Secure Remote Access Series

Enable mobile and remote worker productivity while protecting from threats

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.

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 SonicWALL Mobile Connect™ application 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 SonicWALL Mobile Connect application via the Apple App Store, Google Play and the Kindle store. New with Windows 8.1, Windows tablets and laptops ship pre-installed with the Mobile Connect application. For PCs and laptops, including Windows®, Mac OS and Linux® computers, the solution supports clientless, secure browser access and thin-client VPN access.

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 Dell SonicWALL Clean VPN™ decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment.

Benefits:

- Cross-platform support for increased mobile worker productivity
- Single access gateway to all network resources; mobile app, clientless or web-delivered clients work 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
Features
Cross-platform support—SRA can be deployed across a wide range of environments and devices, including smartphones, tablets, laptops, desktops and kiosks for both managed and unmanaged devices. Dell SonicWALL SRA makes your users more productive by providing easy access to email, files, applications and more from popular devices including iOS and Android smartphones and tablets; Windows 8.1 tablets and laptops; and Mac OS®, Windows and Linux computers.

Single access gateway; 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 and back-connect applications like VoIP. SRAs are either clientless with browser access to the customizable SRA Workplace portable or use mobile apps or lightweight web-delivered clients, reducing management overhead and support calls. Administrators have even greater control over portal access, content and design with the Dell SonicWALL WorkPlace Portal.

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, iOS, Android, Kindle and Linux—from managed or unmanaged devices.

SonicWALL Mobile Connect app—SonicWALL Mobile Connect™ app for iOS, Mac OSX, 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 stores 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 addressing and routing conflicts common with other solutions.

Dell SonicWALL 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—Dell SonicWALL 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 for SMB – anytime, anywhere access
Simple, secure mobile access to resources
The SRA Series for SMB can be used to provide Windows, Mac OS, iOS, Linux, Android and Kindle users with access to a broad range of resources.

Granular access to authorized users
The SRA Series for SMB 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 (iOS7 only), copied to the clipboard, printed or cached securely within the Mobile Connect app. For iOS7 devices, 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.

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 for SMB Series

#### Performance

<table>
<thead>
<tr>
<th>Model</th>
<th>User capacity*</th>
<th>Assist technicians</th>
<th>Concurrent user license</th>
<th>Secure Virtual Access (licensed together)</th>
<th>Virtual Assist or Secure Assistance</th>
<th>Meeting participants</th>
<th>User Capacity</th>
<th>Secure Virtual Meeting**</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRA 1600</td>
<td>25-included/500-licensable/100-recommended</td>
<td>10-concurrent technician maximum</td>
<td>Starts with 5 concurrent users</td>
<td>25 user maximum</td>
<td>75</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRA 4600</td>
<td>5-included/50-licensable/25-recommended</td>
<td>100-concurrent technician maximum</td>
<td>Starts with 25 users</td>
<td>25-user maximum</td>
<td>75</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Hardware

- **SRA 1600**: Recommended for organizations of any size, with a maximum license of 25 users. Additional user licenses are available in 10, 25, and 100 user increments.
- **SRA 4600**: Recommended for organizations with 250 or more employees, with a maximum license of 5 users. Additional user licenses are available in 5, 10, 25, and 100 user increments. Secure Virtual Meeting** instantly brings meeting participants together securely and cost-effectively.

#### Key Features

- **Network Interface**: Up to 2 gigabit Ethernet, 1 USB, and 1 console interface.
- **Encapsulation**: Secure Virtual Access (licensed together) for secure and cost-effective access.
- **Secure Virtual Meeting** provides instant meeting capabilities.
- **Virtual Assist or Secure Assist** enables secure remote assistance.

### Additional Features

- **Unified policy management**: Yes. Also supports policies which have multiple groups.
- **Logging**: Detailed logging in an easy-to-read format, along with supported email alerts.
- **Single-arm mode**: Yes.

### Applications supported

- **NetExtender**: Any TCP/IP based application: ICMP, VoIP, IMAP, POP, SMTP, FTP, HTTP, HTTPS.
- **Encryption**: ARC4 (128), MD5, SHA-1, SHA-256, SHA-384, SSLv3, TLSv1, TLS 1.1, TLS 1.2, AES (128, 192, 256), AESG (256), RSA, DHE.

### Certifications

- **Server**: Self-signed with editable common name and issued from third parties. Optional: client certificate supported.
- **Cache cleaner**: Configurable. Upon logout, all cached downloads, cookies, and URLS downloaded through the SSL tunnel are erased from the remote computer.

### Client device operating systems supported

- **All operating systems**: Windows 2003, 2008, XP/Vista (32-bit and 64-bit), 7 (32-bit and 64-bit), 8 (32-bit and 64-bit), Mac OS X, Linux Fedora Core 3+/64-bit, Ubuntu 7+/OpenSUSE, Linux 64-bit.
- **Mobile Connect**: Creation/Security: OpenSSL, S/SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, 3DES (168, 256), AES (128), RSA, DHE.
- **Web browsers supported**: Internet Explorer, 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 (HTTPS, HTTP), Send syslog and heartbeat messages to GMS (4.0 and higher), SNMP support.

### Usage monitoring

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

---

For more information, visit the Dell SonicWALL website or contact Dell SonicWALL Support.

---

**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

---

Dell SonicWALL SRA for SMB Series

**SRA 1600**

**SRA 4600**

---

### Dell Software

5 Polaris Way, Alviso, CA 95002 | www.dell.com

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