DESIGN GUIDE

USING FVRF AND IVRF IN DMVPN

1. OVERVIEW

This document provides configuration guidance for users of Cisco® Dynamic Multipoint VPN (DMVPN) technology on Cisco IOS® IPSec routers. The Cisco 7600 Series platform is an exception because it does not support FVRF. The IVRF configuration described below shall work on the Cisco 7600 Series and the Cisco Catalyst® 6500 Series as well. The testing was performed on Cisco 1841 integrated services routers running Cisco IOS Software Releasae 12.3(11)T3. The objective of the testing was to configure and test interaction of DMVPN with Front VRF (FVRF) as well as internal VRF (IVRF).

Advantage: The advantage of using an FVRF is primarily to carve out a separate routing table from the global routing table (where tunnel interface exists). The advantage of using an IVRF is to define a private space to hold the DMVPN and private network information. Both these configurations provide extra security from anyone trying to attack the router from the Internet by separating out routing information. These VRF configurations can be used on both DMVPN hub and spoke.

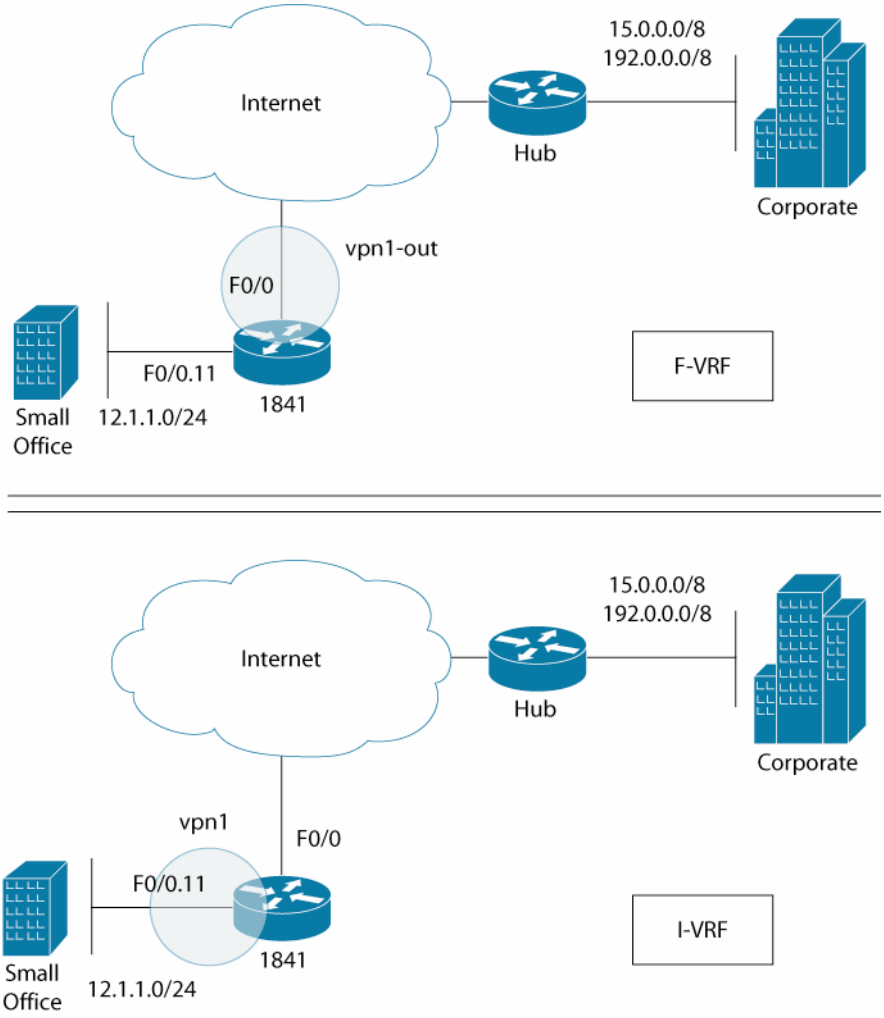
What is the configuration difference? In case of FVRF, the tunnel destination lookup needs to be done in FVRF. Secondly, since the Internet-facing interface is in a VRF, the ISAKMP key lookup is also done in the VRF. As for using IVRF, the tunnel, private subnets, and routing protocol need to be defined in the IVRF space. The tunnel destination and ISAKMP key are looked up in global space for this scenario.

2. AUDIENCE

This configuration guide is targeted for Cisco systems engineers and customer support engineers to provide configuration guidelines and best practices for large-scale DMVPN customer deployments.

3. NETWORK TOPOLOGY

Figure 1. DMVPN VRF Topology



4. SYSTEM COMPONENTS USED IN THE TEST

4.1 1841 Hardware

- 1841 chassis
- AIM-VPN/BPII PLUS

4.2 1841 Software

- Release: 12.3(11)T3

5. FVRF CONFIGURATION

5.1 VRF Configuration

```
ip vrf vpn1-out

 rd 100:1

!
```

5.2 IPSec Configuration

5.2.1 ISAKMP Policy

```
crypto isakmp policy 10

 encr 3des

 authentication pre-share

 group 2

 lifetime 14400

!
```

5.2.2 ISAKMP Keepalive (DPD)

```
crypto isakmp keepalive 60

!
```

5.2.3 IPSec Transform Set

```
crypto ipsec transform-set gre_set esp-3des esp-sha-hmac

 mode transport

!
```

5.2.4 ISAKMP Keyrings

```
! Since the interface on which IPSec encrypted traffic will be sent and received in

! a VRF, we need to define a keyring in that VRF



crypto keyring vpn1 vrf vpn1-out

  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

!
```

5.3 DMVPN Tunnel Configuration

```
!

! Tunnel VRF command actually forces the tunnel destination lookup to be done in the

! vrf vpn1-out.

!
```

```
interface Tunnel1
 bandwidth 128
 ip address 172.20.112.1 255.255.0.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication nsite
 ip nhrp map multicast 124.1.1.1
 ip nhrp map 172.20.1.254 124.1.1.1
 ip nhrp network-id 101
 ip nhrp holdtime 900
 ip nhrp nhs 172.20.1.254
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf vpn1-out
 tunnel protection ipsec profile gre_prof
!
```

5.4 Outbound Interface Configuration

```
interface FastEthernet0/0
 description TO GW FOR PUBLIC IP
 ip vrf forwarding vpn1-out
 ip address 112.1.1.1 255.255.255.0
 load-interval 30
 speed 100
 full-duplex
!
```

5.5 Routing Protocol Configuration

```
!
! OSPF running in between 1841 and the gateway
!
router ospf 254 vrf vpn1-out
 log-adjacency-changes
```

```
 network 112.1.1.0 0.0.0.255 area 0
!
! EIGRP is running over the tunnel
!
router eigrp 10
 passive-interface FastEthernet0/1.11
 network 12.1.1.0 0.0.0.255
 network 172.20.0.0
 no auto-summary
!
```

6. FVRF CONFIGURATION VERIFICATION

6.1 Routing Tables

1841# sh ip route vrf vpn1-out

```
Routing Table: vpn1-out
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/30 is subnetted, 1 subnets
O       1.1.1.0 [110/2] via 112.1.1.2, 00:59:20, FastEthernet0/0
     100.0.0.0/24 is subnetted, 1 subnets
O E2    100.1.1.0 [110/20] via 112.1.1.2, 00:59:20, FastEthernet0/0
     112.0.0.0/24 is subnetted, 4 subnets
C       112.1.1.0 is directly connected, FastEthernet0/0
O       112.3.1.0 [110/2] via 112.1.1.2, 00:59:20, FastEthernet0/0
```

```
O       112.2.1.0 [110/2] via 112.1.1.2, 00:59:20, FastEthernet0/0
O       112.4.1.0 [110/12] via 112.1.1.2, 00:59:20, FastEthernet0/0
     111.0.0.0/24 is subnetted, 3 subnets
O       111.4.1.0 [110/12] via 112.1.1.2, 00:59:20, FastEthernet0/0
O       111.2.1.0 [110/3] via 112.1.1.2, 00:59:28, FastEthernet0/0
O       111.1.1.0 [110/3] via 112.1.1.2, 00:59:28, FastEthernet0/0
     125.0.0.0/24 is subnetted, 2 subnets
O       125.10.1.0 [110/2] via 112.1.1.2, 00:59:28, FastEthernet0/0
O       125.4.1.0 [110/2] via 112.1.1.2, 00:59:29, FastEthernet0/0
```

1841#sh ip route

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

Gateway of last resort is not set

     23.0.0.0/24 is subnetted, 1 subnets
S       23.1.1.0 [1/0] via 24.1.1.100
C    172.20.0.0/16 is directly connected, Tunnel1
     24.0.0.0/24 is subnetted, 1 subnets
C       24.1.1.0 is directly connected, FastEthernet0/1.24
     12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, FastEthernet0/1.11
D    15.0.0.0/8 [90/45602560] via 172.20.1.254, 01:00:21, Tunnel1
D    192.0.0.0/8 [90/32802560] via 172.20.1.254, 01:00:21, Tunnel1
```

6.2 IKE and IPSec SAs

1841#sh crypto isakmp sa

```
dst             src             state          conn-id slot status
124.1.1.1       112.1.1.1       QM_IDLE              1    0 ACTIVE
```

1841#sh cry isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
1     112.1.1.1       124.1.1.1       vpn1-out ACTIVE 3des sha  psk  2  02:57:28 D
       Connection-id:Engine-id =  1:2(hardware)
```

1841#sh cry ipsec sa

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 112.1.1.1

   protected vrf: vpn1-out
   local  ident (addr/mask/prot/port): (112.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (124.1.1.1/255.255.255.255/47/0)
   current_peer 124.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 828, #pkts encrypt: 828, #pkts digest: 828
    #pkts decaps: 826, #pkts decrypt: 826, #pkts verify: 826
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

 local crypto endpt.: 112.1.1.1, remote crypto endpt.: 124.1.1.1
 path mtu 1500, ip mtu 1500
 current outbound spi: 0x95E8732E(2515039022)

 inbound esp sas:
  spi: 0xACA16F64(2896260964)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: AIM-VPN/BPII-PL, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4398156/3306)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

 inbound ah sas:

 inbound pcp sas:

 outbound esp sas:
  spi: 0x95E8732E(2515039022)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: AIM-VPN/BPII-PL, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4398156/3305)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
outbound ah sas:

outbound pcp sas:
```

6.3 Encryption Module

```
1841#sh cry eng conf

   crypto engine name:  Virtual Private Network (VPN) Module
   crypto engine type:  hardware
               State:  Enabled
   VPN Module in slot:  0
         Product Name:  AIM-VPN/BPII-PLUS
    Software Serial #:  55AA
            Device ID:  001E - revision 0000
            Vendor ID:  13A3
          Revision No:  0x001E0000
         VSK revision:  0
         Boot version:  255
          DPU version:  0
          HSP version:  2.3(1) (PRODUCTION PATCH)
         Time running:  00:00:00
          Compression:  Yes
                  DES:  Yes
               3 DES:  Yes
             AES CBC:  Yes (128,192,256)
            AES CNTR:  No
Maximum buffer length:  4096
     Maximum DH index:  1000
     Maximum SA index:  1000
```

```
        Maximum Flow index:  2000
      Maximum RSA key size:  2048
```

7. IVRF CONFIGURATION

7.1 VRF Configuration

```
ip vrf vpn1
 rd 100:1
!
```

7.2 IPSec Configuration

7.2.1 ISAKMP Policy

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400
!
```

7.2.2 ISAKMP Keepalive (DPD)

```
crypto isakmp keepalive 60
!
```

7.2.3 IPSec Transform Set

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

7.2.4 ISAKMP Keyrings

```
! Since the interface on which IPSec-encrypted traffic will be sent and received is
! global, we do NOT need to define a keyring in the VRF.


crypto keyring vpn1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
```

7.3 DMVPN Tunnel Configuration

```
!
! IP VRF forwarding command actually puts the decapsulated traffic in the tunnel
!
interface Tunnel1
 bandwidth 128
 ip vrf forwarding vpn1
 ip address 172.20.112.1 255.255.0.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication nsite
 ip nhrp map multicast 124.1.1.1
 ip nhrp map 172.20.1.254 124.1.1.1
 ip nhrp network-id 101
 ip nhrp holdtime 900
 ip nhrp nhs 172.20.1.254
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile gre_prof
!
```

7.4 Inside Interface Configuration

```
interface FastEthernet0/1.11
 description traffic interface
 encapsulation dot1Q 11
 ip vrf forwarding vpn1
 ip address 12.1.1.1 255.255.255.0!
```

7.5 Routing Protocol Configuration

```
!
! OSPF running in between 1841 and the gateway
!
router ospf 10
```

```
 log-adjacency-changes
 network 112.1.1.0 0.0.0.255 area 0
!
! EIGRP is running over the tunnel in a VRF
!
router eigrp 10
 auto-summary
 !
 address-family ipv4 vrf vpn1
 network 12.1.1.0 0.0.0.255
 network 172.20.0.0
 no auto-summary
 autonomous-system 10
 exit-address-family
!
```

8. IVRF CONFIGURATION VERIFICATION

8.1 Routing Tables

1841# sh ip route vrf vpn1

```
Routing Table: vpn1
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

```
C    172.20.0.0/16 is directly connected, Tunnel1
     12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, FastEthernet0/1.11
D    15.0.0.0/8 [90/45602560] via 172.20.1.254, 00:06:18, Tunnel1
D    192.0.0.0/8 [90/32802560] via 172.20.1.254, 00:06:18, Tunnel1

1841#sh ip route

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

Gateway of last resort is not set

     1.0.0.0/30 is subnetted, 1 subnets
O       1.1.1.0 [110/2] via 112.1.1.2, 00:08:38, FastEthernet0/0
     100.0.0.0/24 is subnetted, 1 subnets
O E2    100.1.1.0 [110/20] via 112.1.1.2, 00:08:38, FastEthernet0/0
     23.0.0.0/24 is subnetted, 1 subnets
S       23.1.1.0 [1/0] via 24.1.1.100
     112.0.0.0/24 is subnetted, 4 subnets
C       112.1.1.0 is directly connected, FastEthernet0/0
O       112.3.1.0 [110/2] via 112.1.1.2, 00:08:38, FastEthernet0/0
O       112.2.1.0 [110/2] via 112.1.1.2, 00:08:38, FastEthernet0/0
O       112.4.1.0 [110/12] via 112.1.1.2, 00:08:38, FastEthernet0/0
     24.0.0.0/24 is subnetted, 1 subnets
C       24.1.1.0 is directly connected, FastEthernet0/1.24
     111.0.0.0/24 is subnetted, 3 subnets
```

```
O       111.4.1.0 [110/12] via 112.1.1.2, 00:08:40, FastEthernet0/0
O       111.2.1.0 [110/3] via 112.1.1.2, 00:08:40, FastEthernet0/0
O       111.1.1.0 [110/3] via 112.1.1.2, 00:08:40, FastEthernet0/0
     125.0.0.0/24 is subnetted, 2 subnets
O       125.10.1.0 [110/2] via 112.1.1.2, 00:08:40, FastEthernet0/0
O       125.4.1.0 [110/2] via 112.1.1.2, 00:08:40, FastEthernet0/0
     124.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O E2    124.8.0.0/16 [110/100] via 112.1.1.2, 00:08:40, FastEthernet0/0
O       124.11.1.0/24 [110/3] via 112.1.1.2, 00:08:40, FastEthernet0/0
O E2    124.6.0.0/16 [110/100] via 112.1.1.2, 00:08:40, FastEthernet0/0
O E2    124.7.0.0/16 [110/100] via 112.1.1.2, 00:08:40, FastEthernet0/0
```

8.2 IKE and IPSec SAs

1841#sh crypto isakmp sa

```
dst             src             state          conn-id slot status
124.1.1.1       112.1.1.1       QM_IDLE              2    0 ACTIVE
```

1841#sh cry isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
2     112.1.1.1       124.1.1.1               ACTIVE 3des sha  psk  2  03:50:40 D
       Connection-id:Engine-id =  2:2(hardware)
```

1841#sh cry ipsec sa

```
interface: Tunnel1
```

```
 Crypto map tag: Tunnel1-head-0, local addr 112.1.1.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (112.1.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (124.1.1.1/255.255.255.255/47/0)
current_peer 124.1.1.1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 137, #pkts encrypt: 137, #pkts digest: 137
 #pkts decaps: 153, #pkts decrypt: 153, #pkts verify: 153
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0

  local crypto endpt.: 112.1.1.1, remote crypto endpt.: 124.1.1.1
  path mtu 1500, ip mtu 1500
  current outbound spi: 0x586839F4(1483225588)

  inbound esp sas:
   spi: 0x7427980B(1948751883)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Transport, }
     conn id: 2004, flow_id: AIM-VPN/BPII-PL, crypto map: Tunnel1-head-0
     sa timing: remaining key lifetime (k/sec): (4448783/3005)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:
```

```
outbound esp sas:
 spi: 0x586839F4(1483225588)
   transform: esp-3des esp-sha-hmac ,
   in use settings ={Transport, }
   conn id: 2003, flow_id: AIM-VPN/BPII-PL, crypto map: Tunnel1-head-0
   sa timing: remaining key lifetime (k/sec): (4448784/3004)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

8.3 Encryption Module

1841#sh cry eng conf

```
   crypto engine name:  Virtual Private Network (VPN) Module
   crypto engine type:  hardware
                State:  Enabled
   VPN Module in slot:  0
         Product Name:  AIM-VPN/BPII-PLUS
    Software Serial #:  55AA
            Device ID:  001E - revision 0000
            Vendor ID:  13A3
           Revision No:  0x001E0000
         VSK revision:  0
         Boot version:  255
          DPU version:  0
          HSP version:  2.3(1) (PRODUCTION PATCH)
         Time running:  00:00:00
          Compression:  Yes
                  DES:  Yes
```

```
                  3 DES:  Yes
                AES CBC:  Yes (128,192,256)
               AES CNTR:  No
     Maximum buffer length:  4096
          Maximum DH index:  1000
          Maximum SA index:  1000
        Maximum Flow index:  2000
      Maximum RSA key size:  2048
```

9. LIMITATIONS/CAVEATS/INTEGRATION ISSUES/GUIDELINES

There is a known DDTS at the time of writing this configuration guide in Cisco IOS Software Release 12.3(14)T3, where configuring FVRF will cause tracebacks. The issue is not seen in Release 12.3(11)T3. The DDTS ID is: CSCei63568.

10. RELATED DOCUMENTS

Cisco.com documentation: http://www.cisco.com/warp/public/732/Tech/security/ipsec/dmvpn/

11. APPENDIX A

11.1 FVRF Configuration

```
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 1841
!
boot-start-marker
boot system flash:c1841-advipservicesk9-mz.123-11.T3
boot-end-marker
!
enable password lab
!
clock timezone EST -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
```

```
ip cef
!
ip vrf vpn1-out
 rd 100:1
!
no ip domain lookup
!
crypto keyring vpn1 vrf vpn1-out
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400
crypto isakmp keepalive 60
!
!
crypto ipsec transform-set gre_set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile gre_prof
 set transform-set gre_set
!
interface Tunnel1
 bandwidth 128
 ip address 172.20.112.1 255.255.0.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication nsite
 ip nhrp map multicast 124.1.1.1
 ip nhrp map 172.20.1.254 124.1.1.1
```

```
 ip nhrp network-id 101
 ip nhrp holdtime 900
 ip nhrp nhs 172.20.1.254
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf vpn1-out
 tunnel protection ipsec profile gre_prof
!
interface FastEthernet0/0
 description TO DMVPNGW FOR PUBLIC IP
 ip vrf forwarding vpn1-out
 ip address 112.1.1.1 255.255.255.0
 load-interval 30
 speed 100
 full-duplex
!
interface FastEthernet0/1
 description Private Interface
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1.11
 description traffic interface
 encapsulation dot1Q 11
 ip address 12.1.1.1 255.255.255.0
!
interface FastEthernet0/1.24
 description mgmt net
 encapsulation dot1Q 24
```

```
 ip address 24.1.1.161 255.255.255.0
!
router eigrp 10
 passive-interface FastEthernet0/1.11
 network 12.1.1.0 0.0.0.255
 network 172.20.0.0
 no auto-summary
!
router ospf 254 vrf vpn1-out
 log-adjacency-changes
 network 112.1.1.0 0.0.0.255 area 0
!
ip classless
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
end
```

12. APPENDIX B

12.1 IVRF Configuration

```
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 1841
!
enable password lab
!
clock timezone EST -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
ip cef
!
ip vrf vpn1
 rd 100:1
!
no ip domain lookup
!
crypto keyring vpn1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400
crypto isakmp keepalive 60
!
```

```
crypto ipsec transform-set gre_set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile gre_prof
 set transform-set gre_set
!
interface Tunnel1
 bandwidth 128
 ip vrf forwarding vpn1
 ip address 172.20.112.1 255.255.0.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication nsite
 ip nhrp map multicast 124.1.1.1
 ip nhrp map 172.20.1.254 124.1.1.1
 ip nhrp network-id 101
 ip nhrp holdtime 900
 ip nhrp nhs 172.20.1.254
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile gre_prof
!
interface FastEthernet0/0
 description TO DMVPN-GSR2 FAS 2/1 FOR PUBLIC IP
 ip address 112.1.1.1 255.255.255.0
 load-interval 30
 speed 100
 full-duplex
!
interface FastEthernet0/1
 description dmvpn interface
```

```
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1.11
 description traffic interface
 encapsulation dot1Q 11
 ip vrf forwarding vpn1
 ip address 12.1.1.1 255.255.255.0
!
interface FastEthernet0/1.24
 description mgmt net
 encapsulation dot1Q 24
 ip address 24.1.1.161 255.255.255.0
!
router eigrp 10
 auto-summary
 !
 address-family ipv4 vrf vpn1
 network 12.1.1.0 0.0.0.255
 network 172.20.0.0
 no auto-summary
 autonomous-system 10
 exit-address-family
!
router ospf 10
 log-adjacency-changes
 network 112.1.1.0 0.0.0.255 area 0
!
ip classless
!
```

```
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password lab
 login
end
```


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 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

205233.BH_ETMG_KS_10.05

Printed in the USA