보안 IP 멀티캐스트 구축

목차

소개

이 문서에서는 IP 멀티캐스트 네트워크 인프라를 보호하기 위한 모범 사례에 대한 일반적인 지침을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IP 멀티캐스트

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 몇 가지 기본 개념, 용어에 대해 설명하고 다음과 같은 주제에 대해 설명합니다.

- 일반적으로 특정 플랫폼과 네트워크를 보호하는 메커니즘.
- 모든 ASM(Source Multicast) 및 SSM(Source Specific Multicast) 모델
- 멀티캐스트 MVPN(Virtual Private Network) 보안.
- 멀티캐스트 데이터 플레인 또는 컨트롤 플레인 트래픽에 대해 기밀성과 무결성을 제공하는 GET(Group Encrypted Transport) VPN(Virtual Private Network) 아키텍처입니다.

용어

IP 멀티캐스트에는 두 가지 기존 서비스 모델이 있습니다.

1. 모든 ASM(Source Multicast)

2. SSM(Source Specific Multicast)

ASM에서 수신기는 IGMP(Internet Group Membership Protocol) 또는 MLD(Multicast Listener Discovery) 멤버십 보고서를 통해 그룹 G에 가입하여 그룹을 나타냅니다. 이 보고서는 모든 소스에서 그룹 G로 전송된 트래픽을 요청하므로 이름이 "any source"입니다. 반면, SSM에서는 수신자가 소스 S에 의해 정의된 특정 채널에 합류하여 그룹 G에 전송합니다. 이러한 서비스 모델 각각에 대해서는 아래에서 자세히 설명합니다.

모든 소스 멀티캐스트

ASM 모델은 두 가지 프로토콜 클래스로 구성됩니다. "dense mode flood-and-prune" 및 "sparse mode explicit join":

i) Dense Mode Flood-and-Prune 프로토콜(DVMRP/MOSPF/PIM-DM)

Dense 모드 프로토콜에서는 네트워크의 모든 라우터가 모든 트리, 해당 소스 및 수신기를 인식합니다. DVMRP(Distance Vector Multicast Routing Protocol) 및 PIM(Protocol Independent Multicast) dense mode 정보와 같은 프로토콜은 전체 네트워크에 "활성 소스" 정보를 플러딩하고, 특정 트리의 트래픽이 원치 않는 토폴로지의 일부에 "Prune State(정리 상태)"를 생성하여 트리를 구축합니다. 플러드 및 정리 프로토콜이라고도 합니다. MOSPF(Multicast Open Shortest Path First)에서는 트리의 구축을 지원하기 위해 네트워크 전체에 수신자에 대한 정보가 플러딩됩니다.

네트워크의 일부 영역에 구축된 모든 트리는 네트워크의 모든 라우터(구성된 경우 관리 범위 내)에 리소스 사용률(컨버전스 영향 포함)을 항상 유발할 수 있으므로 Dense 모드 프로토콜은 바람직하지 않습니다. 이러한 프로토콜은 이 글의 나머지 부분에서 더 이상 논의되지 않는다.

ii) 스파스 모드 명시적 조인 프로토콜(PIM-SM/PIM-BiDir)

스파스 모드 명시적 조인 프로토콜의 경우, 수신자가 그룹에 대한 명시적 IGMP/MLD 멤버십 보고서(또는 "조인")를 전송하지 않는 한 디바이스는 네트워크에서 그룹별 상태를 생성하지 않습니다. ASM의 이 변형은 확장성이 뛰어난 것으로 알려져 있으며 멀티캐스트 중점 패러다임입니다.

이는 대부분의 멀티캐스트 구축에서 이 시점에 사용한 PIM-Sparse Mode의 기본입니다. 이는 많은(소스) - 많은(수신기) 애플리케이션에 점점 더 많이 구축되고 있는 양방향 PIM(PIM-BiDir)의 기반이기도 합니다.

이러한 프로토콜은 "스파스" 수신기 모집단의 IP 멀티캐스트 전달 트리를 효율적으로 지원하고 소스와 수신기 간의 경로에 있는 라우터에서만 컨트롤 플레인 상태를 생성하므로 스파스 모드라고 합니다. 또한 PIM-SM/BiDir에서는 RP(Rendezvous Point)입니다. 네트워크의 다른 부분에서는 상태를 생성하지 않습니다. 라우터의 상태는 다운스트림 라우터 또는 수신자로부터 조인을 수신할 때만 명시적으로 작성됩니다. 따라서 이름은 "명시적 조인 프로토콜"입니다.

PIM-SM과 PIM-BiDir은 모두 "공유 트리"를 사용하므로 모든 소스의 트래픽이 수신자에게 전달될 수 있습니다. 공유 트리의 멀티캐스트 상태를 (*,G) 상태라고 합니다. 여기서 *는 ANY SOURCE의

와일드카드입니다. 또한 PIM-SM은 특정 소스의 트래픽과 관련된 상태 생성을 지원합니다. 이를 SOURCE TREE라고 하며, 관련 상태를 (S,G) 상태라고 합니다.

소스별 멀티캐스트

SSM은 수신기(또는 일부 프록시)가 (S,G) "조인"을 전송하여 소스 S가 그룹 G로 보낸 트래픽을 수신하도록 표시할 때 사용되는 모델입니다. 이는 IGMPv3/MLDv2 "INCLUDE" 모드 멤버십 보고서를 통해 가능합니다. 이 모델을 SSM(Source-Specific Multicast) 모델이라고 합니다. SSM은 라우터 간에 명시적 조인 프로토콜을 사용하도록 지정합니다. 이를 위한 표준 프로토콜은 PIM-SSM이며, 이는 (S,G) 트리를 생성하는 데 사용되는 PIM-SM의 하위 집합입니다. SSM에 공유 트리(*,G) 상태가 없습니다.

따라서 멀티캐스트 수신자는 ASM 그룹 G에 "가입"하거나 SSM(S,G) 채널에 "가입"할 수 있습니다. "ASM 그룹 또는 SSM 채널"이라는 용어가 반복되지 않도록 하기 위해 (멀티캐스트) 플로우라는 용어가 사용됩니다. 이는 플로우가 ASM 그룹 또는 SSM 채널일 수 있음을 의미합니다.

관련 멀티캐스트 프로토콜/패킷 유형

멀티캐스트 네트워크를 보호하려면 일반적으로 발생하는 패킷 유형 및 이를 차단하는 방법을 이해하는 것이 중요합니다. 다음과 같은 세 가지 주요 프로토콜이 있습니다.

1. IGMP / MLD
2. PIM
3. MSDP

다음 절에서는 이러한 각각의 프로토콜과 각각의 프로토콜에서 발생할 수 있는 문제들에 대해 각각 논의한다.

IGMP/MLD 패킷

IGMP/MLD는 멀티캐스트 수신자가 특정 멀티캐스트 그룹에 대한 콘텐츠를 수신할 라우터에 신호를 보내는 데 사용하는 프로토콜입니다. IGMP(Internet Group Membership Protocol)는 IPv4에서 사용되는 프로토콜이고 MLD(Multicast Listener Discovery)는 IPv6에서 사용되는 프로토콜입니다.

일반적으로 구축되는 두 가지 버전의 IGMP는 IGMPv2와 IGMPv3입니다. 또한 일반적으로 구축되는 두 가지 버전의 MLD는 MLDv1과 MLDv2입니다.

IGMPv2와 MLDv1은 기능적으로 동일하며, IGMPv3와 MLDv2는 기능적으로 동일하다.

이러한 프로토콜은 다음 링크에 지정됩니다.

IGMPv2: RFC 2236

MLDv1: RFC 3590

IGMPv3 및 MLDv2: RFC 4604

IGMPv2 및 IGMPv3는 프로토콜일 뿐만 아니라 IPv4 IP 프로토콜(특히 프로토콜 번호 2)입니다. 이 RFC에 설명된 대로 멀티캐스트 그룹 멤버십을 보고하는 데 사용될 뿐만 아니라 DVMRP, PIM 버전 1, mtrace 및 mrinfo 같은 다른 IPv4 멀티캐스트 프로토콜에서도 사용됩니다. 이는 IGMP를 필터링할 때(예: Cisco IOS® ACL을 통해) 기억해야 합니다. IPv6에서 MLD는 IPv6 프로토콜이 아닙니다. 대신 ICMPv6는 MLD 패킷을 전달하는 데 사용됩니다. PIM 버전 2는 IPv4 및 IPv6에서 동일한 프로토콜 유형입니다(프로토콜 번호 103).

PIM 제어 패킷

이 섹션에서는 멀티캐스트 및 유니캐스트 PIM 제어 패킷에 대해 설명합니다. Auto-RP와 BSR(Bootstrap Router)은 PIM-SM 네트워크에서 랑데부 포인트를 선택하고 Group-to-RP 할당을 제어하는 방법입니다.

멀티캐스트 PIM 제어 패킷

멀티캐스트 PIM 제어 패킷에는 다음이 포함됩니다.

- **PIM Hello** - PIM Hello 패킷은 PIM 인접 디바이스를 설정하기 위해 동일한 네트워크에 연결된 라우터로 전송되는 링크-로컬 범위 IP 멀티캐스트 패킷입니다.
- **PIM Join/Prune** - PIM Join/Prune은 멀티캐스트 상태를 생성/제거하기 위해 전송되는 링크-로컬 범위 IP 멀티캐스트 패킷이며 PIM 인접 디바이스로만 전송됩니다. 어설션, 보고 억제 및 기타 PIM 프로토콜 세부사항을 용이하게 하기 위해 LAN 내에서 멀티캐스트되지만, 항상 특정 네이버로 전달됩니다.
- **PIM DF-elect** - PIM Designated Forwarder는 연결된 수신기 또는 다운스트림 PIM 네이버 대신 RP로 전송되는 (*,G) 조인을 담당하는 Bi-Dir PIM 라우터입니다. PIM 라우터가 동일한 그룹 G에 대해 동일한 세그먼트에서 (*,G) JOINS를 전송하는 다른 라우터를 탐지하는 경우, RP에 대한 최상의 경로를 가진 라우터를 확인하는 선택이 있습니다.
- **PIM Assert** - PIM Assert는 특정 인터페이스(S,G)에 대한 패킷을 특정 인터페이스에서 능동적으로 전달하는 네트워크 세그먼트에 연결된 PIM 라우터가 전달된 동일한(S,G)에 대한 패킷을 동일한 인터페이스에서 수신하기 시작할 때 전송되는 링크 로컬 IP 멀티캐스트 패킷입니다. 이 이벤트는 해당 라우터(S,G)에 대해 SF(Single Forwarder)라고 생각하는 다른 라우터가 있음을 나타냅니다. Assert 메커니즘은 해당(S,G)에 대해 고유한 SF를 선택합니다. PIM SF 라우터는 특정(S,G) 스트림에 대한 패킷을 전달하도록 선택됩니다. PIM을 사용하면 서로 다른 라우터가 서로 다른 (S,G)를 대신하여 SF의 역할을 수행할 수 있습니다. 이상적으로 (S,G)당 SF는 하나뿐입니다. SF와 지정된 라우터를 혼동하지 마십시오. PIM 전용 라우터는 PIM-SM 네트워크의 RP로 전송되는 JOIN/PRUNES 또는 소스 레지스터를 담당하는 라우터입니다.
- **PIM 부트스트랩** - PIM 부트스트랩 메시지가 PIMv2 네트워크에서 전송되어 특정 그룹 G에 대한 Rendezvous Point를 동적으로 선택할 수 있게 합니다.

유니캐스트 PIM 제어 패킷

유니캐스트 PIM 제어 패킷은 RP로 전송되거나 RP에서 전송되며 다음과 같습니다.

- **Source Register Packet**(소스 레지스터 패킷) - PIM 소스 레지스터 패킷을 전송하여 Rendezvous Point에 새 멀티캐스트 소스를 등록합니다. 소스가 멀티캐스트 패킷을 전송하기 시작하면 즉시, 소스 네트워크에 연결된 전용 라우터는 RP에 유니캐스트 레지스터 스트림을

전송하여 RP가 담당하는 멀티캐스트 그룹에 대해 활성 소스가 있음을 나타냅니다.
소스 레지스터 패킷은 원래 멀티캐스트 스트림의 유니캐스트 캡슐화로서 전송됩니다.
PIM 레지스터 메시지는 프로세스 레벨 전환되며 RP가 레지스터 중지 메시지를 보낼 때까지만 전송됩니다. 이러한 패킷의 성능 영향은 소스(S,G) 흐름당 속도에 비례합니다.

- **Register Stop Packet(**등록 중지 패킷) - PIM 등록 중지 패킷은 Rendezvous Point에서 등록 메시지를 전송한 PIM DR로 전송됩니다. Register Stop 메시지는 RP가 소스에서 기본적으로 멀티캐스트 패킷을 수신하기 시작하는 즉시 전송됩니다.
- **BSR Candidate-Rendezvous Point Advertisement Packet** - PIM BSR C-RP-Advertisement Packets는 BSR이 선택되면 BSR로 전송되어 후보 RP를 광고합니다.

그림 1: PIM 유니캐스트 패킷

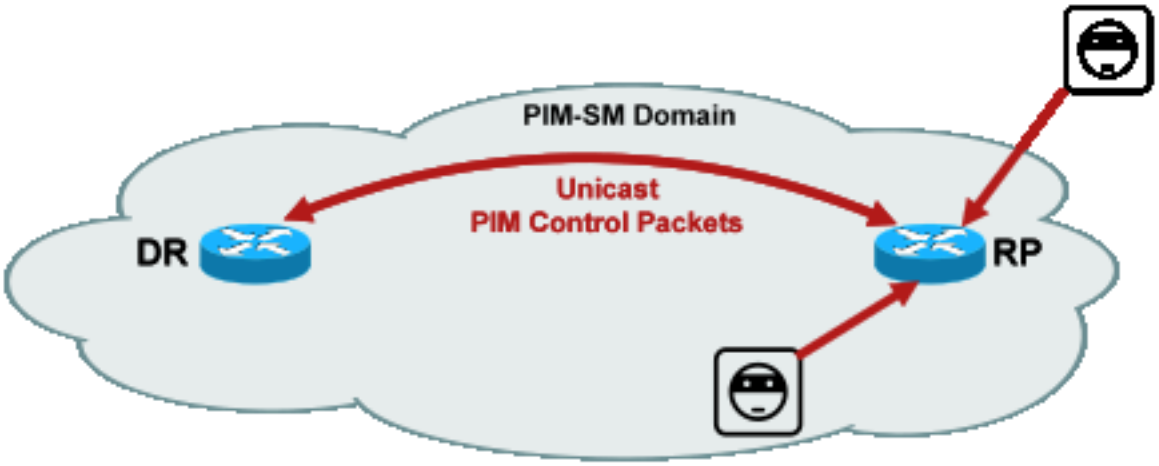


Fig1

_PIM_unicast

이러한 패킷을 악용하는 공격은 유니캐스트 패킷이므로 어디서든 발생할 수 있습니다.

Auto-RP 패킷

Auto-RP는 Cisco에서 개발한 프로토콜로서 PIMv2 BSR과 동일한 용도로 사용됩니다. Auto-RP는 BSR 이전에 개발되었으며 IPv4만 지원합니다. BSR은 IPv4 및 IPv6를 지원합니다. Auto-RP의 매핑 에이전트는 BSR의 부트스트랩 라우터와 동일한 기능을 수행합니다. BSR에서는 C-RP의 메시지가 부트스트랩 라우터에 유니캐스트됩니다. Auto-RP에서 메시지는 나중에 설명하는 것처럼 경계에서 더 쉬운 필터를 허용하는 매핑 에이전트로 멀티캐스트를 통해 전송됩니다. Auto-RP에 대해서는 다음 링크에서 자세히 설명합니다.
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Cisco IOS에서는 AutoRP/BSR 패킷이 항상 전달되고 현재 비활성화되지 않습니다. 이는 Auto-RP의 경우 특정 보안 노출을 나타낼 수 있습니다.

그림 2: Auto-RP 패킷

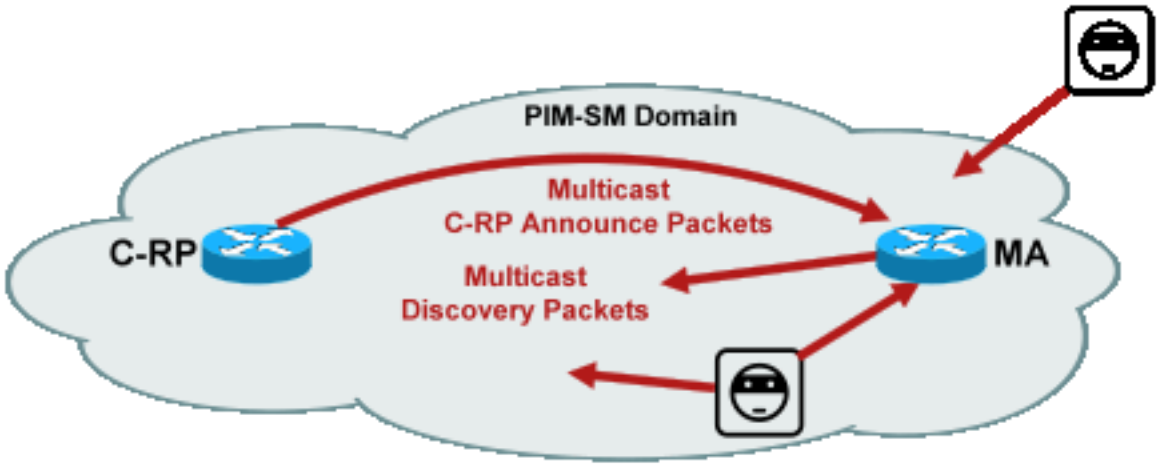


그림 2_AutoRP_packets

참고: Auto-RP는 PIM-SM RP 공지 및 검색을 위한 메커니즘으로 사용되지만 PIM 패킷(IP 프로토콜 103)을 사용하지 않습니다. 대신 멀티캐스트 주소가 있는 UDP(User Datagram Protocol) 포트 496 패킷을 사용합니다.

Auto-RP에서 사용하는 패킷 유형은 두 가지입니다.

- C-RP-Announce 패킷: 이러한 패킷은 모든 매핑 에이전트로 멀티캐스트되며 IANA(Internet Assigned Numbers Authority) 예약된 "잘 알려진" 주소(224.0.1.39)를 사용합니다. RP가 RP로 작동할 수 있는 RP 주소 및 그룹 범위를 알리기 위해 C-RP에 의해 전송됩니다.
- C-RP 검색 패킷: 이러한 패킷은 모든 PIM 라우터에 멀티캐스트되며 IANA 예약 "잘 알려진" 주소(224.0.1.40)를 사용합니다. Auto-RP 매핑 에이전트에서 특정 그룹 범위의 RP로 선택된 특정 C-RP를 알립니다.

이러한 각 패킷 유형은 네트워크를 통해 플러딩됩니다.

Cisco IOS에서는 224.0.1.39와 224.0.1.40이 PIM Dense Mode에서 모두 전달되므로, 해당 그룹이 RP 정보를 배포하는 데 사용될 때 해당 그룹에 대한 RP에 대한 사전 지식이 없는 문제가 방지됩니다. 이는 PIM Dense Mode의 유일한 권장 사용입니다.

Cisco IOS XR에서 Auto-RP 메시지는 인접 디바이스에서 인접 디바이스로의 홉별로 RPF(Reverse Path Forwarding) 플러딩 홉입니다. 따라서 Cisco IOS XR에서 Auto-RP를 지원하기 위해 PIM DM mroute 상태를 생성할 필요가 없습니다. 실제로 Cisco IOS XR는 PIM-DM을 전혀 지원하지 않습니다.

MSDP(Multicast Service Discovery Protocol) 패킷

MSDP는 IPv4 프로토콜로서 한 도메인의 소스가 각 랑데부 지점을 통해 다른 도메인의 수신기에 알려지도록 합니다. MSDP는 RFC 3618에 지정됩니다.

PIM 도메인 간에 활성 소스에 대한 정보를 공유하기 위해 MSDP가 사용됩니다. 소스가 한 도메인에서 활성화되면 MSDP는 모든 피어 도메인이 이 새 소스에 대해 적시에 학습하도록 합니다. 그러면 수신자가 관심을 갖는 그룹으로 전송된 경우 다른 도메인의 수신자가 이 새 소스에 신속하게 연결

할 수 있습니다. MSDP는 ASM/PIM-SM 멀티캐스트 통신에 필요하며 각 도메인의 Rendezvous Point 간에 구성된 유니캐스트 TCP(Transport Control Protocol) 연결을 통해 실행됩니다.

멀티캐스트 환경의 위협

신뢰 및 신뢰 경계의 영역

문서의 이 섹션은 네트워크의 기능 엔터티별로 구성됩니다. 앞서 설명한 위협 모델은 이러한 엔터티를 중심으로 형성됩니다. 예를 들어, 이 문서에서는 라우터가 구축된 위치와 상관없이 멀티캐스트 관점에서 멀티캐스트 네트워크의 라우터를 보호하는 방법에 대해 설명합니다. 마찬가지로, 네트워크 전반의 보안 조치를 구축하는 방법, 또는 전용 라우터, 랑데부 지점 등에 대한 조치를 구축하는 방법에 대해서도 고려해야 합니다

여기에 설명된 위협도 이러한 논리를 따르며, 네트워크의 논리적 기능에 따라 구성됩니다.

위협 개요

추상적인 수준에서, 모든 멀티캐스트 구축은 보안의 다양한 측면에 대한 여러 위협의 영향을 받을 수 있습니다. 보안의 주요 측면은 기밀성, 무결성 및 가용성입니다.

- **기밀성에 대한 위협**: 대부분의 애플리케이션에서 멀티캐스트 트래픽은 암호화되지 않으므로 경로의 모든 회선 또는 네트워크 요소에서 수신 대기하거나 캡처할 수 있도록 누구에게나 개방됩니다. GET VPN에 대한 섹션에서는 이러한 공격을 방지하기 위해 멀티캐스트 트래픽을 암호화하는 방법에 대해 설명합니다.
- **트래픽 무결성에 대한 위협**: GET VPN과 같은 애플리케이션 수준 보안 또는 네트워크 기반 보안이 없으면 멀티캐스트 트래픽은 전송 중 수정될 가능성이 높습니다. 이는 OSPF, PIM 및 기타 여러 프로토콜과 같은 멀티캐스트를 사용하는 컨트롤 플레인 트래픽에서 특히 중요합니다.
- **네트워크 무결성에 대한 위협**: 이 문서에 설명된 보안 메커니즘이 없으면 무단 발신자, 수신자 또는 손상된 네트워크 요소가 멀티캐스트 네트워크에 액세스하거나 권한 없이 트래픽을 주고받거나(서비스 도난) 네트워크 리소스에 과부하가 발생할 수 있습니다.
- **가용성에 대한 위협**: 합법적인 사용자가 리소스를 사용할 수 없게 만들 수 있는 서비스 거부 공격 가능성이 많습니다.

다음 섹션에서는 네트워크의 각 논리적 기능에 대한 위협에 대해 설명합니다.

라우터에 대한 기본 위협

라우터가 멀티캐스트를 지원하는지, 그리고 공격이 멀티캐스트 트래픽이나 프로토콜을 포함하는지 여부와 관계없이 라우터에 대한 여러 가지 근본적인 위협이 있습니다.

DoS(서비스 거부) 공격은 네트워크에서 가장 중요한 일반 공격 벡터입니다. 원칙적으로 모든 네트워크 요소는 DoS 공격의 표적이 될 수 있으며, 이로 인해 적법한 사용자에 대한 잠재적인 후속 서비스 손실 또는 저하로 요소를 오버로드할 수 있습니다. 유니캐스트에 적용되는 기본 네트워크 보안

권장 사항을 따르는 것이 가장 중요합니다.

멀티캐스트 공격이 항상 의도적인 것이 아니라 종종 우발적인 것이라는 점이 중요합니다. 예를 들어 2004년 3월에 처음 관찰된 위티 웜은 IP 주소에 대한 무작위 공격을 통해 확산된 웜의 한 예입니다. 주소 공간의 완전한 임의 지정으로 인해 멀티캐스트 IP 대상도 웜의 영향을 받았습니다. 많은 조직에서 웜이 여러 가지 다른 멀티캐스트 대상 주소로 패킷을 전송했기 때문에 많은 첫 번째 홉 라우터가 축소되었습니다. 그러나 라우터는 관련 상태 생성과 함께 그러한 멀티캐스트 트래픽 로드의 범위를 정하지 않았으며 효과적으로 리소스 소진을 경험했습니다. 이는 엔터프라이즈에서 멀티캐스트가 사용되지 않는 경우에도 멀티캐스트 트래픽을 보호해야 하는 필요성을 보여줍니다.

라우터에 대한 일반적인 위협은 다음과 같습니다.

- 모든 유형의 패킷 플러드; 예를 들어, 느린(punt) 경로와 같은 하드웨어 경로, SSH(Secure Shell), 텔넷, BGP(Border Gateway Protocol), OSPF, NTP(Network Time Protocol) 등을 포함하는 관리 또는 제어 평면 포트와 같은 소프트웨어 경로에 대해 설명합니다
- 라우터의 기능을 차후에 악용하면서 라우터에 침입하는 행위 약한 텔넷 또는 SSH 암호 및 약한 SNMP(Simple Network Management Protocol) 커뮤니티 문자열은 최신 네트워크에서 흔히 발생하는 문제입니다.
- 컨피그레이션 오류 또는 내부자 공격과 같은 운영 문제는 전체 네트워크 및 해당 트래픽의 보안을 위협할 수 있습니다.

라우터에서 멀티캐스트가 활성화된 경우 유니캐스트 외에도 보호되어야 합니다. IP 멀티캐스트를 사용해도 근본적인 위협 모델은 변경되지 않습니다. 그러나 공격을 받을 수 있는 추가 프로토콜(PIM, IGMP, MLD, MSDP)을 지원하므로 특별히 보호해야 합니다. 유니캐스트 트래픽이 이러한 프로토콜에서 사용되는 경우 위협 모델은 라우터에서 실행하는 다른 프로토콜과 동일합니다.

멀티캐스트 트래픽은 기본적으로 "수신기 중심"이며 원격 대상을 대상으로 할 수 없기 때문에 라우터를 공격하는 유니캐스트 트래픽과 같은 방식으로 사용할 수 없습니다. 공격 대상이 멀티캐스트 스트림에 명시적으로 "연결"되어야 합니다. 대부분의 경우(Auto-RP가 주요 예외) 라우터는 "링크 로컬" 멀티캐스트 트래픽만 수신 및 수신합니다. 링크 로컬 트래픽은 전달되지 않습니다. 따라서 멀티캐스트 패킷을 사용하는 라우터에 대한 공격은 직접 연결된 공격자에서만 발생할 수 있습니다.

소스 측의 위협

PC 또는 비디오 서버가 네트워크와 동일한 관리 제어 하에 있지 않을 때도 있습니다. 따라서 네트워크 사업자의 입장에서는 송신자가 대부분 신뢰할 수 없는 것으로 취급된다. PC와 서버의 강력한 기능과 복잡한 보안 설정(불완전한 경우가 많음)을 고려할 때 발신자는 멀티캐스트를 비롯한 모든 네트워크에 대해 실질적인 위협을 가합니다. 이러한 위협은 다음과 같습니다.

- **레이어 2 공격:** 레이어 2에는 다양한 유형의 공격을 수행하기 위한 다양한 공격 양식이 있습니다. 이는 유니캐스트 및 멀티캐스트에 적용됩니다. 이러한 공격 양식은 멀티캐스트에 국한되지 않으므로 이 문서에서는 자세히 설명하지 않습니다. 자세한 내용은 Cisco 보도 자료 "LAN 스위치 보안", ISBN-10을 참조하십시오. 1-58705-467-1 .
- **멀티캐스트 트래픽**으로 공격**:** 앞서 설명한 것처럼, 그룹에 대한 리스너가 없는 경우 첫 번째 홉

라우터가 멀티캐스트 트래픽을 전달하지 않으므로 멀티캐스트 트래픽으로 공격을 진행하기가 어렵습니다. 그러나 첫 번째 홉은 멀티캐스트 패킷으로 다양한 방법으로 공격을 받을 수 있습니다.

- 네트워크 포화 공격: 공격자는 가용 대역폭의 활용도를 초과하여 멀티캐스트 패킷을 세그먼트로 플러딩할 수 있으며, 이는 DoS 상태로 이어질 수 있습니다.
- 멀티캐스트 상태 공격: 첫 번째 홉 라우터는 멀티캐스트 패킷으로 플러딩되어 너무 많은 상태와 그에 따른 DoS 공격 상태를 생성할 수 있습니다.
- 발신자는 전송된 PIM Hello를 통해 PIM DR이 되려고 시도할 수 있습니다. 이러한 경우 LAN을 오가는 트래픽이 발생하지 않습니다.
- BiDir-PIM DF에 대한 PIM DF 선택 패킷은 스푸핑될 수 있습니다. 이러한 경우 LAN을 오가는 트래픽이 발생하지 않습니다.
- 발신자는 AutoRP RP-discovery 또는 BSR 부트스트랩 메시지를 스푸핑할 수 있습니다. 이렇게 하면 가짜 RP를 효과적으로 알리고 PIM-SM/BiDir 서비스를 중단하거나 중단합니다.
- 발신자는 PIM source register/register-stop 메시지와 같은 유니캐스트 공격을 소싱하거나 BSR 알림 패킷을 보내고 가짜 BSR을 알릴 수 있습니다.
- 필터링되지 않는 한 발신자는 유효한 멀티캐스트 그룹에 전송할 수 있습니다. 소스 주소가 스푸핑되어 에지에서 차단되지 않는 경우, 발신자는 합법적인 발신자의 소스 IP 주소를 사용할 수 있으며, 네트워크의 일부에서 콘텐츠를 재정의할 수 있습니다.
- 컨트롤 플레인 프로토콜에 대한 멀티캐스트 공격: OSPF 및 DHCP(Dynamic Host Configuration Protocol)와 같이 멀티캐스트와 연결되지 않은 여러 프로토콜에서는 멀티캐스트 패킷을 사용하며, 이 패킷을 사용하여 이러한 프로토콜을 공격할 수 있습니다
- **마스커레이드(Masquerade):** 발신자가 다른 발신자인 것처럼 가장할 수 있는 여러 공격 양식이 있습니다. 스푸핑된 소스 IP 주소는 그러한 공격 형태 중 하나입니다.
- **서비스 도용:** 발신자를 통제하지 않는 한, 발신자 측에서 부정한 방법으로 멀티캐스트 서비스를 이용할 수 있다.

참고: 일반적으로 호스트는 PIM 패킷을 보내거나 받지 않습니다. 이를 수행하는 호스트는 공격을 시도할 수 있습니다.

수신자 측의 위협

또한 수신기는 일반적으로 상당한 CPU 전력 및 대역폭을 사용하는 플랫폼이며 다양한 공격 형태를 허용합니다. 이는 대부분 발신자 측의 위협과 동일합니다. 레이어 2 공격은 중요한 공격 벡터로 남아 있습니다. 공격 벡터가 일반적으로 IGMP(또는 앞서 언급한 대로 레이어 2 공격)라는 점을 제외하면 수신기 측에서도 가짜 수신기 및 서비스 도난이 가능합니다.

Rendezvous Point 및 BSR에 대한 위협

PIM-SM RP 및 PIM-BSR은 멀티캐스트 네트워크의 중요한 지점이므로 공격자의 중요한 표적입니다. 첫 번째 홉 라우터가 아닐 경우 PIM 유니캐스트를 포함하는 유니캐스트 공격 양식만 이러한 요소에 직접 대상이 될 수 있습니다. RP 및 BSR에 대한 위협은 다음과 같습니다.

- "라우터에 대한 기본 위협" 섹션에 설명된 모든 일반 공격 양식
- 스푸핑된 소스 IP 주소를 사용하는 PIM 유니캐스트 공격은 악의적인 디바이스에서 전송하는 PIM 레지스터 또는 레지스터 중지 메시지를 통해 DoS 공격을 허용합니다.

멀티캐스트 및 유니캐스트 보안(비교)

상태 고려 사항/필터

소스, 3개의 수신기(A, B, C), 스위치(S1), 2개의 라우터(R1 및 R2)를 보여 주는 그림 3의 토폴로지를 생각해 보십시오. 파란색 선은 유니캐스트 스트림을 나타내고 빨간색 선은 멀티캐스트 스트림을 나타냅니다. 세 수신기 모두 멀티캐스트 흐름의 멤버입니다.

그림 3: 라우터 및 스위치의 복제

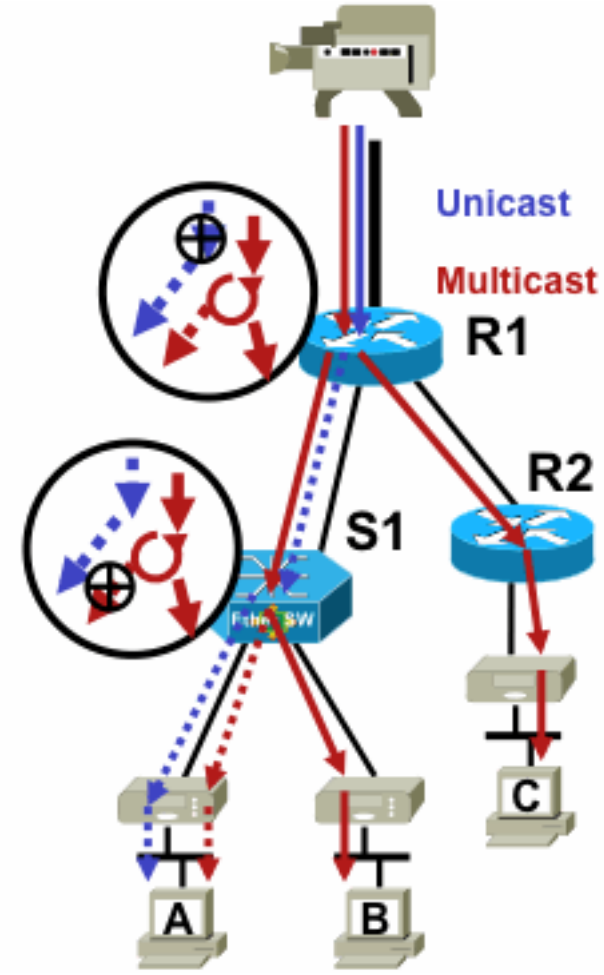


그림 3_replication_RS

특정 소스에서 특정 수신기로의 트래픽 흐름을 금지하려면

- 유니캐스트 스트림의 경우 발신자에서 수신자까지의 경로 어디에나 필터를 설치합니다.
- 그러나 멀티캐스트 스트림의 경우 관리자는 필터를 설치할 위치를 보다 구체적으로 지정해야 합니다. 수신기측 필터에서 수신기까지의 마지막 복제 지점 뒤에 소스 뒤의 첫 번째 복제 지점 앞에 있는 소스 측 필터.

멀티캐스트 소스의 공격

이 섹션은 ASM 및 SSM 서비스 모델 모두에 적용되며, 수신자측 명시적 조인의 수신에 따라 트래픽

이 전달됩니다.

유니캐스트 스트림의 경우 암시적 수신기 보호가 없습니다. 유니캐스트 소스는 이 대상에서 트래픽을 요청하지 않은 경우에도 목적지로 트래픽을 전송할 수 있습니다. 따라서 엔드포인트를 보호하기 위해 방화벽과 같은 방어 메커니즘이 일반적으로 사용됩니다. 반면 멀티캐스트는 프로토콜에 내장된 몇 가지 암시적 보호 기능이 있습니다. 트래픽은 문제의 흐름에 합류한 수신기에만 도달하는 것이 좋습니다.

ASM을 사용하면 소스에서 활성 RP에서 지원하는 모든 그룹에 대한 멀티캐스트 트래픽 전송을 통해 트래픽 삽입 또는 DoS 공격을 시작할 수 있습니다. 이 트래픽은 이상적으로는 수신기에 도달하지 않지만, 경로의 첫 번째 홉 라우터 및 제한적인 공격을 허용하는 RP에 최소한 도달할 수 있습니다. 그러나 악의적인 소스가 대상 수신자가 관심 있는 그룹을 알고 적절한 필터가 없는 경우 해당 그룹에 트래픽을 전송할 수 있습니다. 이 트래픽은 수신자가 그룹의 수신 대기하는 동안 수신됩니다.

SSM을 사용하면 원치 않는 소스에 의한 공격은 해당 (S,G) 채널에 참여한 수신자가 없는 경우 트래픽이 중단되는 첫 번째 홉 라우터에서만 가능합니다. 수신기에서 명시적인 조인 상태가 존재하지 않는 모든 SSM 트래픽을 무시하므로 첫 번째 홉 라우터에 대한 상태 공격으로 이어지지 않습니다. 이 모델에서는 "조인"이 소스별로 다르기 때문에 악의적인 소스에서 대상이 어떤 그룹에 관심이 있는지 알기에 충분하지 않습니다. 여기서는 스푸핑된 IP 소스 주소와 잠재적 라우팅 공격이 성공해야 합니다.

국가 공격

네트워크에 수신기가 없어도 PIM-SM은 소스에 가장 가까운 첫 번째 홉 라우터 및 Rendezvous Point에 (S,G) 및 (*,G) 상태를 생성합니다. 따라서 소스 첫 번째 홉 라우터의 네트워크 및 PIM-SM RP에서 상태 공격이 발생할 가능성이 있습니다.

악의적인 소스가 트래픽을 여러 그룹에 전송하기 시작하면 탐지된 각 그룹에 대해 네트워크의 라우터가 소스 및 RP에서 상태를 생성합니다. 단, 문제의 그룹이 RP 컨피그레이션에 의해 허용되어야 합니다.

따라서 PIM-SM은 소스의 상태 및 트래픽 공격을 받습니다. 소스가 올바른 접두사 내에서 소스 IP 주소를 임의로 변경하거나, 다시 말해, 주소의 호스트 비트만 스푸핑되는 경우 공격이 악화될 수 있습니다.

그림 4: ASM RP 공격

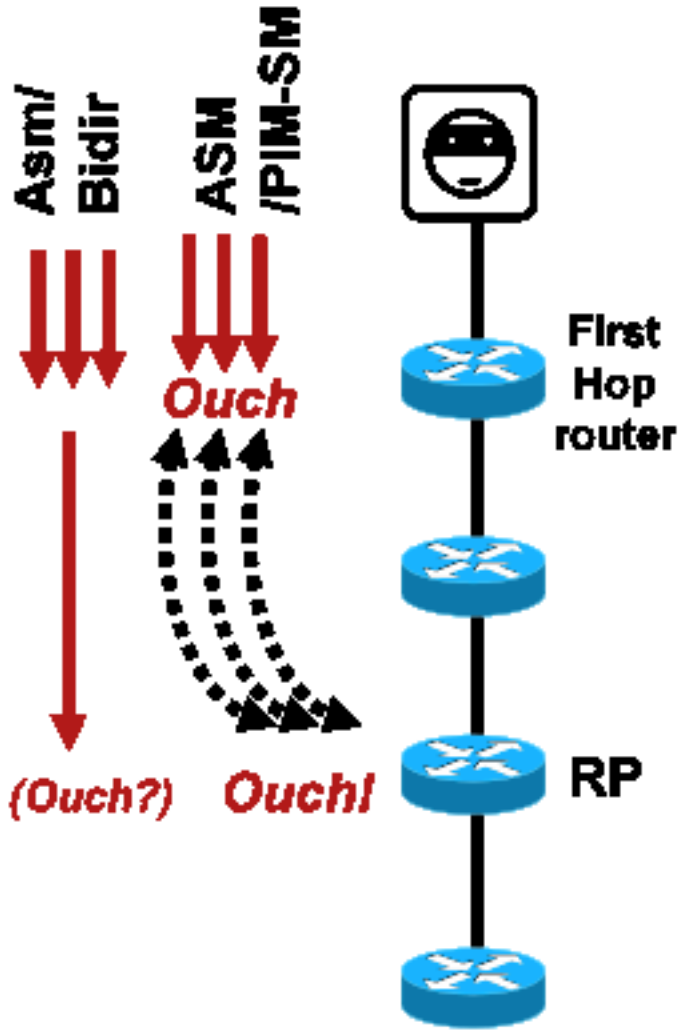


그림 4_ASM_RP_Attacks

PIM-SSM과 마찬가지로 소스로부터의 PIM-BiDir 상태 생성 공격은 불가능합니다. PIM-BiDir의 트래픽은 RP로 전달된 트래픽 뿐만 아니라 수신자의 조인에 의해 생성된 상태로 전달됩니다. 따라서 조인은 RP로만 이동하므로 RP 뒤에 있는 수신자에 도달할 수 있습니다. RP로의 상태-전달 트래픽은 (*,G/M) 상태라고 하며 RP 컨피그레이션(정적, 자동 RP, BSR)에 의해 생성됩니다. 출처가 있는 경우에는 변경되지 않습니다. 따라서 공격자는 PIM-BiDir RP에 멀티캐스트 트래픽을 보낼 수 있지만 PIM-SM과 달리 PIM-BiDir RP는 "활성" 엔터티가 아니며 대신 PIM-BiDir 그룹에 대한 트래픽을 전달하거나 버립니다.

> **참고:** 일부 Cisco IOS 플랫폼(*,G/M) 상태는 지원되지 않습니다. 이러한 경우 소스가 여러 PIM-BiDir 그룹에 대한 멀티캐스트 트래픽 전송으로 라우터를 공격할 수 있으며, 이로 인해 (*,G) 상태가 생성됩니다. 예를 들어 Catalyst 6500 스위치는 (*,G/M) 상태를 지원합니다.

수신자가 시작한 공격

공격은 멀티캐스트 수신기에서 발생할 수 있습니다. IGMP/MLD 보고서를 전송하는 모든 수신기는 일반적으로 첫 번째 홉 라우터에 상태를 생성합니다. 유니캐스트에는 상응하는 메커니즘이 없습니다.

그림 5: 수신측 명시적 조인 기반 트래픽 포워딩

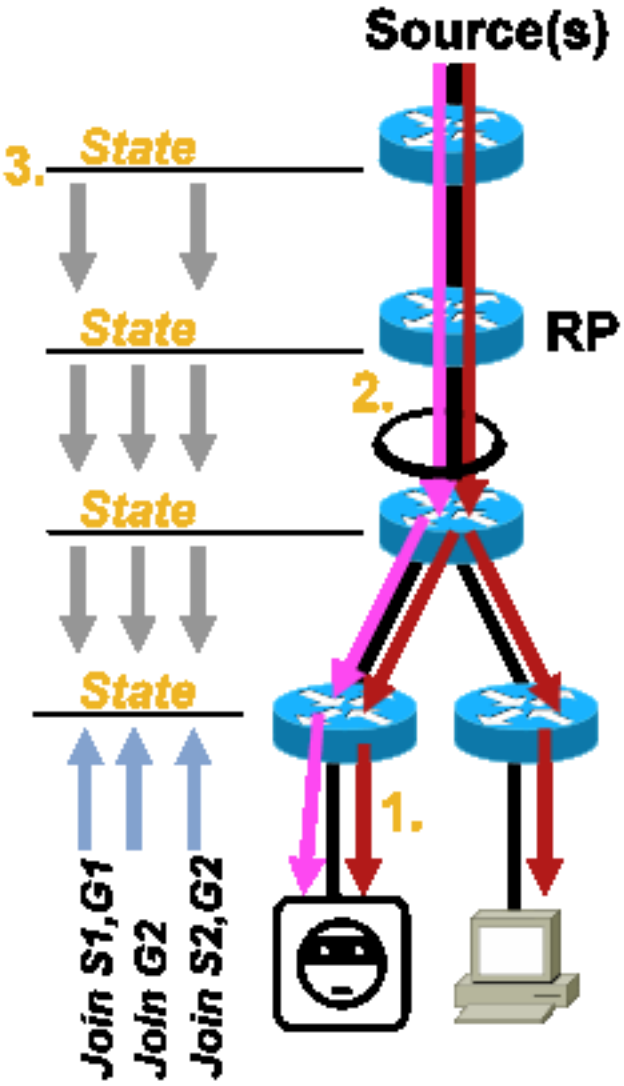


그림5_Receiver_Explicit_Join

수신기 공격은 다음 세 가지 유형이 될 수 있습니다.

1. 멀티캐스트 수신자는 승인되지 않은 플로우에 참가를 시도하고 승인되지 않은 콘텐츠를 수신하려고 시도할 수 있습니다.
2. 멀티캐스트 수신기는 여러 그룹 또는 채널에 관심을 가져 잠재적으로 사용 가능한 네트워크 대역폭을 오버로드할 수 있습니다. 이러한 종류의 공격은 다른 잠재적 콘텐츠 수신자에 대한 공유 대역폭 공격이 됩니다.
3. 멀티캐스트 수신기는 라우터 또는 스위치에 대한 공격을 시도할 수 있습니다. 대량의 멀티캐스트 트리 상태를 생성하고 라우터 용량을 과부하 상태로 만들 수 있는 많은 수의 IGMP 보고서를 생성할 수 있습니다. 그러면 멀티캐스트 통합 시간이 증가하거나 라우터의 DoS가 증가할 수 있습니다.

다음 섹션인 Security within a Multicast Network(멀티캐스트 네트워크 내의 보안)에서 이러한 종류의 공격을 완화하는 다양한 방법

멀티캐스트 네트워크 내의 보안

네트워크 요소 보안

보안은 포인트 기능이 아니라 모든 네트워크 설계의 본질적인 부분입니다. 따라서 네트워크의 모든 지점에서 보안을 고려해야 합니다. 모든 네트워크 요소를 적절하게 보호하는 것이 무엇보다 중요합니다. 모든 기술에 적용할 수 있는 한 가지 가능한 공격 시나리오는 침입자에 의해 파괴되는 라우터입니다. 침입자가 라우터를 제어하게 되면 공격자는 다양한 공격 시나리오를 실행할 수 있습니다. 따라서 각 네트워크 요소는 모든 유형의 기본 공격은 물론 특정 멀티캐스트 공격에도 적절하게 보호되어야 합니다.

CoPP(컨트롤 플레인 정책)

CoPP는 Router ACL(rACL)의 발전이며 대부분의 플랫폼에서 사용할 수 있습니다. 원칙은 같다. 라우터로 향하는 트래픽만 CoPP에 의해 폴리싱됩니다.

서비스 정책은 정책 맵 및 클래스 맵과 함께 QoS(quality of service) 정책과 동일한 구문을 사용합니다. 따라서 컨트롤 플레인을 향하는 특정 트래픽에 대해 속도 제한기를 사용하여 rACL(허용/거부)의 기능을 확장합니다.

> **참고:** Catalyst 9000 Series 스위치와 같은 특정 플랫폼에서는 기본적으로 CoPP가 활성화되어 있으며 보호가 대체되지 않습니다. 자세한 내용은 CoPP 가이드를 참조하십시오.

라이브 네트워크에서 rACL 또는 CoPP를 조정, 수정 또는 생성하려는 경우 주의해야 합니다. 두 기능 모두 컨트롤 플레인에 대한 모든 트래픽을 필터링할 수 있으므로 필요한 모든 컨트롤 플레인 및 관리 플레인 프로토콜이 명시적으로 허용되어야 합니다. 필요한 프로토콜의 목록이 커서 TACACS(Terminal Access Controller Access Control System)와 같은 덜 명확한 프로토콜을 간과하기 쉽습니다. 모든 기본이 아닌 rACL 및 CoPP 컨피그레이션은 프로덕션 네트워크에 구축하기 전에 항상 랩 환경에서 테스트해야 합니다. 또한 초기 구축은 "허용" 정책으로만 시작해야 합니다. 이렇게 하면 ACL 적중 카운터로 예기치 않은 적중을 검증할 수 있습니다.

멀티캐스트 환경에서 멀티캐스트가 제대로 작동하려면 rACL 또는 CoPP에서 필요한 멀티캐스트 프로토콜(PIM, MSDP, IGMP 등)을 허용해야 합니다. PIM-SM 시나리오에서는 소스의 멀티캐스트 스트림에 있는 첫 번째 패킷을 제어 플레인 패킷으로 사용하여 디바이스의 제어 플레인에서 멀티캐스트 상태를 생성하는 데 도움이 됩니다. 따라서 rACL 또는 CoPP에서 관련 멀티캐스트 그룹을 허용하는 것이 중요합니다. 플랫폼별 예외 사항이 많으므로 구축 전에 관련 문서를 참조하고 계획된 컨피그레이션을 테스트하는 것이 중요합니다.

LPTS(Local Packet Transport Service)

Cisco IOS XR에서 LPTS(Local Packet Transport Service)는 Cisco IOS의 CoPP와 마찬가지로 라우터의 컨트롤 플레인에 대한 트래픽의 폴리서 역할을 합니다. 또한 유니캐스트 및 멀티캐스트 트래픽을 포함하는 수신 트래픽을 필터링하고 속도를 제한할 수 있습니다.

멀티캐스트 전용 보안

멀티캐스트 지원 네트워크에서 각 네트워크 요소는 멀티캐스트 전용 보안 기능으로 보호되어야 합니다. 이 섹션에서는 일반 라우터 보호를 위해 간략하게 설명합니다. 모든 라우터에 필요하지 않지만 네트워크의 특정 위치에만 필요한 기능 및 라우터 간의 상호 작용(예: PIM 인증)이 필요한 기능에 대해서는 다음 섹션에서 설명합니다.

Mroute 제한

mroute limit 명령은 라우터에서 전역적으로 멀티캐스트 경로의 양을 제한하며 DoS 공격을 방지하는 데 도움이 됩니다.

```
ip multicast route-limit <mroute-limit> <warning-threshold>
```

그림 6: Mroute 제한

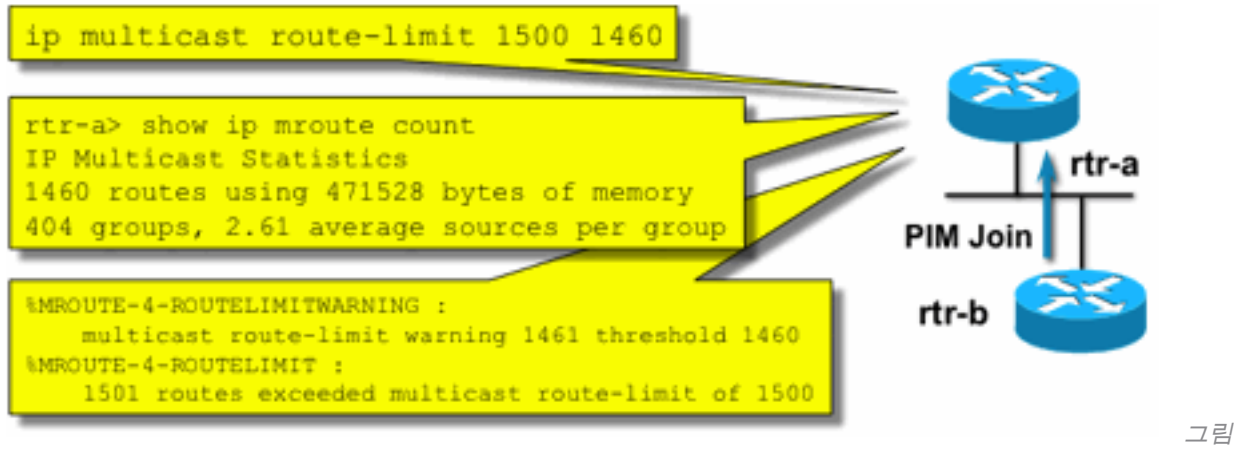


그림 6_Mroute_Limits

Mroute 제한은 멀티캐스트 라우팅 테이블에 허용된 mroute 수에 대한 임계값을 설정할 수 있도록 합니다. 멀티캐스트 경로 제한이 활성화된 경우 구성된 제한을 초과하는 멀티캐스트 상태가 생성되지 않습니다. 경고 임계값도 있습니다. 경로 수가 경고 임계값을 초과하면 syslog 경고 메시지가 트리거됩니다. 경로 제한에서 상태를 트리거할 추가 패킷은 삭제됩니다.

ip multicast route-limit 명령도 MVRF별로 사용할 수 있습니다.

SAP 수신 비활성화: ip sap 수신 거부

sap listen 명령을 사용하면 라우터가 SAP/SDP(Session Announcement Protocol/Session Description Protocol) 메시지를 수신합니다. SAP/SDP는 MBONE(Multicast Backbone) 시절의 레거시 프로토콜입니다. 이러한 메시지는 향후 또는 현재 사용할 수 있는 멀티캐스트 콘텐츠에 대한 디렉토리 정보를 나타냅니다. 라우터 CPU 및 메모리 리소스에 대한 DoS 소스일 수 있으므로 이 기능을 비활성화해야 합니다.

mrinfo 정보에 대한 액세스 제어 - "ip multicast mrinfo-filter" 명령

mrinfo 명령(Cisco IOS 및 일부 Microsoft Windows 및 Linux 버전에서도 사용 가능)은 다양한 메시지를 사용하여 멀티캐스트 라우터에 정보를 쿼리합니다. **ip multicast mrinfo-filter** global configuration 명령을 사용하여 이 정보에 대한 액세스를 소스의 하위 집합으로 제한하거나 완전히 비활성화할 수 있습니다.

다음 예에서는 192.168.1.1에서 제공된 쿼리를 거부하지만 다른 모든 소스에서 쿼리가 허용됩니다.

```
ip multicast mrinfo-filter 51

access-list 51 deny 192.168.1.1
access-list 51 permit any
```
이 예에서는 다음을 거부합니다 *mrinfo* 모든 소스의 요청:

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

> **참고:** 모든 ACL에서 예상한 대로, *거부*는 패킷이 필터링됨을 의미하고 허용은 *패킷*이 허용됨을 의미합니다.

mrinfo **명령**을 진단 목적으로 사용하는 경우 소스 주소의 하위 집합에서만 쿼리를 허용하도록 적절한 ACL을 사용하여 **ip multicast mrinfo-filter 명령**을 구성하는 것이 좋습니다. mrinfo 명령에서 제공하는 *정보*는 SNMP를 통해서도 검색할 수 있습니다. mrinfo 요청의 전체 블록(디바이스의 쿼리에서 모든 소스 차단)을 사용하는 것이 좋습니다.

네트워크 보안

이 섹션에서는 PIM 멀티캐스트 및 유니캐스트 제어 패킷을 보호하는 다양한 방법, Auto-RP 및 BSR에 대해 설명합니다.

멀티캐스트 그룹 비활성화

ip multicast **group-range/ipv6 multicast group range 명령**을 사용하여 ACL에서 거부된 그룹에 대한 모든 작업을 비활성화할 수 있습니다.

```
ip multicast group-range <std-acl>
ipv6 multicast group-range <std-acl>
```
ACL에서 거부된 그룹에 대해 패킷이 나타나는 경우 PIM, IGMP, MLD, MSDP를 비롯한 모든 제어 프로토콜에서 패킷이 삭제되고 데이터 플레인에서도 삭제됩니다. 따라서 이러한 그룹 범위에 대해 IGMP/MLD 캐시 엔트리, PIM, Multicast Routing Information Base/MRIB(Multicast Forwarding Information Base) 상태가 생성되지 않으며 모든 데이터 패킷이 즉시 삭제됩니다.

이러한 명령은 디바이스의 전역 컨피그레이션에 입력됩니다.

권장 사항은 네트워크의 모든 라우터에 이 명령을 구축하여 사용 가능한 시간과 장소에서 네트워크 외부에서 시작되는 모든 멀티캐스트 트래픽을 제어하는 것입니다. 이러한 명령은 데이터 플레인 및 컨트롤 플레인에 영향을 줍니다. 사용 가능한 경우 이 명령은 표준 ACL보다 더 광범위한 적용 범위를 제공하므로 이 명령을 사용하는 것이 좋습니다.

PIM 보안

PIM 네이버 제어

PIM 인접 디바이스를 설정하려면 PIM 라우터가 PIM Hello를 수신해야 합니다. PIM 네이버십은

DR(Designated Router) 선택 및 DR 장애 조치와 전송/수신된 PIM Join/Prune/Assert 메시지의 기반이기도 합니다.

그림 7: PIM 네이버 제어

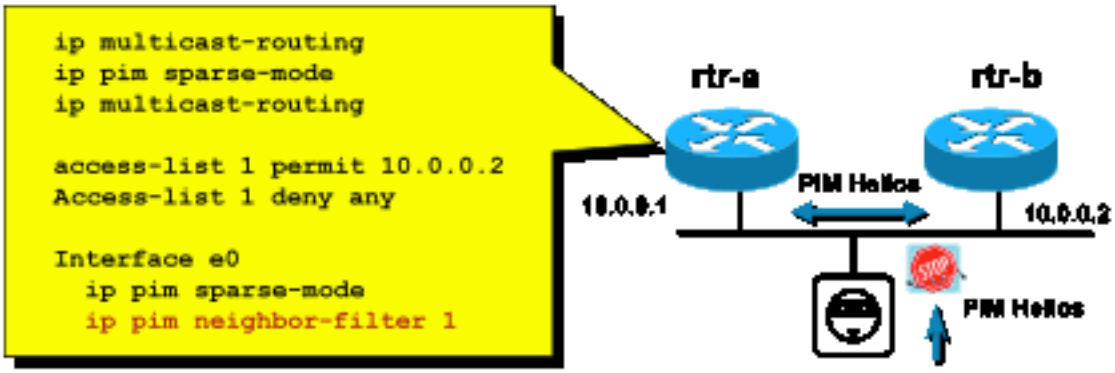


Fig7_PIM_neighbor_control

원치 않는 인접 디바이스를 금지하려면 **ip pim neighbor-filter** 그림 7에 표시된 명령입니다. 이 명령은 Hello, Join/Prune 패킷 및 BSR 패킷을 포함하는 모든 비허용 인접 디바이스 PIM 패킷에서 필터링합니다. 세그먼트의 호스트는 PIM 네이버인 것처럼 가장하기 위해 소스 IP 주소를 스푸핑할 수 있습니다. 세그먼트의 스푸핑 시도로부터 소스 주소를 방지하거나 액세스 스위치에서 VLAN ACL을 사용하여 호스트의 PIM 패킷을 방지하려면 레이어 2 보안 메커니즘(즉, IP 소스 가드)이 필요합니다. ACL에서 "log-input" 키워드를 사용하여 ACE와 일치하는 패킷을 기록할 수 있습니다.

PIM Join/Prune 패킷이 PIM 인접 디바이스로 전송되어 특정 (S,G) 또는 (*,G) 경로에서 해당 인접 디바이스를 추가하거나 제거합니다. PIM 멀티캐스트 패킷은 TTL(Time-To-Live)=1로 전송된 링크 로컬 멀티캐스트 패킷입니다. 이러한 모든 패킷은 잘 알려진 All-PIM-Routers 주소로 멀티캐스트됩니다. 224.0.0.13 . 즉, 이러한 모든 공격은 공격을 받은 라우터와 동일한 서브넷에서 시작해야 합니다. 공격에는 위조된 Hello, Join/Prune 및 Assert 패킷이 포함될 수 있습니다.

> **참고:** PIM 멀티캐스트 패킷의 TTL 값을 1보다 큰 값으로 인위적으로 높이거나 조정해도 문제가 발생하지 않습니다. All-PIM-Routers 주소는 항상 라우터에서 로컬로 수신되고 처리됩니다. 일반 및 합법적인 라우터에서 직접 전달하지 않습니다.

PIM-SM 레지스터 메시지의 잠재적인 플러드로부터 RP를 보호하려면 DR에서 해당 메시지를 속도 제한해야 합니다. ip pim **register-rate-limit 명령을** 사용합니다.

ip pim register-rate-limit <count>

그림 8: PIM-SM 레지스터 터널 제어

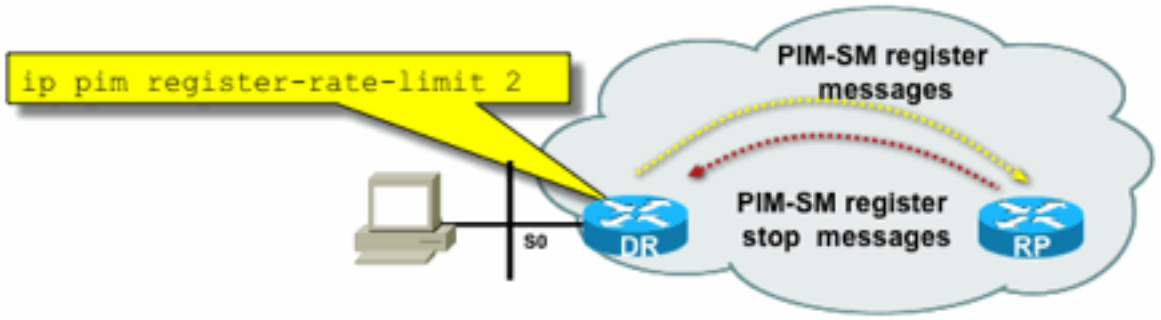


그림 8_PIMSM_RegTunnel

PIM 유니캐스트 패킷을 사용하여 RP를 공격할 수 있습니다. 따라서 RP는 이러한 공격에 대해 인프라 ACL로 보호될 수 있습니다. 멀티캐스트 발신자 및 수신자는 PIM 패킷을 전송할 필요가 없으므로 PIM 프로토콜(IP 프로토콜 103)은 일반적으로 가입자 에지에서 필터링될 수 있습니다.

Auto-RP Control - RP Announce 필터

ip pim rp-announce filter 명령은 가능한 경우 Auto-RP로 구성할 수 있는 추가 보안 조치입니다.

ip pim rp-announce-filter
매핑 에이전트에서 어떤 라우터를 그룹 범위/그룹 모드에 대한 후보 RP로 수락할지를 제어하도록 구성할 수 있습니다.

그림 9: Auto-RP - RP Announce 필터

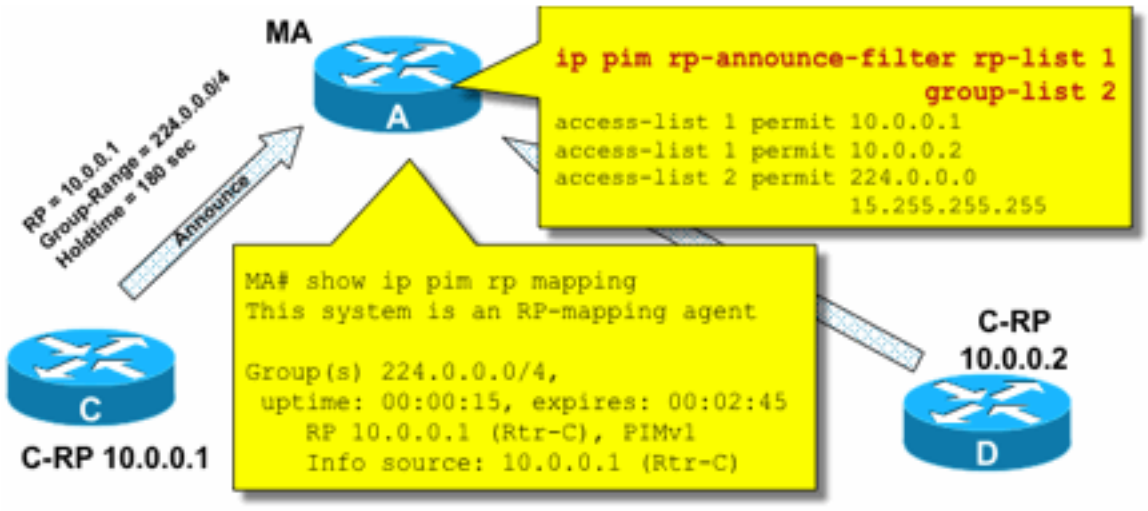


그림 9_AutoRP_RP_Announce

Auto-RP 제어 - Auto-RP 메시지 제한

AutoRP 패킷, RP-announce(224.0.1.39) 또는 RP-discover(224.0.1.40)를 특정 PIM 도메인으로 제한하려면 multicast boundary 명령을 사용합니다.

```
ip multicast boundary
```

그림 10: 멀티캐스트 경계 명령

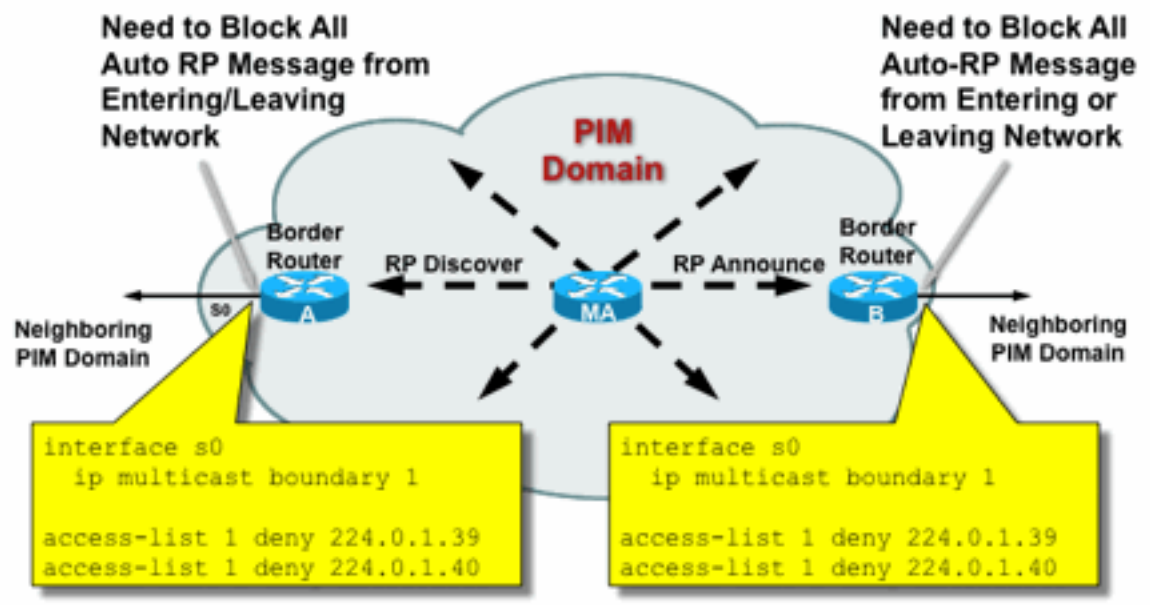


그림 10_Mcast_Boundary

BSR 제어 - BSR 메시지 제한

이 **ip pim bsr-border** pim 도메인 경계에서 BSR 메시지를 필터링하는 명령입니다. BSR 메시지는 링크 로컬 멀티캐스트와 함께 hop-by-hop 전달되므로 ACL이 필요하지 않습니다.

그림 11: BSR 경계

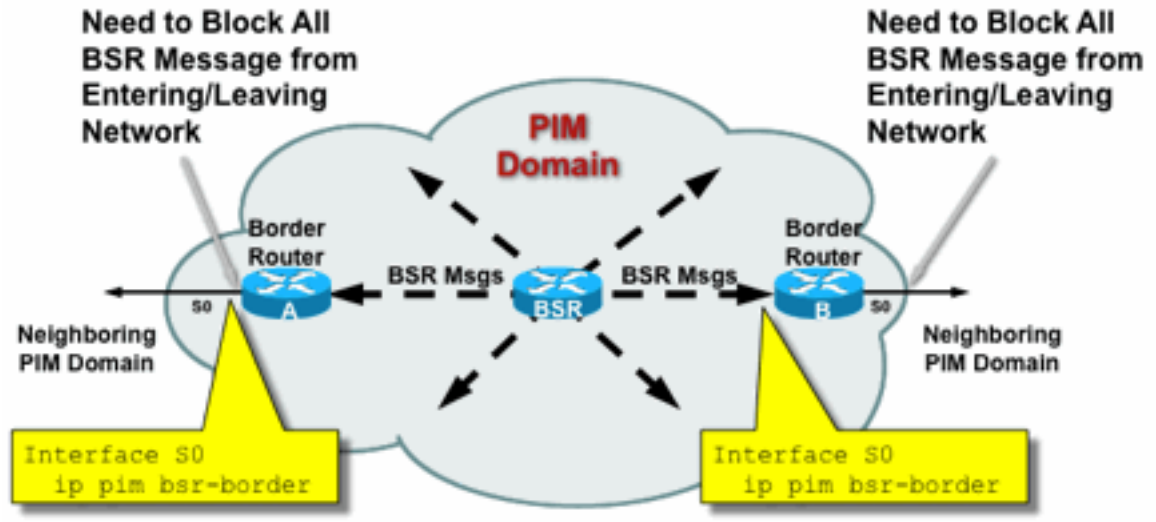


Fig11_BSR_Rout

er

RP/PIM-SM 관련 필터

이 마지막 섹션에서는 PIM-SP 및 RP 제어 플레인 패킷과 Auto-RP, BSR 및 MSDP 메시지에 대한 필터에 대해 설명합니다.

Auto-RP 필터

그림 12는 주소 범위와 함께 Auto-RP 필터의 예를 보여줍니다. 영역을 바인딩하는 두 가지 다른 방법이 표시됩니다. 두 ACL은 Auto-RP 관점에서 동일합니다.

그림 12: Auto-RP 필터/범위

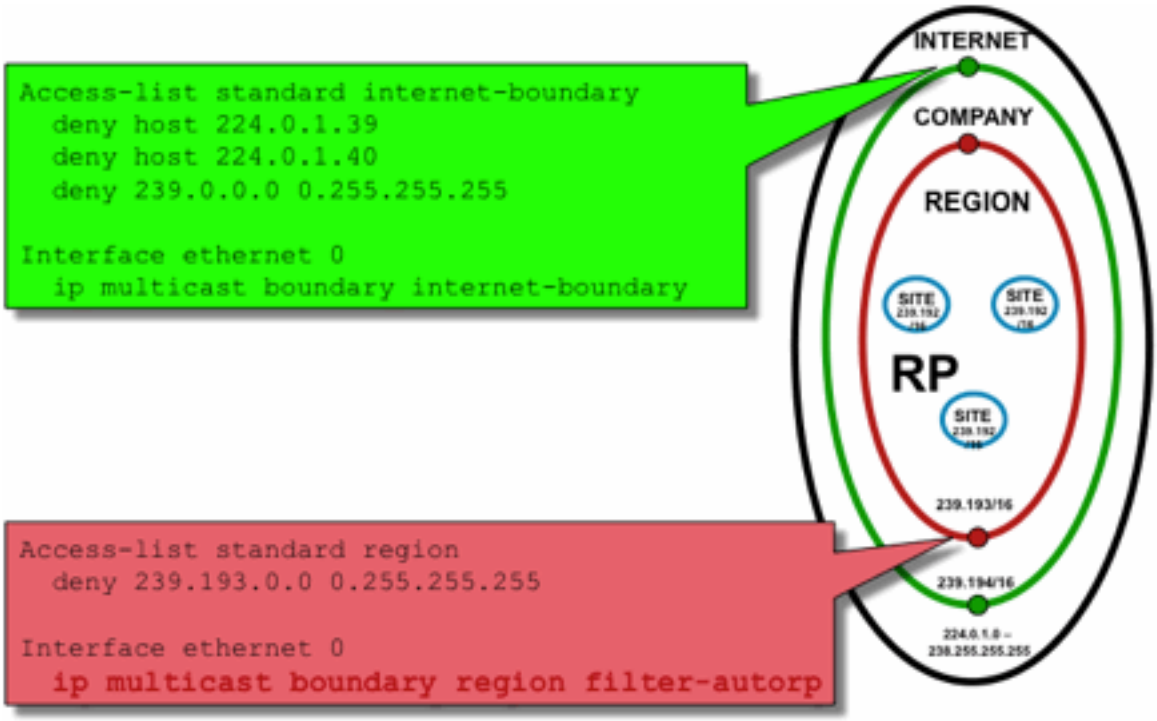


그림 12_AutoRP_Filtering_Scoping

Auto-RP에 대한 인터페이스 경계 필터의 아이디어는 auto-rp 공지가 지원 영역에만 도달하도록 보장하는 것입니다. 지역, 회사 및 인터넷 전반의 범위가 정의되며, 각각의 경우 각 범위에 RP 및 Auto-RP 광고가 있습니다. 관리자는 지역 RP를 지역 라우터에만 알리고, 회사 RP를 지역 및 회사 라우터에만 알리고, 모든 인터넷 RP를 전역적으로 사용할 수 있기를 원합니다. 더 높은 수준의 범위가 가능합니다.

그림에서 볼 수 있듯이 근본적으로 Auto-RP 패킷을 필터링하는 두 가지 방법이 있습니다. 인터넷 경계는 auto-rp 제어 그룹(224.0.1.39 및 224.0.1.40)을 명시적으로 호출하여 모든 Auto-RP 패킷에 대해 필터가 생성됩니다. 이 방법은 Auto-RP 패킷이 전달되지 않는 관리 도메인의 에지에서 사용할 수 있습니다. Region 경계에서는 filter-auto-rp 키워드를 사용하여 Auto-RP 패킷 내에서 rp-to-group-range 알림을 검사합니다. ACL에 의해 알림이 명시적으로 거부되면 패킷이 전달되기 전에 Auto-RP 패킷에서 알림이 제거됩니다. 이 예에서는 전사적 RP를 영역 내에서 알 수 있도록 하는 반면, 전사적 RP는 영역에서 기업의 나머지 영역으로 경계에서 필터링됩니다.

도메인 간 필터 및 MSDP

이 예에서 ISP1은 PIM-SM 전송 공급자 역할을 합니다. 네이버와의 MSDP 피어링만 지원하며, (S,G)만 허용하지만 경계 라우터에서는 (*,G) 트래픽은 허용하지 않습니다.

도메인 간(대개 자동 시스템 간)에는 두 가지 기본 보안 조치가 있습니다.

1. multicast boundary 명령을 통해 데이터 **플레인을** 보호합니다. 이렇게 하면 멀티캐스트 트래픽이 정의된 그룹(및 잠재적으로 소스)에 대해서만 수락됩니다.
2. MSDP(도메인 간 컨트롤 플레인 트래픽)를 보호합니다. 이는 다음과 같은 여러 개별 보안 조치로 구성됩니다. MSDP 콘텐츠 제어, 상태 제한 및 네이버 인증

그림 13은 ISP1의 보더 라우터 중 하나에 대한 인터페이스 필터 구성의 예입니다.

도메인 경계에서 데이터 평면을 보호하려면(*,G) 필터를 사용하여 "host 0.0.0.0" 및 관리적으로 범위가 지정된 주소에 대해 multicast boundary **명령을** 사용합니다.

그림 13: 도메인 간(*,G) 필터

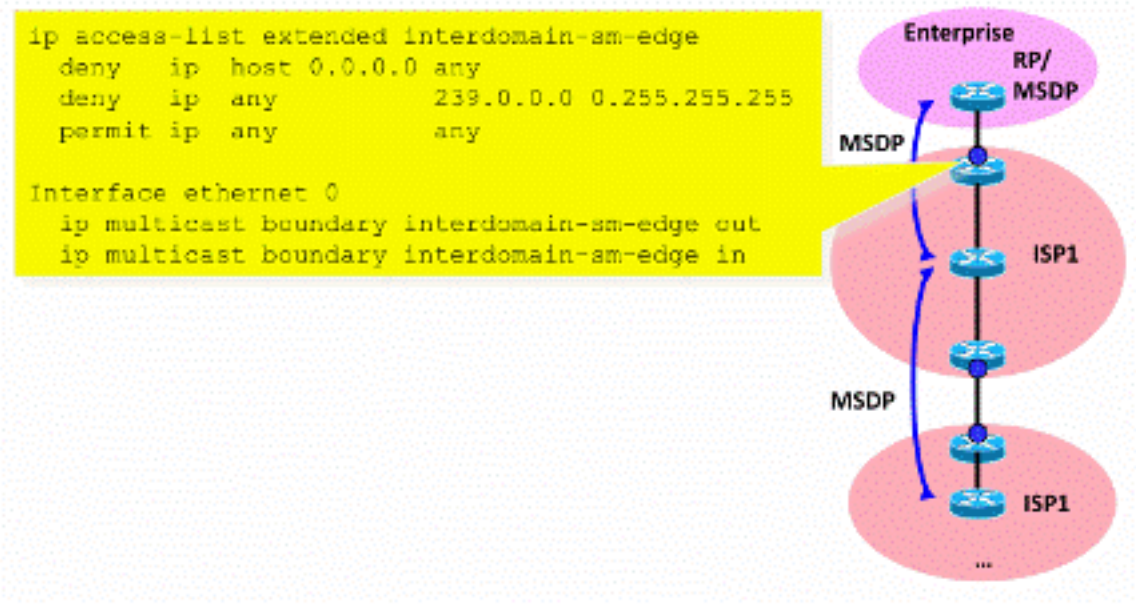


그림 13_Interdomain_Filter

컨트롤 플레인을 보호하려면 세 가지 기본 보안 조치를 통해 MSDP를 강화합니다.

1) MSDP SA 필터

MSDP SA 필터를 통해 MSDP 메시지의 내용을 필터링하는 것은 "모범 사례"입니다. 이 필터의 주요 아이디어는 인터넷 전반의 애플리케이션이 아니며 소스 도메인을 넘어 포워딩할 필요가 없는 애플리케이션 및 그룹에 대한 멀티캐스트 상태의 전파를 방지하는 것입니다. 보안의 관점에서 볼 때, 필터는 알려진 그룹(및 잠재적으로 발신자)만 허용하고 알 수 없는 발신자 및/또는 그룹은 거부하는 것이 좋습니다.

일반적으로 허용되는 모든 발신자 및/또는 그룹을 명시적으로 나열할 수는 없습니다. 모든 그룹(MSDP 메시 그룹 없음)에 대해 단일 RP가 있는 PIM-SM 도메인의 기본 컨피그레이션 필터를 사용하는 것이 좋습니다.

```
!--- Filter MSDP SA-messages.
         !--- Replicate the following two rules for every external MSDP peer.
         !
         ip msdp sa-filter in <peer_address> list 111
         ip msdp sa-filter out <peer_address> list 111
         !
         !--- The redistribution rule is independent of peers.
         !
```

```
ip msdp redistribute list 111
!
!--- ACL to control SA-messages originated, forwarded.
!
!--- Domain-local applications.
access-list 111 deny   ip any host 224.0.2.2     !
access-list 111 deny   ip any host 224.0.1.3     ! Rwhod
access-list 111 deny   ip any host 224.0.1.24    ! Microsoft-ds
access-list 111 deny   ip any host 224.0.1.22    ! SVRLOC
access-list 111 deny   ip any host 224.0.1.2     ! SGI-Dogfight
access-list 111 deny   ip any host 224.0.1.35    ! SVRLOC-DA
access-list 111 deny   ip any host 224.0.1.60    ! hp-device-disc
!--- Auto-RP groups.
access-list 111 deny   ip any host 224.0.1.39
access-list 111 deny   ip any host 224.0.1.40
!--- Scoped groups.
access-list 111 deny   ip any 239.0.0.0 0.255.255.255
!--- Loopback, private addresses (RFC 6761). access-list 111 deny ip 10.0.0.0
0.255.255.255 any access-list 111 deny ip 127.0.0.0 0.255.255.255 any access-list 111 deny ip
172.16.0.0 0.15.255.255 any access-list 111 deny ip 192.168.0.0 0.0.255.255 any !--- Default
SSM-range. Do not do MSDP in this range. access-list 111 deny ip any 232.0.0.0 0.255.255.255
access-list 111 permit ip any any !
```

가능한 한 엄격하게 필터링하는 것이 좋으며 인바운드 및 아웃바운드 양방향으로 필터링하는 것이 좋습니다.

MSDP SA 필터 권장 사항에 대한 자세한 내용은 다음을 참조하십시오.
https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) MSDP 상태 제한

여러 AS(Autonomous Systems) 간에 MSDP가 활성화된 경우 네이버에서 수신한 "SA(Source-Active)" 메시지로 인해 라우터에 구축된 상태의 양을 제한하는 것이 좋습니다. **ip msdp sa-limit 명령**을 사용할 수 있습니다.

ip msdp sa-limit <peer> <limit>

그림 14: MSDP 컨트롤 플레인

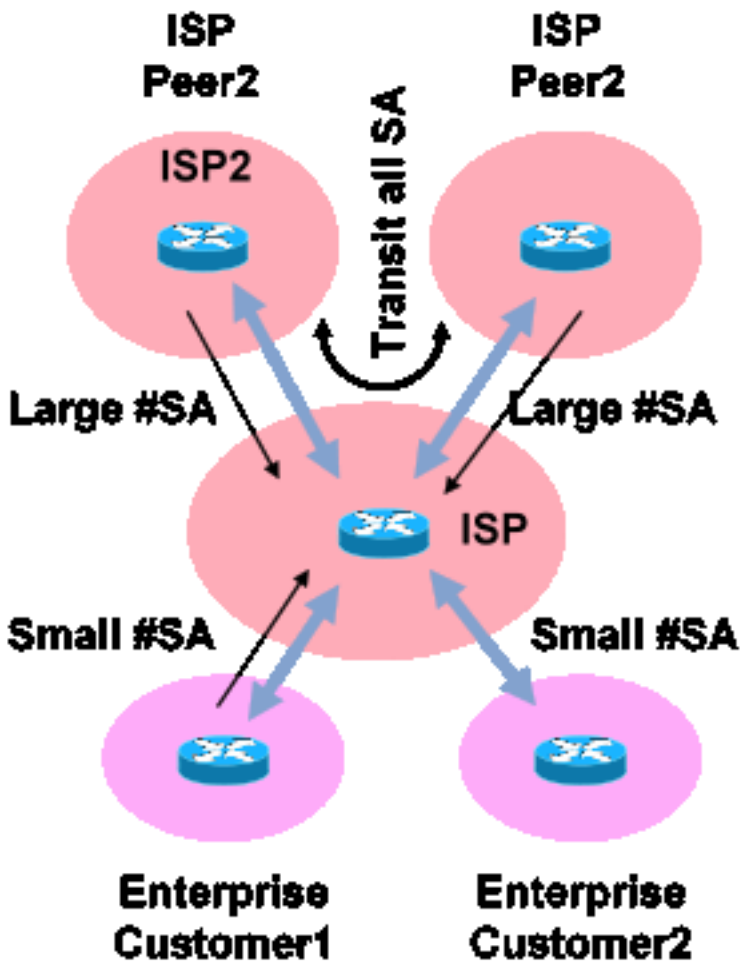


그림14_MSDP_ControlPlane

ip msdp sa-limit 명령을 사용하면 MSDP 피어에서 수락된 SA 메시지로 인해 생성된 SA 상태의 수를 제한할 수 있습니다. 몇 가지 간단한 경험적 권장 사항은 다음과 같습니다.

- stub-neighbor의 작은 제한
- 트랜짓 네이버의 큰 제한(예: 인터넷의 최대 #SAs)
- 트랜짓 ISP - 플랫폼에서 지원할 수 #SAs 최대 구성

3) MSDP MD5 네이버 인증

MSDP 피어에서 MD5(Message-Digest Algorithm) 비밀번호 인증을 사용하는 것이 좋습니다. 이는 RFC 6691에서 BGP를 보호하는 데 사용하는 것과 동일한 TCP MD5 서명 옵션을 사용합니다.

그림 15: MSDP MD5 네이버 인증

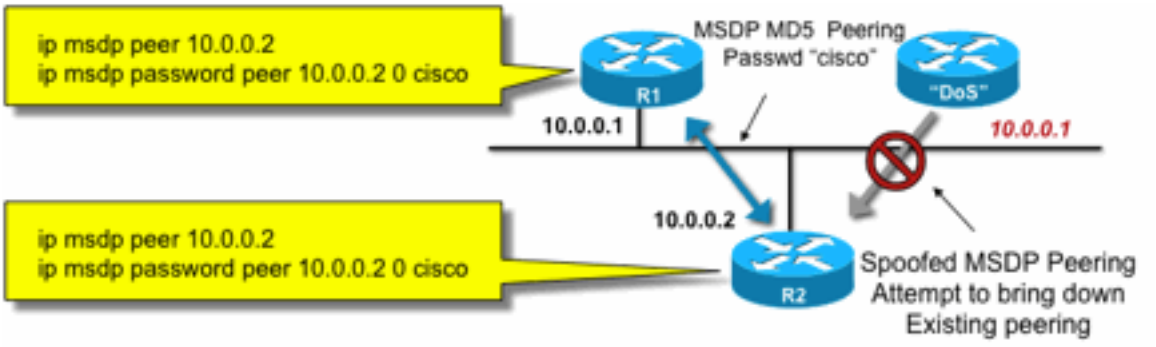


Fig15_MSDP_MD5Auth

이러한 세 가지 MSDP 보안 권장 사항은 서로 다른 목표를 추구합니다.

- 인접 디바이스 인증(MD5 사용)을 통해 신뢰할 수 있는 MSDP 피어만 메시지를 보낼 수 있습니다.
- SA 필터는 신뢰할 수 있는 MSDP 피어도 사전 합의된 소스/그룹 정책에 부합하는 SA 알림만 보낼 수 있도록 보장합니다.
- SA 제한은 또한 합법적인 피어로부터의 합법적인(S,G) 공지를 사용하더라도 사용 가능한 메모리를 소진할 수 없도록 합니다.

발신자/소스 문제

발신자에서 발생하는 많은 멀티캐스트 보안 문제는 적절한 유니캐스트 보안 메커니즘으로 완화할 수 있습니다. 여기에는 여러 유니캐스트 보안 메커니즘이 권장됩니다.

- **소스 주소 스푸핑 보호**(액세스 계층의 유니캐스트 역방향 경로 전달, uRPF 또는 ACL 및 IP 소스 보호)
- **인프라 ACL**(deny ip any (to) <core address space>)

그러한 조치는 코어에 대한 직접적인 공격을 차단하는 데 사용될 수 있다. 예를 들어, 이는 RP에 대한 PIM 유니캐스트 패킷을 사용하는 공격과 같은 문제도 해결합니다. RP는 네트워크 "내부"이므로 인프라 ACL에 의해 보호됩니다.

패킷 필터 기반 액세스 제어 - 제어 소스

그림 16의 예에서는 필터가 1홉 멀티캐스트 라우터(Designated Router)의 LAN 인터페이스(E0)에 구성됩니다. 필터는 "source"라는 확장 액세스 제어 목록에 의해 정의됩니다. 이 ACL은 소스 LAN에 연결된 Designated Router의 소스 연결 인터페이스에 적용됩니다. 실제로 멀티캐스트 트래픽의 특성 때문에 소스가 활성화될 수 있는 모든 LAN 연결 인터페이스에 유사한 필터를 구성해야 할 수 있습니다. 어떤 경우에는 소스 활동이 어디에서 발생하는지 정확히 알 수 없으므로 네트워크의 모든 인그레스 포인트에 이러한 필터를 적용하는 것이 좋습니다.

그림 16: 제어 소스

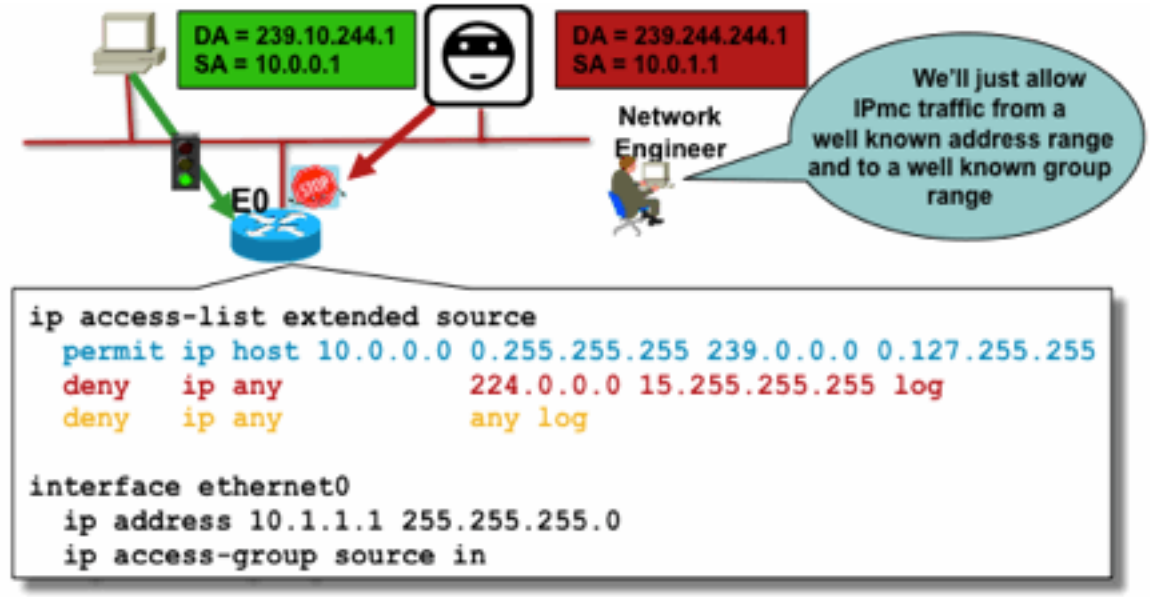


Fig16_Controlling_Sources

이 필터의 목적은 특정 소스 또는 소스 주소 범위에서 특정 그룹 또는 그룹 주소 범위로 이동하는 트래픽을 방지하는 것입니다. 이 필터는 PIM이 경로를 생성하고 상태를 제한하기 전에 작동합니다.

표준 데이터 플레인 ACL입니다. 이는 하이엔드 플랫폼의 ASIC에서 구현되며 성능 페널티가 발생하지 않습니다. 데이터 플레인 ACL은 원치 않는 트래픽의 컨트롤 플레인 영향을 최소화하기 때문에 직접 연결된 소스의 컨트롤 플레인보다 권장되고 선호됩니다. 패킷을 전송할 수 있는 대상(IP 멀티캐스트 그룹 주소)을 제한하는 것도 매우 효과적입니다. 라우터 명령이므로 스푸핑된 소스 IP 주소를 극복할 수 없습니다(이 섹션의 앞 부분 참조). 따라서 추가 L2(Layer 2) 메커니즘을 제공하거나 특정 LAN/VLAN(Local Area Network/Virtual Local Area Network)에 연결할 수 있는 모든 디바이스에 대해 일관된 정책을 제공하는 것이 좋습니다.

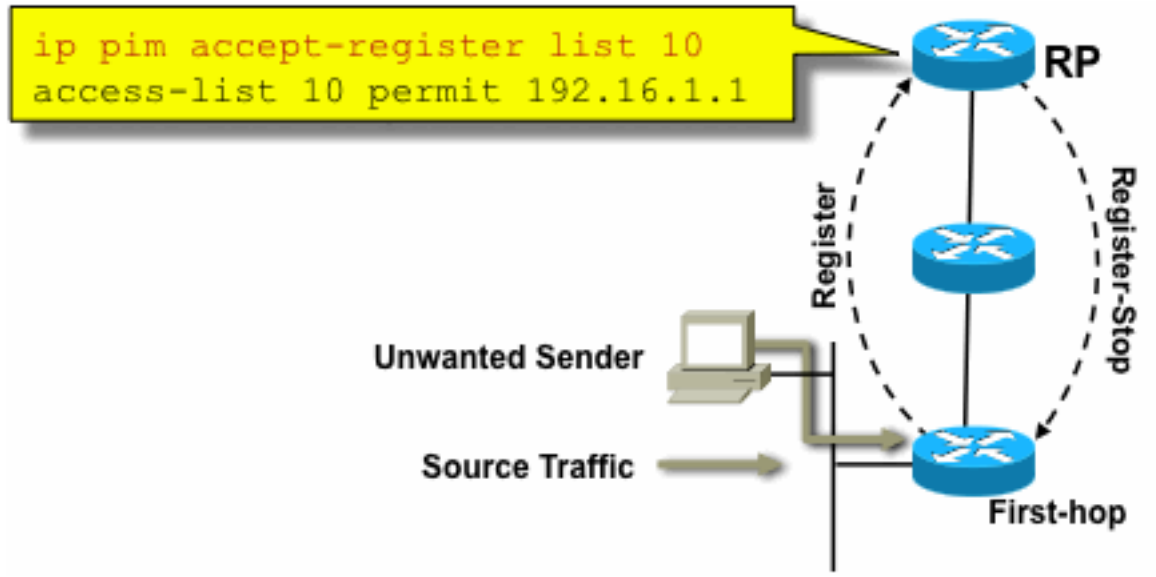
> **참고:** ACL의 "log" 키워드는 특정 ACL 항목에 대한 적중을 파악하는 데 매우 유용합니다. 그러나 이 경우 CPU 리소스가 소모되므로 신중하게 처리해야 합니다. 또한 하드웨어 기반 플랫폼에서 ACL 로그 메시지는 CPU에 의해 생성되므로 CPU 영향을 고려해야 합니다.

PIM-SM 소스 제어

보안 관점에서 ASM/PIM-SM 아키텍처의 실제 장점 중 하나는 Rendezvous Point가 모든 그룹 범위에 대해 네트워크의 모든 소스에 대해 단일 제어 지점을 제공한다는 점입니다. 이는 accept-register 필터라는 디바이스에서 활용할 수 있습니다. 이 필터에 대한 명령은 다음과 같습니다.

```
ip pim accept-register / ipv6 pim accept-register
```

그림 17: PIM-SM 소스 제어



그림

17_PIMSM_Control

PIM-SM 네트워크에서 원치 않는 트래픽 소스는 이 명령으로 제어할 수 있습니다. 소스 트래픽이 첫 번째 홉 라우터에 도달하면 첫 번째 홉 라우터(DR)는 (S,G) 상태를 생성하고 RP에 PIM Source Register 메시지를 보냅니다. 소스가 RP에 구성된 accept-register 필터 목록에 나열되지 않은 경우 RP는 등록을 거부하고 즉시 Register-Stop 메시지를 DR로 다시 보냅니다.

표시된 예에서는 소스 주소에서만 필터링하는 간단한 ACL이 RP에 적용되었습니다. RP에서 확장 ACL을 사용하여 소스 및 그룹을 필터링할 수도 있습니다.

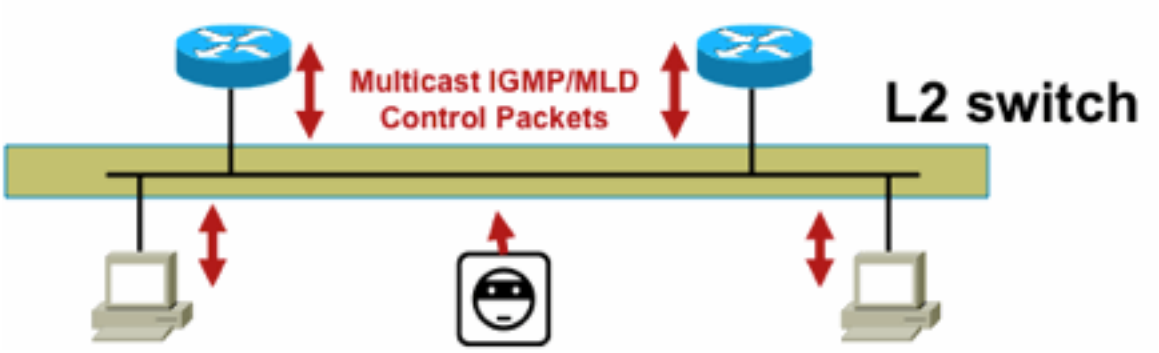
RP에서 pim accept-**register 명령**을 사용하면 소스의 첫 번째 홉 라우터에서 PIM-SM(S,G) 상태가 계속 생성되므로 소스 필터의 단점이 있습니다. 이 경우 수신기에서 소스에 대해 로컬이고 소스와 RP 사이에 위치한 트래픽이 발생할 수 있습니다. 또한 pim **accept-register** 명령은 RP의 제어 플레인에서 작동합니다. 이는 가짜 레지스터 메시지로 RP를 오버로드하기 위해 사용될 수 있으며, DoS 상태를 유발할 수 있습니다.

모든 DR의 간단한 데이터 플레인 ACL을 네트워크에 모든 인그레스 포인트에 적용하는 것과 같은 다른 방법 외에도 RP에 pim accept-register 명령을 적용하는 것이 좋습니다. DR의 인그레스 ACL은 완벽하게 구성되고 운영되는 네트워크에서는 충분하지만 에지 라우터에서 잘못 구성된 경우 RP에 **pim accept-register 명령**을 보조 보안 메커니즘으로 구성하는 것이 좋습니다. 동일한 목표를 가진 계층화된 보안 메커니즘을 "심층 방어"라고 하며, 보안의 일반적인 설계 원칙입니다.

수신기 문제 - 제어 IGMP/MLD

대부분의 수신기 문제는 IGMP/MLD 수신기 프로토콜 상호 작용의 도메인에 속합니다.

그림 18: 제어 IGMP



그림

18_Controlling_IGMP

IGMP 또는 MLD 패킷이 필터링되면 다음 사항을 기억하십시오.

- IPv4: IGMP는 IPv4 프로토콜 유형(IPv4 프로토콜 2)입니다
- IPv6: MLD는 ICMPv6 프로토콜 유형 패킷에서 전달됩니다

IP Multicast가 활성화되자마자 IGMP 프로세스가 기본적으로 활성화됩니다. IGMP 패킷도 이러한 프로토콜을 전달하므로 멀티캐스트가 활성화될 때마다 이러한 모든 프로토콜이 활성화됩니다.

- PIMv1 - PIMv1은 PIM의 첫 번째 버전이며 마이그레이션을 위해 Cisco IOS에서 항상 활성화됩니다. 현재 구축에서는 모두 PIMv2를 사용합니다.
- Mrinfo - Mrinfo는 Cisco IOS가 멀티캐스트 네이버를 표시하기 위해 상속한 Unix 명령입니다. mrinfo 명령 대신 SNMP를 사용하는 것이 좋습니다.
- DVMRP - DVMRP는 확장 특성이 매우 제한적인 레거시 고밀도 모드 거리 벡터 프로토콜입니다. DVMRP에 대한 Cisco IOS 지원이 중단되었거나 이미 더 이상 사용되지 않습니다.
- Mtrace - Mtrace는 유니캐스트 "traceroute"의 멀티캐스트 버전이며 유용한 툴입니다

자세한 내용은 IANA의 IGMP(Internet Group Management Protocol) 유형 번호를 참조하십시오

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254

Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
 0  172.16.0.10
-1  172.16.0.8 PIM  thresh^ 0  0 ms
-2  172.16.0.6 PIM  thresh^ 0  2 ms
-3  172.16.0.5 PIM  thresh^ 0  894 ms
-4  172.16.0.3 PIM  thresh^ 0  893 ms
-5  172.16.0.2 PIM  thresh^ 0  894 ms
-6  172.16.0.1 PIM  thresh^ 0  893 ms
```

유니캐스트 IGMP 패킷(IGMP/UDLR용)은 필터링할 수 있습니다. 이는 공격 패킷일 가능성이 높고 유효한 IGMP 프로토콜 패킷이 아니기 때문입니다. 유니캐스트 IGMP 패킷은 단방향 링크 및 기타 예외 조건을 지원하기 위해 Cisco IOS에서 지원됩니다.

위조된 IGMP/MLD 쿼리 패킷은 예상한 것보다 낮은 IGMP 버전을 초래할 수 있습니다.

특히 하위 IGMP 버전으로 전송된 쿼리는 이 쿼리를 수신하는 모든 호스트가 하위 버전으로 되돌아갈 수 있기 때문에 호스트는 IGMP 쿼리를 보내지 않는 것이 좋습니다. IGMPv3/SSM 호스트가 있는 경우 SSM 스트림을 "공격"할 수 있습니다. IGMPv2의 경우 이로 인해 대기 시간이 더 길어질 수 있습니다.

단일 IGMP 쿼리 기가 있는 비이중화 LAN이 있는 경우 라우터는 수신된 IGMP 쿼리를 삭제해야 합니다.

이중화/공통 패시브 LAN이 있는 경우 IGMP 스누핑을 지원하는 스위치가 필요합니다. 이 경우 다음과 같은 두 가지 특정 기능을 사용할 수 있습니다.

- 라우터 가드
- IGMP 최소 버전 명령

라우터 가드

스위치가 해당 포트에서 멀티캐스트 라우터 제어 패킷(IGMP 일반 쿼리, PIM Hello 또는 CGMP Hello)을 수신하는 경우 모든 스위치 포트는 멀티캐스트 라우터 포트가 될 수 있습니다. 스위치 포트가 멀티캐스트 라우터 포트가 되면 모든 멀티캐스트 트래픽이 해당 포트로 전송됩니다. 이 문제는 "Router Guard"를 통해 방지할 수 있습니다. Router Guard 기능은 IGMP 스누핑을 활성화하지 않아도 됩니다.

Router Guard 기능을 사용하면 지정된 포트를 멀티캐스트 호스트 포트로 지정할 수 있습니다. 멀티캐스트 라우터 제어 패킷이 수신되더라도 포트가 라우터 포트가 될 수 없습니다.

이러한 패킷 유형은 Router Guard가 활성화된 포트에서 수신될 경우 폐기됩니다.

- IGMP 쿼리 메시지
- IPv4 PIMv2 메시지
- IGMP PIM 메시지(PIMv1)
- IGMP DVMRP 메시지
- 라우터 포트 RGMP(Group Management Protocol) 메시지
- CGMP(Cisco Group Management Protocol) 메시지

이러한 패킷이 폐기되면 Router Guard로 인해 패킷이 삭제되었음을 나타내는 통계가 업데이트됩니다.

IGMP 최소 버전

허용되는 IGMP 호스트의 최소 버전을 구성할 수 있습니다. 예를 들어 모든 IGMPv1 호스트 또는 모든 IGMPv1 및 IGMPv2 호스트를 허용하지 않을 수 있습니다. 이 필터는 멤버십 보고서에만 적용됩니다.

호스트가 공통 "패시브" LAN에 연결된 경우(예: IGMP 스누핑을 지원하지 않거나 구성되지 않은 스위치), 라우터가 이러한 잘못된 쿼리에 대해 수행할 수 있는 작업은 트리거된 "이전 버전" 멤버십 보고서를 무시하는 것 외에 없으며 자체적으로 축소되지 않습니다.

IGMP 쿼리는 모든 호스트에 표시되어야 하므로, 고정 키 IPSec과 같은 사전 공유 키와 함께 HMAC(Hash-based message authentication) 메커니즘을 사용하여 "유효한 라우터"에서 IGMP 쿼리를 인증할 수는 없습니다. 두 개 이상의 라우터가 공통 LAN 세그먼트에 연결된 경우 IGMP 쿼리 발생기 선택이 필요합니다. 이 경우 사용할 수 있는 유일한 필터는 쿼리를 전송하는 다른 IGMP 라우터의 소스 IP 주소를 기반으로 하는 ip 액세스 그룹 필터입니다.

"일반" 멀티캐스트 IGMP 패킷을 허용해야 합니다.

이 필터는 수신기 포트에서 "정상" IGMP 패킷만 허용하고 알려진 "불량" 패킷을 필터링하는 데 사용할 수 있습니다.

```
ip access-list extended igmp-control
   <snip>
   deny   igmp any any  pim        ! No PIMv1
   deny   igmp any any  dvmrp      ! No DVMRP packets
   deny   igmp any any  host-query ! Do not use this command with redundant routers.
                                   ! In that case this packet type is required !
   permit igmp any host 224.0.0.22 ! IGMPv3 membership reports
   permit igmp any any  14         ! Mtrace responses
   permit igmp any any  15         ! Mtrace queries
   permit igmp any 224.0.0.0 10.255.255.255 host-query  ! IGMPv1/v2/v3 queries
   permit igmp any 224.0.0.0 10.255.255.255 host-report ! IGMPv1/v2 reports
   permit igmp any 224.0.0.0 10.255.255.255 7           ! IGMPv2 leave messages
   deny   igmp any any             ! Implicitly deny unicast IGMP here!
<snip> permit ip any any ! Permit other packets interface ethernet 0 ip access-group igmp-
control in
```

참고: 이 유형의 IGMP 필터는 수신 ACL 또는 CoPP에 사용할 수 있습니다. 두 애플리케이션 모두에서 라우팅 및 관리 플레인 프로토콜과 같이 처리되는 다른 트래픽에 대한 필터와 결합해야 합니다.

그림 19: 호스트 수신측 액세스 제어

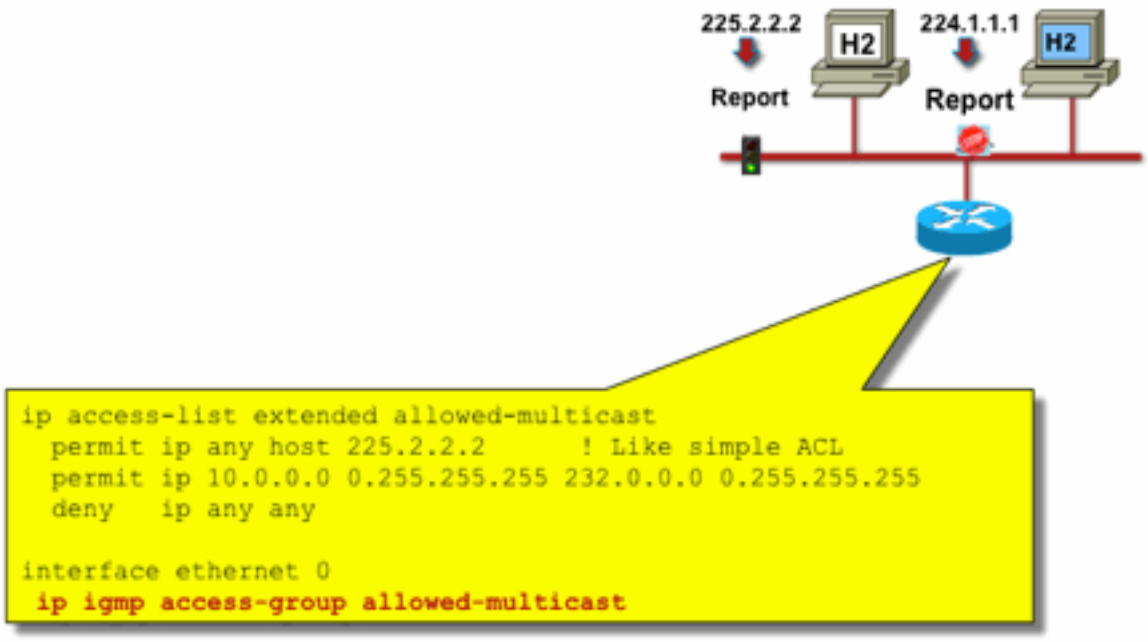


그림 19_Host_Receiver_Access

수신기에 대한 트래픽을 필터링하려면 데이터 플레인 트래픽을 필터링하지 않고 컨트롤 플레인 프로토콜 IGMP를 필터링합니다. IGMP는 멀티캐스트 트래픽을 수신하는 데 필요한 전제 조건이므로 데이터 플레인 필터가 필요하지 않습니다.

특히 수신자가 참가할 수 있는 멀티캐스트 흐름(명령이 구성된 인터페이스에 연결됨)을 제한할 수 있습니다. 이 경우 **ip** igmp access-**group / ipv6 mld access-group 명령을** 사용합니다.

ip igmp access-group / ipv6 mld access-group

ASM 그룹의 경우 이 명령은 대상 주소를 기반으로 필터링만 합니다. 그러면 ACL의 소스 IP 주소가 무시됩니다. IGMPv3/MLDv2를 사용하는 SSM 그룹의 경우 소스 및 대상 IP에서 필터링됩니다.

다음 예에서는 모든 IGMP 스피커에 대해 지정된 그룹을 필터링합니다.

```
access-list 1 deny 226.1.0.0 0.0.255.255
access-list 1 permit any log
! interface ethernet 1/3 ip igmp access-group 1
```

다음 예에서는 지정된 그룹에 대한 특정 IGMP 스피커(따라서 특정 멀티캐스트 수신기)를 필터링합니다.

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface Ethernet0/3
 ip igmp access-group test5
```

참고: ASM 그룹의 경우 소스가 무시됩니다.

허용 제어

액세스 제어는 네트워크 상태와 독립적으로 특정 흐름에 대해 이진 응답, 예 응답 또는 아니요 응답을 제공합니다. 대조에 의한 승인 제어는 액세스 제어 메커니즘을 통과했다고 가정할 때 발신자/수신자가 사용할 수 있는 리소스의 수를 제한합니다. 멀티캐스트 환경에서 승인 제어를 지원하기 위해 다양한 장치가 사용 가능합니다.

전역 및 인터페이스당 IGMP 제한

관심 있는 멀티캐스트 수신자와 가장 가까운 라우터에서는 전역적으로 그리고 인터페이스당 참여하는 IGMP 그룹의 수를 제한할 수 있습니다. **ip** igmp limit**/ipv6 mld limit 명령을** 활용할 수 있습니다.

```
ip igmp limit <n> [ except <ext-acl> ]
ipv6 mld limit <n> [ except <ext-acl> ]
```

이 제한은 항상 인터페이스별로 그리고 전역적으로 구성하는 것이 좋습니다. 각각의 경우, 제한은 IGMP 캐시에 있는 엔트리의 수를 의미한다.

다음 두 예에서는 이 명령을 사용하여 가정용 광대역 네트워크의 에지에서 그룹 수를 제한하는 방법을 보여 줍니다.

예 1 - 수신 그룹을 SDR 알림에 수신 채널 1개를 더한 값으로만 제한

SDR(Session Directory)은 일부 멀티캐스트 수신자에 대한 채널 가이드의 역할을 합니다. 자세한 내용은 RFC 2327을 참조하십시오.

일반적인 요구 사항은 수신자가 SD 그룹과 하나의 채널을 수신하도록 제한하는 것입니다. 다음 예제 컨피그레이션을 사용할 수 있습니다.

```
ip access-list extended channel-guides
  permit ip any host 239.255.255.254 ! SDR announcements
  deny   ip any any
```

```
ip igmp limit 1 except channel-guides

interface ethernet 0
  ip igmp limit 2 except channel-guides
```

이 예의 액세스 목록은 채널 안내서만 지정합니다. global **ip igmp limit** 명령은 각 IGMP 소스를 단일(1) 채널로 제한하지만 채널 가이드를 포함하지 않습니다. 채널 가이드는 항상 수신할 수 있습니다. interface 명령은 전역 명령을 재정의하고 이 인터페이스에서 채널 가이드 외에 2개의 채널을 수신할 수 있게 합니다.

예 2 - 어그리게이션-DSLAM 링크의 승인 제어

이 명령은 대역폭 허용 제어 형식을 제공하는 데에도 사용할 수 있습니다. 예를 들어, 각각 4Mbps인 300개의 SDTV 채널을 배포해야 하고 DSLAM(Digital-Subscriber-Line-Access-Multiplexer)에 1Gbps 링크가 있는 경우, TV 대역폭을 500Mbps로 제한하고 나머지는 인터넷 및 기타 용도로 남겨두도록 정책 결정을 내릴 수 있습니다. 이 경우 IGMP 상태를 500Mbps/4Mbps = 125 IGMP 상태로 제한할 수 있습니다.

이 경우 이 컨피그레이션을 사용할 수 있습니다.

그림 20: 인터페이스별 IGMP 제한 사용; Agg-DSLAM 링크의 승인 제어

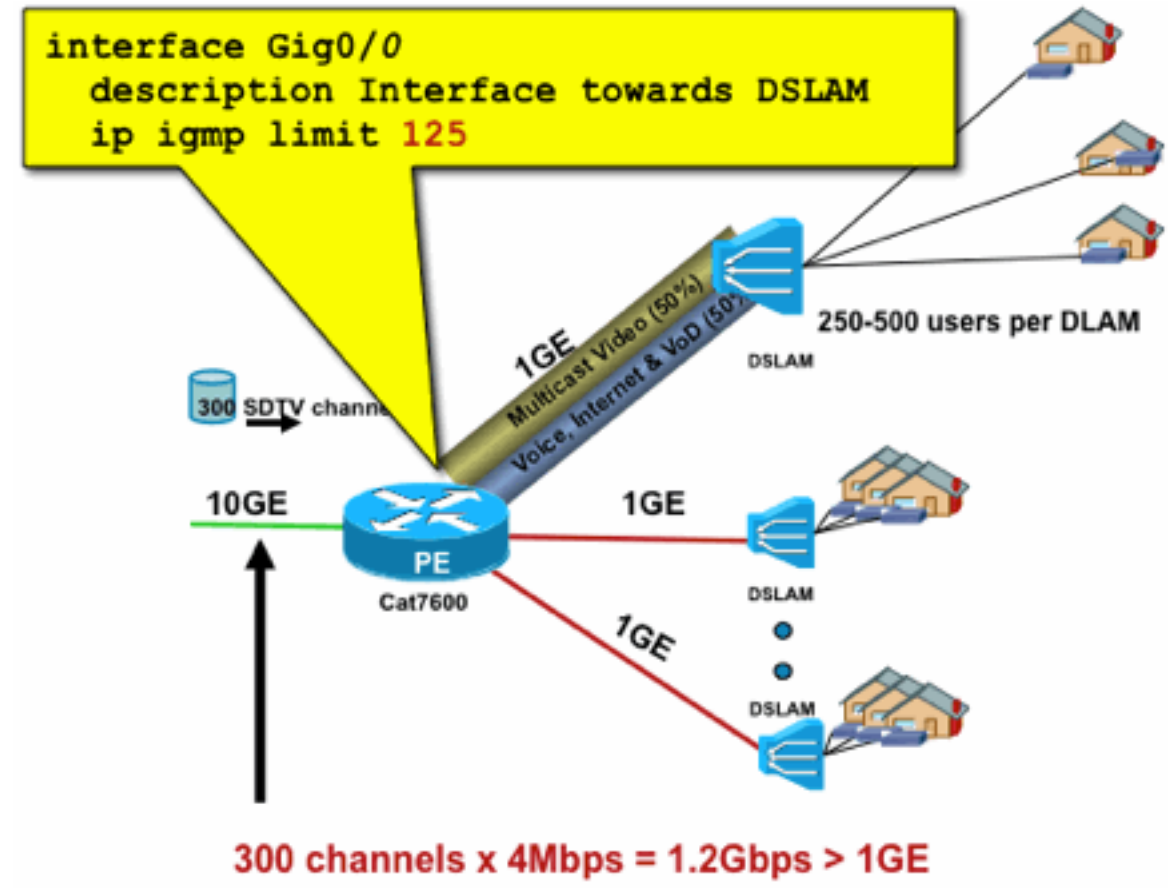


그림 20_PerInterface_IGMP

인터페이스당 경로 제한

인터페이스별 경로 상태 제한의 활성화는 좀 더 일반적인 승인 제어 형식입니다. 이 명령은 발신 인터페이스에서 IGMP 및 PIM 상태를 제한할 뿐만 아니라 수신 인터페이스에서 상태 제한 방식을 제공합니다.

ip multicast **limit 명령**을 사용합니다.

ip multicast limit [rpf | out | connected] <ext-acl> <max>
상태는 입력 및 출력 인터페이스에서 별도로 제한될 수 있습니다. 직접 연결된 소스 상태도 "연결된 " 키워드의 사용으로 제한될 수 있습니다. 다음 예에서는 이 명령의 사용을 설명합니다.

예 1 - Agg-DSLAM 링크의 이그레스 승인 제어

이 예에서는 300개의 SD TV 채널이 있습니다. 각 SD 채널에는 4Mbps가 필요하며 총 500Mbps를 넘지 않는다고 가정합니다. 마지막으로 Basic, Extended, Premium 번들을 지원해야 한다고 가정합니다. 대역폭 할당 예:

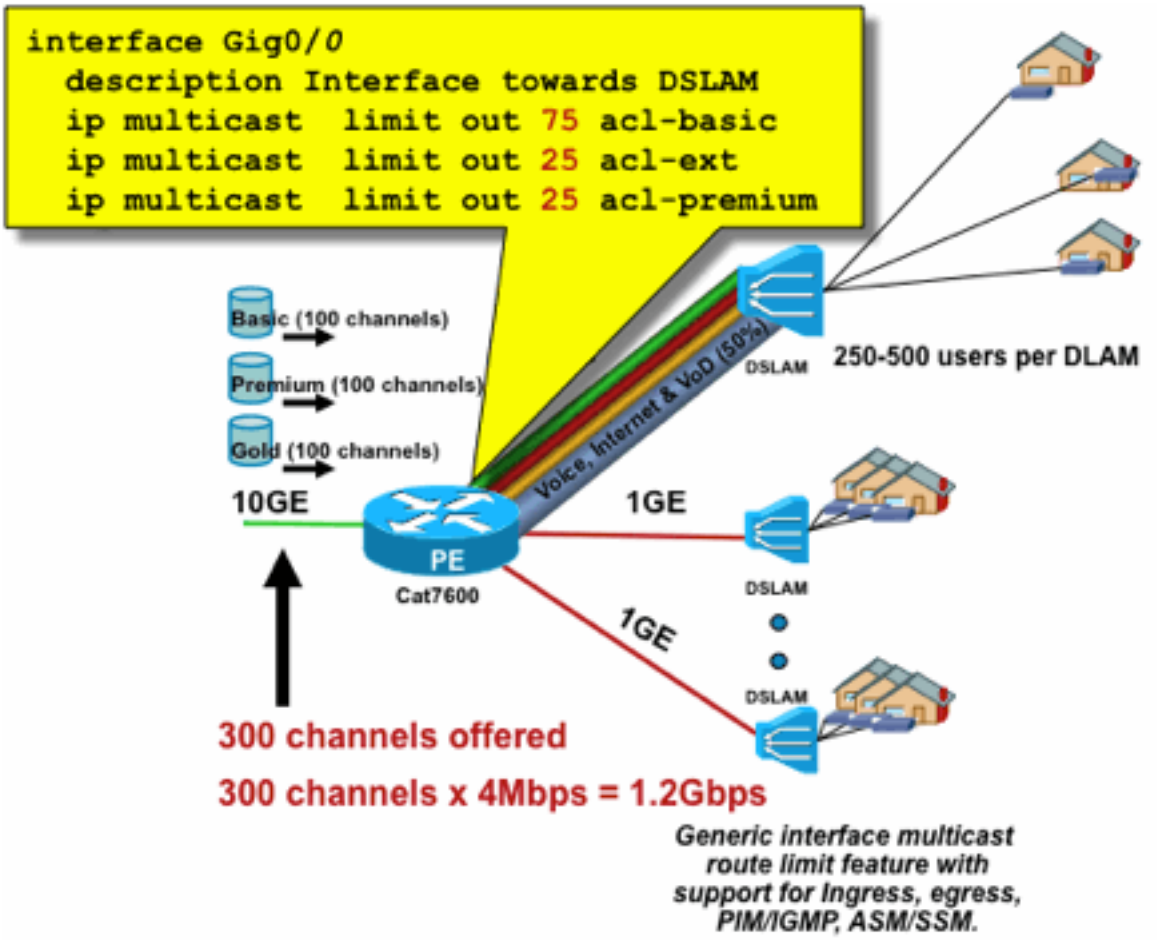
- 60%/300Mbps 기본
- 20%/100Mbps 확장
- 20%/100Mbps 프리미엄

그런 다음 채널당 4Mbps를 사용하고 DSLAM 업링크를 다음으로 제한합니다.

- 기본 75개 주
- 확장 25개 주
- 프리미엄 25개 주

PEAgg에서 DSLAM을 향하는 아웃바운드 인터페이스에 대한 제한을 구성합니다.

그림 21: 인터페이스당 경로 제한 사용; Agg-DSLAM 링크의 승인 제어



그림

예 2 - Agg-DSLAM 링크의 인그레스 수락 제어

업스트림 디바이스의 아웃바운드 인터페이스에 대한 "발신" 제한 대신 다운스트림 디바이스의 RPF 인터페이스에 대한 RPF 제한을 사용할 수 있습니다. 이는 이전 예와 실질적으로 동일한 결과이며 다운스트림 디바이스가 Cisco IOS 디바이스가 아닌 경우 유용할 수 있습니다.

그림 22: 인터페이스당 경로 제한 사용; 입력 허용 제어

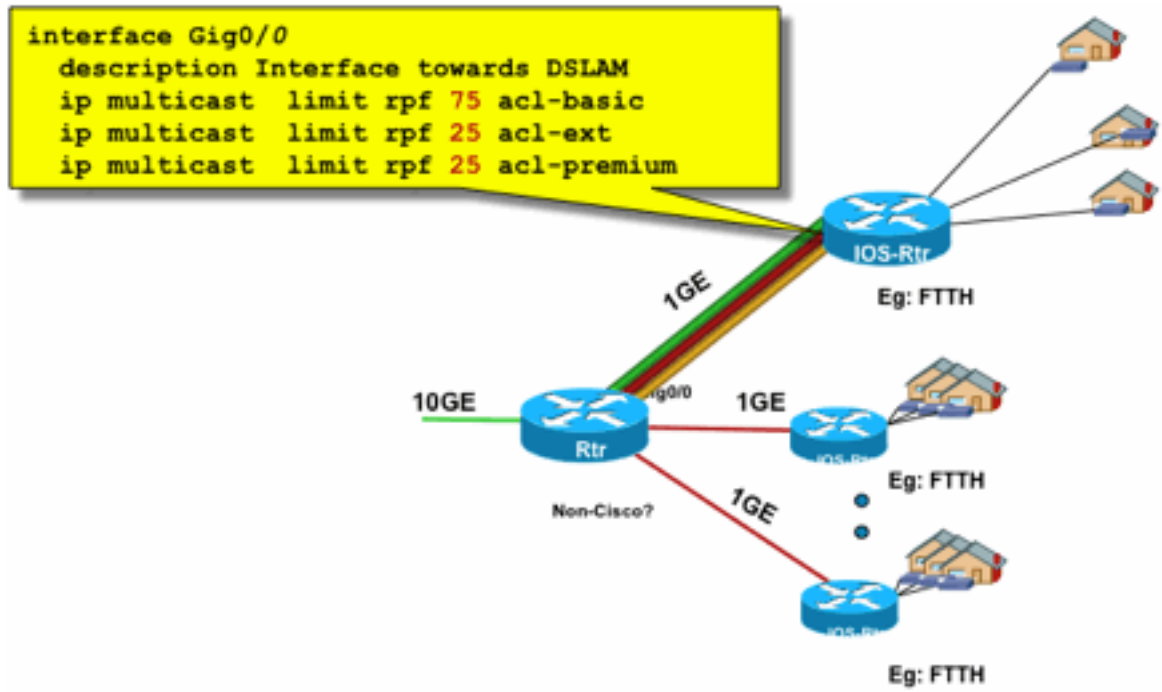


그림 22_PerInterface_Mroute_inputControl

예 3 - 대역폭 기반 제한

여러 콘텐츠 공급자 간에 액세스 대역폭을 더 세분화하고 각 콘텐츠 공급자에게 DSLAM에 대한 업링크에서 대역폭의 공평한 공유를 제공할 수 있습니다. 이 경우 **ip** multicast **limit cost 명령을 사용합니다**.

ip multicast limit cost <ext-acl> <multiplier>
이 명령을 사용하면 ip 멀티캐스트 제한에서 확장 ACL과 일치하는 상태에 "cost"("multiplier"에 지정된 값 사용)를 지정할 수 있습니다.

이 명령은 전역 명령이며 여러 동시 비용을 구성할 수 있습니다.

이 예에서는 서로 다른 3개의 콘텐츠 제공자가 네트워크에 대한 공정한 액세스를 지원할 필요가 있습니다. 또한 이 예제에서는 다양한 유형의 MPEG(Moving Picture Experts Group) 스트림을 지원해야 합니다.

MPEG2 SDTV: 4Mbps
MPEG2 HDTV: 18Mbps
MPEG4 SDTV: 1.6Mbps
MPEG4 HDTV: 6Mbps

이 경우 각 스트림 유형에 대역폭 비용을 할당하고 나머지 750Mbps를 이 컨피그레이션을 사용하는 세 개의 콘텐츠 공급자 간에 공유할 수 있습니다.

```
ip multicast limit cost acl-MP2SD-channels   4000 ! from any provider ip multicast limit cost
acl-MP2HD-channels 18000 ! from any provider ip multicast limit cost acl-MP4SD-channels 1600 !
from any provider ip multicast limit cost acl-MP4HD-channels 6000 ! from any provider !
interface Gig0/0 description --- Interface towards DSLAM --- <snip> ! CAC ip multicast limit out
250000 acl-CP1-channels ip multicast limit out 250000 acl-CP2-channels ip multicast limit out
250000 acl-CP3-channels
```

그림 23: 인터페이스별 Mroute 상태 제한에 대한 비용 계수

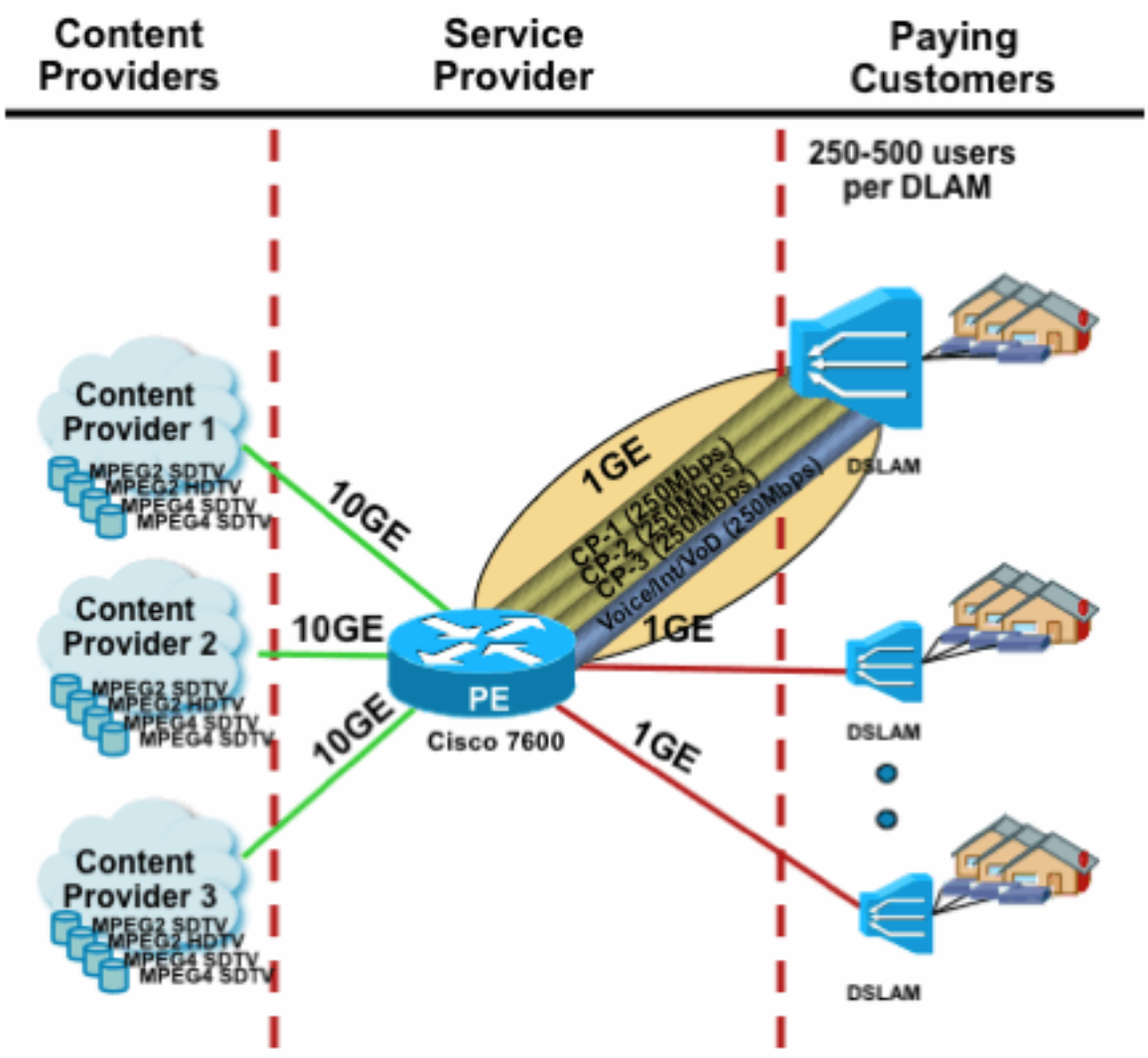


그림 23_Cost_PerInterface

멀티캐스트 및 IPSec

VPN 가져오기 소개

유니캐스트와 마찬가지로, 기밀성 또는 무결성 보호를 위해 멀티캐스트 트래픽도 보호되어야 하는 경우가 있습니다. 이러한 서비스가 필요할 수 있는 두 가지 주요 영역은 다음과 같습니다.

- 멀티캐스트 스트림의 암호화(예: 기밀 데이터를 멀티캐스트를 사용하는 대규모 수신기 집합으

로 스트리밍하는 뱅킹 애플리케이션) - 이는 데이터 플레인 보안입니다.
- 멀티캐스트, OSPF 또는 PIM을 사용하는 컨트롤 플레인 프로토콜의 암호화(예: 컨트롤 플레인 보안)입니다.

프로토콜로서의 IPSec [RFCs 6040, 7619, 4302, 4303, 5282]은 특히 유니캐스트 트래픽(RFC별)로 제한됩니다. 이 경우 두 유니캐스트 피어 간에 "SA(Security Association)"가 설정됩니다. 멀티캐스트 트래픽에 IPSec을 적용하려면 GRE 터널 내에서 멀티캐스트 트래픽을 캡슐화한 다음 유니캐스트인 GRE 터널에 IPSec을 적용하는 옵션이 있습니다. 새로운 방식에서는 그룹의 모든 구성원 간에 설정된 단일 보안 연결을 사용합니다. GDOI(Group Domain of Interpretation) [RFC 6407]은 이 달성 방법을 정의합니다.

Cisco는 GDOI를 기반으로 GET(Group Encryption Transport) VPN이라는 기술을 개발했습니다. 이 기술은 "draft-ietf-msec-ipsec-extensions" 문서에 정의된 대로 "Tunnel Mode with Address Preservation"을 사용합니다. GET VPN에서는 먼저 그룹의 모든 구성원 간에 그룹 보안 연결이 설정됩니다. 그 후에는 주소 보존과 함께 터널 모드를 사용하는 ESP(encapsulated security payload) 또는 AH(authentication header)를 사용하여 트래픽이 보호됩니다.

요약하면, GET VPN은 원래 헤더의 주소 정보를 사용하는 멀티캐스트 패킷을 캡슐화한 다음 ESP를 사용하여 그룹 정책과 관련하여 내부 패킷을 보호합니다.

GET VPN의 장점은 멀티캐스트 트래픽이 보안 캡슐화 메커니즘의 영향을 전혀 받지 않는다는 것입니다. 라우팅된 IP 헤더 주소는 원래 IP 헤더와 동일하게 유지됩니다. 멀티캐스트 트래픽은 GET VPN을 사용하거나 사용하지 않고 동일한 방식으로 보호할 수 있습니다.

GET VPN 노드에 적용되는 정책은 그룹 키 서버에서 중앙에서 정의되며 모든 그룹 노드에 배포됩니다. 따라서 모든 그룹 노드는 동일한 정책 및 그룹 트래픽에 적용되는 동일한 보안 설정을 갖습니다. 표준 IPSec과 마찬가지로 암호화 정책은 보호해야 할 트래픽 유형을 정의합니다. 이렇게 하면 GET VPN을 다양한 용도로 사용할 수 있습니다.

GET VPN을 사용하여 멀티캐스트 데이터 플레인 트래픽 암호화

네트워크 전반의 암호화 정책이 그룹 키 서버에 설정되고 GET VPN 엔드포인트에 배포됩니다. 정책에 IPSec 정책(IPSec 모드 - 여기서 사용할 보안 알고리즘(예: AES)을 지정합니다. 또한 ACL에 정의된 대로 어떤 트래픽을 보호할 수 있는지 설명하는 정책이 포함되어 있습니다.

GET VPN은 멀티캐스트 및 유니캐스트 트래픽에 사용할 수 있습니다. 유니캐스트 트래픽을 보호하기 위한 정책은 ACL에 의해 정의될 수 있습니다.

```
permit ip 10.0.0.0   0.255.255.255   10.0.0.0   0.255.255.255
```

이렇게 하면 10/8에서 소스 IP로, 10/8에서 대상 IP로 모든 트래픽이 암호화됩니다. 다른 모든 트래픽(예: 10/8에서 다른 주소로의 트래픽)은 GET VPN에서 무시됩니다.

멀티캐스트 트래픽에 대한 GET VPN의 적용은 기술적으로 동일합니다. 예를 들어, 이 ACE(access-control entry)를 사용하여 모든 소스에서 각 멀티캐스트 그룹으로의 트래픽을 보호할 수 있습니다.

```
permit ip any 239.192.0.0 0.0.255.255
```

이 정책은 모든 소스("any") 및 239.192로 시작하는 모든 멀티캐스트 그룹과 일치합니다. 다른 멀티캐스트 그룹에 대한 트래픽은 보호되지 않습니다.

참고: 암호화 ACL의 구축에 많은 주의를 기울여야 합니다. 관리 트래픽 또는 GET VPN 도메인 외부에서 시작되었지만 내부에서 종료되는 트래픽(즉, 하나의 암호화 엔드포인트만 통과하는 트래픽)은 GDOI 정책에서 제외해야 합니다.

일반적인 실수는 다음과 같습니다.

- 허용 ip any 224.0.0.0 0.255.255.255: 또한 OSPF 트래픽 및 기타 컨트롤 플레인 트래픽도 암호화합니다. 이 트래픽은 피어 라우터로 가는 트래픽입니다.
- 관리 트래픽은 네트워크 내부에서 종료되는 암호화 정책에서 제외되지 않습니다. 여기에는 GDOI 트래픽 자체가 포함됩니다.

GET VPN을 사용하여 컨트롤 플레인 트래픽 인증

일반적으로 라우팅 프로토콜과 같은 컨트롤 플레인 트래픽을 인증하여 메시지가 신뢰할 수 있는 피어에서 오도록 하는 것이 좋습니다. 이는 BGP와 같은 유니캐스트를 사용하는 컨트롤 플레인 프로토콜의 경우 비교적 간단합니다. 그러나 많은 컨트롤 플레인 프로토콜에서 멀티캐스트 트래픽을 사용합니다. 예를 들면 OSPF, RIP, PIM이 있습니다. 전체 목록은 IANA의 IPv4 멀티캐스트 주소 공간 레지스트리를 참조하십시오.

이러한 프로토콜 중 일부는 RIP(Routing Information Protocol) 또는 EIGRP(Enhanced Interior Group Routing Protocol)와 같은 내장형 인증이 있으며, 다른 일부는 IPSec을 사용하여 이 인증을 제공합니다(예: OSPFv3, PIM). 후자의 경우 GET VPN은 이러한 프로토콜을 보호하는 확장 가능한 방법을 제공합니다. 대부분의 경우, 요구 사항은 프로토콜 메시지 인증, 즉 메시지가 신뢰할 수 있는 피어에 의해 전송되었음을 확인하는 것입니다. 그러나 GET VPN은 이러한 메시지의 암호화도 허용합니다.

이러한 컨트롤 플레인 트래픽을 보호하려면(일반적으로 인증만) ACL로 트래픽을 설명하고 GET VPN 정책에 포함해야 합니다. 세부 정보는 보호할 프로토콜에 따라 다릅니다. 여기서 ACL에 인그레스 GET VPN 노드(캡슐화됨)만 통과하는 트래픽 또는 이그레스 노드도 포함되는지 확인해야 합니다.

PIM 프로토콜을 보호하는 두 가지 기본적인 방법이 있습니다.

- **허용 ip any 224.0.0.13 0.0.0.0**: 이는 "All PIM Routers" 멀티캐스트 그룹입니다. 그러나 유니캐스트 PIM 메시지는 보호하지 않습니다
- **permit pim any any**: 이는 멀티캐스트 또는 유니캐스트 사용 여부와 상관없이 PIM 프로토콜을 보호합니다

참고: 이 명령은 개념을 설명하는 데 도움이 되는 예로 제공됩니다. 예를 들어, BSR 또는 Auto-RP와 같이 PIM을 부트스트랩하는 데 사용되는 특정 PIM 프로토콜을 제외해야 합니다. 모든 방법에는 구축에 따라 특정 장점과 불편함이 있습니다. 자세한 내용은 GET VPN으로 PIM을 보호하는 방법에 대한 특정 문헌을 참조하십시오.

결론

네트워크에서 멀티캐스트가 점점 더 보편화되고 있습니다. 가정용/가정용 광대역 네트워크에서 IPTV 서비스의 등장과 전 세계 많은 금융 시장에서 전자 거래 애플리케이션으로의 전환은 멀티캐스트를 절대적인 요구 사항으로 만드는 요구 사항의 두 가지 예에 불과합니다. 멀티캐스트는 다양한 구성, 운영 및 관리 문제를 수반합니다. 핵심 과제 중 하나는 보안입니다.

이 문서에서는 멀티캐스트를 보호할 수 있는 다양한 방법을 살펴보았습니다.

- 먼저 전반적인 멀티캐스트 제어 및 데이터 플레인을 살펴보고, 유니캐스트와의 차이점이 새로운 보안 문제를 어떻게 야기하는지 설명합니다.
- 다음으로, 멀티 캐스트 네트워크에서 발생하는 주요 프로토콜, 특히 IGMP, PIM, MSDP에 대한 검토를 좀 더 자세히 살펴보았다. 각 사례마다 보안 위협에 대한 설명과 이러한 위협을 완화하기 위한 권장 모범 사례가 제공되었습니다.
- 또한 특정 비디오 플로우에 필요한 대역폭의 양에 비해 대역폭이 제한될 수 있는 광대역 에지 네트워크와 같은 일부 특정 애플리케이션에서 멀티캐스트를 보호하는 방법의 특정 예가 있습니다.
- 마지막으로, GET VPN 아키텍처는 보안 VPN을 제공하기 위해 IPSec과 통합된 멀티캐스트를 사용하는 수단으로 설명되었습니다.

멀티캐스트 보안을 염두에 두고 유니캐스트와 어떻게 다른지 기억하십시오. 멀티캐스트 전송은 동적 상태 생성을 기반으로 하며, 멀티캐스트는 동적 패킷 복제를 포함하며, 멀티캐스트는 PIM JOIN/PRUNE 메시지에 응답하여 단방향 트리를 구축합니다. 이 전체 환경의 보안에는 Cisco IOS 명령의 풍부한 프레임워크를 이해하고 구축하는 작업이 포함됩니다. 이러한 명령은 주로 프로토콜 작업, 상태(멀티캐스트) 또는 CoPP와 같은 패킷에 대해 배치된 폴리서의 보호를 중심으로 합니다. 이러한 명령을 올바르게 사용하면 IP 멀티캐스트에 대해 강력한 보호 서비스를 제공할 수 있습니다.

요약하면, 이 문서에서는 여러 가지 접근 방식을 장려하고 설명합니다.

1. SSM의 광범위한 사용 - (S,G) 포워딩도 사용할 수 있는 가장 간단한 PIM 모드입니다.
2. ASM 서비스가 필요한 경우 강력한 서비스를 제공할 수 있는지 확인합니다. 고정 정의된 RP를 사용하면 동적 RP 알림보다 더 안전한 컨트롤 플레인이 제공됩니다. Auto-RP 및 BSR이 더 유연함
3. PIM-SM이 활성화된 경우 RP에 대한 레지스터 터널과 같은 특정 취약성의 영역을 살펴보고 DR이 항상 잘 보호되는지 확인합니다. CoPP는 이러한 영역에서 매우 유용합니다.
4. 도메인 간 ASM 서비스가 필요한 경우 BiDir PIM을 구축할 수 있는지 여부를 고려합니다.
5. 글로벌 mroute/igmp 상태 제한 사용 - 정상적인 상황 및 최악의 경우 필요한 최대 상태의 예상과 함께 플랫폼의 기능을 이해합니다. 플랫폼의 기능 내에서 제한을 구성하여 네트워크가 최대 한도까지 작동하도록 합니다.
6. 기본 필터 - 액세스 레이어에서 PIM을 차단하는 rACL/CoPP 및 인프라 ACL

IP 멀티캐스트는 다양한 애플리케이션 서비스를 제공하기 위한 흥미롭고 확장 가능한 수단입니다. 유니캐스트와 마찬가지로 다양한 영역에서 보안이 되어야 합니다. 이 문서에서는 IP 멀티캐스트 네트워크를 보호하는 데 사용할 수 있는 기본 구성 요소를 제공합니다.

관련 정보

- 엔터프라이즈 IP 멀티캐스트 주소 할당 지침
- IPv4 IGMP 필터 구성
- 그룹 암호화 전송 VPN

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.