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, education, retail, healthcare and service provider, the SuperMassive Series is ideal for securing distributed enterprise networks, data centers and service providers.

The combination of SonicWall's SonicOS operating system, patented* Reassembly-Free Deep Packet Inspection® (RFDPI) technology and massively multi-core, highly scalable hardware architecture, the SuperMassive 9000 Series deliver industry-leading application control, intrusion prevention, malware protection and TLS/SSL decryption and inspection at multi-gigabit speeds. The SuperMassive Series is thoughtfully designed with power, space and cooling (PSC) in mind, providing the leading Gbps/watt NGFW in the industry for high performance packet and data processing, 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 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 various forms of malware before they enter the network and provides protection against evolving threats — without file size, performance or latency limitations.

The RFDPI engine also performs full decryption and inspection of TLS/SSL and SSH encrypted traffic as well as non-proxyable applications, enabling complete protection regardless of transport or protocol. It looks deep inside every packets (the header and data part) searching for protocol non-compliance, threats, zero-days, intrusions, and even defined criteria to detect and prevent attacks hidden inside encrypted traffic, cease the spread of infections, and thwart command and control (C&C) communications and data exfiltration. Inclusion and exclusion rules allow total control to customize which traffic is subject to decryption and inspection based on specific organizational compliance and/or legal requirements.

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 Capture Labs threats research team. Additionally, SonicOS, an advanced purpose-built operating system, provides integrated tools that allow for custom application identification and control.

SuperMassive 9000 Series

Benefits:

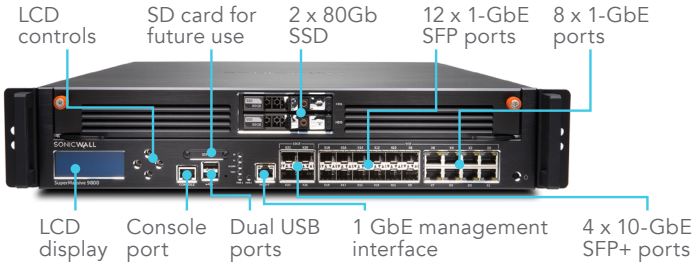
- Get complete breach prevention including high performance intrusion prevention, low latency malware protection and cloud-based sandboxing
- Gain full granular application identification, control and visualization
- Find and block hidden threats with decryption and inspection of TLS/SSL and SSH encrypted traffic, without performance problems
- Scale security performance for 10/40 Gbps data centers
- Adapt to service-level increases and ensure network services and resources are available and protected

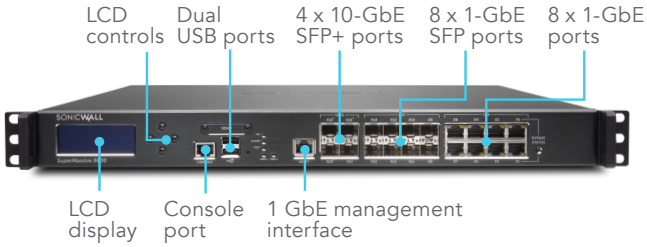
**U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361*

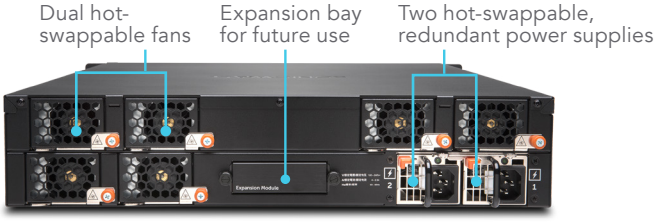
Series lineup

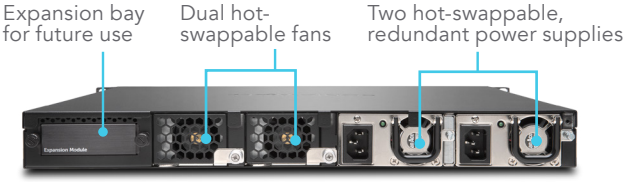
The SonicWall SuperMassive 9000 Series features 4 x 10-GbE SFP+, up to 12 x 1-GbE SFP, 8 x 1-GbE copper and 1 GbE management interfaces, with an expansion port for an additional 2 x 10- GbE SFP+ interfaces (future release). The 9000 Series features hot-swappable fan modules and power supplies.

SuperMassive 9000 Series







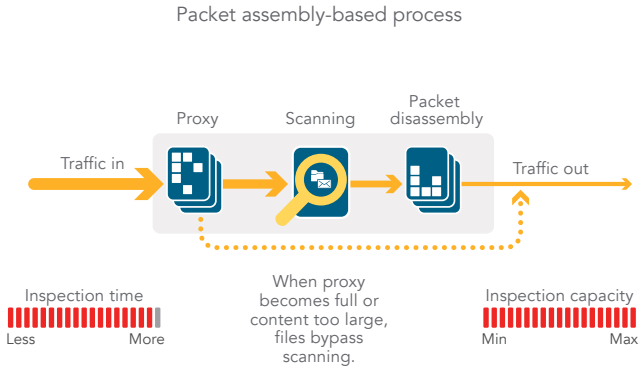


Capability	9200	9400	9600	9800
Processing cores	24	32	32	64
Firewall throughput	15 Gbps	20 Gbps	20 Gbps	28 Gbps
Application intelligence throughput	5 Gbps	10 Gbps	11.5 Gbps	20 Gbps
Intrusion prevention system (IPS) throughput	5 Gbps	10 Gbps	11.5 Gbps	18 Gbps
Anti-malware	3.5 Gbps	4.5 Gbps	5 Gbps	9.0 Gbps
Maximum DPI connections	1.5 M	1.5 M	2.0 M	2.5 M
Deployment modes	**9200**	**9400**	**9600**	**9800**
L2 bridge mode	Yes	Yes	Yes	Yes
Wire mode	Yes	Yes	Yes	Yes
Gateway/NAT mode	Yes	Yes	Yes	Yes
Tap mode	Yes	Yes	Yes	Yes
Transparent mode	Yes	Yes	Yes	Yes

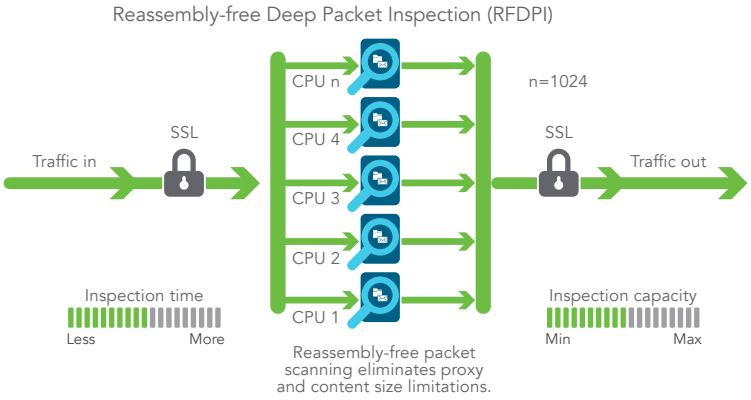
Reassembly-Free Deep Packet Inspection engine

RFDPI is a single-pass, low latency inspection system that performs stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts, malware and identify application traffic regardless of port and protocol. This proprietary 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 obfuscation and evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including TLS/SSL decryption, it is analyzed against a single proprietary memory representation of multiple signature databases: intrusion attacks, malware, botnet 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 preset 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 proxy-based architecture

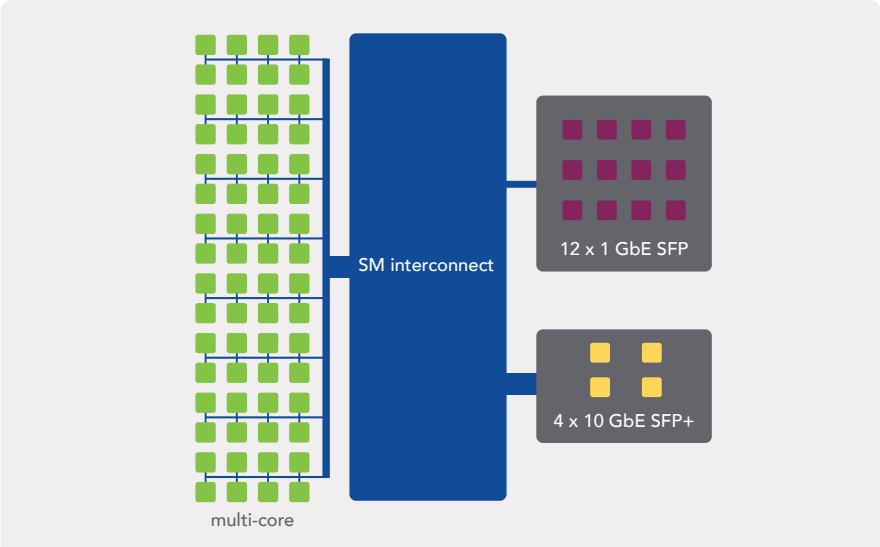


SonicWall stream-based architecture

Extensible architecture for extreme scalability and performance

The RFDPI engine is purposely designed with a keen focus 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 multi-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.



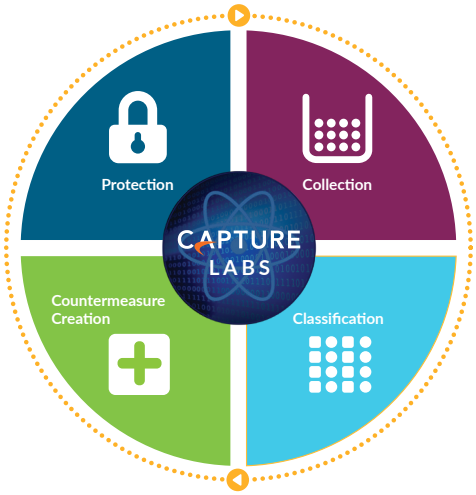
SONICWALL®

Capture Labs

The dedicated, in-house SonicWall Capture Labs threats research team researches and develops countermeasures to deploy to customer firewalls for up-to-date protection. The team gathers data on potential threat data from several sources including our award-winning network sandboxing service, Capture Advanced Threat Protection, as well as more than 1 million SonicWall sensors located around the globe that monitor traffic for emerging threats. It is analyzed via machine learning using SonicWall's Deep Learning Algorithms to extract the DNA from the code to see if it is related to any known forms of malicious code.

SonicWall NGFW customers with the latest security capabilities are provided continuously updated threat protection around the clock. New updates take 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[1], which extends the onboard signature intelligence with tens of millions of signatures, and growing by millions annually. This CloudAV database is accessed by the firewall via a proprietary, lightweight protocol to augment the inspection done on the appliance. With Capture Advanced Threat Protection[1], a cloud-based multi-engine sandbox, organizations can examine suspicious files and code in an isolated environment to stop advanced threats such as zero-day attacks.



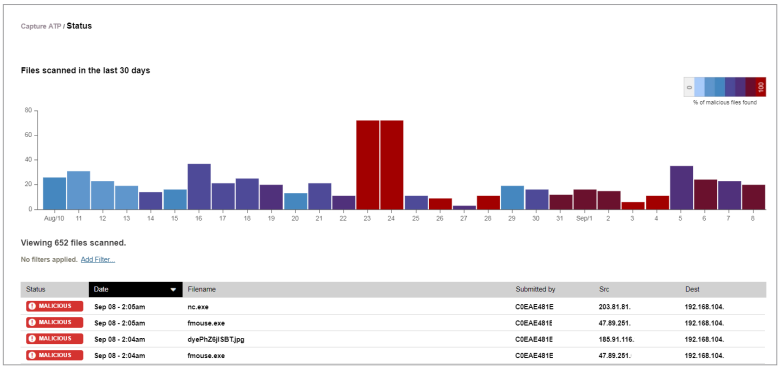
[1] Requires added subscription

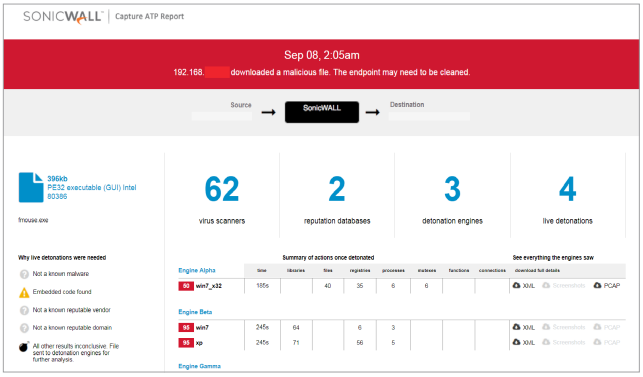
Advanced threat protection

SonicWall Capture Advanced Threat Protection Service[1] is a cloud-based multi-engine sandbox that extends firewall threat protection to detect and prevent zero-day threats. Suspicious files are sent to the cloud for analysis with the option to hold them at the gateway until a verdict is determined. The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior. When a file is identified as malicious, a hash is immediately created within Capture and later a signature is sent to firewalls to prevent follow-on attacks.

The service analyzes a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

Capture provides an at-a-glance threat analysis dashboard and reports, which detail the analysis results for files sent to the service, including source, destination and a summary plus details of malware action once detonated.





SONICWALL®

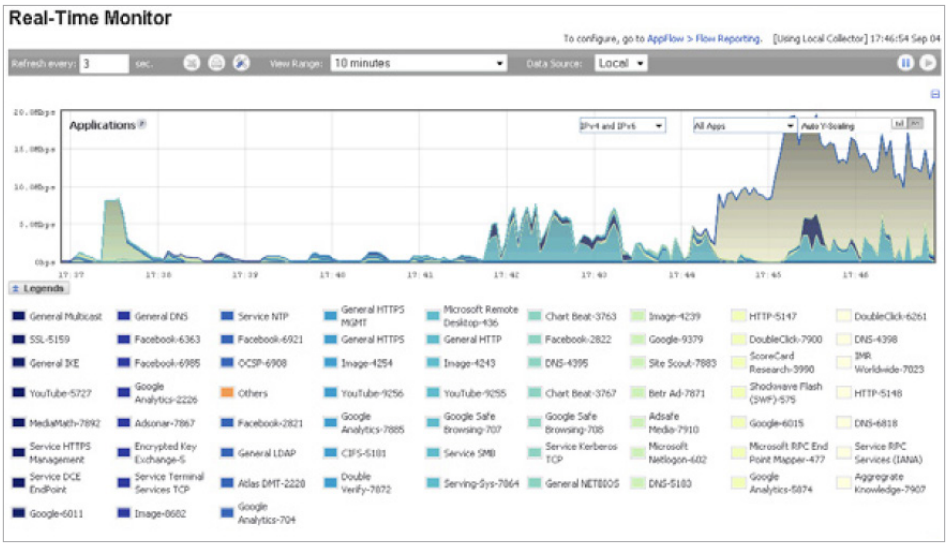
Application intelligence and control

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[1] 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.

Global management and reporting

For highly regulated organizations wanting to achieve a fully coordinated security governance, compliance and risk management strategy, the optional SonicWall Global Management System[1] (GMS®) provides administrators a unified, secure and extensible platform to manage SonicWall firewalls, wireless access points and switches through a correlated and auditable workstream process. GMS 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; user activities; application identifications; flow analytics and forensics; compliance and audit reporting; and more. GMS also meets the firewall

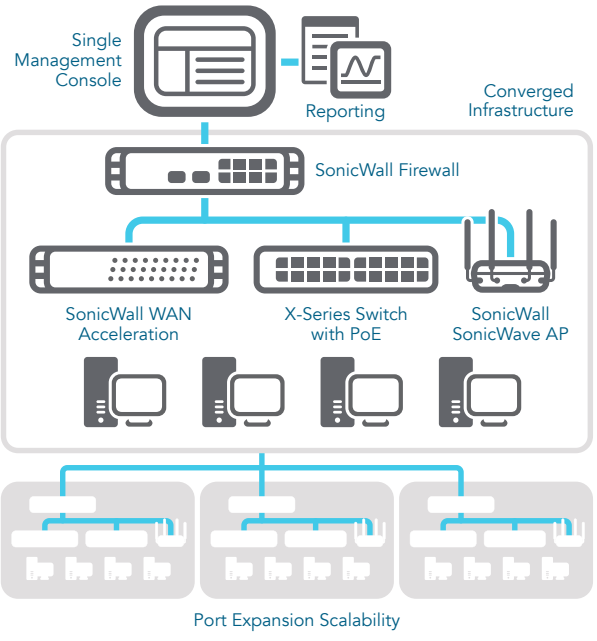


change management requirements of enterprises through a workflow automation feature. With GMS workflow automation, all enterprises will gain agility and confidence in deploying the right firewall policies, at the right time and in conformance to compliance regulations. GMS provides a coherent way to 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.

SonicWall GMS Secure Compliance Enforcement

Benefits

- Centralized management
- Error-free policy management
- Strong access control
- Comprehensive audit trails
- PCI, HIPAA, SOX report templates
- Lower operating costs



[1] *Requires added subscription*

SONICWALL®

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.

Firewall and networking	
Feature	Description
Threat API	All the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
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.
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.
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.
Flexible deployment options	The SuperMassive Series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes.
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.
Single and cascaded Dell X-Series network switch management	Manage security settings of additional ports, including Portshield, HA, POE and POE+, under a single pane of glass using the firewall management dashboard for Dell's X-Series network switch.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credential from social networking service such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.
Multi-domain authentication	Enables simple and fast way to administer security polices across all network domains. Manage individual policy to a single domain or group of domains.

Management and reporting	
Feature	Description
Global Management System[1] (GMS)	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.

Features

Virtual private networking (VPN)	
Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
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 identification	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. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

Capture advanced threat protection[1]	
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 to malicious activity
Block Until Verdict	Provides the ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.
Broad File Type Analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS and multi-browser environments.
Rapid Deployment of Signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture subscriptions and GRID Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.

Encrypted threat prevention[1]	
Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects SSL/TLS 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 TLS/SSL encrypted traffic. Included with security subscriptions for all models.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH.

Intrusion prevention[1]	
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.

Features

Threat prevention[1]	
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 malware protection	A continuously updated database of tens of millions of 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	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they 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, SMBv1/v2 and others, 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.

Application intelligence and control[1]	
Feature	Description
Application control	Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity.
Custom application identification	Control 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 allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic.
Granular control	Control 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[1]	
Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to websites containing information or images that are objectionable or unproductive with Content Filtering Service.
Enforced content filtering client	Extend policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Block 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.
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[1]	
Feature	Description
Multi-layered protection	Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure 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 option	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 decrease 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 transmit confidential data, providing greater desktop security and performance.

[1] *Requires added subscription*

Feature summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- Threat API

SSL/SSH decryption and inspection[2]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL Control

Capture advanced threat protection[2]

- 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 prevention[2]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection engine
- Granular IPS rule set
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[2]

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

Application identification[2]

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

Web content filtering[2]

- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth management for CFS categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSEC client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

Networking

- Dynamic LAG using LACP
- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller[1]
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire/virtual wire mode, tap mode, NAT mode
- 3G/4G WAN failover (not on SuperMassive 9800)
- Asymmetric routing
- Common Access Card (CAC) support

Wireless

- MU-MIMO
- Wireless planning tool
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Guest cyclic quota

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
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- LCD management screen
- Dell X-Series switch management[1]

[1] Not supported on SonicOS 6.2.7.7
[2] Requires added subscription

SONICWALL®

SuperMassive 9000 Series system specifications

Firewall General	9200	9400	9600	9800
Operating system	SonicOS			
Security processing cores	24	32		64
Interfaces	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE, 1GbE Management, 1 Console			4x10GbE SFP+, 12x1GbE SFP, 8x1GbE, 1GbE Management, 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*			
Management	CLI, SSH, GUI, GMS			
SSO users	80,000	90,000	100,000	110,000
Maximum SonicPoints supported	128			-
Logging	Analyzer, Local Log, Syslog			
High availability	Active/Passive with State Sync, Active/Active DPI with State Sync			
Firewall/VPN Performance	**9200**	**9400**	**9600**	**9800**
Firewall Inspection Throughput[1]	15 Gbps	20 Gbps	20 Gbps	28 Gbps
Full DPI Performance2 (GAV/GAS/IPS)	3 Gbps	4.4 Gbps	4.5 Gbps	9 Gbps
Application Inspection Throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	20 Gbps
IPS Throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	18 Gbps
Anti-Malware Inspection Throughput[1]	3.5 Gbps	4.5 Gbps	5.0 Gbps	9 Gbps
IMIX performance	4.4 Gbps	5.5 Gbps	5.5 Gbps	6 Gbps
SSL inspection and decryption throughput (DPI SSL)[2]	1.0 Gbps	2.0 Gbps	2.0 Gbps	3 Gbps
VPN Throughput[3]	5 Gbps	10 Gbps	11.5 Gbps	14 Gbps
Connections per second	100,000/sec	130,000/sec	130,000/sec	226,000/sec
Maximum connections (SPI)	5.0M	7.5M	10.0M	3.0M
Maximum connections (DPI)	1.5M	1.5M	2.0M	2.5M
DPI SSL connections[6] (Maximum)	8,000 (15,500[6])	10,000 (17,500[6])	12,000 (22,500[6])	48,000
VPN	**9200**	**9400**	**9600**	**9800**
Site-to-Site VPN Tunnels	10,000			25,000
IPSec VPN clients (Maximum)	2,000(4,000)	2,000(6,000)	2,000(10,000)	
SSL VPN NetExtender Clients (Maximum)	2 (3,000)	2 (3,000)	50 (3,000)	50 (50)
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	LDAP (multi-domains), XAUTH/RADIUS, SSO, 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[4], ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[4], Common Criteria NDPP[4], ICSA Anti-Virus[4]			
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	21.53	21.43	21.28	14.40
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 (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI, CU			
Environment	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. [4] Applies to SuperMassive 9200, 9400 and 9600. SuperMassive 9800 UC APL certification is pending. [5] Supported on SonicOS 6.1 and 6.2. [6] For every 125,000 DPI connections reduced, the number of available DPI SSL connections increases by 750. *Future use. All specifications, features and availability are subject to change.*

SONICWALL®

SuperMassive 9000 Series ordering information

Product	SKU
SuperMassive 9800 Total Secure Advance Edition (1-year)	01-SSC-0312
SuperMassive 9600 Total Secure Advance Edition (1-year)	01-SSC-1719
SuperMassive 9400 Total Secure Advance Edition (1-year)	01-SSC-1718
SuperMassive 9200 Total Secure Advance Edition (1-year)	01-SSC-1717
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 Intelligence, 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 Intelligence, 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 Intelligence, 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**
Advanced Gateway Security Suite: Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for SuperMassive 9800 (1-year)	01-SSC-1183
Capture Advanced Threat Protection for SuperMassive 9800 (1-year)	01-SSC-1188
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 Intelligence, 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 a SonicWall SE for a complete list of supported SFP and SFP+ modules.*

SONICWALL®

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

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

Datasheet-SuperMassive-US-VG-MKTG476

SONICWALL®