Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

BRKSEC-3012

Scott Wainner

Cisco Networkers 2007

HOUSEKEEPING

- We value your feedback, don’t forget to complete your online session evaluations after each session and complete the Overall Conference Evaluation which will be available online from Friday.
- Visit the World of Solutions on Level -01!
- Please remember this is a ‘No Smoking’ venue!
- Please switch off your mobile phones!
- Please remember to wear your badge at all times including the Party!
- Do you have a question? Feel free to ask them during the Q&A section or write your question on the Question form given to you and hand it to the Room Monitor when you see them holding up the Q&A sign.

Session Objectives and Pre-requisites

- Session Objectives

  Understand the value of Group Encrypted Transport (GET) enabled VPN services

  Provide a functional description of the GET-enable VPN components

  Demonstrate methods of deployment

  Provide guidance on optimized deployment models

- Pre-requisites

  Network Infrastructure Protection (BRKSEC-2013)

  Multicast Security (RST-2262)

  Advanced Multicast Concepts (RST-3261)

  Advanced Site-to-Site IPSec (BRKSEC-3006)

  IPSec Knowledge (TECSEC-2001)

Agenda

- Motivations for GET-enabled IPVPN
- GET-enabled IPVPN Overview
- GET Deployment Properties
- GET-enabled VPN Reliability
- VPN Network Transitions
- Quality of Service Interoperability
- Multicast Architectural Considerations
- Operational Support

Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

Motivations for GET-enabled IPVPN

IP VPN Security

- Requirements / Goals
  - Single Point Bootstrap Provisioning
  - Network Segmentation
  - Scalable Architecture for Routing
  - Optimal Forwarding Plane
  - Security
- Security Functions
  - Transport Security (Encryption, Authentication, Authorization)
  - Protection (Partitioned, Firewall, Access Controls)
  - Prevention / Detection (Intrusion, Denial of Service)

The Paradox

- IP VPN for …

  Any to Any Connectivity

  Hierachical and Scalable Routing

  Efficient Multicast Distribution

  Segmentation from the Internet

  Simplified QoS Models

- IPSec VPN for …

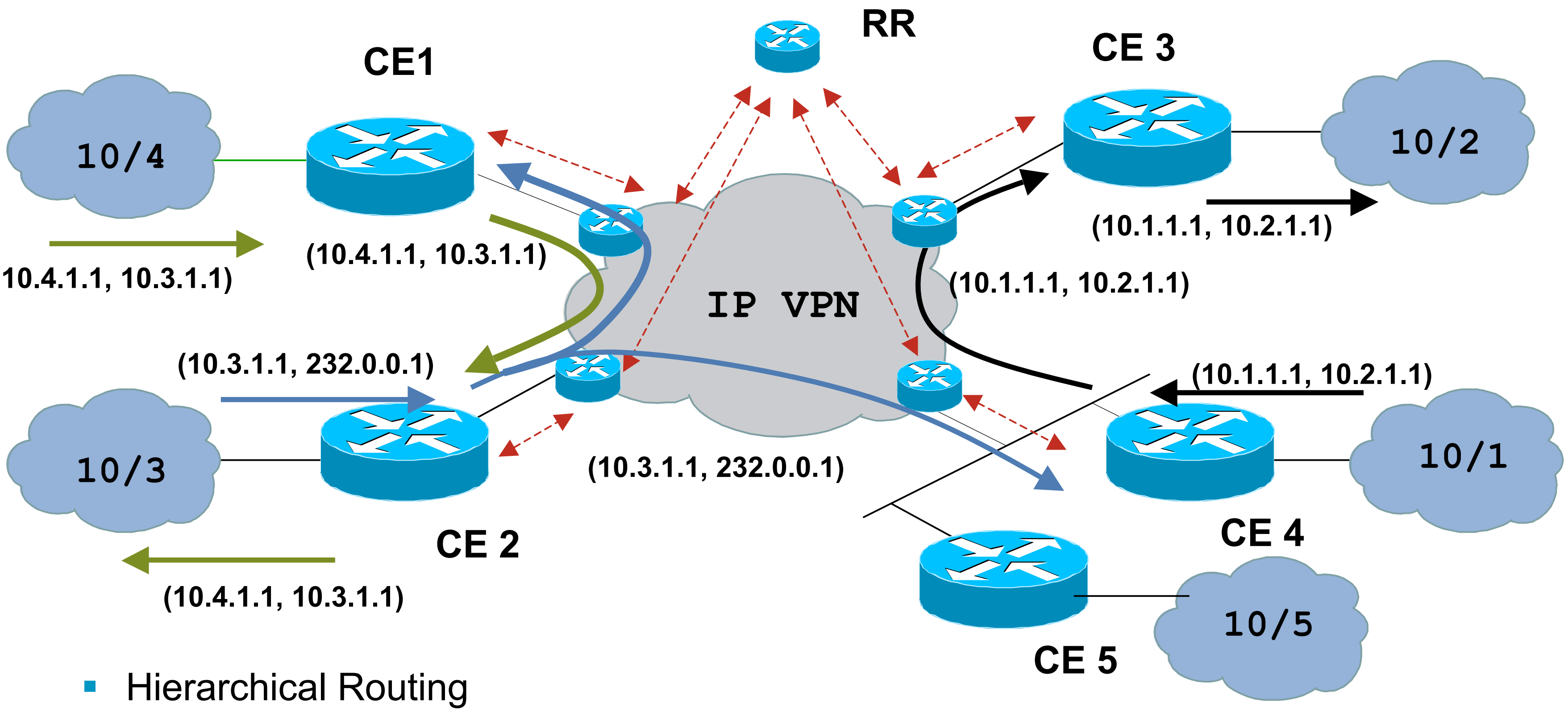
  Confidentiality

  Integrity

  Authentication

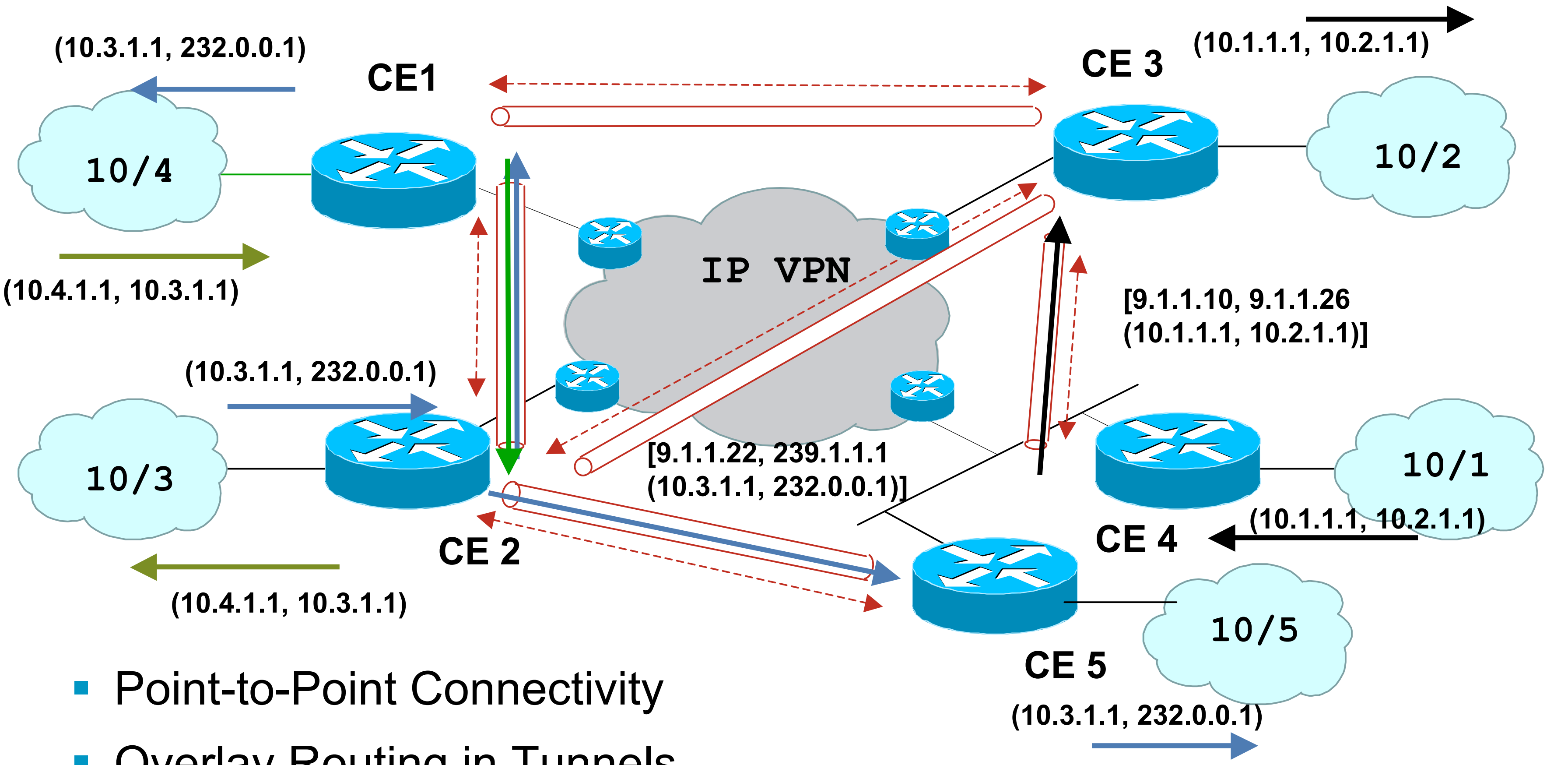
- The technologies are ORTHOGNAL and CONFLICT with each other

IP VPN Attributes



- Hierarchical Routing
- Any-to-Any Connectivity
- Redundancy Established by IP VPN PE and P
- IP VPN PE and P Replication

IPsec Attributes



- Point-to-Point Connectivity
- Overlay Routing in Tunnels
- Redundancy Established by CE
- Multicast Replication Induced at CE

Network Paradigm Assessment

- IP VPN (e.g. MPLS VPN)
  - ▲ Any-to-any connectivity without CE-CE Tunnel Adjacency
  - ▲ Single Point Provisioning on per CE basis
  - ▲ Distributed or Hierarchical Routing for Scalability
  - ▲ Optimal traffic forwarding
  - ▶ Security
    - ▼ Confidentiality (segmentation only)
    - ▲ Segmentation
    - ▼ Integrity
- IPsec
  - ▼ Scalability Constraints of Point-to-Point Tunnel Adjacency
  - ▼ Per Peer Provisioning
  - ▼ Scalability Constraints of Point-to-Point Overlay Routing or Route Insertion
  - ▼ Traffic forwarding according to non-optimal Tunnel overlay
  - ▲ Security
    - ▲ Segmentation
    - ▲ Confidentiality
    - ▲ Integrity

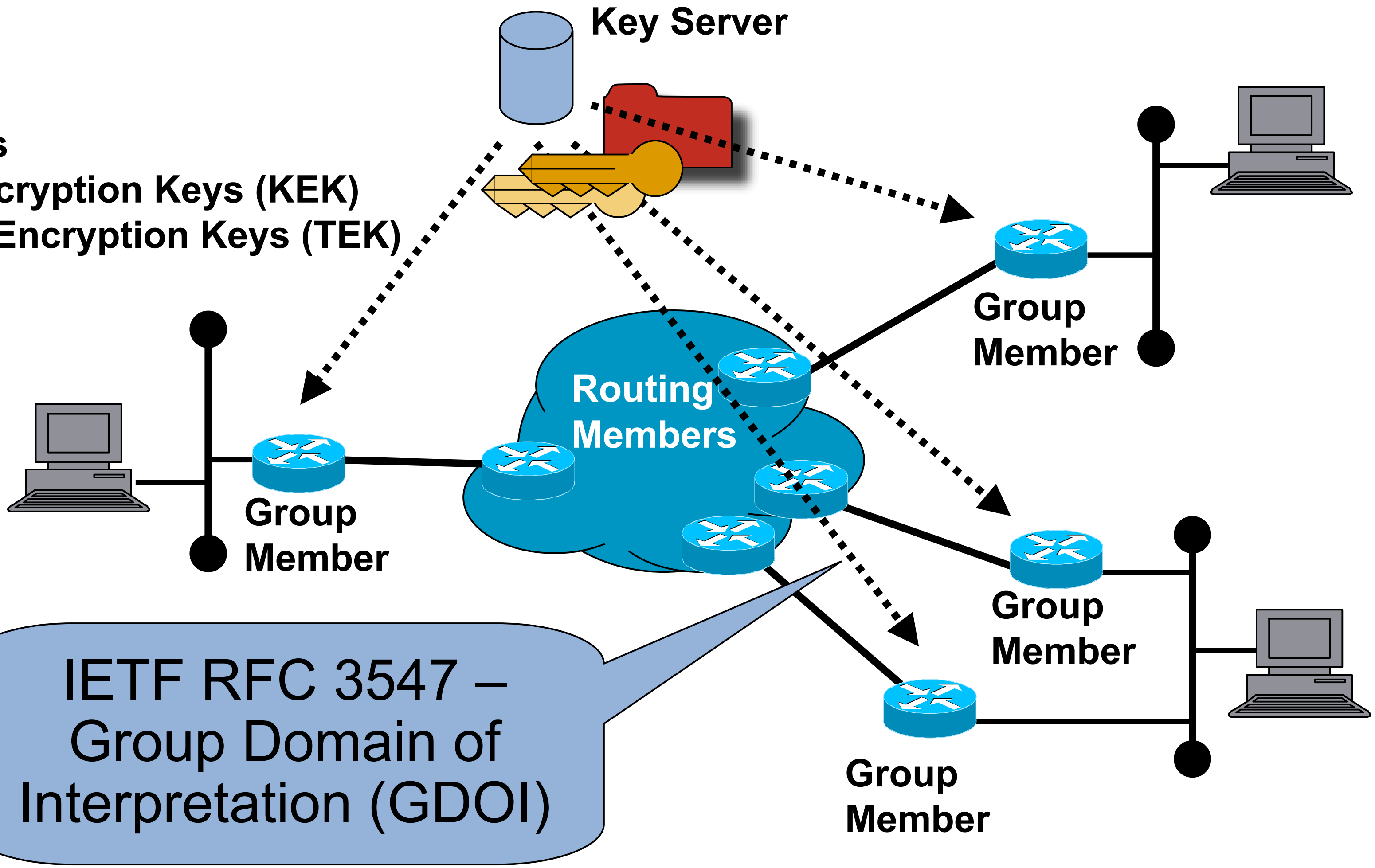
Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

GET-enabled IPVPN Overview

Group Security Elements

- Key Server(s)
    - Validation of Group Members
    - Manager of the Group Security Policies
    - Creation of Group Keys
    - Distribution of Group Policies and Keys
- Group Members
    - Encryption Devices
    - Routing Between Protected and Unprotected Network Regions
    - Multicast Participation
- Routing Members
    - Forwarding / Replicating Encrypted Traffic between Group Members
    - Forwarding Unencrypted Traffic To GM's and From GM's

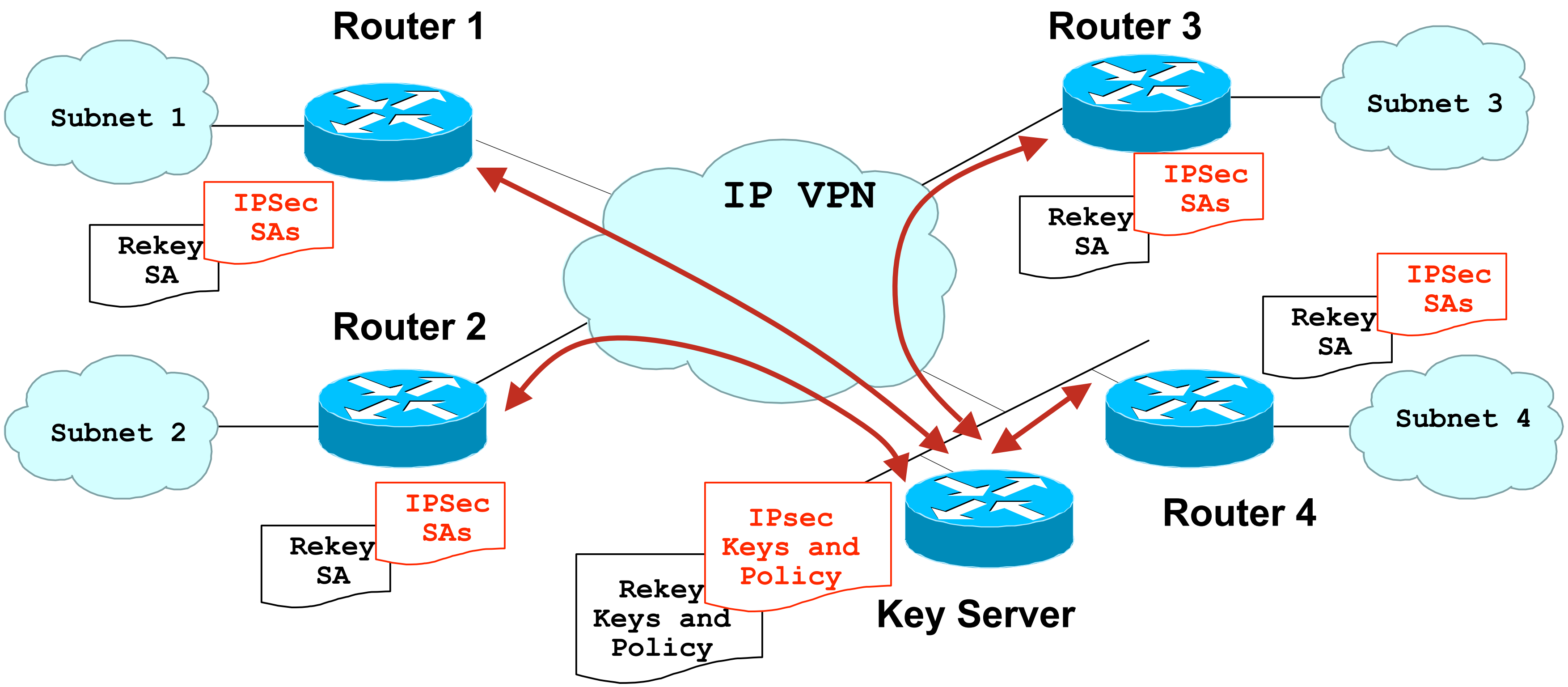
Group Security Elements



- Policies
- Key Encryption Keys (KEK)
- Traffic Encryption Keys (TEK)

IETF RFC 3547 – Group Domain of Interpretation (GDOI)

GDOI Registration



- 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

Group Security Association

- Group Members share a security association
  - Security association is not to a specific group member
  - Security association is with a set of group members
- Safe when VPN gateways are working together to protect the same traffic
  - The VPN gateways are trusted in the same way
  - Traffic can flow between any of the VPN gateways

Group Security Concepts

- Multicast Principle

  IETF MSEC WG defined a means of encrypting multicast traffic from a source to any receiver and from multiple sources to multiple receivers

  The source does not know the set of potential receivers; therefore, the source must assume that the receiver has the appropriate key

  A presumption was made that unicast would be handled by classic IPsec encryption methods

  But what about PIM-SM with Rendezvous Points?

- Unicast Corollary

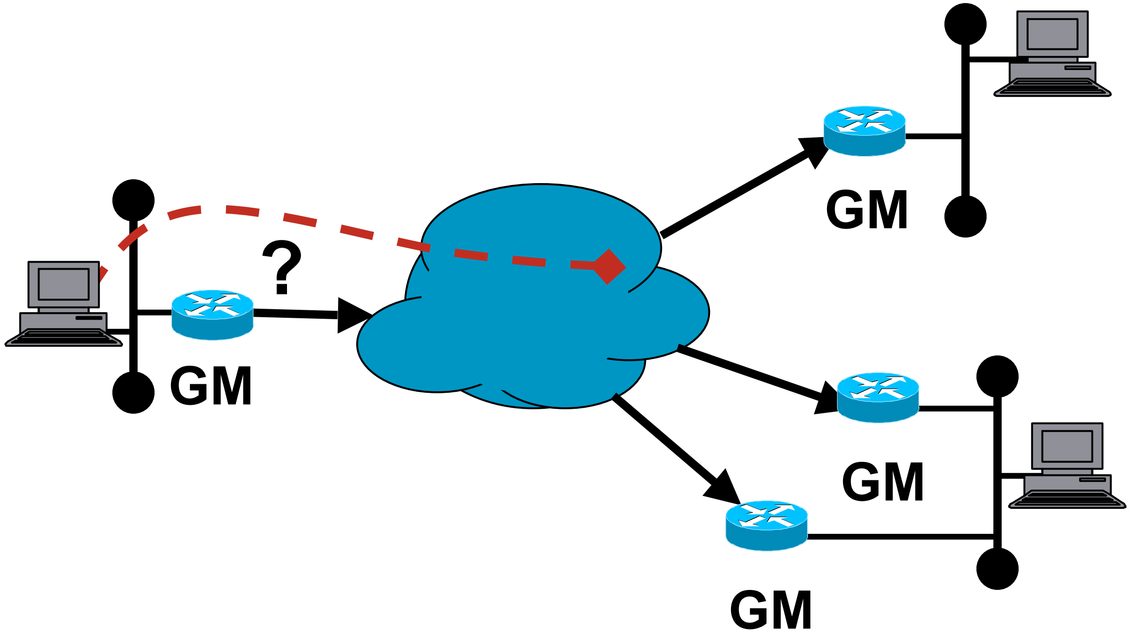
  Applying group keys to unicast data flows

  Why does the security association have to be point to point?

Data Protection
Secure
Multicast

Secure Data Plane Multicast

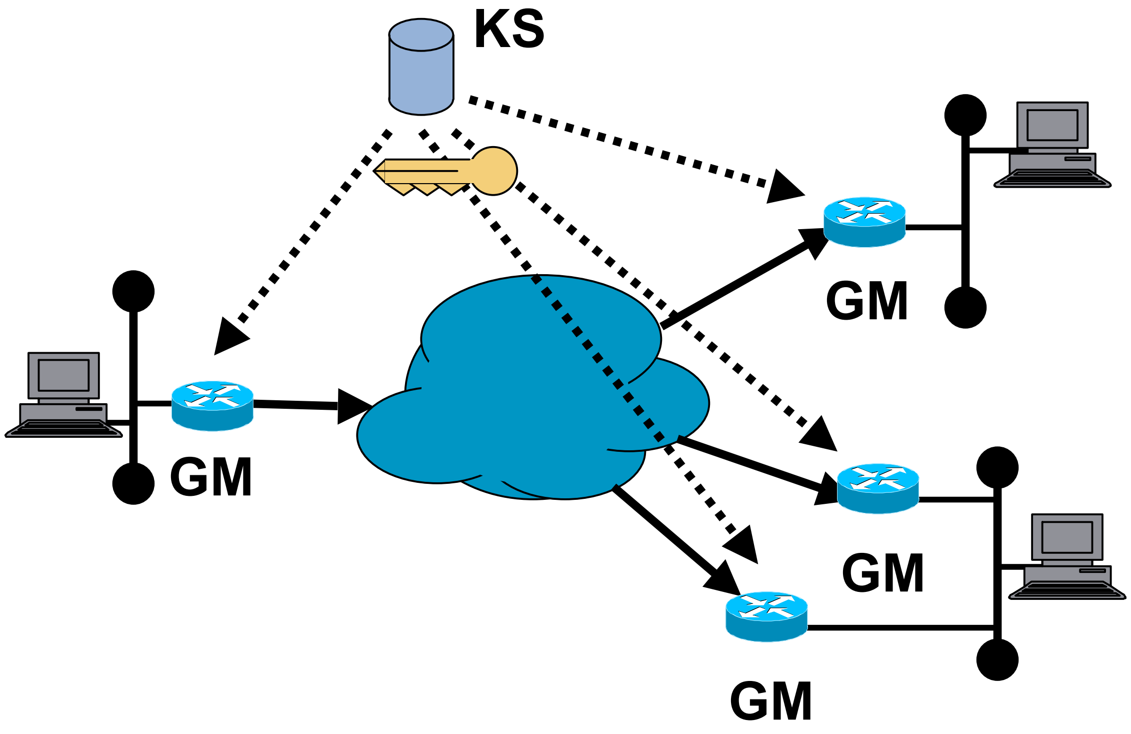
- Premise: Sender does not know the potential recipients



Data Protection
Secure
Multicast

Secure Data Plane Multicast

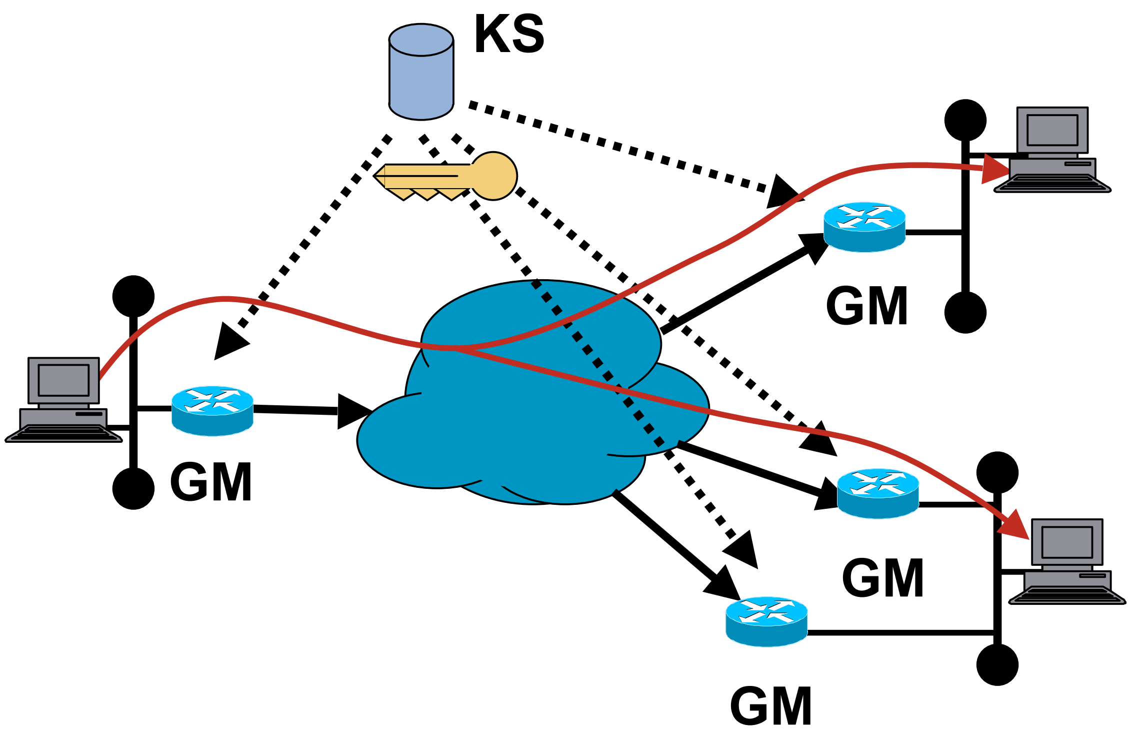
- Premise: Sender does not know the potential recipients
- Sender assumes that legitimate group members obtain Traffic Encryption Key from key server for the group



Data Protection
Secure
Multicast

Secure Data Plane Multicast

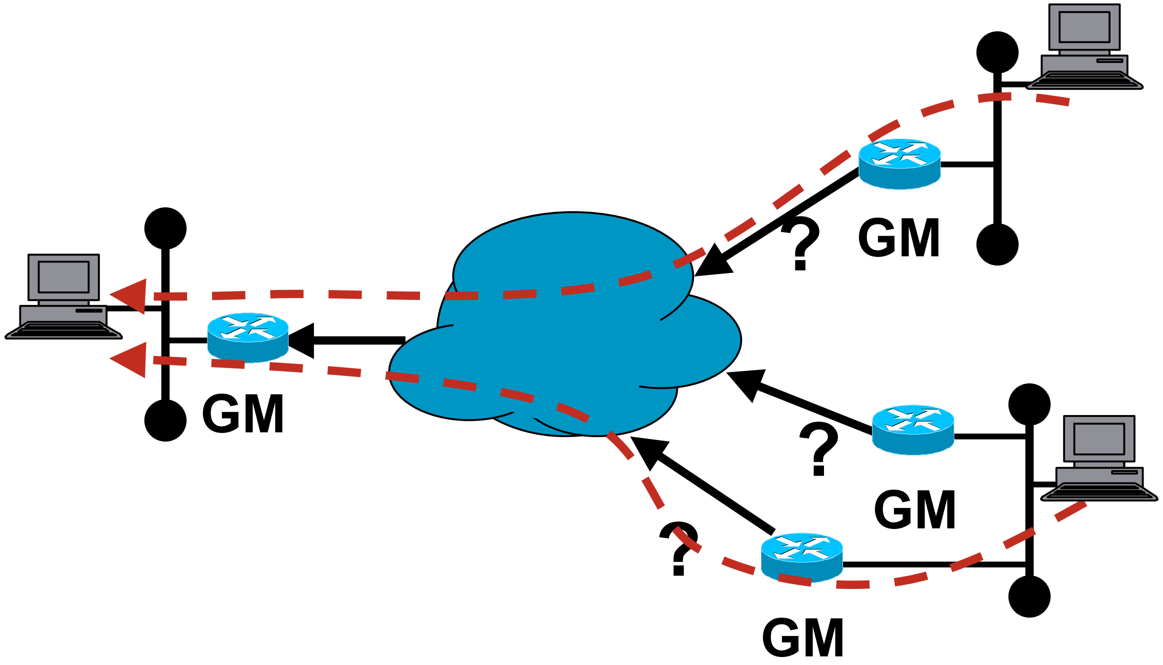
- Premise: Sender does not know the potential recipients
- Sender assumes that legitimate group members obtain Traffic Encryption Key from key server for the group
- Encrypt Multicast with IP Address Preservation
- Replication In the Core based on original (S,G)



Data Protection
Secure
Unicast

Secure Data Plane Unicast Corollary

- Premise: Receiver does not know the potential encryption sources

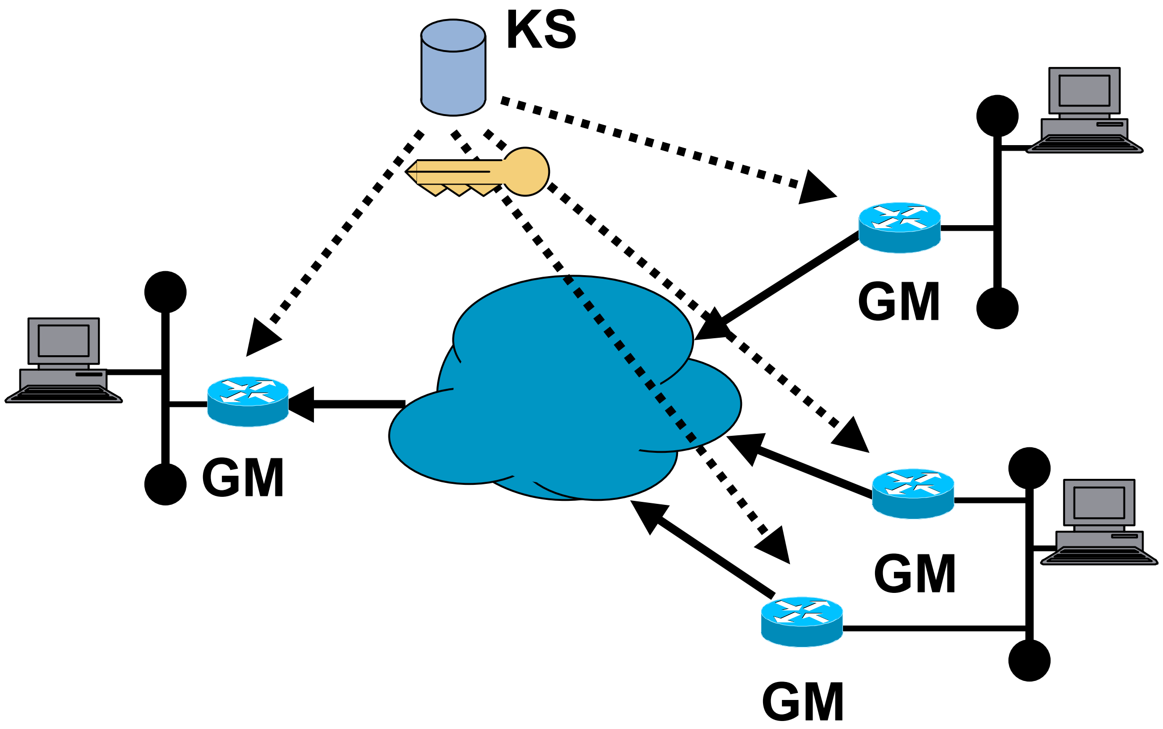


Secure Data Plane Unicast Corollary

Data Protection
Secure Unicast

- Premise: Receiver does not know the potential encryption sources

- Receiver assumes that legitimate group members obtain Traffic Encryption Key from key server for the group



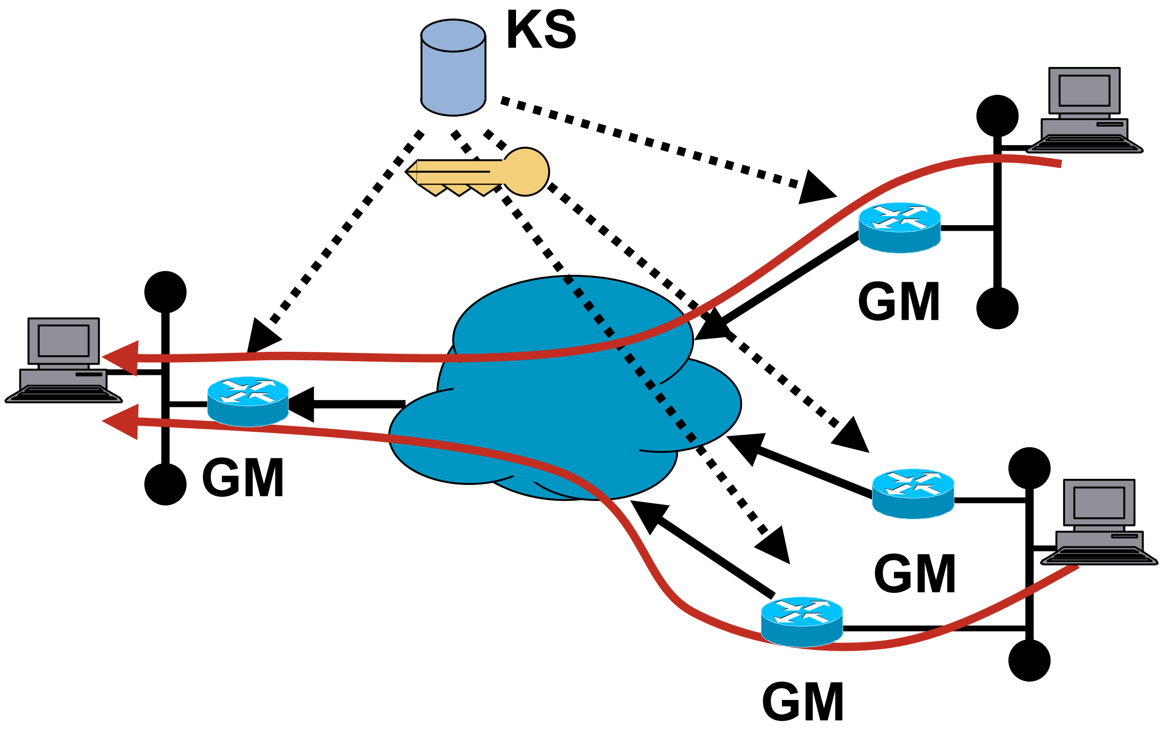
Data Protection
Secure
Unicast

Secure Data Plane Unicast Corollary

- Premise: Receiver does not know the potential encryption sources

- Receiver assumes that legitimate group members obtain Traffic Encryption Key from key server for the group

- Receiver can authenticate the group membership



Group Security Methods

- Group Affinity Security

  Group Association on Group Member

  Group Association on Key Server

  Group Membership Authentication

- Group Authorization

  KS Authorized Encryption

  KS Authorized Encryption Exceptions

  GM Authorized Encryption Exceptions

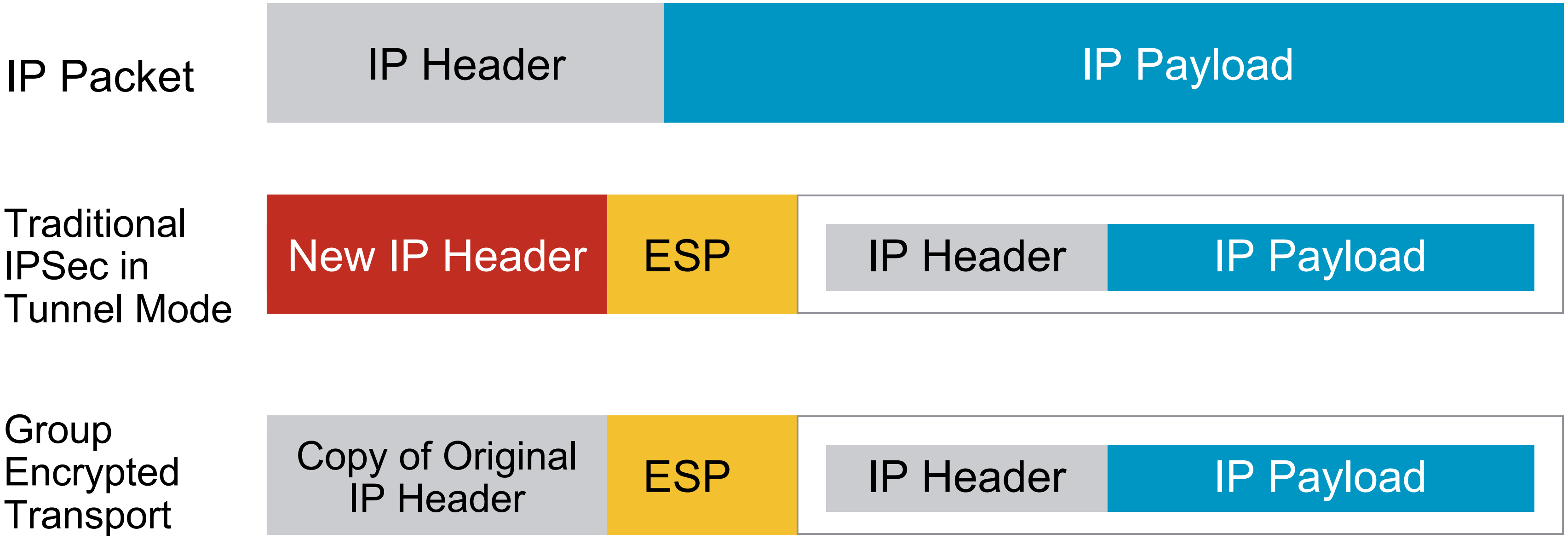
- Encryption Methods

  IPsec Tunnel Mode with IP Header Preservation

  Anti-Replay

  Strict vs Loose Modes

IPSec Tunnel Mode with IP Address Preservation



IP Packet

IP Header | IP Payload

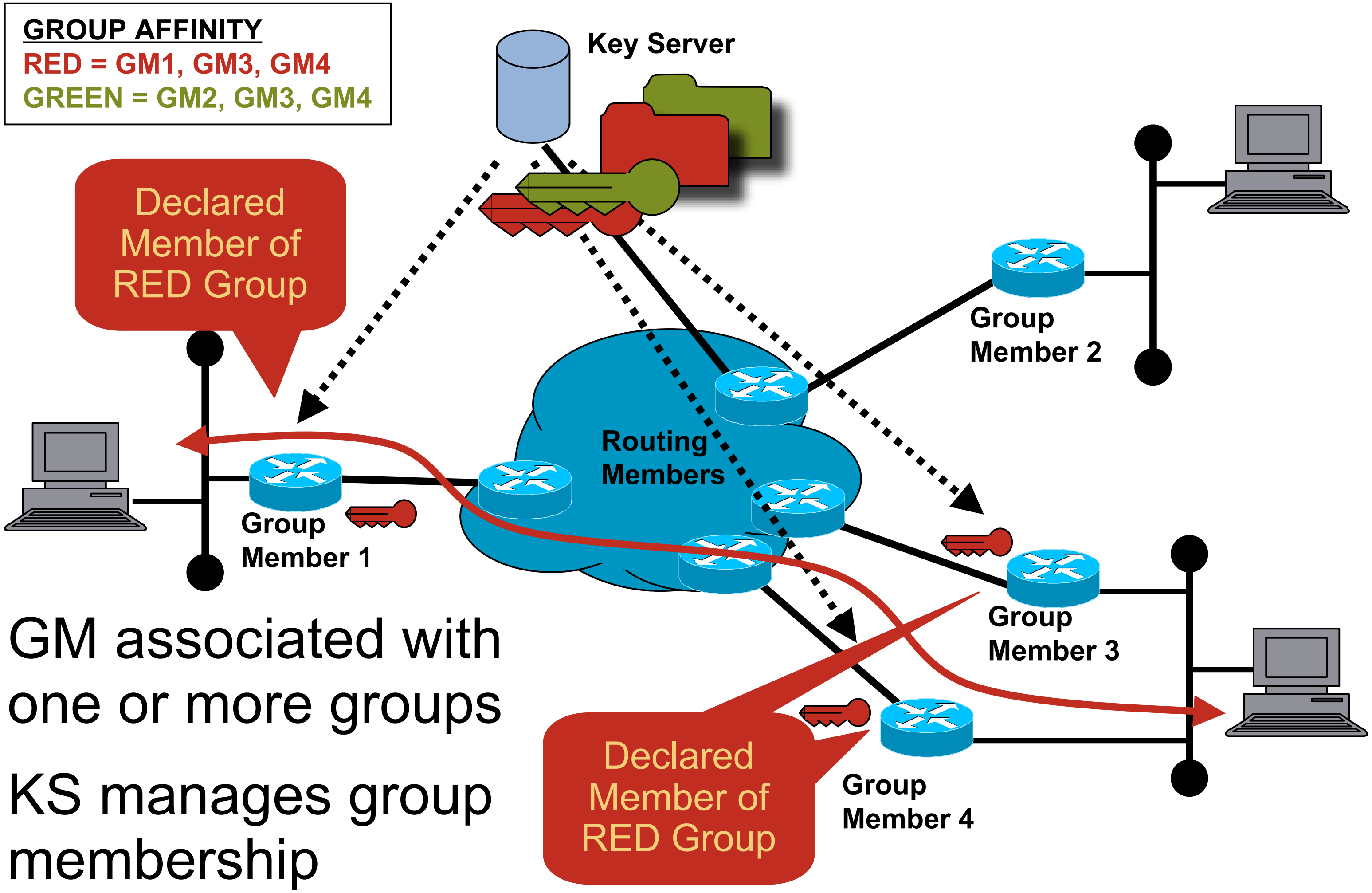
Traditional IPSec in Tunnel Mode

New IP Header | ESP | IP Header | IP Payload

Group Encrypted Transport

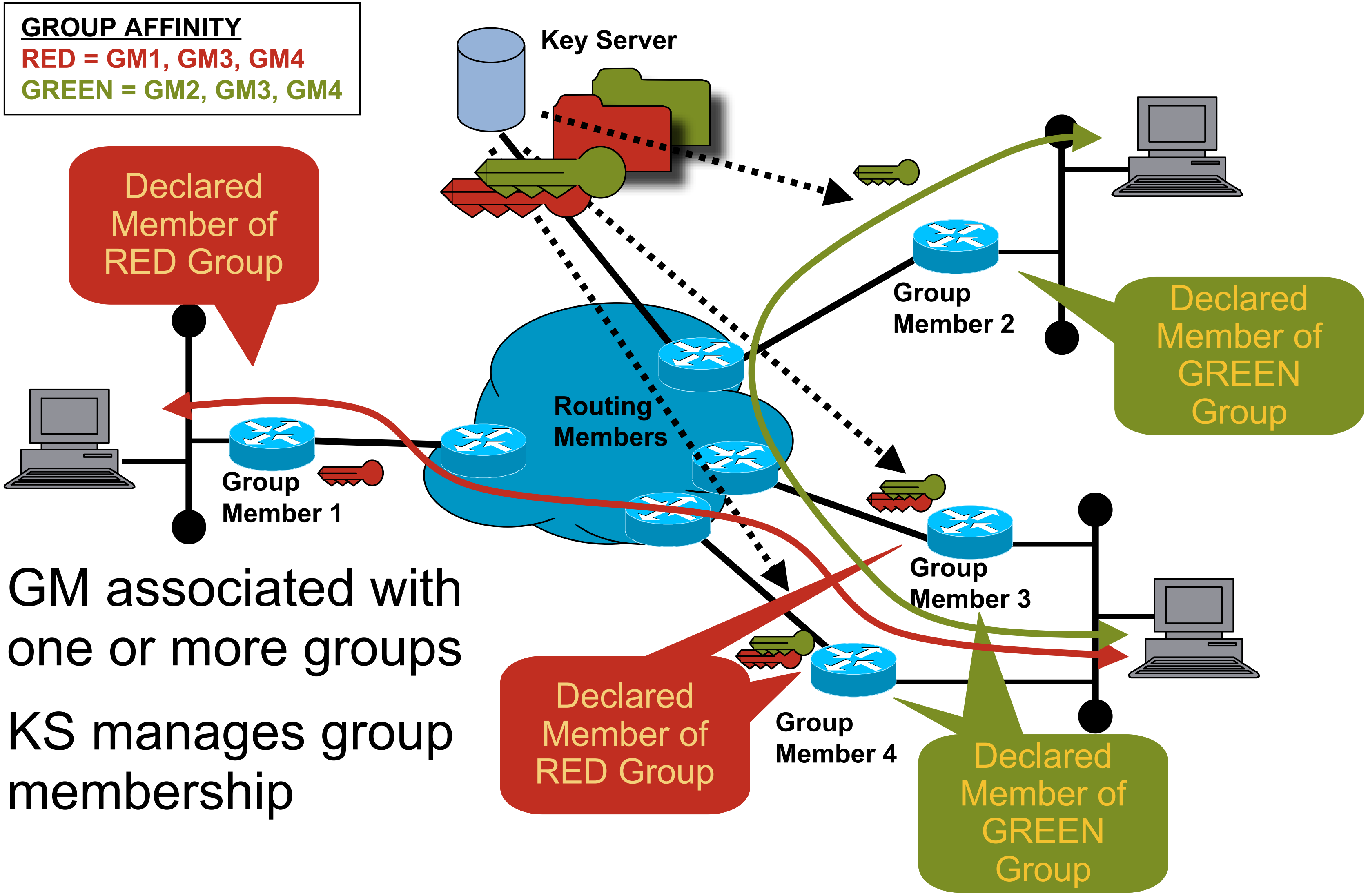
Copy of Original IP Header | ESP | IP Header | IP Payload

Group Affinity (RED Affinity)



- GM associated with one or more groups
- KS manages group membership

Group Affinity (GREEN Affinity)

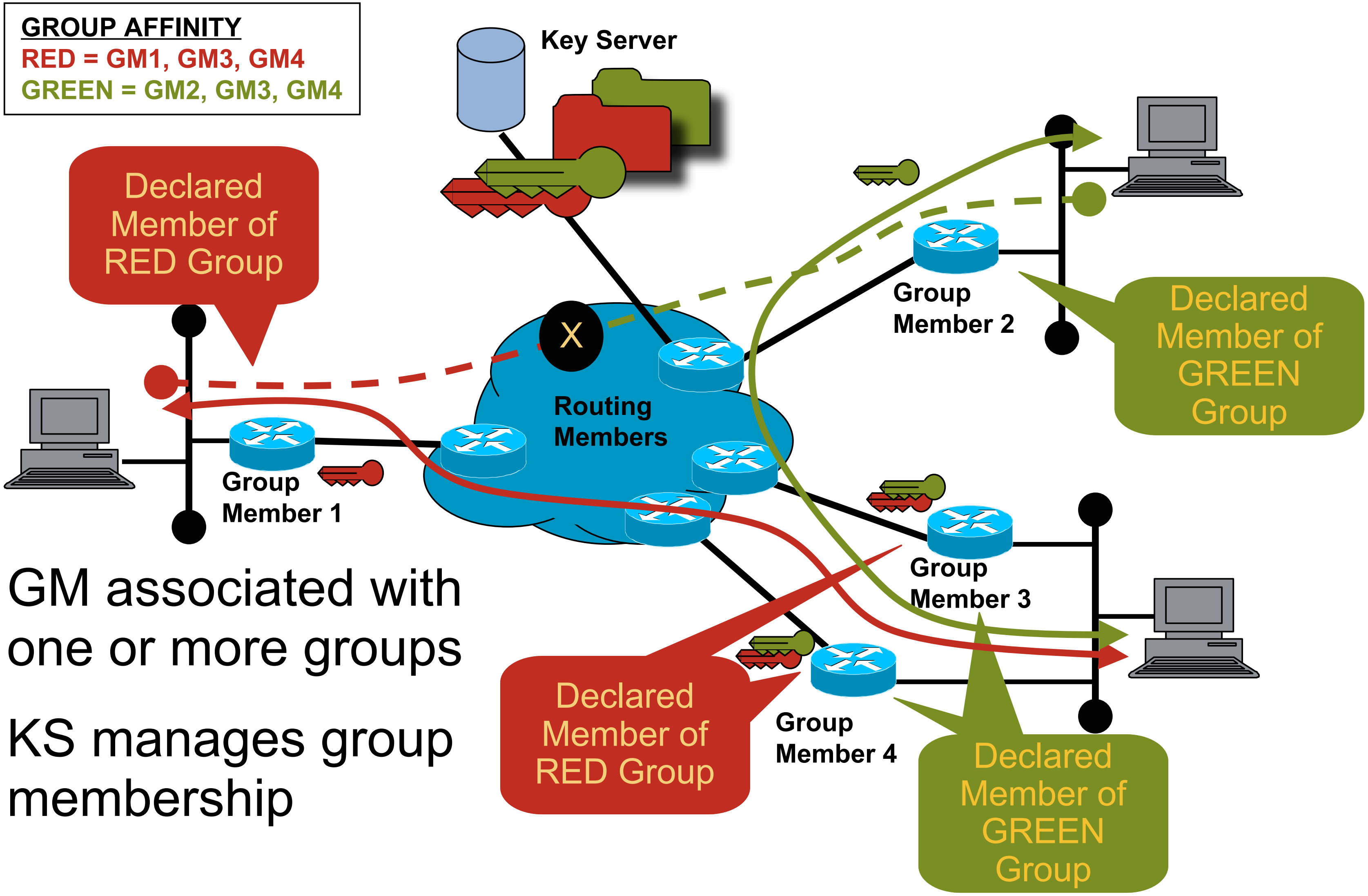


GROUP AFFINITY
RED = GM1, GM3, GM4
GREEN = GM2, GM3, GM4

Key Server
Declared Member of RED Group
Routing Members
Group Member 1
Group Member 2
Declared Member of GREEN Group
Group Member 3
Group Member 4
Declared Member of RED Group
Declared Member of GREEN Group

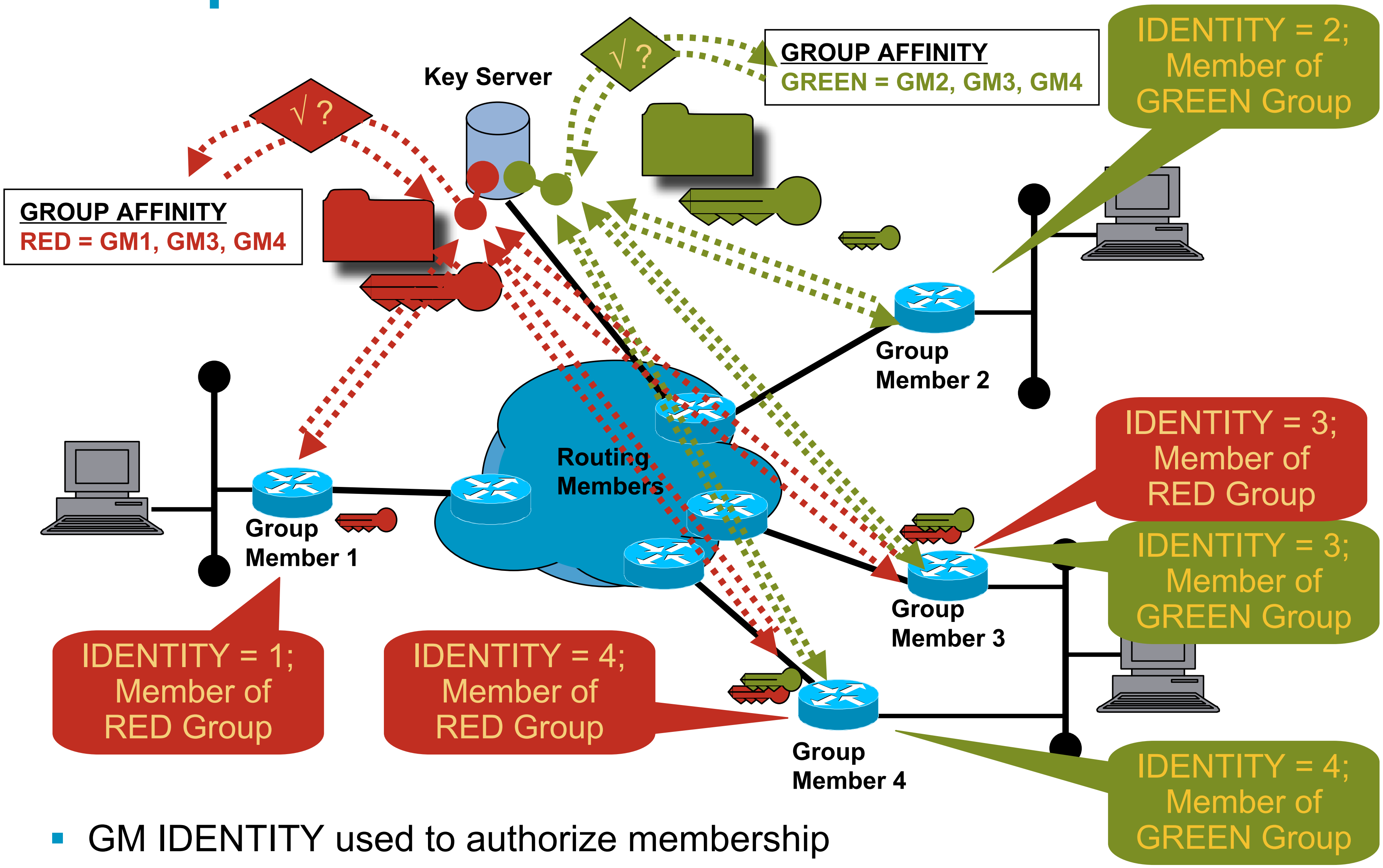
- GM associated with one or more groups
- KS manages group membership

Group Affinity (Mutually Exclusive)



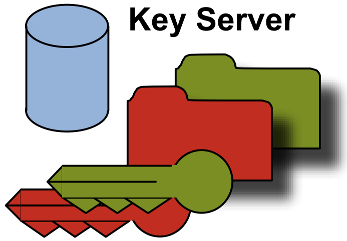
- GM associated with one or more groups
- KS manages group membership

Group Authorization


Key Server
√ ?
√ ?
GROUP AFFINITY
RED = GM1, GM3, GM4
GROUP AFFINITY
GREEN = GM2, GM3, GM4
IDENTITY = 2; Member of GREEN Group
Group Member 2
Routing Members
Group Member 1
IDENTITY = 3; Member of RED Group
IDENTITY = 3; Member of GREEN Group
Group Member 3
IDENTITY = 1; Member of RED Group
IDENTITY = 4; Member of RED Group
Group Member 4
IDENTITY = 4; Member of GREEN Group

- GM IDENTITY used to authorize membership

Encryption Methods



- Key Server maintains policy and encryption attributes per group

- IPsec Attributes
    - IPsec Tunnel Mode w/Header Preservation
    - Receive-Only
    - 3DES
- Policy
    - ‘permit ip 10/8 10/8’

- IPsec Attributes
    - IPsec Tunnel Mode w/Header Preservation
    - Anti-Replay
    - AES
- Policy
    - ‘permit ip 10/8 232/8’

Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

GET Deployment Properties

Group Policy Considerations

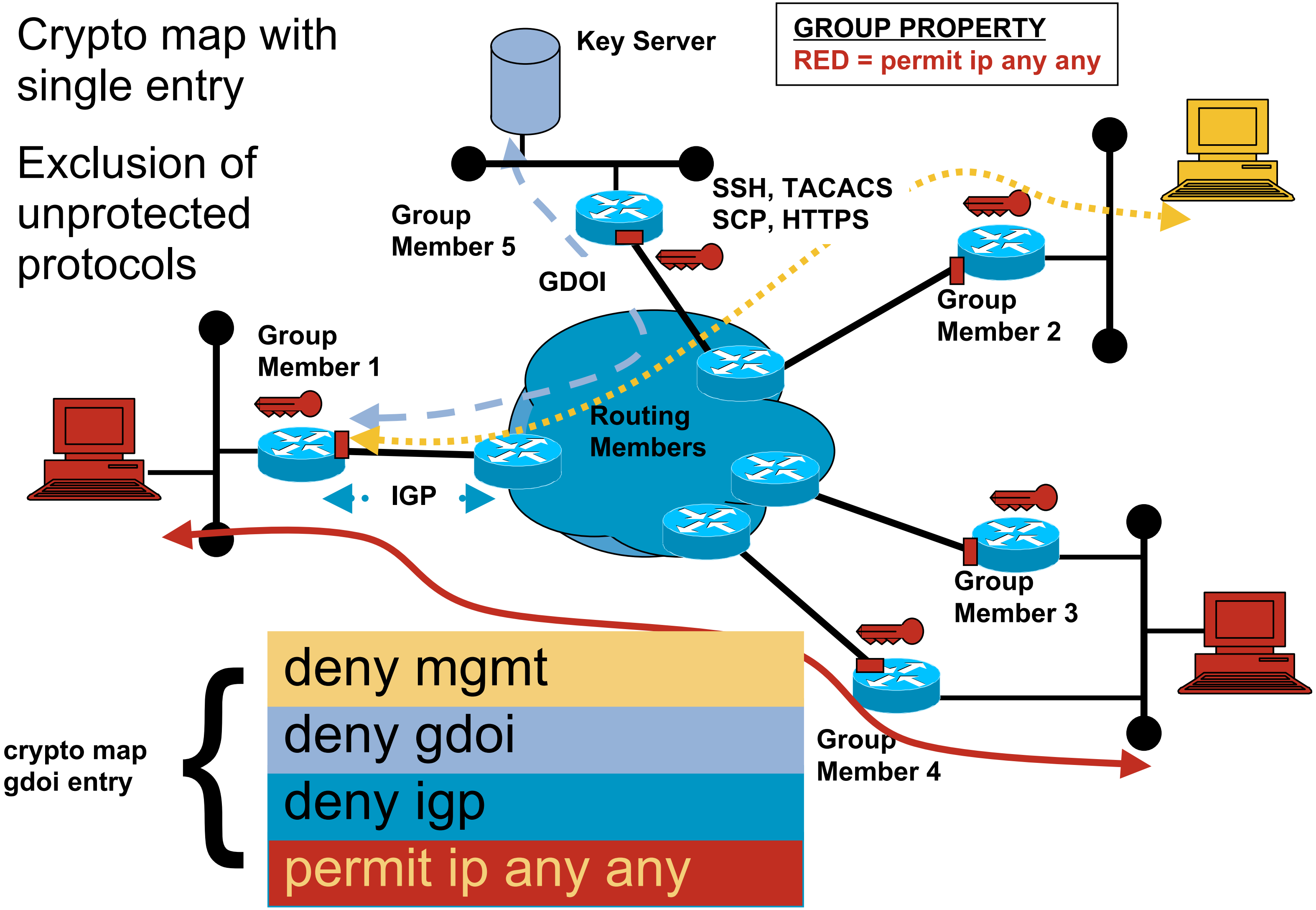
- What may already be protected?
  - Management Plane
    - Internet Key Exchange / Group Domain of Interpretation
    - SSH, TACACS, HTTPS
- What should not be protected with Group Security?
  - Control Plane
    - Routing Exchanges (OSPF, BGP)
- What needs to be protected with Group Security?
  - Data Plane
    - Enterprise Transactions
    - Enterprise Multicast Streams
- What may be protected with Group Security?
  - Data Plane
    - Internet Transactions
    - Diagnostics (LAN-LAN vs. WAN-WAN vs. WAN-LAN)

Group Policy Protection

- Scope of Data Plane Protection – What class of traffic needs protection?
  - Unicast from LANs Only
  - Multicast from LANs Only
  - Unicast and Multicast from LANs
  - All Traffic
- Scope Exclusion – What should not be encrypted?
  - Control Plane
    - Routing Control Plane (IGP, PIM)
    - Crypto Control Plane (GDOI)

Group Policy Considerations

- Crypto map with single entry
- Exclusion of unprotected protocols



deny mgmt

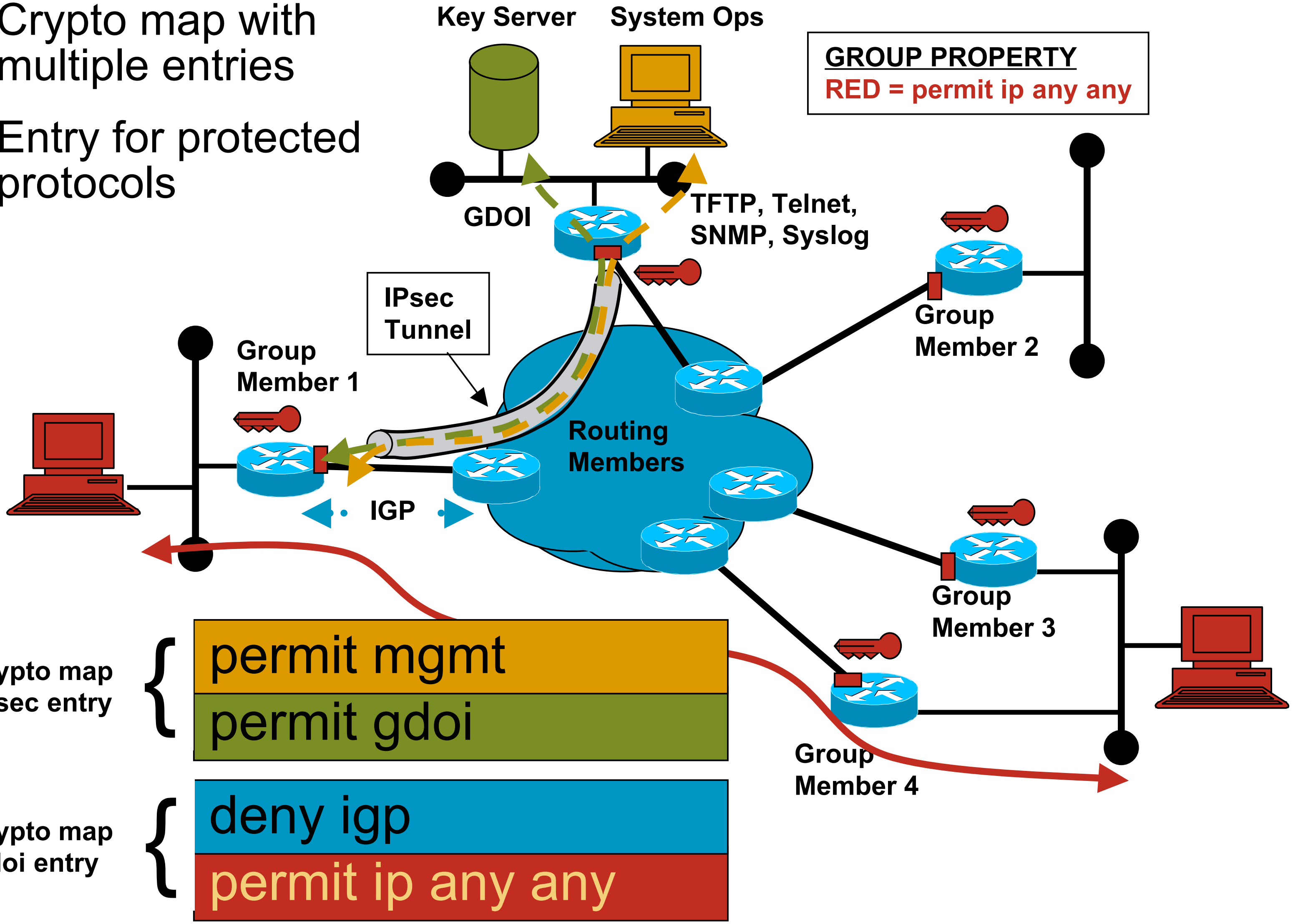
deny gdoi

deny igp

permit ip any any

Group Policy Considerations

- Crypto map with multiple entries
- Entry for protected protocols



crypto map IPsec entry {
- permit mgmt
- permit gdoi

crypto map gdoi entry {
- deny igp
- permit ip any any

Group Policy Distribution

- Group Keys
  - Key Encryption Keys (Default Lifetime of 24 hours)
  - Traffic Encryption Keys (Default Lifetime of 1 hour)
- Key Distribution
  - Unicast
    - Infrastructure Capable of Unicast Only
    - Requirement for Rekey Acknowledgement
    - Time Required for Serialized Key and Policy Distribution
  - Multicast
    - Infrastructure Capable of Multicast
    - Quick Key and Policy Distribution

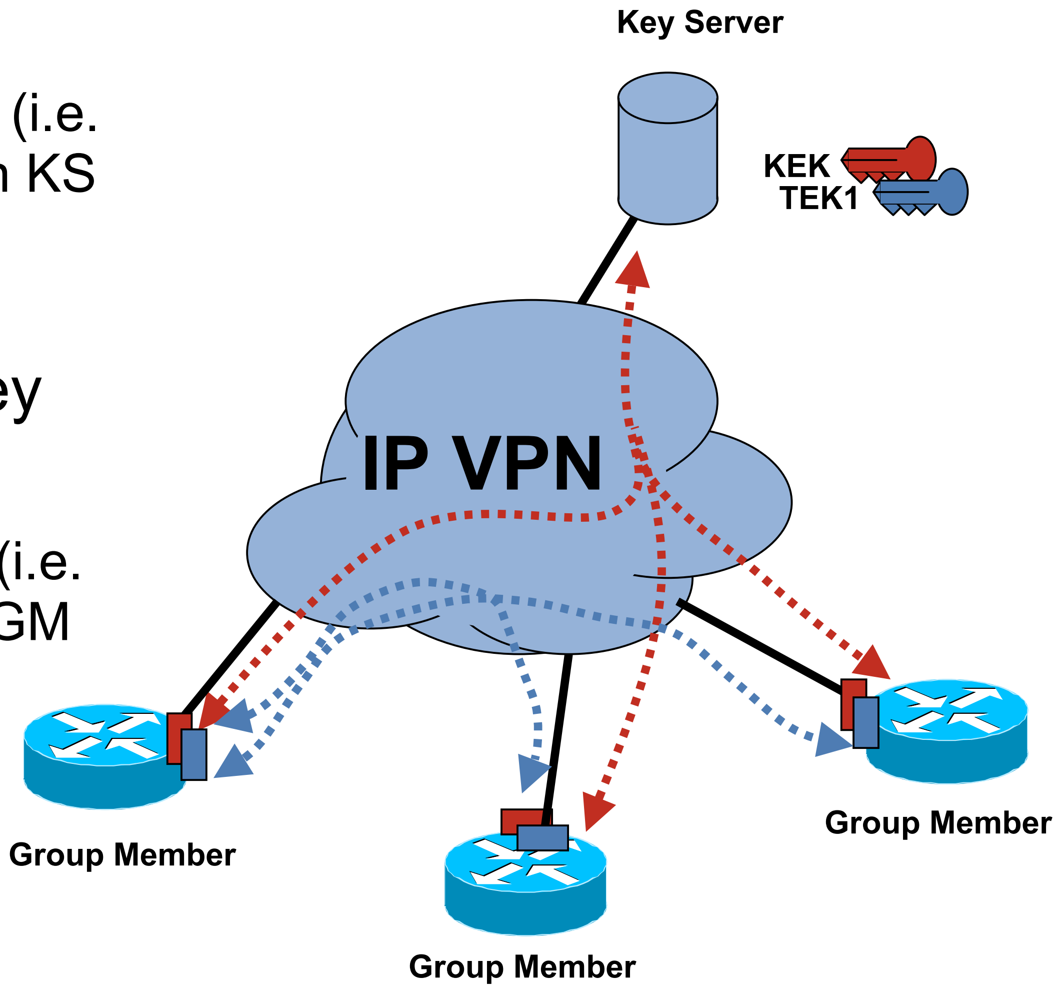
Group Keys

- Key Encryption Key (KEK)

  Used to encrypt GDOI (i.e. control traffic) between KS and GM

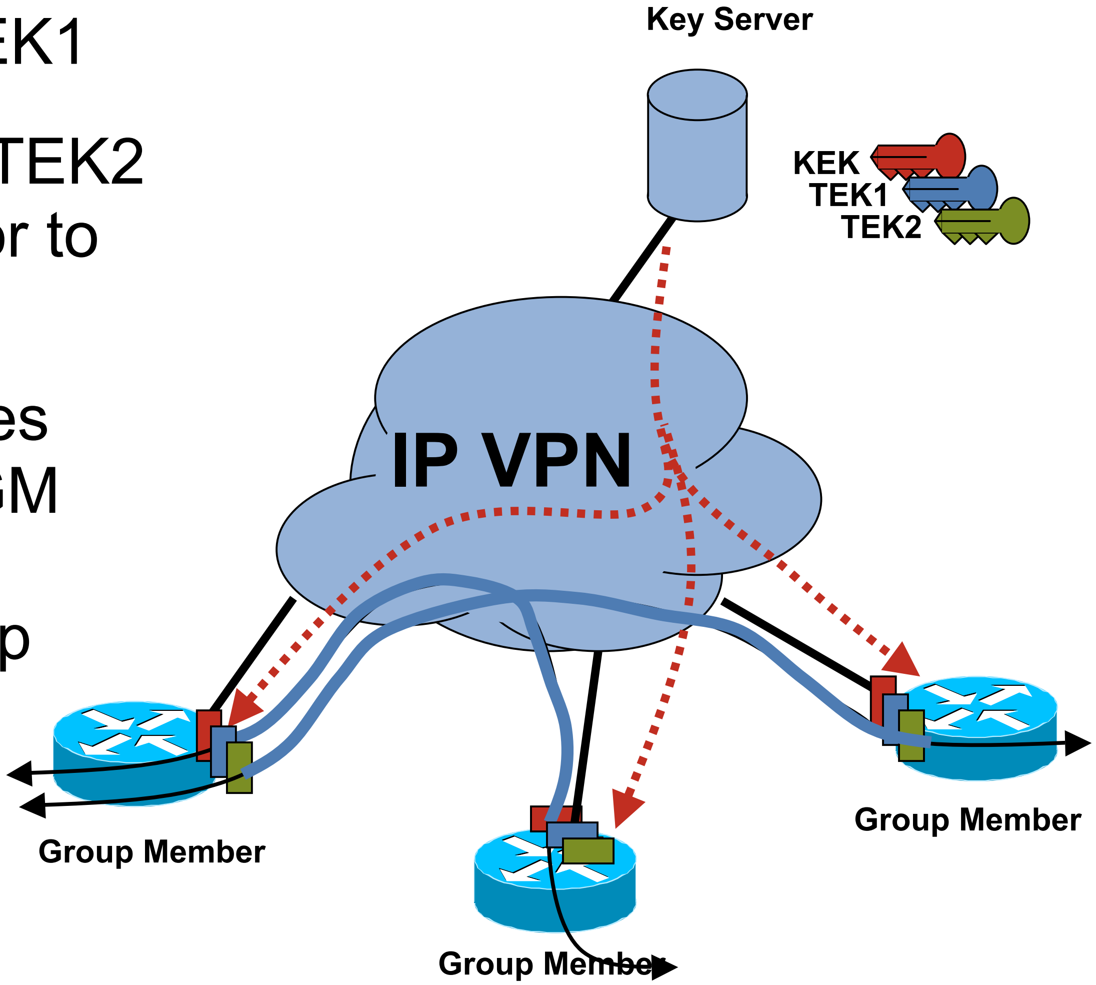
- Traffic Encryption Key (TEK)

  Used to encrypt data (i.e. user traffic) between GM



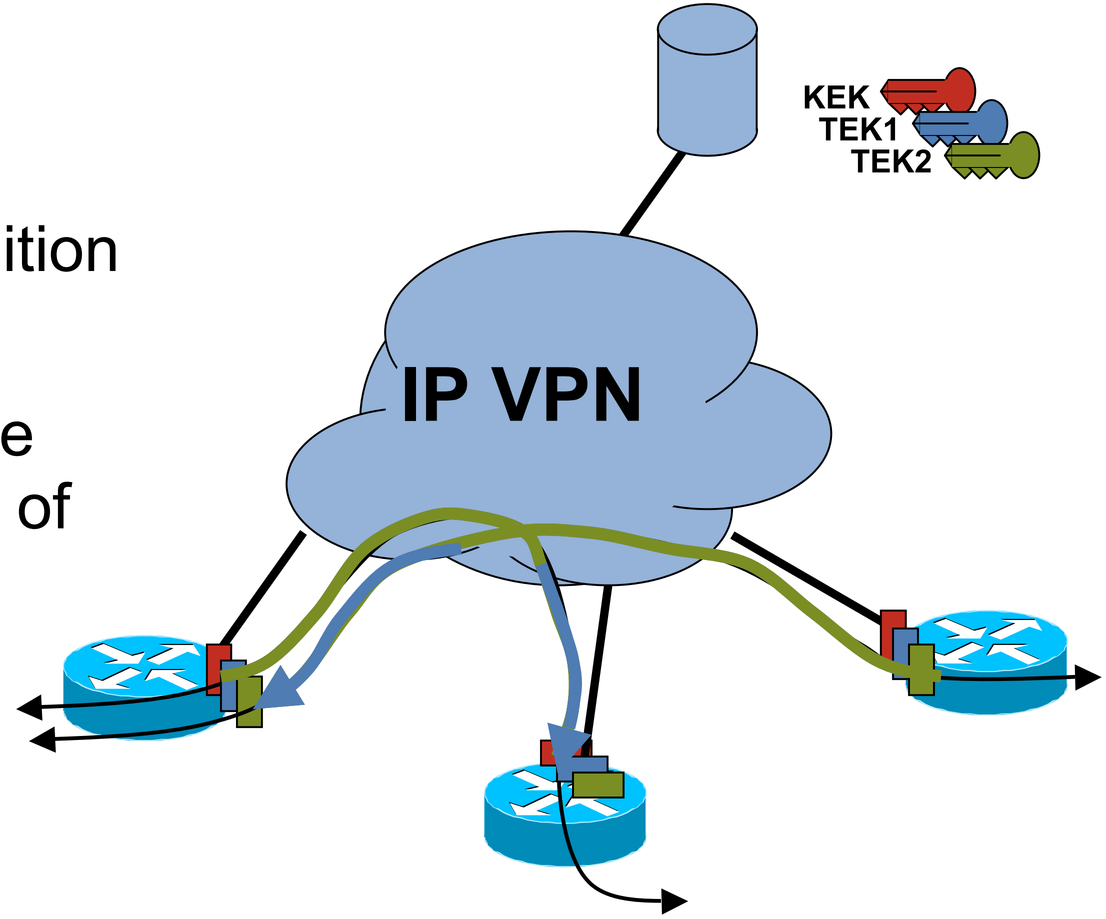
Group Keys

- Key Server monitors expiration time of TEK1
- Key Server creates TEK2 to replace TEK1 prior to expiration
- Key Server distributes TEK2 to all known GM via unicast or via multicast rekey group
- Group Members install new TEK2



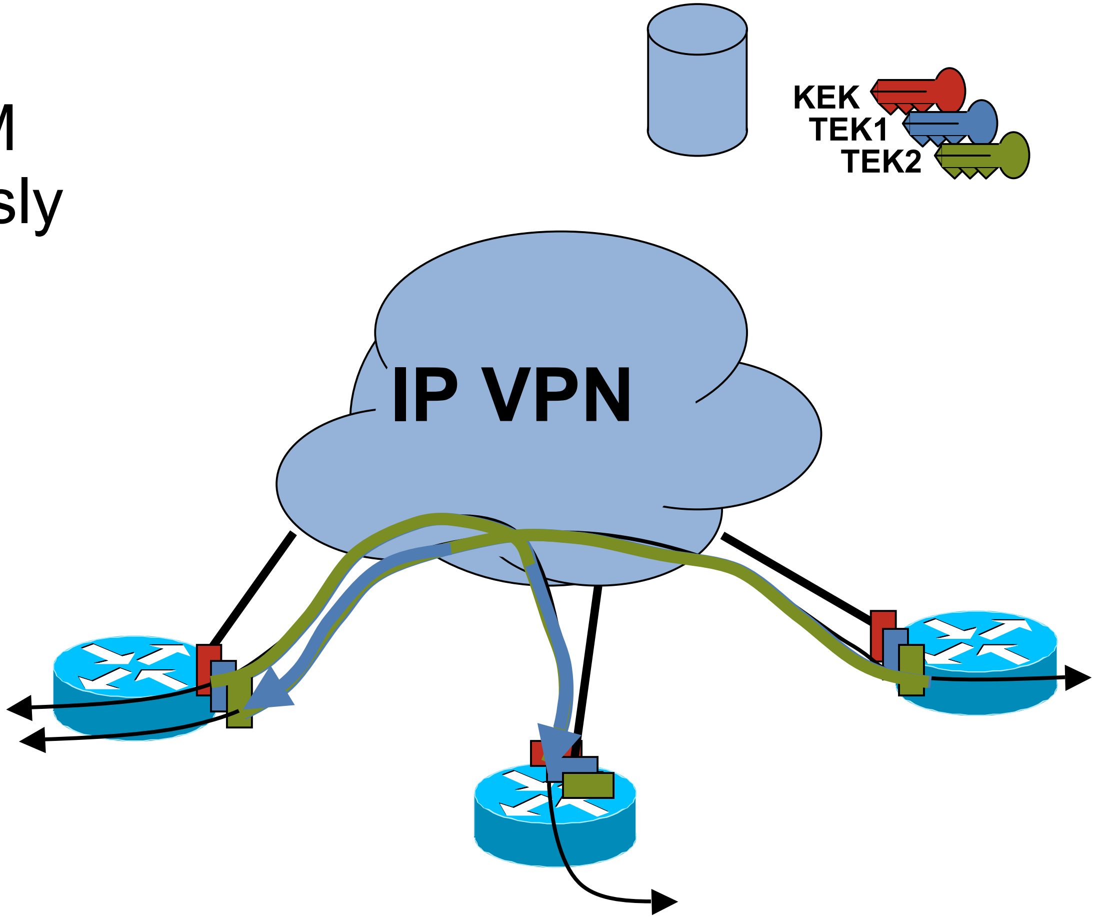
Group Keys

- All GM’s capable of decrypting with TEK1 and TEK2
- GM’s pseudo-synchronously transition encryption to TEK2
- GM’s continue to use TEK1 for decryption of data ‘in flight’.



Group Keys

- All GM transitioned to TEK2 encryption
- TEK1 expires on GM pseudo-synchronously



Multicast Key Distribution

- Multicast Key Distribution over Multicast Enabled Network

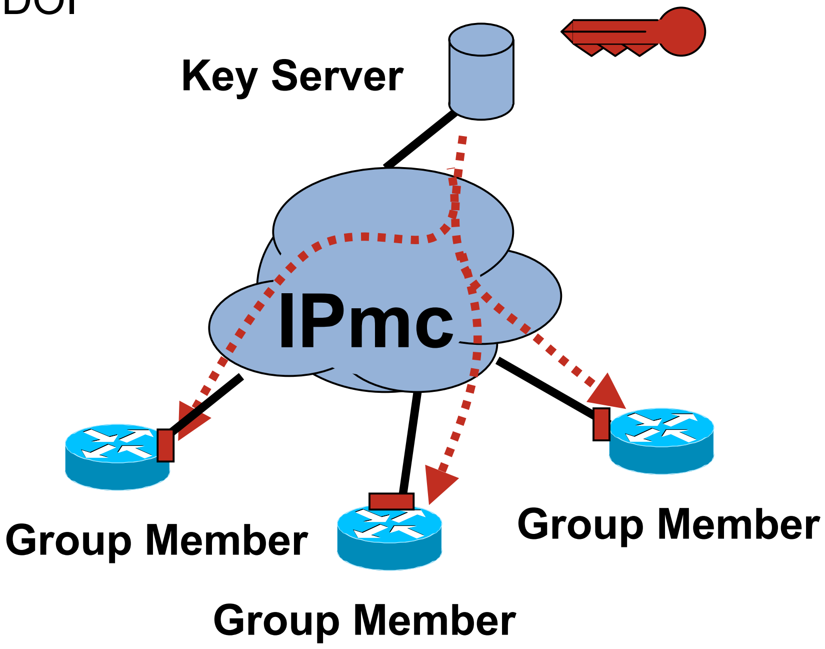
  Via Multicast Formatted Key Message and Network Replication

  Repetitive Broadcast N-Times

  Fallback to Group Member GDOI Unicast Registration

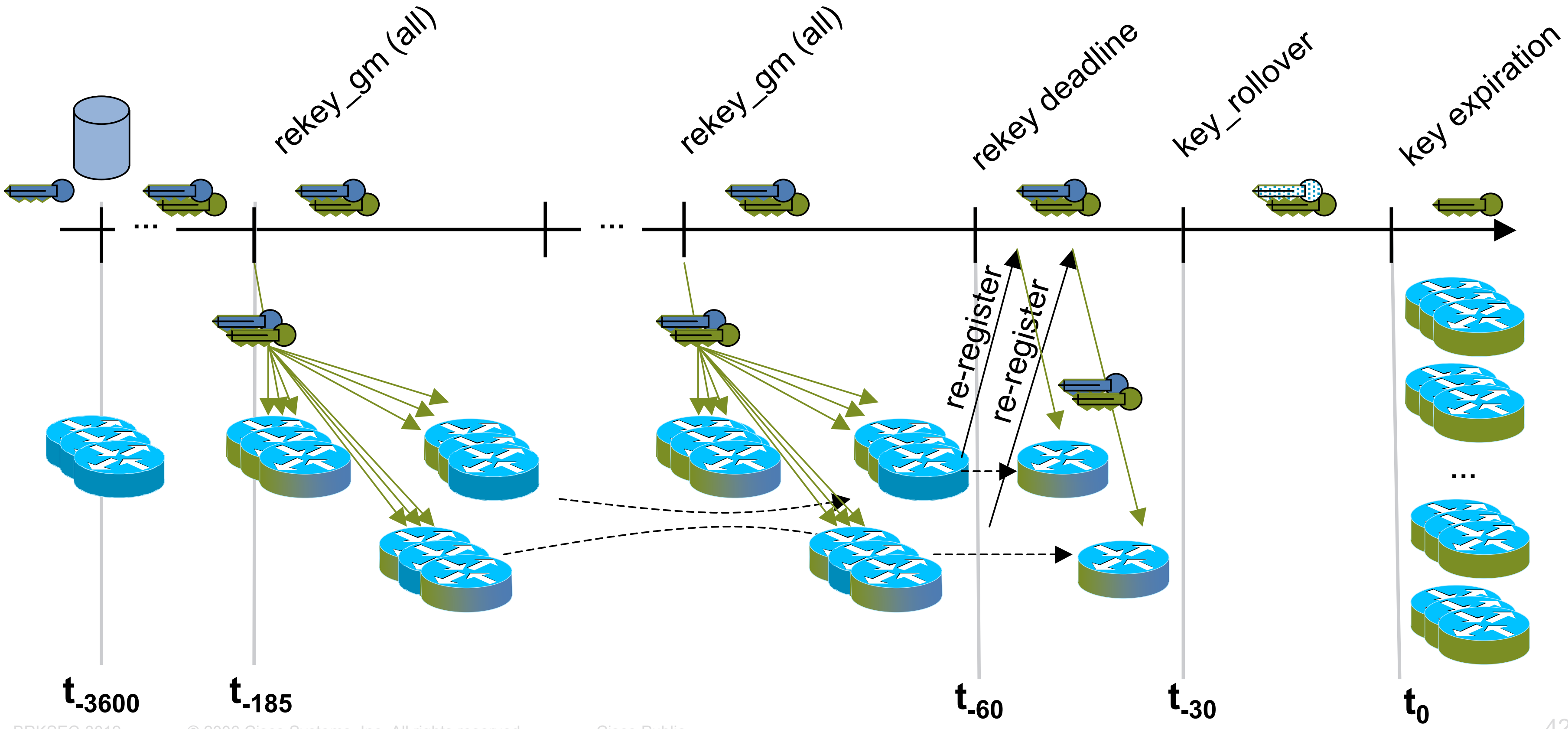
REKEY_MC_Group 232.0.0.1
Group Member = 192.168.3.2
Group Member = 192.168.3.3
Group Member = 192.168.3.4
KEK_old = <key_value>
KEK_new = <key_value>
TEK1 = <key_value1>
TEK2 = <key_value2>

Protect: 10.0.0.0/8 to 10.0.0.0/8
Protect: 10.0.0.0/8 to 232.0.1.0/24



Multicast Rekey Model

- KS Calculates Time Required to Pre-position Next TEK with M-number of retries
- Transmits Multicast Rekey in M-times to all Group Members

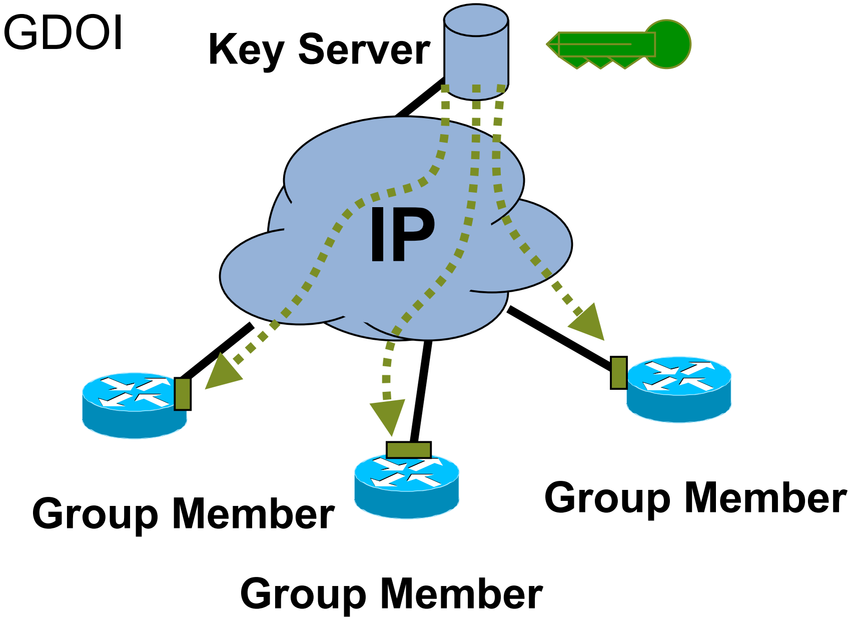


Unicast Key Distribution

- Unicast Key Distribution over non-Multicast Enabled Network
  - Via per-Peer Unicast Formatted Key Message
  - Repetitive Unicast N-Times for Unacknowledged Members
  - Fallback to Group Member GDOI Unicast Registration

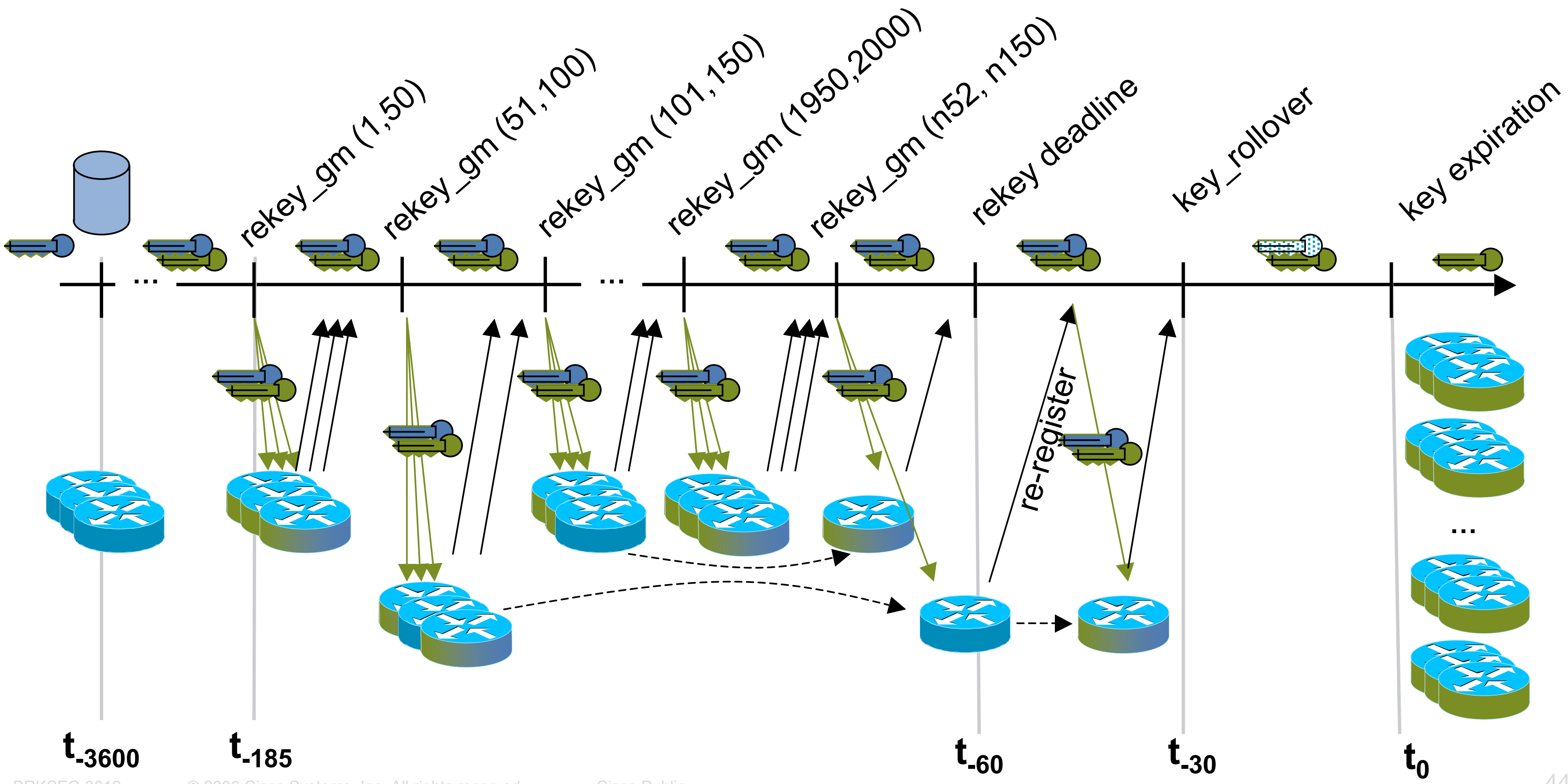
REKEY_UNICAST
Group Member = 192.168.3.2
Group Member = 192.168.3.3
Group Member = 192.168.3.4
KEK_old = <key_value>
KEK_new = <key_value>
TEK1 = <key_value1>
TEK2 = <key_value2>

Protect: 10.0.0.0/8 to 10.0.0.0/8
Protect: 10.0.0.0/8 to 232.0.1.0/24



Unicast Rekey Model

- KS Calculates Time Required to Pre-position Next TEK with N-number of Group Members and retries
- Transmits Unicast Rekey in Batches of 50 Members



Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

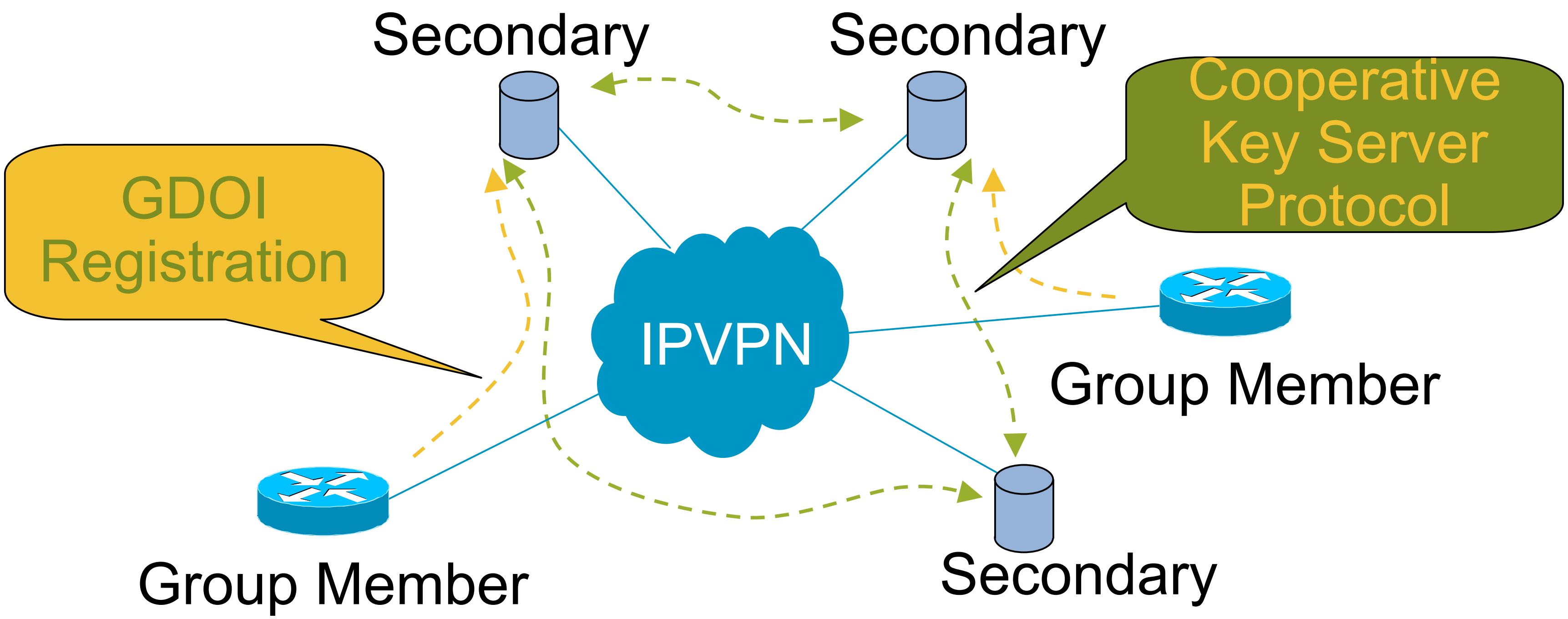
GET Reliability

Reliable Key Server Processes

- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

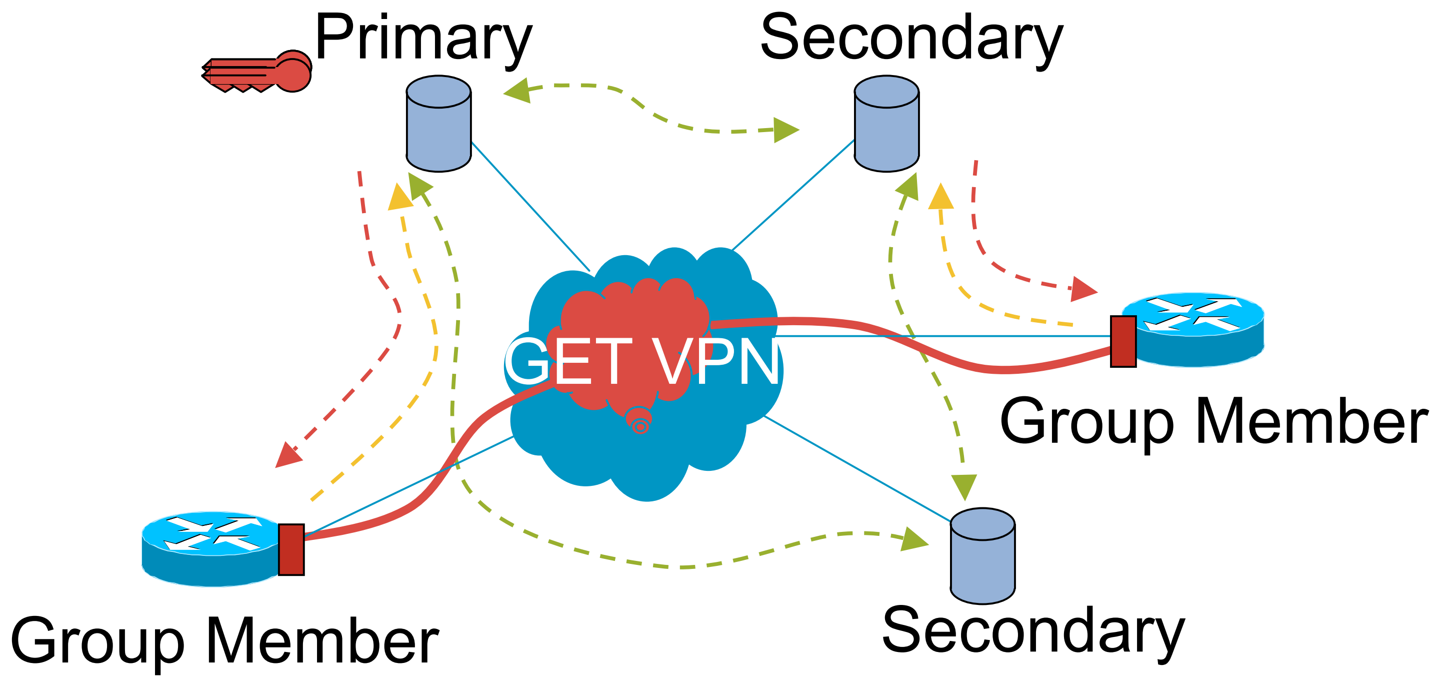
Cooperative Key Server: Roles

- Key Servers Bootstrap into Secondary Role
- Key Servers setup sessions between themselves and exchange key server state
- Group Members Bootstrap with repeated Registration Attempts
- Group Member Registration Fails Until a Primary Key Server is Elected



Cooperative Key Server: Roles

- A Key Server is Elected Primary, Creates Keys, and Distributes Keys
- Group Members Complete Registration to an available Key Server and Receive Policy and Keys



Reliable Key Server Processes

- Cooperative Key Server

  Key Server Roles

  Primary Key Server Processes

  Secondary Key Server Processes

- Failure Scenarios

  Key Server Failure

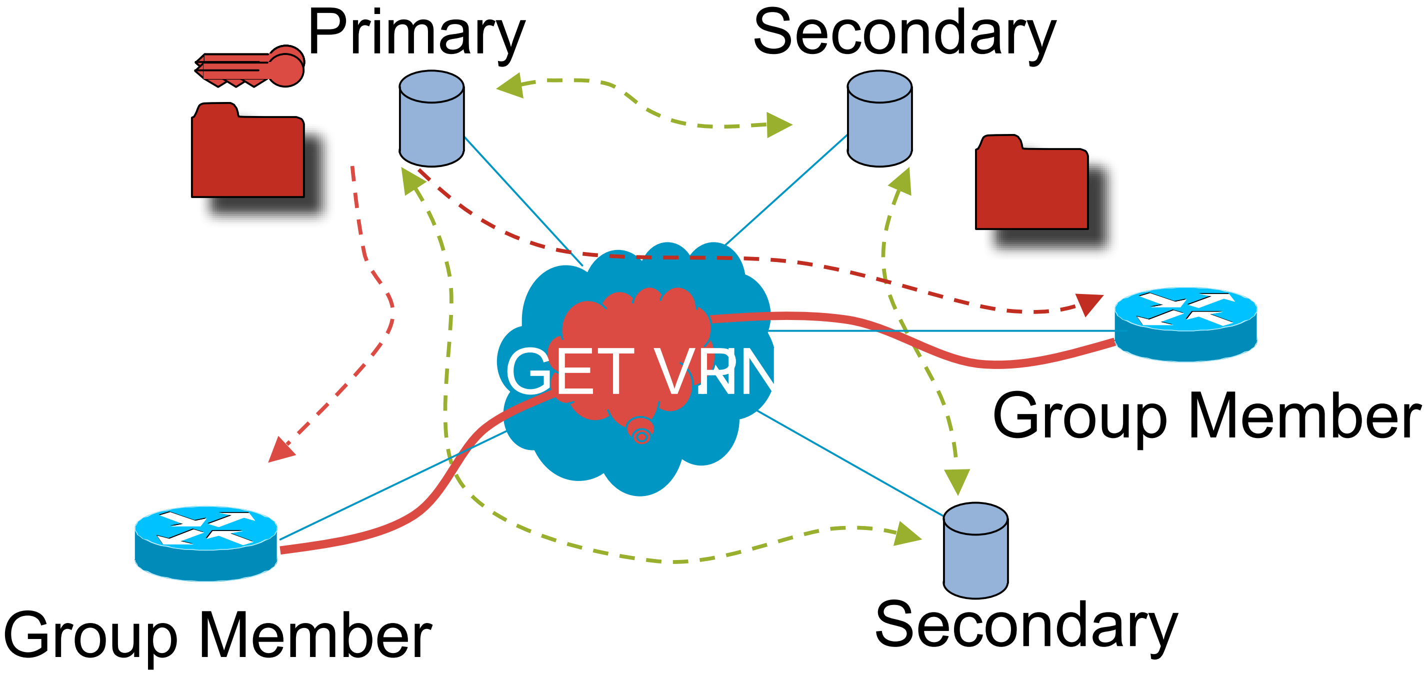
  Key Server Recovery

  Network Partition

  Network Merge

Cooperative Key Server: Primary Processes

- Primary Key Server Generates new Keys on a Periodic Basis
- Primary Checks Consistency of Policies and Coordinates Group Member List with Secondary KS
- Primary Distributes Keys to Secondary KS and Group Members
- Primary Notifies Secondary of Primary Presence

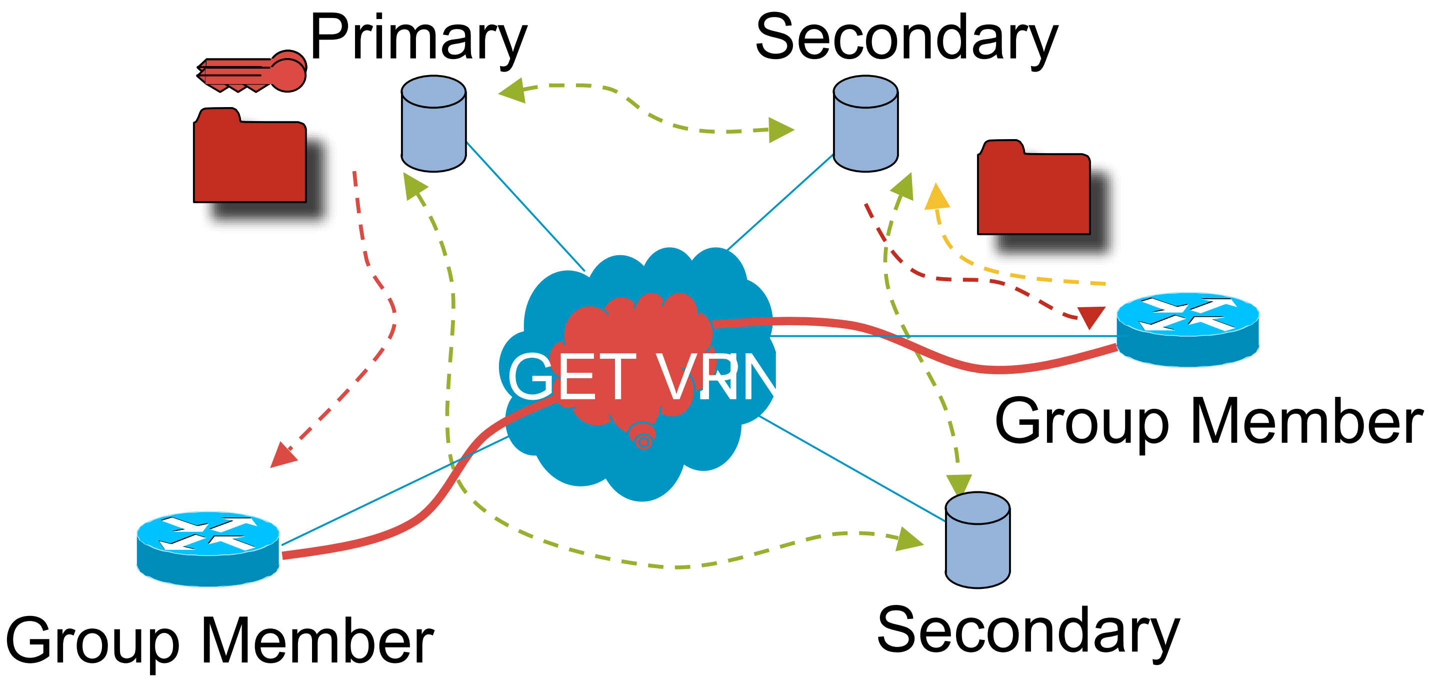


Reliable Key Server Processes

- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

Cooperative Key Server: Secondary Processes

- Secondary Key Server Checks Consistency of Policies with Primary Key Server
- Secondary Key Server Authenticates Group Members and Updates Group Member List with Primary KS
- Secondary Key Server Provides Keys and Policies to Registering Group Members
- Secondary Key Server Monitors Presence of Primary Key Server



Reliable Key Server Processes

- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

Reliable Key Server Processes

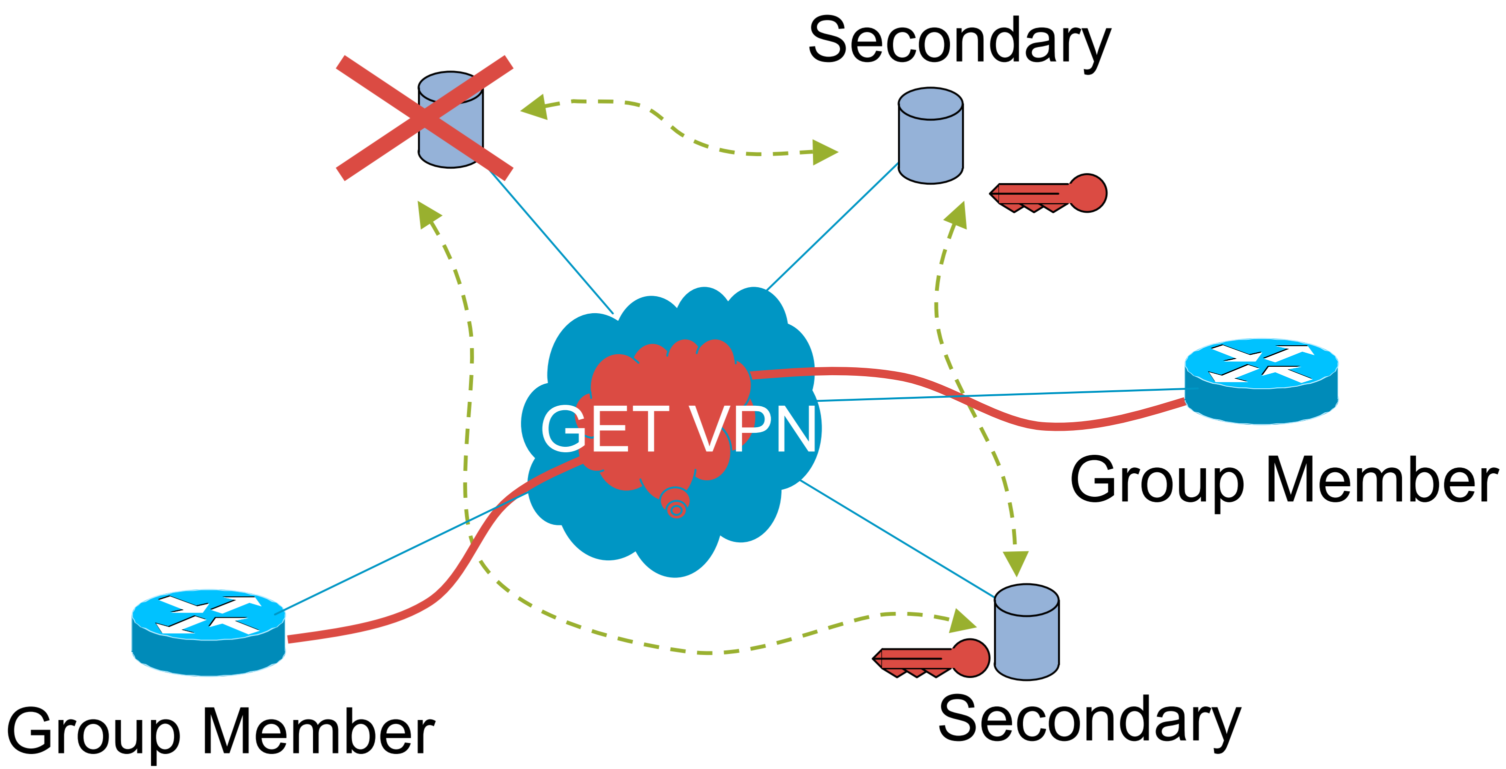
- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

Failure Scenarios: Key Server Failure

- Primary Key Server Database Lost (not disconnected)

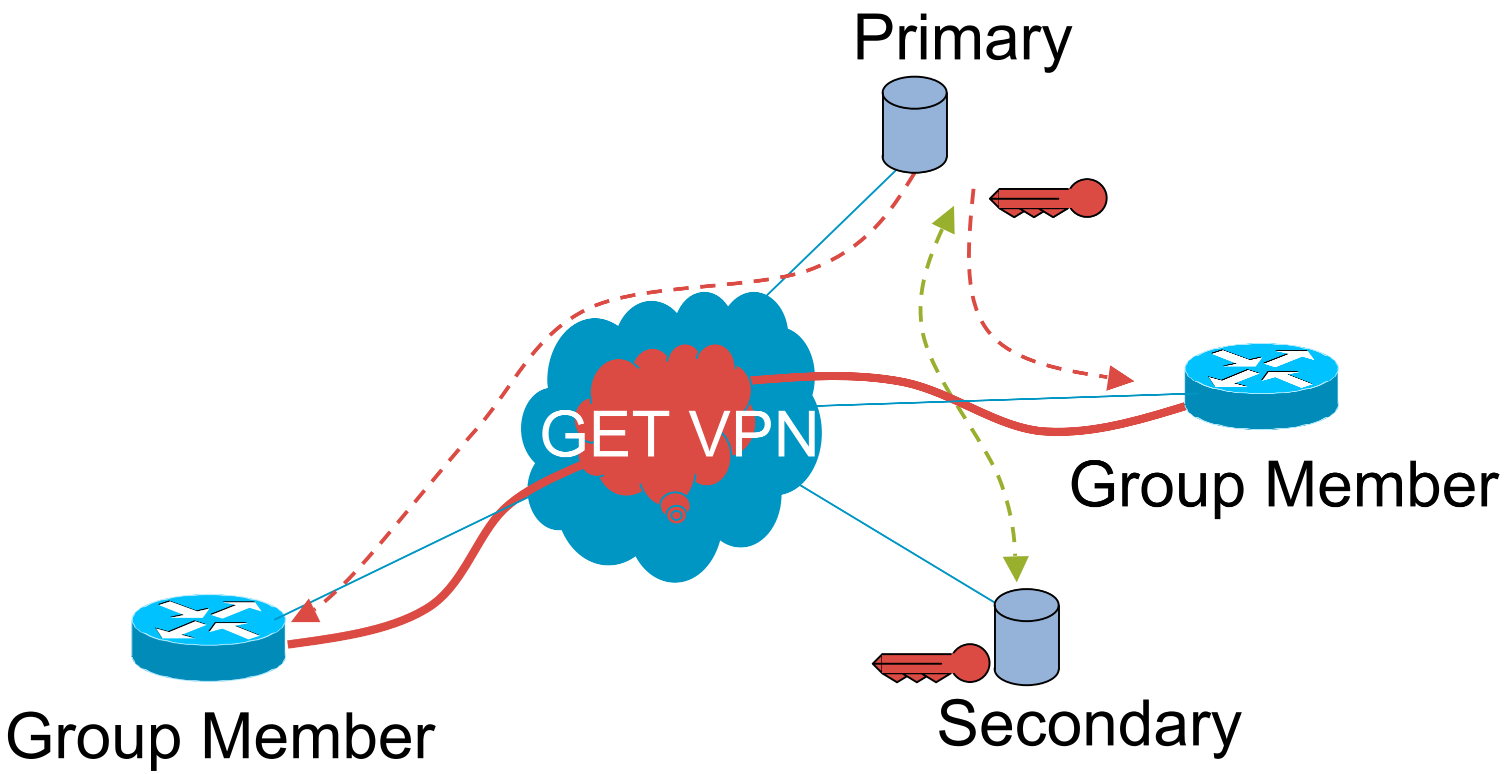
  System Reboot, GDOI Database Cleared

- Secondary Key Servers Detect Loss of Primary



Failure Scenarios: Key Server Failure

- One Secondary KS Elected as New Primary KS
- Elected Primary Manages Policies, Keys, and Group Member List
- Elected Primary Now Responsible for Group Rekey Messages

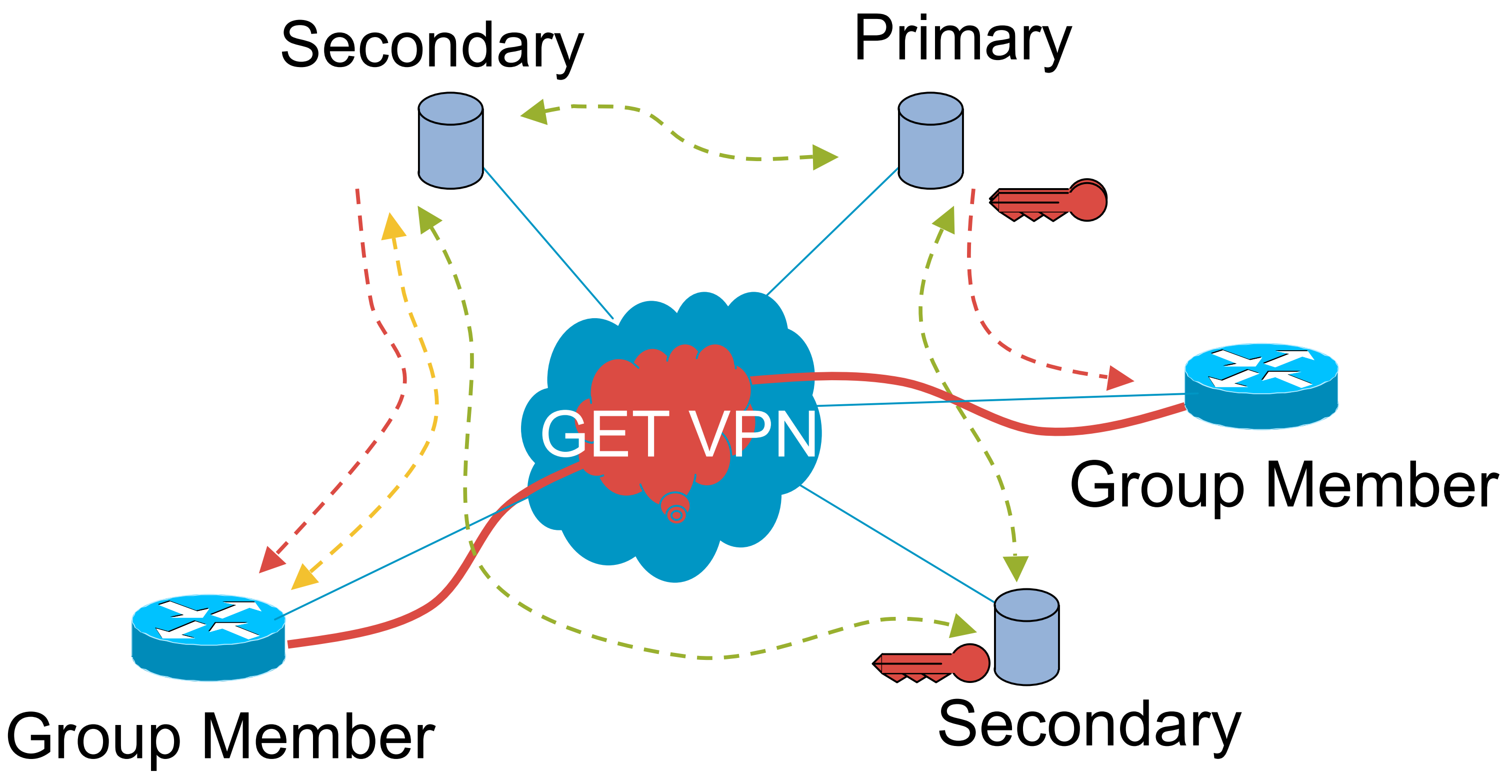


Reliable Key Server Processes

- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

Failure Scenarios: Key Server Recovery

- Restored KS Recovers and Assumes Secondary Role
- Validates Policy with the Primary and Receives Keys and Group Member List
- Restored Key Server Eligible for Registrations

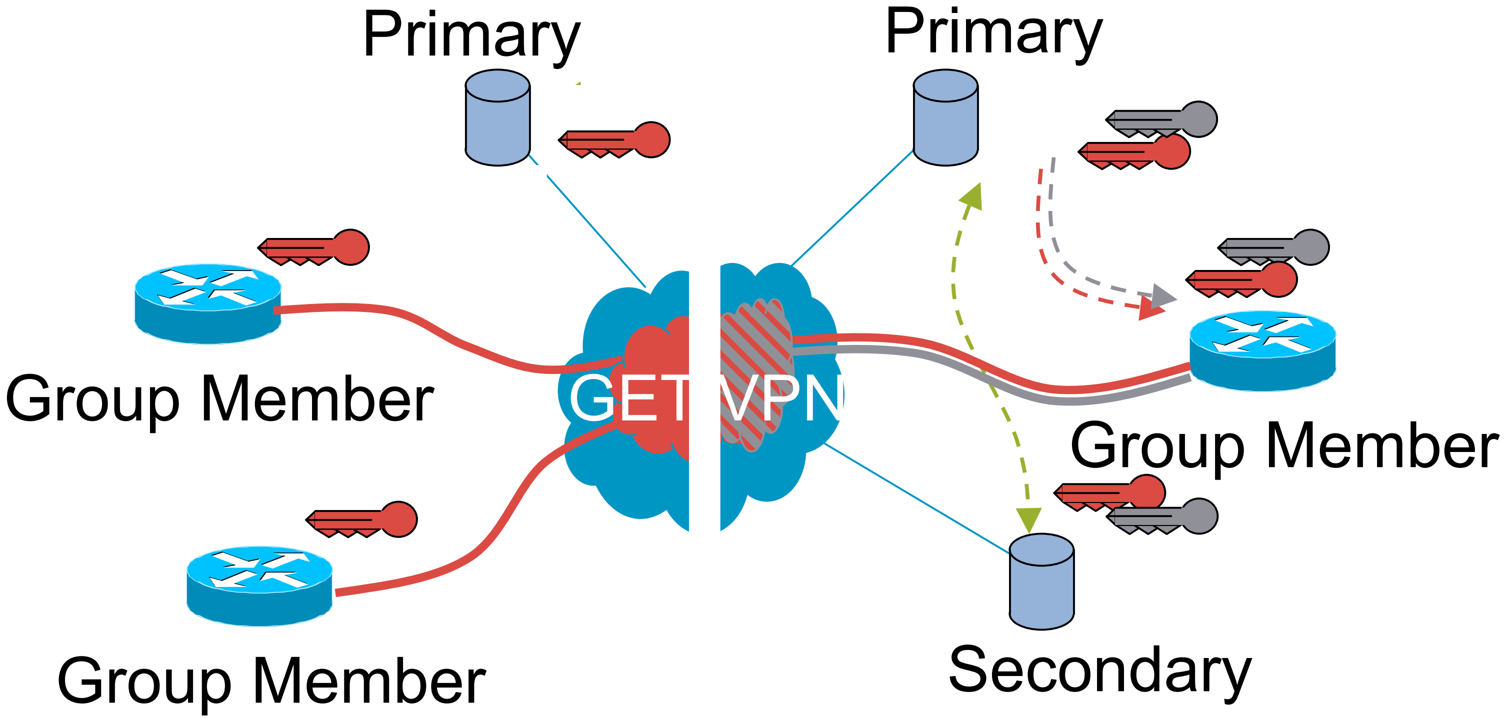


Reliable Key Server Processes

- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

Failure Scenarios: Key Server Partition

- Primary Elected in Each Network Partition
- Elected Primary Creates New Keys and Distributes to Group Members

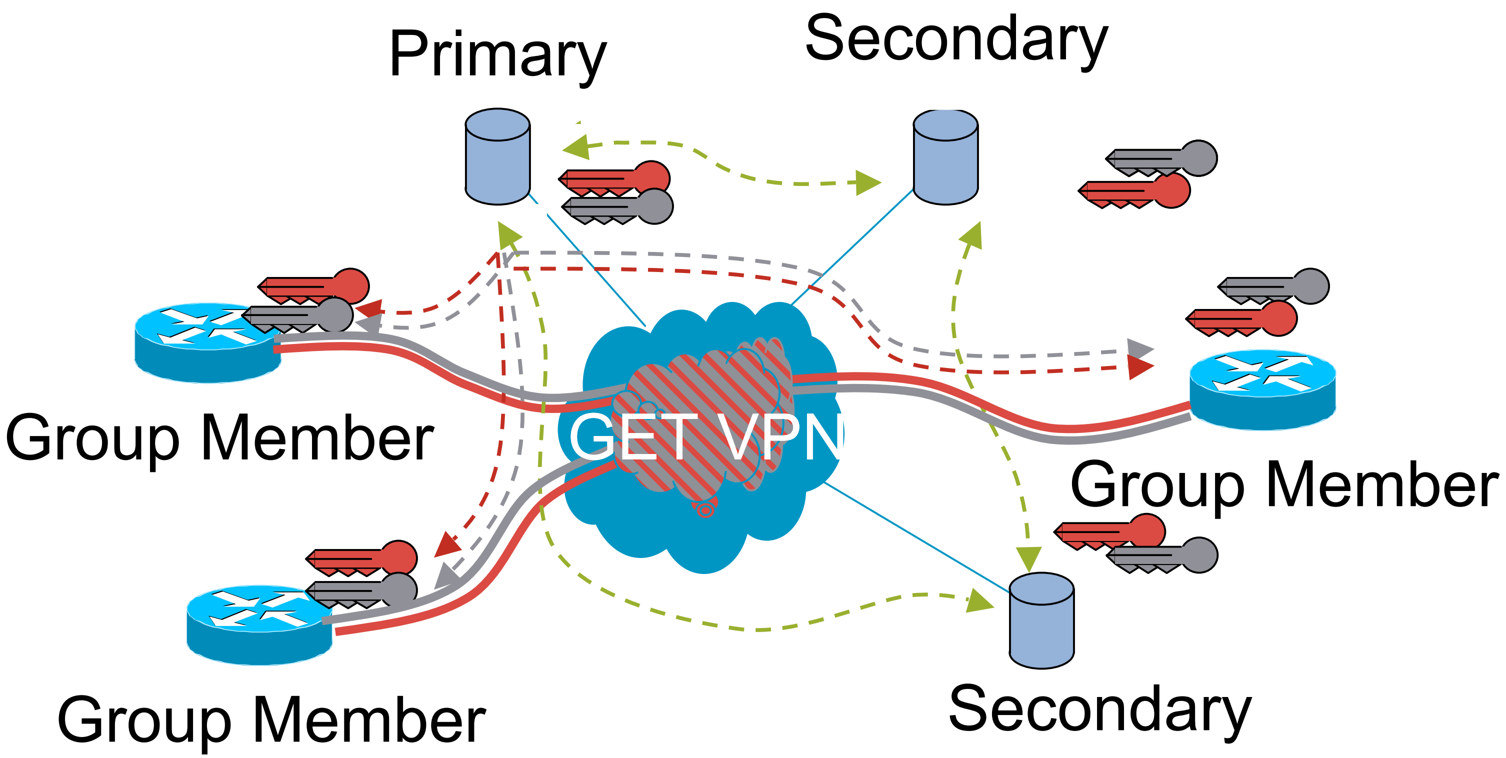


Reliable Key Server Processes

- Cooperative Key Server
  - Key Server Roles
  - Primary Key Server Processes
  - Secondary Key Server Processes
- Failure Scenarios
  - Key Server Failure
  - Key Server Recovery
  - Network Partition
  - Network Merge

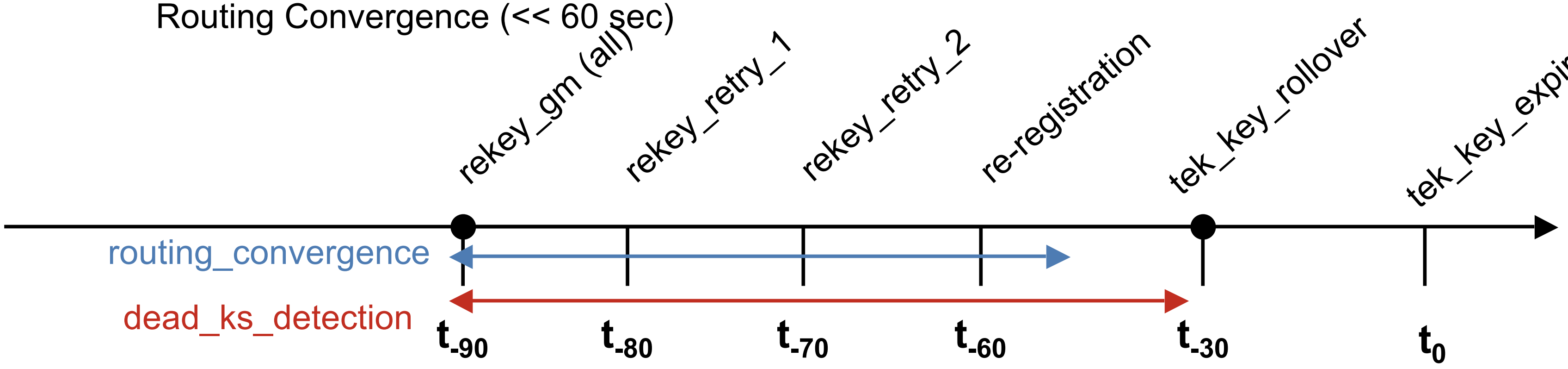
Failure Scenarios: Key Server Merge

- Lower Priority Primary KS Demoted to Secondary KS
- Demoted Key Server Provides Key Set to Elected Primary KS
- Elected Primary Synchronizes Keys with all Secondary KS
- Elected Primary Distributes Keys to All Group Members



Reliable Key Server Processes

- Recommendations
  - Make Routing Convergence Faster Than Dead Key Server Detection
    - Avoid key servers from partitioning the network unnecessarily
    - A partitioned network requires a merge immediately upon completion of routing convergence
  - Make Dead Key Server Detection Faster than Rekey + Registration Interval
    - Avoid TEK SA Expiration before new Primary elected
- Example
  - Rekey + Registration Interval (60 sec)
    - Rekey (30 seconds - 3 attempt, 2 retries at 10 second intervals)
    - Re-registration (30 seconds)
  - Dead Key Server Detection (< 60 sec)
  - Routing Convergence (<< 60 sec)



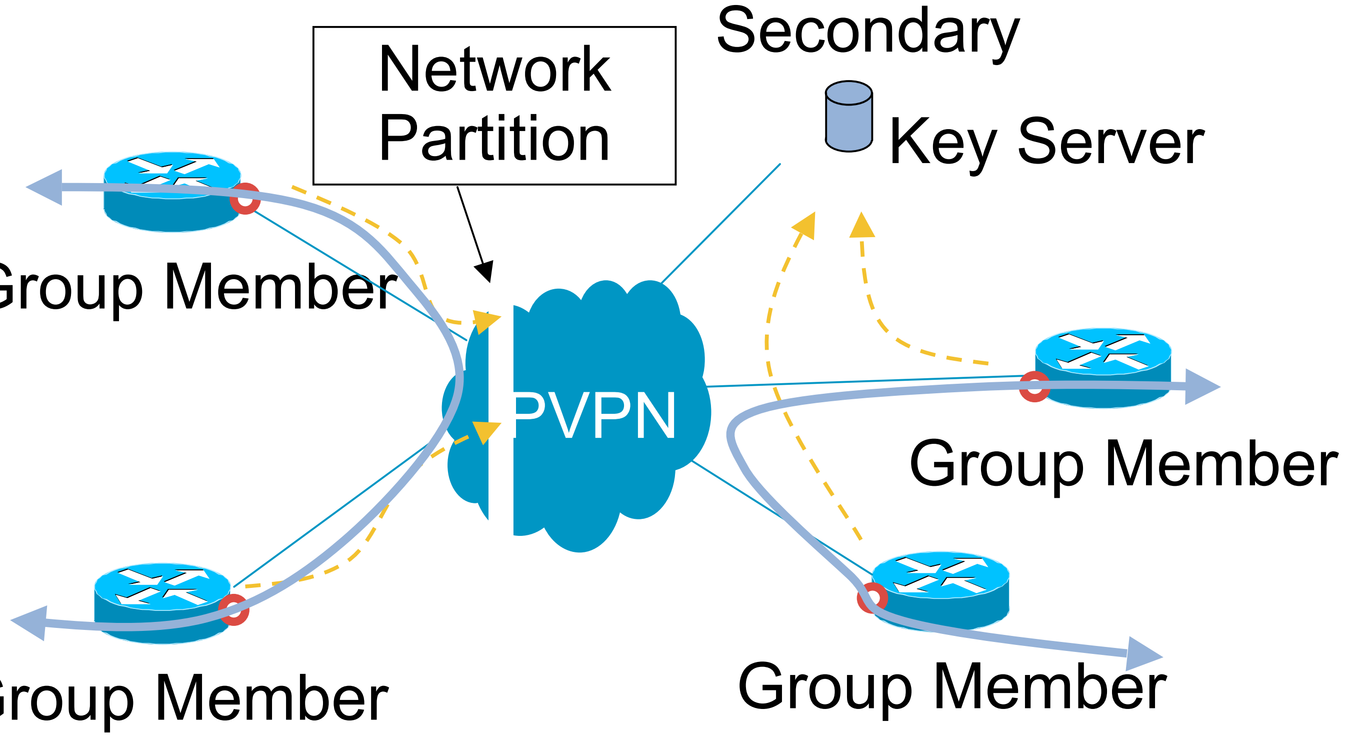
Reliable Group Member Model

- Group Member Bootstrap (Before Authentication)
- Group Member State (After Authentication)
- Redundant GET Enabled Interfaces

Pre-Authenticated GM Bootstrap

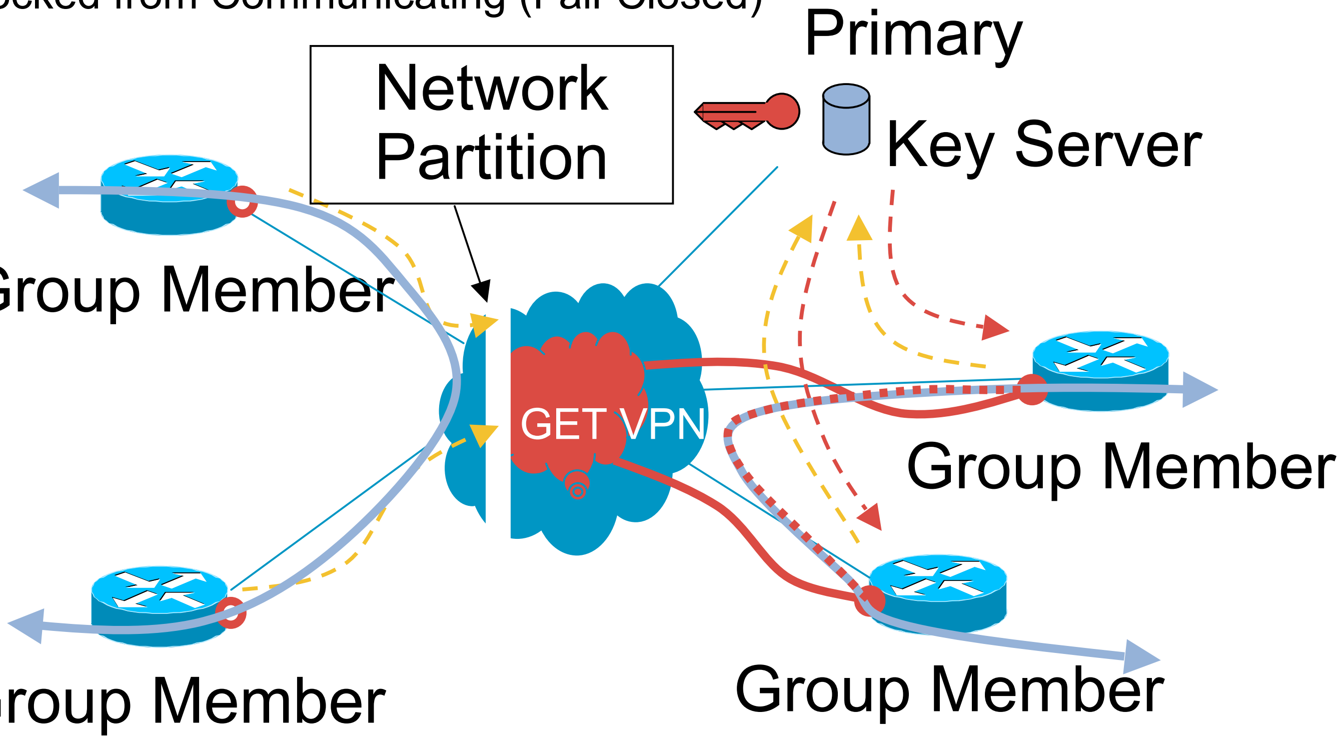
- Group Members Perpetually Attempt Registration to a Key Server
- Communication State Between GM's Dependent Upon Policy and Access-Lists

  Fail-Open or Fail-Closed



Pre-Authenticated GM Bootstrap

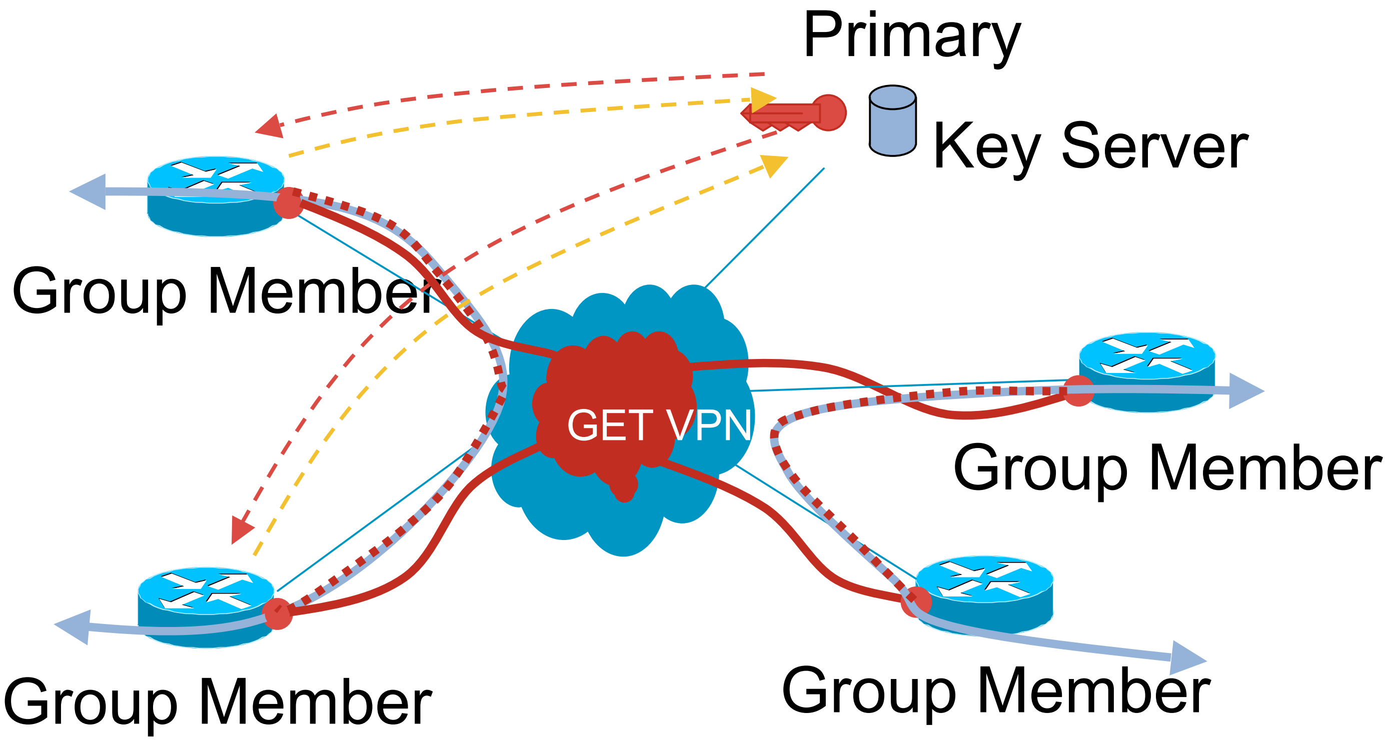
- Successfully Registered GM
  - Establish Communications using the Group Policy
- Unsuccessful GM Registration
  - GM Remain Isolated as a Group (Fail-Open)
  - Blocked from Communicating (Fail-Closed)



Pre-Authenticated GM Bootstrap

- Successfully Registered GM

  Group Members Persistently Attempt Registration until Success



Pre-Authenticated GM Bootstrap

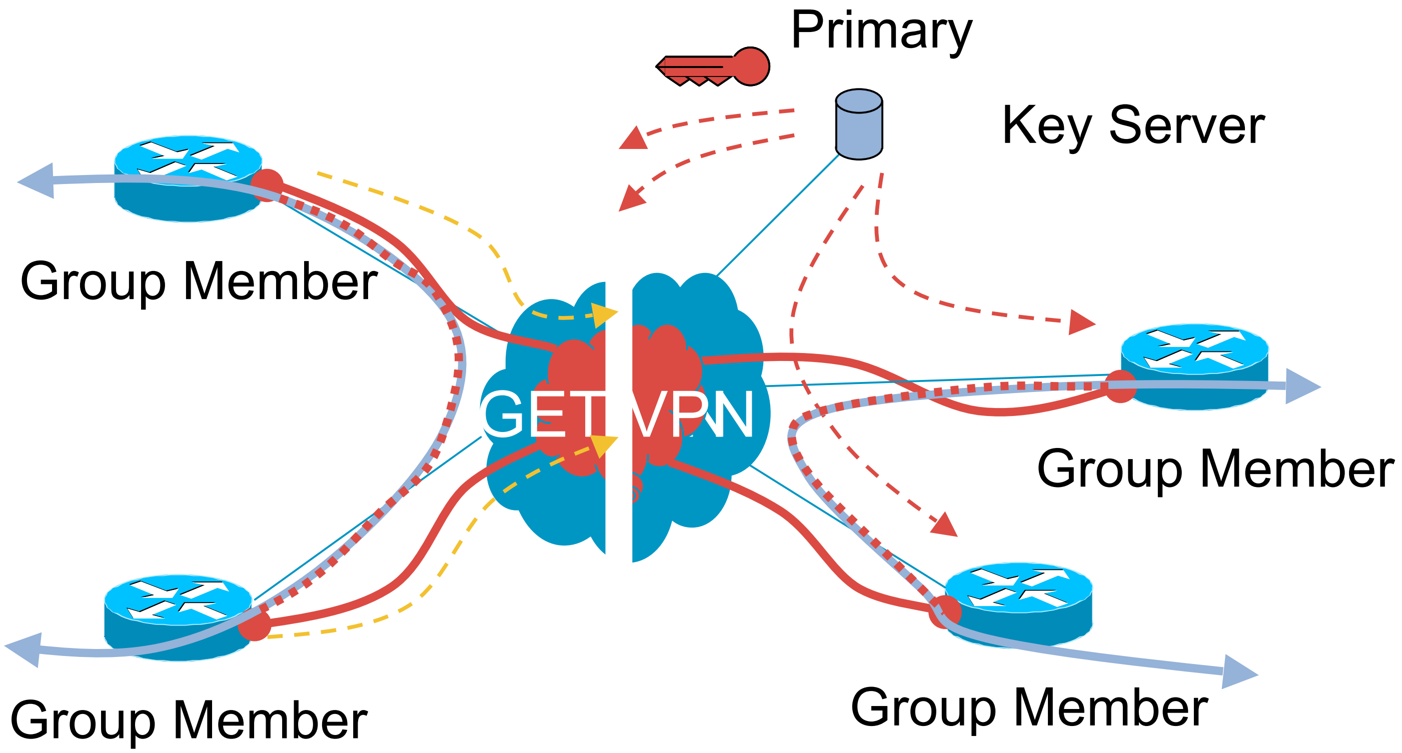
- Persistent Effort by GM to Obtain KS Policy
- Fail-Open: Clear-text Transmission is Acceptable
  - Do Nothing
    - Crypto Map Applied
    - No Policy Downloaded (i.e. no permit downloaded from KS)
    - Traffic Matches Null Policy
    - Traffic Passed in Clear
- Fail-Closed: Clear-text Transmission is Not-Acceptable
  - Filter All Traffic via ACL
    - Permit Control Plane (IGP/BGP, PIM, GDOI)
    - Permit Management Plane (SSH, TACACS, …)
    - Permit Encrypted Data Plane (ESP)
    - Deny All Other Traffic

Reliable Group Member Model

- Pre-Authenticated Group Member Bootstrap
- Post-Authenticated Group Member State
- Redundant GET Enabled Interfaces

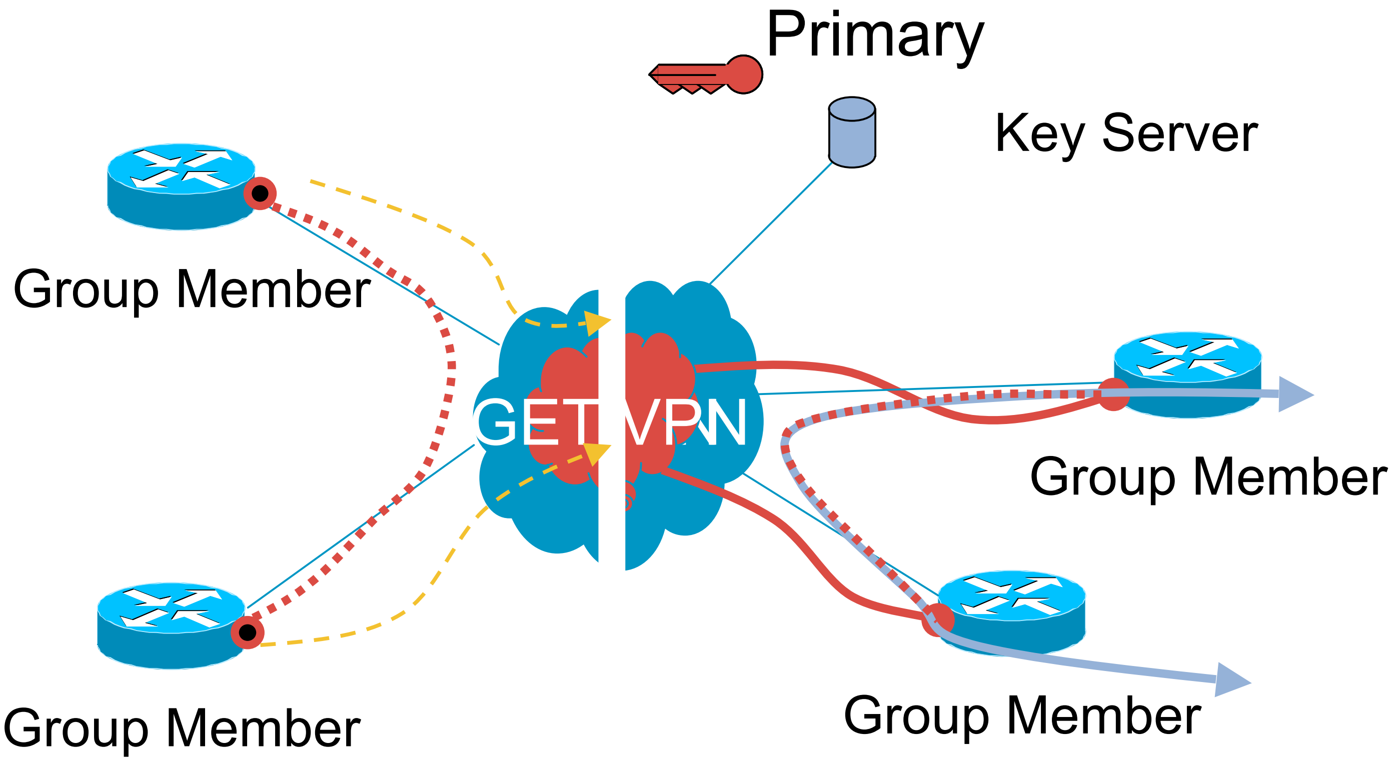
Post-Authenticated GM Bootstrap

- Group Members partitioned from Key Servers cannot obtain rekey messages
- Partitioned group members attempt to re-register after TEK expiration



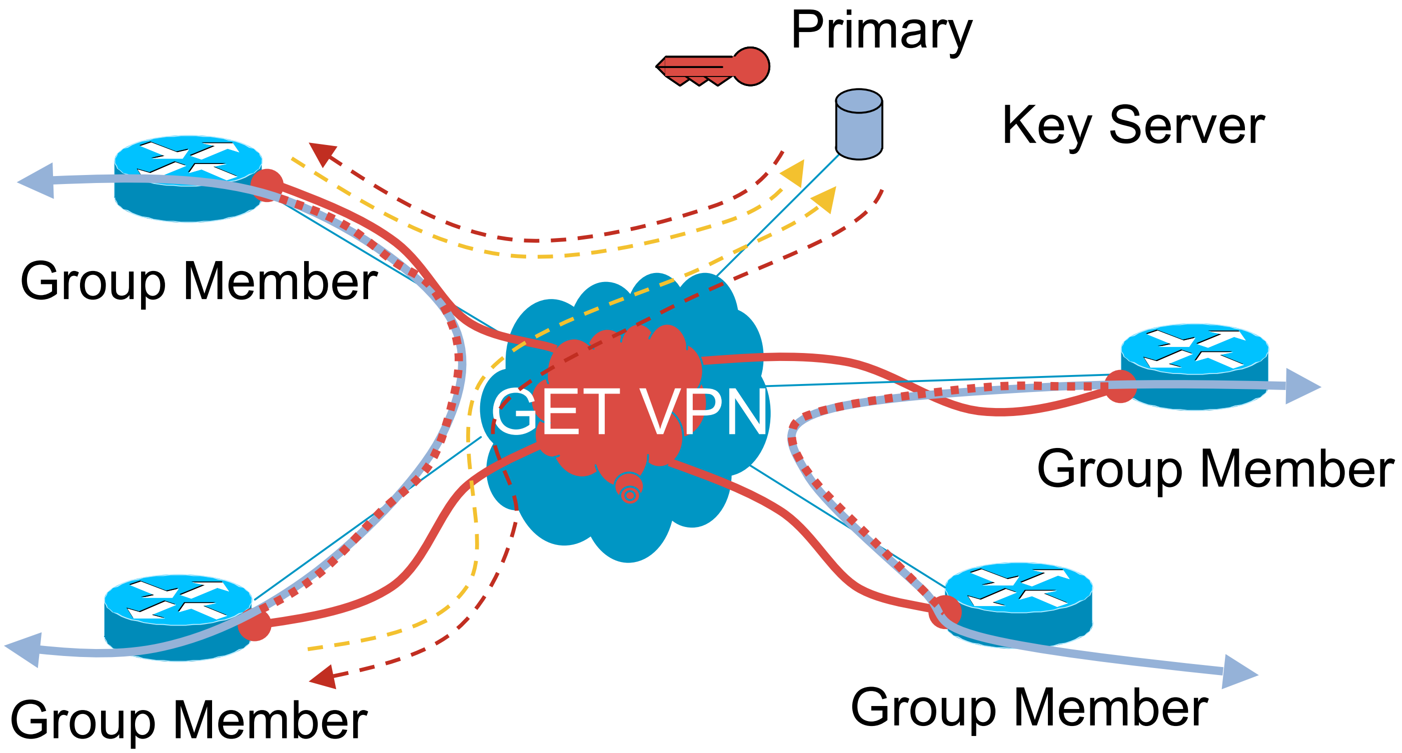
Post-Authenticated GM Bootstrap

- Group members with expired security association repeatedly attempt to complete registration
- Policy persists but the key material expires
- Communication is blocked (fail-closed) until new key material is obtained



Post-Authenticated GM Bootstrap

- Partitioned group members persist in attempted registration until success
- Communication remains blocked until registration is complete



Post-Authenticated GM State

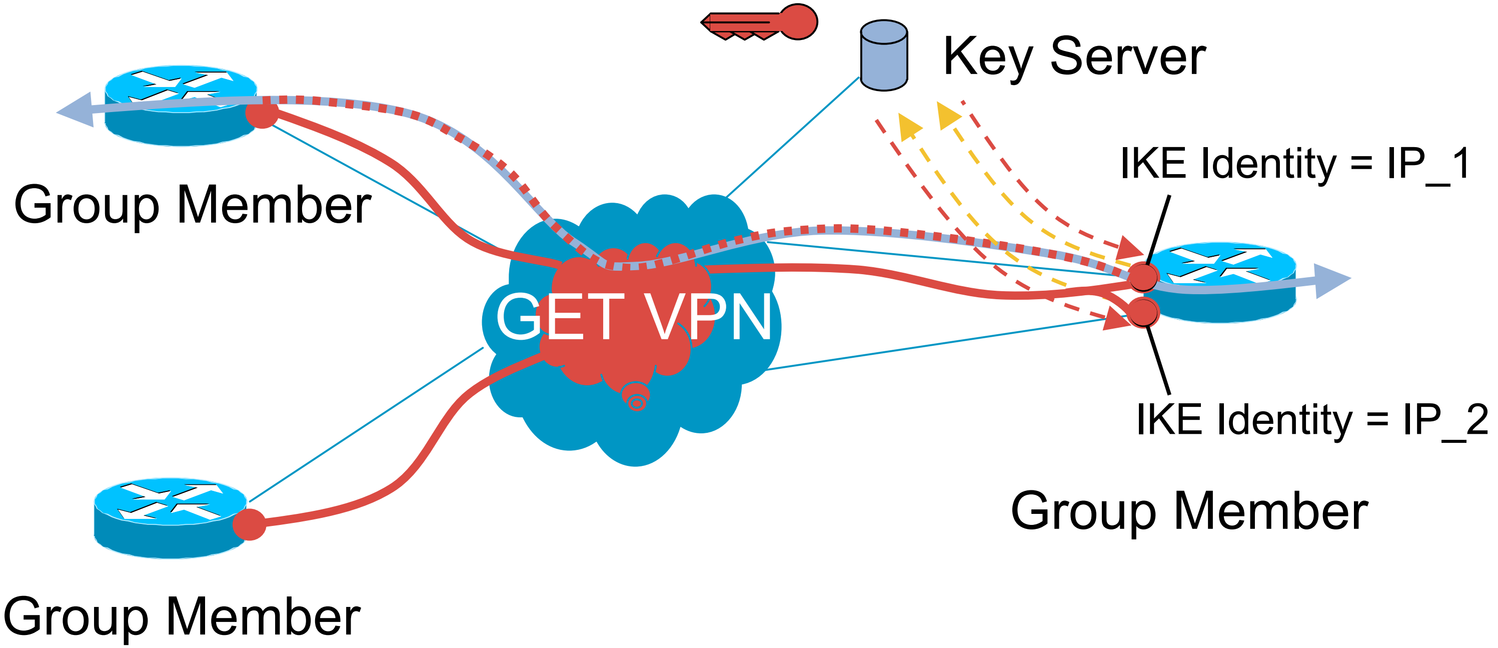
- GM Retains Stale IPsec Policy but no Security Association
- Persistent Effort by GM to Refresh KS Policy
- Fail-Closed:
    - Clear-text Transmission is Prevented Since Policy Exists
- Successful Re-registration Restores Connectivity

Reliable Group Member Model

- Pre-Authenticated Group Member Bootstrap
- Post-Authorized Group Member State
- Redundant GET Enabled Interfaces
  - Multiple IKE Identities
  - Single IKE Identity

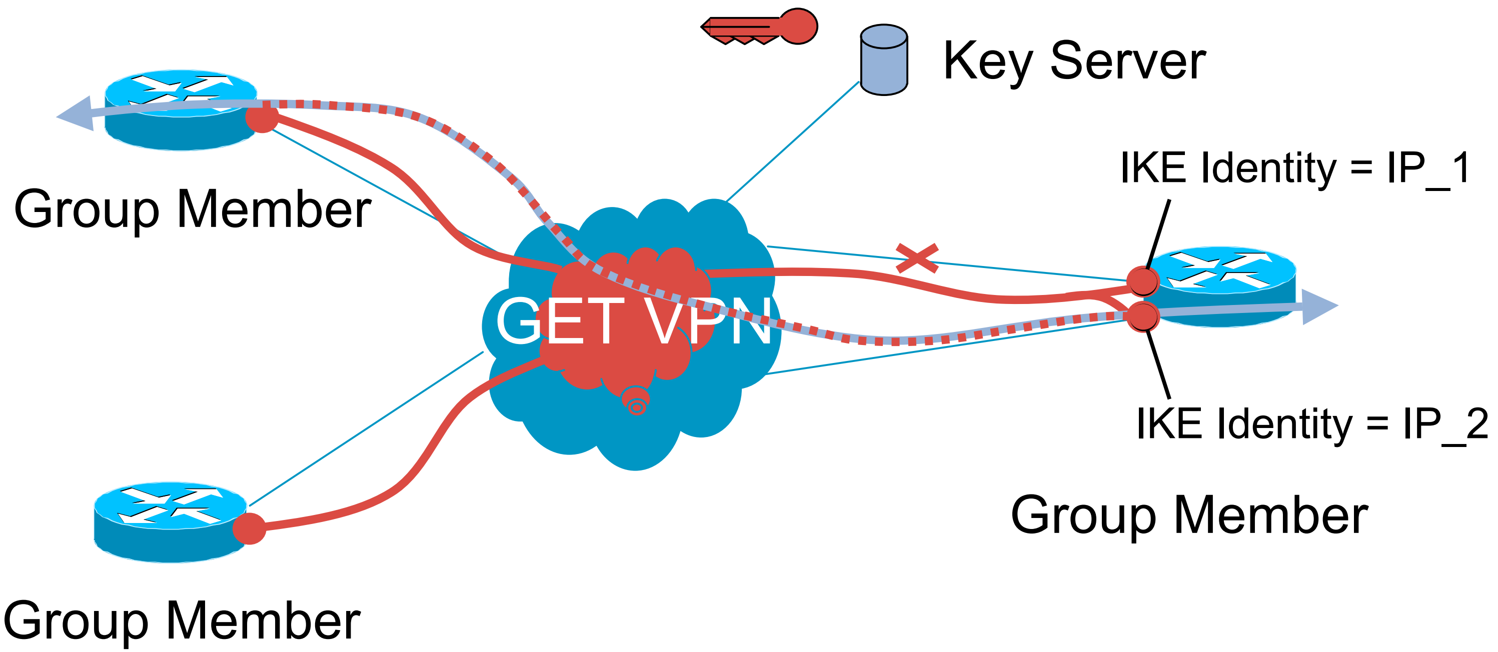
Redundant GET Interfaces: Multiple IKE Identities

- Common crypto map applied to two or more interfaces
- Each interface represents a unique IKE identity
- Key Server manages state for each IKE identity
- Data path may use either interface since the policies and keys are the same



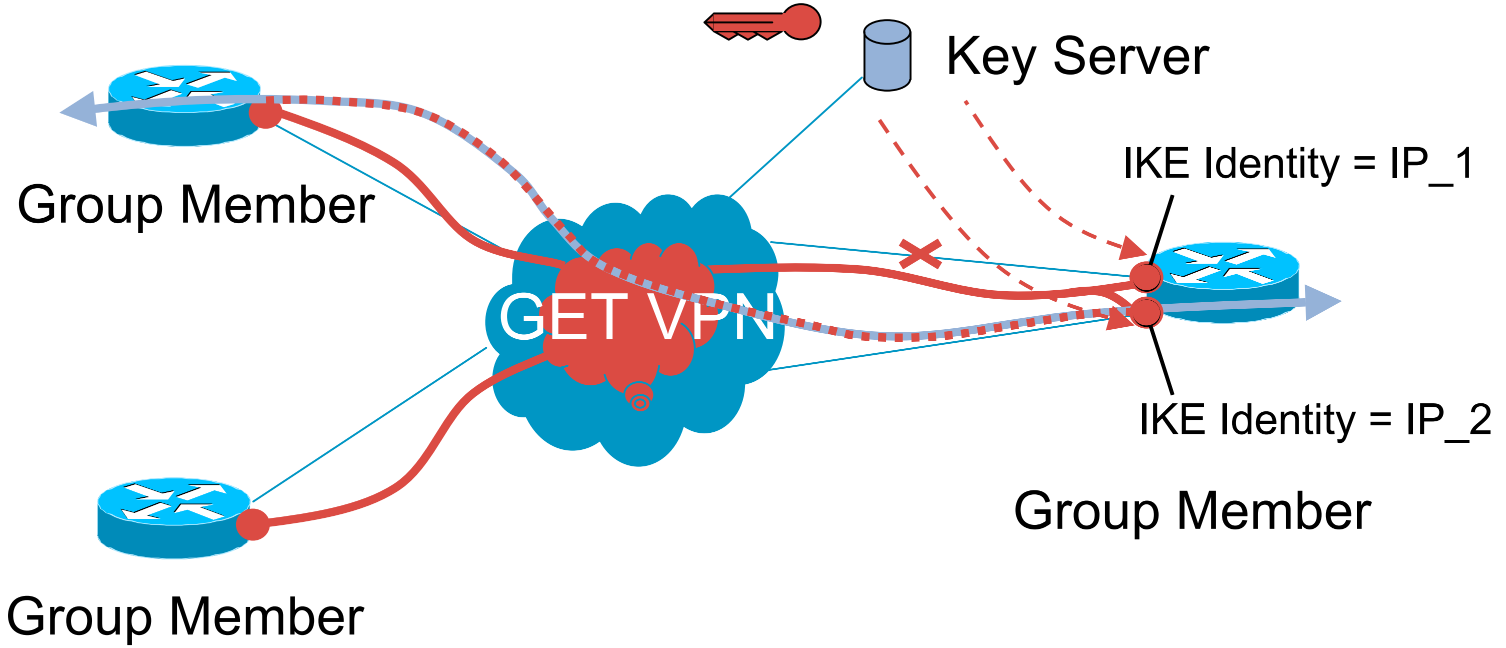
Redundant GET Interfaces: Multiple IKE Identities

- Failure of a GET-enabled interface causes routing convergence
- Alternate path chosen based on optimal calculated route
- Alternate path is immediately viable since crypto policies and keys are identical



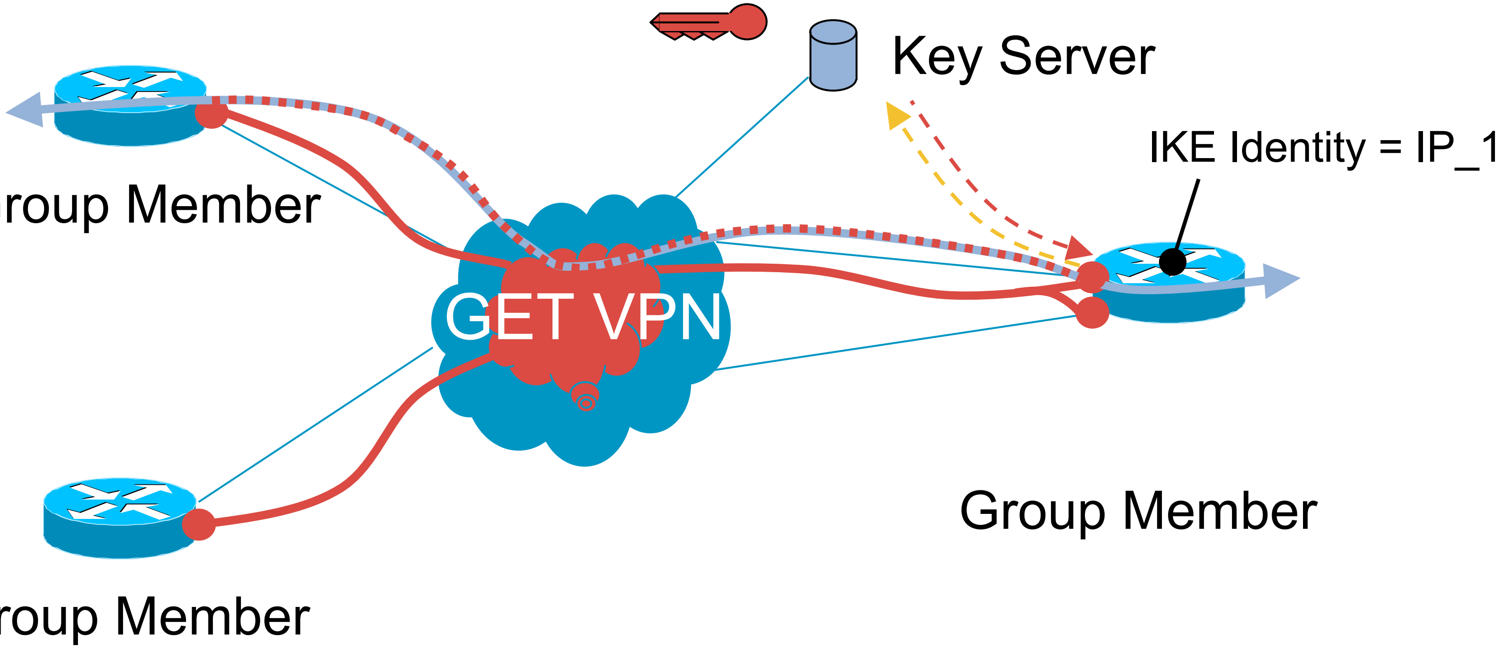
Redundant GET Interfaces: Multiple IKE Identities

- Key Server attempts to rekey each IKE Identity
- Key server fails to rekey downed interface and removes the IKE Identity from the database
- Both paths remain viable because at least one IKE identity succeeds in receiving rekey messages



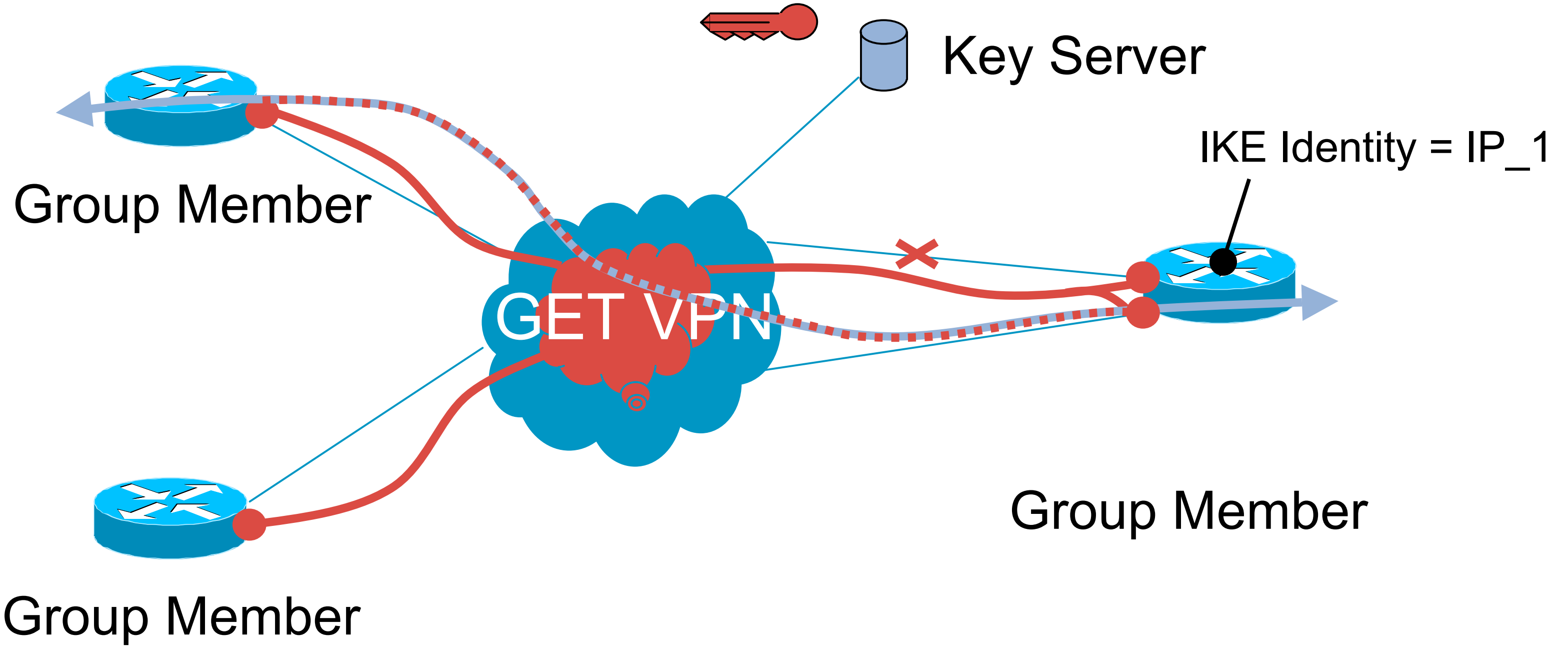
Redundant GET Interfaces: Single IKE Identity

- Common crypto map applied to two or more interfaces
- Common IKE Identity represents all interfaces
- Key Server manages state for single IKE identity for group member
- Data path may use either interface since the policies and keys are the same



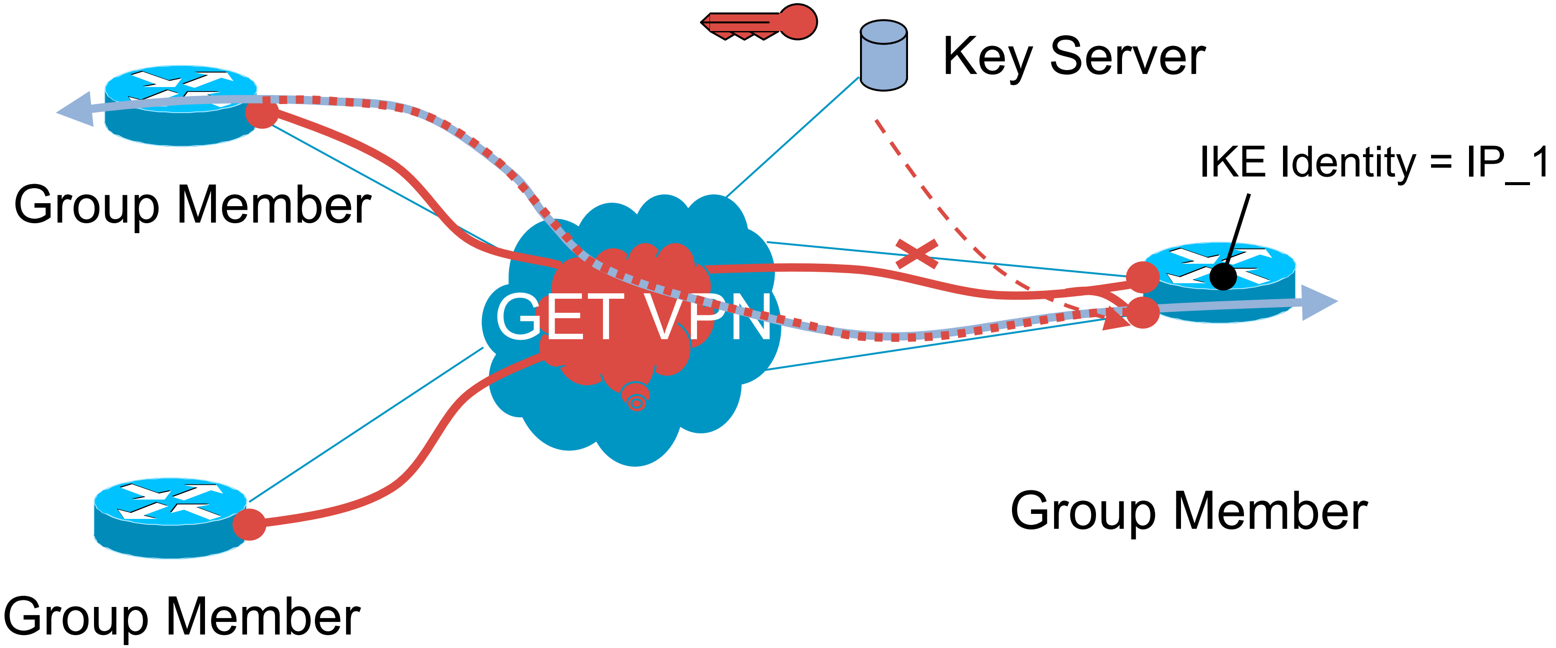
Redundant GET Interfaces: Single IKE Identity

- Failure of a GET-enabled interfaces causes routing convergence
- Alternate path chosen based on optimal calculated route
- Alternate path is immediately viable since crypto policies and keys are identical



Redundant GET Interfaces: Single IKE Identity

- Key Server attempts to rekey single IKE Identity
- Key server succeeds in rekeying common IKE Identity using alternate path
- Both paths remain viable because at common IKE identity succeeds in receiving rekey messages



Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

GET Network Transitions

GET Network Transitions

- Clear-text VPN

  An IP VPN that uses no encryption

- IPSec VPN

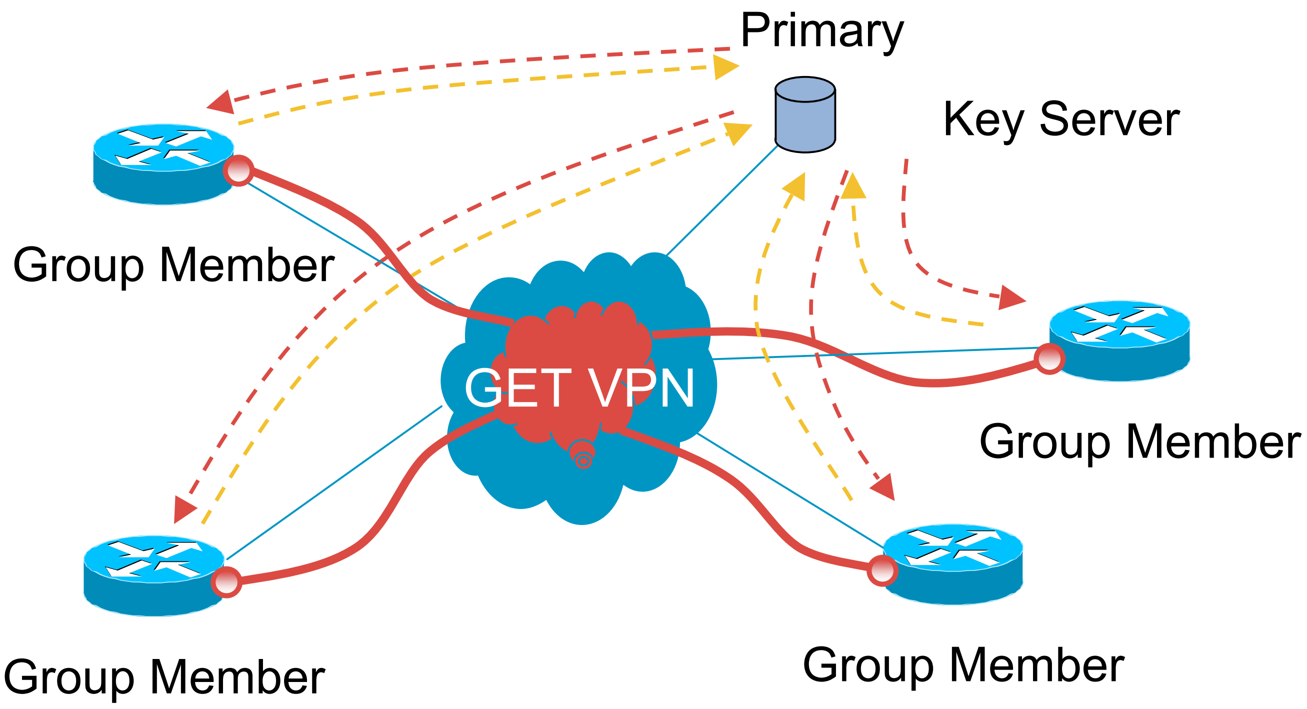
  An IP VPN that uses encryption with point to point IPSec security associations

- IPSec over GRE

  An IP VPN that applies encryption to point-to-point GRE

Clear-Text Transition

- Key Server configured to pre-position policies and keys using Receive-Only attribute
- Group members receive key material and policies allowing decryption, but do not perform encryption
- Each site can be incrementally added to the network until all the sites are members

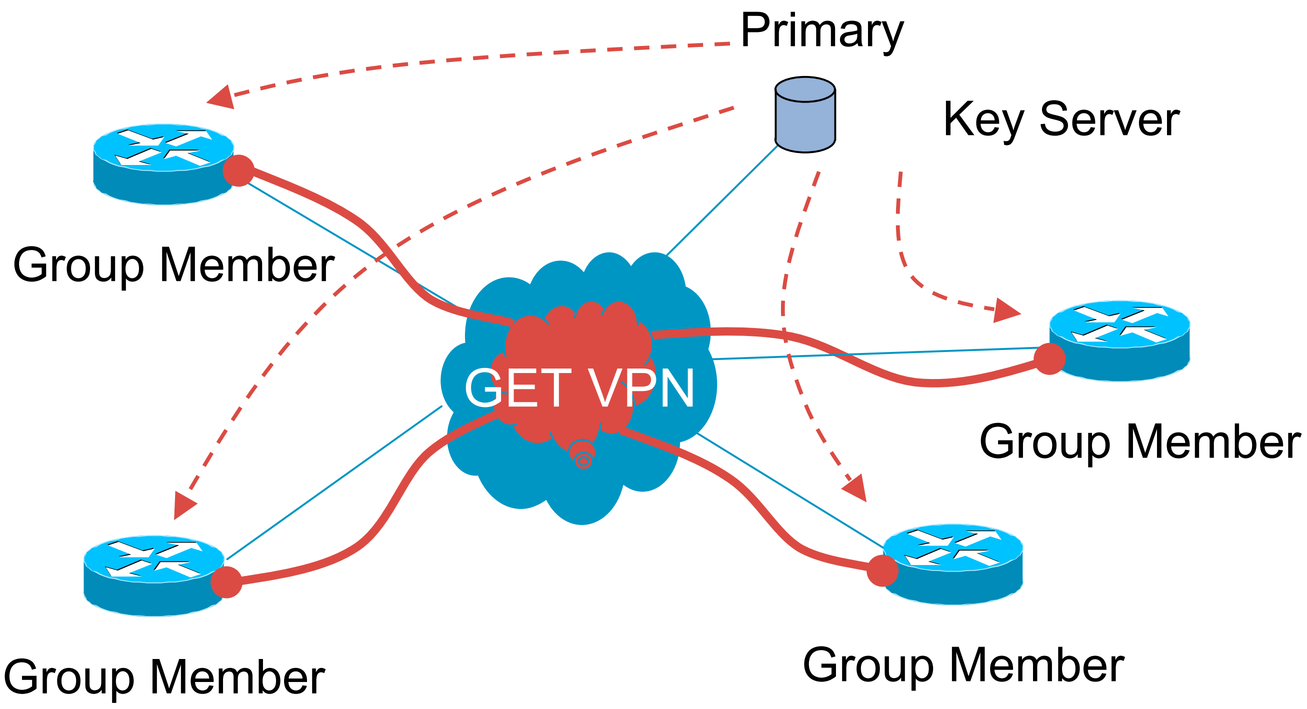


Clear-Text Transition

- Key Server has modified policy of removing Receive-Only attribute
- Key Server pushes new policy out to all group members
- Group members automatically transition to encryption

  Phase 1: Passive-Mode (encrypt while receiving encrypted or clear-text)

  Phase 2: Normal Mode (all encryption and decryption)



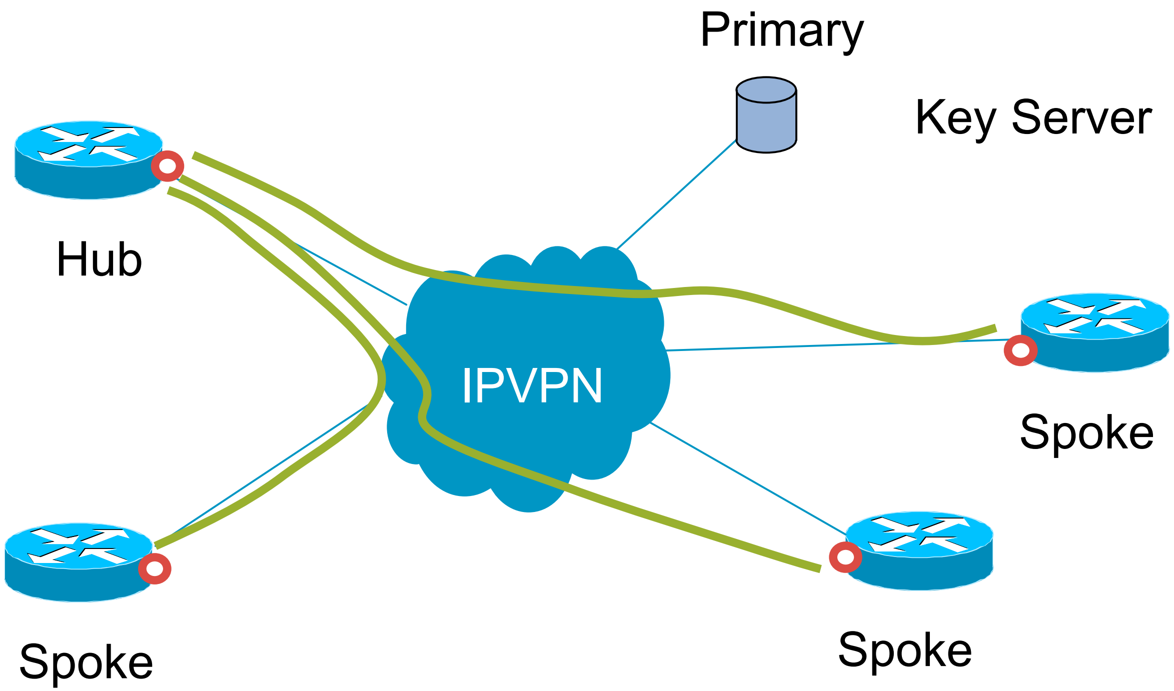
Clear-text Transition

- IPsec Crypto Maps
  1. Apply Group Association in Receive-Only Mode
  2. Removal of Receive-Only Statements
- All Peers GDOI Enabled Prior to Transition
- Transition through Passive-Mode to Receive-only Mode
- Symmetric Routing

```
crypto gdoi group diffint
 identity number 3333
 server local
   receive-only
```

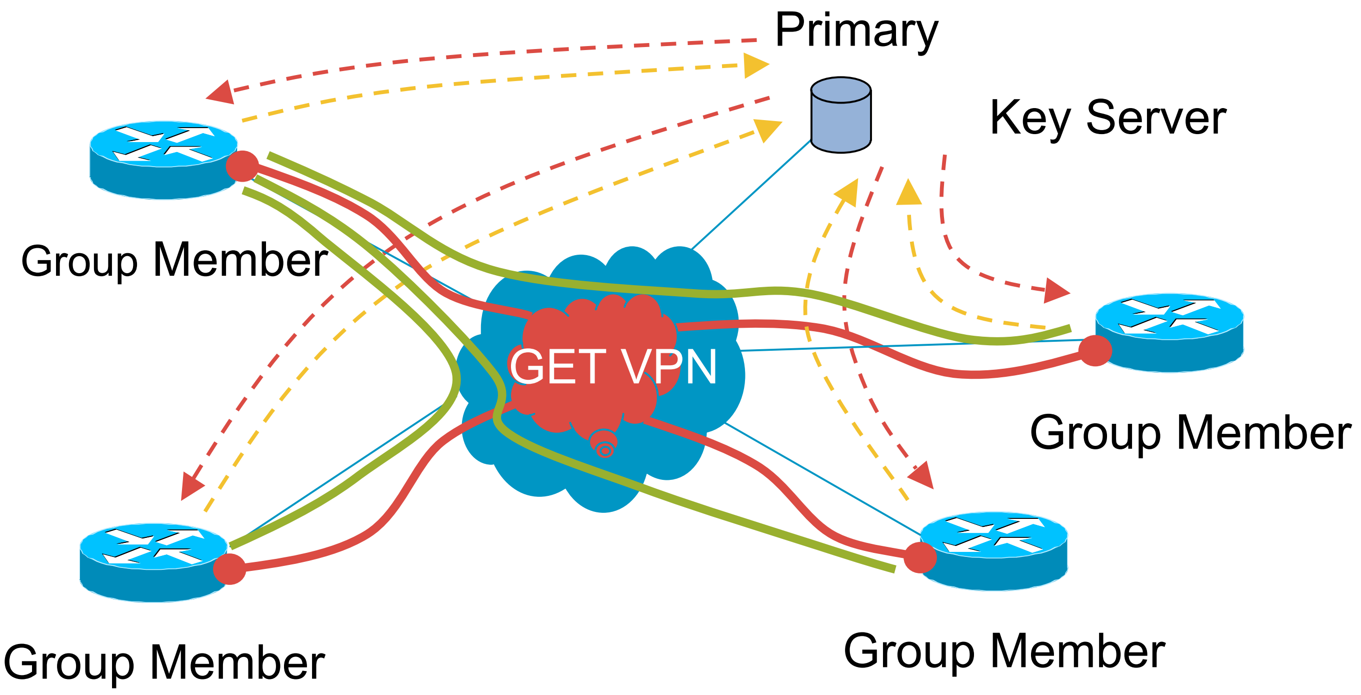
IPsec Transition

- Traditional Hub-and-Spoke IPSec VPN established using point-to-point IPSec Security Associations
- Key Server introduced to IP VPN environment



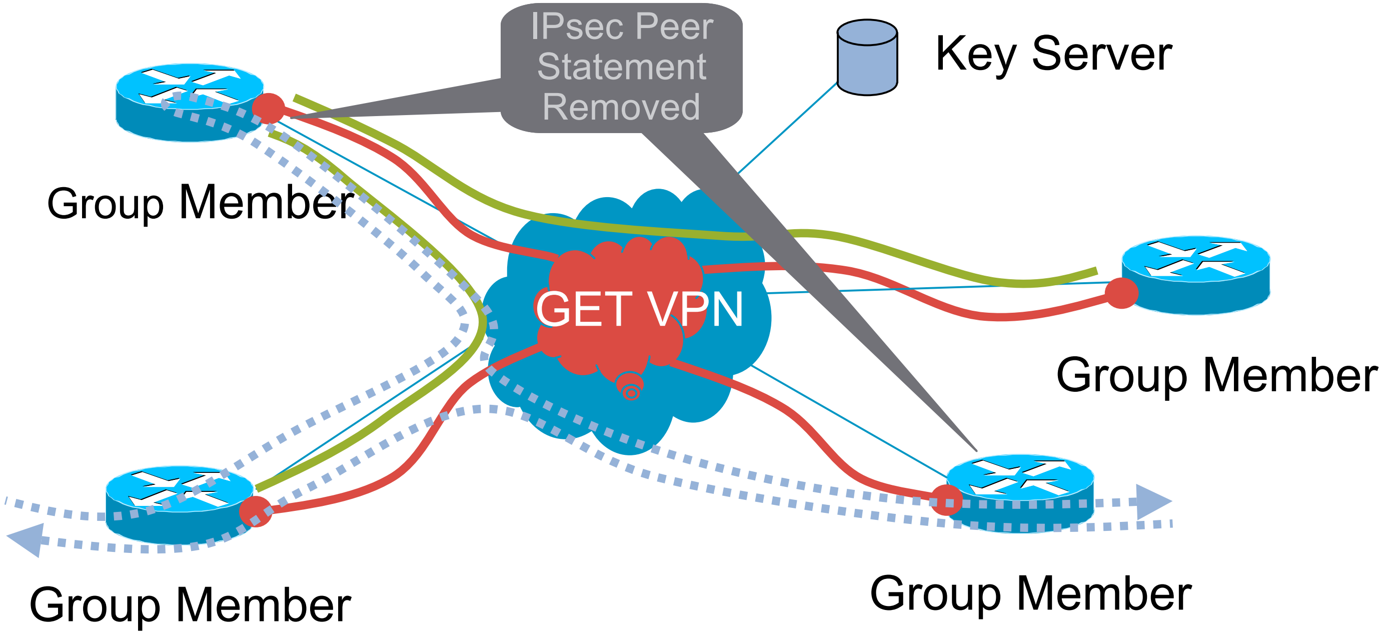
IPsec Transition

- Each site configured to support GET as the default protection mechanism (last entry on the crypto map list)
- Point-to-point IPsec connections remain the preferred protection mechanism



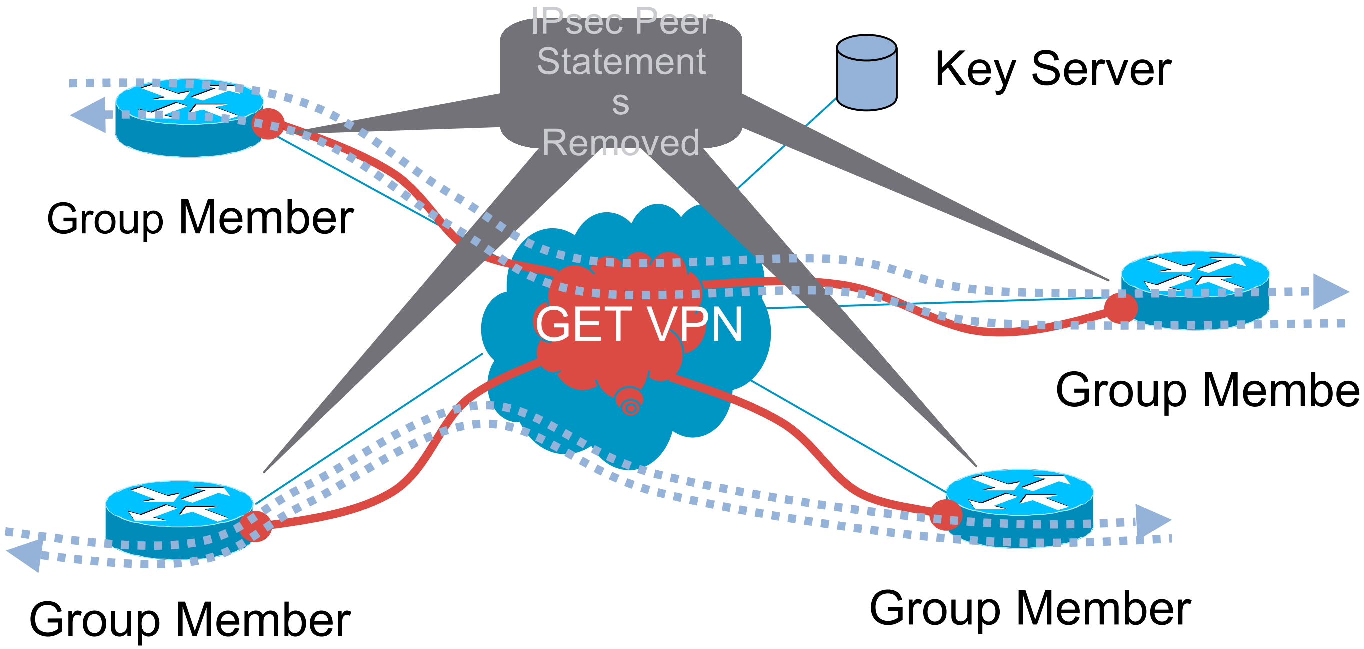
IPsec Transition

- Individual sites can have their point-to-point IPSec configurations removed along with the peer's reciprocal configuration
- Traffic flow will be asymmetric between converted and unconverted sites
- Traffic flow will be symmetric between converted sites and between unconverted sites



IPsec Transition

- All of the point-to-point IPSec security associations have been removed
- All of the sites have transitioned to the default GET VPN crypto map entry
- All traffic flow is symmetric and follows the optimal shortest path



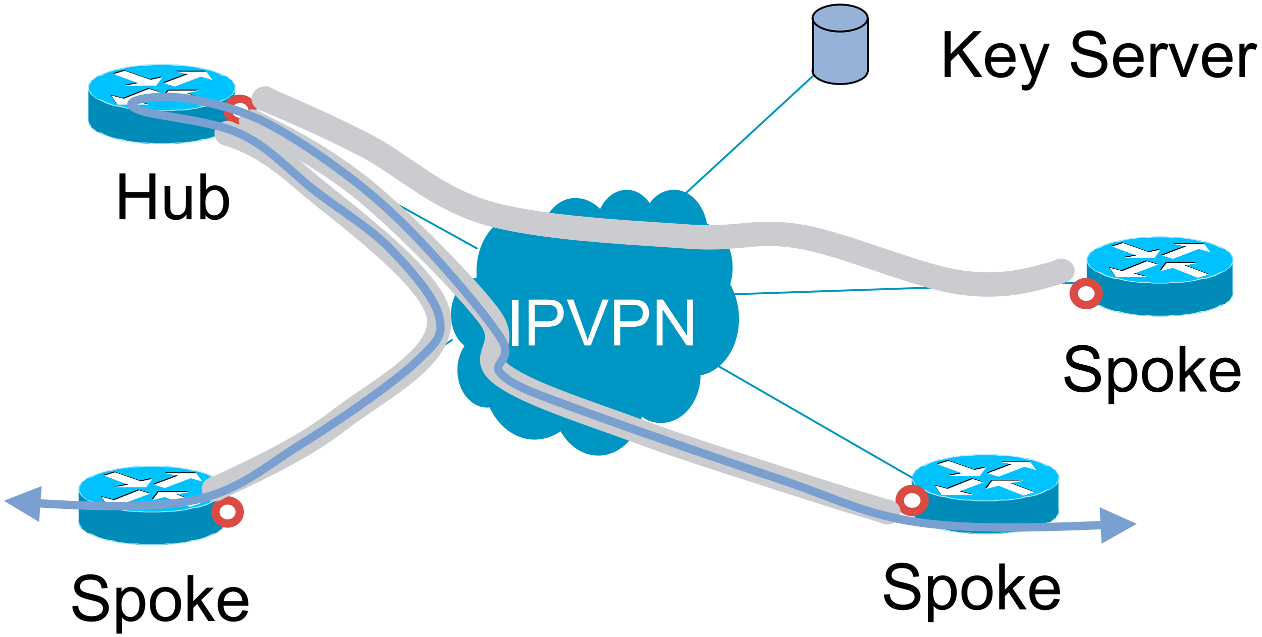
IPsec Transition

- IPsec Crypto Maps
  1. IPsec Point to Point Peers
  2. Addition of Group Association
  3. Removal of Point to Point Peer Statements
- All Peers GDOI Enabled Prior to Transition
- Asymmetric Routing during Transition

```
crypto map hub 10 IPsec-isakmp
  set peer 10.1.1.2
  set transform p2p-IPsec
  match address spoke1
crypto map hub 20 IPsec-isakmp
  set peer 10.1.2.2
  set transform p2p-IPsec
  match address spoke2
crypto map hub 30 gdoi
  set group wan
```

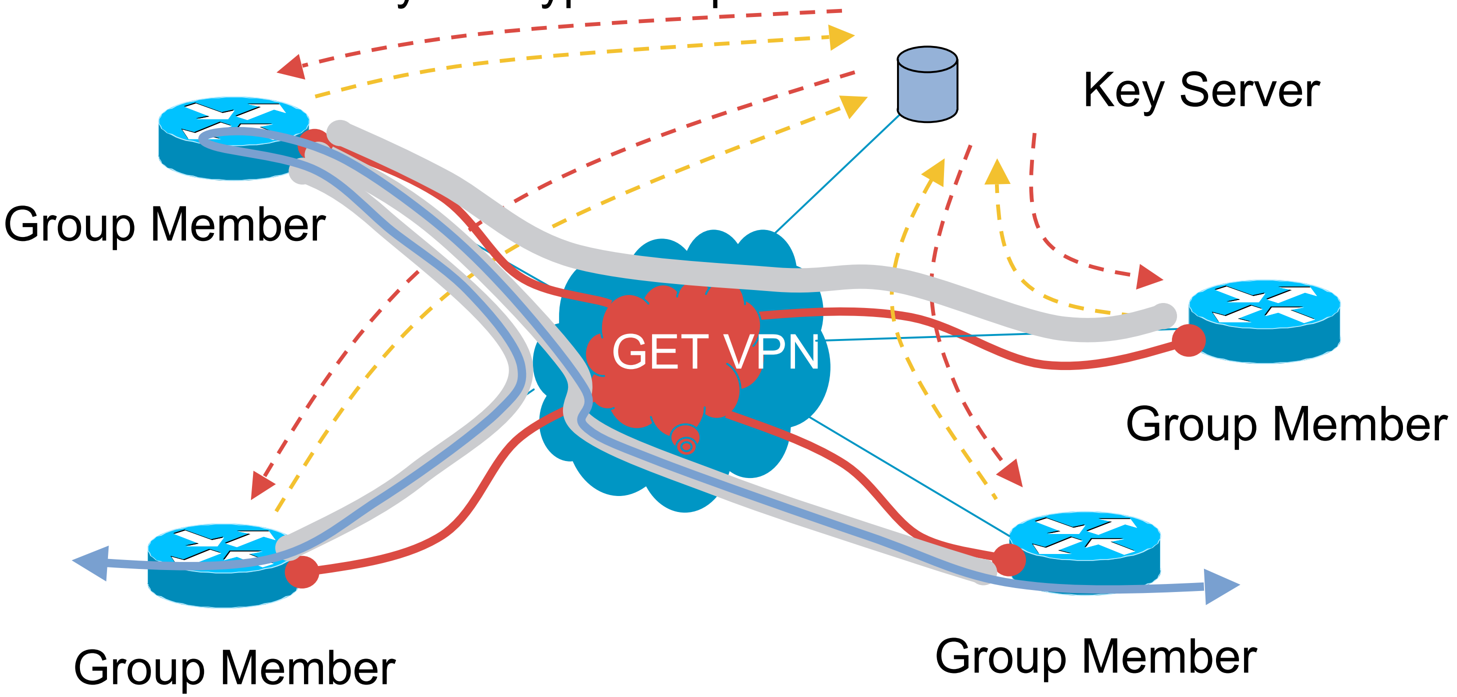
GRE+IPsec Transition

- Hub-and-Spoke GRE tunnels established with IPSec protection
  - Tunnel Protection applied to Tunnel Interface
  - Crypto Map applied to Physical Interface
- Key Server introduced to IP VPN



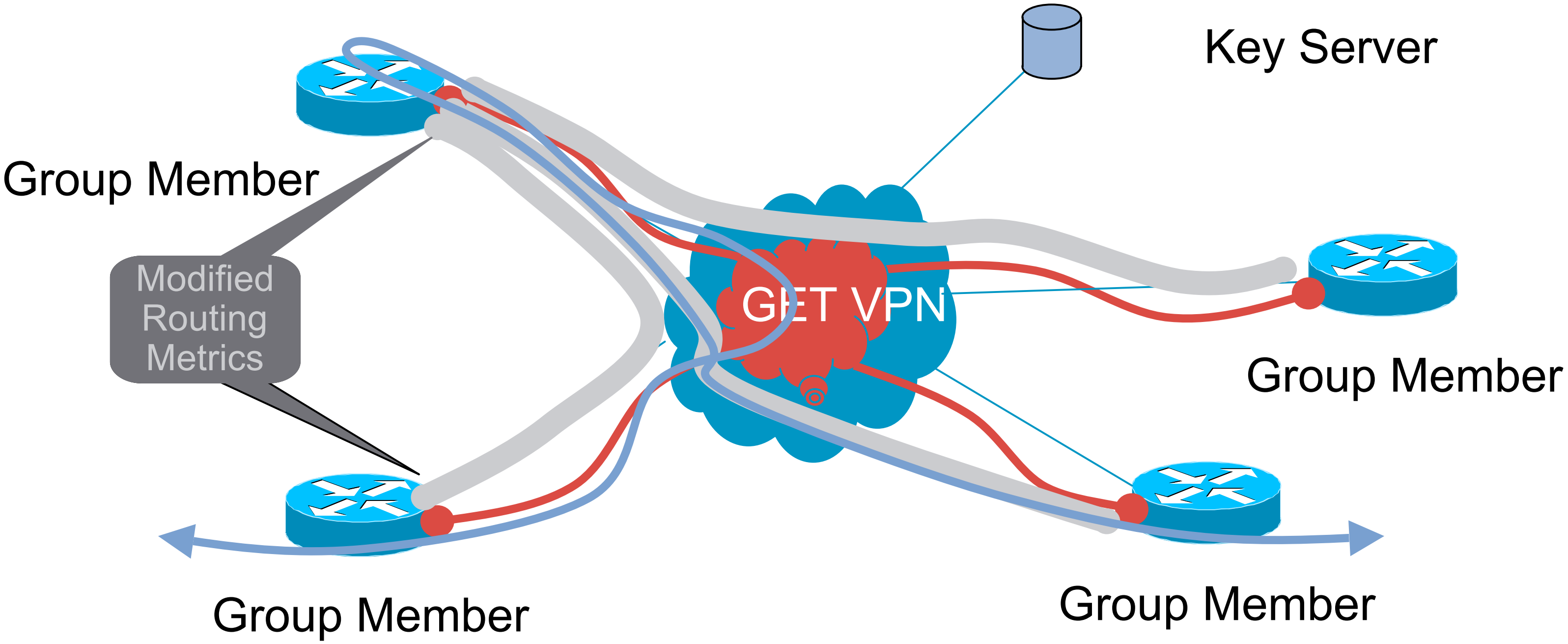
GRE+IPsec Transition

- Individual sites transitioned to GET VPN
  - GRE Tunnel Protection
    - GDOI crypto map excludes ESP traffic (i.e. GRE+IPSec)
  - Crypto Map Protection of GRE
    - GDOI last entry on crypto map list



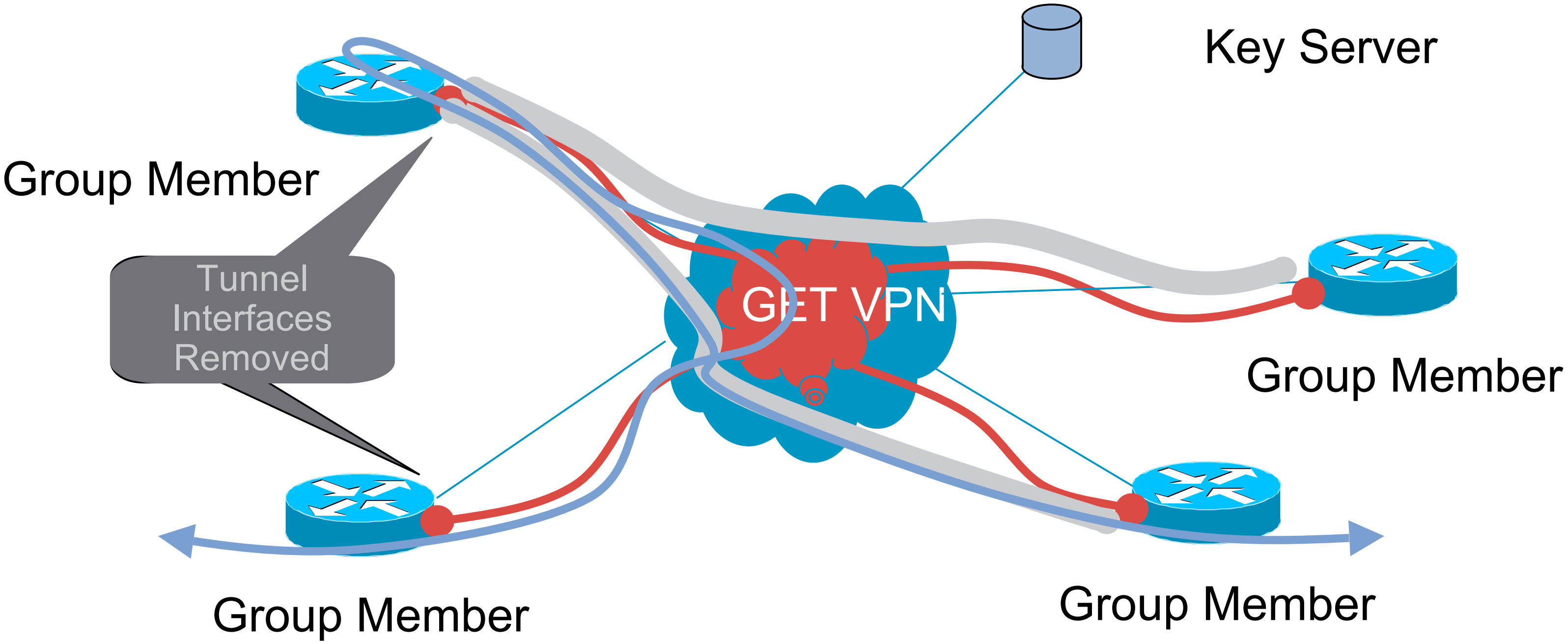
GRE+IPsec Transition

- Routing Metrics Modified on Tunnel Interfaces
- Routed Path Modified to include GET-enabled Core



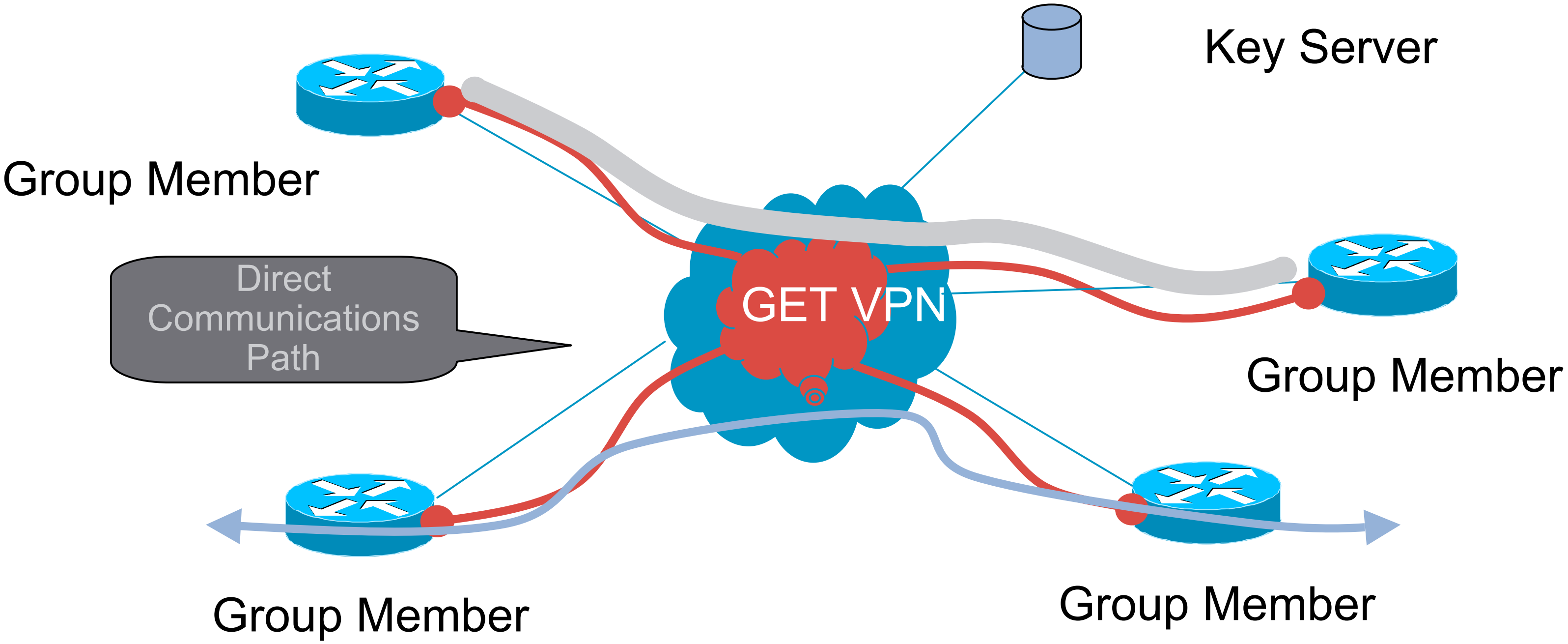
GRE+IPsec Transition

- GET-enabled interfaces are confirmed operational
- Tunnel interfaces can be removed on a per-peer basis



GRE+IPsec Transition

- GET-enabled interfaces are confirmed operational
- Tunnel interfaces can be removed on a per-peer basis



GRE+IPsec Transition

- GRE Protected Tunnels
  1. GRE/IPsec Peers
  2. Addition of Group Association
  3. Modified Routing Metrics
  4. Removal of GRE/IPsec Peers
- GDOI Enabled on Per Peer Basis Prior to Transition
- Symmetric Routing during Transition

```
interface tunnel 1
  tunnel protection IPsec profile gre
interface tunnel 2
  tunnel protection IPsec profile gre
interface serial 0
  crypto map get-vpn
```

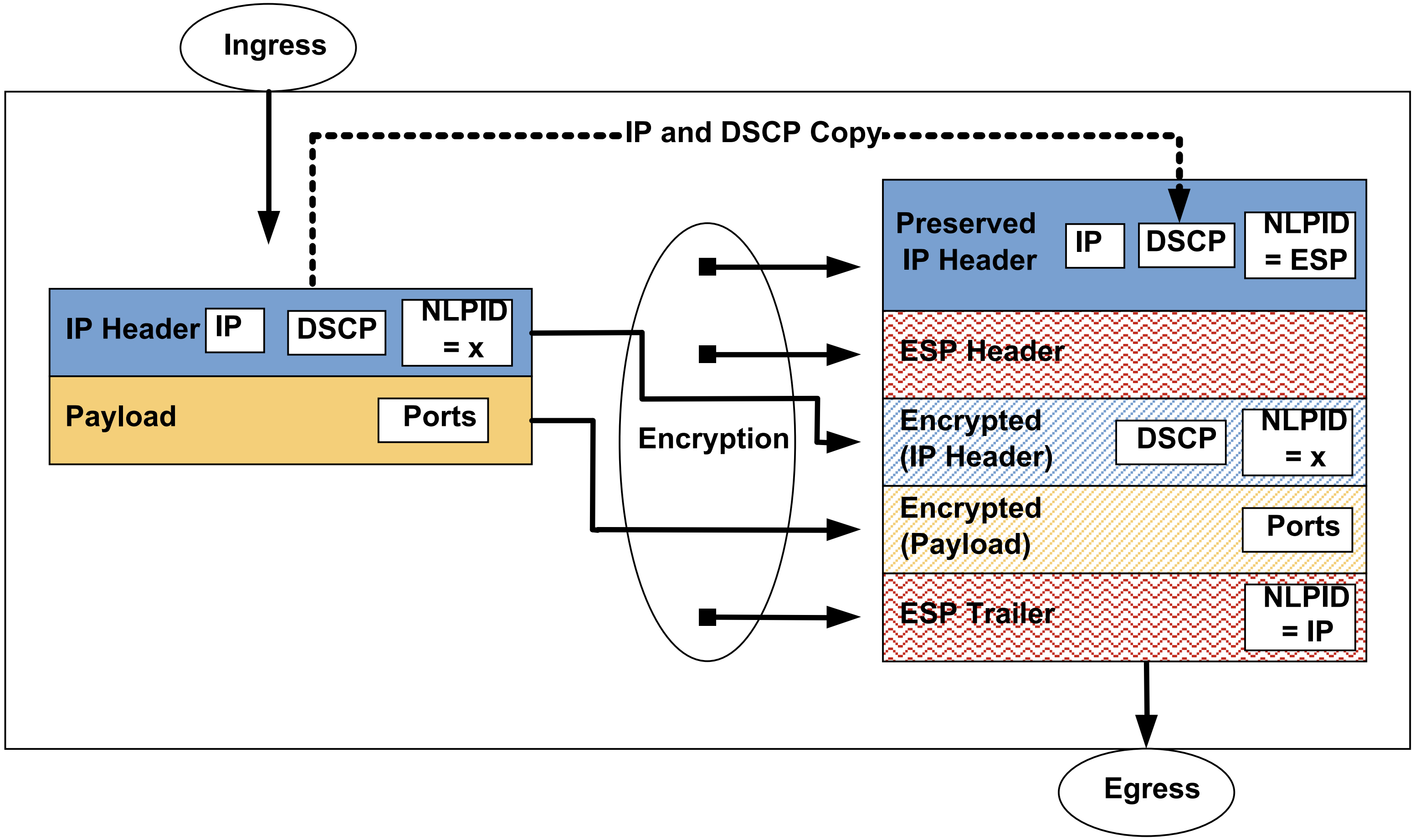
Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

Quality of Service Interoperability

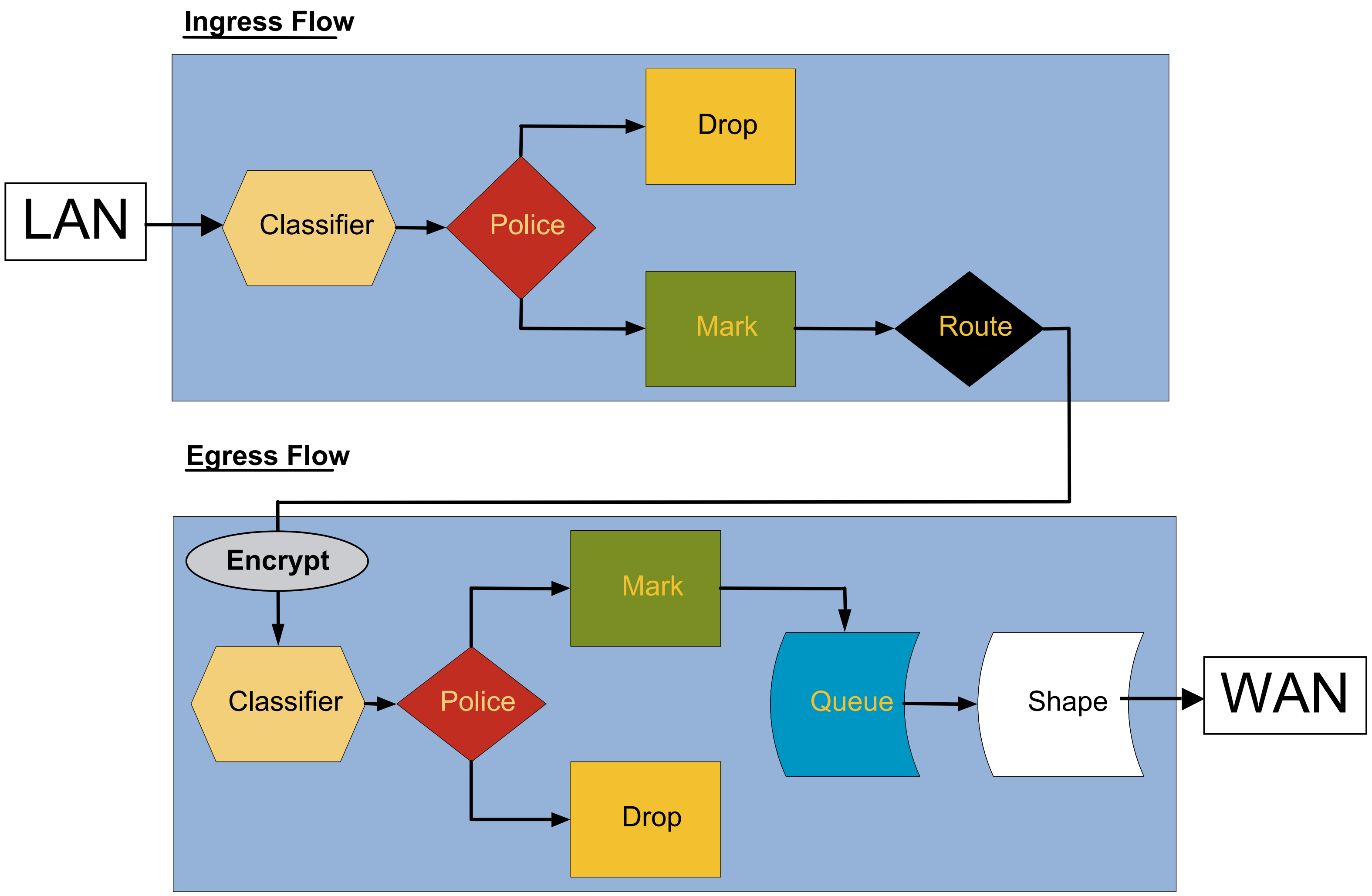
QoS-Enabled GET Interfaces

- Attributes
  - Original IP Header
    - Source_IP, Destination_IP, Protocol, S_Port, D_Port, DSCP
  - Preserved IP Header
    - Source_IP, Destination_IP, DSCP
- QoS Model Recommendations
  - Priority Queue and Class Queues
    - Private Ingress Interface – Classify, Mark
    - Public Egress Interface – Map, Queue, Encrypt

QoS Attribute Preservation



QoS Flow Model



Call Admission Control

- RSVP Messages must be interpreted by intermediate routers in order to be relevant
- Encapsulated RSVP messages
  - IPsec Tunnel Mode IP Address Preservation masks the RSVP IP Protocol ID of 46
  - Non-RSVP flags are set to indicated lack of end-to-end continuity of RSVP messaging
  - RSVP functions only on RSVP capable routers
- Hop-by-hop RSVP Messages
  - IPsec proxy can explicitly exclude protection of RSVP messages
    - deny udp any any eq 46
    - deny udp any eq 46 any
  - RSVP control plane operates in clear-text
  - Data plane operates in cipher-text

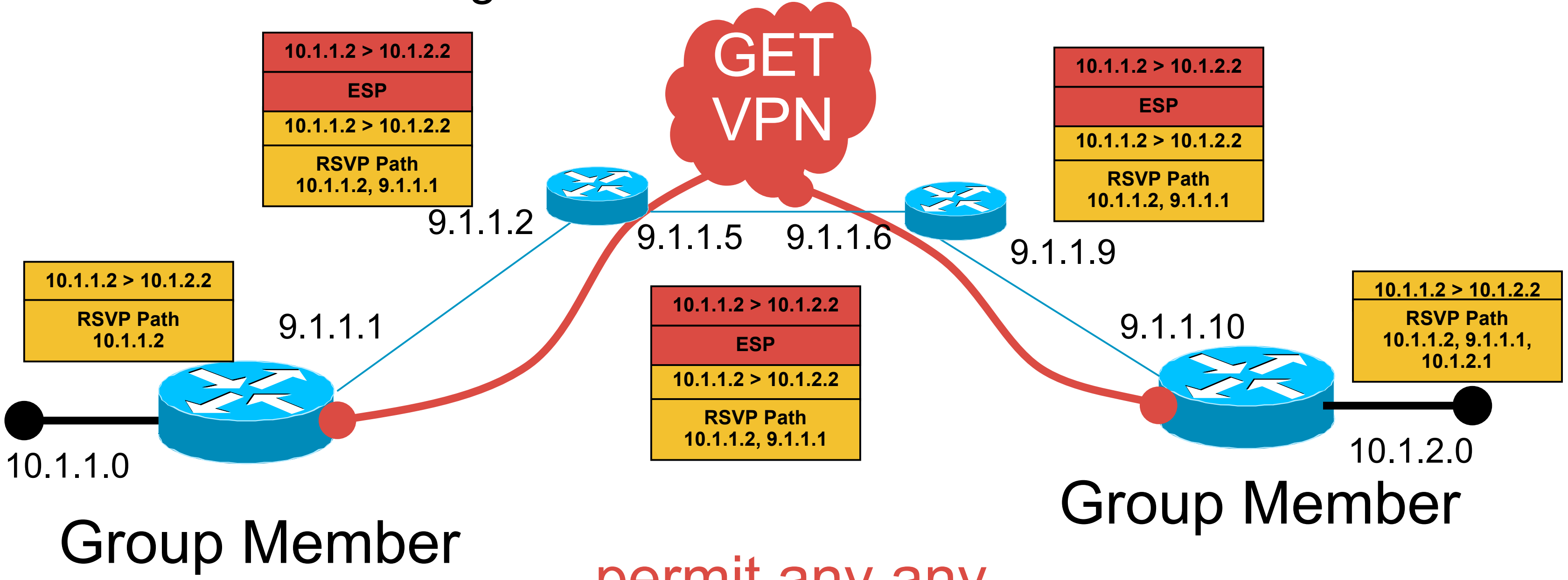
Encrypted Call Admission Control

- RSVP on ‘Non-RSVP Capable’ Path

  Reservation Request (PATH) in the Forward Direction using Original IP Header but Encrypted RSVP

  Intermediate routers have no visability to RSVP messages

  Path message excludes intermediate chain of routers



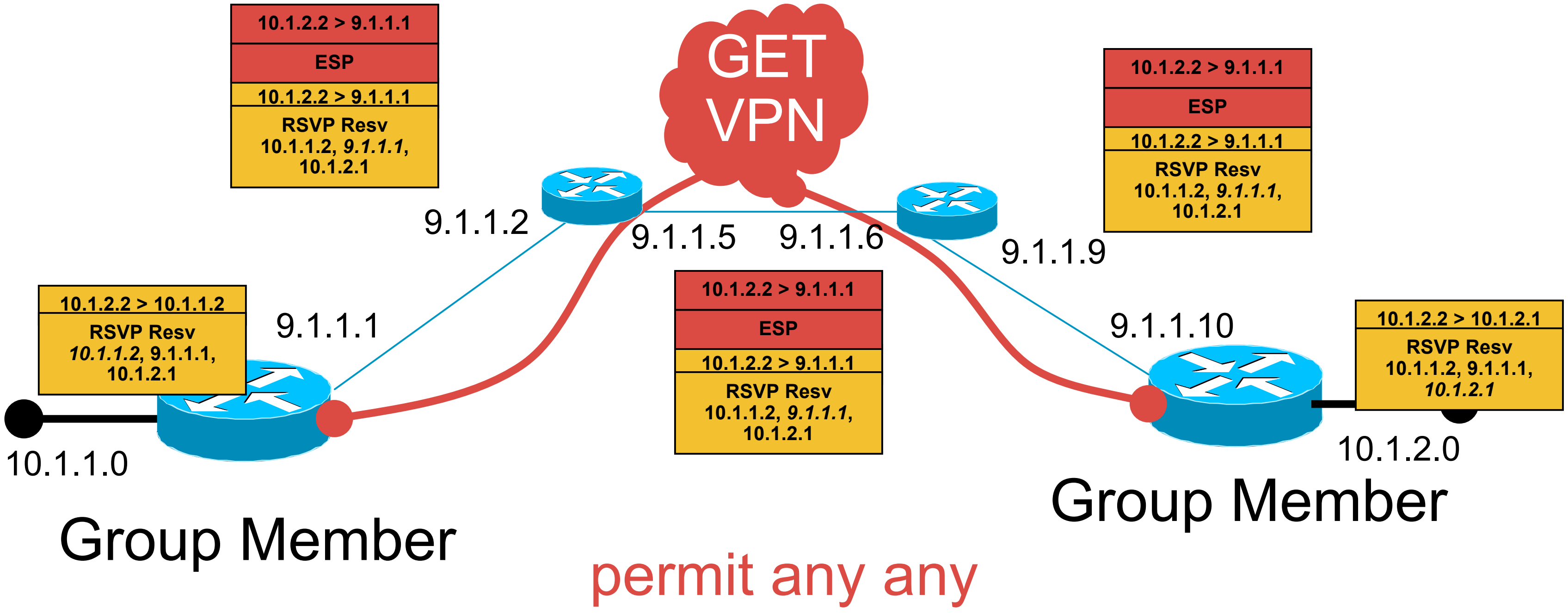
permit any any

Encrypted Call Admission Control

- RSVP on ‘Non-RSVP Capable’ Path

  Reservation Response (RESV) in the Reverse Direction using PATH Chain

  RESV directed back to last known RSVP-capable router



10.1.2.2 > 9.1.1.1
ESP
10.1.2.2 > 9.1.1.1
RSVP Resv
10.1.1.2, *9.1.1.1*,
10.1.2.1

10.1.2.2 > 9.1.1.1
ESP
10.1.2.2 > 9.1.1.1
RSVP Resv
10.1.1.2, *9.1.1.1*,
10.1.2.1

10.1.2.2 > 9.1.1.1
ESP
10.1.2.2 > 9.1.1.1
RSVP Resv
10.1.1.2, *9.1.1.1*,
10.1.2.1

10.1.2.2 > 10.1.1.2
RSVP Resv
10.1.1.2, 9.1.1.1,
10.1.2.1

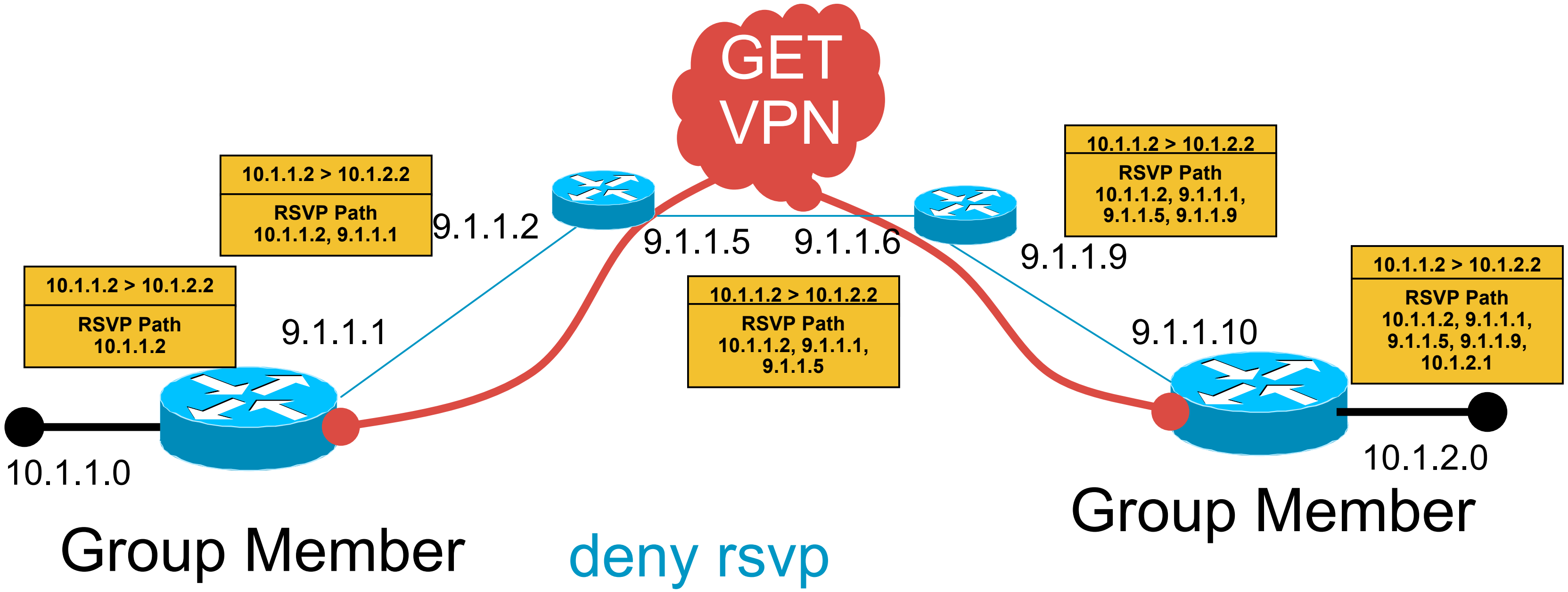
10.1.2.2 > 10.1.2.1
RSVP Resv
10.1.1.2, 9.1.1.1,
10.1.2.1

Clear-text Call Admission Control

- Int-Serv RSVP

  Hop-by-hop Reservation Request (PATH) in the Forward Direction using Original IP Header but Encrypted RSVP

  Hop-by-hop Reservation Response (RESV) in the Reverse Direction using PATH Chain



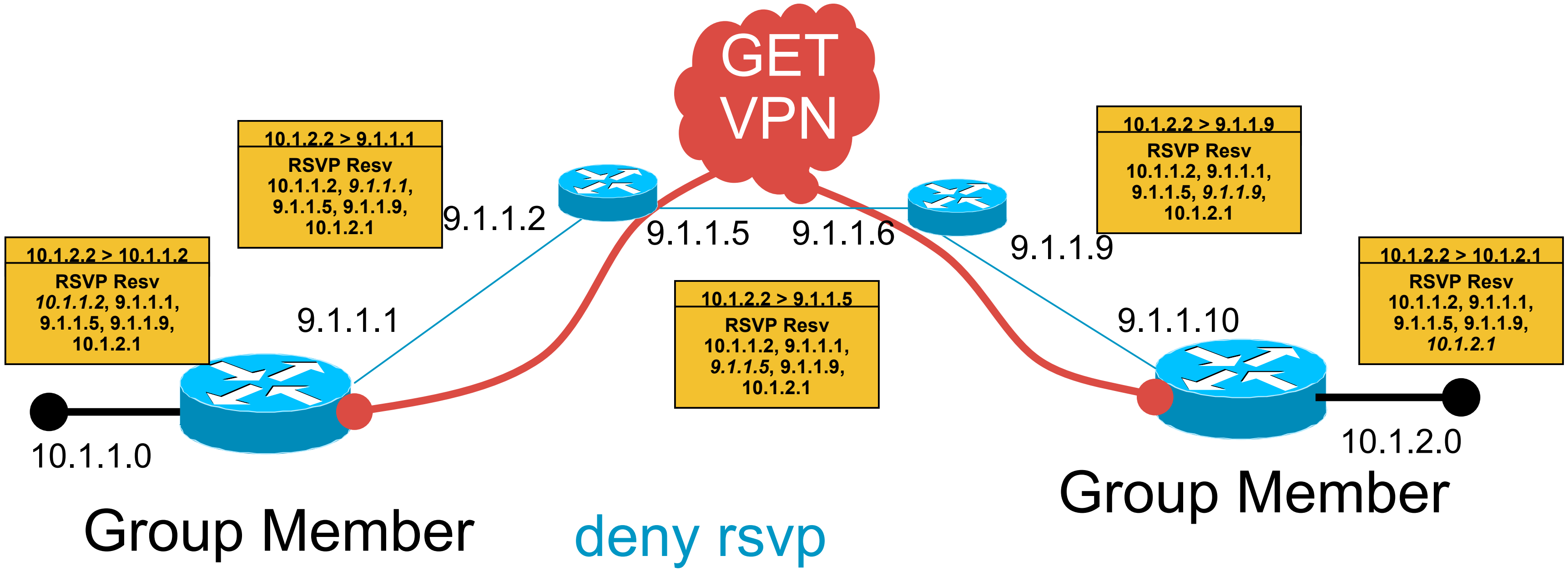
deny rsvp
permit any any

Clear-text Call Admission Control

- Int-Serv RSVP

  Hop-by-hop Reservation Request (PATH) in the Forward Direction using Original IP Header but Encrypted RSVP

  Hop-by-hop Reservation Response (RESV) in the Reverse Direction using PATH Chain



10.1.2.2 > 10.1.1.2
RSVP Resv
10.1.1.2, 9.1.1.1, 9.1.1.5, 9.1.1.9, 10.1.2.1

10.1.2.2 > 9.1.1.1
RSVP Resv
10.1.1.2, *9.1.1.1*, 9.1.1.5, 9.1.1.9, 10.1.2.1

10.1.2.2 > 9.1.1.5
RSVP Resv
10.1.1.2, 9.1.1.1, *9.1.1.5*, 9.1.1.9, 10.1.2.1

10.1.2.2 > 9.1.1.9
RSVP Resv
10.1.1.2, 9.1.1.1, 9.1.1.5, *9.1.1.9*, 10.1.2.1

10.1.2.2 > 10.1.2.1
RSVP Resv
10.1.1.2, 9.1.1.1, 9.1.1.5, 9.1.1.9, *10.1.2.1*

deny rsvp
permit any any

Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

Multicast Architecture

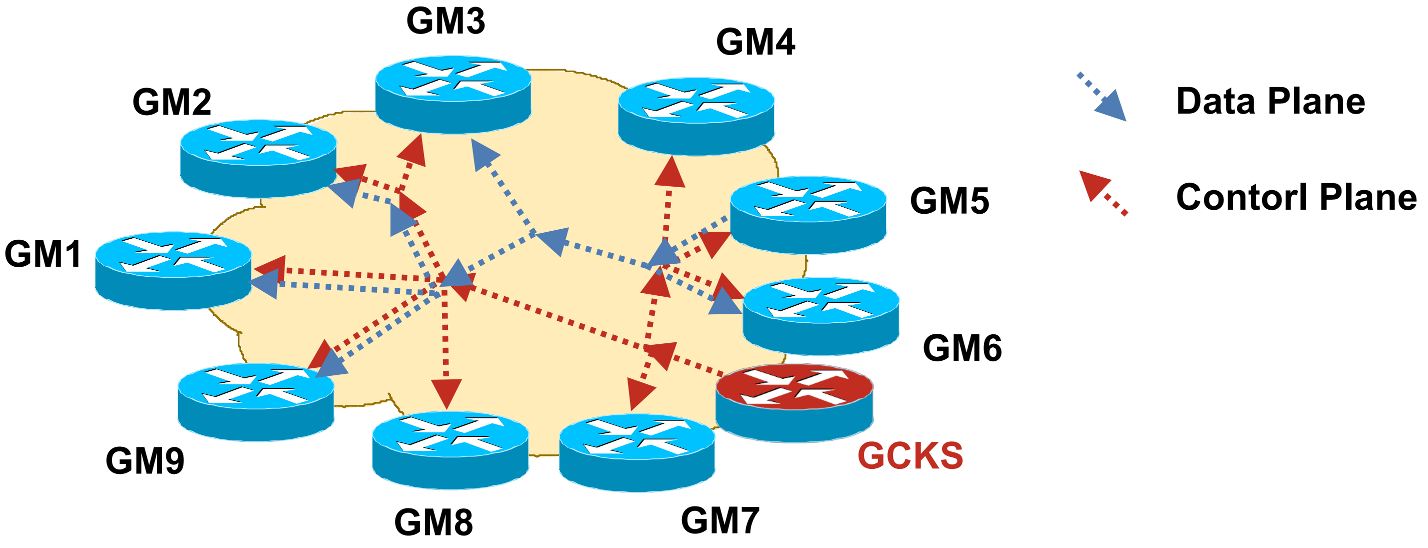
Multicast Security Architecture

- Recommended Multicast Infrastructure

  Data Plane May use PIM-SM, PIM-BiDir, SSM, etc.

  Control Plane (i.e. GDOI Rekey) should use PIM-SM, PIM-DM, or PIM-BiDir

  PIM-SSM is not supported for GDOI Rekeys



PIM-SM Recommendations

- PIM-SM for Data Plane

  Insure data plane RP's are protected by a group member

  PIM-Register is a multicast packet in a unicast tunnel so insure IPsec proxy includes unicast flows

  Source and RP must be protected by Group Policy (i.e. unicast)

  Insure Auto-RP for data plane does not serve multicast rekey group

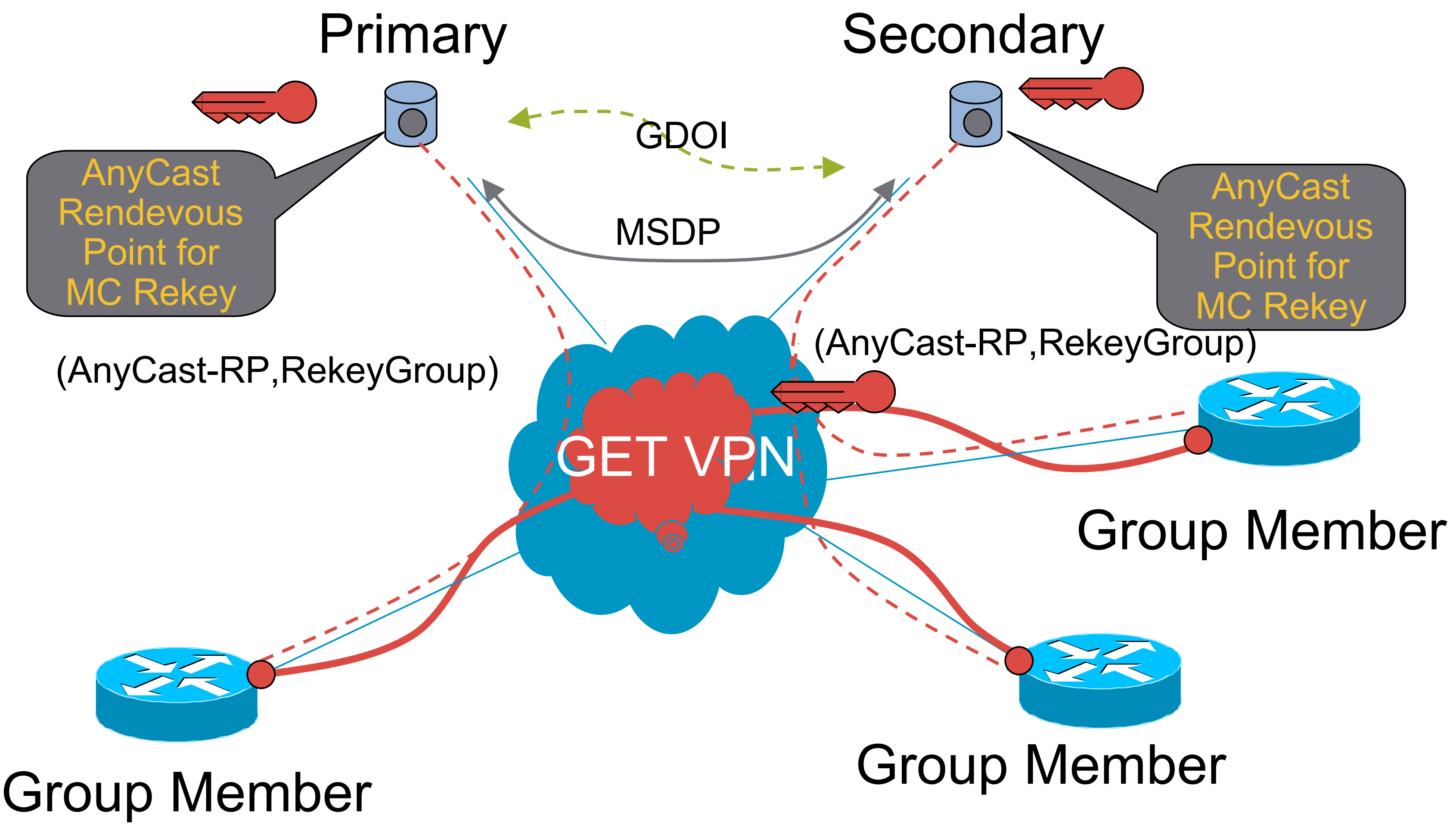
- PIM-SM for Control Plane

  Use AnyCast RP on Key Servers for multicast rekey only

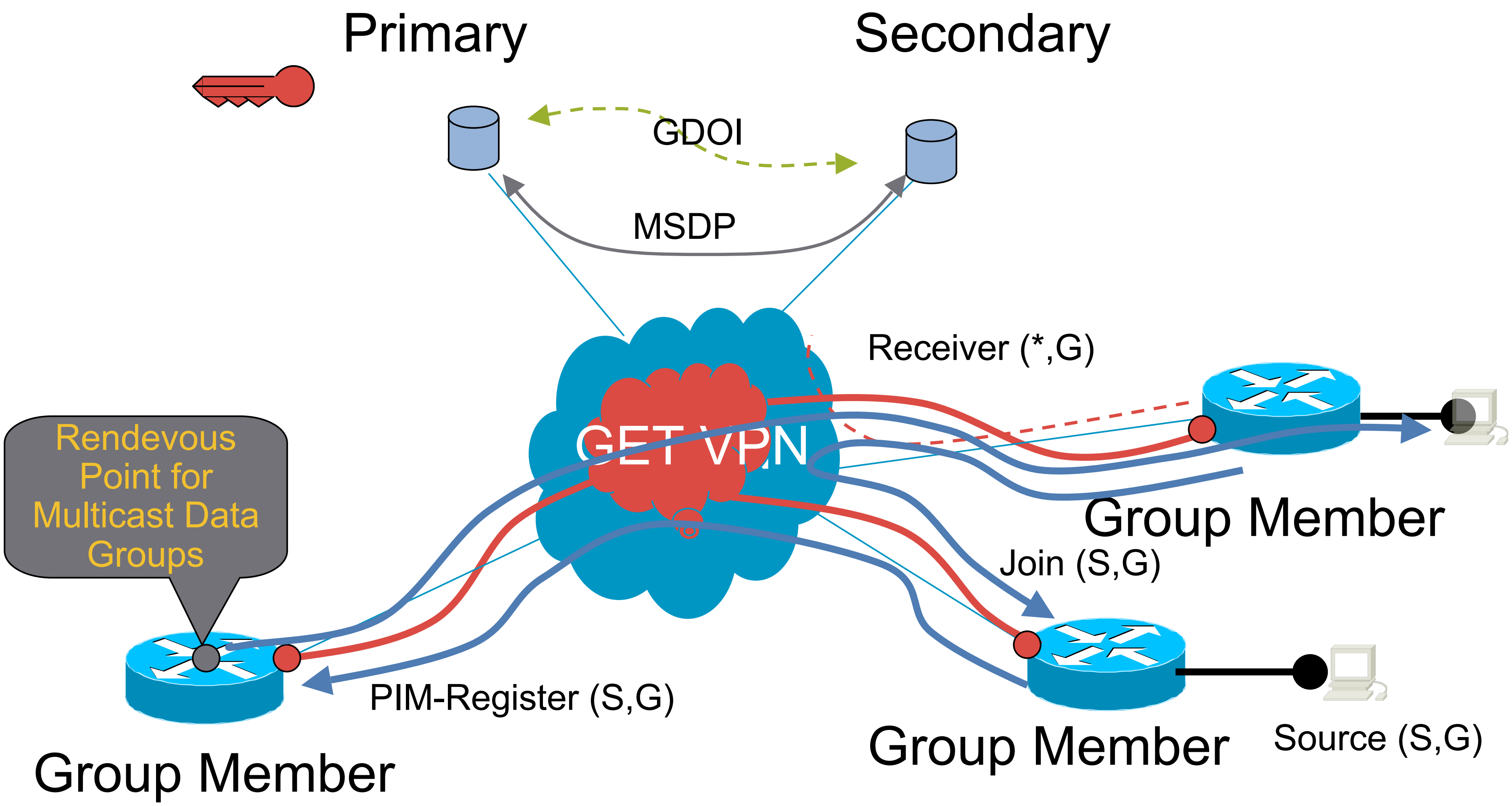
  Use MSDP Between Key Servers

  Static RP assignment on group members pointing to AnyCast RP address

PIM-SM Multicast Rekey



PIM-SM Multicast Data Plane



Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

Operational Support

Operational Support

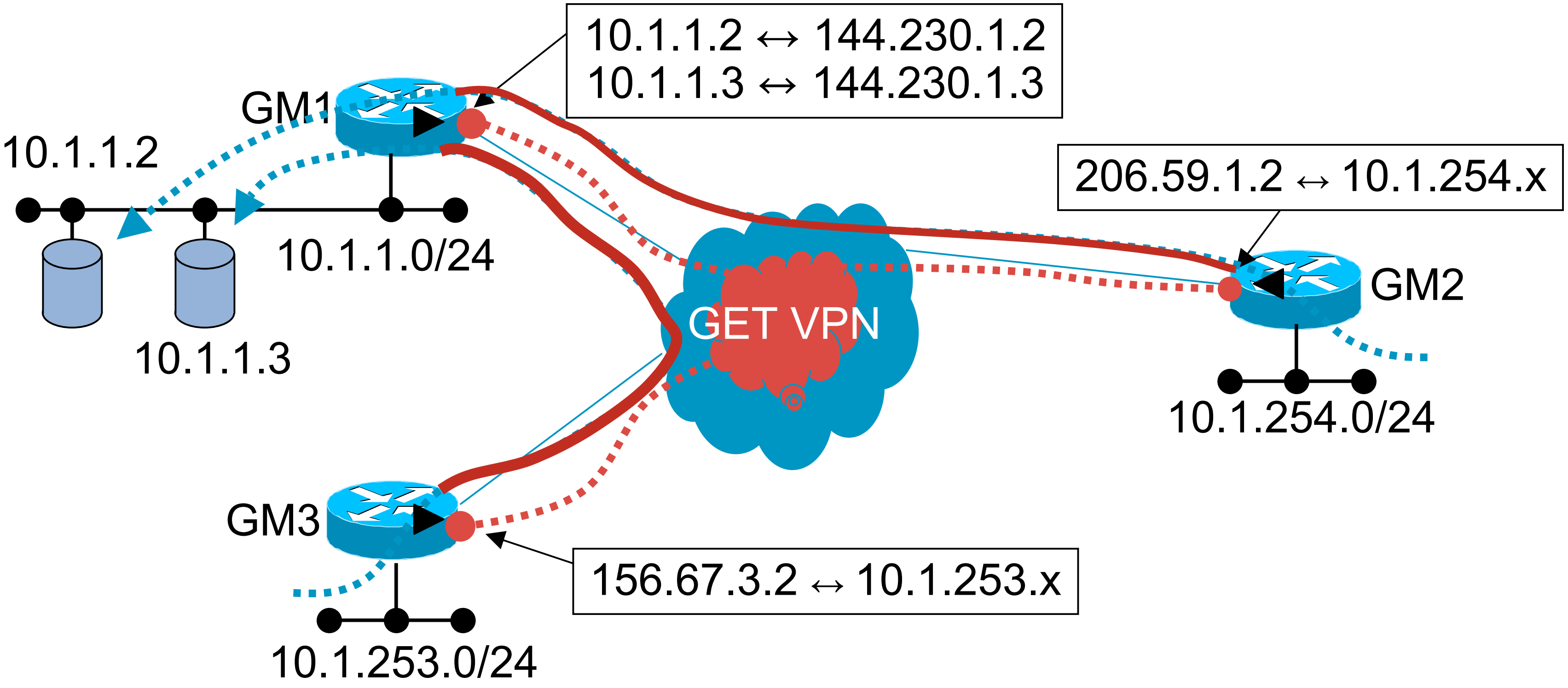
- Caveats and Limitations
- Deployment Example
- Management Methods
- Caveats and Limitations

Fragmentation and MTU

- Issues for Large Frames
  - Lack of Tunnel Interface
  - No Path MTU Discovery from WAN
  - Multicast Can’t use Path MTU Discovery
- Tools for Treatment of Large Frames on WAN
  - Look Ahead Fragmentation (LAF)
    - Fragment large frames before encryption on VPN Gateway
  - TCP MSS Settings
    - Set TCP MSS value 100 Bytes smaller than smallest MTU on WAN
  - DF Clear
    - Clear the DF bit on frames to allow LAF

Network Addressing (NAT)

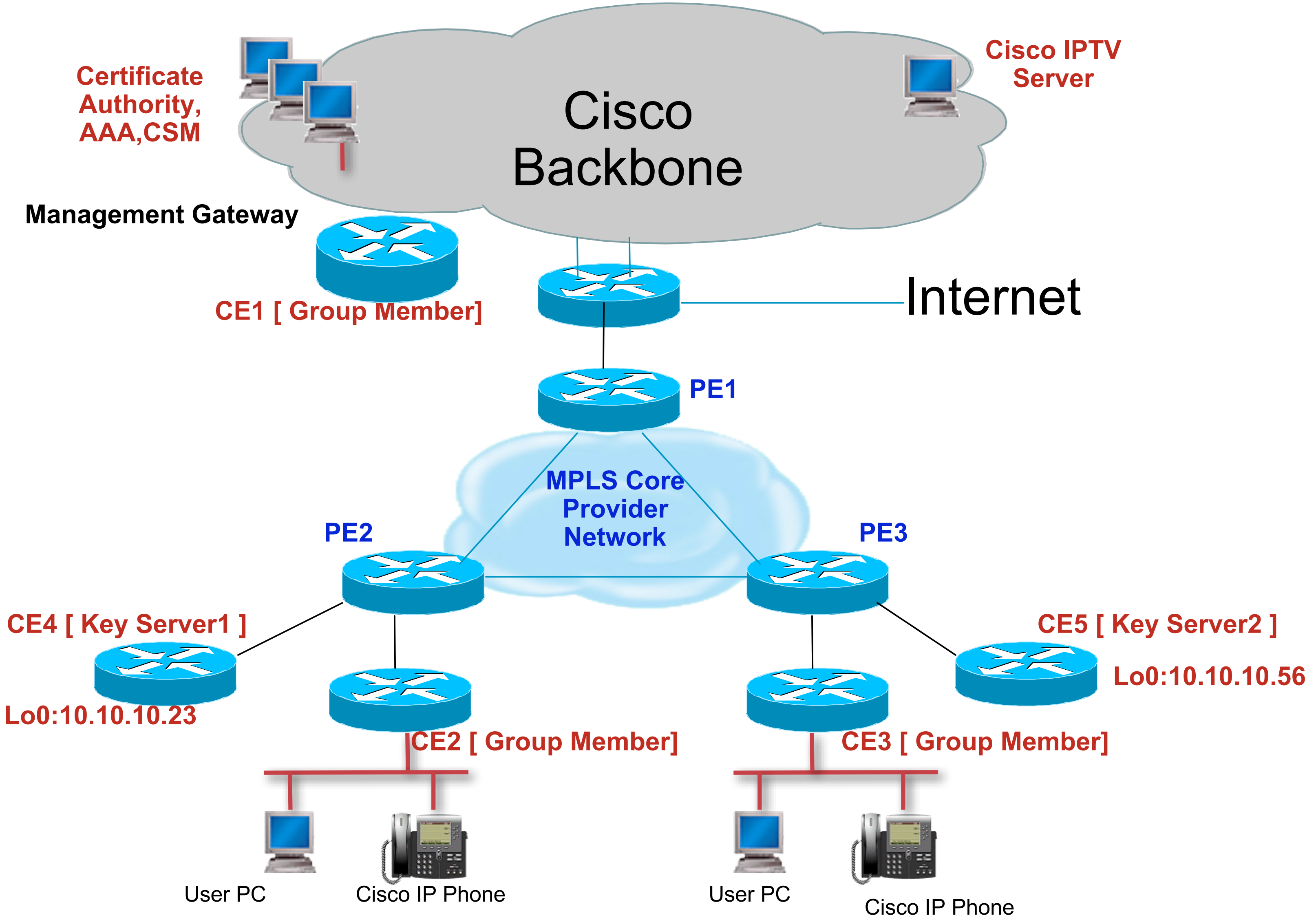
- NAT/PAT – translation BEFORE encryption and AFTER decryption
- NAT/PAT between encryption and decryption prevents return traffic!
- IPSec Policy – 'permit ip any any' allows PAT on dynamically assigned IP addresses
- Client-to-Server (i.e. Web, POP3, DNS) – Assigned Static Translations
- Client-to-Client – Not viable without Static Translations



Operational Support

- Caveats and Limitations
- Deployment Example
- Management Methods
- Platforms Supported

Deployment – Private MPLS core based



Key server (contd.)

```
crypto gdoi group GETVPN-ALPHA                                  // GET VPN Group defined //
 identity number 1357924680
 server local                                                   // This router as Key server //
  rekey address ipv4 getvpn-rekey-multicast-group               // Multicast group for rekey //
  rekey lifetime seconds 10800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa                    // RSA key used for rekey //
  rekey transport unicast                                       // Rekey using Unicast //
  sa ipsec 1
   profile getvpn
   match address ipv4 sa-acl                                    // policy defined by sa-acl //
   replay time window-size 5                                    // time based anti-replay //
  address ipv4 10.10.10.23                                      // used as rekey source address //
  redundancy                                                    // enables co-operative key server //
   local priority 100                                           // to define primary //
   peer address ipv4 10.10.10.56                                // secondary key server address //
   protocol retransmit 2 timeout periodic 30 role 30 sec-peruser 5 refresh 20 pri-peruser 5
                                                                // co-op timers //
```

Key server … (contd.)

```
ip access-list extended getvpn-rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848 // rekey multicast group ks_1 //
 permit udp host 10.10.10.56 eq 848 host 239.192.1.190 eq 848 // rekey multicast group ks_2 //

ip access-list extended sa-acl
 deny   ip any host 239.192.1.190                 // excludes multicast rekey traffic from TEK encryption //
 deny  ip 10.1.1.224 0.0.0.31 10.5.5.96 0.0.0.31   // excludes management traffic from TEK encryption //
 deny  ip 10.5.5.96 0.0.0.31 10.1.1.224 0.0.0.31   // excludes management traffic from TEK encryption //
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255         // encrypt unicast dataplane
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255        // encrypt unicast dataplane
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255        // encrypt unicast dataplane
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255         // encrypt unicast dataplane
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255        // encrypt unicast dataplane
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255        // encrypt unicast dataplane
    …                                          // Removed some more corporate networks entries for simplicity //
 permit ip any 239.192.0.0 0.0.255.255                 // encrypt multicast dataplane
```

Group Member Configuration

```
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto gdoi group getvpn                    // GET VPN  group defined //
 identity number 1357924680
 server address ipv4 10.10.10.56
 server address ipv4 10.10.10.23
!
crypto map gdoi 1 gdoi
 set group getvpn
 match address no-encryption-acl
 qos pre-classify
crypto map gdoi 2 ipsec-isakmp              // management tunnel //
 description Management Tunnel
 set peer x.x.x.x                 < Address removed >
 set transform-set mgmt-3des
 match address mgmt_acl
!
Interface Loopback0
 description Management interface
 ip address 10.1.1.227 255.255.255.255
!
```

Group Member (contd.)

```
interface Vlan10
 description Inside interface
 ip address 10.1.1.1 255.255.255.128
 ip pim sparse-dense-mode
 ip inspect test in
 ip tcp adjust-mss 1360
!
interface GigabitEthernet0/0
 description outside interface
 ip address 10.10.10.14 255.255.255.252
 ip access-group fw_acl in
 ip pim sparse-dense-mode
 ip tcp adjust-mss 1360
 duplex auto
 speed auto
 media-type sfp
 no keepalive
 crypto map gdoi
 service-policy output shaper
!
ip access-list extended no-encryption-acl
 deny   ip host 10.10.10.14 host 10.10.10.13          // excludes CE-PE traffic from group key encryption //
 deny   ip 10.1.1.0 0.0.0.255 host 10.10.10.23
 deny   ip any host 239.192.1.190           // optional, excludes multicast rekey from group key encryption //
ip access-list extended mgmt_acl              // only management traffic goes via management tunnel //
 permit ip host 10.1.1.225 10.5.5.96 0.0.0.31
```

Group Member (contd.)

```
ip access-list extended fw_acl
 permit esp any any
 permit udp any any eq 848                                     // for GDOI registration //
 permit udp any any eq isakmp                                  // for management tunnel //
 permit tcp 10.10.10.0 0.0.0.255 eq bgp 10.10.10.0 0.0.0.255
 permit tcp 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 eq bgp
 permit pim any any
 permit igmp any any
 permit udp any host 224.0.1.39
 permit udp any host 224.0.1.40
 permit ip 10.5.5.96 0.0.0.31 10.10.10.0 0.0.0.255
 permit tcp host 10.10.10.23 host 10.10.10.14 eq telnet
 permit tcp host 10.10.10.23 host 10.10.10.14 eq 22
 permit tcp host 10.10.10.56 host 10.10.10.14 eq telnet
 permit tcp host 10.10.10.56 host 10.10.10.14 eq 22
 permit udp host 10.5.5.97 eq ntp any
 permit udp host 192.5.41.40 eq ntp any
 permit udp any any eq bootpc
 permit tcp any eq tacacs host 10.10.10.14
 permit icmp any any
 deny   ip any any log
```

Operational Support

- Caveats and Limitations
- Deployment Example
- Management Methods
- Platforms Supported

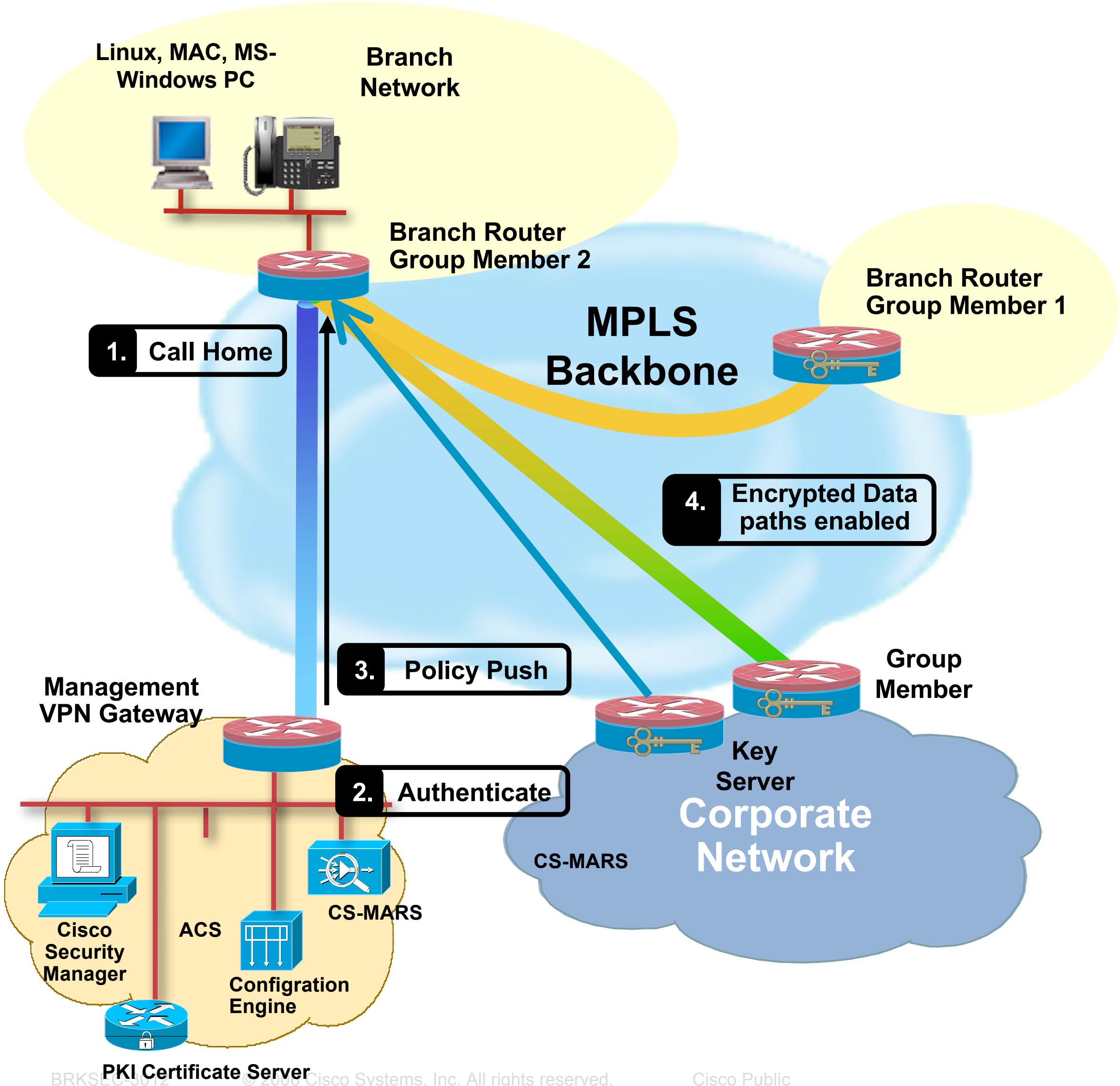
Zero-Touch: Admin perspective

- New Router is directly sent to the remote branch/site
- Device is connected to the IP VPN core
- GET VPN configuration is pushed using SDP – Secure Device Provisioning
- Cisco Security Manager (CSM) is used to generate the configuration

  CSM does not have embedded GET VPN configurations yet, but

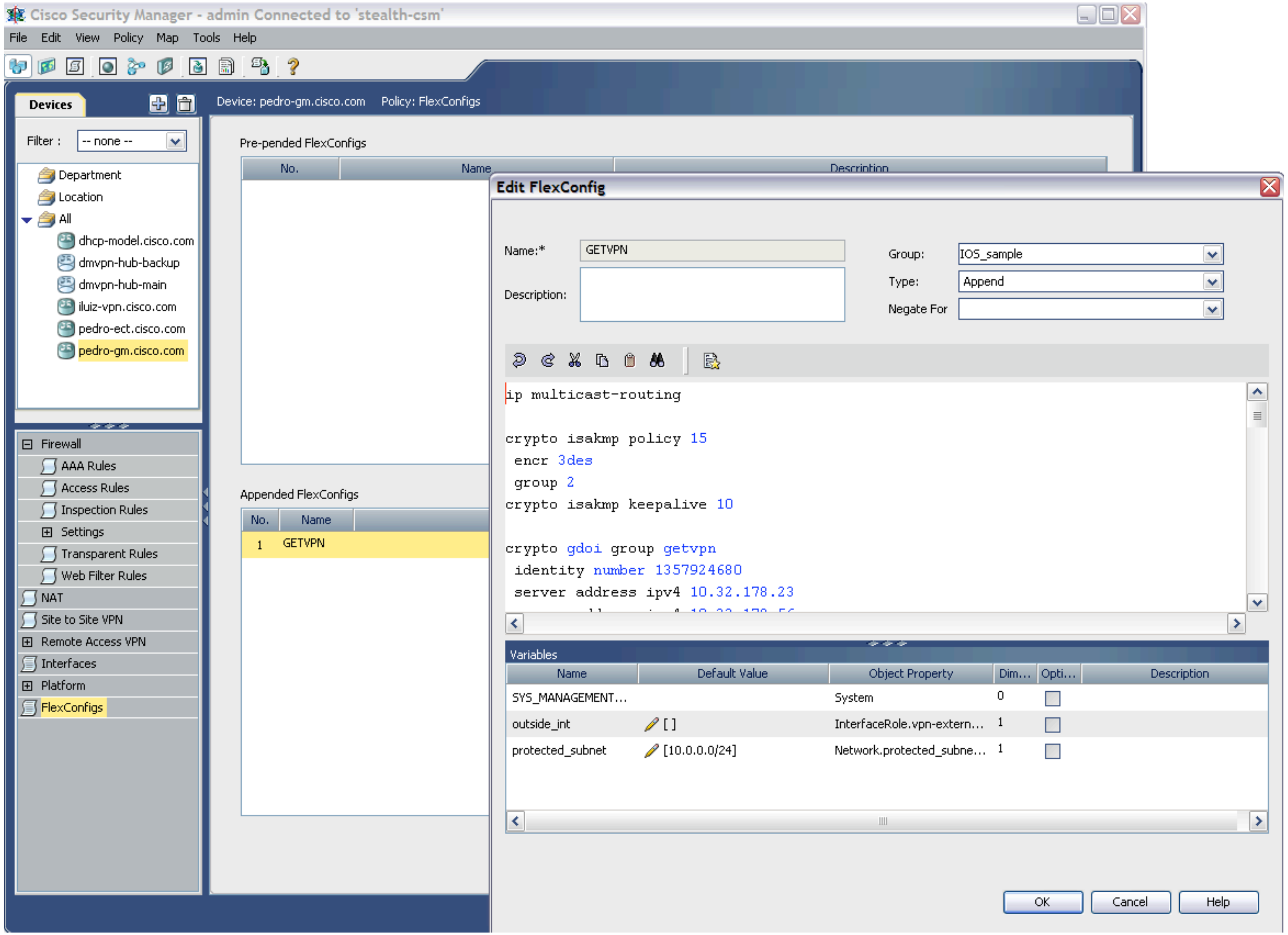
  CSM supports GET VPN using templates (FlexConfigs).
- The Cisco Configuration Engine stages the config file and waits for the “call-home” event from the remote router

ECT Solution – GET VPN Deployment Model



1. Remote routers “calls home” and management tunnel is set up
2. Management server authenticates remote router using certificate authority and AAA servers
3. Management server pushes GET VPN config including new PKI certificate
4. New Branch (Group Member 2) gets the group keys from the Key Server
5. Now the new GM can encrypt traffic to and decrypt traffic from any other branches and the corporate network

GET VPN in CSM with FlexConfigs



No.	Name
1	GETVPN

Name:* GETVPN

Description:

Group: IOS_sample

Type: Append

Negate For:

```
ip multicast-routing

crypto isakmp policy 15
 encr 3des
 group 2
crypto isakmp keepalive 10

crypto gdoi group getvpn
 identity number 1357924680
 server address ipv4 10.32.178.23
 server address ipv4 10.32.178.56
```

Name	Default Value	Object Property	Dim...	Opti...	Description
SYS_MANAGEMENT...		System	0	□	
outside_int	[]	InterfaceRole.vpn-extern...	1	□	
protected_subnet	[10.0.0.0/24]	Network.protected_subne...	1	□	

Operational Support

- Caveats and Limitations
- Deployment Example
- Management Methods
- Platforms Supported

IOS Platform Support

Platform	Group Member	Key Server
Software	Yes	Not recommended
870	Yes	Not recommended
1800/1841	Yes	Not recommended
2800	Yes	Yes
3800 (AIM-II/AIM-III)	Yes	Yes
7200 NPEG1, VAM2+	Yes	Yes
7304 NPEG1, VAM2+	Yes	Yes
7200 NPEG2, VAM2+	No	Yes
7200 NPEG2, VSA	12.5 pi1	12.5 pi1
6500 VPN-SPA	No	No

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

🟩 **Shipping in 12.4 (11) T1**

🟥 **Not Committed, H/W Acceleration needs to be fixed.**

Network Solutions Integrated Testing Environment (NSITE) Scalability Testbed

Platform Role	871	1841	2821	2851	3825 (AIM-SSL/VPN)	3845	7200 NPE-G1 (VAM2+)	7200 NPE-G2 (VAM 2+)	7301 (VAM2+)
GM	X	X	X	X	X	*	X	X	X
KS		*	*	*	*	X	X	X	X

* Not tested yet

- Hybrid lab comprising of Real and Simulated GMs
- Wide variety of ISR platforms
- 7301/VAM2+ simulating a large number of GMs
- Functionality testing completed for a variety of KSs but scalability study performed for a subset

KS Scalability Summary for 7200

Number of Groups	Rekey Transport	GMs per group	Total GMs	CPU spikes
1	Multicast	2000	2000	10%
1	Unicast	200*	200*	5%
100	Unicast	10	1000	-

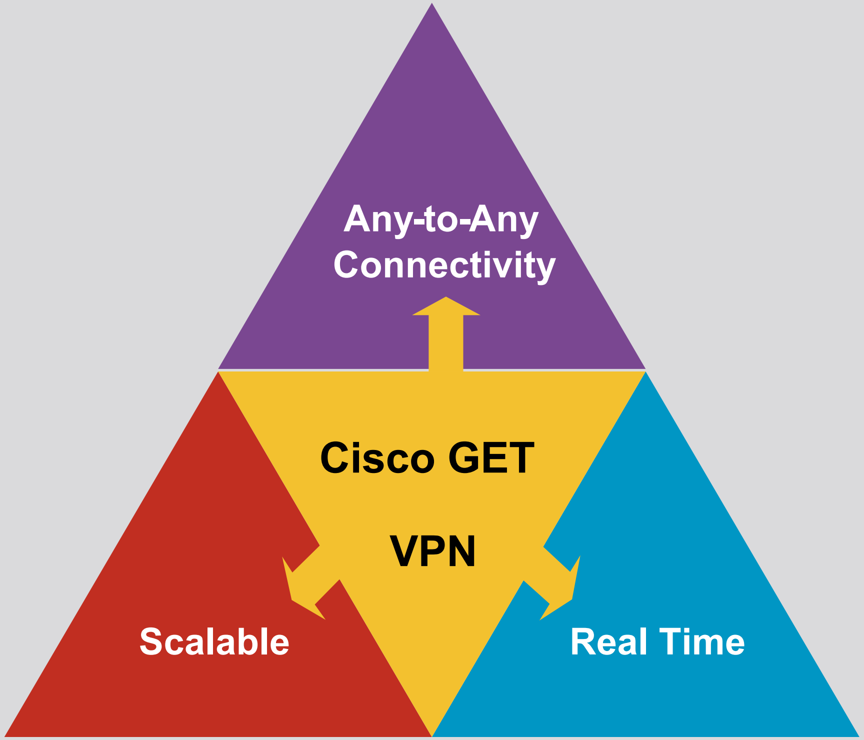
* Internal Test-bed limitation of 200 physical group members; preliminary tests indicate 7200 can perform unicast rekey for 2000 group members

Advanced Site-to-Site IPsec VPN: Group Encrypted Transport (GET)

Summary

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

General Recommendations

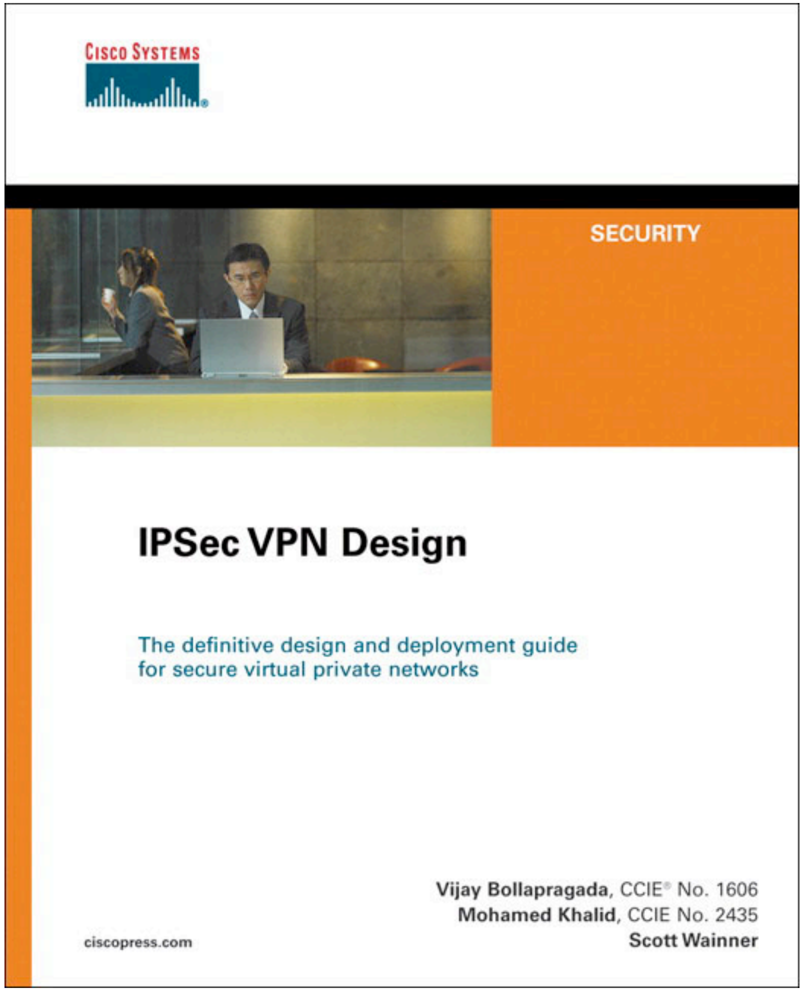
- Cryptography
  - AES-CBC
  - PKI for Group Member / Key Server Authentication
  - TEK lifetimes of at least 1 hour
  - KEK lifetimes at least 24 hours
  - Multicast Rekey for KEK / TEK Key Distribution
- Architectural
  - Distribute Group Member’s Preferred Registration Across Multiple Key Servers
  - Simplify configuration by symmetric IPsec proxy policies

    (eg. ‘permit ip any any’ or ‘permit ip 10/8 10/8’)
  - Universally consistent control plane / management plane selection
  - Physical separate KS sites with redundant and highly reliable paths between KS

Recommended Reading

BRKSEC - 3012

- IPSec VPN Design



CISCO SYSTEMS

SECURITY

IPSec VPN Design

The definitive design and deployment guide for secure virtual private networks

Vijay Bollapragada, CCIE® No. 1606
Mohamed Khalid, CCIE No. 2435
Scott Wainner

ciscopress.com

Available in the Cisco Company Store

Further Reading - References

- CCO

  Configuration - http://www.cisco.com/en/US/partner/products/ps6441/products_feature_guide09186a008078e4f9.html

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

- Recommended Reading:

  IPSec VPN Design

- IETF

  RFC 3547

  Group Domain of Interpretation

  RFC 2401 thru RFC 2410

  IPsec Protocols

  RFC 3740

  Multicast Security Architecture

  RFC 4046

  Multicast Security Group Key Management Architecture

Meet the Experts
Security

- Andres Gasson
  Consulting Systems Engineer

- Christophe Paggen
  Technical Marketing Engineer

- Eric Vyncke
  Distinguished Consulting Engineer

- Erik Lenten
  Technical Marketing Engineer

- Fredéric Detienne
  CA Technical Leader

- Luc Billot
  Consulting Engineer

Meet the Experts
Security

- Michael Behringer
  Distinguished System Engineer

- Olivier Dupont
  Corporate Dev Consulting Engineer

- Peter Matthews
  Technical Marketing Engineer

- Scott Wainner
  Distinguished System Engineer

- Steinthor Bjarnason
  Consulting Engineer

Q and A