Cisco WebVPN for Routers

Industry’s First Routing and Security Platform with SSL VPN Remote Access Connectivity
SSL VPN Enables SMB/Commercial Remote Access Needs

SMB/Commercial Customers’ Security Drivers*

Customers need*:

**Increased requirement for operational efficiency**
- Proliferation of mobile workers
- Greater collaboration requirements—partners, vendors, customers

**While still facing:**
- Increased security threats
- Increased regulatory compliance burdens

SSL VPN technology offers mid-market customers

- Immediate and spur-of-the-moment employee access, whether on the road or as a teleworker
- Secure remote access without worry of operating system, device interoperability, or access to partner systems
- Threat defense and authentication capabilities reduce threat risk
- When combined with endpoint security, SSL VPN eases proof of regulatory compliance

*Source: Cisco®-sponsored research/Gartner June 2004
Customers See High Value in Intelligent Services Integration

- 64 percent of customers preferred integrated services
- Reasons:
  - Ease of support & management
  - Lower operational costs
  - Better performance, scalability
  - Lower capital costs
  - Move intelligence to branch
  - Feature interoperability

Functions that SHOULD be router integrated

Source: Yankee Group Research Inc., Jan 2006
Cisco Routers with WebVPN
Industry’s First Routing and Security Platform with SSL VPN

Supply partner
Requires access to ordering databases

Branch office
Requires site-to-site

Hourly employee
Requires access to online schedule and timesheets (specific apps)

Mobile user

Employee at Home/Mobile user
Requires consistent LAN-like access

Internet

Strategic services platform

Cisco IOS® Router

Comprehensive security:
- SSL VPN
- Cisco® Secure Desktop
- IPSec VPN
- Firewall
- Intrusion Prevention

Integrated security, voice and LAN, WLAN, WAN access
- Single box to operate and manage
- Simplified and consistent security policies
- Easier network design and traffic policing
- Reduced total cost of ownership & improved service availability
- Leverage network infrastructure investments to add remote users
Platforms: Cisco 1800, 2800, 3700, 3800 Series Routers

Clientless Access

- SSL
- Internet
- Web browser

Full Network Access

- Internet
- IP over SSL
- Web browser

Web-based + application helper

- Browser-based (clientless)
- Intranet web pages, Outlook Web access, Citrix, Windows File Share (CIFS)
- Application helper for non-webified applications like POP/SMTP, IM, Telnet

IP-based applications

- SSL VPN client for virtually any application e.g. Cisco® Softphone
- Dynamically-loaded client may be permanently installed or removed automatically

Cisco Router and Security Device Manager – Simple GUI-based provisioning and management with step-by-step Wizards for turn-key deployment

Cisco Secure Desktop – Prevents digital leakage, protects user privacy, easy to implement & manage, works with desktop guest permissions

Virtualization and VRF awareness – Pool resources while masking the physical attributes and boundaries of the resources
Cisco Routers with WebVPN
SSL VPN Portfolio and Pricing

- Simple and cost-effective pricing—all WebVPN functionality included in single license
- License packs available in 10, 25, and 100 increments
- Demo licenses: Two-user demo license available on Cisco® 870–3800 Series Integrated Services Routers and Cisco 7200 and 7301 Routers

<table>
<thead>
<tr>
<th>Price</th>
<th>Model</th>
<th>SSL VPN Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Business / Branch</td>
<td>Cisco 1800</td>
<td>Up to 25 SSL VPN sessions</td>
</tr>
<tr>
<td>Medium Business / Branch</td>
<td>Cisco 2800</td>
<td>Up to 75 SSL VPN sessions</td>
</tr>
<tr>
<td>Medium Business / Branch</td>
<td>Cisco 3800</td>
<td>Up to 100 SSL VPN sessions</td>
</tr>
<tr>
<td>Medium Business / Branch</td>
<td>Cisco 7200/7301</td>
<td>Up to 150 SSL VPN sessions</td>
</tr>
</tbody>
</table>
Typical Scenario with Multiple Devices

- Multiple devices to manage and support
- Security policies may be inconsistent
- More complexity in network design
Cisco Routers with WebVPN

Industry’s First Routing and Security Platform with SSL VPN Remote Access Connectivity

One box to learn, deploy, provision, manage, maintain

- Reduced total cost of ownership & improved service availability
- Simplified and consistent security policies
- Easier network design and traffic policing
- Leverage network infrastructure investments

SSL VPN
Application firewall
Intrusion prevention
Network Admission Control
URL filtering
IPSec
802.1x
Firewall

Security

IP Communications
Wireless

Networking

Cisco® Router and Security Device Manager (SDM)
Manage all security, routing and wireless

Network

OSPF
GRE
EIGRP
NHRP
NAT
IP Multicast
DHCP
NetFlow
NBAR
ACL
WAN
LAN
BGP
QoS
OER

Session Number
Presentation_ID
© 2005 Cisco Systems, Inc. All rights reserved.
Cisco Confidential
Clientless Access
Customizable Remote Application Access

- Clientless Web-based access allows anywhere access to network resources
- Web content transformation provides compatibility with Web pages containing HTML and JavaScript
- Uniform and efficient application delivery via fully clientless Citrix support
- Applications: Intranet (HTML and JavaScript), Citrix, Windows File Share (CIFS)
- Multiple browser support ensures broad connection compatibility
Java-based application helper supplements clientless access by providing connectivity to non-webified applications like:

- POP, SMTP, or IMAP e-mail
- Instant messaging
- Calendar
- Client-initiated TCP-based applications like Telnet
Cisco SSL VPN Client
Full Network Access

Leverages depth of Cisco® encryption client experience to deliver a lightweight, stable, and easy-to-support SSL VPN tunneling client

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec-like application access through “Web-pushed” client</td>
<td>Application-agnostic full network access</td>
</tr>
<tr>
<td>Touchless central site configuration</td>
<td>Low operating cost</td>
</tr>
<tr>
<td>Compatible with Cisco Softphone for VoIP support</td>
<td>Multimedia data, voice desktops for greatest user productivity</td>
</tr>
<tr>
<td>Client may be either removed at end of session or left permanently installed</td>
<td>No trace of client after session provides better security</td>
</tr>
<tr>
<td>Less than 250 KB download</td>
<td>Fast client download time</td>
</tr>
<tr>
<td>No reboot required after installation</td>
<td>Improved productivity, better user satisfaction</td>
</tr>
</tbody>
</table>
Cisco Secure Desktop
Security/Auditing Compliance

Issue: HIPAA, Sarbanes-Oxley, and numerous other regulations require privacy of sensitive information

Cisco® Secure Desktop eases regulatory compliance associated with remote access through:

– Easily demonstrated separation or “sandboxing” of all session data and downloaded content to compliance auditors

– Extensive logging for Cisco Secure Desktop activities

  Was it loaded on endpoint?
  Did it execute properly?

– Validation of remote system security posture prior to session initiation

– Full session data overwrite using government approved DoD sanitation algorithm
Cisco Secure Desktop
Comprehensive Endpoint Security for SSL VPN

Complete preconnect assessment:
Location assessment—managed or unmanaged desktop?
Security posture assessment—AV operational/up-to-date, personal firewall operational, malware present?

Comprehensive session protection:
• Data sandbox and encryption protects every aspect of session
• Malware detection with hooks to Microsoft free antispyware software

Post-session clean up:
• Encrypted partition overwrite (not just deletion) using DoD algorithm
• Cache, history, and cookie overwrite
• File download and e-mail attachment overwrite
• Auto-complete password overwrite

Works with desktop guest permissions
No admin privileges required
Use Case Scenario
Regional Law Firm with Multiple Offices

Small office

Site-to-Site VPN
Securely interconnect branch communications

Lawyer at courthouse

Remote access SSL VPN
• No software to install & maintain on PCs
• Secure access to Citrix, e-mail
• Endpoint security with Cisco Secure Desktop

Secure IPSec tunnel

Internet

Cisco® 2851 Integrated Services Router

Main office

Integrated VPN, security, routing, & IPC services
• Single box to operate and manage
• Up to 75 concurrent SSL VPN users
• Modular, future proof investment

Secure SSL VPN tunnel with Cisco Secure Desktop

Improved staff productivity—On-road access to business applications
Compliance with regulations—All remote communications fully encrypted and logged
Proactive threat defense—Application firewall, inline intrusion prevention, touchless end-point security (Cisco Secure Desktop)
Cisco Router and Security Device Manager (SDM) v2.3 – Delivers Ease of Use

- Fast and easy deployment and management of integrated services on Cisco IOS® routers
  - Easy-to-use, Web-based GUI for single device management
  - Loaded on router from factory at no additional cost
  - Less than 30 minutes to deploy fixed configuration ISRs
  - Featured on Cisco® 800—7301 routers
  - Supported in seven international languages

- What’s new (v2.3):
  - Integrated Cisco IOS WebVPN Management
    - Simple GUI-based provisioning and monitoring, step-by-step wizards for easy turnkey deployments
  - IPS security dashboard
    - Real-time updates on top threats with Cisco IPS Alert Center
  - Real-time network and application monitoring
    - NetFlow-based top N statistics, application traffic monitoring, search operations on event tables
  - On-box URL filtering management
    - Enables zero-touch provisioning for high-volume deployments
  - Simplified Cisco IOS Router image management

“Cisco Router and Security Device Manager significantly reduces technical expertise required to configure Cisco routers.”

ED MIER, MIERCOM
Cisco IOS WebVPN Wizard – WebVPN Gateway Creation

IP address and name of the WebVPN service
This is the IP address users will use to access the WebVPN portal page. If multiple WebVPN services are configured in this router, the unique name will be used to distinguish this service.

IP address: 172.28.54.95
Name: mycontext

URL users will use to login to this WebVPN service: https://172.28.54.95/mycontext

Digital certificate used for the WebVPN service
When users connect to the WebVPN portal page using a web browser, this digital certificate will be sent to their web browser. The browser will use this certificate to authenticate the router.

Certificate: SSLVPN
Cisco IOS WebVPN Wizard – WebVPN Full Tunnel Configuration Wizard

Full Tunnel
Download the full tunnel WebVPN client onto the user’s PC to have full tunnel connectivity. The client PC will get a new IP address from this router and will be part of the corporate network.

IP address pool
Create a new or select an existing address pool from which clients will be given an IP address when they connect.

IP address pool: sdm-pool

DNS and WINS Servers
Specify the domain name servers (DNS) and WINS servers that will be used to receive domain names and host names of corporate websites and windows servers.

Primary DNS Server: 172.26.54.1
Secondary DNS Server: 172.26.54.2
Primary WINS Server: 172.26.54.11
Secondary WINS Server: 172.26.54.12

Full Tunnel Client Software
The full tunnel client software should be installed on your router, so that it can be downloaded by clients when they connect to WebVPN service on this router. Specify the location of full tunnel software install bundle.

Location: c:\webvpn\svc.pkg

Click here to browse to www.cisco.com to get the latest WebVPN full tunnel client software.

Advanced Options
You can configure advanced options such as split tunneling, split DNS, Clients MSIE settings etc., by clicking on the Advanced... button.

Advanced...
Summary

Industry’s first router to integrate SSL VPN as a form of secure remote access connectivity

- Richest remote access and site-to-site secure access capabilities in the industry
- Cost-effective SSL VPN solution
- Integrating security in a router saves money and time
- Cisco® Secure Desktop and encryption supports burden-of-proof for regulatory compliance

- Cisco Router and Security Device Manager adds support for SSL VPN, IPS Security dashboard, and real-time network and application monitoring
ICSA-Certified Cisco IOS Firewall
What’s New in 12.4(6)T?

- Zone-based policy and SNMP MIB for easier administration
- Improved performance for faster session set up and bandwidth
- Improved resiliency through stateful failover
- Efficient shared state with inline intrusion prevention for improved performance

* Cisco® 3800/7200/7301 routers only