White Paper

Cisco IOS Secure Multicast

Cisco IOS® Secure Multicast is the first native IP Multicast encryption that does not rely on a tunnel-based architecture, lowering administrative overhead and helping ensure optimum WAN flexibility.

SUMMARY

Cisco IOS Secure Multicast is a set of hardware and software features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS device. It combines the keying protocol Group Domain of Interpretation (GDOI) with hardware-based IP Security (IPsec) encryption to provide users an efficient method to secure IP Multicast group traffic. With Cisco IOS Secure Multicast, a router can apply encryption to IP Multicast traffic without having to configure tunnels.

Cisco IOS Secure Multicast provides the following benefits:

- **Multicast traffic protection**—It provides the ability to protect multicast traffic without any form of additional encapsulation.
- **Scalability**—It allows for one-to-many and many-to-many relationships.
- **Manageability**—It allows for easier configuration and enhanced manageability.
- **Native IPsec encapsulation**—It provides native IPsec encapsulation for IP Multicast traffic.
- **Key and policies distribution**—It offers a centralized key and policies distribution mechanism through the GDOI key server.
- **Simplified troubleshooting**—It simplifies troubleshooting by lowering overall complexity.
- **Extensible standards-based framework**—It uses an extensible, standards-based framework.

CHALLENGE

Any organization trying to deploy IP Multicast securely faces various challenges, including authenticating network devices, encrypting IP Multicast traffic in transit without the use of tunnels (point to point and point to multipoint), and deploying a keying mechanism that can scale to hundreds or thousands of network nodes without increasing administrative overhead.

Deploying encryption of IP Multicast traffic with IPsec requires tunneling of IP broadcast and IP Multicast packets. Although this is a perfectly fine and a preferable method, in some cases—remote-access security solutions provide a tunnel between a remote system and a corporate gateway—it is not very efficient. A critical challenge for any solution in environments such as distribution of enterprise audio, video, and other media is efficiency.

Another challenge in protecting “native” multicast packets requires taking advantage of and interoperating with the existing multicast infrastructure. Native multicast implements several protocols for distributing the group information, and the IPsec mechanism to distribute cryptographic keys in larger WAN deployments must work in concert with those protocols.

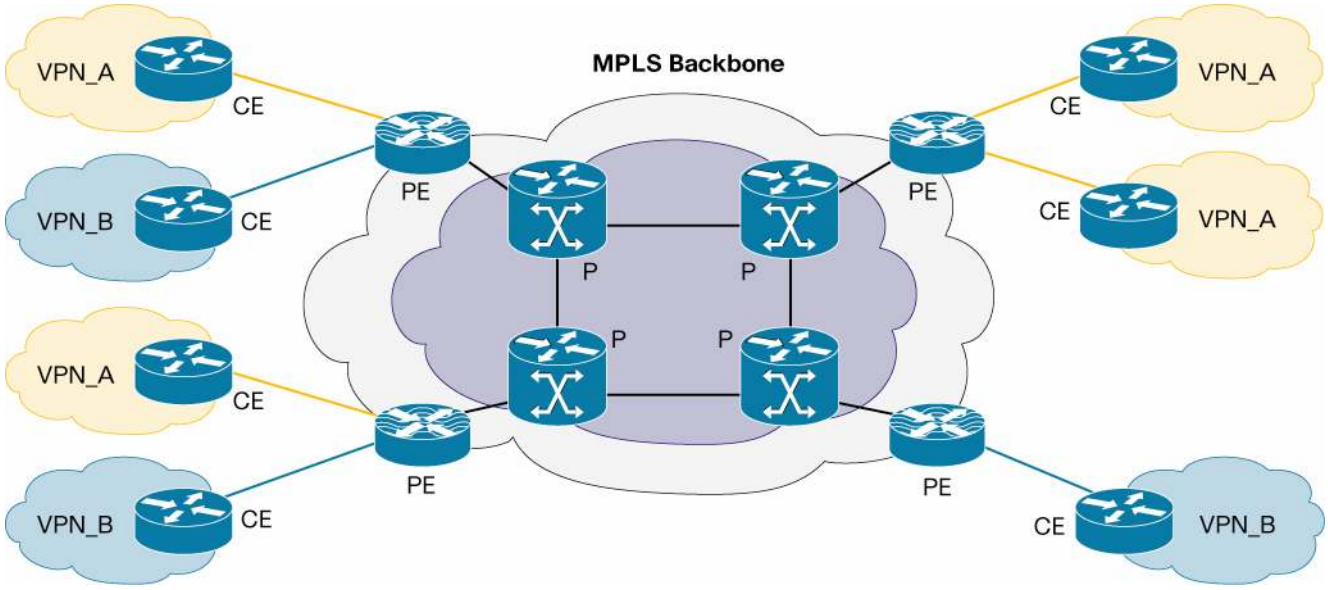
Finally, Cisco® experience with IPsec suggest that ongoing management of this infrastructure in the real enterprise is another critical challenge. Cryptographic keys have to be passed onto the authenticated hosts, and mechanisms must be put in place for eliminating rogue elements in these authenticated groups.

SOLUTION

In certain network scenarios, other than IPsec remote-access networks, it is more efficient to apply encryption to non-tunneled (that is, “native”) IP Multicast packets. Encrypting IP Multicast packets natively allows IP Multicast routing (for example, Protocol Independent Multicast [PIM]) to route the packets regardless of the fact the content is encrypted. A native IP Multicast encapsulation also avoids the needless packet replication that occurs when encapsulating IP Multicast packets using unicast tunnels.

IP Multicast-enabled networks can transport encrypted multicast traffic natively over an IP core. An IP Multicast encryption-enabled router can forward IP Multicast packets to the core network, which is careful to distribute the multicast packets only to other customer edge devices that belong to the same customer. However, with secure multicast, the IP Multicast traffic is protected with encryption in case packets are erroneously delivered (Figure 1).

Figure 1. MPLS Backbone



Cisco IOS Secure Multicast relies on the GDOI protocol (RFC 3547) to distribute the policy and keys for the group (control plane) and relies on IPsec (RFC 2401) to protect the data plane.

IP SECURITY

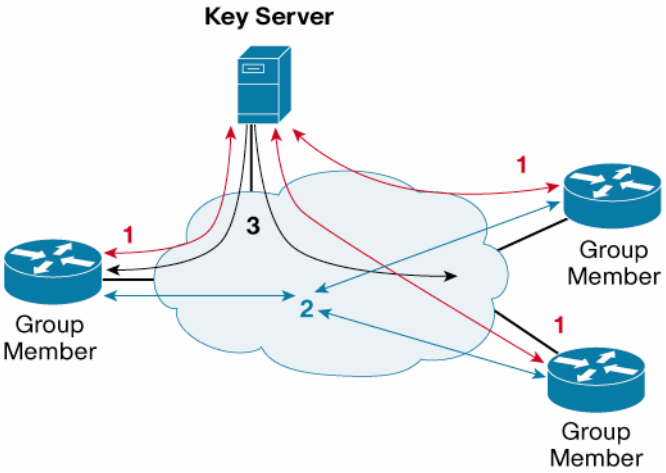
IPsec is a well-known protocol that defines an architecture to provide various security services for traffic at the IP layer. The components and how they fit together with each other and into the IP environment are described in the IETF RFC 2401. A variety of IP Multicast applications benefit from the encryption of native IP Multicast packets.

Scalable Keying Mechanism and Network Device Authentication

Group Domain of Interpretation

GDOI is defined as the ISAKMP Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a group controller or key server (GCKS), which establishes security associations among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association. The Phase 2 exchange is defined in IETF RFC 3547. The topology shown in Figure 2 and the corresponding text explain how this protocol works.

Figure 2. Protocol Flows That Are Necessary for Group Members to Participate in a Group

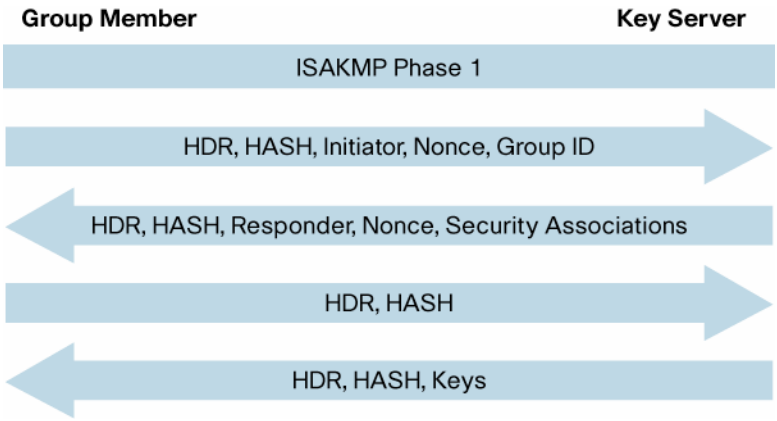


The topology in Figure 2 shows the protocol flows that are necessary for group members to participate in a group:

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

The GDOI protocol is protected by an ISAKMP Phase 1 exchange. The GDOI key server and the GDOI group member must have the same ISAKMP policy. This Phase 1 ISAKMP policy should be strong enough to protect the GDOI protocol that follows. The GDOI protocol is a four-message exchange that follows the Phase 1 ISAKMP policy. The phase 1 ISAKMP exchange can be main mode or aggressive mode.

Figure 3. Shows the ISAKMP Phase 1 Exchange



The messages (the ISAKMP Phase 1 messages and the four GDOI protocol messages) are referred to as the GDOI registration, and the entire exchange shown in Figure 3 is a unicast exchange between the group member and the key server. During the registration, the group member receives the address of the multicast group and registers with the group to receive the multicast rekeys. After the registration is successful, the key server sends a multicast rekey to all the registered group members in a group.

Note: The GDOI protocol uses User Datagram Protocol (UDP) port 848 (with Network Address Translation-Traversal (NAT-T); it floats to 4848).

Key Server

The responsibilities of the key server include maintaining the policy and creating and maintaining the keys for the group. Typically, the policies specific to a group are defined in the key server. When a group member registers, it downloads these policies and the keys to the group member. The key server also regularly rekeys the group before existing keys expire.

The key server has two modes: servicing registration requests and sending rekeys. A group member can register at any time and receive the most current policy and keys. When a group member registers with the key server, the key server verifies the group ID that the group member is attempting to join. If this ID is a valid group ID, the key server sends the security association policy to the group member. After the group member acknowledges that it can handle the downloaded policy, the key server downloads the respective keys.

The key server can download two types of keys: the key encryption key (KEK) and the traffic encryption key (TEK). The TEK becomes the IPsec security association with which the group members within the same group communicate. The KEK encrypts the rekey message.

The GDOI server sends out rekey messages when there is an impending IPSec security association expiration or when the policy has changed on the key server (using the command-line interface [CLI]). The rekey messages may also be retransmitted periodically to account for possible packet loss, which can occur because rekey messages are sent without the use of any reliable transport. There is no efficient feedback mechanism by which receivers can indicate that they did not receive a rekey message, so retransmission seeks to bring all receivers up-to-date.

Group Member

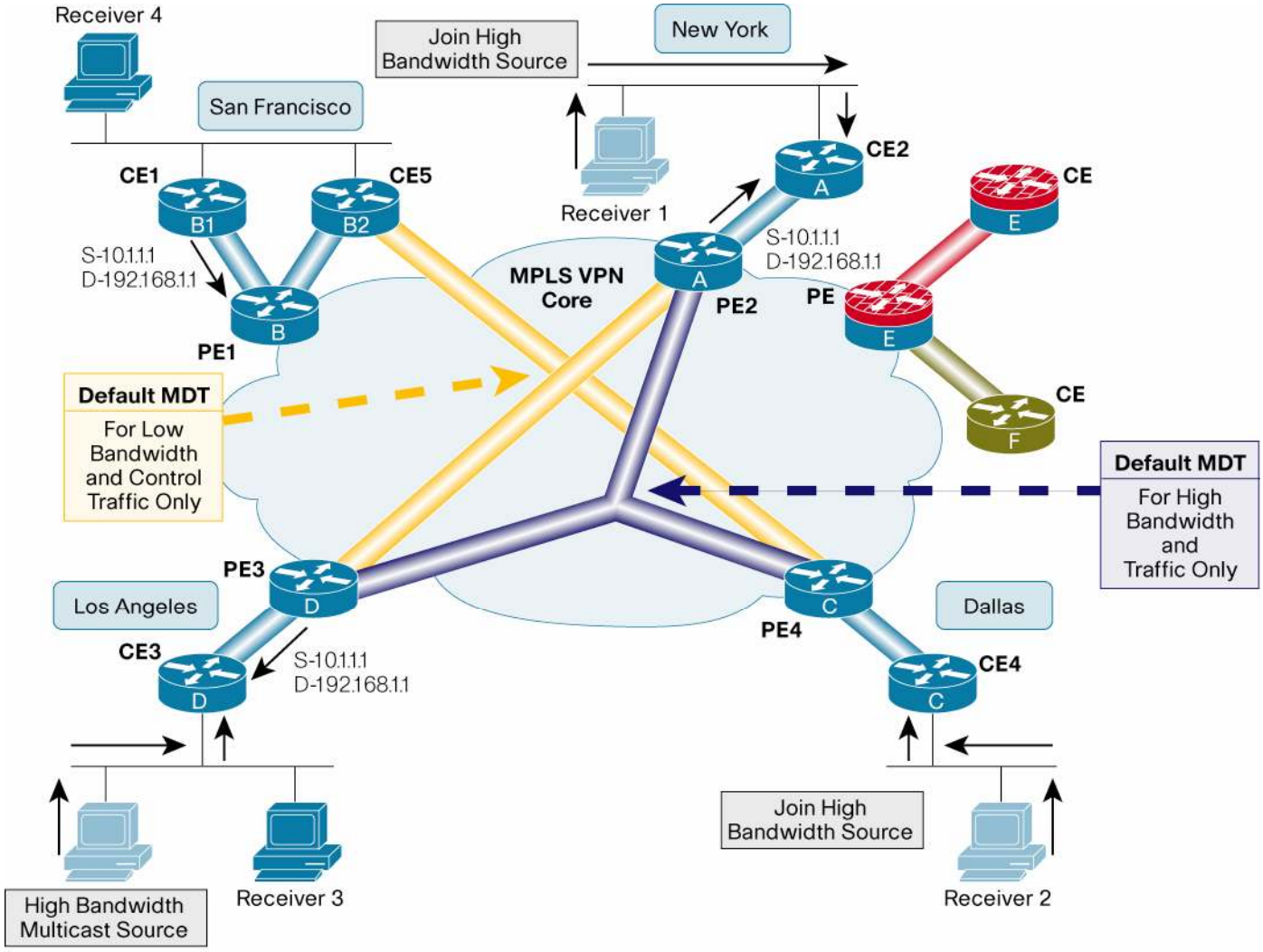
The group member registers with the key server to get the IPsec security association(s) needed to communicate with the group. The group member provides the group ID to the key server to get the respective policy and keys for this group. These keys are refreshed periodically, and before the current IPsec security associations expire, so that there is no loss of traffic.

Cisco IOS Secure Multicast can be used with all modes of multicast. The PIM-sparse mode should be used with the retransmit CLI option because the multicast shared tree can be torn down if there is no traffic on the shared tree.

Deployment Example: Multicast VPN over an MPLS Network

Figure 4 shows an example of multicast VPN packets that are being sent over a Multiprotocol Label Switching (MPLS) network.

Figure 4. Multicast VPN over an MPLS Network



- Customer CE devices joins the MPLS Core through provider's PE devices.
- The MPLS Core forms a Default MDT for a given customer.
- A High Bandwidth source for that customer starts sending traffic.
- Interested receivers 1 and 2 join that High Bandwidth source.
- Data-MDT is formed for this High Bandwidth source.

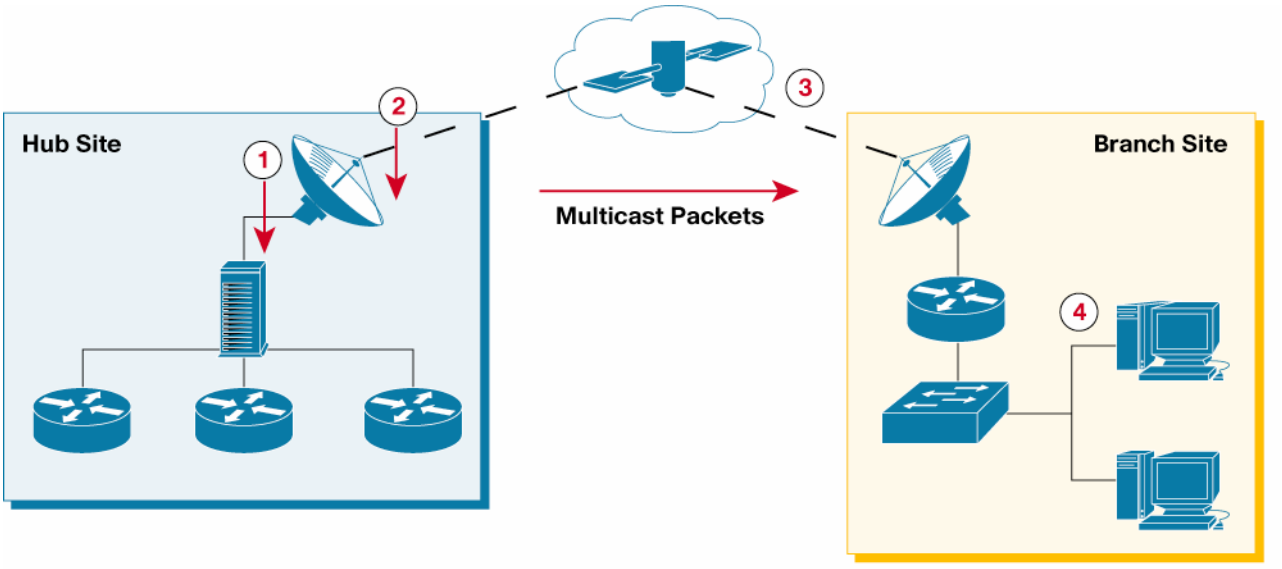
Secure Multicast is used to protect the multicast data.

In Figure 4, a customer within an MPLS network has four customer edge (CE) devices attached to the MPLS network. One multicast sender (IP address 10.1.1.1) is sending packets on the IP Multicast address 192.168.1.1. These packets are encrypted by CE1 before distribution into the provider edge (PE) network. Router PE1 creates a VPN packet, which is forwarded to P1. The multicast VPN packet code on P1 forwards the packet toward both CE2 and CE3 because systems behind those routers have joined the 192.168.1.1 group and are "listening" for those packets. Devices CE2 and CE3 decrypt the IP Multicast packets and further distribute them in the network.

IP Multicast over Satellite

Figure 5 shows an example of encrypted IP packets that are being sent over satellite links.

Figure 5. IP Multicast over Satellite



1. The hub site encrypts IP Multicast packets and forward them to the satellite-sending unit.
2. The satellite-sending unit transmits the IP packets to the satellite.
3. The router in the branch site decrypts multicast packets and forwards the packet to the receivers in the branch.

In Figure 5, a router in a hub has encrypted IP Multicast packets and forwarded them to the satellite sending unit. The satellite sending unit transmits the IP packets to the satellite, where the satellite retransmits the IP packet toward the dish antennas located at branch sites. At each branch, a router decrypts the IP Multicast packets and forwards them into the branch network.

CONCLUSION

With Cisco IOS Secure Multicast, users can enjoy the benefits of encryption of “native IP multicast” traffic within their larger enterprise environment. Cisco IOS Secure Multicast helps customers extend their reach to all of their corporate IP multicast applications, while providing enhanced security. Having been tested with many applications and delivered across multiple platforms, Cisco IOS Secure Multicast enhances user experience and efficiently secures multicast applications. The unique integration between GDOI and IPsec provides a level of trust on the corporate internal network that is similar to the existing cryptographic techniques. This ability to provide a unique model differentiates Cisco Systems® from its competitors.

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 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 the USA C11-341514-00 03/06