Network Security Appliance-Serie

Next-Generation Firewalls

Unternehmen sind heute beispiellosen Sicherheitsbedrohungen ausgesetzt. Cyberangriffe nehmen nicht nur dramatisch zu, sie werden auch immer raffinierter und können jede Organisation empfindlich treffen – angefangen beim Verlust von Unternehmens-, Kunden- und persönlichen Daten oder den Diebstahl geistigen Eigentums bis hin zu Rufschädigung und Produktivitätseinbußen. Effizienter Netzwerkschutz ist eine komplexe Aufgabe. Bei der Auswahl einer passenden Lösung muss daher klar sein, welche speziellen Anforderungen erfüllt sein müssen. In vielen Firmen nutzen immer mehr Mitarbeiter ihre privaten Geräte (vor allem Smartphones und Tablets) im Unternehmensnetzwerk. Doch BYO (Bring Your Own) beeinträchtigt die Performance und die Produktivität. Hinzu kommt, dass mobile Anwendungen wie Social Media und Video-Streaming extrem viel Bandbreite verbrauchen. Für IT-Verantwortliche ergibt sich daraus ein Dilemma: Sie müssen die Sicherheit ihres Netzwerks gewährleisten und gleichzeitig eine hohe Produktivität aufrechterhalten. Nicht selten deaktivieren sie Sicherheitsfunktionen, um die Netzwerkperformance auf einem hohen Niveau zu halten – und gefährden so das Netzwerk.

Das gehört jetzt der Vergangenheit an. Mit Dell SonicWALL sorgen Sie für Sicherheit und Produktivität, ohne dabei die Performance Ihres Netzwerks zu beeinträchtigen. Die Dell™ SonicWALL™ Network Security Appliance (NSA)-Serie ist eine der sichersten und leistungsstärksten Next-Generation Firewall-Produktreihen. Sie gewährleistet kompromisslose Enterprise-Class-Sicherheit und -Leistung und basiert auf der gleichen Architektur wie die SuperMassive-Serie, das Flaggschiff unserer Next-Generation Firewalls, das ursprünglich für die anspruchsvollsten Telekommunikationsanbieter und Unternehmen weltweit entwickelt wurde. Gleichzeitig steht sie für das exzellente Preis-Leistungs-Verhältnis und die hohe Benutzerfreundlichkeit, die man von Dell erwartet. Nach jahrelanger Forschung und Entwicklung wurde die NSA-Serie von Grund auf für verteilte Unternehmen, kleine bis mittlere Firmen, Zweigniederlassungen, Schulen und Behörden konzipiert. Die NSA-Serie basiert auf einer revolutionären, ultraskalierbaren Multicore-Architektur und einer patentierten* Reassembly-Free Deep Packet Inspection® (RFDPI)-Single-Pass-Engine. Sie gewährleistet höchste Sicherheit, Leistung und Skalierbarkeit und bietet die höchste Anzahl gleichzeitiger Verbindungen, die geringsten Latenzzeiten und die meisten Verbindungen pro Sekunde ihrer Klasse – ganz ohne Einschränkungen beim Datenvolumen. Die führende Technologie der NSA-Serie wurde von renommierten Instituten in unabhängigen Produkttests geprüft bzw. vielfach ausgezeichnet.

Im Gegensatz zu den veralteten Firewall- und Intrusion-Prevention-Produkten anderer Anbieter prüft die NSA-Serie den gesamten Verkehr, unabhängig von Port oder Protokoll. Sie bietet branchenweit die höchsten On-the-fly-Entschlüsselungsgeschwindigkeiten für SSL-verschlüsselte Daten und kann so selbst die neuesten verschlüsselten Malware-Angriffe stoppen. Zudem lassen sich dank der Integration mit Authentifizierungsservern und der granularen Anwendungskontrolle Nutzungsregeln effizient durchsetzen, die Bandbreite verwalten

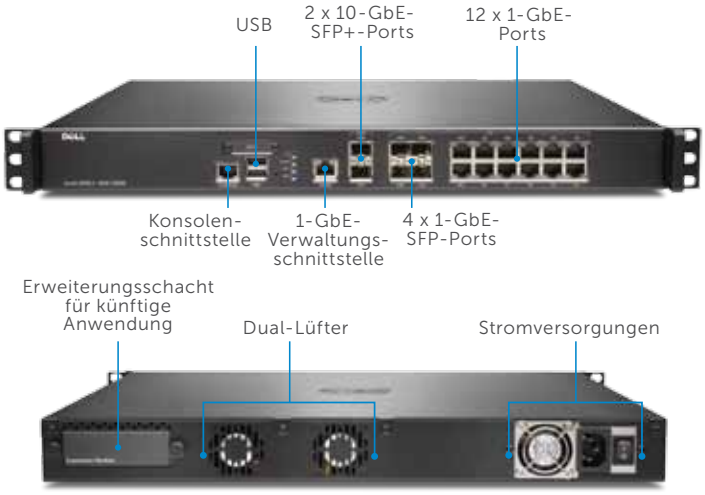
- **Best-in-Class-Sicherheit**
- **Multicore-Architektur**
- **Extrem hohe Performance**
- **Intrusion Prevention**
- **Malware-Schutz am Gateway**
- **Secure Remote Access**
- **Secure Wireless**
- **URL Filtering**
- **Spamschutz am Gateway**
- **Anwendungskontrolle**
- **Zentrale Verwaltung**

und die Produktivität erhöhen. Im Unterschied zu veralteten Mehrgeräte-Lösungen, bei denen keine Bedrohungsinformationen ausgetauscht werden, bietet die NSA-Serie sowohl Firewall- als auch IPS-Funktionen. Auf diese Weise können effektive Regeln erstellt und durchgesetzt werden, um die Sicherheit zu optimieren. Gleichzeitig lassen sich Risiken für das Unternehmen sowie der Verwaltungsaufwand reduzieren. Mit dem Dell SonicWALL Global Management System (GMS) können verteilte Unternehmen Tausende SonicWALL-Sicherheitsappliances über eine einheitliche Oberfläche verwalten und so ihren Administrationsaufwand und ihre TCO (Total Cost of Ownership) verringern. Der Benutzer erhält einen detaillierten Echtzeit-Überblick über alle Netzwerkaktivitäten und kann umfassende interne und externe Berichte erstellen.

*U.S.- Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Die Next-Generation Firewalls der Dell SonicWALL NSA-Serie nutzen Multicore-Hardware-Design und Reassembly-Free Deep Packet Inspection der neuesten Technologie, um das Netzwerk ohne Beeinträchtigung der Leistung vor internen und externen Angriffen zu schützen. Die NSA-Serie kombiniert Intrusion Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten, Application Intelligence und Anwendungskontrolle, Hochverfügbarkeitsfeatures sowie moderne Netzwerkfunktionen.

Network Security Appliance 3600

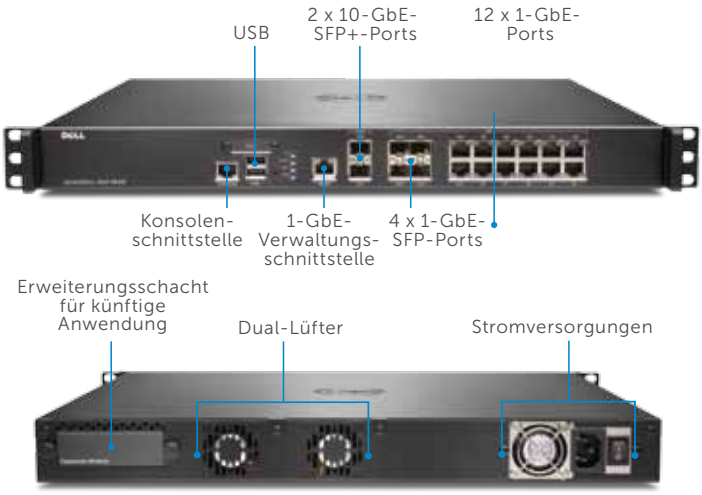


Die Dell SonicWALL NSA 3600 eignet sich ideal für Zweigniederlassungen in verteilten Netzwerkumgebungen sowie für kleine bis mittlere Unternehmen und für Einzelhandelsgeschäfte.

Firewall	NSA 3600
Firewall-Durchsatz[1]	3,4 GBit/s
IPS-Durchsatz[2]	1,1 GBit/s
Anti-Malware-Durchsatz[2]	600 MBit/s
Full DPI-Durchsatz[2]	500 MBit/s
IMIX-Durchsatz[3]	900 MBit/s
Max. Anzahl von DPI-Verbindungen	175.000
Neue Verbindungen pro Sek.	20.000/Sek.

Beschreibung	Artikelnummer
NSA 3600 (nur Firewall)	01-SSC-3850
NSA 3600 TotalSecure (1 Jahr)	01-SSC-3853
Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-4429
Gateway Anti-Malware/IPS (1 Jahr)	01-SSC-4435
Silver 24/7-Support (1 Jahr)	01-SSC-4302

Network Security Appliance 4600

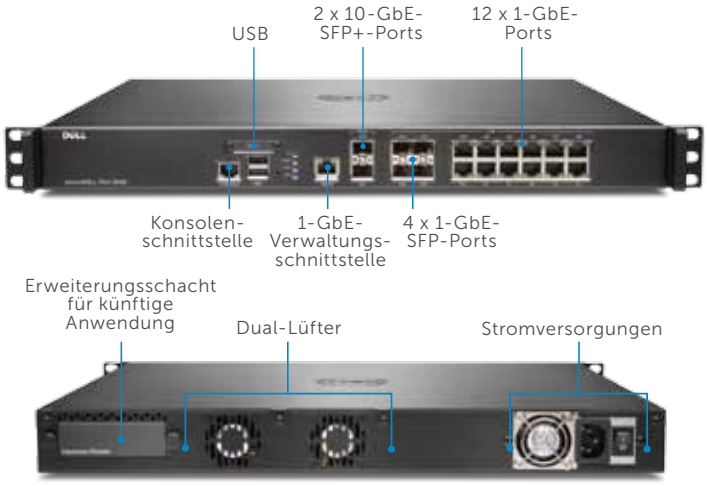


Die Dell SonicWALL NSA 4600 eignet sich ideal für Zweigniederlassungen und kleine bis mittlere Unternehmen, die ihre Durchsatzkapazität und Performance optimieren möchten.

Firewall	NSA 4600
Firewall-Durchsatz[1]	6,0 GBit/s
IPS-Durchsatz[2]	2,0 GBit/s
Anti-Malware-Durchsatz[2]	1,1 GBit/s
Full DPI-Durchsatz[2]	800 MBit/s
IMIX-Durchsatz[3]	1,6 GBit/s
Max. Anzahl von DPI-Verbindungen	250.000
Neue Verbindungen pro Sek.	40.000/Sek.

Beschreibung	Artikelnummer
NSA 4600 (nur Firewall)	01-SSC-3840
NSA 4600 TotalSecure (1 Jahr)	01-SSC-3843
Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-4405
Secure Upgrade Plus (3 Jahre)	01-SSC-4267
Silver 24/7-Support (1 Jahr)	01-SSC-4290

Network Security Appliance 5600

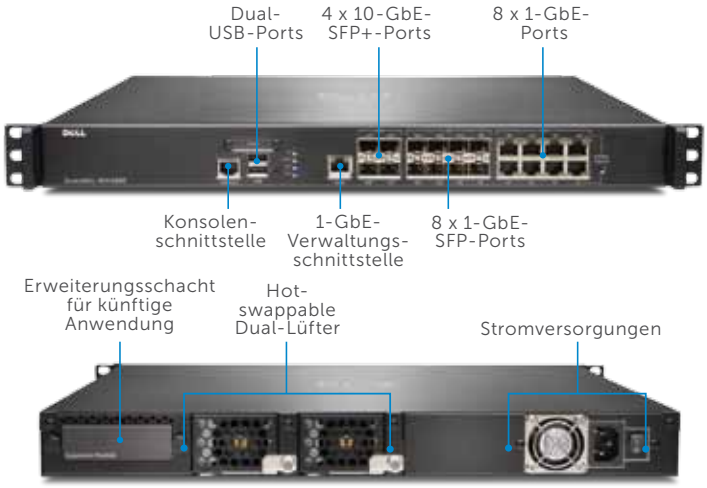


Die Dell SonicWALL NSA 5600 eignet sich ideal für verteilte Unternehmen sowie für die Zweigniederlassungen und Netzwerkumgebungen von Unternehmen, die einen erheblichen Durchsatz benötigen.

Firewall	NSA 5600
Firewall-Durchsatz[1]	9,0 GBit/s
IPS-Durchsatz[2]	3,0 GBit/s
Anti-Malware-Durchsatz[2]	1,7 GBit/s
Full DPI-Durchsatz[2]	1,6 GBit/s
IMIX-Durchsatz[3]	2,4 GBit/s
Max. Anzahl von DPI-Verbindungen	500.000
Neue Verbindungen pro Sek.	60.000/Sek.

Beschreibung	Artikelnummer
NSA 5600 (nur Firewall)	01-SSC-3830
NSA 5600 TotalSecure (1 Jahr)	01-SSC-3833
Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-4234
Gateway Anti-Malware/IPS (1 Jahr)	01-SSC-4240
Gold 24/7-Support (1 Jahr)	01-SSC-4284

Network Security Appliance 6600



Die Dell SonicWALL NSA 6600 eignet sich ideal für größere verteilte Netzwerkumgebungen sowie für Unternehmenszentralen, die eine hohe Durchsatzkapazität und Performance benötigen.

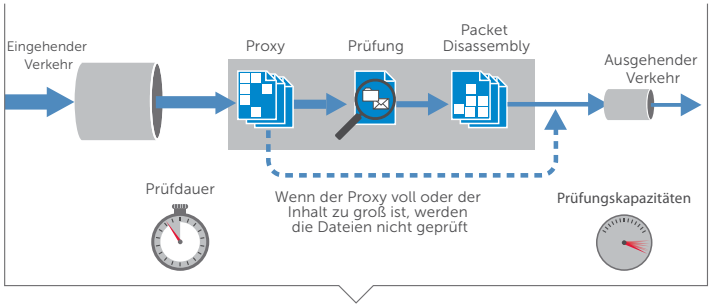
Firewall	NSA 6600
Firewall-Durchsatz[1]	12,0 GBit/s
IPS-Durchsatz[2]	4,5 GBit/s
Anti-Malware-Durchsatz[2]	3,0 GBit/s
Full DPI-Durchsatz[2]	3,0 GBit/s
IMIX-Durchsatz[3]	3,5 GBit/s
Max. Anzahl von DPI-Verbindungen	600.000
Neue Verbindungen pro Sek.	90.000/Sek.

Beschreibung	Artikelnummer
NSA 6600 (nur Firewall)	01-SSC-3820
NSA 6600 TotalSecure (1 Jahr)	01-SSC-3823
Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-4210
Gateway Anti-Malware/IPS (1 Jahr)	01-SSC-4216
Gold 24/7-Support (1 Jahr)	01-SSC-4278

Reassembly-Free Deep Packet Inspection-Engine

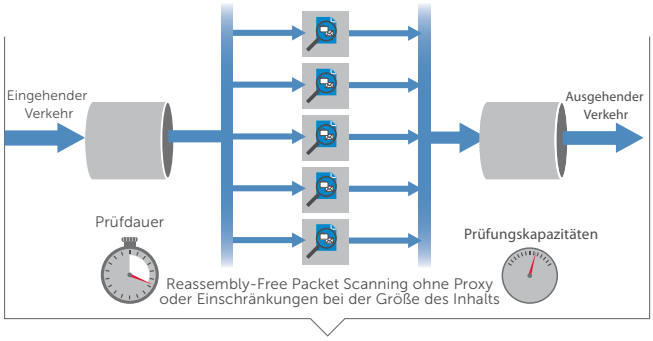
Die Dell SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI)-Engine bietet einen optimalen Schutz vor Bedrohungen und umfassende Anwendungskontrolle, ohne die Leistung zu beeinträchtigen. Dabei prüft die patentierte Engine die Payload von Datenströmen, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren. Durch die RFDPI-Engine wird der Netzwerkverkehr mehrfach umfassend normalisiert und entschlüsselt. Auf diese Weise lassen sich raffinierte Umgehungsversuche verhindern, die darauf abzielen, Erkennungsmechanismen zu stören und bösartigen Code in das Netzwerk einzuschleusen. Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall aktualisiert und mit diesen Datenbanken abgeglichen. Dabei wird geprüft, ob ein Angriff oder ein anderes sicherheitsrelevantes Ereignis eintritt. Ist dies der Fall, wird eine vordefinierte Aktion ausgeführt. In den meisten Fällen wird die Verbindung beendet. Anschließend werden entsprechende Logging- und Benachrichtigungs-Events erzeugt. Die Engine kann jedoch auch nur für Prüfungen konfiguriert werden oder – wenn die Anwendungserkennung aktiv ist – so, dass für den restlichen Anwendungsverkehr Layer-7-Bandbreitenverwaltungsdienste bereitgestellt werden, sobald die Anwendung erkannt wird.

Verfahren mit Packet Assembly



Architektur anderer Anbieter

Verfahren ohne Packet Assembly

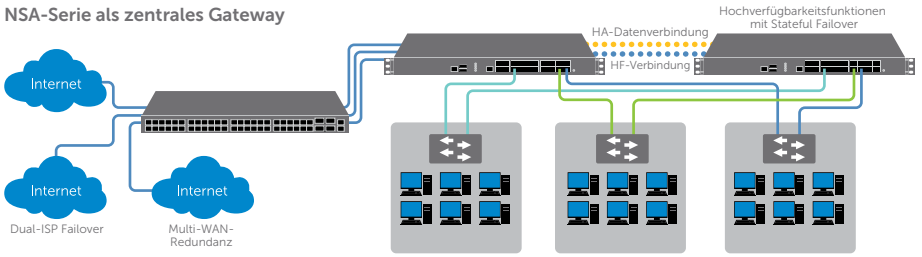


Dell SonicWALL-Architektur

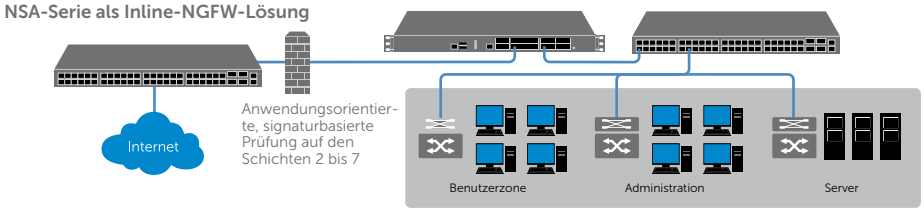
Flexible, individuell anpassbare Implementierungsoptionen – die NSA-Serie im Überblick

Alle SonicWALL Network Security Appliance-Lösungen bieten Next-Generation Firewall-Schutz. Dank ihrer bahnbrechenden Multicore-Architektur und Reassembly-Free Deep Packet Inspection-Technologie bietet die NSA-Serie internen und externen Netzwerkschutz, ohne die Performance zu beeinträchtigen. Jede Appliance der NSA-Serie verfügt über High-Speed-Intrusion Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten, leistungsstarke Application Intelligence und Anwendungskontrolle sowie zahlreiche erweiterte flexible Netzwerk- und Konfigurationsfeatures. Die NSA-Serie bietet eine erschwingliche Plattform, die sich in den unterschiedlichsten Netzwerkumgebungen von Unternehmen, Zweigniederlassungen und verteilten Organisationen leicht implementieren und verwalten lässt.

NSA-Serie als zentrales Gateway



NSA-Serie als Inline-NGFW-Lösung

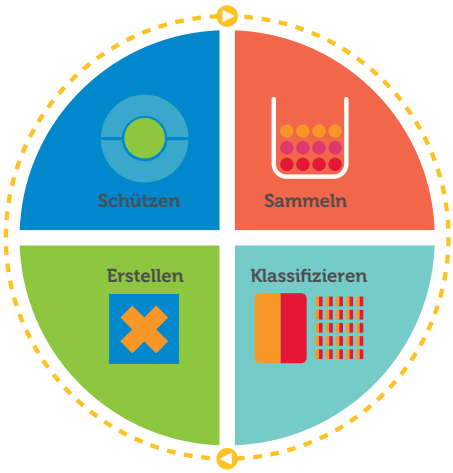


SonicWALL

Sicherheit und Schutz

Das interne Dell SonicWALL Threat Research Team ist für die Erforschung und Entwicklung von Abwehrmechanismen zuständig. Diese werden in die Firewalls implementiert, um aktuellen Schutz zu gewährleisten. Das Team nutzt weltweit über eine Million Sensoren, die Malware-Muster sammeln und Daten zu den neuesten Bedrohungen liefern. Diese Informationen werden anschließend für wichtige Funktion wie Intrusion Prevention, Anti-Malware und Anwendungserkennung eingesetzt. Kunden mit Next-Generation Firewalls von Dell SonicWALL, die mit den neuesten Sicherheitsfunktionen ausgestattet sind, erhalten rund um die Uhr Updates zu den aktuellsten Bedrohungen. Die Updates sind sofort wirksam, erfordern keine Neustarts und verursachen keinerlei Unterbrechungen. Die Signaturen auf den Appliances bieten Schutz vor einer großen Vielfalt an Bedrohungen. Eine einzige Signatur deckt dabei bis zu Zehntausende verschiedene Bedrohungen ab.

Zusätzlich zu den Abwehrmechanismen auf der Appliance bieten die NSA-Produkte auch Zugang zum Dell SonicWALL CloudAV Service. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um über 12 Millionen Signaturen erweitert. Die Firewall greift über ein proprietäres schlankes Protokoll auf die CloudAV-Datenbank zu, um die Prüfmöglichkeiten auf der Appliance zu erweitern. Dank effizienter Geo-IP- und Botnet-Filter-Funktionen sind die Next-Generation Firewalls von Dell SonicWALL in der Lage, den Verkehr aus gefährlichen Domänen oder ganzen Regionen zu blockieren, um die Sicherheitsrisiken im Netzwerk zu reduzieren.



Application Intelligence and Control

Application Intelligence liefert detaillierte Informationen zum Anwendungsverkehr im Netzwerk. Administratoren haben so die Möglichkeit, die Anwendungskontrolle entsprechend den geschäftlichen Prioritäten zu steuern und zu planen, unproduktive Anwendungen einzuschränken und potenziell gefährliche Anwendungen zu blockieren. Auffälligkeiten werden mittels Echtzeit-Visualisierung augenblicklich identifiziert. So können unverzüglich Gegenmaßnahmen eingeleitet werden, um das Netzwerk vor ein- oder ausgehenden Angriffen zu schützen oder Performance-Engpässe zu verhindern.

Dell SonicWALL Application Traffic Analytics liefert detaillierte Informationen zum Anwendungsverkehr, zur Bandbreitennutzung sowie zu Sicherheitsbedrohungen und bietet leistungsstarke Troubleshooting- und Forensik-Funktionen. Sichere Single Sign-on (SSO)-Funktionen sorgen für mehr

Benutzerfreundlichkeit, erhöhen die Produktivität und reduzieren die Support-Anfragen.

Das Dell SonicWALL Global Management System (GMS®) vereinfacht mit seiner intuitiven webbasierten Oberfläche die Verwaltung der Anwendungserkennungs- und -kontrollfunktionen.

Funktionen

RFDPI-Engine	
Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection (RFDPI)	Diese hochleistungsfähige, proprietäre und patentierte Engine führt eine streambasierte bidirektionale Verkehrsanalyse durch, um Eindringversuche und Malware zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy.
Bidirektionale Prüfung	Der ein- und ausgehende Datenverkehr wird auf Bedrohungen geprüft, um zu verhindern, dass das Netzwerk zum Verbreiten von Malware oder als Ausgangsplattform für Angriffe genutzt wird, falls ein infizierter Computer in das Netzwerk gelangt.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxies stattfindet, lassen sich Millionen gleichzeitiger Datenströme mit der DPI-Technologie bei minimalen Latenzzeiten scannen, ohne dabei das Datenvolumen oder die Dateigrößen einzuschränken. Dies funktioniert sowohl bei gängigen Protokollen als auch bei Raw-TCP-Streams.
Hohe Parallelität und Skalierbarkeit	Gemeinsam mit der Multicore-Architektur ermöglicht das einzigartige Design der RFDPI-Engine einen hohen DPI-Durchsatz sowie extrem hohe Geschwindigkeiten beim Aufbau neuer Sitzungen. Verkehrsspitzen in anspruchsvollen Netzwerken lassen sich so besser bewältigen.
Single-Pass-Inspection	Eine Single-Pass-DPI-Architektur prüft den Verkehr auf Malware und Eindringversuche und sorgt gleichzeitig für die Erkennung von Anwendungen. Dadurch werden DPI-bedingte Latenzzeiten drastisch verkürzt. Außerdem wird sichergestellt, dass sämtliche Informationen zu Bedrohungen innerhalb einer einheitlichen Architektur verarbeitet werden.

Intrusion Prevention	
Funktion	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes Intrusion Prevention System (IPS) nutzt Signaturen und andere Abwehrmechanismen, um Paket-Payloads auf Schwachstellen und Exploits zu prüfen, und deckt dabei eine Vielzahl an Angriffen und Schwachstellen ab.
Automatische Signaturen-Updates	Das Dell SonicWALL Threat Research Team analysiert kontinuierlich Bedrohungen und sorgt für die ständige Aktualisierung einer umfassenden Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Die neuen Updates sind sofort wirksam und erfordern keine Neustarts oder sonstigen Betriebsunterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Verbesserter Schutz vor internen Bedrohungen durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Intrusion Prevention. Dies verhindert, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten.
Erkennen und Blockieren von Command-and-Control (CnC)-Aktivitäten durch Botnets	Erkennen und Blockieren von Command-and-Control-Verkehr, der von Bots im lokalen Netzwerk ausgeht und an IPs und Domänen geleitet wird, die nachweislich Malware verbreiten oder bekannte CnC-Punkte sind.
Erkennen und Verhindern von Protokollmissbrauch/-anomalien	Erkennen und Verhindern von Angriffen, die Protokolle missbrauchen, um unbemerkt am IPS vorbeizukommen.
Zero-Day-Schutz	Ständige Updates zu den neuesten Exploit-Techniken und -Methoden decken Tausende verschiedener Exploits ab und schützen das Netzwerk vor Zero-Day-Angriffen.
Umgehungsschutz	Umfassende Normalisierungs- und Entschlüsselungsmethoden sowie weitere Maßnahmen verhindern, dass Bedrohungen Umgehungstechniken auf den Ebenen 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.

Funktionen

Threat Prevention	
Funktion	Beschreibung
Malware-Schutz am Gateway	Die RFDPI-Engine prüft den gesamten Verkehr auf Viren, Trojaner, Keylogger und andere Malware in Dateien unbegrenzter Größe und über alle Ports und TCP-Streams hinweg. Die Prüfung erfolgt sowohl in ein- als auch ausgehender Richtung sowie innerhalb von Zonen.
CloudAV	Die Cloud-Server von Dell SonicWALL verfügen über eine ständig aktualisierte Datenbank mit über 12 Millionen Bedrohungssignaturen. Diese ergänzt die lokalen Signaturendatenbanken und sorgt dafür, dass die RFDPI-Technologie eine größtmögliche Anzahl an Bedrohungen abdeckt.
Sicherheitsupdates rund um die Uhr	Das Dell SonicWALL Threat Research Team analysiert neue Bedrohungen und stellt Abwehrmechanismen bereit – 24 Stunden am Tag, 7 Tage die Woche. Neue Updates zu Bedrohungen werden automatisch an Firewalls vor Ort mit aktivierten Sicherheitsservices weitergeleitet und sind sofort wirksam, ohne dass Neustarts nötig sind oder andere Unterbrechungen verursacht werden.
SSL-Prüfung	Blitzschnelle, proxylose Entschlüsselung und Prüfung von SSL-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im SSL-verschlüsselten Verkehr lauern.
Bidirektionale Raw-TCP-Prüfung	Die RFDPI-Engine ist in der Lage, Raw-TCP-Streams bidirektional auf sämtlichen Ports zu prüfen. So lassen sich Angriffe verhindern, bei denen veraltete Sicherheitssysteme umgangen werden, die sich lediglich auf ein paar bekannte Ports konzentrieren.
Unterstützung zahlreicher Protokolle	Identifizierung gängiger Protokolle wie HTTP/S, FTP, SMTP, SMBv1/v2 und andere, bei denen Daten nicht in Raw-TCP-Paketen gesendet werden. Payloads werden für die Malware-Prüfung entschlüsselt, auch wenn sie keine bekannten Standardports nutzen.

Application Intelligence and Control	
Funktion	Beschreibung
Anwendungskontrolle	Kontrolle von Anwendungen oder einzelnen Anwendungsmerkmalen, die anhand einer kontinuierlich erweiterten Datenbank mit über 4.300 Anwendungssignaturen von der RFDPI-Engine erkannt werden. Dadurch lässt sich die Netzwerksicherheit und -produktivität erhöhen.
Personalisierbare Anwendungs-identifizierung	Erstellung von Signaturen auf der Grundlage bestimmter Parameter oder Muster, die nur bei der Netzwerkkommunikation bestimmter Anwendungen vorkommen. So lassen sich benutzerdefinierte Anwendungen kontrollieren und eine erweiterte Kontrolle über das Netzwerk erreichen.
Bandbreitenverwaltung auf Anwendungsebene	Einschränkung oder Priorisierung von Anwendungen oder Anwendungskategorien, um die verfügbare Bandbreite für kritische Anwendungen zu maximieren und unerwünschten Anwendungsverkehr einzuschränken oder ganz zu blockieren.
Visualisierung von internem und externem Verkehr	Erkennung der Bandbreitennutzung und Analyse des Netzwerkverhaltens mit Echtzeit-Visualisierung des internen Anwendungsverkehrs und Berichten zum externen Anwendungsverkehr via NetFlow/IPFix.
Granulare Kontrolle	Kontrolle von Anwendungen oder bestimmten Anwendungskomponenten auf der Grundlage von Zeitplänen, Benutzergruppen, Ausschlusslisten und einer Reihe von Aktivitäten mit voller SSO-Benutzeridentifizierung durch LDAP-/AD-/Terminal Services-/Citrix-Integration.

Funktionen

Firewall und Networking

Funktion	Beschreibung
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass alle Firewall-Zugriffsregeln erfüllt werden.
Schutz vor DDoS-/DoS-Angriffen	Dank SYN-Flood-Schutz lassen sich DoS-Angriffe mit Layer-3-SYN-Proxy- und Layer-2-SYN-Blacklisting-Technologien abwehren. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsgeschwindigkeit vor DoS-/DDoS-Angriffen schützen.
Flexible Implementierung	Die NSA-Serie lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
Hochverfügbarkeit/ Clustering	Die NSA-Serie unterstützt die Hochverfügbarkeitsmodi Active/Passive mit State-Synchronisierung, Active/Active DPI und Active/Active Clustering. Beim Active/Active DPI-Modus wird die Deep Packet Inspection-Last an die Kerne der passiven Appliance weitergegeben, um den Durchsatz zu erhöhen.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden.
Regelbasiertes Routing	Erstellen von protokollbasierten Routen für die Umleitung des Datenverkehrs zu einer bevorzugten WAN-Verbindung mit Failback-Möglichkeit auf ein sekundäres WAN bei einem Stromausfall.
Erweiterte QoS	Garantierte Unterstützung kritischer Datenübertragung dank 802.1p und DSCP-Tagging sowie Remapping von VoIP-Datenverkehr im Netzwerk.
H.323-Gatekeeper- und SIP-Proxy-Support	Blockieren von Spam-Anrufen, da alle eingehenden Anrufe vom H.323-Gatekeeper oder SIP-Proxy autorisiert und authentifiziert werden müssen.

Management und Reporting

Funktion	Beschreibung
Global Management System	Dell SonicWALL GMS ermöglicht es, über eine einzige Verwaltungsschnittstelle mit intuitiver Oberfläche mehrere Dell SonicWALL-Appliances zu überwachen und zu konfigurieren und Berichte dazu zu erstellen. Dies reduziert nicht nur die Kosten, sondern auch die Komplexität bei der Verwaltung.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche erlaubt eine schnelle und bequeme Konfiguration, eine umfassende CLI und Support für SNMPv2/3.
Berichte zum IPFIX-/ NetFlow-Datenstrom	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Unterstützt wird auch die Berichterstellung mit Tools wie Dell SonicWALL Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben.

Virtual Private Networking

Funktion	Beschreibung
IPSec VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPSec VPN kann die NSA-Serie als VPN-Konzentrator für Tausende großer Standorte, Zweigniederlassungen oder Home Offices eingesetzt werden.
SSL VPN- oder IPSec Client-Remote Access	Durch Einsatz der clientlosen SSL-VPN-Technologie oder eines leicht zu verwaltenden IPSec-Clients ist der unkomplizierte Zugriff auf E-Mail, Dateien, Rechner, Intranet-Sites und Anwendungen von zahlreichen unterschiedlichen Plattformen möglich.
Redundantes VPN-Gateway	Bei mehreren WANs lässt sich ein primäres und sekundäres VPN konfigurieren, um ein einfaches automatisches Failover und Failback für alle VPN-Sitzungen zu ermöglichen.
Routenbasiertes VPN	Die Möglichkeit, ein dynamisches Routing über VPN-Links durchzuführen, sorgt für Ausfallsicherheit durch Umleitung des Datenverkehrs über alternative Verbindungen zwischen Endgeräten, falls ein temporärer VPN-Tunnel ausfällt.

Funktionen

Content- bzw. kontextorientierte Sicherheitsfunktionen

Funktion	Beschreibung
Nachverfolgung der Benutzeraktivitäten	Stellt Informationen zur Benutzerkennung und -aktivität bereit, die auf der nahtlosen SSO-Integration für AD/LDAP/Citrix/Terminal Services sowie umfassenden DPI-Daten basieren.
GeoIP: Identifizierung des Datenverkehrs nach Ländern	Identifizierung und Kontrolle des Netzwerkverkehrs aus oder in bestimmte Länder. Schützt das Netzwerk vor Angriffen bzw. Sicherheitsbedrohungen bekannten oder verdächtigen Ursprungs. Zudem kann verdächtiger Verkehr, der vom Netzwerk ausgeht, analysiert werden.
DPI-Filterung nach regulären Ausdrücken	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern.

Die SonicOS-Funktionen im Überblick

Firewall
- Reassembly-Free Deep Packet Inspection
- Deep Packet Inspection für SSL-Verkehr
- Stateful Packet Inspection
- TCP-Reassemblierung
- Stealth-Modus
- Common Access Card (CAC)-Unterstützung
- Schutz vor DoS-Angriffen
- UDP-/ICMP-/SYN-Flood-Schutz

Intrusion Prevention
- Signaturbasierte Prüfung
- Automatische Signaturenupdates
- Schutz vor ausgehenden Bedrohungen
- IPS-Ausschlussliste
- Auf GeoIP und Reputation basierende Filterfunktionen
- Abgleich regulärer Ausdrücke

Anti-Malware
- Streambasierte Malware-Prüfung
- Gateway Anti-Virus
- Gateway Anti-Spyware
- SSL-Entschlüsselung
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- CloudAV-Datenbank zu Bedrohungen

Anwendungskontrolle
- Anwendungskontrolle
- Blockieren von Anwendungskomponenten
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Visualisierung des Anwendungsverkehrs
- Schutz vor Datenlecks
- Berichte zu Anwendungen über NetFlow/IPFIX
- Nachverfolgung der Benutzeraktivitäten (SSO)
- Umfassende Anwendungssignaturendatenbank

Web Content Filtering
- URL Filtering
- Anti-Proxy-Technologie
- Blockieren mithilfe von Schlüsselwörtern
- Bandbreitenverwaltung mit CFS-Ratingkategorien
- Unified Policy-Konzept mit Anwendungskontrolle
- 56 Content Filtering-Kategorien

VPN
- IPSec VPN für Site-to-Site-Konnektivität
- SSL VPN- oder IPSec Client-Remote Access
- Redundantes VPN-Gateway
- Mobile Connect für Apple® iOS und Google® Android™
- Routenbasiertes VPN (OSPF, RIP)

Networking
- Dynamic Routing
- SonicPoint Wireless Controller*
- Regelbasiertes Routing
- Erweiterte NAT
- DHCP-Server
- Bandbreitenmanagement
- Link Aggregation
- Port-Redundanz
- Hochverfügbarkeitsmodus A/P mit State Sync
- A/A Clustering
- Lastverteilung beim ein-/ausgehenden Verkehr
- L2-Bridge-, Wire-, Tap-, NAT-Modus

VoIP
- Erweiterte QoS
- Bandbreitenmanagement
- DPI für VoIP-Daten
- H.323-Gatekeeper- und SIP-Proxy-Support

Verwaltung und Überwachung
- Web-Oberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Externes Reporting (Scrutinizer)
- Zentralisierte Management- und Reporting-Funktionen
- Logging
- Netflow-/IPFIX-Export
- Visualisierung des Anwendungsverkehrs
- LCD-Bildschirm
- Zentralisierte Regelverwaltung
- Single Sign-On (SSO)
- Terminal Service-/Citrix-Unterstützung
- Integrierte Forensik-Funktionen von Solera Networks

NSA-Serie – Systemdaten

	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Betriebssystem	SonicOS 6.1			
Sicherheits-Cores	6	8	10	24
10-GbE-Schnittstellen	2 x 10-GbE-SFP+			4 x 10-GbE-SFP+
1-GbE-Schnittstellen	4 x 1-GbE-SFP, 12 x 1-GbE			8 x 1-GbE-SFP, 8 x 1-GbE (1 LAN-Bypass-Paar)
Verwaltungsschnittstellen	1 GbE, 1 Konsole			
Speicher (RAM)	2,0 GB	2,0 GB	4,0 GB	4,0 GB
Erweiterung	1 Erweiterungssteckplatz (Rückseite)*, SD-Karte*			
Firewall Inspection-Durchsatz[1]	3,4 GBit/s	6,0 GBit/s	9,0 GBit/s	12,0 GBit/s
Full DPI-Durchsatz[2]	500 MBit/s	800 MBit/s	1,6 GBit/s	3,0 GBit/s
Application Inspection-Durchsatz[2]	1,1 GBit/s	2,0 GBit/s	3,0 GBit/s	4,5 GBit/s
IPS-Durchsatz[2]	1,1 GBit/s	2,0 GBit/s	3,0 GBit/s	4,5 GBit/s
Anti-Malware Inspection-Durchsatz[2]	600 MBit/s	1,1 GBit/s	1,7 GBit/s	3,0 GBit/s
IMIX-Durchsatz[3]	900 MBit/s	1,6 GBit/s	2,4 GBit/s	3,5 GBit/s
SSL-Prüfung und -Entschlüsselung (DPI SSL)[2]	300 MBit/s	500 MBit/s	800 MBit/s	1,3 GBit/s
VPN-Durchsatz[3]	1,5 GBit/s	3,0 GBit/s	4,5 GBit/s	5,0 GBit/s
Verbindungen pro Sekunde	20.000/Sek.	40.000/Sek.	60,000/Sek.	90.000/Sek.
Max. Anzahl von Verbindungen (SPI)	325.000	500.000	750.000	1.000.000
Max. Anzahl von Verbindungen (DPI)	175.000	250.000	500.000	600.000
Unterstützte SonicPoints (max.)	48	64	96	96
VPN				
Site-to-Site-Tunnel	800	1.500	4.000	6.000
IPSec VPN-Clients (max.)	50 (1.000)	500 (3.000)	2.000 (4.000)	2.000 (6.000)
SSL VPN-Lizenzen (max.)	2 (30)	2 (30)	2 (50)	2 (50)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256-Bit)/MD5, SHA-1			
Schlüsselaustausch	Diffie Hellman-Gruppen 1, 2, 5, 14			
Routenbasiertes VPN	RIP, OSPF			
Networking				
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay			
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT, transparenter Modus			
VLAN-Schnittstellen	512			
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast			
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p			
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminal Services, Citrix			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Zertifikate	VPNC, ICSA Firewall, ICSA Anti-Virus			
Zertifikate (ausstehend)	FIPS 140-2, Common Criteria EAL1+			
Common Access Card (CAC)	ausstehend			
Hardware				
Stromversorgung	einfach, fest 250 W			
Lüfter	dual, fest			dual, redundant, hot-swappable
Eingangsspannung	100-240 VAC, 60-50 Hz			
Maximale Leistungsaufnahme (W)	74,3	86,7	90,9	113,1
Gehäuse	rackfähig (1 HE)			
Abmessungen	43,3 x 48,5 x 4,5 cm			
Gewicht	6,15 kg			6,77 kg
WEEE-Gewicht	6,46 kg			8,97 kg
Versandgewicht	9,43 kg			11,85 kg
Erfüllt folgende Standards/Normen	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE, ANATEL, BSMI			
Umgebungstemperatur	0-40 °C			
Luftfeuchtigkeit	10-90 %, nicht kondensierend			

[1] Testmethoden: Maximalleistung auf Basis von RFC 2544 (für Firewall). Die tatsächliche Leistung kann je nach Netzwerkbedingungen bzw. aktivierten Diensten variieren.
[2] Messung des Full DPI/GatewayAV-/Anti-Spyware-/IPS-Durchsatzes mittels Industriestandard-HTTP Performance-Test WebAvalanche von Spirent und Ixia Test-Tools. Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. [3] VPN-Durchsatzmessung mittels UDP-Verkehr mit 1280 Bytes pro Paket gemäß RFC 2544. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten. *Für künftige Anwendungen.

Bestellinformationen zur NSA-Serie

Produkt	Artikelnummer
NSA 3600, 2 SFP+-10-GbE-Ports, 4 SFP-1-GbE-Ports, 12 Kupfer-1-GbE-Ports	01-SSC-3850
NSA 4600, 2 SFP+-10-GbE-Ports, 4 SFP-1-GbE-Ports, 12 Kupfer-1-GbE-Ports	01-SSC-3840
NSA 5600, 2 SFP+-10-GbE-Ports, 4 SFP-1-GbE-Ports, 12 Kupfer-1-GbE-Ports	01-SSC-3830
NSA 6600, 4 SFP+-10-GbE-Ports, 8 SFP-1-GbE-Ports, 8 Kupfer-1-GbE-Ports	01-SSC-3820
NSA 3600 – Support und Sicherheitsabos	**Artikelnummer**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für 3600 (1 Jahr)	01-SSC-4429
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für 3600 (1 Jahr)	01-SSC-4435
Silver 24/7-Support für NSA 3600 (1 Jahr)	01-SSC-4302
Content Filtering Premium Business Edition für 3600 (1 Jahr)	01-SSC-4441
Comprehensive Anti-Spam Service für NSA 3600 (1 Jahr)	01-SSC-4447
NSA 4600 – Support und Sicherheitsabos	**Artikelnummer**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für 4600 (1 Jahr)	01-SSC-4405
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für 4600 (1 Jahr)	01-SSC-4411
Silver 24/7-Support für NSA 4600 (1 Jahr)	01-SSC-4290
Content Filtering Premium Business Edition für 4600 (1 Jahr)	01-SSC-4417
Comprehensive Anti-Spam Service für NSA 4600 (1 Jahr)	01-SSC-4423
NSA 5600 – Support und Sicherheitsabos	**Artikelnummer**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für 5600 (1 Jahr)	01-SSC-4234
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für 5600 (1 Jahr)	01-SSC-4240
Gold 24/7-Support für NSA 5600 (1 Jahr)	01-SSC-4284
Content Filtering Premium Business Edition für 5600 (1 Jahr)	01-SSC-4246
Comprehensive Anti-Spam Service für NSA 5600 (1 Jahr)	01-SSC-4252
NSA 6600 – Support und Sicherheitsabos	**Artikelnummer**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für 6600 (1 Jahr)	01-SSC-4210
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für 6600 (1 Jahr)	01-SSC-4216
Gold 24/7-Support für NSA 6600 (1 Jahr)	01-SSC-4278
Content Filtering Premium Business Edition für 6600 (1 Jahr)	01-SSC-4222
Comprehensive Anti-Spam Service für NSA 6600 (1 Jahr)	01-SSC-4228
Module und Zubehör*	**Artikelnummer**
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twinaxial-Kabel	01-SSC-9787
10GBASE SFP+ 3M Twinaxial-Kabel	01-SSC-9788
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Kupfermodul	01-SSC-9791
Management und Reporting	**Artikelnummer**
Dell SonicWALL GMS Software-Lizenz (10 Nodes)	01-SSC-3363
Dell SonicWALL GMS E-Class 24/7-Software-Support für 10 Nodes (1 Jahr)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance mit Softwarelizenz für Flow-Analysemodul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-3443
Dell SonicWALL Scrutinizer mit Softwarelizenz für Flow-Analysemodul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-4002
Dell SonicWALL Scrutinizer mit Softwarelizenz für Advanced Reporting-Modul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-3773

*Für eine vollständige Liste der unterstützten SFP- und SFP+-Module wenden Sie sich bitte an einen Dell-SE.