Deployment of Cisco IOS Software-Based SSLVPN in Cisco's Internal Enterprise Class Teleworker Network

The Cisco® Enterprise Class Teleworker solution is a highly scalable Cisco IOS® Software-based solution that securely integrates the network infrastructure, management infrastructure, managed services, and applications across the entire enterprise, including LAN, WAN, branch, and teleworker locations.

The solution is an integral part of the Cisco Service-Oriented Network Architecture (SONA), a framework that enables enterprise customers to build integrated systems across a fully converged, intelligent network. Using the Cisco SONA framework, the enterprise network can evolve into an Intelligent Information Network-one that offers the kind of end-to-end functions and centralized, unified control that promote true business transparency and agility.

Cisco Systems® has successfully deployed the Enterprise Class Teleworker solution within its own organization, increasing productivity and improving efficiency while enabling "zero-touch" deployment, manageability, and low-to-negative total cost of ownership (TCO). Enterprises and service providers can use the Cisco ECT solution to offer the benefits of network services to their end users and customers, while maintaining an effective Return of Investment (ROI).

For ECT/SONA Solution Overview, refer to:

http://www.cisco.com/en/US/products/ps6660/prod_brochure0900aecd803fc7ec.html

For ECT/SONA solution, services and applications support, refer to the following Cisco.com link:

http://cisco.com/go/ect/

Cisco IOS® SSLVPN provides remote secure corporate network (intranet) access over the standard public Internet using only a web browser and its native Secure Socket Layer (SSL) encryption. SSL authentication and encryption/decryption operates at the application level, which eliminates the need for any special-purpose software installation at the client side. An SSL-enabled web browser and e-mail client can be used to access e-mail, intranet, and various applications and resources inside the corporate network. The end host supporting the browser could be any IP-based host (PC, Macs, Linux/UNIX, etc.).

PURPOSE AND SCOPE

This guide describes how a Cisco IOS Software-based router can be configured and deployed as an SSLVPN gateway.

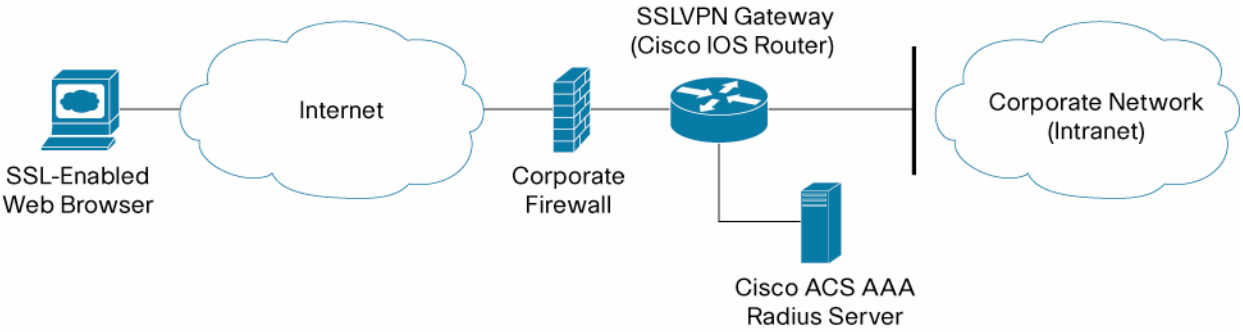
SSLVPN can be used as a standalone secure remote access to corporate services. It can also be deployed as a complement to the Enterprise-Class Teleworker (ECT) solution for the mobile users that sometimes need to have access to the corporate intranet from a public Internet access location. There is no need to install any software on the end host; only an SSL-enabled web browser is needed.

The SSLVPN gateway can be configured in a standalone router, or combined with an ECT converged VPN hub.

The SSLVPN gateway can be configured manually, or using Cisco Secure Device Manager (SDM). Cisco SDM is a Web-style graphical user interface (GUI) tool that can be used to configure Cisco IOS® routers. It usually comes with a router's factory default configuration and can be invoked from any Java-enabled browser that has connectivity to the Cisco IOS router to be configured. This guide shows how to configure the gateway manually. For more details on SDM go to http://www.cisco.com/en/US/products/ps6809/products_ios_protocol_option_home.html

NETWORK ARCHITECTURE

Figure 1. SSLVPN Topology for an Enterprise-Class Teleworker Deployment



SSL VPN is configured in a Cisco IOS router.

Using an SSL-enabled web browser, the user establishes a connection to the SSLVPN gateway. Once the user has been authenticated with the Cisco Access Control Server (ACS), an SSLVPN session is established and the user can access the internal corporate network.

Since the SSLVPN gateway provides an entrance into the corporate network, it should always be installed behind a firewall. Only the SSL port (port 443) should be opened on the corporate firewall for secure access back to the SSLVPN gateway.

FEATURE DESCRIPTION

Using an SSL-enabled web browser (Internet Explorer, Netscape, or the equivalent), the user can establish a connection to the SSLVPN gateway. The initial user request to the SSLVPN gateway will be responded to with a user logon HTML page. The username and password will be submitted to the gateway for authentication with a RADIUS server (Cisco ACS), and a session will only be granted if the authentication is successful.

If a session is established, it is maintained by sending a session cookie to the user browser. This cookie has to be embedded in all the following user HTTP requests for authentication at the SSLVPN gateway. If the cookie is missing or incorrect, the session will be dropped, and the user can no longer access the corporate network.

Normally, the session remains until the user logs out, the session times out, or the session is cleared from the SSLVPN gateway.

Cisco IOS SSLVPN delivers three modes of SSL VPN access: clientless mode, thin-client mode, and full-tunnel client mode.

In clientless access mode, once the user is authenticated and a session is established, an SSLVPN portal page and toolbar is displayed on the user's web browser. From this page, the user can access all available HTTP sites, access web e-mail, and browse Common Internet File System (CIFS) file servers.

Note: If a "popup blocker" is enabled, it is possible that the small SSLVPN toolbar window is not displayed. To avoid this, disable the popup blocker for this SSLVPN session page.

In thin-client mode, clicking on the "Start Application Access" link gives the user access to all the internal servers configured through TCP port forwarding. Note: Java Runtime Environment (JRE) is needed on your end host to make this application run properly.

TCP port forwarding is achieved by letting the user download a Java applet, which will initiate an HTTP request to the SSLVPN gateway from the client. The SSLVPN gateway will create a TCP connection to the internal server, and after the initial setup the connection between the client and the internal server will be treated as an SSL tunnel with TCP packets being switched directly from either direction.

In full-tunnel client mode, an SSL tunnel is used to move data to and from the internal networks at the network (IP) layer. When the user logs into the SSLVPN gateway, the SSL VPN client (SVC) is automatically downloaded and installed at the end user's PC, and the tunnel connection is established. Once the connection is established, the user has full VPN access to the corporate network. Using full tunnel mode it is also possible to have voice support. Using the Cisco softphone IP Communicator the user can register with the Cisco Call manager in the corporate network, and thus have a portable "office phone".

PLATFORMS AND IMAGES

Recommended platforms for Cisco IOS SSLVPN gateway are:

- Cisco 3845
- Cisco 3825

Supported platforms for Cisco IOS SSLVPN are:

- Cisco 1800 Series
- Cisco 2800 Series
- Cisco 3700 Series
- Cisco 3800 Series
- Cisco 7200 Series
- Cisco 7301

Cisco IOS SSLVPN is available in Cisco IOS Software Release 12.4(6)T and later.

CONFIGURATION

The following SSLVPN-specific configurations are required on the gateway.

Configuring the Public Key Infrastructure

SSLVPN is based on HTTPS, which requires a public key infrastructure (PKI) trustpoint to be configured.

One of the first things checked within a certificate is the expiration. A valid date is required and the router has to have the correct time. To configure the router as a Network Time Protocol (NTP) client, use the following configuration:

```
ntp server <ntp-server-ip>
```

The host name and the domain name must be set as well:

```
hostname webvpn-gateway
ip domain name cisco.com
```


After this, RSA keys can be generated:

```
webvpn-gateway(config)#crypto key generate rsa general-keys label
webvpn-certificate modulus 1024
The name for the keys will be: webvpn-certificate-server.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
```

To configure a trustpoint and enroll with the certificate server, use the following configuration:

```
crypto pki trustpoint <trustpoint-name>
enrollment url http://certificate-server
```

The SSLVPN gateway will use a default trustpoint name of “SSLVPN”. To tell the SSLVPN gateway to use a trustpoint with another name, the following configuration is used:

```
webvpn
ssl trustpoint <trustpoint-name>
```

For more details on the certificate management, see Appendix B.

Configuring the User Database

A user database is needed for authenticating the end user with the SSLVPN gateway. The database can be local or any RADIUS/TACACS+ authentication, authorization, and accounting (AAA) server. Cisco ACS is used for ECT.

To configure a local database, use the following configuration:

```
aaa new-model
username user1 secret 0 passwd1
aaa authentication login default local
```

It is recommended to use a separate AAA server like Cisco ACS so that unique passwords can be provided for each user, and so that user connections can be logged. This is how the SSLVPN gateway will be configured to use a remote AAA RADIUS server for authentication purposes:

```
aaa new-model
aaa group server radius sslvpn
server-private <radius-server> auth-port 1812 acct-port 1813 key <radius-key>
aaa authentication login default local group sslvpn
ip http authentication aaa
```


SSLVPN Configuration

The following sections describe how to enable and configure SSLVPN.

Configuring the Virtual Gateway

Before using the SSLVPN feature, a virtual gateway must be configured and put in service. This specifies the IP address and port to use for SSLVPN and configures the trustpoint to use. The IP address should be a public IP address configured on an interface or loopback interface on the SSLVPN gateway. The default port is 443, and the default trustpoint name is “SSLVPN”. By putting the virtual gateway in service, SSLVPN service is enabled on the gateway.

```
webvpn gateway webvpn-gw
 ip address 10.10.10.30 port 443
 ssl trustpoint SSLVPN
 inservice
```

Configuring the Virtual Context

A SSLVPN virtual context must be configured to associate the virtual SSLVPN gateway with the configured features. Multiple virtual contexts can be configured on the secure gateway, giving access to various features and access modes, depending on the domain configured for each context. Following is an example of configuring a virtual context and putting it in service:

```
webvpn context webvpn_context
 title “WebVPN BETA TESTING”
 gateway webvpn-gw domain default
 inservice
```

The end user gets access to the different features configured in each context by specifying the domain in the URL when accessing the SSLVPN gateway: https://<SSLVPN-gateway-IP>/<domain-name>. If no domain name is specified in the URL, the default context will be used.

Multiple contexts can be configured, giving different levels of access. For example, two contexts can be configured, one with domain clientless giving only clientless access, and one with domain tunnel giving full-tunnel access. By going to https://<SSLVPN-gateway>/clientless, the user will only get clientless access to the SSLVPN gateway. By going to https://<SSLVPN-gateway>/tunnel, the user will get full-tunnel access to the internal network.

Configuring the Group Policy

A group policy is configured for each SSLVPN virtual instance. The group policy specifies the SSLVPN features and parameters to be used for this virtual instance. The Citrix, CIFS, Cisco Secure Desktop, thin-client mode, and full-tunnel mode features can be enabled or disabled in the group policy, which is then associated with the SSLVPN context.

Configuration example for URL list, port forwarding, CIFS, full-tunnel mode, and Citrix:

```
policy group policy-group
   url-list “url-list”
   port-forward “portlist”
   nbns-list “cifs-servers”
   functions file-access
   functions file-browse
   functions file-entry
   functions svc-enabled
```



```
svc address-pool “webvpn-pool”
svc split include 10.0.0.0 255.0.0.0
svc split include 192.168.0.0 255.255.0.0
svc dns-server primary 10.2.2.2
citrix enabled
```

Associating the group policy with the SSLVPN context:

```
webvpn context webvpn_context
 default-group-policy policy-group
```

Configuring Clientless Mode

In clientless mode, the user is able to access the internal corporate network by only using the SSL-enabled web browser on the client PC. The applications available in this remote access mode are:

- Web browsing
- File sharing (CIFS)
- Web-based e-mail
- Citrix server access

Configuring Web Browsing

A URL box is provided on the portal page to allow web browsing. Lists of web server links can be configured and will be displayed on the portal page. These URL lists are provided for ease of navigating the internal websites. The URL lists are configured in the SSLVPN context sub mode, and must be defined in the group policy for the given SSLVPN context. If you have enabled Citrix in the group policy, you can add a link in the URL list to the Citrix server.

```
url-list “Internal web”
   heading “Internal”
   url-text “OWA” url-value “email.domain.com”
   url-text “Homepage” url-value “www.domain.com”
 !
 url-list “Citrix”
   heading “Citrix”
   url-text “Citrix Server” url-value http://citrix-server.domain.com
```

The URL lists must be associated with the SSLVPN context by configuring it in the context’s policy group:

```
webvpn context webvpn_context
 policy group policy-group
  url-list “Internal web”
  url-list “Citrix”
```


Configuring CIFS

A CIFS browsing box is provided on the portal page to allow browsing and file access of files on the remote NBNS (NetBIOS Name Service) servers. NBNS servers are configured in the SSLVPN context sub mode, and the NBNS list must be defined in the group policy for the given SSLVPN context.

```
nbns-list cifs-servers
   nbns-server 10.10.10.50
   nbns-server 10.10.10.60
```

The NBNS list must be associated with the SSLVPN context by configuring it in the context's policy group. The file functions allowed by the CIFS server are also configured in the policy group.

```
webvpn context webvpn_context
 policy group policy-group
   nbns-list "cifs-servers"
   functions file-access
   functions file-browse
   functions file-entry
```

Configuring OWA

Web e-mail such as Microsoft OWA 2003 is supported in SSLVPN. No special configuration is required to use this feature. A link can be configured on the portal page to allow the user to connect to the Microsoft Exchange server and read web-based e-mail.

Configuring Citrix

Access to a Citrix server can be enabled, allowing users to run applications hosted on the Citrix server. Citrix service is enabled in the policy group sub mode.

```
webvpn context webvpn_context
 policy group policy-group
   citrix enabled
```

A link to the Citrix server can be provided to the end user on the portal page by configuring it in a URL list.

Configuring Thin-Client Mode (TCP Port Forwarding)

Thin-client mode, also called TCP port forwarding, provides access for remote end users to client and server applications that communicate over known, fixed TCP ports. Each internal server and port number that the user can have access to has to be configured on the gateway. The entries specify the local port number and the destination server name and port number to use for TCP port forwarding.

Sample configuration configuring access to an internal mail server and Secure Shell (SSH) Protocol:

```
port-forward "portlist"
   local-port 30019 remote-server "ssh-server.domain.com" remote-port 22 description "SSH"
   local-port 30020 remote-server "email.domain.com" remote-port 143 description "IMAP"
   local-port 30021 remote-server "email.domain.com" remote-port 110 description "POP"
   local-port 30022 remote-server "email.domain.com" remote-port 25 description "SMTP"
```

The port forward list must be associated with the SSLVPN context by configuring it in the context's policy group:

```
webvpn context webvpn_context
```



```
 policy group policy-group
   port-forward “portlist”
```

Thin-client mode requires Sun Microsystems Java Runtime Environment (JRE) to be installed on the client PC. In thin-client mode, the user has to download a Java applet by clicking on the “Start application access” link provided in the portal page. An application access window will pop up, showing a list of servers the user has access to. The client can then use any available application to connect to the listed servers. In this example, the user can use any e-mail client and SSH client to connect to the available servers.

Configuring SSLVPN Tunneling Client (Full-Tunnel Mode)

To get access in the full-tunnel mode, a SSL VPN client is downloaded on the client PC. Before the client PC can download this client, the SSL VPN client package must be installed on the internal flash device on the SSLVPN gateway.

Configuration example:

```
service internal
webvpn install svc flash:sslclient-win-1.0.2.127.pkg
```

In full-tunnel mode, the SSLVPN gateway supplies an IP address to each of the clients logged into the gateway. A local IP address pool must be configured on the gateway, and this pool must be specified in the policy group configuration for the SSLVPN context that allows full-tunnel mode access.

Configuring the IP address pool:

```
ip local pool webvpn-pool 10.1.1.2 10.1.1.62
```

Full-tunnel mode must be enabled in the SSLVPN context by configuring it in the context’s policy group. Split tunneling can also be configured to specify which traffic should be tunneled to the internal network, and which traffic should be sent directly to the Internet.

```
webvpn context webvpn_context
 policy group policy-group
   functions svc-enabled
   svc address-pool “webvpn-pool”
   svc split include 10.0.0.0 255.0.0.0
   svc split include 192.168.0.0 255.255.0.0
   svc dns-server primary 10.2.2.2
```

When the end user logs into an SSLVPN gateway domain that has full-tunnel mode enabled, the SSL VPN client is automatically downloaded and installed on the end-user PC. The routing table on the PC is modified to route the internal traffic to the internal network, and all other traffic directly to the Internet.

Configuring Cisco Secure Desktop

Cisco Secure Desktop eliminates all traces of sensitive data by providing a single, secure location for session activity and removal on the client system. Cisco Secure Desktop helps ensure that cookies, browser history, temporary files, and downloaded content are removed from the system after a remote user has logged out or after an SSLVPN session has timed out.

First, the Cisco Secure Desktop package must be installed on the internal flash device on the SSLVPN gateway, then Cisco Secure Desktop can be enabled in the context sub mode.

Installing the Cisco Secure Desktop package:

```
service internal
webvpn install csd flash: securedesktop-3.0.2.278-K9.pkg
```

Configuring Cisco Secure Desktop in a context:

```
webvpn context webvpn-context
 csd enable
```

Before the client can use the Cisco Secure Desktop feature, the Cisco Secure Desktop Manager must be launched to configure settings for the context in which Cisco Secure Desktop was enabled. This is done by going to https://<gateway-ip>/csd_admin, and logging in as "admin" with the enable password configured on the SSLVPN gateway.

Using the Cisco Secure Desktop Manager, you can configure the VPN feature policies to use for remote users at different locations. Access can be differentiated based on IP address, certificate, and file and registry information. System detection can also be done before giving the user access to the SSLVPN features.

More details on configuring Cisco Secure Desktop Manager can be found in the Cisco Secure Desktop Configuration Guide:

http://www.cisco.com/en/US/products/ps6742/tsd_products_support_series_home.html

When the end user navigates to an SSLVPN gateway domain that has Cisco Secure Desktop enabled, the secure desktop is installed on the end-user PC. Once the desktop is installed, the user can go to the secure desktop and log in to create an SSLVPN session. Depending on the access configured in the SSLVPN context specified for this domain, the user can get clientless, thin-client, or full-tunnel client access to the internal network. The user can also switch between the secure desktop and the guest computer (regular desktop) by clicking in the respective icon/menu option.

TROUBLESHOOTING

The following section describes the troubleshooting commands available.

SSLVPN Troubleshooting Commands

To help troubleshooting possible problems, the following debug commands can be used

- **debug webvpn aaa** **AAA debugs**
- **debug webvpn cifs** **CIFS debugs**
- **debug webvpn citrix** **Citrix debugs**
- **debug webvpn cookie** **cookie debugs**
- **debug webvpn count** **data count code debugs**
- **debug webvpn csd** **Cisco Secure Desktop debugs**
- **debug webvpn data** **data code debugs**
- **debug webvpn dns** **DNS debugs**
- **debug webvpn emweb** **emweb debugs**
- **debug webvpn emweb state** **emweb state debugs**
- **debug webvpn http** **HTTP debugs**
- **debug webvpn package** **client package debugs**
- **debug webvpn port-forward** **port-forward debugs**
- **debug webvpn sdps** **Shim Data Path debugs**
- **debug webvpn sock** **Socket Layer debugs**
- **debug webvpn sock flow** **Socket async flow debugs**
- **debug webvpn timer** **timer code debugs**
- **debug webvpn trie** **trie code debugs**
- **debug webvpn tunnel** **tunnel debugs**
- **debug webvpn tunnel detail** **Detailed display of tunnel transactions**
- **debug webvpn tunnel traffic** **Tunnel data packets debugs**
- **debug webvpn url_disp** **URL disp code debugs**
- **debug webvpn webservice** **web service debugs**
- **debug webvpn** **basic debugs**

Note: Enabling debug commands affects performance, and enabling multiple debug commands at the same time will make the gateway very slow.

Sessions can be monitored on the SSLVPN gateway using the following show commands:

- **show webvpn context**

```
webvpn-gateway#show webvpn context
Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host
```



```
Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      up    up
csd                 webvpn-g csd               -        up    up
tunnel              webvpn-g tunnel            -        up    up
```

- **show webvpn context <context-name>**

```
webvpn-gateway#show webvpn context Default_context
Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authentication Domain not configured
Default Group Policy: default
Not associated with any WebVPN Gateway
Domain Name and Virtual Host not configured
Maximum Users Allowed: 10000 (default)
NAT Address not configured
VRF Name not configured
```

- **show webvpn gateway**

```
webvpn-gateway#show webvpn gateway
Gateway Name                      Admin  Operation
------------                      -----  ---------
webvpn-gw                         up     up
webvpn-gateway                    down   down
```

- **show webvpn gateway <gateway-name>**

```
webvpn-gateway#show webvpn gateway webvpn-gw
Admin Status: up
Operation Status: up
IP: 10.10.10.30, port: 443
SSL Trustpoint: SSLVPN
```

- **show webvpn install package csd**
  - Displays all the installed csd files
- **show webvpn install package svc**
  - Displays all the installed svc files
- **show webvpn install status csd**

```
webvpn-gateway#show webvpn install status csd
SSLVPN Package Cisco-Secure-Desktop version installed:
CISCO CSD CAT6K
3,1,0,9
Fri 07/22/2005 10:49:35.07 b
```


- **show webvpn install status svc**

```
webvpn-gateway#show webvpn install status svc
SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43 D
```

- **show webvpn nbns context all**

```
webvpn-gateway#show webvpn nbns context all
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
```

- **show webvpn policy group <policy-name> context all**

```
webvpn-gateway#show webvpn policy group csdpolicy context all
WEBVPN: group policy = csdpolicy ; context = csd
      url list name = “cisco-list”
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = “portlist”
      nbns list name = “cifs-servers”
      functions = file-access file-browse file-entry svc-enabled
      citrix enabled
      address pool name = “webvpn-pool”
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
      split include = 10.0.0.0 255.0.0.0
      split include = 192.168.0.0 255.255.0.0
      DNS primary server = <dns-server>
```

- **show webvpn session context <context-name>**
  - Shows current session information for a specific context.
- **show webvpn session context all**
  - Shows current session information for all contexts
- **show webvpn session user <username>**
  - Shows current session information for a specified user

- **show webvpn stats cifs**
  - Shows SSLVPN CIFS statistics
- **show webvpn stats citrix**
  - Shows SSLVPN Citrix statistics
- **show webvpn stats context <context-name>**
  - Shows all statistics for an SSLVPN context
- **show webvpn stats detail**
  - Shows detailed SSLVPN statistics
- **show webvpn stats mangle**
  - Shows SSLVPN URL mangling statistics
- **show webvpn stats port-forward**
  - Shows SSLVPN port-forward statistics
- **show webvpn stats socket**
  - Shows SSLVPN socket statistics
- **show webvpn stats tunnel**
  - Shows SSLVPN tunnel statistics

Clear commands are available that will clear the NBNS cache, clear the SSLVPN sessions, and clear the statistics:

- clear webvpn nbns
- clear webvpn session
- clear webvpn stats

APPENDIX A: FULL CONFIGURATION FOR SSLVPN

This configuration shows a full SSLVPN configuration.

```
hostname sslvpn-gateway
!
aaa new-model
!
aaa group server radius ssl-users
 server-private <server ip> auth-port 1812 acct-port 1813 key <aaa-key>
!
aaa authentication login default local group ssl-users
!
aaa session-id common
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
!
```



```
ip domain name cisco.com
ip host sslvpn-gateway.cisco.com <server ip>
ip name-server <server ip>
!
crypto pki trustpoint SSLVPN
 enrollment url http://ca-server:80
 serial-number none
 fqdn sslvpn-gateway.cisco.com
 ip-address none
 subject-name CN=sslvnp-gateway.cisco.com
 revocation-check crl
!
crypto pki certificate chain SSLVPN
 certificate <removed>
 certificate ca <removed>
!
interface GigabitEthernet0/0
 ip address 10.10.10.30 255.255.255.240
 duplex full
 speed 100
 media-type rj45
 negotiation auto
!
!
ip classless
ip local pool webvpn-pool 10.10.10.50 10.10.10.100
ip route 0.0.0.0 0.0.0.0 10.10.10.40
!
!
no ip http server
no ip http secure-server
ip http authentication aaa
!
!
line con 0
 exec-timeout 300 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 session-timeout 15
 exec-timeout 300 0
 password <password>
 transport input ssh
!
scheduler allocate 20000 1000
```



```
ntp clock-period 17179207
ntp server <ntp-server-ip>
!
webvpn gateway webvpn-gw
 ip address 10.10.10.30 port 443
 ssl trustpoint SSLVPN
 inservice
 !
webvpn install svc flash:/webvpn/svc.pkg
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context Default_context
 title “WebVPN BETA TESTING”
 ssl encryption
 ssl authenticate verify all
 !
 url-list “cisco-list”
   heading “Cisco”
   url-text “OWA” url-value “owa.cisco.com”
   url-text “Home” url-value “www.cisco.com”
!
 url-list “Citrix”
   heading “Citrix”
   url-text “Citrix Server” url-value “http://<citrix-server”
 !
 nbns-list cifs-servers
   nbns-server <nbns-server1>
   nbns-server <nbns-server2>
 login-
message “UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit
permission to access  this device. All activities performed on this device are logged and
violations of this policy may result in disciplinary action.”
 !
 port-forward “portlist”
   local-port 30019 remote-server ssh-server remote-port 22 description “SSH”
   local-port 30020 remote-server mailserver remote-port 143 description “IMAP”
   local-port 30021 remote-server mailserver remote-port 110 description “POP”
   local-port 30022 remote-server mailserver remote-port 25 description “SMTP”
 !
 policy group default
   url-list “cisco-list”
   port-forward “portlist”
   nbns-list “cifs-servers”
   functions file-access
   functions file-browse
   functions file-entry
```



```
    citrix enabled
 default-group-policy default
 inservice
!
!
webvpn context csd
 ssl encryption
 ssl authenticate verify all
 !
 url-list “cisco-list”
   heading “Cisco”
   url-text “OWA” url-value “owa.cisco.com”
   url-text “Home” url-value “www.cisco.com”
 !
 nbns-list cifs-servers
   nbns-server <nbns-server1>
   nbns-server <nbns-server2>
 login-
message “UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit
permission to access  this device. All activities performed on this device are logged and
violations of this policy may result in disciplinary action.”
 !
 port-forward “portlist”
   local-port 30019 remote-server ssh-server remote-port 22 description “SSH”
   local-port 30020 remote-server mailserver remote-port 143 description “IMAP”
   local-port 30021 remote-server mailserver remote-port 110 description “POP”
   local-port 30022 remote-server mailserver remote-port 25 description “SMTP”
 !
 policy group csdpolicy
   url-list “cisco-list”
   port-forward “portlist”
   nbns-list “cifs-servers”
   functions file-access
   functions file-browse
   functions file-entry
   functions svc-enabled
   svc address-pool “webvpn-pool”
   svc split include 10.0.0.0 255.0.0.0
   svc split include 20.0.0.0 255.255.0.0
   svc dns-server primary 171.68.226.120
   citrix enabled
 default-group-policy csdpolicy
 gateway webvpn-gw domain csd
 csd enable
 inservice
!
end
```


APPENDIX B: CERTIFICATE MANAGEMENT

The SSLVPN server can be deployed with a certificate issued by an in-house certificate server or by a public trusted certificate server (such as Verisign). If an in-house certificate server is used, the web browsers will prompt users to accept the certificate every time a session is established to the SSLVPN gateway, until the root certificate is permanently installed into the browser's trusted root store. This can be avoided if a certificate issued by a public root is used. Most of the well-known public roots are already packaged with the prominent browsers such as Internet Explorer, Mozilla, etc.

If users are using non-PC based platforms (PDAs, for example), using a public root becomes even more useful since the PDA browsers don't have an option to install certificates.

Configuration

Note: Before doing any certificate-related configuration, make sure that the router's clock and time zone is accurately configured.

Configuration for Offline Enrollment

```
crypto pki trustpoint myca
 enrollment terminal
 fqdn none
 subject-name cn=webvpn.mydomain.com,o=The Company,c=US,st=California
 revocation-check crl
 rsakeypair webvpn.mydomain.com
```

The RSA keypair name and common name in the subject-name should match the actual URL used for connecting to the SSLVPN gateway. If there is a mismatch, the web browsers will issue a warning, and the users will be prompted to accept the certificate.

Configuration for SCEP

The below sample is for a Microsoft Certificate Server.

```
crypto pki trustpoint myca
 enrollment mode ra
 enrollment url http://my-ca:80/certsrv/mscep/mscep.dll
 fqdn none
 serial-number
 subject-name cn=webvpn.mydomain.com,o=The Company
 revocation-check crl
 rsakeypair webvpn.mydomain.com
```

Generating an RSA Key Pair

RSA keys must be generated using the actual URL used for connecting to the SSLVPN gateway as the name.

```
webvpn-gateway(config)#crypto key generate rsa general-keys label webvpn.mydomain.com
modulus 1024
The name for the keys will be: webvpn.mydomain.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
```

The RSA keys can be generated as exportable or non-exportable. Appending the exportable keyword to the command above will generate exportable RSA keys.

Exportable RSA keys should be carefully evaluated before use because using exportable RSA keys introduces the risk that these keys might be exposed. The advantage of using exportable keys is that in case of hardware failure, the gateway can be easily replaced with a new router, and the keys and certificates can be imported from backup. However, the saved backup copy of the keys has to be kept very safe.

Non-exportable keys cannot be copied from the gateway, but in case of "write erase," flash corruption, or hardware failure, the certificates are lost. In this case, new certificates must be generated, and the user has the overhead of contacting the certificate vendor for new certificates, possibly at extra cost. If an in-house certificate authority (CA) server is used, this is not a big issue.

Installing an In-House Certificate

If the certificate server supports Simple Certificate Enrollment Protocol (SCEP), the certificate can be requested from the CA server using the following command:

```
webvpn-gateway(config)#crypto pki authenticate myca
Certificate has the following attributes:
       Fingerprint MD5: 1CB6EDEA 204E5336 6FE33243 C3381FF51
      Fingerprint SHA1: D91C23DB 7A04D176 F1332E3E 1F234837 63132D30

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

The certificate can then be enrolled, and the CA will send a signed certificate:

```
webvpn-gateway(config)#cry pki enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: webvpn.mydomain.com
% The serial number in the certificate will be: 00E2C3D1
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate myca verbose' command will show the fingerprint.
```

If the certificate server does not support SCEP, an offline method needs to be used as explained in the next section.

Installing Certificate Issued by Public Certificate Authority

Usually the public certificate authorities use a web-based or e-mail-based certificate enrollment mechanism.

Generating the CSR File

Whether the offline enrollment method is e-mail or web, the steps on the router are the same. First, a certificate signing request (CSR) needs to be generated. The CSR can be generated only after the corresponding RSA keypair and trustpoint is configured. Once the CSR is

generated, issue the command to enrollment. Authentication is not necessary at this time. It may not be known from which certificate server the certificate is going to be issued. One vendor can operate multiple certificate servers. If it is known, authentication can be performed after downloading the root certificate. If not, wait to authenticate until the certificate is issued.

The enrollment request will display the CSR on the router console as below. Copy only the base64-encoded portion and save it in a text file with .csr extension. Some vendors may need it to be enclosed in "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" lines. Following is a sample CSR generation:

```
test-router(config)#crypto pki enroll myca
% Start certificate enrollment ..

% The subject name in the certificate will include: cn=test
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIIBgDCB6gIBADAPMQ0wCwYDVQQDEwR0ZXN0MIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQDZR9FGP8ZoFBhv3EzziW7o5pJRwnen4H1Ha4n0vWGYo1+tNz915laO
rWUDk/3TqomYXykCx0U04Maec+jKhSbqy9fypp+Hvf7qEKcf2XlkXnWT7bHcIcpw
EKzOSwaOni+kagQF9Qu2+lKP59RoikEqTtqIVqqQlNGDKG+rSFc75wIDAQABoDIw
DwYJKoZIhvcNAQkHMQITADAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIF
oDANBgkqhkiG9w0BAQQFAAOBgQBFEsbPnLqHj83TMX3bSZjOz+EVWLSHXYJQgvdU
S5S3UtgCoWsalmttY5rZ+qafRwQxEE39zvOX9XnalZDgMt5+QxyZSzbu+3Nllmv7
+z5clhPFbnCW9MZrIEDkwzgniGmPB91jUfUTyoN6FTRlLTpyXVj/iOKPiljUPXOR
TZzUVA==

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
test-router(config)#
```


The resulting CSR file (myca.csr) will look like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBgDCB6gIBADAPMQ0wCwYDVQQDEwR0ZXN0MIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQDZR9FGP8ZoFBhv3EzziW7o5pJRwnen4H1Ha4n0vWGYo1+tNz915laO
rWUDk/3TqomYXykCx0U04Maec+jKhSbqy9fypp+Hvf7qEKcf2XlkXnWT7bHcIcpw
EKzOSwaOni+kagQF9Qu2+lKP59RoikEqTtqIVqqQlNGDKG+rSFc75wIDAQABoDIw
DwYJKoZIhvcNAQkHMQITADAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIF
oDANBgkqhkiG9w0BAQQFAAOBgQBFEsbPnLqHj83TMX3bSZjOz+EVWLSHXYJQgvdU
S5S3UtgCoWsalmttY5rZ+qafRwQxEE39zvOX9XnalZDgMt5+QxyZSzbu+3Nllmv7
+z5clhPFbnCW9MZrIEDkwzgniGmPB91jUfUTyoN6FTRlLTpyXVj/iOKPiljUPXOR
TZzUVA==
-----END CERTIFICATE REQUEST-----
```

The user will now have to send this CSR to the certificate vendor by e-mail or the Internet. The vendor will return the signed certificate as a text file in base64-encoded format. Make sure that the vendor sends all the files encoded in base64; these files will usually have a .cer extension. The vendor may also provide the corresponding root certificate in the same format. If the root certificate is not provided, it can be easily exported from a standard web browser. First, open the issued certificate and look at the “issued by” field. Opening the certificate is as simple as double clicking on the .cer file on a Windows platform. Once the issuer is identified, open the root certificate store of the browser and look for the certificate of the issuer. Once it is located, export it as a .cer file.

The next step is authenticating and loading the enrolled certificate on the SSLVPN router.

Loading the Root Certificate

To load the root certificate (authentication), issue the **crypto pki authenticate <trust point>** command and paste the content of the root certificate file. Then type **quit** on a new line or simply press the “Enter” key on a new line.

```
test-router(config)#crypto pki authenticate myca

Enter the base 64 encoded CA certificate.
End with a blank line or the word “quit” on a line by itself
-----BEGIN CERTIFICATE-----
<certificate content here>
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
       Fingerprint MD5: <actual finger print>
      Fingerprint SHA1: <actual finger print>

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

test-router(config)#
```


Loading the Router Certificate

Now the certificate issued by the vendor needs to be installed on the SSLVPN router. This is the certificate identifying the server; it will be presented to SSLVPN clients during SSL negotiation. The command is **crypto pki import <trustpoint name> certificate**. Paste the certificate file content followed by a **quit** or blank line.

```
test-router(config)#crypto pki import myca certificate
% The fully-qualified domain name will not be included in the certificate

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself

-----BEGIN CERTIFICATE-----
<paste the certificate content here>
-----END CERTIFICATE-----

% Router Certificate successfully imported

test-router(config)#
```

Now the router is ready to function as a SSLVPN server.

APPENDIX C: CLIENT ACCESS RESTRICTION

This section explains how to restrict access to SSLVPN full-tunnel mode based on the antivirus software and operating system on the client end host system.

Configure Using Cisco Secure Desktop

Cisco Secure Desktop has a mechanism for restricting access to SSLVPN full-tunnel mode based on the existence of antivirus software and operating system on the client PC. These access criteria are configured in the Cisco Secure Desktop admin page.

To enable the checking for antivirus software and OS version, Cisco Secure Desktop and full-tunnel mode should be configured on the SSLVPN gateway for a virtual context.

To configure, log into https://<webvpn-gateway>/csd_admin, and select the correct virtual context.

Go to the VPN Feature Policy under the location you are configuring the access for.

Select “ON if criteria are matched” for full tunneling and click on the “…” button.

This pops up a window where the criteria can be configured. Select the appropriate antivirus software and OS version, and save your changes.

A client who logs in from a PC that does not match the OS and antivirus criteria will not be able to establish a SSLVPN tunnel to the gateway.

Configure Using Network Access Control

The Cisco IOS Software NAC feature helps ensure that only computers with up-to-date antivirus program and operating system updates can get SSLVPN tunnel access to the corporate network. This requires the Cisco Trust Agent to be installed on the computer. If the Cisco trust agent is not installed access will be denied and no further information will be given.

The Cisco Trust Agent collects the OS type, OS version, antivirus version, and antivirus data files version and passes it on to the NAC router. The NAC router forwards this information to the RADIUS server, which validates the data. Only when the information has been validated will the machine be given complete access; otherwise, access will be denied. If this is the case, a user trying to access any url inside the corporate network will be redirected to a page that will tell him what to do to get his system to comply with the access rules.

This scenario requires a NAC router installed between the SSLVPN gateway and the corporate network. No additional configuration is required on the SSLVPN gateway to use this feature.

NAC configuration:

```
aaa new-model
aaa group server radius nac
 server-private x.x.x.x auth-port y acct-port z key 0 <key>
 ip radius source-interface Ethernet0
!
aaa authentication eou default group nac
aaa authorization network default group nac
!
ip admission name stealth_nac eapoudp list nac_acl
!
! Allow IP phone
identity profile eapoudp
 device authorize type cisco ip phone policy ip_phone
identity policy ip_phone
 access-group nac_ip_phone_acl
!
! Allow clientless devices
eou allow clientless
eou timeout status-query 30
eou timeout revalidation 18000
! Enable logging of NAC messages
eou logging
!
interface Ethernet0
ip access-group nac_inbound_acl in
ip admission stealth_nac
!
ip http server
ip http secure-server
ip http authentication aaa
ip http client source-interface Ethernet0
!
```



```
ip access-list extended nac_acl
remark --- NAC qualifying ACL ---
deny udp any any eq domain
deny udp any any eq netbios-ns
deny udp any any eq netbios-dgm
! Deny lines are used to bypass NAC
permit ip any 10.10.10.0 0.0.255
! NAC will intercept the access matching the permit lines
! Use “permit ip any any” if all access needs to be tested for NAC
deny ip any any
!
ip access-list extended nac_inbound_acl
remark --- NAC Inbound ACL -----------
permit udp any any eq domain
permit udp any any eq netbios-ns
permit udp any any eq netbios-dgm
permit ip any host <ip address of Ethernet0>
! Above line is needed to permit EAPoUDP protocol.
! It also helps local administration.
deny ip any 10.10.10.0 0.0.255
! Above lines are for the traffic which should be blocked
permit ip any any
! Permit lines allow traffic which need not be NAC tested.
!
radius-server vsa send authentication
```


Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C07-372106-00 10/06