

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

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

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

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.

dentity		
IP Туре;	Static	×
Host Name:	demo-gm1	
Domain Name:	cisco.com	
JP Address:	-	
Display Name:*	demo-gm1.csco.com	
OS Type:*	105 - 12.3+	¥
Transport Protocol:	Telnet	Ŷ
	System Cartest	
iscover Device Set	tings	
Discover;	Policies and Inventory	¥
	Platform Settings	
	Firewall Policies	
	DPS Policies	
	RA VPN Policies	
	Discour Palmes for Securi	

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.

Username:	demo		
Password:*	***	Confirm:*	+++
Enable Password:	** *	Confirm:*	[+++]
TTP Credentials			
	Use Primary Cradentials		
	Usemane:		
	Pataword:		
	Southing		
ITTP Porti	80		
ITTPS Port:	443	Use Def	suit
PS RDEP Model	Use Default (HTTPS)	1	
		and the second	

2.3 Check Device Discovery status

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

		1100		
Status		Discovery completed with warr	ings	
Devices to be discovered:		1		
Deviced	discovered successfully:	1		
Devices	discovered with errors:	0		
	ry Details			
Discove		2	2044	Discovered From
Type	None	SAMALEA	pizer.	

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.

	Test, contacts	
Cisco Secure Cesitos (Router A	Filter- (+ none +-)	💽 Edit Test Object. 🛛 🛛
II Gederitain Pia Objecta PiexConfigs BE Proposals	n wuahtpladdess	None-* Mant0-IP Description: Start 0.1P address oversidable
II Impect Maps	vetual+ttpTeinetAddre	m (3)
al Interface Roles	5 Vian-2P	Devenuence 0 w Number Of Name 1 + Number Of Columns 1+
PSec Transform Sets	Van nask	line in the second s
LDAP Attribute Maps	🤤 vlaninativicni.	10.5.110.201
PRI Engliveras		
Print Forwarding Last	Un VanFreindpAddress	
1 Services	HarMofslpAddens	
-CE Port Lists	vpdrAccospt(NaInL2to	6
5 Services	vpdivAcceptDialinPptp	6
SA Noribura	vpdnClentAccounting	
25. VFN Bookavarts	vpdnClentAuthenticab	ion l
P SS. Whi Calorisation	D vpdvClentAuthentscatz	An opened a second s
311, VTN Geterneys	vpdrClentConfiguration	v4 Category w
SS. WHI Sould Turved Lists	vpdn:GentConfiguration	Inc. PAken Value Override per Device
Tant Oblets	pdnClientConfiguratio	overndes: None Edit
Time Ranges	up vpdsClentConfiguration	m
S Traffic Flows	vpdrClentConfiguration	International Cancel Help
TUNE Groups	u vpdrémabiebriterface	· · · · · · · · · · · · · · · · · · ·
C S S S S S S S S S S S S S S S S S S S	Deplaying: 124 of 124 objects	4

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.

ALCONTRACT -	GETVPN-DEMO		
Description:			
Topology:*	Full Mesh		
IPSec Technology:*	GET VPN	~	
Discover From:*	Config Archive		
	G		
On	Key Server	Group Member Group Member	ber

Press "Next" button.

Select the GM and KS devices as shown below:

Pilker :	none	*		demo-ks1.cisco.co
- 30	evice Groups			n 💽
-	Location		404	i 💽
é	All .			<>
				demo-gm1.cisco.com
			22	
				j

Press "Finish" button.

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

		1000			
Statu	e .	VPN discovery s	uccessful		
Devic	es to be discovered:	2			
Device	es discovered successfully:	2			
Device	es discovered with errors:	0			
Discon	very Details				Processed & co
Type	Name	Severty	State	Capita Bochave	Discovered fro
Discov Type 時	Very Details Name GETVPN-DEMO	Severativ	State VPN discovery successful	Config Andrive	Discovered fire
Type S	GETVPN-DEMO demo-ks1.cisco.com	Severity ©	State VPN discovery successful Parang Device Configuration: Ios	Conflig Archive Conflig Archive	Discovered fro

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:

entionings Sele	ector			
ailable FlexConF	igs:		Selected FlexConfigs:	
Filter : pop				Name
and a Transit	Add FlexConfig	lini		
ASA_add	AC			
ASA_add	Ett			
ASA_com	man Name:* demo-get	vpn-flexconfig	Group:	
ASA_CODY	_in		Type:	henend
ASA_csd_	ima Description:			
ASA_defin	e.(Negate For	
ASA_esta	blist			
ASA_ftp_	moc DCAD (M B		
ASA_gere	irat			
ASA_IP_A	udit			
ASA_MGO	p			
ASA_no_r	out			
ASA_NO_S	the c			
ASA_priv	egr management		*****	
ASA_rout	e m			
ASA_RSA	Ke	Default Yalue	Object Property	Dm., Opti
ASA AVE	ma			
ASA SYSO	pt			
ASA vietu	al			

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 \$VIan10-IP: From the Flexconfig page at the first occurrence of this variable: right click, select "Insert Policy object" menu, then select "Text object", Select VIan10-IP. Text Object Property Selector Window will pop-up. Enter Variable Name as VIan10-IP. All the other places in Flexconfig where you want to use this variable, simply enter \$VIan10-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
Т
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 255.255.248
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 255.255.258.248
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
ī
interface FastEthernet0/1/0
switchport access vlan 10
spanning-tree portfast
ī
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
ı.
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
ī
! 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 255.255.258.248
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.

🕞 deno-gnil cicco.com				
Hostname Menory Societ Device Provision Societ Device Provision Societ Access Memory Societ Access Methods Societ Access	de ResConfig Name:* demoja_fecconfig Description:	Group: Type: Negate For	[Append	* *
Logeng Quality of Service Routing Point Dop Econ Econ Com Com Com Com Com Service Au Service Service	bostname (SID_DOITRANE ip source-route ip oef ip domain name FRVD_DOMAIN_NAME ip multicast-routing no ipv6 cef			
4	15			13

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-pel
 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
ī
#icmd-begin
crypto key import rsa rekeyrsa exportable terminal passphrase
% Enter PEM-formatted public .*| #icmd-cert-begin
----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDr0jfi+oIVG7LAkx0LinTV16+X
BXPG1p82SUsSUsM2zTLwoPmyfpDczFk7Xn3N+dtGqQe/9IN3M+RF0xk/PyM1PGBi
F7ysqjLPjOo8NBreXk7FEhPEp68HJ2jMUH1xBOJeX6XwRXYylEFV1CeFc9enXxvr
5CPLTSYqXk5RuBl14wIDAQAB
----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+YmUIaQ2Q63b2x+c mRMrcMfou2vvg0J4RpuIgY8yKcRERbZRn3WXr+VG41ewbR0JDwgvWYJiAvG5feh4 mawFD0xos1oXZnRV9KKMnkA5NJEvrW0ZRC16t4K446tQ4p81xVzValgQSi/CSoqu UVf4rendHroNrr+f9Go+d4bnBHuKCD0J2YoG+aYsr3YHfi15ezEZiyaaktxTa45q ZKTOAroYPj+RFz61AXCJF0Lt0GrsIwlh+Aq24/CnMhHu6YhJj38/e1WSeaRDzF+Q cN7bAftIpGJvUgY4mer72oB4q0bLnNFlN3kfwTC2s835rK4Ydf9qVlKzpr/gbubb d/p1NUo5jZYWGwvYJPddcR98hmFM9yuj/KqjFa2Liyv148n/AV8Pj+lKkNoGo+j+ 7ya0CxGc17Ury+jJjA7zP22gVBqLSktriiFLrPLj5WHmIVmfitsDF3mIJti17i22 +beNtePWxRq712rTsnL8EjRoX/43JR4sFJmoxiRUgXVwAjR3TisuBR5LqnIhvDbN urUMC8IcHZaOW3jnzCTJ6aGe89tVT2Qy2vrHuZeq7n+zIVMcCavz7ZId0+I1/YPN Hq/+ZuX193q/1s49ChCFKrNOpprvLGZdbTB6Wcku1t93T4c8Tt3pu9aUXL+gHG8D FM+17kLqZ93f+FmA0aEGtFd60Uvr50qQ8ovPm8D3I+5ZEH1avbEPkXcCqV0CNzT0 SEQqZUrxo8r68rzLmfH+Ir2Ifh7zQy1hFs3m1303phENdn61BsMQxg== -----END RSA PRIVATE KEY----quit

```
#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-pel
ip address 10.5.110.22 255.255.255.252
ı.
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
ı
```

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.

P Type:	Statu:
sost Name:	[demo-gm2
onialn Name:	cisco.com
P Address:	-
Asplay Name:*	demo-gm2.cisco.com
	Clone VPN Assignments

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:

	100	10.1 I I I I I I I I I I I I I I I I I I I			337	
		Name:* demo-g	jetvpn-flexcon/ig	Groupt		
Dentes	2 (1)	and the second sec		Type:	Prepend	
Filter : none		Description:		Negate For		
Carpartment		2 C X D	0 86 12			
T AL		hervice times	tamma debug datetime	localtime show-th	ne none	
demo-amil.clico.com		service times	tamps log datetime 1	coltine show time	TODE	
demo-gm2.cisco.com		1				
demo-4s1.osco.com		ana new-model				
🔄 demo-ks2.ciscu.com		10				
Transferration - Contraction (20)		ana authentic	ation ppp default los	cal		
		≣t				
inspector wates	0	and a concept of the test				
arspectormaes El Settings	•	ana session-1	d common			
Brispection males Settings Diansparent Rules	0	ana session-1 clock timezon	d common m pat -8			
Bispecuerreges Settings Transparent Rules Web Filter Rules	•	ana session-1 clock timezon	d common e pat -8			
Dispector reads Settings Transporent Rules Web Piter Rules Jone Based Preval Rules	0	ana session-i clock timezon	d common e pat -8			
Dispector reads Settings Transparent Rules Web Piter Rules Zone Based Preveal Pulse JPS	•	ana session-i clock timezon clock timezon clock f	d comenos e pat -8	Object Report	Den	
Dispector reads Settings Transparent Rules Web Pitter Rules Socie Based Previal Rules JPS NAT	0	ana session-i clock timezon () Variates Name Name	d common e pat -8 Defait Value	Object Property	Dim	
Dispector reads Settings Transparent Rules Wab Pitter Rules Jone Based Prevail Rules JPS NAT Site to Site WPU	C	ana session-i clock timeton () Vadoles Name SV5_DOMAIN_NAME	d common s pat -8 Defait value	Object Property System	- Dim	
Dispector Hoads Settings Transporent Rules Web Pitter Rules Zone Based Prevail Rules IPS NAT Size to Size UPN Remote Access VPN	<	ana session-i clock timeson last summer S <u>Variotics</u> Norm SV5_DOMAIN_NAME Visni0-IP	d common m pat -8 Defail Value / 10.5.110.209	Object Property System FreeForm VLANJO-IP, d	Dam O lata 0	
Inspector reads Settings Transporent Rules Web Pitter Rules Zone Eased Pareval Pulse IPS NAT Ste to Ste UPN Renote Access VPN Unterfaces	e .	ana session-i clock timeton c. valeto	d comeson = pat -8 Default value / 10.5.110.209	Object Property System FreeForm MLANIO-IP-d	Dam O lata 0	
Inspector reads Settings Transporent Rules Web Pitter Rules Zone Based Prawall Pulse JPS NAT Size to Size VPN Arenote Access VPN Untarfaces Platform	c	ana session-i clock timeton clock timeton c valot- valot- Norm Sv5_DOMADA JAME Visni0-IP	d common m pat -8 Defail Velue	Object Property System FreeForm //LANJO-JP.d	0 0 lata 0	

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.

_		
Quère:	Declared (1 oct 11 decises completed)	
Deployment: Job Name:	mars. jpb 2009-02-06 16:53:01.574	
Devices To Be Deployed:	1	
Devices Decloyed Successfully:	1	
Devices Deployed With Errors	0	

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-pel
 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:

Devices	🔁 🗂 D	evice: demo-ks1.cisi	acom		
Filter : - none	•	Filter: (none -	-)		
Department	_	Name	~	contai	ns
a Location		Туре	N	ame	IPSec
✓ () All	cisco.com :om	295	GETVPN,	_DEMO	GET VPN
🕒 demo-ks1.ciscr	Device Pro	perties			
	Show in M	ap View			
	Glone Devi	ice			
F Firewal	Copy Polic	les Between Devices			

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.

demo-gm1.cisco.com	Create a Clone of	"demo-ks1.cisco.com"		×
demo-ks1.cisco.com	New Device's Id	lentity		
	1P Type:	10 mile	14	
	Host Name:	demo-ks2		
*****	Domain Name:	cisco.com		
in the second se	TD Address			
AAA Rules	IP ADD/essi	L.		
Access Rules	Display Name:*	demo-ks2.cisco.com		
Inspection Rules		Clone VPN Assignments		
Settings				
Transparent Rules		OK Cancel	Help	1
Web Filter Rules	-			1
Zone Based Firewall Rules				

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.

Pitter 1 - none - se	Tiker: (none)				
Con Department			¥		~
Cocation	Interface Type	Interface Name -	Erseblett	IF Address	IP Addr
- <u>-</u> Al	GigabitEthernet	GigabitEthernet0/1	true	10.5.110.26/30	Static
demo-gm-master.cisco.com	Ggsbittthemet	Ggabt@themet0j2	true	10.5.110.53/30	Static
demo-gmt.cisco.com	GigabitEthernet	-GigabitEthernet0/3	false		Static
demo-ks2 cisco.com	Loopbeck:	Loopback0	true	10.5.110.99/32	Static
Site to Site VPN					
Penote Access VPN					
Diterfaces					
E Settings					

4.4.3 Change Routing Values

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

Jucebion All	FO	teri (~ none ~) dit Setup		
demo-gm-master.cisco.com demo-gm1.cisco.com	44	AS Number :*	(1-65535)	
demo-ks1.cisco.com			10.5.110.24/30,10.5.110.52/30,10.5.1	
		Networks:*		Select
A Summer Internet				
Menory				
Secure Device Provisioning		Description Industry and		
E Server Access		Property and a does.		1
E Identity				
602.1x			and the second se	
Network Admission Control			Auto-Summary	
E Logging				
Quality of Service				1000
El Routing			OK	Cancel
BGP				s-stuff
S EIGRP				
GSPF Interface				

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:

VPNs V C	VPN: GETVPN_DEMO Policy Assigned: local	Pak Asu	y Key Servers gred for this VPN	1000
	🗢 Filter: (none)			
	×	M		-Acchr -
	Device	Identity.	Priority	Registration Inf
Group Encryption Policy Group Encryption Policy Group Members DE Proposal Policy for GET VPN Key Servers Preshared Key Public Key Infrastructure				

C 2 C VPN: No VPNs Defined VPN CETVPN, DEMO Fiteri (- none -) and Ne w Key Serv demo-ks1.cis fiker: - none -× 💌 🔄 🊙 Device Groups 🛄 🎯 Department Cocation - 🗹 🥥 Al 🕑 🕒 demo-ks2.cisco.com Global Settings for GET VPN Group Encryption Policy Group Members IKE Proposal Policy for GET VPN Key Servers Preshared Key Public Key DVrastructure VEN Summary

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

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

	1 Provide Statistics			-
	Device	Identi	ty Poority	
	demo-ks1.cisco.com	Loopback0	żt	
	demo-ks2.ceco.com	Loopback	16	
and the second se	Priority:*	22		
roup Encryption Policy			Select	
roup Encryption Maley roup Members	Registration Interface:			
oup Encryption Maky oup Members E Proposal Policy for GET VPN In Servers	Registration Interface:			
oup Encryption Policy oup Members E Proposel Policy for GET VPN In Servers Inhared Key	Registration Interface:	OK	Cancel Help	
Incup Encryption Policy Incup Members 2: Propensil Policy For GET VPM ey Servers unihared Key ublic Key Infrastructure	Registration Interface:		Cancel Help	

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.

VPNs	828	VPN: GETVPN-DEMO Policy Assigned: <u>— local —</u>		Policy: Global Settings for GET VP Assigned To: <u>this VPN</u>
ST OF LANACE	ENO	ISAKMP Settings	_ sec.	
		Identity:* SA Requests System Limit:	Address 75	<u>w</u>
		SA Requests System Threshold:	75	76
Global Setting	s for GET VPN	IPSec Settings		

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:

- =	Changed Dev	vices		
Ē	demo-gm	-maeter.seco.com		
E	🗌 😁 demo-kst	L.cisco.com		
15	🔄 😁 demo-ks2	2.cisco.com		
	Ed	it deploy method	Add o	ther devices
	Ed	R deploy method	Add o	ther devices
I of 4 dev	Ed	it deploy method	Add o	ther devices

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.

har function according to the	tails							
-	_	-						
Sature		Detkwe	d (1 out of 1 devices com	(Jeted.)				
Deployment Job Na	met.	admin to	ab 2009-05-20 10:32:37.	359				
Devices To Be Depl	oved	1						
Devices Deployed Successfully:		1	1					
Devices Deployed	With Errors:	0						
Deployment Details	(1/1 loaded	0						
	8	tatus	Summery	Method		Config	Transcri	
Device	Device St		3	Cariforn		64	12	
Device demo-ks2.ctsco.com	SUCCEEDE	D	A warring: I	DEVICE		40	90	

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-gml
!
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
ı.
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-pel
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
ı.
interface FastEthernet0/1/0
switchport access vlan 10
spanning-tree portfast
!
interface FastEthernet0/1/1
switchport access vlan 10
spanning-tree portfast
ī
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
ı.
interface Vlan10
 ip address 10.5.110.201 255.255.258.248
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
Т
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
L.
ip forward-protocol nd
no ip http server
no ip http secure-server
1
ip pim ssm range 1
ip nat inside source list 10 interface Dialer10 overload
1
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$8E1Y$NwMO0Bvpl07z7DD1SCx0o.
!
no aaa new-model
no ip source-route
ip cef
1
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
Т
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
I.
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-pel
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
I.
ip access-list extended dgvpn-rekey-multicast-group
```

```
Data Sheet
```

```
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
T.
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
I.
interface GigabitEthernet0/1
description Connected to demo-pel
ip address 10.5.110.26 255.255.255.252
ip pim sparse-mode
duplex auto
speed auto
media-type rj45
no negotiation auto
ī
interface GigabitEthernet0/2
description Connected to demo-lns
ip address 10.5.110.53 255.255.252
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
ı.
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
ı.
access-list 1 permit 239.192.0.0 0.0.255.255
```

```
Data Sheet
```

```
!
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:

Group Encrypted Transport. A scalable VPN using group technology.
Cisco Security Manager
Group Domain of Interpretation, RFC 3547. A group key management system that is complimentary to IKE.
Internet Key Exchange, RFC 2409. A pair-wise key management system used to negotiation IPsec tunnels.
IP Protocol Security, RFC 2401. The common name for a set of protocols that protect IP packets.
Internet Security Association and Key Management Protocol, RFC 2408. ISAKMP defines payloads for exchanging key generation and authentication data.
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.
Group Member
Key Server
Point-to-Point Protocol
PPP over Ethernet
Layer 2 Network Server
Layer 2 Access Concentrator
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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco Stadum/Vision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIP, CCIP, CCNP, CCPP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, ILYNX, IOS, IPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Printed in USA

C11-587394-00 03/10