VRF-lite Based Group Encrypted Transport VPN

Introduction

Virtual Private Networks (VPNs) provide a highly secure way for customers to share bandwidth over an ISP backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table. A VPN routing table is called a VPN routing/forwarding (VRF) table. VRFs are generally associated with MPLS based VPNs.

With the VRF-lite feature, multiple VPN routing/forwarding instances can be supported in customer edge devices. VRF-lite extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office. This also helps the customer to share the same CE for various internal departments while maintaining separate VRF table for each department.

Now, the intention of this document is to enable Cisco IOS GET VPN on the CE's VRF-lite interfaces. Cisco IOS GET VPN is well documented at http://www.cisco.com/go/getvpn.

Document Scope

This document provides deployment guidelines to enable Cisco IOS GET VPN on the VRF-lite interfaces for an enterprise network. This document does not cover in-depth technical details about various features comprising Cisco IOS GET VPN. Please refer to the References section for more details.

Recommended Platforms and Images

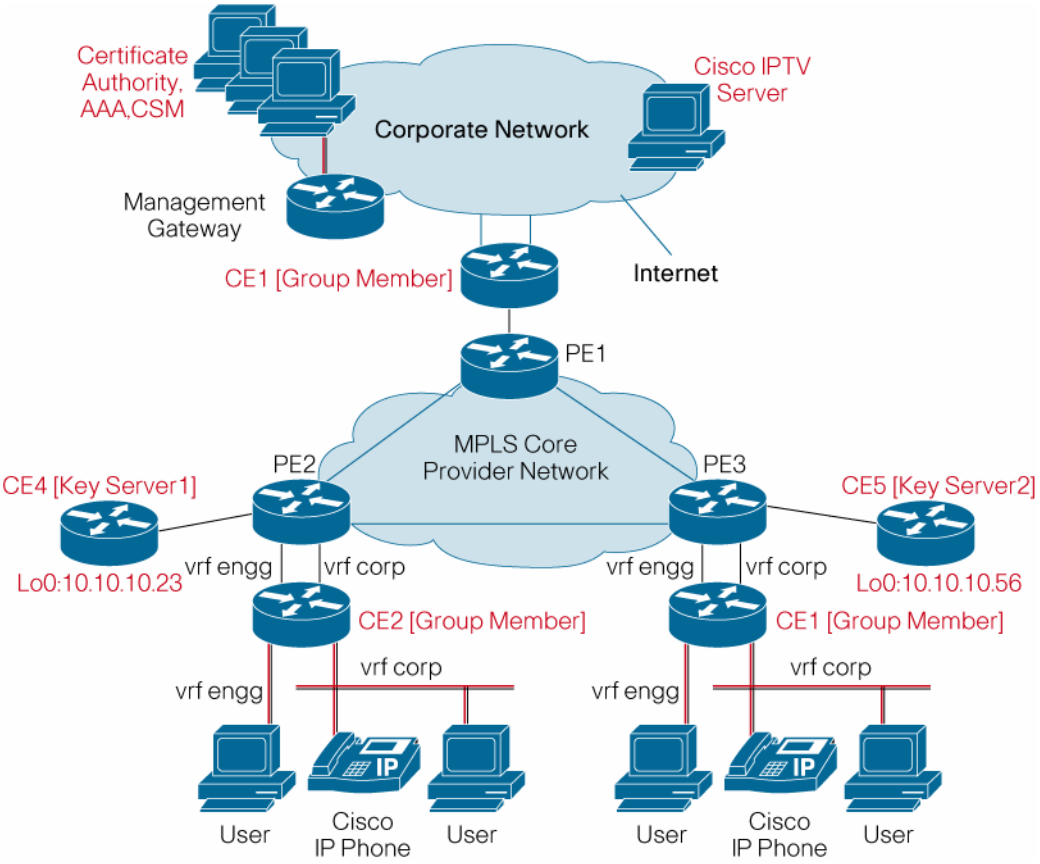
Images based on Cisco IOS Software Release 12.4(11)T2 are recommended for both key server and group member routers. The recommended image subset is 'adventerprisek9' for both the key server and the group member routers.

Key server: Cisco 2800/3800 Series Integrated Service Routers, Cisco 7200 Series Routers, Cisco 7301 Routers

Group member: Cisco 1800/2800/3800 Series Integrated Service Routers, Cisco 7200 Series Routers, Cisco 7301 Routers

Topology

Figure 1. VRF-lite Based GETVPN Topology



Note: The topology and the deployment components shown in this document are based on the deployment guide posted at http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6811/prod_white_paper0900aecd805cc40d.shtml. Refer this link for more details.

Deployment

Key server is not VRF aware. So, based on a single or multiple MPLS VPNs (PE VRFs) used in PE for each GETVPN group, there can be two cases.

Case (1): [Refer Figure 1]. PE uses a single MPLS VPN (PE VRF) for all the group member VRFs (CE VRFs). For this, group members can use the same certificate for authentication for all the crypto maps applied on VRF interfaces. No overlapping addresses can be supported in the group member VRFs because the PE has all the group member addresses in a single VRF. However, traffic excluded from any of the encryption policies are subject to be routed across group member VRFs.

Case (2): To use overlapping addresses between group member VRFs, PE should also use a unique MPLS VPN (PE VRFs) for each of the group member VRFs. In addition, a separate key server must be dedicated for each VRF, mainly because the key server is not VRF-aware. For this, group members should also use a separate certificate for authentication for each crypto map. The

group member configuration is almost the same as in case 1 except that the additional certificate trustpoints and different key server addresses should be required.

Note: For both cases above, each VRF interface requires a unique crypto map and each crypto map MUST use different GET VPN group. Hence key server must be configured with multiple GET VPN groups to support multiple VRFs in group members.

This deployment focuses on the Case (1), i.e, all the group member VRFs are connected to a single MPLS VPN in PE, hence no overlapping addresses can be used among group member VRFs. For the key server, the additional configuration involves multiple GET VPN groups based on group member VRFs, no other configuration is needed. VRFs are defined only in the group members. Each VRF defined in CE are associated with sub-interfaces between CE-PE links.

VRF “corp” is configured on selective group members only to showcase this deployment, however, resources in this VRF is accessible from other group members which do not use VRF. VRF “engg” is defined only in two group members for this deployment. A separate routing instance is configured for vrf “engg” in these two group members. Management tunnel is setup using a global routing table using loopback interface.

Note: Since no routing protocol is defined for management loopback interface, an exclusive static route is configured in PE and redistributed in MPLS VPN.

The following key server and group member configurations show only the necessary configurations required for GET VPN and VRF Lite. Refer the Full Configuration section for more details.

Key Server Configuration

```
!!!! The following configuration enables the key server in a router.
Each group defined in the key server has an identity that is shared
among the members within the group. Here the identity is set to 1234
for group ‘VRF-CORP’ and 5678 for group ‘VRF-ENGG’.  Also VRF-CORP
group uses multicast rekeying while VRF-ENGG uses unicast rekeying.
!!!
!
crypto isakmp policy 1                    // PKI authentication //
 encr aes
 group 2
!
crypto ipsec transform-set aes esp-aes  esp-sha-hmac
!
crypto ipsec profile vpnprof
 set transform-set aes
crypto ipsec profile vrf
 set security-association lifetime seconds 28800
 set transform-set aes
!
crypto gdoi group VRF-CORP    // GETVPN group defined for VRF corp //
 identity number 1234
 server local
  rekey algorithm aes 128      // Key encryption key is AES 128 //
  rekey address ipv4 rekey-multicast-group   // multicast rekeying
method //
  rekey lifetime seconds 10800
```

```
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa rekeyrsa
 sa ipsec 1
  profile vpnprof
  match address ipv4 sa-acl
  replay time window-size 5
 address ipv4 10.10.10.23
 redundancy             // Cooperative key servers enabled //
  local priority 100
  peer address ipv4 10.10.10.56
!
 ip access-list extended rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848
 permit udp host 10.10.10.56 eq 848 host 239.192.1.190 eq 848
!
ip access-list extended sa-acl
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
!
crypto gdoi group VRF-ENGG   // GETVPN group defined for VRF engg //
 identity number 5678
 server local
  rekey algorithm aes 128      // Key encryption key is AES 128 //
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa vrfrsa
  rekey transport unicast         // unicast rekeying method //
  sa ipsec 1
   profile vrf             // TEK “AES” defined in profile //
   match address ipv4 vrf-acl
   replay time window-size 5
  address ipv4 10.10.10.23
  redundancy                // Cooperative key server enabled //
   local priority 75
   peer address ipv4 10.10.10.56
!
ip access-list extended vrf-acl
 permit ip 10.2.1.0 0.0.0.255 10.2.2.0 0.0.0.255
 permit ip 10.2.2.0 0.0.0.255 10.2.1.0 0.0.0.255
```

Note: AES keys are difficult to hack, hence it is highly recommended to use “AES” for Traffic Encryption key (TEK) and Key encryption key (KEK). Also, AES keys can be used for longer duration as shown above using 8 hour TEK lifetime. In addition, AES is used for IKE phase 1 negotiations. However, 3DES is also supported but is not recommended for longer lifetimes.

Group Member Configuration

```
!!!! Only the necessary commands required to enable VRF lite and
GETVPN are shown here. For setting up management interface and more
VRF details, refer the Full Configuration section !!!!
!
ip vrf corp                     // VRF enabled globally //
 rd 65002:1
 route-target export 65002:1
 route-target import 65002:1
!
interface FastEthernet0                 // Interface for vrf corp //
 description outside interface
 ip vrf forwarding corp
 ip address 10.10.10.30 255.255.255.248
!
router bgp 65002
!
address-family ipv4 vrf corp  // Separate routing instance for vrf
corp //
 neighbor 10.10.10.29 remote-as 65001
!
crypto isakmp policy 1           //Using PKI authentication. //
 encr aes
 group 2
!
crypto isakmp keepalive 10
!
crypto gdoi group vrf-corp                    !! for vrf corp !!
 identity number 1234
 server address ipv4 10.10.10.56           // Register to Secondary
key server //
 server address ipv4 10.10.10.23
!
crypto gdoi group vrf-engg                   !! for vrf engg !!
 identity number 5678
 server address ipv4 10.10.10.23         // Register to Primary key
server //
 server address ipv4 10.10.10.56
!
crypto map corp local-address FastEthernet0     // Uses correct
interface for session end points //
crypto map corp 1 gdoi
 set group vrf-corp
 match address no-encryption-acl
!
crypto map engg local-address FastEthernet0.1
crypto map engg 1 gdoi
 set group vrf-engg
!
interface FastEthernet0
 description outside interface
 no ip dhcp client request tftp-server-address
```

```
 ip vrf forwarding corp   // FastEthernet0 is enabled for vrf corp //
 ip address 10.10.10.86 255.255.255.252
 duplex auto
 speed auto
 crypto map corp          // crypto map corp for vrf corp //
!
interface FastEthernet0.1
 description Outside Interface
 encapsulation dot1Q 14
 ip vrf forwarding engg
 ip address 10.10.10.98 255.255.255.252
 crypto map engg        // crypto map engg for vrf engg //
!
ip access-list extended no-encryption-acl
 deny   ip 10.1.1.0 0.0.0.255 host 10.10.10.23
 deny   ip 10.1.1.0 0.0.0.255 host 10.10.10.56
 deny   ip any host 239.192.1.190
```

Note: This deployment use different multicast RPs for multicast rekeying and multicast data purpose. The RP used for multicast data is protected by encryption policy and is present behind the group member at corporate network. The RP used for multicast rekeying is configured in MPLS/VPN address space and is not protected by the encryption policy. Refer Verification section on group member for the output.

Verification

Key Server 1:

```
keyserver1#sh crypto gdoi ks coop
Crypto Gdoi Group Name :VRF-CORP
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 10.10.10.23
        Local Priority: 100
        Local KS Role: Primary   , Local KS Status: Alive
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 9
                Antireplay Sequence Number: 883

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 10.10.10.56
                Peer Priority: 75
                Peer KS Role: Secondary , Peer KS Status: Alive
                Antireplay Sequence Number: 2

                IKE status: Established

               <Output Omitted >
```

```
Crypto Gdoi Group Name :VRF-ENGG
        Group handle: 2147483651, Local Key Server handle: 2147483652

        Local Address: 10.10.10.23
        Local Priority: 75
        Local KS Role: Primary   , Local KS Status: Alive
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 11
                Antireplay Sequence Number: 878

        Peer Sessions:
        Session 1:
                Server handle: 2147483653
                Peer Address: 10.10.10.56
                Peer Priority: 100
                Peer KS Role: Secondary , Peer KS Status: Alive
                Antireplay Sequence Number: 0

                IKE status: Established

           < Output Omitted >

keyserver1#sh crypto gdoi ks policy
Key Server Policy:
For group VRF-CORP (handle: 2147483650) server 10.10.10.23 (handle:
2147483650):

  # of teks : 2  Seq num : 11
  KEK POLICY (transport type : Multicast)
    spi : 0x2BA6BE18E540FACC1BF58F1BD658D57E
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16           key size          : 16
    Remaining life(sec): 4087        orig lifetime(sec): 10800
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : rekeyrsa

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x8D65C328    access-list          : sa-acl
    # of transforms    : 0             transform            : ESP_AES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 16            sig key size         : 20
    orig life(sec)     : 3600          remaining life(sec)  : 3490
    override life (sec): 0             antireplay window size: 5

  Replay Value 17230.09 secs
For group VRF-CORP (handle: 2147483650) server 10.10.10.56 (handle:
2147483651):
```

```
Key Server Policy:
For group VRF-ENGG (handle: 2147483651) server 10.10.10.23 (handle:
2147483652):

  # of teks : 1  Seq num : 4
  KEK POLICY (transport type : Unicast)
    spi : 0xCE5F6963A49D2DF4C0FA4D1BDA67F8F
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 16
    Remaining life(sec): 68901       orig lifetime(sec): 86400
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : vrfrsa

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xFE85A522    access-list           : vrf-acl
    # of transforms    : 0             transform             : ESP_AES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 16            sig key size          : 20
    orig life(sec)     : 28800         remaining life(sec)   : 11300
    override life (sec): 0             antireplay window size: 5

  Replay Value 17226.62 secs
For group VRF-ENGG (handle: 2147483651) server 10.10.10.56 (handle:
2147483653):

keyserver1#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group VRF-CORP : 11

Group Member ID   : 10.10.10.86
Group ID          : 1234
Group Name        : VRF-CORP
Key Server ID     : 10.10.10.23

Group Member ID   : 10.10.10.30
Group ID          : 1234
Group Name        : VRF-CORP
Key Server ID     : 10.10.10.56

    < Output Omitted >
Number of rekeys sent for group VRF-ENGG : 2

Group Member ID   : 10.10.10.70
Group ID          : 5678
Group Name        : VRF-ENGG
Key Server ID     : 10.10.10.23
```

```
Rekeys sent       : 3
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0

Sent seq num :    2    3    4    0
Rcvd seq num :    0    0    0    0

Group Member ID   : 10.10.10.98
Group ID          : 5678
Group Name        : VRF-ENGG
Key Server ID     : 10.10.10.23
Rekeys sent       : 3
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0

Sent seq num :    2    3    4    0
Rcvd seq num :    0    0    0    0

keyserver1# sh crypto gdoi ks rekey
Group VRF-CORP (Multicast)
    Number of Rekeys sent               : 11
    Number of Rekeys retransmitted      : 0
    KEK rekey lifetime (sec)            : 10800
        Remaining lifetime (sec)        : 4014
    Retransmit period                   : 10
    Number of retransmissions           : 2
    IPSec SA 1  lifetime (sec)          : 3600
        Remaining lifetime (sec)        : 3465
    Number of registrations after rekey : 0


Group VRF-ENGG (Unicast)
    Number of Rekeys sent               : 2
    Number of Rekeys retransmitted      : 6
    KEK rekey lifetime (sec)            : 86400
        Remaining lifetime (sec)        : 68829
    Retransmit period                   : 10
    Number of retransmissions           : 2
    IPSec SA 1  lifetime (sec)          : 28800
        Remaining lifetime (sec)        : 11230

keyserver1#
```

Key server 2:

```
keyserver2#sh crypto gdoi ks coop
Crypto Gdoi Group Name :VRF-CORP
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 10.10.10.56
        Local Priority: 75
```

```
        Local KS Role: Secondary , Local KS Status: Alive
        Secondary Timers:
                Sec Primary Periodic Time: 30
                Remaining Time: 13, Retries: 0
                Antireplay Sequence Number: 3

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 10.10.10.23
                Peer Priority: 100
                Peer KS Role: Primary   , Peer KS Status: Alive
                Antireplay Sequence Number: 893

                IKE status: Established
    <Output Omitted >
Crypto Gdoi Group Name :VRF-ENGG
        Group handle: 2147483651, Local Key Server handle: 2147483652

        Local Address: 10.10.10.56
        Local Priority: 100
        Local KS Role: Secondary , Local KS Status: Alive
        Secondary Timers:
                Sec Primary Periodic Time: 30
                Remaining Time: 15, Retries: 0
                Antireplay Sequence Number: 1

        Peer Sessions:
        Session 1:
                Server handle: 2147483653
                Peer Address: 10.10.10.23
                Peer Priority: 75
                Peer KS Role: Primary   , Peer KS Status: Alive
                Antireplay Sequence Number: 888

                IKE status: Established
        < Output Omitted >
keyserver2#sh crypto gdoi ks policy
Key Server Policy:
For group VRF-CORP (handle: 2147483650) server 10.10.10.56 (handle:
2147483650):

For group VRF-CORP (handle: 2147483650) server 10.10.10.23 (handle:
2147483651):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Multicast)
    spi : 0x2BA6BE18E540FACC1BF58F1BD658D57E
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16           key size          : 16
```

```
    Remaining life(sec): 3956        orig lifetime(sec): 10800
    sig hash algorithm : enabled     sig key length    : 1024
    sig size           : 128
    sig key name       : rekeyrsa

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x8D65C328    access-list          : sa-acl
    # of transforms    : 0             transform            : ESP_AES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 16            sig key size         : 20
    orig life(sec)     : 3600          remaining life(sec)  : 3408
    override life (sec): 0             antireplay window size: 5

  Replay Value 17359.93 secs

Key Server Policy:
For group VRF-ENGG (handle: 2147483651) server 10.10.10.56 (handle:
2147483652):

For group VRF-ENGG (handle: 2147483651) server 10.10.10.23 (handle:
2147483653):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0xCE5F6963A49D2DF4C0FA4D1BDA67F8F
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 16
    Remaining life(sec): 68772       orig lifetime(sec): 86400
    sig hash algorithm : enabled     sig key length    : 1024
    sig size           : 128
    sig key name       : vrfrsa

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xFE85A522    access-list          : vrf-acl
    # of transforms    : 0             transform            : ESP_AES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 16            sig key size         : 20
    orig life(sec)     : 28800         remaining life(sec)  : 11174
    override life (sec): 0             antireplay window size: 5

  Replay Value 17356.09 secs

keyserver2#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group VRF-CORP : 0         // Key server is
secondary, so no rekeys sent //

Group Member ID   : 10.10.10.30
```

```
Group ID          : 1234
Group Name        : VRF-CORP
Key Server ID     : 10.10.10.56

Group Member ID   : 10.10.10.86
Group ID          : 1234
Group Name        : VRF-CORP
Key Server ID     : 10.10.10.23

Number of rekeys sent for group VRF-ENGG : 0              // Key
server is secondary, so no rekeys sent //

Group Member ID   : 10.10.10.70
Group ID          : 5678
Group Name        : VRF-ENGG
Key Server ID     : 10.10.10.23
Rekeys sent       : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0

Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

Group Member ID   : 10.10.10.98
Group ID          : 5678
Group Name        : VRF-ENGG
Key Server ID     : 10.10.10.23
Rekeys sent       : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0

Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

keyserver2#
```

Group Member 1:

```
!! The following output shows the multicast RP used for multicast
rekeying and multicast data are different. Also the RP is learned
through Auto-RP, hence the group member configuration may not reflect
this. !!

group-member1#sh ip pim vrf corp rp map
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4              // Multicast data group address //
  RP 192.168.1.13 (rp.cisco.com), v2v1
    Info source: 192.168.1.13 (rp.cisco.com), elected via Auto-RP
         Uptime: 08:29:08, expires: 00:02:02
Group(s) 239.192.1.190/32      // Multicast rekeying group address //
  RP 10.10.10.25 (?), v2v1
```

```
    Info source: 10.10.10.25 (?), elected via Auto-RP
         Uptime: 1d19h, expires: 00:02:52
Acl: multicast_rp_blockdensemode, Static
    RP: 192.168.1.13 (rp.cisco.com)

group-member1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
172.16.10.1  10.10.10.78    QM_IDLE           2006    0 ACTIVE
// Management Tunnel //
10.10.10.56    10.10.10.30    GDOI_IDLE         2005    0 ACTIVE
10.10.10.23    10.10.10.70    GDOI_IDLE         2008    0 ACTIVE
239.192.1.190   10.10.10.23    GDOI_REKEY        2019    0 ACTIVE
// Multicast rekey for vrf corp //
10.10.10.70    10.10.10.23    GDOI_REKEY        2018    0 ACTIVE
// Unicast rekey for vrf engg //

IPv6 Crypto ISAKMP SA

group-member1#sh crypto gdoi gm
Group Member Information For Group vrf-corp:
    IPSec SA Direction      : Both
    ACL Received From KS    : gdoi_group_vrf-corp_temp_acl
    Re-register
        Remaining time      : 3140 secs

Group Member Information For Group vrf-engg:
    IPSec SA Direction      : Both
    ACL Received From KS    : gdoi_group_vrf-engg_temp_acl
    Re-register
        Remaining time      : 11246 secs

group-member1#sh crypto gdoi gm rekey
Group vrf-corp (Multicast)
    Number of Rekeys received (cumulative)       : 164
    Number of Rekeys received after registration : 164
    Multicast destination address                : 239.192.1.190

Group vrf-engg (Unicast)
    Number of Rekeys received (cumulative)       : 8
    Number of Rekeys received after registration : 8
    Number of Rekey Acks sent                    : 8
group-member1#
```

Group Member 2:

```
The following ping generated from a pc behind group member 2 on vrf
engg.
C:\>ping -n 100 10.2.1.3

Pinging 10.2.1.3 with 32 bytes of data:
```

```
Reply from 10.2.1.3: bytes=32 time=40ms TTL=126
Reply from 10.2.1.3: bytes=32 time=42ms TTL=126
Reply from 10.2.1.3: bytes=32 time=42ms TTL=126
…..
Reply from 10.2.1.3: bytes=32 time=42ms TTL=126
Reply from 10.2.1.3: bytes=32 time=41ms TTL=126

Ping statistics for 10.2.1.3:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 43ms, Average = 41ms

C:\ >
group-member2#show crypto session ivrf engg detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: FastEthernet0.1
Session status: UP-NO-IKE
Peer:  port 848 fvrf: engg ivrf: engg
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: permit ip 10.2.2.0/255.255.255.0 10.2.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 100 drop 0 life (KB/Sec) 4529328/1449
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4529324/1449
  IPSEC FLOW: permit ip 10.2.1.0/255.255.255.0 10.2.2.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4514092/1449
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4514092/1449

Interface: FastEthernet0.1
Uptime: 3d23h
Session status: UP-IDLE
Peer: 10.10.10.23 port 848 fvrf: engg ivrf: engg
      Phase1_id: keyserver1.cisco.com
      Desc: (none)
  IKE SA: local 10.10.10.98/848 remote 10.10.10.23/848 Active
          Capabilities:(none) connid:2101 lifetime:6w2d
  IKE SA: local 10.10.10.98/848 remote 10.10.10.23/848 Active
          Capabilities:D connid:2098 lifetime:18:33:28
  IKE SA: local 10.10.10.98/848 remote 10.10.10.23/848 Active
          Capabilities:(none) connid:2103 lifetime:6w2d

group-member2#sh crypto isakmp sa detail
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
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth
DH Lifetime Cap.

2370  10.10.10.102   172.16.10.1           ACTIVE 3des sha  rsig 2
23:59:51 D      // Management Tunnel //
       Engine-id:Conn-id =  SW:370

2358  10.10.10.98    10.10.10.23    engg     ACTIVE aes sha  rsig 2
00:34:37 D
       Engine-id:Conn-id =  SW:358

2369  239.192.1.190   10.10.10.23    corp     ACTIVE aes sha  psk  0
0     // KEK using AES //
       Engine-id:Conn-id =  SW:369

2368  10.10.10.98    10.10.10.23    engg     ACTIVE aes  sha  psk  0
0       // KEK using AES //
       Engine-id:Conn-id =  SW:368


IPv6 Crypto ISAKMP SA

group-member2#sh crypto gdoi gm rekey
Group vrf-corp (Multicast)
    Number of Rekeys received (cumulative)       : 263
    Number of Rekeys received after registration : 263
    Multicast destination address                : 239.192.1.190


Group vrf-engg (Unicast)
    Number of Rekeys received (cumulative)       : 8
    Number of Rekeys received after registration : 8
    Number of Rekey Acks sent                    : 8

group-member2#
```

Limitations / Final Notes

- Key server is not VRF aware.
- Need unique crypto map per group member vrf interface.
- Each crypto map must use different GETVPN group for registration.
- No overlapping addresses can be used between group member VRFs.
- If a group member cannot successfully register with the key server, the group member may transmit all data traffic in clear text. This would allow bridging traffic from one VRF to another within group member through the single PE VRF. The user must deploy necessary outbound ACLs in the group member VRF to protect from sending clear-text traffic. An

example ACL "block_clear_text" is given in the Full Configuration section for group member.

- Any traffic excluded from the encryption policy may also be bridged between group member VRFs through the single PE VRF. The user could apply encryption policy for all or most of the enterprise traffic and also use the ACL “block_clear_text” mentioned above.
- When a group member use the same certificate for authenticating multiple VRF sessions, it is not possible to use “authorization” command in the GETVPN group to securely authorize the group member VRF to join the respective GETVPN group.

Reference

Group Domain of Interpretation—RFC 3547 http://www.ietf.org/rfc/rfc3547.txt

Cisco IOS GET VPN Architecture and Features
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/htgetvpn.htm

Cisco Enterprise-Class Teleworker Solution
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_brochure0900aecd803fc7ec.html

Cisco ECT-Based GETVPN Deployment Guide
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6811/prod_white_paper0900aecd805cc40d.shtml

Public Key Infrastructure Integration with Cisco Enterprise-Class Teleworker Solution
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/prod_white_paper0900aecd805249e3.shtml

Cisco IOS IPsec High Availability for Management Gateway Configuration
http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd80278edf.shtml

Full Configuration

Full Configuration—Key Server 1

```
keyserver1#sh startup-config
Using 5372 out of 522232 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log uptime
service password-encryption
!
hostname keyserver1
!
boot-start-marker
boot system flash disk2:c7200-adventerprisek9-mz.124-11.T2
boot-end-marker
!
logging buffered 100000
```

```
enable secret  <removed>
!
aaa new-model
!
aaa group server radius pki-aaa-server        // AAA server resides in
management subnet //
 server-private 172.16.1.106 auth-port 1812 acct-port 1813 key
<removed>
!
aaa authentication login admin group tacacs+ enable
aaa authorization exec admin group tacacs+
aaa authorization network pkiaaa group pki-aaa-server
!
aaa session-id common
clock timezone pst -8
clock summer-time pdt recurring
ip cef
!
ip domain name cisco.com
ip host ios-cert-server 172.16.1.117
ip name-server 192.168.1.183
ip multicast-routing
ip ssh rsa keypair-name sshrsa
!
multilink bundle-name authenticated
!
crypto pki trustpoint ios-cert-server
 enrollment url http://ios-cert-server:80
 serial-number
 revocation-check crl
 rsakeypair keyserver1.cisco.com
 auto-enroll 60
 authorization list pkiaaa          // verifies the device
authorization in AAA server //
!
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
controller ISA 1/1
!
crypto isakmp policy 1                    // PKI authentication //
 encr aes
 group 2
!
!
crypto ipsec transform-set aes esp-aes  esp-sha-hmac
!
crypto ipsec profile vpnprof
 set transform-set aes
```

```
crypto ipsec profile vrf
 set security-association lifetime seconds 28800
 set transform-set aes
!
crypto gdoi group VRF-CORP    // GETVPN group defined for VRF corp //
 identity number 1234
 server local
  rekey algorithm aes 128
  rekey address ipv4 rekey-multicast-group
  rekey lifetime seconds 10800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
 sa ipsec 1
   profile vpnprof
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.10.10.23
  redundancy                    // Cooperative key server enabled //
   local priority 100
   peer address ipv4 10.10.10.56
!
crypto gdoi group VRF-ENGG    // GETVPN group defined for VRF engg //
 identity number 5678
 server local
  rekey algorithm aes 128
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa vrfrsa
  rekey transport unicast              // unicast rekeying method //
  sa ipsec 1
   profile vrf
   match address ipv4 vrf-acl
   replay time window-size 5
  address ipv4 10.10.10.23
  redundancy                    // Cooperative key server enabled //
   local priority 75
   peer address ipv4 10.10.10.56
!
interface Loopback0
 ip address 10.10.10.23 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1
 description Connected to PE2
 ip address 10.10.10.26 255.255.255.252
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
```

```
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no keepalive
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router bgp 65002
 no synchronization
 bgp log-neighbor-changes
 network 10.10.10.23 mask 255.255.255.255
 neighbor 10.10.10.25 remote-as 65001
 no auto-summary
!
no ip http server
no ip http secure-server
!
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode          //
RP for multicast data //
!
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 extended rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848
 permit udp host 10.10.10.56 eq 848 host 239.192.1.190 eq 848
ip access-list extended sa-acl
 deny   ip any host 239.192.1.190
 deny   ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31                  //
to exclude management traffic //
 deny   ip  172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31                 //
to exclude management traffic //
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
```

```
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
ip access-list extended vrf-acl
 permit ip 10.2.1.0 0.0.0.255 10.2.2.0 0.0.0.255
 permit ip 10.2.2.0 0.0.0.255 10.2.1.0 0.0.0.255
!
logging alarm informational
!
tacacs-server host 192.168.1.137
tacacs-server timeout 3
tacacs-server directed-request
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 password 7 < removed >
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login authentication admin
line vty 5 15
 transport input ssh
 transport output all
!
ntp clock-period 17179850
ntp server 172.16.1.97 prefer
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
keyserver1#
```

Full Configuration—Key Server 2

```
keyserver2#sh startup-config
Using 5100 out of 522232 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log uptime
service password-encryption
!
```

```
hostname keyserver2
!
boot-start-marker
boot system flash disk2:c7200-adventerprisek9-mz.124-11.T2
boot-end-marker
!
logging queue-limit 100
logging buffered 100000
enable secret  <removed>
!
aaa new-model
!
aaa group server radius pki-aaa-server
 server-private 172.16.1.106 auth-port 1812 acct-port 1813 key
<removed>
!
aaa authentication login admin group tacacs+ enable
aaa authorization exec admin group tacacs+
aaa authorization network pkiaaa group pki-aaa-server
!
aaa session-id common
clock timezone pst -8
clock summer-time pdt recurring
!
ip cef
ip domain name cisco.com
ip host ios-cert-server 172.16.1.117
ip name-server 192.168.1.183
!
ip multicast-routing
ip ssh rsa keypair-name sshrsa
!
multilink bundle-name authenticated
!
crypto pki trustpoint ios-cert-server
 enrollment url http://ios-cert-server:80
 serial-number
 revocation-check crl
 rsakeypair keyserver2.cisco.com
 auto-enroll 60
!
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
crypto isakmp policy 1
 encr aes
 group 2
!
crypto ipsec transform-set aes esp-aes  esp-sha-hmac
```

```
!
crypto ipsec profile vpnprof
 set transform-set aes
crypto ipsec profile vrf
 set security-association lifetime seconds 28800
 set transform-set aes
!
crypto gdoi group VRF-CORP    // GETVPN group defined for VRF corp //
 identity number 1234
 server local
  rekey algorithm aes 128
  rekey address ipv4 rekey-multicast-group
  rekey lifetime seconds 10800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile vpnprof
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.10.10.56
  redundancy
   local priority 75
   peer address ipv4 10.10.10.23
!
crypto gdoi group VRF-ENGG    // GETVPN group defined for VRF engg //
 identity number 5678
 server local
  rekey algorithm aes 128
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa vrfrsa
  rekey transport unicast               // unicast rekeying method //
  sa ipsec 1
   profile vrf
   match address ipv4 vrf-acl
   replay time window-size 5
  address ipv4 10.10.10.23
  redundancy                                      // Cooperative key
server enabled //
   local priority 100
   peer address ipv4 10.10.10.56
!
interface Loopback0
 ip address 10.10.10.56 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1
 description Connected to PE3
 ip address 10.10.10.54 255.255.255.252
 ip pim sparse-dense-mode
 duplex auto
```

```
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router bgp 65002
 no synchronization
 bgp log-neighbor-changes
 network 10.10.10.56 mask 255.255.255.255
 neighbor 10.10.10.53 remote-as 65001
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.10.10.53
!
no ip http server
no ip http secure-server
!
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode
!
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 extended rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848
 permit udp host 10.10.10.56 eq 848 host 239.192.1.190 eq 848
ip access-list extended sa-acl
 deny   ip any host 239.192.1.190
 deny   ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31                  //
to exclude management traffic //
 deny   ip  172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31                 //
to exclude management traffic //
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
ip access-list extended vrf-acl
```

```
 permit ip 10.2.1.0 0.0.0.255 10.2.2.0 0.0.0.255
 permit ip 10.2.2.0 0.0.0.255 10.2.1.0 0.0.0.255
logging alarm informational
!
tacacs-server host 192.168.1.137
tacacs-server timeout 3
tacacs-server directed-request
!
control-plane
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 password < removed >
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login authentication admin
line vty 5 15
 transport input ssh
 transport output all
!
ntp clock-period 17179914
ntp server 172.16.1.97
!
end
keyserver2#
```

Full Configuration—Group Member 1

```
group-member1#sh running-config
Building configuration...

Current configuration : 26154 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname group-member1
!
boot-start-marker
boot system flash:c181x-adventerprisek9-mz.124-11.T2
boot-end-marker
!
logging buffered 100000
```

```
enable secret <removed>
!
aaa new-model
!
aaa session-id common
clock timezone PST -8
clock summer-time PDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.1.1.1
!
ip dhcp pool client                        // DHCP pool for VRF corp //
   network 10.1.1.0 255.255.255.248
   domain-name cisco.com
   option 150 ip 192.168.1.70
   netbios-name-server 192.168.1.238
   dns-server 192.168.1.183
   default-router 10.1.1.1
!
ip dhcp pool vrf                           // DHCP pool for VRF engg //
   import all
   network 10.2.1.0 255.255.255.0
   default-router 10.2.1.1
   domain-name cisco.com
   netbios-name-server 192.168.1.238
   dns-server 192.168.1.183
!
ip vrf corp
 rd 65002:1
 route-target export 65002:1
 route-target import 65002:1
!
ip vrf engg
 rd 65002:2
 route-target export 65002:2
 route-target import 65002:2
!
ip domain lookup source-interface FastEthernet0.2       // DNS lookup
use management interface //
ip domain name cisco.com
ip host ios-cert-server 172.16.1.117
ip host mgmt-ca 172.16.1.102
ip name-server 192.168.1.183
ip multicast-routing
ip multicast-routing vrf corp                    // for receiving
multicast rekeys //
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 esmtp
ip inspect name test skinny
ip inspect name test sip
no ip igmp snooping
login on-failure log
!
multilink bundle-name authenticated
!
crypto pki trustpoint mgmt-ca
 enrollment mode ra
 enrollment url http://mgmt-ca:80
 serial-number
 revocation-check none
 source interface Loopback0
 auto-enroll 60
!
crypto pki trustpoint ios-cert-server             // Same certificate
is used for both GETVPN  crypto maps //
 enrollment url http://ios-cert-server:80
 serial-number
 revocation-check crl
 source interface Loopback0                      // Triggers management
tunnel bringup first to download CRLs //
 auto-enroll 75
!
crypto pki certificate chain mgmt-ca
 certificate <removed>
 certificate ca <removed>
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
class-map match-any call-setup
 match  dscp af31
 match  dscp af32
 match  dscp cs3
 match  precedence 3
class-map match-any internetwork-control
 match  dscp cs6
 match access-group name gdoi_acl
class-map match-any qos
 match access-group name test
class-map match-any voice
 match  dscp ef
```

```
 match  dscp cs5
 match  precedence 5
!
policy-map voip_ipsec_dsl
 description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class voice
  priority 128
 class call-setup
  bandwidth percent 2
 class internetwork-control
  bandwidth percent 5
 class class-default
  fair-queue
  random-detect
!
crypto logging session
!
crypto isakmp policy 1
 encr aes
 group 2
!
crypto ipsec transform-set mgmt-3des esp-3des esp-sha-hmac
crypto gdoi group vrf-corp
 identity number 1234
 server address ipv4 10.10.10.56
 server address ipv4 10.10.10.23
!
crypto gdoi group vrf-engg
 identity number 5678
 server address ipv4 10.10.10.23
 server address ipv4 10.10.10.56
!
crypto map corp local-address FastEthernet0
crypto map corp 1 gdoi
 set group vrf-corp
 match address no-encryption-acl
 qos pre-classify
!
crypto map engg local-address FastEthernet0.1
crypto map engg 1 gdoi
 set group vrf-engg
!
crypto map mgmt local-address FastEthernet0.2
crypto map mgmt 1 ipsec-isakmp
 description Management Tunnel
 set peer 172.16.10.1
 set transform-set mgmt-3des
 match address mgmt_acl
!
```

```
interface Loopback0             // Used to setup management tunnel //
  description management interface
  ip address 10.1.1.226 255.255.255.255
!
interface FastEthernet0                  // Interface for vrf corp //
 description outside interface
 no ip dhcp client request tftp-server-address
 ip vrf forwarding corp
 ip address 10.10.10.30 255.255.255.252
 ip access-group block_clear_text out
 ip pim sparse-dense-mode
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map corp
!
interface FastEthernet0.1                // Interface for vrf engg //
 encapsulation dot1Q 11
 ip vrf forwarding engg
 ip address 10.10.10.70 255.255.255.252
 crypto map engg
!
interface FastEthernet0.2            // Management Interface  in
global table //
 encapsulation dot1Q 13
 ip address 10.10.10.78 255.255.255.252
 crypto map mgmt
!
interface FastEthernet1
 no ip address
 shutdown
!
interface FastEthernet2
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet3
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
```

```
interface FastEthernet9
!
interface Dot11Radio0
 no ip address
 shutdown
 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 Dot11Radio1
 no ip address
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
!
interface Vlan1
 no ip address
!
interface Vlan10
 description inside interface
 ip vrf forwarding corp
 ip address 10.1.1.1 255.255.255.248
 ip pim sparse-dense-mode
 ip virtual-reassembly
 ip tcp adjust-mss 1360
!
interface Vlan20
 description inside interface
 ip vrf forwarding engg
 ip address 10.2.1.1 255.255.255.0
!
router bgp 65002
 no synchronization
 bgp router-id 10.10.10.30
 bgp log-neighbor-changes
 no auto-summary
 !
 address-family ipv4 vrf engg                    // Separate routing
instance for vrf engg //
 neighbor 10.10.10.69 remote-as 65001
 neighbor 10.10.10.69 activate
 no synchronization
 network 10.2.1.0 mask 255.255.255.0
 exit-address-family
 !
 address-family ipv4 vrf corp                    // Separate routing
instance for vrf corp //
 neighbor 10.10.10.29 remote-as 65001
 neighbor 10.10.10.29 activate
 no synchronization
```

```
 network 10.1.1.0 mask 255.255.255.248
 exit-address-family
!
ip route 0.0.0.0 0.0.0.0 10.10.10.77
ip route 172.16.1.96 255.255.255.224 10.10.10.29
!
ip http server
no ip http secure-server
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode
// Optional //
ip pim vrf corp rp-address 192.168.1.13 multicast_rp_blockdensemode
// To support multicast //
ip nat inside source list nat_acl interface FastEthernet0 overload
!
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 extended block_clear_text
 permit esp any any
 permit udp any eq 848 any eq 848
 permit pim host 10.10.10.30 host 10.10.10.29
 deny   ip 10.1.1.0 0.0.0.255 10.0.0.0 0.255.255.255
 deny   ip 10.1.1.0 0.0.0.255 172.16.0.0 0.15.255.255
 deny   ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
 permit ip any any
ip access-list extended fw_acl
 permit esp any any
 permit udp any any eq 848
 permit udp any any eq isakmp
 permit tcp 10.10.10.0 0.0.0.255 eq bgp 10.10.10.0 0.0.0.255
 permit tcp 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 eq bgp
 permit pim any any
 permit igmp any any
 permit udp any host 224.0.1.39
 permit udp any host 224.0.1.40
 permit ip 172.16.1.96 0.0.0.31 10.10.10.0 0.0.0.255
 permit tcp host 10.10.10.23 10.10.10.0 0.0.0.255 eq 22
 permit udp host 172.16.1.97 eq ntp any
 permit udp any any eq bootpc
 permit icmp any any
 deny   ip any any log
ip access-list extended nat_acl
 deny   ip 10.1.1.0 0.0.0.255 10.0.0.0 0.255.255.255
 deny   ip 10.1.1.0 0.0.0.255 172.16.0.0 0.15.255.255
 deny   ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
 permit ip 10.1.1.0 0.0.0.255 any
```

```
ip access-list extended no-encryption-acl
 deny   ip host 10.10.10.30 host 10.10.10.29
 deny   ip 10.1.1.0 0.0.0.255 host 10.10.10.23
 deny   ip any host 239.192.1.190
 deny   ip 10.1.1.0 0.0.0.255 host 10.10.10.56
ip access-list extended mgmt_acl
 permit ip host 10.1.1.226 172.16.1.96 0.0.0.31
!
control-plane
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password <removed>
!
ntp clock-period 17180282
ntp server 172.16.1.97
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end

group-member1#
```

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C07-402003-00 3/07