멀티캐스트

이 장에서는 멀티캐스트 라우팅 프로토콜을 사용하도록 Secure Firewall Threat Defense 디바이스를 구성하는 방법을 설명합니다.

멀티캐스트 라우팅 정보

멀티캐스트 라우팅은 단일 정보 스트림을 수천 개의 기업 수신자와 가정으로 동시에 제공함으로써 트래픽을 줄이는 대역폭 절약 기술입니다. 멀티캐스트 라우팅을 활용하는 분야로는 화상 회의, 기업 통신, 원거리 학습, 소프트웨어 배포, 주식 시세 및 뉴스가 있습니다.

멀티캐스트 라우팅 프로토콜은 소스나 수신자에 추가적인 부담을 주지 않고 경쟁 기술 중에서도 가장 적은 네트워크 대역폭을 사용하여 소스 트래픽을 여러 수신자에게 보냅니다. 멀티캐스트 패킷은 PIM(Protocol Independent Multicast) 및 기타 지원 멀티캐스트 프로토콜로 활성화되는 위협 방지 디바이스에 의해 네트워크에서 복제되어 여러 수신자에게 데이터를 가장 효율적으로 제공할 수 있습니다.

위협 방지 디바이스는 stub 멀티캐스트 라우팅과 PIM 멀티캐스트 라우팅을 모두 지원합니다. 하지만 두 라우팅을 하나의 위협 방지 디바이스에 동시에 구성할 수는 없습니다.

참고 멀티캐스트 라우팅에 대해 UDP 및 비 UDP 전송이 모두 지원됩니다. 그러나 비 UDP 전송에는 FastPath 최적화가 없습니다.

IGMP 프로토콜

IP 호스트가 IGMP(Internet Group Management Protocol)를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터로 보고합니다. IGMP는 특정 LAN의 멀티캐스트 그룹에서 개별 호스트를 동적으로 등록하는 데 사용됩니다. 호스트는 IGMP 메시지를 로컬 멀티캐스트 라우터로 전송함으로써 그룹 멤버십을 식별합니다. IGMP에서 라우터가 IGMP 메시지를 듣고 주기적으로 쿼리를 보내 특정 서브넷에서 어떤 그룹이 활성 상태이고 어떤 그룹이 비활성 상태인지 파악합니다.

IGMP는 그룹 주소(Class D IP 주소)를 그룹 식별자로 사용합니다. 호스트 그룹 주소 범위는 224.0.0.0 ~ 239.255.255.255입니다. 224.0.0.0 주소는 어떤 그룹에도 할당되지 않습니다. 224.0.0.1 주소는 서브넷의 모든 시스템에 할당됩니다. 224.0.0.2 주소는 서브넷의 모든 라우터에 할당됩니다.

참고 threat defense 디바이스에서 멀티캐스트 라우팅을 활성화할 경우 IGMP 버전 2가 모든 인터페이스에서 자동으로 활성화됩니다.

멀티캐스트 그룹으로의 쿼리 메시지

threat defense 디바이스는 쿼리 메시지를 보내 어떤 멀티캐스트 그룹이 인터페이스에 연결된 네트워크의 멤버인지 확인합니다. 멤버는 특정 그룹에 대한 멀티캐스트 패킷을 받고 싶다는 의미의 IGMP 보고 메시지로 응답합니다. 쿼리 메시지는 주소가 224.0.0.1이고 time-to-live 값이 1인 전체 시스템 멀티캐스트 그룹으로 전달됩니다.

이 메시지는 주기적으로 전송되어 threat defense 디바이스에 저장된 멤버십 정보를 새로 고침합니다. threat defense 디바이스가 아직 인터페이스에 연결된 멀티캐스트 그룹의 로컬 멤버가 없다고 확인하면 해당 그룹의 멀티캐스트 패킷을 연결된 네트워크로 더 이상 전달하지 않고 prune 메시지를 다시 패킷 소스로 전송합니다.

기본적으로 서브넷의 PIM 지정 라우터가 쿼리 메시지 전송을 담당합니다. 기본적으로 125초마다 한 번 전송됩니다.

쿼리 응답 시간을 변경할 경우 IGMP 쿼리에서 알려지는 최대 쿼리 응답 시간은 기본적으로 10초입니다. 이 시간 내에 threat defense 디바이스가 호스트 쿼리에 대한 응답을 받지 못하면 그 그룹이 삭제됩니다.

stub 멀티캐스트 라우팅

Stub 멀티캐스트 라우팅은 동적 호스트 등록을 제공하고 멀티캐스트 라우팅을 촉진합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 위협 방지 디바이스는 IGMP 프록시 에이전트 역할을 합니다. 멀티캐스트 라우팅에 완전히 참여하는 대신 위협 방지 디바이스는 IGMP 메시지를 업스트림 멀티캐스트 라우터로 전송하고 이 라우터가 멀티캐스트 데이터 전송을 설정합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 위협 방지 디바이스는 PIM 스파스 또는 양방향 모드에 대해 구성될 수 없습니다. IGMP 스텁 멀티캐스트 라우팅에 참여 중인 인터페이스에서 PIM을 활성화해야 합니다.

위협 방지 디바이스는 PIM-SM과 양방향 PIM을 모두 지원합니다. PIM-SM은 기본 유니캐스트 라우팅 정보 기반 또는 별도의 멀티캐스트 지원 라우팅 정보 기반을 사용하는 멀티캐스트 라우팅 프로토콜입니다. 또한 멀티캐스트 그룹당 단일 RP(랑데부 포인트)를 루트로 삼는 단방향 공유 트리를 구축하고 선택적으로 멀티캐스트 소스별로 최단 경로 트리를 생성합니다.

PIM 멀티캐스트 라우팅

양방향 PIM은 멀티캐스트 소스와 수신자를 연결하는 양방향 공유 트리를 구축하는 PIM-SM의 변형입니다. 양방향 트리는 멀티캐스트 토폴로지의 각 링크에서 작동하는 DF(Designated Forwarder) 선택 프로세스를 사용하여 구축됩니다. 멀티캐스트 데이터는 DF의 도움을 받아 소스에서 RP(랑데부 포인트)로 전달되고 따라서 소스별 상태 없이도 공유 트리에서 수신자를 따르게 됩니다. DF 선택은 RP 검색 중에 이루어지고 RP에 대한 기본 경로를 제공합니다.

참고 위협 방지 디바이스가 PIM RP인 경우 위협 방지 디바이스의 변환되지 않은 외부 주소를 RP 주소로 사용합니다.

PIM 소스별 멀티캐스트 지원

위협 방지 디바이스는 PIM SSM(Source Specific Multicast) 기능 및 관련된 구성을 지원하지 않습니다. 그러나 위협 방지 디바이스는 마지막 홉 라우터로 배치되는 경우를 제외하고 SSM 관련 패킷이 통과하도록 허용합니다.

SSM은 IPTV 같은 일대다 애플리케이션에 대한 데이터 전달 메커니즘으로 분류됩니다. SSM 모델은 (S,G) 쌍으로 표시된 "채널"의 개념을 사용하며, 여기서 S는 소스 주소이고 G는 SSM 대상 주소입니다. 채널 가입은 IGMPv3 같은 그룹 관리 프로토콜을 사용하여 수행됩니다. SSM이 특정 멀티캐스트 소스를 확인한 경우, 수신 클라이언트가 공유 RP(랑데부 포인트)에서 수신하는 대신 소스에서 직접 멀티캐스트 스트림을 수신하게 합니다. 액세스 제어 메커니즘은 현재 SM(Sparse Mode) 또는 SDM(Sparse-Dense Mode) 구현으로 사용할 수 없는 보안 향상을 제공하는 SSM 내에서 도입되었습니다.

PIM-SSM은 RP 또는 공유 트리를 사용하지 않는 점에서 PIM-SM과 다릅니다. 대신, 멀티캐스트 그룹의 소스 주소에 대한 정보가 IGMPv3(로컬 리시버십 프로토콜)를 통해 리시버에서 제공되고 소스별 트리를 직접 구축하는 데 사용됩니다.

멀티캐스트 양방향 PIM

멀티캐스트 양방향 PIM은 여러 소스와 수신자가 동시에 서로 통신하고 화상회의, Webex 회의 및 그룹 채팅에서 각 참가자가 멀티캐스트 트래픽의 소스 및 수신자가 될 수 있는 네트워크에 유용합니다. PIM 양방향 모드가 사용되면 RP는 공유 트리에 대해서만 (*, G) 항목을 만듭니다. (S, G) 항목은 없습니다. 각 (S, G) 항목의 상태 테이블이 유지되지 않으므로 RP에서 리소스가 보존됩니다.

PIM 스파스 모드에서 트래픽은 공유 트리 아래로만 흐릅니다. PIM 양방향 모드에서는 트래픽이 공유 트리의 위아래로 흐릅니다.

또한 PIM 양방향 모드는 PIM register/register-stop 메커니즘을 사용하여 소스를 RP에 등록하지 않습니다. 각 소스는 언제든지 소스로 전송을 시작할 수 있습니다. 멀티캐스트 패킷이 RP에 도착하면 공유 트리(수신자가 있는 경우)로 전달되거나 삭제(수신자가 없는 경우)됩니다. 하지만 RP의 경우 소스에 멀티캐스트 트래픽 전송을 중지하도록 알릴 방법이 없습니다.

네트워크상의 소스와 수신자 사이의 중간에 RP가 있어야 하므로 RP의 위치를 생각해야 합니다.

PIM 양방향 모드에는 RPF(Reverse Path Forwarding) 확인이 없습니다. 대신 DF(Designated Forwarder) 개념을 사용하여 루프를 방지합니다. 이 DF는 멀티캐스트 트래픽을 RP에 전송할 수 있는 세그먼트의 유일한 라우터입니다. 멀티캐스트 트래픽을 전달하는 세그먼트당 하나의 라우터만 있으면 루프가 없습니다. DF는 다음 메커니즘을 사용하여 선택됩니다.

- RP에 가장 낮은 메트릭을 가진 라우터가 DF입니다.
- 메트릭이 동일한 경우 IP 주소가 가장 큰 라우터가 DF가 됩니다.

PIM BSR(부트스트랩 라우터)

PIM BSR(부트스트랩 라우터)은 그룹에 대해 RP 정보를 릴레이하기 위해, 그리고 RP 기능을 위해 후보 라우터를 사용하는 동적 RP(랑데부 포인트) 선택 모델입니다. RP 기능은 RP 검색을 포함하며 RP에 대한 기본 경로를 제공합니다. RP 기능은 이를 위해 디바이스 집합을 BSR 선택 프로세스에 참여하는 C-BSR(후보 BSR)로 구성하여 후보 중에서 BSR을 선택하는 방식을 이용합니다. BSR을 선택한 후 C-RP(후보 랑데부 포인트)로 구성된 디바이스는 선택한 BSR로 그룹 매핑을 전송하기 시작합니다. 그런 다음 BSR은 홉에 기반하여 PIM 라우터 간에 이동하는 BSR 메시지를 통해 멀티캐스트 트리 아래의 모든 기타 디바이스로 그룹-RP 매핑 정보를 배포합니다.

이 기능은 RP를 동적으로 확인하는 수단을 제공하는데, 이는 RP가 정기적으로 아래위로 이동할 수 있는 대규모의 복잡한 네트워크에서 매우 필수적입니다.

PIM BSR(부트스트랩 라우터) 용어

다음 조건은 PIM BSR 구성에서 자주 참조됩니다.

- BSR(부트스트랩 라우터) — BSR은 PIM을 사용하여 RP(랑데부 포인트) 정보를 다른 라우터에 홉별로 알립니다. 선택 프로세스 이후에 여러 후보 BSR 중에서 단일 BSR이 선택됩니다. 이 부트스트랩 라우터의 주목적은 모든 C-RP(Candidate-RP) 알림을 RP-set(RP 집합)이라고 하는 데이터베이스에 수집하고 이를 BSR 메시지로 60초마다 네트워크에 있는 다른 모든 라우터에 정기적으로 전송하는 것입니다.
- BSR(부트스트랩 라우터) 메시지 — BSR 메시지는 All-PIM-Routers(모든 PIM 라우터) 그룹에 대한 멀티캐스트입니다(TTL이 1). 이러한 메시지를 수신하는 모든 PIM 네이버는 메시지를 수신한 인터페이스를 제외한 모든 인터페이스 외부로 해당 메시지를 TTL을 1로 재전송합니다. BSR 메시지는 RP 집합 및 현재 활성 BSR의 IP 주소를 포함합니다. 이를 통해 C-RP는 자신의 C-RP 메시지를 유니캐스트할 위치를 확인합니다.
- C-BSR(후보 부트스트랩 라우터) — 후보-BSR로 구성된 디바이스는 BSR 선택 메커니즘에 참여합니다. 우선순위가 가장 높은 C-BSR은 BSR로 선택됩니다. C-BSR의 우선순위가 가장 높은 IP 주소는 타이 브레이커로 사용됩니다. BSR 선택 프로세스는 선점형입니다. 예를 들어, 우선순위가 더 높은 새로운 C-BSR이 가동되면 새로운 선택 프로세스가 트리거됩니다.
- C-RP(후보 랑데부 포인트) — RP는 소스 및 멀티캐스트 데이터의 수신자가 만나는 공간의 역할을 합니다. C-RP로 구성된 디바이스는 정기적으로 유니캐스트를 통해 선택한 BSR로 직접 멀티캐스트 그룹 매핑 정보를 알립니다. 이러한 메시지에는 그룹 범위, C-RP 주소 및 보류 시간이 포함되어 있습니다. 현재 BSR의 IP 주소는 네트워크의 모든 라우터에서 수신하는 정기적인 BSR

메시지에서 확인됩니다. 이러한 방법으로 BSR은 현재 작동 중이며 연결 가능한 RP를 확인합니다.

참고 C-RP가 BSR 트래픽에 대한 필수 요구 사항인 경우에도 위협 방지 디바이스는 C-RP로 작동하지 않습니다. 라우터만 C-RP로 작동할 수 있습니다. 따라서 BSR 테스트 기능을 위해 라우터를 토폴로지에 추가해야 합니다.

- BSR 선택 메커니즘 — 각 C-BSR은 BSR Priority(BSR 우선순위) 필드를 포함하는 부트스트랩 메시지(BSM)를 시작합니다. 도메인 내의 라우터는 도메인 전체에서 BSM을 플러딩합니다. 자신보다 우선순위가 높은 C-BSR를 알고 있는 C-BSR은 일정 기간 동안 추가 BSM 전송을 표시하지 않습니다. 나머지 단일 C-BSR은 선택된 BSR이 되며 해당 BSM은 도메인에 있는 모든 기타 라우터에 자신이 선택된 BSR임을 알립니다.

멀티캐스트 그룹 개념

멀티캐스트는 그룹 개념을 기반으로 합니다. 임의의 수신자 그룹이 특정 데이터 스트림 수신에 관심을 표현합니다. 이 그룹은 물리적 또는 지리적 경계가 없이 호스트가 인터넷의 어디에나 위치할 수 있습니다. 특정 그룹으로 향하는 데이터 수신에 관심이 있는 호스트는 IGMP를 사용하여 그룹에 참여해야 합니다. 호스트가 그룹의 일원이어야만 데이터 스트림을 받을 수 있습니다.

멀티캐스트 주소

멀티캐스트 주소는 그룹에 참여하고 이 그룹으로 전송된 트래픽을 수신하고자 하는 임의의 IP 호스트 그룹입니다.

클러스터링

멀티캐스트 라우팅은 클러스터링을 지원합니다. 스팬 EtherChannel 클러스터링에서 제어 유닛은 빠른 경로 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 전송합니다. fast-path 전달이 설정된 후에는 데이터 유닛이 멀티캐스트 데이터 패킷을 전송할 수 있습니다. 모든 데이터 흐름은 완전한 흐름입니다. Stub 전달 흐름도 지원됩니다. Spanned EtherChannel 클러스터링에서는 하나의 유닛만 멀티캐스트 패킷을 받기 때문에 제어 유닛으로의 리디렉션이 일반적입니다.

멀티캐스트 라우팅 요구 사항 및 사전 요건

모델 지원

Threat Defense

Threat Defense Virtual

지원되는 도메인

모든

사용자 역할

관리자

네트워크 관리자

멀티캐스트 라우팅 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

IPv6

IPv6를 지원하지 않습니다.

멀티캐스트 그룹

224.0.0.0과 224.0.0.255 사이의 주소 범위는 라우팅 프로토콜 및 기타 토폴로지 검색 또는 유지 보수 프로토콜 (예: 게이트웨이 검색 및 그룹 멤버십 보고)의 사용을 위해 예약됩니다. 따라서 주소 범위 224.0.0/24의 인터넷 멀티캐스트 라우팅은 지원되지 않습니다. 예약된 주소에 대해 멀티캐스트 라우팅을 활성화하는 경우 IGMP 그룹이 생성되지 않습니다.

클러스터링

IGMP 및 PIM에 대한 클러스터링에서 이 기능은 기본 유닛에서만 지원됩니다.

추가 지침

- 멀티캐스트 호스트(예: 224.1.2.3)에 대한 트래픽을 허용하려면 인바운드 보안 영역에서 액세스 제어 또는 사전 필터 규칙을 구성해야 합니다. 그러나 규칙에 대한 대상 보안 영역을 지정하거나 초기 연결을 검증하는 동안 이를 멀티캐스트 연결에 적용할 수는 없습니다.
- PIM이 구성된 인터페이스는 비활성화 할 수 없습니다. 인터페이스에서 PIM을 구성한 경우(PIM 프로토콜 구성, 12 페이지 참조) 멀티캐스트 라우팅 및 PIM을 비활성화해도 PIM 구성은 제거되지 않습니다. 인터페이스를 비활성화하려면 PIM 구성을 제거(삭제)해야합니다.
- PIM/IGMP 멀티캐스트 라우팅은 트래픽 영역의 인터페이스에서 지원되지 않습니다.
- threat defense를 RP(랑데부 포인트) 및 첫 번째 홉 라우터로 동시에 구성하지 마십시오.
- HSRP 대기 IP 주소는 PIM 네이버 관계에 참여하지 않습니다. 따라서 RP 라우터 IP가 HSRP 대기 IP 주소를 통해 라우팅되는 경우 멀티 캐스트 라우팅이 Threat Defense에서 작동하지 않습니다. 따라서 멀티 캐스트 트래픽이 성공적으로 통과하려면 RP 주소에 대한 경로가 HSRP 대기 IP 주소가 아닌지 확인하는 대신 경로 주소를 인터페이스 IP 주소로 구성합니다.

- 가상 라우팅을 사용하는 디바이스의 경우 멀티캐스트는 전역 가상 라우터에만 구성할 수 있으며 사용자 정의 가상 라우터에는 구성할 수 없습니다.

IGMP 기능 구성

IP 호스트가 IGMP를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터에 보고합니다. IGMP는 특정 LAN의 멀티캐스트 그룹에서 개별 호스트를 동적으로 등록하는 데 사용됩니다. 호스트는 IGMP 메시지를 로컬 멀티캐스트 라우터로 전송함으로써 그룹 멤버십을 식별합니다. IGMP에서 라우터가 IGMP 메시지를 듣고 주기적으로 쿼리를 보내 특정 서브넷에서 어떤 그룹이 활성 상태이고 어떤 그룹이 비활성 상태인지 파악합니다.

이 섹션에서는 인터페이스별로 선택적인 IGMP 설정을 구성하는 방법을 설명합니다.

프로시저

단계 **1** 멀티캐스트 라우팅 활성화, 7 페이지.
단계 **2** IGMP 프로토콜 구성, 8 페이지.
단계 **3** IGMP 액세스 그룹 구성, 9 페이지.
단계 **4** IGMP 고정 그룹 구성, 10 페이지.
단계 **5** IGMP 조인 그룹 구성, 11 페이지.

멀티캐스트 라우팅 활성화

threat defense 디바이스에서 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 기본적으로 IGMP 및 PIM이 활성화됩니다. IGMP는 그룹에서 어떤 멤버가 직접 연결된 서브넷에 존재하는지 학습하는 데 사용됩니다. 호스트는 IGMP 보고 메시지를 전송함으로써 멀티캐스트 그룹에 참여합니다. PIM은 멀티캐스트 데이터 그램을 전달하기 위한 전달 테이블 유지에 사용됩니다.

참고 멀티캐스트 라우팅에 대해서는 UDP 전송 레이어만 지원됩니다.

다음 목록에는 특정 멀티캐스트 테이블에 대한 최대 항목 수가 나와 있습니다. 이 제한에 도달하면 새로운 엔트리가 삭제됩니다.

- MFIB—30,000
- IGMP 그룹-30,000
- PIM 경로 —72,000

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Enable Multicast Routing(**멀티캐스트 라우팅 활성화**)** 확인란을 선택합니다.

이 확인란을 선택하면 디바이스에서 IP 멀티캐스트 라우팅이 활성화됩니다. 이 확인란 선택을 취소하면 IP 멀티캐스트 라우팅이 비활성화됩니다. 기본적으로 멀티캐스트는 비활성화되어 있습니다. 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 멀티캐스트가 활성화됩니다.

인터페이스별로 멀티캐스트를 비활성화할 수 있습니다. 이 정보는 특정 인터페이스에 멀티캐스트 호스트가 없음을 알고 있고 threat defense 디바이스가 해당 인터페이스로 호스트 쿼리 메시지를 보내는 것을 막고 싶을 때 유용합니다.

IGMP 프로토콜 구성

전달 인터페이스, 쿼리 메시지 및 시간 간격과 같은 인터페이스별로 IGMP 파라미터를 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Protocol(**프로토콜**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add IGMP parameters(IGMP 파라미터 추가**)** 대화 상자를 사용하여 새 IGMP 파라미터를 threat defense 디바이스에 추가합니다. **Edit IGMP parameters(IGMP** 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** - 드롭다운 목록에서 구성하려는 IGMP 프로토콜에 대한 인터페이스를 선택합니다.
- **Enable IGMP(IGMP** 활성화**)** - IGMP를 활성화하려면 확인란을 선택합니다.

  참고 특정 인터페이스에 대한 IGMP 비활성화는 특정 인터페이스에 멀티캐스트 호스트가 없음을 알고 있고 디바이스가 해당 인터페이스로 호스트 쿼리 메시지를 보내는 것을 막고 싶을 때 유용합니다.

- **Forward Interface(**인터페이스 전달**)** - 드롭다운 목록에서 IGMP 메시지를 전달할 특정 인터페이스를 선택합니다.

대신 IGMP 프록시 에이전트 역할을 하고 IGMP 메시지를 하나의 인터페이스에 연결된 호스트에서 다른 인터페이스에 연결된 업스트림 멀티캐스트 라우터로 전달하도록 Secure Firewall Threat Defense 디바이스를 구성합니다.

- **Version(**버전**)** - IGMP 버전 1 또는 2를 선택합니다.

  기본적으로 threat defense 디바이스는 몇 가지 추가 기능을 활성화하는 IGMP 버전 2를 실행합니다.

  참고 서브넷의 모든 멀티캐스트 라우터는 같은 버전의 IGMP를 지원해야 합니다. threat defense 디바이스는 자동으로 버전 1 라우터를 감지하고 버전 1로 전환하지 않습니다. 그러나 IGMP 버전 1과 2 호스트를 서브넷에서 혼용할 수는 있습니다. IGMP 버전 2를 실행 중인 threat defense 디바이스는 IGMP 버전 1 호스트가 있을 때에도 정상 작동합니다.

- **Query Interval(**쿼리 간격**)** - 지정된 라우터가 IGMP 호스트 쿼리 메시지를 전송하는 간격(초 단위)입니다. 범위는 1~ 600입니다. 기본값은 125입니다.

  참고 threat defense 디바이스가 지정된 시간 초과 값 동안 쿼리 메시지를 받지 못하면 디바이스가 지정 라우터가 되고 쿼리 메시지 전송을 시작합니다.

- **Response Time(**응답 시간**)** - threat defense 디바이스가 그룹을 삭제하기 전의 간격(초)입니다. 범위는 1~25입니다. 기본값은 10입니다.

  이 시간 내에 threat defense 디바이스가 호스트 쿼리에 대한 응답을 받지 못하면 그 그룹이 삭제됩니다.

- **Group Limit(**그룹 제한**)** - 인터페이스에 참여할 수 있는 호스트의 최대 수입니다. 범위는 1~500입니다. 기본값은 500입니다.

  인터페이스별로 IGMP 멤버십 보고에서 비롯되는 IGMP 멤버십 상태의 수를 제한할 수 있습니다. 구성된 제한을 초과하는 멤버십 보고는 IGMP 캐시에 입력되지 않고 초과된 멤버십 보고에 대한 트래픽은 전달되지 않습니다.

- **Query Timeout(**쿼리 시간 초과**)** - 이전 요청자가 역할을 중지한 후 threat defense 디바이스가 인터페이스의 요청자 역할을 대신하기 전까지의 시간(초)입니다. 범위는 60~300입니다. 기본값은 255입니다.

단계 **5** **OK(**확인**)**를 클릭하여 IGMP 프로토콜 구성을 저장합니다.

IGMP 액세스 그룹 구성

액세스 제어 목록을 사용하여 멀티캐스트 그룹에 대한 액세스를 제어할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **Access Group(**액세스 그룹**)**을 선택합니다.

단계 **3** **Access Group(**액세스 그룹**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add IGMP Access Group parameters(IGMP 액세스 그룹 파라미터 추가**)** 대화 상자를 사용하여 액세스 그룹 테이블에 새 액세스 그룹을 추가합니다. **Edit IGMP Access Group parameters(IGMP** 액세스 그룹 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

a) **Interface(**인터페이스**)** 드롭다운 목록에서 액세스 그룹이 연결된 인터페이스를 선택합니다. 기존 액세스 그룹을 편집할 때는 연결된 인터페이스를 변경할 수 없습니다.

b) 다음 중 하나를 클릭합니다.

- **Standard Access List(**표준 액세스 목록**)** - **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정를 참조하십시오.
- **Extended Access List(**확장 액세스 목록**)** - **Extended Access List(**확장 액세스 목록**)** 드롭다운 목록에서 확장 ACL을 선택하거나 **Add(**추가**)** (+)을 클릭하여 새 확장 ACL을 생성합니다. 절차는 확장 ACL 개체 설정를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 액세스 그룹 구성을 저장합니다.

IGMP 고정 그룹 구성

그룹 멤버가 해당 그룹 멤버를 보고할 수 없거나 네트워크 세그먼트에 그룹 멤버가 없을 수 있지만 해당 그룹의 멀티캐스트 트래픽이 해당 네트워크 세그먼트로 전송되게 하려고 합니다. 고정 참여 IGMP 그룹을 구성하면 해당 그룹에 대한 멀티캐스트 트래픽을 해당 세그먼트로 보낼 수 있습니다. 이 방법을 통해 threat defense 디바이스는 패킷 자체를 수신하지 않고 전달만 합니다. 따라서 빠른 전환이 가능합니다. 발신 인터페이스가 IGMP 캐시에 나타나지만 이 인터페이스는 멀티캐스트 그룹의 멤버가 아닙니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Static Group(**고정 그룹**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add IGMP Static Group parameters(IGMP 고정 그룹 파라미터 추가**)** 대화 상자를 이용하여 멀티캐스트 그룹을 고정으로 인터페이스에 할당합니다. **Edit IGMP Static Group(IGMP** 고정 그룹 수정**)** 대화 상자를 이용하여 기존 고정 그룹 할당을 변경합니다.

참고 이 명령을 사용하는 방화벽이 명령이 적용되는 인터페이스의 PIM DR(Designated Router)인 경우 IGMP 고정 그룹을 사용하면 PIM에서 소스 또는 RP(Rendezvous Point)로 조인 요청을 전송할 수 있습니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 멀티캐스트 그룹을 고정으로 할당할 인터페이스를 선택합니다. 기존 항목을 편집할 경우 이 값을 변경할 수 없습니다.
- **Multicast Groups(**멀티캐스트 그룹**)** 드롭다운 목록에서 인터페이스를 할당할 멀티캐스트 그룹을 선택하거나 **Add(**추가**)** (+)을 클릭하여 새 멀티캐스트 그룹을 만들 수 있습니다. Creating Network Objects(네트워크 개체 생성)에서 절차를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 고정 그룹 구성을 저장합니다.

IGMP 조인 그룹 구성

인터페이스를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. threat defense 디바이스를 멀티캐스트 그룹에 참여하도록 구성하면 업스트림 라우터가 해당 그룹에 대한 멀티캐스트 라우팅 테이블 정보를 유지하고 해당 그룹에 대한 경로를 활성 상태로 유지하게 됩니다.

참고 특정 그룹에 대한 멀티캐스트 패킷을 인터페이스로 전달하면서 IGMP 고정 그룹 구성, 10 페이지 디바이스에서 패킷을 해당 그룹의 일부로 수락하지 않도록 하려면 threat defense 섹션을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Join Group(**조인 그룹**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add IGMP Join Group parameters(IGMP 조인 그룹 파라미터추가**)** 대화 상자에서 threat defense 디바이스를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. **Edit IGMP Join Group parameters(IGMP** 조인 그룹 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

참고 이 명령을 사용하는 방화벽이 명령이 적용되는 인터페이스의 PIM DR(Designated Router)인 경우 IGMP 조인 그룹을 사용하면 PIM에서 소스 또는 RP(Rendezvous Point)로 조인 요청을 전송할 수 있습니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 멀티캐스트 그룹의 멤버로 정할 인터페이스를 선택합니다. 기존 항목을 편집할 경우 이 값을 변경할 수 없습니다.
- **Join Group(**조인 그룹**)** 드롭다운 목록에서 인터페이스를 할당할 멀티캐스트 그룹을 선택하거나 **Plus(**더하기**)**를 클릭하여 새 멀티캐스트 그룹을 만들 수 있습니다. Creating Network Objects(네트워크 개체 생성)에서 절차를 참조하십시오.

PIM 기능 구성

라우터는 PIM을 사용하여 멀티캐스트 다이어그램 전달에 사용할 전달 테이블을 유지합니다. Secure Firewall Threat Defense 디바이스에서 멀티캐스트 라우팅을 활성화할 경우 PIM 및 IGMP가 모든 인터페이스에서 자동으로 활성화됩니다.

참고 PIM은 PAT에서 지원되지 않습니다. PIM 프로토콜은 포트를 사용하지 않고 PAT는 포트를 사용하는 프로토콜에서만 작동합니다.

이 섹션은 선택적인 PIM 설정을 구성하는 방법을 설명합니다.

프로시저

단계 **1** PIM 프로토콜 구성, 12 페이지.
단계 **2** PIM 네이버 필터 구성, 13 페이지.
단계 **3** PIM 양방향 네이버 필터 구성, 14 페이지.
단계 **4** PIM 랑데부 포인트 설정, 15 페이지.
단계 **5** PIM 라우트 트리 설정, 16 페이지.
단계 **6** PIM 요청 필터 설정, 17 페이지.
단계 **7** 멀티캐스트 경계 필터 설정, 20 페이지.

PIM 프로토콜 구성

특정 인터페이스에서 PIM을 활성화하거나 비활성화할 수 있습니다.

지정된 라우터(DR) 우선 순위를 구성할 수도 있습니다. DR은 PIM 등록, 참여 및 prune 메시지를 RP로 보내는 것을 담당합니다. 네트워크 세그먼트에 멀티캐스트 라우터가 하나 이상 있는 경우 DR 선택은 DR 우선 순위를 따릅니다. 여러 디바이스의 DR 우선 순위가 동일한 경우 IP 주소가 가장 높은 디바이스가 DR이 됩니다. 기본적으로 threat defense의 DR 우선 순위는 1입니다.

PIM DR 선택을 위해 라우터 쿼리 메시지가 사용될 수 있습니다. PIM DR은 라우터 쿼리 메시지 전송을 담당합니다. 기본적으로 라우터 쿼리 메시지는 30초마다 전송됩니다. 또한 threat defense는 60초마다 PIM 참여 또는 prune 메시지를 보냅니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Protocol(**프로토콜**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add PIM parameters(PIM 파라미터 추가**)** 대화 상자를 사용하여 새 PIM 파라미터를 디바이스에 추가합니다. **Edit PIM parameters(PIM** 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** - 드롭다운 목록에서 구성하려는 PIM 프로토콜에 대한 인터페이스를 선택합니다.
- **Enable PIM(PIM** 활성화**)** - PIM을 활성화하려면 확인란을 선택합니다.
- **DR Priority(DR** 우선 순위**)** - 선택한 인터페이스에 대한 DR 값입니다. 서브넷에서 DR 우선 순위가 가장 높은 라우터가 지정 라우터가 됩니다. 유효한 값의 범위는 0 ~ 4294967294입니다. 기본 DR 우선 순위는 1입니다. 이 값을 0으로 설정하면 threat defense 디바이스 인터페이스가 지정 라우터가 될 자격을 잃게 됩니다.
- **Hello Interval(Hello** 간격**)** - 인터페이스에서 PIM hello 메시지를 보내는 간격(초)입니다. 범위는 1~3600입니다. 기본값은 30입니다.
- **Join Prune Interval(**조인 **Prune** 간격**)** - 인터페이스에서 PIM 조인 및 prune 알림을 전송하는 간격(초)입니다. 범위는 10~600입니다. 기본값은 60입니다.

단계 **5** **OK(**확인**)**를 클릭하여 PIM 프로토콜 구성을 저장합니다.

PIM 네이버 필터 구성

PIM 네이버가 될 수 있는 라우터를 정의할 수 있습니다. PIM 네이버가 될 수 있는 라우터를 필터링함으로써 다음을 할 수 있습니다.

- 권한이 없는 라우터가 PIM 네이버가 되는 것을 막습니다.
- 연결된 stub 라우터가 PIM에 참여하는 것을 막습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Neighbor Filter(**네이버 필터**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add PIM Neighbor Filter(PIM 네이버 필터 추가**)** 대화 상자를 사용하여 새 PIM 네이버 필터를 디바이스에 추가합니다. **Edit PIM Neighbor Filter(PIM** 네이버 필터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 PIM 인접한 라우터 필터를 추가할 인터페이스를 선택합니다.
- **Standard Access List(**표준 액세스 목록**) - Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정를 참조하십시오.

  참고 **Add Standard Access List Entry(**표준 액세스 목록 항목 추가**)** 대화 상자에서 **Allow(**허용**)**를 선택하여 멀티캐스트 그룹 알림이 인터페이스를 통과하도록 합니다. **Block(**차단**)**을 선택하면 지정된 멀티캐스트 그룹 알림이 인터페이스를 통과할 수 없습니다. 인터페이스에서 멀티캐스트 경계가 구성된 경우 모든 멀티캐스트 트래픽은 네이버 필터 엔트리로 허용되지 않는 한 인터페이스를 통과할 수 없습니다.

단계 **5** **OK(**확인**)**를 클릭하여 PIM 네이버 필터 구성을 저장합니다.

PIM 양방향 네이버 필터 구성

PIM 양방향 네이버 필터는 네이버가 DF 선택에 참여할 수 있다고 정의하는 ACL입니다. 인터페이스에 대해 PIM 양방향 네이버 필터가 구성되지 않은 경우에는 제한 사항이 없습니다. PIM 양방향 네이버 필터가 구성된 경우 ACL에서 허용된 네이버만 DF 선택 프로세스에 참여할 수 있습니다.

양방향 PIM은 멀티캐스트 라우터가 축소된 상태 정보를 유지할 수 있게 합니다. 세그먼트의 모든 멀티캐스트 라우터가 양방향으로 활성화되어 있어야 DF를 선택할 수 있습니다.

PIM 양방향 네이버 필터가 활성화된 경우 ACL에 의해 허용된 라우터는 양방향을 지원하는 것으로 간주됩니다. 따라서 다음은 참입니다.

- 허용된 네이버가 양방향 모드를 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 네이버가 양방향 모드를 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 네이버가 양방향 모드를 지원하지 않을 경우 DF 선택이 일어날 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 2 **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 3 **Bidirectional Neighbor Filter(**양방향 네이버 필터**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add PIM Bidirectional Neighbor Filter(PIM 양방향 네이버 필터 추가**)** 대화 상자를 사용하여 PIM 양방향 네이버 필터 ACL에 대한 ACL 항목을 생성합니다. **Edit PIM Bidirectional Neighbor Filter(PIM** 양방향 네이버 필터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 4 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 PIM 양방향 네이버 필터 ACL 항목을 구성할 인터페이스를 선택합니다.
- **Standard Access List(**표준 액세스 목록**) - Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정를 참조하십시오.

  참고 **Add Standard Access List Entry(**표준 액세스 목록 항목 추가**)** 대화 상자에서 **Allow(**허용**)**를 선택하면 지정된 디바이스가 DR 선택 프로세스에 참여할 수 있습니다. **Block(**차단**)**을 선택하면 지정된 디바이스가 DF 선택 프로세스에 참여할 수 없습니다.

단계 5 **OK(**확인**)**를 클릭하여 PIM 양방향 네이버 필터 구성을 저장합니다.

PIM 랑데부 포인트 설정

threat defense 디바이스가 하나 이상의 그룹에 대해 RP 역할을 하도록 구성할 수 있습니다. ACL에 지정된 그룹 범위가 PIM RP 그룹 매핑을 결정합니다. ACL이 지정되지 않은 경우 해당 그룹에 대한 RP가 전체 멀티캐스트 그룹 범위(224.0.0.0/4)에 적용됩니다. 양방향 PIM에 대한 자세한 내용은 멀티캐스트 양방향 PIM, 3 페이지 섹션을 참조하십시오.

RP에는 다음 제한 사항이 적용됩니다.

- 동일한 RP 주소를 두 번 사용할 수 없습니다.
- 하나 이상의 RP에 All Groups를 지정할 수 없습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 2 **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Rendezvous Points(**랑데부 포인트**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add Rendezvous Point(랑데부 포인트 추가**)** 대화 상자를 사용하여 랑데부 포인트 테이블에 새로운 항목을 생성합니다. **Edit Rendezvous Point(**랑데부 포인트 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Rendezvous Point IP address(**랑데부 포인트 **IP** 주소**)** 드롭다운 목록에서 RP 역할로 추가할 IP 주소를 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 네트워크 개체를 만듭니다. Creating Network Objects(네트워크 개체 생성)에서 절차를 참조하십시오.
- 지정된 멀티캐스트 그룹이 양방향 모드에서 작동하는 경우 **Use bi-directional forwarding(**양방향 전달 사용**)** 확인란을 선택하십시오. 양방향 모드에서 threat defense 디바이스가 멀티캐스트 패킷을 수신하고 직접 연결된 멤버나 PIM 네이버가 없는 경우 다시 소스로 prune 메시지를 보냅니다.
- **Use this RP for all Multicast Groups(**모든 멀티캐스트 그룹에 대해 이 **RP** 사용**)**를 선택하여 인터페이스의 모든 멀티캐스트 그룹에 대해 지정된 RP를 사용합니다.
- **Use this RP for all Multicast Groups as specified below(**아래 지정된 대로 멀티캐스트 그룹에 이 **RP** 사용**)**를 클릭하여 지정된 RP와 함께 사용할 멀티캐스트 그룹을 지정한 다음 **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 랑데부 포인트 구성을 저장합니다.

PIM 라우트 트리 설정

기본적으로 PIM 리프 라우터는 첫 번째 패킷이 새로운 소스에 도달한 직후 가장 짧은 경로의 트리에 참여합니다. 이 방법은 지연을 줄이지만 공유 트리보다 더 많은 메모리가 필요합니다. 모든 멀티캐스트 그룹에 대해 또는 특정 멀티캐스트 주소에 한정하여 threat defense 디바이스가 최단 경로 트리에 참여할지 아니면 공유 트리를 사용할지 구성할 수 있습니다.

Multicast Groups(멀티캐스트 그룹) 테이블에 지정되지 않은 그룹에 대해서는 최단 경로 트리가 사용됩니다. Multicast Groups(멀티캐스트 그룹) 테이블은 공유 트리를 사용할 멀티캐스트 그룹을 표시합니다. 테이블 엔트리는 위에서 아래로 처리됩니다. 특정 그룹에 대한 거부 규칙을 테이블 상단에 배치하고 멀티캐스트 그룹 범위에 대한 허용 규칙을 거부 구문 아래에 배치하면 일정한 범위의 멀티캐스트 그룹을 포함하되 해당 범위 내 특정 그룹을 제외하는 엔트리를 만들 수 있습니다.

참고 이 동작은 SPT(Shortest Path Switchover)로 알려져 있습니다. 항상 공유 트리 옵션을 사용하는 것이 좋습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 2 **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 3 **Route Tree(**경로 트리**)**에서 경로 트리에 대한 경로를 선택합니다.

- **Shortest Path(**최단 경로**)**를 클릭하여 모든 멀티캐스트 그룹에 대해 최단 경로 트리를 사용합니다.
- **Shared Tree(**공유 트리**)**를 클릭하여 모든 멀티캐스트 그룹에 대해 공유 트리를 사용합니다.
- **Shared tree for below mentioned group(**아래 언급한 그룹에 대한 공유 트리**)**을 클릭하여 멀티캐스트 그룹 표에 명시된 그룹을 지정한 다음 **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 **Add(**추가**)** (+)을 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정를 참조하십시오.

단계 4 **OK(**확인**)**를 클릭하여 경로 트리 구성을 저장합니다.

PIM 요청 필터 설정

threat defense 디바이스가 RP 역할을 수행하는 경우 특정 멀티캐스트 소스의 등록을 제한하여 권한이 없는 소스가 RP에 등록하지 못하도록 할 수 있습니다. threat defense 디바이스가 PIM 레지스터 메시지를 수락하는 멀티캐스트 소스를 정의할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 2 **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 3 **Request Filter(**요청 필터**)**에서 threat defense 디바이스가 RP 역할을 할 때 등록을 허용할 멀티캐스트 소스를 정의합니다.

- **Filter PIM register messages using:(**다음을 사용하여 **PIM** 등록 메시지 필터링**)** 드롭다운 목록에서 **None(**없음**)**, **Access List(**액세스 목록**)** 또는 **Route Map(**경로 맵**)**을 선택합니다.
- 드롭다운 목록에서 **Access List(**액세스 목록**)**를 선택하는 경우, 확장 ACL을 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 확장 ACL을 생성합니다. 절차는 확장 ACL 개체 설정를 참조하십시오.

참고 **Add Extended Access List Entry(**확장 액세스 목록 항목 추가**)** 대화 상자에서 드롭다운 목록의 **Allow(**허용**)**를 선택하여 지정된 멀티캐스트 트래픽의 지정된 소스를 threat defense 디바이스에 등록할 수 있도록 허용하는 규칙을 생성하거나 **Block(**차단**)**을 선택하여 지정된 멀티캐스트 트래픽의 지정된 소스를 디바이스에 등록할 수 없도록 하는 규칙을 생성합니다.

- **Route Map(**경로 맵**)**을 선택하는 경우, **Route Map(**경로 맵**)** 드롭다운 목록에서 경로 맵을 선택하거나 **Add(**추가**)** (+)를 클릭하여 새로운 경로 맵을 만들 수 있습니다. Creating Network Objects(네트워크 개체 생성)에서 절차를 참조하십시오.

단계 **4** **OK(**확인**)**를 클릭하여 요청 필터 구성을 저장합니다.

Secure Firewall Threat Defense 디바이스를 후보 BSR(Bootstrap Router)로 구성

threat defense 디바이스를 후보 BSR로 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Bootstrap Router**에서 **Configure this FTD as a Candidate Bootstrap Router (C-BSR)(**이 **FTD**를 **C-BSR(Candidate Bootstrap Router)**로 구성**)** 확인란을 선택하여 C-BSR 설정을 수행합니다.

a) **Interface(**인터페이스**)** 드롭다운 목록에서 BSR 주소가 파생된 threat defense 디바이스에서 인터페이스를 선택하여 후보로 설정합니다.

이 인터페이스는 PIM을 사용하여 활성화되어야 합니다.

b) **Hash mask length(**해시 마스크 길이**)** 필드에서 해시 함수가 호출되기 전에 그룹 주소로 AND 처리할 마스크의 길이(최대 32비트)를 입력합니다. 시드 해시가 동일한 모든 그룹은 동일한 RP와 일치합니다. 예를 들어, 이 값이 24인 경우, 그룹 주소의 첫 번째 24비트만 중요합니다. 이를 통해 여러 그룹에 대해 하나의 RP를 얻을 수 있습니다. 범위는 0~32입니다.

c) **Priority(**우선 순위**)** 필드에서 후보 BSR의 우선 순위를 입력합니다. 더 큰 우선순위를 지닌 BSR이 우선시됩니다. 우선순위 값이 동일한 경우, 더 큰 IP 주소를 지닌 라우터는 BSR입니다. 범위는 0~255입니다. 기본값은 0입니다.

단계 **4** (선택 사항) **Add(**추가**)** (+)을 클릭하여 PIM BSR 메시지가 전송 또는 수신되지 않는 인터페이스를 **Configure this FTD as a Border Bootstrap Router (BSR)(**이 **FTD**를 **Border Bootstrap Router**로 구성**)** 섹션에서 선택합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 PIM BSR 메시지가 전송 또는 수신되지 않는 인터페이스를 선택합니다.

RP 또는 BSR 알림은 RP 정보 교환의 두 도메인을 효과적으로 격리하여 필터링됩니다.

- BSR을 활성화하려면 **Enable Border BSR(Border BSR 활성화)** 확인란을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 부트스트랩 라우터 구성을 저장합니다.

멀티캐스트 라우트 설정

고정 멀티캐스트 경로를 구성함으로써 유니캐스트 트래픽에서 멀티캐스트 트래픽을 분리할 수 있습니다. 예를 들어 소스와 목적지 사이의 경로가 멀티캐스트 라우팅을 지원하지 않을 경우 해결책은 두 멀티캐스트 디바이스 사이에 GRE 터널을 구성하여 멀티캐스트 패킷을 터널을 통해 전송하는 것입니다.

PIM을 사용하는 경우 threat defense 디바이스는 유니캐스트 패킷을 다시 소스로 보내는 인터페이스와 같은 인터페이스에서 패킷을 수신할 것으로 기대합니다. 멀티캐스트 라우팅을 지원하지 않는 경로를 바이패스할 때와 같이 일부 경우에서는 유니캐스트 패킷이 하나의 경로를 따르고 멀티캐스트 패킷이 다른 경로를 따르도록 할 수 있습니다.

고정 멀티캐스트 경로가 알려지거나 재배포되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **Multicast Routes(**멀티캐스트 경로**)** > **Add(**추가**)** 또는 **Edit(**편집**)**을 선택합니다.

Add Multicast Route Configuration(멀티캐스트 경로 구성 추가**)** 대화 상자를 사용하여 새로운 멀티캐스트 경로를 threat defense 디바이스에 추가합니다. **Edit Multicast Route Configuration(**멀티캐스트 경로 구성 편집**)** 대화 상자를 사용하여 기존 멀티캐스트 경로를 변경합니다.

단계 **3** **Source Network(**소스 네트워크**)** 드롭다운 상자에서 기존 네트워크를 선택하거나 **Add(**추가**)** (+)를 클릭하여 새 네트워크를 추가합니다. Creating Network Objects(네트워크 개체 생성)에서 절차를 참조하십시오.

단계 **4** 경로를 전달하도록 인터페이스를 설정하려면 **Interface(**인터페이스**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)** 드롭다운 목록에서 멀티캐스트 경로에 대한 수신 인터페이스를 선택합니다.
- **Output Interface/Dense(**출력 인터페이스**/Dense)** 드롭다운 목록에서 경로가 전달되는 대상 인터페이스를 선택합니다.
- **Distance(**거리**)** 필드에 멀티캐스트 경로 거리를 입력합니다. 범위는 0~255입니다.

단계 **5** 경로를 전달하도록 RPF 주소를 설정하려면 **Address(**주소**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

- **RPF Address(RPF** 주소**)** 필드에 멀티캐스트 경로의 IP 주소를 입력합니다.
- **Distance(**거리**)** 필드에 멀티캐스트 경로 거리를 입력합니다. 범위는 0~255입니다.

단계 **6** **OK(**확인**)**를 클릭하여 멀티캐스트 경로 구성을 저장합니다.

멀티캐스트 경계 필터 설정

주소 범위 지정은 도메인 경계 필터를 정의하여 같은 IP 주소를 가진 RP 도메인이 서로 섞이지 않도록 합니다. 범위 지정은 대형 도메인 내 서브넷 경계와 도메인과 인터넷 사이의 경계에서 이루어집니다.

멀티캐스트 그룹 주소에 대한 인터페이스에서 관리적으로 범위가 지정된 경계 필터를 설정할 수 있습니다. IANA는 관리적으로 범위가 지정된 주소로 239.0.0.0~239.255.255.255의 멀티캐스트 주소 범위를 지정했습니다. 이 주소 범위는 다른 조직이 관리하는 도메인에서 재사용될 수 있습니다. 주소는 전역에서 고유한 주소가 아닌 로컬 주소로 간주됩니다.

표준 ACL은 영향을 받는 주소의 범위를 정의합니다. 경계 필터를 설정할 때 어느 방향으로도 경계를 건너는 멀티캐스트 데이터 패킷 흐름은 허용되지 않습니다. 경계 필터를 통해 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있습니다.

자동 RP 검색 및 알림 메시지를 관리적으로 범위가 지정된 경계에서 구성, 검사 및 필터링할 수 있습니다. 경계 ACL에 의해 거부된 Auto-RP 패킷의 모든 Auto-RP 패킷 그룹 범위 알림은 삭제됩니다. Auto-RP 그룹 범위 알림은 Auto-RP 그룹 범위의 모든 주소가 경계 ACL에 의해 허용된 경우에만 경계 필터에서 허용 및 통과됩니다. 주소가 하나라도 허용되지 않은 경우 전체 그룹 범위가 필터링되고 Auto-RP 메시지가 전달되기 전에 Auto-RP 메시지에서 삭제됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **Multicast Boundary Filter(**멀티캐스트 경계 필터**)**를 선택한 다음 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add Multicast Boundary Filter(멀티캐스트 경계 필터 추가**)** 대화상자를 사용하여 새 멀티캐스트 경계 필터를 디바이스에 추가합니다. **Edit Multicast Boundary Filter(**멀티캐스트 경계 필터 편집**)** 대화상자를 사용하여 기존 파라미터를 변경합니다.

관리적으로 범위가 지정된 멀티캐스트 주소에 대한 멀티캐스트 경계를 구성할 수 있습니다. 멀티캐스트 경계는 멀티캐스트 데이터 패킷 흐름을 제한하고 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있게 합니다. 인터페이스에서 특정 멀티캐스트 경계가 정의된 경우 필터 ACL에 의해 허용된 멀티캐스트 트래픽만 인터페이스를 통과합니다.

단계 **3** **Interface(**인터페이스**)** 드롭다운 목록에서 멀티캐스트 경계 필터 ACL을 구성할 인터페이스를 선택합니다.

단계 **4** **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 **Add(**추가**)** (+)을 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정를 참조하십시오.

단계 **5** 경계 ACL에 의해 거부된 소스에서 Auto-RP 메시지를 필터링하려면 **Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary(**경계 **ACL**에 의해 거부된 **Auto-RP** 패킷의 모든 **Auto-RP** 패킷 그룹 범위 알림 제거**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 모든 Auto-RP 메시지가 전달됩니다.

단계 **6** **OK(**확인**)**를 클릭하여 멀티캐스트 경계 필터를 저장합니다.