DMVPN to Group Encrypted Transport VPN Migration

This document provides the steps for Dynamic Multipoint VPN (DMVPN) to Group Encrypted Transport VPN migration.

DMVPN to Group Encrypted Transport VPN Migration

Following are the steps involved in migrating from DMVPN to Group Encrypted Transport VPN:

1. Hub-and-spoke and spoke-to-spoke DMVPN (multipoint generic routing encapsulation [mGRE]) tunnels are established with IP Security (IPsec) protection. Tunnel protection is applied to the tunnel interface.
2. The key server is introduced to the IP VPN.
3. Routing metrics are modified on the tunnel interfaces.
4. The routed path is modified to include the Group Encrypted Transport-enabled core.
5. Symmetric routing between branch offices is enabled in the hub. Headquarters is transitioned to use Group Encrypted Transport VPN encryption first. The Group Domain of Interpretation (GDOI) cryptography map excludes Encapsulating Security Payload (ESP) traffic (that is, Generic Routing Encapsulation [GRE] + IPsec) so that traffic is not encrypted twice (once by DMVPN and a second time by GRE).
6. Individual sites are transitioned to Group Encrypted Transport VPN one at a time. Group Encrypted Transport-enabled interfaces are confirmed operational. Symmetric routing between branch offices is required during transition for network stability.
7. DMVPN is removed from branch offices and headquarters. Tunnel interfaces are removed on a per-peer basis. GRE and IPsec peers and modified routing metrics are removed.

These seven steps are described in detail in the following sections.

Step 1: DMVPN IPSec Protection

DMVPN IPsec encryption is deployed between branch offices and headquarters.

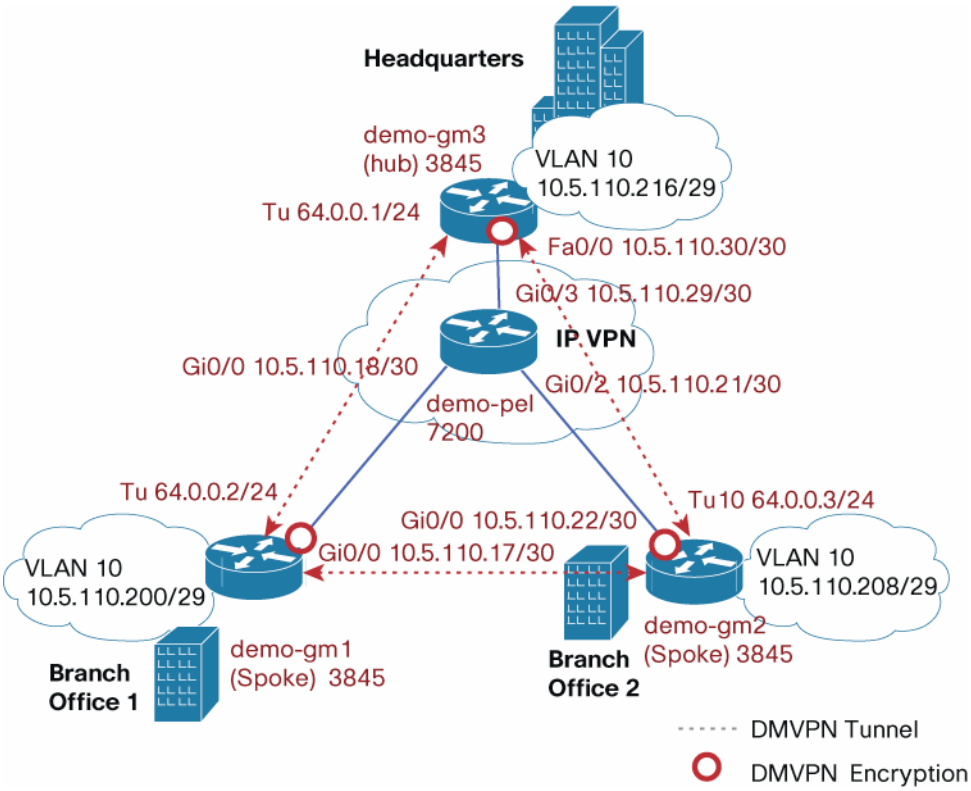
DMVPN Solution Test Setup Topology

Solution test setup consists of two DMVPN spoke routers, demo-gm1 and demo-gm2, located in branch offices and one DMVPN hub router, demo-gm3, located at headquarters. The IP VPN network is simulated by “demo-pe1”. The Cisco 3845 Integrated Services Router platform routers running the Cisco IOS® Software 12.4(22)T IOS image are used.

Hub-and-spoke and spoke-to-spoke DMVPN (mGRE) tunnels are established with IPsec protection, and DMVPN encryption is applied to the tunnel interface. Figure 1 shows the DMVPN topology.

The Enhanced IGRP (EIGRP) routing protocol is used for DMVPN. Provider equipment uses the Border Gateway Protocol (BGP) routing protocol.

Figure 1. =DMVPN Topology Diagram



Provider Edge Equipment Configuration

The configuration used in **demo-pe1** follows:

```
hostname demo-pe1
interface GigabitEthernet0/1
 description connected to demo-gm1
 ip address 10.5.110.18 255.255.255.252
!
interface GigabitEthernet0/2
 description Connected to demo-gm2
 ip address 10.5.110.21 255.255.255.252
!
interface GigabitEthernet0/3
 description Connected to demo-gm3
 ip address 10.5.110.29 255.255.255.252
!
interface FastEthernet1/0
 description Connected to demo-ks1
 ip address 10.5.110.14 255.255.255.252
!
```

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.16 mask 255.255.255.252
 network 10.5.110.20 mask 255.255.255.252
 network 10.5.110.28 mask 255.255.255.252
 neighbor 10.5.110.17 remote-as 200
 neighbor 10.5.110.22 remote-as 300
 neighbor 10.5.110.30 remote-as 400
 no auto-summary
!
```

Customer Equipment Configuration

The configuration used in **demo-gm1** follows:

```
hostname demo-gm1
ip dhcp pool demo
   network 10.5.110.200 255.255.255.248
   default-router 10.5.110.201
! DMVPN related configuration
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
crypto isakmp key cisco123 address 10.5.110.30
crypto isakmp key cisco123 address 10.5.110.22
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
!
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport require
!
crypto ipsec profile demo-dmvpn-profile
 set transform-set t1
!
interface Tunnel10
 bandwidth 2000
 ip address 64.0.0.2 255.255.255.0
 no ip redirects
 ip mtu 1400
```

```
 ip pim sparse-dense-mode
 ip nhrp map multicast 10.5.110.30
 ip nhrp map 64.0.0.1 10.5.110.30
 ip nhrp network-id 100000
 ip nhrp nhs 64.0.0.1
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 2000
 qos pre-classify
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile demo-dmvpn-profile
interface GigabitEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.17 255.255.255.252
! PC and phones connected to this port
interface FastEthernet0/1/1
 switchport access vlan 10
 spanning-tree portfast
!
interface Vlan10
 ip address 10.5.110.201 255.255.255.248
 no autostate
!
router eigrp 44
 network 10.5.110.200 0.0.0.7
 network 64.0.0.0 0.0.0.255
 no auto-summary
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.5.110.18 remote-as 100
 no auto-summary
```

```
! default route
ip route 0.0.0.0 0.0.0.0 10.5.110.18
```

The configuration used in **demo-gm2** follows:

```
hostname demo-gm2
!
ip dhcp pool demo
   network 10.5.110.208 255.255.255.248
   default-router 10.5.110.209
! DMVPN related configuration
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
crypto isakmp key cisco123 address 10.5.110.30
crypto isakmp key cisco123 address 10.5.110.17
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
!
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport require
!
crypto ipsec profile demo-dmvpn-profile
 set transform-set t1
!
interface Tunnel10
 bandwidth 2000
 ip address 64.0.0.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-dense-mode
 ip nhrp map multicast 10.5.110.30
 ip nhrp map 64.0.0.1 10.5.110.30
 ip nhrp network-id 100000
 ip nhrp nhs 64.0.0.1
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
```

```
 delay 2000
 qos pre-classify
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile demo-dmvpn-profile
!
interface GigabitEthernet0/0
 description connected to demo-pe1
! PC and phones connected to this port
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
interface Vlan10
 ip address 10.5.110.209 255.255.255.248
 no autostate
!
router eigrp 44
 network 10.5.110.208 0.0.0.7
 network 64.0.0.0 0.0.0.255
 no auto-summary
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.5.110.21 remote-as 100
 no auto-summary
!
! default route
ip route 0.0.0.0 0.0.0.0 10.5.110.21
```

The configuration used in **demo-gm3** follows:

```
hostname demo-gm3
!
ip dhcp pool demo
   network 10.5.110.216 255.255.255.248
```

```
   default-router 10.5.110.217
! DMVPN related configuration
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
crypto isakmp key cisco123 address 10.5.110.17
crypto isakmp key cisco123 address 10.5.110.22
!
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport require
!
crypto ipsec profile demo-dmvpn-profile
 set transform-set t1
!
interface Tunnel5
 bandwidth 2000
 ip address 64.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 44
 delay 2000
 qos pre-classify
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile demo-dmvpn-profile
!
interface FastEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.30 255.255.255.252
! PC and phone connected to this port
```

```
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
interface Vlan10
 ip address 10.5.110.217 255.255.255.248
 no autostate
!
router eigrp 44
 ! redistribute corporate network
 redistribute static
 network 10.5.110.216 0.0.0.7
 network 64.0.0.0 0.0.0.255
 no auto-summary
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.5.110.29 remote-as 100
 no auto-summary
```

DMVPN Encryption Verification

DMVPN operation is verified using the following commands from the headquarters router demo-gm3:

```
demo-gm3#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel5, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1     10.5.110.17        64.0.0.2    UP 00:06:57     D
     1     10.5.110.22        64.0.0.3    UP    1d00h     D
```

EIGRP routes to private networks are verified in headquarters and branch offices as follows:

```
demo-gm3#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
D       10.5.110.200/29 [90/1794560] via 64.0.0.2, 00:05:52, Tunnel5
D       10.5.110.208/29 [90/1794560] via 64.0.0.3, 00:06:32, Tunnel5
```

DMVPN encryption from headquarters to branch-office 1 is verified as follows:

```
demo-gm3#show crypto ipsec sa | incl ecaps
    #pkts decaps: 415, #pkts decrypt: 415, #pkts verify: 415
```

The PC connected to the private network in branch-office 1 is pinged:

```
demo-gm3#ping 10.5.110.204 source vlan 10 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.5.110.204, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.217
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/8 ms
demo-gm3#show crypto ipsec sa | incl ecaps
    #pkts decaps: 515, #pkts decrypt: 515, #pkts verify: 515
```

DMVPN operation in the branch-office 1 router is verified for demo-gm1 as follows:

```
demo-gm1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1     10.5.110.30        64.0.0.1    UP 02:15:28     S
     1     10.5.110.22        64.0.0.3    UP 00:00:06     D
```

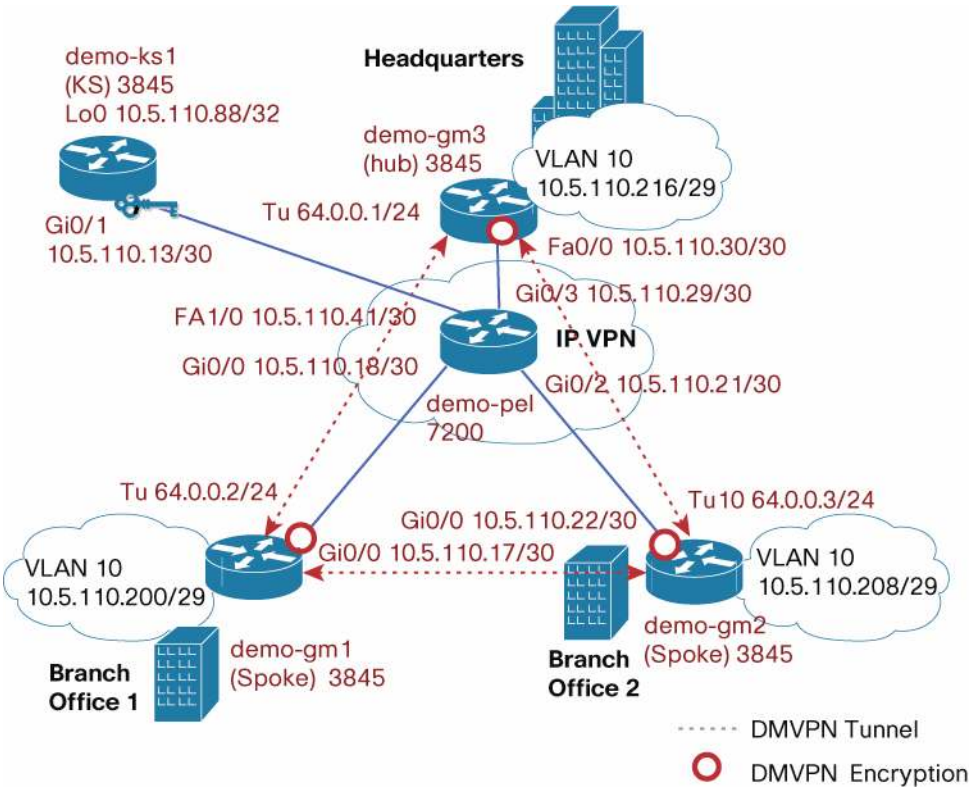
The route to the private network at the headquarters (demo-gm3) router is checked as follows:

```
demo-gm1#show ip route 10.5.110.217
Routing entry for 10.5.110.216/29
  Known via "eigrp 44", distance 90, metric 1794560, type internal
  Redistributing via eigrp 44
  Last update from 64.0.0.1 on Tunnel10, 00:16:48 ago
  Routing Descriptor Blocks:
  * 64.0.0.1, from 64.0.0.1, 00:16:48 ago, via Tunnel10
```

Step 2: Key Server Introduced to IP VPN

Add a Group Encrypted Transport VPN key server (KS) to the IP VPN network as shown in the network topology diagram in Figure 2.

Figure 2. Adding Key Server to IP VPN



Provider Edge Equipment Configuration

The configuration is added in demo-pe1 as follows:

```
interface FastEthernet1/0
 description Connected to demo-ks1
 ip address 10.5.110.14 255.255.255.252
!
router bgp 100
 network 10.5.110.12 mask 255.255.255.252
```

```
 neighbor 10.5.110.13 remote-as 800
!
```

The key system configuration follows:

The configuration added in **demo-ks1** follows:

```
hostname demo-ks1
! IKE Policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
! Preshared keys
crypto isakmp key dGvPnPsK address 10.5.110.17
crypto isakmp key dGvPnPsK address 10.5.110.22
crypto isakmp key dGvPnPsK address 10.5.110.30
crypto isakmp keepalive 15 periodic
!   Crypto GDOI attributes
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900        ! TEK lifetime
 set transform-set aes128
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756                           ! group id
 server local                                         ! Key server
  rekey algorithm aes 128                             ! rekey algorithm
  rekey lifetime seconds 28800                        ! KEK lifetime
  rekey authentication mypubkey rsa rekeyrsa          ! rekey Authentication
  rekey transport unicast                             ! unicast rekey method
  sa ipsec 1                                          ! security association
   profile getvpn-profile                             ! Crypto attribute selection
   match address ipv4 sa-acl                          ! Encryption Policy
   replay time window-size 5                          ! Replay time window size
  address ipv4 10.5.110.88                            ! KS address
! KS address used for sending rekeys
interface Loopback0
 ip address 10.5.110.88 255.255.255.255
!
interface GigabitEthernet0/1
```

```
 description Connected to demo-pe1
 ip address 10.5.110.13 255.255.255.252
!
router bgp 800
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.12 mask 255.255.255.252
 network 10.5.110.88 mask 255.255.255.255
 neighbor 10.5.110.14 remote-as 100
 no auto-summary
! GDOI Encryption policy
ip access-list extended sa-acl
 deny   udp any eq 848 any eq 848     ! GDOI in clear
 deny   tcp any any eq ssh            ! Secure Shell control traffic in clear
 deny   tcp any eq ssh any            ! Secure Shell control traffic in clear
 deny   esp any any                   ! Exclude ESP traffic (GRE+IPSec)
 deny   tcp any eq bgp any            ! Exclude BGP
 deny   tcp any any eq bgp            ! Exclude BGP
 deny   udp any eq isakmp any eq isakmp ! Exclude IKE control traffic
 deny   eigrp any any                   ! Exclude EIGRP control traffic
 deny   igmp any any                    ! Exclude IGMP
 deny   pim any 224.0.0.13              ! Exclude PIM control
 deny   ip any 224.0.0.0 0.0.255.255    ! Exclude link-layer control protocols
 deny   udp any any eq ntp              ! Exclude NTP
 deny   udp any any eq snmp             ! Exclude SNMP
 deny   udp any any eq syslog           ! Exclude syslog
 permit ip any any                      ! Encrypt everything else
!
```

Key System Operation Verification

The operation of the key system is verified using the following command-line interface (CLI) command:

```
demo-ks1#show crypto gdoi
GROUP INFORMATION
    Group Name               : GETVPN-DEMO (Unicast)
    Group Identity           : 1357924756
    Group Members            : 9
    IPSec SA Direction       : Both
    Active Group Server      : Local
```

```
Redundancy               : Configured
    Local Address        : 10.5.110.88
    Local Priority       : 20
    Local KS Status      : Alive
Group Rekey Lifetime     : 28800 secs
Group Rekey
    Remaining Lifetime   : 24224 secs
Rekey Retransmit Period  : 10 secs
Rekey Retransmit Attempts: 2
Group Retransmit
    Remaining Lifetime   : 0 secs
  IPSec SA Number        : 1
  IPSec SA Rekey Lifetime: 900 secs
  Profile Name           : getvpn-profile
  Replay method          : Time Based
  Replay Window Size     : 5
  SA Rekey
     Remaining Lifetime  : 275 secs
  ACL Configured         : access-list sa-acl
Group Server list        : Local
```

Step 3: Routing Metrics Modified on Tunnel Interfaces

Multiprotocol Label Switching (MPLS) service providers typically use the BGP routing protocol. We need to advertise routes in customer equipment to the provider VPN with the BGP routing protocol to make Group Encrypted Transport VPN group members (GMs) work effectively. When private network routes in headquarters and branch offices are advertised through BGP, BGP routes take precedence over EIGRP because the BGP administrative distance is lower (20 compared to the administrative distance of EIGRP, which is 90). This process disrupts existing DMVPN traffic between branch offices and headquarters. EIGRP routing metrics are modified on tunnel interfaces to keep existing DMVPN traffic flowing through the GRE tunnels while provisioning Group Encrypted Transport VPN group members by adding the following configuration in demo-gm1, demo-gm2 and demo-gm3:

```
router eigrp 44
distance eigrp 15 15
```

This configuration change sets the administrative distance of both EIGRP internal routes and externally distributed EIGRP routes to 15 in the local routing table. It sets the administrative distance of the EIGRP route lower than that for the BGP routes.

Verifying the Routing Metrics Modified on Tunnel Interfaces

The administrative distance of EIGRP routes for the private network set to 15 (instead of default value 90) is verified by executing the following CLI in demo-gm3:

```
demo-gm3#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
D       10.5.110.200/29 [15/1794560] via 64.0.0.2, 00:08:41, Tunnel5
D       10.5.110.208/29 [15/1794560] via 64.0.0.3, 00:08:42, Tunnel5
```

Step 4: Routed Path Modified to Include Group Encrypted Transport-Enabled Core

Next we need to advertise routes of physical interfaces connected to the provider edge, and routes of the private network used in headquarters and branch-office customer edge routers using the BGP routing protocol as follows:

The following configuration is added in demo-gm1:

```
router bgp 200
 network 10.5.110.16 mask 255.255.255.252
!
```

The following configuration is added in demo-gm2:

```
router bgp 300
  network 10.5.110.20 mask 255.255.255.252
!
```

The following configuration is added in demo-gm3:

```
router bgp 400
 network 10.5.110.28 mask 255.255.255.252
!
```

Verifying BGP Routing Table Includes Group Encrypted Transport VPN-Enabled Core Routes

The BGP routes in the headquarters router are checked as follows:

```
demo-gm3#show ip route bgp
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B       10.5.110.88/32 [20/0] via 10.5.110.29, 04:40:50
B       10.5.110.12/30 [20/0] via 10.5.110.29, 04:40:50
B       10.5.110.16/30 [20/0] via 10.5.110.29, 04:40:50
B       10.5.110.20/30 [20/0] via 10.5.110.29, 04:40:50
```

However, EIGRP routes are preferred from the headquarters router (demo-gm3) to reach the private network in branch offices:

```
demo-gm3#show ip route 10.5.110.204
Routing entry for 10.5.110.200/29
  Known via "eigrp 44", distance 15, metric 1794560, type internal
```

```
  Redistributing via eigrp 44
  Last update from 64.0.0.2 on Tunnel5, 00:03:12 ago
  Routing Descriptor Blocks:
  * 64.0.0.2, from 64.0.0.2, 00:03:12 ago, via Tunnel5
      Route metric is 1794560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 2/255, Hops 1


demo-gm3#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
D       10.5.110.200/29 [15/1794560] via 64.0.0.2, 00:03:26, Tunnel5
D       10.5.110.208/29 [15/1794560] via 64.0.0.3, 00:03:26, Tunnel5
```

Step 5: Symmetric Routing Between Branch Offices Enabled and Headquarters Transitioned to Group Encrypted Transport VPN

We have already added security-assurance [[correct? If not, pls tell what SA stands for; avoid two-letter acronyms]] policy in the key system so that the GDOI cryptography map excludes ESP traffic (that is, GRE + IPsec). This step is done so that traffic is not encrypted twice (once by DMVPN and second time by GRE). In this step traffic flows through DMVPN tunnels until the individual sites are transitioned to Group Encrypted Transport VPN. After the transition, traffic is routed outside of the DMVPN tunnel and encrypted by Group Encrypted Transport VPN. The following configuration needs to be added at the headquarters and branch-office customer edges to make them part of the Group Encrypted Transport VPN group.

Provision Group Encrypted Transport VPN in Headquarters (demo-gm3)

Group Encrypted Transport VPN group encryption is enabled by adding the following configuration in demo-gm3. After adding the configuration and applying the cryptography map, demo-gm3 becomes a group member of Group Encrypted Transport VPN-DEMO group encryption.

```
! IKE configuration needed for GETVPN
crypto isakmp policy 1
 encr 3des
 authentication pre-share         ! Preshared key is used in this example
 group 2
!
crypto isakmp key dGvPnPsK address 10.5.110.88    ! Preshared key
!
crypto gdoi group GETVPN-DEMO     ! Group encryption
 identity number 1357924756       ! Group identity for member
 server address ipv4 10.5.110.88  ! KS address to register
!
crypto map demo-gdoi 1 gdoi       ! Group Crypto map entry
```

```
 set group GETVPN-DEMO            ! Group membership
```

The following configuration is added in demo-gm3 to add a local private network to BGP:

```
router bgp 400
network 10.5.110.216 mask 255.255.255.248
```

The following configuration is added in demo-gm3 (DMVPN hub) to enable symmetric routing between branch offices during Group Encrypted Transport VPN transition. Branch offices are transitioned to use Group Encrypted Transport VPN encryption one at a time.

```
! It is possible some of the branches use DMVPN and EIGRP (non-converted sites) while
! other branches have transitioned to GETVPN (converted sites). To make symmetric
! routing between branches work, we need to redistribute non converted sites EIGRP
! routes learned by the hub into BGP routes.
! Basically this injects EIGRP routes of non-converted sites to BGP
! Makes traffic from converted sites to non-converted sites flow to hub using
! GET VPN and then via DMVPN from hub to non-converted site
!
  redistribute eigrp 44
! Redistribute converted site BGP routes into EIGRP. This provide symmetric route.
! Makes traffic from non-converted sites to converted sites flow via hub using DMVPN
! tunnel and then from hub to converted site via GET VPN on WAN
router eigrp 44
  redistribute bgp 400 metric 1500 100 255 1 1500
```

First apply a GDOI cryptography map in the headquarters router by applying Group Encrypted Transport VPN group encryption to the WAN interface as follows:

demo-gm3(config)#int Fa0/0

```
demo-gm3(config-if)#crypto map demo-gdoi
*Jun 11 22:33:28.044: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88 for
group GETVPN-DEMO using address 10.5.110.30
*Jun 11 22:33:28.056: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
*Jun 11 22:33:28.176: %GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN-DEMO transitioned to
Unicast Rekey.
*Jun 11 22:33:28.200: %GDOI-5-GM_REGS_COMPL: Registration to KS 10.5.110.88 complete
for group GETVPN-DEMO using address 10.5.110.30
```

Verify Traffic Between Individual Sites Gets Encrypted by DMVPN

After adding GDOI encryption, traffic between sites flows through DMVPN tunnels. The following is done in the headquarters group member (demo-gm3) to verify it.

Verify that the route to the PC is connected to the private network in branch-office 1 from demo-gm3:

```
demo-gm3#show ip route 10.5.110.204
Routing entry for 10.5.110.200/29
  Known via "eigrp 44", distance 15, metric 1794560, type internal
  Redistributing via eigrp 44
  Last update from 64.0.0.2 on Tunnel5, 02:43:47 ago
  Routing Descriptor Blocks:
  * 64.0.0.2, from 64.0.0.2, 02:43:47 ago, via Tunnel5
      Route metric is 1794560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1


demo-gm3#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
D       10.5.110.200/29 [15/1794560] via 64.0.0.2, 02:43:50, Tunnel5
D       10.5.110.208/29 [15/1794560] via 64.0.0.3, 02:43:52, Tunnel5
```

Ping the PC connected to the private network in branch-office 1 from demo-gm3:

```
demo-gm3#ping 10.5.110.204 source vlan 10 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.5.110.204, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.217
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/8 ms
```

Step 6: Individual Sites Transitioned to Group Encrypted Transport VPN One at a Time

Each branch office is transitioned to use Group Encrypted Transport VPN encryption from DMVPN encryption as follows:

Note: Monitor traffic loss during individual branch-office transition to Group Encrypted Transport VPN by executing the following command in the headquarters group member (demo-gm3). Ping the PC connected to the private network in branch-office 1:

```
demo-gm3#ping 10.5.110.204 source vlan 10 rep 10000
*Jun 11 23:19:20.807: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO from
10.5.110.88 to 10.5.110.30 with seq # 33
```

```
Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 10.5.110.204, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.217
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output excluded>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (9993/10000), round-trip min/avg/max = 1/1/48 ms
*Jun 11 23:21:12.251: %PIM-5-NBRCHG: neighbor 64.0.0.2 DOWN on interface Tunnel5 non
DR
```

Seven packets are lost during route convergence from the EIGRP route to the BGP route.

Transition Branch-Office 1 Group Member (demo-gm1) to Use Group Encrypted Transport VPN Encryption

Transition one branch office at a time by doing the following five steps in the group member:

- Add a Group Encrypted Transport VPN cryptography configuration on the branch-office router to be converted.
- Add a local private network to BGP.
- Apply the cryptography map on the physical interface connecting toward the provider edge.
- Shut the DMVPN tunnel to transition branch-office traffic to use Group Encrypted Transport VPN encryption.
- Verify a symmetric route between branch offices.
- Verify Group Encrypted Transport VPN functions.

Add Group Encrypted Transport VPN Configuration in Branch-Office 1 (demo-gm1)

Group Encrypted Transport VPN group encryption is enabled by adding the following configuration in demo-gm1. After adding the configuration and applying the cryptography map, demo-gm1 becomes a group member of Group Encrypted Transport VPN-DEMO group encryption.

```
! IKE configuration needed for GETVPN
crypto isakmp policy 1
 encr 3des
 authentication pre-share         ! Preshared key is used in this example
 group 2
!
crypto isakmp key dGvPnPsK address 10.5.110.88 ! Preshared key
!
crypto gdoi group GETVPN-DEMO     ! Group encryption
 identity number 1357924756       ! Group identity for member
 server address ipv4 10.5.110.88  ! KS address to register
!
crypto map demo-gdoi 1 gdoi       ! Group Crypto map entry
 set group GETVPN-DEMO            ! Group membership
!
```

Add a private local network to the BGP routing table.

```
router bgp 200
 network 10.5.110.200 mask 255.255.255.248
!
```

Apply Group Encrypted Transport VPN group encryption to the WAN interface as follows:

```
demo-gm1(config)#int Gi0/0
demo-gm1(config-if)#crypto map demo-gdoi
demo-gm1(config-if)#end
*Jun 11 15:14:22 pst: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88 for group GETVPN-DEMO using address 10.5.110.17
*Jun 11 15:14:22 pst: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
*Jun 11 15:14:22 pst: %GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN-DEMO transitioned to Unicast Rekey.
*Jun 11 15:14:22 pst: %GDOI-5-GM_REGS_COMPL: Registration to KS 10.5.110.88 complete for group GETVPN-DEMO using address 10.5.110.17
```

During ping traffic flow, shut down the DMVPN tunnel in the branch-office 1 group member (demo-gm1) as follows:

```
demo-gm1(config)#int Tu 10
demo-gm1(config-if)#shut
demo-gm1(config-if)#end
*Jun 11 16:24:20 pst: %PIM-5-NBRCHG: neighbor 64.0.0.1 DOWN on interface Tunnel10 non DR
*Jun 11 16:24:20 pst: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 11 16:24:20 pst: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 44: Neighbor 64.0.0.1 (Tunnel10) is down: interface down
* *Jun 11 16:24:22 pst: %LINK-5-CHANGED: Interface Tunnel10, changed state to administratively down
*Jun 11 16:24:23 pst: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to down
```

Now EIGRP routes are removed in the demo-gm1 group member:

```
demo-gm1#show ip route eigrp
```

Verify a symmetric route between local networks of branch-office routers demo-gm1 and demo-gm2.

Traffic uses GDOI encryption between demo-gm1 and demo-gm3, and uses DMVPN IPsec encryption between demo-gm3 and demo-gm2.

Check the route from the branch-office 1 (demo-gm1) private network to the branch-office 2 (demo-gm2) private network as follows:

```
demo-gm1#show ip route 10.5.110.209
Routing entry for 10.5.110.208/29
  Known via "bgp 200", distance 20, metric 0
  Tag 100, type external
  Last update from 10.5.110.18 00:04:17 ago
  Routing Descriptor Blocks:
  * 10.5.110.18, from 10.5.110.18, 00:04:17 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 100
demo-pe1#show ip route 10.5.110.209
Routing entry for 10.5.110.208/29
  Known via "bgp 100", distance 20, metric 1794560
  Tag 400, type external
  Last update from 10.5.110.30 00:14:00 ago
  Routing Descriptor Blocks:
  * 10.5.110.30, from 10.5.110.30, 00:14:00 ago
      Route metric is 1794560, traffic share count is 1
      AS Hops 1
      Route tag 400

demo-pe1#show ip route | incl 10.5.110.208
B       10.5.110.208/29 [20/1794560] via 10.5.110.30, 00:14:15
```

The route in that configuration is redistributed from EIGRP to BGP in demo-gm3.

```
demo-gm3#show ip route 10.5.110.209
Routing entry for 10.5.110.208/29
  Known via "eigrp 44", distance 15, metric 1794560, type internal
  Redistributing via eigrp 44, bgp 400
  Advertised by bgp 400
  Last update from 64.0.0.3 on Tunnel5, 00:41:34 ago
  Routing Descriptor Blocks:
  * 64.0.0.3, from 64.0.0.3, 00:41:34 ago, via Tunnel5
      Route metric is 1794560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 2000 Kbit
```

```
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 168/255, Hops 1
```

Check the reverse route from the branch-office 2 (demo-gm2) private network to the branch-office 1 (demo-gm1) private network as follows:

Traffic uses DMVPN IPsec encryption between demo-gm2 and demo-gm3, and uses GDOI encryption between demo-gm3 and demo-gm1.

```
demo-gm2#show ip route 10.5.110.204
Routing entry for 10.5.110.200/29
  Known via "eigrp 44", distance 170, metric 2244096
  Tag 100, type external
  Redistributing via eigrp 44
  Last update from 64.0.0.1 on Tunnel10, 00:36:53 ago
  Routing Descriptor Blocks:
  * 64.0.0.1, from 64.0.0.1, 00:36:53 ago, via Tunnel10
      Route metric is 2244096, traffic share count is 1
      Total delay is 21000 microseconds, minimum bandwidth is 1500 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1
      Route tag 100

demo-gm2#show ip route | incl 200
D EX    10.5.110.200/29 [170/2244096] via 64.0.0.1, 00:37:09, Tunnel10
```

The display output of that configuration shows that the Group Encrypted Transport VPN converted site private network route is redistributed from the BGP to the EIGRP table, making traffic from nonconverted site demo-gm2 to converted site demo-gm1 flow through the headquarters router (demo-gm3) using the DMVPN tunnel.

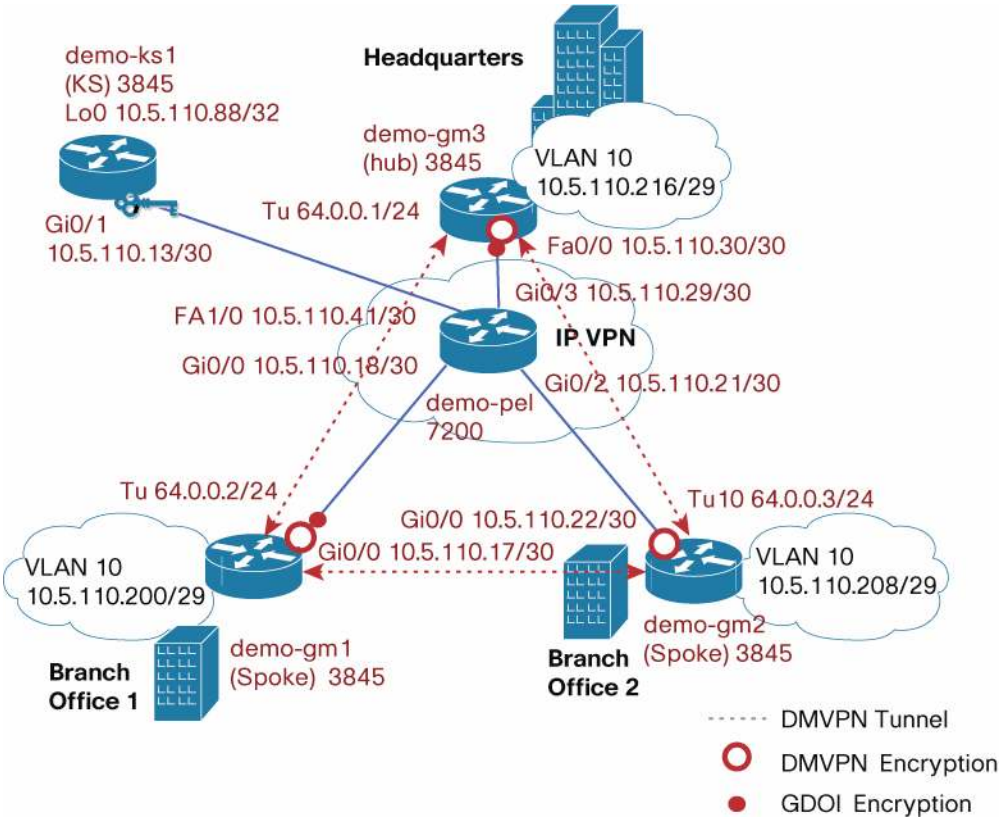
```
demo-gm3#show ip route 10.5.110.204
Routing entry for 10.5.110.200/29
  Known via "bgp 400", distance 20, metric 0
  Tag 100, type external
  Redistributing via nhrp
  Last update from 10.5.110.29 00:29:45 ago
  Routing Descriptor Blocks:
  * 10.5.110.29, from 10.5.110.29, 00:29:45 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 100
```

```
demo-pe1#show ip route 10.5.110.204
Routing entry for 10.5.110.200/29
  Known via "bgp 100", distance 20, metric 0
  Tag 200, type external
  Last update from 10.5.110.17 01:22:50 ago
  Routing Descriptor Blocks:
  * 10.5.110.17, from 10.5.110.17, 01:22:50 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 200
```

Topology After Enabling Group Encrypted Transport VPN Incryption in Branch-Office 1

Figure 3 shows the topology after adding Group Encrypted Transport VPN encryption in individual sites. At this point, traffic between private networks between branch offices gets encrypted by DMVPN.

Figure 3. Topology After Adding Group Encrypted Transport VPN Encryption at Headquarters and Branch-Office 1



Verify that the route from branch-office 1 to the headquarters private network uses an MPLS path:

```
demo-gm1#show ip route 10.5.110.217
Routing entry for 10.5.110.216/29
  Known via "bgp 200", distance 20, metric 0
```

```
  Tag 100, type external
  Last update from 10.5.110.18 00:13:19 ago
  Routing Descriptor Blocks:
  * 10.5.110.18, from 10.5.110.18, 00:13:19 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 100
```

Now Group Encrypted Transport-enabled interfaces are confirmed operational using following CLI commands:

To check whether the group member is participating in Group Encrypted Transport VPN encryption, execute the following CLI command:

```
demo-gm1#show crypto gdoi
GROUP INFORMATION
    Group Name               : GETVPN-DEMO
    Group Identity           : 1357924756
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 10.5.110.88
    Group Server list        : 10.5.110.88
    GM Reregisters in        : 217 secs
    Rekey Received(hh:mm:ss) : 00:23:28
    Rekeys received
         Cumulative          : 0
         After registration  : 0
    Rekey Acks sent          : 0
 ACL Downloaded From KS 10.5.110.88:
   access-list  deny udp any port = 848 any port = 848
   access-list  deny tcp any any port = 23
   access-list  deny tcp any port = 23 any
   access-list  deny esp any any
   access-list  deny tcp any port = 179 any
   access-list  deny tcp any any port = 179
   access-list  deny udp any port = 500 any port = 500
   access-list  deny ospf any any
   access-list  deny eigrp any any
   access-list  deny igmp any any
   access-list  deny pim any any
```

```
   access-list  deny ip any 224.0.0.0 0.0.255.255
   access-list  deny udp any any port = 123
   access-list  deny udp any any port = 161
   access-list  deny udp any any port = 514
   access-list  permit ip any any
KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 5398
    Encrypt Algorithm        : AES
    Key Size                 : 128
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024
TEK POLICY:
  GigabitEthernet0/0:
    IPsec SA:
        sa direction:inbound
        spi: 0x9BA7DF6(163216886)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (98)
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:outbound
        spi: 0x9BA7DF6(163216886)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (97)
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:inbound
        spi: 0x156DAB5C(359508828)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (880)
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:outbound
        spi: 0x156DAB5C(359508828)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (857)
```

```
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:inbound
        spi: 0x9BA7DF6(163216886)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (73)
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:outbound
        spi: 0x9BA7DF6(163216886)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (73)
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:inbound
        spi: 0x156DAB5C(359508828)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (857)
        Anti-Replay(Time Based) : 5 sec interval
    IPsec SA:
        sa direction:outbound
        spi: 0x156DAB5C(359508828)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (827)
        Anti-Replay(Time Based) : 5 sec interval
```

Verify the Internet Key Exchange (IKE) connection between the group member and the key system to receive rekeys:

```
demo-gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.5.110.17     10.5.110.88     GDOI_REKEY        1566 ACTIVE
10.5.110.88     10.5.110.17     GDOI_IDLE         1565 ACTIVE
```

Verify whether traffic is encrypted by Group Encrypted Transport VPN by using the following CLIs:

```
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 297, #pkts encrypt: 297, #pkts digest: 297
```

Ping the headquarters private network address from branch-office 1 as follows:

```
demo-gm1#ping 10.5.110.217 source vlan 10 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.5.110.217, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms

demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 397, #pkts encrypt: 397, #pkts digest: 397
```

The previous output shows that the Internet Control Message Protocol (ICMP) traffic between branch-office 1 and headquarters is encrypted.

Verify reachability between private networks in demo-gm1 and dem-gm2 as follows:

```
demo-gm1#ping 10.5.110.209 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.209, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Transition Next Branch-Office (branch-office 2) Group Member (demo-gm2) to Use Group Encrypted Transport VPN Encryption

Follow the same process described in the previous section for transitioning the demo-gm2 group member to use Group Encrypted Transport VPN encryption.

The following configuration is added in **demo-gm2**:

Add Group Encrypted Transport VPN Configuration in Branch-Office 2 (demo-gm2)

Group Encrypted Transport VPN group encryption is enabled by adding the following configuration in demo-gm2. After adding configuration and applying the cryptography map, demo-gm2 becomes a group member of Group Encrypted Transport VPN-DEMO group encryption.

```
! IKE configuration needed for GETVPN
crypto isakmp policy 1
 encr 3des
 authentication pre-share        ! Preshared key is used in this example
 group 2
!
```

```
crypto isakmp key dGvPnPsK address 10.5.110.88    ! Preshared key
!
crypto gdoi group GETVPN-DEMO     ! Group encryption
 identity number 1357924756       ! Group identity for member
 server address ipv4 10.5.110.88  ! KS address to register
!
crypto map demo-gdoi 1 gdoi       ! Group Crypto map entry
 set group GETVPN-DEMO            ! Group membership
```

Add a private local network to the BGP routing table:

```
router bgp 300
  network 10.5.110.208 mask 255.255.255.248
```

Apply Group Encrypted Transport VPN group encryption to the WAN interface as follows:

```
demo-gm2(config)#int Gi0/0
demo-gm2(config-if)#crypto map demo-gdoi
demo-gm2(config-if)#end
*Jun 11 15:29:03: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88 for group
GETVPN-DEMO using address 10.5.110.22
*Jun 11 15:29:03: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
*Jun 11 15:29:03: %GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN-DEMO transitioned to
Unicast Rekey.
*Jun 11 15:29:03: %GDOI-5-GM_REGS_COMPL: Registration to KS 10.5.110.88 complete for
group GETVPN-DEMO using address 10.5.110.22
```

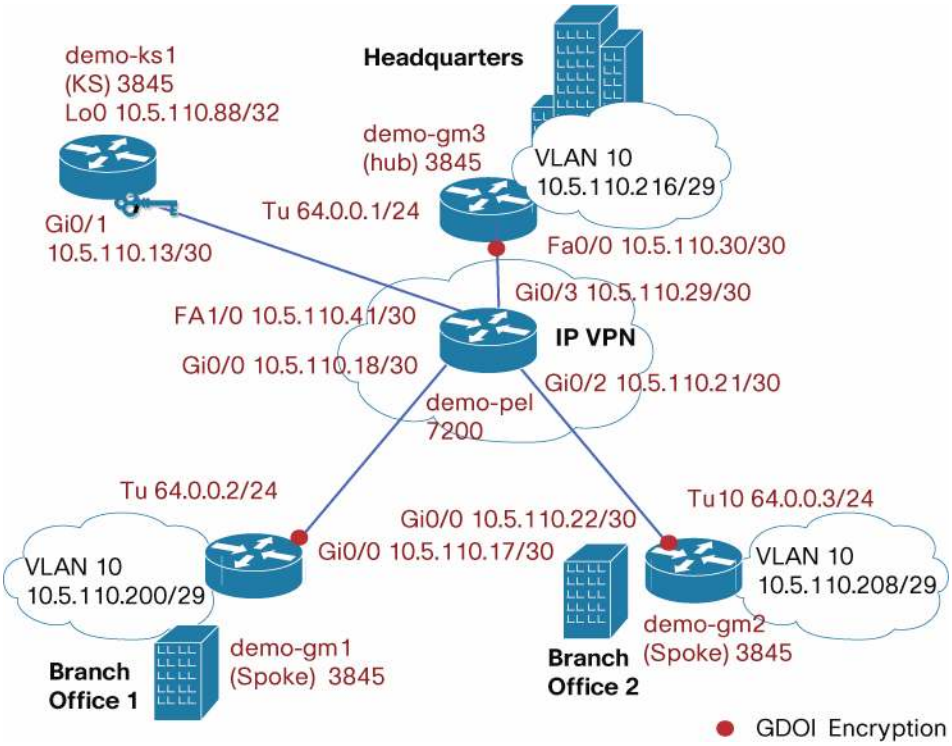
Shut down the DMVPN tunnel in the branch-office 2 group member (demo-gm2) as follows:

```
demo-gm2(config)#int Tu 10
demo-gm2(config-if)#shut
demo-gm2(config-if)#end
Shut down the DMVPN tunnel in demo-gm3 as follows:
demo-gm3(config)#int Tu 5
demo-gm3(config-if)#shut
demo-gm3(config-if)#exit
```

Topology After Individual Sites Transitioned to Group Encrypted Transport VPN

Figure 4 shows the topology after individual sites are transitioned to use Group Encrypted Transport VPN encryption and DMVPN tunnels are shut down.

Figure 4. Topology After Individual Sites Are Transitioned to Use Group Encrypted Transport VPN Encryption



Transition Each Subsequent Branch-Office Group Member to Use Group Encrypted Transport VPN Encryption

Follow the same process described in the previous section for transitioning each group member to use Group Encrypted Transport VPN encryption. During the transition process, three general traffic patterns may be observed:

1. Between converted site and converted site: This traffic should flow directly between the group member through the Group Encrypted Transport VPN-encrypted WAN infrastructure.
2. Between converted site and nonconverted site: This traffic should flow through the DMVPN hub. Traffic between the converted site and hub is encrypted using Group Encrypted Transport VPN on the WAN, whereas traffic between the hub and the nonconverted site is encrypted and tunneled through DMVPN.
3. Between nonconverted site and nonconverted site: This traffic should flow through the usual DMVPN processes, where initial connections flow through the hub and subsequently communications may flow directly between the branch offices if DMVPN spoke-to-spoke tunnels are built.

Although the transition process does induce nonoptimal routing, the forward and reverse paths should be symmetric.

Step 7: Clean Up DMVPN Configuration from Branch Offices and Headquarters Group Members

Clean up DMVPN configuration from the branch-office 1 group member (demo-gm1) as follows:

```
demo-gm1(config)#no router eigrp 44
demo-gm1(config)#no ip route 0.0.0.0 0.0.0.0 10.5.110.18
demo-gm1(config)#no interface Tunnel10
```

Clean up DMVPN configuration from the branch-office 1 group member (demo-gm2) as follows:

```
demo-gm2(config)#no router eigrp 44
demo-gm2(config)#no ip route 0.0.0.0 0.0.0.0 10.5.110.21
demo-gm2(config)#no interface Tunnel10
```

Clean up DMVPN configuration from the headquarters group members (demo-gm3) as follows:

```
demo-gm3(config)#no router eigrp 44
demo-gm3(config)#router bgp 400
demo-gm3(config-router)#no redistribute eigrp 44
demo-gm3(config)#no interface Tunnel5
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-598811-00 04/10