



## SonicWALL Secure Remote Access-Serie

SECURE REMOTE ACCESS

**Benutzerfreundlicher und erschwinglicher Secure Remote Access ohne Client**

- **Nahtlose Integration mit nahezu allen Firewalls**
- **NetExtender-Technologie**
- **Personalisiertes Web-Portal**
- **Remote Support**
- **Remote PC Control**
- **Web Application Firewall Service**
- **Zwei-Faktor-Authentifizierung ohne Token**
- **Unterstützung von mobilen Geräten**
- **Lastverteilung**
- **Hochverfügbarkeitsoptionen**
- **Spike Licenses**
- **Unified Policy**
- **SonicWALL Clean VPN**

Die Anzahl und Bedeutung mobiler Arbeitsplätze hat in den letzten Jahren enorm zugenommen. Man kann heute beinahe an jedem beliebigen Ort arbeiten: zuhause, am Flughafen oder im Café. Die Nachfrage nach einem sicheren Remote-Zugriff auf immer mehr Ressourcen und von immer mehr Remote-Geräten und Plattformen (z. B. Smartphones und Tablet-Geräten) ist größer denn je. Dementsprechend steigt auch der Bedarf an Remote PC Control- und Remote Support-Lösungen. Während herkömmliche IPSec-Lösungen für feste Site-to-Site-VPNs durchaus geeignet sind, kann die Vorinstallation und Wartung von IPSec Clients auf verteilten oder Remote-Geräten kostspielig und ineffizient sein. Um auf Katastrophenfälle vorbereitet zu sein, müssen Unternehmen außerdem dafür sorgen, dass ihre Mitarbeiter an anderen Standorten weiterarbeiten können. Darüber hinaus müssen sie in der Lage sein, einen sprunghaften Anstieg an Remote Access-Benutzern zu bewältigen.

Mit seiner Secure Remote Access (SRA)-Serie bietet SonicWALL® einen clientlosen Zugriff auf Netzwerkebene für Windows®, Windows Mobile, Apple® Mac OS®, iOS, Linux® und Google Android® sowie einen optionalen Web Application Firewall Service und Remote-Support für mehrere Plattformen. Außerdem profitieren kleine und mittlere Unternehmen (KMUs) von granularen Unified Policy-Funktionen, einer Zwei-Faktor-Authentifizierung, Lastverteilung und Hochverfügbarkeit. Die SRA-Serie erlaubt autorisierten mobilen Mitarbeitern und Partnern den sicheren Netzwerkzugriff via SSL VPN mit einem Standard-Webbrowser. Dabei lassen sich die Lösungen der SRA-Serie ganz unkompliziert und flexibel in nahezu jedem Netzwerk installieren, ohne dass vorinstallierte Clients erforderlich sind. Dies spart Kosten, die für die Bereitstellung und Wartung herkömmlicher IPSec VPNs anfallen würden.

Über SonicWALL Virtual Assist\* können Techniker mit Windows-Systemen Remote-Support für Windows-, Mac OS- oder Linux-Geräte leisten.

Die im App Store<sup>SM</sup> zum Download verfügbare SonicWALL Mobile Connect™ Unified Client App für iOS bietet Apple iPad™-, iPhone®- und iPod touch®-Benutzern vollen Zugriff auf Netzwerk-Ressourcen von Unternehmen und Bildungseinrichtungen.

### Funktionen und Vorteile

#### **Nahtlose Integration mit nahezu allen Firewalls.**

Ermöglicht es Unternehmen, die bestehende Netzwerk-Infrastruktur weiter zu nutzen.

**NetExtender-Technologie.** Ermöglicht den Zugriff auf Ressourcen, Dienste und Anwendungen auf Netzwerkebene.

**Personalisiertes Web-Portal.** Dem Benutzer werden nur die Ressourcen angezeigt, auf die er gemäß Unternehmensregeln zugreifen darf.

**Remote Support.** Mit SonicWALL Virtual Assist\* können Techniker die bestehende Infrastruktur nutzen, um Kunden je nach Bedarf sicheren Support zu bieten.

**Remote PC Control** mit SonicWALL Virtual Access\* bietet Administratoren oder autorisierten Endbenutzern einen sicheren Remote-Zugang. Damit können sie von jedem beliebigen Ort aus auf ihre unverwalteten Windows-, Macintosh oder Linux-Rechner zugreifen.

**Web Application Firewall Service\*.** Schützt Webanwendungen vor webbasierten Bedrohungen, wie Cross-Site Scripting, Injection-Angriffen und Cookie Tampering, um die Einhaltung der OWASP Top 10- und PCI DSS-Richtlinien sicherzustellen. Darüber hinaus beugt der WAF Service dem Diebstahl von Kreditkarten- und Sozialversicherungsnummern vor.

**Zwei-Faktor-Authentifizierung ohne Token.** Die SSL VPN-Appliance generiert ein Einmalpasswort und sendet es an das mobile Gerät oder an die E-Mail-Adresse eines Remote-Benutzers. Kombiniert mit dem Netzwerknamen und dem Passwort des Benutzers bietet die Appliance erweiterten Schutz vor Keyloggern.

**Unterstützung von mobilen Geräten** für unterschiedliche Systeme, wie Windows Mobile-, Google® Android-, iOS (iPhone, iPad und iPod touch)- und Symbian-Plattformen.

Dies ermöglicht einen einfachen Zugriff auf E-Mail sowie Bookmark-Unterstützung für iPhone® und iPad™. Die umfassende ActiveSync-Unterstützung erlaubt einen unkomplizierten Zugriff auf Kalender, E-Mail und Kontakte. Mit NetExtender sind Verbindungen für Windows Mobile- und Google Android-Geräte auf Netzwerkebene möglich. Die SonicWALL Mobile Connect Unified Client App für iOS bietet Apple iPad™-, iPhone®- und iPod touch®-Benutzern vollen Zugriff auf Netzwerkebene.

**Lastverteilung.** Ermöglicht die Verteilung von Verbindungsanfragen auf mehrere Webserver.

**Hochverfügbarkeitsoptionen.** Durch Einsatz eines Appliance-Paares für ein aktives Backup lässt sich die Verfügbarkeit erhöhen. Gleichzeitig sind die Daten von Remote-Benutzern zuverlässig vor Verlust geschützt.

**Spike Licenses\*.** Bieten die Möglichkeit, die Anzahl von Remote-Benutzerlizenzen innerhalb kürzester Zeit zu erhöhen, um während Unterbrechungen oder in Notfallsituationen eine ununterbrochene Verfügbarkeit zu gewährleisten.

**Unified Policy.** Zeigt Lesezeichen und granulare Regeln auf einer zentralen Seite an und reduziert damit nicht nur den Aufwand bei der Konfiguration und Fehlerbehebung, sondern auch bei der Verwaltung. Administratoren können auf einfache Weise mehrere LDAP-Regeln erstellen, mit denen der Zugriff auf bestimmte Anwendungen und Ressourcen eingeschränkt oder gesperrt wird.

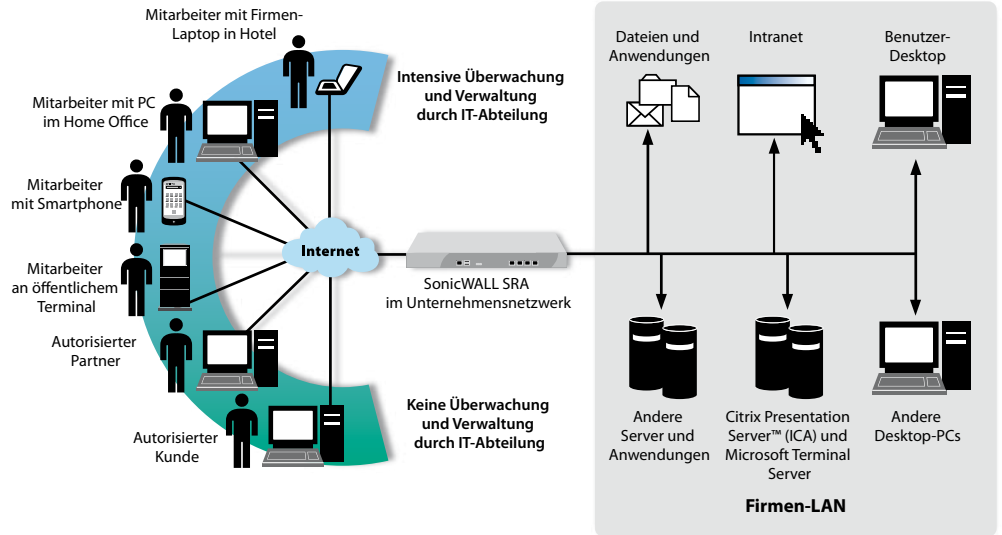
**SonicWALL Clean VPN™.** Durch den kombinierten Einsatz mit einer SonicWALL-Firewall wird die Integrität des VPN-Zugriffs gewährleistet und bössartige Bedrohungen werden neutralisiert, bevor sie ins Unternehmensnetzwerk gelangen.

\* Zusätzliche Lizenz erforderlich; als Software-Add-On-Modul verfügbar.



**Granularer Zugriff für autorisierte Benutzer**

Die SRA-Serie für kleine und mittlere Unternehmen (KMUs) dehnt den sicheren Remote-Zugriff von verwalteten Mitarbeiter-PCs auf die unverwalteten Geräte remote tätiger Mitarbeiter, Partner und Kunden aus. Dank individueller Zugangssteuerungsoptionen ist dabei eine unvermindert hohe Sicherheit gewährleistet.



**Sicherer  
Remote-Zugriff  
– kostengünstig  
und einfach  
in der Anwendung**



**Vielfältige Zugriffsmöglichkeiten**

Die SonicWALL SRA-Serie kann eingesetzt werden, um Benutzern Zugriff auf vielfältige Ressourcen zu bieten.

- NetExtender ermöglicht einen nativen Zugriff auf Anwendungen im Unternehmensnetzwerk, wie z. B. Microsoft® Outlook.
- Das Virtual Office-Portal erlaubt den Webzugriff auf Intranet (HTTP, HTTPS)-, Datei (FTP, CIFS)-, Desktop (Citrix®, Terminal Server, VNC)- und Terminal (Telnet, SSH)-Ressourcen.
- Unterstützt eine Anwendung URL Rewriting, kann über Lesezeichen auf sie zugegriffen werden (andernfalls per Application Offloading).

**Einfache Verwaltung**

Die Lösungen der SRA-Serie mit Unified Policy bieten eine intuitive webbasierte Verwaltungsoberfläche mit kontextsensitiver Hilfe, die für mehr Benutzerfreundlichkeit sorgt. Außerdem können mehrere Produkte mit dem SonicWALL Global Management System (GMS Version 4.0 oder höher) zentral verwaltet werden. Mit dem Analyzer-Reporting-Tool von SonicWALL lässt sich der Netzwerkzugriff über die Lösungen mühelos überwachen.



**Remote PC Control**

In Unternehmen mit verteilten Netzwerken, Zweigniederlassungen, Disaster Recovery-Zweitstandorten, externen Managed Services oder Telearbeitern kann es nötig sein, dass ein Administrator, Techniker, Service Provider oder autorisierter Mitarbeiter von einem Remote-Standort aus für administrative Aufgaben auf bestimmte PCs im LAN zugreift. SonicWALL Virtual Assist mit Virtual Access-Lizenz gewährleistet hierbei eine sichere Remote-Kontrolle von unverwalteten Windows-basierten Desktop-Computern und sorgt so für mehr Produktivität.

**Erweiterte Sicherheitslösung**

Die Appliances der SonicWALL SRA-Serie lassen sich nahtlos in fast jede Netzwerktopologie integrieren und können unkompliziert mit nahezu allen Fremdanbieter-Firewalls installiert werden. Die Kombination mit einer SonicWALL-Firewall mit Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service sowie Application Intelligence und Anwendungskontrolle bietet erweiterte Netzwerksicherheit. Der Einsatz von NetExtender in Kombination mit Enforced Client Anti-Virus and Anti-Spyware auf verwalteten Rechnern gewährleistet außerdem die Sicherheit von Endpunkten. Virtual Assist lässt sich nahtlos integrieren, da das Tool die lokalen und externen Authentifizierungsfunktionen der Appliance nutzt. Außerdem prüft der Web Application Firewall Service Layer 7-Verkehr mittels Reverse Proxy-Analyse auf bekannte Signaturen und sperrt den Zugriff, falls Anwendungsbedrohungen wie SQL Injection-Angriffe identifiziert werden. Anschließend wird der Benutzer auf eine Seite mit Informationen zum aufgetretenen Fehler weitergeleitet.

**Auszeichnungen**



**Zertifikate**

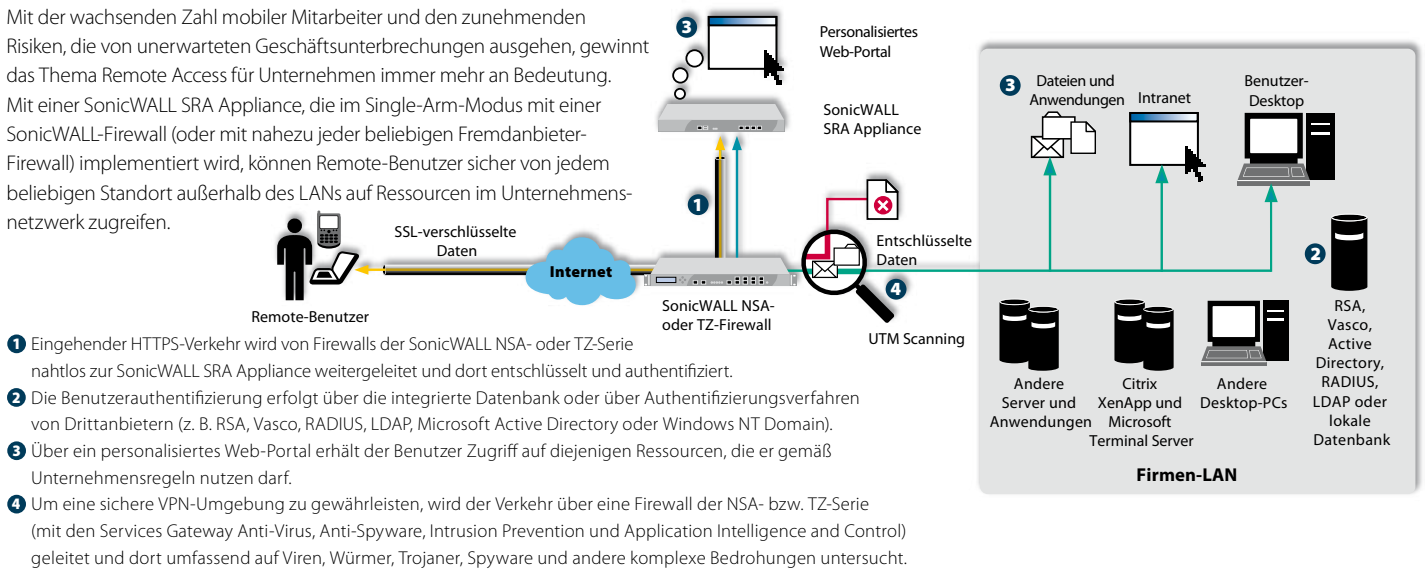


(SRA 1200, SRA 4200)



### Remote Access-Lösung

Mit der wachsenden Zahl mobiler Mitarbeiter und den zunehmenden Risiken, die von unerwarteten Geschäftsunterbrechungen ausgehen, gewinnt das Thema Remote Access für Unternehmen immer mehr an Bedeutung. Mit einer SonicWALL SRA Appliance, die im Single-Arm-Modus mit einer SonicWALL-Firewall (oder mit nahezu jeder beliebigen Fremdanbieter-Firewall) implementiert wird, können Remote-Benutzer sicher von jedem beliebigen Standort außerhalb des LANs auf Ressourcen im Unternehmensnetzwerk zugreifen.



1. Eingehender HTTPS-Verkehr wird von Firewalls der SonicWALL NSA- oder TZ-Serie nahtlos zur SonicWALL SRA Appliance weitergeleitet und dort entschlüsselt und authentifiziert.
2. Die Benutzerauthentifizierung erfolgt über die integrierte Datenbank oder über Authentifizierungsverfahren von Drittanbietern (z. B. RSA, Vasco, RADIUS, LDAP, Microsoft Active Directory oder Windows NT Domain).
3. Über ein personalisiertes Web-Portal erhält der Benutzer Zugriff auf diejenigen Ressourcen, die er gemäß Unternehmensregeln nutzen darf.
4. Um eine sichere VPN-Umgebung zu gewährleisten, wird der Verkehr über eine Firewall der NSA- bzw. TZ-Serie (mit den Services Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control) geleitet und dort umfassend auf Viren, Würmer, Trojaner, Spyware und andere komplexe Bedrohungen untersucht.

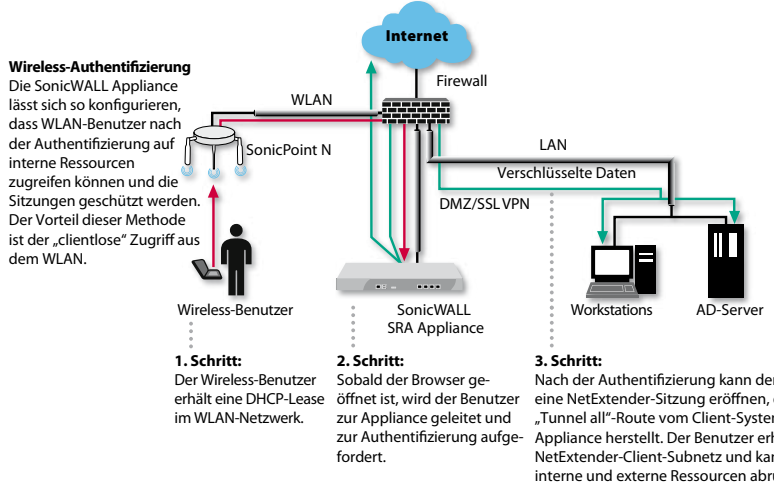
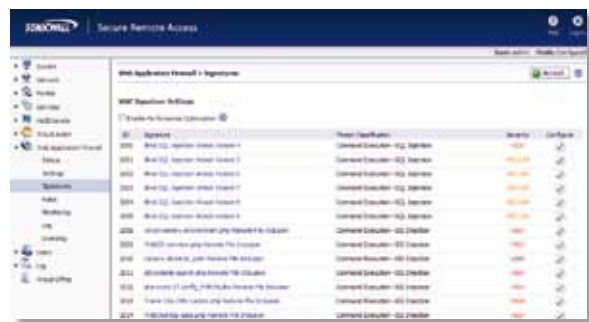


### Remote Support-Lösung

Aufgrund der zunehmenden Zahl remote tätiger Mitarbeiter und weltweit verteilter Kunden wird es immer wichtiger, dass Organisationen Remote Support für extern genutzte Geräte wie Laptops oder Privat-PCs bereitstellen. Ineffizienter Support mit teuren und umständlichen Tools kann dazu führen, dass IT Service Level Agreements nicht eingehalten werden und die Produktivität remote tätiger Mitarbeiter leidet. Mit SonicWALL Virtual Assist, einem Remote-Support-Tool für verteilte Netzwerke und Service-Provider, können Techniker auf fremde Windows-, Macintosh- oder Linux-Rechner zugreifen. Der Kunde erteilt dem Techniker dabei die Berechtigung zu chatten, Dateien zu übertragen, auf den Kundenrechner zuzugreifen und Neustarts durchzuführen, um Probleme zu identifizieren und zu beheben.

### Web Application Firewall und PCI-Compliance

Der SonicWALL Web Application Firewall Service bietet Unternehmen eine umfassende, erschwingliche und gut integrierte Compliance-Lösung für Webanwendungen, die sich leicht verwalten und implementieren lässt. Der Service unterstützt die Einhaltung der OWASP Top Ten- und PCI DSS-Richtlinien und schützt vor Injection- und Cross-Site Scripting-Angriffen (XSS), vor dem Diebstahl von Kreditkarten- und Sozialversicherungsnummern, Cookie Tampering und Cross-Site Request Forgery (CSRF). Dynamische Signaturen-Updates und individuell erstellbare Regeln bieten Schutz vor bekannten und unbekanntem Sicherheitschwachstellen. Der Web Application Firewall Service kann komplexe webbasierte Angriffe erkennen, Webanwendungen (u. a. SSL VPN-Portale) schützen und den Zugriff sperren, wenn Malware in einer Webanwendung entdeckt wurde. Benutzer werden anschließend auf eine Seite mit Informationen zum aufgetretenen Fehler weitergeleitet. Der SonicWALL Web Application Firewall Service ist eine leicht zu implementierende Lösung mit erweiterbaren Statistik- und Reporting-Optionen zur Einhaltung von Compliance-Richtlinien.



- Wireless-Authentifizierung**  
Die SonicWALL Appliance lässt sich so konfigurieren, dass WLAN-Benutzer nach der Authentifizierung auf interne Ressourcen zugreifen können und die Sitzungen geschützt werden. Der Vorteil dieser Methode ist der „clientlose“ Zugriff aus dem WLAN.
1. Schritt: Der Wireless-Benutzer erhält eine DHCP-Lease im WLAN-Netzwerk.
  2. Schritt: Sobald der Browser geöffnet ist, wird der Benutzer zur Appliance geleitet und zur Authentifizierung aufgefordert.
  3. Schritt: Nach der Authentifizierung kann der Benutzer eine NetExtender-Sitzung eröffnen, die eine „Tunnel all“-Route vom Client-System zur Appliance herstellt. Der Benutzer erhält ein NetExtender-Client-Subnetz und kann jetzt interne und externe Ressourcen abrufen.

### Clean Wireless Remote Access-Lösung

Immer mehr Unternehmen, Universitäten, Krankenhäuser und Behörden implementieren drahtlose Netzwerke mit SSL VPN als sichere und zentralisierte Lösung zur Zugriffskontrolle. SonicWALL SSL VPNs lassen sich nahtlos mit den Wireless Access-Lösungen von SonicWALL integrieren. Durch die Implementierung einer SonicWALL SSL VPN-Lösung zusammen mit einer SonicWALL-Firewall (mit den Services Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control) und SonicWALL SonicPoints wird sichergestellt, dass Benutzer überall auf dem Firmengelände auf das Netzwerk zugreifen können und dass die Wireless-Verbindungen über das SSL-Protokoll verschlüsselt werden. Ein weiterer Vorteil besteht darin, dass sich remote tätige Mitarbeiter außerhalb des Firmengeländes über eine SSL VPN-Verbindung in das Unternehmensnetzwerk einloggen können. Mithilfe eines einzigen Gateways können IT-Abteilungen zentral und gezielt kontrollieren, welcher Benutzer auf welche Ressourcen zugreift.

# Technische Daten



SonicWALL SRA 1200  
5 Benutzer 01-SSC-6063

## SRA 1200 Zusätzliche Benutzer (max. 50 Benutzer)

Zusätzlich 1 gleichzeitiger Benutzer  
01-SSC-6067

Zusätzlich 5 gleichzeitige Benutzer  
01-SSC-6068

Zusätzlich 10 gleichzeitige Benutzer  
01-SSC-6069

**SRA 1200 – Support**  
SonicWALL Dynamic Support 24/7  
für bis zu 25 Benutzer (1 Jahr)  
01-SSC-8868

SonicWALL Dynamic Support 8/5  
für bis zu 25 Benutzer (1 Jahr)  
01-SSC-8871



SonicWALL SRA 4200  
25 Benutzer 01-SSC-5998

## SRA 4200 – Zusätzliche Benutzer (max. 500 Benutzer)

Zusätzlich 10 gleichzeitige Benutzer  
01-SSC-5999

Zusätzlich 25 gleichzeitige Benutzer  
01-SSC-6005

Zusätzlich 100 gleichzeitige Benutzer  
01-SSC-6012

## SRA 4200 – Support

SonicWALL Dynamic Support 24/7 für bis zu  
100 Benutzer (1 Jahr)\* 01-SSC-6013

SonicWALL Dynamic Support 8/5 für bis zu  
100 Benutzer (1 Jahr)\* 01-SSC-6022

SonicWALL Dynamic Support 24/7 für  
101 bis 500 Benutzer (1 Jahr)\* 01-SSC-6029

SonicWALL Dynamic Support 8/5 für  
101 bis 500 Benutzer (1 Jahr)\* 01-SSC-6035



**SRA Virtual Appliance**  
SonicWALL SRA Virtual Appliance,  
5 Benutzer 01-SSC-8469

## SRA Virtual Appliance – Zusätzliche Benutzer (max. 50 Benutzer)

Zusätzlich 5 gleichzeitige Benutzer  
01-SSC-9182

Zusätzlich 10 gleichzeitige Benutzer  
01-SSC-9183

Zusätzlich 25 gleichzeitige Benutzer  
01-SSC-9184

## Support für SRA Virtual Appliance

SonicWALL Dynamic Support 8/5 für bis zu  
25 Benutzer (1 Jahr) 01-SSC-9188

SonicWALL Dynamic Support 24/7 für bis zu  
25 Benutzer (1 Jahr) 01-SSC-9191

SonicWALL Dynamic Support 8/5 für bis zu  
50 Benutzer (1 Jahr) 01-SSC-9194

SonicWALL Dynamic Support 24/7 für bis zu  
50 Benutzer (1 Jahr) 01-SSC-9197

\*Support-Lizenzen auch für  
mehrere Jahre erhältlich



## SonicWALL Deutschland

Tel: +49 89 4545 946 www.sonicwall.de

## SonicWALL Schweiz

Tel: +41 44 810 31 35 www.sonicwall.ch

## SonicWALL Österreich

Tel: +41 44 810 31 35 www.sonicwall.at

## SonicWALL Secure Remote Access-Serie

### Leistung

<b>SRA 1200</b>	Empfohlen für Unternehmen mit bis zu 50 Mitarbeitern
Gleichzeitige Benutzer-Lizenzen*	Angefangen bei 5 gleichzeitigen Benutzern, zusätzliche Benutzer-Lizenzen für 5 und 10 Benutzer verfügbar
Maximal zulässige Anzahl gleichzeitiger Virtual Assist-Techniker	10
Maximale Anzahl gleichzeitiger Benutzer*	50
<b>SRA 4200</b>	Empfohlen für Unternehmen mit bis zu 500 Mitarbeitern
Gleichzeitige Benutzer-Lizenzen*	Angefangen bei 25 Benutzern. Zusätzliche Lizenzen für 10, 25 und 100 Benutzer verfügbar
Maximal zulässige Anzahl gleichzeitiger Virtual Assist-Techniker	25
Maximale Anzahl gleichzeitiger Benutzer*	500
<b>SRA Virtual Appliance</b>	Empfohlen für Unternehmen jeder Größenordnung
Gleichzeitige Benutzer-Lizenzen*	Benutzer-Lizenzen für 5, 10 und 25 Benutzer verfügbar
Maximal zulässige Anzahl gleichzeitiger Virtual Assist-Techniker	25
Maximale Anzahl gleichzeitiger Benutzer*	50

\*Die maximal unterstützte Benutzeranzahl wird durch Faktoren wie Zugriffsmechanismen, die Anwendungsnutzung und den Umfang des Anwendungsverkehrs begrenzt.

### Die wichtigsten Funktionen

#### Unterstützte Anwendungen

Proxy	Citrix (ICA), HTTP, HTTPS, FTP, SSH, Telnet, RDP, VNC, Windows* File Sharing (Windows SMB/CIFS), OWA 2003/2007/2010
NetExtender	Sämtliche TCP/IP-basierte Anwendungen: ICMP, VoIP, IMAP, POP, SMTP etc.

#### Verschlüsselung

ARC4 (128), MD5, SHA-1, SSLv3, TLSv1, 3DES (168, 256), AES (256), SHA-1, RSA, DHE

#### Authentifizierung

RSA, Vasco, Einmalpasswörter, interne Benutzerdatenbank, RADIUS, LDAP, Microsoft Active Directory, Windows NT Domain

#### RDP-Unterstützung

Ja. Mit Unterstützung für Terminal Server-Farmen (nur JAVA-Client) und Remote-Anwendungen (nur Active-X)

#### Unterstützung mehrerer Domänen

Ja

#### Unterstützung mehrerer Portale

Ja

#### Individuelle Zugangssteuerung

Auf Benutzer-, Benutzergruppen- und Netzwerkressourcenebene

#### Sitzungssicherheit

Timeout von inaktiven Sitzungen verhindert die unberechtigte Nutzung dieser Sitzungen.

#### Zertifikate

Server Eigensigniert mit editierbarem Common Name bzw. Übernahme von Fremdanbietern

#### Client

Optionale Client-Zertifikate unterstützt

#### Cache Cleaner

Optional. Nach Abmelden des Benutzers werden sämtliche über den SSL-Tunnel heruntergeladenen Dateien, Cookies und URLs aus dem Cache des Remote-Computers gelöscht.

#### Unterstützte Betriebssysteme auf Client-PCs

Proxy	Alle Betriebssysteme
NetExtender	Windows 2000, 2003, XP/Vista (32 Bit und 64 Bit), 7 (32 Bit und 64 Bit), Win Mobile 6.5 (Pocket PC), Win Mobile 6.5 (Classic/Professional), MacOS 10.4+ und SnowLeopard (PowerPC und Intel), Linux Fedora Core 3+ / Ubuntu 7+ / OpenSUSE, Linux 64 Bit, Google® Android <sup>1</sup>
Mobile Connect	iOS 4.2 und höher

#### Unterstützte Webbrowser

Microsoft Internet Explorer, Firefox Mozilla, Chrome, Opera, Safari

#### Personalisiertes Portal

Dem Remote-Benutzer werden nur die Ressourcen angezeigt, die vom Administrator gemäß Unternehmensregeln freigegeben wurden.

#### Verwaltung

Web-Oberfläche (HTTP, HTTPS), Senden von Syslog und Heartbeat-Meldungen an GMS (4.0 oder höher)

SNMP-Unterstützung

### Nutzungskontrolle

Grafische Anzeige der Speicher-, CPU und Bandbreitennutzung sowie der Benutzer

### Unified Policy

Ja. Unterstützt auch Regeln mit mehreren AD-Gruppen

### Logging

Detailliertes Logging in benutzerfreundlichem Format, E-Mail-Alarmfunktion mit Syslog-Unterstützung

### Single-Arm-Modus

Ja

### SonicWALL Virtual Assist oder Virtual Access (zusammen lizenziert)

Verbindung zu Remote-PC, Chat, FTP und Diagnose-Tools

### IPv6-Unterstützung

Basic

### Lastverteilung

HTTP/HTTPS-Lastverteilung mit Failover und Mechanismen wie beispielsweise Weighted Requests, Weighted Traffic oder Least Requests

### Hochverfügbarkeitsoptionen

Nur bei SRA 4200

### Application Offloading

Ja

### Web Application Firewall

Ja

### Hardware

#### Gehärtete Sicherheitsappliance

SRA 1200 Ja

SRA 4200 Ja

#### Hardwarebeschleunigte Verschlüsselung

SRA 1200 Nein

SRA 4200 Ja

#### Schnittstellen

SRA 1200 2 Gigabit Ethernet, 2 USB, 1 Konsolenanschluss

SRA 4200 4 Gigabit Ethernet, 2 USB, 1 Konsolenanschluss

#### Prozessoren

SRA 1200 x86-Hauptprozessor

SRA 4200 x86-Hauptprozessor, Verschlüsselungsbeschleunigung

#### Speicher (RAM)

SRA 1200 1 GB

SRA 4200 2 GB

#### Flash-Speicher

SRA 1200 1 GB

SRA 4200 1 GB

#### Stromversorgung/Netzspannung

SRA 1200 Intern, 100-240 VAC, 50-60 Mhz

SRA 4200 Intern, 100-240 VAC, 50-60 Mhz

#### Leistungsaufnahme (max.)

SRA 1200 53 W

SRA 4200 75 W

#### Wärmeabgabe

SRA 1200 181,0 BTU

SRA 4200 256,0 BTU

#### Abmessungen

SRA 1200 43,2 x 25,7 x 4,5 cm

SRA 4200 43,2 x 25,7 x 4,5 cm

#### Gewicht

SRA 1200 4,30 kg

SRA 4200 4,30 kg

#### WEEE-Gewicht

SRA 1200 4,50 kg

SRA 4200 4,50 kg

#### Erfüllt folgende Standards/Normen

FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, MIC, NOM, UL, cUL, TÜV/GS, CB

#### Umgebungsbedingungen

0-40° C

Luftfeuchtigkeit 5-95 % relative Luftfeuchtigkeit, nicht kondensierend

#### MTBF

SRA 1200 13,0 Jahre

SRA 4200 8,3 Jahre

### SRA Virtual Appliance

#### SRA Virtual Appliance – Voraussetzungen für virtualisierte Umgebung

Hypervisor:	VMware ESXi und ESX (ab Version 4.0)
Appliance-Kapazität (Festplatte):	2 GB
Zugewiesener Speicher:	2 GB

<sup>1</sup> Root-Zugriff erforderlich.

Weitere Informationen über die SonicWALL Secure Remote Access-Lösungen erhalten Sie unter [www.sonicwall.com](http://www.sonicwall.com).

## SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™