Implementazioni multicast IP sicure

Sommario

Introduzione

In questo documento vengono fornite linee guida generali sulle best practice per proteggere un'infrastruttura di rete IP multicast.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Multicast IP

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento vengono illustrati alcuni concetti di base e viene fornita una descrizione degli argomenti elencati di seguito.

- Meccanismi per proteggere una piattaforma specifica e la rete in generale.
- Qualsiasi modello ASM (Source Multicast) e SSM (Source Specific Multicast).
- Sicurezza Multicast Virtual Private Network (MVPN).
- Architettura VPN (Virtual Private Network) di Group Encrypted Transport (GET) che fornisce

riservatezza e integrità per il traffico del data plane o del control plane multicast.

Terminologia

Nel multicast IP sono disponibili due modelli di servizi classici:

1. Any Source Multicast (ASM)

2. Multicast specifico di origine (SSM)

In ASM, il ricevente si unisce a un gruppo G tramite un rapporto di appartenenza IGMP (Internet Group Membership Protocol) o MLD (Multicast Listener Discovery) per indicare il gruppo. Questo report richiede il traffico inviato da qualsiasi origine al gruppo G, da cui il nome "qualsiasi origine". Al contrario, in SSM, il ricevitore si unisce a un canale specifico definito da una sorgente S, che invia a un gruppo G. Ciascuno di questi modelli di servizio è descritto in dettaglio di seguito.

Any Source Multicast

Il modello ASM è caratterizzato da due classi di protocollo: "dense mode flood-and-prune" e "sparse mode explicit join":

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

Nei protocolli a modalità densa, tutti i router della rete sono a conoscenza di tutte le strutture, delle relative origini e dei ricevitori. Protocolli come il DVMRP (Distance Vector Multicast Routing Protocol) e PIM (Protocol Independent Multicast) inondano le informazioni sulla "fonte attiva" sull'intera rete e creano alberi tramite la creazione di "Stato di eliminazione" in parti della topologia in cui il traffico per un albero specifico è indesiderato. Sono anche chiamati protocolli di inondazione e prugna. In Multicast Open Shortest Path First (MOSPF), le informazioni sui ricevitori vengono trasmesse in tutta la rete per supportare la creazione di alberi.

I protocolli in modalità Dense non sono desiderabili perché ogni albero incorporato in una parte della rete può sempre causare l'utilizzo delle risorse (con impatto sulla convergenza) su tutti i router della rete (o all'interno dell'ambito amministrativo, se configurato). Questi protocolli non vengono ulteriormente discussi nel prosieguo di questo articolo.

ii) Protocolli di join espliciti in modalità sparsa (PIM-SM/PIM-BiDir)

Con i protocolli di join espliciti in modalità sparse, i dispositivi non creano uno stato specifico del gruppo nella rete a meno che un ricevitore non abbia inviato un rapporto di appartenenza esplicito IGMP/MLD (o "join") per un gruppo. Questa variante di ASM è ben scalabile ed è il paradigma multicast della messa a fuoco.

Questa è la base per la modalità di sparsità PIM, utilizzata fino a questo punto dalla maggior parte delle distribuzioni multicast. Questa è anche la base per PIM bidirezionale (PIM-BiDir), che viene sempre più implementato per applicazioni MOLTI (sorgenti) a MOLTI (ricevitori).

Questi protocolli sono chiamati modalità sparse perché supportano in modo efficiente strutture di recapito multicast IP con una popolazione di ricevitori "sparsa" e creano uno stato del control plane solo sui router nel percorso tra le origini e i ricevitori e in PIM-SM/BiDir, il Rendezvous Point (RP). Non creano mai uno stato in altre parti della rete. Lo stato di un router viene generato in

modo esplicito solo quando riceve un join da un router o un ricevitore downstream, da cui il nome "protocolli di join espliciti".

Sia PIM-SM che PIM-BiDir utilizzano "ALBERI CONDIVISI", che consentono l'inoltro del traffico da qualsiasi origine a un destinatario. Lo stato multicast in una struttura condivisa è detto stato (*,G), dove * è un carattere jolly per QUALSIASI ORIGINE. Inoltre, PIM-SM supporta la creazione di stati correlati al traffico proveniente da una specifica origine. Questi sono noti come ALBERI DI ORIGINE e lo stato associato viene indicato come stato (S,G).

Multicast specifico dell'origine

SSM è il modello utilizzato quando il ricevitore (o un proxy) invia (S,G) "join" per indicare che desidera ricevere il traffico inviato dalla sorgente S al gruppo G. Ciò è possibile con i report di appartenenza in modalità "INCLUDE" di IGMPv3/MLDv2. Questo modello viene indicato come modello SSM (Source-Specific Multicast). SSM impone l'uso di un protocollo di join esplicito tra router. Il protocollo standard per questo è PIM-SSM, che è semplicemente il sottoinsieme di PIM-SM usato per creare alberi (S,G). Stato alberi condivisi (*,G) non presente in SSM.

I ricevitori multicast possono quindi "unirsi" a un gruppo ASM G o "unirsi" (o più precisamente "sottoscrivere" a) a un canale SSM (S,G). Per evitare la ripetizione del termine "gruppo ASM o canale SSM", viene utilizzato il termine flusso (multicast), che implica che il flusso potrebbe essere un gruppo ASM o un canale SSM.

Protocolli Multicast Pertinenti / Tipi Di Pacchetto

Per proteggere una rete multicast, è importante conoscere i tipi di pacchetto più comuni e come proteggerli. I protocolli principali da seguire sono tre:

1. IGMP/MLD
2. PIM
3. MSDP

Nella sezione successiva, ciascuno di questi protocolli viene discusso e vengono illustrati i problemi che possono sorgere rispettivamente con ciascuno di essi.

Pacchetti IGMP/MLD

IGMP / MLD è il protocollo utilizzato dai ricevitori multicast per segnalare ad un router che desiderano ricevere contenuti per un particolare gruppo multicast. IGMP (Internet Group Membership Protocol) è il protocollo utilizzato in IPv4, mentre MLD (Multicast Listener Discovery) è il protocollo utilizzato in IPv6.

Esistono due versioni di IGMP comunemente distribuite, IGMPv2 e IGMPv3. Esistono inoltre due versioni di MLD comunemente distribuite, MLDv1 e MLDv2.

IGMPv2 e MLDv1 sono equivalenti dal punto di vista funzionale, mentre IGMPv3 e MLDv2 sono equivalenti dal punto di vista funzionale.

Questi protocolli sono specificati nei seguenti collegamenti:

IGMPv2: RFC 2236

MLDv1: RFC 3590

IGMPv3 e MLDv2: RFC 4604

IGMPv2 e IGMPv3 non sono solo un protocollo ma anche un protocollo IP IPv4 (in particolare, il protocollo numero 2). Non viene utilizzato solo come descritto in queste RFC per segnalare l'appartenenza a un gruppo multicast, ma anche da altri protocolli multicast IPv4 come DVMRP, PIM versione 1, mtrace e mrinfo. Questo è importante da ricordare quando si cerca di filtrare i dati IGMP (ad esempio tramite ACL Cisco IOS®). In IPv6, MLD non è un protocollo IPv6. per trasportare i pacchetti MLD viene invece utilizzato ICMPv6. PIM versione 2 è lo stesso tipo di protocollo in IPv4 e IPv6 (numero di protocollo 103).

Pacchetti di controllo PIM

In questa sezione vengono discussi i pacchetti di controllo PIM multicast e unicast. Vengono discussi sia Auto-RP che Bootstrap Router (BSR), due modi per selezionare i punti di rendering e controllare le assegnazioni da gruppo a RP nelle reti PIM-SM.

Pacchetti controllo PIM multicast

I pacchetti di controllo PIM multicast includono:

- **PIM Hello** - Il pacchetto PIM Hello è un pacchetto multicast IP con ambito locale al collegamento inviato a un router collegato alla stessa rete per stabilire i router adiacenti PIM.
- **PIM Join/Prune** - I PIM Join/Prune sono pacchetti multicast IP con ambito locale al collegamento inviati per creare/rimuovere lo stato multicast e vengono inviati solo ai vicini PIM. Sono multicast all'interno della LAN per facilitare l'asserzione, la soppressione dei report e altri dettagli del protocollo PIM, ma sono sempre indirizzati a un router adiacente specifico.
- **PIM DF-elect** - PIM Designated Forwarder è il router PIM Bi-Dir responsabile per (*,G) JOIN inviati al punto di ripristino per conto di ricevitori collegati o vicini PIM downstream. Nei casi in cui un router PIM rileva un altro router che invia (*,G) JOIN sullo stesso segmento per lo stesso gruppo G, è possibile scegliere il router con il percorso migliore per l'RP.
- **PIM Assert** - PIM Assert sono pacchetti multicast IP locali al collegamento inviati quando un router PIM collegato a un segmento di rete che inoltra attivamente i pacchetti per un particolare (S,G) da un'interfaccia particolare inizia a RICEVERE i pacchetti per quello stesso (S,G) sulla stessa interfaccia su cui vengono inoltrati. Questo evento indica la presenza di un altro router che potrebbe essere il Single Forwarder (SF) per questo (S,G). Il meccanismo Assert seleziona un'unica IF per tale (S,G). Il router PIM SF viene scelto per inoltrare i pacchetti per un particolare flusso (S,G). PIM consente a router diversi di svolgere il ruolo di IF per conto di (S,G) diversi, idealmente esiste solo un SF per (S,G). Non confondere l'IF con il router designato. Il PIM Designated Router è il router responsabile per JOIN / PRUNES o

SOURCE REGISTERS che vengono inviati al RP in una rete PIM-SM.
- **PIM Bootstrap** - I messaggi PIM Bootstrap vengono inviati in una rete PIMv2 per facilitare la scelta dinamica di un Rendezvous Point per un particolare gruppo G.

Pacchetti di controllo PIM unicast

I pacchetti di controllo PIM unicast vengono indirizzati da o verso l'RP e includono:

- **Source Register Packet** - I pacchetti PIM Source Register vengono inviati per registrare una nuova origine multicast con un punto di rendering. Non appena un'origine inizia a inviare pacchetti multicast, il router designato collegato alla rete di origine invia un flusso di registro unicast all'RP per indicare che esiste un'origine attiva per un gruppo multicast di cui l'RP è responsabile.
  I pacchetti del registro di origine vengono inviati come incapsulamento unicast del flusso multicast originale.
  I messaggi PIM register sono commutati a livello di processo e vengono inviati solo fino a quando l'RP non invia un messaggio di interruzione del registro. L'impatto di questi pacchetti sulle prestazioni è proporzionale alla velocità dell'origine (per flusso (S,G)).
- **Register Stop Packet** - PIM Register Stop I pacchetti vengono inviati dal punto di rendering al DR PIM che ha inviato il messaggio Register. I messaggi Register Stop vengono inviati non appena l'RP inizia a ricevere pacchetti multicast nativi dall'origine.
- **BSR Candidate-Rendezvous Point Advertisement Packet** - PIM BSR C-RP-Advertisement I pacchetti vengono inviati al BSR per pubblicizzare un RP candidato una volta scelto il BSR.

Figura 1: PIM Unicast Packets

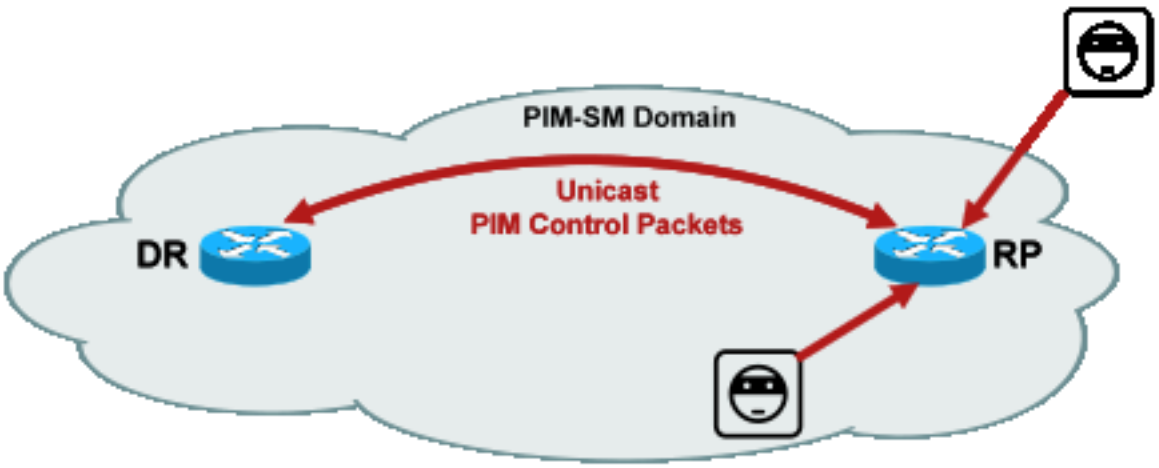

Fig1

_PIM_unicast

Gli attacchi che sfruttano tali pacchetti possono avere origine ovunque, in quanto si tratta di pacchetti unicast.

Pacchetti Auto-RP

Auto-RP è un protocollo sviluppato da Cisco che ha lo stesso scopo di PIMv2 BSR. Auto-RP è stato sviluppato prima di BSR e supporta solo IPv4. BSR supporta IPv4 e IPv6. L'agente di mapping in Auto-RP svolge la stessa funzione del router bootstrap in BSR. Nel BSR, i messaggi provenienti dal C-RP sono unicast verso il router bootstrap. In Auto-RP, i messaggi vengono inviati tramite multicast all'agente di mapping, che consente filtri più semplici al limite, come descritto più avanti. Auto-RP è descritto in dettaglio in questo link: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

In Cisco IOS, i pacchetti AutoRP/BSR vengono sempre inoltrati e al momento non sono disabilitati. Ciò può presentare una particolare esposizione per la sicurezza nel caso di Auto-RP.

Figura 2: Pacchetti Auto-RP

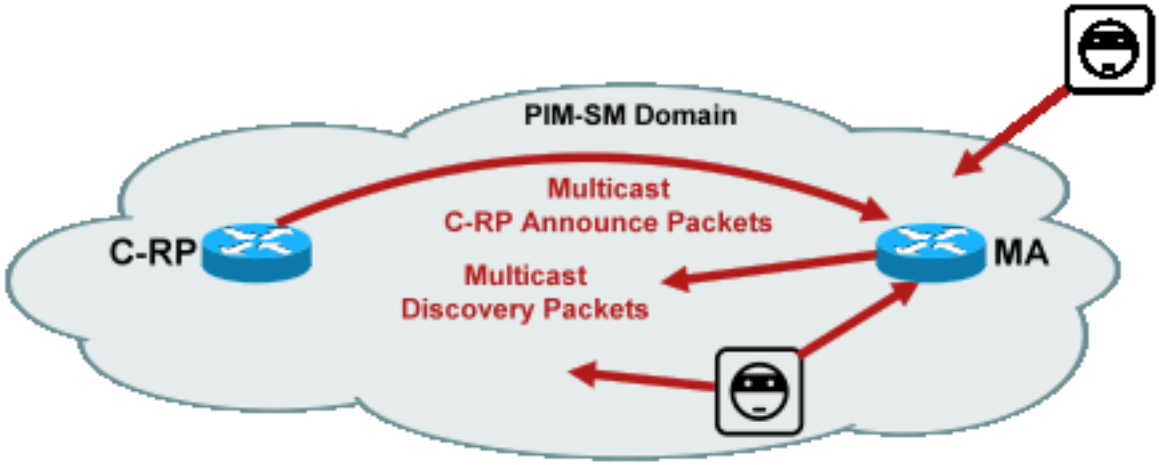

Fig2_AutoRP_packets

Nota: Sebbene Auto-RP sia utilizzato come meccanismo per l'annuncio e il rilevamento di PIM-SM RP, non utilizza pacchetti PIM (IP protocol 103); utilizza la porta UDP (User Datagram Protocol) 496 pacchetti con indirizzi multicast.

Per Auto-RP vengono utilizzati due tipi di pacchetti:

- Pacchetti C-RP-Announce: questi pacchetti sono multicast per tutti gli agenti di mapping e utilizzano un indirizzo "conosciuto" riservato IANA (Internet Assigned Numbers Authority) (24.0.1.39). Sono inviati da un C-RP per annunciare l'indirizzo RP e l'intervallo di gruppi per cui tale RP è in grado di agire come RP.
- Pacchetti di individuazione C-RP: questi pacchetti sono multicast per tutti i router PIM e usano un indirizzo IANA riservato "conosciuto" (24.0.1.40). Vengono inviati dall'agente di mapping Auto-RP per annunciare il C-RP specifico che viene scelto come RP per un particolare intervallo di gruppi.

Ognuno di questi tipi di pacchetto deve essere inoltrato tramite la rete.

In Cisco IOS, sia la versione 224.0.1.39 che la versione 224.0.1.40 vengono inoltrate in modalità Densa PIM per evitare il problema della mancata conoscenza preliminare dell'RP di un gruppo quando tale gruppo viene utilizzato per distribuire informazioni RP. Questo è l'unico uso

consigliato della modalità PIM Dense.

In Cisco IOS XR, i messaggi Auto-RP sono hop-by-hop con flooding (RPF) inverso da router adiacente a router adiacente. Pertanto, non è necessario creare uno stato di route PIM DM per supportare Auto-RP in Cisco IOS XR. Infatti, Cisco IOS XR non supporta affatto PIM-DM.

Pacchetti Multicast Service Discovery Protocol (MSDP)

MSDP è il protocollo IPv4 che consente di annunciare un'origine in un dominio a un destinatario in un altro dominio tramite i rispettivi punti di rendering. MSDP è specificato nella RFC 3618.

Per condividere informazioni sulle origini attive tra domini PIM, viene utilizzato MSDP. Se un'origine diventa attiva in un dominio, MSDP garantisce che tutti i domini peer vengano a conoscenza di questa nuova origine in modo tempestivo, consentendo ai ricevitori di altri domini di entrare rapidamente in contatto con questa nuova origine nel caso in cui questa sia stata inviata a un gruppo in cui i ricevitori hanno un interesse. MSDP è necessario per le comunicazioni multicast ASM/PIM-SM ed è eseguito su una connessione TCP (Transport Control Protocol) unicast configurata tra i punti di Rendezvous nei rispettivi domini.

Minacce in un ambiente multicast

Zone di trust e limiti di trust

Questa sezione del documento è organizzata per entità funzionali nella rete. Il modello di minaccia discusso è strutturato intorno a queste entità. In questo documento viene ad esempio illustrato come proteggere un router in una rete multicast (dal punto di vista multicast), indipendentemente dalla posizione in cui è distribuito. Analogamente, esistono considerazioni su come implementare misure di sicurezza a livello di rete o misure su un router designato, un punto di rendering e così via

Anche le minacce qui descritte seguono questa logica e sono organizzate secondo la funzione logica della rete.

Panoramica delle minacce

A livello astratto, qualsiasi distribuzione multicast può essere soggetta a una serie di minacce su diversi aspetti della sicurezza. Gli aspetti chiave della sicurezza sono la riservatezza, l'integrità e la disponibilità.

- **Minacce alla riservatezza**: Nella maggior parte delle applicazioni, il traffico multicast non è crittografato ed è pertanto accessibile a chiunque per l'ascolto o l'acquisizione su qualsiasi elemento di rete o linea del percorso. Nella sezione su GET VPN vengono illustrati i metodi per crittografare il traffico multicast e prevenire tali attacchi.
- **Minacce all'integrità del traffico**: Senza la sicurezza a livello di applicazione o basata su rete, ad esempio GET VPN, il traffico multicast è vulnerabile alle modifiche in transito. Ciò è

particolarmente importante per il traffico del control plane che utilizza il multicast, ad esempio OSPF, PIM e molti altri protocolli.
- **Minacce all'integrità della rete**: Senza i meccanismi di sicurezza descritti in questo documento, mittenti non autorizzati, destinatari o elementi di rete compromessi possono accedere alla rete multicast, inviare e ricevere traffico senza autorizzazione (furto di servizio) o sovraccaricare le risorse di rete.
- **Minacce alla disponibilità**: Esistono diverse possibilità di attacco Denial of Service che possono rendere le risorse non disponibili agli utenti legittimi.

Nelle sezioni seguenti vengono descritte le minacce per ogni funzione logica della rete.

Minacce di base contro un router

Contro un router esistono diverse minacce fondamentali che sono indipendenti dal fatto che il router supporti il multicast e che l'attacco riguardi il traffico multicast o i protocolli.

Gli attacchi DoS (Denial of Service) sono i più importanti vettori di attacco generici in una rete. In linea di principio, ogni elemento di rete può essere bersaglio di un attacco DoS, che può sovraccaricare l'elemento con una potenziale perdita o degradazione del servizio per gli utenti legittimi. È di fondamentale importanza seguire le raccomandazioni di base per la sicurezza della rete che si applicano a unicast.

Va notato che gli attacchi multicast non sono sempre intenzionali, ma spesso accidentali. Ad esempio, il worm Witty, osservato per la prima volta nel marzo 2004, è un esempio di worm che si è diffuso attraverso attacchi casuali a indirizzi IP. Come conseguenza della completa randomizzazione dello spazio di indirizzi, anche le destinazioni IP multicast sono state influenzate dal worm. In molte organizzazioni, alcuni router di primo hop sono stati compressi perché il worm ha inviato pacchetti a molti indirizzi di destinazione multicast diversi. I router, tuttavia, non avevano l'ambito per un carico di traffico multicast di questo tipo con la creazione dello stato associato e l'esaurimento effettivo delle risorse. Ciò dimostra la necessità di proteggere il traffico multicast, anche se questo non viene utilizzato in un'organizzazione.

Le minacce generiche contro i router includono:

- tutti i tipi di flooding di pacchetti; ad esempio, su percorsi hardware come percorsi lenti (punt) e percorsi software come porte di gestione o control plane, che includono Secure Shell (SSH), Telnet, Border Gateway Protocol (BGP), OSPF, Network Time Protocol (NTP) e così via
- intrusioni nel router e successivo sfruttamento delle funzionalità sul router; le password Telnet o SSH deboli e le stringhe della community SNMP (Simple Network Management Protocol) deboli sono un problema comune nelle reti moderne.
- Problemi operativi come configurazioni errate o attacchi insider possono mettere a rischio la sicurezza dell'intera rete e il suo traffico.

Quando su un router è abilitato il multicast, oltre a unicast deve essere protetto. L'uso del multicast IP non modifica il modello di minaccia fondamentale; consente tuttavia l'utilizzo di protocolli

aggiuntivi (PIM, IGMP, MLD, MSDP) che potrebbero essere soggetti ad attacchi, che devono essere protetti in modo specifico. Quando in questi protocolli viene utilizzato il traffico unicast, il modello di rischio è identico agli altri protocolli eseguiti dal router.

Èimportante notare che il traffico multicast non può essere utilizzato allo stesso modo del traffico unicast per attaccare un router perché il traffico multicast è fondamentalmente "gestito dal destinatario" e non può essere indirizzato a una destinazione remota. Una destinazione di attacco deve essere esplicitamente "unita" al flusso multicast. Nella maggior parte dei casi (l'eccezione principale è Auto-RP), i router ascoltano e ricevono solo il traffico multicast "link local". Il traffico locale del collegamento non viene mai inoltrato. Pertanto, gli attacchi a un router con pacchetti multicast possono avere origine solo da utenti connessi direttamente.

Minacce dal lato dell'origine

Le sorgenti multicast, che si tratti di PC o server video, talvolta non sono sottoposte allo stesso controllo amministrativo della rete. Pertanto, dal punto di vista dell'operatore di rete, il mittente è per lo più considerato non attendibile. Date le potenti funzionalità di PC e server e le complesse impostazioni di sicurezza, spesso incomplete, i mittenti rappresentano una minaccia sostanziale contro qualsiasi rete, inclusa la rete multicast. Queste minacce includono:

- **Attacchi di livello 2:** sul livello 2 è presente una vasta gamma di forme di attacco per eseguire vari tipi di attacchi. Si applicano sia a unicast che a multicast. Poiché queste forme di attacco non sono specifiche del multicast, non vengono descritte in dettaglio in questo documento. Per ulteriori informazioni, consultare il libro Cisco Press "LAN Switch Security", ISBN-10: 1-58705-467-1 .
- **Attacchi con traffico multicast:** come descritto in precedenza, è difficile condurre attacchi con traffico multicast poiché il router del primo hop non inoltra il traffico multicast a meno che non ci sia un listener per il gruppo. Tuttavia, il primo hop può essere attaccato in diversi modi con pacchetti multicast:
- Attacchi di saturazione della rete: Un utente malintenzionato può inondare un segmento di pacchetti multicast, sovrautilizzando la larghezza di banda disponibile, il che può portare a una condizione DoS.
- Attacchi di stato multicast: Il router del primo hop è invaso da pacchetti multicast, che possono creare uno stato troppo grande e una conseguente condizione di attacco DoS.
- Un mittente potrebbe tentare di diventare il DR PIM tramite gli helper PIM inviati. In questi casi, non è possibile inoltrare il traffico da o verso la LAN.
- I pacchetti di selezione DF PIM per BiDir-PIM DF potrebbero essere oggetto di spoofing. In questi casi, non è possibile inoltrare il traffico da o verso la LAN.
- Un mittente potrebbe contraffare i messaggi di bootstrap di AutoRP-discovery o BSR. In questo modo verrebbe effettivamente annunciato un falso RP e verrebbe interrotto un servizio PIM-SM/BiDir.
- Un mittente potrebbe generare attacchi unicast, ad esempio messaggi PIM source register/register-stop, o inviare pacchetti BSR e annunciare un falso BSR.
- Un mittente può inviare messaggi a qualsiasi gruppo multicast valido, a meno che non sia filtrato. Se un indirizzo di origine viene oggetto di spoofing e non viene impedito nel perimetro della rete, il mittente può utilizzare l'indirizzo IP di origine di un mittente legittimo e

sovrascrivere il contenuto in alcune parti della rete.
- Attacchi multicast ai protocolli del control plane: Alcuni protocolli non associati al multicast, ad esempio OSPF e DHCP (Dynamic Host Configuration Protocol), utilizzano pacchetti multicast che possono essere utilizzati per attaccare tali protocolli
- **Mascheramento:** ci sono diverse forme di attacco in cui un mittente può fingere di essere un altro mittente. Gli indirizzi IP di origine oggetto di spoofing sono uno di questi tipi di attacchi.
- **Furto di servizio:** a meno che i mittenti non siano controllati, è possibile utilizzare il servizio multicast in modo illegittimo dal lato mittente.

Nota: Gli host in genere non inviano o ricevono pacchetti PIM. L'host che esegue questa operazione può probabilmente tentare un attacco.

Minacce dal lato del ricevitore

Il ricevitore è anche tipicamente una piattaforma con una notevole potenza della CPU e larghezza di banda, e consente una serie di forme di attacco. Queste sono per la maggior parte identiche alle minacce dal lato mittente. Gli attacchi di livello 2 rimangono un importante vettore di attacco. I ricevitori falsi e i furti di servizio sono possibili anche sul lato ricevente, tranne per il fatto che il vettore di attacco è in genere un attacco IGMP (o di livello 2, come accennato).

Minacce contro un Rendezvous Point e BSR

I PIM-SM RP e i PIM-BSR sono punti critici in una rete multicast, e sono quindi preziosi bersagli per un attacco. Quando nessuno dei due è il router del primo hop, solo le forme di attacco unicast, che includono il protocollo PIM unicast, possono essere indirizzate direttamente verso questi elementi. Le minacce contro RP e BSR includono:

- Tutte le forme di attacco generiche, come descritto nella sezione "Minacce di base contro un router".
- Gli attacchi unicast PIM, potenzialmente con indirizzi IP di origine oggetto di spoofing, consentono attacchi DoS, anche se i messaggi PIM di registrazione o di arresto del registro inviati da un dispositivo dannoso.

Multicast e Unicast Security (a confronto)

Considerazioni sullo stato/filtri

Si consideri la topologia nella Figura 3, che mostra una fonte, tre ricevitori (A, B, C), uno switch (S1) e due router (R1 e R2). La linea blu rappresenta un flusso unicast, mentre la linea rossa rappresenta un flusso multicast. Tutti e tre i ricevitori sono membri del flusso multicast.

Figura 3: Replica in router e switch

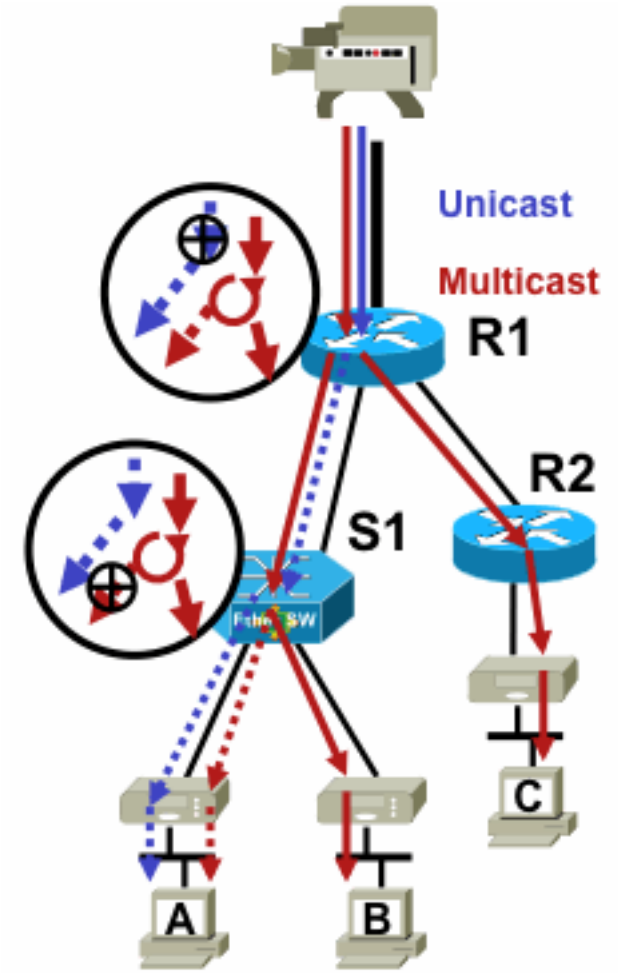

Fig3_replication_RS

Per inibire il flusso del traffico da un'origine specifica a un ricevitore specifico:

- Per il flusso unicast, installare un filtro in qualsiasi punto del percorso dal mittente al destinatario.
- Per il flusso multicast, tuttavia, gli amministratori devono essere più specifici su dove installare i filtri: sul filtro del lato ricevente dopo l'ultimo punto di replica prima del ricevitore; sul filtro del lato origine prima del primo punto di replica dopo l'origine.

Attacchi Da Fonti Multicast

Questa sezione è valida sia per i modelli di servizio ASM sia per SSM, in cui il traffico viene inoltrato in base alla ricezione di join espliciti sul lato ricevente.

Per i flussi unicast non è prevista la protezione implicita del ricevitore. Un'origine unicast può inviare traffico a una destinazione, anche se questa destinazione non ha richiesto il traffico. Pertanto, i meccanismi di difesa, ad esempio i firewall, vengono in genere utilizzati per proteggere i punti finali. Il multicast, d'altro canto, ha una protezione implicita integrata nei protocolli. Il traffico idealmente raggiunge solo un ricevitore che si è unito al flusso in questione.

Con ASM, le origini possono avviare l'inserimento del traffico o attacchi DoS attraverso la trasmissione del traffico multicast a qualsiasi gruppo supportato da un RP attivo. Questo traffico idealmente non raggiunge un destinatario, ma può raggiungere almeno il router del primo hop nel percorso, oltre al router RP, che consente attacchi limitati. Se tuttavia una fonte dannosa è a conoscenza di un gruppo a cui un destinatario è interessato e non sono disponibili filtri appropriati, può inviare traffico a tale gruppo. Questo traffico viene ricevuto finché i ricevitori ascoltano il gruppo.

Con SSM, gli attacchi da fonti indesiderate sono possibili solo sul router del primo hop dove il traffico si arresta se nessun ricevitore si è unito a quel canale (S,G). Ciò non porta a alcun attacco di stato sul router del primo hop perché ignora tutto il traffico SSM per cui non esiste alcuno stato di join esplicito dai ricevitori. In questo modello non è sufficiente che un'origine dannosa sappia a quale gruppo è interessata una destinazione perché i "join" sono specifici dell'origine. In questo caso, per la riuscita dell'operazione sono necessari indirizzi di origine IP oggetto di spoofing più potenziali attacchi di routing.

Attacchi di stato

Anche senza ricevitori presenti in una rete, PIM-SM crea lo stato (S,G) e (*,G) sul router del primo hop più vicino alla sorgente e anche sul punto di rendering. Esiste quindi la possibilità di un attacco di stato sulla rete al router del primo hop di origine e sul PIM-SM RP.

Se una fonte dannosa inizia a inviare traffico a più gruppi, per ognuno dei gruppi rilevati i router della rete creano lo stato all'origine e all'RP, a condizione che i gruppi in questione siano autorizzati dalla configurazione RP.

Pertanto, PIM-SM è soggetto ad attacchi di stato e di traffico da parte delle fonti. L'attacco può essere aggravato se l'origine modifica il proprio indirizzo IP di origine in modo casuale all'interno del prefisso corretto, o in altre parole, vengono falsificati solo i bit host dell'indirizzo.

Figura 4: Attacchi RP ASM

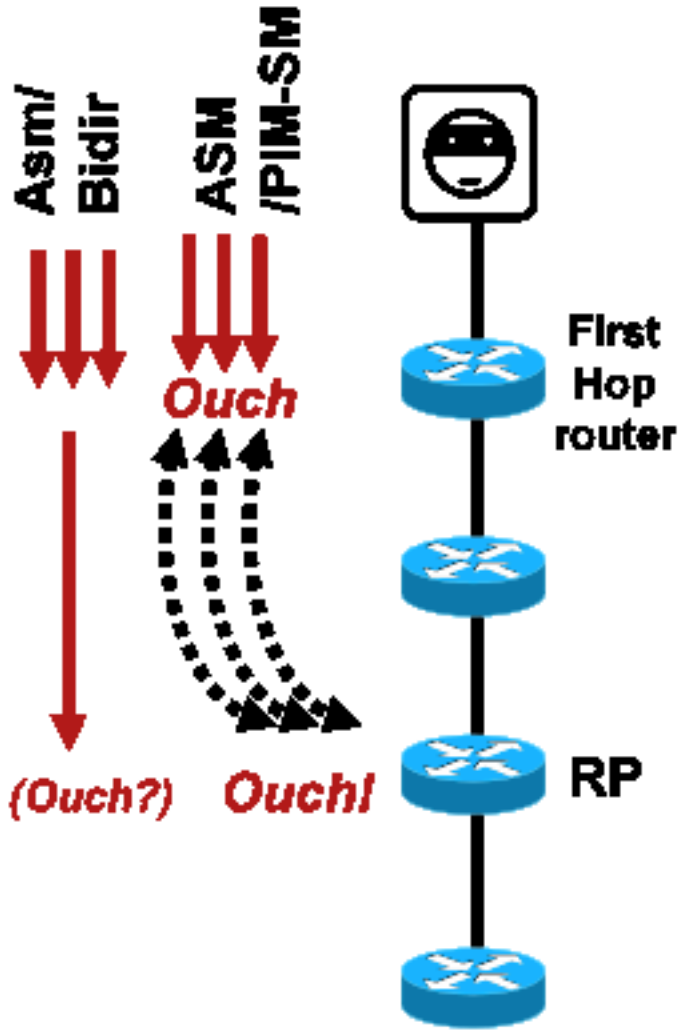

Fig4_ASM_RP_Attacks

Come nel caso del PIM-SSM, gli attacchi PIM-BiDir per la creazione di stati da fonti sono impossibili. Il traffico in PIM-BiDir viene inoltrato sullo stato creato dai join dai ricevitori e sullo stato inoltrato al RP, in modo che possa raggiungere i ricevitori dietro al RP, poiché i join vanno solo al RP. Il traffico da stato a stato successivo all'RP viene chiamato stato (*,G/M) e viene creato dalla configurazione RP (statica, Auto-RP, BSR). Non cambia in presenza di fonti. Pertanto, gli aggressori possono inviare traffico multicast a un PIM-BiDir RP, ma a differenza di PIM-SM, un PIM-BiDir RP non è un'entità "attiva", ma semplicemente inoltra o scarta il traffico per i gruppi PIM-BiDir.

> **Nota:** Su alcune piattaforme Cisco IOS (*,G/M) lo stato non è supportato. In questi casi, le origini possono attaccare il router trasmettendo il traffico multicast a più gruppi PIM-BiDir, causando la creazione dello stato (*,G). Ad esempio, lo switch Catalyst 6500 supporta gli stati (*,G/M).

Attacchi originati dal ricevitore

Gli attacchi possono provenire da ricevitori multicast. Qualsiasi ricevitore che invia un report IGMP/MLD in genere crea lo stato sul router del primo hop. In unicast non esiste un meccanismo equivalente.

Figura 5: Inoltro del traffico basato sul join esplicito lato ricevitore

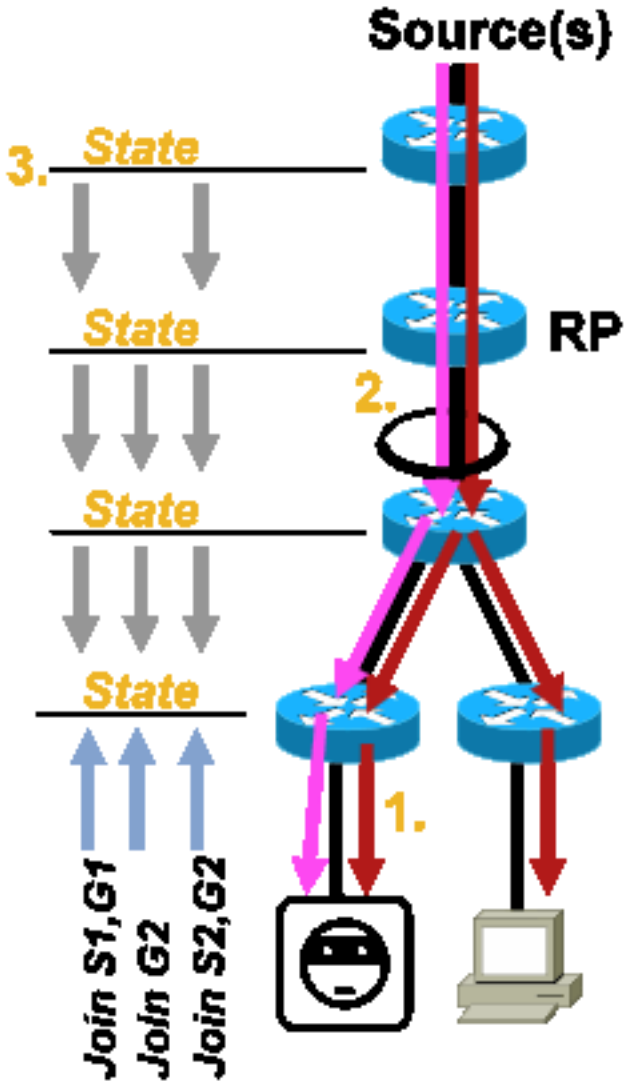

Fig5_Receiver_Explicit_Join

Gli attacchi dei ricevitori possono essere di tre tipi:

1. Un ricevitore multicast può tentare di unirsi a un flusso per il quale non è autorizzato e di ricevere contenuto che non è autorizzato a ricevere.
2. Un ricevitore multicast può potenzialmente sovraccaricare la larghezza di banda di rete disponibile a causa dell'interesse in molti gruppi o canali. Questo tipo di attacco diventa un attacco di larghezza di banda condivisa contro altri potenziali destinatari di contenuti.
3. Un ricevitore multicast può tentare di lanciare un attacco contro router o switch. È possibile generare un numero elevato di report IGMP, che possono creare una grande quantità di stato della struttura multicast e sovraccaricare potenzialmente la capacità del router. Ciò a sua volta può causare un aumento dei tempi di convergenza multicast o un aumento della funzionalità DoS del router.

Nella sezione successiva, dedicata alla protezione all'interno di una rete multicast, sono disponibili diversi metodi per mitigare questo tipo di attacchi.

Sicurezza all'interno di una rete multicast

Sicurezza degli elementi di rete

La sicurezza non è una caratteristica specifica, ma una parte intrinseca di ogni progettazione di rete. Per questo motivo, la sicurezza deve essere presa in considerazione in ogni punto della rete. È di fondamentale importanza che ogni singolo elemento della rete sia adeguatamente protetto. Un possibile scenario di attacco, applicabile a qualsiasi tecnologia, è un router sovvertito da un intruso. Una volta che un intruso ha il controllo di un router, può eseguire una serie di diversi scenari di attacco. Ciascun elemento di rete deve pertanto essere adeguatamente protetto da qualsiasi forma di attacco di base e da attacchi multicast specifici.

Control Plane Policing (CoPP)

Il protocollo CoPP è l'evoluzione degli ACL del router (o ACL) e è disponibile sulla maggior parte delle piattaforme. Il principio è lo stesso: solo il traffico destinato al router è sottoposto a policy dal protocollo CoP.

I criteri del servizio utilizzano la stessa sintassi dei criteri Quality of Service, con mappe dei criteri e mappe delle classi. Pertanto, estende la funzionalità degli rACL (autorizzazione/rifiuto) con limitatori di velocità per alcuni traffici verso il control plane.

> **Nota:** Su alcune piattaforme, ad esempio gli switch Catalyst serie 9000, il protocollo CoPP è abilitato per impostazione predefinita e la protezione non è sostituita. Per ulteriori informazioni, vedere la guida del protocollo CoPP.

Se si decide di regolare, modificare o creare gli ACL o il CoPP in una rete attiva, è necessario procedere con cautela. Poiché entrambe le funzionalità sono in grado di filtrare tutto il traffico diretto al control plane, tutti i protocolli del control plane e del management obbligatori devono essere esplicitamente autorizzati. L'elenco dei protocolli richiesti è molto ampio e può essere facile ignorare i protocolli meno ovvi, come il Terminal Access Controller Access Control System (TACACS). Tutte le configurazioni rACL e CoPP non predefinite devono essere sempre testate in un ambiente lab prima della distribuzione nelle reti di produzione. Inoltre, le installazioni iniziali devono iniziare solo con una politica di "autorizzazione". Ciò consente la convalida di eventuali riscontri imprevisti con contatori di riscontri ACL.

In un ambiente multicast, i protocolli multicast richiesti (PIM, MSDP, IGMP, ecc.) devono essere consentiti in rACL o CoPP affinché il multicast funzioni correttamente. È importante ricordare che il primo pacchetto in un flusso multicast dall'origine in uno scenario PIM-SM viene utilizzato come pacchetto del piano di controllo, per facilitare la creazione dello stato multicast, fino al piano di controllo del dispositivo. È quindi importante autorizzare i gruppi multicast rilevanti negli elenchi ACL o CoPP. Poiché esistono numerose eccezioni specifiche della piattaforma, è importante consultare la documentazione pertinente e testare qualsiasi configurazione pianificata prima della distribuzione.

Servizio Local Packet Transport Service (LPTS)

Su Cisco IOS XR, il servizio LPTS (Local Packet Transport Service) svolge il ruolo di policer del traffico diretto al control plane del router, in modo simile al protocollo CoPP su Cisco IOS. Inoltre, il traffico di ricezione, che include il traffico unicast e multicast, può essere filtrato e la velocità limitata.

Sicurezza specifica del multicast

In una rete abilitata per il multicast, ogni elemento di rete deve essere protetto con funzionalità di protezione specifiche per il multicast. come descritto in questa sezione, per la protezione generica del router. Nella sezione successiva vengono descritte le funzionalità che non sono necessarie su ogni router, ma solo in percorsi specifici della rete, e le funzionalità che richiedono l'interazione tra router (ad esempio l'autenticazione PIM).

Limiti route

Il comando route limit limita la quantità di route multicast a livello globale su un router e consente di prevenire attacchi DoS.

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

Figura 6: Limiti route

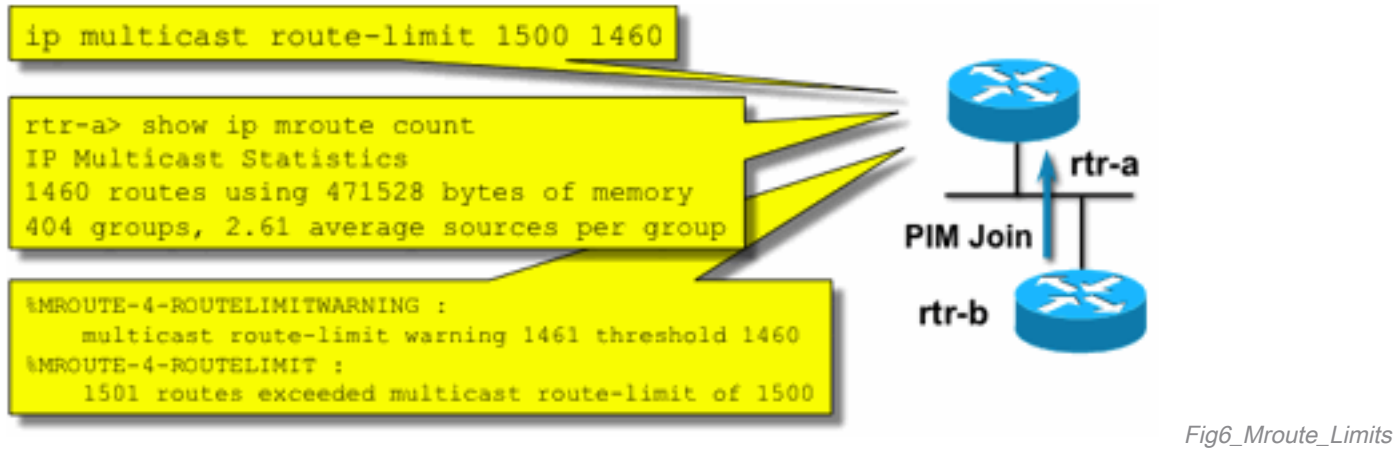

Fig6_Mroute_Limits

I limiti delle route consentono di impostare una soglia per il numero di route consentite nella tabella di routing multicast. Se è abilitato un limite di route multicast, non viene creato alcuno stato multicast oltre il limite configurato. Esiste anche una soglia di avvertenza. Quando il numero di route supera la soglia di avviso, vengono attivati messaggi di avviso syslog. Al limite di route, eventuali altri pacchetti che attiverebbero lo stato vengono scartati.

il comando **ip multicast route-limit** è disponibile anche per MVRF.

Disabilita ascolto SAP: nessun ascolto ip sap

Il comando **sap** Listen determina la ricezione da parte di un router di messaggi SDP (Session Announcement Protocol/Session Description Protocol). SAP/SDP è un protocollo legacy che risale ai giorni della backbone multicast (MBONE). Questi messaggi indicano informazioni sulle directory relative al contenuto multicast disponibili in futuro o al momento. Poiché questa può essere

l'origine di un'operazione DoS contro le risorse di memoria e CPU del router, è necessario disabilitare questa funzionalità.

Controllare l'accesso alle informazioni mrinfo - comando "ip multicast mrinfo-filter"

Il comando mrinfo (disponibile su Cisco IOS e anche su alcune versioni di Microsoft Windows e Linux) utilizza vari messaggi per interrogare un router multicast e ottenere informazioni. Il comando di configurazione globale **ip multicast mrinfo-filter** può essere usato per limitare l'accesso a queste informazioni a un sottoinsieme di origini o per disabilitarle completamente.

In questo esempio vengono negate le query originate da 192.168.1.1, mentre le query sono consentite da qualsiasi altra origine:

```
ip multicast mrinfo-filter 51

access-list 51 deny 192.168.1.1
access-list 51 permit any
```

Questo esempio nega *mrinfo* richieste provenienti da qualsiasi origine:

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

> **Nota:** Come previsto con gli ACL, il valore *deny* indica che il pacchetto è filtrato, mentre il valore *allow* indica che il pacchetto è autorizzato.

Se il comando **mrinfo** viene usato a scopo diagnostico, si consiglia di configurare il comando **ip multicast mrinfo-filter** con un ACL appropriato per consentire le query solo da un sottoinsieme di indirizzi di origine. Le informazioni fornite dal comando *mrinfo* possono essere recuperate anche tramite SNMP. Si consiglia vivamente di completare blocchi di richieste mrinfo (bloccare qualsiasi origine dalle query del dispositivo).

Sicurezza della rete

In questa sezione vengono illustrati vari modi per proteggere i pacchetti di controllo multicast e unicast PIM, nonché Auto-RP e BSR.

Disabilita gruppi multicast

I comandi **ip multicast group-range/ipv6 multicast group range** possono essere usati per disabilitare tutte le operazioni per i gruppi negati dall'ACL:

```
ip multicast group-range <std-acl>
ipv6 multicast group-range <std-acl>
```

Se vengono visualizzati pacchetti per uno dei gruppi negati dall'ACL, vengono scartati in tutti i protocolli di controllo, compresi PIM, IGMP, MLD, MSDP, e vengono anche scartati sul piano dati. Pertanto, per questi intervalli di gruppi non vengono mai create voci della cache IGMP/MLD, stato PIM, Multicast Routing Information Base/Multicast Forwarding Information Base (MRIB/MFIB) e

tutti i pacchetti di dati vengono immediatamente eliminati.

Questi comandi vengono immessi nella configurazione globale del dispositivo.

Si consiglia di distribuire questo comando su tutti i router della rete, quando e dove disponibile, in modo che tutto il traffico multicast proveniente dall'esterno della rete venga controllato. Questi comandi hanno effetto sul piano dati e sul piano di controllo. Se disponibile, questo comando offre una copertura più ampia degli ACL standard ed è preferibile.

PIM Security

PIM Neighbor Control

Un router PIM deve ricevere gli helo PIM per stabilire una relazione PIM. La vicinanza PIM è anche la base per la scelta del router designato (DR) e il failover DR, oltre che per i messaggi PIM Join/Prune/Assert inviati/ricevuti.

Figura 7: PIM Neighbor Control

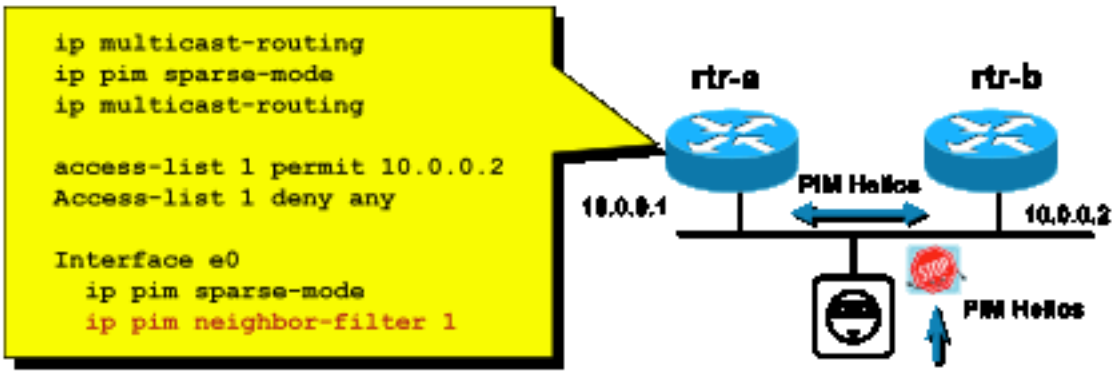

Fig7_PIM_neighbor_control

Per inibire la presenza di vicini indesiderati, utilizzare il **ip pim neighbors-filter** illustrato nella Figura 7. Questo comando filtra tutti i pacchetti PIM adiacenti non consentiti, compresi i pacchetti Hellos, Join/Prune e BSR. Gli host sul segmento possono potenzialmente contraffare l'indirizzo IP di origine per fingere di essere adiacenti al PIM. Per impedire che gli indirizzi di origine provino a falsificare i tentativi su un segmento o usare un ACL VLAN nello switch di accesso, sono necessari meccanismi di sicurezza di layer 2 (ossia IP source guard). La parola chiave "log-input" può essere usata negli ACL per registrare i pacchetti che corrispondono all'ACE.

Il pacchetto di unione/eliminazione PIM viene inviato a un router adiacente PIM per aggiungere o rimuovere tale router da un percorso particolare (S,G) o (*,G). I pacchetti multicast PIM sono pacchetti multicast locali di collegamento inviati con un valore TTL (Time-To-Live)=1. Tutti questi pacchetti sono multicast all'indirizzo noto di tutti i router PIM: 224.0.0.13 . Ciò significa che tutti gli attacchi di questo tipo devono avere origine nella stessa subnet del router attaccato. Gli attacchi possono includere pacchetti forgiati Hello, Join/Prune e Assert.

Nota: Un aumento artificiale o una regolazione del valore TTL nei pacchetti multicast PIM su

un valore superiore a 1 non crea problemi. L'indirizzo All-PIM-Router viene sempre ricevuto e trattato localmente su un router. Non viene mai inoltrato direttamente da router normali e legittimi.

Per proteggere l'RP da una potenziale inondazione di messaggi di registro PIM-SM, il DR deve limitare questi messaggi. Utilizzare il comando **ip pim register-rate-limit**:

```
ip pim register-rate-limit <count>
```

Figura 8: Controllo tunnel registro PIM-SM

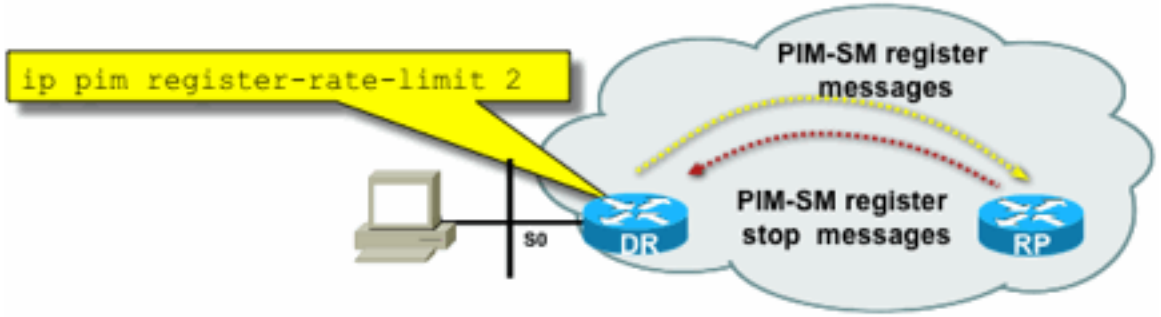

Fig8_PIMSM_Reg Tunnel

I pacchetti unicast PIM possono essere utilizzati per attaccare l'RP. Pertanto, l'RP può essere protetto da ACL di infrastruttura contro tali attacchi. Tenere presente che i mittenti e i riceventi multicast non hanno mai bisogno di inviare pacchetti PIM, quindi il protocollo PIM (protocollo IP 103) può in genere essere filtrato sul perimetro del sottoscrittore.

Controllo Auto-RP - Filtro annuncio RP

Il comando **ip pim rp-notice filter** è una misura di sicurezza aggiuntiva che può essere configurata con Auto-RP quando possibile:

```
ip pim rp-announce-filter
```

È possibile configurare l'agente di mapping in modo da controllare quali router vengono accettati come RP candidati per intervalli di gruppi/modalità gruppo.

Figura 9: Auto-RP - Filtro annuncio RP

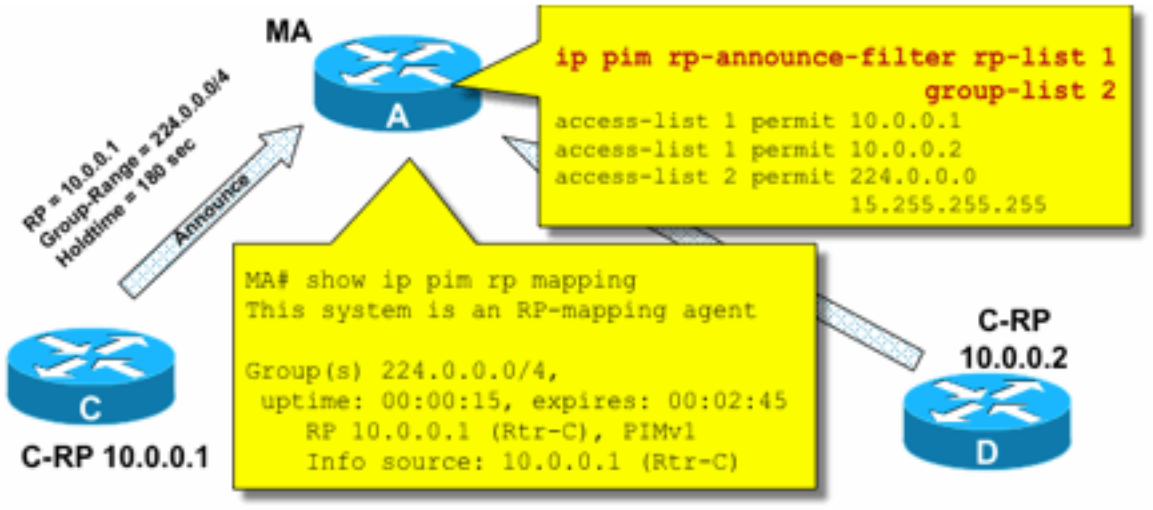

Fig9_AutoRP_RP_Announce

Controllo Auto-RP - Vincola messaggi Auto-RP

Utilizzare il comando multicast boundary per vincolare i pacchetti AutoRP, RP-notice (24.0.1.39) o RP-discover (224.0.1.40) a un particolare dominio PIM:

```
ip multicast boundary
```

Figura 10: Comando Limite Multicast

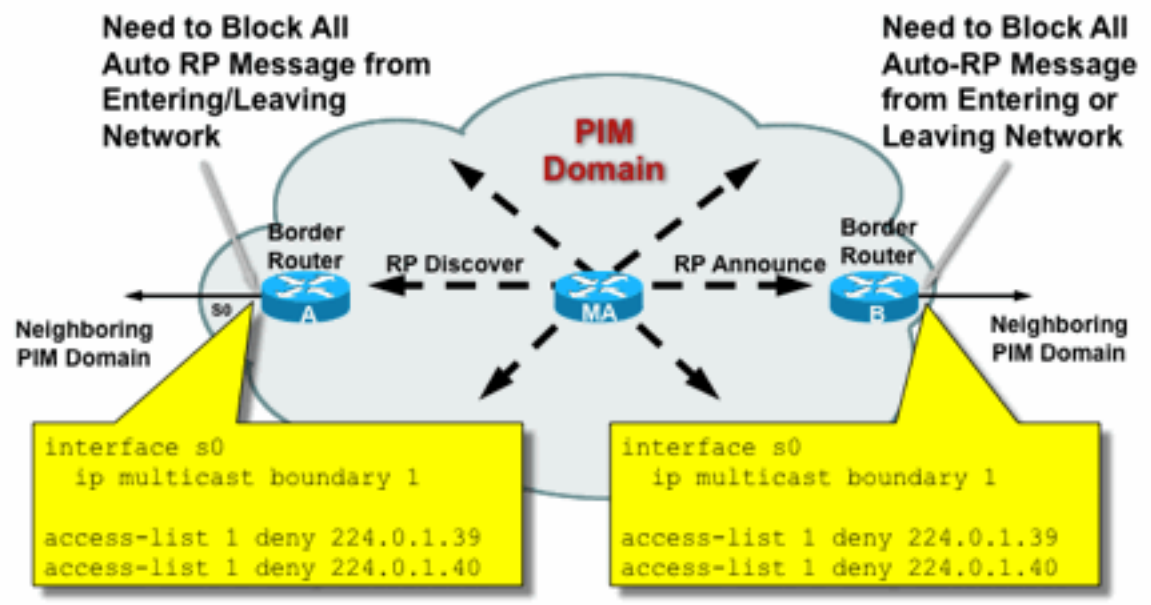

Fig10_Mcast_Boundary

Controllo BSR - Limitazione dei messaggi BSR

Utilizzare il **bordo bsr ip pim** per filtrare i messaggi BSR al bordo di un dominio PIM. Non è necessario alcun ACL poiché i messaggi BSR vengono inoltrati hop per hop con il multicast locale del collegamento.

Figura 11: Bordo BSR

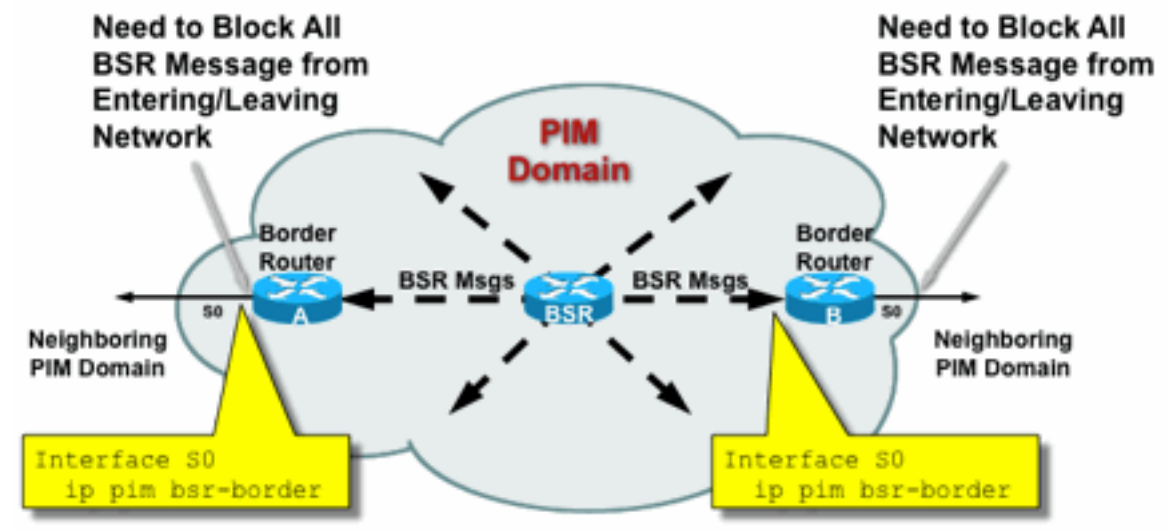

Fig11_BSR_Router

Filtri correlati a RP / PIM-SM

In questa sezione finale vengono trattati i filtri in base ai pacchetti del control plane PIM-SP e RP, nonché i messaggi Auto-RP, BSR e MSDP.

Filtri Auto-RP

La Figura 12 mostra un esempio di filtri Auto-RP in combinazione con gli ambiti degli indirizzi. Vengono mostrati due modi diversi per collegare una regione. I due ACL sono equivalenti nella prospettiva Auto-RP.

Figura 12: Filtri/ambiti RP automatici

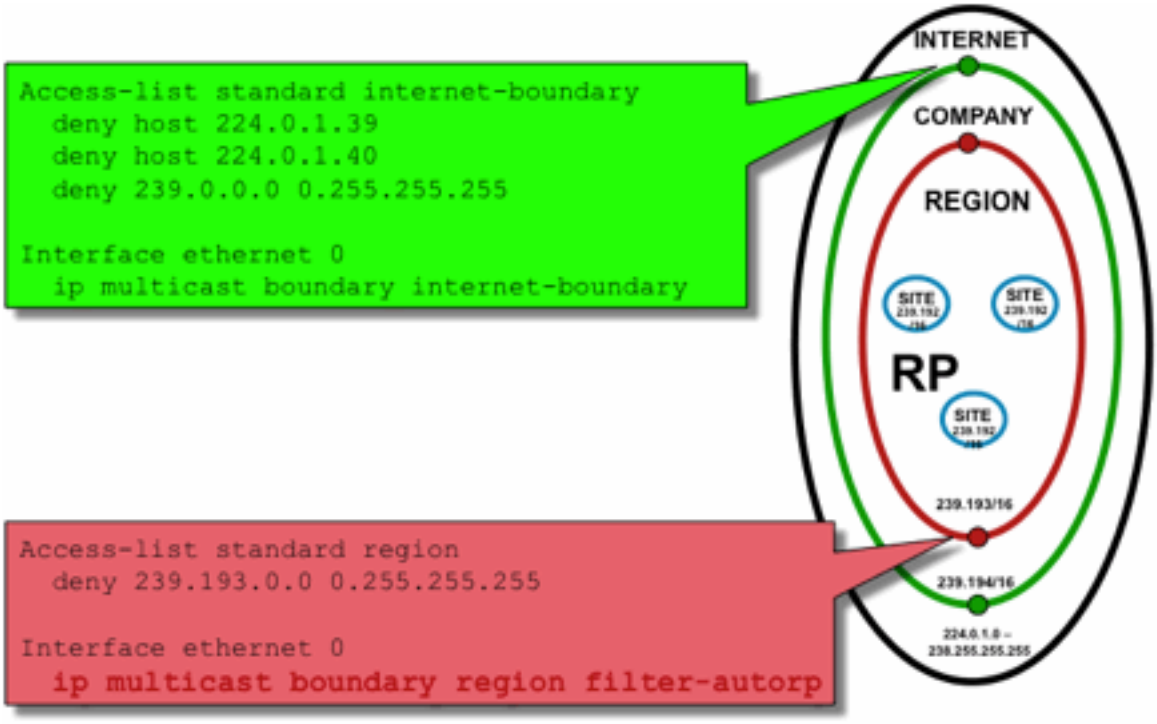

Fig12_AutoRP_Filtering_Scoping

L'idea dei filtri dei limiti di interfaccia per Auto-RP è quella di garantire che gli annunci auto-rp raggiungano solo le regioni che supportano. Sono definiti ambiti regionali, aziendali e a livello di Internet e in ogni caso sono presenti RP e annunci Auto-RP in ogni ambito. Gli amministratori desiderano solo che le RP regionali siano note ai router regionali, le RP aziendali ai router regionali e aziendali e desiderano che tutte le RP Internet siano disponibili a livello globale. Sono possibili ulteriori livelli di ambito.

Come mostrato nella figura, esistono due modi fondamentalmente diversi di filtrare i pacchetti Auto-RP: Il limite Internet richiama esplicitamente i gruppi di controllo auto-rp (224.0.1.39 e 224.0.1.40), che danno luogo a filtri per tutti i pacchetti Auto-Rp. Questo metodo può essere utilizzato al limite di un dominio amministrativo, dove non vengono passati pacchetti Auto-RP. Il limite Region utilizza la parola chiave filter-auto-rp per causare un esame degli annunci rp-to-group-range all'interno dei pacchetti Auto-RP. Quando un annuncio viene esplicitamente negato dall'ACL, viene rimosso dal pacchetto Auto-RP prima che il pacchetto venga inoltrato. Nell'esempio, questo consente di conoscere le RP a livello aziendale all'interno delle regioni, mentre le RP a livello regionale sono filtrate al limite della regione per il resto dell'azienda.

Filtri interdominio e MSDP

Nell'esempio, ISP1 agisce come provider di transito PIM-SM. Supportano solo il peer MSDP con i router adiacenti e accettano solo (S,G), ma non il traffico (*,G) sui router di confine.

Nell'interdominio (generalmente tra sistemi autonomi) è necessario adottare due misure di sicurezza di base:

1. Proteggere il piano dati tramite il comando **multicast boundary**. In questo modo il traffico multicast viene accettato solo per gruppi definiti e potenzialmente per le origini.
2. Proteggere il traffico del control plane (MSDP) tra domini. Si tratta di una serie di misure di sicurezza distinte: Controllo contenuto MSDP, limitazione dello stato e autenticazione router adiacenti.

La Figura 13 fornisce un esempio di configurazione di un filtro di interfaccia su uno dei router di confine dell'ISP1.

Per proteggere il piano dati al confine del dominio, inibire (*,G) i join tramite filtri contro "host 0.0.0.0" e indirizzi con ambito amministrativo tramite il comando **multicast boundary**:

Figura 13: Filtro interdominio (*,G)

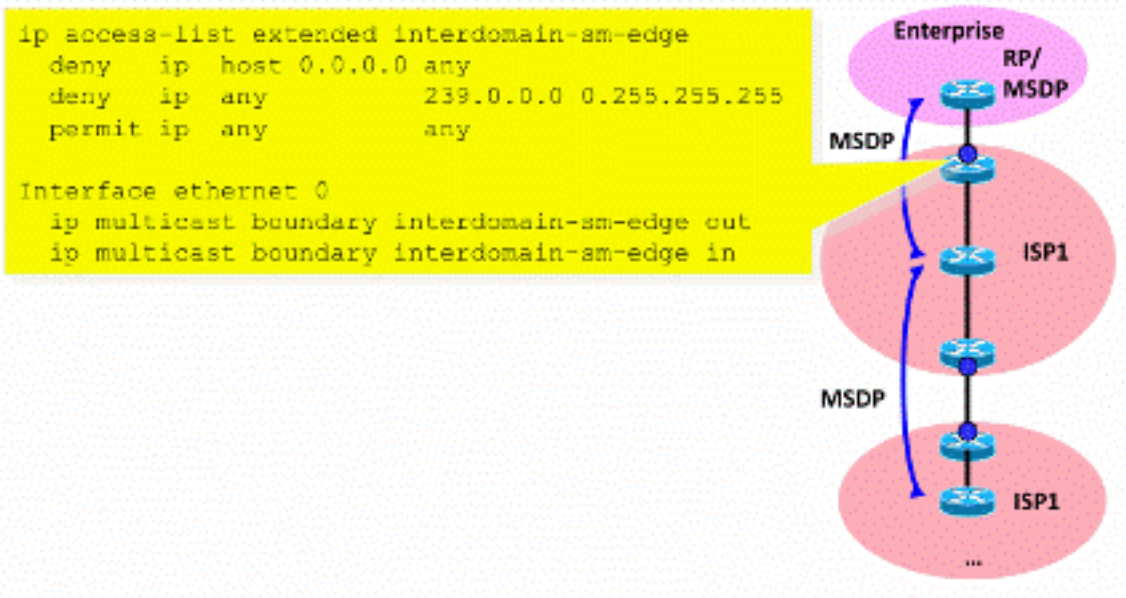

Fig13_Filtro_Interdominio

Per proteggere il control plane, fortificare MSDP tramite tre misure di sicurezza di base:

1) Filtri SA MSDP

Èconsigliabile filtrare il contenuto dei messaggi MSDP tramite i filtri SA MSDP. L'idea principale di questo filtro è evitare la propagazione dello stato multicast per le applicazioni e i gruppi che non sono applicazioni a livello di Internet e che non devono essere inoltrati oltre il dominio di origine. Idealmente, dal punto di vista della sicurezza, i filtri consentono solo i gruppi noti (e potenzialmente i mittenti) e negano tutti i mittenti e/o i gruppi sconosciuti.

Generalmente non è possibile elencare esplicitamente tutti i mittenti e/o i gruppi consentiti. si consiglia di utilizzare il filtro di configurazione predefinito per i domini PIM-SM con un singolo RP per ogni gruppo (senza mesh-group MSDP):

```
!--- 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 !
```

È consigliabile filtrare nel modo più rigoroso possibile e in entrambe le direzioni, in entrata e in uscita.

Utilizzare per ulteriori dettagli sulle raccomandazioni relative ai filtri SA MSDP: https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2) Limitazione dello stato di MSDP

Quando MSDP è abilitato tra più sistemi autonomi (AS), si consiglia di limitare la quantità di stato generato nel router a causa dei messaggi "Source-Active" (SA) ricevuti dai router adiacenti. È possibile utilizzare il comando **ip msdp sa-limit**:

```
ip msdp sa-limit <peer> <limit>
```

Figura 14: Control Plane MSDP

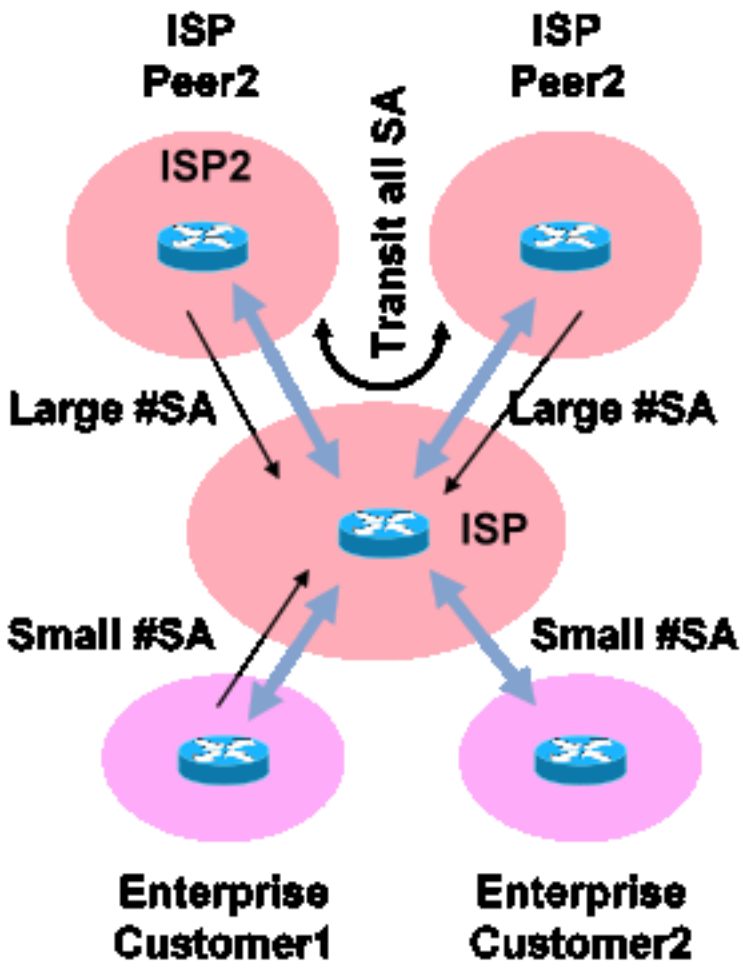

Fig14_MSDP_ControlPlane

Il comando **ip msdp sa-limit** consente di limitare il numero di stati SA creati in seguito all'accettazione di messaggi SA da un peer MSDP. Alcune semplici raccomandazioni pratiche includono:

- Limite minimo da stub-neighbor
- Limite grande dal router adiacente di transito (ad esempio, il numero massimo di associazioni di protezione in Internet)
- ISP transit - configurare il numero massimo di #SA supportati dalla piattaforma

3) Autenticazione router adiacente MSDP MD5

Èconsigliabile utilizzare l'autenticazione della password MD5 (Message-Digest Algorithm) sui peer MSDP. In questo modo viene utilizzata l'opzione di firma TCP MD5, equivalente all'utilizzo descritto nella RFC 691 per proteggere BGP.

Figura 15: Autenticazione router adiacente MSDP MD5

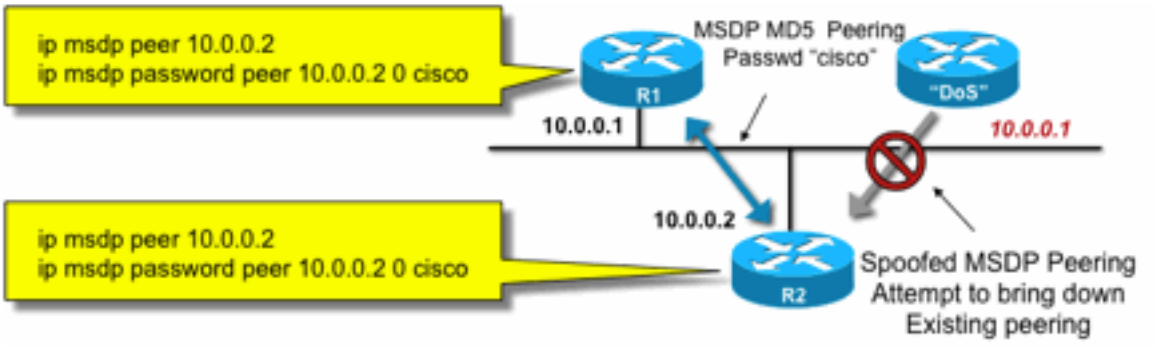

Fig15_MSDP_MD5Auth

Le tre raccomandazioni di sicurezza di MSDP seguenti perseguono obiettivi diversi:

- L'autenticazione tramite router adiacenti (con MD5) garantisce che solo i peer MSDP attendibili possano inviare messaggi.
- I filtri SA garantiscono che anche un peer MSDP attendibile possa inviare solo annunci SA in linea con i criteri di origine/gruppo prestabiliti.
- Il limite dell'associazione di protezione garantisce inoltre che, anche con gli annunci legittimi (S,G) provenienti da peer legittimi, la memoria disponibile non possa essere esaurita.

Problemi mittente/origine

Molti problemi di protezione multicast che hanno origine presso il mittente possono essere risolti con meccanismi di protezione unicast appropriati. Di seguito sono riportati alcuni meccanismi di protezione unicast consigliati:

- **Protezione da spoof dell'indirizzo di origine** (inoltro percorso inverso unicast, uRPF o ACL e protezione origine IP per il livello di accesso)
- **ACL di infrastruttura** (deny ip any (to) <spazio indirizzi principale>)

Tali misure possono essere utilizzate per bloccare attacchi diretti al nucleo. Ad esempio, questa procedura potrebbe risolvere problemi come attacchi che usano pacchetti unicast PIM all'RP, che si trova "all'interno" della rete e sarebbe quindi protetto dall'ACL dell'infrastruttura.

Controllo degli accessi basato sul filtro pacchetti - Origini controllo

Nell'esempio mostrato nella Figura 16, il filtro è configurato sull'interfaccia LAN (E0) del router multicast del primo hop (router designato). Il filtro è definito da un elenco di controllo di accesso esteso denominato "source". Questo ACL viene applicato all'interfaccia dell'origine del router designato collegato alla LAN di origine. A causa della natura del traffico multicast, potrebbe essere necessario configurare un filtro simile su tutte le interfacce connesse a una LAN sulle quali le origini potrebbero diventare attive. Poiché non è sempre possibile sapere esattamente dove si verifica l'attività di origine, si consiglia di applicare tali filtri a tutti i punti di ingresso nella rete.

Figura 16: Origini controllo

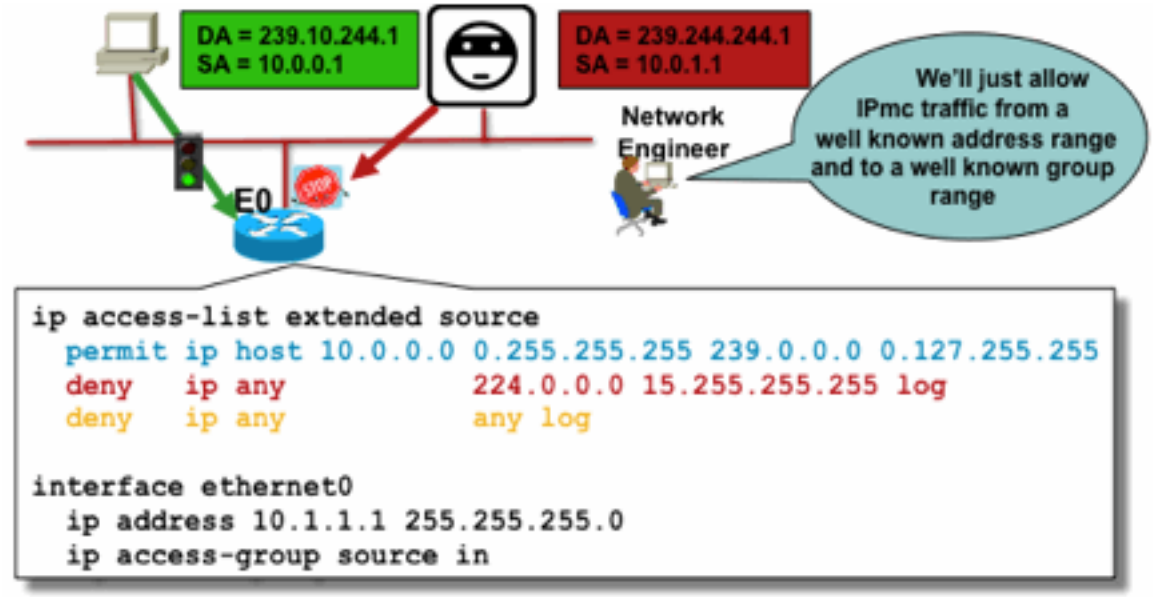

Fig16_Origini_Controllo

Lo scopo di questo filtro è impedire il traffico da un'origine o un intervallo di indirizzi di origine specifico a un gruppo o un intervallo di indirizzi di gruppo specifico. Questo filtro agisce prima che PIM crei route e contribuisce a limitare lo stato.

Questo è un ACL di un piano dati standard. Questo viene implementato sugli ASIC su piattaforme di fascia alta e non comporta alcuna penalizzazione delle prestazioni. Gli ACL dei piani dati sono consigliati e preferiti sul piano di controllo per le origini con connessione diretta, in quanto riducono al minimo l'impatto del piano di controllo del traffico indesiderato. È anche molto efficace limitare la destinazione (indirizzi di gruppi multicast IP) a cui è possibile inviare i pacchetti. Poiché si tratta di un comando di router, non può superare un indirizzo IP di origine oggetto di spoofing (vedere la parte precedente di questa sezione). Pertanto, si consiglia di fornire meccanismi aggiuntivi di layer 2 (L2) o una policy coerente per tutti i dispositivi che possono connettersi a una particolare rete locale/VLAN (Virtual Local Area Network).

> **Nota:** La parola chiave "log" in un ACL è molto utile per capire i riscontri relativi a una voce dell'ACL specifica; tuttavia, questa operazione consuma risorse della CPU e deve essere gestita con attenzione. Inoltre, sulle piattaforme basate su hardware, i messaggi di log ACL vengono prodotti da una CPU, quindi è necessario considerare l'impatto della CPU.

Controllo del codice sorgente PIM-SM

Uno dei vantaggi effettivi dell'architettura ASM/PIM-SM dal punto di vista della sicurezza è il fatto che Rendezvous Point fornisce un unico punto di controllo per tutte le fonti nella rete per qualsiasi intervallo di gruppi. Questa condizione può essere sfruttata con un dispositivo chiamato filtro accept-register. Il comando per questo filtro è il seguente:

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

Figura 17: Controllo del codice sorgente PIM-SM

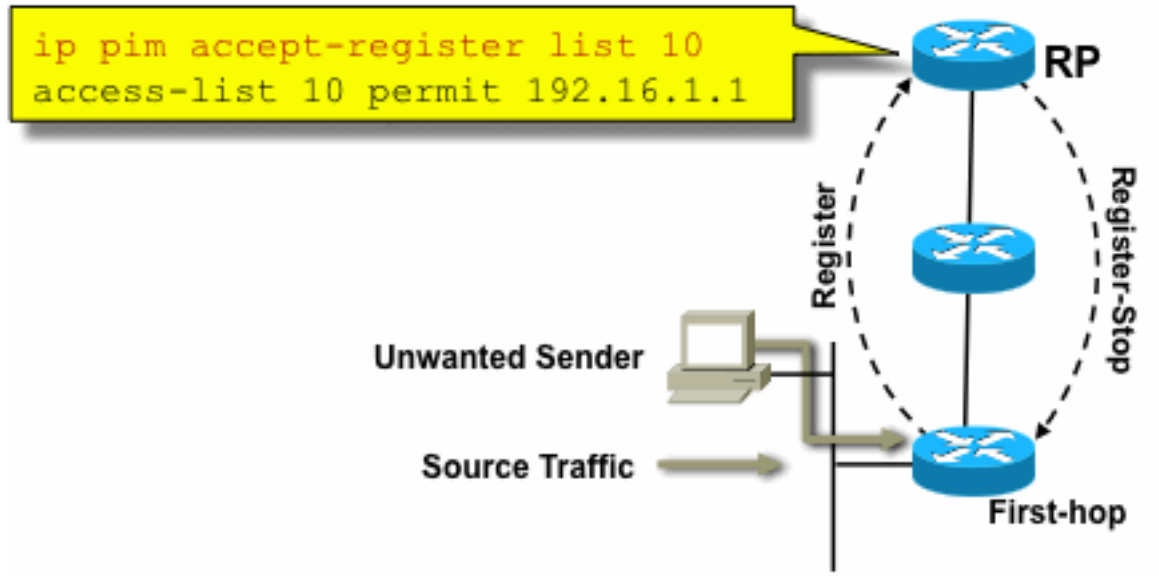

Fig17_PIMSM_Control

In una rete PIM-SM, con questo comando è possibile controllare una fonte di traffico indesiderata. Quando il traffico di origine colpisce il router del primo hop, il router del primo hop (DR) crea lo stato (S,G) e invia un messaggio PIM Source Register all'RP. Se l'origine non è elencata nell'elenco di filtri di accettazione-registrazione (configurato nell'RP), l'RP rifiuta il registro e invia un messaggio di registrazione-interruzione immediato al DR.

Nell'esempio mostrato, un ACL semplice è stato applicato all'RP, che filtra solo l'indirizzo di origine. È possibile anche filtrare l'origine E il gruppo usando un ACL esteso sull'RP.

I filtri di origine presentano alcuni inconvenienti perché con il comando **pim accept-register** sull'RP, lo stato PIM-SM (S,G) viene ancora creato sul router del primo hop dell'origine. Ciò può generare traffico nei ricevitori locali verso l'origine e situati tra l'origine e l'RP. Inoltre, il comando **pim accept-register** funziona sul piano di controllo dell'RP. Ciò potrebbe essere utilizzato per sovraccaricare l'RP con messaggi di registro falsi e probabilmente causare una condizione DoS.

Si consiglia di applicare il comando pim accept-register sull'RP in aggiunta ad altri metodi, come l'applicazione di semplici ACL data plane su tutti i DR, su tutti i punti in entrata nella rete. Sebbene gli ACL in entrata sul DR siano sufficienti in una rete perfettamente configurata e gestita, si consiglia di configurare il comando **pim accept-register** sull'RP come meccanismo di sicurezza secondario in caso di configurazioni errate sui router perimetrali. I meccanismi di sicurezza a più livelli con lo stesso obiettivo sono chiamati "difesa in profondità" ed è un principio di progettazione comune nella sicurezza.

Problemi del ricevitore - Controllo IGMP/MLD

La maggior parte dei problemi del ricevitore rientrano nel dominio delle interazioni del protocollo del ricevitore IGMP/MLD.

Figura 18: Controlla IGMP

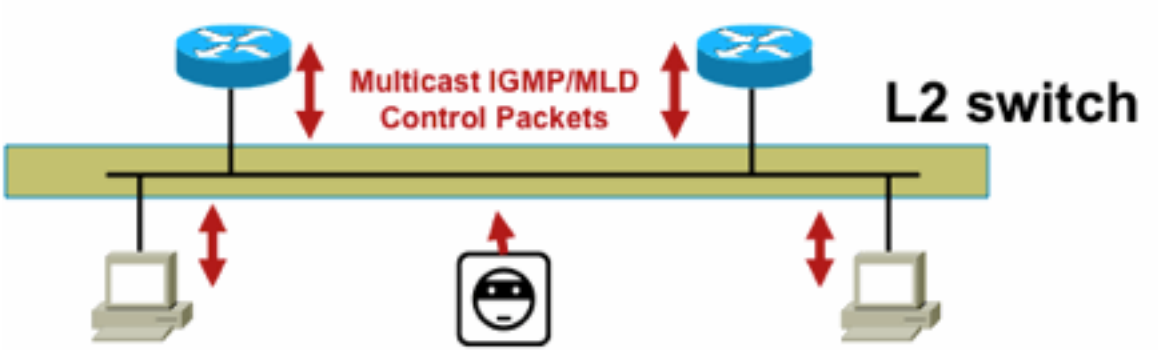

Fig18_Controlling_IGMP

Quando i pacchetti IGMP o MLD vengono filtrati, tenere presente quanto segue:

- IPv4: IGMP è un tipo di protocollo IPv4 (protocollo IPv4 2)
- IPv6: MLD è contenuto in pacchetti di tipo protocollo ICMPv6

Il processo IGMP è abilitato per impostazione predefinita non appena il multicast IP è abilitato. Anche i pacchetti IGMP sono dotati di questi protocolli, e quindi tutti questi protocolli sono abilitati quando è abilitato il multicast:

- PIMv1 - PIMv1 è stata la prima versione di PIM ed è sempre abilitata in Cisco IOS per la migrazione. Tutte le distribuzioni correnti utilizzano PIMv2.
- Mrinfo - Mrinfo è un comando Unix ereditato da Cisco IOS per visualizzare i router adiacenti multicast. Cisco consiglia di utilizzare il protocollo SNMP anziché il comando mrinfo.
- DVMRP - DVMRP è un protocollo vettoriale di distanza in modalità densa preesistente con caratteristiche di scalabilità molto limitate. Il supporto Cisco IOS per DVMRP è stato ritirato o è già obsoleto.
- Mtrace: Mtrace è l'equivalente multicast di "traceroute" unicast ed è uno strumento utile

Per ulteriori informazioni, vedere Numeri di tipo IGMP (Internet Group Management Protocol) di IANA

```
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
```

È possibile filtrare i pacchetti IGMP unicast (per IGMP/UDLR), in quanto si tratta molto probabilmente di pacchetti di attacco e di pacchetti di protocollo IGMP non validi. I pacchetti IGMP unicast sono supportati da Cisco IOS a supporto dei collegamenti unidirezionali e di altre condizioni di eccezione.

I pacchetti di query IGMP/MLD forgiati possono produrre una versione IGMP inferiore al previsto.

In particolare, gli host idealmente non inviano mai query IGMP perché una query inviata con una

versione IGMP inferiore può causare il ripristino della versione inferiore di tutti gli host che ricevono la query. In presenza di host IGMPv3 / SSM, questo può "attaccare" i flussi SSM. Nel caso di IGMPv2, ciò può determinare latenze di uscita più lunghe.

Se è presente una LAN non ridondante con un singolo query IGMP, il router deve eliminare le query IGMP ricevute.

Se esiste una LAN passiva ridondante/comune, è necessario uno switch in grado di eseguire lo snooping IGMP. In questo caso sono disponibili due caratteristiche specifiche:

- Protezione router
- IGMP versione minima, comando

Protezione router

Qualsiasi porta dello switch può diventare una porta del router multicast se lo switch riceve un pacchetto di controllo del router multicast (IGMP General Query, PIM Hello o CGMP Hello) su tale porta. Quando una porta dello switch diventa una porta del router multicast, tutto il traffico multicast viene inviato a tale porta. Per evitare questo problema, usare "Router Guard". La funzione Router Guard non richiede l'attivazione dello snooping IGMP.

La funzione Router Guard consente di designare una porta specificata come porta host multicast. La porta non può diventare una porta router, anche se vengono ricevuti pacchetti di controllo del router multicast.

Questi tipi di pacchetto vengono scartati se vengono ricevuti su una porta con Router Guard abilitato:

- Messaggi di query IGMP
- Messaggi IPv4 PIMv2
- messaggi IGMP PIM (PIMv1)
- Messaggi IGMP DVMRP
- Messaggi RGMP (Router-port Group Management Protocol)
- Messaggi CGMP (Cisco Group Management Protocol)

Quando i pacchetti vengono scartati, vengono aggiornate le statistiche che indicano che i pacchetti vengono scartati a causa di Router Guard.

Versione minima IGMP

Èpossibile configurare la versione minima di host IGMP consentita. Ad esempio, è possibile non consentire tutti gli host IGMPv1 o tutti gli host IGMPv1 e IGMPv2. Questo filtro si applica solo ai rapporti di appartenenza.

Se gli host sono collegati a una LAN "passiva" comune (ad esempio, uno switch che non supporta lo snooping IGMP o che non è configurato per esso), non vi è nulla che un router possa fare per queste query false se non ignorare i report di appartenenza alla "vecchia versione" che vengono quindi attivati e non eseguire il fallback stesso.

Poiché le query IGMP devono essere visibili per tutti gli host, non è possibile utilizzare un meccanismo di autenticazione dei messaggi basato su hash (HMAC) con una chiave già condivisa, ad esempio IPSec con chiave statica, per autenticare le query IGMP da "router validi". Se due o più router sono collegati a un segmento LAN comune, è necessaria la scelta di un query IGMP. In questo caso, l'unico filtro utilizzabile è un filtro del gruppo di accesso ip basato

sull'indirizzo IP di origine dell'altro router IGMP che invia le query.

I pacchetti IGMP multicast "normali" devono essere autorizzati.

Questo filtro può essere usato sulle porte del ricevitore per consentire solo pacchetti IGMP "buoni" e per filtrare quelli "sbagliati":

```
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
```

> **Nota:** Questo tipo di filtro IGMP può essere usato negli ACL di ricezione o nei CoPP. In entrambe le applicazioni, deve essere combinata con filtri per altro traffico gestito, come i protocolli del routing e del piano di gestione.

Figura 19: Controllo degli accessi lato ricevitore host

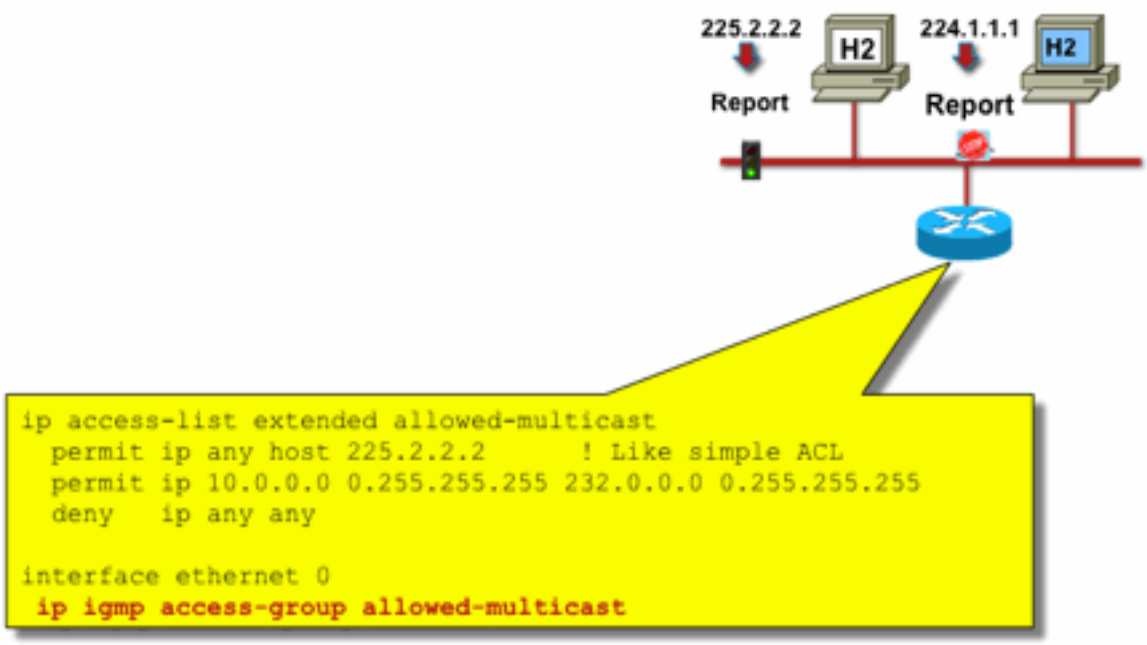

Fig19_Host_Receiver_Access

Per filtrare il traffico verso un ricevitore, non filtrare il traffico del piano dati, bensì il protocollo IGMP del piano di controllo. Poiché IGMP è un prerequisito necessario per ricevere il traffico multicast, non sono necessari filtri del piano dati.

In particolare, è possibile limitare i flussi multicast che i ricevitori possono unire (collegati all'interfaccia su cui è configurato il comando). In questo caso, usare il comando **ip igmp access-group / ipv6 mld access-group**:

```
ip igmp access-group / ipv6 mld access-group
```

Per i gruppi ASM, questo comando filtra solo in base all'indirizzo di destinazione. L'indirizzo IP di origine nell'ACL viene quindi ignorato. Per i gruppi SSM che utilizzano IGMPv3 / MLDv2, filtra l'indirizzo IP di origine e quello di destinazione.

Questo esempio filtra un determinato gruppo per tutti gli altoparlanti IGMP:

```
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
```

In questo esempio vengono filtrati gli altoparlanti IGMP specifici (e quindi i ricevitori multicast specifici) per un determinato gruppo:

```
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
```

> **Nota:** Per i gruppi ASM, l'origine viene ignorata.

Controllo ammissione

Il controllo dell'accesso fornisce una risposta binaria, sì o no per determinati flussi, indipendentemente dallo stato della rete. Il controllo dell'ingresso limita invece il numero di risorse che un mittente/destinatario può utilizzare, supponendo che abbia superato i meccanismi di controllo dell'accesso. Sono disponibili vari dispositivi per il controllo dell'ammissione in un ambiente multicast.

Limiti IGMP globali e per interfaccia

Sul router più vicino ai ricevitori multicast interessati, è possibile limitare il numero di gruppi IGMP uniti sia a livello globale che per interfaccia. È possibile utilizzare i comandi **ip igmp limit/ipv6 mld limit**:

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

Si consiglia di configurare sempre questo limite per interfaccia e anche a livello globale. In ogni caso, il limite si riferisce al numero di voci nella cache IGMP.

Nei due esempi seguenti viene illustrato come utilizzare questo comando per limitare il numero di gruppi ai margini di una rete a banda larga residenziale.

Esempio 1 - Limitare i gruppi ricevuti agli annunci SDR e a un solo canale ricevuto

La directory di sessione (SDR) funge da guida di canale per alcuni ricevitori multicast. Per ulteriori informazioni, vedere la RFC 2327.

Un requisito comune è quello di limitare i ricevitori a ricevere il gruppo SD più un canale. È possibile utilizzare la seguente configurazione di esempio:

```
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
```

L'elenco degli accessi in questo esempio specifica solo la guida dei canali; il comando **ip igmp limit** globale limita ciascuna origine IGMP a un singolo (1) canale, ma non include la guida dei canali, che può sempre essere ricevuta. Il comando interface sostituisce il comando globale e consente la ricezione di due (2) canali, oltre alla guida dei canali, su questa interfaccia.

Esempio 2 - Controllo ammissione su collegamento Aggregazione-DSLAM

Questo comando può essere utilizzato anche per fornire una forma di controllo dell'ammissione della larghezza di banda. Ad esempio, se fosse necessario distribuire 300 canali SDTV, ciascuno di 4 Mbps, e fosse presente un collegamento a 1 Gbps al DSLAM (Digital-Subscriber-Line-Access-Multiplexer), è possibile prendere una decisione di policy per limitare la larghezza di banda della TV a 500 Mbps e lasciare il resto per Internet e altri usi. In tal caso, è possibile limitare gli stati IGMP a 500 Mbps/4 Mbps = 125 stati IGMP.

Questa configurazione può essere utilizzata in questo caso:

Figura 20: uso dei limiti IGMP per interfaccia; Controllo dell'ingresso sul collegamento Agg-DSLAM

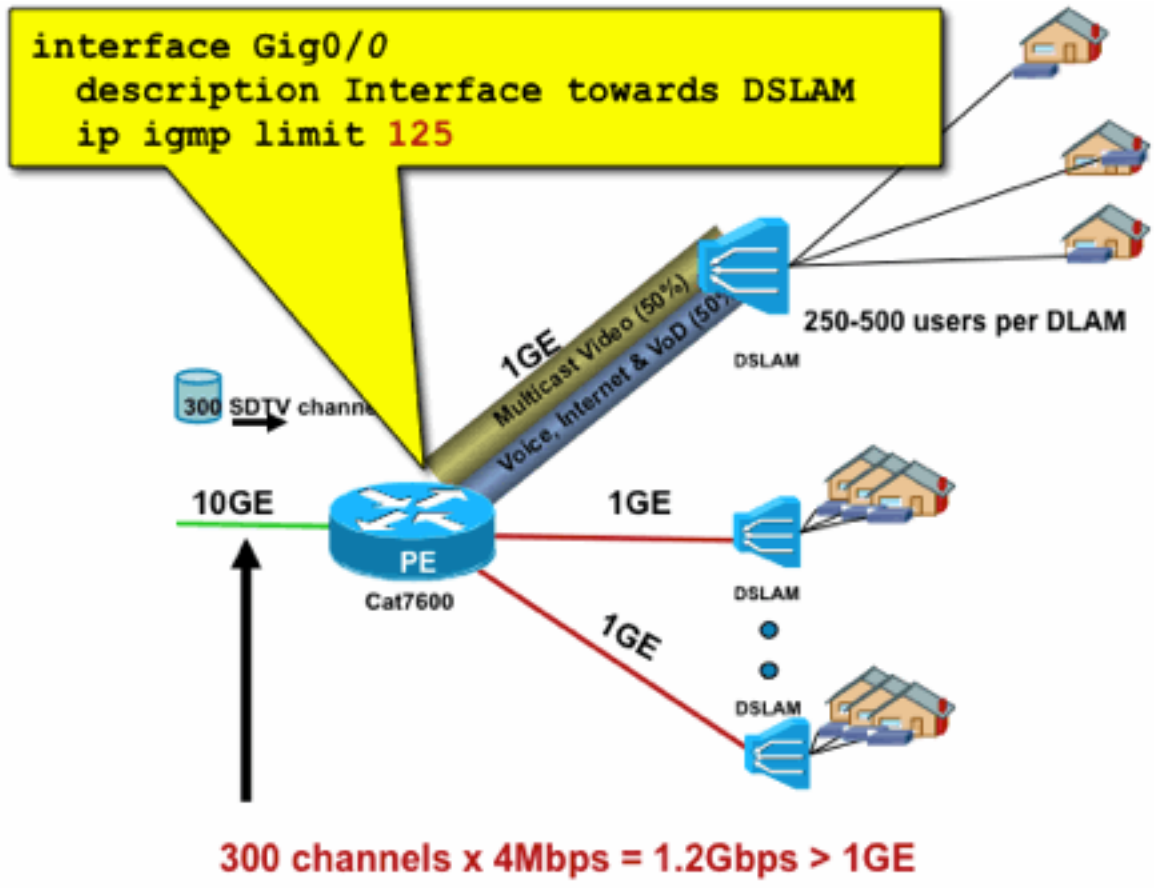

Fig20_PerInterface_IGMP

Limiti route per interfaccia

L'abilitazione dei limiti di stato per interfaccia è una forma più generica di controllo dell'ammissione. Non solo limita lo stato IGMP e PIM su un'interfaccia in uscita, ma fornisce anche un modo per limitare lo stato sulle interfacce in ingresso.

Utilizzare il comando **ip multicast limit**:

```
ip multicast limit [ rpf | out | connected ] <ext-acl> <max>
```

Lo stato può essere limitato separatamente sulle interfacce di input e output. Lo stato dell'origine collegato direttamente può essere limitato usando la parola chiave "connected" (connesso). Gli esempi illustrano l'utilizzo di questo comando:

Esempio 1 - Controllo dell'ingresso in uscita sul collegamento Agg-DSLAM

In questo esempio sono disponibili 300 canali TV SD. Si supponga che ogni canale SD necessiti di 4 Mbps, per un totale non superiore a 500 Mbps. Infine, si supponga che sia necessario supportare i pacchetti Basic, Extended e Premium. Esempio di allocazione della larghezza di banda:

- 60% / 300 Mbps - Base
- Estensione 20% / 100 Mbps
- Premium 20% / 100 Mbps

Quindi utilizzare 4 Mbps per canale, limitare l'uplink DSLAM a:

- Basic 75 stati
- 25 stati estesi
- 25 stati Premium

Configurare il limite sull'interfaccia in uscita rivolta al DSLAM dal PEAgg:

Figura 21: uso dei limiti di rotta per interfaccia; Controllo dell'ingresso sul collegamento Agg-DSLAM

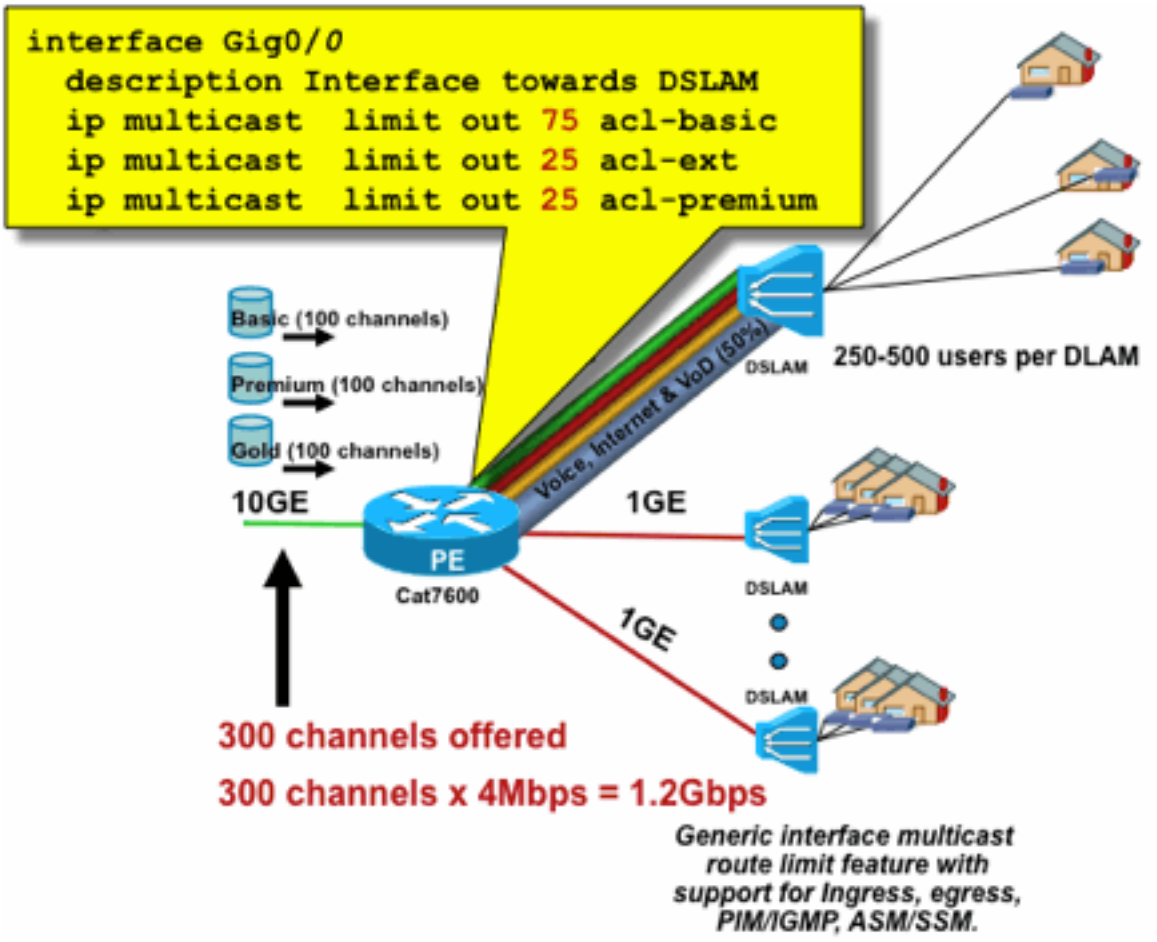

Fig21_PerInterface_Mroute

Esempio 2 - Controllo dell'ingresso sul collegamento Agg-DSLAM

Anziché il limite di "uscita" sull'interfaccia in uscita del dispositivo a monte, è possibile utilizzare i limiti RPF sull'interfaccia RPF del dispositivo a valle. Il risultato è identico a quello dell'esempio precedente e potrebbe essere utile se il dispositivo a valle non è un dispositivo Cisco IOS.

Figura 22: uso dei limiti di rotta per interfaccia; Controllo ingresso

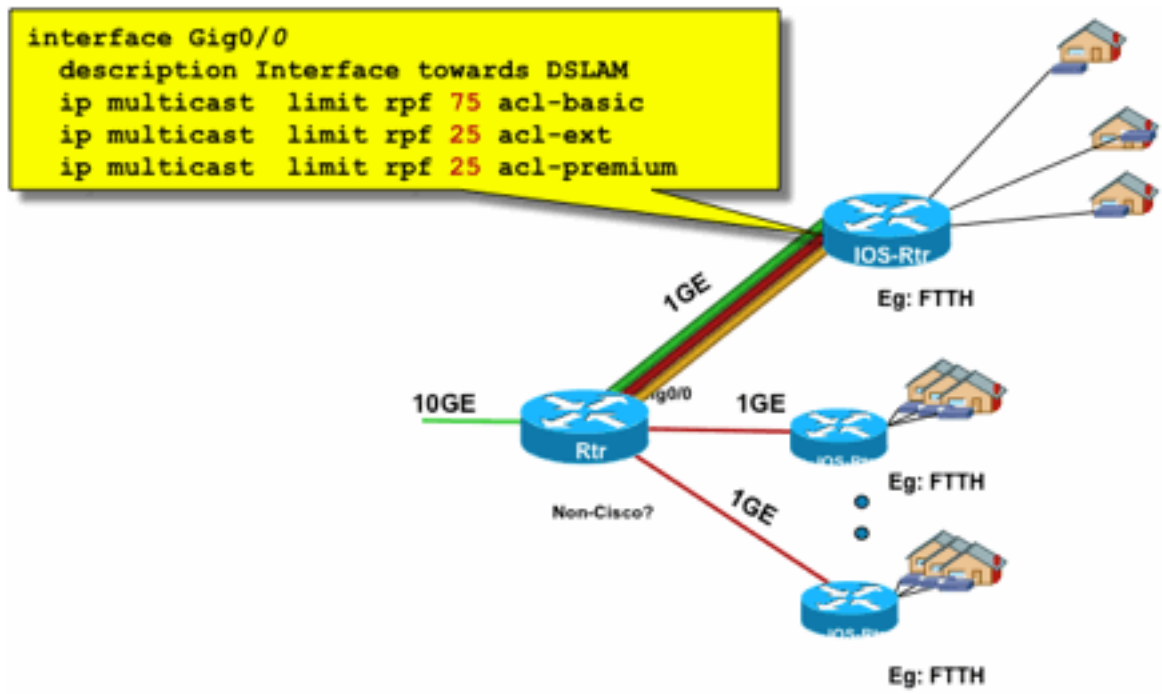

Fig22_PerInterface_Mroute_inputControl

Esempio 3 - Limiti basati sulla larghezza di banda

Èpossibile suddividere ulteriormente la larghezza di banda di accesso tra più provider di contenuti e offrire a ogni provider una quota equa della larghezza di banda sull'uplink al DSLAM. In tal caso, usare il **comando ip multicast limit cost**:

ip multicast limit cost <ext-acl> <multiplier>

Con questo comando è possibile attribuire un "costo" (usare il valore specificato in "moltiplicatore") a qualsiasi stato che corrisponda all'ACL esteso nel limite multicast ip.

Questo comando è globale ed è possibile configurare più costi simultanei.

In questo esempio, è necessario supportare tre diversi provider di contenuti con un accesso equo a ciascuno nella rete. Inoltre, nell'esempio riportato, è necessario supportare i flussi MPEG (Moving Picture Experts Group) di vari tipi:

MPEG2 SDTV: 4 Mbps
HDTV MPEG2: 18 Mbps
MPEG4 SDTV: 1,6 Mbps
HDTV MPEG4: 6 Mbps

In questo caso, è possibile allocare i costi della larghezza di banda a ciascun tipo di flusso e condividere il resto dei 750 Mbps tra i tre provider di contenuti con questa configurazione:

```
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
```

Figura 23: Fattore di costo per limiti di stato route per interfaccia

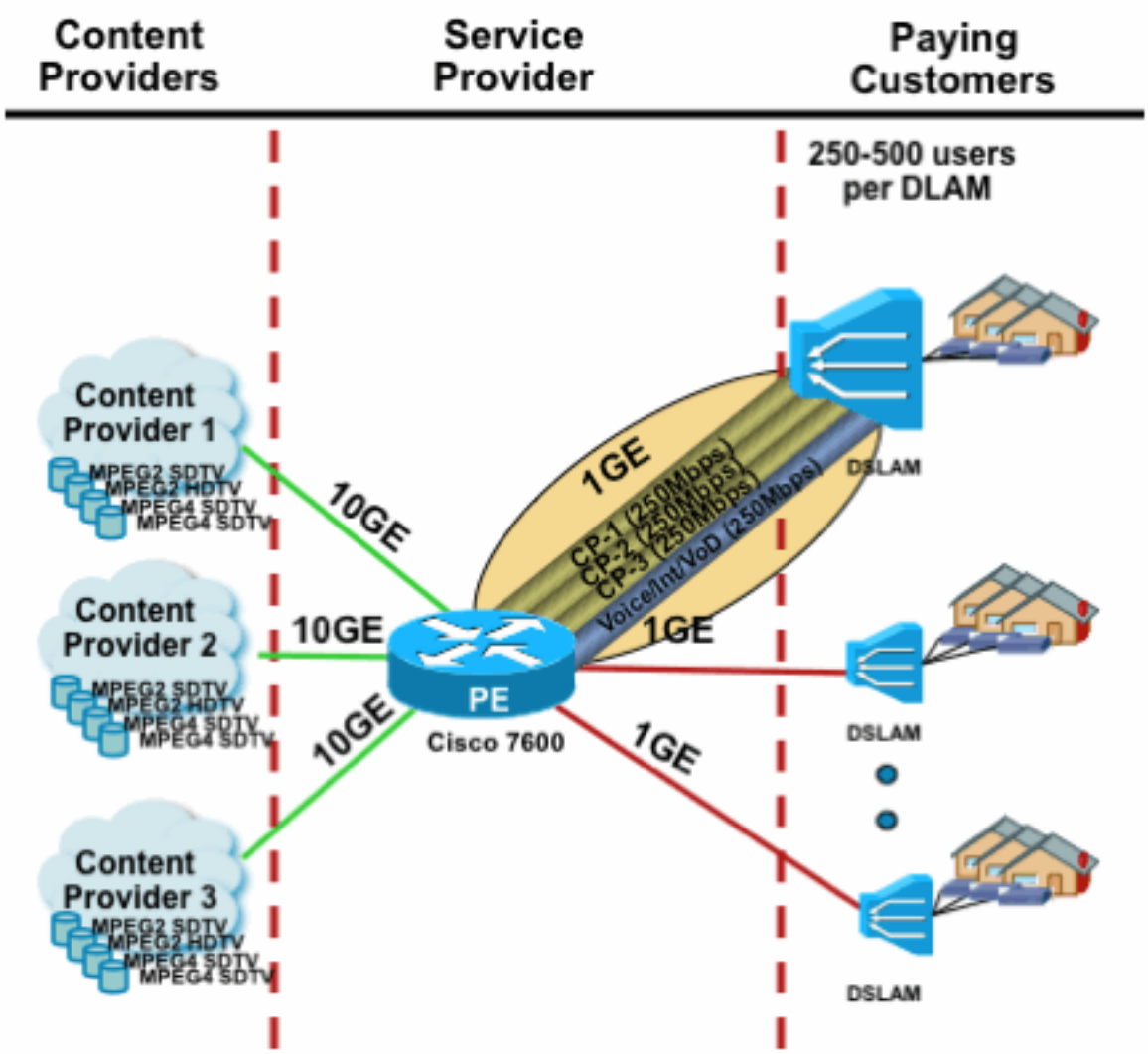

Fig23_Cost_P erInterface

Multicast e IPSec

Introduzione a GET VPN

Come nel caso del traffico unicast, anche il traffico multicast a volte deve essere protetto per garantire la riservatezza o l'integrità. Vi sono due aree principali in cui tali servizi potrebbero essere richiesti:

- Crittografia dei flussi multicast (ad esempio nelle applicazioni bancarie che inviano dati riservati a un ampio gruppo di ricevitori che utilizzano il multicast): si tratta di sicurezza del piano dati.
- Crittografia dei protocolli del control plane che utilizzano multicast, OSPF o PIM, ad esempio. Si tratta di control plane security.

IPSec come protocollo [RFC 6040, 7619, 4302, 4303, 5282] è specificamente limitato al traffico unicast (RFC). Lì viene stabilita una "associazione di sicurezza" (SA) tra due peer unicast. Per

applicare il protocollo IPSec al traffico multicast, è possibile incapsulare il traffico multicast all'interno di un tunnel GRE e quindi applicare il protocollo IPSec al tunnel GRE, che è unicast. Un approccio più recente utilizza una singola associazione di sicurezza stabilita tra tutti i membri del gruppo. Il Group Domain of Interpretation (GDOI) [RFC 6407] definisce come ottenere questo risultato.

Basata su GDOI, Cisco ha sviluppato una tecnologia chiamata Group Encryption Transport (GET) VPN. Questa tecnologia utilizza la modalità tunnel con conservazione degli indirizzi, come definita nel documento "draft-ietf-msec-ipsec-extensions". In GET VPN, viene innanzitutto stabilita un'associazione di sicurezza di gruppo tra tutti i membri del gruppo. Successivamente il traffico viene protetto, tramite ESP (encapsulated security payload) o AH (authentication header), che utilizza la modalità tunnel con la conservazione degli indirizzi.

In sintesi, GET VPN incapsula un pacchetto multicast che utilizza le informazioni sull'indirizzo dell'intestazione originale e quindi protegge il pacchetto interno in relazione ai criteri di gruppo, ad esempio con un ESP.

Il vantaggio di GET VPN è che il traffico multicast non è affatto influenzato dai meccanismi di incapsulamento della sicurezza. Gli indirizzi dell'intestazione IP instradata rimangono invariati rispetto all'intestazione IP originale. Il traffico multicast può essere protetto nello stesso modo con o senza GET VPN.

Il criterio applicato ai nodi GET VPN viene definito a livello centrale in un server chiavi di gruppo e distribuito a tutti i nodi del gruppo. Pertanto, tutti i nodi del gruppo dispongono dello stesso criterio e delle stesse impostazioni di protezione applicate al traffico del gruppo. Analogamente agli standard IPSec, i criteri di crittografia definiscono il tipo di traffico da proteggere. Ciò consente di utilizzare GET VPN per vari scopi.

Usa GET VPN per crittografare il traffico del piano dati multicast

Il criterio di crittografia a livello di rete viene impostato nel server delle chiavi di gruppo e distribuito agli endpoint GET VPN. Il criterio contiene il criterio IPSec (modalità IPSec - qui: modalità tunnel con mantenimento dell'intestazione) e algoritmi di sicurezza da utilizzare (ad esempio AES). Contiene anche una policy che descrive quale traffico può essere protetto, come definito da un ACL.

GET VPN può essere utilizzato per il traffico multicast e unicast. Un ACL potrebbe definire un criterio per proteggere il traffico unicast:

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

In questo modo viene crittografato tutto il traffico con un IP di origine da 10/8 e un IP di destinazione 10/8. Tutto il resto del traffico, ad esempio, il traffico tra 10/8 e un altro indirizzo, verrà ignorato da GET VPN.

L'applicazione di GET VPN per il traffico multicast è tecnicamente la stessa. Ad esempio, questa voce di controllo di accesso può essere utilizzata per proteggere il traffico da qualsiasi origine ai rispettivi gruppi multicast:

```
permit ip any 239.192.0.0 0.0.255.255
```

Questo criterio corrisponde a tutte le origini ("any") e a tutti i gruppi multicast che iniziano con 239.192. Il traffico verso altri gruppi multicast non è protetto.

> **Nota:** Molta attenzione deve essere prestata alla costruzione degli ACL crittografici. Il traffico di gestione o il traffico che ha origine all'esterno del dominio GET VPN ma termina all'interno (ossia il traffico che passa solo un endpoint crittografico), deve essere escluso dal criterio GDOI.

Gli errori più comuni includono:

- permettere ip qualsiasi 224.0.0.0 0.255.255.255: In questo modo viene crittografato anche il traffico OSPF e altro traffico del control plane, ad esempio destinato a un router peer.
- Il traffico di gestione non è escluso dai criteri di crittografia, che terminano all'interno della rete. Questo include il traffico GDOI stesso.

Usa GET VPN per autenticare il traffico del Control Plane

Èin genere consigliabile autenticare il traffico del control plane, ad esempio i protocolli di routing, per garantire che i messaggi provengano da un peer attendibile. Questa operazione è relativamente semplice per i protocolli del control plane che utilizzano unicast, ad esempio BGP. Tuttavia, molti protocolli del control plane utilizzano il traffico multicast. Gli esempi sono OSPF, RIP e PIM. Per l'elenco completo, vedere IANA's IPv4 Multicast Address Space Registry.

Alcuni di questi protocolli dispongono di un'autenticazione incorporata, ad esempio RIP (Routing Information Protocol) o EIGRP (Enhanced Interior Group Routing Protocol), altri si basano su IPSec per fornire questa autenticazione (ad esempio OSPFv3, PIM). In quest'ultimo caso, GET VPN fornisce un modo scalabile per proteggere questi protocolli. Nella maggior parte dei casi, il requisito è l'autenticazione tramite protocollo o, in altre parole, la verifica che un messaggio sia stato inviato da un peer attendibile. Tuttavia, GET VPN consente anche la crittografia di tali messaggi.

Per proteggere (in genere solo per l'autenticazione) il traffico del control plane, è necessario descrivere il traffico con un ACL e includerlo nella policy GET VPN. I dettagli variano a seconda del protocollo da proteggere, in cui è necessario decidere se l'ACL include il traffico che passa solo per un nodo GET VPN in entrata (incapsulato) o anche per un nodo in uscita.

Per proteggere i protocolli PIM, è possibile procedere in due modi:

- **allow ip any 24.0.0.13 0.0.0.0**: Questo è il gruppo multicast "Tutti i router PIM". Tuttavia, non protegge i messaggi PIM unicast
- **consentire pim any**: Ciò protegge il protocollo PIM, indipendentemente dal fatto che venga utilizzato multicast o unicast

> **Nota:** I comandi sono forniti come esempi per spiegare un concetto. Ad esempio, è necessario escludere alcuni protocolli PIM utilizzati per avviare PIM, come BSR o Auto-RP. Entrambi i metodi presentano alcuni vantaggi e inconvenienti che dipendono dall'implementazione. Per ulteriori informazioni, consultare la documentazione specifica su come proteggere PIM con GET VPN.

Conclusioni

Il multicast è un servizio sempre più comune nelle reti. L'emergere dei servizi IPTV nelle reti a banda larga domestiche/residenziali e il passaggio ad applicazioni di commercio elettronico in molti mercati finanziari mondiali sono solo due esempi di requisiti che fanno del multicast un requisito assoluto. Il multicast è accompagnato da una serie di problematiche diverse relative a configurazione, funzionamento e gestione. Una delle sfide principali è la sicurezza.

Questo documento esamina una varietà di modi in cui il multicast può essere protetto:

- Innanzitutto, è possibile esaminare i piani dati e di controllo multicast complessivi e spiegare in che modo le differenze rispetto a unicast presentano nuove sfide in termini di sicurezza.
- Successivamente, è stato esaminato in dettaglio un esame dei protocolli chiave rilevati in una rete multicast, in particolare IGMP, PIM e MSDP. In ogni caso, è stata fornita una descrizione delle minacce alla sicurezza e delle best practice consigliate per attenuarle.
- Inoltre, alcuni esempi specifici su come il multicast può essere protetto in alcune applicazioni specifiche, come le reti a banda larga, dove la larghezza di banda può essere limitata rispetto alla quantità di larghezza di banda richiesta da flussi video specifici.
- Infine, l'architettura GET VPN è stata descritta come un mezzo di multicast integrato con IPSec per la fornitura di VPN sicure.

Con in mente la sicurezza multicast, ricordate che è diverso da unicast. La trasmissione multicast si basa sulla creazione di uno stato dinamico, il multicast implica la replica dinamica dei pacchetti e crea alberi unidirezionali in risposta ai messaggi PIM JOIN / PRUNE. La sicurezza di questo intero ambiente implica la comprensione e l'implementazione di una ricca struttura di comandi Cisco IOS. Questi comandi sono principalmente incentrati sulla protezione delle operazioni di protocollo, degli stati (multicast) o dei policer posizionati su pacchetti come CoPP. Con l'uso corretto di questi comandi è possibile fornire un servizio protetto per il multicast IP.

In sintesi, questo documento promuove e descrive diversi approcci:

1. Uso diffuso di SSM: è la modalità PIM più semplice che consente anche l'uso dell'inoltro (S,G).
2. Se sono necessari servizi ASM, assicurarsi che sia possibile fornire un servizio affidabile: l'utilizzo di RP definiti staticamente offre un control plane più sicuro rispetto agli annunci RP dinamici. Auto-RP e BSR sono più flessibili
3. Se il PIM-SM è abilitato, esaminare le aree di particolare vulnerabilità, come il tunnel di registrazione all'RP, e assicurarsi che il DR sia sempre ben protetto. Il CoPP è molto utile in queste aree.
4. Se sono necessari servizi ASM tra domini, valutare se è possibile distribuire la funzionalità PIM Bidirezionale.
5. Usa limiti di stato route globale/igmp: consente di comprendere le funzionalità delle piattaforme insieme alla quantità massima di stato necessaria in circostanze normali e nello scenario peggiore. Configurare i limiti all'interno delle funzionalità della piattaforma che consentono alla rete di funzionare al massimo.
6. Filtri fondamentali: ACL/CoPP e ACL di infrastruttura, che bloccano il PIM al livello di accesso

IP Multicast è un mezzo entusiasmante e scalabile per offrire una varietà di servizi applicativi. Come per il formato unicast, anche questo formato deve essere protetto in una vasta gamma di aree. In questo documento vengono illustrati gli elementi di base che è possibile utilizzare per proteggere una rete multicast IP.

Informazioni correlate

- Linee guida per l'allocazione di indirizzi multicast IP aziendali
- Configura filtri IGMP IPv4
- Group Encrypted Transport VPN

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).