 보조 **NTP** - 사용 가능한 네트워크 시간 프로토콜 서버의 IP 주소입니다.
- **POP3** 서버 - POP3(Post Office Protocol) 서버의 IP 주소입니다.
- **SMTP** 서버 - SMTP(Simple Mail Transfer Protocol) 서버의 IP 주소입니다.
- **DNS** 접미사 - 확인할 수 없는 정규화되지 않은 호스트 이름이 입력될 때 클라이언트가 로컬에서 사용할 접미사입니다.

STEP 3 | (선택 사항) DHCP 서버가 해당 클라이언트에 보내는 공급업체별 또는 사용자 지정 DHCP 옵션을 구성합니다.

1. 사용자 지정 DHCP 옵션 섹션에서 DHCP 옵션을 식별하는 설명이 포함된 이름을 추가합니다.
2. 제공할 서버를 구성할 옵션 코드를 입력합니다(범위는 1~254). (옵션 코드는 RFC 2132를 참조하십시오.)
3. 옵션 코드가 **43**이면 공급업체 클래스 식별자 필드가 나타납니다. 옵션 60을 포함하는 클라이언트 요청에서 오는 값에 대한 일치로 사용되는 문자열 또는 16진수 값(접두사 0x 포함)인 VCI를 입력합니다. 서버는 테이블에서 들어오는 VCI를 찾아서 찾은 다음 옵션 43과 해당 옵션 값을 반환합니다.
4. **DHCP** 서버 상속 소스에서 상속 - DHCP 서버의 미리 정의된 옵션에 대해 상속 소스를 지정하고 공급업체별 옵션과 사용자 정의 옵션도 이 소스에서 상속하려는 경우에만 이 옵션을 선택합니다.
5. 상속 소스 상태 확인 - 상속 소스를 선택한 경우 이 링크를 클릭하면 동적 **IP** 인터페이스 상태가 열리고 DHCP 클라이언트에서 상속된 옵션이 표시됩니다.
6. **DHCP** 서버 상속 소스에서 상속을 선택하지 않은 경우 옵션 유형을 선택합니다. **IP** 주소, **ASCII** 또는 **16**진수. 16진수 값은 0x 접두사로 시작해야 합니다.
7. DHCP 서버가 해당 옵션 코드에 대해 제공할 옵션 값을 입력합니다. 별도의 줄에 여러 값을 입력할 수 있습니다.
8. 확인을 클릭합니다.

STEP 4 | (선택 사항) 다른 공급업체별 또는 사용자 지정 DHCP 옵션을 추가합니다.

1. 다른 사용자 지정 DHCP 옵션을 입력하려면 이전 단계를 반복합니다.
   - 옵션 이름이 같은 옵션 코드에 대해 여러 옵션 값을 입력할 수 있지만 옵션 코드의 모든 값은 유형(**IP** 주소, **ASCII** 또는 **16**진수)이 같아야 합니다. 하나의 유형을 상속 또는 입력하고 동일한 옵션 코드 및 동일한 옵션 이름에 대해 다른 유형을 입력하면 두 번째 유형이 첫 번째 유형을 덮어씁니다.

     옵션에 대해 여러 값을 입력할 때 선호하는 순서대로 값을 입력하거나 사용자 지정 DHCP 옵션을 이동하여 목록에서 선호하는 순서를 얻습니다. 옵션을 선택하고 위로 이동 또는 아래로 이동을 클릭합니다.
   - 다른 옵션 이름을 사용하여 옵션 코드를 두 번 이상 입력할 수 있습니다. 이 경우 옵션 코드의 옵션 유형은 여러 옵션 이름에서 다를 수 있습니다.
2. 확인을 클릭합니다.

STEP 5 | DHCP 서버가 주소를 선택하고 DHCP 클라이언트에 할당하는 IP 주소의 상태 저장 풀을 식별합니다.

> 네트워크의 네트워크 관리자가 아닌 경우 네트워크 관리자에게 *DHCP* 서버에서 할당하도록 지정할 수 있는 네트워크 계획의 유효한 *IP* 주소 풀을 요청합니다.

1. **IP** 풀 필드에서 이 서버가 클라이언트에 주소를 할당할 IP 주소 범위를 추가합니다. IP 서브넷 및 서브넷 마스크(예: 192.168.1.0/24) 또는 IP 주소 범위(예: 192.168.1.10-192.168.1.20)를 입력합니다.
   - 유동 IP 주소 할당을 위해서는 IP 풀 또는 예약 주소가 필수입니다.
   - 할당한 정적 IP 주소가 방화벽 인터페이스가 서비스하는 서브넷에 속하는 한 정적 IP 주소 할당을 위해 IP 풀은 선택 사항입니다.
2. (선택 사항) 다른 IP 주소 풀을 지정하려면 이 단계를 반복합니다.

STEP 6 | (선택 사항) 동적으로 할당되지 않을 IP 풀의 IP 주소를 지정합니다. **MAC** 주소도 지정하면 디바이스가 DHCP를 통해 IP 주소를 요청할 때 예약된 주소가 해당 디바이스에 할당됩니다.

> 예약된 주소 할당에 대한 설명은 DHCP 주소 지정 섹션을 참조하십시오.

1. 예약된 주소 필드에서 추가를 클릭합니다.
2. DHCP 서버에서 동적으로 할당하지 않으려는 **IP** 풀의 IP 주소(*x.x.x.x* 형식)를 입력합니다.
3. (선택 사항) 방금 지정한 IP 주소를 영구적으로 할당할 디바이스의 **MAC** 주소(*xx:xx:xx:xx:xx:xx* 형식)를 지정합니다.
4. (선택 사항) 앞의 두 단계를 반복하여 다른 주소를 예약합니다.

STEP 7 | 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

인터페이스를 DHCP 클라이언트로 구성

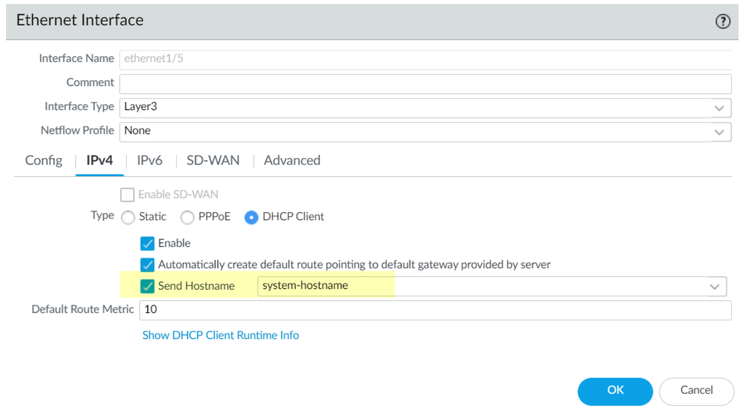
방화벽 인터페이스를 DHCP 클라이언트로 구성하기 전에 레이어 3 인터페이스(이더넷, 이더넷 하위 인터페이스, VLAN, VLAN 하위 인터페이스, 집계 또는 집계 하위 인터페이스)를 구성하고 인터페이스가 가상 라우터 및 영역에 할당되었는지 확인합니다. DHCP를 사용하여 인터페이스에 대한 IPv4 주소를 요청해야 하는 경우 인터페이스를 DHCP 클라이언트로 구성합니다.

관리 인터페이스를 DHCP 클라이언트로 구성할 수도 있습니다.

STEP 1 | 인터페이스를 DHCP 클라이언트로 구성합니다.

1. 네트워크 > 인터페이스를 선택합니다.
2. 이더넷 탭 또는 **VLAN** 탭에서 레이어 3 인터페이스를 추가하거나 DHCP 클라이언트가 될 구성된 계층 3 인터페이스를 선택합니다.
3. **IPv4** 탭을 선택하고 유형에서 **DHCP** 클라이언트를 선택합니다.
4. 활성화를 선택합니다.
5. (선택 사항) 기본적으로 활성화된 서버에서 제공하는 기본 게이트웨이를 가리키는 기본 경로 자동 생성 옵션을 활성화합니다. 이 옵션을 활성화하면 방화벽이 기본 게이트웨이에 대한 정적 경로를 생성합니다. 이는 클라이언트가 방화벽의 경로 테이블에서 경로를 유지할 필요가 없는 많은 데스티네이션에 액세스하려고 할 때 유용합니다.
6. (선택 사항) 호스트 이름 보내기 옵션을 활성화하여 호스트 이름을 DHCP 클라이언트 인터페이스에 할당하고 해당 호스트 이름(옵션 12)을 DHCP 서버로 보냅니다. 그러면 DHCP 서버가 호스트 이름을 DNS 서버에 등록할 수 있습니다. 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 시

스템 호스트네임을 나타냅니다. 또는 인터페이스의 호스트 이름을 입력합니다. 이 이름은 대문자와 소문자, 숫자, 마침표(.), 하이픈(-), 밑줄(_)을 포함하여 최대 64자까지 가능합니다.



7. (선택 사항) 방화벽과 DHCP 서버 간의 경로에 대한 기본 경로 지표(우선 순위 수준)를 입력합니다(범위는 1~65,535, 기본값은 10). 경로 선택 시 번호가 낮은 경로가 우선 순위가 높습니다. 예를 들어 메트릭이 10인 경로는 메트릭이 100인 경로보다 먼저 사용됩니다.

   *방화벽과 **DHCP** 서버 간의 경로에 대한 기본 경로 메트릭은 기본적으로 **10**입니다. 고정 기본 경로 **0.0.0.0/0**이 **DHCP** 인터페이스를 송신 인터페이스로 사용하는 경우 해당 경로의 기본 메트릭도 **10**입니다. 따라서 메트릭이 **10**인 두 개의 경로가 있으며 방화벽은 경로 중 하나를 무작위로 선택하고 다른 경로를 한 번 선택할 수 있습니다.*

   *서버에서 제공하는 기본 게이트웨이를 가리키는 기본 경로 자동 생성 옵션을 활성화하고, 가상 라우터를 선택하고, 레이어 **3** 인터페이스에 대한 정적 경로를 추가하고, 메트릭(기본값은 **10**)을 **10**(이 예에서는 **100**)보다 큰 값으로 변경한다고 가정하고 변경 사항을 커밋합니다. 경로 테이블에서 경로의 메트릭은 **100**을 나타내지 않습니다. 대신 **10**이 구성된 값 **100**보다 우선하므로 예상대로 기본값 **10**을 나타냅니다. 그러나 고정 경로의 메트릭을 **10**보다 작은 값(예: **6**)으로 변경하면 구성된 메트릭 **6**을 나타내도록 경로 테이블의 경로가 업데이트됩니다.*

8. (선택 사항) DHCP 서버에서 상속된 클라이언트의 모든 설정을 보려면 **DHCP** 클라이언트 런타임 정보 표시 옵션을 활성화합니다.

STEP 2 | 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

이제 이더넷 인터페이스는 이더넷 탭의 **IP** 주소로 **Dynamic-DHCP** 클라이언트를 표시해야 합니다.

STEP 3 | (선택 사항) 방화벽에서 DHCP 클라이언트로 구성된 인터페이스를 확인합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 **IP** 주소를 확인하여 DHCP 클라이언트를 나타내는 인터페이스를 확인합니다.
2. 네트워크 > 인터페이스 > **VLAN**을 선택하고 **IP** 주소를 확인하여 DHCP 클라이언트를 나타내는 인터페이스를 확인합니다.

관리 인터페이스를 DHCP 클라이언트로 구성

방화벽의 관리 인터페이스는 IPv4용 DHCP 클라이언트를 지원하므로 관리 인터페이스가 DHCP 서버에서 IPv4 주소를 수신할 수 있습니다. 관리 인터페이스는 또한 방화벽이 호스트 이름과 클라이언트 식별자를 각각 DHCP 서버에 보낼 수 있도록 하는 DHCP 옵션 12 및 옵션 61을 지원합니다.

기본적으로 AWS 및 Azure™에 배포된 VM 시리즈 방화벽은 관리 인터페이스를 DHCP 클라이언트로 사용하여 정적 IP 주소가 아닌 해당 IP 주소를 가져옵니다. 클라우드 배포에는 이 기능이 제공하는 자동화가 필요하기 때문입니다. 관리 인터페이스의 DHCP는 AWS 및 Azure의 VM 시리즈 방화벽을 제외하고 VM 시리즈 방화벽에 대해 기본적으로 꺼져 있습니다. WildFire 및 Panorama 모델의 관리 인터페이스는 이 DHCP 기능을 지원하지 않습니다.

- 하드웨어 기반 방화벽 모델*(VM* 시리즈 아님*)*의 경우 가능하면 정적 *IP* 주소로 관리 인터페이스를 구성하십시오.
- 방화벽이 *DHCP*를 통해 관리 인터페이스 주소를 획득하는 경우 해당 방화벽을 제공하는 *DHCP* 서버에 *MAC* 주소 예약을 할당합니다. 예약은 방화벽이 다시 시작된 후에도 관리 *IP* 주소를 유지하도록 합니다. *DHCP* 서버가 *Palo Alto Networks®* 방화벽인 경우 주소 예약을 위해 인터페이스를 DHCP 서버로 구성의 *6*단계를 참조하십시오.

관리 인터페이스를 DHCP 클라이언트로 구성하는 경우 다음 제한 사항이 적용됩니다.

- 제어 링크(HA1 또는 HA1 백업), 데이터 링크(HA2 또는 HA2 백업) 또는 패킷 전달(HA3) 통신을 위해 HA 구성에서 관리 인터페이스를 사용할 수 없습니다.
- 서비스 경로를 사용자 정의할 때 **MGT**를 소스 인터페이스로 선택할 수 없습니다 (**Device** > **Setup** > **Services** > **Service Route Configuration** > **Customize**). 그러나 기본값 사용을 선택하여 관리 인터페이스를 통해 패킷을 라우팅할 수 있습니다.
- 관리 인터페이스의 동적 IP 주소를 사용하여 HSM(하드웨어 보안 모듈)에 연결할 수 없습니다. HSM은 IP 주소를 사용하여 방화벽을 인증하고 런타임 중에 IP 주소가 변경되면 HSM에 대한 작업이 작동을 중지하므로 HSM 클라이언트 방화벽의 IP 주소는 정적 IP 주소여야 합니다.

이 작업의 전제 조건은 관리 인터페이스가 DHCP 서버에 연결할 수 있어야 한다는 것입니다.

STEP 1 | DHCP 서버에서 IP 주소(IPv4), 넷마스크(IPv4) 및 기본 게이트웨이를 수신할 수 있도록 관리 인터페이스를 DHCP 클라이언트로 구성합니다.

선택적으로 사용하는 오케스트레이션 시스템이 이 정보를 수락하는 경우 관리 인터페이스의 호스트 이름과 클라이언트 식별자를 DHCP 서버로 보낼 수도 있습니다.

1. 디바이스 > 설정 > 관리를 선택하고 관리 인터페이스 설정을 편집합니다.
2. **IP** 유형에서 **DHCP** 클라이언트를 선택합니다.
3. (선택 사항) DHCP 검색 또는 요청 메시지에서 방화벽이 DHCP 서버로 보낼 옵션 중 하나 또는 둘 다를 선택합니다.
   - 호스트 이름 보내기 - DHCP 옵션 12의 일부로 호스트 이름(디바이스 > 설정 > 관리에 정의됨)을 보냅니다.
   - 클라이언트 **ID** 보내기 - DHCP 옵션 61의 일부로 클라이언트 식별자를 보냅니다. 클라이언트 식별자는 DHCP 클라이언트를 고유하게 식별하고 DHCP 서버는 이를 사용하여 구성 매개변수 데이터베이스를 인덱싱합니다.
4. 확인을 클릭합니다.

STEP 2 | (선택 사항) DHCP 서버의 호스트 이름과 도메인을 허용하도록 방화벽을 구성합니다.

1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 편집합니다.
2. 다음 옵션 중 하나 또는 둘 다를 선택합니다.
   - **DHCP** 서버 제공 호스트 이름 수락 - 방화벽이 DHCP 서버의 호스트 이름을 수락하도록 허용합니다(유효한 경우). 활성화되면 DHCP 서버의 호스트 이름이 디바이스 > 설정 > 관리에 지정된 기존 호스트 이름을 덮어씁니다. 호스트 이름을 수동으로 구성하려면 이 옵션을 선택하지 마십시오.
   - **DHCP** 서버 제공 도메인 수락 - 방화벽이 DHCP 서버의 도메인을 수락하도록 허용합니다. DHCP 서버의 도메인(DNS 접미사)은 디바이스 > 설정 > 관리에 지정된 기존 도메인을 덮어씁니다. 도메인을 수동으로 구성하려면 이 옵션을 선택하지 마십시오.
3. 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

STEP 4 | DHCP 클라이언트 정보를 봅니다.

1. 디바이스 > 설정 > 관리 및 관리 인터페이스 설정을 선택합니다.
2. **DHCP** 클라이언트 런타임 정보 표시를 클릭합니다.

STEP 5 | (선택 사항) 임대 기간에 관계없이 DHCP 서버로 DHCP 임대를 갱신합니다.

이 옵션은 네트워크 문제를 테스트하거나 해결할 때 편리합니다.

1. 디바이스 > 설정 > 관리를 선택하고 관리 인터페이스 설정을 편집합니다.
2. **DHCP** 클라이언트 런타임 정보 표시를 클릭합니다.
3. 갱신을 클릭합니다.

STEP 6 | (선택 사항) DHCP 서버에서 제공된 다음 DHCP 옵션을 해제합니다.

- IP 주소
- 넷마스크
- 기본 게이트웨이
- DNS 서버(기본 및 보조)
- NTP 서버(기본 및 보조)
- 도메인(DNS 접미사)

릴리스는 *IP* 주소를 해제하여 네트워크 연결을 끊고 관리 액세스를 위해 구성된 다른 인터페이스가 없는 경우 방화벽을 관리할 수 없게 만듭니다.

CLI 작동 명령 **`request dhcp client management-interface release`**를 사용합니다.

인터페이스를 DHCP 릴레이 에이전트로 구성

방화벽 인터페이스가 클라이언트와 서버 간에 DHCP 메시지를 전송하도록 하려면, 방화벽을 DHCP 릴레이 에이전트로 구성해야 합니다. 인터페이스는 최대 8개의 외부 IPv4 DHCP 서버와 8개의 외부 IPv6 DHCP 서버에 메시지를 전달할 수 있습니다. 클라이언트 DHCPDISCOVER 메시지는 구성된 모든 서버로 전송되고, 응답하는 첫 번째 서버의 DHCPOFFER 메시지는 요청한 클라이언트로 다시 중계됩니다.

용량은 다음과 같습니다.

- PA-5200 시리즈 및 PA-7000 시리즈 방화벽을 제외한 모든 방화벽 모델에서 총 500개의 DHCP 서버(IPv4) 및 DHCP 릴레이 에이전트(IPv4 및 IPv6)를 구성할 수 있습니다.
- PA-5220 방화벽에서는 구성된 DHCP 서버 수를 뺀 최대 500개의 DHCP 서버와 최대 2,048개의 DHCP 릴레이 에이전트를 구성할 수 있습니다. 예를 들어 500개의 DHCP 서버를 구성하는 경우 1,548개의 DHCP 릴레이 에이전트를 구성할 수 있습니다.
- PA-5250, PA-5260 및 PA-7000 시리즈 방화벽에서 최대 500개의 DHCP 서버와 최대 4,096개의 DHCP 릴레이 에이전트에서 구성된 DHCP 서버 수를 뺀 값을 구성할 수 있습니다. 예를 들어, 500개의 DHCP 서버를 구성하는 경우 3,596개의 DHCP 릴레이 에이전트를 구성할 수 있습니다.

DHCP 릴레이 에이전트를 구성하기 전에, 레이어 3 이더넷 또는 레이어 3 VLAN 인터페이스를 구성했는지, 인터페이스가 가상 라우터 및 영역에 할당되었는지 확인합니다.

STEP 1 | DHCP 릴레이를 선택합니다.

Network > **DHCP** > **DHCP** 릴레이를 선택합니다.

STEP 2 | DHCP 릴레이 에이전트가 통신할 각 DHCP 서버의 IP 주소를 지정합니다.

1. 인터페이스 필드에서 DHCP 릴레이 에이전트로 사용할 인터페이스를 선택합니다.
2. 지정할 DHCP 서버 주소의 유형을 나타내는 **IPv4** 또는 **IPv6** 중 하나를 선택합니다.
3. **IPv4**를 선택한 경우 **DHCP** 서버 **IP** 주소 필드에서 DHCP 메시지를 릴레이할 DHCP 서버의 주소를 추가합니다.
4. **IPv6**를 선택한 경우 **DHCP** 서버 **IPv6** 주소 필드에 DHCP 메시지를 릴레이할 DHCP 서버 주소를 추가합니다. 멀티캐스트 주소를 지정하는 경우 발신 인터페이스도 지정합니다.
5. (선택 사항) 앞의 세 단계를 반복하여 IP 주소 패밀리당 최대 8개의 DHCP 서버 주소를 입력합니다.

STEP 3 | 구성을 커밋합니다.

확인 및 커밋을 클릭합니다.

DHCP 모니터링 및 문제 해결

CLI에서 명령을 실행하여 DHCP 서버가 할당했거나 DHCP 클라이언트가 할당된 동적 주소 임대의 상태를 볼 수 있습니다. 또한 시간이 초과되어 자동으로 해제되기 전에 임대를 해제할 수 있습니다.

- DHCP 서버 정보 보기
- DHCP 리스 해제
- DHCP 클라이언트 정보 보기
- DHCP에 대한 디버그 출력 수집

DHCP 서버 정보 보기

DHCP 풀 통계, DHCP 서버가 할당한 IP 주소, 해당 MAC 주소, 임대 상태 및 기간, 임대가 시작된 시간을 보려면 이 작업을 수행하십시오. 주소가 예약된 주소로 구성된 경우 **상태** 열은 **예약됨**을 나타내며 **지속 시간** 또는 **임대 시간**이 없습니다. 임대가 무제한으로 구성된 경우 **기간**열에 **0**값이 표시됩니다.

- DHCP 풀 통계, 할당된 DHCP 서버의 IP 주소, MAC 주소, 임대 상태 및 기간, 임대 시작 시간을 봅니다.

```
admin@PA-220> show dhcp server lease interface all
```

```
interface: "ethernet1/2" Allocated IPs: 1, Total number of IPs
 in pool: 5. 20.0000% used ip mac state duration lease_time
 192.168.3.11 f0:2f:af:42:70:cf committed 0 Wed Jul 2 08:10:56 2014
 admin@PA-220>
```

- DHCP 서버가 클라이언트에 할당한 옵션을 봅니다.

```
admin@PA-220> show dhcp server settings all
```

```
Interface     GW           DNS1         DNS2        DNS-Suffix Inherit
 source
 ----------------------------------------------------------------------------
 ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10
             ethernet1/3 admin@PA-220>
```

DHCP 리스 해제

DHCP 리스를 해제하기 위한 몇 가지 옵션을 가집니다.

- 보류 타이머가 자동으로 그것들을 해제되기 전에 이더넷1/2와 같은, 인터페이스(서버)의 만료된 DHCP 리스를 해제합니다. 해당 주소는 IP 풀에서 다시 사용할 수 있습니다.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

- 특정 IP 주소의 리스를 해제합니다(예를 들어, 192.168.3.1).

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

- 예를 들어, f0:2c:ae:29:71:34와 같은 특정 MAC 주소의 리스를 해제합니다.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac
 f0:2c:ae:29:71:34
```

DHCP 클라이언트 정보 보기

방화벽이 DHCP 클라이언트로 작동할 때 방화벽으로 전송된 IP 주소 임대의 상태를 보려면 다음 CLI 커맨드 중 하나를 사용합니다.

- `admin@PA-220>`**`show dhcp client state <interface_name>`**
- `admin@PA-220>` **`show dhcp client state all`**

```
Interface State IP Gateway Leased-until
 ------------------------------------------------------------------------------
 ethernet1/1 Bound 10.43.14.80 10.43.14.1 70315 admin@PA-220>
```

DHCP에 대한 디버그 출력 수집

DHCP에 대한 디버그 출력을 수집하려면 다음 명령 중 하나를 사용합니다.

- `admin@PA-220>` **`debug dhcpd`**
- `admin@PA-220>` **`debug management-server dhcpd`**

DNS

DNS(Domain Name System)는 www.paloaltonetworks.com과 같은 사용자 친화적인 도메인 이름을 IP 주소로 변환(해석)하여 사용자가 인터넷이나 사설 네트워크의 컴퓨터, 웹사이트, 서비스 또는 기타 리소스에 액세스할 수 있도록 하는 프로토콜입니다.

DNS 개요

DNS는 사용자가 IP 주소를 기억할 필요가 없고 개별 컴퓨터가 IP 주소에 매핑된 방대한 양의 도메인 이름을 저장할 필요가 없도록 네트워크 리소스에 대한 사용자 액세스를 가능하게 하는 중요한 역할을 수행합니다. DNS는 클라이언트/서버 모델을 사용합니다. DNS 서버는 캐시에서 도메인을 조회하고 필요한 경우 해당 IP 주소로 클라이언트에 응답할 수 있을 때까지 다른 서버에 쿼리를 전송하여 DNS 클라이언트에 대한 쿼리를 해결합니다.

도메인 이름의 DNS 구조는 계층적입니다. 도메인 이름의 최상위 도메인(TLD)은 일반 TLD(gTLD): com, edu, gov, int, mil, net 또는 org(gov 및 mil은 미국 전용) 또는 국가 코드일 수 있습니다. (ccTLD)(예: au(호주) 또는 us(미국)). ccTLD는 일반적으로 국가 및 종속 지역용으로 예비되어 있습니다.

FQDN(정규화된 도메인 이름)에는 최소한 호스트 이름, 두 번째 수준 도메인 및 DNS 구조에서 호스트의 위치를 완전히 지정하는 TLD가 포함됩니다. 예를 들어 www.paloaltonetworks.com은 FQDN입니다.

Palo Alto Networks® 방화벽이 사용자 인터페이스 또는 CLI에서 FQDN을 사용할 때마다 방화벽은 DNS를 사용하여 해당 FQDN을 확인해야 합니다. ®FQDN 쿼리가 시작된 위치에 따라 방화벽은 쿼리를 해결하는 데 사용할 DNS 설정을 결정합니다.

FQDN의 DNS 레코드에는 TTL(Time-to-Live)값이 포함되며, 기본적으로 방화벽은 최소 FQDN 새로 고침 설정보다 크거나 같은 경우나, TTL이 최소 FQDN 새로 고침 시간을 구성하지 않은 경우 기본 설정인 30초와 동일할 때, 개별 TTL에 기반한 캐시에서 각 FQDN을 새로 고침합니다. TTL 값을 기반으로 FQDN을 새로 고치는 것은 고가용성 서비스를 보장하기 위해 자주 FQDN을 새로 고쳐야 하는 클라우드 플랫폼 서비스에 대한 액세스를 보호하는 데 특히 유용합니다. 예를 들어, Autoscaling을 지원하는 클라우드 환경은 서비스를 동적으로 확장 및 축소하기 위한 FQDN 해상도에 의존하며, FQDN의 빠른 해상도는 이러한 시간에 민감한 환경에서 매우 중요합니다.

최소 FQDN 새로 고침 시간을 구성하여 방화벽이 적용하는 TTL 값의 작은 크기를 제한합니다. IP 주소가 자주 변경되지 않는 경우 방화벽이 항목을 불필요하게 새로 고치지 않도록 더 큰 최소 FQDN 새로 고침 시간을 설정할 수 있습니다. 방화벽은 DNS TTL 시간과 구성된 최소 FQDN 새로 고침 시간 중 더 큰 시간을 사용합니다.

예를 들어 두 개의 FQDN에는 다음과 같은 TTL 값이 있습니다. 최소 FQDN 새로 고침 시간은 더 작은(빠른) TTL 값을 재정의합니다.

	TTL	최소 **FQDN** 새로 고침 **= 26**인 경우	실제 새로 고침 시간
FQDN A	20		26
FQDN B	30		30

FQDN 새로 고침 타이머는 방화벽이 FQDN을 확인하는 DNS 서버 또는 DNS 프록시 개체로부터 DNS 응답을 수신할 때 시작됩니다.

또한 DNS 서버에 연결할 수 없는 경우 방화벽이 부실(만료) FQDN 확인을 계속 사용하는 기간을 구성하기 위해 부실 시간 제한을 설정할 수 있습니다. 부실 시간 초과 기간이 끝날 때 DNS 서버에 여전히 연결할 수 없으면 부실 FQDN 항목이 확인되지 않습니다(방화벽에서 부실 FQDN 항목 제거).

다음 방화벽 작업은 DNS와 관련됩니다.

- 호스트 이름을 확인할 수 있도록 하나 이상의 DNS 서버로 방화벽을 구성하십시오. 사용 사례 1: 방화벽에 DNS 확인 필요에 표시된 대로 기본 및 보조 DNS 서버 또는 이러한 서버를 지정하는 DNS 프록시 개체를 구성합니다.
- 사용 사례 2에 표시된 것처럼 방화벽이 보안 정책 규칙, 보고 및 관리 서비스(예: 이메일, Kerberos, SNMP, syslog 등)에 의해 시작된 DNS 확인을 처리하는 방법을 사용자 지정합니다. ISP 테넌트는 DNS 프록시를 사용하여 가상 시스템 내에서 보안 정책, 보고 및 서비스에 대한 DNS 확인을 처리합니다.
- 사용 사례 3과 같이 클라이언트의 DNS 서버 역할을 하도록 방화벽을 구성합니다. 방화벽은 클라이언트와 서버 사이에서 DNS 프록시 역할을 합니다.
- DNS 쿼리를 사용하여 네트워크에서 감염된 호스트를 식별하도록 스파이웨어 방지 프로파일을 구성합니다.
- 회피 서명을 활성화한 다음 위협 방지를 위한 회피 서명을 활성화합니다.
- 인터페이스를 DHCP 서버로 구성합니다. 이렇게 하면 방화벽이 DHCP 서버 역할을 하고 DNS 정보를 DHCP 클라이언트에 전송하여 프로비저닝된 DHCP 클라이언트가 해당 DNS 서버에 접근할 수 있습니다.

DNS 프록시 개체

DNS 프록시로 구성된 경우 방화벽은 DNS 클라이언트와 서버 사이의 중개자입니다. DNS 프록시 캐시에서 쿼리를 해결하여 DNS 서버 자체로 작동합니다. DNS 프록시 캐시에서 도메인 이름을 찾지 못하면 방화벽은 특정 DNS 프록시 개체(DNS 쿼리가 도착한 인터페이스에서)의 항목 중에서 도메인 이름과 일치하는 항목을 검색합니다. 방화벽은 일치 결과에 따라 쿼리를 적절한 DNS 서버로 전달합니다. 일치하는 항목이 없으면 방화벽은 기본 DNS 서버를 사용합니다.

DNS 프록시 개체는 방화벽이 DNS 프록시로 작동하는 방식을 결정하는 설정을 구성하는 곳입니다. 단일 가상 시스템에 DNS 프록시 개체를 할당하거나 모든 가상 시스템에서 공유할 수 있습니다.

- DNS 프록시 개체가 가상 시스템용인 경우 다른 정보와 함께 기본 및 보조 DNS 서버 주소를 지정하는 DNS 서버 프로파일을(를) 지정할 수 있습니다. DNS 서버 프로파일은 구성을 단순화합니다.
- DNS 프록시 개체가 공유되는 경우 최소한 DNS 서버의 기본 주소를 지정해야 합니다.

DNS** 서비스로 여러 테넌트**(ISP** 가입자**)**를 구성할 때 각 테넌트에는 고유한 **DNS** 프록시가 정의되어 있어야 합니다**.

프록시 개체에서 방화벽이 DNS 프록시 역할을 하는 인터페이스를 지정합니다. 인터페이스의 DNS 프록시는 서비스 경로를 사용하지 않습니다. DNS 요청에 대한 응답은 항상 DNS 요청이 도착한 가상 라우터에 할당된 인터페이스로 전송됩니다.

DNS 프록시 개체 구성인 경우 정적 FQDN-주소 매핑이 있는 DNS 프록시를 제공할 수 있습니다. 또한 도메인 이름 쿼리(프록시 규칙과 일치)가 전달되는 DNS 서버를 제어하는 DNS 프록시 규칙을 만들 수도 있습니다. 방화벽에서 최대 256개의 DNS 프록시 개체를 구성할 수 있습니다. 이 DNS 프록시 개체가 **Device** > **Setup** > **Services** > **DNS** 또는 **Device** > **Virtual Systems** > **vsys** > **General** > **DNS** 프록시에 할당된 경우 캐시 및 캐시 **EDNS** 응답(**Network** > **DNS** 프록시 > 고급 아래)을 활성화해야 합니다. 또한 이 DNS 프록시 개체에**DNS** 프록시 규칙이 구성되어 있는 경우 해당 규칙도 캐시를 활성화해야 합니다(이 매핑으로 확인된 도메인 캐싱 켜기).

방화벽이 FQDN 쿼리를 수신하고 도메인 이름이 DNS 프록시 캐시에 없으면 방화벽은 FQDN 쿼리의 도메인 이름을 DNS 프록시 개체의 DNS 프록시 규칙에 있는 도메인 이름과 비교합니다. 단일 DNS 프록시 규칙에 여러 도메인 이름을 지정하는 경우 규칙의 도메인 이름 중 하나와 일치하는 쿼리는 규칙과 쿼리가 일치함을 의미합니다. DNS 프록시 규칙 및 FQDN 일치을(는) 방화벽이 FQDN이 DNS 프록시 규칙의 도메인 이름과 일치하는지 여부를 결정하는 방법을 설명합니다. 규칙과 일치하는 DNS 쿼리는 확인할 프록시 개체에 대해 구성된 기본 DNS 서버로 전송됩니다.

DNS 서버 프로파일

가상 시스템의 구성을 단순화하기 위해 DNS 서버 프로파일을 사용하면 구성 중인 가상 시스템, DNS 서버의 상속 소스 또는 기본 및 보조 IP 주소, DNS 서버로 전송되는 패킷에 사용되는 소스 인터페이스 및 소스 주소(서비스 경로)를 지정할 수 있습니다. 소스 인터페이스는 라우팅 테이블이 있는 가상 라우터를 결정합니다. 대상 IP 주소는 소스 인터페이스가 할당된 가상 라우터의 경로 테이블에서 조회됩니다. 대상 IP 송신 인터페이스의 결과가 소스 인터페이스와 다를 수 있습니다. 패킷은 경로 테이블 조회에 의해 결정된 대상 IP 송신 인터페이스를 벗어나지만 소스 IP 주소는 구성된 주소가 됩니다. 원본 주소는 DNS 서버의 응답에서 대상 주소로 사용됩니다.

가상 시스템 보고서 및 가상 시스템 서버 프로파일은 가상 시스템에 대해 지정된 DNS 서버(있는 경우)로 쿼리를 보냅니다. (사용된 DNS 서버는 디바이스 > 가상 시스템 > 일반 > **DNS** 프록시에 정의되어 있습니다.) 가상 시스템에 대해 지정된 DNS 서버가 없으면 방화벽에 대해 지정된 DNS 서버를 쿼리합니다.

DNS 서버 프로필 구성 가상 시스템 전용입니다. 전역 공유 위치용이 아닙니다.

다중 테넌트 DNS 배포

방화벽은 요청이 시작된 위치에 따라 DNS 요청을 처리하는 방법을 결정합니다. ISP가 방화벽에 여러 테넌트를 있는 환경을 다중 테넌트라고 합니다. 다중 테넌트 DNS 배포에는 세 가지 사용 사례가 있습니다.

- 글로벌 관리 **DNS** 해결— 방화벽은 소프트웨어 업데이트 서비스와 같은 관리 이벤트에 대한 FQDN을 해결하기 위해 관리 평면에서 요청이 필요합니다. 특정 가상 라우터에서 DNS 요청이 들어오지 않기 때문에 방화벽은 서비스 경로를 사용하여 DNS 서버에 도달합니다.
- 가상 시스템에 대한 정책 및 보고서 **FQDN** 해상도-보안 정책, 보고서 또는 서비스의 DNS 쿼리의 경우 가상 시스템(테넌트)과 관련된 DNS 서버 집합을 지정하거나 전역 DNS 서버로 기본값으로 지정할 수 있습니다. 사용 사례에 가상 시스템당 다른 DNS 서버 집합이 필요한 경우 DNS 프록시 개체를 구성해야 합니다. 해상도는 DNS 프록시가 할당된 가상 시스템에 맞춥니다. 이 가상 시스템에 적용할 수 있는 특정 DNS 서버가 없는 경우 방화벽은 전역 DNS 설정을 사용합니다.
- 가상 시스템에 대한 데이터플레인 **DNS** 해상도-이 메서드는 DNS 해상도에 대한 네트워크 요청이라고도 합니다. 테넌트의 가상 시스템을 구성하여 네트워크의 테넌트의 DNS 서버에서 지정된 도메인 이름이 해결되도록 할 수 있습니다. 이 메서드는 ***DNS*** 분할을 지원하므로 테넌트는 자체 서버에서 해결되지 않은 나머지 DNS 쿼리에 자체 ISP DNS 서버도 사용할 수 있습니다. DNS 프록시 개체 규칙은 분할 DNS를 제어하며 테넌트의 도메인은 DNS 서버 프로파일에서 구성된 DNS 서버로 DNS 요청을 리디렉션합니다. DNS 서버 프로파일에는 기본 및 보조 DNS 서버가 지정되어 있으며 기본 DNS 설정을 재정의하는 IPv4 및 IPv6에 대한 DNS 서비스 경로도 지정되어 있습니다.

다음 표는 DNS 해상도 유형을 요약합니다. 바인딩 위치는 해상도에 사용되는 DNS 프록시 개체를 결정합니다. 실제 예를 든 목적은, 서비스 공급자가 방화벽과 테넌트(구독자) 가상 시스템에 필요한 DNS 쿼리를 해결하기 위해 DNS 서비스를 제공하도록 DNS 설정을 구성하는 방법을 보여주려는 것입니다.

해상도 유형	위치**:** 공유	위치**:** 특정 **Vsys**
관리 평면에서 수행되는 방화벽 DNS 해결	바인딩: 글로벌 사용 사례 1에 대한 설명	해당 사항 없음
관리 평면에서 수행되는 보안 프로파일, 보고 및 서버 프로파일 해결	바인딩: 글로벌 사례 사용과 동일한 동작 1	바인딩: 특정 vsys 사용 사례 2에 대한 설명
방화벽의 인터페이스에 연결된 DNS 클라이언트 호스트에 대한 DNS 프록시 해상도, 데이터 평면에서 수행되는 DNS 서버로 방화벽을 통과	바인딩: 인터페이스 서비스 경로: DNS 요청이 수신된 인터페이스 및 IP 주소입니다. 사용 사례 3에 대한 설명	

- 사용 사례 1: 방화벽에 DNS 확인 필요
- 사용 사례 2: ISP 테넌트는 DNS 프록시를 사용하여 가상 시스템 내에서 보안 정책, 보고 및 서비스에 대한 DNS 레졸루션을 처리합니다.
- 사용 사례 3: 방화벽은 클라이언트와 서버 사이에서 DNS 프록시 역할을 합니다.

DNS 프록시 개체 구성

방화벽이 DNS 프록시 역할을 하는 경우 이 작업을 수행하여 DNS 프록시 개체를 구성합니다. 프록시 개체는 모든 가상 시스템 간에 공유되거나 특정 가상 시스템에 적용할 수 있습니다.

방화벽이 *DNS* 프록시 역할을 할 수 있도록 활성화되면 만들어진 *HTTP* 또는 *TLS* 요청을 감지한 회피 서명은 클라이언트가 원래 *DNS* 쿼리에 지정된 도메인 이외의 도메인에 연결하는 인스턴스에 경고할 수 있습니다. 모범 사례로 *DNS* 프록시를 구성한 후 회피 서명을 활성화하여 만들어진 요청이 감지되면 경고를 트리거합니다.

STEP 1 | DNS 프록시 개체에 대한 기본 설정을 구성합니다.

1. 네트워크 > **DNS** 프록시를 선택하고 새 개체를 추가합니다.
2. 활성화가 선택되었는지 확인합니다.
3. 개체의 이름을 입력합니다.
4. 위치의 경우 개체가 적용되는 가상 시스템을 선택합니다. 공유를 선택하는 경우 기본 DNS 서버 주소와 선택적으로 보조 주소를 지정해야 합니다.
5. 서버 프로파일의 가상 시스템을 선택한 경우 DNS 서버 프로파일을 선택하거나 **DNS** 서버 프로파일을 클릭하여 새 프로파일을 구성합니다. DNS 서버 프로파일 구성을 참조하십시오.
6. 상속 소스의 경우 기본 DNS 서버 설정을 상속할 원본을 선택합니다. 기본값은 없음입니다.
7. 인터페이스의 경우 DNS 프록시 개체가 적용되는 인터페이스 추가를 클릭하고 지정합니다.
   - DNS 조회를 수행하기 위해 DNS 프록시 개체를 사용하는 경우 인터페이스가 필요합니다. 방화벽은 이 인터페이스에서 DNS 요청을 듣고 프록시합니다.
   - 서비스 경로에 DNS 프록시 개체를 사용하는 경우 인터페이스는 선택 사항입니다.

STEP 2 | (선택 사항) DNS 프록시 규칙을 지정합니다.

1. **DNS** 프록시 규칙 탭에서 규칙의 이름을 추가합니다.
2. 방화벽이 해결된 도메인을 캐시하려는 경우 이 매핑에서 해결된 도메인캐싱을 켭니다.
3. 도메인 이름의 경우 방화벽이 FQDN 쿼리를 비교하는 행당 하나의 항목인 하나 이상의 도메인을 추가합니다. 쿼리가 규칙의 도메인 중 하나와 일치하는 경우 쿼리가 해결될 다음 서버 중 하나로 전송됩니다(이전 단계에서 구성한 내용에 따라 다름).
   - 이 프록시 개체에 대해 직접 지정된 기본 또는 보조 DNS 서버입니다.
   - 이 프록시 개체에 대한 DNS 서버 프로필에 지정된 기본 또는 보조 DNS 서버입니다.

   DNS 프록시 규칙 및 FQDN 매칭은 방화벽이 FQDN의 도메인 이름과 DNS 프록시 규칙과 일치하는 방법을 설명합니다. 일치하는 항목이 없는 경우 기본 DNS 서버가 쿼리를 해결합니다.
4. 위치를 설정한 항목에 따라 다음 중 하나를 수행합니다.
   - 가상 시스템을 선택한 경우 **DNS** 서버 프로파일을 선택합니다.
   - 공유를 선택한 경우 기본 주소와 선택적으로 보조 주소를 입력합니다.
5. 확인을 클릭합니다.

STEP 3 | (선택 사항)정적 FQDN-주소 항목으로 DNS 프록시를 제공합니다. 정적 DNS 항목을 사용하면 방화벽이 DNS 서버에 쿼리를 보내지 않고도 FQDN을 IP 주소로 확인할 수 있습니다.

1. 정적 항목 탭에서 이름을추가합니다.
2. 정규화된 도메인 이름(**FQDN**)을 입력합니다.
3. 주소의 경우 FQDN을 매핑해야 하는 IP 주소를 추가합니다.

   항목에 대한 추가 IP 주소를 제공할 수 있습니다. 방화벽은 DNS 응답에서 모든 IP 주소를 제공하고 클라이언트는 사용할 주소를 선택합니다.
4. 확인을 클릭합니다.

STEP 4 | 캐싱을 활성화하고 DNS 프록시에 대한 다른 고급 설정을 구성합니다.

1. 고급 탭에서 **TCP** 쿼리를 선택하여 TCP를 사용하여 DNS 쿼리를 활성화합니다.
   - 최대 보류 중인 요청- 방화벽이 지원할 최대 동시 TCP DNS 요청을 입력합니다(범위는 64-256; 기본값은 64개).
2. **UDP** 쿼리 재시도의 경우 다음을 입력합니다.
   - 간격**(**초**)**—응답이 수신되지 않은 경우 다른 요청이 전송된 시간(초)입니다(범위는 1~30개, 기본값은 2).
   - 시도— 다음 DNS 서버가 쿼리된 후 UDP 쿼리 시도 횟수(첫 번째 시도 제외)는 범위(범위는 1~30개, 기본값은 5)입니다.
3. 방화벽이 학습하는 FQDN-주소 매핑을 캐시할 수 있도록 캐시를 선택합니다. 이 DNS 프록시 개체가 방화벽이 생성하는 쿼리(즉, 디바이스 > 설정 > 서비스 > **DNS**에서 또는 디바이스 > 가상 시스템에서 사용되고 가상 시스템 및 일반 > **DNS** 프록시)를선택하는 경우 캐시(기본적으로 활성화됨)를 사용하도록 설정해야 합니다.
   - **TTL** 활성화를 선택하여 방화벽이 프록시 개체에 대한 DNS 해결 항목을 캐시하는 시간을 제한합니다. 기본적으로 비활성화됩니다.
     - 프록시 개체에 대한 모든 캐시된 항목이 제거된 유지 시간**(**초**)**를입력합니다. 항목을 제거한 후 새 DNS 요청을 해결하고 다시 캐시해야 합니다. 범위는 60-86,400입니다. 기본 TTL은 없습니다. 방화벽이 캐시 메모리가 부족할 때까지 항목이 유지됩니다.
   - 캐시 **EDNS** 응답-이 DNS 프록시 개체가 방화벽이 생성하는 쿼리(즉, 디바이스 > 설정 > 서비스 > **DNS**, 또는 디바이스 > 가상 시스템 하에서 사용되고 가상 시스템 및 일반 > **DNS** 프록시)를 선택하는 경우 이 설정을 사용하도록 설정해야 합니다.

STEP 5 | 변경 내용을 커밋합니다.

확인 및 커밋을 클릭합니다.

DNS 서버 프로필 구성

가상 시스템 구성을 단순화하는, DNS 서버 프로필을 구성합니다. 기본 **DNS** 또는 보조 **DNS** 주소는 가상 시스템이 DNS 서버로 보내는 DNS 요청을 만드는 데 사용됩니다.

STEP 1 | DNS 서버 프로필의 이름을 지정하고 해당 프로필이 적용되는 가상 시스템을 선택한 다음 기본 및 보조 DNS 서버 주소를 지정합니다.

1. 디바이스 > 서버 프로파일 > **DNS**를 선택하고 DNS 서버 프로파일의 이름을 추가합니다.
2. 위치에서 프로파일이 적용되는 가상 시스템을 선택합니다.
3. 상속 소스에 대, DNS 서버 주소가 상속되지 않은 경우 없음을 선택합니다. 그렇지 않으면 프로파일이 설정을 상속해야 하는 DNS 서버를 지정합니다. DNS 서버를 선택하는 경우 상속 소스 상태 확인을 클릭하여 해당 정보를 확인합니다.
4. 기본 **DNS** 서버의 IP 주소를 지정하거나 상속 소스를 선택한 경우 상속된 상태로 둡니다.

   IP 주소 대신 FQDN을 지정하면, 해당 FQDN의 DNS가 장치 **>** *가상 시스템* **>** ***DNS*** *프록시에서 확인됩니다.*

5. 보조 **DNS** 서버의 IP 주소를 지정하거나 상속 소스를 선택한 경우 상속됨 상태로 둡니다.

STEP 2 | 대상 DNS 서버에 IPv4 또는 IPv6의 IP 주소 패밀리 유형이 있는지 여부에 따라 방화벽이 자동으로 사용하는 서비스 경로를 구성합니다.

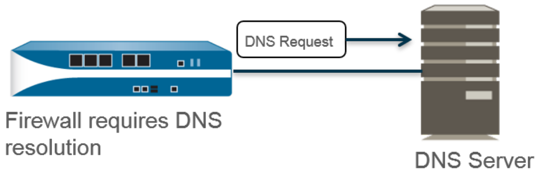
1. 대상 DNS 주소가 IPv4 주소인 경우 서비스 경로 **IPv4**를 클릭하여 후속 인터페이스와 IPv4 주소를 서비스 경로로 사용할 수 있도록 합니다.
2. 소스 인터페이스를 지정하여 서비스 경로가 사용할 DNS 서버의 소스 IP 주소를 선택합니다. 방화벽은 해당 인터페이스에 할당된 가상 라우터를 결정한 다음 가상 라우터 라우팅 테이블에서 경로 조회를 수행하여(기본 **DNS** 주소를 기반으로) 대상 네트워크에 도달합니다.
3. DNS 서버로 가는 패킷이 소싱되는 IPv4 소스 주소를 지정하십시오.
4. 대상 DNS 주소가 IPv6 주소인 경우 서비스 경로 **IPv6**를 클릭하여 후속 인터페이스와 IPv6 주소를 서비스 경로로 사용할 수 있도록 합니다.
5. 소스 인터페이스를 지정하여 서비스 경로가 사용할 DNS 서버의 소스 IP 주소를 선택합니다. 방화벽은 해당 인터페이스에 할당된 가상 라우터를 결정한 다음 가상 라우터 라우팅 테이블에서 경로 조회를 수행하여(기본 **DNS** 주소를 기반으로) 대상 네트워크에 도달합니다.
6. DNS 서버로 가는 패킷이 소싱되는 IPv6 소스 주소를 지정하십시오.
7. 확인을 클릭합니다.

STEP 3 | 구성을 커밋합니다.

확인 및 커밋을 클릭합니다.

사용 사례 1: 방화벽에 DNS 확인 필요

이 사용 사례에서 방화벽은 보안 정책 규칙, 보고, 관리 서비스(예: 이메일, Kerberos, SNMP, syslog 등) 및 소프트웨어 업데이트 서비스, 동적 소프트웨어, WildFire와 같은 관리 이벤트에 대한 FQDN을 확인하는 클라이언트 요청 DNS 해결책입니다. 동적 환경에서 FQDN은 더 자주 변경됩니다. 정확한 DNS 확인을 통해 방화벽은 정확한 정책을 시행하고 보고 및 관리 서비스를 제공하며 관리 이벤트를 처리할 수 있습니다. 공유 전역 DNS 서비스는 관리 플레인 기능에 대한 DNS 확인을 수행합니다.



STEP 1 | 방화벽이 DNS 확인에 사용할 기본 및 보조 DNS 서버를 구성합니다.

> *방화벽에서 하나 이상의 DNS 서버를 수동으로 구성해야 합니다. 그렇지 않으면 호스트 이름을 확인할 수 없습니다. 방화벽은 ISP와 같은 다른 소스의 DNS 서버 설정을 사용할 수 없습니다.*

1. 여러 가상 시스템을 지원하는 방화벽의 경우 서비스 설정(디바이스 > 설정 > 서비스 > 전역, 디바이스 > 설정 > 서비스하지 않는 경우).
2. 서비스 탭에서 **DNS**에 대해 서버를 선택하고 기본 **DNS** 서버 주소 및 보조 **DNS** 서버 주소를 입력합니다.
3. 3단계로 진행합니다.

STEP 2 | 또는 분할 DNS, DNS 프록시 재정의, DNS 프록시 규칙, 정적 항목 또는 DNS 상속과 같은 고급 DNS 기능을 구성하려는 경우 DNS 프록시 개체를 구성할 수 있습니다.

1. 여러 가상 시스템을 지원하는 방화벽의 경우 서비스 설정(디바이스 > 설정 > 서비스 > 전역, 디바이스 > 설정 > 서비스하지 않는 경우).
2. 서비스 탭에서 **DNS**에 대해 **DNS** 프록시 개체를 선택합니다.
3. **DNS** 프록시 목록에서 전역 DNS 서비스를 구성하는 데 사용할 DNS 프록시를 선택하거나 **DNS** 프록시를 선택하여 다음과 같이 새 DNS 프록시 개체를 구성합니다.
   1. 활성화한 다음 DNS 프록시 개체의 이름을 입력합니다.
   2. 여러 가상 시스템을 지원하는 방화벽에서 위치에 대해 방화벽 전체의 전역 DNS 프록시 서비스와 공유를 선택합니다.

      > *공유 DNS 프록시 개체는 테넌트 가상 시스템에 속하는 특정 서비스 경로가 필요하지 않기 때문에 DNS 서버 프로파일을 사용하지 않습니다.*

   3. 기본 DNS 서버 IP 주소를 입력합니다. 선택적으로 보조 DNS 서버 IP 주소를 입력합니다.
4. 고급 탭을 선택합니다. 캐시가 활성화되고 캐시 **EDNS** 응답이 활성화되어 있는지 확인합니다(둘 다 기본적으로 활성화되어 있음).
5. 확인을 클릭하여 DNS 프록시 개체를 저장합니다.

STEP 3 | (선택 사항) 최소 **FQDN** 새로 고침 시간**(**초**)**을 설정하여 방화벽이 FQDN 캐시 항목을 새로 고치는 빈도를 제한합니다.

기본적으로 방화벽은 TTL이 최소 FQDN 새로 고침 설정보다 크거나 같은 경우(또는 TTL이 또는 최소 FQDN 새로 고침 시간을 구성하지 않은 경우 기본 설정인 30초와 동일함)DNS 레코드의 FQDN을 위한 개별 TTL에 기반한 캐시에서 각 FQDN을 새로 고침합니다. 최소 FQDN 새로 고침 시간을 설정하려면 값을 초 단위로 입력합니다(범위는 0~14,400, 기본값은 30). 0으로 설정하면 방화벽이 DNS 레코드의 TTL 값을 기반으로 FQDN을 새로 고칩니다. 방화벽은 최소 FQDN 새로 고침 시간을 적용하지 않습니다. 방화벽은 DNS TTL 시간과 최소 FQDN 새로 고침 시간 중 더 높은 시간을 사용합니다.

> *DNS*의 *FQDN*에 대한 *TTL*이 짧지만 *FQDN* 해상도가 *TTL* 시간 프레임만큼 자주 변경되지 않으므로 더 빠른 새로 고침이 필요하지 않은 경우 *FQDN* 새로 고침을 필요 이상으로 더 자주 시도하지 않도록 최소 *FQDN* 새로 고침 시간을 설정해야 합니다.

STEP 4 | (선택 사항) DNS 서버에 연결할 수 없는 경우 방화벽이 계속 부실 FQDN 확인을 사용하는 시간(분 범위는 0 ~ 10,080, 기본값은 1,440)인 **FQDN** 부실 항목 시간 초과**(**분**)**를 지정합니다.

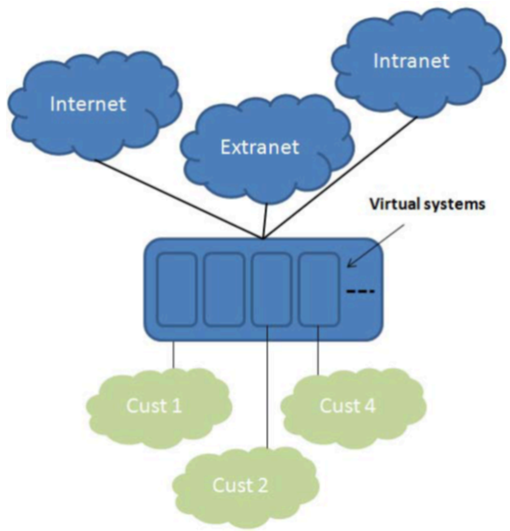
0으로 설정하면 방화벽이 부실 FQDN 항목을 계속 사용하지 않습니다.

> *FQDN* 부실 항목 시간 제한이 잘못된 트래픽 전달*(*보안 위험을 초래할 수 있음*)*을 허용하지 않을 만큼 충분히 짧고 계획되지 않은 네트워크 중단을 일으키지 않고 트래픽 연속성을 허용할 만큼 충분히 긴지 확인합니다.

STEP 5 | 확인 및 커밋을 클릭합니다.

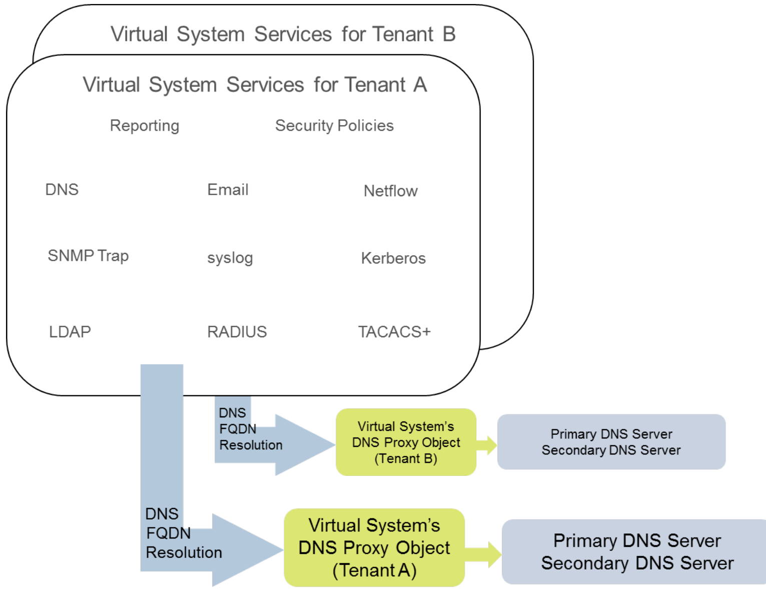
사용 사례 2: ISP 테넌트는 DNS 프록시를 사용하여 가상 시스템 내에서 보안 정책, 보고 및 서비스에 대한 DNS 해결을 처리합니다.

이 사용의 경우 여러 테넌트(ISP 구독자)가 방화벽에 정의되고 각 테넌트는 서비스 및 관리 도메인을 분할하기 위해 별도의 가상 시스템(vsys) 및 가상 라우터를 할당합니다. 다음 그림은 방화벽 내의 여러 가상 시스템을 보여 줍니다.



각 테넌트는 자체 네트워크에 정의된 보안 정책 규칙, 보고 및 관리 서비스(예: 이메일, Kerberos, SNMP, syslog 등)에 대한 자체 서버 프로파일을 보유하고 있습니다.

이러한 서비스에서 시작한 DNS 해상도의 경우 각 가상 시스템은 DNS 프록시 개체 각 테넌트가 가상 시스템 내에서 DNS 해상도를 처리하는 방식을 사용자 지정할 수 있도록 자체적으로 구성됩니다. 위치가 있는 모든 서비스는 가상 시스템에 대해 구성된 DNS 프록시 개체를 사용하여 다음 그림에 나온 것과 같이 FQDN을 해결하기 위해 기본(또는 보조) DNS 서버를 결정합니다.



STEP 1 | 각 가상 시스템에 대해 사용할 DNS 프록시를 지정합니다.

1. 디바이스 > 가상 시스템을 선택하고 가상 시스템의 **ID**(범위는 1-255)를 추가하고 선택적 이름(이 예에서는 Corp1 Corporation)을 추가합니다.
2. 일반 탭에서 **DNS** 프록시를 선택하거나 새 프록시를 만듭니다. 이 예에서 Corp1 DNS Proxy는 Corp1 Corporation의 가상 시스템에 대한 프록시로 선택됩니다.
3. 인터페이스의 경우 추가를 클릭합니다. 이 예에서 Ethernet1/20은 이 테넌트 전용입니다.
4. 가상 라우터의 경우 추가를 클릭합니다. 라우팅 기능을 분리하기 위해 가상 시스템에 Corp1 VR이라는 가상 라우터를 할당했습니다.
5. 확인을 클릭합니다.

STEP 2 | 가상 시스템에 대한 DNS 해상도를 지원하도록 DNS 프록시와 서버 프로파일을 구성합니다.

1. 네트워크 > **DNS** 프록시를 선택하고 추가를 클릭합니다.
2. 활성화를 클릭하고 DNS 프록시의 이름을 입력합니다.
3. 위치에 대해 테넌트의 가상 시스템(이 예에서는 Corp1 Corporation(vsys6))을 선택합니다. (대신 공유DNS 프록시 리소스를 선택할 수 있습니다.)
4. 서버 프로파일에서 프로파일을 선택하거나 생성하여 이 테넌트의 보안 정책, 보고 및 서버 프로파일 서비스에 대한 DNS 확인에 사용할 DNS 서버를 사용자 지정합니다.

   프로파일이 아직 구성되지 않은 경 우 서버 프로파일 필드에서 **DNS** 서버 프로파일을 클릭하여 DNS 서버 프로필 구성을(를) 수행합니다.

   DNS 서버 프로파일은 이 가상 시스템에 대한 관리 DNS 해결에 사용할 기본 및 보조 DNS 서버의 IP 주소를 식별합니다.
5. 또한 이 서버 프로파일에 대해 선택적으로 서비스 경로 **IPv4**및/또는 서비스 경로 **IPv6**을 구성하여 DNS 요청에 사용할 소스 인터페이스를 방화벽에 지시합니다. 해당 인터페이스에 둘 이상의 IP 주소가 있는 경우 소스 주소도 구성하십시오.
6. 고급 탭을 선택합니다. 캐시가 활성화되고 캐시 **EDNS** 응답이 활성화되어 있는지 확인합니다(둘 다 기본적으로 활성화되어 있음). DNS 프록시 개체가 디바이스 > 가상 시스템 > **vsys** > 일반 > **DNS** 프록시에서 사용되는 경우 필요합니다.
7. 확인을 클릭합니다.
8. 확인 및 커밋을 클릭합니다.

   ***DNS** 프록시 규칙을 사용하여 분할 **DNS**와 같은 선택적 고급 기능을 구성할 수 있습니다. 별도의 **DNS** 서버 프로파일을 사용하여 필요한 경우 **DNS** 프록시 규칙의 도메인 이름과 일치하는 **DNS** 해상도를 다른 **DNS** 서버 집합으로 리디렉션할 수 있습니다. 사례 **3**을 사용하면 분할 **DNS**가 있습니다.*

   동일한 DNS 프록시 개체에 두 개의 별도의 DNS 서버 프로파일을 사용하는 경우, 하나는 DNS 프록시에 대해, DNS 프록시 규칙에 대해 하나씩 사용하는 경우 다음과 같은 동작이 발생합니다.

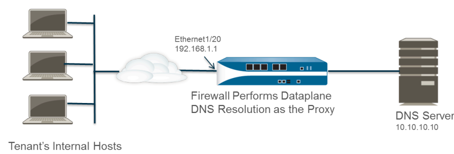
   - DNS 프록시에서 사용하는 DNS 서버 프로파일에 서비스 경로가 정의된 경우가 우선순위를 가지며 사용됩니다.
   - DNS 프록시 규칙에 사용되는 DNS 서버 프로파일에 서비스 경로가 정의된 경우 사용되지 않습니다. 서비스 경로가 DNS 프록시에서 사용하는 DNS 서버 프로파일에 정의된 경로와 다른 경우 커밋 프로세스 중에 다음 경고 메시지가 표시됩니다.

   ```
   경고: DNS 프록시 개체에 정의된 DNS 서비스 경로가 DNS 프록시 규칙의 서비스 경로와 다릅니다. DNS 프록시 개체의 서비스 경로를 사용합니다.
   ```

   - DNS 서버 프로파일에 서비스 경로가 정의되지 않으면 필요한 경우 전역 서비스 경로가 사용됩니다.

사용 사례 3: 방화벽은 클라이언트와 서버 사이에서 DNS 프록시 역할을 합니다.

이 사용 사례에서 방화벽은 DNS 클라이언트와 DNS 서버 사이에 있습니다. 방화벽의 DNS 프록시는 방화벽 인터페이스에 연결된 테넌트의 네트워크에 상주하는 호스트의 DNS 서버 역할을 하도록 구성됩니다. 이러한 시나리오에서 방화벽은 데이터플레인에서 DNS 확인을 수행합니다.



이 시나리오는 DNS 프록시 규칙이 도메인 이름 일치를 기반으로 DNS 요청을 DNS 서버 집합으로 리디렉션하도록 설정한 구성인 분할 *DNS*를 사용하는 경우에 발생합니다. 일치하는 항목이 없으면 서버 프로파일이 요청을 보낼 DNS 서버를 결정하므로 두 가지 분할 DNS 확인 방법이 사용됩니다.

> 데이터플레인 *DNS* 확인의 경우 *PAN-OS*의 *DNS* 프록시에서 외부 *DNS* 서버로의 소스 *IP* 주소는 프록시 주소*(*원래 요청의 대상 *IP)*가 됩니다*. DNS* 서버 프로파일에 정의된 서비스 경로는 사용되지 않습니다*.* 예를 들어*,* 요청이 호스트 *172.16.1.1*에서 *192.168.1.1*의 *DNS* 프록시에 대한 것이라면 *DNS* 서버에 대한 요청*(10.10.10.10)*은 *192.168.1.1*의 소스와 *10.10.10.10*의 대상을 사용합니다*.*

STEP 1 | 네트워크 > **DNS** 프록시를 선택하고 추가를 클릭합니다.

STEP 2 | 활성화를 클릭하고 DNS 프록시의 이름을 입력합니다.

STEP 3 | 위치에 대해 테넌트의 가상 시스템(이 예에서는 Corp1 Corporation(vsys6))을 선택합니다.

STEP 4 | 인터페이스에 대해 테넌트의 호스트(이 예에서는 Ethernet1/20)에서 DNS 요청을 수신할 인터페이스를 선택합니다.

STEP 5 | 서버 프로파일을 선택하거나 생성하여 이 테넌트에 대한 DNS 요청을 해결하도록 DNS 서버를 사용자 지정합니다.

STEP 6 | **DNS** 프록시 규칙 탭에서 규칙의 이름을 추가합니다.

STEP 7 | (선택 사항) 이 매핑으로 확인된 도메인의 캐싱 켜기를 선택합니다.

STEP 8 | 행당 하나의 항목으로 하나 이상의 도메인 이름을 추가합니다. DNS 프록시 규칙 및 FQDN 일치에서는 방화벽이 FQDN을 DNS 프록시 규칙의 도메인 이름과 일치시키는 방법을 설명합니다.

STEP 9 | **DNS** 서버 프로파일의 경우 프로파일을 선택합니다. 방화벽은 DNS 요청의 도메인 이름을 **DNS** 프록시 규칙에 정의된 도메인 이름과 비교합니다. 일치하는 항목이 있으면 규칙에 정의된 **DNS** 서버 프로파일을 사용하여 DNS 서버를 결정합니다.

STEP 10 | 이 예에서 요청의 도메인이 myweb.corp1.com과 일치하면 myweb DNS 서버 프로파일에 정의된 DNS 서버가 사용됩니다. 일치하는 항목이 없으면 서버 프로파일(Corp1 DNS Server Profile)에 정의된 DNS 서버가 사용됩니다.

STEP 11 | 확인을 두 번 클릭합니다.

DNS 프록시 규칙 및 FQDN 일치

DNS 프록시 규칙을 사용하는 DNS 프록시 개체로 방화벽을 구성하면 방화벽은 DNS 쿼리의 FQDN을 DNS 프록시 규칙의 도메인 이름과 비교합니다. 방화벽 비교는 다음과 같이 작동합니다.

DNS 프록시 규칙과 **FQDN** 비교	예**:**
방화벽은 먼저 DNS 프록시 규칙의 FQDN 및 도메인 이름을 토큰화합니다. 도메인 이름에서 마침표(.)로 구분된 문자열은 토큰입니다.	`*.boat.fish.com`은 4개의 토큰으로 구성: `[*][boat][fish][com]`
일치 프로세스는 FQDN과 규칙의 도메인 이름 간의 정확한 토큰 일치입니다. 부분 문자열이 일치하지 않습니다.	규칙: `fishing` FQDN: `fish` — 일치하지 않음
정확한 일치 요구 사항에 대한 예외는 와일드카드(별표(*))를 사용하는 것입니다. *는 하나 이상의 토큰과 일치합니다. 이는 와일드카드(*)로만 구성된 규칙이 하나 이상의 토큰이 있는 FQDN과 일치함을 의미합니다.	규칙: `*.boat.com` FQDN: `www.boat.com` — 일치 FQDN: `www.blue.boat.com` — 일치 FQDN: `boat.com` — 일치하지 않음
	규칙: `*` FQDN: `boat` — 일치 FQDN: `boat.com` — 일치 FQDN: `www.boat.com` — 일치
선행 토큰, 토큰 사이 또는 후행 토큰(단, 단일 토큰 내 다른 문자 사용 불가)과 같은 모든 위치에서 *를 사용할 수 있습니다.	규칙: `www.*.com` FQDN: `www.boat.com` — 일치 FQDN: `www.blue.boat.com` — 일치
	규칙: `www.boat.*` FQDN: `www.boat.com` — 일치 FQDN: `www.boat.fish.com` — 일치
	규칙: `www.boat*.com` — 무효
여러 와일드카드(*)는 도메인 이름의 모든 위치(앞의 토큰, 토큰 사이 또는 후행 토큰)에 나타날 수 있습니다. 연속되지 않은 각 *는 하나 이상의 토큰과 일치합니다.	규칙: `a.*.d.*.com` FQDN: `a.b.d.e.com` — 일치 FQDN: `a.b.c.d.e.f.com` — 일치

DNS 프록시 규칙과 FQDN 비교	예:
	FQDN: **a.d.d.e.f.com** — 일치(첫 번째 ***는 d**와 일치, 두 번째 ***는 e** 및 **f**와 일치) FQDN: **a.d.e.f.com** — 일치하지 않음(첫 번째 ***는 d**와 일치하고 규칙의 후속 **d**는 일치하지 않음)
와일드카드가 연속 토큰에 사용되는 경우 첫 번째 *는 하나 이상의 토큰과 일치합니다. 두 번째 *는 하나의 토큰과 일치합니다. 이는 *.*로만 구성된 규칙이 두 개 이상의 토큰이 있는 모든 FQDN과 일치함을 의미합니다.	토큰 앞에 오는 연속 와일드카드: 규칙: ***.*.boat.com** FQDN: **www.blue.boat.com** — 일치 FQDN: **www.blue.sail.boat.com** — 일치
	토큰 사이의 연속 와일드카드: 규칙: **www.*.*.boat.com** FQDN: **www.blue.sail.boat.com** — 일치 FQDN: **www.big.blue.sail.boat.com** — 일치
	연속적인 와일드카드 후행 토큰: 규칙: **www.boat.*.*** FQDN: **www.boat.fish.com** — 일치 FQDN: **www.boat.fish.ocean.com** — 일치
	연속 와일드카드만 해당: 규칙: *.* FQDN: **boat** — 일치하지 않음 FQDN: **boat.com** — 일치 FQDN: **www.boat.com** — 일치
연속 및 비연속 와일드카드는 동일한 규칙에 나타날 수 있습니다.	규칙: **a.*.d.*.*.com** FQDN: **a.b.c.d.e.f.com** — 일치(첫 번째 ***는 b** 및 **c**와 일치, 두 번째 ***는 e**와 일치, 세 번째 ***는 f**와 일치) FQDN: **a.b.c.d.e.com** — 일치하지 않음(첫 번째 ***는 b** 및 **c**와 일치하고 두 번째 ***는 e**와 일치하고 세 번째 ***는** 일치하지 않음)
암시적 꼬리 일치 동작은 추가 약칭을 제공합니다.	규칙: **www.boat.fish** FQDN: **www.boat.fish.com** — 일치

DNS 프록시 규칙과 FQDN 비교	예:
규칙의 마지막 토큰이 *가 아니면 FQDN에 규칙에 없는 추가 후행 토큰이 있더라도 규칙의 모든 토큰이 FQDN과 일치하면 비교가 일치합니다.	FQDN: **`www.boat.fish.ocean.com`** — 일치 FQDN: **`www.boat.fish`** — 일치
이 규칙은 *로 끝나므로 암시적 꼬리 일치 규칙이 적용되지 않습니다. *는 명시된 대로 작동합니다. 하나 이상의 토큰과 일치합니다.	규칙: **`www.boat.fish.*`** FQDN: **`www.boat.fish.com`** — 일치 FQDN: **`www.boat.fish.ocean.com`** — 일치 FQDN: **`www.boat.fish`** — 일치하지 않음(이 FQDN에는 규칙의 *와 일치하는 토큰이 없습니다.)
FQDN이 둘 이상의 규칙과 일치하는 경우 순위 결정 알고리즘은 가장 구체적인(가장 긴) 규칙을 선택합니다. 즉, 알고리즘은 더 많은 토큰과 더 적은 와일드카드(*)를 사용하는 규칙을 선호합니다.	규칙 1: **`*.fish.com`** — 일치 규칙 2: **`*.com`** — 일치 규칙 3: **`boat.fish.com`** — 매치 및 타이 브레이커 FQDN: **`boat.fish.com`** FQDN은 세 가지 규칙 모두와 일치합니다. 방화벽은 규칙 3이 가장 구체적이기 때문에 규칙 3을 사용합니다.
	규칙 1: **`*.fish.com`** — 일치하지 않음 규칙 2: **`*.com`** — 일치 규칙 3: **`boat.fish.com`** — 일치하지 않음 FQDN: **`fish.com`** *에 일치시킬 토큰이 없기 때문에 FQDN이 규칙 1과 일치하지 않습니다.
	규칙 1: **`*.fish.com`** — 매치 및 타이 브레이커 규칙 2: **`*.com`** — 일치 규칙 3: **`boat.fish.com`** — 일치하지 않음 FQDN: **`blue.boat.fish.com`** FQDN은 규칙 1 및 규칙 2와 일치합니다(*가 하나 이상의 토큰과 일치하기 때문). 방화벽은 규칙 1이 가장 구체적이기 때문에 규칙 1을 사용합니다.
와일드카드(*) 및 암시적 꼬리 일치 규칙으로 작업할 때 FQDN이 둘 이상의 규칙과 일치하고 순위 결정 알고리즘이 규칙의 가중치를 동일하게 적용하는 경우가 있을 수 있습니다.	다음을 변경합니다. 규칙: **`www.boat`** 다음으로 변경합니다.

DNS 프록시 규칙과 **FQDN** 비교	예**:**
모호성을 피하기 위해 암시적 꼬리 일치 또는 와일드카드(*)가 있는 규칙이 겹칠 수 있는 경우 꼬리 토큰을 지정하여 암시적 꼬리 일치 규칙을 바꾸십시오.	규칙: **`www.boat.com`**
모호성 및 예기치 않은 결과를 방지하기 위해 DNS 프록시 규칙을 생성하기 위한 모범 사례	
FQDN을 둘 이상의 규칙과 일치시킬 수 있는 암시적 꼬리 일치를 호출하지 않도록 도메인 이름에 최상위 도메인을 포함합니다.	**`boat.com`**
와일드카드(*)를 사용하는 경우 맨 왼쪽 토큰으로만 사용하십시오. 이 방법은 와일드카드 DNS 레코드와 DNS의 계층적 특성에 대한 일반적인 이해를 따릅니다.	**`*.boat.com`**
하나의 규칙에 하나 이상의 *를 사용하지 마십시오.	
*를 사용하여 DNS 서버와 연결된 기본 규칙을 설정하고 더 많은 토큰이 있는 규칙을 사용하여 다른 서버와 연결하는 규칙에 대한 예외를 구축합니다. 순위 결정 알고리즘은 일치하는 토큰의 수를 기반으로 가장 구체적인 일치 항목을 선택합니다.	규칙: **`*.corporation.com`** - DNS 서버 A 규칙: **`www.corporation.com`** - DNS 서버 B 규칙: **`*.internal.corporation.com`** - DNS 서버 C 규칙: **`www.internal.corporation.com`** — DNS 서버 D FQDN: **`mail.internal.corporation.com`** — DNS 서버 C와 일치 FQDN: **`mail.corporation.com`** — DNS 서버 A와 일치

DDNS

DDNS(동적 DNS) 서비스가 DNS 클라이언트에 정확한 IP 주소를 제공하기 위해 IP 주소에 대한 도메인 이름 매핑을 업데이트하는 방법에 대해 알아봅니다.

- 동적 DNS 개요
- 방화벽 인터페이스에 대한 동적 DNS 구성

동적 DNS 개요

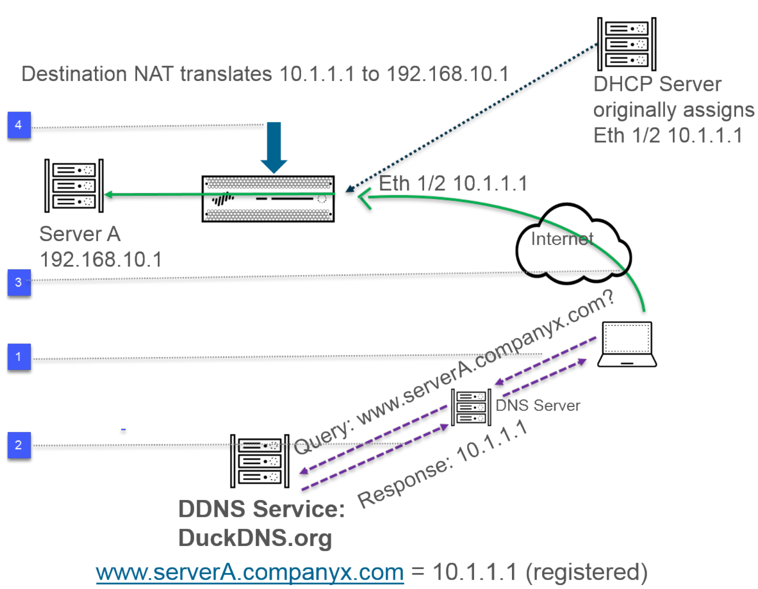
방화벽 뒤에서 호스팅되는 서비스가 있고 방화벽에서 대상 NAT 정책을 사용하여 해당 서비스에 액세스하거나 방화벽에 대한 원격 액세스를 제공해야 하는 경우 IPv4 주소 변경을 등록할 수 있거나(인터페이스가 동적 주소를 수신하는 DHCP 클라이언트인지 여부 동적 DNS(DDNS) 서비스 공급자와의 인터페이스에 대한 정적 주소) IPv6 주소 변경(고정 주소만)이 있습니다. DDNS 서비스는 DNS 클라이언트에 정확한 IP 주소를 제공하기 위해 도메인 이름-IP 주소 매핑을 자동으로 업데이트합니다. 그러면 DNS 클라이언트는 방화벽과 방화벽 뒤의 서비스에 액세스할 수 있습니다. DDNS는 서비스를 호스팅하는 분기 배포에 자주 사용됩니다. 방화벽 인터페이스에 대한 DDNS 지원이 없으면 클라이언트에 정확한 IP 주소를 제공하기 위해 외부 구성 요소가 필요합니다.

방화벽은 다음 DDNS 서비스 공급자를 지원합니다. DuckDNS, DynDNS, FreeDNS Afraid.org 동적 API, FreeDNS Afraid.org 및 No-IP. 개별 DDNS 서비스 공급자는 호스트 이름에 대해 지원하는 IP 주소 수 및 IPv6 주소 지원 여부처럼 제공하는 서비스를 결정합니다. Palo Alto Networks®는 콘텐츠 업데이트를 사용하여 새로운 DDNS 서비스 제공자를 추가하고 서비스에 대한 업데이트를 제공합니다.

고가용성*(HA)* 구성의 경우 방화벽이 현재 *Palo Alto Networks* 콘텐츠 릴리스 버전을 기반으로 *DDNS* 구성을 유지하므로 *HA* 방화벽 피어*(*활성*/*수동 또는 활성*/*활성*)*의 콘텐츠 버전이 동기화되어 있는지 확인하십시오. *Palo Alto Networks*는 콘텐츠 릴리스를 통해 기존 *DDNS* 서비스를 변경하거나 더 이상 사용하지 않을 수 있습니다. 또한 *DDNS* 서비스 제공자는 제공하는 서비스를 변경할 수 있습니다. *HA* 피어 간의 콘텐츠 릴리스 버전이 일치하지 않으면 *DDNS* 서비스를 사용하는 기능에 문제가 발생할 수 있습니다.

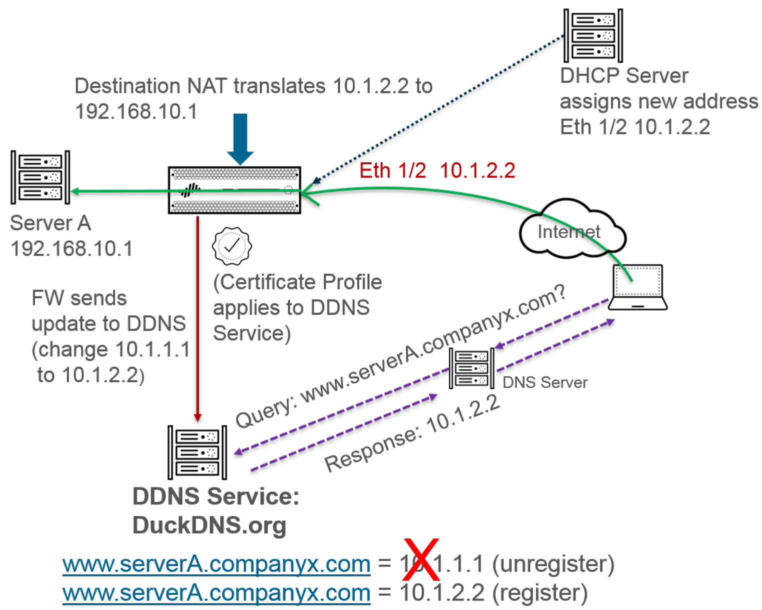
방화벽은 *PPPoE(Point-to-Point Protocol over Ethernet)* 종료 지점인 인터페이스를 통한 *DDNS*를 지원하지 않습니다.

다음 예에서 방화벽은 DDNS 서비스 제공자의 DDNS 클라이언트입니다. 처음에 DHCP 서버는 이더넷 1/2 인터페이스에 IP 주소 10.1.1.1을 할당합니다. 대상 NAT 정책은 공용 10.1.1.1을 방화벽 뒤에 있는 서버 A의 실제 주소(192.168.10.1)로 변환합니다.



1. 사용자가 www.serverA.companyx.com에 접속을 시도하면 사용자는 로컬 DNS 서버에 IP 주소를 쿼리합니다. www.serverA.companyx.com(예시로 duckdns.org 레코드의 CNAME으로 설정: serverA.companyx.duckdns.org)은 DDNS 공급자(이 예에서는 DuckDNS)에 속한 도메인입니다. DNS 서버는 쿼리를 해결하기 위해 DDNS 공급자와 함께 레코드를 확인합니다.
2. DNS 서버는 www.serverA.companyx.com의 IP 주소인 10.1.1.1로 사용자에게 응답합니다.
3. 대상이 10.1.1.1인 사용자 패킷은 방화벽 인터페이스 이더넷 1/2로 이동합니다.
4. 이 예에서 방화벽은 대상 NAT를 수행하고 패킷을 대상으로 보내기 전에 10.1.1.1을 192.168.10.2로 변환합니다.

일정 시간이 지나면 DHCP가 방화벽 인터페이스에 새 IP 주소를 할당하여 다음과 같이 DDNS 업데이트를 트리거합니다.



1. DHCP 서버는 이더넷 1/2에 새 IP 주소(10.1.2.2)를 할당합니다.
2. 방화벽은 새 주소를 수신하면 DDNS 서비스가 등록하는 www.serverA.companyx.com의 새 주소로 DDNS 서비스에 업데이트를 보냅니다. (방화벽은 또한 구성한 업데이트 간격에 따라 정기적인 업데이트를 보냅니다. 방화벽은 HTTPS 포트 443을 통해 DDNS 업데이트를 보냅니다.)

따라서 다음에 클라이언트가 www.serverA.companyx.com의 IP 주소를 DNS 서버에 쿼리하고 DNS 서버가 DDNS 서비스를 확인할 때 DDNS 서비스는 업데이트된 주소(10.1.2.2)를 보냅니다. 따라서 사용자는 업데이트된 인터페이스 주소를 사용하여 방화벽 인터페이스를 통해 서비스 또는 애플리케이션에 성공적으로 액세스합니다.

방화벽이 *HA* 활성/수동 모드로 구성된 경우 두 개의 *HA* 방화벽 상태가 수렴되는 동안 방화벽이 *DDNS* 업데이트를 *DDNS* 서비스로 보냅니다. *HA* 상태가 수렴되면 수동 방화벽에서 *DDNS*가 비활성화됩니다. 예를 들어, 두 개의 *HA* 방화벽이 처음 부팅될 때 둘 다 *HA* 활성 모드인지 수동 모드인지 설정할 때까지 둘 다 *DDNS* 업데이트를 보냅니다. 이 간격 동안 시스템 로그에 *DDNS* 업데이트가 계속 표시됩니다. *HA* 상태가 수렴되고 각 방화벽이 클라이언트에 활성 또는 수동임을 알리면 수동 방화벽이 더 이상 *DDNS* 업데이트를 보내지 않습니다. *(HA* 활성/활성 모드에서 각 방화벽은 독립적인 *DDNS* 구성을 가지며 *DDNS* 구성을 동기화하지 않습니다.*)*

방화벽 인터페이스에 대한 동적 DNS 구성

방화벽 인터페이스에 대한 DDNS를 구성하기 전에:

- DDNS 공급자에 등록한 호스트 이름을 확인합니다.
- DDNS 서비스에서 공용 SSL 인증서를 가져와 방화벽으로 가져옵니다.
- (FreeDNS Afraid.org v1 또는 FreeDNS Afraid.org Dynamic API v1을 사용하는 경우) DDNS 서버의 동적 DNS 서비스 탭에는 다음 옵션이 포함됩니다. 동일한 **IP**의 업데이트를 함께 연결하시겠습니까**?** 이 옵션이 활성화되면 DDNS 서비스는 단일 호스트 이름 및 IP 주소에 대한 DNS 레코드뿐만 아니라 변경되는 이전 IP 주소를 포함하는 DNS 레코드의 모든 호스트 이름을 업데이트합니다. 업데이트하지 않으려는 호스트의 DNS 레코드 업데이트를 방지하려면 동일한 **IP**의 링크 업데이트를 함께 비활성화해야 합니까**?** DDNS 서버가 DDNS 업데이트에 있는 새 IP 주소로 특정 호스트 이름을 포함하는 DNS 레코드만 업데이트하도록 옵션을 선택합니다.

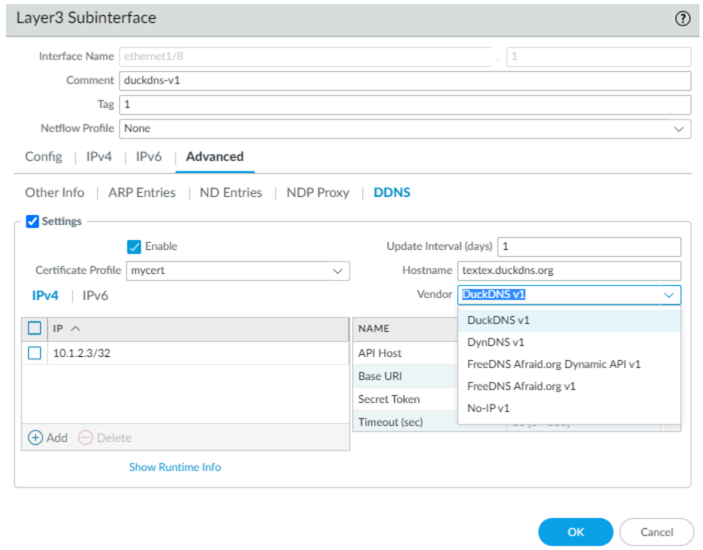
STEP 1 | DDNS를 구성합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 레이어 3 인터페이스, 하위 인터페이스 또는 AE(집계 이더넷) 인터페이스를 선택하거나 네트워크 > 인터페이스 > **VLAN** 및 인터페이스 또는 하위 인터페이스를 선택합니다.
2. 고급 > **DDNS**를 선택하고 설정을 선택합니다.
3. DDNS를 활성화합니다. DDNS를 구성하려면 처음에 DDNS를 활성화해야 합니다. (DDNS 구성이 완료되지 않은 경우 부분 구성이 손실되지 않도록 설정하지 않고 저장할 수 있습니다.)
4. FQDN에 매ping된 IP 주소를 업데이트하기 위해 방화벽이 DDNS 서비스에 전송하는 업데이트 간격**(**일**)**인 업데이트 간격(일)을 입력합니다(기본값은 1, 범위는 1-30). IP 주소가 변경되는 빈도에 따라 간격을 선택합니다. (방화벽이 정기적으로 보내는 업데이트는 주소 변경을 수신할 때 방화벽이 보내는 업데이트에 추가됩니다. 정기적으로 전송되는 업데이트는 예를 들어 주소 변경마다 전송된 업데이트가 손실되지 않도록 하기 위한 것입니다.)
5. DDNS 서비스에 이미 등록된 인터페이스의 호스트 이름을 입력합니다(예: www.Servera.CompanyX.com 또는 ServerA).

   *이 호스트 이름이 **DDNS** 서비스에 등록한 호스트 이름과 일치하는지 확인합니다. 호스트 이름에 대한 **FQDN**을 입력해야 합니다. 방화벽은 구문이 도메인 이름에 대해 **DNS**에서 허용하는 유효한 문자만 사용하는지 확인하는 경우를 제외하고 호스트 이름의 유효성을 검사하지 않습니다.*
6. **IPv4**를 선택하고 인터페이스에 할당된 IPv4 주소를 하나 이상 선택하거나 호스트 이름과 연결할 IPv4 주소 추가(예: 10.1.1.1)를 선택합니다. DDNS 서비스에서 허용하는 만큼의 IPv4 주소만 선택할 수 있습니다. 선택한 모든 IPv4 주소가 DDNS 서비스에 등록됩니다. IPv4 주소 또는 IPv6 주소를 하나 이상 선택합니다.
7. **IPv6**를 선택하고 인터페이스에 할당된 하나 이상의 IPv6 주소를 선택하거나 호스트 이름과 연결할 IPv6 주소를 추가합니다. DDNS 서비스가 허용하는 만큼만 IPv6 주소를 선택할 수 있습니다. 선택된 모든 IPv6 주소는 DDNS 서비스에 등록됩니다. IPv4 주소 또는 IPv6 주소를 하나 이상 선택합니다.
8. DDNS 서비스에서 가져온 SSL 인증서를 사용하여 새 인증서 프로파일(인증서 프로파일)을 선택하거나 만들어 방화벽이 DDNS 서비스에 처음 연결하여 IP 주소를 등록할 때마다 DDNS 서비스의 SSL 인증서를 확인합니다. 방화벽이 DDNS 서비스에 연결하여 업데이트를 보내면 DDNS

서비스는 방화벽이 DDNS 서비스를 인증할 수 있도록 CA(인증 기관)에서 서명한 SSL 인증서를 방화벽에 제공합니다.

9. DDNS 서비스에 사용 중인 공급업체(및 버전 번호)를 선택합니다.



Palo Alto Networks®는 콘텐츠 업데이트를 통해 지원되는 *DDNS* 서비스 제공업체를 변경할 수 있습니다.

공급업체 필드에서 *Palo Alto Network DDNS* 선택은 *SD-WAN* 및 *ZTP*와 같은 *Palo Alto Networks* 기능을 위해 예약된 *DDNS* 서비스이며 이 현재 작업에 대해 선택해서는 안 됩니다. 해당 지원 기능이 활성화되지 않은 상태에서 실수로 *Palo Alto Networks DDNS*를 선택하면 오류 메시지가 나타납니다.

10. 공급업체 선택에 따라 공급업체 필드 아래의 공급업체별 이름 및 값 필드가 결정됩니다. 일부 값 필드는 방화벽이 DDNS 서비스에 연결하는 데 사용하는 매개변수를 알리기 위해 읽기 전용입니다. DDNS 서비스가 사용자에게 제공하는 암호 및 DDNS 서비스에서 업데이트를 수신하지 않는 경우 방화벽이 사용하는 시간 초과와 같은 나머지 값 필드를 구성합니다.

11. 확인을 클릭합니다.

STEP 2 | (선택 사항) 방화벽이 관리 인터페이스가 아닌 인터페이스를 사용하여 DDNS 서비스와 통신하도록 하려면 DDNS에 대한 서비스 경로를 구성합니다(외부 서비스에 대한 네트워크 액세스 설정).

STEP 3 | 변경 사항을 커밋합니다.

STEP 4 | 인터페이스에 대한 DDNS 정보를 봅니다.

1. 네트워크 > 인터페이스 > 이더넷 또는 네트워크 > 인터페이스 > **VLAN**을 선택하고 구성한 인터페이스를 선택합니다. DDNS가 구성된 인터페이스는 기능 필드에 DDNS 아이콘 을 표시합니다.
2. 고급 > **DDNS** 및 설정을 선택합니다.
3. 마지막 반환 코드(마지막 FQDN 업데이트의 결과) 및 DDNS 서비스가 FQDN 업데이트를 받은 마지막 시간(날짜 및 시간) 을 포함하여 인터페이스에 대한 DDNS 정보를 보려면 런타임 정보 표시를 선택합니다.

NAT

이 섹션에서는 NAT(Network Address Translation) 및 NAT용 방화벽을 구성하는 방법에 대해 설명합니다. NAT를 사용하면 라우팅할 수 없는 개인 IPv4 주소를 하나 이상의 전역적으로 라우팅 가능한 IPv4 주소로 변환하여, 조직의 라우팅 가능한 IP 주소를 보존할 수 있습니다. NAT를 사용하면 공용 주소에 액세스해야 하는 호스트의 실제 IP 주소를 공개하지 않고 포트 포워딩을 수행하여 트래픽을 관리할 수 있습니다. NAT를 사용하여 동일한 IP 서브넷을 가진 네트워크가 서로 통신할 수 있도록 하여 네트워크 설계 문제를 해결할 수 있습니다. 방화벽은 레이어 3 및 가상 와이어 인터페이스에서 NAT를 지원합니다.

NAT64 옵션은 IPv6 주소와 IPv4 주소 간에 변환하여 서로 다른 IP 주소 지정 체계를 사용하는 네트워크 간 연결을 제공하므로 IPv6 주소 지정으로의 마이그레이션 경로를 제공합니다. IPv6-to-IPv6 네트워크 접두사 변환(NPTv6)은 하나의 IPv6 접두사를 다른 IPv6 접두사로 변환합니다. PAN-OS는 이 모든 기능을 지원합니다.

내부 네트워크 내에서 사설 IP 주소를 사용하는 경우 NAT를 사용하여 사설 주소를 외부 네트워크에서 라우팅할 수 있는 공용 주소로 변환해야 합니다. PAN-OS에서는 어떤 패킷 주소와 포트가 변환이 필요한지, 변환된 주소와 포트가 무엇인지 방화벽에 지시하는 NAT 정책 규칙을 만듭니다.

- NAT 정책 규칙
- 소스 NAT 및 대상 NAT
- DNS 재작성 사용 사례가 있는 대상 NAT
- NAT 규칙 용량
- 동적 IP 및 포트 NAT 초과 신청
- 데이터플레인 NAT 메모리 통계
- NAT 구성
- NAT 구성 예

NAT 정책 규칙

- NAT 정책 개요
- 주소 개체로 식별된 NAT 주소 풀
- NAT 주소 풀의 프록시 ARP

NAT 정책 개요

최소한 패킷의 소스 영역 및 대상 영역과 일치하도록 NAT 규칙을 구성합니다. 존 외에도 패킷의 데스티네이션 인터페이스, 소스 및 데스티네이션 주소, 서비스를 기반으로 일치 기준을 구성할 수 있습니다. 여러 NAT 규칙을 구성할 수 있습니다. 방화벽은 위에서 아래로 순서대로 규칙을 평가합니다. 패킷이 단일 NAT 규칙의 기준과 일치하면 패킷에 추가 NAT 규칙이 적용되지 않습니다. 따라서 NAT 규칙 목록은 패킷에 대해 만든 가장 구체적인 규칙이 적용되도록 가장 구체적인 것에서 가장 덜 구체적인 순서로 지정해야 합니다.

고정 NAT 규칙은 다른 형태의 NAT보다 우선하지 않습니다. 따라서 고정 NAT가 작동하려면 고정 NAT 규칙이 방화벽 목록에 있는 다른 모든 NAT 규칙보다 우선해야 합니다.

NAT 규칙은 주소 변환을 제공하며, 패킷을 허용하거나 거부하는 보안 정책 규칙과 다릅니다. 정의한 영역을 기반으로 필요한 규칙을 결정할 수 있도록 방화벽이 NAT 규칙 및 보안 정책 규칙을 적용할 때 방화벽의 논리 흐름을 이해하는 것이 중요합니다. NAT 트래픽을 허용하도록 보안 정책 규칙을 구성해야 합니다.

침입 시 방화벽은 패킷을 검사하고 경로 조회를 수행하여 이그레스 인터페이스와 존을 결정합니다. 그런 다음 방화벽은 패킷이 소스 및/또는 대상 영역을 기반으로 정의된 NAT 규칙 중 하나와 일치하는지 확인합니다. 그런 다음 원래(NAT 이전) 소스 및 대상 주소를 기반으로 하지만 NAT 이후 영역을 기반으로 패킷과 일치하는 보안 정책을 평가하고 적용합니다. 마지막으로 송신 시 일치하는 NAT 규칙에 대해 방화벽은 소스 및/또는 대상 주소와 포트 번호를 변환합니다.

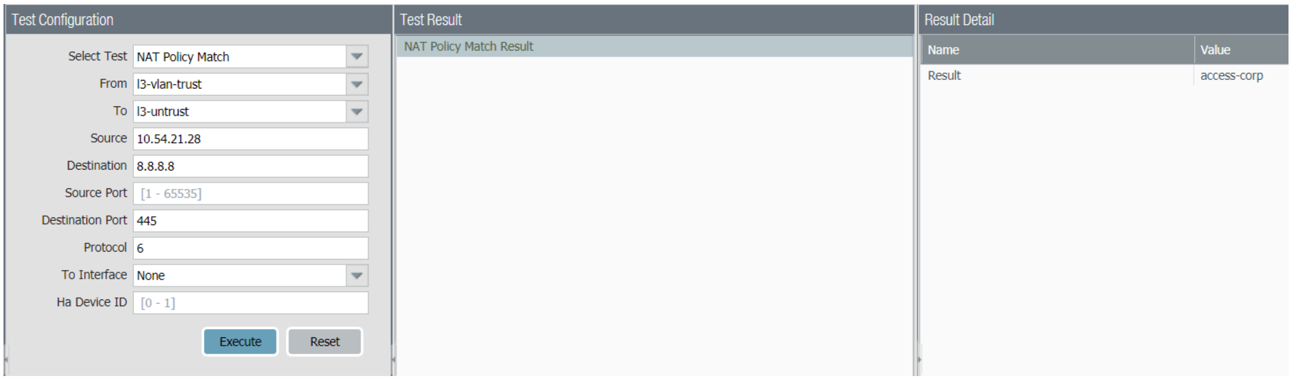
패킷이 방화벽을 떠날 때까지 IP 주소 및 포트 변환이 발생하지 않는다는 점에 유의하십시오. NAT 규칙 및 보안 정책은 원래 IP 주소(NAT 이전 주소)에 적용됩니다. NAT 규칙은 NAT 이전 IP 주소와 연결된 존을 기반으로 구성됩니다.

보안 정책은 패킷이 허용되는지 여부를 결정하기 위해 사후 NAT 영역을 검사하기 때문에 보안 정책은 NAT 규칙과 다릅니다. NAT의 본질은 소스 또는 대상 IP 주소를 수정하는 것이므로 패킷의 나가는 인터페이스와 영역이 수정될 수 있으므로 보안 정책은 NAT 이후 영역에 적용됩니다.

통화 관리자가 전화를 대신하여 ***SIP*** 메시지를 보내 연결을 설정하기 때문에 ***SIP*** 통화에서 방화벽을 통과할 때 단방향 오디오가 발생하는 경우가 있습니다***. Call Manager***의 메시지가 방화벽에 도달하면 ***SIP ALG***는 ***NAT***를 통해 전화기의 ***IP*** 주소를 입력해야 합니다***.*** 통화 관리자와 전화기가 동일한 보안 영역에 있지 않은 경우 전화기 ***IP*** 주소의 ***NAT*** 조회는 통화 관리자 영역을 사용하여 수행됩니다***. NAT*** 정책은 이를 고려해야 합니다***.***

No-NAT 규칙은 NAT 정책에서 나중에 정의된 NAT 규칙 범위 내에서 정의된 IP 주소를 제외할 수 있도록 구성됩니다. 비 NAT 정책을 정의하려면 모든 일치 기준을 지정하고 원본 번역 열에서 원본 번역 없음을 선택합니다.

디바이스 > 문제 해결을 선택하고 NAT 규칙에 대한 트래픽 일치를 테스트하여 처리된 NAT 규칙을 확인할 수 있습니다. 예:



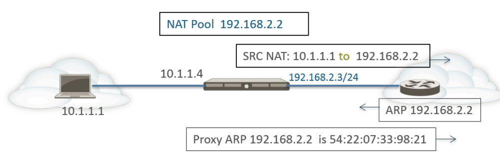
주소 개체로 식별된 NAT 주소 풀

NAT 정책 규칙에서 동적 **IP** 또는 동적 **IP** 및 포트 NAT 주소 풀을 구성할 때 일반적으로 주소 개체를 사용하여 변환된 주소 풀을 구성합니다. 각 주소 개체는 호스트 IP 주소, IP 주소 범위 또는 IP 서브넷이 될 수 있습니다.

NAT 규칙과 보안 정책 규칙 모두 주소 개체를 사용하기 때문에 *NAT*에 사용되는 주소 개체의 이름을 *"NAT-name."*과 같이 접두사로 지정하여 두 규칙을 구별하는 것이 가장 좋습니다.

NAT 주소 풀의 프록시 ARP

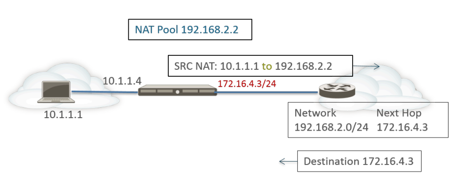
NAT 주소 풀은 인터페이스에 바인딩되지 않습니다. 다음 그림은 NAT 주소 풀에서 주소에 대한 프록시 ARP를 수행할 때 방화벽의 동작을 보여 줍니다.



방화벽은 클라이언트의 소스 NAT를 수행하여 소스 주소 10.1.1.1을 NAT 풀의 주소로 변환합니다(192.168.2.2). 변환된 패킷이 라우터로 전송됩니다.

반환 트래픽의 경우 라우터는 192.168.2.2에 도달하는 방법을 알지 못하므로(IP 주소가 NAT 주소 풀의 주소일 뿐이므로) 방화벽에 ARP 요청 패킷을 보냅니다.

- 주소 풀(192.168.2.2)이 이그레스(egress)/인그레스(ingress) 인터페이스 IP 주소(192.168.2.3/24)와 동일한 서브넷에 있는 경우, 방화벽은 위의 그림과 같이 IP 주소의 레이어 2 MAC 주소를 나타내는 라우터에 프록시 ARP 회신을 보낼 수 있습니다.
- 주소 풀(192.168.2.2)이 방화벽의 인터페이스의 서브넷이 아닌 경우 방화벽은 라우터에 프록시 ARP 회신을 보내지 않습니다. 즉, 라우터는 아래 그림과 같이 반환 트래픽이 방화벽으로 다시 라우팅되도록 하기 위해 192.168.2.2로 향하는 패킷을 보낼 위치를 알기 위해 필요한 경로로 구성되어야 합니다.



소스 NAT 및 대상 NAT

방화벽은 소스 주소 및/또는 포트 변환과 대상 주소 및/또는 포트 변환을 모두 지원합니다.

- 소스 NAT
- 대상 NAT

소스 NAT

소스 NAT는 일반적으로 내부 사용자가 인터넷에 액세스하는 데 사용합니다. 소스 주소가 변환되어 비공개로 유지됩니다. 소스 NAT에는 세 가지 유형이 있습니다.

- **DIPP(**동적 **IP** 및 포트**)** - 여러 호스트가 소스 IP 주소를 포트 번호가 다른 동일한 공용 IP 주소로 변환할 수 있도록 합니다. 동적 변환은 IP 주소, 주소 범위, 서브넷 또는 이들의 조합이 되도록 변환된 주소 풀로 구성하는 NAT 주소 풀에서 사용 가능한 다음 주소로 이루어집니다.

  NAT 주소 풀에서 다음 주소를 사용하는 대신 DIPP를 사용하면 인터페이스 자체의 주소를 지정할 수 있습니다. NAT 규칙에서 인터페이스를 지정하는 이점은 NAT 규칙이 이후에 인터페이스에서 획득한 모든 주소를 사용하도록 자동으로 업데이트된다는 것입니다. DIPP는 인터페이스 기반 NAT 또는 NAPT(네트워크 주소 포트 변환)라고도 합니다.

  DIPP에는 동일한 변환된 IP 주소와 포트 쌍이 동시에 사용될 수 있는 횟수인 기본 NAT 초과 구독 비율이 있습니다. 자세한 내용은 동적 IP 및 포트 NAT 오버서브스크립션 및 DIPP NAT에 대한 초과 가입률 수정을(를) 참조하십시오.

  (2세대 PA-7050-SMC-B 또는 PA-7080-SMC-B 스위치 관리 카드를 사용하지 않는 PA-7000 시리즈 방화벽에만 영향을 줌) DIPP NAT와 함께 지점 간 터널 프로토콜(PPTP)을 사용하는 경우, 방화벽은 하나의 연결에 대해서만 변환된 IP 주소 및 포트 쌍을 사용하도록 제한되고, 방화벽은 DIPP NAT를 지원하지 않습니다. 해결 방법은 PA-7000 시리즈 방화벽을 2세대 SMC-B 카드로 업그레이드하는 것입니다.

- 동적 **IP** - 소스 IP 주소만(포트 번호 없음) NAT 주소 풀에서 사용 가능한 다음 주소로 일대일 동적 변환을 허용합니다. NAT 풀의 크기는 주소 변환이 필요한 내부 호스트의 수와 같아야 합니다. 기본적으로 소스 주소 풀이 NAT 주소 풀보다 크고 결국 모든 NAT 주소가 할당되면 주소 변환이 필요한 새 연결이 삭제됩니다. 이 기본 동작을 무시하려면 고급**(**동적 **IP/**포트 폴백**)**를 사용하여 필요할 때 DIPP 주소를 사용할 수 있습니다. 두 경우 모두 세션이 종료되고 풀의 주소를 사용할 수 있게 되면 새 연결을 변환하기 위해 할당될 수 있습니다.

  동적 IP NAT는 동적 IP NAT 주소 예약 옵션을 지원합니다.

- 정적 **IP** - 소스 IP 주소의 1:1 정적 변환을 허용하지만 소스 포트는 변경되지 않은 상태로 둡니다. 정적 IP 변환의 일반적인 시나리오는 인터넷에서 사용할 수 있어야 하는 내부 서버입니다.

대상 NAT

대상 NAT는 방화벽이 대상 주소를 다른 대상 주소로 변환할 때 들어오는 패킷에 대해 수행됩니다. 예를 들어 공용 대상 주소를 개인 대상 주소로 변환합니다. 대상 NAT는 포트 전달 또는 포트 변환을 수행하는 옵션도 제공합니다.

대상 NAT는 정적 및 동적 변환을 허용합니다.

- 고정 **IP** - 여러 형식으로 일대일 고정 변환을 구성할 수 있습니다. 변환된 패킷이 동일한 형식이고 동일한 수의 IP 주소를 지정하는 한 원본 패킷이 단일 대상 IP 주소, IP 주소 범위 또는 IP 넷마스크를 갖도록 지정할 수 있습니다. 방화벽은 매번 원래 대상 주소를 동일한 변환 대상 주소로 정적으로 변환합니다. 즉, 목적지 주소가 둘 이상인 경우 방화벽은 원래 패킷에 대해 구성된 첫 번째 목적지 주소를 변환된 패킷에 대해 구성된 첫 번째 목적지 주소로 변환하고, 두 번째 원래 목적지 주소를 구성된 두 번째 변환된 목적지 주소로 변환하는 등 항상 동일한 변환을 사용합니다.

  대상 NAT를 사용하여 고정 IPv4 주소를 변환하는 경우 방화벽의 한쪽에서 DNS 서비스를 사용하여 다른 쪽에서 클라이언트의 FQDN을 확인할 수도 있습니다. IPv4 주소를 포함하는 DNS 응답이 방화벽을 통과할 때 DNS 서버는 내부 IP 주소를 외부 디바이스에 제공하거나 그 반대의 경우도 마찬가지입니다. PAN-OS 9.0.2 및 이후 9.0 릴리스부터 클라이언트가 대상 서비스에 도달하기 위해 적절한 주소를 수신하도록 DNS 응답(규칙과 일치)의 IP 주소를 다시 쓰도록 방화벽을 구성할 수 있습니다. 해당 DNS 재작성 사용 사례는 이러한 재작성을 구성하는 방법을 결정합니다.

- 동적 **IP(**세션 배포 포함**)** - 대상 NAT를 사용하면 원래 대상 주소를 동적 IP 주소가 있는 대상 호스트 또는 서버로 변환할 수 있습니다. 이는 DNS에서 여러 주소를 반환할 수 있는 FQDN을 사용하는 주소 개체를 의미합니다. 동적 IP(세션 배포 포함)는 IPv4 주소만 지원합니다. 동적 IP 주소를 사용하는 대상 NAT는 동적 IP 주소 지정을 사용하는 클라우드 배포에서 특히 유용합니다.

  변환된 대상 주소가 둘 이상의 주소로 확인되면 방화벽은 들어오는 NAT 세션을 여러 주소에 분산하여 향상된 세션 분산을 제공합니다. 배포는 라운드 로빈(기본 방법), 소스 IP 해시, IP 모듈로, IP 해시 또는 최소 세션과 같은 여러 방법 중 하나를 기반으로 합니다. DNS 서버가 FQDN에 대해 32개 이상의 IPv4 주소를 반환하는 경우 방화벽은 패킷의 처음 32개 주소를 사용합니다.

  > 변환된 주소가 *IPv6* 주소로만 확인되는 *FQDN* 유형의 주소 개체인 경우 대상 *NAT* 정책 규칙은 *FQDN*을 확인되지 않은 것으로 간주합니다*.*

  동적 **IP(**세션 배포 포함**)**를 사용하면 여러 pre-NAT 대상 IP 주소 ***M***을 여러 post-NAT 대상 IP 주소 ***N***으로 변환할 수 있습니다. 다대다 변환은 단일 NAT 규칙을 사용하여 ***M*** x ***N*** 대상 NAT 변환이 있을 수 있음을 의미합니다.

> 대상 *NAT*의 경우 모범 사례는 다음과 같습니다*.*
>
> - 방화벽이 원래 대상 *IP* 주소의 수가 변환된 대상 *IP* 주소의 수와 동일한지 확인하고 확인할 수 있도록 하는 정적 *IP* 주소에 대해 정적 ***IP*** 주소 변환을 사용합니다*.*
> - *FQDN* 기반 동적 주소에 대해서만 동적 ***IP(***세션 배포 포함***)*** 주소 변환을 사용합니다*(*방화벽은 *IP* 주소 번호 확인을 수행하지 않음*).*

다음은 방화벽이 허용하는 대상 NAT 변환의 일반적인 예입니다.

변환 유형	원래 패킷의 대상 주소	변환된 패킷의 대상 주소에 매핑	참고
고정 **IP**	192.168.1.1	2.2.2.2	원본 패킷과 변환된 패킷은 각각 하나의 가능한 대상 주소를 갖습니다.

변환 유형	원래 패킷의 대상 주소	변환된 패킷의 대상 주소에 매핑	참고
	192.168.1.1-192.168.1.4	2.2.2.1-2.2.2.4	원본 패킷과 변환된 패킷에는 각각 다음과 같은 4개의 가능한 대상 주소가 있습니다. 192.168.1.1은 항상 2.2.2.1에 매핑됩니다. 192.168.1.2는 항상 2.2.2.2에 매핑됩니다. 192.168.1.3은 항상 2.2.2.3에 매핑됩니다. 192.168.1.4는 항상 2.2.2.4에 매핑됩니다.
	192.168.1.1/30	2.2.2.1/30	원본 패킷과 변환된 패킷에는 각각 다음과 같은 4개의 가능한 대상 주소가 있습니다. 192.168.1.1은 항상 2.2.2.1에 매핑됩니다. 192.168.1.2는 항상 2.2.2.2에 매핑됩니다. 192.168.1.3은 항상 2.2.2.3에 매핑됩니다. 192.168.1.4는 항상 2.2.2.4에 매핑됩니다.
동적 **IP(**세션 배포 포함**)**	192.168.1.1/30	domainname.com	원래 패킷에는 4개의 대상 주소가 있으며, 예를 들어 변환된 대상 주소의 FQDN이 5개의 IP 주소로 확인되면 단일 NAT 규칙에 20개의 가능한 대상 NAT 변환이 있습니다.

대상 NAT의 일반적인 용도 중 하나는 단일 공용 대상 주소를 서버 또는 서비스에 할당된 여러 개인 대상 호스트 주소에 매핑하는 여러 NAT 규칙을 구성하는 것입니다. 이 경우 대상 호스트를 식별하기 위해 대상 포트 번호가 사용됩니다. 예:

- 포트 포워딩 - 공용 대상 주소와 포트 번호를 개인 대상 주소로 변환할 수 있지만 포트 번호는 동일하게 유지합니다.

- 포트 변환 - 공개 대상 주소와 포트 번호를 개인 대상 주소와 다른 포트 번호로 변환하여 실제 포트 번호를 비공개로 유지할 수 있습니다. NAT 정책 규칙의 변환된 패킷 탭에 변환된 포트를 입력하여 포트 변환을 구성합니다. 포트 변환이 있는 대상 NAT의 예를 참조하십시오.

DNS 재작성 사용 사례가 있는 대상 NAT

대상 NAT를 사용하여 한 IPv4 주소에서 다른 IPv4 주소로 정적 변환을 수행하는 경우, 방화벽의 한쪽에서 DNS 서비스를 사용하여 클라이언트에 대한 FQDN을 확인할 수도 있습니다. IP 주소가 포함된 DNS 응답이 방화벽을 통과하여 클라이언트로 이동할 때, 방화벽은 해당 IP 주소에 대해 NAT를 수행하지 않으므로, DNS 서버가 외부 디바이스에 내부 IP 주소를 제공하거나 또는 그 반대의 경우도 마찬가지입니다. DNS 클라이언트가 대상 서비스에 연결할 수 없습니다.

이 문제를 방지하려면, NAT 정책 규칙에 대해 구성된 변환된 IP 주소를 기반으로 DNS 응답(A 레코드로부터)내의 IP 주소를 다시 쓰도록 방화벽을 구성할 수 있습니다. 방화벽은 클라이언트에 응답을 전달하기 전에 DNS 응답의 IPv4 주소(FQDN 확인)에 대해 NAT를 수행합니다. 따라서, 클라이언트는 대상 서비스에 도달하기 위해 적절한 주소를 받습니다. 단일 NAT 정책 규칙은 방화벽이 규칙과 일치하는 패킷에 대해 NAT를 수행하도록 하고, 또한 방화벽이 규칙의 원래 대상 주소 또는 변환된 대상 주소와 일치하는 DNS 응답의 IP 주소에 대해 NAT를 수행하도록 합니다.

DNS 재작성은 전역 수준에서 발생합니다. 방화벽은 원본 패킷 탭의 대상 주소를 변환된 패킷 탭의 대상 주소로 매핑합니다. 원래 패킷 탭의 다른 모든 필드는 무시됩니다. DNS 응답 패킷이 도착하면 방화벽은 다음과 같이 방향에 따라 매핑된 대상 주소 중 하나와 일치하는 A 레코드가 응답에 포함되어 있는지 확인합니다.

방화벽이 NAT 규칙과 관련하여 DNS 응답의 IP 주소에서 NAT를 수행하는 다음의 방법을 지정해야 합니다. 역방향 또는 순방향:

- 역방향 - DNS 응답이 규칙의 변환된 대상 주소와 일치하는 경우, 규칙에서 사용하는 역변환을 사용하여 DNS 응답을 변환합니다. 예를 들어, 규칙이 IP 주소 **1.1.1.10**을 **192.168.1.10**으로 변환하는 경우, 방화벽은 **192.168.1.10**의 **DNS** 응답을 **1.1.1.10**으로 다시 씁니다.
- 순방향 - DNS 응답이 규칙의 원래 대상 주소와 일치하는 경우, 규칙에서 사용하는 것과 동일한 변환을 사용하여 DNS 응답을 변환합니다. 예를 들어, 규칙이 IP 주소 **1.1.1.10**을 **192.168.1.10**으로 변환하면, 방화벽은 **1.1.1.10**의 **DNS** 응답을 **192.168.1.10**으로 다시 씁니다.

DNS 재작성이 비활성화된 중첩 *NAT* 규칙이 있고 그 아래에 *DNS* 재작성이 활성화되고 중첩에 포함된 *NAT* 규칙이 있는 경우 방화벽은 중첩 *NAT* 규칙*(*역방향 또는 순방향 설정 중 하나*)*에 따라 *DNS* 응답을 다시 씁니다*.* 다시 쓰기가 우선 적용되며 *NAT* 규칙의 순서는 무시됩니다*.*

DNS 재작성 구성에 대한 사용 사례를 고려하십시오.

- DNS 재작성 역방향 사용 사례가 있는 대상 NAT
- DNS Rewrite Forward 사용 사례가 있는 대상 NAT

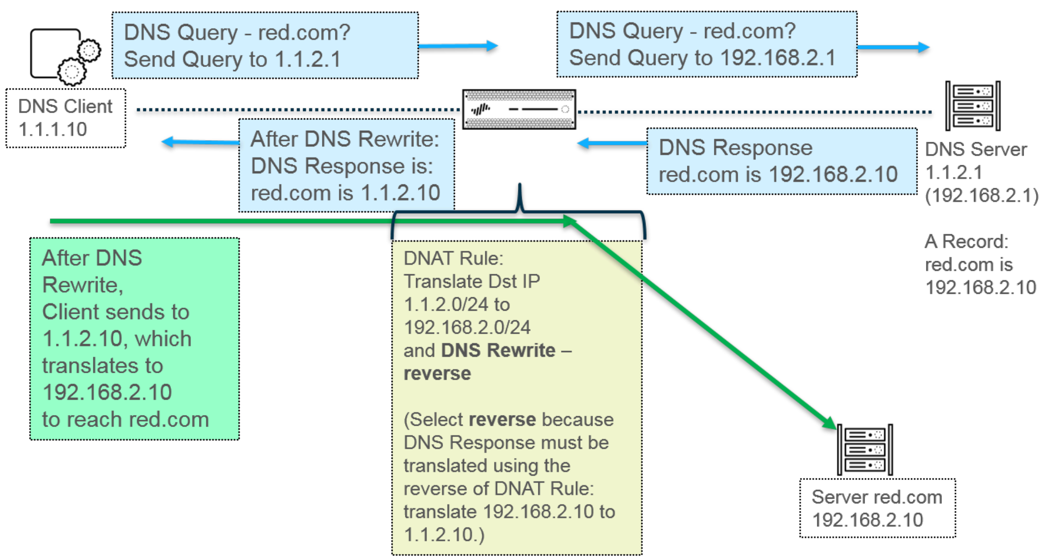
DNS 재작성 역방향 사용 사례가 있는 대상 **NAT**

다음 사용 사례는 역방향으로 활성화된 DNS 재작성과 대상 NAT를 보여줍니다. 이 두 사용 사례의 차이점은 단순히 DNS 클라이언트, DNS 서버 및 대상 서버가 방화벽의 공개 또는 내부 쪽에 있는지 여부입니다. 두 경우 모두 DNS 클라이언트는 최종 대상 서버의 방화벽 반대편에 있습니다. (DNS 클라이언트와

최종 대상 서버가 방화벽의 같은 쪽에 있는 경우 DNS Rewrite Forward 사용 사례가 있는 대상 NAT 3과 4를 고려하십시오.)

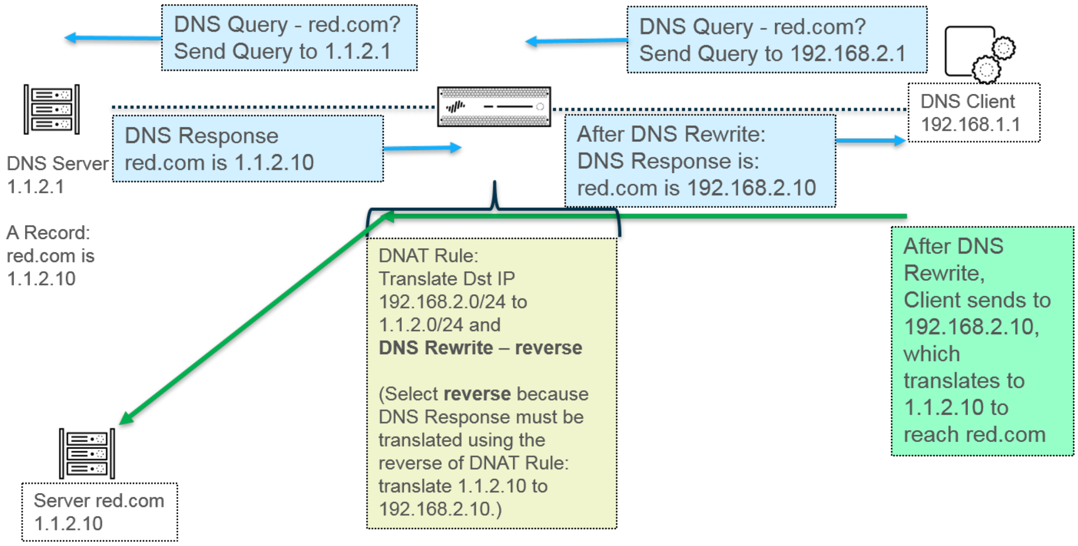
사용 사례 1은 방화벽의 공용 측에 있는 DNS 클라이언트를 보여 주는 반면 DNS 서버와 최종 대상 서버는 모두 내부 측에 있습니다. 이 경우 역방향으로 DNS를 다시 작성해야 합니다. DNS 클라이언트는 red.com의 IP 주소를 쿼리합니다. NAT 규칙에 따라 방화벽은 쿼리(원래 공개 주소 1.1.2.1로 이동)를 내부 주소 192.168.2.1로 변환합니다. DNS 서버는 red.com의 IP 주소가 192.168.2.10이라고 응답합니다. 규칙에는 **Enable DNS Rewrite - reverse** 및 192.168.2.10의 DNS 응답이 규칙에 있는 192.168.2.0/24의 대상 변환 주소와 일치하므로 방화벽이 규칙에서 사용하는 역변환을 사용하여 DNS 응답을 변환합니다. 규칙에 따르면 1.1.2.0/24를 192.168.2.0/24로 변환하므로 방화벽은 192.168.2.10의 DNS 응답을 1.1.2.10으로 다시 씁니다. DNS 클라이언트는 응답을 수신하고 1.1.2.10으로 보냅니다. 이 규칙은 서버 red.com에 도달하기 위해 192.168.2.10으로 변환됩니다.

사용 사례 1 요약: DNS 클라이언트와 대상 서버는 방화벽의 반대편에 있습니다. DNS 서버는 NAT 규칙의 변환된 대상 주소와 일치하는 주소를 제공하므로 NAT 규칙의 역변환을 사용하여 DNS 응답을 변환합니다.



사용 사례 2는 방화벽의 내부 측에 있는 DNS 클라이언트를 보여 주는 반면 DNS 서버와 최종 대상 서버는 모두 공개 측에 있습니다. 이 경우 역방향으로 DNS를 다시 작성해야 합니다. DNS 클라이언트는 red.com의 IP 주소를 쿼리합니다. NAT 규칙에 따라 방화벽은 쿼리(원래 내부 주소 192.168.2.1로 이동)를 공용 주소 1.1.2.1로 변환합니다. DNS 서버는 red.com의 IP 주소가 1.1.2.10이라고 응답합니다. 규칙에는 **Enable DNS Rewrite - reverse** 및 1.1.2.10의 DNS 응답이 규칙에 있는 1.1.2.0/24의 대상 변환 주소와 일치하므로 방화벽이 규칙에서 사용하는 역변환을 사용하여 DNS 응답을 변환합니다. 규칙에 따르면 192.168.2.0/24를 1.1.2.0/24로 변환하므로 방화벽은 DNS 응답 1.1.2.10을 192.168.2.10으로 다시 씁니다. DNS 클라이언트는 응답을 수신하고 192.168.2.10으로 보냅니다. 이 규칙은 서버 red.com에 도달하기 위해 1.1.2.10으로 변환됩니다.

사용 사례 2 요약은 사용 사례 1 요약과 동일합니다. DNS 클라이언트와 대상 서버는 방화벽의 반대편에 있습니다. DNS 서버는 NAT 규칙의 변환된 대상 주소와 일치하는 주소를 제공하므로 NAT 규칙의 역변환을 사용하여 DNS 응답을 변환합니다.



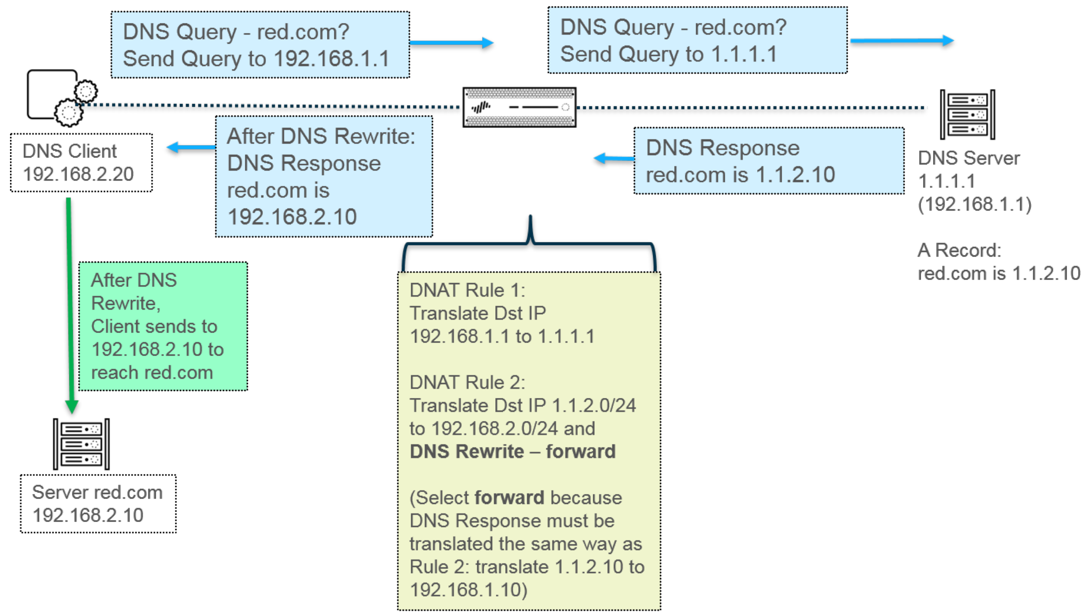
DNS 재작성을 구현하려면 DNS 재작성으로 대상 NAT 구성을(를) 수행합니다.

DNS Rewrite Forward 사용 사례가 있는 대상 NAT

다음 사용 사례는 순방향으로 활성화된 DNA 재작성의 대상 NAT를 보여줍니다. 이 두 사용 사례의 차이점은 단순히 DNS 클라이언트, DNS 서버 및 대상 서버가 방화벽의 공개 또는 내부 쪽에 있는지 여부입니다. 두 경우 모두 DNS 클라이언트는 최종 대상 서버와 동일한 방화벽 쪽에 있습니다. (DNS 클라이언트와 최종 대상 서버가 방화벽의 반대편에 있는 경우 DNS 재작성 역방향 사용 사례가 있는 대상 NAT 1과 2를 고려하십시오.)

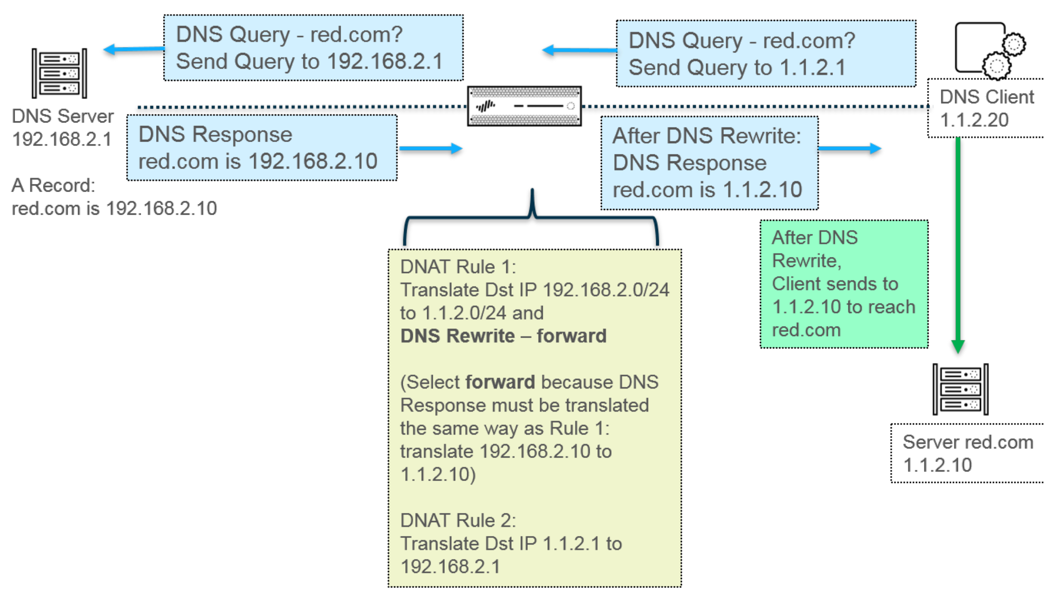
사용 사례 3은 DNS 클라이언트와 최종 대상 서버가 모두 방화벽의 내부 측에 있고 DNS 서버가 공개 측에 있는 경우를 보여줍니다. 이 경우 순방향으로 DNS를 재작성해야 합니다. DNS 클라이언트는 red.com의 IP 주소를 쿼리합니다. 규칙 1에 따라 방화벽은 쿼리(원래 내부 주소 192.168.1.1로 이동)를 1.1.1.1로 변환합니다. DNS 서버는 red.com의 IP 주소가 1.1.2.10이라고 응답합니다. 규칙 2에는 **DNS** 재작성 활성화 **-** 포워드가 포함되며 1.1.2.10의 DNS 응답은 규칙 2의 원래 대상 주소 1.1.2.0/24와 일치하므로, 방화벽은 규칙에서 사용하는 것과 동일한 변환을 사용하여 DNS 응답을 변환합니다. 규칙 2는 1.1.2.0/24를 192.168.2.0/24로 변환하도록 지시하므로 방화벽은 DNS 응답 1.1.2.10을 192.168.2.10으로 다시 씁니다. DNS 클라이언트는 응답을 수신하고 서버 red.com에 도달하기 위해 192.168.2.10으로 보냅니다.

사용 사례 3 요약: DNS 클라이언트와 대상 서버는 방화벽의 같은 쪽에 있습니다. DNS 서버는 NAT 규칙의 원래 대상 주소와 일치하는 주소를 제공하므로 NAT 규칙과 동일한(정방향) 변환을 사용하여 DNS 응답을 변환합니다.



사용 사례 4는 DNS 클라이언트와 최종 대상 서버가 모두 방화벽의 공개 측에 있고 DNS 서버가 내부 측에 있는 경우를 보여줍니다. 이 경우 순방향으로 DNS를 재작성해야 합니다. DNS 클라이언트는 red.com의 IP 주소를 쿼리합니다. 규칙 2에 따라 방화벽은 쿼리(원래 공개 대상 1.1.2.1로 이동)를 192.168.2.1로 변환합니다. DNS 서버는 red.com의 IP 주소가 192.168.2.10이라고 응답합니다. 규칙 1에는 **DNS** 재작성 활성화 **-** 포워드가 포함되어 있으며 192.168.2.10의 DNS 응답은 규칙 1의 원래 대상 주소 192.168.2.0/24와 일치하므로, 방화벽은 규칙에서 사용하는 것과 동일한 변환을 사용하여 DNS 응답을 변환합니다. 규칙 1에 따르면 192.168.2.0/24를 1.1.2.0/24로 변환하여 방화벽이 DNS 응답 192.168.2.10을 1.1.2.10으로 다시 씁니다. DNS 클라이언트는 응답을 수신하고 서버 red.com에 도달하기 위해 1.1.2.10으로 보냅니다.

사용 사례 4 요약은 사용 사례 3 요약과 동일합니다. DNS 클라이언트와 대상 서버는 방화벽의 같은 쪽에 있습니다. DNS 서버는 NAT 규칙의 원래 대상 주소와 일치하는 주소를 제공하므로 NAT 규칙과 동일한(정방향) 변환을 사용하여 DNS 응답을 변환합니다.



DNS 재작성을 구현하려면 DNS 재작성으로 대상 NAT 구성을(를) 수행합니다.

NAT 규칙 용량

허용되는 NAT 규칙의 수는 방화벽 모델을 기반으로 합니다. 개별 규칙 제한은 고정, 동적 IP(DIP) 및 동적 IP 및 포트(DIPP) NAT에 대해 설정됩니다. 이러한 NAT 유형에 사용되는 규칙 수의 합계는 총 NAT 규칙 용량을 초과할 수 없습니다. DIPP의 경우 규칙 제한은 방화벽의 초과 구독 설정(8, 4, 2 또는 1)과 규칙당 하나의 변환된 IP 주소를 가정합니다. 모델별 NAT 규칙 제한 및 변환된 IP 주소 제한을 보려면 방화벽 비교 도구를 사용하십시오.

NAT 규칙으로 작업할 때 고려할 사항:

- 풀 리소스가 부족하면 모델의 최대 규칙 수에 도달하지 않았더라도 NAT 규칙을 추가로 생성할 수 없습니다.
- NAT 규칙을 통합하면 로깅 및 보고도 통합됩니다. 통계는 규칙 내의 모든 주소가 아니라 규칙에 따라 제공됩니다. 세분화된 로깅 및 보고가 필요한 경우 규칙을 결합하지 마십시오.

동적 IP 및 포트 NAT 오버서브스크립션

DIPP(동적 IP 및 포트) NAT를 사용하면 변환된 각 IP 주소와 포트 쌍을 동시 세션에서 여러 번(8, 4 또는 2회) 사용할 수 있습니다. IP 주소 및 포트의 이러한 재사용 가능성(오버서브스크립션이라고 함)은 공용 IP 주소가 너무 적은 고객에게 확장성을 제공합니다. 설계는 호스트가 다른 대상에 연결되어 있다는 가정을 기반으로 하므로 세션을 고유하게 식별할 수 있고 충돌 가능성이 거의 없습니다. 실제로 오버서브스크립션 비율은 주소/포트 풀의 원래 크기를 크기의 8, 4 또는 2배로 늘립니다. 예를 들어 허용되는 기본 제한인 64K 동시 세션에 오버서브스크립션 비율 8을 곱하면 512K 동시 세션이 허용됩니다.

허용되는 오버서브스크립션 요금은 모델에 따라 다릅니다. 오버서브스크립션률은 전 세계적으로 적용됩니다. 방화벽에 적용됩니다. 이 오버서브스크립션 비율은 기본적으로 설정되며 오버서브스크립션을 불필요하게 만드는 데 사용할 수 있는 공용 IP 주소가 충분하더라도 메모리를 소모합니다. 기본 설정에서 더 낮은 설정 또는 1(오버서브스크립션 없음을 의미)로 요금을 줄일 수 있습니다. 감소된 속도를 구성하면 가능한 소스 디바이스 변환 수는 줄어들지만 DIP 및 DIPP NAT 규칙 용량은 증가합니다. 기본 비율을 변경하려면 DIPP NAT에 대한 초과 가입률 수정을(를) 참조하십시오.

플랫폼 기본값을 선택하면 제품 선택 도구에 표시된 대로 명시적 초과 가입 구성이 해제되고 모델에 대한 NAT 기본 DIPP 풀 초과 가입 비율이 적용됩니다. 플랫폼 기본 설정을 사용하면 소프트웨어 릴리스의 업그레이드 또는 다운그레이드를 허용합니다.

방화벽은 NAT 규칙당 최대 256개의 변환된 IP 주소를 지원하고 각 모델은 변환된 IP 주소의 최대 수를 지원합니다(모든 NAT 규칙이 결합된 경우). 오버서브스크립션으로 인해 규칙당 변환된 최대 주소(256개)가 초과되면 방화벽은 커밋을 성공시키기 위해 오버서브스크립션 비율을 자동으로 줄입니다. 그러나 NAT 규칙으로 인해 모델에 대해 변환된 최대 주소를 초과하는 변환이 발생하면 커밋이 실패합니다.

데이터플레인 NAT 메모리 통계

show running global-ippool 명령은 풀에 대한 NAT 메모리 소비와 관련된 통계를 표시합니다. Size 열에는 리소스 풀이 사용 중인 메모리의 바이트 수가 표시됩니다. 비율 열에는 초과 신청 비율(DIPP 풀 전용에 대한)이 표시됩니다. 풀 및 메모리 통계 행은 다음 샘플 출력에 설명되어 있습니다.

```
admin@PA-7050-HA-0 (active-primary)> show running global-ippool

Idx  Type             From                       To          Num    Ref.Cnt   Size      Ratio
1    Dynamic IP       201.0.0.0-201.0.255.255    210.0.0.0   4096   2         657072    N/A
2    Dynamic IP       202.0.0.0-202.0.0.255      220.0.0.0   256    1         41232     N/A
3    Dynamic IP/Port  200.0.2.100-200.0.2.100    200.0.3.11  1      1         68720     8

Usable NAT DIP/DIPP shared memory size: 58490064     ← Total physical NAT memory (bytes)
Used NAT DIP/DIPP shared memory size: 767024 (1.3%)  ← Bytes and % of usable NAT memory
Dynamic IP NAT Pool: 2 (1.19%)          ← Number of DIP pools in use and % of total usable memory that all DIP pools use
Dynamic IP/Port NAT Pool: 1 (0.12%)     ← Number of DIPP pools in use and % of total usable memory that all DIPP pools use
```

가상 시스템에 대한 NAT 풀 통계의 경우, **show running ippool** 명령에는 NAT 규칙당 사용된 메모리 크기와 사용된 초과 신청 비율(DIPP 규칙에 대한)을 나타내는 열이 있습니다. 다음은 명령에 대한 샘플 출력입니다.

```
admin@PA-7050-HA-0 vsys1 (active-primary)>  show running ippool

VSYS 1 has 4 NAT rules, DIP and DIPP rules:
Rule          Type              Used     Available      Mem Size      Ratio
------------  ---------------   -------  ------------   ------------  -------
nat1          Dynamic IP        0        4096             788144          0
nat2          Dynamic IP        0        256               49424          0
nat3          Dynamic IP/Port   0        638976           100976          4
nat11         Dynamic IP        0        4096             788144          0
```

show running nat-rule-ippool rule 명령의 출력 필드에는 NAT 규칙당 사용된 메모리(바이트)가 표시됩니다. 다음은 둘러싸인 규칙에 대한 메모리 사용량이 있는, 명령에 대한 샘플 출력입니다.

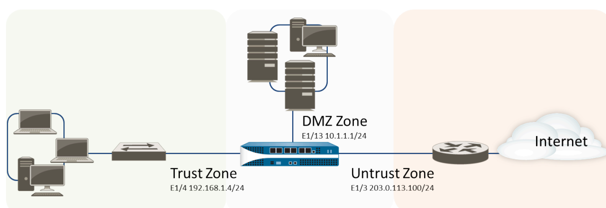
```
admin@PA-7050-HA-0 (active-primary)> show running nat-rule-ippool rule nat1

VSYS 1 Rule nat1:
Rule: nat1, Pool index: 1,  memory usage: 788144
------------------------------------------------------------
Reserve IP: no
201.0.0.0-201.0.255.255  =>
          210.0.0.0-210.0.15.255

Source          Xlat-Source      Ref.Cnt (F)      TTL(s)

Total IPs in use: 0
Total entries in time-reserve cache: 0
Total freelist left: 4096
```

NAT 구성

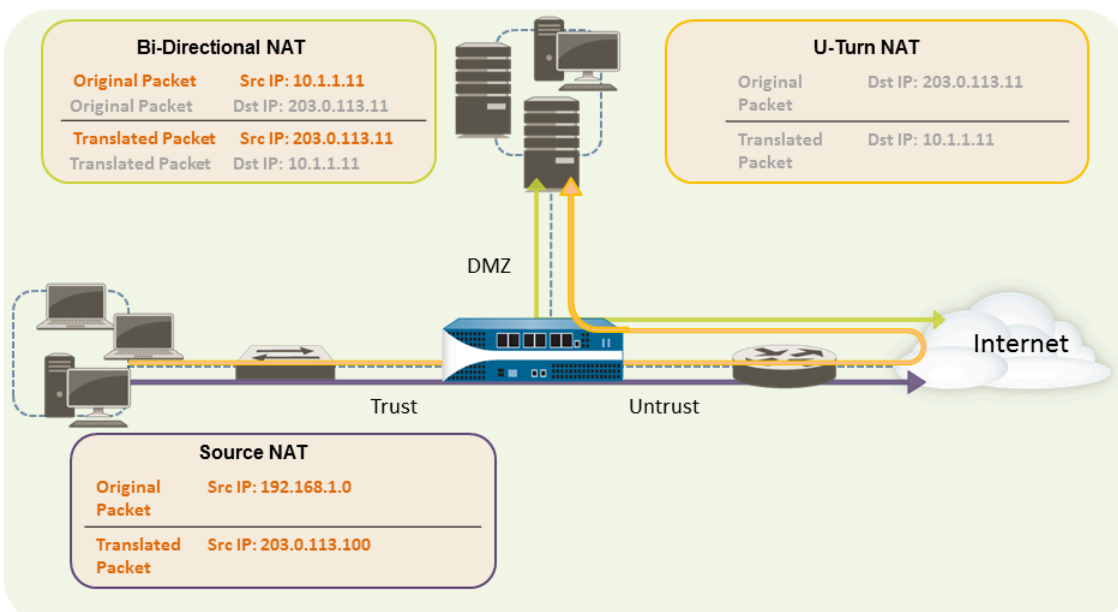
다음 작업을 수행하여 NAT의 다양한 측면을 구성합니다. 아래 예 외에도, NAT 구성 예 섹션에 예가 있습니다.

- 내부 클라이언트 IP 주소를 공용 IP 주소로 변환(소스 DIPP NAT)
- 내부 네트워크의 클라이언트가 공용 서버에 접속하도록 작동(대상 U-Turn NAT)
- 공용 서버에 대해 양방향 주소 변환 작동(정적 소스 NAT)
- DNS 재작성으로 대상 NAT 구성
- 동적 IP 주소를 사용하여 대상 NAT 구성
- DIPP NAT에 대한 초과 신청률 수정
- 동적 IP NAT 주소 예약
- 특정 호스트 또는 인터페이스에 대해 NAT 미작동

이 섹션의 처음 세 가지 NAT 예는 다음 토폴로지를 기반으로 합니다.



이 토폴로지를 기반으로, 다음과 같이 생성해야 하는 세 가지 NAT 정책이 있습니다.



- 내부 네트워크의 클라이언트가 인터넷의 리소스에 접속할 수 있도록 하려면, 내부 192.168.1.0 주소를 공개적으로 라우팅 가능한 주소로 변환해야 합니다. 이 경우, 내부 영역에서 방화벽을 떠나는 모든 패킷의 소스 주소로 송신 인터페이스 주소 203.0.113.100을 사용하여, 소스 NAT(위의 보라색 인클로저

및 화살표)를 구성합니다. 지침으로 내부 클라이언트 IP 주소를 공용 IP 주소(소스 DIPP NAT)로 변환을 참조하십시오.

- 내부 네트워크의 클라이언트가 DMZ 영역의 공용 웹 서버에 접속할 수 있도록 하려면, 외부 네트워크에서 패킷을 리디렉션하는 NAT 규칙을 구성해야 합니다. 여기서 원래 라우팅 표 조회는 패킷 내 203.0.113.11의 대상 주소를 기반으로 10.1.1.11의 DMZ 네트워크에 있는 웹 서버의 실제 주소로 이동해야 한다고 결정합니다. 이렇게 하려면 대상 주소를 DMZ 영역의 주소로 변환하기 위해 신뢰 영역(패킷의 소스 주소가 있는 곳)에서 비신뢰 영역(원래 대상 주소가 있는 곳)까지의 NAT 규칙을 생성해야 합니다. 이러한 유형의 대상 NAT를 ***U-Turn NAT***(위의 노란색 인클로저 및 화살표)라고 합니다. 지침은 내부 네트워크의 클라이언트가 공용 서버(대상 U-Turn NAT)에 접속할 수 있도록 작동을 참조하십시오.
- DMZ 네트워크의 사설 IP 주소와 외부 사용자가 접속할 수 있는 공개 주소를 모두 갖고 있는 웹 서버가 요청을 보내고 받을 수 있도록 작동시키려면, 방화벽은 공용 IP 주소에서 들어오는 패킷을 사설 IP 주소로, 나가는 패킷을 사설 IP 주소에서 공용 IP 주소로 변환해야 합니다. 방화벽에서는, 단일 양방향 정적 소스 NAT 정책(녹색 인클로저 및 위의 화살표)로 이를 달성할 수 있습니다. 공개 서버(정적 소스 NAT)에 대해 양방향 주소 변환 작동을 참조합니다.

내부 클라이언트 IP 주소를 공용 IP 주소로 변환(소스 DIPP NAT)

내부 네트워크의 클라이언트가 요청을 보낼 때 패킷의 소스 주소에는 내부 네트워크의 클라이언트에 대한 IP 주소가 포함됩니다. 내부적으로 사설 IP 주소 범위를 사용하는 경우 네트워크에서 나가는 패킷의 소스 IP 주소를 공개적으로 라우팅 가능한 주소로 변환하지 않는 한 클라이언트의 패킷을 인터넷에서 라우팅할 수 없습니다.

방화벽에서 소스 주소(및 선택적으로 포트)를 공용 주소로 변환하는 소스 NAT 정책을 구성하여 이를 수행할 수 있습니다. 이를 수행하는 한 가지 방법은 다음 절차에 표시된 대로 모든 패킷의 소스 주소를 방화벽의 이그레스 인터페이스로 변환하는 것입니다.

STEP 1 | 사용하려는 외부 IP 주소에 대한 주소 개체를 만듭니다.

1. 개체 > 주소를 선택하고 개체에 대한 이름 및 설명(선택 사항)을 추가합니다.
2. 유형에서**IP** 넷마스크를 선택한 다음 방화벽에 있는 외부 인터페이스의 IP 주소(이 예에서는 203.0.113.100)를 입력합니다.
3. 확인을 클릭합니다.

> 정책에서 주소 개체를 사용할 필요는 없지만 주소가 참조되는 모든 정책을 업데이트하지 않고 한 곳에서 업데이트할 수 있도록 허용하여 관리를 단순화하기 때문에 모범 사례입니다.

STEP 2 | NAT 정책을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 정책을 설명하는 이름을 입력합니다.
3. (선택 사항) 정책을 정렬하거나 필터링할 수 있는 키워드 또는 구문인 태그를 입력합니다.
4. **NAT** 유형으로 **ipv4**(기본값)를 선택합니다.
5. 원본 패킷 탭의 원본 영역섹션에서 내부 네트워크에 대해 생성한 영역을 선택하고(추가를 클릭한 다음 영역 선택) 대상 영역 목록에서 외부 네트워크에 대해 생성한 영역을 선택합니다.
6. 변환된 패킷 탭에서 화면의 소스 주소 변환 섹션에 있는 변환 유형 목록에서 동적 **IP** 및 포트를 선택합니다.
7. 주소 유형에는 두 가지 선택 사항이 있습니다. 변환된 주소를 선택한 다음 추가를 클릭할 수 있습니다. 방금 만든 주소 개체를 선택합니다.

   대체 주소 유형은 인터페이스 주소이며, 이 경우 변환된 주소는 인터페이스의 IP 주소가 됩니다. 이 선택의 경우 인터페이스를 선택하고 인터페이스에 둘 이상의 **IP** 주소가 있는 경우 선택적으로 IP 주소를 선택합니다.
8. 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

STEP 4 | (선택 사항) CLI에 액세스하여 변환을 확인합니다.

1. **`show session all`** 명령을 사용하여 소스 IP 주소 및 포트와 변환된 해당 IP 주소 및 포트를 확인할 수 있는 세션 테이블을 봅니다.
2. *show session id <id_number>*를 사용하여 세션에 대한 자세한 내용을 확인합니다.
3. 동적 IP NAT를 구성한 경우 **`show counter global filter aspect session stability drop | match nat`** 명령을 사용하여 NAT IP 할당으로 인해 실패한 세션이 있는지 확인합니다. 새 연결이 변환되어야 할 때 동적 IP NAT 풀의 모든 주소가 할당되면 패킷이 삭제됩니다.

내부 네트워크의 클라이언트가 공용 서버에 액세스할 수 있도록 설정(대상 U-Turn NAT)

내부 네트워크의 사용자가 DMZ에 있는 기업 웹 서버에 대한 액세스 요청을 보내면 DNS 서버는 이를 공인 IP 주소로 확인합니다. 요청을 처리할 때 방화벽은 패킷의 원래 대상(공용 IP 주소)을 사용하고 패킷을 언트러스트 영역의 이그레스(egress) 인터페이스로 라우팅합니다. 방화벽이 트러스트 영역의 사용자로부터 요청을 받을 때 웹 서버의 공용 IP 주소를 DMZ 네트워크의 주소로 변환해야 함을 알기 위해서는 방화벽이 다음을 수행할 수 있도록 하는 대상 NAT 규칙을 생성해야 합니다. 다음과 같이 DMZ 영역에 대한 이그레스(Egress) 인터페이스로 요청을 보냅니다.

STEP 1 | 웹 서버에 대한 주소 개체를 생성합니다.

1. 개체 > 주소를 선택하고 주소 개체에 대해 이름 및 선택적 설명을 추가합니다.
2. 유형에 대해 **IP Netmask**를 선택하고 이 예에서는 웹 서버의 공개 IP 주소 203.0.113.11을 입력합니다.

   확인을 클릭하여 주소 개체 유형을 **IP** 넷마스크에서 **FQDN**으로 전환할 수 있으며 FQDN이 나타나면 이 **FQDN** 사용을 클릭합니다. 또는 유형에 대해 **FQDN**을 선택한 다음 주소 개체에 사용할 FQDN을 입력합니다. FQDN을 입력하고 확인을 클릭하면 FQDN이 확인되는 IP 주소가 필드에 나타납니다. 이 IP 주소를 사용하여 FQDN에서 IP 넷마스크로 주소 개체 유형을 전환하려면 이 주소 사용을 클릭합니다. 그러면 유형이 필드에 나타나는 IP 주소와 함께 **IP** 넷마스크로 전환됩니다.
3. 확인을 클릭합니다.

STEP 2 | NAT 정책을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 NAT 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. 원본 패킷 탭의 원본 영역섹션에서 내부 네트워크에 대해 생성한 영역을 선택하고(추가를 클릭한 다음 영역 선택) 대상 영역 목록에서 외부 네트워크에 대해 생성한 영역을 선택합니다.
4. 대상 주소 섹션에서 공용 웹 서버에 대해 생성한 주소 개체를 추가합니다.
5. 변환된 패킷 탭에서 대상 주소 변환에 대해 변환 유형에 대해 정적 **IP**를 선택한 다음 DMZ 네트워크의 웹 서버 인터페이스에 할당된 IP 주소(이 예에서는 10.1.1.11)를 입력합니다. 또는 변환 유형을 동적 **IP**(세션 배포 포함)로 선택한 다음 변환된 주소를 IP 넷마스크, IP 범위 또는 FQDN을 사용하는 주소 개체 또는 주소 그룹으로 입력할 수 있습니다. 이들 중 하나라도 DNS에서 여러 주소를 반환할 수 있습니다. 변환된 대상 주소가 둘 이상의 주소로 확인되는 경우 방화벽은 선택할 수 있는 여러 방법 중 하나를 기반으로 들어오는 NAT 세션을 여러 주소에 분산합니다. 라운드 로빈(기본 방법), 소스 **IP** 해시, **IP** 모듈로, **IP** 해시 또는 최소 세션
6. 확인을 클릭합니다.

STEP 3 | 커밋을 클릭합니다.

공용 서버에 양방향 주소 변환 사용(정적 소스 NAT)

공용 서버가 물리적으로 위치한 네트워크 세그먼트에 개인 IP 주소가 할당된 경우 서버의 소스 주소를 이그레스(egress)에 따라 외부 주소로 변환하는 원본 NAT 규칙이 필요합니다. 정적 NAT 규칙을 만들어 내부 소스 주소인 10.1.1.11을 예제에서 외부 웹 서버 주소인 203.0.113.11로 변환합니다.

그러나 공용 서버는 패킷을 보내고 받을 수 있어야 합니다. 방화벽이 패킷을 DMZ 네트워크로 라우팅할 수 있도록 공용 주소(인터넷 사용자로부터 들어오는 패킷의 대상 IP 주소)를 개인 주소로 변환하는 상호 정책이 필요합니다. 다음 절차에 설명된 대로 양방향 정적 NAT 규칙을 생성합니다. 양방향 변환은 정적 NAT전용 옵션입니다.

STEP 1 | 웹 서버의 내부 IP 주소에 대한 주소 개체를 생성합니다.

1. 개체 > 주소를 선택하고 개체에 대한 이름 및 설명(선택 사항)을 추가합니다.
2. 유형 목록에서 **IP Netmask**를 선택한 다음 DMZ 네트워크에 있는 웹 서버의 IP 주소(이 예에서는 10.1.1.11)를 입력합니다.
3. 확인을 클릭합니다.

> 웹 서버의 공용 주소에 대한 주소 개체를 아직 만들지 않은 경우 이제 해당 개체를 만들어야 합니다.

STEP 2 | NAT 정책을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 NAT 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. 원본 패킷 탭에서 소스 영역 섹션에서 DMZ용으로 생성한 영역을 선택하고(추가 클릭 후 영역 선택) 대상 영역 목록에서 외부 네트워크용으로 생성되었습니다.
4. 소스 주소 섹션에서 내부 웹 서버 주소에 대해 생성한 주소 개체를 추가합니다.
5. 변환된 패킷 탭에서 소스 주소 변환 섹션의 변환 유형 목록에서 고정 **IP**를 선택한 다음 주소 개체를 선택합니다. 변환된 주소 목록에서 외부 웹 서버 주소에 대해 생성했습니다.
6. 양방향 필드에서 예를 선택합니다.
7. 확인을 클릭합니다.

STEP 3 | 커밋합니다.

커밋을 클릭합니다.

DNS 재작성으로 대상 NAT 구성

IPv4 주소의 정적 변환을 수행하는 대상 NAT 정책 규칙을 구성할 때, 방화벽이 규칙에 대해 구성된 원래 또는 변환된 IP 주소를 기반으로 DNS 응답의 IPv4 주소를 다시 쓰도록 규칙을 또한 구성할 수도 있습니다. 방화벽은 클라이언트에 응답을 전달하기 전에 DNS 응답(규칙과 일치)내 IPv4 주소(FQDN 해결)에 대해 NAT를 수행합니다. 따라서, 클라이언트는 대상 서비스에 도달하기 위해 적절한 주소를 받습니다.

DNS 재작성 사용 사례를 보고 재작성이 역방향 또는 순방향으로 발생하도록 지정할 지 여부를 결정하는데 도움을 줍니다.

> *DNS* 재작성을 작동시킨 동일한 *NAT* 규칙에서 양방향 소스 주소 변환을 작동시킬 수 없습니다.

STEP 1 | 방화벽이 규칙과 일치하는 IPv4 주소의 정적 변환을 수행하도록 지정하는 대상 NAT 정책 규칙을 생성하고 해당 IPv4 주소(A 레코드로부터)가 NAT 규칙에서 원본 또는 변환된 대상 주소와 일치할 때 DNS 응답에서 방화벽 재작성 IP 주소도 또한 지정합니다.

1. 정책 > **NAT**를 선택하고 NAT 정책 규칙을 추가합니다.
2. (선택 사항) 일반 탭에서 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. **NAT** 유형에서 **ipv4**를 선택합니다.
4. 원본 패킷 탭에서 대상 주소를 추가합니다.

   또한 원본 영역 또는 모든 출처 영역을 선택해야 하지만, ***DNS*** 재작성은 전역 수준에서 발생합니다. 원본 패킷 탭의 대상 주소만 일치합니다. ***DNS*** 재작성은 원본 패킷 탭의 다른 모든 필드를 무시합니다.

5. 변환된 패킷 탭의 대상 주소 변환에서 정적 **IP**가 될 변환 유형을 선택합니다 .
6. 변환된 주소를 선택하거나 새 주소를 입력합니다.
7. **DNS** 다시 쓰기를 사용하도록 설정하고 방향을 선택합니다.
   - DNS 응답내 IP 주소에 NAT 규칙이 지정하는 반대 변환이 필요한 경우 역방향(기본 설정)을 선택합니다. DNS 응답이 규칙내 변환된 대상 주소와 일치하는 경우, 규칙에서 사용하는 역변환을 사용하여 DNS 응답을 변환합니다. 예를 들어, 규칙이 IP 주소 1.1.1.10을 192.168.1.10으로 변환하는 경우, 방화벽은 192.168.1.10의 DNS 응답을 1.1.1.10으로 다시 씁니다.
   - DNS 응답의 IP 주소에 NAT 규칙이 지정하는 것과 동일한 변환이 필요한 경우 전달을 선택합니다. DNS 응답이 규칙내 원래 대상 주소와 일치하는 경우, 규칙에서 사용하는 것과 동일한 변환을 사용하여 DNS 응답을 변환합니다. 예를 들어, 규칙이 IP 주소 1.1.1.10을 192.168.1.10으로 변환하면, 방화벽은 1.1.1.10의 DNS 응답을 192.168.1.10으로 다시 씁니다.
8. 확인을 클릭합니다.

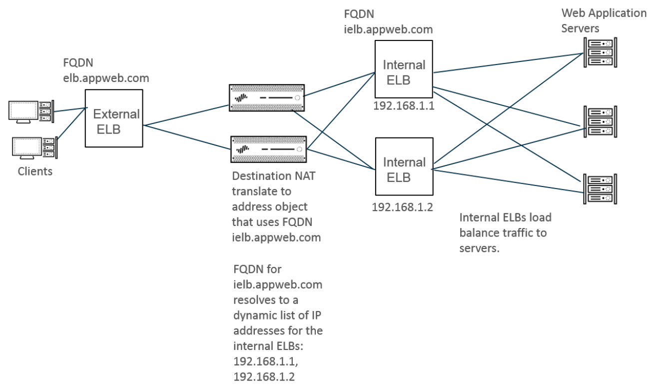
STEP 2 | 변경 사항을 커밋합니다.

동적 IP 주소를 사용하여 대상 NAT 구성

대상 NAT을(를) 사용하여 원래 대상 주소를 동적 IP 주소가 있고 FQDN을 사용하는 대상 호스트 또는 서버로 변환합니다. 동적 IP 주소를 사용하는 대상 NAT는 일반적으로 동적 IP 주소 지정을 사용하는 클라우드 배포에서 특히 유용합니다. 클라우드의 호스트 또는 서버에 새로운(동적) IP 주소가 있는 경우 DNS 서버에 지속적으로 쿼리하여 NAT 정책 규칙을 수동으로 업데이트할 필요가 없으며 최신 FQDN-to-IP 주소 매ping이 있는 서버로 DNS를 업데이트하기 위해 별도의 외부 구성 요소를 사용할 필요도 없습니다.

동적 IP 주소를 사용하여 대상 NAT를 구성하는 경우 FQDN만 사용해야 합니다(IP 넷마스크 또는 IP 범위가 아님).

다음 예제 토폴로지에서 클라이언트는 클라우드에서 웹 애플리케이션을 호스팅하는 서버에 연결하려고 합니다. 외부 ELB(Elastic Load Balancer)는 서버에 연결하는 내부 ELB에 연결되는 방화벽에 연결합니다. 예를 들어 시간이 지남에 따라 Amazon Web Services(AWS)는 서비스 수요에 따라 내부 ELB에 할당된 FQDN의 IP 주소를 추가(및 제거)합니다. 내부 ELB에 NAT용 FQDN을 사용하는 유연성은 정책이 서로 다른 시간에 다른 IP 주소로 확인되도록 하여 업데이트가 동적이기 때문에 대상 NAT를 더 쉽게 사용할 수 있도록 합니다.



STEP 1 | 주소를 변환할 서버의 FQDN을 사용하여 주소 개체를 생성합니다.

1. 개체 > 주소를 선택하고 이름을 기준으로 주소 개체를 추가합니다(예: **`Post-NAT-Internal-ELB`**).
2. 유형으로 **FQDN**을 선택하고 FQDN을 입력합니다. 이 예에서 FQDN은 **`ielb.appweb.com`**입니다.
3. 확인을 클릭합니다.

STEP 2 | 대상 NAT 정책을 만듭니다.

1. 일반 탭에서 정책 > **NAT**를 선택하고 이름별로 NAT 정책 규칙 추가를 선택합니다.
2. **NAT** 유형으로 **ipv4**를 선택합니다.
3. 원본 패킷 탭에서 소스 영역과 대상 영역을 추가합니다.
4. 변환된 패킷 탭의 대상 주소 변환 섹션에서 변환 유형으로 동적 **IP(**세션 배포 포함**)**를 선택합니다.
5. 변환된 주소에서 FQDN에 대해 만든 주소 개체를 선택합니다. 이 예에서 FQDN은 **`post-NAT-Internal-ELB`**입니다.
6. 세션 배포 방법에서 다음 중 하나를 선택합니다.
   - 라운드 로빈(기본값) - 새 세션을 IP 주소에 순환 순서로 할당합니다. 배포 방법을 변경할 이유가 없는 한 라운드 로빈 배포가 적합할 수 있습니다.
   - 소스 **IP** 해시 - 소스 IP 주소의 해시를 기반으로 새 세션을 할당합니다. 단일 소스 IP 주소에서 오는 트래픽이 있는 경우 소스 IP 해시를 선택하지 마십시오. 다른 방법을 선택하십시오.
   - **IP Modulo** - 방화벽은 들어오는 패킷의 소스 및 대상 IP 주소를 고려합니다. 방화벽은 XOR 연산과 모듈로 연산을 수행합니다. 결과적으로 방화벽이 새 세션을 할당하는 IP 주소를 결정합니다.
   - **IP** 해시 - 소스 및 대상 IP 주소의 해시를 기반으로 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.

   방화벽은 여러 *IP* 주소 간에 세션을 배포하기 전에 대상 *IP* 주소 목록에서 중복 *IP* 주소를 제거하지 않습니다*.* 방화벽은 세션을 중복되지 않은 주소에 배포하는 것과 동일한 방식으로 중복 주소에 세션을 배포합니다*. (*예를 들어 변환된 주소가 주소 개체의 주소 그룹이고 한 주소 개체가 *IP* 주소로 확인되는 *FQDN*이고 다른 주소 개체가 동일한 *IP* 주소를 포함하는 범위인 경우 변환 풀에 중복 주소가 발생할 수 있습니다*.)*
7. 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋합니다.

STEP 4 | (선택 사항) 방화벽이 FQDN을 새로 고치는 빈도(사용 사례 1: 방화벽에 DNS 확인 필요)를 구성할 수 있습니다.

DIPP NAT에 대한 초과 가입률 수정

DIPP NAT 초과 가입을 사용할 필요가 없는 충분한 공용 IP 주소가 있는 경우 초과 가입 비율을 줄여 더 많은 DIP 및 DIPP NAT 규칙을 허용할 수 있습니다.

STEP 1 | DIPP NAT 초과 가입률을 봅니다.

1. 디바이스 > 설정 > 세션 > 세션 설정을 선택합니다. **NAT** 초과 구독 비율 설정을 봅니다.

STEP 2 | DIPP NAT 초과 가입 비율을 설정합니다.

1. 세션 설정 섹션을 편집합니다.
2. **NAT** 초과 구독 비율 목록에서 원하는 비율에 따라 **1x**, **2x**, **4x** 또는 **8x**를 선택합니다.

   플랫폼 기본 설정은 모델에 대한 기본 초과 구독 설정을 적용합니다. 초과 구독을 원하지 않으면 ***1x***를 선택하십시오.
3. 확인을 클릭하고 변경 사항을 커밋합니다.

동적 IP NAT 주소 예약

동적 IP NAT 주소를 구성 가능한 기간 동안 예약하여 변환이 필요한 다른 소스 IP 주소에 변환된 주소로 할당되지 않도록 할 수 있습니다. 구성된 경우 예약은 진행 중인 모든 변환된 동적 IP 주소와 모든 새 변환에 적용됩니다.

진행 중인 변환과 새 변환 모두에 대해 소스 IP 주소가 사용 가능한 변환된 IP 주소로 변환될 때 특정 소스 IP와 관련된 모든 세션이 만료된 후에도 해당 페어링이 유지됩니다. 각 소스 IP 주소에 대한 예약 타이머는 해당 소스 IP 주소 변환을 사용하는 모든 세션이 만료된 후에 시작됩니다. 동적 IP NAT는 일대일 변환입니다. 하나의 소스 IP 주소는 구성된 풀에서 사용 가능한 주소 중에서 동적으로 선택되는 하나의 변환된 IP 주소로 변환됩니다. 따라서 예약된 변환된 IP 주소는 새 세션이 시작되지 않아 예약이 만료될 때까지 다른 소스 IP 주소에 사용할 수 없습니다. 활성 세션이 없는 기간이 지난 후 소스 IP/변환된 IP 매핑에 대한 새 세션이 시작될 때마다 타이머가 재설정됩니다.

기본적으로 예약되어 있는 주소는 없습니다. 방화벽 또는 가상 시스템에 대한 동적 IP NAT 주소를 예약할 수 있습니다.

- 방화벽에 대한 동적 IP NAT 주소를 예약합니다.

  다음 명령을 입력합니다.

  ```
  admin@PA-3250# set setting nat reserve-ip yes
  ```

  ```
  admin@PA-3250# set setting nat reserve-time <1-604800 secs>
  ```

- 가상 시스템에 대한 동적 IP NAT 주소를 예약합니다.

  다음 명령을 입력합니다.

  ```
  admin@PA-3250# set vsys <vsysid> setting nat reserve-ip yes
  ```

  ```
  admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800
   secs>
  ```

  예를 들어 주소가 30개인 동적 IP NAT 풀이 있고 **nat 예약 시간**이 28800초(8시간)로 설정된 경우 20개의 변환이 진행 중이라고 가정합니다. 이제 20개의 변환이 예약되어 있으므로 각 소스 IP/변환된 IP 매핑을 사용하는 마지막 세션(모든 애플리케이션)이 만료되면 변환된 IP 주소는 해당 소스 IP 주소에 대해 8시간 동안 예약됩니다. 이 경우 해당 소스 IP 주소를 다시 변환해야 합니다. 또한 나머지 10개의

변환된 주소가 할당되면 각 주소는 소스 IP 주소용으로 예약되며, 각 주소는 해당 소스 IP 주소의 마지막 세션이 만료될 때 시작되는 타이머가 있습니다.

이러한 방식으로 각 소스 IP 주소는 풀에서 동일한 NAT 주소로 반복적으로 변환될 수 있습니다. 변환된 해당 주소에 대한 활성 세션이 없더라도 풀에서 예약된 변환된 IP 주소가 다른 호스트에 할당되지 않습니다.

소스 IP/변환된 IP 매핑의 모든 세션이 만료되고 8시간의 예약 타이머가 시작된다고 가정합니다. 해당 변환에 대한 새 세션이 시작되면 타이머가 중지되고 세션이 모두 끝날 때까지 계속됩니다. 이때 예약 타이머가 다시 시작되어 변환된 주소가 예약됩니다.

예약 타이머는 **`set setting nat reserve-ip no`** 명령을 입력하여 비활성화하거나 **`nat reserve-time`**을 다른 값으로 변경할 때까지 동적 IP NAT 풀에서 유효합니다.

예약에 대한 CLI 명령은 동적 IP 및 포트(DIPP) 또는 정적 IP NAT 풀에 영향을 주지 않습니다.

특정 호스트 또는 인터페이스에 대해 NAT 비활성화

소스 NAT 및 대상 NAT 규칙 모두 주소 변환을 비활성화하도록 구성할 수 있습니다. 서브넷의 특정 호스트나 특정 인터페이스에서 나가는 트래픽에 대해 NAT가 발생하지 않도록 하려는 예외가 있을 수 있습니다. 다음 절차는 호스트에 대해 소스 NAT를 비활성화하는 방법을 보여줍니다.

STEP 1 | NAT 정책을 만듭니다.

1. 정책 > **NAT**을 선택하고 정책에 대한 설명이 포함된 이름을 추가를 클릭합니다.
2. 원본 패킷 탭의 원본 영역섹션에서 내부 네트워크에 대해 생성한 영역을 선택하고(추가를 클릭한 다음 영역 선택) 대상 영역 목록에서 외부 네트워크에 대해 생성한 영역을 선택합니다.
3. 소스 주소에서 추가를 클릭하고 호스트 주소를 입력합니다. 확인을 클릭합니다.
4. 변환된 패킷 탭에 있는 화면의 소스 주소 변환 섹션에 있는 변환 유형 목록에서 없음을 선택합니다.
5. 확인을 클릭합니다.

STEP 2 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

NAT 규칙은 위에서 아래로 순서대로 처리되므로 면제하려는 소스에 대한 주소 변환이 발생하기 전에 처리되도록 NAT 면제 정책을 다른 NAT 정책보다 먼저 배치하십시오.

NAT 구성 예

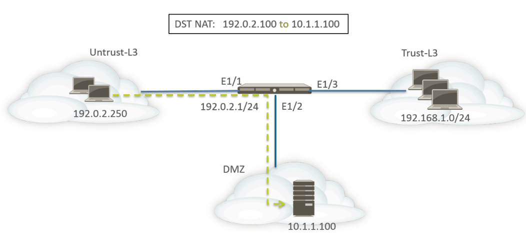
- 대상 NAT 예 - 일대일 매핑
- 포트 변환이 있는 대상 NAT 예
- 대상 NAT 예 - 일대다 매핑
- 소스 및 대상 NAT 예제
- 가상 와이어 소스 NAT 예제
- 가상 와이어 정적 NAT 예
- 가상 회선 대상 NAT(DNAT)

대상 NAT 예 - 일대일 매핑

NAT 및 보안 규칙을 구성할 때 가장 흔한 실수는 영역 및 주소 개체에 대한 참조입니다. 대상 NAT 규칙에 사용되는 주소는 항상 패킷에서 원래 IP 주소(즉, 미리 변환된 주소)를 참조합니다. NAT 규칙내 대상 영역은 원래 패킷에서의 대상 IP 주소(즉, NAT 이전 대상 IP 주소)의 경로 조회 후에 결정됩니다.

보안 정책내 주소는 원래 패킷에서의 IP 주소(즉, NAT 이전 주소)도 또한 참조합니다. 그러나, 대상 영역은 최종 호스트가 물리적으로 연결된 영역입니다. 즉, 보안 규칙내 대상 영역은 NAT 이후 대상 IP 주소의 경로 조회 후에 결정됩니다.

일대일 대상 NAT 매핑의 다음 예에서, 언트러스트-L3이라는 영역의 사용자는 IP 주소 192.0.2.100을 사용하여 DMZ라는 영역의 서버 10.1.1.100에 접속합니다.



NAT 규칙을 구성하기 전에, 이 시나리오에 대한 이벤트 순서를 고려합니다.

- ☐ 호스트 192.0.2.250은 주소 192.0.2.100(대상 서버의 공용 주소)에 대한 ARP 요청을 보냅니다.
- ☐ 방화벽은 이더넷1/1 인터페이스에서 대상 192.0.2.100에 대한 ARP 요청 패킷을 수신하고 요청을 처리합니다. 방화벽은 구성된 대상 NAT 규칙 때문에 자체 MAC 주소로 ARP 요청에 응답합니다.
- ☐ NAT 규칙은 일치에 대해 평가됩니다. 대상 IP 주소를 변환하려면, 대상 IP 192.0.2.100을 10.1.1.100으로 변환하기 위해 언트러스트-L3 영역에서 언트러스트-L3 영역으로 대상 NAT 규칙을 생성해야 합니다.
- ☐ 변환된 주소를 결정한 후, 방화벽은 대상 10.1.1.100에 대한 경로 조회를 수행하여 송신 인터페이스를 결정합니다. 이 예에서, 송신 인터페이스는 DMZ 영역내 이더넷1/2입니다.

- ☐ 방화벽은 언트러스트-L3 영역에서 DMZ로 트래픽이 허용되는지 확인하기 위해 보안 정책 조회를 수행합니다.

  정책 방향은 수신 영역 및 서버가 물리적으로 위치한 영역과 일치합니다.

  보안 정책은 대상 주소가 *192.0.2.100*인, 원본 패킷내 *IP* 주소를 참조합니다.

- ☐ 방화벽은 패킷을 서버 출력 인터페이스 이더넷1/2로 전달합니다. 패킷이 방화벽을 벗어나면 대상 주소가 10.1.1.100으로 변경됩니다.

이 예에서, 주소 개체는 웹서버 사설(10.1.1.100) 및 웹서버 공용(192.0.2.100)에 대해 구성됩니다. 구성된 NAT 규칙은 다음과 같습니다.

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

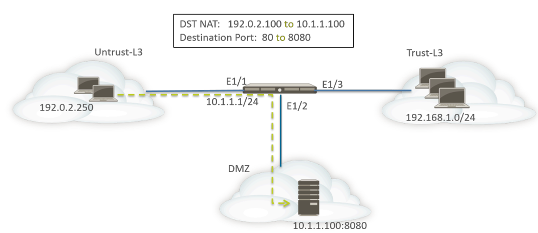
NAT 규칙의 방향은 경로 조회 결과를 기반으로 합니다.

언트러스트-L3 영역에서 서버에 대한 접속을 제공하도록 구성된 보안 정책은 다음과 같습니다.

	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

포트 변환이 있는 대상 NAT 예

이 예에서, 웹 서버는 포트 8080에서 HTTP 트래픽을 수신하도록 구성됩니다. 클라이언트는 IP 주소 192.0.2.100 및 TCP 포트 80을 사용하는 웹 서버에 접속합니다. 대상 NAT 규칙은 IP 주소와 포트를 모두 10.1.1.100 및 TCP 포트 8080으로 변환하도록 구성됩니다. 주소 개체는 웹서버 사설(10.1.1.100) 및 서버 공용 (192.0.2.100)에 대해 구성됩니다.



방화벽에서 다음 NAT 및 보안 규칙을 구성해야 합니다.

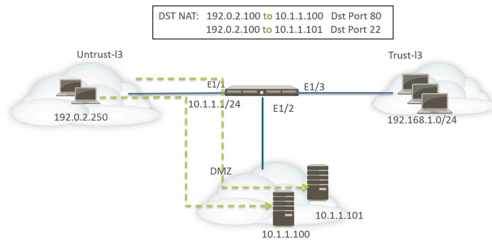
		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

show session all CLI 명령을 사용하여 변환을 확인합니다.

대상 NAT 예 - 일대다 매핑

이 예에서, 하나의 IP 주소는 두 개의 서로 다른 내부 호스트에 매핑됩니다. 방화벽은 애플리케이션을 사용하여 방화벽이 트래픽을 전달하는 내부 호스트를 식별합니다.



모든 HTTP 트래픽은 호스트 10.1.1.100으로 전송되고 SSH 트래픽은 서버 10.1.1.101로 전송됩니다. 다음 주소 개체가 필요합니다.

- 서버의 미리 변환된 하나의 IP 주소에 대한 주소 개체
- SSH 서버의 실제 IP 주소에 대한 주소 개체
- 웹 서버의 실제 IP 주소에 대한 주소 개체

해당 주소 개체가 생성됩니다.

- 공용-서버: 192.0.2.100
- SSH-서버: 10.1.1.101
- 사설 웹서버: 10.1.1.100

NAT 규칙은 다음과 같습니다.

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	service-http	none	destination-translation address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

보안 규칙은 다음과 같습니다.

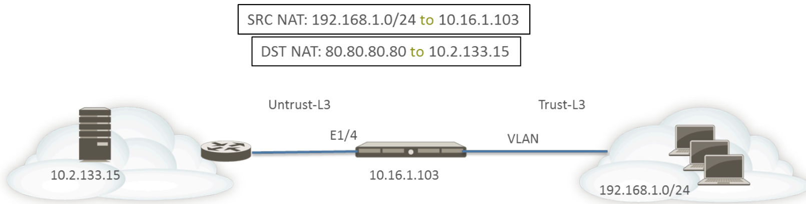
			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow
SSH access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	ssh	any	Allow

소스 및 대상 NAT 예제

이 예제에서는 NAT 규칙은 클라이언트와 서버 간의 패킷의 소스 및 대상 IP 주소를 모두 변환합니다.

- 출처 NAT-트러스트-L3 영역의 클라이언트에서 트러스트-L3 영역의 서버로 패킷의 소스 주소는 네트워크 192.168.1.0/24의 개인 주소에서 방화벽의 이그레스(egress) 인터페이스의 IP 주소로 변환됩니다(10.16.1.103). 동적 IP 및 포트 변환으로 인해 포트 번호도 변환됩니다.

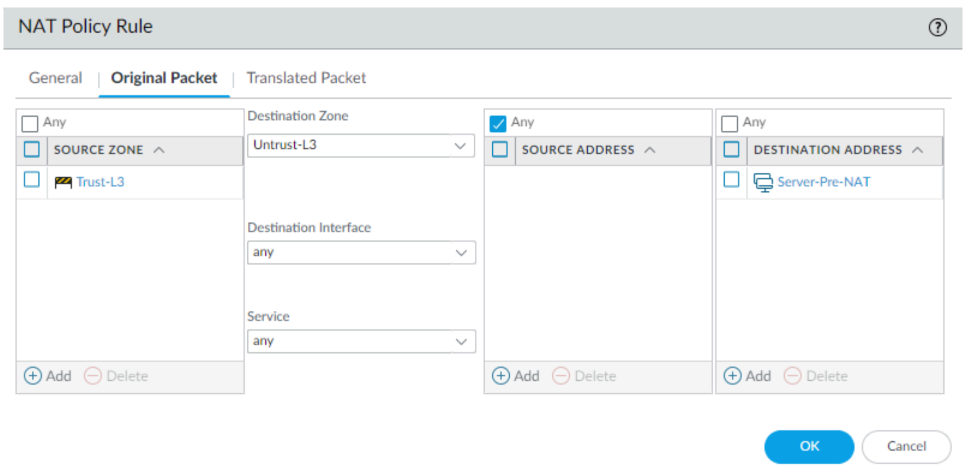
- 대상 NAT- 클라이언트에서 서버로 패킷의 대상 주소는 서버의 공용 주소(80.80.80.80)에서 서버의 개인 주소(10.2.133.15)로 변환됩니다.

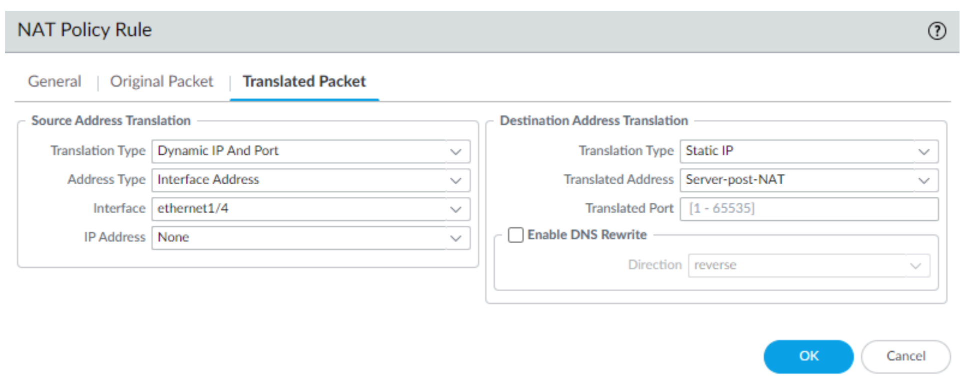


다음 주소 개체는 대상 NAT에 대해 생성됩니다.

- Server-Pre-NAT: 80.80.80.80
- Server-post-NAT: 10.2.133.15

다음 스크린샷에서는 예제의 소스 및 대상 NAT 정책을 구성하는 방법을 보여 줍니다.





변환을 확인하려면 CLI 명령 표시 세션을 사용하여 **`모든 필터 대상 80.80.80.80`**을 사용합니다. 클라이언트 주소 192.168.1.11 및 포트 번호는 10.16.1.103 및 포트 번호로 변환됩니다. 대상 주소 80.80.80.80은 10.2.133.15로 변환됩니다.

가상 와이어 소스 NAT 예제

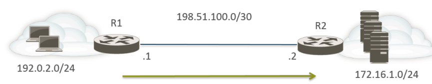
Palo Alto Networks® 방화벽의 가상 와이어 배포에는 최종 디바이스에 보안을 투명하게 제공하는 이점이 포함됩니다. 가상 와이어로 구성된 인터페이스에 대해 NAT를 구성할 수 있습니다. 모든 NAT 유형은 소스 NAT(동적 IP, 동적 IP 및 포트, 정적) 및 대상 NAT가 허용됩니다.

가상 와이어의 인터페이스에는 IP 주소가 할당되어 있지 않으므로 IP 주소를 인터페이스 IP 주소로 변환할 수 없습니다. IP 주소 풀을 구성해야 합니다.

가상 와이어 인터페이스에서 NAT를 수행할 때는 소스 주소를 이웃 디바이스가 통신하는 것과 다른 서브넷으로 변환하는 것이 좋습니다. 방화벽은 NAT 주소에 대한 ARP를 프록시하지 않습니다. 패킷을 가상 와이어 모드에서 변환하려면 업스트림 및 다운스트림 라우터에서 적절한 라우팅을 구성해야 합니다. 이웃 장치는 가상 와이어의 다른 쪽 끝에 있는 장치 인터페이스에 있는 IP 주소에 대한 ARP 요청을 해결할 수 있습니다. 프록시 ARP에 대한 자세한 내용은 NAT 주소 풀의 프록시 ARP를 참조하십시오.

아래 소스 NAT 예제에서는 폭스 바겐 트러스트라는 가상 와이어 영역에서 폭스 바겐 트러스트라는 존으로 보안 정책(표시되지 않음)이 구성됩니다.

다음 토폴로지에서 두 개의 라우터는 서브넷 192.0.2.0/24와 172.16.1.0/24 사이의 연결을 제공하도록 구성됩니다. 라우터 간의 링크는 서브넷 198.51.100.0/30으로 구성됩니다. 정적 라우팅은 네트워크 간의 연결을 설정하기 위해 두 라우터에서 구성됩니다. 방화벽이 환경에 배포되기 전에 각 라우터의 토폴로지 및 라우팅 테이블은 다음과 같습니다.



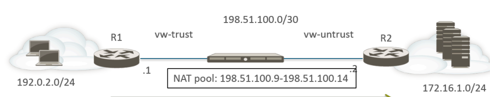
R1의 경로:

대상	다음 홉
172.16.1.0/24	198.51.100.2

R2의 경로:

대상	다음 홉
192.0.2.0/24	198.51.100.1

이제 방화벽은 두 계층 3 장치 사이의 가상 와이어 모드에 배포됩니다. 범위 198.51.100.9 ~ 198.51.100.14가 있는 NAT IP 주소 풀이 방화벽에 구성됩니다. 네트워크 172.16.1.0/24의 서버에 액세스하는 서브넷 192.0.2.0/24의 클라이언트로부터의 모든 통신은 198.51.100.9에서 198.51.100.14 범위의 번역된 소스 주소를 사용하여 R2에 도착합니다. 서버의 응답은 이러한 주소로 전달됩니다.



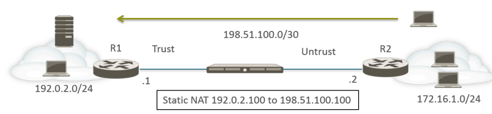
소스 NAT가 작동하려면 R2에서 적절한 라우팅을 구성해서 다른 주소로 향하는 패킷이 삭제되지 않도록 해야 합니다. 아래 라우팅 표에는 R2의 수정된 라우팅 테이블이 표시됩니다. 이 경로는 데스티네이션 198.51.100.9-198.51.100.14로의 트래픽을 보장하며(즉, 서브넷198.51.100.8/29에 호스트됨) R1에 방화벽을 통해 다시 전송됩니다.

R2의 경로:

대상	다음 홉
198.51.100.8/29	198.51.100.1

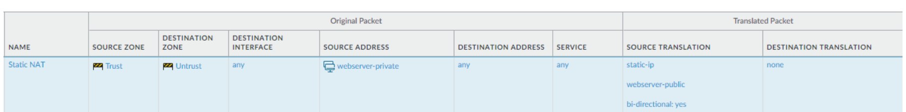
가상 와이어 정적 NAT 예

이 예제에서는 보안 정책이 트러스트라는 가상 와이어 존에서 트러스트 해제라는 가상 와이어 영역으로 구성됩니다. 호스트 192.0.2.100은 정적으로 198.51.100.100을 주소로 변환합니다. 양방향 옵션을 사용하도록 설정하면 방화벽은 트러스트 해제 영역에서 트러스트 영역까지 NAT 정책을 생성합니다. 언트러스트 존의 클라이언트는 IP 주소 198.51.100.100을 사용하여 서버에 액세스하며 방화벽은 198.0.2.100으로 변환됩니다. 서버가 192.0.2.100으로 시작한 모든 연결은 소스 IP 주소 198.51.100.100으로 변환됩니다.



R2의 경로:

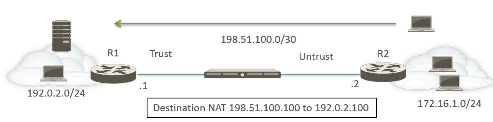
대상	다음 홉
198.51.100.100/32	198.51.100.1



	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Static NAT	Trust	Untrust	any	webserver-private	any	any	static-ip webserver-public bi-directional: yes	none

가상 회선 대상 NAT(DNAT)

언트러스트 존의 클라이언트는 방화벽이 192.0.2.100으로 변환하는 IP 주소 198.51.100.100을 사용하여 서버에 액세스합니다. NAT 및 보안 정책은 모두 언트러스트 존에서 트러스트 존으로 구성되어야 합니다.



R2의 경로:

대상	다음 홉
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
DST NAT	Untrust	Trust	any	any	webserver-public	any	none	destination-translation address: webserver-private

NPTv6

IPv6-to-IPv6 네트워크 접두사 변환(NPTv6)은 한 IPv6 접두사를 다른 IPv6 접두사(포트 번호는 변경되지 않음)로 상태 비저장 정적 변환을 수행합니다. NPTv6의 주요 네 가지 이점:

- 공급자 독립 주소가 여러 데이터 센터에서 보급되어 발생하는 비대칭 라우팅 문제를 방지할 수 있습니다.
- NPTv6을 사용하면 반환 트래픽이 트래픽을 전송한 동일한 방화벽에 도착하도록 보다 구체적인 경로를 알릴 수 있습니다.
- 개인 및 공용 주소는 독립적입니다. 다른 하나에 영향을 주지 않고 하나를 변경할 수 있습니다.
- 고유 로컬 주소 전역적으로 라우팅 가능한 주소로 변환할 수 있습니다.

이 주제는 NAT에 대한 기본적인 이해를 바탕으로 합니다. NPTv6을 구성하기 전에 NAT 개념에 익숙해야 합니다.

- NPTv6 개요
- NPTv6 작동 방식
- NDP 프록시
- NPTv6 및 NDP 프록시 예제
- NPTv6 정책 만들기

NPTv6 개요

이 섹션에서는 IPv6-to-IPv6 NPTv6 네트워크 접두사 변환(NPTv6) 및 구성 방법에 대해 설명합니다. NPTv6은 RFC 6296에 정의되어 있습니다. Palo Alto Networks®는 RFC에 정의된 모든 기능을 구현하지는 않지만 구현한 기능에서 RFC를 준수합니다.

NPTv6은 한 IPv6 접두사를 다른 IPv6 접두사로 상태 비저장 변환을 수행합니다. 상태 비저장이며, 다시 말해 변환된 주소의 포트 또는 세션을 추적하지 않습니다. NPTv6은 Stateful인 NAT66과 다릅니다. Palo Alto Networks는 NPTv6 RFC 6296 접두사 변환을 지원합니다. NAT66을 지원하지 않습니다.

IPv4 공간의 제한된 주소로 NAT을(를) 라우팅할 수 없는 개인 IPv4 주소를 하나 이상의 전역적으로 라우팅 가능한 IPv4 주소로 변환하는 데 필요했습니다. IPv6 주소 지정을 사용하는 조직의 경우 IPv6 주소가 풍부하기 때문에 IPv6 주소를 IPv6 주소로 변환할 필요가 없습니다. 그러나 방화벽에서 IPv6 접두사를 NPTv6을 사용하는 이유 변환해야 합니다.

***NPTv6**은 보안을 제공하지 않는다는 점을 이해하는 것이 중요합니다. 일반적으로 상태 비저장 네트워크 주소 변환은 보안을 제공하지 않습니다. 주소 변환 기능을 제공합니다. **NPTv6**은 포트 번호를 숨기거나 변환하지 않습니다. 트래픽이 의도한 대로 제어되도록 각 방향에서 방화벽 보안 정책을 올바르게 설정해야 합니다.*

NPTv6은 IPv6 주소의 접두사 부분을 변환하지만 호스트 부분이나 애플리케이션 포트 번호는 변환하지 않습니다. 호스트 부분은 단순히 복사되므로 방화벽 양쪽에서 동일하게 유지됩니다. 호스트 부분은 패킷 헤더 내에서도 계속 볼 수 있습니다.

NPTv6은 다음 방화벽 모델에서 지원됩니다(하드웨어 조회가 있는 NPTv6이지만 패킷은 CPU를 통과함).

- PA-7000 시리즈 방화벽
- PA-5200 시리즈 방화벽
- PA-3200 시리즈 방화벽
- PA-800 방화벽
- PA-220 방화벽

VM 시리즈 방화벽은 NPTv6을 지원하지만 하드웨어가 세션 조회를 수행하도록 할 수 없습니다.

- 고유 로컬 주소
- NPTv6을 사용하는 이유

고유 로컬 주소

RFC 4193, 고유 로컬 IPv6 유니캐스트 주소는 IPv6 유니캐스트 주소인 고유 로컬 주소(ULA)를 정의합니다. 이들은 RFC 1918, 사설 인터넷을 위한 주소 할당에서 식별된 사설 IPv4 주소와 동등한 IPv6 주소로 간주될 수 있습니다. 이 주소는 전역적으로 라우팅할 수 없습니다.

ULA는 전역적으로 고유하지만 전역적으로 라우팅할 수 있을 것으로 예상되지 않습니다. 로컬 통신을 위한 것이며 사이트와 같은 제한된 영역이나 소수의 사이트 사이에서 라우팅할 수 있습니다. Palo Alto Networks®는 ULA 할당을 권장하지 않지만 NPTv6으로 구성된 방화벽은 ULA를 포함하여 전송된 접두사를 변환합니다.

NPTv6을 사용하는 이유

전역적으로 라우팅 가능한 공용 IPv6 주소가 부족하지 않지만 IPv6 주소를 변환해야 하는 이유가 있습니다. NPTv6:

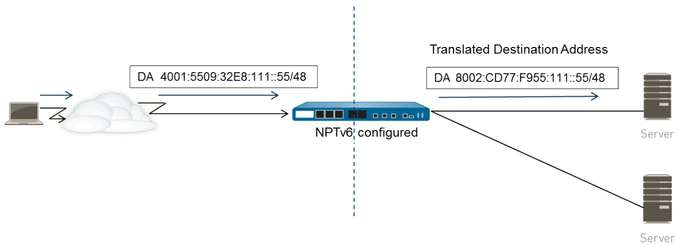
- 비대칭 라우팅 방지 - 공급자 독립 주소 공간(예: /48)이 여러 데이터 센터에서 전역 인터넷에 보급되는 경우 비대칭 라우팅이 발생할 수 있습니다. NPTv6을 사용하면 지역 방화벽에서 보다 구체적인 경로를 알릴 수 있으며 반환 트래픽은 소스 IP 주소가 변환기에 의해 변환된 동일한 방화벽에 도달합니다.
- 주소 독립성 제공 - 전역 접두사가 변경된 경우(예: ISP에 의해 또는 조직 병합의 결과로) 로컬 네트워크 내부에서 사용되는 IPv6 접두사를 변경할 필요가 없습니다. 반대로 인터넷에서 사설망의 서비스에 액세스하는 데 사용되는 주소를 방해하지 않고 내부 주소를 마음대로 변경할 수 있습니다. 두 경우 모두 네트워크 주소를 재할당하는 대신 NAT 규칙을 업데이트합니다.
- 라우팅에 대한 **ULA** 변환 - 사설 네트워크 내에서 할당할 수 있으며 방화벽이 이를 전역적으로 라우팅 가능한 주소로 변환하도록 고유 로컬 주소을(를) 할 수 있습니다. 따라서 개인 주소 지정의 편리함과 변환되고 라우팅 가능한 주소의 기능을 사용할 수 있습니다.
- **IPv6** 접두사에 대한 노출 감소 - IPv6 접두사는 네트워크 접두사를 변환하지 않은 경우보다 덜 노출되지만 NPTv6은 보안 조치가 아닙니다. 각 IPv6 주소의 인터페이스 식별자 부분은 변환되지 않습니다. 방화벽의 양쪽에서 동일하게 유지되며 패킷 헤더를 볼 수 있는 모든 사람이 볼 수 있습니다. 또한 접두사는 안전하지 않으며, 다른 사용자에 의해 정해질 수 있습니다.

NPTv6 작동 방식

NPTv6에 대한 정책을 구성하면 Palo Alto Networks® 방화벽이 양방향으로 정적 일대일 IPv6 변환을 수행합니다. 변환은 RFC 6296에 설명된 알고리즘을 기반으로 합니다.

한 사용 사례에서 NPTv6을 수행하는 방화벽은 내부 네트워크와 전역적으로 라우팅 가능한 접두사를 사용하는 외부 네트워크(예: 인터넷) 사이에 있습니다. 데이터그램이 아웃바운드 방향으로 갈 때 내부 소스 접두사는 외부 접두사로 대체됩니다. 이것은 소스 변환으로 알려져 있습니다.

또 다른 사용 사례에서는 데이터그램이 인바운드 방향으로 이동하는 경우 대상 접두사가 내부 접두사로 대체됩니다(대상 변환이라고 함). 아래 그림은 대상 변환 및 NPTv6의 특성을 보여줍니다. IPv6 주소의 접두어 부분만 변환됩니다. 주소의 호스트 부분은 변환되지 않으며 방화벽 양쪽에서 동일하게 유지됩니다. 아래 그림에서 호스트 식별자는 방화벽 양쪽에서 111::55입니다.



NPTv6은 보안을 제공하지 않는다는 점을 이해하는 것이 중요합니다. NPTv6 NAT 정책을 계획하는 동안 각 방향에서 보안 정책도 구성해야 합니다.

NAT 또는 NPTv6 정책 규칙은 원본 주소와 변환된 주소를 둘 다 모두로 설정할 수 없습니다.

IPv6 접두사 변환을 원하는 환경에서는 세 가지 방화벽 기능이 함께 작동합니다. NPTv6 NAT 정책, 보안 정책 및 NDP 프록시.

방화벽은 다음을 변환하지 않습니다.

- 방화벽이 ND(Neighbor Discovery) 캐시에 있는 주소.
- 서브넷 0xFFFF(RFC 6296, 부록 B에 따름).
- IP 멀티캐스트 주소.
- 접두사 길이가 /31 이하인 IPv6 주소.
- 링크 로컬 주소. 방화벽이 가상 와이어 모드에서 작동하는 경우 변환할 IP 주소가 없고 방화벽이 링크 로컬 주소를 변환하지 않습니다.
- TCP 인증 옵션(RFC 5925)을 사용하여 피어를 인증하는 TCP 세션의 주소입니다.

NPTv6을 사용하는 경우 NPTv6이 느린 경로에서 수행되기 때문에 빠른 경로 트래픽의 성능에 영향을 줍니다.

NPTv6은 방화벽이 터널을 시작하고 종료하는 경우에만 IPSec IPv6에서 작동합니다. 원본 및/또는 대상 IPv6 주소가 수정되기 때문에 전송 IPSec 트래픽이 실패합니다. 패킷을 캡슐화하는 NAT 통과 기술을 사용하면 IPSec IPv6이 NPTv6과 함께 작동할 수 있습니다.

- 체크섬 중립 매핑
- 양방향 변환

- NPTv6 특정 서비스에 적용

체크섬 중립 매핑

방화벽이 수행하는 NPTv6 매핑 변환은 체크섬 중립적입니다. 즉, "... 표준 인터넷 체크섬 알고리즘[RFC 1071]을 사용하여 체크섬을 계산할 때 동일한 IPv6 의사 헤더 체크섬을 생성하는 IP 헤더가 생성됩니다. " 체크섬 중립 매핑에 대한 자세한 내용은 RFC 6296, 섹션 2.6을 참조하세요.

NPTv6을 사용하여 대상 NAT를 수행하는 경우, **테스트 nptv6** CLI 명령 구문에 방화벽 인터페이스의 내부 IPv6 주소와 외부 접두사/접두사 길이를 제공할 수 있습니다. CLI는 해당 대상에 도달하기 위해 NPTv6 구성에서 사용할 체크섬 중립, 공용 IPv6 주소로 응답합니다.

양방향 변환

NPTv6 정책 만들기일 때, 변환된 패킷 탭의 양방향 옵션은 방화벽이 구성한 변환의 반대 방향으로 해당 NAT 또는 NPTv6 변환을 생성하는 편리한 방법을 제공합니다. 기본설정으로, 양방향 변환이 미작동됩니다.

양방향 변환을 사용하도록 설정하는 경우, 양방향으로 트래픽을 제어할 수 있는 보안 정책이 있는지 확인하는 것이 매우 중요합니다. 이러한 정책이 없으면 양방향 기능을 사용하면 원하지 않을 수도 있는 양방향으로 패킷을 자동으로 변환할 수 있습니다.

특정 서비스에 적용된 NPTv6

NPTv6의 Palo Alto Networks 구현은 패킷을 필터링하여 변환 대상 패킷을 제한하는 기능을 제공합니다. NPTv6은 포트 변환을 수행하지 않습니다. NPTv6은 IPv6 접두사만 변환하므로 동적 IP 및 포트(Dynamic IP and Port, DIPP) 변환 개념이 없습니다. 그러나 특정 서비스 포트에 대한 패킷만 NPTv6 변환을 받도록 지정할 수 있습니다. 그렇게 하려면 NPTv6 정책 만들기 원래 패킷에 서비스를 지정합니다.

NDP 프록시

IPv6용 NDP(Neighbor Discovery Protocol)는 IPv4용 ARP(Address Resolution Protocol)에서 제공하는 기능과 유사한 기능을 수행합니다. RFC 4861은 IPv6(IP 버전 6)에 대한 Neighbor Discovery를 정의합니다. 호스트, 라우터 및 방화벽은 NDP를 사용하여 연결된 링크에 있는 이웃의 링크 계층 주소를 결정하고, 연결할 수 있는 이웃을 추적하고, 변경된 이웃의 링크 계층 주소를 업데이트합니다. 피어는 자신의 MAC 주소와 IPv6 주소를 알리고 피어로부터 주소를 요청하기도 합니다.

NDP는 노드가 노드를 대신하여 패킷을 전달할 수 있는 인접 디바이스가 있는 경우 프록시 개념도 지원합니다. 디바이스(방화벽)는 NDP Proxy의 역할을 수행합니다.

Palo Alto Networks® 방화벽은 인터페이스에서 NDP 및 NDP 프록시를 지원합니다. 주소에 대한 NDP 프록시로 작동하도록 방화벽을 구성하면 방화벽이 ND(Neighbor Discovery) 광고를 보내고 방화벽 뒤의 디바이스에 할당된 IPv6 접두사의 MAC 주소를 요청하는 피어의 ND 요청에 응답할 수 있습니다. 방화벽이 프록시 요청에 응답하지 않는 주소(부정 주소)를 구성할 수도 있습니다.

실제로 NDP는 기본적으로 활성화되어 있으며 다음과 같은 이유로 NPTv6을 구성할 때 NDP 프록시를 구성해야 합니다.

- NPTv6의 상태 비저장 특성에는 방화벽이 지정된 NDP 프록시 주소로 전송된 ND 패킷에 응답하고 부정된 NDP 프록시 주소에 응답하지 않도록 지시하는 방법이 필요합니다.

  ***NDP* 프록시는 방화벽이 방화벽 뒤에 있는 주소에 도달하지만 이웃은 방화벽 뒤에 있지 않다고 나타내므로 *NDP* 프록시 구성에서 이웃의 주소를 무효화하는 것이 좋습니다.**

- NDP는 방화벽이 ND 캐시에 이웃의 MAC 주소와 IPv6 주소를 저장하도록 합니다. (NPTv6 및 NDP 프록시 예제의 그림 참조) 방화벽은 ND 캐시에서 찾은 주소에 대해 NPTv6 변환을 수행하지 않습니다. 그렇게 하면 충돌이 발생할 수 있기 때문입니다. 캐시에 있는 주소의 호스트 부분이 이웃 주소의 호스트 부분과 겹치고 캐시의 접두사가 이웃과 동일한 접두사로 변환되는 경우(방화벽의 이그레스 인터페이스가 이웃과 동일한 서브넷)에는 이웃의 합법적인 IPv6 주소와 정확히 동일한 변환된 주소를 갖게 되며 충돌이 발생합니다. (ND 캐시의 주소에서 NPTv6 변환을 수행하려는 시도가 발생하면 정보 syslog 메시지가 이벤트를 기록합니다. `NPTv6 변환에 실패했습니다.`)

NDP 프록시가 활성화된 인터페이스가 IPv6 주소에 대한 MAC 주소를 요청하는 ND 요청을 수신하면 다음 시퀀스가 발생합니다.

- [ ] 방화벽은 ND 캐시를 검색하여 요청의 IPv6 주소가 없는지 확인합니다. 주소가 있으면 방화벽은 ND 요청을 무시합니다.
- [ ] 소스 IPv6 주소가 0이면 패킷이 중복 주소 감지 패킷이고 방화벽은 ND 요청을 무시합니다.
- [ ] 방화벽은 NDP 프록시 주소의 가장 긴 접두사 일치 검색을 수행하고 요청의 주소와 가장 일치하는 항목을 찾습니다. NDP 프록시 목록에서 일치 항목에 대한 부정 필드가 선택되면 방화벽은 ND 요청을 삭제합니다.
- [ ] 가장 긴 접두사 일치 검색이 일치하고 일치하는 주소가 부정되지 않은 경우에만 NDP 프록시가 ND 요청에 응답합니다. 방화벽은 ND 패킷으로 응답하여 쿼리 대상을 향한 다음 홉의 MAC 주소로 자체 MAC 주소를 제공합니다.

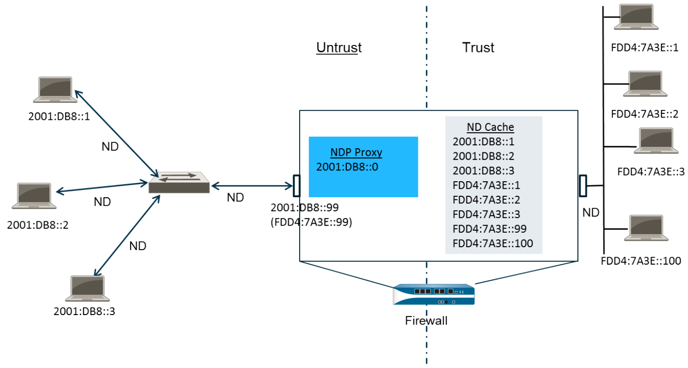
NDP를 성공적으로 지원하기 위해 방화벽은 다음에 대해 NDP Proxy를 수행하지 않습니다.

- 중복 주소 감지(DAD).

- ND 캐시의 주소(이러한 주소는 방화벽에 속하지 않고 검색된 이웃에 속하기 때문).

NPTv6 및 NDP 프록시 예제

다음 그림은 NPTv6와 NDP 프록시가 함께 작동하는 방법을 보여줍니다.



- NPTv6 예제 내 ND 캐시
- NPTv6 예제 내 NDP 프록시
- NPTv6 예제 내 NPTv6 번역
- ND 캐시의 인접 항목이 변환되지 않음

NPTv6 예제의 ND 캐시

위의 예에서 여러 피어는 스위치를 통해 방화벽에 연결하며 피어와 스위치 사이, 스위치와 방화벽 사이, 방화벽과 신뢰 측 디바이스 사이에서 ND가 발생합니다.

방화벽이 피어를 알게 되면 해당 주소를 ND 캐시에 저장합니다. 신뢰할 수 있는 피어 FDDA:7A3E::1, FDDA:7A3E::2 및 FDDA:7A3E::3은 트러스트 측의 방화벽에 연결됩니다. FDDA:7A3E::99는 방화벽 자체의 변환되지 않은 주소입니다. 공개 주소는 2001:DB8::99입니다. 신뢰할 수 없는 쪽의 피어 주소가 검색되어 ND 캐시에 나타납니다. 2001:DB8::1, 2001:DB8::2 및 2001:DB8::3.

NPTv6 예제의 NDP 프록시

이 시나리오에서는 방화벽이 방화벽 뒤에 있는 디바이스의 접두사에 대해 NDP 프록시 역할을 하기를 원합니다. 방화벽이 지정된 주소/범위/접두사 집합에 대한 NDP 프록시이고 ND 요청 또는 광고에서 이 범위의 주소를 확인하는 경우 해당 특정 주소를 가진 디바이스가 먼저 응답하지 않는 한 방화벽은 응답합니다. 주소는 NDP 프록시 구성에서 부정되지 않으며 주소는 ND 캐시에 없습니다. 방화벽은 접두사 변환(아래 설명)을 수행하고 해당 주소가 디바이스에 할당되거나 할당되지 않을 수 있는 트러스트 측으로 패킷을 보냅니다.

이 예에서 ND 프록시 테이블에는 네트워크 주소 2001:DB8::0이 포함되어 있습니다. 인터페이스가 2001:DB8::100에 대한 ND를 볼 때 L2 스위치의 다른 디바이스는 패킷을 요구하지 않으므로 프록시 범위로 인해 방화벽이 패킷을 요구하고 FDD4:7A3E::100으로 변환한 후 방화벽은 다음을 트러스트 측으로 내보냅니다.

NPTv6 예제의 NPTv6 변환

이 예에서 원본 패킷은 FDD4:7A3E::0의 소스 주소와 임의의 대상으로 구성됩니다. 변환된 패킷은 2001:DB8::0의 변환된 주소로 구성됩니다.

따라서 소스가 FDD4:7A3E::0인 나가는 패킷은 2001:DB8::0으로 변환됩니다. 네트워크 2001:DB8::0에서 대상 접두사가 있는 수신 패킷은 FDD4:7A3E::0으로 변환됩니다.

ND 캐시의 인접 항목이 변환되지 않음

이 예에서는 호스트 식별자 :1, :2 및 :3인 호스트가 방화벽 뒤에 있습니다. 해당 호스트의 접두사가 방화벽 너머에 있는 접두사로 변환되고 해당 디바이스에도 호스트 식별자 :1, :2 및 :3이 있는 경우 주소의 호스트 식별자 부분이 변경되지 않은 상태로 유지되기 때문에 변환된 결과 주소 기존 디바이스에 속하게 되며 주소 지정 충돌이 발생합니다. 겹치는 호스트 식별자와의 충돌을 피하기 위해 NPTv6은 ND 캐시를 찾은 주소를 변환하지 않습니다.

NPTv6 정책 만들기

하나의 IPv6 접두사를 다른 IPv6 접두사로 변환하도록 NAT NPTv6 정책을 구성하려는 경우 이 작업을 수행합니다. 이 작업의 전제 조건은 다음과 같습니다.

- IPv6을 사용하도록 설정합니다. 디바이스 > 설정 > 세션을 선택합니다. 편집을 클릭하고 **IPv6** 방화벽을 선택합니다.
- 유효한 IPv6 주소와 IPv6이 활성화된 레이어 3 이더넷 인터페이스를 구성합니다. 네트워크 > 인터페이스 > 이더넷을 선택하고, 인터페이스를 선택한 다음, **IPv6** 탭에서 인터페이스에서 **IPv6** 활성화를 선택합니다.
- NPTv6은 보안을 제공하지 않으므로 네트워크 보안 정책을 만드십시오.
- 소스 변환, 대상 변환 또는 둘 다를 원하는지 결정합니다.
- NPTv6 정책을 적용할 영역을 식별합니다.
- 원본 및 변환된 IPv6 접두사를 식별합니다.

STEP 1 | 새 NPTv6 정책을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 NPTv6 정책 규칙에 대한 설명이 포함된 이름을 입력합니다.
3. (선택 사항) 설명 및 태그를 입력합니다.
4. **NAT** 유형에 대해 **NPTv6**를 선택합니다.

STEP 2 | 들어오는 패킷에 대한 일치 기준을 지정합니다. 모든 기준과 일치하는 패킷은 NPTv6 변환 대상입니다.

두 가지 변환 유형 모두에 영역이 필요합니다.

1. 원본 패킷 탭에서 소스 영역에 대해 정책이 적용되는 임의 또는 추가를 그대로 둡니다.
2. 정책이 적용되는 대상 영역을 입력합니다.
3. (선택 사항) 대상 인터페이스를 선택합니다.
4. (선택 사항) 변환되는 패킷 유형을 제한하려면 서비스를 선택합니다.
5. 소스 변환을 수행하는 경우 소스 주소를 입력하거나 임의를 선택합니다. 주소는 주소 개체일 수 있습니다. 다음 제약 조건이 소스 주소 및 대상 주소에 적용됩니다.
   - 원본 패킷 및 변환된 패킷에 대한 소스 주소 및 대상 주소의 접두사는 xxxx:xxxx::/yy 형식이어야 하지만 접두사의 선행 0은 삭제할 수 있습니다.
   - IPv6 주소는 인터페이스 식별자(호스트) 부분을 정의할 수 없습니다.
   - 지원되는 접두사 길이의 범위는 /32 ~ /64입니다.
   - 소스 주소와 대상 주소는 모두 모두로 설정할 수 없습니다.
6. 소스 변환을 수행하는 경우 선택적으로 대상 주소를 입력할 수 있습니다. 대상 변환을 수행하는 경우 대상 주소가 필요합니다. 대상 주소(주소 개체가 허용됨)는 범위가 아니라 IPv6 주소뿐 아니라 넷마스크여야 합니다. 접두사 길이는 /32에서 /64(포함) 사이의 값이어야 합니다. 예를 들어, 2001:db8::/32입니다.

STEP 3 | 변환된 패킷을 지정합니다.

1. 변환된 패킷 탭에서 소스 변환을 수행하려면 소스 주소 변환 섹션에서 변환 유형에 대해 정적 **IP**를 선택합니다. 원본 변환을 수행하지 않으려면 없음을 선택합니다.
2. 정적 **IP**를 선택한 경우 변환된 주소 필드가 나타납니다. 변환된 IPv6 접두사 또는 주소 개체를 입력합니다. 이전 단계에 나열된 제약 조건을 참조하십시오.

   변환된 주소를 방화벽의 신뢰할 수 없는 인터페이스 주소의 접두사로 구성하는 것이 가장 좋습니다. 예를 들어, 신뢰할 수 없는 인터페이스의 주소가 *2001:1a:1b:1::99/64*인 경우 변환된 주소를 *2001:1a:1b:1::0/64*로 만드십시오.
3. (선택 사항) 방화벽이 구성한 변환의 반대 방향으로 해당 NPTv6 변환을 생성하도록 하려면 양방향을 선택합니다.

   양방향 변환을 사용하는 경우 양방향 트래픽을 제어하기 위한 보안 정책 규칙이 있는지 확인하는 것이 매우 중요합니다. 이러한 정책 규칙이 없으면 양방향 변환을 통해 패킷이 자동으로 양방향으로 변환될 수 있으며 이는 원하지 않을 수 있습니다.
4. 목적지 변환을 하려면 목적지 주소 변환을 선택하십시오. 변환된 주소 필드에서 주소 개체를 선택하거나 내부 대상 주소를 입력합니다.
5. 확인을 클릭합니다.

STEP 4 | NDP 프록시를 구성합니다.

주소에 대한 NDP 프록시로 작동하도록 방화벽을 구성하면 방화벽이 ND(Neighbor Discovery) 광고를 보내고 방화벽 뒤의 디바이스에 할당된 IPv6 접두사의 MAC 주소를 요청하는 피어의 ND 요청에 응답할 수 있습니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 인터페이스를 선택합니다.
2. 고급 > **NDP** 프록시 탭에서 **NDP** 프록시 사용을 선택하고 추가를 클릭합니다.
3. NDP 프록시가 활성화된 **IP** 주소를 입력합니다. 주소, 주소 범위 또는 접두어 및 접두어 길이가 될 수 있습니다. IP 주소의 순서는 중요하지 않습니다. 이러한 주소는 NPTv6 정책에서 구성한 변환된 주소와 이상적으로 동일합니다.

   주소가 서브넷인 경우 *NDP* 프록시는 서브넷의 모든 주소에 응답하므로 다음 단계에 설명된 대로 부정이 선택된 서브넷의 이웃을 나열해야 합니다.
4. (선택 사항) NDP 프록시를 사용하지 않으려는 주소를 하나 이상 입력하고 부정을 선택합니다. 예를 들어, 이전 단계에서 구성된 IP 주소 범위 또는 접두사 범위에서 주소의 더 작은 하위 집합을 무효화할 수 있습니다. 방화벽의 이웃 주소를 부정하는 것이 좋습니다.

STEP 5 | 구성을 커밋합니다.

확인 및 커밋을 클릭합니다.

NAT64

NAT64는 IPv4 네트워크와 통신해야 하는 동안 IPv6으로 변환하는 방법을 제공합니다. IPv6 전용 네트워크에서 IPv4 네트워크로 통신해야 하는 경우 NAT64를 사용하여 소스 및 대상 주소를 IPv6에서 IPv4로 또는 그 반대로 변환합니다. NAT64를 사용하면 IPv6 클라이언트가 IPv4 서버에 액세스할 수 있고 IPv4 클라이언트가 IPv6 서버에 액세스할 수 있습니다. NAT64를 구성하기 전에 NAT를 이해해야 합니다.

NAT64 개요

Palo Alto Networks® 방화벽에서 두 가지 유형의 NAT64 변환을 구성할 수 있습니다. 각각은 두 IP 주소 패밀리 간에 양방향 변환을 수행합니다.

- 방화벽은 여러 IPv6 주소를 하나의 IPv4 주소에 매핑하여 IPv4 주소를 보존하는 상태 저장 IPv6 시작 통신 NAT64를 지원합니다. (하나의 IPv6 주소를 하나의 IPv4 주소에 매핑하므로 IPv4 주소를 보존하지 않는 상태 비저장 NAT64를 지원하지 않습니다.)IPv6 시작 통신을 위한 NAT64 구성 .
- 방화벽은 IPv4 주소 및 포트 번호를 IPv6 주소에 매핑하는 정적 바인딩을 사용하여 IPv4 시작 통신을 지원합니다. IPv4 시작 통신을 위한 NAT64 구성. 또한 IPv4 주소 및 포트 번호를 여러 포트 번호가 있는 IPv6 주소로 변환하여 더 많은 IPv4 주소를 보존하는 포트 다시 쓰기도 지원합니다. 포트 변환을 사용하여 IPv4 시작 통신을 위한 NAT64 구성.

단일 IPv4 주소는 NAT44 및 NAT64에 사용할 수 있으며, NAT64 전용 IPv4 주소 풀을 예약하지 않습니다.

NAT64는 레이어 3 인터페이스, 하위 인터페이스 및 터널 인터페이스에서 작동합니다. IPv6 시작 통신을 위해 Palo Alto Networks 방화벽에서 NAT64를 사용하려면 NAT 기능에서 DNS 쿼리 기능을 분리할 수 있는 제삼자 DNS64 서버 또는 솔루션이 있어야 합니다. DNS64 서버는 공용 DNS 서버에서 받는 IPv4 주소를 IPv6 호스트의 IPv6 주소로 인코딩하여 IPv6 호스트와 IPv4 DNS 서버 사이에서 변환합니다.

Palo Alto Networks는 다음 NAT64 기능을 지원합니다.

- 헤어피닝 (NAT U-Turn), 또한 NAT64 은 소스 접두사가 64::/n인 들어오는 모든 IPv6 패킷을 삭제하여 헤어핀 루프 공격을 방지합니다.
- RFC 6146 및 방화벽에 따른 TCP/UDP/ICMP 패킷 변환은 ALG(응용 수준 게이트웨이)를 사용하지 않는 다른 프로토콜을 변환하기 위해 최선을 다합니다. 예를 들어 방화벽은 GRE 패킷을 변환할 수 있습니다. 이 변환에는 NAT44와 동일한 제한이 있습니다. 별도의 제어 및 데이터 채널을 사용할 수 있는 프로토콜에 대한 ALG가 없으면 방화벽이 반환 트래픽 흐름을 이해하지 못할 수 있습니다.
- RFC 4884에 따른 원래 데이터그램 필드의 ICMP 길이 속성에 대한 IPv4와 IPv6 간의 변환입니다.

IPv4 포함 IPv6 주소

NAT64는 RFC 6052, IPv4/IPv6 변환기의 IPv6 주소 지정에 설명된 대로 IPv4 포함 IPv6 주소를 사용합니다. IPv4 포함 IPv6 주소는 32비트에 IPv4 주소가 인코딩된 IPv6 주소입니다. IPv6 접두사 길이(그림의 PL)는 다음과 같이 IPv6 주소에서 IPv4 주소가 인코딩되는 위치를 결정합니다.

```
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| PL | 0--------------------32----40----48----56-----64----72----80----88----96----104---------------|
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 32 |       prefix        | v4(32)                  |  u  |  suffix                                 |
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 40 |       prefix              | v4(24)            |  u  | (8)  | suffix                           |
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 48 |       prefix                    | v4(16)      |  u  |  (16)     | suffix                      |
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 56 |       prefix                          | v4(8) |  u  |    v4(24)       | suffix                |
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 64 |       prefix                                  |  u  |       v4(32)          | suffix          |
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 96 |       prefix                                                          | v4(32)                |
+--+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

방화벽은 이러한 접두사를 사용하여 /32, /40, /48, /56, /64 및 /96 서브넷에 대한 변환을 지원합니다. 단일 방화벽은 여러 접두사를 지원합니다. 각 NAT64 규칙은 하나의 접두사를 사용합니다. 접두사는 Well-Known Prefix(64:FF9B::/96) 또는 주소 변환기(DNS64 디바이스)를 제어하는 조직에 고유한 NSP(Network-Specific Prefix)일 수 있습니다. NSP는 일반적으로 조직의 IPv6 접두사 내의 네트워크입니다. DNS64 디바이스는 일반적으로 u 필드와 접미사를 0으로 설정합니다. 방화벽은 해당 필드를 무시합니다.

DNS64 서버

DNS를 사용해야 하고 IPv6에서 시작된 통신을 사용하여 NAT64 변환을 수행하려면 잘 알려진 접두사 또는 NSP로 설정된 타사 DNS64 서버 또는 기타 DNS64 솔루션을 사용해야 합니다. IPv6 호스트가 인터넷에서 IPv4 호스트 또는 도메인에 액세스하려고 하면 DNS64 서버는 해당 호스트 이름에 매핑된 IPv4 주소에 대한 신뢰할 수 있는 DNS 서버를 쿼리합니다. DNS 서버는 주소 레코드(A 레코드)를 호스트 이름에 대한 IPv4 주소가 포함된 DNS64 서버에 반환합니다.

DNS64 서버는 IPv4 주소를 육각형으로 변환하고 IPv6 접두사(잘 알려진 접두사 또는 NSP)의 적절한 옥텟으로 인코딩하여 접두사 길이에 따라 사용하도록 설정되어 있으며, 이로 인해 IPv4-Embedded IPv6 주소가 생성됩니다. DNS64 서버는 IPv4 임베디드 IPv6 주소를 IPv4 호스트 이름으로 매핑하는 IPv6 호스트에 AAAA 레코드를 보냅니다.

경로 MTU 검색

IPv6은 패킷을 조각화하지 않으므로 방화벽은 패킷 조각화 필요성을 줄이기 위해 두 가지 방법을 사용합니다.

- 방화벽이 DF(조각화하지 않음) 비트가 0인 IPv4 패킷을 변환할 때 이는 보낸 사람이 방화벽이 너무 큰 패킷을 조각화할 것으로 예상하지만 방화벽이 IPv6 네트워크에 대한 패킷을 조각화하지 않음을 나타내는데(전송 이후) IPv6은 패킷을 조각화하지 않기 때문입니다. 대신 방화벽이 IPv4 패킷을 변환하기 전에 조각화하는 최소 크기를 구성할 수 있습니다. **NAT64 IPv6** 최소 네트워크 **MTU** 값은 이 설정에서 RFC 6145, IP/ICMP 변환 알고리즘을 준수합니다. **NAT64 IPv6** 최소 네트워크 **MTU**를 최대값(디바이스 > 설정 > 세션)으로 설정하면 방화벽이 IPv4 패킷을 IPv6으로 변환하기 전에 IPv6 최소 크기로 조각화할 수 있습니다. (**NAT64 IPv6** 최소 네트워크 **MTU**는 인터페이스 MTU를 변경하지 않습니다.)
- 방화벽이 단편화를 줄이기 위해 사용하는 다른 방법은 경로 MTU 검색(Path MTU Discovery, PMTUD)입니다. IPv4 시작 통신에서 변환할 IPv4 패킷에 DF 비트가 설정되어 있고 송신 인터페이스의 MTU가 패킷보다 작은 경우 방화벽은 PMTUD를 사용하여 패킷을 삭제하고 ICMP 'Destination Unreachable - fragmentation required'를 반환합니다. ' 메시지를 소스로 보냅니다. 소스는 해당 대상에 대한 경로 MTU를 낮추고 경로 MTU의 연속적인 감소가 패킷 전달을 허용할 때까지 패킷을 재전송합니다.

IPv6 시작 통신

방화벽에 대한 IPv6 시작 통신은 IPv4 토폴로지의 소스 NAT와 유사합니다. IPv6 호스트가 IPv4 서버와 통신해야 하는 경우 IPv6 시작 통신에 대해 NAT64를 구성합니다.

NAT64 정책 규칙에서 원래 소스를 IPv6 호스트 주소 또는 Any로 구성합니다. 대상 IPv6 주소를 Well-Known Prefix 또는 DNS64 서버가 사용하는 NSP로 구성합니다. (규칙에서 전체 IPv6 대상 주소를 구성하지 않습니다.)

DNS를 사용해야 하는 경우 DNS64 서버를 사용하여 IPv4 DNS "A" 결과를 NAT64 접두사와 병합된 "AAAA" 결과로 변환해야 합니다. DNS를 사용하지 않는 경우 RFC 6052 규칙에 따라 방화벽에 구성된 IPv4 대상 주소와 NAT64 접두사를 사용하여 주소를 생성해야 합니다.

DNS를 사용하는 환경의 경우 아래 토폴로지 예는 DNS64 서버와의 통신을 보여줍니다. DNS64 서버는 잘 알려진 접두사 64:FF9B::/96나 RFC 6052(/32, /40,/48,/56,/64 또는 /96)에 준수하는 네트워크 특정 접두사를 사용하도록 설정되어야 합니다.

방화벽의 변환된 쪽에서 변환 유형은 Stateful NAT64를 구현하기 위한 동적 IP 및 포트여야 합니다. 소스 변환 주소를 방화벽에서 송신 인터페이스의 IPv4 주소로 구성합니다. 데스티네이션 변환 필드를 구성하지 않습니다. 방화벽은 먼저 규칙의 원래 대상 주소에서 접두사 길이를 찾은 다음 접두사를 기반으로 수신 패킷의 원래 대상 IPv6 주소에서 인코딩된 IPv4 주소를 추출하여 주소를 변환합니다.

방화벽은 NAT64 규칙을 확인하기 전에 들어오는 패킷의 데스티네이션 보안 영역을 찾기 위해 경로 조회를 수행해야 합니다. NAT64 접두사는 방화벽에서 라우팅할 수 없어야 하므로 데스티네이션 영역 할당을 통해 NAT64 접두사에 도달할 수 있는지 확인해야 합니다. 방화벽은 NAT64 접두사를 기본 경로에 할당하거나 경로가 없기 때문에 NAT64 접두사를 삭제합니다. NAT64 접두사가 송신 인터페이스 및 영역과 연결된 라우팅 테이블에 없기 때문에 방화벽은 데스티네이션 영역을 찾지 못합니다.

또한 터널 인터페이스를 구성해야 합니다(종료 지점 없음). NAT64 접두사를 터널에 적용하고 적절한 영역을 적용하여 NAT64 접두사가 있는 IPv6 트래픽이 적절한 대상 영역에 할당되도록 합니다. 또한 터널은 트래픽이 NAT64 규칙과 일치하지 않는 경우 NAT64 접두사가 있는 IPv6 트래픽을 삭제하는 이점이 있습니다. 방화벽에 구성된 라우팅 프로토콜은 라우팅 테이블에서 IPv6 접두사를 검색하여 데스티네이션 영역을 찾은 다음 NAT64 규칙을 확인합니다.

다음 그림은 이름 확인 프로세스에서 DNS64 서버의 역할을 보여줍니다. 이 예에서 DNS64 서버는 Well-Known Prefix 64:FF9B::/96을 사용하도록 구성되어 있습니다.

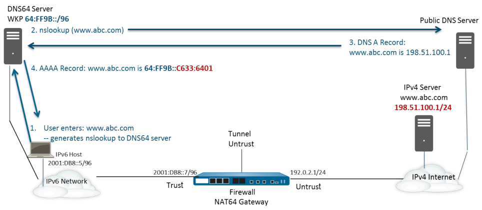
1. IPv6 호스트의 사용자는 DNS64 서버에 대한 이름 서버 조회(nslookup)를 생성하는 URL www.abc.com을 입력합니다.

2. DNS64 서버는 nslookup을 www.abc.com의 공용 DNS 서버로 보내 IPv4 주소를 요청합니다.

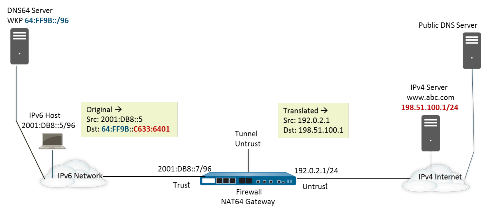
3. DNS 서버는 DNS64 서버에 IPv4 주소를 제공하는 A 레코드를 반환합니다.

4. DNS64 서버는 IPv6 사용자에게 AAAA 레코드를 보내 IPv4 점으로 구분된 10진수 주소 198.51.100.1을 C633:6401 16진수로 변환하고 자체 IPv6 접두사인 64:FF9B::/96에 포함시킵니다. [198 = C6 16진수; 51 = 33 16진수; 100 = 64 16진수; 1 = 01 16진수.] 결과는 IPv4 포함 IPv6 주소 64:FF9B::C633:6401입니다.

/96 접두사에서 IPv4 주소는 IPv6 주소로 인코딩된 마지막 4개의 옥텟입니다. DNS64 서버가 /32, /40, /48, /56 또는 /64 접두사를 사용하는 경우 IPv4 주소는 RFC 6052에 표시된 대로 인코딩됩니다.



트랜스페어런트 이름 확인 시 IPv6 호스트는 DNS64 서버에 의해 결정된 IPv6 소스 주소 및 대상 IPv6 주소 64:FF9B::C633:6401이 포함된 패킷을 방화벽으로 보냅니다. 방화벽은 NAT64 규칙에 따라 NAT64 변환을 수행합니다.



IPv6 시작 통신을 위한 NAT64 구성

이 구성 작업 및 해당 주소는 IPv6 시작 통신의 수치에 해당합니다.

STEP 1 | 방화벽에서 작동하도록 IPv6을 활성화합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. **IPv6** 방화벽 사용을 선택합니다.
3. 확인을 클릭합니다.

STEP 2 | IPv6 대상 주소에 대한 주소 개체를 만듭니다(사전 변환).

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름(예: NAT64-IPv4 서버)을 입력합니다.
3. 유형 에서 **IP** 넷마스크를 선택하고 RFC 6052(/32, /40, /48, /56, /64 또는 /96) 와 호환되는 넷마스크를 사용하여 IPv6 접두사를 입력합니다. 잘 알려진 접두사 또는 DNS64 서버에 구성된 네트워크별 접두사입니다.

   이 예에서는 64:FF9B::/96을 입력합니다.

   소스와 대상의 넷마스크**(**접두사 길이**)**가 같아야 합니다**.**

   방화벽은 접두사 길이에 따라 수신 패킷의 원래 대상 IPv6 주소에서 인코딩된 IPv4 주소를 추출하기 때문에 전체 대상 주소를 입력하지 않습니다. 이 예에서 수신 패킷의 접두사는 16진수로 된 C 633:6401(IPv4 대상 주소 198.51.100.1)으로 인코딩됩니다.
4. 확인을 클릭합니다.

STEP 3 | (선택 사항) IPv6 소스 주소에 대한 주소 개체를 만듭니다(사전 변환).

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름을 입력합니다.
3. 유형에서 **IP** 넷마스크를 선택하고 IPv6 호스트의 주소(이 예에서는 2001:DB8::5/96)를 입력합니다.
4. 확인을 클릭합니다.

STEP 4 | (선택 사항) IPv4 소스 주소에 대한 주소 개체를 만듭니다(변환됨).

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름을 입력합니다.
3. 유형에서 **IP** 넷마스크를 선택하고 방화벽 이그레스 인터페이스의 IPv4 주소(이 예에서는 192.0.2.1)를 입력합니다.
4. 확인을 클릭합니다.

STEP 5 | NAT64 규칙을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 NAT64 규칙의 이름(예: nat64_ipv6_init)을 입력합니다.
3. (선택 사항) 설명을 입력합니다.
4. **NAT** 유형에 대해 **nat64**를 선택합니다.

STEP 6 | 원본 소스 및 대상 정보를 지정합니다.

1. 원본 패킷의 경우 신뢰할 수 있는 영역인 소스 영역을 추가합니다.
2. 대상 영역(이 예에서는 Untrust 영역)을 선택합니다.
3. (선택 사항) 대상 인터페이스 또는 기본값(임의)을 선택합니다.
4. 소스 주소에 대해 임의 또는 IPv6 호스트에 대해 생성한 주소 개체 추가를 선택합니다.
5. 대상 주소에 대해 IPv6 대상 주소에 대해 생성한 주소 개체를 추가합니다(이 예에서는 NAT64-IPv4 서버).
6. (선택 사항) 서비스에서 임의를 선택합니다.

STEP 7 | 변환된 패킷 정보를 지정합니다.

1. 변환된 패킷의 경우 소스 주소 변환의 변환 유형에서 동적 **IP** 및 포트를 선택합니다.
2. 주소 유형에서 다음 중 하나를 수행합니다.
   - 변환된 주소를 선택하고 IPv4 소스 주소에 대해 생성한 주소 개체를 추가합니다.
   - 인터페이스 주소를 선택합니다. 이 경우 변환된 소스 주소는 방화벽 이그레스 인터페이스의 IP 주소 및 넷마스크입니다. 이 선택의 경우 인터페이스를 선택하고 인터페이스에 둘 이상의 IP 주소가 있는 경우 선택적으로 **IP** 주소를 선택합니다.
3. 대상 주소 변환을 선택하지 않은 상태로 둡니다. (방화벽은 NAT64 규칙의 원래 대상에 지정된 접두사 길이를 기반으로 수신 패킷의 IPv6 접두사에서 IPv4 주소를 추출합니다.)
4. 확인을 클릭하여 NAT64 정책 규칙을 저장합니다.

STEP 8 | 128 이외의 넷마스크를 사용하여 루프백 인터페이스를 에뮬레이트하도록 터널 인터페이스를 구성합니다.

1. 네트워크 > 인터페이스 > 터널을 선택하고 터널 추가를 선택합니다.
2. 인터페이스 이름에 숫자 접미사(예: .2)를 입력합니다.
3. 구성 탭에서 NAT64 구성 중인 가상 라우터를 선택합니다.
4. 보안 영역에서 IPv4 서버 대상(신뢰 영역)과 연결된 대상 영역을 선택합니다.
5. **IPv6** 탭에서 인터페이스에서 **IPv6** 사용을 선택합니다.
6. 추가를 클릭하고 주소에 대해 새 주소를 선택합니다.
7. 주소의 이름을 입력합니다.
8. (선택 사항) 터널 주소에 대한 설명을 입력합니다.
9. 유형에서 **IP** 넷마스크를 선택하고 IPv6 접두사 및 접두사 길이를 입력합니다(이 예에서는 64:FF9B::/96).
10. 확인을 클릭합니다.
11. 인터페이스에서 주소 활성화를 선택하고 확인을 클릭합니다.
12. 확인을 클릭합니다.
13. 확인을 클릭하여 터널을 저장합니다.

STEP 9 | 신뢰 영역의 NAT 트래픽을 허용하는 보안 정책을 만듭니다.

1. 정책 > 보안 및 규칙 이름 추가를 선택합니다.
2. 소스를 선택하고 소스 영역을 추가한 후 신뢰를 선택합니다.
3. 소스 주소에 대해 임의를 선택합니다.
4. 대상을 선택하고 대상 영역을 추가합니다. 신뢰하지 않음을 선택합니다.
5. 애플리케이션에 임의를 선택합니다.
6. 작업에 대해 허용을 선택합니다.
7. 확인을 클릭합니다.

STEP 10 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

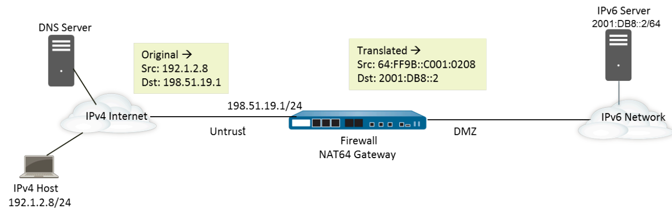
STEP 11 | NAT64 세션의 문제를 해결하거나 봅니다.

```
> show session id <session-id>
```

IPv4 시작 통신을 위한 NAT64 구성

IPv6 서버에 대한 IPv4 시작 통신은 IPv4 토폴로지의 대상 NAT와 유사합니다. 대상 IPv4 주소는 일대일 정적 IP 변환(다대일 변환 아님)을 통해 대상 IPv6 주소에 매ping됩니다.

방화벽은 소스 IPv4 주소를 RFC 6052에 정의된 Well-Known Prefix 64:FF9B::/96으로 인코딩합니다. 변환된 대상 주소는 실제 IPv6 주소입니다. IPv4 시작 통신의 사용 사례는 일반적으로 조직이 공개, 비신뢰 영역에서 조직의 DMZ 영역에 있는 IPv6 서버에 대한 액세스를 제공할 때입니다. 이 토폴로지는 DNS64 서버를 사용하지 않습니다.



STEP 1 | 방화벽에서 작동하도록 IPv6을 활성화합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. **IPv6** 방화벽 사용을 선택합니다.
3. 확인을 클릭합니다.

STEP 2 | (선택 사항) IPv4 패킷의 DF 비트가 0으로 설정된 경우(IPv6는 패킷을 프래그먼트하지 않으므로) 변환된 IPv6 패킷이 대상 IPv6 네트워크의 경로 MTU를 초과하지 않는지 확인합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. **NAT64 IPv6** 최소 네트워크 **MTU**의 경우 방화벽이 IPv6로 변환하기 위해 IPv4 패킷을 프래그먼트화할 최소 바이트 수를 입력합니다(범위는 1280-9216, 기본값은 1280).

   변환 전에 방화벽이 *IPv4* 패킷을 프래그먼트하지 않도록 하려면 *MTU*를 *9216*으로 설정합니다. 변환된 *IPv6* 패킷이 여전히 이 값을 초과하면 방화벽은 패킷을 삭제하고 대상에 연결할 수 없음을 나타내는 *ICMP* 패킷을 발행합니다.
3. 확인을 클릭합니다.

STEP 3 | IPv4 대상 주소에 대한 주소 개체를 만듭니다(사전 변환).

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름을 입력합니다(예: nat64_ip4server).
3. 유형에 대해 **IP Netmask**를 선택하고 Untrust 영역에 방화벽 인터페이스의 IPv4 주소를 입력합니다. 주소는 넷마스크를 사용하지 않거나 /32의 넷마스크만 사용해야 합니다. 이 예에서는 198.51.19.1/32를 사용합니다.
4. 확인을 클릭합니다.

STEP 4 | IPv6 소스 주소(변환됨)에 대한 주소 개체를 만듭니다.

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름(예: nat64_ip6source)을 입력합니다.
3. 유형에서 **IP** 넷마스크를 선택하고 RFC 6052(/32, /40, /48, /56, /64 또는 /96)와 호환되는 넷마스크를 사용하여 NAT64 IPv6 주소를 입력합니다.

   이 예에서는 64:FF9B::/96을 입력합니다.

   (방화벽은 IPv4 소스 주소 192.1.2.8로 접두사를 인코딩합니다. 이는 16진수로 C001:0208입니다.)
4. 확인을 클릭합니다.

STEP 5 | IPv6 대상 주소(변환됨)에 대한 주소 개체를 만듭니다.

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름(예: nat64_server_2)을 입력합니다.
3. 유형에서 **IP** 넷마스크를 선택하고 IPv6 서버(대상) 의 IPv6 주소를 입력합니다. 주소는 넷마스크를 사용하지 않거나 /128의 넷마스크만 사용해야 합니다. 이 예에서는 2001:DB8::2/128을 사용합니다.
4. 확인을 클릭합니다.

STEP 6 | NAT64 규칙을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 NAT64 규칙의 이름(예: nat64_ipv4_init)을 입력합니다.
3. **NAT** 유형에 대해 **nat64**를 선택합니다.

STEP 7 | 원본 소스 및 대상 정보를 지정합니다.

1. 원본 패킷의 경우 신뢰할 수 없는 영역인 소스 영역을 추가합니다.
2. 대상 영역(예: 트러스트 또는 DMZ 영역)을 선택합니다.
3. 소스 주소에 대해 임의 또는 IPv4 호스트의 주소 개체 추가를 선택합니다.
4. 대상 주소에 대해 IPv4 대상의 주소 개체(이 예에서는 nat64_ip4server)를 추가합니다.
5. 서비스에 대해 임의를 선택합니다.

STEP 8 | 변환된 패킷 정보를 지정합니다.

1. 변환된 패킷의 경우 소스 주소 변환, 변환 유형에서 정적 **IP**를 선택합니다.
2. 변환된 주소에 대해 생성한 소스 변환된 주소 개체인 nat64_ip6source를 선택합니다.
3. 대상 주소 변환의 경우 변환된 주소에 대해 단일 IPv6 주소(이 예에서는 주소 개체(이 예에서는 nat64_server_2 또는 서버의 IPv6 주소)를 지정합니다.
4. 확인을 클릭합니다.

STEP 9 | Untrust 영역의 NAT 트래픽을 허용하는 보안 정책을 만듭니다.

1. 정책 > 보안 및 규칙 이름 추가를 선택합니다.
2. 소스를 선택하고 소스 영역을 추가합니다. 신뢰하지 않음을 선택합니다.
3. 소스 주소에 대해 임의를 선택합니다.
4. 대상을 선택하고 대상 영역을 추가합니다. **DMZ**를 선택합니다.
5. 작업에 대해 허용을 선택합니다.
6. 확인을 클릭합니다.

STEP 10 | 변경 사항을 커밋합니다.

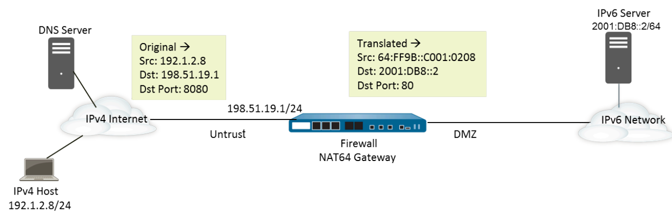
커밋을 클릭합니다.

STEP 11 | NAT64 세션의 문제를 해결하거나 봅니다.

```
> show session id <session-id>
```


포트 변환을 사용하여 IPv4 시작 통신을 위한 NAT64 구성

이 작업은 IPv4 시작 통신을 위한 NAT64 구성 작업을 기반으로 하지만 IPv6 네트워크를 제어하는 조직은 공용 대상 포트 번호를 내부 대상 포트 번호로 변환하여 방화벽의 IPv4 비신뢰 측의 사용자에게 비공개로 유지하는 것을 선호합니다. 이 예에서 포트 8080은 포트 80으로 변환됩니다. 이를 위해 NAT64 정책 규칙의 원본 패킷에서 대상 포트를 8080으로 지정하는 새 서비스를 생성합니다. 변환된 패킷의 경우 변환된 포트는 80입니다.



STEP 1 | 방화벽에서 작동하도록 IPv6을 활성화합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. **IPv6** 방화벽 사용을 선택합니다.
3. 확인을 클릭합니다.

STEP 2 | (선택 사항) IPv4 패킷의 DF 비트가 0으로 설정된 경우(IPv6는 패킷을 프래그먼트하지 않으므로) 변환된 IPv6 패킷이 대상 IPv6 네트워크의 경로 MTU를 초과하지 않는지 확인합니다.

1. 디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.
2. **NAT64 IPv6** 최소 네트워크 **MTU**의 경우 방화벽이 IPv6로 변환하기 위해 IPv4 패킷을 프래그먼트화하는 최소 바이트 수를 입력합니다(범위는 1280-9216, 기본값은 1280).

   변환 전에 방화벽이 *IPv4* 패킷을 프래그먼트하지 않도록 하려면 *MTU*를 *9216*으로 설정합니다. 변환된 *IPv6* 패킷이 여전히 이 값을 초과하면 방화벽은 패킷을 삭제하고 대상에 연결할 수 없음을 나타내는 *ICMP* 패킷을 발행합니다.
3. 확인을 클릭합니다.

STEP 3 | IPv4 대상 주소에 대한 주소 개체를 만듭니다(사전 변환).

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름을 입력합니다(예: nat64_ip4server).
3. 유형에서 **IP** 넷마스크를 선택하고 Untrust 영역에 있는 방화벽 인터페이스의 IPv4 주소 및 넷마스크를 입력합니다. 이 예에서는 198.51.19.1/24를 사용합니다.
4. 확인을 클릭합니다.

STEP 4 | IPv6 소스 주소(변환됨)에 대한 주소 개체를 만듭니다.

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름(예: nat64_ip6source)을 입력합니다.
3. 유형에서 **IP** 넷마스크를 선택하고 RFC 6052(/32, /40, /48, /56, /64 또는 /96)와 호환되는 넷마스크를 사용하여 NAT64 IPv6 주소를 입력합니다.

   이 예에서는 64:FF9B::/96을 입력합니다.

   (방화벽은 IPv4 소스 주소 192.1.2.8로 접두사를 인코딩합니다. 이는 16진수로 C001:0208입니다.)
4. 확인을 클릭합니다.

STEP 5 | IPv6 대상 주소(변환됨)에 대한 주소 개체를 만듭니다.

1. 개체 > 주소를 선택하고 추가를 클릭합니다.
2. 개체의 이름(예: nat64_server_2)을 입력합니다.
3. 유형에서 **IP** 넷마스크를 선택하고 IPv6 서버(대상) 의 IPv6 주소를 입력합니다. 이 예에서는 2001:DB8::2/64를 사용합니다.

   소스와 대상의 넷마스크(접두사 길이)가 같아야 합니다.
4. 확인을 클릭합니다.

STEP 6 | NAT64 규칙을 만듭니다.

1. 정책 > **NAT**을 선택하고 추가를 클릭합니다.
2. 일반 탭에서 NAT64 규칙의 이름(예: nat64_ipv4_init)을 입력합니다.
3. **NAT** 유형에 대해 **nat64**를 선택합니다.

STEP 7 | 원본 소스 및 대상 정보를 지정하고 변환을 단일 수신 포트 번호로 제한하는 서비스를 만듭니다.

1. 원본 패킷의 경우 신뢰할 수 없는 영역인 소스 영역을 추가합니다.
2. 대상 영역(예: 트러스트 또는 DMZ 영역)을 선택합니다.
3. 서비스에 대해 새 서비스를 선택합니다.
4. 서비스 이름(예: Port_8080)을 입력합니다.
5. 프로토콜로 **TCP**를 선택합니다.
6. 대상 포트에 8080을 입력합니다.
7. 확인을 클릭하여 서비스를 저장합니다.
8. 소스 주소에 대해 임의 또는 IPv4 호스트의 주소 개체 추가를 선택합니다.
9. 대상 주소에 대해 IPv4 대상의 주소 개체(이 예에서는 nat64_ip4server)를 추가합니다.

STEP 8 | 변환된 패킷 정보를 지정합니다.

1. 변환된 패킷의 경우 소스 주소 변환, 변환 유형에서 정적 **IP**를 선택합니다.
2. 변환된 주소에 대해 생성한 소스 변환된 주소 개체인 nat64_ip6source를 선택합니다.
3. 대상 주소 변환의 경우 변환된 주소에 대해 단일 IPv6 주소(이 예에서는 주소 개체(이 예에서는 nat64_server_2 또는 서버의 IPv6 주소)를 지정합니다.
4. 방화벽이 공용 대상 포트 번호를 변환하는 개인 대상 변환된 포트 번호(이 예에서는 80)를 지정합니다.
5. 확인을 클릭합니다.

STEP 9 | Untrust 영역의 NAT 트래픽을 허용하는 보안 정책을 만듭니다.

1. 정책 > 보안 및 규칙 이름 추가를 선택합니다.
2. 소스를 선택하고 소스 영역을 추가합니다. 신뢰하지 않음을 선택합니다.
3. 소스 주소에 대해 임의를 선택합니다.
4. 대상을 선택하고 대상 영역을 추가합니다. **DMZ**를 선택합니다.
5. 작업에 대해 허용을 선택합니다.
6. 확인을 클릭합니다.

STEP 10 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

STEP 11 | NAT64 세션의 문제를 해결하거나 봅니다.

```
> show session id <session-id>
```

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 전달 테이블에 추가합니다. 선택한 경로에 정전이 발생하지 않는 한 다른 경로를 사용하지 않습니다.

가상 라우터에서 ECMP 기능을 활성화하면 방화벽이 전달 테이블의 대상에 대해 최대 4개의 동일한 비용 경로를 가질 수 있으므로 방화벽이 다음을 수행할 수 있습니다.

- 로드 밸런싱 흐름(세션)은 여러 동일한 비용 링크를 통해 동일한 대상으로 이동합니다.
- 일부 링크를 사용하지 않은 상태로 두지 않고 동일한 대상에 대한 링크에서 사용 가능한 모든 대역폭을 효율적으로 사용합니다.
- 라우팅 프로토콜 또는 RIB 테이블이 대체 경로/경로를 선택할 때까지 기다릴 필요 없이 링크가 실패할 경우 다른 ECMP 구성원에 대한 트래픽을 동일한 대상으로 동적으로 이동합니다. 이렇게 하면 링크가 실패할 때 가동 중지 시간을 줄이는 데 도움이 됩니다.

ECMP는 PA-7000 시리즈, PA-5200 시리즈 및 PA-3200 시리즈에서 하드웨어 전달 지원과 함께 모든 Palo Alto Networks® 방화벽 모델에서 지원됩니다. VM 시리즈 방화벽은 소프트웨어를 통해서만 ECMP를 지원합니다. 하드웨어를 오프로드할 수 없는 세션의 경우 성능이 영향을 받습니다.

ECMP는 레이어 3, 레이어 3 하위 인터페이스, VLAN, 터널 및 통합 이더넷 인터페이스에서 지원됩니다.

ECMP는 정적 경로와 방화벽이 지원하는 모든 동적 라우팅 프로토콜에 대해 구성할 수 있습니다.

용량이 경로 수를 기반으로 하기 때문에 ECMP는 경로 테이블 용량에 영향을 미치므로 경로가 4개인 ECMP 경로는 경로 테이블 용량의 엔트리 4개를 소비합니다. ECMP 구현은 트래픽 흐름을 특정 인터페이스에 매핑하기 위해 세션 기반 태그에서 더 많은 메모리를 사용하기 때문에 라우팅 테이블 용량을 약간 줄일 수 있습니다.

정적 경로를 사용하는 가상 라우터 간 라우팅은 ECMP를 지원하지 않습니다.

HA 피어가 실패할 때 ECMP 경로 선택에 대한 자세한 내용은 활성/활성 HA 모드의 ECMP를 참조하십시오.

다음 섹션에서는 ECMP 및 구성 방법에 대해 설명합니다.

- ECMP 부하 분산 알고리즘
- 가상 라우터에서 ECMP 구성
- 여러 BGP 자율 시스템에 ECMP 사용
- ECMP 확인

ECMP 부하 분산 알고리즘

방화벽의 RIB(Routing Information Base)에 단일 대상에 대한 여러 개의 동일한 비용 경로가 있다고 가정해 보겠습니다. 동일한 비용 경로의 최대 수는 기본적으로 2로 설정됩니다. ECMP는 RIB에서 FIB(Forwarding Information Base)로 복사할 최상의 두 개의 동일한 비용 경로를 선택합니다. 그런 다음 ECMP는 부하 분산 방법을 기반으로 FIB의 두 경로 중 방화벽이 이 세션 동안 대상에 사용할 경로를 결정합니다.

ECMP 로드 밸런싱은 패킷 수준이 아니라 세션 수준에서 수행됩니다. 새 세션의 시작은 방화벽(ECMP)이 동일한 비용 경로를 선택할 때입니다. 단일 대상에 대한 동일한 비용 경로는 ECMP 경로 구성원 또는 ECMP 그룹 구성원으로 간주됩니다. ECMP는 설정한 로드 밸런싱 알고리즘에 따라 FIB의 대상에 대한 여러 경로 중 ECMP 흐름에 사용할 경로를 결정합니다. 가상 라우터는 로드 밸런싱 알고리즘을 하나만 사용할 수 있습니다.

기존 가상 라우터에서 ***ECMP***를 활성화, 비활성화 또는 변경하면 시스템이 가상 라우터를 다시 시작하여 기존 세션이 종료될 수 있습니다.

네 가지 알고리즘 선택은 다음과 같이 서로 다른 우선 순위를 강조합니다.

- 해시 기반 알고리즘은 세션 고정성을 우선시함 - **IP** 모듈로 및 **IP** 해시 알고리즘은 소스 및 대상 주소와 같은 패킷 헤더의 정보를 기반으로 해시를 사용합니다. 지정된 세션의 각 흐름 헤더에는 동일한 소스 및 대상 정보가 포함되어 있으므로 이러한 옵션은 세션 고정성을 우선시합니다. **IP** 해시 알고리즘을 선택하면 해시가 소스 및 대상 주소를 기반으로 하거나 해시가 소스 주소만을 기반으로 할 수 있습니다. 소스 주소만을 기반으로 하는 IP 해시를 사용하면 동일한 소스 IP 주소에 속하는 모든 세션이 사용 가능한 여러 경로에서 항상 동일한 경로를 사용합니다. 따라서 경로는 고정된 것으로 간주되며 필요한 경우 문제를 해결하기가 더 쉽습니다. 동일한 대상에 대한 많은 수의 세션이 있고 ECMP 링크를 통해 균등하게 분배되지 않는 경우 선택적으로 해시 시드 값을 설정하여 로드 밸런싱을 추가로 무작위화할 수 있습니다.
- 균형 잡힌 알고리즘이 로드 밸런싱의 우선 순위 지정 - 균형 잡힌 라운드 로빈 알고리즘은 들어오는 세션을 링크 전체에 균등하게 분산하여 세션 고정보다 로드 밸런싱을 선호합니다. (라운드 로빈은 가장 최근에 선택한 항목이 선택되는 순서를 나타냅니다.) 또한 ECMP 그룹에서 새 경로가 추가되거나 제거되면(예: 그룹의 경로가 다운된 경우) 가상 라우터는 그룹의 링크에서 세션의 균형을 다시 조정합니다. 또한 세션의 흐름이 중단되어 경로를 전환해야 하는 경우, 세션과 연결된 원래 경로를 다시 사용할 수 있게 되면 가상 라우터가 다시 한 번 로드 균형을 재조정할 때 세션의 흐름이 원래 경로로 되돌아갑니다.
- 가중 알고리즘은 링크 용량 및**/**또는 속도의 우선 순위를 지정 - ECMP 프로토콜 표준의 확장으로서 Palo Alto Networks® 구현은 방화벽의 송신 인터페이스의 다양한 링크 용량 및 속도를 고려하는 가중 라운드 로빈 로드 밸런싱 옵션을 제공합니다. 이 옵션을 사용하면 링크 용량, 속도 및 대기 시간과 같은 요소를 사용하여 링크 성능을 기반으로 인터페이스에 **ECMP** 가중치(범위는 1~255, 기본값은 100)를 할당하여 사용 가능한 링크를 최대한 활용하도록 로드 균형을 유지할 수 있습니다.

  예를 들어, 방화벽에 ISP에 대한 중복 링크(ethernet1/1(100Mbps) 및 ethernet1/8(200Mbps))가 있다고 가정합니다. 이는 동일한 비용의 경로이지만 ethernet1/8을 통한 링크는 더 큰 대역폭을 제공하므로 ethernet1/1 링크보다 더 큰 로드를 처리할 수 있습니다. 따라서 로드 균형 조정 기능이 링크 용량과 속도를 고려하도록 하려면 ethernet1/8에 가중치 200을 할당하고 ethernet1/1에 가중치 100을 할당할 수 있습니다. 2:1 가중치 비율은 가상 라우터가 ethernet1/1로 보내는 세션 수보다 2배 많은 세션을 ethernet1/8로 보내도록 합니다. 그러나 ECMP 프로토콜은 본질적으로 세션 기반이므로 가중 라

운드 로빈 알고리즘을 사용할 때 방화벽은 최선의 방식으로만 ECMP 링크를 통해 로드 밸런싱을 수행할 수 있습니다.

ECMP 가중치는 경로 선택(비용이 다를 수 있는 경로에서 경로 선택)이 아니라 로드 균형 조정(선택되는 동일한 비용 경로에 영향을 미치기 위해)을 결정하기 위해 인터페이스에 할당된다는 점을 명심하십시오.

더 낮은 가중치로 저속 또는 저용량 링크를 할당합니다. 더 높은 가중치를 가진 고속 또는 고용량 링크를 할당하십시오. 이러한 방식으로 방화벽은 동일한 비용 경로 중 하나인 저용량 링크를 과도하게 구동하지 않고 이러한 비율에 따라 세션을 분산할 수 있습니다.

가상 라우터에서 ECMP 구성

가상 라우터에서 ECMP를 활성화하려면 다음 절차를 따르십시오. 전제 조건은 다음과 같습니다.

- 가상 라우터에 속하는 인터페이스를 지정합니다(네트워크 > 가상 라우터 > 라우터 설정 > 일반).
- IP 라우팅 프로토콜을 지정합니다.

기존 가상 라우터에 대해 ECMP를 활성화, 비활성화 또는 변경하면 시스템이 가상 라우터를 다시 시작하여 세션이 종료될 수 있습니다.

STEP 1 | 가상 라우터에 대해 ECMP를 활성화합니다.

1. 네트워크 > 가상 라우터를 선택하고 ECMP를 활성화할 가상 라우터를 선택합니다.
2. 라우터 설정 > **ECMP**를 선택하고 사용을 선택합니다.

STEP 2 | (선택 사항) 서버에서 클라이언트로 패킷의 대칭 반환을 활성화합니다.

대칭 반환을 선택하여 반환 패킷이 연결된 수신 패킷이 도착한 동일한 인터페이스로 나가게 합니다. 즉, 방화벽은 ECMP 인터페이스를 사용하는 대신 반환 패킷을 보낼 수신 인터페이스를 사용합니다. 대칭 반환 설정은 로드 밸런싱보다 우선합니다. 이 동작은 서버에서 클라이언트로의 트래픽 플로우에 대해서만 발생합니다.

STEP 3 | 방화벽에서 발생하는 IKE 및 IPSec 트래픽이 IPSec 터널의 소스 IP 주소가 속한 물리적 인터페이스를 빠져나가도록 하려면 엄격한 소스 경로를 활성화합니다.

ECMP를 활성화하면 기본적으로 방화벽에서 발생하는 IKE 및 IPSec 트래픽이 ECMP 로드 밸런싱 방법을 결정하는 인터페이스를 송신합니다. 또는 Strict Source Path를 활성화하여 방화벽에서 시작되는 IKE 및 IPSec 트래픽이 항상 IPSec 터널의 소스 IP 주소가 속한 물리적 인터페이스를 빠져나가도록 할 수 있습니다. 방화벽에 동일한 대상에 대해 동일한 비용의 경로를 제공하는 둘 이상의 ISP가 있는 경우 이 기능을 활성화합니다. ISP는 일반적으로 역방향 경로 전달(RPF) 검사(또는 IP 주소 스푸ping을 방지하기 위한 다른 검사)를 수행하여 트래픽이 도착한 동일한 인터페이스에서 나가는지 확인합니다. ECMP는 구성된 ECMP 방법을 기반으로 송신 인터페이스를 선택하기 때문에(소스 인터페이스를 송신 인터페이스로 선택하는 대신) 이는 ISP가 기대하는 것이 아니며 ISP가 합법적인 반환 트래픽을 차단할 수 있습니다. 이 경우 방화벽이 IPSec 터널의 소스 IP 주소가 속한 인터페이스인 Egress 인터페이스를 사용하고 RPF 검사에 성공하고 ISP가 반환 트래픽을 허용하도록 Strict Source Path를 활성화합니다.

STEP 4 | RIB(라우팅 정보 기반)에서 FIB(전달 정보 기반)로 복사할 수 있는 동일한 비용 경로(대상 네트워크에 대한)의 최대 수를 지정합니다.

허용되는 최대 경로에 **2**, **3** 또는 **4**를 입력합니다. 기본: 2.

STEP 5 | 가상 라우터에 대한 로드 밸런싱 알고리즘을 선택합니다. 로드 밸런싱 방법 및 차이점에 대한 자세한 내용은 ECMP 로드 밸런싱 알고리즘을 참조하십시오.

부하 분산의 경우 방법 목록에서 다음 옵션 중 하나를 선택합니다.

- **IP Modulo**(기본값) - 패킷 헤더에 있는 소스 및 대상 IP 주소의 해시를 사용하여 사용할 ECMP 경로를 결정합니다.
- **IP** 해시 - 사용할 ECMP 경로를 결정하는 두 가지 IP 해시 방법이 있습니다(5단계에서 해시 옵션 선택).
  - 소스 주소의 해시를 사용합니다(PAN-OS 8.0.3 이상 릴리스에서 사용 가능).
  - 소스 및 대상 IP 주소의 해시를 사용합니다(기본 IP 해시 방법).
- 균형 잡힌 라운드 로빈 - ECMP 경로 간에 라운드 로빈을 사용하고 경로 수가 변경되면 경로 균형을 다시 조정합니다.
- 가중 라운드 로빈 - 라운드 로빈 및 상대 가중치를 사용하여 ECMP 경로 중에서 선택합니다. 아래 6단계에서 가중치를 지정합니다.

STEP 6 | (IP 해시만 해당) IP 해시 옵션을 구성합니다.

방법으로 **IP** 해시를 선택한 경우:

1. 동일한 소스 IP 주소에 속하는 모든 세션이 항상 사용 가능한 여러 경로에서 동일한 경로를 사용하도록 하려면 소스 주소만 사용(PAN-OS 8.0.3 이상 릴리스에서 사용 가능)을 선택합니다. 이 IP 해시 옵션은 경로 정적성을 제공하고 문제 해결을 용이하게 합니다. 이 옵션을 선택하지 않거나 PAN-OS 8.0.3 이전 릴리스를 사용하는 경우 IP 해시는 소스 및 대상 IP 주소(기본 IP 해시 방법)를 기반으로 합니다.

   소스 주소만 사용을 선택하는 경우 *Panorama*에서 *PAN-OS 8.0.2, 8.0.1* 또는 *8.0.0*을 실행하는 방화벽으로 구성을 푸시하면 안 됩니다.

2. **IP** 해시 계산에서 소스 또는 대상 포트 번호를 사용하려면 소스/대상 포트 사용을 선택합니다.

   Use Source Address Only와 함께 이 옵션을 활성화하면 동일한 소스 *IP* 주소에 속한 세션의 경우에도 경로 선택이 무작위화됩니다.

3. 해시 시드 값(최대 9자리 정수)을 입력합니다. 로드 밸런싱을 추가로 무작위화하려면 해시 시드 값을 지정하십시오. 해시 시드 값을 지정하는 것은 동일한 튜플 정보를 가진 많은 수의 세션이 있는 경우에 유용합니다.

STEP 7 | (가중 라운드 로빈만 해당) ECMP 그룹의 각 인터페이스에 대한 가중치를 정의합니다.

가중치 기반 라운드 로빈을 방법으로 선택한 경우 동일한 대상으로 라우팅되는 트래픽의 출구 지점인 각 인터페이스에 대한 가중치를 정의합니다(즉, ISP에 대한 중복 링크를 제공하거나 기업 네트워크의 핵심 비즈니스 애플리케이션에 대한 인터페이스를 제공합니다).

가중치가 높을수록 새 세션에 대해 동일한 비용 경로가 더 자주 선택됩니다.

더 많은 *ECMP* 트래픽이 더 빠른 링크를 통과하도록 더 빠른 링크에 느린 링크보다 더 높은 가중치를 부여합니다.

1. 추가를 클릭하고 인터페이스를 선택하여 ECMP 그룹을 생성합니다.
2. ECMP 그룹에 다른 인터페이스를 추가합니다.
3. 가중치를 클릭하고 각 인터페이스에 대한 상대 가중치를 지정합니다(범위는 1-255, 기본값은 100).

STEP 8 | 구성을 저장합니다.

1. 확인을 클릭합니다.
2. ECMP 구성 변경 프롬프트에서 예를 클릭하여 가상 라우터를 다시 시작합니다. 가상 라우터를 다시 시작하면 기존 세션이 종료될 수 있습니다.

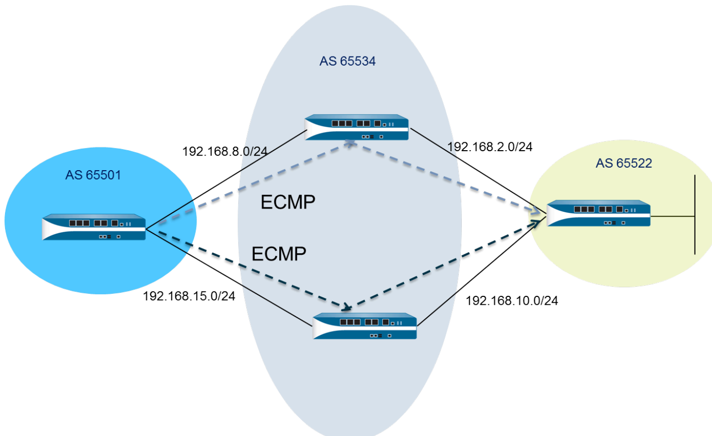
   이 메시지는 *ECMP*를 사용하여 기존 가상 라우터를 수정하는 경우에만 표시됩니다.

STEP 9 | 변경 사항을 커밋합니다.

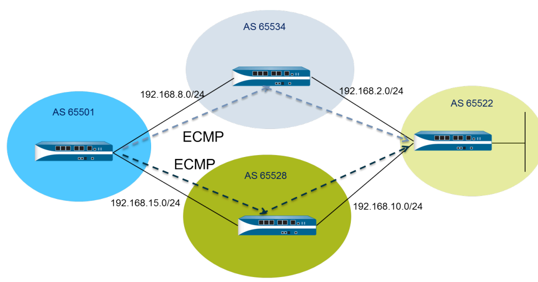
구성을 커밋합니다.

여러 BGP 자율 시스템에 ECMP 사용

BGP가 구성되어 있고 여러 자율 시스템에서 ECMP를 활성화하려는 경우 다음 작업을 수행합니다. 이 작업은 BGP가 이미 구성되어 있다고 가정합니다. 다음 그림에서 대상에 대한 두 개의 ECMP 경로는 단일 BGP 자율 시스템의 단일 ISP에 속하는 두 개의 방화벽을 통과합니다.



다음 그림에서 대상에 대한 두 개의 ECMP 경로는 서로 다른 BGP 자율 시스템의 서로 다른 두 ISP에 속하는 두 개의 방화벽을 통과합니다.



STEP 1 | ECMP를 구성합니다.

가상 라우터에서 ECMP 구성을 참조하십시오.

STEP 2 | BGP 라우팅의 경우 여러 자율 시스템에서 ECMP를 활성화합니다.

1. 네트워크 > 가상 라우터를 선택하고 여러 BGP 자율 시스템에 대해 ECMP를 활성화할 가상 라우터를 선택합니다.
2. **BGP** > 고급을 선택하고 **ECMP** 다중 **AS** 지원을 선택합니다.

STEP 3 | 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

ECMP 확인

ECMP용으로 구성된 가상 라우터는 FIB(Forwarding Information Base) 테이블에서 어떤 경로가 ECMP 경로인지 나타냅니다. 경로에 대한 ECMP 플래그(E)는 해당 경로에 대한 다음 홉에 대한 이그레스 인터페이스에 대해 ECMP에 참여하고 있음을 나타냅니다. ECMP를 확인하려면 다음 절차를 사용하여 FIB를 살펴보고 일부 경로가 동일한 비용의 다중 경로인지 확인합니다.

STEP 1 | 네트워크 > 가상 라우터를 선택합니다**.**

STEP 2 | ECMP를 활성화한 가상 라우터의 행에서 자세한 런타임 통계를 클릭합니다.

STEP 3 | FIB를 보려면 라우팅 > 포워딩 테이블을 선택합니다.

표에서 동일한 대상*(*다른 인터페이스 외부*)*에 대한 여러 경로에는 *E* 플래그가 있습니다*.* 별표*(*)*는 *ECMP* 그룹의 기본 경로를 나타냅니다*.*

LLDP

Palo Alto Networks 방화벽®은 LLDP(Link Layer Discovery Protocol)를 지원합니다. 이 프로토콜은 링크 계층에서 작동하여 인접 디바이스와 해당 기능을 검색합니다. LLDP를 사용하면 방화벽 및 기타 네트워크 디바이스가 LLDP 데이터 단위(LLDPDU)를 이웃과 주고받을 수 있습니다. 수신 디바이스는 SNMP(Simple Network Management Protocol)가 액세스할 수 있는 MIB에 정보를 저장합니다. LLDP를 사용하면 방화벽이 일반적으로 가상 와이어를 통과하는 핑 또는 추적 루트에 의해 감지되지 않는 가상 와이어에서 특히 문제를 더 쉽게 해결할 수 있습니다.

LLDP 개요

LLDP(Link Layer Discovery Protocol)는 MAC 주소를 사용하여 OSI 모델의 레이어 2에서 작동합니다. LLDPDU는 이더넷 프레임에 캡슐화된 TLV(유형 길이 값) 요소의 시퀀스입니다. IEEE 802.1AB 표준은 LLDPDU에 대한 세 가지 MAC 주소를 정의합니다. 01-80-C2-00-00-0E, 01-80-C2-00-00-03 및 01-80-C2-00-00-00.

Palo Alto Networks® 방화벽은 LLDP 데이터 유닛을 송수신하기 위해 하나의 MAC 주소만 지원합니다. 01-80-C2-00-00-0E. 전송할 때 방화벽은 01-80-C2-00-00-0E를 데스티네이션 MAC 주소로 사용합니다. 수신 시 방화벽은 대상 MAC 주소로 01-80-C2-00-00-0E를 사용하여 데이터그램을 처리합니다. 방화벽이 인터페이스에서 LLDPDU에 대한 다른 두 MAC 주소 중 하나를 수신하는 경우 방화벽은 다음과 같이 이 기능 이전에 수행한 것과 동일한 전달 작업을 수행합니다.

- 인터페이스 유형이 vwire이면 방화벽은 데이터그램을 다른 포트로 전달합니다.
- 인터페이스 유형이 L2인 경우 방화벽은 데이터그램을 나머지 VLAN으로 플러딩합니다.
- 인터페이스 유형이 L3인 경우 방화벽은 데이터그램을 삭제합니다.

Panorama 및 WildFire 어플라이언스는 지원되지 않습니다.

LLDP를 지원하지 않는 인터페이스 유형은 탭, 고가용성(HA), 미러 해독, 가상 와이어/vlan/L3 하위 인터페이스 및 PA-7000 시리즈 LPC(로그 처리 카드) 인터페이스입니다.

LLDP 이더넷 프레임의 형식은 다음과 같습니다.

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

LLDP 이더넷 프레임 내에서 TLV 구조는 다음 형식을 갖습니다.

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

LLDP에서 지원되는 TLV

LLDPDU에는 필수 및 선택적 TLV가 포함됩니다. 다음 표에는 방화벽이 지원하는 필수 TLV가 나열되어 있습니다.

필수 **TLV**	**TLV** 유형	설명
섀시 ID TLV	1	방화벽 섀시를 식별합니다. 각 방화벽에는 정확히 하나의 고유한 섀시 ID가 있어야 합니다. Palo Alto Networks® 모델에서 섀시 ID 하위 유형은 4(MAC 주소)이며 고유성을 보장하기 위해 Eth0의 MAC 주소를 사용합니다.
포트 ID TLV	2	LLDPDU가 전송되는 포트를 식별합니다. 각 방화벽은 전송된 각 LLDPDU 메시지에 대해 하나의 포트 ID를 사용합니다. 포트 ID 하위 유형은 5(인터페이스 이름)이며 전송 포트를 고유하게 식별합니다. 방화벽은 인터페이스의 ifname을 포트 ID로 사용합니다.
TTL(수명) TLV	3	피어로부터 받은 LLDPDU 정보가 로컬 방화벽에서 유효한 것으로 유지되는 기간(초)을 지정합니다(범위는 0-65,535). 값은 LLDP 유지 시간 승수의 배수입니다. TTL 값이 0이면 디바이스와 관련된 정보가 더 이상 유효하지 않으며 방화벽이 MIB에서 해당 항목을 제거합니다.
LLDPDU TLV의 끝	0	LLDP 이더넷 프레임에서 TLV의 끝을 나타냅니다.

다음 표에는 Palo Alto Networks 방화벽이 지원하는 선택적 TLV가 나열되어 있습니다.

선택적 **TLV**	**TLV** 유형	방화벽 구현 목적 및 참고 사항
포트 설명 TLV	4	방화벽의 포트를 영숫자 형식으로 설명합니다. ifAlias 개체가 사용됩니다.
시스템 이름 TLV	5	영숫자 형식으로 구성된 방화벽 이름입니다. sysName 개체가 사용됩니다.
시스템 설명 TLV	6	영숫자 형식으로 방화벽을 설명합니다. sysDecr 개체가 사용됩니다.
시스템 기능	7	다음과 같이 인터페이스의 배포 모드를 설명합니다. • L3 인터페이스는 라우터(비트 6) 기능과 "기타" 비트(비트 1)로 보급됩니다. • L2 인터페이스는 MAC 브리지(비트 3) 기능과 "기타" 비트(비트 1)로 광고됩니다.

선택적 **TLV**	**TLV** 유형	방화벽 구현 목적 및 참고 사항
		• 가상 와이어 인터페이스는 리피터(비트 2) 기능과 "기타" 비트(비트 1)로 보급됩니다.
관리 주소	8	다음과 같이 방화벽 관리에 사용되는 하나 이상의 IP 주소: • 관리(MGT) 인터페이스의 IP 주소 • 인터페이스의 IPv4 및/또는 IPv6 주소 • 루프백 주소 • 관리 주소 필드에 입력한 사용자 정의 주소 관리 IP 주소가 제공되지 않은 경우 기본값은 전송 인터페이스의 MAC 주소입니다. 지정된 관리 주소의 인터페이스 번호가 포함됩니다. 관리 주소가 지정된 하드웨어 인터페이스의 OID도 포함됩니다(해당되는 경우). 둘 이상의 관리 주소가 지정된 경우 목록의 맨 위에서 시작하여 지정된 순서대로 전송됩니다. 최대 4개의 관리 주소가 지원됩니다. 이것은 선택적 매개변수이며 비활성화된 상태로 둘 수 있습니다.

LLDP 시슬로그 메시지 및 SNMP 트랩

방화벽은 SNMP 관리자가 모니터링할 수 있는 MIB에 LLDP 정보를 저장합니다. 방화벽이 LLDP 이벤트에 대한 SNMP 트랩 알림 및 syslog 메시지를 보내도록 하려면 LLDP 프로파일에서 **SNMP Syslog** 알림을 활성화해야 합니다.

RFC 5424, Syslog 프로토콜 및 RFC 1157, A Simple Network Management Protocol에 따라 LLDP는 MIB 변경이 발생할 때 syslog 및 SNMP 트랩 메시지를 보냅니다. 이러한 메시지는 기본적으로 5초로 설정되고 구성 가능한 LLDP 전역 설정인 알림 간격에 의해 속도가 제한됩니다.

LLDP syslog 및 SNMP 트랩 메시지는 비율이 제한되어 있으므로 해당 프로세스에 제공된 일부 LLDP 정보는 LLDP 상태 정보 보기에서 표시되는 현재 LLDP 통계와 일치하지 않을 수 있습니다. 이는 정상적인 예상 동작입니다.

인터페이스(이더넷 또는 AE)당 최대 5개의 MIB를 수신할 수 있습니다. 각각의 다른 소스에는 하나의 MIB가 있습니다. 이 제한을 초과하면 `tooManyNeighbors` 오류 메시지가 트리거됩니다.

LLDP 구성

LLDP를 구성하고 LLDP 프로파일을 생성하려면 수퍼유저 또는 디바이스 관리자(deviceadmin)여야 합니다. 방화벽 인터페이스는 최대 5개의 LLDP 피어를 지원합니다.

STEP 1 | 방화벽에서 LLDP를 활성화합니다.

네트워크 > **LLDP**를 선택하고 LLDP 일반 섹션을 편집합니다. 활성화를 선택합니다.

STEP 2 | (선택 사항) LLDP 전역 설정을 변경합니다.

1. 전송 간격**(**초**)** 에서 LLDPDU가 전송되는 간격(초)을 지정합니다. 범위는 1~3600입니다. 기본값은 30입니다.
2. 전송 지연**(**초**)**의 경우 TLV 요소를 변경한 후 전송되는 LLDP 전송 간의 지연 시간(초)을 지정합니다. 지연은 많은 네트워크 변경으로 인해 LLDP 변경 수가 급증하거나 인터페이스가 플랩되는 경우 LLDPDU로 세그먼트가 플러딩되는 것을 방지하는 데 도움이 됩니다. 전송 지연은 전송 간격보다 작아야 합니다. 범위는 1~600입니다. 기본값은 2입니다.
3. **Hold Time Multiple**에 대해 **Transmit Interval**을 곱한 값을 지정하여 총 TTL Hold Time을 결정합니다. 범위는 1~100입니다. 기본값은 4입니다. 승수 값에 관계없이 최대 TTL 보류 시간은 65535초입니다.
4. 알림 간격에 대해 MIB 변경이 발생할 때 LLDP Syslog 메시지 및 SNMP 트랩이 전송되는 간격(초)을 지정합니다. 범위는 1~ 3600입니다. 기본값은 5입니다.
5. 확인을 클릭합니다.

STEP 3 | LLDP 프로파일을 만듭니다.

선택적 TLV에 대한 설명은 LLDP에서 지원되는 TLV를 참조하십시오.

1. 네트워크 > 네트워크 프로파일 > **LLDP** 프로파일을 선택하고 LLDP 프로파일의 이름을 추가합니다.
2. 모드에서 전송**-**수신(기본값), 전송 전용 또는 수신 전용을 선택합니다.
3. SNMP 알림 및 syslog 메시지를 활성화하려면 **SNMP Syslog** 알림을 선택합니다. 활성화된 경우 전역 알림 간격이 사용됩니다. 방화벽은 디바이스 로그 > 설정 > 시스템 **SNMP** 트랩 프로파일 및 **Syslog** > 프로파일에 구성된 대로 **SNMP** 트랩과 **syslog** 이벤트를 모두 전송합니다.
4. 선택적 TLV의 경우 전송하려는 TLV를 선택합니다.
   - 포트 설명
   - 시스템 이름
   - 시스템 설명
   - 시스템 기능
5. (선택 사항) 관리 주소를 선택하여 하나 이상의 관리 주소를 추가하고 이름 추가를 선택합니다.
6. 관리 주소를 가져올 인터페이스를 선택합니다. 관리 주소 TLV가 활성화된 경우 하나 이상의 관리 주소가 필요합니다. 관리 IP 주소가 구성되지 않은 경우 시스템은 전송 인터페이스의 MAC 주소를 관리 주소 TLV로 사용합니다.
7. **IPv4** 또는 **IPv6**을 선택하고 인접 필드의 목록에서 IP 주소(선택한 인터페이스에 구성된 주소 나열)를 선택하거나 주소를 입력합니다.
8. 확인을 클릭합니다.
9. 관리 주소는 최대 4개까지 허용됩니다. 관리 주소를 두 개 이상 지정하면 목록의 맨 위에서 시작하여 지정된 순서대로 전송됩니다. 주소 순서를 변경하려면 주소를 선택하고 위로 이동 또는 아래로 이동 버튼을 사용합니다.
10. 확인을 클릭합니다.

STEP 4 | 인터페이스에 LLDP 프로파일을 할당합니다.

1. 네트워크 > 인터페이스를 선택하고 LLDP 프로파일을 할당할 인터페이스를 선택합니다.
2. 고급 > **LLDP**를 선택합니다.
3. **LLDP** 활성화를 선택하여 LLDP 프로파일을 인터페이스에 할당합니다.
4. 프로파일에서 생성한 프로파일을 선택합니다. 없음을 선택하면 기본 기능으로 LLDP가 활성화됩니다. 세 개의 필수 TLV를 보내고 송수신 모드를 활성화합니다.

   새 프로파일을 만들려면 **LLDP** 프로파일을 클릭하고 위의 지침 단계를 따릅니다.
5. 확인을 클릭합니다.

STEP 5 | 변경 사항을 커밋합니다.

LLDP 설정 및 상태 보기

다음 절차를 수행하여 LLDP 설정 및 상태를 봅니다.

STEP 1 | LLDP 전역 설정을 봅니다.

네트워크 > **LLDP**를 선택합니다.

LLDP 일반 화면에서 가능은 LLDP의 활성화 여부를 나타냅니다.

- LLDP를 사용하도록 설정하면 구성된 전역 설정(전송 간격, 전송 지연, 보류 시간 배수 및 알림 간격)이 표시됩니다.
- LLDP를 사용하지 않으면 전역 설정의 디폴트 값이 표시됩니다.

이러한 값에 대한 설명은 LLDP 구성의 두 번째 단계를 참조하십시오.

STEP 2 | LLDP 상태 정보를 봅니다.

1. 상태 탭을 선택합니다.
2. (선택 사항) 표시되는 정보를 제한하는 필터를 입력합니다.

   인터페이스 정보**:**

   - 인터페이스 - LLDP 프로파일이 할당된 인터페이스의 이름입니다.
   - **LLDP** - LLDP 상태: 사용 가능하거나 비활성화됨.
   - 모드 - 인터페이스의 LLDP 모드: Tx/Rx, Tx 전용 또는 Rx 전용.
   - 프로파일 - 인터페이스에 할당된 프로파일의 이름입니다.

   전송 정보**:**

   - 총 전송 - 인터페이스를 전송한 LLDPDU의 수.
   - 삭제된 전송 - 오류로 인해 인터페이스를 전송하지 않은 LLDPDU의 수입니다. 예를 들어, 시스템이 전송을 위해 LLDPDU를 구성할 때 길이 오류가 발생합니다.

   받은 정보**:**

   - 총 수신 - 인터페이스에서 수신된 LLDP 프레임의 수입니다.
   - 삭제된 **TLV** - 수신 시 폐기된 LLDP 프레임 수입니다.
   - 오류 - 인터페이스에서 수신되고 오류가 포함된 TVL 수입니다. TLV 오류 유형은 다음과 같습니다. 하나 이상의 필수 TV 누락, 순서가 없는, 범위를 벗어난 정보 또는 길이 오류가 포함됩니다.
   - 인식되지 않음 - LLDP 로컬 에이전트가 인식하지 못하는 인터페이스에서 수신된 TVL 수입니다. 예를 들어, TLV 유형은 예약된 TLV 범위에 있습니다.
   - 에이지 아웃 - 적절한 TTL 만료로 인해 MIB 수신에서 삭제된 항목 수입니다.

STEP 3 | 인터페이스에서 볼 수 있는 각 이웃에 대한 요약 LLDP 정보를 봅니다.

1. 피어 탭을 선택합니다.
2. (선택 사항) 표시되는 정보를 제한하는 필터를 입력합니다.

   로컬 인터페이스 - 인접 디바이스를 감지한 방화벽의 인터페이스입니다.

   원격 섀시 **ID** - 피어의 섀시 ID. MAC 주소가 사용됩니다.

   포트 **ID** - 피어의 포트 ID입니다.

   이름 - 피어 이름입니다.

   자세한 정보 - 필수 및 선택적 TVL를 기반으로 하는 다음 원격 피어 세부 정보를 제공합니다.

   - 섀시 유형: MAC 주소입니다.
   - MAC 주소: 피어의 MAC 주소입니다.
   - 시스템 이름: 피어의 이름입니다.
   - 시스템 설명: 피어에 대한 설명입니다.
   - 포트 설명: 피어의 포트 설명입니다.
   - 포트 유형: 인터페이스 이름입니다.
   - 포트 ID: 방화벽은 인터페이스의 ifname을 사용합니다.
   - 시스템 기능: 시스템의 기능입니다. O = 기타, P = 리피터, B = 브리지, W = 무선 LAN, R = 라우터, T = 전화
   - 사용 가능한 기능: 피어에서 사용할 수 있는 기능입니다.
   - 관리 주소: 피어의 관리 주소입니다.

LLDP 통계 지우기

특정 인터페이스에 대한 LLDP 통계를 지울 수 있습니다.

특정 인터페이스에 대한 LLDP 통계를 지웁니다.

1. 네트워크 > **LLDP** > 상태를 선택하고 왼쪽 열에서, LLDP 통계를 지우려는 인터페이스를 하나 이상 선택합니다.
2. 화면 하단에서 **LLDP** 통계 지우기를 클릭합니다.

BFD

방화벽은 두 라우팅 피어 간의 양방향 경로 내 오류를 인식하는 프로토콜인, 양방향 전달 감지(BFD)(RFC 5880)를 지원합니다. BFD 오류 감지는 링크 모니터링 또는 헬로 패킷 또는 하트비트와 같은, 빈번한 동적 라우팅 상태 확인을 통해 달성할 수 있는 것보다 더 빠른 시스템 대체 작동을 제공하므로, 매우 빠릅니다. 고가용성과 매우 빠른 장애 조치가 필요한 임무 수행에 필수적인 데이터 센터 및 네트워크에는 BFD가 제공하는 매우 빠른 오류 감지가 필요합니다.

- BFD 개요
- BFD 구성
- 참조: BFD 세부 정보

BFD 개요

BFD를 작동시키면 BFD는 3방향 핸드셰이크를 사용하여 한 끝점(방화벽)에서 링크 끝점의 BFD 피어로 세션을 설정합니다. 제어 패킷은 핸드셰이크를 수행하고 피어가 제어 패킷을 보내고 받을 수 있는 최소 간격을 포함하여, BFD 프로필에 구성된 매개변수를 협상합니다. IPv4 및 IPv6 모두에 대한 BFD 제어 패킷은 UDP 포트 3784를 통해 전송됩니다. 멀티홉 지원을 위한 BFD 제어 패킷은 UDP 포트 4784를 통해 전송됩니다. 두 포트를 통해 전송되는 BFD 제어 패킷은 UDP 패킷으로 캡슐화됩니다.

BFD 세션이 설정된 후 BFD의 Palo Alto Networks® 구현은 비동기 모드에서 작동합니다. 즉, 두 엔드 포인트가 협상된 간격으로 서로 제어 패킷(헬로우 패킷과 같은 기능)을 보냅니다. 피어가 감지 시간(협상된 전송 간격에 감지 시간 승수를 곱한 값으로 계산) 내에 제어 패킷을 수신하지 않으면, 피어는 세션이 중단된 것으로 간주합니다. (방화벽은 주기적이 아닌 필요할 때만 제어 패킷을 보내는, 디맨드 모드를 지원하지 않습니다.)

정적 경로에 대해 BFD를 작동시키고 방화벽과 BFD 피어 간의 BFD 세션이 실패하면, 방화벽은 RIB 및 FIB 표에서 실패한 경로를 제거하고 우선 순위가 낮은 대체 경로가 인계되도록 허용합니다. 라우팅 프로토콜에 대해 BFD를 작동시키면, BFD는 라우팅 프로토콜에 피어에 대한 대체 경로로 전환하도록 알립니다. 따라서, 방화벽과 BFD 피어는 새로운 경로로 다시 수렴됩니다.

BFD 프로필을 사용하면 BFD 설정을 구성하고 방화벽의 하나 이상의 라우팅 프로토콜 또는 고정 경로에 적용할 수 있습니다. 프로필을 구성하지 않고 BFD를 작동시키면, 방화벽은 기본 BFD 프로필(모든 기본 설정 포함)을 사용합니다. 기본 BFD 프로필을 변경할 수 없습니다.

인터페이스가 서로 다른 BFD 프로필을 사용하는 여러 프로토콜을 실행하는 경우, BFD는 원하는 최소 **Tx** 간격이 가장 낮은 프로필을 사용합니다. 동적 라우팅 프로토콜은 BFD를 참조합니다.

능동/수동 HA 피어는 BFD 구성 및 세션을 동기화합니다. 능동/능동 HA 피어는 그렇지 않습니다.

BFD는 RFC 5880에서 표준화되었습니다. PAN-OS는 RFC 5880의 모든 구성 요소를 지원하지 않습니다. BFD의 지원되지 않는 RFC 구성 요소를 참조합니다.

PAN-OS는 RFC 5881, www.rfc-editor.org/rfc/rfc5881.txt도 또한 지원합니다. 이 경우, BFD는 IPv4 또는 IPv6을 사용하는 두 시스템 간의 단일 홉을 추적하므로, 두 시스템이 서로 직접 연결됩니다. BFD는 또한 BGP로 연결된 피어에서 여러 홉을 추적합니다. PAN-OS는 RFC 5883, www.rfc-editor.org/rfc/rfc5883.txt에 설명된 대로 BFD 캡슐화를 따릅니다. 그러나, PAN-OS는 인증을 지원하지 않습니다.

- BFD 모델, 인터페이스 및 클라이언트 지원
- BFD의 지원되지 않는 RFC 구성 요소
- 정적 경로에 대한 BFD
- 동적 라우팅 프로토콜을 위한 BFD

BFD 모델, 인터페이스 및 클라이언트 지원

다음 방화벽 모델은 BFD를 지원하지 않습니다. PA-800 시리즈, PA-400 시리즈, PA-220 및 VM-50 방화벽. BFD를 지원하는 모델은 제품 선택 도구에 나열된대로, 최대 BFD 세션 수를 지원합니다.

BFD는 물리적 이더넷, 통합 이더넷(AE), VLAN 및 터널 인터페이스(사이트 간 VPN 및 LSVPN)과 레이어 3 하위 인터페이스에서 실행됩니다.

지원되는 BFD 클라이언트는 다음과 같습니다.

- 단일 홉으로 구성된 고정 경로(IPv4 및 IPv6)
- OSPFv2 및 OSPFv3(인터페이스 유형에는 브로드캐스트, 점-대-점 및 점-대-여러 점이 포함됨)
- 단일 홉 또는 다중 홉으로 구성된 BGP IPv4 및 IPv6(IBGP, EBGP)
- RIP(단일 홉)

BFD의 지원되지 않는 RFC 구성 요소

- 수요 모드
- 인증
- 에코 패킷을 보내거나 받는 행위 그러나 방화벽은 가상 와이어 또는 탭 인터페이스에 도착하는 에코 패킷을 전달합니다. (BFD 에코 패킷에는 소스 및 대상에 대해 동일한 IP 주소가 있습니다.)
- 투표 시퀀스
- 혼잡 제어

정적 경로에 대한 BFD

정적 경로에서 BFD를 사용하려면, 정적 경로의 반대쪽에 있는 방화벽과 피어 모두가 BFD 세션을 지원해야 합니다. 정적 경로는 다음 홉 유형이 **IP** 주소인 경우에만 BFD 프로필을 가질 수 있습니다.

인터페이스가 피어에 대한 둘 이상의 고정 경로로 구성된 경우(BFD 세션은 동일한 소스 IP 주소와 동일한 대상 IP 주소를 가짐), 단일 BFD 세션이 여러 고정 경로를 자동으로 처리합니다. 이 동작은 BFD 세션을 줄입니다. 고정 경로가 다른 BFD 프로필을 갖는 경우, 가장 짧은 원하는 최소 전송 간격을 가지는 프로필이 적용됩니다.

DHCP 또는 PPPoE 클라이언트 인터페이스에서 고정 경로에 대해 BFD를 구성하려는 배포에서는, 두 커밋을 수행해야 합니다. 고정 경로에 대해 BFD를 작동시키려면 다음 홉 유형이 **IP** 주소여야 합니다. 그러나 DHCP 또는 PPPoE 인터페이스 커밋에서, 인터페이스 IP 주소와 다음 홉 IP 주소(기본 게이트웨이)를 알 수 없습니다.

먼저 인터페이스에 대해 DHCP 또는 PPPoE 클라이언트를 작동시키고, 커밋을 수행하고, DHCP 또는 PPPoE 서버가 클라이언트 IP 주소와 기본 게이트웨이 IP 주소를 방화벽으로 보낼 때까지 기다립니다. 그런 다음 (DHCP 또는 PPPoE 클라이언트의 기본 게이트웨이 주소를 다음 홉으로 사용하여) 고정 경로를 구성하고, BFD를 작동하고, 두 번째 커밋을 수행할 수 있습니다.

동적 라우팅 프로토콜을 위한 BFD

방화벽은 정적 경로에 대한 BFD 외에도, BGP, OSPF 및 RIP 라우팅 프로토콜에 대한 BFD를 지원합니다.

다중 홉 BFD의 Palo Alto Networks® 구현은 RFC 5883의 캡슐화 부분인 다중 홉 경로용 BFD(Bidirectional Forwarding Detection, 양방향 전달 감지)를 따르지만 인증은 지원하지 않습니다. 해결 방법은 BGP용 VPN 터널내 BFD를 구성하는 것입니다. VPN 터널은 BFD 인증의 중복 없이 인증을 제공할 수 있습니다.

OSPFv2 또는 OSPFv3 브로드캐스트 인터페이스에 대해 BFD를 작동시킬 때, OSPF는 DR(지정 라우터) 및 BDR(백업 지정 라우터)로만 BFD 세션을 설정합니다. 지점간 인터페이스에서, OSPF는 직접 이웃과 BFD 세션을 설정합니다. 점대다점 인터페이스에서, OSPF는 각 피어와 BFD 세션을 설정합니다.

방화벽은 OSPF 또는 OSPFv3 가상 링크에서 BFD를 지원하지 않습니다.

각 라우팅 프로토콜은 인터페이스에서 독립적인 BFD 세션을 가질 수 있습니다. 또는, 둘 이상의 라우팅 프로토콜(BGP, OSPF 및 RIP)이 인터페이스에 대한 공통 BFD 세션을 공유할 수 있습니다.

동일한 인터페이스에서 여러 프로토콜에 대해 BFD를 작동시키고, 프로토콜에 대한 소스 IP 주소와 대상 IP 주소도 또한 동일한 경우, 프로토콜은 단일 BFD 세션을 공유하므로, 프로토콜은 단일 BFD 세션을 공유하므로, 인터페이스에서 데이터플레인 오버헤드(CPU)와 트래픽 부하를 모두 줄입니다. 이러한 프로토콜에 대해 다른 BFD 프로필을 구성하는 경우, 원하는 최소 **Tx** 간격이 가장 낮은 하나의 BFD 프로필만 사용됩니다. 프로필이 동일한 원하는 최소 **Tx** 간격을 갖는 경우, 처음 생성된 세션에서 사용된 프로필이 적용됩니다. 정적 라우트와 OSPF가 동일한 세션을 공유하는 경우, 커밋 직후 정적 세션이 생성되기 때문에, OSPF가 인접 항목이 작동할 때까지 기다리는 동안, 정적 라우트의 프로필이 적용됩니다.

이러한 경우 단일 BFD 세션을 사용하는 이점은 이 동작이 리소스를 보다 효율적으로 사용한다는 것입니다. 방화벽은 저장된 리소스를 사용하여 다른 인터페이스에서 더 많은 BFD 세션을 지원하거나 또는 다른 소스 IP 및 대상 IP 주소 쌍에 대해 BFD를 지원할 수 있습니다.

동일한 인터페이스에서 IPv4 및 IPv6은 동일한 BFD 프로필을 사용할 수 있더라도, 항상 다른 BFD 세션을 생성합니다.

BGP 및 *HA* 경로 모니터링을 위해 *BFD*를 모두 구현하는 경우, *Palo Alto Networks*는 *BGP* 정상 재시작을 구현하지 않을 것을 권장합니다. *BFD* 피어의 인터페이스가 실패하고 경로 모니터링이 실패하면, *BFD*는 라우팅 테이블로부터 영향을 받는 경로를 제거하고 정상 재시작이 적용되기 전에 이 변경 사항을 수동 *HA* 방화벽에 동기화할 수 있습니다. *BGP*용 *BFD*, *BGP*용 정상 재시작 및 *HA* 경로 모니터링을 구현하기로 결정한 경우, 기본값보다 더 큰 원하는 최소 *Tx* 간격 및 더 큰 감지 시간 승수로 *BFD*를 구성해야 합니다.

BFD 구성

지원되는 방화벽 모델 및 인터페이스가 포함된 BFD 개요을(를) 읽은 후 BFD를 구성하기 전에 다음을 수행합니다.

- 하나 이상의 가상 라우터를 구성합니다.
- BFD를 정적 경로에 적용하는 경우 하나 이상의 정적 경로를 구성합니다.
- 라우팅 프로토콜에 BFD를 적용하는 경우 라우팅 프로토콜(BGP, OSPF, OSPFv3 또는 RIP)을 구성합니다.

BFD 구현의 효율성은 트래픽 부하, 네트워크 조건, *BFD* 설정이 얼마나 적극적인지, 데이터플레인이 얼마나 바쁜지 등 다양한 요인에 따라 달라집니다.

STEP 1 | BFD 프로파일을 만듭니다.

기존 *BFD* 세션이 사용하고 있는 *BFD* 프로파일의 설정을 변경하고 변경 사항을 커밋하면 방화벽이 해당 *BFD* 세션을 삭제하고 새 설정으로 다시 만들기 전에 방화벽이 로컬 상태가 *admin*으로 설정된 *BFD* 패킷을 아래의 관리자에게 보냅니다. 피어 디바이스는 RFC 5882, 섹션 *3.2*의 피어 구현에 따라 라우팅 프로토콜 또는 정적 경로를 사용하거나 사용하지 않을 수 있습니다.

1. 네트워크 > 네트워크 프로파일 > **BFD** 프로파일을 선택하고 BFD 프로파일의 이름을 추가합니다. 이름은 대소문자를 구분하며 방화벽에서 고유해야 합니다. 문자, 숫자, 공백, 하이픈 및 밑줄만 사용하십시오.
2. BFD가 작동하는 모드를 선택합니다.
   - 활성 - BFD가 제어 패킷을 피어로 보내기 시작합니다(기본값). BFD 피어 중 하나 이상은 활성 상태여야 합니다. 둘 다 활성일 수 있습니다.
   - 수동 - BFD는 피어가 제어 패킷을 보낼 때까지 기다렸다가 필요에 따라 응답합니다.

STEP 2 | BFD 간격을 구성합니다.

1. 원하는 최소 **Tx** 간격**(ms)**을 입력합니다. 이것은 BFD 프로토콜(BFD라고 함)이 BFD 제어 패킷을 보내는 최소 간격(밀리초)입니다. 따라서 피어와 전송 간격을 협상하고 있습니다. PA-7000

및 PA-5200 시리즈 방화벽의 최소값은 50입니다. VM 시리즈 방화벽의 최소값은 200입니다. 최대값은 2,000이며 기본값은 1,000입니다.

PA-7000 시리즈 방화벽에서 원하는 최소 ***Tx*** 간격을 *100* 이상으로 설정하는 것이 좋습니다*. 100*보다 작은 값은 *BFD* 플랩을 일으킬 위험이 있습니다*.*

동일한 인터페이스에서 다른 *BFD* 프로파일을 사용하는 여러 라우팅 프로토콜이 있는 경우 동일한 원하는 최소 ***Tx*** 간격으로 *BFD* 프로파일을 구성합니다*.*

2. 필요한 최소 수신 간격**(ms)**을 입력합니다. 이것은 BFD가 BFD 제어 패킷을 수신할 수 있는 최소 간격(밀리초)입니다. PA-7000 및 PA-5200 시리즈 방화벽의 최소값은 50입니다. VM 시리즈 방화벽의 최소값은 200입니다. 최대값은 2,000이며 기본값은 1,000입니다.

PA-7000 시리즈 방화벽에서 필요한 최소 수신 간격을 *100* 이상으로 설정하는 것이 좋습니다*. 100*보다 작은 값은 *BFD* 플랩을 일으킬 위험이 있습니다*.*

STEP 3 | BFD 감지 시간 승수를 구성합니다.

감지 시간 승수를 입력합니다. 로컬 시스템은 원격 시스템에서 수신한 감지 시간 승수에 원격 시스템의 합의된 전송 간격을 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. 범위는 2~50입니다. 기본값은 3입니다.

예를 들어, 300ms x 3(검출 시간 승수) = 900ms 감지 시간의 전송 간격입니다.

BFD 프로파일을 구성할 때 방화벽은 일반적으로 네트워크 또는 데이터 센터의 가장자리에 있는 세션 기반 디바이스이며 전용 라우터보다 링크가 느릴 수 있다는 점을 고려하십시오*.* 따라서 방화벽은 허용되는 가장 빠른 설정보다 더 긴 간격과 더 높은 승수가 필요할 수 있습니다*.* 감지 시간이 너무 짧으면 문제가 단순히 트래픽 정체인 경우 잘못된 오류 감지가 발생할 수 있습니다*.*

STEP 4 | BFD 유지 시간을 구성합니다.

유지 시간**(ms)**을 입력합니다. 이것은 BFD가 BFD 제어 패킷을 전송하기 전에 링크가 발생한 후 지연(밀리초)입니다. **Hold Time**은 BFD Active 모드에만 적용됩니다. BFD는 **Hold Time** 동안 BFD 제어 패킷을 수신하면 이를 무시합니다. 범위는 0-120000입니다. 기본값은 0이며, 이는 전송 보류 시간이 사용되지 않음을 의미합니다. BFD는 링크가 설정된 직후 BFD 제어 패킷을 보내고 받습니다.

STEP 5 | (선택 사항 - BGP IPv4 구현에만 해당) BFD 프로파일에 대한 홉 관련 설정을 구성합니다.

1. BGP 멀티홉을 통한 BFD를 활성화하려면 멀티홉을 선택합니다.
2. 최소 **Rx TTL**을 입력합니다. 이것은 BGP가 멀티홉 BFD를 지원할 때 BFD가 BFD 제어 패킷에서 수락(수신)하는 최소 실행 시간 값(홉 수)입니다. (범위는 1-254이며 기본값은 없습니다.)

   방화벽은 구성된 최소 **Rx TTL**보다 작은 TTL을 수신하는 경우 패킷을 삭제합니다. 예를 들어, 피어가 5홉 떨어져 있고 피어가 TTL이 100인 BFD 패킷을 방화벽으로 전송하고 방화벽의 최소 **Rx TTL**이 96 이상으로 설정되면 방화벽은 패킷을 삭제합니다.

STEP 6 | BFD 프로파일을 저장합니다.

확인을 클릭합니다.

STEP 7 | (선택 사항) 정적 경로에 대해 BFD를 활성화합니다.

방화벽과 정적 경로의 반대쪽에 있는 피어 모두 BFD 세션을 지원해야 합니다.

1. 네트워크 > 가상 라우터를 선택하고 정적 경로가 구성된 가상 라우터를 선택합니다.
2. 정적 경로 탭을 선택합니다.
3. **IPv4** 또는 **IPv6** 탭을 선택합니다.
4. BFD를 적용할 정적 경로를 선택합니다.
5. 인터페이스를 선택합니다(DHCP 주소를 사용하는 경우에도 해당). 인터페이스 설정은 없음이 아니어야 합니다.
6. 다음 홉의 경우 **IP** 주소를 선택하고 아직 지정하지 않은 경우 IP 주소를 입력합니다.
7. **BFD** 프로파일에서 다음 중 하나를 선택합니다.
   - 기본값 - 기본 설정만 사용합니다.
   - 구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.
   - 새 **BFD** 프로파일 - BFD 프로파일을 생성할 수 있습니다.

   없음***(BFD*** 비활성화***)***을 선택하면 이 정적 경로에 대한 ***BFD***가 비활성화됩니다***.***
8. 확인을 클릭합니다.

IPv4 또는 **IPv6** 탭의 BFD 열은 정적 경로에 대해 구성된 BFD 프로파일을 나타냅니다.

STEP 8 | (선택 사항) 모든 BGP 인터페이스 또는 단일 BGP 피어에 대해 BFD를 활성화합니다.

*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 프로그래밍하는 피어에 대한 *BGP* 연결을 중지합니다. 피어 디바이스는 *BGP* 연결 끊김을 확인하여 재수렴을 초래할 수 있습니다. 재수렴이 프로덕션 트래픽에 영향을 미치지 않는 피크가 아닌 시간에 *BGP* 인터페이스에 대해 *BFD*를 활성화합니다.

BGP 및 *HA* 경로 모니터링을 위해 *BFD*를 모두 구현하는 경우 *Palo Alto Networks*는 *BGP Graceful Restart*를 구현하지 않을 것을 권장합니다. *BFD* 피어의 인터페이스가 실패하고 경로 모니터링이 실패하면 *BFD*는 라우팅 테이블에서 영향을 받는 경로를 제거하고 *Graceful Restart*가 적용되기 전에 이 변경 사항을 수동 *HA* 방화벽과 동기화할 수 있습니다. *BGP*를 위한 *BFD, BGP*를 위한 *Graceful Restart, HA* 경로 모니터링을 구현하기로 결정했다면, 기본값보다 더 큰 *Desired Minimum Tx Interval*과 더 큰 *Detection Time Multiplier*로 *BFD*를 구성해야 합니다.

1. 네트워크 > 가상 라우터를 선택하고 BGP가 구성된 가상 라우터를 선택합니다.
2. **BGP** 탭을 선택합니다.
3. (선택 사항) 가상 라우터의 모든 BGP 인터페이스에 BFD를 적용하려면 **BFD** 목록에서 다음 중 하나를 선택하고 확인을 클릭합니다.
   - 기본값 - 기본 설정만 사용합니다.
   - 구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.
   - 새 **BFD** 프로파일 - BFD 프로파일을 생성할 수 있습니다.

   없음*(**BFD** 비활성화)*을 선택하면 가상 라우터의 모든 *BGP* 인터페이스에 대해 *BFD*가 비활성화됩니다. 단일 *BGP* 인터페이스에 대해 *BFD*를 활성화할 수 없습니다.
4. (선택 사항) 단일 BGP 피어 인터페이스에 대해 BFD를 활성화하려면(비활성화되어 있지 않은 한 BGP에 대한 **BFD** 설정을 재정의) 다음 작업을 수행합니다.
   1. 피어 그룹 탭을 선택합니다.
   2. 피어 그룹을 선택합니다.
   3. 피어를 선택합니다.
   4. **BFD** 목록에서 다음 중 하나를 선택합니다.

      기본값 - 기본 설정만 사용합니다.

      Inherit-vr-global-setting(기본값) - BGP 피어는 가상 라우터의 BGP에 대해 전역적으로 선택한 BFD 프로파일을 상속합니다.

      구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.

      Disable BFD를 선택하면 *BGP* 피어에 대한 *BFD*가 비활성화됩니다.
5. 확인을 클릭합니다.

6. 확인을 클릭합니다.

BGP - Peer Group/Peer 목록의 BFD 열은 인터페이스에 대해 구성된 BFD 프로파일을 나타냅니다.

STEP 9 | (선택 사항) OSPF 또는 OSPFv3에 대해 전역적으로 또는 OSPF 인터페이스에 대해 BFD를 활성화합니다.

1. 네트워크 > 가상 라우터를 선택하고 OSPF 또는 OSPFv3가 구성된 가상 라우터를 선택합니다.
2. **OSPF** 또는 **OSPFv3** 탭을 선택합니다.
3. (선택 사항) **BFD** 목록에서 다음 중 하나를 선택하여 모든 OSPF 또는 OSPFv3 인터페이스에 대해 BFD를 활성화하고 확인을 클릭합니다.
   - 기본값 - 기본 설정만 사용합니다.
   - 구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.
   - 새 **BFD** 프로파일 - BFD 프로파일을 생성할 수 있습니다.

   없음***(BFD*** 비활성화***)***을 선택하면 가상 라우터의 모든 ***OSPF*** 인터페이스에 대해 ***BFD***가 비활성화됩니다. 단일 ***OSPF*** 인터페이스에 대해 ***BFD***를 활성화할 수 없습니다.
4. (선택 사항) 단일 OSPF 피어 인터페이스에서 BFD를 사용하도록 설정하여 비활성화되어 있지 않은 한 OSPF에 대한 **BFD** 설정을 재정의하려면 다음 작업을 수행합니다.
   1. 영역 탭을 선택하고 영역을 선택합니다.
   2. 인터페이스 탭에서 인터페이스를 선택합니다.
   3. **BFD** 목록에서 다음 중 하나를 선택하여 지정된 OSPF 피어에 대한 BFD를 구성합니다.

      기본값 - 기본 설정만 사용합니다.

      Inherit-vr-global-setting(기본값) - OSPF 피어는 가상 라우터의 OSPF 또는 OSPFv3에 대한 **BFD** 설정을 상속합니다.

      구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.

      Disable BFD를 선택하면 ***OSPF*** 또는 ***OSPFv3*** 인터페이스에 대한 ***BFD***가 비활성화됩니다.
   4. 확인을 클릭합니다.
5. 확인을 클릭합니다.

OSPF 인터페이스 탭의 BFD 열은 인터페이스에 대해 구성된 BFD 프로파일을 나타냅니다.

STEP 10 | (선택 사항) 전역적으로 RIP 또는 단일 RIP 인터페이스에 대해 BFD를 활성화합니다.

1. 네트워크 > 가상 라우터를 선택하고 RIP가 구성된 가상 라우터를 선택합니다.
2. **RIP** 탭을 선택합니다.
3. (선택 사항) **BFD** 목록에서 다음 중 하나를 선택하여 가상 라우터의 모든 RIP 인터페이스에 대해 BFD를 활성화하고 확인을 클릭합니다.

   - 기본값 - 기본 설정만 사용합니다.
   - 구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.
   - 새 **BFD** 프로파일 - BFD 프로파일을 생성할 수 있습니다.

   *없음(**BFD** 비활성화)을 선택하면 가상 라우터의 모든 **RIP** 인터페이스에 대해 **BFD**가 비활성화됩니다. 단일 **RIP** 인터페이스에 대해 **BFD**를 활성화할 수 없습니다.*

4. (선택 사항) 단일 RIP 인터페이스에 대해 BFD를 활성화하여 RIP에 대한 **BFD** 설정을 재정의하려면 다음 작업을 수행합니다.

   1. 인터페이스 탭을 선택하고 인터페이스를 선택합니다.
   2. **BFD** 목록에서 다음 중 하나를 선택합니다.

      기본값 - 기본 설정만 사용합니다.

      Inherit-vr-global-setting(기본값) - RIP 인터페이스는 가상 라우터에 대해 전역적으로 RIP에 대해 선택한 BFD 프로파일을 상속합니다.

      구성한 BFD 프로파일 - BFD 프로파일 만들기를 참조하십시오.

      *없음(**BFD** 비활성화)을 선택하면 **RIP** 인터페이스에 대해 **BFD**가 비활성화됩니다.*

   3. 확인을 클릭합니다.
5. 확인을 클릭합니다.

인터페이스 탭의 BFD 열은 인터페이스에 대해 구성된 BFD 프로파일을 나타냅니다.

STEP 11 | 구성을 커밋합니다.

커밋을 클릭합니다.

STEP 12 | BFD 요약 및 세부 정보를 봅니다.

1. 네트워크 > 가상 라우터를 선택하고 원하는 가상 라우터를 찾은 다음 추가 런타임 통계를 클릭합니다.
2. **BFD** 요약 정보 탭을 선택하여 BFD 상태 및 런타임 통계와 같은 요약 정보를 확인합니다.
3. (선택 사항) 참조를 보려는 인터페이스 행에서 세부 정보를 선택합니다. BFD 세부 정보.

STEP 13 | 라우팅 구성에서 참조하는 BFD 프로파일을 모니터링합니다. BFD 통계, 상태 및 상태를 모니터링합니다.

다음 CLI 작동 명령 사용:

- **show routing bfd active-profile [**<*name*>**]**
- **show routing bfd details [interface**<*name*>**][local-ip**<*ip*>**][multihop][peer-ip** <*ip*>**][session-id][virtual-router**<*name*>**]**
- **show routing bfd drop-counters session-id** <*session-id*>
- **show counter global | match bfd**

STEP 14 | (선택 사항) BFD 전송, 수신 및 드롭 카운터를 지웁니다.

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | (선택 사항) 디버깅을 위한 BFD 세션을 지웁니다.

```
clear routing bfd session-state session-id all | <1-1024>
```

참조: BFD 세부 정보

가상 라우터에 대한 다음 BFD 정보를 보려면 BFD 요약 및 세부 정보 보기의 BFD 구성 중 12단계를 참조하십시오.

이름	값(예시)	설명
세션 ID	1	BFD 세션의 ID 번호입니다.
인터페이스	ethernet1/12	BFD가 실행되는 위치에서 선택한 인터페이스입니다.
프로토콜	정적(IPV4) OSPF	인터페이스에서 BFD를 실행하는 정적 경로(정적 경로의 IP 주소 제품군) 및/또는 동적 라우팅 프로토콜입니다.
로컬 IP 주소	10.55.55.2	인터페이스의 IP 주소입니다.
인접 IP 주소	10.55.55.1	BFD 이웃의 IP 주소입니다.
BFD 프로파일	기본값 *(이 BFD 세션에는 여러 BFD 프로파일이 있습니다. 가장 낮은 'Desired Minimum Tx Interval(ms)'은 유효 프로파일을 선택하는 데 사용됩니다.)	인터페이스에 적용된 BFD 프로파일의 이름입니다. 샘플 인터페이스에는 다른 프로파일로 BFD를 실행하는 정적 경로와 OSPF가 모두 있으므로 방화벽은 **Desired Minimum Tx Interval**이 가장 낮은 프로파일을 사용합니다. 이 예에서 사용된 프로파일은 기본 프로파일입니다.
상태(로컬/원격)	up/up	로컬 및 원격 BFD 피어의 BFD 상태입니다. 가능한 상태는 admin down, down, init 및 up입니다.
가동 시간	2h 36m 21s 419ms	BFD가 작동된 시간(시, 분, 초 및 밀리초)입니다.
판별자(로컬/원격)	1391591427/1	로컬 및 원격 BFD 피어에 대한 판별자.
모드	액티브	인터페이스에서 BFD가 구성된 모드: 능동 또는 수동.
수요 모드	비활성화됨	PAN-OS는 BFD Demand Mode를 지원하지 않으므로 항상 Disabled 상태입니다.
멀티홉	비활성화됨	BFD 멀티홉: 활성화 또는 비활성화.

이름	값(예시)	설명
멀티홉 TTL		멀티홉의 TTL, 범위는 1-254입니다. 멀티홉이 비활성화된 경우 필드가 비어 있습니다.
로컬 진단 코드	0(진단 없음)	로컬 시스템의 마지막 상태 변경 이유를 나타내는 진단 코드: 0 - 진단 없음 1 - 제어 감지 시간 만료됨 2 - 에코 기능 실패 3 - 이웃 신호 세션 중단 4 - 전달 평면 재설정 5 - 경로 아래로 6 - 연결된 경로 아래로 7 - 관리적으로 다운 8 - 연결된 경로를 아래로 역방향
마지막으로 받은 원격 진단 코드	0(진단 없음)	BFD 피어에서 마지막으로 받은 진단 코드입니다.
전송 보류 시간	0ms	BFD가 BFD 제어 패킷을 전송하기 전에 링크가 발생한 후의 보류 시간(밀리초)입니다. 0ms의 홀드 시간은 즉시 전송을 의미합니다. 범위는 0-120000ms입니다.
수신된 최소 수신 간격	1000ms	피어로부터 수신된 최소 Rx 간격입니다. BFD 피어가 제어 패킷을 수신할 수 있는 간격입니다. 최대값은 2000ms입니다.
협상된 전송 간격	1000ms	BFD 피어가 서로 BFD 제어 패킷을 전송하기로 동의한 전송 간격 (밀리초) 입니다. 최대값은 2000ms입니다.
수신 승수	3	BFD 피어에서 수신한 감지 시간 승수 값입니다. 전송 시간에 승수를 곱하면 감지 시간이 됩니다. BFD가 감지 시간이 만료되기 전에 피어로부터 BFD 제어 패킷을 수신하지 않으면 오류가 발생한 것입니다. 범위는 2-50입니다.
감지 시간(초과)	3000ms (0)	계산된 감지 시간(협상 전송 간격에 승수를 곱한 값) 및 감지 시간이 초과된 시간(밀리초)입니다.
Tx 제어 패킷(마지막)	9383(420ms 전)	전송된 BFD 제어 패킷의 수(및 BFD가 가장 최근의 제어 패킷을 전송한 이후의 시간).

이름	값(예시)	설명
Rx 제어 패킷(마지막)	9384(407ms 전)	수신된 BFD 제어 패킷의 수(및 BFD가 가장 최근의 제어 패킷을 수신한 이후의 시간).
에이전트 데이터 플레인	슬롯 1 - DP 0	PA-7000 시리즈 방화벽에서 이 BFD 세션에 대한 패킷을 처리하도록 할당된 데이터플레인 CPU.
오류	0	BFD 오류 수입니다.
상태 변경을 일으키는 마지막 패킷		
버전	1	BFD 버전입니다.
폴 비트	0	BFD 폴 비트, 0은 설정되지 않음을 나타냅니다.
원하는 최소 Tx 간격	1000ms	상태 변경을 유발하는 마지막 패킷의 원하는 최소 전송 간격입니다.
필요한 최소 수신 간격	1000ms	상태 변경을 일으키는 마지막 패킷의 필수 최소 수신 간격입니다.
승수 감지	3	상태 변경을 일으키는 마지막 패킷의 승수를 감지합니다.
내 판별자	1	원격 판별자입니다. 판별자는 피어가 여러 BFD 세션을 구별하는 데 사용하는 고유한 0이 아닌 값입니다.
사용자의 판별자	1391591427	로컬 판별자. 판별자는 피어가 여러 BFD 세션을 구별하는 데 사용하는 고유한 0이 아닌 값입니다.
진단 코드	0(진단 없음)	상태 변경을 일으키는 마지막 패킷의 진단 코드입니다.
길이	24	BFD 제어 패킷의 길이(바이트)입니다.
수요 비트	0	PAN-OS는 BFD 요구 모드를 지원하지 않으므로 요구 비트는 항상 0(비활성화)으로 설정됩니다.
최종 비트	0	PAN-OS는 폴 시퀀스를 지원하지 않으므로 최종 비트는 항상 0(비활성화)으로 설정됩니다.
멀티포인트 비트	0	이 비트는 BFD에 대한 향후 지점 간 확장을 위해 예약되어 있습니다. 송신과 수신 모두 0이어야 합니다.
컨트롤 플레인 독립 비트	1	• 1로 설정하면 전송 시스템의 BFD 구현은 제어 평면과 운명을 공유하지 않습니다(즉, BFD는 전달 평면에서 구현되고 제어 평면에서 중단을 통해 계속 기능할

이름	값(예시)	설명
		수 있음). PAN-OS에서 이 비트는 항상 1로 설정됩니다. • 0으로 설정하면 전송 시스템의 BFD 구현은 제어 평면과 운명을 공유합니다.
인증 현재 비트	0	PAN-OS는 BFD 인증을 지원하지 않으므로 Authentication Present Bit는 항상 0으로 설정됩니다.
필요한 최소 에코 수신 간격	0ms	PAN-OS는 BFD Echo 기능을 지원하지 않으므로 항상 0ms입니다.

세션 설정 및 시간 초과

이 섹션에서는 IPv6, NAT64, NAT 초과 구독, 점보 프레임 크기, MTU, 가속화된 에이징 및 캡티브 포털 인증 외에도 TCP, UDP 및 ICMPv6 세션에 영향을 주는 전역 설정에 대해 설명합니다. 이미 진행 중인 세션에 새로 구성된 보안 정책을 적용할 수 있는 설정(세션 다시 일치)도 있습니다.

아래의 처음 몇 가지 주제에서는 OSI 모델, TCP, UDP 및 ICMP의 전송 레이어에 대한 간략한 요약을 제공합니다. 프로토콜에 대한 자세한 내용은 해당 RFC를 참조하십시오. 나머지 항목에서는 세션 시간 초과 및 설정에 대해 설명합니다.

- 전송 레이어 세션
- TCP
- UDP
- ICMP
- 특정 ICMP 또는 ICMPv6 유형 및 코드 제어
- 세션 시간 초과 구성
- 세션 배포 정책
- 세션 설정 구성
- TCP 분할 핸드셰이크 세션 설정 방지

전송 레이어 세션

네트워크 세션은 일정 기간 동안 지속되는 둘 이상의 통신 디바이스 간에 발생하는 메시지 교환입니다. 세션이 설정되고 세션이 종료되면 해제됩니다. 다른 유형의 세션은 OSI 모델의 세 가지 레이어인 전송 레이어, 세션 레이어 및 애플리케이션 레이어에서 발생합니다.

전송 레이어은 OSI 모델의 레이어 4에서 작동하여 신뢰할 수 있거나 신뢰할 수 없는 종단 간 전달 및 데이터 흐름 제어를 제공합니다. 전송 레이어에서 세션을 구현하는 인터넷 프로토콜에는 TCP(전송 제어 프로토콜) 및 UDP(사용자 데이터그램 프로토콜)가 있습니다.

TCP

TCP(Transmission Control Protocol)(RFC 793)는 인터넷 프로토콜(IP) 제품군의 주요 프로토콜 중 하나로 널리 퍼져 있어 IP와 함께 ***TCP/IP***로 자주 참조됩니다. TCP는 세그먼트를 송수신하는 동안 오류 검사를 제공하고 수신된 세그먼트를 승인하며 잘못된 순서로 도착한 세그먼트를 재정렬하기 때문에 안정적인 전송 프로토콜로 간주됩니다. TCP는 또한 삭제된 세그먼트의 재전송을 요청하고 제공합니다. TCP는 상태 저장 및 연결 지향적입니다. 즉, 세션 기간 동안 발신자와 수신자 간의 연결이 설정됩니다. TCP는 패킷의 흐름 제어를 제공하므로 네트워크의 혼잡을 처리할 수 있습니다.

TCP는 세션 설정 중에 핸드셰이크를 수행하여 세션을 시작하고 승인합니다. 데이터가 전송된 후 세션은 순서대로 닫힙니다. 여기서 각 측은 FIN 패킷을 전송하고 ACK 패킷으로 이를 확인합니다. TCP 세션을 시작하는 핸드셰이크는 개시자와 리스너 간의 3방향 핸드셰이크(3개의 메시지 교환)이거나 4방향 또는 5방향 분할 핸드셰이크 또는 동시 교환과 같은 변형일 수 있습니다. TCP 분할 핸드셰이크 드롭은(는) TCP 분할 핸드셰이크 세션 설정 방지 방법을 설명합니다.

TCP를 전송 프로토콜로 사용하는 애플리케이션에는 HTTP(Hypertext Transfer Protocol), HTTPS(HTTP Secure), FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol), Telnet, POP3(Post Office Protocol version 3), 인액세스 프로토콜(IMAP) 및 보안 셸(SSH)이 있습니다.

다음 주제는 TCP의 PAN-OS 구현에 대한 세부사항을 설명합니다.

- TCP Half Closed 및 TCP 시간 대기 타이머
- 확인되지 않은 RST 타이머
- TCP 분할 핸드셰이크 드롭
- 최대 세그먼트 크기(MSS)

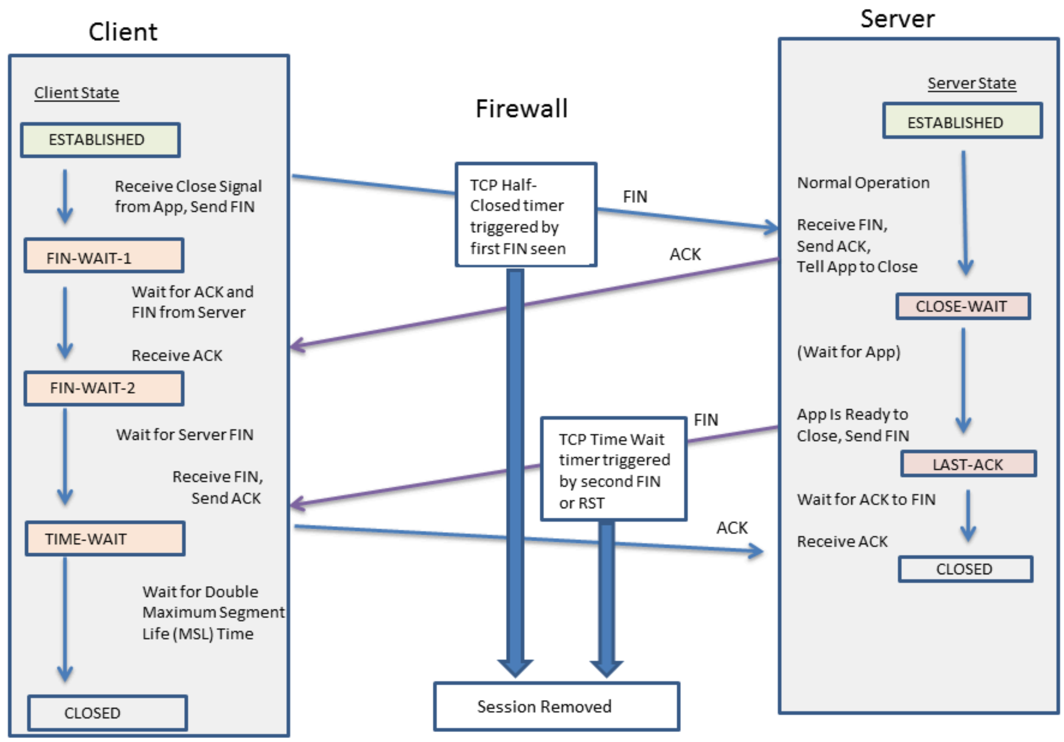
패킷 기반 공격 보호를 구성하여 바람직하지 않은 특성을 가진 IP, TCP 및 IPv6 패킷을 삭제하거나 패킷을 영역으로 허용하기 전에 패킷에서 바람직하지 않은 옵션을 제거할 수 있습니다. 또한 경보를 트리거하는 초당 SYN 연결 속도(기존 세션과 일치하지 않음)를 지정하여 홍수 방지를 구성하고, 방화벽이 SYN 패킷을 임의로 삭제하거나 SYN 쿠키를 사용하도록 하고, 최대 비율을 초과하는 SYN 패킷을 삭제하도록 할 수 있습니다.

TCP Half Closed 및 TCP 시간 대기 타이머

TCP 연결 종료 절차는 방화벽이 세션에서 보는 첫 번째 FIN에 의해 트리거되는 TCP Half Closed 타이머를 사용합니다. 연결의 한쪽에서만 FIN을 보냈기 때문에 타이머의 이름은 TCP Half Closed입니다. 두 번째 타이머인 TCP 시간 대기는 두 번째 FIN 또는 RST에 의해 트리거됩니다.

방화벽에 첫 번째 FIN에 의해 트리거된 타이머가 하나만 있는 경우 설정이 너무 짧으면 반쯤 닫힌 세션이 조기에 닫힐 수 있습니다. 반대로 설정이 너무 길면 세션 테이블이 너무 커져 모든 세션을 사용할 수 있습니다. 두 개의 타이머를 사용하면 상대적으로 긴 TCP Half Closed 타이머와 짧은 TCP Time Wait 타이머를 사용할 수 있으므로 완전히 닫힌 세션을 빠르게 에이징하고 세션 테이블의 크기를 제어할 수 있습니다.

다음 그림은 TCP 연결 종료 절차 중에 방화벽의 두 타이머가 트리거되는 경우를 보여줍니다.



TCP 시간 대기 타이머는 다음과 같은 이유로 TCP Half Closed 타이머보다 작은 값으로 설정해야 합니다.

- 첫 번째 FIN이 표시된 후 허용되는 더 긴 시간은 세션을 완전히 닫는 연결 시간의 반대쪽을 제공합니다.
- Time Wait 시간이 더 짧은 이유는 두 번째 FIN 또는 RST가 표시된 후 세션이 오랫동안 열려 있을 필요가 없기 때문입니다. 시간 대기 시간이 짧을수록 리소스가 더 빨리 확보되지만 방화벽이 다른 데이터그램의 최종 ACK 및 가능한 재전송을 볼 수 있는 시간이 여전히 허용됩니다.

TCP 시간 대기 타이머를 TCP Half Closed 타이머보다 큰 값으로 구성하면 커밋이 수락되지만 실제로 TCP 시간 대기 타이머는 TCP Half Closed 값을 초과하지 않습니다.

타이머는 전역적으로 또는 애플리케이션별로 설정할 수 있습니다. 전역 설정은 기본적으로 모든 애플리케이션에 사용됩니다. 애플리케이션 수준에서 TCP 대기 타이머를 구성하면 전역 설정을 무시합니다.

확인되지 않은 RST 타이머

방화벽이 확인할 수 없는 재설정(RST) 패킷을 수신하는 경우(TCP 창 내에 예기치 않은 시퀀스 번호가 있거나 비대칭 경로에서 온 것이기 때문에) 확인되지 않은 RST 타이머는 세션의 에이징 아웃을 제어합니다. 기본값은 30초입니다. 범위는 1-600초입니다. 미확인 RST 타이머는 아래 두 번째 글머리 기호에 설명된 추가 보안 조치를 제공합니다.

RST 패킷에는 세 가지 가능한 결과 중 하나가 있습니다.

- TCP 창 외부에 있는 RST 패킷은 삭제됩니다.

- TCP 창 내부에 있지만 정확한 예상 시퀀스 번호가 없는 RST 패킷은 확인되지 않고 확인되지 않은 RST 타이머 설정이 적용됩니다. 이 동작은 공격이 임의의 RST 패킷을 방화벽으로 보내 기존 세션을 중단시키려는 DoS(서비스 거부) 공격을 방지하는 데 도움이 됩니다.
- TCP 창 내에 있고 정확한 예상 시퀀스 번호를 갖는 RST 패킷은 TCP 시간 대기 타이머 설정의 적용을 받습니다.

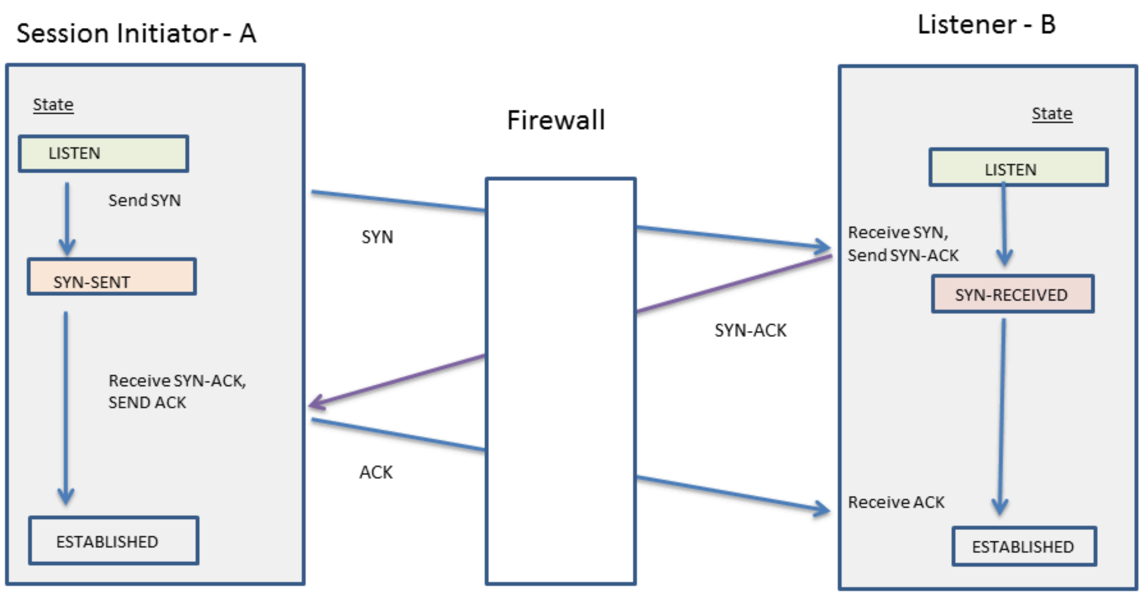
TCP 분할 핸드셰이크 드롭

영역 보호 프로파일의 분할 핸드셰이크 옵션은 세션 설정 절차가 잘 알려진 3방향 핸드셰이크를 사용하지 않고 대신 4방향 또는 5방향 분할 핸드셰이크나 동시 열기와 같은 변형을 사용하는 경우 TCP 세션이 설정되는 것을 방지합니다.

Palo Alto Networks® 차세대 방화벽은 분할 핸드셰이크 옵션을 활성화하지 않고도 분할 핸드셰이크 및 동시 개방형 세션 설정을 위해 세션과 모든 레이어 7 프로세스를 올바르게 처리합니다. 그럼에도 불구하고 분할 핸드셰이크 옵션(TCP 분할 핸드셰이크 drop을 유발함)을 사용할 수 있습니다. 영역 보호 프로파일에 대해 분할 핸드셰이크 옵션이 구성되고 해당 프로파일이 영역에 적용되는 경우 표준 3방향 핸드셰이크를 사용하여 해당 영역의 인터페이스에 대한 TCP 세션을 설정해야 합니다. 변형은 허용되지 않습니다.

분할 핸드셰이크 옵션은 기본적으로 비활성화되어 있습니다.

다음은 개시자(일반적으로 클라이언트)와 수신기(일반적으로 서버) 간에 PAN-OS 방화벽을 사용하여 TCP 세션을 설정하는 데 사용되는 표준 3방향 핸드셰이크를 보여줍니다.



분할 핸드셰이크 옵션은 영역에 할당된 영역 보호 프로파일에 대해 구성됩니다. 영역의 구성원인 인터페이스는 서버에서 보낸 모든 동기화(SYN) 패킷을 삭제하여 다음과 같은 핸드셰이크 변형을 방지합니다. 그림에서 문자 A는 세션 개시자를 나타내고 B는 리스너를 나타냅니다. 핸드셰이크의 번호가 매겨진 각 세그먼트에는 송신자에서 수신자로 세그먼트의 방향을 나타내는 화살표가 있으며 각 세그먼트는 제어 비트 설정을 나타냅니다.

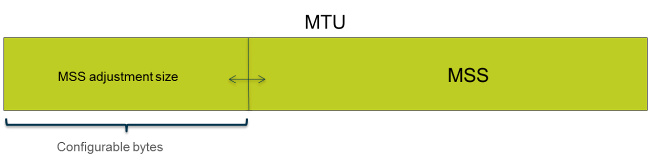
4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

TCP 분할 핸드셰이크 세션 설정을 방지할 수 있습니다.

최대 세그먼트 크기(MSS)

MTU(최대 전송 단위)는 단일 TCP 패킷으로 전송할 수 있는 최대 바이트 수를 나타내는 값입니다. MTU에는 헤더 길이가 포함되므로 MTU에서 헤더의 바이트 수를 뺀 값은 단일 패킷으로 전송할 수 있는 최대 데이터 바이트 수인 최대 세그먼트 크기(MSS)와 같습니다.

구성 가능한 MSS 조정 크기(아래 참조)를 사용하면 방화벽이 기본 설정에서 허용하는 것보다 긴 헤더가 있는 트래픽을 포워딩할 수 있습니다. 캡슐화는 헤더에 길이를 추가하므로, 예를 들어 VLAN 태그가 있는 MPLS 헤더 또는 터널링된 트래픽을 수용하기 위해 바이트를 허용하도록 MSS 조정 크기를 늘립니다.



패킷에 대해 DF(조각화하지 않음) 비트가 설정된 경우 더 긴 헤더로 인해 패킷 길이가 허용된 MTU를 초과하지 않도록 더 큰 MSS 조정 크기와 더 작은 MSS를 갖는 것이 특히 유용합니다. DF 비트가 설정되고 MTU를 초과하면 더 큰 패킷이 삭제됩니다.

패킷에 DF 비트가 설정되어 있더라도 이그레스(egress) 인터페이스 MTU를 초과하는 IPv4 패킷을 분할하도록 방화벽을 전역적으로 구성할 수 있습니다. CLI 명령 ***`debug dataplane set ip4-df-ignore yes`****를 사용하여 레이어 3 물리적 인터페이스 및 IPsec 터널 인터페이스에 대해 이 옵션을 활성화합니다. CLI 명령* ***`debug dataplane set ipv4-df-ignore no`****를 사용하여 방화벽을 기본 동작으로 복원합니다.*

방화벽은 다음 레이어 3 인터페이스 유형에서 IPv4 및 IPv6 주소에 대해 구성 가능한 MSS 조정 크기를 지원합니다. 이더넷, 하위 인터페이스, 통합 이더넷(AE), VLAN 및 루프백. IPv6 MSS 조정 크기는 인터페이스에서 IPv6을 사용하도록 설정한 경우에만 적용됩니다.

인터페이스에서 IPv4 및 IPv6을 사용하도록 설정하고 MSS 조정 크기가 두 IP 주소 형식 간에 다른 경우 IP 유형에 해당하는 적절한 MSS 값이 TCP 트래픽에 사용됩니다.

IPv4 및 IPv6 주소의 경우 방화벽은 예상보다 큰 TCP 헤더 길이를 수용합니다. TCP 패킷의 헤더 길이가 계획한 것보다 큰 경우 방화벽은 MSS 조정 크기로 다음 두 값 중 큰 값을 선택합니다.

- 구성된 MSS 조정 크기
- TCP 헤더의 길이(20) +TCP SYN의 IP 헤더 길이의 합계

이 동작은 필요한 경우 방화벽이 구성된 MSS 조정 크기를 재정의함을 의미합니다. 예를 들어 MSS 조정 크기를 42로 구성하는 경우 MSS는 1458(기본 MTU 크기에서 조정 크기 [1500 - 42]을 뺀 값)과 같을 것으로 예상됩니다. 그러나 TCP 패킷에는 헤더에 추가 4바이트의 IP 옵션이 있으므로 MSS 조정 크기(20+20+4)는 44로 구성된 MSS 조정 크기인 42보다 큽니다. 결과 MSS는 1500-44=1456바이트이며 예상보다 작습니다.

MSS 조정 크기를 구성하려면 세션 설정 구성을 참조하십시오.

UDP

UDP(User Datagram Protocol)(RFC 768)는 IP 제품군의 또 다른 주요 프로토콜이며 TCP의 대안입니다. UDP는 세션을 설정하기 위한 핸드셰이크가 없고 발신자와 수신자 사이에 연결이 없다는 점에서 상태 비저장 및 비연결입니다. 패킷은 단일 목적지에 도달하기 위해 다른 경로를 취할 수 있습니다. UDP는 데이터그램의 승인, 오류 검사, 재전송 또는 재정렬을 제공하지 않기 때문에 신뢰할 수 없는 프로토콜로 간주됩니다. 이러한 기능을 제공하는 데 필요한 오버헤드가 없으면 UDP는 대기 시간을 줄이고 TCP보다 빠릅니다. UDP는 데이터가 목적지에 도착하도록 보장하는 메커니즘이나 보장이 없기 때문에 최선형 프로토콜이라고 합니다.

UDP 데이터그램은 IP 패킷에 캡슐화됩니다. UDP는 데이터 무결성을 위해 체크섬을 사용하지만 네트워크 인터페이스 수준에서는 오류 검사를 수행하지 않습니다. 오류 검사는 불필요한 것으로 간주되거나 UDP 자체가 아닌 애플리케이션에서 수행됩니다. UDP에는 패킷의 흐름 제어를 처리하는 메커니즘이 없습니다.

UDP는 VoIP(Voice over IP), 오디오 및 비디오 스트리밍, 온라인 게임과 같이 더 빠른 속도와 시간에 민감한 실시간 전달이 필요한 애플리케이션에 자주 사용됩니다. UDP는 트랜잭션 지향적이므로 DNS(Domain Name System) 및 TFTP(Trivial File Transfer Protocol)와 같은 많은 클라이언트의 작은 쿼리에 응답하는 애플리케이션에도 사용됩니다.

방화벽의 영역 보호 프로파일을 사용하여 플러드 보호를 구성하고 경보를 트리거하고 UDP 패킷을 무작위로 삭제하도록 방화벽을 트리거하고 방화벽이 삭제되도록 하는 초당 UDP 연결 속도(기존 세션과 일치하지 않음)를 지정할 수 있으며, 최대 속도를 초과하는 UDP 패킷을 낮추는 방화벽의 원인이 됩니다. (UDP는 연결이 없지만 방화벽은 세션 기반으로 IP 패킷의 UDP 데이터그램을 추적합니다. 따라서 UDP 패킷이 기존 세션과 일치하지 않으면 새 세션으로 간주되고 임계값에 대한 연결로 계산됩니다.)

ICMP

ICMP(Internet Control Message Protocol)(RFC 792)는 인터넷 프로토콜 제품군의 또 다른 주요 프로토콜 중 하나입니다. OSI 모델의 네트워크 계층에서 작동합니다. ICMP는 진단 및 제어 목적으로 사용되어 IP 작업에 대한 오류 메시지나, 요청된 서비스나 호스트 또는 라우터의 도달 가능성에 대한 메시지를 보냅니다. traceroute 및 ping과 같은 네트워크 유틸리티는 다양한 ICMP 메시지를 사용하여 구현됩니다.

ICMP는 실제 세션을 열거나 유지하지 않는 비연결형 프로토콜입니다. 그러나 두 디바이스 간의 ICMP 메시지는 세션으로 간주될 수 있습니다.

Palo Alto Networks® 방화벽은 ICMPv4 및 ICMPv6을 지원합니다. 다음과 같은 여러 방법으로 ICMPv4 및 ICMPv6 패킷을 제어할 수 있습니다.

- ICMP 및 ICMPv6 패킷 기반 보안 정책 규칙을(를) 만들고 규칙에서 **icmp** 또는 **ipv6-icmp** 애플리케이션을 선택합니다.
- 세션 설정 구성 수행 시 ICMPv6 속도 제한을(를) 제어합니다.
- 경보를 트리거하는 초당 ICMP 또는 ICMPv6 연결 속도(기존 세션과 일치하지 않음)를 지정하여 Flood Protection을 구성하고, ICMP 또는 ICMPv6 패킷을 무작위로 삭제하도록 방화벽을 트리거하고, 최대 속도를 초과하는 ICMP 또는 ICMPv6 패킷을 방화벽이 삭제하도록 합니다.
- 패킷 기반 공격 보호 구성 패킷 기반 공격 보호:
  - ICMP의 경우 특정 유형의 패킷을 삭제하거나 특정 패킷의 전송을 억제할 수 있습니다.
  - ICMPv6 패킷(유형 1, 2, 3, 4 및 137)의 경우 방화벽이 ICMP 세션 키를 사용하여 ICMPv6 패킷의 허용 여부를 결정하는 보안 정책 규칙과 일치하도록 지정할 수 있습니다. (방화벽은 보안 정책 규칙을 사용하여 세션 일치를 결정하기 위해 포함된 패킷을 사용하는 기본 동작을 무시합니다.) 방화벽이 보안 정책 규칙과 일치하는 ICMPv6 패킷을 삭제하면 방화벽이 트래픽 로그에 세부 정보를 기록합니다.

ICMP 및 ICMPv6 패킷 기반 보안 정책 규칙

방화벽은 보안 정책 규칙이 세션을 허용하는 경우에만 ICMP 또는 ICMPv6 패킷을 포워딩합니다(방화벽이 다른 패킷 유형에 대해 수행하는 방식). 방화벽은 패킷이 ICMP 또는 ICMPv6 오류 패킷인지 또는 ICMP 또는 ICMPv6 정보 패킷이 아닌 리디렉션 패킷인지에 따라 두 가지 방법 중 하나로 세션 일치를 결정합니다.

- **ICMP** 유형 **3, 5, 11** 및 **12** 및 **ICMPv6** 유형 **1, 2, 3, 4** 및 **137** - 기본적으로 방화벽은 오류(호출 패킷)를 일으킨 소스 데이터그램에서 정보의 포함된 IP 패킷 바이트를 조회합니다. 포함된 패킷이 기존 세션과 일치하는 경우 방화벽은 동일한 세션과 일치하는 보안 정책 규칙에 지정된 작업에 따라 ICMP 또는 ICMPv6 패킷을 전달하거나 삭제합니다. (패킷 기반 공격 보호를 사용하여 ICMPv6 유형에 대한 이 기본 동작을 재정의할 수 있습니다.)
- 나머지 **ICMP** 또는 **ICMPv6** 패킷 유형 - 방화벽은 ICMP 또는 ICMPv6 패킷을 새 세션에 속한 것처럼 처리합니다. 보안 정책 규칙이 패킷(방화벽이 **icmp** 또는 **ipv6-icmp** 세션으로 인식)과 일치하는 경우

방화벽은 보안 정책 규칙 작업에 따라 패킷을 포워딩하거나 삭제합니다. 보안 정책 카운터 및 트래픽 로그는 작업을 반영합니다.

패킷과 일치하는 보안 정책 규칙이 없으면 방화벽은 영역 내 트래픽을 허용하고 영역 간 트래픽을 차단하는 기본 보안 정책 규칙을 적용합니다(이러한 규칙에는 기본적으로 로깅이 비활성화되어 있음).

기본 규칙을 재정의하여 로깅을 활성화하거나 기본 작업을 변경할 수 있지만 특정 경우에 대한 기본 동작을 변경하면 해당 기본 규칙이 영향을 미치는 모든 트래픽에 영향을 미치므로 변경하지 않는 것이 좋습니다. 대신 *ICMP* 또는 *ICMPv6* 패킷을 명시적으로 제어하고 기록하는 보안 정책 규칙을 생성합니다.

오류 또는 리디렉션 패킷이 아닌 ICMP 또는 ICMPv6 패킷을 처리하기 위해 명시적 보안 정책 규칙을 만드는 방법에는 두 가지가 있습니다.

- 모든 **ICMP** 또는 **ICMPv6** 패킷을 허용(또는 거부)하는 보안 정책 규칙 생성 - 보안 정책 규칙에서 애플리케이션 **icmp** 또는 **ipv6-icmp**를 지정합니다. 방화벽은 방화벽을 통해 각각 ICMP 프로토콜 번호(1) 또는 ICMPv6 프로토콜 번호(58)와 일치하는 모든 IP 패킷을 허용(또는 거부)합니다.
- 사용자 지정 애플리케이션 및 보안 정책 규칙을 만들어 해당 애플리케이션에서 들어오거나 나가는 패킷을 허용(또는 거부)할 수 있습니다. - 이보다 세분화된 접근 방식을 사용하면 특정 ICMP 또는 ICMPv6 유형 및 코드 제어을(를) 할 수 있습니다.

ICMPv6 속도 제한

ICMPv6 속도 제한은 플러드 및 DDoS 시도를 방지하기 위한 제한 메커니즘입니다. 구현은 오류 패킷 속도와 토큰 버킷을 사용하여 제한을 가능하게 하고 ICMP 패킷이 방화벽으로 보호되는 네트워크 세그먼트를 플러딩하지 않도록 합니다.

먼저 글로벌 **ICMPv6** 오류 패킷 속도(초당)는 방화벽을 통해 ICMPv6 오류 패킷이 허용되는 속도를 제어하며, 기본값은 초당 100패킷이며 범위는 초당 10 ~ 65535패킷입니다. 방화벽이 ICMPv6 오류 패킷 속도에 도달하면 토큰 버킷이 재생되고 다음과 같이 제한이 발생합니다.

논리 토큰 버킷의 개념은 ICMP 메시지를 전송할 수 있는 속도를 제어합니다. 버킷의 토큰 수는 구성할 수 있으며 각 토큰은 보낼 수 있는 ICMPv6 메시지를 나타냅니다. 토큰 수가 ICMPv6 메시지를 보낼 때마다 감소됩니다. 버킷이 0 토큰에 도달하면 다른 토큰이 버킷에 추가될 때까지 ICMPv6 메시지를 더 이상 보낼 수 없습니다. 토큰 버킷의 기본 크기는 100토큰(패킷)입니다. 범위는 10 ~ 65535 토큰입니다.

기본 토큰 버킷 크기 또는 오류 패킷 속도를 변경하려면 세션 설정 구성 섹션을 참조하십시오.

특정 ICMP 또는 ICMPv6 유형 및 코드 제어

이 작업을 사용하여 사용자 지정 ICMP 또는 ICMPv6 애플리케이션을 생성한 다음 해당 애플리케이션을 허용하거나 또는 거부하는 보안 정책 규칙을 생성합니다.

STEP 1 | ICMP 또는 ICMPv6 메시지 유형 및 코드에 대한 사용자 지정 애플리케이션을 생성합니다.

1. 개체 > 애플리케이션을 선택하고 사용자 정의 애플리케이션을 추가합니다.
2. 구성 탭에서 맞춤 애플리케이션의 이름과 설명을 입력합니다. 예를 들어 ping6이라는 이름을 입력합니다.
3. 범주에서 네트워킹을 선택합니다.
4. 하위 범주에 대해 **ip-protocol**을 선택합니다.
5. 기술에 대해 네트워크 프로토콜을 선택합니다.
6. 확인을 클릭합니다.
7. 고급 탭에서 **ICMP** 유형 또는 **ICMPv6** 유형을 선택합니다.
8. 유형에 허용하거나 거부할 ICMP 또는 ICMPv6 메시지 유형을 지정하는 숫자(범위는 0-255)를 입력합니다. 예를 들어 에코 요청 메시지(ping)는 128입니다.
9. 유형에 코드가 포함된 경우 허용하거나 거부하려는 유형 값에 적용되는 코드 번호(범위는 0-255)를 입력합니다. 일부 유형 값에는 코드 0만 있습니다.
10. 확인을 클릭합니다.

STEP 2 | 생성한 사용자 지정 애플리케이션을 허용하거나 또는 거부하는 보안 정책 규칙을 생성합니다.

보안 정책 규칙을 생성합니다. 애플리케이션 탭에서, 방금 생성한 사용자 지정 애플리케이션의 이름을 지정합니다.

STEP 3 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

세션 시간 초과 구성

세션 시간 초과는 세션에서 비활성 후 PAN-OS가 방화벽에서 세션을 유지하는 기간을 정의합니다. 기본적으로 프로토콜의 세션 시간 초과가 만료되면 PAN-OS는 세션을 닫습니다. 특히 TCP, UDP 및 ICMP 세션에 대해 여러 시간 초과를 정의할 수 있습니다. 기본 시간 초과는 다른 유형의 세션에 적용됩니다. 시간 초과는 전역적입니다. 즉, 방화벽에서 해당 유형의 모든 세션에 적용됩니다.

방화벽이 캐시에 ARP 항목(IP 주소-하드웨어 주소 매ping)을 유지하는 기간을 제어하는 전역 ARP 캐시 시간 초과 설정을 구성할 수도 있습니다.

전역 설정 외에도 개체 > 애플리케이션 탭에서 개별 애플리케이션에 대한 시간 초과를 정의할 수 있습니다. 방화벽은 설정된 상태의 애플리케이션에 애플리케이션 시간 초과를 적용합니다. 구성된 경우 애플리케이션의 시간 초과는 전역 TCP 또는 UDP 세션 시간 초과를 재정의합니다.

애플리케이션 수준에서 ***TCP*** 또는 ***UDP*** 타이머를 변경하면 미리 정의된 애플리케이션 및 공유 사용자 지정 애플리케이션에 대한 이러한 타이머가 모든 가상 시스템에서 구현됩니다. 가상 시스템에 대해 애플리케이션의 타이머가 달라야 하는 경우 사용자 지정 애플리케이션을 만들고 고유한 타이머를 할당한 다음 사용자 지정 애플리케이션을 고유한 가상 시스템에 할당해야 합니다.

TCP, UDP, ICMP, Captive Portal 인증 또는 기타 유형의 세션에 대한 전역 세션 시간 초과 설정의 기본값을 변경해야 하는 경우 다음 작업을 수행하십시오. 모든 값은 초 단위입니다.

기본값은 최적 값입니다. 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.

STEP 1 | 세션 시간 초과에 액세스합니다.

디바이스 > 설정 > 세션을 선택하고 세션 시간 초과를 편집합니다.

STEP 2 | (선택 사항) 기타 시간 초과를 변경합니다.

- 기본값 - 비 TCP/UDP 또는 비 ICMP 세션이 응답 없이 열릴 수 있는 최대 시간 길이입니다(범위는 1~15,999,999, 기본값은 30).
- 기본값 삭제 - PAN-OS가 방화벽에 구성된 보안 정책을 기반으로 세션을 거부한 후 비 TCP/UDP 세션이 열린 상태로 유지되는 최대 시간(범위는 1~15,999,999, 기본값은 60)입니다.
- 스캔 - 세션이 비활성으로 간주된 후 열려 있는 최대 시간입니다. 애플리케이션에 대해 정의된 애플리케이션 살수 임계값을 초과하면 애플리케이션이 비활성화된 것으로 간주됩니다(범위는 5~30, 기본값은 10).
- 인증 포털 - Captive Portal 웹 양식에 대한 인증 세션 시간 초과입니다. 요청된 콘텐츠에 액세스하려면 사용자가 이 양식에 인증 자격 증명을 입력하고 성공적으로 인증되어야 합니다(범위는 1~15,999,999, 기본값은 30).
- 유휴 타이머 및 사용자를 다시 인증해야 하는 만료 시간과 같은 다른 인증 포털 시간 초과를 정의하려면 디바이스 > 사용자 식별 > 인증 포털 설정을 선택합니다. 인증 포털 구성을 참조하십시오.

STEP 3 | (선택 사항) TCP 시간 초과를 변경합니다.

- **Discard TCP** - TCP 세션이 방화벽에 구성된 보안 정책에 따라 거부된 후 열린 상태로 유지되는 최대 시간입니다. 범위는 1~15,999,999입니다. 기본값은 90입니다.
- **TCP** - TCP 세션이 설정됨 상태(핸드셰이크가 완료된 후 및/또는 데이터가 전송된 후)가 된 후 응답 없이 TCP 세션이 열려 있는 최대 시간입니다. 범위는 1~15,999,999입니다. 기본값은 3,600입니다.
- **TCP** 핸드셰이크 - 세션을 완전히 설정하기 위해 SYN-ACK 수신과 후속 ACK 사이에 허용되는 최대 시간입니다. 범위는 1~60입니다. 기본값은 10입니다.
- **TCP** 초기화 - TCP 핸드셰이크 타이머를 시작하기 전에 SYN과 SYN-ACK 수신 사이에 허용되는 최대 시간입니다. 범위는 1~60입니다. 기본값은 5입니다.
- **TCP Half Closed** - 첫 번째 FIN 수신과 두 번째 FIN 또는 RST 수신 사이의 최대 시간입니다. 범위는 1~604,800입니다. 기본값은 120입니다.
- **TCP** 시간 대기 - 두 번째 FIN 또는 RST를 수신한 후의 최대 시간입니다. 범위는 1~600입니다. 기본값은 15입니다.
- 확인되지 않은 **RST** - 확인할 수 없는 RST를 수신한 후 최대 시간 길이(RST가 TCP 창 내에 있지만 예기치 않은 시퀀스 번호가 있거나 RST가 비대칭 경로에서 온 경우). 범위는 1~600입니다. 기본값은 30입니다.
- (선택 사항) 기타 시간 초과 변경 섹션에서 검색시간 초과를 참조하십시오.

STEP 4 | (선택 사항) UDP 시간 초과를 변경합니다.

- **Discard UDP** - UDP 세션이 방화벽에 구성된 보안 정책에 따라 거부된 후 열린 상태로 유지되는 최대 시간입니다. 범위는 1~15,999,999입니다. 기본값은 60입니다.
- **UDP** - UDP 세션이 UDP 응답 없이 열려 있는 최대 시간입니다. 범위는 1~15,999,999입니다. 기본값은 30입니다.
- (선택 사항) 기타 시간 초과 변경 섹션에서 검색시간 초과를 참조하십시오.

STEP 5 | (선택 사항) ICMP 시간 초과를 변경합니다.

- **ICMP** - ICMP 응답 없이 ICMP 세션을 열 수 있는 최대 시간입니다. 범위는 1~15,999,999입니다. 기본값은 6입니다.
- (선택 사항) 기타 시간 초과 변경 섹션에서 기본값 삭제 및 검색 시간 초과를 참조하십시오.

STEP 6 | 확인 및 커밋을 클릭합니다.

STEP 7 | (선택 사항) ARP 캐시 시간 초과를 변경합니다.

1. CLI에 액세스하고 방화벽이 캐시에 ARP 항목을 보관하는 시간(초)을 지정합니다. 작동 명령 **`set system setting arp-cache-timeout`** <*value*>를 사용합니다. 여기서 범위는 60 ~ 65,535입니다. 기본값은 1,800입니다.

   시간 초과를 줄이고 캐시의 기존 항목에 새 시간 초과보다 큰 TTL이 있는 경우 방화벽은 해당 항목을 제거하고 ARP 캐시를 새로 고칩니다. 시간 초과를 늘리고 기존 항목의 TTL이 새 시간 초과보다 작으면 TTL에 따라 만료되고 방화벽은 더 큰 시간 초과 값으로 새 전체를 캐시합니다.
2. 작동 가능한 CLI 명령 **`show system setting arp-cache-timeout`**을 사용하여 ARP 캐시 시간 초과 설정을 확인합니다.

세션 설정 구성

이 항목에서는 시간 초과 값 이외의 세션에 대한 다양한 설정에 대해 설명합니다. 기본 설정을 변경해야 하는 경우 다음 작업을 수행하십시오.

STEP 1 | 세션 설정을 변경합니다.

디바이스 > 설정 > 세션을 선택하고 세션 설정을 편집합니다.

STEP 2 | 진행 중인 세션에 새로 구성된 보안 정책 규칙을 적용할지 여부를 지정합니다.

새로 구성된 보안 정책 규칙을 이미 진행 중인 세션에 적용하려면 구성 정책 변경 시 모든 세션 다시 일치를 선택합니다. 이 기능은 기본적으로 활성화되어 있습니다. 이 확인란의 선택을 취소하면 정책 규칙 변경 사항이 정책 변경 사항을 커밋한 후에 시작된 세션에만 적용됩니다.

예를 들어 Telnet을 허용하는 연결된 정책 규칙이 구성된 동안 Telnet 세션이 시작되었고 이후에 Telnet을 거부하는 정책 변경을 커밋한 경우 방화벽은 수정된 정책을 현재 세션에 적용하고 차단합니다.

STEP 3 | IPv6 설정을 구성합니다.

- **ICMPv6** 토큰 버킷 크기 - 기본값: 토큰 100개. ICMPv6 속도 제한 섹션을 참조하십시오.
- **ICMPv6** 오류 패킷 속도**(**초당**)** - 기본값: 100. ICMPv6 속도 제한 섹션을 참조하십시오.
- **IPv6** 방화벽 활성화 - IPv6에 대한 방화벽 기능을 활성화합니다. IPv6이 활성화되지 않은 경우 모든 IPv6 기반 구성이 무시됩니다. 인터페이스에 대해 IPv6이 활성화된 경우에도 IPv6이 작동하려면 **IPv6** 방화벽 설정도 활성화되어야 합니다.

STEP 4 | 점보 프레임을 활성화하고 MTU를 설정합니다.

1. 이더넷 인터페이스에서 점보 프레임 지원을 활성화하려면 점보 프레임 활성화를 선택합니다. 점보 프레임의 최대 전송 단위(MTU)는 9,216바이트이며 특정 모델에서 사용할 수 있습니다.
2. 점보 프레임을 활성화했는지 여부에 따라 전역 **MTU**를 설정합니다.
   - 점보 프레임을 활성화하지 않은 경우 전역 **MTU**의 기본값은 1,500바이트입니다. 범위는 576~1,500바이트입니다.
   - 점보 프레임을 활성화한 경우 전역 **MTU**의 기본값은 9,192바이트입니다. 범위는 9,192~9,216바이트입니다.

   > *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 비순차 적***,** *애플리케이션 식별 및 기타 패킷 처리 작업 전용 대기열 크기가 줄어듭니다***.** ***PAN-OS 8.1****부터 점보 프레임 전역* ***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 자동으로 점보 프레임 크기를 상속합니다. 따라서 점보 프레임을 활성화하기 전에 점보

프레임을 원하지 않는 인터페이스가 있는 경우 해당 인터페이스의 MTU를 1500바이트 또는 다른 값으로 설정해야 합니다.

점보 프레임이 활성화된 구성을 가져오고(**디바이스 > 설정 > 작업 > 가져오기**) 로드한 다음 아직 점보 프레임이 활성화되지 않은 방화벽에 커밋하면 점보 프레임 활성화 설정이 구성에 커밋되지 않습니다. 먼저 점보 프레임을 활성화하고 재부팅한 다음 구성을 가져오고 로드하고 커밋해야 합니다.

STEP 5 | NAT 세션 설정을 조정합니다.

- **NAT64 IPv6** 최소 네트워크 **MTU** - IPv6 변환 트래픽에 대한 전역 MTU를 설정합니다. 기본값인 1,280바이트는 IPv6 트래픽에 대한 표준 최소 MTU를 기반으로 합니다.
- **NAT** 초과 가입 비율 - NAT가 DIPP(동적 IP 및 포트) 변환으로 구성된 경우 초과 가입 비율은 동일한 변환된 IP 주소 및 포트 쌍을 동시에 사용할 수 있는 횟수를 곱하도록 구성할 수 있습니다. 비율은 1, 2, 4 또는 8입니다. 기본 설정은 방화벽 모델을 기반으로 합니다.
- 1의 비율은 초과 구독이 없음을 의미합니다. 변환된 각 IP 주소와 포트 쌍은 한 번에 한 번만 사용할 수 있습니다.
- 설정이 플랫폼 기본값인 경우 요금의 사용자 구성이 비활성화되고 모델에 대한 기본 초과 구독 요금이 적용됩니다.

초과 구독 비율을 줄이면 소스 디바이스 변환 수가 줄어들지만 더 높은 NAT 규칙 용량을 제공합니다.

STEP 6 | 가속 노화 설정을 조정합니다.

유휴 세션의 더 빠른 에이징을 활성화하려면 **Accelerated Aging**을 선택합니다. 임계값(%) 및 배율 인수를 변경할 수도 있습니다.

- 가속화된 에이징 임계값 - 가속화된 에이징이 시작될 때 가득 찬 세션 테이블의 백분율입니다. 기본값은 80%입니다. 세션 테이블이 이 임계값(% full)에 도달하면 PAN-OS는 모든 세션에 대한 에이징 계산에 Accelerated Aging Scaling Factor를 적용합니다.
- **Accelerated Aging Scaling Factor** - 가속 에이징 계산에 사용되는 스케일링 계수. 기본 배율 인수는 2이며, 이는 구성된 유휴 시간보다 두 배 빠른 속도로 노화가 가속화됨을 의미합니다. 구성된 유휴 시간을 2로 나누면 시간 초과가 1/2로 빨라집니다. 세션의 가속화된 에이징을 계산하기 위해 PAN-OS는 구성된 유휴 시간(해당 세션 유형에 대해)을 배율 인수로 나누어 더 짧은 시간 초과를 결정합니다.

예를 들어, 배율 인수가 10인 경우 일반적으로 3600초 후에 시간 초과되는 세션은 10배 더 빠른 시간 초과(시간의 1/10), 즉 360초가 됩니다.

STEP 7 | 패킷 버퍼 보호를 활성화합니다.

1. 패킷 버퍼를 압도하고 합법적인 트래픽이 삭제되도록 하는 세션에 대해 방화벽이 조치를 취하도록 하려면 패킷 버퍼 보호를 선택하십시오. 기본적으로 활성화되어 있습니다.
2. 패킷 버퍼 보호를 활성화하면 방화벽이 패킷 버퍼 남용에 대응하는 방식을 지시하는 임계값과 타이머를 조정할 수 있습니다.

   - 경고**(%)**: 패킷 버퍼 사용률이 이 임계값을 초과하면 방화벽이 로그 이벤트를 생성합니다. 임계값은 기본적으로 50%로 설정되며 범위는 0%에서 99%입니다. 값을 0%로 설정하면 방화벽이 로그 이벤트를 생성하지 않습니다.
   - 활성화**(%)**: 패킷 버퍼 사용률이 이 임계값을 초과하면 방화벽은 악의적인 세션에 RED(임의 조기 삭제)를 적용합니다. 임계값은 기본적으로 80%로 설정되며 범위는 0%에서 99%입니다. 값을 0%로 설정하면 방화벽이 RED를 적용하지 않습니다.

   경고 이벤트는 시스템 로그에 기록됩니다. 삭제된 트래픽, 폐기된 세션 및 차단된 *IP* 주소에 대한 이벤트는 위협 로그에 기록됩니다.

   - 블록 유지 시간**(**초**)**: RED 완화 세션이 삭제되기 전에 계속될 수 있는 시간입니다. 기본적으로 블록 유지 시간은 60초입니다. 범위는 0~65,535초입니다. 값이 0으로 설정되면 방화벽은 패킷 버퍼 보호를 기반으로 세션을 삭제하지 않습니다.
   - 차단 기간**(**초**)**: 이 설정은 세션이 삭제되거나 IP 주소가 차단되는 기간을 정의합니다. 기본값은 0초에서 15,999,999초 사이의 3,600초입니다. 이 값이 0으로 설정되면 방화벽은 패킷 버퍼 보호를 기반으로 세션을 삭제하거나 IP 주소를 차단하지 않습니다.

STEP 8 | 멀티캐스트 경로 설정 패킷의 버퍼링을 활성화합니다.

1. 멀티캐스트 경로 설정 버퍼링을 선택하면 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. 이 옵션은 기본적으로 비활성화되어 있습니다.
2. 버퍼링을 활성화하면 흐름당 버퍼 크기를 지정하는 버퍼 크기를 조정할 수도 있습니다. 방화벽은 최대 5,000개의 패킷을 버퍼링할 수 있습니다.

   가상 라우터를 처리하는 가상 라우터에서 멀티캐스트 설정을 구성하여 멀티캐스트 경로 만료 시간 설정**(**초**)** 가상 라우터 구성의 멀티캐스트 **>** 고급 탭에서 세션이 끝난 후 방화벽의 라우팅 테이블에 멀티캐스트 경로가 남아 있는 기간**(**초**)**을 조정할 수도 있습니다.

STEP 9 | 세션 설정을 저장합니다.

확인을 클릭합니다.

STEP 10 | 레이어 3 인터페이스에 대한 최대 세그먼트 크기(MSS) 조정 크기 설정을 조정합니다.

1. 네트워크 > 인터페이스를 선택하고 이더넷, **VLAN** 또는 루프백을 선택한 다음 레이어 3 인터페이스를 선택합니다.
2. 고급 > 기타 정보를 선택합니다.
3. **TCP MSS** 조정을 선택하고 다음 중 하나 또는 둘 모두에 대한 값을 입력합니다.
   - **IPv4 MSS** 조정 크기(범위는 40~300바이트, 기본값은 40바이트).
   - **IPv6 MSS** 조정 크기(범위는 60~300바이트, 기본값은 60바이트).
4. 확인을 클릭합니다.

STEP 11 | 변경 사항을 커밋합니다.

커밋을 클릭합니다.

STEP 12 | 점보 프레임 구성을 변경한 후 방화벽을 재부팅합니다.

1. 디바이스 > 설정 > 작업을 선택합니다.
2. 디바이스 재부팅을 클릭합니다.

세션 배포 정책

세션 배포 정책은 PA-5200 및 PA-7000 시리즈 방화벽이 방화벽의 데이터 플레인 프로세서(DP) 간에 보안 처리(앱 ID, 콘텐츠 ID, URL 필터링, SSL 복호화 및 IPsec)를 배포하는 방법을 정의합니다. 각 정책은 특정 유형의 네트워크 환경 및 방화벽 구성을 위해 특별히 설계되어 방화벽이 세션을 최대한의 효율성으로 배포할 수 있도록 합니다. 예를 들어 해시 세션 배포 정책은 대규모 소스 NAT를 사용하는 환경에 가장 적합합니다.

방화벽의 DP 수는 방화벽 모델에 따라 다릅니다.

방화벽 모델	데이터플레인 프로세서
PA-7000 시리즈	설치된 NPC(네트워크 처리 카드)의 수에 따라 다릅니다. 각 NPC에는 여러 DP(데이터 플레인 프로세서)가 있으며 방화벽에 여러 NPC를 설치할 수 있습니다.
PA-5220 방화벽	1 ***PA-5220** 방화벽에는 **DP**가 하나만 있으므로 세션 배포 정책이 적용되지 않습니다. 정책을 기본값(라운드 로빈)으로 설정한 상태로 둡니다.*
PA-5250 방화벽	2
PA-5260 및 PA-5280 방화벽	3
PA-5450 방화벽	설치된 데이터 처리 카드(DPC)의 수에 따라 다릅니다.

다음 항목에서는 사용 가능한 세션 배포 정책, 활성 정책을 변경하는 방법 및 세션 배포 통계를 보는 방법에 대한 정보를 제공합니다.

- 세션 배포 정책 설명
- 세션 배포 정책 변경 및 통계 보기

세션 배포 정책 설명

다음 표에서는 사용자의 환경과 방화벽 구성에 가장 적합한 정책을 결정하는 데 도움이 되는 세션 배포 정책에 대한 정보를 제공합니다.

세션 배포 정책	설명
고정	방화벽이 보안 처리에 사용할 데이터플레인 프로세서(DP)를 지정할 수 있습니다.

세션 배포 정책	설명
	디버깅 목적으로 이 정책을 사용합니다.
해시	방화벽은 소스 주소 또는 대상 주소의 해시를 기반으로 세션을 배포합니다. 해시 기반 배포는 잠재적인 IP 주소 또는 포트 충돌을 방지하여 NAT 주소 리소스 관리의 효율성을 향상시키고 NAT 세션 설정의 대기 시간을 줄입니다. 동적 IP 변환이나 동적 IP 및 포트 변환 또는 둘 다를 사용하는 대규모 소스 NAT를 사용하는 환경에서 이 정책을 사용합니다. 동적 IP 변환을 사용하는 경우 **소스** 주소 옵션을 선택합니다. 동적 IP 및 포트 변환을 사용하는 경우 **대상** 주소 옵션을 선택합니다.
인그레스(ingress) 슬롯(PA-7000 시리즈 방화벽의 기본값)	(PA-7000 시리즈 방화벽만 해당) 세션의 첫 번째 패킷이 도착한 동일한 NPC의 DP에 새 세션이 할당됩니다. DP 선택은 세션 로드 알고리즘을 기반으로 하지만, 이 경우 세션은 수신 NPC의 DP로 제한됩니다. 트래픽 및 네트워크 토폴로지에 따라 이 정책은 일반적으로 트래픽이 스위치 패브릭을 통과해야 할 가능성을 줄입니다. 수신 및 송신 모두 동일한 NPC에 있는 경우 이 정책을 사용하여 지연 시간을 줄입니다. 방화벽에 NPC(예: PA-7000 20G 및 PA-7000 20GXM)가 혼합되어 있는 경우 이 정책은 증가된 용량을 해당 NPC로 분리하여 NPC 장애의 영향을 격리할 수 있습니다.
임의	방화벽은 세션 처리를 위해 DP를 임의로 선택합니다.
라운드 로빈(PA-5200 시리즈 방화벽의 기본값)	방화벽은 입력, 출력 및 보안 처리 기능이 모든 데이터플레인 간에 공유되도록 활성 데이터플레인 간의 라운드 로빈 알고리즘을 기반으로 데이터플레인 프로세서를 선택합니다. 간단하고 예측 가능한 로드 밸런싱 알고리즘으로 충분할 정도로 수요가 낮은 환경에서 이 정책을 사용합니다. 수요가 많은 환경에서는 세션 로드 알고리즘을 사용하는 것이 좋습니다.
세션 로드	이 정책은 라운드 로빈 정책과 유사하지만 가중치를 기반으로 한 알고리즘을 사용하여 DP 간의 균형을 이루기 위해 세션을 분산하는 방법을 결정합니다. 세션 수명 주기가 다양하기 때문에 DP에 항상 동일한 부하가 발생하지는 않을 수 있습니다. 예를 들어 방화벽에 3개의 DP가 있고 DP0의 용량이 25% 이고 DP1이 25% 이고 DP2가 50% 인 경우 새 세션 할당은 용량이 더 낮은 DP에 가중치가 부여됩니다. 따라서 시간이 지남에 따라 로드 밸런싱을 개선할 수 있습니다

세션 배포 정책	설명
	슬롯 간 집계 인터페이스 그룹 또는 비대칭 포워딩이 있는 환경과 같이 세션이 여러 NPC 슬롯에 분산되는 환경에서 이 정책을 사용합니다. 방화벽에 세션 용량이 다른 NPC 조합(예: PA-7000 20G 및 PA-7000 20GXM NPC의 조합)이 있는 경우에도 이 정책 또는 인그레스(ingress) 슬롯 정책을 사용할 수 있습니다.
대칭-해시	(PAN-OS 8.0 이상을 실행하는 PA-5200 시리즈 및 PA-7000 시리즈 방화벽) 방화벽은 정렬된 소스 및 대상 IP 주소의 해시로 DP를 선택합니다. 이 정책은 방화벽이 NAT를 사용하지 않는다고 가정할 때 서버 간(s2c) 및 클라이언트-서버(c2s) 트래픽에 대해 동일한 결과를 제공합니다. 수요가 많은 IPsec 또는 GTP 배포에서 이 정책을 사용합니다. 이러한 프로토콜을 사용하면 각 방향이 플로우 튜플이 서로 파생될 수 없는 단방향 플로우로 처리됩니다. 이 정책은 양방향이 동일한 DP에 할당되도록 하여 성능을 향상시키고 대기 시간을 줄여 DP 간 통신이 필요하지 않습니다.

세션 배포 정책 변경 및 통계 보기

다음 표에서는 활성 세션 배포 정책을 보고 변경하는 방법과 방화벽의 각 DP(데이터플레인 프로세서)에 대한 세션 통계를 보는 방법을 설명합니다.

업무	명령

활성 세션 배포 정책을 표시합니다.	**`show session distribution policy`** 명령을 사용하여 활성 세션 배포 정책을 봅니다.
	
	다음 출력은 인그레스 슬롯 배포 정책이 활성화된 슬롯 2, 10, 11 및 12에 4개의 NPC가 설치된 PA-7080 방화벽에서 나온 것입니다.
	
	`> show session distribution policy`
	
	`Ownership Distribution Policy: ingress-slot`
	
	`Flow Enabled Line Cards: [2, 10, 11, 12]Packet Processing Enabled Line Cards: [2, 10, 11, 12]`

활성 세션 배포 정책을 변경합니다.	**`set session distribution-policy <policy>`** 명령을 사용하여 활성 세션 배포 정책을 변경합니다. 예를 들어 세션 로드 정책을 선택하려면 다음 명령을 입력합니다.

업무	명령
	`> set session distribution-policy session-load`
세션 배포 통계를 봅니다.	**show session distribution statistics** 명령을 사용하여 방화벽의 데이터플레인 프로세서(DP)와 각 활성 DP의 세션 수를 확인합니다. 다음 출력은 PA-7080 방화벽에서 불러온 것입니다. `> show session distribution statistics DP Active Dispatched Dispatched/sec ------------------------------------------ s1dp0 78698 7829818 1473 s1dp1 78775 7831384 1535 s3dp0 7796 736639 1488 s3dp1 7707 737026 1442` **DP 활성 열**에는 설치된 NPC의 각 데이터플레인이 나열됩니다. 처음 두 문자는 슬롯 번호를 나타내고 마지막 세 문자는 데이터플레인 번호를 나타냅니다. 예를 들어 s1dp0은 슬롯 1의 NPC에 있는 데이터 플레인 0을 나타내고 s1dp1은 슬롯 1의 NPC에 있는 데이터 플레인 1을 나타냅니다. `Dispatched` 열은 방화벽이 마지막으로 재부팅된 이후 데이터플레인이 처리한 총 세션 수를 표시합니다. `Dispatched/sec` 열은 디스패치 비율을 나타냅니다. `Dispatched` 열에 숫자를 추가하면 총계는 방화벽의 활성 세션 수와 같습니다. **show session info CLI** 명령을 실행하여 활성 세션의 총 수를 볼 수도 있습니다. *PA-5200* 시리즈 방화벽 출력은 *DP* 수가 모델에 따라 다르고 *NPC* 슬롯*(s1)*이 하나뿐이라는 점을 제외하면 비슷합니다.

TCP 분할 핸드셰이크 세션 설정 방지

표준 3방향 핸드셰이크를 사용하지 않는 한 TCP 세션이 설정되지 않도록 영역 보호 프로파일에서 TCP 분할 핸드셰이크 드롭을 구성할 수 있습니다. 이 작업에서는 TCP 분할 핸드셰이크가 세션을 설정하지 못하도록 하려는 인터페이스에 대한 보안 영역을 할당했다고 가정합니다.

STEP 1 | 3방향 핸드셰이크 이외의 다른 방법을 사용하여 세션을 설정하는 TCP 세션을 방지하도록 영역 보호 프로파일을 구성합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택하고 새 프로파일 추가(또는 기존 프로파일 선택)를 선택합니다.
2. 새 프로파일을 생성하는 경우 프로파일의 이름 및 설명(선택 사항)을 입력합니다.
3. 패킷 기반 공격 보호 > **TCP** 삭제를 선택하고 핸드셰이크 분할을 선택합니다.
4. 확인을 클릭합니다.

STEP 2 | 프로파일을 하나 이상의 보안 영역에 적용합니다.

1. 네트워크 > 영역을 선택하고 영역 보호 프로파일을 할당할 영역을 선택합니다.
2. 영역 창의 영역 보호 프로파일목록에서 이전 단계에서 구성한 프로파일을 선택합니다.

   또는 영역 보호 프로파일을 클릭하여 여기에서 새 프로파일 만들기를 시작할 수 있습니다. 이 경우 계속 진행합니다.
3. 확인을 클릭합니다.
4. (선택 사항) 추가 영역에 프로파일을 적용하려면 1-3단계를 반복합니다.

STEP 3 | 변경 사항을 커밋합니다.

확인 및 커밋을 클릭합니다.

터널 콘텐츠 검사

방화벽은 터널을 종료하지 않고 일반 텍스트 터널 프로토콜의 트래픽 내용을 검사할 수 있습니다.

- 일반 라우팅 캡슐화(GRE)(RFC 2784)
- 암호화되지 않은 IPSec 트래픽 [IPSec(RFC 2410) 및 전송 모드 AH IPSec에 대한 NULL 암호화 알고리즘]
- GPRS(General Packet Radio Service) 사용자 데이터용 터널링 프로토콜(GTP-U)
- 가상 확장 가능 근거리 통신망(VXLAN)(RFC 7348)

> 터널 콘텐츠 검사는 암호화된 트래픽을 전달하는 ***VPN*** 또는 ***LSVPN*** 터널이 아닌 일반 텍스트 터널을 위한 것입니다.

터널 콘텐츠 검사를 사용하여 이러한 유형의 터널의 트래픽과 다른 평문 터널(예: GRE 터널 내부의 Null 암호화 IPSec 터널) 내에 중첩된 트래픽에 대한 보안, DoS 보호 및 QoS 정책을 시행할 수 있습니다. ACC에서 터널 검사 로그 및 터널 활동을 보고 터널링된 트래픽이 회사 보안 및 사용 정책을 준수하는지 확인할 수 있습니다.

모든 방화벽 모델은 GRE, 암호화되지 않은 IPSec 및 VXLAN 프로토콜에 대한 터널 콘텐츠 검사를 지원합니다. GTP 보안을 지원하는 방화벽만 GTP-U 터널 콘텐츠 검사를 지원합니다. 호환성 매트릭스에서 GTP 및 SCTP 보안을 지원하는 모델별 PAN-OS 릴리스를 참조하십시오.

디폴트로 지원되는 방화벽은 터널 가속을 수행하여 GRE 터널, VXLAN 터널 및 GTP-U 터널을 통과하는 트래픽의 성능과 처리량을 개선합니다. 터널 가속은 하드웨어 오프로딩을 제공하여 흐름 조회를 수행하는 데 걸리는 시간을 줄이고 터널 트래픽이 내부 트래픽을 기반으로 보다 효율적으로 분산되도록 합니다. 그러나 터널 가속 비활성화을(를) 사용하여 문제를 해결할 수 있습니다.

- 터널 콘텐츠 검사 개요
- 터널 콘텐츠 검사 구성
- 검사된 터널 활동 보기
- 로그에서 터널 정보 보기
- 태그가 지정된 터널 트래픽을 기반으로 사용자 지정 보고서 만들기
- 터널 가속 비활성화

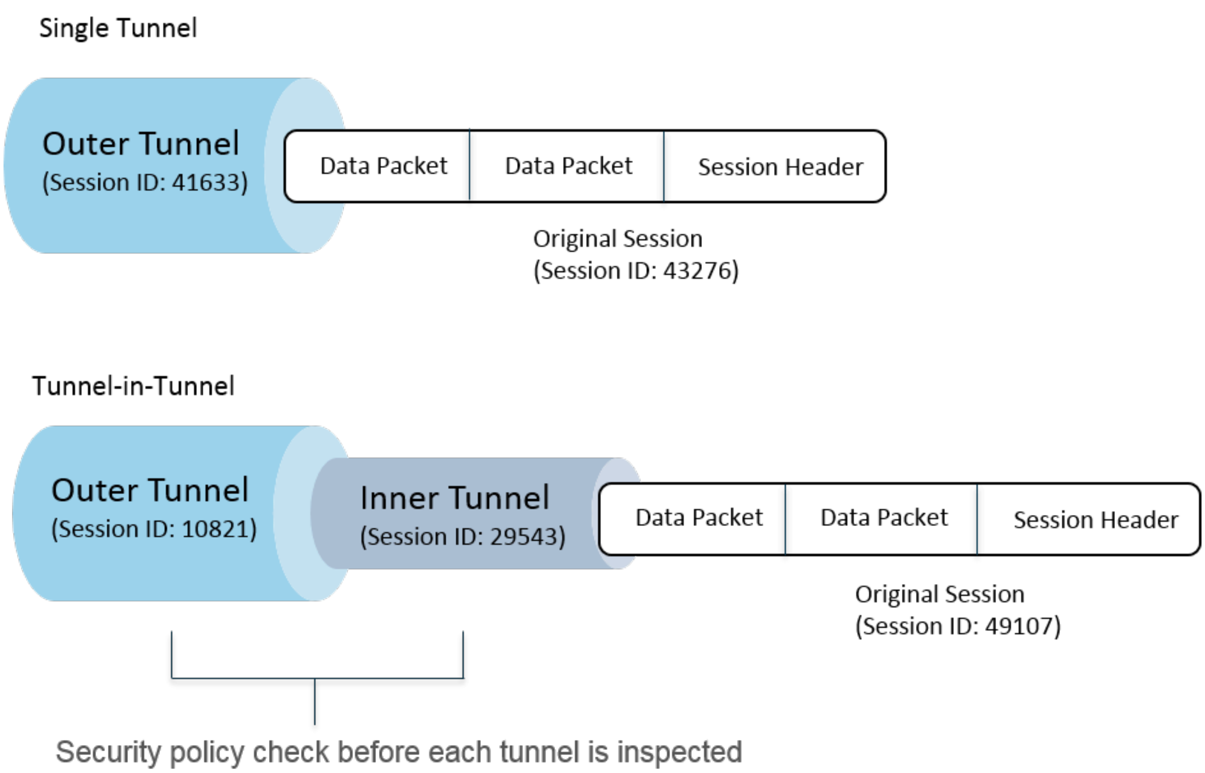
터널 콘텐츠 검사 개요

방화벽은 먼저 터널을 종료할 기회가 없는 네트워크의 어느 곳에서든 터널 콘텐츠를 검사할 수 있습니다. 방화벽이 GRE, 암호화되지 않은 IPSec, GTP-U 또는 VXLAN 터널의 경로에 있는 한 방화벽은 터널 콘텐츠를 검사할 수 있습니다.

- 터널 콘텐츠 검사를 원하는 엔터프라이즈 고객은 GRE, VXLAN 또는 암호화되지 않은 IPSec를 사용하여 방화벽의 트래픽 일부 또는 전부를 가질 수 있습니다. 보안, QoS 및 보고상의 이유로 터널 내부의 트래픽을 검사하려고 합니다.
- 서비스 공급자 고객은 GTP-you를 사용하여 모바일 디바이스에서 데이터 트래픽을 터널로 처리합니다. 터널 프로토콜을 종료하지 않고 내부 콘텐츠를 검사하고 사용자의 사용자 데이터를 기록하려고 합니다.

방화벽은 이더넷 인터페이스, 하위 인터페이스, AE 인터페이스, VLAN 인터페이스, VPN 및 LSVPN 터널 인터페이스에 대한 터널 콘텐츠 검사를 지원합니다. (방화벽이 검사하는 클리어텍스트 터널은 방화벽에서 종료되는 VPN 또는 LSVPN 터널 내부에 있을 수 있으므로 VPN 또는 LSVPN 터널 인터페이스가 가능합니다. 즉, 방화벽이 VPN 또는 LSVPN 엔드포인트인 경우 방화벽은 터널 콘텐츠 검사가 지원하는 암호화되지 않은 터널 프로토콜의 트래픽을 검사할 수 있습니다.)

터널 콘텐츠 검사는 레이어 3, 레이어 2, 가상 와이어 및 탭 배포에서 지원됩니다. 터널 콘텐츠 검사는 공유 게이트웨이 및 가상 시스템 대 가상 시스템 통신에서 작동합니다.



앞그림은 방화벽이 수행할 수 있는 두 단계의 터널 검사 수준을 보여 줍니다. 터널 검사 정책 규칙으로 구성된 방화벽이 패킷을 수신하는 경우:

- 방화벽은 먼저 보안 정책 검사를 수행하여 패킷의 터널 프로토콜(애플리케이션)이 허용되는지 또는 거부되는지 여부를 확인합니다. (IPv4 및 IPv6 패킷은 터널 내부에서 지원되는 프로토콜입니다.)
- 보안 정책이 패킷을 허용하는 경우 방화벽은 패킷을 소스 영역, 소스 주소, 소스 사용자, 대상 존 및 대상 주소를 기반으로 하는 터널 검사 정책 규칙에 일치시킵니다. 터널 검사 정책 규칙은 방화벽이 검사하는 터널 프로토콜, 허용되는 최대 캡슐화 수준(단일 터널 또는 터널 내터널)을 결정하며, RFC 2780당, 엄격한 헤더 검사를 통과하지 못하는 터널 프로토콜이 포함된 패킷을 허용할지 여부, 알 수 없는 프로토콜을 포함하는 패킷을 허용할지 여부를 결정합니다.
- 패킷이 터널 검사 정책 규칙의 일치 기준을 통과하는 경우 방화벽은 보안 정책(필수)과 지정할 수 있는 선택적 정책의 적용을 받는 내부 콘텐츠를 검사합니다. 원래 세션에 대해 지원되는 정책 형식이 다음 표에 나열됩니다.
- 방화벽이 다른 터널을 찾은 경우 방화벽은 두 번째 헤더에 대한 패킷을 재귀적으로 구문 분석하고 현재 캡슐화의 수준 2에 있으므로, 터널 영역과 일치하는 두 번째 터널 검사 정책 규칙은 방화벽이 패킷을 계속 처리하기 위해 두 수준의 최대 터널 검사 수준을 허용해야 합니다.
  - 규칙에 두 가지 수준의 검사를 허용하는 경우 방화벽은 이 내부 터널에 대한 보안 정책 검사를 수행한 다음 터널 검사 정책 검사를 수행합니다. 내부 터널에서 사용하는 터널 프로토콜은 외부 터널에서 사용하는 터널 프로토콜과 다를 수 있습니다.
  - 규칙에 두 가지 수준의 검사가 허용되지 않는 경우 방화벽은 구성한 최대 터널 검사 수준보다 캡슐화 수준이 더 높은 패킷을 삭제하도록 구성했는지 여부에 대한 작업을 기반으로 합니다.

기본적으로 터널에 캡슐화된 콘텐츠는 터널과 동일한 보안 영역에 속하며 해당 영역을 보호하는 보안 정책 규칙의 적용을 받습니다. 그러나 터널 존을 구성할 수 있으므로 터널의 보안 정책 규칙과 다른 내부 콘텐츠에 대한 보안 정책 규칙을 구성할 수 있습니다. 터널 존에 대해 다른 터널 검사 정책을 사용하는 경우 방화벽이 두 번째 캡슐화를 보고 있기 때문에 항상 두 수준의 최대 터널 검사 수준이 있어야 합니다.

방화벽은 방화벽에서 종료되는 터널의 트래픽과 일치하는 터널 검사 정책 규칙을 지원하지 않습니다. 방화벽은 내부 터널 세션과 일치하는 패킷을 삭제합니다. 예를 들어 방화벽에서 IPSec 터널이 종료되면, 종료하는 터널과 일치하는 터널 검사 정책 규칙을 만들지 마십시오. 방화벽은 이미 내부 터널 트래픽을 검사하므로 터널 검사 정책 규칙이 필요하지 않습니다.

터널 콘텐츠 검사는 공유 게이트웨이 및 가상 시스템 간 시스템 통신에서 작동하지만 터널 영역을 공유 게이트웨이 또는 가상 시스템 간 시스템 통신에 할당할 수 없습니다. 해당 규칙은 속한 존과 동일한 보안 정책 규칙의 적용을 받습니다.

내부 터널 세션과 외부 터널 세션 모두 방화벽 모델의 최대 세션 용량에 계산됩니다.

다음 표는 외부 터널 세션, 내부 터널 세션 및 내부 원본 세션에 적용할 수 있는 정책 유형의 확인 표시를 나타냅니다.

정책 유형	외부 터널 세션	내부 터널 세션	내부, 원래 세션
앱 재정의	✓ VXLAN 전용	–	✓
DoS 보호	✓	✓	✓

정책 유형	외부 터널 세션	내부 터널 세션	내부, 원래 세션
NAT	✓	–	–
정책 기반 포워딩(PBF) 및 대칭 반환	✓	–	–
QoS	–	–	✓
보안(필수)	✓	✓	✓
User-ID	✓	✓	✓
존 보호	✓	✓	✓

VXLAN은 다른 프로토콜과 다릅니다. 방화벽은 두 개의 서로 다른 세션 키 집합 중 하나를 사용하여 VXLAN에 대한 외부 터널 세션을 만들 수 있습니다.

- VXLAN UDP 세션-6튜플 키(영역, 소스 IP, 대상 IP, 프로토콜, 소스 포트 및 대상 포트)는 VXLAN UDP 세션을 만듭니다.
- VNI 세션- 터널 ID(VXLAN 네트워크 식별자 또는 VNI)를 통합하고 존, 소스 IP, 대상 IP, 프로토콜 및 터널 ID(VNI)를 사용하여 VNI 세션을 만드는 5튜플 키입니다.

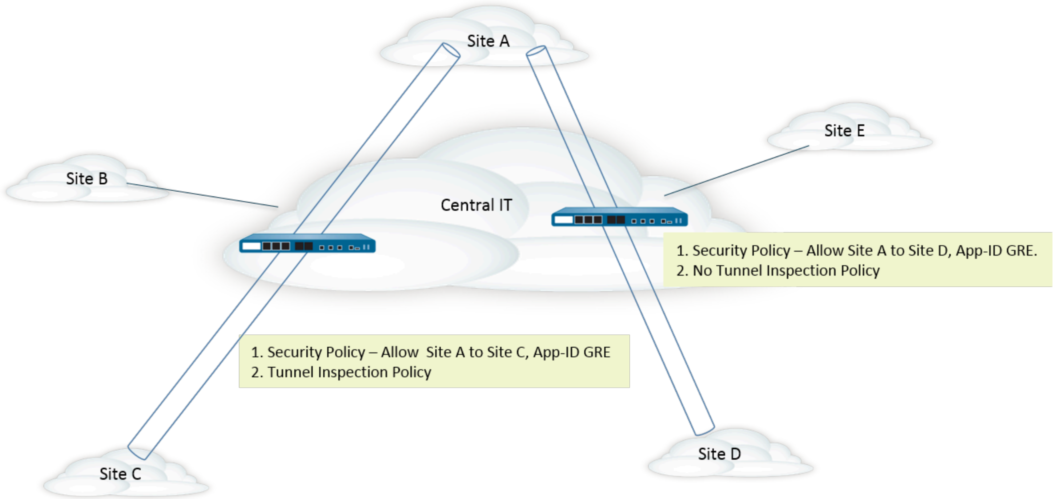
ACC에서 검사된 터널 활동 보기를 하거나 로그에서 터널 정보 보기를 할 수 있습니다. 빠른 보기를 용이하게 하기 위해 모니터 태그를 구성하여 터널 활동을 모니터링하고 해당 태그로 로그 결과를 필터링할 수 있습니다.

ACC 터널 활동은 다양한 뷰에서 데이터를 제공합니다. 터널 ID 사용의 경우, 터널 모니터 태그 및 터널 애플리케이션 사용의 경우 바이트, 세션, 위협, 콘텐츠 및 **URL**에 대한 데이터는 트래픽 요약 데이터베이스에서 가져옵니다. 터널 사용자의 경우 터널로 된 원본 IP 및 터널에 있는 대상 IP 활동, 바이트 및 세션 데이터는 트래픽 요약 데이터베이스에서 나왔으며, 위협에 대한 데이터는 위협 요약에서 비롯되며, URL 요약에서 나온 **URL**에 대한 데이터 및 데이터 데이터베이스에서 나온 콘텐츠에 대한 데이터는 위협 로그의 하위 집합입니다.

인터페이스에서 NetFlow를 활성화하면 NetFlow는 외부 터널에 대한 통계를 캡처하여 이중 계수를 방지합니다(외부 및 내부 흐름의 바이트 계산).

방화벽 모델에 대한 터널 검사 정책 규칙 및 터널 영역 용량은 제품 선택 도구를 참조하십시오.

다음 그림은 여러 부서를 실행하고 서로 다른 보안 정책과 터널 검사 정책을 사용하는 기업을 보여 줍니다. 중앙 IT 팀은 지역 간 연결을 제공합니다. 터널은 사이트 A를 사이트 C에 연결합니다. 다른 터널은 사이트 A를 사이트 D에 연결합니다. 중앙 IT에 연결하는 또 다른 터널은 각 터널의 경로에 방화벽을 배치합니다. 사이트 A와 C 사이의 터널의 방화벽은 터널 검사를 수행합니다. 사이트 A와 D 사이의 터널에 있는 방화벽에는 트래픽이 매우 민감하기 때문에 터널 검사 정책이 없습니다.


Site A
Site B
Site E
Central IT
1. Security Policy – Allow Site A to Site D, App-ID GRE.
2. No Tunnel Inspection Policy
1. Security Policy – Allow Site A to Site C, App-ID GRE
2. Tunnel Inspection Policy
Site C
Site D

터널 콘텐츠 검사 구성

터널을 통해 허용하는 터널 프로토콜에 대한 터널 콘텐츠 검사를 구성하려면 이 작업을 수행하십시오.

STEP 1 | 소스 영역에서 대상 영역으로 터널을 통해 특정 애플리케이션(예: GRE 애플리케이션)을 사용하는 패킷을 허용하는 보안 정책 규칙을 만듭니다.

보안 정책 규칙 만들기

방화벽은 세션 시작 시, 세션 종료 시 또는 둘 다에 터널 검사 로그를 생성할 수 있습니다. 보안 정책 규칙에 대해 작업을 지정할 때 ***GRE*** 세션과 같이 수명이 긴 터널 세션에 대해 세션 시작 시 로그를 선택합니다.

STEP 2 | 터널 검사 정책 규칙을 만듭니다.

1. 정책 > 터널 검사 및 정책 규칙 추가를 선택합니다.
2. 일반 탭에서 영숫자로 시작하고 영숫자, 밑줄, 하이픈, 마침표 및 공백 문자를 포함하는 터널 검사 정책 규칙 이름을 입력합니다.
3. (선택 사항) 설명을 입력합니다.
4. (선택 사항) 보고 및 로깅을 위해 터널 검사 정책 규칙이 적용되는 패킷을 식별하는 태그를 지정합니다.

STEP 3 | 터널 검사 정책 규칙이 적용되는 패킷의 소스를 결정하는 기준을 지정합니다.

1. 소스 탭을 선택합니다.
2. 영역 목록에서 소스 영역을 추가합니다(기본값은 임의).
3. (선택 사항) 소스 주소를 추가합니다. IPv4 또는 IPv6 주소, 주소 그룹 또는 영역 주소 개체(임의)를 입력할 수 있습니다.
4. (선택 사항) 지정한 주소를 제외한 모든 주소를 선택하려면 부정을 선택합니다.
5. (선택 사항) 소스 사용자를 추가합니다(기본값은 임의). 알려진 사용자는 인증된 사용자입니다. 알 수 없는 사용자는 인증되지 않았습니다.

STEP 4 | 터널 검사 정책 규칙이 적용되는 패킷의 대상을 결정하는 기준을 지정합니다.

1. 대상 탭을 선택합니다.
2. 영역 목록에서 대상 영역을 추가합니다(기본값은 임의).
3. (선택 사항) 대상 주소를 추가합니다. IPv4 또는 IPv6 주소, 주소 그룹 또는 지리적 지역 주소 개체를 입력할 수 있습니다(기본값: 임의).

   새 주소 또는 주소 그룹을 구성할 수도 있습니다.
4. (선택 사항) 지정한 주소를 제외한 모든 주소를 선택하려면 부정을 선택합니다.

STEP 5 | 방화벽이 이 규칙에 대해 검사할 터널 프로토콜을 지정합니다.

1. 검사 탭을 선택합니다.
2. 방화벽에서 검사할 하나 이상의 터널 프로토콜을 추가합니다.

    - **GRE** - 방화벽은 터널에서 GRE(Generic Route Encapsulation)를 사용하는 패킷을 검사합니다.
    - **GTP-U**—방화벽은 터널에서 GPRS(General Packet Radio Service) Tunneling Protocol for User Data(GTP-U)를 사용하는 패킷을 검사합니다.
    - 암호화되지 않은 **IPSec** - 방화벽은 터널에서 암호화되지 않은 IPSec(Null EncryVpted IPSec 또는 전송 모드 AH IPSec)을 사용하는 패킷을 검사합니다.
    - **VXLAN** - 방화벽은 터널에서 VXLAN(Virtual Extensible Local Area Network) 터널링 프로토콜을 사용하는 패킷을 검사합니다.

STEP 6 | 방화벽이 검사하는 캡슐화 수준과 방화벽이 패킷을 삭제하는 조건을 지정합니다.

1. 옵션 검사를 선택합니다.
2. 방화벽이 검사할 최대 터널 검사 수준을 선택합니다.

    - 한 수준(기본값) - 방화벽이 외부 터널에 있는 콘텐츠만 검사합니다.

      VXLAN의 경우 방화벽은 VXLAN 페이로드를 검사하여 터널 내에서 캡슐화된 콘텐츠 또는 애플리케이션을 찾습니다. VXLAN 검사는 외부 터널에서만 발생하므로 **One Level**을 선택해야 합니다.
    - 두 수준**(**터널 내 터널**)** - 방화벽은 외부 터널에 있는 콘텐츠와 내부 터널에 있는 콘텐츠를 검사합니다.
3. 방화벽이 각 조건에서 패킷을 삭제할지 여부를 지정하려면 다음 중 일부, 모두 또는 없음을 선택합니다.

    - 최대 터널 검사 수준을 초과하는 경우 패킷 삭제 - 방화벽은 최대 터널 검사 수준에 대해 구성된 것보다 더 많은 수준의 캡슐화를 포함하는 패킷을 삭제합니다.
    - 터널 프로토콜이 엄격한 헤더 검사에 실패하면 패킷 삭제 - 방화벽은 프로토콜에 대한 RFC와 호환되지 않는 헤더를 사용하는 터널 프로토콜이 포함된 패킷을 삭제합니다. 비준수 헤더는 의심스러운 패킷을 나타낼 수 있습니다. 이 옵션을 사용하면 방화벽이 RFC 2890에 대해 GRE 헤더를 확인합니다.

      방화벽이 RFC 2890 이전 버전의 ***GRE***를 구현하는 디바이스로 ***GRE***를 터널링하는 경우 터널 프로토콜이 엄격한 헤더 검사에 실패하면 패킷 삭제 옵션을 활성화하면 안 됩니다**.**
    - 터널 내부의 알 수 없는 프로토콜인 경우 패킷 삭제 - 방화벽은 방화벽이 식별할 수 없는 터널 내부의 프로토콜이 포함된 패킷을 삭제합니다.

      예를 들어, 이 옵션을 선택하면 방화벽이 읽을 수 없기 때문에 터널 검사 정책 규칙과 일치하는 암호화된 IPSec 패킷을 삭제합니다. 따라서 IPSec 패킷을 허용할 수 있으며 방화벽은 null로 암호화된 IPSec 및 AH IPSec 패킷만 허용합니다.
    - 스캔한 **VXLAN** 터널을 소스로 반환 - 트래픽이 방화벽으로 리디렉션(조정)되면 VXLAN이 패킷을 캡슐화합니다. 트래픽 조정은 퍼블릭 클라우드 환경에서 가장 일반적입니다. 원본 VXLAN 터널 엔드포인트(VTEP)로 캡슐화된 패킷을 반환하려면 스캔한 **VXLAN** 터널을 원본

으로 반환을 활성화합니다. 이 옵션은 레이어 3, 레이어 3 하위 인터페이스, 통합 인터페이스 레이어 3 및 VLAN에서만 지원됩니다.

4. 확인을 클릭합니다.

STEP 7 | 터널 검사 정책 규칙을 관리합니다.

터널 검사 정책 규칙을 관리하려면 다음을 사용하십시오.

- (필터 필드) - 필터 필드에 명명된 터널 정책 규칙만 표시합니다.
- 삭제 - 선택한 터널 정책 규칙을 제거합니다.
- 복제 - 추가 버튼의 대안입니다. 선택한 규칙을 새 이름으로 복제한 다음 수정할 수 있습니다.
- 활성화 - 선택한 터널 정책 규칙을 활성화합니다.
- 비활성화 - 선택한 터널 정책 규칙을 비활성화합니다.
- 이동 - 선택한 터널 정책 규칙을 목록에서 위 또는 아래로 이동합니다. 패킷은 위에서 아래로 순서대로 규칙에 대해 평가됩니다.
- 사용하지 않는 규칙 강조 표시 - 마지막으로 방화벽을 다시 시작한 이후로 일치하는 패킷이 없는 터널 정책 규칙을 강조 표시합니다.

STEP 8 | (선택 사항) 터널 콘텐츠에 대한 터널 소스 영역 및 터널 대상 영역을 생성하고 각 영역에 대한 보안 정책 규칙을 구성합니다.

가장 좋은 방법은 터널 트래픽에 대한 터널 영역을 만드는 것입니다. 따라서 방화벽은 동일한 *5-*튜플*(*소스 *IP* 주소 및 포트*,* 대상 *IP* 주소 및 포트*,* 프로토콜*)*을 갖는 터널링된 패킷과 터널링되지 않은 패킷에 대해 별도의 세션을 생성합니다.

PA-5200 시리즈 방화벽의 터널 트래픽에 터널 영역을 할당하면 방화벽이 소프트웨어에서 터널 검사를 수행합니다. 터널 검사는 하드웨어로 오프로드되지 않습니다.

1. 터널 콘텐츠가 외부 터널의 영역에 대한 보안 정책 규칙(이전에 구성됨)과 다른 보안 정책 규칙의 적용을 받도록 하려면 네트워크 > 존을 선택하고 터널 소스 영역의 이름 추가를 선택합니다.
2. 위치에서 가상 시스템을 선택합니다.
3. 유형에서 터널을 선택합니다.
4. 확인을 클릭합니다.
5. 이 하위 단계를 반복하여 터널 대상 영역을 만듭니다.
6. 터널 소스 영역에 대한 보안 정책 규칙을 구성합니다.

   터널 트래픽의 발신자나 트래픽 흐름의 방향을 알지 못할 수 있고 터널을 통해 애플리케이션에 대한 트래픽을 부주의하게 금지하고 싶지 않기 때문에 두 터널 영역을 소스 영역으로 지정하고 두 터널 영역을 대상으로 지정합니다. 보안 정책 규칙에서 영역을 지정하거나 원본 및 대상 영역 둘 다에 대해 모두를 선택합니다. 그런 다음 애플리케이션을 지정합니다.
7. 터널 대상 영역에 대한 보안 정책 규칙을 구성합니다. 터널 소스 영역에 대한 보안 정책 규칙을 구성하기 위한 이전 단계의 팁은 터널 대상 영역에도 적용됩니다.

STEP 9 | (선택 사항) 내부 내용에 대해 터널 소스 영역 및 터널 대상 영역을 지정합니다.

1. 내부 내용에 대해 터널 소스 영역 및 터널 대상 영역(방금 추가한 영역) 을 지정합니다. 정책 > 터널 검사를 선택하고 일반 탭에서 생성한 터널 검사 정책 규칙의 이름을 선택합니다.
2. 검사를 선택합니다.
3. 보안 옵션을 선택합니다.
4. 보안 옵션 사용(기본적으로 비활성화됨)을 통해 내부 콘텐츠 소스가 지정한 터널 소스 영역에 속하도록 하고 내부 콘텐츠 대상이 지정한 터널 대상 영역에 속하도록 합니다.

   보안 옵션을 활성화하지 않으면 내부 콘텐츠 원본은 외부 터널 원본과 동일한 원본 영역에 속하고 내부 콘텐츠 대상은 외부 터널 대상과 동일한 대상 영역에 속하므로 동일한 보안이 적용되며, 이러한 외부 영역에 적용되는 정책 규칙이란 뜻입니다.
5. 터널 소스 영역에서 해당 영역과 연결된 정책이 터널 소스 영역에 적용되도록 이전 단계에서 생성한 적절한 터널 영역을 선택합니다. 그렇지 않으면 기본적으로 내부 콘텐츠는 외부 터널에서 사용되는 것과 동일한 원본 영역을 사용하고 외부 터널 원본 영역의 정책은 내부 콘텐츠 원본 영역에도 적용됩니다.
6. 터널 대상 영역에 대해 이전 단계에서 생성한 적절한 터널 영역을 선택하여 해당 영역과 연결된 정책이 터널 대상 영역에 적용되도록 합니다. 그렇지 않으면 기본적으로 내부 콘텐츠는 외부 터널에서 사용되는 것과 동일한 대상 영역을 사용하고 외부 터널 대상 영역의 정책은 내부 콘텐츠 대상 영역에도 적용됩니다.

   터널 검사 정책 규칙에 대해 터널 소스 영역 및 터널 대상 영역을 구성하는 경우 터널 검사 정책 규칙의 일치 기준에서 소스 영역을 임의로 지정하고 대상 영역을 임의로 지정하는 대신, 특정 소스 영역(3단계) 및 특정 대상 영역(4단계)을 구성해야 합니다. 이 팁은 영역 재할당 방향이 상위 영역에 적절하게 일치하도록 합니다.

   PA-5200 시리즈 또는 PA-7080 방화벽에서 VXLAN을 검사하는 동안 멀티캐스트 언더레이를 사용하면 내부 세션이 여러 데이터플레인에서 복제되고 경쟁 조건이 발생할 수 있습니다. 일부 패킷의 손실을 방지하기 위해 다음 요구 사항이 적용됩니다.

   - *각 VXLAN 터널 엔드포인트(VTEP)로 가는 외부 VXLAN 패킷과 일치하도록 별도의 터널 콘텐츠 검사 규칙을 구성해야 합니다.*
   - *별도의 규칙에서 터널 영역을 할당합니다. 다른 터널 영역을 사용하면 각 엔드포인트에 대해 내부 세션이 달라집니다. 경쟁 조건이 발생하지 않고 패킷 드롭이 표시되지 않습니다.*
7. 확인을 클릭합니다.

STEP 10 | 터널 검사 정책 규칙과 일치하는 트래픽에 대한 모니터링 옵션을 설정합니다.

1. 정책 > 터널 검사를 선택하고 생성한 터널 검사 정책 규칙을 선택합니다.
2. 검사 > 모니터 옵션을 선택합니다.
3. 로깅 및 보고를 위해 유사한 트래픽을 그룹화하려면 모니터 이름을 입력합니다.
4. 모니터 태그(숫자)를 입력하여 로깅 및 보고를 위해 유사한 트래픽을 그룹화합니다(범위는 1~16,777,215). 태그 번호는 전역적으로 정의됩니다.

   이 필드는 VXLAN 프로토콜에는 적용되지 않습니다. VXLAN 로그는 자동으로 VXLAN 헤더의 VNI ID를 사용합니다.

   터널 트래픽에 태그를 지정하면 나중에 터널 검사 로그에서 모니터 태그를 필터링하고 ACC를 사용하여 모니터 태그를 기반으로 터널 활동을 볼 수 있습니다.
5. 보안 규칙 로그 설정을 재정의하여 선택한 터널 검사 정책 규칙을 충족하는 세션에 대한 로깅 및 로그 전달 옵션을 활성화합니다. 이 설정을 선택하지 않으면 터널 트래픽에 적용되는 보안 정책 규칙의 로그 설정에 따라 터널 로그 생성 및 로그 전달이 결정됩니다. 트래픽 로그와 별도로 터널 로그를 저장하도록 터널 검사 로그 설정을 구성하여 트래픽 로그를 제어하는 보안 정책 규칙의 로그 전달 설정을 재정의할 수 있습니다. 터널 검사 로그는 외부 터널(GRE, 암호화되지 않은 IPSec, VXLAN 또는 GTP-U) 세션을 저장하고 트래픽 로그는 내부 트래픽 흐름을 저장합니다.
6. 세션 시작 시 트래픽을 기록하려면 세션 시작 시 기록을 선택합니다.

   터널 로그에 대한 모범 사례는 터널이 오랜 시간 동안 유지될 수 있기 때문에 세션 시작과 세션 종료 시 모두 기록하는 것입니다. 예를 들어 GRE 터널은 라우터가 부팅될 때 나타나며 라우터가 재부팅될 때까지 종료되지 않습니다. 세션 시작 시 로그인하지 않으면 활성 GRE 터널이 있다는 것을 ACC에서 볼 수 없습니다.
7. 세션 종료 시 트래픽을 기록하려면 세션 종료 시 기록을 선택합니다.
8. 방화벽이 터널 검사 규칙을 충족하는 세션에 대한 터널 로그를 전달하는 위치를 결정하는 로그 전달 프로파일을 선택합니다. 또는 로그 전달을 구성하는 경우 새 로그 전달 프로파일을 만들 수 있습니다.
9. 확인을 클릭합니다.

STEP 11 | (선택 사항, VXLAN에만 해당) **VXLAN ID(VNI)** 를 구성합니다. 기본적으로 모든 VXLAN 네트워크 인터페이스(VNI)가 검사됩니다. 하나 이상의 VXLAN ID를 구성하는 경우 정책은 해당 VNI만 검사합니다.

VXLAN 프로토콜만 터널 ID 탭을 사용하여 VNI를 지정합니다.

1. 터널 **ID** 탭을 선택하고 추가를 클릭합니다.
2. 이름을 지정합니다. 이름은 편의를 위한 것이며 로깅, 모니터링 또는 보고의 요소가 아닙니다.
3. **VXLAN ID(VNI)** 필드에 단일 VNI, 쉼표로 구분된 VNI 목록, VNI 범위(하이픈을 구분 기호로 사용) 또는 이들의 조합을 입력합니다. 예를 들어 다음을 지정할 수 있습니다.

   ```
   1677002,1677003,1677011-1677038,1024
   ```

STEP 12 | (선택 사항) 세션 재일치(디바이스 > 설정 > 세션)를 사용하도록 설정한 경우 다음을 사용하지 않도록 설정하여 터널 검사 정책을 만들거나 수정할 때 방화벽이 기존 세션을 삭제하지 않도록 합니다.터널 보안 정책 규칙을 제어하는 영역에 대해 비 **SYN TCP**를 거부합니다.

다음과 같은 경우 방화벽에 다음 경고가 표시됩니다.

- 터널 검사 정책 규칙을 만듭니다.
- 프로토콜을 추가하거나 최대 터널 검사 수준을 한 수준에서 두 수준으로 늘려 터널 검사 정책 규칙을 편집합니다.
- 새 영역을 추가하거나 한 영역을 다른 영역으로 변경하여 보안 옵션 탭에서 보안 옵션을 활성화합니다.

경고**:** 기존 터널 세션에서 터널 검사 정책을 활성화하면 터널 내부의 기존 *TCP* 세션이 *non-syn-tcp* 흐름으로 처리됩니다**.** 터널 검사 정책이 활성화되어 있을 때 기존 세션이 삭제되지 않도록 하려면 영역 보호 프로파일을 사용하여 영역에 대한 ***Reject Non-SYN TCP*** 설정을 ***no***로 설정하고 터널의 보안 정책을 제어하는 영역에 적용합니다**.** 기존 세션이 방화벽에 의해 인식되면***yes*** 또는 ***global***로 설정하여 ***Reject Non-SYN TCP*** 설정을 다시 활성화할 수 있습니다**.**

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택하고 프로파일 추가를 선택합니다.
2. 프로파일의 이름을 입력합니다.
3. 패킷 기반 공격 보호 > **TCP** 삭제를 선택합니다.
4. 비 **SYN TCP** 거부에서 아니요를 선택합니다.
5. 확인을 클릭합니다.
6. 네트워크 > 영역을 선택하고 터널 보안 정책 규칙을 제어하는 영역을 선택합니다.
7. 영역 보호 프로파일에서 방금 만든 영역 보호 프로파일을 선택합니다.
8. 확인을 클릭합니다.
9. 이전 세 하위 단계(12.f, 12.g 및 12.h)를 반복하여 터널 보안 정책 규칙을 제어하는 추가 영역에 영역 보호 프로파일을 적용합니다.
10. 방화벽이 기존 세션을 인식한 후 **yes** 또는 **global**로 설정하여 **Reject Non-SYN TCP**를 다시 활성화할 수 있습니다.

STEP 13 | (선택 사항) 터널의 트래픽 조각화를 제한합니다.

1. 네트워크 > 네트워크 프로파일 > 영역 보호를 선택하고 이름으로 프로파일을 추가합니다.
2. 설명을 입력합니다.
3. 패킷 기반 공격 보호 > **IP** 삭제 > 조각화된 트래픽을 선택합니다.
4. 확인을 클릭합니다.
5. 네트워크 > 영역을 선택하고 조각화를 제한할 터널 영역을 선택합니다.
6. 영역 보호 프로파일의 경우 방금 만든 프로파일을 선택하여 터널 영역에 영역 보호 프로파일을 적용합니다.
7. 확인을 클릭합니다.

STEP 14 | 변경 사항을 커밋합니다.

검사된 터널 활동 보기

검사된 터널의 활동을 보려면 다음 작업을 수행하십시오.

STEP 1 | **ACC**를 선택하고 가상 시스템 또는 모든 가상 시스템을 선택합니다.

STEP 2 | 터널 활동을 선택합니다.

STEP 3 | 지난 24시간 또는 지난 30일처럼 보려는 기간을 선택합니다.

STEP 4 | 전역 필터의 경우 + 또는 - 버튼을 클릭하여 터널 활동에서 ACC 필터를 사용합니다.

STEP 5 | 검사된 터널 활동 보기 각 창의 데이터를 바이트, 세션, 위협, 콘텐츠 또는 **URL**별로 표시 및 정렬할 수 있습니다. 각 창은 그래프 및 테이블 형식으로 터널 데이터의 다른 측면을 표시합니다.

- 터널 **ID** 사용 - 각 터널 프로토콜은 해당 프로토콜을 사용하는 터널의 터널 ID를 나열합니다. 표는 프로토콜에 대한 총 바이트, 세션, 위협, 콘텐츠 및 URL을 제공합니다. 터널 ID에 마우스를 가져가면 터널 ID별 분석 결과를 얻을 수 있습니다.
- 터널 모니터 태그 - 각 터널 프로토콜은 해당 태그를 사용하는 터널의 터널 모니터 태그를 나열합니다. 표는 태그와 프로토콜에 대한 총 바이트, 세션, 위협, 콘텐츠 및 URL을 제공합니다. 터널 모니터 태그 위로 마우스를 가져가면 태그별 분석 결과를 얻을 수 있습니다.
- 터널링된 애플리케이션 사용 - 애플리케이션 범주는 미디어, 일반 관심, 협업 및 네트워킹으로 그룹화된 애플리케이션 유형을 그래픽으로 표시하고 위험에 따라 색상으로 구분합니다. 애플리케이션 테이블에는 애플리케이션당 사용자 수도 포함됩니다.
- 터널링된 사용자 활동 - 예를 들어 날짜 및 시간의 x축을 따라 전송된 바이트 및 수신된 바이트의 그래프를 표시합니다. 그래프의 한 지점 위로 마우스를 가져가면 해당 지점의 데이터를 볼 수 있습니다. 소스 사용자 및 대상 사용자 테이블은 사용자별 데이터를 제공합니다.
- 터널링된 소스 **IP** 활동 - 예를 들어 IP 주소에서 공격자의 바이트, 세션 및 위협에 대한 그래프와 테이블을 표시합니다. 그래프의 한 지점 위로 마우스를 가져가면 해당 지점의 데이터를 볼 수 있습니다.
- 터널링된 대상 **IP** 활동 - 대상 IP 주소를 기반으로 그래프와 테이블을 표시합니다. 예를 들어, IP 주소에서 피해자당 위협을 봅니다. 그래프의 한 지점 위로 마우스를 가져가면 해당 지점의 데이터를 볼 수 있습니다.

로그에서 터널 정보 보기

터널 검사 로그 자체를 보거나 다른 유형의 로그에서 터널 검사 정보를 볼 수 있습니다.

GRE, 암호화되지 않은 **IPSec** 및 **GTP-U** 프로토콜

- TCI 트래픽 규칙이 일치하면 GRE, IPSec 및 GTP-U 프로토콜이 터널 로그 유형, 일치하는 프로토콜, 구성된 모니터 이름 및 모니터 태그(번호)와 함께 터널 검사 로그에 기록됩니다.
- 일치하는 TCI 규칙이 없으면 모든 프로토콜이 트래픽 로그 아래에 기록됩니다.

VXLAN 프로토콜

- TCI 트래픽 규칙이 일치하면 VXLAN 프로토콜이 터널(VXLAN) 로그 유형, 구성된 모니터 이름 및 터널 ID(VNI)와 함께 터널 검사 로그에 기록됩니다.

  내부 세션의 트래픽 로그에서 Tunnel Inspected 플래그는 VNI 세션을 나타냅니다. 상위 세션은 내부 세션이 생성될 때 활성 상태였던 세션이므로 ID가 현재 세션 ID와 일치하지 않을 수 있습니다.
- 일치하는 TCI 규칙이 없으면 VNI 세션은 UDP 프로토콜, 소스 포트 0 및 대상 포트 4789(기본값)를 사용하여 트래픽 로그에 기록됩니다.

◉ 터널 검사 로그를 봅니다.

1. 모니터 > 로그 > 터널 검사를 선택하고 로그 데이터를 확인하여 트래픽에 사용된 터널 애플리케이션 및 헤더의 엄밀한 검사에 실패한 패킷의 높은 수와 같은 우려 사항을 식별합니다.
2. 상세 로그 보기()를 클릭하면 로그에 대한 세부 정보를 볼 수 있습니다.

◉ 터널 검사 정보에 대한 다른 로그를 봅니다.

1. 모니터 > 로그를 선택합니다.
2. 트래픽, 위협, **URL** 필터링, **WildFire** 제출, 데이터 필터링 또는 통합을 선택합니다.
3. 로그 항목의 경우 세부 로그 보기() 를 클릭합니다.
4. 플래그 창에서 **Tunnel Inspected** 플래그가 선택되어 있는지 확인합니다. Tunnel Inspected 플래그는 방화벽이 터널 검사 정책 규칙을 사용하여 내부 콘텐츠 또는 내부 터널을 검사했음을 나타냅니다. 상위 세션 정보는 외부 터널(내부 터널 기준) 또는 내부 터널(내부 콘텐츠 기준)을 나타냅니다.

   트래픽, 위협, **URL** 필터링, **WildFire** 제출, 데이터 필터링 로그에서 내부 세션 로그의 상세 로그 보기에서는 직접적인 상위 정보만 표시되고 터널 로그 정보는 표시되지 않습니다. 두 가지 수준의 터널 검사를 구성한 경우 이 직접 상위의 상위 세션을 선택하여 두 번째 상위 로그를 볼 수 있습니다. (터널 로그 정보를 보려면 이전 단계와 같이 터널 검사 로그를 모니터링해야 합니다.)
5. 터널 검사된 내부 세션에 대한 로그를 보고 있는 경우 일반 섹션에서 상위 세션 보기 링크를 클릭하여 외부 세션 정보를 확인하십시오.

태그가 지정된 터널 트래픽을 기반으로 사용자 지정 보고서 생성

터널 트래픽에 적용한 태그를 기반으로 정보를 수집하는 보고서를 생성할 수 있습니다.

STEP 1 | 모니터 > 사용자 지정 보고서 관리를 선택하고 추가를 클릭합니다.

STEP 2 | 데이터베이스에 대한, 트래픽, 위협, URL, 데이터 필터링, 또는 WildFire 제출 로그를 선택합니다.

STEP 3 | 사용 가능한 열에 대해, 보고서에서 원하는 다른 데이터와 함께 플래그 및 모니터 태그를 선택합니다.

사용자 정의 보고서를 또한 생성할 수도 있습니다.

터널 가속 비활성화

기본적으로 지원되는 방화벽은 터널 가속을 수행하여 GRE 터널, VXLAN 터널 및 GTP-U 터널을 통과하는 트래픽의 성능과 처리량을 개선합니다. 터널 가속은 하드웨어 오프로딩을 제공하여 흐름 조회를 수행하는 데 걸리는 시간을 줄이고 터널 트래픽이 내부 트래픽을 기반으로 보다 효율적으로 분산되도록 합니다.

GRE 및 VXLAN 터널 가속은 PA-7000-100G-NPC-A 및 PA-7050-SMC-B 또는 PA-7080-SMC-B가 있는 PA-3200 시리즈 방화벽 및 PA-7000 시리즈 방화벽에서 지원됩니다. 터널 가속을 비활성화하여 문제를 해결할 수 있습니다. 터널 가속을 비활성화하면 GRE, VXLAN 및 GTP-U 터널에 대해 동시에 비활성화됩니다.

STEP 1 | 디바이스 > 설정 > 관리를 선택하고 일반 설정을 편집합니다.

STEP 2 | 비활성화하려면 터널 가속을 선택 취소합니다.

STEP 3 | 확인을 클릭합니다.

STEP 4 | 커밋합니다.

STEP 5 | 방화벽을 재부팅합니다.

STEP 6 | (선택 사항) 터널 가속 상태를 확인합니다.

1. CLI에 액세스합니다.
2. **> show tunnel-acceleration**

   시스템 출력은 `Enabled` 또는 `Disabled`입니다. GTP-U에만 해당하는 추가 상태 및 이유:

   - `비활성화됨` - 방화벽 모델에서 GTP-U 터널 가속이 지원되지 않거나 GTP 보안이 비활성화됩니다.
   - `오류(GTP-U가 포함된 TCI가 예기치 않게 구성됨)` - 터널 가속이 활성화된 경우 GTP-U 프로토콜이 포함된 TCI가 구성됩니다.
   - `활성화됨` - 터널 가속이 활성화되었습니다. GTP-U 터널 가속은 아직 실행되지 않습니다. GTP 보안이 활성화되었지만 아직 재부팅되지 않았습니다.
   - `설치됨` - GTP-U 터널 가속이 실행 중입니다.

네트워크 패킷 브로커

네트워크 패킷 브로커는 네트워크 트래픽을 필터링하고 하나 이상의 타사 보안 어플라이언스의 외부 보안 체인으로 포워드합니다. Network Packet Broker는 PAN-OS 8.1에 도입된 Decryption Broker 기능을 대체하고 복호화되지 않은 TLS 트래픽과 비 TLS 트래픽(일반 텍스트) 및 복호화된 TLS 트래픽 전달을 포함하도록 기능을 확장합니다. 모든 유형의 트래픽을 처리하는 기능은 금융 및 정부 기관과 같은 매우 높은 보안 환경에서 특히 중요합니다.

Network Packet Broker는 PA-7000 시리즈, PA-5400 시리즈, PA-5200 시리즈, PA-3400 시리즈, PA-3200 시리즈 디바이스 및 VM-300 및 VM-700 모델에서 지원됩니다. 방화벽이 세션 트래픽에 대해 신뢰할 수 있는 제3자(또는 메시지 가로채기)로 설정된 경우 SSL 전달 프록시 암호 해독을 활성화해야 합니다.

방화벽 인터페이스는 암호 해독 브로커와 *GRE* 터널 엔드포인트가 될 수 없습니다.

- 네트워크 패킷 브로커 개요
- 네트워크 패킷 브로커 작동 방식
- 네트워크 패킷 브로커 배포 준비
- 트랜스페어런트 브리지 보안 체인 구성
- 라우팅된 레이어 3 보안 체인 구성
- 네트워크 패킷 브로커 HA 지원
- 네트워크 패킷 브로커에 대한 사용자 인터페이스 변경 사항
- 네트워크 패킷 브로커의 한계
- 네트워크 패킷 브로커 문제 해결

네트워크 패킷 브로커 개요

전체 보안 제품군의 일부로 하나 이상의 타사 보안 어플라이언스(보안 체인)를 사용하는 경우 Network Packet Broker를 사용하여 네트워크 트래픽을 필터링하고 해당 보안 어플라이언스로 전달할 수 있습니다. Network Packet Broker는 PAN-OS 8.1에 도입된 Decryption Broker 기능을 대체합니다.

Decryption Broker와 마찬가지로 Network Packet Broker는 암호 해독 기능과 보안 체인 관리를 제공합니다. 이는 해당 기능을 위한 전용 디바이스를 지원하는 복잡성을 제거하여 네트워크를 단순화하고 자본 및 운영 비용을 절감합니다. 또한 Decryption Broker와 마찬가지로 Network Packet Broker는 보안 체인에 대한 경로가 정상인지 확인하고 체인이 다운될 경우 트래픽을 처리할 수 있는 옵션을 제공합니다.

Network Packet Broker는 방화벽의 보안 체인 전달 기능을 확장하여 복호화된 TLS 트래픽뿐만 아니라 복호화되지 않은 TLS 및 비 TLS(일반 텍스트) 트래픽을 필터링하여 애플리케이션, 사용자, 디바이스, IP 주소 및 존을 기반으로 하나 이상의 보안 체인으로 전달할 수 있습니다. 이러한 기능은 금융 및 정부 기관과 같은 매우 높은 보안 환경에서 특히 유용합니다.

업그레이드 및 다운그레이드:

- Decryption Broker 라이선스가 있는 방화벽에서 PAN-OS 10.2로 업그레이드하는 경우:
  - 방화벽을 재부팅하면 라이선스 이름이 자동으로 Network Packet Broker로 변경됩니다.

    방화벽이 스탠드얼론 방화벽인지, *HA* 쌍의 일부인지 또는 *Panorama*에서 방화벽으로 *Network Packet Broker* 라이선스를 푸시하는지 여부에 관계없이 라이선스를 적용하고 사용자 인터페이스를 업데이트하려면 방화벽을 재부팅해야 합니다.
  - PAN-OS는 기존 Decryption Broker Forwarding 프로파일(**Profiles** > **Decryption** > **Forwarding Profile**)을 패킷 브로커 프로파일로 변환합니다.
  - PAN-OS는 트래픽을 보안 체인으로 전달하기 위한 기존 암호 해독 정책 규칙을 네트워크 패킷 브로커 정책 규칙으로 변환합니다.
  - PAN-OS는 사용자 인터페이스에서 Decryption Broker 프로파일을 제거하고 패킷 브로커 프로파일(**Profiles** > **Packet Broker**)로 대체하고 네트워크 패킷 브로커 정책(**Policies** > **Network Packet Broker**)도 추가합니다.
- PAN-OS 10.1에서 PAN-OS 10.0으로 다운그레이드하는 경우:
  - PAN-OS는 기존 패킷 브로커 프로파일을 암호 해독 브로커 전달 프로파일로 변환합니다.
  - PAN-OS는 네트워크 패킷 브로커 규칙베이스를 제거하고 경고 메시지를 인쇄합니다. 네트워크 패킷 브로커 정책 규칙을 암호 해독 전달에 대한 암호 해독 정책 규칙으로 다시 구성해야 합니다.
  - 라이선스 이름은 Network Packet Broker로 유지됩니다(재부팅 후 모든 PAN-OS 버전에서 라이선스 이름이 Decryption Broker에서 Network Packet Broker로 변경되며 Decryption Broker의 작동에는 영향을 미치지 않습니다). 그러나 이 기능은 Network Packet Broker 기능이 아니라 Decryption Broker 기능입니다.
  - PAN-OS는 사용자 인터페이스에서 Network Packet Broker 프로파일을 제거하고 이를 Decryption Forwarding 프로파일로 대체하며 또한 사용자 인터페이스에서 Network Packet Broker 정책을 제거합니다(대체는 없습니다. 암호 해독 정책 규칙을 사용하여 보안 체인에 해독된 Forward 프록시 트래픽만 전달합니다).

네트워크 패킷 브로커 사용을 위한 요구 사항:

- 방화벽에 무료 Packet Broker 라이선스를 설치해야 합니다. 무료 라이선스가 없으면 인터페이스에서 패킷 브로커 정책 및 프로파일에 액세스할 수 없습니다.
- 방화벽에는 전용 패킷 브로커 전달 인터페이스 쌍으로 사용할 수 있는 레이어 3 이더넷 인터페이스가 두 개 이상 있어야 합니다.
  - 여러 쌍의 전용 Network Packet Broker 전달 인터페이스를 구성하여 서로 다른 보안 체인에 연결할 수 있습니다.
  - 각 보안 체인에 대해 전용 Network Packet Broker 인터페이스 쌍은 동일한 보안 영역에 있어야 합니다.
  - 전용 인터페이스 쌍은 보안 체인의 첫 번째 디바이스와 마지막 디바이스에 연결됩니다.

  ***Network Packet Broker*는 라우팅된 레이어 *3* 보안 체인과 트랜스페어런트 브리지 레이어 *1* 보안 체인을 지원합니다. 라우팅된 레이어 *3* 체인의 경우 한 쌍의 패킷 브로커 전달 인터페이스가 적절하게 구성된 스위치, 라우터 또는 기타 디바이스를 사용하여 여러 레이어 *3* 보안 체인에 연결하여 방화벽과 보안 체인 간에 필요한 레이어 *3* 라우팅을 수행할 수 있습니다.**

- 전용 네트워크 패킷 브로커 전달 인터페이스는 동적 라우팅 프로토콜을 사용할 수 없습니다.
- 방화벽이 수정된 세션을 원래 세션과 일치시킬 수 없어 트래픽을 삭제하기 때문에 보안 체인의 어떤 디바이스도 원본 또는 대상 IP 주소, 원본 또는 대상 포트 또는 원본 세션의 프로토콜을 수정할 수 없습니다.

네트워크 패킷 브로커는 다음을 지원합니다.

- 복호화된 TLS, 복호화되지 않은 TLS 및 비TLS 트래픽.
- SSL 전달 프록시, SSL 인바운드 검사 및 암호화된 SSH 트래픽.
- 라우팅된 레이어 3 보안 체인.
- 투명 브리지 레이어 1 보안 체인.

  동일한 방화벽에서 라우팅된 레이어 *3* 및 레이어 *1* 투명 브리지 보안 체인을 모두 구성할 수 있지만 각 유형에 대해 서로 다른 쌍의 전달 인터페이스를 사용해야 합니다.

- 체인을 통한 단방향 트래픽 흐름: 체인에 대한 모든 트래픽은 하나의 전용 인터페이스에서 방화벽을 빠져 나와 다른 전용 인터페이스에서 방화벽으로 돌아가므로 모든 트래픽은 전용 Network Packet Broker 인터페이스 쌍을 통해 같은 방향으로 흐릅니다.

  두 방화벽 전달 인터페이스는 동일한 존에 있어야 합니다.

- 보안 체인을 통한 양방향 트래픽 흐름:
  - 클라이언트-서버(c2s) 트래픽은 하나의 전용 방화벽 브로커 인터페이스에서 방화벽을 빠져 나와 다른 전용 방화벽 브로커 인터페이스에서 방화벽으로 돌아갑니다.
  - 서버-클라이언트(s2c) 트래픽은 c2s 트래픽과 동일한 두 개의 전용 방화벽 브로커 인터페이스를 사용하지만 트래픽은 보안 체인을 통해 반대 방향으로 흐릅니다. s2c 트래픽이 체인으로 이동하는 방화벽 브로커 인터페이스는 c2s 트래픽이 체인에서 방화벽으로 반환되는 동일한 인터페이스입니다.

s2c 트래픽이 방화벽으로 반환되는 방화벽 브로커 인터페이스는 c2s 트래픽이 체인으로 나가는 것과 동일한 인터페이스입니다.

두 방화벽 전달 인터페이스는 동일한 존에 있어야 합니다.

*Network Packet Broker*는 멀티캐스트, 브로드캐스트 또는 암호 해독된 *SSH* 트래픽을 지원하지 않습니다.

네트워크 패킷 브로커 작동 방식

방화벽을 타사 보안 디바이스 체인에 연결하기 위한 상위 수준 워크플로는 다음과 같습니다.

1. 전달할 복호화되지 않은 TLS, 복호화된 TLS 및 비 TLS(TCP 및 UDP) 트래픽을 식별합니다.
2. 보안 체인 토폴로지를 식별합니다. 각 보안 체인의 디바이스가 트래픽을 투명하게 전달하는지(브리징) 또는 디바이스가 레이어 3 정보를 기반으로 트래픽을 라우팅하는지 여부를 결정합니다. 여러 보안 체인을 사용하면 트래픽 로드 밸런싱에 도움이 됩니다. 또한 보안 체인(트래픽은 방화벽에서 정상적인 처리를 거쳐 그에 따라 전달 또는 차단됨)을 우회할지, 보안 체인이 상태 확인에 실패할 경우 트래픽을 차단할지 결정합니다.
3. 트래픽을 보안 체인으로 전달할 방화벽에 무료 네트워크 패킷 브로커 라이센스를 설치하십시오.
4. 트래픽을 하나 이상의 보안 체인으로 전달하고 해당 인터페이스에서 네트워크 패킷 브로커를 활성화하기 위해 하나 이상의 방화벽 인터페이스 쌍을 식별합니다.
5. 하나 이상의 패킷 브로커 프로파일을 구성합니다.
6. 하나 이상의 네트워크 패킷 브로커 정책을 구성합니다.

타사 보안 디바이스 체인을 사용하여 트래픽을 검사하려면 방화벽에서 세 가지 개체를 구성합니다.

- 인터페이스 - 방화벽에서 보안 체인으로 트래픽을 전달하고 보안 체인에서 처리된 트래픽을 다시 수신하기 위한 하나 이상의 레이어 3 이더넷 방화벽 인터페이스 쌍입니다. 프로파일에서 인터페이스 쌍을 지정해야 하므로 프로파일 및 정책 규칙을 구성하기 전에 네트워크 패킷 브로커 인터페이스 쌍을 구성하십시오.
- 패킷 브로커 프로파일 - 프로파일은 정책에서 정의한 트래픽을 보안 체인으로 전달하는 방법을 제어합니다. 각 네트워크 패킷 브로커 정책 규칙에는 연결된 패킷 브로커 프로파일이 있습니다. 프로파일은 보안 체인이 라우팅된 레이어 3 체인인지 레이어 1 트랜스페이런트 브리지 체인인지, 체인을 통한 트래픽 방향(단방향 또는 양방향)인지, 전용 Network Packet Broker 방화벽 인터페이스인지, 방화벽과 보안 체인 사이에서 연결 상태를 모니터링하는 방법을 정의합니다. 다중 라우팅된 레이어 3 보안 체인의 경우 각 체인의 첫 번째 및 마지막 디바이스와 연결된 트래픽에 대한 세션 배포(로드 밸런싱) 방법을 지정할 수 있습니다.
- 네트워크 패킷 브로커 정책 규칙 - 정책 규칙은 각 보안 체인으로 전달하거나 여러 라우팅(계층 3) 체인에 대한 로드 밸런싱을 위해 애플리케이션 트래픽을 정의합니다. 정책 규칙은 보안 체인으로 전달할 트래픽의 소스 및 대상, 사용자, 애플리케이션 및 서비스를 정의합니다. 정책 규칙은 또한 보안 체인으로 전달할 트래픽 유형을 정의합니다. 암호 해독된 TLS 트래픽, 암호 해독되지 않은 TLS 트래픽, 비TLS 트래픽 또는 트래픽 유형의 조합을 선택할 수 있습니다. 또한 각 정책 규칙에 패킷 브로커 프로파일을 추가하여 트래픽(및 기타 모든 프로파일 특성)을 전달할 보안 체인을 지정합니다.

  Policy Optimizer를 사용하여 Network Packet Broker 정책 규칙을 검토하고 강화합니다.

애플리케이션 트래픽을 Network Packet Broker 정책 규칙과 일치시키기 위해 Network Packet Broker는 방화벽 App-ID 캐시에서 애플리케이션을 찾습니다. 애플리케이션이 App-ID 캐시에 없으면 방화벽은 보안 체인을 우회하고 보안 정책 허용 규칙에 구성된 모든 위협 검사를 트래픽에 적용합니다. 애플리케이션이 App-ID 캐시에 있는 경우 방화벽은 네트워크 패킷 브로커 정책 규칙 및 연결된 패킷 브로커 프로파일에 지정된 방식으로 트래픽을 보안 체인으로 전달합니다.

복호화되지 않은 TLS 및 비 TLS 트래픽의 경우 방화벽은 첫 번째 세션의 App-ID 캐시에 애플리케이션을 설치하므로 방화벽은 네트워크 패킷 브로커 정책 및 프로파일에 지정된 대로 트래픽을 처리합니다.

해독된 TLS 트래픽의 경우 애플리케이션의 첫 번째 세션에서 Network Packet Broker는 세션이 해독되고 있다는 사실을 모르고 "ssl"을 애플리케이션으로 봅니다. 기본 특정 애플리케이션은 아직 알려지지 않았거나 App-ID 캐시에 설치되지 않았기 때문에 브로커 조회가 실패하고 트래픽이 보안 체인을 우회합니다. 트래픽은 보안 정책 허용 규칙에 구성된 모든 위협 검사의 대상이 됩니다. 방화벽이 트래픽을 해독할 때 방화벽은 특정 애플리케이션을 학습하고 이를 App-ID 캐시에 설치합니다. 동일한 애플리케이션에 대한 두 번째 및 후속 암호 해독 세션의 경우 특정 애플리케이션이 이제 App-ID 캐시에 있고 방화벽이 예상대로 트래픽을 보안 체인으로 전달하기 때문에 Network Packet Broker 조회에 성공합니다.

네트워크 패킷 브로커 배포 준비

네트워크 패킷 브로커 배포를 준비하려면 다음 작업을 수행하십시오.

1. 무료 네트워크 패킷 브로커 라이선스를 얻고 활성화하십시오.
    1. 고객 지원 포털에 로그인합니다.
    2. 왼쪽 탐색 창에서 자산 > 디바이스를 선택합니다.
    3. 암호 해독 브로커 또는 암호 해독 포트 미러링을 활성화하려는 디바이스를 찾고 작업(연필 아이콘)을 선택합니다.
    4. 라이선스 활성화에서 기능 라이선스 활성화를 선택합니다.
    5. 네트워크 패킷 브로커 무료 라이선스를 선택하십시오.
    6. 동의 및 제출을 클릭합니다.
2. 방화벽에 라이선스를 설치합니다.
    1. 디바이스 > 라이선스를 선택합니다.
    2. 라이선스 서버에서 라이선스 키 검색을 클릭합니다.
    3. 디바이스 > 라이선스 페이지에 네트워크 패킷 브로커 라이선스가 현재 방화벽에서 활성 상태임을 표시하는지 확인하십시오.
    4. 방화벽을 다시 시작합니다(디바이스 > 설정 > 작업). 네트워크 패킷 브로커는 방화벽이 다시 시작될 때까지 구성에 사용할 수 없습니다.

    *Panorama*에서 관리 방화벽으로 네트워크 패킷 브로커 라이선스를 푸시할 수 있습니다. 라이선스를 적용하고 사용자 인터페이스를 업데이트하려면 방화벽을 재부팅해야 합니다.
3. 네트워크 패킷 브로커에 대한 App-ID 캐시를 활성화합니다.
    1. App-ID 캐시는 기본적으로 비활성화되어 있습니다. 구성 모드 CLI 명령

        ```
        admin@PA-3260# set deviceconfig setting application cache yes
        ```

        를 사용하여 활성화합니다.
    2.
        ```
        admin@PA-3260# set deviceconfig setting application use-cache-
        for-identification yes
        ```

        명령을 사용하여 방화벽이 App-ID 캐시를 사용하여 애플리케이션을 식별하도록 활성화합니다.

    ```
    admin@PA-3260> show running application setting Application
     setting 명령을 사용하여 설정이 애플리케이션 캐시가 예로 설정되어 있
    고 appid에 캐시 사용이 예로 설정되어 있는지 확인합니다. Application
     cache : yes Supernode : yes Heuristics : yes Cache Threshold :
     1 Bypass when exceeds queue limit: no Traceroute appid : yes
     Traceroute TTL threshold : 30 Use cache for appid : yes Use
     simple appsigs for ident : yes Use AppID cache on SSL/SNI : no
    ```



```
Unknown capture : on Max. unknown sessions : 5000 Current unknown
sessions : 33 Application capture : off
```

```
Current APPID Signature Memory Usage : 16768 KB (Actual 16461 KB)
 TCP 1 C2S : regex 11898 states TCP 1 S2C : regex 4549 states UDP 1
 C2S : regex 4263 states UDP 1 S2C : regex 1605 states
```

4. 하나 이상의 보안 체인으로 전달할 트래픽을 식별합니다.
5. 각 보안 체인에 대한 토폴로지를 식별하고 방화벽에서 구성하는 보안 체인 유형을 결정하는 레이어 1 투명 브리지 전달 또는 라우팅된 레이어 3 전달을 사용할지 여부를 결정합니다. 고려 사항은 다음과 같습니다.
   - 여러 체인에 걸쳐 트래픽을 로드 밸런싱할 것인지(라우팅된 레이어 3 보안 체인을 사용하여 라우터, 스위치 또는 기타 라우팅 디바이스를 통해 여러 체인에 세션을 배포할 것인지), 단일 체인을 사용하거나, 여러 유형의 트래픽에 대해 서로 다른 보안 체인을 사용할지 여부. 다중 레이어 1 투명 브리지 체인의 경우 레이어 1 연결이 라우팅되지 않기 때문에 각 보안 체인에 대해 전용 방화벽 인터페이스 쌍이 필요합니다.
   - 보안 체인을 통해 단방향 또는 양방향 트래픽 흐름을 사용할지 여부.
6. 전용 네트워크 패킷 브로커 전달 인터페이스로 사용할 방화벽 인터페이스 쌍을 결정하십시오.
   - 레이어 1 투명 브리지 체인의 경우 각 레이어 1 보안 체인에 대해 한 쌍의 전용 방화벽 인터페이스가 필요합니다. 특정 트래픽을 다른 보안 체인으로 보내도록 정책 규칙을 구성할 수 있습니다.
   - 라우팅된 레이어 3 체인의 경우 한 쌍의 전용 방화벽 인터페이스가 스위치, 라우터 또는 기타 라우팅 가능 디바이스를 통해 여러 레이어 3 보안 체인 간에 트래픽을 로드 밸런싱할 수 있습니다.
   - 라우팅된 레이어 3 체인의 경우 여러 쌍의 전용 방화벽 인터페이스를 사용하여 다른 정책 규칙을 사용하여 다른 보안 체인에 특정 트래픽을 보낼 수 있습니다.

트랜스페어런트 브리지 보안 체인 구성

레이어 1 트랜스페어런트 브리지 보안 체인은 직접 연결된 일련의 데이터 검사 및 처리 보안 디바이스를 통해 한 방화벽 인터페이스의 트래픽을 전달한 다음 트래픽을 라우팅할 필요 없이 다른 방화벽 인터페이스를 통해 다시 전달합니다.

레이어 1 트랜스페어런트 브리지 보안 체인을 구성하기 전에 네트워크 패킷 브로커 배포 준비단계를 수행하고 방화벽과 보안 체인 디바이스 간의 물리적 연결이 올바른지 확인하십시오.

여러 투명 브리지 보안 체인에 세션을 분산하려면 트래픽 부하를 분산하는 데 사용할 각 보안 체인에 대해 방화벽에 하나의 레이어 1 투명 브리지 보안 체인을 만듭니다. 방화벽의 각 트랜스페어런트 브리지 보안 체인에는 두 개의 전용 레이어 3 이더넷 인터페이스가 필요합니다. 구성하려는 토폴로지에 사용 가능한 이더넷 인터페이스가 충분한지 확인하십시오.

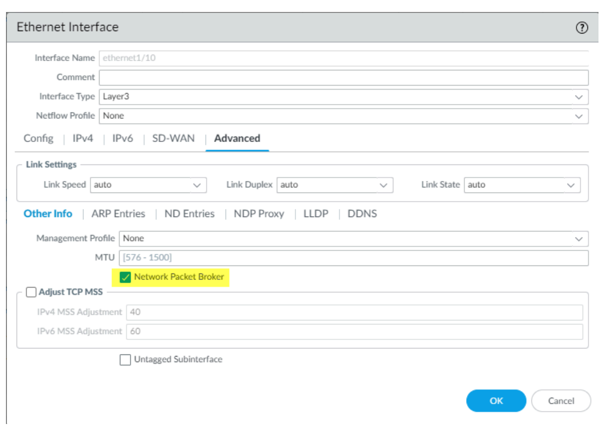
레이어 *1* 트랜스페어런트 브리지 보안 체인은 라우팅되지 않기 때문에 다른 보안 체인으로 장애 조치할 수 없습니다.

STEP 1 | 네트워크 패킷 브로커 전달 인터페이스로 2개의 Layer 3 이더넷 인터페이스를 활성화합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택합니다.
2. 두 개의 네트워크 패킷 브로커 전달 인터페이스 중 하나로 사용할 사용하지 않는 이더넷 인터페이스를 선택합니다.
3. 인터페이스 유형을 **Layer3**으로 설정합니다.
4. 구성 탭에서 인터페이스를 할당할 영역을 선택합니다.

   동일한 영역에서 두 보안 체인 인터페이스를 모두 구성해야 합니다.

5. 구성 탭에서 모범 사례로 전용 가상 라우터를 사용하거나 생성하여 인터페이스를 할당합니다. 전용 가상 라우터를 사용하면 네트워크 패킷 브로커 인터페이스 트래픽이 다른 트래픽과 분리된 상태로 유지됩니다.
6. 고급을 선택한 다음 네트워크 패킷 브로커를 선택하여 인터페이스를 활성화합니다.



7. 확인을 클릭하여 인터페이스 구성을 저장합니다.
8. 사용하지 않는 다른 이더넷 인터페이스에서 이 절차를 반복하여 다른 네트워크 패킷 브로커 전달 인터페이스를 구성합니다.

STEP 2 | 레이어 1 트랜스페어런트 브리지 보안 체인으로 트래픽을 전달하는 방법을 제어하도록 패킷 브로커 프로파일을 구성합니다.

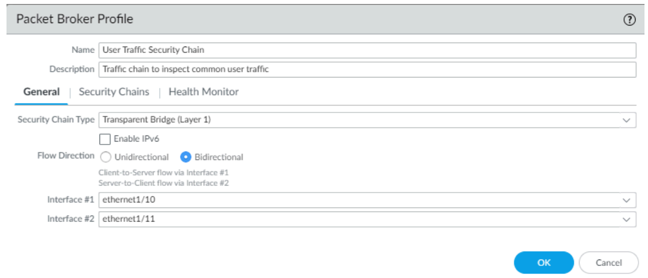
1. 개체 > 패킷 브로커 프로파일을 선택하고 새 프로파일을 추가하거나 기존 프로파일을 수정합니다.
2. 목적을 쉽게 식별할 수 있도록 프로파일에 이름과 설명을 지정합니다.
3. 일반 탭에서:
   - 보안 체인 유형으로 트랜스페어런트 브리지**(**레이어 **1)**를 선택합니다.
   - 트래픽이 IPv6 트래픽인 경우 **IPv6**을 활성화합니다.
   - 흐름 방향을 선택합니다.

     네트워크 토폴로지는 단방향 또는 양방향 흐름을 사용할지 여부를 결정합니다**.** 성능은 어느 방법을 사용해도 거의 동일합니다**.**

     하나의 방화벽 인터페이스를 사용하여 c2s 및 s2c 세션 흐름을 모두 보안 체인으로 전달하고 다른 방화벽 인터페이스를 사용하여 보안 체인에서 두 세션 흐름을 다시 수신하려면 단방향을 선택합니다.

     인터페이스 **#1**을 사용하여 c2s 흐름을 보안 체인으로 전달하고 보안 체인에서 s2c 흐름을 수신하고 인터페이스 **#2**를 사용하여 s2c 흐름을 보안 체인으로 전달하고 보안 체인에서 c2s 흐름을 수신하려면 양방향을 선택합니다. .
   - **Interface #1** 및 **Interface #2**에서 네트워크 패킷 브로커 전달 인터페이스 쌍을 지정합니다. 두 인터페이스 모두 네트워크 패킷 브로커에 대해 이미 활성화되어 있어야 합니다(네트워크 패킷

브로커 배포 준비 참조) 사용할 수 있습니다. 어떤 인터페이스가 **Interface #1**이고 어떤 인터페이스가 **Interface #2**인지 설정할 때 흐름의 방향성에 주의하십시오.



4. 보안 체인 탭은 트랜스페어런트 브리지에 사용되지 않습니다.

5. 상태 모니터 탭에서:

- 보안 체인에 장애가 발생할 경우 발생하는 상황을 제어할 수 있도록 수행할 상태 모니터링 유형을 선택합니다. 경로 모니터링, **HTTP** 모니터링 및 **HTTP** 모니터링 대기 시간 중에서 하나, 둘 또는 모두를 선택할 수 있습니다.

  경로 모니터링 - ping을 사용하여 디바이스 연결을 확인합니다.

  HTTP 모니터링 - 디바이스 가용성 및 응답 시간을 확인합니다.

  HTTP 모니터링 대기 시간 - 디바이스 처리 속도와 효율성을 확인합니다. 이 옵션을 선택하면 **HTTP** 모니터링도 자동으로 활성화됩니다.

- 하나 이상의 상태 모니터링 유형을 활성화하면 보안 체인 상태 오류가 있는 경우 방화벽이 보안 체인 트래픽을 처리하는 방법을 결정하는 상태 확인 오류 시 옵션이 활성화됩니다. 옵션은 보안 체인 우회 및 세션 차단입니다.

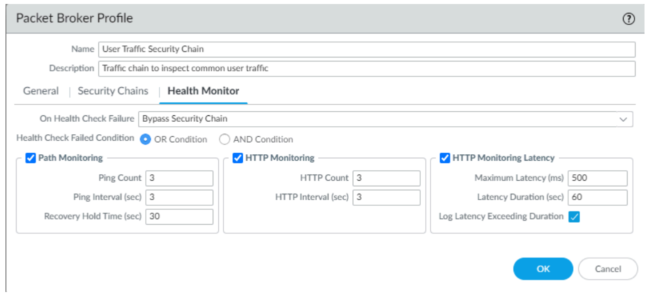
  보안 체인 우회 - 방화벽은 트래픽을 보안 체인 대신 대상으로 전달하고 구성된 보안 프로파일 및 보호를 트래픽에 적용합니다.

  세션 차단 - 방화벽이 세션을 차단합니다.

  선택하는 방법은 보안 체인을 통해 트래픽을 실행할 수 없는 경우 트래픽을 처리할 방법에 따라 다릅니다.

- 상태 확인 옵션을 하나 이상 선택하는 경우, 방화벽이 상태 확인에 실패했다고 기록하길 원하는지(상태 확인 실패 조건), 모니터링 옵션 중 하나라도 실패한 조건(**OR** 조건)을 기록하는 경우 또는 모든 선택한 모니터링 옵션은 실패한 조건(**AND** 조건)을 기록하는지 선택합니다. 예를 들어 세 가지 상태 확인 옵션을 모두 활성화하고 옵션 중 하나가 실패 조건을 기록하는 경우 **OR** 조건을 선택하면 방화벽은 보안 체인 연결이 실패한 것으로 간주하고 상태 확인 실패 시에서 지정

한 작업을 실행합니다. **AND** 조건을 선택한 경우 두 가지 상태 메트릭이 여전히 정상이므로 방화벽은 연결을 정상으로 간주합니다.

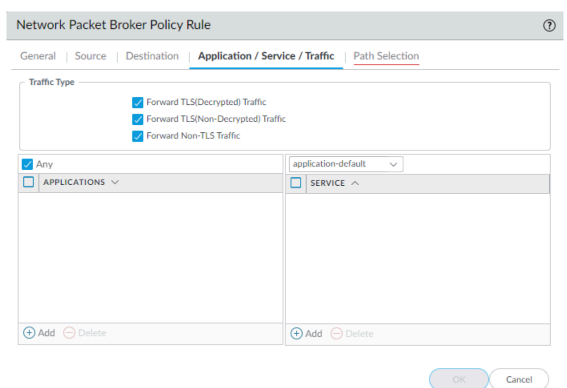


6. 확인을 클릭하여 프로파일을 저장합니다.

STEP 3 | 패킷 브로커 정책을 구성하여 레이어 1 트랜스페어런트 브리지 보안 체인으로 전달할 트래픽을 정의합니다.

1. 정책 > 네트워크 패킷 브로커를 선택하고 새 정책 규칙을 추가하거나 기존 정책 규칙을 수정합니다.
2. 일반 탭에서 정책 규칙의 이름 및 설명을 지정하여 목적을 쉽게 식별하고 감사 설명을 추가하고 사용하는 경우 태그를 적용합니다.
3. 소스 탭에서 보안 체인에 규칙을 전달할 트래픽의 소스 영역, IP 주소, 사용자 및 디바이스를 식별합니다.
4. 대상 탭에서 규칙이 보안 체인에 전달할 트래픽의 대상 영역, IP 주소 및 디바이스를 식별합니다.
5. 애플리케이션/서비스/트래픽 탭에서 규칙이 보안 체인에 전달할 애플리케이션 및 서비스를 식별합니다. 규칙이 내부 사용자 지정 애플리케이션과 같이 비표준 포트를 사용할 것으로 예상되는 애플리케이션을 제어하지 않는 한 비표준 포트를 사용하여 회피 동작을 나타내는 애플리케이션이 차단되도록 서비스를 애플리케이션 기본값으로 설정하는 것이 가장 좋습니다.

   트래픽 유형에 대해 규칙이 보안 체인에 전달할 모든 트래픽 유형을 선택하십시오. **TLS(Decrypted)** 트래픽 전달이 기본 선택입니다. **Forward TLS(Decrypted)** 트래픽, **Forward TLS(Non-Decrypted)** 및 **Forward Non-TLS** 트래픽의 조합을 선택하여 보안 체인으로 전달할 수 있습니다.



6. 경로 선택 탭에서 2단계에서 만든 패킷 브로커 프로파일을 선택하거나 새 프로파일을 만들어 정책 규칙이 제어하는 트래픽을 보안 체인으로 보내는 방법을 제어합니다.

STEP 4 | 1단계~3단계를 반복하여 더 많은 레이어 1 투명 브리지 보안 체인을 만듭니다.

각 레이어 1 트랜스페어런트 브리지 보안 체인에 대해:

- 네트워크 패킷 브로커 포워딩 인터페이스로 사용되는 두 개의 이더넷 인터페이스는 각 보안 체인 전용이어야 합니다. 트랜스페어런트 브리지 보안 체인에 사용되는 이더넷 인터페이스는 다른 용도로 사용하거나 다른 트래픽을 전달할 수 없습니다.
- 네트워크 패킷 브로커 전달 인터페이스의 각 쌍은 하나의 레이어 1 트랜스페어런트 브리지 보안 체인에 연결됩니다.

트랜스페어런트 브리지 보안 체인 간에 트래픽을 비교적 균등하게 분할하는 네트워크 패킷 브로커 정책 규칙을 생성하여 트래픽을 로드 밸런싱할 수 있습니다. 또한 정책 규칙을 사용하여 특정 보안 체인을 통해 특정 트래픽 및 트래픽 유형을 지정할 수 있습니다.

레이어 1 트랜스페어런트 브리지 보안 체인은 라우팅되지 않기 때문에 다른 보안 체인으로 장애 조치할 수 없습니다. 패킷 브로커 프로파일의 상태 모니터 탭을 사용하여 트랜스페어런트 브리지 보안 체인이 실패할 경우 트래픽을 처리하는 방법을 구성합니다.

라우팅된 레이어 3 보안 체인 구성

라우팅된 레이어 3 보안 체인은 트래픽을 일련의 데이터 검사 및 처리 보안 디바이스로 전달한 다음 방화벽에 있는 두 개의 전용 전달 인터페이스를 사용하여 방화벽으로 다시 전달합니다.

라우팅된 레이어 3 보안 체인을 구성하기 전에 에 대한 네트워크 패킷 브로커 배포 준비단계를 수행하고 방화벽과 보안 체인 디바이스 간의 물리적 연결이 올바른지 확인합니다. 구성할 토폴로지에 사용할 수 있는 이더넷 인터페이스가 방화벽에 충분한지 확인합니다.

방화벽에서 구성하는 라우팅된 각 레이어 3 보안 체인에는 2개의 전용 레이어 3 이더넷 인터페이스가 필요하며, 이 인터페이스는 적절하게 구성된 라우터를 사용하여 하나의 레이어 3 보안 체인에 연결하거나 세션(로드 균형)을 최대 64개의 레이어 3 보안 체인이나 스위치 또는 방화벽과 보안 체인 사이의 유사한 디바이스에 배포할 수 있습니다.

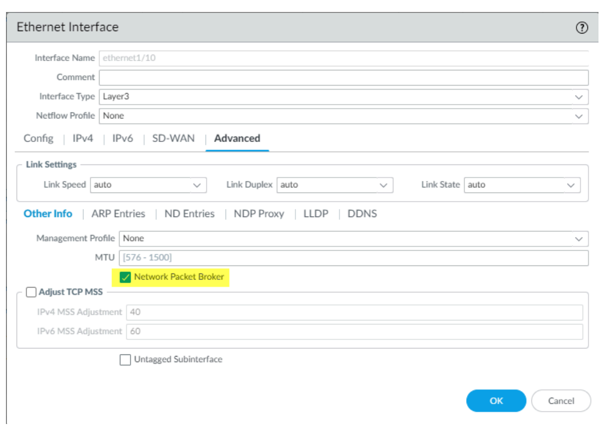
*네트워크 패킷 브로커는 라우팅된 레이어 **3** 보안 체인에서 **IPv6** 트래픽을 전달할 수 없습니다. **IPv6** 트래픽을 전달하려면 투명 브리지(레이어 **1)** 보안 체인을 사용하십시오.*

STEP 1 | 네트워크 패킷 브로커 전달 인터페이스로 2개의 Layer 3 이더넷 인터페이스를 활성화합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택합니다.
2. 두 개의 네트워크 패킷 브로커 전달 인터페이스 중 하나로 사용할 사용하지 않는 이더넷 인터페이스를 선택합니다.
3. 인터페이스 유형을 **Layer3**으로 설정합니다.
4. 구성 탭에서 인터페이스를 할당할 영역을 선택합니다.

   동일한 영역에서 두 보안 체인 인터페이스를 모두 구성해야 합니다.

5. 구성 탭에서 모범 사례로 전용 가상 라우터를 사용하거나 생성하여 인터페이스를 할당합니다. 전용 가상 라우터를 사용하면 네트워크 패킷 브로커 인터페이스 트래픽이 다른 트래픽과 분리된 상태로 유지됩니다.
6. 고급을 선택한 다음 네트워크 패킷 브로커를 선택하여 인터페이스를 활성화합니다.



7. 확인을 클릭하여 인터페이스 구성을 저장합니다.
8. 사용하지 않는 다른 이더넷 인터페이스에서 이 절차를 반복하여 다른 네트워크 패킷 브로커 전달 인터페이스를 구성합니다.

STEP 2 | 라우팅된 레이어 3 보안 체인으로 트래픽을 전달하는 방법을 제어하도록 패킷 브로커 프로파일을 구성합니다.

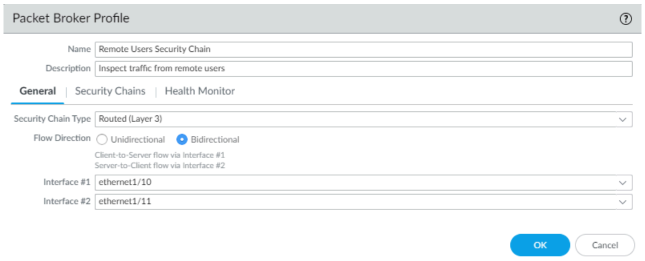
1. 개체 > 패킷 브로커 프로파일을 선택하고 새 프로파일을 추가하거나 기존 프로파일을 수정합니다.
2. 목적을 쉽게 식별할 수 있도록 프로파일에 이름과 설명을 지정합니다.
3. 일반 탭에서:
   - 보안 체인 유형으로 라우팅**(**레이어 **3)**을 선택합니다.
   - 흐름 방향을 선택합니다.

     네트워크 토폴로지는 단방향 또는 양방향 흐름을 사용할지 여부를 결정합니다**.** 성능은 어느 방법을 사용해도 거의 동일합니다**.**

     하나의 방화벽 인터페이스를 사용하여 c2s 및 s2c 세션 흐름을 모두 보안 체인으로 전달하고 다른 방화벽 인터페이스를 사용하여 보안 체인에서 두 세션 흐름을 다시 수신하려면 단방향을 선택합니다.

     인터페이스 **#1**을 사용하여 c2s 흐름을 보안 체인으로 전달하고 보안 체인에서 s2c 흐름을 수신하고 인터페이스 **#2**를 사용하여 s2c 흐름을 보안 체인으로 전달하고 보안 체인에서 c2s 흐름을 수신하려면 양방향을 선택합니다. .
   - **Interface #1** 및 **Interface #2**에서 네트워크 패킷 브로커 전달 인터페이스 쌍을 지정합니다. 네트워크 패킷 브로커(1단계 참조)를 사용하려면 두 인터페이스 모두 이미 활성화되어 있어야 합

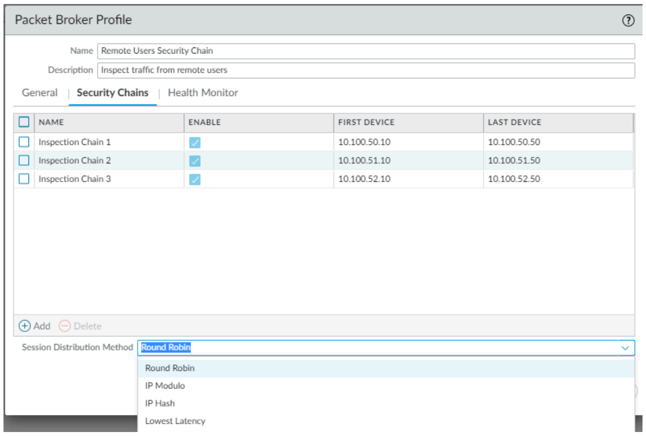
니다. 어떤 인터페이스가 **Interface #1**이고 어떤 인터페이스가 **Interface #2**인지 설정할 때 흐름의 방향성에 주의하십시오.



세션 분배(로드 밸런싱)는 새 세션에만 적용됩니다. 방화벽은 세션 중에 트래픽을 재조정하지 않습니다. 방화벽은 상태가 "작동"(활성, 정상)인 보안 체인에만 세션을 배포합니다.

4. 보안 체인 탭에서 연결하려는 라우팅된 각 레이어 3 보안 체인의 첫 번째 및 마지막 디바이스의 IP 주소를 추가합니다. 하나 이상의 보안 체인을 지정해야 합니다. 그렇지 않으면 방화벽이 트래픽을 체인으로 라우팅할 수 없고 프로파일을 저장할 수 없습니다.

   라우팅된 레이어 3 보안 체인을 여러 개 지정하는 경우 적절한 라우팅을 수행하기 위해 방화벽과 보안 체인 사이에 올바르게 구성된 라우터, 스위치 또는 유사한 디바이스도 배치해야 합니다. 또한 보안 체인 간의 트래픽 로드 밸런싱을 위해 세션 배포 방법을 지정합니다.



5. 상태 모니터 탭에서:

   - 보안 체인에 장애가 발생할 경우 발생하는 상황을 제어할 수 있도록 수행할 상태 모니터링 유형을 선택합니다.

     경로 모니터링, **HTTP** 모니터링 및 **HTTP** 모니터링 대기 시간 중에서 하나, 둘 또는 모두를 선택할 수 있습니다.

     경로 모니터링 - ping을 사용하여 디바이스 연결을 확인합니다.

     HTTP 모니터링 - 디바이스 가용성 및 응답 시간을 확인합니다.

     HTTP 모니터링 대기 시간 - 디바이스 처리 속도와 효율성을 확인합니다. 이 옵션을 선택하면 **HTTP** 모니터링도 자동으로 활성화됩니다.

   - 하나 이상의 상태 모니터링 유형을 활성화하면 보안 체인 상태 오류가 있는 경우 방화벽이 보안 체인 트래픽을 처리하는 방법을 결정하는 상태 확인 오류 시 옵션이 활성화됩니다.

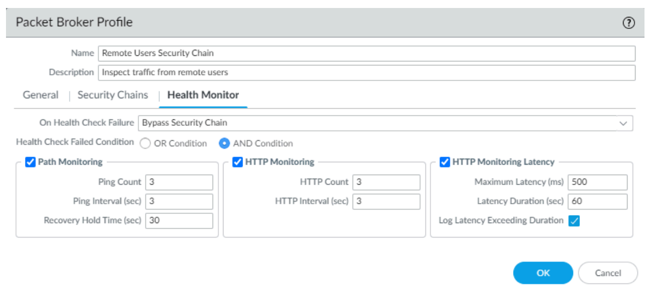
라우팅된 레이어 3 네트워크 패킷 브로커 인터페이스의 한 세트에 여러 보안 체인을 구성하는 경우 보안 체인 오류가 발생하면 트래픽이 나머지 정상적인 보안 체인으로 장애 조치됩니다. 장애 조치 트래픽을 처리하는 데 사용할 수 있는 보안 체인이 없는 경우 방화벽은 상태 확인 실패 시 구성된 작업을 수행합니다. 옵션은 보안 체인 우회 및 세션 차단입니다.

보안 체인 우회 - 방화벽은 트래픽을 보안 체인 대신 대상으로 전달하고 구성된 보안 프로파일 및 보호를 트래픽에 적용합니다.

세션 차단 - 방화벽이 세션을 차단합니다.

선택하는 방법은 보안 체인을 통해 트래픽을 실행할 수 없는 경우 트래픽을 처리할 방법에 따라 다릅니다.

- 상태 확인 옵션을 하나 이상 선택하는 경우, 방화벽이 상태 확인에 실패했다고 기록하길 원하는지(상태 확인 실패 조건), 모니터링 옵션 중 하나라도 실패한 조건(**OR** 조건)을 기록하는 경우 또는 모든 선택한 모니터링 옵션은 실패한 조건(**AND** 조건)을 기록하는지 선택합니다. 예를 들어 세 가지 상태 확인 옵션을 모두 활성화하고 옵션 중 하나가 실패 조건을 기록하는 경우 **OR** 조건을 선택하면 방화벽은 보안 체인 연결이 실패한 것으로 간주하고 상태 확인 실패 시에서 지정한 작업을 실행합니다. **AND** 조건을 선택한 경우 두 가지 상태 메트릭이 여전히 정상이므로 방화벽은 연결을 정상으로 간주합니다.



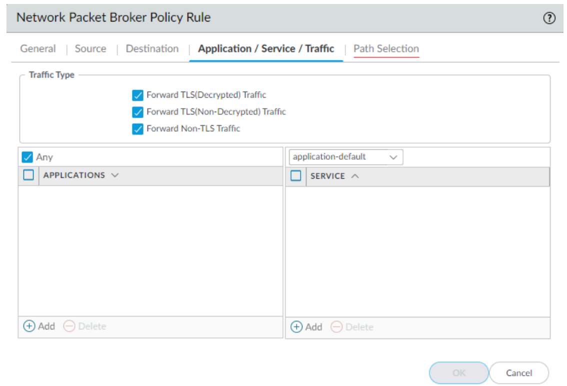
6. 확인을 클릭하여 프로파일을 저장합니다.

STEP 3 | 라우팅된 레이어 3 보안 체인으로 전달할 트래픽을 정의하도록 패킷 브로커 정책을 구성합니다.

1. 정책 > 네트워크 패킷 브로커를 선택하고 새 정책 규칙을 추가하거나 기존 정책 규칙을 수정합니다.
2. 일반 탭에서 정책 규칙의 이름 및 설명을 지정하여 목적을 쉽게 식별하고 감사 설명을 추가하고 사용하는 경우 태그를 적용합니다.
3. 소스 탭에서 보안 체인에 규칙을 전달할 트래픽의 소스 영역, IP 주소, 사용자 및 디바이스를 식별합니다.
4. 대상 탭에서 규칙이 보안 체인에 전달할 트래픽의 대상 영역, IP 주소 및 디바이스를 식별합니다.
5. 애플리케이션/서비스/트래픽 탭에서 규칙이 보안 체인에 전달할 애플리케이션 및 서비스를 식별합니다. 규칙이 내부 사용자 지정 애플리케이션과 같이 비표준 포트를 사용할 것으로 예상되는 애플리케이션을 제어하지 않는 한 비표준 포트를 사용하여 회피 동작을 나타내는 애플리케이션이 차단되도록 서비스를 애플리케이션 기본값으로 설정하는 것이 가장 좋습니다.

   트래픽 유형에 대해 규칙이 보안 체인에 전달할 모든 트래픽 유형을 선택하십시오. **TLS(Decrypted)** 트래픽 전달이 기본 선택입니다. **Forward TLS(Decrypted)** 트래픽, **Forward**

TLS(Non-Decrypted) 및 **Forward Non-TLS** 트래픽의 조합을 선택하여 보안 체인으로 전달할 수 있습니다.



6. 경로 선택 탭에서 2단계에서 만든 패킷 브로커 프로파일을 선택하거나 새 프로파일을 만들어 정책 규칙이 제어하는 트래픽을 보안 체인으로 보내는 방법을 제어합니다.

STEP 4 | 서로 다른 전용 방화벽 인터페이스 쌍을 사용하는 별도의 라우팅된 레이어 3 보안 체인을 생성하려면 1단계부터 3단계까지 반복하여 더 많은 네트워크 패킷 브로커 보안 체인을 생성하십시오. 네트워크 패킷 브로커 전달 인터페이스로 사용되는 2레이어 3 이더넷 인터페이스는 보안 체인 전용이어야 하며 다른 용도로 사용하거나 다른 트래픽을 전달할 수 없습니다.

네트워크 패킷 브로커 HA 지원

보안 체인 오류로부터 보호하기 위해 패킷 브로커 프로파일에서 사용할 수 있는 경로 및 대기 시간 상태 모니터링 외에도 방화벽 오류로부터 보호하기 위해 네트워크 패킷 브로커 전달 인터페이스가 있는 방화벽에서 High Availability(HA)을 구성할 수도 있습니다. 경로 모니터링과 HA를 모두 구성하면 보안 체인 장애뿐만 아니라 방화벽 장애도 방지할 수 있습니다.

네트워크 패킷 브로커는 능동/수동 HA 쌍을 지원합니다. 전용 브로커 전달 인터페이스가 패킷 브로커 프로파일에 지정되어야 하기 때문에 활성/활성 HA 쌍은 지원되지 않습니다.

장애 조치 후 SSL 상태가 HA 노드 간에 동기화되지 않기 때문에 복호화된 SSL 트래픽이 재설정됩니다. 세션이 올바르게 동기화되고 TCP 시퀀스가 올바르게 다시 학습되면 일반 텍스트 트래픽이 재개됩니다.

네트워크 패킷 브로커에 대한 사용자 인터페이스 변경 사항

Network Packet Broker는 PAN-OS 8.1에 도입된 복호화 Broker 기능을 대체하고 암호 해독되지 않은 TLS 및 비TLS 트래픽과 암호 해독된 TLS 트래픽을 보안 체인으로 전달하는 기능을 포함하도록 기능을 확장합니다. Network Packet Broker를 지원하기 위해 PAN-OS 10.2 사용자 인터페이스가 다음과 같이 변경되었습니다.

- 새 정책(정책 > 네트워크 패킷 브로커)을 사용하면 보안 체인으로 포워드하도록 특정 트래픽을 구성하고 패킷 브로커 프로파일을 연결하여 지정된 트래픽을 보안 체인으로 포워드하는 방법을 제어할 수 있습니다.

  복호화 브로커는 복호화 정책 규칙을 사용하여 복호화된 ***TLS*** 트래픽만 보안 체인으로 전달했습니다**.** 새로운 네트워크 패킷 브로커 정책 규칙을 사용하면 해독된 ***TLS*** 트래픽뿐만 아니라 암호화된 ***TLS*** 트래픽 및 비***TLS*** 트래픽도 선택할 수 있습니다**.**

- 새 프로파일(개체 > 패킷 브로커 프로파일)은 이전 개체 > 복호화 > 복호화 브로커 프로파일을 대체하며 이를 통해 트래픽을 보안 체인으로 포워드하고 경로 및 대기 시간 상태를 모니터링하는 방법을 정확히 구성할 수 있습니다. 일반 탭에서 전용 방화벽 네트워크 패킷 브로커 포워딩 인터페이스 쌍을 입력하는 필드의 이름이 각각 "기본 인터페이스" 및 "보조 인터페이스"에서 인터페이스 **#1** 및 인터페이스 **#2** 변경되었습니다.
- 정책 > 네트워크 패킷 브로커를 선택하면 정책 최적화에서 규칙 사용 옵션을 선택하여 네트워크 패킷 브로커 정책 사용 정보를 볼 수 있습니다. 규칙 사용 통계는 사용하지 않는 Network Packet Broker 규칙을 유지해야 하는지 또는 규칙을 삭제하고 룰베이스를 강화하여 공격 표면을 줄일 수 있는지 평가하는 데 도움이 됩니다.
- Network Packet Broker가 Decryption Broker를 대체했기 때문에 복호화 정책은 더 이상 보안 체인에 대한 브로커링 트래픽을 처리하지 않습니다. 이러한 이유로 옵션 탭에서 암호 해독 및 포워드 옵션은 더 이상 정책에서 수행할 수 있는 작업이 아니며 이제 암호 해독 프로필만 암호 해독 정책에서 유효하기 때문에 전달 프로파일 필드도 제거되었습니다.
- **Network** > **Interfaces** > 이더넷에서 **Interface Type**을 레이어 3으로 설정한 후 **Advanced** 탭을 선택하면 Network Packet Broker의 포워딩 인터페이스로 인터페이스를 활성화하는 확인란의 이름이 "Decrypt Forward"에서 **Network Packet Broker**로 변경됩니다.
- **Device** > **Admin** 역할의 경우 웹 **UI**탭에 두 가지 변경 사항이 있습니다.
  - 정책에서 이제 **Network Packet Broker** 관리자 역할 권한을 구성할 수 있습니다.
  - 개체에서 **Decryption** > **Forwarding** 프로파일옵션이 제거되고 관리자 역할 권한에 대한 패킷 브로커 프로파일 옵션으로 대체됩니다.
- 방화벽에서 모니터 > 관리 사용자 지정 보고서에 대해 세부 로그에서 데이터베이스로 트래픽 로그를 선택하면 사용 가능한 열 목록에서 이제 보안 체인으로 전달을 선택할 수 있습니다.

  Panorama의 **Monitor** > **Manage Custom Reports**에 대해 세부 로그에서 **Panorama Traffic Log**를 데이터베이스로 선택하면 사용 가능한 열 목록에서 이제 보안 체인으로 전달을 선택할 수 있습니다.
- 트래픽 로그에서 "Decrypt Forward" 열의 이름이 **Forwarded to Security Chain**으로 변경되었습니다. 트래픽 로그의 상세 보기에서 플래그 섹션에서 "Decrypt Forwarded" 확인란의 이름이 **Forwarded to Security Chain**으로 변경되었습니다.

- 이 기능의 무료 라이센스는 "Decryption Broker"에서 **Packet Broker**로 이름이 변경되었습니다. 방화벽에 무료 Decryption Broker 라이선스가 있는 경우 PAN-OS 10.1로 업그레이드하면 이름이 자동으로 변경됩니다. 변경 사항은 이름에만 있으며 기능에는 영향을 주지 않습니다.

네트워크 패킷 브로커의 한계

대부분의 Palo Alto Networks 플랫폼은 Network Packet Broker를 지원하지만 일부는 지원하지 않으며 일부는 제한이 있습니다.

- Prisma Access 또는 NSX에서는 지원되지 않습니다.
- AWS, Azure 및 GCP는 라우팅된 레이어 3 보안 체인만 지원합니다.

Network Packet Broker에는 관리 방화벽용 Panorama에 대한 몇 가지 제한 사항과 몇 가지 사용 제한 사항이 있습니다. Panorama에서:

- Network Packet Broker 라이선스를 관리 방화벽에 푸시하는 경우 라이선스 및 관련 사용자 인터페이스 요소가 설치되도록 방화벽을 재부팅해야 합니다.
- 패킷 브로커 프로파일에서 특정 인터페이스를 구성하기 때문에 공유 컨텍스트에서 패킷 브로커 프로파일을 생성할 수 없습니다.
- 다른 디바이스 그룹은 동일한 패킷 브로커 프로파일을 공유할 수 없습니다.
- Panorama는 10.1 이전 PAN-OS 버전을 실행하는 방화벽이 포함된 디바이스 그룹에 네트워크 패킷 브로커 구성(네트워크 패킷 브로커 정책 규칙 및 프로파일)을 푸시할 수 없습니다.

  여러 PAN-OS 버전의 방화벽이 포함된 디바이스 그룹에서 네트워크 패킷 브로커를 사용하고 이러한 방화벽 중 일부가 10.1 이전의 PAN-OS 버전을 실행하는 경우 10.2 이전 방화벽을 PAN-OS로 업그레이드해야 합니다. Network Packet Broker 구성을 푸시하기 전에 디바이스 그룹에서 10.2 이전 방화벽을 제거하거나 10.2 이전 방화벽을 제거하십시오.

  Panorama를 사용하여 암호 해독 정책 규칙에 연결된 패킷 브로커 프로파일을 암호 해독 브로커 라이선스가 설치된 10.1 이전 방화벽으로 푸시할 수 있습니다. 규칙에 대한 작업(옵션 탭)은 암호 해독 및 포워드여야 하며 패킷 브로커 프로파일을 규칙에 연결해야 합니다(옵션 탭의 암호 해독 프로파일 설정). 10.2 이전 방화벽은 Packet Broker 프로파일을 Decryption Broker에 대한 Decryption Forwarding 프로파일로 사용합니다. 암호 해독 정책 규칙은 방화벽이 프로파일을 적용하는 트래픽을 결정합니다.

  복호화 정책 규칙이 제어하는 트래픽은 복호화된 SSL 트래픽이어야 합니다(Decryption Broker는 암호화된 SSL 트래픽 또는 일반 텍스트 트래픽을 지원하지 않음).
- PAN-OS 10.0에서 PAN-OS 10.1로 업그레이드하면 Decryption Broker에 사용되는 로컬 암호 해독 정책 규칙만 Network Packet Broker 규칙으로 마이그레이션됩니다. Panorama에서 방화벽으로 푸시된 암호 해독 브로커 정책 규칙은 Panorama에서 자동으로 마이그레이션되지만 방화벽에서는 자동으로 마이그레이션되지 않습니다. 방화벽에 로컬로 구성된 암호 해독 브로커 정책 규칙은 해당 방화벽의 네트워크 패킷 브로커 규칙으로만 마이그레이션됩니다. Panorama에 구성된 규칙의 경우 Panorama는 Panorama의 Network Packet Broker 규칙으로 마이그레이션된 암호 해독 브로커 규칙을 동기화하기 위해 방화벽에 또 다른 커밋 푸시를 수행해야 합니다.
- PAN-OS 10.2에서 PAN-OS 10.0으로 다운그레이드하면 네트워크 패킷 브로커 규칙이 자동으로 제거됩니다.

Network Packet Broker의 다음과 같은 몇 가지 사용 제한 사항:

- Network Packet Broker 방화벽이 SNAT(소스 네트워크 주소 변환)도 수행하고 트래픽이 일반 텍스트 트래픽인 경우 방화벽은 트래픽에 대해 NAT를 수행하고 트래픽을 보안 체인으로 전달합니다. 보안 체인 어플라이언스는 원래 소스 주소가 아닌 NAT 주소만 봅니다.

  1. 방화벽은 클라이언트의 트래픽에 대해 NAT를 수행합니다.
  2. 방화벽은 트래픽을 보안 체인으로 전달하고 모든 라우팅은 NAT 주소를 기반으로 해야 합니다.
  3. 패킷의 소스 주소는 이제 NAT 주소이므로 보안 체인 어플라이언스는 NAT 주소만 봅니다. 실제 클라이언트 원본 주소는 표시되지 않습니다.
  4. 보안 체인이 트래픽을 방화벽으로 반환할 때 방화벽은 사용자가 누구인지 알지 못합니다.

  해당 세션에 대한 트래픽 로그를 확인하고 패킷을 해당 로그와 연관시켜 소스 사용자가 세션에 대해 누구인지 알 수 있습니다. 트래픽 로그에는 원본 사용자를 확인할 수 있는 원본 주소와 SNAT 주소가 모두 포함됩니다.

  방화벽이 아닌 다른 디바이스에서 *NAT*를 수행하면 이 시나리오를 피할 수 있습니다.

- 복호화된 SSH, 멀티캐스트 및 브로드캐스트 트래픽은 지원되지 않습니다.
- RSA 인증서가 사용되는 경우 SSL 인바운드 검사에 대해 클라이언트 인증이 지원되지 않습니다.
- 레이어 1 투명 브리지 모드에서 보안 체인이 실패하면 투명 브리지 연결을 사용할 때 전용 Network Packet Broker 방화벽 인터페이스의 각 쌍이 하나의 보안 체인에만 연결되기 때문에 장애 조치가 없습니다. (레이어 1에서는 트래픽을 라우팅할 수 없으며 다음에 연결된 디바이스로만 전달할 수 있습니다.)
- 레이어 1 트랜스페이런트 모드에서만 IPv6 트래픽을 전달할 수 있습니다. 라우팅(레이어 3) 모드에서는 IPv6 트래픽을 전달할 수 없습니다.
- 터널 또는 루프백 인터페이스를 Network Packet Broker 인터페이스로 사용할 수 없습니다.
- Network Packet Broker 인터페이스는 동적 라우팅 프로토콜을 사용할 수 없습니다.
- 두 인터페이스는 동일한 영역에 있어야 합니다.
- 보안 체인의 디바이스는 방화벽이 수정된 세션을 원래 세션과 일치시킬 수 없어 트래픽을 삭제하므로 원래 세션의 소스 IP 주소, 대상 IP 주소, 소스 포트, 대상 포트 또는 프로토콜을 수정할 수 없습니다.
- Network Packet Broker의 고가용성은 능동/수동 HA 방화벽 쌍에 대해서만 지원됩니다. 네트워크 패킷 브로커의 고가용성은 활성/활성 방화벽 쌍에 대해 지원되지 않습니다.
- SSL 트래픽에는 고가용성이 지원되지 않습니다. 장애 조치 시 SSL 세션이 재설정됩니다.
- PAN-OS 10.0에서 PAN-OS 10.1로 업그레이드하면 Decryption Broker에 사용되는 로컬 암호 해독 정책 규칙이 Network Packet Broker 규칙으로 마이그레이션됩니다.
- PAN-OS 10.2에서 PAN-OS 10.0으로 다운그레이드하면 네트워크 패킷 브로커 규칙이 자동으로 제거됩니다.

네트워크 패킷 브로커 문제 해결

네트워크 패킷 브로커를 구성하는 데 문제가 발생하면 다음 항목을 확인하십시오.

- 방화벽 구성:
  - 전달 인터페이스 쌍에서 다음 홉 경로가 올바른 디바이스 인터페이스를 지정하는지 확인하십시오.
  - 체인 디바이스 및 방화벽 인터페이스의 IP 주소를 확인하고 패킷 브로커 프로파일에 올바르게 입력되었는지 확인합니다.
  - HA가 활성화된 경우 프로파일에 올바른 인터페이스가 지정되었는지 확인합니다.
  - 체인을 통한 트래픽의 흐름 방향을 확인하십시오.
  - 프로파일이 적절한 보안 체인 유형을 나타내는지 확인하십시오.
- 보안 체인 구성, 확인:
  - 보안 체인의 각 어플라이언스에 대한 IP 주소, 다음 홉 주소 및 기본 게이트웨이.
  - IP 주소 지정, 다음 홉 및 기본 게이트웨이 구성 오류에 대한 방화벽과 보안 체인(라우터, 스위치 등) 사이의 모든 디바이스 구성.
  - 방화벽과 체인 사이의 경로입니다.
- 방화벽 트래픽 로그를 확인하여 중개된 트래픽에 대해 예상대로 설정된 "전달됨" 플래그가 표시되는지 확인합니다.
- 유용한 CLI 명령은 다음과 같습니다.
  - `룰베이스 네트워크 패킷 브로커 표시`
  - `실행 중인 네트워크 패킷 브로커 상태 표시`
  - `실행 중인 네트워크 패킷 브로커 통계 표시`
  - `실행 중인 애플리케이션 캐시 모두 표시`
  - `실행 중인 애플리케이션 설정 표시` - App-ID 캐시가 활성화되어 있는지, 캐시가 App-ID에 사용되는지 확인하고 캐시 임계값 설정 등을 확인합니다.

Advanced 라우팅

PAN-OS® 10.2는 방화벽을 확장하고 대규모 데이터 센터, ISP, 엔터프라이즈 및 클라우드 사용자에게 안정적이고 고성능이며 가용성이 높은 라우팅 기능을 제공할 수 있는 고급 라우팅 엔진을 제공합니다. 고급 라우팅 엔진은 표준 기반 구성으로 작업을 단순화하므로 다른 라우터 공급업체와 유사하므로 학습 곡선이 줄어듭니다. 프로토콜 구성 프로파일과 세분화된 필터링 프로파일은 여러 논리적 라우터 및 가상 시스템에서 작동합니다. 경로 재배포는 재배포 프로파일을 사용하여 간소화됩니다. BGP 피어 그룹 및 피어는 구성을 상속하여 BGP를 보다 민첩하게 만들 수 있습니다.

고급 라우팅 엔진은 정적 경로, BGP, MP-BGP, OSPFv2, OSPFv3, RIPv2, IPv4 멀티캐스트 라우팅, BFD, 재분배, RIB로의 경로 필터링, 액세스 목록, 접두사 목록 및 경로 맵을 지원합니다.

지원되지 않는 기능은 레거시 라우팅 엔진에서 고급 라우팅 엔진으로 전달되지 않습니다. 필요한 모든 기능이 지원된다는 것을 알 때까지 고급 라우팅을 사용하도록 설정해서는 안 됩니다.

고급 라우팅 엔진을 지원하는 모델은 다음과 같습니다. 해당 모델:

- PA-7000 시리즈
- PA-5400 시리즈
- PA-5200 시리즈
- PA-3400 시리즈
- PA-3200 시리즈
- PA-400 시리즈
- VM-Series
- M-700 어플라이언스
- M-600 어플라이언스
- M-500 어플라이언스
- M-300 어플라이언스
- M-200 어플라이언스

고급 라우팅 프로파일에 대해 알아보고 다음 작업을 수행하여 고급 라우팅을 구성합니다.

- 고급 라우팅 사용
- 논리적 라우터 개요
- 논리 라우터 구성
- 정적 경로 만들기
- 고급 라우팅 엔진에서 BGP 구성
- BGP 라우팅 프로파일 만들기
- 고급 라우팅 엔진에 대한 필터 만들기

- 고급 라우팅 엔진에서 OSPFv2 구성
- OSPF 라우팅 프로파일 만들기
- 고급 라우팅 엔진에서 OSPFv3 구성
- OSPFv3 라우팅 프로파일 만들기
- 고급 라우팅 엔진에서 RIPv2 구성
- RIPv2 라우팅 프로파일 만들기
- BFD 프로파일 만들기
- (PAN-OS 10.2.2 이상 10.2 릴리스) IPv4 멀티캐스트 구성
- (PAN-OS 10.2.2 이상 10.2 릴리스) 멀티캐스트 라우팅 프로파일 생성
- (PAN-OS 10.2.2 이상 10.2 릴리스) IPv4 MRoute 생성

고급 라우팅 사용

지원되는 방화벽에는 레거시 라우팅 엔진을 사용하는 구성과 고급 라우팅 엔진을 사용하는 구성이 있을 수 있지만 한 번에 하나의 라우팅 엔진만 적용됩니다. 방화벽이 사용할 엔진을 변경할 때마다(각각 고급 엔진 또는 레거시 엔진에 액세스하기 위해 고급 라우팅을 사용하거나 사용하지 않도록 설정) 구성을 커밋하고 방화벽을 재부팅해야 변경 내용이 적용됩니다.

고급 라우팅 엔진으로 전환하기 전에 현재 구성을 백업하십시오.

마찬가지로 고급 라우팅을 사용하거나 사용하지 않도록 설정하는 템플릿으로 Panorama를 구성하는 경우 템플릿을 커밋하고 디바이스에 푸시한 후 변경 내용을 적용하려면 템플릿의 디바이스를 다시 부팅해야 합니다.

*Panorama*를 구성할 때 모두 동일한 고급 라우팅 설정(모두 사용 또는 모두 사용 안 함)을 사용하는 디바이스에 대한 디바이스 그룹 및 템플릿을 만듭니다. *Panorama*는 고급 라우팅이 활성화된 구성을 고급 라우팅을 지원하지 않는 저가형 방화벽으로 푸시하지 않습니다. 이러한 방화벽의 경우 *Panorama*는 레거시 구성이 있는 경우 레거시 구성을 푸시합니다.

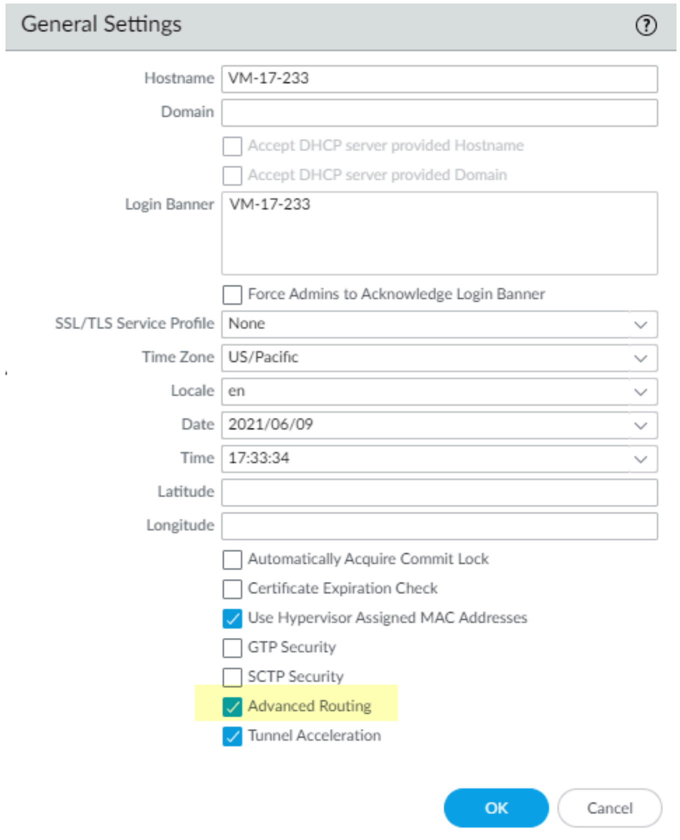
고급 라우팅 엔진은 여러 논리적 라우터(레거시 라우팅 엔진의 가상 라우터라고 함)를 지원합니다. 지원되는 논리적 라우터의 수는 방화벽 모델에 따라 다르며 레거시 라우팅 엔진에서 지원되는 가상 라우터 수와 동일합니다. 고급 라우팅 엔진에는 보다 편리한 메뉴 옵션이 있으며 BGP 피어 그룹 또는 피어에 적용하는 프로파일(예: 인증, 타이머, 주소 패밀리 또는 재배포 프로파일)에서 쉽게 구성할 수 있는 많은 설정이 있습니다. 고급 라우팅 엔진에는 많은 정적 경로, OSPF, OSPFv3, RIPv2, 멀티캐스트 및 BFD 설정도 있습니다.

고급 라우팅 엔진은 RIB 필터링을 지원하므로 다른 라우팅 프로토콜에서 받은 정적 경로 또는 경로와 일치하는 경로 맵을 만들어 논리적 라우터의 RIB에 설치된 경로를 필터링할 수 있습니다. 이 기능은 RIB 또는 FIB 용량이 작은 방화벽에서 유용합니다. 다른 곳에 필요한 메모리를 사용하지 않고도 필요한 라우팅 업데이트를 전파할 수 있습니다.

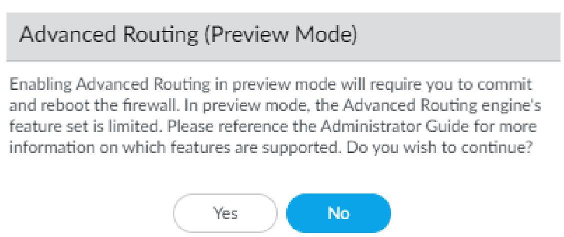
STEP 1 | 고급 라우팅을 사용하도록 설정하기 전에 현재 구성을 백업합니다.

STEP 2 | 고급 라우팅 엔진을 사용하도록 설정합니다.

1. 디바이스 > 설정 > 관리를 선택하고 일반 설정을 수정합니다.
2. 고급 라우팅을 사용하도록 설정합니다.



3. 확인을 클릭하기 전에 레거시 라우팅 엔진에 대한 구성을 백업했는지 확인하십시오.
4. 확인을 클릭합니다.
5. 미리보기 모드에 대한 메시지가 나타납니다. 계속하려면 예를 클릭합니다.

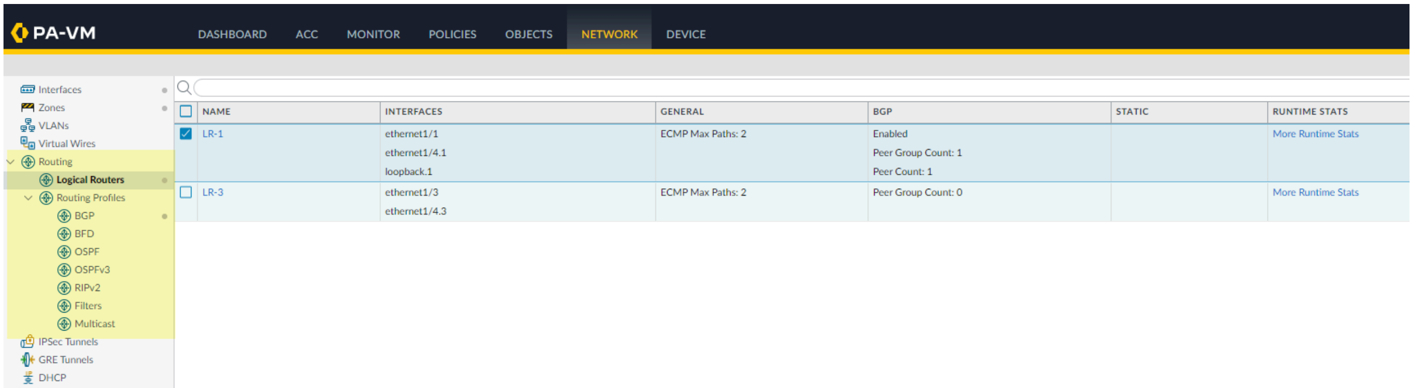


6. 커밋합니다.
7. 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.

STEP 3 | 방화벽에 다시 로그인합니다.

STEP 4 | 네트워크를 선택합니다.

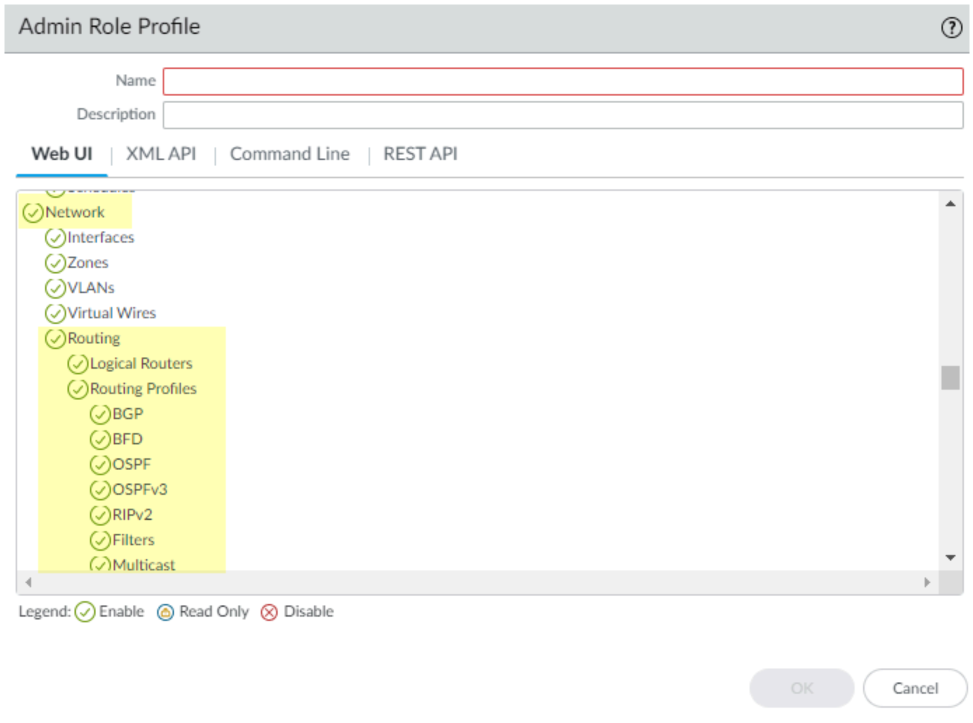
레거시 메뉴의 단일 항목(가상 라우터)보다 업계 표준이고 더 자세한 메뉴 항목을 확인합니다. 라우팅에는 논리적 라우터 및 라우팅 프로파일이 포함되며, 여기에는 **BGP**, **BFD**, **OSPF**, **OSPFv3**, **RIPv2**, 필터 및 멀티캐스트가 포함됩니다.



STEP 5 | 인터페이스를 선택하고 고정 IP 주소 또는 인터페이스를 DHCP 클라이언트로 구성(으)로 하나 이상의 계층 3 인터페이스를 구성합니다.

STEP 6 | (선택 사항) 관리자 역할 프로파일을 만들어 고급 라우팅 엔진에 대한 논리적 라우터 및 라우팅 프로파일에 대한 세부적인 액세스를 제어합니다.

1. 디바이스 > 관리자 역할을 선택하고 이름으로 관리자 역할 프로파일을 추가합니다.
2. 웹 **UI**를 선택합니다.
3. 다음 옵션을 활성화, 비활성화하거나 읽기 전용을 선택합니다. 네트워크, 라우팅, 논리적 라우터, 라우팅 프로파일, **BGP**, **BFD**, **OSPF**, **OSPFv3**, **RIPv2**, 필터 및 멀티캐스트(기본값은 사용)



4. 확인을 클릭합니다.
5. 관리자에게 역할을 할당합니다. 방화벽 관리자 계정을 구성합니다.

STEP 7 | 변경 사항을 커밋합니다.

STEP 8 | 논리적 라우터를 구성하여 계속합니다.

논리적 라우터 개요

방화벽은 논리적 라우터를 사용하여 정적 경로를 수동으로 정의하거나 하나 이상의 레이어 3 라우팅 프로토콜 (동적 경로)에 참여함으로써 다른 서브넷에 대한 레이어 3 경로를 가져옵니다. 방화벽이 이러한 방법을 통해 얻은 경로는 방화벽의 IP RIB(라우팅 정보 기반)를 채웁니다. 패킷이 도착한 서브넷과 다른 서브넷으로 향하는 경우 논리 라우터는 RIB에서 최상의 경로를 가져와 FIB(전달 정보 베이스)에 배치하고 패킷을 FIB에 정의된 다음 홉 라우터로 전달합니다. 방화벽은 이더넷 스위칭을 사용하여 동일한 IP 서브넷에 있는 다른 디바이스에 도달합니다. (ECMP을(를) 사용하는 경우 FIB로 가는 하나의 최상의 경로에 대한 예외가 발생합니다. 이 경우 모든 동일 비용 경로는 FIB로 이동합니다.)

방화벽에 정의된 이더넷, VLAN 및 터널 인터페이스는 레이어 3 패킷을 수신 및 포워드합니다. 대상 존은 포워드 기준에 따라 나가는 인터페이스에서 파생되며 방화벽은 정책 규칙을 참조하여 각 패킷에 적용되는 보안 정책을 식별합니다. 다른 네트워크 디바이스로 라우팅하는 것 외에도 가상 라우터는 다음 홉이 다른 가상 라우터를 가리키도록 지정된 경우 동일한 방화벽 내의 다른 가상 라우터로 라우팅할 수 있습니다.

동적 라우팅 프로토콜 (BGP, OSPF, OSPFv3 또는 RIP) 에 참여하고 정적 경로를 추가할 수레이어 3 인터페이스 구성 있습니다. 또한 가상 라우터 간에 공유되지 않는 별도의 경로 집합을 유지 관리하는 여러 가상 라우터를 생성할 수 있으므로 서로 다른 인터페이스에 대해 서로 다른 라우팅 동작을 구성할 수 있습니다.

각 논리 라우터에서 루프백 인터페이스를 구성하고 두 루프백 인터페이스 간에 정적 경로를 만든 다음 이러한 두 인터페이스 간에 피어링하도록 동적 라우팅 프로토콜을 구성하여 한 논리적 라우터에서 다른 논리 라우터로의 동적 라우팅을 구성할 수 있습니다.

방화벽에 정의된 각 계층 3 이더넷, 루프백, VLAN 및 터널 인터페이스는 논리적 라우터와 연결되어야 합니다. 각 인터페이스는 하나의 논리적 라우터에만 속할 수 있지만 논리적 라우터에 대해 여러 라우팅 프로토콜과 정적 경로를 구성할 수 있습니다. 논리 라우터에 대해 구성하는 정적 경로 및 동적 라우팅 프로토콜에 관계없이 한 가지 일반 구성이 필요합니다.

논리 라우터 구성

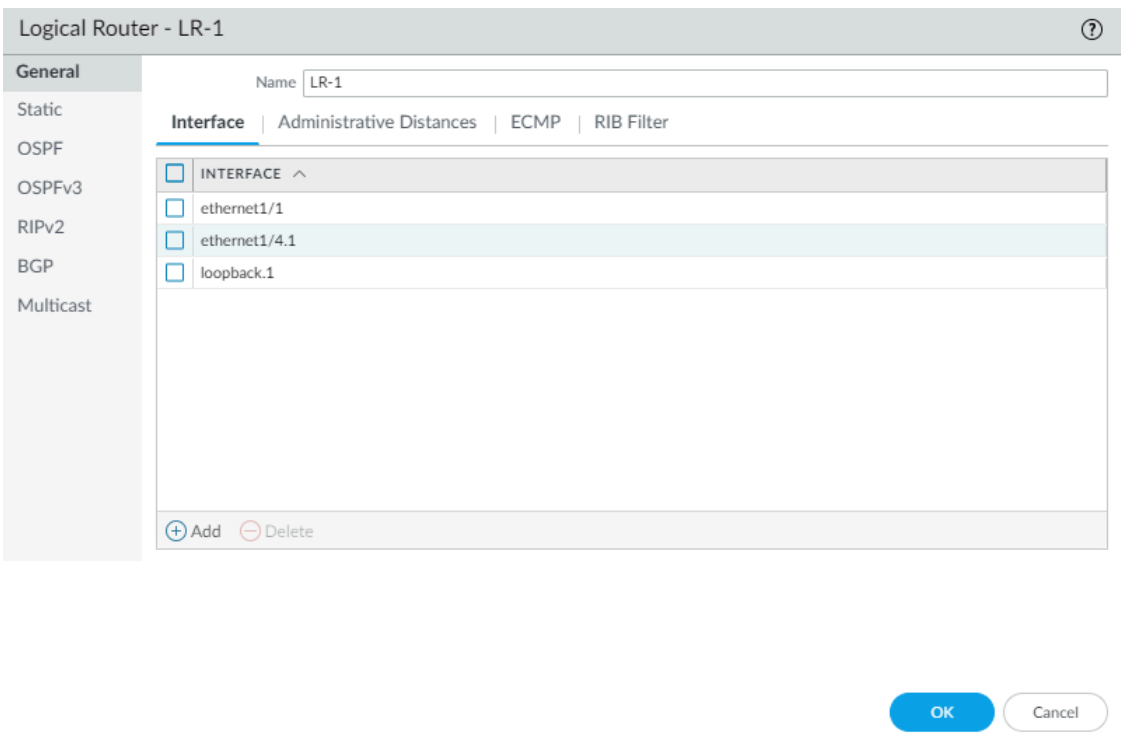
네트워크 라우팅을 수행하려면 고급 라우팅 엔진에서 하나 이상의 논리 라우터를 구성해야 합니다. 기본 논리 라우터는 없습니다. 논리적 라우터는 별도의 라우팅 정보 기반을 유지하고 경로가 다른 논리적 라우터에 노출되지 않도록 합니다. 고급 라우팅 엔진에 대해 지원되는 논리적 라우터의 수는 방화벽 모델에 따라 다릅니다.

논리적 라우터를 구성하려면 먼저 해야 합니다고급 라우팅 사용.

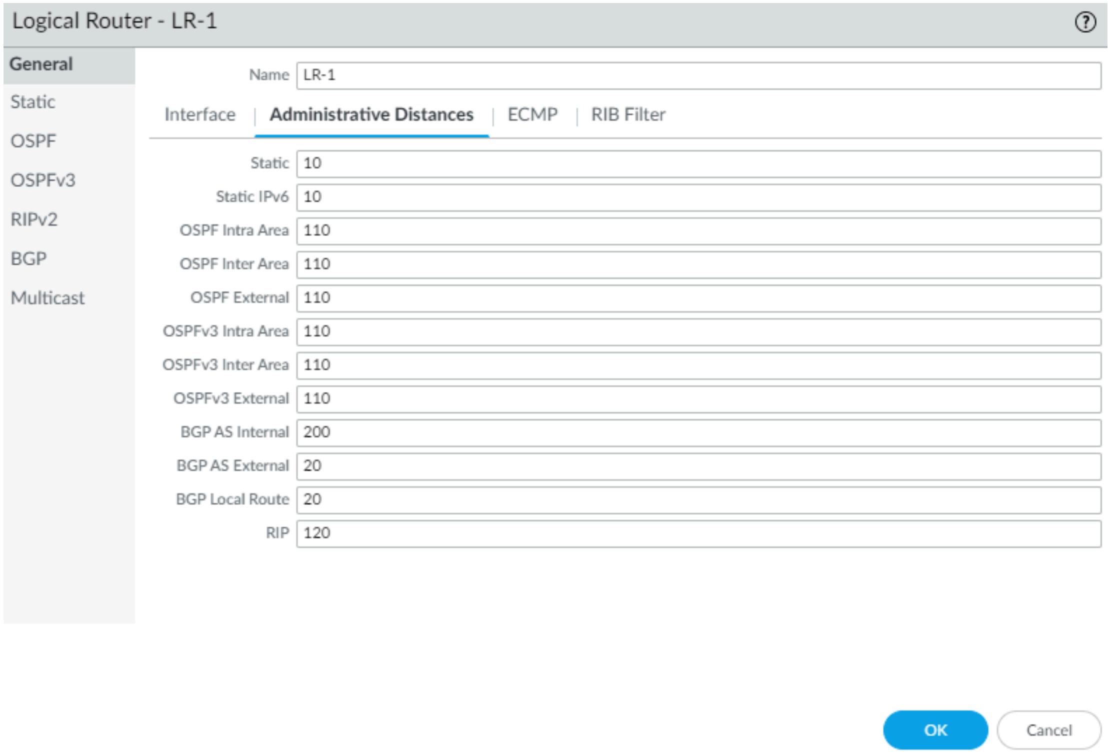
STEP 1 | 네트워크 > 라우팅 > 논리 라우터를 선택하고 최대 31자를 사용하여 이름으로 논리 라우터를 추가합니다. 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 영숫자 문자, 밑줄(_) 또는 하이픈(-) 의 조합을 포함할 수 있습니다. 점(.) 이나 공백은 사용할 수 없습니다.

STEP 2 | 논리적 라우터에 인터페이스를 추가합니다.

1. 논리 라우터 일반 탭에서 인터페이스 탭을 선택합니다.
2. 인터페이스 목록에서 선택하여 논리 라우터에 인터페이스를 추가합니다. 인터페이스는 하나의 논리적 라우터에만 속할 수 있습니다. LR-1이라는 논리적 라우터에 대한 다음 예와 같이 인터페이스를 더 추가하려면 이 단계를 반복합니다.



STEP 3 | (선택 사항) 다양한 유형의 경로에 대한 전역 관리 거리(기본 설정에서) 를 변경하려면 관리 거리를 선택합니다.

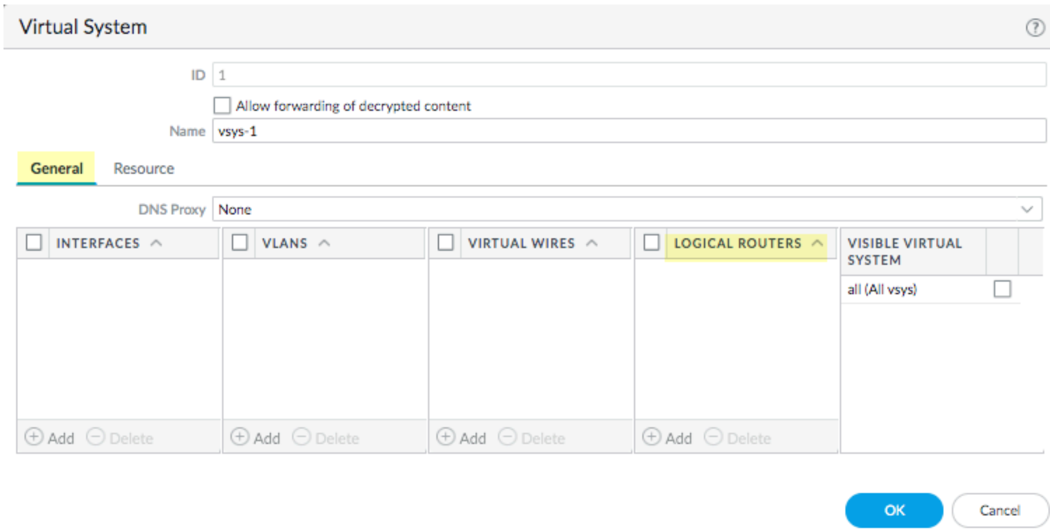


- 정적 - 범위는 1~255입니다. 기본값은 10입니다.
- 정적 **IPv6** - 범위는 1~255입니다. 기본값은 10입니다.
- **OSPF** 내부 영역 - 범위는 1~255입니다. 기본값은 110입니다.
- **OSPF** 영역 간 - 범위는 1~255입니다. 기본값은 110입니다.
- **OSPF** 외부 - 범위는 1~255입니다. 기본값은 110입니다.
- **OSPFv3** 영역 간 - 범위는 1~255입니다. 기본값은 110입니다.
- **OSPFv3** 영역 간 - 범위는 1~255입니다. 기본값은 110입니다.
- **OSPFv3** 외부 - 범위는 1~255입니다. 기본값은 110입니다.
- **BGP AS** 내부 - 범위는 1~255입니다. 기본값은 200입니다.
- **BGP AS** 외부 - 범위는 1~255입니다. 기본값은 20입니다.
- **BGP** 로컬 경로 - 범위는 1~255입니다. 기본값은 120입니다.
- **RIP** - 범위는 1~255입니다. 기본값은 120입니다.

STEP 4 | 확인을 클릭합니다.

STEP 5 | (여러 가상 시스템을 지원하는 방화벽에서) 가상 시스템에 논리 라우터를 할당합니다.

1. 디바이스 > 가상 시스템을 선택하고 가상 시스템 및 일반을 선택합니다.
2. 하나 이상의 논리 라우터를 추가합니다.
3. 확인을 클릭합니다.



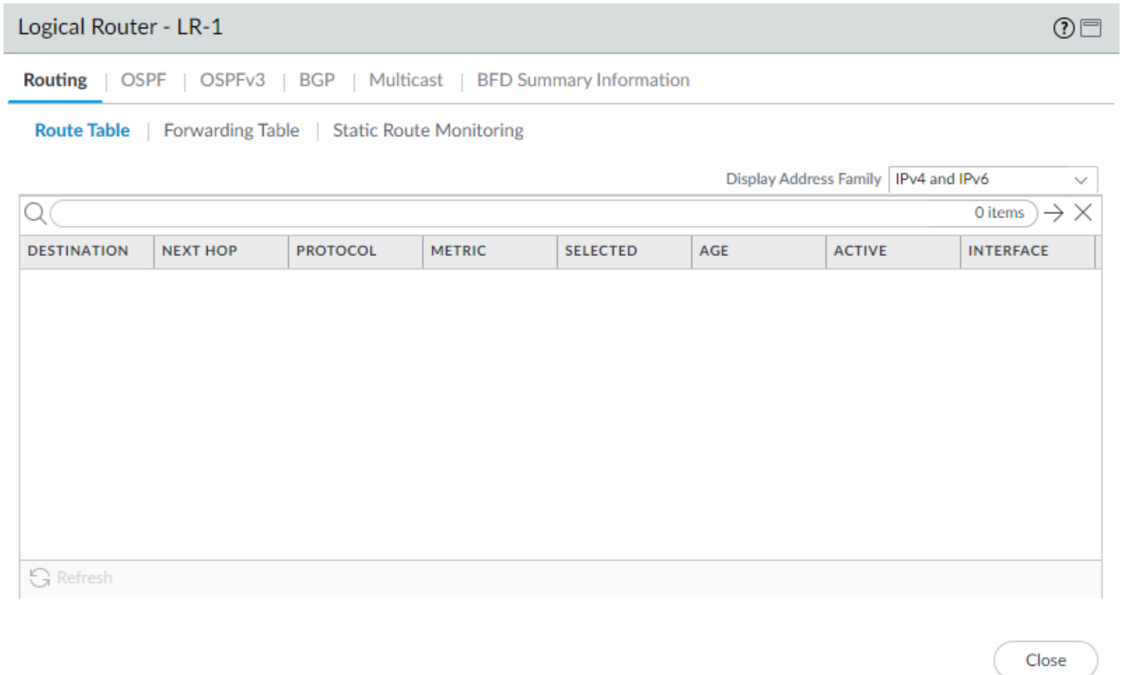
STEP 6 | 확인을 클릭합니다.

STEP 7 | (선택 사항) 네트워크 > 라우팅 > 논리 라우터로 이동하여 논리 라우터에 대한 ECMP를 구성하고 논리 라우터를 선택한 후 일반 > **ECMP**를 선택합니다. 레거시 라우팅 엔진의 가상 라우터와 마찬가지로 논리 라우터에 대해 ECMP를 구성합니다.

STEP 8 | 변경 사항을 커밋합니다.

STEP 9 | (선택 사항) 논리 라우터에 대한 런타임 통계를 봅니다.

1. 특정 논리 라우터의 경우 맨 오른쪽에서 추가 런타임 통계를 선택합니다.
2. 모든 프로토콜의 라우팅 테이블을 보려면 라우팅 탭에서 라우팅 테이블 및 주소 패밀리 표시를 선택합니다. **IPv4** 및 **IPv6**, **IPv4** 전용 또는 **IPv6** 전용 중에서 선택할 수 있습니다.



3. FIB(전달 정보 베이스) 의 항목을 보려면 전달 테이블을 선택합니다.
4. 정적 경로 모니터링을 선택하여 모니터링 중인 정적 경로를 확인합니다.
5. **BGP** 탭을 선택한 다음 요약을 선택하여 BGP 설정을 확인합니다.
6. BGP 피어 설정을 보려면 피어를 선택합니다.
7. BGP 피어 그룹 설정을 보려면 피어 그룹을 선택합니다.
8. 경로 및 주소 패밀리 표시 선택: **IPv4** 및 **IPv6**, **IPv4** 전용 또는 **IPv6** 전용을 선택하여 BGP 경로의 속성을 볼 수 있습니다.

STEP 10 | CLI에 액세스하여 고급 라우팅 정보를 봅니다. PAN-OS CLI 퀵 스타트에는 CLI 치트 시트에 다음과 같은 명령이 나열되어 있습니다. 네트워킹.

정적 경로 만들기

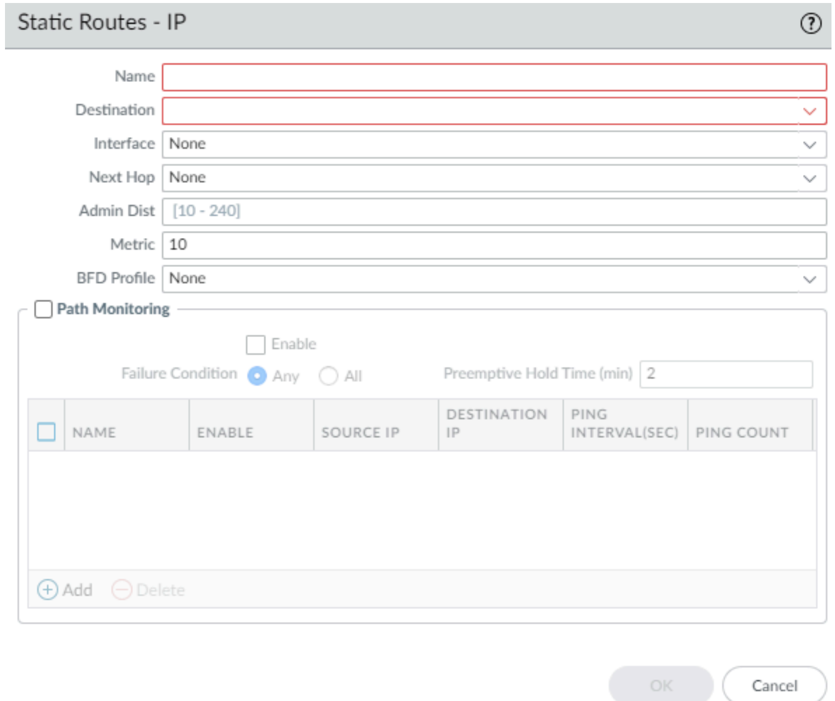
고급 라우팅 엔진에서 논리적 라우터에 대한 정적 경로를 만듭니다.

STEP 1 | 논리 라우터 구성.

STEP 2 | 정적 경로를 만듭니다.

1. 네트워크 > 라우팅 > 논리적 라우터를 선택하고 논리적 라우터를 선택합니다.
2. 정적을 선택하고 **IPv4** 또는 **IPv6** 정적 경로를 이름(최대 63자)으로 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.
3. 대상에 경로 및 넷마스크를 입력합니다(예: IPv4 주소의 경우 192.168.2.0/24, IPv6 주소의 경우 2001:db8:123:1::0/64). 기본 경로를 생성하는 경우 기본 경로(IPv4 주소의 경우 0.0.0.0/0 또는 IPv6 주소의 경우 ::/0)를 입력합니다. 또는 IP 넷마스크 유형의 주소 개체를 선택하거나 만들 수 있습니다.
4. 인터페이스의 경우 패킷이 다음 홉으로 이동하는 데 사용할 나가는 인터페이스를 지정합니다. 인터페이스를 지정하면 이 정적 경로의 다음 홉에 대해 경로 테이블의 인터페이스를 사용하는 대신 방화벽이 사용하는 인터페이스를 보다 엄격하게 제어할 수 있습니다.
5. 다음 홉에서 다음 중 하나를 선택합니다.
   - **IP** 주소 또는 **IPv6** 주소 - 특정 다음 홉으로 라우팅할 때 IP 주소(예: 192.168.56.1 또는 2001:db8:49e:1::1)를 입력합니다. IPv6 다음 홉 주소를 사용하려면 인터페이스에서 **IPv6**을 활성화(레이어 3 인터페이스 구성할 때)해야 합니다. 기본 경로를 만드는 경우 다음 홉에서 **IP** 주소를 선택하고 인터넷 게이트웨이의 IP 주소(예: 192.168.56.1 또는 2001:db8:49e:1::1)를 입력해야 합니다. 또는 IP 넷마스크 유형의 주소 개체를 만들 수 있습니다. 주소 개체에는 IPv4의 경우 /32 또는 IPv6의 경우 /128의 넷마스크가 있어야 합니다.
   - 다음 **LR** - 논리적 라우터 목록의 다음 논리적 라우터를 다음 홉으로 만들려면 선택합니다.
   - **FQDN** - 정규화된 도메인 이름을 입력합니다.
   - 폐기 - 이 대상으로 지정된 패킷을 삭제하려면 선택합니다.
   - 없음 - 경로에 대한 다음 홉이 없는 경우 선택합니다. 예를 들어, 지점간 연결은 패킷이 이동하는 방법이 한가지 뿐이므로 다음 홉이 필요하지 않습니다.
6. 정적 경로에 대한 관리자 거리를 입력합니다(범위는 10~240, 기본값은 10). 이 값은 논리적 라우터에 대해 지정된 정적 또는 정적 **IPv6** 관리 거리를 재정의합니다.
7. 정적 경로에 대한 측정항목을 입력합니다(범위는 1~65,535, 기본값은 10).

8. (선택 사항) BFD를 사용하려면 생성한 **BFD** 프로파일을 선택하거나 기본 프로파일을 선택하거나 BFD 프로파일을 생성하여 정적 경로에 적용합니다. 기본값은 없음**(BFD** 비활성화**)**입니다.



STEP 3 | (선택 사항) 정적 경로에 대한 경로 모니터링을 구성합니다. 최대 128개의 정적 경로를 모니터링할 수 있습니다.

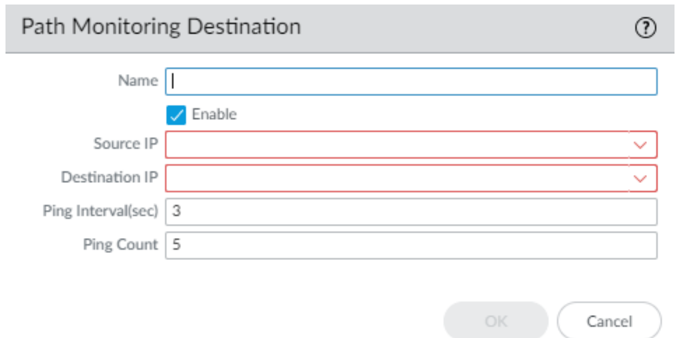
1. 경로 모니터링을 선택하여 경로 모니터링의 구성을 허용합니다(기본값은 사용 안 함).
2. 경로 모니터링을 사용하도록 설정합니다(기본값은 사용 안 함).
3. 실패 조건은 정적 경로에 대한 경로 모니터링이 모니터링되는 대상을 하나(임의) 또는 모든 모니터링되는 대상을 기반으로 하는지 여부를 결정합니다. 방화벽이 RIB 및 FIB에서 정적 경로를 제거하고 다음으로 낮은 메트릭이 있는 정적 경로를 추가하려면 ICMP에서 정적 경로에 대해 모니터링되는 대상 중 임의 또는 모두에 연결할 수 없는지 여부에 관계없이 실패 조건을 선택합니다.FIB와 동일한 목적지로 이동합니다.

   예를 들어 대상이 유지 관리를 위해 단순히 오프라인일 때 단일 모니터링 대상이 경로 실패를 알리는 가능성을 방지하려면 모두를 선택합니다.
4. (선택 사항) 선점 대기 시간**(**최소**)**을 지정하고, 방화벽이 정적 경로를 RIB에 다시 설치하기 전에 다운된 경로 모니터가 Up 상태로 유지되어야 하는 시간(분)입니다. 범위는 0~1,440이며, 기본

값은 2입니다. 0으로 설정하면 방화벽이 경로 모니터가 켜지는 즉시 RIB에 경로를 다시 설치합니다.

경로 모니터는 정적 경로에 대해 모니터링되는 모든 대상을 평가하고 일부 또는 모두 실패 조건에 따라 나타납니다. 보류 시간 동안 링크가 다운되거나 플랩되면 링크가 다시 시작되면 경로 모니터가 다시 시작되고 선점 대기 시간이 재설정되어 타이머가 0에서 다시 시작됩니다.

5. 이름으로 경로 모니터링 대상을 추가합니다.



6. 경로 모니터링 대상을 활성화합니다.
7. 소스 **IP**의 경우 모니터링되는 대상에 대한 ICMP ping에서 방화벽이 사용하는 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 선택하고 이더넷 인터페이스 행에서 동적 **DHCP** 클라이언트를 클릭합니다. IP 주소는 동적 IP 인터페이스 상태 창에 표시됩니다.
8. 대상 **IP**에 방화벽이 경로를 모니터링할 IP 주소 또는 주소 개체를 입력합니다. 모니터링되는 대상과 정적 경로 대상은 동일한 주소 패밀리(IPv4 또는 IPv6)를 사용해야 합니다.

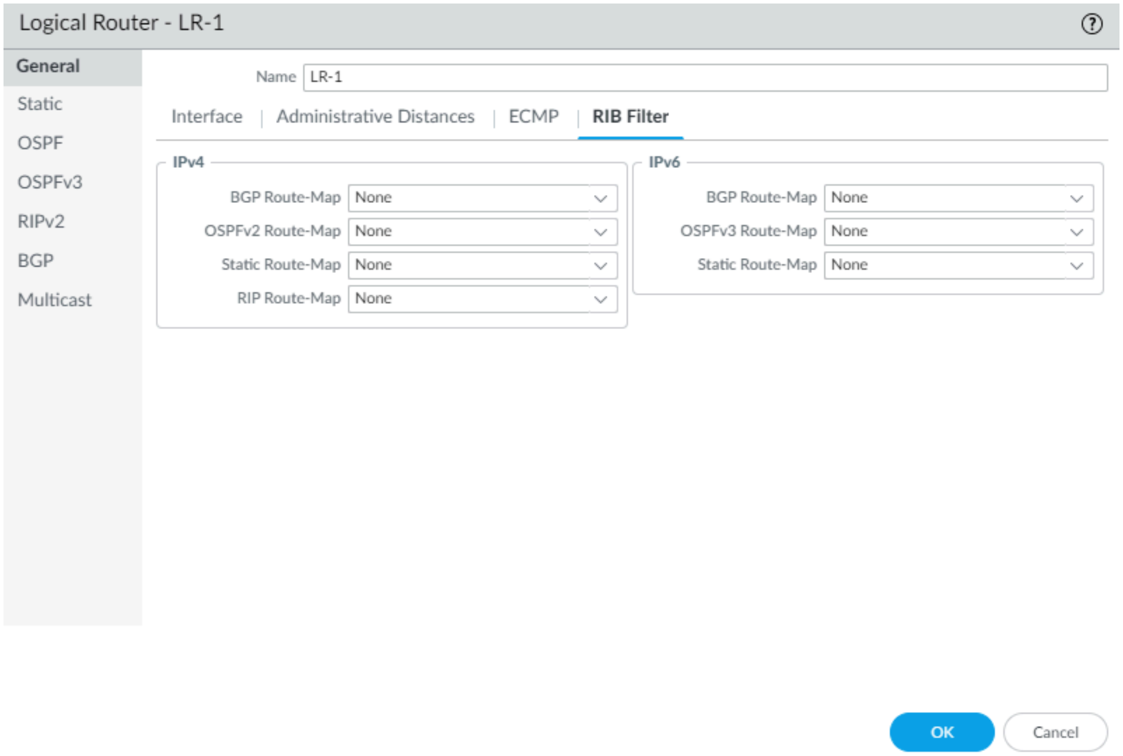
   대상 *IP* 주소는 신뢰할 수 있는 엔드포인트에 속해야 합니다**.** 자체 불안정하거나 신뢰할 수없는 디바이스에서 경로 모니터링을 기반으로해서는 안됩니다**.**

9. (선택 사항) ICMP **Ping** 간격**(**초**)**을 초 단위로 지정하여 방화벽이 경로를 모니터링하는 빈도를 결정합니다(범위는 1~60, 기본값은 3).
10. (선택 사항) 방화벽이 정적 경로 다운을 고려하고 RIB 및 FIB에서 제거하기 전에 대상에서 반환되지 않는 패킷의 ICMP **Ping** 카운트를 지정합니다(범위는 3~10, 기본값은 5).
11. 확인을 클릭하여 경로 모니터 대상을 저장합니다.
12. 확인을 두 번 클릭하여 정적 경로를 저장합니다.

STEP 4 | (선택 사항) 전역 RIB에 배치되는 정적 경로를 제어합니다.

정적 경로를 구성하고 재배포할 수 있지만 프로토콜의 로컬 경로 테이블 또는 전역 RIB에서는 원하지 않을 수 있습니다. 전역 RIB에 특정 정적 경로만 추가할 수 있습니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **RIB** 필터를 선택하여 루트가 전역 RIB에 추가되는 것을 허용하거나 루트가 추가되지 않도록 합니다.



3. IPv4 정적 경로 및 연결된 경로를 필터링하려면 정적 경로 지도에 대해 재배포 경로 지도를 선택하거나 새 경로 지도를 생성합니다.
4. IPv6 정적 경로 및 연결된 경로를 필터링하려면 정적 경로 지도에 대해 재배포 경로 지도를 선택하거나 새 경로 지도를 생성합니다.
5. 확인을 클릭합니다.

STEP 5 | (선택 사항) 정적 IPv4 및 정적 IPv6 경로의 기본 관리 거리를 논리적 라우터 내에서 변경합니다.

STEP 6 | 변경 사항을 커밋합니다.

STEP 7 | CLI에 액세스하여 **`show advanced-routing static-route-path-monitor`** 명령을 입력하여 정적 경로 모니터를 봅니다. PAN-OS CLI 빠른 시작은 CLI 치트 시트에 추가 명령을 나열합니다. 네트워킹.

고급 라우팅 엔진에서 BGP 구성

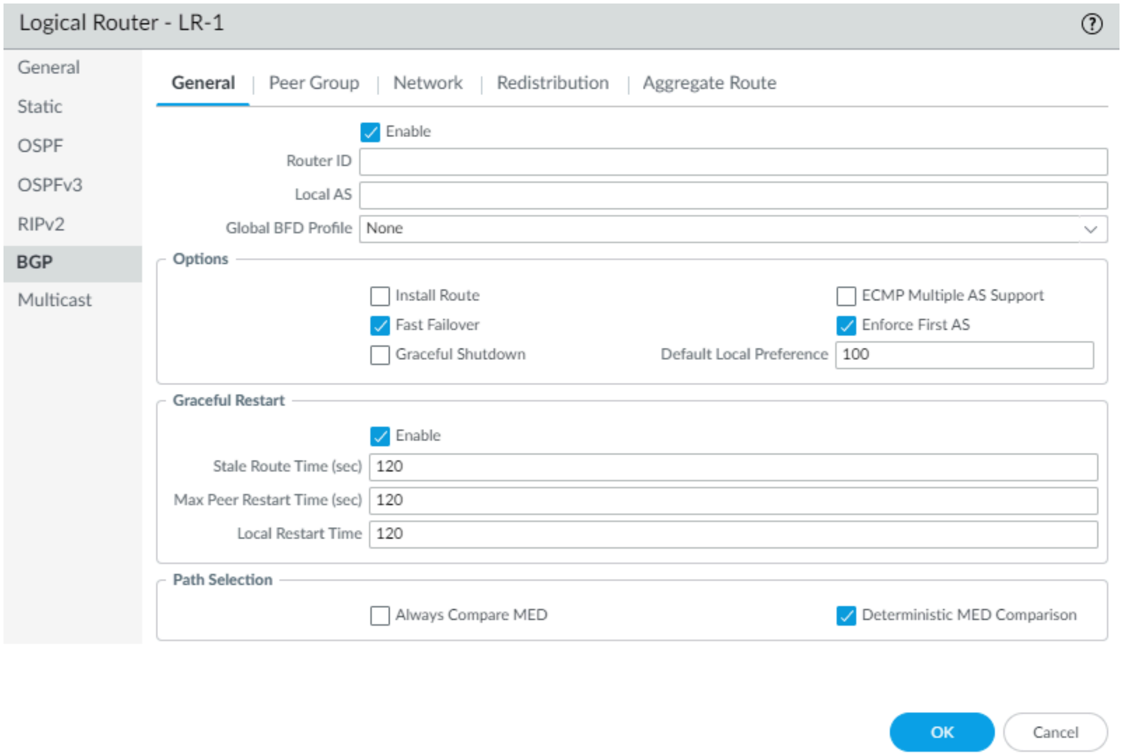
고급 라우팅 엔진에서 논리 라우터에 대한 BGP를 구성하려면 다음 작업을 수행합니다.

BGP를 구성하기 전에 BGP 피어 그룹, 피어, 재배포 규칙 및 집계 라우팅 정책에 적용할 수 있는 여러 가지 유용한 라우팅 프로파일 및 필터를 고려하여 구성 시간을 절약하고 일관성을 유지합니다. 프로파일과 필터를 미리 만들거나 BGP 구성을 진행하면서 만들 수 있습니다.

STEP 1 | 논리 라우터 구성.

STEP 2 | BGP를 활성화하고 일반 BGP 설정을 구성합니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. 이 논리 라우터에 대해 **BGP** > 일반 및 BGP 활성화를 선택합니다.



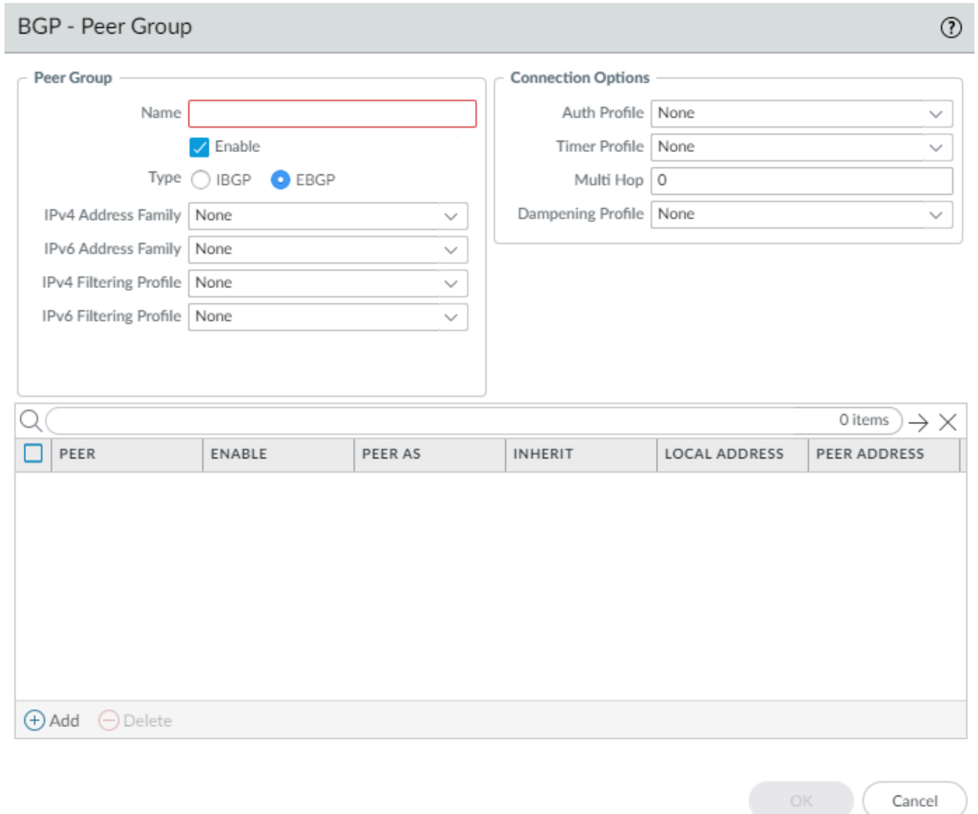
3. 라우터 **ID**가 고유한지 확인하기 위해 일반적으로 IPv4 주소인 논리 라우터의 BGP에 라우터 ID를 할당합니다.
4. 논리 라우터가 속한 AS의 번호인 로컬 **AS**를 할당합니다. 범위는 1~4,294,967,295입니다.
5. BFD를 BGP에 적용하려면 전역 **BFD** 프로파일에 대해 생성한 BFD 프로파일을 선택하거나 기본 프로파일을 선택하거나 새 BFD 프로파일을 만듭니다. 기본값은 없음**(BFD** 사용 안 함**)**입니다.
6. 학습된 BGP 경로를 전역 라우팅 테이블에 설치하려면 경로 설치를 선택합니다. 기본값은 비활성화되어 있습니다.
7. 빠른 장애 조치 를 선택하여 BGP가 해당 피어에 대한 링크가 다운될 경우 보류 시간이 만료될 때까지 기다리지 않고 해당 피어와의 세션을 종료하도록 합니다. 기본값은 활성화되어 있습니다.
8. 유지 관리 작업 중에 BGP가 eBGP 피어링 링크의 기본 설정을 낮추어 BGP가 RFC 8326을 기반으로 대체 경로를 선택하고 전달할 수 있도록 하려면 정상 종료를 선택합니다. 기본값은 비활성화되어 있습니다.
9. ECMP를 구성하고 여러 BGP 자율 시스템에서 ECMP를 실행하려는 경우 **ECMP** 다중 **AS** 지원을 선택합니다. 기본값은 비활성화되어 있습니다.
10. 방화벽이 eBGP 피어의 자체 AS 번호를 AS_PATH 속성의 첫 번째 AS 번호로 나열하지 않는 eBGP 피어에서 들어오는 업데이트 패킷을 삭제하도록 하려면 첫 번째 **AS**를 적용합니다. 기본값은 사용하도록 설정됩니다.

11. 여러 경로 간에 기본 설정을 결정하는 데 사용할 수 있는 기본 로컬 기본 설정을 지정합니다. 범위는 0~4,294,967,295이며 기본값은 100입니다.
12. 정상 재시작을 활성화하고 다음 타이머를 구성합니다.
    - 부실 라우트 시간**(**초**)** - 라우트가 부실 상태를 유지할 수 있는 시간(초)을 지정합니다(범위는 1 ~ 3,600, 기본값은 120).
    - 최대 피어 다시 시작 시간**(**초**)** - 로컬 디바이스가 피어 디바이스에 대한 유예 기간 다시 시작 시간으로 허용하는 최대 시간(초)을 지정합니다(범위는 1~3,600, 기본값은 120).
    - 로컬 다시 시작 시간 - 로컬 디바이스가 다시 시작되기를 기다리는 시간(초)을 지정합니다. 이 값은 피어에게 광고됩니다(범위는 1~3,600, 기본값은 120).
13. 경로 선택:
    - 항상 **MED** 비교 - 서로 다른 자율 시스템의 인접 경로를 선택하려면 이 비교를 활성화합니다. 기본값은 비활성화되어 있습니다.
    - 결정적 **MED** 비교 - IBGP 피어(동일한 자치 시스템의 BGP 피어)에 의해 광고되는 경로 중에서 선택하려면 이 비교를 활성화합니다. 기본값은 활성화됩니다.
14. 확인을 클릭합니다.

STEP 3 | BGP 피어 그룹을 구성합니다.

1. > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **BGP** > 피어 그룹을 선택하고 이름으로 BGP 피어 그룹을 추가합니다(최대 63자). 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 영숫자, 밑줄 또는 하이픈을 0개 이상 포함해야 합

니다. 점(.) 또는 공백은 사용할 수 없습니다. 이름은 논리 라우터 내에서 그리고 모든 논리적 라우터에서 고유해야 합니다.



3. 피어 그룹을 활성화합니다.
4. 피어 그룹 유형을 선택합니다. **IBGP** 또는 **EBGP**.
5. 피어 그룹에 대해 여러 **IPv4** 주소 패밀리 옵션을 지정하려면 생성한 **AFI** 프로파일을 선택하거나 기본 프로파일을 선택하거나 새 BGP 주소 패밀리 프로파일을 생성합니다. 기본값은 없음입니다.
6. 피어 그룹에 대해 여러 **IPv6** 주소 패밀리 옵션을 지정하려면 생성한 **AFI** 프로파일을 선택하거나 기본 프로파일을 선택하거나 새 BGP 주소 패밀리 프로파일을 만듭니다. 기본값은 없음입니다.
7. 피어 그룹에 **IPv4** 필터링 프로파일 옵션을 적용하려면 생성한 **BGP** 필터링 프로파일을 선택하거나 새 BGP 필터링 프로파일을 만듭니다. 기본값은 없음입니다.

   BGP 필터링 프로파일은 *BGP* 경로 가져오기 또는 내보내기, 로컬 *BGP RIB*에 추가되는 경로를 허용 또는 금지하고, 경로를 조건부로 광고하며, 댐핑되거나 요약된 경로의 기능 억제를 해제하는 등 *IPv4*에 대한 여러 *BGP* 옵션을 구성하는 방법을 설명합니다.

8. 피어 그룹에 **IPv6** 필터링 프로파일 옵션을 적용하려면 생성한 **BGP** 필터링 프로파일을 선택하거나 새 BGP 필터링 프로파일을 만듭니다. 기본값은 없음입니다.

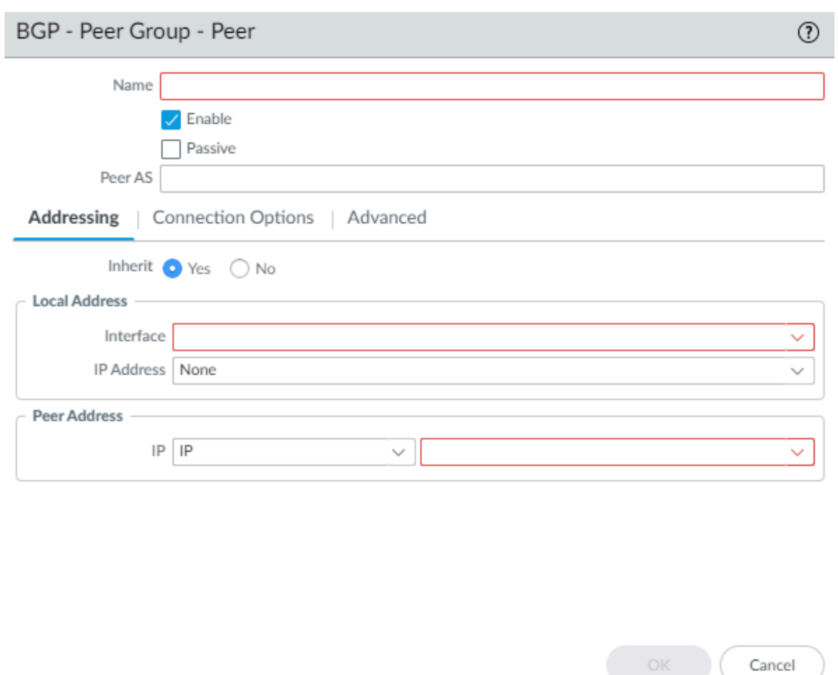
> BGP 필터링 프로파일은 *BGP* 경로 가져오기 또는 내보내기, 로컬 *BGP RIB*에 추가되는 경로를 허용 또는 금지하고, 경로를 조건부로 광고하고, 댐핑되거나 요약된 경로의 기능 억제 해제와 같은 *IPv6*에 대한 여러 *BGP* 옵션을 구성하는 방법을 설명합니다.

9. 연결 옵션에서 인증 프로파일을 선택하거나 새 BGP 인증 프로파일을 만들어 피어 그룹의 BGP 피어 간의 MD5 인증을 제어합니다. 기본값은 없음입니다.
10. 타이머 프로파일을 선택하거나 새 BGP 타이머 프로파일을 생성하여 keepalive에 영향을 주는 다양한 BGP 타이머를 제어하고 경로를 알리는 메시지를 업데이트합니다. 기본값은 없음입니다.
11. 멀티 홉 - IP 헤더의 TTL(지속 시간) 값을 설정합니다(범위는 0 - 255, 기본값은 0). 기본값 0은 eBGP의 경우 1을 의미합니다. 기본값 0은 iBGP의 경우 255를 의미합니다.
12. 댐핑 프로파일을 선택하거나 새 댐핑 프로파일을 작성하여 안정화될 때까지 플래ping 루트가 사용되지 않도록 페널티를 가하는 방법을 결정합니다. 기본값은 없음입니다.

STEP 4 | 피어 그룹에 BGP 피어를 추가합니다.

1. 이름으로 피어를 추가합니다(최대 63자). 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 영숫자, 밑줄 또는 하이픈을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 사용할 수 없습니다. 이름은 논리 라우터 내에서 그리고 모든 논리적 라우터에서 고유해야 합니다.
2. 피어를 활성화합니다. 기본값은 활성화되어 있습니다.
3. 피어가 이웃과의 세션을 시작하지 못하도록 하려면 수동을 선택합니다. 기본값은 비활성화되어 있습니다.
4. 피어가 속한 피어 **AS**를 입력합니다. 범위는 1에서 4,294,967,295까지입니다.
5. 주소 지정을 선택하고 피어가 IPv4 및 IPv6 AFI를 상속하고 피어 그룹에서 프로파일을 필터링할지 여부를 선택합니다. 예(기본값) 또는 아니요.
6. 예를 선택한 경우 피어에 대해 다음을 지정합니다.
   - 로컬 주소에서 BGP를 구성할 인터페이스를 선택합니다. 인터페이스에 둘 이상의 IP 주소가 있는 경우 해당 인터페이스의 **IP** 주소를 BGP 피어로 선택합니다.
   - 피어 주소에 대해 IP를 선택하고 **IP** 주소를 선택하거나 주소 개체를 만들거나 **FQDN**을 선택하고 FQDN 또는 FQDN 유형인 주소 개체를 입력합니다.

   방화벽은 FQDN의 DNS 확인에서 하나의 IP 주소(각 IPv4 또는 IPv6 주소 유형에서)만 사용합니다. DNS 확인이 둘 이상의 주소를 반환하는 경우 방화벽은 BGP 피어에 대해 구성된 IP 제품군 유형(IPv4 또는 IPv6)과 일치하는 기본 IP 주소를 사용합니다. 기본 IP 주소는 DNS 서버가 초기 응답에서 반환하는 첫 번째 주소입니다. 방화벽은 주소가 순서에 관계없이 후속 응답에 표시되는 한 이 주소를 선호하는 대로 유지합니다.

7. 피어 그룹에서 상속 주소 지정에 대해 아니요를 선택한 경우 피어에 대해 다음을 지정합니다.

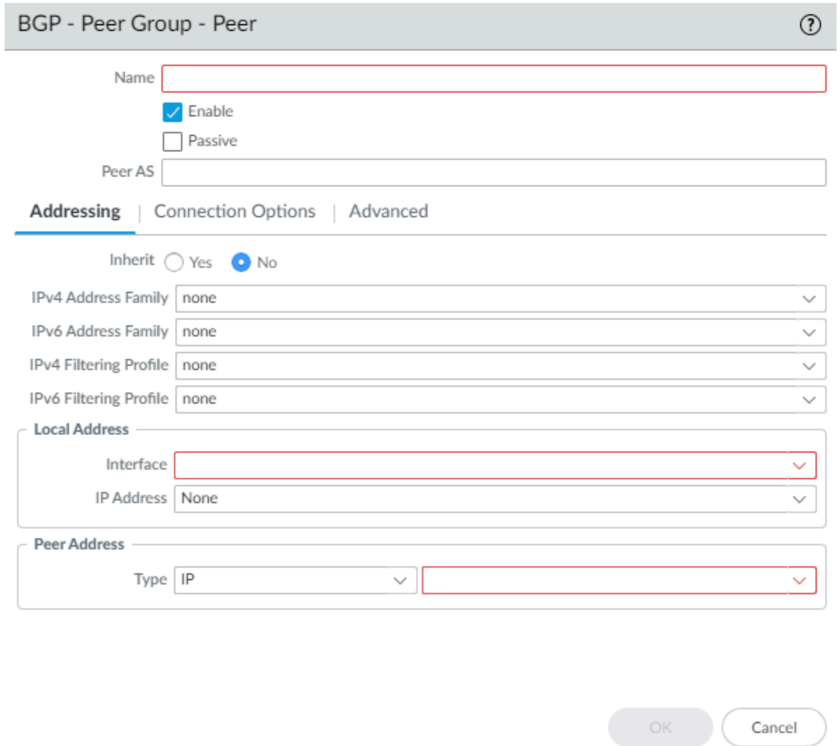
- 피어에 대해 여러 **IPv4** 주소 패밀리 옵션을 지정하려면 생성한 **AFI** 프로파일을 선택하고 기본 프로파일을 선택한 다음 상속**(**피어 그룹에서 상속**)**을 선택하거나 새 BGP 주소 패밀리 프로파일을 만듭니다.기본값은 없음**(IPv4 AFI** 사용 안 함**)** 입니다.

  > *AFI* 프로파일을 사용하면 피어가 경로 리플렉터 클라이언트임을 지정할 수 있습니다**.** 경로 리플렉터는 모든 피어의 모든 광고를 다른 모든 피어에 반영하므로 *iBGP*를 완전히 메시할 필요가 없습니다**.** 피어를 경로 리플렉터 클라이언트로 선언하면 *BGP* 프로세스는 해당 피어에 대한 모든 업데이트를 반영합니다**.**

- 피어에 대해 여러 **IPv6** 주소 패밀리 옵션을 지정하려면 생성한 **AFI** 프로파일을 선택하거나 상속**(**피어 그룹에서 상속**)**을 선택하거나 새 BGP 주소 패밀리 프로파일을 생성합니다. 기본값은 없음**(IPv6 AFI** 비활성화**)**입니다.

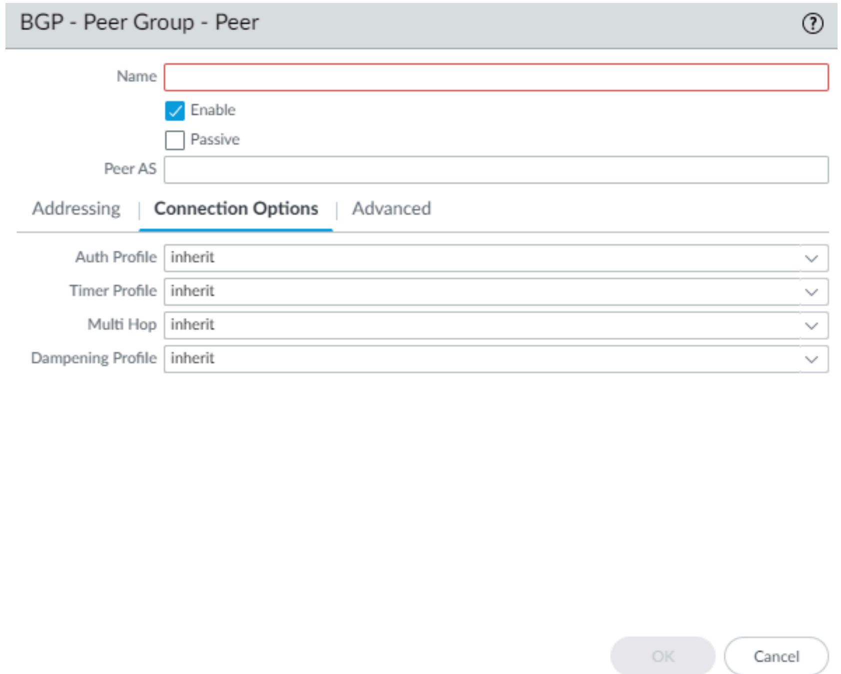
  > *AFI* 프로파일을 사용하면 피어가 경로 리플렉터 클라이언트임을 지정할 수 있습니다**.** 경로 리플렉터는 모든 피어의 모든 광고를 다른 모든 피어에 반영하므로 *iBGP*를 완전히 메시할 필요가 없습니다**.** 피어를 경로 리플렉터 클라이언트로 선언하면 *BGP* 프로세스는 해당 피어에 대한 모든 업데이트를 반영합니다**.**

- **IPv4** 필터링 프로파일 옵션을 피어에 적용하려면 생성한 **BGP** 필터링 프로파일을 선택하거나 상속**(**피어 그룹에서 상속**)**을 선택하거나 새 BGP 필터링 프로파일을 만듭니다. 기본값은 없음**(IPv4** 필터링 사용 안 함**)**입니다.
- **IPv6** 필터링 프로파일 옵션을 피어에 적용하려면 생성한 **BGP** 필터링 프로파일을 선택하거나 상속**(**피어 그룹에서 상속**)**을 선택하거나 새 BGP 필터링 프로파일을 만듭니다. 기본값은 없음**(IPv6** 필터링 사용 안 함**)**입니다.
- 로컬 주소에서 BGP를 구성할 인터페이스를 선택합니다. 인터페이스에 둘 이상의 IP 주소가 있는 경우 해당 인터페이스의 **IP** 주소를 BGP 피어로 선택합니다.
- 피어 주소에 대해 IP를 선택하고 **IP** 주소를 선택하거나 주소 개체를 만들거나 **FQDN**을 선택하고 FQDN 또는 FQDN 유형인 주소 개체를 입력합니다.

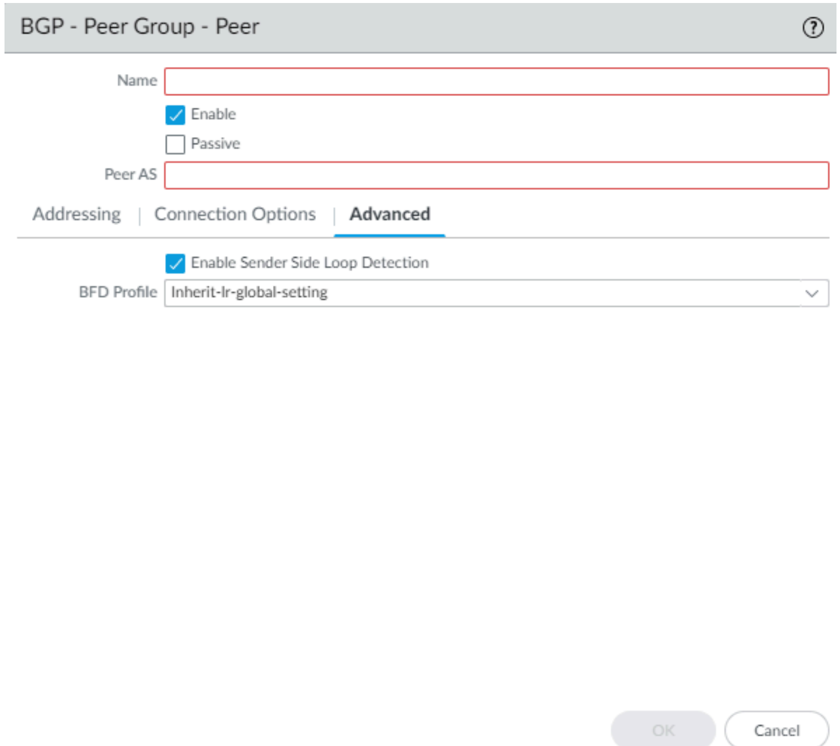


BGP 피어 그룹에 *IPv4* 주소 패밀리 프로파일과 *IPv6* 주소 패밀리 프로파일이 모두 적용된 경우 해당 피어 그룹에 속한 모든 피어는 자동으로 주소 지정이 상속 아니요로 설정됩니다(피어는 두 주소 패밀리를 모두 사용할 수 없으므로). 피어 그룹의 모든 피어에도 *IPv4* 주소 패밀리 프로파일, *IPv6* 주소 패밀리 프로파일, *IPv4* 필터링 프로파일 및 *IPv6* 필터링 프로파일이 기본적으로 없음으로 설정됩니다. 상속(피어 그룹에서 상속)을 선택하거나 피어에 대한 특정 프로파일을 선택하여 피어 그룹을 재정의할 수 있습니다. 예를 들어 *IPv4* 주소 패밀리 프로파일을 상속하고 *IPv4* 필터링 프로파일을 상속하도록 피어를 구성하고 *IPv6* 주소 패밀리 프로파일 및 *IPv6* 필터링 프로파일을 선택하여 피어 그룹에서 해당 프로파일을 재정의할 수 있습니다.

8. 피어 그룹의 설정과 다른 설정을 적용하려면 피어에 대한 연결 옵션을 선택합니다.



9. 인증 프로파일을 선택하거나 상속**(**피어 그룹에서 상속**)**(기본값)하거나 새 BGP 인증 프로파일을 생성하여 BGP 피어 간의 MD5 인증을 제어합니다.
10. 타이머 프로파일을 선택하거나, 상속**(**피어 그룹에서 상속**)**(기본값) 하거나, 새 BGP 타이머 프로파일을 만들거나, 기본 프로파일을 선택하여 keepalive에 영향을 주는 다양한 BGP 타이머를 제어하고 경로를 알리는 메시지를 업데이트합니다.
11. IP 헤더의 TTL(TTL) 값인 멀티 홉을 설정합니다(범위는 0~255). 기본 설정은 상속**(**피어 그룹에서 상속**)**입니다.
12. 댐핑 프로파일을 선택하거나, 상속**(**피어 그룹에서 상속**)**(기본값)하거나, 새 댐핑 프로파일을 생성하여 안정화될 때까지 플래ping 루트가 사용되지 않도록 페널티를 가하는 방법을 결정합니다.
13. 방화벽이 업데이트에서 경로를 보내기 전에 FIB에 있는 경로의 AS_PATH 특성을 확인하도록 하려면 고급 및 발신자 측 루프 검색 사용을 선택하여 피어 AS 번호가 AS_PATH 목록에 없는지 확인합니다. 그럴 경우 방화벽은 라우팅 루프를 방지하기 위해 AS 번호를 제거합니다.
14. **BFD** 프로파일을 피어에 적용하려면(논리적 라우터 수준에서 BGP에 대해 BFD가 비활성화되어 있지 않은 한 BGP에 대한 BFD 설정을 재정의함) 다음 중 하나를 선택합니다.
    - 기본 프로파일.
    - 기존 BFD 프로파일.
    - **Inherit-lr-global-setting (**프로토콜의 전역 **BFD** 프로파일 상속**)**(기본값) - 피어는 논리 라우터에 대해 BGP에 대해 전역적으로 선택한 BFD 프로파일을 상속합니다.
    - 피어에 대해 없음**(BFD** 사용 안 함**)**입니다.
    - 새 BFD 프로파일을 만듭니다.



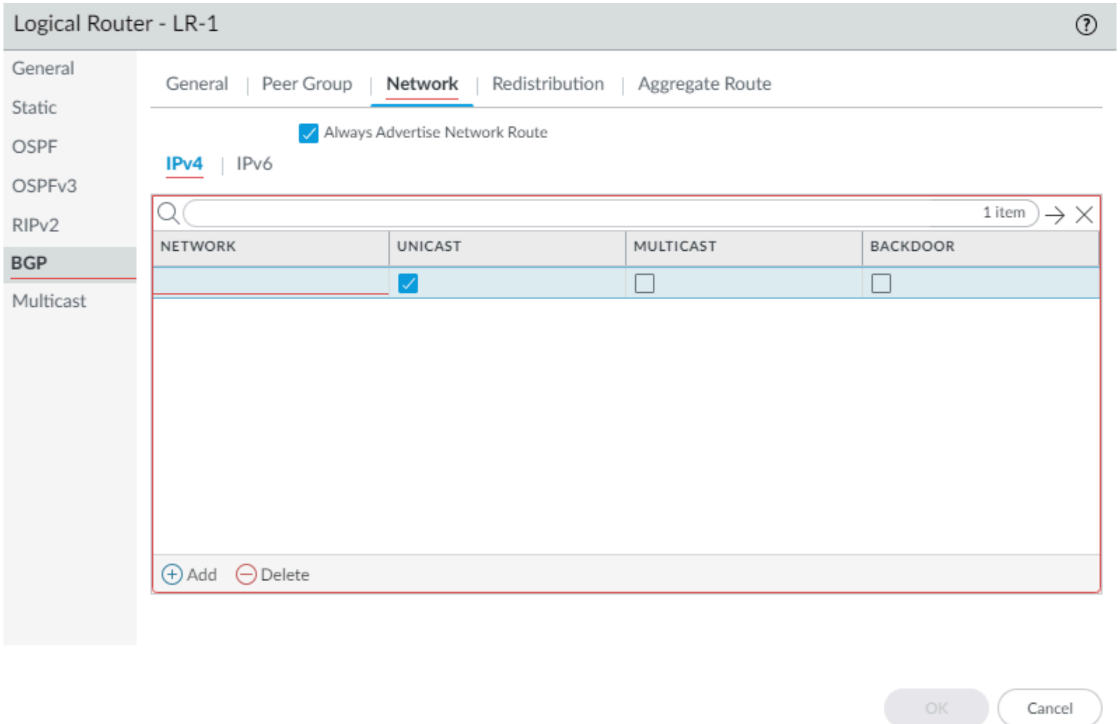
15. 확인을 클릭합니다.

STEP 5 | 인접 네트워크에 알릴 네트워크 접두사를 지정합니다.

> 네트워크 기능은 방화벽을 다른 서브넷으로 이동하거나 네트워크를 일시적으로 변경한 후에 특히 유용합니다.

1. 네트워크를 선택합니다.
2. 연결 가능 여부에 관계없이 구성된 네트워크 경로를 항상 BGP 피어에 광고하려면 항상 네트워크 경로 광고(기본값 사용)를 선택합니다. 이 옵션을 선택하지 않으면 방화벽은 로컬 라우팅 테이블을 사용하여 확인된 경우에만 네트워크 라우트를 알립니다.
3. **IPv4** 또는 **IPv6**을 선택하여 접두사 유형을 선택합니다.
4. 네트워크 접두사를 추가하여 이웃에게 알립니다.
5. 유니캐스트 주소 패밀리에 이 네트워크 경로를 알리려면 유니캐스트를 선택합니다. 기본값은 활성화되어 있습니다. 이 확인란을 선택하지 않으면 방화벽이 유니캐스트 SAFI의 경로를 알리지 않습니다.
6. (IPv4만 해당) 이 네트워크 경로를 멀티캐스트 주소 패밀리에 알리려면 멀티캐스트를 선택합니다. 기본값은 비활성화되어 있습니다. 방화벽은 멀티캐스트 SAFI에서 이 네트워크 경로를 알리지 않습니다.
7. (IPv4만 해당) BGP가 접두사를 AS 외부에 광고하지 못하도록 하고 대신 경로를 AS 내에 유지하려면 백도어를 선택합니다. 백도어는 IGP 경로보다 관리 거리가 높은 BGP 경로입니다. 내부적

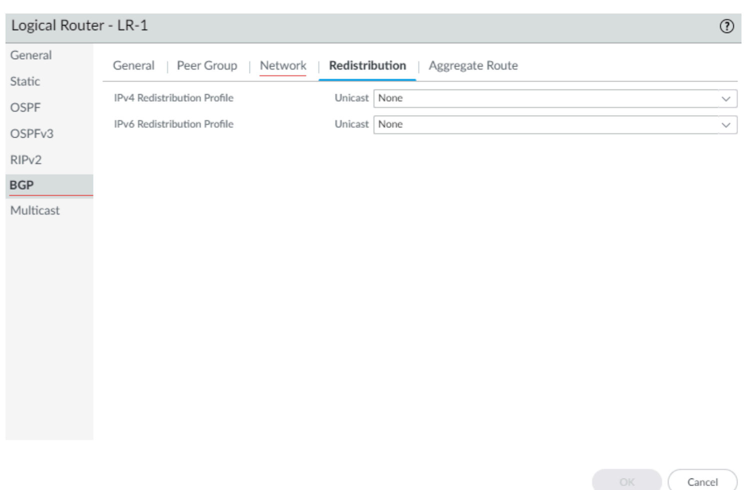
으로 접두사에 대한 관리 거리가 증가하여 접두사가 선호되지 않지만 다른 곳에서 링크가 실패하더라도 필요한 경우 계속 사용할 수 있습니다. 기본값은 비활성화입니다.



STEP 6 | 정적, 연결된 경로, OSPF, OSPFv3 또는 RIPv2 경로를 BGP로 재배포합니다.

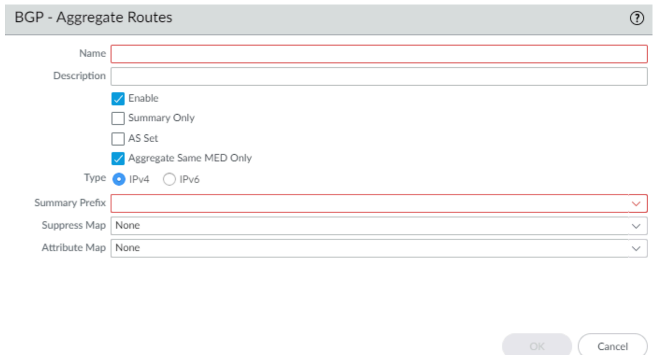
> *BGP* 재배포 프로파일 내에서 경로 맵의 유연성을 사용하여 재배포할 경로를 결정하는 조건을 지정하고 설정할 속성을 지정합니다**.**

1. 재배포를 선택합니다.
2. IPv4 경로를 재배포하려면 **IPv4** 재배포 프로파일 **-** 유니캐스트에 대해 BGP 재배포 프로파일을 선택하거나 새 재배포 프로파일을 만듭니다. 기본값은 없음입니다.
3. IPv6 경로를 재배포하려면 IPv6 재배포 프로파일 - 유니캐스트에 대해 BGP 재배포 프로파일을 선택하거나 새 재배포 프로파일을 만듭니다. 기본값은 없음입니다.



STEP 7 | BGP가 학습한 다음 피어에 알리는 경로를 요약하는 집계 경로 정책을 만듭니다.

1. 경로 집계를 선택하고 이름을 기준으로 집계 경로 정책을 추가합니다(최대 63자). 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 영숫자, 밑줄 및 하이픈을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
2. 정책에 대한 유용한 설명을 입력합니다.
3. 정책을 활성화합니다.



4. 요약 전용을 선택하여 요약된 경로가 아닌 요약 접두사만 이웃에게 광고합니다. 이를 통해 트래픽을 줄이고 이웃의 라우팅 테이블 크기를 불필요하게 늘리는 것을 방지합니다(기본값은 비활

성화됨). 집계 경로와 집계 경로를 구성하는 개별 경로를 모두 광고하려면 요약 전용을 선택하지 않은 상태로 둡니다.

요약 전용 및 맵 표시 안 함은 함께 사용할 수 없으며 둘 다 지정할 수 없습니다.

요약 전용을 사용하지만 개별 경로를 광고하려는 경우 개별 경로에서 일치하는 억제 해제 맵 경로 맵이 포함된 BGP 필터링 프로파일을 생성합니다.

5. 집합 경로를 구성하는 AS 번호 목록과 함께 접두사를 알리려면 **AS** 세트를 선택합니다. 기본값은 비활성화되어 있습니다.
6. 경로에 동일한 MED(다중 종료 판별자) 값이 있는 경우에만 경로 집계를 수행하려면 동일한 **MED**만 집계를 선택합니다. 기본값은 활성화되어 있습니다.
7. 집계 경로 유형을 선택합니다. **IPv4** 또는 **IPv6**입니다.
8. 요약할 경로를 계산한 다음 IP 주소/넷마스크 또는 주소 개체를 지정하여 해당 경로를 포괄하는 요약 접두사를 입력합니다.
9. 개별 경로가 집계되지 않도록 하려면(집계 표시 안 함) 맵 경로 맵 표시 안 함을 선택하거나 일치 조건이 해당 경로를 포함하는 IPv4 또는 IPv6 주소 액세스 목록 또는 접두사 목록을 지정하는 새 BGP 경로 맵을 생성합니다. 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.

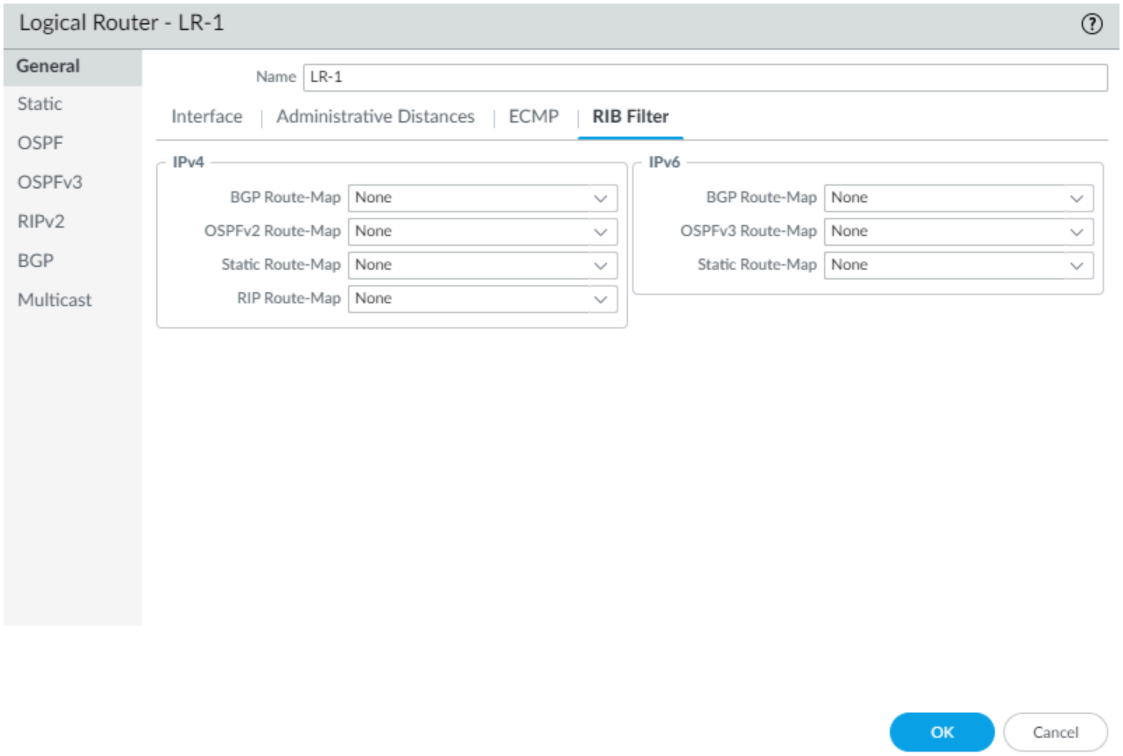
10. 요약 접두사(해당 경로 조합을 방금 만들었기 때문에 속성이 없음)에 대한 속성 정보를 설정하려면 속성 맵 경로 맵을 선택하거나 새 BGP 경로 맵을 만들고 요약 접두사(일치 조건 없음)의 속성을 설정합니다. 경로 맵이 없는 경우(없음) 요약 접두사는 기본 속성을 갖습니다. 기본값은 없음입니다.

STEP 8 | 확인을 클릭합니다.

STEP 9 | (선택 사항) 전역 RIB에 배치되는 BGP 경로를 제어합니다.

경로를 학습하고 재배포하지만 프로토콜의 로컬 라우팅 테이블이나 전역 RIB에서는 경로를 원하지 않을 수 있습니다. 전역 RIB에 특정 경로만 추가할 수 있습니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **RIB** 필터를 선택하여 루트가 전역 RIB에 추가되는 것을 허용하거나 루트가 추가되지 않도록 합니다.



3. IPv4 BGP 경로를 필터링하려면 IPv4 영역에서 **BGP** 경로 맵에 대해 재배포 경로 맵을 선택하거나 새 경로 맵을 생성합니다.
4. IPv6 BGP 경로를 필터링하려면 IPv6 영역에서 **BGP** 경로 맵에 대해 재배포 경로 맵을 선택하거나 새 경로 맵을 생성합니다.
5. 확인을 클릭합니다.

BGP 라우팅 프로파일 만들기

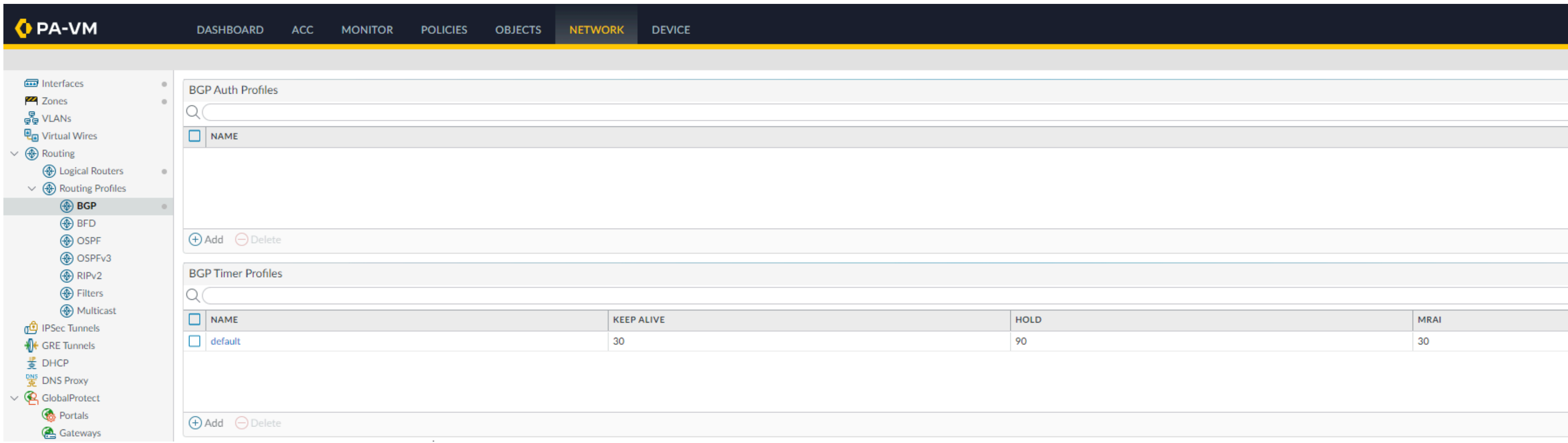
고급 라우팅 엔진에서 BGP에는 프로파일에서 쉽게 구성한 다음 BGP 피어 그룹 또는 피어 또는 재배포 규칙에 적용할 수 있는 다양한 설정이 있습니다. 프로파일을 재사용하여 여러 논리적 라우터 및 가상 시스템에 적용합니다. 동일한 유형의 여러 프로파일을 만들어 서로 다른 피어 그룹과 피어를 다르게 처리합니다. BGP 피어 그룹 및 피어는 전역 프로파일을 상속합니다. BGP 피어 그룹에 대한 프로파일을 만들어 전역 프로파일을 재정의하고 피어가 속한 피어 그룹의 프로파일을 재정의하는 BGP 피어에 대한 프로파일을 만들 수도 있습니다.

이 항목에서는 BGP 라우팅 프로파일과 이를 만드는 방법에 대해 설명합니다.

- **BGP** 인증 프로파일 - 협상 중에 BGP 피어 간에 서로 통신할 수 있는지 여부를 결정하는 데 사용되는 MD5 인증의 비밀 키를 지정합니다. BGP 피어 그룹 또는 피어 구성에서 프로파일을 참조합니다.
- **BGP** 타이머 프로파일 - keepalive에 영향을 주는 다양한 BGP 타이머를 제어하고 경로를 알리는 메시지를 업데이트합니다. BGP 피어 그룹 또는 피어 구성에서 프로파일을 참조합니다.
- **BGP** 주소 패밀리 프로파일 - BGP 자율 시스템이 두 가지 유형의 주소를 모두 사용할 때 IPv6 또는 IPv4의 동작을 결정합니다. BGP 피어 그룹 또는 피어 구성에서 프로파일을 참조합니다.
- **BGP** 댐핑 프로파일 - 플랩핑 경로를 불이익으로 만들어 안정화될 때까지 사용하지 못하도록 하는 방법을 결정합니다. BGP 피어 그룹 또는 피어 구성에서 프로파일을 참조합니다.
- **BGP** 재배포 프로파일 - 정적, 연결됨, OSPF, OSPFv3 또는 RIP 경로(할당된 경로 맵의 기준을 충족함)를 BGP에 재배포하고 경로 맵 세트 속성을 재분배된 경로에 적용합니다. 네트워크 > 라우팅 > 논리적 라우터 > **BGP** > 재분배에서 프로파일을 참조하십시오.
- **BGP** 필터링 프로파일 - 피어 그룹 또는 피어에 동시에 여러 필터를 적용하여 다음을 수행합니다.
  - 특정 AS 경로에서 오는 경로를 수락합니다(AS 경로 액세스 목록 기반).
  - 특정 AS 경로가 있는 경로를 알립니다(AS 경로 액세스 목록 기준).
  - 배포 목록 또는 접두사 목록(둘 다 동일한 필터링 프로파일에 있지 않음)을 기반으로 로컬 BGP RIB에 대한 경로를 수락합니다. 배포 목록은 접두사 범위를 가져오기 위해 와일드카드 마스크가 있는 원본 IP 주소를 기반으로 합니다. 접두사 목록은 네트워크 주소/접두사 길이를 기반으로 합니다.
  - 배포 목록 또는 접두사 목록(둘 다 동일한 필터링 프로파일에 있지 않음)을 기반으로 로컬 BGP RIB의 경로를 알립니다.
  - 경로 맵 속성 기준을 충족하는 경로를 로컬 BGP RIB에 수락하고 선택적으로 속성을 설정합니다.
  - 경로 맵 속성 기준을 충족하고 선택적으로 속성을 설정하는 경로를 알립니다.
  - 존재하는 경로를 조건부로 알립니다(존재하는 기준 충족).
  - 조건을 충족하는 경로 이외의 경로를 조건부로 광고합니다(존재하지 않는 기준 충족).
  - 댐핑 또는 요약 경로를 억제하지 마십시오.

STEP 1 | BGP 인증 프로파일을 만듭니다.

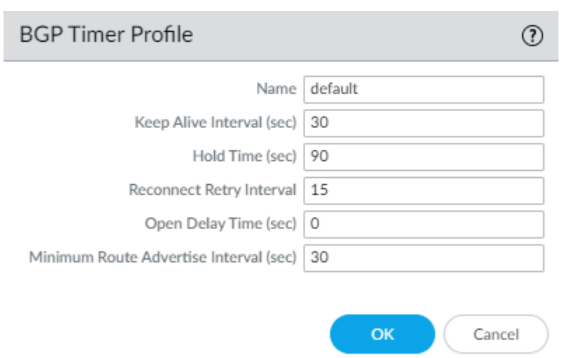
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **BGP**를 선택합니다.



2. 프로파일을 식별하기 위해 이름(최대 63자)으로 **BGP** 인증 프로파일을 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.
3. 암호 및 암호 확인을 입력합니다. 암호는 MD5 인증에서 키로 사용됩니다.
4. 확인을 클릭합니다.

STEP 2 | BGP 타이머 프로파일을 만듭니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **BGP**를 선택합니다.
2. BGP 타이머 프로파일 창에서 기본 BGP 타이머 프로파일을 선택하여 기본 프로파일 설정을 확인합니다.



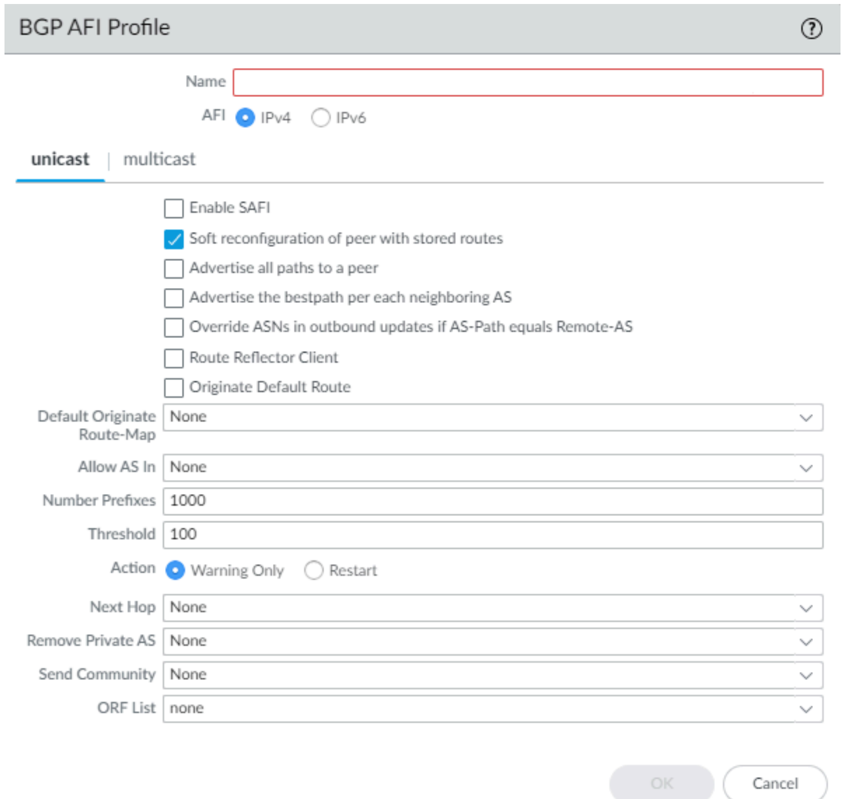
3. 기본 BGP 타이머 프로파일 설정이 필요한 설정이 아닌 경우 이름별 **BGP** 타이머 프로파일을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
4. 연결 유지 간격**(**초**)** 설정 - BGP 스피커가 연결 유지를 피어에게 보내는 간격(초)입니다(범위는 0~1,200, 기본값은 30). 보류 시간 간격 동안 피어로부터 Keepalive를 수신하지 않으면 BGP 피

어링이 닫힙니다. 종종 보류 시간은 BGP 피어링이 중단되기 전 3개의 누락된 Keepalive를 허용하기 위해 라이브 유지 간격의 세 배입니다.

5. 보류 시간**(**초**)** 설정—피어 연결이 종료되기 전에 피어의 연속 Keepalive 또는 Update 메시지 사이에 경과할 수 있는 시간(초)(범위는 3~3,600, 기본값은 90).
6. 다시 연결 다시 시도 간격 설정 - 피어에 연결을 다시 시도하기 전에 유휴 상태에서 대기하는 시간(초)입니다(범위는 1~3,600, 기본값은 15).
7. 열기 지연 시간**(**초**)** 설정 - 피어에 대한 TCP 연결을 열고 BGP 연결을 설정하기 위해 첫 번째 BGP 열기 메시지를 보내는 사이의 지연 시간(초)입니다(범위는 0 ~ 240, 기본값은 0).
8. 최소 경로 광고 간격**(**초**)** 설정 - BGP 스피커가 피어에 대한 특정 대상 경로의 광고 및/또는 철회 사이에 경과해야 하는 최소 시간(초)입니다(범위는 1~600, 기본값은 30).
9. 확인을 클릭합니다.

STEP 3 | MP-BGP을(를) 사용하려면 공유 속성의 BGP 주소 AFI(패밀리 식별자) 프로파일을 만듭니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **BGP**를 선택합니다.
2. 이름(최대 63자)으로 **BGP** 주소 계열 프로파일을 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.



3. **IPv4** 또는 **IPv6** AFI를 선택하여 프로파일 유형을 지정합니다.
4. 유니캐스트 또는 멀티캐스트를 선택합니다.

   멀티캐스트는 ***IPv4 AFI*** 프로파일에 대해서만 지원됩니다.

5. 프로파일에 대해 유니캐스트 SAFI를 활성화하려면 유니캐스트 탭에서 **SAFI** 활성화를 수행합니다. 프로파일에 대해 멀티캐스트 SAFI를 활성화하려면 멀티캐스트 탭에서 **SAFI** 활성화를 수행

합니다. **SAFI** 활성화가 유니캐스트 및 멀티캐스트 모두에 선택되어 있으면 두 SAFI가 모두 활성화됩니다. BGP 프로파일이 유효하려면 하나 이상의 SAFI를 사용하도록 설정해야 합니다.

6. 저장된 경로가 있는 피어의 소프트 재구성을 선택하여 BGP 피어의 설정이 업데이트된 후 방화벽이 자체의 소프트 재설정을 수행하도록 합니다. (기본적으로 활성화되어 있습니다.)
7. 모든 경로를 피어에 알림 - BGP가 네트워크 내에서 다중 경로 기능을 유지하기 위해 이웃에 대한 알려진 모든 경로를 알리도록 합니다.
8. 각 인접 **AS**에 대한 최적 경로를 알려 BGP가 네트워크 내에서 다중 경로 기능을 보존하기 위해 인접에 대해 가장 잘 알려진 경로를 광고하도록 합니다. 모든 자율 시스템에 동일한 경로를 알리려면 이 옵션을 비활성화합니다.
9. **AS-Path**가 **Remote-AS**와 같은 경우 아웃바운드 업데이트의 **ASN** 재정의 - 이 설정은 동일한 AS 번호(예: AS 64512)에 속하는 여러 사이트가 있고 그 사이에 다른 AS가 있는 경우에 유용합니다. 두 사이트 사이의 라우터는 AS 64512에 액세스할 수 있는 경로를 알리는 업데이트를 수신합니다. 두 번째 사이트가 AS 64512에도 있기 때문에 업데이트를 삭제하지 않도록 하기 위해 중간 라우터는 AS 64522를 자체 ASN(예: ASN)으로 대체합니다.
10. BGP 피어를 IBGP 네트워크의 경로 리플렉터 클라이언트로 만들려면 경로 리플렉터 클라이언트를 활성화합니다.
11. 기본 경로 시작 - 기본 경로를 생성하고 로컬 BGP RIB에 배치하려면 선택합니다.
12. 기본 원래 경로 맵 - 기본 경로의 속성을 제어하기 위해 경로 맵을 선택하거나 생성합니다.
13. **AS**로 허용:
    - 원점 - 방화벽의 자체 AS가 AS_PATH에 있는 경우에도 경로를 수락합니다.
    - 발생 - 방화벽의 자체 AS가 AS_PATH에 있을 수 있는 횟수입니다.
    - 없음 - (기본 설정) 아무 조치도 취하지 않습니다.
14. 숫자 접두사 - 피어에서 수락(학습)할 접두사의 최대 수입니다. 범위는 1~4,294,967,295이며, 기본값은 1,000입니다.
15. 임계값 - 최대 접두사 수의 백분율입니다. 접두사가 BGP 로컬 RIB에 추가됩니다. 피어가 임계값보다 많이 보급되면 방화벽은 지정된 작업(경고만 또는 다시 시작)을 수행합니다. 범위는 1~100이고 기본값은 100입니다.
16. 작업 - 시스템 로그의 경고만 메시지 또는 최대 접두사 수를 초과한 후 BGP 피어 연결을 다시 시작합니다.
17. 다음 홉을 선택합니다.
    - 자체 - 방화벽이 다음 홉 주소(수신하는 업데이트에서)를 보내기 전에 업데이트에서 자체 IP 주소로 변경하도록 합니다. 이는 방화벽이 EBGP 라우터(다른 AS) 및 IBGP 라우터(자체 AS)와 통신할 때 유용합니다. 예를 들어 AS 64512에 도착하는 BGP 업데이트의 다음 홉 주소가 업데이트가 AS 64518을 송신한 라우터 2의 송신 인터페이스의 IP 주소라고 가정합니다. 업데이트는 라우터 2가 광고하는 네트워크에 연결하려면 라우터 2의 다음 홉 주소를 사용함을 나타냅니다. 그러나 방화벽이 AS 64512의 iBGP 인접 라우터에 해당 업데이트를 보내는 경우 라우터 2의 변경되지 않은 다음 홉은 AS 64512 외부에 있으며 iBGP 인접 라우터에는 해당 업데이트에 대한 경로가 없습니다. 자체를 선택하면 방화벽이 다음 홉을 자체 IP 주소로 변경하여 iBGP 인접 라우터가 해당 다음 홉을 사용하여 방화벽에 연결할 수 있도록 합니다.
    - 자체 적용 - 포스는 반사된 경로에 대해 다음 홉을 self로 설정합니다.

- 없음 - (기본 설정) 원래 다음 홉을 속성에 유지합니다.

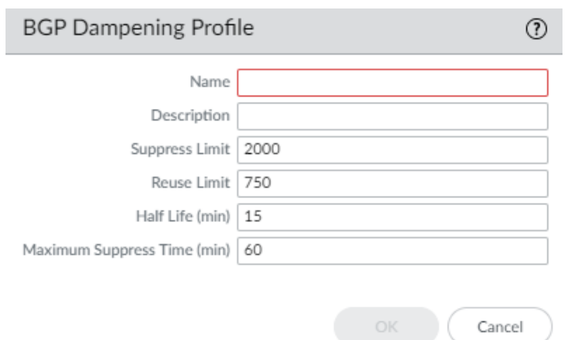
18. 방화벽이 다른 AS의 피어에 보내는 업데이트의 AS_PATH 속성에서 BGP가 비공개 AS 번호를 제거하도록 하려면 개인 **AS** 제거에서 다음 중 하나를 선택합니다.
    - 모두 - 모든 개인 AS 번호를 제거합니다.
    - **AS** 교체 - 모든 개인 AS 번호를 방화벽의 AS 번호로 교체합니다.
    - 없음 - (기본 설정) 아무 조치도 취하지 않습니다.
19. 커뮤니티 보내기에서 아웃바운드 업데이트 패킷으로 보낼 BGP 커뮤니티 속성 유형을 선택합니다.
    - 모두 - 모든 커뮤니티를 보냅니다.
    - 둘 다 - 표준 및 확장 커뮤니티를 보냅니다.
    - 확장됨 - 확장된 커뮤니티를 보냅니다(RFC 4360).
    - 대규모 - 대규모 커뮤니티(RFC 8092)를 보냅니다.
    - 표준 - 표준 커뮤니티(RFC 1997)를 보냅니다.
    - 없음 - (기본 설정) 커뮤니티를 보내지 않습니다.
20. **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. ORF 기능 설정을 선택합니다.
    - 없음 - (기본 설정) 피어 그룹 또는 피어(이 AFI 프로파일이 적용된 경우)에는 ORF 기능이 없습니다.
    - 둘 다 - 피어 그룹 또는 피어(이 AFI 프로파일이 적용되는 경우)가 접두사 목록을 보내고 접두사 목록을 수신하여 ORF를 구현할 수 있음을 알립니다.
    - 수신 - 피어 그룹 또는 피어(이 AFI 프로파일이 적용되는 위치)가 ORF를 구현하기 위한 접두사 목록을 수신할 수 있다고 알립니다. 로컬 피어는 원격 피어의 ORF 기능과 접두사 목록을 수신하며 이를 아웃바운드 경로 필터로 구현합니다.
    - 전송 - 피어 그룹 또는 피어(이 AFI 프로파일이 적용되는 위치)가 ORF를 구현하기 위해 접두사 목록을 보낼 수 있다고 알립니다. 원격 피어(수신 기능 포함)는 ORF 기능을 수신하고 발신자에게 경로를 알릴 때 수신한 접두사 목록을 아웃바운드 경로 필터로 구현합니다.

    ORF는 두 가지 잠재적인 문제에 대한 해결책입니다. a) 원치 않는 경로를 광고하여 대역폭을 낭비하고 b) 수신 피어가 원하는 경로 접두사를 필터링합니다. 다음을 수행하여 ORF를 구현합니다.

    1. 주소 패밀리 프로파일에서 ORF 기능을 지정합니다.
    2. 보낸 사람인 피어 그룹 또는 피어(보내기 또는 둘 다 기능)의 경우 피어 그룹/피어가 수신하려는 접두사 집합을 포함하는 접두사 목록을 만듭니다.
    3. BGP 필터링 프로파일을 만들고 인바운드 접두사 목록에서 만든 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 있으면 됩니다.
21. 확인을 클릭합니다.

STEP 4 | BGP 댐핑 프로파일을 생성합니다.

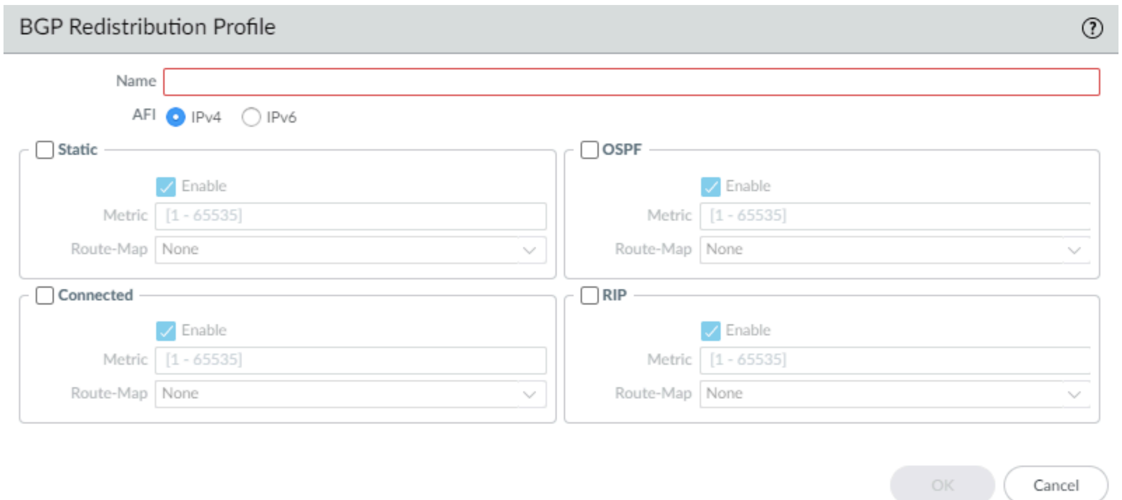
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **BGP**를 선택합니다.
2. 이름으로 **BGP** 감쇠 프로파일을 추가합니다. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 유용한 설명을 입력합니다.
4. 제한 억제 - 억제 값(플래핑에 대한 패널티의 누적 값)을 입력합니다. 이 지점에서 피어에서 오는 모든 경로가 댐핑됩니다. 범위는 1~20,000입니다. 기본값은 2,000입니다.
5. 재사용 제한 - 반감기에 대해 설명된 절차에 따라 경로를 재사용할 수 있는 시기를 제어하는 값을 입력합니다. 범위는 1~20,000이고 기본값은 750입니다.
6. 반감기**(**분**)** - 플랩 경로에 적용되는 안정성 메트릭(페널티)을 제어하기 위한 반감기 시간의 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.
7. 최대 억제 시간**(**최소**)** - 경로가 얼마나 불안정했는지에 관계없이 억제할 수 있는 최대 시간(분)을 입력합니다. 범위는 1~255입니다. 기본값은 60입니다.



8. 확인을 클릭합니다.

STEP 5 | BGP 재배포 프로파일을 만들어 정적, 연결된 경로 및 OSPF 경로(해당 경로 맵과 일치)를 BGP에 재배포합니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **BGP**를 선택합니다.
2. 이름(최대 63자)으로 **BGP** 재배포 프로파일을 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.
3. 재배포할 경로의 **AFI**를 선택합니다. **IPv4** 또는 **IPv6**입니다.

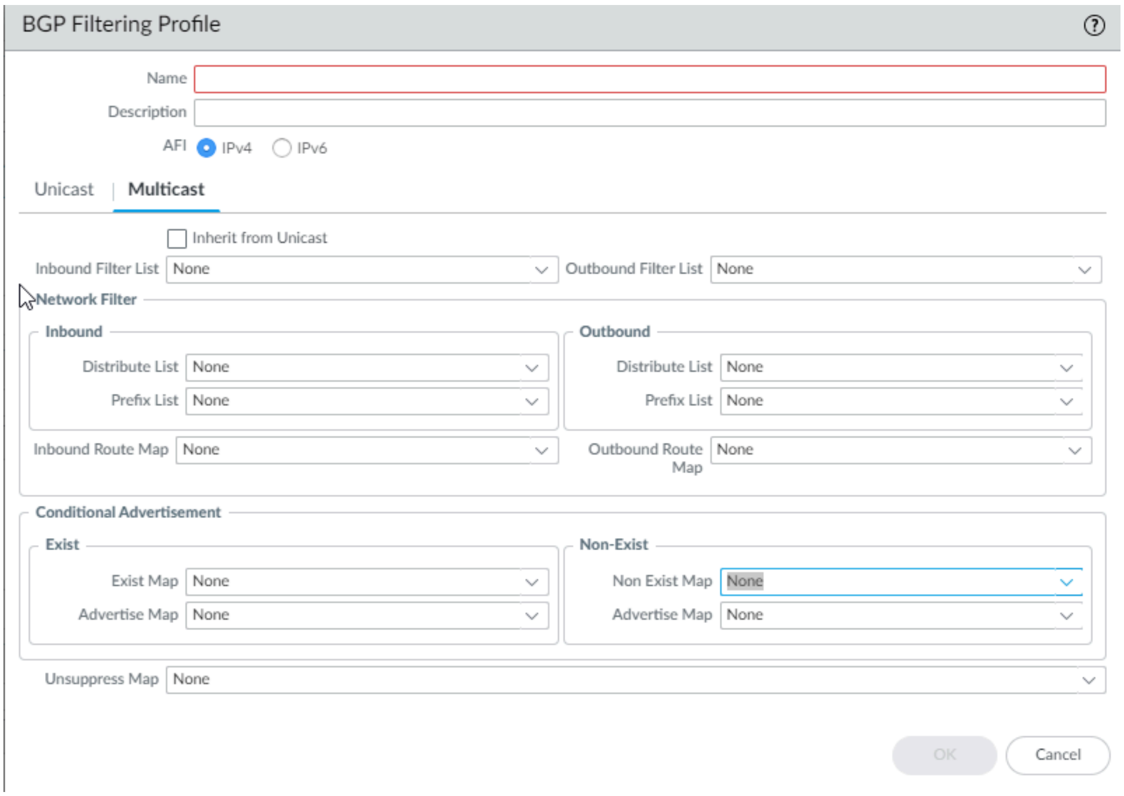


4. 정적을 선택하여 정적 경로 재분배를 구성합니다.
5. IPv4 또는 IPv6 고정 경로의 재배포를 활성화합니다(선택한 AFI 기반).
6. BGP로 재배포되는 고정 경로에 적용하도록 메트릭을 구성합니다(범위는 1~65,535).
7. 경로 맵을 선택하여 재배포할 정적 경로를 결정하는 일치 기준을 지정합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
8. 연결됨을 선택하여 연결된 경로 재배포를 구성합니다.
9. 로컬로 연결된 IPv4 또는 IPv6 경로의 재배포를 사용하도록 설정합니다(선택한 AFI에 따라).
10. BGP로 재분배되는 연결된 경로에 적용하도록 메트릭을 구성합니다 (범위는1 - 65,535).
11. 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.
12. (IPv4 AFI에만 해당) OSPFv2를 선택하여 **OSPFv2** 경로 재배포를 구성합니다.
13. OSPFv2 경로의 재배포를 사용하도록 설정합니다.
14. BGP로 재분배되는 OSPF 경로에 적용하도록 메트릭을 구성합니다(범위는 1 - 65,535).
15. 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.
16. (IPv4 AFI에만 해당) RIPv2를 선택하여 **RIPv2** 경로 재배포를 구성합니다.
17. RIPv2 경로의 재배포를 사용하도록 설정합니다.

18. BGP로 재분배되는 RIP 경로에 적용하도록 메트릭을 구성합니다(범위는 1 - 65,535).
19. 경로 맵을 선택하여 재분배할 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.
20. (IPv6 AFI에만 해당) OSPFv3을 선택하여 **OSPFv3** 경로 재배포를 구성합니다.
21. OSPFv3 경로의 재배포를 사용하도록 설정합니다.
22. BGP로 재분배되는 OSPFv3 경로(범위는 1 - 65,535)에 적용되도록 메트릭을 구성합니다 .
23. 경로 맵을 선택하여 재배포할 OSPFv3 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.
24. 확인을 클릭합니다.

STEP 6 | BGP 필터링 프로파일을 만듭니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **BGP**를 선택합니다.
2. 이름으로 **BGP** 필터링 프로파일을 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.
3. 유용한 설명을 입력합니다.
4. 필터링할 경로 유형을 나타내려면 **IPv4** 또는 **IPv6** AFI(Address Family Identifier)를 선택합니다.



5. 유니캐스트 또는 멀티캐스트 후속 주소 패밀리 식별자(SAFI)를 선택합니다.
6. 유니캐스트의 경우, 인바운드 필터 목록 - AS 경로 액세스 목록을 선택하거나 새 AS 경로 액세스 목록을 생성하여 피어로부터 경로를 수신할 때 동일한 AS 경로를 가진 경로는 피어 그룹 또는 피어에서 가져오므로 로컬 BGP RIB에 추가됩니다.
7. 네트워크 필터 영역에서 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.
8. 접두사 목록 - 접두사 목록을 사용하여 네트워크 접두사를 기반으로 BGP가 수신하는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 인바운드 배포 목록과 상호 배타적입니다.
9. 인바운드 경로 맵 - 경로 맵을 사용하여 로컬 BGP RIB(조건 일치)에 허용되는 경로를 훨씬 더 세부적으로 제어하고 경로에 대한 속성을 설정합니다(옵션 설정). 예를 들어 경로의 AS 경로 앞에 AS를 추가하여 경로 기본 설정을 제어할 수 있습니다.

인바운드 경로 맵이 인바운드 배포 목록 또는 접두사 목록으로 구성된 경우 경로 맵과 목록의 조건이 모두 충족되어야 합니다(논리적 *AND).*

10. 아웃바운드 필터 목록 - AS 경로 액세스 목록을 선택하거나 새 AS 경로 액세스 목록을 만들어 동일한 AS 경로를 가진 경로만 피어 라우터(이 필터가 적용되는 피어 그룹 또는 피어)에 보급되도록 지정합니다.
11. 아웃바운드 - 배포 목록 - 액세스 목록을 사용하여 대상의 IP 주소를 기반으로 BGP가 보급하는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 아웃바운드 접두사 목록과 상호 배타적입니다.
12. 접두사 목록 - 접두사 목록을 사용하여 네트워크 접두사를 기반으로 BGP가 알리는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 아웃바운드 배포 목록과 상호 배타적입니다.
13. 아웃바운드 경로 맵 - 경로 맵을 사용하여 BGP가 광고하는 경로(일치 기준)를 훨씬 더 잘 제어하고 보급된 경로의 속성을 설정할 수 있습니다.

    아웃바운드 경로 맵이 아웃바운드 배포 목록 또는 접두사 목록으로 구성된 경우 경로 맵과 목록의 조건이 모두 충족되어야 합니다*(논리적 **AND**)*.

14. 다른 경로가 존재하거나 로컬 BGP RIB에 존재하지 않는 경우 광고할 경로를 제어할 수 있는 조건부 광고를 구성합니다. 로컬 BGP RIB에 없는 경로는 피어링 또는 연결 가능성 실패를 나타낼 수 있습니다. 조건부 광고는 여러 ISP를 통해 인터넷에 대한 링크가 있고 기본 공급자에 대한 연결이 끊어진 경우를 제외하고 트래픽을 다른 공급자가 아닌 한 공급자로 라우팅하려는 경우와 같이 한 AS로 경로를 다른 AS로 강제 적용하려는 경우에 유용합니다. 조건부 광고 존재 영역에서:
    - 존재 맵 필드에서 경로 맵을 선택하거나 생성하여 조건부 광고에 대한 일치 기준을 지정합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.

- 맵 광고 - 조건이 충족될 경우(존재 맵의 경로가 로컬 BGP RIB에 있음) 광고할 경로를 지정하려면 경로 맵을 선택하거나 생성합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.

15. 조건부 광고 존재하지 않는 영역에서:

    - 존재하지 않는 맵 필드에서 경로 맵을 선택하거나 생성하여 조건부로 알리기 위해 로컬 BGP RIB에 존재하지 않는 경로에 대한 일치 기준을 지정합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.
    - 맵 광고 - 경로 맵을 선택하거나 생성하여 존재하지 않는 맵의 경로가 로컬 BGP RIB에 없을 때 알릴 경로를 지정합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.

16. 맵 억제 해제 - 억제를 해제하려는 경로의 경로 맵을 선택하거나 만듭니다(요약되어 억제되지 않음) 억제되었거나 감쇠 기준을 충족하기 때문에 억제되었지만 특정 경로를 보급(억제되지 않음)하려는 경로입니다.
17. (IPv4 AFI에만 해당) 멀티캐스트를 선택하여 MP-BGP 멀티캐스트 경로를 필터링합니다. 유니캐스트 SAFI의 모든 필터링을 멀티캐스트 SAFI에도 적용하려면 유니캐스트에서 상속을 선택합니다. 그렇지 않으면 다음 필터링 필드를 계속 구성합니다.
18. 멀티캐스트, 인바운드 필터 목록 - AS 경로 액세스 목록을 지정하거나 새 AS 경로 액세스 목록을 생성하여 피어로부터 경로를 수신할 때만 동일한 AS 경로를 가진 경로는 피어 그룹 또는 피어에서 가져오므로 로컬 BGP RIB에 추가됩니다.
19. 네트워크 필터 영역에서 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.
20. 접두사 목록 - 접두사 목록을 사용하여 네트워크 접두사를 기반으로 BGP가 수신하는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 인바운드 배포 목록과 상호 배타적입니다.
21. 인바운드 경로 맵 - 경로 맵을 사용하여 로컬 BGP RIB(조건 일치)에 허용되는 경로를 훨씬 더 세부적으로 제어하고 경로에 대한 속성을 설정합니다(옵션 설정). 예를 들어 경로의 AS 경로 앞에 AS를 추가하여 경로 기본 설정을 제어할 수 있습니다.

    인바운드 경로 맵이 인바운드 배포 목록 또는 접두사 목록으로 구성된 경우 경로 맵과 목록의 조건이 모두 충족되어야 합니다*(*논리적 *AND).*

22. 아웃바운드 필터 목록 - AS 경로 액세스 목록을 선택하거나 새 AS 경로 액세스 목록을 만들어 동일한 AS 경로를 가진 경로만 피어 라우터(이 필터가 적용되는 피어 그룹 또는 피어)에 보급되도록 지정합니다.
23. 아웃바운드 - 배포 목록 - 액세스 목록을 사용하여 대상의 IP 주소를 기반으로 BGP가 보급하는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 아웃바운드 접두사 목록과 상호 배타적입니다.
24. 접두사 목록 - 접두사 목록을 사용하여 네트워크 접두사를 기반으로 BGP가 알리는 BGP 라우팅 정보를 필터링합니다. 단일 필터링 프로파일의 아웃바운드 배포 목록과 상호 배타적입니다.
25. 아웃바운드 경로 맵 - 경로 맵을 사용하여 BGP가 광고하는 경로(일치 기준)를 훨씬 더 잘 제어하고 보급된 경로의 속성을 설정할 수 있습니다.

    아웃바운드 경로 맵이 아웃바운드 배포 목록 또는 접두사 목록으로 구성된 경우 경로 맵과 목록의 조건이 모두 충족되어야 합니다*(*논리적 *AND).*

26. 다른 경로가 존재하거나 로컬 BGP RIB에 존재하지 않는 경우 광고할 경로를 제어할 수 있는 조건부 광고를 구성합니다. 로컬 BGP RIB에 없는 경로는 피어링 또는 연결 가능성 실패를 나타낼 수 있습니다. 조건부 광고는 여러 ISP를 통해 인터넷에 대한 링크가 있고 기본 공급자에 대한 연결이 끊어진 경우를 제외하고 트래픽을 다른 공급자가 아닌 한 공급자로 라우팅하려는 경우와 같이 한 AS로 경로를 다른 AS로 강제 적용하려는 경우에 유용합니다. 조건부 광고 존재 영역에서:
    - 존재 맵 필드에서 경로 맵을 선택하거나 생성하여 조건부 광고에 대한 일치 기준을 지정합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.
    - 맵 광고 - 조건이 충족될 경우(존재 맵의 경로가 로컬 BGP RIB에 있음) 광고할 경로를 지정하려면 경로 맵을 선택하거나 생성합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.
27. 조건부 광고 존재하지 않는 영역에서:
    - 존재하지 않는 맵 필드에서 경로 맵을 선택하거나 생성하여 조건부로 알리기 위해 로컬 BGP RIB에 존재하지 않는 경로에 대한 일치 기준을 지정합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.
    - 맵 광고 - 경로 맵을 선택하거나 생성하여 존재하지 않는 맵의 경로가 로컬 BGP RIB에 없을 때 알릴 경로를 지정합니다. 이 필드에서 경로 맵의 일치 부분만 고려됩니다. 설정 부분은 무시됩니다.
28. 맵 억제 해제 - 억제를 해제하려는 경로의 경로 맵을 선택하거나 만듭니다(요약되어 억제되지 않음) 억제되었거나 감쇠 기준을 충족하기 때문에 억제되었지만 특정 경로를 보급(억제되지 않음)하려는 경로입니다.
29. 확인을 클릭합니다.

고급 라우팅 엔진에 대한 필터 만들기

고급 라우팅 엔진은 이 항목에 설명된 필터를 지원합니다. 액세스 목록, 접두사 목록 및 재배포 경로 맵은 BGP, OSPFv2, OSPFv3 및 RIPv2에 적용할 수 있습니다. 액세스 목록 및 접두사 목록은 IPv4 멀티캐스트에도 적용할 수 있습니다. 멀티캐스트 경로 맵은 IPv4 멀티캐스트에 적용됩니다. AS 경로 액세스 목록, 커뮤니티 목록 및 BGP 경로 맵은 BGP에만 적용됩니다.

필터를 만들고 프로파일 또는 기타 적절한 위치에서 필터를 참조하여 피어에서 로컬 RIB로 경로 수락, 피어로 광고 라우팅, 조건부 알림, 속성 설정, 다른 라우터와의 경로 내보내기 및 가져오기, 경로 집계 및 경로 재배포 등을 제어하는 설정을 쉽고 일관되게 적용할 수 있습니다.

- 액세스 목록 - 액세스 목록 사용:
  - IPv4/IPv6 원본 주소 및 IPv4 대상 주소를 기반으로 네트워크 경로를 필터링합니다. IPv4 액세스 목록의 경우 주소 및 와일드카드 마스크로 원본 및 대상 주소를 지정하여 주소 범위를 표현할 수 있습니다. IPv6 액세스 목록은 소스 주소와 서브넷을 지정할 수 있습니다.
  - BGP 필터링 프로파일에서 인바운드 배포 목록(액세스 목록)을 지정하여 BGP가 피어 그룹 또는 피어(인접)에서 수락할 경로를 제어합니다. 즉, 액세스 거부 목록 규칙과 일치하는 경로가 로컬 BGP RIB에 배치되지 않습니다. 액세스 허용 목록 규칙과 일치하는 경로는 로컬 BGP RIB에 배치됩니다. BGP 필터링 프로파일을 IPv4 유니캐스트 필터링 또는 IPv6 유니캐스트 필터링 필드의 BGP 피어 그룹 또는 피어에 적용합니다. (피어에 대해 이 작업을 수행하려면 번호 상속을 선택합니다.) 피어 설정이 피어 그룹 설정보다 우선합니다.
  - BGP 필터링 프로파일에서 아웃바운드 배포 목록(액세스 목록)을 지정하여 네트워크 및 BGP 배포에 따라 방화벽이 피어 그룹 또는 피어에 보급하는 경로를 제어합니다. 그런 다음 BGP 필터링 프로파일을 IPv4 유니캐스트 필터링 또는 필터링 IPv6 유니캐스트 필드의 BGP 피어 그룹 또는 피어에 적용합니다. (피어에 대해 이 작업을 수행하려면 번호 상속을 선택합니다.) 피어 설정이 피어 그룹 설정보다 우선합니다.
  - 재배포 경로 맵의 일치 기준으로 IPv4 또는 IPv6 대상 주소, 다음 홉 또는 경로 원본을 지정합니다.
  - BGP 경로 맵에서 IPv4 주소, 다음 홉 또는 경로 원본과 IPv6 주소에 대한 일치 조건으로 매핑됩니다.
  - OSPFv2 및 OSPFv3에서 ABR(영역 경계 라우터)에 대한 목록 가져오기 및 내보내기 목록.
  - IPv4 멀티캐스트에 대한 PIM 그룹 권한을 지정합니다.

  액세스 목록은 사용자 트래픽을 필터링하거나 보안을 제공하기 위한 것이 아닙니다.

  액세스 목록에는 여러 규칙이 있을 수 있습니다. 경로는 규칙에 대해 순차적으로 평가됩니다. 경로가 규칙과 일치하면 거부 또는 허용 작업이 발생하고 경로가 후속 규칙에 대해 평가되지 않습니다.

  집계된 보기에는 구성된 모든 액세스 목록이 표시됩니다. 액세스 목록을 강조 표시하여 수정하거나 삭제할 수 있습니다.

- 접두사 목록 - 접두사 목록을 사용합니다.
  - 경로 접두사 및 접두사 길이에 따라 로컬 RIB에 추가되는 네트워크 경로를 필터링합니다.
  - BGP 필터링 프로파일에서 인바운드 접두사 목록을 지정하여 BGP가 피어 그룹 또는 피어(인접)에서 수락할 경로를 제어합니다. 즉, 거부 접두사 목록 규칙과 일치하는 경로가 로컬 BGP RIB에 배치

되지 않습니다. 허용 접두사 목록 규칙과 일치하는 경로는 로컬 BGP RIB에 배치됩니다. 그런 다음 BGP 필터링 프로파일을 IPv4 유니캐스트 필터링 또는 필터링 IPv6 유니캐스트 필드의 BGP 피어 그룹에 적용합니다. (피어에 대해 이 작업을 수행하려면 번호 상속을 선택합니다.) 피어 설정이 피어 그룹 설정보다 우선합니다.

- BGP 필터링 프로파일에서 아웃바운드 접두사 목록을 지정하여 네트워크 및 BGP 배포에 따라 방화벽이 피어 그룹 또는 피어에 보급하는 경로를 제어합니다. 그런 다음 BGP 필터링 프로파일을 IPv4 유니캐스트 필터링 또는 필터링 IPv6 유니캐스트 필드의 BGP 피어 그룹 또는 피어에 적용합니다. (피어에 대해 이 작업을 수행하려면 번호 상속을 선택합니다.) 피어 설정이 피어 그룹 설정보다 우선합니다.
- 재배포 경로 맵의 일치 기준으로 IPv4 또는 IPv6 대상 주소, 다음 홉 또는 경로 원본을 지정합니다.
- BGP 경로 맵에서 IPv4 주소, 다음 홉 또는 경로 원본과 IPv6 주소에 대한 일치 조건으로 매핑됩니다.
- 영역의 OSPFv2 또는 OSPFv3 ABR의 경우 인바운드 필터 목록 또는 아웃바운드 필터 목록에 있습니다.
- IPv4 멀티캐스트 PIM 일반 구성에서 SPT 임계값을 지정합니다.
- IPv4 멀티캐스트 경로 맵에서.

접두사 목록에는 여러 규칙이 있을 수 있습니다. 경로는 규칙에 대해 순차적으로 평가됩니다. 경로가 규칙과 일치하면 거부 또는 허용 작업이 발생하고 경로가 후속 규칙에 대해 평가되지 않습니다. 접두사 목록은 접두사 길이(함께 접두사를 식별하는 것)를 가진 접두사를 구성할 수 있고 접두사 길이가 값보다 크거나 작거나 같도록 지정하여 범위를 가질 수 있다는 점에서 유연합니다. 방화벽은 액세스 목록보다 접두사 목록을 더 효율적으로 평가합니다.

- 재배포 경로 맵 - 재배포 프로파일에서 재배포 경로 맵을 사용하여 BGP, OSPFv2, OSPFv3, RIP, 연결 또는 정적 경로(소스 프로토콜)를 BGP, OSPFv2, OSPFv3, RIP 또는 로컬 RIB(대상 프로토콜)에 재배포할 BGP, OSPFv2, OSPFv3, RIP 또는 정적 경로(원본 프로토콜)를 지정합니다. BGP 호스트 경로를 BGP 피어에 재배포할 수도 있습니다. 일치 기준에는 액세스 목록 및 접두사 목록에 지정된 IPv4 및 IPv6 주소가 포함될 수 있습니다.

  재배포 경로 맵에는 여러 항목이 있을 수 있습니다. 경로는 순차적 순서로 항목에 대해 평가됩니다. 경로가 항목과 일치하면 허용되거나 거부되며 경로는 후속 항목에 대해 평가되지 않습니다. 일치하는 항목의 동작이 허용인 경우 방화벽은 경로 맵에서 재분배된 경로로 구성된 속성도 설정합니다.
- 멀티캐스트 경로 맵 - 동적 IGMP 인터페이스의 소스를 필터링하는 멀티캐스트 경로 맵을 생성합니다.

다음 필터는 BGP에만 적용됩니다.

- **AS** 경로 액세스 목록 - AS 경로 액세스 목록을 만듭니다.
  - 다른 라우터에서 가져온 BGP 경로(로컬 BGP RIB로)의 가져오기를 제어하려면 인바운드 필터 목록의 BGP 필터링 프로파일을 사용합니다. 예를 들어 특정 자율 시스템을 통해 제공된 경로만 가져오려고 합니다.
  - BGP 경로를 다른 라우터로 내보내는 것을 제어하려면 아웃바운드 필터 목록의 BGP 필터링 프로파일을 사용합니다.
  - BGP 경로 맵에서 수행할 수 있는 모든 작업을 수행하려면 BGP 경로 맵을 일치 기준으로 사용합니다.
  - BGP 경로를 재배포하려면 BGP 재배포 경로 맵(AS 경로)을 일치 기준으로 사용합니다.

  AS 경로 액세스 목록은 최대 64개의 규칙을 가질 수 있으며 암시적 모든 허용 규칙으로 끝납니다. AS 경로 액세스 목록을 사용하여 자율 시스템을 거부합니다. 경로는 규칙에 대해 순차적으로 평가됩니다. 경로가 규칙과 일치하면 거부 또는 허용 작업이 발생하고 경로가 후속 규칙에 대해 평가되지 않습니다.
- 커뮤니티 목록 - 커뮤니티 목록만들기:
  - BGP 경로 맵에서 참조하여 어떤 식으로든 제어하려는 경로의 BGP 커뮤니티 속성과 일치시킵니다. 예를 들어 경로 그룹(커뮤니티 속성을 공유)을 설정하여 특정 메트릭 또는 로컬 기본 설정을 가질 수 있습니다.
  - BGP 경로 맵의 집합 작업을 참조하여 일치 조건을 충족하는 경로에서 커뮤니티를 제거합니다.
  - 재배포 경로 맵을 사용하여 재배포하려는 경로의 BGP 커뮤니티를 일치시킵니다.

  커뮤니티 목록에는 여러 규칙이 있을 수 있습니다. 경로는 규칙에 대해 순차적으로 평가됩니다. 경로가 규칙과 일치하면 거부 또는 허용 작업이 발생하고 경로가 후속 규칙에 대해 평가되지 않습니다.
- **BGP** 경로 맵 **- BGP** 경로 맵을 만듭니다**.**
  - BGP AFI 프로파일의 기본 원래 경로 맵 필드의 경우 일치 기준은 기본 경로(0.0.0.0)를 생성할 시기를 정의합니다. BGP AFI 프로파일을 BGP 피어 그룹 또는 피어에 적용합니다. 일치 기준은 모든 매개 변수가 될 수 있으며 기존 BGP 경로와 일치하는 경우 기본 경로가 만들어집니다. 경로 맵의 설정 부분은 사용되지 않습니다. 대신 아웃바운드 경로 맵을 사용하여 생성된 기본 경로에 대한 속성을 설정할 수 있습니다.
  - BGP가 피어로 보내는 BGP 특성을 설정(재정의)합니다.
  - NAT의 경우 보급하는 특정 접두사 그룹에 대해 소스 주소 및 IPv4 다음 홉을 설정하려면 NAT 풀에서 공용 IP 주소를 입력하여 개인 IP 주소를 바꿉니다.
  - 정적, 연결된 또는 OSPF 경로를 BGP로 재배포하려면; 그런 다음 BGP 재배포 프로파일에서 BGP 경로 맵을 참조합니다.
  - BGP 필터링 프로파일에서 인바운드 경로 맵 또는 아웃바운드 경로 맵의 BGP 경로 맵을 사용하여 BGP 피어에서 로컬 BGP로 수락(학습)된 경로를 필터링합니다. RIB(인바운드) 또는 BGP 피어에 알립니다(아웃바운드).
  - BGP 경로를 조건부로 보급하려면 BGP 필터링 프로파일에서 경로에 이러한 조건이 있는 경우 광고 맵을 기반으로 경로를 보급하도록 지정하는 기존 맵을 만듭니다 . 또는 이러한 조건이 존재하지 않는 경우 존재하지 않는 광고 맵을 기반으로 경로를 보급하도록 지정합니다.
  - BGP 필터링 프로파일에서 개인 주소가 아닌 공용 NAT 주소를 사용하도록 IPv4 다음 홉을 설정합니다.

- BGP 필터링 프로파일에서 BGP 경로 맵을 사용하여 경로 감쇠 또는 집계로 인해 억제된 경로를 억제 해제합니다.
- 보다 구체적인 경로를 조건부로 필터링하려면 논리적 라우터에 대해 BGP 집계 경로를 구성하고 억제 맵을 제공합니다.
- 집계 경로에 대한 속성을 설정하려면 논리적 라우터에 대해 BGP 집계 경로를 구성하고 속성 맵을 제공합니다.

필터에는 여러 규칙이 있을 수 있습니다. 방화벽은 규칙의 시퀀스 번호(**Seq**)별로 순서대로 필터의 규칙에 대해 패킷 또는 경로를 평가합니다. 패킷 또는 경로가 규칙과 일치하면 거부 또는 허용 작업이 발생하고 패킷 또는 경로가 후속 규칙에 대해 평가되지 않습니다.

AS 경로 액세스 목록을 제외한 모든 필터는 암시적 모든 거부 규칙으로 끝납니다. AS 경로 액세스 목록을 제외한 모든 필터에는 하나 이상의 허용 규칙이 있어야 하며, 그렇지 않으면 검사된 모든 경로/패킷이 거부됩니다. AS Path 액세스 목록은 암시적 모두 허용 규칙으로 끝납니다.

구성된 **Seq** 번호를 선택하여 규칙을 열고 수정합니다. 구성된 규칙에서 작업 필드를 선택하여 허용 또는 거부 작업만 수정합니다.

규칙을 추가할 때 이후 규칙이 필터에 삽입될 수 있도록 규칙 사이에 사용되지 않는 시퀀스 번호를 충분히 남겨 둡니다. 예를 들어 시퀀스 번호 10, 20, 30 등을 사용합니다.

STEP 1 | 이 필터가 적용되는 IPv4 또는 IPv6 주소를 허용하거나 거부하는 액세스 목록을 만듭니다.

1. 네트워크 > 라우팅 > 필터를 선택합니다.
2. 추가 액세스 목록을 이름(최대 63자)으로 필터링합니다. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 유용한 설명을 입력합니다.
4. 액세스 유형 목록을 선택합니다. **IPv4** 또는 **IPv6**입니다.

   1. IPv4의 경우 **IPv4** 항목을 추가하고 규칙에 대한 **Seq** 번호를 입력합니다(범위는 1~65,535).

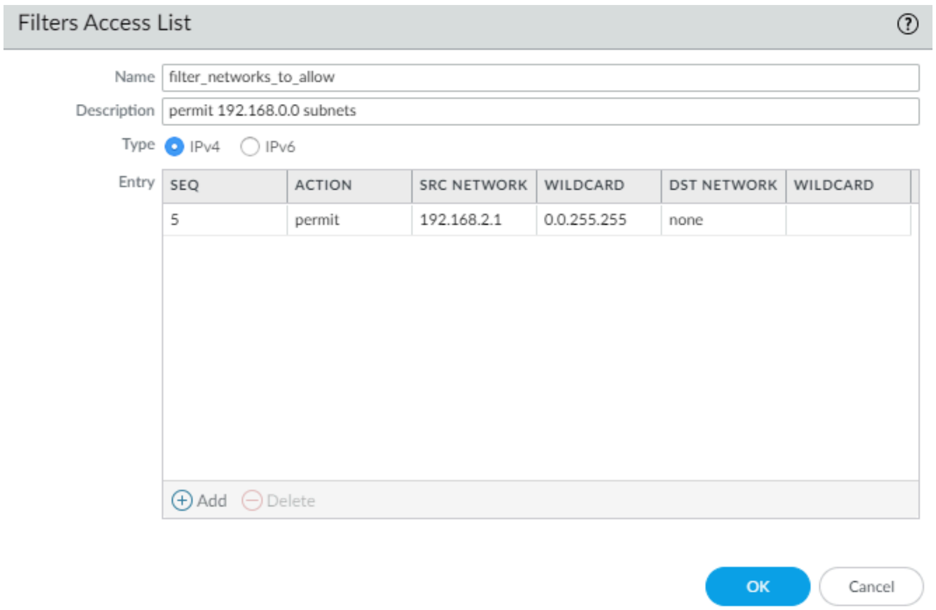
   2. 작업을 선택합니다. 거부 (기본값) 또는 허용.

   3. 소스 주소의 경우 세 가지 옵션이 있습니다. 주소를 선택하고 후속 주소 필드에 IPv4 주소를 입력합니다. 와일드카드 마스크를 입력하여 범위를 나타냅니다. 마스크의 영(0)은 비트가 주

소의 해당 비트와 일치해야 함을 나타냅니다. 마스크의 일(1)은 "관심 없음" 비트를 나타냅니다. 다른 옵션은 임의 또는없음입니다.

4. 대상 주소에 대해 주소를 선택하고 후속 주소 필드에 IPv4 주소를 입력합니다. 와일드카드를 입력합니다. 마스크의 영(0)은 일치해야 하는 비트를 나타냅니다. 마스크의 일(1)은 "관심 없음" 비트를 나타냅니다. 다른 옵션은 임의 또는 없음입니다.

5. 확인을 클릭하여 항목을 저장합니다.



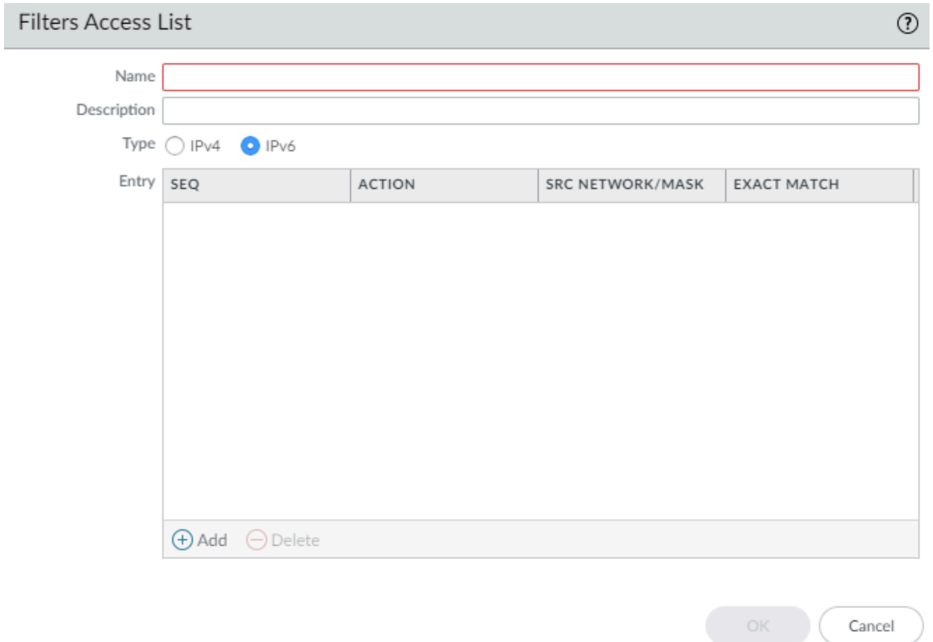
5. 또는 유형을 **IPv6**로 선택합니다.

1. IPv6의 경우 **IPv6** 항목을 추가하고 **Seq** 번호를 입력합니다(범위는 1 ~ 65,535).

2. 작업을 선택합니다. 거부 (기본값) 또는 허용.

3. 소스 주소의 경우 세 가지 옵션이 있습니다. 주소를 선택하고 후속 주소 필드에 IPv6 주소를 입력합니다. 선택적으로 방화벽이 접두사와 접두사 길이를 모두 비교하고 정확히 일치해야 하도록 하려면 이 주소의 정확한 일치를 선택합니다. 그렇지 않으면 방화벽은 경로가 구성된 접두사와 동일한 서브넷에 있는지 여부에 따라 일치 비교를 결정합니다. (소스 주소가 모두 또는 없음인 경우 이 주소와 정확히 일치를 선택할 수 없습니다.) 다른 옵션은 임의 또는 없음입니다.

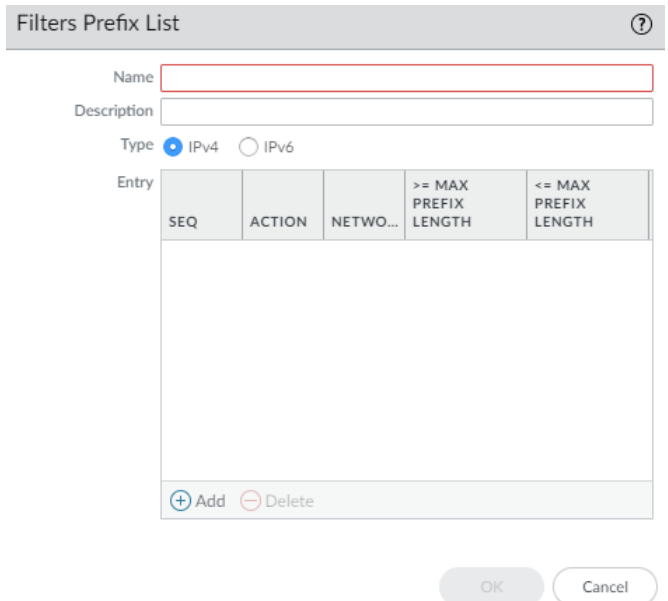
4. 확인을 클릭하여 항목을 저장합니다. 선택적으로 더 많은 항목을 추가합니다.



6. 확인을 클릭하여 액세스 목록을 저장합니다.

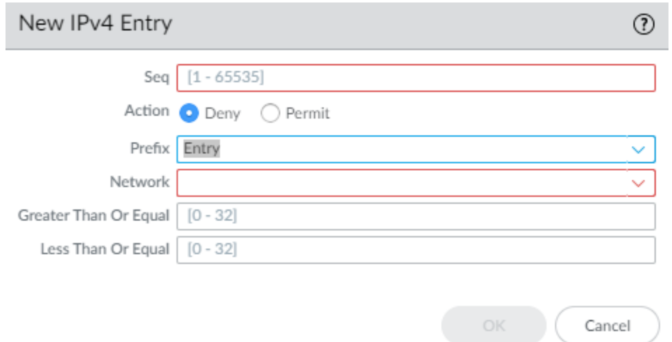
STEP 2 | 접두사 목록을 만듭니다.

1. 네트워크 > 라우팅 > 필터를 선택합니다.
2. 추가 필터링 프리픽스 목록은 이름(최대 63자)입니다. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 유용한 설명을 입력합니다.
4. 필터링할 이 규칙에 대한 접두사의 유형을 선택합니다. **IPv4** 또는 **IPv6**입니다.



   1. IPv4의 경우 **IPv4** 항목을 추가하고 규칙에 대한 **Seq** 번호를 입력합니다. 범위는 1~65,535입니다.
   2. 작업을 선택합니다. 거부 (기본값) 또는 허용.
   3. 접두사의 경우 세 가지 옵션이 있습니다. 기본값은 없음입니다. 또 다른 옵션은 모든 네트워크를 선택하는 것입니다. 세 번째 옵션은 항목을 선택하고 슬래시가 있는 IPv4 네트워크 접두사와 함께 네트워크를 지정하는 기본 접두사 길이(예: 192.168.2.0/24)를 입력하는 것입니다. 선택적으로 접두사 길이가 숫자보다 크거나 같도록 지정합니다(즉, 지정한 기본 길이만큼

크고, 범위는 0에서 32까지임). 선택적으로 숫자에 작거나 같음을 지정하여 범위의 상한값을 지정합니다(최소한 기본 길이만큼 높고 크거나 같음. 구성된 경우 길이, 범위는 0 ~ 32).



경로를 접두사 규칙(IPv4 또는 IPv6)과 비교하는 것은 두 단계 프로세스입니다. 1) 먼저 접두사를 네트워크와 일치시킵니다. 2) 접두사 길이를 마스크 범위(보다 크거나 같거나 작거나 같음)에 일치시킵니다. 예를 들어 네트워크가 192.168.3.0/24인 preflix 목록 규칙과 접두사 길이가 26보다 크거나 같고 30보다 작거나 같은 접두사 길이를 고려하십시오. 다음 표에서는 테스트되는 경로와 해당 경로가 규칙을 통과 또는 실패하는지 여부를 보여 줍니다. 규칙을 통과하는 경로에는 구성된 작업(거부 또는 허용)이 적용됩니다.

샘플 경로	결과
192.168.3.0/28	통과: 네트워크 및 접두사 길이가 규칙과 일치합니다.
192.168.2.0/30	실패: 네트워크가 규칙과 일치하지 않습니다.
192.168.3.0/32	실패: 접두사 길이가 규칙과 일치하지 않습니다.

규칙의 출력 요약에서 LOU는 논리 연산자 단위(같음, 크거나 같음, 작거나 같음)입니다. >=는 값보다 크거나 같은 접두사 길이를 나타냅니다. 접두사 길이 범위 중 가장 낮은 값입니다. <=는 값보다 작거나 같은 접두사 길이를 나타냅니다. 접두사 길이 범위 중 가장 높은 값입니다.

5. 또는 **IPv6** 항목을 추가하고 IPv4 접두사 규칙과 유사한 단계를 따릅니다. IPv6 접두사 길이의 범위는 크거나 같음에서 0~128, 작거나 같음에서 0~128입니다.

   예를 들어, Network 2001:db8:1/48을 사용하는 접두사 목록 규칙과 접두사 길이가 56보다 크거나 같고 64보다 작거나 같음을 고려하십시오. 다음 표에서는 테스트되는 경로와 해당 경로가 규칙을 통과 또는 실패하는지 여부를 보여 줍니다. 규칙을 통과하는 경로에는 구성된 작업(거부 또는 허용)이 적용됩니다.

샘플 경로	결과
2001:db8:1/64	통과: 네트워크 및 접두사 길이가 규칙과 일치합니다.
2001:db8:2/48	실패: 네트워크가 규칙과 일치하지 않습니다.

샘플 경로	결과
2001:db8:1/65	실패: 접두사 길이가 규칙과 일치하지 않습니다.

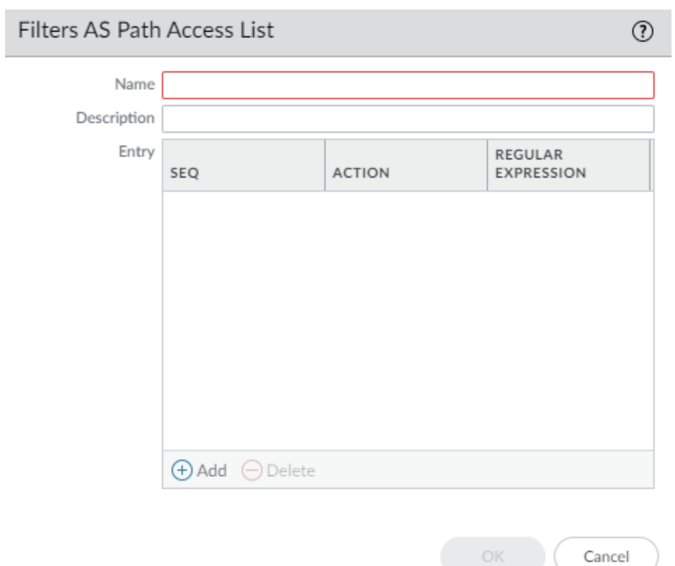
6. 확인을 클릭하여 접두사 항목을 저장합니다. 선택적으로 더 많은 항목을 추가합니다.
7. 확인을 클릭하여 접두사 목록을 저장합니다.

STEP 3 | BGP에 대한 AS 경로 액세스 목록을 만듭니다.

1. 네트워크 > 라우팅 > 필터를 선택합니다.
2. 이름(최대 63자)으로 **AS** 경로 액세스 목록을 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.
3. 유용한 설명을 입력합니다.
4. **Entry**를 추가하고 **Seq** 번호를 입력합니다. 범위는 1~65,535입니다.
5. 작업을 선택합니다. 거부 (기본값) 또는 허용.

   각 *AS* 경로 액세스 목록은 암시적 모든 허용 규칙으로 끝납니다. *AS* 경로 액세스 목록을 사용하여 자율 시스템을 거부합니다.

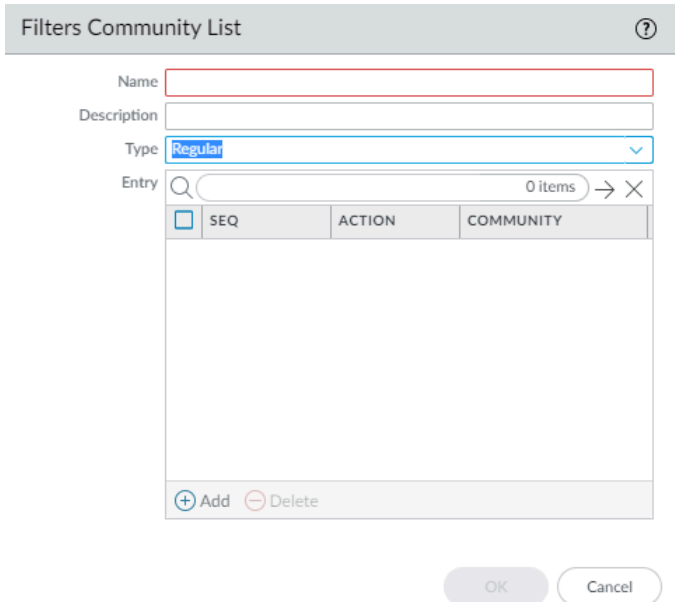
6. **Aspath Regex**(정규식)를 **regex1:regex2:regex3** 형식으로 입력합니다. 여기서 콜론(:)은 세 개의 AS 값을 구분합니다. 허용되는 문자는 1234567890_^|[,{}()]$*+.?-\입니다. 예를 들어 거부 문의 .*65000은 AS 65000에서 시작하는 접두사를 제외합니다.



7. 확인을 클릭하여 항목을 저장합니다. 선택적으로 더 많은 항목을 추가하십시오. AS 경로 액세스 목록에 최대 64개의 항목이 허용됩니다.
8. 확인을 클릭하여 AS 경로 액세스 목록을 저장합니다.

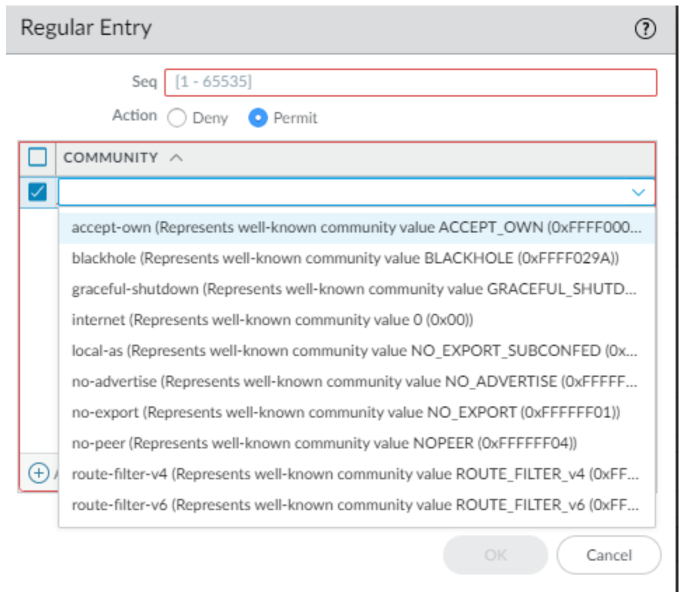
STEP 4 | 커뮤니티 목록을 만듭니다.

1. 네트워크 > 라우팅 > 필터를 선택합니다.
2. 추가 이름(최대 63자)으로 필터링 커뮤니티 목록. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 유용한 설명을 입력합니다.



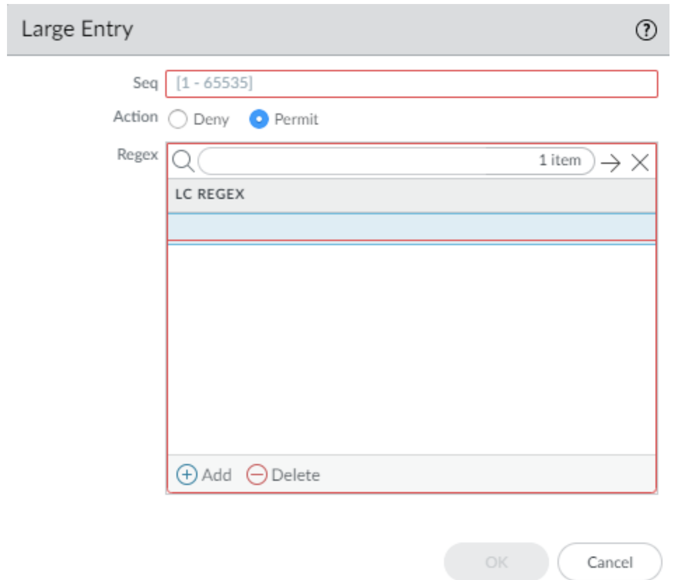
4. 유형을 선택합니다.
   - 일반 - **Seq** 번호(범위: 1~65,535)를 추가하고 액션을 선택합니다. 거부(기본값) 또는 허용 및 하나 이상의 커뮤니티 값을 추가하거나, 하나 이상의 잘 알려진 커뮤니티를 선택하거나, 커뮤니티 값의 조합을 입력합니다. 세로 막대(|)를 사용하여 여러 커뮤니티를 분리합니다(예: **`6409:10|6520:13|internet`**). 일반 항목(규칙)에 최대 16개의 커뮤니티를 입력합니다.
     - AA:NN 형식의 일반 커뮤니티 값입니다. 여기서 AA는 AS 번호이고 NN은 네트워크 번호입니다(각 범위: 0~65,535).
     - **accept-own** - 잘 알려진 커뮤니티 값 ACCEPT-OWN(0xFFFF0001)
     - 블랙홀을 나타냅니다. - 잘 알려진 커뮤니티 값 BLACKHOLE(0xFFFF029A)를 나타냅니다. 인접 네트워크는 접두사로 향하는 트래픽을 폐기해야 합니다.
     - **graceful-shutdown** - 잘 알려진 커뮤니티 값 GRACEFUL_SHUTDOWN(0xFFFF0000)
     - **internet**을 나타냅니다. - 잘 알려진 커뮤니티 값 0(0x00)을 나타냅니다. 모든 BGP 이웃에 접두사를 보급합니다.
     - **local-as** - 잘 알려진 커뮤니티 값 NO_EXPORT_SUBCONFED(0xFFFFFF03)를 나타냅니다. 결과는 연합의 하위 AS 외부에 접두사를 광고하지 않는 것입니다.
     - **no-advertise** - 잘 알려진 커뮤니티 값 NO_ADVERTISE(0xFFFFFF02)를 나타냅니다. 이 커뮤니티를 접두사에 추가하면 수신 BGP 피어가 접두사를 BGP 라우팅 테이블에 배치하지만 다른 이웃에게 접두사를 알리지 않습니다.

- **no-export**—잘 나타냅니다. -알려진 커뮤니티 값 NO_EXPORT(0xFFFFFF01). 이 커뮤니티를 접두사에 추가하면 수신 BGP 피어가 AS 외부의 이웃이 아닌 iBGP 이웃에게만 접두사를 알립니다.
- **no-peer** - 잘 알려진 커뮤니티 값 NOPEER(0xFFFFFF04)를 나타냅니다.
- **route-filter-v4** - 잘 알려진 커뮤니티 값 ROUTE_FILTER_v4(0xFFFF0003)를 나타냅니다.
- **route-filter-v6** - 잘 알려진 커뮤니티 값 ROUTE_FILTER_v6(0xFFFF0005)을 나타냅니다.

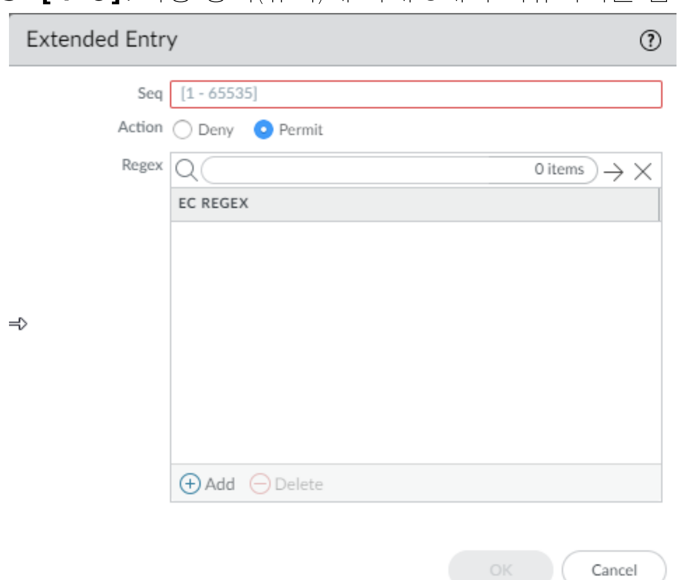


- 대규모 - **Seq** 번호(범위는 1~65,535)를 추가하고 작업을 선택합니다. 거부(기본값) 또는 허용, 대규모 커뮤니티 정규식(LC REGEX) 항목을 추가합니다. 항목에 허용되는 문자는 1234567890_^|[,{}()]$*+.?-\입니다. 각 커뮤니티는 **`regex1:regex2:regex3`** 형식이어

야 합니다. 예: **`203[1-2]:205[2-5]:206[5-6]`**. **Large** 항목(규칙)에 최대 8개의 커뮤니티를 입력합니다.



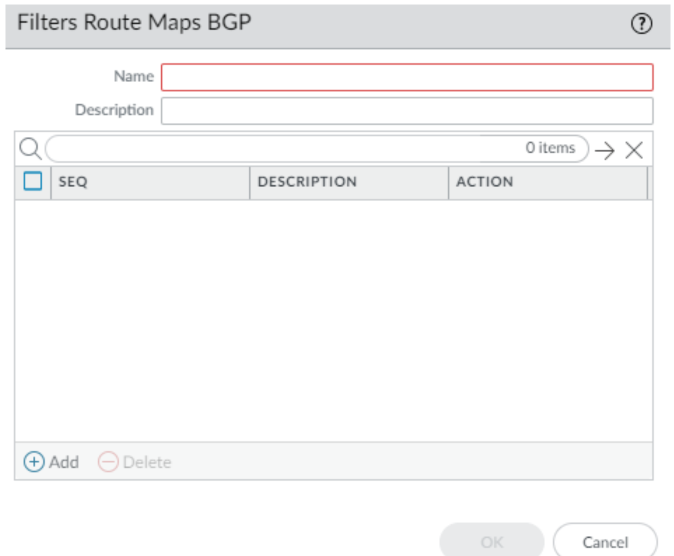
- 확장됨 - **Seq** 번호(범위는 1 ~ 65,535) 추가, 작업 선택: 거부(기본값) 또는 허용, BGP 확장 커뮤니티 정규식(EC REGEX)을 추가합니다. 허용되는 문자는 1234567890_^|[,{}()]$*+.?-\입니다. 각 확장 커뮤니티는 **`regex1:regex2`** 형식이어야 합니다. 예: **`204*[3-8]:205*[4-8]`**. 확장 항목(규칙)에 최대 8개의 커뮤니티를 입력합니다.



5. 확인을 클릭하여 커뮤니티 목록에 항목을 저장합니다. 선택적으로 동일한 유형(일반, 대형 또는 확장)의 항목을 더 추가합니다.
6. 확인을 클릭하여 커뮤니티 목록을 저장합니다.

STEP 5 | BGP 경로 맵을 만듭니다.

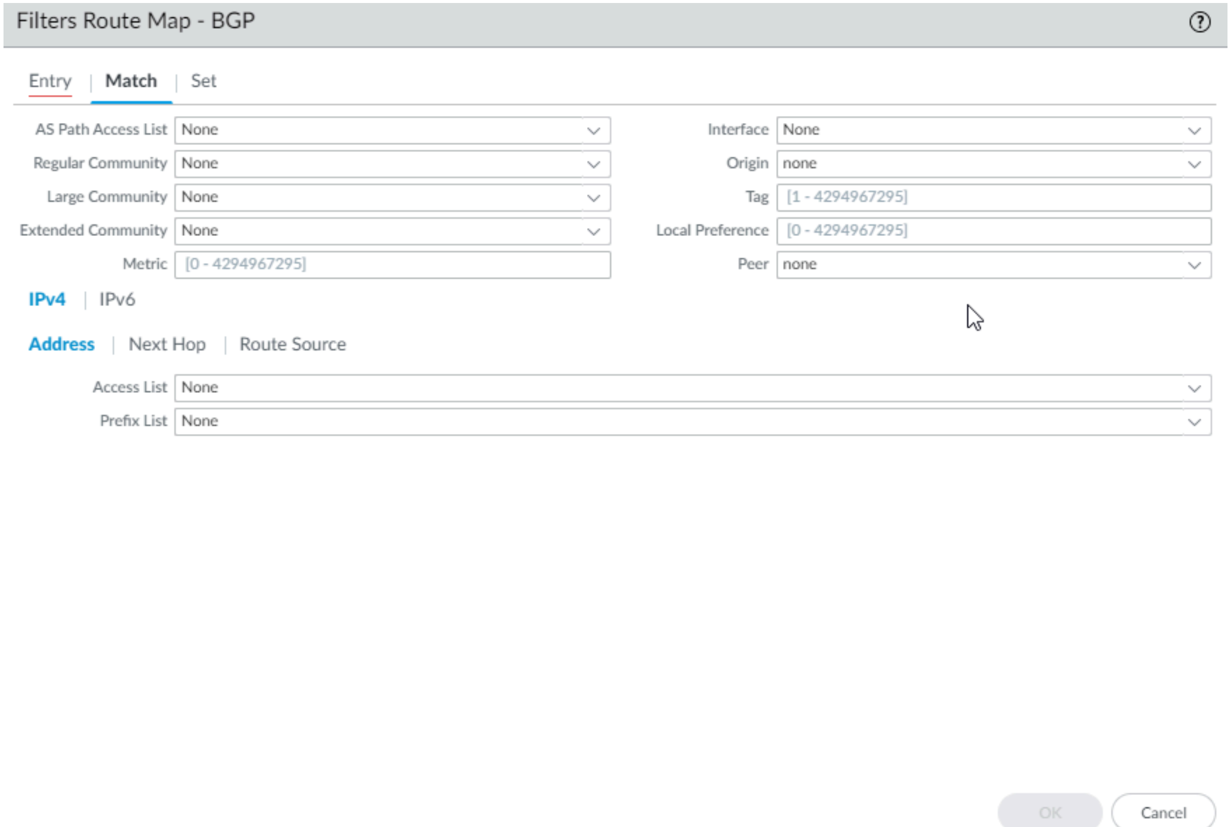
1. 네트워크 > 라우팅 > 필터를 선택합니다.
2. 필터 경로 맵 **BGP**를 이름으로 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 경로 맵에 대한 유용한 설명을 입력합니다.



4. 경로 맵을 추가하고 **Entry** 탭에서 **Seq** 번호를 할당합니다. 범위는 1~65,535입니다.

   다섯 개 이상의 숫자로 구분된 시퀀스 번호를 할당하여 나중에 추가 항목을 삽입할 수 있도록 사용하지 않는 숫자를 지정합니다.

5. 항목(규칙)에 대한 유용한 설명을 입력합니다.
6. 작업에 대해 거부 또는 허용을 선택합니다.
7. 일치 탭에서 이 경로 맵을 사용하는 기능의 적용을 받는 경로를 결정하는 기준을 지정합니다. 여러 속성이 논리적으로 AND로 지정되므로 모든 기준이 충족되어야 합니다.



- **AS** 경로 액세스 목록 - AS 경로 목록을 선택합니다. 기본값은 없음입니다.
- 일반 커뮤니티 - 커뮤니티 목록을 선택합니다. 기본값은 없음입니다.
- 대규모 커뮤니티 - 대규모 커뮤니티 목록을 선택합니다. 기본값은 없음입니다.
- 확장 커뮤니티 - 확장된 커뮤니티 목록을 선택합니다. 기본값은 없음입니다.
- 메트릭 - 0에서 4,294,967,295 사이의 값을 입력합니다.
- 인터페이스 - 모든 논리적 라우터에 대한 모든 인터페이스 목록에서 로컬 인터페이스를 선택합니다. 구성 중인 논리적 라우터에 속하는 인터페이스를 선택해야 합니다. 기본값은 없음입

니다. 커밋 시 방화벽은 선택한 인터페이스가 구성 중인 논리적 라우터에 속하는지 확인합니다.

- 원점 - 경로의 원점(**ebgp**, **ibgp** 또는 **incomplete**)을 선택합니다. 기본값은 없음입니다.
- 태그 - 네트워크에서 의미가 있는 태그 값을 0에서 4,294,967,295 사이의 범위로 입력합니다.
- 로컬 기본 설정 - 0 - 4,294,967,295 범위의 값을 입력합니다.
- 피어 - 피어 이름 또는 로컬**(**정적 또는 재분배된 경로**)**을 선택합니다. 기본값은 없음입니다.

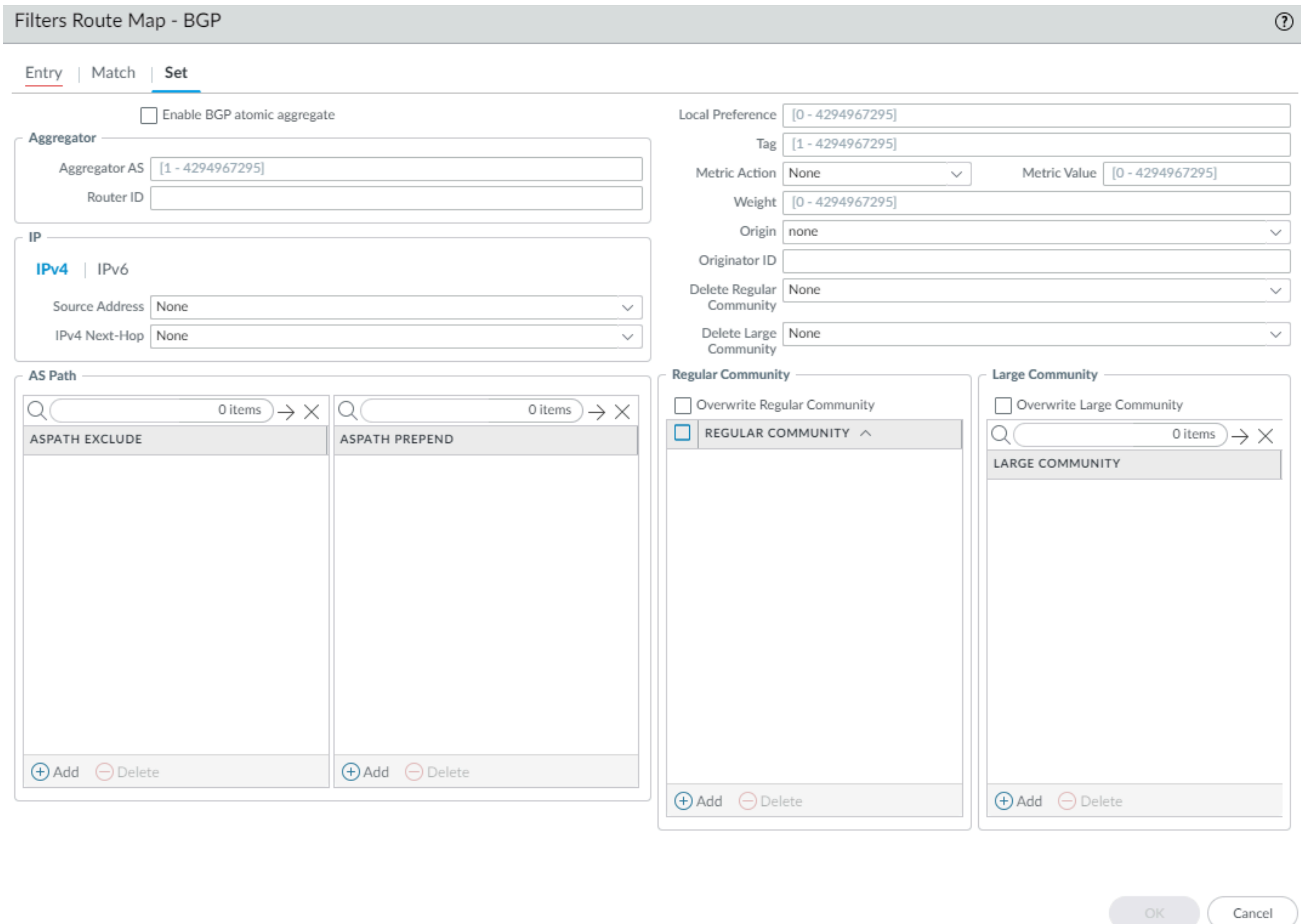
8. **IPv4** 또는 **IPv6**를 선택하여 다양한 유형의 주소와 일치시킵니다. **IPv4**를 선택하는 경우:
   - 주소 탭에서 액세스 목록을 선택하여 일치시킬 주소를 지정합니다.
   - 접두사 목록을 선택하여 일치시킬 주소를 지정합니다. 피어에서 받은 접두사 또는 다른 프로토콜의 프로토콜로 재배포된 접두사와 일치합니다.

     액세스 목록과 접두사 목록이 모두 지정된 경우 두 요구 사항을 모두 충족해야 합니다*(*논리적 *AND).*
   - 다음 홉 탭에서 액세스 목록을 선택하여 일치시킬 다음 홉 주소를 지정합니다.
   - 접두사 목록을 선택하여 일치시킬 다음 홉 주소를 지정합니다.
   - 경로 소스 탭에서 액세스 목록을 선택하여 일치시킬 경로의 소스 IP 주소를 지정합니다. 예를 들어, 액세스 목록은 특정 접두사에 대한 경로를 광고하는 주소가 192.168.2.2인 먼 피어를 허용할 수 있습니다. 이 BGP 경로 맵을 경로의 원본 주소 192.168.2.2에서 일치시킨 다음

피어 주소 192.168.2.2를 경로 원본과 일치시켜 경로를 필터링하거나 해당 경로 원본과 일치하는 경로에 대한 다음 홉을 설정할 수 있습니다.

- 접두사 목록을 지정하여 일치시킬 하나 이상의 원본 네트워크 접두사를 지정합니다.

9. **IPv6**을 선택하는 경우:
    - 주소 탭에서 액세스 목록을 선택하여 일치시킬 주소를 지정합니다.
    - 접두사 목록을 선택하여 일치시킬 주소를 지정합니다.
    - 다음 홉 탭에서 액세스 목록을 선택하여 일치시킬 다음 홉 주소를 지정합니다.
10. 일치 조건을 충족하는 경로에 대해 다음 특성 중 하나를 설정합니다.



- **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.
- 집계 **AS** - 집계 AS를 입력합니다. 집계 속성에는 AS 번호와 집계된 경로를 생성한 라우터의 IP 주소가 포함됩니다. IP 주소는 경로 집계를 수행하는 라우터의 라우터 ID입니다.

- 라우터 **ID** - 집계의 라우터 ID(일반적으로 루프백 주소)를 입력합니다.
- 로컬 기본 설정 - 일치하는 경로가 설정된 로컬 기본설정을 입력합니다. 범위는 0~4,294,967,295입니다. IBGP 업데이트 패킷은 IBGP 피어에게만 보급되는 로컬 기본 설정을 전달합니다. 다른 AS에 대한 경로가 여러 개 있는 경우 방화벽은 가장 높은 로컬 기본 설정을 선호합니다.
- 태그 - 태그를 설정합니다. 범위는 1~4,294,967,295입니다.
- 메트릭 작업 - 작업: 설정, 추가, 또는 뺄셈을 선택합니다. 지정된 메트릭 값을 설정하거나 지정된 메트릭 값을 일치하는 경로의 원래 메트릭 값에 추가하거나 일치하는 경로의 원래 메트릭 값에서 지정된 메트릭 값을 뺄 수 있습니다. 기본값이 설정됩니다. 더하기 또는 빼기 작업을 선택하여 메트릭을 조정하고 일치하는 경로의 우선 순위를 지정하거나 우선 순위를 해제합니다.
- 메트릭 값 - 일치하는 경로를 설정하거나, 원래 메트릭 값에 추가하거나, 빼는 메트릭 값을 입력합니다. 범위는 0~4,294,967,295입니다.
- 가중치 - 가중치(로컬에 적용됨, 전파되지 않음)를 설정합니다. 범위는 0~4,294,967,295입니다.
- 원점 - 일치하는 경로의 원점을 **ebgp**, **ibgp** 또는 **incomplete**(경로가 RIB에 어떻게 추가되었는지 명확하지 않음)로 설정합니다.
- 발신자 **ID**- 일치하는 경로의 발신자의 IP 주소를 설정합니다.
- 일반 커뮤니티 삭제 - 삭제할 일반 커뮤니티를 선택합니다. 기본값은 없음입니다.
- 대규모 커뮤니티 삭제 - 삭제할 대규모 커뮤니티를 선택합니다. 기본값은 없음입니다.
- AFI로 **IPv4** 또는 **IPv6**를 선택합니다.
- **IPv4** 탭에서 모든 논리적 라우터의 모든 소스 주소 목록에서 설정할 소스 주소를 선택하거나 없음을 선택합니다. 커밋 시 방화벽은 선택한 소스 주소가 구성 중인 논리적 라우터에 속해 있는지 확인합니다.
- 없음, 피어 주소**(**피어 주소 사용**)** 또는 변경되지 않음 중에서 설정할 **IPv4 Next-Hop**을 선택합니다.
- **IPv6** 탭에서 **IPv6 Nexthop Prefer Global Address**를 선택하여 다음에 대한 다른 IPv6 주소 유형(링크 로컬 주소, 애니캐스트 주소 또는 멀티캐스트 주소)보다 글로벌 유니캐스트 주소를 선호합니다. 기본적으로 연결된 피어는 글로벌 다음 홉 주소보다 링크-로컬 다음 홉 주소를 선호합니다.
- **IPv6** 탭에서 모든 논리적 라우터의 모든 소스 주소 목록에서 설정할 소스 주소를 선택하거나 없음을 선택합니다. 커밋 시 방화벽은 선택한 소스 주소가 구성 중인 논리적 라우터에 속해 있는지 확인합니다.
- **IPv6 Next-Hop**을 선택하여 없음 또는 피어 주소**(**피어 주소 사용**)**를 설정합니다.
- AS 경로 창에서 일치하는 경로의 AS 경로에서 최대 4개의 AS 경로를 추가하여 연합에서 AS를 제거할 수 있습니다.
- 일치하는 경로의 AS 경로에 **Prepend**에 최대 4개의 AS 경로를 추가합니다(광고의 경로를 덜 바람직하게 만들기 위해).
- 일반 커뮤니티 창에서 일반 커뮤니티 덮어쓰기를 선택하여 일반 커뮤니티를 덮어씁니다.
- 하나 이상의 일반 커뮤니티를 추가하려면 일반 커뮤니티를 추가합니다.

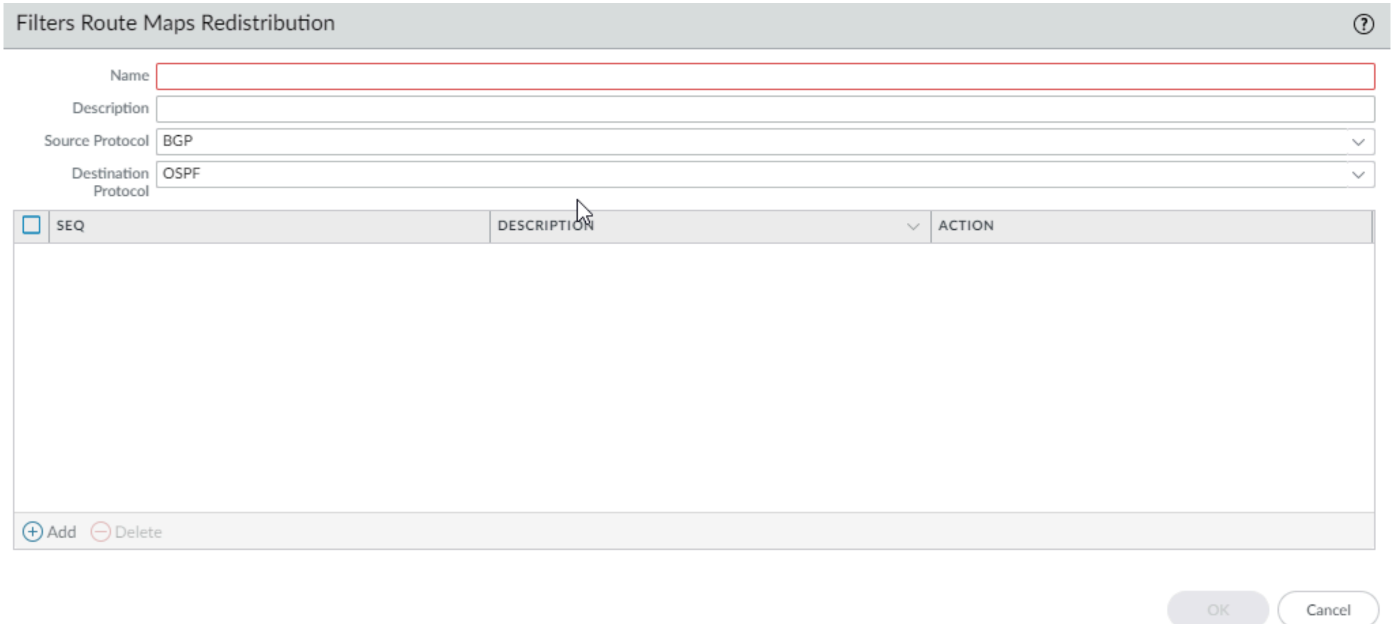
- 대규모 커뮤니티 창에서 대규모 커뮤니티 덮어쓰기를 선택하여 대규모 커뮤니티를 덮어씁니다.
- 하나 이상의 대규모 커뮤니티를 추가하려면 대규모 커뮤니티를 추가합니다.
- 일반 커뮤니티 창에서 일반 커뮤니티 덮어쓰기를 선택하여 일반 커뮤니티를 덮어씁니다.
- 하나 이상의 일반 커뮤니티를 추가하려면 일반 커뮤니티를 추가합니다.
- 대규모 커뮤니티 창에서 대규모 커뮤니티 덮어쓰기를 선택하여 대규모 커뮤니티를 덮어씁니다.
- 하나 이상의 대규모 커뮤니티를 추가하려면 대규모 커뮤니티를 추가합니다.

11. 확인을 클릭하여 경로 맵 항목을 저장합니다. 선택적으로 더 많은 항목을 추가합니다.
12. 확인을 클릭하여 BGP 경로 맵을 저장합니다.

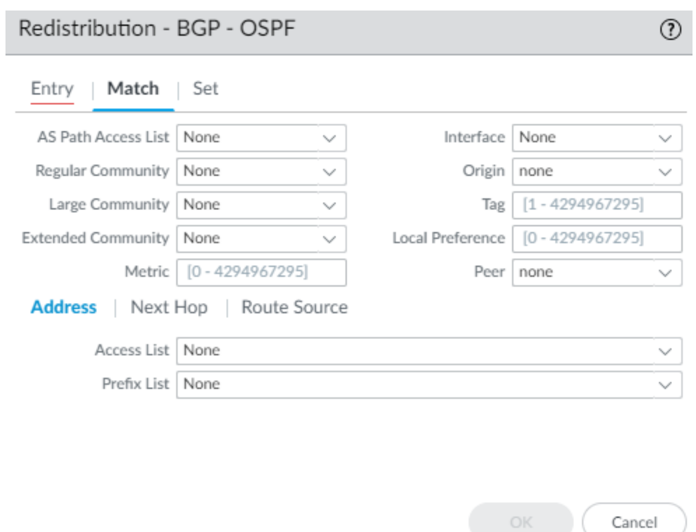
STEP 6 | 재배포 경로 맵을 만듭니다.

1. 네트워크 > 라우팅 > 필터를 선택합니다.
2. 필터 경로 맵 이름별 재배포를 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.
3. 유용한 설명을 입력합니다.
4. 소스 프로토콜에서 재배포하려면 **BGP**, **OSPF**, **OSPFv3**, **RIP** 또는 연결된 정적을 선택합니다. 소스 프로토콜은 매치 선택이 적용되는 위치입니다.
5. 경로를 대상 프로토콜 또는 로컬 RIB로 재배포하려면 **BGP**, **OSPF**, **OSPFv3**, **RIP** 또는 **Rib**를 선택합니다. 대상 프로토콜은 집합 선택이 적용되는 위치입니다. 드롭다운에서 사용할 수 있

는 대상 프로토콜은 선택한 소스 프로토콜에 따라 다릅니다. (이 단계에서는 OSPF에 재배포된 BGP의 예를 보여 줍니다.)

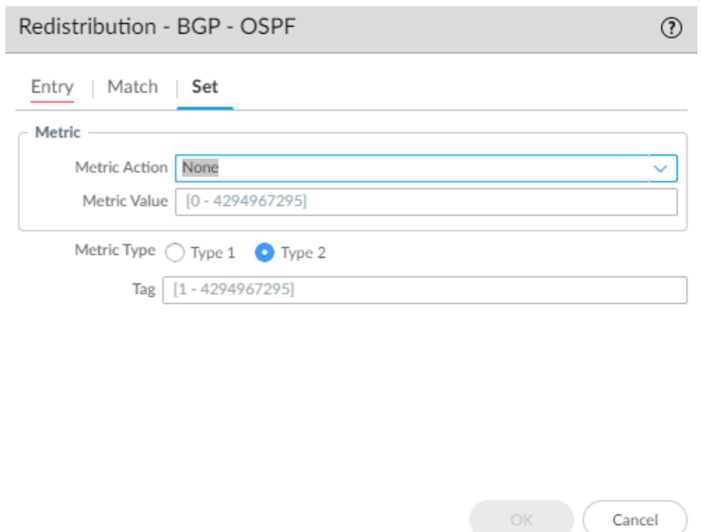


6. 항목을 추가하고 **Seq** 번호를 입력합니다(범위는 1 ~ 65,535).
7. 유용한 설명을 입력합니다.
8. 작업을 선택합니다. 거부 또는 허용.
9. 일치 탭을 선택하여 소스 프로토콜에 대한 조건을 구성합니다. 이 예제에서는 일치시킬 BGP 특성을 지정합니다.



10. **AS** 경로 액세스 목록을 선택합니다. 기본값은 없음입니다.
11. 일반 커뮤니티를 선택합니다. 기본값은 없음입니다.
12. 대규모 커뮤니티를 선택합니다. 기본값은 없음입니다.
13. 확장 커뮤니티를 선택합니다. 기본값은 없음입니다.
14. 메트릭을 입력합니다. 범위는 0~4,294,967,295입니다.

15. 인터페이스를 선택합니다. 기본값은 없음입니다.
16. 경로의 원점(**ebgp**, **ibgp** 또는 **incomplete**)을 선택합니다. 기본값은 없음입니다.
17. 태그를입력합니다. 범위는 1~4,294,967,295입니다.
18. 로컬 기본 설정을 입력합니다. 범위는 0~4,294,967,295입니다.
19. 피어 이름 또는 로컬**(**정적 또는 재분배 경로**)**를 선택합니다. 기본값은 없음입니다.
20. 주소 탭은 경로의 대상 주소를 참조합니다. 액세스 목록을 선택하여 재배포하기 위해 일치해야 하는 대상 주소가 있는 경로를 지정합니다. 기본값은 없음입니다.
21. 접두사 목록을 선택하여 재배포하기 위해 일치해야 하는 대상 주소가 있는 경로를 지정합니다. 기본값은 없음입니다.
22. 설정 탭을 선택하여 이 규칙과 일치하는 경로에서 수행할 작업을 구성하며, 이 작업은 대상 프로토콜에 재배포됩니다. (이 예에서 대상 프로토콜은 OSPF입니다.)



23. 재배포 규칙에 대한 측정항목 작업을 선택합니다. 일치하는 경로의 원래 항목에 메트릭 값을 설정하고 지정된 메트릭 값을 추가할 수 있습니다. 메트릭 값 또는 일치하는 경로의 원래 메트릭 값에서 지정된 메트릭 값을 빼기. 기본값은 없음입니다. 추가 또는 빼기 작업을 선택하여 측정항목을 조정하여 일치하는 경로의 우선순위를 지정하거나 우선순위를 낮춥니다.

    예를 들어 재분배를 사용하여 IGP의 메트릭을 BGP에 넣을 수 있습니다. 메트릭은 동적이며, 절대 숫자로 설정하는 대신 해당 값에 간단히 추가할 수 있습니다.
24. 메트릭에서 설정, 추가 또는 뺄 메트릭 값을 입력합니다. 범위는 0 - 4,294,967,295입니다.
25. 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**(이 예제에서는 OSPF를 대상 프로토콜로 사용하기 때문에).
26. 태그를 지정합니다. 범위는 1 - 4,294,967,295입니다.
27. 규칙을 저장하려면 확인을 클릭합니다. 선택적으로 더 많은 규칙을 추가합니다.
28. 확인을 클릭하여 재배포 경로 맵을 저장합니다.

고급 라우팅 엔진에서 OSPFv2 구성

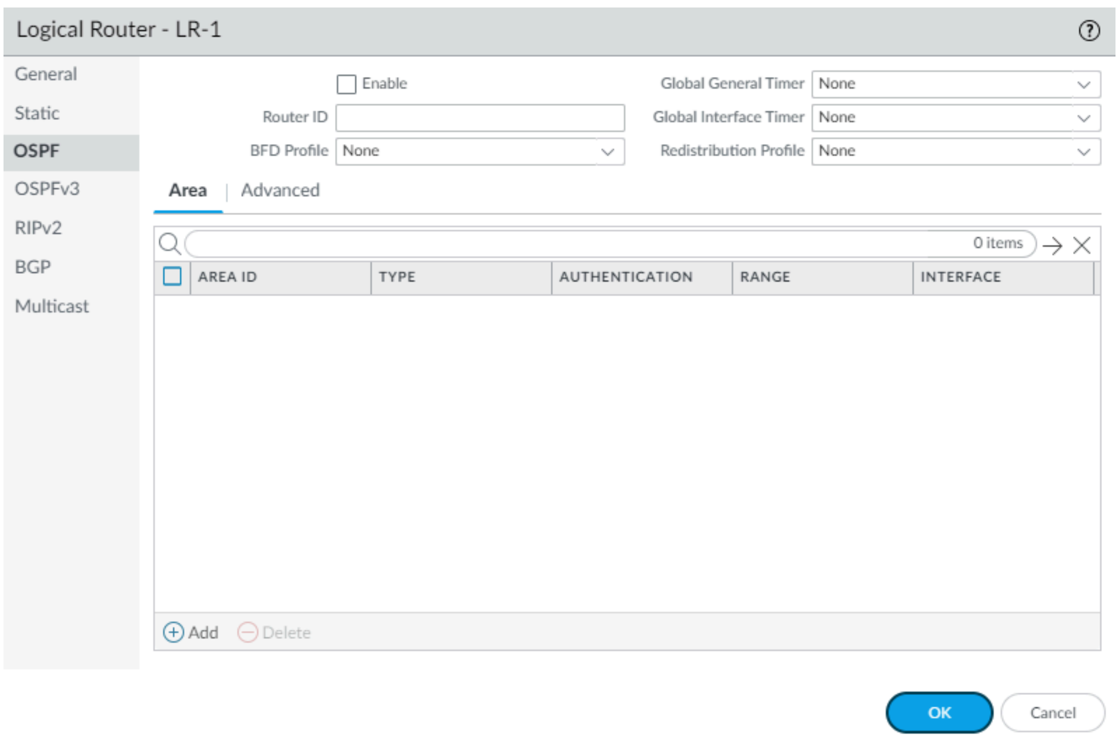
고급 라우팅 엔진은 IPv4 주소 지정만 지원하는 OSPFv2를 지원합니다. OSPFv2를 구성하기 전에 OSPF 컨셉을(를) 이해해야 합니다.

OSPF에 적용할 수 있는 OSPF 라우팅 프로파일 및 필터를 고려하여 구성 시간을 절약하고 일관성을 유지할 수 있습니다. 프로파일과 필터를 미리 만들거나 OSPFv2를 구성할 때 만들 수 있습니다.

STEP 1 | 논리 라우터 구성.

STEP 2 | OSPFv2를 사용하도록 설정하고 일반 설정을 구성합니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **OSPF**를 선택하고 활성화합니다.



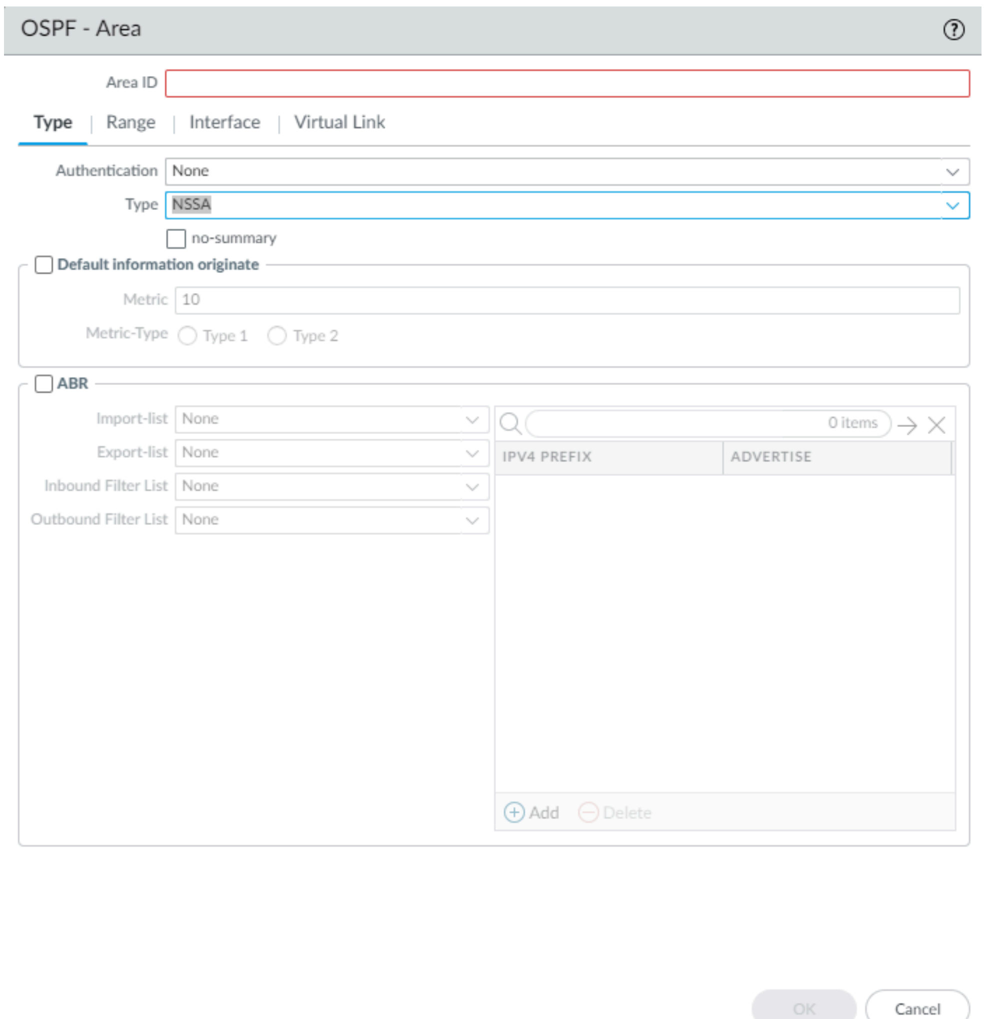
3. IPv4 주소 형식으로 라우터 **ID**를 입력합니다.
4. BFD를 OSPF에 적용하려면 생성한 **BFD** 프로파일을 선택하거나 기본 프로파일을 선택하거나 새 BFD 프로파일을 생성합니다. 기본값은 없음**(BFD** 비활성화**)**입니다.
5. OSPF 전역 일반 타이머 프로파일을 선택하거나 새 프로파일을 만듭니다.
6. OSPF 전역 인터페이스 타이머 프로파일을 선택하거나 새 프로파일을 생성합니다.
7. OSPF 재배포 프로파일을 선택하거나 새 프로파일을 생성하여 IPv4 정적 경로, 연결된 경로, RIPv2 경로, IPv4 BGP 경로 또는 IPv4 기본 경로를 OSPF에 재배포합니다.

STEP 3 | OSPF 영역을 만들고 영역 유형에 따라 특성을 지정합니다.

1. x.x.x.x 형식의 영역 **ID**로 식별되는 영역 및 추가를 선택합니다. 이것은 각 이웃이 동일한 영역의 일부로 수락해야 하는 식별자입니다.
2. 유형 탭을 선택하고 인증에 대해 인증 프로파일을 선택하거나 새 인증 프로파일을 만듭니다.
3. 영역 유형을 선택합니다.
   - 일반 - 제한이 없습니다. 영역은 모든 유형의 경로(영역 내 경로, 영역 간 경로 및 외부 경로)를 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) - NSSA는 스텁 또는 완전히 스텁비 기능을 구현하지만 ASBR(자율 시스템 경계 라우터)을 포함합니다. ASBR에 의해 생성된 유형 7 LSA는 ABR에

의해 유형 5로 변환되고 OSPF 도메인의 나머지 부분으로 플러딩됩니다. (다음 그래픽은 NSSA가 선택된 것을 보여줍니다.)

4. (Stub 및 NSSA 영역만) 요약 없음을 선택하여 영역이 유형 3 요약 LSA를 수신하지 못하도록 하여 해당 영역의 트래픽을 줄입니다.
5. (NSSA 영역만 해당) OSPF가 기본 경로를 시작하도록 하려면 기본 정보 발생을 선택합니다.
   - 기본 경로에 대한 메트릭을 입력합니다. 범위는 1 - 16,777,214이며 기본값은 10입니다.
   - 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**. 유형 E1 비용은 외부 비용과 해당 경로에 도달하기 위한 내부 비용의 합계입니다. 유형 E2는 해당 경로의 외부 비용일 뿐입니다. 예를 들어, 동일한 외부 경로의 부하 분산을 원할 때 유용할 수 있습니다.



6. **ABR**을 선택하여 영역 안팎으로 이동하는 접두사를 필터링한 후 다음 필터를 구성합니다.
   - 가져오기 목록을 선택하거나 새 액세스 목록을 만들어 IPv4 원본 주소를 기반으로 다른 라우터에서 LSA의 영역으로 들어오는 네트워크 경로를 필터링하여 경로가 전역 RIB에 추가되는 것을 허용하거나 금지합니다(액세스 목록의 대상 주소는 비워 둡니다).
   - 내보내기 목록을 선택하거나 새 액세스 목록을 만들어 해당 지역에서 시작된 네트워크 경로를 필터링하여 경로가 다른 영역으로 광고되는 것을 허용하거나 방지합니다.

- 인바운드 필터 목록을 선택하거나 새 접두사 목록을 생성하여 영역으로 들어오는 네트워크 접두사를 필터링합니다.
- 아웃바운드 필터 목록을 선택하거나 새 접두사 목록을 만들어 해당 지역에서 시작된 네트워크 접두사를 필터링하여 경로가 다른 영역으로 광고되지 않도록 합니다.
- 영역의 유형이 **NSSA**이고 **ABR**이 선택된 경우, 그룹을 요약하기 위해 **IPv4 Prefix**를 추가합니다. 외부 서브넷을 단일 유형 7 LSA로 변환한 다음 광고를 선택하면 유형 5 LSA로 변환되고 백본에 광고됩니다.

STEP 4 | 해당 영역의 네트워크 범위를 지정합니다.

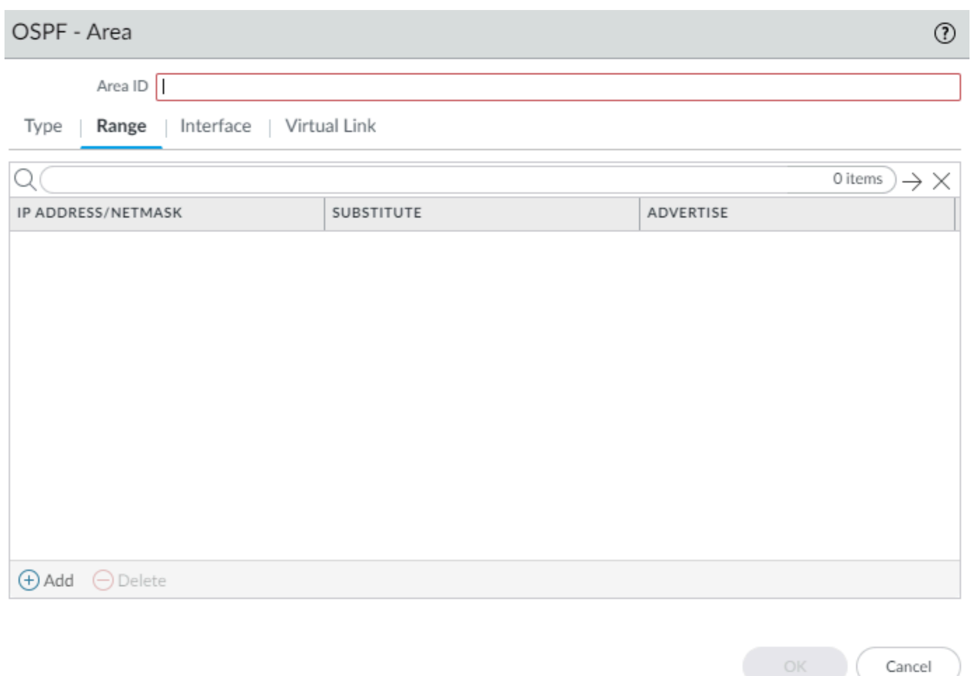
1. 범위를 선택하고 해당 지역의 경로를 요약한 **IP** 주소**/**넷마스크를 추가합니다. 그 결과, 이 범위와 일치하는 라우팅 정보를 가진 Type-3 요약 LSA가 해당 영역에 이 범위에서 하나 이상의 인트라 영역 네트워크(즉, 라우터 또는 네트워크 LSA로 설명됨)가 포함된 경우 백본 영역으로 광고됩니다.

   해당 지역에 대해 *LSDB*에서 학습된 경로를 살펴보고 이 범위를 사용하여 경로를 요약하여 *LSA* 트래픽을 줄입니다.

2. 대체 IP 주소/넷마스크를 입력하여 이전 단계에서 지정한 IP 주소/넷마스크의 영역 내 네트워크가 하나 이상 포함된 경우 이 **IP** 주소**/**넷마스크가 있는 유형 3 요약 LSA가 백본 영역으로 발표되도록 합니다.

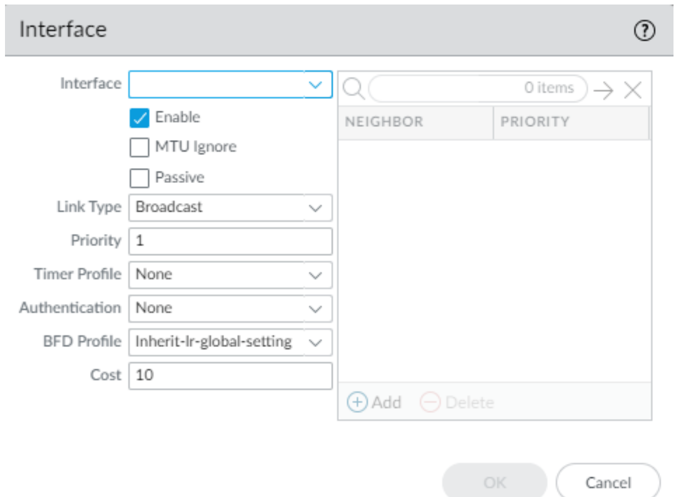
   대체 *IP* 주소/넷마스크를 사용하여 개인 주소를 공용 주소로 변환합니다. 대체 주소는 광고가 비활성화된 경우 효과가 없습니다.

3. 광고를 선택하여 서브넷과 일치하는 LSA(링크 상태 알림)를 보냅니다. 기본값은 사용하도록 설정됩니다.



STEP 5 | 각 인터페이스가 영역에 포함되도록 구성합니다.

1. 하나를 선택하여 인터페이스를 추가하고 활성화합니다.
2. 인접성을 설정하려고 할 때 MTU(최대 전송 단위) 불일치를 무시하려면 **MTU** 무시를 선택합니다(기본값은 비활성화됨, MTU 일치 확인이 발생함). RFC 2328은 인터페이스 MTU를 "조각화 없이 연관된 인터페이스에서 전송할 수 있는 가장 큰 IP 데이터그램의 바이트 크기"로 정의합니다.
3. 수동을 선택하면 인터페이스 네트워크가 광고될 수 있지만 해당 인터페이스에는 인접 관계가 설정되지 않습니다. 이는 리프 인터페이스에 유용합니다.



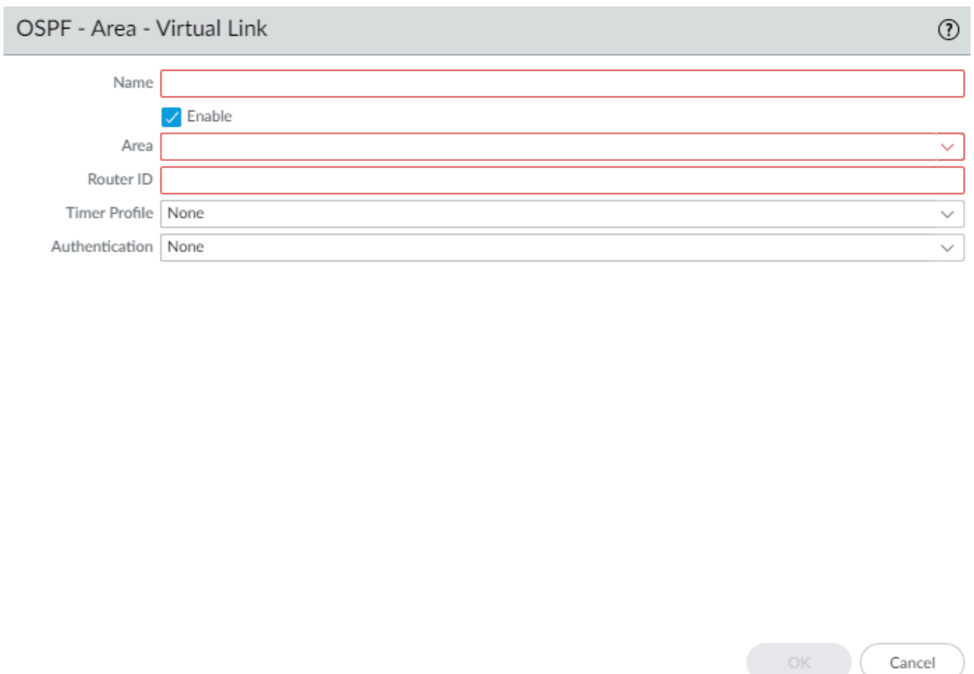
4. 링크 유형을 선택합니다.
   - 브로드캐스트 - 인터페이스를 통해 액세스할 수 있는 모든 인접 네트워크는 이더넷 인터페이스를 통한 OSPF Hello 메시지를 멀티캐스팅하여 자동으로 검색됩니다.
   - **p2p**(point-to-point) - 자동으로 이웃을 검색합니다.
   - **p2mp**(point-to-multipoint) - 인접 항목을 수동으로 정의해야 합니다. 이 인터페이스를 통해 연결할 수 있는 모든 이웃에 대한 이웃 IP 주소와 지정된 라우터(DR) 또는 백업 DR로 선출될 각 이웃의 우선 순위를 추가합니다. 범위는 0에서 255 사이입니다. 기본값은 1입니다.
5. 지정된 라우터(DR) 또는 백업 DR(BDR)으로 선택될 인터페이스의 OSPF 우선 순위를 입력합니다. 범위는 0~255이며, 기본값은 1입니다. 0이 구성되면 라우터가 DR 또는 BDR로 선택되지 않습니다.
6. 인터페이스에 적용할 타이머 프로파일을 선택하거나 새 OSPF 인터페이스 타이머 프로파일을 생성합니다. 이 OSPF 인터페이스 타이머 프로파일은 OSPF에 적용된 전역 인터페이스 타이머를 재정의합니다.
7. 인터페이스에 적용할 인증 프로파일을 선택하거나 새 OSPF 인터페이스 인증 프로파일을 만듭니다. 이 인증 프로파일은 유형(Type 탭의 영역)에 적용된 인증 프로파일을 재정의합니다.
8. 기본적으로 인터페이스는 OSPF용 논리적 라우터에 적용한 BFD 프로파일을 상속합니다(**Inherit-lr-global-setting**). 또는 기본 프로파일을 선택하거나, 다른 **BFD** 프로파일을 선택하

거나, 새 BFD 프로파일 만들기를 선택하거나, 없음**(BFD** 비활성화**)**을 선택합니다. 인터페이스에 대한 BFD를 비활성화합니다.

9. 경로 선택에 영향을 주는 인터페이스의 OSPF 비용을 입력합니다. 범위는 1~65,5535이며 기본값은 10입니다. 경로를 선택하는 동안 누적 비용(사용된 각 인터페이스의 추가 비용)이 더 낮은 경로가 누적 비용이 더 높은 경로보다 선호됩니다.
10. 확인을 클릭합니다.

STEP 6 | ABR에 백본 영역에 대한 물리적 링크가 없는 경우 백본 영역에 대한 물리적 링크가 있는 동일한 영역 내의 이웃 ABR에 대한 가상 링크를 구성한다.

1. 가상 링크를 선택합니다.
2. 이름으로 가상 링크를 추가합니다.
3. 가상 링크를 사용하도록 설정합니다.

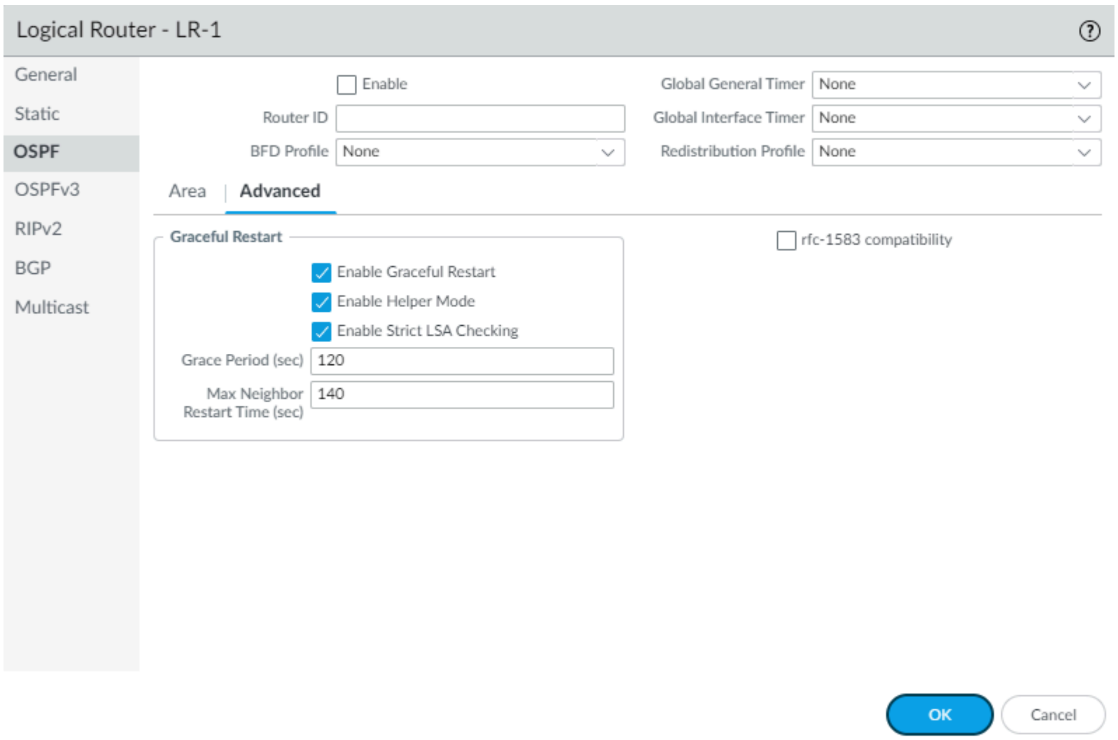


4. 백본 영역에 대한 물리적 링크가 있는 인접 ABR이 있는 환승 영역을 선택합니다.
5. 가상 링크의 원격 끝에 있는 인접 ABR의 라우터 **ID** 를 입력합니다.
6. 타이머 프로파일을 선택하거나 가상 링크에 적용할 새 타이머 프로파일을 만듭니다. 이 OSPF 인터페이스 타이머 프로파일은 OSPF에 적용된 전역 인터페이스 타이머 및 인터페이스에 적용된 OSPF 인터페이스 타이머 프로파일을 재정의합니다.
7. 인증 프로파일을 선택하거나 가상 링크에 적용할 새 인증 프로파일을 만듭니다. 이 인증 프로파일은 영역(유형 탭)에 적용된 인증 프로파일과 인터페이스에 적용된 인증 프로파일을 재정의합니다.
8. 확인을 클릭합니다.

STEP 7 | 확인을 클릭하여 영역을 저장합니다.

STEP 8 | OSPFv2에 대한 OSPF 정상 다시 시작 및 RFC 1583 호환성을 구성합니다.

1. 네트워크 > 라우팅 > 논리적 라우터를 선택하고 논리적 라우터를 선택합니다.
2. **OSPF** > 고급을 선택합니다.
3. **RFC 1583** 호환성을 적용하려면 rfc-1583 호환성을 선택하여 OSPF 라우팅 테이블의 ASBR(자율 시스템 경계 라우터)에 대한 최상의 경로를 허용합니다. 기본값은 비활성화되며, 이는 OSPF 라우팅 테이블이 라우팅 테이블에서 여러 인트라 AS 경로를 유지할 수 있으므로 라우팅 루프를 방지할 수 있음을 의미합니다.

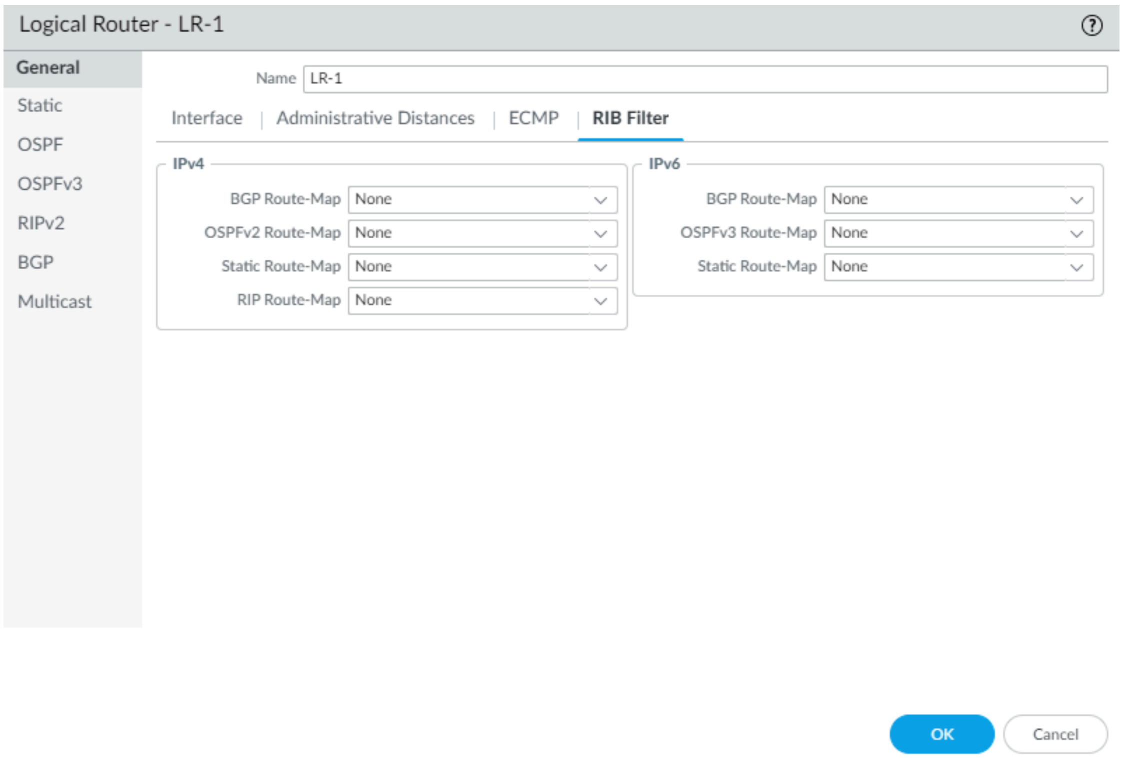


4. 논리적 라우터에 대해 OSPF 정상 다시 시작을 사용하도록 설정하려면 정상 다시 시작을 사용하도록 설정 합니다. 기본값은 활성화되어 있습니다.
5. 도우미 모드를 활성화하여 논리적 라우터가 정상 재시작 도우미 모드에서 작동하도록 설정합니다. 기본값은 활성화되어 있습니다.
6. 엄격한 **LSA** 검사를 사용하도록 설정하여 도우미 라우터가 도우미 모드 수행을 중지하고 링크 상태 알림이 네트워크 토폴로지 변경을 나타내는 경우 정상 재시작 프로세스가 중지되도록 합니다. 기본값은 활성화되어 있습니다.
7. 유예 기간**(**초**)**을 지정합니다. 방화벽이 다운되거나 사용할 수 없게 될 경우 논리적 라우터가 정상적으로 다시 시작되는 시간(초)입니다. 범위는 5~1,800이며 기본값은 120입니다.
8. 최대 인접 재시작 시간**(**초**)**을 지정합니다. 범위는 5~1,800이며, 기본값은 140입니다.
9. 확인을 클릭합니다.

STEP 9 | 영역 내 필터링을 구성하여 전역 RIB에 배치되는 OSPFv2 경로를 결정합니다.

OSPFv2 경로를 배우고 재배포 할 수 있지만 전역 RIB에서는 원하지 않습니다. 전역 RIB에 대한 특정 OSPFv2 경로만 허용할 수 있습니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **RIB** 필터를 선택합니다.
3. 전역 RIB에 대한 **IPv4** OSPFv2 경로를 필터링하려면 **OSPFv2** 경로 맵에서 생성한 재배포 경로 맵을 선택하거나 새 재배포 경로 맵을 생성합니다. 소스 프로토콜은 OSPF이고 대상 프로토콜은 RIB입니다.



4. 확인을 클릭합니다.

STEP 10 | (선택 사항) 논리적 라우터내에서 OSPF 내부 영역, 영역 간 및 외부 경로 에 대한 기본 관리 거리를 변경합니다.

STEP 11 | 커밋합니다.

STEP 12 | OSPFv2 및 LSDB(연결 상태 데이터베이스)에 대한 고급 라우팅 정보를 봅니다. PAN-OS CLI 퀵 스타트에는 CLI 치트 시트에 다음과 같은 명령이 나열되어 있습니다. 네트워킹.

OSPF 라우팅 프로파일 만들기

고급 라우팅 엔진은 OSPFv2를 지원합니다. 프로토콜에 적용할 다음 프로파일을 만들어 구성을 더 쉽고 일관되게 만듭니다. 프로파일은 여러 논리적 라우터와 가상 시스템에서 사용할 수 있습니다. 이 항목에서는 프로파일과 프로파일의 구성 방법에 대해 설명합니다.

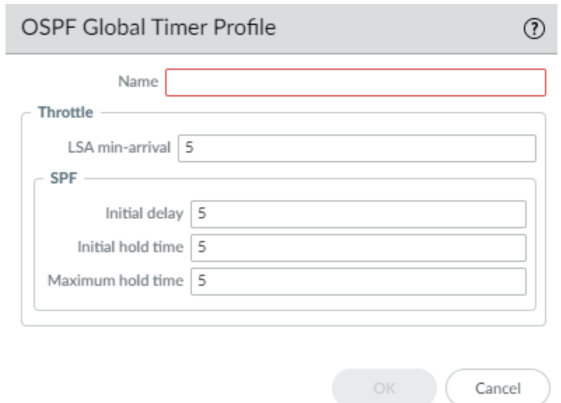
- **OSPF** 글로벌 타이머 프로파일 - OSPFv2 영역에 대한 링크 상태 알림 (LSA) 최소 도착 및 SPF (최단 경로 우선) 타이머에 대한 타이머를 구성합니다. OSPF 일반 컨피그레이션에서 프로파일을 적용합니다.
- **OSPF** 인터페이스 인증 프로파일 - 암호 또는 MD5를 사용하여 인증을 지정합니다. 이러한 프로파일을 OSPF 영역, 인터페이스 및/또는 가상 링크에 적용합니다.
- **OSPF** 인터페이스 타이머 프로파일 - OSPF hello 및 정상 재시작과 같은 인터페이스 작업과 관련된 타이머를 구성합니다. 이러한 프로파일을 OSPF 일반 구성, 인터페이스 및/또는 가상 링크에 적용합니다.
- **OSPF** 재배포 프로파일 - IPv4 정적 경로, 연결된 경로, BGP IPv4 경로, RIPv2 경로 및 IPv4 기본 경로를 OSPF에 재배포하는 방법을 지정합니다. OSPF 일반 컨피그레이션에서 프로파일을 적용합니다.

STEP 1 | OSPF 전역 타이머 프로파일을 만듭니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPF**를 선택합니다.
2. 이름(최대 63자)으로 **OSPF** 글로벌 타이머 프로파일을 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.
3. 동일한 LSA의 두 인스턴스(동일한 광고 라우터 ID, 동일한 LSA 유형 및 동일한 LSA ID)의 전송 사이의 최소 길이 시간(초)인 **LSA** 최소 도착을 입력합니다. 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.
4. SPF 영역에 논리 라우터가 토폴로지 변경을 수신한 시점부터 SPF(최단 경로 우선) 계산을 수행할 때까지의 초기 지연 시간(초)을 입력합니다. 범위는 0 - 600이며 기본값은 5입니다. 값이 낮

을수록 OSPF 재수렴 속도가 빨라집니다. 방화벽과 피어링하는 라우터는 수렴 시간을 최적화하기 위해 동일한 지연 값을 사용해야 합니다.

5. 연속 SPF 계산 사이의 초기 보류 시간(초)을 입력합니다. 범위는 0 - 600이며 기본값은 5입니다.
6. 고정 시간을 유지할 때까지 제한하는 최대 값인 최대 보류 시간(초)을 입력합니다. 범위는 0 - 600이고 기본값은 5입니다.

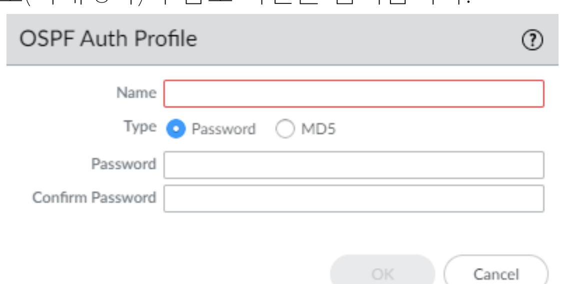


7. 확인을 클릭합니다.

STEP 2 | OSPF 인터페이스 인증 프로파일을 생성합니다.

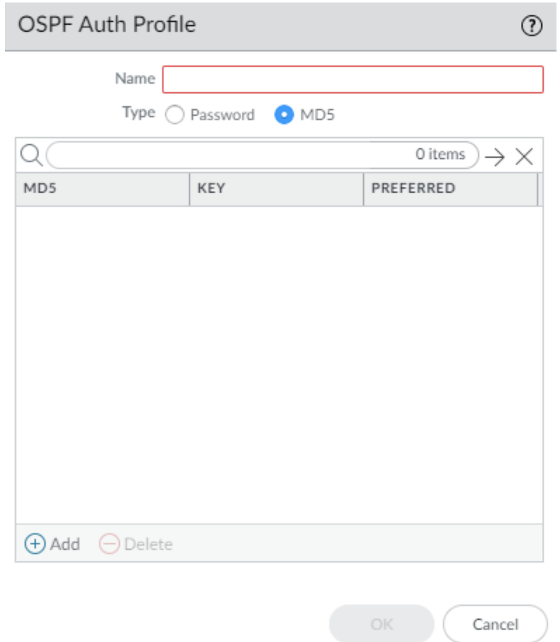
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPF**를 선택합니다.
2. 이름(최대 63자)으로 **OSPF** 인증 프로파일을 추가합니다. 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 인증 유형을 선택합니다. 암호 또는 **MD5**입니다.

   - 암호를 선택한 경우 암호(최대 8자)와 암호 확인을 입력합니다.



   - **MD5**를 선택하는 경우 MD5 키 ID(범위: 0 ~ 255) 및 **Key**(최대 16개의 영숫자)를 추가합니다. 다른 MD5 키보다 MD5 키를 선호하려면 선호를 선택합니다. 커밋하는 동안 방화벽은 위에서 아래로 키 목록을 살펴보고 Preferred key는 목록의 맨 위로 이동합니다. 맨 위의

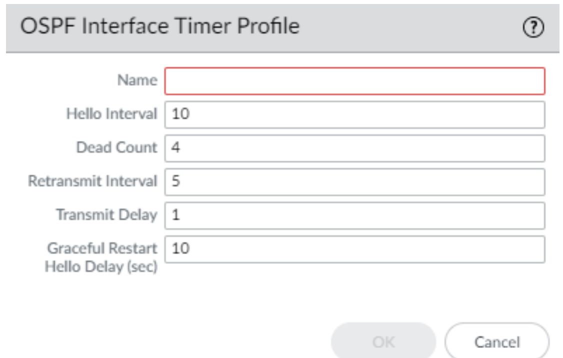
Preferred 키가 사용됩니다. (즉, Preferred MD5 키를 두 개 이상 선택한 경우 Preferred로 선택한 마지막 키가 Preferred 키입니다.)



4. 확인을 클릭합니다.

STEP 3 | OSPF 인터페이스 타이머 프로파일을 생성합니다.

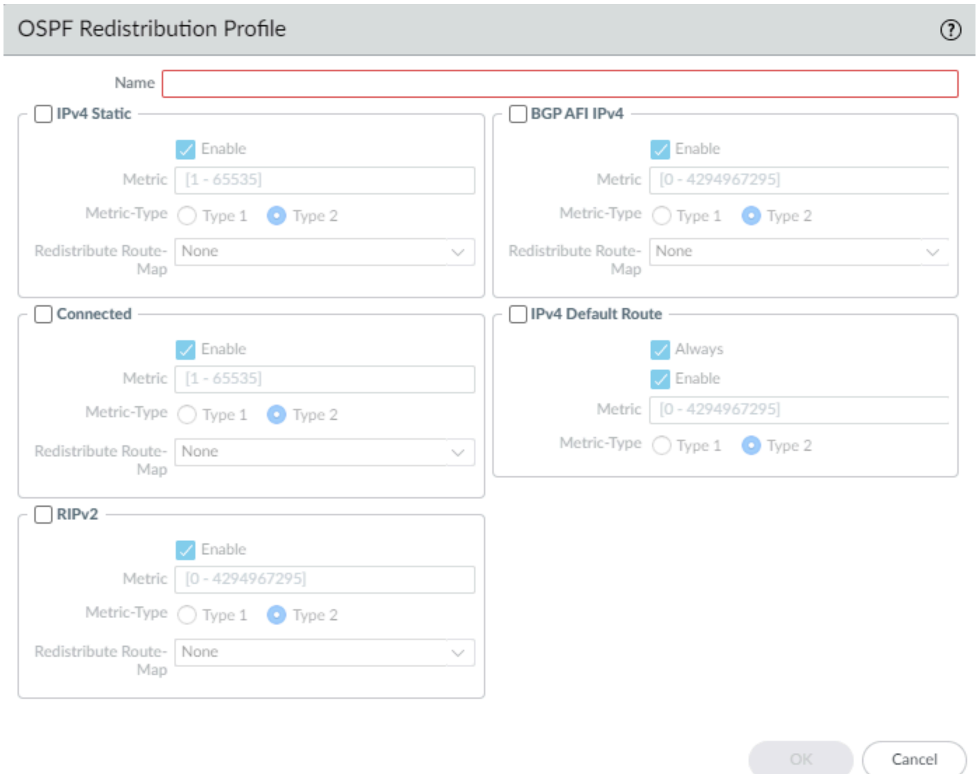
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPF**를 선택합니다.
2. 이름으로 **OSPF** 인터페이스 타이머 프로파일을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.



3. 방화벽이 인접 관계를 유지하기 위해 인터페이스를 전송하는 **Hello** 패킷 사이의 간격**(**초**)**인 **Hello** 간격을 입력합니다**.** 범위는 **1 - 3600**이며 기본값은 **10**입니다**.**
4. OSPF가 인접 디바이스가 다운된 것으로 간주하기 전에 OSPF가 인접 디바이스로부터 hello 패킷을 수신하지 않은 네이버에 대해 Hello 간격이 발생할 수 있는 횟수인 데드 카운트를 입력합니다. 범위는 3에서 20이며 기본값은 4입니다.
5. 인접 라우터에 대한 LSA 재전송 간격(초)을 입력합니다. 범위는 1 - 1800, 기본값은 5입니다.
6. 인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 필요한 시간(초)인 전송 지연을 입력합니다. 업데이트 패킷의 링크 상태 광고는 전송되기 전에 이 숫자만큼 기간이 증가합니다. 범위는 1 ~ 1800입니다. 기본값은 1입니다.
7. 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.
8. 확인을 클릭합니다.

STEP 4 | OSPF 재배포 프로파일을 만들어 IPv4 정적 경로, 연결된 경로, BGP IPv4 경로, RIPv2 경로 및 OSPF에 재배포할 기본 IPv4 경로의 조합을 지정합니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPF**를 선택합니다.
2. 이름(최대 63자)으로 **OSPF** 재배포 프로파일을 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.



3. 프로파일의 이 부분을 구성할 수 있도록 하려면 **IPv4 Static**을 선택합니다.
   - 프로파일의 IPv4 정적 부분을 활성화합니다.
   - OSPF로 재배포되는 정적 경로에 적용할 메트릭을 지정합니다(범위는 1~65,535).
   - 메트릭 유형을 지정합니다. 유형 **1**(OSPF 비용) 또는 유형 **2**(기본값). 목적지에 대한 고정 경로가 두 개 있고 비용이 동일한 경우 유형 1 경로보다 유형 2 경로가 선호됩니다.
   - 경로 맵 재배포를 선택하거나 일치 기준이 OSPF로 재배포할 IPv4 고정 경로를 제어하는 새 재배포 경로 맵 생성을 선택합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재

배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.

4. 연결됨을 선택하여 프로파일의 이 부분을 구성할 수 있습니다.
   - 프로파일의 연결됨 부분을 활성화합니다.
   - OSPF로 재배포되는 연결된 경로에 적용할 메트릭을 지정합니다(범위는 1~65,535).
   - 메트릭 유형을 지정합니다. 유형 **1** 또는 유형 **2**(기본값). 유형 E1 비용은 외부 비용과 해당 경로에 도달하기 위한 내부 비용의 합계입니다. 유형 E2는 해당 경로의 외부 비용일 뿐입니다. 예를 들어, 동일한 외부 경로의 부하 분산을 원할 때 유용할 수 있습니다.
   - 재배포 경로 맵을 선택하거나 일치 기준이 OSPF에 재배포할 연결된 경로를 제어하는 새 재배포 경로 맵을 만듭니다. 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.
5. 프로파일의 이 부분에 대한 구성을 허용하려면 **RIPv2**를 선택합니다.
   - 프로파일의 RIPv2 부분을 활성화합니다.
   - OSPF로 재배포되는 RIPv2 경로에 적용할 메트릭을 지정합니다(범위는 0~4,294,967,295).
   - 메트릭 유형을 지정합니다. 유형 **1** 또는 유형 **2**(기본값).
   - 재배포 경로 맵을 선택하거나 일치 기준이 OSPF로 재배포할 RIPv2 경로를 제어하는 새 재배포 경로 맵을 만듭니다. 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.
6. 프로파일의 이 부분에 대한 구성을 허용하려면 **BGP AFI IPv4**를 선택합니다.
   - 프로파일의 BGP AFI IPv4 부분을 활성화합니다.
   - OSPF로 재배포되는 BGP 경로에 적용할 메트릭을 지정합니다(범위는 0~4,294,967,295).
   - 메트릭 유형을 지정합니다. 유형 **1** 또는 유형 **2**(기본값).
   - 재배포 경로 맵을 선택하거나 일치 기준이 OSPF에 재배포할 BGP IPv4 경로를 제어하는 새 재배포 경로 맵을 만듭니다. 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.
7. 프로파일의 이 부분을 구성할 수 있도록 하려면 **IPv4** 기본 경로를 선택합니다.
   - 항상 IPv4 기본 경로를 OSPF로 재배포하려면 항상을 선택합니다. 기본값은 활성화되어 있습니다.
   - 프로파일의 IPv4 기본 경로 부분을 활성화합니다.
   - OSPF로 재배포되는 기본 경로에 적용할 메트릭을 지정합니다(범위는 0~4,294,967,295).
   - 메트릭 유형을 지정합니다. 유형 **1** 또는 유형 **2**(기본값).
8. 확인을 클릭합니다.

STEP 5 | 커밋합니다.

고급 라우팅 엔진에서 OSPFv3 구성

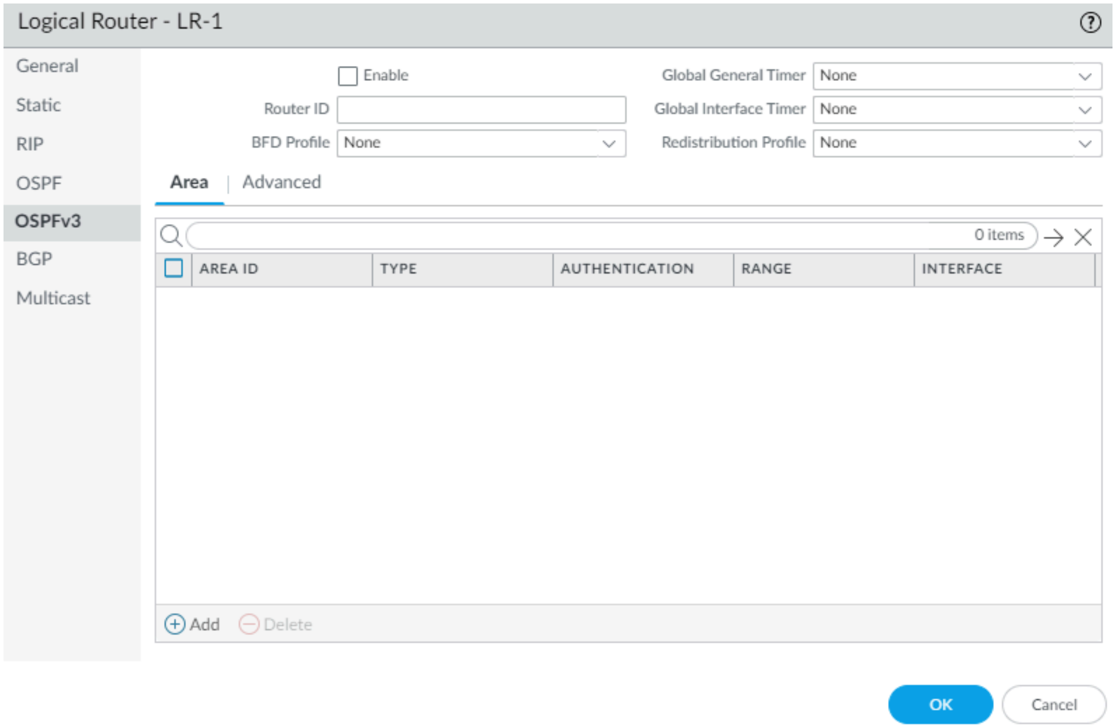
고급 라우팅 엔진은 IPv6 주소 지정만 지원하는 OSPFv3를 지원합니다. OSPFv3를 구성하기 전에 먼저 OSPF 컨셉을(를) 이해해야 합니다.

OSPFv3에 적용할 수 있는 OSPFv3 라우팅 프로파일 및 필터를 고려하여 구성 시간을 절약하고 일관성을 유지할 수 있습니다. 미리 또는 OSPFv3를 구성할 때 프로파일 및 필터를 만들 수 있습니다.

STEP 1 | 논리 라우터 구성.

STEP 2 | 일반 OSPFv3 라우팅 옵션을 구성합니다.

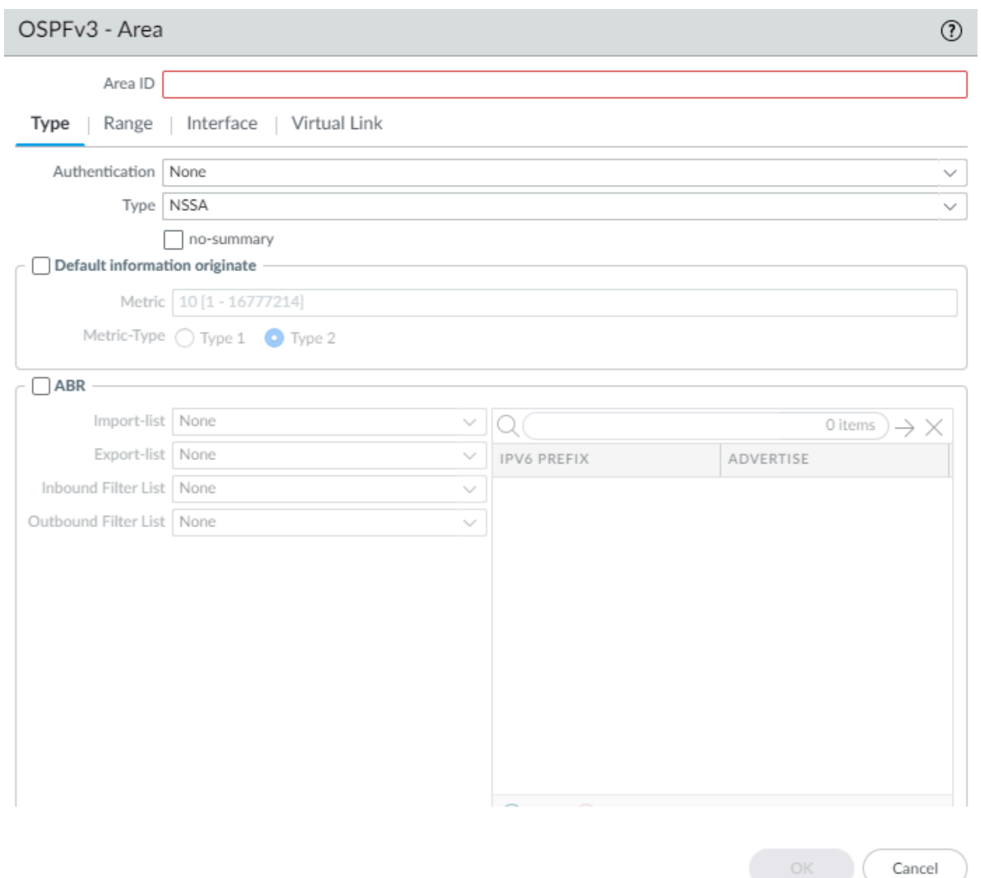
1. 네트워크 > 라우팅 > 논리적 라우터를 선택하고 논리적 라우터를 선택합니다.
2. **OSPFv3**를 선택하고 활성화합니다.



3. 라우터 **ID**가 고유한지 확인하려면 일반적으로 IPv4 주소인 논리적 라우터의 OPSfv3에 라우터 ID를 할당합니다(OSPFv3가 IPv6 주소 지정용이지만).
4. OSPFv3에 BFD를 적용하려면 생성한 **BFD** 프로파일을 선택하거나 기본 프로파일을 선택하거나 논리 라우터에 속하는 모든 OSPFv3 인터페이스에 적용할 새 BFD 프로파일을 만듭니다. 기본값은 없음**(BFD** 비활성화**)**입니다.
5. 전역 일반 타이머 프로파일을 선택하거나 새 프로파일을 만들어 SPF 스로틀 타이머를 설정하고 동일한 LSA(링크 상태 알림)의 인스턴스 도착 사이의 최소 간격을 설정합니다.
6. 전역 인터페이스 타이머 프로파일을 선택하거나 새 프로파일을 생성하여 hello 간격, 재전송 간격 및 기타 설정을 설정합니다.
7. 재배포 프로파일을 선택하거나 새 프로파일을 만들어 IPv6 정적 경로, 연결된 경로, IPv6 BGP 경로 또는 IPv6 기본 경로를 OSPFv3에 재배포합니다.
8. 확인을 클릭합니다.

STEP 3 | OSPFv3 영역을 만들고 영역 유형에 따라 특성을 지정합니다.

1. 네트워크 > 라우팅 > 논리적 라우터를 선택하고 논리적 라우터를 선택합니다.
2. **OSPFv3** > 영역을 선택하고 영역 **ID(IPv4** 주소**)**로 영역을 추가합니다.
3. 유형 탭에서 영역에 대한 인증 프로파일을 선택하거나 새 인증 프로파일을 만듭니다.
4. 영역 유형을 지정합니다.
   - 일반 - 제한이 없습니다. 이 지역은 모든 유형의 경로를 수행할 수 있습니다.
   - **Stub** - 해당 지역의 콘센트가 없습니다. 지역 외부의 목적지에 도달하려면 교통이 다른 지역 및 지역 0에 연결되는 지역 경계 라우터(ABR) 를 통과해야 합니다.
   - **NSSA**(너무 짧지 않은 지역) - 교통량은 OSPF가 아닌 경로를 사용하는 경우에만 해당 지역을 직접 떠날 수 있습니다.
5. (Stub 및 NSSA 영역만) 요약 없음을 선택하여 영역이 유형 3 요약 LSA를 수신하지 못하도록 하여 해당 영역의 트래픽을 줄입니다.
6. (NSSA 영역만 해당) OSPFv3가 기본 경로를 시작하도록 하려면 기본 정보 시작을 선택합니다.
   - 기본 경로에 대한 메트릭을 입력합니다. 범위는 1 - 16,777,214이며 기본값은 10입니다.
   - 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**. 유형 E1 비용은 외부 비용과 해당 경로에 도달하기 위한 내부 비용의 합계입니다. 유형 E2는 해당 경로의 외부 비용일 뿐입니다. 예를 들어, 동일한 외부 경로의 부하 분산을 원할 때 유용할 수 있습니다.



7. 필터링 옵션을 구성하려면 **ABR**을 선택합니다.

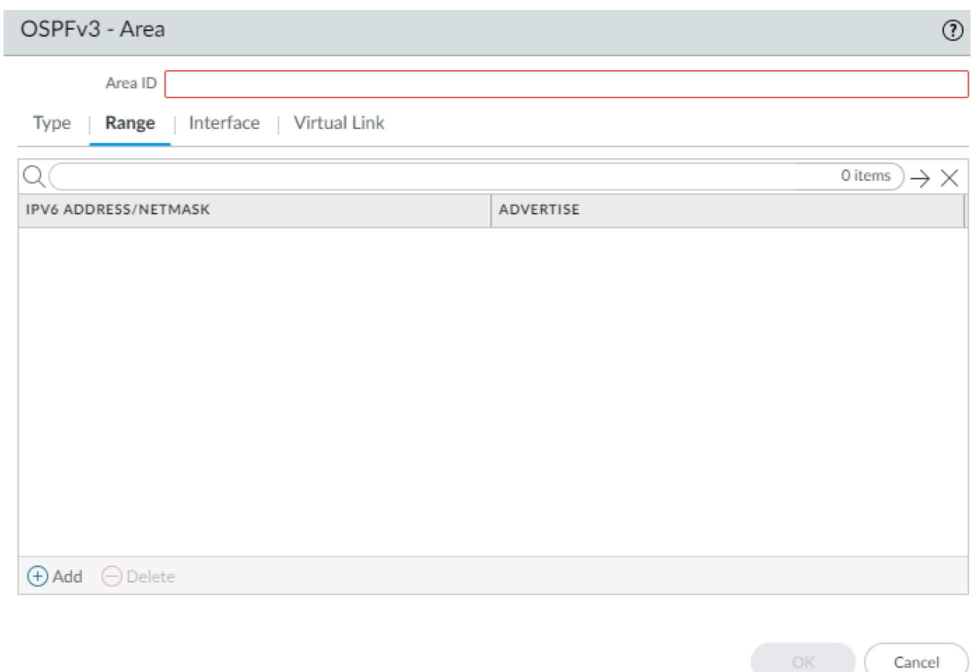
8. 유형 3 LSA를 필터링하려면 가져오기 목록 또는 새 액세스 목록 만들기를 선택하십시오. Type-3 요약 LSA로 지정된 영역에 발표된 경로에 적용됩니다.
9. 내보내기 목록을 선택하거나 새 액세스 목록 만들기를 선택하여 지정된 영역의 영역 내 경로에서 다른 영역에 발표된 Type-3 요약 LSA를 필터링합니다.
10. 인바운드 필터 목록을 선택하거나 새 접두사 목록을 생성하여 영역으로 들어오는 Type-3 요약 LSA를 필터링합니다.

    가져오기 액세스 목록 및 인바운드 접두사 목록을 적용하면 방화벽은 *AND* 작업을 사용합니다*(*두 목록 모두 충족되어야 함*)*.
11. 아웃바운드 필터 목록을 선택하거나 새 접두사 목록을 생성하여 영역에서 Type-3 요약 LSA를 필터링합니다.

    내보내기 액세스 목록 및 아웃바운드 접두사 목록을 적용하면 방화벽은 *AND* 연산을 사용합니다*(*두 목록 모두 충족되어야 함*)*.
12. 영역의 유형이 **NSSA**이고 **ABR**이 선택된 경우, 그룹을 요약하기 위해 **IPv6 Prefix**를 추가합니다. 외부 서브넷을 단일 유형 7 LSA로 변환한 다음 광고를 선택하면 유형 5 LSA로 변환되고 백본에 광고됩니다.

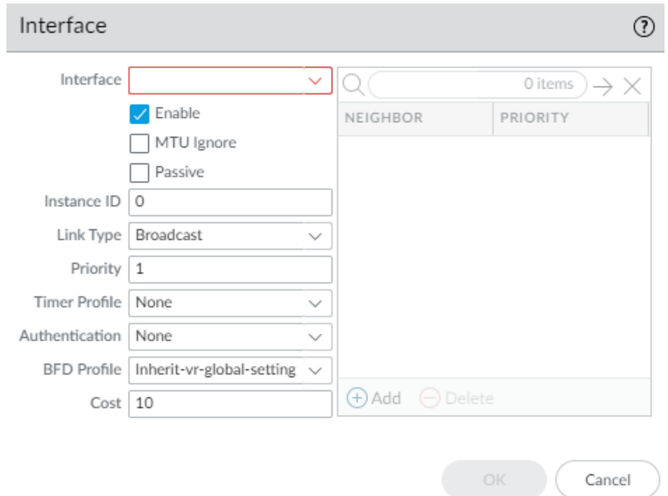
STEP 4 | 영역에 이 범위의 영역 내 네트워크(즉, 라우터 또는 네트워크 LSA로 설명됨) 가 하나 이상 포함된 경우 Type-3 요약 LSA가 백본 영역에 알리는 네트워크 범위를 지정합니다.

1. 범위를 선택하고 해당 지역의 경로를 요약하는 **IPv6** 주소**/**넷마스크를 추가합니다. 영역에 이 범위의 영역 내 네트워크가 하나 이상 포함된 경우 범위와 일치하는 라우팅 정보가 있는 Type-3 요약 LSA가 백본 영역으로 발표됩니다.
2. 광고를 선택하여 LSA의 일치하는 서브넷을 백본 영역에 알립니다. 광고가 아니요로 설정되면 해당 영역에 있는 일치하는 영역 내 접두사는 백본 영역에서 보급되지 않습니다.



STEP 5 | 영역에 인터페이스를 추가합니다.

1. 인터페이스 탭에서 인터페이스를 선택하여 추가합니다.
2. 인터페이스를 활성화합니다.



3. 인접성을 설정하려고 할 때 MTU(최대 전송 단위) 불일치를 무시하려면 **MTU** 무시를 선택합니다(기본값은 비활성화됨, MTU 일치 확인이 발생함).
4. 이 인터페이스에서 OSPF Hello 패킷을 보내지 못하도록 하여 논리 라우터가 인접 항목과 OSPF 인접성을 생성하지 못하도록 하려면 수동을 선택합니다. 그러나 인터페이스는 여전히 링크 상태 데이터베이스에 포함됩니다. 라우터가 없는 곳에서 Hello 패킷을 전송하지 않으려는 경우 스위치에 연결하는 경우와 같이 인터페이스를 수동적으로 만들 수 있습니다.
5. OSPFv3의 인스턴스 하나만 허용되므로 인스턴스 **ID**를 0으로 설정합니다.
6. 링크 유형을 선택합니다.
   - 브로드캐스트 - 인터페이스를 통해 액세스할 수 있는 모든 인접 네트워크는 이더넷 인터페이스를 통한 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 네이버의 인접 IPv6 주소와 지정된 라우터(DR) 또는 백업 DR로 선택될 각 네이버의 우선 순위를 추가합니다. 범위는 0 - 255이며 기본값은 1입니다.
7. 인터페이스의 우선 순위(지정된 라우터(DR) 또는 백업 DR(BDR) 으로 선택할 라우터의 우선 순위를 입력합니다. 범위는 0 - 255, 기본값은 1입니다. 0이 구성되면 라우터가 DR 또는 BDR로 선택되지 않습니다.
8. OSPFv3 인터페이스 타이머 프로파일을 선택하거나 새 프로파일을 생성하여 인터페이스에 적용합니다. 이 OSPFv3 인터페이스 타이머 프로파일은 OSPFv3에 적용된 전역 인터페이스 타이머를 재정의합니다.
9. OSPFv3 인터페이스 인증 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 만듭니다. 이 인증 프로파일은 유형(Type 탭의 영역)에 적용된 인증 프로파일을 재정의합니다.
10. 기본적으로 인터페이스는 OSPFv3의 논리 라우터에 적용한 BFD 프로파일을 상속합니다(**Inherit-vr-global-setting**). 또는 기본 프로파일을 선택하거나, 생성한 **BFD** 프로파일을 선택

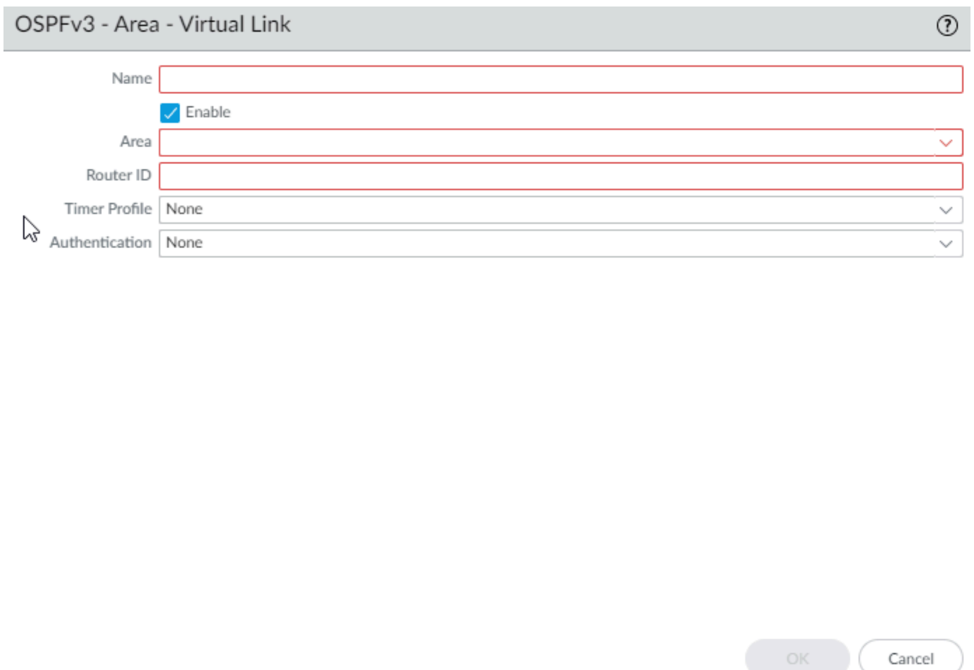
하거나, 새 프로파일을 만들거나, 없음(**BFD** 사용 안 함)을 선택하여 OSPFv3 수준에서 적용된 BFD 프로파일을 재정의합니다.

11. 경로 선택에 영향을 주는 인터페이스의 OSPFv3 비용을 입력합니다. 범위는 1 - 65,5535이며 기본값은 10입니다. 경로를 선택하는 동안 누적 비용(사용된 각 인터페이스의 추가 비용)이 더 낮은 경로가 누적 비용이 더 높은 경로보다 선호됩니다.
12. 확인을 클릭하여 인터페이스를 저장합니다.

STEP 6 | ABR에 백본 영역에 대한 물리적 링크가 없는 경우 백본 영역에 대한 물리적 링크가 있는 동일한 영역 내의 이웃 ABR에 대한 가상 링크를 구성한다.

다음 설정은 *ABR*(영역 경계 라우터)에 대해 정의해야 하며 백본 영역*(0.0.0.0)* 내에 정의되어야 합니다.

1. 가상 링크를 선택합니다.
2. 이름으로 가상 링크를 추가합니다(최대 31자).
3. 가상 링크를 사용하도록 설정합니다.

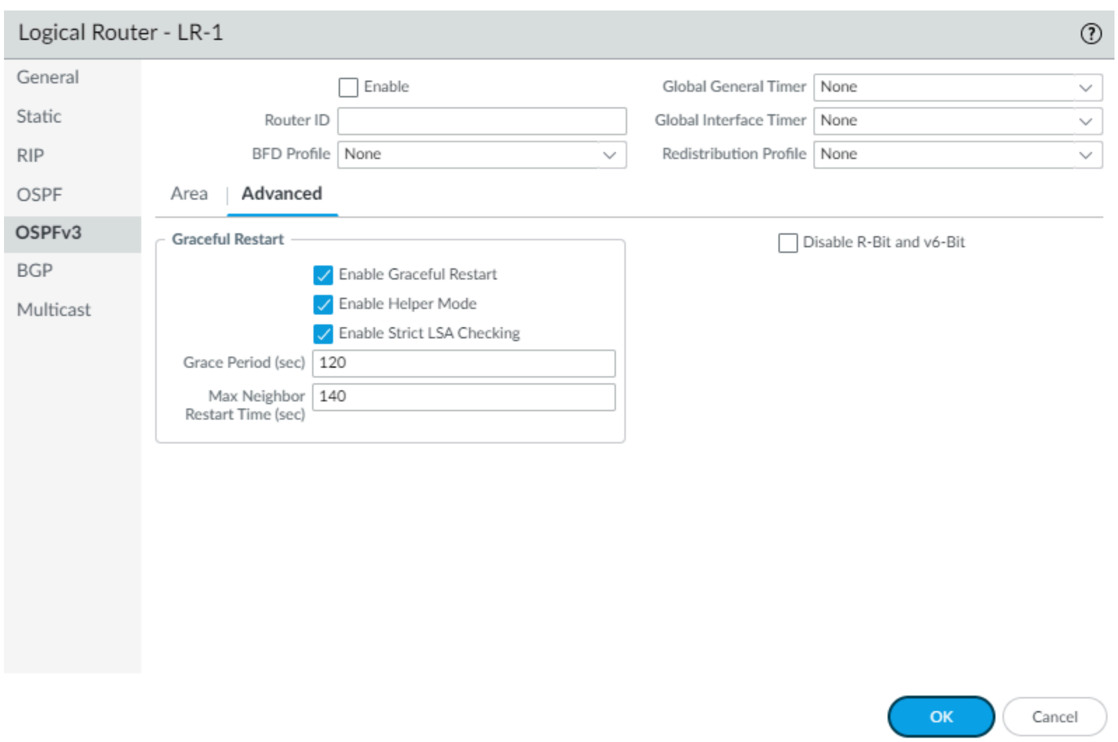


4. 백본 영역에 대한 물리적 링크가 있는 인접 ABR이 있는 환승 영역을 선택합니다.
5. 가상 링크의 원격 끝에 있는 인접 ABR의 라우터 **ID** 를 입력합니다.
6. OSPFv3 인터페이스 타이머 프로파일을 선택하거나 가상 링크에 적용할 새 타이머 프로파일을 만듭니다. 이 OSPFv3 인터페이스 타이머 프로파일은 OSPFv3에 적용된 전역 인터페이스 타이머 및 인터페이스에 적용된 OSPFv3 인터페이스 타이머 프로파일을 재정의합니다.
7. OSPF 인터페이스 인증 프로파일을 선택하거나 가상 링크에 적용할 새 인증 프로파일을 만듭니다. 이 인증 프로파일은 영역(유형 탭)에 적용된 인증 프로파일과 인터페이스에 적용된 인증 프로파일을 재정의합니다.
8. 확인을 클릭합니다.

STEP 7 | 확인을 클릭하여 영역을 저장합니다.

STEP 8 | 고급 OSPFv3 기능을 구성합니다.

1. 네트워크 > 라우팅 > 논리적 라우터를 선택하고 논리적 라우터를 선택합니다.
2. **OSPFv3** > 고급을 선택합니다.
3. 정상 재시작을 활성화하여 논리적 라우터에 대해 정상 재시작을 활성화합니다. 기본값은 활성화되어 있습니다.
4. 도우미 모드를 활성화하여 논리적 라우터가 정상 재시작 도우미 모드에서 작동하도록 설정합니다. 기본값은 활성화되어 있습니다.
5. 링크 상태 알림이 네트워크 토폴로지 변경을 나타내는 경우 도우미 라우터에서 도우미 모드 수행을 중지하고 정상 재시작 프로세스를 중지하려면 엄격한 **LSA** 검사를 활성화합니다. 기본값은 활성화되어 있습니다.
6. 유예 기간**(**초**)** - 방화벽이 다운되거나 사용할 수 없게 될 경우 논리 라우터가 정상 재시작을 수행하는 시간(초) 을 입력합니다. 범위는 5 - 1,800이며 기본값은 120입니다.
7. 최대 인접 라우터 다시 시작 시간**(**초**)**을 입력합니다. 이 시간은 논리적 라우터가 도우미 모드일 때 논리적 라우터가 인접 라우터에서 수락하는 최대 유예 기간(초)입니다. 범위는 5 - 1,800이며 기본값은 140입니다.
8. **R-Bit** 및 **V6-bit** 사용 안 함을 선택하여 이 논리적 라우터에서 보낸 라우터 LSA의 R-비트 및 V6비트를 지워 방화벽이 활성화되어 있지 않음을 나타냅니다. 이 상태인 경우 방화벽은 OSPFv3에 참여하지만 전송 트래픽 또는 IPv6 데이터그램을 보내지 않습니다. 이 상태에서는 로컬 트래픽이 여전히 방화벽으로 전달됩니다. 이는 트래픽이 방화벽에 도달할 수 있는 동안 방화벽 주위로 다시 라우팅될 수 있으므로 이중 홈 네트워크로 유지 관리를 수행할 때 유용합니다. RFC 5340을 참조하십시오.

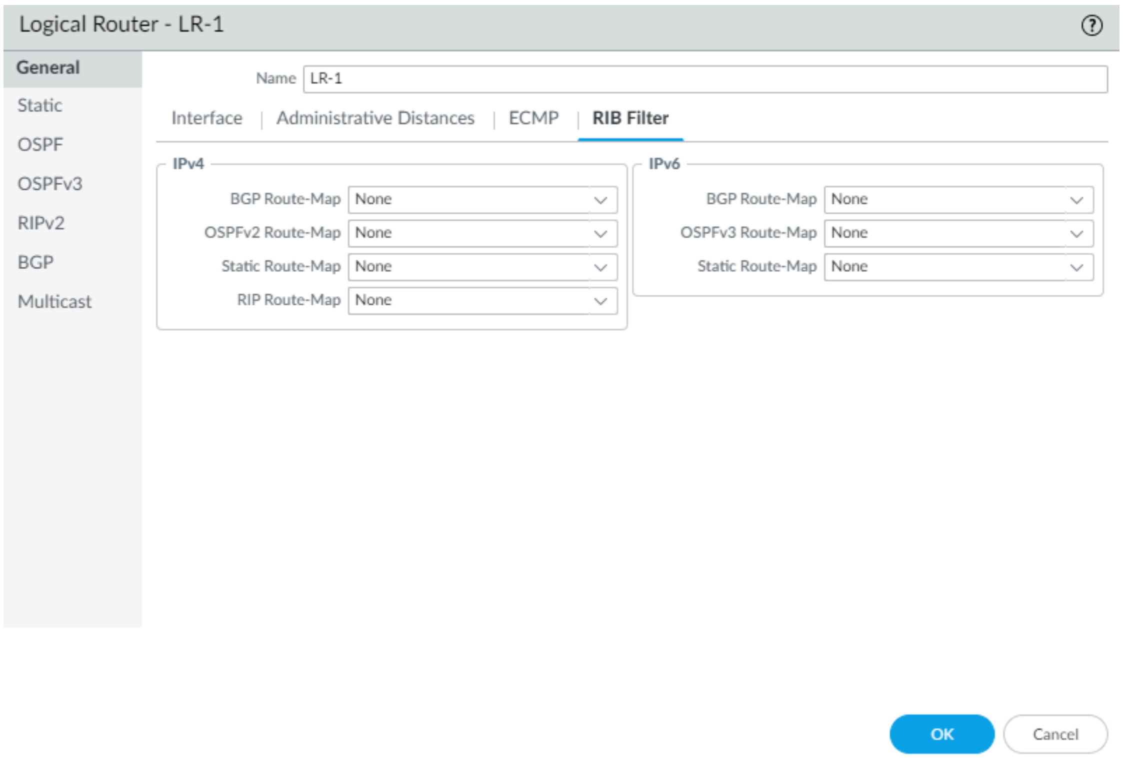


9. 확인을 클릭하여 고급 설정을 저장합니다.

STEP 9 | 영역 내 필터링을 구성하여 전역 RIB에 배치되는 OSPFv3 경로를 결정합니다.

OSPFv3 경로를 학습하고 재배포할 수 있지만 전역 RIB에서는 사용하지 않을 수 있습니다. 전역 RIB에 대한 특정 OSPFv3 경로만 허용할 수 있습니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **RIB** 필터를 선택합니다.
3. 전역 RIB에 대한 **IPv6** OSPFv3 경로를 필터링하려면 **OSPFv3** 경로 맵의 경우 생성한 재배포 경로 맵을 선택하거나 소스 프로토콜이 OSPFv3이고 대상 프로토콜이 RIB인 새 재배포 경로 맵을 만듭니다.



4. 확인을 클릭합니다.

STEP 10 | (선택 사항) 논리 라우터와 관련된 OSPFv3 내부 영역, OSPFv3 영역 간 및 OSPFv3 외부 경로에 대한 기본 관리 거리를 변경합니다.

STEP 11 | 커밋합니다.

STEP 12 | OSPFv3 및 링크 상태 데이터베이스(LSDB) 에 대한 고급 라우팅 정보를 봅니다. PAN-OS CLI 퀵 스타트에는 CLI 치트 시트에 다음과 같은 명령이 나열되어 있습니다. 네트워킹.

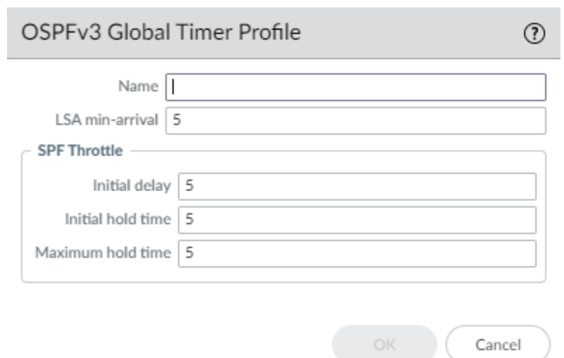
OSPFv3 라우팅 프로파일 만들기

고급 라우팅 엔진은 OSPFv3을 지원합니다. OSPFv3 전역 타이머 프로파일, 인증 프로파일, 인터페이스 타이머 프로파일 및 재배포 프로파일을 만들어 OSPFv3에 적용합니다. 이 항목에서는 프로파일과 프로파일을 만드는 방법에 대해 설명합니다. 고급 라우팅 엔진에서 OSPFv3 구성을(를) 수행할 때 이를 참조하십시오.

- **OSPFv3** 글로벌 타이머 프로파일 - LSA(링크 상태 알림) 간격, SPF 계산 지연, 초기 유지 시간 및 모든 OSPFv3 영역을 적용하는 최대 유지 시간에 대한 타이머를 지정합니다. SPF 제한 설정을 사용하면 네트워크가 불안정한 동안(토폴로지 변경 중) 프로토콜이 LSA 업데이트 전송 속도를 늦출 수 있습니다. 일반 OSPFv3 구성에서 프로파일을 적용합니다. 프로파일은 논리적 라우터의 OSPFv3에 대해 전역적입니다. 둘 이상을 만들어 전역 타이머를 쉽게 변경할 수 있습니다.
- **OSPFv3** 인터페이스 인증 프로파일 - OSPFv3에는 자체 인증 기능이 없으며 IPSec을 사용하여 인접 항목 간의 OSPFv3 메시지를 보호합니다. **OSPFv3** 영역 > 유형 탭에서 프로파일을 적용합니다.
- **OSPFv3** 인터페이스 타이머 프로파일 - 인터페이스 작업과 관련된 타이머(예: OSPFv3 hello 및 정상 재시작)를 지정합니다. 일반 OSPFv3 구성에서 프로파일을 적용합니다.
- **OSPFv3** 재배포 프로파일 - IPv6 정적, 연결된 또는 IPv6 BGP 경로 또는 IPv6 기본 경로를 OSPFv3으로 재배포합니다. 일반 OSPFv3 구성에서 프로파일을 적용합니다.

STEP 1 | OSPFv3 글로벌 타이머 프로파일을 만듭니다.

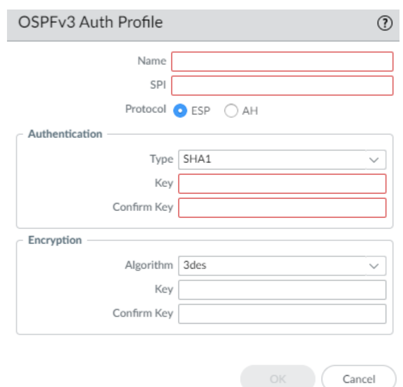
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPFv3**을 선택합니다.
2. 이름으로 **OSPFv3** 글로벌 타이머 프로파일을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 방화벽이 SPF 트리를 다시 계산하는 가장 작은 간격인 **LSA** 최소 도착(초)을 입력합니다. 범위는 1~10이며 기본값은 5입니다. 방화벽은 더 큰 간격(설정보다 덜 빈번함)으로 다시 계산됩니다.
4. SPF 제한 영역에 논리적 라우터가 토폴로지 변경을 수신한 시점부터 SPF(최단 경로 우선) 계산을 수행할 때까지 초기 지연(초)을 입력합니다. 범위는 0~600이며 기본값은 5입니다.
5. 처음 두 개의 연속 SPF 계산 사이의 초기 유지 시간(초)을 입력합니다. 범위는 0~600이며 기본값은 5입니다. 각 후속 보류 시간은 보류 시간이 최대 보류 시간에 도달할 때까지 이전 보류 시간의 두 배입니다.
6. 최대 보류 시간(초)을 입력합니다. 이 값은 유지 시간이 안정적으로 유지될 때까지 증가하는 가장 큰 값입니다. 범위는 0~600이며 기본값은 5입니다.



7. 확인을 클릭합니다.

STEP 2 | OSPFv3 인터페이스 인증 프로파일을 만듭니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPFv3**을 선택합니다.
2. 이름(최대 63자)으로 **OSPFv3** 인증 프로파일을 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.
3. OSPFv3 인접성의 양쪽 끝 간에 일치해야 하는 **SPI**(보안 정책 인덱스)를 입력합니다.
4. 프로토콜을 선택합니다. **ESP**(보안 페이로드 캡슐화)(권장) 또는 **AH**(인증 헤더).
5. 인증 유형을 선택합니다.
   - **SHA1**(기본값) 보안 해시 알고리즘 1.
   - **SHA256**
   - **SHA384**
   - **SHA512**
   - **MD5**
   - 없음
6. 총 40개의 16진수에 대해 8개의 16진수 문자로 구성된 5개의 16진수 섹션을 사용하여 인증 **Key**를 입력합니다(예: A5DEC4DD155A695A8B983AACEAA5A97C6AECB6D1).
7. 동일한 키를 입력하여 키를 확인합니다.



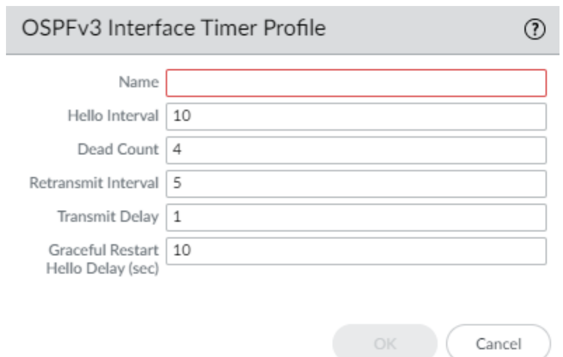
8. (ESP 전용) 암호화 알고리즘을 선택합니다.
   - **3des**(기본값)
   - **aes-128-cbc**
   - **aes-192-cbc**
   - **aes-256-cbc**
   - **null**
9. 암호화 키를 십진수 형식으로 입력합니다. ESP 암호화 유형에 따라 올바른 섹션 수를 사용합니다.
   - **3des** - 키에 총 6개의 16진수 섹션을 사용합니다.
   - **aes-128-cbc** - 키에 총 4개의 16진수 섹션을 사용합니다.
   - **aes-192-bc** - 키에 총 6개의 16진수 섹션을 사용합니다.

- **aes-256-bc** - 키에 총 8개의 16진수 섹션을 사용합니다.

10. 동일한 키를 입력하여 키를 확인합니다.
11. 확인을 클릭합니다.

STEP 3 | OSPFv3 인터페이스 타이머 프로파일을 만듭니다.

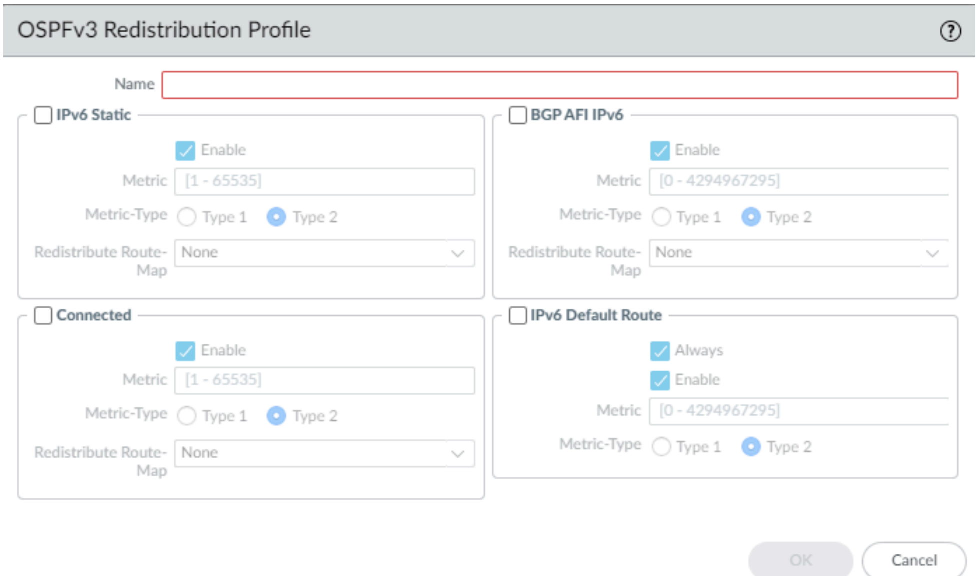
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPFv3**을 선택합니다.
2. 이름으로 **OSPFv3** 인터페이스 타이머 프로파일을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.



3. OSPFv3이 Hello 패킷을 보내는 간격(초)인 **Hello Interval**을 입력합니다. 범위는 1~3,600이며 기본값은 10입니다.
4. OSPFv3이 인접 라우터를 다운한 것으로 간주하기 전에 OSPFv3이 인접 라우터로부터 Hello 패킷을 수신하지 않고 인접 라우터에서 헬로 간격이 발생할 수 있는 횟수인 데드 카운트를 입력합니다. 범위는 3~20이며, 기본값은 4입니다.
5. OSPFv3이 LSA를 재전송하기 전에 OSPFv3이 이웃으로부터 LSA에 대한 ACK를 수신하기 위해 대기하는 시간(초)인 재전송 간격을 입력합니다. 범위는 1 ~ 1,800이며, 기본값은 5입니다.
6. OSPFv3이 LSA를 인터페이스로 보내기 전에 LSA를 전송하는 것을 지연시키는 시간(초)인 전송 지연을 입력합니다. 범위는 1~1,800이며, 기본값은 1입니다.
7. 정상 다시 시작 **hello** 지연**(**초**)**을 초 단위로 입력합니다. 범위는 1~10이며 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. 예를 들어 **Hello Interval**이 10초이고 데드 카운트가 4이면 데드 타이머가 40초가 됩니다. 정상 재시작 **Hello** 지연이 10초로 설정된 경우 Hello 패킷의 10초 지연은 40초 데드 타이머 내에서 편안하게 이루어지므로 인접성은 정상적인 재시작 동안 시간 초과되지 않습니다.
8. 확인을 클릭합니다.

STEP 4 | OSPFv3 재배포 프로파일을 만들어 IPv6 정적 경로, 연결된 경로, IPv6 BGP 경로 및 OSPFv3에 재배포할 기본 IPv6 경로의 조합을 지정합니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **OSPFv3**을 선택합니다.
2. 이름으로 **OSPFv3** 재배포 프로파일을 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.



3. 프로파일의 이 부분 구성을 허용하려면 **IPv6** 정적을 선택합니다.
   - 프로파일의 IPv6 정적 재배포 부분을 사용하도록 설정합니다.
   - OSPFv3에 재배포된 IPv6 정적 경로에 적용할 메트릭을 입력합니다. 범위는 1 ~ 65,535입니다.
   - 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**.
   - 경로 맵 재배포를 선택하거나 일치 기준이 OSPFv3으로 재배포할 IPv6 고정 경로를 제어하는 새 재배포 경로 맵을 생성합니다. 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.
4. 연결됨을 선택하여 프로파일의 이 부분을 구성할 수 있습니다.
   - 프로파일의 연결된 경로 재분배 부분을 활성화합니다.
   - OSPFv3에 재분배된 연결된 경로에 적용할 메트릭을 입력합니다. 범위는 1~65,535입니다.
   - 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**.
   - 경로 맵 재배포를 선택하거나 일치 기준이 OSPFv3으로 재배포할 연결된 경로를 제어하는 새 재배포 경로 맵을 생성합니다. 기본값은 없음입니다. 경로 맵 세트 구성에 Metric Action 및 Metric Value가 포함되어 있으면 재배포 경로에 적용됩니다. 그렇지 않으면 이 재배포 프

로파일에 구성된 지표가 재배포 경로에 적용됩니다. 마찬가지로 경로 맵 세트 구성의 지표 유형은 이 재배포 프로파일에 구성된 지표 유형보다 우선합니다.

5. **BGP AFI IPv6**을 선택하여 프로파일의 이 부분을 구성할 수 있도록 합니다.
    - 프로파일의 BGP AFI IPv6 경로 재배포 부분을 사용하도록 설정합니다.
    - OSPFv3에 재배포된 IPv6 BGP 경로에 적용할 메트릭을 입력합니다. 범위는 0 - 4,294,967,295입니다.
    - 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**.
    - 재배포 경로 맵을 선택하거나 일치 기준이 IPv6 BGP 경로를 제어하여 OSPFv3에 재배포할 새 재배포 경로 맵을 만듭니다. 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.
6. **IPv6** 기본 경로를 선택하여 프로파일의 이 부분을 구성할 수 있도록 합니다.
    - 항상을 선택하여 라우터에 기본 경로가 없는 경우에도 OSPFv3에 대한 기본 경로를 항상 만들고 재배포합니다. 기본값이 활성화됩니다. 항상이 설정되지 않은 경우 ABR에 기본 경로가 없는 경우 기본 경로가 재배포되지 않습니다.
    - 프로파일을 IPv6 기본 경로 재배포 부분으로 사용하도록 설정합니다.
    - OSPFv3에 재배포된 IPv6 기본 경로에 적용할 메트릭을 입력합니다. 범위는 0~4,294,967,295입니다.
    - 메트릭 유형을 선택합니다. 유형 **1** 또는 유형 **2**.
7. 확인을 클릭합니다.

STEP 5 | 커밋합니다.

고급 라우팅 엔진에서 RIPv2 구성

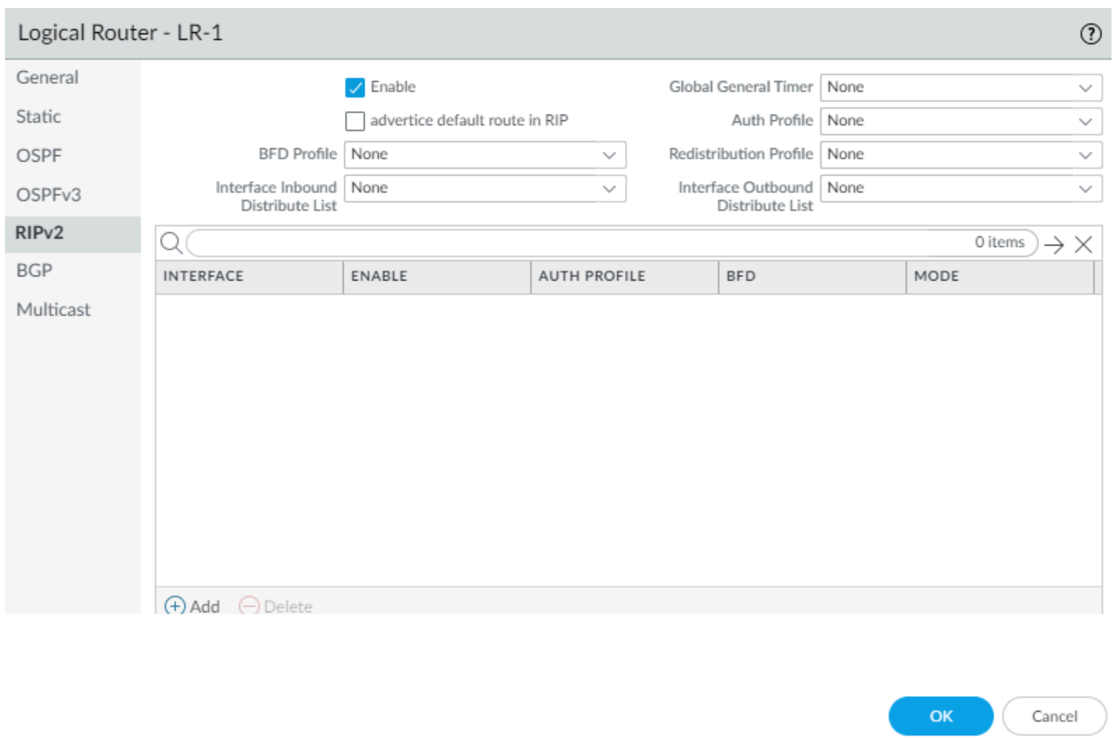
고급 라우팅 엔진은 RIPv2를 지원합니다.

RIPv2에 적용할 수 있는 RIPv2 라우팅 프로파일 및 필터를 고려하여 구성 시간을 절약하고 일관성을 유지합니다. 프로파일과 필터를 미리 만들거나 RIPv2를 구성할 때 만들 수 있습니다.

STEP 1 | 논리 라우터 구성.

STEP 2 | RIPv2를 사용하도록 설정하고 일반 설정을 구성합니다.

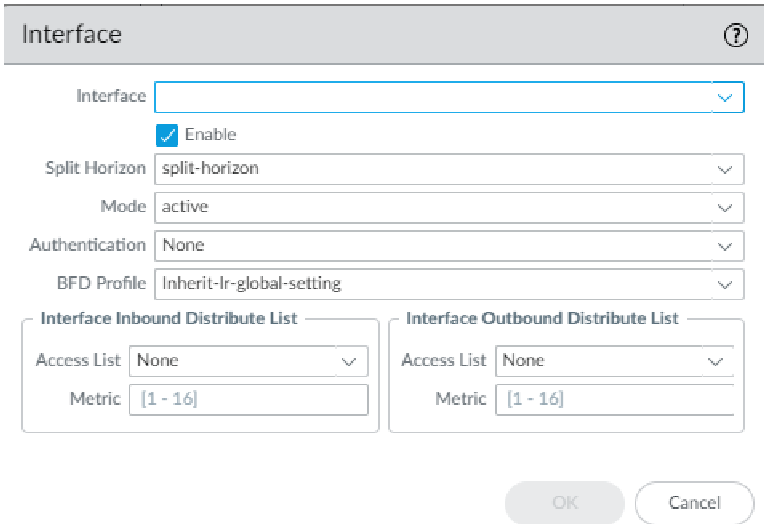
1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **RIPv2**를 선택하고 사용하도록 설정합니다.



3. **RIP**에서 기본 경로 광고를 선택하여 라우팅 엔진의 RIB에 없는 경우에도 기본 경로를 광고합니다.을 수행했습니다.
4. BFD를 RIPv2에 적용하려면 생성한 **BFD** 프로파일을 선택하거나 기본 프로파일을 선택하거나 새 BFD 프로파일을 생성합니다. 기본값은 없음**(BFD** 비활성화**)**입니다.
5. 전역 일반 타이머를 선택하거나 새 RIPv2 전역 타이머 프로파일을만듭니다.
6. 인증 프로파일을 선택하거나 새 RIPv2 인증 프로파일을 생성합니다.
7. 재배포 프로파일을 선택하거나 새 재배포 프로파일을 만들어 IPv4 정적 경로, 연결된 경로, BGP IPv4 경로 또는 OSPFv2 경로를 RIPv2에 재배포 합니다.
8. 전역 인바운드 배포 목록을 선택하여 허용되는 수신 경로를 제어합니다.
9. 전역 아웃바운드 배포 목록을 선택하여 RIP 인접 라우터에 광고되는 경로를 제어합니다.

STEP 3 | RIPv2에 대한 인터페이스를 구성합니다.

1. 하나를 선택하여 인터페이스를 추가하고 활성화합니다.



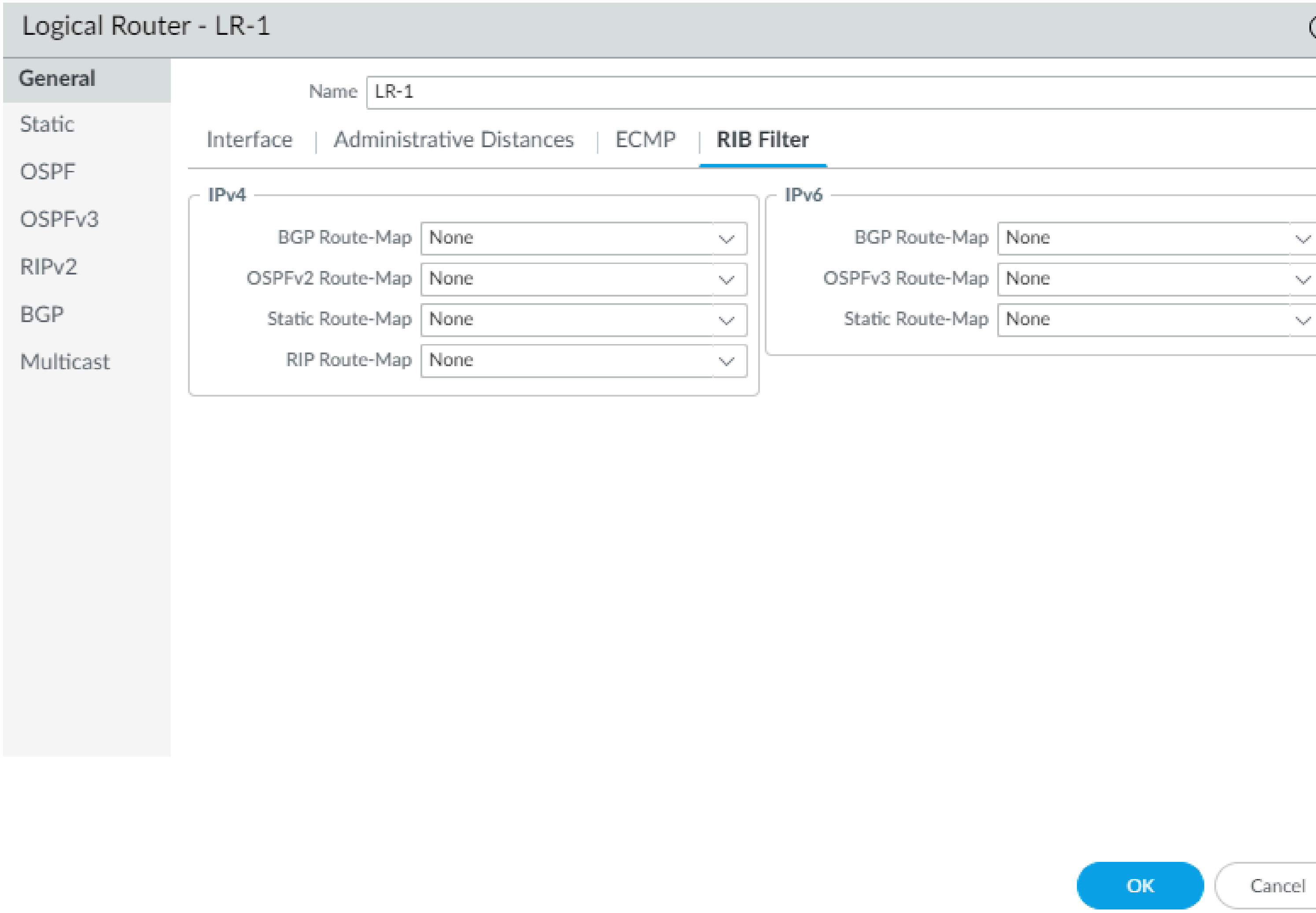
2. 수평 분할에 대해 다음 중 하나를 선택합니다.
   - **split-horizon** - 경로가 수신된 동일한 인터페이스에서 경로를 다시 알리지 않습니다.
   - **no-split-horizon** - 분할 수평선을 사용하지 않도록 설정합니다.
   - **no-split-horizon-with-poison-reverse** - 광고가 수신된 동일한 인터페이스에서 광고를 다시 허용하고 이러한 경로에 대한 메트릭을 RIP에 허용되는 최대값(16)으로 설정합니다.
3. 모드를 선택합니다.
   - **active** - 인터페이스가 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.
4. 논리적 라우터 수준에서 적용한 프로파일을 재정의하려면 인증 프로파일을 선택합니다.
5. 기본적으로 인터페이스는 RIPv2(**Inherit-lr-global-setting**)용 논리적 라우터에 적용한 BFD 프로파일을 상속합니다. 또는 다른 **BFD** 프로파일을 선택하거나, 새 BFD 프로파일을 생성하거나, 없음**(BFD** 비활성화**)**을 선택하여 인터페이스에 대한 BFD를 비활성화합니다.
6. 인터페이스 인바운드 배포 목록의 경우 액세스 목록을 선택하여 이 인터페이스로 오는 경로를 제어합니다.
7. 들어오는 경로에 적용되는 메트릭을 지정합니다. 범위는 1에서 16까지입니다.
8. 인터페이스 아웃바운드 배포 목록에서 액세스 목록을 선택하여 이 인터페이스에서 RIP 인접 라우터에 광고된 경로를 제어합니다.
9. 광고된 경로에 적용할 메트릭을 지정합니다. 범위는 1에서 16까지입니다.
10. 확인을 클릭합니다.

STEP 4 | 확인을 클릭합니다.

STEP 5 | (선택 사항) 전역 RIB에 배치되는 RIP 경로를 제어합니다.

경로를 학습하고 재배포하지만 프로토콜의 로컬 라우팅 테이블이나 전역 RIB에서는 경로를 원하지 않을 수 있습니다. 전역 RIB에 특정 경로만 추가할 수 있습니다.

1. 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.
2. **RIB** 필터를 선택하여 루트가 전역 RIB에 추가되는 것을 허용하거나 루트가 추가되지 않도록 합니다.



3. RIB로 가는 RIPv2 경로를 필터링하려면 IPv4 영역에서 **RIP Route-Map**에 대해 재배포 경로 맵을 선택하거나 새 경로 맵을 생성합니다.
4. 확인을 클릭합니다.

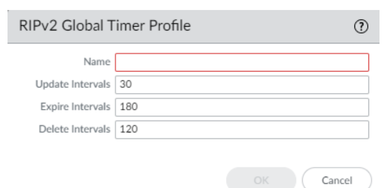
RIPv2 라우팅 프로파일 만들기

고급 라우팅 엔진은 RIPv2를 지원합니다. 프로토콜에 적용할 다음 프로파일을 만듭니다. 프로파일은 여러 논리적 라우터와 가상 시스템에서 사용할 수 있습니다. 이 항목에서는 프로파일과 프로파일의 구성 방법에 대해 설명합니다.

- **RIPv2** 글로벌 타이머 프로파일 - RIPv2 업데이트, 만료 및 삭제 간격을 지정합니다. RIPv2 일반 구성에서 프로파일을 적용합니다.
- **RIPv2** 인터페이스 인증 프로파일 - 암호 또는 MD5를 사용하여 RIPv2 인증을 지정합니다. RIPv2 일반 구성에 프로파일을 적용합니다.
- **RIPv2** 재배포 프로파일 - IPv4 정적 경로, 연결된 경로, BGP IPv4 경로 및 OSPFv2 경로를 RIPv2로 재배포하는 방법을 지정합니다. RIPv2 일반 구성에서 프로파일을 적용합니다.

STEP 1 | RIPv2 글로벌 타이머 프로파일을 만듭니다.

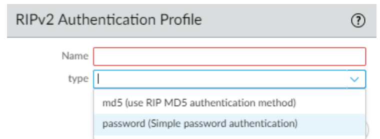
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **RIPv2**를 선택합니다.
2. 이름으로 **RIPv2** 글로벌 타이머 프로파일을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 허용되지 않습니다.



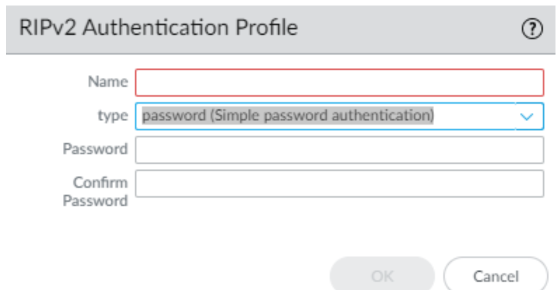
3. 정기적으로 예약된 업데이트 메시지 사이의 시간인 업데이트 간격(초)을 지정합니다. 범위는 5~2,147,483,647이며 기본값은 30입니다.
4. 만료 간격(초)을 지정합니다. 즉, 경로를 업데이트하지 않고 라우팅 테이블에 포함할 수 있는 시간의 길이입니다. 범위는 5 - 2,147,483,647이며 기본값은 180입니다. 만료 간격에 도달한 후에도 삭제 간격에 도달할 때까지 경로는 업데이트 메시지에 계속 포함됩니다.
5. 삭제 간격(초)을 지정하고, 범위는 5~2,147,483,647이며, 기본값은 120입니다. 라우팅 테이블에서 만료된 경로가 삭제 간격에 도달하면 라우팅 테이블에서 삭제됩니다.
6. 확인을 클릭합니다.

STEP 2 | RIPv2 인증 프로파일을 만듭니다.

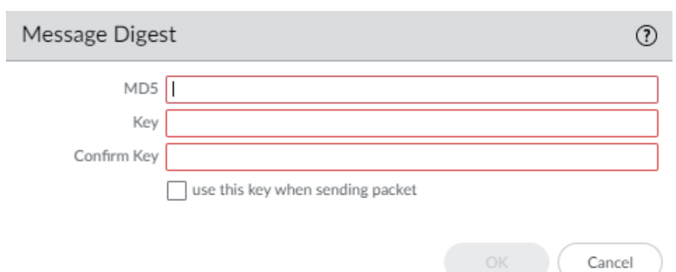
1. 네트워크 > 라우팅 > 라우팅 프로파일 > **RIPv2**를 선택합니다.
2. 이름으로 **RIPv2** 인증 프로파일을 추가합니다(최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.



3. 유형 인증: **md5(RIP MD5** 인증 방법 사용**)** 또는 암호**(**단순 암호 인증**)**를 지정합니다.
4. 간단한 비밀번호 인증의 경우 비밀번호(최대 16자)와 비밀번호 확인을 입력합니다.



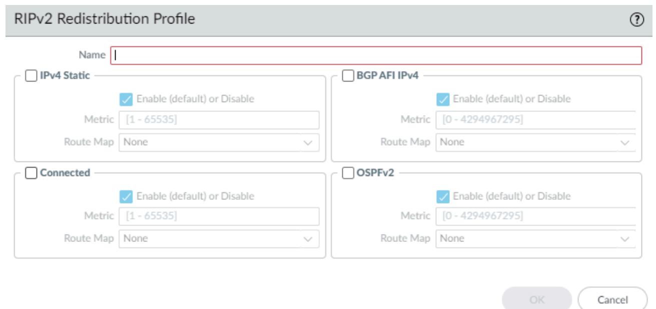
5. **RIP MD5** 인증의 경우:
   - MD5 키-ID를 추가합니다. 범위는 0에서 255까지입니다.
   - 키(영숫자 최대 16자) 및 키 확인을 입력합니다.
   - 이 키를 기본 키로 설정하려면 패킷을 보낼 때 이 키 사용을 선택합니다.



6. 확인을 클릭합니다.

STEP 3 | RIPv2 재배포 프로파일을 만들어 RIPv2에 재배포할 IPv4 정적 경로, 연결된 경로, BGP IPv4 경로 및 OSPFv2 경로의 조합을 지정합니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > **RIPv2**를 선택합니다.
2. 이름으로 **RIPv2** 재배포 프로파일을 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.



3. 프로파일의 이 부분을 구성할 수 있도록 하려면 **IPv4 Static**을 선택합니다.
   - 프로파일의 IPv4 정적 재배포 부분을 사용하도록 설정합니다.
   - RIPv2로 재분배되는 정적 경로에 적용할 메트릭을 지정합니다(범위는 1 - 65,535).
   - 경로 맵 재배포를 선택하거나 일치 기준이 RIPv2로 재배포할 IPv4 고정 경로를 제어하는 새 재배포 경로 맵을 생성합니다. 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.

4. 연결됨을 선택하여 프로파일의 이 부분을 구성할 수 있습니다.
   - 프로파일의 연결된 경로 재분배 부분을 활성화합니다.
   - RIPv2로 재분배되는 연결된 경로에 적용할 메트릭을 지정합니다(범위는 1 - 65,535).
   - 경로 맵 재배포 또는 새 재배포 경로 맵 생성을 선택합니다. 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.
5. 프로파일의 이 부분에 대한 구성을 허용하려면 **BGP AFI IPv4**를 선택합니다.
   - 프로파일의 BGP IPv4 경로 재배포 부분을 사용하도록 설정합니다.
   - RIPv2로 재분배되는 BGP 경로에 적용할 메트릭을 지정합니다(범위는 0 - 4,294,967,295).
   - 경로 맵 재배포 또는 새 재배포 경로 맵 생성을 선택합니다. 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.
6. **OSPFv2**를 선택하여 프로파일의 이 부분을 구성할 수 있도록 합니다.
   - 프로파일의 OSPFv2 경로 재배포 부분을 사용하도록 설정합니다.
   - 프로파일의 IPv4 기본 경로 재배포 부분을 사용하도록 설정합니다.
   - RIPv2로 재분배되는 기본 경로에 적용할 메트릭을 지정합니다(범위는 0 - 4,294,967,295).
   - 경로 맵 재배포 또는 새 재배포 경로 맵 생성을 선택합니다. 기본값은 없음입니다. 경로 맵 집합 구성에 메트릭 작업 및 메트릭 값이 포함된 경우 재배포된 경로에 적용됩니다. 그렇지 않으면 이 재배포 프로파일에 구성된 지표가 재배포 경로에 적용됩니다.
7. 확인을 클릭합니다.

BFD 프로파일 만들기

고급 라우팅 엔진에서는 BFD(양방향 전달 감지) 프로파일을 사용하여 정적 경로 또는 라우팅 프로토콜에 BFD 설정을 쉽게 적용할 수 있습니다. 기본 프로파일(읽기 전용) 을 사용하거나 새 BFD 프로파일을 만들 수 있습니다.

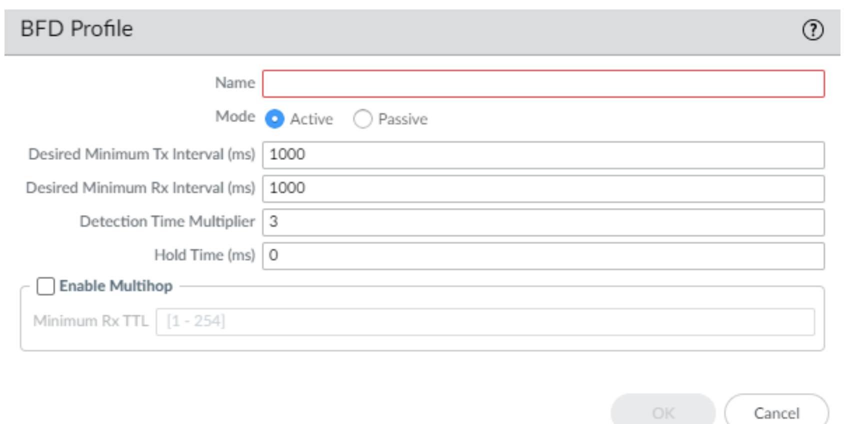
BFD 프로파일을 만들기 전에 다음을 수행합니다.

- 논리 라우터 구성.
- 정적 경로에 BFD를 적용하는 경우 하나 이상의 정적 경로를 구성합니다.
- 라우팅 프로토콜에 BFD를 적용하는 경우 라우팅 프로토콜(**BGP**, **OSPF, OSPFv3** 또는 **RIPv2**)을 구성합니다. 예를 들어 일반 BGP 설정을 구성할 때 BFD 프로파일을 적용할 수 있습니다.

BFD 구현의 효과는 트래픽 로드, 네트워크 상태, *BFD* 설정이 얼마나 공격적인지, 데이터플레인의 사용량과 같은 다양한 요인에 따라 달라집니다.

STEP 1 | 네트워크 > 라우팅 > 라우팅 프로파일 > **BFD**를 선택합니다.

STEP 2 | 이름으로 BFD 프로파일을 추가합니다(최대 63자). 이름은 대소문자를 구분하며 방화벽에서 고유해야 합니다. 문자, 숫자, 하이픈 및 밑줄만 사용합니다. 점(.) 또는 공백은 사용할 수 없습니다.



STEP 3 | BFD가 작동하는 모드를 선택합니다.

- 활성 - BFD가 제어 패킷을 피어로 보내기 시작합니다(기본값). BFD 피어 중 하나 이상은 활성 상태여야 합니다. 둘 다 활성일 수 있습니다.
- 수동 - BFD는 피어가 제어 패킷을 보낼 때까지 기다렸다가 필요에 따라 응답합니다.

STEP 4 | BFD 프로토콜이 BFD 제어 패킷을 전송할 최소 간격인 원하는 최소 **Tx** 간격**(ms)**을 입력합니다. 따라서 피어와 전송 간격을 협상합니다. PA-7000 시리즈, PA-5200 시리즈 및 PA-5450 방화벽

의 범위는 50~10,000이고 PA-3200 시리즈의 범위는 100~10,000이며 VM 시리즈의 범위는 200~10,000입니다. 기본값은 1,000입니다.

동일한 인터페이스에서 다른 *BFD* 프로파일을 사용하는 여러 라우팅 프로토콜이 있는 경우 동일한 원하는 최소 *Tx* 간격으로 *BFD* 프로파일을 구성합니다.

PA-7000 시리즈 방화벽에서 원하는 최소 *Tx* 간격을 *100* 이상으로 설정합니다. 값이 *100*보다 작으면 *BFD* 플랩이 발생할 위험이 있습니다.

STEP 5 | 필요한 최소 수신 간격**(ms)**을 입력합니다. 이것은 BFD가 BFD 제어 패킷을 수신할 수 있는 최소 간격(밀리초)입니다. PA-7000 시리즈, PA-5200 시리즈 및 PA-5450 방화벽의 범위는 50~10,000이고 PA-3200 시리즈의 범위는 100~10,000이며 VM 시리즈의 범위는 200~10,000입니다. 기본값은 1,000입니다.

PA-7000 시리즈 방화벽에서 원하는 최소 수신 간격을 *100* 이상으로 설정합니다. 값이 *100*보다 작으면 *BFD* 플랩이 발생할 위험이 있습니다.

STEP 6 | 감지 시간 승수를 입력합니다. 범위는 2에서 255까지이며 기본값은 3입니다.

로컬 시스템은 원격 시스템에서 수신한 감지 시간 승수에 원격 시스템의 합의된 전송 간격을 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 프로파일을 만들 때 방화벽은 일반적으로 네트워크 또는 데이터 센터의 가장자리에 있는 세션 기반 디바이스이며 전용 라우터보다 링크 속도가 느릴 수 있다는 점을 고려합니다. 따라서 방화벽은 허용되는 가장 빠른 설정보다 더 긴 간격과 더 높은 승수가 필요할 수 있습니다. 감지 시간이 너무 짧으면 문제가 단순히 트래픽 정체인 경우 잘못된 오류 감지가 발생할 수 있습니다.

STEP 7 | BFD가 BFD 제어 패킷을 전송하기 전에 링크가 시작된 후 지연 시간(밀리초)인 보류 시간**(ms)** 을 입력합니다. 홀드 타임은 BFD **Active** 모드에만 적용됩니다. BFD는 홀드 타임 동안 BFD 제어 패킷을 수신하면 이를 무시합니다. 범위는 0에서 120,000까지입니다. 기본값은 0이며 이는 전송 보류 시간이 사용되지 않음을 의미합니다. BFD는 링크가 설정된 직후 BFD 제어 패킷을 보내고 받습니다.

STEP 8 | BGP가 멀티홉 BFD를 지원할 때 BFD가 BFD 제어 패킷에서 수락(수신) 하는 최소 Rx TTL인 최소 **Rx TTL**을 입력합니다. 범위는 1~254이고 기본값은 없습니다.

방화벽은 구성된 최소 **Rx TTL**보다 작은 TTL을 수신하는 경우 패킷을 삭제합니다. 예를 들어 피어가 5홉 떨어져 있고 피어가 TTL이 100인 BFD 패킷을 방화벽으로 전송하고 방화벽의 최소 **Rx TTL**이 96 이상으로 설정된 경우 방화벽은 패킷을 삭제합니다.

STEP 9 | 확인을 클릭합니다.

IPv4 멀티캐스트 구성

고급 라우팅 엔진은 논리적 라우터에 대해 IPv4 멀티캐스트를 지원합니다. IP 멀티캐스트, IGMP 및 PIM의 개념을 이해하고 있어야 합니다.

고급 라우팅 엔진의 IPv4 멀티캐스트는 레거시 라우팅 엔진에서 지원되지 않는 기능을 지원합니다.

- 인터페이스에서 정적 IGMPv3 또는 IGMPv2 수신기를 지정하는 기능인 IGMP 정적 조인입니다. 해당 PIM Join 메시지가 업스트림으로 전송됩니다.
- PIM(Protocol Independent Multicast)은 RPF(Reverse-Path Forwarding) 조회 모드를 지원합니다. MRIB만, URIB만 및 MRIB-the-URIB.

IPv4 멀티캐스트는 IGMPv1을 지원하지 않습니다.

IPv4 멀티캐스트를 구성할 때 구성을 더 쉽고 일관성 있게 만들기 위해 PIM 인터페이스 타이머 및 IGMP 인터페이스 쿼리에 대해 멀티캐스트 라우팅 프로파일 생성을(를) 수행합니다. 멀티캐스트 경로 맵을 생성하여 PIM 그룹 권한을 제어할 수 있습니다.

유니캐스트 트래픽이 멀티캐스트 트래픽과 다른 경로를 사용하도록 하려면 IPv4 MRoute 생성을(를) 수행할 수도 있습니다.

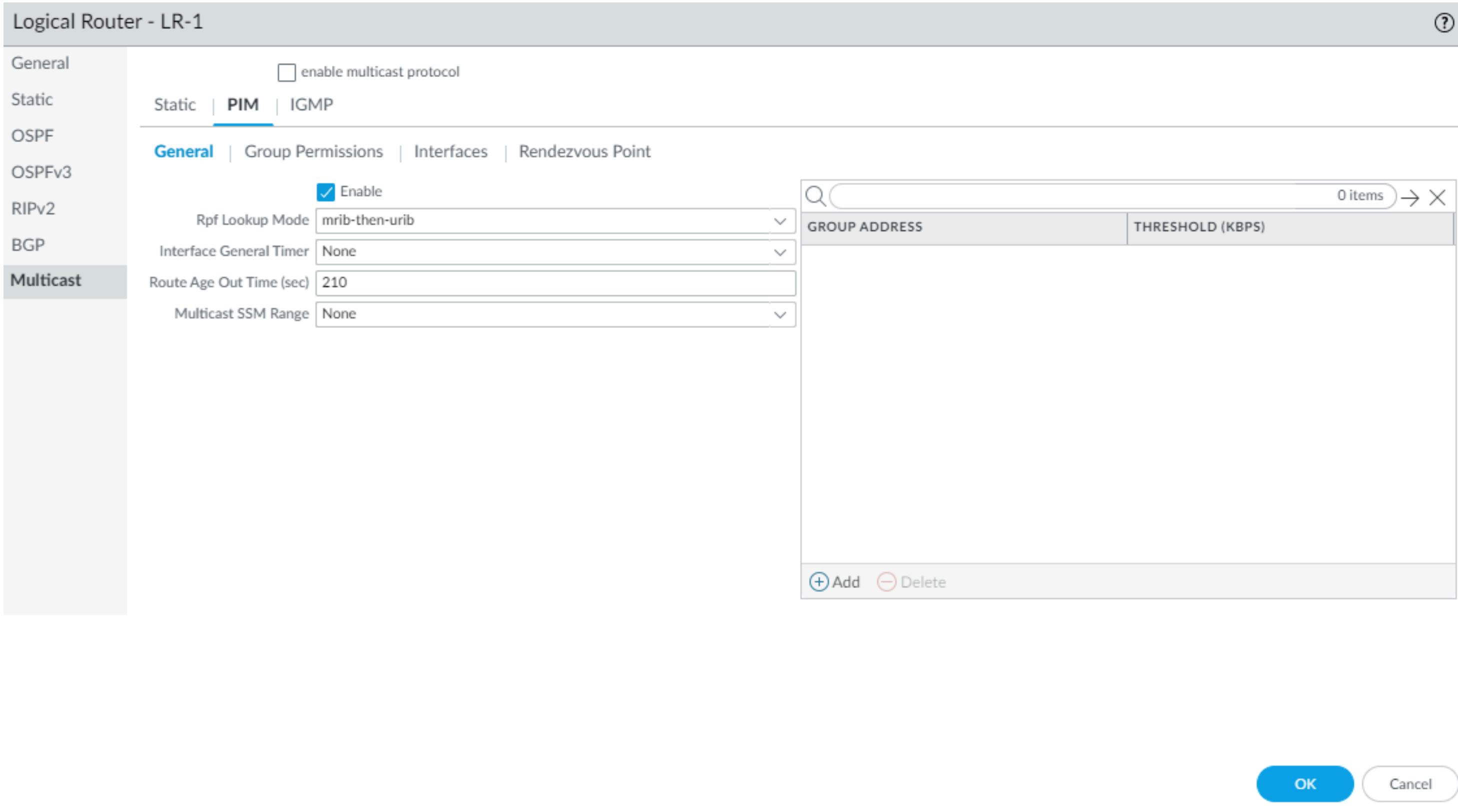
STEP 1 | 논리 라우터 구성.

STEP 2 | 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.

STEP 3 | 멀티캐스트를 선택하고 멀티캐스트 프로토콜을 활성화합니다.

STEP 4 | 논리적 라우터에 대한 일반 PIM 매개변수를 구성합니다.

1. **PIM** > 일반을 선택하고 PIM을 활성화합니다.



2. 논리적 라우터가 멀티캐스트 패킷에 포함된 소스 주소에 도달하기 위해 나가는 인터페이스를 찾기 위해 찾는 위치를 결정하는 **RPF** 조회 모드를 선택합니다. RIB에 저장된 발신 인터페이스가 멀티캐스트 패킷이 도착한 인터페이스와 일치하면 논리적 라우터는 패킷을 수락하고 전달합니다. 그렇지 않으면 패킷이 삭제됩니다.

   - **mrib-only** - 멀티캐스트 RIB만 찾습니다.
   - **mrib-then-urib** - 먼저 멀티캐스트 RIB를 찾습니다. 멀티캐스트 RIB에 경로가 없으면 유니캐스트 RIB에서 찾습니다.

- **urib-only** - 유니캐스트 RIB에서만 찾습니다.

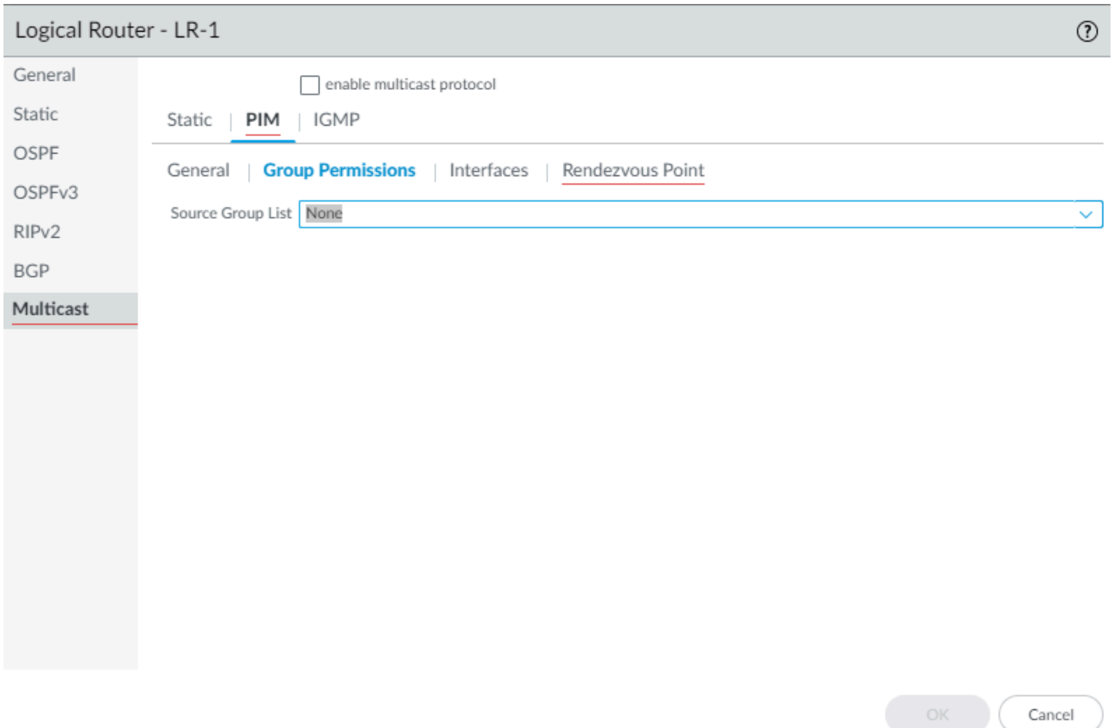
RPF 조회 모드는 PIM 조인에 사용할 경로를 선택하기 위해 경로 조회를 수행할 위치도 제어합니다.

3. 인터페이스 일반 타이머의 경우 PIM 인터페이스 타이머 프로파일을 선택하거나 새 IPv4 PIM 인터페이스 타이머 프로파일을 생성합니다. 기본값은 없음입니다.
4. **Route Age Out Time(**초**)** 지정 - 멀티캐스트 그룹과 소스 사이의 세션이 종료된 후 멀티캐스트 경로가 mRIB에 남아 있는 시간(초)입니다. 범위는 210~7,200입니다. 기본값은 210입니다.
5. SSM(Source-Specific Multicast)을 구성하려면 **Multicast SSM Range**에서 멀티캐스트 트래픽을 수신자에게 전달할 수 있도록 허용된 소스 주소를 지정하는 접두사 목록을 선택(또는 새로 생성)합니다. 기본값은 없음**(**접두사 목록 없음**)**입니다.
6. 멀티캐스트 그룹 또는 접두사에 대한 최단 경로 트리(SPT) 임계값을 구성하려면 접두사 목록을 선택하거나 새로 생성하여 그룹 주소(배포 트리를 지정하는 멀티캐스트 그룹 또는 접두사)를 추가합니다.
7. 임계값 속도를 초당 킬로비트(kbps)로 지정합니다. 멀티캐스트 그룹/접두사에 대한 멀티캐스트 트래픽이 이 임계값보다 빠르게 논리적 라우터에 도달하면 지정된 그룹/접두사로 라우팅이 공유 트리(Rendezvous Point[RP]에서 제공됨)에서 SPT 배포로 전환됩니다.
   - **0(**첫 번째 데이터 패킷 켜기**)**(기본값) - 논리 라우터가 그룹/접두사에 대한 첫 번째 데이터 패킷을 수신하면 논리 라우터가 공유 트리에서 그룹/접두사에 대한 SPT로 전환합니다.
   - 논리적 라우터가 해당 멀티캐스트 그룹 또는 접두사에 대한 SPT 배포로 전환되는 모든 인터페이스 및 기간 동안 멀티캐스트 그룹/접두사에 대해 도달할 수 있는 초당 총 킬로비트 수를 입력합니다. 범위는 0~4,294,967,295입니다.
   - 안 함**(spt**로 전환하지 않음**)** - PIM 라우터는 계속해서 공유 트리를 사용하여 패킷을 멀티캐스트 그룹/접두사로 전달합니다.

STEP 5 | PIM 그룹 권한을 지정하여 논리적 라우터가 수락하는 PIM Join 메시지 및 Register 메시지와 논리적 라우터가 전달하는 멀티캐스트 트래픽을 제어합니다.

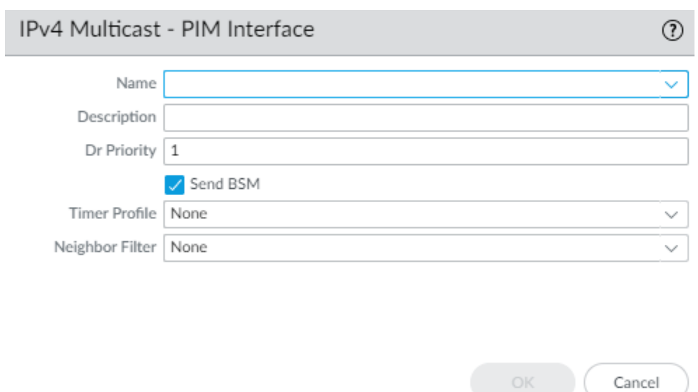
1. **PIM** > 그룹 권한을 선택합니다.
2. 논리적 라우터를 전송하기 위해 특정 소스(S,G)에서 특정 대상 멀티캐스트 그룹에 대한 패킷을 제어하려면 소스 그룹 목록에 대해 생성한 액세스 목록을 선택하거나 새로 생성합니다. 액세스

목록은 소스가 멀티캐스트 소스를 지정하고 대상이 멀티캐스트 그룹을 지정하는 확장 액세스 목록일 수 있습니다. 기본값은 없음(액세스 목록 없음)입니다.



STEP 6 | 인터페이스에 대한 PIM 특성을 구성합니다.

1. **PIM** > 인터페이스를 선택하고 이름으로 인터페이스 추가를 선택합니다.



2. 인터페이스에 대한 유용한 설명을 입력합니다.
3. 인터페이스의 **DR** 우선 순위(지정된 라우터 우선 순위)를 지정하여 어떤 라우터가 PIM Join 메시지, PIM Register 메시지 및 Prune 메시지를 Rendezvous Point(RP)로 전달할지 제어합니다.

범위는 1에서 4,294,967,295입니다. 기본값은 1입니다. LAN상의 PIM 디바이스들 중에서, DR 우선순위가 구성되면, 가장 높은 우선순위 값을 갖는 디바이스가 DR을 선택합니다.

4. **BSM**을 전송하여 부트스트랩 메시지 전파를 허용합니다(기본적으로 활성화됨).

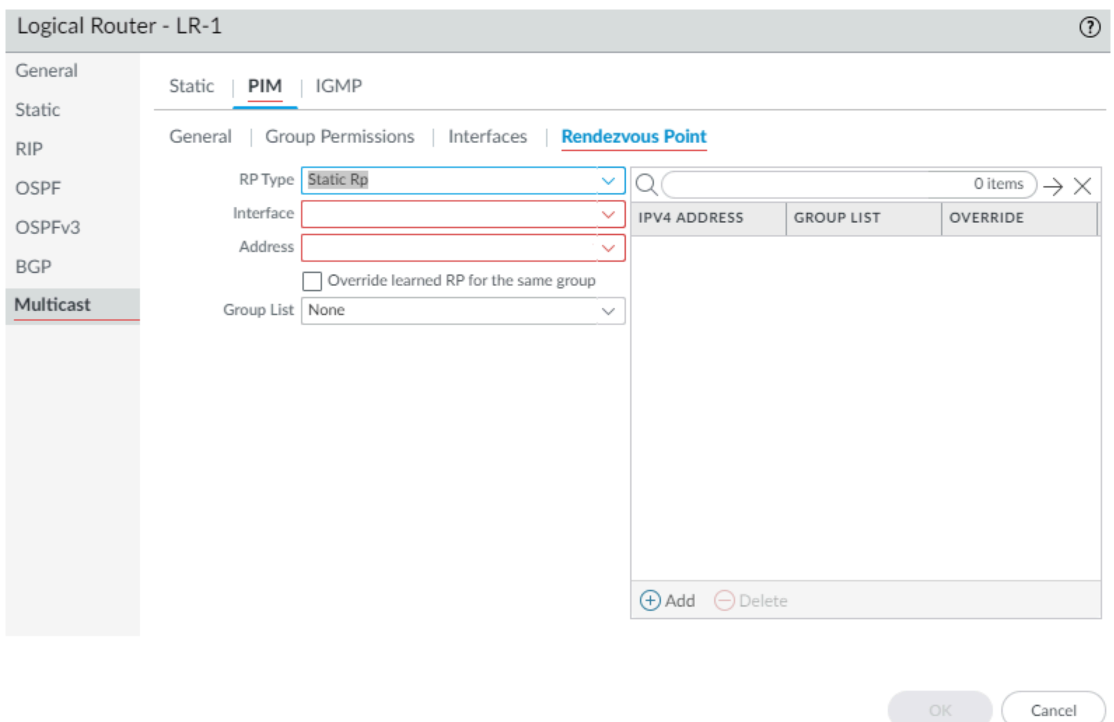
   고급 라우팅 엔진은 ***BSR*** 역할을 할 수 없지만 ***BSM*** 메시지를 보내고 릴레이할 수 있습니다**.**

5. 인터페이스에 대한 타이머 프로파일은 IPv4 PIM 인터페이스 타이머 프로파일을 선택하여 재정의하지 않는 한 일반 PIM 섹션에서 상속됩니다. 기본값은 없음입니다.
6. 생성한 액세스 목록을 사용하여 **Neighbor Filter**를 지정하거나 새 액세스 목록을 생성하여 논리적 라우터의 PIM 이웃이 되는 것이 허용되거나 거부되는 디바이스의 접두사를 지정합니다.
7. 확인을 클릭합니다.

STEP 7 | (ASM 전용) ASM(Any-Source Multicast) 환경에 대한 PIM RP(Rendezvous Point)를 구성합니다.

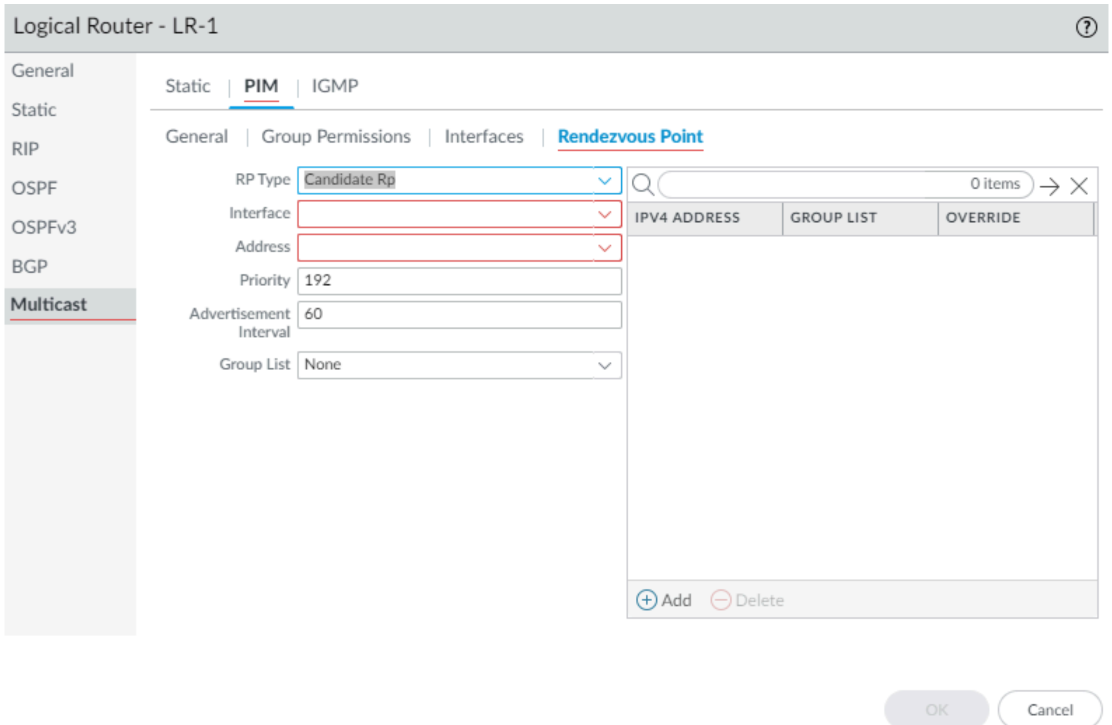
> 후보 *RP*와 정적 *RP*를 구성할 수 있습니다. 그들은 상호 배타적이지 않습니다.

1. **PIM** > 랑데뷰 포인트를 선택합니다.
2. 로컬 **RP** 유형 선택: 정적 **RP** 또는 후보 **RP**입니다. 기본값은 없음입니다.
3. 정적 **RP**를 선택하면 멀티캐스트 그룹에 대한 RP의 정적 매ping이 설정됩니다. PIM 도메인의 다른 PIM 라우터에서 동일한 RP를 명시적으로 구성해야 합니다. 다음을 구성합니다.
   - RP가 멀티캐스트 패킷을 송수신하는 RP 인터페이스를 선택합니다. 유효한 인터페이스 유형은 Layer3 인터페이스(이더넷, VLAN, 루프백, 통합 이더넷(AE), 터널 및 하위 인터페이스 포함)입니다.
   - 인터페이스의 주소를 선택합니다. 선택한 인터페이스의 IP 주소가 목록을 채웁니다.
   - 이 정적 RP가 그룹 목록의 그룹에 대해 선택된 RP 대신 RP 역할을 하도록 동일한 그룹에 대해 학습된 **RP** 재정의를 선택합니다.
   - 액세스 목록을 선택하거나 새 액세스 목록을 만들어 정적 RP가 RP 역할을 하는 멀티캐스트 그룹의 그룹 목록을 지정합니다. 기본값은 없음(액세스 목록 없음)입니다.



4. 후보 **RP**를 선택하는 경우:
   - 후보 RP가 멀티캐스트 패킷을 송수신하는 인터페이스를 선택합니다. 유효한 인터페이스 유형은 Layer3 인터페이스(이더넷, VLAN, 루프백, 통합 이더넷(AE), 터널 및 하위 인터페이스 포함)입니다.
   - 인터페이스의 주소를 선택합니다.

- 후보 RP의 우선 순위를 지정합니다. 범위는 0에서 255 사이입니다. 기본값은 192입니다. 낮은 우선 순위 값은 높은 우선 순위를 나타냅니다.
- 보 RP가 다른 라우터에 광고를 보내는 빈도(초)인 광고 간격을 지정합니다. 범위는 1 ~ 26,214입니다. 기본값은 60입니다.
- 후보 RP가 수락하는 그룹을 제어하려면 생성한 IPv4 액세스 목록인 그룹 목록을 선택하거나 새 액세스 목록을 생성합니다. 기본값은 없음**(**액세스 목록 없음**)**입니다. 액세스 목록이 적용되지 않으면 논리적 라우터가 모든 그룹에 대한 RP로 자신을 알리기 시작합니다.

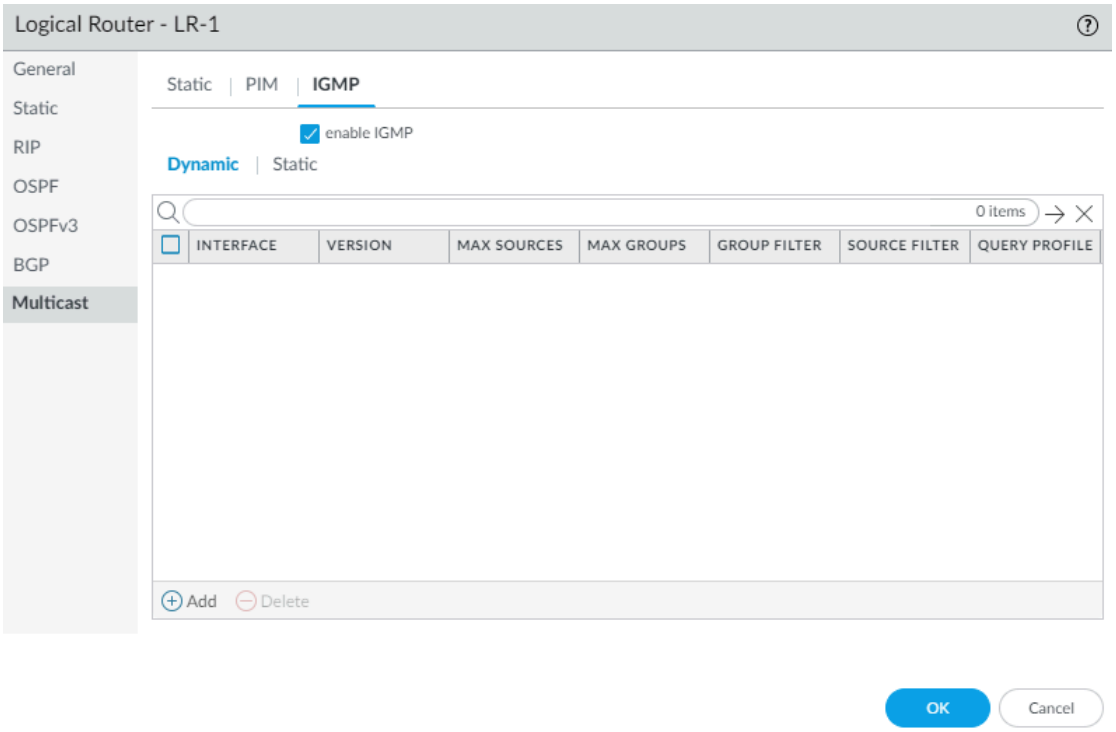


5. 원격(외부) RP의 **IPv4** 주소를 추가합니다.
6. 그룹 목록을 선택하여 원격 RP가 RP 역할을 하는 멀티캐스트 그룹을 지정하거나 새 액세스 목록을 만듭니다. 기본값은 없음**(**액세스 목록 없음**)**입니다.
7. 그룹 목록의 그룹에 대해 동적으로 학습(선택)되는 RP 대신 정적으로 구성한 원격 RP를 RP로 사용하려면 재정의를 선택합니다.
8. 확인을 클릭합니다.

STEP 8 | 확인을 클릭하여 PIM 설정을 저장합니다.

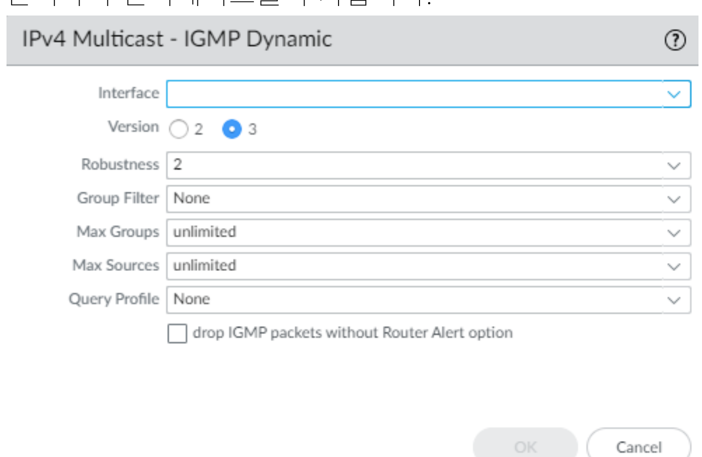
STEP 9 | 멀티캐스트 수신기와 마주하는 인터페이스에서 IGMP를 구성합니다.

1. IGMP를 선택하고 **IGMP**를 활성화합니다.



2. 동적 IGMP 인터페이스를 구성하려면 동적을 선택합니다.

   1. 목록에서 하나를 선택하여 인터페이스를 추가합니다.



   2. IGMP 버전 선택: **2** 또는 **3**.

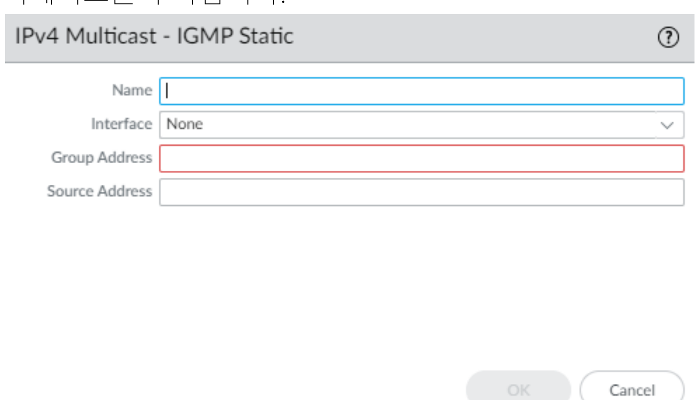
   3. 1에서 7 사이의 견고성 값을 선택합니다. 기본값은 2입니다.

*(Robustness * QueryInterval) + MaxQueryResponseTime*은 논리적 라우터에서 *Join* 메시지가 유효한 기간을 결정합니다. 논리적 라우터가 그룹 나가기 메시지를 수신하는 경우 *Robustness * LastMemberQueryInterval*은 논리적 라우터가 그룹 나가기 항목을 삭제하기 전에 대기하는 시간입니다. 이 논리적 라우터가 있는 서브넷에서 패킷이 손실되기 쉬운 경우 견고성 값을 늘립니다. 조인 메시지의 경우 *Robustness* 값 *1*이 무시됩니다. 그룹 나가기 메시지의 경우 논리적 라우터는 *Robustness* 값을 마지막 멤버 쿼리 수로도 사용합니다.

4. 그룹 필터의 경우 인터페이스가 IGMP 조인을 수락할 소스 및 그룹을 제어하기 위해 액세스 목록을 선택하거나 새 액세스 목록을 생성합니다. 기본값은 없음(액세스 목록 없음)입니다.
5. **Max Groups**에 IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 그룹 수를 입력합니다. 범위는 1~65,535입니다. 기본값은 범위에서 가장 높은 값을 의미하는 무제한입니다.
6. **Max Sources**에 IGMP가 인터페이스에 대해 동시에 처리할 수 있는 최대 소스 수를 입력합니다. 범위는 1~65,535입니다. 기본값은 범위에서 가장 높은 값을 의미하는 무제한입니다.
7. 쿼리 프로파일의 경우 생성한 IGMP 인터페이스 쿼리 프로파일을 선택하거나 인터페이스에 적용할 새 프로파일을 생성합니다. 기본값은 없음입니다.
8. 수신 IGMPv2 또는 IGMPv3 패킷에 IP 라우터 경고 옵션(RFC 2113)이 있어야 하려면 라우터 경고 없이 **IGMP** 패킷 삭제 옵션을 선택합니다. 그렇지 않으면 삭제됩니다. (기본값은 비활성화되어 있습니다.)
9. 확인을 클릭하여 동적 IGMP 인터페이스를 저장합니다.

3. 정적 IGMP 인터페이스를 구성하려면 정적을 선택합니다.

1. 이름으로 정적 인터페이스를 추가합니다.



2. 인터페이스를 정적 IGMP 인터페이스로 선택합니다.
3. 정적 IGMP 구성원의 멀티캐스트 그룹 주소를 입력합니다.
4. 멀티캐스트 그룹(S,G)으로 멀티캐스트 트래픽을 전송하는 발신자의 소스 주소를 입력합니다. 이(S,G) 조합에 대한 트래픽은 정적 IGMP 인터페이스에서 허용됩니다.
5. 확인을 클릭하여 정적 IGMP 인터페이스를 저장합니다.

STEP 10 | 확인을 클릭하여 멀티캐스트 구성을 저장합니다.

STEP 11 | 커밋합니다.

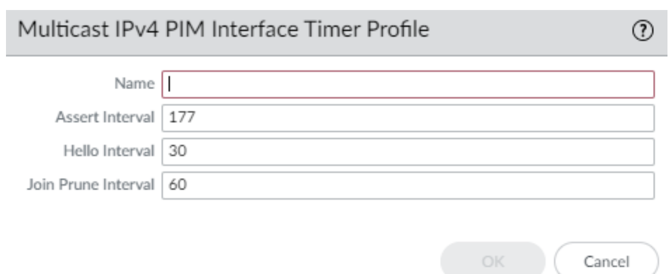
멀티캐스트 라우팅 프로파일 생성

고급 라우팅 엔진에서 IPv4 멀티캐스트 구성에 적용할 다음 라우팅 프로파일을 만듭니다.

- 멀티캐스트 **IPv4 PIM** 인터페이스 타이머 프로파일 - PIM 일반 탭 (인터페이스 일반 타이머) 및 PIM 인터페이스 탭에서 인터페이스 일반 타이머를 재정의합니다.
- 멀티캐스트 **IPv4 IGMP** 인터페이스 쿼리 프로파일 - 동적 IGMP 인터페이스의 경우 IGMP 탭에서 사용합니다.

STEP 1 | 멀티캐스트 IPv4 PIM 인터페이스 타이머 프로파일을 생성합니다.

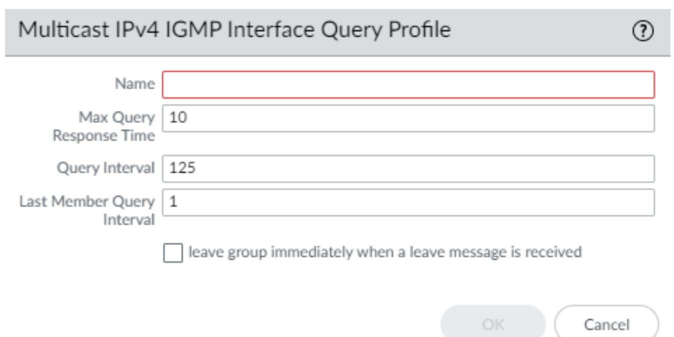
1. 네트워크 > 라우팅 > 라우팅 프로파일 > 멀티캐스트를 선택합니다.
2. 이름으로 멀티캐스트 **IPv4 PIM** 인터페이스 타이머 프로파일 을 추가합니다. (최대 63자). 이름은 영숫자 문자, 밑줄(_) 또는 하이픈(-)으로 시작해야 하며 영숫자 문자, 밑줄 또는 하이픈의 조합을 포함할 수 있습니다. 점(.) 또는 공백은 사용할 수 없습니다.
3. 어설션 간격 지정 - 논리 라우터가 PIM 전달자를 선택할 때 다중 액세스 네트워크의 다른 PIM 라우터에 보내는 PIM 어설트 메시지 사이의 시간(초). 범위는 0 ~ 65,534입니다. 기본값은 177입니다.
4. **Hello** 간격 지정 - 논리적 라우터가 인터페이스 그룹의 각 인터페이스에서 PIM 인접 인터페이스로 보내는 PIM Hello 메시지 사이의 시간 (초) 입니다. 범위는 1~180이며 기본값은 30입니다.
5. 조인 정리 간격 지정 - 논리 라우터가 멀티캐스트 소스를 향해 업스트림으로 보내는 PIM 조인 메시지 간(및 PIM 정리 메시지 간) 시간(초)입니다. 범위는 60~600이며 기본값은 60입니다.



6. 확인을 클릭합니다.

STEP 2 | 멀티캐스트 IPv4 IGMP 인터페이스 쿼리 프로파일을 생성합니다.

1. 네트워크 > 라우팅 > 라우팅 프로파일 > 멀티캐스트를 선택합니다.
2. 이름 으로 멀티캐스트 **IPv4 IGMP** 인터페이스 쿼리 프로파일 을 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.
3. 최대 쿼리 응답 시간 지정 - 수신자가 IGMP 멤버십에 응답할 수 있는 최대 시간 (초) 을 지정합니다. 논리적 라우터가 수신자가 그룹에 대한 멀티캐스트 패킷을 더 이상 수신하기를 원하지 않는다고 판단하기 전에 쿼리 메시지를 표시합니다. 범위는 1-25이며 기본값은 10입니다.
4. 쿼리 간격 지정 - 논리적 라우터가 수신기에 보내는 IGMP 멤버십 쿼리 메시지 사이의 시간(초)은 수신기가 그룹에 대한 멀티캐스트 패킷을 수신하기를 원하는지 여부를 결정합니다. 범위는 1 ~ 1,800입니다. 기본값은 125입니다.
5. 마지막 구성원 쿼리 간격 지정 - 수신자가 그룹 탈퇴 메시지를 보낸 후 논리적 라우터가 보내는 그룹별 쿼리에 수신자가 응답하는 데 허용되는 시간(초)입니다. 범위는 1 ~ 25입니다. 기본값은 1입니다.
6. 나가기 메시지를 받았을 때 즉시 그룹 탈퇴를 사용하도록 설정하는 경우 멀티캐스트 그룹에 구성원이 하나만 있고 논리 라우터가 해당 그룹에 대한 IGMP Leave 메시지를 수신할 때 이 설정을 사용하면 논리 라우터가 멀티캐스트에서 해당 그룹 및 발신 인터페이스를 제거합니다.마지막 멤버 쿼리 간격이 만료될 때까지 기다리지 않고 MRib(라우팅 정보 베이스) 및 멀티캐스트 전달 정보 베이스(mFiB)를 즉시 사용할 수 있습니다. 이 설정을 사용하면 네트워크 리소스가 절약됩니다. (기본값은 사용 안 함입니다.)



7. 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋합니다.

IPv4 MRoute 생성

고급 라우팅 엔진을 사용하면 논리적 라우터에 대한 라우팅을 IPv4 멀티캐스트 구성할 수 있습니다. PIM은 유니캐스트 RIB를 확인하여 방화벽이 유니캐스트 패킷을 소스로 다시 보내는 데 사용하는 것과 동일한 인터페이스에서 패킷을 수신했는지 여부를 확인한다는 점을 기억합니다.

유니캐스트 패킷이 멀티캐스트 패킷과 다른 경로를 사용하도록 하려는 토폴로지에서는 mroute를 구성할 수 있습니다. mroute는 멀티캐스트 소스를 가리키는 정적 유니캐스트 경로입니다. mroute는 멀티캐스트 RIB(MRIB)에 저장됩니다. PIM은 RPF 검사에 유니캐스트 RIB를 사용하는 대신 RPF 검사에 mroute를 사용합니다. PIM이 RPF 검사에 MRIB 또는 URIB를 사용하는지 여부는 PIM에 대해 구성된 RPF 조회 모드에 따라 다릅니다. RPF 검사 중에 사용된 mroute는 가장 긴 접두사 일치가 있는 mroute입니다.

mroute는 예를 들어 경로에 있는 일부 디바이스가 멀티캐스트 라우팅을 지원하지 않아 멀티캐스트 라우터를 연결하는 데 터널이 사용되는 경우에 유용합니다.

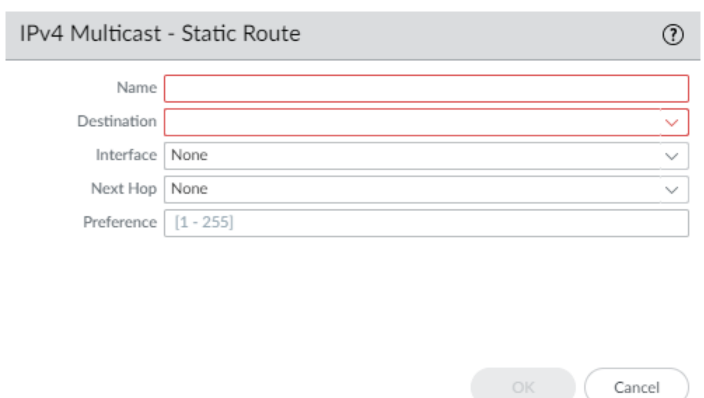
STEP 1 | 논리 라우터 구성.

STEP 2 | 네트워크 > 라우팅 > 논리 라우터를 선택하고 논리 라우터를 선택합니다.

STEP 3 | 멀티캐스트를 선택하고 멀티캐스트 프로토콜을 활성화합니다.

STEP 4 | mroute를 생성합니다.

1. 정적을 선택하고 이름으로 mroute를 추가합니다. 이름은 영숫자, 밑줄(_) 또는 하이픈(-) 으로 시작해야 하며 영숫자, 밑줄 또는 하이픈을 0개 이상 포함해야 합니다. 점(.) 또는 공백은 사용할 수 없습니다.



2. 방화벽이 RPF 검사를 수행하는 멀티캐스트 소스 또는 서브넷인 mroute의 대상(IPv4 주소/마스크 또는 주소 개체)을 입력합니다.
3. 멀티캐스트 소스에 대한 유니캐스트 경로에 대한 송신 인터페이스를 선택합니다.
4. 소스에 대한 다음 홉 라우터의 IPv4 주소(또는 주소 개체)를 입력합니다.
5. 경로에 대한 기본 설정을 입력합니다. 범위는 1~255입니다.
6. 확인을 클릭합니다.

STEP 5 | 확인을 클릭합니다.

STEP 6 | 변경 사항을 커밋합니다.

