



Implementing Group Domain of Interpretation in a Dynamic Multipoint Virtual Private Network

INTRODUCTION

Group Domain of Interpretation (GDOI) is a group key protocol whereby all group members register with a key server. The concept is to use a group (common) key among a group of routers for encryption and decryption. The key server and a few group members have the ability to form a group; the key server authenticates the group member and distributes group keys and policies to the group members. The traffic encrypted by a group member can be decrypted by any other group member registered with the same key server. No additional security negotiation is needed between any two group members when they want to encrypt traffic between them. More details are given in the following sections.

Dynamic Multipoint VPN (DMVPN) provides spoke-to-hub and spoke-to-spoke connectivity solutions using multipoint generic routing encapsulation (mGRE) and Next Hop Resolution Protocol (NHRP). If spoke-to-spoke direct connectivity is enabled in the network, the spoke maintains a permanent IP Security (IPsec) tunnel to the hub, but the spoke-to-spoke IPsec tunnel is dynamic (on demand). Whenever spoke-to-spoke connectivity is desired, the originating spoke will send an NHRP resolution request to the hub, and the destination spoke and the hub will respond with a nonbroadcast, multiaccess (NBMA) address mapped to the destination's NHRP address.

Once the mapping is received, the spoke will initiate a dynamic IPsec tunnel with the destination spoke using the same mGRE interface. Traffic will start passing through this dynamic tunnel. Until this dynamic tunnel is built, traffic continues to pass through the hub. To get any response from the destination spoke, the same procedure is initiated by the destination spoke toward the originating spoke. Creation of a dynamic tunnel prevents the hub from being bombarded with spoke-to-spoke traffic but introduces some delay in setting up the tunnel. Though this delay exists for any direct communication between spokes, certain real-time applications, such as voice, might still look to avoid it. By using GDOI technology, the delay caused by IPsec negotiation is eliminated, which is the major contributor to the overall delay. GDOI is not a replacement for DMVPN.

DOCUMENT SCOPE

This document describes the topology setup of the configuration of GDOI in the deployment of an Enterprise-Class Teleworker (ECT) solution. It provides a step-by-step explanation and discusses the specific hardware and software required to set up this network. This document does not go into detail explaining DMVPN and its deployment on specific platforms. The reader is expected to be familiar with DMVPN concepts.

GDOI IN DMVPN NETWORK DEPLOYMENT

To understand this deployment, a brief introduction is given regarding GDOI followed by the high-level packet flow in this implementation.

Note: Cisco Systems® implements the GDOI protocol using the Cisco IOS® Software Secure Multicast feature, which was introduced in Cisco IOS Software Release 12.4(6)T.

GDOI describes a protocol for a group of systems to download encryption keys and security policy from a key server. The key server is a router that distributes encryption keys to a group of systems (group members). Group members that setup Internet Key Exchange (IKE) sessions with the key server download encryption keys and policies required for encryption. Both group members and key servers use

identity strings to represent a group. The basic goal behind a GDOI implementation is to overcome the limitations of regular IPsec-like pairwise keys, point-to-point tunnel, no multicast support, etc. With GDOI, all group members within a group can send and receive encrypted traffic between them using the same group key obtained from the key server. Any encrypted traffic within the same group can be decrypted by any group member. There is no need to build point-to-point IPsec sessions between various group members, avoiding the use of pairwise keys. Unlike plain IPsec, GDOI maintains a single IPsec session between the group member and key server, and no other IPsec sessions exist between group members.

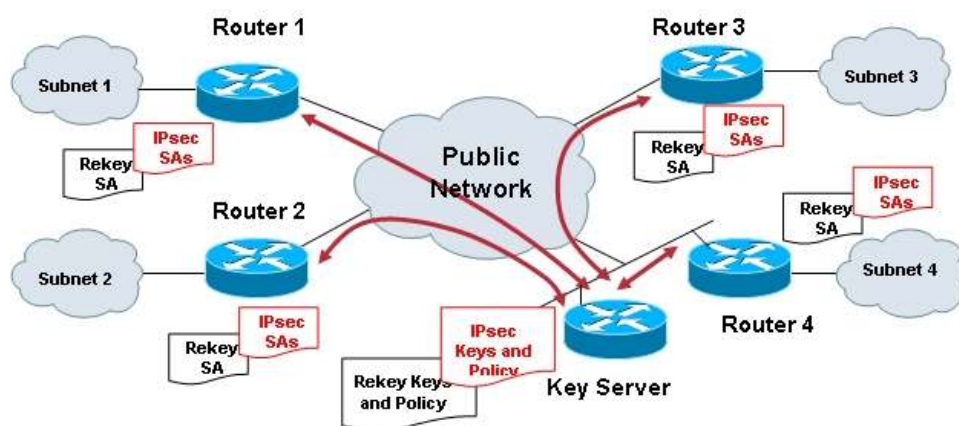
The security policies and access lists are defined on the key server. The access list can also include multicast entries. To support multicast encryption, all the group members should have multicast capability between them. Since policies are defined only on the key server, the same set of policies is downloaded to all group members within a group. The key server pushes new group keys (also known as a rekey) whenever needed, like IPsec security associations (SAs) lifetime expiration, clearing the GDOI session. Key servers can use either unicast or multicast key distribution for rekeying. To support multicast rekeying, all group members should have multicast capability.

GDOI requires a group member registered with the key server; GDOI registration occurs in two phases.

1. IKE phase 1 (the same used in plain IPsec)
2. GDOI registration protocol (similar to quick mode in IPsec)

GDOI uses User Datagram Protocol (UDP) 848 to establish its IKE sessions between the key server and the group members. Upon receiving a registration request, the key server authenticates the router, performs an optional authorization check, and downloads the policy and keys to the group member. The group member is ready to use these encryption keys. The key server pushes new keys to the group (also known as rekeying the group) whenever needed, similar to SA expiration. The key server can host multiple groups and each group will have a different group key.

Figure 1. GDOI Registration



How does GDOI help in a DMVPN network?

In an ECT solution, DMVPN is implemented using tunnel protection enabled in the tunnel interfaces of both hub and spokes. Tunnel protection uses IPsec profiles, which install policies dynamically during tunnel negotiation between them. From the deployment perspective, each spoke maintains a permanent IPsec tunnel with the hub, and any spoke-to-spoke connectivity requires the spoke to send out a NHRP resolution request to the hub. Upon receiving an NHRP resolution reply, the spoke will dynamically create another IPsec tunnel directly with the destination spoke. A new set of pairwise keys is negotiated between spokes directly, and a point-to-point tunnel is created. As mentioned previously, this introduces a delay in setting up direct tunnels. By integrating GDOI within the DMVPN, delay can be reduced by eliminating this creation of direct tunnels between spokes.

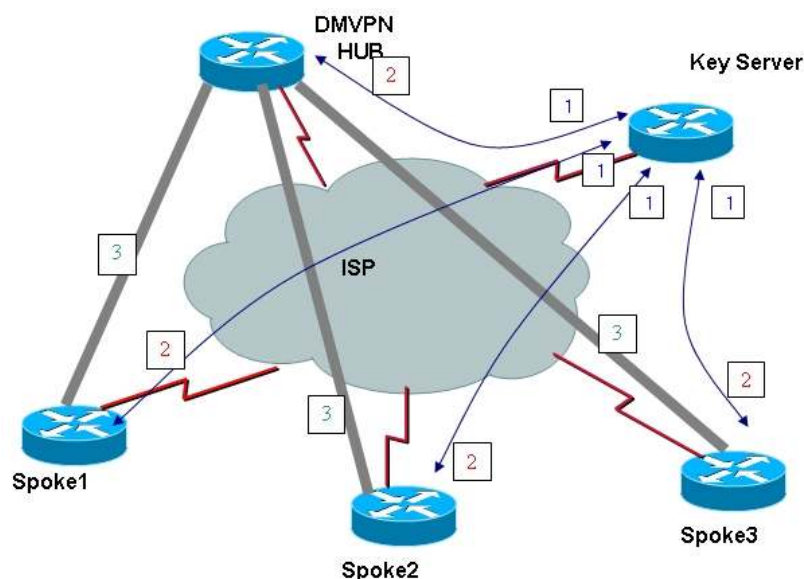
With GDOI, the spokes and hubs are group members and group keys can be distributed to the hub and all spokes, eliminating the need for point-to-point IPsec sessions between them. Any group member can talk to any other group member using the same key. This means the spoke changes the destination address to forward traffic directly to other spokes once NHRP resolution is completed. This reduces the delay between spoke-to-spoke connections by eliminating creation of dynamic IPsec tunnels between them. With this integration, each spoke maintains a GDOI session only with the key server and there is no permanent tunnel between the hub and spoke. The spoke maintains NHRP entries for the hub; the spoke still needs to contact the hub first whenever spoke-to-spoke connectivity is required. The key server can push “gre any any” to all group members to achieve the same result as DMVPN using tunnel protection. This requires no other change in the key server as new spokes are added. Also, GDOI does not support IPsec profiles, so tunnel protection is removed from tunnel interfaces and GDOI is tied to the physical interface.

Following is the summary of packet flow in the DMVPN network using GDOI.

1. The hub and all spokes, configured as group members, register with the GDOI key server.
2. The key server distributes group key and IPsec policy to all group members; IPsec policy defines the traffic selectors. For DMVPN, “gre any any” could secure all tunnel traffic.
3. A spoke-to-hub tunnel is established using NHRP. All packets traveling via the DMVPN tunnel are now encrypted using the group key.
4. The spoke sends an NHRP resolution request to the hub for any spoke-to-spoke communication.
5. Upon receiving an NHRP resolution reply from the hub, the spoke sends traffic directly to other spokes with group key encryption. Until the NHRP resolution reply is received, spoke-to-spoke traffic continues via the hub with group key encryption.

Note: Multicast traffic will be forwarded to the hub for any spoke-to-spoke communication, even with this deployment.

Figure 2. Packet Flow



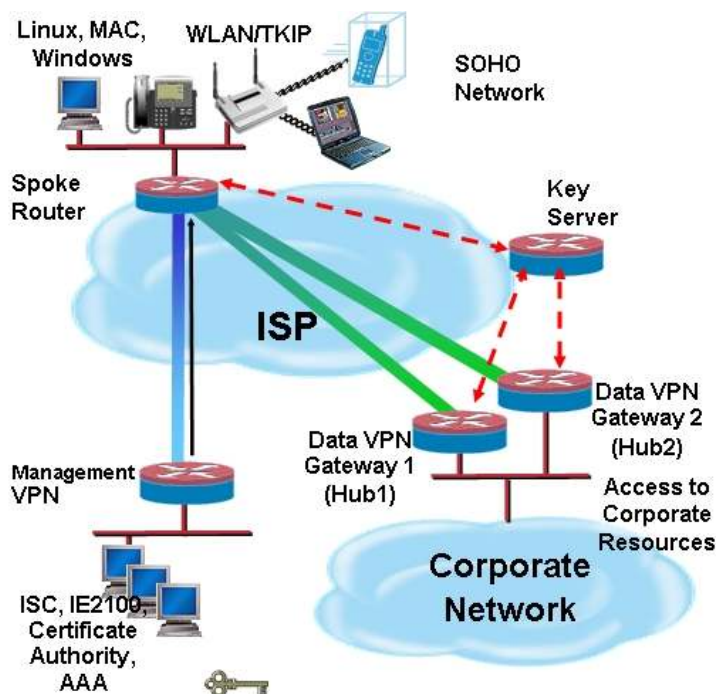
Note: Points 4 and 5 are not shown in the diagram; they are exchanged between the hub and the spokes over the tunnel formed in step 3.

NETWORK ARCHITECTURE

TOPOLOGY

The following topology shows deploying GDOI in an existing ECT solution. The detailed packet flow using GDOI has been explained in the previous section.

Figure 3. GDOI in the Original ECT Solution



RECOMMENDED PLATFORMS AND IMAGES

Images based on Cisco IOS Software Release 12.4(9)T are required to enable GDOI. The following platforms are suggested for various roles of this deployment.

- **Key server:** Cisco 1700 Series Modular Access Router and above
- **Group member configured for DMVPN hub:** Cisco 3800 Integrated Service Router and above
- **Group member configured for DMVPN spoke:** Cisco 871 Ethernet Broadband Router and above

DEPLOYMENT

GDOI is deployed in our ECT solution setup and both data and voice are tested in this network. The delay created when initiating voice calls does not exist. From the ECT perspective, GDOI is tied to the physical interface; it does not support IPsec profiles, and tunnel protection is removed from the tunnel interfaces. GDOI can coexist with plain IPsec tunnels used for manageability.

INITIAL SETUP

Both hub and spoke are configured as GDOI group members and a separate router is configured for the GDOI key server. The following configuration is required to enable GDOI in a DMVPN setup.

Key Server Configuration

!!!! The following configuration enables keyserver in a router. Each group defined in keyserver has an identity which is shared among the members within the group. Here identity is set to 1234 for group 'dmvpn'. Key server also defines the policies using access-list 105 to be distributed to group members upon registration. !!!!

```
!  
crypto gdoi group dmvpn  
identity number 1234  
server local  
rekey lifetime seconds 300  
sa ipsec 1  
profile dmvpn-gdoi  
match address ipv4 105  
!
```

!!!! ISAKMP and IPsec profile configuration are defined below. As the setup is using PKI certificates, configurations involving PKI are not shown here. !!!!

```
!  
crypto isakmp policy 1  
encr 3des  
!  
crypto isakmp keepalive 10  
!  
!  
crypto ipsec transform-set t1 esp-3des esp-sha-hmac  
mode transport require  
!  
crypto ipsec profile dmvpn-gdoi  
set security-association lifetime seconds 300  
set transform-set t1  
!
```

!!!! The following configuration shows that there is no crypto map associated with any physical interface. !!!!

```
!  
interface Loopback0  
description interface used for tunnel setup  
ip address 192.168.1.1 255.255.255.255  
!  
interface FastEthernet0/0  
description to ISP  
ip address 10.1.1.1 255.255.255.240  
duplex auto  
speed auto  
!
```

!!!! The following acl defines the policies to be pushed to group members. 'gre any any' is used here to encrypt all traffic seen in dmvpn tunnel interface, just to achieve the same as dmvpn with tunnel protection. !!!!

```
!
```

```
access-list 105 permit gre any any
```

Note: One advantage with this acl 105 is that there is no additional configuration required in key server for newly added spokes within the same group/dmvpn. Only respective spokes need to be configured for GDOI.

Group Member Configuration on DMVPN Hub

!!!! IPsec transform-sets and profile configurations are not required as they are part of negotiation with key server when establishing GDOI session. Only ISAKMP configurations are required to be defined. !!!!

```
!  
crypto isakmp policy 1  
  encr 3des  
!  
crypto isakmp keepalive 10  
!
```

!!!! Group member is defined with same identity and location of key server. !!!!

```
!  
crypto gdoi group dmvpn  
  identity number 1234  
  server address ipv4 192.168.1.1  
!
```

!!!! Crypto map has a new type 'gdoi' and is tied to group member created above. !!!!

```
!  
crypto map gdoi 1 gdoi  
  set group dmvpn  
!
```

!!!! Tunnel protection is removed from tunnel interface. !!!!

```
!  
interface Tunnel100  
  description DMVPN - EIGRP network  
  bandwidth 2000  
  ip address 1.1.1.1 255.255.255.0  
  no ip redirects  
  ip mtu 1400  
  no ip next-hop-self eigrp 7  
  ip pim nbma-mode  
  ip pim sparse-dense-mode  
  ip multicast rate-limit out 768  
  ip nhrp map multicast dynamic  
  ip nhrp network-id 1000  
  ip nhrp holdtime 600  
  ip nhrp server-only  
  ip tcp adjust-mss 1360  
  no ip split-horizon eigrp 7  
  no ip mroute-cache  
  delay 1500
```

```

tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 10000
!
interface Loopback0
ip address 192.1.1.2 255.255.255.0
no ip redirects
!

```

!!!! GDOI is enabled by applying crypto map to physical interface. !!!!

```

!
interface GigabitEthernet0/0
ip address 10.1.1.2 255.255.255.240
crypto map gdoi
!

```

Group Member Configuration on DMVPN Spoke

!!!! IPsec transform-sets and profile configurations are not required as they are part of negotiation with key server when establishing GDOI session. Only ISAKMP configurations are required to be defined. !!!!

```

!
crypto isakmp policy 1
encr 3des
crypto isakmp keepalive 10
!

```

!!!! Group member is defined with same identity and location of key server. !!!!

```

!
crypto gdoi group dmvpn
identity number 1234
server address ipv4 192.168.1.1
!

```

!!!! Crypto map with type gdoi is defined along with management tunnel. From the spoke's perspective, it may be necessary to keep management tunnel active along with GDOI session (as part of ECT solution) for the following reasons. Management tunnel is point-to-point and mostly used for management purpose as well as to access PKI/AAA servers in a secure mode. !!!!

```

!
crypto map mgmt-gdoi 1 ipsec-isakmp
description Management Tunnel
set peer 192.168.1.10
set transform-set mgmt-ipsec
match address mgmt_acl
crypto map mgmt-gdoi 2 gdoi
set group dmvpn
!

```

!!!! Tunnel protection is removed from tunnel interface. !!!!

```

!
interface Tunnel10

```

```
bandwidth 2000
ip address 1.1.1.11 255.255.254.0
no ip redirects
ip mtu 1400
ip nhrp map multicast 192.1.1.2
ip nhrp map 1.1.1.1 192.1.1.2
ip nhrp network-id 1000
ip nhrp holdtime 300
ip nhrp nhs 1.1.1.1
ip nhrp registration no-unique
ip pim sparse-dense-mode
ip multicast rate-limit out 128
ip tcp adjust-mss 1360
no ip mroute-cache
load-interval 30
delay 2000
qos pre-classify
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key 10000
!
```

!!!! GDOI is enabled by applying crypto map to physical interface. !!!!

```
!
interface FastEthernet4
description outside interface
ip address dhcp client-id FastEthernet4
ip access-group fw_acl in
crypto map mgmt-gdoi
!
```

!!!! The following line is added to firewall acl to permit GDOI packets (udp 848). !!!!

```
!
ip access-list extended fw_acl
permit udp any any eq 848
!
```


BENEFITS

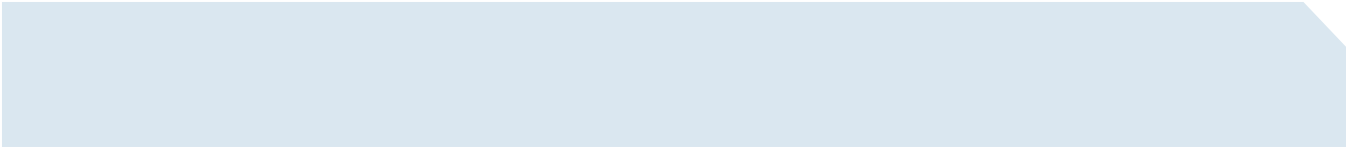
- The hub and all spokes use group key for encryption and decryption.
- No separate IPsec spoke-to-spoke tunnel is required.
- There is minimal or no delay in setting up voice calls between spokes.
- Hub and spokes will have a single GDOI session with the key server.
- If rekey is enabled, spokes don't need to re-register with the key server.
- It is easy to migrate from DMVPN with tunnel protection to GDOI-based DMVPN.

CAVEATS / FINAL NOTES

- An additional device is needed to function as the GDOI key server.
- There is no redundancy support for key servers.
- If rekey fails for any GM, GM must re-register with the key server after SA lifetime expiration; this may cause temporary disconnect in the network.
- Tunnel protection needs to be removed from the mGRE interface; though no issues are observed for spoke-to-spoke, this may cause packet loss in between, due to the separation of NHRP and crypto functions.
- The GDOI crypto map must be applied in the physical interface for the hub and all spokes.
- The image must be upgraded to Cisco IOS Software Release 12.4(9)T in the hub and all spokes.
- There is no support for mixed GDOI based DMVPN spokes and DMVPN spokes with tunnel protection.
- GDOI based DMVPN spokes behind Network Address Translation (NAT) are NOT supported for spoke to hub or spoke to spoke tunnel. The support may be available in later GDOI_DMVPN phases.
- For rekey to work, an exclusive Internet Group Management Protocol (IGMP) join is needed in the mGRE interface.
- If GM has to be removed from a group, the changes may take as long as traffic encryption keys lifetime remains.
- If direct spoke to spoke traffic is blocked, it would cause traffic blackhole as NHRP and crypto functions are separated. There may be improvements in later GDOI_DMVPN phases.
- Provisioning and Management support for GDOI_DMVPN solution in Cisco Security Manager 3.0 through flexconfig (templates)

REFERENCES

1. Enterprise Class Teleworker Deployment Guide:
http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd801dc5b2.shtml
2. Layered Security in a VPN Deployment:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_white_paper0900aecd8046cbc4.shtml
3. Secure Voice and Wireless in a VPN Deployment:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6814/prod_white_paper0900aecd8044177c.pdf
4. Integrated Easy VPN and Dynamic Multipoint VPN:
http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd80267995.shtml
5. Deployment of Secure Socket Layer VPNs:
http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd8029d630.shtml
6. Cisco IOS IPsec High Availability:
http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd80278edf.shtml

- 
7. RFC3547 - Group Domain of Interpretation (GDOI): <http://www.ietf.org/rfc/rfc3547.txt>

APPENDIX A: CONFIGURATION

CISCO 2811 INTEGRATED SERVICES ROUTER (KEY SERVER)

Management subnet – 10.32.200.x

DMVPN hub subnet – 10.32.100.x

DMVPN subnet – 1.1.1.x

Spoke internal subnet – 10.10.10.x

Full configuration

```
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname 2811-key-server
!
boot-start-marker
boot system flash c2800nm-adventerprisek9-mz.124-9.T
boot-end-marker
!
logging buffered 51200 warnings
enable secret 5 < deleted >
!
aaa new-model
!
!
aaa group server radius acs_server
server-private 10.32.200.1 auth-port 1812 acct-port 1813 key 7 <deleted>
!
aaa authentication login admin group tacacs+ enable
aaa authorization network pkiaaa group acs_server
!
aaa session-id common
!
resource policy
!
clock timezone pst -8
clock summer-time pdt recurring
ip subnet-zero
no ip source-route
!
!
ip cef
no ip dhcp use vrf connected
!
```

```
!  
ip tftp source-interface Loopback0  
ip domain name test.com  
ip host test-ca.test.com 10.32.200.10  
ip multicast-routing  
no ip ips deny-action ips-interface  
!  
!  
crypto pki trustpoint test-ca  
  enrollment mode ra  
  enrollment url http://test-ca:80/certsrv/mscep/mscep.dll  
  serial-number  
  revocation-check crl  
  authorization list pkiaaa  
!  
!  
crypto pki certificate chain test-ca  
  certificate <deleted>  
  certificate ca <deleted>  
!  
!  
class-map match-any imp  
  match qos-group 1  
class-map match-all voice  
  match ip dscp ef  
!  
!  
policy-map p1  
  class imp  
  class voice  
  class class-default  
    fair-queue  
!  
!  
!  
crypto isakmp policy 1  
!  
crypto isakmp policy 2  
  encr 3des  
!  
crypto isakmp policy 3  
  encr aes 256  
crypto isakmp keepalive 10  
!  
!  
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
```

```
mode transport require
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
crypto ipsec transform-set t4 esp-aes 256 esp-sha-hmac
mode transport require
!
crypto ipsec profile dmvpn-gdoi
set transform-set t1
!
crypto gdoi group dmvpn
identity number 1234
server local
rekey lifetime seconds 86400
sa ipsec 1
profile dmvpn-gdoi
match address ipv4 105
!
!
!
!
interface Loopback0
ip address 192.168.1.1 255.255.255.255
!
interface FastEthernet0/0
description connected to Gateway for ISP
ip address 10.32.100.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Async0/0/0
no ip address
!
interface Async0/0/1
no ip address
!
router ospf 1
log-adjacency-changes
network 10.32.100.0 0.0.0.255 area 0
network 192.168.1.1 0.0.0.0 area 0
!
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.32.100.100
!
!
ip http server
ip http authentication aaa
no ip http secure-server
ip pim bidir-enable
ip pim rp-address x.x.x.x multicast_rp_blockdensemode
ip pim ssm range multicast_ssm_range
!
ip access-list standard multicast_rp_blockdensemode
  remark ACL to block dense-mode operation of client broadcasts
  remark during routing instability (applied to pim rp-address command)
  deny 224.0.1.39
  deny 224.0.1.40
  permit any
ip access-list standard multicast_ssm_range
  remark ACL to define SSM admin range
  permit < Internal SSM range >
!
!
!
!
control-plane
!
!
!
!
!
mgcp behavior rsip-range tgcp-only
!
!
!
!
!
```

```
banner login ^C
```

```
Login Banner
```

```
C i s c o S y s t e m s
```

```
  ||      ||  
  ||      ||      Cisco Systems, Inc.  
  |||     |||  
  ..:|||||:..:|||||:..
```

```
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
```

```
You must have explicit permission to access or configure this  
device. All activities performed on this device are logged and  
violations of this policy may result in disciplinary action.
```

```
Contact admin@cisco.com for details.
```

```
^C
```

```
banner motd ^CC
```

```
C i s c o S y s t e m s
```

```
  ||      ||  
  ||      ||      Cisco Systems, Inc.  
  |||     |||      IT-Transport  
  .:|||||:|:.....:|||||:..
```

```
US, Asia & Americas support:    + 1 408 526 8888
```

```
EMEA support:                  + 31 020 342 3888
```

```
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
```

```
You must have explicit permission to access or configure this  
device. All activities performed on this device are logged and  
violations of this policy may result in disciplinary action.
```

```
^C
```

```
!
```

```
line con 0
```

```
exec-timeout 600 0
```

```
transport output all
```

```
stopbits 1
```

```
line aux 0
```

```
stopbits 1
```

```
line 0/0/0 0/0/1
```

```
stopbits 1
```

```
speed 115200
```

```
flowcontrol hardware
```

```
line vty 0 4
```

```
exec-timeout 120 0
```

```
authorization exec tacacs+
```

```
login authentication admin
```

```
transport input all
```

```
transport output all
line vty 5 15
transport input ssh
transport output all
!
scheduler allocate 20000 1000
ntp clock-period 17179772
ntp server <IP_ADD of public NTP server>
ntp server <IP_ADD of public NTP server>
!
end
```

CISCO 3845 INTEGRATED SERVICES ROUTER (GROUP MEMBER / DMVPN HUB)

Cisco 3845 Integrated Services Router is configured for DMVPN hub running Cisco IOS Software Release 12.4(9)T image.

Management subnet – 10.32.200.x

DMVPN hub subnet – 10.32.100.x

DMVPN subnet – 1.1.1.x

Spoke internal subnet – 10.10.10.x

Full configuration

```
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname 3845-group-member-hub
!
boot-start-marker
boot system flash c3845-adventerprisek9-mz.124-9.T
boot-end-marker
!
logging buffered 100000 debugging
enable secret 5 < deleted >
!
aaa new-model
!
!
aaa group server radius acs_server
server-private 10.32.200.1 auth-port 1812 acct-port 1813 key 7 <deleted>
!
aaa authentication login admin group tacacs+ enable
aaa authorization network pkiaaa group acs_server
!
aaa session-id common
```



```
!
resource policy
!
clock timezone pst -8
clock summer-time pdt recurring
ip subnet-zero
no ip source-route
ip cef
!
!
no ip dhcp use vrf connected
!
!
ip tftp source-interface Loopback0
ip domain name test.com
ip host test-ca.cisco.com 10.32.200.10
ip multicast-routing
no ip ips deny-action ips-interface
!
!
!
!
crypto pki trustpoint test-ca
  enrollment mode ra
  enrollment url http://test-ca:80/certsrv/mscep/mscep.dll
  serial-number
  revocation-check crl
  auto-enroll 70
  authorization list pkiaaa
!
!
crypto pki certificate chain test-ca
  certificate < deleted >
  certificate ca < deleted >
no crypto engine onboard 0
no crypto engine aim 0
!
!
class-map match-any imp
  match qos-group 1
class-map match-all voice
  match ip dscp ef
!
!
policy-map p1
  class imp
```

```

class voice
class class-default
    fair-queue
!
!
!
crypto isakmp policy 1
!
crypto isakmp policy 2
    encr 3des
!
crypto isakmp policy 3
    encr aes 256
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
    mode transport require
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
crypto ipsec transform-set t4 esp-aes 256 esp-sha-hmac
    mode transport require
!
crypto gdoi group dmvpn
    identity number 1234
    server address ipv4 192.168.1.1
!
!
crypto map gdoi 1 gdoi
    set group dmvpn
!
!
!
!
interface Tunnel100
description DMVPN - EIGRP network
bandwidth 2000
ip address 1.1.1.1 255.255.255.0
no ip redirects
ip mtu 1400
no ip next-hop-self eigrp 7
ip pim nbma-mode
ip pim sparse-dense-mode
ip multicast rate-limit out 768
ip nhrp map multicast dynamic
ip nhrp network-id 1000
ip nhrp holdtime 600

```

```
ip nhrp server-only
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
no ip mroute-cache
delay 1500
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 10000
!
interface Loopback0
ip address 192.1.1.2 255.255.255.255
no ip redirects
!
interface GigabitEthernet0/0
description Interface connected to Gateway for ISP
ip address 10.32.100.2 255.255.255.0
ip pim sparse-dense-mode
duplex auto
speed auto
media-type rj45
crypto map gdoi
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
media-type rj45
negotiation auto
!
router eigrp 1
 redistribute static route-map split_in
 redistribute bgp 100 route-map split_in
 network 1.1.1.0 0.0.0.255
 default-metric 1000 100 255 1 1500
 no auto-summary
 no eigrp log-neighbor-changes
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 metric 10 subnets route-map split_out
 network 10.32.100.0 0.0.0.255 area 0
 network 192.1.1.2 0.0.0.0 area 0
!
router bgp 100
 no synchronization
```

```

bgp log-neighbor-changes
bgp redistribute-internal
neighbor 10.32.100.200 remote-as 100
distance bgp 20 20 200
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.100.100
ip route < Corporate Internal Networks > 210
!
!
ip http server
ip http authentication aaa
no ip http secure-server
ip pim bidir-enable
ip pim rp-address x.x.x.x multicast_rp_blockdensemode
ip pim ssm range multicast_ssm_range
!
ip access-list standard multicast_rp_blockdensemode
remark ACL to block dense-mode operation of client broadcasts
remark during routing instability (applied to pim rp-address command)
deny 224.0.1.39
deny 224.0.1.40
permit any
ip access-list standard multicast_ssm_range
permit < Internal SSM range >
ip access-list standard split_in
permit < Corporate Internal Networks >
ip access-list standard split_out
permit < Spoke Subnets >
permit < ... >
permit < ... >
logging < Syslog_Server >
snmp-server engineID local <deleted>
snmp-server community <deleted>
snmp-server community <deleted>
snmp-server community <deleted>
snmp-server enable traps tty
snmp-server host < y.y.y.y > < community >
!
route-map split_in permit 10
match ip address split_in
!
route-map split_out permit 10
match ip address split_out
!

```

```

!
!
!
tacacs-server host <deleted>
tacacs-server host <deleted>
tacacs-server timeout 3
tacacs-server directed-request
!
control-plane
!
!
!
!
mgcp behavior rsip-range tgcp-only
!
!
!
!
!
banner login ^C

```

```

C i s c o S y s t e m s
  ||                ||
  ||                ||      Cisco Systems, Inc.
  ||||             ||||    IT-Transport
.:|||||:|:.....:|||||:..
US, Asia & Americas support:    + 1 408 526 8888
EMEA support:                  + 31 020 342 3888
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
You must have explicit permission to access or configure this
device. All activities performed on this device are logged and
violations of this policy may result in disciplinary action.

```

^C

```

banner motd ^C

```

```

C i s c o S y s t e m s
  ||                ||
  ||                ||      Cisco Systems, Inc.
  ||||             ||||    IT-Transport
.:|||||:|:.....:|||||:..
US, Asia & Americas support:    + 1 408 526 8888
EMEA support:                  + 31 020 342 3888
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
You must have explicit permission to access or configure this
device. All activities performed on this device are logged and
violations of this policy may result in disciplinary action.

```

^C

```

!
line con 0
  exec-timeout 600 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  exec-timeout 120 0
  authorization exec tacacs+
  login authentication admin
  transport input all
  transport output all
line vty 5 15
  transport input ssh
  transport output all
!
scheduler allocate 20000 1000
ntp clock-period 17179527
ntp server < IP_ADD of public NTP server >
ntp server < IP_ADD of public NTP server >
!
end

```

CISCO 871 INTEGRATED SERVICES ROUTER (GROUP MEMBER / DMVPN SPOKE)

Cisco 871 Integrated Services Router configured as spoke running c870-adventerprise9-mz.124-9.T image.

This configuration may include some basic security configurations such as Auth Proxy, context-based access control (CBAC), or firewall. Please refer to the deployment guides listed in the reference section for additional details.

Management subnet – 10.32.200.x

DMVPN hub subnet – 10.32.100.x

DMVPN subnet – 1.1.1.x

Spoke internal subnet – 10.10.10.x

Full configuration

```

version 12.4
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname 871-group-member-spoke
!
boot-start-marker
boot system flash:c870-adventerprise9-mz.124-9.T
boot-end-marker
!

```

```
logging buffered 100000 debugging
no logging console
no logging cns-events
enable secret 5 <deleted>
!
aaa new-model
!
!
aaa group server radius acs_server
    server-private 10.32.200.1 auth-port 1645 acct-port 1646 key 7 <deleted>
    ip radius source-interface BVI1
    deadtime 1
!
aaa group server radius radius-eap
    server-private 10.10.10.1 auth-port 1812 acct-port 1813 key 7 <deleted>
!
aaa authentication login default local group acs_server
aaa authentication login eap_methods group radius-eap
aaa authorization exec default local
aaa authorization auth-proxy default group acs_server
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip dhcp use vrf connected
no ip dhcp conflict logging
!
ip dhcp pool client
    import all
    network 10.10.10.0 255.255.255.240
    domain-name test.com
    option 150 ip <TFTP address used by IP phone>
    netbios-name-server <Corporate NETBIOS servers>
    dns-server <Corporate DNS servers / Public DNS servers>
    default-router 10.10.10.1
    update arp
!
ip dhcp pool public
    import all
    network 192.168.2.0 255.255.255.0
```

```

    default-router 192.168.2.1
!
!
ip cef
ip tftp source-interface BV11
no ip domain lookup
ip domain name test.com
ip host test-ca 10.32.200.10
ip host ie2100 10.32.200.11
ip ftp source-interface BV11
ip multicast-routing
ip inspect name test tcp
ip inspect name test udp
ip inspect name test realaudio
ip inspect name test rtsp
ip inspect name test tftp
ip inspect name test ftp
ip inspect name test h323
ip inspect name test netshow
ip inspect name test streamworks
ip inspect name test skinny
ip inspect name test sip
ip auth-proxy auth-proxy-banner http
ip auth-proxy name authproxy http inactivity-time 60 list proxy_acl
ip admission auth-proxy-banner http
no ip ips deny-action ips-interface
!
! Configuration for PKI certificates
crypto pki trustpoint test-ca
    enrollment mode ra
    enrollment url http://test-ca:80/certsrv/mscep/mscep.dll
    serial-number
    revocation-check none
    source interface BV11
!
!
crypto pki certificate chain test-ca
    certificate < deleted >
    certificate ca < deleted >
!
!
class-map match-any call-setup
    match ip dscp af31
    match ip dscp af32
    match ip dscp cs3
    match ip precedence 3
```



```

class-map match-any internetwork-control
  match ip dscp cs6
  match access-group name ike_acl
class-map match-any voice
  description Note LLQ for ATM/DSL G.729=64K, G.711=128K
  match ip dscp ef
  match ip dscp cs5
  match ip precedence 5
!
!
!
crypto isakmp policy 1
  encr 3des
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime seconds 14400
!
crypto ipsec transform-set mgmt-ipsec esp-3des esp-sha-hmac
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
  mode transport
!
!
!
crypto gdoi group dmvpn
  identity number 1234
  server address ipv4 192.168.1.1
!
!
crypto map mgmt-gdoi 1 ipsec-isakmp
  description Management Tunnel
  set peer 192.168.1.10
  set transform-set mgmt-ipsec
  match address mgmt_acl
crypto map mgmt-gdoi 2 gdoi
  description gdoi
  set group dmvpn
!
!
  bridge irb
!
! !!!Tunnel configuration includes dual-DMVPN hub for redundancy !!!
interface Tunnel10
  bandwidth 2000
  ip address 1.1.1.11 255.255.255.0

```

```

no ip redirects
ip mtu 1400
ip nhrp map 1.1.1.1 192.1.1.2
ip nhrp map 1.1.1.2 192.1.1.3
ip nhrp map multicast 192.1.1.2
ip nhrp map multicast 192.1.1.2
ip nhrp network-id 1000
ip nhrp holdtime 300
ip nhrp nhs 1.1.1.1
ip nhrp nhs 1.1.1.2
ip nhrp registration no-unique
ip pim sparse-dense-mode
ip multicast rate-limit out 128
ip tcp adjust-mss 1360
no ip mroute-cache
load-interval 30
delay 2000
qos pre-classify
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key 10000
!
!
!
!
interface FastEthernet0
  switchport access vlan 10
  spanning-tree portfast
!
interface FastEthernet1
  switchport access vlan 10
  spanning-tree portfast
!
interface FastEthernet2
  switchport access vlan 10
  spanning-tree portfast
!
interface FastEthernet3
  switchport access vlan 20
  spanning-tree portfast
!
! !!! GDOI is enabled via crypto map mgmt-gdoi !!!
interface FastEthernet4
  description outside interface
  ip address dhcp client-id FastEthernet4
  ip access-group fw_acl in

```

```

no ip proxy-arp
ip nat outside
ip virtual-reassembly
duplex auto
no cdp enable
crypto map mgmt-gdoi
!
interface Dot11Radio0
no ip address
!
broadcast-key vlan 10 change 30
!
!
encryption vlan 10 mode ciphers wep128
!
encryption vlan 20 key 1 size 128bit 7 <deleted> transmit-key
encryption vlan 20 mode ciphers wep128
!
ssid home
    vlan 20
    authentication open
!
ssid wifi
    vlan 10
    authentication open
    authentication network-eap eap_methods
    authentication key-management wpa optional
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.1
encapsulation dot1Q 10
no snmp trap link-status
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
description Internet access
encapsulation dot1Q 20
no snmp trap link-status
bridge-group 2

```

```
bridge-group 2 subscriber-loop-control
bridge-group 2 spanning-disabled
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
!
interface Vlan1
no ip address
!
interface Vlan10
no ip address
bridge-group 1
bridge-group 1 spanning-disabled
!
interface Vlan20
no ip address
bridge-group 2
bridge-group 2 spanning-disabled
!
! !!! following configuration uses split-tunneling !!!
interface BVI1
description inside interface
ip address 10.10.10.1 255.255.255.240
ip access-group auth_proxy_inbound_acl in
ip pim sparse-dense-mode
ip nat inside
ip inspect test in
ip auth-proxy pxy
ip virtual-reassembly
ip tcp adjust-mss 1360
hold-queue 40 out
!
!
interface BVI2
ip address 192.168.2.1 255.255.255.0
ip pim sparse-dense-mode
ip nat inside
ip inspect test in
ip virtual-reassembly
!
router eigrp 1
network 1.1.1.0 0.0.0.255
network 10.10.10.0 0.0.0.15
distribute-list dmvpn_acl out
no auto-summary
no eigrp log-neighbor-changes
```

```

!
ip classless
ip route 0.0.0.0 0.0.0.0 dhcp
ip route 192.1.1.2 255.255.255.240 dhcp
ip route < DMVPN_hubs > dhcp
ip route <Corporate Internal networks > dhcp
!
ip http server
no ip http secure-server
ip http client source-interface BV11
!
ip nat inside source list nat_acl interface FastEthernet4 overload
!
!
ip access-list standard dmvpn_acl
  permit 10.10.10.0 0.0.0.15
!
ip access-list extended auth_proxy_acl
  remark --- Auth-Proxy ACL -----
  deny   < access to corporate internal networks >
  permit tcp any < Corp. Internal Networks > eq www
ip access-list extended auth_proxy_inbound_acl
  remark --- Auth-Proxy Inbound ACL -----
  permit udp any any eq domain
  permit udp any any eq netbios-ns
  permit udp any any eq netbios-dgm
  permit tcp any any eq 2000
  permit udp any any eq tftp
  permit udp any any eq 5060
  permit < Specific hosts within Corp. Network >
  deny   ip any < Corp Internal Networks >
  permit ip any any          !!! For internet access
ip access-list extended fw_acl
  remark ---- DMVPN Firewall ----
  permit esp any any
  permit gre any any
  permit udp any any eq isakmp
  permit udp any any eq 848      !!! permit udp 848 for GDOI
  permit udp any eq isakmp any
  permit udp any eq non500-isakmp any
  permit ip < access from management network >
  permit udp host x.x.x.x eq ntp any
  permit udp host x.x.x.x  eq ntp any
  permit tcp < DMVPN_HUB > any eq 22
  permit tcp < DMVPN_HUB > any eq telnet
  permit udp any any eq bootpc

```

```

permit icmp any any
deny ip any any
ip access-list extended nat_acl
deny ip any 10.32.200.0 0.0.0.255
permit ip 10.10.10.1 0.0.0.15 any
permit ip 192.168.1.0 0.0.0.255 any
ip access-list extended mgmt_acl
permit ip host 10.10.10.1 10.32.200.0 0.0.0.255
ip radius source-interface BVI1
!
radius-server local
nas 10.10.10.1 key 7 <deleted>
group radius_eap
!
user user.wlan nthash 7 <deleted>
!
control-plane
!
bridge 1 route ip
bridge 2 route ip
banner incoming ^C

```

```

C i s c o   S y s t e m s
  ||         ||
  ||         ||           Cisco Systems, Inc.
 ||||        ||||
..:|||||:..:|||||:..

```

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.

Contact admin@cisco.com for details.

^C

banner motd ^C

You have connected to \$(hostname) on \$(line).

```

C i s c o   S y s t e m s
  ||         ||
  ||         ||           Cisco Systems, Inc.
 ||||        ||||
..:|||||:..:|||||:..

```

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
You must have explicit permission to access or configure this device. All activities performed on this device are logged and violations of this policy may result in disciplinary action.

Contact admin@cisco.com for details.

^C

!

line con 0

logging synchronous

no modem enable

stopbits 1

line aux 0

line vty 0 4

logging synchronous

!

scheduler max-task-time 5000

ntp clock-period 17179055

ntp server < Corporate_NTP server >

ntp server < Corporate NTP server > source BVI1 prefer

cns trusted-server all-agents ie2100

cns trusted-server all-agents ie2100-backup

cns event ie2100 11011 source 10.10.10.1 keepalive 180 3

cns event ie2100-backup 11011 backup

cns image server http://ie2100/cns/HttpMsgDispatcher status

http://ie2100/cns/HttpMsgDispatcher

cns config notify all interval 5 old-format

cns config partial ie2100 80 source 10.10.10.1

end

APPENDIX B: VERIFICATION AND TROUBLESHOOTING

Most of the verification and debugging commands for IPsec and DMVPN are still applicable as they were previously, except for the addition of GDOI portion. For reference, listed below are GDOI command outputs in both key server and group member.

Key Server:

2811-key-server#sh crypto gdoi

Groupname	Identity	Server
dmvpn	1234	local
IPSec SA 1		
profile name = dmvpn-gdoi		
rekey life = 300		
TEK: remaining life = 41		
access-list 105 permit gre any any		
rekey life = 300		

2811-key-server#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
192.168.1.1	10.32.100.2	GDOI_IDLE	1323	0	ACTIVE

IPv6 Crypto ISAKMP SA

Group Member (Hub & Spoke):

3845-group-member-hub#sh crypto gdoi

Groupname	Identity	Server
dmvpn	1234	192.168.1.1

Other commands which are useful :

Sh crypto isakmp sa

Sh crypto ipsec sa

Sh crypto session detail

Sh ip nhrp detail

Troubleshooting commands :

Debug crypto isakmp

Debug crypto ipsec

Debug crypto gdoi

Debug crypto pki transactions

Debug crypto engine packet detail

APPENDIX C: GDOI REKEY IN DMVPN NETWORK

The goal for enabling GDOI rekey is to avoid group members re-registering with the key server upon their SA lifetime expiration. This is a continuation of GDOI in DMVPN deployment written in this guide. Please refer the topology and Figure 3 mentioned earlier in the document.

Rekey must be enabled exclusively in the GDOI key server unlike plain IPsec, where rekey happens by default using the same IKE SA. When a group member registers with the key server, the key server pushes two IKE SAs, GDOI_IDLE and GDOI_REKEY, to the group member. GDOI_IDLE is used to download initial group IPsec SAs and GDOI_REKEY is used to download new group IPsec SAs (aka rekey SA). The key server will push rekey SAs periodically based on lifetime expiration for group IPsec SAs. Also with each rekey, the SA will have a lifetime expiration and further rekeying happens based on the lifetime expiration set in the present rekey SAs. The advantages of enabling GDOI rekey is that group members do not need to re-register with the key server upon group IPsec SA lifetime expiration. New group IPsec SAs are downloaded from the key server even before the existing SA lifetime expires.

The key server should send rekey SAs to every group member within a short time to avoid any issues related to using invalid or expired group keys by any of the group members. That will cause disconnect between group members. However, individually updating all group members with rekey SAs in a fairly large network poses scalability issues and may limit the number of group members. Hence sending rekey SAs using multicast transport greatly enhances the usability and will be efficient in a large network. However, sending rekey SAs using multicast transport means the entire network between the key server and all group members must be multicast-capable. While multicast capability across the entire network may be possible within an enterprise, it cannot be possible when group members are connected via the Internet. Even for this GDOI-based DMVPN deployment, the group members are directly connected to the Internet through which they set up the mGRE tunnels. Hence, downloading rekey SAs directly from the key server cannot be achieved and the group member has to re-register again with the key server once the group IPsec SA lifetime expires.

The best way to download GDOI rekey SAs from the key server is through the mGRE tunnel itself. This is possible mainly because GDOI uses the underlying network's multicast capability for sending rekeys. However, this requires three considerations:

1. Multicast support should be enabled in the mGRE tunnel interface.
2. The mGRE tunnel interface should join the multicast IGMP group for which rekey SAs are sent.
3. The multicast source address should be reachable through the tunnel (mGRE) interface.

The first consideration is the basic requirement for enabling multicast support. The second includes manually configuring the mGRE tunnel interface to join the IGMP group. This is required so as to receive the rekey SAs for the IGMP group, otherwise rekey SAs will not be received if no interface is joining the IGMP group. This is in accordance with multicast routing. The third is required simply because the source address of the rekey SA is reachable via the physical interface through which the GDOI session is established. However, multicast routing does a Reverse Path Forwarding (RPF) check for the source address of each multicast packet against the interface it received. If the source address is reachable through the physical interface and the multicast packet is received through the mGRE tunnel interface, the packet will be dropped due to RPF check failure. This is not only applicable to the source address of the multicast packet, but also to the rendezvous point (RP) if Protocol Independent Multicast (PIM) sparse mode is used. Hence, it is required to specify a static multicast route to reach both source address and rendezvous point, if required, through the mGRE tunnel interface. This will make sure the source address is reachable through the mGRE tunnel interface.

Rekey is enabled in the key server by way of specifying the multicast IGMP group address to which rekey SAs are sent, as well as the RSA authentication key and other information, such as retransmit interval and rekey lifetime expiration. Once rekey is enabled in the key server, group members download the multicast IGMP group information along with downloading group IPsec SAs during the registration process. Currently, GDOI can enable the interface, in which the crypto map is enabled, for joining the multicast IGMP group upon GDOI session establishment. The assumption is that the interface has PIM enabled for multicast capability, but this is not enough to receive rekey SAs as there is no PIM enabled in the interface. Also, when multicast rekey SAs are received through the mGRE tunnel interface, there will not be any outgoing interface associated in the multicast routing table for this IGMP group. Either PIM should be enabled in the physical interface

or the mGRE tunnel interface should be joined manually for the IGMP group. For the risks involved in enabling PIM on the physical interface where it is connected to the Internet, it is considered safe to enable the IGMP join-group in the mGRE tunnel interface manually. There can be an enhancement to specify the required interface for joining the multicast IGMP group later.

These considerations are explained for a DMVPN using GDOI setup and can work well if both the DMVPN hub and key server are located in the same location and have direct connection between each other. Hence, multicast rekey packets can be forwarded from the key server to the DMVPN hub and then replicated through mGRE tunnel interfaces. This would be even more efficient if the DMVPN hub could also be the key server, but the present code does not support this combination.

In summary, here are the steps taken to enable GDOI rekey in this deployment:

- Define rekey SA in the key server; includes RSA key for authentication, rekey multicast address using ACL, and rekey lifetime.
- Enable multicast routing in the key server and all group members.
- Enable PIM sparse-dense-mode in the data path between the key server and group members, including mGRE interfaces.
- Enable IGMP join-group in mGRE interfaces only on group members configured for spokes; this group should match the rekey multicast address configured in the key server.
- Define static mroute for multicast source and rendezvous point (RP) via the mGRE interface in the group members configured for spokes.

Let's take a look at the following configurations from the key server and group member. For ease of understanding, only the relevant configurations are included.

Key Server Configuration

```
ip multicast-routing    // Multicast support is enabled in Router //
!
crypto gdoi group dmvpn
  identity number 1234
  server local
    rekey address ipv4 103    // multicast address specified to which Rekey SAs sent //
    rekey lifetime seconds 300 // configurable lifetime value for Rekey SAs //
    rekey retransmit 10 number 2 // configurable retransmit parameters //
    rekey authentication mypubkey rsa gdoirekey // Rekey authentication RSA key //
  sa ipsec 1
    profile dmvpn-gdoi
    match address ipv4 105
  !
interface Loopback0
  ip address 192.168.1.1 255.255.255.255
  ip pim sparse-dense-mode    // Multicast PIM enabled in Source interface //
!
interface FastEthernet0/0
  ip address 10.1.1.1 255.255.255.240
  ip pim sparse-dense-mode    // Multicast PIM enabled in physical interface //
!
// The following access-list 103 defines the multicast group address to which Rekey SAs
are sent //
access-list 103 permit udp host 192.168.1.1 eq 848 host 229.1.1.1 eq 848
```

```
access-list 105 permit gre any any
```

Group Member Configuration on DMVPN Hub

```
ip multicast-routing // Multicast support is enabled in Router //
!
interface Tunnel100
ip pim dr-priority 10 // PIM dr-priority to elect Hub as DR always //
ip pim nbma-mode // Nbma-mode is defined due to mGRE //
ip pim sparse-mode // Multicast PIM enabled in mGRE Tunnel interface //
!
interface GigabitEthernet0/0
ip pim sparse-dense-mode // Multicast PIM enabled in physical interface //
```

Group Member Configuration on DMVPN Spoke

```
ip multicast-routing // Multicast support is enabled in Router //
!
interface Tunnel10
ip pim sparse-dense-mode // Multicast PIM enabled in mGRE Tunnel interface //
ip igmp join-group 229.1.1.1 // Multicast IGMP group joined for Rekey address //
!
interface FastEthernet4
crypto map mgmt-gdoi // physical interface to setup GDOI session //
!
// The following multicast static route will override RPF check failure for the source
address //
ip mroute 192.168.1.1 255.255.255.255 1.1.1.1
```

Rekey Verification

```
3845-group-member-hub #sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
229.1.1.1    192.168.1.1    GDOI_REKEY     12335    0  ACTIVE
```

```
IPv6 Crypto ISAKMP SA
```

```
3845-group-member-hub #
3845-group-member-hub #sh crypto gdoi
Group Information
  Group Name           : dmvpn
  Group Identity       : 1234
  Group Members Registered : 0
  Group Server         : 192.168.1.1
```

```
3845-group-member-hub #
```

```
871-group-member-spoke#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	slot	status
229.1.1.1	192.168.1.1	GDOI_REKEY	2128	0	ACTIVE
192.168.1.10	24.1.2.4	QM_IDLE	2107	0	ACTIVE

IPv6 Crypto ISAKMP SA

871-group-member-spoke#

871-group-member-spoke #sh crypto gdoi

Group Information

Group Name	: dmvpn
Group Identity	: 1234
Group Members Registered	: 0
Group Server	: 192.168.1.1

871-group-member-spoke #



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Printed in USA

C07-353406-00 06/06