Secure Multicast
Agenda

• Why IP Multicast?
• IP Multicast Security Challenges
• Secure IP Multicast Solution and Benefits
• Technical Details
• Platform Support and Useful Links
Why IP Multicast?
Unicast vs. Multicast

Unicast software distribution

Multiply times number of Unicast endpoints

Expected behavior for Unicast-based applications

Take advantage of Multicast-based applications that provide same service
Unicast vs. Multicast

Multicast software distribution

Multicast MoH

One-to-few streams sent to group(s) of receivers

Video/Streaming media

Convert Unicast applications to Multicast, if supported

Multicast-enabled infrastructure allows for new technologies

Less BW consumed to provide same service
Less CPU utilization on source devices
Less overall impact on network devices replicating and forwarding traffic
Why IP Multicast over VPN?

- Efficiently deploy and scale distributed group applications across a VPN
- Reduce network load associated with sending the same data to multiple receivers
- Alleviates high host/router processing requirements for serving individual connections across VPN tunnels
- To IP Multicast, VPN is just another WAN type
IP Multicast Security Challenges
Secure Multicast : Business Problem

Securely and efficiently protect Multicast network data traffic from multimedia, video, voice, on an IP network

Benefits:
• Help in complying with mandates for encryption
• Increase productivity & save cost

Applications

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Enterprise</th>
<th>Small/Medium Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Native IPv4 / IPv6 Internet secured Multicast</td>
<td>• Stock trading, corporate communications, e-learning, hoot-and-holler over IP, videoconferencing, content delivery, conferencing</td>
<td>• e-learning</td>
</tr>
<tr>
<td>• Secured Multicast VPN</td>
<td></td>
<td>• IP surveillance</td>
</tr>
<tr>
<td>• Triple-play &amp; video broadcast</td>
<td></td>
<td>• Content delivery</td>
</tr>
</tbody>
</table>

© 2005 Cisco Systems, Inc. All rights reserved.
## Cisco IOS Secure Multicast

**Overcoming Existing IP Multicast Security Challenges**

<table>
<thead>
<tr>
<th>Tunnel Based</th>
<th>Secure Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bolted on</td>
<td>Built in</td>
</tr>
<tr>
<td>Complex architecture</td>
<td>Seamless integration</td>
</tr>
<tr>
<td>Wasted capital</td>
<td>Investment protection</td>
</tr>
<tr>
<td>Rigid design</td>
<td>Flexible design</td>
</tr>
<tr>
<td>Simple transport</td>
<td>Intelligent transport</td>
</tr>
</tbody>
</table>

*Fueled by demand for agility within a security framework*
Secure IP Multicast Solution and Benefits
What is Secure Multicast

Features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS® device

- A new security framework
  Architecture and components necessary in order for Cisco IOS Software to provide scalable security to IP Multicast group traffic

- A new key management paradigm
  An ISAMKP domain of interpretation (DOI) for group key management called the “group domain of interpretation" (GDOI)

- A way to provide scalable security to native IP Multicast packets
  Scalable security (e.g. encryption and authentication) to native IP Multicast packets
  Native Multicast encryption avoids the needless packet replication that occurs when encapsulating IP Multicast packets using Unicast tunnels
## Benefits of Cisco IOS Secure Multicast in VPN Deployments

<table>
<thead>
<tr>
<th>Previous Limitation</th>
<th>Feature and Associated Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast traffic encryption was supported through IPsec tunnels:</td>
<td>• Group mode encryption with group SA:</td>
</tr>
<tr>
<td>• Not scalable</td>
<td>No need for 2 IPSec + 1 IKE SA <em>per spoke</em></td>
</tr>
<tr>
<td>• Difficult to troubleshoot</td>
<td>Allows much higher scalability, simplifies troubleshooting</td>
</tr>
<tr>
<td>• Limited QoS support</td>
<td>• Group controller/key server:</td>
</tr>
<tr>
<td></td>
<td>Key and policies distributed using centralized mechanism</td>
</tr>
<tr>
<td></td>
<td>• Extensible standards-based framework:</td>
</tr>
<tr>
<td></td>
<td>Supports Multicast today and extends to support Unicast in future</td>
</tr>
<tr>
<td>No optimal security for native multicast in mVPN type architectures</td>
<td><strong>Native Multicast encryption</strong></td>
</tr>
<tr>
<td></td>
<td>• Supports Multicast encryption in mVPN architectures</td>
</tr>
<tr>
<td></td>
<td>• Day-one transparent interoperability between various core Cisco IOS® technologies; e.g. native multicast encryption</td>
</tr>
<tr>
<td>Overlay VPN network</td>
<td><strong>Leverage core for Multicast replication</strong></td>
</tr>
<tr>
<td>Overlay routing resulting in suboptimal convergence</td>
<td>• Investment protection: New architecture leverages the core and investment costs spent on building core</td>
</tr>
</tbody>
</table>

Multicast traffic encryption was supported through IPsec tunnels:
- Not scalable
- Difficult to troubleshoot
- Limited QoS support

No optimal security for native multicast in mVPN type architectures

Overlay VPN network
- Overlay routing resulting in suboptimal convergence
Secure Multicast Application: mVPN

Before

• Scalability – an issue (N^2 problem)
• Highly inefficient

After: Secure Multicast

• Multicast data traffic protected by IPSec
• Multicast key distribution solved by GDOI
• Allows MPLS VPN customers to access Multicast content
• Standards based
Large-Scale IPSec WAN Aggregation

**Deployment Models**

Comparison of Deployment Models

<table>
<thead>
<tr>
<th></th>
<th>Dynamic Routing</th>
<th>Meshing</th>
<th>HA</th>
<th>QoS</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec only</td>
<td>No</td>
<td>No</td>
<td>Stateful failover</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>IPSec and GRE</td>
<td>Yes</td>
<td>No</td>
<td>RP</td>
<td>Yes*</td>
<td>Yes (hub replicated)</td>
</tr>
<tr>
<td>DMVPN (Hub-Spoke)</td>
<td>Yes</td>
<td>No</td>
<td>RP</td>
<td>Yes*</td>
<td>Yes (hub replicated)</td>
</tr>
<tr>
<td>DMVPN (Spoke-Spoke)</td>
<td>Yes</td>
<td>Dynamic full mesh</td>
<td>RP</td>
<td>Yes*</td>
<td>Yes (hub-spoke)</td>
</tr>
<tr>
<td>IPSec VTI/Easy VPN</td>
<td>No</td>
<td>No</td>
<td>Stateful failover</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>Secure Multicast</td>
<td>Yes</td>
<td>Yes</td>
<td>RP</td>
<td>Yes*</td>
<td>Scalable</td>
</tr>
</tbody>
</table>

*Note: See specific topologies for limitations*
Secure IP Multicast Detailed Presentation Continued: Technical Details
What’s a Group?

• Three or more parties who send and receive the same data transmitted over a network
• Transmission can be Multicast, or Unicast (identical data sent to multiple parties)
• Parties can be routers, PCs, telephones, any IP device
• There are many different examples of group topologies
Multicast Group Models: Example

**Multicast Models: Single-source Multicast**
- Multicast sender
- Receiver 1
- Receiver 2
- Receiver 3
- Example: IP/TV multicast presentation

**Multicast Models: Multiple-source Multicast**
- IP Multicast Group Member 1
- IP Multicast Group Member 2
- IP Multicast Group Member 3
- IP Multicast Group Member 4
- IP Multicast Group Member 5
- Example: multicast video conference

**Multicast Models: Multipoint control unit**
- MCU server
- Conference Participant 1
- Conference Participant 2
- Conference Participant 3
- Example: Video conference MCU

**Multicast Models: Publish-Subscribe unicast**
- Content engine
- Receiver 1
- Receiver 2
- Receiver 3
- Example: Video-on-demand service
Secure Groups

To secure a group you need:

• Data Encryption Protocol
  – IPSec
  – SRTP

• Key Management Protocol
  – Provides keys for data encryption
IPSec Key Management

- Pair-wise key management
  - IKE
  - KINK
  - Manual IPSec keys
- Group key management
  - Manual IPSec keys
  - GDOI (Group domain of interpretation for ISAKMP)

GDOI enables native Multicast encryption
Relationship of GDOI to IKE:
GDOI Coexists with IKE

• IKE Phase 1 is used to provide confidentiality, integrity, and replay protection
  IKE Phase 1 is UNCHANGED

• A newly defined Phase 2 exchange (called GDOI registration) is run rather than IKE Phase 2.
  IKE Phase 2 is UNUSED and UNCHANGED.

• A new DOI number is used to differentiate GDOI exchanges from IKE Phase 2
  At the end of IKE Phase 1 a state machine looks at the DOI number to determine next exchange

• A GDOI service must listen on a port other than port 500 (IKE)
# Quick Comparison of IKEv1, IKEv2 vs. GDOI

<table>
<thead>
<tr>
<th>Feature</th>
<th>IKEv1</th>
<th>IKEv2</th>
<th>GDOI</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC documents</td>
<td>2407/2408/ 2409</td>
<td>RFC 4306</td>
<td>RFC 3547</td>
</tr>
<tr>
<td>UDP port</td>
<td>500, 4500</td>
<td>500, <strong>4500</strong></td>
<td>848</td>
</tr>
<tr>
<td>Phases</td>
<td>2, Ph. 1 (6/3 messages), Ph. 2 (3 messages)</td>
<td>2, Ph. 1 (4 messages), Ph. 2 (2 messages)</td>
<td>2, Ph. 1 (6/3 messages), Ph. 2 (4 messages)</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Signature, PSK, PKI</td>
<td>Signature, PSK, PKI</td>
<td>Signature, PSK, PKI</td>
</tr>
<tr>
<td>SA negotiation</td>
<td>Responder selects initiator’s proposal</td>
<td>Same as IKEV1, proposal structure simplified</td>
<td>Not negotiated, GDOI is used to push keys and policies</td>
</tr>
<tr>
<td>Identity hiding</td>
<td>Yes in MM, No in AM</td>
<td>Yes</td>
<td>Yes in MM, No in AM</td>
</tr>
<tr>
<td>Keep-alives</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Anti-DoS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UDP/NAT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Reliability</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PFS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP/CP</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
RFC 3547—GDOI (Group Domain of Interpretation)


- An ISAKMP DOI for group key management
- RFC 3547—Cisco® championed the effort
- GDOI specification presents an ISAMKP DOI for group key management to support secure group communications
- GDOI describes a protocol for a group of systems ("group members") to download keys and security policy from a key server
- GDOI manages group security associations, which are used by IPSec and potentially other data security protocols running at the IP or application layers
Secure Multicast: Implementation of Group Domain of Interpretation (GDOI)

- Key distribution mechanism (RFC3547)
  - IETF Multicast Security (msec) WG
- Group member security protections
  - IKE Phase 1 provides member authentication, confidentiality, and integrity
  - GDOI registration provides authorization and replay protection
- Distribute keys and policy for groups
  - Security associations
  - Secret keys, public keys
- Efficiently adjust group membership
- Intended for use with small or large groups.
  - The desire to support large groups drives the design.

* GSA = Group Security Association

© 2003 Cisco Systems, Inc. All rights reserved.
GDOI Group Key management

- In a group key management model, GDOI is the protocol run between a group member and a "group controller/key server" (GCKS).
- The GDOI protocol establishes security associations among authorized group members.
- A group member registers with the key server to obtain keys.
- The GDOI registration defines two phases of negotiation.
- Phase I is protected via IKE Phase I.
- The key server rekeys the group (pushes new keys) when needed. Rekey messages can be IP multicast packets for efficiency.
- Public signature keys and preshared keys, the only methods of IKE authentication.
GDOI Exchanges

• GDOI defines a registration exchange for initial group key mgmt
  
    Follows the IKE Phase 1

• GDOI defines a rekey exchange for subsequent key updates
  
    Can be multicast for efficiency
Registration Protocol

**Initiator**
- Member requests to join group in ID payload

**Responder**
- Key Server returns policy in SA payload
- Member agrees to policy
- Key Server returns keys in KD payload

HDR*, HASH (1)
Each router registers with the key server. The key server authenticates the router, performs an authorization check, and downloads the encryption policy and keys to the router.
Rekey Protocol

- The “cookie pair” in the ISAKMP HDR acts as a SPI which identifies the group
- SEQ contains a counter used for replay protection
- SA and KD are same format as during registration
- SIG contains a digital signature of the packet
GDOI Rekey

- The key server generates and pushes new IPSec keys and policy to the routers when necessary
- Rekey messages can also cause group members to be ejected from the group
Multicast / Unicast Key Distribution

- Multicast key distribution over multicast-enabled network
  
  Via multicast-formatted key message and network replication
  
  Fallback to group member GDOI Unicast registration

 KEK = 235687404
 Protect: 10.0.0.0/8 to 10.0.0.0/8
 Group Member = 192.168.3.4
 Group Member = 192.168.3.2
 Group Member = 192.168.3.3
GDOI Example: VoIP Audio Conference

- VoIP phones behind IPSec- or SRTP-capable routers
- An audio conference is reached by dialing a special phone number
- Router recognizes that the phone number is associated with a conference

Note: A theoretical example is illustrated in following slides, but we don’t actually have any such teleconference technology for IP phones.
Configuration Setup

GDOI key server

GDOI client 1

GDOI client 2

GDOI client 3

GDOI client 4

Policy for x1234:
IP addr=239.1.1.2,
SPI=0x12049a92,
IPSEC policy: 3DES/SHA,
3DES key=<three keys>,
SHA key=<key>
First Client Call

Phone dials x1234

GDOI registration for x1234

Policy for x1234:
IP addr=239.1.1.2,
SPI=0x12049a92,
IPSEC policy: 3DES/SHA,
3DES key=<three keys>,
SHA key=<key>

GDOI key server
First Client Call Completed

“Hello?”

Encrypted voice multicast packets

Policy for x1234:
IP addr=239.1.1.2,
SPI=0x12049a92,
IPSEC policy: 3DES/SHA,
3DES key=<three keys>,
SHA key=<key>

GDOI key server
Second Client Call

“Hello?”

Encrypted voice multicast packets

IPSec SA

GDOI registration for x1234

Policy for x1234:
IP addr=239.1.1.2,
SPI=0x12049a92,
IPSEC policy: 3DES/SHA,
3DES key=<three keys>,
SHA key=<key>
Second Client Call Completed

“Hello!”

Encrypted voice multicast packets

“Hello?”

GDOI key server
Conference Call Complete

“Who’s on the call?”

“I’m here.”

Encrypted voice multicast packets

“Hello?”

“I’m here.”

GDOI key server

© 2005 Cisco Systems, Inc. All rights reserved.
Rekey Message Sent

“Yak, yak.”

Encrypted voice multicast packets

Policy for x1234:
- IP addr=239.1.1.2,
- SPI=0x97b3a243,
- IPSEC policy: 3DES/SHA,
- 3DES key=<three keys>,
- SHA key=<key>

GDOI key server
New SA Installed

Encrypted voice multicast packets

Policy for x1234:
IP addr=239.1.1.2,
SPI=0x97b3a243,
IPSEC policy: 3DES/SHA,
3DES key=<three keys>,
SHA key=<key>

GDOI key server
Steps in configuration

Key server configuration

Group members

Clearing a GM registration with a key server

Verifying secure multicast

ISAKMP Policies

- crypto isakmp policy 1
  - authentication pre-share
- crypto isakmp key p address 10.0.3.1
- crypto isakmp key p address 10.0.3.2
- crypto isakmp key p address 10.0.4.2

Key Server Config

- crypto ipsec transform-set e esp-des
- crypto ipsec transform-set gdoi-p esp-3des esp-sha-hmac
- crypto ipsec profile gdoi-p
- set security-association lifetime seconds 3600
- set transform-set gdoi-p
- crypto gdoi group gdoigroupname
  - identity number 3333
  - server local
  - rekey address ipv4 1020
  - rekey lifetime seconds 36000
  - rekey authentication mypubkey rsa mykeys
  - sa ipsec 1
    - profile gdoi-p

  - match address ipv4 101

! The following line is the access control list downloaded from the key server to the group member
! This line tells the group members which encrypted traffic is acceptable in this SSM configuration:
access-list 101 permit ip host 10.0.1.1 host 192.168.5.1

! The following line is the rekey access control list to which multicast addresses the rekeys are to be sent:
access-list 102 permit udp host 10.0.5.2 eq 848 host 192.168.1.2 eq 848
Cisco IOS CLI-Configuration

Steps in configuration

Key server configuration

Group members

Clearing a GM registration with a key server

Verifying secure multicast

ISAKMP Policies

- crypto isakmp policy 1
- authentication pre-share
- crypto isakmp key key1 address 10.0.5.2

Group Member Config

- crypto gdoi group diffint
- identity number 3333
- server address ipv4 10.0.5.2

- crypto map diffint 10 gdoi
- set group diffint

- interface Loopback0
- ip address 10.65.9.2 255.255.255.255
- ip pim sparse-dense-mode

- ip pim bidir-enable
- ip pim send-rp-announce Loopback0 scope 16 group-list 1
- ip pim send-rp-discovery scope 16

interface Ethernet0/0
- ip address 10.0.3.2 255.255.255.0
- ip mtu 1000
- ip pim sparse-dense-mode
- no ip route-cache

- crypto map diffint
**Cisco IOS CLI-Configuration**

**Steps in configuration**

**Key server configuration**

- **clear crypto gdoi**
  
  **Clears current group-member registration with the key server and starts a new registration.**
  
  **All current group-member policy is deleted. A new registration is started.**

**Group members**

- **show crypto gdoi**

  **Displays information about a GDOI configuration.**
Multicast Group Security Configuration

**Group Controller / Key Server Configuration**
crypto ipsec transform-set gdoi-trans esp-3des esp-sha-hmac
crypto ipsec profile gdoi-p
  set security-association lifetime seconds 120
  set transform-set gdoi-trans
crypto gdoi group diffint
  identity number 3333
  rekey address ipv4 101
  rekey lifetime seconds 300
  rekey authentication mypubkey rsa <mykeys>
sa ipsec 1
  profile gdoi-p
    match address ipv4 120
    address ipv4 <gdoi_source>
access-list 120 permit ip <s_prefix/mask> <d_prefix/mask>
access-list 101 permit udp host <gdoi_source> eq 848 host <mroute> eq 848
ip pim ssm default

**Group Member Configuration**
ip pim ssm default
Secure Multicast: General Design Considerations

- HW encryption modules required and recommended
- Running routing protocols doesn’t require a tunneling protocol
- Set MTU on all network devices to 1400 to avoid fragmentation
- Summarize routes
Secure Multicast: General Design Considerations
Which Mode—Sparse or Dense

“Sparse mode Good! Dense mode Bad!”

PIM-SM (RFC 2362)

• Assumes no hosts wants multicast traffic unless they specifically ask for it

• Uses a rendezvous point (RP)
  Senders and receivers “rendezvous” at this point to learn of each others existence.
    Senders are “registered” with RP by their first-hop router
    Receivers are “joined” to the shared tree (rooted at the RP) by their local designated router (DR)

• Appropriate for…
  Wide scale deployment for both densely and sparsely populated groups in the enterprise
  Optimal choice for all production networks regardless of size and membership density
RP Resource Demands

- (*,G) entry – 260 bytes + outgoing interface list overhead
- (S,G) entry – 212 bytes + outgoing interface list overhead
- Outgoing interface list overhead—80 bytes per OIL entry

Example of 10 groups with 6 sources per group:
# of (*,G)s > (260 + (<# of OIL entries> x 80) = 10 (260 + (3 x 80)) = 5000 bytes for (*,G)
# of (S,G)s > (212 + (<# of OIL entries> x 80) = 60 (212 + (3 x 80)) = 27,120 bytes for (S,G)
Total of 32,120 bytes for mroute table memory requirements
GDOI Usage

• Application scenarios:
  – Encryption of IP packets sent over satellite links
  – Hoot-and-holler audio conferencing
  – Multicast router control traffic
  – Real-time content replication
  – IP/TV
  – mVPN
Application Scenario: Encryption of IP Packets Sent over Satellite Links

1. The hub site encrypts IP multicast packets and forwards them to the satellite-sending unit.
2. The satellite-sending unit transmits the IP packets to the satellite.
3. The satellite retransmits the IP packet toward the dish antennas located at branch sites.
4. The router in the branch site decrypts multicast packets and forwards the packet to branch sites.
## Elements of End-to-End Architecture

<table>
<thead>
<tr>
<th>Source discovery</th>
<th>Cable</th>
<th>DSL</th>
<th>ETTH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SDR, SIP Web (SSM)</td>
<td>RP (ISM), URD</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content sourcing</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MPEG1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPEG2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPEG4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reliability</th>
<th>PGM,DF, Tibco,</th>
<th>PGM, Sub-Sec conver</th>
<th>PGM,DF, Tibco,</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP redundancy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content requesting</th>
<th></th>
<th>IGMPv2 v2 app/stack</th>
<th>IGMPv3 v3 app/stack</th>
<th>MLDv2 v2 app/v2 stack</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Routing</th>
<th>BGP4+, MTR</th>
<th>PIM-SM, SSM,, bidir</th>
<th>MvVPN, UDLR , MPLS P2MP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Forwarding</th>
<th>Rate-limit, CAR</th>
<th>RSVP</th>
<th>Rate-limit, CAR</th>
<th>App</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>QoS</th>
<th>App</th>
<th>App</th>
<th>App</th>
<th>App</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Management</th>
<th>App</th>
<th>MRM, HP-nnmm</th>
<th>App</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Access control</th>
<th>App</th>
<th>ACL, DOCSIS, Mcast-AAA</th>
<th>App</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Accounting</th>
<th>App</th>
<th>Multicast netflow</th>
<th>Mcast-AAA</th>
<th>App</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th>App</th>
<th>Native in IPSec, GDOI</th>
<th>GDOI</th>
<th>App</th>
</tr>
</thead>
</table>
Application Scenario: Encryption of IP Packets Sent over Satellite Links

Key features:

• Hardware accelerated

• Support for dynamic routing (EIGRP, OSPF, etc.)

Good for:

• The solution is good for enterprise, commercial, and governmental organizations who wish to enable secure video communications through the use of broadband satellite connectivity

• Branch offices with more than 1-2 subnets

• Multicast requirements
Application Scenario: Encryption of IP Packets Sent over Satellite Links—*Best Practices*

- For multicast control traffic enable PIM sparse mode
- Digital certificates/PKI for group member authentication
Application Scenario: Security for Multicast VPN

- 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 & 2 join that high-bandwidth source
- Data-MDT is formed for this high-bandwidth source
- GDOI is used to protect the multicast data
Application Scenario: Security for Multicast VPN

Key features:

- Security for mVPN packets which are flowing through the provider in a native multicast deployment
- DoS protection for the mVPN edge systems
- Comprehensive protection: Protection in the customer premise between CPE devices, protection in the provider domain between PE devices
- Dynamic routing (EIGRP, OSPF, etc.)

Good for:

- Customers already using mVPN but need security
- Up to 240 branch offices with more than 1-2 subnets
- Multicast requirements
Application Scenario: Security for Multicast VPN—Best Practices

- Digital certificates/PKI for tunnel authentication
- For multicast control traffic enable PIM sparse mode
- Protected GDOI key server behind an edge router
Application Scenario: Integration of GDOI with Dynamic Multipoint VPN

- DMVPN hub and all spokes are configured as group members. All group members register with the key server.

- Key server distributes group and IPSec policy information to all group members.

- A spoke-to-hub tunnel is established using NHRP. All packets traveling via the DMVPN tunnel are now encrypted using group key.

- The spoke sends a NHRP resolution request to the hub for any spoke-to-spoke communication.

Benefit: By using secure multicast functionality in DMVPN network, the delay caused by IPSec negotiation is eliminated.

Note: Multicast traffic will still be forwarded to hub for any spoke to spoke even with this deployment.
Application Scenario: Integration of GDOI with Dynamic Multipoint VPN

Key features:

• GDOI with DMVPN
• Dynamic routing (EIGRP, OSPF, etc.)
• Dead Peer Detection (DPD)

Good for:

• DMVPN customers wishing to deploy voice with VPN
• Branch offices with more than 1-2 subnets
• Multicast requirements
Application Scenario: Integration of GDOI with Dynamic Multipoint VPN—Best Practices

- EIGRP (or OSPF, etc.) dynamic routing, <1000 peers per head end
- Primary and secondary (or more) IPSec/GRE tunnels to alternate head ends, using routing cost for preference
- Typically static crypto maps, unless branches have dynamic IP addresses, then dynamic crypto map required on head end
- Configure DPD to detect loss of communication
- Digital certificates/PKI for tunnel authentication
Application Scenario: Secure PIM Control Traffic with IPSec

PIM control packets can be encrypted

- Session peer is set to 224.0.0.13 (PIM control messages)
- Supports multiple IPSec options
  - Hash functions: MD5, SHA1
  - Security protocols: Authentication Header (AH), Encapsulating Security Payload (ESP)
  - Encryption algorithms: DES, 3DES, AES
- Recommended IPSec mode: Transport
- Recommended key method: Manual

- IPSec AH is the recommended security protocol in the PIM-SM and PIM-Bidir IETF drafts
- Initial Cisco IOS® Software Release – 12.4(6)T
Platform Support and Useful Links
## Cisco IOS Platform Support

<table>
<thead>
<tr>
<th>Platform</th>
<th>Group Member</th>
<th>Key Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Yes</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Cisco® 850/870 Series Access routers</td>
<td>Yes</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Cisco 1800/1841</td>
<td>Yes</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Cisco 2800</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 3800 (AIM-II/AIM-III)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 7200 NPEG1, VAM2+</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 7300 NPEG1, VAM2+</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 7200 NPEG2, VAM2+</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 7300 NPEG2, VAM2+</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 7200 NPEG2, VSA</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 7300 NPEG2, VSA</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 7600 VPN-SPA</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Useful Links

- http://www.cisco.com/go/multicast