GM and KS Deployment Using CSM GETVPN Policies

Last Updated: 05/22/09

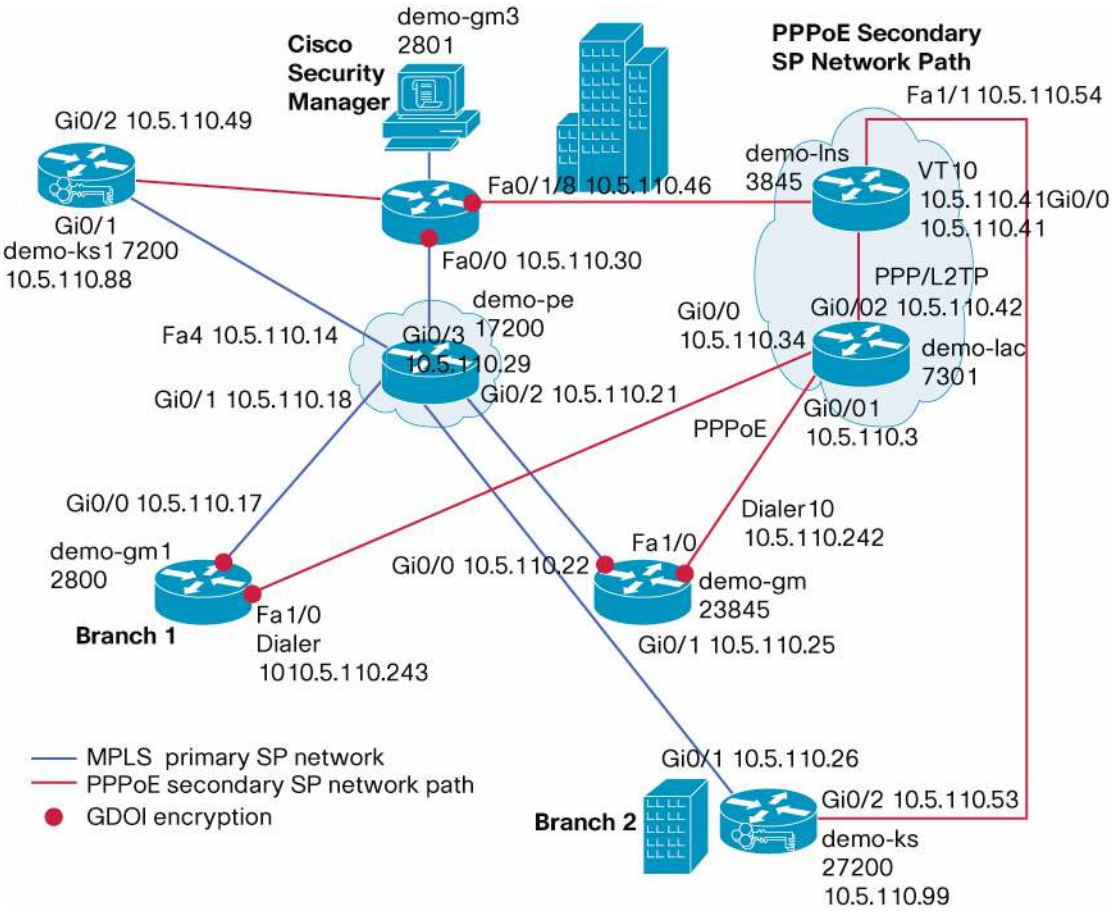
Cisco Security Manager (CSM) can be used to deploy and manage Group Member (GM) and Key Server (KS) configurations efficiently. CSM allows painless rapid deployment of GMs. CSM is an enterprise-class tool which allows the administrator to easily deploy and manage huge number of GMs.

This document provides step by step procedure for deploying GETVPN GMs and KSs running IOS version 12.4 22T using CSM version 3.3. Before using CSM for deploying new GMs, get at least 2 GMs and 1 Key Server (KS) working. This will be helpful to discover configuration from the working GM and KS and use it for creating master configuration devices for deployment.

1 GETVPN Deployment using CSM overview

1.1 Network Topology

Figure 1. Demo GETVPN Network Topology



GETVPN example deployment setup consists of three GMs (Group Members) and two KS (Key Server) are included in the setup. “demo-pe1” simulates the MPLS primary SP network. One Key server is located in the Headquarters. Other Key server is connected behind GM in one of the branch. Both KSs have path to primary MPLS SP network and secondary PPPoE SP network.

GMs between branches and headquarters are also connected via secondary PPPoE service provider network. This secondary network will be used when there is network outage in primary SP network. GM between branches is connected to demo-lac via PPPoE interface. PPPoL2TP tunnel connects between demo-lac and demo-lns.

GDOI encryption is done on the customer network side in the GM routers. Traffic flowing through the interface connected to primary SP network and the interface connected to the secondary service provider network are GDOI encrypted.

KS1 and KS2 are connected to both MPLS and PPPoE networks. GMs encrypt traffic using GDOI group GETVPN-DEMO-MPLS for MPLS network and encrypt traffic GETVPN-DEMO-PPPOE GDOI group for PPPoE network

Following table summarizes GDOI groups and IP addresses for the GM interfaces:

GDOI group	GDOI encryption in demo-gm1 interface	GDOI encryption in demo-gm2 interface	GDOI encryption in demo-gm3 interface
GETVPN-DEMO-MPLS GDOI group for primary MPLS network (LAN)	Gi0/0 10.5.110.17	Gi0/0 10.5.110.22	Fa0/0 10.5.110.30
GETVPN-DEMO-PPPOE group for secondary SP network (WAN)	Dialer 10 10.5.110.243	Dialer 10 10.5.110.242	Fa0/1/8 10.5.110.46

2. Create GM and KS Master Device in CSM Client

This section describes step by step process of creating master devices by discovering a GETVPN GM (demo-gm1) and KS (demo-ks1) using CSM client. Log into CSM Client. First step involves creating a master GM device. This master GM device will be cloned and used for deploying other GMs. Master GM device is created by discovering an existing GM.

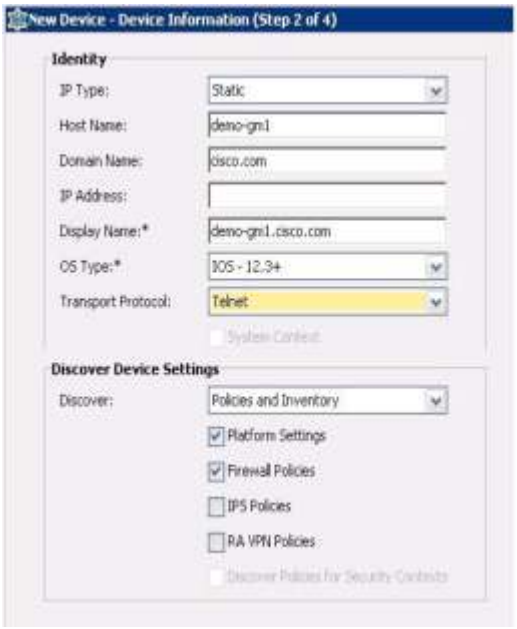
2.1 Discover the GM

Discover configuration from a well working GM. In this example demo-gm1’s configuration is discovered.

Start Cisco Security Manager Client from CSM. Log into CSM Client.

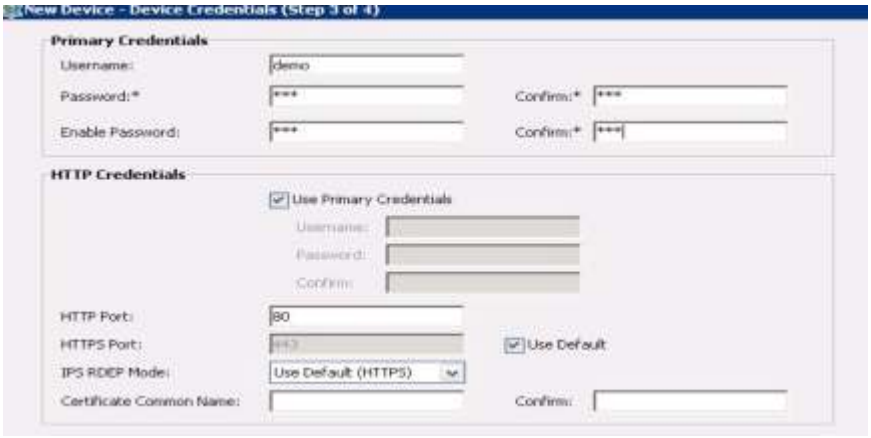
From CSM client window select File menu, then select New Device, Select Add Device from Network and click Next.

Discover GM by entering following values as shown below and enter Next:



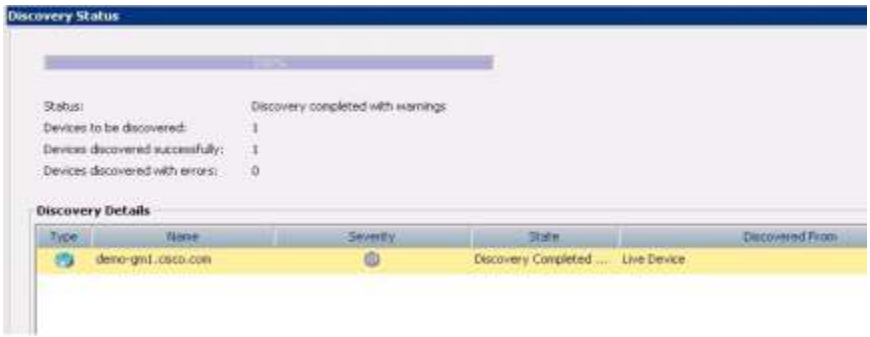
2.2 Device credentials

Enter Device Credentials as shown below, click Next and click Finished.



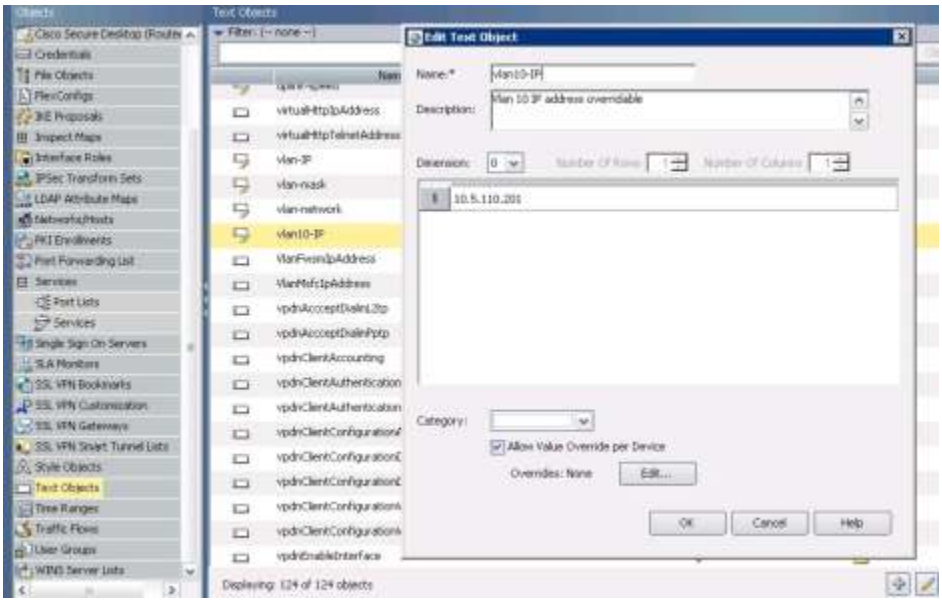
2.3 Check Device Discovery status

Check discovery status of the device. Device should be discovered in CSM client.



2.4 Add a Text Variable for VLAN 10 IP Address

Add a text variable as follows for making VLAN 10 IP address customizable for every new device. VLAN 10 is private network that changes for every GM. Devices like Personal Computer and phones are connected to VLAN 10. From Tools menu select Policy Object Manager, select Text objects and add VLAN 10 IP variable as follows. Once you enter the value, save and from File menu submit.



2.5 Discover Key Server configuration

Discover configuration of the primary KS demo-ks1 using same process described in sections 2.2.1 to 2.2.3. Select demo-ks1 device and select Platform, Device Admin, Accounts and Credentials menu. Right click and select “Unassign policy”. Credentials are not required since all the GETVPN devices are initially configured with user credentials. To save this configuration, select file menu and click “submit”. Configuration will not be applied to the device database, until it is submitted.

2.6 Discover GETVPN policies

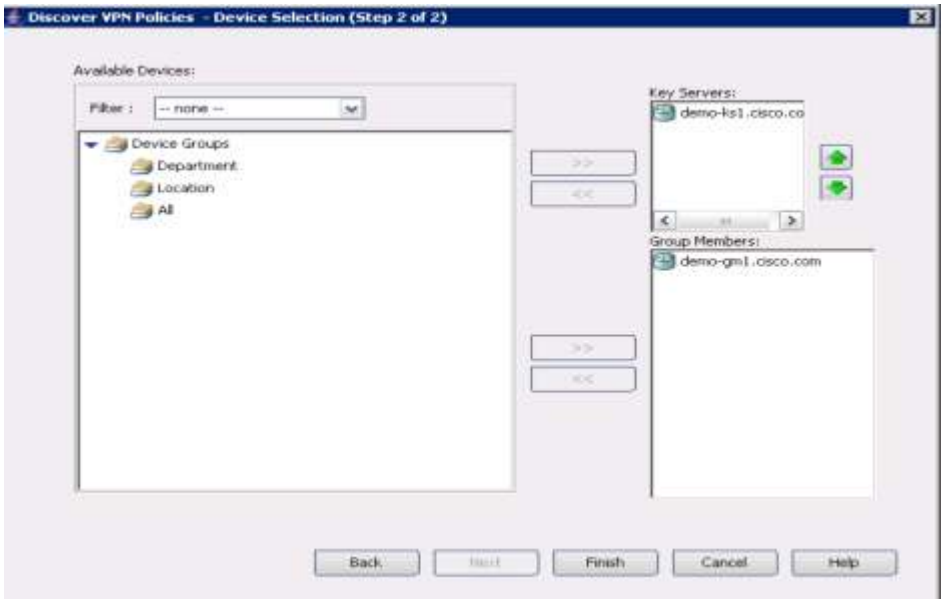
To discover GETVPN policies from GMs and KSs, following needs to be done:

From the “Policy” menu, select “Discover VPN Policies…”, fill in name and technology fields as follows:

In this example VPN policies are discovered using existing configuration stored in the CSM after GM and KS are discovered. Alternatively you can discover VPN policies from network by setting “Network” value in the “Discover from” field. End result will be same for both these methods.

Press “Next” button.

Select the GM and KS devices as shown below:



Press “Finish” button.

Discovery status screen will show the discovery status as given below:

Press close button and from file menu click “submit”.

2.7 Add GETVPN Flexconfig in GM

CLIs that are not supported by CSM needed to be added in Flexconfig.

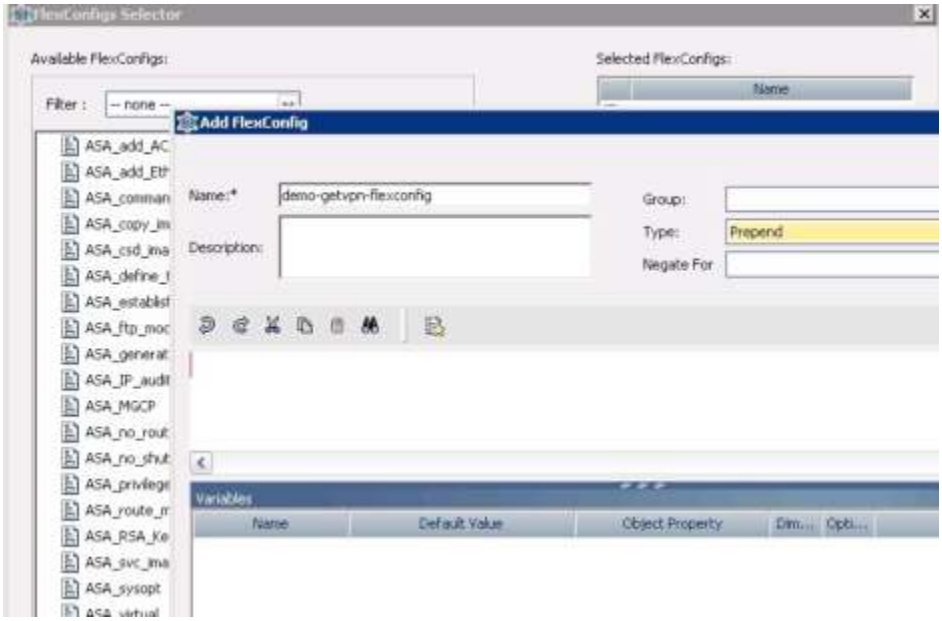
Process of identifying CLIs that are not supported by CSM is as follows: Select discovered device, right click and preview the full configuration of the discovered device. Then select the discovered device and clone it to a new device and preview configuration of cloned device. The difference between CLIs present in the discovered device configuration and cloned device configuration are the CLIs that are not supported by CSM.

Add missing CLIs that not supported by CSM in demo-getvpn Flexconfig as shown below.:

Select demo-gm1 device.

Select Routing and EIGRP menu, right click and select “Unassign Policy…”. EIGRP policy is added in the flexconfig for GM.

Next select Flexconfigs and Select +. Enter demo-getvpn-flexconfig as Flexconfig name. Select flexconfig type as Prepend. Add following configuration as Flexconfig that is common to all the GMs, press Save and from File menu click submit:



Add the following CLIs in the flexconfig that are not part of the configuration generated by CSM..

There are a few variables you need to add in this Flexconfig.

Procedure for adding $Vlan10-IP: From the Flexconfig page at the first occurrence of this variable: right click, select “Insert Policy object” menu, then select “Text object”, Select Vlan10-IP. Text Object Property Selector Window will pop-up. Enter Variable Name as Vlan10-IP. All the other places in Flexconfig where you want to use this variable, simply enter $Vlan10-IP.

Procedure for adding $SYS_DOMAIN_NAME – From the Flexconfig page where you want to enter the domain name, right click and select “Insert System Variables” , “Device” and “SYS_DOMAIN_NAME”.

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
```

```
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
clock timezone pst -8
clock summer-time pst recurring
!
ip cef
!
ip dhcp pool demo
 network $Vlan10-IP 255.255.255.248
 domain-name $SYS_DOMAIN_NAME
 default-router $Vlan10-IP
!
ip domain name $SYS_DOMAIN_NAME
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
bba-group pppoe global
!
interface Vlan10
 ip address $Vlan10-IP 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 ip igmp join-group 239.255.255.249 source 10.5.110.218
 ip igmp join-group 239.255.255.250 source 10.5.110.218
 no autostate
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet1/0
 description connected to demo-lac
```

```
 no switchport
 no ip address
 ip pim sparse-mode
 ip tcp adjust-mss 1452
 pppoe enable group global
 pppoe-client dial-pool-number 10
!
interface Dialer10
 ip address negotiated
 ip mtu 1492
 ip pim sparse-mode
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer pool 10
 ppp authentication pap
 ppp pap sent-username demo@cisco.com password lab
!
! You can configure EIGRP policy directly in CSM without unassigning EIGRP policy.
Following provides
! flexibility to make use of Vlan10_IP variable.
router eigrp 44
network $Vlan10-IP 255.255.255.248
network 10.5.110.240 0.0.0.7
no auto-summary
!
ip pim ssm range 1
ip nat inside source list 10 interface Dialer10 overload
!
access-list 1 permit 239.192.0.0 0.0.255.255
access-list 1 permit 239.255.0.0 0.0.255.255
access-list 10 permit 10.5.110.200 0.0.0.7
dialer-list 10 protocol ip list 10
```

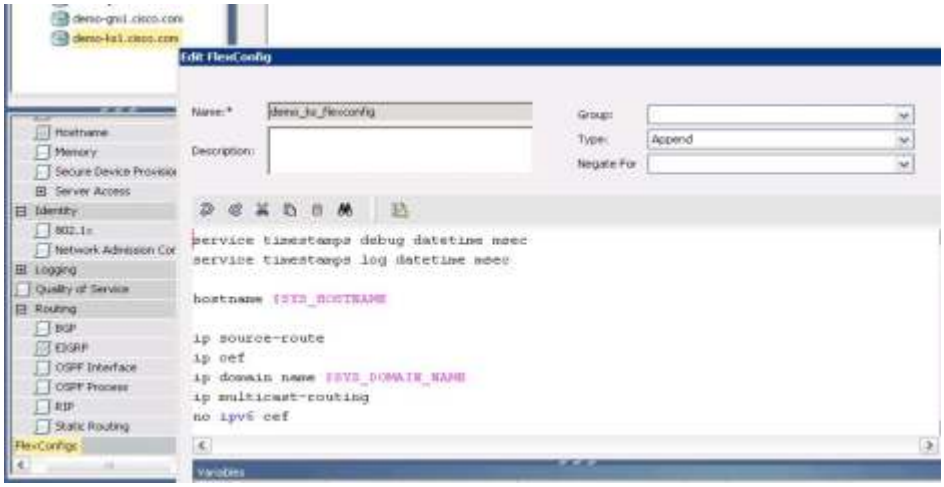
Once you add the Flexconfig, Select File menu and click “submit”.

2.8 Add GETVPN Flexconfig in KS

We need to add CLIs not generated by CSM in the Flexconfig.

Add demo_ks_flexconfig Flexconfig as shown below. Select demo-ks1 master device.

Next select Flexconfigs and Select +. Enter demo-ks-flexconfig as Flexconfig name. Select flexconfig type as Append. Add following configuration as Flexconfigs that is common to all the KSs that were not generated by CSM.



Press Save and from File menu and click submit.

```
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname $SYS_HOSTNAME
!
ip source-route
ip cef
ip domain name $SYS_DOMAIN_NAME
ip multicast-routing
no ipv6 cef
!
interface Loopback0
ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-pe1
 ip pim sparse-mode
!
interface GigabitEthernet0/2
 description Connected to demo-lns
 ip pim sparse-mode
```

```
!
ip pim ssm range 1
ip access-list standard 1
 permit 239.192.0.0 0.0.255.255
!
#icmd-begin
crypto key import rsa rekeyrsa exportable terminal passphrase
% Enter PEM-formatted public .*| #icmd-cert-begin
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDr0jfi+oIVG7LAkx0LinTVl6+X
BXPG1p82SUsSUsM2zTLwoPmyfpDczFk7Xn3N+dtGqQe/9IN3M+RF0xk/PyMlPGBi
F7ysqjLPjOo8NBreXk7FEhPEp68HJ2jMUH1xBOJeX6XwRXYylEFV1CeFc9enXxvr
5CPLTSYqXk5RuBlI4wIDAQAB
-----END PUBLIC KEY-----
quit
#icmd-cert-end
% Enter PEM-formatted encrypted private .*| #icmd-cert-begin
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F725B4F4D54B85C2

32sFSCoSUmT+b7e0ucJf8oQ7r23b+vOunbrJSwJ8J2/E9P47+YmUIaQZQ63b2x+c
mRMrcMfou2vvg0J4RpuIgY8yKcRERbZRn3WXr+VG41ewbR0JDwgvWYJiAvG5feh4
mawFD0xos1oXZnRV9KKMnkA5NJEvrW0ZRC16t4K446tQ4p8lxVzValgQSi/CSoqu
UVf4rendHroNrr+f9Go+d4bnBHuKCD0J2YoG+aYsr3YHfi15ezEZiyaaktxTa45q
ZKTOAroYPj+RFz61AXCJF0Lt0GrsIwlh+Aq24/CnMhHu6YhJj38/e1WSeaRDzF+Q
cN7bAftIpGJvUgY4mer72oB4q0bLnNFlN3kfwTC2s835rK4Ydf9qVlKzpr/gbubb
d/p1NUo5jZYWGwvYJPddcR98hmFM9yuj/KqjFa2Liyv148n/AV8Pj+lKkNoGo+j+
7ya0CxGc17Ury+jJjA7zPz2gVBqLSktriiFLrPLj5WHmIVmfitsDF3mIJtil7i22
+beNtePWxRq7l2rTsnL8EjRoX/43JR4sFJmoxiRUgXVwAjR3TisuBR5LqnIhvDbN
urUMC8IcHZaOw3jnzCTJ6aGe89tVT2Qy2vrHuZeq7n+zIVMcCavz7ZId0+I1/YPN
Hq/+ZuXl93q/1s49ChCFKrNOpprvLGZdbTB6Wcku1t93T4c8Tt3pu9aUXL+gHG8D
FM+l7kLqZ93f+FmAOaEGtFd60Uvr50qQ8ovPm8D3I+5ZEH1avbEPkXcCqV0CNzT0
SEQqZUrxo8r68rzLmfH+Ir2Ifh7zQy1hFs3m1303phENdn6lBsMQxg==
-----END RSA PRIVATE KEY-----
quit
#icmd-cert-end
```

```
#icmd-end
!
```

3 Deploying GMs

Once master (demo-gm1) GM device for a particular platform is created, it can be used for provisioning other GMs with same Platform type. In the example given in this document, Cisco 2851 platform is used.

3.1 Prepare New Device for Deployment as GM

Before pushing GM configuration to new device that needs to be deployed as GM, the device should have network connectivity and user credentials. Here is the minimum configuration needed for demo-gm2 router before deploying configuration from the CSM. Minimum configuration includes the following: IP address, routes, hostname, domain name, and user credentials. Following is the minimum configuration is required to push the configuration from CSM:

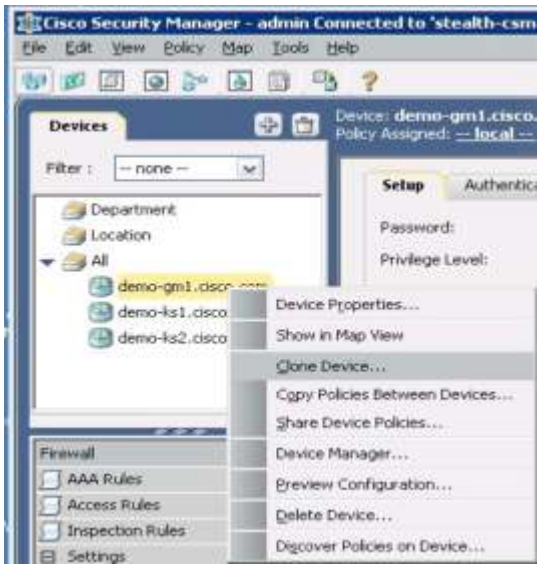
```
service password-encryption
!
hostname demo-gm2
!
enable secret 5 lab
!
username demo password lab
!
interface GigabitEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.22 255.255.255.252
!
router eigrp 44
 network 10.5.110.20 0.0.0.3
 no auto-summary
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 lab
 login
!
```

3.2 Connect New Device to Network with IP Address

Configure the new device with IP address so that configuration can be pushed from CSM. Very minimum configuration is required. Complete running configuration for this step is given in section 3.1.

3.3 Clone Device to Deploy New GM

Select the master device “demo-gm1.cisco.com”, right click on it and select “clone device” as follows:



3.4 Clone Device to Deploy New GM

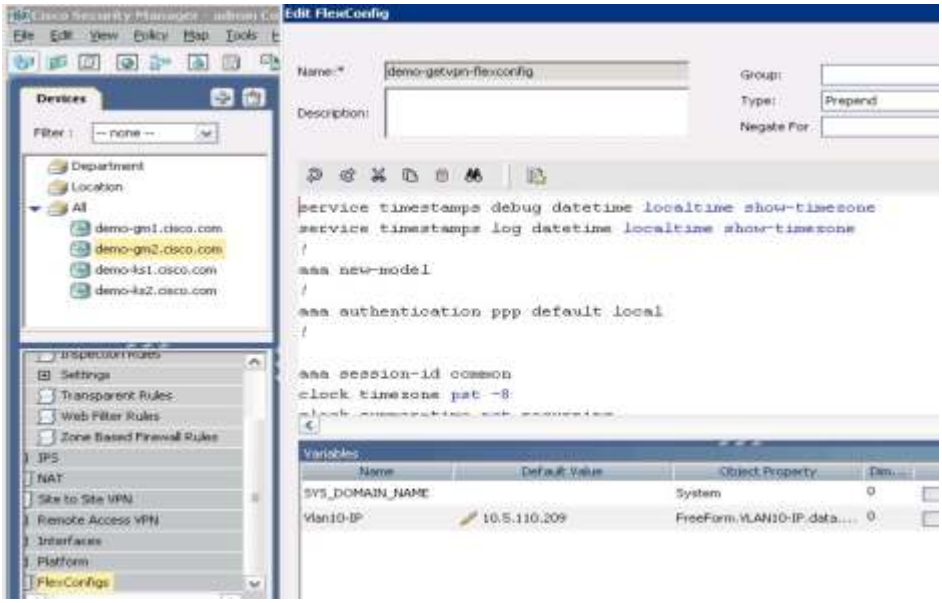
Enter new GM Identity as follows: IP address need to be entered if host name is not published with DNS. After entering required values, click OK.

3.5 Change IP Address of Interface

Select dem-gm2 device and select interfaces menu. Change appropriate IP address for Gi0/0 for this GM. Save the Flexconfig. From File menu select submit.

3.6 Select New GM Device and Enter VLAN 10 IP

Select the newly cloned GM and select FlexConfig menu, select demo-getvpn Flexconfig and edit the Flexconfig. Change the VLAN 10 address from the allocated private network subnet for this GM as follows:



Save the Flexconfig.

3.7 Deploy GM by Pushing Configuration from CSM

From the File menu select “submit and deploy”, select the GM device you want to deploy (demo-gm2) and press the Deploy button.

3.8 Verify GM Configuration Deployment Status

Verify the GM deployment status. You should not see any error. GM should be up and running. Verify “show crypto gdoi” on GM to check GETVPN encryption is enabled. Your GM will receive multicast rekeys from the KS.

4 Deploying KSs

Once one KS device for a particular platform is created, it can be used for provisioning other KSs with same Platform type. In the example given in this document, Cisco 7200 platform is used.

4.1 Prepare New Device for Deployment as KS

Before pushing KS configuration to new device that needs to be deployed as KS, the device should have network connectivity and user credentials. Here is the configuration of demo-ks2 router before deploying configuration from CSM. Minimum configuration includes the following: IP address, routes, hostname, domain name, and user credentials. Following is the minimum configuration is required to push the configuration from CSM:

```
service password-encryption
!
```

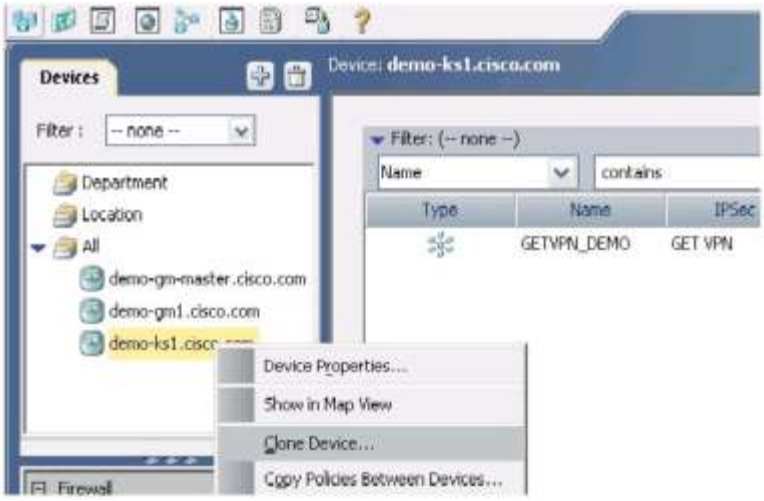
```
hostname demo-ks2
!
enable secret 5 $1$Sc9M$a3JvpcoxdtRCXoI/7JUuV.
!
username demo password lab
!
interface GigabitEthernet0/1
 description Connected to demo-pe1
 ip address 10.5.110.26 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
!
router eigrp 44
 network 10.5.110.24 0.0.0.3
 no auto-summary
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 011F0706
 login
!
```

4.2 Connect New Device to Network with IP Address

Configure the new device with IP address so that configuration can be pushed from CSM. Very minimum configuration is required. Complete running configuration for this step is given in section 4.1.

4.3 Clone Device to Deploy new KS

Select the master KS device “demo-ks1.cisco.com”, right click on it and select “clone device” as follows:



Enter new KS Identity as follows: IP address need to be entered if host name is not published with DNS. After entering required values, click OK.

4.4 Edit Required Values for New KS

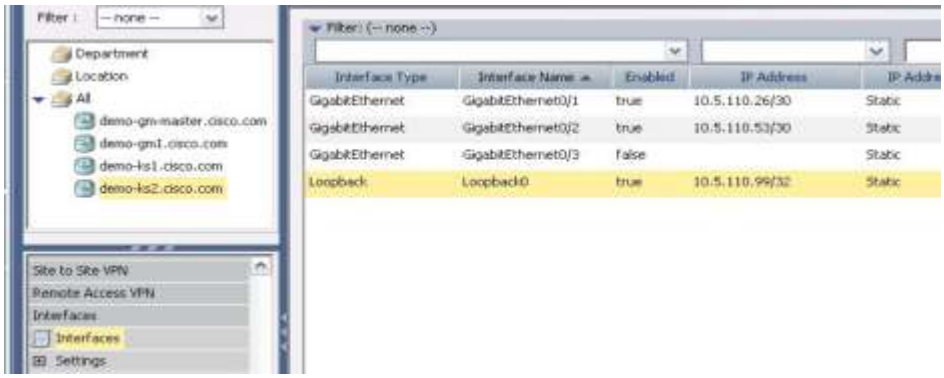
Select demo-ks2 device.

4.4.1 Change Host Name

Select Platform, Device Admin and Hostname. Enter hostname as demo-ks2.

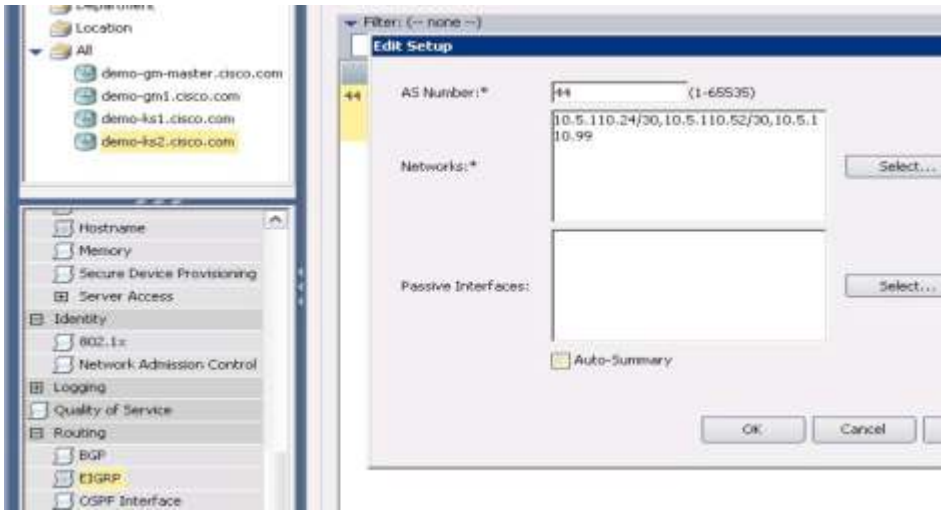
4.4.2 Change Interface IP Addresses

Select Interfaces menu and select Interfaces sub-menu under that. Change IP value for demo-ks2 interfaces as follows: Select each interface and change the IP address.



4.4.3 Change Routing Values

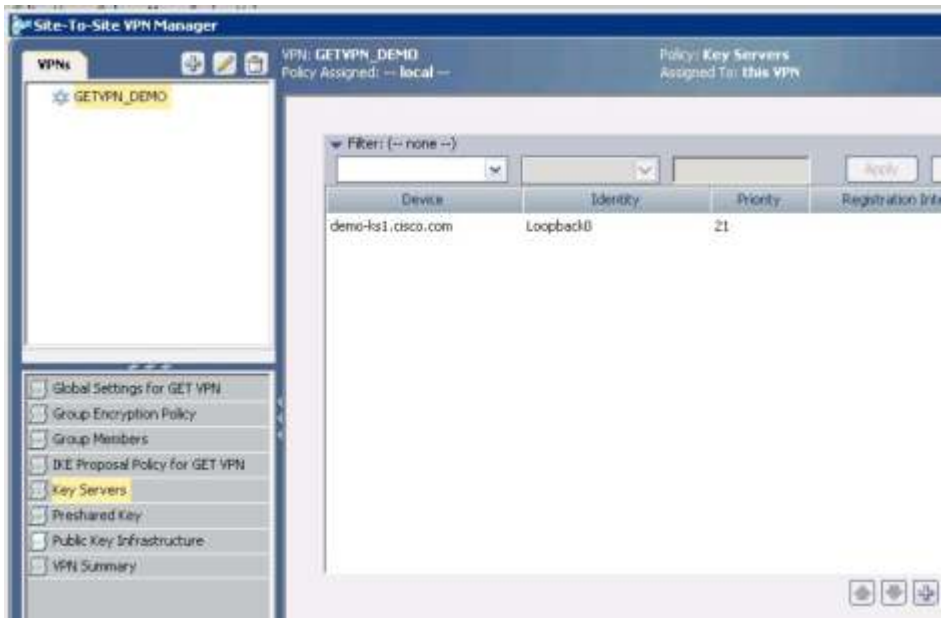
Select Routing and EIGRP menu and edit the routing values for demo-ks2 device as follows:



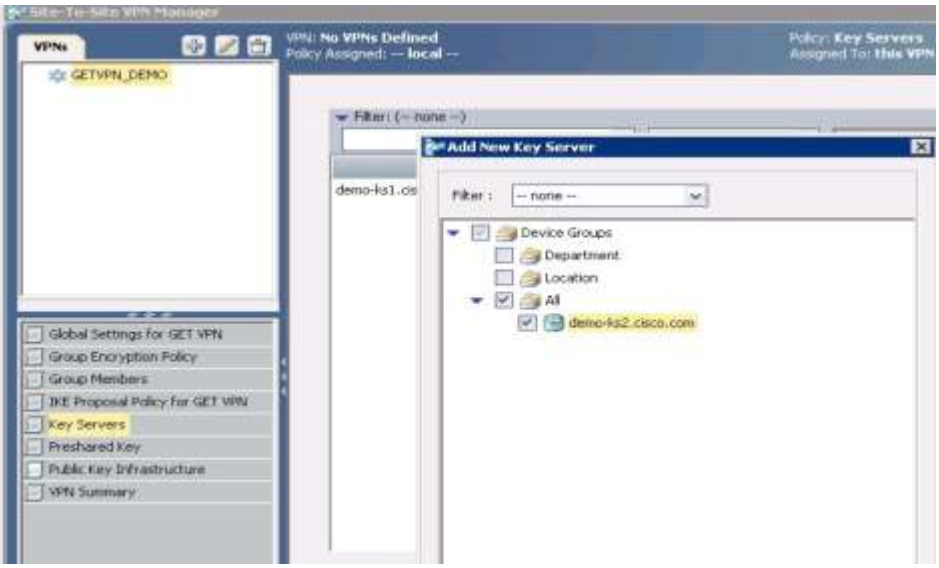
Select File menu and click “submit”.

4.5 Adding New KS to the GETVPN Topology

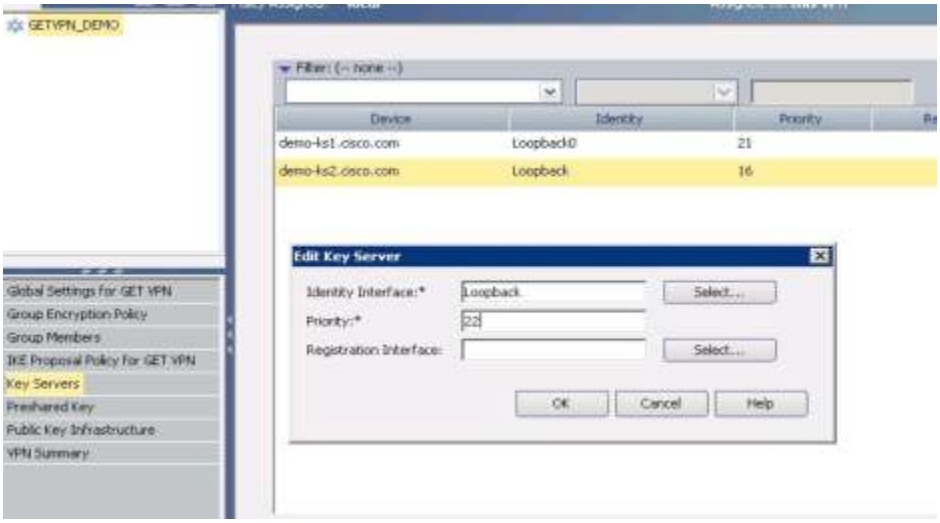
Select “Site-To-Site VPN Manager” icon at the top and select “Key Servers” menu and press “+” button as follows:



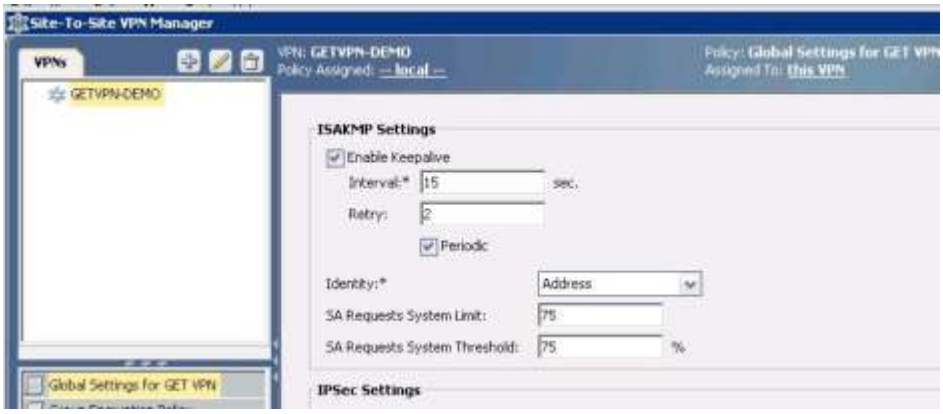
Add new KS by selecting demo-ks2.cisco.com and press OK.



Change the redundancy priority of demo-ks2 to 22 as follows:



Select Global Settings for GET VPN menu, in ISAKMP Settings select Enable Keepalive, set Interval to 15 secs and Retry to 2 secs. Select Periodic.



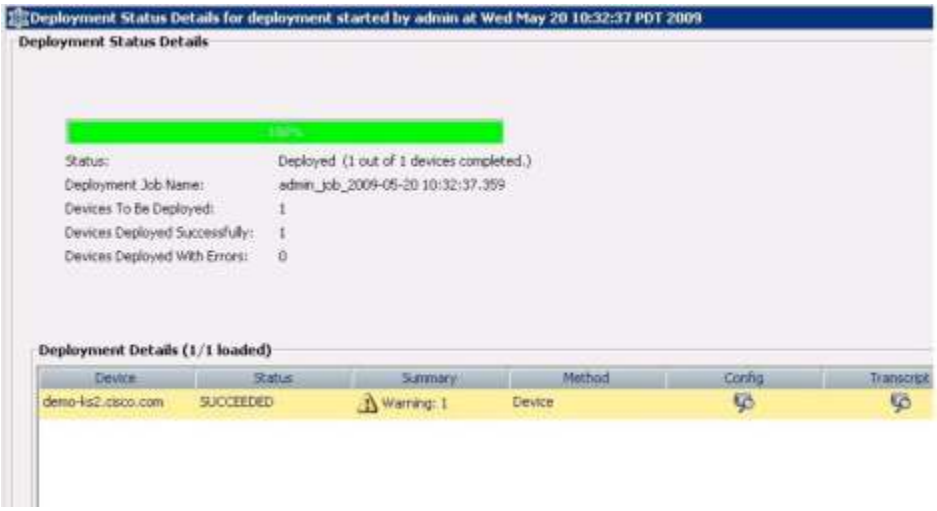
Press Save button. Select File menu and click “submit”.

4.6 Deploy new KS by Pushing Configuration from CSM

From the File menu select “submit and deploy”, select the KS device you want to deploy as follows and press the Deploy button:

4.7 Verify KS Configuration Deployment Status

Verify the demo-ks2 KS deployment status. You should not see any error. New co-op KS should be up and running.



5 Reference Configuration

Complete configuration of devices used in this document is listed below.

5.1 Configuration of demo-gm1

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname demo-gm1
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-22.T
```

```
boot-end-marker
!
logging message-counter syslog
enable password 7 060A0E23
!
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
clock timezone pst -8
clock summer-time pst recurring
!
dot11 syslog
no ip source-route
!
ip cef
!
ip dhcp pool demo
  network 10.5.110.200 255.255.255.248
  domain-name cisco.com
  default-router 10.5.110.201
!
ip domain name cisco.com
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
multilink bundle-name authenticated
!
username demo password 7 060A0E23
archive
 log config
 hidekeys
!
crypto isakmp policy 1
 encr 3des
```

```
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 10.5.110.88
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
!
crypto map CSM_CME_GigabitEthernet0/0 local-address Vlan10
crypto map CSM_CME_GigabitEthernet0/0 1 gdoi
 set group GETVPN-DEMO
!
bba-group pppoe global
!
interface GigabitEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.17 255.255.255.252
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 crypto map CSM_CME_GigabitEthernet0/0
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/1/1
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet1/0
 description connected to demo-lac
 no switchport
 no ip address
 ip pim sparse-mode
 ip tcp adjust-mss 1452
```

```
 pppoe enable group global
 pppoe-client dial-pool-number 10
!
interface Vlan10
 ip address 10.5.110.201 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no autostate
!
interface Dialer10
 ip address negotiated
 ip mtu 1492
 ip pim sparse-dense-mode
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer pool 10
 ppp authentication pap
 ppp pap sent-username demo@cisco.com password 7 1042081B
 crypto map CSM_CME_GigabitEthernet0/0
!
router eigrp 44
 network 10.5.110.16 0.0.0.3
 network 10.5.110.200 0.0.0.7
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip pim ssm range 1
ip nat inside source list 10 interface Dialer10 overload
!
access-list 1 permit 239.192.0.0 0.0.255.255
```

```
access-list 1 permit 239.255.0.0 0.0.255.255
access-list 10 permit 10.5.110.200 0.0.0.7
dialer-list 10 protocol ip list 10
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 011F0706
!
end
```

5.2 Configuration of demo-ks1

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname demo-ks1
!
boot-start-marker
boot system disk2:c7200-adventerprisek9-mz.124-22.T
boot-end-marker
!
logging message-counter syslog
logging buffered 100000
enable secret 5 $1$8E1Y$NwMO0BvplO7z7DD1SCx0o.
!
no aaa new-model
no ip source-route
ip cef
!
ip domain name cisco.com
ip multicast-routing
no ipv6 cef
!
multilink bundle-name authenticated
```

```
!
username cisco password 0 getvpn-demo
archive
 log config
 hidekeys
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 10.5.110.99
crypto isakmp key dGvPnPsK address 10.5.110.201
crypto isakmp key dGvPnPsK address 10.5.110.209
crypto isakmp key dGvPnPsK address 10.5.110.217
crypto isakmp keepalive 15 periodic
!
crypto ipsec transform-set aes128 esp-aes esp-sha-hmac
!
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900
 set transform-set aes128
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server local
 rekey algorithm aes 128
 rekey address ipv4 dgvpn-rekey-multicast-group
 rekey lifetime seconds 28800
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa rekeyrsa
 sa ipsec 1
  profile getvpn-profile
  match address ipv4 sa-acl
  replay time window-size 5
 address ipv4 10.5.110.88
 redundancy
  local priority 21
```

```
  peer address ipv4 10.5.110.99
!
interface Loopback0
 ip address 10.5.110.88 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-pe1
 ip address 10.5.110.13 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 description Connected to demo-lns
 ip address 10.5.110.49 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router eigrp 44
 network 10.5.110.12 0.0.0.3
 network 10.5.110.48 0.0.0.3
 network 10.5.110.88 0.0.0.0
 no auto-summary
!
ip forward-protocol nd
ip http server
ip http secure-server
!
ip pim ssm range 1
!
ip access-list extended dgvpn-rekey-multicast-group
```

```
 permit ip any host 239.192.1.190
ip access-list extended sa-acl
 deny  udp any eq 848 any eq 848
 deny  tcp any any eq telnet
 deny  tcp any eq telnet any
 deny  esp any any
 deny  tcp any eq bgp any
 deny  tcp any any eq bgp
 deny  udp any eq isakmp any eq isakmp
 deny  ospf any any
 deny  eigrp any any
 deny  igmp any any
 deny  pim any any
 deny  ip any 224.0.0.0 0.0.255.255
 deny  udp any any eq ntp
 deny  udp any any eq snmp
 deny  udp any any eq syslog
 permit ip any any
!
logging alarm informational
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
end
```

5.3 Configuration of demo-ks2

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

```
hostname demo-ks2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
logging buffered 100000
enable password 7 082D4D4C
!
no aaa new-model
ip source-route
ip cef
!
ip domain name cisco.com
ip multicast-routing
no ipv6 cef
!
username demo password 7 020A0559
archive
 log config
 hidekeys
!
crypto isakmp policy 6
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 10.5.110.201
crypto isakmp key dGvPnPsK address 10.5.110.88
crypto isakmp key ****** address 10.5.110.209
crypto isakmp key ****** address 10.5.110.217
crypto isakmp keepalive 15 periodic
!
crypto ipsec transform-set CSM_TS_1 esp-aes esp-sha-hmac
!
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900
 set transform-set CSM_TS_1
```

```
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server local
 rekey algorithm aes 128
 rekey address ipv4 CSM_REKEY_MULTICAST_ACL_1
 rekey lifetime seconds 28800
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa rekeyrsa
 sa ipsec 1
  profile getvpn-profile
  match address ipv4 sa-acl_1
  replay time window-size 5
 address ipv4 10.5.110.99
 redundancy
  local priority 22
  peer address ipv4 10.5.110.88
!
interface Loopback0
 ip address 10.5.110.99 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-pe1
 ip address 10.5.110.26 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 description Connected to demo-lns
 ip address 10.5.110.53 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
```

```
 media-type rj45
 no negotiation auto
!
router eigrp 44
 network 10.5.110.24 0.0.0.3
 network 10.5.110.52 0.0.0.3
 network 10.5.110.99 0.0.0.0
 no auto-summary
!
ip forward-protocol nd
ip http server
ip http secure-server
!
ip pim ssm range 1
!
ip access-list extended CSM_REKEY_MULTICAST_ACL_1
 permit udp host 10.5.110.99 eq 848 host 239.192.1.190 eq 848
 permit udp host 10.5.110.88 eq 848 host 239.192.1.190 eq 848
ip access-list extended sa-acl_1
 deny  udp any eq 848 any eq 848
 deny  tcp any any eq telnet
 deny  tcp any eq telnet any
 deny  esp any any
 deny  tcp any eq bgp any
 deny  tcp any any eq bgp
 deny  udp any eq isakmp any eq isakmp
 deny  ospf any any
 deny  eigrp any any
 deny  igmp any any
 deny  pim any any
 deny  ip any 224.0.0.0 0.0.255.255
 deny  udp any any eq ntp
 deny  udp any any eq snmp
 deny  udp any any eq syslog
 permit ip any any
!
access-list 1 permit 239.192.0.0 0.0.255.255
```

```
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 0507070D
 login
!
end
```

6 Glossary

The following list describes acronyms and definitions for terms used throughout this document:

GETVPN	Group Encrypted Transport. A scalable VPN using group technology.
CSM	Cisco Security Manager
GDOI	Group Domain of Interpretation, RFC 3547. A group key management system that is complimentary to IKE.
IKE	Internet Key Exchange, RFC 2409. A pair-wise key management system used to negotiation IPsec tunnels.
IPsec	IP Protocol Security, RFC 2401. The common name for a set of protocols that protect IP packets.
ISAKMP	Internet Security Association and Key Management Protocol, RFC 2408. ISAKMP defines payloads for exchanging key generation and authentication data.
SA	Security Association. SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic.
GM	Group Member
KS	Key Server
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
LNS	Layer 2 Network Server
LAC	Layer 2 Access Concentrator
L2TP	Layer 2 Tunneling Protocol

For more information about the Cisco GETVPN, visit http://getvpn.cisco.com/ or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C11-587394-00 03/10