Tunnel-less VPN's with Group Encrypted Transport (GET) VPN

Siva Natarajan
Product Manager, Security Technology Group

GET VPN Now!

Presenter: Donovan Williams, Product Manager, Security Technology Group

Agenda

- Problem Statement
- Solution
- Benefits
- Main Use Cases
- Higher Level View: How does it work?
- Platform support and useful links

Problem Statement

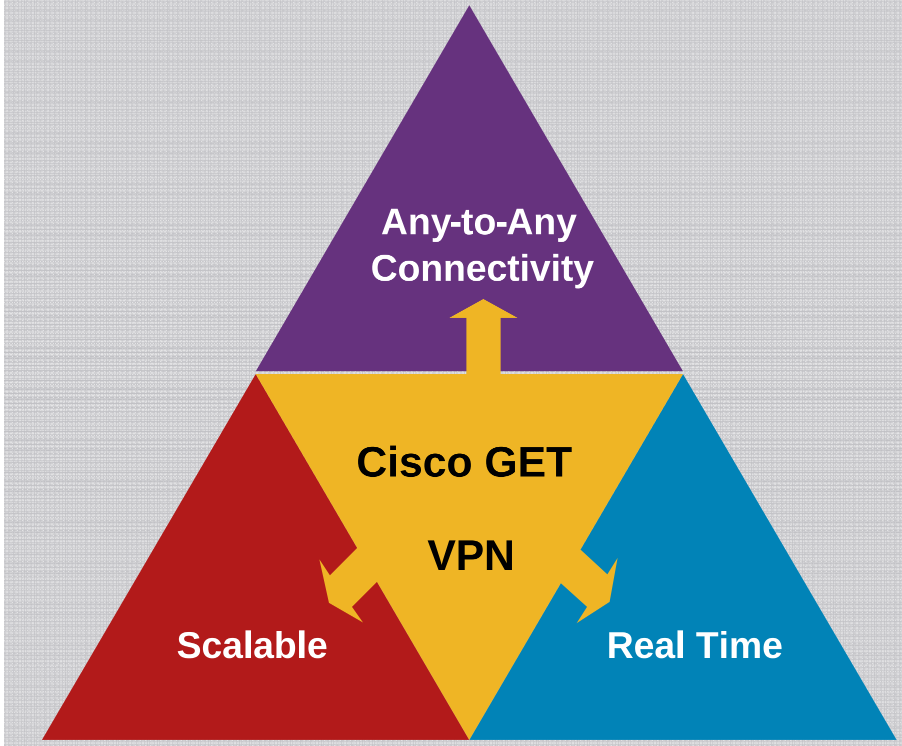
- Today's Enterprise WAN technologies force a trade-off between QoS-enabled branch interconnectivity and transport security
  - –Networked applications such as voice, video and web-based applications drive the need for instantaneous, branch interconnected, QoS-enabled WANs
  - –Distributed nature of network applications result in increased demands for scalable branch to branch interconnectivity
  - –Increased network security risks and regulatory compliance have driven the need for WAN transport security
  - –Need for balanced control of security management between enterprises and service providers
- Service providers want to deliver security services on top of WANs such as MPLS without compromising their SLAs

Agenda

- Problem Statement
- Solution & Benefits
- Main Use Cases
- Higher Level View: How does it work?
- Platform support and useful links

Cisco Group Encrypted Transport (GET) VPN – Solution for Tunnel-less VPNs

Cisco GET VPN delivers a revolutionary solution for tunnel-less, any-to-any branch confidential communications

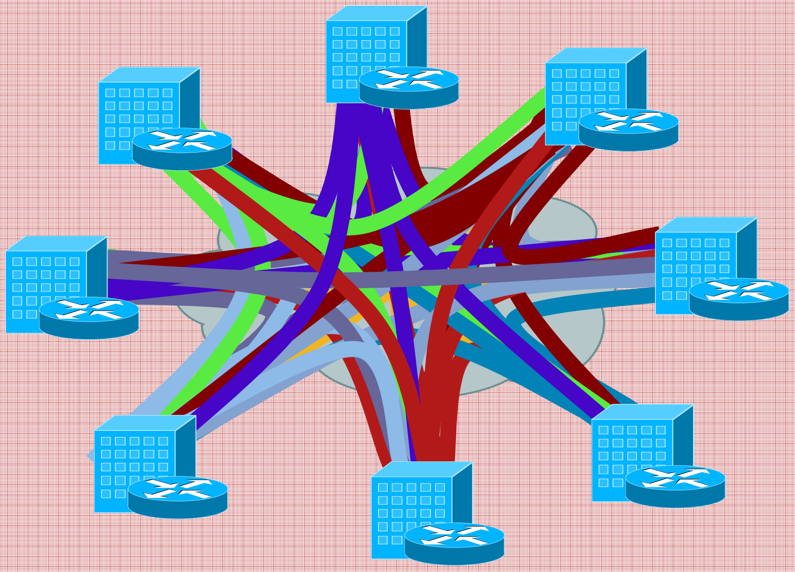


- **Large-scale any-to-any encrypted communications**
- **Native routing without tunnel overlay**
- **Optimal for QoS and Multicast support - improves application performance**
- **Transport agnostic - private LAN/WAN, FR/AATM, IP, MPLS**
- **Offers flexible span of control among subscribers and providers**
- **Available on Cisco Integrated Services Routers; Cisco 7200 and Cisco 7301 with Cisco IOS 12.4(11)T**

Tunnel-less VPN - A New Security Model

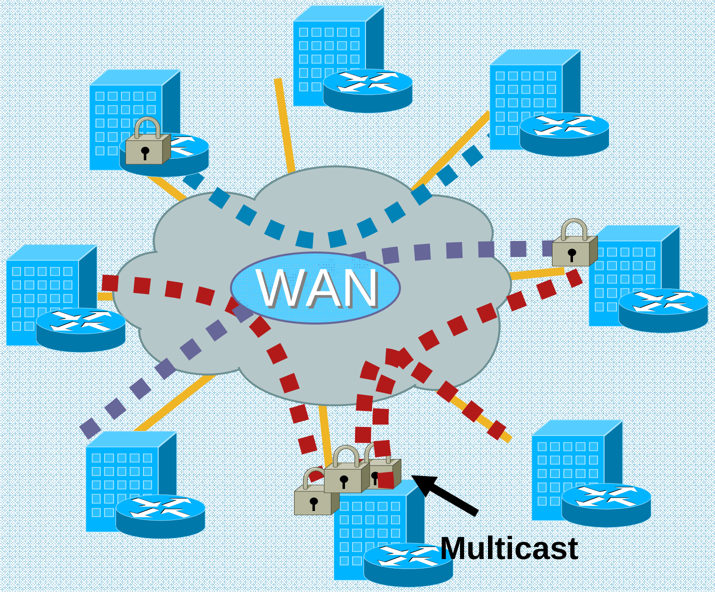
Any-to-Any encryption: Before and After GET VPN

Before: IPsec P2P Tunnels



- Scalability—an issue (N^2 problem)
- Overlay routing
- Any-to-any instant connectivity can’t be done to scale
- Limited advanced QoS
- Multicast replication inefficient

After: Tunnel-less VPN



- Scalable architecture for any-to-any connectivity and encryption
- No overlays – native routing
- Any-to-any instant connectivity
- Advanced QoS
- Efficient Multicast replication

Benefits of Cisco GET VPN

Previous Limitations	New Feature and Benefits
Multicast traffic encryption through IPsec tunnels: – Not scalable – Difficult to troubleshoot	**Encryption supported for Native Multicast and Unicast traffic with GDOI** – Allows higher scalability – Simplifies Troubleshooting – Extensible standards-based framework
Overlay VPN Network – Overlay Routing – Sub-optimal Multicast replication – Lack of Advanced QoS	**No Overlay** – Leverages Core network for Multicast replication via IP Header preservation – Optimal Routing introduced in VPN – Advanced QoS for encrypted traffic
Full Mesh Connectivity – Hub and Spoke primary support – Spoke to Spoke not scalable	**Any to Any Instant Enterprise Connectivity** – Leverages core for instant communication – Optimal for Voice over VPN deployments

Agenda

- Problem Statement
- Solution & Benefits
- Main Use Cases
- Higher Level View: How does it work?
- Platform support and useful links

Customer Deployment Scenarios

Customers for Group Encrypted Transport fall into two categories:

Key Targets

Enterprises (Enterprises Purchasing Private WAN (e.g. MPLS) Connectivity from SP but wanting to manage GET themselves)

- Meet security policy or regulatory requirements
- Provides data privacy via crypto while maintaining any-to-any connectivity and QoS
- Streamlines multicast across crypto

SP Managed CPE/Security Services (SP selling connectivity, security services to Enterprises, commercial etc). SP manages GET

- Meet security policy or regulatory requirements
- Provides data privacy via crypto while maintaining any-to-any connectivity and QoS
- Streamlines multicast across crypto

Additional Value

For Enterprise IPSec VPNs (over public Internet)

Enhances DMVPN and GRE-based S-S VPNs by:

- Providing manageable, highly scalable meshing capability very cost-effectively
- Simplifies key management in larger deployments

Agenda

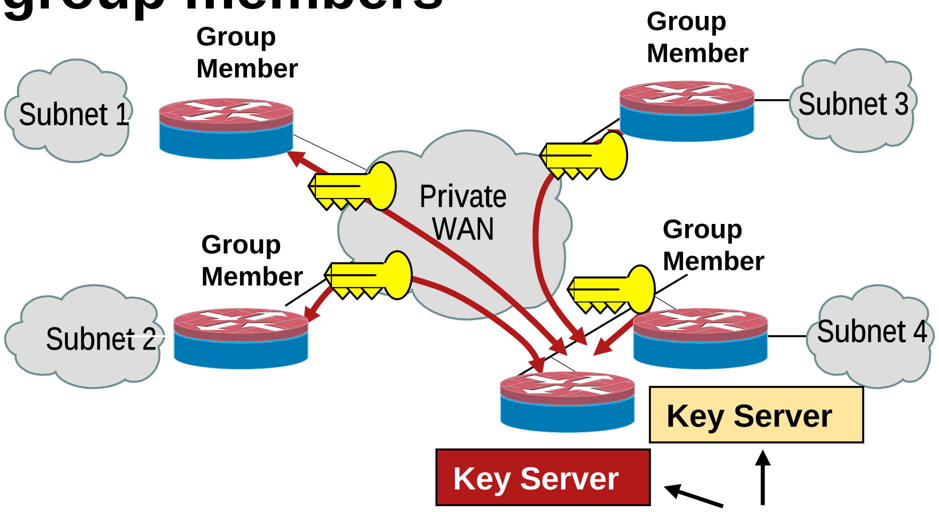
- Problem Statement
- Solution & Benefits
- Main Use Cases
- Higher Level View: How does it work?

How Cisco GET VPN Works

GET simplifies security policy and key distribution by using Group Domain of Interpretation (GDOI)

- GDOI:
  - A key distribution mechanism
  - Group Key Model
  - Standards-based (RFC 3547)
- GET uses GDOI and adds:
  - Cooperative Key Servers for high availability & geographic distribution
  - Secure Unicast control/data plane via encryption
  - Unicast/Multicast key distribution

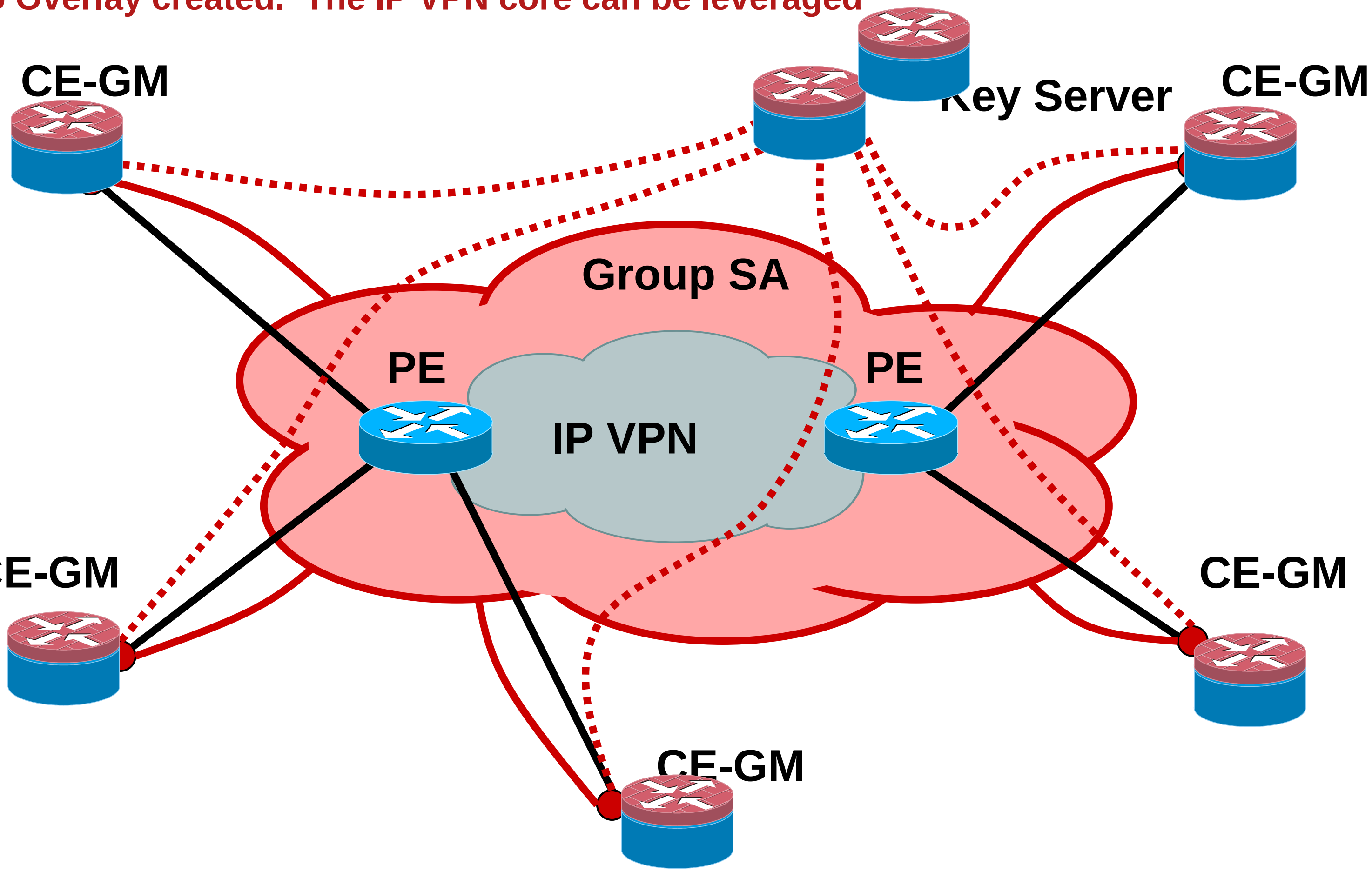
Key Server: Authenticates group members, distributes keys and policies; group member provisioning is minimized. Application traffic is encrypted by group members



GET adds cooperative Key Servers for high availability

Cisco Group Encrypted Transport (GET) VPN – Solution for Tunnel-less VPNs Security

- Crypto Map defines persistent Group SA attachment with any-to-any connectivity.
- Dormant control plane until rekey required
- No Overlay created. The IP VPN core can be leveraged

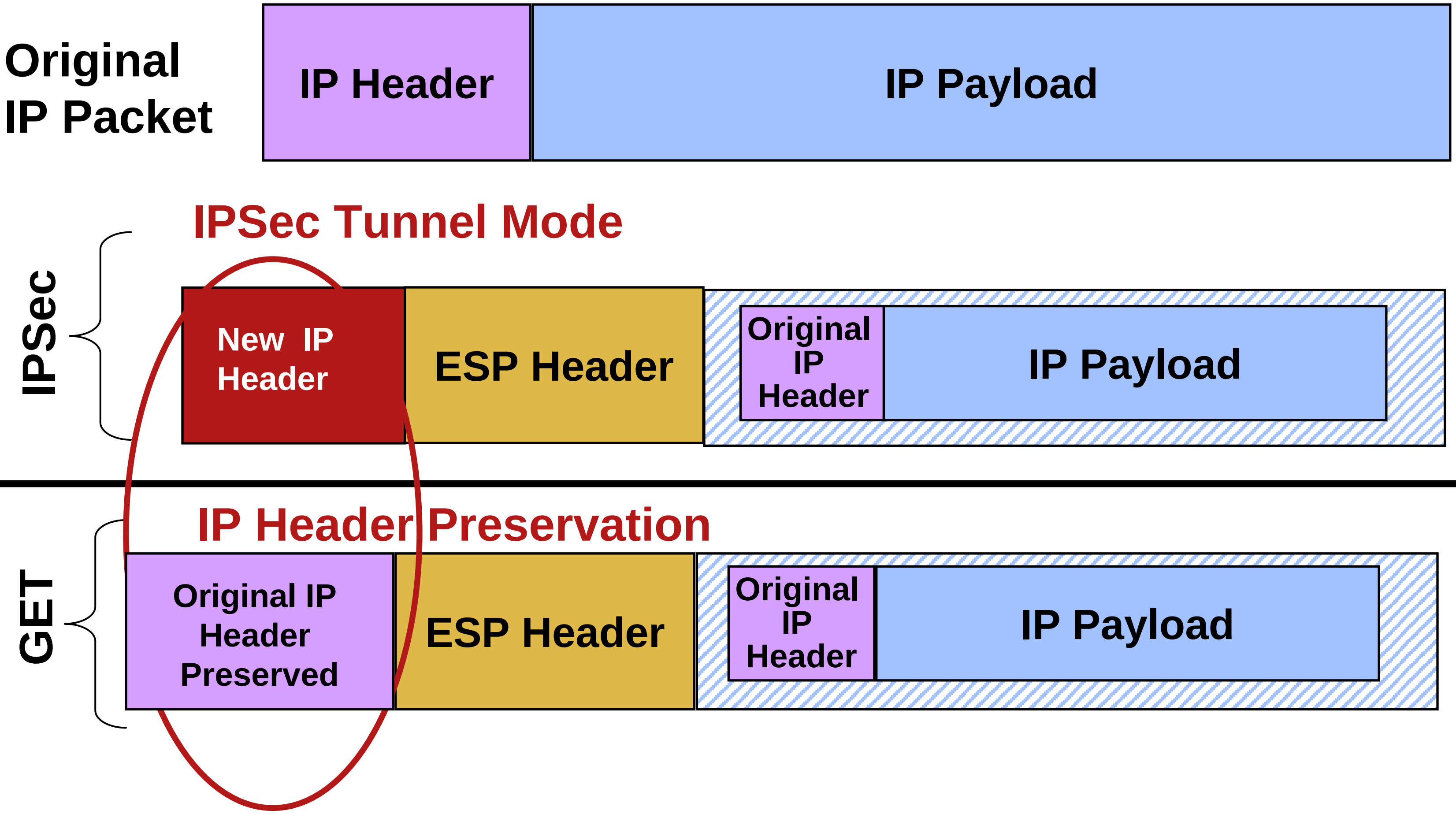


GM: Group Member

Group SA: SA shared between Group Members

How GET VPN Prevents Overlay Routing

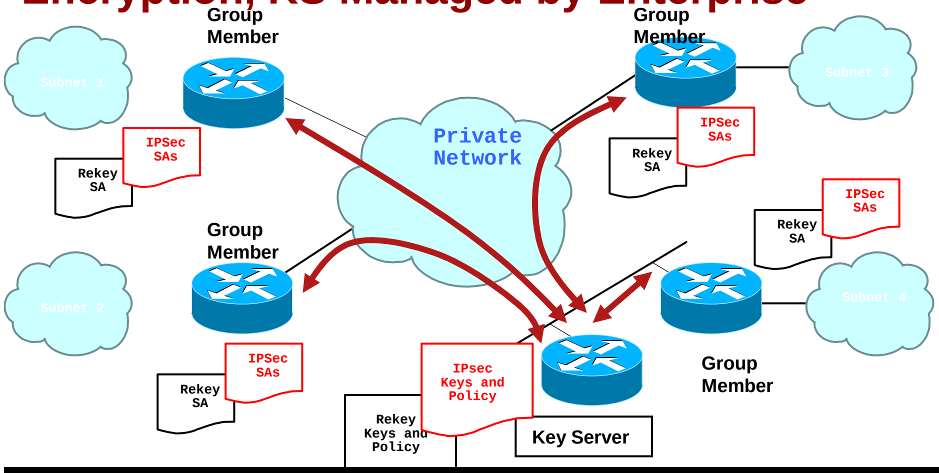
Cisco GET VPN uses IP header preservation to mitigate routing overlay and to preserve QoS and multicast capabilities



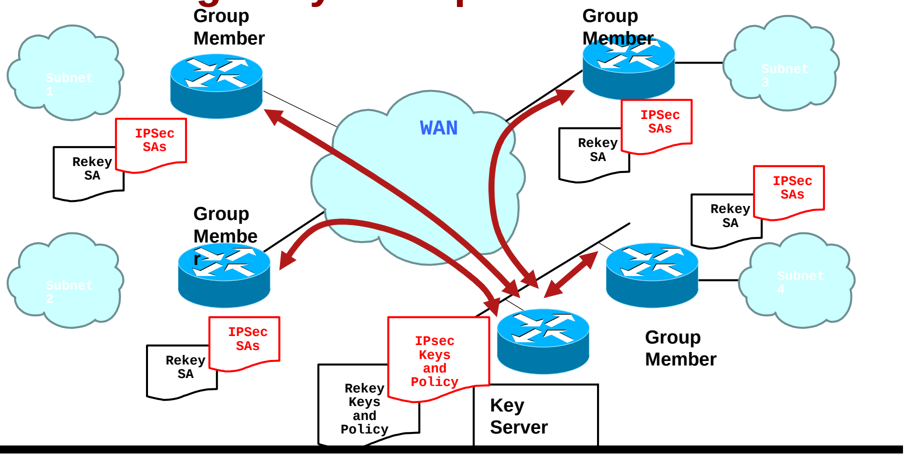
Scenarios Overview

Application Scenarios: GET in the Enterprise/SP WAN

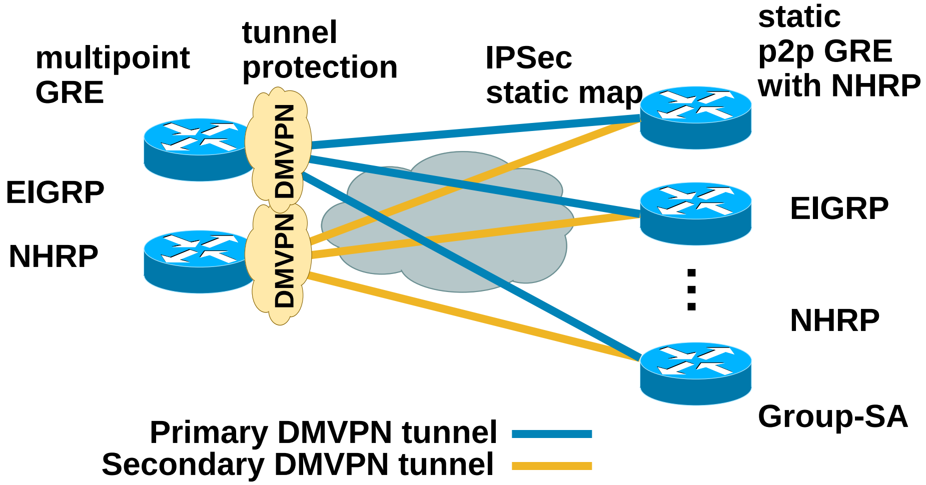
Enterprise owned CPE, CE-CE with GET Encryption, KS Managed by Enterprise



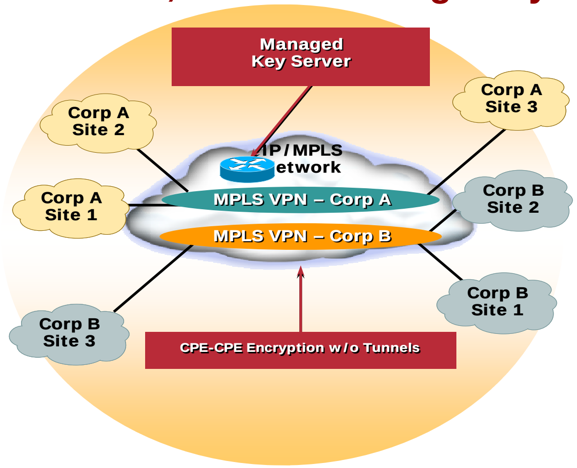
Managed CPE with GET Encryption, with KS Managed by Enterprise



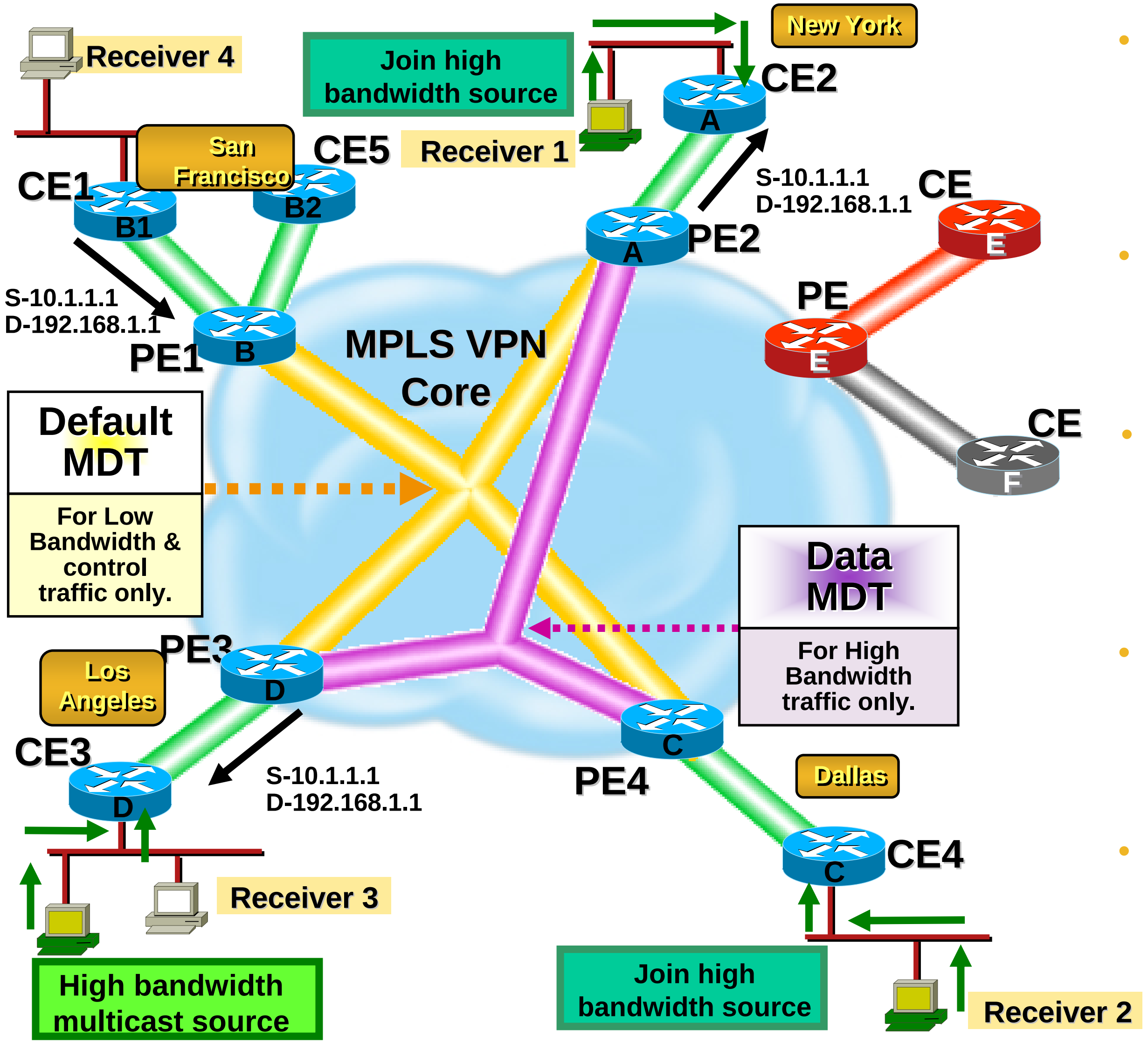
DMVPN (mGRE over IPSec) with GET



Hosted GET, with KS Managed by SP

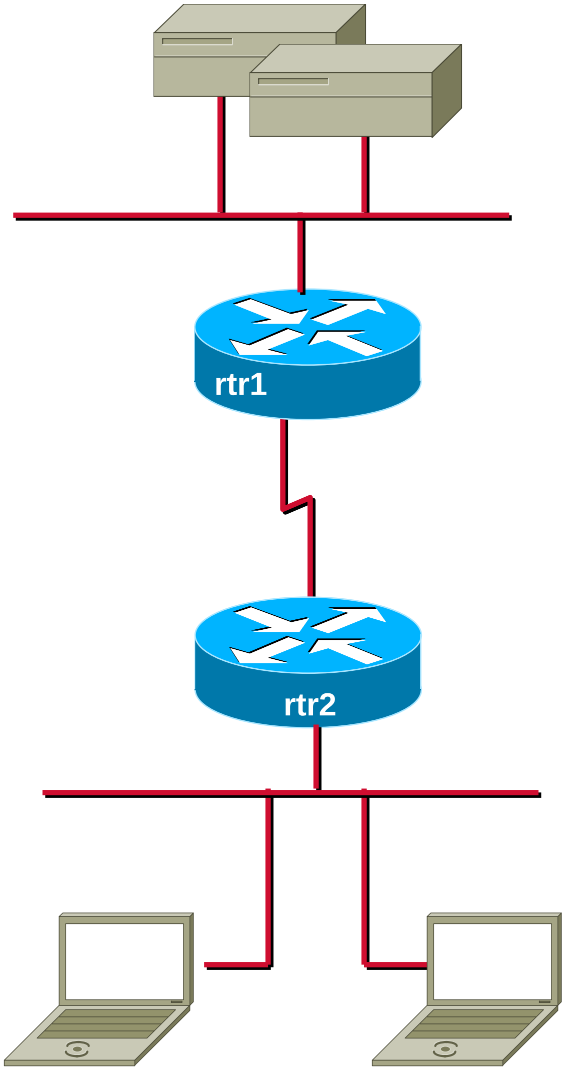


Application Scenario: Security for Multicast VPN



- 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
- GET VPN is used to protect the multicast data

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 IOS Release – 12.4(6)T

Platform Support and Useful Links

GET VPN IOS Platform Support

Platform	Group Member	Key Server
Software	Yes	Not recommended
850/870	Yes	Not recommended
1800/1841	Yes	Not recommended
2800	Yes	Not recommended
3800 (AIM-II/AIM-III-SSL)	Yes	Yes
7200 NPEG1, VAM2+	Yes	Yes
7300 NPEG1, VAM2+	Yes	Yes
7200 NPEG2, VAM2+	Yes	Yes
7300 NPEG2, VAM2+	Yes	Yes
7200 NPEG2, VSA	No	No
7300 NPEG2, VSA	No	No
6500/7600 VPN-SPA	No	No

🟨 **Not Committed, but**
No known issues.
Expected to be in pi4

🟩 **Shipping in pi3**

🟧 **Not Committed, H/W**
Acceleration. Expected
To be fixed in pi1

🟥 **Not Committed, H/W**
Acceleration needs
to be fixed. No plans

For more information

http://www.cisco.com/go/getvpn/

Backup

Detailed Overview of GET VPN

Group Encrypted Transport Enabled VPN Features

- **Key Management**
  - –GDOI Registration/Rekey
  - –Unicast and/or Multicast Key Distribution
  - –Cooperative Key Server for High Availability
- **Policy Management**
  - –Centralized Policy Distribution from PRIMARY Group Controller Key Server
  - –Group Member Policy Exception (e.g. local deny)
  - –Group Member Policy Merge (concatenate KS policy with GM policy)
- **IPSec Data Plane**
  - –IPSec Tunnel Mode with IP Address Preservation
  - –Passive Security Associations for Graceful Roll-out (i.e. Receive Only SA)
  - –Pseudo-time Synchronous Anti-Replay Protection
- **Enhanced Debugging (fault isolation)**

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.

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 co-exists 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.

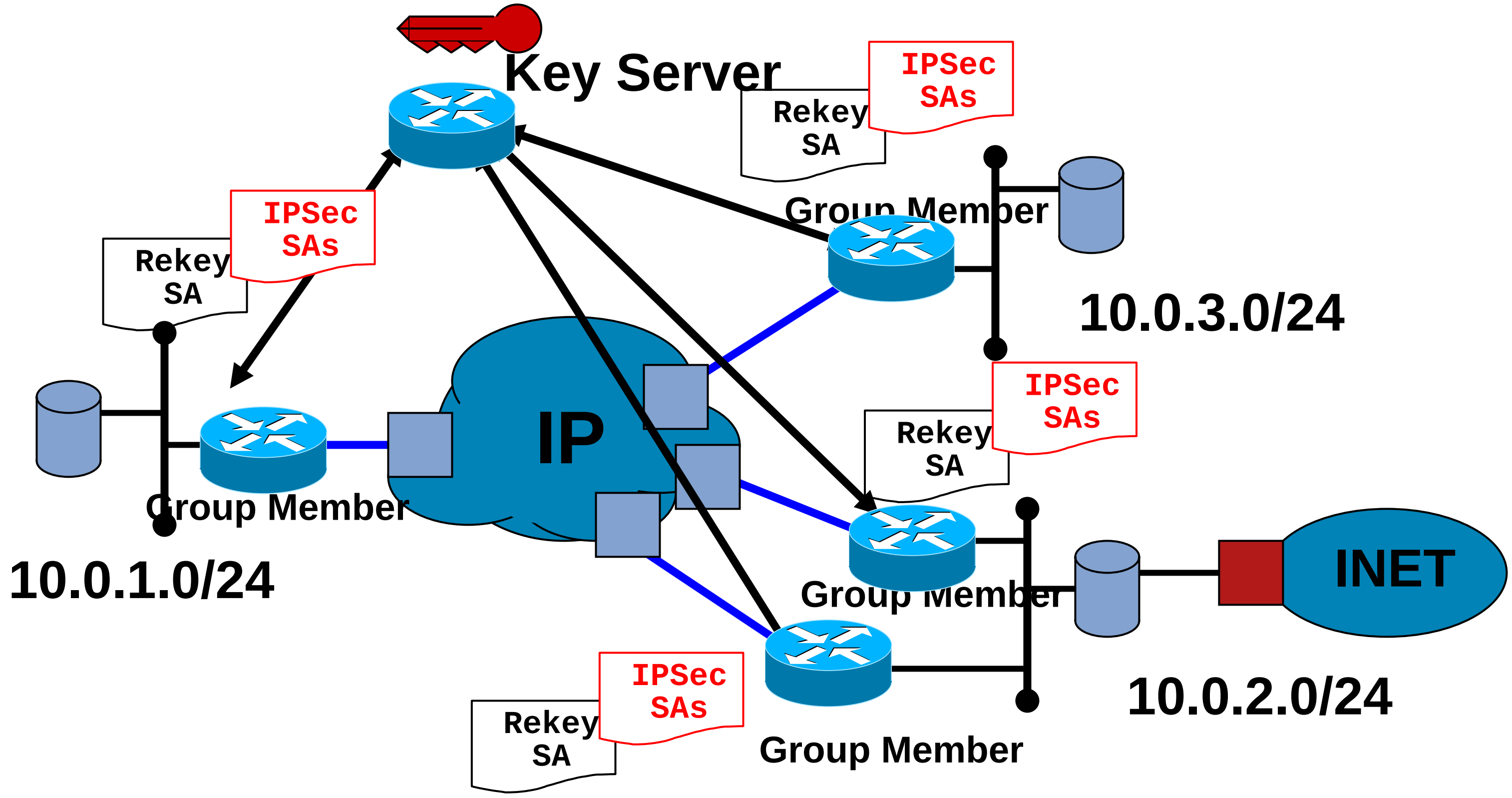
  At the end of IKE Phase 1 a state machine looks at the DOI number to determine next exchange.

- A GDOI service must listen on a port other than port 500 (IKE).

Quick Comparison of IKEv1, IKEv2 vs. GDOI

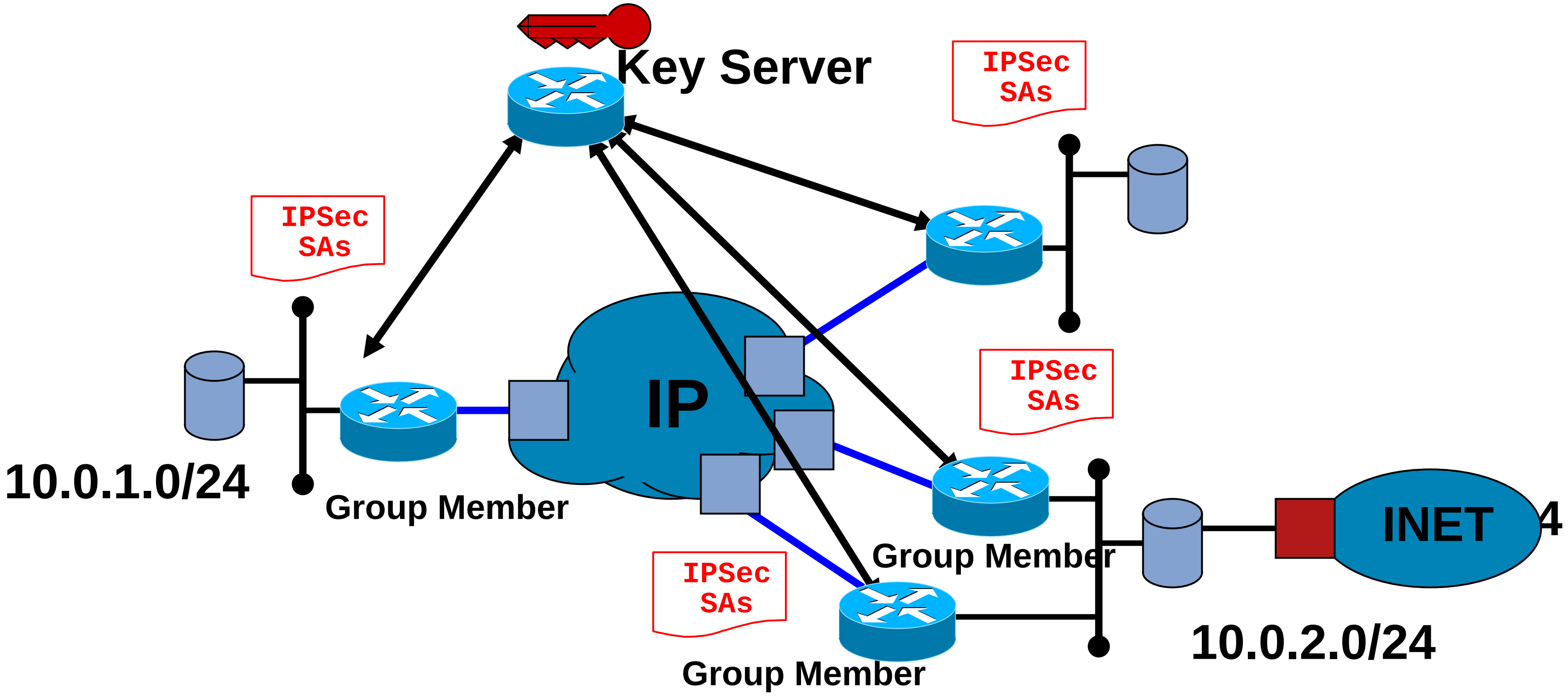
	IKEv1	IKEv2	GDOI
RFC Documents	**2407/2408/ 2409**	RFC 4306	RFC 3547
UDP port	**500, 4500**	**500,** 4500	**848**
Phases	**2, Ph. 1 (6/3 messages), Ph. 2 (3 messages)**	**2, Ph. 1 (4 messages), Ph. 2 (2 messages)**	**2, Ph. 1 (6/3 messages),** **Ph. 2 (4 messages)**
Authentication Type	**Signature, PSK, PKI**	Signature, PSK, PKI	Signature, PSK, PKI
SA Negotiation	**Responder selects Initiator's Proposal**	Same as IKEV1, proposal structure simplified	Not negotiated, GDOI is used to push keys and policies
Identity Hiding	**Yes in MM, No in AM**	Yes	Yes in MM, No in AM
Keep-alives	**No**	Yes	No
Anti-DoS	**No**	Yes*	Yes*
UDP/NAT	**No**	Yes	No
Reliability	**No**	**Yes**	**Yes**
PFS	**Yes**	Yes	Yes
EAP/CP	**No**	Yes	No

GDOI Registration
Key Distribution



- Each router registers with the Key Server.
- Key Server authenticates the router, performs an authorization check.
- Key Server downloads the encryption policy and keys to the router

GDOI Rekey
Key Distribution

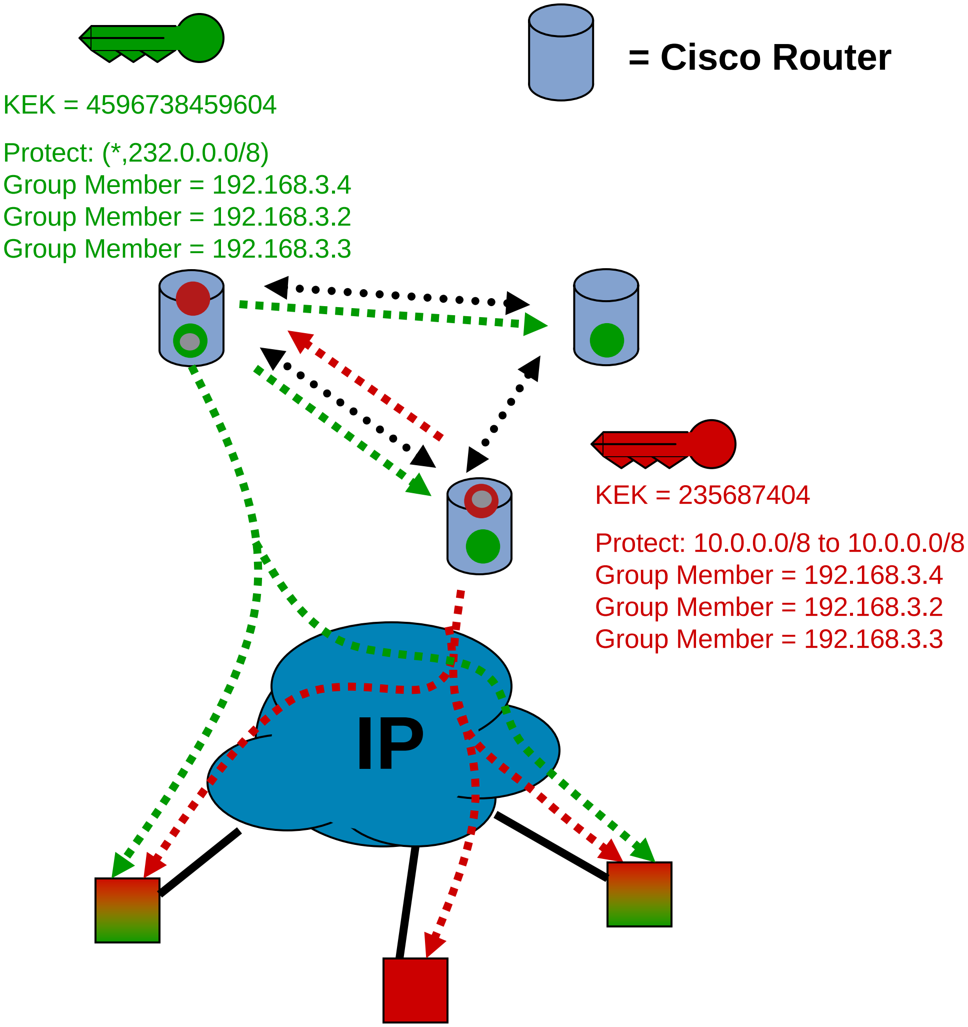


- The key server generates and pushes new IPsec keys and policy to the routers when necessary
- Re-key messages can also cause group members to be ejected from the group
- Rekeys can be sent either using multicast or unicast

Cooperative Key Server
Key Distribution

- **Primary Key Server Designated Per Group**
- **Multiple Secondary Key Servers Per Group**
- **Synchronization of Policy Database for Graceful Fail-over**

  Synchronized - Group Policy, Active Group Members, Key Encryption Key, Traffic Encryption Key



= Cisco Router

KEK = 4596738459604

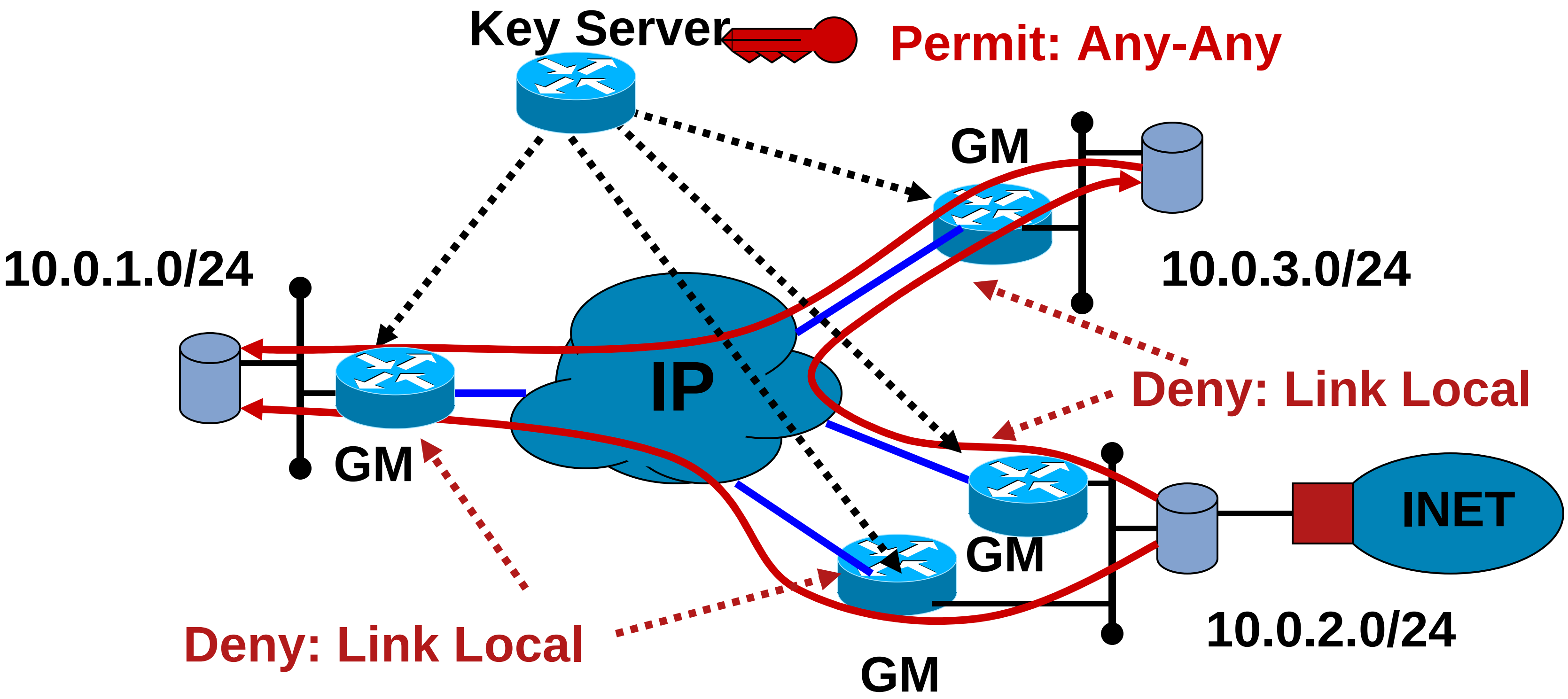
Protect: (*,232.0.0.0/8)
Group Member = 192.168.3.4
Group Member = 192.168.3.2
Group Member = 192.168.3.3

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

Policy Management

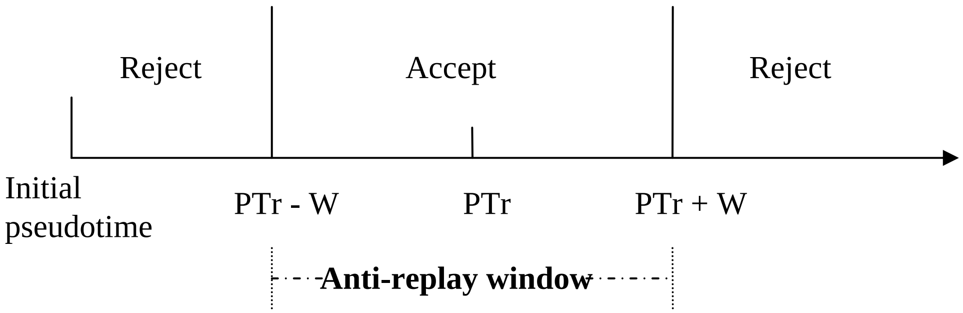
- Local Policy Configured by Group Member
- Global Policy Configured and Distributed by Key Server
- Global Policy Appended to Local Policy



Pseudo-Synchronous Anti-Replay

- Replay Based on Synchronization of Pseudo-time Across Group Members
- Key Server Manages Relative Clock Time (not Universal Clock Time)
- Group Members Periodically Re-sync Pseudo-time with every Rekey
- No Existing Fields in IPSec Header are Viable for Pseudo-time (while maintaining IPSec compliance)

Example



- **If Sender's Pseudo Time falls in the below Receiver window, packet accepted else packet is discarded**

Fault Isolation

- Show and Debugging capabilities for Key server

  show crypto gdoi ks, debug crypto gdoi ks

- Show and Debugging capabilities for Group Member

  show crypto gdoi gm, debug crypto gdoi gm etc

- Multi-level Debug/Fault Isolation capabilities for various user roles e.g.

  debug crypto gdoi error

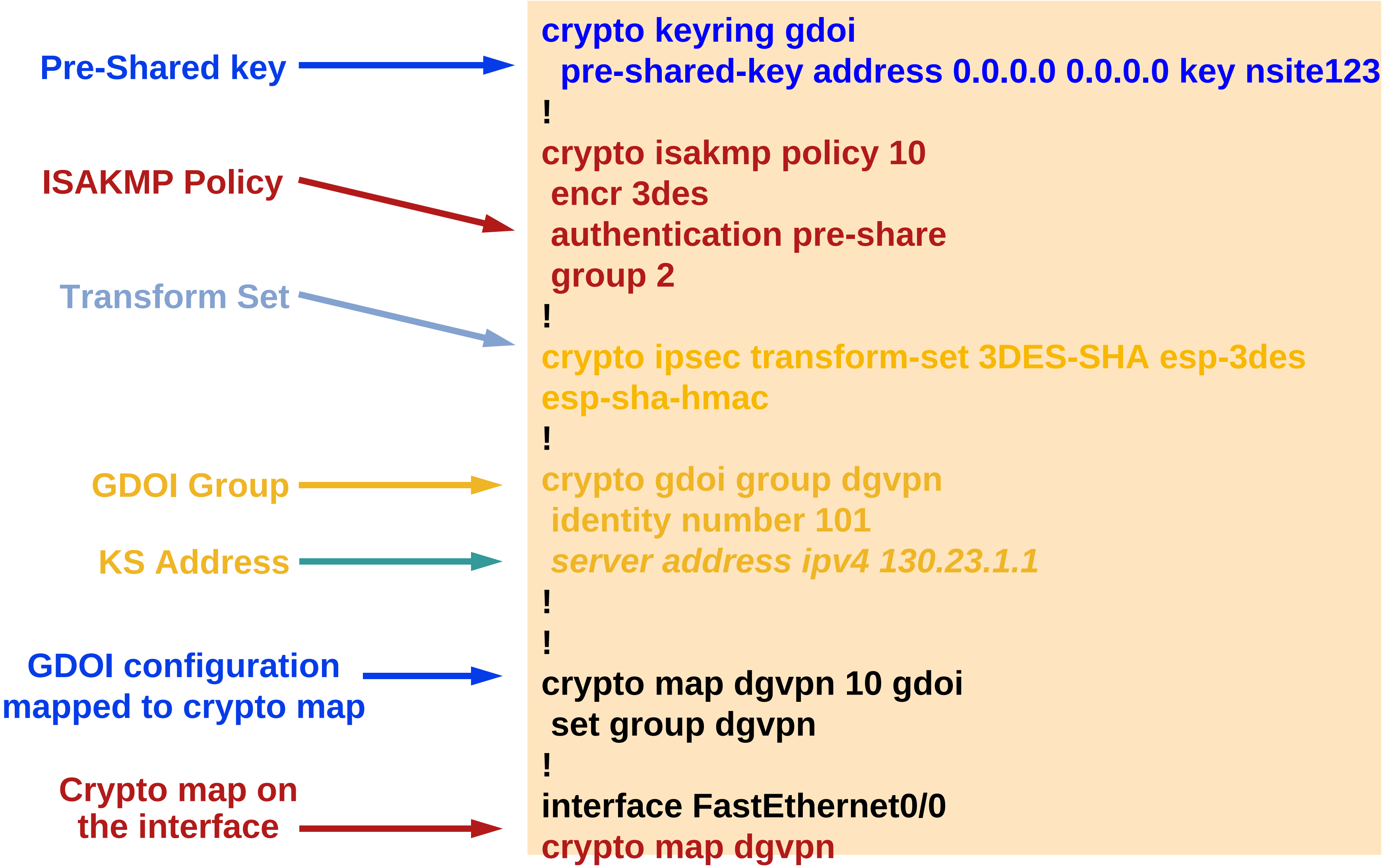
  debug crypto gdoi terse

  debug crypto gdoi customer

  debug crypto gdoi engineer

  debug crypto gdoi packet

GM Configuration



Pre-Shared key

ISAKMP Policy

Transform Set

GDOI Group

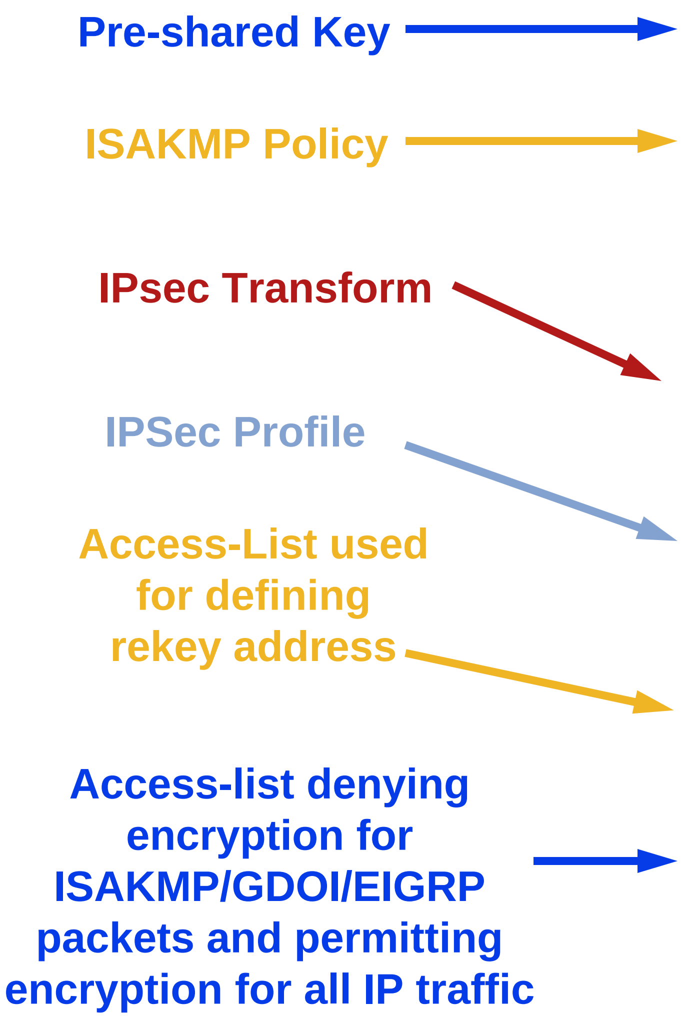
KS Address

GDOI configuration mapped to crypto map

Crypto map on the interface

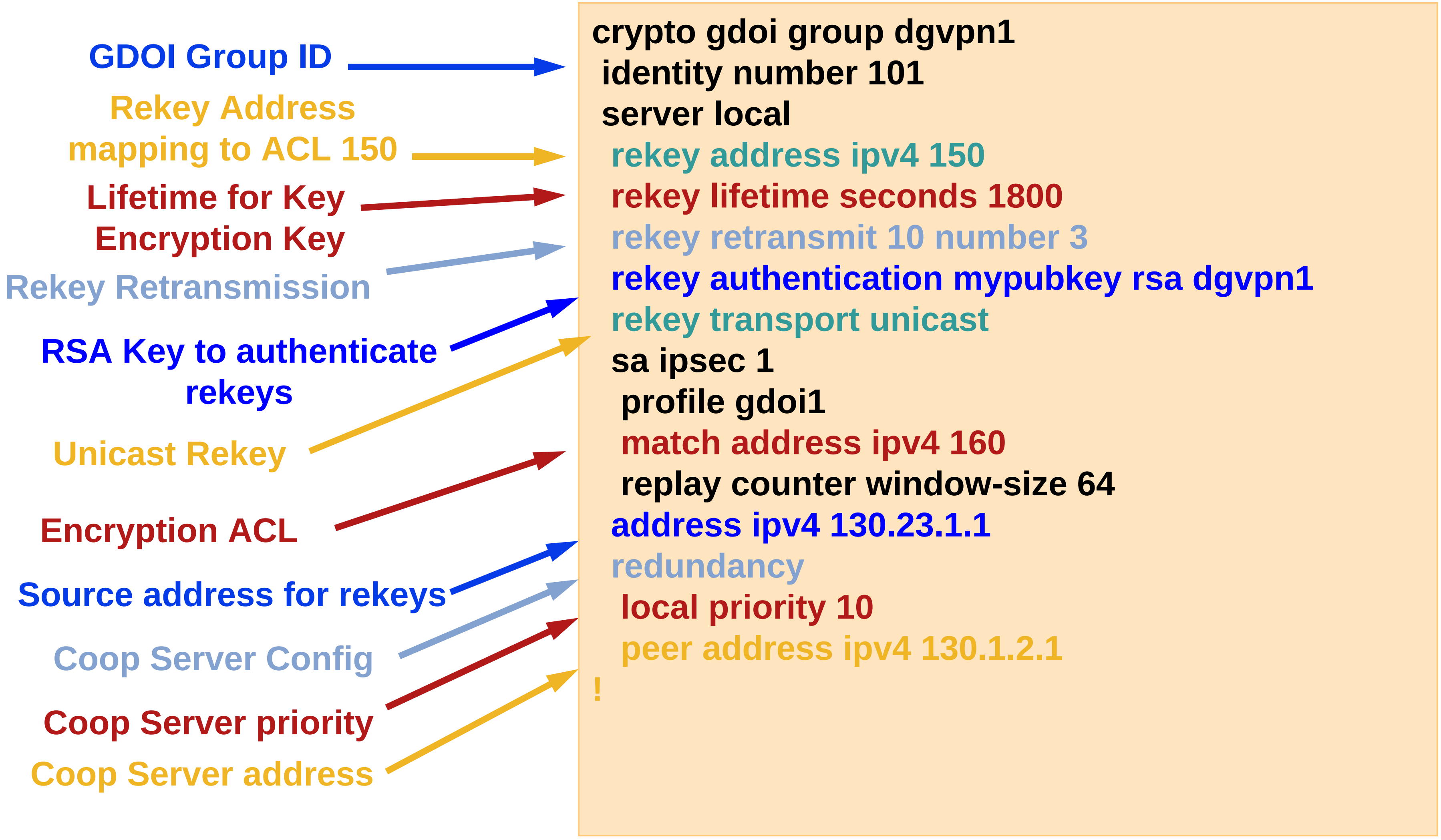
```
crypto keyring gdoi
  pre-shared-key address 0.0.0.0 0.0.0.0 key nsite123
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto ipsec transform-set 3DES-SHA esp-3des esp-sha-hmac
!
crypto gdoi group dgvpn
 identity number 101
 server address ipv4 130.23.1.1
!
!
crypto map dgvpn 10 gdoi
 set group dgvpn
!
interface FastEthernet0/0
crypto map dgvpn
```

GKCS Configuration


Pre-shared Key
ISAKMP Policy
IPsec Transform
IPSec Profile
Access-List used for defining rekey address
Access-list denying encryption for ISAKMP/GDOI/EIGRP packets and permitting encryption for all IP traffic

```
crypto keyring gdoi1
  pre-shared-key address 0.0.0.0 0.0.0.0 key nsite123
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto ipsec transform-set 3DES-SHA esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi1
 set security-association lifetime seconds 900
 set transform-set 3DES-SHA
!
access-list 150 permit ip any any
!
access-list 160 deny   eigrp any any
access-list 160 deny   udp any any eq isakmp
access-list 160 deny   udp any any eq 848
access-list 160 permit ip any any
```

GKCS Configuration (cont.)



GDOI Group ID

Rekey Address mapping to ACL 150

Lifetime for Key Encryption Key

Rekey Retransmission

RSA Key to authenticate rekeys

Unicast Rekey

Encryption ACL

Source address for rekeys

Coop Server Config

Coop Server priority

Coop Server address

```
crypto gdoi group dgvpn1
 identity number 101
 server local
  rekey address ipv4 150
  rekey lifetime seconds 1800
  rekey retransmit 10 number 3
  rekey authentication mypubkey rsa dgvpn1
  rekey transport unicast
  sa ipsec 1
   profile gdoi1
   match address ipv4 160
   replay counter window-size 64
  address ipv4 130.23.1.1
  redundancy
   local priority 10
   peer address ipv4 130.1.2.1
!
```

IPSec VPN Features in IOS 12.2(18)SXF2

- Encrypted Multicast over GRE for IPSec VPN SPA
  - IPSec SPA Only, no VPNSM
  - Up to 500 tunnels
  - Limited broadcast sources
  - VRF-Aware IPSec
  - GRE Tunnel Protection (TP)
- Sup32 support for IPSec VPN SPA and VPNSM
- IOS Sup2 Image available