SonicWall SuperMassive Series

Uncompromising, high-performance, next-generation firewall protection for your enterprise network.

The SonicWall SuperMassive Series is SonicWall's next-generation firewall (NGFW) platform designed for large networks to deliver scalability, reliability and deep security at multi-gigabit speeds with near zero latency.

Built to meet the needs of enterprise, government, university and service provider deployments, the SuperMassive Series is ideal for securing enterprise networks, data centers and service providers.

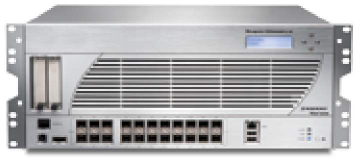
Combining its massively multi-core architecture and SonicWall's patented* Reassembly-Free Deep Packet Inspection® (RFDPI) technology, the SuperMassive E10000 and 9000 Series deliver industry-leading application control, intrusion prevention, malware protection and SSL inspection at multi-gigabit speeds. The SuperMassive Series is designed with power, space and cooling (PSC) in mind, providing the leading Gbps/watt NGFW in the industry for application control and threat prevention.

The SonicWall RFDPI engine scans every byte of every packet across all ports, 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 This technology is superior to outdated proxy designs that reassemble content using sockets bolted to anti-malware programs, which are plagued with inefficiencies and the overhead of socket memory thrashing, which 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 enable the identification of productive and unproductive application traffic in real time, and traffic 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 the SonicWall Threats Research Team. Additionally, SonicOS, an advanced purpose-built operating system, provides integrated tools that allow for custom application identification and control.

The design of the SuperMassive Series firewalls provides near-linear performance and scales up to 96 cores of processing power to deliver up to 40 Gbps of firewall throughput, 30 Gbps of threat prevention, and 30 Gbps of application inspection and control. The SuperMassive E10000 Series is field upgradeable, future-proofing the security infrastructure investment as network bandwidth and security requirements increase.

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



SuperMassive E10000 Series

SuperMassive 9000 Series

Benefits:

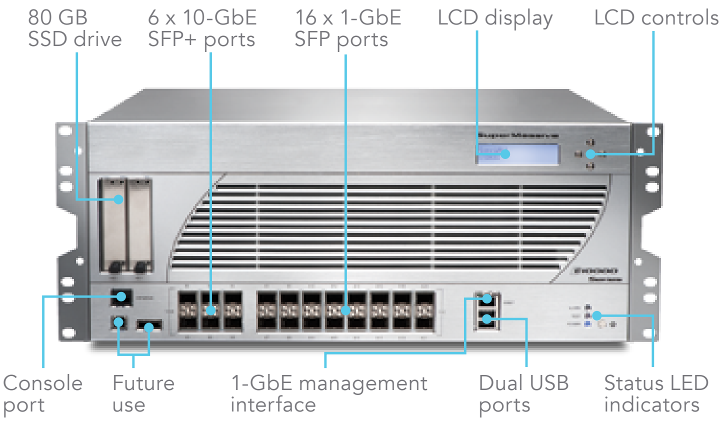
- Complete threat protection including high performance intrusion prevention, low latency malware protection and network sandboxing
- Superior granular application intelligence, control and visualization
- Full inspection of SSL encrypted traffic without the overhead, latency and memory thrashing associated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

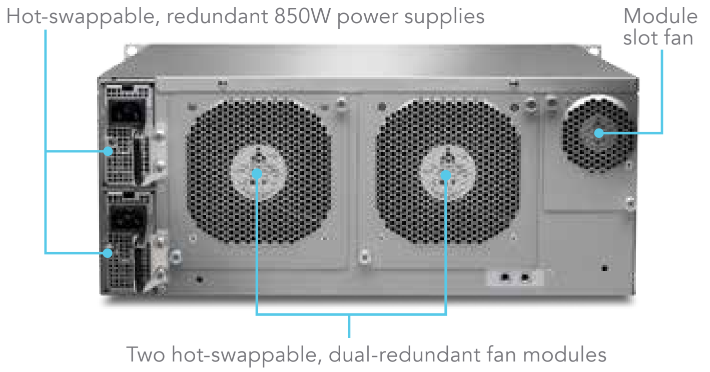
Series lineup

The SonicWall SuperMassive E10000 Series chassis includes 6 x 10-GbE SFP+ and 16 x 1-GbE SFP ports, redundant 850W AC power supplies and hot-swappable, dual-redundant fan modules, and it massively scales up to 96 processing cores.

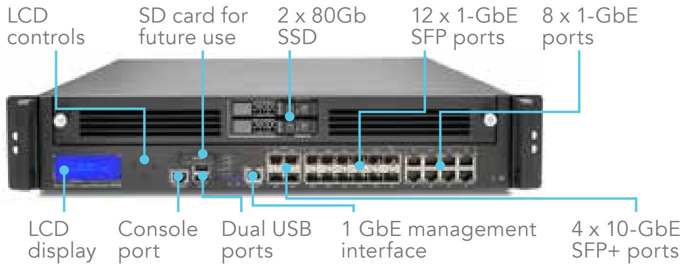
The SonicWall SuperMassive 9000 Series features 4 x 10-GbE SFP+, up to 12 x 1-GbE SFP, 8 x 1-GbE copper and 1 GbE management interfaces, with an expansion port for an additional 2 x 10-GbE SFP+ interfaces (future release). The 9000 Series features hot-swappable fan modules and power supplies.

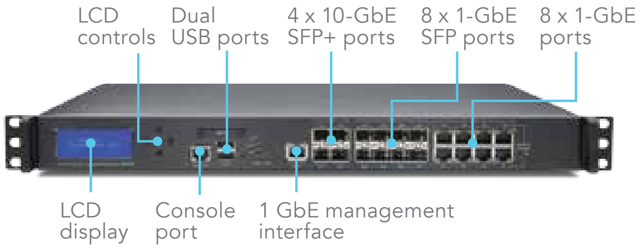
SuperMassive E10000 Series

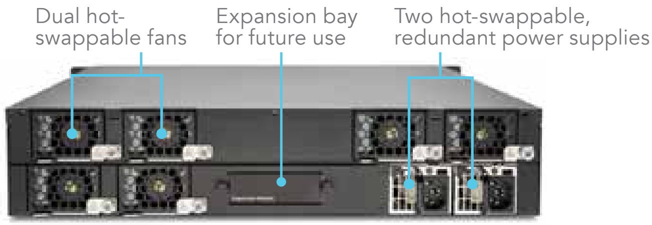


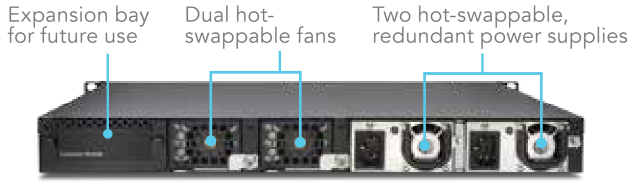

Hot-swappable, redundant 850W power supplies
Module slot fan
Two hot-swappable, dual-redundant fan modules

SuperMassive 9000 Series






Dual hot-swappable fans
Expansion bay for future use
Two hot-swappable, redundant power supplies

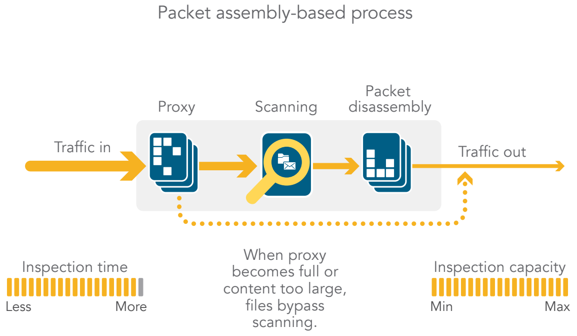

Expansion bay for future use
Dual hot-swappable fans
Two hot-swappable, redundant power supplies

Capability	9200	9400	9600	9800	E10400	E10800
Processing cores	24	32	32	64	48	96
Firewall throughput	15 Gbps	20 Gbps	20 Gbps	40 Gbps	20 Gbps	40 Gbps
Application intelligence throughput	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps	15 Gbps	28 Gbps
Intrusion prevention system (IPS) throughput	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps	15 Gbps	30 Gbps
Anti-malware	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps	6 Gbps	12 Gbps
Maximum DPI connections	1.25 M	1.25 M	1.5 M	2.5 M	5 M	10 M
Deployment modes	**9200**	**9400**	**9600**	**9800**	**E10400**	**E10800**
L2 bridge mode	Yes	Yes	Yes	Yes	Yes	Yes
Wire mode	Yes	Yes	Yes	Yes	Yes	Yes
Gateway/NAT mode	Yes	Yes	Yes	Yes	Yes	Yes
Tap mode	Yes	Yes	Yes	Yes	Yes	Yes
Transparent mode	Yes	Yes	Yes	Yes	Yes	Yes

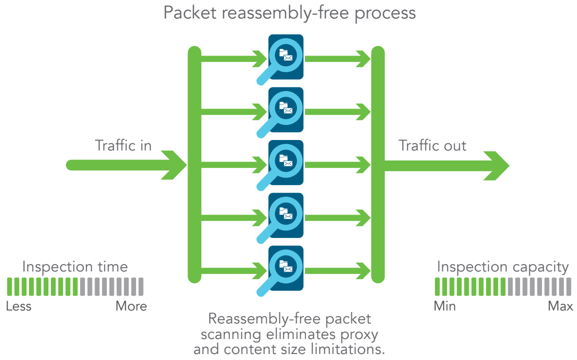
Reassembly-Free Deep Packet Inspection engine

The RFDPI engine provides superior threat protection and application control without compromising performance. This patented engine relies on streaming traffic payload inspection in order to detect threats at Layers 3-7. The RFDPI engine takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including SSL decryption, it is analyzed against a single proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken. In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in the case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified.



Competitive architecture

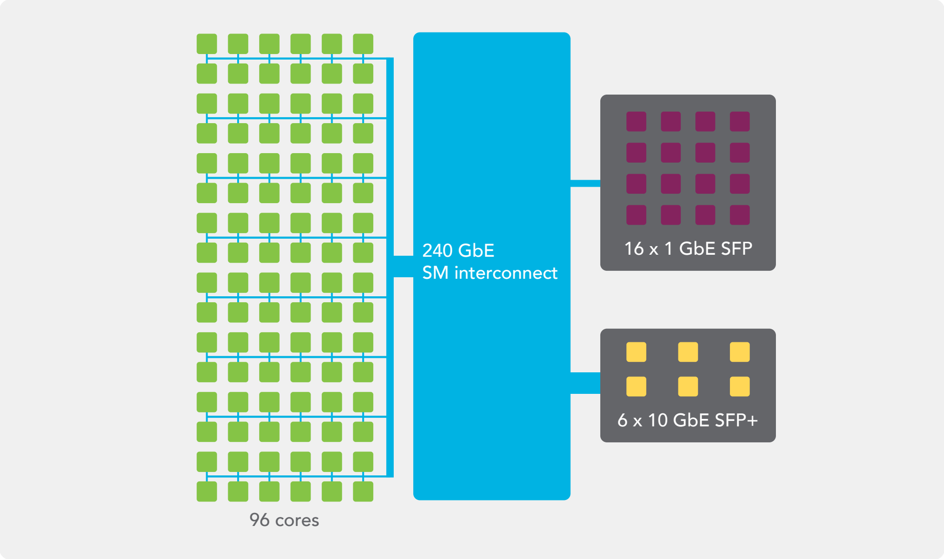

Packet reassembly-free process
Traffic in
Traffic out
Inspection time
Less
More
Inspection capacity
Min
Max
Reassembly-free packet scanning eliminates proxy and content size limitations.

SonicWall architecture

Extensible architecture for extreme scalability and performance

The RFDPI engine is designed from the ground up with an emphasis on providing security scanning at a high level of performance, to match both the inherently parallel and ever-growing nature of network traffic. When combined with 24-, 32-, 48-, 64- or 96-core processor systems, this parallelism-centric software architecture scales up perfectly to address the demands of deep packet inspection (DPI) at high traffic loads. The SuperMassive platform relies on processors that, unlike x86, are optimized for packet, crypto and network processing while retaining flexibility and programmability in the field — a weak point for ASICs systems. This flexibility is essential when new code and behavior updates are necessary to protect against new attacks that require updated and more sophisticated detection techniques.

Another aspect of the platform design is the unique ability to establish new connections on any core in the system, providing ultimate scalability and the ability to deal with traffic spikes. This approach delivers extremely high new session establishment rates (new conn/sec) while deep packet inspection is enabled — a key metric that is often a bottleneck for data center deployments.



Security and protection

The dedicated, in-house SonicWall Threats Research Team works on researching and developing countermeasures to deploy to the firewalls in the field for up-to-date protection. The team leverages more than one million sensors across the globe for malware samples and for telemetry feedback on the latest threat information, which in turn is fed into the intrusion prevention, anti-malware and application detection capabilities. SonicWall NGFW customers with the latest security capabilities are provided continuously updated threat protection around the clock, with new updates taking effect immediately without reboots or interruptions. The signatures on the appliances protect against wide classes of attacks, covering up to tens of thousands of individual threats with a single signature.

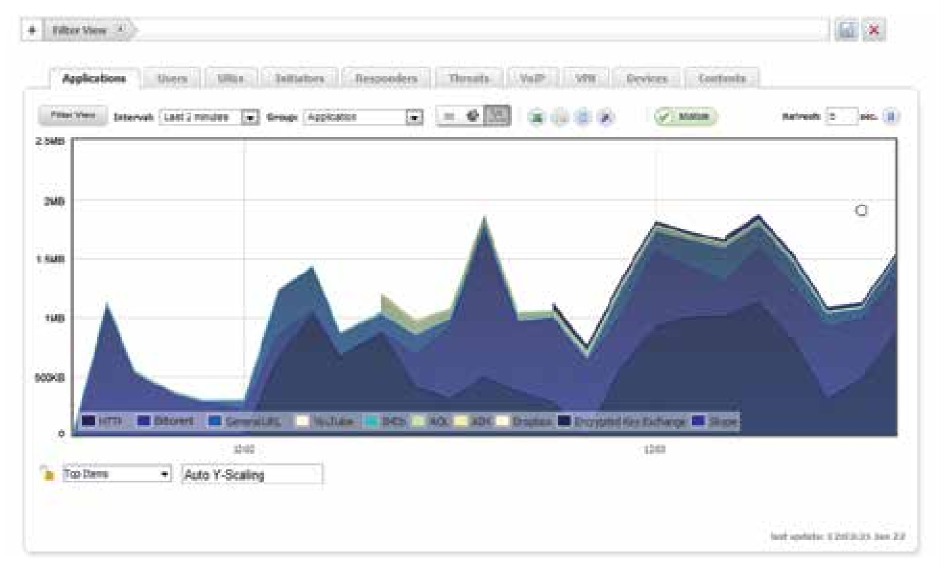
In addition to the countermeasures on the appliance, SuperMassive firewalls also have access to the SonicWall CloudAV Service, which extends the onboard signature intelligence with more than seventeen million signatures, and growing. This CloudAV database is accessed via a proprietary, lightweight protocol by the firewall to augment the inspection done on the appliance. With Capture Advanced Threat Protection, a cloud-based network sandbox, organizations can examine suspicious files and code in an isolated environment to stop advanced threats such as zero-day attacks.

Protection
Collection
Creation
Classification

Application intelligence and control

Application intelligence informs administrators of application traffic traversing their network so they can schedule application controls based on business priority, throttle unproductive applications and block potentially dangerous applications. Real-time visualization identifies traffic anomalies as they happen, enabling immediate countermeasures against potential inbound or outbound attacks or performance bottlenecks.

SonicWall Application Traffic Analytics provide granular insight into application traffic, bandwidth utilization and security threats, as well as powerful troubleshooting and forensics capabilities. Additionally, secure single sign-on (SSO) capabilities ease the user experience, increase productivity and reduce support calls. Management of application intelligence and control is simplified by the intuitive web-based interface.



Interval: Last 2 minutes

Group: Application

Refresh: 5 sec.

Global management and reporting

For larger, distributed enterprise deployments, the optional SonicWall Global Management System (GMS®) provides administrators a unified, secure and extensible platform to manage SonicWall security appliances. It enables enterprises to easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities, and govern all operational aspects of the security infrastructure, including centralized policy management and enforcement, real-time event monitoring, analytics and reporting, and more. GMS also meets the firewall change management requirements of enterprises through a workflow automation feature. With GMS workflow automation, all enterprises will gain agility and confidence in deploying the right firewall policies, at the right time and in conformance to compliance regulations. GMS provides a better way to manage network security by business processes and service levels, dramatically simplifying lifecycle management of your overall security environments as compared to managing on a device-by-device basis.

Features

RFDPI engine	
Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

Capture advanced threat protection	
Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility into malicious activity.
Broad file type and size analysis	Analyzes a broad range of file types including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems (Windows, Android, Mac OS X) and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with an active SonicWall Capture subscription as well as Capture Threat Network Gateway Anti-virus and IPS signature databases plus URL, IP and domain reputation databases within 48 hours.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.

Intrusion prevention	
Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take effect immediately, without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly detection and prevention	Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

Threat prevention	
Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
CloudAV	A continuously updated database of over 17 million threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	The SonicWall Threat Research Team analyzes new threats and releases countermeasures 24 hours a day, 7 days a week. New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
SSL inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in SSL encrypted traffic.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally, preventing attacks that try to sneak by outdated security systems that focus on securing a few well-known ports.
Extensive protocol support	Identifies common protocols, such as HTTP/S, FTP, SMTP and SMB v1/v2, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard, well-known ports.

Features

Application intelligence and control

Feature	Description
Application control	Controls applications, or individual application features, which are identified by the RFDPI engine against a continuously expanding database of over 3600 application signatures, to increase network security and enhance network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.
Application bandwidth management	Granularly allocates and regulates available bandwidth for critical applications or application categories while inhibiting non-essential application traffic.
On-box/off-box traffic visualization	Identifies bandwidth utilization and analyzes network behavior with real-time, on-box application traffic visualization and off-box application traffic reporting via NetFlow/IPFix.
Granular control	Controls applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

Content filtering

Feature	Description
Inside/outside content filtering	Content Filtering Service enforces acceptable use policies and blocks access to websites containing information or images that are objectionable or unproductive. Content Filtering Client extends policy enforcement to block internet content for devices located outside the firewall perimeter.
Granular controls	Blocks content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Dynamic rating architecture	All requested web sites are cross-referenced against a dynamically updated database in the cloud categorizing millions of URLs, IP addresses and domains in real time.
YouTube for Schools	Enables teachers to choose from hundreds of thousands of free educational videos from YouTube EDU that are organized by subject and grade and that align with common educational standards.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.

Enforced anti-virus and anti-spyware

Feature	Description
Multi-layered protection	A firewall's gateway anti-virus solution provides the first layer of defense at the perimeter; however, viruses can still enter the network through laptops, thumb drives and other unprotected systems. Utilizes a layered approach to anti-virus and anti-spyware protection to extend to both client and server.
Automated enforcement	Ensures every computer accessing the network has the most recent version of anti-virus and anti-spyware signatures installed and active, eliminating the costs commonly associated with desktop anti-virus and anti-spyware management.
Automated deployment and installation	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Always on, automatic virus protection	Frequent anti-virus and anti-spyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they can transmit confidential data, providing greater desktop security and performance.

Firewall and networking

Feature	Description
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DDoS/DoS attack protection	SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The SuperMassive Series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With the latest SonicOS 6.2, the hardware will support filtering and wire mode implementations.
High availability/clustering	The SuperMassive Series supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI and Active/Active clustering high availability modes. Active/Active DPI offloads the deep packet inspection load to cores on the passive appliance to boost throughput.
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods.
Policy-based routing	Creates 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.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.

Features

Management and reporting	
Feature	Description
Global Management System	SonicWall GMS monitors, configures and reports on multiple SonicWall appliances through a single management console with an intuitive interface, reducing management costs and complexity.
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Scrutinizer or other tools that support IPFIX and NetFlow with extensions.

Virtual private networking (VPN)	
Feature	Description
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the SuperMassive 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	Utilizes 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.

Content/context awareness	
Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix1/Terminal Services1 SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic *i*dentification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

[1] *Supported on SonicOS 6.1 and 6.2. Not supported on SonicOS 6.2.1.*

[2] *Requires added subscription.*

Feature summary

Firewall

- Reassembly-Free Deep Packet Inspection
- SSL decryption and inspection
- Stateful packet inspection
- Stealth mode
- Common Access Card (CAC) support
- DOS attack protection
- UDP/ICMP/SYN flood protection
- IPv6 security
- Management and monitoring: IPv4 and IPv6 management
- Networking: IPv6

Capture advanced threat protection2

- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates
- Auto-block capability

Intrusion prevention2

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection engine
- Granular IPS rule set
- GeoIP and reputation-based filtering
- Regular expression matching
- UDP/ICMP/SYN flood protection

Anti-malware2

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application intelligence

- Application control
- Application component blocking
- Application bandwidth management
- Custom application signature creation
- Application traffic visualization
- Data leakage prevention
- Application reporting over NetFlow/ IPFIX
- User activity tracking (SSO)
- Comprehensive application signature database

Web content filtering2

- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth management for CFS categories
- Unified policy model with app control
- 56 content filtering categories
- Content Filtering Client (SonicOS 6.2)

VPN

- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSEC client remote access
- Redundant VPN gateway
- Mobile Connect for Apple® iOS and Google® Android™
- Route-based VPN (OSPF, RIP)

Networking

- Jumbo frames (SonicOS 6.0.5 and 6.2 only)
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Layer-2 network discovery
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing
- SonicPoint wireless controller[1]
- Policy-based routing
- Advanced NAT
- DHCP server
- Bandwidth management
- Link aggregation
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire mode, tap mode, NAT mode

VoIP

- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

Management and monitoring

- Web GUI
- Command-line interface (CLI)
- SNMPv2/v3
- Off-box reporting (Scrutinizer)
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Application and bandwidth visualizer
- LCD management screen
- Single sign-on (SSO)
- Terminal service/Citrix support[1]
- BlueCoat Security Analytics Platform

SuperMassive E10000 Series system specifications

	E10400	E10800
Operating system	SonicOS	
Security processing cores	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)	32 GB	64 GB
Storage	80 GB SSD, flash	
Firewall inspection throughput[1]	20 Gbps	40 Gbps
Application inspection throughput[2]	15 Gbps	30 Gbps
IPS throughput[2]	15 Gbps	28 Gbps
Anti-malware inspection throughput[2]	6 Gbps	12 Gbps
IMIX performance	4.3 Gbps	9 Gbps
SSL-DPI performance	3 Gbps	5 Gbps
VPN throughput[3]	7.5 Gbps	11 Gbps
Latency	24μs	
Connections per second	200,000/sec	400,000/sec
Maximum connections (SPI)	6 M	12 M
Maximum connections (DPI)	5 M	10 M
SSO users	40,000	60,000
VPN	E10400	E10800
Site-to-site tunnels	10,000	
IPSec VPN clients (max)	2,000 (10,000)	
Encryption	DES, 3DES, AES (128, 192, 256-bit)	
Authentication	MD5, SHA-1, Common Access Card (CAC)	
Key exchange	Diffie Hellman Groups 1, 2, 5, 14	
Route-based VPN	RIP, OSPF	
Networking	E10400	E10800
IP address assignment	Static, internal DHCP server, DHCP relay	
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT, transparent mode	
VLAN interfaces	1024	2048
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	
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	FIPS 140-2, Common Criteria NDPP, IPv6 Phase 2, VPAT, VPNC	
Third-party verification	NSS NGFW Recommended and NSS IPS Recommended	
Hardware	E10400	E10800
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)	550	750
MTBF @25°C in hours	120,790	
MTBF @25°C in years	13.789	
Form factor	4U Rack Mountable	
Dimensions	17x18x7 in (43x43.5x17.8 cm)	
Weight	61 lb (27.7 kg)	67 lb (30.3 k
WEEE weight	62 lb (28.1 kg)	68 lb (30.8 kg)
Shipping weight	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	

[1] Testing methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. [2] Full DPI/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. [3] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.

SuperMassive 9000 Series system specifications

	9200	9400	9600	9800
Operating system	SonicOS			
Security processing cores	24	32		64
10 GbE interfaces	4 x 10-GbE SFP+			
1 GbE interfaces	8 x 1-GbE SFP, 8 x 1 GbE (1 LAN bypass pair)			12 x 1-GbE SFP, 8 x 1 GbE
Management interfaces	1 GbE, 1 console			
Memory (RAM)	8 GB	16 GB	32 GB	64 GB
Storage	Flash			2x 80GB SSD, Flash
Expansion	1 expansion slot (rear)*, SD card*			
Firewall inspection throughput[1]	15 Gbps	20 Gbps		40 Gbps
Application inspection throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
IPS throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
Anti-malware inspection throughput[2]	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps
IMIX performance	4.4 Gbps	5.5 Gbps		9 Gbps
SSL-DPI	1 Gbps	2 Gbps	2 Gbps	5 Gbps
VPN throughput[3]	5 Gbps	10 Gbps	11.5 Gbps	18 Gbps
Latency	17μs			
Connections per second	100,000/sec	130,000/sec		280,000/sec
Maximum connections (SPI)	1.25 M		1.5 M	3 M
Maximum connections (DPI)	1 M		1.25 M	2.5 M
SSO users	80,000	90,000	100,000	110,000
Maximum SonicPoints supported	128			-
VPN	9200	9400	9600	9800
Site-to-site tunnels	10,000			25,000
IPSec VPN clients (max)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)	2,000 (10,000)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF			
Networking	9200	9400	9600	9800
IP address assignment	Static, DHCP, PPPoE, L2TP and PPTP client, internal DHCP server, DHCP relay[4]			
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[5], Citrix[5]			
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	UC APL[6], ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[6], Common Criteria NDPP[6]			
Certifications pending	ICSA Anti-Virus			
Hardware	9200	9400	9600	9800
Power supply	Dual-redundant, hot-swappable, 300 W			Dual-redundant, hot-swappable, 500 W
Fans	Dual-redundant, hot-swappable			
Display	Front LED display			
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	200			350
MTBF @25°C in hours	188,719	187,702	186,451	126,144
MTBF @25°C in years	21.543	21.427	21.284	14.400
Form factor	1U rack-mountable			2U rack-mountable
Dimensions	17x19.1x1.75 in (43.3x48.5x4.5 cm)			17x24x3.5 in (9x60x43 cm)
Weight	18.1 lb (8.2 kg)			40.5 lb (18.38 kg)
WEEE weight	23 lb (10.4 kg)			49.5 lb (22.4 kg)
Shipping weight	29.3 lb (13.3 kg)			65 lb (29.64 kg)
Major regulatory	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE , ANATEL, BSMI			
Environment	32-105 F, 0-40 deg C			15-40 deg C
Humidity	10-90% non-condensing			

*[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. [2] Full DPI/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. [3] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. [4] PPPoE, L2TP and PPTP clients are not supported on SM9800. [5] Supported on SonicOS 6.1 and 6.2. [6] Applies to SuperMassive 9200, 9400 and 9600. SuperMassive 9800 UC APL certification is pending. *Future use. All specifications, features and availability are subject to change.*

SuperMassive E10000 Series ordering information

Product	SKU
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 E10200 to E10400 upgrade	01-SSC-9497
SuperMassive E10400 to E10800 upgrade	01-SSC-9498
SuperMassive E10400 support and security subscriptions	**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
SuperMassive E10800 support and security subscriptions	**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
Modules and accessories*	**SKU**
SuperMassive E10000 Series system fan field replaceable unit (FRU)	01-SSC-8885
SuperMassive E10000 Series SSD fan module	01-SSC-8886
SuperMassive E10000 Series power supply FRU	01-SSC-8887
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twinax Cable	01-SSC-9787
10GBASE SFP+ 3M Twinax Cable	01-SSC-9788
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Copper Module	01-SSC-9791
Management and reporting	**SKU**
SonicWall GMS 10-node software license	01-SSC-3363
SonicWall GMS E-Class 24x7 Software Support for 10 nodes (1-year)	01-SSC-6514
SonicWall Scrutinizer virtual appliance with Flow Analytics Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3443
SonicWall Scrutinizer with Flow Analytics Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-4002
SonicWall Scrutinizer Advanced Reporting Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3773

**Please consult with an SE for a complete list of supported SFP and SFP+ modules.*

SuperMassive 9000 Series ordering information

Product	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 and security subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for SuperMassive 9200 (1-year)	01-SSC-1570
Capture Advanced Threat Protection for SuperMassive 9200 (1-year)	01-SSC-1575
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9200 (1-year)	01-SSC-4172
Intrusion Prevention, Anti-Malware, CloudAV, Application Intellience, Control and Visualization for SuperMassive 9200 (1-year)	01-SSC-4202
Content Filtering Premium Business Edition for 9200 (1-year)	01-SSC-4184
Platinum Support for the SuperMassive 9200 (1-year)	01-SSC-4178
SuperMassive 9400 support and security subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for SuperMassive 9400 (1-year)	01-SSC-1580
Capture Advanced Threat Protection for SuperMassive 9400 (1-year)	01-SSC-1585
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9400 (1-year)	01-SSC-4136
Intrusion Prevention, Anti-Malware, CloudAV, Application Intellience, Control and Visualization for SuperMassive 9400 (1-year)	01-SSC-4166
Content Filtering Premium Business Edition for 9400 (1-year)	01-SSC-4148
Platinum Support for the SuperMassive 9400 (1-year)	01-SSC-4142
SuperMassive 9600 support and security subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for SuperMassive 9600 (1-year)	01-SSC-1590
Capture Advanced Threat Protection for SuperMassive 9600 (1-year)	01-SSC-1595
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9600 (1-year)	01-SSC-4100
Intrusion Prevention, Anti-Malware, CloudAV, Application Intellience, Control and Visualization for SuperMassive 9600 (1-year)	01-SSC-4130
Content Filtering Premium Business Edition for 9600 (1-year)	01-SSC-4112
Platinum Support for the SuperMassive 9600 (1-year)	01-SSC-4106
SuperMassive 9800 support and security subscriptions	**SKU**
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9800 (1-year)	01-SSC-0809
Intrusion Prevention, Anti-Malware, CloudAV, Application Intellience, Control and Visualization for SuperMassive 9800 (1-year)	01-SSC-0827
Content Filtering Premium Business Edition for 9800 (1-year)	01-SSC-0821
Gold 24x7 Support for the SuperMassive 9800 (1-year)	01-SSC-0815
Modules and accessories*	**SKU**
SonicWall SuperMassive 9800 Series system fan FRU	01-SSC-0204
SonicWall SuperMassive 9800 Series power supply AC FRU	01-SSC-0203
SonicWall SuperMassive 9000 Series system fan FRU	01-SSC-3876
SonicWall SuperMassive 9000 Series power supply AC FRU	01-SSC-3874
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Copper Module	01-SSC-9791
Management and reporting	**SKU**
SonicWall GMS 10-node software license	01-SSC-3363
SonicWall GMS E-Class 24x7 Software Support for 10 nodes (1-year)	01-SSC-6514
SonicWall Scrutinizer virtual appliance with Flow Analytics Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3443
SonicWall Scrutinizer with Flow Analytics Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-4002
SonicWall Scrutinizer Advanced Reporting Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3773

**Please consult with an SE for a complete list of supported SFP and SFP+ modules.*

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com