

# Cisco IOS SSL VPN: Router-Based Remote Access for Employees and Partners

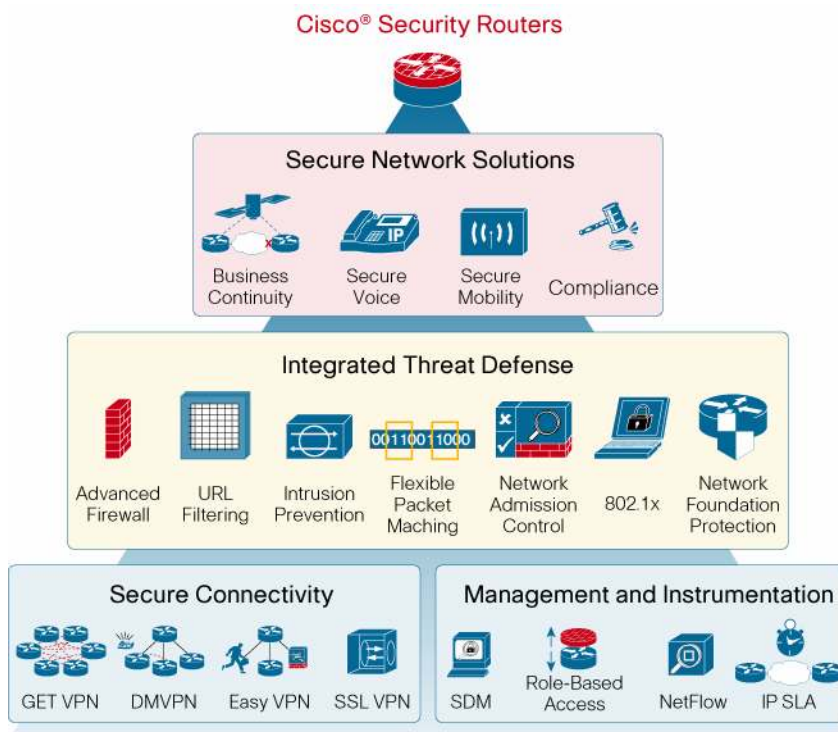
## Product Overview

Cisco IOS<sup>®</sup> SSL VPN is the first router-based solution offering Secure Sockets Layer (SSL) VPN remote-access connectivity integrated with industry-leading security and routing features on a converged data, voice, and wireless platform. SSL VPN is compelling; the security is transparent to the end user and easy for IT to administer.

With Cisco IOS SSL VPN, end users gain access securely from home or any Internet-enabled location such as wireless hotspots. Cisco IOS SSL VPN also enables companies to extend corporate network access to offshore partners and consultants, keeping corporate data protected all the while.

Cisco IOS SSL VPN in conjunction with the dynamically downloaded Cisco AnyConnect VPN Client provides remote users with full network access to virtually any corporate application. Remote end-user computers are secured with the included Cisco Secure Desktop application, helping prevent data such as cookies, browser history, temporary files, and downloaded content from being left behind and pilfered after a session terminates. Cisco IOS SSL VPN features easy-to-use wizards that simplify deployment, and powerful tools to monitor and manage sessions in real time. Cisco IOS SSL VPN is a single-box VPN, security, and routing solution, unlike other vendor products that require multiple devices and management systems (Figure 1).

**Figure 1.** Cisco Security Routers with Cisco IOS SSL VPN

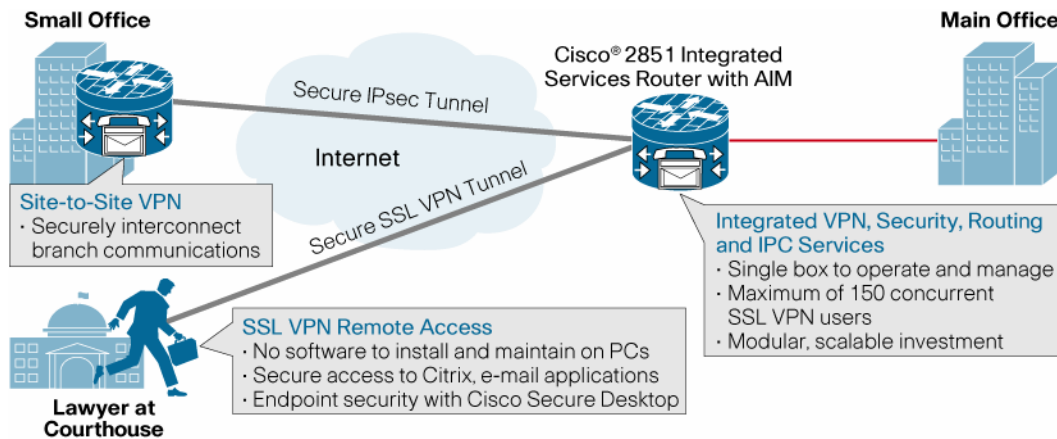


An integrated solution is easier to learn, deploy, provision, manage, and maintain, and has higher availability. This integrated solution has lower initial capital expenditure, lower deployment costs, and lower ongoing operational costs than competing multiple-device solutions.

## Applications

Cisco IOS SSL VPN is useful for small and medium-sized businesses (SMBs) looking to extend remote access to employees and business partners. In addition, enterprises with a large number of small or medium-sized branches can use the Cisco IOS SSL VPN to combine remote access gateway capabilities with branch routers, thereby providing load-distribution functionality and redundancy to central-site VPN gateways. Figure 2 illustrates an application example for Cisco IOS SSL VPN.

**Figure 2.** Application Example: Regional Law Firm with Multiple Offices



- **Improved staff productivity:** On-road access to business applications
- **Compliance with regulations:** All communications encrypted and logged
- **Proactive threat defense:** Application firewall, inline IPS, and touchless end-point security

## Features and Benefits

- **Advanced full-network access:** The Cisco IOS SSL VPN solution offers extensive application support through its dynamically downloaded AnyConnect VPN Client, enabling network-layer connectivity to virtually any application.
- **Comprehensive endpoint security:** The Cisco Secure Desktop offers pre-connection security-posture assessment and seeks to minimize data such as cookies, browser history, temporary files, and downloaded content from being left behind after an SSL VPN session terminates.
- **Ease of deployment and management:** Intuitive, Web-based interface with wizards simplifies configuration. Advanced monitoring and management allow zero-touch remote endpoint management.
- **SSL VPN gateway network integration:** Advanced authentication and access-control features pinpoint who gains access to what; virtualization allows efficient segmentation into departments, customers, or other groups of users.
- **Simple and cost-effective licensing:** The simple licensing structure of Cisco IOS SSL VPN (no added licenses for special features), combined with the consolidated technology platform, provides customers with unparalleled cost savings and competitive per-user pricing.

### Advanced Full-Network Access: Cisco AnyConnect VPN Client

With the Cisco AnyConnect VPN Client (Table 1), Cisco delivers a lightweight, centrally configured, easy-to-support SSL VPN tunneling client that allows access to virtually any application. The Cisco AnyConnect VPN Client can be loaded with any SSL-enabled browser and dynamically made available to the user in one of three methods: ActiveX, Java, or an .exe file.

**Table 1.** Cisco AnyConnect VPN Client: Features and Benefits

Feature	Description and Benefit
<b>Universal Application Access</b>	This feature provides full client capabilities over SSL, including access to Cisco IP SoftPhone and voice-over-IP (VoIP) support, increasing remote-user productivity.
<b>Ease of Download and Installation</b>	<ul style="list-style-type: none"> <li>• Dynamic download and multiple delivery methods help ensure transparent download and distribution with Java, ActiveX, or .exe.</li> <li>• Small download size helps ensure rapid delivery.</li> <li>• No reboot is required after installation.</li> </ul>
<b>Increased Security</b>	Client can be either removed at the end of a session or left permanently installed.
<b>Zero-Touch Remote Administration</b>	Central-site configuration provides integration, with no administration on the remote client side needed.

## Comprehensive Endpoint Security: Cisco Secure Desktop

The potential for network security attacks increases with the extension of the network to both secure and external endpoints. Whether users are accessing the network from a corporate-managed PC, personal machine, or public terminal, the Cisco Secure Desktop application, included with Cisco IOS SSL VPN, seeks to minimize data leakage or theft from the SSL session.

The Host Integrity Verification feature in Cisco Secure Desktop performs pre-connection posture assessment to verify that the endpoint seeking access possesses the particular antivirus, firewall, and OS or service pack features required, and detects certain installed malware before granting access to the network. Cisco Secure Desktop then creates a secure vault for session information by generating a virtual “sandbox” on the machine.

During the session, information is encrypted and written to the Cisco Secure Desktop partition on the hard drive. At the close of the session, the secure vault is eradicated using a U.S. Department of Defense (DoD) sanitization algorithm. Session information, including cache files, history, cookies, file downloads, and passwords, are encrypted in real time, reducing the risk that data is left behind. This feature is unique; many comparable cache-cleaning products attempt a post-session cleanup of tracked files.

The automatic timeout features of Cisco Secure Desktop help ensure that session information is erased, whether or not the user takes the active role in terminating the session. Cisco Secure Desktop can often run with guest permissions, providing advanced protection on endpoints regardless of Web settings, browser types, or system privileges.

Table 2 lists features of Cisco Secure Desktop.

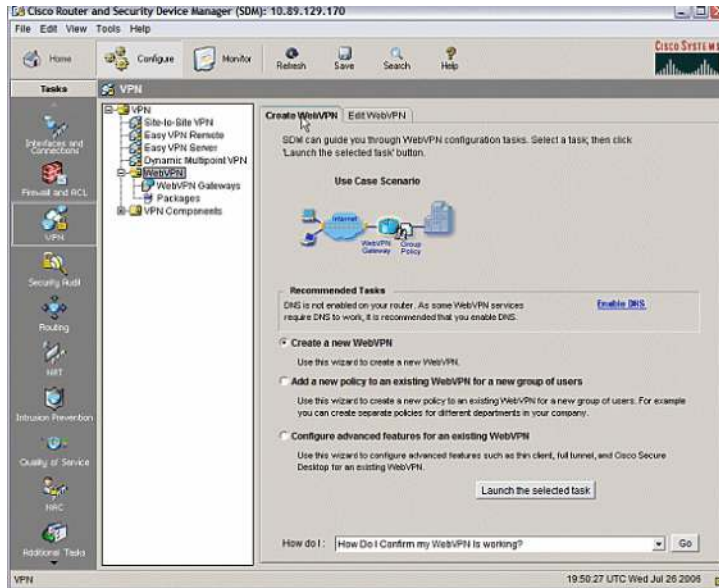
**Table 2.** Cisco Secure Desktop: Comprehensive Security from the Network to the Endpoint

Feature	Description and Benefit
<b>Available with Guest Permissions</b>	Users accessing the network from remote machines may not have administrator privileges on all systems. Cisco Secure Desktop can often be installed with only guest permissions, helping ensure delivery and installation on all systems.
<b>Pre-Connection Posture Assessment</b>	Host integrity verification checking detects the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access.
<b>Comprehensive Session Protection</b>	Additional protection is provided for all data associated with the session, including passwords, file download history, cookies, and cache files. All session data is encrypted to the secure vault of Cisco Secure Desktop.
<b>End-of-Session Data Cleanup</b>	Data in the secure vault is overwritten at the end of the session.
<b>Keystroke Logger Detection</b>	Cisco Secure Desktop performs an initial check for certain software-based keystroke logging software at the start of the session. If an anomalous program begins running inside the secure vault after session initiation, the user is prompted to stop the suspicious activity.

## Ease of Deployment and Management

Cisco Router and Security Device Manager (SDM) Version 2.3.1 or later provides advanced wizards to make it easy to configure Cisco IOS SSL VPN. Cisco SDM is included in Cisco Router Security bundles.

**Figure 3.** Cisco Router and Security Device Manager: Wizard-Based Management



Group-based management features allow administrators to design security policies and authentication methods for each group, a feature that is essential when extending network resources to non-corporate-managed users and endpoints.

In addition, Cisco IOS CLI can also be used to configure and monitor SSL VPN, for users who prefer that option.

For medium-sized or large installations, Cisco Security Manager Version 3.1 or later provides enterprise-class scalable SSL VPN configuration on Cisco routers and adaptive security appliances.

## SSL VPN Gateway Network Integration

The Cisco IOS SSL VPN service running on Cisco routers allows the integration of SSL VPN with IP services on the router.

Table 3 lists the primary network integration capabilities.

**Table 3.** Cisco IOS SSL VPN Gateway Network Integration

Feature	Benefit
<b>User Authentication: RADIUS or Authentication, Authorization, and Accounting (AAA) Server</b>	<ul style="list-style-type: none"> <li>Ability to require users to authenticate with a username and password</li> </ul>
<b>Network Access Control</b>	<ul style="list-style-type: none"> <li>Advanced options to control network access based on IP address, Differentiated Services Code Point/type of service (DSCP/ToS), TCP/UDP port, per-user, and per-group</li> </ul>
<b>Multiple Contexts</b>	<ul style="list-style-type: none"> <li>Ability to divide into multiple contexts, each a logical representation of the Cisco IOS SSL VPN service, complete with separate policies and configuration</li> </ul>
<b>Virtual Route Forwarding (VRF) Awareness:</b> <ul style="list-style-type: none"> <li>VRF mapping</li> <li>Single IP model (URL-based or login-name-based)</li> <li>Multiple IP model</li> <li>Per-VRF AAA server</li> <li>Per-VRF Domain Name System (DNS) server</li> <li>Per-VRF gateway</li> <li>Per-VRF number of users</li> </ul>	<ul style="list-style-type: none"> <li>Ability for service providers to easily integrate the SSL VPN gateway into a shared MPLS network</li> <li>Increased security by separating specific routes from global routing table</li> <li>Support for overlapping IP address pools</li> </ul>

## Simple and Cost-Effective Licensing

Cisco IOS SSL VPN is a licensed feature available on Cisco routers running the Cisco IOS Advanced Security feature set. Cisco Router Security bundles entitle you to a certain number of free users; beyond that, you need to purchase additional feature licenses. Table 4 specifies the number of free users and the maximum number of users supported on each platform.

**Table 4.** Number of Concurrent SSL VPN 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
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	–

The feature licenses are available in packs of 10, 25, or 100 simultaneous users directly from the Cisco.com configuration tool or through your Cisco partner or account team; Table 7 provides ordering information.

**Note:** Customers ordering Cisco 1840, 2800, or 3800 HSEC bundles need only purchase the incremental number of licenses over and above the number already included. For example, to order the maximum 100 users on the Cisco 2811 HSEC bundle, add feature licenses adding up to 90 users (for example: 2 x 25 + 4 x 10).

## Product Specifications

Table 5 provides a listing of product specifications.

**Table 5.** Product Specifications

<b>End-user operating systems supported</b>	Windows 2000, Windows XP, and Windows Vista
<b>Browser Compatibility</b>	Netscape, Internet Explorer, Firefox, and Mozilla
<b>Protocols</b>	SSL 3.0 and 3.1; and Transparent LAN Services (TLS) 1.0 configuration and management
<b>Cypher Suites</b>	<ul style="list-style-type: none"> <li>• SSL_RSA_WITH_RC4_128_MD5</li> <li>• SSL_RSA_WITH_RC4_128_SHA</li> <li>• SSL_RSA_WITH_DES_CBC_SHA</li> <li>• SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul>
<b>Configuration Management</b>	Console command-line interface (CLI), HTTP, HTTPS, Telnet, Secure Shell (SSH) Protocol, and Web-based Cisco SDM
<b>Syslog Support</b>	Console display, external server, and internal buffer

## System Requirements

Table 6 lists the hardware and software requirements to install and use Cisco IOS SSL VPN.

**Table 6.** System Requirements

<b>Hardware</b>	Cisco SR500, 870, 880, 890, 1800, 1900, 2800, 2900, 3800, 3900, 7200 Series and Cisco 7301 Routers
<b>Cisco IOS Software Release</b>	Cisco IOS 12.4(9)T or later recommended
<b>Cisco IOS Software Feature Set</b>	Advanced Security or higher

**Note:** SSL VPN is supported in IOS Software. For hardware acceleration of IOS SSL VPN, a VPN AIM is required. This is supported on the Cisco 1841, 2800, and 3800 Series Integrated Services Routers

### Ordering Information

Tables 7 and 8 provide a list of feature license part numbers. Customers can add these to the configuration while ordering the router system. Features licenses are platform specific and are not interchangeable.

In addition, customers with existing Cisco integrated services routers can gain support for Cisco IOS SSL VPN through a software upgrade, by purchasing these feature licenses and upgrading their Cisco IOS Software feature set as applicable.

To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center.

**Table 7.** Ordering Information for ISRs (870, 880, 890, 1800, 2800, and 3800 Series Routers)

Product Name	Part Number
Feature License SSL VPN for Up to 10 Users (incremental)	FL-WEBVPN-10-K9
Feature License SSL VPN for Up to 25 Users (incremental)	FL-WEBVPN-25-K9
Feature License SSL VPN for Up to 100 Users (incremental)	FL-WEBVPN-100-K9
Feature License SSL VPN for Up to 10 Users (incremental)	FL-WEBVPN-10-K9=
Feature License SSL VPN for Up to 25 Users (incremental)	FL-WEBVPN-25-K9=
Feature License SSL VPN for Up to 100 Users (incremental)	FL-WEBVPN-100-K9=

**Table 8.** Ordering Information for the ISRs Generation 2 (1900, 2900, and 3900 Series Routers)

Product Name	Part Number
Feature License SSL VPN for Up to 10 Users (incremental)	FL-SSLVPN10-K9
Feature License SSL VPN for Up to 25 Users (incremental)	FL-SSLVPN25-K9
Feature License SSL VPN for Up to 100 Users (incremental)	FL-SSLVPN100-K9
Feature License SSL VPN for Up to 10 Users (incremental)	FL-SSLVPN10-K9=
Feature License SSL VPN for Up to 25 Users (incremental)	FL-SSLVPN25-K9=
Feature License SSL VPN for Up to 100 Users (incremental)	FL-SSLVPN100-K9=

**Note:** Part numbers ending in "=" are spares and can be ordered independently of any other product(s).

### Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies.

### For More Information

Visit the [Cisco Software Center](#) to download Cisco IOS Software. Cisco IOS Software Release 12.4(9)T Advanced Security Image or later is recommended to install and use the Cisco IOS SSL VPN feature set.

