# SonicWall Network Security Appliance (NSA) Series

Bewährte Sicherheit und Performance für mittelgroße Netzwerke

Die SonicWall Network Security Appliance (NSA) Series bietet mittelgroßen Netzwerken, Zweigniederlassungen und verteilten Unternehmen eine hoch entwickelte Sicherheitsplattform für einen zuverlässigen Schutz vor raffinierten 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 arbeiten mit fortschrittlichen Sicherheitstechnologien, die einen überragenden Bedrohungsschutz bieten. 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 integrierten Funktionen wie Intrusion-Prevention, Anti-Malware und Web-/URL-Filtering nutzt die NSA Series den Cloud-basierten SonicWall Capture-Multi-Engine-Sandboxing-Service, 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 fünf Jahre in Folge aufgrund ihrer effizienten Schutzmechanismen als eine der branchenweit besten bewertet.

Darüber hinaus bieten die Next-Generation-Firewalls von SonicWall einen umfassenden Schutz, weil sie unabhängig von Übertragung oder Protokoll eine vollständige Entschlüsselung und Prüfung von TLS-/SSL- und SSH-verschlüsselten Verbindungen sowie von nicht proxyfähigen Anwendungen durchführen. Alle Pakete (Header und Daten) werden gründlich geprüft. Dabei suchen die SonicWall-Firewalls nach Nichteinhaltung von Protokollen, Bedrohungen, Zero-Day-Angriffen, Eindringversuchen und sogar nach definierten Kriterien zur Erkennung und Abwehr versteckter Angriffe, die Kryptografie einsetzen. Außerdem blockieren sie verschlüsselte Malware-Downloads, verhindern die Ausbreitung von Infektionen und unterbinden Command-and-control(C&C)-Kommunikation sowie das Herausschleusen vertraulicher Daten. Eine umfassende Kontrolle erlauben Auswahl- und Ausschlussregeln, mit denen sich festlegen lässt, welcher Verkehr entschlüsselt und geprüft werden soll, um bestimmte Compliance-Anforderungen in Organisationen und/oder rechtliche Vorgaben zu erfüllen.

Sind Deep Packet Inspection-Funktionen wie zum Beispiel Intrusion-Prevention, Viren- und Spyware-Schutz sowie TLS-/SSL-Entschlüsselung/-Prüfung auf der Firewall aktiviert, leidet oft die Netzwerkleistung darunter – manchmal sogar extrem. Die NSA-Firewalls bieten jedoch 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. Daher arbeitet SonicWall mit seinem eigenen internen Capture Labs 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 Capture Threat-Netzwerk. SonicWall nimmt auch an gemeinsamen Brancheninitiativen teil und steht mit Threat-Research-Communitys im

## Vorteile:

### Überragender Bedrohungsschutz und exzellente Performance

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

### Mehr Netzwerkkontrolle und Flexibilität

- Leistungsstarkes SonicOS-Betriebssystem
- Application-Intelligence und Anwendungskontrolle
- Netzwerksegmentierung mit VLANs
- Sichere Highspeed-WLAN-Verbindung

### 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*

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.

## 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) zu segmentieren. Netzwerkadministratoren können so ein virtuelles LAN-Interface erstellen, das 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. In Verbindung mit den SonicWave 802.11ac Wave 2 Wireless Access Points bieten unsere Firewalls eine drahtlose Netzwerksicherheitslösung, die führende Next-Generation-Firewall-Funktionen mit Highspeed-Wireless-Technologie vereint und eine hohe Netzwerksicherheit und Performance der Enterprise-Klasse über das gesamte drahtlose Netzwerk hinweg garantiert.

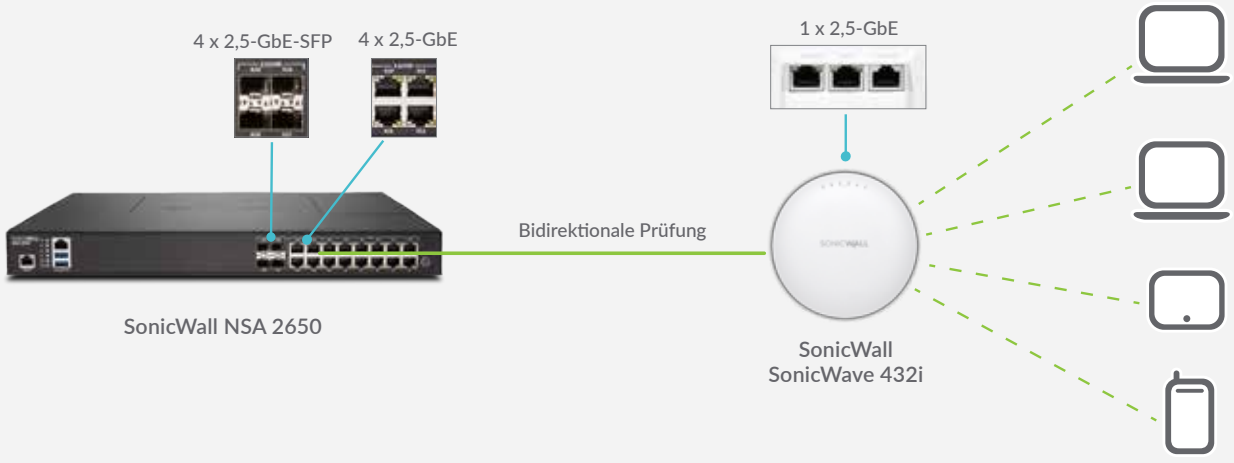
## Einfache Implementierung, Einrichtung und laufende Verwaltung

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 SonicWave 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.

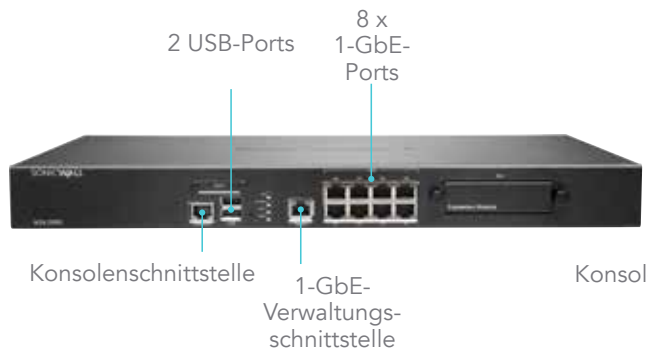
## Sichere Highspeed-WLAN-Verbindung

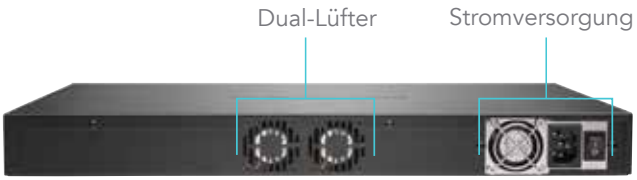
Kombiniert mit einem SonicWall SonicWave 802.11ac Wave 2 Wireless Access Point wird aus der Next-Generation-Firewall NSA 2650 eine drahtlose Highspeed-Netzwerksicherheitslösung. Sowohl die SonicWall-Firewalls NSA 2650 als auch die SonicWave Access Points verfügen über 2,5-GbE-Ports, um den hohen drahtlosen Wave-2-Wireless-Multi-Gigabit-Durchsatz zu ermöglichen Die NSA 2650 durchleuchtet den gesamten ein- und ausgehenden drahtlosen Verkehr im Netzwerk mittels Deep Packet Inspection und beseitigt anschließend gefährliche Bedrohungen wie Malware und Eindringversuche selbst bei verschlüsselten Verbindungen. Weitere Sicherheits- und Kontrollfunktionen wie Content-Filtering, Anwendungskontrolle, Application Intelligence und Capture Advanced Threat Protection können als zusätzliche Sicherheitsschicht auf den drahtlosen Netzwerkverkehr angewendet werden.



## Network Security Appliance 2600

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

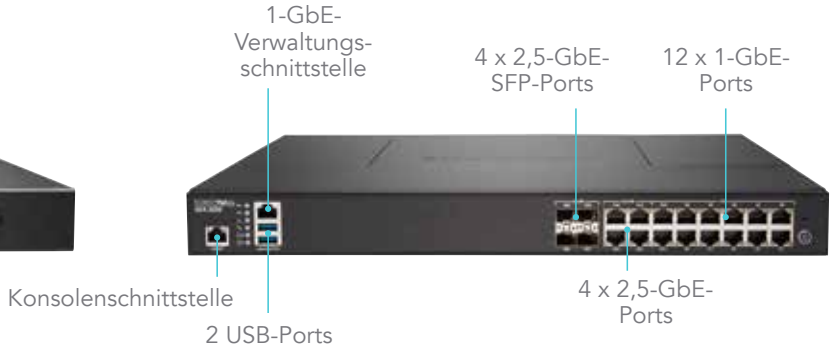


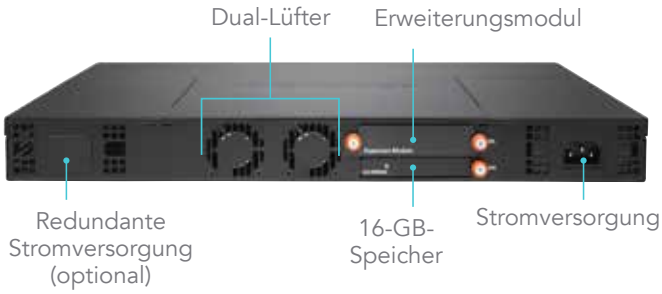




| Firewall | NSA 2600 |
|---|---|
| Firewall-Durchsatz | 1,9 GBit/s |
| IPS-Durchsatz | 700 MBit/s |
| Anti-Malware-Durchsatz | 400 MBit/s |
| Full-DPI-Durchsatz | 300 MBit/s |
| IMIX-Durchsatz | 600 MBit/s |
| Max. Anzahl von DPI-Verbindungen | 250.000 |
| Neue Verbindungen/Sekunde | 15.000/Sek. |
| **Beschreibung** | **Artikelnummer** |
| NSA 2600 (nur Firewall) | 01-SSC-3860 |
| NSA 2600 TotalSecure Advanced (1 Jahr) | 01-SSC-1712 |

## Network Security Appliance NSA 2650

Die NSA 2650 bietet mittelgroßen Organisationen und verteilten Unternehmen einen ultraschnellen Bedrohungsschutz für Tausende verschlüsselter Verbindungen und eine noch größere Anzahl von unverschlüsselten Verbindungen.

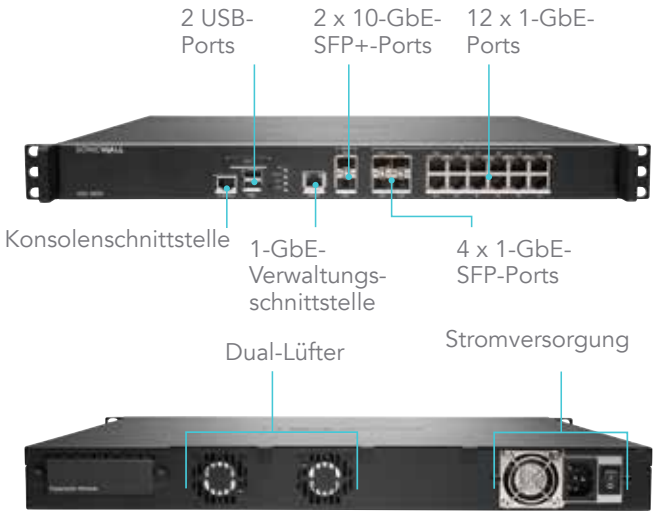



| Firewall | NSA 2650 |
|---|---|
| Firewall-Durchsatz | 3,0 GBit/s |
| IPS-Durchsatz | 1,4 GBit/s |
| Anti-Malware-Durchsatz | 600 MBit/s |
| Full-DPI-Durchsatz | 600 MBit/s |
| IMIX-Durchsatz | 700 MBit/s |
| Max. Anzahl von DPI-Verbindungen | 500.000 |
| Neue Verbindungen/Sekunde | 15.000/Sek. |
| **Beschreibung** | **Artikelnummer** |
| NSA 2650 (nur Firewall) | 01-SSC-1936 |
| NSA 2650 TotalSecure Advanced (1 Jahr) | 01-SSC-1988 |

## Network Security Appliance 3600

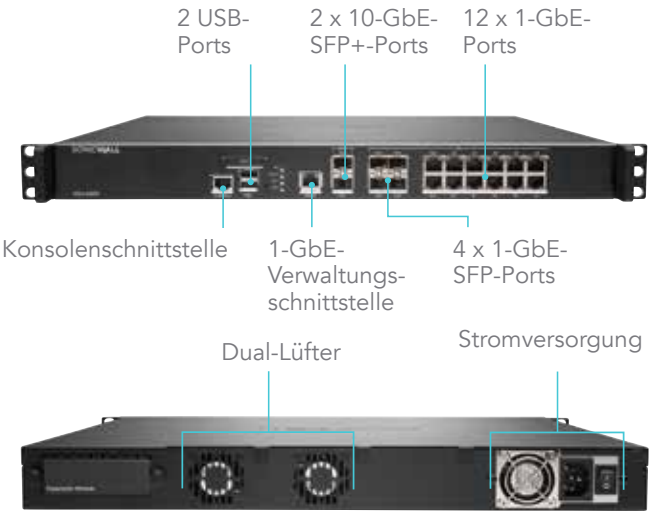
Die SonicWall NSA 3600 ist ideal für Zweigniederlassungen und kleine bis mittlere Unternehmen geeignet, die ihre Durchsatzkapazität und Performance optimieren möchten.




| Firewall | NSA 3600 |
|---|---|
| Firewall-Durchsatz | 3,4 GBit/s |
| IPS-Durchsatz | 1,1 GBit/s |
| Anti-Malware-Durchsatz | 600 MBit/s |
| Full-DPI-Durchsatz | 500 MBit/s |
| IMIX-Durchsatz | 900 MBit/s |
| Max. Anzahl von DPI-Verbindungen | 375.000 |
| Neue Verbindungen/Sekunde | 20.000/Sek. |
| **Beschreibung** | **Artikelnummer** |
| Nur Firewall | 01-SSC-3850 |
| TotalSecure Advanced (1 Jahr) | 01-SSC-1713 |

## Network Security Appliance 4600

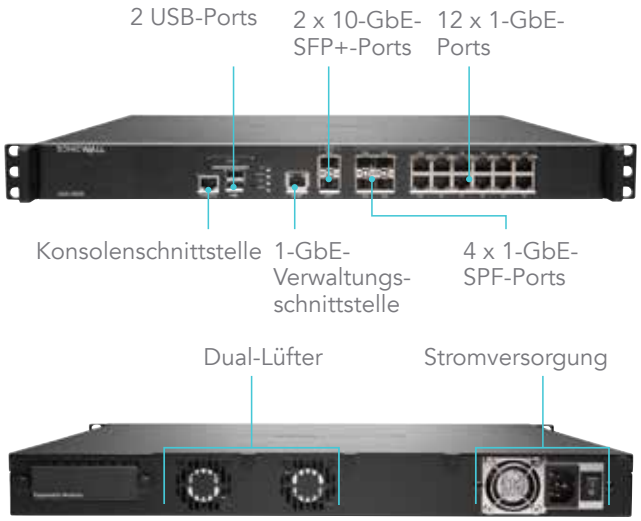
Die SonicWall NSA 4600 schützt wachstumsstarke mittlere Organisationen und Zweigniederlassungen mit Enterprise-Class-Features und kompromissloser Performance.




| Firewall | NSA 4600 |
|---|---|
| Firewall-Durchsatz | 6,0 GBit/s |
| IPS-Durchsatz | 2,0 GBit/s |
| Anti-Malware-Durchsatz | 1,1 GBit/s |
| Full-DPI-Durchsatz | 800 MBit/s |
| IMIX-Durchsatz | 1,6 GBit/s |
| Max. Anzahl von DPI-Verbindungen | 1.000.000 |
| Neue Verbindungen/Sekunde | 40.000/Sek. |
| **Beschreibung** | **Artikelnummer** |
| Nur Firewall | 01-SSC-3840 |
| TotalSecure Advanced (1 Jahr) | 01-SSC-1714 |

## Network Security Appliance 5600

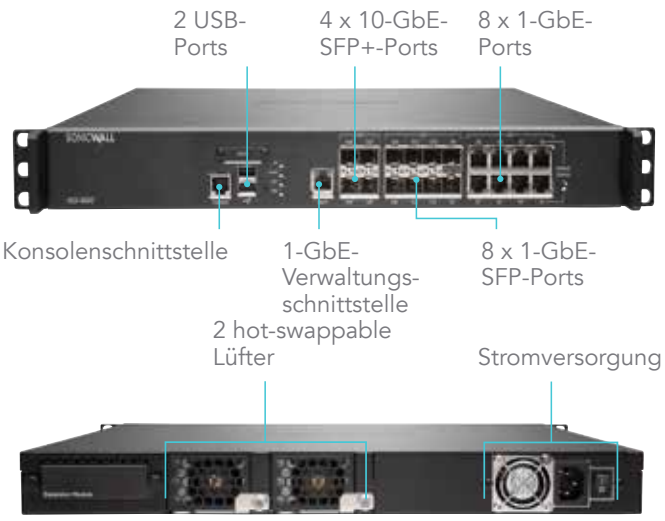
Die SonicWall NSA 5600 eignet sich ideal für verteilte Unternehmen sowie für deren Zweigniederlassungen und Netzwerkumgebungen, die eine erhebliche Durchsatzkapazität benötigen.




| 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 | 1.000.000 |
| Neue Verbindungen/Sekunde | 60.000/Sek. |
| **Beschreibung** | **Artikelnummer** |
| NSA 5600 (nur Firewall) | 01-SSC-3830 |
| NSA 5600 TotalSecure Advanced (1 Jahr) | 01-SSC-1715 |

## Network Security Appliance 6600

Die SonicWall NSA 6600 ist für größere verteilte Netzwerkumgebungen sowie für Unternehmenszentralen ausgelegt, die eine hohe Durchsatzkapazität und Performance benötigen.



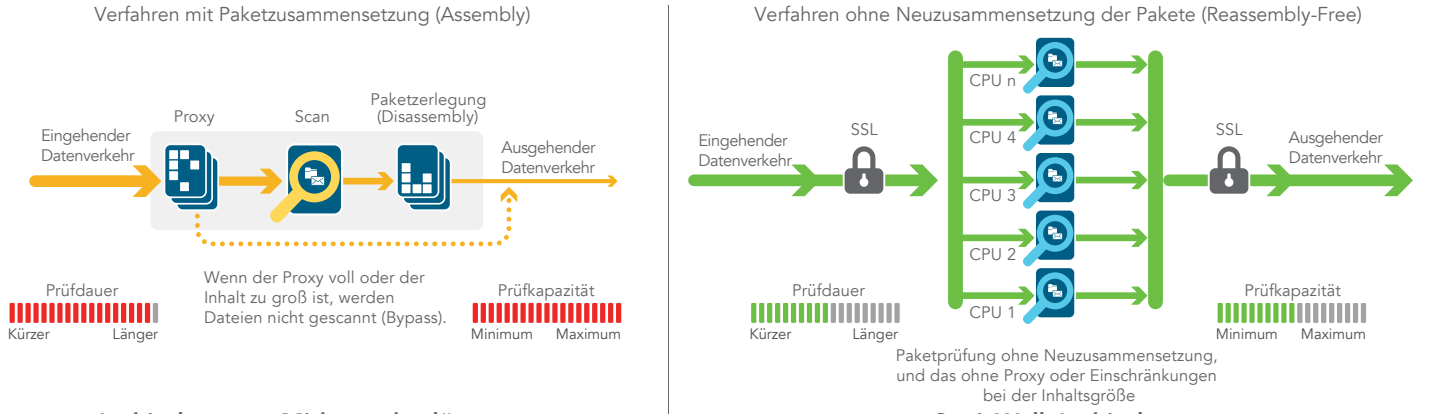

| Firewall | NSA 6600 |
|---|---|
| Firewall-Durchsatz | 12,0 GBit/s |
| IPS-Durchsatz | 4,5 GBit/s |
| Anti-Malware-Durchsatz | 3,0 GBit/s |
| Full-DPI-Durchsatz | 3,0 GBit/s |
| IMIX-Durchsatz | 3,5 GBit/s |
| Max. Anzahl von DPI-Verbindungen | 1.000.000 |
| Neue Verbindungen/Sekunde | 90.000/Sek. |
| **Beschreibung** | **Artikelnummer** |
| NSA 6600 (nur Firewall) | 01-SSC-3820 |
| NSA 6600 TotalSecure Advanced (1 Jahr) | 01-SSC-1716 |

## Reassembly-Free Deep Packet Inspection-Engine

Bei der SonicWall Reassembly-Free Deep Packet Inspection (RFDPI)-Engine handelt es sich um ein Single-Pass-Prüfsystem mit niedriger Latenz, das streambasierte bidirektionale Verkehrsanalysen in Hochgeschwindigkeit durchführt, um Eindringversuche und Malware-Downloads zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy. Die proprietäre 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.

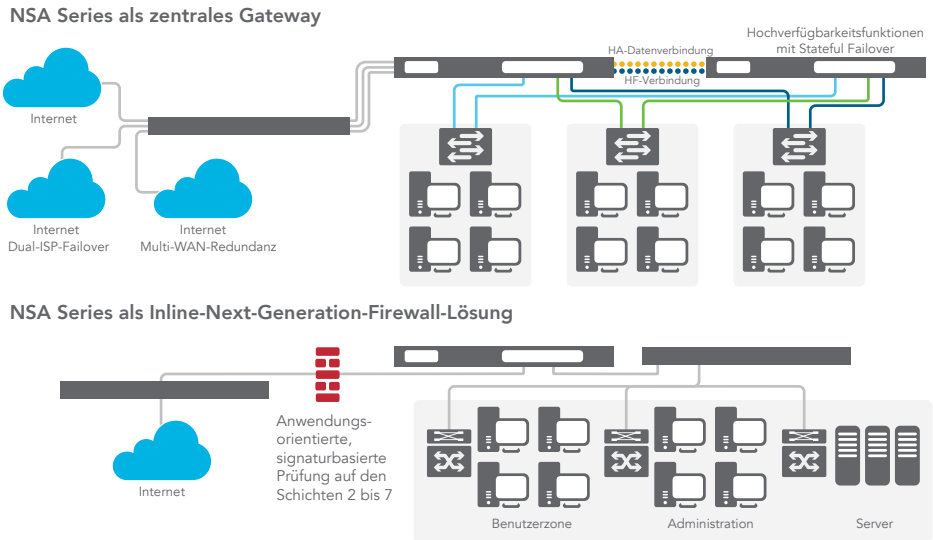
Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall aktualisiert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





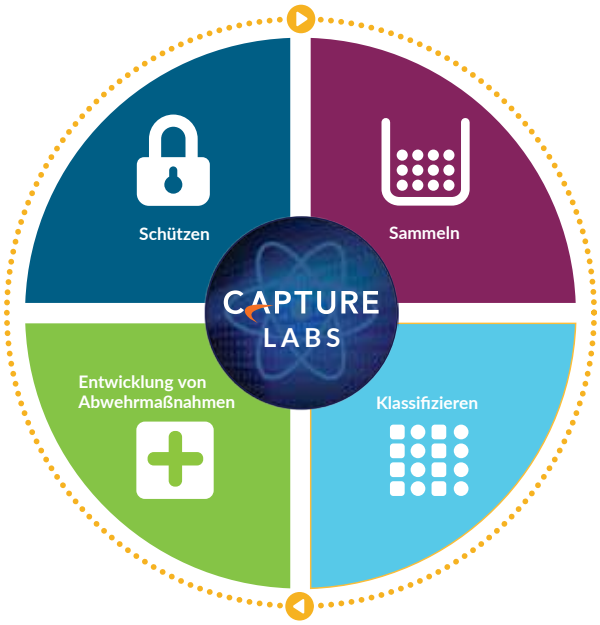

SONICWALL®

## Capture Labs

Das interne SonicWall Capture Labs Threat Research-Team entwickelt Abwehrmaßnahmen, die umgehend in den Kunden-Firewalls implementiert werden, um einen aktuellen Schutz zu gewährleisten. Das Team sammelt Daten zu potenziellen Bedrohungen aus mehreren Quellen, darunter aus unserem prämierten Netzwerk-Sandboxing-Service Capture Advanced Threat Protection sowie aus über 1 Million SonicWall-Sensoren, die rund um den Globus den Verkehr auf neue Bedrohungen prüfen. Die Daten werden mithilfe von Machine-Learning-Funktionen auf Basis der Deep-Learning-Algorithmen von SonicWall analysiert. Dabei wird die DNA aus dem Code extrahiert und auf Übereinstimmung mit bereits bekannten Formen bösartigen Codes geprüft.

Kunden mit Next-Generation-Firewalls von SonicWall erhalten rund um die Uhr Updates zu den aktuellsten Bedrohungen. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige 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 zu SonicWall CloudAV. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um über 20 Millionen Signaturen erweitert. Die Firewall greift über ein proprietäres, schlankes Protokoll auf die CloudAV-Datenbank zu, um die Prüfmöglichkeiten auf der Appliance zu erweitern. Mit Capture Advanced Threat Protection, einer Cloud-basierten Multi-Engine-Sandbox, können Organisationen verdächtige Dateien und verdächtigen Code in einer isolierten Umgebung untersuchen, um raffinierte Bedrohungen wie Zero-Day-Angriffe zu stoppen.

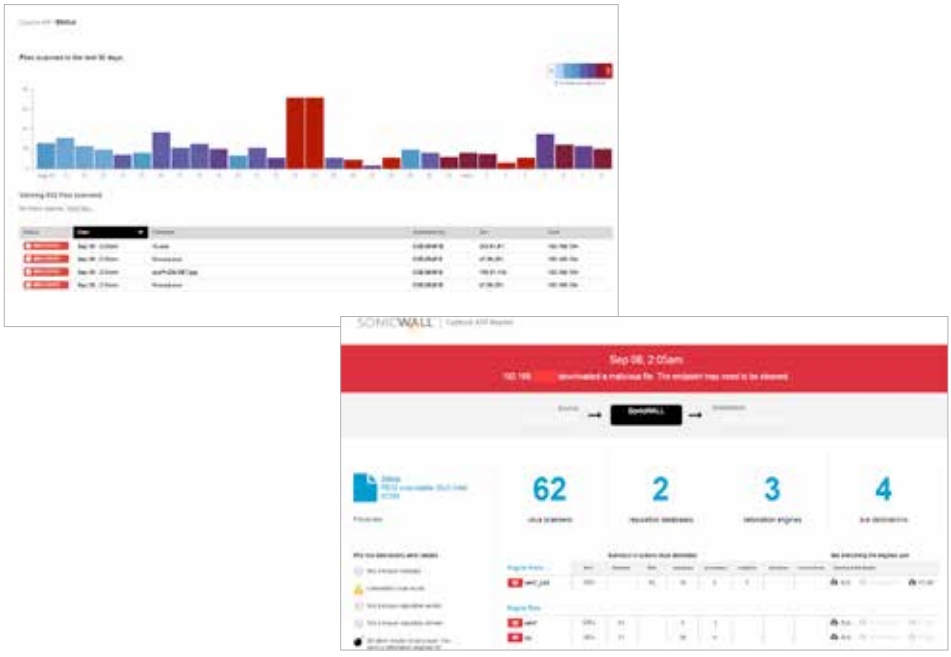



## Schutz vor raffinierten Bedrohungen

Beim SonicWall Capture Advanced Threat Protection-Service handelt es sich um eine Cloud-basierte Multi-Engine-Sandbox, die den Firewall-Bedrohungsschutz erweitert, um Zero-Day-Bedrohungen zu erkennen und abzuwehren. Verdächtige Dateien werden zur Analyse in die Cloud übertragen und können am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist. Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus und analysiert dessen Verhalten. Wird eine Datei als bösartig identifiziert, erstellt der Capture-Service umgehend einen Hash. Später erhalten die Firewalls eine Signatur, um Folgeangriffe zu verhindern.

Der Service unterstützt ein breites Spektrum an Betriebssystemen und analysiert zahlreiche Dateitypen, einschließlich ausführbare Programme, DLL, PDFs, MS-Office-Dokumente, Archive, JAR und APK.

Capture bietet ein übersichtliches Bedrohungsanalyse-Dashboard und Berichte mit detaillierten Analyseergebnissen für die an den Service weitergeleiteten Dateien, z. B. Quelle, Ziel und eine Zusammenfassung mit genauen Angaben zu den eingeleiteten Anti-Malware-Maßnahmen.



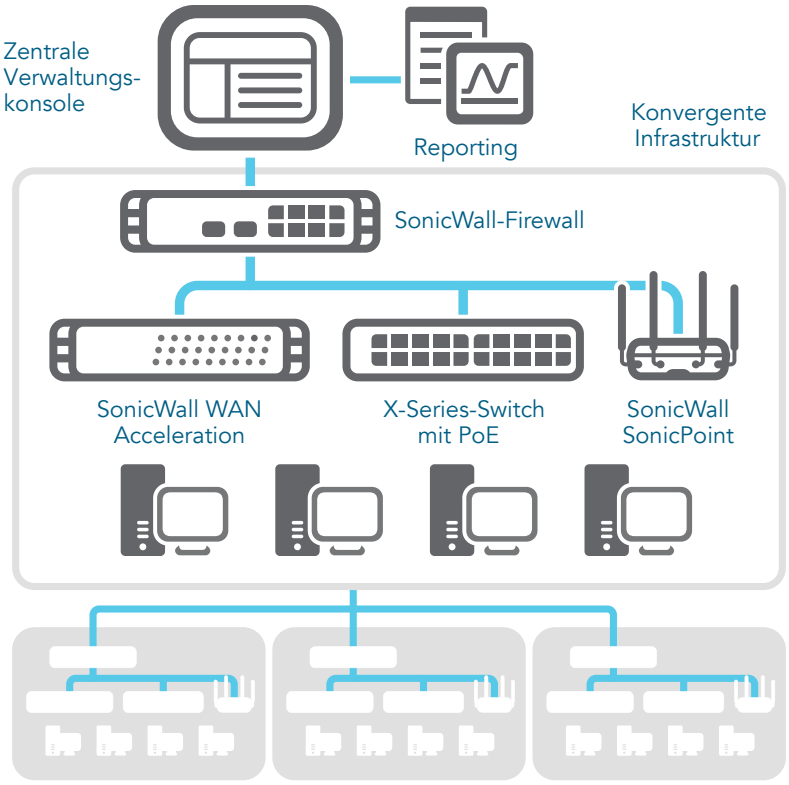
## Globales Management und Reporting

In stark reglementierten Organisationen, die eine komplett aufeinander abgestimmte Sicherheits-, Governance-, Compliance- und Risikomanagement-Strategie benötigen, bietet das SonicWall Global Management System (GMS®) Administratoren eine einheitliche, sichere und erweiterbare Plattform, um SonicWall-Firewalls, Wireless Access Points und Switches der Dell X-Series über einen korrelierten und prüfbaren Workstream-Prozess zu verwalten. Mit GMS können Unternehmen die Verwaltung ihrer Sicherheitsappliances unkompliziert konsolidieren, Administration und Fehlerbehebung vereinfachen und alle betrieblichen Aspekte der Sicherheitsinfrastruktur steuern. Unter anderem bietet die Plattform zentralisierte Richtlinienverwaltung und -durchsetzung, Echtzeit-Ereignisüberwachung, Benutzeraktivitäten, Anwendungsidentifizierung, Datenstromanalyse und -forensik sowie Compliance- und Audit-Reporting etc. Dank einer Funktion zur Workflow-Automatisierung können Unternehmen mit GMS zudem auch alle Änderungen an ihren Firewalls effektiv verwalten. Mithilfe der GMS-Workflow-Automatisierung können alle Unternehmen geeignete Firewall-Regeln flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit Compliance-Vorgaben implementieren. Dank GMS lässt sich die Netzwerksicherheit einheitlich auf Geschäftsprozesse und Servicelevel abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, statt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt. GMS ist als Software-, Cloud- und Virtual-Appliance-Option verfügbar.

## SonicWall GMS: Zuverlässige Einhaltung von Compliance-Vorgaben

### Vorteile

- Zentrale Verwaltung
- Fehlerfreie Regelverwaltung
- Strenge Zugriffskontrolle
- Umfassende Audit-Trails
- PCI-, HIPAA-, SOX-Berichtsvorlagen
- Niedrigere Betriebskosten




Skalierbarkeit durch Porterweiterung

## 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. |

| Firewall und Networking | |
|---|---|
| Funktion | Beschreibung |
| API gegen Bedrohungen | Durch diese API erhält die Firewall sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Diese nutzt sie, um raffinierte Bedrohungen wie Zero-Day-Angriffe, Insider-Bedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv zu bekämpfen. |
| Stateful Packet Inspection | Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die Firewall-Zugriffsregeln erfüllt werden. |
| Hochverfügbarkeit/Clustering | Die NSA Series unterstützt die Hochverfügbarkeitsmodi Active/Passive (A/P) mit State-Synchronisierung, Active/Active-(A/A)-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. |
| 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. |
| IPv6-Unterstützung | Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) hat gerade erst begonnen. Mit SonicOS unterstützt die Hardware Filtering- und Wire-Implementierungsmodi. |
| Flexible Implementierungsoptionen | Die NSA Series lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren. |
| WAN-Lastverteilung | Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden. Regelbasiertes Routing sorgt für das Erstellen von protokollbasierten Routen für die Umleitung des Datenverkehrs zu einer bevorzugten WAN-Verbindung mit Failback-Möglichkeit auf ein sekundäres WAN bei einem Stromausfall. |
| Verbesserte QoS (Quality of Service) | 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. |
| Verwaltung einzelner und hintereinandergeschalteter Switches der Dell X-Series | Verwaltung der Sicherheitseinstellungen zusätzlicher Ports, einschließlich Portshield, HA, POE und POE+ über eine einzige Konsole mithilfe des Firewall-Management-Dashboards für Dells X-Series-Network-Switch. |
| Biometrische Authentifizierung | Unterstützung von Authentifizierungsmethoden für Mobilgeräte, bei denen eine Duplizierung oder Weitergabe nicht ohne Weiteres möglich ist, wie z. B. bei der Fingerabdruckerkennung. So lässt sich die Identität des Nutzers auf sichere Weise prüfen, bevor ein Zugriff auf das Netzwerk gewährt wird. |
| Offene Authentifizierung und Social Login | Erlaubt Gastbenutzern das Einloggen mit ihren Anmeldedaten aus sozialen Netzwerken wie Facebook, Twitter oder Google+ und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung. |

| Management und Reporting | |
|---|---|
| Funktion | Beschreibung |
| Global Management System (GMS) | 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 Befehlszeilenschnittstelle und bietet 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 SonicWall Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben. |

| Virtual Private Networking (VPN) | |
|---|---|
| Funktion | Beschreibung |
| Auto-Provisioning für VPNs | Durch Automatisierung der Site-to-Site-VPN-Gateway-Erstausstattung zwischen den SonicWall-Firewalls ist die Implementierung komplexer verteilter Firewalls ein Kinderspiel. Funktionen für Sicherheit und Konnektivität werden umgehend und automatisch ausgeführt. |

| | |
|---|---|
| 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- oder 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[1]/Terminaldienste[1] 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. Möglichkeit, individuelle Länder- und Botnet-Listen zu erstellen, um einen nicht korrekten Landes- oder Botnet-Tag in Verbindung mit einer IP-Adresse zu überschreiben. Eliminiert unerwünschtes Filtering von IP-Adressen aufgrund einer Fehlklassifikation. |
| DPI-Filterung nach regulären Ausdrücken | Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern. Es besteht die Möglichkeit, individuelle Länder- und Botnet-Listen zu erstellen, um einen nicht korrekten Landes- oder Botnet-Tag in Verbindung mit einer IP-Adresse zu überschreiben. |

## Breach Prevention-Aboservices

| **Capture Advanced Threat Protection** | |
|---|---|
| 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. |
| 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. |
| Analyse unterschiedlichster Dateitypen und -größen | Der Service unterstützt die Analyse unterschiedlichster Dateitypen, darunter ausführbare Programme (PE), DLL, PDFs, MS-Office-Dokumente, Archive, JAR und APK sowie unterschiedliche Betriebssysteme wie Windows, Android, Mac OS X 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 SonicWall Capture-Abos aufgespielt und in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt. |

| **Schutz vor verschlüsselten Bedrohungen** | |
|---|---|
| Funktion | Beschreibung |
| SSL-/TLS-Entschlüsselung und -Prüfung | SSL-/TLS-verschlüsselter Datenverkehr wird in Echtzeit und ohne Umweg über einen Proxy entschlüsselt und auf Malware, Eindringversuche und Datenlecks überprüft. Gleichzeitig werden Richtlinien für Anwendungs-, URL- und Inhaltskontrolle angewendet, um das Netzwerk gegen versteckte Bedrohungen in SSL-verschlüsseltem Datenverkehr abzusichern. Dieser Service ist bei allen NSA-Modellen in den Sicherheits-Abonnements inbegriffen. |
| SSH-Prüfung | Durch die Deep Packet Inspection-Prüfung von SSH-verschlüsseltem Verkehr (DPI-SSH) werden Daten, die über SSH-Tunnel übertragen werden, entschlüsselt und durchleuchtet, um Angriffe zu verhindern, die sich SSH zunutze machen. |
| **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. |
| 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 Schichten 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen. |
| **Bedrohungsschutz** | |
| 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-Malware-Schutz | Eine kontinuierlich aktualisierte Datenbank mit über 20 Millionen Bedrohungssignaturen auf den SonicWall-Cloud-Servern ergänzt die lokalen Signaturendatenbanken und sorgt dafür, dass die RFDPI-Engine eine größtmögliche Anzahl an Bedrohungen abdeckt. |
| Sicherheitsupdates rund um die Uhr | 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. |
| 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 und Anwendungskontrolle | |
|---|---|
| Funktion | Beschreibung |
| Anwendungskontrolle | Die RFDPI-Engine nutzt eine kontinuierlich erweiterte Datenbank mit Tausenden von Anwendungssignaturen, um Anwendungen oder einzelne Anwendungsfunktionen zu identifizieren und zu kontrollieren. Dadurch lassen sich Netzwerksicherheit und -produktivität erhöhen. |
| Identifizierung benutzerdefinierter Anwendungen | Die Lösung erstellt 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. |
| 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. |
| Enforced Content Filtering Client | Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte 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. |
| 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 Firewall ist die erste Verteidigungsstufe am Netzwerkrand. Zusammen mit dem Endpunktschutz verhindert sie das Eindringen von Viren über Laptops, USB-Sticks und andere ungeschützte Systeme. |
| Option für 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. |
| Option für 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. |

## Die SonicOS-Funktionen im Überblick

### Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- API gegen Bedrohungen

### SSL-/SSH-Entschlüsselung und -Prüfung[1]

- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL Control

### Capture Advanced Threat Protection[1]

- 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

### Intrusion-Prevention[1]

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- Durchsetzung von GeoIP-Regeln
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

### Malware-Schutz[1]

- Streambasierte Malware-Scans
- Virenschutz am Gateway
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloud-basierte Malware-Datenbank

### Anwendungsidentifizierung[1]

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

### Filterung von Webinhalten[1]

- URL-Filtering
- Anti-Proxy-Technologie
- Blockieren mithilfe von Schlüsselwörtern
- Bandbreitenverwaltung anhand von CFS-Ratingkategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

### VPN

- Auto-Provisioning für VPNs
- 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, BGP)

### Networking

- PortShield
- Jumbo-Frames
- IPv6
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- RSTP (Rapid Spanning Tree Protocol)
- Portspiegelung
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation (statisch und dynamisch)
- Port-Redundanz
- Hochverfügbarkeitsmodus A/P mit State-Sync
- A/A-Clustering
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge-, Wire-/Virtual-Wire-, Tap-Modus
- 3G-/4G-WAN-Failover
- Asymmetrisches Routing
- Common Access Card(CAC)-Unterstützung

### Wireless

- MU-MIMO
- Grundrissansicht
- Topologieansicht
- Band-Steering
- Beamforming
- AirTime-Fairness
- MiFi-Extender
- Zeitlich limitierter Zugriff durch Gastnutzer

### VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- H.323-Gatekeeper- und SIP-Proxy-Support

### Verwaltung und Überwachung

- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting
- Logging
- NetFlow-/IPFIX-Export
- Cloud-basiertes Konfigurations-Back-up
- BlueCoat Security Analytics Platform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- Dell X-Series-Switch-Verwaltung einschließlich hintereinandergeschalteter Switches

[1]*Erfordert zusätzliches Abo.*



SONICWALL

## NSA Series – Systemdaten

| Firewall allgemein | NSA 2600 | NSA 2650 | NSA 3600 | NSA 4600 | NSA 5600 | NSA 6600 |
|---|---|---|---|---|---|---|
| Betriebssystem | SonicOS 6.5 | | | | | |
| Security-Prozessor-Cores | 4 | 4 | 6 | 8 | 10 | 24 |
| Schnittstellen | 8 x 1-GbE, 1-GbE-Verwaltungs-schnittstelle, 1 Konsole | 4 x 2,5-GbE-SFP, 4 x 2,5-GbE, 12 x 1-GbE, 1-GbE-Verwaltungs-schnittstelle, 1 Konsole | 2 x 10-GbE-SFP+, 4 x 1-GbE-SFP, 12 x 1-GbE, 1-GbE-Verwaltungs-schnittstelle, 1 Konsole | 2 x 10-GbE-SFP+, 4 x 1-GbE-SFP, 12 x 1-GbE, 1-GbE-Verwaltungs-schnittstelle, 1 Konsole | 2 x 10-GbE-SFP+, 4 x 1-GbE-SFP, 12 x 1-GbE, 1-GbE-Verwaltungs-schnittstelle, 1 Konsole | 4 x 10-GbE-SFP+, 8 x 1-GbE-SFP, 8 x 1-GbE, 1-GbE-Verwaltungs-schnittstelle, 1 Konsole |
| Erweiterung | 1 Erweiterungs-steckplatz (Rückseite)*, SD-Karte* | 1 Erweiterungs-steckplatz (Rückseite)*, 16-GB-Speichermodul | 1 Erweiterungssteckplatz (Rückseite)*, SD-Karte* | | | |
| Verwaltung | CLI, SSH, GUI, GMS | | | | | |
| SSO-Benutzer | 30.000 | 40.000 | 40.000 | 50.000 | 60.000 | 70.000 |
| Maximal unterstützte Anzahl von Access Points | 32 | 48 | 48 | 64 | 96 | 128 |
| Logging | Analyzer, lokale Logdatei, Syslog | | | | | |
| **Firewall-/VPN-Performance** | **NSA 2600** | **NSA 2650** | **NSA 3600** | **NSA 4600** | **NSA 5600** | **NSA 6600** |
| Firewall-Inspection-Durchsatz[1] | 1,9 GBit/s | 3,0 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 | 600 MBit/s | 500 MBit/s | 800 MBit/s | 1,6 GBit/s | 3,0 GBit/s |
| Application-Inspection-Durchsatz[2] | 700 MBit/s | 1,4 GBit/s | 1,1 GBit/s | 2,0 GBit/s | 3,0 GBit/s | 4,5 GBit/s |
| IPS-Durchsatz[2] | 700 MBit/s | 1,4 GBit/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 | 600 MBit/s | 1,1 GBit/s | 1,7 GBit/s | 3,0 GBit/s |
| IMIX-Durchsatz | 600 MBit/s | 700 MBit/s | 900 MBit/s | 1,6 GBit/s | 2,4 GBit/s | 3,5 GBit/s |
| TLS/SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2] | 200 MBit/s | 300 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 | 1,5 GBit/s | 3,0 GBit/s | 4,5 GBit/s | 5,0 GBit/s |
| Verbindungen pro Sekunde | 15.000/Sek. | 15.000/Sek. | 20.000/Sek. | 40.000/Sek. | 60.000/Sek. | 90.000/Sek. |
| Maximale Anzahl von Verbindungen (SPI) | 500.000 | 1.000.000 | 750.000 | 1.000.000 | 1.500.000 | 1.500.000 |
| Maximale Anzahl von Verbindungen (DPI)[4] | 250.000 | 500.000 | 375.000 | 500.000 | 1.000.000 | 1.000.000 |
| Standardmäßige/Maximale Anzahl von Verbindungen (DPI-SSL)[4] | 1.000/1.000 | 12.000/13.500 | 2.000/2.750 | 3.000/4.500 | 4.000/8.500 | 6.000/10.500 |
| **VPN** | **NSA 2600** | **NSA 2650** | **NSA 3600** | **NSA 4600** | **NSA 5600** | **NSA 6600** |
| Site-to-Site-Tunnel | 250 | 1.000 | 1.000 | 3.000 | 4.000 | 6.000 |
| IPSec-VPN-Clients (max.) | 10 (250) | 50 (1.000) | 50 (1.000) | 500 (3.000) | 2.000 (4.000) | 2.000 (6.000) |
| SSL-VPN-NetExtender-Clients (max.) | 2 (250) | 2 (350) | 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, 14v | | | | | |
| Routenbasiertes VPN | RIP, OSPF | | | | | |
| **Networking** | **NSA 2600** | **NSA 2650** | **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 | 256 | 400 | 500 |
| Routing-Protokolle | BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing | | | | | |
| QoS | Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p | | | | | |
| Authentifizierung | LDAP (mehrere Domains), XAUTH/RADIUS, SSO, 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 | | | | | |
| Hochverfügbarkeit | Active/Passive mit State Sync | | Active/Passive mit State Sync<br>Active/Active-Clustering | | Active/Passive mit State Sync,<br>Active/Active DPI mit State Sync<br>Active/Active-Clustering | |
| **Hardware** | **NSA 2600** | **NSA 2650** | **NSA 3600** | **NSA 4600** | **NSA 5600** | **NSA 6600** |
| Stromversorgung | Einfach, fest, 200 W | 2, redundant, 120 W (eine im Lieferumfang enthalten) | 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 | 74,3 | 86,7 | 90,9 | 113,1 |
| MTBF bei 25 °C in Stunden | 176.540 | 146.789 | 146.789 | 139.783 | 134.900 | 116.477 |
| MTBF bei 25 °C in Jahren | 20,15 | 16,76 | 16,76 | 15,96 | 15,40 | 13,30 |
| Formfaktor | rackfähig (1 HE) | | | | | |
| Abmessungen | 4,5 x 48,5 x 43 cm | | | | | |
| Gewicht | 4,6 kg | 6,15 kg | 6,15 kg | | | 6,77 kg |
| WEEE-Gewicht | 5,0 kg | 6,46 kg | 6,46 kg | | | 8,97 kg |
| Versandgewicht | 6,5 kg | 9,43 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 (eingeschaltet / bei Lagerung) | 0°-40° C / -40°-70° C) | | | | | |
| Luftfeuchtigkeit | 10-90%, nicht kondensierend | | | | | |

*[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] Der Full-DPI-/GatewayAV-/Anti-Spyware-/IPS-Durchsatz wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia Testtools nach Branchenstandard gemessen. Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren.*

*[3] Der VPN-Durchsatz wurde gemäß RFC 2544 gemessen, unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.*

*[4] Für jede 125.000 DPI-Verbindungen, die reduziert werden, steigt die Anzahl verfügbarer DPI-SSL-Verbindungen um 750.*

** Für künftige Anwendung. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.*



SONICWALL®

## Bestellinformationen zur NSA Series

| NSA 2650 | Artikelnummer |
|---|---|
| NSA 2650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-1988 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NSA 2650 (1 Jahr) | 01-SSC-1783 |
| Capture Advanced Threat Protection für NSA 2650 (1 Jahr) | 01-SSC-1935 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NSA 2650 (1 Jahr) | 01-SSC-1976 |
| Silver 24/7-Support für NSA 2650 (1 Jahr) | 01-SSC-1541 |
| Content Filtering Premium Service für NSA 2650 (1 Jahr) | 01-SSC-1970 |
| Enforced Client Anti-Virus & Anti-Spyware | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NSA 2650 (1 Jahr) | 01-SSC-2001 |
| **NSA 3600** | **Artikelnummer** |
| NSA 3600 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-1713 |
| 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 Service für NSA 3600 (1 Jahr) | 01-SSC-4441 |
| Enforced Client Anti-Virus & Anti-Spyware | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NSA 3600 (1 Jahr) | 01-SSC-4447 |
| **NSA 4600** | **Artikelnummer** |
| NSA 4600 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-1714 |
| 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 Service für NSA 4600 (1 Jahr) | 01-SSC-4417 |
| Enforced Client Anti-Virus & Anti-Spyware | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NSA 4600 (1 Jahr) | 01-SSC-4423 |
| **NSA 5600** | **Artikelnummer** |
| NSA 5600 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-1715 |
| 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 Service für NSA 5600 (1 Jahr) | 01-SSC-4246 |
| Enforced Client Anti-Virus & Anti-Spyware | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NSA 5600 (1 Jahr) | 01-SSC-4252 |
| **NSA 6600** | **Artikelnummer** |
| NSA 6600 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-1716 |
| 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 Service für NSA 6600 (1 Jahr) | 01-SSC-4222 |
| Enforced Client Anti-Virus & Anti-Spyware | 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 Ihren lokalen SonicWall-Ansprechpartner.*

## Modellnummern (Zulassung):

NSA 2600–1RK29-0A9

NSA 2650-1RK38-0C8

NSA 3600–1RK26-0A2

NSA 4600–1RK26-0A3

NSA 5600–1RK26-0A4

NSA 6600–1RK27-0A5

## Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com



Datasheet-NetworkSecurityAppliance-US-VG-MKTG453

SONICWALL®