SonicWALL Secure Remote Access Series
for the SMB

Easy-to-use, affordable and clientless secure remote access

- **Seamless integration behind virtually any firewall**
- **Clientless connectivity**
- **NetExtender technology**
- **Granular policy configuration controls**
- **Personalized Web portal**
- **Remote support**
- **Tokenless two-factor authentication**
- **Mobile device support**
- **Application offloading**
- **Context-sensitive help**
- **Enhanced layered security in a SonicWALL environment**

In recent years, there has been an increased dependence on mobile workers. This has prompted a need for providing secure remote access to network resources as well as remote control PC access. SonicWALL® provides a solution that meets the needs of organizations with demanding remote workforce requirements. SonicWALL Secure Remote Access (SRA) solutions are simple to deploy and even easier to use for a fraction of the price of most other products.

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

Remote support is also easy to implement using SonicWALL Virtual Assist.* It is a clientless tool that enables a technician to assume control of a customer's computer in order to provide assistance. As a result, service can be provided on-demand while keeping costs low.

Features and Benefits

Seamless integration behind virtually any firewall enables organizations to leverage the existing network infrastructure.

Clientless connectivity removes the need for a pre-installed VPN client, thus freeing administrators from a tedious and costly task.

NetExtender technology enables network level access to resources, services and applications.

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.

A **personalized Web portal** displays only those resources that are available to the user based on company policy.

Remote support using SonicWALL Virtual Assist* enables technicians to provide secure on-demand assistance to customers while leveraging the existing infrastructure.

Tokenless two-factor authentication provides enhanced protection against key loggers by combining a unique one-time password, generated by the SSL VPN appliance and sent to a remote user's mobile device or e-mail address, with the user's network user name and password.

Mobile device support to access an entire intranet as well as Web-based applications provides greater flexibility for a remote workforce.

Application offloading** enables users to access Web applications securely by leveraging strong authentication and granular access policy features.

Context-sensitive help is provided throughout the administrative interface and end-user portal, increasing management flexibility and ease-of-use.

Enhanced layered security is enabled when deployed alongside a SonicWALL Network Security Appliance which utilizes powerful deep packet inspection technology to scan traffic for malicious threats such as viruses, worms, Trojans and spyware. The combined solution is known as SonicWALL Clean VPN.
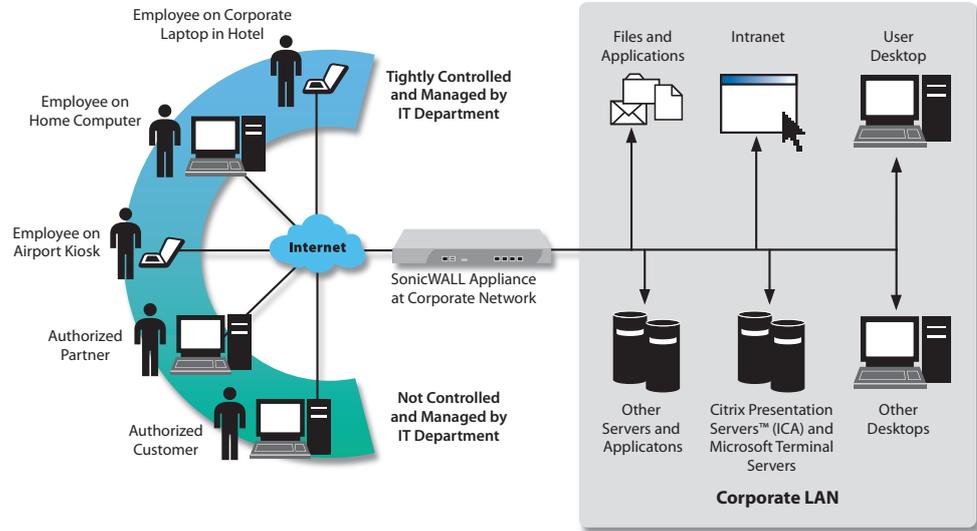
SONICWALL®

Granular Access to Authorized Users

The SonicWALL Secure Remote Access (SRA) Series for small- to medium-sized businesses (SMB) extends secure remote access beyond managed employees to unmanaged remote employees, partners, and customers. A customizable portal enables users to access specific resources via a Web browser as defined by a company's IT policy.

Secure

remote access

that's easy to

deploy, use and

won't break

your budget

Employee on Corporate Laptop in Hotel

Employee on Home Computer

Employee on Airport Kiosk

Internet

Authorized Partner

Authorized Customer

Tightly Controlled and Managed by IT Department

SonicWALL Appliance at Corporate Network

Not Controlled and Managed by IT Department

Files and Applications — Intranet — User Desktop

Other Servers and Applicatons

Citrix Presentation Servers™ (ICA) and Microsoft Terminal Servers

Other Desktops

Corporate LAN

Awards

(SSL-VPN 200)

Certifications

(SSL-VPN 200/4000)

(SSL-VPN 4000)

Broad Access to Resources

SonicWALL SRA solutions for SMB can be used to provide users with access to a broad range of resources.

- NetExtender enables native access to corporate network applications such as Microsoft® Outlook

- The Virtual Office portal enables Web-based access to intranet (HTTP, HTTPS), file (FTP, CIFS), desktop (Citrix®*, Terminal Server, VNC), and terminal (Telnet, SSH) resources

Simple to Manage

SonicWALL SSL VPN solutions feature an intuitive Web-based management interface which offers context sensitive help to enhance usability. In addition, multiple products can be centrally managed using the SonicWALL Global Management System (GMS v4.0+). Resource access via the products can be effortlessly monitored using the SonicWALL ViewPoint reporting tool.
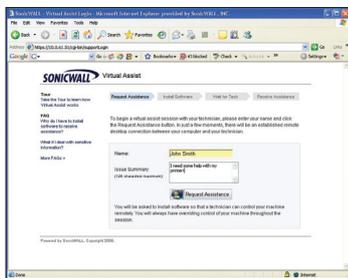
Remote Support

SonicWALL Virtual Assist* can be easily configured and licensed via the administrative interface as a cost effective alternative to traditional remote support tools. Browser-based thin clients are pushed to Technicians and Customers in order to establish a session through the cloud via an SSL VPN product.
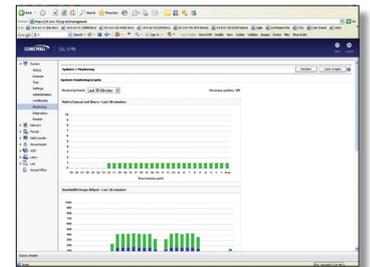
Enhanced Solution

SonicWALL Secure Remote Access appliances integrate seamlessly into virtually any network topology and can be easily deployed alongside any third-party firewall. When deployed with a SonicWALL Network Security/Unified Threat Management (UTM) firewall appliance running Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service along with Application Firewall, enhanced security benefits are realized. Moreover, endpoint security can be enforced by deploying NetExtender in conjunction with Enforced Client Anti-Virus and Anti-Spyware on managed PCs. Virtual Assist also benefits from the seamless integration by leveraging the appliance's local and external authentication facilities.

*Available only on the SSL-VPN 4000 and SRA 4200

Remote Access Solution

With an increasingly mobile workforce and greater threats of unexpected disruptions, remote access has become a business necessity. A SonicWALL SRA appliances for the SMB product deployed in one-arm mode alongside a SonicWALL UTM product or virtually any other third party firewall enables remote users to securely access corporate network resources from anywhere outside the LAN.
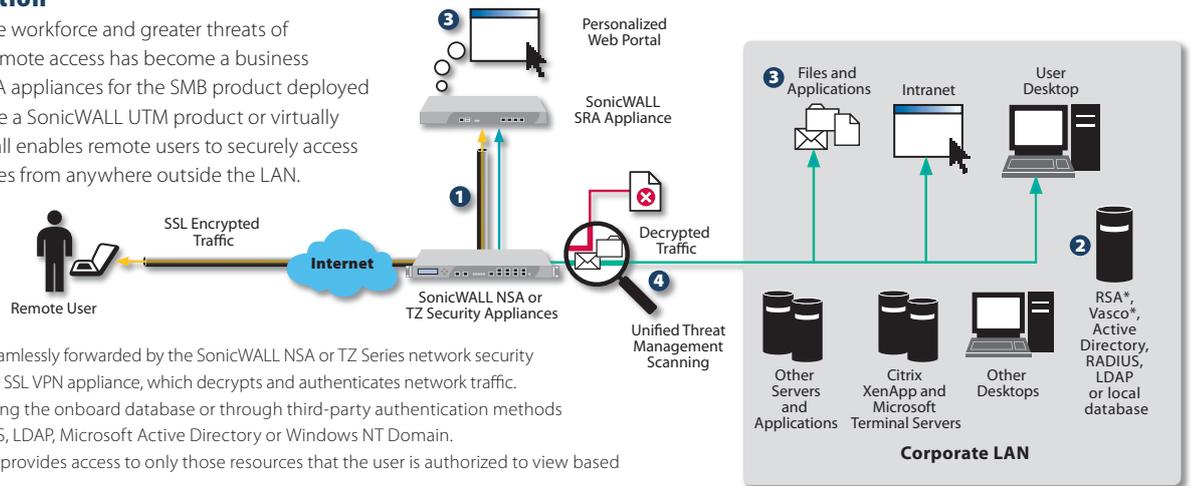
❶ Incoming HTTPS traffic is seamlessly forwarded by the SonicWALL NSA or TZ Series network security appliance to the SonicWALL SSL VPN appliance, which decrypts and authenticates network traffic.

❷ Users are authenticated using the onboard database or through third-party authentication methods such as RSA*, Vasco, 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 NSA or TZ Series network security appliance where it is fully inspected for viruses, worms, Trojans, spyware and other sophisticated threats by the SonicWALL Unified Threat Management solution.

**Available only on the SRA 4200 and SSL-VPN 4000
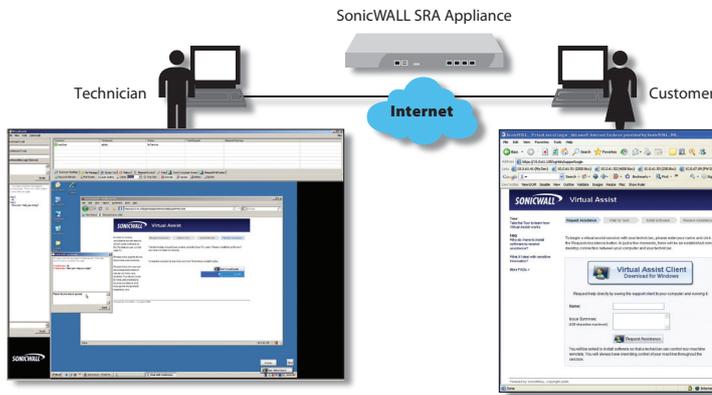
Remote Support Solution

With more employees working remotely and customers dispersed globally, it is becoming increasingly important for organizations to provide remote support for off-site business devices such as laptops or home PCs. Ineffective support using expensive and cumbersome tools can undermine IT service level agreements and inhibit remote worker productivity. Using a SonicWALL Virtual Assist on an SSL-VPN 4000 or SRA 4200 appliance, a Technician can instantly access a remote device over the Web, transfer files, and chat with the end user, enabling rapid diagnosis and problem resolution, without the need for pre-installed "fat" client.

Disaster Recovery Solution

Disaster recovery can be triggered by a catastrophic event like a hurricane or epidemic, or by something as simple as a regional power outage, severe weather, flu outbreaks, or flooding of an office building because of a burst water pipe. Business disruption can mean lost opportunities, revenues, or reputation. SonicWALL SSL VPN and CDP products with a subscription to SonicWALL CDP Offsite Data Backup Service enable employees that are not able to physically get to the corporate office, access your corporate resources remotely via a secure SSL VPN connection. Corporate resources are always accessible as they are backed up both locally and offsite.
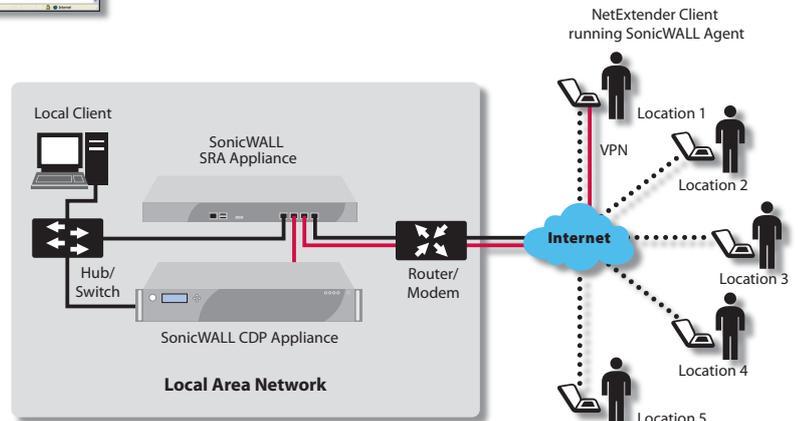
Wireless Authentication
The SonicWALL appliance can be configured to authenticate WLAN users, granting these users access to internal resources while keeping the session secure. The benefit to this method of acccess is "clientless" access from the WLAN.
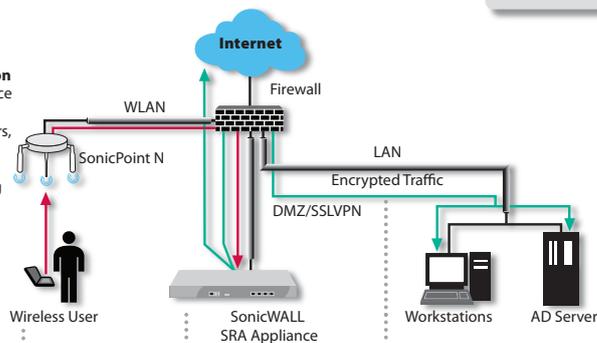
Step 1:
Wireless user obtains DHCP lease on the WLAN network.

Step 2:
When browser is opened, the user is redirected to the appliance and prompted for authentication.

Step 3:
Once authenticated, the user can open a NetExtender session which will create a "tunnel all" route from the client's system to the appliance. The user will be given a NetExtender client subnet and can now access internal and external resources.

Clean Wireless Solution

More corporations, universities, hospitals and governmental organizations are implementing wireless networks and using SSL VPN as a secure and centralized access control solution. SonicWALL SSL VPNs integrate seamlessly with SonicWALL wireless access solutions. A SonicWALL SSL VPN deployed alongside a SonicWALL UTM firewall and several SonicPoints ensure that users get access from anywhere on campus and the wireless connections are encrypted via the SSL protocol. As an added bonus, remote workers away from campus can connect into the corporate network via an SSL VPN connection. IT maintains centralized, granular access control over who can access what resources from using a single gateway.

Specifications

Performance

SSL-VPN 200	Recommended for organizations with 50 or fewer employees
Concurrent User License:	Unrestricted
Recommended Maximum Concurrent Users:	10
SRA 4200	Recommended for organizations with 500 or fewer employees
Maximum allowable concurrent Virtual Assist technicians:	5
Concurrent User License:	Unrestricted
Recommended Maximum Concurrent Users:	50
SSL-VPN 4000	Recommended for organizations with 500 or more employees
Maximum allowable concurrent Virtual Assist technicians:	25
Concurrent User License:	Unrestricted
Recommended Maximum Concurrent Users:	200

Key Features

Applications Supported	
Proxy	Citrix (ICA),* HTTP, HTTPS, FTP, SSH, Telnet, RDP, VNC, Windows® file sharing (Windows SMB/CIFS)
NetExtender	Any TCP/IP based application: ICMP, VoIP, IMAP, POP, SMTP, etc.
Encryption	DES (128), 3DES (128, 256), AES (128, 192, 256), ARC4 (128), MD5, SHA-1
Authentication	RSA,* Vasco, One-time Passwords, 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	Configurable. 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/Vista (32-bit and 64-bit) Win Mobile 5 (Pocket PC), Win Mobile 6 (Classic/Professional), MacOS 10.4+ (PowerPC and Intel), Linux Fedora Core 3+ / Ubuntu 7+ / OpenSUSE
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), Send syslog and heartbeat messages to GMS (4.0 and higher)
Usage Monitoring	Graphical monitoring of memory, CPU, users and bandwidth usage*
Logging	Detailed logging in an easy-to-read format, Syslog supported e-mail alerts
Single-Arm Mode	Yes
SonicWALL Virtual Assist*	Connection to remote PC, chat, FTP and diagnostic tools
IPv6 Support*	Basic
Application offloading*	Yes

Hardware

Hardened Security Appliance		
	SSL-VPN 200	Yes
	SRA 4200	Yes
	SSL-VPN 4000	Yes
Cryptographic Hardware Acceleration		
	SSL-VPN 200	Yes
	SRA 4200	Yes
	SSL-VPN 4000	Yes
Interfaces		
	SSL-VPN 200	(5) 10/100 Ethernet
	SRA 4200	(4) Gigabit Ethernet, (2) USB, (1) Console
	SSL-VPN 4000	(6) 10/100 Ethernet, (1) Serial port
Processors		
	SSL-VPN 200	SonicWALL security processor, cryptographic accelerator
	SRA 4200	x86 main processor, cryptographic accelerator
	SSL-VPN 4000	P4 Celeron main processor, cryptographic accelerator
Memory (RAM)		
	SSL-VPN 200	128 MB
	SRA 4200	2 GB
	SSL-VPN 4000	1 GB
Flash Memory		
	SSL-VPN 200	16 MB
	SRA 4200	1 GB
	SSL-VPN 4000	128 MB
Power Supply		
	SSL-VPN 200	20W, 12VDC, 1.66A
	SRA 4200	Internal
	SSL-VPN 4000	Internal
Max Power Consumption		
	SSL-VPN 200	10.4 W
	SRA 4200	75 W
	SSL-VPN 4000	108 W
Total Heat Dissipation		
	SSL-VPN 200	35.6 BTU
	SRA 4200	256.0 BTU
	SSL-VPN 4000	368.3 BTU
Dimensions		
	SSL-VPN 200	7.45 x 4.55 x 1.06 in 18.92 x 11.56 x 2.69 cm
	SRA 4200	17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm
	SSL-VPN 4000	17.00 x 13.25 x 1.75 in 43.18 x 33.66 x 4.45 cm
Weight		
	SSL-VPN 200	3.00 lbs 1.36 kg
	SRA 4200	15.00 lbs 6.80 kgs
	SSL-VPN 4000	18.50 lbs 8.39 kg
Major Regulatory Compliance		FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, MIC, NOM, UL, cUL, TUV/GS, CB
Environment		32-105° F, 0-40° C Humidity 5-95% RH, non-condensing
MTBF		
	SSL-VPN 200	9.0 years
	SRA 4200	8.3 years
	SSL-VPN 4000	9.2 years

Available only on the SSL-VPN 4000 and SRA 4200

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

SonicWALL Dynamic Support
8x5 (1-year)
01-SSC-5642

SonicWALL Dynamic Support
8x5 (2-year)
01-SSC-6244

SonicWALL Dynamic Support
8x5 (3-year)
01-SSC-6245

SonicWALL Dynamic Support
24x7 (1-year)
01-SSC-5643

SonicWALL Dynamic Support
24x7 (2-year)
01-SSC-6246

SonicWALL Dynamic Support
24x7 (3-year)
01-SSC-6247

SonicWALL SRA 4200
50 User
01-SSC-5980

SonicWALL Dynamic Support 8x5
Up to 50 users (1-year)
01-SSC-5687

SonicWALL Dynamic Support 8x5
Up to 50 users (2-year)
01-SSC-5988

SonicWALL Dynamic Support 8x5
Up to 50 users (3-year)
01-SSC-5989

SonicWALL Dynamic Support 24x7
Up to 50 users (1-year)
01-SSC-5984

SonicWALL Dynamic Support 24x7
Up to 50 users (2-year)
01-SSC-5985

SonicWALL Dynamic Support 24x7
Up to 50 users (3-year)
01-SSC-5986

SonicWALL SSL-VPN 4000
(US/Canada)
01-SSC-5960

SonicWALL Dynamic Support
8x5 (1-year)
01-SSC-6248

SonicWALL Dynamic Support
8x5 (2-year)
01-SSC-6249

SonicWALL Dynamic Support
8x5 (3-year)
01-SSC-6250

SonicWALL Dynamic Support
24x7 (1-year)
01-SSC-6251

SonicWALL Dynamic Support
24x7 (2-year)
01-SSC-6252

SonicWALL Dynamic Support
24x7 (3-year)
01-SSC-6253

For more information on SonicWALL Secure Remote Access for SMB solutions, visit **www.sonicwall.com**.