Cisco IOS GETVPN VRF-Aware GDOI GM Solution Deployment Guide

Introduction to GETVPN
The Cisco IOS GETVPN is a tunnel-less VPN technology that provides end-to-end security for network traffic in a native mode and maintaining the fully meshed topology. It uses the core network's ability to route and replicate the packets between various sites within the enterprise. Cisco IOS GETVPN preserves the original source and destination IP addresses information in the header of the encrypted packet for optimal routing. Hence, it is largely suited for an enterprise running over a private IP-enabled network such as MPLS VPN, VPLS, or FR/ATM. It is also better suited to encrypt IP-based multicast and broadcast traffic which might traverse a satellite network or IP multicast enabled core.

Cisco IOS GET VPN uses the IETF’s standard RFC-3547 Group Domain of Interpretation (GDOI) as the key management protocol and RFC-2406 for IPSec for encryption.

VRF-Aware GDOI Group Member (GM)
Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. In a normal GETVPN deployment, both data and control traffic (such as registration and re-key) use the same VRF. In a VRF-aware GDOI GM configuration, control traffic can be separated from data traffic using a separate VRF. The GM has the ability to route control traffic (registration & rekeys) through a VRF that is different from the VRF used for routing encrypted data traffic. Basically registration & rekeys are routed through one VRF and the policies downloaded are applied to a crypto-map applied in a different VRF. A service provider may assign the key management control traffic to a management VRF on a GM where separate designated VRF’s are used to service individual customer’s encrypted traffic. An enterprise could use it for departmental VPNs so they don’t have to replicate the key server infrastructure for every department.

Purpose and Scope
This document provides basic deployment guidelines to enable Cisco IOS Group Encrypted Transport VPN (GETVPN) with VRF-Aware GDOI feature in an enterprise network. This document does not cover in-depth technical details about various features comprising Cisco IOS GETVPN. Please refer to the References section for additional documents.
Recommended Platforms and Images

Images based on Cisco IOS Software Release 15.0(1) M or above are required for group member routers while it is recommended for key server routers. The recommended image subset is `advipservicesk9` 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**: 1800/2800/3800 Series Integrated Service Routers (ISR), Cisco 7200 Series Routers, Cisco 7301 Routers, and 1900/2900/3900 ISR-G2 platforms.

Deployment

A new CLI is introduced to configure the registration interface under the GDOI group. This registration interface is used to route the GDOI registrations through the VRF configured on that interface for this particular group and registration requests would be sourced with the IP address configured on the register address interface. After successful registration the IPSec policy will be applied to the interface where the crypto map is applied.

Example:

```bash
crypto gdoi group GET-GROUP1
   identity number 1357924680
   server address ipv4 10.32.178.23
   server address ipv4 10.32.178.56
   client registration interface FastEthernet0.3
```

Here the Group member will use ‘FastEthernet0.3’ interface to register the group ‘GET-GROUP1’ with configured Key Servers. The future registration and rekey will happen through this interface. If this interface cannot reach any of the configured Key servers, registration of the group will fail.

If client registration interface under a GDOI group is not configured, GM will use the either the specified local-address configured for the crypto map or the IP address associated with the interface where the crypto-map is applied. If client registration interface is not specified then, by default, the registration would happen through the default interface/VRF where the crypto map is applied and VRF-aware GDOI is inherently disabled.
In this setup different crypto map applied to different interfaces, each interface is in a different VRF context namely CustomerA and CustomerB. All these groups are accessing the same key servers (coop) and these key servers are accessible through separate control traffic VRF named 'management'.

**Sample GM Configuration (For Unicast Rekey)**

/!!!/ Only the necessary commands required to enable VRF-Aware GETVPN are shown here. For more VRF details, refer the Full Configuration section!!!/

```plaintext
crypto isakmp policy 1
  encr aes
  group 2
  lifetime 300
!
crypto gdoi group GET-GROUP1
  identity number 1357924680
  server address ipv4 10.32.178.23
  server address ipv4 10.32.178.56
  client registration interface FastEthernet0.3
!
```
crypto gdoi group GET-GROUP2
  identity number 4567
  server address ipv4 10.32.178.23
  server address ipv4 10.32.178.56
  client registration interface FastEthernet0.3
!
!
crypto map getvpn-map1 1 gdoi
  set group GET-GROUP1
!
crypto map getvpn-map2 1 gdoi
  set group GET-GROUP2
!
interface FastEthernet0.1
  encapsulation dot1Q 1
  ip vrf forwarding CustomerA
  ip address 10.32.178.98 255.255.255.252
duplex auto
  speed auto
crypto map getvpn-map1
!
!
interface FastEthernet0.2
  encapsulation dot1Q 10
  ip vrf forwarding CustomerB
  ip address 10.32.178.70 255.255.255.252
  ip pim sparse-mode
  crypto map getvpn-map2
!
interface FastEthernet0.3
  encapsulation dot1Q 20
  ip vrf forwarding management
  ip address 10.32.178.109 255.255.255.252
!

Here the registration interface for both groups is the same. There is one registration through the interface FastEthernet0.3 for every group configured and associated with a crypto map. There are two registrations for the above example given. Note that there will be only one IKE SA established for these registrations.

For group GET-GROUP1 we have the registration interface as FastEthernet0.3, this would represent one Group Member. After successful registration, policies would be downloaded and associated with the crypto map on the interface FastEthernet0.1

For group GET-GROUP2 also has the registration interface as FastEthernet0.3, this would represent another GM. After successful registration, policies would be downloaded and associated with the crypto map on the interface FastEthernet0.2

If both registrations are successful with the first Key Server configured, then there would be only one IKE SA established for both the registrations to that key server.
Sample KS Configuration (For Unicast Rekey)

crypto isakmp policy 1
  encr aes
  group 2
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set aes256 esp-aes 256 esp-sha-hmac
!
crypto ipsec profile profile1
  set security-association lifetime seconds 900
  set transform-set aes256
!
crypto ipsec profile profile2
  set security-association lifetime seconds 900
  set transform-set aes256
!
!
crypto gdoi group GET-GROUP1
  identity number 1357924680
  server local
    rekey algorithm aes 256
    rekey lifetime seconds 14400
    rekey retransmit 10 number 3
    rekey authentication mypubkey rsa rekeyA
    rekey transport unicast
    sa ipsec 1
      profile profile1
      match address ipv4 getA-acl
      no replay
      address ipv4 10.32.178.23
    redundancy
      local priority 50
      peer address ipv4 10.32.178.56
      peer address ipv4 10.32.178.57
!
!
crypto gdoi group GET-GROUP2
  identity number 4567
  server local
    rekey algorithm aes 256
    rekey lifetime seconds 14400
    rekey retransmit 10 number 3
    rekey authentication mypubkey rsa rekeyB
    rekey transport unicast
    sa ipsec 1
      profile profile2
      match address ipv4 getB-acl
      no replay
      address ipv4 10.32.178.23
redundancy
local priority 5
peer address ipv4 10.32.178.56
peer address ipv4 10.32.178.57
!

Verification

PING to the Key Server with client registration interface as source.

GM1#ping vrf management 10.32.178.56 source fastEthernet 0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.32.178.56, timeout is 2 seconds:
Packet sent with a source address of 10.32.178.110
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Trace route to the Key Server

GM1#traceroute vrf management 10.32.178.56
Type escape sequence to abort.
Tracing the route to 10.32.178.56
  1 10.32.178.109 [AS 65004] 0 msec 4 msec 0 msec
  2 10.32.178.54 [AS 65004] 0 msec * 0 msec
GM1#

show crypto isakmp sa
This command displays the active ISAKMP sessions on the router and is common for standard IPSec and GEVPN.
The output below is from a Group Member. The ISAKMP SAs with ‘GDOI_IDLE’ status are created as result of GMs registration with KS. Registration SA is same for both GDOI groups as the GM uses the same interface for registration. The SA labeled “GDOI_REKEY” is used for rekey. There will be a separate REKEY SA for each group.
GM1#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.32.178.109 10.32.178.23 GDOI_REKEY 2020 ACTIVE
10.32.178.23 10.32.178.109 GDOI_IDLE 2019 ACTIVE
10.32.178.109 10.32.178.23 GDOI_REKEY 2021 ACTIVE
IPv6 Crypto ISAKMP SA
GM1#
**Show crypto gdoi**
This command displays the all basic details about the GETVPN status. The output is different for Key Server and Group Member.

On Group Member:

The output shows the GM used the same VRF for registering both groups.

GM1#show crypto gdoi

GROUP INFORMATION

<table>
<thead>
<tr>
<th>Group Name</th>
<th>GET-GROUP1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Identity</td>
<td>1357924680</td>
</tr>
<tr>
<td>Rekeys received</td>
<td>93</td>
</tr>
<tr>
<td>IPSec SA Direction</td>
<td>Both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Server list</th>
<th>10.32.178.23</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.32.178.56</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group member</th>
<th>10.32.178.109</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf: management</td>
<td></td>
</tr>
<tr>
<td>Registration status</td>
<td>Registered</td>
</tr>
<tr>
<td>Registered with</td>
<td>10.32.178.23</td>
</tr>
<tr>
<td>Re-registers in</td>
<td>790 sec</td>
</tr>
<tr>
<td>Succeeded registration</td>
<td>1</td>
</tr>
<tr>
<td>Attempted registration</td>
<td>1</td>
</tr>
<tr>
<td>Last rekey from</td>
<td>10.32.178.23</td>
</tr>
<tr>
<td>Last rekey seq num</td>
<td>3</td>
</tr>
<tr>
<td>Unicast rekey received: 93</td>
<td></td>
</tr>
<tr>
<td>Rekey ACKs sent</td>
<td>93</td>
</tr>
<tr>
<td>Rekey Rcvd(hh:mm:ss)</td>
<td>00:01:01</td>
</tr>
</tbody>
</table>

Rekeys cumulative

<table>
<thead>
<tr>
<th>Total received</th>
<th>93</th>
</tr>
</thead>
<tbody>
<tr>
<td>After latest register</td>
<td>93</td>
</tr>
<tr>
<td>Rekey Acks sent</td>
<td>93</td>
</tr>
</tbody>
</table>
ACL Downloaded From KS 10.32.178.23:
<output truncated>

KEK POLICY:
- Rekey Transport Type: Unicast
- Lifetime (secs): 12774
- Encrypt Algorithm: AES
- Key Size: 256
- Sig Hash Algorithm: HMAC_AUTH_SHA
- Sig Key Length (bits): 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:

FastEthernet0.1:
- IPsec SA:
  - spi: 0xAA0BE09C(2852905116)
  - transform: esp-256-aes esp-sha-hmac
  - sa timing:remaining key lifetime (sec): (838)
  - Anti-Replay(Time Based): 10 sec interval

- Group Name: GET-GROUP2
- Group Identity: 4567
- Rekeys received: 93
- IPSec SA Direction: Both

- Group Server list: 10.32.178.23
  10.32.178.56

- Group member: 10.32.178.109 vrf: management
- Registration status: Registered
- Registered with: 10.32.178.23
- Re-registers in: 206 sec
- Succeeded registration: 1
Attempted registration: 1
Last rekey from       : 10.32.178.23
Last rekey seq num   : 4
Unicast rekey received: 93
Rekey ACKs sent      : 93
Rekey Rcvd(hh:mm:ss) : 00:10:43

Rekeys cumulative
Total received       : 93
After latest register: 93
Rekey Acks sents     : 93

ACL Downloaded From KS 10.32.178.23:
<output truncated>

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs)      : 11550
Encrypt Algorithm    : AES
Key Size             : 256
Sig Hash Algorithm   : HMAC_AUTH_SHA
Sig Key Length (bits): 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
FastEthernet0.2:
IPsec SA:
    spi: 0xE704734B(3875828555)
    transform: esp-256-aes esp-sha-hmac
    sa timing:remaining key lifetime (sec): (256)
    Anti-Replay(Time Based) : 15 sec interval
**Best Practices**

The GETVPN GM requires data plane traffic to enter and exit the same VRF in order for the crypto to be applied properly. VRF-lite means that all the traffic traversing in the particular VRF should be confined to the same VRF after route lookup. GET VPN with VRF-lite support does not address route leaking. Route leaking occurs when traffic enters one routing VRF context and is forwarded in a different VRF routing context. If route leaking is configured on the GM, packets originating in a different route context will be sent out in clear text from the VRF interface where the crypto map is applied.

Following scenarios are not supported:

- Traffic coming from non-VRF global interface to any VRF interface with GDOI crypto map.
- Traffic coming from one VRF and leaving another VRF interface with GDOI crypto map.
- If route leaking is required to make the traffic flow from an interface participating in global routing to another interface with VRF forwarding or vice-versa, the route leaking function must be applied on a router prior to reaching the Group Member router such that traffic entering and exiting the Group Member stays within the same VRF before and after encryption. See GETVPN Design and Implementation guide at [http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/GETVPN_DIG_version_1_0_External.pdf](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/GETVPN_DIG_version_1_0_External.pdf).

**Multicast Rekey Configuration**

The following sections cover the configuration needs to be incorporated into the basic configuration for enabling multicast rekeying.

**Key Server Configuration for Multicast Rekey**

This is a sample incremental configuration needed to convert the GEVPN deployment from unicast to multicast rekey.

```plaintext
! Enable multi-cast routing
ip multi-cast routing
! Enable SSM mode
ip pim ssm range 1
!
! ACL list used in SSM range command
access-list 1 permit 239.192.1.190 0.0.0.0
!
interface GigabitEthernet0/1
  ip pim sparse-mode
!
crypto gdoi group GDOI-GROUP1
  server local
  ! Default rekey method is multicast
  no rekey transport unicast
  ! Multicast group for re-keying. This is specified as a ACL
  rekey address ipv4 getvpn-rekey-multicast-group
  rekey retransmit 10 number 3
!
! Add these ACEs in GETVPN policy ACLs
ip access-list extended <acl name>
deny ip any 224.0.0.0 0.255.255.255
```
deny pim any host 224.0.0.13
!
ip access-list extended getvpn-rekey-multicast-group
    permit ip any host 239.192.1.190

**Group Member Configuration for Multicast Rekey**

Following configuration need to be added to the GMs to receive multicast rekey. This can be used only if multicast routing is enabled on rest of the network. Below configuration uses SSM for multicast. The configuration may need to be changed according to the existing multicast mechanism deployed in the network.

![configuration](image)

**Full Configuration**

**Group Member Configuration**

```bash
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

hostname get-gm

boot-start-marker
boot system flash:c181x-advipservicesk9-mz.150-1.M
boot-end-marker

logging buffered 100000
enable secret 5 <removed>
enable password 7 <removed>

! aaa new-model
!

! aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
```
!  
!  
!  
clock timezone PST -8  
clock summer-time PST recurring  
!  
crypto pki trustpoint beta-ca  
enrollment mode ra  
enrollment url <removed>1  
serial-number  
fingerprint <removed>  
revocation-check none  
!  
!  
crypto pki certificate chain beta-ca  
<removed>  
dot11 syslog  
!  
ip source-route  
!  
!  
ip dhcp pool CustomerA  
vrf CustomerA  
  network 10.32.176.152 255.255.255.248  
domain-name a.com  
default-router 10.32.176.153  
netbios-name-server <removed>  
option 150 ip <removed>  
dns-server <removed>  
!  
ip dhcp pool CustomerB  
vrf CustomerB  
  network 10.32.176.128 255.255.255.248  
domain-name b.com  
dns-server <removed>  
option 150 ip <removed>  
default-router 10.32.176.129  
netbios-name-server <removed>  
!  
ip vrf CustomerA  
rd 1:100  
route-target export 1:100  
route-target import 1:100  
!  
ip vrf CustomerB  
rd 1:200  
route-target export 1:200  
route-target import 1:200  
!
ip vrf management
dr 1:299
route-target export 1:299
route-target import 1:299
!
ip cef
no ip domain lookup
ip host beta-ca 10.34.250.101
ip name-server <removed>
ip multicast-routing
ip multicast-routing vrf CustomerA
ip multicast-routing vrf CustomerB
ip multicast-routing vrf management
no ip igmp ssm-map query dns
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
!
crypto isakmp policy 1
encr aes
group 2
lifetime 300
!
crypto gdoi group GET-GROUP1
identity number 1357924680
server address ipv4 10.32.178.23
server address ipv4 10.32.178.56
client registration interface FastEthernet0.3
!
crypto gdoi group GET-GROUP2
identity number 4567
server address ipv4 10.32.178.23
server address ipv4 10.32.178.56
client registration interface FastEthernet0.3
!
!
crypto map getvpn-map1 1 gdoi
set group GET-GROUP1
!
crypto map getvpn-map2 1 gdoi
set group GET-GROUP2
!
interface FastEthernet0.1
encapsulation dot1Q 1
ip vrf forwarding CustomerA
ip address 10.32.178.98 255.255.255.252
duplex auto
speed auto
crypto map getvpn-map1
!

interface FastEthernet0.2
encapsulation dot1Q 10
ip vrf forwarding CustomerB
ip address 10.32.178.70 255.255.255.252
ip pim sparse-mode
crypto map getvpn-map2
!

interface FastEthernet0.3
encapsulation dot1Q 20
ip vrf forwarding management
ip address 10.32.178.109 255.255.255.252
!

interface FastEthernet1
no ip address
shutdown
duplex auto
speed auto
!

interface FastEthernet2
switchport access vlan 10
spanning-tree portfast
!

interface FastEthernet3
switchport access vlan 10
!

interface FastEthernet4
switchport access vlan 10
!

interface FastEthernet5
switchport access vlan 10
!

interface FastEthernet6
switchport access vlan 10
spanning-tree portfast
!

interface FastEthernet7
switchport access vlan 20
spanning-tree portfast
!
!
interface FastEthernet8
switchport access vlan 20
spanning-tree portfast
!
!
interface Vlan1
no ip address
!
!
interface Vlan10
    ip vrf forwarding CustomerA
    ip address 10.32.176.129 255.255.255.248
    ip pim sparse-mode
    ip tcp adjust-mss 1360
    no autostate
!
!
interface Vlan20
    ip vrf forwarding CustomerB
    ip address 10.32.176.153 255.255.255.248
    ip pim sparse-mode
    ip tcp adjust-mss 1360
    no autostate
!
!
interface Async1
    no ip address
    encapsulation slip
!
!
router bgp 65002
    bgp router-id 10.32.178.98
    bgp log-neighbor-changes
    neighbor 10.32.178.97 remote-as 65001
!
address-family ipv4
    no synchronization
    neighbor 10.32.178.97 activate
    no auto-summary
    exit-address-family
!
address-family ipv4 vrf CustomerA
    no synchronization
    bgp router-id 10.32.178.98
    network 10.32.176.152 mask 255.255.255.248
    neighbor 10.32.178.97 remote-as 65001
neighbor 10.32.178.97 activate
exit-address-family

address-family ipv4 vrf CustomerB
no synchronization
bgp router-id 10.32.178.70
network 10.32.176.128 mask 255.255.255.248
neighbor 10.32.178.69 remote-as 65001
neighbor 10.32.178.69 activate
exit-address-family

address-family ipv4 vrf management
no synchronization
redistribute connected
neighbor 10.32.178.110 remote-as 65001
neighbor 10.32.178.110 activate
neighbor 10.32.178.110 as-override
exit-address-family

ip forward-protocol nd
no ip http server
ip http secure-server

access-list 1 permit 239.192.0.0 0.0.255.255

control-plane

line con 0
exec-timeout 0 0
line 1
modem InOut
stopbits 1
speed 115200
flowcontrol hardware
line aux 0
line vty 0 4
exec-timeout 0 0
password 7 <removed>
transport input all
line vty 5 193
password 7 <removed>
transport input all
exception data-corruption buffer truncate
ntp server 198.123.30.132
Key Server1 Configuration

! service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
service internal
!
hostname ks1
!
boot-start-marker
boot system disk2:c7200-advipservicesk9-mz.150-1.M
boot-end-marker
!
logging message-counter syslog
logging buffered 100000
enable secret 5 <removed>
!
aaa new-model
!
aaa group server tacacs+ vty_access
!
aaa authentication login admin group tacacs+ enable
!
!
aaa session-id common
clock timezone pst -8
clock summer-time PDT recurring
ip source-route
ip cef
!
no ip domain lookup
ip domain name Cisco.com
ip host beta-ca 10.34.250.101
ip name-server <removed>
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice dsp waitstate 24898
!
crypto pki trustpoint beta-ca
   enrollment mode ra
   enrollment url <removed>
serial-number
revocation-check none
auto-enroll
!
!
crypto pki certificate chain beta-ca
certificate 10C34F80000000000005FD
<truncated>
log config
  hidekeys
  !
!
crypto isakmp policy 1
  encr aes
  group 2
  !
crypto ipsec transform-set aes256 esp-aes 256 esp-sha-hmac
  !
crypto ipsec profile profile1
  set security-association lifetime seconds 7200
  set transform-set aes256
  !
crypto ipsec profile profile2
  set security-association lifetime seconds 7200
  set transform-set aes256
  !
!
crypto gdoi group GET-GROUP1
  identity number 1357924680
  server local
  rekey algorithm aes 256
  rekey lifetime seconds 86400
  rekey retransmit 10 number 3
  rekey authentication mypubkey rsa rekeyA
  rekey transport unicast
  sa ipsec 1
    profile profile1
    match address ipv4 customerA-acl
    no replay
    address ipv4 10.32.178.23
    redundancy
      local priority 50
    peer address ipv4 10.32.178.56
    peer address ipv4 10.32.178.57
    !
crypto gdoi group GET-GROUP2
  identity number 4567
  server local
  rekey algorithm aes 256
  rekey lifetime seconds 86400
rekey retransmit 10 number 3
rekey authentication mypubkey rsa rekeyB
rekey transport unicast
sa ipsec 1
profile profile2
match address ipv4 customerB-acl
no replay
address ipv4 10.32.178.23
redundancy
local priority 5
peer address ipv4 10.32.178.56
peer address ipv4 10.32.178.57

!

ip ssh version 1
buffers huge size 64000

!

interface Loopback0
ip address 10.32.178.23 255.255.255.255
ip pim sparse-mode

!

interface GigabitEthernet0/1
description Connected to pe2
ip address 10.32.178.26 255.255.255.252
ip pim sparse-mode
duplex auto
speed auto
media-type rj45
no negotiation auto
hold-queue 4096 in
hold-queue 4096 out

!
router bgp 65002
bgp log-neighbor-changes
neighbor 10.32.178.25 remote-as 65001

!
address-family ipv4
neighbor 10.32.178.25 activate
no auto-summary
no synchronization
network 10.32.178.23 mask 255.255.255.255
network 10.32.178.26 mask 255.255.255.255
exit-address-family

!
address-family ipv4 multicast
neighbor 10.32.178.25 activate
no auto-summary
network 10.32.178.23 mask 255.255.255.255
exit-address-family
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.32.178.25
ip http server
ip http secure-server
!
!
ip pim ssm range 1
ip tacacs source-interface Loopback0
!
!
ip access-list extended customerA-acl
deny   udp any host 10.32.17.19 eq tftp
deny   udp host 10.32.17.19 eq tftp any
deny   udp any eq 848 any eq 848
deny   ip any 224.0.0.0 0.255.255.255
deny   pim any host 224.0.0.13
deny   igmp any any
deny   icmp any any
deny   tcp any any eq telnet
deny   tcp any eq telnet any
deny   tcp any eq bgp any
deny   tcp any any eq bgp
deny   eigrp any any
deny   udp any any eq ntp
deny   udp any any eq snmp
deny   udp any eq snmp any
deny   udp any any eq snmptrap
deny   udp any any eq syslog
deny   tcp any any eq tacacs
deny   tcp any eq tacacs any
permit ip any any
!
ip access-list extended customerB-acl
deny   udp any eq 848 any eq 848
deny   ip any 224.0.0.0 0.255.255.255
deny   pim any host 224.0.0.13
deny   igmp any any
deny   tcp any any eq telnet
deny   tcp any eq telnet any
deny   tcp any eq bgp any
deny   tcp any any eq bgp
deny   eigrp any any
deny   udp any any eq ntp
deny   udp any any eq snmp
deny   udp any eq snmp any
deny   udp any any eq snmptrap
deny   udp any any eq syslog
deny   tcp any any eq tacacs
deny   tcp any eq tacacs any
permit ip any any
!
!
!
tacacs-server host <removed>
tacacs-server host <removed>
tacacs-server timeout 15
! tacacs-server directed-request
!
control-plane
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
line con 0
    password 7 <removed>
    transport output all
    stopbits 1
line aux 0
    transport output all
    stopbits 1
line vty 0 4
    exec-timeout 0 0
    logging synchronous
    login authentication admin
    transport input all
    transport output all
line vty 5 15
    exec-timeout 0 0
    transport input all
    transport output all
!
exception data-corruption buffer truncate
ntp server <removed>
ntp server <removed>
end

Key Server2 Configuration
!
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
service internal
!
hostname ks2
!
boot-start-marker
boot system disk2:c7200-advipservicesk9-mz.150-1.M
boot-end-marker
!
logging message-counter syslog
logging queue-limit 100
logging buffered 65555
enable secret 5 <removed>
!
aaa new-model
!
!
aaa group server tacacs+ vty_access
  server <removed>
  server <removed>
!
aaa authentication login admin group tacacs+ enable
aaa authorization exec admin group tacacs+
!
!
aaa session-id common
clock timezone pst -8
clock summer-time PDT recurring
ip source-route
ip cef
!
!
!
!
no ip domain lookup
ip domain name cisco.com
ip host beta-ca 10.34.250.101
ip name-server <removed>
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice dsp waitstate 24898
!
crypto pki trustpoint beta-ca
  enrollment mode ra
  enrollment url <removed>
  serial-number
  revocation-check none
  auto-enroll
!
!
crypto pki certificate chain beta-ca
certificate 479663B9000100000C3F
< truncated >
username cisco secret 5 <removed>
archive
  log config
  hidekeys
!
!
crypto isakmp policy 1
  encr aes
  group 2
!
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set aes256 esp-aes 256 esp-sha-hmac
!
crypto ipsec profile profile1
  set security-association lifetime seconds 7200
  set transform-set aes256
!
crypto ipsec profile profile2
  set security-association lifetime seconds 7200
  set transform-set aes256
!
crypto gdoi group GET-GROUP1
  identity number 1357924680
  server local
    rekey algorithm aes 256
    rekey lifetime seconds 84400
    rekey retransmit 10 number 3
    rekey authentication mypubkey rsa rekeyA
    rekey transport unicast
    sa ipsec 1
    profile profile1
    match address ipv4 customerA-acl
    no replay
    address ipv4 10.32.178.56
    redundancy
    local priority 80
    peer address ipv4 10.32.178.23
    peer address ipv4 10.32.178.57
!
crypto gdoi group GET-GROUP2
  identity number 4567
  server local
    rekey algorithm aes 256
    rekey lifetime seconds 84400
    rekey retransmit 10 number 3
    rekey authentication mypubkey rsa rekeyB
rekey transport unicast
sa ipsec 1
  profile profile2
  match address ipv4 customerB-acl
  no replay
  address ipv4 10.32.178.56
redundancy
  local priority 3
  peer address ipv4 10.32.178.23
  peer address ipv4 10.32.178.57
!
ip ssh version 1
buffers huge size 64000
!
interface Loopback0
  ip address 10.32.178.56 255.255.255.255
  ip pim sparse-mode
!
interface GigabitEthernet0/1
  description Connected to pe1
  ip address 10.32.178.54 255.255.255.252
  ip pim sparse-mode
duplex full
  speed 1000
  media-type rj45
  no negotiation auto
  hold-queue 4096 in
  hold-queue 4096 out
!
router bgp 65002
  bgp log-neighbor-changes
  neighbor 10.32.178.53 remote-as 65001
  address-family ipv4
    neighbor 10.32.178.53 activate
    no auto-summary
    no synchronization
    network 10.32.178.56 mask 255.255.255.255
    exit-address-family
  !
  address-family ipv4 multicast
    neighbor 10.32.178.53 activate
    no auto-summary
    network 10.32.178.56 mask 255.255.255.255
    exit-address-family
  !
ip forward-protocol nd
  ip route 0.0.0.0 0.0.0.0 10.32.178.53
  no ip http server
  ip http secure-server
!                          
! ip pim ssm range 1      
ip tacacs source-interface Loopback0   
!                          
ip access-list extended customerA-acl
  deny   udp any host 10.32.17.19 eq tftp   
deny   udp host 10.32.17.19 eq tftp any   
deny   udp any eq 848 any eq 848   
deny   ip any 224.0.0.0 0.255.255.255   
deny   pim any host 224.0.0.13   
deny   igmp any any   
deny   icmp any any   
deny   tcp any any eq telnet   
deny   tcp any eq telnet any   
deny   tcp any eq bgp any   
deny   tcp any any eq bgp   
deny   eigrp any any   
deny   udp any eq ntp   
deny   udp any any eq snmp   
deny   udp any eq snmp any   
deny   udp any eq snmp any   
deny   udp any eq snmptrap   
deny   udp any any eq syslog   
deny   tcp any any eq tacacs   
deny   tcp any eq tacacs any   
permit ip any any   
ip access-list extended customerB-acl
  deny   udp any eq 848 any eq 848   
deny   ip any 224.0.0.0 0.255.255.255   
deny   pim any host 224.0.0.13   
deny   igmp any any   
deny   tcp any any eq telnet   
deny   tcp any eq telnet any   
deny   tcp any eq bgp any   
deny   tcp any any eq bgp   
deny   eigrp any any   
deny   udp any any eq ntp   
deny   udp any any eq snmp   
deny   udp any eq snmp any   
deny   udp any eq snmptrap   
deny   udp any any eq syslog   
deny   tcp any any eq tacacs   
deny   tcp any eq tacacs any   
permit ip any any   
!                          
logging alarm informational  
!                          
tacacs-server host <removed>  
tacacs-server host <removed>
tacacs-server timeout 15
  tacacs-server directed-request
!
  control-plane
!
!
  mgcp fax t38 ecm
  mgcp behavior g729-variants static-pt
!
!
  dial-peer cor custom
!
!
!
  line con 0
  exec-timeout 0 0
  stopbits 1
  line aux 0
  stopbits 1
  line vty 0 4
  exec-timeout 0 0
  login authentication admin
  line vty 5 15
  exec-timeout 0 0
  transport input ssh
  transport output all
  line vty 16 1869
  !
  exception data-corruption buffer truncate
  ntp server <removed>
  ntp server <removed>
end

References

CISCO IOS GETVPN Start Page: http://www.cisco.com/go/getvpn

Cisco IOS GETVPN Solution Deployment Guide:


GETVPN Design and Implementation Guide:

GETVPN Configuration Guide:

GDOI RFC: http://www.ietf.org/rfc/rfc3547.txt
VRF-lite Based Group Encrypted Transport VPN: