Cisco on Cisco Best Practices
Cisco Remote Access Design: Cisco Virtual Office Solution

Design Document
Cisco Virtual Office

Cisco Virtual Office is an end-to-end solution that provides secure remote site connectivity for telecommuters.

Contents

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE DESIGN RECOMMENDATIONS AND CONFIGURATIONS PROVIDED IN THIS DOCUMENT ARE SPECIFIC TO CISCO IT REQUIREMENTS. CISCO SYSTEMS DOES NOT ENDORSE OR APPROVE THE CONFIGURATIONS TO BE USED FOR ANY CUSTOMER. THE DESIGN STANDARDS PROVIDED HERE ARE MERELY PROVIDED TO SHARE CISCO IT BEST PRACTICES. EACH AND EVERY CUSTOMER REQUIREMENT WOULD BE DIFFERENT AND HENCE THOROUGH ANALYSIS AND RESEARCH SHOULD BE DONE BEFORE APPLYING ANY DESIGN STANDARD.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL INFORMATION IS PROVIDED “AS IS” WITH ALL FAULTS. CISCO DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1. Introduction

This document gives a comprehensive description of the Cisco® Virtual Office (formerly known as Enterprise-Class Teleworker) solution so that IT engineers can understand and critique it, which will result in an improved product.

1.1 Background

One obstacle that full-time teleworkers encounter is the inability to access all the applications and services that are available at a conventional workplace. Another obstacle is the necessity of having a separate telephone number at the remote workplace, which presents both logistical and financial challenges. Both of these obstacles have a direct effect on worker productivity and the company's profits.

The Cisco Virtual Office solution provides the following capabilities:

- Security
- Large-scale deployment
- Management
- IP telephony
- Resiliency
- Agility
- Full service suite availability

Cisco Virtual Office provides a transparent end-to-end solution that enables teleworkers to function remotely as if they were onsite at a corporate facility, enhancing productivity and reducing operating expenses.

This solution also addresses other business concerns such as distributed workforce, business continuity, localized weather phenomena, health alerts, and natural or human-caused disasters.

1.2 Problems and Opportunities

1.2.1 Problems

- Teleworkers are not always enabled with all of the services required to emulate an office environment, including:
    - IP telephony with quality-of-service (QoS)
    - Multicast
    - Hosting of collaboration applications
    - Video

- Corporate networks can be compromised because of nonsecure home networks
- No centralized management of remote-access solutions
- Separate phone line used at an additional cost

1.2.2 Opportunities

- Ability to remotely manage and push corporate policies/standards across a network of widely distributed remote access points, while allowing the expansion of the telecommuting network without creating new security vulnerabilities.

- Ability to provide full visibility of the remote site and remotely configure and manage policies for the spoke router in a manner that is transparent to the end user.

- Support of the full range of converged applications. Data, voice, video, and real-time collaboration services all work well over the system, because the solution provides QoS guarantees based on Cisco IOS® Software.

- Ability to integrate IP telephony into the remote site/home (phase II). This results in "single-number reachability," with employees having the same phone number at the corporate desk and in the home office. This results in fewer extensions and telephony accounts to manage and significantly lower long-distance charges because of toll bypass.

1.3 Project Objectives Statement

The objectives of the Cisco Virtual Office project are to build and deploy an automated and integrated suite of tools and products to provide a complete solution that enables the enterprise's ability to improve teleworker productivity, responds to business agility and resiliency problems, and reduces remote security breaches and operational expenses. Cisco Virtual Office is intended for full-time telecommuters and employees who work a significant amount of time at their residence. It is intended to complement the software VPN client, which should be targeted for traveling workers.

1.3.1 Project Implementation Objectives

The primary objectives of implementation are broken down per the following phases.

Phase 1:

- Cisco IOS Software–based Cisco 831 Ethernet Broadband Router configured and deployed as a managed hardware VPN client taking full advantage of various Cisco IOS Software security features
- Full suite of applications and services to ease product ordering, installation, and implementation

Phase 2:

- IP telephony offered with the Cisco IOS Software–based hardware VPN client as a single solution for all employees who meet entitlement requirements
- Incorporation of new features that build upon and enhance the Phase 1 deliverables such as 802.1x user authentication and Network Admission Control (NAC) technology

Phase 3:

- Support for a Cisco IOS Software–based hardware client that includes an 802.11x wireless network interface
- Improvement of existing Cisco Virtual Office features, applications, and services

1.3.2 Company Objectives

Cisco Systems® is implementing Cisco Virtual Office to provide a foundation and model for how it envisions enterprises will enable and support remote/distributed teleworking to enhance productivity, increase worker satisfaction, and decrease security compromises and operational expenses.

Cisco expects that the project implementation will directly address four primary factors for change:

- A site-to-site “always on” VPN connection with which the user is fully integrated into the corporate network.
- Support for the full range of converged applications. Data, voice, video, and real-time collaboration services all work well over the system, because the solution provides Cisco IOS Software–based QoS guarantees.
- The ability to remotely implement, manage, and enforce corporate policies/standards across a network of widely distributed remote access points, while at the same time allowing the expansion of the telecommuting network without creating new security vulnerabilities.

1.4 Expected Benefits

The Cisco Virtual Office solution is expected to deliver a production system to businesses that will:

- Increase productivity and employee satisfaction. Teleworkers will have access to all the applications and services available to employees with conventional workspaces, with a single-number phone line, including the ability to access data, voice, and video applications.[1] Also, Cisco Virtual Office can allow employees who work several hours at home each day on global teams and employees who work several days at home each week to enjoy the benefits of a conventional office, increasing productivity and satisfaction.
- Provide resilience and agility to the workforce. The solution will enable business/operational continuity in the event of uncontrollable situations that might adversely affect the ability of workers to commute to their conventional offices.
- Provide managed security and encryption of data at the remote work site. The solution will create a platform on which enriched, secure remote access can be realized and will support secure remote-access points that do not compromise the corporate host network.
- Lower operational costs. The solution avoids costs associated with traditional toll services.

[2] Provided teleworkers have minimum service levels from their ISP, including a minimum bandwidth of 128kbps, with 256kbps preferred, and latency less than 200 ms.

2. Architecture Overview

By implementing the Cisco Virtual Office solution, Cisco is introducing a secure end-to-end solution for bringing enterprise-quality voice, video, and data into the home offices of full-time telecommuters and "day extenders.[2]" In the headend, the existing solution incorporates the Cisco Security Manager , Cisco CNS 2100 Series Intelligence Engine, ,management gateway, and data gateways. Utilizing a broad set of APIs based on Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML), these systems are integrated with the existing corporate IT network management infrastructure, including the authentication, authorization, and accounting (AAA) servers.

In the remote end, the solution incorporates simple and easy-to-deploy solutions and robust Cisco IOS Software security features such as antitheft protection, antivirus protection, and several authentication mechanisms, including PKI-AAA based and Auth-Proxy–AAA–based user authentication.

Based on this infrastructure, the remote end can be automatically provisioned/decommissioned and fully controlled and managed, while maintaining the ability to apply, change, and audit security policies. Figure1 provides a pictorial overview of the Cisco Virtual Office solution.

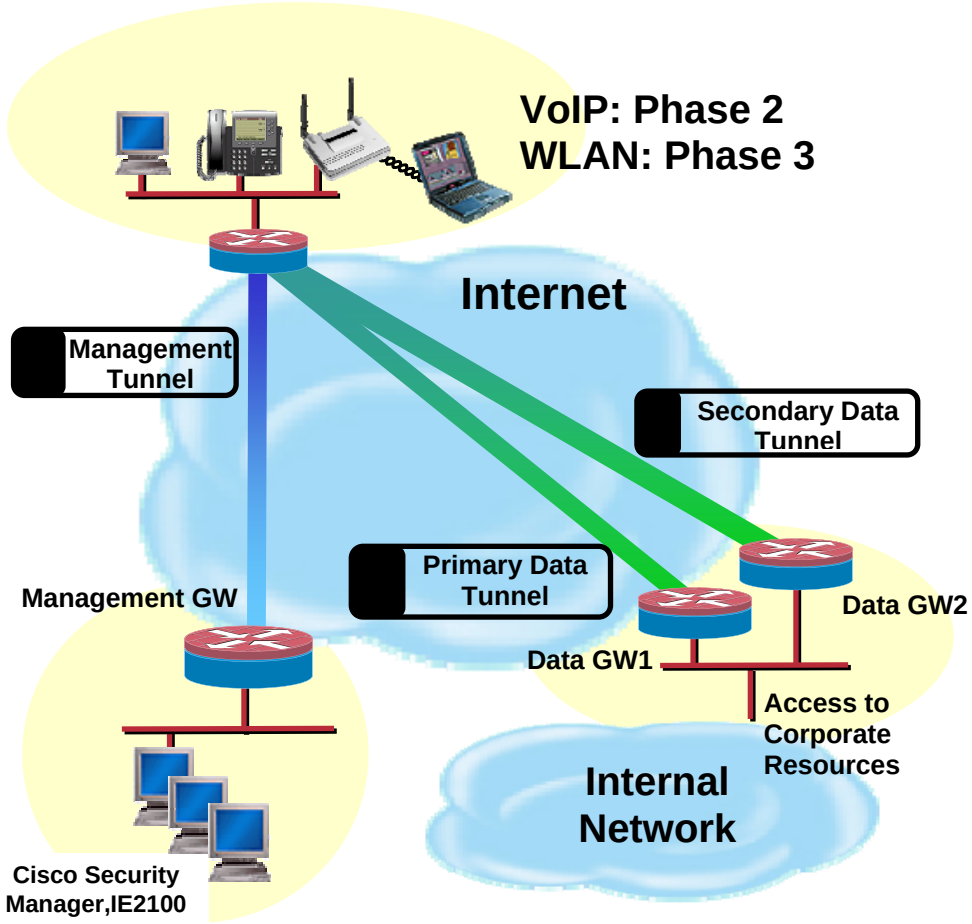
Cisco Virtual Office is a complete solution built upon end-to-end:

- Connectivity
- Security
- Provisioning
- Management

New features in each of these areas have enabled IT to implement Cisco Virtual Office that provides a secure, flexible, and autoprovisioned service to Cisco employees.

[2] Day extenders are employees who normally work from conventional offices, but also spend several hourworking in their homes each day.

Figure 1 Cisco Virtual Office Spoke Router Connectivity



- Spoke routers "call home" and management tunnel is set up
- Management GW authenticates spoke router using PKI-AAA integration
- ISC pushes & audits policy over management tunnel
- Spoke router establishes VPN tunnel w/Data GW1, gains access to corporate resources
- VPN tunnel established w/Data GW2 and stays active for failover (<= 15 seconds)

3. Technical Design

Details of the Cisco Virtual Office solution are covered in the following sections:

- Connectivity
- Security
- Management
- Provisioning

3.1 Connectivity

The Cisco Virtual Office solution offers secure end-to-end connectivity for spoke routers. Each spoke is configured with a separate plain IP Security (IPSec) management tunnel and two IPSec data tunnels based on Dynamic Multipoint VPN (DMVPN). The respective tunnels terminate on a Management Gateway **[**and the two Data GWs at a corporate site with an Internet POP. The Management GW for a specific spoke router does not have to be located at the same corporate site as the Data GWs. All spoke routers run EIGRP AS<AS#>. Failover for spokes between Data GW routers is controlled via EIGRP. The following pages provide detailed connectivity information as follows:

- Plain IPSec-Based Management Tunnel
- DMVPN-Based Data Tunnels
- IP Connectivity
- IP Services

3.1.1 Plain IPSec-Based Management Tunnel

A plain IPSec tunnel will be established between the spoke router and the management GW. On the spoke router, the management tunnel is implemented using a static crypto-map configured so that spoke routers must initiate the negotiation for establishing the IPSec tunnel. The management GW is configured with a dynamic crypto map. CNS traffic from the spokes destined to the management subnet should initiate the ISAKMP negotiation between the spoke router and the Management GW, leading to the establishment of an IPSec tunnel between the two devices and providing connectivity for the management GW, Cisco Security Manager, Cisco CNS 2100 Series Intelligence Engine, and certificate servers.

The Management GW authorizes the spoke router for the management tunnel using PKI-AAA integration. Specifically, PKI-AAA integration is configured under the trustpoints for each certificate server on the Management GW. In order to verify that the certificate presented by the spoke router is valid, the Management GW acts as a proxy and sends the device name of the spoke router extracted from the certificate to the regional ACS servers via RADIUS. If the device has a valid account in the appropriate group on the ACS

server, then it will honor the authorization request, and the Management GW will continue to negotiate the IPSec security association with the spoke router. If the spoke router does not have a valid account in the correct group on the AAA server, then the Management GW will reject the spoke router certificate and will not negotiate an IPSec security association with the spoke router.
Certificates issued by the trustpoints of either the certificate server 1 in each management hub or the SDP Registrar will be used to authenticate the appropriate spoke router management tunnel. For spoke routers configured via SDP the management tunnel will be authorized using the SDP Registrar trustpoint, while spoke routers configured via the Certificate Proxy method will be authorized under the certificate server 1 in each management hub. For details of these configuration methods please see section 3.4.2 of this document. Briefly, the certificate server currently operating on the SDP Registrar will eventually be eliminated when the SDP Registrar software supports the sub-CS mode of configuration. It was decided not to run the SDP Registrar in RA mode because of the significantly longer delay (over one minute) that clients will experience during the provisioning process.

This plain IPSec tunnel will be configured to use tunnel mode, 3DES data encryption, and the Secure Hash Algorithm (SHA) as its hash. IKE parameters are negotiated using 3DES encryption with all other IKE parameters set at default, including hash (SHA), group (768 bit Diffie-Hellman), and lifetime (86,400 seconds = 1 day).

Spoke Router Configuration

crypto isakmp policy 1 | Defines IKE policy and sets it to the highest priority
encr 3des | Sets encryption to 3DES for IKE negotiation
crypto isakmp keepalive 10 5 | 10 seconds between DPD messages and 5 DPDs before tearing down SA if no response. DPD is used to detect peer status
crypto isakmp nat keepalive 10 | 10 seconds between NAT keepalives, which are sent if IPSec does not send or receive a packet within a specified period. If NAT keepalives are enabled, then the value must be less than the NAT mapping expiration timer of 20 seconds.

crypto ipsec transform-set t1 esp-3des esp-sha-hmac | specifies properties for IPSec encryption for the management tunnel

crypto map ISC_CME 1 ipsec-isakmp
description Management Tunnel - SMG
set peer < IP address of loopback interface of Management GW>
set security-association lifetime kilobytes <kbps> | IPSec SA lifetime in kilobytes
set security-association lifetime seconds <seconds> | IPSec SA lifetime in seconds
set transform-set t1 | transform-set t1 to be used for IPSec encryption for management tunnel
match address smg_acl | traffic that should trigger crypto-map

interface Ethernet1
crypto map ISC_CME
ip access-list extended smg_acl | ACL that is matched to establish management tunnel

permit ip host <ip address of spoke router E0 interface> <management hub subnet> <wildcard mask for management hub subnet> | only traffic sourced from Interface Ethernet 0 of the spoke Cisco 831 Ethernet Broadband Router can initiate, negotiate, and traverse the management tunnel.

Management GW Configuration

crypto isakmp policy 1
encr 3des
crypto isakmp keepalive 10 5 |
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10 | dynamic crypto map "dmap"
set transform-set t1
!
crypto map ibv local-address Loopback0 | specifies IP address of Loopback 0 to be used with the crypto map "ibv"
crypto map ibv 1 ipsec-isakmp dynamic dmap | the first sequence of the ibv crypto map should negotiate IPSec parameters using ISAKMP as a dynamic crypto map dmap
interface Loopback0
!
ip address <Management GW routable loopback interface ip address> 255.255.255.255
interface FastEthernet0/0
crypto map ibv

3.1.2 DMVPN-Based Data Tunnels

The fundamental technologies comprising DMVPN[3] are IPSec, Next Hop Resolution Protocol (NHRP), and multipoint Generic Routing Encapsulation (mGRE).

3.1.2.1 IPSec

DMVPN uses the concepts of "IPSec Profiles" and "Tunnel Protection" that are applied to the tunnel interface instead of the physical interface. ACLs do not have to be defined for the tunnel configuration. An important advantage of DMVPN is that in a plain IPSec environment, removing a crypto map from the physical interface or modifying the access-lists carries the risk of losing connectivity with the remote spoke. In a DMVPN environment, crypto maps or IPSec policies are not applied to the physical interface. As a result, it becomes easier to manage the network because changes of policy can be performed while minimizing the risk of connectivity loss.

[3] http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba1.html#53110.

The Data GWs use the dynamic property of NHRP to allow all of the DMVPN spokes to register with it. The spoke router establishes an IPSec security association (SA) with the Data GWs and seamlessly joins the NHRP database without any modification of the Data GW's DMVPN tunnel configuration. This dynamic NHRP mapping is similar in function to the "dynamic crypto map" feature in plain IPSec.

Similar to the plain IPSec Management VPN tunnel, the DMVPN-Based IPSec Data tunnels are configured using 3DES encryption, with the Secure Hash Algorithm (SHA) the preferred hash. IKE parameters are also negotiated using 3DES encryption with all other parameters set at default, including hash (SHA), group (768 bit Diffie-Hellman), and lifetime (86,400 seconds = 1 day). However, IPSec transport mode is implemented for the data VPN tunnels in order to permit users to install their spoke router in a PAT environment. Because the data is first encrypted in GRE prior to the IPSec encryption, the IP address of the true end-points will not be revealed in the IP header. As a result there is no additional security risk incurred by implementing transport vs. tunnel mode. The DMVPN data tunnels are authorized using the same PKI-AAA integration mechanism utilized to authorize the management tunnels. The Data GWs are configured with the PKI-AAA integration to authorize the data tunnels using the certificate server 2 in each management hub.

3.1.2.2 mGRE Tunnel Interface

Because it utilizes mGRE, DMVPN requires one tunnel definition on both hub data GWs and the spoke router(s). As a result, a single GRE interface supports multiple IPSec tunnels and simplifies the size and complexity of the configuration on both the hub and spoke routers. Note that each tunnel interface should be conservatively limited to a maximum of 350 spokes because multicast packet duplication by the mGRE interface could overwhelm the packet queue into the crypto engine. When there are 350 spokes configured on the tunnel interface, then we just add an additional tunnel interface. All of the EIGRP neighbors across all of the mGRE interfaces can be configured in the same EIGRP AS. However, we will be limited by the number of spokes that can be connected to a hub router due the limit of how many neighbors EIGRP can accommodate, which is estimated to be around 800-1000 routers.

As a result of the maximum of 350 spokes per tunnel interface, a /23 subnet will be required to accommodate each corresponding pair of tunnel interfaces on the Data GWs and all 350 spoke routers in the mGRE interface. Since all routers participate in the same mGRE instance, all tunnel interfaces on the spokes as well as the pair on the Data GWs will be configured with a /23 subnet mask. In Cisco Virtual Office, nonroutable address blocks will be assigned to the tunnel subnets. These addresses will not be reachable from outside of specific Data GWs or spoke routers participating in the associated EIGRP AS or mGRE instance.

Multicast is being offered to clients on an as-requested basis. However, under the proposed Data GW configuration, multicast will be suitable only for general purposes and will not scale to large-scale audiences such as company meetings. For large scale meetings clients will continue to have to rely upon the multicast to unicast solution made available to other VPN

clients. Capacity for multicast enabled clients is limited to 250 active multicast sessions on a Data GW by the VAM2. Further, at 128Kbps, 350 sessions would require 45Mbps and an interface queue with a minimum of 350 packets just to accommodate the multicast replication that is sent through the VAM2. As a result the CPU on the Data GWs would spike and the QoS implications are also likely to be high.

3.1.2.3 NHRP

NHRP is a client and server protocol in which the hub is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of each spoke. Each client registers its public IP address with the server when it boots and queries the NHRP database for public IP addresses of the destination spokes in order to build direct tunnels. By default, the interesting traffic for NHRP is all non-NHRP packets, and this traffic will initiate NHRP packets so a client will try to join the NHRP fabric upon startup.

DMVPN Configurations

The spoke router GRE tunnel is preconfigured with information about the hub router using NHRP commands.

Spoke Router DMVPN Configuration

crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
mode transport | Transport mode is required to accommodate spokes operating in a PAT environment where multiple spoke routers may be assigned the same IP address on the Ethernet 1 Public interface.

crypto ipsec profile ISC_IPSEC_PROFILE_1 | An IPSec profile abstracts the IPSec policy settings into a single profile that can be used in other parts of the Cisco IOS Software configuration.
set security-association lifetime kilobytes 530000000
set security-association lifetime seconds 14400
set transform-set ISC_TS_1

interface Tunnel0
description Provisioned by ISC: Peer location = ABC-office device = ABC-sdg1
bandwidth 2000
ip address <ip-address-mGRE-tunnel-interface> <subnet-mask-mGRE-tunnel-interface> | The mGRE tunnel interface on the spoke routers and the associated mGRE tunnel interface on the Data GWs are on the same IP subnet.
no ip redirects
ip mtu 1400
ip nhrp map <primary-Data-GW-mGRE-tunnel-interface-IP-address> <primary-Data- GW-routable-loopback-interface-IP-address> | Statically maps routable IP Address of Primary Data GW to the Primary Data GW's Tunnel (mGRE) Interface IP address for NHRP.

ip nhrp map multicast <primary-Data-GW-routable-loopback-interface-IP-address> | Configures the primary Data GW as destination for broadcast or multicast packets sent over the mGRE tunnel interface.
ip nhrp map <secondary-Data-GW-mGRE-tunnel-interface-IP-address> <secondary- Data-GW-routable-loopback-interface-IP-address> | Statically maps routable IP Address of Secondary Data GW to the Secondary Data GW's Tunnel (mGRE) Interface IP address.
ip nhrp map multicast <secondary-Data-GW-routable-loopback-interface-IP-address> | Configures the secondary Data GW as destination for broadcast or multicast packets sent over the mGRE tunnel interface.
ip nhrp network-id <network-identifier> | Enables NHRP on this interface. All spoke routers and backup hub routers in the same logical NHRP fabric must use the same network identifier. For Cisco Virtual Office the same network identifier on the same interface on each router comprising a Data GW pair is maintained.

ip nhrp holdtime 300 | Specifies how many seconds the NHRP clients should maintain the addresses provided in NHRP responses.
ip nhrp nhs <IP address of mGRE interface of Primary GW> | IP Address of Primary Data GW mGRE Interface IP address.
ip nhrp nhs <IP address of mGRE interface of Secondary GW> | IP Address of Secondary Data GW mGRE Interface IP address.
qos pre-classify
tunnel source Ethernet1 | Ethernet 1 is the WAN interface of the Cisco 831 Ethernet Broadband Router
tunnel mode gre multipoint | Enables GRE tunneling in multipoint fashion. The mGRE interface with all its spokes and Data GWs is an NBMA network.
tunnel key <Tunnel_Key_No> | Must match the tunnel key identifier on the hub to differentiate the traffic for each mGRE interface (DMVPN instance)
tunnel protection ipsec profile ISC_IPSEC_PROFILE_1 | Associates the IPSec profile ISC_IPSEC_PROFILE_1 with the GRE interface. It specifies that the IPSec encryption will be completed after the GRE encapsulation has been added to the packet

Data GW DMVPN Configuration
crypto isakmp policy 1
encr 3des
crypto isakmp keepalive 30 5
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
mode transport require
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
crypto ipsec profile ect-profile-1
set transform-set t1 t2
Only the loopback 1 interface on the hub Data GW is accessible from the Internet via ESP, ISAMKP, and UDP port 4500 (NAT-T).
interface Loopback1 |
ip address <routable IP address of loopback interface of Data GW> 255.255.255.255

interface Tunnel <Tunnel-interface-number> | mGRE Tunnel Interface; currently should not exceed 800-1000 spoke routers per Data GW or 375 spoke routers per mGRE interface.
description DMVPN w/o ST
bandwidth 2000
ip address <IP-address-tunnel-interface> <subnet-mask-tunnel-interface> | Subnet for tunnel interfaces on both hubs and spoke routers in DMVPN cloud. For most cases the mask will be a /23 as the number of spokes per mGRE interface is limited to 375.
no ip redirects
ip mtu 1400
ip pim nbma-mode | PIM configured for NBMA mode for the mGRE interface
ip pim sparse-dense-mode
ip multicast rate-limit out 768
ip nhrp map multicast dynamic | NHRP will automatically create a broadcast/multicast mapping for spoke routers when they register with the NHRP server
ip nhrp network-id <Network_ID_No> | as specified for the specific Data GW hub and tunnel interface

ip nhrp holdtime 600 | NBMA addresses are advertised as valid for 600 seconds in positive authoritative NHRP responses.

ip nhrp server-only | Prevents the hub from initiating any NHRP requests; as a result, the hub can only respond to NHRP requests
no ip split-horizon eigrp <AS_No> | Split horizon on the mGRE tunnel interface must be disabled; otherwise, EIGRP will not advertise routes learned via the mGRE interface back out that interface – not required unless split-tunneling is enabled.
delay 2000
tunnel source Loopback1
tunnel mode gre multipoint | Enables a GRE tunnel to be used in multipoint fashion. Multipoint tunnels require that you configure a tunnel key. Otherwise, unexpected GRE traffic could easily be received by the tunnel interface. For simplicity, we recommend that the tunnel key correspond to the NHRP network
tunnel key <Tunnel_Key_No> | The tunnel key will be the same as the ip nhrp network-id.
tunnel protection ipsec profile ect-profile-1 shared | Associates this tunnel interface with the IPSec profile ect-profile-1

3.1.3 IP Connectivity

IP Connectivity for the spoke routers and all core equipment is covered in the following sections:

- Spoke routers
- Data GWs
- Management GW

3.1.3.1 Spoke Routers

The interface Ethernet 0 of each spoke router is assigned a /28 RFC 1918 address and subnet that are routable in the internal Cisco network. This subnet will be part of a larger address block that is configured on the NAT infrastructure to allow access to the Internet. The spoke routers are configured to run EIGRP using the internal AS. Their only EIGRP neighbors are the two Data GWs. The spoke router Tunnel 0 and Ethernet 0 interfaces are configured as EIGRP interfaces in the internal AS, and spoke routers are configured to advertise only subnets assigned to these interfaces.

Spoke routers are configured with one of three methods to assign or obtain an IP address on the E1 interface: DHCP, Static, and PPPoE. The user is required to correctly configure their E1 interface and also provide this information when requesting the Cisco Virtual Office service. Instructions written for users instructing them on how to configure their Cisco 831 Ethernet Broadband Router to gain Internet access using Cisco Router Web Setup (RWS) is made available on the Remote Access Webpages. This information will be supplemented by guidelines on how to use Secure Device Manager (SDM) to also allow users to configure their routers.A user will have to open a case to changes ISPs or the method to assign the IP address to the Ethernet 1 or Dial 1 interface.

Each spoke will be configured with three static routes pointing out the E1 interface for the following destinations:

- Management subnet for the spoke
- Loopback address of the Management GW
- Loopback addresses of Data GW subnet

Spoke routers with interface E1 addresses assigned statically or via PPPoE require an additional floating static default route that is superseded by the default route learned via EIGRP once routing is established between the spoke and Data GWs.

Spoke Router IP Configuration

interface Ethernet0
description Provisioned by ISC (private interface)
ip address <router ip address of subnet assigned to spoke router> 255.255.255.240 | RFC 1918 subnet routable in Cisco; all spoke router subnets assigned a /28
ip nat inside | NAT required to permit access to the Internet if IPSec tunnels are not established
ip inspect ISC_inside_1 in
ip tcp adjust-mss 1264 | 136 bytes less than MTU of tunnel interface to accommodate IPSec and GRE encapsulation
cdp enable
hold-queue 100 out

interface Ethernet1
description Provisioned by ISC (public interface)
ip address dhcp | IP Address on public interface assigned via DHCP

ip access-group ISC_FIREWALL_outside_inbound_1 in
ip nat outside
ip route-cache flow
duplex auto
fair-queue
no cdp enable

router eigrp <AS_No>

network <ip-subnet-interface-E0> <wildcard-subnet-mask-E0-subnet>
network <ip-subnet-interface-T0> <wildcard-subnet-mask-of-T0-subnet>
distribute-list ISC_IPSEC_REDISTRIBUTE_LIST_1 out
no auto-summary
eigrp stub connected | Data GWs will not send EIGRP queries to the spoke routers if all spokes are configured as EIGRP stubs

ip classless
ip route <IP-subnet-Data-GW's> <Data GW IP subnet mask> <dhcp | next-hop IP address| dialer1> | static route to next hop to reach the Data GWs; next hop depends upon method used to assign IP address to the interface E1 (static or dhcp) or D1 (PPPoE)
ip route <IP-address-Management-GW-routable-loopback-interface> <loopback- interface-mask> <dhcp|next-hop-IP-address|dialer1> | static route to next hop to reach Management GW loopback interface
ip route <IP-subnet-Management-subnet> <IP-subnet-mask-Management-subnet> <dhcp | next-hop-IP-address| dialer1> | static route to next hop to reach Management subnet

ip nat inside source route-map ISC_IP_NAT_DYNAMIC_ROUTEMAP_1 interface <Ethernet1| Dialer1> overload | WAN interface that is assigned an IP address (Ethernet 1 for dhcp and static and Dialer 1 for PPPoE)

ip access-list standard ISC_IPSEC_REDISTRIBUTE_LIST_1
permit <IP-subnet-interface-Ethernet-0> <wildcard subnet mask for Ethernet 0>
permit <IP-subnet-interface-Tunnel-0> <wildcard subnet mask for Tunnel 0>

ip access-list extended ISC_IP_NAT_DYNAMIC_ACL_1
permit ip <IP-subnet- interface-Ethernet-0> <IP-subnet-interface-Tunnel-0> any

route-map ISC_IP_NAT_DYNAMIC_ROUTEMAP_1 permit 10
match ip address ISC_IP_NAT_DYNAMIC_ACL_1

An example of the floating static route that is applied to spoke routers with the IP address assigned statically or via PPPoE to the outside interface:
ip route 0.0.0.0 0.0.0.0 <dialer1|next-hop-IP-address> 240 | Administrative distance of 240; default route learned from EIGRP will supersede this route.

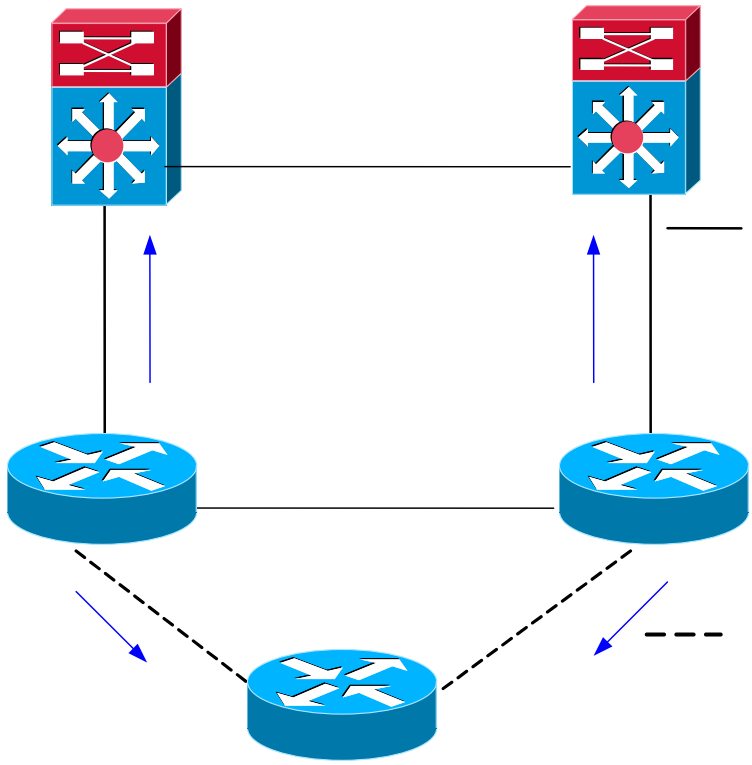
3.1.3.2 Data GWs

The Data GWs are configured for hub-to-spoke operation. The Data GWs run EIGRP and have redundant connections to the corporate network.

3.1.3.2.1 Standard Data GW Configuration Without Building Failover

Figure 2 shows the Data GW connectivity for sites with the GWs located in the same physical location or without building failover. The Data GWs advertise a summary of the IP subnets assigned to the spoke routers into the corporate EIGRP AS to the routers upstream from the Data GWs. The Data GWs are configured to accept only the default route from the corporate EIGRP AS. An Offset-list is applied on the secondary Data GW, to help ensure seamless failover in the event the primary Data GW stops routing.

Figure 2 Cisco Virtual Office Data GW (SDG) Connectivity Without Building Failover



Standard Data GW Configuration Without Building Failover

interface Loopback0
ip address <routable-IP-address> 255.255.255.255

interface Port-channel1
ip address <IP-address-Port-channel-interface> <subnet-mask-port-channel-interface>
ip pim sparse-dense-mode
hold-queue 150 in

interface Tunnel10
description DMVPN w/o ST
bandwidth 2000
ip address <IP-address-tunnel-interface> <subnet-mask-tunnel-interface> | the mGRE tunnel interface on the spoke routers and the associated mGRE tunnel interface on the Data GWs are on the same IP subnet.
no ip redirects
ip mtu 1400
no ip next-hop-self eigrp <AS#> | not required if spoke-to-spoke tunnels are not permitted
ip pim nbma-mode | PIM configured for NBMA mode for the mGRE interface
ip pim sparse-dense-mode
ip multicast rate-limit out 768
ip nhrp map multicast dynamic | NHRP will automatically create a broadcast/multicast mapping for spoke routers when they register with the NHRP server
ip nhrp network-id <Network_ID_No> | as specified for this Data GW hub and tunnel interface
ip nhrp holdtime 600
ip nhrp server-only | Prevents the hub from initiating NHRP requests; as a result, the hub can only respond to NHRP requests
no ip split-horizon eigrp <AS_No> | Split horizon on the mGRE tunnel interface must be disabled; otherwise, EIGRP will not advertise routes learned via the mGRE interface back out that interface – required if split-tunneling is enabled.
delay 2000
tunnel source Loopback0
tunnel mode gre multipoint | Enables a GRE tunnel to be used in multipoint fashion. Multipoint tunnels require that you configure a tunnel key. Otherwise, unexpected GRE traffic could easily be received by the tunnel interface. For simplicity, we recommend that the tunnel key correspond to the NHRP network id.
tunnel key <Network_ID_No> | The tunnel key will be the same as the ip nhrp network-id.
tunnel protection ipsec profile ect-profile-1 shared | Associates this tunnel interface with the IPSec profile ect-profile-1
!
interface GigabitEthernet0/1
description <next-hop-router-name> <next-hop-router-interface>
ip address <ip-address-data-gw> <subnet-mask-interface-g0/1> | subnet mask set to /28 for interfaces in the same subnet, G0/1 interfaces in same subnet

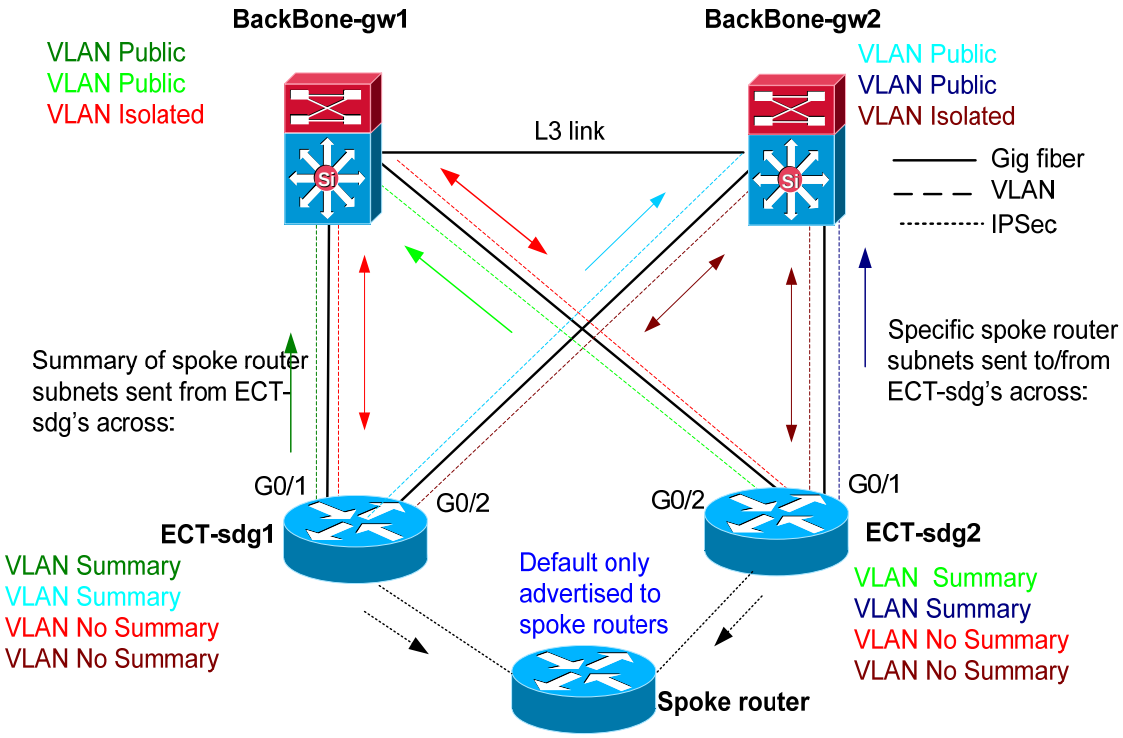
ip pim sparse-dense-mode
duplex full
speed 100
media-type rj45 | if available, sites may implement gigabit connectivity using GBICs
no negotiation auto
!
!
interface GigabitEthernet0/2
description <next-hop-router-name> <next-hop-router-interface>
ip pim sparse-dense-mode
duplex full
speed 100
media-type rj45
no negotiation auto
channel-group 1
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no negotiation auto
channel-group 1
!
router eigrp <AS_No>
offset-list OFFSET out 10000000 Tunnel10 | Applied only on secondary Data GW for failover
network <IP-address-block-non-routable-interface-IP-addresses> | for most installations this is 10.0.0.0
network <IP-address-block routable-interface-IP-addresses> | Loopback interface routable IP address subnet
distribute-list ECT_VALID_ROUTES out GigabitEthernet0/1 | Permits only spoke router Ethernet subnets and Data GW interfaces to be advertised from the Data GW
distribute-list DEFAULT_ONLY in GigabitEthernet0/1 | Data GW only requires default as long as spoke routers are configured in non-split-tunneling configuration
distribute-list DEFAULT_ONLY out Tunnel10 | For non-split-tunneling spoke route configurations, only default will be advertised via EIGRP
distribute-list SPOKE_ROUTES in Tunnel10 | Eliminates possibility of spoke routers advertising route for other part of network back into corporate
no auto-summary
!
ip classless
!
!
ip access-list standard DEFAULT_ONLY
permit 0.0.0.0

ip access-list standard OFFSET | Required only on secondary Data GW in an mGRE instance
permit any
ip access-list standard ECT_VALID_ROUTES
permit <ip-address-interface-L0> | the IP address of the routable Loopback interface address
permit <ip-address-interface-L0-opposite-SDG> | the IP address of the routable Loopback interface address of the opposite SDG
permit <ip-address-block-spoke-routers> <wildcard-subnet-mask>
permit <ip-address-subnet-opposite-SDG-G0/1-subnet> <wildcard-subnet-mask>
permit <ip-address-block-mGRE-interface-subnets> <wildcard-subnet-mask> | not initially required to advertise mGRE interfaces from Data GWs but will be implemented by Phase 2
ip access-list standard SPOKE_ROUTES
permit <ip-address-block-spoke-routers> <wildcard-subnet-mask>
permit <ip-address-block-mGRE-interface-subnets> <wildcard-subnet-mask>

3.1.3.2.2 Standard Data GW with Building Failover

The Data GW connectivity, shown in Figure 3, has been set up to provide failover of the Data GWs when the routers are in physically different locations. To accomplish this, trunking between the Cisco Virtual Office Data GWs and the upstream layer 3 switches is required. Two subinterfaces in two different VLANs, a “Public” and “Private” VLAN, have been configured on each physical interface on each Cisco Virtual Office Data GW. The next hop routers form EIGRP neighbor relationships with the Cisco Virtual Office Data GWs through the Public VLANs. The Cisco Virtual Office Data GWs form EIGRP neighbor relationships with each through the Private (isolated) VLAN in which only the Cisco Virtual Office Data GWs are configured with IP addresses. Separate VLANs are used in order to prevent Spanning Tree protocol convergence during a physical link failure. In addition to the Cisco Virtual Office Data GW connectivity configuration, the associated next hop router configuration is provided for this topology in the following pages.

Figure 3 Cisco Virtual Office Data GW Topology and Routing for Sites with Building Failover



Cisco Virtual Office Primary Data GW Connectivity Configuration for Sites with Building Failover

interface Loopback0
ip address <routable-IP-address> <host-subnet-mask>
!
interface Tunnel10
description DMVPN mGRE interface
bandwidth 2000
ip address <IP-address-tunnel-interface> <subnet-mask-tunnel-interface> | the mGRE tunnel interface on the spoke routers and the associated mGRE tunnel interface on the Data GWs are on the same IP subnet.
no ip redirects
ip mtu 1400
no ip next-hop-self eigrp <AS#> | not required if spoke-to-spoke tunnels are not permitted
ip pim nbma-mode
ip pim sparse-dense-mode
ip multicast rate-limit out 768
ip nhrp map multicast dynamic | PIM configured for NBMA mode for the mGRE interface| NHRP will automatically create a broadcast/multicast mapping for spoke routers when they register with the NHRP server
ip nhrp network-id <Network_ID_No> | as specified for the specific Data GW hub and tunnel interface
ip nhrp holdtime 600
ip nhrp server-only | Prevents the hub from initiating any NHRP requests; as a result, the hub can only respond to NHRP requests
no ip split-horizon eigrp <AS_No> | Split horizon on the mGRE tunnel interface must be disabled; otherwise, EIGRP will not advertise routes learned via the mGRE interface back out that interface – not required now but will be if split-tunneling is enabled.
delay 2000
tunnel source Loopback0
tunnel mode gre multipoint | Enables a GRE tunnel to be used in multipoint fashion. Multipoint tunnels require that you configure a tunnel key. Otherwise, unexpected GRE traffic could easily be received by the tunnel interface. For simplicity, we recommend that the tunnel key correspond to the NHRP network
tunnel key <Network_ID_No> | The tunnel key will be the same as the ip nhrp network-id.
tunnel protection ipsec profile ect-profile-1 shared | Associates this tunnel interface with the IPSec profile ect-profile-1

interface GigabitEthernet0/1
description <next-hop-router-name> <next-hop-router-interface>
no ip address
duplex full
speed 1000
media-type GBICs

negotiation auto
!
interface GigabitEthernet0/1.100
description ECT Public
encapsulation dot1Q 100
ip address <"public"-vlan-ip-address> <subnet-mask> | /30 subnet unique between this interface and next hop router
ip summary-address eigrp <AS_No> <IP-address-subnet-spoke-routers> <wildcard-subnet-mask>
ip summary-address eigrp <AS_No> <IP-address-subnet-NHRP-(mGRE)-subnet> <wildcard-subnet-mask> | may be added in later phases if we want to advertise the subnet for the mGRE interfaces
!
interface GigabitEthernet0/1.102
description <next-hop-router> ECT Private
encapsulation dot1Q 102
ip address <"private"-vlan-ip-address> <subnet-mask> | /29 subnet currently is used between the corresponding interfaces on the Data GWs.
!
interface GigabitEthernet0/2
description <next-hop-router> <next-hop-router-interface>
no ip address
duplex full
speed 1000
media-type GBICs
negotiation auto
!
interface GigabitEthernet0/2.200
description <next-hop-router> ECT Public
encapsulation dot1Q 200
ip address <"public"-vlan-ip-address> <subnet-mask> | /30 subnet unique between this interface and next hop router
ip summary-address eigrp <AS_No> <IP-address-subnet-spoke-routers> <wildcard-subnet-mask>
ip summary-address eigrp <AS_No> <IP-address-subnet-NHRP-(mGRE)-subnet> <wildcard-subnet-mask>
!
interface GigabitEthernet0/2.202
description <next-hop-router> ECT Private
encapsulation dot1Q 202
ip address <"private"-vlan202-ip-address> <subnet-mask> | Currently /29 subnet between the corresponding interfaces on the Data GWs.
!
router eigrp <AS_No>
network <IP-address-block-non-routable-interface-IP-addresses>
network <IP-address-block routable-interface-IP-addresses>
distribute-list ECT_Valid_Routes out GigabitEthernet0/1.100
distribute-list ECT_Valid_Routes out GigabitEthernet0/2.200
distribute-list Permit_Default out Tunnel10
distribute-list SPOKE_ROUTES in Tunnel10


```
no auto-summary
!
ip access-list standard ECT_Valid_Routes
 remark ACL to filter valid ECT routes
permit <ip-address-interface-L1> | the IP address of the routable Loopback interface address
permit <ip-address-block-spoke-routers> <wildcard-subnet-mask>
 permit <ip-address-block-mGRE-interface-subnets> <wildcard-subnet-mask> | necessary only if
mGRE interface subnets are advertised into corporate network
!
ip access-list standard Permit_Default
 remark --Default route--
 permit 0.0.0.0
!
ip access-list standard SPOKE_ROUTES
 permit <ip-address-block-spoke-routers> <wildcard-subnet-mask>
 permit <ip-address-block-mGRE-interface-subnets> <wildcard-subnet-mask>
```

Cisco Virtual Office Secondary Data GW Connectivity Configuration for Sites with Building Failover

```
interface Loopback0
 ip address <routable-IP-address> <host-subnet-mask>
!
interface Tunnel10
description DMVPN mGRE interface
 bandwidth 2000
 ip address <IP-address-tunnel-interface> <subnet-mask-tunnel-interface>  no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp <AS#>
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip nhrp map multicast dynamic
 ip nhrp network-id <Network_ID_No>
 ip nhrp holdtime 600
 ip nhrp server-only
 no ip split-horizon eigrp <AS_No>
 delay 2000
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key <Network_ID_No>
 tunnel protection ipsec profile ect-profile-1 shared

interface GigabitEthernet0/1
 description <next-hop-router-name> <next-hop-router-interface>
 no ip address
 duplex full
```


speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet0/1.201
description ECT Public
encapsulation dot1Q 100
ip address <"public"-vlan-ip-address> <subnet-mask> | "Public" VLANs currently /30 subnet unique between this interface and next hop router
ip summary-address eigrp <AS_No> <IP-address-subnet-spoke-routers> <wildcard-subnet-mask>
ip summary-address eigrp <AS_No> <IP-address-subnet-NHRP-(mGRE)-subnet> <wildcard-subnet-mask> | necessary only if the mGRE interface subnet is advertised into the corporate network
!
interface GigabitEthernet0/1.202
description <next-hop-router> ECT Private
encapsulation dot1Q 102
ip address <"private"-vlan-ip-address> <subnet-mask> | "Private" VLANs currently are a /29 subnet between the corresponding interfaces on the Data GWs.
!
interface GigabitEthernet0/2
description to <next-hop-router> <next-hop-router-interface>
no ip address
duplex auto
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet0/2.101
description <next-hop-router> ECT Public
encapsulation dot1Q 101
ip address <"public"-vlan-ip-address> <subnet-mask>
ip summary-address eigrp <AS_No> <IP-address-subnet-spoke-routers> <wildcard-subnet-mask>
ip summary-address eigrp <AS_No> <IP-address-subnet-NHRP-(mGRE)-subnet> <wildcard-subnet-mask>
!
interface GigabitEthernet0/2.102
description <next-hop-router> ECT Public
encapsulation dot1Q 200
ip address <"private"-vlan-ip-address> <subnet-mask> | "Private" VLANs currently are a /29 subnet between the corresponding interfaces on the Data GWs.
ip summary-address eigrp <AS_No> <IP-address-subnet-spoke-routers> <wildcard-subnet-mask>
ip summary-address eigrp <AS_No> <IP-address-subnet-NHRP-(mGRE)-subnet> <wildcard-subnet-mask>
!
interface GigabitEthernet0/3
no ip address
shutdown

duplex auto
speed auto
media-type rj45
no negotiation auto
!
router eigrp <AS#>
offset-list OFFSET out 10000000 Tunnel10 | Only required on Secondary Data GW for lower routing metric and failover
network <IP-address-block-non-routable-interface-IP-addresses>
network <IP-address-block routable-interface-IP-addresses>
distribute-list ECT_Valid_Routes out GigabitEthernet0/1.201
distribute-list ECT_Valid_Routes out GigabitEthernet0/2.101
distribute-list Permit_Default out Tunnel10
distribute-list SPOKE_ROUTES in Tunnel10
no auto-summary
!
ip access-list standard ECT_Valid_Routes
remark ACL to filter valid ECT routes
permit <Routable_Loopback_IP_Address_for VPN_Tunnel_Terminations>
permit <IP_Subnet for mGRE Interfaces> <Wildcard_Subnet_Mask>
ip access-list standard OFFSET
permit any
ip access-list standard Permit_Default
remark --Default route--
permit 0.0.0.0
ip access-list standard SPOKE_ROUTES
permit <ip-address-block-spoke-routers> <wildcard-subnet-mask>
permit <ip-address-block-mGRE-interface-subnets> <wildcard-subnet-mask>

Cisco Virtual Office Data GW's Next-Hop Router 1 Cisco Virtual Office Related Connectivity Configuration for Sites with Building Failover

interface GigabitEthernet4/1 | connection between redundant Cisco Virtual Office Data GW next-hop routers
description <next-hop-router-name>
ip address <ip-address> <subnet-mask>
ip access-group sqlfix in
ip access-group sqlfix out
ip pim sparse-dense-mode
ip route-cache flow
mls qos trust dscp

interface GigabitEthernet4/2
description <primary ECT Data GW> int g0/1 | interface connected to Primary Cisco Virtual Office Data GW
no ip address
switchport
switchport trunk encapsulation dot1q

switchport trunk allowed vlan <vlan #s> | Public VLAN and Private VLAN
switchport mode trunk
end

interface GigabitEthernet4/3
description <secondary ECT Data GW> int g0/2 | interface connected to Secondary Cisco Virtual Office Data GW
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan <vlan #s>2 | Public VLAN and Private VLAN
switchport mode trunk

interface Vlan<#>
description <primary ECT Data GW> Public
ip address <"public"-vlan-ip-address> <subnet-mask> | "Public" VLANs currently /30 subnet unique between this interface and next hop router

interface Vlan<#>
description <secondary ECT Data GW> Public
ip address <"public"-vlan-ip-address> <subnet-mask> | "Public" VLANs currently /30 subnet unique between this interface and next hop router

interface Vlan<#>
description ECT Private VLAN for <corresponding ECT Data GW next hop router> | "Private" VLANs currently are a /29 subnet between the corresponding interfaces on the Data GWs. This is a layer 2 connection on the next hop routers. Only the Cisco Virtual Office Data GWs have an IP address on this subnet.
no ip address

Cisco Virtual Office Data GW's Next-Hop Router 2 Cisco Virtual Office Related Connectivity Configuration for Sites with Building Failover
interface GigabitEthernet4/1 | connection between redundant Cisco Virtual Office Data GW next-hop routers
description <next-hop-router-name>
ip address <ip-address> <subnet-mask>
ip access-group sqlfix in
ip access-group sqlfix out
ip pim sparse-dense-mode
ip route-cache flow
mls qos trust dscp

interface GigabitEthernet4/2
description <primary ECT Data GW> int g0/1 | interface connected to Primary Cisco Virtual Office Data GW

no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan <#s> | Public VLAN and Private VLAN
switchport mode trunk
end

interface GigabitEthernet4/3
description <secondary ECT Data GW> int g0/2 | interface connected to Secondary Cisco Virtual Office Data GW
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan <#s> | Public VLAN and Private VLAN
switchport mode trunk
end

interface Vlan<#>
description <primary ECT Data GW> Public
ip address <"public"-vlan-ip-address> <subnet-mask> | "Public" VLANs currently /30 subnet unique between this interface and next hop router
end

interface Vlan<#>
description <secondary ECT Data GW> Public
ip address <"public"-vlan101-ip-address> <subnet-mask> | "Public" VLANs currently /30 subnet unique between this interface and next hop router
ip access-group sqlfix in
end

interface Vlan<#>
description ECT Private VLAN for <corresponding ECT Data GW next hop router> | "Private" VLANs currently are a /29 subnet between the corresponding interfaces on the Data GWs. This is a layer 2 connection on the next hop routers. Only the Cisco Virtual Office Data GWs have an IP address on this subnet.
no ip address

3.1.3.3 Management GW

The Cisco Virtual Office Management GW connectivity is shown in Figure 4. The Cisco Virtual Office Management GW and equipment on the management subnet, including the Cisco CNS 2100 Series Intelligence Engine, ISC server, and certificate servers, are located in the regional data center. The Management GW is configured with a static default route pointing to its interface connected to the corporate network. The Management GW will be configured to preempt the Data Center GWs as the primary router in an HSRP environment. A second HSRP

group will be configured on the Data Center GWs, and the standby IP address of this HSRP group will be the next hop configured on the static default route of the Cisco Virtual Office Management GW.

Management GW

```
crypto isakmp policy 1
 encr 3des
!
crypto isakmp keepalive 30 5
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10
 set transform-set t1
!
crypto map ibv local-address Loopback1
crypto map ibv 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 <non-routable-IP-address> 255.255.255.255
!
interface Loopback1
<routable-IP-address> 255.255.255.255

interface FastEthernet0/0
 <IP-address-ECT-mgmt-subnet> 255.255.255.240
 ip helper-address <regional-DHCP-server1> | to expedite rebuilding of servers in event of failure
 ip helper-address <regional-DHCP-server2>
 speed 100
 full-duplex
 standby ip <HSRP-group-1-IP-address>
 standby priority 110 | Cisco Virtual Office Mgmt GW should preempt other next-hop routers for the HSRP address
 standby preempt
 crypto map ibv | dynamic crypto map for spoke routers to establish tunnels with the Management GW
!
interface FastEthernet0/1
 no ip address
 shutdown
 speed 100
 full-duplex
!
interface FastEthernet1/0
 no ip address
 shutdown
duplex auto
```


speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

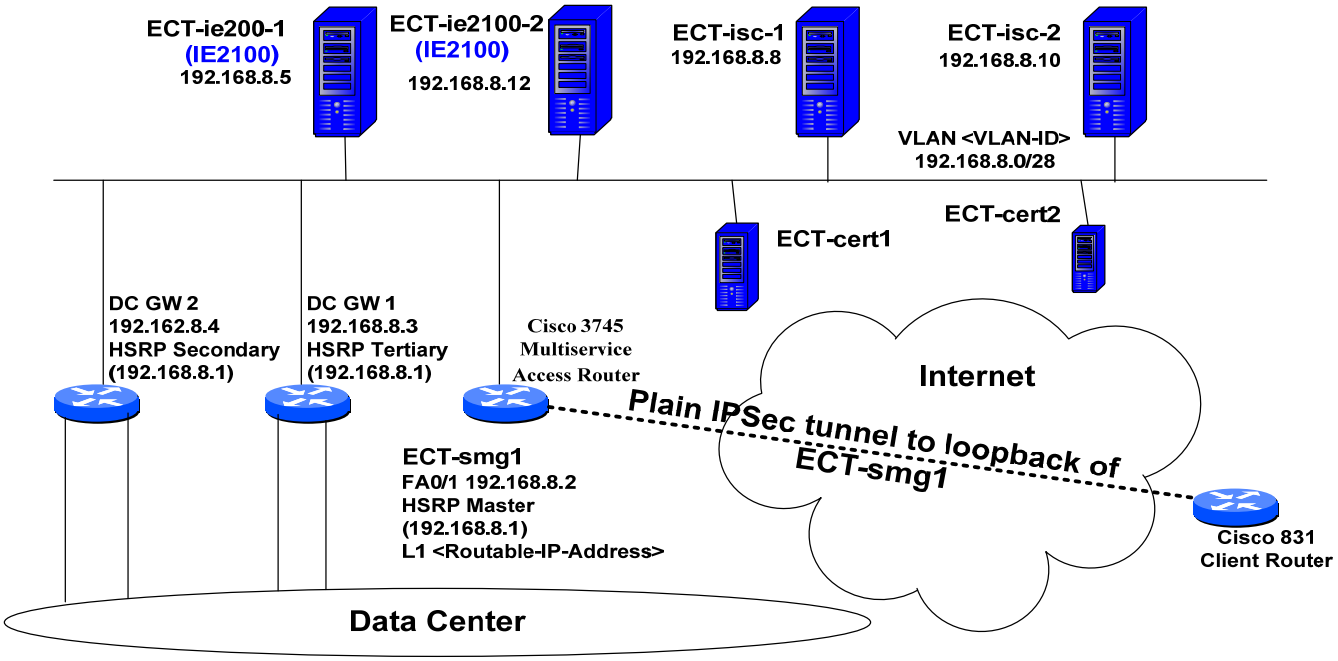
Data Center GW Cisco Virtual Office Management Subnet Configuration (Secondary HSRP Group Member)

interface Vlan<VLAN-interface-number>
description ECT VLAN (HSRP primary is <ECT-regional-Management-GW)
ip address <ip-address> 255.255.255.240
no ip redirects
ip route-cache flow
standby ip <HSRP-group-1-IP-address>
standby priority 105 | Data Center GWs will be configured as secondary and tertiary routers in HSRP group 1
standby preempt
standby <HSRP-group-number-2> *ip <ip-address-HSRP-group-number-2>* | Only the Data Center GWs will be configured in HSRP group 2
end

ip route <IP-address-Management-GW-int-Loopback-1> 255.255.255.255 <IP-address-Management-GW-int-management-subnet>
ip route <IP-address-Certificate-Server-1-int-Loopback-1> 255.255.255.255 <IP-address-Certificate-Server-1-int-management-subnet>
ip route <IP-address-Certificate-Server-2-int-Loopback-1> 255.255.255.255 <IP-address-Certificate-Server-2-int-management-subnet>

Figure 4 Management GW Connectivity

ECT-smg1 configured with static default route pointing to interface FA0/1. Static routes are configured on the DC GW's for the loopback interfaces of the Management GW, and Certificate Servers.
Data sourced from the 192.168.8.0/28 subnet destined to ECT spoke routers will be sent to ECT-smg1 (HSRP Master 192.168.8.1) which will send it out the plain IPSec tunnel. Data from 192.168.8.0/28 hosts destined for corporate network will be sent to 192.168.8.1 and then routed to the corporate network. Data from corporate network destined for hosts on 192.168.8.0/28 will be sent directly to hosts on 192.168.8.0/28 via DC GW's.



3.1.4 IP Services

The spoke routers can be configured to provide the following value-added services:

- QoS
- Multicast

3.1.4.1 QoS

Spoke routers will be configured with the QoS settings appropriate for the upstream BW as provided by users at the time they register for the Cisco Virtual Office service. Configurations will be provided for upstream BW from 128kbps. However, IT will strongly recommend that all users subscribe for ISP service with a minimum upstream bandwidth of 256kbps. The spoke router configuration for QoS has been tested successfully on the Cisco Virtual Office pilot. At this time the QoS policy can only be applied to a physical interface on the spoke Cisco 831 Ethernet Broadband Router. Future enhancements to the QoS policy are dependent upon the capability of ISC to push the QoS SR with dependencies to account for services such as video using VT Advantage. Traffic shaping BWs will initially be offered at 128, 192, 256, 384, and 512.

As the spoke routers are under IT control, the spoke routers can be considered trusted edge devices. However, measures will be examined to remark all packets originating from the spoke routers to precedence 0.

Spoke Router QoS Configuration

```
ip access-list extended ISC_OUT_QOS_ACL_Cisco-IT_ECT_VOICE_ONE_Control
  permit UDP any any eq isakmp
!
class-map match-all ISC_OUT_Cisco-IT_ECT_VOICE_ONE_VoIP
  match ip precedence 5
!
class-map match-all ISC_OUT_Cisco-IT_ECT_VOICE_ONE_Signaling
  match ip precedence 3
!
class-map match-any ISC_OUT_Cisco-IT_ECT_VOICE_ONE_Control
  match access-group name ISC_OUT_QOS_ACL_Cisco-IT_ECT_VOICE_ONE_Control
  match ip precedence 6
  match ip precedence 7
!
policy-map ISC_OUT_Cisco-IT_ECT_VOICE_ONE
  class ISC_OUT_Cisco-IT_ECT_VOICE_ONE_VoIP
    priority 80 | reserves up to 80kbps for VoIP bearer
  class ISC_OUT_Cisco-IT_ECT_VOICE_ONE_Signaling
    bandwidth percent 10 | reserves up to 10 percent of bandwidth for VoIP signaling
  class ISC_OUT_Cisco-IT_ECT_VOICE_ONE_Control
    bandwidth percent 10 | reserves up to 10 percent of bandwidth for routing protocol and
ISAKMP
```


class class-default
fair-queue
random-detect
!
policy-map ISC_OUT_Cisco-IT_ECT_VOICE_ONE_TOP
class class-default
shape average <bandwidth-in-bits-per-second> | traffic shaping from 128kbps to 768kbps
service-policy ISC_OUT_Cisco-IT_ECT_VOICE_ONE
!
interface Ethernet1
service-policy output ISC_OUT_Cisco-IT_ECT_VOICE_ONE_TOP | applies the policy-map that incorporates traffic shaping and class-maps to the Ethernet 1 interface

3.1.4.1.1 Service Assurance Agent

Service Assurance Agent (SAA) is configured on the spoke routers in the Cisco Virtual Office-Product configlet. This data can be used to troubleshoot user issues with respect to poor VoIP quality. The following commands are set up on each spoke router:

rtr responder
rtr 10 | Specifies an identification number for the SAA operation to be configured, and enters SAA RTR configuration mode.
type jitter dest-ipaddr <IP-address-secondary-Data-GW-tunnel-interface> dest-port 16384 codec g729a | initially all Cisco Virtual Office clients will be configured to measure the Mean Opinion Score for a g729a call (8Kbps)
tag jitter-with-voice-scores | jitter-with-voice-score is simply a label
frequency 180 | run every 180 seconds
rtr schedule 10 life forever start-time now

The secondary Data GW at each Data GW pair is set up to be an SAA responder to the SAA traffic initiated by the spoke routers.
rtr responder

3.1.4.2 Multicast

Multicast will be configured on spoke routers initially on an as-requested basis by users opening a case. The multicast configuration on the Data GWs is per the IT Transport template. At this time capacity for multicast enabled clients is limited to 250 active multicast sessions on the Data GW by the VAM2. Further, at 128Kbps, 350 sessions would require 45Mbs of bandwidth, and an interface queue at least 350 packets deep just to hold the multicast replication to be sent through the VAM2. The CPU on the Data GWs would dramatically increase just performing the multicast replication, before considering the probable QoS implications. As a result of these limitations, the multicast service that is offered will be general-purpose and should not be used for large-audience programs like company meetings.

Spoke Router Multicast Configuration

ip multicast-routing
interface Tunnel 0
ip pim sparse-dense-mode

interface Ethernet 0
ip pim sparse-dense-mode

3.2 Security

- Spoke router antitheft and user authentication measures
- Cisco IOS Software–based PKI
- Underlying security features

3.2.1 Spoke Router Antitheft and User Authentication Measures

- Loss of RSA private key
- Auth-proxy

3.2.1.1 Loss of RSA Private Key

If router is stolen, Boot Flash (ROMMON) is hacked, and password recovery is attempted, the private key is erased. Without the private key, the spoke router cannot successfully negotiate IPSec connectivity with the Management or Data GWs. This feature was made available for the Cisco Virtual Office pilot in Version 12.3(2)XA for the Cisco 831 Ethernet Broadband Router. By limiting spoke routers to only Cisco 831 Ethernet broadband routers, we can make sure that users cannot gain unauthorized access to the enable mode. Essentially a user cannot downgrade the Cisco IOS Software on the spoke router, perform password recovery, restore the spoke router to the initially deployed image, and have the router retain the capability of the router to establish the VPN tunnels to the Management and Data GWs because the RSA private key is destroyed.

3.2.1.2 Authentication Proxy

Authentication Proxy will be configured on all spoke routers. Authentication Proxy is a Cisco feature that will be configured to require users to authenticate when they attempt to access Cisco internal network resources from devices connected to the spoke router Ethernet 0. The authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by the authentication proxy. If no entry exists, the authentication proxy responds to the request, forcing the user's device to open a browser window and prompting the user for a username and password. Users must successfully authenticate in order to access the network resources.

In the Cisco Virtual Office deployment, users will be authenticated per IP address from the Ethernet 0 subnet. User access will be authenticated against the Active Directory servers. If the authentication succeeds, the user's authorization profile is retrieved from the AAA server. Authentication Proxy uses the information in this profile to create dynamic access control entries (ACEs) and add them to the inbound (input) access control list (ACL) of an input interface and to the outbound (output) ACL of an output interface, if an output ACL exists at the interface. For the Cisco Virtual Office spoke routers, the ACL is on the input interface (E0) and permits any traffic.

If the user passes authentication, dynamic access-control list entries are added to the interface configuration. The authentication proxy customizes each of the access list entries in the user profile by replacing the source IP addresses in the downloaded access list with the source IP address of the authenticated host. The authentication proxy sends a message to the user confirming that the login was successful, and the device will then be given immediate access to the Cisco internal network resource. As a result, if there is no traffic to a device with an IP address that has already successfully authenticated against the authentication proxy, then the dynamic ACEs will be deleted, and any user trying to access internal Cisco network resources from a device using the same IP address, including the orginal device, will have to reauthenticate.

If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries. If the user fails to authenticate after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy. The login page is refreshed each time the user makes requests to access information from a Web server.

Spoke Router Configuration for Auth-Proxy

radius-server host <IP-address-ACS-server> auth-port 1645 acct-port 1646 timeout 10 retransmit 3 key | the ACS server will be specific for the Data GW for the spoke router

```
radius-server timeout 3
!
ip domain lookup source-interface Ethernet0
ip radius source-interface Ethernet0
!
aaa authentication login default local group radius
aaa authorization exec default local
aaa authorization auth-proxy default group radius
aaa session-id common
!
ip auth-proxy max-login-attempts <#>

ip auth-proxy inactivity-timer <#s>
ip auth-proxy auth-proxy-banner http |
```


ip auth-proxy name ISC_AUTH_PROXY http list ISC_AUTH_PROXY_1
!
ip http server
ip http authentication aaa
ip http client source-interface Ethernet 0 |

ip radius source-interface Ethernet0 | Not

interface Ethernet0
description Provisioned by ISC (private interface)
ip address <IP-address-spoke-router-subnet> 255.255.255.240
ip access-group ISC_FIREWALL_inside_inbound_1 in | ACL that denies access to corporate network prior to authenticating via authentication proxy

ip inspect ISC_inside_1 in
ip auth-proxy ISC_AUTH_PROXY1 | ACL which if match permit is found triggers authentication proxy process
interface Ethernet1
ip access-group ISC_FIREWALL_outside_inbound_1 in

ip access-list extended ISC_AUTH_PROXY_1 | ACL which if match permit is found triggers authentication proxy
deny tcp any host <Call_Manager-IP-Address> eq www | Exclude phone related HTTP traffic
deny tcp any host <ACNS_CE-IP Address> eq www | Exclude Anti-Virus DAT and engine updates
deny tcp any host <Server-IP-Address> eq www | Exclude software distribution server
permit ip any <Routable-IP Address Block> <Wildcard_Subnet_Mask> | Permit corporate net

ip access-list extended ISC_FIREWALL_inside_inbound_1 | ACL that denies access to corporate network prior to authenticating via authentication proxy
permit udp any <ECT-Spoke-Router IP-addresses> <Wildcard_Subnet_Mask> eq 21862 | Cisco Virtual Office Spoke router subnets - only configured on spoke routers with tunnels to the Data GW's terminating tunnels from this spoke router: udp port 21862 is for the Cisco Trust Agent (NAC)
permit tcp any <ECT-Spoke-Router IP-addresses> <Wildcard_Subnet_Mask> eq 22 | port 22 is SSH
permit tcp any <ECT-Spoke-Router IP-addresses> <Wildcard_Subnet_Mask> eq telnet
permit udp any any eq bootps
permit tcp any any eq domain
permit udp any any eq domain
permit ip any host <ACS-Server-IP-Address> | (ACS authentication servers for auth-proxy)
permit tcp any any range 1719 1720 | VTAdvantage traffic
permit udp any any range 24576 24656 | IP phone ports used to initiate a call
permit udp any any range 2326 2340 | VTAdvantage streaming protocols
permit udp any any eq 5445 | VTAdvantage traffic
permit tcp any any eq 2000 | SIP

permit udp any any eq tftp | for IP Phone's firmware
permit udp any <ip-address-block-IP-telephones> <wildcard-subnet-mask> range 16384 32767 | VoIP data packets
permit tcp any host <Call_Manager-IP-Address> eq www | phone-related HTTP traffic
permit tcp any host <ACNS_CE-IP Address> eq www | Anti-virus DAT and engine updates
permit tcp any <ip-address-AD-servers> <wildcard-subnet-mask> eq 1026 | Windows Messenger traffic to AD servers
permit tcp any <ip-address-AD-servers> <wildcard-subnet-mask> eq 389 | LDAP traffic to AD servers
permit tcp any <ip-address-AD-server> <wildcard-subnet-mask> eq 88 | Kerberos traffic to AD servers
permit tcp any <ip-address-AD-server> <wildcard-subnet-mask>eq 445 | Microsoft Directory Services to AD servers
permit tcp any <ip-address-AD-server> <wildcard-subnet-mask> eq 135 | Windows RPC traffic to AD servers
permit udp any <ip-address-AD-server> <wildcard-subnet-mask> eq 389 | LDAP traffic to AD servers
permit udp any <ip-address-AD-server> <wildcard-subnet-mask> eq 88 | Kerberos traffic to AD servers
permit udp any <ip-address-AD-server> <wildcard-subnet-mask> eq 445 | Microsoft Directory Services to AD servers
permit tcp any host <ip-address-SSH-server> eq 22 | SSH server
permit ip any <ip-address-block-SW-VPN-concentrators> <wildcard-subnet-mask> | VPN Concentrators
permit ip any <ip-address-block-ECT-Management-subnet> <wildcard-subnet-mask> | Cisco Virtual Office Management subnet
deny ip any <ip-address-block-corporate blocks> <wildcard-subnet-mask> | Deny corporate net
permit ip any any | Permit access to any network

3.2.2.1 PKI Architecture

- Purpose of certificates
- PKI-AAA integration
- Certificate servers
- Multiple trustpoints
- Certificate lifetimes and autoenroll
- Backup of the certificate server public and private keys

3.2.2.1.1 Purpose of Certificates

Public Key Infrastructure (PKI) x.509 digital certificates are used in Cisco Virtual Office to validate the identity of the spoke routers in order to authorize the establishment of the IPSec management and data tunnels with the respective GW. The spoke router and the GW present their certificates to other devices during the initial stages of negotiation of the IPSec tunnel

with the GW. Before the GW and spoke router successfully complete the tunnel negotiation, the routers must confirm that the certificate presented by the specified device is valid and authentic. In the Cisco Virtual Office deployment, the spoke routers and the GWs are enrolled in the same certificate servers, simplifying the validation procedure, as the routers do not have query certificate authorities as a part of validation. Also as part of the validation process the GWs are configured to authorize spoke routers using PKI-AAA integration.

3.2.2.1.2 PKI-AAA Integration

In Cisco Virtual Office, PKI-AAA integration is configured on the Management and Data GWs as part of the IPSec tunnel negotiation process to authorize spoke routers to establish tunnels with the appropriate GW. PKI-AAA integration is configured under each certificate server trustpoint on all of the Management and Data GWs. The GWs verify that a certificate presented by a device that is attempting to establish an IPSec security association with the GW is valid. The Management and Data GWs act as a proxy and send the authorization request via RADIUS to AAA servers that support fixed passwords. For Cisco Virtual Office these are the regional EMAN ACS servers. If the spoke router has a valid account in the correct group on the AAA server, then it will validate the Authorization request, and the GW will continue to negotiate an IPSec security association with the spoke router. If the spoke router does not have a valid account in the correct group on the AAA server, then the GW will reject the spoke router certificate and will not negotiate an IPSec security association with the spoke router.

Certificate Revocation Lists (CRLs) are configured as optional on the trustpoints for GWs used to authenticate spoke routers. In practice, PKI-AAA integration is much more effective than a CRL in shutting down the service if it is determined that there has been a violation of a policy, virus, worm, or DoS attack. Certificate revocation is designated to revoke the rights of the user to participate in any particular SA or authentication domain under one trustpoint. However, CRLs are not updated instantly. Further, revoking the certificate does not affect the connectivity immediately. Instead, it prevents the spoke from reestablishing the connection.

With PKI-AAA authorization, the AAA server record for the targeted spoke router can be disabled or terminated, and the security associations cleared from the Management and Data GWs. This is covered in greater detail in the management section of this document.

3.2.2.1.4 Multiple Trustpoints

Spoke routers are configured with two trustpoints, and enrolled in two different PKI servers in the security domain. The specific certificate servers that enroll the router depend upon the method used to provision the router. Spoke routers provisioned with the On-line scenario using SDP are enrolled in the SDP Registrar certificate server, as well as the CERT2 server. Spoke routers deployed with the Offline and In-house methods are enrolled in the CERT1 and CERT2 certificate servers. The Management GW is enrolled in the SDP Registrar and CERT1 certificate servers. All Data GWs are enrolled in the CERT2 certificate server. With this

arrangement, the certificates issued by CERT1 would authenticate the management tunnel, while the certificates issued by CERT2 would authenticate the data tunnel.

It was decided that the management tunnels should be authenticated by certificates issued by a different certificate server than the data tunnels. As a result, a scenario may occur in which the certificate issued to a spoke router for the data tunnel could be invalid, and as a result the data tunnels could not be established. However the certificate for the management tunnel may still be valid, enabling the management tunnel to be established, in order that the spoke router configuration could be updated and enrolled in the certificate server that issued the failed certificate.

3.2.2.1.5 Certificate Lifetimes and Autoenroll

All spoke routers will be configured with 1024 bit RSA keys. Certificates issued to spoke routers from the CERT1 and CERT2 servers will have a lifetime of one year. The spoke routers are configured to autoenroll certificates from these PKI servers after 70% of the certificate lifetime has expired. Certificates issued from the SDP Registrar will have a lifetime of three years. The SDP certificate server is not configured to permit autoenroll due to concerns it is accessible through the FW.

3.2.2.1.6 Backup of the Certificate Server Public and Private Keys

The keys for the PKI certificate servers are exported in the respective certificate server directory on the ISC host as well as in the respective certificate server directory on the ISC host in the local management subnet.

3.2.2.2 PKI Server and Spoke Router Configurations and Explanations

- PKI configuration on the spoke routers
- PKI configuration on data GW
- Configuration of the AAA server Cisco Virtual Office group profile
- PKI configuration on the management GW

3.2.2.2.1 PKI Configuration of the Spoke Routers

In order to authenticate and enroll a device with a certificate server, the device must have its own RSA public and private key pair. In Cisco Virtual Office, we use 1024 bit keys. Next a trustpoint must be set on the spoke router, which identifies the certificate server in which the router will enroll. Then the spoke router must authenticate with the certificate server in order to obtain the CA certificate, and finally enroll in the certificate server to obtain its own device certificate that is issued by the same certificate server.

To generate the RSA key pair on a Cisco Router, the conventional method is to run the required command in configuration mode on the router. This method is not employed in any of the three Cisco Virtual Office provisioning models: SDP, CERT-Proxy, and In-House.

<site-username-vpn> (config)#*crypto key generate rsa*
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: *1024* | To set the number of bits in the key modulus
% Generating 1024 bit RSA keys ...[OK]

In the On-line provisioning method the RSA keypair is generated under the trustpoint configuration with the *rsakeypair* command, which is the next step. Configuring the trustpoint is traditionally basically a matter of pasting the commands in the spoke router configuration. In the On-line provisioning method, the trustpoint for the certificate server that generates the certificate for authenticating the management tunnel (the SDP Registrar) will be configured automatically by the SDP template, which will paste the commands to the router. For the other provisioning methods, the trustpoint commands are included in the SITE_CERT_PROXY (Off-line provisioning method) and the SITE_IN_HOUSE_831 templates (In-House provisioning method), and are pasted in the router configuration. Under the Off-line provisioning method, the initial RSA key-pair (CERT-proxy) and the certificate server certificate (CA cert) as well as the certificate for the spoke router are pasted in the router configuration. The In-house provisioning method follows conventional methods, in which the spoke router generates its own RSA key pair and then authenticates and enrolls with the certificate server, since the router will be connected to the corporate network.

The trustpoint configuration requires that the hostname be defined, and, to prevent possible DNS issues from affecting the authentication and enrollment processes, the IP address is mapped to the hostname of the certificate server on the router for the enrollment URL.

hostname <site-username-vpn>

crypto ca trustpoint <site-building-access-cert1> | site CERT1 server for management hub
enrollment url http:// <site-building-access-cert1>:80 | CERT1 | site CERT1 server for management hub
serial-number
revocation-check none
source interface Ethernet0 | The source interface is not specified until after the initial certificate enrollment. Only used for re-enrollment.
auto-enroll 70
!
The certificates to authenticate the data tunnels are generated by the regional management hub CERT2 server. Under the In-house provisioning method, the trustpoint commands and the CA certificate for the CERT2 server are pasted into the spoke router configurations, via the SDP template. Similarly, under the Off-line provisioning method, the trustpoint commands and the CA certificate for the CERT2 server are pasted into the spoke router configurations, via CERT_PROXY template. For the In-house provisioning method, only the trustpoint commands are pasted in the router, via the SITE_IN_HOUSE_831 template. For the In-house method, the

command to authenticate the spoke router is then pasted into the configuration. Under all three provisioning methods, the commands will be pasted in the spoke router via the respective template to enroll it in the certificate server and obtain its device certificate via the management VPN tunnel.

crypto ca trustpoint <site-building-access-cert2>:
enrollment mode ra
enrollment url http:// <site-building-access-cert2>:80
serial-number
revocation-check none
source interface Ethernet0
auto-enroll 70
!

The following command authenticates the spoke router in the CERT2 server for the In-house provisioning method.

Crypto ca authenticate < site-building-access-cert2> | site CERT2 server for management hub; for example, sjck-access-cert2

Upon successful enrollment the device and CA certificate generated by each certificate server will be viewable in the router configuration. However, to simplify the configuration for troubleshooting purposes, you can view just certificate numbers if the “show run brief” command is executed in the enable mode. For routers configured via the On-line method, certificates will be generated by the respective Data hub SDP Registrar.

crypto ca certificate chain < site-building-access-cert1>
certificate XX | only the certificate number is shown in HEX (this is unique for each spoke router enrolled in the same CERT1 or SDP Registrar certificate server)
certificate ca XX | only the CA certificate number shown in HEX (this is common for each spoke router enrolled in the same CERT1 or SDP Registrar certificate server)
crypto ca certificate chain < site-building-access-cert2>
certificate XX | the certificate number is shown in HEX (this is unique for each spoke router enrolled in the same CERT2 server)
certificate ca 01 | the CA certificate number shown in HEX (this is common for each spoke router enrolled in the same CERT2 server)

3.2.2.2.2 PKI Configuration of the Data GW

The Data GWs at a Data Hub are enrolled in the respective Management Hub CERT2 certificate server. Once the Data GW has network connectivity it can be enrolled in the CERT2 server first by:

1. generating the RSA key pair
2. configuring the CERT2 server as a trustpoint on the Data GW
3. authenticating the Data GW with the CERT2 server to obtain the CA certificate

4. enrolling the Data GW with the CERT2 server to obtain its device certificate

hostname <site-building-access-sdg#> | Data GW # for a respective data hub
!
aaa new-model
!
!
aaa authorization network pkiaaa group radius | authorization list pkiaaa
radius-server host <IP-address-ACS-server> auth-port 1645 acct-port 1646 key | IP address of ACS servers

crypto ca trustpoint <site-building-access-cert2> | hostname of CERT2 server at respective Management Hub
enrollment url http:// <site-building-access-cert2>:80 | hostname of CERT2 server at respective Management Hub
serial-number
crl optional
auto-enroll 70
authorization list pkiaaa | the list pkiaaa forces authorization of spoke routers that present root and device certificates issued by the certificate server CERT2.
!
crypto ca certificate chain <site-building-access-cert2> | hostname of CERT2 server at respective Management Hub: for example, sjck-access-cert2
certificate XXXX | the certificate number is shown in HEX (this is unique for each spoke router enrolled in the same CERT2 server)
certificate ca 01 | the CA certificate number shown in HEX (this is common for each spoke router enrolled in the same CERT2 server)
!
radius-server host <IP-address-EMAN-ACS-server> auth-port 1645 acct-port 1646 key | ACS servers will authenticate the spoke router authorizing the negotiation of the IPSec tunnel. The Data GW checks the certificate offered by the spoke router against the configured AAA server. If the device does not have an account on the AAA server that is a member of the group Cisco Virtual Office, then the certificate will be rejected. On the ACS server, the group Cisco Virtual Office has the reply attribute pki:cert-application=all in the AAA server group profile.

3.2.2.2.3 Configuration of the AAA Server Cisco Virtual Office Group Profile

check_items= {
6=5
}
reply_attributes= {
9,1="pki:cert-application=all"
6=5
}

3.2.2.2.4 PKI Configuration of the Management GW

hostname <site-building-access-smg1> | Management GW for Management
aaa new-model
aaa authorization network pkiaaa group radius
!
crypto ca trustpoint <site-building-access-cert1> | CERT1 server for management hub *enrollment mode ra*
enrollment url http:// <site-building-access-cert1>:80 | CERT1 server for management hub
crl optional
authorization list pkiaaa | the list pkiaaa forces authorization of spoke routers that present root and device certificates issued by the CERT1 server for management hub
!
crypto ca trustpoint <site-building-access-reg1> | SDP Registrar for a Data GW Hub
enrollment url http:// <site-building-access-reg1>:8000 | enrollment is over TCP port 8000
crl optional

serial-number none
auto-enroll 70
authorization list pkiaaa
authorization username subjectname commonname

!
crypto ca certificate chain <site-building-access-cert1> | CERT1 server for management hub
certificate XXXX | the certificate number is shown in HEX (this number is unique for each spoke router enrolled in the same CERT1 server)
certificate ca XXXX | the CA certificate number shown in HEX (this is common for each spoke router enrolled in the same CERT1 server)
crypto ca certificate chain <site-building-access-reg1>
certificate XXXX | the CA certificate number shown in HEX (this is common for each spoke router enrolled in the same SDP Registrar server)
certificate ca XXXX | the CA certificate number shown in HEX (this is common for each spoke router enrolled in the same SDP Registrar server)

radius-server host <IP-address-ACS-server> auth-port 1645 acct-port 1646 key | ACS servers will authenticate the spoke router authorizing the negotiation of the IPSec tunnel. The Data GW checks the certificate offered by the spoke router against the configured AAA server (in Cisco Virtual Office these are the local director addresses for the ACS servers). If the device does not have an account on the AAA server that is a member of the group Cisco Virtual Office, then

the certificate will be rejected. On the ACS server, the group Cisco Virtual Office has the reply attribute pki:cert-application=all in the AAA server group profile.

3.2.2.2.5 PKI Configuration of the Certificate Server

Before configuring the certificate server function on the Cisco IOS Software–based certificate server, there must be network connectivity between the certificate server and the storage location for the certificates. In Cisco Virtual Office, we use the Management Hub ISC tftpboot/<IP-address-cer#> directory and make sure that the certificate server has write access to this directory. Without write access the certificate server will not be able to start and maintain operations.

hostname <site-building-access-cert#> | CERT# server for management hub!
crypto pki server <site-building-access-cert#> | PKI Server configuration for certificate server
database level complete | specifies that each certificate includes the most complete information available so that the new certificates can be issued without conflict, the serial number and subject name of each certificate are stored in the certificate, and each certificate is written to a database
database url tftp://<IP-address-ISC>/<site-building-access-cert#> | Directory location where the certificates are saved via TFTP
grant auto | automatically grants certificate upon initial and renewal requests
mode sub-cs | The stand-alone certificate servers (not including the SDP registrars) are operated as sub-CS (subordinate Certificate Server) mode except the SJ Certificate servers, which are the root certificate servers for each respective group of servers.

When the *no shut* command is issued on the crypto pki server SDPserver, the pki server will try to write its CA certificate to the database URL. Failure to write this data will cause the PKI server startup to fail and to shut down. The following commands will appear in the router configuration after the command; no shut is issued under the pki server SDPserver when the pki server is successfully started.

crypto pki trustpoint <site-building-access-cert#> |The PKI server reasserts itself as the certificate server
revocation-check crl | though configured not actively being used for now
rsakeypair <site-building-access-cert#> | automatically enrolls the Cisco IOS Software–based certificate server in the certificate server configured on the same device

crypto pki trustpoint SDPhttps | SDPhttps is the label for a trustpoint, which obtains a device certificate from the PKI server SDPserver
enrollment url http:// <site-building-access-cert#>:80 | Specifies the URL of the certificate authority on which your router should send certificate requests
serial-number none | do not use the serial number in the certificate
fqdn none | do not use the fully qualified domain name in the certificate request

ip-address none | do not use the IP address in the certificate request
subject-name CN=<site-building-access-cert#.cisco.com>| Specifies the requested subject name that will be used in the certificate request. If the *x-500-name* argument is not specified, the FQDN, which is the default subject name, will be used. In the Cisco Virtual Office certificate servers this is the certificate server hostname, such as sjck-access-cert1.

crypto pki certificate chain <site-building-access-cert#>
certificate ca XX | | the certificate server will authenticate with itself and maintain the CA certificate
certificate XX | this is the device certificate issued by the certificate server
crypto pki certificate chain SDPhttps
certificateXX | this is the device certificate issued by the SDP Registrar
certificate ca XX | this is the same CA certificate as listed under the chain SDPserver

3.2.2.2.6 PKI Configuration of the SDP Registrar PKI Server

Because of the naming convention used for the PKI server configured on the SDP Registrar, each Data GW Hub is consistently named SDPserver.

crypto pki server SDPserver | specifies the name of the PKI server and contains its configuration information
database level complete | specifies that each certificate includes the most complete information available so that the new certificates can be issued without conflict, the serial number and subject name of each certificate are stored in the certificate, and each certificate is written to a database
database url tftp://<DNS-name-ISC>/<site-building-access-reg1> | Directory location where the certificates are saved via TFTP
grant auto | automatically grants certificate upon initial and renewal requests
shut |

When the *no shut* command is issued on the crypto pki server SDPserver, the pki server will try to write its CA certificate to the database URL. Failure to write this data will cause the PKI server startup to fail and to shut down. The following commands will appear in the router configuration after the command no shut is issued under the pki server SDPserver when the pki server is successfully started.
crypto pki trustpoint SDPserver | the trustpoint specifies info related to the certificate server that the router will enroll – in this case the SDP Registrar is enrolling with itself
revocation-check crl | A CRL does not exist and this command is ignored
rsakeypair SDPserver | Auto-enrolls the trustpoint in the certificate server
!
crypto pki trustpoint SDPhttp | SDPhtp is the label for a trustpoint, which obtains a device certificate from the PKI server SDPserver
enrollment url http:// <site-building-access-reg1>:<tcp-port-number> | Specifies the URL of the certificate authority on which your router should send certificate requests

serial-number none | do not use the serial number in the certificate
fqdn none | do not use the fully qualified domain name in the certificate request
ip-address none | do not use the IP address in the certificate request
subject-name CN=<site-building-access-reg1>.cisco.com |
revocation-check crl | | a CRL does not exist and this command is ignored
!
crypto pki certificate chain SDPserver
certificate ca XX | | this is the same CA certificate as listed under the chain SDPhttp
crypto pki certificate chain SDPhttp
certificateXX | this is the device certificate issued to this SDP Registrar by itself
certificate ca XX | this is the same CA certificate as listed under the chain SDPserver

3.2.3 Underlying Security Features

While security is stressed throughout the Cisco Virtual Office solution, the next section reviews security related that are not covered in other sections:

- Content-Based Access Control (CBAC) Stateful Firewall
- Privilege Level: Providing User Access to Enable Mode Troubleshooting Commands

3.2.3.1 Content-Based Access Control (CBAC) Stateful Firewall

CBAC is deployed on all of the Cisco Virtual Office spoke routers in a consistent manner via the ISC FW SR. Because CBAC is deployed by an SR, its configuration will be monitored and maintained by ISC.

CBAC Configuration on Cisco Virtual Office Spoke Router

ip inspect name ISC_inside_1 tcp
ip inspect name ISC_inside_1 rtsp
ip inspect name ISC_inside_1 smtp
ip inspect name ISC_inside_1 h323
ip inspect name ISC_inside_1 realaudio
ip inspect name ISC_inside_1 tftp
ip inspect name ISC_inside_1 skinny
ip inspect name ISC_inside_1 ftp
ip inspect name ISC_inside_1 udp
ip inspect name ISC_inside_1 netshow
ip inspect name ISC_inside_1 sip

interface Ethernet0
ip inspect ISC_inside_1 in

3.2.3.2 Privilege Level: Providing User Access to Enable Mode Troubleshooting Commands

Users will be provided exec level access to their router with the admin account and a static password configured on each router, and accessible via telnet from devices connected to the

Ethernet 0 interface or console. In order to provide users access to common troubleshooting commands on their spoke routers without divulging the enable password, the Privilege Level command has been implemented. The actual large number of commands made available is based upon experience from the Cisco Virtual Office pilot but may be supplemented as required.

Privilege Level Configuration on Spoke Routers

privilege exec level 1 clock set
privilege exec level 1 clock
privilege exec level 1 undebug crypto ipsec
privilege exec level 1 undebug crypto isakmp
privilege exec level 1 undebug crypto
privilege exec level 1 undebug pppoe data
privilege exec level 1 undebug pppoe packets
privilege exec level 1 undebug pppoe events
privilege exec level 1 undebug pppoe elog
privilege exec level 1 undebug pppoe errors
privilege exec level 1 undebug pppoe
privilege exec level 1 undebug ip dhcp server class
privilege exec level 1 undebug ip dhcp server linkage
privilege exec level 1 undebug ip dhcp server events
privilege exec level 1 undebug ip dhcp server
privilege exec level 1 undebug ip dhcp
privilege exec level 1 undebug ip routing
privilege exec level 1 undebug ip packet
privilege exec level 1 undebug ip
privilege exec level 1 undebug all
privilege exec level 1 undebug
privilege exec level 1 terminal monitor
privilege exec level 1 terminal no monitor
privilege exec level 1 terminal no
privilege exec level 1 terminal
privilege exec level 1 show crypto isakmp sa
privilege exec level 1 show crypto isakmp
privilege exec level 1 show crypto ipsec sa
privilege exec level 1 show crypto ipsec
privilege exec level 1 show crypto engine brief
privilege exec level 1 show crypto engine accelerator statistic
privilege exec level 1 show crypto engine accelerator
privilege exec level 1 show crypto engine connections
privilege exec level 1 show crypto engine
privilege exec level 1 show crypto
privilege exec level 1 show ip dhcp server
privilege exec level 1 show ip dhcp
privilege exec level 1 show ip
privilege exec level 1 show
privilege exec level 1 no debug crypto ipsec

privilege exec level 1 no debug crypto isakmp
privilege exec level 1 no debug crypto
privilege exec level 1 no debug pppoe data
privilege exec level 1 no debug pppoe packets
privilege exec level 1 no debug pppoe events
privilege exec level 1 no debug pppoe elog
privilege exec level 1 no debug pppoe errors
privilege exec level 1 no debug pppoe
privilege exec level 1 no debug ip dhcp server class
privilege exec level 1 no debug ip dhcp server linkage
privilege exec level 1 no debug ip dhcp server events
privilege exec level 1 no debug ip dhcp server
privilege exec level 1 no debug ip dhcp
privilege exec level 1 no debug ip routing
privilege exec level 1 no debug ip packet
privilege exec level 1 no debug ip
privilege exec level 1 no debug all
privilege exec level 1 no debug
privilege exec level 1 no
privilege exec level 1 debug crypto ipsec
privilege exec level 1 debug crypto isakmp
privilege exec level 1 debug crypto
privilege exec level 1 debug pppoe data
privilege exec level 1 debug pppoe packets
privilege exec level 1 debug pppoe events
privilege exec level 1 debug pppoe elog
privilege exec level 1 debug pppoe errors
privilege exec level 1 debug pppoe
privilege exec level 1 debug ip dhcp server class
privilege exec level 1 debug ip dhcp server linkage
privilege exec level 1 debug ip dhcp server events
privilege exec level 1 debug ip dhcp server
privilege exec level 1 debug ip dhcp
privilege exec level 1 debug ip routing
privilege exec level 1 debug ip packet detail
privilege exec level 1 debug ip packet
privilege exec level 1 debug ip
privilege exec level 1 debug all
privilege exec level 1 debug
privilege exec level 1 clear crypto isakmp
privilege exec level 1 clear crypto
*privilege exec level 1 clear ip auth-proxy cache **
privilege exec level 1 clear ip auth-proxy cache
privilege exec level 1 clear ip auth-proxy
privilege exec level 1 clear ip dhcp binding
privilege exec level 1 clear ip dhcp server
privilege exec level 1 clear ip dhcp
privilege exec level 1 clear ip

privilege exec level 1 clear interface
privilege exec level 1 clear counters
privilege exec level 1 clear
privilege exec level 1 ping
privilege exec level 1 traceroute

3.3 Management

- Separate management VPN tunnel
- Cisco CNS 2100 Series Intelligence Engine–based CNS transport mechanisms
- CSM fully managed service

3.3.1 Separate Management IPSec Tunnel

Cisco Virtual Office spoke routers will maintain a management tunnel that provides the connectivity to enable
CNS connectivity, which is used to push new spoke router configurations, monitoring spoke routers, and activate policy changes. Spoke routers are configured so that the devices on the Management subnet in a security domain can only be reached from the spoke router Ethernet 0 interface, preventing access for any other devices on the spoke router private subnet. Since the users' data connectivity is over separate IPSec tunnels, changes to the policies can be performed on the spoke router, minimizing the risk of losing connectivity for the end user.

3.3.2 Cisco CNS 2100 Series Intelligence Engine–Based CNS Transport Mechanism

In order to take advantage of the control offered by the CNS technology, Cisco Virtual Office utilizes the CNS server on the Cisco CNS 2100 Series Intelligence Engine and the following CNS agents and related services on the spoke routers:

- CNS event agent
- CNS exec agent
- CNS partial config agent
- CNS image agent and service

In addition, CNS allows you to set a trusted server for a single CNS agent or all CNS agents. An attempt to connect to a server not on the list will result in an error message being displayed. An error will be generated when the CNS exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address.

CNS Trusted Server Command Implemented on a Spoke Router

cns trusted-server all-agents <URL> |

The CNS agent configuration commands for the Cisco Virtual Office spoke routers are included in the initial configlets applied to the routers. Once the management tunnel is established, then CNS connectivity should immediately follow.

3.3.2.1 CNS Event Agent

The CNS Event Agent must be enabled before any of the other CNS agents are configured because the CNS event agent provides a transport connection to the CNS Event Bus for all other CNS agents. The other CNS agents use the connection to the CNS Event Bus to send and receive messages. The CNS event agent does not read or modify the messages.

The Cisco CNS 2100 Series Intelligence Engine at each management hub exchanges CNS messages with every spoke and forwards these messages over the TIBCO bus to all listeners, specifically the ISC server at the hub. In addition, the Cisco CNS 2100 Series Intelligence Engine will generate and send two messages to the ISC server on behalf of the spoke routers:

- Connect: sent when a spoke router first establishes a CNS connection with the Cisco CNS 2100 Series Intelligence Engine
- Disconnect: sent when the CNS agent on the spoke is not reachable

All other CNS messages are initiated by the CNS agent on the spoke or the CNS server on the ISC.

The CNS Event Agent Activation Command on a Spoke Router
cns event <Regional-IE2100-hostname> 11011 source <spoke-router-interface-E0-IP-address> keepalive 180 3 | 11011 is the TCP port to send CNS event information to the CNS engine; keepalive is 180 seconds; retry count is 3

The generation of too many CNS event logging messages can negatively affect the publishing time of standard CNS event messages. In order to reduce the number of CNS Event logging messages on spoke routers, the CNS Event Agent is configured not to send out these messages with the command
no logging cns-events.

3.3.2.2 CNS Exec Agent

The CNS Exec Agent allows a remote application to execute an EXEC mode CLI command on a Cisco IOS Software device by sending an event message containing the command. A restricted set of EXEC CLI commands, including the Show commands, are supported.

The CNS Exec Agent Activation Command on a Spoke Router
cns exec 80 source <spoke-router-interface-E0-IP-address> | over port 80

3.3.2.3 CNS Partial Config Agent

As the name implies, the CNS Partial Config Agent is used to push or pull partial configuration commands to or from a spoke router. You must enable the CNS Event Agent before configuring the CNS Partial Config Agent. The CNS Event Agent sends an event with the subject "cisco.mgmt.cns.config.load" to specify whether configuration data can be pushed to the CNS Partial Configuration Agent or pulled from a configuration server by the CNS Partial Configuration Agent:

- Push model - the event message delivers the configuration data to the Partial Configuration Agent
- Pull model - the event message triggers the Partial Configuration Agent to pull the configuration data from the CNS Configuration Engine

The cns trusted-server command specifies which CNS configuration engine(s) can be used by the CNS Partial Configuration Agent. By default, NVRAM will be updated except when the

no-persist keyword is configured. One of the following messages will be published on the CNS Event Bus after the partial configuration is complete:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the partial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the partial configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure—CNS configuration agent encountered an error and was not able to apply the configuration.

The CNS Partial Configuration Agent Activation Command on Spoke Routers
cns config partial <Regional-IE2100-hostname> 80 source <spoke-router-interface-E0-IP-address>

3.3.2.4 CNS Image Agent and Service

The CNS Image Service is an automated, scalable, and secure mechanism designed to distribute Cisco IOS Software images and related software updates to Cisco IOS Software devices that have Cisco Intelligence Agents.[4]

In general, the image management engine of the Cisco CNS 2100 Series Intelligence Engine enables:

- All spoke routers to be associated with one or more images
- All spoke routers to be associated with one or more groups
- Inventory control of spoke routers before upgrade deployment
- Simulated image upgrades before the actual deployment
- The option(s) whether new image(s) can/should overwrite the existing ones, or if the flash contents should be deleted and then a new image installed
- The distribution (copy) and/or the activation of images
- The scheduling of image upgrades to performed immediately, or in the future
- Support of the "concurrency factor," which allows system administrators to stop/postpone the upgrade of a group or domain, if **"x"** devices cannot be upgraded, or if the upgrade has failed

The Image Management Engine interacts with the Image Management Agent, which runs on every CPE. The basic functions of the image agent are:

cisco.mgmt.cns.image.* – Events related to the image distribution agent
cisco.mgmt.cns.image.checkServer
cisco.mgmt.cns.image.inventoryRequest
cisco.mgmt.cns.image.upgradeRequest
cisco.mgmt.cns.image.status

The minimum set of commands necessary to facilitate the engine-agent functionality are as follows:
cns trusted-server all-agents <URL>
cns image server http://<URL>

The **cns image server** command uses the URL to contact the image management server and starts the CNS Image Agent process to listen for image-related events on the CNS Event Bus. For Cisco Virtual Office to make sure that the image management will utilize the existing secure management tunnel and Cisco IOS Software FTP-based transport, two more commands are required:
ip http client source-interface Ethernet0
ip ftp source-interface Ethernet0

3.3.3 ISC Fully Managed Service and Management Platform Integration

The Fully Managed Service (FMS) of ISC will be implemented in Cisco Virtual Office to provide control over spoke routers. A new spoke router will be assigned to the group of "managed" devices that are controlled and monitored, when the device is initially created in ISC. A check box in ISC indicates if the FMS is active for a spoke. If the support engineer needs to perform certain configuration/policy changes, that engineer needs to uncheck the box and lock it after the configuration change is done. If these changes are scheduled and performed from ISC, for example, via the deployment of an FW SR, then FMS will accept and register the change. However, if the change is originated from a non-ISC source, FMS triggers a set of functions to audit the spoke router configuration and notifies the supporting teams about the configuration/policy change, security violation, connect/disconnect events, etc. FMS allows this functionality to be customized, invoking an external script to perform additional functions, if certain conditions are met.

FMS has the following CNS inputs:

- CNS messages provided by CNS agents
- Connect and Disconnect messages provided by the CNS engine

FMS operates on the premise that the ISC CNS Server is constantly listening to Tibco events generated by completion of the enforcement audits. One audit completion Tibco event will be sent for each SR assigned to the device. For both Config-change and Connect events the following actions will be taken by the CNS Server:

- Upon receipt of successful enforcement audit events, the CNS Server will log this information and take no further action.

- Upon receipt of a failed enforcement audit event, the CNS Server will take the following actions:

(a) Send an e-mail to the list of e-mail recipients subscribed in the vpnsc.properties file announcing the failed enforcement audit. The e-mail will include device name, SR, timestamp, etc. For Cisco Virtual Office, the recipient will be the support organization responsible for the hub and spoke routers.

(b) Call an external script, which can be defined in vpnsc.properties, to take further action, such as disconnect the services of the faulty user. The script can be configured with arguments such as the IP address of the device in question.

For Cisco Virtual Office the action taken by the corporate management platform and FMS is shown in the four scenarios listed below and in Figure 5:

- Disconnect
- Connect
- Config-change
- Automatic/manual disconnect

Disconnect

The intention of the Disconnect scenario is to make sure that when the CNS engine sends a Disconnect event, there is no ill intent, and all Security Associations (SAs) between the spoke router and the management and data GWs are terminated.

Connect

The objective of the connect scenario is to make sure that the spoke router configuration is identical with the configuration in the ISC repository. The corporate management platform will not react if the ISP part of the configuration has changed. If the configuration has changed, then those changes will be reversed or set to the current configuration per the latest SRs.

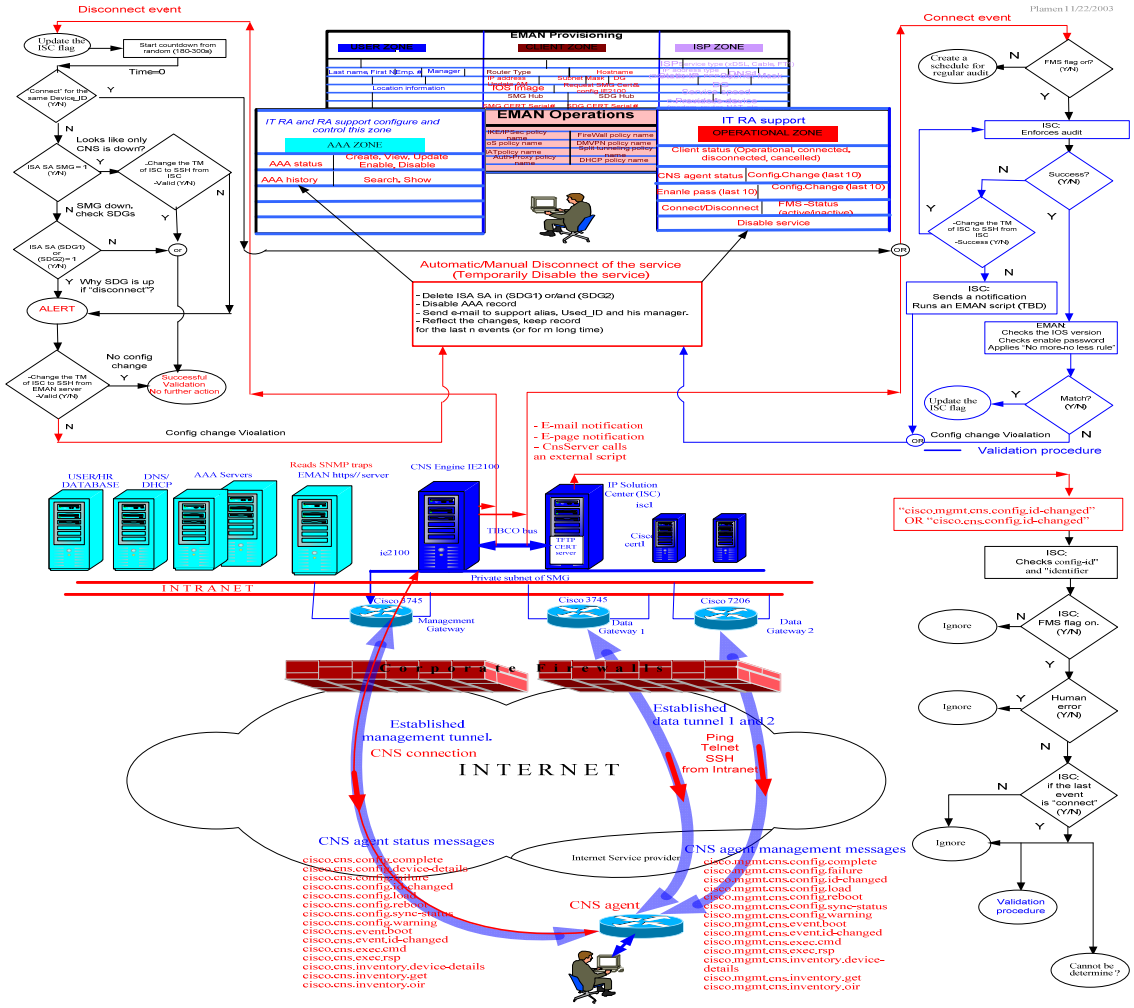
Config-change

The objective of a Config-change scenario is to make sure that the change in the spoke configuration is not based on a non-ISC source.

Automatic/Manual Disconnect

The objective of automatic/manual disable service scenario is to use PKI+AAA integration and shut down the service in a matter of seconds, if required, such as when there is no doubt about intrusion or when an employee is terminated. In this case the AAA record for the spoke router would be deleted or disabled, and the SAs would be terminated.

Figure 5 Fully Managed Service and Proposed Corporate Management Platform Integration



3.4 Provisioning

Provisioning of the Cisco Virtual Office service is presented as follows:

- User subscription and automated configuration generation
- Spoke router provisioning scenarios
- Automated policy deployment and audit

3.4.1 User Subscription and Automated Configuration Generation

- User subscription
- IP Solution Center integration
- Spoke router configuration in ISC

3.4.1.1 User Subscription

After a user completes the IT User Request Form, the request is routed to the user's manager for approval, and then the user is notified of the manager's decision. To complete the User Request Form, the user must provide information about Internet connectivity, including how the IP address is assigned to the Ethernet 1 interface, ISP, upstream and downstream bandwidth, home address, and telephone number associated with the Internet service.

3.4.1.2 ISC Integration

Upon manager approval, the IT management platform will provision a Cisco 831 Ethernet Broadband Router for the user to establish VPN data connectivity with the closest Cisco Virtual Office data GW hub. The hostname for the router will be site_code-username-vpn. The IT management platform will configure and populate a /28 subnet in Address Management for the router and subnet addresses, as well as create an account on the regional ACS (fixed AAA) servers that will authenticate the spoke routers using PKI-AAA integration. Using available APIs, the IT management platform will also create or define spoke router configuration in ISC.

3.4.1.3 Spoke Router Configuration in ISC

ISC maintains the concepts of Service Requests (SRs) and Templates, as well as data related to IP connectivity to deploy and manage devices. Next is an overview of what data is stored and how it is provisioned from ISC per the following:

- Repository information
- Templates, data files, and configlets
- Service requests

3.4.1.3.1 Repository Information

ISC maintains the following information for each spoke router in its repository:

- Device
- CPE

- Customer Site

3.4.1.3.1.1 Device

In ISC, the Device is a physical entity. It contains the information for the hub and spoke routers used to populate the Data File. Below is information found in the Device with the Cisco Virtual Office specific information in parentheses:

- Hostname
- Domain name
- Description
- Management IP Address (on a Cisco 831 Ethernet Broadband Router spoke router this is the IP address associated with interface Ethernet 0)
- Groups that the router is associated with
- Login username and password
- Enable password
- Terminal session protocol (CNS)
- SNMP strings
- Fully managed switch (enabled by default for spoke routers)
- CNS Device Event notification (hostname)
- Cisco CNS 2100 Series Intelligence Engine associated with the spoke router (determined by site of management hub)
- CNS Device Transport (HTTP)
- Hardware platform (Cisco 831 Ethernet Broadband Router for the spoke routers)
- Image version

3.4.1.3.1.2 CPE

In ISC the CPE is a logical entity. Within the CPE, the interface definitions for the spoke router are specified. For example, the Cisco 831 Ethernet Broadband Router has Ethernet 0 (inside) and Ethernet 1 (outside) interfaces. In the CPE, the role of each interface in the SR for the spoke routers (IPSec, FW, NAT, and QoS) is specified.

3.4.1.3.1.3 Customer Site

In ISC the Customer Site, the customer (Cisco IT), and the CPE are specified. ISC requires this information in order to create an FW SR.

3.4.1.3.2 ISC Templates, Data Files, and Configlets

Templates are a combination of Cisco IOS Software CLI commands and a variation of commands from Velocity, a template language that is part of the Apache open source package. A template can be applied to a CPE, a site (location), a customer (Cisco IT), or a group of devices: for example, “San Jose 831 routers.” Router templates will be maintained by IT RA

engineers. ISC instantiates the appropriate template with variables stored in the Data File associated with a spoke router to create a Configlet. Templates, Data Files, and Configlets can be manipulated to enable three basic initial deployment scenarios, On-line, Off-line, and In-house, which are covered in the Deployment Scenarios section.

3.4.1.3.3 Service Requests

Service Requests (SRs) represent a feature of the ISC to implement, modify, or eliminate policies on the spoke routers. SRs can be implemented for the following policies: IPSec, Stateful FW, QoS, and NAT.

SRs are created in ISC by populating the ISC SR editor. Each SR type, such as an IPSec SR, has a different menu with variables that must be populated to create the SR. Variables will differ based upon the location of the Data GWs, the address subnet assigned to a user, and the bandwidth made available to a user from the ISP. At this time, all SRs are applied to the public interface on the Cisco 831 Ethernet Broadband Router (usually interface Ethernet 1 except for spoke routers configured as PPPoE clients), except QoS, which must be applied to the physical Ethernet 1 interface. The private interface for all SRs is always Ethernet 0.

The IT management platform will assign spoke routers to SRs in ISC after the user has been approved for the Cisco Virtual Office service. The SR will be in a “wait-to-deploy” state until the ISC receives a CNS Connect event.

Configuring commands on a spoke router via an SR is always preferred to a Template, because upon deployment of an SR, ISC will then perform a “Collect Config” of the spoke router and audit it via the CNS mechanism to verify that the SR was successfully deployed. Periodic audits of SRs may also be implemented, and if it is found that commands related to the SR have been modified, then the router configuration will be modified to reflect the configuration per the latest SR if the router is under the Fully Managed Service (FMS) (see the section on End-to-End Management for more information).

In ISC, spokes are subscribed to an SR, and then the SR is deployed. ISC maintains the status of the SR with respect to each spoke. Any SR state other than “Deployed” will cause the ISC to attempt to re-deploy the service. The “Deployed” state means the SR was successfully deployed and audited on all spoke routers configured in the SR.

The following are valid SR states:

- Deployed
- Wait_to_deploy
- Failed_to_deploy
- Pending
- Invalid
- Lost

3.4.2 Spoke Router Provisioning Scenarios

Three provisioning scenarios are available for Cisco Virtual Office spoke routers:

- On-line
- Off-line
- In-house

The On-line and Off-line scenarios offer a method to eliminate the need of an IT engineer to configure the spoke router and may also be referred to as Zero Touch Deployment scenarios. In-house provisioning has been successfully implemented during the Cisco Virtual Office pilot. All three scenarios configure the spoke router so that it can establish a VPN tunnel with the appropriate Management GW.

3.4.2.1 On-line Provisioning Scenario

- User Responsibility
- SDP Configuration and Certificates Server Enrollment

3.4.2.1.1 User Responsibility

To minimize Total Cost of Ownership (TCO), the provisioning process offloads the physical configuration of the spoke router from IT RA engineers to automated processes and the end user. This new configuration paradigm is referred to as the Zero Touch Deployment (ZTD) model. The user will be responsible for ordering the router and configuring it to provide Internet connectivity to a host connected to the Ethernet 0 interface using CRWS, SDM, the CLI, or any other tool. Initially IT recommends CRWS as the configuration tool for users who are unfamiliar with Cisco IOS Software.

Essentially there are three easy Webpages: the welcome page, introduction page, and completion page. The first page requires the user to connect to the SDP Registrar at the Data GW hub, entering the following information in the address bar of a browser window:

After entering a username and one-time password (OTP) and successfully authenticating with the OTP AAA servers, the user will be greeted with a welcome message that provides brief but concise information on the steps users should take. An example of this message for the SJ SDP Registrar is shown in Figure 6. Users will then click “START” in this screen to paste the same URL for the SDP Registrar in the box as shown in Figure 7, and again successfully authenticate with the OTP. This duplication is now required due to a bug with the PKI Framework, and it is anticipated that it will be resolved in the PI5 Cisco IOS Software release of 12.3. Next the user will be presented another Welcome screen indicating that the username and password have been accepted and asking the user to press the “Next” button, as shown in Figure 8. The user will be presented the screen shown in Figure 9 that informs the user that the router is now being enrolled in the VPN network. Eventually the user will be presented with a

screen indicating that the configuration process is complete and asking the user to release and renew the IP address of the PC.

Cisco Virtual Office Device Deployment (via SDP)

Topics On This Page:

Once properly connected to your Cisco Virtual Office router via an Ethernet cable connection. You will have to setup your router to connect to the Internet.

Your Cisco Virtual Office router comes installed with the Secure Device Manager (SDM) tool to facilitate this function. You should have completed connecting your Cisco Virtual Office router to the Internet via SDM at this point.

This section will guide you through completing your Cisco Virtual Office device deployment and configuration using the SDP utility. Here are the steps you must complete to connect your Cisco Virtual Office router to the corporate network and complete your Cisco Virtual Office router's configuration for this service. This is the second of two steps in configuring your Cisco Virtual Office service.

Key Points to Remember

Your Cisco Virtual Office service will be fully configured utilizing an automated deployment model. Please follow all instructions without deviation as your service may not be properly configured otherwise.

Additionally, if you have a Firewall configured on your ISP device or on another device between the Cisco Virtual Office router and your ISP you will need to open the following ports in order for your Cisco Virtual Office service to connect, configure and function.

UDP 500, Protocol 50, UDP 4500

Note: Do not attempt to alter your Cisco Virtual Office router for this function (firewall). It will be configured, per the IT standard, for you.

Getting Connected to the SDP Utility

1. Obtain an IP from your new 831 router
2. Open your web browser and enter into your Address Bar...
3. The SDP Welcome page
4. Connect to the Registration Server
5. Security Certificate Prompt
6. Login to the Registration Server
7. Login Acceptance
8. Enrolling
9. Verify connectivity to the Internet
10. Authentication to the Corporate Network using Authentication-Proxy or 802.1x Feature

1. Obtain an IP from your new 831 router

One method to verify that your PC has obtained an IP Address from your Cisco Virtual Office router is described here.

a. From your **Start** menu, select **Run...**.
b. In the **Open**: field of the **Run** dialogue box, enter **`cmd`** and press the **OK** button.
c. In the ensuing **Command Prompt** window, enter **`ipconfig`** at the command prompt as shown below in Figure 1.

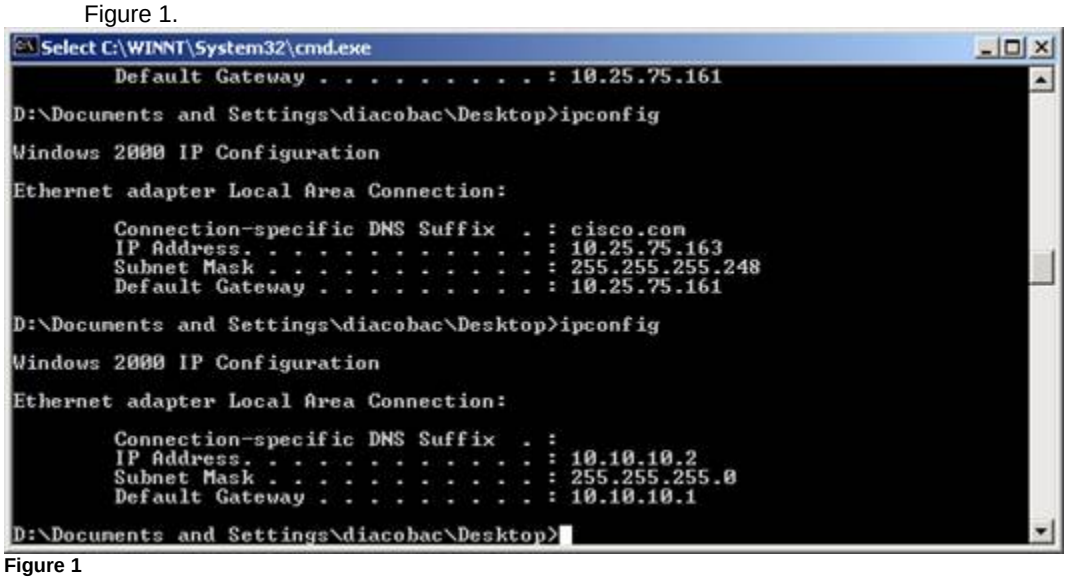


Figure 1

d. If you do not have an IP Address in this subnet you can enter the command **`ipconfig /renew`** which will cause your adapter to attempt to retrieve a new IP Address.

Note: If you just completed the Router Web Setup (SDM) tool it is recommended that you renew your IP Address before continuing.

2. Open your web browser and enter into your Address Bar the following:

https://join-hub1-vpn...com/sdp/intro

Note: In the example above we are using hub1. You will have to select the hub closest to you as provided in the table below, as applicable:

Cisco Virtual Office Hub Selection	
Hub site 1	*https://join-hub1-vpn...com*
Hub site 2	*https://join-hub2-vpn...com*

This will direct you to the hub registration server and will initiate the Secure Device Provisioning (SDP) utility for proper router deployment and configuration.

a. Accept the prompt for certificate
b. Provide your **username** and authentication **password** which will take you to the following page; Figure 2.

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

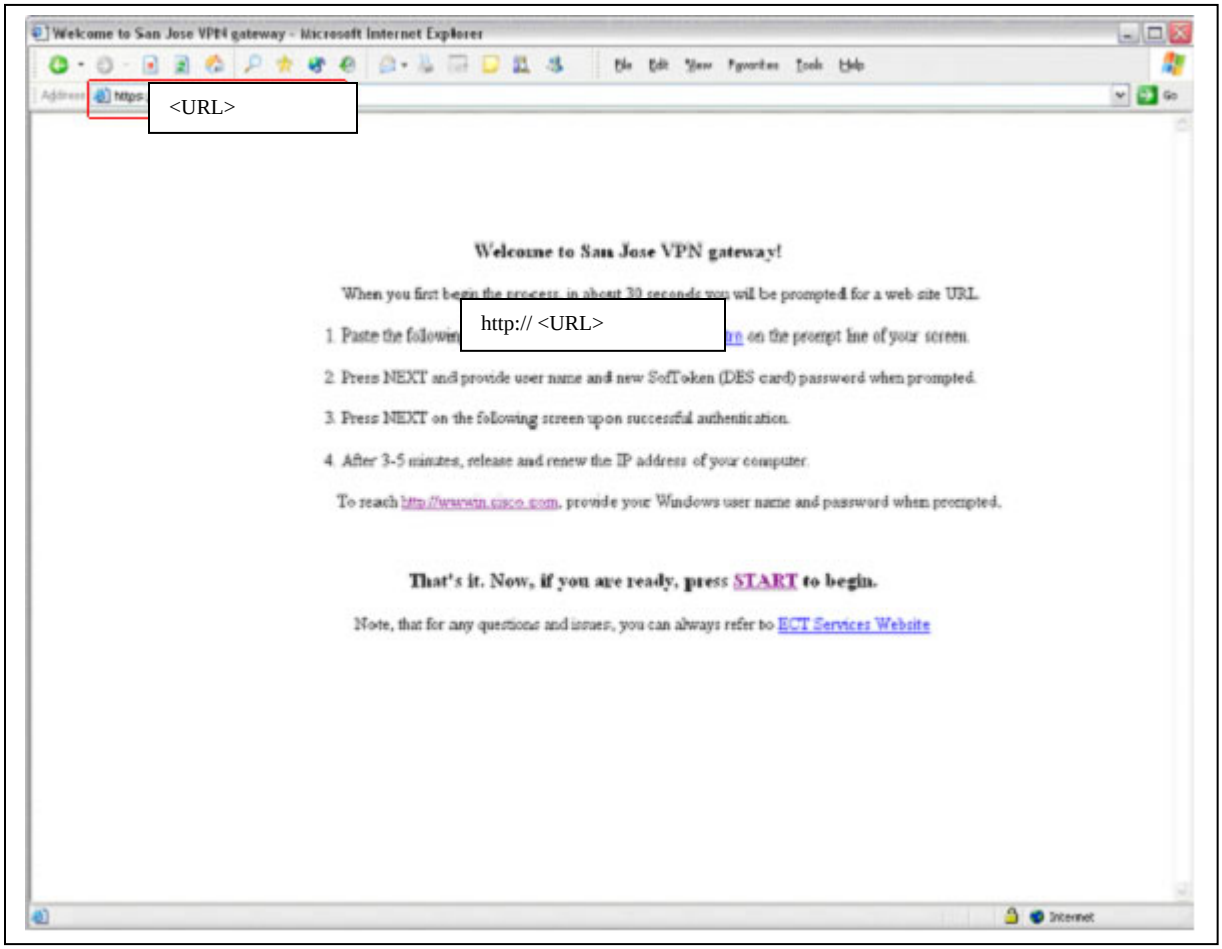


Figure 2

3. The Secure Device Provisioning (SDP) Welcome page

1. The Welcome page will display instructions for completion of the enrollment/configuration of your Cisco Virtual Office router. Once you are ready to continue select **START** to begin.
    a. The page should display the current Status, currentactivity Message, and instructions on What to do next; as shown in Figure 3.

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

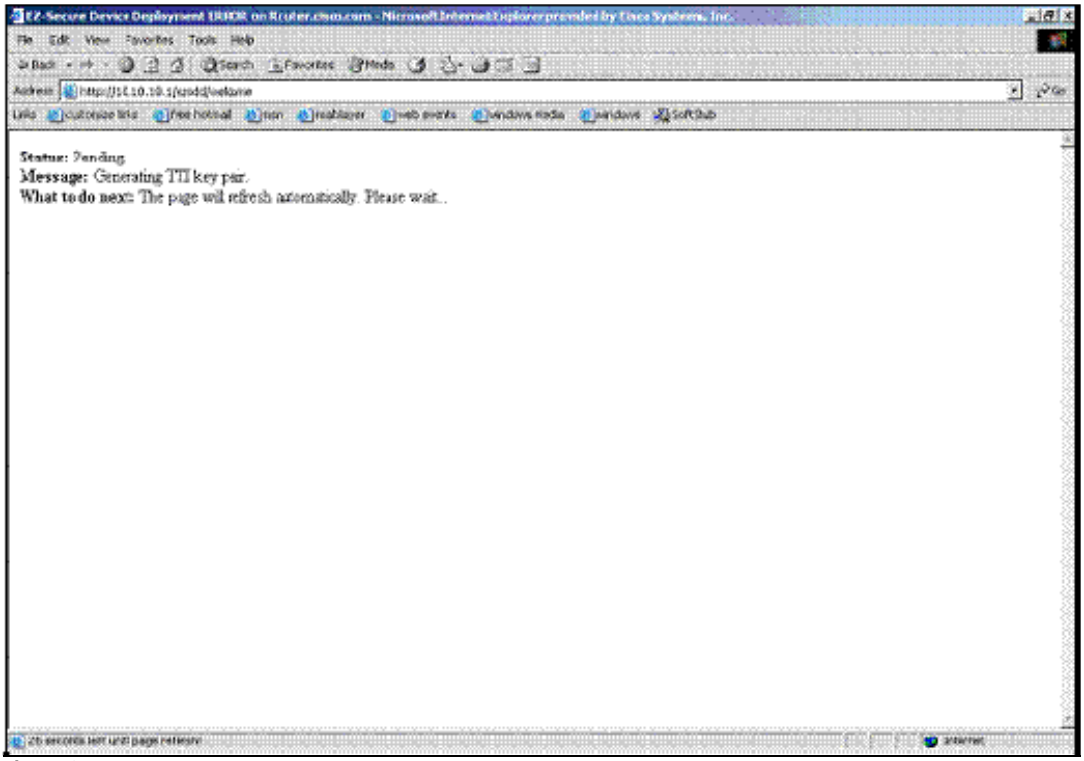


Figure 3

4. Connect to the Registration Server

When your screen refreshes it should look like Figure 4.

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

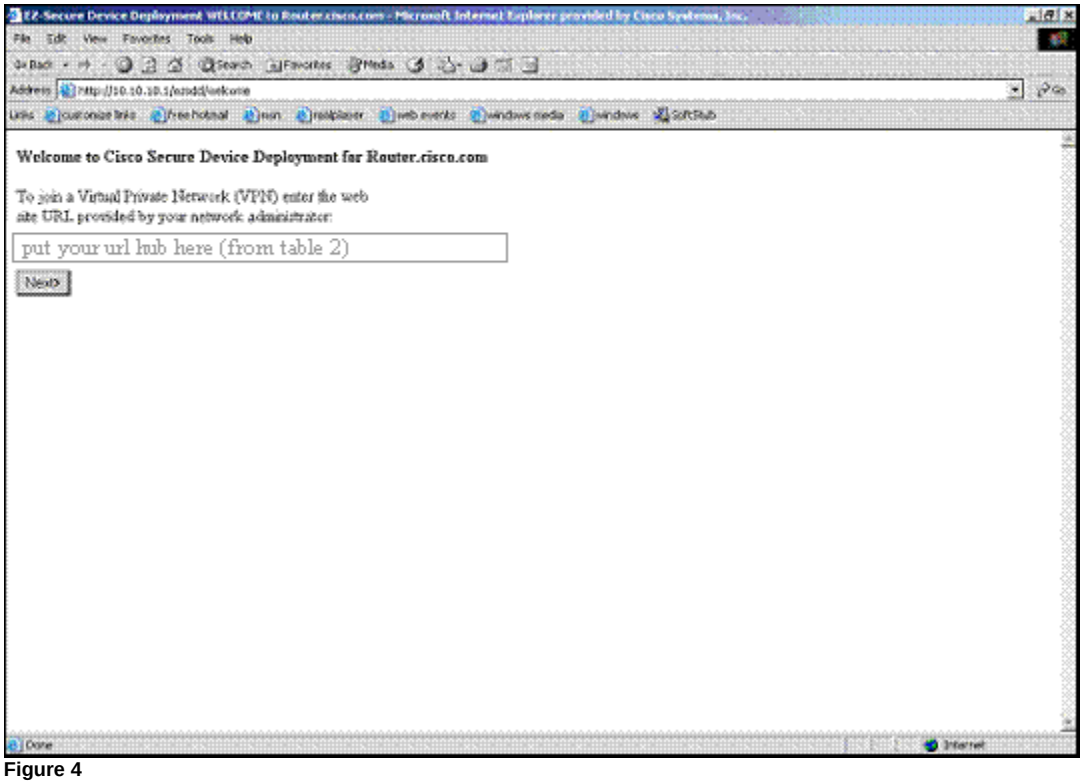


Figure 4

1. You will now need to enter the URL for your regional Registration server. In the above example, the hub location is hub1. Select your nearest hub location, as applicable, and select **Next**.

HINT: This should be the same information that auto-populated during your registration for the Cisco Virtual Office service.

5. Security Certificate Prompt

The expected response from the Registration server is a pop-up Security Alert window which indicates your Security Certificate is valid and asking you to accept to proceed; Figure 5.

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

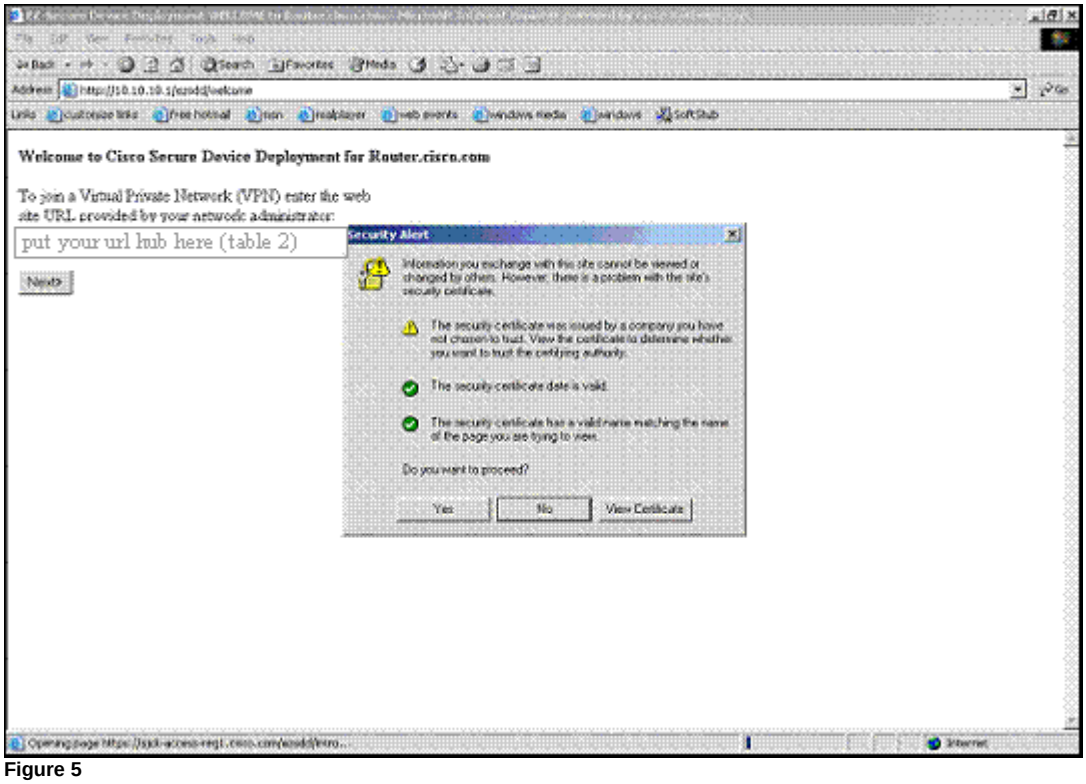


Figure 5

1. Select **Yes** at this prompt to proceed.

6. Login to the Registration Server

This will generate a prompt for you to log in; Figure 6.

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

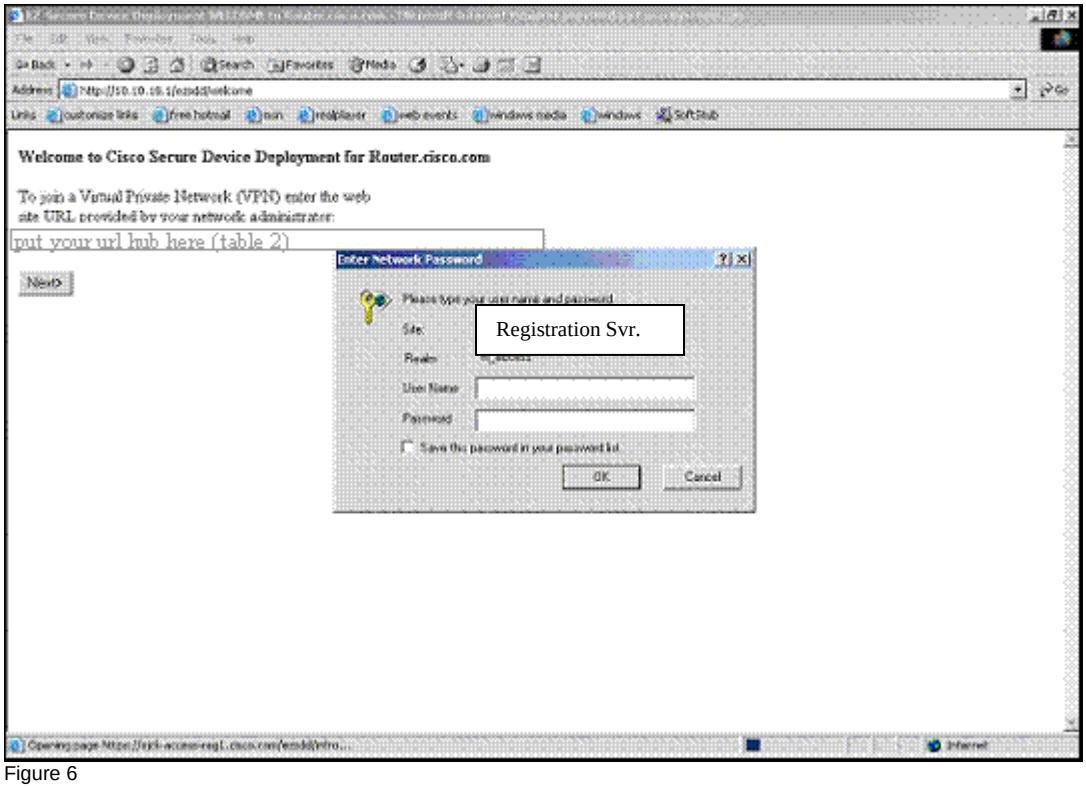


Figure 6

This is similar to your standard VPN login where you will enter your **username** (userid) and authentication **password**. Enter that information and select **OK** to continue.

7. Login Acceptance

Once your userid and password have been accepted your screen will display the results of your login attempt; Figure 7.

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

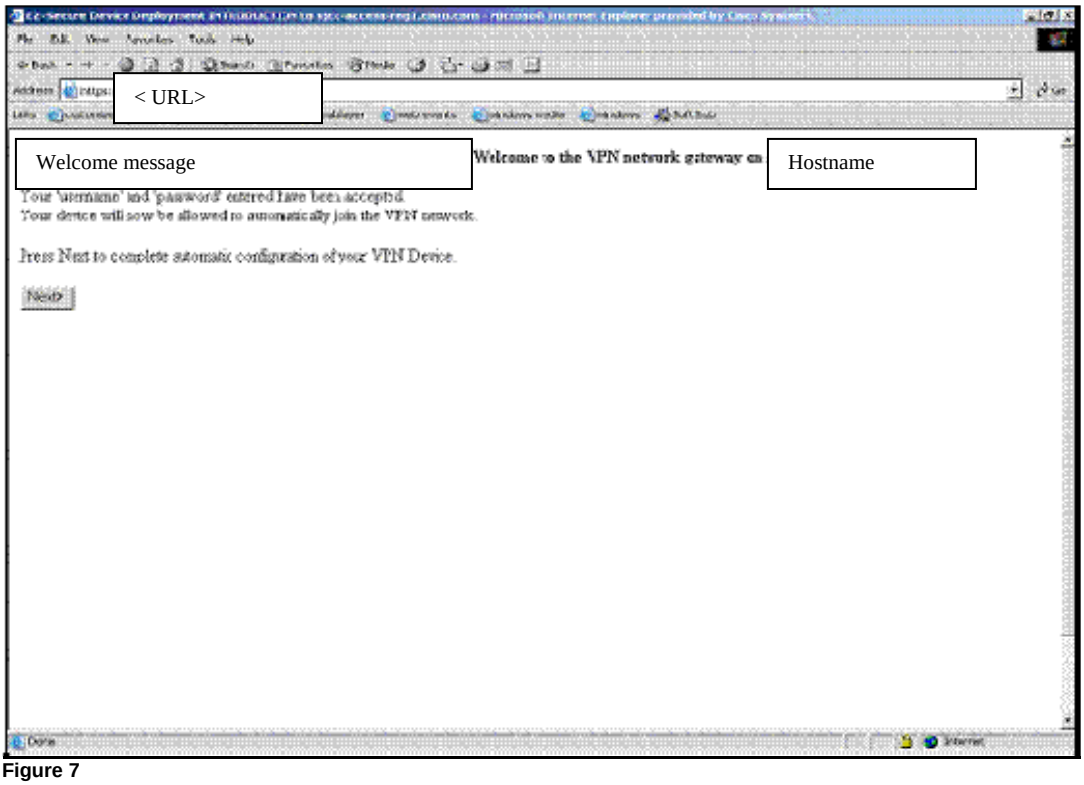


Figure 7

1. Select **Next** to allow the SDP utility to complete the configuration of your Cisco Virtual Office router.

8. Enrolling

The process will now continue with enrolling your Cisco Virtual Office router; Fig. 8. The complete configuration process can take several minutes. During this time it is recommended that you **NOT** attempt to select any of the offerings on the page; i.e. "Click here to see the running-config."

*** Screenshots below for the device deployment and configuration using Secure Device Provisioning (SDP) will look different, as SDP will be used in lieu of "Easy Secure Device Deployment (EzSDD)":**

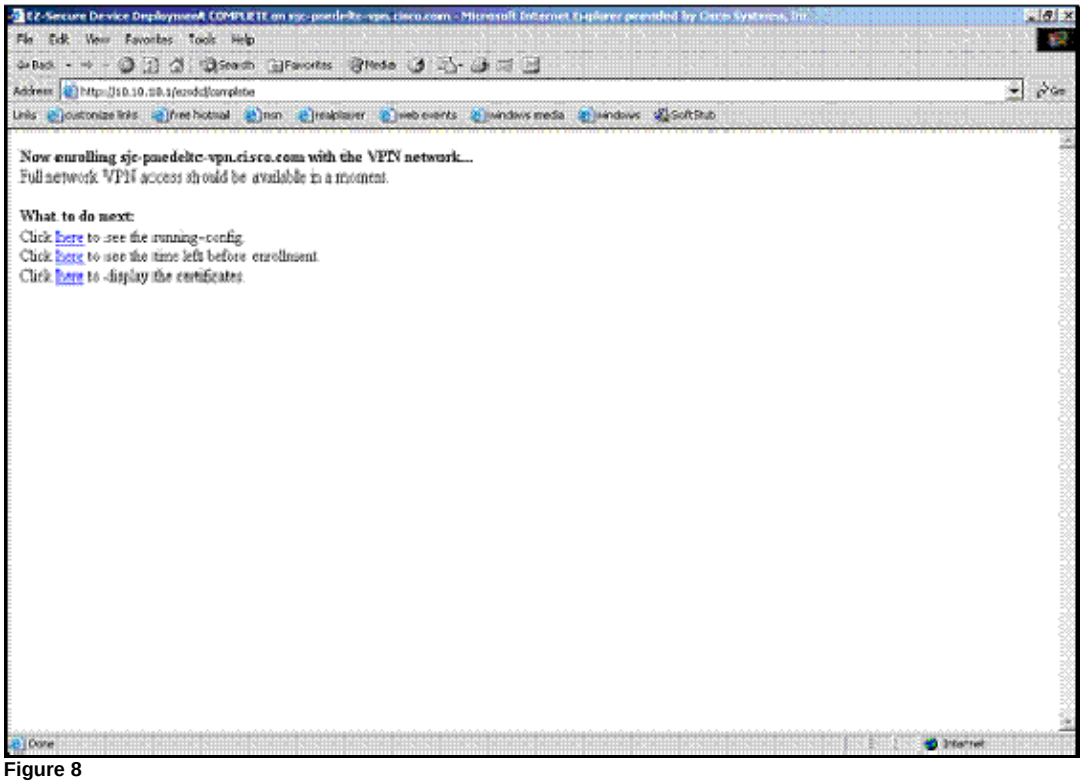


Figure 8

Note: Please be patient and wait a while for the process to complete. DO NOT interrupt the process as this will cause your service to not be fully deployed.

9. Verify Connectivity to the Internet

After a short time you can check your configuration by attempting to obtain a new IP Address from your Cisco Virtual Office router

Once you have a valid IP Address (ie. x.x.x.x, not the 10.10.10.x as previous to configuration) open your browser and attempt to connect to an external site. This should be something other than your corporate internal home page; ie. www.yahoo.com.

1. If this is successful then proceed with testing to a corporate internal site.
2. If you start page is a corporate internal site you will be prompted to authenticate as described in the next section.

10. Authentication to the Corporate Network using Authentication-Proxy / 802.1x Authentication Feature

Once your Cisco Virtual Office router configuration is complete you will be able to access the corporate internal network via the VPN tunnels that have been created. Before you will be allowed to pass any data or access any internal resources you will have to authenticate.

1. From your browser you must attempt to connect to an internal site to get the authentication prompt; Figure 9.

*** Screenshots below for the Authentication Proxy will look different, given it will be replaced 802.1x authentication:**

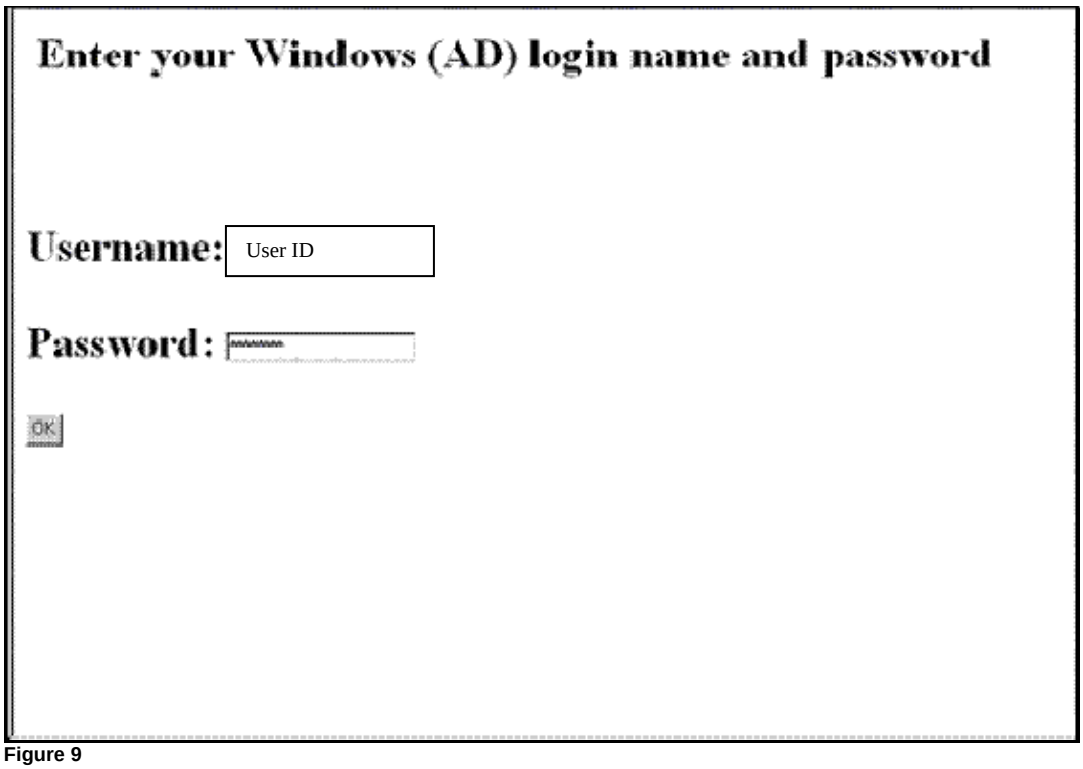


Figure 9

2. As directed enter your Active Directory (AD) login. This is the same login you use when starting your laptop/computer connection to the corporate network.

   Note: You may have to include your Domain with you username as in this example.

   If your authentication is successful you will either see another pop-up window or your screen will change to reflect Figure 10.

*** Screenshots below for the Authentication Proxy will look different, given it will be replaced 802.1x authentication:**

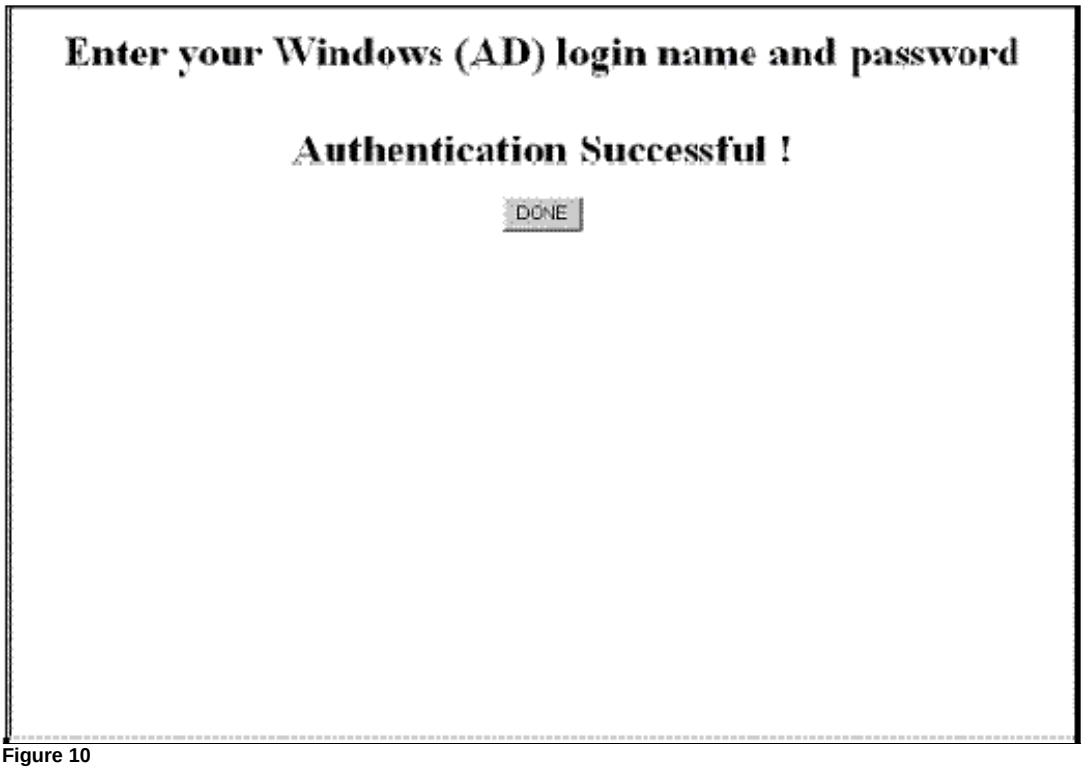


Figure 10

3. Select **DONE** to complete this step, or wait a little while and your browser may refresh automatically.

Note: If your authentication fails you will not be able to connect to the internal corporate network. Please ensure that you are using the correct password.

Congratulations! You are now ready to begin using your Cisco Virtual Office service! Please reference our Cisco Virtual Office web site for any further information regarding your new service.

Figure 7 SDP Deployment Screen

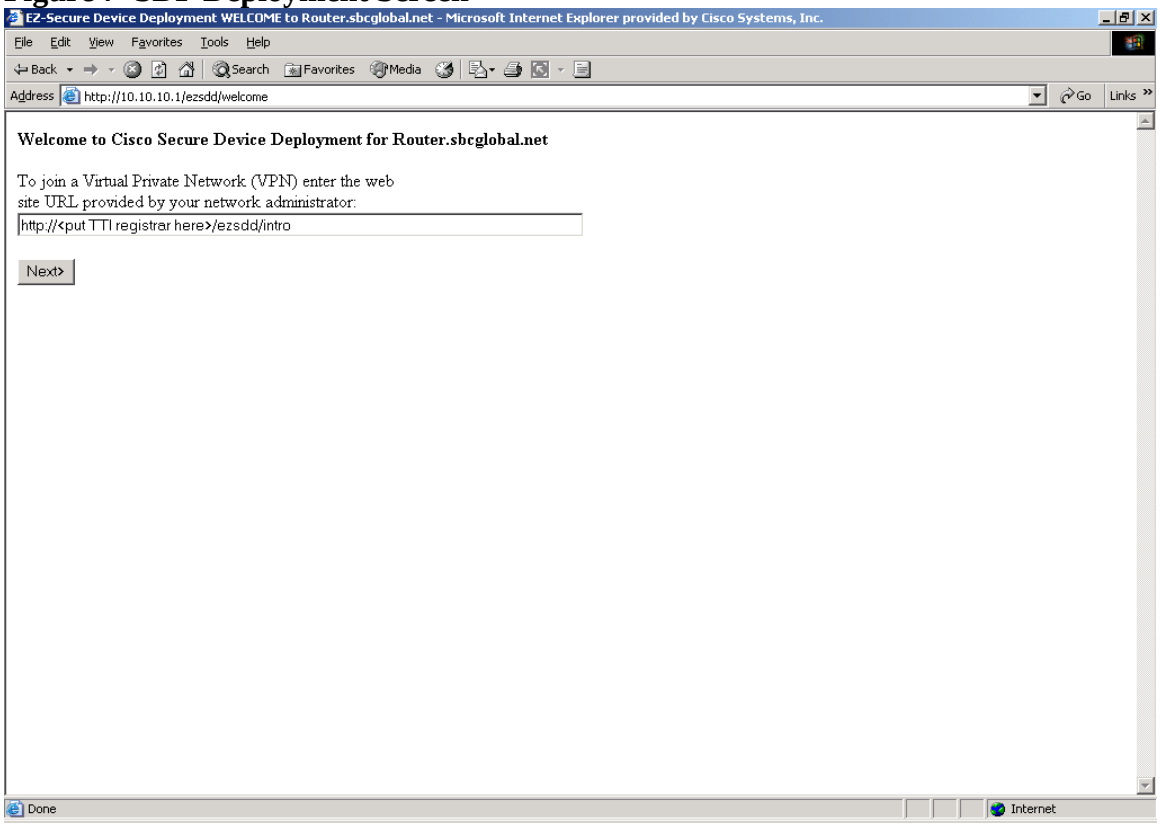


Figure 8 SDP Authentication Accepted Screen

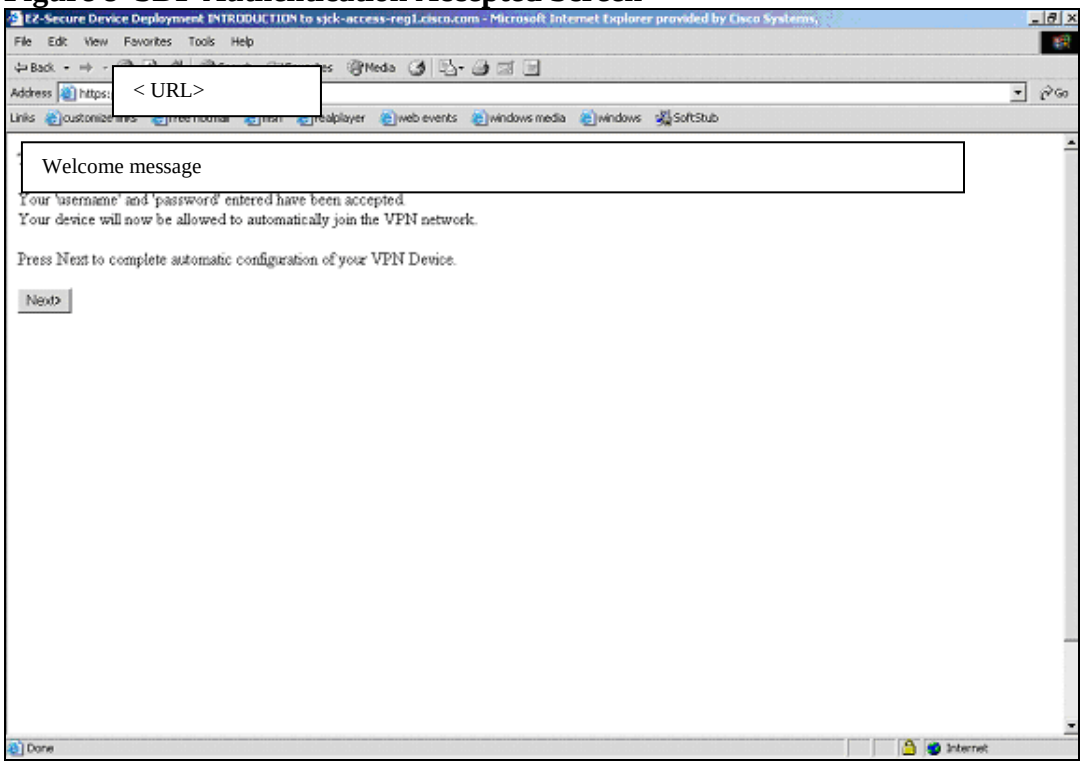
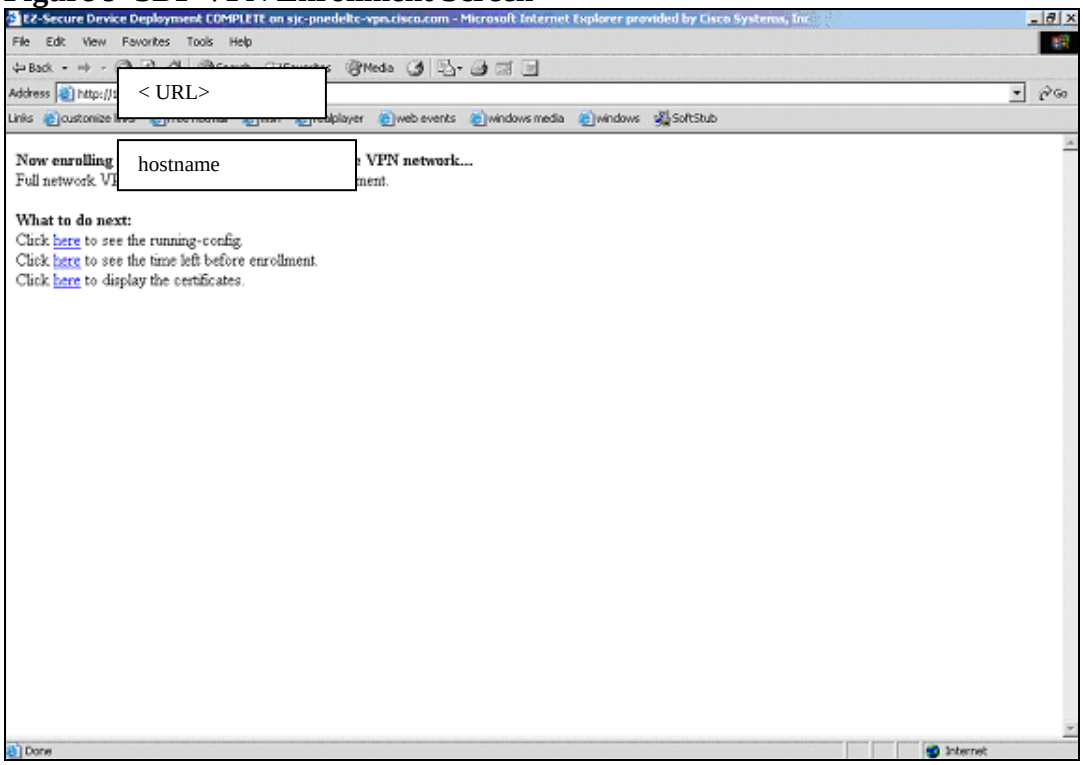


Figure 9 SDP VPN Enrollment Screen



3.4.2.1.2 SDP Configuration and PKI Certificates

Once the user configures the router for Internet access in the On-line provisioning scenario, Cisco Virtual Office relies upon Easy Secure Device Deployment[5] (SDP) to start the provisioning process, as graphically shown in Figure 10. From the point of view of managing the Cisco Virtual Office deployment, the provisioning process includes two phases.

5

<http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801ee176.html>.

In the first SDP phase, the user, the SDP Introducer, interacts with the spoke router, the SDP Petitioner, and establishes a Trusted Transitive Introduction (TTI) relationship with the SDP Registrar router at the location of the user's intended Data GWs. The SDP Registrar acts as a proxy for user authentication. After successful OTP user authentication, it intercepts the login_name provided by the user and requests a customized bootstrap configlet from ISC, which ISC creates by instantiating the SDP template shown below. The SDP Configlet is copied to the spoke router using the SDP Registrar – Petitioner TTI relationship, and the spoke router is enrolled in the certificate server that issues certificates used to authenticate the management IPSec tunnel.

SDP Template for Spoke Router

hostname ${u}| Variable ${u}=Spoke router hostname, u=username that the SDP Registrar obtains when the user authenticates with the OTP

privilege exec level 1 clock set
do clock set #systemCurrentTimeInIOSFormat()

username admin password
enable secret

ip cef
logging console debug
no ip domain lookup

service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service tcp-keepalives-in
service tcp-keepalives-out
service linenumber
service sequence-numbers
service password-encryption
service compress-config
no service config
no service udp-small-servers
no service tcp-small-servers
no service finger
no ip finger
no service pad
no ip source-route
no ip bootp server
no ip gratuitous-arps

clock timezone <timezone> -<#> |
clock summer-time <timezone> recurring | if appropriate
ntp server <IP-address-Public-Internet-server> | multiple servers configured
ntp server <IP-address-Management-GW-Fast-Ethernet- Management-Subnet> source Ethernet0

ip host <Hostname-IE2100> <IP-address-IE2100> | Regional Management Subnet Cisco CNS 2100 Series Intelligence Engine
ip host <Hostname-ISC> <IP-address-ISC> | Regional Management Subnet ISC

ip host <join-Site_Code-vpn>.cisco.com <IP-address-SDP-Registrar> | Regional Data GW SDP Registrar IP address
ip host <site_code-access-reg1>.cisco.com <IP-address-SDP-Registrar> | Regional Data GW SDP Registrar IP address
ip host <CERT1-Hostname> <IP-address>
ip host <CERT2-Hostname> <IP-address>

ip subnet-zero
ip domain-name cisco.com
ip domain lookup source-interface Ethernet0
ip radius source-interface Ethernet0
ip http client source-interface e0
ip ftp source-interface e0
ip tftp source-interface e0

ip name server <IP-address-Cisco-internal-DNS> | multiple DNS servers can be defined based upon Hub

!set $k =''
!set $s =''
!set $l =''

crypto ca trustpoint $l | Variable l=Certificate Server Trustpoint label. The “l” variable is instantiated by the Registrar
enroll url http://join-Site_code-vpn.cisco.com:80
rsakeypair $k $s | Variable k=Crypto wui tti label on the SDP Registrar. Variable s=RSA key size in bits. The “k” and “s” variables are instantiated by the SDP Registrar. The <join-Site_code-vpn.cisco.com> host is the regional SDP registrar
revocation-check none
subject-name CN=$u | Specifies the requested subject name that will be used in the certificate request. In Cisco Virtual Office $u=Site_code-username-vpn.cisco.com, for example sjc-pnedeltc-vpn.cisco.com
password none |
serial-number none | do not use the serial number in the certificate
auto-enroll 70 | attempt to re-enroll with the certificate authority when 70 percent of the life of the certificate has expired
fqdn none | | do not use the fully qualified domain name in the certificate request
ip-address none | do not use the IP address in the certificate request

$c | Variable c=Certificate Server certificate chain. The “c” variable is instantiated by the SDP Registrar
crypto ca enroll $l | Enrolls the spoke router in the Certificate Server trustpoint identified by the “l” variable.

crypto isakmp enable

no cdp run
no service config

crypto isakmp policy 1
encr 3des
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
crypto ipsec transform-set t1 esp-3des esp-sha-hmac

ip access-list extended smg_acl
permit ip host #systemGetAddr($management_ip) <IP-subnet-regional-Management-HUB>
<wildcard-subnet-mask> | The variable “management_ip” = <IP-address-spoke-router-interface-E0> and is substantiated from the ISC repository

crypto map ISC_CME 1 ipsec-isakmp
description Management Tunnel - SMG
set peer <IP-address-Regional-Management-GW>
set security-association lifetime kilobytes 530000000
set security-association lifetime seconds 14400
set transform-set t1
match address smg_acl

Interface Ethernet0
ip address $management_ip $subnet | The variables $management_ip and $subnet are substantiated from the ISC Repository. All spoke routers will be provided a /28 subnet routable in the internal Cisco network. The variable “management_ip” = <IP-address-spoke-router-interface-E0>
ip address <ip address> <mask> secondary | Sets the default IP address and subnet configured on the Ethernet 0 subnet of the Cisco 831 Ethernet Broadband Router, *<ip address> <mask>* to secondary

Interface Ethernet1 | Applies crypto map for Management tunnel to Public interface
crypto map ISC_CME

interface Dialer1 | Applies crypto map for Management tunnel to Public interface

cns trusted-server all-agents <IE2100-hostname>.cisco.com
cns event <IP-address-IE2100> 11011 source $management_ip keep 180 3 |The variable “management_ip” =<IP-address-spoke-router-interface-E0>

cns config partial <IP-address-IE2100> source systemGetAddr($management_ip) | The variable "management_ip" =<IP-address-spoke-router-interface-E0>

cns image server http://<IE2100-Hostname>.cisco.com/cns/HttpMsgDispatcher status http://<IE2100-Hostname>.cisco.com/cns/HttpMsgDispatcher |
<IE2100-Hostname>= Cisco CNS 2100 Series Intelligence Engine for the respective Management hub, such as ie-sjc2-1-n for SJ

cns exec 80 source #systemGetAddr($management_ip) | The variable "management_ip" =<IP-address-spoke-router-interface-E0>

cns config notify all

no logging cns-events

ip host <CERT2-Hostname> <IP-address-CERT2> | CERT2 for respective Management Hub

crypto ca trustpoint <CERT2-Hostname> | CERT2 hostname is used as label for CERT2 trustpoint on the spoke routers
enrollment mode ra
enrollment url http://<CERT2-Hostname>:80
crl optional
serial-number
source interface ethernet0
auto-enroll 70
exit

crypto ca certificate chain sjck-access-cert2
certificate ca XX | XX represents the certificate number of the CA certificate
<CA-Certificate-CERT2> | the CA certificate is pasted into the spoke router via the SDP template
end

The TTI configuration on the SDP Registrar follows.

SDP Registrar TTI Configuration
aaa group server radius fixedaaa
server <IP-address-ACS-server> auth-port 1645 acct-port 1646 | The "fixedaaa" server verifies that the device has an account. For Cisco Virtual Office this will be the regional EMAN ACS server IP
!
aaa group server radius tti
server <IP-address-AAA-server> auth-port 1645 acct-port 1646 | The "tti" server verifies that the user is a Cisco employee. This is the Infosec OTP AAA servers.
!

aaa authentication login tti group tti
aaa authorization network tti-parameters group tti
!
no crypto wui tti petitioner | This router not configured as the SDP petitioner. The spoke routers are configured as SDP
!
crypto wui tti registrar | This router is configured as the SDP Registrar .
pki-server SDPserver | SDP Registrar does not support RA mode yet. The pki server must run on the SDP Registrar at this time (see Security section).
template config <url>
authentication list tti | the user must authenticate against the OTP servers
authorization list fixedaaa | the device must have an account on the ACS server in order to be authorized; otherwise the On-line configuration process will fail

At this point the spoke router establishes a plain IPSec VPN tunnel with the management hub and enables a CNS agent on the spoke router. In the second SDP phase, commands are pushed to the spoke from the ISC in the Device Specific Configlet over the VPN tunnel. The Device Specific Configlet is created when the Site_Code-Production Template is instantiated from the ISC Data File for that specific spoke router. The Device Specific Configlet consists of all remaining non-SR commands that are applied on the spoke router by attaching the Device Specific Configlet to the IPSec SR. Both the SDP and Device Specific Configlets are required because all of the template commands cannot be included in the SDP Configlet in order to minimize the risk of misconfiguration due to improper downloads during the download of the SDP Configlet. In addition to commands, the Device Specific Configlet contains the root certificate for the certificate server that issues certificates used to authenticate the Data IPSec VPN tunnels. This reduces the time required to enroll the spoke router in this certificate server when the Device Specific Configlet is pushed to the spoke router.

3.4.2.2 Off-line Provisioning Scenario

In the Off-line Provisioning scenario it is possible to reduce the number of steps required to provision a spoke router vs. the On-line scenario, and possibly further simplifying the provisioning process and experience for users.

- ISC CERT-Proxy Feature
- Certificate and Configlet Installation

3.4.2.2.1 ISC CERT-Proxy Feature

Key to the Off-line Provisioning scenario is the ISC CERT-Proxy feature, which is available in ISC version 3.2.02. The ISC CERT-Proxy feature allows ISC to mimic an Cisco IOS Software device during the Certificate Authority enrollment process using the SCEP protocol to request a device certificate. It enables the ISC administrators and authorized users who have access to supplemental tools to obtain a device certificate for a spoke router on behalf of the spoke router.

The CA Proxy uses SCEP (Simple Certificate Enrollment Protocol), a Cisco designed protocol, to allow devices to enroll and retrieve certificates from a CA.[6] ISC acts as a proxy, generating device keys, creating the CSR file (Certificate Server Request), and requesting the Certificate from the CA. The ISC system uses the device attributes supplied as part of the certificate request.

ISC CERT-Proxy Template

CA Server Type can take these values - MS, Cisco IOS Software, Netscape, Entrust
MS - Microsoft, Netscape - for Netscape, Entrust - for Entrust

[6] http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm.


```
##$login_name
hostname $hostname

#set($aaa_name = "${hostname}.cisco.com")

##set($aaa_name = $hostname.cisco.com)

#set ($output = $TMSystem.execSysCmd("/apps/SD/isc/isc/bin/runscep $aaa_name IOS <IP-address-
CERT1> challenge $aaa_name 1024 $aaa_name"))

##set ($output = $TMSystem.execSysCmd("/apps/SD/isc/isc/bin/runscep $aaa_name IOS <IP-address-
CERT1> challenge $aaa_name 1024"))

#set ($errorcode = $TMSystem.getExecCmdStatus())

## TPOINT is Trustpoint label to associate certificate
## or pkcs-12 file with. This should be configured
## before using this crypto ca import command

#if ($errorcode == "0")
#icmd-begin
crypto ca import <site_code-building-access-cert1> pkcs12 terminal password
End with a blank line | #icmd-cert-begin
$output
quit
#icmd-cert-end
#icmd-end
#else
#systemThrowException(2 "Error:Certificate not granted by CA Server:${output}" )
#end

privilege exec level 1 clock set
do clock set #systemCurrentTimeInIOSFormat()

username admin password
enable secret

ip cef
logging console debug
no ip domain lookup

service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service tcp-keepalives-in
service tcp-keepalives-out
service linenumber
service sequence-numbers
```



```
service password-encryption
service compress-config
no service config
no service udp-small-servers
no service tcp-small-servers
no service finger
no ip finger
no service pad
no ip source-route
no ip bootp server
no ip gratuitous-arps

clock timezone <timezone> <UTC-offset>
clock summer-time <timezone> recurring
ntp server <IP-address-Public-NTP-server>
ntp server <IP-address-Management-GW-Management-subnet> source Ethernet0
ip subnet-zero
ip domain-name cisco.com
ip host <Hostname-SDP-Registrar  <IP-address>
ip host <Hostname-CERT1> <IP-address-CERT1>
ip host <Hostname-CERT1> <IP-address-CERT2>
ip host <Hostname-ISC> <IP-address-ISC>
ip host <Hostname-IE2100> <IP-address-IE2100>

ip domain name cisco.com
ip domain lookup source-interface Ethernet0
ip radius source-interface Ethernet0
ip http client source-interface e0
ip ftp source-interface e0
ip tftp source-interface e0

aaa new-model

ip name-server <IP-address-internal-DNS>
ip name-server <IP-address-internal-DNS>
ip name-server <IP-address-internal-DNS>

crypto isakmp enable

no cdp run
no service config
alias exec i sh ip int brief
alias exec ss sh cry is sa
alias exec rr show run brie

crypto isakmp policy 1
 encr 3des
```


crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
crypto ipsec transform-set t1 esp-3des esp-sha-hmac

ip access-list extended smg_acl
permit ip host #systemGetAddr($management_ip) <IP-subnet-Management-Hub> <wildcard-subnet-mask>

crypto map ISC_CME 1 ipsec-isakmp
description Management Tunnel - SMG
set peer <IP-address-Management-GW-Loopback1>
set security-association lifetime kilobytes <kB>
set security-association lifetime seconds <secs>
set transform-set t1
match address smg_acl
exit

Interface Ethernet0
ip address $management_ip <mask> | $management_ip = interface E0

Interface Ethernet1
crypto map ISC_CME

interface Dialer1
crypto map ISC_CME

cns trusted-server all-agents <Hostname-IE2100>.cisco.com

cns event <Hostname-IE2100>.cisco.com 11011 source $management_ip keep 180 3 | management_ip = interface E0 ip address

cns config partial <Hostname-IE2100>.cisco.com source #systemGetAddr($management_ip)

cns image server http:// <Hostname-IE2100>.cisco.com/cns/HttpMsgDispatcher status http:// <Hostname-IE2100>. /cns/HttpMsgDispatcher

cns exec 80 source #systemGetAddr($management_ip)

cns config notify all

no logging cns-events

crypto pki trustpoint <Hostname-CERT1>
enrollment url http://<Hostname-CERT1>:80
crl optional
serial-number


```
 source interface ethernet0
 auto-enroll 70
 exit


ip host <Hostname-CERT2> <IP-address-CERT2>

crypto ca trustpoint <Hostname-CERT2>
 enrollment mode ra
 enrollment url http://<Hostname-CERT2>:80
 crl optional
 serial-number
 source interface ethernet0
 auto-enroll 70
 exit


crypto ca certificate chain <Hostname-CERT2>
certificate ca XX
  end
```

3.4.2.2.2 Certificate and Configlet Installation

Once the device certificate for the spoke is generated, it can be downloaded to the CPE by one of three simple methods:

- Authorized personnel access the spoke router CLI using telnet or SSH and paste the BASE 64 pkcs12 certificate into the router by an interactive process that requires positive confirmation to accept the certificate.[7] This is the method that will be used on the Cisco Virtual Office implementation.

- Instruct a download and import of a binary pkcs12 certificate using FTP, TFTP, SCP, or other supported Cisco IOS Software file transfer method using the CNS agent on the device.

- Request the user to install the certificate via the CLI, as part of a Configlet that consists of all of the commands required to establish a management VPN tunnel. Because the PKCS12 file generated by scep_client includes the CA certificate, device certificate, and device private key, this information, added to a configlet that is customized for the user's router with CNS CLIs and IPs, could be sent to the user by secure means. However, the method to deliver this Configlet is under development to security concerns.

[7] This process is documented at: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bd1.html#51847.

3.4.2.3 In-House Provisioning Scenario

The In-house provisioning scenario is the configuration of the spoke routers at a Cisco office by IT engineers on behalf of other users. The In-house provisioning scenario is manually intensive, but it is assumed that there will continue to be a limited requirement for this deployment scenario for executives and other special cases. Under this scenario, the spoke router must be connected to the internal corporate network.

3.4.3 Automated Policy Deployment and Audit

After the spoke router establishes a management VPN tunnel, it sends a CNS "connect" event to the CNS Engine (Cisco CNS 2100 Series Intelligence Engine). The Cisco CNS 2100 Series Intelligence Engine then sends a Connect event message on behalf of the spoke router to the ISC server, a CNS server, over the TIBCO bus. Upon receiving the Connect event, ISC should then deploy all SRs that have been prepared for the spoke router via the CNS transport mechanism and the Cisco CNS 2100 Series Intelligence Engine.

The SRs are:

- IPSec
- FW
- QoS
- N

3.4.3.1 IPSec SR

The IPSec SR is the first SR that will be deployed to the spoke router. However, recall that under the On-line Provisioning Scenario the Device Specific Configlet will still have not been deployed. The Device Specific Configlet contained Template commands that must be configured on the spoke router that were not included in the SDP Config File. The IPSec SR offers the feature to attach a configlet to the SR, and upon SR deployment the configlet will be deployed before any of the SR commands. Cisco Virtual Office uses this feature to deploy the Device Specific Configlet.

The IPSec SR includes information to configure the mGRE interface (Tunnel 0) on the spoke routers, including all DMVPN-related IPSec and EIGRP information. Specific router commands that will be deployed as part of the IPSec SR for each Cisco Virtual Office spoke router are shown below.

IPSec SR Commands

```
crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile ISC_IPSEC_PROFILE_1
 set security-association lifetime kilobytes <kB>
```


set security-association lifetime seconds <secs>
set transform-set ISC_TS_1

interface Tunnel0
description Provisioned by ISC: Peer location = <location>
bandwidth 2000
ip address <IP-address-tunnel-interface> <subnet-mask-tunnel-interface> | the mGRE tunnel interface on the spoke routers and the associated mGRE tunnel interface on the Data GWs are on the same IP subnet
no ip redirects
ip mtu 1400
ip nhrp map <IP-address-tunnel-interface-primary-Data-GW> <IP-address-loopback-interface-primary-Data-GW> | maps the Data GW Loopback interface that is used for IPSec tunnel terminations to the mGRE interface of the primary Data GW
ip nhrp map multicast <IP-address-tunnel-interface-primary-Data-GW>
ip nhrp map multicast dynamic | NHRP will automatically create a broadcast/multicast mapping for the spoke router when it registers with the NHRP server (Data GW) using the IP address defined in the previous command
ip nhrp map <IP-address-tunnel-interface-secondary-Data-GW> <IP-address-loopback-interface-secondary-Data-GW> | maps the Data GW Loopback interface that is used for IPSec tunnel terminations to the mGRE interface of the secondary Data GW
ip nhrp map multicast <IP-address-tunnel-interface-secondary-Data-GW>
ip nhrp network-id <network-ID> | as specified for the specific Data GW hub and tunnel interface
ip nhrp holdtime 300
ip nhrp nhs <IP-address-tunnel-interface-primary-Data-GW> | next-hop-server IP address for NHRP protocol
ip nhrp nhs <IP-address-tunnel-interface-secondary-Data-GW>
no ip route-cache cef
no ip route-cache
no ip mroute-cache
qos pre-classify
tunnel source Ethernet1
tunnel mode gre multipoint | Enables a GRE tunnel to be used in multipoint fashion. Multipoint tunnels require that you configure a tunnel key. Otherwise, unexpected GRE traffic could easily be received by the tunnel interface. For simplicity, we recommend that the tunnel key correspond to the NHRP network
tunnel key <tunnel-key> | The tunnel key will be the same as the ip nhrp network-id.
tunnel protection ipsec profile ISC_IPSEC_PROFILE_1 shared | Associates this tunnel interface with the IPSec profile ISC_IPSEC_PROFILE_1

router eigrp <AS-Number>
network <IP-subnet-ethernet0 > 0.0.0.15 | each spoke router provided a /28 subnet
network <IP-subnet-mGRE> 0.0.1.255 | each mGRE interface will initially be configured with a wildcard subnet mask of /23

distribute-list ISC_IPSEC_REDISTRIBUTE_LIST_1 out | limits
no auto-summary
eigrp stub connected | informs Data GWs that the spoke router is a stub router and, as a result, Data GWs will not send queries to the spoke router

ip access-list standard ISC_IPSEC_REDISTRIBUTE_LIST_1
permit <ip-address-subnet-spoke-router> <wildcard-subnet-mask> | allows advertisement of only the Ethernet 0 subnet
permit <ip-address-subnet-mgre-interface> <wildcard-subnet-mask> | allows advertisement of the Tunnel 0 (mGRE) interface

3.4.3.2 Firewall SR

The stateful FW SR includes information to configure the Cisco IOS Software FW on the spoke router, including its application to the Ethernet 0 (inside interface). In addition to CBAC, Auth-Proxy is configured via the FW SR. An example of the specific commands configured with the FW SR with the exception of Auth-proxy related commands are shown below.

FW SR Commands

aaa new-model
aaa authentication login default local group radius
aaa authorization auth-proxy default group radius

ip auth-proxy name ISC_AUTH_PROXY http list ISC_AUTH_PROXY_1
ip auth-proxy inactivity-timer 1440
ip auth-proxy max-login-attempts 5
ip auth-proxy auth-proxy-banner http |

ip inspect name ISC_inside_1 tcp
ip inspect name ISC_inside_1 rtsp
ip inspect name ISC_inside_1 smtp
ip inspect name ISC_inside_1 h323
ip inspect name ISC_inside_1 realaudio
ip inspect name ISC_inside_1 tftp
ip inspect name ISC_inside_1 skinny
ip inspect name ISC_inside_1 ftp
ip inspect name ISC_inside_1 udp
ip inspect name ISC_inside_1 netshow
ip inspect name ISC_inside_1 sip

interface Ethernet0
ip inspect ISC_inside_1 in
ip auth-proxy ISC_AUTH_PROXY
ip access-group ISC_FIREWALL_inside_inbound_1 in

interface Ethernet1
ip access-group ISC_FIREWALL_outside_inbound_1 in

ip access-list extended ISC_FIREWALL_outside_inbound_1
permit ip <IP-subnet-Management-Hub> <wildcard-subnet-mask> <IP-subnet-spoke-router-E0-interface> <wildcard-subnet-mask>
permit udp any any eq non500-isakmp
permit esp any any

permit icmp any any
permit udp any any eq isakmp
permit gre any any
permit udp any any eq bootpc
permit udp host <IP-address-public-NTP-server> any eq ntp

ip access-list extended ISC_AUTH_PROXY_1
deny tcp any host <Call_Manager-IP-Address> eq www
deny tcp any host <ACNS_CE-IP Address> eq www
deny tcp any host <Server-IP-Address> eq www
permit ip any <Routable-IP Address Block> <Wildcard_Subnet_Mask>

ip access-list extended ISC_FIREWALL_inside_inbound_1
permit udp any <ECT-Spoke-Router IP-addresses> <Wildcard_Subnet_Mask> eq 21862 permit tcp any <ECT-Spoke-Router IP-addresses> <Wildcard_Subnet_Mask> eq 22
permit tcp any <ECT-Spoke-Router IP-addresses> <Wildcard_Subnet_Mask> eq telnet
permit udp any any eq bootps
permit tcp any any eq domain
permit udp any any eq domain
permit ip any host <ACS-Server-IP-Address>
permit tcp any any range 1719 1720
permit udp any any range 24576 24656
permit udp any any range 2326 2340
permit udp any any eq 5445
permit tcp any any eq 2000
permit udp any any eq tftp
permit udp any <ip-address-block-IP-telephones> <wildcard-subnet-mask> range 16384 32767
permit tcp any host <Call_Manager-IP-Address> eq www
permit tcp any host <ACNS_CE-IP Address> eq www
permit tcp any <ip-address-AD-servers> <wildcard-subnet-mask> eq 1026
permit tcp any <ip-address-AD-servers> <wildcard-subnet-mask> eq 389
permit tcp any <ip-address-AD-server> <wildcard-subnet-mask> eq 88
permit tcp any <ip-address-AD-server> <wildcard-subnet-mask>eq 445
permit tcp any <ip-address-AD-server> <wildcard-subnet-mask> eq 135
permit udp any <ip-address-AD-server> <wildcard-subnet-mask> eq 389
permit udp any <ip-address-AD-server> <wildcard-subnet-mask> eq 88
permit udp any <ip-address-AD-server> <wildcard-subnet-mask> eq 445
permit tcp any host <ip-address-SSH-server> eq 22

permit ip any <ip-address-block-SW-VPN-concentrators> <wildcard-subnet-mask>
permit ip any <ip-address-block-ECT-Management-subnet> <wildcard-subnet-mask>
deny ip any <ip-address-block-corporate blocks> <wildcard-subnet-mask>
permit ip any any

ip http authentication aaa

radius-server host <IP-address-RADIUS-server> timeout 10 retransmit 3 key

3.4.3.3 QoS SR

In the Cisco Virtual Office deployment the traffic shaping value will vary depending upon the user's upstream bandwidth. It will be configured per the information provided by the user in the IT User Request Form. Below is an example of the commands configured on a spoke router by the QoS SR.

QoS SR Commands

```
ip access-list extended ISC_OUT_QOS_ACL_Cisco-IT_SJ_VOICE_ONE_Control
 permit UDP any any eq isakmp
!
class-map match-all ISC_OUT_Cisco-IT_SJ_VOICE_ONE_VoIP
 match ip precedence 5
!
class-map match-all ISC_OUT_Cisco-IT_SJ_VOICE_ONE_Signaling
 match ip precedence 3
!
class-map match-any ISC_OUT_Cisco-IT_SJ_VOICE_ONE_Control
 match access-group name ISC_OUT_QOS_ACL_Cisco-IT_SJ_VOICE_ONE_Control
 match ip precedence 6
 match ip precedence 7
!
policy-map ISC_OUT_Cisco-IT_SJ_VOICE_ONE
 class ISC_OUT_Cisco-IT_SJ_VOICE_ONE_VoIP
  priority 80
 class ISC_OUT_Cisco-IT_SJ_VOICE_ONE_Signaling
  bandwidth percent 10
 class ISC_OUT_Cisco-IT_SJ_VOICE_ONE_Control
  bandwidth percent 10
 class class-default
  fair-queue
  random-detect
!
policy-map ISC_OUT_Cisco-IT_SJ_VOICE_ONE_TOP
 class class-default
  shape average <bandwidth-in-bits-per-second>
```


service-policy ISC_OUT_Cisco-IT_SJ_VOICE_ONE
!
interface Ethernet1
service-policy output ISC_OUT_Cisco-IT_SJ_VOICE_ONE_TOP

3.4.3.4 NAT SR

Spoke routers properly configured with NAT enable devices connected to the Ethernet 0 to access the Internet even if for some reason the VPN tunnels are down. The NAT SR consists of the commands shown below. ISC employs a route-map to perform NAT on the spoke routers. There are no alternatives if changes to the NAT configuration are to be deployed as an SR and as a result monitored versus configuration changes implemented via template commands.

NAT SR Example Commands

interface Ethernet0
ip nat inside

interface Ethernet1
ip nat outside

ip nat inside source route-map ISC_IP_NAT_DYNAMIC_ROUTEMAP_1 interface Ethernet1 overload

ip access-list extended ISC_IP_NAT_DYNAMIC_ACL_1
deny ip <IP-subnet-ethernet-0> <wildcard-subnet-mask> <IP-Subnet-Management-subnet> <wildcard-subnet-mask> | NAT is not applied to the Cisco Virtual Office management traffic
permit ip <IP-subnet-ethernet-0> <wildcard-subnet-mask> any

route-map ISC_IP_NAT_DYNAMIC_ROUTEMAP_1 permit 10
match ip address ISC_IP_NAT_DYNAMIC_ACL_1

Additional Sources

1. Dynamic Multipoint VPN
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba1.html#53110

2. IPSec Profiles
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tsr/fipsencr/sftipsec.htm#1056276

3. <http://www.cisco.com/en/US/partner/about/ac123/ac114/ac173/Q2-04/dmvpn.html>
Cisco Packet Vol. 16. No. 2. Second Quarter 2004
Cisco IOS Software DMVPN reinforces teleworker initiative with unmatched end-to-end security, connectivity, deployment, and management.
Plamen Nedeltchev, Gautam Aggarwal, Helder Antunes, and David Iacobacci

4. Detailed description of DMVPN
<http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba1.html#53110>

5. PKI AAA Integration
<http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/products_feature_guide09186a00801b0692.html>

6. Service Assurance Agent Configuration
<http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d3a94.htm