Firepower Threat Defense에 대한 투명 또는 라우팅 방화벽 모드

이 장에서는 방화벽 모드를 라우팅 또는 투명 모드로 설정하는 방법 및 각 방화벽 모드에서 방화벽이 어떻게 작동하는지에 대해 설명합니다.

참고 방화벽 모드는 일반 방화벽 인터페이스에만 영향을 주고 인라인 집합이나 패시브 인터페이스 등 IPS 전용 인터페이스에는 영향을 주지 않습니다. 두 개의 방화벽 모드 모두에서 IPS 전용 인터페이스를 사용할 수 있습니다. IPS 전용 인터페이스에 대한 자세한 내용은 Firepower Threat Defense 인라인 집합 및 패시브 인터페이스의 내용을 참조하십시오. 인라인 집합은 "투명 인라인 집합"으로 익숙할 수 있지만 인라인 인터페이스 유형은 이 장 및 방화벽 유형 인터페이스에서 설명한 투명 방화벽 모드와는 관련이 없습니다.

방화벽 모드 정보

Firepower Threat Defense 디바이스에서는 일반 방화벽 인터페이스에 대해 두 가지 방화벽 모드(라우팅 방화벽 모드 및 투명 방화벽 모드)를 지원합니다.

라우팅 방화벽 모드 정보

라우팅 모드에서 Firepower Threat Defense 디바이스는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다.

통합 라우팅 및 브리징을 통해 네트워크에서 여러 인터페이스를 그룹화하는 "브리지 그룹"을 사용할 수 있으며, Firepower Threat Defense 디바이스에서는 브리징 기술을 사용하여 인터페이스 간에 트래픽을 통과시킵니다. 각 브리지 그룹에는 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)

가 있습니다. Firepower Threat Defense 디바이스에서는 BVI와 일반 라우팅 인터페이스 간을 라우팅합니다. 클러스터링, EtherChannel, 이중 멤버 인터페이스가 필요하지 않은 경우, 투명 모드 대신 라우팅 모드를 사용하는 것을 고려할 수 있습니다. 라우팅 모드에서는 투명 모드에서와 같이 하나 이상의 격리된 브리지 그룹을 가질 수 있지만, 혼합 구축을 위한 일반적인 라우팅 인터페이스도 가집니다.

투명 방화벽 모드 정보

일반적으로 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다. 그러나 다른 방화벽과 마찬가지로 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다.

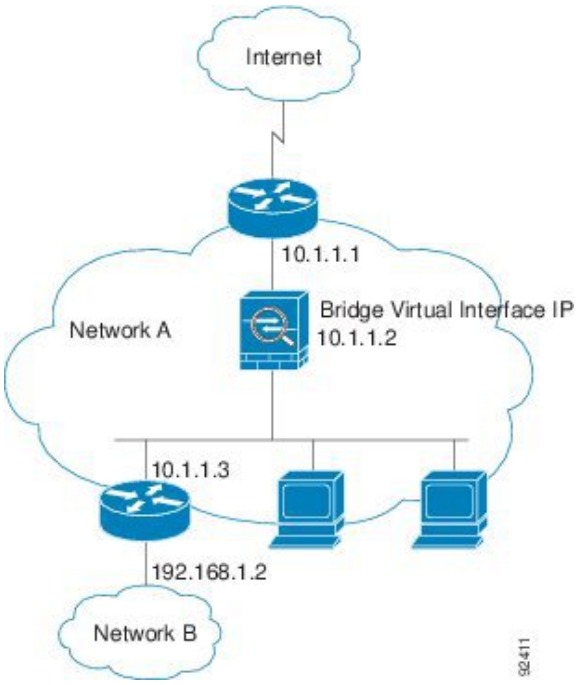
Layer 2 연결성은 네트워크의 내부 및 외부 인터페이스를 그룹화하는 "브리지 그룹"을 사용하여 획득할 수 있으며, Firepower Threat Defense 디바이스에서는 브리징 기술을 사용하여 인터페이스 간에 트래픽을 통과시킵니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 여러 네트워크에 대해 여러 개의 브리지 그룹을 사용할 수 있습니다. 투명 모드에서 이러한 브리지 그룹은 서로 통신할 수 없습니다.

네트워크에서 투명 방화벽 사용

Firepower Threat Defense 디바이스에서는 인터페이스 간의 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로, 투명 모드를 기존 네트워크에서 쉽게 도입할 수 있습니다.

다음 그림에는 외부 디바이스가 내부 디바이스와 동일한 서브넷에 존재하는 일반적인 투명 방화벽 네트워크가 나와 잇습니다. 내부 라우터와 호스트는 외부 라우터에 직접 연결되어 있는 것으로 표시됩니다.

그림 *1:* 투명 방어벽 네트워크



진단 인터페이스

각 BVI(Bridge Virtual Interface) IP 주소 이외에도 브리지 그룹에 속하지 않은 별도의 진단 슬롯/포트 인터페이스를 추가할 수 있으며, 이렇게 하면 Firepower Threat Defense 디바이스에는 관리 트래픽만 허용됩니다.

라우팅 모드 기능의 트래픽 전달

투명 방화벽에서 직접 지원되지 않는 기능의 경우, 업스트림 및 다운스트림 라우터를 통해 트래픽이 전달되도록 허용하여 해당 기능을 지원할 수 있습니다. 예를 들어, 액세스 규칙을 사용하여 DHCP 트래픽(지원되지 않는 DHCP 릴레이 기능 대신) 또는 IP/TV에서 생성된 것과 같은 멀티캐스트 트래픽을 허용할 수 있습니다. 또한 투명 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수도 있습니다. 액세스 규칙을 기반으로 OSPF, RIP, EIGRP 또는 BGP 트래픽의 통과를 허용할 수 있습니다. 마찬가지로, HSRP 또는 VRRP와 같은 프로토콜이 Firepower Threat Defense 디바이스를 통과할 수 있습니다.

브리지 그룹 정보

브리지 그룹은 Firepower Threat Defense 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 그룹은 투명 방화벽 모드와 라우팅 방화벽 모드에서 지원됩니다. 다른 방화벽 인터페이스와 마찬가지로 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다.

BVI(Bridge Virtual Interface)

각 브리지 그룹에는 BVI(Bridge Virtual Interface)가 있습니다. Firepower Threat Defense 디바이스에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 BVI IP 주소를 사용합니다. BVI IP 주소는 브리지 그룹 멤버 인터페이스와 동일한 서브넷에 있어야 합니다. BVI는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

투명 모드에서는 브리지 그룹 멤버 인터페이스만 이름이 지정되고 인터페이스 기반 기능과 함께 사용될 수 있습니다.

라우팅 모드에서는 BVI가 브리지 그룹 및 기타 라우팅 인터페이스 간에 게이트웨이 역할을 합니다. 브리지 그룹/라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다. 일부 인터페이스 기반 기능에는 BVI 자체를 사용할 수 있습니다.

- DHCPv4 서버 — BVI에서만 DHCPv4 서버 구성을 지원합니다.
- 고정 경로 — BVI에 대한 고정 경로는 구성할 수 있지만, 멤버 인터페이스에 대한 고정 경로는 구성할 수 없습니다.
- Firepower Threat Defense 디바이스에서 시작되는 기타 트래픽 및 syslog 서버 — syslog 서버(또는 SNMP 서버나 Firepower Threat Defense 디바이스에서 트래픽이 시작되는 기타 서비스)를 지정하는 경우 BVI 또는 멤버 인터페이스를 지정할 수 있습니다.

라우팅 모드에서 BVI 이름을 지정하지 않는 경우 Firepower Threat Defense 디바이스에서는 브리지 그룹 트래픽을 라우팅하지 않습니다. 이 구성을 사용하면 브리지 그룹에 대한 투명 방화벽 모드가 복제됩니다. 클러스터링, EtherChannel, 이중 멤버 인터페이스가 필요하지 않은 경우, 라우팅 모드를 대신 사용하는 것을 고려할 수 있습니다. 라우팅 모드에서는 투명 모드에서와 같이 하나 이상의 격리된 브리지 그룹을 가질 수 있지만, 혼합 구축을 위한 일반적인 라우팅 인터페이스도 가집니다.

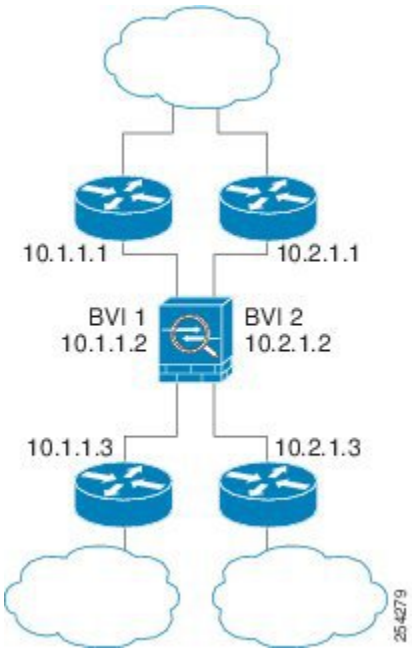
투명 방화벽 모드의 브리지 그룹

브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 트래픽은 Firepower Threat Defense 디바이스 내의 다른 브리지 그룹으로 라우팅되지 않으며, 트래픽은 외부 라우터에 의해 Firepower Threat Defense 디바이스의 다른 브리지 그룹으로 다시 라우팅되기 전에 Firepower Threat Defense 디바이스에서 나가야 합니다. 브리지 기능은 브리지 그룹마다 따로 있지만, 다른 여러 기능은 모든 브리지 그룹이 공유합니다. 예를 들어, 모든 브리지 그룹은 syslog 서버 또는 AAA 서버 컨피그레이션을 공유합니다.

브리지 그룹당 여러 인터페이스를 포함할 수 있습니다. 지원되는 브리지 그룹 및 인터페이스의 정확한 수는 방화벽 모드에 대한 지침, 11 페이지의 내용을 참조하십시오. 브리지 그룹당 3개 이상의 인터페이스를 사용하는 경우, 동일한 네트워크에 있는 여러 세그먼트 간의 통신은 제어할 수 있지만 내부 및 외부 간의 통신은 제어할 수 없습니다. 예를 들어, 서로 통신하는 것을 허용하지 않을 내부 세그먼트가 3개 있는 경우, 각 세그먼트를 개별 인터페이스에 두고 외부 인터페이스하고만 통신하도록 허용할 수 있습니다. 또는 원하는 만큼만 액세스하는 것을 허용하기 위해 인터페이스 간에 액세스 규칙을 맞춤화할 수 있습니다.

다음 그림에는 2개의 브리지 그룹이 있는 Firepower Threat Defense 디바이스에 연결된 2개의 네트워크가 나와 있습니다.

그림 *2: 2*개의 브리지 그룹이 있는 투명 방화벽 네트워크

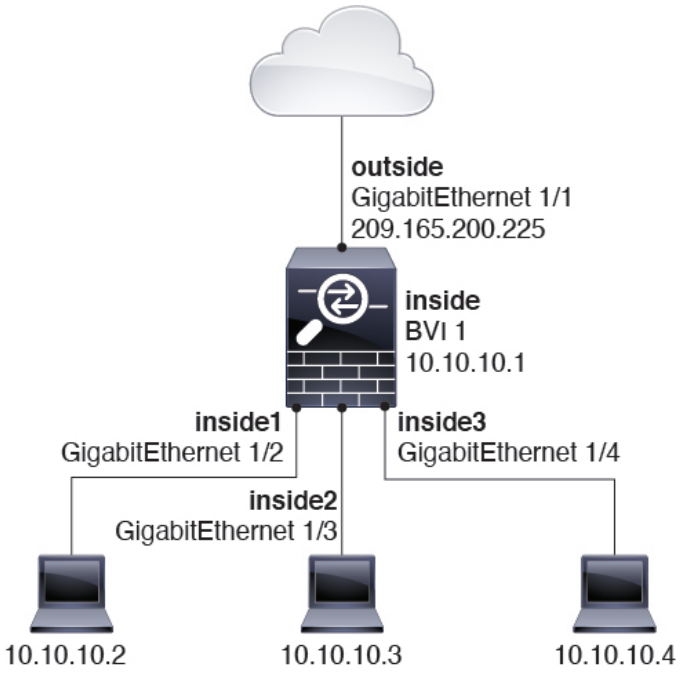


라우팅 방화벽 모드의 브리지 그룹

브리지 그룹 트래픽은 다른 브리지 그룹 또는 라우팅 인터페이스로 라우팅될 수 있습니다. 브리지 그룹의 BVI 인터페이스에 이름을 할당하지 않는 방법을 통해 브리지 그룹 트래픽을 격리하도록 선택할 수 있습니다. BVI에 이름을 지정하면 BVI에서는 다른 일반 인터페이스와 마찬가지로 라우팅에 참여합니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 FTD에서 추가 인터페이스를 사용하는 것입니다. 예를 들어 일부 디바이스에 대한 기본 구성에서는 외부 인터페이스를 일반 인터페이스로 포함한 다음, 내부 브리지 그룹에 할당된 기타 모든 인터페이스를 포함합니다. 이 브리지 그룹의 목적이 외부 스위치를 교체하는 것이므로 모든 브리지 그룹 인터페이스가 자유롭게 통신할 수 있도록 액세스 정책을 구성해야 합니다.

그림 3: 내부 브리지 그룹 및 외부 라우팅 인터페이스를 사용하는 라우팅 방화벽 네트워크



Layer 3 트래픽 허용

- 유니캐스트 IPv4 및 IPv6 트래픽을 사용하려면 액세스 규칙이 브리지 그룹을 통과하는 것이 허용되어야 합니다.
- ARP는 액세스 규칙 없이도 양방향에서 브리지 그룹을 통과할 수 있습니다. ARP 트래픽은 ARP 감시로 제어할 수 있습니다.
- IPv6 네이버 검색 및 라우터 요청 패킷은 액세스 규칙을 사용하여 전달될 수 있습니다.
- 액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽을 전달할 수 있습니다.

허용되는 MAC 주소

액세스 정책에서 허용하는 경우 다음과 같은 대상 MAC 주소가 브리지 그룹을 통과할 수 있습니다 (Layer 3 트래픽 허용, 6 페이지 참조). 이 목록에 없는 모든 MAC 주소는 손실됩니다.

- FFFF.FFFF.FFFF와 같은 TRUE 브로드캐스트 목적지 MAC 주소
- 0100.5E00.0000에서 0100.5EFE.FFFF 사이의 IPv4 멀티캐스트 MAC 주소
- 3333.0000.0000에서 3333.FFFF.FFFF 사이의 IPv6 멀티캐스트 MAC 주소
- 0100.0CCC.CCCD와 같은 BPDU 멀티캐스트 주소

BPDU 처리

Spanning Tree Protocol을 사용하여 루프를 방지하기 위해 기본적으로 BPDU가 전달됩니다.

기본적으로 BPDU는 고급 검사에 포워딩되며 이런 유형의 패킷에 필수 사항은 아니지만 예를 들어 검사 재시작을 위해 차단될 경우 문제가 발생할 수도 있습니다. 고급 검사에서 BPDU를 항상 제외하는 것이 좋습니다. 이를 위해 FlexConfig를 사용하여 BPDU를 신뢰하고 각 구성원 인터페이스에 대한 고급 검사에서 이를 제외하는 EtherType ACL을 설정합니다. Firepower Threat Defense에 대한 FlexConfig 정책의 내용을 참조하십시오.

FlexConfig 개체는 다음 명령을 배포하여 <if-name>을 인터페이스 이름으로 교체합니다. 디바이스에서 각 브리지 그룹 멤버 인터페이스를 처리하기 위한 액세스 그룹 명령을 필요한 만큼 추가합니다. ACL에 다른 이름을 선택할 수도 있습니다.

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC 주소 대 경로 조회 비교

브리지 그룹 내 트래픽의 경우 패킷의 발신 인터페이스는 경로 조회 대신 대상 MAC 주소 조회를 수행하여 확인할 수 있습니다.

그러나 다음과 같은 상황에는 경로 조회가 필요합니다.

- Firepower Threat Defense 디바이스에서 시작되는 트래픽 — 예를 들어, syslog 서버가 위치한 원격 네트워크로 향하는 트래픽을 위해 Firepower Threat Defense 디바이스에서 기본/고정 경로를 추가합니다.
- VoIP(Voice over IP) 및 TFTP 트래픽, 1홉 이상 떨어져 있는 엔드포인트 — 보조 연결에 성공하도록 원격 엔드포인트로 향하는 트래픽을 위해 Firepower Threat Defense 디바이스에서 고정 경로를 추가합니다. Firepower Threat Defense 디바이스에서는 보조 연결을 허용하기 위해 액세스 제어 정책에서 임시 "핀홀"을 생성합니다. 연결에서 기본 연결보다 다양한 IP 주소 집합을 사용할 수 있기 때문에, Firepower Threat Defense 디바이스에서는 올바른 인터페이스에서 핀홀을 설치하기 위해 경로 조회를 수행해야 합니다.

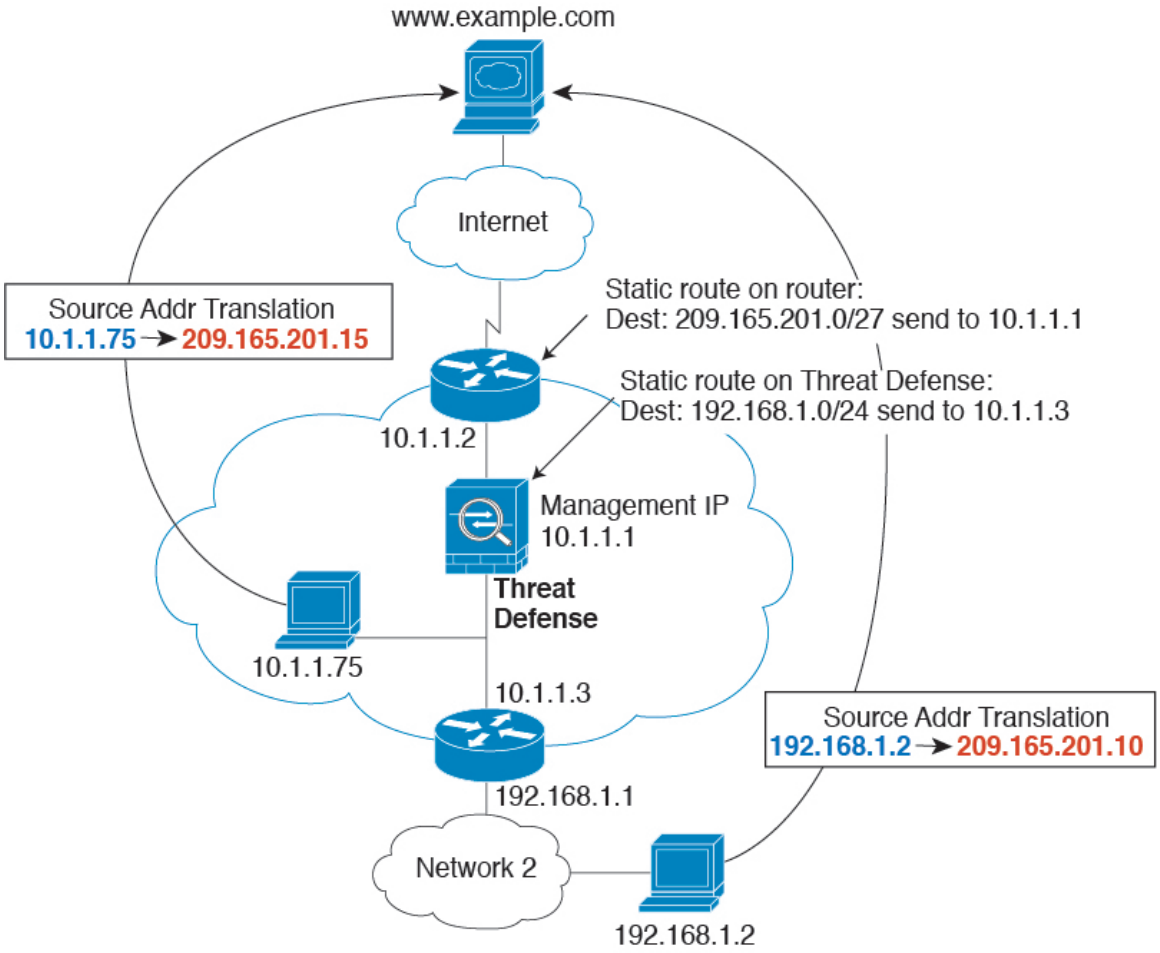
  영향을 받는 애플리케이션은 다음과 같습니다.

  - H.323
  - RTSP
  - SIP
  - Skinny(SCCP)
  - SQL*Net
  - SunRPC
  - TFTP

- Firepower Threat Defense 디바이스에서 NAT를 수행하는 1홉 이상 떨어져 있는 트래픽 — 원격 네트워크로 향하는 트래픽을 위해 Firepower Threat Defense 디바이스에서 고정 경로를 구성합니다. 또한 Firepower Threat Defense 디바이스로 전송될 매핑된 주소로 향하는 트래픽을 위해 업스트림 라우터에 고정 경로가 필요합니다.

  이 라우팅 요구 사항은 NAT가 활성화되어 있는 DNS 및 VoIP용 임베디드 IP 주소에도 마찬가지로 적용되며, 임베디드 IP 주소는 1홉 이상 떨어져 있습니다. Firepower Threat Defense 디바이스에서는 올바른 이그레스 인터페이스를 식별해야 변환을 수행할 수 있습니다.

그림 ***4: NAT*** 예: 브리지 그룹 내부의 ***NAT***



투명 모드의 브리지 그룹에 대해 지원되지 않는 기능

다음 표에는 투명 모드의 브리지 그룹에서 지원되지 않는 기능이 나와 있습니다.

표 ***1:*** 투명 모드에서 지원되지 않는 기능

기능	설명
동적 DNS	—

기능	설명
DHCP 릴레이	투명 방화벽에서는 DHCPv4 서버 역할을 수행할 수 있으나, DHCP 릴레이를 지원하지는 않습니다. 2개의 액세스 규칙을 사용하여 DHCP 트래픽이 통과되도록 할 수 있으므로 DHCP 릴레이가 필요하지 않습니다. 이러한 액세스 규칙 중 하나는 DHCP 요청이 내부 인터페이스에서 외부 인터페이스로 전달되도록 하고, 나머지 하나는 서버의 응답을 다른 방향으로 전달할 수 있도록 합니다.
동적 라우팅 프로토콜	그러나 브리지 그룹 멤버 인터페이스의 Firepower Threat Defense 디바이스에서 시작된 트래픽에 대한 고정 경로를 추가할 수 있습니다. 또한 액세스 규칙을 사용하여 동적 라우팅 프로토콜이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다.
멀티캐스트 IP 라우팅	액세스 규칙에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다.
QoS	—
통과 트래픽의 VPN 종료	투명 방화벽에서는 브리지 그룹 멤버 인터페이스에서만 관리 연결에 Site-to-Site VPN 터널을 지원합니다. 그러나 이로 인해 Firepower Threat Defense 디바이스를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 액세스 규칙을 사용하여 VPN 트래픽이 ASA를 통과하도록 할 수 있으나, 이로 인해 관리 이외 연결이 종료되지는 않습니다.

라우팅 모드의 브리지 그룹에 대해 지원되지 않는 기능

다음 표에는 라우팅 모드의 브리지 그룹에서 지원되지 않는 기능이 나와 있습니다.

표 ***2:*** 라우팅 모드에서 지원되지 않는 기능

기능	설명
EtherChannel 멤버 인터페이스	물리적 인터페이스, 이중 인터페이스 및 하위 인터페이스만 브리지 그룹 멤버 인터페이스로 지원됩니다. 진단 인터페이스도 지원되지 않습니다.
클러스터링	브리지 그룹은 클러스터링에서 지원되지 않습니다.

기능	설명
동적 DNS	—
DHCP 릴레이	라우팅 방화벽은 DHCPv4 서버로 작동할 수 있지만, BVI 또는 브리지 그룹 멤버 인터페이스에서 DHCP 릴레이를 지원하지는 않습니다.
동적 라우팅 프로토콜	그러나 BVI에 고정 경로를 추가할 수 있습니다. 또한 액세스 규칙을 사용하여 동적 라우팅 프로토콜이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다. 비 브리지 그룹 인터페이스에서는 동적 라우팅을 지원합니다.
멀티캐스트 IP 라우팅	액세스 규칙에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다. 비 브리지 그룹 인터페이스에서는 멀티캐스트 라우팅을 지원합니다.
QoS	비 브리지 그룹 인터페이스에서는 QoS를 지원합니다.
통과 트래픽의 VPN 종료	BVI에서 VPN 연결을 종료할 수 없습니다. 비 브리지 그룹 인터페이스에서는 VPN을 지원합니다. 브리지 그룹 멤버 인터페이스에서는 관리 연결에만 Site-to-Site VPN 터널을 지원합니다. 그러나 이로 인해 Firepower Threat Defense 디바이스를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 액세스 규칙을 사용하여 VPN 트래픽이 브리지 그룹을 통과하도록 할 수 있으나, 이로 인해 관리 이외 연결이 종료되지는 않습니다.

기본 설정

브리지 그룹 기본값

기본적으로 모든 ARP 패킷은 브리지 그룹 내에서 전달됩니다.

방화벽 모드에 대한 지침

모델 지침

- 브리지 ixgbevf 인터페이스를 사용하는 VMware의 Firepower Threat Defense Virtual의 경우 브리지 그룹이 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.

브리지 그룹 지침(투명 모드 및 라우팅 모드)

- 브리지 그룹당 64개의 인터페이스가 있는 최대 250개의 브리지 그룹을 생성할 수 있습니다.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- Firepower Threat Defense 디바이스는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.
- IPv4에서는 관리 트래픽과 Firepower Threat Defense 디바이스를 거칠 트래픽 모두 브리지 그룹마다 BVI용 IP 주소가 필요합니다. IPv6 주소는 지원되지만 BVI에는 필요하지 않습니다.
- IPv6 주소만 수동으로 구성할 수 있습니다.
- BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다.
- 관리 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- Firepower 1010의 경우, 동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수 없습니다.
- Firepower 4100/9300의 경우, 데이터 공유 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 투명 모드에서는 1개 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 투명 모드에서는 BVI IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 Firepower Threat Defense 디바이스의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 투명 모드에서는 관리 트래픽의 반환 경로를 제공하는 데 필요한 기본 경로가 하나의 브리지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브리지 그룹의 인터페이스 및 브리지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브리지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 일반 고정 경로를 지정해야 합니다.
- 투명 모드에서 PPPoE는 진단 인터페이스에 대해 지원되지 않습니다.
- 라우팅 모드에서 브리지 그룹 및 기타 라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다.

- 라우팅 모드에서 FTD 정의된 EtherChannel 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 브리지 그룹 멤버를 사용할 때 FTD를 통과하는 것이 허용되지 않습니다. BFD를 실행하는 FTD의 양쪽 측면에 두 개의 네이버가 있는 경우, FTD는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

방화벽 모드 설정

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

CLI에서 초기 시스템 설정을 수행할 때 방화벽 모드를 설정할 수 있습니다. 방화벽 모드 변경은 설정을 삭제하므로 호환되지 않는 설정이 없도록 설정 중 방화벽 모드를 설정하는 것을 권장합니다. 나중에 방화벽 모드를 변경하려면 CLI에서 변경해야 합니다.

프로시저

단계 **1** FMC에서 FTD 디바이스를 등록 취소합니다.

디바이스를 등록 취소할 때까지 모드를 변경할 수 없습니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
b) 매니지드 디바이스 목록에서 디바이스를 선택합니다.
c) 디바이스를 삭제(휴지통 클릭)한 뒤 확인하고 시스템이 디바이스를 제거할 때까지 기다립니다.

단계 **2** FTD 디바이스 CLI에 액세스합니다. 콘솔 포트에서 액세스하는 것이 좋습니다.

진단 인터페이스에 SSH를 사용하면 모드를 변경할 때 인터페이스 설정을 삭제하며 연결이 끊어집니다. 그 경우 관리 인터페이스에 연결해야 합니다.

단계 **3** 방화벽 모드 변경

configure firewall[**routed** | **transparent**]

예제**:**

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

단계 **4** FMC로 다시 등록:

configure manager add {*hostname* | *ip_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *ip_address* | **DONTRESOLVE** }는 FMC의 완전히 검증된 호스트 명 또는 IP 주소를 지정합니다. FMC의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용합니다.
- *reg_key*는 디바이스를 FMC에 등록하는 데 필요한 고유 영숫자 등록 키입니다.
- *nat_id*는 FMC와 장치 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름이 **DONTRESOLVE**로 설정된 경우 반드시 필요합니다.