



Secure Sockets Layer Virtual Private Network (SSL VPN)

The Secure Sockets Layer Virtual Private Network (SSL VPN) feature provides support in the Cisco IOS software for remote user access to enterprise networks from anywhere on the internet. Remote access is provided through a Secure Socket Layer-enabled (SSL-enabled) SSL VPN gateway. The SSL VPN gateway allows remote users to establish a secure VPN tunnel. The SSL VPN feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using original HTTP over SSL (HTTPS) browser support through the full-tunnel client support.

- [Prerequisites for SSL VPN, on page 1](#)
- [Restrictions for SSL VPN, on page 1](#)
- [Information About SSL VPN, on page 2](#)
- [How to Configure SSL VPN, on page 4](#)
- [Configuration Examples for SSL VPN, on page 18](#)
- [Additional References for SSL VPN, on page 20](#)
- [Feature Information for SSL VPN, on page 21](#)

Prerequisites for SSL VPN

To securely access resources on a private network behind an SSL VPN gateway, the remote user of an SSL VPN service must have the following:

- An account (login name and password).
- Support for full tunnel mode using Cisco AnyConnect client.
- Administrative privileges to install Cisco AnyConnect client.

Restrictions for SSL VPN

- ACLs do not support DENY statements.
- Using Cisco AnyConnect VPN, if you create tunnels at a high bring-up rate, a failure might occur. When creating a large number of VPN SSL sessions, for example, 1000, use a bring-up rate of 15 TPS or lower. If you use a higher TPS rate, a failure might occur.

- SSLVPN Peer Detection (PD) is supported only with AnyConnect client Version 3.x and later.

Information About SSL VPN

SSL VPN Overview

Cisco IOS XE SSL VPN is a router-based solution offering SSL VPN remote-access connectivity integrated with industry-leading security and routing features on a converged data, voice, and wireless platform. The security is transparent to end users and is easy to administer. With Cisco IOS XE SSL VPN, end users gain access securely from home or any internet-enabled location such as wireless hotspots. Cisco IOS XE SSL VPN also enables companies to extend corporate network access to offshore partners and consultants, keeping corporate data protected all the while. Cisco IOS XE SSL VPN, in conjunction with the dynamically downloaded Cisco AnyConnect VPN client, provides remote users with full network access to virtually any corporate application.

SSL VPN delivers the following three modes of SSL VPN access, of which only tunnel mode is supported in Cisco IOS XE software:

- **Clientless:** Clientless mode provides secure access to private web resources and to web content. This mode is useful for accessing most content that you would expect to access in a web browser, such as internet access, databases, and online tools that use a web interface.
- **Thin Client (port-forwarding Java applet):** Thin client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH).
- **Full-Tunnel Mode:** Full-tunnel client mode offers extensive application support through its dynamically downloaded Cisco AnyConnect VPN client (next-generation SSL VPN client) for SSL VPN. Full-tunnel client mode delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that provides network layer access to virtually any application.



Note SSL VPN will not work if `ip http secure-server` is enabled.

This feature is supported on the following platforms:

Platform	Supported Cisco IOS XE Release
Cisco Cloud Services Router 1000V Series	Cisco IOS XE Release 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 Integrated Services Router	Cisco IOS XE Cupertino 17.7.1a
Cisco 4451 Integrated Services Router	
Cisco 4431 Integrated Services Router	

Remote Access Modes

In a typical clientless remote access scenario, remote users establish an SSL tunnel to move data to and from the internal networks at the application layer, for example, web and email. In tunnel mode, remote users use an SSL tunnel to move data at the network (IP) layer. Therefore, tunnel mode supports most IP-based applications. Tunnel mode supports many popular corporate applications, for example, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet.

SSL VPN support that is provided by full-tunnel mode is as follows:

- Works like clientless IPsec VPN
- Tunnel client loaded through Java or ActiveX
- Application agnostic; supports all IP-based applications
- Scalable
- Local administrative permissions required for installation

Full-tunnel client mode offers extensive application support through its dynamically downloaded Cisco AnyConnect VPN client (next-generation SSL VPN client) for SSL VPN. Full-tunnel client mode delivers a lightweight, centrally configured, and easy-to-support SSL VPN tunneling client that provides network layer access to virtually any application. The advantage of SSL VPN comes from its accessibility from almost any internet-connected system without needing to install additional desktop software. Cisco SSL AnyConnect VPN allows remote users to access enterprise networks on the internet through an SSL VPN gateway. During the establishment of the SSL VPN with the gateway, the Cisco AnyConnect VPN client is downloaded and installed on the remote user equipment (laptop, mobile, PDA, and so on). The tunnel connection is established when a remote user logs into the SSL VPN gateway. The tunnel connection is determined by the group policy configuration. By default, the Cisco AnyConnect VPN client is removed from the client PC after the connection is closed. However, you have the option to keep the Cisco AnyConnect VPN client installed on the client equipment.

Cisco SSL AnyConnect VPN easily accesses the services within the company's network and simplifies the VPN configuration on the SSL VPN gateway, thereby reducing the overhead for system administrators.

SSL VPN CLI Constructs

SSL Proposal

SSL proposal specifies the cipher suites that are supported. Each cipher suite defines a key exchange algorithm, a bulk encryption algorithm, and a MAC algorithm. One of the cipher suites that is configured would be chosen from the client's proposal during SSL negotiation. If the intersection between a client's proposed suites and configured suites is a null set, the negotiation terminates. Ciphers are currently selected based on the client's priority.

The SSL proposal is used in SSL handshake protocol for negotiating encryption and decryption. The default SSL proposal is used with SSL policy in the absence of any user-defined proposal. The default proposal has ciphers in the order shown here:

```
protection rsa-aes256-sha1 rsa-aes128-sha1 rsa-3des-ede-sha1 rsa-3des-ede-sha1
```

SSL Policy

SSL policy defines the cipher suites to be supported and the trust point to be used during SSL negotiation. SSL policy is a container of all the parameters used in the SSL negotiation. The policy selection is done by matching the session parameters against the parameters configured under the policy. There is no default policy. Every policy is associated with a proposal and a trustpoint.

SSL Profile

The SSL VPN profile defines authentication and accounting lists. A profile selection depends on policy and URL values. Profile may, optionally, be associated with a default authorization policy.

The following rules apply:

- The policy and URL must be unique for an SSL VPN profile.
- At least one authorization method must be specified to bring up the session.
- The three authorization types, namely user, group and cached can coexist.
- There is no default authorization.
- The order of precedence for authorization is user authorization, cache authorization, and group authorization. If group authorization override is configured, the order of precedence is group authorization, user authorization, and cache authorization.

SSL Authorization Policy

The SSL authorization policy is a container of authorization parameters that are pushed to a remote client and are applied either locally on the virtual-access interface, or globally on the device. The authorization policy is referred from the SSL VPN profile.

SSL VPN MIB

The SSL VPN MIB represents the Cisco implementation-specific attributes of a Cisco entity that implements SSL VPN. The MIB provides operational information in Cisco's SSL VPN implementation by managing the SSL VPN, trap control, and notification groups. For example, the SSL VPN MIB provides the number of active SSL tunnels on the device.

How to Configure SSL VPN

The following sections provide information about the various tasks involved in configuring SSL VPN.

Configuring an SSL Proposal

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ssl proposal *proposal-name***

4. **protection**
5. **end**
6. **show crypto ssl proposal** [*proposal name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	crypto ssl proposal <i>proposal-name</i> Example: Device(config)# crypto ssl proposal proposal1	Defines an SSL proposal name, and enters crypto SSL proposal configuration mode.
Step 4	protection Example: Device(config-crypto-ssl-proposal)# protection rsa-3des-ede-sha1 rsa-aes128-sha1	Specifies one or more cipher suites that are as follows: <ul style="list-style-type: none"> • rsa-3des-ede-sha1 • rsa-aes128-sha1 • rsa-aes256-sha1 • rsa-rc4128-md5
Step 5	end Example: Device(config-crypto-ssl-proposal)# end	Exits SSL proposal configuration mode and returns to privileged EXEC mode.
Step 6	show crypto ssl proposal [<i>proposal name</i>] Example: Device# show crypto ssl proposal	(Optional) Displays the SSL proposal.

Configuring an SSL Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ssl policy** *policy-name*
4. **ip address local** *ip-address* [*vrf vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*]

5. **ip interface local** *interface-name* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*]
6. **pki trustpoint** *trustpoint-name* **sign**
7. **ssl proposal** *proposal-name*
8. **no shut**
9. **end**
10. **show crypto ssl policy** [*policy-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	crypto ssl policy <i>policy-name</i> Example: Device(config)# crypto ssl policy policy1	Defines an SSL policy name and enters SSL policy configuration mode.
Step 4	ip address local <i>ip-address</i> [vrf <i>vrf-name</i>] [port <i>port-number</i>] [standby <i>redundancy-name</i>] Example: Device(config-crypto-ssl-policy)# ip address local 10.0.0.1 port 446	Specifies the local IP address to start the TCP listener. Note Running this command or the ip interface local command is mandatory.
Step 5	ip interface local <i>interface-name</i> [vrf <i>vrf-name</i>] [port <i>port-number</i>] [standby <i>redundancy-name</i>] Example: Device(config-crypto-ssl-policy)# ip interface local FastEthernet redundancy1	Specifies the local interface to start the TCP listener. Note Running this command or the ip address local command is mandatory.
Step 6	pki trustpoint <i>trustpoint-name</i> sign Example: Device(config-crypto-ssl-policy)# pki trustpoint tp1 sign	(Optional) Specifies the trustpoint to be used to send the server certificate during an SSL handshake. Note If this command is not specified, a default self-signed trustpoint is used. If there is no default self-signed trustpoint, the system creates a default self-signed certificate.
Step 7	ssl proposal <i>proposal-name</i> Example: Device(config-crypto-ssl-policy)# ssl proposal pr1	(Optional) Specifies the cipher suites to be selected during an SSL handshake. Note If a proposal is not specified, the default proposal is used.

	Command or Action	Purpose
Step 8	no shut Example: Device(config-crypto-ssl-policy)# no shut	Starts the TCP listener based on the configuration.
Step 9	end Example: Device(config-crypto-ssl-policy)# end	Exits SSL policy configuration mode and returns to privileged EXEC mode.
Step 10	show crypto ssl policy [<i>policy-name</i>] Example: Device# show crypto ssl policy	(Optional) Displays the SSL policies.

Configuring an SSL Profile

Before you begin

For details of AAA configuration, see the [Authentication Authorization and Accounting Configuration Guide](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ssl profile** *profile-name*
4. **aaa accounting user-pass list** *list-name*
5. **aaa authentication user-pass list** *list-name*
6. **aaa authorization group** [**override**] **user-pass list** *aaa-listname* *aaa-username*
7. **aaa authorization user user-pass** {**cached** | **list** *aaa-listname* *aaa-username*}
8. **match policy** *policy-name*
9. **match url** *url-name*
10. **no shut**
11. **end**
12. **show crypto ssl profile** [*profile-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	crypto ssl profile <i>profile-name</i> Example: Device(config)# crypto ssl profile profile1	Defines an SSL profile and enters SSL profile configuration mode.
Step 4	aaa accounting user-pass list <i>list-name</i> Example: Device(config-crypto-ssl-profile)# aaa accounting user-pass list list1	Specifies authentication, authorization, and accounting (AAA) method list.
Step 5	aaa authentication user-pass list <i>list-name</i> Example: Device(config-crypto-ssl-profile)# aaa authentication user-pass list list2	Specifies the AAA method list.
Step 6	aaa authorization group [override] user-pass list <i>aaa-listname</i> <i>aaa-username</i> Example: Device(config-crypto-ssl-profile)# aaa authorization group override user-pass list list1 user1	Specifies the AAA method list and username for group authorization. <ul style="list-style-type: none"> • group: Specifies group authorization. • override: (Optional) Specifies that attributes from group authorization should take precedence while merging attributes. By default, user attributes take precedence. • user-pass: Specifies the user password-based authorization. • aaa-listname: AAA method list name. • aaa-username: Username that must be used in the AAA request. Refers to the SSL authorization policy name defined on the device.
Step 7	aaa authorization user user-pass {cached list <i>aaa-listname</i> <i>aaa-username</i>} Example: Device(config-crypto-ssl-profile)# aaa authorization user user-pass list list1 user1	Specifies the AAA method list and username for user authorization. <ul style="list-style-type: none"> • user—Specifies user authorization. • user-pass— Specifies the user password-based authorization. • cached—Specifies that the attributes received during EAP authentication or obtained from the AAA preshared key must be cached. • aaa-listname—AAA method list name.

	Command or Action	Purpose
		<ul style="list-style-type: none"> <i>aaa-username</i>—Username that must be used in the AAA authorization request.
Step 8	match policy <i>policy-name</i> Example: Device(config-crypto-ssl-profile)# match policy policy1	Uses match statements to select an SSL profile for a peer based on the SSL policy name.
Step 9	match url <i>url-name</i> Example: Device(config-crypto-ssl-profile)# match url www.abc.com	Uses match statements to select an SSL profile for a peer based on the URL.
Step 10	no shut Example: Device(config-crypto-ssl-profile)# no shut	Specifies that profile cannot be shut until the policy specified in the match policy command is in use.
Step 11	end Example: Device(config-crypto-ssl-profile)# end	Exits SSL profile configuration mode and returns to privileged EXEC mode.
Step 12	show crypto ssl profile [<i>profile-name</i>] Example: Device# show crypto ssl profile	(Optional) Displays the SSL profile.

Configuring an SSL Authorization Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ssl authorization policy** *policy-name*
4. **banner** *banner-text*
5. **client profile** *profile-name*
6. **def-domain** *domain-name*
7. Run one of the following commands:
 - **dns** *primary-server* [*secondary-server*]
 - Or
 - **ipv6 dns** *primary-server* [*secondary-server*]
8. **dpd-interval** {**client** | **server**} *interval*
9. **homepage** *homepage-text*
10. **include-local-lan**
11. **ipv6 prefix** *prefix*

12. **keepalive** *seconds*
13. **module** *module-name*
14. **msie-proxy exception** *exception-name*
15. **msie-proxy option** {*auto* | *bypass* | *none*}
16. **msie-proxy server** {*ip-address* | *dns-name*}
17. **mtu** *bytes*
18. **netmask** *mask*
19. Run one of the following commands:
 - **pool** *name*
 - Or
 - **ipv6 pool** *name*
20. **rekey time** *seconds*
21. Run one of the following commands:
 - **route set access-list** *acl-name*
 - Or
 - **ipv6 route set access-list** *access-list-name*
22. **smartcard-removal-disconnect**
23. **split-dns** *string*
24. **timeout** {*disconnect seconds* | *idle seconds* | *session seconds*}
25. **wins** *primary-server* [*secondary-server*]
26. **end**
27. **show crypto ssl authorization policy** [*policy-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	crypto ssl authorization policy <i>policy-name</i> Example: Device(config)# crypto ssl authorization policy policy1	Specifies the SSL authorization policy and enters SSL authorization policy configuration mode.
Step 4	banner <i>banner-text</i> Example:	Specifies the banner. The banner is displayed after the successful setup of the tunnel.

	Command or Action	Purpose
	Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel. NOTE: DO NOT dial emergency response numbers (e.g. 911,112) from software telephony clients. Your exact location and the appropriate emergency response agency may not be easily identified.	
Step 5	<p>client profile <i>profile-name</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# client profile Employee</pre>	<p>Specifies the AnyConnect client profile. The profile must already be specified using the crypto vpn anyconnect profile command. See section Example: Specifying the AnyConnect Image and Profile, on page 18 for sample configuration of the AnyConnect image and profile.</p> <p>For details of AnyConnect configuration, see the Cisco AnyConnect Secure Mobility Client Administrator Guide.</p>
Step 6	<p>def-domain <i>domain-name</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# def-domain example.com</pre>	<p>Specifies the default domain. This parameter specifies the default domain that the client can use.</p>
Step 7	<p>Run one of the following commands:</p> <ul style="list-style-type: none"> • dns <i>primary-server</i> [<i>secondary-server</i>] • Or • ipv6 dns <i>primary-server</i> [<i>secondary-server</i>] <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100</pre> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2</pre>	<p>Specifies an IPv4-based or IPv6-based address for the primary and secondary Domain Name Service (DNS) servers.</p> <ul style="list-style-type: none"> • <i>primary-server</i>: IP address of the primary DNS server. • <i>secondary-server</i>: (Optional) IP address of the secondary DNS server.
Step 8	<p>dpd-interval {<i>client</i> <i>server</i>} <i>interval</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# dpd-interval client 1000</pre>	<p>Configures dead peer detection (DPD) globally for the client or server.</p> <ul style="list-style-type: none"> • client—DPD for the client mode. The default value is 300 (five minutes). • server—DPD for the server mode. The default value is 300 (five minutes). • <i>interval</i>—Interval, in seconds. The range is from 5 to 3600.
Step 9	<p>homepage <i>homepage-text</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com</pre>	<p>Specifies the SSL VPN home page URL.</p>

	Command or Action	Purpose
Step 10	include-local-lan Example: <pre>Device(config-crypto-ssl-auth-policy)# include-local-lan</pre>	Permits the remote user to access resources on a local LAN, such as a network printer.
Step 11	ipv6 prefix <i>prefix</i> Example: <pre>Device(config-crypto-ssl-auth-policy)# ipv6 prefix 64</pre>	Defines the IPv6 prefix for IPv6 addresses. <ul style="list-style-type: none"> • <i>prefix</i>—Prefix length. The range is from 1 to 128.
Step 12	keepalive <i>seconds</i> Example: <pre>Device(config-crypto-ssl-auth-policy)# keepalive 500</pre>	Enables setting the minimum, maximum, and default values, in seconds for keepalive.
Step 13	module <i>module-name</i> Example: <pre>Device(config-crypto-ssl-auth-policy)# module gina</pre>	Enables the server gateway to download the appropriate module for VPN to connect to a specific group. <ul style="list-style-type: none"> • dart—Downloads the AnyConnect Diagnostic and Reporting Tool (DART) module. • gina—Downloads the Start Before Logon (SBL) module.
Step 14	msie-proxy exception <i>exception-name</i> Example: <pre>Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2</pre>	The DNS name or the IP address specified in the <i>exception-name</i> argument that must not be sent through the proxy.
Step 15	msie-proxy option {<i>auto</i> <i>bypass</i> <i>none</i>} Example: <pre>Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass</pre>	Specifies the proxy settings for the Microsoft Internet Explorer browser. The proxy settings are required to specify an internal proxy server and to route the browser traffic through the proxy server when connecting to the corporate network. <ul style="list-style-type: none"> • auto—Browser is configured to auto detect proxy server settings. • bypass—Local addresses bypass the proxy server. • none—Browser is configured to not use the proxy server.
Step 16	msie-proxy server {<i>ip-address</i> <i>dns-name</i>} Example: <pre>Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2</pre>	The IP address or the DNS name, optionally followed by the port number of the proxy server. <p>Note This command is required if the msie-proxy option bypass command is specified.</p>

	Command or Action	Purpose
Step 17	<p>mtu <i>bytes</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# mtu 1000</pre>	<p>(Optional) Enables setting the minimum, maximum, and default MTU value.</p> <p>Note The value specified in this command overrides the default MTU specified in the Cisco AnyConnect Secure client configuration. If not specified, the value specified in the Cisco AnyConnect Secure client configuration is the MTU value. If the calculated MTU is less than the MTU specified in this command, this command is ignored.</p>
Step 18	<p>netmask <i>mask</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0</pre>	<p>Specifies the netmask of the subnet from which the IP address is assigned to the client.</p> <ul style="list-style-type: none"> • <i>mask</i>—Subnet mask address.
Step 19	<p>Run one of the following commands:</p> <ul style="list-style-type: none"> • pool <i>name</i> • Or • ipv6 pool <i>name</i> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# pool abc</pre> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool</pre>	<p>Defines a local IPv4 or IPv6 address pool for assigning IP addresses to the remote access client.</p> <ul style="list-style-type: none"> • <i>name</i>—Name of the local IP address pool. <p>Note The local IP address pool must already be defined using the ip local pool command.</p>
Step 20	<p>rekey time <i>seconds</i></p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# rekey time 1110</pre>	<p>Specifies the rekey interval, in seconds. The default value is 3600.</p>
Step 21	<p>Run one of the following commands:</p> <ul style="list-style-type: none"> • route set access-list <i>acl-name</i> • Or • ipv6 route set access-list <i>access-list-name</i> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# route set access-list acl1</pre> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1</pre>	<p>Establishes IPv4 or IPv6 routes the access list that must be secured through tunnels.</p> <ul style="list-style-type: none"> • <i>acl-name</i>—Access list name.
Step 22	<p>smartcard-removal-disconnect</p> <p>Example:</p> <pre>Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect</pre>	<p>Enables smartcard removal disconnect and specifies that the client should terminate the session when the smart card is removed.</p>

	Command or Action	Purpose
Step 23	split-dns <i>string</i> Example: <pre>Device(config-crypto-ssl-auth-policy)# split-dns example.com example.net</pre>	Allows you to specify up to ten split domain names, which the client should use for private networks.
Step 24	timeout { disconnect <i>seconds</i> idle <i>seconds</i> session <i>seconds</i> } Example: <pre>Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000</pre>	Specifies the timeout, in seconds. <ul style="list-style-type: none"> • disconnect <i>seconds</i>—Specifies the retry duration, in seconds, for Cisco AnyConnect client to reconnect to the server gateway. The default value is 0. • idle <i>seconds</i>—Specifies the idle timeout, in seconds. The default value is 1800 (30 minutes). • session <i>seconds</i>—Specifies the session timeout, in seconds. The default value is 43200 (12 hours).
Step 25	wins <i>primary-server</i> [<i>secondary-server</i>] Example: <pre>Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115</pre>	Specifies the internal Windows Internet Naming Service (WINS) server addresses. <ul style="list-style-type: none"> • <i>primary-server</i>—IP address of the primary WINS server. • <i>secondary-server</i>—(Optional) IP address of the secondary WINS server.
Step 26	end Example: <pre>Device(config-crypto-ssl-auth-policy)# end</pre>	Exits SSL authorization policy configuration mode and returns to privileged EXEC mode.
Step 27	show crypto ssl authorization policy [<i>policy-name</i>] Example: <pre>Device(config-crypto-ssl-auth-policy)# show crypto ssl authorization policy</pre>	(Optional) Displays the SSL authorization policy.

Verifying SSL VPN Configurations

This section describes how to use **show** commands to verify the SSL VPN configurations:

SUMMARY STEPS

1. **enable**
2. **show crypto ssl proposal** [*name*]
3. **show crypto ssl policy** [*name*]
4. **show crypto ssl profile** [*name*]
5. **show crypto ssl authorization policy** [*name*]
6. **show crypto ssl session** {**user** *user-name* | **profile** *profile-name*}
7. **show crypto ssl stats** [**profile** *profile-name*] [**tunnel**] [**detail**]

8. clear crypto ssl session {profile *profile-name*| user *user-name*}**DETAILED STEPS****Procedure****Step 1 enable****Example:**

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 show crypto ssl proposal [*name*]**Example:**

```
Device# show crypto ssl proposal
```

```
SSL Proposal: sslprop
Protection: 3DES-SHA1
```

Displays the SSL proposal.

Step 3 show crypto ssl policy [*name*]**Example:**

```
Device# show crypto ssl policy
```

```
SSL Policy: sslpolicy
Status      : ACTIVE
Proposal    : sslprop
IP Address  : 10.78.106.23
Port        : 443
fvrf       : 0
Trust Point: TP-self-signed-1183786860
Redundancy  : none
```

Displays the SSL policies.

Step 4 show crypto ssl profile [*name*]**Example:**

```
Device# show crypto ssl profile
```

```
SSL Profile: sslprofile
Status: ACTIVE
Match Criteria:
  URL: none
  Policy:
    sslpolicy
AAA accounting List      : local
AAA authentication List :none
AAA authorization cached :true
AAA authorization user List :default
AAA authorization user name: sslauth
AAA authorization group List :none
AAA authorization group name: none
```

Verifying SSL VPN Configurations

```

Authentication Mode      : user credentials
Interface                : SSLVPN-VIF1
  Status: ENABLE

```

Displays the SSL profile.

Step 5 **show crypto ssl authorization policy** [*name*]**Example:**

```
Device# show crypto ssl authorization policy
```

```

SSL Auth Policy: sslauth
V4 Parameter:
  Address Pool: SVC_POOL
  Netmask: 255.255.255.0
  Route ACL : split-include
Banner                : none
Home Page             : none
Idle timeout          : 300
Disconnect Timeout    : 0
Session Timeout       : 43200
Keepalive Interval    : 0
DPD Interval          : 300
Rekey
  Interval: 0
  Method : none
Split DNS              : none
Default domain        : none
Proxy Settings
  Server: none
  Option: NULL
  Exception(s): none
Anyconnect Profile Name :
SBL Enabled            : NO
MAX MTU                : 1406
Smart Card
Removal Disconnect     : NO

```

Displays the SSL authorization policy.

Step 6 **show crypto ssl session** {*user user-name* | *profile profile-name*}**Example:**

```
Device# show crypto ssl session user LAB
```

```

Session Type          : Full Tunnel
Client User-Agent     : AnyConnect Windows 3.0.08057

Username              : LAB                      Num Connection : 1
Public IP             : 10.163.209.245
Profile               : sslprofile              Policy Group    : sslauth
Last-Used             : 00:00:02                Created         : *00:58:44.219 PDT Thu Jul 25 2013
Session Timeout       : 43200                   Idle Timeout    : 300
DPD GW Timeout        : 300                     DPD CL Timeout  : 300
Address Pool          : sslvpn-pool             MTU Size        : 1406
Rekey Time            : 0                       Rekey Method    :
Lease Duration        : 43200
Tunnel IP             : 10.1.1.2                 Netmask         : 255.255.255.0
Rx IP Packets         : 0                       Tx IP Packets   : 125
CSTP Started          : 00:01:12                 Last-Received   : 00:00:02
CSTP DPD-Req sent     : 0                       Virtual Access  : 0
Msie-ProxyServer      : None                   Msie-PxyPolicy  : Disabled
Msie-Exception        :

```



```
Client Ports      : 34552
```

```
Device# show crypto ssl session profile sslprofile
```

```
SSL profile name: sslprofile
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
LAB                10.163.209.245    1                00:00:33 00:00:00
Error receiving show session info from remote cores
```

Displays SSL VPN session information.

Step 7 **show crypto ssl stats** [*profile profile-name*] [*tunnel*] [*detail*]

Example:

```
Device# show crypto ssl stats
```

```
SSLVPN Global statistics:
Active connections      : 0          AAA pending reqs      : 0
Peak connections       : 1          Peak time              : 1w6d
Authentication failures : 21
VPN session timeout    : 1          VPN idle timeout      : 0
User cleared VPN sessions: 0        Login Denied          : 0
Connect succeed        : 1          Connect failed        : 0
Reconnect succeed     : 0          Reconnect failed     : 0
IP Addr Alloc Failed   : 0          VA creation failed    : 0
Route Insertion Failed : 0
IPV6 Addr Alloc Failed : 0
IPV6 Route Insert Failed : 0
IPV6 Hash Insert Failed : 0
IPV6 STC Alloc Failed  : 0
in CSTP control        : 5          out CSTP control      : 3
in CSTP data           : 21         out CSTP data         : 8
```

```
Device# show crypto ssl stats tunnel profile prf1
```

```
SSLVPN Profile name : prf1
Tunnel Statistics:
Active connections      : 0
Peak connections       : 0          Peak time              : never
Connect succeed        : 0          Connect failed        : 0
Reconnect succeed     : 0          Reconnect failed     : 0
DPD timeout           : 0
Client
in CSTP frames         : 0          in CSTP control       : 0
in CSTP data           : 0          in CSTP bytes         : 0
out CSTP frames        : 0          out CSTP control      : 0
out CSTP data          : 0          out CSTP bytes        : 0
cef in CSTP data frames : 0        cef in CSTP data bytes : 0
cef out CSTP data frames : 0       cef out CSTP data bytes : 0
Server
In IP pkts             : 0          In IP bytes           : 0
Out IP pkts            : 0          Out IP bytes          : 0
```

Displays SSL VPN statistics.

Step 8 **clear crypto ssl session** {*profile profile-name*|*user user-name*}

Example:

```
Device# clear crypto ssl session sslprofile
```

Clears SSL VPN session.

Configuration Examples for SSL VPN

Example: Creating a Virtual Template for SSL VPN

The following example shows how to create a template for SSL VPN:

```
Device> enable
Device# configure terminal
Device(config)# interface virtual-template 1 type vpn
Device(config-if)# ip unnumbered Te0/0/4
Device(config-if)# ip tcp adjust-mss 1300
Device(config-if)# end
```

Example: Specifying the AnyConnect Image and Profile

The following example shows how to specify the Cisco AnyConnect image and profile:

```
Device> enable
Device# configure terminal
Device(config)# crypto vpn anyconnect bootflash:/webvpn/anyconnect-win-3.1.04072-k9.pkg
sequence 1
Device(config)# crypto vpn anyconnect profile Employee bootflash:/Employee.xml
Device(config)# end
```

Example: Configuring an SSL Proposal

The following example shows how to configure an SSL proposal:

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl proposal proposal1
Device(config-crypto-ssl-proposal)# protection rsa-3des-ede-sha1 rsa-aes128-sha1
Device(config-crypto-ssl-proposal)# end
```

Example: Configuring an SSL Policy

The following example shows how to configure an SSL policy:

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl policy policy1
Device(config-crypto-ssl-policy)# ip address local 10.0.0.1 port 443
Device(config-crypto-ssl-policy)# pki trustpoint tp1 sign
Device(config-crypto-ssl-policy)# ssl proposal proposal1
Device(config-crypto-ssl-policy)# no shut
Device(config-crypto-ssl-policy)# end
```

Example: Configuring an SSL Profile

The following example shows how to configure an SSL profile:

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl profile profile1
Device(config-crypto-ssl-profile)# aaa accounting user-pass list list1
Device(config-crypto-ssl-profile)# aaa authentication user-pass list list2
Device(config-crypto-ssl-profile)# aaa authorization group override user-pass list list1
user1
Device(config-crypto-ssl-profile)# aaa authorization user user-pass list list1 user1
Device(config-crypto-ssl-profile)# match policy policy1
Device(config-crypto-ssl-profile)# match url www.abc.com
Device(config-crypto-ssl-profile)# virtual-template 1
Device(config-crypto-ssl-profile)# no shut
Device(config-crypto-ssl-profile)# end
```

Example: Configuring an SSL Authorization Policy

The following example shows how to configure an SSL authorization policy:

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile Employee
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0
Device(config-crypto-ssl-auth-policy)# pool abc
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

The following example shows how to enable IPv6 support for SSL VPN:

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile profile1
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
```

```

Device(config-crypto-ssl-auth-policy) # include-local-lan
Device(config-crypto-ssl-auth-policy) # ipv6 prefix 64
Device(config-crypto-ssl-auth-policy) # ipv6 route set access-list acl1
Device(config-crypto-ssl-auth-policy) # keepalive 500
Device(config-crypto-ssl-auth-policy) # module gina
Device(config-crypto-ssl-auth-policy) # msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy) # msie-proxy option bypass
Device(config-crypto-ssl-auth-policy) # msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy) # mtu 1000
Device(config-crypto-ssl-auth-policy) # ipv6 pool ipv6pool
Device(config-crypto-ssl-auth-policy) # rekey interval 1110
Device(config-crypto-ssl-auth-policy) # route set access-list acl1
Device(config-crypto-ssl-auth-policy) # smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy) # split-dns abc1
Device(config-crypto-ssl-auth-policy) # timeout disconnect 10000
Device(config-crypto-ssl-auth-policy) # wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy) # end

```

Additional References for SSL VPN

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
Recommended cryptographic algorithms	Next Generation Encryption

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SSL VPN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for SSL VPN

Feature Name	Release	Feature Information
SSL VPN	Cisco IOS XE Release 17.7.1a	The SSL VPN feature is introduced. This feature provides support in the Cisco IOS XE software for remote user access to enterprise networks from anywhere on the internet.

