Secure Remote Access Series

Enable mobile and remote worker productivity while protecting from threats

The Dell SonicWALL Secure Remote Access (SRA) Series provides mobile and remote workers using smartphones, tablets or laptops — whether managed or unmanaged BYOD — with fast, easy, policy-enforced access to mission-critical applications, data and resources, without compromising security.

For mobile devices, the solution includes the intuitive Dell SonicWALL Mobile Connect app that provides iOS, Android, Kindle Fire, Windows, and Mac OS X devices secure access to allowed network resources, including shared folders, client-server applications, intranet sites and email.

Users and IT administrators can download the Mobile Connect app via the Apple App Store, Google Play and the Kindle store and Windows 8.1 smartphones, tablets and laptops ship pre-installed with the Mobile Connect app. The solution also supports clientless, secure browser access, including support for industry standard HTML 5 browsers and thin-client VPN access for PCs and laptops, including Windows, Mac OS X and Linux computers.

To protect from rogue access and malware, the SRA Series appliance connects only authorized users and trusted devices to permitted resources. When integrated with a Dell SonicWALL next-generation firewall as a Clean VPN, the combined solution delivers centralized access control, malware protection, application control and content filtering. The multi-layered protection of Clean VPN decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment.

Why you need SRA

The proliferation of mobile devices in the workplace has increased the demand for secure access to mission-critical applications, data and resources. Granting that access offers important productivity benefits to the organization, but introduces significant risks as well.

For example, an unauthorized person might access company resources using a lost or stolen device; an employee’s mobile device might act as a conduit to infect the network with malware; or corporate data might be intercepted over third-party wireless networks. Also, loss of business data stored on devices can occur if rogue personal apps or unauthorized users gain access to that data.

Securing these devices is becoming increasingly difficult, as organizations may no longer influence device selection or control device management. Organizations must implement solutions that safeguard access to ensure only authorized users and devices that meet security policy are granted network access, and that company data in-flight and at rest on the device are secure. Unfortunately, this often involves complex multi-box solutions from multiple vendors and adds significantly to the total cost of ownership behind providing mobile access. Organizations are looking for easy-to-use, cost-effective and secure mobile access solutions that address the needs of their increasingly mobile workforces.

Benefits:

- Single access gateway to all network resources, via mobile app, clientless or web-delivered clients, works to lower IT overhead and TCO
- Common user experience across all operating systems facilitates ease of use from any endpoint
- Mobile Connect app for iOS, Android, Windows 8.1 and Mac OS X offers mobile device ease of use
- Context aware authentication ensures only authorized users and trusted mobile devices are granted access
- One-click secure intranet file browse and on-device data protection
- Adaptive addressing and routing deploys appropriate access methods and security levels
- Setup wizard makes deployment easy
- Efficient object-based policy management of all users, groups, resources and devices
- Web Application Firewall enables PCI compliance
Fast, easy, policy-enforced access to mission-critical applications, data and resources, without compromising security.

**Features**

Single access gateway for mobile app, clientless or web-delivered clients — SRA lowers IT costs by enabling network managers to easily deploy and manage a single secure access gateway that extends remote access via SSL VPN for both internal and external users to all network resources — including web-based, client/server, host-based (such as virtual desktop) and back-connect applications (such as VoIP). SRAs are either clientless with browser access to the customizable SRA Workplace portal or use mobile apps or lightweight web-delivered clients, reducing management overhead and support calls.

Common user experience across all operating systems — SRA technology provides transparent access to network resources from any network environment or device. An SRA provides a single gateway for smartphone, tablet, laptop and desktop access and a common user experience across all operating systems — including Windows, Mac OS X, iOS, Android, Kindle and Linux — from managed or unmanaged devices.

Mobile Connect app — Mobile Connect app for iOS, Mac OS X, Android, Kindle and Windows 8.1 mobile devices provides users with easy, network-level access to corporate and academic resources over encrypted SSL VPN connections. Mobile Connect is easily downloadable from the Apple App Store, Google Play or Kindle store and embedded with Windows 8.1 devices.

Context awareness — Access to the corporate network is granted only after the user has been authenticated and mobile device integrity has been verified.

Protects data at rest on mobile devices — Authenticated users can securely browse and view allowed intranet file shares and files from within the Mobile Connect app. Administrators can establish and enforce mobile application management policy.

Adaptive addressing and routing — Adaptive addressing and routing dynamically adapts to networks, eliminating conflicts common with other solutions.

Setup wizard — All SRAs are easy to set up and deploy in just minutes. The set-up wizard provides an easy, intuitive “out-of-the-box” experience with rapid installation and deployment.

Unified policy — SRA unified policy offers easy, object-based policy management of all users, groups, resources and devices while enforcing granular control based on both user authentication and endpoint interrogation.
Dell SonicWALL SRA Series – anytime, anywhere access

Simple, secure mobile access to resources

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

Granular access to authorized users

The SRA Series extends secure mobile and remote access beyond managed employees to unmanaged mobile and remote employees, partners and customers by employing policy-enforced fine-grained access controls.
Context-aware authentication
Best-in-class, context-aware authentication grants access only to trusted devices and authorized users. Mobile devices are interrogated for essential security information such as jailbreak or root status, device ID, certificate status and OS versions prior to granting access. Laptops and PCs are also interrogated for the presence or absence of security software, client certificates, and device ID. Devices that do not meet policy requirements are not allowed network access and the user is notified of non-compliance.

Protection of data at rest on mobile devices
Authenticated Mobile Connect users can securely browse and view allowed intranet file shares and files from within the Mobile Connect app. Administrators can establish and enforce mobile application management policy for the Mobile Connect app to control whether files viewed can be opened in other apps (iOS 7 and newer), copied to the clipboard, printed or cached securely within the Mobile Connect app. For iOS 7 and newer, this allows administrators to isolate business data from personal data stored on the device and reduces the risk of data loss. In addition, if the user’s credentials are revoked, content stored in the Mobile Connect app is locked and can no longer be accessed or viewed.

Clean VPN
When deployed with a Dell SonicWALL next-generation firewall, Mobile Connect establishes a Clean VPN, an extra layer of protection that decrypts and scans all SSL VPN traffic for malware before it enters the network.

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.

Easy-to-use, cost-effective and secure mobile access that addresses the needs of your increasingly mobile workforce.
Incoming 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.

Users are authenticated using the onboard database or through third-party authentication methods such as LDAP.

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

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.

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.
### Specifications

#### Dell SonicWALL SRA Series

<table>
<thead>
<tr>
<th>Performance</th>
<th>SRA 1600</th>
<th>SRA 4600</th>
<th>SRA Virtual Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent user license</td>
<td>Recommended for organizations with 50 or fewer employees</td>
<td>Recommended for organizations with 250 or fewer employees</td>
<td>Recommended for organizations of any size</td>
</tr>
<tr>
<td>User capacity</td>
<td>Starts with 5 concurrent users. Additional user licenses are available in 5 and 10 user increments.</td>
<td>Starts with 25 users. Additional user licenses are available in 10, 25 and 100 user increments</td>
<td>User licenses available in 5, 10, and 25 user increments</td>
</tr>
<tr>
<td>Secure Virtual Assist technicians</td>
<td>30-day trial-included/10-concurrent technicians maximum</td>
<td>30-day trial-included/25-concurrent technicians maximum</td>
<td>30-day trial-included/25-concurrent technicians maximum</td>
</tr>
<tr>
<td>Maximum allowable Meeting participants</td>
<td>–</td>
<td>75</td>
<td>75</td>
</tr>
</tbody>
</table>

#### Key features

- **Applications supported**:
  - Web portal access: Supports HTML5, proxy and application offloading
  - Virtual Desktop Infrastructure (VDI): Citrix (ICA), RDP
  - Mobile Connect and NetExtender: Any TCP/IP based application: ICMP, VoIP, IMAP, POP, SMTP, etc.

- **Encryption**: ARC4 (128), MD5, SHA-1, SHA-256, SSLv3, TLSv1, TLS 1.1, TLS 1.2, 3DES (168, 256), AES (256), RSA, DHE

- **Authentication**: Dell Quest Defender, other two-factor authentication solutions, One-time Passwords, Internal user database, RADIUS, LDAP, Microsoft Active Directory and Single Sign On (SSO) for most web based apps, RDP and VNC.

- **Multiple domain support**: Yes

- **Client support**:
  - Web portal access: Internet Explorer, Mozilla, Chrome, Opera, and Safari browsers
  - Mobile Connect: iOS 4.2 and higher, OS X 10.9 and higher, Android 4.0 and higher, Kindle Fire running Android 4.0 and higher and Windows 8.1

- **Personalized portal**: The remote user sees only those resources that the administrator has granted access to based on company policy

- **Usage monitoring**: Graphical monitoring of memory, CPU, users and bandwidth usage

---

1. The recommended number of users supported is based on factors such as access mechanisms, applications accessed and application traffic being sent.
2. Available in conjunction with Secure Virtual Assist for SRA 4600 and SRA Virtual Appliances only.
3. Refer to the latest SRA release notes and admin guide for supported configurations.
4. Botnet filtering and Geolocation-based policies require an active support contract to be in place on the hardware or virtual appliance.
# Dell SonicWALL SRA for SMB Series

## Hardware

<table>
<thead>
<tr>
<th>Feature</th>
<th>SRA1600</th>
<th>SRA4600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardened security appliance</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Interfaces</td>
<td>(2) gigabit Ethernet, (2) USB, (1) console</td>
<td>(4) gigabit Ethernet, (2) USB, (1) console</td>
</tr>
<tr>
<td>Processors</td>
<td>x86 main processor</td>
<td>x86 main processor</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>1 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Flash memory</td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Power supply/input</td>
<td>Internal, 100-240VAC, 50-60MHz</td>
<td>Internal, 100-240VAC, 50-60MHz</td>
</tr>
<tr>
<td>Max power consumption</td>
<td>47 W</td>
<td>50 W</td>
</tr>
<tr>
<td>Total heat consumption</td>
<td>158.0 BTU</td>
<td>171.0 BTU</td>
</tr>
<tr>
<td>Dimensions</td>
<td>17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm</td>
<td>17.00 x 10.13 x 1.75 in 43.18 x 25.73 x 4.45 cm</td>
</tr>
<tr>
<td>Appliance weight</td>
<td>9.50 lbs 4.30 kg</td>
<td>9.50 lbs 4.30 kg</td>
</tr>
<tr>
<td>WEEE weight</td>
<td>10.0 lbs 4.50 kg</td>
<td>10.0 lbs 4.50 kg</td>
</tr>
<tr>
<td>Major regulatory compliance</td>
<td>FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TUV/GS, CB</td>
<td>FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TUV/GS, CB</td>
</tr>
<tr>
<td>Environment</td>
<td>32-105˚ F, 0-40˚ C, Humidity 5-95% RH, non-condensing</td>
<td>32-105˚ F, 0-40˚ C, Humidity 5-95% RH, non-condensing</td>
</tr>
<tr>
<td>MTBF</td>
<td>18.3 years</td>
<td>17.8 years</td>
</tr>
</tbody>
</table>

## SRA Virtual Appliance

- **SRA Virtual appliance virtualized environment requirements (Minimum):**
  - Hypervisor: VMWare ESXi and ESX (version 4.0 and newer)
  - Appliance size (on disk): 2 GB
  - Allocated memory: 2 GB

## Dell SonicWALL SRA Virtual Appliance, 5 User

- **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

## Dell SonicWALL SRA Virtual Appliance, 25 User

- **SRA virtual appliance additional users** (500 user maximum)
  - Add 5 Concurrent Users…………………….01-SSC-9182
  - Add 10 Concurrent Users…………………….01-SSC-9183
  - Add 25 Concurrent Users…………………….01-SSC-9184

## Dell SonicWALL 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

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

---

**Dell Software**
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com

If you are located outside North America, you can find local office information on our Web site.

© 2015 Dell, Inc. ALL RIGHTS RESERVED. Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

**DataSheet-SonicWALL-SRASeries-US-VG-25825**