GETVPN

OVER

DMVPN

Topology Details –

- HOME-SYD-RTR02 is GETVPN KS.
- R2 & R3 are GETVPN Members.
- R2 is DMVPN Hub.
- R3 is DMVPN Spoke.
- HOME-PIX01 is Firewall between R2 and R3.

IP Addressing Details –

- HOME-SYD-RTR01 is on 10.249.1.5.
- R2 is 10.249.200.1/24 & 192.168.200.1/24.
- R3 is 10.249.10.1/24 & 192.168.170.1/24
- HOME-PIX01 is 10.249.1.6/24 & 10.249.10.6/24.

HOME-SYD-RTR02 GETVPN Configuration –

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 20
 encr 3des
 group 5
!
crypto isakmp policy 40
 encr 3des
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set GETVPN esp-3des esp-sha-hmac
!
crypto ipsec profile GETVPN
 set security-association lifetime seconds 86400
 set transform-set GETVPN
!
crypto gdoi group GETVPN
 identity number 1
 server local
  rekey address ipv4 102
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa MYKEYSR1
  sa ipsec 1
   profile GETVPN
   match address ipv4 101
   replay counter window-size 64
  address ipv4 10.249.1.5
  redundancy
   local priority 100
   peer address ipv4 10.249.1.51
```

```
!
access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 101 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 101 permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 101 permit ip 172.18.0.0 0.0.255.255 172.18.0.0 0.0.255.255
access-list 101 permit gre any any
access-list 102 permit udp host 10.249.1.5 eq 848 host 239.0.1.2 eq 848
```

R2 GETVPN Configuration –

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 20
 encr 3des
 hash md5
 group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set GETVPN esp-3des esp-sha-hmac
 mode transport
!
crypto gdoi group GETVPN
 identity number 1
 server address ipv4 10.249.1.5
!
!
crypto map GETVPN 10 gdoi
 set group GETVPN
!
interface Vlan200
 ip address 10.249.200.1 255.255.255.0
 no autostate
 crypto map GETVPN
!
```

R3 GETVPN Configuration –

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 20
 encr 3des
 hash md5
 group 2
```

```
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!

crypto ipsec transform-set GETVPN esp-3des esp-sha-hmac
 mode transport
!

crypto gdoi group GETVPN
 identity number 1
 server address ipv4 10.249.1.5
!
!
crypto map GETVPN 10 gdoi
 set group GETVPN
!

interface GigabitEthernet0/0
 ip address 10.249.10.1 255.255.255.0
 duplex auto
 speed auto
 crypto map GETVPN
 !
```

R2 DMVPN Configuration –

```
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 10.249.10.1 255.255.255.255
!
!
crypto ipsec transform-set GETVPN esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN
 set security-association lifetime seconds 86400
 set transform-set GETVPN
 set isakmp-profile DMVPN
!
!
interface Tunnel0
 ip address 172.18.0.1 255.255.255.0
 no ip redirects
 ip mtu 1436
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1234
 tunnel source Vlan200
 tunnel mode gre multipoint
!
router eigrp 100
 network 172.18.0.0 0.0.0.255
```

```
 network 192.168.200.0
!
```

R3 DMVPN Configuration –

```
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 10.249.200.1 255.255.255.255
!
crypto ipsec profile DMVPN
 set security-association lifetime seconds 86400
 set transform-set GETVPN
 set isakmp-profile DMVPN
!
interface Tunnel0
 ip address 172.18.0.2 255.255.255.0
 no ip redirects
 ip mtu 1436
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map multicast 10.249.200.1
 ip nhrp map 172.18.0.1 10.249.200.1
 ip nhrp network-id 1234
 ip nhrp nhs 172.18.0.1
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 !
router eigrp 100
 network 172.18.0.0 0.0.0.255
 network 192.168.170.0
!
```

HOME-PIX01 Configuration –

```
interface Ethernet0
 description "Connected to Inside"
 nameif Inside
 security-level 100
 ip address 10.249.1.6 255.255.255.0
!
interface Ethernet1
 description "Connected to Outside"
 nameif Outside
 security-level 0
 ip address 10.249.10.6 255.255.255.0
!
access-list NONAT extended permit ip 10.249.1.0 255.255.255.0 10.249.10.0 255.255.255.0
access-list NONAT extended permit ip 10.249.200.0 255.255.255.0 10.249.10.0 255.255.255.0
```

```
access-list PERMITOUTSIDE extended permit icmp any any
access-list PERMITOUTSIDE extended permit tcp any eq 848 host 10.249.1.5 eq 848
access-list PERMITOUTSIDE extended permit tcp any eq 848 host 239.0.1.2 eq 848
access-list PERMITOUTSIDE extended permit esp any any
access-list PERMITOUTSIDE extended permit ah any any
access-list PERMITOUTSIDE extended permit udp any eq 848 host 239.0.1.2 eq 848
access-list PERMITOUTSIDE extended permit udp any eq 848 host 10.249.1.5 eq 848
access-list PERMITOUTSIDE extended permit udp any any eq isakmp
access-list PERMITOUTSIDE extended permit gre any any
!
nat (Inside) 0 access-list NONAT
access-group PERMITOUTSIDE in interface Outside
route Inside 0.0.0.0 0.0.0.0 10.249.1.4 1
route Inside 10.249.0.0 255.255.0.0 10.249.1.4 1
route Outside 192.168.170.0 255.255.255.0 10.249.10.1 1
!
```

Commands to verify –

```
HOME-SYD-RTR02#show crypto gdoi ks
Total group members registered to this box: 3

Key Server Information For Group GETVPN:
   Group Name             : GETVPN
   Group Identity         : 1
   Group Members          : 3
   IPSec SA Direction     : Both
   ACL Configured:
      access-list 101
   Redundancy             : Configured
      Local Address       : 10.249.1.5
      Local Priority      : 100
      Local KS Status     : Alive
      Local KS Role       : Primary


HOME-SYD-RTR02#show cry
HOME-SYD-RTR02#show crypto gdoi
HOME-SYD-RTR02#show crypto gdoi ks mem
HOME-SYD-RTR02#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group GETVPN : 0

Group Member ID    : 10.249.10.1
 Group ID          : 1
 Group Name        : GETVPN
 Key Server ID     : 10.249.1.5

Group Member ID    : 10.249.100.1
```

```
 Group ID         : 1
 Group Name       : GETVPN
 Key Server ID    : 10.249.1.5

Group Member ID    : 10.249.200.1
 Group ID         : 1
 Group Name       : GETVPN
 Key Server ID    : 10.249.1.5

R2#show crypto gdoi
GROUP INFORMATION

    Group Name              : GETVPN
    Group Identity          : 1
    Crypto Path             : ipv4
    Key Management Path     : ipv4
    Rekeys received         : 0
    IPSec SA Direction      : Both

     Group Server list      : 10.249.1.5

    Group member            : 10.249.200.1     vrf: None
      Version               : 1.0.6
      Registration status   : Registered
      Registered with       : 10.249.1.5
      Re-registers in       : 42234 sec
      Succeeded registration: 1
      Attempted registration: 1
      Last rekey from       : 0.0.0.0
      Last rekey seq num    : 0
      Multicast rekey rcvd  : 0
      allowable rekey cipher: any
      allowable rekey hash  : any
      allowable transformtag: any ESP

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

 ACL Downloaded From KS 10.249.1.5:
   access-list   permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
   access-list   permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
   access-list   permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
   access-list   permit ip 172.18.0.0 0.0.255.255 172.18.0.0 0.0.255.255
   access-list   permit gre any any

KEK POLICY:
    Rekey Transport Type     : Multicast
    Lifetime (secs)          : 43761
    Encrypt Algorithm        : 3DES
```

```
   Key Size               : 192
   Sig Hash Algorithm       : HMAC_AUTH_SHA
   Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Vlan200:
   IPsec SA:
      spi: 0xF8FDAA75(4177373813)
      transform: esp-3des esp-sha-hmac
      sa timing:remaining key lifetime (sec): (43763)
      Anti-Replay(Counter Based) : 64
      tag method : disabled
      alg key size: 24 (bytes)
      sig key size: 20 (bytes)
      encaps: ENCAPS_TUNNEL

R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
239.0.1.2       10.249.1.5      GDOI_REKEY       1002 ACTIVE
10.249.1.5      10.249.200.1    GDOI_IDLE        1001 ACTIVE

IPv6 Crypto ISAKMP SA

R2#show crypto ipsec sa

interface: Vlan200
   Crypto map tag: GETVPN, local addr 10.249.200.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/47/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/47/0)
  Group: GETVPN
  current_peer 0.0.0.0 port 848
    PERMIT, flags={}
   #pkts encaps: 374, #pkts encrypt: 374, #pkts digest: 374
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

   R2#ping 192.168.170.1 source 192.168.200.1 repeat 500
   Type escape sequence to abort.
   Sending 500, 100-byte ICMP Echos to 192.168.170.1, timeout is 2 seconds:
   Packet sent with a source address of 192.168.200.1
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 1/1/12 ms

R2#show crypto ipsec sa
protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
  Group: GETVPN
  current_peer 0.0.0.0 port 848
    PERMIT, flags={}
   #pkts encaps: 500, #pkts encrypt: 500, #pkts digest: 500
   #pkts decaps: 500, #pkts decrypt: 500, #pkts verify: 500
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 10.249.200.1, remote crypto endpt.: 0.0.0.0
    plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Vlan200
    current outbound spi: 0xF8FDAA75(4177373813)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xF8FDAA75(4177373813)
       transform: esp-3des esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: GETVPN
       sa timing: remaining key lifetime 12 hours, 8 mins
       Kilobyte Volume Rekey has been disabled
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)

R3#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
      N - NATed, L - Local, X - No Socket
      # Ent --> Number of NHRP entries with same NBMA peer
      NHS Status: E --> Expecting Replies, R --> Responding
      UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
   1    10.249.200.1      172.18.0.1    UP 00:20:39     S

R3#show crypto gdoi
```

GROUP INFORMATION

Group Name : GETVPN
Group Identity : 1
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.249.1.5

Group member : 10.249.10.1 vrf: None
Registration status : Registered
Registered with : 10.249.1.5
Re-registers in : 42047 sec
Succeeded registration: 1
Attempted registration: 2
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Multicast rekey rcvd : 0

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

ACL Downloaded From KS 10.249.1.5:
access-list permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list permit ip 172.18.0.0 0.0.255.255 172.18.0.0 0.0.255.255
access-list permit gre any any

KEK POLICY:
Rekey Transport Type : Multicast
Lifetime (secs) : 45051
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
GigabitEthernet0/0:
IPsec SA:
spi: 0xF8FDAA75(4177373813)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (43613)
Anti-Replay : Disabled