Advanced IPSec with GET VPN

Nadhem J. AlFardan
Consulting System Engineer
Cisco Systems

nalfarda@cisco.com

Agenda

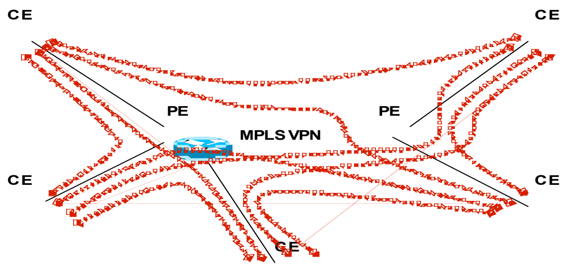
- Motivations for GET-enabled IPVPN
- GET-enabled IPVPN Overview
- GET Deployment Properties
- GET-enabled VPN Reliability
- General Recommendations

Motivations for GET VPN

Challenges with Existing Security and IP VPN

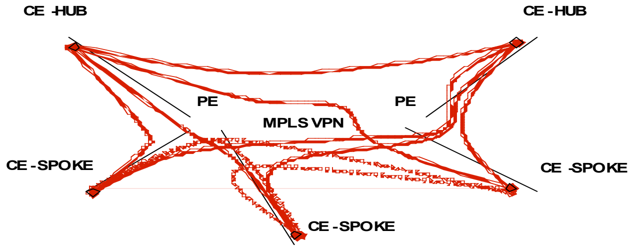
IPSec Peer Crypto Map Security

- Full Mesh of crypto map entries and dormant until packet flow initiates SA creation



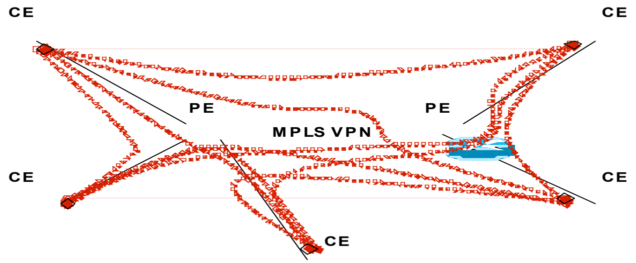
IPSec DMVPN Security

- Persistent Partial Mesh with potential mesh based on dynamic crypto map entry.
- Dormant spoke-to-spoke until packet flow initiates SA creation



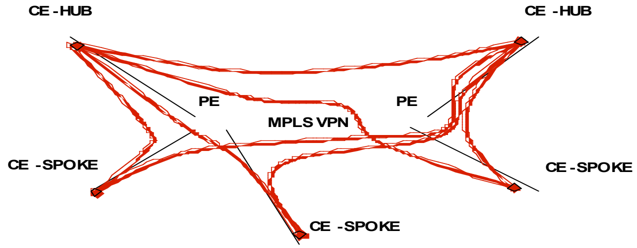
IPSec TED Crypto Map Security

- Potential mesh based on dynamic crypto map entry and dormant until packet flow initiates SA creation



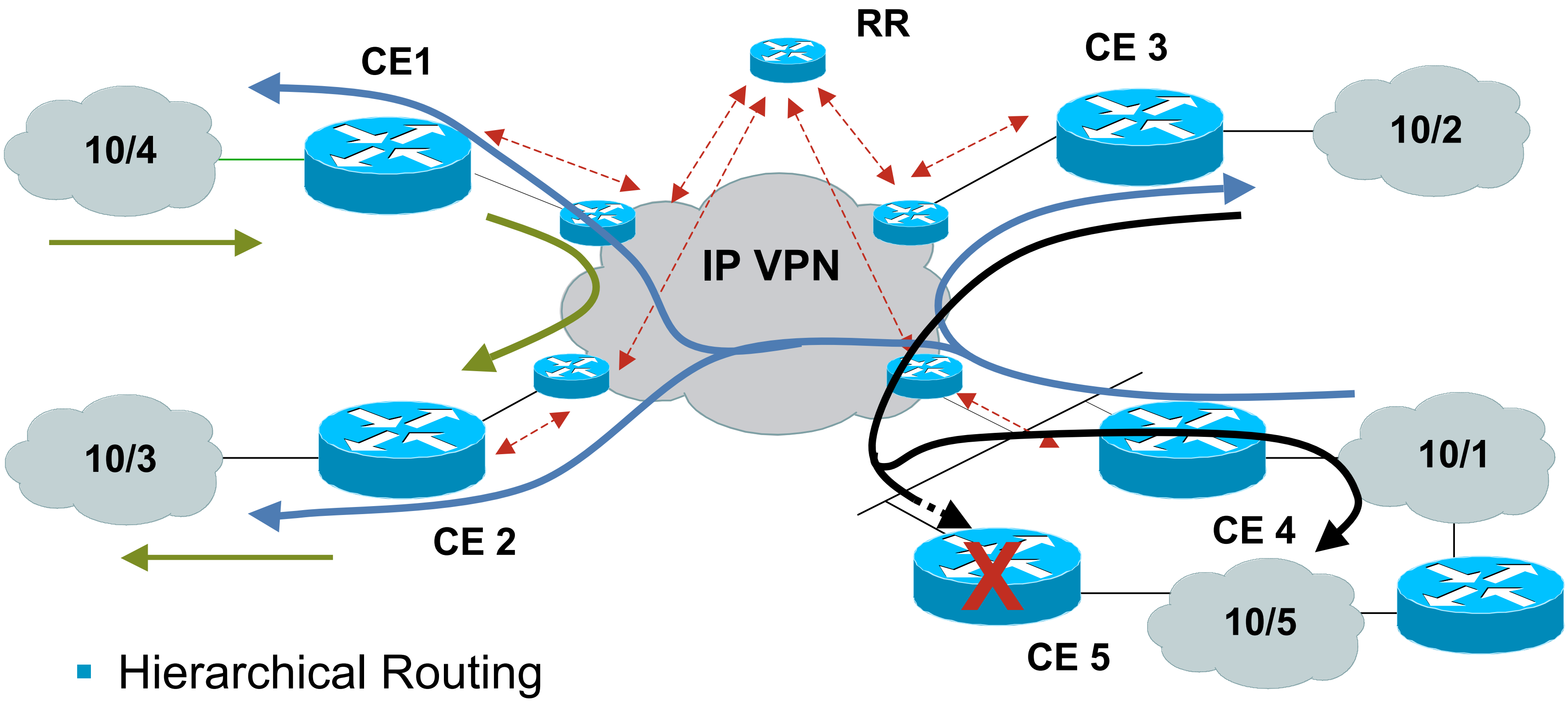
IPSec GRE Security

- Persistent Partial Mesh with potential mesh based on dynamic crypto map entry.



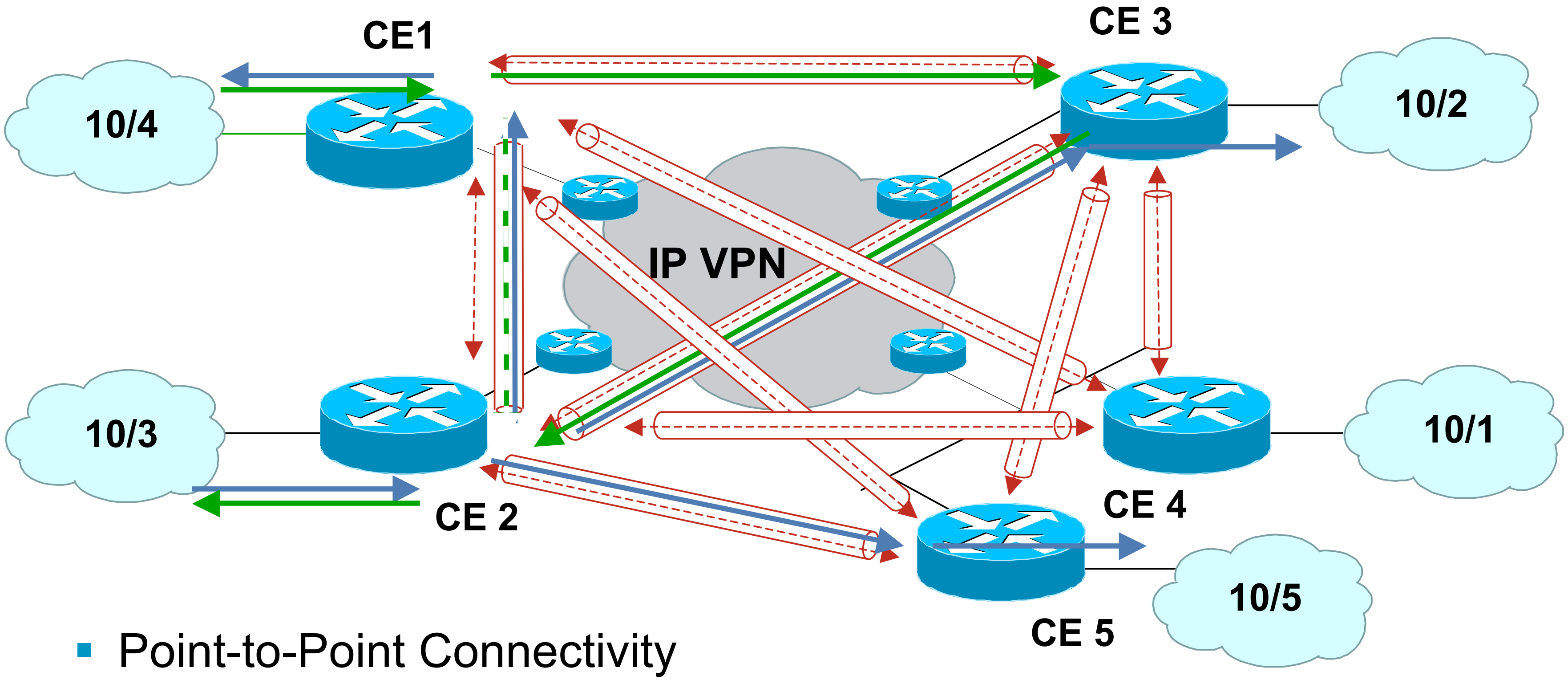
Existing Models Create Overlay networks on IP VPN mitigating the value of IP VPN

MPLS VPN Attributes



- Hierarchical Routing
- Any-to-Any Connectivity
- Redundancy Established between CE and PE
- MPLS 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

- MPLS VPN
  - ▲ Any-to-any connectivity without CE-CE Tunnel Adjacency
  - ▲ Single Point Provisioning on per CE basis
  - ▲ Distributed and 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

Reconciliation of the Network Paradigms

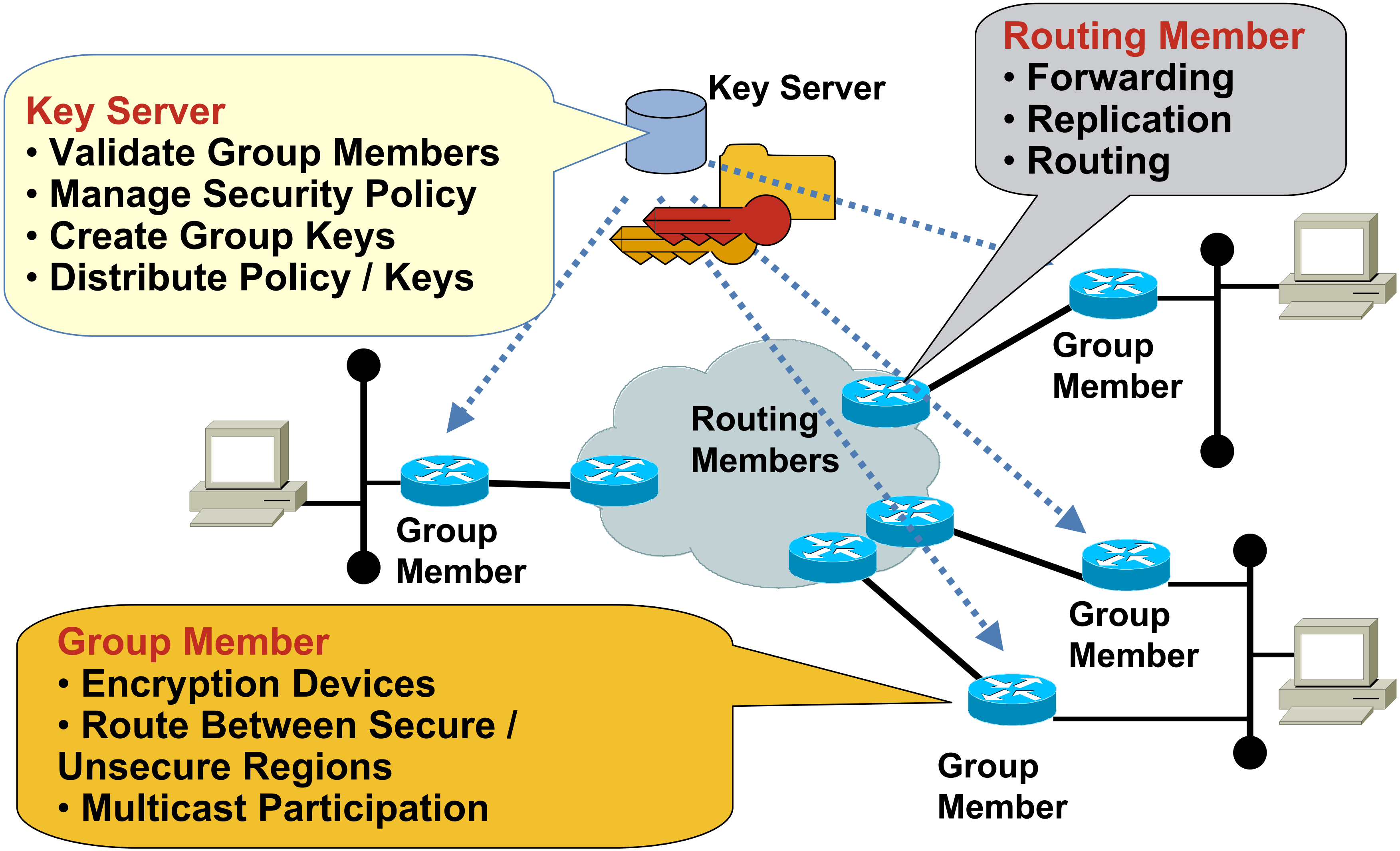
- So Now What?
- Resolution

  A new security paradigm for multicast and unicast communication on an MPLS VPN

  Security paradigm does not ‘create’ the VPN, it uses an existing MPLS VPN

GET
Technical Overview

Group Security Functions

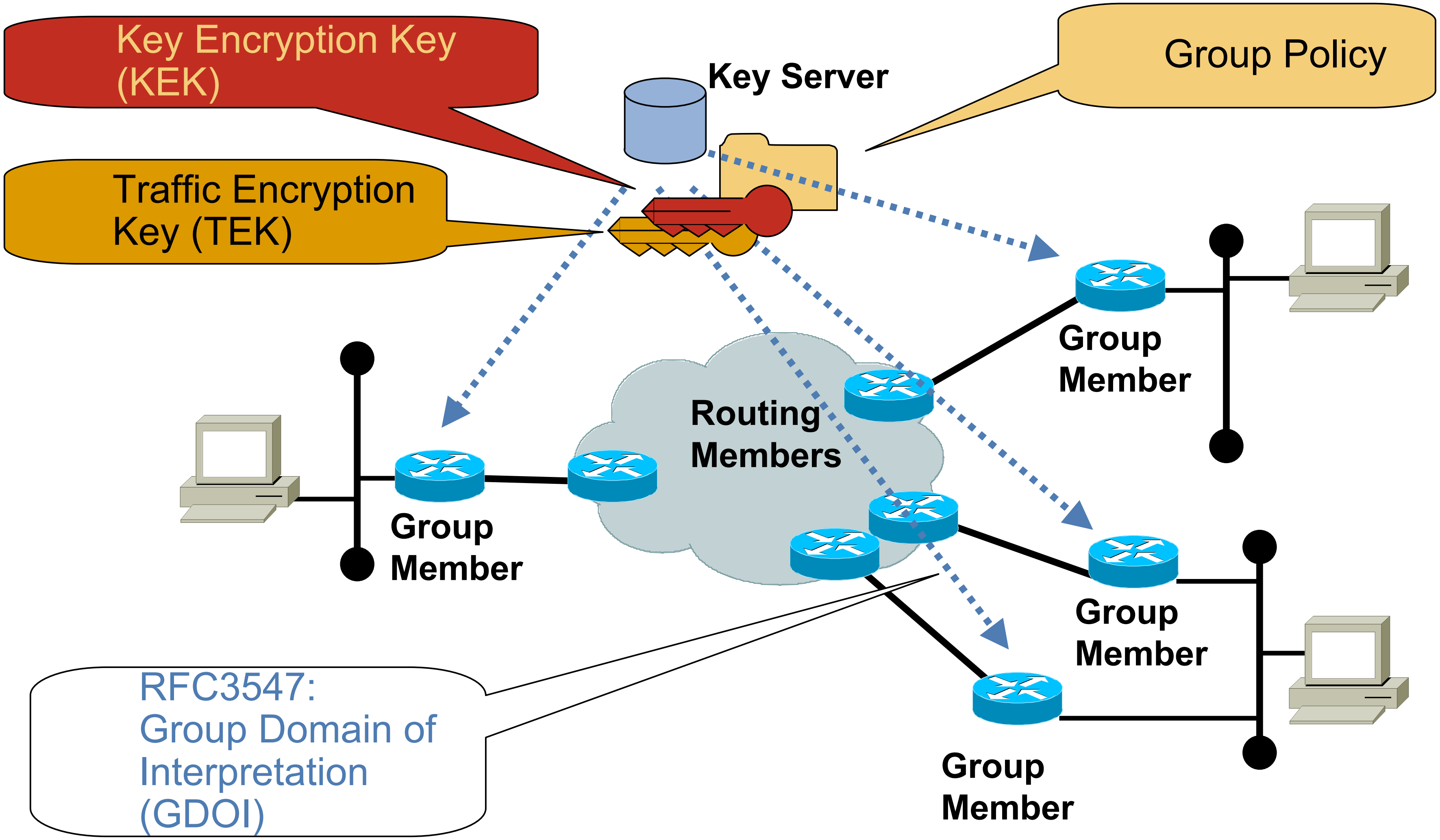


Key Server
- Validate Group Members
- Manage Security Policy
- Create Group Keys
- Distribute Policy / Keys

Routing Member
- Forwarding
- Replication
- Routing

Group Member
- Encryption Devices
- Route Between Secure / Unsecure Regions
- Multicast Participation

Group Security Elements



Key Encryption Key (KEK)

Traffic Encryption Key (TEK)

Group Policy

RFC3547: Group Domain of Interpretation (GDOI)

Group Security Association

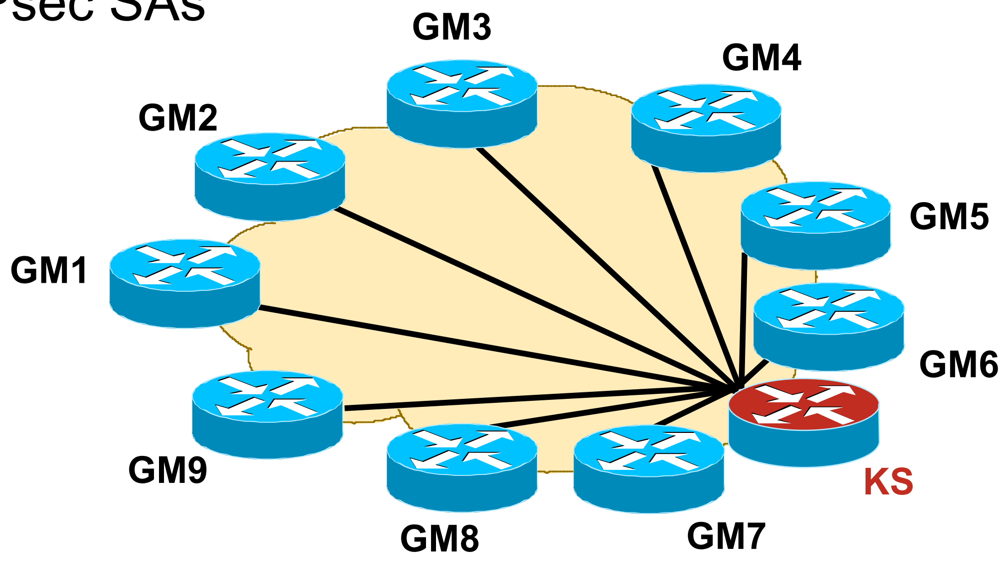
- Group Members share a security association
  - Security association is not to a specific group member
  - Security association is with a set of group members
- Safe when VPN gateways are working together to protect the same traffic
  - The VPN gateways are trusted in the same way
  - Traffic can flow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

Basic GET VPN Architecture

- Step 1: Group Members (GM) “register” via GDOI with the Key Server (KS)

  KS authenticates & authorizes the GM

  KS returns a set of IPsec SAs for the GM to use

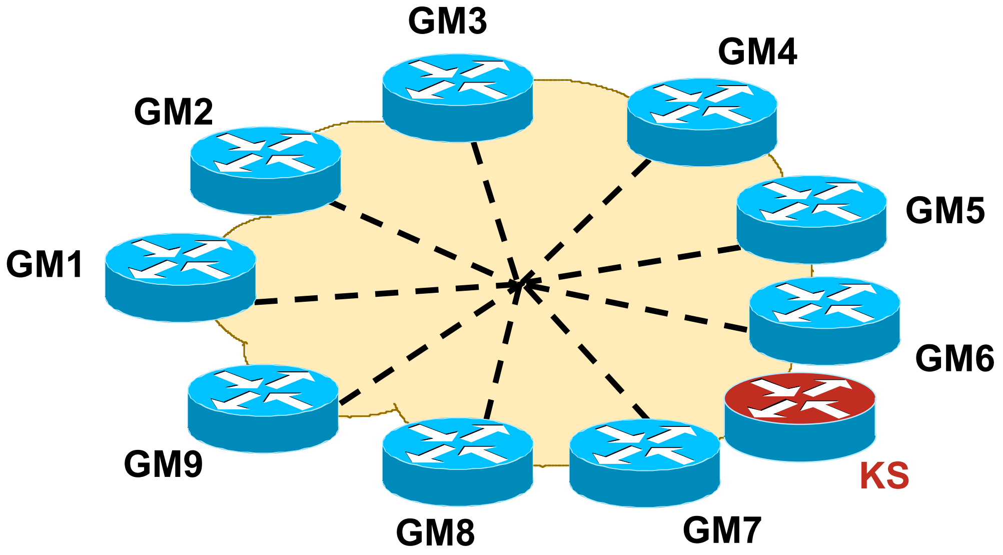


Basic GET VPN Architecture

- Step 2: Data Plane Encryption

  GM exchange encrypted traffic using the group keys

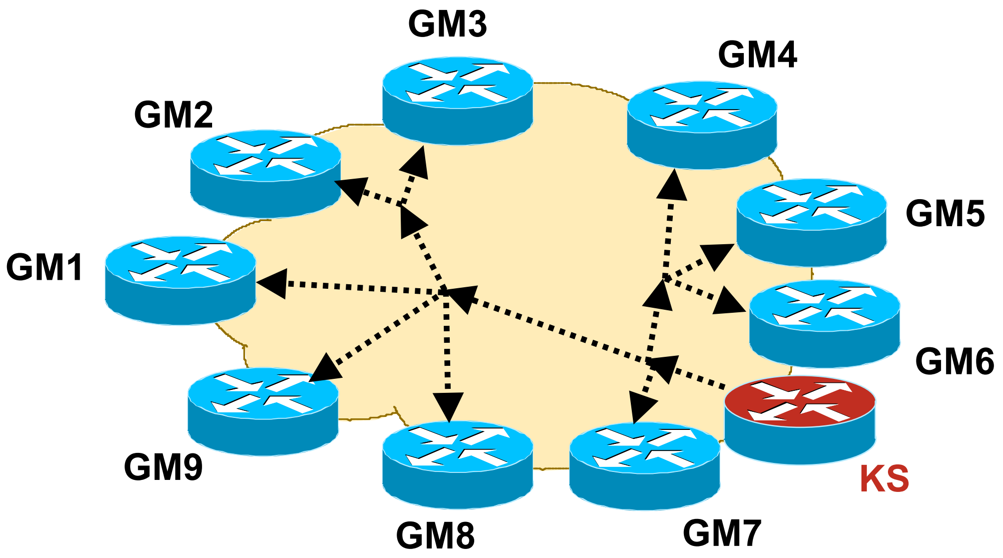
  The traffic uses IPSec Tunnel Mode with “address preservation”



Basic GET VPN Architecture

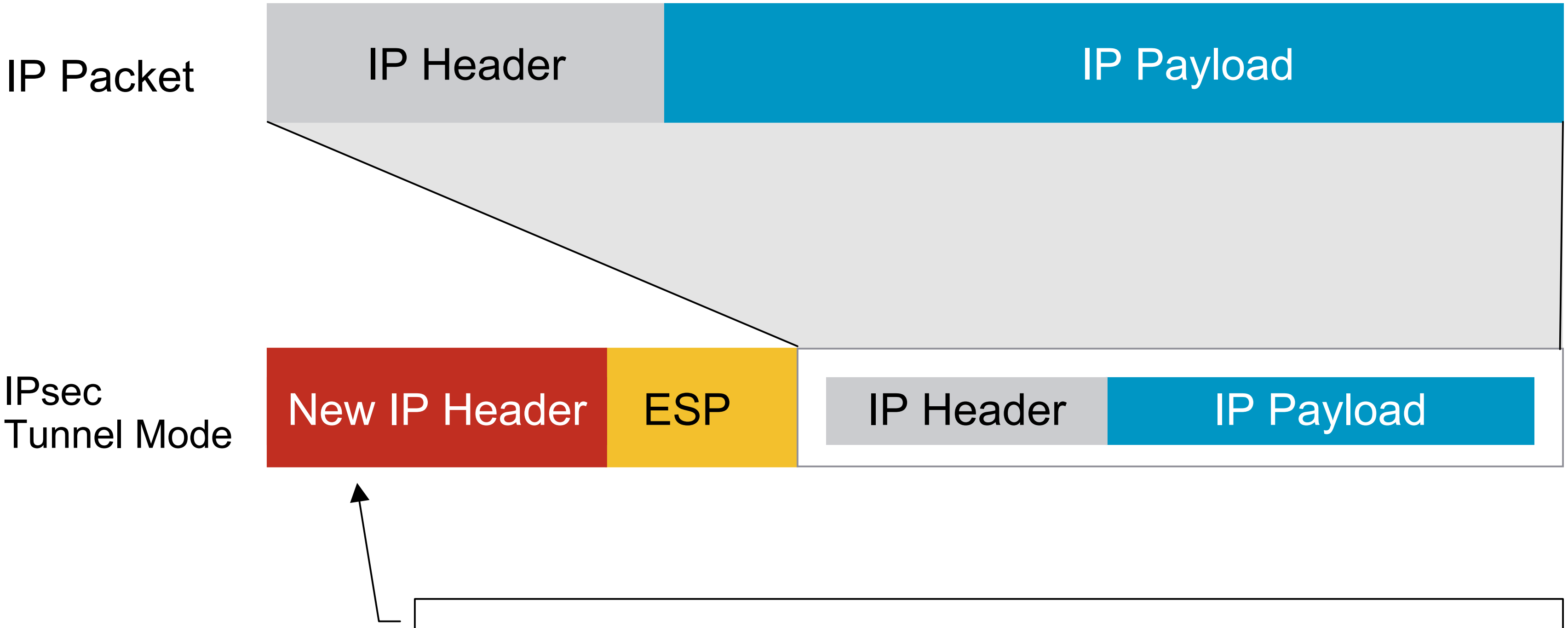
- Step 3: Periodic Rekey of Keys

  KS pushes out replacement IPsec keys before current IPsec keys expire. This is called a "rekey"



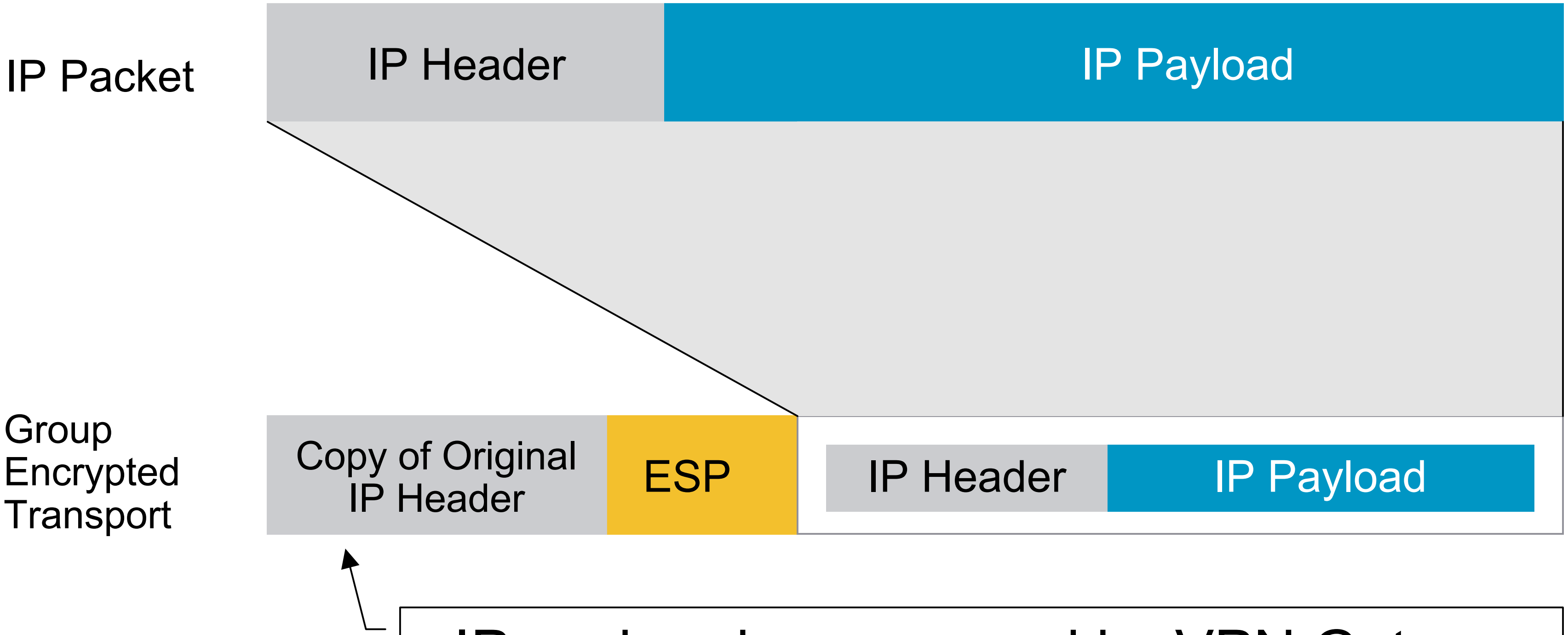
GET Deployment Properties

IPsec Tunnel Mode



- IPsec header inserted by VPN Gateway
- New IP Address requires overlay routing

IPsec Tunnel Mode with IP Address Preservation

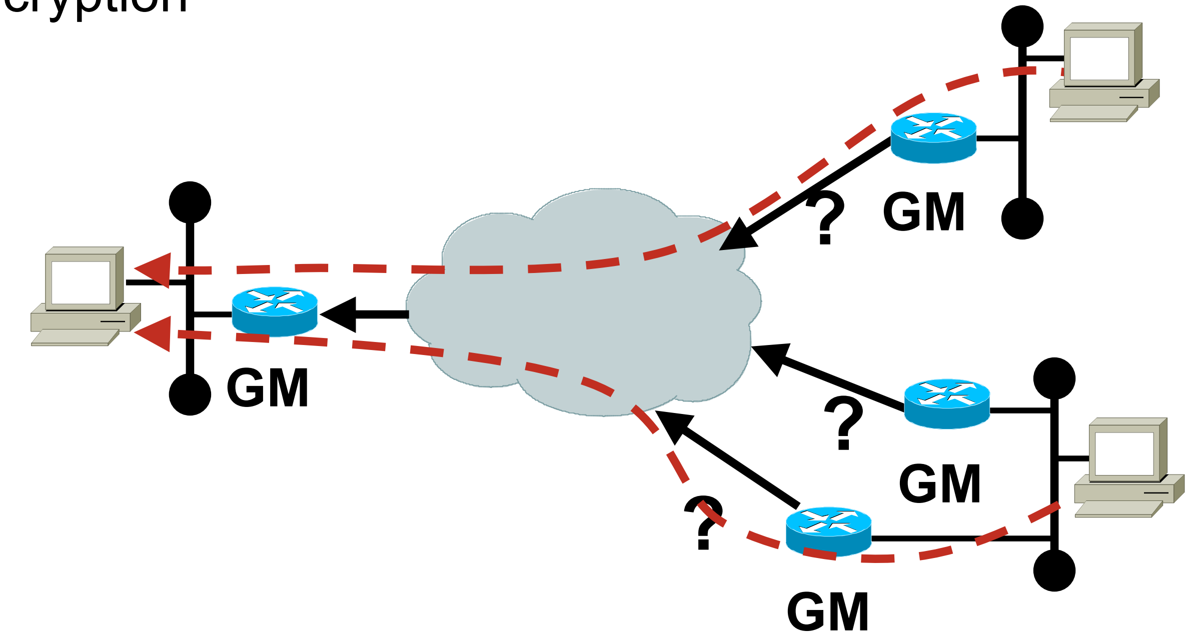


- IPsec header preserved by VPN Gateway
- Preserved IP Address uses original routing plane

Secure Data Plane Unicast

Data Protection Secure Unicast

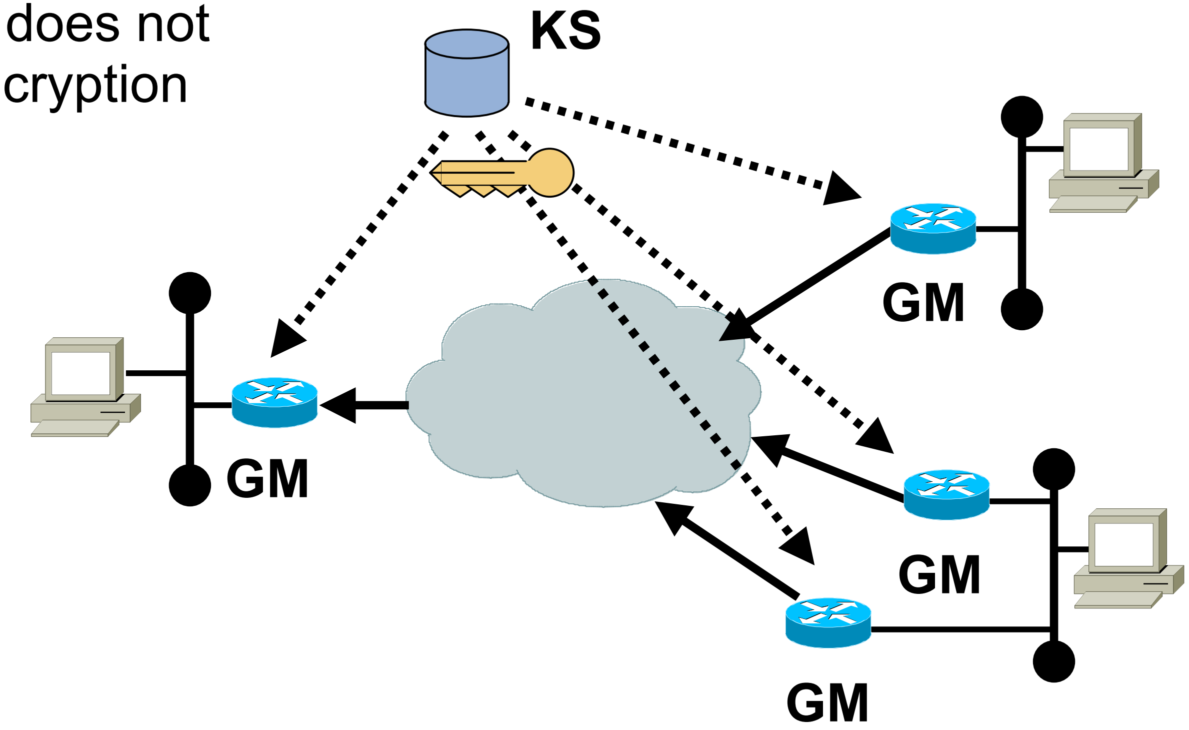
- Premise: Receiver advertises destination prefix but does not know the potential encryption sources



Secure Data Plane Unicast

Data Protection
Secure
Unicast

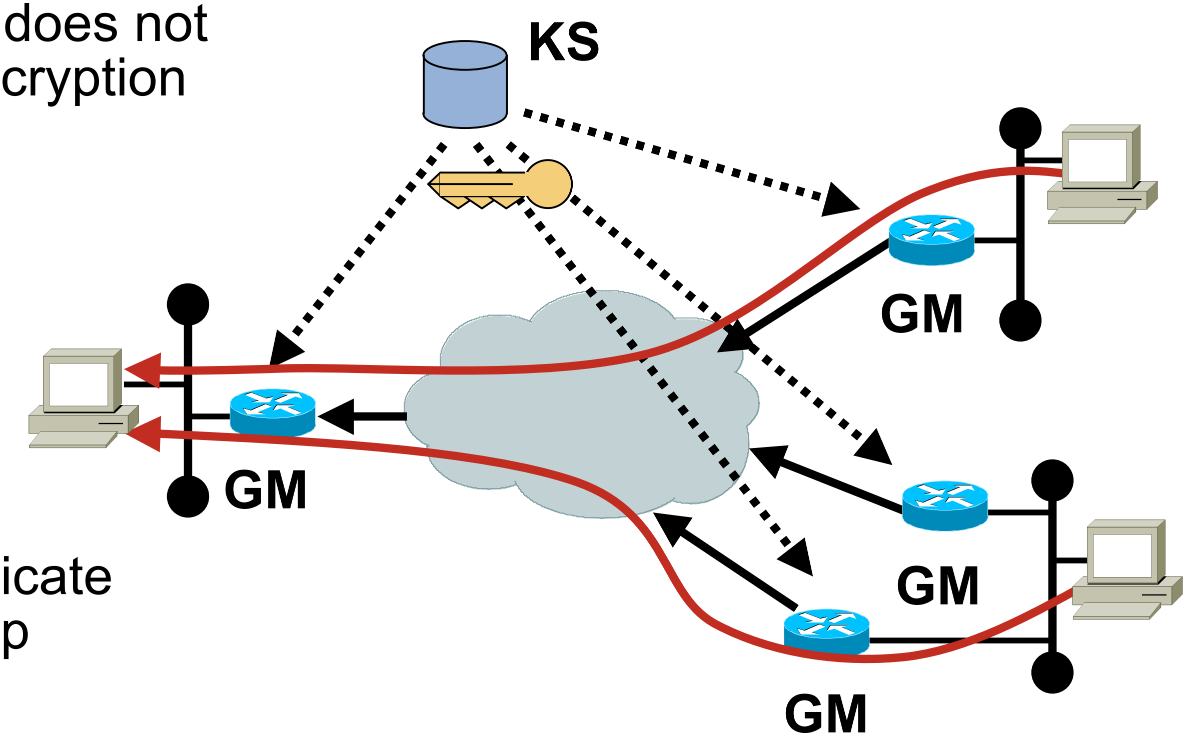
- Premise: Receiver advertises destination prefix but does not know the potential encryption sources
- Receiver assumes that legitimate group members obtain Traffic Encryption Key from key server for the group



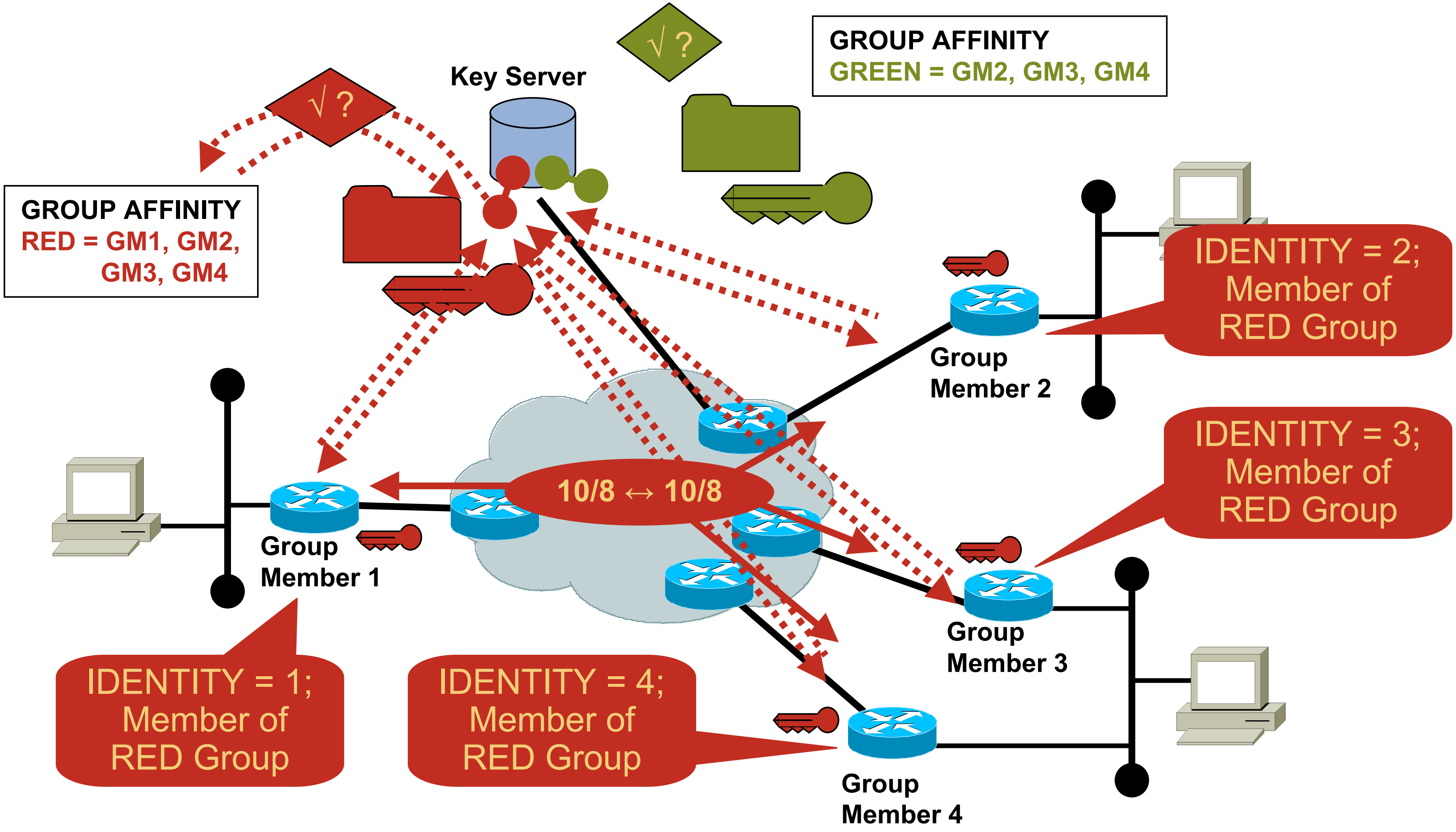
Secure Data Plane Unicast

Data Protection
Secure
Unicast

- Premise: Receiver advertises destination prefix but 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

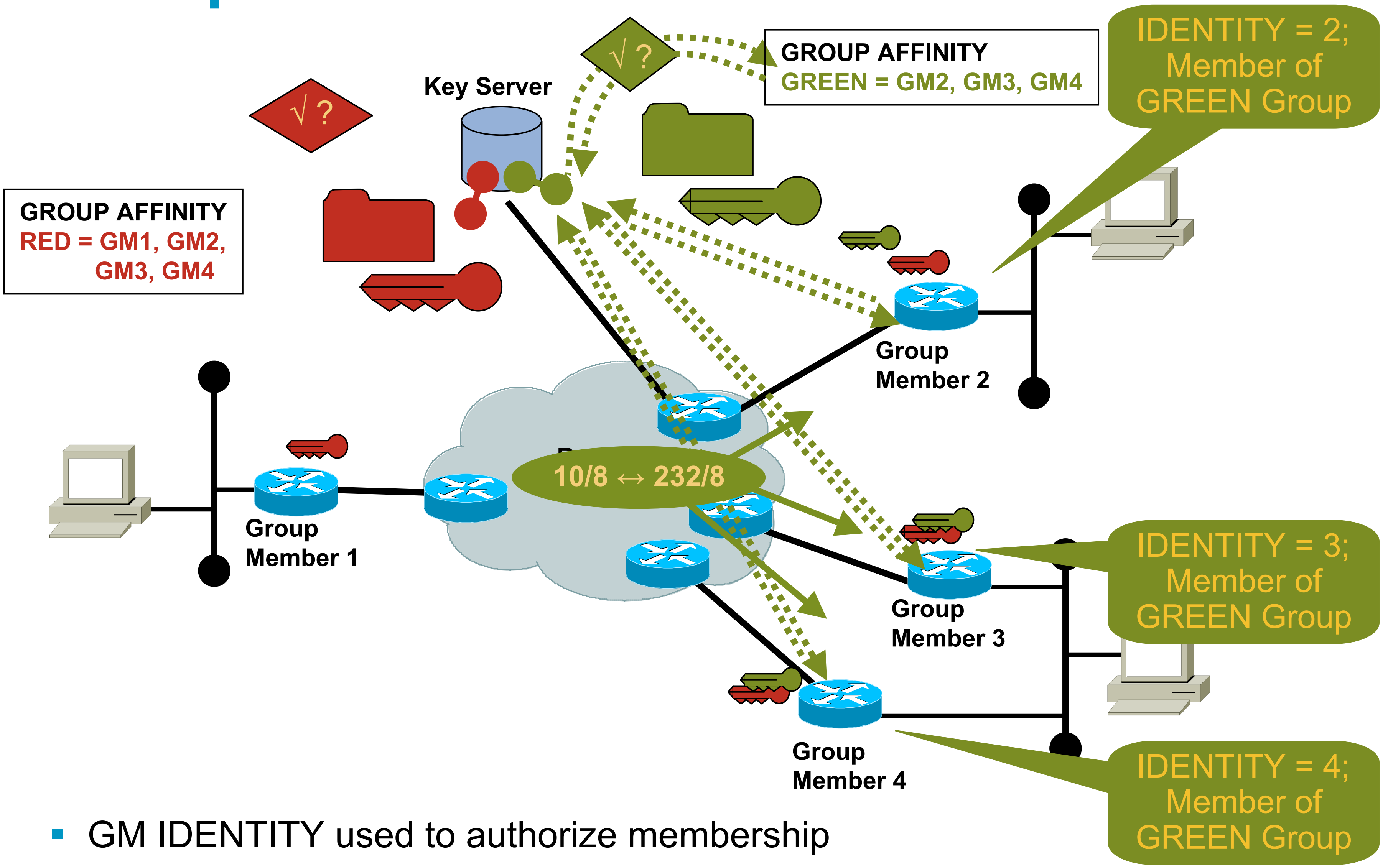


Group Authorization



- GM IDENTITY used to authorize membership

Group Authorization



- GM IDENTITY used to authorize membership

Group Policy Considerations

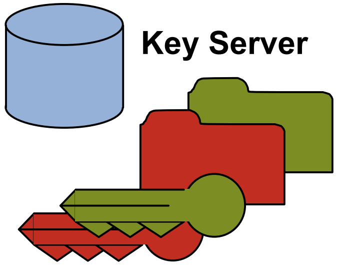
- What may already be protected?
  - Management Plane
    - SSH, TACACS, HTTPS
- What should not be protected with Group Security?
  - Control Plane
    - Internet Key Exchange / Group Domain of Interpretation
    - Routing Exchanges (OSPF, BGP)
- What needs to be protected with Group Security?
  - Data 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)

Encryption Methods

- Key Server maintains policy and encryption attributes per group



- IPsec Attributes
  - IPsec Tunnel Mode w/Header Preservation
  - 3DES
- Policy
  'permit ip 10/8 10/8'

Unicast

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

Unicast and Multicast

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

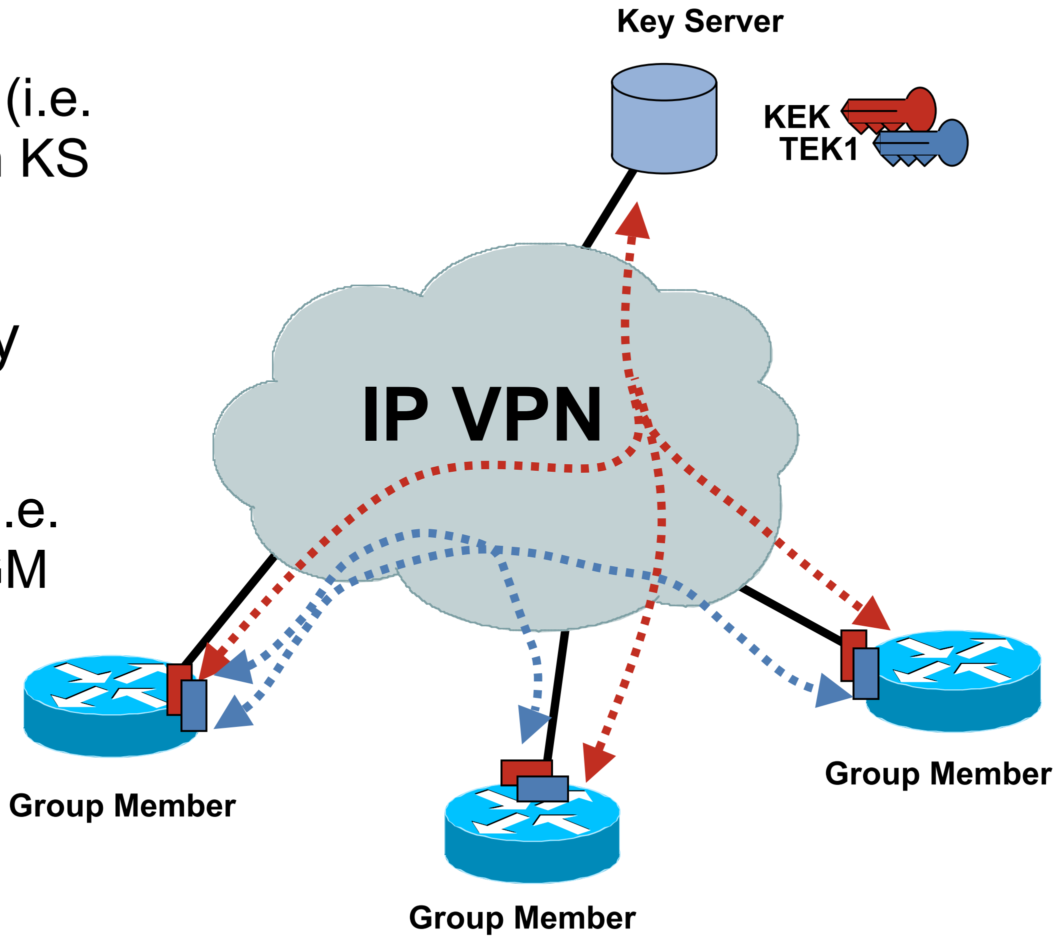
Group Keys

- Key Encryption Key (KEK)

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

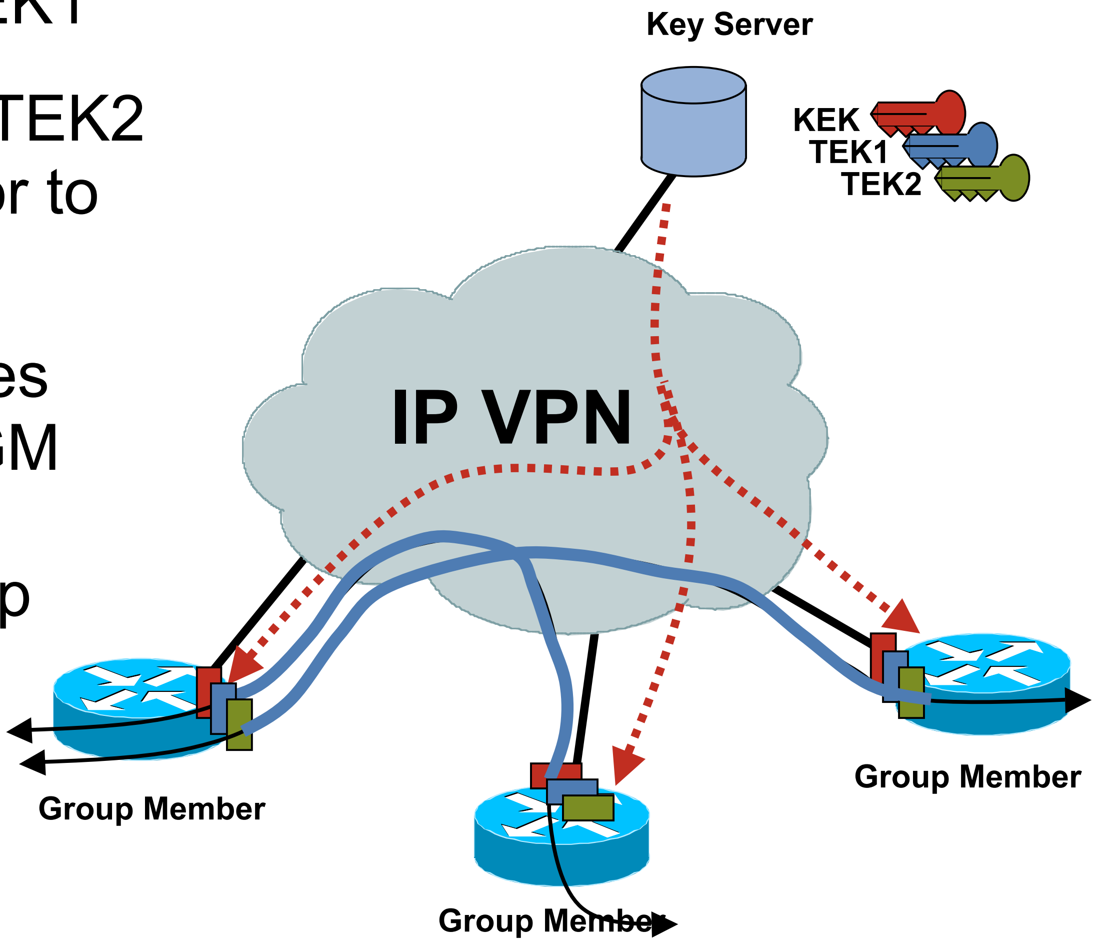
- Traffic Encryption Key (TEK)

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



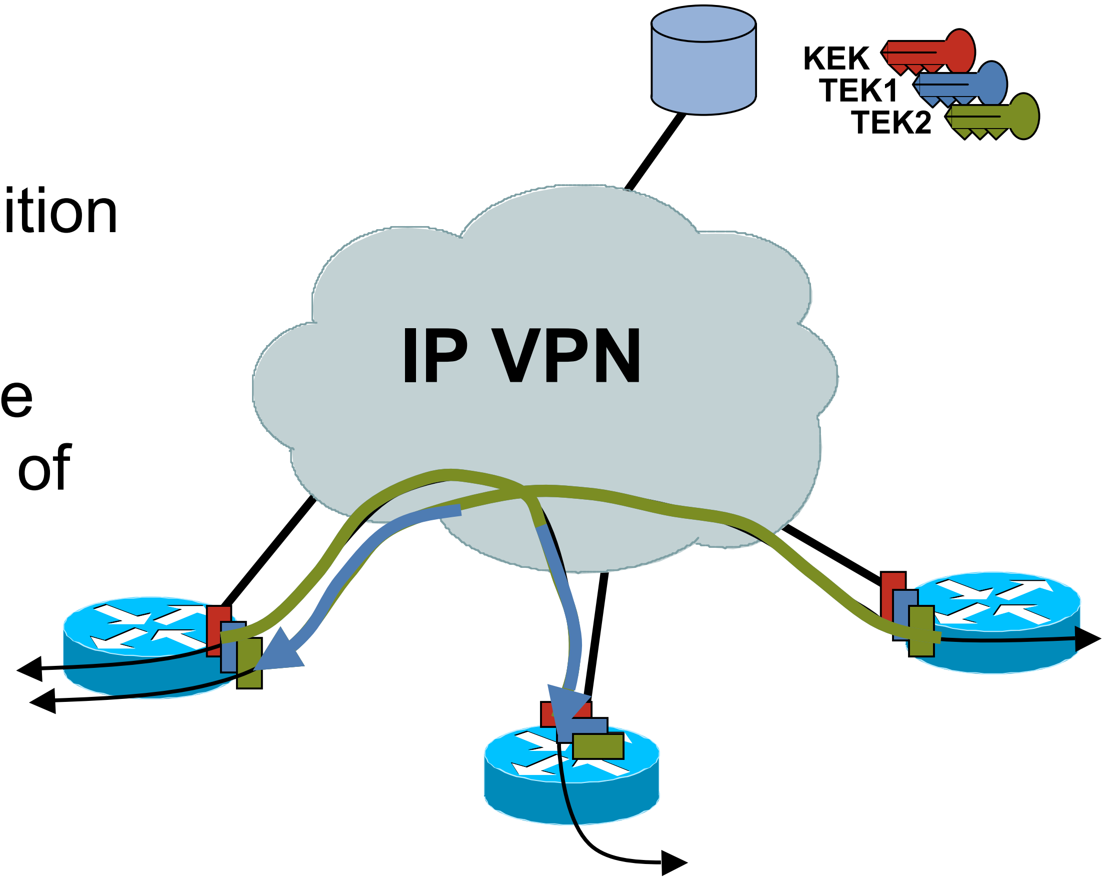
Group Keys

- 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



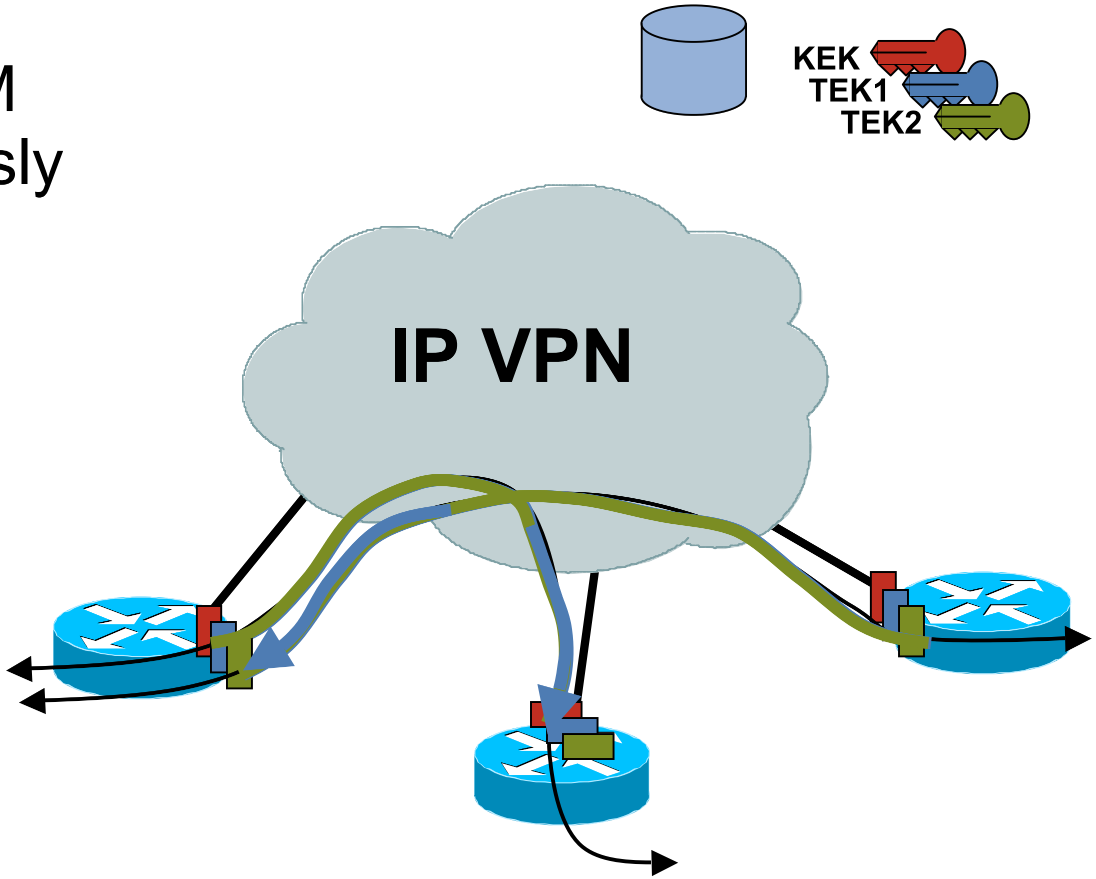
Group Keys

- 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

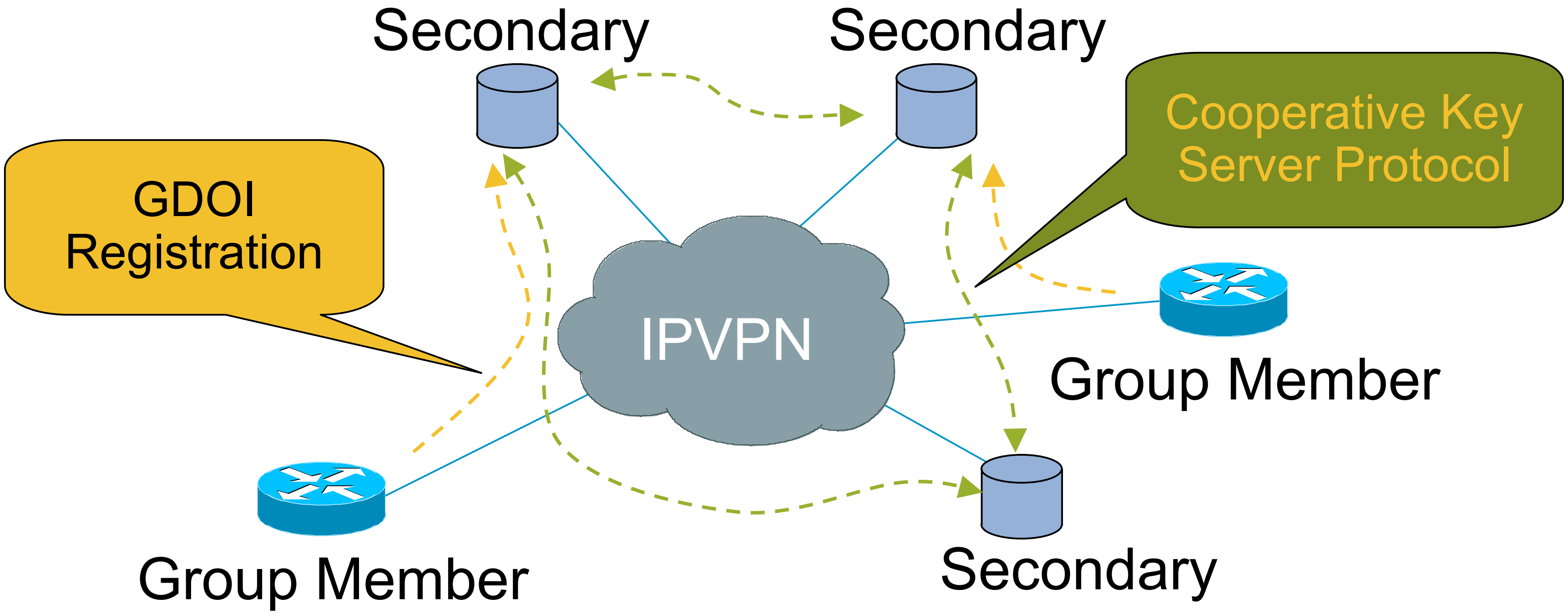
- All GM transitioned to TEK2 encryption
- TEK1 expires on GM pseudo-synchronously



GET Reliability

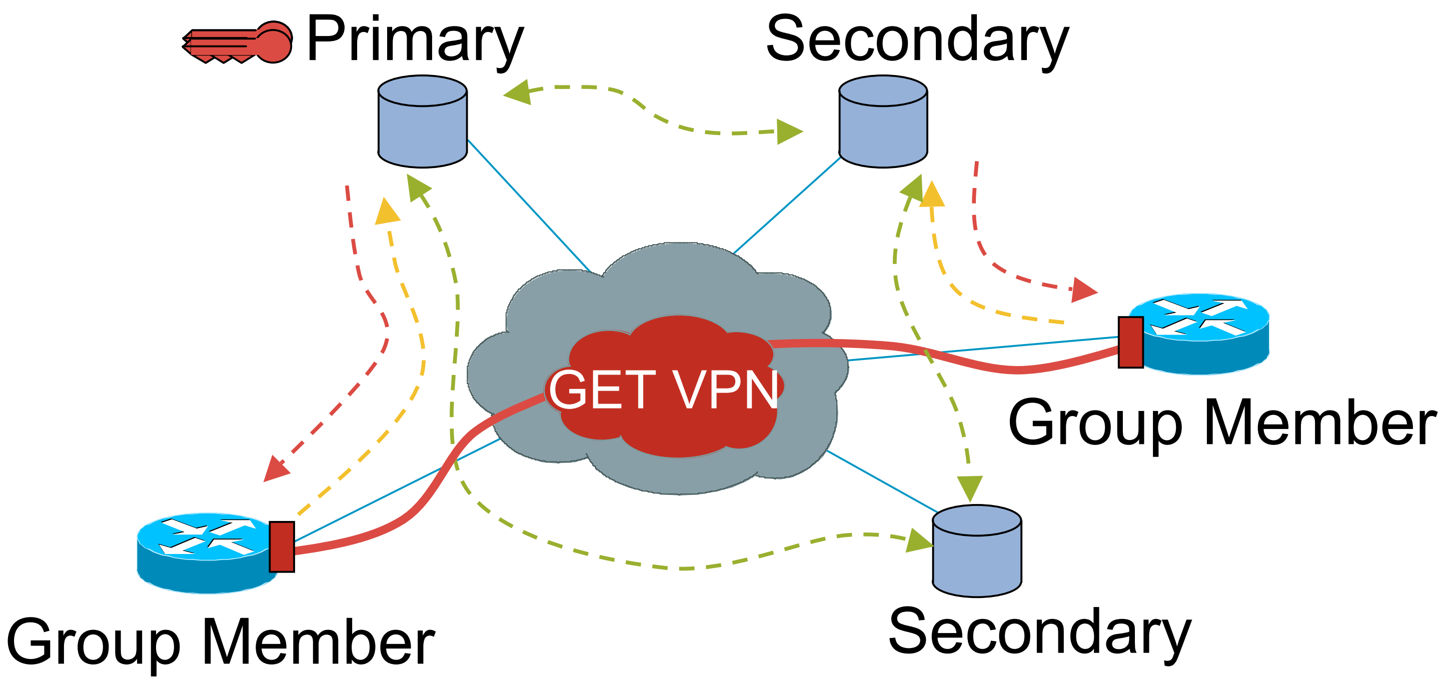
Cooperative Key Server: Roles

- 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



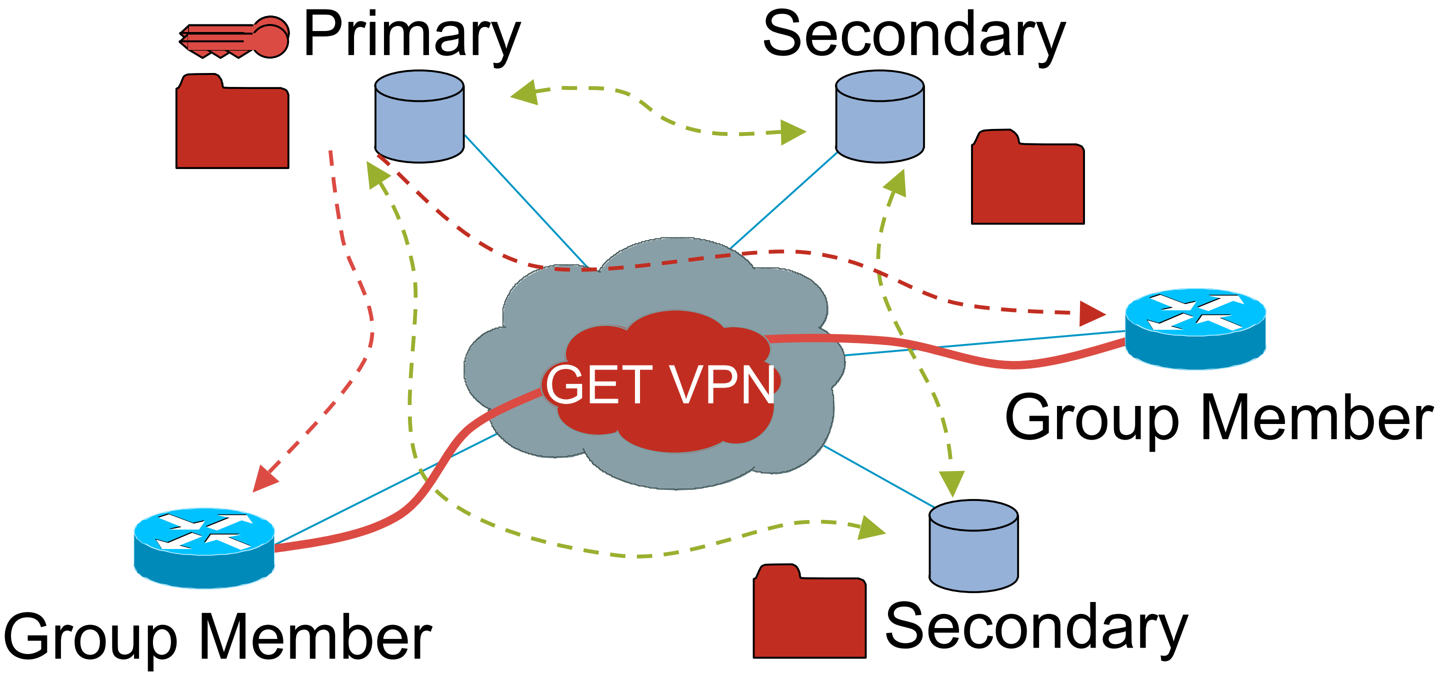
Cooperative Key Server: Roles

- 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



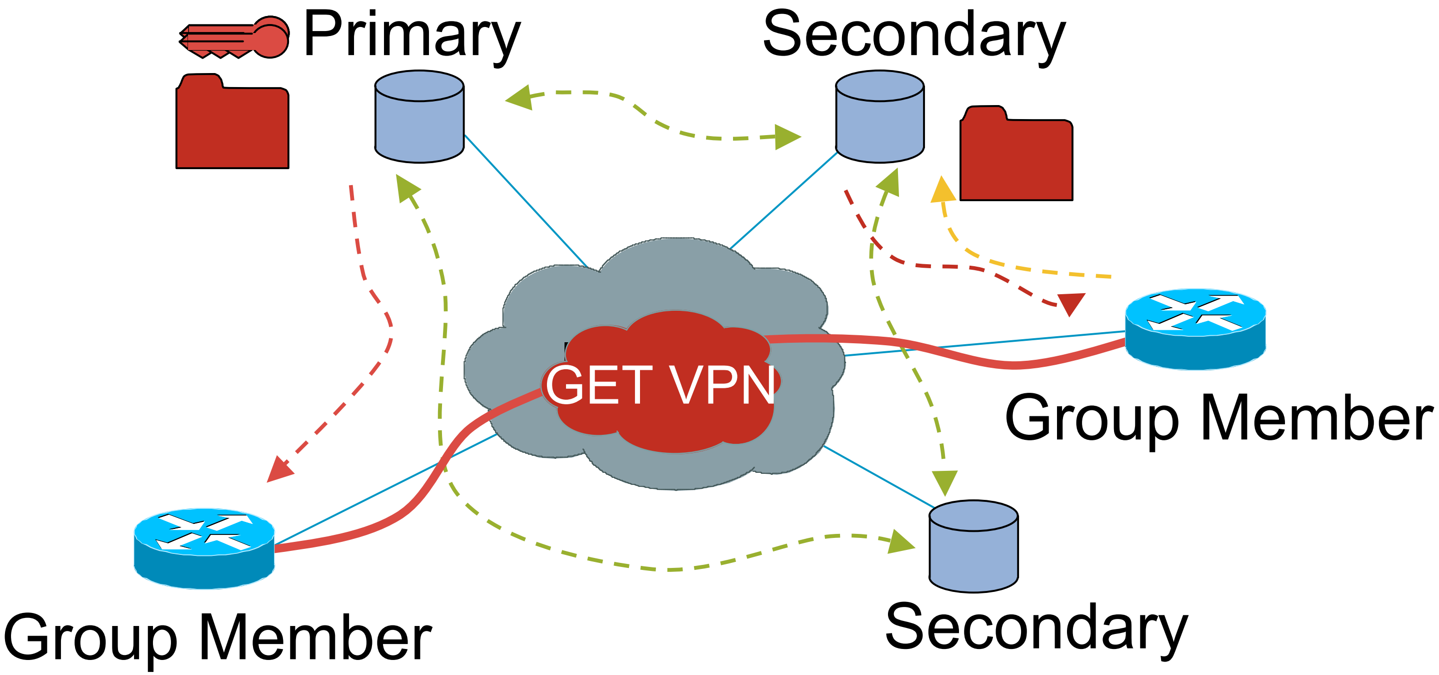
Cooperative Key Server: Primary Processes

- 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



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

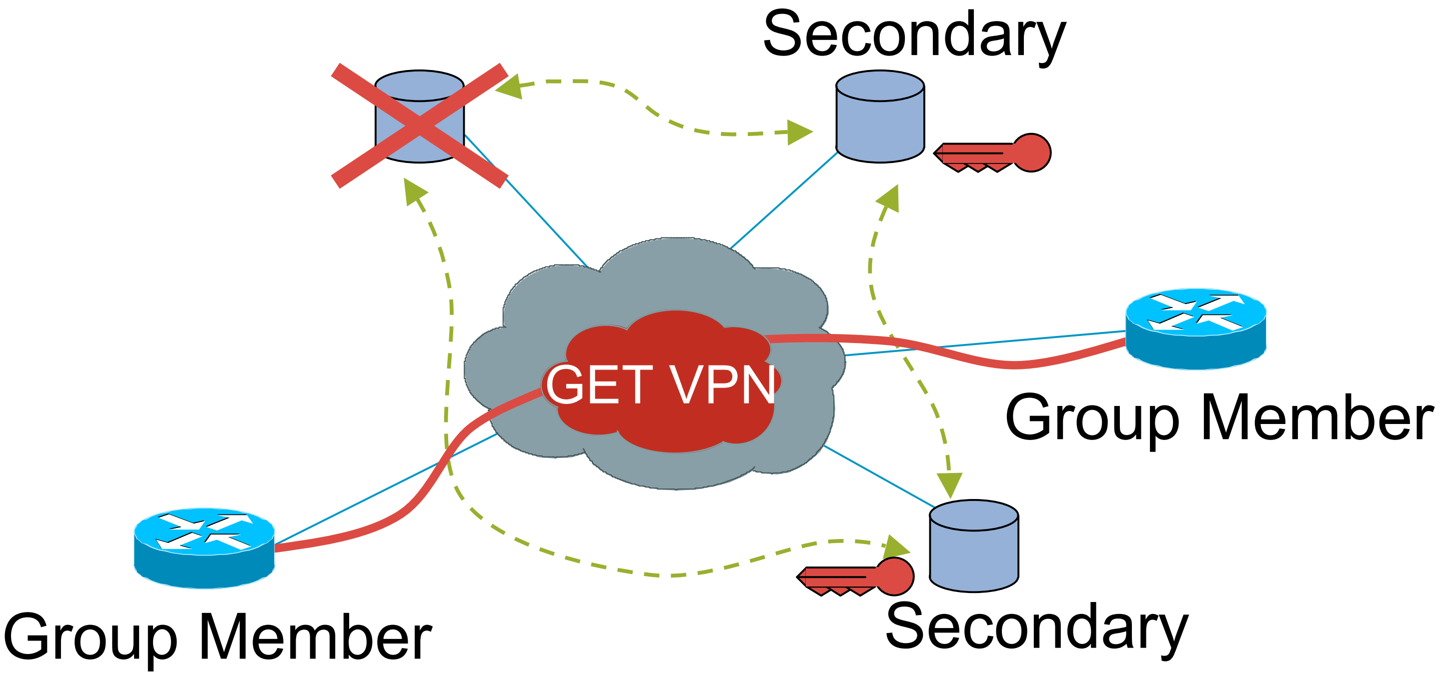


Failure Scenarios: Key Server Failure

- Primary Key Server Database Lost (not disconnected)

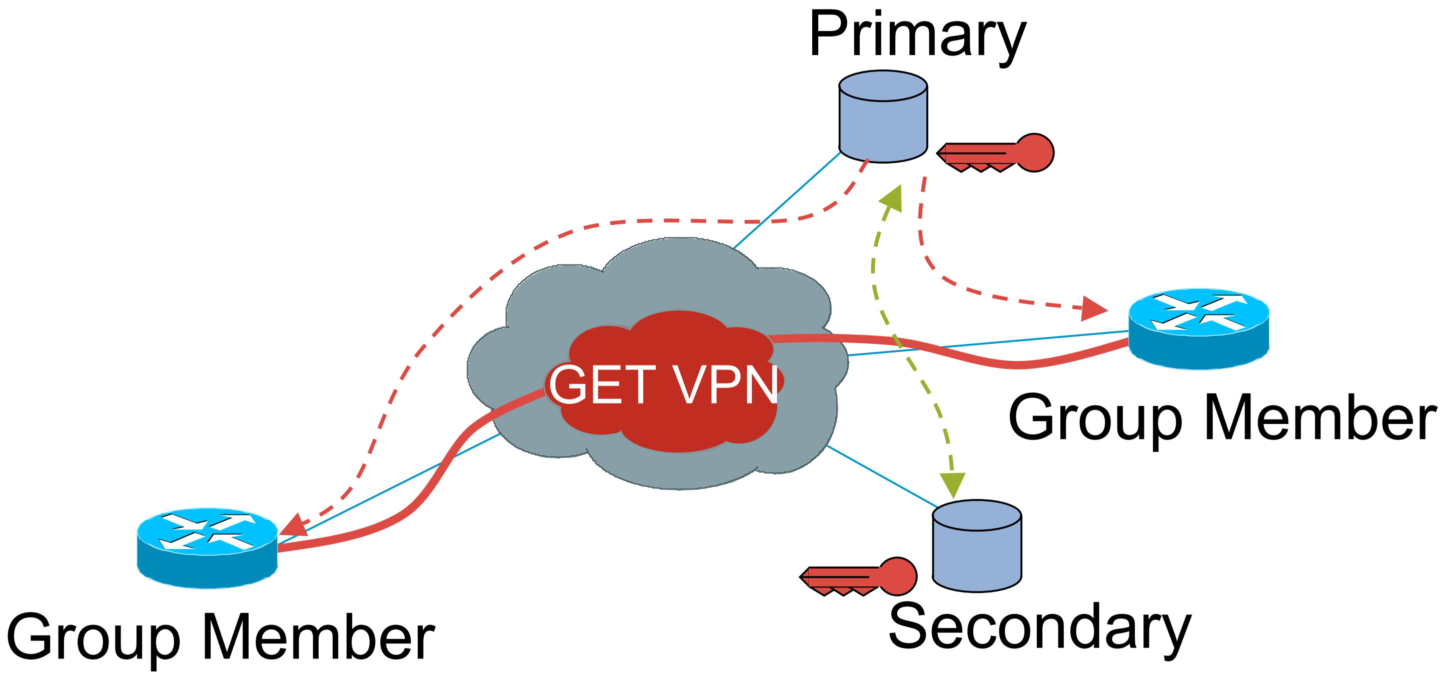
  System Reboot, GDOI Database Cleared

- Secondary Key Servers Detect Loss of Primary



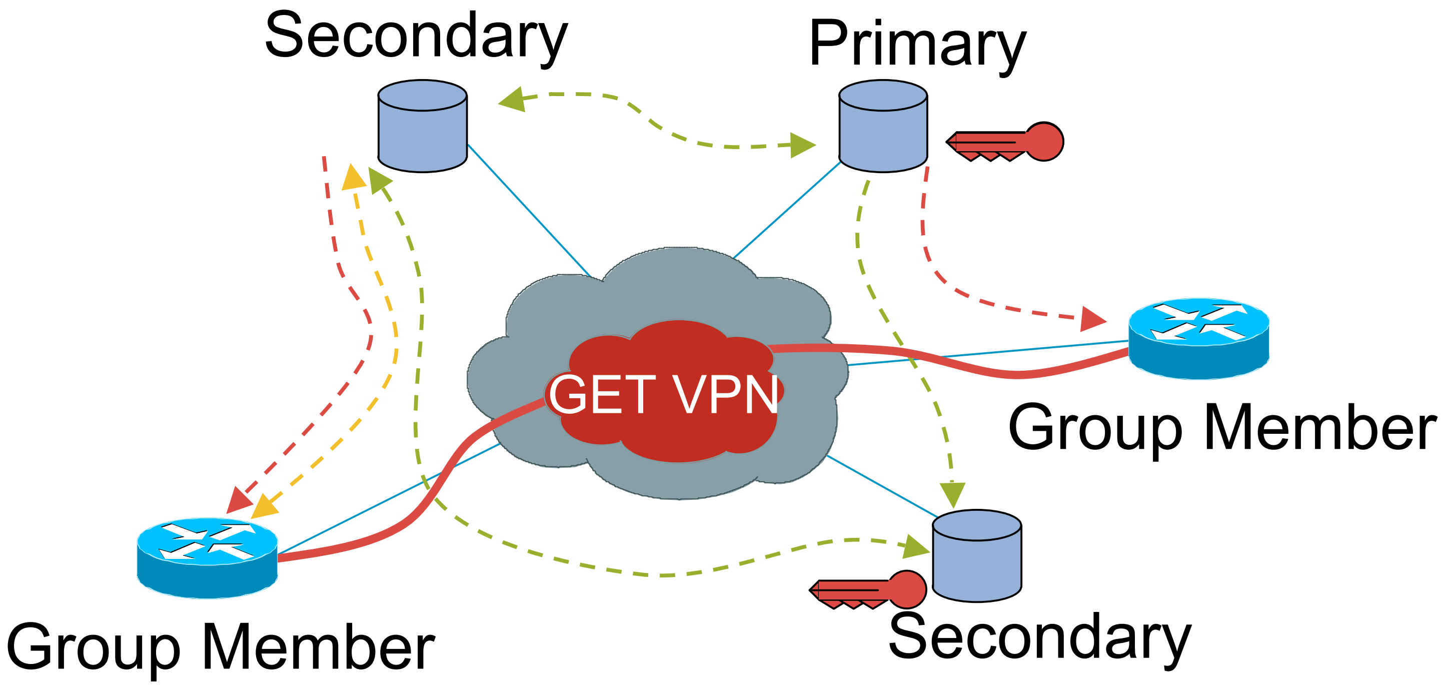
Failure Scenarios: Key Server Failure

- 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



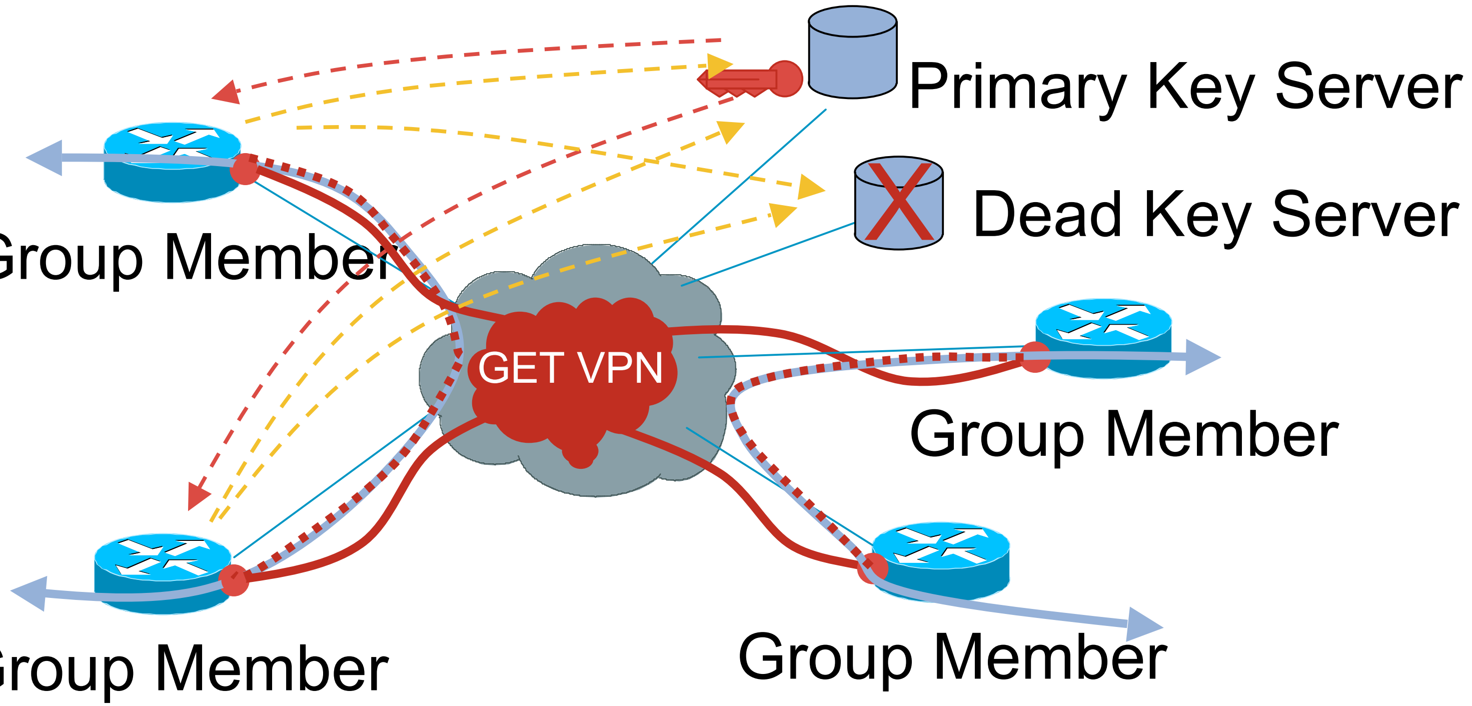
Failure Scenarios: Key Server Recovery

- 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



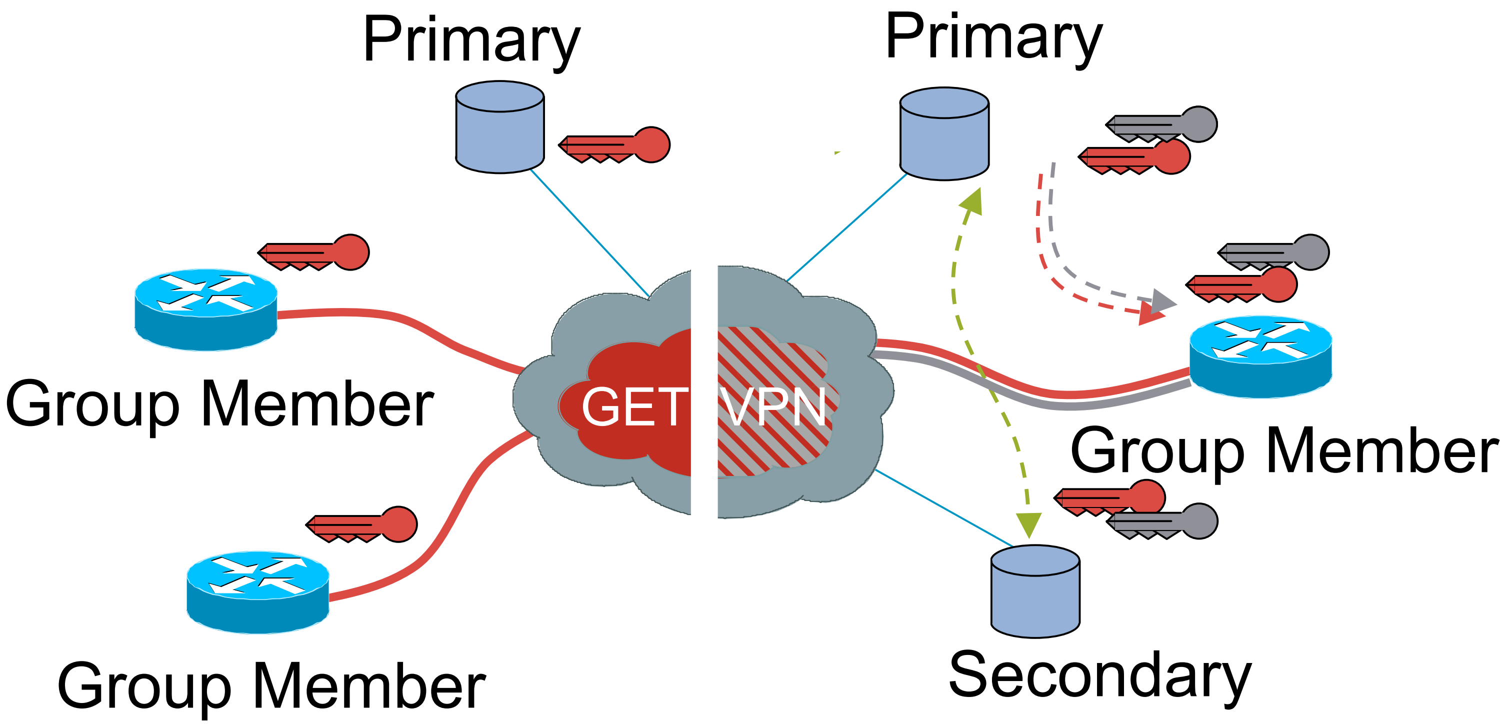
Redundant Key Server

- Group Members Attempt to Register to a Key Server
- Group Member Configured with Ordered Set of Key Server



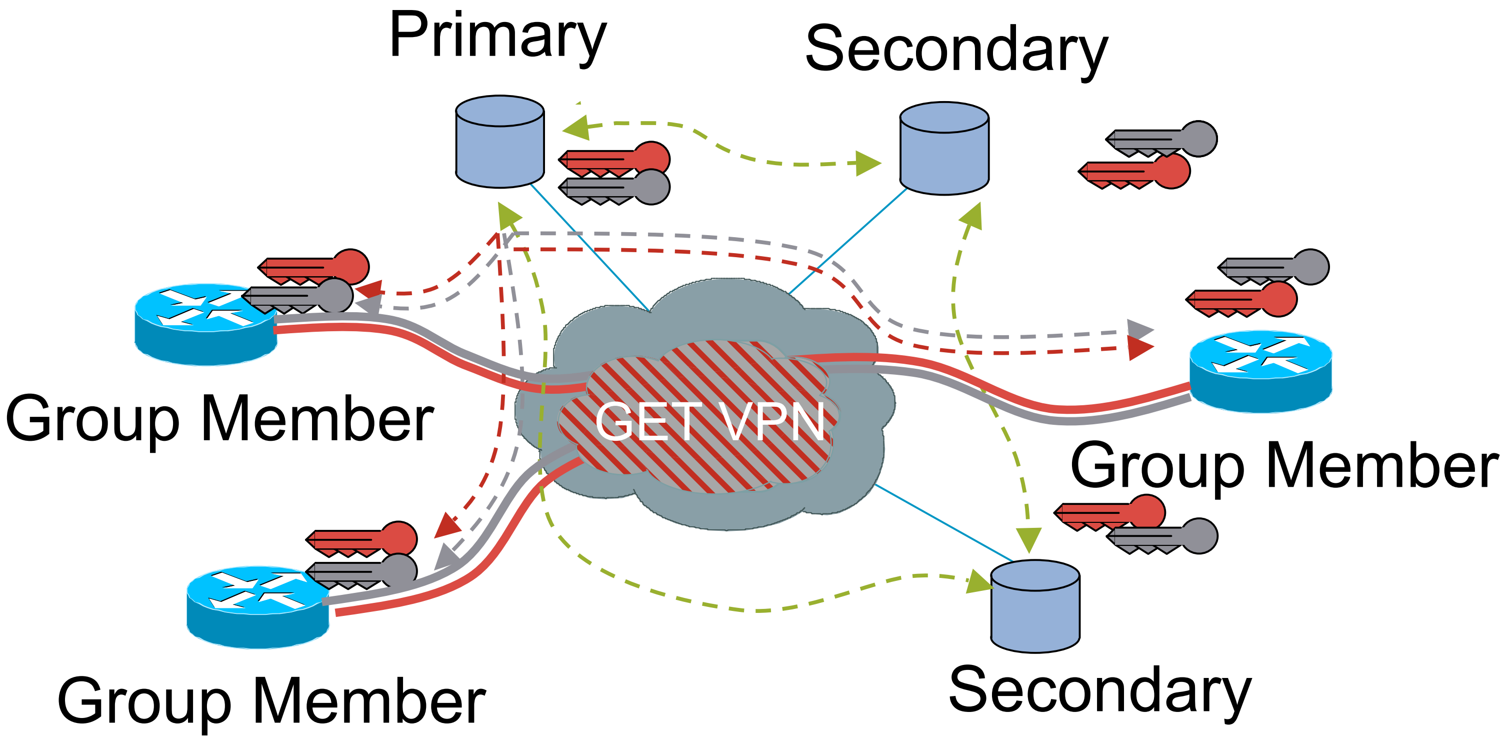
Failure Scenarios: Key Server Partition

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



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



General Architectural Recommendations

- **Key Server Architectural Considerations**

  Distribute Group Member's Preferred Registration Across Multiple Key Servers

  Simplify configuration by using symmetric IPsec proxy identities for entire VPN (eg. 'permit ip any any' or 'permit ip 10/8 10/8')

  Separate KS sites physically but provide highly reliable Cooperative KS connectivity via diverse paths between KS

- **Group Member Architectural Considerations**

  Consistent control plane / management plane selection on all Group Member PE-CE (i.e. IGP, SSH, SYSLOG, etc.)

  Distinct Address Ranges for Management, Data Plane, and Control

Q and A