



# Cisco Group Encrypted Transport VPN – Technical Overview



**December 2006**

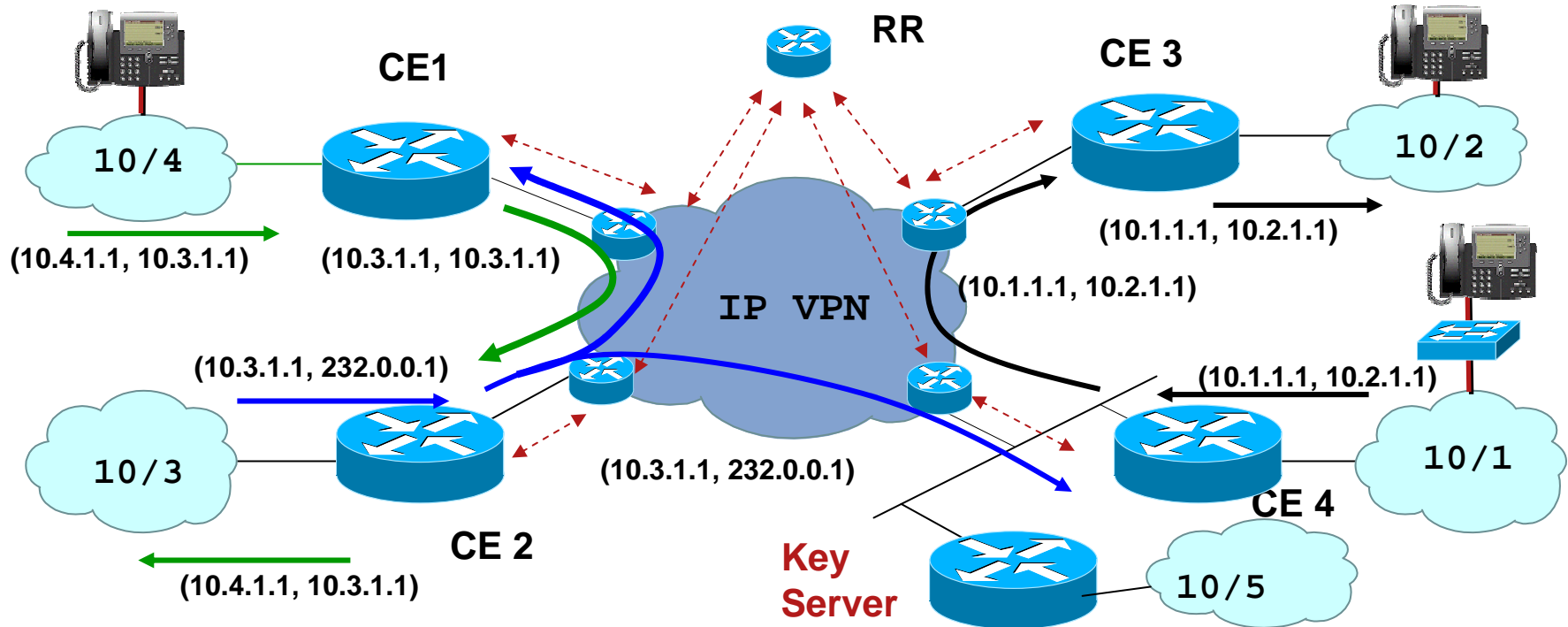
# Agenda

- Problem Statement
- Solution: Group Encrypted Transport
- Technology Components
- Feature Overview
- Provisioning and Management

# 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

# Solution: Cisco Group Encrypted Transport VPN



## Branch

- **Encrypted Any-Any connectivity**
- Hierarchical Routing (without tunnels)
- Native QoS support
- Native Multicast Encryption

## Enterprise Core

- Any-to-Any Connectivity
- Redundancy Established by Core Routers
- Core for Multicast Replication

## Branch

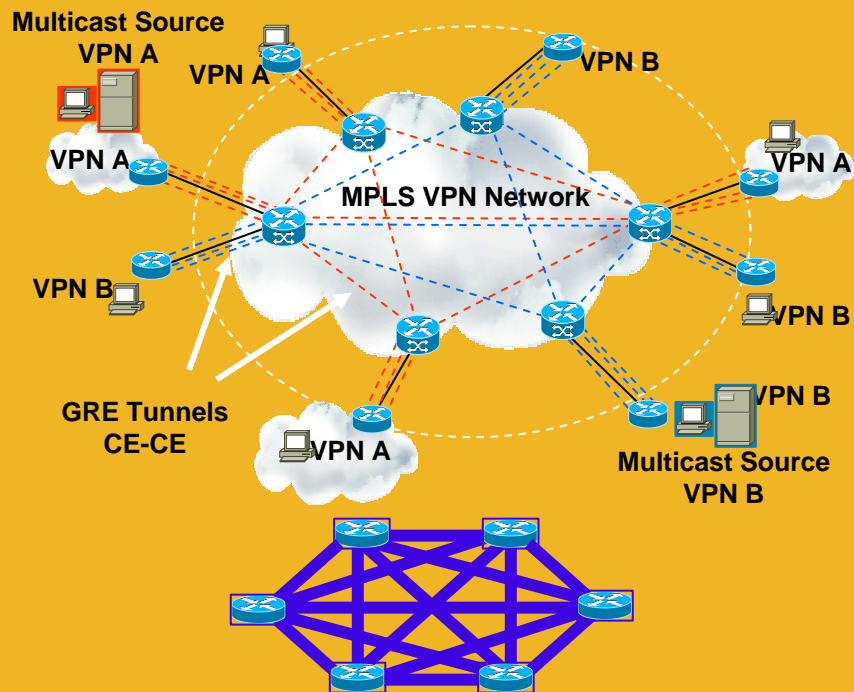
- Transparent Service Integration (e.g., MPLS)
- Integration with DMVPN
- Highly Scalable Full Meshes
- Monitoring/Management: centralized policy distribution CLI/GUI

# Benefits of Cisco GET VPN

Previous Limitations	New Feature and Benefits
<p>Multicast traffic encryption through IPsec tunnels:</p> <ul style="list-style-type: none"><li>– Not scalable</li><li>– Difficult to troubleshoot</li></ul>	<p><b>Encryption supported for Native Multicast and Unicast traffic with GDOI</b></p> <ul style="list-style-type: none"><li>– Allows higher scalability</li><li>– Simplifies Troubleshooting</li><li>– Extensible standards-based framework</li></ul>
<p>Overlay VPN Network</p> <ul style="list-style-type: none"><li>– Overlay Routing</li><li>– Sub-optimal Multicast replication</li><li>– Lack of Advanced QoS</li></ul>	<p><b>No Overlay</b></p> <ul style="list-style-type: none"><li>– Leverages Core network for Multicast replication via IP Header preservation</li><li>– Optimal Routing introduced in VPN</li><li>– Advanced QoS for encrypted traffic</li></ul>
<p>Full Mesh Connectivity</p> <ul style="list-style-type: none"><li>– Hub and Spoke primary support</li><li>– Spoke to Spoke not scalable</li></ul>	<p><b>Any to Any Instant Enterprise Connectivity</b></p> <ul style="list-style-type: none"><li>– Leverages core for instant communication</li><li>– Optimal for Voice over VPN deployments</li></ul>

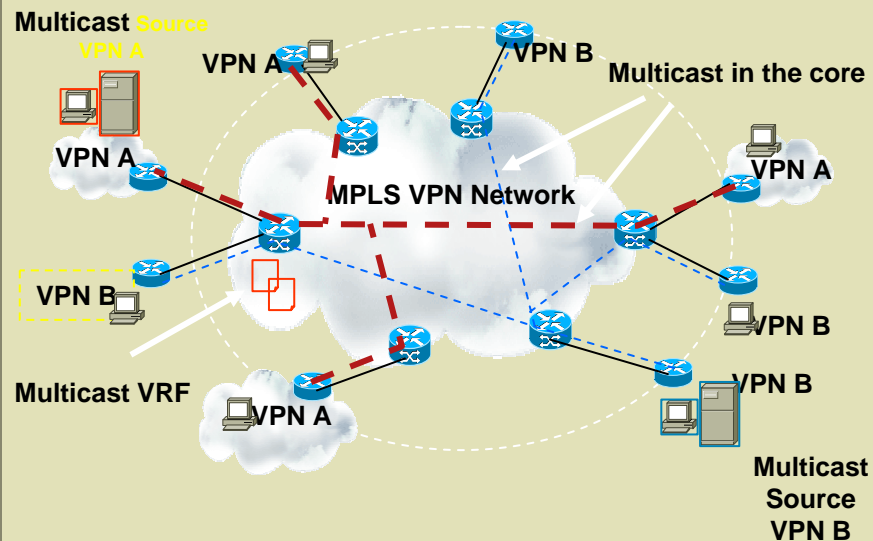
# Cisco GET VPN: Before and After

## Before: CE-CE Protection with Peer-Based Model



- Scalability – an issue ( $N^2$  problem)
- Any-Any Instant Connectivity a issue
- Overlay Routing
- Multicast replication inefficient
- Unable to Leverage Advanced QoS

## After: CE-CE Protection with Group-Based Model



- Highly Scalable Model
- Any-Any instant connectivity with Security
- No Overlay Routing
- Efficient Multicast replication
- Standards based advanced QoS

# Customer Deployment Scenarios

Customers for Cisco GET VPN fall into two categories:

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

- Meet security policy or regulatory requirements
- Want to self-manage VPN keys and group policies

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

- Meet security policy or regulatory requirements
- Complete outsourcing of branch office CPEs, group policies and VPN key management


**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

# Site-to-Site VPN Portfolio

## Positioning & Differentiators

	GET VPN	DMVPN	IPSec (P2P/GRE)	Easy VPN with VTI
<b>When to Use?</b>	Existing Private WAN (FR/ATM)  Encryption on IP VPN w/o Tunnels  Virtualized WAN infrastructure	Replacement for, or existing FR/ATM WAN  Alternative/Backup WAN  Virtualized WAN infrastructure	Replacement for/Existing Traditional FR/ATM WAN  Alternative/Backup WAN	Replacement for/Existing Traditional FR/ATM WAN  Alternative/Backup WAN
<b>What it Does?</b>	Provides scalable, full-time any-any secure connectivity  Enables participation of smaller routers in large meshed networks  Simplified key management	Simplifies configuration for hub & spoke VPNs  Provides low-scale, on-demand meshing	Encryption of pipe	Simplifies configuration for hub & spoke VPNs
<b>Scale</b>	Any Scale Hub/Spoke  Any Scale Mesh	High Scale Hub/Spoke  Low Scale Meshing	High Scale Hub/Spoke for IPsec (Low Scale for GRE)	High Scale Hub/Spoke
<b>Native Multicast</b>	Yes	No – treats like unicast traffic by tunneling it	No – treats like unicast traffic by tunneling it	No – treats like unicast traffic by tunneling it
<b>Dynamic Routing</b>	Yes– No need for overlay Routing	Yes—with Overlay Routing	Yes for GRE (with Overlay routing)	No – not supported
<b>Failover Method</b>	Routing based	Routing based	Stateful Failover	Stateful Failover 
<b>QoS</b>	Yes	Yes	Yes	Yes
<b>Keys</b>	Group-based	Peer-based	Peer-based	Peer-based



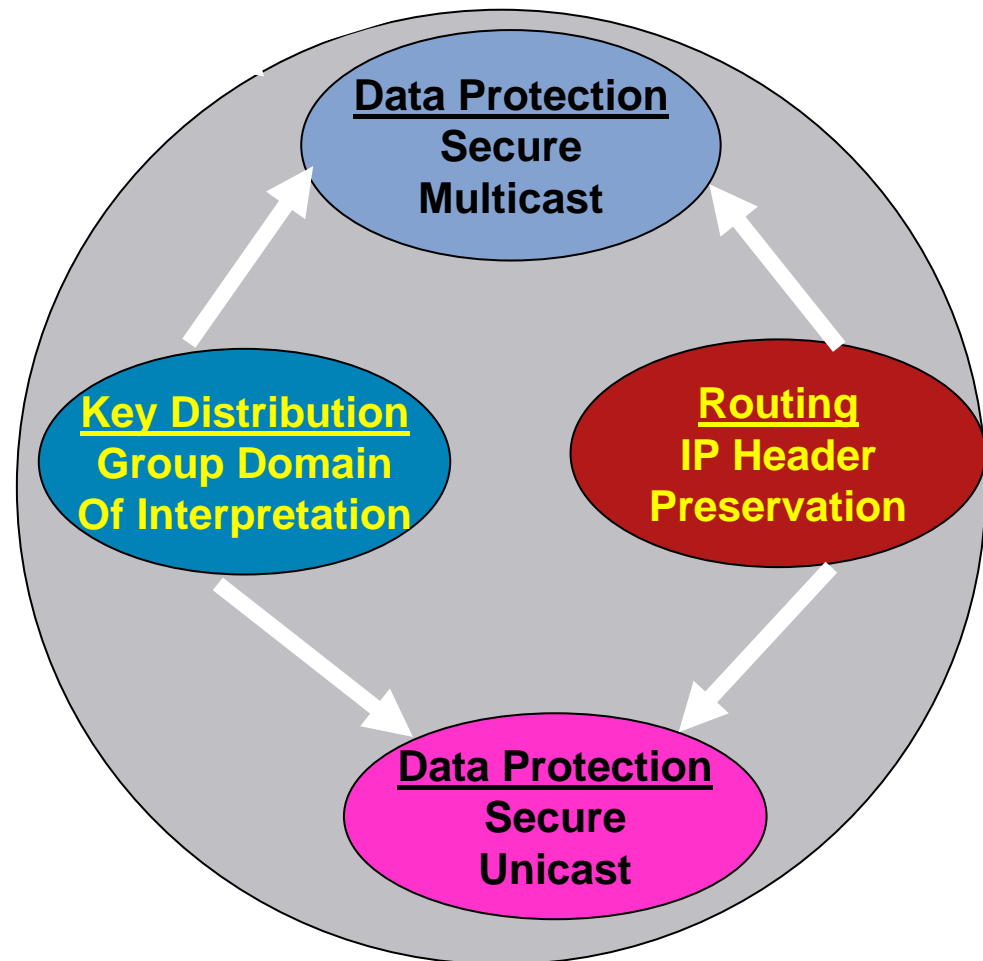
# Technology Components



# Group GET VPN

## Concepts and Relationship

- **Key Distribution** GDOI--Key distribution mechanism (RFC3547)
  - Group Keys/Keys between Peer
  - Encrypted Control Plane
- **Routing Continuity**
  - No overlay Routing
- **Multicast Data Protection**
  - Encrypt Native Multicast
  - Replication in the core based on (S,G)
- **Unicast Data Protection** IPsec is a well-known RFC (RFC2401)
  - Encrypt Unicast with IPsec



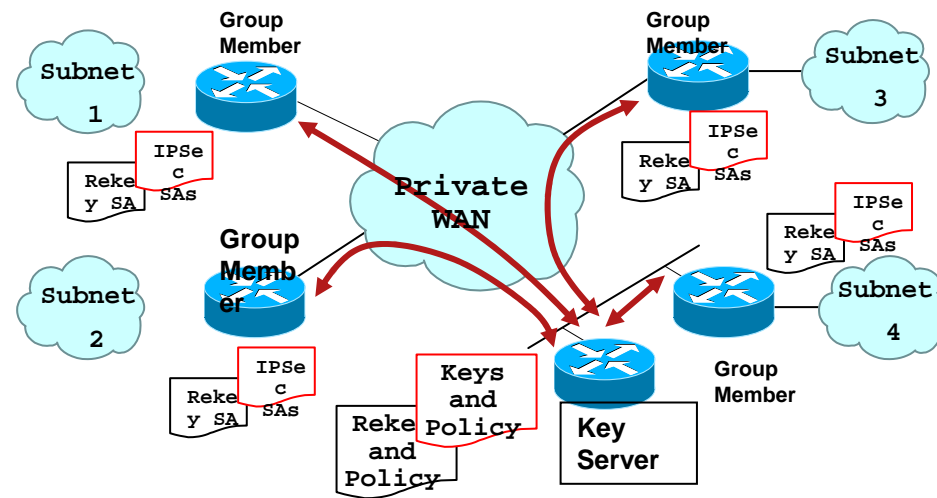
# Secure Key Distribution

## ■ Multicast and Unicast Control Plane:

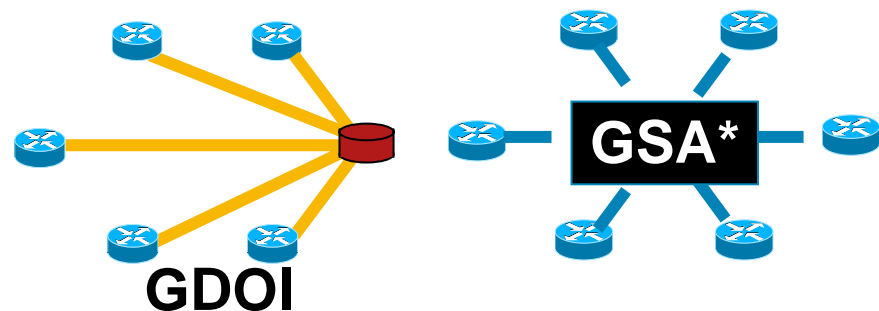
### GDOI--Key distribution mechanism

- RFC 3547
- Group Keys
- Unicast/Multicast Key distribution
- Cooperative Key Server for High Availability
- Secure Control Plane via Encryption

## Group Domain of Interpretation (GDOI)



## Reduces State Complexity

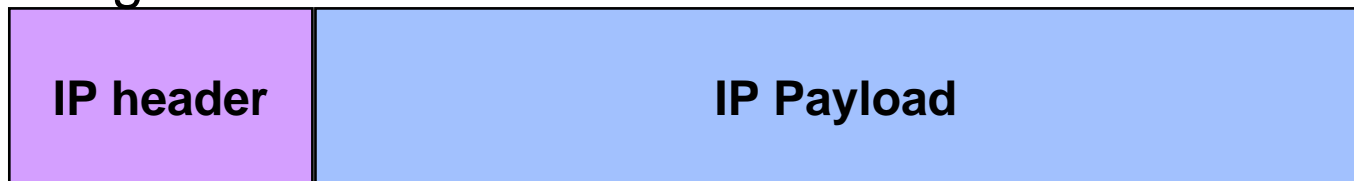


\* GSA = Group Security Association

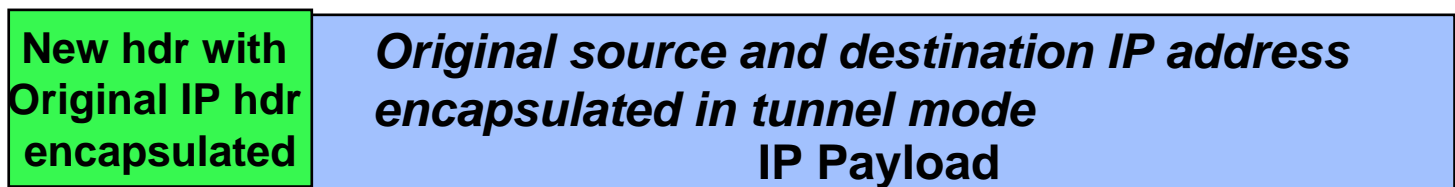
# Routing Continuity:

## IPsec Tunnel Mode with IP Header Preservation

Original IP Packet

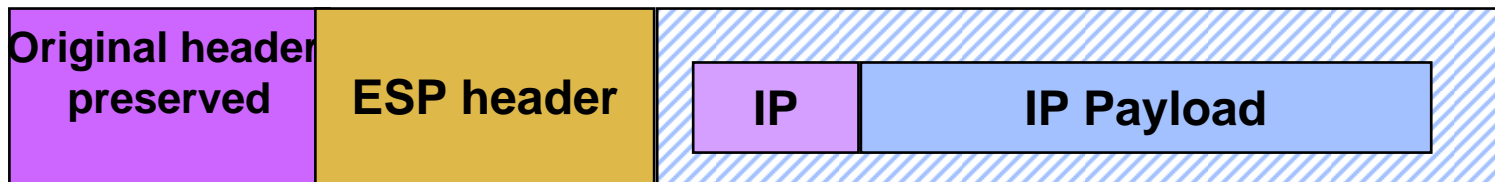


IPSec Tunnel Mode



IP Header Preservation

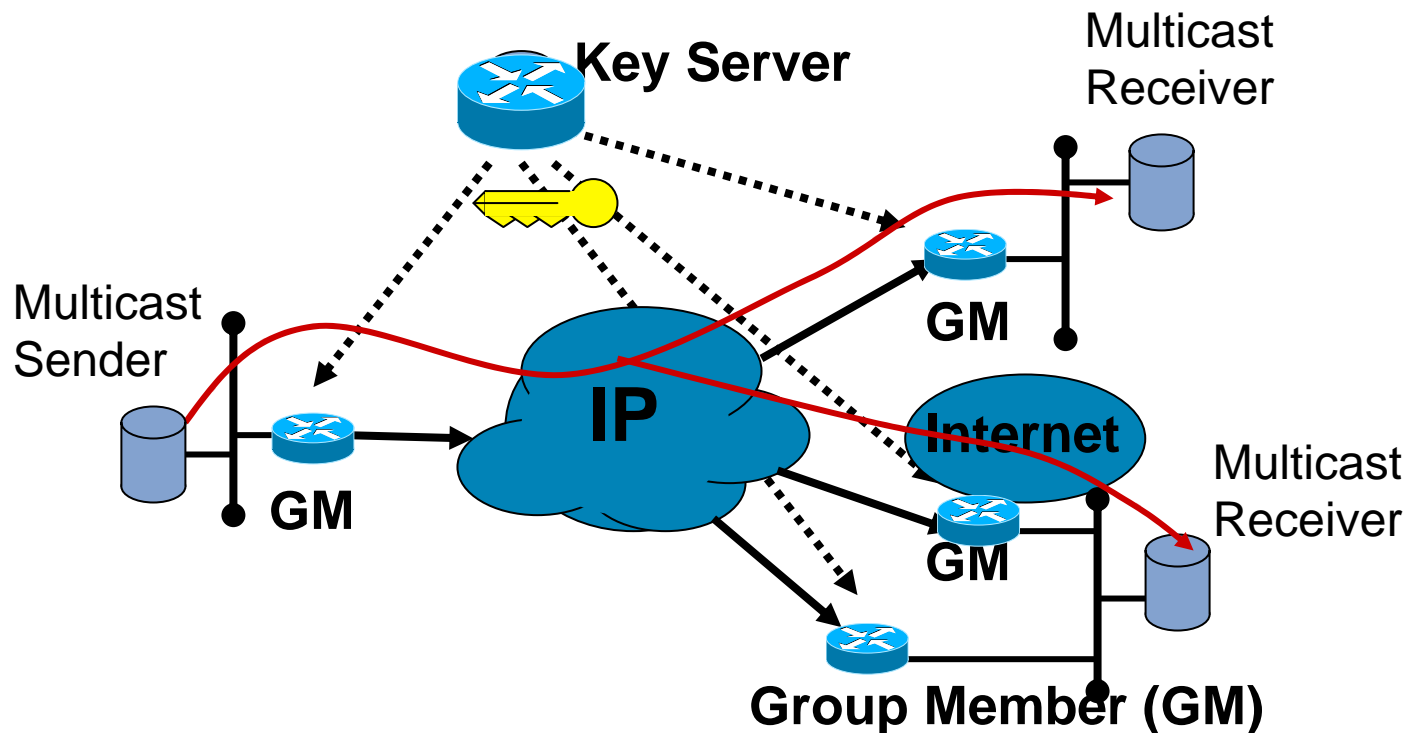
GET  
VPN



This mode is already necessary when encrypting IP multicast packets in order to preserve the (S,G). **Mitigates the requirement for a routing overlay network**

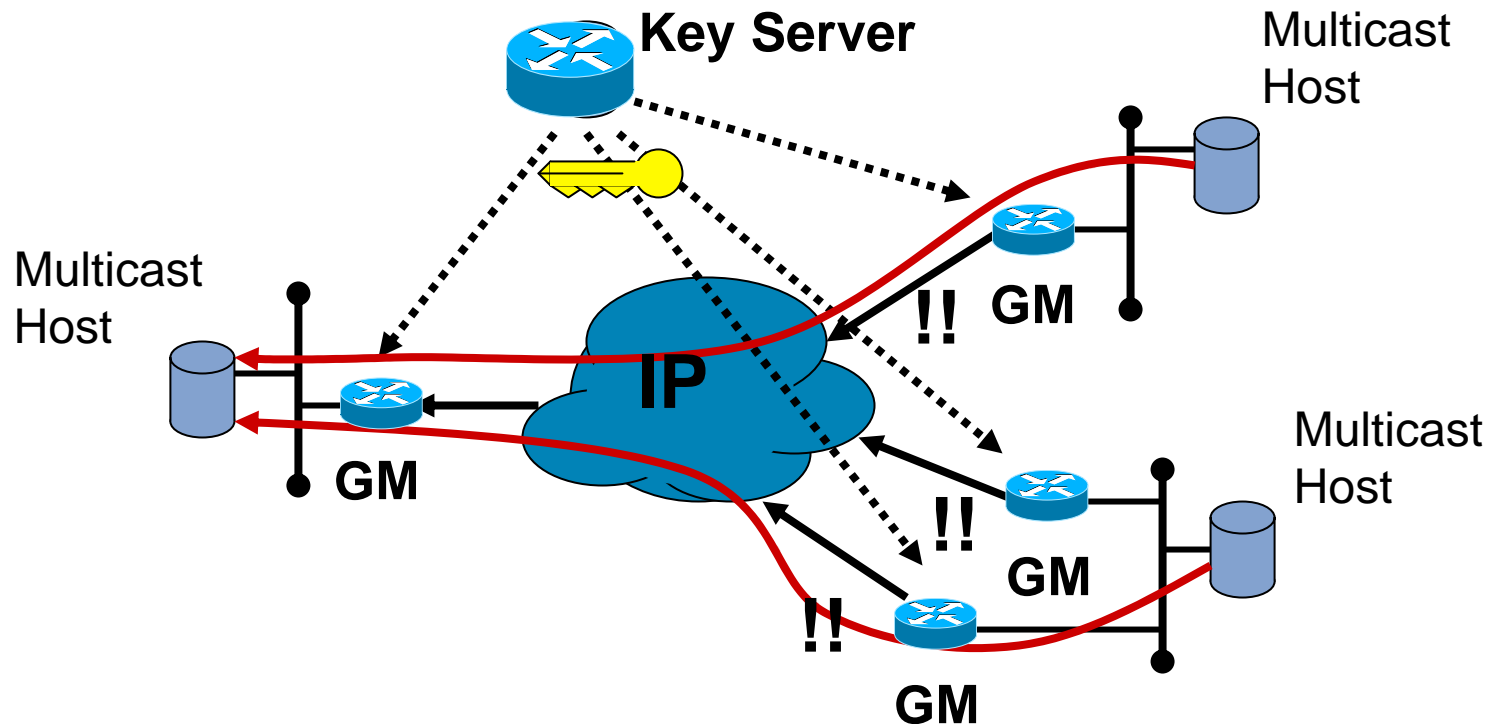
# Secure Multicast

## Data Protection



- Legitimate group members obtain Traffic Encryption Key from key server for the group
- Multicast Sender Encrypts Multicast with IP Address Preservation
- Replication of Multicast packet in the Core based on original (S,G)

# Secure Unicast Data Protection



- Group member assumes that legitimate group members obtain Traffic Encryption Key from key server for the group
- Group members can authenticate the group membership
- Group member Encrypts Unicast with Group SA

# Detailed Feature Overview



# 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**

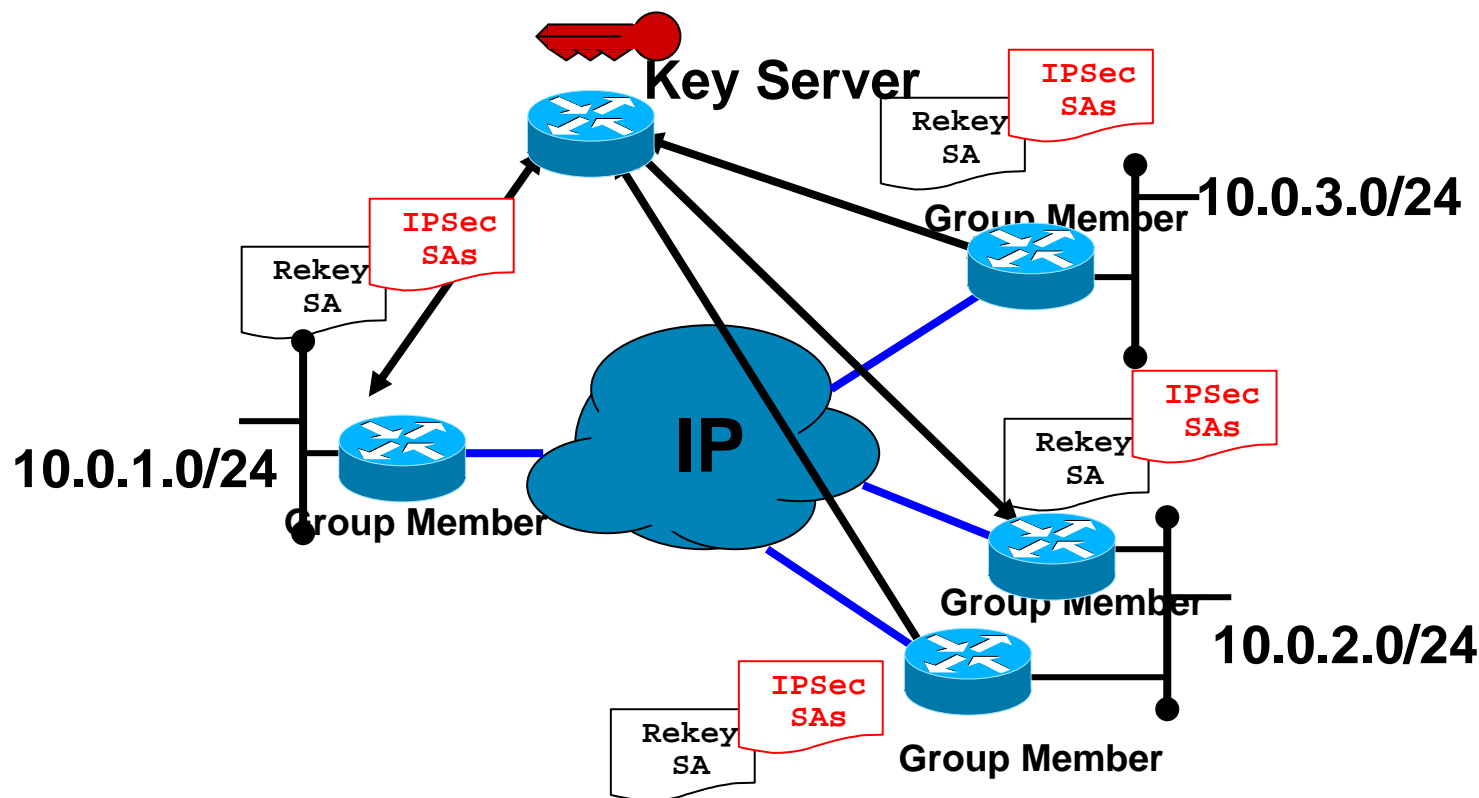
- IPSec Tunnel Mode with IP Address Preservation
- Passive Security Associations for Graceful Roll-out (i.e. Receive Only SA)
- Pseudo-time Synchronous Anti-Replay Protection

- **Enhanced Debugging (fault isolation)**



# GDOI Registration

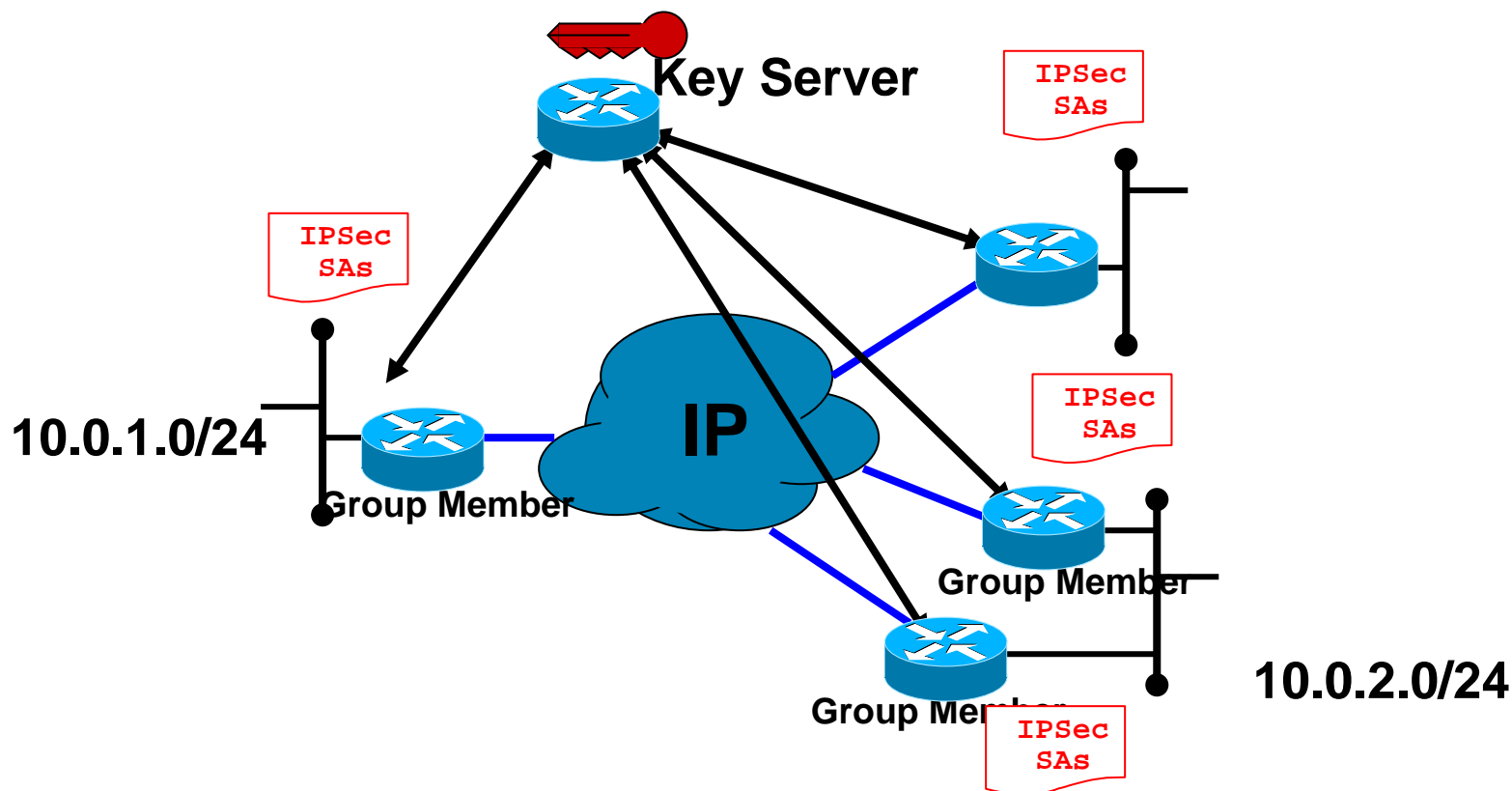
## Key Distribution



- 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

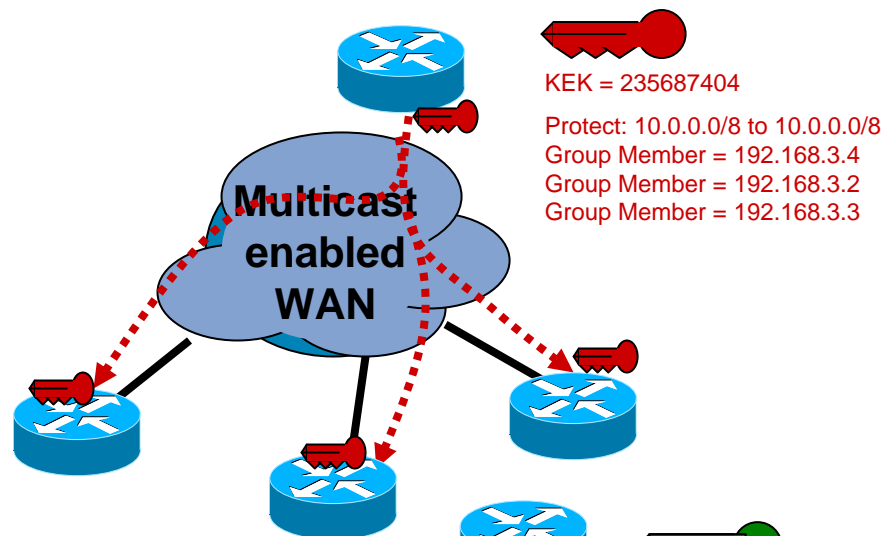


- The key server generates and pushes new IPsec keys and policy to the routers when necessary
- Re-key messages can also cause group members to be ejected from the group

# Multicast / Unicast Key Distribution

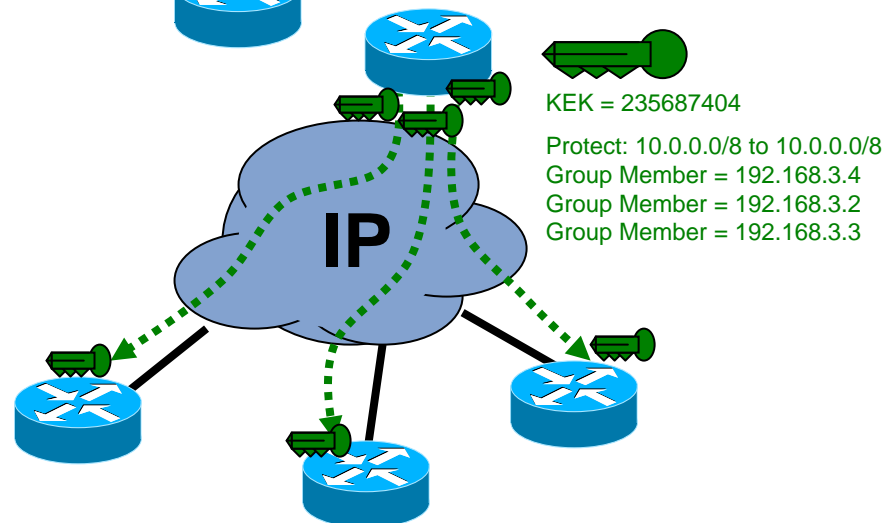
## ■ Multicast Key Distribution over Multicast Enabled Network

- Via Multicast Formatted Key Message and Network Replication
- Fallback to Group Member GDOI Unicast Registration



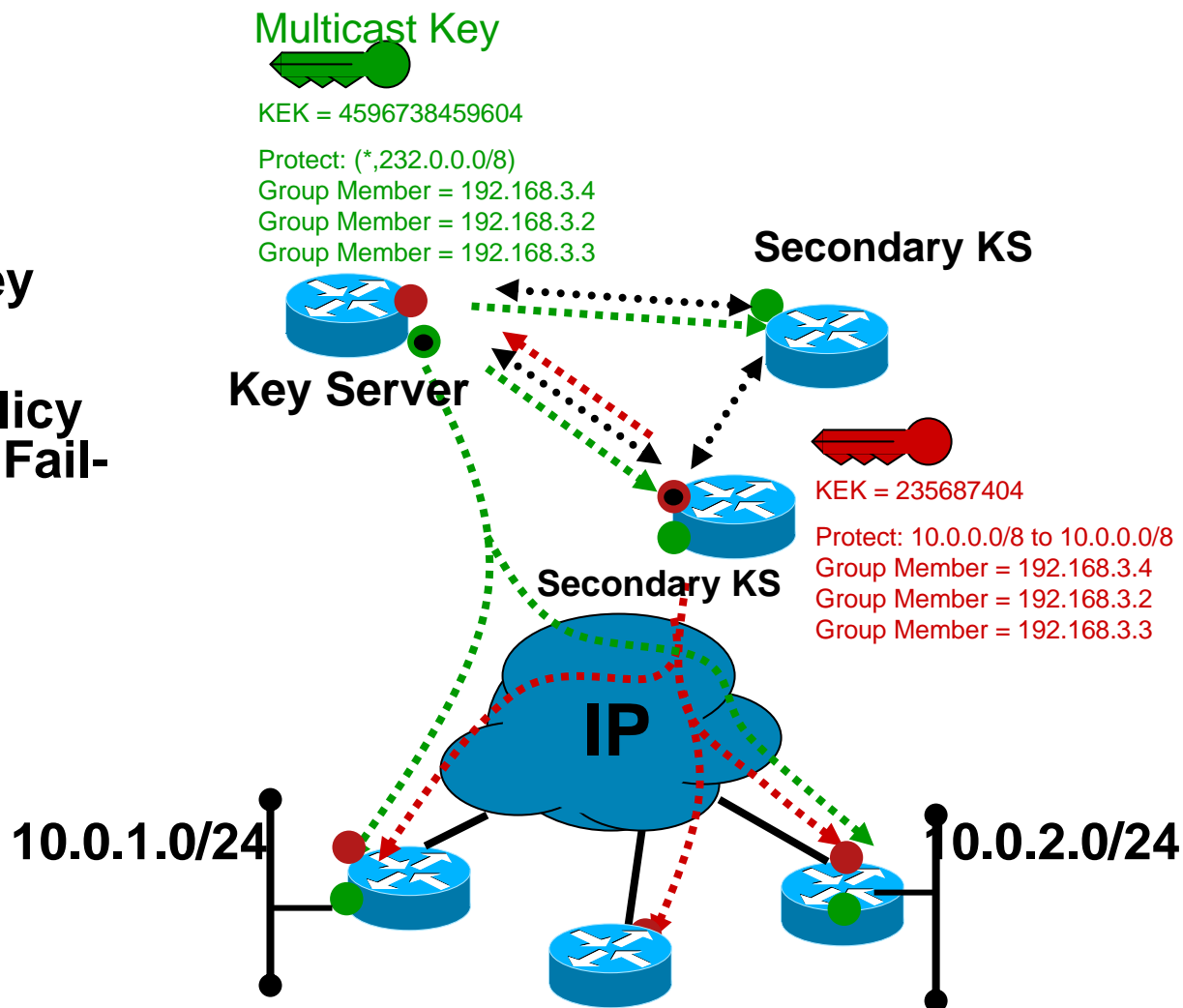
## ■ Unicast Key Distribution over non-Multicast Enabled Network

- Via per-Peer Unicast Formatted Key Message



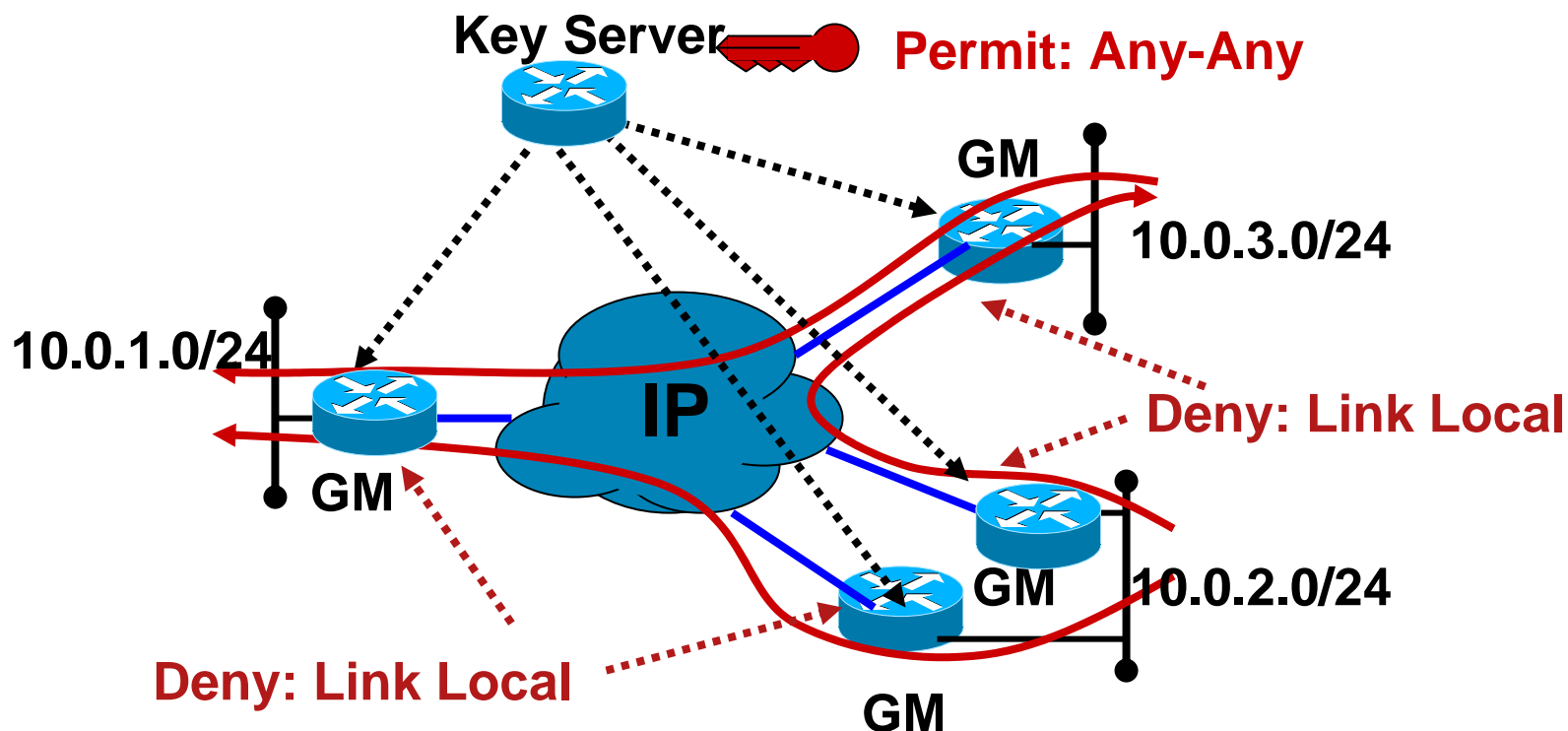
# Cooperative Key Server Key Distribution

- Primary Key Server designated per Group
- Multiple Secondary Key Servers per Group
- Synchronization of Policy Database for Graceful Fail-over



# Policy Management

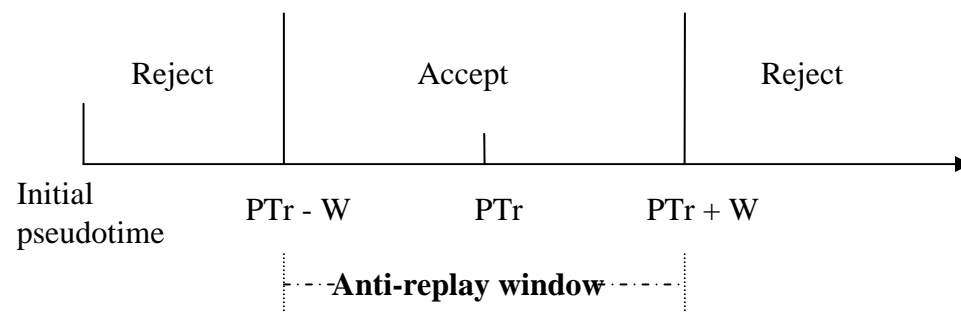
- Local Policy Configured by Group Member
- Global Policy Configured and Distributed by Key Server
- Global Policy Appended to Local Policy



# 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 PseudoTime falls in the below Receiver window, packet accepted else packet is discarded**

# Design Scenarios



# Cisco GET VPN

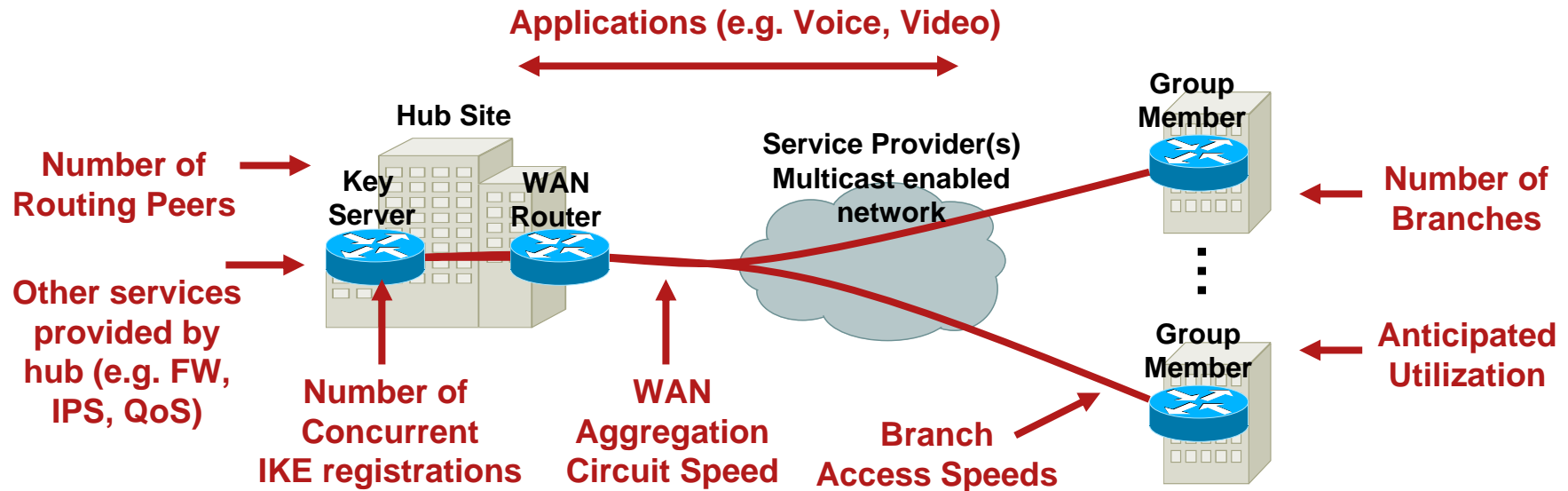
## Critical Design Considerations

- Encryption standard?
  - DES, 3DES, AES
- IKE Authentication type?
  - Pre-shared Keys (PSK), X.509
  - Digital Certificates (PKI)
- Additional Enterprise Security Requirements?
  - Group Authentication
  - User Authentication
- QoS requirements?
  - LLQ, Traffic Shaping, interface level, per-VPN tunnel
- IP Multicast applications?
  - Natively Multicast Encryption
- Any-to-any requirements?
  - Yes, any-to-any traffic
- Addressing of remote routers?
  - Static IP addresses or dynamic
- Scalability?
  - 10's, 100's, or 1000's of branches
- Aggregate bandwidth and throughput requirements?
  - DS3, multi DS3, OC3, OC12, OC48
- Traffic Mix?
  - pps, bps and packet size



# Cisco GET VPN

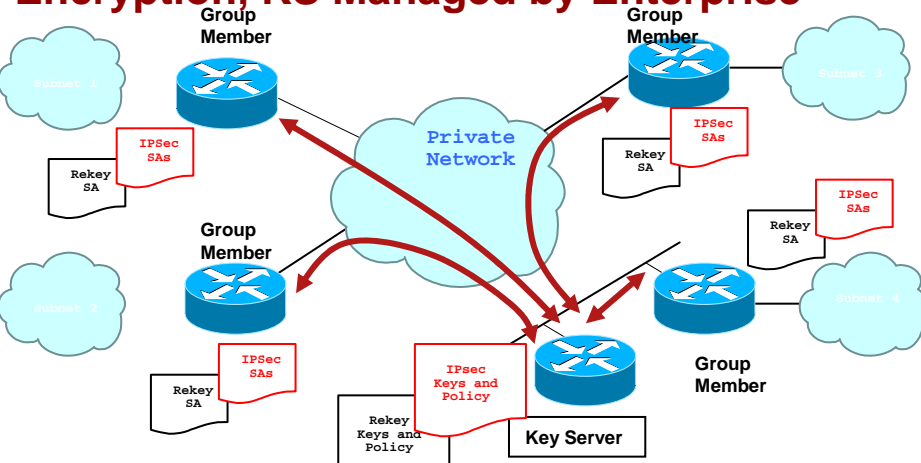
## General Design Considerations



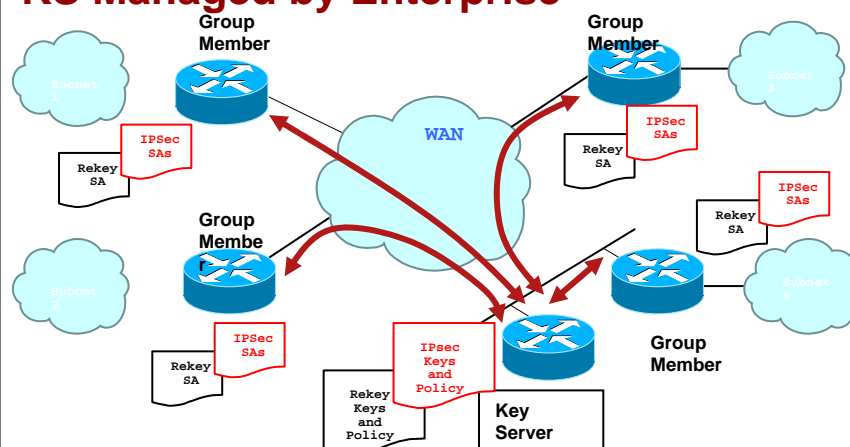
- Proper Addressing is an absolute must to have easier policies
- HW Encryption modules required and recommended
- Routing protocols do not require a tunneling protocol
- "pre-fragmentation" and "ignore the DF bit" should be set on the GET VPN devices
- Summarize Routes

# Group Encrypted Transport in Enterprise/SP WAN Scenarios

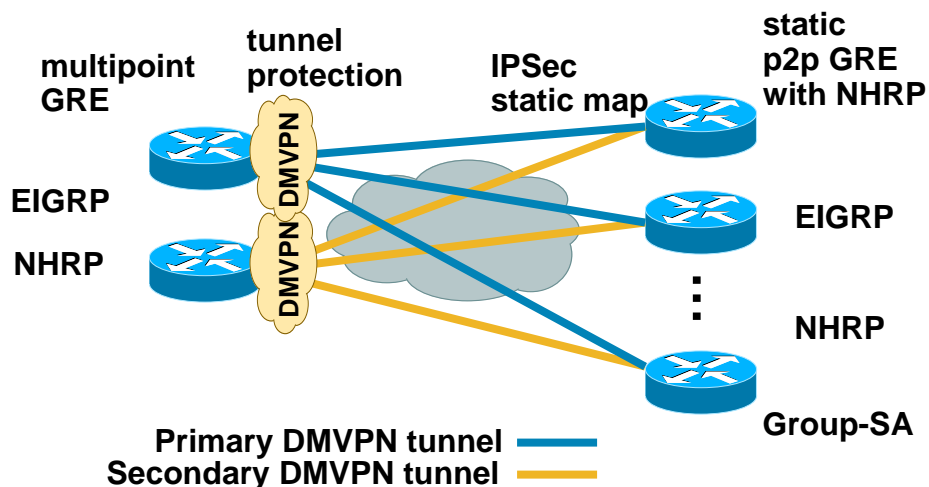
## Enterprise owned CPE, CE-CE with GET Encryption, KS Managed by Enterprise



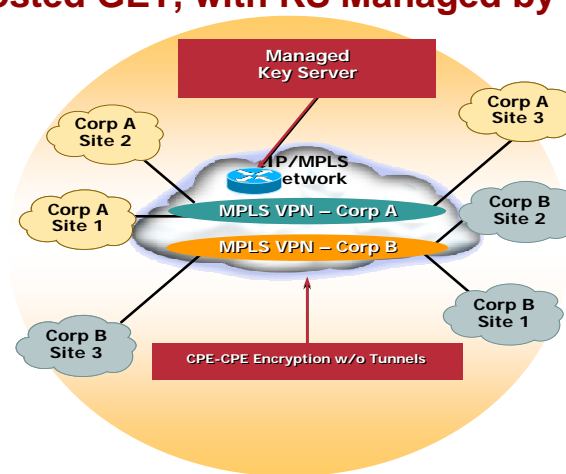
## Managed CPE with GET Encryption, with KS Managed by Enterprise



## DMVPN (mGRE over IPsec) with GET



## Hosted GET, with KS Managed by SP



# Provisioning and Management



# Management of Cisco GET VPN

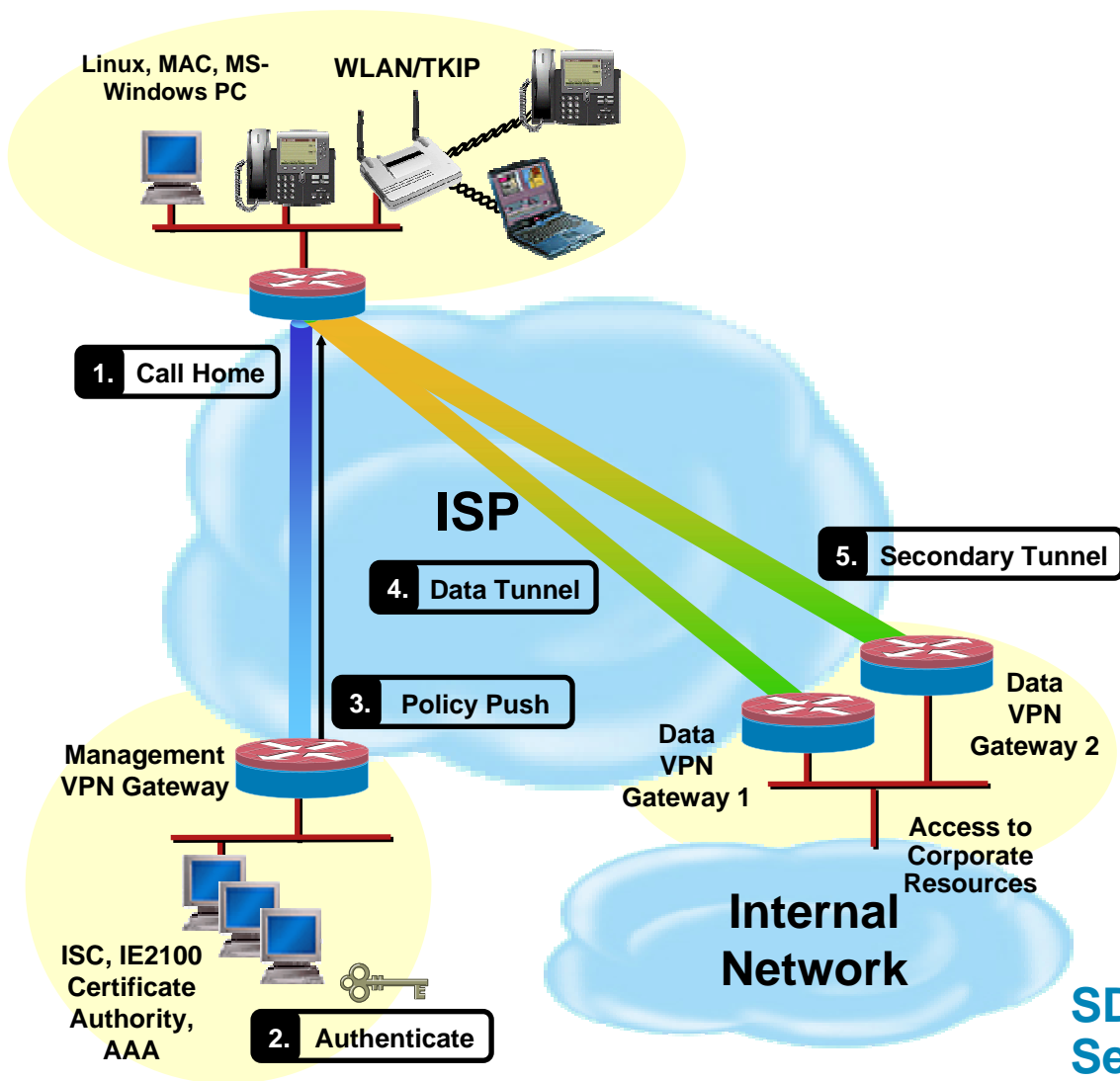
- Centralized Provisioning by pushing keys and policies from Key Server
- Secure Device Provisioning (SDP) available to bootstrap Group Member configurations when using public key infrastructure (PKI)
- SDP support available in both CSM and SDM
- CSM Flex-Config for both Key Server and Group Member--provisioning
- Cisco IOS Command-line interface available for provisioning, monitoring, and troubleshooting
- Cisco IOS NetFlow support for Monitoring of GET VPN traffic
- DMVPN with Group Encrypted Transport can be configured with CSM

# 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

# DMVPN with Group Encrypted Transport

## “Bootstrap” Provisioning of Remote Routers



1. Remote routers “call home” and management tunnel is set up
2. Management server authenticates remote router using certificate authority and AAA servers
3. Management server pushes policy including new certificate
4. Remote router establishes primary tunnel (DMVPN) and access to corporate resources
5. Secondary tunnel (DMPVN) is established and stays active for instant failover
6. Use flex-config on CSM to provision Group members in GET VPN

**SDP:**  
**Secure Device Provisioning**

# Summary

- Enterprise WAN technologies previously forced a trade-off between QoS-enabled branch interconnectivity and security
- Cisco introduces Group Encrypted Transport (GET) VPN, a next-generation WAN security technology:
  - Easy-to-manage, high-scale, any-to-any encrypted communications
  - Secured packets use existing WAN-agnostic routing infrastructure without tunnels
  - Networkwide QoS and Multicast capabilities preserved; improves application performance
  - Offers flexible span of control among subscribers and providers
- GET VPN's group-key mechanism simplifies key management and reduces latency, improving any-to-any connectivity capabilities
- IP header preservation prevents overlay routing

