Cisco IOS SSL VPN

Q. What is Cisco IOS® SSL VPN or SSL VPN?

A. Secure Sockets Layer (SSL)-based VPN is an emerging technology that provides remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. SSL VPN provides the flexibility to support secure access for all users, regardless of the endpoint host from which they are establishing the connection. Cisco IOS SSL VPN does not require a VPN client to be preinstalled on the endpoint host.

Q. How does the licensing work for Cisco IOS SSL VPN?

A. There are two types of licencing schemes for Cisco IOS SSL VPN.

For the Cisco 870, 1800, 2800, 3800, and 7200 series routers, licenses are cost-effective paper licenses just like CCME or SRST licenses. There's no software key to enable the feature hence there is no support issue with using Cisco IOS SSL VPN once you have the Advanced Security or higher Cisco IOS image loaded on the Router. You can purchase the Feature license as a spare in packs of 10, 25 and 100 simultaneous users directly from Cisco.com configuration tool. If you already have a router, use the spare SKUs as follows: FL-WEBVPN-10-K9= FL-WEBVPN-25-K9= FL-WEBVPN-100-K9= depending upon the number of supported users for your platform.

For the Cisco 890, 1900, 2900, and 3900 NGX series ISRs, licensing will be enforced through the Cisco Product Licensing Registration Portal. The next generation of ISRs will also use a new set of SKUs as follows: FL-SSLVPN10-K9(=), FL-SSLVPN25-K9(=), and FL-SSLVPN100-K9(=). For more details on licensing, please visit http://www.cisco.com/en/US/products/ps9677/products_ios_technology_home.html.

Licenses are not interchangeable between the ISRs and NGX Series ISRs.

Q. Is it reasonable to implement both IP Security (IPsec) and SSL VPN in my network?

A. In many cases, IPsec and SSL VPN are complementary, because they solve different problems. This complementary approach allows a single device to address all remote-access user requirements (Figure 1).

Figure 1. Best Usage for IPsec and SSL VPN Solutions

Q. What are my options if IPsec ports are being blocked at the hotel firewall? Will SSL VPN help me?

A. Most users have success with IPsec from hotels, especially with the TCP or User Datagram Protocol (UDP) tunneling options. SSL VPN should work from these locations, as TCP port 443 (port used by SSL VPN) is already allowed for access to other secure Web servers.

Q. Are there problems in establishing an SSL VPN tunnel through firewalls?

A. Generally, ports required for Web traffic are open on firewalls, and SSL VPN uses these same ports, so it should not be a problem. If the firewall is blocking everything, then you would need to allow HTTPS traffic (TCP port 443 and UDP port 443 for DTLS) to allow SSL VPN traffic.

Q. Do companies require both SSL VPN and IPsec, and will most companies need to deploy both at some point?

A. Many customers have expressed interest in simultaneously supporting SSL VPN and IPsec connectivity. Cisco Systems® helps you support all your remote-access needs on a single platform at the same time.

Q. Are SSL VPN and IPsec VPN mutually exclusive, or can both solutions be offered from one location?

A. Customers can use both SSL VPN and IPsec VPNs simultaneously on Cisco® routers. Deploying SSL VPN and IPsec VPN solutions on the same box reduces the cost of operations and simplifies the network design.

Q. With the support of SSL VPN for remote access, why would I need IPsec?

A. These technologies are complementary. SSL allows you to secure clients independently, but remote sites with multiple PCs can use Cisco Easy VPN technology, taking advantage of IPsec.

Q. Can I use Dynamic Multipoint VPN (DMVPN), Easy VPN, and SSL VPN on the same Cisco IOS Software router?

A. Yes. This scenario lets customers run all security services, including Cisco IOS Firewall, Cisco IOS IPS, IPsec VPNs, quality of service (QoS), Network Address Translation (NAT), and routing along with SSL VPN on a single integrated services router.

Q. How do I determine when to use the Cisco IOS Software routers for SSL VPN versus using an appliance-based solution?

A. The Cisco IOS Software VPN security routers are the most widely deployed and most diverse family of VPN solutions in the industry today. Cisco VPN security routers represent the best options for customers of all sizes who want to integrate network and security services in a single device. Using the Cisco IOS Advanced Security feature set-a security-specific option for Cisco IOS Software-customers can combine the richest VPN feature set available for site-to-site and remote-access VPNs, with state-of-the-art firewall, intrusion prevention, and extensive Cisco IOS Software capabilities, including QoS, NAT, multicast, extensive WAN interface support, wireless support, dial backup, and advanced routing support. Customers who prefer a standalone security device should use the appliance-based solution.

Q. Is SSL VPN the same as SSL offloading?

A. No, SSL-based VPN is different from SSL offloading. SSL VPN works by tunneling the application traffic through an encrypted SSL VPN tunnel, whereas SSL offloading works by SSL acceleration for packets going to the inside Web servers.

Supported Software and Hardware

Q. What platforms does Cisco IOS SSL VPN support?

A. The Cisco IOS SSL VPN is supported on the Cisco ISR Series Routers, NGX Series ISR Routers, 7200, and 7301 routers running Advanced security images of Cisco IOS Software Release 12.4(6)T. Table 1 gives the maximum concurrent number of users supported per platform.

Table 1. Recommended Concurrent Number of Users Supported per Platform

Platform	Licenses Included with High Performance Security (HSEC) Bundles	Maximum Number of Users	
		Without Advanced Integration Module	With Advanced Integration Module
Cisco UC/SR500, 870, 880, and 890 Series Routers	-	10 users	-
Cisco 1800 and 1900 Fixed Routers	-	25 licensed users	-
Cisco 1841 and 2801 Routers	10 free users	-	75 licensed users
Cisco 1941 and 2901 Routers	-	75 licensed users	N/A

Platform	Licenses Included with High Performance Security (HSEC) Bundles	Maximum Number of Users	
		Without Advanced Integration Module	With Advanced Integration Module
Cisco 2811 and 2821 Routers	10 free users	-	100 licensed users
Cisco 2911 and 2921 Routers	-	100 licensed users	N/A
Cisco 2851 Routers	10 free users	-	150 licensed users
Cisco 2951 Routers	-	150 licensed users	N/A
Cisco 3800 Series Routers	25 free users	-	200 licensed users
Cisco 3900 Series Routers	-	200 licensed users	N/A
Cisco 7200 Series and Cisco 7301 Routers	-	200 licensed users	-

Q. Is there hardware support for Cisco IOS SSL VPN encryption?

A. Cisco modular ISR Routers (1800, 2800, 3800) require SSL VPN hardware acceleration with the AIM modules (AIM-VPN/SSL). For more details on these hardware AIM modules please visit: http://www.cisco.com/en/US/products/ps6657/products_data_sheet0900aecd804ff58a.html.

Platform	Onboard Crypto Engine	VPN-ISM
8xx	Y	N
1921	N	N
1941	N	Y
2901	N	Y
2911	N	Y
2921	N	Y
2951	Y	Y
3925	Y	Y
3945	Y	Y
3925E	Y	N
3945E	Y	N

Q. Note: ISM does not support DTLSWhat features are available in Cisco IOS Software Release 12.4 (6)T for Cisco IOS SSL VPN?

A. The SSL VPN in Cisco IOS Software Release 12.4(6)T supports the SSL VPN client (SVC) along with Cisco Secure Desktop and virtualization support:

- **SSL VPN Client (full network client Cisco IOS SSL VPN)** - Full network client mode offers extensive application support through its dynamically downloaded SSL VPN client for Cisco IOS SSL VPN. With the Full Network Client for Cisco IOS SSL VPN, Cisco delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client (AnyConnect Client) that allows network-layer connectivity access to virtually any application.

- **Virtualization and VRF support** - VPN routing and forwarding (VRF), which creates virtualization, can be used to create various customer or departmental contexts that can have different configuration, while still using overlapping address space.

Q. What are some of the latest features available as part of the Cisco IOS Software Release 12.4(24)T for Cisco IOS SSL VPN?

A. The SSL VPN in Cisco IOS Software Release 12.4(24)T has enhanced the existing SSL VPN capability highlighted above to support the following features.

Table 2. Cisco IOS SSL VPN Feature Support in 12.4(15)T

Feature	Description
Cisco AnyConnect Localization	Support for AnyConnect in localized language.
Client side certificate support	Authentication of clients through the use of digital certificates.
Support for 64-bit AnyConnect client	AnyConnect support for 64-bit Windows Operating systems.
Sesson Resumption	Session resumption allows pseudo ip mobility for clients that roam between networks. When the client moves from one network to another, the VPN connection will automatically renegotiate without the need for the user to resupply their credentials.

Feature Details

Q. What SSL VPN offering is available with Cisco IOS Software?

A. Cisco's IOS SSL VPN feature is focused on full tunnel connectivity based on either the SVC or AnyConnect clients.

Q. What is the level of encryption for Cisco IOS SSL VPN?

A. Most standard Web browsers support Triple Data Encryption Standard (3DES), DES, Rivest Cipher 4-128 (RC4-128), and 40-bit encryption. Cisco IOS SSL VPN by default selects the RC4-128 encryption, and all other encryption levels are configurable options.

Q. Do SSL VPN solutions use digital certificates, or something else?

A. A Cisco router configured as a Cisco IOS SSL VPN gateway requires a digital certificate like any other HTTPS (SSL) Web server. A client accesses the https://router_ip to start the SSL VPN connection and is authenticated with a username and password (no client-side certificate is required).

Q. Is it necessary to install a digital certificate in the Cisco IOS Software routers for SSL VPN?

A. Yes, a certificate is required for browser-based access. You can use either the router command-line interface (CLI) or Cisco Configuration Professional(CCP) to generate a self-signed certificate on the router (setup does not require any certificate-authority server) or you can set up an external certificate-authority server to provide the required certificate. For small- and midsized-business (SMB) and commercial customers without an external certificate server, Cisco recommends using the persistent self-signed certificate. Details about persistent self-signed certificates are available at http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html.

Q. How can I use SSL or IPsec certificates on my Cisco VPN for authentication?

A. Certificates for IPsec can be loaded into the VPN client native certificate manager or the Microsoft Common Application Programming Interface (CAPI) store (accessible from Internet Explorer). For SSL VPN, you can download the certificate from the SSL VPN gateway and install it in your Web browser.

Q. Can a service provider create multiple SSL VPN contexts and associate VRFs with them for our customers?

A. Absolutely. You can create multiple SSL VPN contexts and then have a specific customer VRF be associated with them to keep customers' routing information separate.

Q. Will the Cisco IOS SSL VPN work with browsers other than Internet Explorer?

A. Yes. The Cisco IOS SSL VPN takes a browser-independent approach to SSL VPN, including support for Mozilla (Firefox), Netscape, and Internet Explorer.

Full Network Access

Q. What protocols can be tunneled through Cisco IOS SSL VPN?

A. The IOS SSL VPN clients are agnostic to the type of traffic and tunnels traffic much like the Cisco IPsec VPN clients. The difference of course is that SSL is used.

Q. With IPsec VPN, I use the Cisco IPsec VPN client. Can I use the same client with SSL VPN?

A. No, you cannot use the IPsec VPN client for SSL VPN connectivity. A Web browser would be used to get the initial SSL VPN tunnel up and in case you require full network access, an SSL VPN Client is automatically downloaded to that end user (using Java or Active X).

Q. Do I need to preinstall any VPN client on the client machine to use full-network-access SSL VPN?

A. The main advantage of using SSL VPN is that it does not require a preinstalled client on the client machine. Always make your initial connection to the SSL VPN gateway using your Web browser (using https://gateway_address). To obtain full network access through the SSL VPN gateway an SSL VPN client (SVC or AnyConnect) is downloaded to the client PC upon connection. The SSL VPN client is installed either once or upon each connection, depending on your gateway configuration.

Q. Do I assign IP address pools for users using SSL VPN client (full network access) as I do for IPsec clients?

A. Yes, you do need to assign IP addresses to SSL VPN clients connecting to the router using an SSL VPN client, and you need to make sure the network address is part of the inside network.

Q. Do I need administrative privileges on the machine to download the SSL VPN client?

A. Yes, administrative privileges are required for a user to download the SSL VPN client on the machine. For users with administrative privileges, the SSL VPN client is downloaded (using Java or Active X) if the client specific configuration is enabled on the Cisco IOS SSL VPN gateway. If the SSL VPN client is installed on a machine permanently (using an installer stub), then administrative rights are required only during the SSL VPN client install time. Nonadministrative users can use the SSL VPN client on the client PC after the client is permanently installed on that PC.

Management

Q. Does Cisco SDM support Cisco IOS SSL VPN?

A. The Cisco IOS SSL VPN is supported by Cisco SDM v2.3 with Cisco IOS Software Release 12.4(6)T, which is included free of charge as part of all router security bundles. Additionally, Cisco SDM can be downloaded for free at http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm.

Q. Can I easily configure the Cisco IOS SSL VPN or SSL VPN using the Cisco CCP?

A. The Cisco CCP provides wizards for both basic and advanced configurations, making configuration of Cisco IOS SSL VPN very simple.

Q. Where can I find more documentation about Cisco IOS SSL VPN for Cisco IOS Software Release 12.4(24)T?

A. You can find additional documentation at http://www.cisco.com/go/iossslvpn.

For More Information

For more information about the Cisco IOS SSL VPN and SSL VPN solution, visit http://www.cisco.com/go/iossslvpn for the product homepage or contact your local Cisco account representative or Cisco Technical Assistance Center (TAC).

Acknowledgement

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C67-60008-09 04/13