CISCO VALIDATED PROFILE

Enterprise Routing Voice, 4G LTE, and GETVPN

April 2017

Table of Contents

Profile Introduction

Cisco is transforming the network edge with the Cisco ASR1K/ISR4K Series Aggregation Services Routers, a new line of midrange routers that establish a new price-to-performance class offering, benefiting both enterprises and service providers. These routers provide a great opportunity for simplifying the WAN edge and significantly decreasing network-operating expenses. By efficiently integrating a critical set of WAN edge functions such as WAN aggregation, Internet edge services, VPN termination, etc. into a single platform, this solution can help enterprises meet their business objectives by facilitating deployment of advanced service in a secure, scalable, and reliable manner while minimizing the total cost of ownership.

Cisco WAN aggregation solutions distinguish themselves from other solutions by offering multiservice routers with the highest performance, availability, and density for concurrent data, as well as security, voice, and application-acceleration services with the maximum headroom for growth. The solutions feature embedded security, performance, and memory enhancement. High-performance interfaces featuring the latest WAN technologies can help enterprises meet the needs of the most demanding WAN network.

This document covers enterprise solution profiles built with the below features.

Security

The Cisco IOS Group Encrypted Transport VPN (GETVPN) is a tunnel-less VPN technology that provides end-to-end security for network traffic. Cisco IOS GETVPN preserves the original source and destination IP address information in the header of the encrypted packet for optimal routing. It is therefore largely suited for enterprise running over private multiprotocol label switching (MPLS).

Voice

This profile covers basic voice features, media gateway control protocol (MGCP), H323 call flow, Cisco Unified Survivable Remote Site Telephony (SRST), conferencing, and MGCP Foreign eXchange Subscriber (FXS) analog endpoints interoperated with IP phones. Cisco Unifies Communication Manager (CUCM) controls the MGCP endpoint and the IP phones. MGCP enables the remote control and management of voice and data communications devices at the edge of multiservice IP packet networks. MGCP simplifies the configuration and administration of voice gateways and supports multiple (redundant) call agents, eliminating the potential for a single point of failure in controlling the Cisco IOX gateway in the network.

4G LTE

The Cisco 4G LTE solution include standalone wireless routers, modular router plus 4G LTE interface modules, and antennas. Cisco combines the speed, reliability, and rapid deployment benefits of 4G LTE wireless networks with the intelligent routing capabilities of Cisco ISRs. That means that the rich Cisco IOS software service set, long available over landlines, now reaches across the wireless WAN. You get the enhanced quality of service (QoS), security, and other Layer 3 networking services you enjoy with your Cisco landline routers in the mobile WAN. That is unique to the Cisco solution.

Table 1 *Profile feature summary*

Deployment areas	Features
Security	GETVPN GM GETVPN key server (KS) with mixed group COOP KS Group security association GM registration Public Key Infrastructure (PKI)-based authentication Local ACL on GETVPN group member (GM)
Key management	PKI client authentication/enrollment directly to root certification authority (CA) PKI client authentication/enrollment via registration authorities (RA) PKI client authentication/enrollment to Microsoft CA PKI client rollover with root enroll retry with auto enroll when CA not reachable
4G LTE	4G dialer/chat-script NAT over 4G LTE Network mobility (NEMO) mobile routing Proxy mobile IP (PMIP) routing
Voice	MGCP H323 SRST Conferencing
Troubleshooting	Wireshark

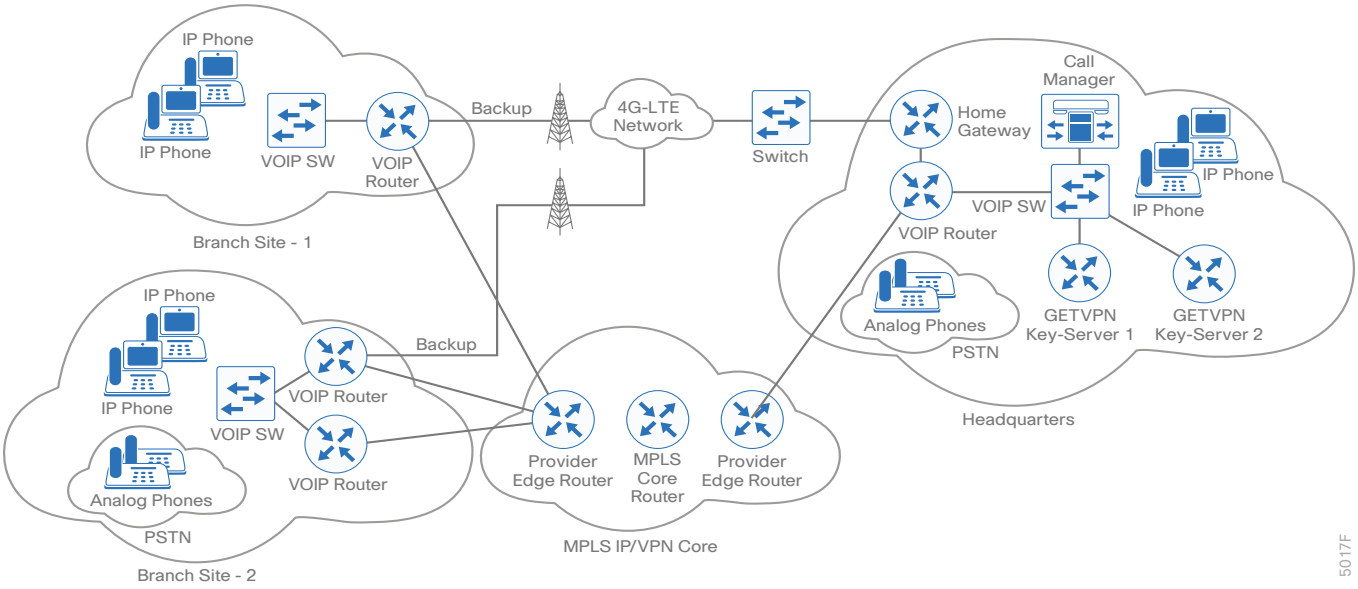
Network Profile

Based on the research, customer feedback, and configuration samples, the profile is designed with a deployment topology that is generic and can easily be modified to fit any specific deployment scenario. This profile caters to Enterprise network deployments.

TOPOLOGY DIAGRAM

Figure 1 show the topology that is used for the validation of the profile. The left portion of the topology represents the deployment where ISR4K is used as branch routers and voice gateways. The right portion of the topology represents a data center deployment with ASR1K along with CUCM, GETVPN, key servers, and root CA server.

Figure 1 *Topology overview*



HARDWARE & FEATURE SPECIFICATIONS

This section describes the 3-D feature matrix where the hardware platforms are listed along with their place-in-network (PIN) and the relevant Vertical deployment.

Key Vertical Features

Table 2 defines the 3-D hardware, PIN, and the features deployed.

Table 2 3-D feature summary with hardware and PIN

Deployment layer (PIN)	Platforms	Critical vertical features
Key server	Primary co-operative (COOP) KS- ISR3945e/ISR4451 Secondary COOP KS- ISR3945e/ISR4331	Group Domain of Interpretation (GDOI) group Traffic encryption key (TEK)/key encryption key (KEK) lifetime COOP KS GM registration PKI-based authentication Local ACL on GETVPN GM
Group member	ISR4431 ISR4451 ISR4331 ISR4351 ISR3945 ISR2921	GDOI PKI-based authentication Local ACL/fail-close ACL GM routing awareness
MPLS-core	PE1- ASR1002 PE2- ASR1002 P - ISR3945	MPLS Border gateway protocol Open shortest path first protocol
Certificate authority	IOS CA Server - ISR4431 Microsoft Root CA Server	PKI
Voice	ISR4331 ISR4431 ISR4351 ISR4451 ISR2951 ISR3945	MGCP SRST H323 Digital signal processor farm

Hardware Profile

Table 3 defines the set of relevant servers, test equipment, and endpoints that are used to complete the end-to-end deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complements the actual physical topology shown in Figure 1.

Table 3 Hardware profile of servers and endpoints

HW and VM	Software Version	Description
Ixia	IxNetwork and IxExplorer Version X	Generate traffic streams
Pagent	Cisco IOS	Generate traffic streams
CUCM	Version 9.1.x	CUCM server for mapping IP phones and MGCP FXO/FXS analog phones
Windows Server	Window Server 2012	Root CA
Cisco Unified IP Phones 796x, 884x, 886x, 896x	Cisco Unified IP Phones	Endpoints
Analog phones	–	Plain old telephone service phones

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 4 below are executed using the topology shown in Figure 1, along with the test environment shown in Table 3, previously explained in this document.

Images are loaded on the devices under test via tftp server using the management interface.

To validate a new release, the network topology is upgraded with the new software image with existing configuration composed of the use cases and relevant traffic profile. The addition of new use cases acquired from the field or customer deployment are added on top of the existing configuration.

With respect to longevity for this profile, setup, the CPU, and memory use/leaks are monitored during the validation phase. Furthermore, to test the robustness of the software release and platform under test, negative events are triggered during the use case execution process.

USE CASES

Table 4 describes the use cases that were executed as a part of this profile testing. These use cases are divided into buckets of technology areas to show the complete coverage of the deployments scenarios.

These technology buckets are composed of system upgrade, security, network service, monitoring & troubleshooting, simplified management, and system health monitoring, along with system and network resiliency.

Table 4 *List of use case scenarios*

No	Focus area	Use cases
System upgrade		
1	Upgrade	Network administrator should be able to perform router upgrade and downgrade between releases seamlessly. ▪ All of the applied configurations should be migrated seamlessly during the upgrade/downgrade operation
Security		
2	ACL/policy	Network admin wants to have routing bases on the crypto status. ▪ Inspect traffic based on types of traffic or source/destination address ▪ Crypto policy is applied correctly, GMs registration is successful, and traffic passes through seamlessly.
3	Fail-Close ACL	Network admin wants to drop unencrypted traffic. ▪ Apply Fail-Close ACL on the WAN interface of the GM. Traffic between the GMs drops until the both GMs register successfully.

Table 4 continued

Network services		
4	4G LTE	Network admin ensures that the 4G-LTE connectivity and services on top of LTE are functioning correctly. ▪ Verify 4G/LTE connections on the DUT ▪ Verify the chat script is defined for the data cell and applied to the async line ▪ Verify dynamic NAT translation is functioning correctly ▪ Verify NEMO functionality ▪ Verification of PMIP routing over 4G LTE
5	Voice	Network admin wants to ensure that the voice call flow, conferencing, Call Manager features and basic VoIP features are functioning correctly. ▪ Verify mediate gateway control protocol functionality ▪ Verify H323 and session initiation protocol (SIP) call flow functionality ▪ Voice gateways ▪ Conference bridges ▪ IP telephones with remote-site survivability ▪ Session initiation protocol and skinny client control protocol signaling ▪ Verify conferencing ▪ Voice call manager ▪ Basic call processing (dial plan) ▪ CUCM features verification
6	PMIP over 4G LTE	Network admin wants to ensure that the PMIP over 4G LTE functionality is working correctly. ▪ MAG binding is established correctly ▪ Tunnel template is used to build PMIP tunnel ▪ Mobile networks are being advertised correctly ▪ Mobile network advertisement is updated automatically when PMIP configuration changes ▪ PMIP statistics show correct registration information

Table 4 continued

7	NEMO over 4G LTE	Network admin to verify that network mobility functionality over 4G LTE is working correctly. ▪ Mobile IP enabled on the router ▪ Mobile networks are being advertised ▪ Mobile router is registered ▪ Cellular interface has a single tunnel collocated care-of-address for roaming ▪ Mobile networks advertised by the mobile router are learned by the headend router
8	NAT over 4G LTE	Network admin to verify NAT functionality over 4G LTE. ▪ Inside local address should be translated to inside global address when the traffic from the LAN is going out to the Internet/WAN. The return traffic from WAN to LAN should always be directed to the inside global address of the inside hosts
9	QOS over 4G LTE	Network admin needs to enhance the user experience by ensuring traffic and application delivery using QoS policies over 4G LTE interface. ▪ Traffic types: VoIP, Data
10	GETVPN GM Registration	Network admin to verify GETVPN GM registration functionality. ▪ Verify GM registration to KS ▪ Verify GM registration to second KS in the list when first is not reachable ▪ Verify TEK, KEK, ACL downloads ▪ Traffic validation between GMs
11	GETVPN COOP KS	Network admin to verify KS COOP functionality. ▪ Verify COOP roles and statuses on primary and secondary ▪ Swap the roles of primary and secondary ▪ Bring down COOP and bring it back up ▪ Verify TEK, KEK, policy generation and policy sync between COOP KSs ▪ Verify COOP failure with IKEv2 profile mismatch

Table 4 continued

12	PKI	Network admin wants to ensure PKI enrollment/authentication is functioning correctly. ▪ Client authorization and enrollment directly to root-CA ▪ Client authorization and enrollment via RA ▪ Client authorization and enrollment directly to sub-CA ▪ Client authorization and enrollment directly to Microsoft CA ▪ Auto-enrollment to root-CA ▪ Auto-enrollment to sub-CA ▪ Auto-enrollment via RA ▪ Enrollment retry with auto enrollment when CA not reachable ▪ Verify GDOI registration failure when certificate is revoked ▪ Verify GDOI registration failure when certificate is invalid
Monitoring & troubleshooting		
13	Wireshark	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ Wireshark–data plane & control plane capturing
14	Show CLI	Enable IT admins to determine network resource use and capacity planning by monitoring encrypted traffic flows using show CLIs.
Simplified management		
15	Manageability	Simplified network troubleshooting and debugging for IT admin. ▪ Monitor network for alarms, syslog, and traps
System health monitoring		
16	System health	Monitor system health for CPU use, memory consumption, and memory leaks during testing.
System & network resiliency, robustness		
17	System resiliency	Verify system level resiliency during the following events. ▪ Online insertion and removal (OIR) ▪ Power failure ▪ WAN/LAN interface flaps ▪ SIP/SPA reload/OIR
18	Network resiliency	Verify that the system holds well during a network-level resiliency. ▪ GETVPN KS aggressive rekey

Table 4 continued

19	Negative events, triggers	Verify that the system holds well and recovers to working condition after the following negative events are triggered. ▪ Configuration changes: add/remove configuration snippets, configuration replace ▪ Clear counters, clear routes ▪ Routing protocol interface flap ▪ IPsec, GDOI events such as clear gdoi session, clear sa counters, modify KS ACL on the fly

Appendix A: References

CCO Configuration Guides:

GETVPN Deployment Guides

http://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_1_0_External.pdf

http://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/deployment_guide_c07_554713.html

Cisco 4G LTE Software Configuration and Deployment

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/ehwic-4g-ltesw-book.html#con_1427426

http://www.cisco.com/c/dam/en/us/td/docs/routers/access/interfaces/software/deployment/guide/c07-731484-00-ngewan.pdf

Cisco Voice Configuration Library

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

MGCP Configuration

http://www.cisco.com/c/en/us/td/docs/ios/voice/cminterop/configuration/guide/12_4t/vc_12_4t_book/vc_ucm_mgcp_gw.pdf

Appendix B: Configuration Snippets

This appendix contains sample configuration snippets to give you a general idea about the configuration used in some of the use cases. Your actual configuration would require further customization for actual deployments. For detailed configuration options/best practices, refer to the CCO documentation.

CERTIFICATE AUTHORITY

```
crypto pki server CISCO-IOS-CA
 database level complete
 no database archive
 issuer-name CN=CISCO-IOS-CA.cisco.local L=SanJose St=CA C=US
 grant auto
 lifetime certificate 730
 lifetime ca-certificate 1095
 enrollment url http://10.224.8.2:80
 database url crl nvram:
crypto pki server CISCO-IOS-CA
 no shutdown
```

4G LTE

```
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!The chat script used to make a call!
!
interface GigabitEthernet0/1/0
switchport access vlan 18
!switch port part of LAN to connect local user
!
interface GigabitEthernet0/1/1
no ip address
!
interface GigabitEthernet0/1/2
no ip address
!
interface Cellular0/0/0
 ip address negotiated
 no ip unreachables
```

```
 ip nat outside
! NAT enabled
load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 2
 dialer-group 2 !>>dialer group number must match the dialer list number
 !
interface Vlan18
ip address 192.168.18.1 255.255.255.0
ip nat inside
!Vlan 18 is used as LAN interface and traffic from entering via this ! !inter-
face is NAT'ed
!
ip nat inside source list 2 interface Cellular0/0/0 overload
!NAT statement to match the NAT traffic as per access-list 2
ip route 0.0.0.0 0.0.0.0 Cellular0/0/0
!Default route pointing to the cellular interface
!
dialer watch-list 2 ip 5.6.7.8 0.0.0.0
dialer watch-list 2 delay route-check initial 60
dialer watch-list 2 delay connect 1
!
access-list 1 permit any
! define what traffic can trigger the dialer
access-list 2 permit 192.168.18.0 0.0.0.255
dialer-list 1 protocol ip list 1
!associate acl 1 to dialer-list 1
!
line 0/0/0
!line associated with cellular 0/0/0
script dialer lte
! "lte" matches to dialer string and the chat-script name
modem InOut
!
```

MOBILE IP

```
!
hostname mobile-router
!
router mobile
!this commands turns on the mobile ip functionality on the router


ip route 192.171.187.187 255.255.255.255 Cellular0/1/0
ip route 223.255.0.0 255.255.0.0 1.3.0.1
!
ip mobile secure home-agent 66.174.185.193 spi decimal 256 key ascii NeMo algo-
rithm hmac-md5
!This statement defines the encryption details and authentication using !ascii
value. The ascii value must match to that of the HA configuration on !the HQ
side router


ip mobile router
 address 1.2.3.4 255.255.255.0
 collocated single-tunnel
 home-agent 66.174.185.193
 mobile-network Loopback1
 mobile-network Loopback2
 template Tunnel434
 register retransmit initial 2000 maximum 2000 retry 2
 register extend expire 40 retry 10 interval 4
 register lifetime 180
 reverse-tunnel
 tunnel mode gre
!
```

PROXY MOBILE IP

```
! PMIP Domain and MAG Configuration
!
ipv6 mobile pmipv6-domain 4Gsystest
 replay-protection timestamp window 255
 encap udptunnel
 lma pmip-lma
```

```
  ipv4-address 192.171.187.188
 mobile-map MobileMAP 10
  match access-list HomeACL
  set link-type CELL-C4451 NULL
 mobile-map MobileMAP 30
  match access-list LocalACL
  set link-type CELL-C4451 NULL
 nai 4Gnai-C4451
  lma pmip-lma

ipv6 mobile pmipv6-mag mag3 domain 4Gsystest
 tunnel-template Tunnel435
 heartbeat interval 60 retries 2 timeout 60
 heartbeat interval 300 retries 1 label CELL-C4451 timeout 300
 address dynamic
  roaming interface Cellular0/2/0 priority 1 egress-att LTE label CELL-C4451
 replay-protection timestamp window 255
 interface Loopback0
 lma pmip-lma 4Gsystest
  ipv4-address 192.171.187.188
 logical-mn 4Gnai-C4451
  mobile network Loopback10 label LOOP10
  reverse-tunnel route ipv4 0.0.0.0 0 210
  reverse-tunnel route ipv4 10.224.200.14 32
!  home interface Loopback0

! Tunnel template for PMIP
!
interface Tunnel435
 description TEMPLATE FOR 4G CONFIGURATION
 no ip address
 ip mtu 1300
 ip flow monitor FLOW-MONITOR-1 input
 ip nat outside
 ip virtual-reassembly in
 ip tcp adjust-mss 1200
```

```
 ip policy route-map clear-df
 tunnel path-mtu-discovery
 crypto map GETVPN-MAP-1
end

! LMA Configuration

ipv6 mobile pmipv6-domain 4Gsystest
 replay-protection timestamp window 255
 encap udptunnel
 nai 4Gnai-C4451
  network 4Gnet-C4451
ipv6 mobile pmipv6-lma pmip-lma domain 4Gsystest
 address ipv4 192.171.187.188
 heartbeat interval 300 retries 1 label CELL-C4451
 heartbeat interval 60 retries 2
 bce maximum 128000
 replay-protection timestamp window ignore
 dynamic mag learning
 network 4Gnet-C4451
  pool ipv4 v4pool-C4451 pfxlen 24
  mobile-network pool 20.20.0.0 pool-prefix 16 network-prefix 32
  mobile-network pool 221.221.0.0 pool-prefix 16 network-prefix 32
!
```

VOICE

```
!
controller T1 0/0/0
 cablelength long 0db
 pri-group timeslots 1-24 service mgcp
!
interface Serial0/0/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
```

```
 isdn bind-l3 ccm-manager
 no cdp enable
!
voice-port 0/0/0:23
!
!
!
!
!
mgcp
mgcp call-agent 10.224.10.2 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode cisco
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
no mgcp package-capability res-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp validate domain-name
mgcp fax t38 inhibit
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
ccm-manager music-on-hold
!
ccm-manager mgcp
no ccm-manager fax protocol cisco
ccm-manager config server 10.224.10.2
ccm-manager config
```

```
!
dial-peer voice 1 pots
 destination-pattern 2001
!
dial-peer voice 2 pots
 destination-pattern 2002
!
dial-peer voice 3 pots
 destination-pattern 2003
!
dial-peer voice 4 pots
 destination-pattern 2004
!
dial-peer voice 5 pots
 destination-pattern 1...
 direct-inward-dial
 forward-digits all
!
dial-peer voice 2000 voip
 destination-pattern 1T
 session target ipv4:10.224.6.1
!
!
!
call-manager-fallback
 max-conferences 8 gain -6
 transfer-system full-consult
 limit-dn 7960 3
 limit-dn 7962 3
 limit-dn 8945 3
 ip source-address 10.224.2.1 port 2000
 max-ephones 50
 max-dn 50
 dialplan-pattern 1 .... extension-length 4
 keepalive 20
 default-destination 1001
 time-format 24
!
```

GETVPN

GETVPN Policy Configuration

```
crypto isakmp policy 11
 encr aes
 group 2
!
crypto gdoi group GETVPNGROUP
 identity number 11111
 server address ipv4 10.224.21.2
 server address ipv4 10.224.22.2
!
!
crypto map GDOIMAP local-address Loopback0
crypto map GDOIMAP gdoi fail-close
crypto map GDOIMAP 11 gdoi
 set group GETVPNGROUP
!
! Apply on Tunnel bound to 4G LTE Cellular Interface
!
interface Tunnel434
 no ip address
 crypto map GDOIMAP
!
```

GETVPN key Server - Primary

```
!
crypto isakmp policy 11
 encr aes
 group 2
!
!
crypto ipsec transform-set AES128-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto ipsec profile IPSEC_PROFILE
```

```
 set security-association lifetime seconds 7200
 set transform-set AES128-SHA
!
!
crypto gdoi group GETVPNGROUP
 identity number 11111
 server local
  rekey authentication mypubkey rsa Cisco123
  rekey transport unicast
  sa ipsec 11
   profile IPSEC_PROFILE
   match address ipv4 getvpn-acl
   replay counter window-size 64
   no tag
  address ipv4 10.224.21.2
  redundancy
   local priority 100
   peer address ipv4 10.224.22.2
!
!
ip access-list extended getvpn-acl
 deny   udp any eq 848 any
 deny   udp any any eq 848
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   eigrp any any
 deny   ospf any any
 deny   udp any eq rip any eq rip
 deny   tcp any eq bgp any eq bgp
 deny   tcp any eq 22 any eq 22
 deny   tcp any eq 22 any
 deny   udp any eq snmp any eq snmp
 deny   udp any eq snmptrap any eq snmptrap
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 permit ip any any
!
```

GETVPN Key Server - Secondary

```
crypto isakmp policy 11
 encr aes
 group 2
crypto isakmp key COOPKEY address 10.224.21.2
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set AES128-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto ipsec profile IPSEC_PROFILE
 set security-association lifetime seconds 7200
 set transform-set AES128-SHA
!
!
crypto gdoi group GETVPNGROUP
 identity number 11111
 server local
  rekey authentication mypubkey rsa Cisco123
  rekey transport unicast
  sa ipsec 11
   profile IPSEC_PROFILE
   match address ipv4 getvpn-acl
   replay counter window-size 64
   no tag
  address ipv4 10.224.22.2
  redundancy
   local priority 10
   peer address ipv4 10.224.21.2
!
!
ip access-list extended getvpn-acl
 deny   udp any eq 848 any
 deny   udp any any eq 848
 deny   tcp any eq bgp any
```

```
 deny   tcp any any eq bgp
 deny   eigrp any any
 deny   ospf any any
 deny   udp any eq rip any eq rip
 deny   tcp any eq bgp any eq bgp
 deny   tcp any eq 22 any eq 22
 deny   tcp any eq 22 any
 deny   udp any eq snmp any eq snmp
 deny   udp any eq snmptrap any eq snmptrap
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 permit ip any any
!
```

Please use the feedback form to send comments and suggestions about this guide.

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.