Dell SonicWALL Next-Generation Firewalls der SuperMassive-Serie

Netzwerksicherheit

Die Dell™ SonicWALL™ SuperMassive™-Serie – Dells Next-Generation Firewall (NGFW)-Plattform für große Netzwerke – bietet höchste Skalierbarkeit, Zuverlässigkeit und Sicherheit bei Multi-Gigabit-Geschwindigkeiten und minimalen Latenzzeiten.

Sie wurde für die Anforderungen großer Unternehmen, staatlicher Einrichtungen sowie von Universitäten und Service-providern entwickelt und eignet sich ideal für den Schutz von Enterprise-Netzwerken und Datencentern.

Dank ihrer ultraskalierbaren Multicore-Architektur und der patentierten* Reassembly-Free Deep Packet Inspection® (RFDPI)-Technologie von Dell SonicWALL bieten die SuperMassive-Serien E10000 und 9000 modernste Funktionen für Intrusion Prevention, Anwendungs-kontrolle, Malware-Schutz und SSL-Prüfung bei Multi-Gigabit-Geschwindigkeiten. Entwickelt wurde die SuperMassive-Serie mit besonderem Augenmerk auf Stromverbrauch, Platzbedarf und Kühlung. Daher bietet sie als NGFW den höchsten Durchsatz pro Watt (GBit/s/Watt) in den Bereichen Anwendungskontrolle und Threat Prevention.

Die RFDPI-Engine von Dell 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 veralteten Proxy-Designs mit Reassemblierung überlegen, bei denen Sockets an Anti-Malware-Programme gekoppelt werden. Hier kommt es immer wieder zu einer ineffizienten Verarbeitung und zu Socket-Memory-Thrashing, was zu hoher Latenz, verminderter Leistung und Einschränkungen beim Datenvolumen führt. Die RFDPI-Engine ermöglicht dagegen eine umfassende Prüfung der Dateiinhalte und wehrt Bedrohungen ab, bevor sie in das Netzwerk gelangen können. Auf diese Weise bietet sie Schutz vor Millionen unterschiedlicher Malware-Varianten ohne Einschränkungen bei Datenvolumen, Performance oder Latenzzeit. Weil auch SSL-verschlüsselter Verkehr und nicht-proxyfähige Anwendungen intensiv geprüft werden, garantiert die RFDPI-Technologie zudem vollen Schutz, unabhängig von Übertragung und Protokoll.

Durch die Analyse des Anwendungs-verkehrs lässt sich arbeitsrelevanter und nicht arbeitsrelevanter Anwendungsverkehr in Echtzeit anzeigen und mit effektiven Regeln auf der Anwendungsebene kontrollieren. Die Anwendungskontrolle kann sowohl nach Benutzern als auch nach Gruppen sowie mit Zeitplänen und Ausschlusslisten durchgeführt werden. Alle Anwendungs-, Intrusion Prevention- und Malware-Signaturen werden laufend von Dell SonicWALLs Threat Research Team aktualisiert. Darüber hinaus bietet SonicOS – ein spezielles, hochentwickeltes Betriebssystem – integrierte Tools für eine personalisierbare Anwendungs-identifizierung und -kontrolle.

Die Hardware der SuperMassive-Serie erlaubt nahezu lineare Leistungs-steigerungen und lässt sich auf bis zu 96 Prozessorkerne skalieren. Damit ist sie in der Lage, einen Durchsatz von bis zu 30 GBit/s bei Threat Prevention und 30 GBit/s bei der Anwendungsprüfung und -kontrolle bereitzustellen. Die vor Ort erweiterbare SuperMassive E10000-Serie ist eine zukunftssichere Investition, die mit der Netzwerkbandbreite und den Sicherheitsanforderungen dynamischer Unternehmen mitwachsen kann.

SuperMassive E10000-Serie

SuperMassive 9000-Serie

- **Umfassender Schutz vor Bedrohungen mit High-Performance-Intrusion Prevention und Malware-Schutz bei minimalen Latenzzeiten**
- **Hochentwickelte, granulare Application Intelligence, Anwendungs-kontrolle und -visualisierung**
- **Umfassende Prüfung von SSL-verschlüsseltem Verkehr ohne den zusätzlichen Aufwand, die hohe Latenz und dem Memory-Thrashing von socketbasierten SSL-Proxies**
- **Ultraskalierbare Multicore-Architektur für 10- bzw. 40-GBit/s-Infrastrukturen**

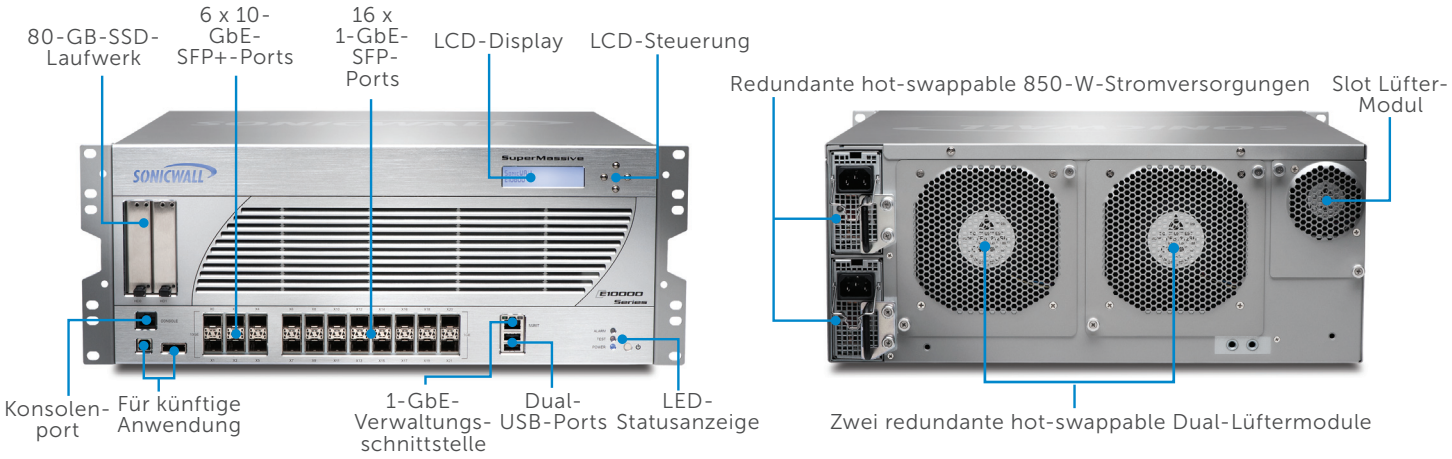
U.S.-Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361

Überblick über die SuperMassive E10000-Serie

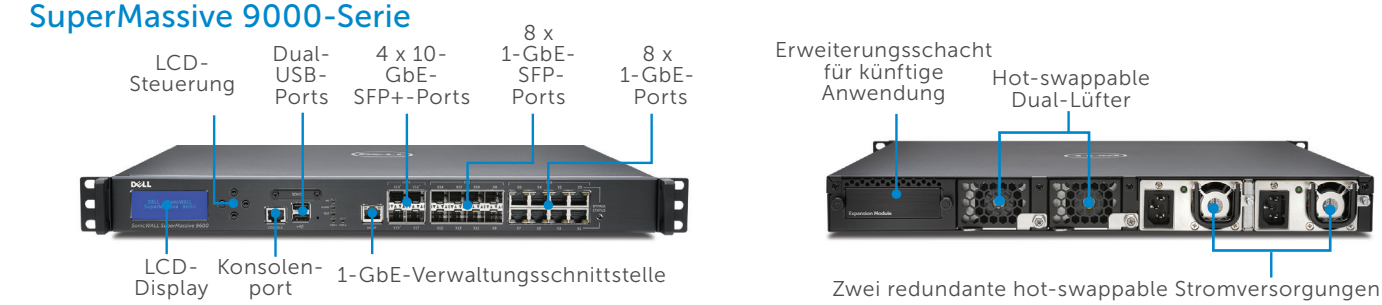
Die Gehäuse der Dell SonicWALL SuperMassive E10000-Serie enthalten 6 x 10-GbE-SFP+- und 16 x 1-GbE-SFP-Ports, redundante 850-W-AC-Stromversorgungen sowie redundante, hot-swappable Dual-Lüftermodule und lassen sich auf bis zu 96 Prozessorkerne skalieren.

Die Dell SonicWALL SuperMassive 9000-Serie verfügt über 4 x 10-GbE-SFP+-, 8 x 1-GbE-SFP- und 8 x 1-GbE-Kupfer-Schnittstellen sowie 1-GbE-Verwaltungsschnittstellen. Zudem enthält sie einen Erweiterungsanschluss für weitere 2 x 10-GbE-SFP+-Schnittstellen (für künftige Releases). Die 9000er-Serie bietet hot-swappable Dual-Lüftermodule und Stromversorgungen.

SuperMassive E10000-Serie



SuperMassive 9000-Serie



Funktionen	9200	9400	9600	E10200	E10400	E10800
Prozessorkerne	24	32	32	24	48	96
Firewall-Durchsatz	15 GBit/s	20 GBit/s	20 GBit/s	10 GBit/s	20 GBit/s	40 GBit/s
Application Intelligence-Durchsatz	5 GBit/s	8 GBit/s	9,7 GBit/s	7,5 GBit/s	15 GBit/s	30 GBit/s
IPS-Durchsatz	5 GBit/s	8 GBit/s	9,7 GBit/s	7,5 GBit/s	15 GBit/s	30 GBit/s
Anti-Malware-Durchsatz	3,5 GBit/s	4,5 GBit/s	5,0 GBit/s	3,0 GBit/s	6,0 GBit/s	12 GBit/s
Maximale Anzahl von Verbindungen	1,25 Mio.	1,25 Mio.	1,5 Mio.	3,0 Mio.	6,0 Mio.	12,0 Mio.

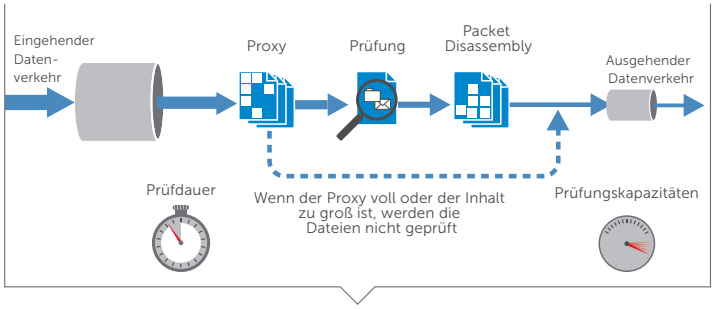
Bereitstellungsmodi	9200	9400	9600	E10200	E10400	E10800
L2-Bridge-Modus, transparenter Modus	Ja	Ja	Ja	Ja	Ja	Ja
Wire-Modus	Ja	Ja	Ja	Ja	Ja	Ja
Gateway-/NAT-Modus	Ja	Ja	Ja	Ja	Ja	Ja
Tap-Modus	Ja	Ja	Ja	Ja	Ja	Ja
Transparenter Bridge-Modus	Ja	Ja	Ja	Ja	Ja	Ja

DELL Software

Reassembly-Free Deep Packet Inspection-Engine

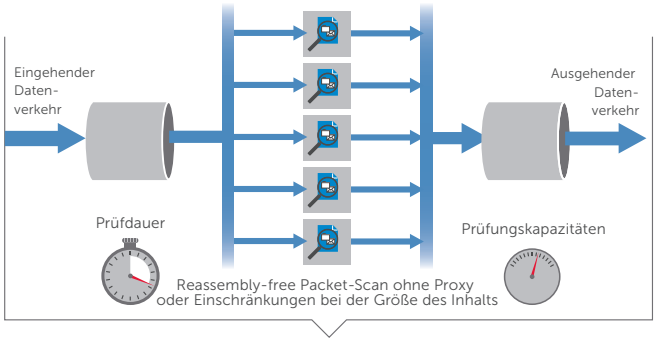
Die Dell SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI)-Engine bietet einen optimalen Schutz vor Bedrohungen und umfassende Anwendungskontrolle, ohne die Leistung zu beeinträchtigen. Dabei prüft die patentierte Engine die Payload von Datenströmen, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren. Durch die RFDPI-Engine wird der Netzwerkverkehr mehrfach umfassend normalisiert und entschlüsselt. Auf diese Weise lassen sich raffinierte Umgehungsversuche verhindern, die darauf abzielen, Erkennungsmechanismen zu stören und bösartigen Code in das Netzwerk einzuschleusen. Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall aktualisiert und mit diesen Datenbanken abgeglichen. Dabei wird geprüft, ob ein Angriff oder ein anderes sicherheitsrelevantes Ereignis eintritt. Ist dies der Fall, wird eine vordefinierte Aktion ausgeführt. In den meisten Fällen wird die Verbindung beendet. Anschließend werden entsprechende Logging- und Benachrichtigungs-Events erzeugt. Die Engine kann jedoch auch nur für Prüfungen konfiguriert werden oder – wenn die Anwendungserkennung aktiv ist – so, dass für den restlichen Anwendungsverkehr Layer-7-Bandbreitenverwaltungsdienste bereitgestellt werden, sobald die Anwendung erkannt wird.

Verfahren mit Packet Assembly



Architekturen anderer Anbieter

Reassembly-free Packet-Scan

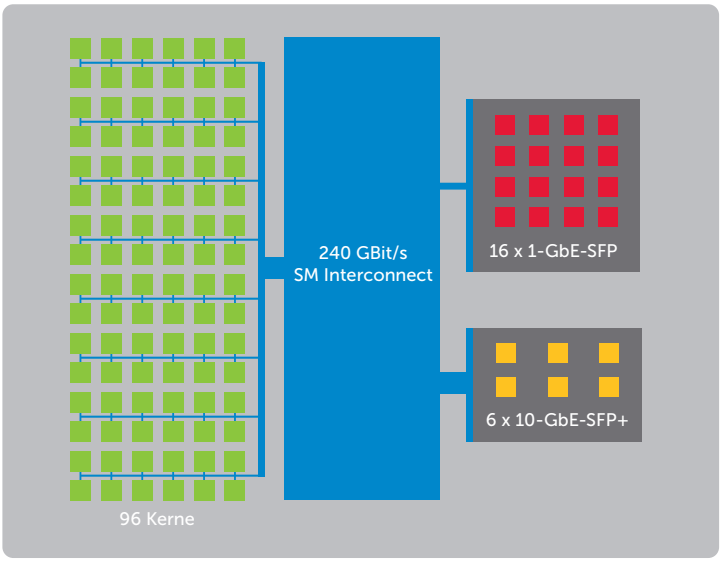


Dell SonicWALL-Architektur

Erweiterbare Architektur für höchste Skalierbarkeit und Performance

Die RFDPI-Engine wurde von Grund auf so entwickelt, dass Sicherheitsprüfungen mit hohen Durchsatzraten durchgeführt werden können. Auf diese Weise wird den Anforderungen der parallelen Verarbeitung sowie der ständig steigenden Bandbreite Rechnung getragen. Diese Architektur ermöglicht eine parallele Verarbeitung und lässt sich in Kombination mit 24-, 32-, 48- oder 96-Kern-Prozessoren optimal skalieren. Eine effektive Deep Packet Inspection-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.



DELL Software

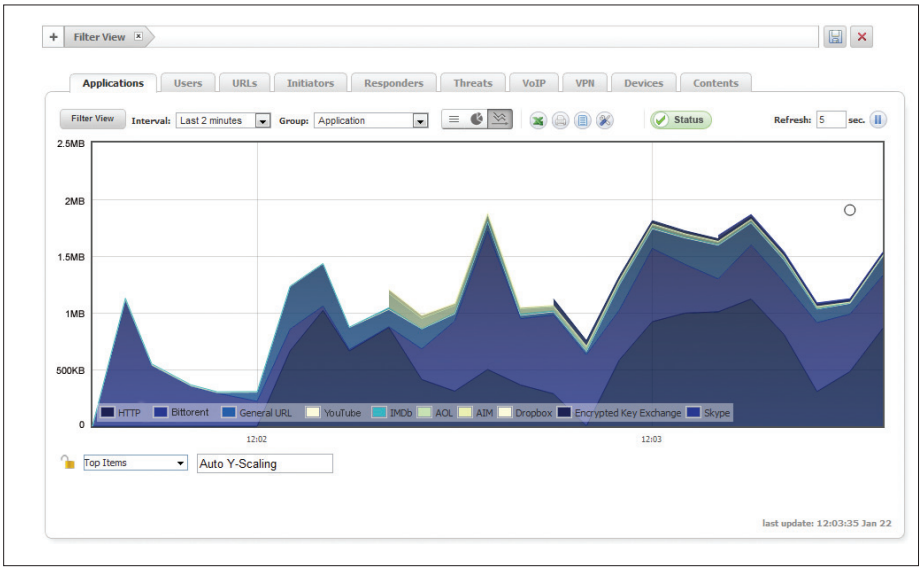
Sicherheit und Schutz

Das interne Dell SonicWALL Threats Research Team ist für die Erforschung und Entwicklung von Abwehrmechansimen zuständig. Diese werden in die Firewalls implementiert, um aktuellen Schutz zu gewährleisten. Dabei nutzt das Team weltweit über eine Million Sensoren, die Malware-Muster sammeln und Daten zu den neuesten Bedrohungen liefern. Diese werden anschließend als Grundlage für die Intrusion Prevention-, Anti-Malware- und Anwendungserkennungsfunktionen genutzt. Kunden mit Next-Generation Firewalls von Dell SonicWALL, die mit den neuesten Sicherheitsfunktionen ausgestattet sind, erhalten rund um die Uhr Updates zu den aktuellsten Bedrohungen. Die Updates sind sofort wirksam, erfordern keine Neustarts und verursachen keinerlei Unterbrechungen. Die Signaturen auf den Appliances bieten Schutz vor einer großen Vielfalt an Bedrohungen. Eine einzige Signatur deckt dabei bis zu Zehntausende verschiedene Bedrohungen ab. Zusätzlich zu den Abwehrmechanismen auf der Appliance bieten die SuperMassive-Firewalls auch Zugang zum Dell SonicWALL CloudAV Service. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um derzeit über 12 Millionen Signaturen erweitert. Die Firewall greift über ein proprietäres schlankes Protokoll auf die CloudAV-Datenbank zu, um die Prüfung, die auf der Appliance durchgeführt wird, zu erweitern. Dank effizienter Geo-IP- und Botnet-Filter-Funktionen sind die NGFWs von Dell SonicWALL in der Lage, den Verkehr aus gefährlichen Domänen oder ganzen Regionen zu blockieren, um die Sicherheitsrisiken im Netzwerk zu reduzieren.

Application Intelligence and Control

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 werden mittels Echtzeit-Visualisierung augenblicklich identifiziert. So können unverzüglich Gegenmaßnahmen eingeleitet werden, um das Netzwerk vor ein- oder ausgehenden Angriffen zu schützen oder Performance-Engpässe zu verhindern.

Dell SonicWALL Application Traffic Analytics liefert detaillierte Informationen zum Anwendungsverkehr, zur Bandbreitennutzung sowie zu Sicherheitsbedrohungen und bietet leistungsstarke Troubleshooting- und Forensik-Funktionen. Sichere Single Sign-on (SSO)-Funktionen sorgen für mehr Benutzerfreundlichkeit, erhöhen die Produktivität und reduzieren die Support-Anfragen. Das Dell SonicWALL Global Management System (GMS®) vereinfacht mit seiner intuitiven webbasierten Oberfläche die Verwaltung der Anwendungserkennungs- und -kontrollfunktionen.



Software

Funktionen

RFDPI-Engine	
Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection (RFDPI)	Diese hochleistungsfähige, proprietäre und patentierte 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 auf Bedrohungen geprüft, um zu verhindern, dass das Netzwerk zum Verbreiten von Malware oder als Ausgangsplattform für Angriffe genutzt wird, falls ein infizierter Computer in das Netzwerk gelangt.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxies 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.

Intrusion Prevention	
Funktion	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes Intrusion Prevention System (IPS) nutzt Signaturen und andere Abwehrmechanismen, um Paket-Payloads auf Schwachstellen und Exploits zu prüfen, und deckt dabei eine Vielzahl an Angriffen und Schwachstellen ab.
Automatische Signaturen-Updates	Das Dell SonicWALL Threat Research Team analysiert kontinuierlich Bedrohungen und sorgt für die ständige Aktualisierung einer umfassenden Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien deckt. Die neuen Updates sind sofort wirksam und erfordern keine Neustarts oder sonstigen Betriebsunterbrechungen.
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 Ebenen 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.

Funktionen

Threat Prevention	
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	Die Cloud-Server von Dell SonicWALL verfügen über eine ständig aktualisierte Datenbank mit über 12 Millionen Bedrohungssignaturen. Diese ergänzt die lokalen Signaturendatenbanken und sorgt dafür, dass die RFDPI-Technologie eine große Vielfalt an Bedrohungen abdeckt.
Sicherheitsupdates rund um die Uhr	Das Dell SonicWALL Threat Research Team analysiert neue Bedrohungen und stellt Abwehrmechanismen bereit – 24 Stunden am Tag, 7 Tage die Woche. 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.
SSL-Prüfung	Blitzschnelle, proxylose Entschlüsselung und Prüfung von SSL-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im SSL-verschlüsselten Verkehr lauern.
Bidirektionale Raw-TCP-Prüfung	Die RFDPI-Engine ist in der Lage, Raw-TCP-Streams bidirektional auf sämtlichen Ports zu prüfen. So lassen sich Angriffe verhindern, bei denen veraltete Sicherheitssysteme umgangen werden, die sich lediglich auf ein paar bekannte Ports konzentrieren.
Unterstützung zahlreicher Protokolle	Identifizierung gängiger Protokolle wie HTTP/S, FTP, SMTP, SMBv1/v2 und andere, bei denen Daten nicht in Raw-TCP-Paketen gesendet werden. Payloads werden für die Malware-Prüfung entschlüsselt, auch wenn sie keine bekannten Standardports nutzen.

Application Intelligence and Control	
Funktion	Beschreibung
Anwendungskontrolle	Kontrolle von Anwendungen oder einzelnen Anwendungsmerkmalen, die anhand einer kontinuierlich erweiterten Datenbank mit über 4.300 Anwendungssignaturen von der RFDPI-Engine erkannt werden. Dadurch lässt sich die Netzwerksicherheit und -produktivität erhöhen.
Personalisierbare Anwendungsidentifizierung	Erstellung von 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	Einschränkung oder Priorisierung von Anwendungen oder Anwendungskategorien, um die verfügbare Bandbreite für kritische Anwendungen zu maximieren und unerwünschten Anwendungsverkehr einzuschränken oder ganz zu blockieren.
Visualisierung von internem und externem Verkehr	Erkennung der Bandbreitennutzung und Analyse des Netzwerkverhaltens mit Echtzeit-Visualisierung des internen Anwendungsverkehrs und Berichten zum externen Anwendungsverkehr via NetFlow/IPFix.
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-/Terminal Services-/Citrix-Integration.

Funktionen

Firewall und Networking	
Funktion	Beschreibung
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass alle Firewall-Zugriffsregeln erfüllt werden.
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.
Flexible Implementierung	Die SuperMassive-Serie lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
Hochverfügbarkeit/ Clustering	Die SuperMassive-Serie unterstützt die Hochverfügbarkeitsmodi Active/Passive mit State-Synchronisierung, Active/Active 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.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden.
Regelbasiertes Routing	Erstellen von protokollbasierten Routen für die Umleitung des Datenverkehrs zu einer bevorzugten WAN-Verbindung mit Failback-Möglichkeit auf ein sekundäres WAN bei einem Stromausfall.
Erweiterte QoS	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.

Management und Reporting	
Funktion	Beschreibung
Global Management System	Dell SonicWALL GMS ermöglicht es, über eine einzige Verwaltungsschnittstelle mit intuitiver Oberfläche mehrere Dell SonicWALL-Appliances zu überwachen und zu konfigurieren und Berichte dazu zu erstellen. Dies reduziert nicht nur die Kosten, sondern auch die Komplexität bei der Verwaltung.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche erlaubt eine schnelle und bequeme Konfiguration, eine umfassende CLI und 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 Dell SonicWALL Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben.

Virtual Private Networking	
Funktion	Beschreibung
IPSec VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPSec VPN kann die SuperMassive-Serie als VPN-Konzentrator für Tausende großer Standorte, Zweigniederlassungen oder Home Offices eingesetzt werden.
SSL VPN- oder IPSec Client-Remote Access	Durch Einsatz der clientlosen SSL-VPN-Technologie oder eines leicht zu verwaltenden IPSec-Clients ist der unkomplizierte Zugriff auf E-Mail, Dateien, Rechner, Intranet-Sites und Anwendungen von zahlreichen unterschiedlichen Plattformen möglich.
Redundantes VPN-Gateway	Bei 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	Die Möglichkeit, ein dynamisches Routing über VPN-Links durchzuführen, sorgt für Ausfallsicherheit durch Umleitung des Datenverkehrs über alternative Verbindungen zwischen Endgeräten, falls ein temporäres VPN-Tunnel ausfällt.

Funktionen

Content- bzw. kontextorientierte Sicherheitsfunktionen

Funktion	Beschreibung
Nachverfolgung der Benutzeraktivitäten	Stellt Informationen zur Benutzerkennung und -aktivität bereit, die auf der nahtlosen SSO-Integration für AD/LDAP/Citrix/Terminal Services sowie umfassenden DPI-Daten basieren.
GeoIP: Identifizierung des Datenverkehrs nach Ländern	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.
DPI-Filterung nach regulären Ausdrücken	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern.

Die SonicOS-Funktionen im Überblick

Firewall
- Reassembly-Free Deep Packet Inspection
- Deep Packet Inspection für SSL-Verkehr
- Stateful Packet Inspection
- TCP-Reassemblierung
- Stealth-Modus
- Common Access Card (CAC)-Unterstützung
- Schutz vor DoS-Angriffen
- UDP-/ICMP-/SYN-Flood-Schutz

Intrusion Prevention
- Signaturbasierte Prüfung
- Automatische Signaturenupdates
- Schutz vor ausgehenden Bedrohungen
- IPS-Ausschlussliste
- Auf GeoIP und Reputation basierende Filterfunktionen
- Abgleich regulärer Ausdrücke
- UDP-/ICMP-/SYN-Flood-Schutz

Anti-Malware
- Streambasierte Malware-Prüfung
- Gateway Anti-Virus
- Gateway Anti-Spyware
- SSL-Entschlüsselung
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- CloudAV-Datenbank zu Bedrohungen

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

Web Content Filtering
- URL Filtering
- Anti-Proxy-Technologie
- Blockieren mithilfe von Schlüsselwörtern
- Bandbreitenverwaltung mit CFS-Ratingkategorien
- Unified Policy-Konzept mit Anwendungskontrolle
- 56 Content Filtering-Kategorien

VPN
- IPSec VPN für Site-to-Site-Konnektivität
- SSL VPN- oder IPSec Client-Remote Access
- Redundantes VPN-Gateway
- Mobile Connect für Apple® iOS und Google® Android™
- Routenbasiertes VPN (OSPF, RIP)

Networking
- Dynamic Routing
- SonicPoint Wireless Controller*
- Regelbasiertes Routing
- Erweiterte NAT
- DHCP-Server
- Bandbreitenmanagement
- Link Aggregation
- Port-Redundanz
- Hochverfügbarkeitsmodus A/P mit State Sync
- A/A Clustering
- Lastverteilung beim ein-/ausgehenden Verkehr
- L2-Bridge-, Wire-, Tap-, NAT-Modus

VoIP
- Erweiterte QoS
- Bandbreitenmanagement
- DPI für VoIP-Daten
- H.323-Gatekeeper- und SIP-Proxy-Support

Verwaltung und Überwachung
- Web-Oberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Externes Reporting (Scrutinizer)
- Global Management System mit Regelverwaltungs- und Reporting-Funktionen
- Logging
- Netflow-/IPFIX-Export
- Visualisierung des Anwendungsverkehrs
- LCD-Bildschirm
- Zentralisierte Regelverwaltung
- Single Sign-On (SSO)
- Terminal Service-/Citrix-Unterstützung
- Integrierte Forensik-Funktionen von Solera Networks

*SonicPoint Wireless Controller für die 9000er Serie zum Zeitpunkt der Veröffentlichung verfügbar

SuperMassive E10000-Serie – Systemdaten

	E10200	E10400	E10800
Betriebssystem		SonicOS	
Kerne	24	48	96
10-GbE-Schnittstellen		6 x 10-GbE-SFP+	
1-GbE-Schnittstellen		16 x 1-GbE-SFP	
Verwaltungsschnittstellen		1 GbE, 1 Konsole	
Speicher (RAM)	16 GB	32 GB	64 GB
Speicher		80 GB SSD, Flash	
Firewall Inspection-Durchsatz	10 GBit/s	20 GBit/s	40 GBit/s
Application Inspection-Durchsatz	7,5 GBit/s	15 GBit/s	30 GBit/s
IPS-Durchsatz	7,5 GBit/s	15 GBit/s	30 GBit/s
Anti-Malware Inspection-Durchsatz	3,0 GBit/s	6,0 GBit/s	12 GBit/s
VPN-Durchsatz	5,0 GBit/s	10 GBit/s	20 GBit/s
Verbindungen pro Sekunde	160.000/Sek.	320.000/Sek.	640.000/Sek.
Max. Anzahl von Verbindungen (SPI)	3,0 Mio.	6,0 Mio.	12,0 Mio.
Max. Anzahl von Verbindungen (DPI)	2,5 Mio.	5,0 Mio.	10,0 Mio.
VPN			
Site-to-Site-Tunnel		10.000	
IPSec VPN-Clients (max.)		2.000 (10.000)	
SSL VPN-Lizenzen (max.)		50 (50)	
Verschlüsselung		DES, 3DES, AES (128, 192, 256-Bit)	
Authentifizierung		MD5, SHA-1	
Schlüsselaustausch		Diffie Hellman-Gruppen 1, 2, 5, 14	
Routenbasiertes VPN		RIP, OSPF	
Networking			
IP-Adressenzuweisung		Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay	
NAT-Modi		1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT, transparenter Modus	
VLAN-Schnittstellen		512	
Routing-Protokolle		BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast	
QoS		Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p	
Authentifizierung		XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminal Services, Citrix	
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 (ausstehend)		FIPS 140-2, Common Criteria EAL4+, NEBS, ICSA Firewall	
Zertifikate		„Recommend"-Bewertung von NSS für NGFW und IPS	
Common Access Card (CAC)-Unterstützung		ausstehend	
Hardware			
Stromversorgung		dual, redundant, hot-swappable, 850 W	
Lüfter		dual, redundant, hot-swappable	
Display		Front-LED-Display	
Eingangsspannung		100-240 VAC, 60-50 Hz	
Maximale Leistungsaufnahme (W)	400	550	750
Gehäuse		rackfähig (4 HE)	
Abmessungen		43 x 43,5 x 17,8 cm	
Gewicht	26,3 kg	27,7 kg	30,3 kg
WEEE-Gewicht	26,8 kg	28,1 kg	30,8 kg
Versandgewicht	35,8 kg	37,2 kg	39,9 kg
Erfüllt folgende Standards/Normen		FCC Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE	
Umgebungstemperatur		5-40 °C	
Luftfeuchtigkeit		10-90 %, nicht kondensierend	

Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten

SuperMassive 9000-Serie – Systemdaten

	9200	9400	9600
Betriebssystem	SonicOS		
Kerne	24	32	
10-GbE-Schnittstellen	4 x 10-GbE-SFP+		
1-GbE-Schnittstellen	8 x 1-GbE-SFP, 8 x 1-GbE (1 LAN-Bypass-Paar)		
Verwaltungsschnittstellen	1 GbE, 1 Konsole		
Speicher (RAM)	8 GB	16 GB	32 GB
Erweiterung	1 Erweiterungssteckplatz (Rückseite)*, SD-Karte*		
Firewall Inspection-Durchsatz	15 GBit/s	20 GBit/s	
Application Inspection-Durchsatz	5 GBit/s	8 GBit/s	9,7 GBit/s
IPS-Durchsatz	5 GBit/s	8 GBit/s	9,7 GBit/s
Anti-Malware Inspection-Durchsatz	3,5 GBit/s	4,5 GBit/s	5 GBit/s
IMIX-Performance (GBit/s)	4,5 GBit/s	5,5 GBit/s	
VPN-Durchsatz	5,0 GBit/s	10 GBit/s	11,5 GBit/s
Verbindungen pro Sekunde	110.000/Sek.	150.000/Sek.	
Max. Anzahl von Verbindungen (SPI)	1,25 Mio.		1,5 Mio.
Max. Anzahl von Verbindungen (DPI)	1,0 Mio.		1,25 Mio.
Unterstützte SonicPoints (max.)	96	128	
VPN			
Site-to-Site-Tunnel	6.000	10.000	
IPSec VPN-Clients (max.)	2.000 (4.000)	2.000 (6.000)	2.000 (10.000)
SSL VPN-Lizenzen (max.)	2 (50)		50 (50)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256-Bit)/MD5, SHA-1		
Schlüsselaustausch	Diffie Hellman-Gruppen 1, 2, 5, 14		
Routenbasiertes VPN	RIP, OSPF		
Networking			
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay		
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT, transparenter Modus		
VLAN-Schnittstellen	512		
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast		
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p		
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminal Services, Citrix		
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 (ausstehend)	FIPS 140-2, Common Criteria EAL4+, ICSA Firewall		
Common Access Card (CAC)	ausstehend		
Hardware			
Stromversorgung	dual, redundant, hot-swappable, 300 W		
Lüfter	dual, redundant, hot-swappable		
Display	Front-LED-Display		
Eingangsspannung	100-240 VAC, 60-50 Hz		
Maximale Leistungsaufnahme (W)	300		
Gehäuse	rackfähig (1 HE)		
Abmessungen	43,3 x 48,5 x 4,5 cm		
Gewicht	8,2 kg		
WEEE-Gewicht	10,4 kg		
Versandgewicht	13,3 kg		
Erfüllt folgende Standards/Normen	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE, ANATEL, BSMI		
Umgebungstemperatur	0-40 °C		
Luftfeuchtigkeit	10-90 %, nicht kondensierend		

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

SuperMassive E10000-Serie – Bestellinformationen

Produkt	Artikelnummer
SuperMassive E10200, 6 SFP+-10-GbE-Ports, 16 SFP-1-GbE-Ports, Dual-Lüfter, Dual-AC-Stromversorgungen	01-SSC-8882
SuperMassive E10400, 6 SFP+-10-GbE-Ports, 16 SFP-1-GbE-Ports, Dual-Lüfter, Dual-AC-Stromversorgungen	01-SSC-8881
SuperMassive E10800, 6 SFP+-10-GbE-Ports, 16 SFP-1-GbE-Ports, Dual-Lüfter, Dual-AC-Stromversorgungen	01-SSC-8856
System-Upgrades	**Artikelnummer**
Upgrade von SuperMassive E10200 auf E10400	01-SSC-9497
Upgrade von SuperMassive E10400 auf E10800	01-SSC-9498
SuperMassive E10200 – Support und Sicherheitsabos	**Artikelnummer**
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für E10200 (1 Jahr)	01-SSC-9518
Application Intelligence and Control – Application Intelligence, Control and Visualization für E10200 (1 Jahr)	01-SSC-9524
Content Filtering Premium Business Edition für E10200 (1 Jahr)	01-SSC-9521
Platinum-Support für SuperMassive E10200 (1 Jahr)	01-SSC-9530
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für E10200 (1 Jahr)	01-SSC-9533
SuperMassive E10400 – Support und Sicherheitsabos	**Artikelnummer**
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für E10400 (1 Jahr)	01-SSC-9536
Application Intelligence and Control – Application Intelligence, Control and Visualization für E10400 (1 Jahr)	01-SSC-9542
Content Filtering Premium Business Edition für E10400 (1 Jahr)	01-SSC-9539
Platinum-Support für SuperMassive E10400 (1 Jahr)	01-SSC-9548
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für E10400 (1 Jahr)	01-SSC-9551
SuperMassive E10800 – Support und Sicherheitsabos	**Artikelnummer**
Application Intelligence and Control – Application Intelligence, Control and Visualization für E10800 (1 Jahr)	01-SSC-9560
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für E10800 (1 Jahr)	01-SSC-9554
Content Filtering Premium Business Edition für E10800 (1 Jahr)	01-SSC-9557
Platinum-Support für SuperMassive E10800 (1 Jahr)	01-SSC-9566
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention und Content Filtering mit Support für E10800 (1 Jahr)	01-SSC-9569
Module und Zubehör*	**Artikelnummer**
Systemlüfter für die SuperMassive E10000-Serie (FRU)	01-SSC-8885
SSD-Lüftermodul für die SuperMassive E10000-Serie	01-SSC-8886
Stromversorgung für die SuperMassive E10000-Serie (FRU)	01-SSC-8887
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twinaxial-Kabel	01-SSC-9787
10GBASE SFP+ 3M Twinaxial-Kabel	01-SSC-9788
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Kupfermodul	01-SSC-9791
Management und Reporting	**Artikelnummer**
Dell SonicWALL GMS Software-Lizenz (10 Nodes)	01-SSC-3363
Dell SonicWALL GMS E-Class 24/7 Software-Support für 10 Nodes (1 Jahr)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance mit Softwarelizenz für Flow-Analysemodul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-3443
Dell SonicWALL Scrutinizer mit Softwarelizenz für Flow-Analysemodul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-4002
Dell 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 Dell SE

Für diese Appliance-Serie sind die Security Monitoring Services von Dell SecureWorks verfügbar. Weitere Informationen erhalten Sie unter **www.dell.com/secureworks**.

SuperMassive 9000-Serie – Bestellinformationen

Produkt	Artikelnummer
SuperMassive 9600	01-SSC-3880
SuperMassive 9600 High Availability	01-SSC-3881
SuperMassive 9400	01-SSC-3800
SuperMassive 9400 High Availability	01-SSC-3801
SuperMassive 9200	01-SSC-3810
SuperMassive 9200 High Availability	01-SSC-3811
SuperMassive 9200 – Support und Sicherheitsabos	**Artikelnummer**
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**
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**
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
Module und Zubehör*	**Artikelnummer**
Systemlüfter für die Dell SonicWALL SuperMassive 9000-Serie (FRU)	01-SSC-3876
AC-Stromversorgung für die Dell SonicWALL SuperMassive 9000-Serie (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**
Dell SonicWALL GMS Software-Lizenz (10 Nodes)	01-SSC-3363
Dell SonicWALL GMS E-Class 24/7 Software-Support für 10 Nodes (1 Jahr)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance mit Softwarelizenz für Flow-Analysemodul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-3443
Dell SonicWALL Scrutinizer mit Softwarelizenz für Flow-Analysemodul für bis zu 5 Nodes (inklusive 1 Jahr 24/7-Software-Support)	01-SSC-4002
Dell 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 Dell-SE

Für diese Appliance-Serie sind die Security Monitoring Services von Dell SecureWorks verfügbar. Weitere Informationen erhalten Sie unter **www.dell.com/secureworks**.

DELL Software