# SonicWall Network Security Appliance (NSa) Series

Branchenweit bewährte Effektivität und Leistung für mittelgroße Netzwerke, geografisch weit verteilte Großunternehmen und Rechenzentren

Die SonicWall Network Security Appliance (NS*a*) Series bietet größeren Organisationen – angefangen bei Firmen mit mittelgroßen Netzwerken bis hin zu verteilten Unternehmen und Rechenzentren – zuverlässigen Schutz vor raffinierten Bedrohungen in Form einer hoch entwickelten Sicherheitsplattform. Die NS*a* Series nutzt innovative Deep-Learning-Technologien in der SonicWall Capture Cloud Plattform und bietet Organisationen genau die automatisierte Echtzeiterkennung und -prävention von Sicherheitslücken, die sie brauchen.

## Hochmoderner, extrem leistungsstarker Bedrohungsschutz.

Heutige Netzwerkbedrohungen sind extrem schwer zu fassen und lassen sich mithilfe traditioneller Methoden kaum noch identifizieren. Um hoch entwickelten Angriffen die Stirn zu bieten, ist ein moderner Ansatz gefragt, der in großem Umfang Sicherheitsdaten in der Cloud nutzt. Ohne diese Cloud-Daten sind Gateway-Sicherheitslösungen den komplexen Bedrohungen unserer Tage einfach nicht gewachsen. Die Next-Generation-Firewalls der NS*a* Series arbeiten mit zwei hoch entwickelten Sicherheitstechnologien, die einen erstklassigen Bedrohungsschutz bieten und Cyberkriminellen einen Schritt voraus sind. Optimiert wird unser Multi-Engine-Service Capture Advanced Threat Protection (ATP) durch unsere zum Patent angemeldete Real-Time Deep Memory Inspection (RTDMI™)-Technologie. Die RTDMI-Engine ist durch eine direkte Prüfung des Speichers in der Lage, massive Zero-Day-Bedrohungen sowie unbekannte Malware proaktiv aufzudecken und abzuwehren. Aufgrund der Echtzeitarchitektur ist die SonicWall RTDMI-Technologie sehr präzise, reduziert falsche Positivmeldungen und kann komplexe Angriffe selbst dann entschärfen, wenn die am stärksten geschützten Bereiche des Schadcodes weniger als 100 Nanosekunden sichtbar sind. Gemeinsam mit der patentierten* Reassembly-Free Deep Packet Inspection (RFDPI)-Single-Pass-Engine von SonicWall lassen sich jedes einzelne Paket und jedes einzelne Byte durchleuchten. Dabei wird der ein- und ausgehende Datenverkehr direkt in der Firewall auf Bedrohungen geprüft. Die NS*a* Series nutzt neben integrierten Funktionen wie Intrusion-Prevention, Anti-Malware und Web-/URL-Filtering auch die SonicWall Capture Cloud Plattform, um selbst die gefährlichsten Bedrohungen am Gateway zu stoppen.

Darüber hinaus bieten die SonicWall-Firewalls einen umfassenden Schutz, weil sie unabhängig von Port oder Protokoll einevollständige Entschlüsselung und Prüfung von TLS-/SSL- und SSH-verschlüsselten Verbindungendurchführen. Alle Pakete (Header und Daten) werden gründlich geprüft. Dabei scannen die Firewalls den gesamten Verkehr auf Nichteinhaltung von Protokollen, Bedrohungen, Zero-Day-Angriffen, Eindringversuchen, sogar auf der Basis definierter Kriterien. Die Deep Packet Inspection-Engine erkennt und verhindert verborgene kryptografische Angriffe, und verhindert die Verbreitung von Bedrohungen, Command-and-Control(C&C)-Kommunikationen und das Herausschleusen von Daten. Eine umfassende Kontrolle wird durch Ein- und Ausschlussregeln ermöglicht, 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 IPS, Viren- und Spyware-Schutz sowie TLS-/SSL-Entschlüsselung/-Prüfung auf der Firewall aktiviert, leidet oft die Netzwerkleistung darunter – manchmal sogar extrem. Die NS*a*-Firewalls bieten jedoch eine Multicore-Hardware-Architektur mit Mikroprozessoren, die über spezielle Sicherheitsfunktionen

## Vorteile:

### Überragender Bedrohungsschutz und exzellente Performance

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

### Mehr Netzwerkkontrolle und Flexibilität

- Sicheres SD-WAN
- Leistungsstarkes SonicOS-Betriebssystem
- Application Intelligence and Control
- Netzwerksegmentierung mit VLANs
- Sichere Highspeed-WLAN-Verbindung

### Einfache Implementierung, Einrichtung und laufende Verwaltung

- Vollautomatische Implementierung mit Zero-Touch Deployment
- Cloud-basierte und lokale zentralisierte Verwaltung
- Skalierbare Firewalls
- Geringe Total Cost of Ownership

**U.S. Patente 7.310.815; 7.600.257; 7.738.380; 7.835.361; 7.991.723*

verfügen. Dieses einzigartige Design – in Kombination mit unseren RTDMI- und RFDPI-Engines – beseitigt die Leistungseinbußen, die oft mit anderen Firewalls einhergehen.

## Mehr Netzwerkkontrolle und Flexibilität

Herzstück der NS*a* 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.

Für verteilte Organisationen, die ein flexibleres Netzwerkdesign benötigen, ist die in SonicOS enthaltene SD-WAN Technologie die perfekte Ergänzung für NS*a*-Firewalls, die in einer Zentrale oder an Remote-Standorten bzw. Zweigniederlassungen implementiert sind. Im Gegensatz zu kostspieligeren veralteten Technologien wie MPLS und T1 können Organisationen mit SD-WAN erschwinglichere öffentliche Internetdienste wählen und gleichzeitig eine hohe Anwendungsverfügbarkeit und eine vorhersehbare Performance sicherstellen.

Jede NS*a*-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.

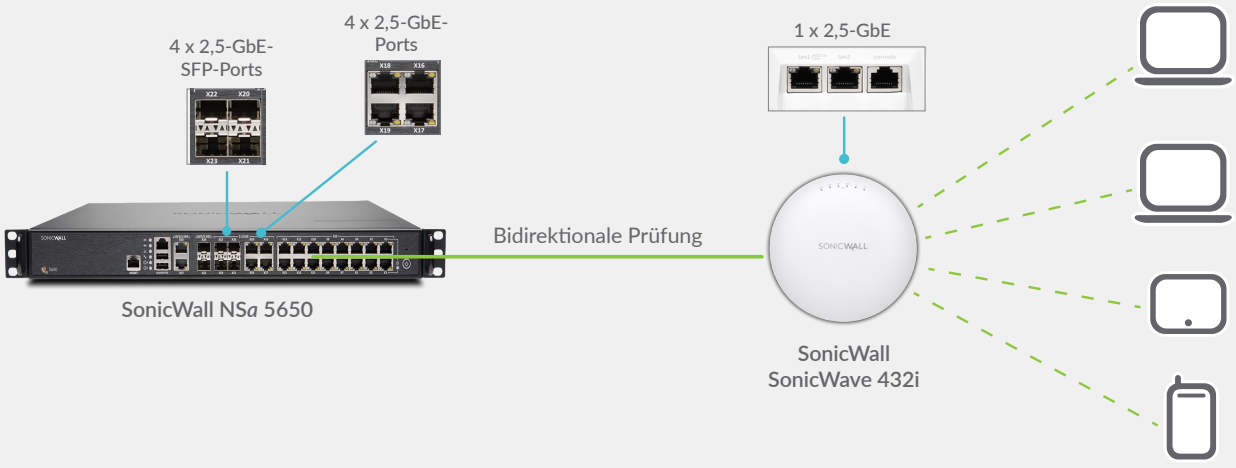
## Einfache Implementierung, Einrichtung und laufende Verwaltung

Wie alle SonicWall-Firewalls integriert auch die NS*a* 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 (WXA) Series. Beide werden von der NS*a* 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.

Verwaltung, Reporting, Lizenzierung und Analysen – allesamt cloudbasiert – erfolgen zentral über das SonicWall Capture Security Center. Eine wichtige Komponente des Capture Security Center ist das Zero-Touch Deployment für die vollautomatische Implementierung. Dieses Cloud-basierte Feature vereinfacht und beschleunigt die Implementierung und Bereitstellung von Firewalls in Zweigniederlassungen und an entfernten SonicWall Standorten. 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 den Next-Generation-Firewalls der NS*a* Series eine drahtlose Highspeed-Netzwerksicherheitslösung. Sowohl die NS*a*-Firewalls 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 Firewalls durchleuchten den gesamten ein- und ausgehenden drahtlosen Verkehr im Netzwerk mittels Deep Packet Inspection-Technologie und beseitigen anschließend gefährliche Bedrohungen wie Malware und Eindringversuche selbst bei SSL-/TLS-verschlüsselten Verbindungen. Weitere Sicherheits- und Kontrollfunktionen wie Content-Filtering, Anwendungserkennung und Kontrolle und Capture Advanced Threat Protection können als zusätzliche Sicherheitsschicht auf den drahtlosen Netzwerkverkehr angewendet werden.

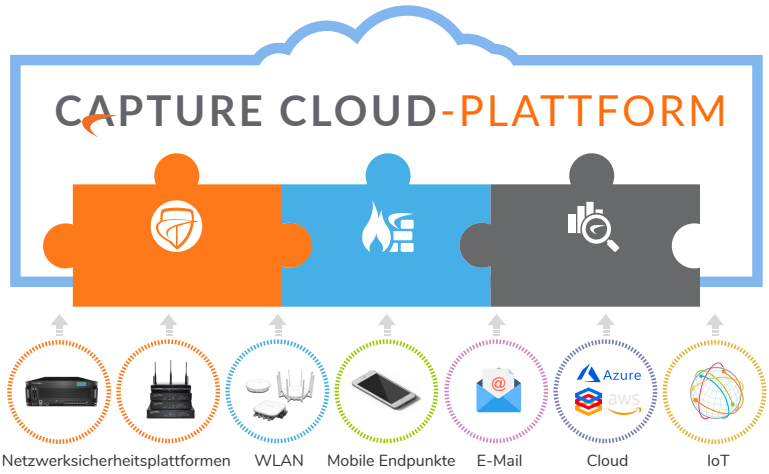


## Capture Cloud-Plattform

Die Capture Cloud-Plattform von SonicWall bietet kleinen wie großen Organisationen eine Cloud-basierte Lösung für Bedrohungsschutz und Netzwerkverwaltung sowie Reporting und Analysen. Die Plattform konsolidiert Bedrohungsinformationen aus mehreren Quellen, zum Beispiel aus unserem prämierten Multi-Engine-Netzwerk-Sandboxing-Service Capture Advanced Threat Protection sowie aus über 1 Million SonicWall Sensoren, die rund um den Globus verteilt sind.

Wird bei eingehenden Daten unbekannter bösartiger Code gefunden, entwickelt das dedizierte interne SonicWall Capture Labs Threat Research-Team Signaturen, die in der Datenbank der Capture Cloud-Plattform gespeichert und in die Kunden-Firewalls implementiert werden, um einen topaktuellen Schutz zu gewährleisten. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen. Die Signaturen auf der Appliance bieten Schutz vor einer großen Vielfalt an Attacken und decken Zehntausende verschiedener Bedrohungen ab. Zusätzlich zu den Abwehrmechanismen auf der Appliance haben die *a*-Firewalls auch einen kontinuierlichen Zugang zur Capture Cloud Plattform-Datenbank. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um mehrere Millionen Signaturen erweitert.

Neben dem effizienten Bedrohungsschutz bietet die Capture Cloud Plattform Administratoren die Möglichkeit, über eine zentrale Stelle spielend leicht Echtzeitberichte und historische Reports zur Netzwerkaktivität zu erstellen.

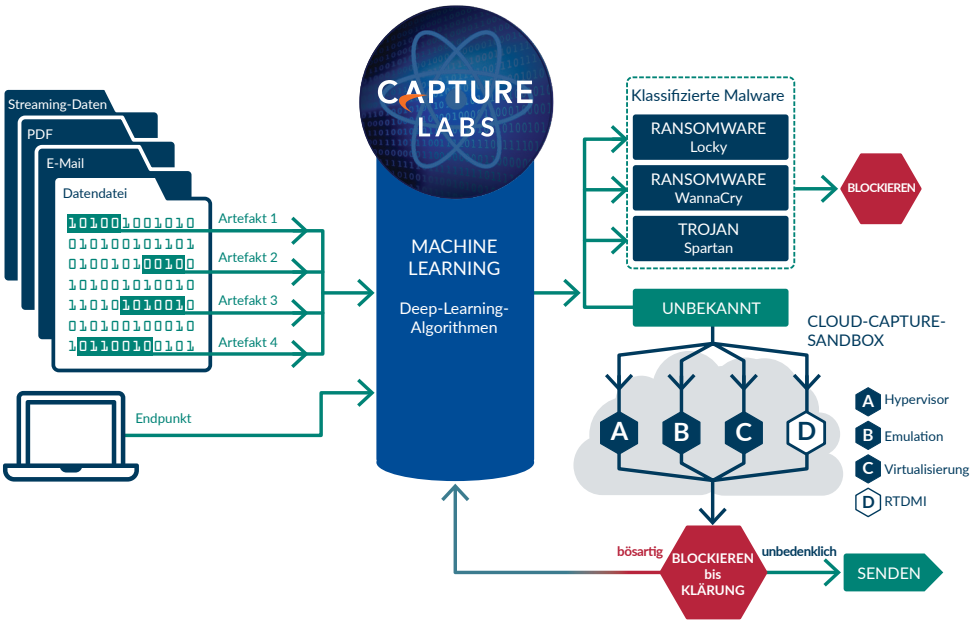



## Schutz vor komplexen Bedrohungen

Herzstück der automatisierten SonicWall Lösung zur Echtzeitprävention von Sicherheitslücken ist der SonicWall Capture Advanced Threat Protection-Service, eine Cloud-basierte Multi-Engine-Sandbox, die den Firewall-Bedrohungsschutz erweitert, um Zero-Day-Bedrohungen zu erkennen und abzuwehren. Verdächtige Dateien werden zur Analyse mittels Deep-Learning- Algorithmen in die Cloud übertragen und können am Gateway gehalten werden, bis der Sicherheitsstatus geklärt ist. Die Multi-Engine-Sandbox-Plattform mit Real-Time Deep Memory Inspection-Technologie, virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus und analysiert dessen Verhalten. Als bösartig identifizierte Dateien werden blockiert und Capture ATP erstellt umgehend einen Hash. Kurz darauf 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.

Für einen umfassenden Endpunktschutz kombiniert SonicWall Capture Client Antivirentechnologien der nächsten Generation mit der Cloud-basierten Multi-Engine-Sandbox von SonicWall.





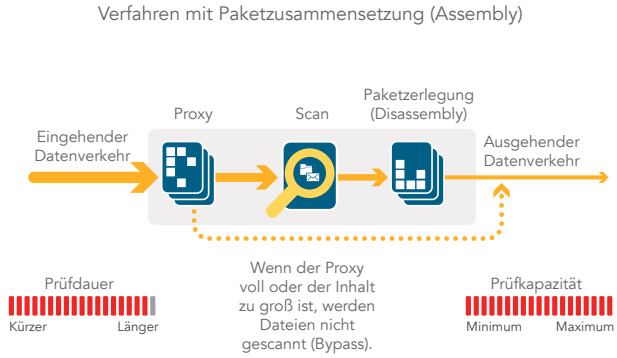

SONICWALL®

## Reassembly-Free Deep Packet Inspection-Engine

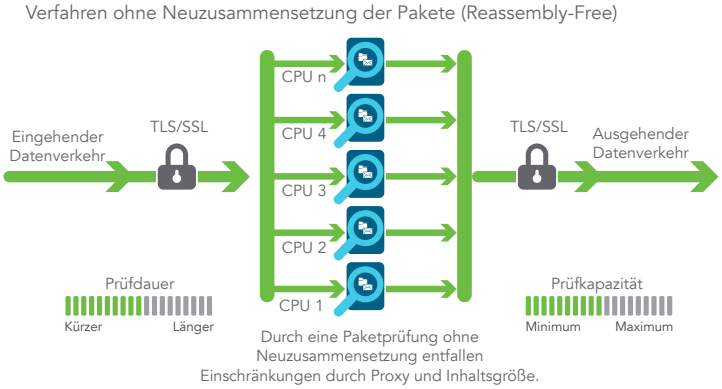
Bei der SonicWall Reassembly-Free Deep Packet Inspection (RFDPI)-Engine handelt es sich um ein Single-Pass-Prüfsystem mit niedriger Latenz, das streambasierte bidirektionale Verkehrsanalysen in Hochgeschwindigkeit durchführt, um Eindringversuche und Malware-Downloads zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig von Port oder Protokoll 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 komplexe 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. TLS-/ 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 und es werden entsprechende Logging- und Benachrichtigungs-Events erzeugt. Die Engine kann jedoch auch nur für Prüfungen eingerichtet werden oder bei aktivierter Anwendungserkennung kann sie so konfiguriert werden, dass für den restlichen Anwendungsverkehr Layer-7-Bandbreitenverwaltungsdienste bereitgestellt werden, sobald die Anwendung erkannt wird.




**Proxybasierte Architektur von Mitbewerberlösungen**




**Streambasierte SonicWall Architektur**

## Zentralisierte Verwaltung und zentrales Reporting

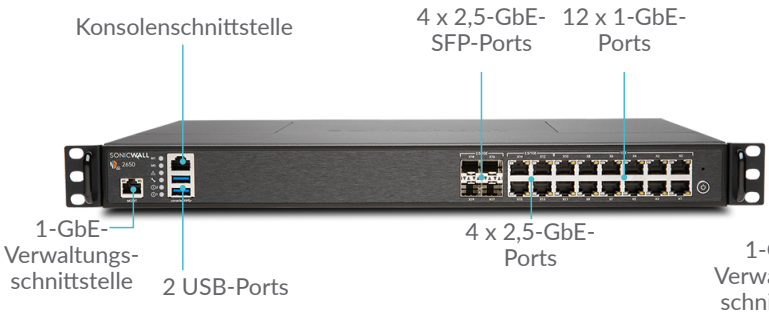
Stark reglementierten Organisationen, die eine komplett aufeinander abgestimmte Security-Governance-, Compliance- und Risikomanagement-Strategie benötigen, bietet SonicWall eine einheitliche, sichere und erweiterbare Plattform, um SonicWall Firewalls, Wireless-Access-Points und Switches der Dell N-Series und X-Series über einen korrelierten und prüfbaren Workstream-Prozess zu verwalten. So 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, einen Einblick in die Benutzeraktivitäten, Anwendungsidentifizierung, Datenstromanalyse und -forensik sowie Compliance- und Audit-Reporting. Dank der Workflow-Automatisierung können Unternehmen geeignete Firewall-Richtlinien flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit Compliance-Vorgaben implementieren und so alle Änderungen an ihren Firewalls effektiv verwalten. Die SonicWall Management und Reporting-Lösungen sind lokal in Form des SonicWall Global Management System und in der Cloud als Capture Security Center verfügbar. Damit lässt sich die Netzwerksicherheit einheitlich auf Geschäftsprozesse und Servicelevel abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, anstatt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt.

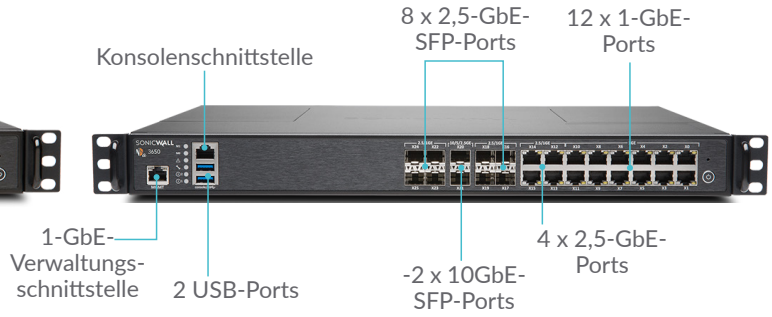
## NS*a* 2650

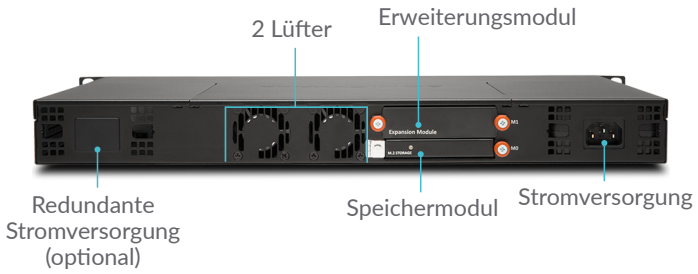
Die NS*a* 2650 bietet mittelgroßen Organisationen und verteilten Unternehmen einen ultraschnellen Bedrohungsschutz für Tausende verschlüsselter Verbindungen und eine noch größere Anzahl unverschlüsselter Verbindungen.

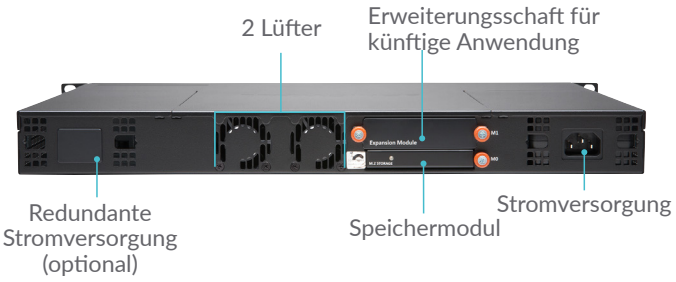
## NS*a* 3650

Die SonicWall NS*a* 3650 eignet sich ideal für Zweigniederlassungen und kleine bis mittlere Unternehmen, die ihre Durchsatzkapazität und Performance optimieren möchten.



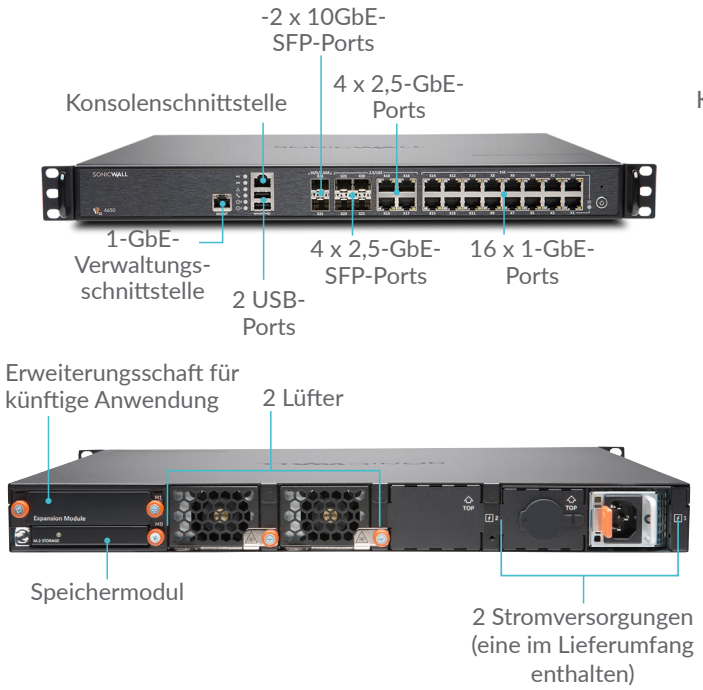




| Firewall | NS*a* 2650 |
|---|---|
| Firewall-Durchsatz | 3,0 GBit/s |
| IPS-Durchsatz | 1,4 GBit/s |
| Anti-Malware-Durchsatz | 1,3 GBit/s |
| Threat-Prevention-Durchsatz | 1,5 GBit/s |
| Maximale Anzahl von Verbindungen | 1.000.000 |
| Neue Verbindungen/Sekunde | 14.000/s |
| Speichermodul | 16 GB |
| **Beschreibung** | **Artikelnummer** |
| NS*a* 2650 (nur Firewall) | 01-SSC-1936 |
| NS*a* 2650 TotalSecure Advanced (1 Jahr) | 01-SSC-1988 |

| Firewall | NS*a* 3650 |
|---|---|
| Firewall-Durchsatz | 3,75 GBit/s |
| IPS-Durchsatz | 1,8 GBit/s |
| Anti-Malware-Durchsatz | 1,5 GBit/s |
| Threat-Prevention-Durchsatz | 1,75 GBit/s |
| Maximale Anzahl von Verbindungen | 2.000.000 |
| Neue Verbindungen/Sekunde | 14.000/s |
| Speichermodul | 32 GB |
| **Beschreibung** | **Artikelnummer** |
| NS*a* 3650 (nur Firewall) | 01-SSC-1937 |
| NS*a* 3650 TotalSecure Advanced (1 Jahr) | 01-SSC-4081 |

## NS*a* 4650

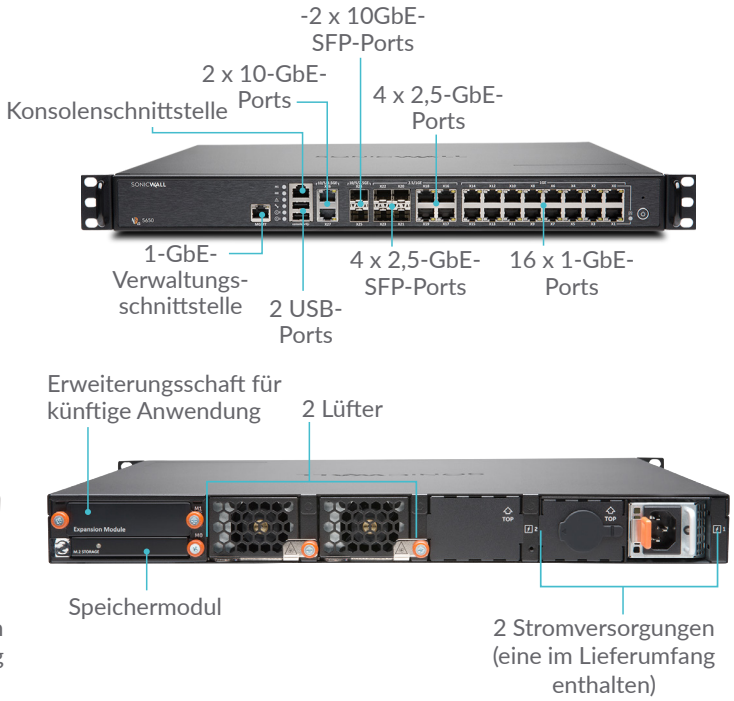
Die SonicWall NS*a 4650* schützt wachstumsstarke mittlere Organisationen und Zweigniederlassungen mit Enterprise-Class-Features und kompromissloser Performance.




| Firewall | NS*a* 4650 |
|---|---|
| Firewall-Durchsatz | 6,0 GBit/s |
| IPS-Durchsatz | 2,3 GBit/s |
| Anti-Malware-Durchsatz | 2,45 GBit/s |
| Threat-Prevention-Durchsatz | 2,5 GBit/s |
| Maximale Anzahl von Verbindungen | 3.000.000 |
| Neue Verbindungen/Sekunde | 40.000/s |
| Speichermodul | 32 GB |
| **Beschreibung** | **Artikelnummer** |
| NS*a* 4650 (nur Firewall) | 01-SSC-1938 |
| NS*a* 4650 TotalSecure Advanced (1 Jahr) | 01-SSC-4094 |

## NS*a* 5650

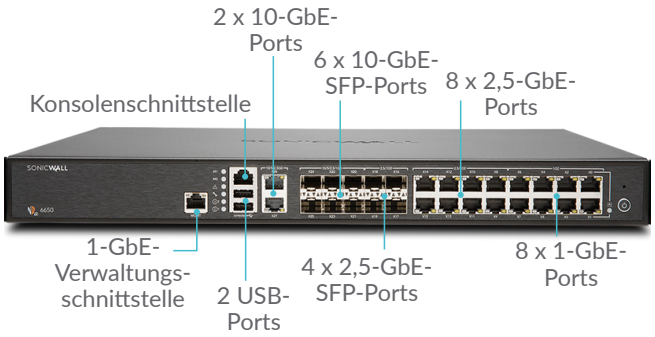
Die SonicWall NS*a* 5650 ist für verteilte Unternehmen sowie für die Zweigniederlassungen und Netzwerkumgebungen von Unternehmen geeignet, die eine erhebliche Durchsatzkapazität und eine hohe Portdichte benötigen.

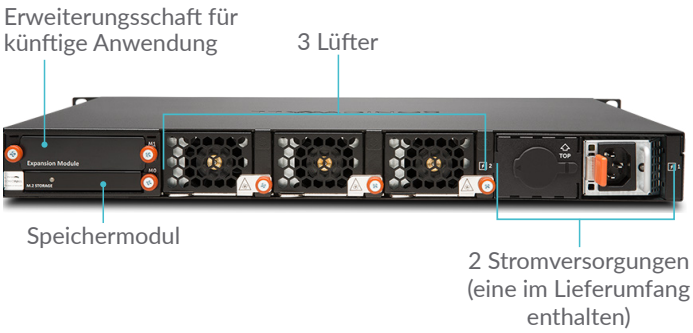



| Firewall | NS*a* 5650 |
|---|---|
| Firewall-Durchsatz | 6,25 GBit/s |
| IPS-Durchsatz | 3,4 GBit/s |
| Anti-Malware-Durchsatz | 2,8 GBit/s |
| Threat-Prevention-Durchsatz | 3,4 GBit/s |
| Maximale Anzahl von Verbindungen | 4.000.000 |
| Neue Verbindungen/Sekunde | 40.000/s |
| Speichermodul | 64 GB |
| **Beschreibung** | **Artikelnummer** |
| NS*a* 5650 (nur Firewall) | 01-SSC-1939 |
| NS*a* 5650 TotalSecure Advanced (1 Jahr) | 01-SSC-4342 |

## NS*a* 6650

Die SonicWall NS*a* *6650* ist für große verteilte Netzwerkumgebungen sowie für Unternehmenszentralen ausgelegt, die eine hohe Durchsatzkapazität und Performance benötigen.

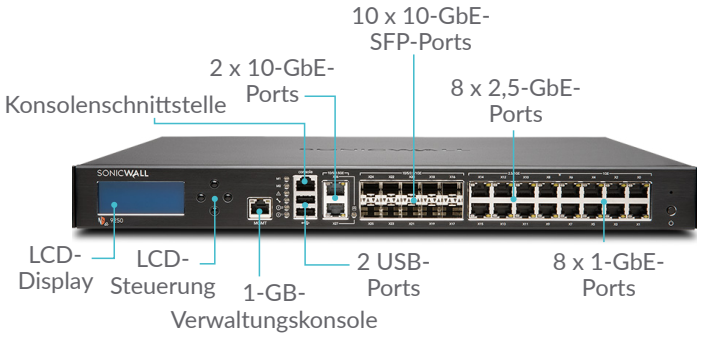


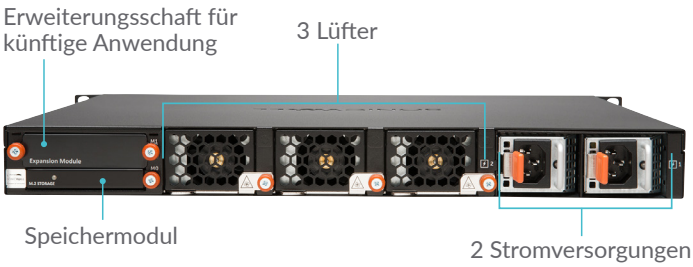




| Firewall | NS*a* 6650 |
|---|---|
| Firewall-Durchsatz | 12,0 GBit/s |
| IPS-Durchsatz | 6,0 GBit/s |
| Anti-Malware-Durchsatz | 5,4 GBit/s |
| Threat-Prevention-Durchsatz | 5,5 GBit/s |
| Maximale Anzahl von Verbindungen | 5.000.000 |
| Neue Verbindungen/Sekunde | 90.000/s |
| Speichermodul | 64 GB |
| **Beschreibung** | **Artikelnummer** |
| NS*a* 6650 (nur Firewall) | 01-SSC-1940 |
| NS*a* 6650 TotalSecure Advanced (1 Jahr) | 01-SSC-2209 |

## NS*a* 9250/9450/9650

Die SonicWall NS*a* 9250/9450/9650 bieten verteilten Unternehmen und Rechenzentren eine hohe Skalierbarkeit und einen umfassenden Schutz bei Multi-Gigabit-Geschwindigkeiten.




| Firewall | NS*a* 9250 | NS*a* 9450 | NS*a* 9650 |
|---|---|---|---|
| Firewall-Durchsatz | 12,0 GBit/s | 17,1 GBit/s | 17,1 GBit/s |
| IPS-Durchsatz | 7,2 GBit/s | 10,2 GBit/s | 10,3 GBit/s |
| Anti-Malware-Durchsatz | 6,5 GBit/s | 8,0 GBit/s | 8,5 GBit/s |
| Threat-Prevention-Durchsatz | 6,5 GBit/s | 9,0 GBit/s | 9,4 GBit/s |
| Maximale Anzahl von Verbindungen | 7.500.000 | 10.000.000 | 12.500.000 |
| Neue Verbindungen/Sekunde | 90.000/s | 130.000/s | 130.000/s |
| Speichermodule | 1 TB, 128 GB | 1 TB, 128 GB | 1 TB, 256 GB |
| **Beschreibung** | **Artikelnummer** | **Artikelnummer** | **Artikelnummer** |
| NS*a* (nur Firewall) | 01-SSC-1941 | 01-SSC-1942 | 01-SSC-1943 |
| NS*a* TotalSecure Advanced (1 Jahr) | 01-SSC-2854 | 01-SSC-4358 | 01-SSC-3475 |

## 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. |

| Funktion | Beschreibung |
|---|---|
| Sicheres SD-WAN | Mit einem sicheren SD-WAN können verteilte Unternehmen geschützte, leistungsstarke Netzwerke über Remote-Standorte hinweg aufbauen, betreiben und verwalten, ohne auf kostspieligere Technologien wie MPLS zurückgreifen zu müssen. Auf diese Weise können sie Daten, Anwendungen und Services mithilfe einfach verfügbarer und erschwinglicher öffentlicher Internetdienste bereitstellen. |
| REST-APIs | Durch diese API erhält die Firewall sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Diese nutzt diese, um komplexe Bedrohungen wie Zero-Day-Angriffe, Insiderbedrohungen, 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 NS*a* 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) ist noch nicht abgeschlossen. Mit SonicOS unterstützt die Hardware Filtering- und Wire-Implementierungsmodi. |
| Flexible Implementierungsoptionen | Die NS*a* 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. |
| 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 hintereinander geschalteter Switches der Dell N-Series und X-Series | Verwaltung der Sicherheitseinstellungen zusätzlicher Ports, einschließlich Portshield, HA, PoE und PoE+ über eine zentrale Stelle mithilfe des Firewall-Management-Dashboards für Dells Netzwerk-Switches der N-Series und X-Series. |
| 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. |
| **Verwaltung und Reporting** | |
| Funktion | Beschreibung |
| Cloud-basierte und lokale Verwaltung | Die SonicWall Appliances lassen sich über die Cloud durch das SonicWall Capture Security Center sowie lokal durch das SonicWall Global Management System (GMS) konfigurieren und verwalten. |
| 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 sowie die Berichterstellung mit Tools wie SonicWall Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen unterstützen, zu ermöglichen. |
| **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 NS*a*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/ Citrix1/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. 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. |
| Real-Time Deep Memory Inspection (RTDMI) | Diese zum Patent angemeldete Cloud-basierte Technologie erkennt und blockiert Malware, die kein schädliches Verhalten zeigt und seine zerstörerische Kraft durch Verschlüsselung verbirgt. Weil die RTDMI Engine die Malware proaktiv zwingt, sich im Arbeitsspeicher zu enttarnen, erkennt und blockiert sie Massenmarkt- und Zero Day-Bedrohungen sowie unbekannte Malware. |
| 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 (entweder einzeln oder als Gruppe), 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 ATP-Abos aufgespielt und in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt. |
| Capture Client | Capture Client ist eine einheitliche Client-Plattform mit mehreren Funktionen für die Endpunktsicherheit, darunter einem hoch entwickelten Malware-Schutz und einem umfassenden Einblick in den verschlüsselten Datenverkehr. Die Plattform bietet mehrschichtige Sicherheitstechnologien, umfassendes Reporting und einen zuverlässigen Endpunktschutz. |
| **Schutz vor verschlüsselten Bedrohungen** | |
| Funktion | Beschreibung |
| TLS-/SSL-Entschlüsselung und -Prüfung | Proxylose On-the-Fly-Entschlüsselung und -Prüfung von TLS-/SSL-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im verschlüsselten Verkehr lauern. Dieser Service ist bei allen NS*a* Series-Modellen in den Sicherheitsabos 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. Malware-Schutz durch Capture Cloud | Eine kontinuierlich aktualisierte Datenbank mit mehreren 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 and Control | |
|---|---|
| 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 sämtlicher nicht notwendige 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 und Content Filtering Client lassen sich Richtlinien zu Nutzungseinschränkungen effektiv durchsetzen und HTTP-/HTTPS-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. |
| Granulare Kontrolle | 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, geeignete Antivirensoftware und/oder DPI-SSL-Zertifikate installiert und aktiviert sind. Somit entfallen die Kosten, die typischerweise für die Verwaltung desktopbasierter Virenschutzlösungen 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. |
| Virenschutz der nächsten Generation | Capture Client nutzt eine statische Artificial-Intelligence(AI)-Engine, um Bedrohungen zu identifizieren, bevor sie ausgeführt werden. Darüber hinaus ermöglicht Capture Client ein Rollback auf einen Zustand vor der Infizierung. |
| 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
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- REST-APIs

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

- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- TLS-/SSL-Kontrolle
- Granulare DPI-SSL-Kontrollen nach Zone oder Regel

### Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- 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
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

### Intrusion-Prevention[1]

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

### Anti-Malware[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
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungssignaturendatenbank

### Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloud-basierte Analysen

### Filterung von HTTP-/HTTPS-Webinhalten[1]

- URL-Filterung
- Vermeidung von Proxys
- Blockieren mithilfe von Schlüsselwörtern
- Richtlinienbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- 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)

### Netzwerk

- Sicheres SD-WAN
- PortShield
- Jumbo-Frames
- 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
- DNS-Sicherheit
- 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, Tap-Modus
- 3G-/4G-WAN-Failover
- Asymmetrisches Routing
- Common Access Card (CAC)-Unterstützung

### Wireless

- WIDS/WIPS
- RF-Spektrumanalyse
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- Automatische Kanalauswahl
- Floor Plan View/Topology View
- Band Steering
- Beamforming
- AirTime-Fairness
- MiFi-Extender
- Zyklische Quote für Gastbenutzer
- LHM-Gast-Portal

### VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- SIP- und H.323-Transformationen nachZugriffsregel
- H.323-Gatekeeper- und SIP-Proxy-Support

### Verwaltung und Überwachung

- Capture Security Center, GMS, Web UI, CLI, REST APIs, SNMPv2/v3
- Logging
- NetFlow-/IPFIX-Export
- Cloud-basiertes Konfigurationsbackup
- BlueCoat Security Analytics Plattform
- Verwaltung von SonicWall-Access-Points
- Dell N-Series- und X-Series-Switch- Verwaltung mit hintereinandergeschalteten Switches

### Lokale Speicherung

- Protokolle
- Reporting
- Firmware-Backups

[1] *Erfordert zusätzliches Abo.*

## NS*a* Series – Systemdaten

| Firewall allgemein | NS*a* 2650 | NS*a* 3650 | NS*a* 4650 | NS*a* 5650 |
|---|---|---|---|---|
| Betriebssystem | SonicOS 6.5.4 | | | |
| Schnittstellen | 4 x 2,5-GbE-SFP, 4 x 2,5-GbE, 12 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole | 2 x 10-GbE-SFP+, 8 x 2,5-GbE-SFP, 4 x 2,5-GbE, 12 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole | 2 x 10-GbE-SFP+, 4 x 2,5-GbE-SFP, 4 x 2,5-GbE, 16 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole | 2 x 10-GbE-SFP+, 2 x 10-GbE, 4 x 2,5-GbE-SFP, 4 x 2,5-GbE, 16 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole |
| Erweiterung | 1 Erweiterungssteckplatz (Rückseite)* | | | |
| Integrierter Speicher (SSD) | 16 GB | 32 GB | 32 GB | 64 GB |
| Management | CLI, SSH, Web-UI, Capture Security Center, GMS, REST-APIs | | | |
| SSO-Benutzer | 40.000 | 50.000 | 60.000 | 70.000 |
| Maximal unterstützte Anzahl von Access-Points | 48 | 96 | 128 | 192 |
| Logging | Analyzer, lokale Logdatei, Syslog | | | |

| Firewall/VPN-Performance | NS*a* 2650 | NS*a* 3650 | NS*a* 4650 | NS*a* 5650 |
|---|---|---|---|---|
| Firewall-Inspection-Durchsatz[1] | 3,0 GBit/s | 3,75 GBit/s | 6,0 GBit/s | 6,25 GBit/s |
| Threat-Prevention-Durchsatz[2] | 1,5 GBit/s | 1,75 GBit/s | 2,5 GBit/s | 3,4 GBit/s |
| Application-Inspection-Durchsatz[2] | 1,85 GBit/s | 2,1 GBit/s | 3,0 GBit/s | 4,25 GBit/s |
| IPS-Durchsatz[2] | 1,4 GBit/s | 1,8 GBit/s | 2,3 GBit/s | 3,4 GBit/s |
| Anti-Malware-Inspection-Durchsatz[2] | 1,3 GBit/s | 1,5 GBit/s | 2,45 GBit/s | 2,8 GBit/s |
| Durchsatz bei TLS/SSL-Entschlüsselung und Prüfung (DPI-SSL)[2] | 300 MBit/s | 320 MBit/s | 675 MBit/s | 800 MBit/s |
| VPN-Durchsatz[3] | 1,45 GBit/s | 1,5 GBit/s | 3,0 GBit/s | 3,5 GBit/s |
| Verbindungen pro Sekunde | 14.000/s | 14.000/s | 40.000/s | 40.000/s |
| Maximale Anzahl von Verbindungen (SPI) | 1.000.000 | 2.000.000 | 3.000.000 | 4.000.000 |
| Maximale Anzahl von Verbindungen (DPI) | 500.000 | 750.000 | 1.000.000 | 1.500.000 |
| Standard/Maximale Anzahl von Verbindungen (DPI-SSL) | 100.000/60.000 | 100.000/40.000 | 175.000/145.000 | 175.000/125.000 |

| VPN | NS*a* 2650 | NS*a* 3650 | NS*a* 4650 | NS*a* 5650 |
|---|---|---|---|---|
| Site-to-Site-Tunnel | 1.000 | 3.000 | 4.000 | 6.000 |
| IPSec-VPN-Clients (max.) | 50 (1.000) | 500 (3.000) | 2.000 (4.000) | 2.000 (6.000) |
| SSL-VPN-NetExtender-Clients (max.) | 2 (350) | 2 (500) | 2 (1.000) | 2 (1.500) |
| 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, BGP | | | |

| Netzwerk | NS*a* 2650 | NS*a* 3650 | NS*a* 4650 | NS*a* 5650 |
|---|---|---|---|---|
| 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 | 400 | 500 |
| Routing-Protokolle | BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing | | | |
| QoS | Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p | | | |
| Authentifizierung | LDAP (mehrere Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC) | | | |
| VoIP | Volle Unterstützung für H323-v1-5, SIP | | | |
| Standards | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | | | |
| Zertifizierungen (in Bearbeitung) | ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall und IPS), UC APL, USGv6, CsFC | | | |
| Hochverfügbarkeit[5] | Active/Passive mit State-Sync | Active/Passive mit State-Sync Active/Active-Clustering | | Active/Passive mit State Sync, Active/Active-DPI mit State-Sync, Active/Active-Clustering |

| Hardware | NS*a* 2650 | NS*a* 3650 | NS*a* 4650 | NS*a* 5650 |
|---|---|---|---|---|
| Netzteil | 2, redundant 120 W (eine im Lieferumfang enthalten) | | 2, redundant 350W (eine im Lieferumfang enthalten) | |
| Lüfter | 2, fest | | 2, auswechselbar | |
| Eingangsspannung | 100–240 V AC, 50–60 Hz | | | |
| Maximaler Stromverbrauch (W) | 37,2 | 46 | 93,6 | 103,6 |
| MTBF bei 25 °C in Stunden | 162.231 | 156.681 | 154.529 | 153.243 |
| MTBF bei 25 °C in Jahren | 18,5 | 17,9 | 17,6 | 17,5 |
| Formfaktor | rackfähig (1 HE) | | | |
| Abmessungen | 43 x 32,5 x 4,5 cm | | 43 x 41,5 x 4,5 cm | |
| Gewicht | 5,2 kg | 5,3 kg | 6,9 kg | 6,9 kg |
| WEEE-Gewicht | 5,5 kg | 5,6 kg | 8,9 kg | 8,9 kg |
| Versandgewicht | 7,7 kg | 7,8 kg | 11,3 kg | 11,3 kg |
| Erfüllt folgende Normen | FCC Klasse A, CE (EMC, LVD, RoHS), C-Tick, VCCI Klasse A, MSIP/KCC Klasse A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI | | | |
| Umgebung (Betrieb/Lagerung) | 0 bis 40 °C/-40 bis 70 °C | | | |
| Luftfeuchtigkeit | 10 bis 90 %, nicht kondensierend | | | |

## NS*a* Series – Systemdaten (Fortsetzung)

| Firewall allgemein | NS*a* 6650 | NS*a* 9250 | NS*a* 9450 | NS*a* 9650 |
|---|---|---|---|---|
| Betriebssystem | SonicOS 6.5.4 | | | |
| Schnittstellen | 6 x 10-GbE-SFP+, 2 x 10-GbE, 4 x 2,5-GbE-SFP, 8 x 2,5-GbE, 8 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole | 10 x 10-GbE-SFP+, 2 x 10-GbE, 8 x 2,5-GbE, 8 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole | 10 x 10-GbE-SFP+, 2 x 10-GbE, 8 x 2,5-GbE, 8 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole | 10 x 10-GbE-SFP+, 2 x 10-GbE, 8 x 2,5-GbE, 8 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole |
| Erweiterung | 1 Erweiterungssteckplatz (Rückseite)* | | | |
| Integrierter Speicher (SSD) | 64 GB | 1TB, 128 GB | 1TB, 128 GB | 1TB, 256 GB |
| Management | CLI, SSH, Web-UI, Capture Security Center, GMS, REST-APIs | CLI, SSH, Web UI, GMS, REST APIs | | |
| SSO-Benutzer | 70.000 | 80.000 | 90.000 | 100.000 |
| Maximal unterstützte Anzahl von Access-Points | 192 | 192 | 192 | 192 |
| Logging | Analyzer, lokale Logdatei, Syslog IPFIX, NetFlow | | | |
| **Firewall/VPN-Performance** | **NS*a* 6650** | **NS*a* 9250** | **NS*a* 9450** | **NS*a* 9650** |
| Firewall-Inspection-Durchsatz[1] | 12,0 GBit/s | 12,0 GBit/s | 17,1 GBit/s | 17,1 GBit/s |
| Threat-Prevention-Durchsatz[2] | 5,5 GBit/s | 6,5 GBit/s | 9,0 GBit/s | 9,4 GBit/s |
| Application-Inspection-Durchsatz[2] | 6,0 GBit/s | 7,8 GBit/s | 10,8 GBit/s | 11,5 GBit/s |
| IPS-Durchsatz[2] | 6,0 GBit/s | 7,2 GBit/s | 10,2 GBit/s | 10,3 GBit/s |
| Anti-Malware-Inspection-Durchsatz[2] | 5,4 GBit/s | 6,5 GBit/s | 8,0 GBit/s | 8,5 GBit/s |
| Durchsatz bei TLS/SSL-Entschlüsselung und Prüfung (DPI-SSL)[2] | 1,45 GBit/s | 1,5 GBit/s | 2,1 GBit/s | 2,25 GBit/s |
| VPN-Durchsatz[3] | 6,0 GBit/s | 6,75 GBit/s | 10,0 GBit/s | 10,0 GBit/s |
| Verbindungen pro Sekunde | 90.000/s | 90.000/s | 130.000/s | 130.000/s |
| Maximale Anzahl von Verbindungen (SPI) | 5.000.000 | 7.500.000 | 10.000.000 | 12.500.000 |
| Maximale Anzahl von Verbindungen (DPI) | 2.000.000 | 3.000.000 | 4.000.000 | 5.000.000 |
| Standard/Maximale Anzahl von Verbindungen (DPI-SSL) | 250.000/170.000 | 250.000/170.000 | 450.000/290.000 | 550.000/320.000 |
| **VPN** | **NS*a* 6650** | **NS*a* 9250** | **NS*a* 9450** | **NS*a* 9650** |
| Site-to-Site-Tunnel | 8.000 | 12.000 | 12.000 | 12.000 |
| IPSec-VPN-Clients (max.) | 2.000 (6.000) | 2.000 (6.000) | 2.000 (6.000) | 2.000 (6.000) |
| SSL-VPN-NetExtender-Clients (max.) | 2 (2.000) | 2 (3.000) | 2 (3.000) | 50 (3.000) |
| 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, BGP | | | |
| **Netzwerk** | **NS*a* 6650** | **NS*a* 9250** | **NS*a* 9450** | **NS*a* 9650** |
| IP-Adressenzuweisung | Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay | | | |
| NAT-Modi | 1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT, transparenter Modus | | | |
| VLAN-Schnittstellen | 512 | | | |
| Routing-Protokolle | BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing | | | |
| QoS | Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p | | | |
| Authentifizierung | LDAP (mehrere Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC) | | | |
| VoIP | Volle Unterstützung für H323-v1-5, SIP | | | |
| Standards | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | | | |
| Zertifizierungen (in Bearbeitung) | ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall und IPS), UC APL, USGv6, CsFC | | | |
| Hochverfügbarkeit[5] | Active/Passive mit State Sync, Active/Active-DPI mit State-Sync, Active/Active-Clustering | | | |
| **Hardware** | **NS*a* 6650** | **NS*a* 9250** | **NS*a* 9450** | **NS*a* 9650** |
| Netzteil | 2, redundant 350W (eine im Lieferumfang enthalten) | 2, redundant, 350 W | | |
| Lüfter | 3, auswechselbar | | | |
| Eingangsspannung | 100–240 V AC, 50–60 Hz | | | |
| Maximaler Stromverbrauch (W) | 144,3 | 86,7 | 90,9 | 113,1 |
| MTBF bei 25 °C in Stunden | 157.193 | 139.783 | 134.900 | 116.477 |
| MTBF bei 25 °C in Jahren | 17,9 | 15,96 | 15,4 | 13,3 |
| Formfaktor | rackfähig (1 HE) | | | |
| Abmessungen | 43 x 41,5 x 4,5 cm | | | |
| Gewicht | 8,1 kg | | 8,1 kg | |
| WEEE-Gewicht | 10,2 kg | | 10,2 kg | |
| Versandgewicht | 12,6 kg | | 12,6 kg | |
| Erfüllt folgende Normen | FCC Klasse A, CE (EMC, LVD, RoHS), C-Tick, VCCI Klasse A, MSIP/KCC Klasse A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI | | | |
| Umgebung (Betrieb/Lagerung) | 0 bis 40 °C/-40 bis 70 °C | | | |
| Luftfeuchtigkeit | 10 bis 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 Threat-Prevention-/Gateway-AV-/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. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen. DPISSL-Performance bei aktiviertem IPS anhand des HTTPS-Verkehrs gemessen.*
[3] *VPN-Durchsatz gemäß RFC 2544 unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte gemessen. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.*
[4] *Pro 125.000 ungenutzten DPI-Verbindungen steigt die Anzahl verfügbarer DPI-SSL-Verbindungen um 3.000 (außer bei NSa 9250 und höher).*
[5] *Active/Active-Clustering und Active/Active-DPI mit State-Sync erfordern den Kauf einer erweiterten Lizenz (außer bei NSa 9250 und höher).*
**Für künftige Anwendung. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.*

## NS*a* Series – Bestellinformationen

| NS*a* 2650 | Artikelnummer |
|---|---|
| NS*a* 2650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-1988 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 2650 (1 Jahr) | 01-SSC-1783 |
| Capture Advanced Threat Protection für NS*a* 2650 (1 Jahr) | 01-SSC-1935 |
| Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 2650 (1 Jahr) | 01-SSC-1976 |
| 24x7 Support für NS*a* 2650 (1 Jahr) | 01-SSC-1541 |
| Content Filtering-Service für NS*a* 2650 (1 Jahr) | 01-SSC-1970 |
| Capture Client | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NS*a* 2650 (1 Jahr) | 01-SSC-2001 |
| **NS*a* 3650** | **Artikelnummer** |
| NS*a* 3650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-4081 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 3650 (1 Jahr) | 01-SSC-3451 |
| Capture Advanced Threat Protection für NS*a* 3650 (1 Jahr) | 01-SSC-3457 |
| Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 3650 (1 Jahr) | 01-SSC-3632 |
| 24x7 Support für NS*a* 3650 (1 Jahr) | 01-SSC-3439 |
| Content Filtering-Service für NS*a* 3650 (1 Jahr) | 01-SSC-3469 |
| Capture Client | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NS*a* 3650 (1 Jahr) | 01-SSC-4030 |
| **NS*a* 4650** | **Artikelnummer** |
| NS*a* 4650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-4094 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 4650 (1 Jahr) | 01-SSC-3493 |
| Capture Advanced Threat Protection für NS*a* 4650 (1 Jahr) | 01-SSC-3499 |
| Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 4650 (1 Jahr) | 01-SSC-3589 |
| 24x7 Support für NS*a* 4650 (1 Jahr) | 01-SSC-3487 |
| Content Filtering-Service für NS*a* 4650 (1 Jahr) | 01-SSC-3583 |
| Capture Client | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NS*a* 4650 (1 Jahr) | 01-SSC-4062 |
| **NS*a* 5650** | **Artikelnummer** |
| NS*a* 5650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-4342 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 5650 (1 Jahr) | 01-SSC-3674 |
| Capture Advanced Threat Protection für NS*a* 5650 (1 Jahr) | 01-SSC-3680 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 5650 (1 Jahr) | 01-SSC-3698 |
| 24x7 Support für NS*a* 5650 (1 Jahr) | 01-SSC-3660 |
| Content Filtering-Service für NS*a* 5650 (1 Jahr) | 01-SSC-3692 |
| Capture Client | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NS*a* 5650 (1 Jahr) | 01-SSC-4068 |
| **NS*a* 6650** | **Artikelnummer** |
| NS*a* 6650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-2209 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 6650 (1 Jahr) | 01-SSC-8761 |
| Capture Advanced Threat Protection für NS*a* 6650 (1 Jahr) | 01-SSC-8930 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 6650 (1 Jahr) | 01-SSC-8979 |
| 24x7 Support für NS*a* 6650 (1 Jahr) | 01-SSC-8663 |
| Content Filtering-Service für NS*a* 6650 (1 Jahr) | 01-SSC-8972 |
| Capture Client | Basierend auf Benutzeranzahl |
| Comprehensive Anti-Spam Service für NS*a* 6650 (1 Jahr) | 01-SSC-9131 |
| **NS*a* 9250** | **Artikelnummer** |
| NS*a* 9250 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-2854 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 9250 (1 Jahr) | 01-SSC-0038 |
| Capture Advanced Threat Protection für NS*a* 9250 (1 Jahr) | 01-SSC-0121 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 9250 (1 Jahr) | 01-SSC-0343 |
| 24x7 Support für NS*a* 9250 (1 Jahr) | 01-SSC-0032 |
| Content Filtering-Service für NS*a* 9250 (1 Jahr) | 01-SSC-0331 |
| Capture Client | Basierend auf Benutzeranzahl |
| **NS*a* 9450** | **Artikelnummer** |
| NS*a* 9450 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-4358 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 9450 (1 Jahr) | 01-SSC-0414 |
| Capture Advanced Threat Protection für NS*a* 9450 (1 Jahr) | 01-SSC-0855 |

## NS*a* Series – Bestellinformationen (Fortsetzung)

| NS*a* 9450 | Artikelnummer |
|---|---|
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 9450 (1 Jahr) | 01-SSC-1196 |
| 24x7 Support für NS*a* 9450 (1 Jahr) | 01-SSC-0407 |
| Content Filtering-Service für NS*a* 9450 (1 Jahr) | 01-SSC-1158 |
| Capture Client | Basierend auf Benutzeranzahl |
| **NS*a* 9650** | **Artikelnummer** |
| NS*a* 9650 TotalSecure Advanced Edition (1 Jahr) | 01-SSC-3475 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Visualisierung von Schatten-IT und 24x7 Support für NS*a* 9650 (1 Jahr) | 01-SSC-2036 |
| Capture Advanced Threat Protection für NS*a* 9650 (1 Jahr) | 01-SSC-2042 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*a* 9650 (1 Jahr) | 01-SSC-2142 |
| 24x7 Support für NS*a* 9650 (1 Jahr) | 01-SSC-1989 |
| Content Filtering-Service für NS*a* 9650 (1 Jahr) | 01-SSC-2136 |
| Capture Client | Basierend auf Benutzeranzahl |
| **Module und Zubehör*** | **Artikelnummer** |
| 10GBASE-SR SFP+ Short Reach Modul | 01-SSC-9785 |
| 10GBASE-LR SFP+ Long Reach Modul | 01-SSC-9786 |
| 10GBASE SFP+ 1M Twinaxial-Kabel | 01-SSC-9787 |
| 10GBASE SFP+ 3M Twinaxial-Kabel | 01-SSC-9788 |
| 1000BASE-SX SFP Short Haul Modul | 01-SSC-9789 |
| 1000BASE-LX SFP Long Haul Modul | 01-SSC-9790 |
| 1000BASE-T SFP Kupfermodul | 01-SSC-9791 |

**Für eine vollständige Liste der unterstützten SFP- und SFP+-Module wenden Sie sich bitte an Ihren lokalen SonicWall-Ansprechpartner*

### SonicWall NS*a*/NS*v* Firewall-Bundle

Die folgenden NS*a* Series-Firewalls sind für den Erhalt einer 1-Jahres-Lizenz für das entsprechende NSv Virtual Appliance TotalSecure Abo* ohne Aufpreis qualifiziert.

| Qualifizierte NS*a*-Firewall | Entsprechende NS*v*-Firewall |
|---|---|
| NS*a* 5650 | NS*v* 200 |
| NS*a* 6650 | NS*v* 200 |
| NS*a* 9250 | NS*v* 400 |
| NS*a* 9450 | NS*v* 400 |
| NS*a* 9650 | NS*v* 400 |

** NSv Virtual Appliance TotalSecure Abos beinhalten NSv Virtual Firewall, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Firewall Service, Content Filtering Service und 24x7-Support.*

### Modellnummern (Zulassung):

NS*a* 2650 – 1RK38-0C8
NS*a* 3650 – 1RK38-0C7
NS*a* 4650 – 1RK39-0C9
NS*a* 5650 – 1RK39-0CA
NS*a* 6650 – 1RK39-0CB
NS*a* 9250 – 1RK39-0CC
NS*a* 9450 – 1RK39-0CD
NS*a* 9650 – 1RK39-0CE

### Partner Enabled Services

Brauchen Sie Hilfe bei der Planung, Einbindung oder Optimierung Ihrer SonicWall-Lösung? SonicWall Advanced Services Partners sind umfassend ausgebildet, um Ihnen erstklassigen professionellen Service zu bieten. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

## Über SonicWall

SonicWall kämpft seit über 27 Jahren gegen Cyberkriminalität und verteidigt kleine und mittelständische Betriebe, größere Unternehmen und Regierungsbehörden weltweit. Unsere preisgekrönten Lösungen zur Erkennung und Prävention von Datenschutzverletzungen in Echtzeit bauen auf der Forschung aus den SonicWall Capture Labs auf und sichern mehr als eine Million Netzwerke sowie E-Mails, Anwendungen und Daten in mehr als 215 Ländern und Gebieten. Die betreffenden Organisationen können sich besser auf ihr Geschäft konzentrieren und müssen sich weniger um ihre Sicherheit sorgen. Weitere Informationen finden Sie auf www.sonicwall.com ode folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.



**SonicWall, Inc.**
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
**www.sonicwall.com**


Datasheet-NetworkSecurityAppliance-US-VG-MKTG5872

SONICWALL®