

E10000
Series

Die SonicWALL® SuperMassive™ E10000-Serie, SonicWALLs Next-Generation Firewall-Plattform für große Netzwerke, bietet höchste Skalierbarkeit, Zuverlässigkeit und Sicherheit in Multi-Gigabit-Geschwindigkeit. 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, Datacentern und Serverfarmen. Dank ihrer ultraskalierbaren Multicore-Architektur und SonicWALLs patentierter* Reassembly-Free Deep Packet Inspection™ (RFDPI)-Technologie bietet die SuperMassive E10000-Serie führende Funktionen für Intrusion Prevention, Anwendungskontrolle, Malware-Sicherheit und SSL-Inspektion in Multi-Gigabit-Geschwindigkeit. Entwickelt wurde die SonicWALL E10000-Serie mit besonderem Augenmerk auf einen geringen Strom-, Platz- und Kühlungsbedarf. Daher bietet sie den höchsten Durchsatz pro Watt (GBit/s/Watt) in den Bereichen Anwendungskontrolle und Threat Prevention.

Die Reassembly-Free Deep Packet Inspection-Engine von SonicWALL scannt jedes einzelne Paket und jedes einzelne Byte. Damit sorgt sie für eine umfassende Content-Kontrolle des gesamten Datenstroms und bietet eine hohe Performance bei 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 Beschränkungen beim Datenvolumen führt. Die RFDPI-Engine dagegen sorgt für eine vollständige Content-Kontrolle. Sie wehrt Bedrohungen ab, bevor sie in das Netzwerk gelangen können und bietet Schutz vor Millionen unterschiedlicher Malware-Varianten ohne Einschränkungen bei Datenvolumen, Performance oder Latenzzeit. Dank intensiver Prüfung von SSL-verschlüsseltem Verkehr und nicht-proxyfähigen Anwendungen bietet sie außerdem umfassenden Schutz unabhängig von Übertragung und Protokoll.

Dank einer Analyse des Anwendungsverkehrs lässt sich arbeitsrelevanter und nicht arbeitsrelevanter Anwendungsverkehr in Echtzeit anzeigen und mit effektiven Regeln auf der Anwendungsebene kontrollieren. Die Anwendungskontrolle kann sowohl nach Benutzer als auch nach Gruppe, sowie mit Zeitplänen und Ausschlusslisten durchgeführt werden. Alle Anwendungs-, Intrusion Prevention- und Malware-Signaturen werden laufend von SonicWALLs Forschungsteam aktualisiert. Darüber hinaus bietet SonicWALLs hochentwickeltes Betriebssystem SonicOS integrierte Tools für eine personalisierbare Anwendungsidentifizierung.

Die Hardware erlaubt nahezu lineare Leistungssteigerungen und lässt sich auf bis zu 96 Prozessorkerne skalieren. Damit ist sie in der Lage, einen Durchsatz von über 40 GBit/s bei der Firewall Inspection, über 30 GBit/s bei der Anwendungsprüfung, über 30 GBit/s bei der Intrusion Prevention und über 10 GBit/s beim Malware-Schutz bereitzustellen. Mit den Modellen E10100, E10200, E10400 und E10800 ist die vor Ort erweiterbare SuperMassive E10000-Serie eine zukunftssichere Investition in eine Sicherheitsinfrastruktur, die mit der Netzwerkbandbreite und den Sicherheitsanforderungen dynamischer Unternehmen mitwachsen kann.

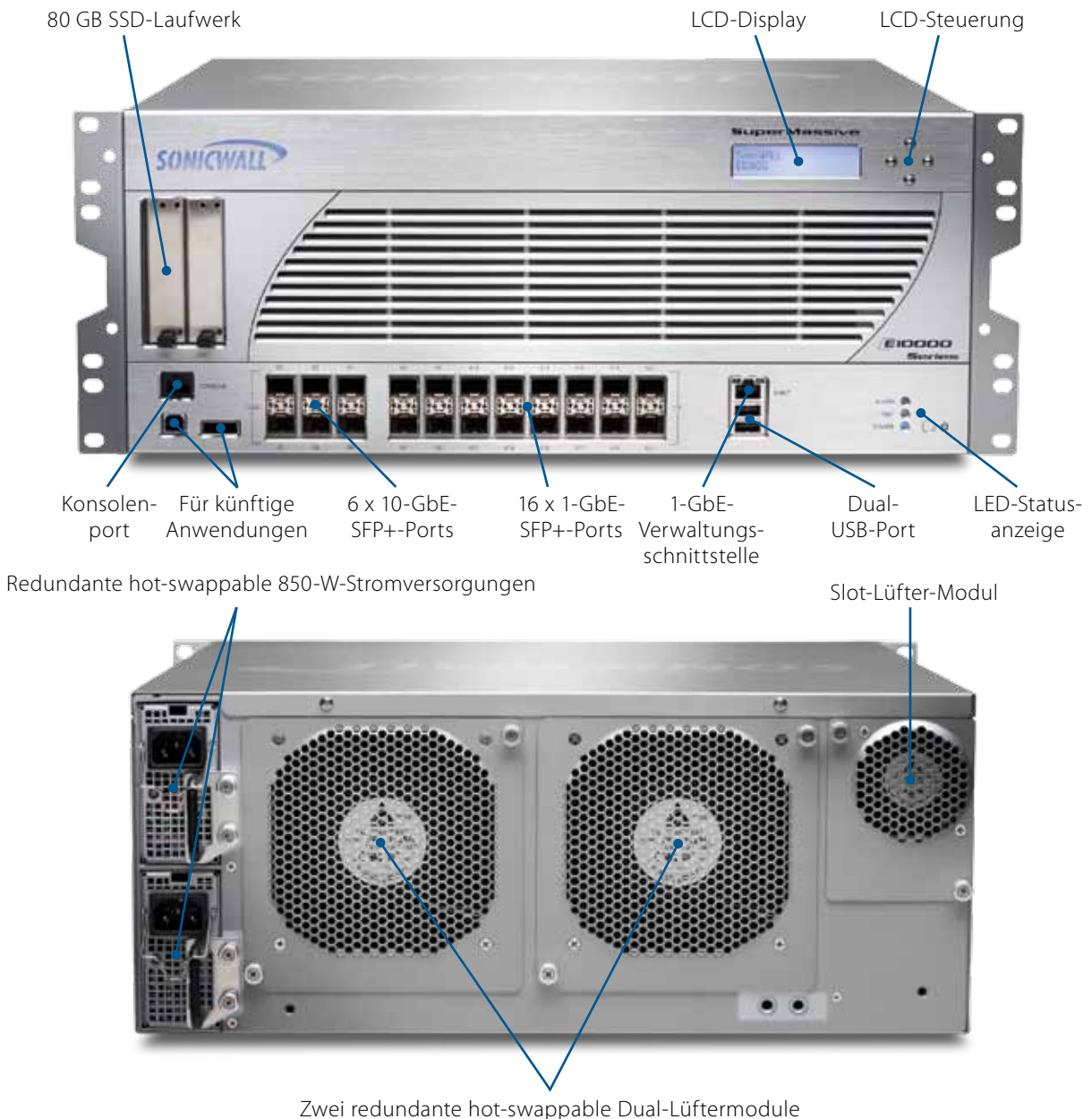
* U.S.-Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361

- Ultraskalierbare Multicore-Architektur für 10/40 GBit/s-Infrastrukturen
- Detaillierte Einblicke dank überlegenem Application Intelligence, Control and Visualization Service
- Umfassender Schutz vor Bedrohungen mit High-Performance-Intrusion Prevention und Malware-Schutz bei minimalen Latenzzeiten
- Umfassende Prüfung von SSL-verschlüsseltem Verkehr ohne den zusätzlichen Aufwand, die hohe Latenz und dem Memory-Thrashing Socket-basierter SSL-Proxies

ÜBERBLICK ÜBER DIE SUPERMASSIVE E10000-SERIE

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

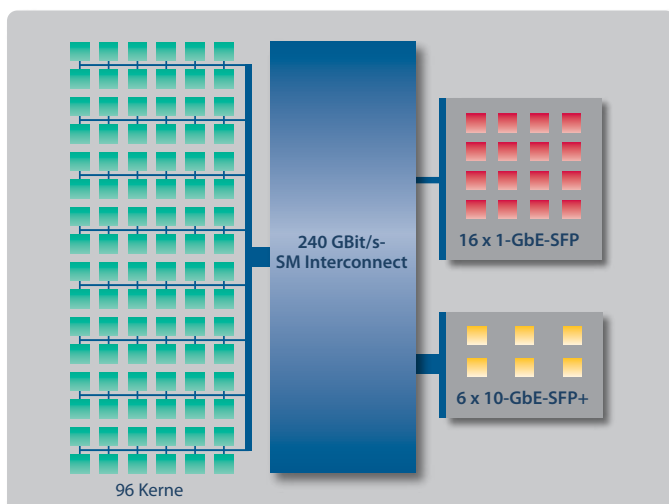
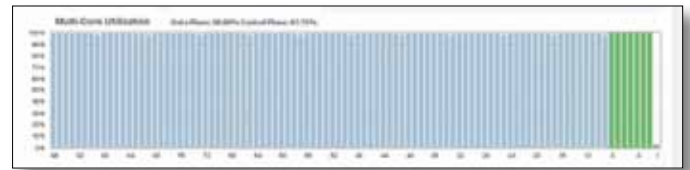
Technische Daten	E10100	E10200	E10400	E10800
Prozessorkerne	12 (+12 Hochverfügbarkeit)	24	48	96
Firewall-Durchsatz	5,0 GBit/s	10 GBit/s	20 GBit/s	40 GBit/s
Application Intelligence-Durchsatz	4,0 GBit/s	7,5 GBit/s	15 GBit/s	30 GBit/s
IPS-Durchsatz	4,0 GBit/s	7,5 GBit/s	15 GBit/s	30 GBit/s
Anti-Malware-Durchsatz	2,0 GBit/s	3,0 GBit/s	6,0 GBit/s	12 GBit/s
Max. Anzahl von Verbindungen	1,5 Mio.	3 Mio.	6 Mio.	12 Mio.
Upgrade-Möglichkeiten	Upgrade auf E10200	Upgrade auf E10400	Upgrade auf E10800	—



ERWEITERBARE ARCHITEKTUR FÜR HÖCHSTE SKALIERBARKEIT UND PERFORMANCE

Skalierbare Performance dank Multicore-Architektur

Die SonicWALL SuperMassive E10000-Serie wurde mit speziellem Fokus auf Performance, Skalierbarkeit und Hochverfügbarkeit entwickelt und bietet großen Unternehmen eine Plattform, die selbst anspruchsvollste Sicherheitsanforderungen erfüllt. Diese Kombination aus Skalierbarkeit und Performance ist SonicWALLs proprietärer Reassembly-Free Deep Packet Inspection-Engine sowie der leistungsstarken Multicore-Architektur zu verdanken, die sich linear für beliebig viele Prozessorkerne skalieren lässt. In Umgebungen mit wachsenden Netzwerksicherheitsanforderungen lässt sich das System aufrüsten, um die verfügbare Performance der SuperMassive-Plattform zu erhöhen.



Für hohe Leistung entwickelt

Die SuperMassive E10000-Serie wurde entwickelt, um die von großen Unternehmen benötigte Deep Packet Inspection mit geringer Latenz bereitzustellen. Der SuperMassive Interconnect bietet einen Non-Blocking-Durchsatz von 240 GBit/s mit weniger als 1 μ s Latenz für eine ungehinderte Kommunikation zwischen den 96 Prozessorkernen und den 6 x 10-GbE-SFP+- und 16 x 1-GbE-SFP-Ports.

Intelligentes Design für überlegenen DPI-Durchsatz

Stateful Packet Inspection ist nach wie vor erforderlich, doch alleine bietet sie keinen ausreichenden Schutz vor den Bedrohungen, die heute von Anwendungen und Inhalten ausgehen. Volle Deep Packet Inspection-Funktionen wie Anwendungs-kontrolle, Intrusion Prevention und Malware-Schutz bieten deutlich mehr Sicherheit und eine bessere Netzwerkkontrolle, dürfen dabei aber die Netzwerkperformance nicht beeinträchtigen.

SonicWALLs patentierte* RFDPI-Engine bietet ein hocheffizientes Single-Pass-Design, bei dem alle Sicherheitsfunktionen in einer einheitlichen Scan- und Regel-Engine konsolidiert sind, und bietet damit die höchste Deep Packet Inspection-Performance auf dem Markt.

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



FUNKTIONEN

Application Intelligence, Control and Visualization

Funktion	Beschreibung
Anwendungskontrolle	Identifizierung und Kontrolle von Anwendungen oder einzelnen Anwendungskomponenten mit RFDPI-Technologie und nicht anhand bekannter Ports und Protokolle.
Bandbreitenverwaltung auf Anwendungsebene	Bandbreitenzuordnung für kritische Anwendungen und Einschränkung von nicht arbeitsrelevantem Anwendungsverkehr gewährleisten eine effiziente Netzwerkauslastung.
Personalisierbare Anwendungsidentifizierung	Erstellen und Konfigurieren einer personalisierbaren Anwendungsidentifizierung auf der Grundlage von Verkehrsparametern oder Mustern, die nur bei der Netzwerkkommunikation bestimmter Anwendungen vorkommen.
Analyse des Anwendungsverkehrs	Bietet Organisationen aussagekräftige Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen. Gleichzeitig stehen leistungsstarke Troubleshooting- und Forensik-Funktionen zur Verfügung.
Anwendungssignaturendatenbank	Eine ständig erweiterte Datenbank mit über 3.500 Anwendungssignaturen erlaubt es Administratoren, die Nutzung der neuesten Anwendungen im Netzwerk nach Kategorie oder individuellen Kriterien zu kontrollieren.
IPFIX/NetFlow Reporting	Anwendungsnutzungsdaten können mittels IPFIX- oder NetFlow-Protokoll exportiert werden, um die Überwachung mit SonicWALL Scrutinizer oder fremden Monitoring- und Reporting-Tools zu ermöglichen. Ähnliche Daten lassen sich über Syslog für den Einsatz in SonicWALL GMS und SonicWALL Analyzer exportieren.
Deep Packet Inspection für SSL-Verkehr	Der SSL-Verkehr wird entschlüsselt und mit der Reassembly-Free Deep Packet Inspection-Engine auf Malware und Eindringlinge gescannt. Außerdem werden Anwendungs-, URL- und Content-Kontroll-Regeln angewendet, um auch schwer zu fassende Bedrohungen auszuschalten.
Nachverfolgung der Benutzeraktivitäten	Die einfache Integration der Benutzererkennung mit Microsoft® Active Directory und anderen Authentifizierungssystemen ermöglicht die Nachverfolgung und Erstellung von Berichten zu einzelnen Benutzerkennungen.
GeolP: Identifizierung des Datenverkehrs nach Ländern	Identifizierung und Kontrolle des Netzwerkverkehrs mit bestimmten Ländern als Herkunfts- und Bestimmungsort.

Gateway Threat Prevention

Malware-Schutz am Gateway	SonicWALLs proprietäre RFDPI-Engine scannt sämtliche Ports und Protokolle auf Viren ohne Einschränkung beim Datenvolumen oder bei der Länge des Datenstroms. Das SonicLab-Forschungsteam bietet laufend aktualisierten Schutz vor Bedrohungen und sorgt für schnellere Reaktionszeiten und Threat Prevention.
Reassembly-Free Deep Packet Inspection	Die Reassembly-Free Deep Packet Inspection-Engine überwacht Malware unabhängig von der Reihenfolge oder der Zeit, in der die Pakete eintreffen, was extrem kurze Latenzzeiten ermöglicht. Darüber hinaus entfallen Beschränkungen bei Datenvolumen und bei der Größe des Datenstroms. Dies ermöglicht mehr Performance und Sicherheit gegenüber veralteten Proxy-Designs mit Reassemblierung, bei denen Sockets an herkömmliche Virenschutz-Programme gekoppelt werden. Hier kommt es immer wieder zu einer ineffizienten Verarbeitung und zu Socket-Memory-Thrashing, was zu hoher Latenz, verminderter Leistung und Beschränkungen beim Datenvolumen führt.
Cloud Anti-Virus (AV)	Die RFDPI-Engine kann nicht nur auf die integrierte Datenbank zugreifen, sie erhält zusätzlich vom SonicWALL Cloud Service Informationen über mehr als vier Millionen Malware-Signaturen, die laufend erweitert werden.
Bidirektionale Prüfung	RFDPI kann für ein- und ausgehende Verbindungen durchgeführt werden, um den Netzwerkverkehr in alle Richtungen zu schützen.
24/7-Signatur-Updates	Das SonicLabs-Forschungsteam erstellt und aktualisiert Signaturendatenbanken, die automatisch an die Firewalls vor Ort gesendet werden. Die enthaltenen Signaturen sind sofort wirksam, ohne dass ein Neustart oder sonstige Betriebsunterbrechungen erforderlich sind.

Intrusion Prevention

Funktion	Beschreibung
Signaturbasierte Prüfung	Eng integrierte, signaturbasierte Intrusion Prevention prüft Paket-Payloads auf Schwachstellen und Exploits, die auf kritische interne Systeme abzielen.
Automatische Signaturen-Updates	SonicWALLs Forschungsteam sorgt für eine ständige Aktualisierung und Bereitstellung einer umfassenden Liste mit über 5.400 IPS-Signaturen und 52 Angriffs-Kategorien. Diese Signaturen sind sofort wirksam und erfordern keine Neustarts oder sonstige Betriebsunterbrechungen.
Threat Prevention für ausgehende Daten	Die Prüfung des ein- und ausgehenden Datenverkehrs verhindert, dass Netzwerke unabsichtlich in Denial-of-Service-Angriffe involviert werden und unterbindet jegliche Command-and-Control-Botnet-Kommunikation.
IPS-Schutz zwischen Netzwerkzonen	Intrusion Prevention kann zwischen internen Sicherheitszonen bereitgestellt werden, um sensible Server zu schützen und interne Angriffe zu verhindern.

VPN

IPSec VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPSec VPN kann die SuperMassive E10000-Serie als VPN-Konzentrator für tausende große 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	Mit mehreren WANs lässt sich ein primäres und sekundäres VPN konfigurieren, um ein einfaches automatisches Failover und Failback für alle VPN-Sitzungen zu ermöglichen.
Route-basiertes 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.

VoIP

Erweiterte QoS	Garantierte Unterstützung kritischer Datenübertragung dank 802.1p und DSCP-Tagging sowie Remapping von VoIP-Datenverkehr im Netzwerk.
DPI von VoIP-Daten	Vordefinierte Signaturen erkennen und blockieren Bedrohungen, die auf VoIP-Daten abzielen.
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.

Firewall und Networking

Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus muss sichergestellt werden, dass die Firewall-Zugriffsregeln erfüllt werden.
Schutz vor DOS-Angriffen	Dank SYN Flood-Schutz lassen sich DOS-Angriffe mit Layer 3-SYN Proxy- und Layer 2-SYN-Blacklisting-Technologien abwehren.
Flexible Bereitstellung	Implementierung in konventionellen NAT-, Layer 2 Bridge-, Wire- und Netzwerk-Tap-Modi.
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.

FUNKTIONEN

Firewall und Networking (Fortsetzung)

Funktion	Beschreibung
Hochverfügbarkeit	Unterstützung für Stateful Active/Passive-, Active/Active DPI- und Active/Active Clustering-Fail-over garantiert eine höhere Zuverlässigkeit durch den Schutz vor Hardware- und Software-Fehlern, und erhöht die Performance, da Reassembly-Free Deep Packet Inspection-Lasten an die verfügbaren Kerne von Einheiten im Standby-Modus weitergegeben werden. werden.
WAN-Lastverteilung	Lastverteilung auf bis zu vier WAN-Schnittstellen mit Round Robin, Spillover oder prozent-basierten Methoden.
Verwaltung und Überwachung	
Web-Oberfläche	Eine intuitive webbasierte Oberfläche erlaubt eine schnelle und bequeme Konfiguration neben der Verwaltung über das SonicWALL Global Management System (GMS®) oder das CLI.
SNMP	SNMP bietet die Möglichkeit, Bedrohungen und Warnmeldungen zu überwachen und darauf zu reagieren.
NetFlow/IPFIX	Erweiterte Datensätze können mittels IPFIX- oder NetFlow-Protokoll exportiert werden, um aussagekräftige Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen sowie leistungsstarke Troubleshooting- und Forensik-Funktionen bereitzustellen. Kompatibel mit SonicWALL Scrutinizer und Monitoring- und Reporting-Tools anderer Anbieter. Ähnliche Daten lassen sich über Syslog für den Einsatz in SonicWALL GMS und SonicWALL Analyzer exportieren.
Zentrale Regelverwaltung	Mit dem SonicWALL Global Management System (GMS®) lassen sich mehrere SonicWALL-Appliances von einer einzigen intuitiven Oberfläche aus überwachen und konfigurieren. Darüber hinaus können Berichte erstellt und die Sicherheitsumgebung an individuelle Regeln angepasst werden.

Die SonicOS-Funktionen im Überblick

Firewall

- Reassembly-Free Deep Packet Inspection
- Deep Packet Inspection für SSL-Daten
- Stateful Packet Inspection
- Schutz vor DOS-Angriffen
- TCP-Reassemblierung
- Stealth-Modus

Anwendungskontrolle

- Anwendungskontrolle
- Blockieren von Anwendungskomponenten
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Visualisierungsfunktionen
- Schutz vor Datenlecks
- IPFIX mit Berichten zu Erweiterungen
- Nachverfolgung der Benutzeraktivitäten
- GeolIP: Identifizierung des Datenverkehrs nach Ländern
- Umfassende Anwendungs-signaturendatenbank

Intrusion Prevention

- Signaturbasierte Prüfung
- Automatische Signaturen-Updates
- Threat Prevention für ausgehende Daten
- IPS-Ausschlussliste
- Protokollmeldungen mit Hyperlinks
- Unified CFS und Anwendungskontrolle mit Bandbreitenbegrenzung

Anti-Malware

- Stream-basierte Malware-Prüfung
- Gateway Anti-Virus
- Gateway Anti-Spyware
- SSL-Entschlüsselung
- Anti-Spam
- Bidirektionale Prüfung
- Keine Einschränkung beim Datenvolumen

VPN

- IPsec VPN für Site-to-Site-Konnektivität
- SSL VPN- oder IPsec Client-Remote Access
- Redundantes VPN-Gateway
- Route-basiertes VPN
- Mobile Connect für iOS

Web Content Filtering

- URL Filtering
- Anti-Proxy-Technologie
- Blockieren von Schlüsselwörtern
- Bandbreitenverwaltung mit CFS-Ratingkategorien
- Unified Policy-Konzept mit Anwendungskontrolle

VoIP

- Erweiterte QoS
- Bandbreitenverwaltung
- DPI von VoIP-Daten
- Volle Interoperabilität
- H.323-Gatekeeper- und SIP-Proxy-Unterstützung

Networking

- Dynamisches Routing
- Regelbasiertes Routing

- Erweiterte NAT
- DHCP-Server
- Bandbreitenverwaltung
- IPv6
- Link Aggregation
- Port-Redundanz
- Hochverfügbarkeit
- Lastverteilung

Verwaltung und Überwachung

- Web-Oberfläche
- Befehlszeilenschnittstelle
- SNMP
- Analyzer-Reporting
- Scrutinizer-Reporting
- Verwaltung und Überwachung von Sicherheitsregeln mit GMS
- Logging
- NetFlow/IPFIX
- Anwendungsvisualisierung
- LCD-Verwaltungsbildschirm
- Zentrale Regelverwaltung
- Single Sign-On
- Terminal Service-/Citrix-Unterstützung
- Integrierte Forensik-Funktionen von Solera Networks

Sicherheitsservices

- Intrusion Prevention Service
- Gateway Anti-Malware Service
- Content Filtering Service
- Enforced Client Anti-Virus and Anti-Spyware Service
- Application Intelligence, Control and Visualization Service

Systemdaten	E10100	E10200	E10400	E10800
Betriebssystem	SonicOS			
Kerne	12 (+12 Hochverfügbarkeit)	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)	8 GB	16 GB	32 GB	64 GB
Speicher	80 GB SSD, Flash			
Firewall Inspection-Durchsatz	5,0 GBit/s	10 GBit/s	20 GBit/s	40 GBit/s
Application Inspection-Durchsatz	4,0 GBit/s	7,5 GBit/s	15 GBit/s	30 GBit/s
IPS-Durchsatz	4,0 GBit/s	7,5 GBit/s	15 GBit/s	30 GBit/s
Anti-Malware Inspection-Durchsatz	2,0 GBit/s	3,0 GBit/s	6,0 GBit/s	12 GBit/s
VPN-Durchsatz	2,5 GBit/s	5,0 GBit/s	10 GBit/s	20 GBit/s
Verbindungen pro Sekunde	80.000/Sek.	160.000/Sek.	320.000/Sek.	640.000/Sek.
Max. Anzahl von Verbindungen (SPI)	1,5 Mio.	3,0 Mio.	6,0 Mio.	12,0 Mio.
Max. Anzahl von Verbindungen (DPI)	1,2 Mio.	2,5 Mio.	5,0 Mio.	10,0 Mio.

VPN

Site-to-Site-Tunnel	10.000	10.000 (20.000)*	10.000 (40.000)*	10.000 (80.000)*
IPSec VPN Clients	2.000	2.000 (4.000)*	2.000 (8.000)*	2.000 (16.000)*
SSL VPN-Lizenzen	20 (1.000)*	50 (2.000)*	50 (4.000)*	50 (8.000)*
Verschlüsselung	DES, 3DES, AES (128, 192, 256-Bit)			
Authentifizierung	MD5, SHA-1			
Schlüsselaustausch	Diffie Hellman-Gruppen 1, 2, 5, 14			
Route-basiertes VPN	RIP, OSPF			

Networking

IP-Adresszuweisung	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			
IPv6	IPv6 RFDPI, Firewall, VPN, NAT; Dual-Stack IPv4/IPv6; IPv6/IPv4- und IPv4/IPv6-Umsetzung; ICMPv6; DHCPv6; DNSv6			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Ausstehende Zertifikate	FIPS 140-2, Common Criteria EAL4+, NEBS, ICISA Firewall			
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)	350	400	550	750
Gehäuse	rackfähig (4 HE)			
Abmessungen	43 x 43,5 x 17,8 cm			
Gewicht	26,3 kg	26,3 kg	27,7 kg	30,3 kg
WEEE-Gewicht	26,8 kg	26,8 kg	28,1 kg	30,8 kg
Versandgewicht	35,8 kg	35,8 kg	37,2 kg	39,9 kg
Erfüllt folgende Standards	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			

*Verfügbar mit erweiterter Lizenz
 Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten

Next-Generation Firewalls der SuperMassive E10000-Serie

BESTELLINFORMATIONEN

Produkt	Artikelnr.
SuperMassive E10100, 6 SFP+-10-GbE-Ports, 16 SFP-1-GbE-Ports, Dual-Lüfter, Dual-AC-Stromversorgungen	01-SSC-8883
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	Artikelnr.
Upgrade von SuperMassive E10100 auf E10200	01-SSC-9496
Upgrade von SuperMassive E10200 auf E10400	01-SSC-9497
Upgrade von SuperMassive E10400 auf E10800	01-SSC-9498
E10100-Services	Artikelnr.
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus für E10100 (1 Jahr)	01-SSC-9500
Application Intelligence and Control - Application Intelligence, Control and Visualization für E10100 (1 Jahr)	01-SSC-9506
Content Filtering Premium Business Edition für E10100 (1 Jahr)	01-SSC-9503
Platinum-Support für SuperMassive E10100 (1 Jahr)	01-SSC-9512
Comprehensive Gateway Security Suite - Application Intelligence, Threat Prevention und Content Filtering mit Support für E10100 (1 Jahr)	01-SSC-9515
E10200-Services	Artikelnr.
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
E10400-Services	Artikelnr.
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
E10800-Services	Artikelnr.
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
Zubehör	Artikelnr.
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



SonicWALL-Lösungen für dynamische Sicherheit

NETWORK
SECURITYSECURE
REMOTE ACCESSWEB & E-MAIL
SECURITYBACKUP &
RECOVERYPOLICY &
MANAGEMENT

SonicWALL Deutschland

Tel: +49 89 4545 946 www.sonicwall.de

SonicWALL Schweiz

Tel: +41 44 810 31 35 www.sonicwall.ch

SonicWALL Österreich

Tel: +41 44 810 31 35 www.sonicwall.at



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™