



SonicWALL Secure Remote Access-Serie für KMUs

SECURE REMOTE ACCESS

Benutzerfreundlicher und erschwinglicher Secure Remote Access ohne Client

- **Nahtlose Integration mit nahezu allen Firewalls**
- **Konnektivität ohne Clients**
- **NetExtender-Technologie**
- **Gezielte Kontrolle bei der Regelkonfiguration**
- **Personalisiertes Web-Portal**
- **Remote-Support**
- **Zwei-Faktor-Authentifizierung ohne Token**
- **Unterstützung von mobilen Geräten**
- **Application Offloading**
- **Kontextsensitive Hilfe**
- **Erweiterte Sicherheit auf allen Netzwerkebenen**

Die Anzahl und Bedeutung mobiler Arbeitsplätze hat in den letzten Jahren enorm zugenommen. Dadurch steigt auch der Bedarf an Remote Access-Lösungen für den sicheren Zugriff auf Netzwerkressourcen sowie Remote Control-Lösungen für PCs. Mit seiner Secure Remote Access (SRA)-Serie bietet SonicWALL® eine intelligente Lösung für die komplexen Bedürfnisse von Organisationen, die auf mobile Mitarbeiter angewiesen sind. Die SonicWALL-Lösungen lassen sich ebenso leicht bereitstellen wie anwenden – und das zu einem Bruchteil der Kosten vergleichbarer Produkte.

Der Remote-Zugriff auf Unternehmensnetzwerke ist heute ganz unkompliziert: Mobile Mitarbeiter können sich mit einem Standard-Browser an einem Portal anmelden und von dort auf E-Mails, Dateien, Web-Anwendungen und interne Websites zugreifen. Werden weitreichendere Funktionen benötigt, etwa ein sicherer Zugriff auf Firmenserver oder lokale Anwendungen, stellt die Appliance dem Desktop oder Laptop-Computer einen herunterladbaren Thin-Client (NetExtender) bereit.

Mithilfe von SonicWALL Virtual Assist* lassen sich auch Remote-Support-Lösungen ganz unkompliziert implementieren. Das clientlose Remote-Support-Tool ermöglicht es Technikern auf die PCs von Kunden zuzugreifen, um diese zu unterstützen. Auf diese Weise kann der erforderliche Support bedarfsorientiert geleistet werden, was die Kosten niedrig hält.

Funktionen und Vorteile

Nahtlose Integration mit nahezu allen Firewalls.

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

Konnektivität ohne Clients. Macht vorinstallierte VPN-Clients überflüssig, so dass für den Administrator keine aufwändigen Tätigkeiten mehr anfallen.

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

Gezielte Kontrolle bei der Regelkonfiguration.

Mithilfe von Regeln kann der Administrator Benutzern festgelegte Anwendungen/Ressourcen zuordnen und den unberechtigten Zugriff auf bestimmte Netzwerkressourcen sperren.

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.

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. Bietet Remote-Mitarbeitern durch den Zugriff auf das gesamte Intranet sowie auf webbasierte Anwendungen mehr Flexibilität.

Application Offloading.** Durch ein robustes Authentifizierungssystem und granulare Zugriffsregeln können Benutzer sicher auf Webanwendungen zugreifen.

Kontextsensitive Hilfe. Steht dem Benutzer auf der Verwaltungsoberfläche und im Endbenutzer-Portal zur Verfügung und sorgt für mehr Benutzerfreundlichkeit und Flexibilität bei der Verwaltung.

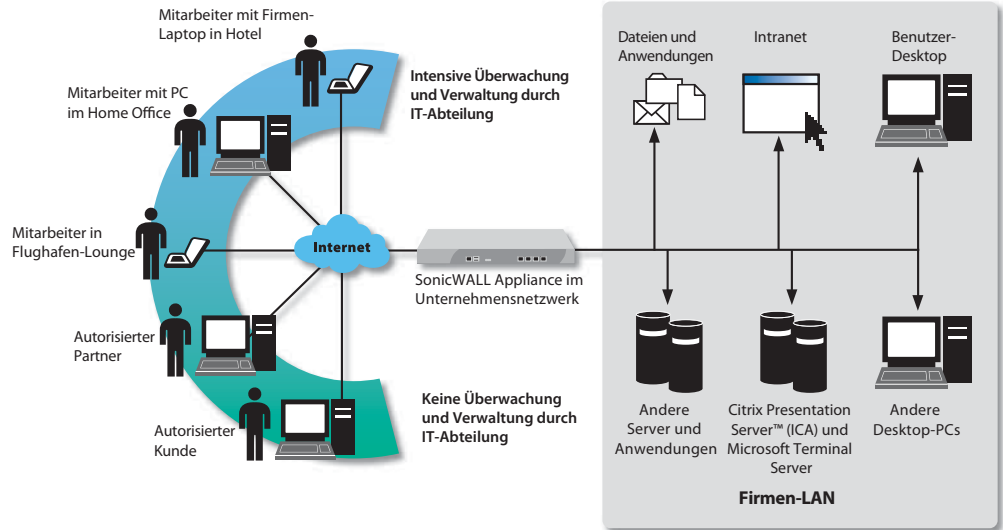
Erweiterte Sicherheit auf allen Netzwerkebenen. Hierfür sorgt die Kombination mit einer SonicWALL Network Security Appliance, die den Verkehr mithilfe der Deep Packet Inspection-Technologie auf Sicherheitsbedrohungen wie Viren, Würmer, Trojaner und Spyware scannt. Diese kombinierte Lösung ist unter dem Namen SonicWALL Clean VPN bekannt.

*Zusätzliche Lizenz erforderlich. Nur als Software-Add-On-Modul bei der SSL-VPN 4000 und SRA 4200 verfügbar.

**Nur bei der SSL-VPN 4000 und SRA 4200 verfügbar

Granularer Zugriff für autorisierte Benutzer

Die SonicWALL Secure Remote Access (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. Entsprechend den IT-Regeln im Unternehmen können Benutzer über ein personalisierbares Portal mit einem Webbrowser auf bestimmte Ressourcen zugreifen.



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



Vielfältige Zugriffsmöglichkeiten

Die SonicWALL SRA-Lösungen für KMUs können 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 webbasierten Zugriff auf Intranet (HTTP, HTTPS)-, Datei (FTP, CIFS)-, Desktop (Citrix®, Terminal Server, VNC)- und Terminal (Telnet, SSH)-Ressourcen

Einfache Verwaltung

Die SSL VPN-Lösungen von SonicWALL 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 ViewPoint-Reporting-Tool von SonicWALL lässt sich der Netzwerkzugriff über die Lösungen mühelos überwachen.



Remote-Support

SonicWALL Virtual Assist* lässt sich über die Verwaltungsoberfläche einfach konfigurieren und lizenzieren und ist eine kosteneffiziente Alternative zu herkömmlichen Remote Support-Tools. Browserbasierte Thin Clients werden automatisch auf den Rechnern von Technikern und Kunden installiert, um eine Cloud-basierte Sitzung über eine SSL VPN-Lösung zu starten.

Erweiterte Sicherheitslösung

Die SonicWALL Secure Remote Access-Appliances lassen sich nahtlos in nahezu jede Netzwerktopologie integrieren und können unkompliziert mit beliebigen Firewalls anderer Anbieter installiert werden. Die Kombination mit einer SonicWALL Network Security/Unified Threat Management (UTM) Firewall Appliance mit Application Firewall und Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service 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.

Auszeichnungen



(SSL-VPN 200)

Zertifikate



(SSL-VPN 200/4000)

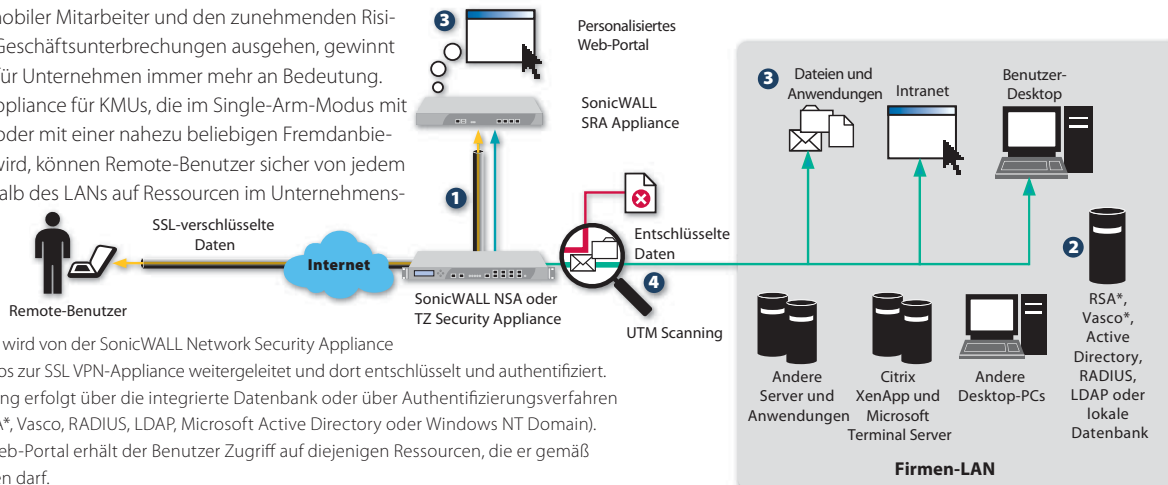


(SSL-VPN 4000)

*Nur bei der SSL-VPN 4000 und SRA 4200 verfügbar

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 für KMUs, die im Single-Arm-Modus mit einem SonicWALL-Produkt oder mit einer nahezu beliebigen Fremdanbieter-Firewall implementiert wird, können Remote-Benutzer sicher von jedem beliebigen Standort außerhalb des LANs auf Ressourcen im Unternehmensnetzwerk zuzugreifen.



1. Eingehender HTTPS-Verkehr wird von der SonicWALL Network Security Appliance der NSA- bzw. TZ-Serie nahtlos zur SSL VPN-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. Der Verkehr wird zur Network Security Appliance der NSA- bzw. TZ-Serie zurückgeleitet und von der SonicWALL Unified Threat Management-Lösung umfassend auf Viren, Würmer, Trojaner, Spyware und andere komplexe Bedrohungen untersucht.

*Nur bei der SRA 4200 und SSL-VPN 4000 verfügbar

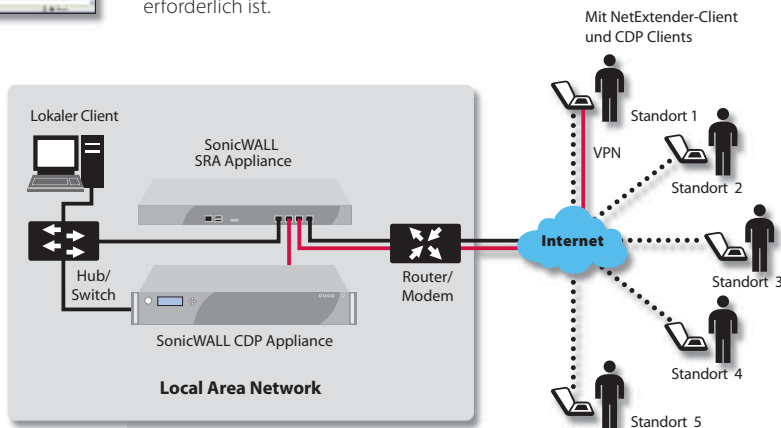


Remote Support-Lösung

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 auf einer SSL-VPN 4000 oder SRA 4200 Appliance kann der Techniker sofort über das Web auf ein Remote-Gerät zugreifen, Dateien übertragen und mit dem Endbenutzer chatten, um das Problem schnell zu analysieren und zu beheben, ohne dass ein vorinstallierter „Fat Client“ erforderlich ist.

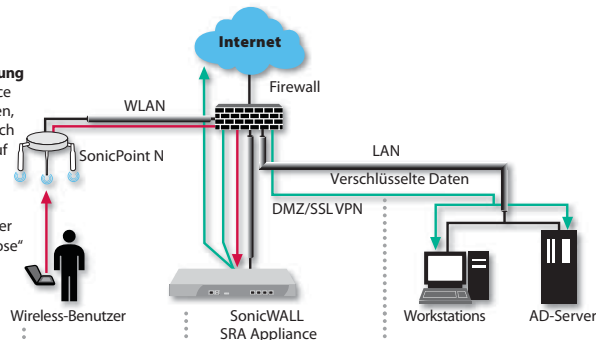
Disaster Recovery-Lösung

Disaster Recovery kann durch eine Katastrophe wie einen Hurrikan oder eine Epidemie ausgelöst werden – aber auch durch kleinere Ereignisse wie einen regionalen Stromausfall, ein Unwetter, eine Grippewelle oder einen Wasserrohrbruch, der ein Bürogebäude unter Wasser setzt. Geschäftsunterbrechungen können dazu führen, dass Unternehmen Geschäfts-Chancen und Umsätze verlieren oder ihren Ruf aufs Spiel setzen. Die SonicWALL SSL VPN- und CDP-Lösungen mit SonicWALL CDP Offsite-Datenbackup-Service-Abo erlauben Mitarbeitern, die nicht in das Firmengebäude kommen können, über eine sichere SSL VPN-Verbindung remote auf die Unternehmensressourcen zuzugreifen. Der Zugriff auf Unternehmensressourcen ist immer gewährleistet, da die Daten sowohl lokal als auch extern gesichert werden.



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-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. Ein SonicWALL SSL VPN, das mit einer SonicWALL UTM Firewall und mehreren SonicPoints implementiert wird, sorgt dafür, 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 SSL VPN-Serie

Leistung

SSL-VPN 200	Empfohlen für Unternehmen mit bis zu 50 Mitarbeitern
Gleichzeitige User-Lizenzen:	Unlimitiert
Empfohlene Anzahl gleichzeitiger Benutzer:	10
SRA 4200	Empfohlen für Unternehmen mit bis zu 500 Mitarbeitern
Maximal zulässige Anzahl gleichzeitiger Virtual Assist-Techniker:	5
Gleichzeitige User-Lizenzen:	Unlimitiert
Empfohlene Anzahl gleichzeitiger Benutzer:	50
SSL-VPN 4000	Empfohlen für Unternehmen mit mindestens 500 Mitarbeitern
Maximal zulässige Anzahl gleichzeitiger Virtual Assist-Techniker:	25
Gleichzeitige User-Lizenzen:	Unlimitiert
Empfohlene Anzahl gleichzeitiger Benutzer:	200

Die wichtigsten Funktionen

Unterstützte Anwendungen	Proxy	Citrix (ICA),* HTTP, HTTPS, FTP, SSH, Telnet, RDP, VNC, Windows* File Sharing (Windows SMB/CIFS)
	NetExtender	Sämtliche TCP/IP-basierte Anwendungen: ICMP, VoIP, IMAP, POP, SMTP etc.
Verschlüsselung		DES (128), 3DES (128, 256), AES (128, 192, 256), ARC4 (128), MD5, SHA-1
Authentifizierung		RSA*, Vasco, Einmalpasswörter, interne Benutzerdatenbank, RADIUS, LDAP, Microsoft Active Directory, Windows NT Domain
Unterstützung mehrerer Domänen		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	Unterstützung optionaler Client-Zertifikate*
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) Win Mobile 5 (Pocket PC), Win Mobile 6 (Classic/Professional), MacOS 10.4 und höher (PowerPC und Intel), Linux Fedora Core 3 und höher / Ubuntu 7 und höher / OpenSUSE
Unterstützte Webbrowser		Microsoft Internet Explorer, Firefox Mozilla
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)
Nutzungskontrolle		Grafische Anzeige der Speicher-, CPU und Bandbreitennutzung* sowie der Benutzer
Logging		Detailliertes Logging in benutzerfreundlichem Format, E-Mail-Alarmfunktion mit Syslog-Unterstützung
Single-Arm-Modus		Ja
SonicWALL Virtual Assist*		Verbindung zu Remote-PC, Chat, FTP und Diagnose-Tools
IPv6-Unterstützung*		Basic
Application Offloading*		Ja

Hardware

Gehärtete Sicherheitsappliance	SSL-VPN 200	Ja
	SRA 4200	Ja
	SSL-VPN 4000	Ja
Hardwarebeschleunigte Verschlüsselung	SSL-VPN 200	Ja
	SRA 4200	Ja
	SSL-VPN 4000	Ja
Schnittstellen	SSL-VPN 200	(5) 10/100 Ethernet
	SRA 4200	(4) Gigabit Ethernet, (2) USB, (1) Konsolenanschluss
	SSL-VPN 4000	(6) 10/100 Ethernet, (1) serieller Anschluss
Prozessoren	SSL-VPN 200	SonicWALL Security-Prozessor, Verschlüsselungsbeschleunigung
	SRA 4200	x86-Hauptprozessor, Verschlüsselungsbeschleunigung
	SSL-VPN 4000	P4 Celeron-Hauptprozessor, Verschlüsselungsbeschleunigung
Speicher (RAM)	SSL-VPN 200	128 MB
	SRA 4200	2 GB
	SSL-VPN 4000	1 GB
Flash-Speicher	SSL-VPN 200	16 MB
	SRA 4200	1 GB
	SSL-VPN 4000	128 MB
Stromversorgung	SSL-VPN 200	20 W, 12 VDC, 1,66 A
	SRA 4200	Intern
	SSL-VPN 4000	Intern
Leistungsaufnahme (max.)	SSL-VPN 200	10,4 W
	SRA 4200	75 W
	SSL-VPN 4000	108 W
Wärmeabgabe	SSL-VPN 200	35,6 BTU
	SRA 4200	256,0 BTU
	SSL-VPN 4000	368,3 BTU
Abmessungen	SSL-VPN 200	18,9 x 11,6 x 2,7 cm
	SRA 4200	43,2 x 25,7 x 4,5 cm
	SSL-VPN 4000	43,2 x 33,7 x 4,5 cm
Gewicht	SSL-VPN 200	1,36 kg
	SRA 4200	6,80 kg
	SSL-VPN 4000	8,39 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	SSL-VPN 200	9,0 Jahre
	SRA 4200	8,3 Jahre
	SSL-VPN 4000	9,2 Jahre

* Nur bei der SSL-VPN 4000 und SRA 4200 verfügbar

Weitere Informationen über die SonicWALL Secure Remote Access-Lösungen für KMUs erhalten Sie unter www.sonicwall.com/de.

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

