SonicWALL Secure Remote Access Series

Easy-To-Use, Affordable and Clientless Secure Remote Access

- **Seamless integration behind virtually any firewall**
- **NetExtender technology**
- **Personalized Web portal**
- **Remote support**
- **Remote PC control**
- **Web Application Firewall Service**
- **Tokenless two-factor authentication**
- **Mobile device support**
- **Load Balancing**
- **High Availability**
- **Unified Policy**
- **SonicWALL Clean VPN**

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 PC control. SonicWALL® provides a solution that meets the needs of organizations with demanding remote workforce requirements. SonicWALL Secure Remote Access (SRA) Series™ solutions, flexibly deployable as a hardware or a virtual appliance, are simple to implement and even easier to use for a fraction of the price of most other products.

Remote access has never been so simple to deploy and use. Mobile employees only require a standard browser to log into a customizable portal that provides access to email, 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.

SonicWALL Virtual Assist/Virtual Access can be easily configured and licensed via the administrative interface as a cost-effective alternative to either traditional remote support tools or remote PC access productivity tools. Browser-based Virtual Assist thin clients can be pushed to technicians and customers to establish an interactive support session using SonicWALL SRA. Alternatively, Virtual Access can increase productivity by enabling IT administrators or authorized end users to gain secure remote access to their unattended Windows-based computers from anywhere via SonicWALL SRA.

Features and Benefits

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

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

A **personalized Web portal** displays only the 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.

Remote PC control using SonicWALL Virtual Access enables administrators or authorized end users to gain secure remote control of their unattended Windows-based computers from anywhere.

Web Application Firewall Service* detects and protects Web applications (including the SSL VPN appliance itself) from Web-based attacks, reducing potential losses and adhering to data protection compliance mandates.

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 email 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.

Load Balancing can be deployed to partition requests across multiple Web servers.

High Availability allows administrators to deploy an active-backup pair of appliances to enhance uptime while reliably providing security for remote access users.

Unified Policy displays granular bookmarks and policies in one centralized page, streamlining configuration, troubleshooting and administrative overhead. Administrators can easily create policies that can restrict user access to specific applications or resources, and prevent unauthorized access.
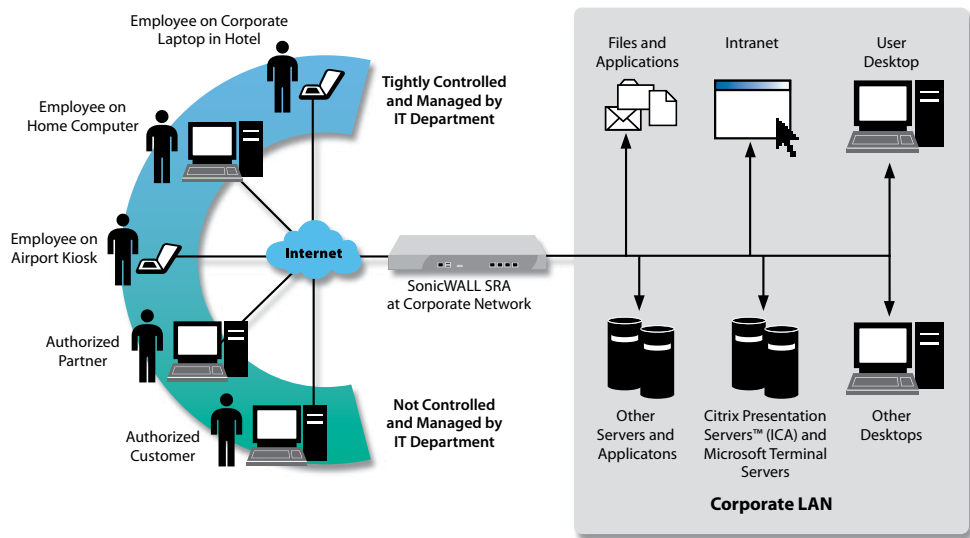
SonicWALL Clean VPN™ both secures the integrity of VPN access and decontaminates malicious threats before they can enter the corporate network through combined deployment with a SonicWALL firewall.

*Additional license required; available as a software add-on module

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Granular Access to Authorized Users

The SonicWALL Secure Remote Access (SRA) Series for small- to medium-sized businesses (SMBs) extends secure remote access beyond managed employees to unmanaged remote employees, partners, and customers without compromising security, by employing fine-grained access controls.

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

Authorized Partner

Authorized Customer

Internet

Tightly Controlled and Managed by IT Department

Not Controlled and Managed by IT Department

SonicWALL SRA at Corporate Network

Files and Applications

Intranet

User Desktop

Other Servers and Applicatons

Citrix Presentation Servers™ (ICA) and Microsoft Terminal Servers

Other Desktops

Corporate LAN

Broad Access to Resources

SonicWALL SRA Series 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
- If an application supports URL rewriting, it can be accessed by bookmarks; otherwise, by offloading

Simple to Manage

SonicWALL SRA solutions feature Unified Policy and an intuitive Web-based management interface that offers context-sensitive help to enhance usability. In addition, multiple products can be centrally managed using the SonicWALL Global Management System (GMS 4.0+). Resource access via the products can be effortlessly monitored using the SonicWALL ViewPoint® reporting tool.

Remote PC Control

In organizations with distributed or branch locations, secondary disaster recovery sites, outsourced managed services or teleworkers, an administrator, technician, trusted service provider or authorized employee may require full control of specific PCs within the LAN from remote locations. SonicWALL Virtual Assist licensed with Virtual Access, enhances productivity by enabling secure remote control of unattended Windows-based computer desktops.

Enhanced Solution

SonicWALL Secure Remote Access Series appliances integrate seamlessly into almost any network topology and can be easily deployed alongside virtually any third-party firewall. Deployment with a SonicWALL firewall running Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service along with Application Intelligence and Control further enhances security benefits. Deploying NetExtender in conjunction with Enforced Client Anti-Virus and Anti-Spyware on managed PCs enforces endpoint security. Virtual Assist also offers seamless integration by leveraging the appliance's local and external authentication facilities. Furthermore, Web Application Firewall Service applies reverse proxy analysis of Layer 7 traffic against known signatures, denies access upon detecting Web application malware, and redirects users to an explanatory error page, by utilizing a dynamically updated signature database to detect sophisticated Web-based attacks and protect Web applications including SSL VPN portals.

Awards

Personal Computer World
BUSINESS
RECOMMENDED

ITR
IT Reviews

Certifications

VASCO Certified

VASCO READY

(SRA 1200, SRA 4200)

RSA SECURED®

Remote Access Solution

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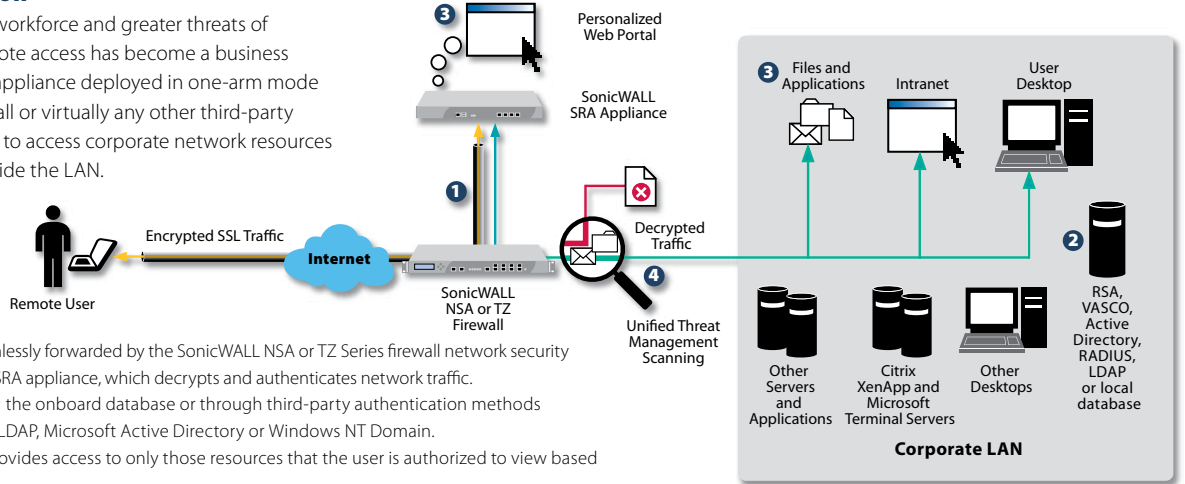
❶ Incoming HTTPS traffic is seamlessly forwarded by the SonicWALL NSA or TZ Series firewall network security appliance to the SonicWALL SRA appliance, which decrypts and authenticates network traffic.

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 To create a Clean VPN environment, traffic is passed through to the NSA or TZ Series firewall (running Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Services where it is fully inspected for viruses, worms, Trojans, spyware and other sophisticated threats.
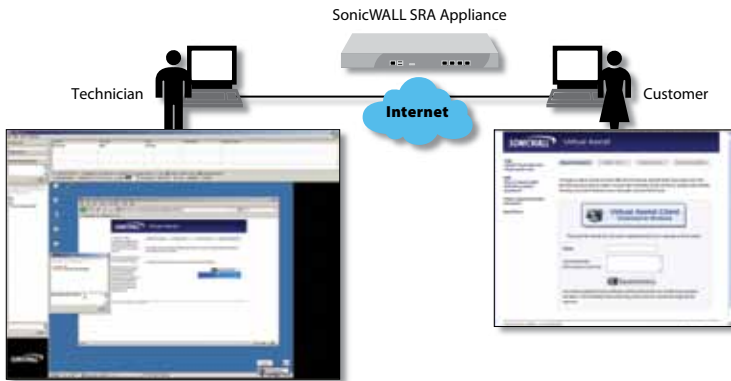
Remote Support Solution

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 and home PCs. Ineffective support using expensive and cumbersome tools can undermine IT service level agreements and inhibit remote worker productivity. Using SonicWALL Virtual Assist on a SRA 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 a pre-installed "fat" client.

Web Application Firewall and PCI Compliance

Available as a licensed service, SonicWALL's Web Application Firewall (WAF) Service allows customers to protect their Web applications against Web-based attacks. WAF provides automatic signature updates for continuous malware protection and intrusion prevention. It can be used in conjunction with strong two-factor authentication which SSL VPN technology provides to control Web site access. By protecting against common protocol and Web-based vulnerabilities, WAF can significantly help financial, healthcare, e-commerce, e-billing and other related businesses attain PCI compliance. It also provides acceleration features such as content caching which can significantly improve the performance of protected Web sites.
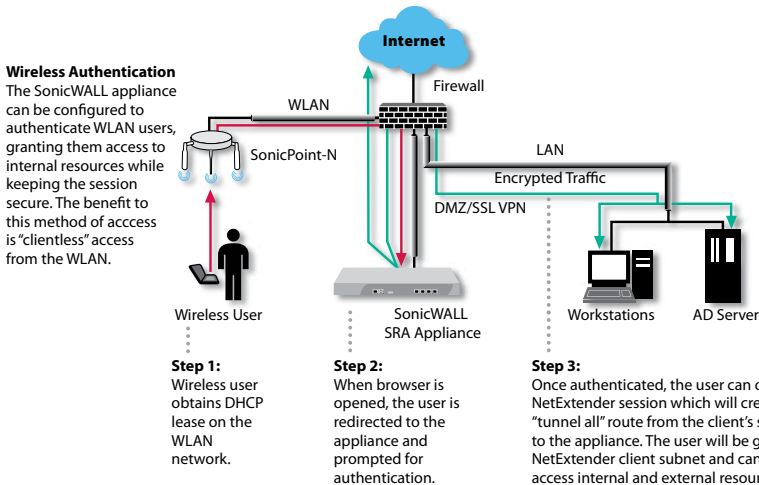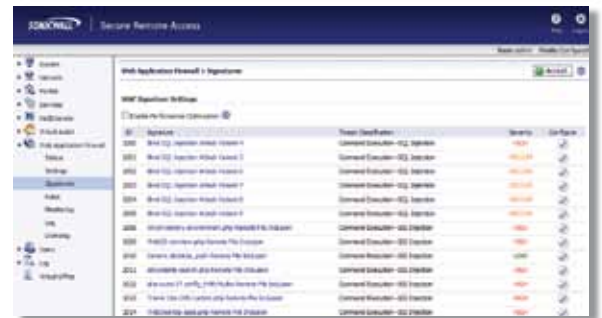
Wireless Authentication
The SonicWALL appliance can be configured to authenticate WLAN users, granting them access to internal resources while keeping the session secure. The benefit to this method of access is "clientless" access from the WLAN.

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 VPN Remote Access 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. When deployed alongside a SonicWALL firewall (running Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Services and several SonicPoints, a SonicWALL SSL VPN solution ensures 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 using a single gateway.

Specifications

SonicWALL SRA 1200, 5 User
01-SSC-6063

SRA 1200 Additional Users
(50 User Maximum)
Add 1 Concurrent User
01-SSC-6067
Add 5 Concurrent Users
01-SSC-6068
Add 10 Concurrent Users
01-SSC-6069

SRA 1200 Support
SonicWALL Dynamic Support 24x7
for up to 25 Users (1-year)
01-SSC-8868
SonicWALL Dynamic Support 8x5
for up to 25 Users (1-year)
01-SSC-8871

SonicWALL SRA 4200, 25 User
01-SSC-5998

SRA 4200 Additional Users
(500 User Maximum)
Add 10 Concurrent Users
01-SSC-5599
Add 25 Concurrent Users
01-SSC-6005
Add 100 Concurrent Users
01-SSC-6012

SRA 4200 Support
SonicWALL Dynamic Support 24x7
for up to 100 Users (1-year)*
01-SSC-6013
SonicWALL Dynamic Support 8x5
for up to 100 users (1-year)*
01-SSC-6022
SonicWALL Dynamic Support 24x7
for 101 to 500 users (1-year)*
01-SSC-6029
SonicWALL Dynamic Support 8x5
for 101 to 500 users (1-year)*
01-SSC-6035

SRA Virtual Appliance
SonicWALL SRA Virtual Appliance, 5 User
01-SSC-8469

**SRA Virtual Appliance
Additional Users**
(50 User Maximum)
Add 5 Concurrent Users
01-SSC-9182
Add 10 Concurrent Users
01-SSC-9183
Add 25 Concurrent Users
01-SSC-9184

SRA Virtual Appliance Support
SonicWALL Dynamic Support 8x5
for up to 25 Users (1-year)*
01-SSC-9188
SonicWALL Dynamic Support 24x7
for up to 25 users (1-year)*
01-SSC-9191
SonicWALL Dynamic Support 8x5
for up to 50 Users (1-year)*
01-SSC-9194
SonicWALL Dynamic Support 24x7
for up to 50 users (1-year)*
01-SSC-9197

*Multi-year support SKUs are available

Performance

SRA 1200 — Recommended for organizations with 50 or fewer employees

Concurrent User License:	Starts with 5 concurrent users. Additional user licenses available in 5 and 10 user increments.
Maximum allowable concurrent Virtual Assist technicians:	10
Maximum Concurrent Users:	50

SRA 4200 — Recommended for organizations with 500 or fewer employees

Concurrent User License:	Starts with 5 users/15 day trial license
Maximum allowable concurrent Virtual Assist technicians:	25
Maximum Concurrent Users:	500

SRA Virtual Appliance — Recommended for organizations of any size

Concurrent User License:	User licenses available in 5, 10, and 25 user increments
Maximum allowable concurrent Virtual Assist technicians:	25
Maximum Concurrent Users:	50

Key Features

Applications Supported

Proxy	Citrix (ICA), HTTP, HTTPS, FTP, SSH, Telnet, RDP, VNC, Windows® file sharing (Windows SMB/CIFS), OWA 2003/2007/2010
NetExtender	Any TCP/IP based application: ICMP, VoIP, IMAP, POP, SMTP, etc.

Encryption	ARC4 (128), MD5, SHA-1, SSLv3, TLSv1, 3DES (168, 256), AES (256), SHA-1, RSA, DHE
Authentication	RSA, Vasco, One-time Passwords, Internal user database RADIUS, LDAP, Microsoft, Active Directory, Windows NT Domain
RDP Support	Yes. Terminal Server farm and Remote Application support included.
Multiple Domain Support	Yes
Multiple Portal 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), 7 (32-bit and 64-bit), Win Mobile 6.5 (Pocket PC), Win Mobile 6.5 (Classic/Professional), MacOS 10.4+ and SnowLeopard (PowerPC and Intel), Linux Fedora Core 3+ / Ubuntu 7+ / OpenSUSE, Linux 64-bit, Google® Android

Web Browsers Supported	Microsoft Internet Explorer, Firefox Mozilla, Chrome, Opera, Safari
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) SNMP Support
Usage Monitoring	Graphical monitoring of memory, CPU, users and bandwidth usage
Unified Policy	Yes. Also supports policies which have multiple AD groups
Logging	Detailed logging in an easy-to-read format, Syslog supported email alerts

Single-Arm Mode	Yes
SonicWALL Virtual Assist or Virtual Access (licensed together)	Connection to remote PC, chat, FTP and diagnostic tools
IPv6 Support	Basic
Load Balancing	HTTP/HTTPs load balancing with failover. Mechanisms include Weighted Requests, Weighted Traffic, Least Requests
High Availability	SRA 4200 only
Application offloading	Yes
Web Application Firewall	Yes

Hardware

Hardened Security Appliance	
SRA 1200	Yes
SRA 4200	Yes

Cryptographic Hardware Acceleration	
SRA 1200	No
SRA 4200	Yes

Interfaces	
SRA 1200	(2) Gigabit Ethernet, (2) USB, (1) Console
SRA 4200	(4) Gigabit Ethernet, (2) USB, (1) Console

Processors	
SRA 1200	x86 main processor
SRA 4200	x86 main processor, cryptographic accelerator

Memory (RAM)	
SRA 1200	1 GB
SRA 4200	2 GB

Flash Memory	
SRA 1200	1 GB
SRA 4200	1 GB

Power Supply/Input	
SRA 1200	Internal, 100-240Vac, 50-60Mhz
SRA 4200	Internal, 100-240Vac, 50-60Mhz

Max Power Consumption	
SRA 1200	53 W
SRA 4200	75 W

Total Heat Dissipation	
SRA 1200	181.0 BTU
SRA 4200	256.0 BTU

Dimensions	
SRA 1200	17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm
SRA 4200	17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm

Appliance Weight	
SRA 1200	9.50 lbs 4.30 kg
SRA 4200	9.50 lbs 4.30 kgs

WEEE Weight	
SRA 1200	10.0 lbs 4.50 kg
SRA 4200	10.0 lbs 4.50 kgs

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	
SRA 1200	13.0 years
SRA 4200	8.3 years

SRA Virtual Appliance

SRA Virtual Appliance Virtualized Environment Requirements

Hypervisor:	VMWare ESXi and ESX (version 4.0 and newer)
Appliance Size (on disk):	80 GB
Allocated Memory:	2 GB

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

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600   F +1 408.745.9300
www.sonicwall.com

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY   SECURE REMOTE ACCESS   WEB AND E-MAIL SECURITY   BACKUP AND RECOVERY   POLICY AND MANAGEMENT

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™