SuperMassive E10000 Series

Next-Generation Firewall

The Dell® SonicWALL® SuperMassive™ E10000 Series is Dell SonicWALL's Next-Generation Firewall platform designed for large networks to deliver scalability, reliability and deep security at multi-gigabit speeds. Built to meet the needs of enterprise, government, university, and service provider deployments, the SuperMassive E10000 Series is ideal for securing enterprise networks, data centers and server farms. Combining its massively multi-core architecture and Dell SonicWALL's patented* Reassembly-Free Deep Packet Inspection® (RFDPI) technology, the SuperMassive E10000 Series delivers industry-leading application control, intrusion prevention, malware protection and SSL inspection at multi-gigabit speeds. The Dell SonicWALL E10000 Series is designed with power, space, and cooling (PSC) in mind, providing the leading Gbps/Watt Next-Generation Firewall in the industry for application control and threat prevention.

Dell SonicWALL's Reassembly-Free Deep Packet Inspection engine scans every byte of every packet delivering full content inspection of the entire stream while providing high performance and low latency. This technology is superior to outdated proxy designs that reassemble content using sockets bolted to anti-malware programs that are plagued with inefficiencies and overhead of socket memory thrashing that leads to high latency, low performance and file size limitations. The RFDPI engine delivers full content inspection to eliminate threats before they enter the network and provides protection against millions of unique malware variants without file size, performance or latency limitations. The RFDPI engine also provides full inspection of SSL-encrypted traffic as well as non-proxyable applications enabling complete protection regardless of transport or protocol.

Application traffic analytics allows for the identification of productive and unproductive application traffic in real time which can then be controlled through powerful application-level policies. Application control can be exercised on both a per-user and per-group basis, along with schedules and exception lists. All application, intrusion prevention, and malware signatures are constantly updated by Dell SonicWALL's Research Team. Additionally, Dell SonicWALL's advanced operating system, SonicOS, provides integrated tools that allow for custom application identification and control.

The design provides near-linear performance increases and scales up to 96 cores of processing power to deliver 40+ Gbps of Firewall throughput, 30+ Gbps of Application Inspection, 30+ Gbps of Intrusion Prevention, and 10+ Gbps of Anti-Malware protection. Consisting of the E10100, E10200, E10400 and E10800, the SuperMassive E10000 Series is field upgradeable, future-proofing the security infrastructure investment as network bandwidth and security requirements increase.

- **Massively scalable multicore architecture designed for 10/40 Gbps infrastructure**
- **Superior granular application intelligence, control and visualization**
- **Complete threat protection including high performance intrusion prevention and low latency malware protection**
- **Full inspection of SSL encrypted traffic without overhead, latency, and memory thrashing associated with socket based SSL proxies**

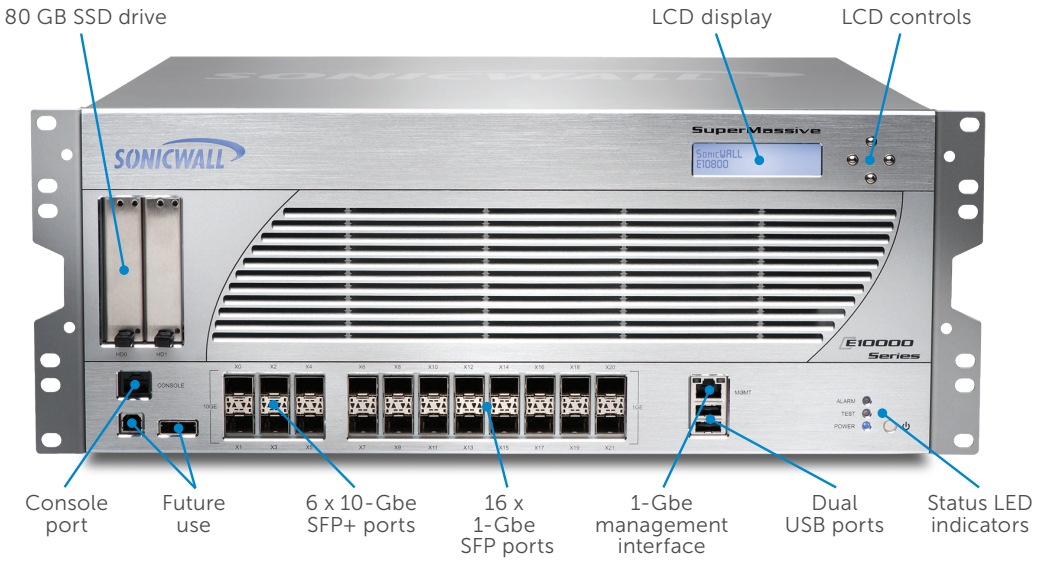
NSS Labs RECOMMEND

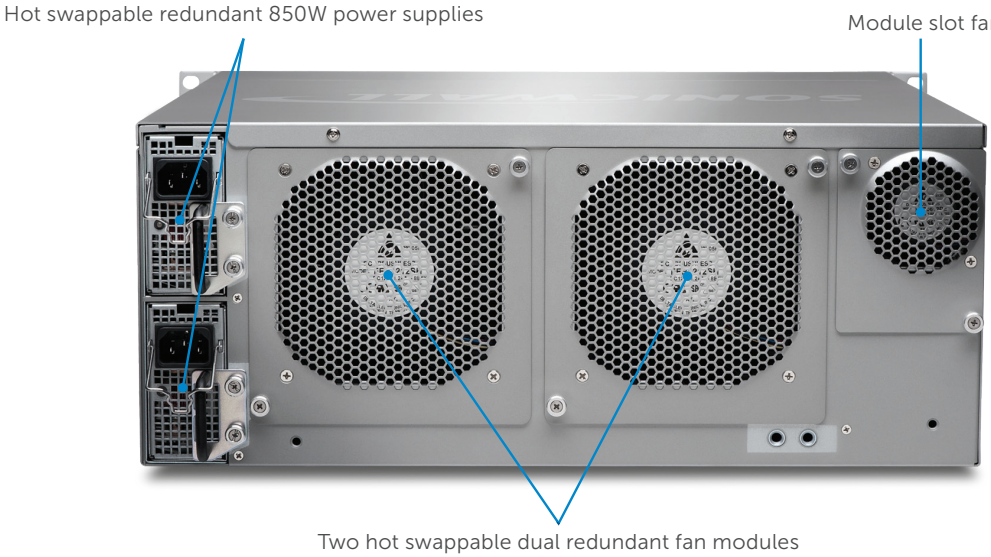
* U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

Series lineup

The Dell SonicWALL SuperMassive chassis includes 6 x 10-GbE SFP+ and 16 x 1-GbE SFP ports, redundant 850W AC power supplies, hot swappable dual redundant fan modules, and massively scales up to 96 processing cores.

Capability	E10100	E10200	E10400	E10800
Processing cores	12 (+12 Integrated HA Mode)	24	48	96
Firewall throughput	5.0 Gbps	10 Gbps	20 Gbps	40 Gbps
Application intelligence throughput	4.0 Gbps	7.5 Gbps	15 Gbps	30 Gbps
IPS throughput	4.0 Gbps	7.5 Gbps	15 Gbps	30 Gbps
Anti-malware throughput	2.0 Gbps	3.0 Gbps	6.0 Gbps	12 Gbps
Maximum connections	1.5M	3.0M	6.0M	12.0M
Upgrade path	Upgradeable to the E10200	Upgradeable to the E10400	Upgradeable to the E10800	—



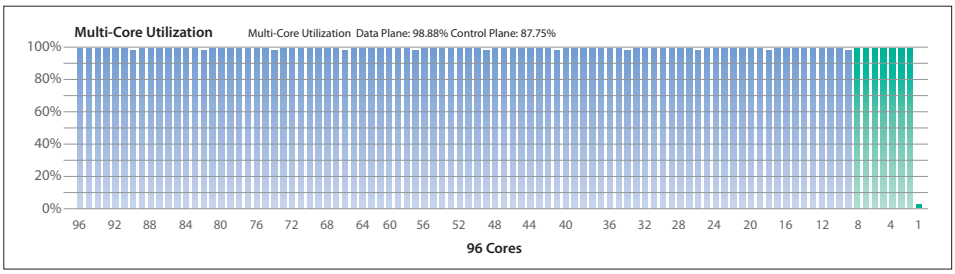


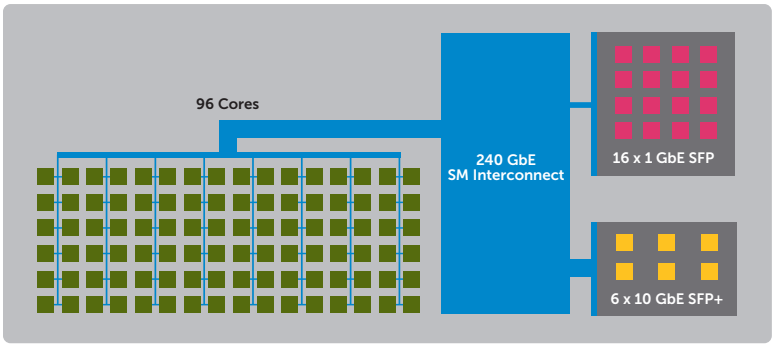
DELL SonicWALL

Extensible architecture for extreme scalability and performance

Scalable performance with a multi-core architecture

The Dell SonicWALL SuperMassive E10000 Series is built with a focus on high performance, scalability and high availability, providing large enterprises a platform to address their most demanding security needs. This combination of scalability and performance is a result of a powerful and massively scalable multi-core architecture paired with Dell SonicWALL's proprietary Reassembly-Free Deep Packet Inspection engine that can scale linearly to any number of processing cores. Environments that see their network security needs grow with time can upgrade their system to increase the available performance of their SuperMassive platform.





Engineered for high performance

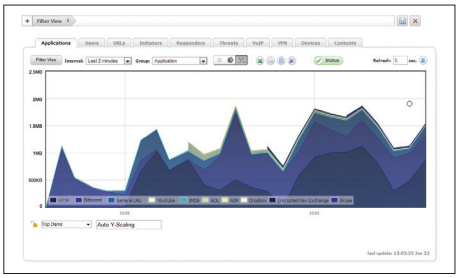
The SuperMassive E10000 Series is engineered to deliver ultra low latency Deep Packet Inspection that large enterprises demand. The SuperMassive fabric interconnect provides 240 GbE of non-blocking bandwidth with less than 1 µs latency for unhindered communication between the 96 processing cores and the 6 x 10-GbE SFP+ and the 16 x 1-GbE SFP ports.

Intelligent design for superior DPI throughput

While stateful packet inspection is still necessary, it alone is insufficient to protect against today's application and content-borne threats. Full deep packet inspection capabilities like application control, intrusion prevention and anti-malware provide a significantly increased level of security and network control, but must do so without diminishing network performance.

Dell SonicWALL's patented* RFDPI engine provides a highly-efficient single-pass design that consolidates all security features into a unified scanning and policy engine, enabling the platform to deliver industry-leading deep packet inspection performance.

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



SonicWALL

Features

Application intelligence and control	
Feature	Description
Application control	Identify and control applications or individual components of an application based on RFDPI technology instead of relying on well-known ports and protocols.
Application bandwidth management	Allocate bandwidth to critical applications while throttling unproductive application traffic for an efficient and productive network.
Custom application identification	Create and configure custom application identification based on traffic parameters or on patterns unique to an application in its network communications.
Application Traffic Analytics	Provides organizations with granular insight into application traffic, bandwidth utilization and security threats in addition to powerful troubleshooting and forensics capabilities.
Application signature database	A continuously expanding database of over 3,500 application signatures ensures that administrators are able to control the usage of all the latest applications on their network at a category or individual level.
IPFIX/Netflow reporting	Export application usage data through IPFIX or NetFlow protocols for monitoring to Dell SonicWALL Scrutinizer or third-party monitoring and reporting tools. Similar data can be exported via syslog to Dell SonicWALL GMS and Dell SonicWALL Analyzer.
Deep Packet Inspection for SSL	SSL traffic is decrypted and inspected for malware and intrusions by the Reassembly-Free Deep Packet Inspection engine in addition to applying application, URL, and content control policies on potentially evasive traffic.
User activity tracking	User identification is seamlessly integrated with Microsoft® Active Directory and other authentication systems enabling tracking and reporting of individual user identification.
GeoIP country traffic identification	Identify and control network traffic going to or coming from specific countries.

Gateway threat prevention	
Gateway anti-malware	Dell SonicWALL's proprietary RFDPI engine scans all ports and protocols for viruses without file size or stream length limitation. SonicLabs Researchers constantly provide updated threat protection, providing faster response times and threat prevention.
Reassembly-Free Deep Inspection (RFDPI)	Reassembly-Free Deep Packet Inspection keeps track of malware regardless of the Packet order or the timing with which the packets arrive, allowing for extreme low latency while eliminating file size and stream size limitation, and providing greater performance and security than outdated proxy designs that reassemble content using sockets bolted to traditional anti-virus programs that are plagued with inefficiencies and overhead of socket memory thrashing that leads to high latency, low performance and file size limitations.
Cloud Anti-Virus (AV)	In addition to utilizing the on-board database, the RFDPI engine also consults with the Dell SonicWALL Cloud Services for additional information on over four million malware signatures and growing.
Bi-directional inspection	RFDPI can be performed on both inbound and outbound connections to provide protection in all network traffic directions.
24x7 signature updates	SonicLabs Research Team team creates and updates signature databases that are propagated automatically to the firewalls in the field, with those signatures taking immediate effect without any reboot or service interruption required.

Features

Intrusion prevention	
Feature	Description
Signature-based scanning	Tightly integrated, signature-based intrusion prevention scans packet payloads for vulnerabilities and exploits that target critical internal systems.
Automatic signature updates	Dell SonicWALL's Research Team continuously updates and deploys an extensive list of over 5,400 IPS signatures covering 52 attack categories. These signatures take immediate effect and do not require reboots or any other interruption in service.
Outbound threat prevention	The ability to inspect both inbound and outbound traffic ensures that the network will not unwittingly be used in Distributed Denial of Service attacks and will prevent any Command and Control Botnet communication.
Intra-Zone IPS protection	Intrusion prevention can be deployed between internal security zones to protect sensitive servers and to prevent internal attacks.

VPN	
IPSec VPN for Site-to-site connectivity	High-performance IPSec VPN allows the SuperMassive E10000 Series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilize clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure by seamlessly re-routing traffic between endpoints through alternate routes.

VoIP	
Advanced QoS	Guarantee critical communications with 802.1p and DSCP tagging and remapping of VoIP traffic on the network.
DPI of VoIP traffic	Predefined signatures detect and block VoIP specific threats.
H.323 gatekeeper and SIP proxy support	Block spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.

Firewall and networking	
Stateful Packet Inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DOS attack protection	SYN Flood protection provides defense against DOS attacks using both layer 3 SYN proxy and layer 2 SYN blacklisting technologies.
Flexible deployment	Can be deployed in traditional NAT, Layer 2 Bridge, Wire Mode and Network Tap modes.
Policy-based routing	Create routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.

Features

Firewall and networking (continued)

Feature	Description
High availability	Supports Stateful Active/Passive, Active/Active DPI and Active/Active Clustering failover to ensure not only increased reliability by protecting against hardware or software faults, but also an increase in performance through Reassembly-Free Deep Packet Inspection workload offloading to the cores available on stand-by units.
WAN load balancing	Load balance up to four WAN interfaces using Round Robin, Spillover or Percentage based methods.

Management and monitoring

Web GUI	An intuitive web-based interface allows quick and convenient configuration in addition to management through Dell SonicWALL Global Management System (GMS®), or the CLI.
SNMP	SNMP provides the ability to protectively monitor and respond to threats and alerts.
Netflow/IPFIX	Export an extended set of data through IPFIX or NetFlow protocols for granular insight into application traffic, bandwidth utilization and security threats in addition to powerful troubleshooting and forensics capabilities. Compatible with Dell SonicWALL Scrutinizer and third-party monitoring and reporting applications. Similar data can be exported via syslog to Dell SonicWALL GMS and Dell SonicWALL Analyzer.
Centralized policy management	With Dell SonicWALL GMS, monitor, configure and report on multiple Dell SonicWALL appliances from a single intuitive interface and customize your security environment to suit your individual policies.

SonicOS feature summary

Firewall
- Reassembly-Free Deep Packet Inspection
- Deep packet inspection for SSL
- Stateful packet inspection
- DOS attack protection
- TCP reassembly
- Stealth mode

Application control
- Application control
- Application component blocking
- Application bandwidth management
- Custom application signature creation
- AppFlow visualization
- Data leakage prevention
- IPFIX with extensions reporting
- User activity tracking
- GeoIP country traffic identification
- Comprehensive application signature database

Intrusion prevention
- Signature-based scanning
- Automatic signature updates
- Outbound threat prevention
- IPS exclusion list
- Hyperlinked log messages
- Unified CFS and app control with bandwidth throttling

Anti-Malware
- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- SSL Decryption
- Anti-spam
- Bi-directional Inspection
- No file size limitation

VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN or IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for Apple® iOS and Google® Android™
- Route-based VPN

Web content filtering
- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth manage CFS rating categories
- Unified policy model with app control

VoIP
- Advanced QoS
- Bandwidth management
- DPI of VoIP traffic
- Full interoperability
- H.323 gatekeeper and SIP proxy support

Networking
- Dynamic routing
- Policy-based routing
- Advanced NAT
- DHCP server
- Bandwidth management
- IPv6
- Link aggregation
- Port redundancy
- High availability
- Load balancing

Management and monitoring
- Web GUI
- Command line interface
- SNMP
- Analyzer reporting
- Scrutinizer reporting
- GMS policy management and reporting
- Logging
- Netflow/IPFIX
- App visualization
- LCD management screen
- Centralized policy management
- Single sign-on
- Terminal service/Citrix support
- Solera Networks Forensics integration

Security services
- Intrusion Prevention Service
- Gateway Anti-Malware Service
- Content Filtering Service
- Enforced Client Anti-Virus and Anti-Spyware – McAfee® or Kaspersky® options
- Application Intelligence, Control and Visualization Service

System specifications

	E10100	E10200	E10400	E10800
Operating system	SonicOS			
Cores	12 (+ 12 HA)	24	48	96
10 GbE interfaces	6 x 10-GbE SFP+			
1 GbE interfaces	16 x 1-GbE SFP			
Management interfaces	1 GbE, 1 Console			
Memory (RAM)	8 GB	16 GB	32 GB	64 GB
Storage	80 GB SSD, Flash			
Firewall inspection throughput	5.0 Gbps	10 Gbps	20 Gbps	40 Gbps
Application inspection throughput	4.0 Gbps	7.5 Gbps	15 Gbps	30 Gbps
IPS throughput	4.0 Gbps	7.5 Gbps	15 Gbps	30 Gbps
Anti-malware inspection throughput	2.0 Gbps	3.0 Gbps	6.0 Gbps	12 Gbps
VPN throughput	2.5 Gbps	5.0 Gbps	10 Gbps	20 Gbps
Connections per second	80,000/sec	160,000/sec	320,000/sec	640,000/sec
Maximum connections (SPI)	1.5M	3.0M	6.0M	12.0M
Maximum connections (DPI)	1.2M	2.5M	5.0M	10.0M
VPN				
Site-to-site tunnels	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 licenses	20 (1,000)*	50 (2,000)*	50 (4,000)*	50 (8,000)*
Encryption	DES, 3DES, AES (128, 192, 256-bit)			
Authentication	MD5, SHA-1			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14			
Route-based VPN	RIP, OSPF			
Networking				
IP address assignment	Static (DHCP PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode			
VLAN interfaces	512			
Routing protocols	BGP*, OSPF, RIPv1/v2, static routes, policy-based routing, multicast			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, terminal services, Citrix			
IPv6	IPv6 RFDPI, firewall, VPN, NAT; Dual stack IPv4/IPv6; IPv6 to/from IPv4 translations; 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			
Certifications pending	FIPS 140-2, Common Criteria EAL4+, NEBS, ICSA Firewall			
Common Access Card (CAC) support	Pending			
Hardware				
Power supply	Dual, redundant, hot swappable, 850 W			
Fans	Dual, redundant, hot swappable			
Display	Front LED display			
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	350	400	550	750
Form factor	4U Rack Mountable			
Dimensions	17x18x7 in (43x43.5x17.8 cm)			
Weight	58 lb (26.3 kg)	58 lb (26.3 kg)	61 lb (27.7 kg)	67 lb (30.3 k
WEEE weight	59 lb (26.8 kg)	59 lb (26.8 kg)	62 lb (28.1 kg)	68 lb (30.8 kg)
Shipping weight	79 lb (35.8 kg)	79 lb (35.8 kg)	82 lb (37.2 kg)	88 lb (39.9 kg)
Major regulatory	FCC Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE			
Environment	40-105 F, 5-40 deg C			
Humidity	10-90% non-condensing			

*Available with expanded license.
All specifications, features and availability are subject to change.

Ordering information

Product	SKU
SuperMassive E10100, 6 SFP+ 10GbE ports, 16 SFP 1GbE ports, dual fans, dual ac power supplies	01-SSC-8883
SuperMassive E10200, 6 SFP+ 10GbE ports, 16 SFP 1GbE ports, dual fans, dual ac power supplies	01-SSC-8882
SuperMassive E10400, 6 SFP+ 10GbE ports, 16 SFP 1GbE ports, dual fans, dual ac power supplies	01-SSC-8881
SuperMassive E10800, 6 SFP+ 10GbE ports, 16 SFP 1GbE ports, dual fans, dual ac power supplies	01-SSC-8856

System Upgrades	SKU
SuperMassive E10100 to E10200 upgrade	01-SSC-9496
SuperMassive E10200 to E10400 upgrade	01-SSC-9497
SuperMassive E10400 to E10800 upgrade	01-SSC-9498

Services E10100	SKU
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for E10100 (1-year)	01-SSC-9500
Application Intelligence and Control –Application Intelligence, Application Control, App Flow Visualization for E10100 (1-year)	01-SSC-9506
Content Filtering Premium Business Edition for E10100 (1-year)	01-SSC-9503
Platinum Support for the SuperMassive E10100 (1-year)	01-SSC-9512
Comprehensive Gateway Security Suite–Application Intelligence, Threat Prevention, Content Filtering with Support for E10100 (1-year)	01-SSC-9515

Services E10200	SKU
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for E10200 (1-year)	01-SSC-9518
Application Intelligence and Control–Application Intelligence, Application Control, App Flow Visualization for E10200 (1-year)	01-SSC-9524
Content Filtering Premium Business Edition for E10200 (1-year)	01-SSC-9521
Platinum Support for the SuperMassive E10200 (1-year)	01-SSC-9530
Comprehensive Gateway Security Suite–Application Intelligence, Threat Prevention, Content Filtering with Support for E10200 (1-year)	01-SSC-9533

Services E10400	SKU
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for E10400 (1-year)	01-SSC-9536
Application Intelligence and Control–Application Intelligence, Application Control, App Flow Visualization for E10400 (1-year)	01-SSC-9542
Content Filtering Premium Business Edition for E10400 (1-year)	01-SSC-9539
Platinum Support for the SuperMassive E10400 (1-year)	01-SSC-9548
Comprehensive Gateway Security Suite–Application Intelligence, Threat Prevention, Content Filtering with Support for E10400 (1-year)	01-SSC-9551

Services E10800	SKU
Application Intelligence and Control–Application Intelligence, Application Control, App Flow Visualization for E10800 (1-year)	01-SSC-9560
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for E10800 (1-year)	01-SSC-9554
Content Filtering Premium Business Edition for E10800 (1-year)	01-SSC-9557
Platinum Support for the SuperMassive E10800 (1-year)	01-SSC-9566
Comprehensive Gateway Security Suite–Application Intelligence, Threat Prevention, Content Filtering with Support for E10800 (1-year)	01-SSC-9569

Accessories	SKU
SuperMassive E10000 Series system fan FRU	01-SSC-8885
SuperMassive E10000 Series SSD fan module	01-SSC-8886
SuperMassive E10000 Series power supply FRU	01-SSC-8887

Security Monitoring Services from Dell SecureWorks are available for this appliance Series. For more information, visit **www.dell.com/secureworks**

DELL SonicWALL