SonicWall Network Security Appliance (NSA) Series

Effiziente, bewährte Sicherheit und Performance für mittelgroße Netzwerke

Die SonicWall Network Security Appliance (NSA) Series bietet mittelgroßen Netzwerken, Zweigniederlassungen und verteilten Unternehmen eine hochleistungsfähige Sicherheitsplattform für einen erweiterten Schutz vor Bedrohungen. Die NSA Series kombiniert Next-Generation-Firewall-Technologie mit unserer patentierten* Reassembly-Free Deep Packet Inspection (RFDPI)-Engine in einer Multicore-Architektur und gewährleistet Organisationen so die Sicherheit, Performance und Kontrolle, die sie benötigen.

Überragender Bedrohungsschutz und exzellente Performance

Die Next-Generation-Firewalls der NSA Series integrieren eine Reihe fortschrittlicher Sicherheitstechnologien, die für einen überragenden Bedrohungsschutz sorgen. Unsere patentierte RFDPI-Single-Pass-Engine scannt jedes einzelne Paket und jedes einzelne Byte. Dabei wird der ein- und ausgehende Datenverkehr gleichzeitig auf Bedrohungen geprüft. Neben Cloud-basierten Services wie CloudAV und der Multi-Engine-Sandbox von SonicWall Capture nutzt die NSA Series integrierte Funktionen wie Intrusion-Prevention, Anti-Malware und Web-/URL-Filtering, um Zero-Day-Bedrohungen am Gateway zu stoppen. Im Gegensatz zu anderen Sicherheitsprodukten, die nicht in der Lage sind, große Dateien auf versteckte Bedrohungen zu prüfen, analysieren die NSA-Firewalls alle Dateien unabhängig von ihrer Größe über alle Ports und Protokolle hinweg. Die Sicherheitsarchitektur der SonicWall-Next-Generation-Firewalls wurde von NSS Labs als eine der branchenweit besten im Hinblick auf die Effizienz ihrer Sicherheitsmechanismen bewertet. Dies ist nun das vierte Jahr in Folge, dass SonicWall die Bewertung „Recommend" von NSS Labs erhält.

Die Next-Generation-Firewalls von SonicWall gehen über Intrusion-Prevention, Malwareschutz und Web-Filtering hinaus und bieten eine zusätzliche Sicherheitsschicht, indem sie SSL-/TLS-verschlüsselten Webverkehr entschlüsseln und in Echtzeit auf versteckte Bedrohungen prüfen. Da der verschlüsselte Webverkehr stetig wächst, können Organisationen ein Drittel ihres Netzwerkverkehrs praktisch nicht einsehen. Deshalb darf die SSL-/TLS-Entschlüsselung und -Prüfung bei keiner Sicherheitslösung fehlen.

Sind Deep-Packet-Inspection-Funktionen wie zum Beispiel Intrusion-Prevention, Viren- und Spyware-Schutz sowie SSL-Entschlüsselung/-Prüfung auf der Firewall aktiviert, leidet oft die Netzwerkleistung darunter – manchmal sogar extrem. Die NSA-Firewalls umfassen eine Multicore-Hardware-Architektur mit Mikroprozessoren, die über spezielle Sicherheitsfunktionen verfügen. Dieses einzigartige Design, in Kombination mit unserer RFDPI-Engine, beseitigt die Leistungseinbußen, die oft mit anderen Firewalls einhergehen.

Heute reichen Bedrohungsinformationen von externen Partnern einfach nicht mehr aus. Aus diesem Grund arbeitet SonicWall mit einem eigenen internen Threat Research-Team – und das schon seit über 15 Jahren. Dieses spezielle Team sammelt, analysiert und prüft Daten aus über einer Million Sensoren in seinem Global Response Intelligent Defense(GRID)-Netzwerk. SonicWall nimmt auch an gemeinsamen Brancheninitiativen teil und steht mit Threat-Research-Communitys im Kontakt, um Informationen zu Angriffen und Schwachstellen zu sammeln und auszutauschen. Auf Basis dieser gemeinsamen Bedrohungsinformationen entwickeln wir Echtzeit-Abwehrmechanismen, die automatisch auf den Firewalls unserer Kunden implementiert werden.

Vorteile:

Überragender Bedrohungsschutz und exzellente Performance

- Patentierte Reassembly-Free Deep Packet Inspection-Technologie
- Integrierter und Cloud-basierter Bedrohungsschutz
- SSL-/TLS-Entschlüsselung und -Prüfung
- Effiziente, bewährte Sicherheit
- Multicore-Hardware-Architektur
- Spezielles internes Threat Research-Team

Mehr Netzwerkkontrolle und Flexibilität

- Leistungsstarkes SonicOS-Betriebssystem
- Application-Intelligence und Anwendungskontrolle
- Netzwerksegmentierung mit VLANs
- Wireless-Netzwerk-Sicherheit

Einfache Implementierung, Einrichtung und laufende Verwaltung

- Fest integrierte Lösung
- Zentrale Verwaltung
- Skalierbarkeit dank mehrerer Hardware-Plattformen
- Geringe Total Cost of Ownership

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

Mehr Netzwerkkontrolle und Flexibilität

Herzstück der NSA Series ist SonicOS, das funktionsreiche Betriebssystem von SonicWall. SonicOS bietet Organisationen die nötige Netzwerkkontrolle und Flexibilität dank Funktionen wie Application-Intelligence und Anwendungskontrolle, Echtzeitvisualisierung, einem Intrusion-Prevention-System (IPS) mit ausgeklügeltem Umgehungsschutz, schnellem Virtual Private Networking (VPN) und anderen robusten Sicherheitsfeatures.

Mithilfe der Application-Intelligence- und Anwendungskontrollfunktionen können Netzwerkadministratoren produktive Anwendungen identifizieren, kategorisieren und von unproduktiven oder potenziell gefährlichen Applikationen unterscheiden. Außerdem können sie durch leistungsstarke Regeln auf Anwendungsebene, die sowohl für einzelne Benutzer als auch für bestimmte Gruppen greifen können, den Datenverkehr kontrollieren (zusammen mit Zeitplänen und Ausnahmelisten). Geschäftskritische Anwendungen können sie priorisieren und ihnen mehr Bandbreite zuweisen, während die Bandbreite für nicht relevante Anwendungen beschränkt wird. Funktionen für die Echtzeitüberwachung und -visualisierung bieten eine grafische Darstellung der Anwendungen, User und Bandbreitennutzung und ermöglichen so detaillierte Einblicke in den gesamten Netzwerkverkehr.

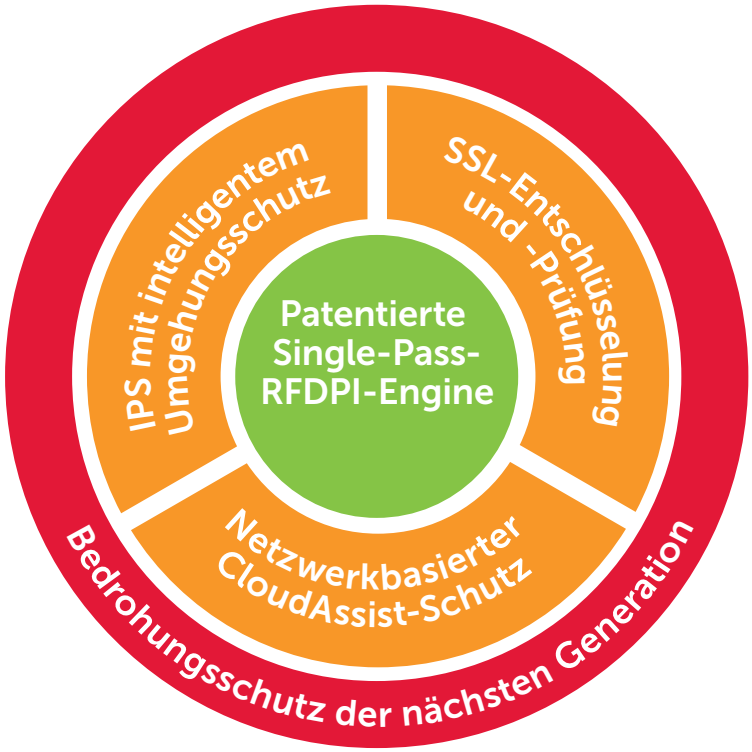
Organisationen, die mehr Flexibilität für ihr Netzwerkdesign benötigen, bietet SonicOS die erforderlichen Tools, um das Netzwerk mithilfe virtueller LANs (VLANs) auf sichere Weise zu segmentieren. Netzwerkadministratoren können so eine Oberfläche für virtuelle LANs erstellen, die eine Netzwerkunterteilung in eine oder mehrere logische Gruppen erlaubt. Darüber hinaus können Administratoren Regeln definieren, die das Maß an Kommunikation mit Geräten in anderen VLANs bestimmen.

Jede NSA-Firewall verfügt über einen Wireless Access Controller, der eine sichere Erweiterung der Netzwerkgrenze mithilfe von Wireless-Technologie erlaubt. Mit den SonicWall-Firewalls und den SonicPoint 802.11ac Wireless Access Points entsteht eine Wireless-Netzwerksicherheitslösung, die führende Next-Generation-Firewall-Funktionen mit Highspeed-Wireless-Technologie vereint. Das Ergebnis sind Netzwerksicherheit und Performance der Enterprise-Klasse über das drahtlose Netzwerk hinweg.

Einfache Implementierung, Einrichtung und laufende Verwaltung

Wie alle SonicWall-Firewalls integriert auch die NSA Series zentrale Technologien rund um Sicherheit, Konnektivität und Flexibilität in einer einzigen umfassenden Lösung. Dazu gehören die SonicPoint Wireless Access Points und die SonicWall WAN Acceleration Appliance (WXA) Series. Beide werden von der NSA-Verwaltungsfirewall automatisch erkannt und bereitgestellt. Durch die Konsolidierung mehrerer Funktionen müssen keine Einzellösungen mehr gekauft und installiert werden – ein großer Vorteil, da diese oft nicht gut miteinander harmonieren. Somit erfordert die Implementierung und Konfiguration der Lösung im Netzwerk weniger Aufwand, was sowohl Zeit als auch Geld spart.

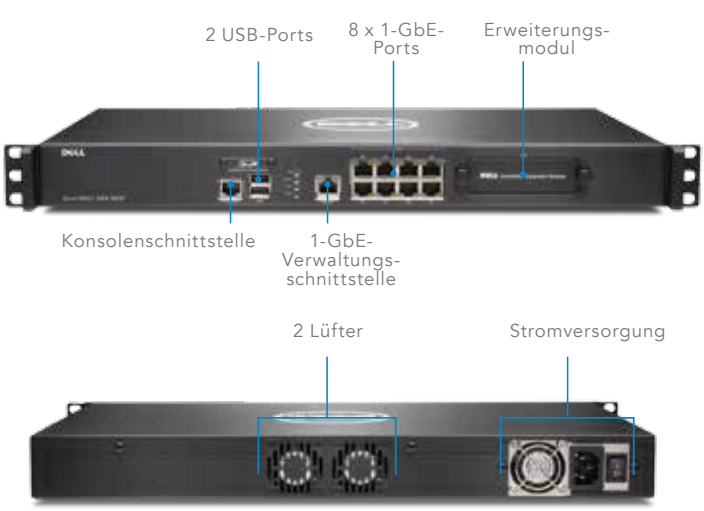
Die kontinuierliche Verwaltung und Überwachung der Netzwerksicherheit erfolgen zentral über die Firewall oder das SonicWall Global Management System (GMS). So können Administratoren über eine einzige Konsole alle Aspekte des Netzwerks verwalten. Dank der einfachen Implementierung, Einrichtung und Verwaltung können Organisationen ihre TCO senken und von einem schnellen ROI profitieren.



SONICWALL™

Network Security Appliance 2600

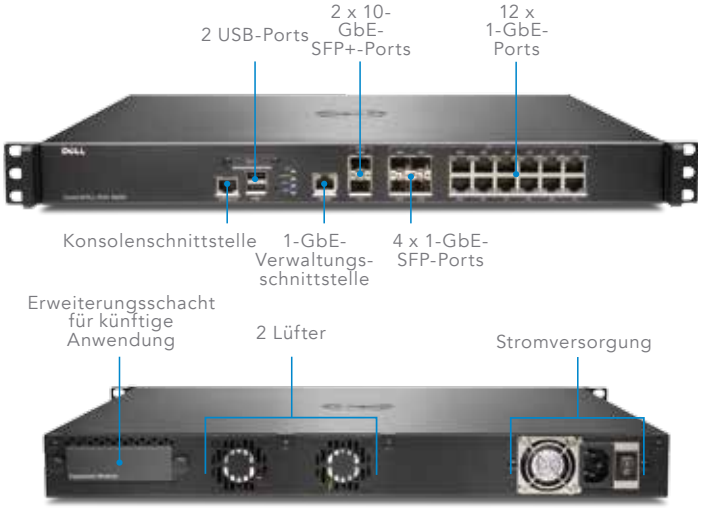
Die SonicWall NSA 2600 wurde für die Anforderungen kleiner Organisationen mit Wachstumspotenzial sowie Zweigniederlassungen und Schulen konzipiert.



Firewall	NSA 2600
Firewall-Durchsatz	1,9 GBit/s
IPS-Durchsatz	700 MBit/s
Anti-Malware-Durchsatz	400 MBit/s
Full-DPI-Durchsatz	300 MBit/s
IMIX-Durchsatz	600 MBit/s
Max. Anzahl von DPI-Verbindungen	125.000
Neue Verbindungen/Sekunde	15.000/Sek.
Beschreibung	**Artikelnummer**
NSA 2600 (nur Firewall)	01-SSC-3860
NSA 2600 TotalSecure (1 Jahr)	01-SSC-3863

Network Security Appliance 3600/4600

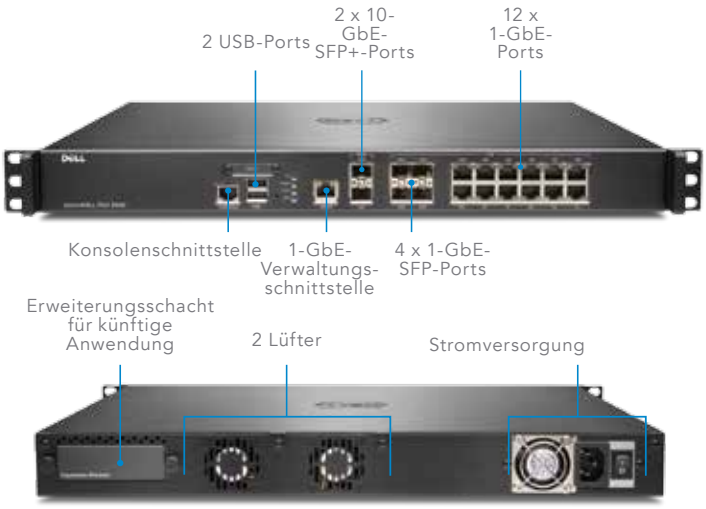
Die SonicWall NSA 3600/4600 eignet sich ideal für Zweigniederlassungen und kleine bis mittlere Unternehmen, die ihre Durchsatzkapazität und Performance optimieren möchten.



Firewall	NSA 3600	NSA 4600
Firewall-Durchsatz	3,4 GBit/s	6,0 GBit/s
IPS-Durchsatz	1,1 GBit/s	2,0 GBit/s
Anti-Malware-Durchsatz	600 MBit/s	1,1 GBit/s
Full-DPI-Durchsatz	500 MBit/s	800 MBit/s
IMIX-Durchsatz	900 MBit/s	1,6 GBit/s
Max. Anzahl von DPI-Verbindungen	175.000	200.000
Neue Verbindungen/Sekunde	20.000/Sek.	40.000/Sek.
Beschreibung	**NSA 3600**	**NSA 4600**
Nur Firewall	01-SSC-3850	01-SSC-3840
TotalSecure (1 Jahr)	01-SSC-3853	01-SSC-3843

Network Security Appliance 5600

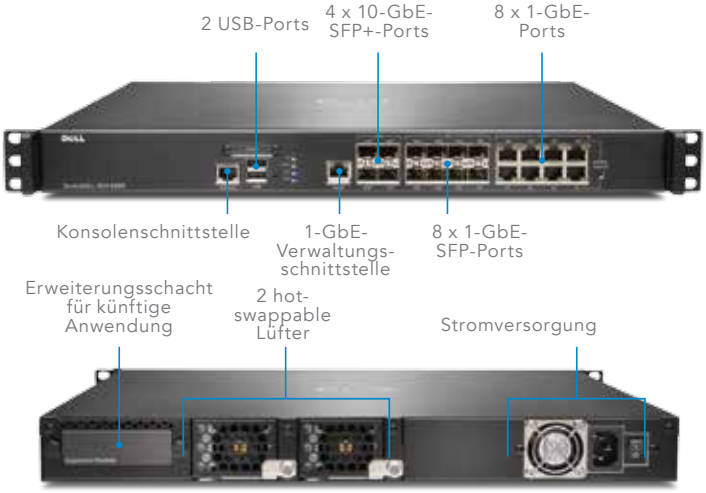
Die SonicWall NSA 5600 eignet sich ideal für verteilte Unternehmen sowie für deren Zweigniederlassungen und Netzwerkumgebungen, die eine erhebliche Durchsatzkapazität benötigen.



Firewall	NSA 5600
Firewall-Durchsatz	9,0 GBit/s
IPS-Durchsatz	3,0 GBit/s
Anti-Malware-Durchsatz	1,7 GBit/s
Full-DPI-Durchsatz	1,6 GBit/s
IMIX-Durchsatz	2,4 GBit/s
Max. Anzahl von DPI-Verbindungen	375.000
Neue Verbindungen/Sekunde	60.000/Sek.
Beschreibung	**Artikelnummer**
NSA 5600 (nur Firewall)	01-SSC-3830
NSA 5600 TotalSecure (1 Jahr)	01-SSC-3833

Network Security Appliance 6600

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



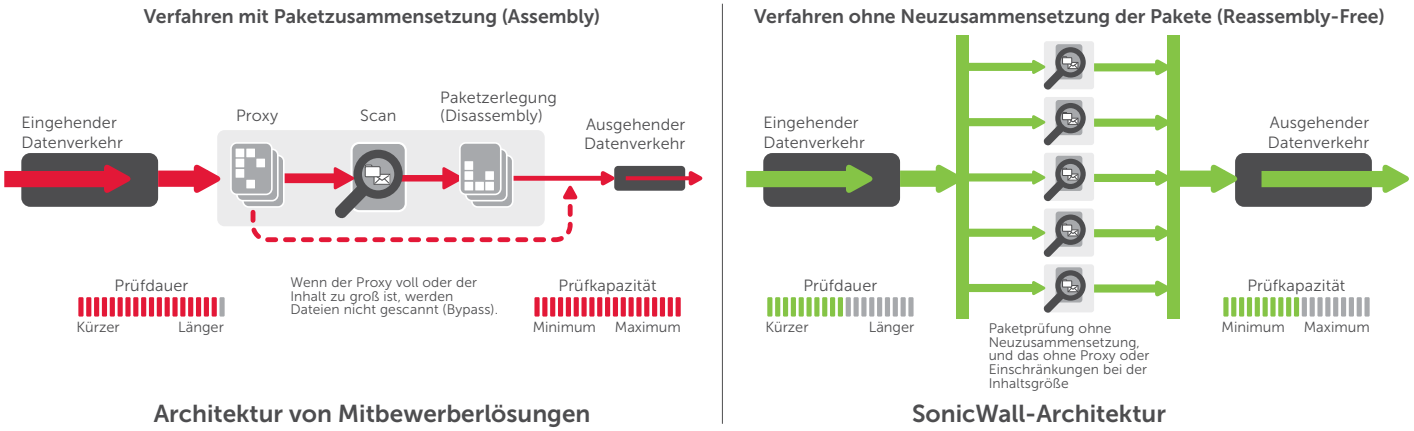
Firewall	NSA 6600
Firewall-Durchsatz	12,0 GBit/s
IPS-Durchsatz	4,5 GBit/s
Anti-Malware-Durchsatz	3,0 GBit/s
Full-DPI-Durchsatz	3,0 GBit/s
IMIX-Durchsatz	3,5 GBit/s
Max. Anzahl von DPI-Verbindungen	500.000
Neue Verbindungen/Sekunde	90.000/Sek.
Beschreibung	**Artikelnummer**
NSA 6600 (nur Firewall)	01-SSC-3820
NSA 6600 TotalSecure (1 Jahr)	01-SSC-3823

Reassembly-Free Deep Packet Inspection-Engine

Die SonicWall Reassembly-Free Deep Packet Inspection(RFDPI)-Engine bietet optimalen Schutz vor Bedrohungen und eine umfassende Anwendungskontrolle, ohne die Leistung zu beeinträchtigen. Die RFDPI-Engine prüft die Payload von Datenströmen, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren. Zudem 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 unbemerkt in das Netzwerk einzuschleusen.

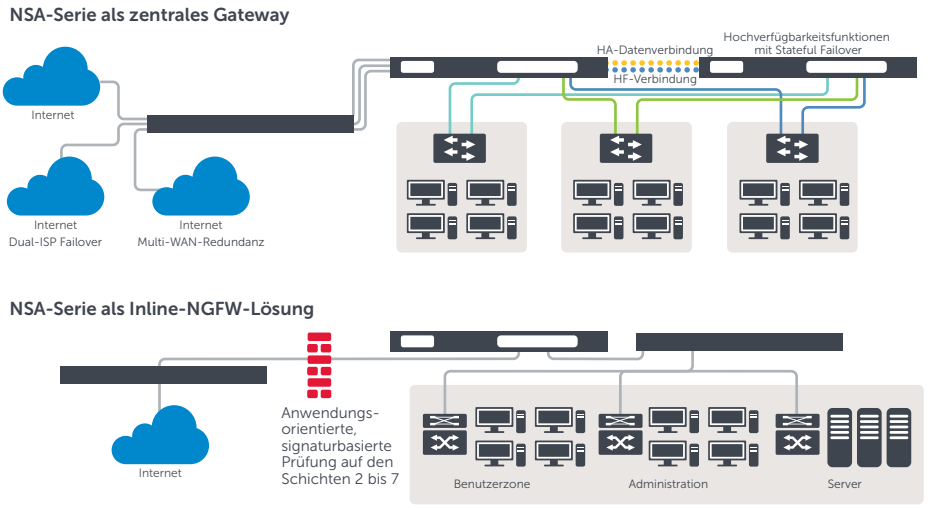
Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall aktualisiert 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.



Flexible, individuell anpassbare Implementierungsoptionen – die NSA Series im Überblick

Alle SonicWall-NSA-Appliances sind mit einem revolutionären Multicore-Hardware-Design und innovativer RFDPI-Technologie ausgestattet. Auf diese Weise schützen sie das Netzwerk vor internen und externen Bedrohungen, ohne die Netzwerkleistung zu beeinträchtigen. Die Next-Generation-Firewalls der NSA Series verfügen über Highspeed-Intrusion-Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten, leistungsstarke Application-Intelligence und Anwendungskontrolle sowie zahlreiche erweiterte, flexible Netzwerk- und Konfigurationsfeatures. Die NSA Series bietet eine erschwingliche Plattform, die sich in den unterschiedlichsten Netzwerkumgebungen von Zweigniederlassungen sowie großen und verteilten Unternehmen leicht implementieren und verwalten lässt.

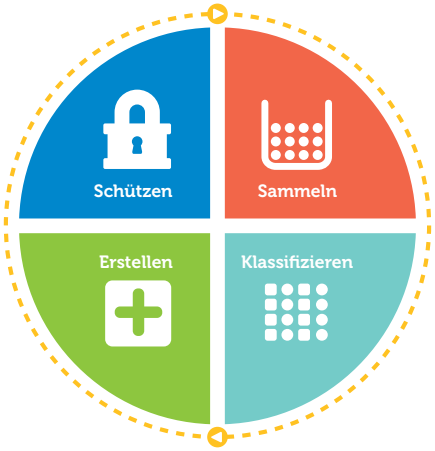


Sicherheit und Schutz

Das interne 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 Telemetriedaten zu den neuesten Bedrohungen liefern. Diese Informationen werden anschließend für wichtige Funktionen wie Intrusion-Prevention, Malware-Schutz und Anwendungserkennung eingesetzt.

Kunden mit Next-Generation Firewalls von SonicWall 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 Attacken. Eine einzige Signatur deckt dabei Zehntausende verschiedene Bedrohungen ab.

Zusätzlich zu den Abwehrmechanismen auf der Appliance bieten die NSA-Produkte auch Zugang zum SonicWall CloudAV Service. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um über 30 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 SonicWall in der Lage, den Verkehr aus gefährlichen Domänen oder ganzen Regionen zu blockieren, um die Sicherheitsrisiken im Netzwerk zu reduzieren.



Application-Intelligence und Anwendungskontrolle

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 im Datenverkehr werden mittels Echtzeitvisualisierung augenblicklich identifiziert. So können unverzüglich Gegenmaßnahmen eingeleitet werden, um das Netzwerk vor potenziellen ein- oder ausgehenden Angriffen zu schützen oder Performance-Engpässe zu verhindern.

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 außerdem für mehr Benutzerfreundlichkeit, erhöhen die Produktivität und reduzieren die Support-Anfragen.

Das SonicWall Global Management System (GMS®) vereinfacht mit seiner intuitiven, webbasierten Oberfläche die Verwaltung der Application-Intelligence- und Anwendungskontrollfunktionen.

SONICWALL™

Funktionen

RFDPI-Engine	
Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection (RFDPI)	Diese hochleistungsfähige, proprietäre und patentierte Prüf-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 gleichzeitig auf Bedrohungen geprüft, um zu verhindern, dass ein infizierter Computer das Netzwerk zum Verbreiten von Malware oder als Ausgangsplattform für Angriffe nutzt.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxys 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.
Capture ATP	
Funktion	Beschreibung
Multi-Engine-Sandbox	Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus, analysiert dessen Verhalten und macht bösartige Aktivitäten transparent.
Analyse unterschiedlichster Dateitypen und -größen	Der Service analysiert unterschiedlichste Dateitypen, darunter ausführbare Programme (PE), DLL, PDFs, MS Office-Dokumente, Archive, JAR und APK sowie unterschiedliche Betriebssysteme (Windows, Android, Mac OSX) und Multi-Browser-Umgebungen.
Schnelle Implementierung von Signaturen	Wird eine Datei als bösartig identifiziert, so wird innerhalb von 48 Stunden eine Signatur auf Firewalls mit aktivem SonicWall Capture-Abo aufgespielt und in die GRID-Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt.
Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus	Um zu verhindern, dass potenziell bösartige Dateien in das Netzwerk eindringen, können die zur Analyse in die Cloud gesendeten Dateien am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist.
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 Signatur-Updates	Das 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 weder einen Neustart noch sonstige Unterbrechungen.
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.

Intrusion-Prevention (Fortsetzung)	
Funktion	Beschreibung
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 Schichten 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.

Bedrohungsschutz	
Funktion	Beschreibung
Netzwerkbasierter Malware-Schutz	Die SonicWall-RFDPI-Engine prüft den gesamten Verkehr auf Viren, Trojaner, Keylogger und andere Malware in beliebig großen Dateien und über alle Ports und TCP-Streams hinweg. Die Prüfung erfolgt sowohl in ein- als auch ausgehender Richtung sowie innerhalb von Zonen.
CloudAV-Malware-Schutz	Eine kontinuierlich aktualisierte Datenbank mit über 30 Millionen Bedrohungssignaturen auf den Cloud-Servern von SonicWall ergänzt die lokalen Signaturendatenbanken und sorgt dafür, dass die RFDPI-Engine eine größtmögliche Anzahl an Bedrohungen abdeckt.
Cloud-basiertes Sandboxing	Der SonicWall Capture Advanced Threat Protection Service setzt auf Cloud-basiertes Multi-Engine-Sandboxing mit umfassender Systemsimulation, Virtualisierung und Analysetechnologien auf Hypervisor-Ebene. Damit lassen sich verdächtige Dateien analysieren, böswilliges Verhalten identifizieren und unbekannte sowie Zero-Day-Angriffe am Gateway blockieren.
Sicherheitsupdates rund um die Uhr	Das 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-Entschlüsselung und -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.
Enforced Anti-Virus and Anti-Spyware Client-Software	Nicht regelkonforme Endpunktgeräte werden automatisch erkannt. Die Anti-Virus- und Anti-Spyware-Software* von SonicWall wird auf jedem einzelnen Rechner über das gesamte Netzwerk hinweg installiert, egal ob sich die Geräte innerhalb des Unternehmensnetzes befinden oder außerhalb über ein VPN verbunden sind. Nur für Windows.

*Erfordert die SonicWall Anti-Virus and Anti-Spyware Client-Software.

Application-Intelligence und Anwendungskontrolle	
Funktion	Beschreibung
Anwendungskontrolle	Kontrolle von Anwendungen oder einzelnen Anwendungsmerkmalen, die anhand einer kontinuierlich erweiterten Datenbank mit über 3.500 Anwendungssignaturen von der RFDPI-Engine erkannt werden. Dadurch lassen sich Netzwerksicherheit und -produktivität erhöhen.
Identifizierung benutzerdefinierter Anwendungen	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	Bandbreitenkapazität kann für kritische Anwendungen oder Anwendungskategorien granular zugewiesen und reguliert werden. Gleichzeitig lässt sich jedweder nicht notwendiger Anwendungsverkehr unterbinden.
Visualisierung von internem und externem Verkehr	Erkennung der Bandbreitennutzung und Analyse des Netzwerkverhaltens mit Echtzeitvisualisierung des internen Anwendungsverkehrs und Berichten zum externen Anwendungsverkehr via NetFlow/IPFix.

Application-Intelligence und Anwendungskontrolle (Fortsetzung)	
Funktion	Beschreibung
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-/Terminaldienst-/Citrix-Integration.

Content-Filtering	
Funktion	Beschreibung
Internes/Externes Content-Filtering	Über den Content Filtering Service lassen sich Richtlinien zu Nutzungseinschränkungen effektiv durchsetzen und Websites mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren. Mit dem Content Filtering Client kann die Richtliniendurchsetzung zudem erweitert werden, um Internetinhalte auch auf Geräten außerhalb der Firewallgrenze zu blockieren.
Gezielte Kontrollmöglichkeiten	Inhalte lassen sich auf Basis der bereits vordefinierten Kategorien oder einer beliebigen Kombination an Kategorien blockieren. Die Filter können für eine bestimmte Tageszeit aktiviert werden, z. B. während Unterrichts- oder Geschäftszeiten, und auf einzelne Benutzer oder Gruppen beschränkt werden.
Dynamische Rating-Architektur	Alle aufgerufenen Websites werden gegen eine dynamisch aktualisierte Datenbank in der Cloud mit Millionen klassifizierter URLs, IP-Adressen und Domänen in Echtzeit abgeglichen.
Web-Caching	URL-Bewertungen werden lokal auf der SonicWall-Firewall zwischengespeichert, sodass jeder weitere Zugriff auf häufig besuchte Websites nur den Bruchteil einer Sekunde dauert.

Durchsetzung von Viren- und Spyware-Schutz	
Funktion	Beschreibung
Mehrstufiger Schutz	Die Gateway-Anti-Virus-Lösung einer Firewall bildet die erste Verteidigungslinie am Netzwerkrand. Allerdings können Viren immer noch über Laptops, USB-Sticks und andere ungeschützte Systeme ins Netzwerk gelangen. Ein mehrschichtiger Viren- und Spyware-Schutz lässt sich sowohl auf den Client als auch auf den Server ausweiten.
Automatisierte Durchsetzung	Es wird sichergestellt, dass auf jedem Computer, der auf das Netzwerk zugreift, die neueste Version der Signaturen für Viren- und Spyware-Schutz installiert und aktiviert ist. Somit entfallen die Kosten, die typischerweise für die Verwaltung von Desktop-Lösungen für Viren- und Spyware-Schutz entstehen.
Automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz werden automatisch und netzwerkweit auf jedem Rechner installiert und bereitgestellt, sodass der administrative Mehraufwand minimiert wird.
Ständig aktiver, automatischer Virenschutz	Der Viren- und Spyware-Schutz wird häufig aktualisiert und transparent auf allen Desktop-PCs und Dateiservern bereitgestellt. Das sorgt für höhere Endbenutzerproduktivität und reduziert den Aufwand für die Sicherheitsverwaltung.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt den eingehenden Verkehr und blockiert die Installation zahlreicher Spyware-Programme auf Desktop-PCs und Laptops, bevor vertrauliche Daten übertragen werden können. Auf diese Weise werden die Sicherheit und die Performance von Desktops erhöht.

Firewall und Networking	
Funktion	Beschreibung
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die 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 Implementierungsoptionen	Die NSA Series lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
IPv6-Unterstützung	Die NSA Series unterstützt das Internetprotokoll IPv6, das die Anzahl verfügbarer IP-Adressen erhöht. Die NSA-Firewalls haben die IPv6-Ready-Phasen 1 und 2 sowie die ICSA Labs-Enterprise-Zertifizierung (einschließlich IPv6-Prüfung) erhalten.

Firewall und Networking (Fortsetzung)	
Funktion	Beschreibung
Hochverfügbarkeit/Clustering	Die NSA Series 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-Unterstützung	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	Das SonicWall GMS ermöglicht es, über eine einzige Verwaltungsschnittstelle mit intuitiver Oberfläche mehrere SonicWall-Appliances zu überwachen und zu konfigurieren und Berichte zu erstellen. Dies reduziert nicht nur die Kosten, sondern auch die Komplexität bei der Verwaltung.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche beschleunigt und vereinfacht die Konfiguration, erlaubt eine umfassende CLI und bietet Support für SNMPv2/3.
Berichte zum Anwendungsdatenstrom	Tools wie SonicWall GMS oder Analyzer erlauben den Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr und ermöglichen somit eine Echtzeitüberwachung bzw. historische Überwachung.

Virtual Private Networking	
Funktion	Beschreibung
IPSec-VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPSec-VPN kann die NSA Series als VPN-Konzentrator für Tausende großer Standorte, Zweigniederlassungen oder Home-Offices eingesetzt werden.
Remote-Zugriff per SSL-VPN und IPsec-Client	Durch Einsatz der clientlosen SSL-VPN-Technologie oder eines leicht zu verwaltenden IPSec-Clients ist der unkomplizierte Zugriff auf E-Mails, Dateien, Rechner, Intranet-Sites und Anwendungen von zahlreichen unterschiedlichen Plattformen möglich.
Redundantes VPN-Gateway	Mit 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	Bei Ausfall eines temporären VPN-Tunnels wird der Datenverkehr reibungslos über alternative Verbindungen zwischen Endgeräten umgeleitet. Dieses dynamische Routing über VPN-Links sorgt für eine hohe Ausfallsicherheit.

Content- bzw. kontextorientierte Sicherheitsfunktionen	
Funktion	Beschreibung
Nachverfolgung der Benutzeraktivitäten	Bereitstellung von Informationen zur Benutzerkennung und -aktivität, die auf der nahtlosen SSO-Integration für AD/LDAP/Citrix/Terminaldienste sowie umfassenden DPI-Daten basieren.
Identifizierung des Datenverkehrs nach Ländern mittels Geo-IP	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 das 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
- Stealth-Modus
- Common Access Card(CAC)-Unterstützung
- Schutz vor DoS-Angriffen
- UDP-/ICMP-/SYN-Flood-Schutz
- SSL-Entschlüsselung und -Prüfung
- IPv6-Sicherheit

Intrusion-Prevention
- Signaturbasierte Prüfung
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granulare IPS-Regeln
- Auf GeoIP und Reputation basierende Filterfunktionen
- Abgleich regulärer Ausdrücke

Malware-Schutz
- Streambasierte Malware-Prüfung
- Gateway-Anti-Virus
- Gateway-Anti-Spyware
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloud-basierte Malware-Datenbank

Anwendungskontrolle
- Anwendungskontrolle
- Blockieren von Anwendungskomponenten
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Nachverfolgung der Benutzeraktivitäten (SSO)
- Umfassende Anwendungs-signaturendatenbank

Filterung von Webinhalten
- URL-Filtering
- Anti-Proxy-Technologie
- Blockieren mithilfe von Schlüsselwörtern
- Bandbreitenverwaltung mit CFS-Ratingkategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- 56 Content-Filtering-Kategorien
- Content Filtering Client

VPN
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPsec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (OSPF, RIP)

Networking
- Jumbo-Frames
- Layer-2-Netzwerkerkennung
- IPv6
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- RSTP (Rapid Spanning Tree Protocol)
- Portspiegelung
- Layer-2-QoS
- Portsicherheit
- Dynamisches 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
- Granulare QoS-Kontrolle
- Bandbreitenmanagement
- DPI für VoIP-Daten
- H.323-Gatekeeper- und SIP-Proxy-Support

Verwaltung und Überwachung
- Web-Oberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Zentralisierte Management- und Reporting-Funktionen
- Logging
- Netflow-/IPFIX-Export
- Visualisierung des Anwendungsverkehrs
- Zentralisierte Regelverwaltung
- Single-Sign-on (SSO)
- Unterstützung für Terminaldienste/Citrix
- BlueCoat Security Analytics Platform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung

IPv6
- IPv6-Filterung
- 6rd (schnelle Bereitstellung)
- DHCP-Präfixdelegierung
- Wire-Modus
- BGP

Capture ATP
- Cloud-basierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Automatische Blockierung

NSA Series – Systemdaten

	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Betriebssystem	SonicOS 6.2.2				
Security-Prozessor-Cores	4 x 800 MHz	6 x 800 MHz	8 x 1,1 GHz	10 x 1,3 GHz	24 x 1,0 GHz
10-GbE-Schnittstellen	—	2 x 10-GbE-SFP+			4 x 10-GbE-SFP+
1-GbE-Schnittstellen	8 x 1-GbE	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			4,0 GB	
Erweiterung	1 Erweiterungssteckplatz (Rückseite)*, SD-Karte*				
Firewall-Inspection-Durchsatz[1]	1,9 GBit/s	3,4 GBit/s	6,0 GBit/s	9,0 GBit/s	12,0 GBit/s
Full-DPI-Durchsatz[2]	300 MBit/s	500 MBit/s	800 MBit/s	1,6 GBit/s	3,0 GBit/s
Application-Inspection-Durchsatz[2]	700 MBit/s	1,1 GBit/s	2,0 GBit/s	3,0 GBit/s	4,5 GBit/s
IPS-Durchsatz[2]	700 MBit/s	1,1 GBit/s	2,0 GBit/s	3,0 GBit/s	4,5 GBit/s
Anti-Malware-Inspection-Durchsatz[2]	400 MBit/s	600 MBit/s	1,1 GBit/s	1,7 GBit/s	3,0 GBit/s
IMIX-Durchsatz[3]	600 MBit/s	900 MBit/s	1,6 GBit/s	2,4 GBit/s	3,5 GBit/s
SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	200 MBit/s	300 MBit/s	500 MBit/s	800 MBit/s	1,3 GBit/s
VPN-Durchsatz[3]	1,1 GBit/s	1,5 GBit/s	3,0 GBit/s	4,5 GBit/s	5,0 GBit/s
Verbindungen pro Sekunde	15.000/Sek.	20.000/Sek.	40.000/Sek.	60.000/Sek.	90.000/Sek.
Maximale Anzahl von Verbindungen (SPI)	225.000	325.000	400.000	562.500	750.000
Maximale Anzahl von Verbindungen (DPI)	125.000	175.000	200.000	375.000	500.000
Unterstützte SonicPoints (max.)	32	48	64	96	128
Single-Sign-on(SSO)-Benutzer	30.000	40.000	50.000	60.000	70.000
VPN	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Site-to-Site-Tunnel	250	1.000	3.000	4.000	6.000
IPSec-VPN-Clients (max.)	10 (250)	50 (1.000)	500 (3.000)	2.000 (4.000)	2.000 (6.000)
SSL-VPN-Lizenzen (max.)	2 (250)	2 (350)	2 (500)	2 (1000)	2 (1500)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128/192/256 Bit), MD5, SHA-1, Suite B Cryptography				
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14				
Routenbasiertes VPN	RIP, OSPF				
Networking	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
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	256	256	256	400	500
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, Terminaldienste, Citrix, Common Access Card (CAC)				
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	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall und IPS), UC APL				

Hardware	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Stromversorgung	200 W	Einfach, fest, 250 W			
Lüfter	2, fest				2, redundant, hot-swappable
Eingangsspannung	100–240 VAC, 60–50 Hz				
Maximaler Stromverbrauch (W)	49,4	74,3	86,7	90,9	113,1
Formfaktor	rackfähig (1 HE)				
Abmessungen	4,5 x 26 x 43 cm	4,5 x 48,5 x 43 cm			
Gewicht	4,6 kg	6,15 kg			6,77 kg
WEEE-Gewicht	5,0 kg	6,46 kg			8,97 kg
Versandgewicht	6,5 kg	9,43 kg			11,85 kg
Erfüllt folgende Standards/Normen	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico CoC nach UL, WEEE , REACH, ANATEL, BSMI, CU				
Umgebungstemperatur	0–40 °C				
Luftfeuchtigkeit	10–90 %, nicht kondensierend				
MTBF (Jahre)	20,2	16,8	16,0	15,4	13,3

[1] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen 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 1.280 Bytes pro Paket gemäß RFC 2544. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.
*Für künftige Anwendung.

Bestellinformationen zur NSA Series

Produkt	Artikelnummer
NSA 2600 TotalSecure (1 Jahr)	01-SSC-3863
NSA 3600 TotalSecure (1 Jahr)	01-SSC-3853
NSA 4600 TotalSecure (1 Jahr)	01-SSC-3843
NSA 5600 TotalSecure (1 Jahr)	01-SSC-3833
NSA 6600 TotalSecure (1 Jahr)	01-SSC-3823
NSA 2600 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NSA 2600 (1 Jahr)	01-SSC-1470
Capture Advanced Threat Protection für NSA 2600 (1 Jahr)	01-SSC-1475
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NSA 2600 (1 Jahr)	01-SSC-4459
Silver 24/7-Support für NSA 2600 (1 Jahr)	01-SSC-4314
Content Filtering Premium Business Edition für NSA 2600 (1 Jahr)	01-SSC-4465
Enforced Client Anti-Virus & Anti-Spyware – Kaspersky	Basierend auf Benutzeranzahl
Comprehensive Anti-Spam Service für NSA 2600 (1 Jahr)	01-SSC-4471
NSA 3600 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NSA 3600 (1 Jahr)	01-SSC-1480
Capture Advanced Threat Protection für NSA 3600 (1 Jahr)	01-SSC-1485
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NSA 3600 (1 Jahr)	01-SSC-4435
Silver 24/7-Support für NSA 3600 (1 Jahr)	01-SSC-4302
Content Filtering Premium Business Edition für NSA 3600 (1 Jahr)	01-SSC-4441
Enforced Client Anti-Virus & Anti-Spyware – Kaspersky	Basierend auf Benutzeranzahl
Comprehensive Anti-Spam Service für NSA 3600 (1 Jahr)	01-SSC-4447
NSA 4600 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NSA 4600 (1 Jahr)	01-SSC-1490
Capture Advanced Threat Protection für NSA 4600 (1 Jahr)	01-SSC-1495
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NSA 4600 (1 Jahr)	01-SSC-4411
Silver 24/7-Support für NSA 4600 (1 Jahr)	01-SSC-4290
Content Filtering Premium Business Edition für NSA 4600 (1 Jahr)	01-SSC-4417
Enforced Client Anti-Virus & Anti-Spyware – Kaspersky	Basierend auf Benutzeranzahl
Comprehensive Anti-Spam Service für NSA 4600 (1 Jahr)	01-SSC-4423

NSA 5600 – Support und Sicherheitsabos	Artikelnummer
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NSA 5600 (1 Jahr)	01-SSC-1550
Capture Advanced Threat Protection für NSA 5600 (1 Jahr)	01-SSC-1555
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NSA 5600 (1 Jahr)	01-SSC-4240
Gold 24/7-Support für NSA 5600 (1 Jahr)	01-SSC-4284
Content Filtering Premium Business Edition für NSA 5600 (1 Jahr)	01-SSC-4246
Enforced Client Anti-Virus & Anti-Spyware – Kaspersky	Basierend auf Benutzeranzahl
Comprehensive Anti-Spam Service für NSA 5600 (1 Jahr)	01-SSC-4252
NSA 6600 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NSA 6600 (1 Jahr)	01-SSC-1560
Capture Advanced Threat Protection für NSA 6600 (1 Jahr)	01-SSC-1565
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NSA 6600 (1 Jahr)	01-SSC-4216
Gold 24/7-Support für NSA 6600 (1 Jahr)	01-SSC-4278
Content Filtering Premium Business Edition für NSA 6600 (1 Jahr)	01-SSC-4222
Enforced Client Anti-Virus & Anti-Spyware – Kaspersky	Basierend auf Benutzeranzahl
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**
SonicWall GMS Software-Lizenz (10 Nodes)	01-SSC-3363
SonicWall GMS E-Class 24/7-Software-Support für 10 Nodes (1 Jahr)	01-SSC-6514

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

Modellnummern (Zulassung):

NSA 2600–1RK29-0A9

NSA 3600–1RK26-0A2

NSA 4600–1RK26-0A3

NSA 5600–1RK26-0A4

NSA 6600–1RK27-0A5

SonicWall
5455 Great America Parkway, Santa Clara, CA 95054
www.sonicwall.com
Informationen zu unseren Niederlassungen außerhalb Nordamerikas finden Sie auf unserer Website.

Datasheet-SonicWall-NetworkSecurityAppliance-NoMT-US-CW-20879

SONICWALL™