Appliances der Secure Remote Access Serie

Für mehr Produktivität Ihrer mobilen und Remote-Mitarbeiter bei gleichzeitigem Schutz vor Bedrohungen

Die Dell SonicWALL Secure Mobile Access (SRA) Serie bietet mobilen und Remote-Mitarbeitern, die im Rahmen einer BYOD-Initiative verwaltete oder nicht verwaltete Smartphones, Tablet-PCs oder Notebooks verwenden, schnell und einfach richtliniengesteuerten Zugriff auf unternehmenskritische Anwendungen, Daten und Ressourcen, ohne die Sicherheit Ihrer Unternehmensdaten zu gefährden.

Für mobile Geräte umfasst die Lösung auch die intuitive Dell SonicWALL Mobile Connect App, die gewährleistet, dass Sie von iOS, Android, Kindle Fire, Windows oder Mac OS X Geräten sicher auf autorisierte Netzwerkressourcen zugreifen können. Zu diesen zählen unter anderem freigegebene Ordner, Anwendungen auf Client-Servern, Intranetseiten und E-Mails.

Benutzer und IT-Administratoren können die Mobile Connect App über den Apple App Store, Google Play oder den Kindle Store herunterladen. Auf Smartphones, Tablet-PCs und Notebooks mit Windows 8.1 ist die Mobile Connect App werkseitig vorinstalliert. Die Lösung unterstützt clientlosen, sicheren Browserzugriff, inklusive Unterstützung für branchenübliche HTML5-Browser und Thin Client-VPN-Zugriff für PCs und Notebooks, darunter Windows, Mac OS X und Linux Geräte.

Dabei gewähren die SRA Appliances ausschließlich autorisierten Benutzern und vertrauenswürdigen Geräten Zugriff auf genehmigte Ressourcen und schützt sie so vor nicht autorisiertem Zugriff und Malware. In Kombination mit einer Dell SonicWALL Firewall der nächsten Generation – und somit einem Clean VPN – profitieren Sie von zentralisierter Zugriffssteuerung, Malware-Schutz, Anwendungskontrolle und Inhaltsfilterung. Das Clean VPN ermöglicht mehrschichtigen Schutz und entschlüsselt und neutralisiert jeglichen autorisierten SSL-VPN-Datenverkehr, bevor die Daten in die Netzwerkumgebung gelangen.

Gründe für die Implementierung einer SRA Appliance

Heutzutage kommen im Arbeitsalltag immer mehr mobile Geräte zum Einsatz. Für Unternehmen wird es angesichts dieser Entwicklung immer wichtiger, den sicheren Zugriff auf geschäftskritische Anwendungen, Daten und Ressourcen zu ermöglichen. Wenn sie diesen Zugriff gewähren, profitieren Organisationen von entscheidenden Produktivitätsvorteilen. Doch gleichzeitig setzen sie ihr Unternehmen dadurch auch erheblichen Risiken aus.

So kann es beispielsweise passieren, dass ein nicht autorisierter Benutzer über ein verlorenes oder gestohlenes Gerät auf Unternehmensressourcen zugreift, dass das mobile Gerät eines Mitarbeiters genutzt wird, um das Netzwerk über dieses mit Malware zu infizieren oder dass nicht autorisierte Benutzer über Wireless-Netzwerke von Drittanbietern an Unternehmensdaten gelangen. Zum Verlust von auf Geräten gespeicherten Unternehmensdaten kann es auch kommen, wenn nicht autorisierte Benutzer oder persönliche Anwendungen auf diese Daten zugreifen.

Die Sicherheit dieser Geräte zu gewährleisten wird immer schwieriger, da Unternehmen nicht unbedingt Einfluss auf die Wahl der Geräte oder deren Verwaltung haben. Organisationen müssen Lösungen für sicheren Zugriff implementieren, um sicherzustellen, dass ausschließlich autorisierte Benutzer und Geräte im Einklang mit Sicherheitsrichtlinien Zugang zum Netzwerk erhalten und dass Unternehmensdaten stets geschützt sind – bei der Übertragung ebenso wie am Speicherort. Allzu häufig bedeutet dies, dass komplexe Einzellösungen verschiedener Anbieter implementiert werden, die die mit der Gewährung des mobilen Zugriffs verbundenen Gesamtkosten deutlich erhöhen. Organisationen benötigen benutzerfreundliche, kosteneffiziente Lösungen für sicheren mobilen Zugriff, die den Anforderungen ihrer zunehmend mobilen Mitarbeiter gerecht werden.

Vorteile:

- Zentrales Zugriffs-Gateway für alle Netzwerkressourcen, mit Zugriff über mobile Anwendungen, Web-Clients oder auch clientlos, senkt den IT-Aufwand und die Gesamtbetriebskosten
- Einheitliche Benutzererfahrung unter allen Betriebssystemen für maximale Benutzerfreundlichkeit auf jedem beliebigen Endgerät
- Mobile Connect App für iOS, Android, Windows 8.1 und Mac OS X Geräte für komfortablen Zugriff über mobile Geräte
- Kontextbezogene Authentifizierung stellt sicher, dass ausschließlich autorisierte Benutzer und vertrauenswürdige mobile Geräte Zugriff erhalten
- Sicherer Intranet-Dateibrowser und im Gerät integrierte Datensicherung
- Adaptive Adressierung und adaptives Routing zur Bereitstellung der jeweils angemessensten Zugriffsmethoden und Sicherheitsstufen
- Einfache Bereitstellung dank Installationsassistenten
- Effiziente objektbasierte Richtlinienverwaltung für alle Benutzer, Gruppen, Ressourcen und Geräte
- Web Application Firewall für zuverlässige PCI-Compliance

Schneller und einfacher richtlinien-gesteuerter Zugriff auf unternehmens-kritische Anwen-dungen, Daten und Ressourcen ohne Gefährdung der Sicherheit von Unternehmensdaten

Funktionen und Merkmale

Zentrales Zugriffs-Gateway für alle Netzwerkressourcen, mit Zugriff über mobile Anwendungen, Web-Clients oder clientlos: Die SRA Appliances senken Ihre IT-Kosten, da sie es Ihren Netzwerkadministratoren ermöglichen, einfach und sicher ein zentrales Zugriffs-Gateway bereitzustellen, das sowohl internen als auch externen Benutzern den Remote-Zugriff über SSL-VPN-Verbindungen auf sämtliche Netzwerkressourcen gewährt – ob webbasiert, hostbasiert (z. B. virtuelle Desktops) oder in Client/Server-Infrastrukturen. Auch Back-Connect-Anwendungen wie VoIP sind abgedeckt. Da die SRA Appliances entweder clientlosen Browserzugriff über das individuell anpassbare SRA WorkPlace Portal oder Zugriff über mobile Anwendungen sowie schlanke Web-Clients bieten, reduzieren sie Ihren Verwaltungsaufwand und die Zahl der Support-Anfragen.

Einheitliche Benutzererfahrung unter allen Betriebssystemen: SRA Technologie ermöglicht den transparenten Zugriff auf Netzwerkressourcen von jeder Netzwerkumgebung und jedem Gerät aus. Die SRA Appliances stellen ein zentrales Gateway für sämtliche Zugriffe von verwalteten und nicht verwalteten Smartphones, Tablet-PCs, Notebooks und Desktop-PCs bereit, mit einer einheitlichen Benutzererfahrung auf allen Plattformen – darunter Windows, Mac OS X, iOS, Android, Kindle und Linux.

Mobile Connect App: Die Mobile Connect App für mobile Geräte mit einem iOS, Mac OS X, Android, Kindle oder Windows 8.1 Betriebssystem ermöglicht Benutzern einfachen Zugriff auf Netzwerkebene auf die Ressourcen ihres Unternehmens oder ihrer Hochschule über verschlüsselte SSL-VPN-Verbindungen. Sie können die Mobile Connect App ganz einfach über den Apple App Store, Google Play oder den Kindle Store herunterladen. Bei Windows 8.1 Geräten ist sie bereits integriert.

Kontextsensitivität: Der Zugriff auf das Unternehmensnetzwerk wird erst dann gewährt, wenn der Benutzer authentifiziert und die Integrität des mobilen Geräts geprüft wurde.

Sicherung von auf mobilen Geräten gespeicherten Daten: Authentifizierte Benutzer können sicher auf autorisierte freigegebene Dateien im Intranet oder über die Mobile Connect App auf Dateien zugreifen. Administratoren können Richtlinien für die Verwaltung von mobilen Anwendungen erstellen und deren Umsetzung erzwingen.

Adaptive Adressierung und adaptives Routing: Durch adaptive Adressierung und dynamisches Routing passt die App sich an Netzwerke an und eliminiert so die bei anderen Lösungen häufig auftretenden Routing-Konflikte.

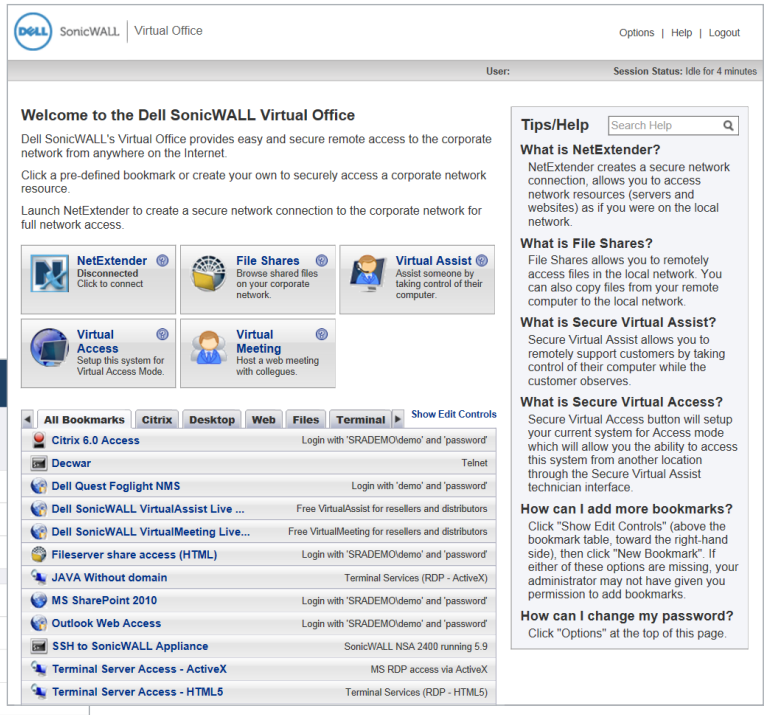
Installationsassistent: Alle SRA Appliances lassen sich einfach und in wenigen Minuten installieren und bereitstellen. Der Installationsassistent sorgt für eine einfache, intuitive Benutzererfahrung, sodass die Appliance schnell installiert, bereitgestellt und sofort einsatzbereit ist.

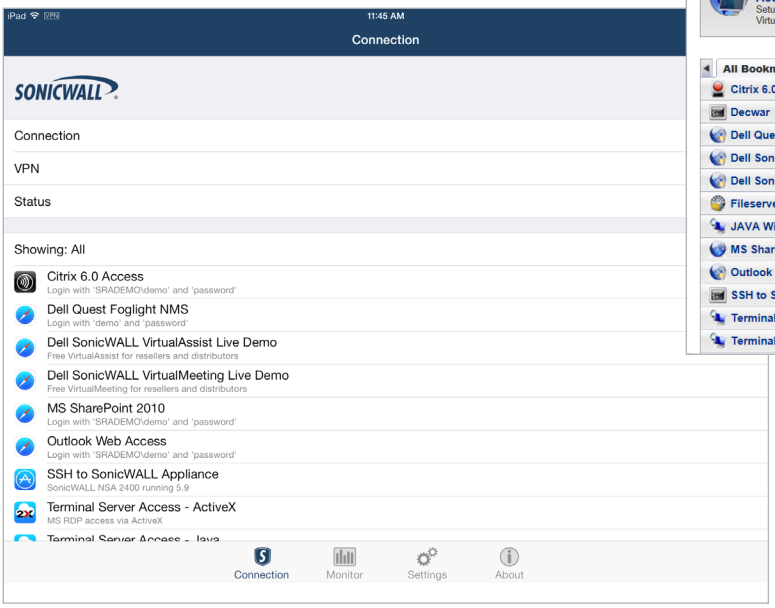
Einheitliche Richtlinien: SRA Unified Policy ermöglicht die einfache, objektbasierte Richtlinienverwaltung für alle Benutzer, Gruppen, Ressourcen und Geräte und gewährleistet gleichzeitig granulare Kontrolle basierend auf Benutzerauthentifizierung und Endpunktkontrolle.

Dell SonicWALL SRA Appliances für zeit- und ortsunabhängigen Zugriff

Einfacher und sicherer mobiler Zugriff auf Ressourcen

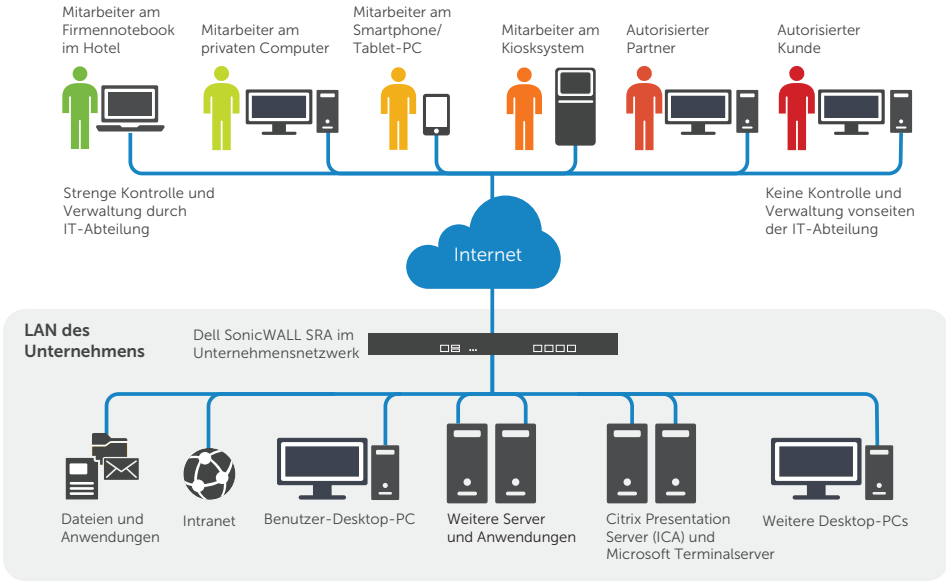
Mit den SRA Appliances ermöglichen Sie Benutzern von Windows, Mac OS X, iOS, Linux, Android und Kindle Geräten Zugriff auf eine Vielzahl an Ressourcen.

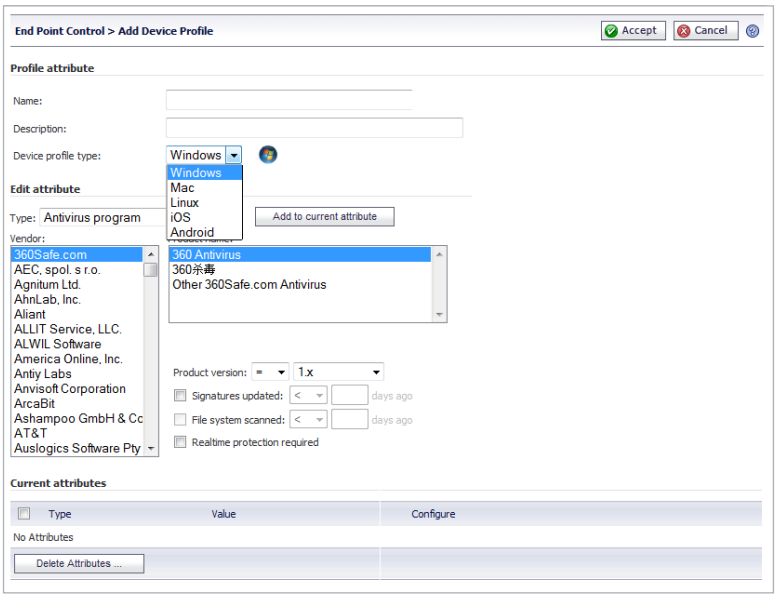




Präzise kontrollierter Zugriff für autorisierte Benutzer

Die SRA Appliances ermöglichen die präzise und richtliniengesteuerte Zugriffskontrolle, sodass Sie nicht nur Ihren Mitarbeitern vor Ort, die mit verwalteten Geräten arbeiten, sicheren mobilen und Remote-Zugriff bieten können, sondern auch mobilen und Remote-Mitarbeitern, Partnern und Kunden mit nicht verwalteten Geräten.





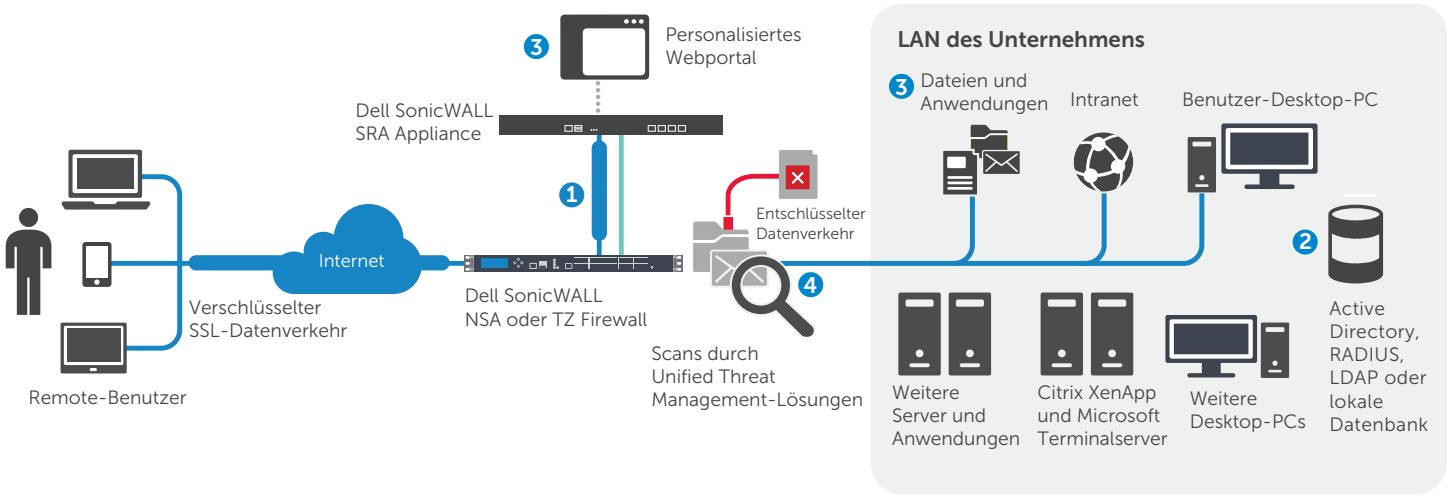
Benutzerfreundliche, kosteneffiziente Lösungen für sicheren mobilen Zugriff, die den Anforderungen Ihrer zunehmend mobilen Mitarbeiter gerecht werden

Kontextbezogene Authentifizierung
Erstklassige Funktionen für kontextbezogene Authentifizierung sorgen dafür, dass nur vertrauenswürdigen Geräten und autorisierten Benutzern Zugriff gewährt wird. Darüber hinaus ermöglichen die Appliances die Abfrage mobiler Geräte auf wichtige Sicherheitsinformationen wie Jailbreak- oder Root-Status, Geräte-ID, Zertifikatstatus und Betriebssystemversion, bevor sie den Zugriff gewähren. Bei Notebooks und PCs können Sie zusätzlich feststellen, ob sie über Sicherheitssoftware, Client-Zertifikate und eine Geräte-ID verfügen oder nicht. Geräten, die die Richtlinienanforderungen nicht erfüllen, wird kein Zugriff auf das Netzwerk gewährt und der Benutzer wird über den Richtlinienverstoß in Kenntnis gesetzt.

Sicherung von auf mobilen Geräten gespeicherten Daten
Authentifizierte Benutzer von Mobile Connect können sicher auf autorisierte freigegebene Dateien im Intranet oder über die Mobile Connect App auf Dateien zugreifen. Administratoren können Richtlinien für die Verwaltung mobiler Anwendungen festlegen und durchsetzen, anhand derer die Mobile Connect App kontrollieren kann, ob angezeigte Dateien in anderen Anwendungen (iOS 7 oder höher) geöffnet, in die Zwischenablage kopiert, gedruckt oder sicher innerhalb der Mobile Connect Anwendung zwischengespeichert werden können. Bei iOS 7 und höher können Administratoren die auf dem Gerät gespeicherten Daten in geschäftliche und persönliche Daten unterteilen und so das Risiko von Datenverlusten reduzieren. Zudem werden Inhalte, die in der Mobile Connect App gespeichert sind, bei Aufhebung der Zugriffsrechte des Benutzers gesperrt und können nicht mehr aufgerufen und angezeigt werden.

Clean VPN
Wenn Mobile Connect mit einer Dell SonicWALL Firewall der nächsten Generation bereitgestellt wird, profitieren Sie von einer zusätzlichen Sicherheitsebene: Ein Clean VPN, in dem der gesamte mobile SSL-VPN-Datenverkehr entschlüsselt und auf Malware überprüft wird, bevor die Daten in das Netzwerk gelangen.

Web Application Firewall und zuverlässige PCI-Compliance
Der Dell SonicWALL Web Application Firewall Service bietet Unternehmen eine umfassende, erschwingliche und optimal integrierte Compliance-Lösung für webbasierte Anwendungen, die einfach zu verwalten und bereitzustellen ist. Sie unterstützt die OWASP Top Ten, gewährleistet Compliance mit dem PCI-DSS und bietet so Schutz vor Injektionsangriffen, Cross-Site Scripting (XSS), Diebstahl von Sozialversicherungsnummern und Kreditkarteninformationen, manipulierten Cookies und Cross-Site Request Forgery (CSRF). Zusätzlich schützen dynamische Signatur-Updates und benutzerdefinierte Regeln vor bekannten und neuen Sicherheitsrisiken. Die Web Application Firewall kann raffinierte webbasierte Angriffe entdecken, Webanwendungen wie SSL-VPN-Portale schützen, den Zugriff verweigern, wenn sie Malware in Webanwendungen findet, und Benutzer auf eine Fehlerseite mit erklärender Benachrichtigung weiterleiten. Sie ist einfach bereitzustellen und bietet erweiterte Optionen für die Statistik- und Berichterstellung, sodass Sie Compliance-Vorgaben zuverlässig einhalten können.



1 Die Dell SonicWALL NSA oder TZ Firewall leitet eingehende Daten nahtlos an die Dell SonicWALL SRA Appliance weiter und diese entschlüsselt und authentifiziert dann den Netzwerkdatenverkehr.

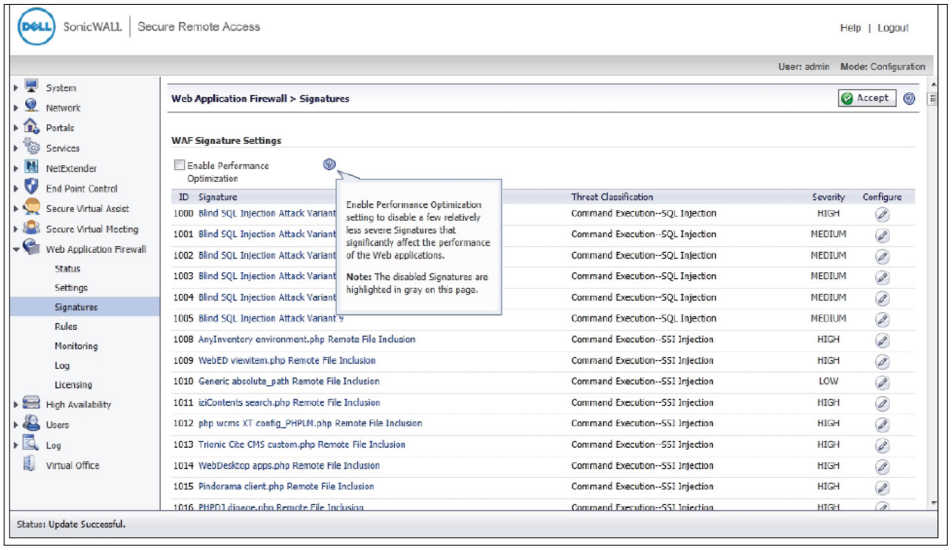
2 Benutzer werden entweder mithilfe der integrierten Datenbank authentifiziert oder anhand von Authentifizierungssystemen von Drittanbietern, wie LDAP, Active Directory, RADIUS, Dell Defender und weitere zweistufige Authentifizierungslösungen.

3 Ein personalisiertes Webportal sorgt dafür, dass Benutzer ausschließlich auf Ressourcen zugreifen können, für deren Zugriff sie Unternehmensrichtlinien zufolge autorisiert sind.

4 Um ein Clean VPN sicherzustellen, wird der Datenverkehr zunächst durch eine NSA oder TZ Firewall geschleust (Gateway-Virenschutz, Spyware-Schutz, Angriffsvermeidung, Anwendungserkennung und -kontrolle) und umfassend auf Viren, Würmer, Trojaner, Spyware und andere raffinierte Bedrohungen überprüft.

Einfache Verwaltung

Die Lösungen der SRA Serie punkten mit einheitlicher Richtlinienverwaltung und einer intuitiven webbasierten Verwaltungsschnittstelle mit kontextbezogener Hilfe für mehr Benutzerfreundlichkeit. Darüber hinaus können Sie mit dem Dell SonicWALL Global Management System (GMS 4.0+) mehrere Produkte zentral verwalten. Gleichzeitig ermöglicht das Berichterstellungstool Dell SonicWALL Analyzer, dass jeglicher Zugriff über diese Produkte auf Ressourcen ganz einfach überwacht werden kann.



Technische Daten

Dell SonicWALL SRA Serie

Leistung			
	SRA 1600	**SRA 4600**	**SRA Virtual Appliance**
	Empfohlen für Organisationen mit maximal 50 Mitarbeitern	Empfohlen für Organisationen mit maximal 250 Mitarbeitern	Empfohlen für Organisationen jeder Größe
Lizenz für gleichzeitige Benutzer	Die erste Lizenz gilt für fünf gleichzeitige Benutzer. Weitere Benutzerlizenzen sind für je fünf oder zehn Benutzer erhältlich.	Die erste Lizenz gilt für 25 Benutzer. Weitere Benutzerlizenzen sind für je zehn, 25 oder 100 Benutzer erhältlich.	Benutzerlizenzen sind für je fünf, zehn oder 25 Benutzer erhältlich.
Empfohlene Anzahl an Benutzern[1]	Lizenz für fünf Benutzer inbegriffen/ maximale Benutzeranzahl: 50/ empfohlen für 25 Benutzer	Lizenz für 25 Benutzer inbegriffen/ maximale Benutzeranzahl: 500/ empfohlen für 100 Benutzer	Lizenz für fünf Benutzer inbegriffen/ maximale Benutzeranzahl: 50
Secure Virtual Assist, Techniker	30-tägiger Testzeitraum inbegriffen/ maximal zehn Techniker gleichzeitig	30-tägiger Testzeitraum inbegriffen/ maximal 25 Techniker gleichzeitig	30-tägiger Testzeitraum inbegriffen/ maximal 25 Techniker gleichzeitig
Maximale Anzahl an Sitzungsteilnehmern	–	75	75
Einheitliche Richtlinien	Ja. Bietet zusätzliche Unterstützung für Richtlinien, die für mehrere AD Gruppen gelten		
Protokollierung	Detaillierte Protokollierung in übersichtlichem Format; Unterstützung für Syslog und E-Mail-Benachrichtigungen		
One-Arm-Modus	Ja	Ja	Ja
Dell SonicWALL Secure Virtual Assist oder Secure Virtual Access (gemeinsame Lizenz)	Remote-Zugriff auf PCs, Chat-Optionen, FTP, Aufzeichnung von Sitzungen und Diagnosetools		
Secure Virtual Meeting[2]	Für spontane sichere und kosteneffiziente Sitzungen		
IPv6-Unterstützung	Standard	Standard	Standard
Lastausgleich	Lastausgleich für HTTP/HTTPS-Anfragen mit Failover; Mechanismen umfassen gewichtete Anfragen, gewichteten Datenverkehr und geringste Anzahl an Anfragen		
Hohe Verfügbarkeit	–	Ja	Ja
Auslagerung von Anwendungen	Ja	Ja	Ja
Web Application Firewall	Ja	Ja	Ja
Endpunktkontrolle (End Point Control, EPC)	Ja	Ja	Ja
Standortbasierte Richtlinien[4]	Ja	Ja	Ja
Botnet-Filterung[4]	Ja	Ja	Ja
Wichtige Funktionen und Merkmale			
Unterstützte Anwendungen[3]	• **Webportalzugriff:** Unterstützung für HTML5, Auslagerung von Proxys und Anwendungen • **Webservices:** HTTP, HTTPS, FTP, SSH, Telnet, VNC, Windows® Dateifreigabe (Windows SMB/CIFS), OWA 2003/2007/2010 • **Virtuelle Desktop-Infrastrukturen (VDI):** Citrix (ICA), RDP • **Mobile Connect und NetExtender:** jegliche TCP/IP-basierte Anwendung: 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, weitere zweistufige Authentifizierungslösungen, Einmalkennwörter, interne Benutzerdatenbank, RADIUS, LDAP, Microsoft Active Directory und einmalige Anmeldung (Single Sign-On, SSO) für die meisten webbasierten Anwendungen, RDP und VNC[3]		
Unterstützung mehrerer Domänen	Ja		
Unterstützung mehrerer Portale	Ja		
Präzise Zugriffssteuerung	Auf Benutzer-, Benutzergruppen- oder Netzwerkressourcenebene		
Sitzungssicherheit	Timeouts bei fehlender Aktivität schützen vor unautorisiertem Zugriff auf nicht aktive Sitzungen		
Zertifikate	• **Server:** selbst signiert, mit editierbarem Common Name, von Drittanbietern importiert • **Client:** optionale Unterstützung für Client-Zertifikate		
Cache-Bereinigung	Konfigurierbar; beim Abmelden werden alle Downloads im Cache, alle Cookies und über den SSL-Tunnel heruntergeladen URLs vom Remote-PC gelöscht		
Client-Unterstützung[3]	• **Webportalzugriff**: Internet Explorer, Mozilla, Chrome, Opera, und Safari Browser • **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 X 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 oder Windows 8.1		
Personalisiertes Portal	Remote-Benutzern werden nur die Ressourcen angezeigt, auf die ihnen der Administrator den Richtlinien des Unternehmens folgend Zugriff gewährt hat.		
Verwaltung	Webbasierte grafische Benutzeroberfläche (HTTP, HTTPS), Syslog- und Heartbeat-Meldungen an GMS (4.0 und höher), Unterstützung für SNMP		
Nutzungsüberwachung	Überwachung mithilfe grafischer Darstellung der Arbeitsspeicher-, Prozessor-, Bandbreitennutzung und Benutzeraktivitäten		

[1]Empfohlene Anzahl der unterstützten Benutzer ist abhängig von Faktoren wie Zugriffsmechanismen, Anwendungen, auf die zugegriffen wird, und dem durch Anwendungen gesendeten Datenverkehr
[2]Nur in Kombination mit Secure Virtual Assist für SRA 4600 und SRA Virtual Appliances verfügbar
[3]Informationen zu unterstützten Konfigurationen finden Sie in den aktuellen SRA Versionshinweisen oder im Administratorhandbuch
[4]Botnet-Filterung und standortbasierte Richtlinien nur bei aktivem Support-Vertrag für die entsprechende Hardware oder virtuelle Appliance

Dell SonicWALL SRA Serie für KMU

Hardware		
	SRA 1600	SRA 4600
Robuste Sicherheits-Appliance	Ja	Ja
Schnittstellen	(2) Gigabit-Ethernet, (2) USB, (1) Konsole	(4) Gigabit-Ethernet, (2) USB, (1) Konsole
Prozessoren	x86-Hauptprozessor	x86-Hauptprozessor
Arbeitsspeicher (RAM)	1 GB	2 GB
Flash-Speicher	1 GB	1 GB
Netzteil	Intern, 100 bis 240 V Wechselstrom, 50 bis 60 Hz	Intern, 100 bis 240 V Wechselstrom, 50 bis 60 Hz
Max. Stromverbrauch	47 W	50 W
Gesamtwärmeabgabe	158,0 BTU	171,0 BTU
Abmessungen	43,18 x 25,73 x 4,45 cm (17 x 10,13 x 1,75 Zoll)	43,18 x 25,73 x 4,45 cm (17 x 10,13 x 1,75 Zoll)
Gewicht der Appliance	4,3 kg (9,5 lb)	4,3 kg (9,5 lb)
WEEE-Gewicht	4,5 kg (10 lb)	4,5 kg (10 lb)
Einhaltung der wichtigsten gesetzlichen Vorschriften	FCC Klasse A, ICES Klasse A, CE, C-Tick, VCCI Klasse A, KCC, ANATEL, BSMI, NOM, UL, cUL, TÜV/GS, CB	
Umgebung	0–40 °C (32–105 °F) Luftfeuchtigkeit: 5–95 % (relative Luftfeuchtigkeit), nicht kondensierend	
MTBF	18,3 Jahre	17,8 Jahre
	SRA Virtual Appliance	
SRA Virtual Appliance, Mindestanforderungen an virtualisierte Umgebung	Hypervisor: VMware ESXi und ESX (Version 4.0 und höher) Appliance-Größe (auf dem Laufwerk): 2 GB Zugewiesener Arbeitsspeicher: 2 GB	

SRA 1600, fünf Benutzer 01-SCC-6594

SRA 1600, zusätzliche Benutzer (maximal 50 Benutzer)
Zusatzlizenz für fünf gleichzeitige Benutzer 01-SSC-7138
Zusatzlizenz für zehn gleichzeitige Benutzer 01-SSC-7139

Support für die SRA 1600
Dell SonicWALL Dynamic Support
mit Rund-um-die-Uhr-Verfügbarkeit
für bis zu 25 Benutzer (ein Jahr) 01-SSC-7141

Dell SonicWALL Dynamic Support
zu Geschäftszeiten für bis
zu 25 Benutzer (ein Jahr) 01-SSC-7144

SRA 4600, 25 Benutzer 01-SSC-6596

SRA 4600, zusätzliche Benutzer (maximal 500 Benutzer)
Zusatzlizenz für zehn gleichzeitige Benutzer 01-SSC-7118
Zusatzlizenz für 25 gleichzeitige Benutzer 01-SSC-7119
Zusatzlizenz für 100 gleichzeitige Benutzer 01-SSC-7120

Support für die SRA 4600

Dell SonicWALL Dynamic Support
mit Rund-um-die-Uhr-Verfügbarkeit
für bis zu 100 Benutzer (ein Jahr) 01-SSC-7123

Dell SonicWALL Dynamic Support
zu Geschäftszeiten für bis
zu 100 Benutzer (ein Jahr) 01-SSC-7126

Dell SonicWALL Dynamic Support
mit Rund-um-die-Uhr-Verfügbarkeit
für 101 bis 500 Benutzer (ein Jahr) 01-SSC-7129

Dell SonicWALL Dynamic Support
zu Geschäftszeiten für 101 bis 500 Benutzer
(ein Jahr) 01-SSC-7132

Dell SonicWALL SRA Virtual Appliance,
fünf Benutzer 01-SSC-8469

SRA Virtual Appliance, zusätzliche Benutzer
(maximal 50 Benutzer)
Zusatzlizenz für fünf gleichzeitige Benutzer 01-SSC-9182
Zusatzlizenz für zehn gleichzeitige Benutzer 01-SSC-9183
Zusatzlizenz für 25 gleichzeitige Benutzer 01-SSC-9184

Support für die SRA Virtual Appliance
Dell SonicWALL Dynamic Support
zu Geschäftszeiten für bis zu 25 Benutzer
(ein Jahr) 01-SSC-9188

Dell SonicWALL Dynamic Support
mit Rund-um-die-Uhr-Verfügbarkeit
für bis zu 25 Benutzer (ein Jahr) 01-SSC-9191

Dell SonicWALL Dynamic Support
zu Geschäftszeiten für bis zu 50 Benutzer
(ein Jahr) 01-SSC-9194

Dell SonicWALL Dynamic Support
mit Rund-um-die-Uhr-Verfügbarkeit
für bis zu 50 Benutzer (ein Jahr) 01-SSC-9197

Weitere Informationen zu den Dell SonicWALL Secure Remote Access Lösungen finden Sie unter www.sonicwall.com.

Dell Software
www.dell.com
Informationen zu unseren Niederlassungen außerhalb Nordamerikas finden Sie auf unserer Webseite.

DataSheet-SonicWALL-SRASeries-US-VG-25825