Secure Remote Access-Serie

Erhöhen Sie die Produktivität Ihrer mobilen und Remote-Mitarbeiter und verbessern Sie den Schutz vor Bedrohungen

Mit der zunehmenden Verbreitung von Mobilgeräten am Arbeitsplatz steigt auch die Nachfrage nach einem sicheren Zugriff auf geschäftskritische Anwendungen, Daten und Ressourcen. Ein erweiterter Zugriff bietet Unternehmen handfeste Produktivitätsvorteile, öffnet aber gleichzeitig einer Vielzahl von Bedrohungen Tür und Tor.

Die Gefahren lauern überall: Unternehmensdaten könnten über fremde Wireless-Netzwerke abgefangen werden, unbefugte Benutzer könnten über verloren gegangene oder gestohlene Geräte auf Unternehmensressourcen zugreifen oder Mobilgeräte von Mitarbeitern könnten als Einfallstor für Malware dienen und das Netzwerk infizieren. Zudem droht der Verlust von Unternehmensdaten, die auf Geräten gespeichert sind, etwa wenn unerwünschte private Anwendungen oder unberechtigte Benutzer darauf zugreifen.

Der Schutz dieser Geräte durch das Unternehmen gestaltet sich zunehmend schwieriger, da es immer häufiger der Benutzer selbst ist, der sein Gerät auswählt und verwaltet. Organisationen brauchen eine leistungsstarke Lösung, die einen sicheren Zugriff gewährleistet und nur autorisierten Benutzern sowie Geräten, die den Sicherheitsrichtlinien entsprechen, einen Zugang in das Netzwerk ermöglicht. Gleichzeitig muss diese Lösung den Schutz aller Unternehmensdaten sicherstellen – egal ob diese gerade übertragen werden oder im Gerät ruhen. Leider kommen hierbei oft komplexe, mehrteilige Lösungen verschiedener Anbieter zum Einsatz, die schwer zu verwalten sind und die TCO für den mobilen Zugriff deutlich in die Höhe treiben. Benötigt werden jedoch benutzerfreundliche, kostengünstige und sichere Lösungen für den mobilen Zugriff, die genau auf die Anforderungen der zunehmend mobilen Mitarbeiter zugeschnitten sind.

Mit den Appliances der Dell™ SonicWALL™ Secure Remote Access (SRA)-Serie profitieren mobile und Remote-Mitarbeiter von einem schnellen, einfachen und regelbasierten Zugriff auf geschäftskritische Anwendungen, Daten und Ressourcen, ohne die Sicherheit zu beeinträchtigen – ganz gleich, ob sie dabei verwaltete oder unverwaltete Smartphones, Tablets oder Laptops verwenden.

Für Mobilgeräte umfasst die Lösung die intuitive SonicWALL Mobile Connect™-Anwendung. Diese ermöglicht iOS-, Android-, Kindle Fire-, Windows- und Mac OS X-Geräten einen sicheren Zugriff auf zugelassene Netzwerkressourcen, einschließlich gemeinsam genutzter Ordner, Client-Server-Anwendungen, Intranet-Sites und E-Mail.

Benutzer und IT-Administratoren können die SonicWALL Mobile Connect-Applikation im Apple-eigenen App Store, über Google Play oder im Kindle Store herunterladen. Neu mit Windows 8.1: Auf Windows-Tablets und -Laptops ist Mobile Connect vorinstalliert. Für PCs und Laptops, darunter Windows®-, Mac OS- und Linux®-Computer, unterstützt die Lösung einen sicheren, clientlosen Zugriff per Browser oder einen Thin-Client-VPN-Zugriff.

Die SRA-Serie gewährt nur autorisierten Benutzern und vertrauenswürdigen Geräten Zugriff auf zugelassene Ressourcen und bietet so effizienten Schutz vor unberechtigtem Zugriff und Malware. Bei Integration mit einer Dell SonicWALL Next-Generation Firewall als Clean VPN™ bietet die kombinierte Lösung eine zentrale Zugriffskontrolle sowie Malware-Schutz, Anwendungskontrolle und Content Filtering. Die Multi-Layer-Schutzfunktionen von Dell SonicWALL Clean VPN™ entschlüsseln und dekontaminieren sämtlichen autorisierten SSL-VPN-Verkehr, bevor er in das Netzwerk gelangt.

Vorteile:

- Plattformübergreifende Unterstützung für eine erhöhte Produktivität mobiler Mitarbeiter
- Verringerter IT-Verwaltungsaufwand und reduzierte TCO dank einheitlichem Access Gateway für den Zugriff auf sämtliche Netzwerkressourcen, Zugriff ohne Client oder mit webbasierten Clients sowie mit mobiler Anwendung
- Einheitliche Benutzererfahrung über alle Betriebssysteme hinweg verbessert die Benutzerfreundlichkeit von sämtlichen Endpunkten aus
- Mobile Connect-App für iOS, Android, Windows 8.1 und Mac OS X verbessert die Benutzerfreundlichkeit des Mobilgeräts
- Kontextsensible Authentifizierung stellt sicher, dass nur autorisierten Benutzern und vertrauenswürdigen Mobilgeräten Zugriff gewährt wird
- Sicheres Durchsuchen von Dateien im Intranet und integrierte Datensicherheit mit nur einem Klick
- Adaptive Adressierungs- und Routingfunktionen nutzen geeignete Zugriffsverfahren und Sicherheitsniveaus
- Setup-Assistent vereinfacht die Implementierung
- Effiziente, objektbasierte Regelverwaltung für sämtliche Benutzer, Gruppen, Ressourcen und Geräte
- Web Application Firewall und PCI-Compliance

Funktionen

Plattformübergreifende Unterstützung. Die SRA-Serie lässt sich über eine Vielzahl von Geräten und Umgebungen hinweg einsetzen, darunter Smartphones, Tablets, Laptops, Desktop-PCs und öffentliche Terminals. Dabei spielt es keine Rolle, ob es sich um verwaltete oder unverwaltete Geräte handelt. Mit Dell SonicWALL SRA können Benutzer von gängigen Geräten aus (z. B. iOS- und Android-Smartphones und -Tablets, Windows 8.1-Tablets und -Laptops sowie Mac OS®-, Windows- und Linux-Computern) ohne Weiteres auf E-Mail, Dateien, Anwendungen usw. zugreifen und so ihre Produktivität steigern.

Einheitliches Access Gateway mit mobilen Apps, ohne Client bzw. mit webbasierten Clients. Mit der SRA-Serie können IT-Administratoren Kosten einsparen, indem sie ein einheitliches, sicheres und einfach zu verwaltendes Access Gateway implementieren. Interne wie externe Benutzer können so per SSL-VPN auf sämtliche Netzwerkressourcen zugreifen – darunter web- und hostbasierte Anwendungen sowie Client-Server- und Back-Connect-Anwendungen wie VoIP. Die SRA-Lösungen von Dell SonicWALL funktionieren entweder ohne Client mit einem Zugriff per Browser auf das anpassbare SRA WorkPlace-Portal oder sie nutzen mobile Anwendungen bzw. webbasierte Lightweight-Clients, was den Verwaltungsaufwand und die Support-Anfragen reduziert. Das Dell SonicWALL WorkPlace-Portal bietet Administratoren jetzt noch mehr Kontrolle beim Zugriff sowie bei Inhalt und Gestaltung des Portals.

Einheitliche Benutzererfahrung über alle Betriebssysteme hinweg. Die SRA-Serie sorgt für einen transparenten Zugriff auf Netzwerkressourcen von beliebigen Netzwerkumgebungen und Geräten aus. Die SRA-Appliance dient als Gateway für den Zugriff per Smartphone, Tablet, Laptop und Desktop-PC und bietet Benutzern von verwalteten und unverwalteten Geräten über alle Betriebssysteme hinweg – u. a. Windows, Mac OS, iOS, Android, Kindle und Linux – eine einheitliche Benutzererfahrung.

SonicWALL Mobile Connect-App. SonicWALL Mobile Connect™ für iOS-, Mac OS X-, Android-, Kindle- und Windows 8.1-Mobilgeräte bietet einen einfachen Zugriff auf Netzwerkressourcen über verschlüsselte SSL-VPN-Verbindungen (z. B. in Unternehmen oder Bildungseinrichtungen). Mobile Connect lässt sich einfach im Apple-eigenen App Store℠, über Google Play oder in Kindle Stores herunterladen und in Windows 8.1-Geräte einbetten.

Kontextorientierte Sicherheitsfunktionen. Der Zugriff auf das Unternehmensnetzwerk wird erst dann gewährt, wenn der Nutzer authentifiziert und die Integrität des Mobilgeräts verifiziert wurden.

Schutz für gespeicherte Daten auf Mobilgeräten. Authentifizierte Benutzer können zugelassene Intranetdateifreigaben und Dateien aus der Mobile Connect-Anwendung sicher durchsuchen und anzeigen. Administratoren können Regeln für die Verwaltung mobiler Anwendungen erstellen und durchsetzen.

Adaptive Adressierungs- und Routingfunktionen. Adressierung und Routing werden dynamisch an das jeweilige Netzwerk angepasst. Die bei anderen Lösungen häufig auftretenden Adress- und Routingkonflikte gehören damit der Vergangenheit an.

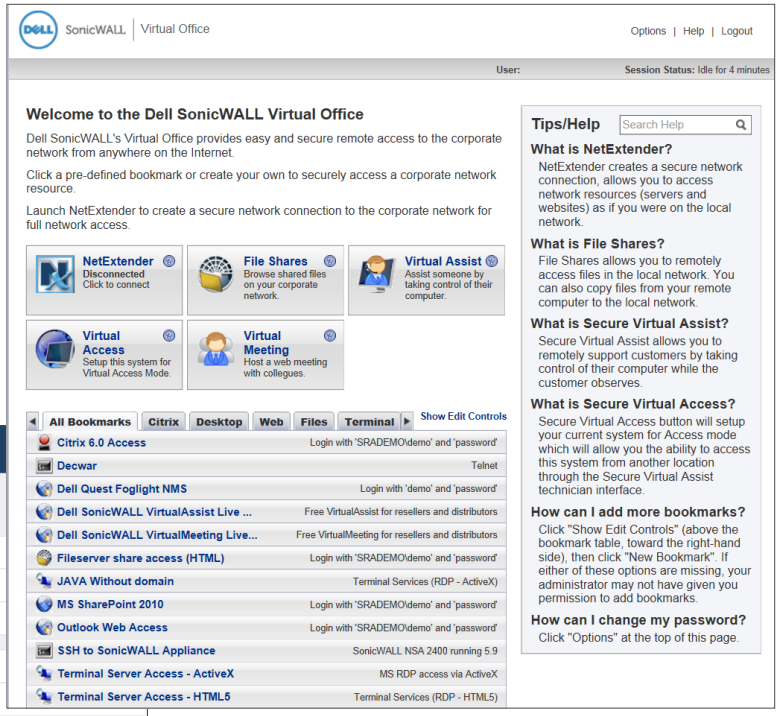
Dell SonicWALL-Setup-Assistent. Die SRA-Appliances können in Minutenschnelle installiert und bereitgestellt werden. Der Setup-Assistent bietet maximale Benutzerfreundlichkeit und sorgt für eine schnelle und unkomplizierte Installation und Bereitstellung.

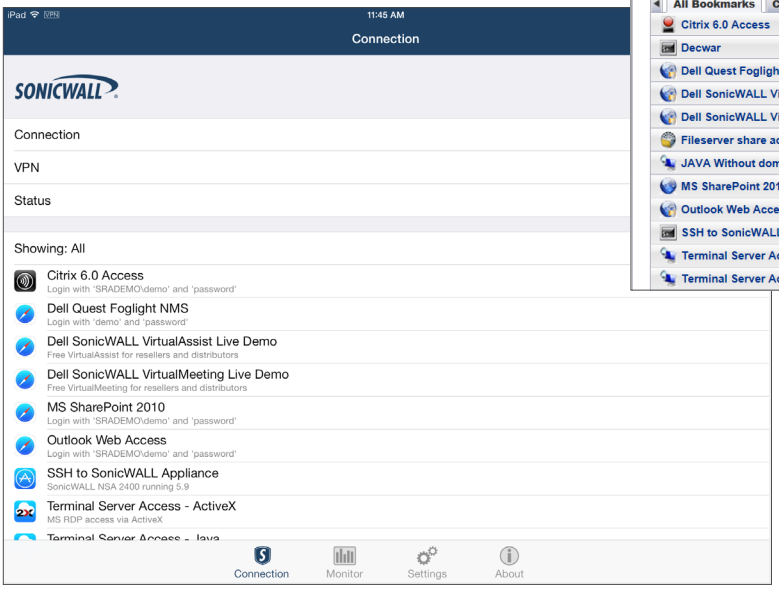
Unified Policy. Dell SonicWALL SRA Unified Policy bietet ein einfaches objektbasiertes Policy Management für sämtliche Benutzer, Gruppen, Ressourcen und Geräte und ermöglicht eine granulare Kontrolle mittels Benutzerauthentifizierung und Abfrage von Endpunkten.

Dell SonicWALL SRA-Serie für KMUs – sicherer Remote-Zugriff jederzeit und von jedem Ort aus

Einfacher und sicherer mobiler Zugriff auf Ressourcen

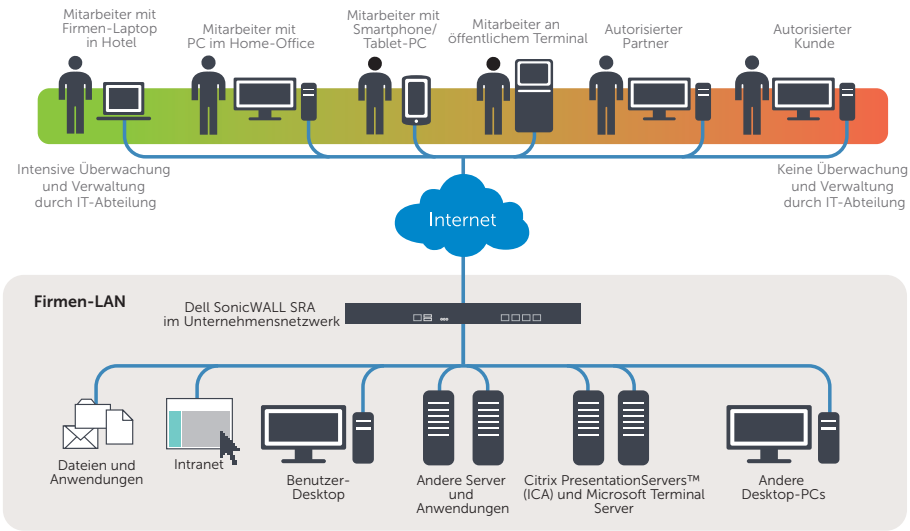
Die SRA-Serie für KMUs kann eingesetzt werden, um Windows-, Mac OS-, iOS-, Linux-, Android- und Kindle-Benutzern Zugriff auf vielfältige Ressourcen zu bieten.



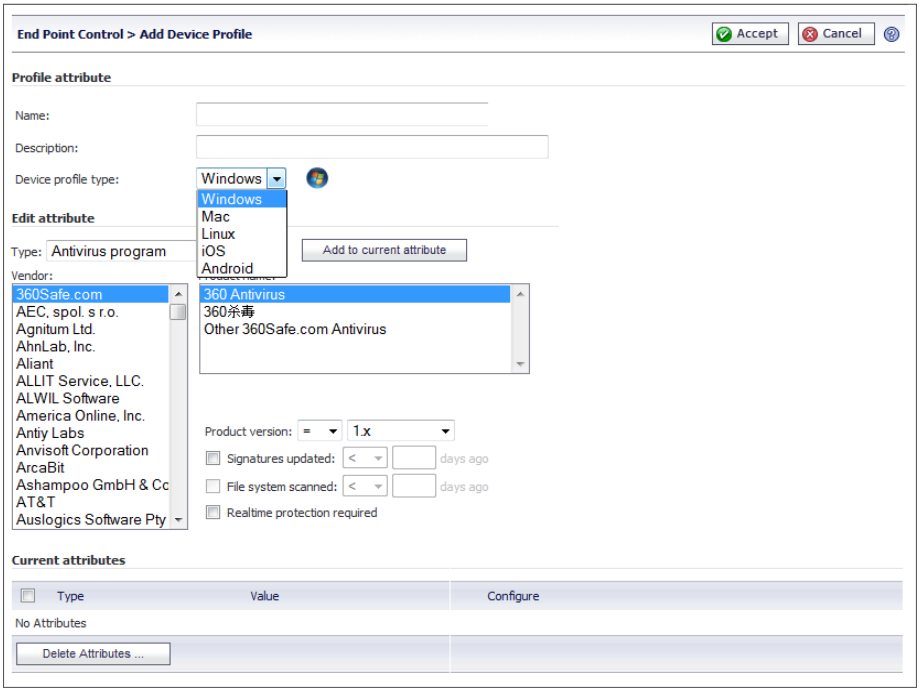


Granularer Zugriff für autorisierte Benutzer

Mittels regelbasierten, granularen Zugangssteuerungsoptionen weitet die SRA-Serie für kleine und mittlere Unternehmen (KMUs) den sicheren mobilen und Remote-Zugriff von verwalteten Mitarbeiter-PCs auf die unverwalteten Geräte mobiler sowie remote tätiger Mitarbeiter, Partner und Kunden aus.



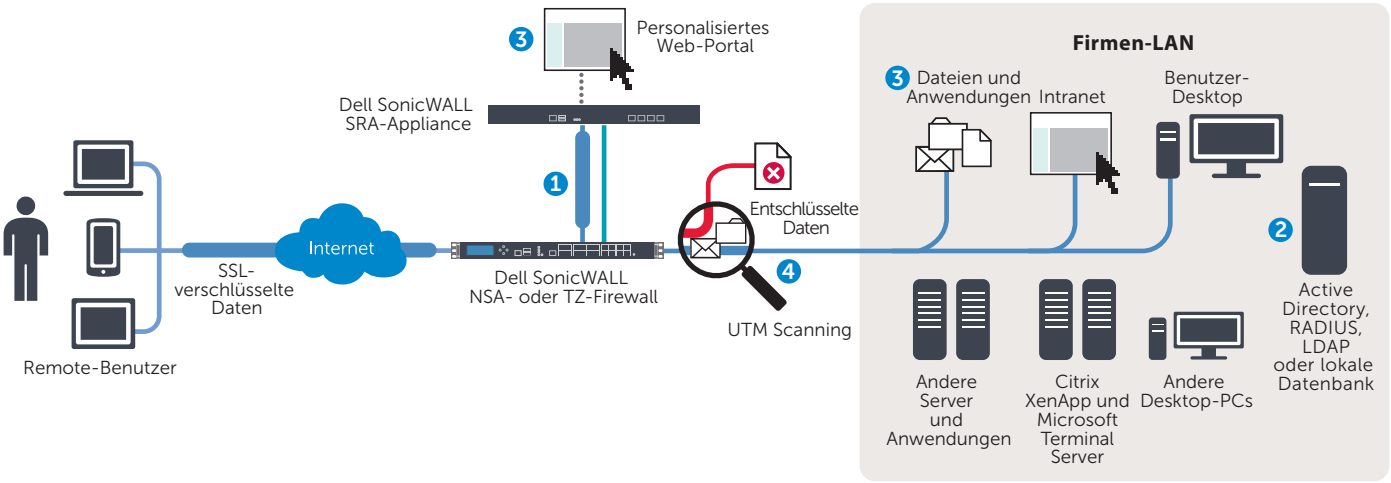
Kontextsensible Authentifizierung
Eine erstklassige kontextsensible Authentifizierung garantiert, dass nur autorisierte Benutzer und vertrauenswürdige Geräte Zugang erhalten. Bevor Mobilgeräten der Zugriff gewährt wird, werden sie abgefragt und auf essenzielle sicherheitsrelevante Informationen überprüft, u. a. Jailbreak- bzw. Root-Status, Geräte-ID, Zertifikatsstatus und Version des Betriebssystems. Auch Laptops und PCs werden auf vorhandene bzw. fehlende Sicherheitssoftware, Client-Zertifikate und Geräte-ID überprüft. Wenn ein Gerät die Regelanforderungen nicht erfüllt, wird der Zugriff auf das Netzwerk verweigert. Dem Benutzer wird die Nichteinhaltung mitgeteilt.



Schutz für ruhende Daten auf Mobilgeräten
Authentifizierte Mobile Connect-Nutzer können zugelassene Intranetdateifreigaben und Dateien innerhalb der Mobile Connect-Anwendung sicher durchsuchen und anzeigen. Administratoren können für Mobile Connect Regeln zur Verwaltung mobiler Anwendungen erstellen und durchsetzen. Auf diese Weise lässt sich kontrollieren, ob die angezeigten Dateien auch in anderen Anwendungen (nur iOS 7) angezeigt, in die Zwischenablage kopiert, gedruckt oder in der Mobile Connect-Anwendung sicher zwischengespeichert werden können. Bei iOS 7-Geräten können Administratoren so Unternehmensdaten von privaten Daten auf dem Gerät trennen und das Risiko eines Datenverlusts reduzieren. Wenn außerdem die Authentifizierungsdaten des Benutzers gesperrt sind, werden in Mobile Connect gespeicherte Inhalte blockiert und können nicht mehr genutzt oder angezeigt werden.

Clean VPN
Bei Einsatz mit einer Dell SonicWALL Next-Generation Firewall stellt Mobile Connect ein Clean VPN™ bereit, das als zusätzliche Schutzschicht sämtlichen SSL-VPN-Verkehr entschlüsselt und auf Malware überprüft, bevor dieser das Netzwerk erreicht.

Web Application Firewall und PCI-Compliance
Der Dell SonicWALL Web Application Firewall Service bietet Unternehmen eine umfassende, erschwingliche und gut integrierte Compliance-Lösung für webbasierte Anwendungen, 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 unbekannten Sicherheitsschwachstellen. 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 Web Application Firewall Service ist eine leicht zu implementierende Lösung mit erweiterten Statistik- und Reporting-Optionen zur Einhaltung von Compliance-Richtlinien.



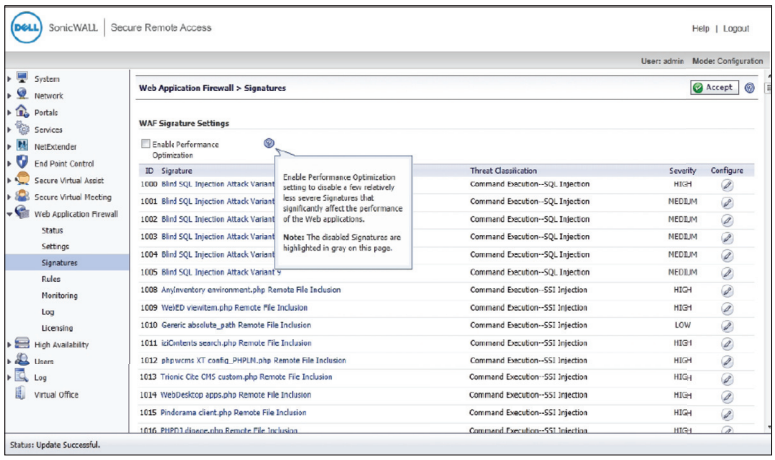
1 Eingehender HTTPS-Verkehr wird von Firewalls der Dell SonicWALL NSA- oder TZ-Serie nahtlos zur Dell SonicWALL SRA-Appliance weitergeleitet und dort entschlüsselt und authentifiziert.

2 Die Benutzerauthentifizierung erfolgt über die integrierte Datenbank oder über Authentifizierungsverfahren von Drittanbietern, wie z. B. LDAP, Active Directory, Radius, Dell Quest Defender und andere Lösungen mit Zwei-Faktor-Authentifizierung.

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.

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 Dell SonicWALL Global Management System (GMS Version 4.0 oder höher) zentral verwaltet werden. Mit dem Analyzer-Reporting-Tool von Dell SonicWALL lässt sich der Netzwerkzugriff über die Lösungen mühelos überwachen.



Technische Daten

Dell SonicWALL SRA-Serie für KMUs

Leistung

SRA 1600	Empfohlen für Unternehmen mit bis zu 50 Mitarbeitern
Gleichzeitige Benutzer-Lizenzen:	Angefangen bei 5 gleichzeitigen Benutzern. Zusätzliche Benutzer-Lizenzen in Schritten von 5 und 10 Benutzern verfügbar.
Secure Virtual Assist-Techniker:	inklusive 30-Tage-Testversion / max. 10 gleichzeitige Techniker
Benutzerkapazität*:	5 enthalten / 50 lizenzierbar / 25 empfohlen
SRA 4600	Empfohlen für Unternehmen mit bis zu 250 Mitarbeitern
Gleichzeitige Benutzer-Lizenzen:	Angefangen bei 25 Benutzern. Zusätzliche Benutzer-Lizenzen in Schritten von 10, 25 und 100 Benutzern verfügbar.
Secure Virtual Assist-Techniker:	inklusive 30-Tage-Testversion / max. 25 gleichzeitige Techniker
Benutzerkapazität*:	25 enthalten / 500 lizenzierbar / 100 empfohlen
Max. Anzahl zugelassener Meetingteilnehmer:	75
SRA Virtual Appliance	Empfohlen für Unternehmen jeder Größenordnung
Gleichzeitige Benutzer-Lizenzen:	Benutzer-Lizenzen in Schritten von 5, 10 und 25 Benutzern verfügbar.
Secure Virtual Assist-Techniker:	inklusive 30-Tage-Testversion / max. 25 gleichzeitige Techniker
Benutzerkapazität*:	5 enthalten / 50 lizenzierbar
Max. Anzahl zugelassener Meetingteilnehmer:	75

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, SHA-256, SHA-384, SSLv3, TLSv1, TLS 1.1, TLS 1.2, 3DES (168, 256), AES (256), RSA, DHE
Authentifizierung	Dell Quest Defender, andere Lösungen mit Zwei-Faktor-Authentifizierung, Einmalpasswörter, interne Benutzerdatenbank, RADIUS, LDAP, Microsoft Active Directory
RDP-Unterstützung	Ja. Mit Unterstützung für Terminal Server-Farmen (nur JAVA-Client) und Remote-Anwendungen (nur Active-X), HTML5
Unterstützung mehrerer Domänen	Ja
Unterstützung mehrerer Portale	Ja
Granulare Zugriffskontrolle	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	Konfigurierbar. 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-Geräten	
Proxy	Alle Betriebssysteme
NetExtender	Windows 2003, 2008, XP/Vista (32 Bit und 64 Bit), 7 (32 Bit und 64 Bit), 8 (32 Bit und 64 Bit), Mac OS 10.4+, Linux Fedora Core 3+ / Ubuntu 7+ / OpenSUSE, Linux 64 Bit
Mobile Connect	iOS 4.2 und höher, OS X 10.9 und höher, Android 4.0 und höher, Kindle Fire mit Android 4.0 und höher sowie Windows 8.1
Unterstützte Webbrowser	Internet Explorer, 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 und höher) SNMP-Unterstützung
Nutzungskontrolle	Grafische Überwachung von Speicher, CPU, Benutzern und Bandbreitennutzung
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
Dell SonicWALL Secure Virtual Assist oder Secure Virtual Access (zusammen lizenziert)	Verbindung zu Remote-PC, Chat und FTP sowie Sitzungsaufzeichnung und Diagnosetools
Secure Virtual Meeting**	Verbindet Meetingteilnehmer unmittelbar auf sichere und kostengünstige Art miteinander
IPv6-Unterstützung	Basic
Lastverteilung	HTTP-/HTTPS-Lastverteilung mit Failover und Mechanismen wie z. B. Weighted Requests, Weighted Traffic oder Least Requests
Hochverfügbarkeitsoptionen	nur bei SRA 4600
Application Offloading	Ja
Web Application Firewall	Ja
End Point Control (EPC)	Ja
Geolocation-basierte Regeln	Ja
Botnet-Filter	Ja

Hardware

Gehärtete Sicherheitsappliance	
SRA 1600	Ja
SRA 4600	Ja
Schnittstellen	
SRA 1600	(2) Gigabit-Ethernet, (2) USB, (1) Konsolenanschluss
SRA 4600	(4) Gigabit-Ethernet, (2) USB, (1) Konsolenanschluss
Prozessoren	
SRA 1600	x86-Hauptprozessor
SRA 4600	x86-Hauptprozessor
Speicher (RAM)	
SRA 1600	1 GB
SRA 4600	2 GB
Flash-Speicher	
SRA 1600	1 GB
SRA 4600	1 GB
Stromversorgung/Netzspannung	
SRA 1600	Intern, 100–240 VAC, 50–60 MHz
SRA 4600	Intern, 100–240 VAC, 50–60 MHz
Leistungsaufnahme (max.)	
SRA 1600	47 W
SRA 4600	50 W
Wärmeabgabe (ges.)	
SRA 1600	158,0 BTU
SRA 4600	171,0 BTU
Abmessungen	
SRA 1600	43,18 x 25,73 x 4,45 cm
SRA 4600	43,18 x 25,73 x 4,45 cm
Gewicht	
SRA 1600	4,30 kg
SRA 4600	4,30 kg
WEEE-Gewicht	
SRA 1600	4,50 kg
SRA 4600	4,50 kg
Erfüllt folgende Standards/Normen	FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TÜV/GS, CB
Umgebungsbedingungen	Temperatur: 0–40 ˚C Luftfeuchtigkeit: 5–95 % relative Luftfeuchtigkeit, nicht kondensierend
MTBF	
SRA 1600	18,3 Jahre
SRA 4600	17,8 Jahre

SRA Virtual Appliance

SRA Virtual Appliance – Mindestvoraussetzungen für virtualisierte Umgebung	
Hypervisor:	VMware ESXi und ESX (ab Version 4.0)
Appliance-Kapazität (Festplatte):	2 GB
Zugewiesener Speicher:	2 GB

*Die empfohlene Anzahl unterstützter Benutzer basiert auf Faktoren wie Zugriffsmechanismen, Anwendungsnutzung und Umfang des Anwendungsverkehrs

**Nur in Verbindung mit Secure Virtual Assist für SRA 4600 und SRA Virtual Appliances erhältlich

SRA 1600, 5 Benutzer 01-SCC-6594

SRA 1600 zusätzliche Benutzer (max. 50 Benutzer)
Zusätzlich 5 gleichzeitige Benutzer 01-SSC-7138
Zusätzlich 10 gleichzeitige Benutzer 01-SSC-7139

SRA 1600 Support
Dell SonicWALL Dynamic Support 24/7 für bis zu 25 Benutzer (1 Jahr) 01-SSC-7141
Dell SonicWALL Dynamic Support 8/5 für bis zu 25 Benutzer (1 Jahr) 01-SSC-7144

SRA 4600, 25 Benutzer 01-SSC-6596

SRA 4600 zusätzliche Benutzer (max. 500 Benutzer)
Zusätzlich 10 gleichzeitige Benutzer 01-SSC-7118
Zusätzlich 25 gleichzeitige Benutzer 01-SSC-7119
Zusätzlich 100 gleichzeitige Benutzer 01-SSC-7120

SRA 4600 Support
Dell SonicWALL Dynamic Support 24/7 für bis zu 100 Benutzer (1 Jahr) 01-SSC-7123
Dell SonicWALL Dynamic Support 8/5 für bis zu 100 Benutzer (1 Jahr) 01-SSC-7126
Dell SonicWALL Dynamic Support 24/7 für 101 bis 500 Benutzer (1 Jahr) 01-SSC-7129
Dell SonicWALL Dynamic Support 8/5 für 101 bis 500 Benutzer (1 Jahr) 01-SSC-7132

SRA Virtual Appliance
Dell 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
Dell SonicWALL Dynamic Support 8/5 für bis zu 25 Benutzer (1 Jahr) 01-SSC-9188
Dell SonicWALL Dynamic Support 24/7 für bis zu 25 Benutzer (1 Jahr) 01-SSC-9191
Dell SonicWALL Dynamic Support 8/5 für bis zu 50 Benutzer (1 Jahr) 01-SSC-9194
Dell SonicWALL Dynamic Support 24/7 für bis zu 50 Benutzer (1 Jahr) 01-SSC-9197

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

Für diese Appliance-Serie sind die Security Monitoring Services von Dell SecureWorks verfügbar. Weitere Informationen erhalten Sie unter **www.dell.com/secureworks.**

Weitere Informationen:

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
Tel.: +1 408.745.9600
Fax: +1 408.745.9300

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
Informationen zu unseren Niederlassungen außerhalb Nordamerikas finden Sie auf unserer Website.

DataSheet-SRASeries-A4-TD611-20140207