GET VPN
Group Encrypted Transport VPN

VPN Service Without Tunnels
Networks today need to support all forms of media—including data, voice, and video—to enhance business communications and lower operating costs. Voice and video applications are accelerating the need for instantaneous, branch-to-branch communications, while network security risks are increasing.

Cisco Group Encrypted Transport VPN, eliminates the need for compromise between network intelligence and data privacy in private WAN environments. Service providers can finally offer managed encryption without a provisioning and management nightmare since GET VPN simplifies the provisioning and management of VPN. GET VPN defines a new category of VPN, one that does not use tunnels.

Benefits
• Simplifies branch-to-branch instantaneous communications — Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub
• Maximizes security — Provides encryption for MPLS networks while maintaining network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)
• Complies with governmental regulation and privacy laws — Helps you meet security compliance and internal regulation by encrypting all WAN traffic
• Offers management flexibility — Eliminates complex peer-to-peer key management with group encryption keys

Restrictions for Cisco Group Encrypted Transport VPN
• If you are encrypting high packet rates for counter-based antireplay, ensure that you do not make the lifetime too long or it can take several hours for the sequence number to wrap. For example, if the packet rate is 100 kilopackets per second, the lifetime should be configured as fewer than 11.93 hours so that the SA is used before the sequence number wraps.
• Transport mode should be used only for Group Encrypted Transport VPN Mode (GM) to GM traffic.
• Crypto maps are not supported on tunnel interface and port-channel interface.
• Because Path MTU Discovery (PMTUD) does not work for GET VPN, there is a possibility that encapsulated packets could be dropped when the df-bit is set and the MTU of an intermediate link is less than the size of the encapsulated packet. In such an event, the router that drops the packet sends a notification to the source IP address on the packet, indicating that the packet has been dropped because the router could not fragment the packet due to the df-bit setting. In GET VPN, this message goes past the encapsulating endpoint directly to the source of the data due to the header preservation feature of GET VPN. Thus, the encapsulating router never knows that it has to fragment the packet to a smaller size before setting the df-bit after encapsulation. It continues to set the df-bit on
the packets and they continue to be dropped at the intermediate router. (This is known as black-holing the traffic.)

**Comparison between IPSEC and GET VPN**

<table>
<thead>
<tr>
<th>IPSEC Crypto</th>
<th>GET Crypto</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main concept</strong></td>
<td>Per link point-to-point security paradigm: each pair of devices establishes a separate security association. (figure3)</td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>Requires the establishment of tunnel to secure the traffic between encrypting gateways. - a new header is added to the packet (figure4). - Limited QoS preservation (only ToS).</td>
</tr>
<tr>
<td><strong>Multicast</strong></td>
<td>- Traditional IPSec encapsulate multicast into encrypted PTP unicast GRE tunnels. - Alternatively, inefficient multicast replication at the HUB using DMVPN with many multicast deployment restrictions (RP, MA and multicast source location at the HUB).</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td>IPSec creates Overlay VPN and secures it over the Internet.</td>
</tr>
</tbody>
</table>
**Management**

- Per-link security management: Each pair holds a security association for each other.
- Resource consumption.
- Alternative centralized HUB-based management with DMVPN though heterogeneous protocol suite (mGRE, NHRP).
- Less scalable.

- Full mesh direct communications between sites. Same group members hold a single security association; don’t care about others on the group.
- Relies on centralized membership management through key servers: A centralized entity (Key Server manage the control plane) and not involved in the data plane communication. Data plane communications don’t require transport through a hub HUB entity.
- Low latency/jitter.
- More scalable.

**Security Perimeter**

- Per-link
- All Sites within the same group.

**Routing**

- Two routing levels (figure 5a): Core routing + Overlay routing between encrypting gateways
- Single end-to-end routing level with MPLS-VPN as the underlying VPN infrastructure (figure 6a).

---

**Cisco Group Encrypted Transport VPN Architecture**

GET VPN encompasses Multicast Rekeying, a way to enable encryption for “native” multicast packets, and unicast rekeying over a private WAN. Multicast Rekeying and GET VPN is based on GDOI as defined in Internet Engineering Task Force (IETF) RFC 3547.

**GDOI**

GDOI is defined as the Internet Security Association Key Management Protocol (ISAKMP) Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a group controller or key server (GCKS), which establishes SAs among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association. The Phase 2 exchange is defined in RFC 6407. The topology shown in the figure below and the corresponding explanation show how this protocol works.
**Group Member**

The group member registers with the key server to get the IPsec SA or SAs that are necessary to communicate with the group. The group member provides the group ID to the key server to get the respective policy and keys for this group. These keys are refreshed periodically, and before the current IPsec SAs expire, so that there is no loss of traffic.

**Key Server**

The responsibilities of the key server include maintaining the policy and creating and maintaining the keys for the group. When a group member registers, the key server downloads this policy and the keys to the group member. The key server also rekeys the group before existing keys expire.

The key server has two responsibilities: servicing registration requests and sending rekeys. A group member can register at any time and receive the most current policy and keys. When a group member registers with the key server, the key server verifies the group ID that the group member is attempting to join. If this ID is a valid group ID, the key server sends the SA policy to the group member. After the group member acknowledges that it can handle the downloaded policy, the key server downloads the respective keys.

There are two types of keys that the key server can download: the key encryption key (KEK) and the traffic encryption key (TEK). The TEK becomes the IPsec SA with which the group members within the same group communicate. The KEK encrypts the rekey message.

The GDOI protocol is protected by an ISAKMP Phase 1 exchange. The GDOI key server and the GDOI group member must have the same ISAKMP policy. This Phase 1 ISAKMP policy should be strong enough to protect the GDOI protocol that follows. The GDOI protocol is a four-message exchange that follows the Phase 1 ISAKMP policy. The Phase 1 ISAKMP exchange can occur in main mode or aggressive mode.

**Rekeying**

Rekey messages are used to refresh IPsec SAs. When the IPsec SAs or the rekey SAs are about to expire, one single rekey message for a particular group is generated on the key server. No new IKE sessions are created for the rekey message distribution. The rekey messages are distributed by the key server over an existing IKE SA.

Rekeying can use multicast or unicast messages. GET VPN supports both unicast and multicast rekeying.
With CSCti89255, KEK rekeys before the KEK timer expires. The group member also starts a timer and expects to receive refreshed keys before timer expiration. If they are not received, the group member initiates a jittered re-registration prior to KEK expiry. KEK is deleted when the KEK lifetime expires. This ensure the following:

- A safer KEK expiry checking mechanism
- A safer KEK re-registration mechanism
- Avoids use of KEK beyond configured lifetime
**Task-1:** Configure GET VPN between R1, R2, R3 & R4 as GM-1, GM-2, GM-3 & GM-4 respectively, Configure Key Server with following parameters:

**ISAKMP Parameters:**
- Encryption: 3DES
- Hash: MD5
- DH Group: 2
- Authentication: Pre-Share
- Key: cisco123

**IPSEC Parameters:**
- Encryption: 3DES
- Hash: SHA

**GDOI Parameters:**
- Group Name: Cisco
- Identity Number: 111
- Server: Local
- Address: 192.1.16.6
- Interested Traffic: Source 10.1.0.0/16, Destination 10.1.0.0/26
Initial Configuration:

Key Server:

interface Ethernet0/0
    ip address 192.1.16.6 255.255.255.0
end

router eigrp 1
    network 192.1.16.0

R1 [Group Member -1]:

interface Ethernet0/0
    ip address 192.1.10.1 255.255.255.0
end

interface Ethernet0/1
    ip address 192.1.16.1 255.255.255.0
end

interface Loopback0
    ip address 10.1.1.1 255.255.255.0
end

router eigrp 1
    network 10.0.0.0
    network 192.1.10.0
    network 192.1.16.0

R2 [Group Member -2]:

interface Ethernet0/0
    ip address 192.1.20.2 255.255.255.0
end

interface Loopback0
    ip address 10.1.2.1 255.255.255.0
end

router eigrp 1
    network 10.0.0.0
    network 192.1.20.0

R3 [Group Member -3]:

interface Ethernet0/0
    ip address 192.1.30.3 255.255.255.0
end

interface Loopback0
    ip address 10.1.3.1 255.255.255.0
end
Task-1: Configure GET VPN between R1, R2, R3 & R4 as GM-1, GM-2, GM-3 & GM-4 respectively, Configure Key Server with following parameters:

Solution:

Step-1: Configure ISAKMP on Key Server [With all the GM’s]:

crypto isakmp policy 1
  encript 3des
  hash md5
  authentication pre-share
  group 2
  crypto isakmp key cisco123 address 192.1.10.1
  crypto isakmp key cisco123 address 192.1.20.2
  crypto isakmp key cisco123 address 192.1.30.3
  crypto isakmp key cisco123 address 192.1.40.4
Step-2: Configure IPSEC Transform Set:

```bash
crypto ipsec transform-set GET-TSET esp-3des esp-sha-hmac
```

Step-3: Configure IPSEC Profile:

```bash
crypto ipsec profile GET-PROF
    set transform-set GET-TSET
```

Step-4: Configure Interested Traffic ACL:

```bash
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
```

Step-5: Configure GDOI Group:

```bash
crypto gdoi group CISCO
    identity number 111
    server local
    sa ipsec 1
        profile GET-PROF
        match address ipv4 101
        address ipv4 192.1.16.6
```

Configure Group Members:

R1 [Group Member -1]:

Step-1: Configure ISAKMP with Key Server to exchange session key:

```bash
crypto isakmp policy 1
    encr 3des
    hash md5
    authentication pre-share
    group 2
    crypto isakmp key cisco123 address 192.1.16.6
```

Step-2: Configure GDOI Group:

```bash
crypto gdoi group ABC
    identity number 111
    server address ipv4 192.1.16.6
```

Step-3: Configure GDOI Crypto Map:

```bash
crypto map CMAP 1 gdoi
    set group ABC
```

Step-4: Apply crypto map to WAN Interface:

```bash
interface Ethernet0/0
    crypto map CMAP
end
```
R2 [Group Member -2]:

Step-1: Configure ISAKMP with Key Server to exchange session key:

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.1.16.6
```

Step-2: Configure GDOI Group:

```
crypto gdoi group ABC
  identity number 111
  server address ipv4 192.1.16.6
```

Step-3: Configure GDOI Crypto Map:

```
crypto map CMAP 1 gdoi
  set group ABC
```

Step-4: Apply crypto map to WAN Interface:

```
interface Ethernet0/0
  crypto map CMAP
end
```

R3 [Group Member -3]:

Step-1: Configure ISAKMP with Key Server to exchange session key:

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.1.16.6
```

Step-2: Configure GDOI Group:

```
crypto gdoi group ABC
  identity number 111
  server address ipv4 192.1.16.6
```

Step-3: Configure GDOI Crypto Map:

```
crypto map CMAP 1 gdoi
  set group ABC
```
Step-4: Apply crypto map to WAN Interface:

```bash
interface Ethernet0/0
    crypto map CMAP
end
```

R4 [Group Member -3]:

Step-1: Configure ISAKMP with Key Server to exchange session key:

```bash
crypto isakmp policy 1
    encr 3des
    hash md5
    authentication pre-share
    group 2
    crypto isakmp key cisco123 address 192.1.16.6
```

Step-2: Configure GDOI Group:

```bash
crypto gdoi group ABC
    identity number 111
    server address ipv4 192.1.16.6
```

Step-3: Configure GDOI Crypto Map:

```bash
crypto map CMAP 1 gdoi
    set group ABC
```

Step-4: Apply crypto map to WAN Interface:

```bash
interface Ethernet0/0
    crypto map CMAP
end
```

As soon as you apply crypto map to WAN interface your GM will get registered to KS and download the configuration from KS, you will get following message:

```
*Feb 25 03:41:30.311: %CRYPTO-5-GM_REGISTER: Start registration to KS 192.1.16.6 for group ABC using address 192.1.10.1 fvrf default ivrf default  
*Feb 25 03:41:30.312: %GDOI-5-SA_TEK_UPDATED: SA TEK was updated  
*Feb 25 03:41:30.313: %GDOI-5-GM_REGS_COMPL: Registration to KS 192.1.16.6 complete for group ABC using address 192.1.10.1 fvrf default ivrf default  
*Feb 25 03:41:30.313: %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies from KS 192.1.16.6 for group ABC & gm identity 192.1.10.1 fvrf default ivrf default
```
Verification:

Group Member:

R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst    src     state     conn-id status
192.1.16.6  192.1.10.1  DOI_IDLE    1001 ACTIVE

R1#show crypto ipsec sa
interface: Ethernet0/0
    Crypto map tag: CMAP, local addr 192.1.10.1

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (10.1.0.0/255.255.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.1.0.0/255.255.0.0/0/0)
    Group: ABC
    current peer 0.0.0.0 port 848
        PERMIT, flags={}

        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts compr. failed: 0
        #pkts not decompressed: 0, #pkts decompress failed: 0
        #send errors 0, #recv errors 0

    local crypto endpt.: 192.1.10.1, remote crypto endpt.: 0.0.0.0

    plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb

    Ethernet0/0
        current outbound spi: 0xB3A0C220(3013657120)
        PFS (Y/N): N, DH group: none

        inbound esp sas:
            spi: 0xB3A0C220(3013657120)

            transform: esp-3des esp-sha-hmac
            in use settings ={Tunnel, }
            conn id: 3, flow_id: SW:3, sibling_flags 80000040, crypto map: CMAP

        sa timing: remaining key lifetime (sec): 1444
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: N
        status: ACTIVE(ACTIVE)

        inbound ah sas:

        inbound pcp sas:

        outbound esp sas:
            spi: 0xB3A0C220(3013657120)

            transform: esp-3des esp-sha-hmac
            in use settings ={Tunnel, }
            conn id: 4, flow_id: SW:4, sibling_flags 80000040, crypto map: CMAP

        sa timing: remaining key lifetime (sec): 1444
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

RI#show crypto gdoi
GROUP INFORMATION

<table>
<thead>
<tr>
<th>Group Name</th>
<th>ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Identity</td>
<td>11</td>
</tr>
<tr>
<td>Crypto Path</td>
<td>ipv4</td>
</tr>
<tr>
<td>Key Management Path</td>
<td>ipv4</td>
</tr>
<tr>
<td>Rekeys received</td>
<td>0</td>
</tr>
<tr>
<td>IPSec SA Direction</td>
<td>Both</td>
</tr>
<tr>
<td>Group Server list</td>
<td>192.1.16.6</td>
</tr>
</tbody>
</table>

Group Member Information For Group ABC:
IPSec SA Direction : Both
ACL Received From KS : gdoi_group_ABC_temp_acl

<table>
<thead>
<tr>
<th>Group member</th>
<th>192.1.10.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>None</td>
</tr>
<tr>
<td>Local addr/port</td>
<td>192.1.10.1/848</td>
</tr>
<tr>
<td>Remote addr/port</td>
<td>192.1.16.6/848</td>
</tr>
<tr>
<td>fvrf/ivrf</td>
<td>None/None</td>
</tr>
<tr>
<td>Version</td>
<td>1.0.8</td>
</tr>
<tr>
<td>Registration status</td>
<td>Registered</td>
</tr>
<tr>
<td>Registered with</td>
<td>192.1.16.6</td>
</tr>
<tr>
<td>Re-registers in</td>
<td>1324 sec</td>
</tr>
<tr>
<td>Succeeded registration : 2</td>
<td></td>
</tr>
<tr>
<td>Attempted registration : 2</td>
<td></td>
</tr>
<tr>
<td>Last rekey from</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Last rekey seq num</td>
<td>0</td>
</tr>
<tr>
<td>Multicast rekey rcvd</td>
<td>0</td>
</tr>
<tr>
<td>DP Error Monitoring</td>
<td>OFF</td>
</tr>
<tr>
<td>Active TEK Number</td>
<td>1</td>
</tr>
</tbody>
</table>

allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Received : never

ACL Downloaded From KS 192.1.16.6:
access-list permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255

TEK POLICY for the current KS-Policy ACEs Downloaded:
Ethernet0/0:
IPsec SA:
sp1: 0xB3A0C220(3013657120)
transform: esp-3des esp-eha-hmac
sa timing:remaining key lifetime (sec): (1419)
Anti-Replay(Counter Based) : 64
tag method : disabled
R1#ping 10.1.2.1 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms

R1#ping 10.1.3.1 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.3.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms

R1#ping 10.1.4.1 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.4.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms

Key Server:

KEY-SERVER#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.1.16.6</td>
<td>192.1.40.4</td>
<td>GDOI_IDLE</td>
<td>1001</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>192.1.16.6</td>
<td>192.1.10.1</td>
<td>GDOI_IDLE</td>
<td>1003</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>192.1.16.6</td>
<td>192.1.30.3</td>
<td>GDOI_IDLE</td>
<td>1002</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>192.1.16.6</td>
<td>192.1.20.2</td>
<td>GDOI_IDLE</td>
<td>1004</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

KEY-SERVER#show crypto ipsec sa
No SAs found

KEY-SERVER#show crypto gdoi detail
GROUP INFORMATION

Group Name : CISCO (Multicast)
Re-auth on new CRL : Disabled
Group Identity : 1
Crypto Path : ipv4
Key Management Path : ipv4
Group Members : 4
IPSec SA Direction : Both
Group Rekey Lifetime : 86400 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 2

IPSec SA Number : 1
IPSec SA Rekey Lifetime: 3600 secs
Profile Name : GET-PROF
Replay method : Count Based
VRF [Virtual Routing & Forwarding]

Virtual Private Networks (VPNs) provide a secure way for customers to share bandwidth over an ISP backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table. A VPN routing table is called a VPN routing/forwarding (VRF) table.

About VRF-lite

VRF-lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but a Layer 3 interface cannot belong to more than one VRF at any time.

Terminology

- \text{ivrf} : Inside VRF, the VRF that contains the clear-text traffic (before encryption for outbound flows and after decryption for inbound flows)
- \text{fvrf} : Front-door VRF (or outside VRF), the VRF that contain the encrypted traffic
- \text{global VRF} : the routing instance that is used if no specific VRF is defined. If no VRF-aware config is used, everything is done in the global VRF and all interfaces are in the global VRF.
**Configuration Example:**

**Task-1:** Configure VRF – CUST-A on R1, R2, R3 & R4 and VRF – CUST-B with dedicated links between R2 & R3 and run EIGRP 100 and 200 Respectively.

**Task-2:** Configure IPSEC Site-to-Site VPN between R2 and R3 for encrypting Traffic between R1 LAN – 10.1.1.0/24 & R4 LAN – 10.2.2.0/24.

**Initial Configuration:**

**R1:**

```plaintext
interface FastEthernet0/0
 ip address 192.1.10.1 255.255.255.0
duplex auto
speed auto
end

interface Loopback0
 ip address 10.1.1.1 255.255.255.0
end
```

**R2:**

```plaintext
ip vrf CUST-A
ip vrf CUST-B

interface FastEthernet0/0
 ip vrf forwarding CUST-A
 ip address 192.1.10.2 255.255.255.0
duplex auto
speed auto
end

interface FastEthernet0/1
 ip vrf forwarding CUST-A
```
ip address 172.16.1.2 255.255.255.0
duplex auto
speed auto
end

interface FastEthernet1/0
ip vrf forwarding CUST-B
ip address 172.16.2.2 255.255.255.0
duplex auto
speed auto
end

interface FastEthernet2/0
ip vrf forwarding CUST-B
ip address 192.1.10.2 255.255.255.0
duplex auto
speed auto
end

R3:

ip vrf CUST-A
ip vrf CUST-B

interface FastEthernet0/0
ip vrf forwarding CUST-A
ip address 192.1.20.3 255.255.255.0
duplex auto
speed auto
end

interface FastEthernet0/1
ip vrf forwarding CUST-A
ip address 172.16.1.3 255.255.255.0
duplex auto
speed auto
end

interface FastEthernet1/0
ip vrf forwarding CUST-B
ip address 172.16.2.3 255.255.255.0
duplex auto
speed auto
end

interface FastEthernet2/0
ip vrf forwarding CUST-B
ip address 192.1.20.3 255.255.255.0
duplex auto
speed auto
end
R4:

interface FastEthernet0/0
  ip address 192.1.20.4 255.255.255.0
duplex auto
  speed auto
end

interface Loopback0
  ip address 10.2.2.2 255.255.255.0
end

R5:

interface FastEthernet0/0
  ip address 192.1.10.5 255.255.255.0
duplex auto
  speed auto
end

interface Loopback0
  ip address 10.1.1.5 255.255.255.0
end

R6:

interface FastEthernet0/0
  ip address 192.1.20.6 255.255.255.0
duplex auto
  speed auto
end

interface Loopback0
  ip address 10.2.2.6 255.255.255.0
end
**Task-1:** Configure VRF – CUST-A on R1, R2, R3 & R4 and VRF – CUST-B with dedicated links between R2 & R3 and run EIGRP 100 and 200 Respectively.

**Solution:**

R1:

```
router eigrp 100
network 10.0.0.0
network 192.1.10.0
no auto-summary
```

R2:

```
router eigrp 1
auto-summary
!
address-family ipv4 vrf CUST-B
  network 172.16.0.0
  network 192.1.10.0
  no auto-summary
  autonomous-system 200
exit-address-family
!
address-family ipv4 vrf CUST-A
  network 172.16.0.0
  network 192.1.10.0
  no auto-summary
  autonomous-system 100
exit-address-family
```

R3:

```
router eigrp 1
auto-summary
!
address-family ipv4 vrf CUST-B
  network 172.16.2.0 0.0.0.255
  network 192.1.20.0
  no auto-summary
  autonomous-system 200
exit-address-family
!
address-family ipv4 vrf CUST-A
  network 172.16.1.0 0.0.0.255
  network 192.1.20.0
  no auto-summary
  autonomous-system 100
exit-address-family
```

R4:

```
router eigrp 100
network 10.0.0.0
network 192.1.20.0
```
no auto-summary

R5:

router eigrp 200
network 10.0.0.0
network 192.1.10.0
no auto-summary

R6:

router eigrp 200
network 10.0.0.0
network 192.1.20.0
no auto-summary

Verification:

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
   ia - IS-IS inter area, * - candidate default, U - per-user
static route
   o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C  192.1.10.0/24 is directly connected, FastEthernet0/0
C  172.16.0.0/24 is subnetted, 1 subnets
   172.16.1.0 [90/307200] via 192.1.10.2, 00:14:38, FastEthernet0/0
D  192.1.20.0/24 [90/332800] via 192.1.10.2, 00:14:38, FastEthernet0/0
D  10.0.0.0/24 is subnetted, 2 subnets
D  10.2.2.0 [90/460800] via 192.1.10.2, 00:14:38, FastEthernet0/0
C  10.1.1.0 is directly connected, Loopback0
R1#

R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
   ia - IS-IS inter area, * - candidate default, U - per-user
static route
   o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
192.1.10.0/24 [90/332800] via 192.1.20.3, 00:13:58, FastEthernet0/0
172.16.0.0/24 is subnetted, 1 subnets
172.16.1.0 [90/307200] via 192.1.20.3, 00:13:58, FastEthernet0/0
192.1.20.0/24 is directly connected, FastEthernet0/0
10.0.0.0/24 is subnetted, 2 subnets
10.0.0.0/24 is directly connected, Loopback0
10.1.1.0 [90/460800] via 192.1.20.3, 00:13:57, FastEthernet0/0

R4#show ip route vrf CUST

Routing Table: CUST-A
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user
static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.1.10.0/24 is directly connected, FastEthernet0/0
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.1.0 is directly connected, FastEthernet0/1
D 192.1.20.0/24 [90/307200] via 172.16.1.3, 00:15:27, FastEthernet0/1
10.0.0.0/24 is subnetted, 2 subnets
D 10.2.2.0 [90/435200] via 172.16.1.3, 00:15:27, FastEthernet0/1
D 10.1.1.0 [90/409600] via 192.1.10.1, 00:15:26, FastEthernet0/0

R2#show ip route vrf CUST-B

Routing Table: CUST-B
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user
static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.1.10.0/24 is directly connected, FastEthernet2/0
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.2.0 is directly connected, FastEthernet1/0
D 192.1.20.0/24 [90/307200] via 172.16.2.3, 00:15:41, FastEthernet1/0
10.0.0.0/24 is subnetted, 2 subnets
D 10.2.2.0 [90/158720] via 172.16.2.3, 00:15:41, FastEthernet1/0
D 10.1.1.0 [90/156160] via 192.1.10.5, 00:15:40, FastEthernet2/0
R2#

R1#ping 10.2.2.2 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/37/52 ms
R1#

R1#traceroute 10.2.2.2 source 10.1.1.1
Type escape sequence to abort.
Tracing the route to 10.2.2.2

1 192.1.10.2 60 msec 44 msec 76 msec
2 172.16.1.3 108 msec 104 msec 108 msec
3 192.1.20.4 108 msec 136 msec *
R1#

Task-2: Configure IPSEC Site-to-Site VPN between R2 and R3 for encrypting Traffic between R1 LAN – 10.1.1.0/24 & R4 LAN – 10.2.2.0/24.

Solution:

R2:

Step-1 [A]: Configure ISAKMP Policy:

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
```

Step-1 [B]: Configure Keyring:

```
crypto keyring KR-1 vrf CUST-A
  pre-shared-key address 172.16.1.3 key cisco123
```

Step-1[C]: Configure ISAKMP Profile:

```
crypto isakmp profile PROF-1
  vrf CUST-A
  keyring KR-1
  match identity address 172.16.1.3 255.255.255.255 CUST-A
```

Step-2: Configure IPSEC Transform Set:

```
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```
Step-3: Configure Interested Traffic ACL:

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
```

Step-4: Configure Crypto map:

```
crypto map CMAP isakmp-profile PROF-1
crypto map CMAP 1 ipsec-isakmp
    set peer 172.16.1.3
    set transform-set TSET
match address 101
```

Step-5: Apply Crypto Map to interface:

```
interface FastEthernet0/1
crypto map CMAP
end
```

R3:

Step-1 [A]: Configure ISAKMP Policy:

```
crypto isakmp policy 1
    encr 3des
    hash md5
    authentication pre-share
    group 2
```

Step-1 [B]: Configure Keyring:

```
crypto keyring KR-1 vrf CUST-A
    pre-shared-key address 172.16.1.2 key cisco123
```

Step-1[C]: Configure ISAKMP Profile:

```
crypto isakmp profile PROF-1
    vrf CUST-A
    keyring KR-1
    match identity address 172.16.1.2 255.255.255.255 CUST-A
```

Step-2: Configure IPSEC Transform Set:

```
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```

Step-3: Configure Interested Traffic ACL:

```
access-list 101 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
```

Step-4: Configure Crypto map:

```
crypto map CMAP isakmp-profile PROF-1
crypto map CMAP 1 ipsec-isakmp
    set peer 172.16.1.2
```
set transform-set TSET
match address 101

Step-5: Apply Crypto Map to interface:

interface FastEthernet0/1
crypto map CMAP
end

Verification:

R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst  src  state  conn-id slot status
172.16.1.3  172.16.1.2  QM_IDLE  1001  0 ACTIVE

R2#show crypto ipsec sa
interface: FastEthernet0/1
    Crypto map tag: CMAP, local addr 172.16.1.2
    protected vrf: CUST-A
    local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
    current peer 172.16.1.3 port 500
        PERMIT, flags={origin_is_acl,}
        #pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
        #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts compr. failed: 0
        #pkts not decompressed: 0, #pkts decompress failed: 0
        #send errors 1, #recv errors 0

    local crypto endpt.: 172.16.1.2, remote crypto endpt.: 172.16.1.3
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
    current outbound spi: 0x82DD20EA(2195529962)
    inbound esp sas:
        spi: 0xDE0EBA70(3725507184)
        transform: esp-3des esp-md5-hmac
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4590314/2663)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
        spi: 0x82DD20EA(2195529962)
        transform: esp-3des esp-md5-hmac
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4590314/2663)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

R1#ping 10.2.2.2 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/137/144 ms

R4#ping 10.1.1.1 source 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/47/60 ms
R4#
VRF Aware GET VPN

**Task-1:** Configure VRF CUST-A between R1 & R2, in which 10.1.1.0/24 should be able to communicate with 10.2.2.0/24.

**Task-2:** Configure VRF CUST-B between R2 & R3, in which 10.1.1.0/24 should be able to communicate with 10.2.2.0/24.

**Task-3:** Configure Route Leaking between VRF CUST-A [R1 & R2], VRF CUST-B [R2 & R3] with global routing, so that all VRF Members can communicate with Key Server [R5].

**Task-4:** Configure GET VPN Setup between R1, R2, R3 & R5, where R5 is acting as Key server for two VPN Groups, R1 & R2 will be participating in VPN Group CUST-A and R2 & R3 will be participating in VPN Group CUST-B.

**Solution:**

R1:

```
interface Ethernet0/0
ip address 192.1.10.1 255.255.255.0
```
interface Loopback0
  ip address 10.1.1.1 255.255.255.0
end

ip route 10.2.2.0 255.255.255.0 192.1.10.2

R3:

interface Ethernet0/0
  ip address 192.1.20.3 255.255.255.0
end

interface Loopback0
  ip address 10.1.1.1 255.255.255.0
end

ip route 10.2.2.0 255.255.255.0 192.1.20.2

R2:

ip vrf CUST-A
ip vrf CUST-B

interface Ethernet0/0
  ip vrf forwarding CUST-A
  ip address 192.1.10.2 255.255.255.0
end

interface Ethernet0/1
  ip vrf forwarding CUST-B
  ip address 192.1.20.2 255.255.255.0
end

ip route vrf CUST-A 10.1.1.1 255.255.255.255 192.1.10.1
ip route vrf CUST-B 10.1.1.1 255.255.255.255 192.1.20.3

Verification:

R2#show ip route vrf CUST-A

Routing Table: CUST-A
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S 10.1.1.1/32 [1/0] via 192.1.10.1
C 10.2.2.0/24 is directly connected, Loopback2
L 10.2.2.2/32 is directly connected, Loopback2
192.1.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.10.0/24 is directly connected, Ethernet0/0
L 192.1.10.2/32 is directly connected, Ethernet0/0
S 192.1.145.0.24/32 [1/0] via 192.1.145.4, Ethernet0/2

R2#ping vrf CUST-A 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R2#ping vrf CUST-B 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/5 ms

R1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
**Task-3:** Configure Route Leaking between VRF CUST-A [R1 & R2], VRF CUST-B [R2 & R3] with global routing, so that all VRF Members can communicate with Key Server [R5].

**Solution:**

**R1:**

```
ip route 192.1.45.0 255.255.255.0 192.1.10.2
```

**R3:**

```
ip route 192.1.45.0 255.255.255.0 192.1.20.2
```

**R4 [ISP]:**

```
ip route 192.1.10.0 255.255.255.0 192.1.24.2
ip route 192.1.20.0 255.255.255.0 192.1.24.2
```

**R2:**

```
ip route 0.0.0.0 0.0.0.0 192.1.24.4
ip route 192.1.10.0 255.255.255.0 Ethernet0/0
ip route 192.1.20.0 255.255.255.0 Ethernet0/1
ip route vrf CUST-A 192.1.45.0 255.255.255.0 Ethernet0/2 192.1.24.4 global
ip route vrf CUST-B 192.1.45.0 255.255.255.0 Ethernet0/2 192.1.24.4 global
```

**Verification:**

**R1#ping 192.1.45.5**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.45.5, timeout is 2 seconds: 
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

**R3#ping 192.1.45.5**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.45.5, timeout is 2 seconds: 
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```
**Task-4:** Configure GET VPN Setup between R1, R2, R3 & R5, where R5 is acting as Key server for two VPN Groups, R1 & R2 will be participating in VPN Group CUST-A and R2 & R3 will be participating in VPN Group CUST-B.

**Solution:**

**R5 [Key Server]:**

**Step-1:** Configure Phase I

```plaintext
crypto isakmp policy 1
.encr 3des
.hash md5
.authentication pre-share
.group 2
.crypto isakmp key cisco123 address 192.1.10.0
.crypto isakmp key cisco123 address 192.1.20.0
```

**Step-2:** Configure Phase II

```plaintext
crypto ipsec transform-set CUST-A esp-aes esp-sha-hmac
.mode tunnel
.crypto ipsec transform-set CUST-B esp-3des esp-md5-hmac
.mode tunnel
```

**Step-3:** Interested Traffic:

```plaintext
access-list 101 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
access-list 102 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

**Step-4:** Configure IPSEC Profile:

```plaintext
crypto ipsec profile CUST-A
.set transform-set CUST-A
.crypto ipsec profile CUST-B
.set transform-set CUST-B
```

**Step-5:** Configure GDOI Groups:

```plaintext
crypto gdoi group CUST-A
.identity number 100
.server local
.sa ipsec 10
.profile CUST-A
.match address ipv4 101
.replay counter window-size 64
.no tag
.address ipv4 192.1.45.5
```
Non-VRF Group Members:

R1:

Step-1: Configure Phase I

crpyto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco123 address 192.1.45.5

Step-2: Configure GDOI Group

crpyto gdoi group ABC
identity number 100
server address ipv4 192.1.45.5

Step-3: Configure GDOI Crypto Map

crpyto map CMAP 1 gdoi
set group ABC

Step-4: Apply Crypto Map to WAN Interface:

interface Ethernet0/0
   crypto map CMAP
end
R3:

**Step-1:** Configure Phase I

```plaintext
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.1.45.5
```

**Step-2:** Configure GDOI Group

```plaintext
crypto gdoi group ABC
  identity number 100
  server address ipv4 192.1.45.5
```

**Step-3:** Configure GDOI Crypto Map

```plaintext
crypto map CMAP 1 gdoi
  set group ABC
```

**Step-4:** Apply Crypto Map to WAN Interface:

```plaintext
interface Ethernet0/0
  crypto map CMAP
end
```

**VRF Aware Group Members:**

R2:

**Step-1:** Configure Phase I

**Step-1 [A]:** Configure ISAKMP Policy

```plaintext
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
```

**Step-1 [B]:** Configure Keyring

```plaintext
crypto keyring CUST-A vrf CUST-A
  pre-shared-key address 192.1.45.5 key cisco123
crypto keyring CUST-B vrf CUST-B
  pre-shared-key address 192.1.45.5 key cisco123
```
**Step-1 [C]:** Configure ISAKMP Profile

```snippet
crypto isakmp profile CUST-A  
  vrf CUST-A  
  keyring CUST-A  
  match identity address 192.1.45.5 255.255.255.255 CUST-A

crypto isakmp profile CUST-B  
  vrf CUST-B  
  keyring CUST-B  
  match identity address 192.1.45.5 255.255.255.255 CUST-B
```

**Step-2:** Configure GDOI Groups:

```snippet
crypto gdoi group CUST-A  
  identity number 100  
  server address ipv4 192.1.45.5

crypto gdoi group CUST-B  
  identity number 200  
  server address ipv4 192.1.45.5
```

**Step-3:** Configure GDOI Crypto Map:

```snippet
crypto map CUST-A isakmp-profile CUST-A

crypto map CUST-A 1 gdoi  
  set group CUST-A

crypto map CUST-B isakmp-profile CUST-B

crypto map CUST-B 1 gdoi  
  set group CUST-B
```

**Step-5:** Apply Crypto Maps to Appropriate WAN Interfaces:

```snippet
interface Ethernet0/0  
  ip vrf forwarding CUST-A  
  crypto map CUST-A
end

interface Ethernet0/1  
  ip vrf forwarding CUST-B  
  crypto map CUST-B
end
```
Verification:

KEY_SERVER# show crypto gdoi ks mem

Group Member Information:

Number of rekeys sent for group CUST-A: 0

Group Member ID: 192.1.10.1, GM Version: 1.0.8
   Group ID: 100
   Group Name: CUST-A
   GM State: Registered
   Key Server ID: 192.1.45.5

Group Member ID: 192.1.10.2, GM Version: 1.0.8
   Group ID: 100
   Group Name: CUST-A
   GM State: Registered
   Key Server ID: 192.1.45.5

Number of rekeys sent for group CUST-B: 0

Group Member ID: 192.1.20.2, GM Version: 1.0.8
   Group ID: 200
   Group Name: CUST-B
   GM State: Registered

Group Member Information:

   Key Server ID: 192.1.45.5

Group Member ID: 192.1.20.3, GM Version: 1.0.8
   Group ID: 200
   Group Name: CUST-B
   GM State: Registered
   Key Server ID: 192.1.45.5

KEY_SERVER#

KEY_SERVER# show crypto gdoi

GROUP INFORMATION

   Group Name: CUST-A (Multicast)
   Re-auth on new CRL: Disabled
   Group Identity: 100
   Crypto Path: ipv4
   Key Management Path: ipv4
   Group Members: 2
   IPSec SA Direction: Both
   Group Rekey Lifetime: 86400 secs
   Rekey Retransmit Period: 10 secs
   Rekey Retransmit Attempts: 2

   IPSec SA Number: 10
   IPSec SA Rekey Lifetime: 3600 secs
   Profile Name: CUST-A
   Replay method: Count Based
   Replay Window Size: 64
Tagging method : Disabled
SA Rekey Remaining Lifetime : 2658 secs
Time to Rekey : 2277 secs
ACL Configured : access-list 101

Group Server list : Local

GROUP INFORMATION

Group Name : CUST-B (Multicast)
Re-auth on new CRL : Disabled
Group Identity : 200
Crypto Path : ipv4
Key Management Path : ipv4
Group Members : 2
IPSec SA Direction : Both
Group Rekey Lifetime : 86400 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 2
IPSec SA Number : 10
IPSec SA Rekey Lifetime: 3600 secs
Profile Name : CUST-B
Replay method : Count Based
Replay Window Size : 64
Tagging method : Disabled
SA Rekey Remaining Lifetime : 2658 secs
Time to Rekey : 2277 secs
ACL Configured : access-list 102

Group Server list : Local

R1#show crypto gdoi
GROUP INFORMATION

Group Name : ABC
Group Identity : 100
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 192.1.45.5

Group Member Information For Group ABC:
IPSec SA Direction : Both
ACL Received From KS : gdoi_group_ABC_temp_acl

Group member : 192.1.10.1  vrf: None
Local addr/port : 192.1.10.1/848
Remote addr/port : 192.1.45.5/848
fvrf/ivrf : None/None
Version : 1.0.8
Registration status : Registered
Registered with : 192.1.45.5
Re-registers in : 2419 sec
Succeeded registration: 3
Attempted registration: 3
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Multicast rekey rcvd : 0
DP Error Monitoring : OFF
Active TEK Number : 1

allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Received : never

ACL Downloaded From KS 192.1.45.5:
  access-list permit ip 10.0.0.0 0.255.255.255 10.0.0.0
  0.255.255.255

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet0/0:
    IPsec SA:
      spi: 0x8F720945(2406615365)
      transform: esp-aes esp-sha-hmac
      sa timing:remaining key lifetime (sec): (2626)
      Anti-Replay(Counter Based) : 64
      tag method : disabled
      alg key size: 16 (bytes)
      sig key size: 20 (bytes)
      encaps: ENCAPS_TUNNEL

R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
192.1.45.5 192.1.10.1 GDOI_IDLE 1001 ACTIVE

Thank You !!!