White Paper

Securing IP Multicast Services in Triple-Play and Mobile Networks

As the role of the service provider in enterprise IP networks expands to bring rich media to consumers and business users as part of wireline and mobile IP networks, the quality of experience is becoming as important to users as the speed and stability of upstream and downstream connections. Network video services are one of the newest applications to enjoy broad popularity, especially for subscribers of converged voice, data, and video (“triple play”) service packages and mobile services. For satisfactory quality of experience, the video data stream must be highly available and extremely secure. Cisco® IP Multicast, the established bandwidth-conservation technology, not only increases the efficiency of network resources and bandwidth but also is extremely secure, from endpoints to network cores, due to an array of protocols, techniques, and topologies.

This paper describes the various technologies that can be deployed in the control plane, data plane, access layer, and infrastructure and through admission control features to secure IP Multicast traffic for these highly demanding services.

SUMMARY

IP Multicast has its own distinct methods for the initiation and reception of video streams, including the creation of distribution trees. Therefore, securing multicast traffic effectively involves a mix of tactics and technologies. Multicast technology in Cisco IOS® Software allows a host to send packets to a subset of all hosts as a group transmission instead of having to send packets to every single user. It helps the network use less bandwidth, reduces redundancy, and allows for easily scalable and economical distributed broadcast video applications.

The five main areas where multicast must be secured are in the control plane, data plane, access control, admission control, and infrastructure. Multicast has been available through Cisco Systems® for more than a decade. With the proper technologies, products, topologies, and best practices, multicast traffic can be both highly available and dependably secure.

CHALLENGE

Converged networks face a variety of threats, with each converged service having its own unique vulnerabilities. For example, unsecured IP Multicast services have been vulnerable to Multicast Source Discovery Protocol (MSDP) storms caused by Internet worms. These worms infect a host, and the host then infects other hosts by checking for vulnerabilities through use of port scans.

Other security challenges facing IP triple-play and mobile networks deploying multicast services include securing devices through authentication, encrypting IP Multicast data in transit, and deploying keying mechanisms through tunneling techniques or through a native IP Multicast deployment that must scale to hundreds or thousands of network nodes.

SOLUTION

Just as the Cisco approach to network security spans network layers, devices, software, and the best practices of users, IP Multicast security involves a variety of approaches. Because attacks and other malicious network activity can occur at any point in a network video broadcast, protections must be carefully applied at every part of the broadcast process.

Control Plane Security

Cisco IOS Software contains routing protocols for multicast traffic that are the basis of control plane security. Both interdomain protocols such as MSDP and Source Specific Multicast (SSM) and intradomain protocols such as Protocol Independent Multicast (PIM) dense mode, PIM sparse mode, and bidirectional PIM can be used singly or in combination to protect multicast traffic.

PIM, PIM-SSM, and Internet Group Management Protocol v3

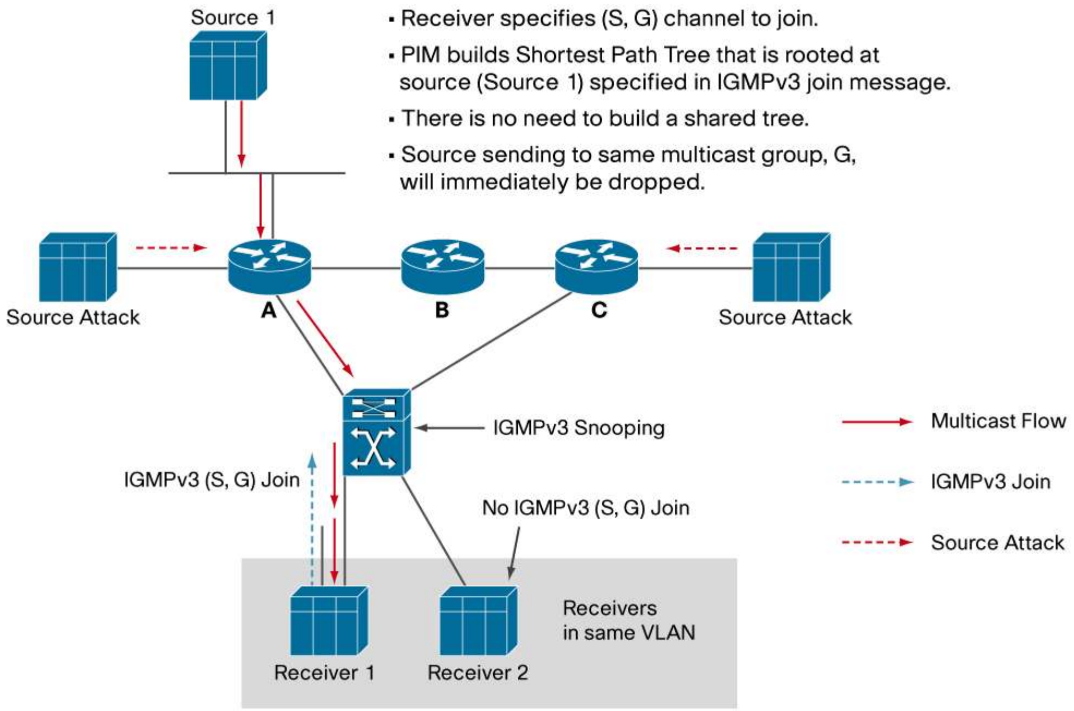
PIM was developed by Cisco as an intradomain routing protocol operating at Layer 3 to build multicast distribution trees across a network. PIM protocols such as PIM sparse mode rely on a rendezvous point to bring sources and receivers together, because receivers inherently are unaware of all the sources that are sending to a particular group. When a receiver joins a multicast group, it may receive multicast streams from multiple sources that are sending to that group. For few-to-many multicast applications, this behavior is expected and desirable. IP video, however, requires a different approach because a single source should be sending to a particular group. Allowing multiple sources to send to the same group would affect the primary stream that receivers are expecting from a particular source and ultimately lead to a poor quality of experience.

The solution to securely transport IP video across an IP backbone is to use the PIM-SSM protocol in the network and Internet Group Management Protocol version 3 (IGMPv3) on the hosts. As an extension of PIM sparse mode, PIM-SSM allows each source of a multicast broadcast to transmit its multicast traffic only to receivers that have explicitly requested that traffic from a particular source. This removes the need for a rendezvous point; it also means that distributed-denial-of-service (DDoS) attacks from unauthorized sources can be inhibited without the need to use filters, typically required in a traditional PIM sparse mode environment to block rogue sources.

When a host wants to join a multicast group, it issues an unsolicited IGMP “join” message to the network’s router. The router then uses a multicast routing protocol such as PIM-SSM to inform other routers of its readiness to receive packets destined for the multicast router. (The router may also use IGMP to periodically query the attached network segments for specific group members to elicit an IGMP “join” response.) As an enhancement to IGMP, IGMPv3 allows users to signal interest in a particular multicast group for a specific source and allows routers to use PIM-SSM in the backbone. In the absence of IGMPv3, interim solutions include SSM-mapping, IGMP v3lite, or URL Rendezvous Directory (URD).

Together with PIM-SSM and IGMPv3, IGMP snooping may be used on a switch to further constrain multicast to only those ports that have requested the stream, as shown in Figure 1.

Figure 1. SSM and IGMPv3 to Protect Against Source Attacks and IGMPv3 Snooping to Constrain Multicast Traffic Within a VLAN


Source 1
▪ Receiver specifies (S, G) channel to join.
▪ PIM builds Shortest Path Tree that is rooted at source (Source 1) specified in IGMPv3 join message.
▪ There is no need to build a shared tree.
▪ Source sending to same multicast group, G, will immediately be dropped.
Source Attack
A
B
C
Source Attack
IGMPv3 Snooping
IGMPv3 (S, G) Join
No IGMPv3 (S, G) Join
Receiver 1
Receiver 2
Receivers in same VLAN
Multicast Flow
IGMPv3 Join
Source Attack

PIM Neighbor Filtering, Rate Limiting, and Announcement Filters

PIM neighbor filters prevent unknown routers from participating in PIM forwarding. Otherwise, unknown routers might succeed in becoming designated routers responsible for sending PIM registers, building the multicast tree, or performing a shortest path tree switchover.

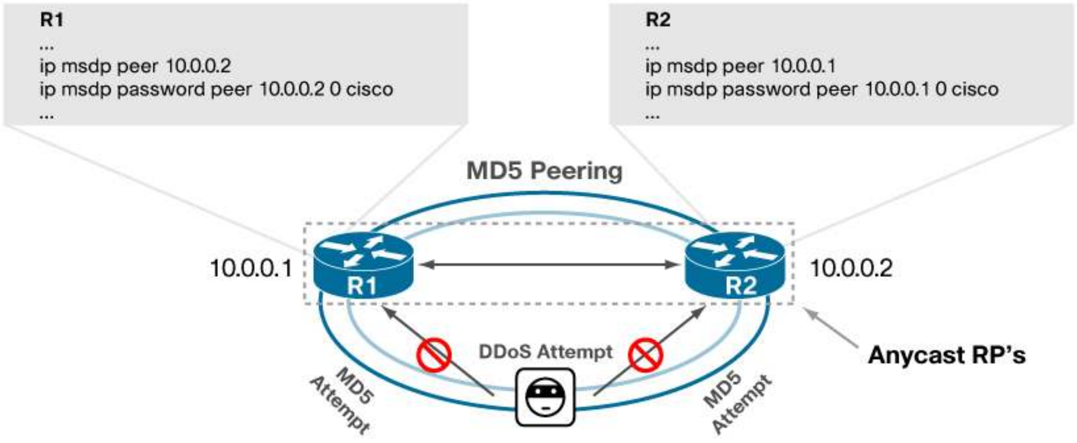
PIM register rate limiters limit the number of PIM register messages that designated routers are allowed to send for each group. Performed at the processor level, PIM register limiting helps protect CPU utilization on the designated router and route processor when there are many multicast transmissions that require PIM register processing at the same time.

PIM Rendezvous point (RP) announcement filters are applied to mapping agents when using Auto-RP, a feature that automatically distributes information to routers about what the RP address is for various multicast groups. These announcement filters are designed to acknowledge RPs that are permitted only by an access list defined by the network administrator. Rogue RPs attempting to hijack another RP are immediately dropped.

PIM Multicast Boundaries and Authentication Features

In addition to their ability to drop multicast data, PIM multicast boundaries provide a way to block PIM control messages from attaching a new branch to an existing tree off the router to which traffic was not intended to flow. Additionally, MSDP Message Digest Algorithm 5 (MD5) authentication can be used to secure multicast sessions between RPs that are used either for interdomain routing or as Anycast RPs. In Figure 2, MD5 authentication is enabled for a TCP connection between MSDP peer routers 1 and 2. An unknown MSDP connection attempt from a DDoS router is dropped.

Figure 2. MSDP MD5 Authentication Providing Security Against a DDoS Attempt



```
R1
...
ip msdp peer 10.0.0.2
ip msdp password peer 10.0.0.2 0 cisco
...
```

```
R2
...
ip msdp peer 10.0.0.1
ip msdp password peer 10.0.0.1 0 cisco
...
```

Data Plane Security

Multicast security in the data plane secures the contents of a multicast transmission, usually through an application that encrypts the data to ensure that only permitted users can access it. IP Security (IPsec) support may also be provided for multicast through the Group Domain of Interpretation (GDOI) protocol, which downloads IPsec keys and security associations to routers. GDOI replaces manually shared keys, mitigating their security weaknesses.

The GDOI protocol requires each group member to contact a key server. Once a group member has been authenticated and authorized by the key server, it is given keys and security associations for the group. The group member may also be given enough policy information for it to authenticate and decrypt (or “rekey”) messages sent from the key server in a special IP Multicast group. These rekey messages allow the group member to receive updated keys and security associations and to receive updates to group membership.

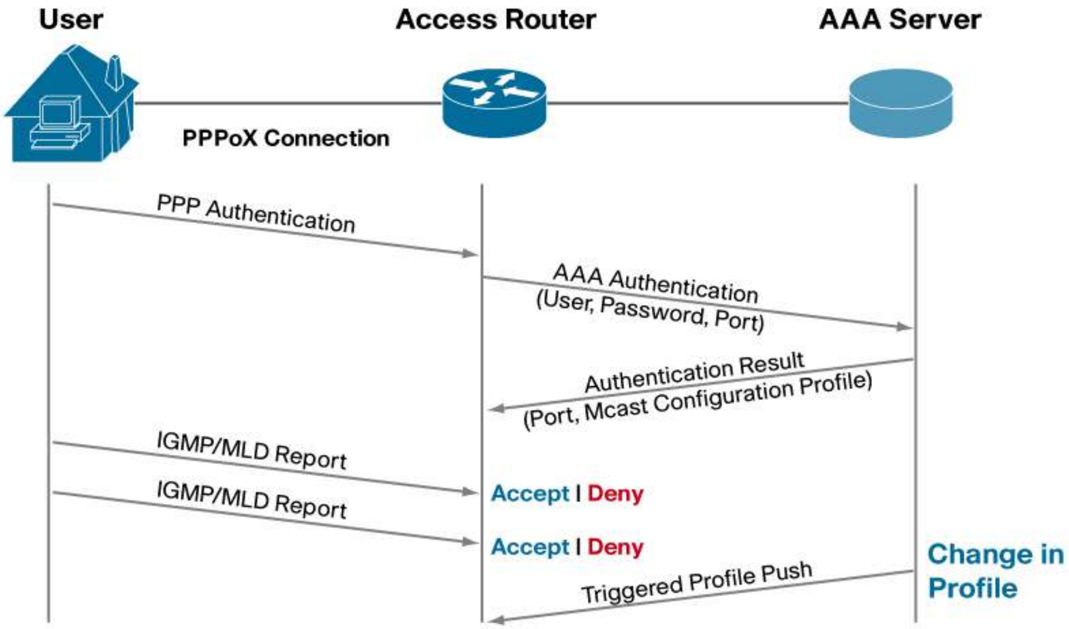
Access Control

Controlling the ability of a device to send and access multicast data is another important facet of multicast security. Interface-specific filters can be applied at the edges of the network to filter access lists for ingress multicast traffic. IGMP filters can also be used to restrict which hosts can join specific multicast groups. A dynamic method of pushing IGMP filters down to routers using the authentication, authorization, and accounting (AAA) service model is called multicast authentication and profile support. It uses existing AAA features in Cisco IOS Software to provide a centralized authentication and accounting framework for multicast users in large groups. With this feature, a content provider could deliver customized channel access directly through a customer’s IP-enabled home television set. Access control of the multicast content requires user authentication and the ability to provision a channel profile per user. The solution must be scalable to accommodate large deployments of 100,000 to 250,000 users.

The Cisco multicast authentication and profile support feature is an evolving solution. The first phase is a static model of preprovisioned IGMP and Multicast Listener Discovery (MLD) protocol access profiles on the access router. Future phases are planned to include this static model plus an on-demand model where AAA requests are sent to an AAA server with an IGMP/MLD join. Future phases are also planned to provide a combined model of static and on-demand capabilities for different group ranges.

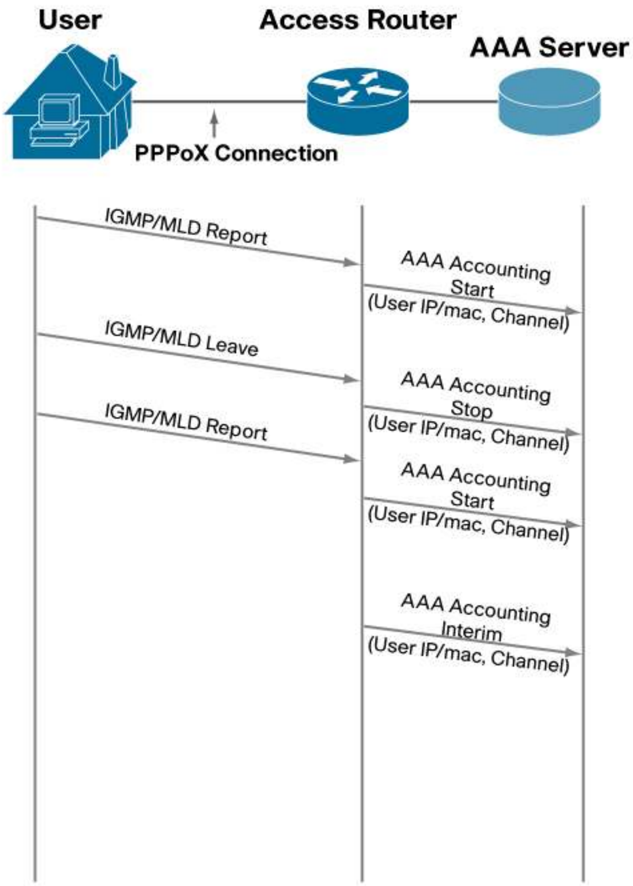
In Figure 3, the user initiates a Point-to-Point Protocol (PPP) session with a local router, which then forwards an AAA authentication request to the AAA server. The server replies with an AAA profile per user port. When the access router receives IGMP/MLD join reports from the host, the access router either accepts or denies the multicast group request. If there are any changes to a user profile, the AAA server pushes the new profile to the access server.

Figure 3. IP Multicast Authentication and Profile Support Using the AAA Service Model



The AAA service model is standards-based and widely accepted. It provides an excellent way of controlling and keeping track of multicast sources and receivers, a process that until recently was tedious and complex. The AAA server also performs receiver-based accounting for monitoring and billing on a per-viewer, per-content basis. The user device can be automatically configured to send a report using IGMP/MLD, as shown in Figure 4.

Figure 4. Multicast AAA Support for Receiver-Based Accounting


User
Access Router
AAA Server
PPPoX Connection
IGMP/MLD Report
AAA Accounting Start (User IP/mac, Channel)
IGMP/MLD Leave
AAA Accounting Stop (User IP/mac, Channel)
IGMP/MLD Report
AAA Accounting Start (User IP/mac, Channel)
AAA Accounting Interim (User IP/mac, Channel)

In this process, the access router sends the AAA server an accounting START record. The user sends an IGMP/MLD “leave” message. The access router sends the AAA accounting server a STOP record. Optionally, the access router may also send interim accounting records to poll user activity. Based on these START/STOP records, network operators can determine the time and byte count information per session for billing and behavioral analysis.

Admission Control

As the popularity of network video applications grows among consumers, admission control functions—which govern transmission and reception of multicast traffic based on available network resources—are vital. Without admission control some users may receive degraded multicast streams, rendering programs unwatchable, and others may receive a “Network Busy” message or nothing at all as network resources are overtaxed. Network admission control is important in maintaining a high quality of experience for digital video consumers. For a more detailed look at Cisco integrated solutions for admission control for broadcast and video on demand, see the white paper “Integrated Video Admission Control for Video-on-Demand and IPTV in IP Next-Generation Networks”.

Admission control features for multicast traffic include the following:

- *IGMP limits* restrict the number of groups users may try to join, either globally or per-interface, on a router.
- *Multicast Route (mroute)* limits set the total number of mroutes allowed on a router. Once the configured limit is reached, no additional mroute entries may be created.

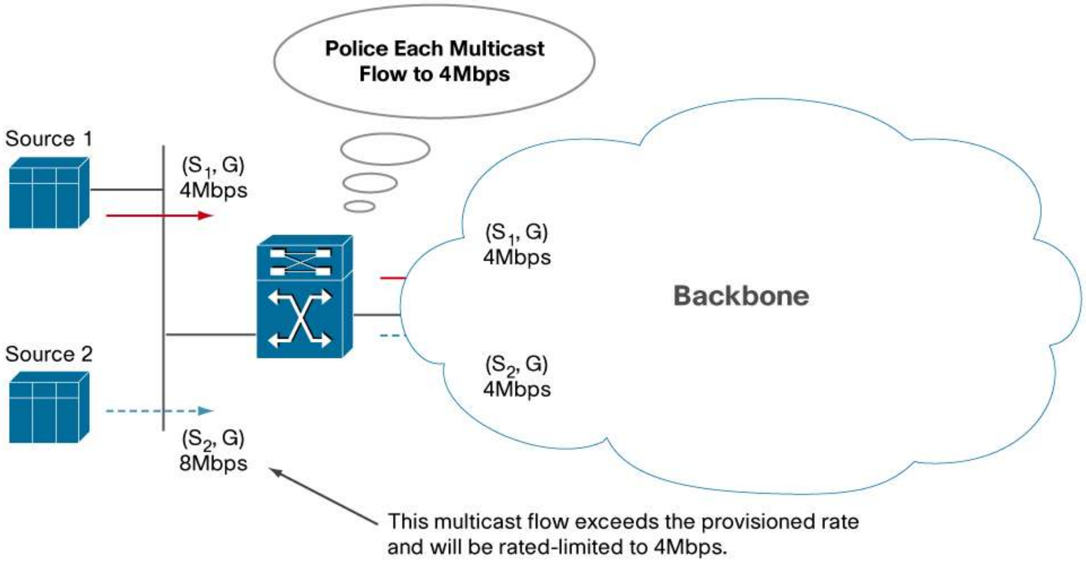
- *Distance Vector Multicast Routing Protocol (DVMRP) route limits* set an upper limit on the total number of DVMRP routes permitted on a router.
- *MSDP source active (SA) limits impose limits* on the total number of MSDP SA messages that can be cached on a router.
- *Multicast group range limits* define a range of multicast groups for which a router is allowed to create Mroute states. Multicast groups not within the specified range cannot be created by the router.

These admission control features may be invoked by service providers and enterprise network administrators based on different criteria, including the service package an end user has purchased or the privileges an enterprise user is entitled to.

Policing Multicast Traffic

Networks delivering IP video broadcasts must ensure that no single source can monopolize all the network's resources. Without proper enforcement, valid multicast flows can easily get overridden by a faulty sender. User-based rate limiting, shown in Figure 5, provides the means to rate limit multicast traffic on a per-flow basis rather than an aggregate basis.

Figure 5. User-Based Rate Limiting in the Cisco Catalyst® 6500 Series Switch


Police Each Multicast Flow to 4Mbps
Source 1
(S1, G) 4Mbps
Source 2
(S2, G) 8Mbps
(S1, G) 4Mbps
(S2, G) 4Mbps
Backbone
This multicast flow exceeds the provisioned rate and will be rated-limited to 4Mbps.

Infrastructure Security

Networks that are configured to use rendezvous points are exposed to PIM dense mode flooding when all possible rendezvous points are lost. PIM dense mode actively attempts to send multicast data to all potential receivers and relies on the receivers "self-pruning," or removing themselves from a multicast group, to achieve a desired distribution. PIM sparse mode relies on an explicit joining method before attempting to send multicast data to receivers in a multicast group. Under PIM dense mode, multicast traffic periodically is flooded throughout the network and forwarded across links where there may not be any interested receivers, wasting bandwidth and potentially overtaxing network resources. Several techniques can be used to secure a network from PIM dense mode flooding:

- Rendezvous point of last resort is a technique used to keep multicast groups in sparse mode when all rendezvous points are lost through dynamic mechanisms such as Auto-Rendezvous Point (Auto-RP) or Bootstrap Routing (BSR). It relies on the use of the static rendezvous point statement and is applied on every router in the network. The static rendezvous point statement points at a local loopback interface that is always up. This results in a rendezvous point that is always available and provides a last resort when all rendezvous points are lost. Note that the rendezvous point of last resort has local significance only. Multicast may still be forwarded between interfaces on the same router but never traverses beyond that router.

- The Auto-RP Listener feature only allows the Auto-RP to use PIM dense mode in a PIM sparse mode environment. Since all interfaces are configured with sparse mode, when all rendezvous points are lost, multicast traffic that falls back to dense mode is not forwarded across those interfaces.
- The Avoid Dense Mode Fallback feature prevents sparse mode multicast groups from ever falling back to dense mode and makes the rendezvous point of last resort technique obsolete.

Multicast and Modular Quality of Service Command-Line Interface

Packets can be classified in a variety of different ways, from input interface to Network-Based Application Recognition (NBAR) for difficult-to-classify applications to arbitrary access control lists. Classification is the first component of the Modular Quality of Service (QoS) Command-Line Interface (MQC), the simple, scalable, and powerful QoS framework in Cisco IOS Software. The MQC allows for the clear separation of the policy applied on the classes of service and the application of a QoS policy on an interface or subinterface. Creating policies through access control lists or MQC enables unwanted IP Multicast traffic destined for the network core to be blocked on all ingress ports of the control plane. Control-plane policing using MQC utilizes modular QoS attributes, providing filtering and rate limiting for control-plane packets, matching criteria for many attributes, multiple match criteria within a class map, and consistency across platforms.

Firewall Support

The Cisco PIX® Firewall 7.0 includes PIM sparse mode routing support. This adds highly secure integration in distributed videoconferencing and collaborative computing environments. There is no need to tunnel multicast and PIM control traffic through the firewall as the Cisco PIX Firewall 7.0 functions as a PIM router, providing stateful control of all multicast traffic crossing it. The Cisco PIX Firewall also supports IGMP Proxy Agent, IGMPv2, IGMP access group, IGMP limits, bidirectional PIM, designated router priority, accept register filter, and multicast source network address translation (NAT).

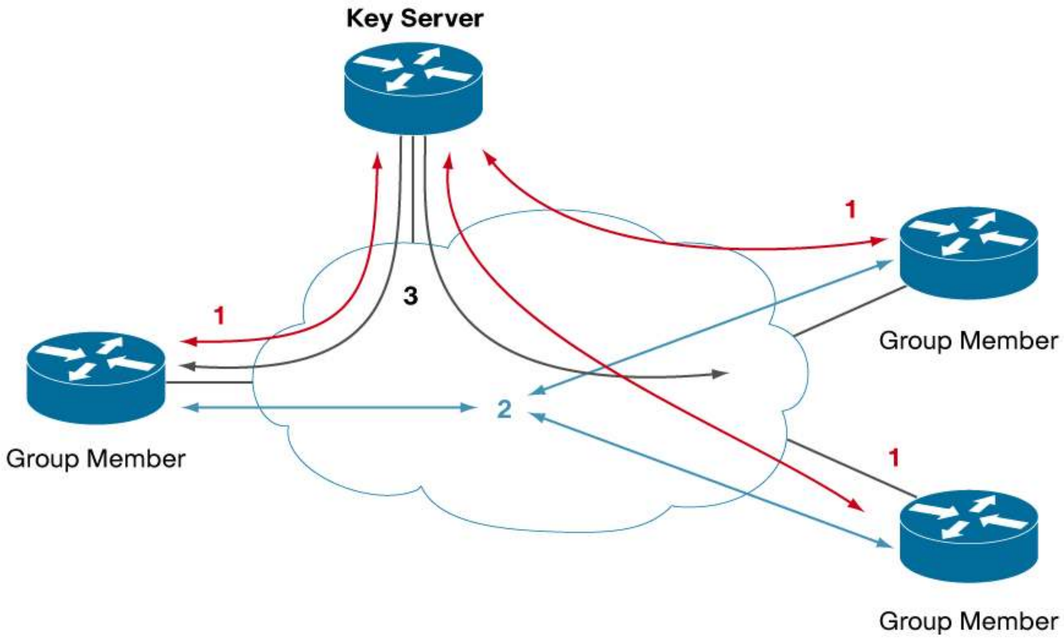
Cisco IOS Firewall also operates with full PIM functionality.

Secure Multicast Using GDOI

The Cisco IOS Software feature Secure Multicast is another security feature for IP Multicast, specifically for enterprise networks with native (nontunneled) multicast traffic. It provides a more efficient way to apply encryption to multicast packets. Encrypting native IP Multicast packets allows PIM to route the packets even though the content is encrypted. Additionally, native multicast encapsulation avoids the packet replication that occurs when packets are encapsulated using unicast tunnels. Networks that are IP Multicast enabled can transport encrypted multicast traffic natively over an IP core. With Secure Multicast, the traffic is protected with encryption in case packets are erroneously delivered. Secure Multicast relies on the GDOI protocol to distribute the policies and keys for the group in the control plan, and it relies on IPsec to protect the data plane.

In a group management model, the GDOI protocol operates between a group member and a group controller key server, which establishes security associations among authorized group members. There are three phases of negotiation, shown in Figure 6.

Figure 6. GDOI Protocol Flows for Group Membership



In phase 1 in Figure 6, multicast group members register with the key server. The key server authenticates and authorizes the group members and downloads the IPsec policy and keys that are necessary for them to encrypt and decrypt IP Multicast packets. In phase 2, group members exchange IP Multicast packets that are encrypted using IPsec. In phase 3, as needed, the key server pushes a rekey message to the group members. The rekey message contains a new IPsec policy and keys to use when the old IPsec security associations expire. Rekey messages are sent in advance of the SA expiration to ensure that valid group keys are always available.

Cisco Secure Multicast enables customers to extend the reach of their IP Multicast services to all corporate multicast Web sites and applications with enhanced security. The Secure Multicast feature is delivered across multiple platforms, has been tested with many applications, and has been enhanced by extensive user experience. The unique integration between GDOI and IPsec provides a level of trust on the corporate internal network that is on par with the existing cryptographic techniques and is a distinctive feature of Cisco offerings.

CONCLUSION

Integrated multicast security features from Cisco for IP networks protect the quality of experience of broadcast video against threats to the integrity of the data and its degradation at every step from content source to receiver. Technologies available in Cisco Software and devices secure traffic and devices in the control plane, data plane, access layer, and infrastructure, and they administer admission control policies for small, medium, and large networks.

Together with Linksys, a division of Cisco Systems, Inc. and Scientific Atlanta, a Cisco company, Cisco is pioneering home networking and particularly the video broadcast and video on demand (VoD) business, adding to Cisco experience in video for enterprise networks. Through technologies like multicast and its many associated security features, Cisco understands the requirements necessary to provide secure, carrier-class broadcast video services and is continually enhancing multicast protections to anticipate and guard against present and future threats.

FOR MORE INFORMATION

Multicast Security
http://www.cisco.com/en/US/products/ps6593/products_ios_protocol_group_home.html

Multicast Solution Architecture
http://www.cisco.com/en/US/products/ps6598/products_ios_protocol_group_home.html

Secure Multicast
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_white_paper0900aecd8047191e.shtml

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C11-372127-00 10/06