SonicWall SuperMassive Series

Leistungsstarke Next-Generation-Firewalls für einen kompromisslosen Netzwerkschutz

Die SonicWall SuperMassive Series – die Next-Generation-Firewall-Plattform für große Netzwerke – bietet höchste Skalierbarkeit, Zuverlässigkeit und Sicherheit bei Multi-Gigabit-Geschwindigkeiten und minimalen Latenzzeiten.

Sie wurde für die Anforderungen großer Unternehmen sowie von Behörden, Bildungseinrichtungen, Einzelhändlern, Healthcare-Organisationen und Serviceprovidern entwickelt und eignet sich ideal für den Schutz von verteilten Enterprise-Netzwerken und Datencentern.

Mit dem SonicWall-SonicOS-Betriebssystem, der patentierten* Reassembly-Free Deep Packet Inspection® (RFDPI)-Technologie und der hoch skalierbaren Hardware-Architektur, die über eine beträchtliche Anzahl an Cores verfügt, bietet die SuperMassive 9000 Series modernste Funktionen für Anwendungskontrolle, Intrusion-Prevention, Malware-Schutz und TLS-/SSL-Entschlüsselung und -Prüfung bei Multi-Gigabit-Geschwindigkeiten. Entwickelt wurde die SuperMassive Series mit besonderem Augenmerk auf Stromverbrauch, Platzbedarf und Kühlung. Daher bietet sie als Next-Generation-Firewall den höchsten Durchsatz pro Watt (GBit/s/Watt) für eine leistungsstarke Paket- und Datenverarbeitung und Anwendungskontrolle und einen effizienten Bedrohungsschutz.

Die RFDPI-Engine von SonicWall scannt jedes einzelne Paket und jedes einzelne Byte über sämtliche Ports hinweg. Damit sorgt sie für eine umfassende Content-Kontrolle des gesamten Datenstroms bei hoher Performance und minimalen Latenzzeiten. Diese Technologie ist Proxy-Designs mit Reassemblierung, bei denen Sockets an Anti-Malware-Programme gekoppelt werden, weit überlegen. Hier kommt es immer wieder zu einer ineffizienten Verarbeitung und zu Socket-Memory-Thrashing, was zu hoher Latenz, verminderter Leistung und Beschränkungen bei der Dateigröße führt.

Die RFDPI-Engine dagegen prüft den kompletten Inhalt, um verschiedene Formen von Malware abzuwehren, bevor sie in das Netzwerk gelangen können, und bietet Schutz vor neuen Bedrohungen – ganz ohne Einschränkungen bei Dateigröße, Performance oder Latenzzeit.

Dank vollständiger Entschlüsselung und Prüfung von TLS-/SSL-verschlüsseltem Verkehr und nicht proxyfähigen Anwendungen bietet sie außerdem umfassenden Schutz unabhängig von Übertragung und Protokoll. Alle Pakete (Header und Datenteil) werden gründlich geprüft. Dabei sucht die Engine nach Protokollverstößen, Bedrohungen, Zero-Days, Eindringversuchen und sogar nach definierten Kriterien zur Erkennung und Abwehr von Angriffen, die sich im verschlüsselten Datenverkehr verstecken. Außerdem verhindert sie die Ausbreitung von Infektionen und unterbindet Command-and-Control(C&C)-Kommunikation sowie das Herausschleusen vertraulicher Daten. Eine umfassende Kontrolle erlauben Auswahl- und Ausschlussregeln, mit denen sich festlegen lässt, welcher Verkehr entschlüsselt und geprüft werden soll, um bestimmte Compliance-Anforderungen in Organisationen und/oder rechtliche Vorgaben zu erfüllen.

Durch die Analyse des Anwendungsverkehrs lässt sich arbeitsrelevanter und nicht arbeitsrelevanter Traffic in Echtzeit anzeigen und mit effektiven Regeln auf Anwendungsebene kontrollieren. Die Anwendungskontrolle kann sowohl nach Benutzer als auch nach Gruppe sowie mit Zeitplänen und Ausnahmelisten durchgeführt werden. Alle Anwendungs-, Intrusion-Prevention- und Malware-Signaturen werden laufend vom SonicWall Capture Labs Threat Research-Team aktualisiert. Darüber hinaus bietet SonicOS – ein spezielles, hoch entwickeltes Betriebssystem – integrierte Tools für die Identifizierung und Kontrolle benutzerdefinierter Anwendungen.

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

SuperMassive 9000 Series

Vorteile:

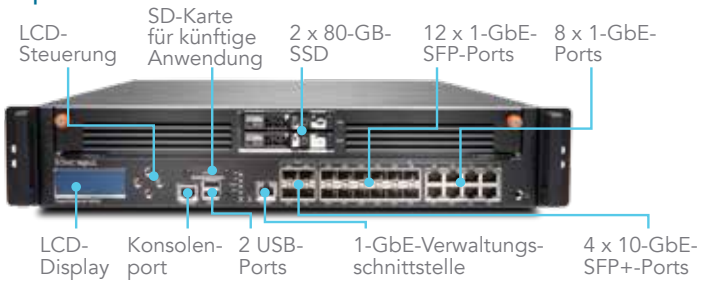
- Umfassende Prävention von Sicherheitslücken mit High-Performance-Intrusion-Prevention, cloudbasiertem Sandboxing und Malware-Schutz bei minimalen Latenzzeiten
- Umfassende, granulare Anwendungsidentifizierung, -kontrolle und -visualisierung
- Identifizierung und Abwehr verborgener Bedrohungen durch Entschlüsselung und Prüfung von TLS-/SSL-/SSH-verschlüsseltem Verkehr ohne Performanceprobleme
- Skalierung der Sicherheitsperformance für Datencenter mit 10/40 GBit/s
- Anpassung an höhere Servicelevels sowie Schutz und hohe Verfügbarkeit von Netzwerkservices und -ressourcen

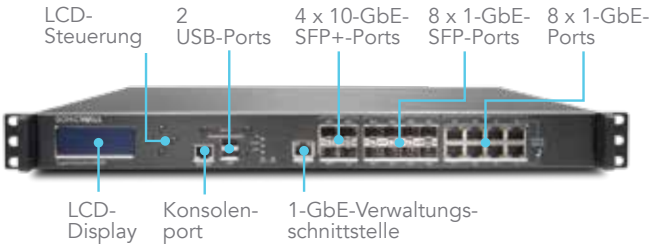
Partner Enabled Services
Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Unsere SonicWall Advanced Services Partner bieten Ihnen erstklassige Professional Services. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

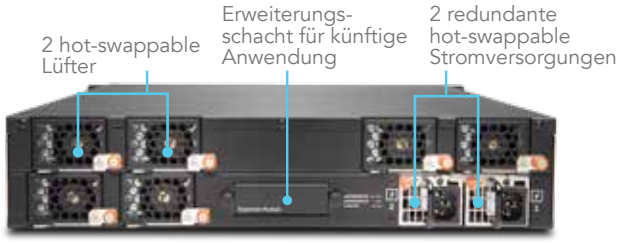
Überblick über die SuperMassive Series

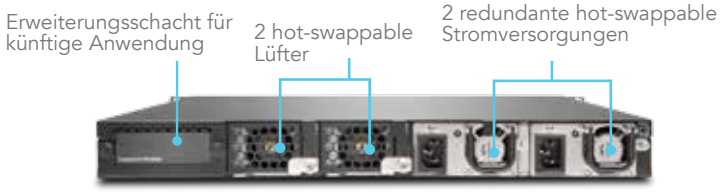
Die SonicWall SuperMassive 9000 Series verfügt über 4 x 10-GbE-SFP+-, bis zu 12 x 1-GbE-SFP- und 8 x 1-GbE-Kupfer-Schnittstellen und 1-GbE-Verwaltungsschnittstellen. Zudem enthält sie einen Erweiterungsanschluss für weitere 2 x 10-GbE-SFP+-Schnittstellen (für künftige Releases). Die 9000 Series bietet hot-swappable Lüftermodule und Stromversorgungen.

SuperMassive 9000 Series







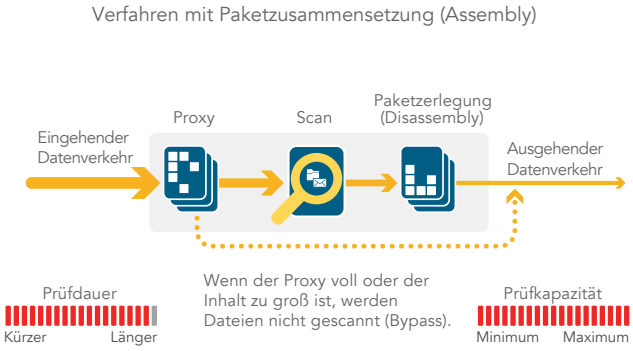


Technische Daten	9200	9400	9600	9800
Prozessorkerne	24	32	32	64
Firewall-Durchsatz	15 GBit/s	20 GBit/s	20 GBit/s	31,8 GBit/s
Application-Inspection-Durchsatz	5 GBit/s	10 GBit/s	11,5 GBit/s	23 GBit/s
Intrusion-Prevention-System(IPS)-Durchsatz	5 GBit/s	10 GBit/s	11,5 GBit/s	21,3 GBit/s
Anti-Malware-Inspection-Durchsatz	3,5 GBit/s	4,5 GBit/s	5 GBit/s	11 GBit/s
Max. Anzahl von DPI-Verbindungen	1,5 Mio.	1,5 Mio.	2,0 Mio.	8,0 Mio.
Implementierungsmodi	**9200**	**9400**	**9600**	**9800**
L2-Bridge-Modus	Ja	Ja	Ja	Ja
Wire-Modus	Ja	Ja	Ja	Ja
Gateway-/NAT-Modus	Ja	Ja	Ja	Ja
Tap-Modus	Ja	Ja	Ja	Ja
Transparenter Modus	Ja	Ja	Ja	Ja

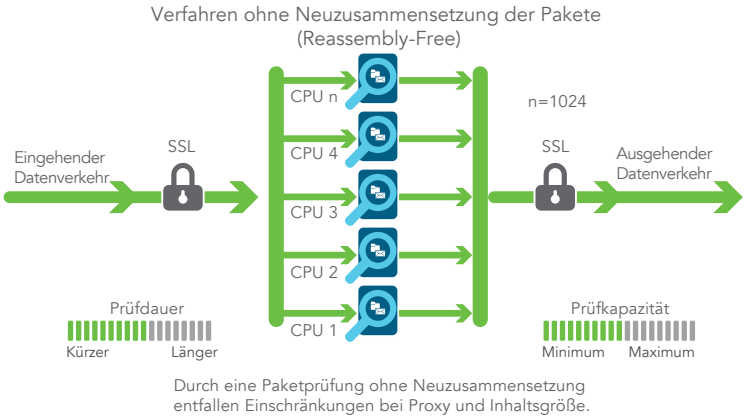
Reassembly-Free Deep Packet Inspection-Engine

Bei der RFDPI-Engine handelt es sich um ein Single-Pass-Prüfsystem mit niedriger Latenz, das streambasierte bidirektionale Verkehrsanalysen in Hochgeschwindigkeit durchführt, um Eindringversuche und Malware zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig von Port oder Protokoll und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy. Dabei prüft die proprietäre Engine die Payload von Datenströmen, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren. Durch die RFDPI-Engine wird der Netzwerkverkehr mehrfach umfassend normalisiert und entschlüsselt. Auf diese Weise lassen sich raffinierte Verschleierungs- und Umgehungsmethoden neutralisieren, die darauf abzielen, Erkennungsmechanismen zu stören und bösartigen Code in das Netzwerk einzuschleusen.

Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. TLS-/SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung mehrerer Signaturendatenbanken analysiert: Eindringversuche, Malware, Botnets 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

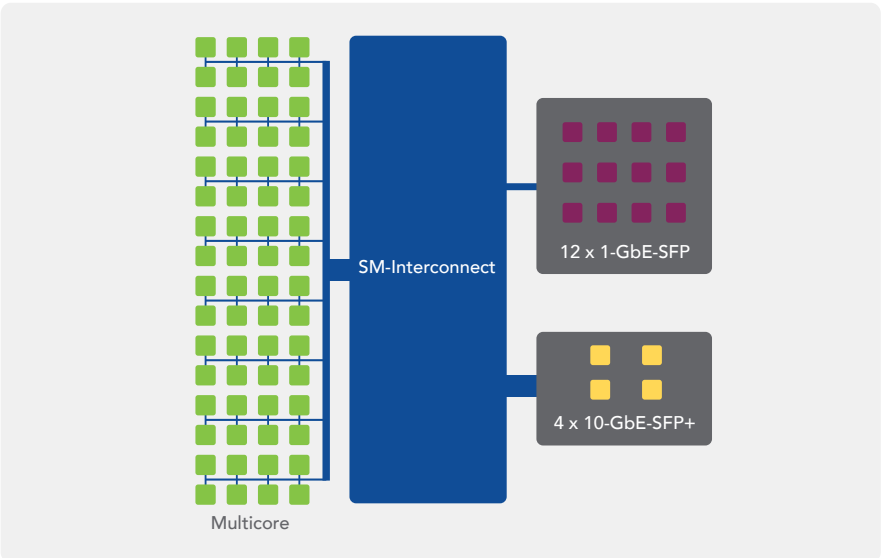


Streambasierte SonicWall-Architektur

Erweiterbare Architektur für höchste Skalierbarkeit und Performance

Die RFDPI-Engine wurde speziell so entwickelt, dass Sicherheitsprüfungen mit hohen Durchsatzraten durchgeführt werden können. Auf diese Weise wird den Anforderungen der parallelen Verarbeitung sowie dem ständig wachsenden Netzwerkverkehr Rechnung getragen. Diese Architektur ermöglicht eine parallele Verarbeitung und lässt sich in Kombination mit Multicore-Prozessoren optimal skalieren. Eine effektive Deep Packet Inspection (DPI)-Prüfung ist so auch bei hohen Verkehrslasten gewährleistet. Die SuperMassive-Plattform arbeitet mit Prozessoren, die im Gegensatz zum x86 für die Verarbeitung von Paketen, verschlüsselten Daten sowie Netzwerkverkehr optimiert sind und dabei gleichzeitig Flexibilität und Programmierbarkeit vor Ort garantieren – ASIC-Systeme können da nicht mithalten.

Diese Flexibilität ist besonders wichtig, wenn neue Updates zu Code und Verhalten nötig sind, um sich vor neuen Angriffen zu schützen, die innovative und technisch ausgefeiltere Erkennungsmethoden erfordern. Ein weiteres einzigartiges Merkmal der Plattform ist, dass sie jeden Systemkern für den Aufbau neuer Verbindungen nutzen kann. Dies bietet höchste Skalierbarkeit und ermöglicht eine bessere Bewältigung von Verkehrsspitzen. Mit diesem Ansatz lassen sich extrem hohe Geschwindigkeiten beim Aufbau neuer Sitzungen (neue Verbindungen/Sekunde) mit aktivierter Deep Packet Inspection erreichen – eine entscheidende Kenngröße, die in Datencentern häufig zu Engpässen führt.



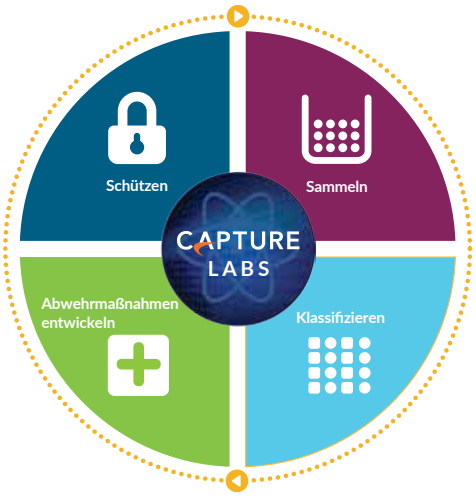
SONICWALL®

Capture Labs

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

Kunden mit Next-Generation-Firewalls von SonicWall, die mit den neuesten Sicherheitsfunktionen ausgestattet sind, erhalten rund um die Uhr Updates zu den aktuellsten Bedrohungen. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen. Die Signaturen auf den Appliances bieten Schutz vor einer breiten Palette an Bedrohungen. Eine einzige Signatur deckt dabei bis zu mehrere Zehntausend Einzelbedrohungen ab.

Zusätzlich zu den Abwehrmechanismen auf der Appliance bieten die SuperMassive-Firewalls auch Zugang zu SonicWall CloudAV[1]. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um mehrere Millionen Signaturen erweitert, wobei jährlich weitere Millionen dazukommen. Die Firewall greift über ein proprietäres, schlankes Protokoll auf die CloudAV-Datenbank zu, um die Prüfmöglichkeiten auf der Appliance zu erweitern. Mit Capture Advanced Threat Protection[1], einer cloudbasierten Multi-Engine-Sandbox, können Organisationen verdächtige Dateien und verdächtigen Code in einer isolierten Umgebung untersuchen, um raffinierte Bedrohungen wie Zero-Day-Angriffe zu stoppen.



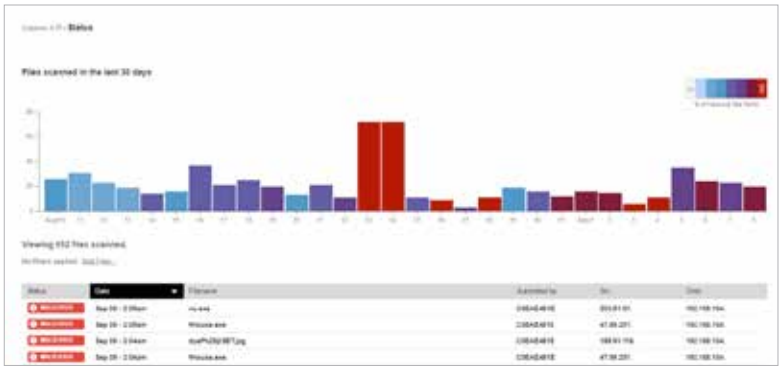
[1]*Erfordert zusätzliches Abo.*

Schutz vor raffinierten Bedrohungen

Beim SonicWall Capture Advanced Threat Protection-Service[1] handelt es sich um eine cloudbasierte Multi-Engine-Sandbox, die den Firewall-Bedrohungsschutz erweitert, um Zero-Day-Bedrohungen zu erkennen und abzuwehren. Verdächtige Dateien werden zur Analyse in die Cloud übertragen und können am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist. Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus und analysiert dessen Verhalten. Wird eine Datei als bösartig identifiziert, erstellt der Capture-Service umgehend einen Hash. Später erhalten die Firewalls eine Signatur, um Folgeangriffe zu verhindern.

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

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



SONICWALL

Application-Intelligence und Anwendungskontrolle

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

SonicWall Application Traffic Analytics[1] liefert detaillierte Informationen zum Anwendungsverkehr, zur Bandbreitennutzung sowie zu Sicherheitsbedrohungen und bietet leistungsstarke Troubleshooting- und Forensik-Funktionen. Sichere Single-Sign-on(SSO)-Funktionen sorgen außerdem für mehr Benutzerfreundlichkeit, erhöhen die Produktivität und reduzieren die Support-Anfragen. Eine intuitive webbasierte Oberfläche vereinfacht die Verwaltung der Application-Intelligence- und Anwendungskontrollfunktionen.

Globales Management und Reporting

Stark reglementierten Organisationen, die eine komplett aufeinander abgestimmte Security-Governance-, Compliance- und Risikomanagement-Strategie benötigen, bietet das optionale SonicWall Global Management System[1] (GMS®) eine einheitliche, sichere und erweiterbare Plattform, um SonicWall-Firewalls, drahtlose Access-Points und Switches mit einem korrelierten und prüfbaren Workstream-Prozess zu verwalten. Mit GMS können Unternehmen die Verwaltung ihrer Sicherheitsappliances unkompliziert konsolidieren, Administration und Fehlerbehebung vereinfachen und alle betrieblichen Aspekte der Sicherheitsinfrastruktur steuern. Unter anderem bietet die Plattform zentralisierte Richtlinienverwaltung und -durchsetzung, Echtzeit-Ereignisüberwachung, Benutzeraktivitäten, Anwendungsidentifizierung, Datenstromanalyse und -forensik sowie Compliance- und Audit-Reporting etc. Dank einer Funktion zur Workflow-Automatisierung können Unternehmen mit GMS zudem auch alle Änderungen an ihren Firewalls effektiv verwalten. Mithilfe der GMS-Workflow-Automatisierung können alle Unternehmen geeignete Firewall-Regeln flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit Compliance-Vorgaben implementieren.

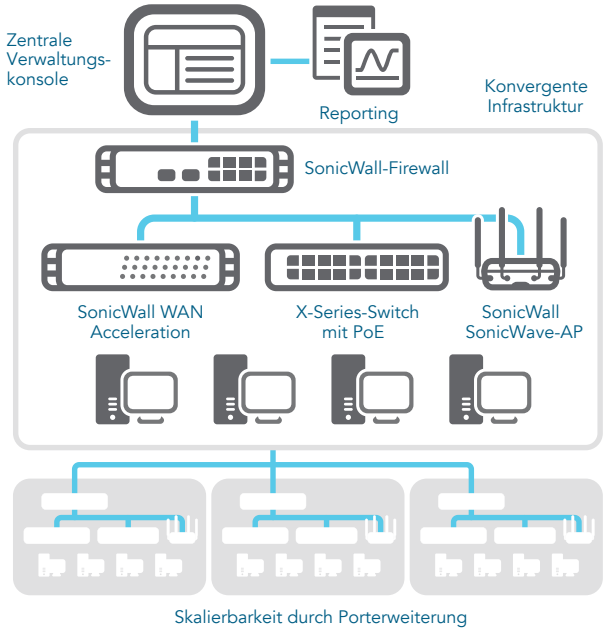
Dank GMS lässt sich die Netzwerksicherheit einheitlich auf Geschäftsprozesse und Servicelevel abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, statt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt.

[1] *Erfordert zusätzliches Abo.*

SonicWall GMS: zuverlässige Einhaltung von Compliance-Vorgaben

Vorteile

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



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 SuperMassive Series unterstützt die Hochverfügbarkeitsmodi Active/Passive (A/P) mit State-Synchronisierung, Active/Active (A/A)-DPI und Active/Active-Clustering. Beim Active/Active-DPI-Modus wird die Deep Packet Inspection-Last an die Kerne der passiven Appliance weitergegeben, um den Durchsatz zu erhöhen.
Schutz vor DDoS-/DoS-Angriffen	Dank SYN-Flood-Schutz lassen sich DoS-Angriffe mit Layer-3-SYN-Proxy- und Layer-2-SYN-Blacklisting-Technologien abwehren. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsgeschwindigkeit vor DoS-/DDoS-Angriffen schützen.
IPv6-Unterstützung	Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) hat gerade erst begonnen. Mit der neuesten Version SonicOS 6.2 unterstützt die Hardware Filtering- und Wire-Implementierungsmodi.
Flexible Implementierungsoptionen	Die SuperMassive Series lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden. Regelbasiertes Routing sorgt für das Erstellen von protokollbasierten Routen für die Umleitung des Datenverkehrs zu einer bevorzugten WAN-Verbindung mit Failback-Möglichkeit auf ein sekundäres WAN bei einem Stromausfall.
Verbesserte QoS (Quality of Service)	Garantierte Unterstützung kritischer Datenübertragung dank 802.1p und DSCP-Tagging sowie Remapping von VoIP-Datenverkehr im Netzwerk.
H.323-Gatekeeper- und SIP-Proxy-Unterstützung	Blockieren von Spam-Anrufen, da alle eingehenden Anrufe vom H.323-Gatekeeper oder SIP-Proxy autorisiert und authentifiziert werden müssen.
Verwaltung einzelner und hintereinandergeschalteter Dell X-Series-Network-Switches	Verwaltung der Sicherheitseinstellungen zusätzlicher Ports, einschließlich Portshield, HA, POE und POE+ über eine einzige Konsole mithilfe des Firewall-Management-Dashboards für Dells X-Series-Network-Switch.
Biometrische Authentifizierung	Unterstützung von Authentifizierungsmethoden für Mobilgeräte, bei denen eine Duplizierung oder Weitergabe nicht ohne Weiteres möglich ist, wie z. B. bei der Fingerabdruckerkennung. So lässt sich die Identität des Nutzers auf sichere Weise prüfen, bevor ein Zugriff auf das Netzwerk gewährt wird.
Offene Authentifizierung und Social Login	Erlaubt Gastbenutzern das Einloggen mit ihren Anmeldedaten aus sozialen Netzwerken wie Facebook, Twitter oder Google+ und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung.
Authentifzierung für mehrere Domänen	Erlaubt eine einfache und schnelle Verwaltung von Sicherheitsregeln über sämtliche Netzwerkdomänen hinweg. Verwaltung individueller Regeln für einzelne Domänen oder Domänengruppen.

Management und Reporting	
Funktion	Beschreibung
Global Management System[1] (GMS)	SonicWall GMS ermöglicht es, über eine einzige Verwaltungsschnittstelle mit intuitiver Oberfläche mehrere SonicWall-Appliances zu überwachen und zu konfigurieren und Berichte zu erstellen. Dies reduziert nicht nur die Kosten, sondern auch die Komplexität bei der Verwaltung.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche beschleunigt und vereinfacht die Konfiguration, erlaubt eine umfassende Befehlszeilenschnittstelle und bietet Support für SNMPv2/3.
Berichte zum IPFIX-/NetFlow-Datenstrom	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Unterstützt wird auch die Berichterstellung mit Tools wie SonicWall Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben.

Funktionen

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.
VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPSec-VPN kann die SuperMassive Series als VPN-Konzentrator für Tausende großer Standorte, Zweigniederlassungen oder Home-Offices eingesetzt werden.
Remote-Zugriff per SSL-VPN- oder IPSec-Client	Durch Einsatz der clientlosen SSL-VPN-Technologie oder eines leicht zu verwaltenden IPSec-Clients ist der unkomplizierte Zugriff auf E-Mails, Dateien, Rechner, Intranet-Sites und Anwendungen von zahlreichen unterschiedlichen Plattformen möglich.
Redundantes VPN-Gateway	Mit mehreren WANs lässt sich ein primäres und sekundäres VPN konfigurieren, um ein einfaches, automatisches Failover und Failback für alle VPN-Sitzungen zu ermöglichen.
Routenbasiertes VPN	Bei Ausfall eines temporären VPN-Tunnels wird der Datenverkehr reibungslos über alternative Verbindungen zwischen Endgeräten umgeleitet. Dieses dynamische Routing über VPN-Links sorgt für eine hohe Ausfallsicherheit.

Content- bzw. kontextorientierte Sicherheitsfunktionen	
Funktion	Beschreibung
Nachverfolgung der Benutzeraktivitäten	Bereitstellung von Informationen zur Benutzerkennung und -aktivität, die auf der nahtlosen SSO-Integration für AD/LDAP/Citrix[1]/ Terminal Services[1] sowie umfassenden DPI-Daten basieren.
Identifizierung des Datenverkehrs nach Ländern mittels Geo-IP	Identifizierung und Kontrolle des Netzwerkverkehrs aus bestimmten Ländern 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.
DPI-Filterung nach regulären Ausdrücken	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern.

Capture Advanced Threat Protection[1]	
Funktion	Beschreibung
Multi-Engine-Sandbox	Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus, analysiert dessen Verhalten und macht bösartige Aktivitäten transparent.
Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus	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.
Analyse unterschiedlichster Dateitypen	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 und Multi-Browser-Umgebungen.
Schnelle Implementierung von Signaturen	Wird eine Datei als bösartig identifiziert, so wird innerhalb von 48 Stunden eine Signatur auf Firewalls mit SonicWall Capture-Abos aufgespielt und in die GRID-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[1]	
Funktion	Beschreibung
TLS-/SSL-Entschlüsselung und -Prüfung	Proxylose On-the-Fly-Entschlüsselung und -Prüfung von SSL-/TLS-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im TLS-/SSL-verschlüsselten Verkehr lauern. Dieser Service ist bei allen Modellen in den Sicherheitsabonnements 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[1]	
Funktion	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes Intrusion-Prevention-System (IPS) nutzt Signaturen und andere Abwehrmechanismen, um Paket-Payloads auf Schwachstellen und Exploits zu prüfen, und deckt dabei eine Vielzahl an Angriffen und Schwachstellen ab.
Automatische Signatur-Updates	Das SonicWall Threat Research-Team analysiert kontinuierlich Bedrohungen und sorgt für die ständige Aktualisierung einer umfassenden Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Verbesserter Schutz vor internen Bedrohungen durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Intrusion-Prevention. Dies verhindert, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten.
Erkennen und Blockieren von Command-and-Control(CnC)-Aktivitäten durch Botnets	Erkennen und Blockieren von Command-and-Control-Verkehr, der von Bots im lokalen Netzwerk ausgeht und an IPs und Domänen geleitet wird, die nachweislich Malware verbreiten oder bekannte CnC-Punkte sind.
Erkennen und Verhindern von Protokollmissbrauch/-anomalien	Erkennen und Verhindern von Angriffen, die Protokolle missbrauchen, um unbemerkt am IPS vorbeizukommen.
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.

Funktionen

Bedrohungsschutz[1]	
Funktion	Beschreibung
Malware-Schutz am Gateway	Die RFDPI-Engine prüft den gesamten Verkehr auf Viren, Trojaner, Keylogger und andere Malware in Dateien unbegrenzter Größe und über alle Ports und TCP-Streams hinweg. Die Prüfung erfolgt sowohl in ein- als auch ausgehender Richtung sowie innerhalb von Zonen.
CloudAV-Malware-Schutz	Eine kontinuierlich aktualisierte Datenbank mit 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 und Anwendungskontrolle[1]	
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[1]	
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[1]	
Funktion	Beschreibung
Mehrstufiger Schutz	Die Firewall ist die erste Verteidigungsstufe am Netzwerkrand. Zusammen mit dem Endpunktschutz verhindert sie das Eindringen von Viren über Laptops, USB-Sticks und andere ungeschützte Systeme.
Option für automatisierte Durchsetzung	Es wird sichergestellt, dass auf jedem Computer, der auf das Netzwerk zugreift, die neueste Version der Signaturen für Viren- und Spyware-Schutz installiert und aktiviert ist. Somit entfallen die Kosten, die typischerweise für die Verwaltung von Desktop-Lösungen für Viren- und Spyware-Schutz entstehen.
Option für automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz werden automatisch und netzwerkweit auf jedem Rechner installiert und bereitgestellt, sodass der administrative Mehraufwand minimiert wird.
Ständig aktiver, automatischer Virenschutz	Der Viren- und Spyware-Schutz wird häufig aktualisiert und transparent auf allen Desktop-PCs und Dateiservern bereitgestellt. Das sorgt für höhere Endbenutzerproduktivität und reduziert den Aufwand für die Sicherheitsverwaltung.
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.

[1] *Erfordert zusätzliches Abo.*

Die Funktionen im Überblick

Firewall

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

SSL-/SSH-Entschlüsselung und -Prüfung[2]

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

Capture Advanced Threat Protection[2]

- Cloudbasierte 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[2]

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granularer IPS-Regelsatz
- GeoIP-Durchsetzung
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[2]

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

Anwendungsidentifizierung[2]

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

Filterung von Webinhalten[2]

- URL-Filtering
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Kategorien
- 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

- Dynamische LAG mittels LACP
- PortShield
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller[1]
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation (statisch und dynamisch)
- Port-Redundanz
- Hochverfügbarkeitsmodus A/P mit State-Sync
- A/A-Clustering
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge-, Wire-/Virtual-Wire-, Tap-, NAT-Modus
- 3G-/4G-WAN-Failover (nicht auf der SuperMassive 9800)
- 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
- DPI für VoIP-Datenverkehr
- 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
- Verwaltung von Switches der Dell N-Series und X-Series[1]

[1] *Nicht auf der SuperMassive 9800 unterstützt.*
[2] *Erfordert zusätzliches Abo.*

SONICWALL®

SuperMassive 9000 Series – Systemdaten

Firewall allgemein	9200	9400	9600	9800
Betriebssystem	SonicOS			
Security-Prozessor-Cores	24	32		64
Schnittstellen	4 x 10-GbE-SFP+, 8 x 1-GbE-SFP, 8 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole			4 x 10-GbE-SFP+, 12 x 1-GbE-SFP, 8 x 1-GbE, 1-GbE-Verwaltungsschnittstelle, 1 Konsole
Speicher (RAM)	8 GB	16 GB	32 GB	64 GB
Speicher	Flash			2 x 80-GB-SSD, Flash
Erweiterung	1 Erweiterungssteckplatz (Rückseite)*, SD-Karte*			
Verwaltung	CLI, SSH, GUI, GMS			
SSO-Benutzer	80.000	90.000	100.000	110.000
Maximal unterstützte Anzahl von Access-Points	128			-
Logging	Analyzer, lokale Logdatei, Syslog			
Hochverfügbarkeit	Active/Passive mit State-Sync, Active/Active-DPI mit State-Sync			
Firewall-/VPN-Performance	**9200**	**9400**	**9600**	**9800**
Firewall-Inspection-Durchsatz[1]	15 GBit/s	20 GBit/s	20 GBit/s	31,8 GBit/s
Threat-Prevention-Durchsatz[2]	3 GBit/s	4,4 GBit/s	4,5 GBit/s	10,5 GBit/s
Application-Inspection-Durchsatz[2]	5 GBit/s	10 GBit/s	11,5 GBit/s	23 GBit/s
IPS-Durchsatz[2]	5 GBit/s	10 GBit/s	11,5 GBit/s	21,3 GBit/s
Anti-Malware-Inspection-Durchsatz[1]	3,5 GBit/s	4,5 GBit/s	5,0 GBit/s	11 GBit/s
IMIX-Durchsatz	4,4 GBit/s	5,5 GBit/s	5,5 GBit/s	7,3 GBit/s
Durchsatz bei SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	1,0 GBit/s	2,0 GBit/s	2,0 GBit/s	3,5 GBit/s
VPN-Durchsatz[3]	5 GBit/s	10 GBit/s	11,5 GBit/s	14,3 GBit/s
Verbindungen pro Sekunde	100.000/Sek.	130.000/Sek.	130.000/Sek.	229.000/Sek.
Maximale Anzahl von Verbindungen (SPI)	5,0 Mio.	7,5 Mio.	10,0 Mio.	20,0 Mio.
Maximale Anzahl von Verbindungen (DPI)	1,5 Mio.	1,5 Mio.	2,0 Mio.	8,0 Mio.
DPI-SSL-Verbindungen[6] (max.)	8.000 (15.500[6])	10.000 (17.500[6])	12.000 (22.500[6])	400.000
VPN	**9200**	**9400**	**9600**	**9800**
Site-to-Site-VPN-Tunnel		10.000		25.000
IPSec-VPN-Clients (max.)	2.000 (4.000)	2.000 (6.000)	2.000 (10.000)	
SSL-VPN-NetExtender-Clients (max.)	2 (3.000)	2 (3.000)	50 (3.000)	50 (3.000)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256 Bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v			
Routenbasiertes VPN	RIP, OSPF			
Networking	**9200**	**9400**	**9600**	**9800**
IP-Adressenzuweisung	Statisch, DHCP-, PPPoE-, L2TP- und PPTP-Client, interner DHCP-Server, DHCP-Relay[4]			
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT, transparenter Modus			
VLAN-Schnittstellen	512			
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast			
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p			
Authentifizierung	LDAP (mehrere Domänen), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste[5], Citrix[5]			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Zertifikate	UC APL[4], ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[4], Common Criteria NDPP[4], ICSA Anti-Virus[4]			
Hardware	**9200**	**9400**	**9600**	**9800**
Stromversorgung	dual, redundant, hot-swappable, 300 W			dual, redundant, hot-swappable, 500 W
Lüfter	dual, redundant, hot-swappable			
Display	Front-LED-Display			
Eingangsspannung	100–240 VAC, 50–60 Hz			
Maximaler Stromverbrauch (W)	200			350
MTBF bei 25 °C in Stunden	188.719	187.702	186.451	126.144
MTBF bei 25 °C in Jahren	21,53	21,43	21,28	14,40
Formfaktor	Rackfähig (1 HE)			Rackfähig (2 HE)
Abmessungen	43,3 x 48,5 x 4,5 cm			9 x 60 x 43 cm
Gewicht	8,2 kg			18,38 kg
WEEE-Gewicht	10,4 kg			22,4 kg
Versandgewicht	13,3 kg			29,64 kg
Erfüllt folgende Standards/Normen	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico CoC nach UL, WEEE, REACH, ANATEL, BSMI, CU			
Umgebungstemperatur	15–40 °C			
Luftfeuchtigkeit	10–90 %, nicht kondensierend			

*[1] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren. [2] Messung des Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatzes mittels Industriestandard-HTTP-Performance-Test WebAvalanche von Spirent und Ixia-Test-Tools. Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen. [3] VPN-Durchsatz gemäß RFC 2544 unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte gemessen. [4] Trifft auf SuperMassive 9200, 9400 und 9600 zu. Die UC APL-Zertifizierung für die SuperMassive 9800 steht noch aus. [5] Unterstützung unter SonicOS 6.1 und 6.2. [6] Pro 125.000 ungenutzte DPI-Verbindungen steigt die Anzahl verfügbarer DPI-SSL-Verbindungen um 750. *Für künftige Anwendung. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.*

SONICWALL®

SuperMassive 9000 Series – Bestellinformationen

Produkt	Artikelnummer
SuperMassive 9800 Total Secure Advanced Edition (1 Jahr)	01-SSC-0312
SuperMassive 9600 Total Secure Advanced Edition (3 Jahre)	02-SSC-0410
SuperMassive 9400 Total Secure Advanced Edition (3 Jahre)	02-SSC-0409
SuperMassive 9200 Total Secure Advanced Edition (3 Jahre)	02-SSC-0408
SuperMassive 9200 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für SuperMassive 9200 (1 Jahr)	01-SSC-1570
Capture Advanced Threat Protection für SuperMassive 9200 (1 Jahr)	01-SSC-1575
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention und Content Filtering mit Support für 9200 (1 Jahr)	01-SSC-4172
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization für SuperMassive 9200 (1 Jahr)	01-SSC-4202
Content Filtering Premium Business Edition für 9200 (1 Jahr)	01-SSC-4184
Platinum-Support für SuperMassive 9200 (1 Jahr)	01-SSC-4178
SuperMassive 9400 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für SuperMassive 9400 (1 Jahr)	01-SSC-1580
Capture Advanced Threat Protection für SuperMassive 9400 (1 Jahr)	01-SSC-1585
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention und Content Filtering mit Support für 9400 (1 Jahr)	01-SSC-4136
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization für SuperMassive 9400 (1 Jahr)	01-SSC-4166
Content Filtering Premium Business Edition für 9400 (1 Jahr)	01-SSC-4148
Platinum-Support für SuperMassive 9400 (1 Jahr)	01-SSC-4142
SuperMassive 9600 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für SuperMassive 9600 (1 Jahr)	01-SSC-1590
Capture Advanced Threat Protection für SuperMassive 9600 (1 Jahr)	01-SSC-1595
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention und Content Filtering mit Support für 9600 (1 Jahr)	01-SSC-4100
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization für SuperMassive 9600 (1 Jahr)	01-SSC-4130
Content Filtering Premium Business Edition für 9600 (1 Jahr)	01-SSC-4112
Platinum-Support für SuperMassive 9600 (1 Jahr)	01-SSC-4106
SuperMassive 9800 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite: Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für SuperMassive 9800 (1 Jahr)	01-SSC-1183
Capture Advanced Threat Protection für SuperMassive 9800 (1 Jahr)	01-SSC-1188
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention und Content Filtering mit Support für 9800 (1 Jahr)	01-SSC-0809
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization für SuperMassive 9800 (1 Jahr)	01-SSC-0827
Content Filtering Premium Business Edition für 9800 (1 Jahr)	01-SSC-0821
Gold 24/7-Support für SuperMassive 9800 (1 Jahr)	01-SSC-0815
Module und Zubehör*	**Artikelnummer**
Systemlüfter für die SonicWall SuperMassive 9800 Series (FRU)	01-SSC-0204
AC-Stromversorgung für die SonicWall SuperMassive 9800 Series (FRU)	01-SSC-0203
Systemlüfter für die SonicWall SuperMassive 9000 Series (FRU)	01-SSC-3876
AC-Stromversorgung für die SonicWall SuperMassive 9000 Series (FRU)	01-SSC-3874
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Kupfermodul	01-SSC-9791
Management und Reporting	**Artikelnummer**
SonicWall GMS Software-Lizenz (10 Nodes)	01-SSC-3363
SonicWall GMS E-Class 24/7 Software Support für 10 Nodes (1 Jahr)	01-SSC-6514
SonicWall Scrutinizer Virtual Appliance mit Softwarelizenz für Flow Analytics-Modul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-3443
SonicWall Scrutinizer mit Softwarelizenz für Flow Analytics-Modul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-4002
SonicWall Scrutinizer mit Softwarelizenz für Advanced Reporting-Modul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-3773

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

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

© 2018 SonicWall Inc. ALLE RECHTE VORBEHALTEN. SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber.

Datasheet-SuperMassive-US-VG-MKTG4043