Migration Guide

Next Generation Enterprise WAN

DMVPN-to-GET VPN Migration Guide

October, 2011

NOTICE: ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

screen font	Terminal sessions and information in the displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Nonprinting characters, such as passwords, are in angle brackets.
< >	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note: Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Cautions indicate that in this situation, you might do something that could result in equipment damage or loss of data.

Warning: Warnings indicate a potential situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.

Introduction

Many customers have been taking advantage of Dynamic Multipoint VPN (DMVPN) solutions for encrypting data traffic over public IP networks. Although DMVPN is a fairly robust solution, it does have some challenges when implemented in newer emerging architectures that support peer-to-peer and other more recent application types. Group Encrypted Transport (GET) VPN has been developed to provide the any-to-any communication and robust IP Multicast. This document provides the steps for DMVPN-to-GET VPN migration.

The Cisco IOS® Software-based GET VPN (Cisco IOS GET VPN) is a tunnel-less technology that provides end-to-end security for voice, video, and data in a native mode for a fully meshed network. It uses the ability of the core network to route and replicate the packets between various sites within the enterprise. Cisco IOS GET VPN preserves the original source and destination addresses in the encryption header for optimal routing; hence, it is largely suited for an enterprise running over a private Multiprotocol Label Switching (MPLS)/IP-based core network. Cisco IOS GET VPN uses Group Domain of Interpretation (GDOI) as the keying protocol for encrypting and decrypting the data packets.

Why GET VPN?

Enterprise customers face numerous security challenges based on their network application and connectivity requirements. Though MPLS VPNs can provide a certain level of security, many critical applications need end-to-end encryption as well. Some solutions involving DMVPN can be used to achieve end-to-end encryption, but these solutions basically follow an overlay “hub-and-spoke” model. This practice could introduce sub-optimal routing even for a fully meshed deployed network using MPLS, could delay setting up a full mesh of connections among all sites, and could result in sub-optimal support for multicast, thereby causing scaling limitations and provisioning and troubleshooting overheads.

Cisco IOS GET VPN is a group key-based solution that provides end-to-end security for both unicast and multicast applications. It is enabled in customer edge routers without using tunnels.

The GDOI protocol, documented in RFC 3547, is the foundation for Cisco IOS GET VPN. For detailed information about Cisco IOS GET VPN architecture and features, please visit http://www.cisco.com/go/getvpn.

Cisco IOS GET VPN Benefits

- Offers a tunnel-less encryption solution
- Uses the underlying routing infrastructure
- Provides for centralized management of policies and keys in the key server
- Offers end-to-end security for voice, video, and data
- Provides any-to-any enterprise connectivity for critical applications
- Offers optimal routing by preserving source and destination addresses in the encryption header
- Offers flexibility to use unicast or multicast rekey mechanisms based on the core network support
- Provides multicast encryption in native mode
- Uses (requires) multicast replication in the MPLS/IP core, removing the need for a group member to replicate multiple copies for each receiver (such as a hub in a hub-and-spoke tunneled network)
- Requires less overhead in provider edge (PE) routers because they do not need to decrypt and encrypt traffic
- Provides efficient distribution of rekeys using multicast transport

- Offers zero-touch provisioning in key server for addition of new group members if planned addressing schemes are in place
- Offers redundancy in key-server failure by using cooperative key-server feature
- Prevents replay attacks
- Selectively bypasses encryption using group-member access control list (ACL)
- Offers a scalable security solution for large-scale networks

DMVPN-to-GET VPN Migration

Following are the steps involved in migrating from DMVPN to GET VPN:

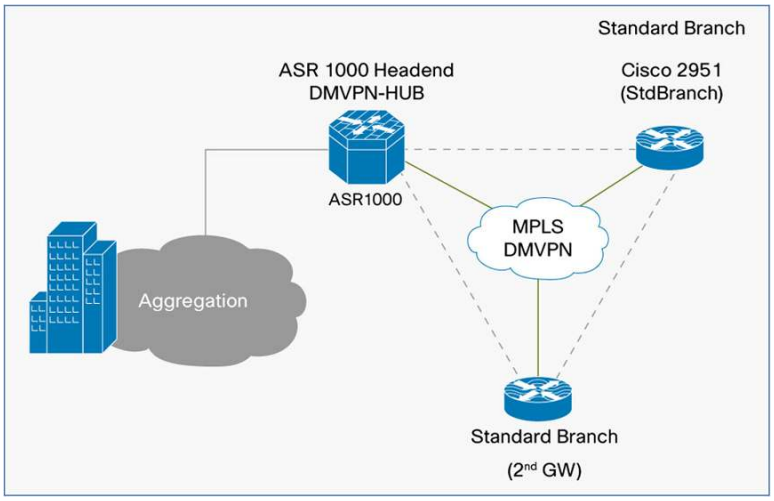
1. Establish hub-and-spoke and spoke-to-spoke DMVPN (multipoint generic routing encapsulation [mGRE]) tunnels with IP Security (IPsec) protection. Apply tunnel protection to the tunnel interface.
2. Introduce key server to IP VPN.
3. Modify routing metrics on tunnel interfaces.
4. Modify routed path to include Group Encrypted Transport-enabled core.
5. Enable symmetric routing between branch offices in the hub. Transition headquarters to use GET VPN encryption first. Exclude Encapsulating Security Payloads (ESP) traffic (that is, GRE + IPsec) on the GDOI crypto map so that traffic is not encrypted twice (once by DMVPN and the second time by GRE).
6. Transition individual sites to GET VPN one at a time. Confirm that Group Encrypted Transport-enabled interfaces are operational. **Note:** Symmetric routing between branch offices is required during transition for network stability.
7. Remove DMVPN from branch offices and headquarters. Remove tunnel interfaces on a per-peer basis. Remove GRE and IPsec peers and remove modified routing metrics.

These steps are described in detail in the following sections.

Step 1. Protect Traffic Between Branch Offices and Headquarters

Deploy DMVPN IPsec encryption between branch offices and headquarters (Figure 1).

Figure 1. DMVPN Topology Diagram



The solution test setup consists of two DMVPN spoke routers, a Cisco 2951 Integrated Services Router (**StdBranch**) and **2nd GW**, located in branch offices, and one DMVPN hub router, a third gateway (**ASR**), located in the headquarters. Branch-office routers are Cisco 3945 Integrated Services Routers running Cisco IOS Software Release 15.1(4)M.

Establish hub-and-spoke and spoke-to-spoke DMVPN (mGRE) tunnels with IPsec protection. Apply DMVPN encryption to the tunnel interface.

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

The MPLS cloud interconnects the headend to the branch-office sites. The customer edge (CE) routers on each site and the headend customer edge router all act as group members (GMs). All these routers are grouped into a GDOI group. Therefore, all key servers (KSs) and group members are part of the same VPN. A Cisco Integrated Services Routers Generation 2 (ISR G2) router acts as a key server. The key server is configured with group policies that are pushed to all group members.

Customer Edge Equipment Configuration

The relevant configuration used in the **StdBranch** branch-office router follows:

```
hostname StdBranch
ip dhcp pool stdbrnch
   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 MPLS
 ip address 10.5.110.17 255.255.255.252

! PC and phones connected to this port

interface GigabitEthernet0/2.1
 description Vlan-Data
 encapsulation dot1Q 31
 ip address 10.6.10.1 255.255.255.0

interface GigabitEthernet0/2.2
 description Vlan-Voice
 encapsulation dot1Q 32
 ip address 10.6.11.1 255.255.255.0

router eigrp 44
 network 10.5.110.200 0.0.0.7
 network 10.6.0.0 0.0.255.255
 network 64.0.0.0 0.0.0.255
 no auto-summary

ip route 0.0.0.0 0.0.0.0 10.5.110.18
```

The relevant configuration used in the **2nd GW** router follows:

```
hostname 2nd GW
!
ip dhcp pool StdBranch
   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 MPLS
 ip address 10.5.110.22 255.255.255.252

! PC and phones connected to this port

interface GigabitEthernet0/2.1
 description Vlan-Data
 encapsulation dot1Q 41
 ip address 10.8.10.1 255.255.255.0

interface GigabitEthernet0/2.2
 description Vlan-Voice
 encapsulation dot1Q 42
 ip address 10.8.11.1 255.255.255.0

router eigrp 44
 network 10.5.110.208 0.0.0.7
 network 10.8.0.0 0.0.255.255
 network 64.0.0.0 0.0.0.255
 no auto-summary

ip route 0.0.0.0 0.0.0.0 10.5.110.21
```

The relevant configuration used in the **ASR** router follows:

```
hostname ASR
!
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 GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile demo-dmvpn-profile
!
interface GigabitEthernet0/0
 description Connected to MPLS
 ip address 10.5.110.30 255.255.255.252

! PC and phone connected to this port

interface GigabitEthernet0/2.1
 description Vlan-Data
 encapsulation dot1Q 51
 ip address 10.7.10.1 255.255.255.0

interface GigabitEthernet0/2.2
 description Vlan-Voice
 encapsulation dot1Q 52
 ip address 10.7.11.1 255.255.255.0
!
router eigrp 44
 ! redistribute corporate network
 redistribute static
 network 10.5.110.216 0.0.0.7
 network 10.7.0.0 0.0.255.255
 network 64.0.0.0 0.0.0.255
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.5.110.31
```

Verify DMVPN operation using the following commands from the headquarters **ASR** router:

```
ASR#show dmvpn

======================================================================

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

Verify eigrp routes to private networks in Headquarters and branches as follows:

ASR#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
```

Verify DMVPN encryption from headquarters to the **StdBranch** gateway as follows:

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

Ping PC connected to private network in Branch1:

ASR#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

ASR#show crypto ipsec sa | incl ecaps
    #pkts decaps: 515, #pkts decrypt: 515, #pkts verify: 515
```

Verify DMVPN operation in the **StdBranch** router:

```
StdBranch#show dmvpn

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
```

Check the route to the private network in the headquarters **ASR** router as follows:

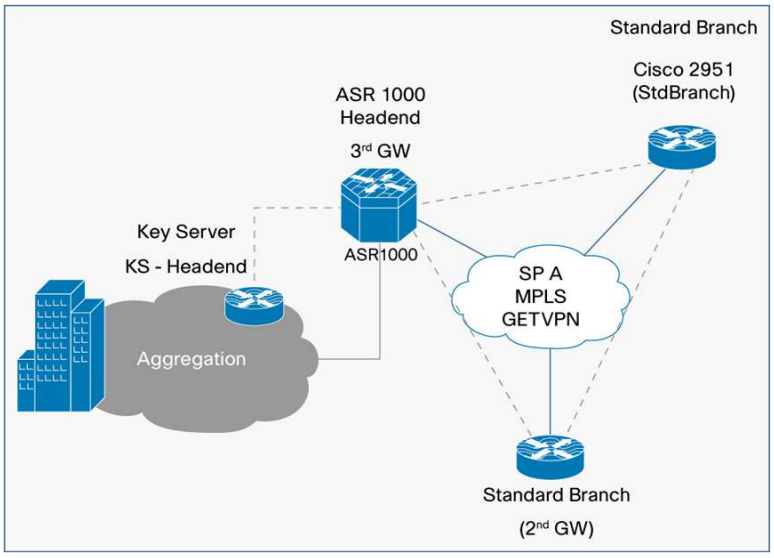
```
ASR##show ip route 10.5.110.217

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. Introduce the Key Server to the IP VPN

Figure 2 shows a topology diagram of GET VPN.

Figure 2. GET VPN Topology Diagram



Add a GET VPN key server to the IP VPN on the aggregation side.

Key-Server Configuration

The configuration added in the key-server headend follows.

More information about the key-server configuration is available in the Next Generation Enterprise WAN (NGEW) Regional WAN Deployment Guide documentation.

More information about the migration from the preshared key type of authentication to Public Key Infrastructure (PKI)-based authentication is available at: http://www.cisco.com/en/US/partner/products/ps6664/products_ios_protocol_option_home.html.

```
hostname KSHeadend

! 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 GET VPN-profile
 set security-association lifetime seconds 900        ! TEK lifetime
 set transform-set aes128
!
crypto gdoi group GET VPN-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 GET VPN-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 MPLS
 ip address 10.5.110.13 255.255.255.252
!

! 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-Server Operation Verification

Verify the operation of the key server using the following command-line interface (CLI) command:

```
KSHeadend#show crypto gdoi
GROUP INFORMATION
    Group Name               : GET VPN-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           : GET VPN-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. Modify Routing Metrics on Tunnel Interfaces

MPLS service providers typically use the BGP routing protocol. Therefore, routes in customer edge equipment must be advertised to the provider VPN with the BGP routing protocol to make GET VPN group members 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 advertising will disrupt 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 GET VPN group members as follows:

Add the following configuration in the **StdBranch**, **2nd GW**, and **ASR** routers:

```
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 also sets the administrative distance of the EIGRP route lower than the BGP routes.

Verify the administrative distance of EIGRP routes for a private network set to 15 (instead of the default value of 90) by executing the following CLI in the **ASR** router:

```
ASR#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. Modify Routed Path to Include Group Encrypted Transport-Enabled Core

The next step is 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:

Add the following configuration in the **StdBranch** router:

```
router bgp 65014
 bgp log-neighbor-changes
 network 10.5.110.16 mask 255.255.255.252
 network 10.6.10.0 mask 255.255.0.0
 network 10.6.11.0 mask 255.255.255.0
 neighbor 10.5.110.18 remote-as 65002
```

Add the following configuration in the **2nd GW** router:

```
router bgp 65015
  network 10.5.110.20 mask 255.255.255.252
  network 10.8.10.0 mask 255.255.255.0
  network 10.8.11.0 mask 255.255.255.0
  neighbor 10.5.110.21 remote-as 65003
```

Add the following configuration in the **ASR** router:

```
router bgp 65016
 network 10.5.110.28 mask 255.255.255.252
 network 10.7.10.0 mask 255.255.255.0
 network 10.7.11.0 mask 255.255.255.0
 neighbor 10.5.110.29 remote-as 65004
```

Verifying the BGP routing table includes GET VPN-enabled core routes:

Check the BGP routes in the headquarters router as follows:

```
ASR#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 (**ASR**) to reach the private network in branch offices:

```
ASR #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

ASR #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. Enable Symmetric Routing Between Branch Offices and Transition Headquarters to GET VPN

We have already added a Security Association (SA) policy in the key system so that the GDOI crypto map excludes ESP traffic (that is, GRE + IPsec). This addition helps ensure that traffic is not encrypted twice (once by DMVPN and the second time by GRE). In this step traffic flows through DMVPN tunnels until the individual sites are transitioned to GET VPN. After the transition, traffic is routed outside of the DMVPN tunnel and encrypted by

GET VPN. You must add the following configuration in headquarters and branch-office customer edge devices to make them part of the GET VPN group.

Provision GET VPN in the headquarters router (**ASR**) first:

GET VPN group encryption is enabled by adding the following configuration in the **ASR** router. After adding the configuration and applying the crypto map, the **ASR** router becomes a group member of GET VPN-DEMO group encryption.

```
! IKE configuration needed for GET VPN

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 GET VPN-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 GET VPN-DEMO            ! Group membership
```

Add the following in the **ASR** router to add the local private network to BGP:

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

Add the following configuration in the **ASR** router (DMVPN hub) to enable symmetric routing between branch offices during GET VPN transition. Transition branch offices to use GET VPN encryption one at a time.

Note: It is possible to have some of the branch offices using DMVPN and EIGRP (nonconverted sites) while other branch offices have transitioned to GET VPN (converted sites). To ensure that symmetric routing between branch offices works, you must redistribute nonconverted-site EIGRP routes learned by the hub into BGP routes. Basically this process injects EIGRP routes of nonconverted sites to BGP, making traffic from converted sites to nonconverted sites flow to the hub using GET VPN and then through DMVPN from the hub to the nonconverted site.

```
Router bgp 400
redistribute eigrp 44
```

Redistribute converted-site BGP routes into EIGRP to provide a symmetric route. This redistribution makes traffic from nonconverted sites to converted sites flow through the hub using a DMVPN tunnel and then from the hub to the converted site through a GET VPN on the WAN.

```

router eigrp 44
```

```
    redistribute bgp 400 metric 1500 100 255 1 1500
```

First apply the GDOI crypto map in the headquarters router as follows:

Apply GET VPN group encryption to the WAN interface:

```
ASR#(config)#int Gig0/0
ASR#(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 GET VPN-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 GET VPN-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 GET VPN-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. To verify this flow, do the following in the headquarters group member (**ASR**):

Verify the route to the PC connected to the private network in the **StdBranch** router from the **ASR** router:

```
ASR#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

ASR#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 the branch-office 1 router (**StdBranch**) from the **ASR** router:

```
ASR#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. Transition Individual Sites to GET VPN One at a Time

Transition each branch office to use GET VPN encryption from DMVPN encryption as follows:

Note: Monitor traffic loss during individual branch-office transition to GET VPN by executing the following command in the headquarters gateway (**ASR**). Ping the PC connected to the private network in the **StdBranch** router:

```
ASR#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 GET VPN-
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
!!!!!!!!!!!!!!!!!!!!
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
7 packets are lost during route convergence from EIGRP route to BGP route.
```

Transition the branch-office 1 group member (**StdBranch**) to use GET VPN encryption:

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

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

Add GET VPN configuration in branch-office 1 (**StdBranch**):

Enable GET VPN group encryption by adding the following configuration in the **StdBranch** router. After adding the configuration and applying the crypto map, the **StdBranch** router becomes a group member of GET VPN-DEMO group encryption:

```
! IKE configuration needed for GET VPN
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 GET VPN-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 GET VPN-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 GET 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 GET VPN-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 GET VPN-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 GET VPN-DEMO using address 10.5.110.17
```

During ping traffic flow, shut down the DMVPN tunnel in branch-office 1 router (**StdBranch**) as follows:

```


StdBranch#(config)#int Tu 10
StdBranch#(config-if)#shut
StdBranch#(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 remove EIGRP routes in the **StdBranch** group member. Verify the route is symmetric between local networks of branch-office routers (**StdBranch** and **2nd GW**). Traffic uses GDOI encryption between the **StdBranch** and **ASR** routers, and uses DMVPN IPsec encryption between the **ASR** and **2nd GW** routers. Check the route from the branch-office 1 (**StdBranch**) private network to the branch-office 2 (**2nd GW**) private network as follows:

```
StdBranch#show ip route eigrp

StdBranch#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
```

Redistribute this route from EIGRP to BGP in the **ASR** router:

```
ASR#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 (**2nd GW**) private network to the branch-office 1 (**StdBranch**) private network as follows:

Traffic uses DMVPN IPsec encryption between the **2nd GW** and **ASR** routers, and uses GDOI encryption between the **ASR** and **StdBranch** routers:

```
2nd GW#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

2nd GW#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 command shows that the GET VPN converted-site private network route is redistributed from BGP to the EIGRP table. This redistribution makes traffic from the nonconverted-site **2nd GW** router to the converted-site **StdBranch** router flow through the headquarters router (**ASR**) using a DMVPN tunnel.

```
ASR#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
```

Following is the topology after adding GET VPN encryption in individual sites. At this point, traffic between private networks and branch offices gets encrypted by DMVPN.

Verify that the route from branch-office 1 (**StdBranch**) to the headquarters private network uses the MPLS path:

```
StdBranch#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 confirm that Group Encrypted Transport-enabled interfaces are operational using following the CLI commands:

To check whether a group member is participating in GET VPN encryption, execute the following CLI command:

```
StdBranch#show crypto gdoi
GROUP INFORMATION
    Group Name               : GET VPN-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 an Internet Key Exchange (IKE) connection between the group member and the key system to receive rekeys:

```
StdBranch#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 GET VPN by using the following CLIs:

```
StdBranch#show crypto ipsec sa | incl encaps
    #pkts encaps: 297, #pkts encrypt: 297, #pkts digest: 297
```

Ping the headquarters private network address from the **StdBranch** router as follows:

```
StdBranch#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

StdBranch#show crypto ipsec sa | incl encaps
    #pkts encaps: 397, #pkts encrypt: 397, #pkts digest: 397
```

The output from that command shows the Internet Control Message Protocol (ICMP) traffic between branch-office 1 and headquarters is encrypted. Verify reachability between private networks in the **StdBranch** and **2nd GW** routers as follows:

```
StdBranch#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 the next branch-office 2 group member (**2nd GW**) to use GET VPN encryption:

Follow the same process described in the previous section for transitioning the **2nd GW** group member to use GET VPN encryption.

Now add GET VPN configuration in branch-office 2 (**2nd GW**):

GET VPN group encryption is enabled by adding the following configuration in **2nd GW**. After adding the configuration and applying the crypto map, **2nd GW** becomes a group member of GET VPN-DEMO group encryption.

```
! IKE configuration needed for GET VPN
```

```
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 GET VPN-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 GET VPN-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 GET VPN group encryption to the WAN interface as follows:

```
2nd GW#(config)#int Gi0/0
2nd GW#(config-if)#crypto map demo-gdoi
2nd GW#(config-if)#end
*Jun 11 15:29:03: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88 for
group GET VPN-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 GET VPN-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 GET VPN-DEMO using address 10.5.110.22
```

Shut down the DMVPN tunnel in the branch-office 2 group member (**2nd GW**) as follows:

```
2nd GW#(config)#int Tu 10
2nd GW#(config-if)#shut
2nd GW#(config-if)#end
```

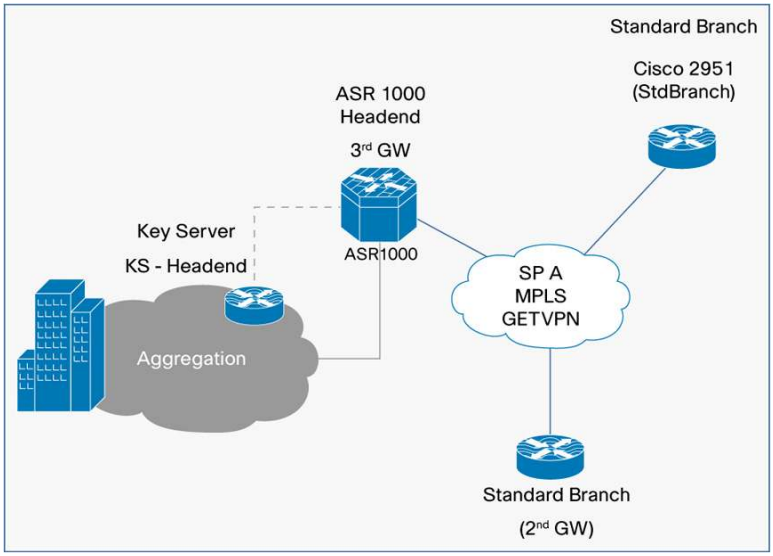
Shut down the DMVPN tunnel in the headquarters group member (**ASR**).

Shut down the DMVPN tunnel in the **ASR** router as follows:

```
ASR#(config)#int Tu 5
ASR#(config-if)#shut
ASR#(config-if)#exit
```

Figure 3 shows the topology after individual sites are transitioned to GET VPN.

Figure 3. Topology After Individual Sites Are Transitioned to Use GET VPN Encryption and DMVPN Tunnels Are Shut Down



Now transition each subsequent branch-office group member to use GET VPN encryption:

Follow the same process described in the previous section for transitioning each group member to use GET VPN encryption. During the transition process, you can observe three general traffic patterns:

- Between converted site and converted site: This traffic should flow directly between the group members through the GET VPN-encrypted WAN infrastructure.
- Between converted site and nonconverted site: This traffic should flow through the DMVPN hub. Traffic between the converted site and the hub is encrypted using GET VPN on the WAN, whereas traffic between the hub and the nonconverted site is encrypted and tunneled through DMVPN.
- 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.

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

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

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

```
StdBranch#(config)#no router eigrp 44
StdBranch#(config)#no ip route 0.0.0.0 0.0.0.0 10.5.110.18
StdBranch#(config)#no interface Tunnel10
```

Clean up the DMVPN configuration from the branch-office 2 group member (**2nd GW**) as follows:

```
2nd GW#(config)#no router eigrp 44
2nd GW#(config)#no ip route 0.0.0.0 0.0.0.0 10.5.110.21
2nd GW#(config)#no interface Tunnel10
```

Clean up the DMVPN configuration from the headquarters group member (**ASR**) as follows:

```
ASR#(config)#no router eigrp 44
ASR#(config)#router bgp 400
ASR#(config-router)#no redistribute eigrp 44
ASR#(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 C07-690217-00 10/11