SONICWALL

SonicWall SuperMassive Series

Kompromissloser, leistungsstarker Next-Generation Firewall-Schutz für Ihr Enterprise-Netzwerk.

Die SuperMassive Series ist SonicWalls Next-Generation Firewall (NGFW) Plattform für große Netzwerke und sorgt für Skalierbarkeit, Zuverlässigkeit und tiefgreifende Sicherheit mit fast latenzfreier Multi-Gigabit-Geschwindigkeit.

Die SuperMassive Series wurde zur Erfüllung des Bedarfs von Großunternehmen, Regierungsbehörden, Schul-, Einzelhandels- und Gesundheitswesen sowie Dienstanbietern entwickelt und eignet sich ideal für den Schutz von verteilten Unternehmensnetzwerken, Rechenzentren und Dienstanbietern.

Mit einer Kombination aus SonicWalls SonicOS Betriebssystem, der patentierten* Reassembly-Free Deep Packet Inspection® (RFDPI) Technologie und einer massiven mehrkernigen, hochskalierbaren Architektur ermöglicht die SuperMassive 9000 Series branchenführende Anwendungskontrolle, Intrusion-Prevention, Malware-Schutz und TLS/SSL-Entschlüsselung und -Prüfung mit Multi-Gigabit-Geschwindigkeit. Bei der Entwicklung der SuperMassive Series wurde sorgfältig auf Leistung, Platzbedarf und Kühlung (Power, Space, Cooling, PSC) geachtet. Das Resultat ist eine in GBit/s branchenführende NGFW mit starker Performance und effizienter Datenverarbeitung, Anwendungskontrolle und Bedrohungsschutz.

Die SonicWall RFDPI-Engine scannt jedes Byte jedes Pakets auf allen Ports und inspiziert den gesamten Inhalt des gesamten Streams -- all das mit hoher Leistung und geringer Latenz. Diese Technologie ist weitaus besser als herkömmliche Proxy-Designs, die den Inhalt unter Verwendung von mit Anti-Malware-Programmen verankerten Sockets reassemblieren, wobei viele Ineffizienzen entstehen, z. B. durch Socket-Memory-Thrashing, was wiederum mit einer hohen Latenz, geringer Leistung und Begrenzung der Dateigrößen einhergeht. Die RFDPI-Engine liefert dagegen eine Inspektion des gesamten Inhalts, um verschiedene Formen von Malware zu eliminieren, bevor diese in das Netzwerk gelangen kann. Zugleich wird Schutz vor sich entwickelnden Bedrohungen geboten, allerdings ohne Einschränkungen in Bezug auf Dateigrößen, Performance oder Latenz.

Des Weiteren führt die RFDPI-Engine eine volle Entschlüsselung und Inspektion des TLS/SSL- und SSH-verschlüsselten Verkehrs sowie aller nicht-proxyfähigen Anwendungen durch, wodurch unabhängig vom Transport oder Protokoll für umfassenden Schutz gesorgt wird. Jedes Paket wird gründlich geprüft (Header und Daten), wobei nach Nichteinhaltung von Protokollen, Bedrohungen, Zero-Day-Angriffen, Eindringversuchen und sogar definierter Kriterien zum Erkennen und Verhindern von Angriffen, die im verschlüsselten Verkehr versteckt sein könnten, gesucht wird. Dadurch wird die Verbreitung von Bedrohungen sowie jegliche Command-and-Control(C&C)-Kommunikationen und das Herausschleusen von Daten verhindert. Eine umfassende Kontrolle wird durch Ein- und Ausschlussregeln ermöglicht, mit denen sich festlegen lässt, welcher Verkehr entschlüsselt und geprüft werden soll, um bestimmte Compliance-Anforderungen in Organisationen und/oder rechtliche Vorgaben zu erfüllen.

Anwendungsverkehr-Analytics ermöglichen die Identifizierung von produktivem und unproduktivem Anwendungsverkehr in Echtzeit. Der Verkehr kann dann durch leistungsstarke Regeln auf Anwendungsebene kontrolliert werden. Die Anwendungskontrolle kann auf Pro-Benutzer- oder Pro-Gruppenbasis erfolgen und Termine und Ausnahmelisten enthalten. Alle Anwendungs-, Intrusion-Prevention- und Malware-Signaturen werden laufend vom SonicWall Capture Labs Threat Research-Team aktualisiert. Darüber hinaus liefert das erweiterte zweckspezifisch entwickelte SonicOS Betriebssystem integrierte Tools für eine anwendungsspezifische Identifizierung und Kontrolle.

SuperMassive 9000 Series

Vorteile:

- Umfassende Abwehr von Bedrohungen sowie leistungsstarke Intrusion-Prevention, latenzarmer Malware-Schutz und Cloud-basiertes Sandboxing
- Komplette granulare Identifizierung, Kontrolle und Visualisierung von Anwendungen
- Aufeckung und Blockierung von versteckten Bedrohungen mit Entschlüsselung und Inspektion des TLS/SSL- und SSH-verschlüsselten Verkehrs ohne Beeinträchtigung der Performance
- Skalierung der Sicherheitsper–formance für 10/40 GBit/s Rechenzentren
- Anpassung an Service-Level-Änderungen und Sicherstellung, dass Netzwerkdienste und Ressourcen verfügbar und geschützt sind

Partner Enabled Services

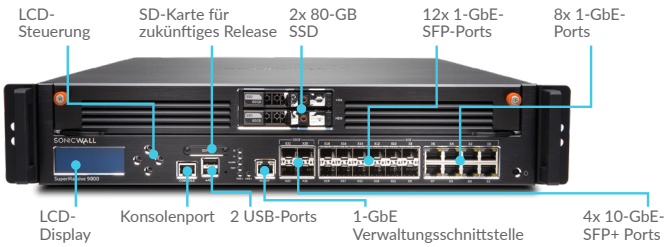
Brauchen Sie Hilfe bei der Planung, Einbindung oder Optimierung Ihrer SonicWall-Lösung? SonicWall Advanced Services Partners sind umfassend ausgebildet, um Ihnen erstklassigen professionellen Service zu bieten. Weitere Informationen finden Sie auf www.sonicwall.com/PES.

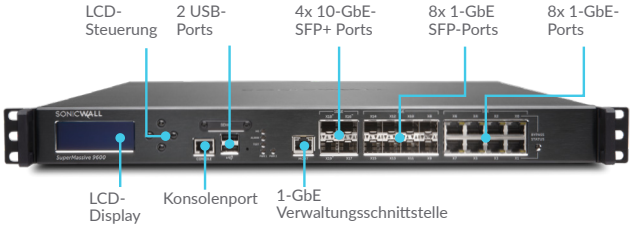
*U.S. Patente 7.310.815; 7.600.257; 7.738.380; 7.835.361

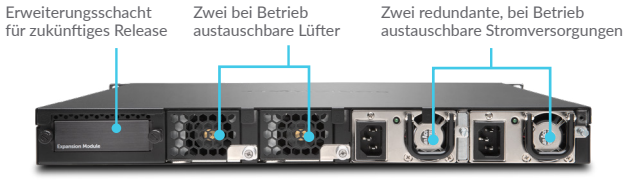
Produkte der Series

Die SonicWall SuperMassive 9000 Series bietet 4x 10-GbE SFP+, bis zu 12x 1-GbE SFP, 8x 1-GbE Kupfer und 1 GbE Management-Schnittstellen sowie einen Erweiterungsanschluss für weitere 2x 10-GbE SFP+ Schnittstellen (zukünftiges Release). Die 9000 Series enthält bei Betrieb austauschbare Lüftermodule und Netzteile.

SuperMassive 9000 Series





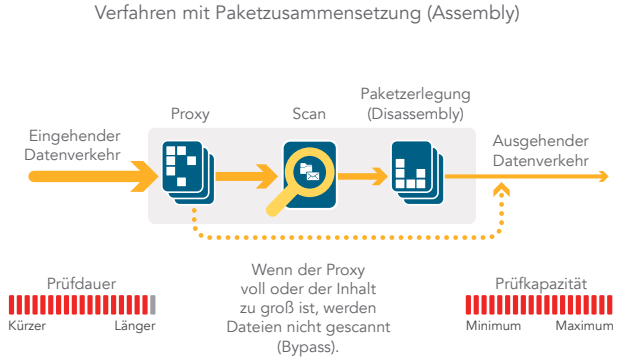


KAPAZITÄT	9200	9400	9600	9800
Prozessorkerne	24	32	32	64
Firewall-Durchsatz	15 GBit/s	20 GBit/s	20 GBit/s	31,8 GBit/s
Application-Inspection-Durchsatz	5 GBit/s	10 GBit/s	11,5 GBit/s	23 GBit/s
Intrusion-Prevention-System (IPS)-Durchsatz	5 GBit/s	10 GBit/s	11,5 GBit/s	21,3 GBit/s
Anti-Malware-Inspection-Durchsatz	3,5 GBit/s	4,5 GBit/s	5 GBit/s	11 GBit/s
Maximale Anzahl von DPI-Verbindungen	1,5 M	1,5 M	2,0 M	8,0 M
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
Transparent-Modus	Ja	Ja	Ja	Ja

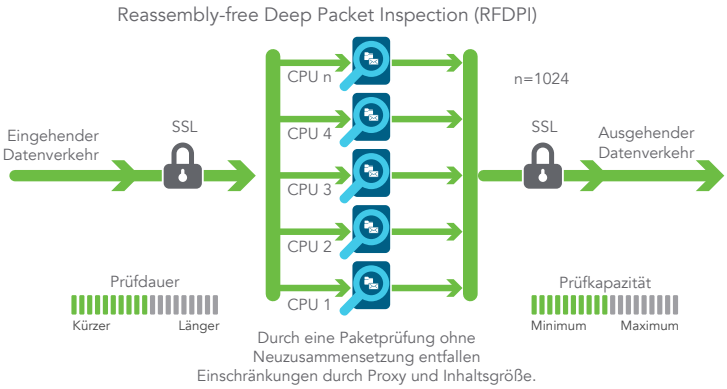
Reassembly-Free Deep Packet Inspection-Engine

Bei der RFDPI-Engine handelt es sich um ein Single-Pass-Prüfsystem mit niedriger Latenz, das streambasierte bidirektionale Verkehrsanalysen in Hochgeschwindigkeit durchführt, um Eindringversuche, Malware-Downloads zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig von Port oder Protokoll und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy. Die proprietäre RFDPI-Engine prüft die Payload von Datenströmen, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren. Zudem wird der Netzwerkverkehr mehrfach umfassend normalisiert und entschlüsselt. Auf diese Weise lassen sich komplexe Verschleierungen und 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 mehrerer Signaturendatenbanken analysiert: Eindringversuche, Malware, Botnet und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall aktualisiert und mit diesen Datenbanken abgeglichen. Dabei wird geprüft, ob ein Angriff oder ein anderes sicherheitsrelevantes Ereignis eintritt. Ist dies der Fall, wird eine vordefinierte Aktion ausgeführt. In den meisten Fällen wird die Verbindung beendet und es werden entsprechende Logging- und Benachrichtigungs-Events erzeugt. Die Engine kann jedoch auch nur für Prüfungen eingerichtet werden oder bei aktivierter Anwendungserkennung kann sie so konfiguriert werden, dass für den restlichen Anwendungsverkehr Layer-7-Bandbreitenverwaltungsdienste bereitgestellt werden, sobald die Anwendung erkannt wird.



Proxybasierte Architektur von Mitbewerberlösungen

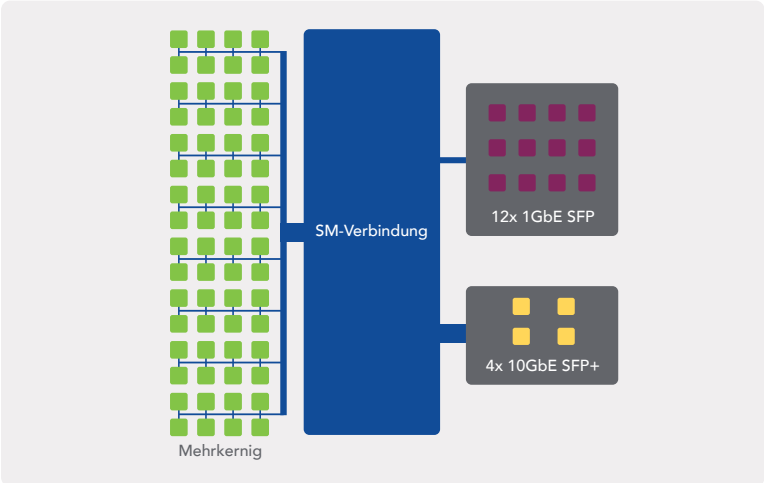


Streambasierte SonicWall Architektur

Erweiterbare Architektur für maximale Skalierbarkeit und Performance

Bei der Entwicklung der RFDPI-Engine lag besonderer Schwerpunkt auf der Bereitstellung eines leistungsstarken Sicherheitsscans, der dem inhärent parallelen und konstant wachsenden Netzwerkverkehr gerecht werden konnte. In Kombination mit mehrkernigen Prozessorsystemen liefert diese parallelitätszentrische Softwarearchitektur eine perfekte Skalierbarkeit, um den Anforderungen der Deep Packet Inspection (DPI) bei hohem Verkehrsaufkommen gerecht werden zu können. Die SuperMassive-Plattform nutzt Prozessoren, die im Gegensatz zu x86-Prozessoren für Paket-, Crypto- und Netzwerkverarbeitung optimiert wurden, ohne die Flexibilität und Programmierbarkeit im Feld zu beeinträchtigen — eine Schwachstelle bei ASIC-Systemen.

Diese Flexibilität ist wichtig, wenn neuer Code und Verhaltens-Updates erforderlich sind, um vor neuen Angriffen zu schützen, für die aktualisierte und ausgefeiltere Erkennungsmethoden benötigt werden. Ein weiterer Aspekt des Plattformdesigns ist die einzigartige Fähigkeit zum Herstellen neuer Verbindungen auf jedem Kern im System. Dadurch wird eine ultimative Skalierbarkeit und eine optimierte Handhabung von Spitzenverkehrsaufkommen ermöglicht. Dieser Ansatz sorgt für extrem hohe Geschwindigkeiten beim Aufbau neuer Sitzungen (neue Verbindungen pro Sekunde) bei aktivierter Deep Packet Inspection — ein wichtiger Messwert, durch den in datenzentrischen Einbindungen oft Engpässe erkannt werden.

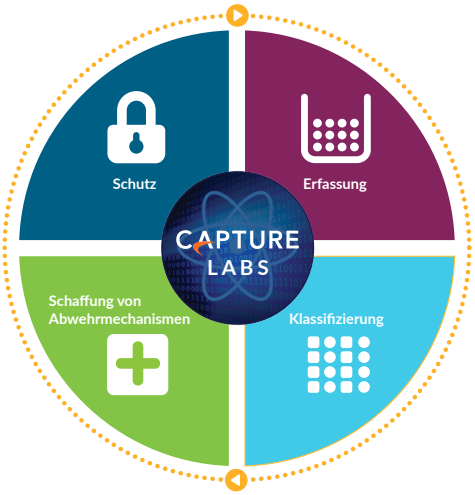


Capture Labs

Das dedizierte interne SonicWall Capture Labs Threat Research-Team erforscht und entwickelt Abwehrmechanismen, die in die Kunden-Firewalls implementiert werden, um einen topaktuellen Schutz zu gewährleisten. Das Team erfasst Bedrohungsinformationen aus mehreren Quellen, zum Beispiel aus unserem prämierten Netzwerk-Sandboxing-Service Capture Advanced Threat Protection sowie aus über 1 Million SonicWall Sensoren, die rund um den Globus verteilt sind und den Verkehr auf neuartige Bedrohungen überwachen. Für die Analyse setzt das Team Machine Learning ein und verwendet dazu SonicWalls Deep-Learning-Algorithmen für die Extraktion der DNA aus dem Code, um festzustellen, ob eine Verbindung zu irgendeiner bekannten Form von Schadcode besteht.

SonicWall NGFW-Kunden verfügen über die neuesten Sicherheitsfähigkeiten und erhalten kontinuierlich rund um die Uhr aktualisierten Bedrohungsschutz. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen. Die Signaturen auf den Appliances bieten Schutz vor einer großen Vielfalt an Attacken und decken Zehntausende verschiedener Bedrohungen mit nur einer Signatur ab.

Zusätzlich zu den Abwehrmechanismen auf der Appliance haben SuperMassive-Firewalls auch Zugang zur SonicWall CloudAV[1], durch die die lokal verfügbare Signaturendatenbank um mehrere zehn Millionen Signaturen erweitert wird. Dieser Datenbank werden jährlich mehrere Millionen Signaturen hinzugefügt. Die Firewall greift über ein proprietäres, schlankes Protokoll auf die CloudAV Datenbank zu, um die von der Appliance durchgeführte Inspektion zu unterstützen. Mit der Cloud-basierten Multi-Engine Sanbox Capture Advanced Threat Protection[1] können Organisationen verdächtige Dateien und Code in einem isolierten Umfeld untersuchen, um komplexe Bedrohungen, wie Zero-Day-Attacken, vorab zu erkennen und zu stoppen.



[1] *Erfordert zusätzliches Abo*

Schutz vor komplexen Bedrohungen

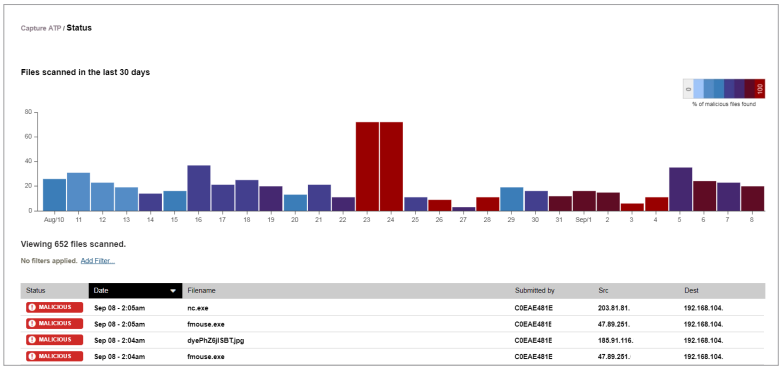
Herzstück der automatisierten SonicWall Lösung zur Echtzeitprävention von Sicherheitslücken sind zwei moderne Technologien für die Malware-Erkennung: Capture Advanced Threat Protection™ (Capture ATP) und Capture Security Appliance™ (CSa).

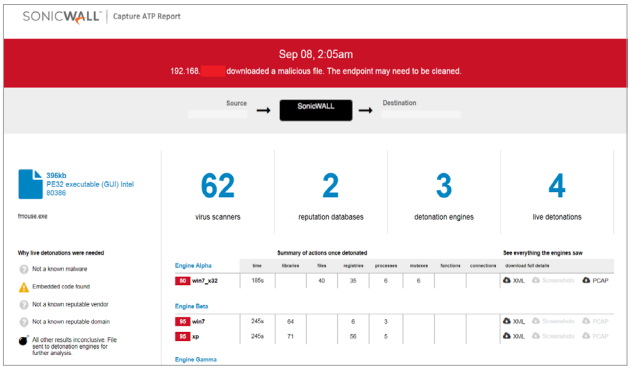
Capture ATP ist eine Cloud-basierte Multi-Engine-Sandbox-Plattform, die Real-Time Deep Memory Inspection™ (RTDMI), virtualisiertes Sandboxing, umfassende Systemsimulation und Analyse auf Hypervisor-Ebene beinhaltet. CSa ist eine On-Prem-Appliance mit RTDMI, die mithilfe von arbeitsspeicherbasierten statischen und dynamischen Verfahren schnellstens genaue Urteile erstellen kann. Beide Lösungen sorgen für einen erweiterten Bedrohungsschutz, indem sie in vielen verschiedenen SonicWall-Lösungen, z. B. in Next-Generation-Firewalls, Zero-Day-Bedrohungen erkennen und verhindern.

Verdächtige Dateien werden zur Analyse mittels Deep-Learning-Algorithmen in eine dieser Lösungen übertragen und können am Gateway gehalten werden, bis der Sicherheitsstatus geklärt ist. Bei Capture ATP werden die als bösartig identifizierten Dateien blockiert und sofort mit Hash-Code in die Capture ATP-Datenbank aufgenommen, damit alle Kunden weitere Angriffe dieser Art erkennen und blockieren können. Letztendlich werden diese Signaturen zur Schaffung einer statischen Abwehr an die Firewalls weitergeleitet. Die von CSa generierten Ergebnisse werden aus Datenschutz- und Compliance-Gründen nicht außerhalb Ihrer Organisation bekanntgegeben.

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

SonicWall Capture Client sorgt für einen umfassenden Endpunktschutz, indem Antivirentechnologien der nächsten Generation mit der Cloud-basierten Multi-Engine-Sandbox von SonicWall verbunden werden und optional in SonicWall Firewalls integriert werden können.

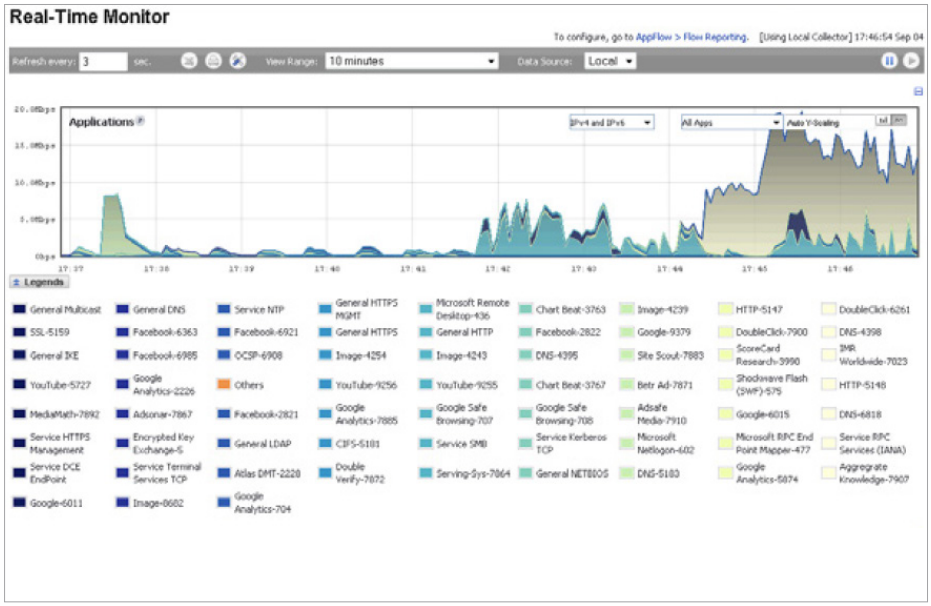




Application-Intelligence und Kontrolle

Durch Application-Intelligence werden Administratoren genau über den Anwendungsverkehr in ihrem Netzwerk informiert, damit sie auf Basis der geschäftlichen Priorität Anwendungskontrollen einteilen, unproduktive Anwendungen drosseln und potenziell gefährliche Anwendungen blockieren können. Verkehrsanomalien werden in Echtzeit visualisiert, sodass bei potenziellen ein- oder ausgehenden Bedrohungen sowie bei Performance-Engpässen sofortige Abhilfemaßnahmen eingeleitet werden können.

SonicWall Application Traffic Analytics[1] gibt Organisationen granularen Einblick in den Anwendungsverkehr, die Bandbreitennutzung und Sicherheitsbedrohungen sowie leistungsstarke Fehlersuche- und Forensikfunktionen. Darüber hinaus wird die Benutzererfahrung durch Single Sign-on (SSO) erleichtert, was gesteigerte Produktivität und weniger Anrufe beim Support zur Folge hat. Verwaltung und Kontrolle der Application-Intelligence werden durch eine intuitive webbasierte Benutzeroberfläche vereinfacht.



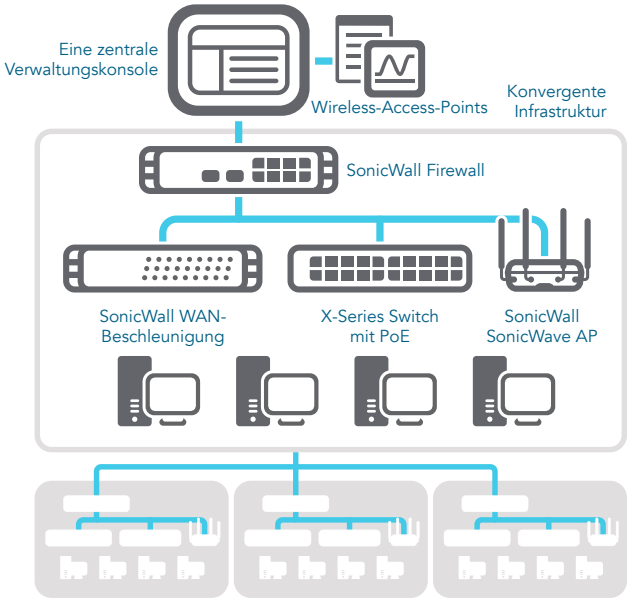
Globales Management und Reporting

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 für die Verwaltung von SonicWall Firewalls, Wireless-Access-Points und Switches über einen korrelierten und prüfbaren Workstream-Prozess. 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, einen Einblick in die Benutzeraktivitäten, Anwendungsidentifizierung, Datenstromanalyse und -forensik sowie Compliance- und Audit-Reporting. GMS erfüllt auch die für Großunternehmen geltenden Change-Management-Anforderungen für Firewalls, da diese Lösung den Workflow automatisiert. Dank der Workflow-Automatisierung können Unternehmen geeignete Firewall-Richtlinien flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit Compliance-Vorgaben implementieren und so alle Änderungen an ihren Firewalls effektiv verwalten. Mit GMS lässt sich die Netzwerksicherheit einheitlich auf Geschäftsprozesse und Servicelevel abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, anstatt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt.

SonicWall GMS Secure Compliance Enforcement

Vorteile

- Zentralisierte Verwaltung
- Fehlerfreies Richtlinien-Management
- Starke Zugangskontrolle
- Umfassende Audit-Trails
- PCI, HIPAA, SOX Berichtsvorlagen
- Reduzierte Betriebskosten



[1] *Erfordert zusätzliches Abo*

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 diese, um komplexe Bedrohungen wie Zero-Day-Angriffe, Insiderbedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv zu bekämpfen.
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die Firewall-Zugriffsregeln erfüllt werden.
Hochverfügbarkeit/Clustering	Die 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) ist noch nicht abgeschlossen. Mit dem neuesten SonicOS 6.2 unterstützt die Hardware Filterungs- 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 erstellt Routen auf Basis des Protokolls, um den Verkehr an eine bevorzugte WAN-Verbindung zu leiten, während bei einem Ausfall jederzeit ein Failback auf ein sekundäres WAN möglich ist.
Verbesserte QoS (Quality of Service)	Garantierte Unterstützung kritischer Datenübertragung dank 802.1p und DSCP-Tagging sowie Remapping von VoIP-Datenverkehr im Netzwerk.
H.323-Gatekeeper- und SIP-Proxy-Support	Blockieren von Spam-Anrufen, da alle eingehenden Anrufe vom H.323-Gatekeeper oder SIP-Proxy autorisiert und authentifiziert werden müssen.
Verwaltung einzelner und hintereinander geschalteter Switches der Dell X-Series	Verwaltung der Sicherheitseinstellungen zusätzlicher Ports, einschließlich Portshield, HA, POE und POE+ über eine zentrale Konsole mithilfe des Firewall-Management-Dashboards für Netzwerk-Switches der Dell X-Series.
Biometrische Authentifizierung	Unterstützung von Authentifizierungsmethoden für Mobilgeräte, bei denen eine Duplizierung oder Weitergabe nicht ohne Weiteres möglich ist, wie z. B. bei der Fingerabdruckerkennung. So lässt sich die Identität des Nutzers auf sichere Weise prüfen, bevor ein Zugriff auf das Netzwerk gewährt wird.
Offene Authentifizierung und Social Login	Erlaubt Gastbenutzern das Einloggen mit ihren Anmeldedaten aus sozialen Netzwerken wie Facebook, Twitter oder Google+ und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung.
Multi-Domain-Authentifizierung	Ermöglicht eine einfache und schnelle Verwaltung von Sicherheitsrichtlinien für alle Netzwerkdomänen. Verwaltung einzelner Richtlinien für eine Domäne oder eine Gruppe von Domänen.

MANAGEMENT UND REPORTING

Funktion	Beschreibung
Global Management System[1] (GMS)	SonicWall GMS überwacht, konfiguriert und protokolliert mehrere SonicWall Appliances über eine zentrale Verwaltungskonsole mit intuitiver Benutzeroberfläche, wodurch Verwaltungskosten und Komplexität reduziert werden.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche beschleunigt und vereinfacht die Konfiguration, erlaubt eine umfassende Befehlszeilenschnittstelle und bietet Support für SNMPv2/3.
IPFIX-/NetFlow Application Flow-Berichte	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung sowie die Berichterstellung mit Tools wie SonicWall Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen unterstützen, zu ermöglichen.

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-zu-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/Citrix1/ Terminal Services1 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.
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 eines weiten Bereichs von Dateitypen	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.

CAPTURE SECURITY APPLIANCE (CSa)

Funktion	Beschreibung
Compliance-zentrische Malware-Erkennung	Analysiert verdächtige Dateien in Ihrem eigenen Umfeld, ohne die Dateien oder Ergebnisse in die Cloud eines Drittanbieters zu setzen.
Eingebaute Integrationen	CSa unterstützt die Einbindung von vorkonfigurierten Integrationslösungen in andere Security-Lösungen (Firewalls und E-Mail-Sicherheit) von SonicWall.
Echtzeitnaher Schutz	SonicWalls patentierte RTDMI-Technologie ermöglicht eine schnelle Erkennung von bekannter und bisher unbekannter Malware, die dann von CSa bis zur Klärung des Sicherheitsstatus durch SonicWall Next-Generation-Firewalls blockiert werden kann.
Implementierung	CSa kann in einem privaten Netzwerk, das direkt mit einer einzelnen Edge-Firewall verbunden ist, konfiguriert werden und ist auch direkt über das Internet oder über das VPN von Filialen-Firewalls erreichbar.

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 verschlüsselten Verkehr lauern. Dieser Service ist bei allen Modellen in den Sicherheitsabos inbegriffen.
SSH-Prüfung	Durch die Deep Packet Inspection-Prüfung von SSH-verschlüsseltem Verkehr (DPI-SSH) werden Daten, die über SSH-Tunnel übertragen werden, entschlüsselt und durchleuchtet, um Angriffe zu verhindern, die sich SSH zunutze machen.

INTRUSION-PREVENTION[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.

Funktionen

INTRUSION-PREVENTION[1] (FORTSETZUNG)	
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.

SCHUTZ VOR BEDROHUNGEN[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.
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.
Durchsetzung des Content-Filtering Client	Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte außerhalb der Firewallgrenzen zu blockieren.
Granulare Kontrolle	Inhalte lassen sich auf Basis der bereits vordefinierten Kategorien oder einer beliebigen Kombination an Kategorien blockieren. Die Filter können für eine bestimmte Tageszeit aktiviert werden, z. B. während Unterrichts- oder Geschäftszeiten, und auf einzelne Benutzer oder Gruppen beschränkt werden.
Web-Caching	URL-Bewertungen werden lokal auf der SonicWall Firewall zwischengespeichert, sodass jeder weitere Zugriff auf häufig besuchte Websites nur den Bruchteil einer Sekunde dauert.

DURCHSETZUNG VON VIREN- UND SPYWARE-SCHUTZ[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 von Antivirensoftware und/oder DPI-SSL-Zertifikaten installiert und aktiviert ist. Somit entfallen die Kosten, die typischerweise für die Verwaltung desktopbasierter Virenschutzlösungen entstehen.
Option für automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz werden automatisch und netzwerkweit auf jedem Rechner installiert und bereitgestellt, sodass der administrative Mehraufwand minimiert wird.
Always-On-Funktionalität für automatischen Virenschutz	Regelmäßige Antivirus- und Antispyware-Updates werden transparent an alle Desktops und Dateiserver geleitet, um die Produktivität der Endbenutzer zu verbessern und den Aufwand für das Sicherheitsmanagement zu reduzieren.
Virenschutz der nächsten Generation	Capture Client nutzt eine Engine mit statischer Künstlicher Intelligenz, 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*

SONICWALL®

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]

- Cloud-basierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

Intrusion-Prevention[2]

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- 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
- Cloud-basierte Malware-Datenbank

Anwendungsidentifizierung[2]

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

Web Content-Filtering[2]

- URL-Filterung
- Vermeidung von Proxys
- 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

- Dynamisches 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
- 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-Modus, Tap-Modus, NAT-Modus
- 3G/4G WAN-Failover (nicht auf SuperMassive 9800)
- Asymmetrisches Routing
- Common Access Card (CAC)-Unterstützung

Wireless

- WIDS/WIPS
- RF-Spektrumanalyse
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- Floor Plan View/Topology View
- Band Steering
- 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
- Cloud-basiertes Konfigurationsbackup
- BlueCoat Security Analytics Plattform
- Verwaltung von SonicWall-Access-Points
- Verwaltung von Dell N-Series und X-Series Switches[1]

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

SuperMassive 9000 Series – Systemdaten

FIREWALL ALLGEMEIN	9200	9400	9600	9800
Betriebssystem	SonicOS			
Security-Prozessorkerne	24	32		64
Schnittstellen	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE, 1GbE Management, 1 Konsole			4x10GbE SFP+, 12x1GbE SFP, 8x1GbE, 1GbE Management, 1 Konsole
Arbeitsspeicher (RAM)	8 GB	16 GB	32 GB	64 GB
Speicher	Flash			2x 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/s	130.000/s	130.000/s	229.000/s
Maximale Anzahl von Verbindungen (SPI)	5.0M	7.5M	10.0M	20.0M
Maximale Anzahl von Verbindungen (DPI)	1.5M	1.5M	2.0M	8.0M
DPI-SSL-Verbindungen[6] (max.)	8.000 (15.500[6])	10.000 (17.500[6])	12.000 (22.500[6])	650.000
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			
NETZWERK	**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, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p			
Authentifizierung	LDAP (Multi-Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste[5], Citrix[5]			
VoIP	Volle Unterstützung für H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Zertifizierungen	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**
Netzteil	Zwei, redundant, hot-swappable, 300 W			Zwei, redundant, hot-swappable, 500 W
Lüfter	Zwei, redundant, hot-swappable			
Display	LED-Display an der Vorderseite			
Eingangsspannung	100–240 V AC, 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 Normen	FCC Klasse A, ICES Klasse A, CE (EMC, LVD, RoHS), C-Tick, VCCI Klasse A, UL/cUL, TÜV/GS, CB, Mexico CoC nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL			
Umgebung	15 – 40 Grad C			
Luftfeuchtigkeit	10 bis 90 %, nicht kondensierend			

[1] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren. [2] Der Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatz wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia-Testtools nach Branchenstandard gemessen. Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen. [3] VPN-Durchsatz unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte gemessen. [4] Gilt für SuperMassive 9200, 9400 und 9600. Die US APL-Zertifizierung für SuperMassive 9800 ist anhängig. [5] Unterstützt unter SonicOS 6.1 and 6.2. [6] Pro 125.000 ungenutzten DPI-Verbindungen steigt die Anzahl verfügbarer DPI-SSL-Verbindungen um 750. *Für zukünftiges Release. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.

SuperMassive 9000 Series – Bestellinformationen

PRODUKT	ARTIKELNUMMER
SuperMassive 9800 Total Secure Advance Edition (1 Jahr)	01-SSC-0312
SuperMassive 9600 Total Secure Advance Edition (3 Jahre)	02-SSC-0410
SuperMassive 9400 Total Secure Advance Edition (3 Jahre)	02-SSC-0409
SuperMassive 9200 Total Secure Advance Edition (3 Jahre)	02-SSC-0408
SUPERMASSIVE 9200 SUPPORT- UND SECURITY-ABOS	**ARTIKELNUMMER**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Schatten-IT-Sichtbarkeit 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, Content-Filtering mit Support für 9200 (1 Jahr)	01-SSC-4172
Intrusion Prevention, Anti-Malware, CloudAV, Application-Intelligence, Kontrolle und Visualisierung 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 SECURITY-ABOS	**ARTIKELNUMMER**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Schatten-IT-Sichtbarkeit 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, Content-Filtering mit Support für 9400 (1 Jahr)	01-SSC-4136
Intrusion Prevention, Anti-Malware, CloudAV, Application-Intelligence, Kontrolle und Visualisierung 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 SECURITY-ABOS	**ARTIKELNUMMER**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Schatten-IT-Sichtbarkeit 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, Content-Filtering mit Support für 9600 (1 Jahr)	01-SSC-4100
Intrusion Prevention, Anti-Malware, CloudAV, Application-Intelligence, Kontrolle und Visualisierung 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 SECURITY-ABOS	**ARTIKELNUMMER**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall Management und Reporting, Schatten-IT-Sichtbarkeit 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, Content-Filtering mit Support für 9800 (1 Jahr)	01-SSC-0809
Intrusion Prevention, Anti-Malware, CloudAV, Application-Intelligence, Kontrolle und Visualisierung für SuperMassive 9800 (1 Jahr)	01-SSC-0827
Content Filtering Premium Business Edition für 9800 (1 Jahr)	01-SSC-0821
24/7 Gold Support für SuperMassive 9800 (1 Jahr)	01-SSC-0815
MODULE UND ZUBEHÖR*	**ARTIKELNUMMER**
SonicWall SuperMassive 9800 Series Systemlüfter FRU	01-SSC-0204
SonicWall SuperMassive 9800 Series austauschbare Stromversorgung AC FRU	01-SSC-0203
SonicWall SuperMassive 9000 Series Systemlüfter FRU	01-SSC-3876
SonicWall SuperMassive 9000 Series austauschbare Stromversorgung AC FRU	01-SSC-3874
10GBASE-SR SFP+ Short Reach Modul	01-SSC-9785
10GBASE-LR SFP+ Long Reach Modul	01-SSC-9786
1000BASE-SX SFP Short Haul Modul	01-SSC-9789
1000BASE-LX SFP Long Haul Modul	01-SSC-9790
1000BASE-T SFP Kupfermodul	01-SSC-9791
VERWALTUNG UND REPORTING	**ARTIKELNUMMER**
SonicWall GMS 10-Knoten Softwarelizenz	01-SSC-3363
SonicWall GMS E-Class 24/7 Software Support für 10 Knoten (1 Jahr)	01-SSC-6514
SonicWall Scrutinizer virtuelle Appliance mit Flow Analytics Modul Softwarelizenz für bis zu 5 Knoten (einschließlich 1 Jahr 24/7 Software-Support)	01-SSC-3443
SonicWall Scrutinizer mit Flow Analytics Modul Softwarelizenz für bis zu 5 Knoten (einschließlich 1 Jahr 24/7 Software-Support)	01-SSC-4002
SonicWall Scrutinizer Advanced Reporting Modul Softwarelizenz für bis zu 5 Knoten (einschließlich 1 Jahr 24/7 Software-Support)	01-SSC-3773

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

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungsbehörden und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com

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

Datasheet-SuperMassive-US-COG-2465

SONICWALL®