SonicWall Network Security Services Platform (NS*sp*) 12000 Series

Skalierbare Sicherheitslösung mit leistungsfähiger Cloud-Datenanalyse

Die SonicWall Network Security Services Platform (NS*sp*) der 12000 Series steht für einen modernen Sicherheitsansatz, der Bedrohungsdaten aus der Cloud mit gerätebasierten Sicherheitsfunktionen in einer skalierbaren, Hochleistungsplattform vereint. Die Next-Generation-Firewalls der NS*sp* Series erfüllen die Anforderungen großer, dezentral organisierter Unternehmen, Rechenzentren und Serviceprovider und nutzen die innovativen Deep-Learning-Sicherheitstechnologien der Capture Cloud Platform, um die komplexesten Bedrohungen ohne Beeinträchtigung der Systemperformance abzuwehren.

Sicherheit für Unternehmen

Die Zahl und Komplexität von Netzwerkangriffen nimmt ständig zu. Zero-Day-Bedrohungen und Eindringversuche lassen sich nur abwehren, wenn zusätzlich zu den hardwarebasierten Sicherheitsfunktionen auch Bedrohungsdaten aus der Cloud genutzt werden. Ohne diese Cloud-Daten sind Gateway-Sicherheitslösungen der Enterprise-Klasse modernen komplexen Bedrohungen nicht gewachsen.

Die SonicWall NS*sp* Series verknüpft die von unserem Capture Labs Threat Research-Team gesammelten Bedrohungsdaten mit den geräteeigenen Sicherheitsfunktionen und ermöglicht so eine kontinuierlich aktualisierte Sicherheitslösung. Der cloudbasierte Capture Advanced Threat Protection(ATP)-Service nutzt die zum Patent angemeldete Real-Time Deep Memory Inspection(RTDMI™)-Technologie, um breit angelegte Zero-Day-Bedrohungen und unbekannte Malware durch eine direkte In-Memory-Überprüfung aktiv zu erkennen und abzuwehren. Aufgrund ihrer Echtzeitarchitektur arbeitet die RTDMI-Technologie von SonicWall extrem präzise und reduziert die Anzahl von Falschmeldungen auf ein Minimum. Außerdem ist sie in der Lage, ausgeklügelte Angriffe dort zu identifizieren und abzuwehren, wo der schädliche Malware-Mechanismus für einen winzigen Augenblick von weniger als 100 Nanosekunden offengelegt wird. Unterstützt wird diese cloudbasierte Sicherheit von SonicWalls patentierter* Single-Pass-Reassembly-Free Deep Packet Inspection (RFDPI®)-Engine, die den eingehenden und ausgehenden Netzwerkverkehr an der Firewall überwacht. Die NS*sp* Series nutzt neben integrierten Funktionen wie Intrusion-Prevention, Anti-Malware und Web-/URL-Filtering auch die SonicWall Capture Cloud Platform, um Bedrohungen in Echtzeit zu erkennen und Unternehmen einen wirksamen Schutz zu bieten.

Angesichts der wachsenden Zahl von verschlüsselten Verbindungen im Web müssen Next-Generation-Firewalls in der Lage sein, auch verschlüsselten Datenverkehr nach versteckten Bedrohungen zu durchsuchen. Die Firewalls von SonicWall bieten rundum Sicherheit, indem sie Hunderttausende TLS-/SSL- und SSH-verschlüsselte Verbindungen unabhängig vom verwendeten Port oder Protokoll vollständig entschlüsseln und analysieren. Alle Pakete werden gründlich geprüft. Dabei scannt die Firewall den gesamten Verkehr auf die Nichteinhaltung von Protokollen, Bedrohungen, Zero-Day-Angriffe, Eindringversuche und sogar benutzerdefinierte Kriterien. Die Deep Packet Inspection-Engine erkennt und verhindert verborgene kryptografische Angriffe, blockiert verschlüsselte Malware-Downloads und verhindert die Verbreitung von Bedrohungen, Command-and-Control(C&C)-Kommunikationen und das Herausschleusen von 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.

Unternehmen brauchen eine Sicherheitslösung, die mit ihnen wächst. SonicWall hat sich hierfür eine Lösung ausgedacht,

Vorteile:

Überragender Bedrohungsschutz und exzellente Performance

- Zum Patent angemeldete Real-Time Deep Memory Inspection-Technologie
- Patentierte Reassembly-Free Deep Packet Inspection-Technologie
- Cloudbasierter und geräteintegrierter Bedrohungsschutz
- TLS-/SSL-Entschlüsselung und -Prüfung
- Effiziente, bewährte Sicherheit
- Mehrere 40-GbE- und 10-GbE-Schnittstellen
- Spezielles Capture Labs Threat Research-Team

Mehr Netzwerkkontrolle und Flexibilität

- Leistungsstarkes SonicOS-Betriebssystem
- Application-Intelligence und Anwendungskontrolle
- Netzwerksegmentierung und Einrichtung von Zonen
- Bereitstellung am Netzwerkrand oder im Rechenzentrum

Skalierbarkeit und Zuverlässigkeit

- Hohe Anzahl an DPI-SSL-Verbindungen
- Verschiedene Konfigurationsoptionen
- Integriertes Speichermodul
- Redundante Stromversorgung und Lüfter

bei der das Hinzufügen zusätzlicher Rechenleistung kein Problem mehr darstellt. Die NS*sp* 12400 kommt mit vier Prozessormodulen und lässt sich auf acht Module erweitern. Die NS*sp* 12800 wird standardmäßig mit acht Prozessormodulen ausgeliefert.

Werden Deep-Packet-Inspection-Funktionen wie IPS, Anti-Malware, Anti-Spyware und TLS-/SSL-Entschlüsselung/-Analyse auf einer Firewall aktiviert, kommt es oft zu einem massiven Abfall der Netzwerkperformance. Nicht so bei den Next-Generation-Firewalls der NS*sp* Series – sie sind mit spezialisierten Security-Prozessoren ausgestattet und liefern mit ihren 40-GbE-Schnittstellen und ihrer Multi-Core-Hardware-Architektur ausreichend Geschwindigkeit. Dieses einzigartige Design – in Kombination mit unseren RTDMI- und RFDPI-Engines – verhindert Leistungseinbußen, wie sie oft bei anderen Firewalls auftreten.

Mehr Netzwerkkontrolle und Flexibilität

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

Mithilfe der Application-Intelligence- und Anwendungskontrollfunktionen lassen sich produktive Anwendungen identifizieren, kategorisieren und von unproduktiven oder potenziell gefährlichen Applikationen unterscheiden. Außerdem können Administratoren durch leistungsstarke Regeln auf Anwendungsebene, die sowohl für einzelne Benutzer als auch für bestimmte Gruppen greifen, den Datenverkehr kontrollieren (zusammen mit Zeitplänen und Ausnahmelisten).

Geschäftskritische Anwendungen können priorisiert und mit mehr Bandbreite ausgestattet werden, während sich die Bandbreite für nicht relevante Anwendungen einschränken lässt. Funktionen für die Echtzeitüberwachung und -visualisierung bieten eine grafische Darstellung der Anwendungen, User und Bandbreitennutzung und ermöglichen so detaillierte Einblicke in den gesamten Netzwerkverkehr.

Unternehmen, die mehr Flexibilität für ihr Netzwerkdesign benötigen, bietet SonicOS die erforderlichen Tools, um das Netzwerk mithilfe virtueller LANs (VLANs) in Zonen zu segmentieren. Netzwerkadministratoren können so ein virtuelles LAN-Interface erstellen, das eine Netzwerkunterteilung in eine oder mehrere logische Gruppen erlaubt.

Einfacheres Management und Reporting

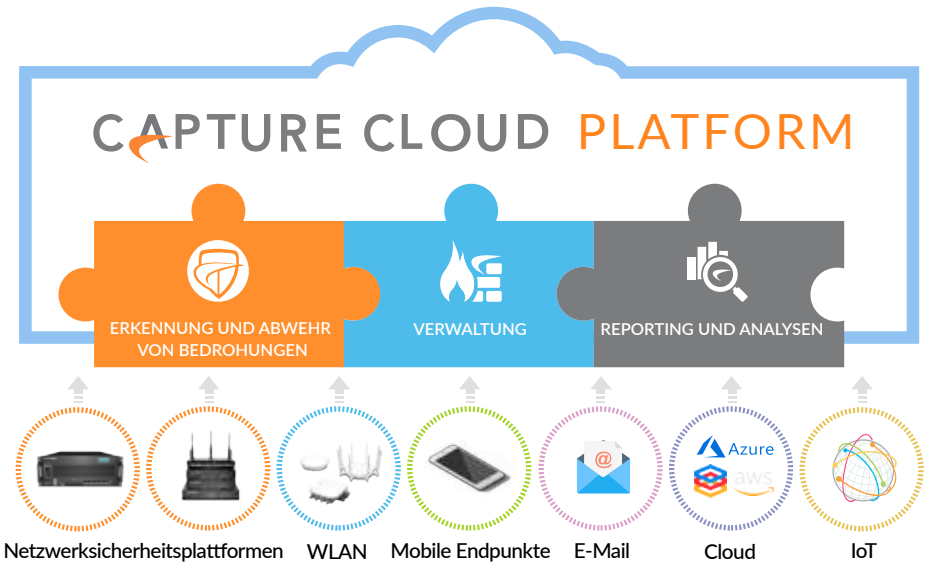
Management, Überwachung and Reporting der Netzwerksicherheit erfolgen über das SonicWall Global Management System (GMS) – ein übersichtliches, zentrales Dashboard, in dem alle für die Verwaltung des Netzwerks erforderlichen Daten in Echtzeit zusammenfließen. Die Administratoren behalten über eine einzige Konsole alle Aspekte des Netzwerks im Blick. Dank der einfachen Implementierung, Einrichtung und Verwaltung können Organisationen ihre TCO senken und von einem schnellen ROI profitieren.

Partner Enabled Services
Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Unsere SonicWall Advanced Services Partner bieten Ihnen erstklassige Professional Services. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

Capture Cloud Platform

Die Capture Cloud Platform von SonicWall bietet kleinen wie großen Organisationen eine cloudbasierte 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 Capture Cloud Platform-Datenbank gespeichert und in den Kunden-Firewalls implementiert werden und einen topaktuellen Schutz 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. Eine einzige Signatur deckt dabei Zehntausende verschiedener Bedrohungen ab. Zusätzlich zu den Abwehrmechanismen



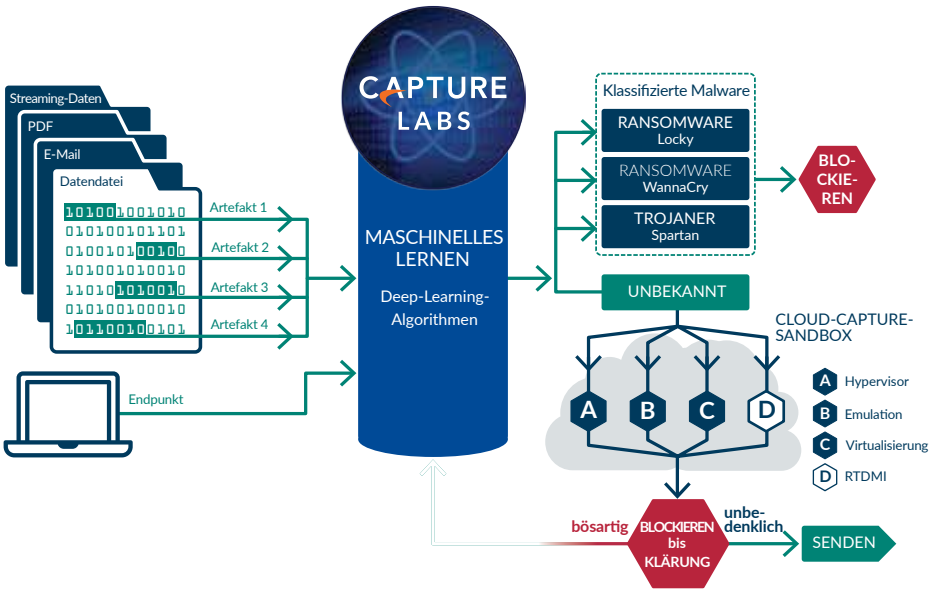
auf der Appliance haben die NS*sp*-Firewalls auch einen kontinuierlichen Zugang zur Capture Cloud Platform-Datenbank. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um mehrere Millionen Signaturen erweitert.

Darüber hinaus bietet die Capture Cloud Platform Administratoren die Möglichkeit, über eine einzige Verwaltungskonsole spielend leicht Echtzeit- und historische Berichte zur Netzwerkaktivität zu erstellen.

Schutz vor raffinierten Bedrohungen

Herzstück der automatisierten SonicWall-Lösung zur Echtzeitprävention von Sicherheitslücken ist der SonicWall Capture Advanced Threat Protection-Service, eine cloudbasierte 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 festgesetzt 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.



SONICWALL

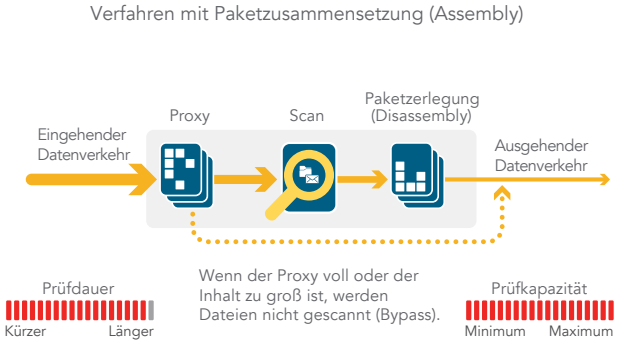
Reassembly-Free Deep Packet Inspection-Engine

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 raffinierte Umgehungsversuche verhindern, die darauf abzielen, Erkennungsmechanismen zu stören und bösartigen Code unbemerkt in das Netzwerk einzuschleusen.

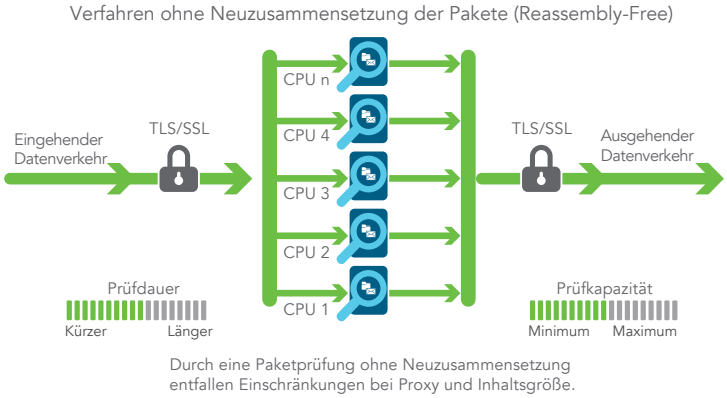
Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. TLS-/SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall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



Proxybasierte Architektur von Mitbewerberlösungen

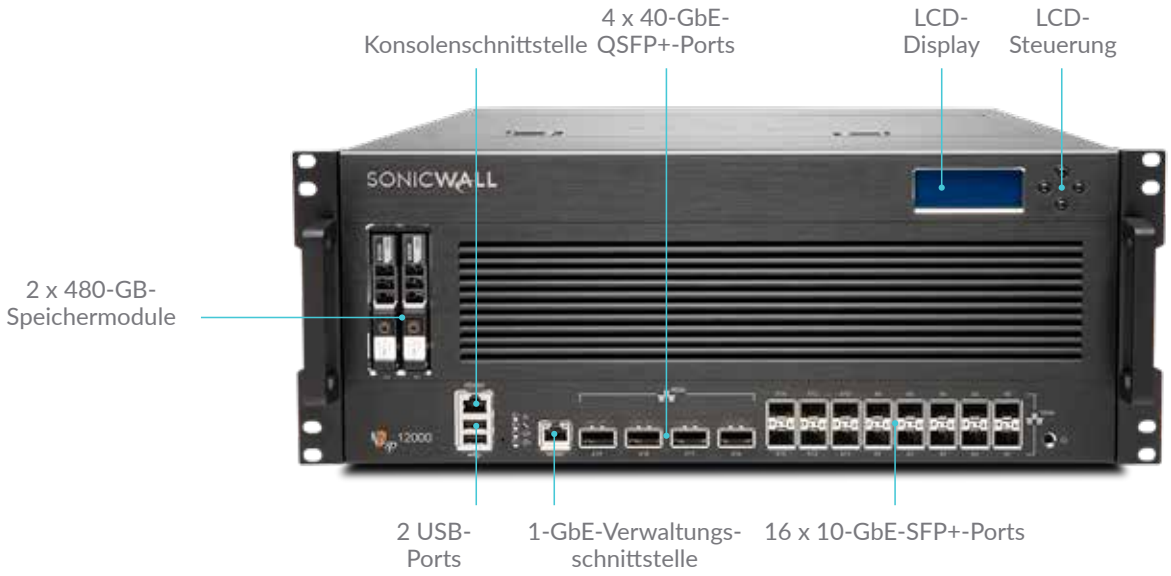


Streambasierte SonicWall-Architektur

Globales Management und 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 WAN-Beschleunigungslösungen 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-Regeln flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit Compliance-Vorgaben implementieren und so alle Änderungen an ihren Firewalls effektiv verwalten. Mit dem SonicWall Global Management System (GMS), der lokalen Management- und Reporting-Lösung von SonicWall, kann die Netzwerksicherheit einheitlich auf Geschäftsprozesse und Servicelevel abgestimmt werden. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, anstatt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt.

NS*sp* 12000 Series



Firewall	NS*sp* 12400	NS*sp* 12800
Firewall-Inspection-Durchsatz	58,4 GBit/s	120,3 GBit/s
IPS-Durchsatz	36,8 GBit/s	73,0 GBit/s
Anti-Malware-Inspection-Durchsatz	33,5 GBit/s	67,5 GBit/s
Threat-Prevention-Durchsatz	33,5 GBit/s	67,5 GBit/s
IMIX-Durchsatz	14,8 GBit/s	29,0 GBit/s
Maximale Anzahl von Verbindungen (DPI)	16.000.000	32.000.000
Neue Verbindungen/Sekunde	430.000/Sek.	860.000/Sek.
Speichermodul	2 x 480 GB	2 x 480 GB
Beschreibung	**Artikelnummer**	**Artikelnummer**
NS*sp* (nur Firewall)	01-SSC-1206	01-SSC-1207
NS*sp* TotalSecure Advanced (1 Jahr)	01-SSC-7883	01-SSC-9139

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

TLS-/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-Steuerung nach Zone oder Regel

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeit-informationen 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

Malware-Schutz[1]

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

Anwendungsidentifizierung[1]

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungs-signaturendatenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung

Filterung von Webinhalten[1]

- URL-Filtering
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- 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

- PortShield
- Jumbo-Frames
- Erweiterte Protokollierung
- VLAN-Trunking
- RSTP (Rapid Spanning Tree Protocol)
- Portspiegelung
- Portsicherheit
- Layer-2-QoS
- Dynamisches Routing (RIP/OSPF/BGP)
- Regelbasiertes Routing
- NAT
- DNS/DNS-Proxy
- 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
- Asymmetrisches Routing
- Common Access Card(CAC)-Unterstützung

Wireless

- WIDS/WIPS
- Analyse des HF-Spektrums
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- Floor Plan View / Topology View
- Bandsteering
- Beamforming
- AirTime-Fairness
- MiFi-Extender
- Zyklische Quote für Gastbenutzer
- LHM-Gast-Portal

VoIP

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

Verwaltung und Überwachung

- GMS, Web, UI, CLI, REST-APIs, SNMPv2/v3
- Logging
- NetFlow-/IPFIX-Export
- Cloudbasiertes Konfigurationsbackup
- BlueCoat Security Analytics Platform
- Verwaltung von SonicWall-Access-Points

Speicher

- Protokolle
- Abrufbare Reports
- Firmware-Backups

[1] Erfordert zusätzliches Abo

SONICWALL

Funktionen

RFDPI-Engine	
Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection (RFDPI)	Diese hochleistungsfähige, proprietäre und patentierte Prüf-Engine führt eine streambasierte bidirektionale Verkehrsanalyse durch, um Eindringversuche und Malware zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy.
Bidirektionale Prüfung	Der ein- und ausgehende Datenverkehr wird gleichzeitig auf Bedrohungen geprüft, um zu verhindern, dass ein infizierter Computer das Netzwerk zum Verbreiten von Malware oder als Ausgangsplattform für Angriffe nutzt.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxys stattfindet, lassen sich Millionen gleichzeitiger Datenströme mit der DPI-Technologie bei minimalen Latenzzeiten scannen, ohne dabei das Datenvolumen oder die Dateigrößen einzuschränken. Dies funktioniert sowohl bei gängigen Protokollen als auch bei Raw-TCP-Streams.
Hohe Parallelität und Skalierbarkeit	Gemeinsam mit der Multicore-Architektur ermöglicht das einzigartige Design der RFDPI-Engine einen hohen DPI-Durchsatz sowie extrem hohe Geschwindigkeiten beim Aufbau neuer Sitzungen. Verkehrsspitzen in anspruchsvollen Netzwerken lassen sich so besser bewältigen.
Single-Pass-Inspection	Eine Single-Pass-DPI-Architektur prüft den Verkehr auf Malware und Eindringversuche und sorgt gleichzeitig für die Erkennung von Anwendungen. Dadurch werden DPI-bedingte Latenzzeiten drastisch verkürzt. Außerdem wird sichergestellt, dass sämtliche Informationen zu Bedrohungen innerhalb einer einheitlichen Architektur verarbeitet werden.
Firewall und Netzwerk	
Funktion	Beschreibung
REST-APIs	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, 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*sp* 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*sp* 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.
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)	Die SonicWall-Appliances lassen sich lokal über 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 Unterstützung 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 SonicWall Analytics sowie 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 NS*sp* 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/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, cloudbasierte Technologie ist in der Lage, Malware, die kein bösartiges Verhalten zeigt oder ihre Mechanismen durch Verschlüsselungsmethoden verschleiert, zu identifizieren und zu blockieren. Die RTDMI-Engine zwingt Malware dazu, ihre Wirkmechanismen im Speicher offenzulegen. So ist sie in der Lage, die in großer Zahl vorkommenden Zero-Day-Bedrohungen sowie unbekannte Malware aufzudecken und abzuwehren.
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 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	TLS-/SSL-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 verschlüsseltem Datenverkehr abzusichern. Dieser Service ist bei allen NS*sp*-Modellen in den Sicherheitsabos enthalten.
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 mit aktivierten Sicherheitsservices weitergeleitet und sind ohne Neustart oder andere Unterbrechungen sofort wirksam.
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, geeignete Antivirensoftware und/oder DPI-SSL-Zertifikate installiert und aktiviert sind. Somit entfallen die Kosten, die typischerweise für die Verwaltung von desktopbasierten 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.

NS*sp* – Systemdaten

Firewall allgemein	NS*sp* 12400	NS*sp* 12800
Betriebssystem	SonicOS 6.5.1.8	
Security-Prozessor-Cores	128	256
Schnittstellen	4 x 40-GbE-QSFP+, 16 x 10-GbE-SFP+, 1-GbE-Verwaltungsschnittstelle, 1 Konsole	4 x 40-GbE-QSFP+, 16 x 10-GbE-SFP+, 1-GbE-Verwaltungsschnittstelle, 1 Konsole
Integrierter Speicher	2 x 480 GB	
Verwaltung	CLI, SSH, Web-UI, GMS, REST-APIs	
SSO-Benutzer	110.000	110.000
Maximal unterstützte Anzahl von Access-Points	128	128
Logging	Analyzer, lokale Logdatei, Syslog, IPFIX, NetFlow	
Firewall-/VPN-Performance	**NS*sp* 12400**	**NS*sp* 12800**
Firewall-Inspection-Durchsatz[1]	58,4 GBit/s	120,3 GBit/s
Threat-Prevention-Durchsatz[2]	33,5 GBit/s	67,5 GBit/s
Application-Inspection-Durchsatz[2]	45,5 GBit/s	91,0 GBit/s
IPS-Durchsatz[2]	36,8 GBit/s	73,0 GBit/s
Anti-Malware-Inspection-Durchsatz[2]	33,5 GBit/s	67,5 GBit/s
IMIX-Durchsatz	14,8 GBit/s	29,0 GBit/s
Durchsatz bei TLS-/SSL-Entschlüsselung und -Prüfung (DPI-SSL)[2]	8,1 GBit/s	17,6 GBit/s
VPN-Durchsatz[3]	24,5 GBit/s	47,0 GBit/s
Verbindungen pro Sekunde	430.000/Sek.	860.000/Sek.
Maximale Anzahl von Verbindungen (SPI)	40.000.000	80.000.000
Maximale Anzahl von Verbindungen (DPI)	16.000.000	32.000.000
Maximale Anzahl von Verbindungen (DPI-SSL)	800.000	1.600.000
VPN	**NS*sp* 12400**	**NS*sp* 12800**
Site-to-Site-VPN-Tunnel	25.000	25.000
IPSec-VPN-Clients (max.)	2.000 (10.000)	2.000 (10.000)
SSL-VPN-NetExtender-Clients (max.)	2 (3.000)	2 (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*sp* 12400**	**NS*sp* 12800**
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	512
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing	
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p	
Authentifizierung	LDAP, 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	
Zertifizierungen (Änderungen möglich)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall und IPS), UC APL, USGv6, CsFC	
Hochverfügbarkeit	Active/Passive mit State-Sync, Active/Active-DPI mit State-Sync, Active/Active-Clustering	
Hardware	**NS*sp* 12400**	**NS*sp* 12800**
Stromversorgung	2, redundant, 1.200 W	
Lüfter	2, auswechselbar	
Eingangsspannung	100–240 VAC, 50–60 Hz	
Maximaler Stromverbrauch (W)	679	965
MTBF bei 25 °C in Stunden	113.114	91.118
MTBF bei 25 °C in Jahren	12,9	10,4
Formfaktor	rackfähig (4 HE)	
Abmessungen	61 x 43 x 18 cm	
Gewicht	26,9 kg	30,5 kg
WEEE-Gewicht	30,7 kg	34,3 kg
Versandgewicht	37,7 kg	41,3 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	
Umgebungstemperatur (Betrieb/Lagerung)	0–40 °C / -40–70 °C	
Luftfeuchtigkeit	10–95 %, 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. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen. DPI-SSL-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.
˙ Für künftige Anwendung. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.

NS*sp* 12000 Series – Bestellinformationen

NS*sp* 12400	Artikelnummer
NS*sp* 12400 TotalSecure Advanced Edition (1 Jahr)	01-SSC-7883
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NS*sp* 12400 (1 Jahr)	01-SSC-6588
Capture Advanced Threat Protection für NS*sp* 12400 (1 Jahr)	01-SSC-6598
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*sp* 12400 (1 Jahr)	01-SSC-7853
24/7-Support für NS*sp* 12400 (1 Jahr)	01-SSC-6384
Content Filtering Service für NS*sp* 12400 (1 Jahr)	01-SSC-7698
NS*sp* 12800	**Artikelnummer**
NS*sp* 12800 TotalSecure Advanced Edition (1 Jahr)	01-SSC-9139
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für NS*sp* 12800 (1 Jahr)	01-SSC-6591
Capture Advanced Threat Protection für NS*sp* 12800 (1 Jahr)	01-SSC-7178
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für NS*sp* 12800 (1 Jahr)	01-SSC-7879
24/7-Support für NS*sp* 12800 (1 Jahr)	01-SSC-6498
Content Filtering Service für NS*sp* 12800 (1 Jahr)	01-SSC-7850
Module und Zubehör*	**Artikelnummer**
NS*sp* 12000 Series-Prozessormodul	01-SSC-1211
NS*sp* 12000 Series-SSD-Modul	01-SSC-1212
NS*sp* 12000 Series-Systemlüfter	01-SSC-1213
NS*sp* 12000 Series-AC-Netzteil	01-SSC-1215

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

Modellnummern (Zulassung):

NS*sp* 12400/12800 – 4RK02-0C0

Über uns

Seit über 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

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

Datasheet-NSsp-US-KJ-MKTG4029