Dell SonicWALL SuperMassive Serie

Netzwerksicherheit

Die Dell™ SonicWALL™ SuperMassive™ Serie ist die Dell Plattform für Firewalls der nächsten Generation (NGFWs) und speziell auf große Netzwerke ausgelegt. Sie bietet Skalierbarkeit, Zuverlässigkeit und höchste Sicherheit – bei Multi-Gigabit-Geschwindigkeiten und praktisch ohne Latenz.

Die SuperMassive Serie wurde auf die Anforderungen großer Unternehmen sowie von Regierungsbehörden, Universitäten und Service Providern zugeschnitten und eignet sich ideal für die Absicherung von Unternehmensnetzwerken, Rechenzentren und Service Provider-Infrastrukturen.

Dank ihrer skalierbaren Multi-Core-Architektur und der patentierten* Dell SonicWALL Reassembly-Free Deep Packet Inspection® Technologie (RFDPI) bieten die SuperMassive E10000 und 9000 Serien branchenführende Leistung in den Bereichen Anwendungskontrolle, Angriffsvermeidung, Malware-Schutz und SSL-Überprüfung bei Multi-Gigabit-Geschwindigkeiten. Bei der Entwicklung der SuperMassive Serie haben wir besonderes Augenmerk auf Stromverbrauch, Platzbedarf und Kühlung gelegt und können Ihnen so die NGFW mit dem branchenweit besten Gbit/s pro Watt-Verhältnis für Anwendungskontrolle und Bedrohungsabwehr bieten.

Die Dell SonicWALL RFDPI Engine scannt jedes Byte in jedem Paket, und das über sämtliche Ports hinweg. So wird der gesamte Inhalt eines Datenstroms geprüft, bei hoher Leistung und niedriger Latenz. Diese Technologie ist veralteten Proxy-Designs überlegen, bei denen Inhaltspakete über fest an Malware-Schutz-Lösungen gekoppelte Sockel neu zusammengesetzt (Reassembly) werden. Solche Architekturen haben typischerweise mit Ineffizienzen und Overhead durch Arbeitsspeicher-Thrashing ("Seitenflattern") auf den Sockeln zu kämpfen. Die Konsequenz: hohe Latenz, niedrige Leistung und Einschränkungen bei der Dateigröße. Die RFDPI Engine ermöglicht eine vollständige Inhaltsprüfung und wehrt Bedrohungen ab, bevor sie in das Netzwerk gelangen. So bietet sie Schutz vor Millionen unterschiedlicher Malware-Varianten, ohne Einschränkungen bei Dateigröße, Leistung oder Latenzzeiten. Zusätzlich prüft die RFDPI Engine den gesamten SSL-verschlüsselten Datenverkehr und alle nicht proxyfähigen Anwendungen intensiv und sorgt so für umfassende Sicherheit, unabhängig von Übertragungsmedium und Protokoll.

Über eine Analyse des Anwendungsdaten-verkehrs lässt sich in Echtzeit produktiver von unproduktivem Anwendungsdatenverkehr unterscheiden und anschließend mithilfe leistungsfähiger Richtlinien auf Anwendungs-ebene kontrollieren. Die Anwendungskontrolle kann für einzelne Benutzer oder für bestimmte Gruppen greifen und bietet sowohl Zeitpläne als auch Ausnahmelisten. Alle Anwendungs-, Angriffsvermeidungs- und Malware-Signaturen werden fortlaufend durch das Dell SonicWALL Threat Research Team aktualisiert. Unser innovatives, speziell für dieses Einsatzszenario optimiertes Betriebssystem SonicOS bringt zudem integrierte Tools für die Identifizierung und Kontrolle benutzerdefinierter Anwen-dungen mit.

Das Design der Firewalls der SuperMassive Serie erlaubt nahezu lineare Leistung und lässt sich auf bis zu 96 Verarbeitungskerne skalieren. So wird ein Firewall-Datendurchsatz von bis zu 40 Gbit/s, ein Datendurchsatz von 30 Gbit/s bei der Bedrohungsabwehr und ein Datendurchsatz von 30 Gbit/s bei der Anwendungsprüfung und -kontrolle erreicht. Upgrades an der SuperMassive E10000 Serie werden direkt auf Ihre Firewalls vor Ort aufgespielt, sodass Ihre Investitionen in Sicherheitsinfrastruktur langfristig geschützt bleiben – auch wenn Ihre Anforderungen an Netzwerkbandbreite und Sicherheit in der Zukunft steigen sollten.

SuperMassive E10000 Serie

SuperMassive 9000 Serie

Vorteile:

- Umfassender Schutz vor Bedrohungen, einschließlich hochleistungsfähiger Angriffsvermeidung und Malware-Schutz mit niedriger Latenz
- Herausragende granulare Anwendungserkennung, -kontrolle und -visualisierung
- Prüfung des gesamten SSL-verschlüsselten Datenverkehrs ohne den Overhead, die hohe Latenz und das Arbeitsspeicher-Thrashing ("Seitenflattern"), die für sockelbasierte SSL-Proxys typisch sind
- Äußerst skalierbare Multi-Core-Architektur, die speziell für Infrastrukturen mit 10/40 Gbit/s entwickelt wurde

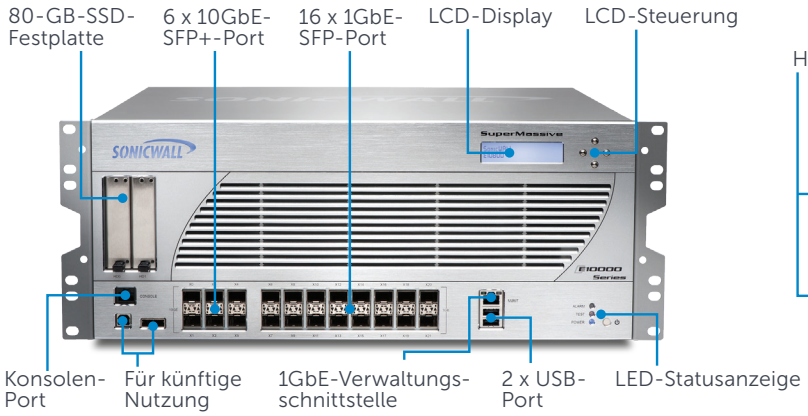
** US- Patente 7310815, 7600257, 7738380 und 7835361*

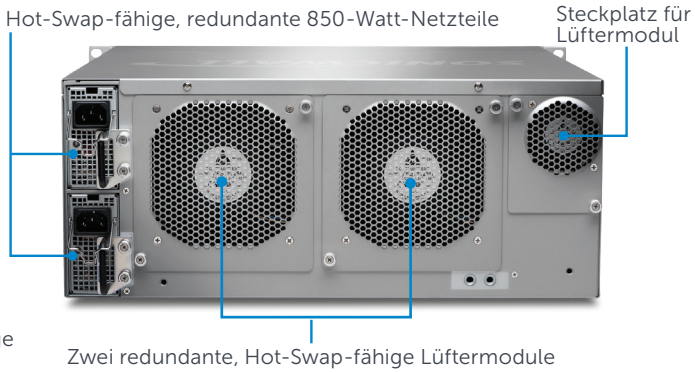
Überblick über die Serie

Das Dell SonicWALL SuperMassive E10000 Gehäuse ist mit sechs 10GbE-SFP+- und 16 1GbE-SFP-Ports, redundanten 850-Watt-Wechselstrom-Netzteilen sowie zwei redundanten, Hot-Swap-fähigen Lüftermodulen ausgestattet. Dank seiner extremen Skalierbarkeit lässt es sich auf bis zu 96 Verarbeitungskerne erweitern.

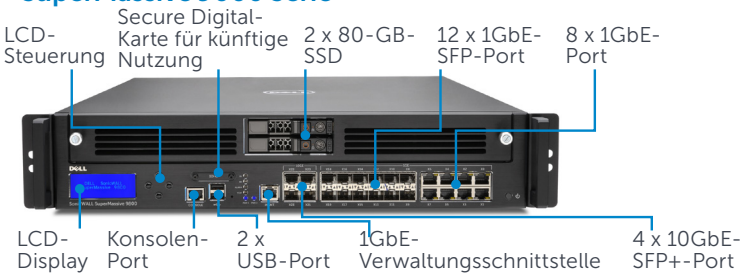
Die Dell SonicWALL SuperMassive 9000 Serie bietet vier 10GbE-SFP+-Ports, bis zu zwölf 1GbE-SFP-Ports, acht 1GbE-Kupferports und eine 1GbE-Verwaltungsschnittstelle sowie einen Erweiterungsport für zwei zusätzliche 10GbE-SFP+-Schnittstellen (zukünftige Version). Auch die 9000 Serie ist mit Hot-Swap-fähigen Lüftermodulen und Netzteilen ausgestattet.

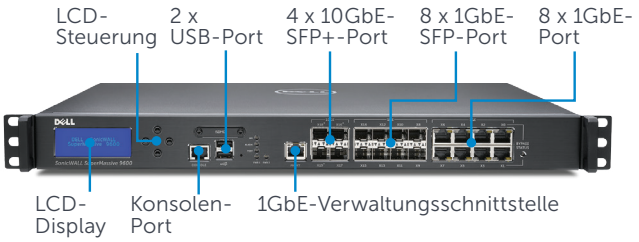
SuperMassive E10000 Serie





SuperMassive 9000 Serie





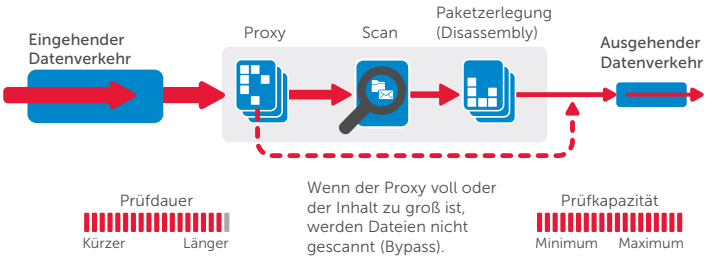
Leistungsmerkmale	9200	9400	9600	9800	E10400	E10800
Verarbeitungskerne	24	32	32	64	48	96
Firewall-Datendurchsatz	15 Gbit/s	20 Gbit/s	20 Gbit/s	40 Gbit/s	20 Gbit/s	40 Gbit/s
Datendurchsatz bei Anwendungserkennung	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	24 Gbit/s	15 Gbit/s	28 Gbit/s
IPS-Datendurchsatz (Intrusion Prevention System)	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	24 Gbit/s	15 Gbit/s	28 Gbit/s
Datendurchsatz bei Malware-Schutz	3,5 Gbit/s	4,5 Gbit/s	5 Gbit/s	10 Gbit/s	6 Gbit/s	12 Gbit/s
Maximale Anzahl an DPI-Verbindungen	1,25 Mio.	1,25 Mio.	1,5 Mio.	2,5 Mio.	5 Mio.	10 Mio.
Bereitstellungsmodi	**9200**	**9400**	**9600**	**9800**	**E10400**	**E10800**
L2-Bridge-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 Modus	Ja	Ja	Ja	Ja	Ja	Ja

Reassembly-Free Deep Packet Inspection Engine

Die RFDPI Engine bietet ein herausragendes Niveau an Bedrohungsschutz und Anwendungskontrolle, ohne die Leistung zu beeinträchtigen. Dabei prüft die patentierte Engine den Payload des Streaming-Datenverkehrs, um Bedrohungen auf den Layern 3 bis 7 zu identifizieren. Die RFDPI Engine normalisiert und entschlüsselt den Netzwerkdatenverkehr mehrfach und umfassend. Auf diese Weise lassen sich sogenannte AET (Advanced Evasion Technique)-Attacken verhindern, die versuchen, Erkennungs-Engines durch die Kombination mehrerer Umgehungsverfahren zu verwirren und Schadcode in das Netzwerk einzuschleusen.

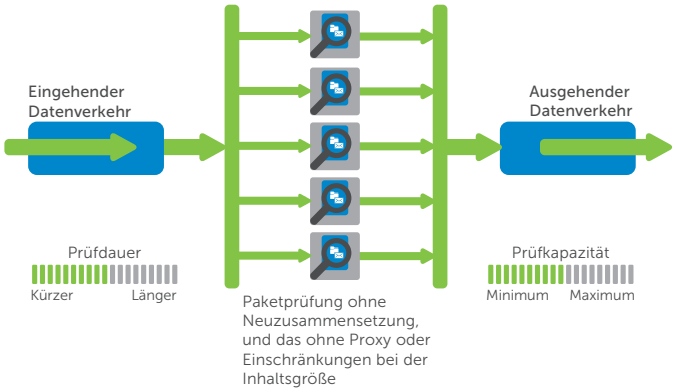
Sobald ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. die SSL-Entschlüsselung), wird es mit einer einzigen, proprietären Speicherdarstellung dreier Signaturdatenbanken abgeglichen: Eindringversuche, Malware und Anwendungen. Anschließend wird der Verbindungsstatus kontinuierlich entsprechend der Position des Streams in Bezug auf diese Datenbanken angepasst, bis ein Angriff oder ein anderes Treffereignis identifiziert wird. Tritt dieser Fall ein, wird eine vordefinierte Aktion eingeleitet. In den meisten Fällen wird die Verbindung beendet und es werden entsprechende Protokollierungs- und Benachrichtigungsereignisse erstellt. Daneben bietet die Engine jedoch auch weitere Konfigurationsmöglichkeiten. So kann sie beispielsweise ausschließlich zur Überprüfung verwendet werden oder bei aktivierter Anwendungserkennung sofort nach Identifizierung einer Anwendung während des restlichen Anwendungs-Streams Bandbreitenverwaltungsservices auf Layer 7 bereitstellen.

Verfahren mit Paketzusammensetzung (Assembly)



Architektur von Mitbewerberlösungen

Verfahren ohne Neuzusammensetzung der Pakete (Reassembly-Free)

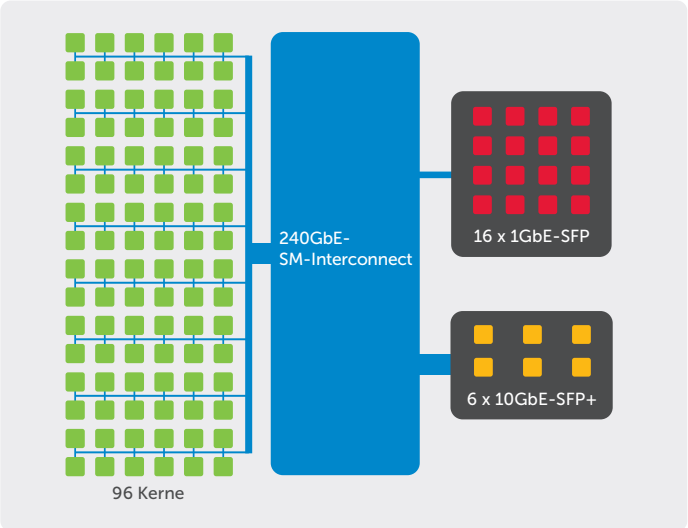


Dell SonicWALL Architektur

Erweiterbare Architektur für extreme Skalierbarkeit und Leistung

Die RFDPI Engine wurde von Grund auf so entwickelt, dass Sicherheitsscans bei hoher Leistung durchgeführt werden können. Damit ist sie perfekt auf den inhärent parallelen und stetig zunehmenden Datenverkehr in modernen Netzwerken abgestimmt. In Kombination mit den Hardwaresystemen mit 24, 32, 48, 64 oder 96 Verarbeitungskernen lässt sich diese für parallele Verarbeitung optimierte Softwarearchitektur mühelos vertikal skalieren und ermöglicht so effiziente Deep Packet Inspection (DPI) auch bei hoher Datenverkehrslast. Die SuperMassive Plattform arbeitet mit Prozessoren, die – anders als x86-Plattformen – speziell auf die Verarbeitung von Paketen, verschlüsselten Daten sowie Netzwerkdatenverkehr ausgelegt sind und dabei gleichzeitig Flexibilität und Programmierbarkeit direkt am Kundenstandort garantieren. ASIC-Systeme können das nicht bieten. Diese Flexibilität ist besonders wichtig, wenn neue Code- und Verhaltens-Updates nötig sind, um sich vor neuen Angriffen zu schützen, die modernste und noch komplexere Erkennungsmethoden erfordern.

Ein weiteres einzigartiges Merkmal der Plattform ist, dass sie auf jedem Kern im System neue Verbindungen aufbauen kann. Das gewährleistet ultimative Skalierbarkeit und erlaubt eine souveräne Bewältigung von Datenverkehrsspitzen. Dank dieses Ansatzes ist auch bei aktivierter Deep Packet Inspection eine extrem hohe Rate an neu aufgebauten Verbindungen pro Sekunde möglich – eine entscheidende Kenngröße, die in Rechenzentren häufig zu Engpässen führt.



Sicherheit und Schutz

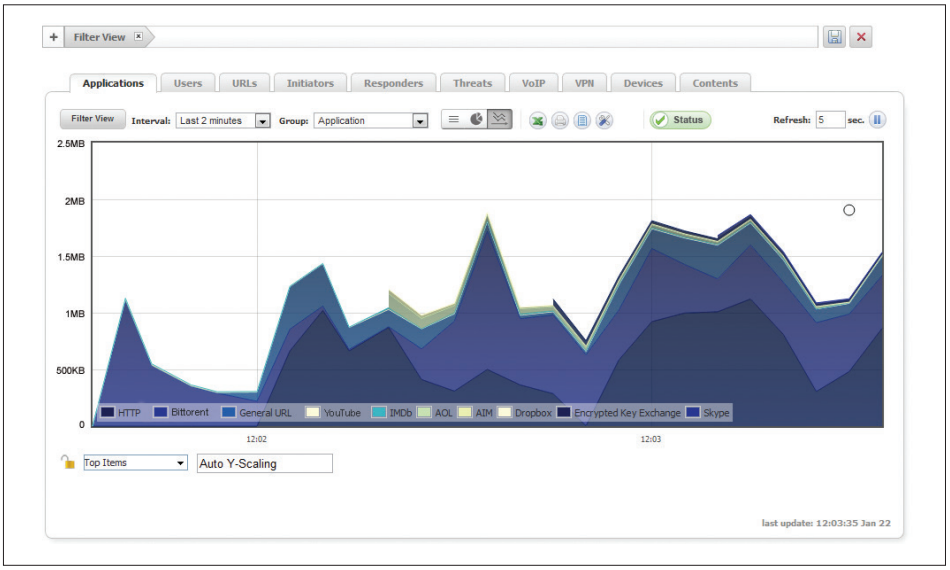
Das dedizierte interne Dell SonicWALL Threat Research Team ist für die Erforschung und Entwicklung von Abwehrmechanismen zuständig. Diese werden für die vor Ort bei unseren Kunden installierten Firewalls bereitgestellt, um jederzeit topaktuellen Schutz zu gewährleisten. Das Team greift dabei auf mehr als eine Million weltweit verteilte Sensoren zurück, die Malware-Muster und Telemetriedaten zu den neuesten Bedrohungen erfassen. Diese Informationen werden anschließend in die Systeme für Angriffsvermeidung, Malware-Schutz und Anwendungserkennung eingespeist. Kunden, die Dell SonicWALL NGFWs mit den neuesten Sicherheitsfunktionen einsetzen, erhalten rund um die Uhr aktualisierten Bedrohungsschutz. Neue Updates werden sofort implementiert – ohne Neustarts oder Betriebsunterbrechungen. 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 selbst bieten die SuperMassive Firewalls auch Zugang zum Dell SonicWALL CloudAV Service. Auf diese Weise wird die lokal verfügbare Signaturdatenbank um einen kontinuierlich wachsenden Pool mit derzeit über 17 Millionen Signaturen erweitert. Der Firewall-Zugriff auf die CloudAV Datenbank erfolgt über ein schlankes, proprietäres Protokoll und ist eine leistungsstarke Ergänzung der Überprüfungsfunktionen der Appliance. Dank effizienter Funktionen für Geo-IP- und Botnet-Filterung sind die Dell SonicWALL NGFWs in der Lage, Datenverkehr aus gefährlichen Domänen oder ganzen Regionen zu blockieren und können so die Sicherheitsrisiken im Netzwerk reduzieren.

Anwendungserkennung und Anwendungskontrolle

Über die Anwendungserkennung stehen Administratoren detaillierte Informationen zum Anwendungsdatenverkehr in ihrem Netzwerk zur Verfügung. So können sie die Anwendungskontrolle an den jeweils aktuellen Geschäftsprioritäten ausrichten, nicht produktive Anwendungen drosseln und potenziell gefährliche Anwendungen blockieren. Auffälligkeiten im Datenverkehr lassen sich dank Echtzeitvisualisierung augenblicklich identifizieren. So können unverzüglich Gegenmaßnahmen eingeleitet werden, um das Netzwerk vor Angriffen über ein- und ausgehenden Datenverkehr zu schützen oder Leistungsengpässe zu verhindern.

Dell SonicWALL Application Traffic Analytics erlaubt granulare Einblicke in den Anwendungsdatenverkehr, die Bandbreitennutzung sowie etwaige Sicherheitsbedrohungen und bietet leistungsstarke Fehlerbehebungs- und Forensikfunktionen. Zusätzlich steigern sichere Funktionen für die einmalige Anmeldung (Single Sign-On, SSO) die Benutzerfreundlichkeit und Produktivität und reduzieren die Anzahl an Support-Anfragen. Die Verwaltung der gesamten Anwendungserkennung und -kontrolle wird durch eine intuitive, webbasierte Oberfläche erheblich vereinfacht.



Globale Verwaltung und Berichterstellung

Mit dem optionalen Dell SonicWALL Global Management System (GMS®) steht Administratoren in größeren, verteilten Unternehmensumgebungen eine einheitliche, sichere und erweiterbare Plattform für die Verwaltung ihrer Dell SonicWALL Sicherheits-Appliances zur Verfügung. Mit ihr können Unternehmen die Verwaltung ihrer Sicherheits-Appliances unkompliziert konsolidieren, die Administration und Fehlerbehebung vereinfachen und alle betrieblichen Aspekte der Sicherheitsinfrastruktur steuern. Unter anderem bietet die Plattform zentralisierte Richtlinienverwaltung und -erzwingung sowie Ereignisüberwachung, Analysen und Berichterstellung in Echtzeit. Dank einer Funktion zur Workflow-Automatisierung können Unternehmen mit GMS zudem auch alle Änderungen an ihren Firewalls effektiv verwalten. Durch die GMS Workflow-Automatisierung kann jedes Unternehmen zum richtigen Zeitpunkt die richtigen Firewall-Richtlinien bereitstellen und so Agilität und Zuverlässigkeit steigern – bei vollständiger Einhaltung aller Compliance-Vorschriften. Mit GMS können Sie die Netzwerksicherheit jetzt besser auf Ihre Geschäftsprozesse und Servicestufen abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab statt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung drastisch vereinfachen lässt.

Merkmale

RFDPI Engine	
Merkmal	Beschreibung
Reassembly-Free Deep Packet Inspection (RFDPI)	Diese hochleistungsfähige proprietäre und patentierte Prüf-Engine führt eine streambasierte, bidirektionale Datenverkehrsanalyse durch, um Eindringversuche und Malware zu erkennen und den Anwendungsdatenverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy.
Bidirektionale Prüfung	Ein- und ausgehender Datenverkehr wird simultan auf Bedrohungen geprüft, um zu verhindern, dass das Netzwerk für die Verteilung von Malware oder als Ausgangspunkt für Angriffe genutzt wird, sollte ein infizierter Computer in die Umgebung gelangen.
Streambasierte Prüfung	Da die Prüfung ohne Proxys und Zwischenspeicherung stattfindet, können für Millionen Netzwerk-Streams gleichzeitig leistungsstarke DPI-Scans durchgeführt werden, bei ultraniedriger Latenz und ohne Einschränkungen bei Datei- oder Stream-Größe. Dabei kann die Engine nicht nur mit gängigen Protokollen, sondern auch mit reinen TCP-Streams umgehen.
Hohe Parallelität und Skalierbarkeit	Dank ihres einzigartigen Designs und der Multi-Core-Architektur erreicht die RFDPI Engine einen hohen DPI-Datendurchsatz und kann extrem viele neue Sitzungen pro Sekunde aufbauen. Datenverkehrsspitzen in anspruchsvollen Netzwerken lassen sich so souverän bewältigen.
Single-Pass-Inspection	Die Single-Pass-DPI-Architektur prüft den Datenverkehr auf Malware und Eindringversuche und stellt Anwendungserkennung bereit. Dadurch werden DPI-bedingte Latenzzeiten drastisch verkürzt. Außerdem wird sichergestellt, dass sämtliche Bedrohungsdaten innerhalb einer einzigen Architektur verarbeitet werden.

Angriffsvermeidung	
Merkmal	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes System zur Angriffsvermeidung (Intrusion Prevention System, IPS) nutzt Signaturen und andere Abwehrmechanismen, um den Paket-Payload auf Schwachstellen und Exploits zu prüfen. Dabei wird ein breites Spektrum an Angriffen und Schwachstellen abgedeckt.
Automatische Signatur-Updates	Das Dell SonicWALL Threat Research Team analysiert kontinuierlich Bedrohungen und aktualisiert fortlaufend unsere umfassende Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Neue Updates sind sofort wirksam und erfordern keine Neustarts oder sonstigen Betriebsunterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Eine Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Angriffsvermeidung steigert die interne Sicherheit und verhindert, dass Bedrohungen sich über Zonengrenzen hinweg ausbreiten.
Erkennung und Blockierung von Command-and-Control-Aktivitäten (CnC) durch Botnets	Die Lösung identifiziert und blockiert Command-and-Control-Datenverkehr, der von Bots im lokalen Netzwerk zu IP-Adressen und Domänen gesendet wird, die als Malware-Quellen oder bekannte CnC-Punkte identifiziert wurden.
Erkennung und Vermeidung von Protokollmissbrauch/ -anomalien	Angriffe, bei denen versucht wird, das IPS durch Protokollmissbrauch zu umgehen, werden identifiziert und blockiert.
Zero-Day-Schutz	Dank kontinuierlicher Updates zu den neuesten Exploit-Methoden und -Techniken wird das Netzwerk effektiv gegen Zero-Day-Attacken geschützt. Dabei werden Tausende Einzel-Exploits abgedeckt.
Umgehungs-schutztechnologie	Umfassende Stream-Normalisierung und -Entschlüsselung sowie weitere Maßnahmen verhindern, dass Angreifer Umgehungstechniken auf den Layern 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.

Merkmale

Bedrohungsabwehr	
Merkmal	Beschreibung
Malware-Schutz am Gateway	Die RFDPI Engine prüft den gesamten Datenverkehr auf Viren, Trojaner, Keylogger und andere Malware – ohne Einschränkungen bei Dateilänge oder -größe und über alle Ports und TCP-Streams hinweg.
CloudAV	Auf den Dell SonicWALL Cloud-Servern steht eine kontinuierlich aktualisierte Datenbank mit über 17 Millionen Bedrohungssignaturen bereit, die als Ergänzung zur integrierten Signaturdatenbank genutzt wird. So bietet die RFDPI Engine umfassenden Schutz vor einer breiten Palette an Bedrohungen.
Sicherheits-Updates rund um die Uhr	Das Dell SonicWALL Threat Research Team analysiert neue Bedrohungen und stellt Abwehrmechanismen bereit – 24 Stunden am Tag, sieben Tage die Woche. Neue Bedrohungs-Updates werden automatisch an Kunden-Firewalls mit aktiven Sicherheitsservices weitergeleitet und sind sofort wirksam, ohne Neustart oder Betriebsunterbrechungen.
SSL-Prüfung	SSL-Datenverkehr wird in Echtzeit und ohne Umweg über einen Proxy entschlüsselt und auf Malware, Eindringversuche und Datenlecks überprüft. Gleichzeitig werden Richtlinien für Anwendungs-, URL- und Inhaltskontrolle angewendet, um das Netzwerk gegen versteckte Bedrohungen in SSL-verschlüsseltem Datenverkehr abzusichern.
Bidirektionale Prüfung von reinem TCP-Datenverkehr	Die RFDPI Engine kann reine TCP-Streams auf jedem beliebigen Port bidirektional scannen. So werden Angriffe abgewehrt, die auf veraltete Sicherheitssysteme ausgelegt sind, bei denen nur einige weithin bekannte Ports abgesichert werden.
Unterstützung für zahlreiche Protokolle	Unsere Lösung identifiziert gängige Protokolle wie HTTP/S, FTP, SMTP und SMBv1/v2, die Daten nicht als reines TCP senden, und entschlüsselt den Payload für die Malware-Prüfung – auch dann, wenn sie nicht über weithin bekannte Standardports laufen.

Anwendungserkennung und -kontrolle	
Merkmal	Beschreibung
Anwendungskontrolle	Die RFDPI Engine nutzt eine kontinuierlich wachsende Datenbank mit über 3.600 Anwendungssignaturen, um Anwendungen oder einzelne Anwendungsfunktionen zu identifizieren und zu kontrollieren. Das steigert die Netzwerksicherheit und erhöht die Netzwerkproduktivität.
Identifizierung benutzerdefinierter Anwendungen	Die Lösung erstellt Signaturen für benutzerdefinierte Anwendungen, um die Kontrolle im Netzwerk weiter zu verstärken. Hierfür nutzt sie spezifische Parameter oder Muster, die für den Netzwerkdatenverkehr der betreffenden Anwendung charakteristisch sind.
Bandbreitenverwaltung auf Anwendungsebene	Bandbreitenkapazität kann für kritische Anwendungen oder Anwendungskategorien granular zugewiesen und reguliert werden. Gleichzeitig lässt sich jedweder nicht absolut notwendiger Anwendungsdatenverkehr unterbinden.
Integrierte/externe Datenverkehrs-visualisierung	Über integrierte Funktionen für die Echtzeitvisualisierung des Anwendungsdatenverkehrs sowie externe Funktionen für die Erstellung von Berichten zum Anwendungsdatenverkehr per NetFlow/IPFIX lässt sich die Bandbreitennutzung identifizieren und das Netzwerkverhalten analysieren.
Granulare Kontrolle	Die Lösung kontrolliert Anwendungen oder spezifische Anwendungskomponenten auf Basis von Zeitplänen, Benutzergruppen, Ausschlusslisten und einer Reihe von Aktivitäten. Dank Integration mit LDAP/AD/Terminaldiensten/Citrix ist eine vollständige SSO-Benutzeridentifizierung möglich.

Merkmale

Inhaltsfilterung	
Merkmal	Beschreibung
Interne/externe Inhaltsfilterung	Über den Content Filtering Service lassen sich Richtlinien zu Nutzungseinschränkungen effektiv erzwingen und Webseiten mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren. Mit dem Content Filtering Client kann die Richtlinienerzwingung zudem erweitert werden, um Internetinhalte auch auf Geräten außerhalb des Firewall-Perimeters 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.
Dynamische Bewertungsarchitektur	Alle angefragten Webseiten werden in Echtzeit mit einer cloudbasierten, dynamisch aktualisierten Datenbank abgeglichen, die Millionen kategorisierter URLs, IP-Adressen und Domänen umfasst.
YouTube für Schulen	Lehrkräften stehen auf YouTube EDU Hunderttausende kostenlose Lernvideos zur Verfügung, die nach Themen und Bildungsstufe sortiert sind und allgemeinen Unterrichtsstandards entsprechen.
Webcaching	URL-Bewertungen werden lokal in der Dell SonicWALL Firewall zwischengespeichert, sodass die Reaktionszeiten beim Aufruf häufig besuchter Webseiten nur Sekundenbruchteile betragen.

Erzwingung von Viren- und Spyware-Schutz	
Merkmal	Beschreibung
Mehrstufiger Schutz	Die Gateway-Virenschutzlösung einer Firewall ist die erste Verteidigungsstufe am Netzwerkperimeter. Viren können jedoch trotzdem über Notebooks, USB-Sticks und andere ungeschützte Systeme in das Netzwerk gelangen. Mit unserem mehrstufigen Ansatz können Sie einen Viren- und Spyware-Schutz implementieren, der sowohl Clientsysteme als auch Server abdeckt.
Automatisierte Erzwingung	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. Das eliminiert die Kosten, die typischerweise mit der Verwaltung von Desktop-Lösungen für Viren- und Spyware-Schutz verbunden sind.
Automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz müssen nicht auf jedem Rechner separat bereitgestellt und installiert werden. Bereitstellung und Installation werden automatisch und netzwerkweit durchgeführt, sodass der administrative Mehraufwand minimiert wird.
Unterbrechungsfreier und 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.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt Desktop-PCs und Notebooks auf eine umfangreiche Palette an Spyware-Programmen und blockiert deren Installation – bevor sie vertrauliche Daten übertragen können. Das steigert die Sicherheit und Leistung Ihrer Desktop-Umgebung.

Merkmale

Firewall und Netzwerkbetrieb

Merkmal	Beschreibung
Stateful Packet Inspection	Der gesamte Netzwerkdatenverkehr wird geprüft und analysiert. Dabei wird sichergestellt, dass Firewall-Zugriffsrichtlinien eingehalten werden.
Schutz vor DDoS-/DoS-Angriffen	Eine Kombination aus SYN-Proxy-Technologie auf Layer 3 und SYN-Blacklisting auf Layer 2 sorgt für SYN-Flood-Schutz und wehrt DOS-Angriffe ab. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsrate vor DoS-/DDoS-Angriffen schützen.
Flexible Bereitstellungsoptionen	Die SuperMassive Serie lässt sich im konventionellen NAT-Modus, als Layer 2-Bridge, im Wire-Modus oder im Network Tap-Modus bereitstellen.
Unterstützung für IPv6	Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) hat gerade erst begonnen. Mit der neuesten Betriebssystemversion SonicOS 6.2 unterstützt die Hardware IPv6-Implementierungen für die Filterung und den Wire-Modus.
Hochverfügbarkeit/ Clustering	Die SuperMassive Serie unterstützt die Hochverfügbarkeitsmodi Active/Passive (A/P) mit Zustandssynchronisierung, Active/Active (A/A) DPI und Active/Active Clustering. Im Active/Active DPI-Modus wird die Deep Packet Inspection auf Kerne auf der passiven Appliance ausgelagert, um den Datendurchsatz zu steigern.
WAN-Lastausgleich	Die Lösung ermöglicht den Lastausgleich über mehrere WAN-Schnittstellen hinweg. Zur Verfügung stehen verschiedene Methoden: Round Robin, Spillover und Percentage.
Richtlinienbasiertes Routing	Diese Funktion erstellt Routen auf Basis des verwendeten Protokolls, um den Datenverkehr auf eine bevorzugte WAN-Verbindung umzuleiten. Bei Ausfällen ist ein Failback auf ein sekundäres WAN möglich.
Erweiterte QoS (Quality of Service)	802.1p, DSCP-Tagging und die Neuzuweisung von VoIP-Datenverkehr im Netzwerk garantieren Bandbreite für kritischen Datenverkehr.
Unterstützung für H.323-Gatekeeper und SIP-Proxys	Alle eingehenden Anrufe müssen durch den H.323-Gatekeeper oder den SIP-Proxy autorisiert und authentifiziert werden. So werden Spam-Anrufe blockiert.

Verwaltung und Berichterstellung

Merkmal	Beschreibung
Global Management System	Dell SonicWALL GMS gibt Ihnen eine einzige Verwaltungskonsole mit intuitiver Oberfläche an die Hand, mit der Sie mehrere Dell SonicWALL Appliances in Ihrem Netzwerk zentral überwachen und konfigurieren sowie Berichte erstellen können. Die Verwaltung wird kostengünstiger und einfacher.
Leistungsstarke Verwaltung auf Geräteebene	Eine intuitive, webbasierte Oberfläche erlaubt eine schnelle und bequeme Konfiguration. Die Lösung stellt Ihnen zudem eine umfassende Befehlsschnittstelle zur Verfügung und unterstützt SNMPv2/3.
IPFIX/NetFlow Berichte zum Anwendungsdatenverkehr	Analysedaten zum Anwendungsdatenverkehr und Daten zur Anwendungsnutzung lassen sich per IPFIX- oder NetFlow-Protokoll exportieren. Anschließend können sie von Tools wie Dell SonicWALL Scrutinizer und anderen Tools, die IPFIX und NetFlow mit Erweiterungen unterstützen, für Überwachung und Berichterstellung genutzt werden – wahlweise in Echtzeit oder verlaufsbasiert.

VPNs (virtuelle private Netzwerke)

Merkmal	Beschreibung
IPsec-VPN für Site-to-Site-Konnektivität	Dank eines hochleistungsfähigen IPsec-VPNs kann die SuperMassive Serie als VPN-Konzentrator für Tausende anderer großer Standorte, Zweigstellen oder Heimbüros genutzt werden.
Remote-Zugriff per SSL-VPN oder IPsec-Client	Benutzer können mithilfe der clientlosen SSL-VPN-Technologie oder eines einfach zu verwaltenden IPsec-Clients unkompliziert auf E-Mails, Dateien, Computer, Intranetseiten und Anwendungen zugreifen, und das über eine Vielzahl verschiedener Plattformen.
Redundantes VPN-Gateway	Wenn Sie mit mehreren WANs arbeiten, können Sie ein primäres und ein sekundäres VPN konfigurieren und so für alle VPN-Sitzung nahtloses automatisches Failover und Failback gewährleisten.

Merkmale

VPNs (Fortsetzung)

Merkmal	Beschreibung
Routenbasiertes VPN	Dank dynamischem Routing über VPN-Links lässt sich auch beim temporären Ausfall eines VPN-Tunnels unterbrechungsfreier Betrieb gewährleisten. Der Datenverkehr zwischen den betroffenen Endpunkten wird nahtlos über alternative Routen geleitet.

Inhalts-/Kontextsensitivität

Merkmal	Beschreibung
Nachverfolgung von Benutzeraktivitäten	Dank nahtloser SSO-Integration von AD/LDAP/Citrix[1]/Terminaldiensten[1] und umfassenden DPI-Daten können Benutzer identifiziert und Benutzeraktivitäten nachverfolgt werden.
Datenverkehrs-identifizierung nach Herkunftsland mittels Geo-IP	Die Lösung kann Datenverkehr in oder aus spezifischen Ländern identifizieren und kontrollieren. So schützen Sie Ihr Netzwerk gegen Angriffe aus bekannten oder vermuteten Bedrohungsquellen und können verdächtigen Datenverkehr aus Ihrem Netzwerk analysieren.
DPI-Filterung mit regulären Ausdrücken	Alle Inhalte, die das Netzwerk passieren, können mithilfe regulärer Ausdrücke identifiziert und kontrolliert werden, um Datenlecks vorzubeugen.

SonicOS Funktions- und Merkmalsübersicht

Firewall
- Reassembly-Free Deep Packet Inspection
- SSL-Entschlüsselung und -Prüfung
- Stateful Packet Inspection
- Stealth-Modus
- Unterstützung für Common Access Cards (CACs)
- Schutz vor DoS-Angriffen
- UDP-/ICMP-/SYN-Flood-Schutz
- IPv6-Sicherheit
- Verwaltung und Überwachung: IPv4- und IPv6-Verwaltung
- Netzwerkbetrieb: IPv6

Angriffsvermeidung
- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granularer IPS-Regelsatz
- Filterung auf Basis von Geo-IP und Reputation
- Abgleich mit regulären Ausdrücken
- UDP-/ICMP-/SYN-Flood-Schutz

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

Anwendungserkennung
- Anwendungskontrolle
- Blockierung von Anwendungskomponenten
- Bandbreitenverwaltung auf Anwendungsebene
- Signaturerstellung für benutzerdefinierte Anwendungen
- Visualisierung des Anwendungsdatenverkehrs
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Nachverfolgung der Benutzeraktivitäten (SSO)
- Umfassende Datenbank mit Anwendungssignaturen

Filterung von Webinhalten
- URL-Filterung
- Anti-Proxy-Technologie
- Schlüsselwortblockierung
- Bandbreitenverwaltung anhand von CFS Kategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- 56 Kategorien für die Inhaltsfilterung
- Content Filtering Client (SonicOS 6.2)

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

Netzwerkbetrieb
- Jumbo Frames (nur SonicOS 6.0.5 und 6.2)
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Layer 2-Netzwerkerkennung
- Portspiegelung
- Layer 2-QoS
- Portsicherheit
- Dynamisches Routing
- SonicPoint Wireless-Controller[1]
- Richtlinienbasiertes Routing
- Erweiterte NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation
- Portredundanz
- Hochverfügbarkeitsmodus A/P mit Zustandssynchronisierung
- A/A-Clustering
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge, Wire-Modus, Tap-Modus, NAT-Modus

VoIP
- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- Unterstützung für H.323-Gatekeeper und SIP-Proxys

Verwaltung und Überwachung
- Webbasierte grafische Benutzeroberfläche
- Befehlsschnittstelle
- SNMPv2/v3
- Externe Berichterstellung (Scrutinizer)
- Zentralisierte Verwaltung und Berichterstellung mit dem Dell SonicWALL Global Management System (GMS)[2]
- Protokollierung
- NetFlow-/IPFIX-Export
- Anwendungs- und Bandbreitenvisualisierung
- LCD-Display für die Verwaltung
- Einmalige Anmeldung (Single Sign-On, SSO)
- Unterstützung für Terminaldienste/Citrix[1]
- Blue Coat Security Analytics Platform

[1] Unterstützt unter SonicOS 6.1 und 6.2. Nicht unterstützt unter SonicOS 6.2.1.
[2] Das Dell SonicWALL Global Management System (GMS) muss separat erworben werden.

Systemspezifikationen SuperMassive E10000 Serie

	E10400	E10800
Betriebssystem	SonicOS	
Dedizierte Verarbeitungskerne für die Sicherheitsfunktionen	48	96
10GbE-Schnittstellen	6 x 10GbE-SFP+	
1GbE-Schnittstellen	16 x 1GbE-SFP	
Verwaltungsschnittstellen	1 x GbE, 1 x Konsole	
Arbeitsspeicher (RAM)	32 GB	64 GB
Massenspeicher	80-GB-SSD-Festplatte, Flash-Speicher	
Datendurchsatz bei Firewall-Überprüfung[1]	20 Gbit/s	40 Gbit/s
Datendurchsatz bei Anwendungsüberprüfung[2]	15 Gbit/s	28 Gbit/s
IPS-Datendurchsatz[2]	15 Gbit/s	28 Gbit/s
Datendurchsatz bei Malware-Überprüfung[2]	6 Gbit/s	12 Gbit/s
IMIX-Leistung	5,3 Gbit/s	10 Gbit/s
SSL-DPI-Leistung	3 Gbit/s	5 Gbit/s
VPN-Datendurchsatz[3]	10 Gbit/s	20 Gbit/s
Latenzzeit	24 µs	
Verbindungen pro Sekunde	200.000/s	400.000/s
Max. Anzahl an Verbindungen (SPI)	6 Mio.	12 Mio.
Max. Anzahl an Verbindungen (DPI)	5 Mio.	10 Mio.
SSO-Benutzer	40.000	60.000
VPN	**E10400**	**E10800**
Site-to-Site-Tunnel	10.000	
IPsec-VPN-Clients (Maximum)	2.000 (10.000)	
Verschlüsselung	DES, 3DES, AES (128/192/256 Bit)	
Authentifizierung	MD5, SHA-1, Common Access Card (CAC)	
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5 und 14	
Routenbasiertes VPN	RIP, OSPF	
Netzwerkbetrieb	**E10400**	**E10800**
IP-Adresszuweisung	Statisch, interner DHCP-Server, DHCP-Relay	
NAT-Modi	1:1, n:1, 1:n, flexible NAT (überlappende IPs), PAT, transparenter Modus	
VLAN-Schnittstellen	1.024	2.048
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, richtlinienbasiertes Routing, Multicast	
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p	
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix	
VoIP	Volle Unterstützung für H.323-v1-5, SIP	
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
Zertifizierungen	FIPS 140-2, Common Criteria NDPP, IPv6 Phase 2, VPAT, VPNC	
Verifizierung durch Dritte	NSS NGFW Recommended (Von NSS empfohlene NGFW) und NSS IPS Recommended (Von NSS empfohlenes IPS)	
Hardware	**E10400**	**E10800**
Stromversorgung	Zwei redundante, Hot-Swap-fähige 850-Watt-Netzteile	
Lüfter	Zwei redundante, Hot-Swap-fähige Lüfter	
Display	LED-Display vorne	
Eingangsleistung	100–240 V Wechselstrom, 50–60 Hz	
Maximaler Stromverbrauch (W)	550	750
MTBF bei 25 °C in Stunden	120.790	
MTBF bei 25 °C in Jahren	13,789	
Formfaktor	4 HE (geeignet für Rack-Montage)	
Abmessungen	43 x 43,5 x 17,8 cm (17 x 18 x 7 Zoll)	
Gewicht	27,7 kg (61 lb)	30,3 kg (67 lb)
WEEE-Gewicht	28,1 kg (62 lb)	30,8 kg (68 lb)
Versandgewicht	37,2 kg (82 lb)	39,9 kg (88 lb)
Wichtige gesetzliche Vorschriften	FCC Klasse A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE	
Umgebung	5–40 °C (40–105 °F)	
Luftfeuchtigkeit	10–90 % (nicht kondensierend)	

[1] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Netzwerkbedingungen und aktivierten Services variieren.
[2] Der Datendurchsatz bei vollständiger DPI/Virenschutz am Gateway/Spyware-Schutz/IPS wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia Testtools nach Branchenstandard gemessen. Die Tests wurden mit mehreren Datenströmen über mehrere Portpaare durchgeführt. [3] Der VPN-Datendurchsatz wurde gemäß RFC 2544 gemessen, unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte. Änderungen von Spezifikationen, Funktionen und Verfügbarkeit vorbehalten.

Systemspezifikationen SuperMassive 9000 Serie

	9200	9400	9600	9800
Betriebssystem	SonicOS			
Dedizierte Verarbeitungskerne für die Sicherheitsfunktionen	24	32		64
10GbE-Schnittstellen	4 x 10GbE-SFP+			
1GbE-Schnittstellen	8 x 1GbE-SFP, 8 x 1GbE (ein LAN-Bypass-Paar)			12 x 1GbE-SFP, 8 x 1GbE
Verwaltungsschnittstellen	1 x GbE, 1 x Konsole			
Arbeitsspeicher (RAM)	8 GB	16 GB	32 GB	64 GB
Massenspeicher	Flash-Speicher			Zwei 80-GB-SSD-Festplatten, Flash-Speicher
Erweiterung	Ein Erweiterungssteckplatz (hinten)*, Secure Digital-Karte*			
Datendurchsatz bei Firewall-Überprüfung[1]	15 Gbit/s	20 Gbit/s		40 Gbit/s
Datendurchsatz bei Anwendungsüberprüfung[2]	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	24 Gbit/s
IPS-Datendurchsatz[2]	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	24 Gbit/s
Datendurchsatz bei Malware-Überprüfung[2]	3,5 Gbit/s	4,5 Gbit/s	5 Gbit/s	10 Gbit/s
IMIX-Leistung	4,4 Gbit/s	5,5 Gbit/s		9 Gbit/s
SSL-DPI	1 Gbit/s	2 Gbit/s	2 Gbit/s	5 Gbit/s
VPN-Datendurchsatz[3]	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	18 Gbit/s
Latenzzeit	17 µs			
Verbindungen pro Sekunde	100.000/s	130.000/s		280.000/s
Max. Anzahl an Verbindungen (SPI)	1,25 Mio.		1,5 Mio.	3 Mio.
Max. Anzahl an Verbindungen (DPI)	1 Mio.		1,25 Mio.	2,5 Mio.
SSO-Benutzer	80.000	90.000	100.000	110.000
Maximale Anzahl unterstützter SonicPoints	128			–
VPN	**9200**	**9400**	**9600**	**9800**
Site-to-Site-Tunnel	10.000			25.000
IPsec-VPN-Clients (Maximum)	2.000 (4.000)	2.000 (6.000)	2.000 (10.000)	2.000 (10.000)
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 und 14v			
Routenbasiertes VPN	RIP, OSPF			
Netzwerkbetrieb	**9200**	**9400**	**9600**	**9800**
IP-Adresszuweisung	Statisch, DHCP-, PPPoE-, L2TP- und PPTP-Client, interner DHCP-Server, DHCP-Relay[4]			
NAT-Modi	1:1, n:1, 1:n, flexible NAT (überlappende IPs), PAT, transparenter Modus			
VLAN-Schnittstellen	512			
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, richtlinienbasiertes Routing, Multicast			
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p			
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste[5], Citrix[5]			
VoIP	Volle Unterstützung für H.323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Zertifizierungen	ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, CSfC, USGv6			
Ausstehende Zertifizierungen	FIPS 140-2, Common Criteria NDPP, ICSA Anti-Virus, UC-APL			
Hardware	**9200**	**9400**	**9600**	**9800**
Stromversorgung	Zwei redundante, Hot-Swap-fähige 300-Watt-Netzteile			Zwei redundante, Hot-Swap-fähige 500-Watt-Netzteile
Lüfter	Zwei redundante, Hot-Swap-fähige Lüfter			
Display	LED-Display vorne			
Eingangsleistung	100–240 V Wechselstrom, 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	21,543	21,427	21,284	14,400
Formfaktor	1 HE (geeignet für Rack-Montage)			2 HE (geeignet für Rack-Montage)
Abmessungen	43,3 x 48,5 x 4,5 cm (17 x 19,1 x 1,75 Zoll)			9 x 60 x 43 cm (17 x 24 x 3,5 Zoll)
Gewicht	8,2 kg (18,1 lb)			18,38 kg (40,5 lb)
WEEE-Gewicht	10,4 kg (23 lb)			22,4 kg (49,5 lb)
Versandgewicht	13,3 kg (29,3 lb)			29,64 kg (65 lb)
Wichtige gesetzliche Vorschriften	FCC Klasse A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE, ANATEL, BSMI			
Umgebung	0–40 °C (32–105 °F)			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 Netzwerkbedingungen und aktivierten Services variieren. [2] Der Datendurchsatz bei vollständiger DPI/Virenschutz am Gateway/Spyware-Schutz/IPS wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia Testtools nach Branchenstandard gemessen. Die Tests wurden mit mehreren Datenströmen über mehrere Portpaare durchgeführt. [3] Der VPN-Datendurchsatz wurde gemäß RFC 2544 gemessen, unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte. [4] PPPoE-, L2TP- und PPTP-Clients werden von der SM9800 nicht unterstützt. [5] Unterstützt unter SonicOS 6.1 und 6.2. *Für künftige Nutzung. Änderungen von Spezifikationen, Funktionen und Verfügbarkeit vorbehalten.

Bestellinformationen SuperMassive E10000 Serie

Produkt	SKU
SuperMassive E10400, sechs 10GbE-SFP+-Ports, 16 1GbE-SFP-Ports, zwei Lüfter, zwei Wechselstrom-Netzteile	01-SSC-8881
SuperMassive E10800, sechs 10GbE-SFP+-Ports, 16 1GbE-SFP-Ports, zwei Lüfter, zwei Wechselstrom-Netzteile	01-SSC-8856
System-Upgrades	**SKU**
Upgrade SuperMassive E10200 auf E10400	01-SSC-9497
Upgrade SuperMassive E10400 auf E10800	01-SSC-9498
SuperMassive E10400 Support- und Sicherheits-Abonnements	**SKU**
Threat Prevention: Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für die E10400 (ein Jahr)	01-SSC-9536
Application Intelligence and Control: Application Intelligence, Application Control, App Flow Visualization für die E10400 (ein Jahr)	01-SSC-9542
Content Filtering Premium Business Edition für die E10400 (ein Jahr)	01-SSC-9539
Platinum Support für die SuperMassive E10400 (ein Jahr)	01-SSC-9548
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering und Support für die E10400 (ein Jahr)	01-SSC-9551
SuperMassive E10800 Support- und Sicherheits-Abonnements	**SKU**
Application Intelligence and Control: Application Intelligence, Application Control, App Flow Visualization für die E10800 (ein Jahr)	01-SSC-9560
Threat Prevention: Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für die E10800 (ein Jahr)	01-SSC-9554
Content Filtering Premium Business Edition für die E10800 (ein Jahr)	01-SSC-9557
Platinum Support für die SuperMassive E10800 (ein Jahr)	01-SSC-9566
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering und Support für die E10800 (ein Jahr)	01-SSC-9569
Module und Zubehör*	**SKU**
Systemlüfter für die SuperMassive E10000 Serie (FRU)	01-SSC-8885
SSD-Lüftermodul für die SuperMassive E10000 Serie	01-SSC-8886
Netzteil für die SuperMassive E10000 Serie (FRU)	01-SSC-8887
10GBASE-SR-SFP+-Modul (Short Reach)	01-SSC-9785
10GBASE-LR-SFP+-Modul (Long Reach)	01-SSC-9786
10GBASE-SFP+-Twinax-Kabel, 1 m	01-SSC-9787
10GBASE-SFP+-Twinax-Kabel, 3 m	01-SSC-9788
1000BASE-SX-SFP-Modul (Short Haul)	01-SSC-9789
1000BASE-LX-SFP-Modul (Long Haul)	01-SSC-9790
1000BASE-T-SFP-Kupfermodul	01-SSC-9791
Verwaltung und Berichterstellung	**SKU**
Dell SonicWALL GMS Softwarelizenz für zehn Knoten	01-SSC-3363
Dell SonicWALL GMS E-Class Software-Support mit Rund-um-die-Uhr-Verfügbarkeit für zehn Knoten (ein Jahr)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance mit Softwarelizenz für das Flow Analytics Modul für bis zu fünf Knoten (einschließlich ein Jahr mit Software-Support rund um die Uhr)	01-SSC-3443
Dell SonicWALL Scrutinizer mit Softwarelizenz für das Flow Analytics Modul für bis zu fünf Knoten (einschließlich ein Jahr mit Software-Support rund um die Uhr)	01-SSC-4002
Softwarelizenz für das Dell SonicWALL Scrutinizer Advanced Reporting Modul für bis zu fünf Knoten (einschließlich ein Jahr mit Software-Support rund um die Uhr)	01-SSC-3773

* Eine vollständige Liste aller unterstützten SFP- und SFP+-Module erhalten Sie von Ihrem Dell SE.

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

Bestellinformationen SuperMassive 9000 Serie

Produkt	SKU
SuperMassive 9800	01-SSC-0200
SuperMassive 9800 High Availability	01-SSC-0801
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 Sicherheits-Abonnements	**SKU**
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering und Support für die 9200 (ein Jahr)	01-SSC-4172
Intrusion Prevention, Anti-Malware, CloudAV und Application Intelligence, Control and Visualization für die SuperMassive 9200 (ein Jahr)	01-SSC-4202
Content Filtering Premium Business Edition für die 9200 (ein Jahr)	01-SSC-4184
Platinum Support für die SuperMassive 9200 (ein Jahr)	01-SSC-4178
SuperMassive 9400 Support- und Sicherheits-Abonnements	**SKU**
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering und Support für die 9400 (ein Jahr)	01-SSC-4136
Intrusion Prevention, Anti-Malware, CloudAV und Application Intelligence, Control and Visualization für die SuperMassive 9400 (ein Jahr)	01-SSC-4166
Content Filtering Premium Business Edition für die 9400 (ein Jahr)	01-SSC-4148
Platinum Support für die SuperMassive 9400 (ein Jahr)	01-SSC-4142
SuperMassive 9600 Support- und Sicherheits-Abonnements	**SKU**
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering und Support für die 9600 (ein Jahr)	01-SSC-4100
Intrusion Prevention, Anti-Malware, CloudAV und Application Intelligence, Control and Visualization für die SuperMassive 9600 (ein Jahr)	01-SSC-4130
Content Filtering Premium Business Edition für die 9600 (ein Jahr)	01-SSC-4112
Platinum Support für die SuperMassive 9600 (ein Jahr)	01-SSC-4106
SuperMassive 9800 Support- und Sicherheits-Abonnements	**SKU**
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering und Support für die 9800 (ein Jahr)	01-SSC-0809
Intrusion Prevention, Anti-Malware, CloudAV und Application Intelligence, Control and Visualization für die SuperMassive 9800 (ein Jahr)	01-SSC-0827
Content Filtering Premium Business Edition für die 9800 (ein Jahr)	01-SSC-0821
Gold Support mit Rund-um-die-Uhr-Verfügbarkeit für SuperMassive 9800 (ein Jahr)	01-SSC-0815
Module und Zubehör*	**SKU**
Systemlüfter für die Dell SonicWALL SuperMassive 9800 Serie (FRU)	01-SSC-0204
Wechselstrom-Netzteil für die Dell SonicWALL SuperMassive 9800 Serie (FRU)	01-SSC-0203
Systemlüfter für die Dell SonicWALL SuperMassive 9000 Serie (FRU)	01-SSC-3876
Wechselstrom-Netzteil für die Dell SonicWALL SuperMassive 9000 Serie (FRU)	01-SSC-3874
10GBASE-SR-SFP+-Modul (Short Reach)	01-SSC-9785
10GBASE-LR-SFP+-Modul (Long Reach)	01-SSC-9786
1000BASE-SX-SFP-Modul (Short Haul)	01-SSC-9789
1000BASE-LX-SFP-Modul (Long Haul)	01-SSC-9790
1000BASE-T-SFP-Kupfermodul	01-SSC-9791
Verwaltung und Berichterstellung	**SKU**
Dell SonicWALL GMS Softwarelizenz für zehn Knoten	01-SSC-3363
Dell SonicWALL GMS E-Class Software-Support mit Rund-um-die-Uhr-Verfügbarkeit für zehn Knoten (ein Jahr)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance mit Softwarelizenz für das Flow Analytics Modul für bis zu fünf Knoten (einschließlich ein Jahr mit Software-Support rund um die Uhr)	01-SSC-3443
Dell SonicWALL Scrutinizer mit Softwarelizenz für das Flow Analytics Modul für bis zu fünf Knoten (einschließlich ein Jahr mit Software-Support rund um die Uhr)	01-SSC-4002
Softwarelizenz für das Dell SonicWALL Scrutinizer Advanced Reporting Modul für bis zu fünf Knoten (einschließlich ein Jahr mit Software-Support rund um die Uhr)	01-SSC-3773

* Eine vollständige Liste aller unterstützten SFP- und SFP+-Module erhalten Sie von Ihrem Dell SE.

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

Weitere Informationen

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
Telefon: +1 408.745.9600
Fax: +1 408.745.9300

DataSheet-SonicWALL-SuperMassive-US-KS-25437