

WebVPN Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

PRODUCT OVERVIEW

The Cisco® WebVPN Services Module (Figure 1) is a high-speed, integrated Secure Sockets Layer (SSL) VPN services module for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers, complementing the existing capabilities in the Cisco portfolio of remote-access products.

Figure 1. The Cisco WebVPN Services Module



Today's increasingly sophisticated and mobile workforces are demanding remote access from multiple fixed and wireless devices, and want access as if they were on their local corporate networks. SSL VPNs offer users the benefit of "anywhere access." Because SSL is included in standard browsers like Microsoft Internet Explorer and Netscape, SSL VPNs offer the possibility of a clientless solution. Users can access their applications from anywhere they have Internet access: from an airport kiosk, from another person's computer, or even using a wireless device. SSL VPNs also work over broadband networks. In addition, SSL VPNs can successfully traverse firewalls and can handle network address translation (NAT) issues, which can be problematic with IP Security (IPsec)-based VPNs.

With the Cisco WebVPN Services Module based on SSL VPN technology, salespeople can download corporate customer relationship management data from the field. Manufacturing plant managers can track inventories and place orders before supplies reach critically low levels. Doctors can transmit prescription authorization from the bedside of a patient. Shop-floor managers at manufacturing firms can place on-the-spot orders.

The Cisco WebVPN Services Module provides easy access to a broad range of Web resources and Web-enabled applications, from almost any computer that can reach Secure HTTP (HTTPS) Internet sites. The module uses the SSL protocol and its successor, Transport Layer Security (TLS), to provide a secure connection between remote users and specific, supported internal resources that are configured at a central site.

The Cisco WebVPN Services Module delivers clientless, thin-client, and SSL tunneling client access methods, enabling the appropriate level of application access based on the end-system deployment environment, such as employees, extranets, and non-company-managed devices. With the SSL VPN Client for WebVPN, Cisco delivers a lightweight, centrally configured, easy-to-

support SSL VPN tunneling client that allows access to virtually any application. The SSL VPN Client for WebVPN is compatible with any SSL-enabled browser and is dynamically pushed to the user. Clientless access with the Cisco WebVPN Services Module allows users to connect with few requirements beyond a basic Web browser; once connected, they can access Web servers or other resources such as shared files and e-mail through Microsoft Outlook Web Access 2003.

Benefits

Scalability

The Cisco WebVPN Services Module is an integrated services module for Cisco Catalyst 6500 Series and Cisco 7600 Series products. A single module is capable of supporting up to 8000 simultaneous users and up to 32,000 concurrent connections. Up to four modules can be supported in a single chassis to support up to 32,000 simultaneous SSL VPN users and 128,000 connections. The scalability and unique virtualization capabilities of the Cisco WebVPN Services Module make it an ideal solution for managed service providers, and simplify the policy creation and enforcement requirements in large enterprises with diverse user populations.

Integrated Module

The Cisco WebVPN Services Module allows any port on a Cisco Catalyst 6500 Series or Cisco 7600 Series device to operate as an SSL VPN port. This is especially important when rack space is at a premium. With the module, the Cisco Catalyst 6500 Series truly emerges as the IP services switching platform of choice for customers that require intelligent services such as firewall services, intrusion detection, and VPN, along with multilayer LAN, WAN, and MAN switching capabilities.

Virtualization and VRF Awareness

Virtualization technology is a way to pool resources while masking the physical attributes and boundaries of the resources from the resource users. Up to 128 virtual routing and forwarding (VRF)-aware virtual contexts are supported per module.

Two primary models are used to map a user to a VRF context:

- **Single-IP model**—Users of different enterprises establish VPN sessions to the single HTTPS proxy. The actual user-to-VRF mapping is done through either the URL name used in the browser or the login name used in the login process.
- **Multiple-IP model**—Users of different enterprises establish VPN sessions to the multiple HTTPS proxies; one enterprise per HTTPS proxy. The user-to-VRF mapping is implied by the HTTPS proxy instance.

Each VRF context supports the following network resources:

- **Per-VRF authentication, authorization, and accounting (AAA) server**—For user authentication
- **Per-VRF domain name system (DNS) server**—For enterprise-level name resolving
- **Per-VRF default gateway**—For routing IP packets within the VRF domain
- **Per-VRF maximum-user-allowed**—For enterprise-level admission control

Advanced Endpoint Security

A primary component of the Cisco WebVPN Services Module, 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.

Broad Application Support for SSL VPN

The Cisco WebVPN Services Module offers extensive application support through its dynamically downloaded SSL VPN client, enabling network-layer connectivity to virtually any application. The module's truly clientless support for Web-based applications allows a low-overhead extension of network resources to VPN users through a standard Web browser. Pure clientless and thin-client port forwarding options may be deployed for environments with limited application access requirements, such as extranets.

Flexibility

IPsec and SSL are complementary technologies that address unique user access requirements; both may be necessary in order for a company to meet the needs of a diverse user base. Support for both IPsec and SSL VPN allows businesses to choose the most appropriate technology for users accessing the network through different scenarios. This provides maximum flexibility and application access all on one platform, alleviating the need to deploy and manage separate infrastructures.

Ease of Deployment

The Cisco WebVPN Services Module comes with integrated device manager support. This helps configure and provision the module without the need for an external element management system, providing a ready-to-deploy solution.

Modes of Operation

Clientless Mode

The following applications are supported in clientless mode (they all rely on the Web browser as the client):

- Web browsing (HTTP/HTTPS)
- File sharing (Common Internet File System [CIFS])
- Web e-mail such as Microsoft Outlook Web Access (HTTP/HTTPS) with WebDAV extensions

Thin-Client Mode

The applications supported in the thin-client mode (TCP Port Forwarding, for example) support TCP/IP client server applications such as mail-based applications (SMTP, POP3, and IMAP4, for example), terminal services, instant messaging, and Telnet.

Tunnel Mode

Tunnel mode redirects a user's VPN traffic at the network layer through an SSL tunnel, providing support for most IP-based applications. While other SSL VPN operation modes offer a limited set of application support, the tunnel mode supports almost all of the popular corporate applications, including Meeting-Maker, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-Mail, and Telnet. Even some legacy applications, such as 3270 terminal emulation, can be supported.

Table 1 lists the features of the Cisco WebVPN Services Module, and Table 2 lists system requirements.

Table 1. Feature Availability

Feature	Description
Scalability	<ul style="list-style-type: none"> • Up to 8000 users • Up to 300 Mbps • Up to 64 SSL VPN virtual contexts and 64 gateways • Up to 4 modules in a chassis
Virtualization	Ability to divide into multiple contexts, with each context as a complete logical representation of the WebVPN Services Module, complete with separate policies and configuration
VRF-Aware	<ul style="list-style-type: none"> • VRF mapping <ul style="list-style-type: none"> ◦ Single-IP model (URL-based or login-name-based) ◦ Multiple-IP model • Per-VRF AAA server • Per-VRF DNS server • Per-VRF gateway • Per-VRF number of users
User Authentication	<ul style="list-style-type: none"> • RADIUS • Windows NT, Active Directory, UNIX NIS • Group-based access control using Cisco Secure Access Control Server (ACS)
End-System Integrity (Cisco Secure Desktop integration)	<ul style="list-style-type: none"> • Antivirus check • Personal firewall check • Seeks to minimize risk of temporary and downloaded files and cookies from remaining on system
Redundancy and Load Sharing	<ul style="list-style-type: none"> • Stateless failover • Cisco IOS[®] Software server-load balancing (SLB) and Content Switching Module integration within the chassis • Active/Active failover
Application Support	Web access, file services, e-mail, Telnet, file transfer, legacy applications, specialized applications
Browser Support	Netscape, Internet Explorer, Firefox
Protocols	SSL 3.0 and 3.1; TLS 1.0
Configuration and Management	Console CLI, HTTP, HTTPS, Telnet, Secure Shell (SSH)
Syslog Support	Console display, external server, internal buffer
Cipher Suites	<ul style="list-style-type: none"> • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_DES_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA
Network Access Control	IP address, Differentiated Services Code Point/Type of Service (DSCP/ToS), TCP/UDP port, per-user, per-group

Table 2. System Requirements

Features	Descriptions
Chassis	Cisco Catalyst 6500 Series or Cisco 7600 Series
Supervisor Engines	Supervisor Engine 720 or Supervisor Engine 2/MSFC2
Chassis Software Compatibility	<ul style="list-style-type: none"> • WebVPN Software Version 1.1 • Native Cisco IOS Software Release <ul style="list-style-type: none"> ◦ 12.2(17d)SXB7 ◦ 12.2(18)SXE2
Maximum Number of Modules in a Chassis	4
Cards/Ports/Slots	1 slot per module
Cisco WebVPN Software Version	1.1
Maintenance Partition (MP) Version	3.1(1)

Ordering Information

To place an order, visit the [Cisco Ordering Home Page](#), or see Table 3.

Table 3. Ordering Information

Part Number	Description
WS-SVC-WEBVPN-K9	WebVPN Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series
WS-SVC-WEBVPN-K9=	WebVPN Services Module (spare)
SC-SVC-WVPN-11-K9	WebVPN Services Module Software 1.1
SC-SVC-WVPN-11-K9=	WebVPN Services Module Software 1.1 (spare)

User Licensing

Cisco WebVPN Services Module comes with the 2500 users configured with the base system. There is no additional licensing required for 2500 users. For additional users, please use the following part numbers.

Table 4. User Licensing

Part Number	Description
FR-SVC-WVPN-5000	Cisco Catalyst 6500 and Cisco 7600 WebVPN 5000 user license
FR-SVC-WVPN-8000	Cisco Catalyst 6500 and Cisco 7600 WebVPN 8000 user license

To download the software, visit the [Cisco Software Center](#) (requires login).

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

Regulatory Compliance

Safety

- UL 1950
- CSA C22.2 No. 950-95
- EN60950
- EN60825-1
- TS001
- CE Marking
- IEC 60950
- AS/NZS3260

EMI

- FCC Part 15 Class A
- ICES-003 Class A
- VCCI Class B

- EN55022 Class B
- CISPR22 Class B
- CE Marking
- AS/NZS3548 Class B

NEBS

- **SR-3580—NEBS:** Criteria Levels (Level 3 compliant)
- **GR-63-CORE—NEBS:** Physical Protection
- **GR-1089-CORE—NEBS:** EMC and Safety

ETSI

- ETS-300386-2 Switching Equipment

Telecommunications

- ITU-T G.610
- ITU-T G.703
- ITU-T G.707
- ITU-T G.783 Sections 9-10
- ITU-T G.784
- ITU-T G.803
- ITU-T G.813
- ITU-T G.825
- ITU-T G.826
- ITU-T G.841
- ITU-T G.957 Table 3
- ITU-T G.958
- ITU-T I.361
- ITU-T I.363
- ITU I.432
- ITU-T Q.2110
- ITU-T Q.2130
- ITU-T Q.2140
- ITU-T Q.2931
- ITU-T O.151
- ITU-T O.171
- ETSI ETS 300 417-1-1
- TAS SC BISDN (1998)
- ACA TS 026 (1997)
- BABT/TC/139 (Draft 1e)



Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)