Cisco Virtual Office:
Converged Virtual Private Network

Deployment Guide

Introduction

This white paper provides detailed design and implementation information relating to the deployment of Converged VPN with the Cisco® Virtual Office.

Please refer to the Cisco Virtual Office overview (http://www.cisco.com/go/cvo) for more information about the solution, its architecture, and all of its components.

This document shows how to configure the Cisco Virtual Office VPN headend routers. Three types of VPN technologies are configured in the same headend to handle multiple methods of connecting to the corporate network: Dynamic Multipoint VPN (DMVPN) for teleworkers and small-office sites, Easy VPN for mobile VPN client users, and Secure Sockets Layer (SSL) VPN for SSL-based mobile users.

With the Cisco Converged VPN solution, you can consolidate all possible VPN deployment types in one headend design. This consolidation can lower your total cost of ownership (TCO) because it helps advance standardization of network infrastructure for achieving efficient networks.

The document provides three configuration samples for the most common VPN headend scenarios:

- Single hub: Cisco 3800 Integrated Services Routers or Cisco 7200 Series Routers
- High-concentration hub with integrated encryption plus a server farm: Cisco Catalyst® 6500 Series Switches with high-performance encryption cards plus a server farm consisting of Cisco 7200 Series Routers
- High-concentration hub with distributed encryption plus a server farm: Cisco Catalyst 6500 Series Switches plus a server farm consisting of Cisco 7200 Series Routers

Platforms and Images

Images based on Cisco IOS® Software Release 12.4(15)T are recommended for headend routers.

The VPN headend router can be one of the following:

- Cisco 3800 Integrated Services Router with a VPN encryption card (AIM-VPN/SSL-3)
- Cisco 7206VXR Router with a Cisco VPN Services Adapter (VSA) encryption card and Cisco 7200 Series NPE-G2 Network Processing Engine
- Cisco Catalyst 6500 with a server-load-balancing (SLB) design and a server farm consisting of Cisco 7206 Routers: The Cisco Catalyst 6500 uses the Cisco Catalyst 6500 Series Supervisor Engine 720 and the Cisco IP Security (IPsec) VPN Shared Port Adapter (SPA) (in the scenario with integrated encryption) and runs Cisco IOS Software Release 12.2(18)SXH2 or later

For SSL VPN full-tunnel mode, you need to install a client package on the hub. AnyConnect Version 2.2.0128 or later is recommended. Please refer to the SSL VPN guide available at http://www.cisco.com/go/cvo for more information about where to get the extra SSL files and how to install them.

Converged VPN Solution

This section shows how to deploy the three main VPN solutions in one hub.

Following is a summary of each of the technologies:

- Dynamic Multipoint VPN: DMVPN provides a full end-to-end VPN solution that allows for dynamic direct, secure connections between remote sites (that is, dynamic spoke-to-spoke tunnel) and full access to corporate services, including multicast forwarding support. For this technology, a Cisco IOS Software router is required at the remote site.
- Enhanced Easy VPN: Enhanced Easy VPN provides a point-to-point secure connection between a remote device and a corporate headend. This technology simplifies the configuration for hardware-based clients, and supports software version clients. For this technology, the remote site can have either a Cisco IOS Software router or a PC running Windows, Mac OS, or Linux.
- SSL VPN: SSLVPN provides secure access to corporate servers from any PC, even if it is connecting from a public location. This technology uses an SSL-enabled web browser to establish an SSL tunnel back to the corporate securely. For this technology, the remote site can be any mobile devices that have Cisco AnyConnect clients available.

In addition to the VPN configuration, you need to provision other services before you can use the VPN:

- Public key infrastructure (PKI) using Cisco IOS Certificate Server or other Certificate Authority
- Authentication, authorization and accounting (AAA) using Cisco Secure Access Control Server (ACS) or other AAA servers

Please refer to the respective guides at http://www.cisco.com/go/cvo for more information.

This document then shows the full configuration that you can use to combine DMVPN with Enhanced Easy VPN and SSL VPN, all in the same hub. For Enhanced Easy VPN, two profiles are configured: one for PKI and one for preshared keys.

Each VPN configuration is shown with different formatting. The rest of the configuration is shared by all.

Following are some notes about the configuration:

- DMVPN and Enhanced Easy VPN can use the same PKI certificate server, or they can each use a different one. For Enhanced Easy VPN, the spokes need to have the subject name OU field set to match the Easy VPN group name.
- When the same WAN-facing interface is shared by Enhanced Easy VPN and DMVPN, you must use the same cryptography profile for protecting both VPNs. The “shared” keyword is used to achieve this objective under the tunnel command. For example:

```
tunnel protection ipsec profile my-profile shared
```

The following Converged VPN headend configuration sample is valid for a Cisco 3845 Integrated Services Router and a Cisco 7206 Router. Only interface names are different from one platform to the other.

Converged VPN Configuration for Cisco 3800 and Cisco 7206

DMVPN
ENHANCED EASY VPN
SSL VPN

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname converged-vpn-hub
!
boot-start-marker
boot-end-marker
!
enable secret <removed>
!
aaa new-model
!
!
aaa group server radius EzVPN-Users
 server-private 10.99.99.6 auth-port 1812 acct-port 1813 key <removed>
 ip radius source-interface Loopback0
!
!!! This AAA group is used to authenticate device's PKI certificates
!!! against their respective AAA profile
!
aaa group server radius pki-aaa-server
 server-private 10.99.99.6 auth-port 1812 acct-port 1813 key <removed>
!
aaa group server radius SSLVPN-Users
 server-private 10.99.99.5 auth-port 1812 acct-port 1813 key <removed>
 ip radius source-interface Loopback1
!
aaa authentication login default local group SSLVPN-Users
aaa authentication login admin group tacacs+ enable
aaa authentication login easyVPN local group EzVPN-Users
aaa authorization exec default none
aaa authorization network easyVPN local group EzVPN-Users
aaa authorization network pkiaaa group pki-aaa-server
!
aaa session-id common
!
!
clock timezone pst -8
```

```
clock summer-time pdt recurring
no ip source-route
ip cef
!
ip domain name cisco.com
ip name-server 172.16.0.10
ip multicast-routing
!
crypto pki trustpoint verisign
 enrollment terminal
 fqdn none
 subject-name cn=web-vpn-server.cisco.com,o=Cisco
Systems,c=US,st=California
 revocation-check crl
 rsakeypair web-vpn-server.cisco.com
!
crypto pki trustpoint dmvpn-pki-server
 enrollment url http://dmvpn-pki-server:80
 serial-number
 ip-address none
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
!
crypto pki trustpoint easyvpn-pki-server
 enrollment url http://easyvpn-pki-server:80
 serial-number
 ip-address none
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
!
!
!
crypto pki certificate map 1 10
 subject-name co easyvpn-pki-group
!
crypto pki certificate chain verisign
 certificate <removed>
 certificate ca <removed>
crypto pki certificate chain dmvpn-pki-server
 certificate ca <removed>
 certificate <removed>
crypto pki certificate chain easyvpn-pki-server
 certificate <removed>
 certificate ca <removed>
!
!
```

```
crypto isakmp policy 10
 encr 3des
 group 2
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
crypto isakmp xauth timeout 10
!
crypto isakmp client configuration group pki-group
 dns 172.16.10.120 172.16.10.183
 wins 172.16.10.28 171.16.10.87
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn-split-tunnel
 save-password
 backup-gateway 172.16.0.2
 banner ^C
You are connecting to a Converged VPN server using PKI
^C
!
crypto isakmp client configuration group pre-shared-group
 key EasyVPN-Secret-KEY
 dns 172.16.10.120 172.16.10.183
 wins 172.16.10.28 171.16.10.87
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn-split-tunnel
 save-password
 firewall are-u-there
 backup-gateway 172.16.0.2
 banner ^C
You are connecting to a Converged VPN server using Pre-shared
 ^C
crypto isakmp profile pre-shared-group
   description PSK group
   match identity group pre-shared-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 3
crypto isakmp profile pki-group
   description PKI group
   ca trust-point dmvpn-pki-server
```

```
   match identity group pki-group
   match certificate 1
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 2
!
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport require
!
crypto ipsec profile my-profile
 set transform-set t1
!
interface Tunnel1
 bandwidth 2000
 ip address 10.250.250.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip nhrp map multicast dynamic
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 7
 ip summary-address eigrp 7 10.100.8.0 255.255.248.0 5
 ip summary-address eigrp 7 10.100.16.0 255.255.240.0 5
 delay 2000
 qos pre-classify
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 12345
 tunnel protection ipsec profile my-profile shared
!
interface Loopback0
 ip address 10.100.200.1 255.255.254.0
 ip ospf network point-to-point
!
interface Loopback1
 ip address 10.100.100.1 255.255.254.0
 ip ospf network point-to-point
!
interface GigabitEthernet0/0
 ip address 172.16.0.1 255.255.255.248
 ip pim sparse-dense-mode
 duplex full
 speed 1000
```

```
 media-type sfp
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
!
interface Virtual-Template2 type tunnel
 ip unnumbered GigabitEthernet0/0
 ip pim dr-priority 10
 ip pim sparse-mode
 ip multicast rate-limit out 768
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile my-profile shared
!
interface Virtual-Template3 type tunnel
 ip unnumbered GigabitEthernet0/0
 ip pim dr-priority 10
 ip pim sparse-mode
 ip multicast rate-limit out 768
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile my-profile shared
!
router eigrp 7
 description DMVPN internal routing
 redistribute ospf 5 route-map split_in
 network 10.250.250.0 0.0.1.255
 default-metric 2000 1000 255 1 1500
 distribute-list split_out in Tunnel1
 no auto-summary
 no eigrp log-neighbor-changes
!
router ospf 5
 descrition Corporate internal routing
 log-adjacency-changes
 area 24 nssa
 redistribute static subnets route-map RRI-spokes
 redistribute eigrp 7 metric 40 subnets route-map split_out
 network 10.100.100.0 0.0.1.255 area 24
 network 10.100.200.0 0.0.1.255 area 24
 network 172.16.0.1 0.0.0.15 area 24
!
!
ip local pool webvpn-pool 10.100.100.2 10.100.101.253
ip local pool easyvpn-pool 10.100.200.2 10.100.201.253
!
ip route 0.0.0.0 0.0.0.0 172.16.0.14
!
```

```
no ip http server
ip http authentication aaa
ip http secure-server
ip http secure-trustpoint verisign
ip pim bidir-enable
ip pim ssm range multicast_ssm_range
!
ip access-list extended ezvpn-split-tunnel
!!! These are internal corporate subnets, which are allowed to
!!! be advertised to EzVPN spokes. In other words, the networks
!!! that are part of the split tunnel
 permit ip 10.0.0.0 0.255.255.255 any
 permit ip 172.16.0.0 0.3.255.255 any
 permit ip 192.168.0.0 0.0.255.255 any
ip access-list extended RRI-spokes
!!! These are Enhanced Easy VPN spokes, which use
!!! network-extension to connect
 permit ip 10.100.27.88 0.0.0.7 any
 permit ip 10.100.11.144 0.0.0.15 any
 permit ip 10.100.13.0 0.0.0.255 any
 permit ip 10.100.11.240 0.0.0.15 any
 permit ip 10.100.27.56 0.0.0.7 any
 permit ip 10.100.22.144 0.0.0.15 any
 permit ip 10.100.22.192 0.0.0.7 any
 permit ip 10.100.24.248 0.0.0.7 any
ip access-list standard no_split_in
!!! This list, if used, allows all internal corporate subnets to
!!! be advertised to DMVPN spokes.
 permit 0.0.0.0
ip access-list standard split_in
!!! These are internal corporate subnets, which are allowed to
!!! be advertised to DMVPN spokes. In other words, the networks
!!! that are part of the split tunnel
 permit 10.0.0.0
 permit 192.168.0.0
 permit 144.254.0.0
 permit 172.16.0.0
ip access-list standard split_out
 Remark: These are DMVPN spokes subnets
 permit 10.100.20.0 0.0.0.255
 permit 10.100.21.0 0.0.0.255
 permit 10.100.22.0 0.0.0.255
 permit 10.100.23.0 0.0.0.255
 permit 10.100.24.0 0.0.0.255
 permit 10.100.25.0 0.0.0.255
 permit 10.100.26.0 0.0.0.255
 permit 10.100.27.0 0.0.0.255
 permit 10.100.28.0 0.0.0.255
```

```
 permit 10.100.29.0 0.0.0.255
 permit 10.100.10.0 0.0.0.255
 permit 10.100.11.0 0.0.0.255
 permit 10.100.12.0 0.0.0.255
 permit 10.100.13.0 0.0.0.255
 permit 10.100.14.0 0.0.0.255
 permit 10.100.15.0 0.0.0.255
!
route-map split_in permit 10
 match ip address split_in
!
route-map split_out permit 10
 match ip address split_out
!
route-map no_split_in permit 10
 match ip address no_split_in
!
route-map RRI-spokes permit 10
!!! Redistribute remote EzVPN-Users spokes subnets from RRI
 match ip address RRI-spokes
!
!
tacacs-server host 172.16.100.3
tacacs-server timeout 3
tacacs-server directed-request
!
!
line con 0
 exec-timeout 60 0
 authorization exec tacacs+
 login authentication admin
 transport output ssh
 stopbits 1
line aux 0
 transport output ssh
 stopbits 1
line vty 0 4
 exec-timeout 60 0
 login authentication admin
 transport input ssh
 transport output ssh
!
ntp server 172.16.10.80
ntp server 172.16.10.150
!
webvpn gateway sslvpn-gw
 ip address 172.16.0.1 port 443
 ssl trustpoint verisign
```

```
 inservice

 !
webvpn install svc flash:/webvpn/svc.pkg
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context csd
 title "Welcome to the pki-group CVO SSLVPN - CSD"
 title-color pink
 ssl authenticate verify all
 !
policy group csdpolicy
   functions svc-enabled
   svc address-pool "webvpn-pool"
   svc keep-client-installed
   svc split include 10.0.0.0 255.0.0.0
   svc split include 172.16.0.0 255.240.0.0
   svc split include 192.168.0.0 255.255.0.0
   svc dns-server primary 172.16.226.120
!
 policy group tunnelpolicy
 default-group-policy csdpolicy
 gateway sslvpn-gw domain csd
 csd enable
 inservice
!
!
webvpn context tunnel
 title "Welcome to the pki-group CVO SSLVPN - tunnel mode"
 title-color lightgreen
 ssl authenticate verify all
 !
 !
 policy group tunnelpolicy
   functions svc-required
   svc address-pool "webvpn-pool"
   svc keep-client-installed
   svc split include 10.0.0.0 255.0.0.0
   svc split include 172.16.0.0 255.240.0.0
   svc split include 192.168.0.0 255.255.0.0
   svc dns-server primary 172.16.226.120
   svc wins-server primary 172.16.2.87
   svc wins-server secondary 172.16.235.228
 default-group-policy tunnelpolicy
 gateway sslvpn-gw domain tunnel
 inservice
```

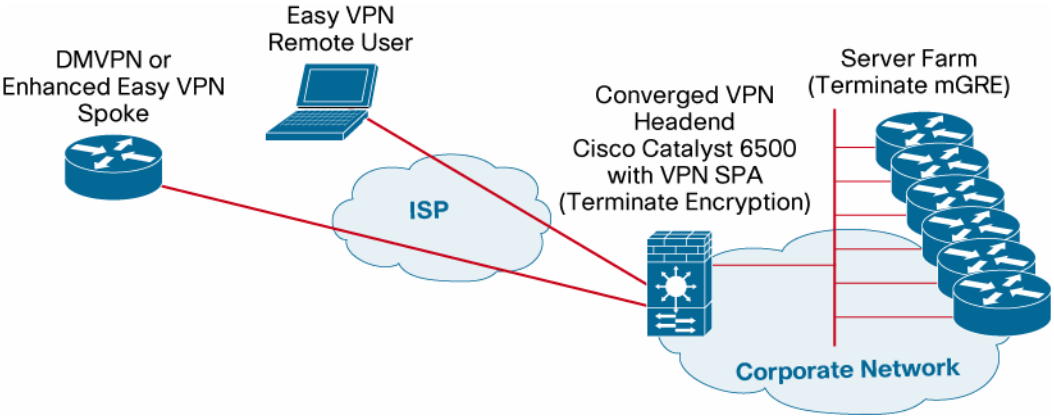
```
!
!
webvpn context voice
 title "Welcome to the CVO SSLVPN - tunnel mode - voice only"
 title-color lightblue
 ssl authenticate verify all
 !
 !
 policy group voicepolicy
   functions svc-enabled
   svc address-pool "webvpn-pool"
   svc keep-client-installed
   svc split include 10.0.0.0 255.0.0.0
   svc split include 172.16.196.70 255.255.255.255
   svc split include 172.16.147.60 255.255.255.255
   svc split include 172.16.147.62 255.255.255.255
   svc split include 172.16.196.72 255.255.255.255
 default-group-policy voicepolicy
 gateway sslvpn-gw domain voice
 inservice
!
!
end
```

Cisco Catalyst 6500 with Server Farm Converged VPN Configuration

Following is a sample configuration for a Converged VPN server based on a Cisco Catalyst 6500 that has a VPN SPA for encryption and a Supervisor Engine 720 as the supervisor engine, and uses a server farm of Cisco 7206 Routers for the DMVPN routing protocol, Next Hop Resolution Protocol (NHRP), and multicast work (Figure 1).

The Cisco Catalyst 6500 uses the Cisco IOS SLB feature to perform load balancing between the real Cisco 7206 servers.

Figure 1. Overview of the High-Concentration Hub with Integrated Encryption for Converged DMVPN and Enhanced Easy VPN



Note: In this example a VPN SPA is used for encrypting both DMVPN and Enhanced Easy VPN traffic. SSL VPN, however, is not supported on the Cisco Catalyst 6500.

For the DMVPN routing, Enhanced IGRP (EIGRP) is used. Configuration of one of the Cisco 7206 server farms is also shown after the Cisco Catalyst 6500 configuration.

In this example EIGRP7 is used internally for DMVPN, and the corporate traffic runs on Open Shortest Path First OSPF5

Cisco Catalyst 6500 Configuration

DMVPN

ENHANCED EASY VPN

```
upgrade fpd auto
upgrade fpd path disk1:
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service counters max age 10
!
hostname 6500-converged-vpn-headend
!
enable secret <removed>
!
aaa new-model
aaa group server radius pki-aaa-server
 server-private <removed> auth-port 1812 acct-port 1813 key <removed>
 ip radius source-interface Loopback0
!
aaa group server radius EzVPN-Users
 server-private <removed> auth-port 1812 acct-port 1813 key  <removed>
 ip radius source-interface Vlan10
!
```

```
aaa authentication login easyVPN local group EzVPN-Users
aaa authorization network pkiaaa group pki-aaa-server
aaa authorization network easyVPN local group EzVPN-Users
!
aaa session-id common
clock timezone pst -8
clock summer-time pdt recurring
ip subnet-zero
no ip source-route
!
!
ip flow-cache timeout active 1
ip multicast-routing
ip sap cache-timeout 30
ip domain-name cisco.com
ip name-server 172.16.0.10
!
ip slb probe PING-PROBE ping
 faildetect 3
!
ip slb serverfarm FARM
 predictor leastconns
 failaction purge
 probe PING-PROBE
 !
 real 10.0.1.2
  maxconns 500
  inservice
 !
 real 10.0.1.3
  maxconns 500
  inservice
!
ip slb vserver GRE
 virtual 172.16.0.2 255.255.255.248 gre
 serverfarm FARM
 no advertise
 idle 30
 inservice
!
!
kerberos local-realm Realm
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
password encryption aes
```

```
no scripting tcl init
no scripting tcl encdir
!
crypto pki trustpoint pki-cert-server
 enrollment url http://pki-cert-server:80
 serial-number
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
!
!
crypto pki certificate chain pki-cert-server
 certificate <removed>
 certificate ca <removed>
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 group 2
!
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
crypto isakmp xauth timeout 10
!
crypto isakmp client configuration group pre-shared-group
 key <removed>
 dns 172.16.10.120 172.16.10.183
 wins 172.16.10.28 171.16.10.87
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn-split-tunnel
 save-password
 firewall are-u-there
 backup-gateway 172.16.0.1
 banner ^C
You are connecting to a Converged VPN server using Pre-shared
 ^C
!
crypto isakmp client configuration group pki-group
 dns 172.16.10.120 172.16.10.183
 wins 172.16.10.28 171.16.10.87
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn-split-tunnel
 save-password
```

```
 backup-gateway 172.16.0.1
 banner ^C
You are connecting to a Converged VPN server using PKI
^C
crypto isakmp profile pre-shared-group
   description PSK group
   match identity group pre-shared-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
crypto isakmp profile pki-group
   description PKI group
   match identity group pki-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
!
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport
!
!
crypto dynamic-map dmap 1
 set transform-set t2
 set isakmp-profile pre-shared-group
 reverse-route
crypto dynamic-map dmap 2
 set transform-set t2
 set isakmp-profile pki-group
 reverse-route
crypto dynamic-map dmap 10
 set transform-set t1
 match address VPNaccept
!
!
crypto map dmvpn_easyvpn local-address Vlan10
crypto map dmvpn_easyvpn 1 ipsec-isakmp dynamic dmap
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
```

```
no spanning-tree vlan 10
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface Loopback0
 ip address 10.100.102.1 255.255.254.0
 ip ospf network point-to-point
!
!
interface FastEthernet3/1
 switchport
 switchport access vlan 55
 switchport mode access
 no ip address
 speed 100
 duplex full
!
interface FastEthernet3/2
 switchport
 switchport access vlan 55
 switchport mode access
 no ip address
 speed 100
 duplex full
!
<cut>
<cut>
<cut>
!
interface GigabitEthernet4/1/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,11,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
```

```
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 switchport
 switchport access vlan 11
 switchport mode access
 no ip address
 media-type rj45
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 172.16.0.2 255.255.255.248
 ip flow ingress
 ip pim sparse-dense-mode
 ip route-cache flow
 no mop enabled
 crypto map dmvpn_easyvpn
 crypto engine subslot 4/1
 hold-queue 1000 in
 hold-queue 1000 out
!
interface Vlan11
 no ip address
 crypto connect vlan 10
 hold-queue 1000 in
 hold-queue 1000 out
!
interface Vlan55
Description Server FARM
 ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
router eigrp 7
 Description DMVPN internal routing
 redistribute ospf 5 route-map split_in
 network 10.0.1.0 0.0.0.255
 default-metric 2000 1000 255 1 1500
 no auto-summary
 no eigrp log-neighbor-changes
!
router ospf 5
```

```
 log-adjacency-changes
 area 24 nssa
 redistribute static subnets route-map RRI-spokes
 redistribute eigrp 7 metric 38 subnets route-map split_out
 network 10.100.102.0 0.0.1.255 area 24
 network 172.16.0.0 0.0.0.15 area 24
!
!
ip local pool easyvpn-pool 10.100.102.2 10.100.103.253
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.0.14
!
no ip http server
!
ip access-list extended ezvpn-split-tunnel
!!! These are internal corporate subnets, which are allowed to
!!! be advertised to DMVPN spokes. In other words, the networks
!!! that are part of the split tunnel
 permit ip 10.0.0.0 0.255.255.255 any
 permit ip 172.16.0.0 0.3.255.255 any
 permit ip 192.168.0.0 0.0.255.255 any
ip access-list extended RRI-spokes
!!! These are Enhanced Easy VPN spokes, which use
!!! network-extension to connect
 permit ip 10.100.27.88 0.0.0.7 any
 permit ip 10.100.11.144 0.0.0.15 any
 permit ip 10.100.13.0 0.0.0.255 any
 permit ip 10.100.11.240 0.0.0.15 any
 permit ip 10.100.27.56 0.0.0.7 any
 permit ip 10.100.22.144 0.0.0.15 any
 permit ip 10.100.22.192 0.0.0.7 any
 permit ip 10.100.24.248 0.0.0.7 any
ip access-list standard no_split_in
!!! This list, if used, allows all internal corporate subnets to
!!! be advertised to DMVPN spokes.
 permit 0.0.0.0
ip access-list standard split_in
!!! These are internal corporate subnets, which are allowed to
!!! be advertised to DMVPN spokes. In other words, the networks
!!! that are part of the split tunnel
 permit 10.0.0.0
 permit 192.168.0.0
 permit 144.254.0.0
 permit 172.16.0.0
ip access-list standard split_out
 Remark: These are DMVPN spokes subnets
 permit 10.100.20.0 0.0.0.255
 permit 10.100.21.0 0.0.0.255
```

```
 permit 10.100.22.0 0.0.0.255
 permit 10.100.23.0 0.0.0.255
 permit 10.100.24.0 0.0.0.255
 permit 10.100.25.0 0.0.0.255
 permit 10.100.26.0 0.0.0.255
 permit 10.100.27.0 0.0.0.255
 permit 10.100.28.0 0.0.0.255
 permit 10.100.29.0 0.0.0.255
 permit 10.100.10.0 0.0.0.255
 permit 10.100.11.0 0.0.0.255
 permit 10.100.12.0 0.0.0.255
 permit 10.100.13.0 0.0.0.255
 permit 10.100.14.0 0.0.0.255
 permit 10.100.15.0 0.0.0.255
ip access-list extended VPNaccept
 permit gre host 10.0.1.0 any
!
route-map no_split_out permit 10
 match ip address no_split_out
!
route-map split_in permit 10
 match ip address split_in
!
route-map split_out permit 10
 match ip address split_out
!
route-map no_split_in permit 10
 match ip address no_split_in
!
route-map RRI-spokes permit 10
!!! Redistribute remote EzVPN-Users spokes subnets from RRI
 match ip address RRI-spokes
!
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 300 0
line vty 0 4
 exec-timeout 300 0
 login authentication admin
 transport input ssh
 transport output ssh
!
monitor event-trace timestamps
ntp clock-period 17180018
ntp server 10.68.10.80
```

```
ntp server 10.68.10.150
end
```

One Cisco 7206 Real Server Example

Note: This router is used only for DMVPN.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Hub1-7200
!
boot-start-marker
boot-end-marker
!
enable secret <removed>
!
no aaa new-model
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
ip cef
!
no ip domain lookup
ip multicast-routing
!
interface Tunnel0
 bandwidth 2000
 ip address 10.250.250.11 255.255.254.0 secondary
 ip address 10.250.250.10 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip nhrp map multicast dynamic
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 7
 ip summary-address eigrp 7 10.100.8.0 255.255.248.0 5
 ip summary-address eigrp 7 10.100.16.0 255.255.240.0 5
 delay 2000
 qos pre-classify
 tunnel source Loopback0
```

```
 tunnel mode gre multipoint
 hold-queue 1000 in
 hold-queue 1000 out
!
interface Loopback0
 ip address 172.16.0.2 255.255.255.248
!
interface GigabitEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 ip pim sparse-dense-mode
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router eigrp 7
 network 10.0.1.0 0.0.0.255
 network 10.255.255.0 0.0.1.255
 default-metric 2250 1000 255 1 1500
 distribute-list block_internal_acl out Tunnel0
 no auto-summary
 eigrp router-id 10.250.250.2
 no eigrp log-neighbor-changes
!
ip route 0.0.0.0 0.0.0.0 10.0.1.1
no ip http server
no ip http secure-server
!
ip pim ssm range multicast_ssm_range
!
ip access-list standard block_internal_acl
 deny   10.0.1.0
 permit any
!
control-plane
```

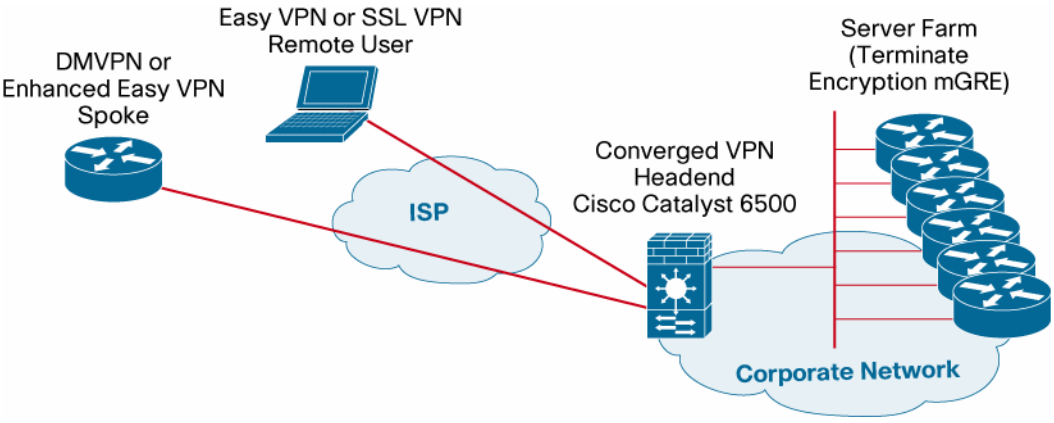
```
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
ntp clock-period 17179919
ntp server 10.0.1.1
!
end
```

Another Cisco Catalyst 6500 with Server Farm Converged VPN Configuration

Alternatively, encryption, multipoint generic routing encapsulation (mGRE), and routing can be terminated at the server farm. In this case, the Cisco Catalyst 6500 uses a Supervisor Engine 720 as the supervisor engine and a server farm of Cisco 7206 Routers for Internet Key Exchange (IKE), IPsec, DMVPN, NHRP, and multicast work (Figure 2).

For SSL VPN, sessions can also be terminated in the server farm.

Figure 2. Overview of the High-Concentration Hub with Distributed Encryption for Converged DMVPN and Enhanced Easy VPN



Cisco Catalyst 6500 Configuration

```
upgrade fpd auto
upgrade fpd path disk1:
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service counters max age 10
```

```
!
hostname 6500-converged-vpn-headend
!
enable secret <removed>
!
aaa new-model
!
aaa session-id common
clock timezone pst -8
clock summer-time pdt recurring
ip subnet-zero
no ip source-route
!
!
ip flow-cache timeout active 1
ip multicast-routing
ip sap cache-timeout 30
ip domain-name cisco.com
ip name-server 172.16.0.10
!
ip slb probe PING-PROBE ping
 faildetect 3
!
ip slb serverfarm FARM
 predictor leastconns
 failaction purge
 probe PING-PROBE
 !
 real 10.0.1.2
  maxconns 500
  inservice
 !
 real 10.0.1.3
  maxconns 500
  inservice
!
ip slb vserver ESP
 virtual 172.16.0.2 255.255.255.248 esp
 serverfarm FARM
 no advertise
 idle 30
 inservice
!
ip slb vserver ISAKMP
 virtual 172.16.0.2 255.255.255.248 udp isakmp
 serverfarm FARM
 no advertise
 idle 30
 inservice
```

```
!
ip slb vserver ISAKMP-4500
 virtual 172.16.0.2 255.255.255.248 udp 4500
 serverfarm FARM
 no advertise
 idle 30
 inservice
!
ip slb vserver SSLVPN
 virtual 172.16.0.2 255.255.255.248 tcp https
 serverfarm FARM
 no advertise
 idle 30
 inservice
!
!
kerberos local-realm Realm
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
password encryption aes
no scripting tcl init
no scripting tcl encdir
!
crypto pki trustpoint pki-cert-server
 enrollment url http://pki-cert-server:80
 serial-number
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
!
!
crypto pki certificate chain pki-cert-server
 certificate <removed>
 certificate ca <removed>
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 10
```

```
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface FastEthernet3/1
 switchport
 switchport access vlan 55
 switchport mode access
 no ip address
 speed 100
 duplex full
!
interface FastEthernet3/2
 switchport
 switchport access vlan 55
 switchport mode access
 no ip address
 speed 100
 duplex full
!
<cut>
<cut>
<cut>
!
interface GigabitEthernet4/1/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,11,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/1
 no ip address
```

```
 shutdown
!
interface GigabitEthernet5/2
 switchport
 switchport access vlan 11
 switchport mode access
 no ip address
 media-type rj45
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 172.16.0.2 255.255.255.248
 ip flow ingress
 ip pim sparse-dense-mode
 ip route-cache flow
 no mop enabled
 crypto map dmvpn_easyvpn
 crypto engine subslot 4/1
 hold-queue 1000 in
 hold-queue 1000 out
!
interface Vlan11
 no ip address
 crypto connect vlan 10
 hold-queue 1000 in
 hold-queue 1000 out
!
interface Vlan55
Description Server FARM
 ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
router eigrp 7
 Description DMVPN internal routing
 redistribute ospf 5 route-map split_in
 network 10.0.1.0 0.0.0.255
 default-metric 2000 1000 255 1 1500
 no auto-summary
 no eigrp log-neighbor-changes
!
router ospf 5
 log-adjacency-changes
 area 24 nssa
 redistribute static subnets route-map RRI-spokes
 redistribute eigrp 7 metric 38 subnets route-map split_out
 network 10.100.102.0 0.0.1.255 area 24
 network 172.16.0.0 0.0.0.15 area 24
```

```
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.0.14
!
no ip http server
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 300 0
line vty 0 4
 exec-timeout 300 0
 login authentication admin
 transport input ssh
 transport output ssh
!
monitor event-trace timestamps
ntp clock-period 17180018
ntp server 10.68.10.80
ntp server 10.68.10.150
end
```

One Cisco 7206 Real Server Example

Note: This router is used for DMVPN, Enhanced Easy VPN, and SSL VPN.

DMVPN
ENHANCED EASY VPN
SSLVPN

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Hub1-7200
!
boot-start-marker
boot-end-marker
!
enable secret <removed>
!
aaa new-model
!
!
aaa group server radius EzVPN-Users
```

```
 server-private 10.99.99.6 auth-port 1812 acct-port 1813 key <removed>
 ip radius source-interface Loopback0
!
!!! This AAA group is used to authenticate device's PKI certificates
!!! against their respective AAA profile
!
aaa group server radius pki-aaa-server
 server-private 10.99.99.6 auth-port 1812 acct-port 1813 key <removed>
!
aaa group server radius SSLVPN-Users
 server-private 10.99.99.5 auth-port 1812 acct-port 1813 key <removed>
 ip radius source-interface Loopback1
!
aaa authentication login default local group SSLVPN-Users
aaa authentication login admin group tacacs+ enable
aaa authentication login easyVPN local group EzVPN-Users
aaa authorization exec default none
aaa authorization network easyVPN local group EzVPN-Users
aaa authorization network pkiaaa group pki-aaa-server
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
ip cef
!
no ip domain lookup
ip multicast-routing
!
crypto pki trustpoint verisign
 enrollment terminal
 fqdn none
 subject-name cn=web-vpn-server.cisco.com,o=Cisco
Systems,c=US,st=California
 revocation-check crl
 rsakeypair web-vpn-server.cisco.com
!
crypto pki trustpoint dmvpn-pki-server
 enrollment url http://dmvpn-pki-server:80
 serial-number
 ip-address none
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
!
crypto pki trustpoint easyvpn-pki-server
 enrollment url http://easyvpn-pki-server:80
```

```
 serial-number
 ip-address none
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
!
!
!
crypto pki certificate map 1 10
 subject-name co easyvpn-pki-group
!
crypto pki certificate chain verisign
 certificate <removed>
 certificate ca <removed>
crypto pki certificate chain dmvpn-pki-server
 certificate ca <removed>
 certificate <removed>
crypto pki certificate chain easyvpn-pki-server
 certificate <removed>
 certificate ca <removed>
!
!
crypto isakmp policy 10
 encr 3des
 group 2
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
crypto isakmp xauth timeout 10
!
crypto isakmp client configuration group pki-group
 dns 172.16.10.120 172.16.10.183
 wins 172.16.10.28 171.16.10.87
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn-split-tunnel
 save-password
 backup-gateway 172.16.0.1
 banner ^C
You are connecting to a Converged VPN server using PKI
^C
!
crypto isakmp client configuration group pre-shared-group
```

```
 key EasyVPN-Secret-KEY
 dns 172.16.10.120 172.16.10.183
 wins 172.16.10.28 171.16.10.87
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn-split-tunnel
 save-password
 firewall are-u-there
 backup-gateway 172.16.0.1
 banner ^C
You are connecting to a Converged VPN server using Pre-shared
 ^C
crypto isakmp profile pre-shared-group
   description PSK group
   match identity group pre-shared-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 3
crypto isakmp profile pki-group
   description PKI group
   ca trust-point dmvpn-pki-server
   match identity group pki-group
   match certificate 1
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 2
!
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport require
!
crypto ipsec profile my-profile
 set transform-set t1
!
interface Tunnel0
 bandwidth 2000
 ip address 10.250.250.11 255.255.254.0 secondary
 ip address 10.250.250.10 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip nhrp map multicast dynamic
 ip nhrp redirect
 ip tcp adjust-mss 1360
```

```
 no ip split-horizon eigrp 7
 ip summary-address eigrp 7 10.100.8.0 255.255.248.0 5
 ip summary-address eigrp 7 10.100.16.0 255.255.240.0 5
 delay 2000
 qos pre-classify
 tunnel source Loopback2
 tunnel mode gre multipoint
 tunnel key 12345
 tunnel protection ipsec profile my-profile shared
!
interface Loopback0
 ip address 10.100.200.1 255.255.254.0
!
interface Loopback1
 ip address 10.100.100.1 255.255.254.0
!
interface Loopback2
 ip address 172.16.0.2 255.255.255.248
!
interface GigabitEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 ip pim sparse-dense-mode
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface Virtual-Template2 type tunnel
 ip unnumbered Loopback2
 ip pim dr-priority 10
 ip pim sparse-mode
 ip multicast rate-limit out 768
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile my-profile shared
!
```

```
interface Virtual-Template3 type tunnel
 ip unnumbered Loopback2
 ip pim dr-priority 10
 ip pim sparse-mode
 ip multicast rate-limit out 768
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile my-profile shared
!
router eigrp 7
 network 10.0.1.0 0.0.0.255
 network 10.250.250.0 0.0.1.255
 default-metric 2250 1000 255 1 1500
 distribute-list block_internal_acl out Tunnel0
 no auto-summary
 eigrp router-id 10.250.250.2
 no eigrp log-neighbor-changes
!
ip local pool webvpn-pool 10.100.100.2 10.100.101.253
ip local pool easyvpn-pool 10.100.200.2 10.100.201.253
!
ip route 0.0.0.0 0.0.0.0 10.0.1.1
no ip http server
no ip http secure-server
!
ip http authentication aaa
ip http secure-server
ip http secure-trustpoint verisign
!
ip pim ssm range multicast_ssm_range
!
ip access-list extended ezvpn-split-tunnel
!!! These are internal corporate subnets, which are allowed to
!!! be advertised to EzVPN spokes. In other words, the networks
!!! that are part of the split tunnel
 permit ip 10.0.0.0 0.255.255.255 any
 permit ip 172.16.0.0 0.3.255.255 any
 permit ip 192.168.0.0 0.0.255.255 any
ip access-list extended RRI-spokes
!!! These are Enhanced Easy VPN spokes, which use
!!! network-extension to connect
 permit ip 10.100.27.88 0.0.0.7 any
 permit ip 10.100.11.144 0.0.0.15 any
 permit ip 10.100.13.0 0.0.0.255 any
 permit ip 10.100.11.240 0.0.0.15 any
 permit ip 10.100.27.56 0.0.0.7 any
 permit ip 10.100.22.144 0.0.0.15 any
 permit ip 10.100.22.192 0.0.0.7 any
 permit ip 10.100.24.248 0.0.0.7 any
```

```
ip access-list standard no_split_in
!!! This list, if used, allows all internal corporate subnets to
!!! be advertised to DMVPN spokes.
 permit 0.0.0.0
ip access-list standard split_in
!!! These are internal corporate subnets, which are allowed to
!!! be advertised to DMVPN spokes. In other words, the networks
!!! that are part of the split tunnel
 permit 10.0.0.0
 permit 192.168.0.0
 permit 144.254.0.0
 permit 172.16.0.0
ip access-list standard split_out
 Remark: These are DMVPN spokes subnets
 permit 10.100.20.0 0.0.0.255
 permit 10.100.21.0 0.0.0.255
 permit 10.100.22.0 0.0.0.255
 permit 10.100.23.0 0.0.0.255
 permit 10.100.24.0 0.0.0.255
 permit 10.100.25.0 0.0.0.255
 permit 10.100.26.0 0.0.0.255
 permit 10.100.27.0 0.0.0.255
 permit 10.100.28.0 0.0.0.255
 permit 10.100.29.0 0.0.0.255
 permit 10.100.10.0 0.0.0.255
 permit 10.100.11.0 0.0.0.255
 permit 10.100.12.0 0.0.0.255
 permit 10.100.13.0 0.0.0.255
 permit 10.100.14.0 0.0.0.255
 permit 10.100.15.0 0.0.0.255
!
route-map split_in permit 10
 match ip address split_in
!
route-map split_out permit 10
 match ip address split_out
!
route-map no_split_in permit 10
 match ip address no_split_in
!
route-map RRI-spokes permit 10
!!! Redistribute remote EzVPN-Users spokes subnets from RRI
 match ip address RRI-spokes
!
ip access-list standard block_internal_acl
 deny   10.0.1.0
 permit any
!
```

```
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
ntp clock-period 17179919
ntp server 10.0.1.1
!
webvpn gateway sslvpn-gw
 ip address 172.16.0.2 port 443
 ssl trustpoint verisign
 inservice

 !
webvpn install svc flash:/webvpn/svc.pkg
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context csd
 title "Welcome to the pki-group CVO SSLVPN - CSD"
 title-color pink
 ssl authenticate verify all
 !
policy group csdpolicy
   functions svc-enabled
   svc address-pool "webvpn-pool"
   svc keep-client-installed
   svc split include 10.0.0.0 255.0.0.0
   svc split include 172.16.0.0 255.240.0.0
   svc split include 192.168.0.0 255.255.0.0
   svc dns-server primary 172.16.226.120
!
 policy group tunnelpolicy
 default-group-policy csdpolicy
 gateway sslvpn-gw domain csd
 csd enable
 inservice
!
!
webvpn context tunnel
```

```
 title "Welcome to the pki-group CVO SSLVPN - tunnel mode"
 title-color lightgreen
 ssl authenticate verify all
 !
 !
 policy group tunnelpolicy
   functions svc-required
   svc address-pool "webvpn-pool"
   svc keep-client-installed
   svc split include 10.0.0.0 255.0.0.0
   svc split include 172.16.0.0 255.240.0.0
   svc split include 192.168.0.0 255.255.0.0
   svc dns-server primary 172.16.226.120
   svc wins-server primary 172.16.2.87
   svc wins-server secondary 172.16.235.228
 default-group-policy tunnelpolicy
 gateway sslvpn-gw domain tunnel
 inservice
!
!
webvpn context voice
 title "Welcome to the CVO SSLVPN - tunnel mode - voice only"
 title-color lightblue
 ssl authenticate verify all
 !
 !
 policy group voicepolicy
   functions svc-enabled
   svc address-pool "webvpn-pool"
   svc keep-client-installed
   svc split include 10.0.0.0 255.0.0.0
   svc split include 172.16.196.70 255.255.255.255
   svc split include 172.16.147.60 255.255.255.255
   svc split include 172.16.147.62 255.255.255.255
   svc split include 172.16.196.72 255.255.255.255
 default-group-policy voicepolicy
 gateway sslvpn-gw domain voice
 inservice
!
!
end
```

References

- Cisco Virtual Office Easy VPN guide: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6808/deployment_guide_c07_458259_ns855_Networking_Solutions_White_Paper.html

- Cisco Virtual Office SSL VPN guide: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6657/white_paper_c07-372106.html
- DMVPN: http://www.cisco.com/go/dmvpn
- Easy VPN: http://www.cisco.com/go/easyvpn
- SSL VPN: http://www.cisco.com/go/sslvpn

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 C11-492817-00 09/08