



SonicWALL

# Secure Remote Access Series for SMB

Comprehensive and easy-to-use clientless secure remote access

Today's small- to mid-sized businesses (SMBs) depend on a mobile workforce. The "Consumerization of IT" is driving "Bring Your Own Device" (BYOD) initiatives to deploy smartphones, tablets and—most commonly—Windows-based laptops and netbooks. These IT-managed and non-IT-managed devices require easily deployed secure remote access and endpoint control. Moreover, IT must support and control remote PCs, and handle spikes in remote access for disaster preparedness.

The Dell™ SonicWALL™ Secure Remote Access (SRA) Series for SMB is one of the most comprehensive secure remote access solutions on the market today. The SRA Series for SMB provides clientless, network-level access for Windows®, Windows Mobile, Mac®, Linux®, Apple iOS and Google® Android™, plus optional Web Application Firewall (WAF) Service and multi-platform remote support. The solution lets authorized mobile workers and contractors connect over SSL VPN using a standard web browser. The SRA Series offers granular unified policy, two-factor authentication, load balancing and high availability. Dell SonicWALL End Point Control™ (EPC™) delivers enterprise-class device identification and enforces granular

security posture requirements on Windows-based devices. Easily and flexibly deployed into virtually any network with no pre-installed clients, the SRA Series eliminates the costs associated with deploying and maintaining traditional IPSec VPNs.

Dell SonicWALL Secure Virtual Assist\* permits Windows-based technicians to support Windows, Mac OS or Linux devices remotely. Dell SonicWALL Secure Virtual Meeting\*\* allows for secure and cost-effective collaboration.

SonicWALL Mobile Connect™, a single unified client app for Apple iOS and Google Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections. It is downloadable from either the App Store<sup>SM</sup> or Google Play.



- Seamless integration behind virtually any firewall
- Mobile device support
- NetExtender technology
- Granular unified policy
- Two-factor authentication
- High availability
- Web Application Firewall Service
- End Point Control (EPC)
- Easy, cost-effective deployment
- Remote support
- Secure Virtual Meeting
- Clean VPN
- Spike licenses
- Load balancing

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

\*\*Available in conjunction with Secure Virtual Assist for SRA 4600 and SRA Virtual Appliances only

## Features and benefits

**Seamless integration behind virtually any firewall** enables easy deployment.

**Mobile device support** delivers ActiveSync-based, as well as clientless, network-level remote access for Windows Mobile, Apple iOS, and Google Android. SonicWALL Mobile Connect, a single unified client app for iOS and Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.

**NetExtender technology** enables network-level access to resources, services and applications from a variety of platforms including Windows, Windows Mobile, Google Android, Mac OS and Linux.

**Granular unified policy** displays bookmarks and policies in one centralized page, easing administration. Multiple and custom LDAP policies can restrict unauthorized access to specific applications or resources.

**Two-factor authentication** provides tokenless, enhanced protection against key loggers by generating a unique one-time password that is sent to a remote user's mobile device or email address.

**High availability** allows administrators to deploy an active-backup pair of SRA 4600 or a pair of SRA 4200 appliances to enhance uptime while reliably providing security for remote access users.

**Web Application Firewall Service\*** blocks cross-site scripting, injection attacks and cookie tampering (in compliance with OWASP Top 10 and PCI DSS), prevents credit card and Social Security number theft, and allows automatic Application Profiling for multiple WAF-enabled portals.

**End Point Control (EPC)** for the SRA Series allows for the unique identification of Windows-based endpoints to tie them to the authorized user as well as the ability to assess the security posture of the device by looking for security components such as anti-virus and anti-spyware software.

**Easy, cost-effective deployment** into virtually any network with no pre-installed clients, the SRA for SMB Series eliminates the cost and complexity of deploying and maintaining traditional IPSec VPNs.

**Remote support** using Dell SonicWALL Secure Virtual Assist\* enables technicians to provide secure on-demand assistance to customers on Windows, Macintosh or Linux systems. Secure Virtual Access\* provides secure remote control of unattended Windows systems.

**Secure virtual meeting\*\*** instantly brings meeting participants together in a secure and cost-effective fashion.

**Clean VPN™** secures the integrity of VPN access, decrypts and removes threats from traffic tunneled over SSL VPN before they enter the network through a combined deployment of a Dell SonicWALL SRA Series appliance with a Dell SonicWALL Next-Generation Firewall.

**Spike licenses\*** can increase licensed remote user count instantly for seamless continuity during disruptions or emergencies.

**Load balancing** can be deployed to partition requests across multiple web servers.

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

\*\*Available in conjunction with Secure Virtual Assist for SRA 4600 and SRA Virtual Appliances only

## Dell SonicWALL SRA Series for SMB – anytime, anywhere access to resources

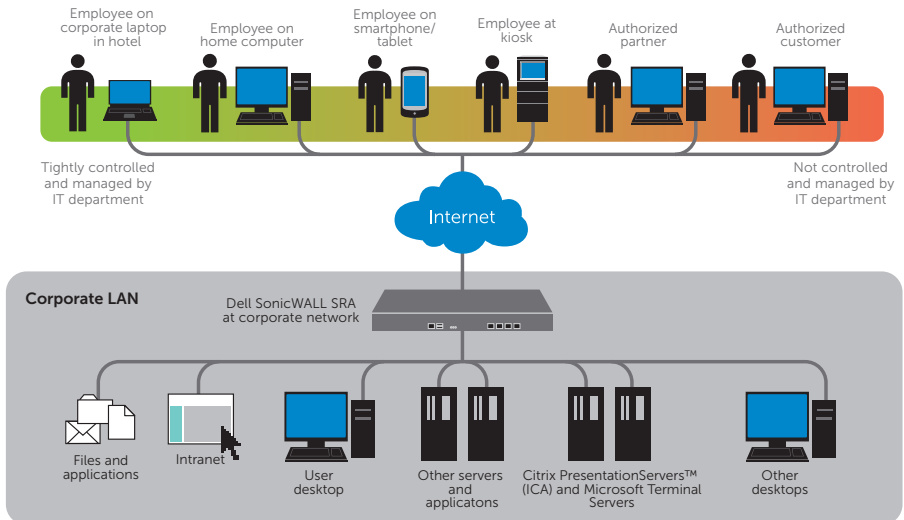
### Granular access to authorized users

The SRA Series for SMB extends secure remote access beyond managed employees to unmanaged remote employees, partners, and customers without compromising security, by employing fine-grained access controls.

#### Awards



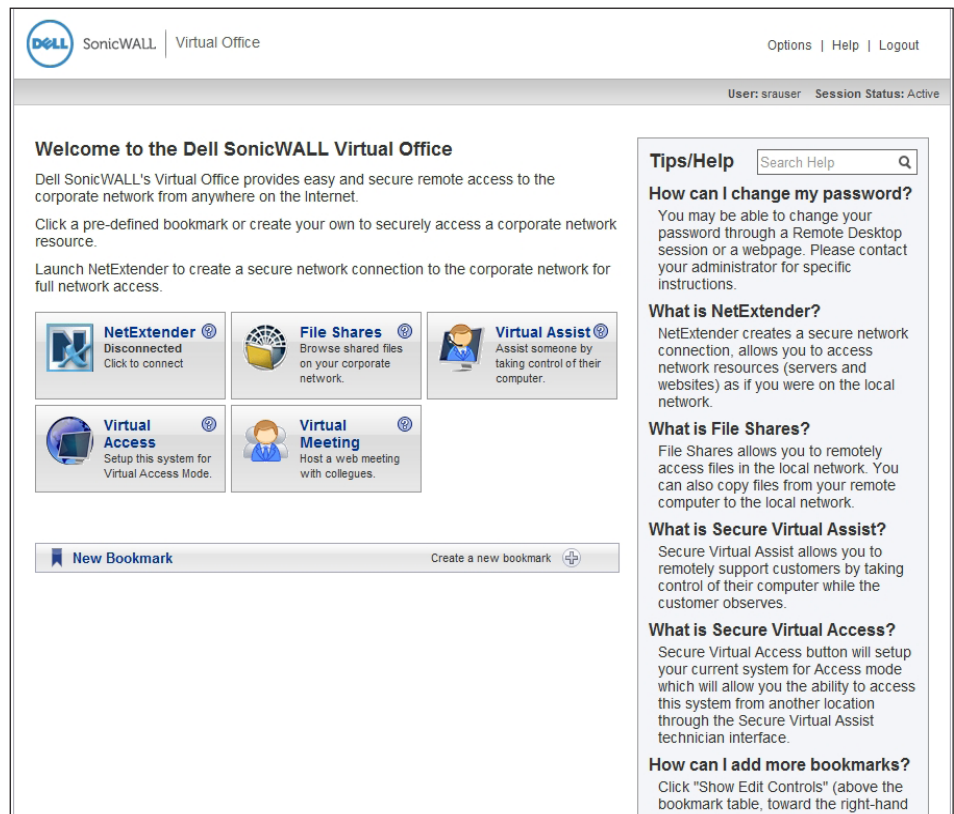
#### Certifications



### Broad access to resources

The SRA Series for SMB can be used to provide Windows, Windows Mobile, Mac OS, iOS, Linux, and Android users with access to a broad range of resources

- Mobile Connect, a single unified client app for iOS and Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections
- NetExtender enables network-level access to resources, services and applications such as Microsoft® Outlook, as well as automatic Client DNS registration
- 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 Application Offloading



### Simple to manage

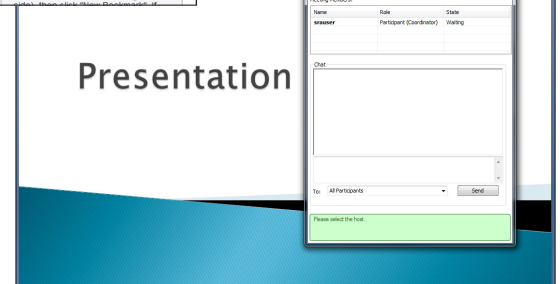
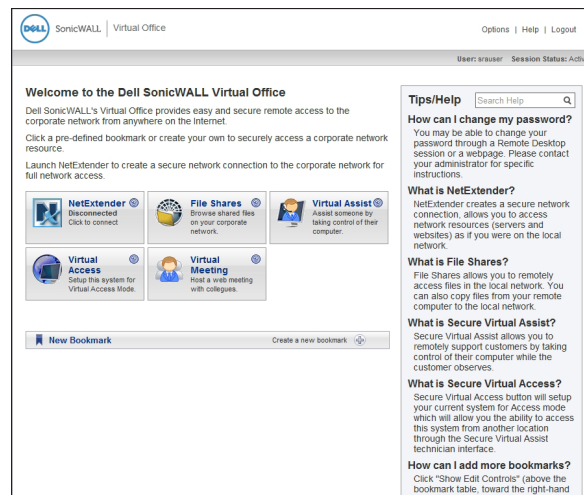
SRA Series solutions feature Unified Policy and an intuitive web-based management interface that offers context-sensitive help to enhance usability. In addition, multiple products

can be centrally managed using the Dell SonicWALL Global Management System (GMS 4.0+). Resource access via the products can be effortlessly monitored using the Dell SonicWALL Analyzer reporting tool.

## Dell SonicWALL secure remote access solutions

### Secure remote PC control, support and collaboration

In organizations with distributed or branch locations, an administrator, technician, or authorized employee may require full control of specific PCs within the LAN from remote locations. Dell SonicWALL Secure Virtual Assist licensed with Secure Virtual Access, enhances productivity by enabling secure remote support of Windows, Mac and Linux systems as well as secure remote control of unattended Windows-based computers. In addition, organizations would like to have a means to conduct cost-effective and secure virtual meetings. Unlike other virtual meeting solutions, Dell SonicWALL Secure Virtual Meeting incorporates all of the security of the SRA for SMB Series to comprehensively protect sensitive and proprietary communications.



## Presentation

### Enhanced solution with Clean VPN

Dell SonicWALL SRA Series for SMB appliances integrate seamlessly into almost any network topology and can be easily deployed alongside virtually any third-party firewall. Deployment with a Dell SonicWALL Next-Generation Firewall running Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service along with application intelligence, control and Visualization further enhances protection benefits. Deploying NetExtender in conjunction

with Enforced Client Anti-Virus and Anti-Spyware on managed PCs enforces endpoint security. Secure 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 vulnerabilities such as SQL Injection attacks, and redirects users to an explanatory error page.

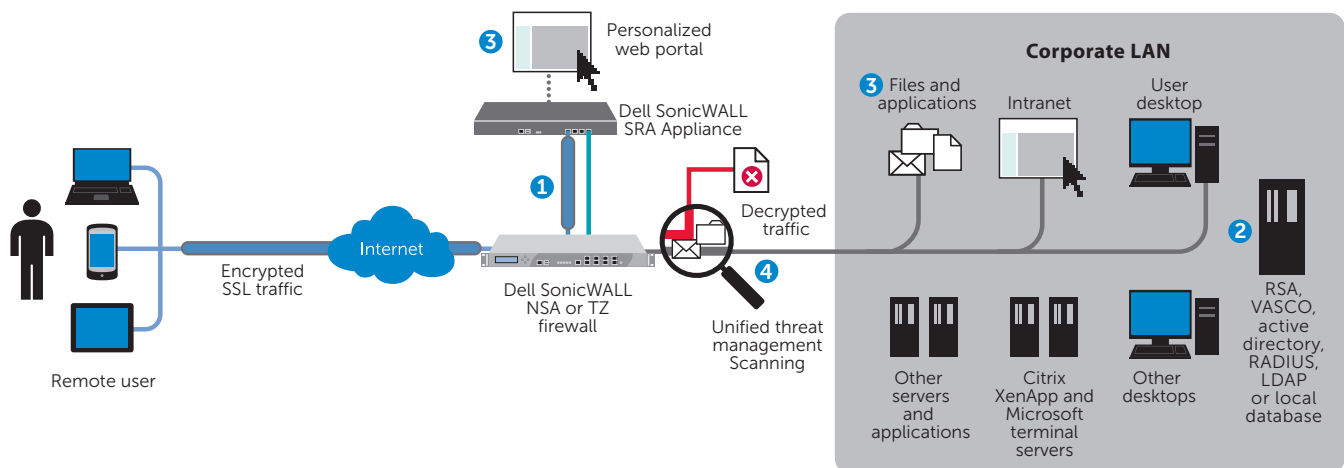
## Dell SonicWALL secure remote access solutions

### Secure remote access solution

With the mobile workforce increasing and greater threats of unexpected

disruptions, remote access has become a business necessity. An SRA appliance deployed in one-arm mode alongside a Dell SonicWALL Next-Generation Firewall (or virtually any other third-party

firewall) enables remote users to access corporate network resources securely from anywhere outside the LAN.



1 Incoming HTTPS traffic is seamlessly forwarded by the Dell SonicWALL NSA or TZ Series firewall to the Dell SonicWALL SRA appliance, which decrypts and authenticates network traffic.

2 Users are authenticated using the onboard database or through third-party authentication methods such as RSA,

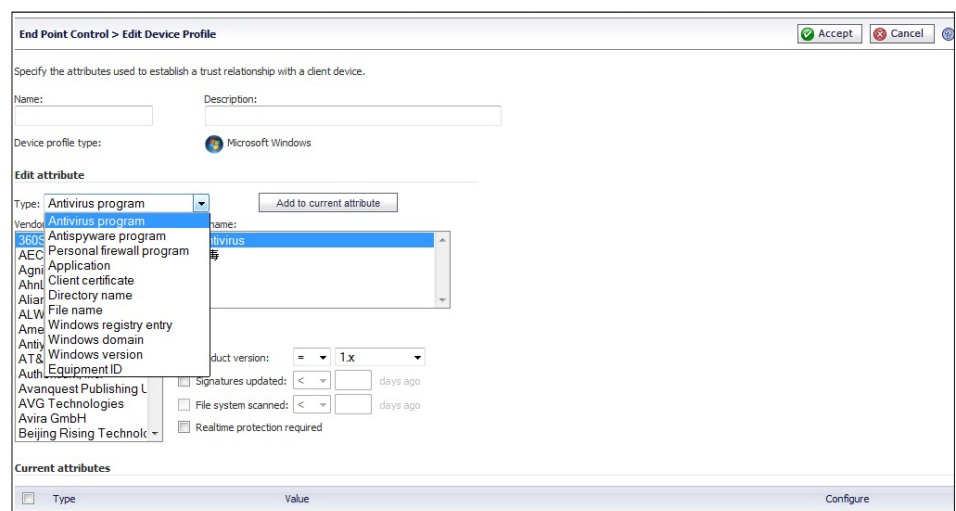
VASCO, RADIUS, LDAP, Microsoft Active Directory or Windows NT Domain.

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

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

### End point control

Dell SonicWALL End Point Control (EPC) for the SRA Series, delivers enterprise-class device identification and enforces granular security posture requirements on Windows-based devices. EPC for the SRA Series allows for the unique identification of Windows-based endpoints as well as the ability to assess the security posture of the device by looking for security components such as anti-virus and anti-spyware software. This helps to establish device trust and reduce the chances of malware entering the network through non-IT-managed devices.

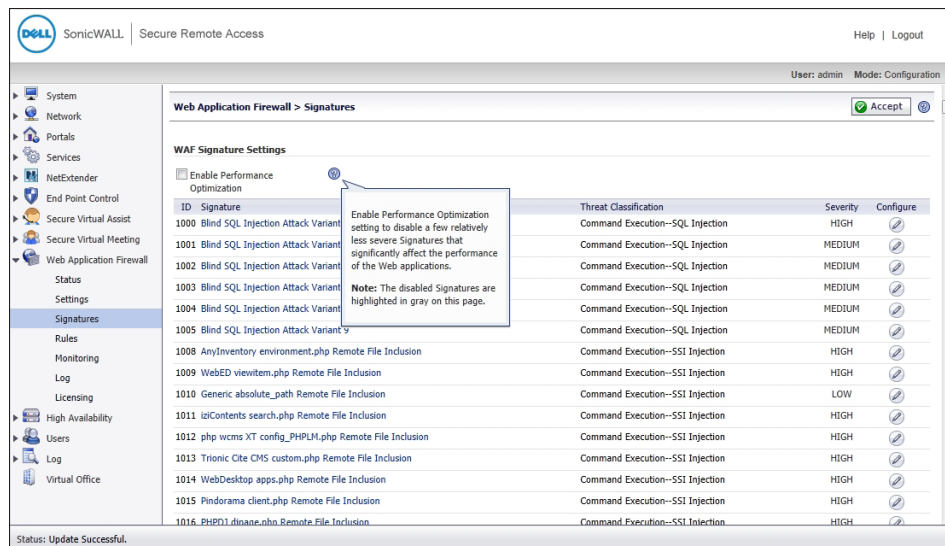




## Dell SonicWALL secure remote access solutions

### Web Application Firewall and PCI compliance

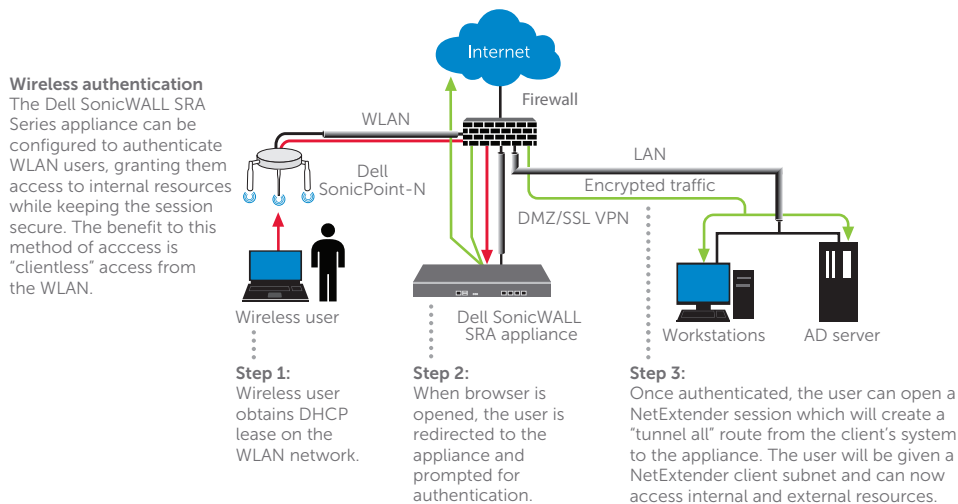
The Dell SonicWALL Web Application Firewall Service offers businesses a complete, affordable, well integrated compliance solution for web-based applications that is easy to manage and deploy. It supports OWASP Top Ten and PCI DSS compliance, providing protection against injection and cross-site scripting attacks (XSS), credit card and Social Security number theft, cookie tampering and cross-site request forgery (CSRF). Dynamic signature updates and custom rules protect against known and unknown vulnerabilities. Web Application Firewall can detect sophisticated web-based attacks and protect web applications (including SSL VPN portals), deny access upon detecting web application malware, and redirect users to an



explanatory error page. It provides an easy-to-deploy offering with advanced statistics and reporting options for meeting compliance mandates. Application profiling enables virtual patching of vulnerabilities.

### Clean Wireless 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. Dell SonicWALL SSL VPNs integrate seamlessly with Dell SonicWALL wireless access solutions. When deployed alongside a Dell SonicWALL Next-Generation Firewall (running Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control) and Dell SonicWALL SonicPoints, a Dell SonicWALL SSL VPN solution ensures that users get access from anywhere on campus, and that 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

## Dell SonicWALL SRA for SMB Series

### Performance

<b>SRA 1600</b>	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 Secure Virtual Assist technicians:	10
Maximum concurrent users*:	50
<b>SRA 4600</b>	Recommended for organizations with 500 or fewer employees
Concurrent user license*:	Starts with 25 users. Additional users licences are available in 10, 25 and 100 user increments.
Maximum allowable concurrent Secure Virtual Assist technicians:	25
Maximum concurrent users*:	500
Maximum allowable Meeting participants:	75
<b>SRA Virtual Appliance</b>	Recommended for organizations of any size
Concurrent user license*:	User licenses available in 5, 10, and 25 user increments
Maximum allowable concurrent Secure Virtual Assist technicians:	25
Maximum concurrent users*:	50
Maximum allowable Meeting participants:	75
*The maximum number of users supported would be limited by factors such as access mechanisms, applications being accessed and application traffic being sent.	

### Key Features

<b>Applications supported</b>	
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.
<b>Encryption</b>	ARC4 (128), MD5, SHA-1, SSLv3, TLSv1, 3DES (168, 256), AES (256), SHA-1, RSA, DHE
<b>Authentication</b>	RSA, Vasco, One-time Passwords, Internal user database RADIUS, LDAP, Microsoft, Active Directory, Windows NT Domain
<b>RDP support</b>	Yes. Terminal Server farm (JAVA client only) and Remote Application support (Active-X only included)
<b>Multiple domain support</b>	Yes
<b>Multiple portal support</b>	Yes
<b>Fine grain access control</b>	At the user, user group and network resource level
<b>Session security</b>	Inactivity timeouts prevent unauthorized use of inactive sessions
<b>Certificates</b>	
Server	Self-signed with editable common name and and imported from third parties
Client	Optional client certificates supported
<b>Cache cleaner</b>	Configurable. Upon logout all cached downloads, cookies and URLs downloaded through the SSL tunnel are erased from the remote computer
<b>Client PC operating systems supported</b>	
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
Mobile Connect	iOS 4.2 and higher, Google Android 4.0 and higher
<b>Web browsers supported</b>	Microsoft Internet Explorer, Firefox Mozilla, Chrome, Opera, Safari
<b>Personalized portal</b>	The remote user sees only those resources that the administrator has granted access to based on company policy
<b>Management</b>	Web GUI (HTTP, HTTPS), Send syslog and heartbeat messages to GMS (4.0 and higher) SNMP Support
<b>Usage monitoring</b>	Graphical monitoring of memory, CPU, users and bandwidth usage
<b>Unified policy</b>	Yes. Also supports policies which have multiple AD groups
<b>Logging</b>	Detailed logging in an easy-to-read format, Syslog supported email alerts
<b>Single-arm mode</b>	Yes
<b>Dell SonicWALL Secure Virtual Assist or Secure Virtual Access (licensed together)</b>	Connection to remote PC, chat, FTP and diagnostic tools

<b>Secure Virtual Meeting (available in conjunction with Secure Virtual Assist for SRA 4600 and SRA Virtual Appliances only)</b>	Instantly brings meeting participants together in securely and cost-effectively
<b>IPv6 support</b>	Basic
<b>Load balancing</b>	HTTP/HTTPS load balancing with failover. Mechanisms include weighted requests, weighted traffic, least requests
<b>High availability</b>	SRA 4600 only
<b>Application offloading</b>	Yes
<b>Web Application Firewall</b>	Yes
<b>Endpoint Control (EPC)</b>	Yes

### Hardware

<b>Hardened security appliance</b>	
SRA 1600	Yes
SRA 4600	Yes
<b>Interfaces</b>	
SRA 1600	(2) gigabit Ethernet, (2) USB, (1) console
SRA 4600	(4) gigabit Ethernet, (2) USB, (1) console
<b>Processors</b>	
SRA 1600	x86 main processor
SRA 4600	x86 main processor
<b>Memory (RAM)</b>	
SRA 1600	1 GB
SRA 4600	2 GB
<b>Flash memory</b>	
SRA 1600	1 GB
SRA 4600	1 GB
<b>Power supply/input</b>	
SRA 1600	Internal, 100-240Vac, 50-60Mhz
SRA 4600	Internal, 100-240Vac, 50-60Mhz
<b>Max power consumption</b>	
SRA 1600	47 W
SRA 4600	50 W
<b>Total heat dissipation</b>	
SRA 1600	158.0 BTU
SRA 4600	171.0 BTU
<b>Dimensions</b>	
SRA 1600	17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm
SRA 4600	17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm
<b>Appliance weight</b>	
SRA 1600	9.50 lbs 4.30 kg
SRA 4600	9.50 lbs 4.30 kgs
<b>WEEE weight</b>	
SRA 1600	10.0 lbs 4.50 kg
SRA 4600	10.0 lbs 4.50 kgs
<b>Major regulatory compliance</b>	FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TUV/GS, CB
<b>Environment</b>	32-105° F, 0-40° C Humidity 5-95% RH, non-condensing
<b>MTBF</b>	
SRA 1600	18.3 years
SRA 4600	17.8 years

### SRA Virtual Appliance

<b>SRA virtual appliance virtualized environment requirements</b>	
Hypervisor:	VMWare ESXi and ESX (version 4.0 and newer)
Appliance size (on disk):	2 GB
Allocated memory:	2 GB



SRA 1600, 5 user 01-SSC-6594

SRA 1600 additional users  
(50 user maximum)  
Add 5 Concurrent users 01-SSC-7138  
Add 10 Concurrent users 01-SSC-7139

SRA 1600 support  
Dell SonicWALL Dynamic Support 24x7  
for up to 25 Users (1-year)\* 01-SSC-7141  
Dell SonicWALL Dynamic Support 8x5  
for up to 25 Users (1-year)\* 01-SSC-7144



SRA 4600, 25 user 01-SSC-6596

SRA 4600 additional users  
(500 user maximum)  
Add 10 Concurrent Users 01-SSC-7118  
Add 25 Concurrent Users 01-SSC-7119  
Add 100 Concurrent Users 01-SSC-7120

SRA 4600 Support  
Dell SonicWALL Dynamic Support 24x7  
for up to 100 Users (1-year)\* 01-SSC-7123  
Dell SonicWALL Dynamic Support 8x5  
for up to 100 users (1-year)\* 01-SSC-7126  
Dell SonicWALL Dynamic Support 24x7  
for 101 to 500 users (1-year)\* 01-SSC-7129  
Dell SonicWALL Dynamic Support 8x5  
for 101 to 500 users (1-year)\* 01-SSC-7132



SRA virtual appliance  
Dell 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  
Dell SonicWALL Dynamic Support 8x5  
for up to 25 users (1-year)\* 01-SSC-9188  
Dell SonicWALL Dynamic Support 24x7  
for up to 25 users (1-year)\* 01-SSC-9191  
Dell SonicWALL Dynamic Support 8x5  
for up to 50 users (1-year)\* 01-SSC-9194  
Dell SonicWALL Dynamic Support 24x7  
for up to 50 users (1-year)\* 01-SSC-9197

\*Multi-year support SKUs are available.

For more information on Dell SonicWALL Secure Remote Access solutions, visit [www.sonicwall.com](http://www.sonicwall.com).

Security Monitoring Services from Dell SecureWorks are available for this appliance Series. For more information, visit [www.dell.com/secureservices](http://www.dell.com/secureservices)