The SonicWALL SSL-VPN Series

Simple, Affordable, Secure and Clientless Remote Access

- ■ **Seamless integration behind virtually any firewall**

- ■ **Clientless connectivity**

- ■ **Unrestricted concurrent user tunnels**

- ■ **NetExtender technology**

- ■ **Granular policy configuration controls**

- ■ **Personalized portal experience**

- ■ **Enhanced layered security in a SonicWALL environment**

The dependency on mobile workers has increased and so has the need to provide secure remote access to network resources such as e-mail, files, intranets and applications. SonicWALL® introduces a solution to meet the needs of companies with remote workers. SonicWALL SSL-VPN security solutions for small to medium sized networks are simple to deploy and even easier to use. They provide organizations with secure remote network and application access for mobile employees at a fraction of the price of most other SSL-VPN solutions. And, unlike solutions that charge a per-tunnel licensing fee, SonicWALL SSL-VPN solutions have no restrictions on the number of concurrent user tunnels, allowing organizations to scale their remote access connectivity as they grow.

Remote access has never been so simple. Mobile employees only require a standard Web browser to log into a Web portal which provides access to e-mail, files, applications and internal Web sites. For even more powerful capabilities such as seamless, secure access to any resource on the corporate network including servers and complex or home-grown applications, the appliances transparently push a downloadable thin client (NetExtender) to the user's desktop or laptop.

Fitting seamlessly behind almost any firewall, the SSL-VPN 200 and SSL-VPN 2000 are very simple to deploy and manage. An intuitive graphical user interface guides the administrator quickly through the installation process and day-to-day maintenance. Moreover, the capability for granular policy configuration provides the administrator with complete and fine-grained control over individual user access to specific network resources.

Features and Benefits

Seamless integration behind virtually any firewall enables organizations to leverage the existing network infrastructure without the need to purchase additional hardware.

Clientless connectivity removes the need for a pre-installed or "fat" VPN client, thus freeing administrators from the tedious and costly task of installing and updating a client on users' PCs.

Offering **unrestricted concurrent user tunnels** instead of per-tunnel licensing significantly reduces the costs associated with deploying a scalable secure remote access solution.

NetExtender technology provides enhanced capabilities such as access to additional resources, services and applications on the corporate network.

Granular policy configuration controls enable network administrators to create policies that "lock down" a user to specific applications/resources and prevent unauthorized access to them.

Customizable Web interface provides a **personalized portal experience** and displays only those resources that are available to the user based on company policy.

Enhanced layered security is enabled when deployed alongside a SonicWALL Internet security appliance which utilizes powerful deep packet inspection technology to scan traffic for malicious threats such as viruses, worms, Trojans and spyware.
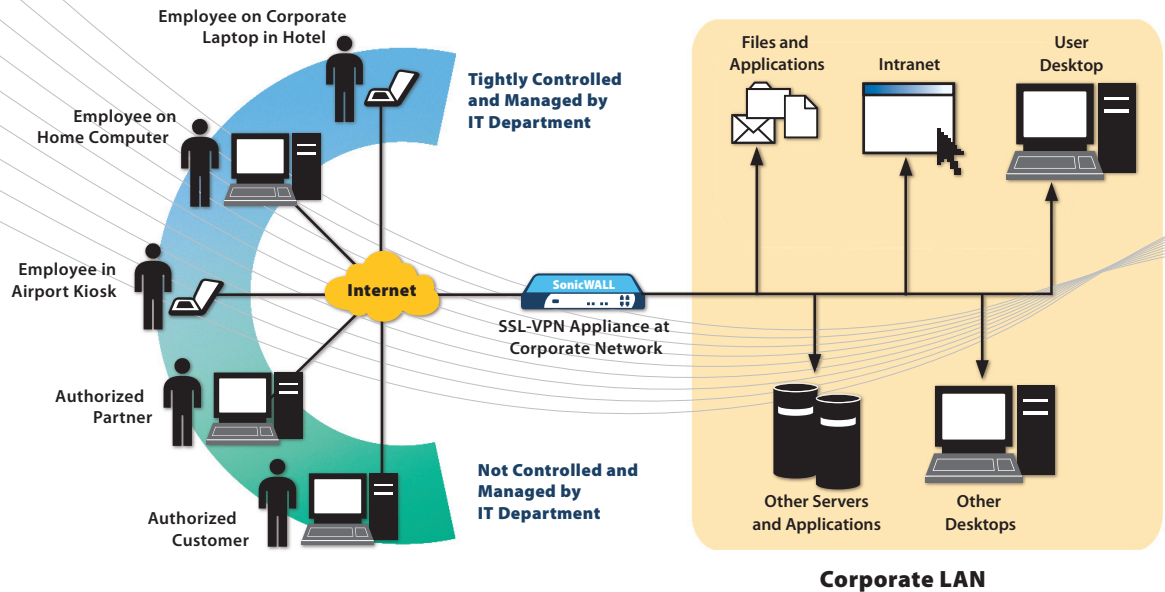
SONICWALL

Key Features

The SonicWALL SSL-VPN Series extends secure remote access beyond remote offices and corporate controlled laptops out to network environments and remote computers that are not controlled and managed by the corporate IT department.

Additionally, granular access controls enable the network administrator to provide not only employees but also trusted partners and customers with remote access to specific and defined resources.

Secure

remote access

that's easy

to use

and won't

break your

budget

Employee on Corporate Laptop in Hotel

Files and Applications

Intranet

User Desktop

Tightly Controlled and Managed by IT Department

Employee on Home Computer

Employee in Airport Kiosk

Internet

SonicWALL

SSL-VPN Appliance at Corporate Network

Authorized Partner

Authorized Customer

Not Controlled and Managed by IT Department

Other Servers and Applications

Other Desktops

Corporate LAN

SonicWALL SSL-VPN solutions can be configured to provide users with simple, secure and clientless remote access to a broad range of resources on the corporate network.

Using only a standard Web browser, users have access to:

- Files and file systems (Includes support for FTP and Windows Network File Sharing)
- Web-based applications
- Microsoft® Outlook Web access and other Web-enabled applications
- HTTP and HTTPS intranets

SonicWALL NetExtender technology provides expanded access to:

- E-mail access through native clients residing on the user's laptop (Microsoft Outlook, Lotus® Notes, etc.)
- Commercial and home-grown applications
- Flexible network access as granted by the network administrator

Added flexibility for access to:

- Applications installed on desktop machines or hosted on an application server
- Full remote control of desktop or server machines
- Terminal Services, VNC, Telnet and SSH

Cost effective alternative to traditional remote access products:

- Access to full remote control of the desktop— however unlike more traditional VNC and RDP, this requires no client software installation

Simple to Use, Simple to Manage

SonicWALL SSL-VPN solutions feature intuitive Web interfaces that simplify remote access and policy management from any location.
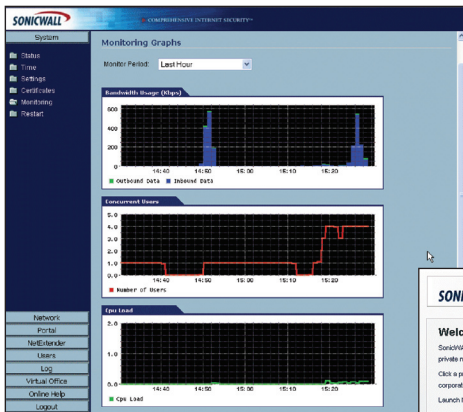
Secure, Easy-to-use Web Management Interface
Administrators will find SonicWALL SSL-VPN solutions very simple to deploy and manage. An easy-to-use graphical user interface makes it simple to configure, monitor and update the appliance and user policies. Additionally, the capability for granular policy configuration provides complete control over individual user access to specific network resources.
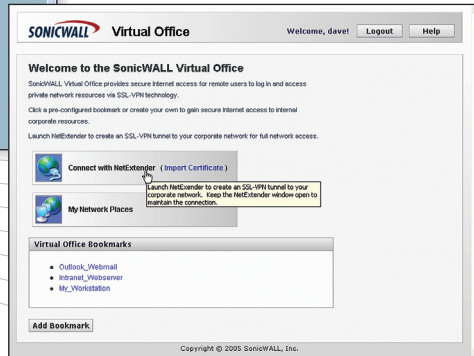
Personalized Portal Experience
Remote users require only a standard browser to launch a personalized Web portal. The user simply points the browser to a specific URL and the SSL-VPN portal automatically displays only those resources that are available to that individual based on company policy.

Seamless Integration Behind Virtually any Firewall

Behind third-party firewalls—SonicWALL SSL-VPN appliances integrate seamlessly into any network topology and can be easily deployed alongside any third-party firewall as a secure remote access solution. This enables IT administrators to leverage the existing network infrastructure without the need to purchase additional hardware.

Enhanced security when used in a SonicWALL network environment—
When deployed with a SonicWALL Internet security appliance running SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service*, SonicWALL SSL-VPN solutions provide enhanced network integration and security benefits.

Endpoint security enforcement
By deploying SonicWALL NetExtender and Network Anti-Virus *plus* Anti-Spyware* on managed PCs, administrators can configure policies that require every computer accessing the network has the most recent version of anti-virus and anti-spyware software installed and active.

* Sold separately
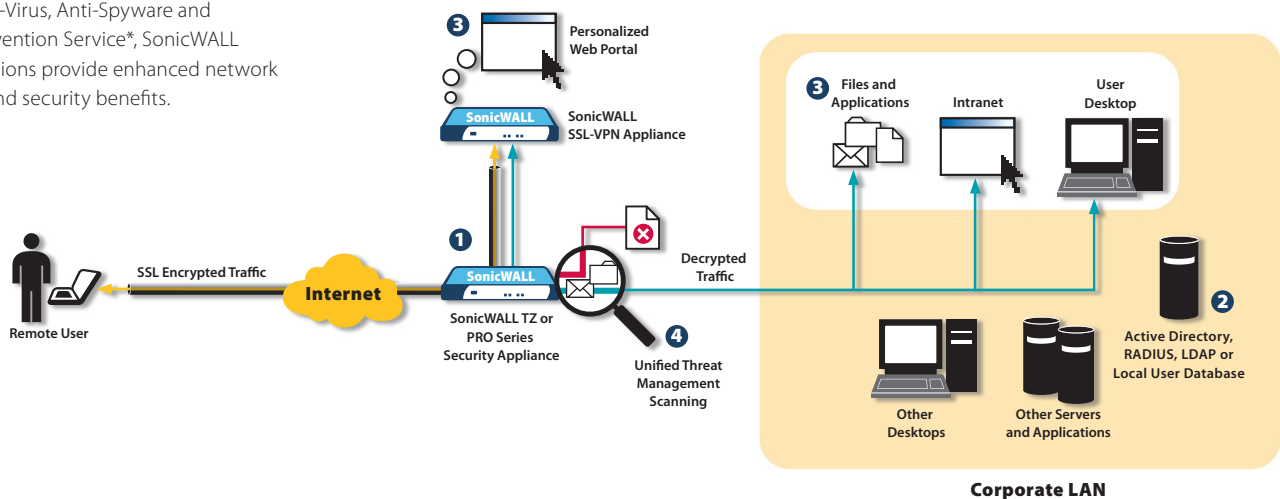
❶ Incoming HTTPS traffic is seamlessly forwarded by the TZ or PRO Series firewall to the SSL-VPN appliance which decrypts and authenticates network traffic.

❷ Users are authenticated using the onboard database or through third-party authentication methods such as RADIUS, LDAP, Microsoft Active Directory or Windows NT Domain.

❸ A personalized Web portal provides access to only those resources that the user is authorized to view based on company policies.

❹ Traffic is passed back to the PRO or TZ Series firewall where it is fully inspected for viruses, worms, Trojans, spyware and other sophisticated threats by the SonicWALL Unified Threat Management solution.

SonicWALL SSL-VPN Series

Performance

SSL-VPN 200	Recommended for organizations with 50 or fewer employees
Concurrent User License	Unrestricted
Recommended Maximum Concurrent Users	
Assuming Common Usage Scenarios	10
Assuming Heavy Usage Scenarios*	5
SSL-VPN 2000	Recommended for organizations with 1,000 or fewer employees
Concurrent User License	Unrestricted
Recommended Maximum Concurrent Users	
Assuming Common Usage Scenarios	100
Assuming Heavy Usage Scenarios*	50

Key Features

Applications Supported	
Proxy	HTTP, HTTPS, FTP, SSH, Telnet, RDP, VNC, Windows® file sharing (Windows SMB/CIFS)
NetExtender	Any TCP/IP based application: ICMP, Citrix, VoIP, IMAP, POP, SMTP, etc.
Encryption	DES (128), 3DES (128, 256), AES (128, 192, 256), ARC4 (128), MD5, SHA-1
Authentication	Internal user database, RADIUS, LDAP, Microsoft Active Directory, Windows NT Domain
Multiple Domain Support	Yes
Fine Grain Access control	At the user, user group and network resource level
Session Security	Inactivity timeouts prevent unauthorized use of inactive sessions
Certificates	
Server	Self-signed with editable common name and and imported from third parties
Client	Optional client certificates supported
Cache Cleaner	Optional. Upon logout all cached downloads, cookies and URLs downloaded through the SSL tunnel are erased from the remote computer
Client PC Operating Systems Supported	
Proxy	All operating systems
NetExtender	Windows 2000, 2003, XP
Web Browsers Supported	Microsoft Internet Explorer, Firefox Mozilla
Personalized Portal	The remote user sees only those resources that the administrator has granted access to based on company policy
Management	Web GUI (HTTP, HTTPS)
Usage Monitoring	Graphic monitoring of memory, CPU, users and bandwidth usage (SSL-VPN 2000 only)
Logging	Detailed logging in an easy-to-read format, Syslog supported e-mail alerts
Single-Arm Mode	Yes

*Requiring, for example, continuous downloading of files
**Defined as multiple concurrent HTTP, HTTPS and FTP proxy sessions

Hardware

Hardened Security Appliance	
SSL-VPN 200	Yes
SSL-VPN 2000	Yes
Cryptographic Hardware Acceleration	
SSL-VPN 200	Yes
SSL-VPN 2000	Yes
Interfaces	
SSL-VPN 200	(5) 10/100 Ethernet
SSL-VPN 2000	(4) 10/100 Ethernet, (1) Serial port
Processors	
SSL-VPN 200	SonicWALL security processor, cryptographic accelerator
SSL-VPN 2000	x86 main processor, cryptographic accelerator
Memory (RAM)	
SSL-VPN 200	128 MB
SSL-VPN 2000	512 MB
Flash Memory	
SSL-VPN 200	16 MB
SSL-VPN 2000	128 MB
Power Supply	
SSL-VPN 200	20W, 12VDC, 1.66A
SSL-VPN 2000	Internal
Max Power Consumption	
SSL-VPN 200	10.4 W
SSL-VPN 2000	48 W
Total Heat Dissipation	
SSL-VPN 200	35.6 BTU
SSL-VPN 2000	163.7 BTU
Dimensions	
SSL-VPN 200	7.45 x 4.55 x 1.06 in 18.92 x 11.56 x 2.69 cm
SSL-VPN 2000	17.00 x 10.00 x 1.75 in 43.18 x 25.40 x 4.45 cm
Weight	
SSL-VPN 200	1.25 lbs 0.57 kg
SSL-VPN 2000	8.50 lbs 3.86 kg
Major Regulatory Compliance	FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, MIC, NOM, UL, cUL, TUV/GS, CB
Environment	40-105° F, 5-40° C Humidity 10-90% non-condensing
MTBF	
SSL-VPN 200	9.0 years
SSL-VPN 2000	11.2 years

SonicWALL SSL-VPN 200
(US/Canada)
01-SSC-5946

SonicWALL Support 8x5
01-SSC-5642

SonicWALL Support 24x7
01-SSC-5643

SonicWALL SSL-VPN 2000
(US/Canada)
01-SSC-5952

SonicWALL Support 8x5
01-SSC-5646

SonicWALL Support 24x7
01-SSC-5647

SonicWALL Value-added Security Services

SonicWALL SSL-VPN solutions integrate seamlessly behind virtually any firewall. In addition, when the SSL-VPN appliance is deployed alongside a SonicWALL Internet security appliance, traffic can be fully inspected for content-based threats such as viruses, spyware and Trojans prior to being forwarded to its final destination on the network.

For more information on SonicWALL security services, including gateway anti-virus, anti-spyware, intrusion prevention and content filtering, please visit our Web site at **http://www.sonicwall.com/products/vpnsoft.html**.