SONICWALL

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 multigigabit 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 pergroup 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 cloudbased 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

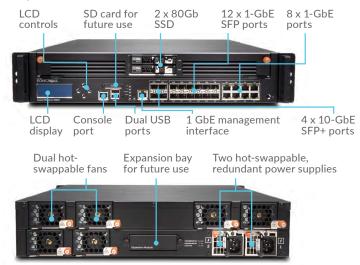
Partner Enabled Services

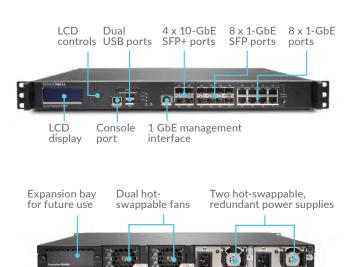
Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

Series lineup

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

SuperMassive 9000 Series





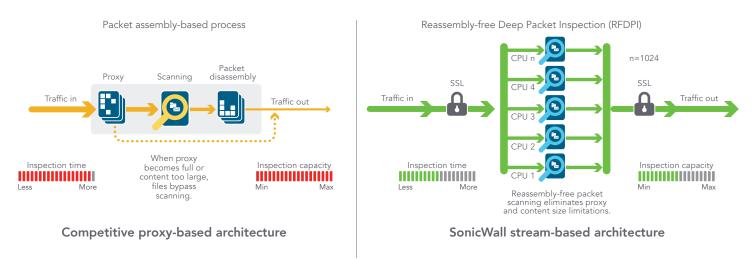
CAPABILITY	9200	9400	9600	9800
Processing cores	24	32	32	64
Firewall throughput	15 Gbps	20 Gbps	20 Gbps	31.8 Gbps
Application inspection throughput	5 Gbps	10 Gbps	11.5 Gbps	23 Gbps
Intrusion prevention system (IPS) throughput	5 Gbps	10 Gbps	11.5 Gbps	21.3 Gbps
Anti-malware inspection throughput	3.5 Gbps	4.5 Gbps	5 Gbps	11 Gbps
Maximum DPI connections	1.5 M	1.5 M	2.0 M	8.0 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.

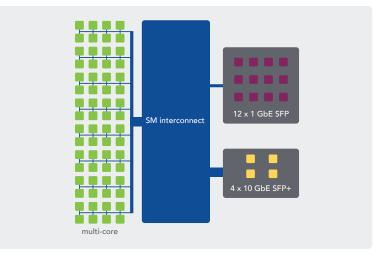
Once a packet undergoes the necessary pre-processing, including TLS/SSL decryption, it is analyzed against a single proprietary memory representation of multiple signature databases: intrusion attacks, malware, botnet and applications. The connection state is then advanced to represent the position of 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.



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 parallelismcentric 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.



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

¹Requires added subscription

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 CloudAV¹, 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 Protection¹, a cloud-based multiengine sandbox, organizations can examine suspicious files and code in an isolated environment to stop advanced threats such as zero-day attacks.



Advanced threat protection

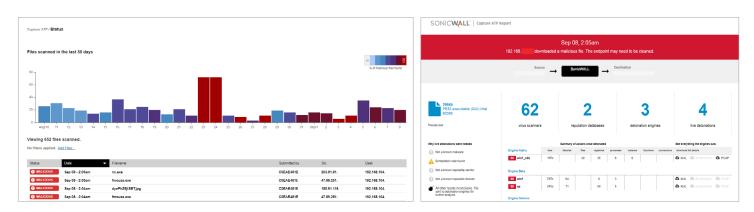
At the center of SonicWall's automated, real-time breach prevention are two advanced malware detection technologies; Capture Advanced Threat Protection™ (Capture ATP) and Capture Security appliance™ (CSa).

Capture ATP is a cloud-based multiengine sandbox platform, which includes Real-Time Deep Memory Inspection[™] (RTDMI), virtualized sandboxing, full system emulation and hypervisor level analysis technology. CSa is an onpremises device that features RTDMI, which utilizes memory-based static and dynamic techniques for fast and accurate verdicts. Both solutions extend advanced threat protection to detect and prevent zero-day threats in a variety of SonicWall solutions such as nextgeneration firewalls.

Suspicious files are sent to either solution where they are analyzed using deep learning algorithms with the option to hold them at the gateway until a verdict is determined. In the case of Capture ATP, when files are identified as malicious, they are blocked, and a hash is immediately created within the Capture ATP database for all customers to leverage to block follow-on attacks. These signatures are eventually sent to firewalls to create static defenses. Results generated by CSa are not shared outside your organization for privacy and compliance reasons.

These services analyze a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

For complete endpoint protection, the SonicWall Capture Client combines nextgeneration antivirus technology with SonicWall's cloud-based multi-engine sandbox with optional integration with SonicWall firewalls.



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 Analytics1 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 webbased interface.

Global management and reporting

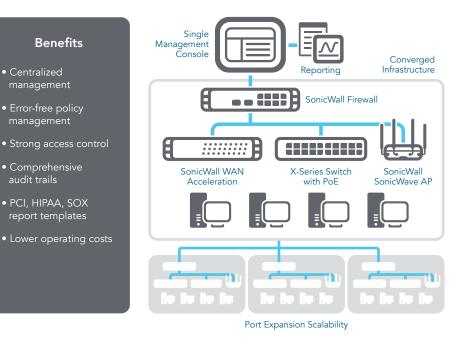
For highly regulated organizations wanting to achieve a fully coordinated security governance, compliance and risk management strategy, the optional SonicWall Global Management System¹ (GMS®) provides administrators a unified, secure and extensible platform to manage SonicWall firewalls, wireless access 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

Real-Time Monitor To configure, go to Appliton > Now Reporting. [Using Local Collector] 17:46:54 Sep 0 Refrecti even yr 🛐 👘 😣 Veni Rarc Local . 10 minutes **n** 63 20,000 Applications 2Port and 1Pv8 -All App 11.180. 10.0057 3.000 19 35 # Legenda General HTTPS MGM1 Microsoft Remote Chart Beat-3763 HTTP-5147 General Makaast Centre of DNS Service NTP 10000-1239 DoubleClick-6261 0212-122 Facebook-6/921 General HTTPS General HTTP Facebook-2822 Google-9379 DoubleCick-7900 DNS-4398 Eacebook 6363 Site Scout-7883 General SKE Image-4254 Image-4243 ENS-4395 -64uide-7023 Shockwave Flash (SWF)-575 HTTP-5148 YouTube-5727 TouTube-9055 Betr Ad-7871 Cothers YouTube-9256 Chart Beat-3767 Google Safe Goode Safe Adsafe Media-7910 MediaMath-7892 Goode-6015 DN5-6818 Advonar-7867 vice HTTPS Mercardt DD" Fed Service RPC Services (TANA) -CPS-5101 Service SMD Daing M service DCE EndPoint Aggregrate Knowledge-7907 Serving-Sys-7864 Seneral NET8005 DNS-5183 Soodle-6011

processes and service levels, dramatically simplifying lifecycle management of your overall security environments as

compared to managing on a device-bydevice basis.

SonicWall GMS Secure Compliance Enforcement



¹Requires added subscription

SONICWALL

audit trails

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 protoco 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			
RESTAPIS	Allows 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 NETW	/ORKING (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, oranch 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, b seamlessly re-routing traffic between endpoints through alternate routes.				
CONTENT/CONTEXT AW	ARENESS				
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 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. 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 TH	HREAT 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, JAF 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.				
Capture Client	Capture Client is a unified client platform that delivers multiple endpoint protection capabilities, including advanced malware protection and support for visibility into encrypted traffic. It leverages layered protection technologies, comprehensive reporting and endpoint protection enforcement.				
CAPTURE SECURITY AP	PLIANCE (CSa)				
Feature	Description				
Compliance-centered malware detection	Analyze suspicious files in your own environment without sending files or results to a third-party cloud.				
Built-in integrations	CSa supports out of the box integrations with other security solutions (firewalls and email security) from SonicWall.				
Near real-time protection	SonicWall's patented RTDMI technology helps detect malware quickly, even for previously unknown malware, that CSa can enable the block until verdict capability on SonicWall next-generation firewalls.				
Deployment	CSa can be configured on a private network directly connected to a singular edge firewall or be reachable over the Internet directly or using VPN by branch firewalls.				
ENCRYPTED THREAT PR	EVENTION ¹				
- eature	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.				
NTRUSION PREVENTION	N ¹				
- eature	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.				



Features

INTRUSION PREVENTIC	DN ¹ CONT'D
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 cove 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.

INREAL 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 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	ldentifies 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 CONTROL¹

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

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-SPYWARE¹

Feature	Description				
Multi-layered protection	tilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses ntering 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.				
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.				
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.				



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
- REST APIs

SSL/SSH decryption and inspection²

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

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
- Block until verdict
- Capture Client

Intrusion prevention²

- 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-malware²

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

¹ Not supported on SuperMassive 9800 ² Requires added subscription

9

Application identification²

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

Web content filtering²

- URL filtering
- Proxy avoidance
- Keyword blocking
- HTTP header insertion
- Bandwidth manage 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

- SonicWall wireless controller
- 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

- WIDS/WIPS
- RF spectrum analysis
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- Floor plan view/Topology view
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Guest cyclic quota
- LHM guest portal

Granular QoS control

• DPI for VoIP traffic

Logging

• Bandwidth management

Management and monitoring

• Cloud-based configuration backup

BlueCoat Security Analytics Platform

• SonicWall access point management

• Dell N-Series and X-Series switch

• Netflow/IPFix exporting

management¹

• H.323 gatekeeper and SIP proxy support

• GMS, Web, UI, CLI, REST APIs, SNMPv2/v3

VoIP

SuperMassive 9000 Series system specifications

OrganStatus	FIREWALL GENERAL	9200		9400	9600	9800	
AddBCD SPN, A	Operating system	SonicOS					
memory local sequence is called set and used set a	Security processing cores	24 32 64					
Bange14000000000000000000000000000000000000	Interfaces		4x10Gb	bE SFP+, 8x1GbE SFP, 8x1GbE, 1GbE Ma	anagement, 1 Console	4x10GbE SFP+, 12x1GbE SFP, 8x1GbE, 1GbE Management, 1 Console	
ImageImageImageStage80.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.000ImageAdvent manage Stage80.00080.00080.000Stage80.00080.00080.00080.00080.000Tead Present montage80.00080.00080.00080.00080.000Tead Present montage80.00080.00080.00080.00080.000Tead Present montage80.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage80.00080.00080.00080.00080.00080.000Stage<	Memory (RAM)		8 GB	16 GB	32 GB	64 GB	
MangenericCLUSHQUIDOTONDADAGE <thdadage< th=""><thd< td=""><td>Storage</td><td></td><td></td><td>Flash</td><td></td><td>2x 80GB SSD, Flash</td></thd<></thdadage<>	Storage			Flash		2x 80GB SSD, Flash	
SiQ on90.0090.0090.0090.0090.00Harman consumptionAdvancements and substrational substratin substrational substrational substrational subs	Expansion			1 expans	ion slot (rear)*, SD card*		
Material121.LingpingAbove: Long Journey Algo SeriesHigh and LingpingAlgo Series Algo Algo SeriesHigh and LingpingAlgo SeriesHigh and LingpingAlgo SeriesAnd Mander Series Algo SeriesAlgo SeriesHigh and LingpingAlgo SeriesAnd Mander Series Algo SeriesAlgo SeriesAlgo Series Algo Series Algo Series Algo SeriesAlgo SeriesAlgo Series Algo Series Algo Series Algo SeriesAlgo SeriesAlgo Series Algo Series Algo Series Algo Series Algo SeriesAlgo SeriesAlgo Serie	Management			CI	LI, SSH, GUI, GMS		
Larger of the starting of the	SSO users		80,000	90,000	100,000	110,000	
Higher discription of the intervalue of the inter	Maximum access points supported			128		-	
index decision from space of the stage o	Logging			Analy	zer, Local Log, Syslog		
investion transplayed14 Bage24 Bage24 Bage14 BageBracker breaction transplayed36 Gags44 Bage45 Gags13 Gags23 GagsPS denotion transcription transplayed36 Gags10 Gags13 Gags23 Gags23 GagsPS denotion transcription transplayed36 Gags10 Gags35 Gags35 Gags35 GagsMIX transplayed46 Gags10 Gags13 Gags35 Gags35 GagsMIX transplayed60 Gags10 Gags13 Gags35 Gags35 GagsVirth transplayed50 Gags10 Gags10 Gags32 Gags35 GagsVirth transplayed50 Gags10 Gags10 Gags36 Gags36 GagsVirth transplayed10 Gags10 Gags10 Gags36 Gags36 GagsVirth transplayed10 Gags10 Gags20 Gags36 Gags36 GagsVirth transplayed200 Gags200 Gags200 Gags36 Gags36 GagsVirth transplayed200 Gags200 Gags200 Gags36 GagsVirth transplayed200 Gags200 Gags200 Gags36 GagsVirth transplayed200 Gags200 Gags36 Gags36 GagsVirth transplaye	High availability			Active/Passive with State	Sync, Active/Active DPI with State Sy	nc	
Incar Anomport3 Gings4.4 Gings4.4 Gings4.1 Gings4.0 GingsAlpelatoin lengedout throughout5 Gings4.0 Gings1.1 S Gings2.1 G GingsMich Khroughout3.2 Gings4.6 Gings5.6 Gings3.6 Gings3.6 GingsSill Khroughout1.0 Gings2.0 Gings3.6 Gings3.6 Gings3.6 GingsWith Khroughout5.0 Gings1.0 Gings2.0 Gings3.6 Gings3.6 GingsWith Khroughout1.0 Gings2.0 Gings1.1 G Ging5.6 GingsWith Khroughout5.0 Gings1.0 Gings1.0 Gings3.6 GingsWith Khroughout5.0 Gings1.0 Gings1.0 Gings2.0 MolessWith Khroughout5.0 Gings1.0 Gings3.0 Gings3.6 GingsWith Khroughout5.0 Gings1.0 Gings3.0 Gings3.0 GingsWith Khroughout5.0 Gings1.0 Gings3.0 Gings3.0 GingsWith Khroughout1.0 Gings2.0 Gings3.0 Gings3.0 GingsWith Khroughout2.00 Gings2.0 Gings3.0 Gings3.0 GingsWith Khroughout2.0 Gings2.0 Gings3.0 Gings3.0 GingsStar Vith Khroughout	FIREWALL/VPN PERFORMANCE	9200		9400	9600	9800	
Appleading15 Gaps10 Gaps11 Gaps12 Gaps108 throughput5.61gs1.6 Gaps1.6 Gaps1.6 Gaps108 throughput3.6 Gaps5.6 Gaps5.6 Gaps3.6 Gaps20. Gaps2.0 Gaps2.0 Gaps3.6 Gaps20. Gaps1.0 Gaps2.0 Gaps3.6 Gaps20. Gaps1.0 Gaps2.0 Gaps3.6 Gaps20. Gaps1.0 Gaps2.0 Gaps3.6 Gaps20. Gaps1.0 Gaps1.0 Gaps1.0 Gaps20. Gaps1.0 Gaps1.0 Gaps2.00 Gaps20. Gaps1.0 Gaps1.0 Gaps2.00 Gaps20. Gaps2.00 Gaps2.00 Gaps2.00 Gaps20. Gaps2.00 Gaps2.00 Gaps2.00 Gaps20. Gaps2.00 Gaps2.00 Gaps2.00 Gaps20. Gaps2.00 Gaps2.00 Gaps2.00 Gaps20.0 Gaps2.00 Gaps2.00 Gaps2.00 Gaps	Firewall Inspection throughput ¹		15 Gbps	20 Gbps	20 Gbps	31.8 Gbps	
Pick may beam5 Gas10 Gas11 Gap11 GapArt Monogloup4.4 Gas5.5 Gas5.6 Gas7.3 GasSD, segment and decryption throughed1.0 Gas2.0 Gas2.0 Gas7.3 GasMV Monogloup5.6 Gas1.0 Gas1.0 Gas7.3 GasConnectioner per second1.00 Gooles1.00 Gooles1.00 Gooles1.00 GoolesMonom connectione (PP)5.5 Gas1.00 Gooles1.00 Gooles2.00 GasMonom connectione (PP)5.5 Gas1.00 Gooles0.00 Gooles2.00 GoolesState (PM) function5.00 Gooles0.00 Gooles2.00 Gooles5.00 GoolesState (PM) function2.00 Gooles2.00 Gooles2.00 Gooles5.00 GoolesState (PM) function2.00 Gooles5.00 Gooles5.00 Gooles5.00 GoolesState (PM) function3.00 Gooles5.00 Gooles5.00 Gooles5.00 GoolesState (PM) function3.00 Gooles5.00 Gooles5.00 Gooles5.00 GoolesState (PM) function3.00 Gooles5.00 Gooles5.00 Gooles5.00 Gooles <t< td=""><td>Threat Prevention throughput²</td><td></td><td>3 Gbps</td><td>4.4 Gbps</td><td>4.5 Gbps</td><td>10.5 Gbps</td></t<>	Threat Prevention throughput ²		3 Gbps	4.4 Gbps	4.5 Gbps	10.5 Gbps	
Anil Alora inspictor throughput12.6 logs4.5 Gaps10.6 caps10.6 caps10.6 caps10.6 caps10.6 caps2.0 caps3.6 capsMY Ntroughput5.6 Gaps10.6 Gaps10.8 Gaps1.8.6 Gaps4.4.3 Gaps4.4.3 GapsVM Ntroughput5.6 Gaps10.8 Gaps1.8.6 Gaps2.20.8 Gaps2.20.8 Gaps2.20.8 GapsSintame constructions per second10.0 Gaps1.0.0 Gaps1.9.0 Gaps2.20.8 Gaps2.20.8 Gaps2.20.8 GapsMaximum constructions [DP]5.6 Ma1.5 M3.0.0 Gaps3.0.0 Gaps <td>Application Inspection throughput²</td> <td></td> <td>5 Gbps</td> <td>10 Gbps</td> <td>11.5 Gbps</td> <td>23 Gbps</td>	Application Inspection throughput ²		5 Gbps	10 Gbps	11.5 Gbps	23 Gbps	
INIX monopoint4.4 Gegs5.5 Gegs5.4 Gegs7.3 GegsCPUNDroughout0.6 Gegs1.0 Gegs1.0 Gegs1.0 Gegs1.0 GegsVENDroughout5.0 Gegs1.00 GODec1.00 GODec1.00 GODec2.00 GODec2.00 GODecMainum concectione (PP)5.0 M2.0 M2.0 M0.0 GOD0.0 GODEMainum concectione (PP)5.0 M0.00 GODE0.00 GODE	IPS throughput ²		5 Gbps	10 Gbps	11.5 Gbps	21.3 Gbps	
Skl agestion and servython throughput (10 Gkps)1.0 Gkps2.0 Gkps3.3 GkpsVPN throughput'6 Gkps100 Okps11.5 Okps11.4 SkpsCamestines processor100 000/loce130 000/loce220 00/locMainum contection (SPI)5.0M7.5M1.0M2.0MDirSt convectioner (Mainum)0.000 17.5001.2000 (2.0C)65.000DirSt convectioner (Mainum)2.000 (10.0002.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (0.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (0.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (10.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (0.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (0.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (0.000)2.000 (0.000)2.000 (0.000)DirSt convectioner (Mainum)2.000 (Mainum)2.000	Anti-Malware Inspection throughput ¹		3.5 Gbps	4.5 Gbps	5.0 Gbps	11 Gbps	
ign sgr) of all of all all all all all all all all all al	IMIX throughput		4.4 Gbps	5.5 Gbps	5.5 Gbps	7.3 Gbps	
Connotections per seand1000/hec130.000/sec12.00.00 (2.500)20.00Maximum connections (DP)1.5M1.5M2.0M6.0MDPI SSC connections' (Maximu)8.000 (15.00')12.000 (2.500')65.000DPI SSC connections' (Maximu)0.000 (15.00')12.000 (2.500')65.000Ster SSE VPM Tunnols10.0002.000 (10.00')50.00 (10.00')SSC VPM Standard (dents (Maximu)2.000 (4.00)2.000 (10.00')50.00 (10.00')SSC VPM Standard (dents (Maximu)2.000 (10.00')50.00 (10.00')50.00 (10.00')SSC VPM Standard (Dents (Maximu)SSC VPM Standard (Dents (Maximu)50.00 (10.00')50.00 (10.00')SSC VPM Standard (Dents (Maximu)SSC VPM S			1.0 Gbps	2.0 Gbps	2.0 Gbps	3.5 Gbps	
Maximu connections (DF)5.047.5410.042.004Maximu connections (DF)0.000 (15500*)0.000 (15500*)0.000 (15500*)DFS3C concelors (Maximu)0.000 (15500*)0.000 (1550*)0.000 (1550*)SIA VFN Met Ander Cinets (Maximu)2.000 (4.000)2.000 (4.000)0.000 (150*)SSA VFN Met Ander Cinets (Maximu)2.000 (4.000)2.000 (4.000)0.000 (4.000)SSA VFN Met Ander Cinets (Maximu)2.000 (4.000)0.000 (4.000)0.000 (4.000)SSA VFN Met Ander Cinets (Maximu)2.000 (4.000)0.000 (4.000)0.000 (4.000)Nationarisa satigationed (4.000)SSA VFN Met Ander Cinets (4.000)0.000 (4.000)SSA VFN Met Ander Cinets (Maximu)2.000 (4.000)0.000 (4.000)0.000 (4.000)SA VFN Met Ander Cinets (4.000)SSA VFN Met Ander Cinets (4.000)0.000 (4.000)SA VFN Met Ander Cinets (4.000)SSA VFN Met Ander Cinets (4.000)0.000 (4.000)SA VFN Met Ander Cinets (4.000)SSA VFN Met Ander Cinets (4.000)0.000 (4.000)SA VFN Met Ander Cinets (4.000)SSA VFN Met Ander Cinets (4.000)0.000 (4.000) <td>VPN throughput³</td> <td></td> <td>5 Gbps</td> <td>10 Gbps</td> <td>11.5 Gbps</td> <td>14.3 Gbps</td>	VPN throughput ³		5 Gbps	10 Gbps	11.5 Gbps	14.3 Gbps	
Maximum cannections (DP)1.5M2.0M8.0MDP SSL connections (Maximum)8.000 (15500')1.0.000 (1560')98009800State-sids VPM Funnels1.0.0002.000 (10.000)2.000 (10.000)State-sids VPM Funnels2.000 (10.000)0.10.00050.10.000SSL VPN Netfletheder Felents (Maximum)2.000 (10.000)50.10.00050.10.000Encryption/unthentication0.12.0002.000 (10.000)50.10.000Encryption/unthentication0.12.00050.10.00050.10.000Encryption/unthentication0.12.0009.009.00Encryption/unthentication9.009.009.00Encryption/unthentication9.009.009.00Parker Satis, DHCP, PEPSE, LT and PTP 10 elem, Internal DHCP server-DHCP relationNationasci Satis, DHCP, PEPSE, LT and PTP 10 elem, Internal DHCP server-DHCP relationVLAN interfaces512Satis, DHCP, PEPSE, RIP-11/2, state frontice, policy-based routing, muticastVLAN interfacesGEPC PEPK, RIP-11/2, state frontice, policy-base	Connections per second		100,000/sec	130,000/sec	130,000/sec	229,000/sec	
DPI SSL connections' (Maximum) 8.000 (15.500') 9.00 9.00 VPN 9200 9400 960 960 Stete-Site VPN Tronles 10.000 2.000 (0.000) 2.000 (0.000) Stete-Site VPN Tronles 2.000 (0.000) 2.000 (0.000) 50 (3.000) Stete-Site VPN Toroles 0.03.000 50 (3.000) 50 (3.000) Enzyteen/attentication DES, 3DES, AES (128, 139, 256-bit)/MDS, SHA-11.Suite B. Common Access Card (CAC) Key exchange Neuto-based VPN 0.050 960	Maximum connections (SPI)		5.0M	7.5M	10.0M	20.0M	
VPN9200940096009800Site-VN Tunnels1.0000.0000 (.000).0000 (.000)Site-VN NetExtender clients (Maximum)2 (.000).000 (.000).000 (.000)Site-VN NetExtender clients (Maximum)2 (.000).000 (.000).000 (.000)Key exchange.0158.302.56.56.103.10.84.1.5.048.6.Common Access Carl (.CCERout-seady VPN.000.000.000IP adress: assignment.011.man; flexible NCIP petpet [.1.5.1.4/-NetTwodSKN.000.000.000IP adress: assignment.011.man; flexible NCIP petpet [.011P and PETP allert, Iteman DHCP surver, DHCP IssignmentNAT modes.11.man; flexible NCIP and PETP allert, Iteman Surver, DHCP IssignmentVALVI interfaces.012.012Authentication.012 (.000).000Op addition forthy max bandwidth pointy max bandwidth pointy maxime to mutations, SUMM PHRADUS, SSO, Newell, Intermal Services; Chirls'VALVI interfaces.012 (.000).000Op addition forthy, max bandwidth pointy, max bandwidth pointy, maxime to mutations, SUMM PHRADUS, SSO, Newell, Intermal Services; Chirls'VALVI interfaces.012 (.000).000Op addition forthy, max bandwidth, pointy,	Maximum connections (DPI)		1.5M	1.5M	2.0M	8.0M	
Stet-o-Site VPN Tunnels 10,000 2,000 (4,000) IPSec VPN clients (Maximum) 2,000 (4,000) 2,000 (4,000) 50 (3,000) 50 (3,000) Excryption/Juthentication DES, 3DES, AES (128, 192, 295 (-bit)/MDS, SHA-1, Suite B, Common Access Card (CAC) Key exchange Route-based VPN TIRP CSPF Recess Card (CAC) Second Card (CAC) Networksed VPN RULE OSSPC Second Card (CAC) Second Card (CAC) NAT modes Static, DHCP, PPP6, [, 127P and PPT (ellert, Internal DHCP server, DHCP relay' NAT modes Second Card (CAC) NAT modes Second ChCP, PPP6, [, 127P and PPT (ellert, Internal DHCP server, DHCP relay' NAT modes Second Card (CAC) NAT modes Second ChCP, PPP6, [, 127P and PPT (ellert, Internal DHCP server, DHCP relay' NAT modes Second Card (CAC) VLA Interfaces Second ChCP, PPP6, [, 127P, and VCP, Second Tuning, multicast Second Card (CAC) Second Card (CAC) VLA Interfaces Second ChCP, PPP6, [, 127P, And VC, Second Card (CAC) Second C	DPI SSL connections ⁶ (Maximum)		8,000 (15,500°)	10,000 (17,500 ⁶)	12,000 (22,500 ⁶)	650,000	
PBec VPN clients (Maximum) 2.000 (4.000) 2.000 (6.000) 50 (3.000) SSL VPN NetExtender clients (Maximum) 2 (3.000) 50 (3.000) 50 (3.000) SSL VPN NetExtender clients (Maximum) 2 (3.000) 50 (3.000) 50 (3.000) Sex personalization correspin 2, 25, 51-k1, Suble B, Corromon Access Carel (JCC) Exerced and Groups 1, 2, 5, 14* Route-soad VPN TB 0, 50P Bed 0 960 960 PETWORKTOK 200 9400 960 960 960 NAT modes 11, manyn, 1, ismayn, Robide NPTP clein, Intermal DPCP server, DPCP relax* F VAX Interfaces BEQ PO SPF, RIV 1/4X, satarated andwidth, DPCP predux* F VAX Interfaces EBQP (SPF, RIV 1/4X, satarated bandwidth, DSCP maxing, BG2, 14 C VAX Interfaces LDAP (mdt-4onnalins, XAUTH/RADUS, SSS, Novel, Internal user database, Terminal Services*, Clittl* C VADP EBQP (SPF, RIV 1/4X, satarated bandwidth, DSCP PPRE, LIZP, PETP RADUS, EEEG (SAUTH/RADUS, SSS, Novel, Internal user database, Terminal Services*, Clittl* Solon Nove VADPI (ClickA Interprise Firewall, IPVS Phase, VPNC, VPAT, FIPS 140-2', Common Criteria NDPP', ICSA Anti-Virus* Solon Nove Standards TCPIRI (PMP, HTPH	VPN	9200		9400	9600	9800	
SSL VPN NeEExtender cellents (Maximum) 2 (3.000) 2 (3.000) 5 (3.000) 5 (3.000) Encryption/authentication DESS.DES.AES (122, 122, 252-bit/LBUB, SSL 46, LGummo Access Card (CAC) Key exchange DIffe Hellman Compas 12, 5, 14 - Rote-based VPN IRP.OSPF Rev Compas 12, 5, 14 - NetTWORKING 200 960 960 960 960 Paddress assignment Static, DEIPOPE, 12TP and PPPU (ethin, Internal DPUP, NPAT, transparent mode - - VLAN Inderfaces SERO.SPF.RP1/L/2, static routers, policy-based routing, multicasticas, policy-based routing, multicasticas, policy-based routing, multicasticas, policy-based routers, policy-based routing, multicasticas, policy-based routing, MAXIPHADOLUS, SSO, Novell, Internal user database. Terminal Services', CINIX ² Authoritación DAP (multi-denamis), XAUTHADOLUS, SSO, Novell, Internal user database. Terminal Services', CINIX ² Stadards TCPIPI/PLOP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNR, DMCP, PPPeE, L2TP, PTP, RADIUS, IEEE 802.3 Certifications UC APL* (CSA Enterprise Firewail, IPNA PP) Sonow News supply Dual, redundant, hot-swappabel Sonow Fars Dual, redundant, hot-swappabel Sonow Sonow Sonow Sonow Sonow Fars Dual, redundan	Site-to-Site VPN Tunnels			10,000		25,000	
Encryption/authentication DES, SDES, AES (128, 192, 256-bit)/MDS, SHA-1, Suite B, Common Access Card (CAC) Key exchange DIffer Hellman Groups 1, 2, 5, 14' Nour-based VPN SIR, OSF NETWORKING 9200 9600 9800 IP address assignment Static, DHCP, PPPC, LIZT and PPTP client, internal DHCP server, DHCP relav' NAT modes 1:1, many, 1:many, fiexible NAT (overlapping IP3), PAT, transparent mode VLAN Interface SIGP, OSPF, RIP/VIA', static routes, policy- based routing, multicast QoS Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1 Authentication CDEP/IPIC, ILTT PROFE, ILTT PROFE, IST PROFE,	IPSec VPN clients (Maximum)		2,000 (4,000)	2,000 (6,000)		2,000 (10,000)	
Key exchange Diffie Hellman Groups 1, 2, 5, 14/ Route-based VPN FIRP, OSF NETWORKNG 900 900 IP address assignment Static, DHCP, PPP6E, L2TP and PPTP client, Internal DHCP server, DHCP relay NAT modes 1:1, manr, 1: manr, Link, DHCP, Nerver, DHCP relay VAD interfaces 522 Routing protocols BGP, OSPF, RIPV1/V2, static routes, policy-based routing, multicast QS Bandwidth priorthy, max Mandwidth, guaranteed bandwidth, BSCP, marking, BO21 Authentication LDAP (multi-domains), XAUTH/RADUS, SSO, Novell, internal user database, Terminal Services', Citrix' Valv ILDAP (multi-thermal, IPV6 Phase, Z, VPNC, VPAT, FIPS 10-2; Common Criteria NPPP, ICSA Anti-Virus' Valve 500 900	SSL VPN NetExtender clients (Maximum)		2 (3,000)	2 (3,000)	50 (3,000)	50 (3,000)	
Rute-based VPN RIP, OSPF NET work NKG 9200 9600 9800 Pa dross assignment State, DHCP, PPp6, L2P1 and PPPT cleant, internal DHCP server, DHCP relay* NAT modes 1:many,: f.umany, f.ubrana NAT (work apping 16%), PAT, transparent DHCP relay* NAT modes 512 Routing protocols BGP, OSPF, RIP-VI/V2, static routes, policy-based notwidth, DSCP marking, B021p Authentication LDAP (multi-domains), XAUTH/RADUS, SSO, Novell, internal user database, Terminal Services*, Citrix* Standards CTP/IPI, TIPI, SPEs, ISAK-MIKKE, SNIP, DHCP, PPFD, L2TP, PEPT, RADUS, IEEE B02.3 Certifications UC API, 'LCSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2'. Common Criteria NDPP', ICSA Anti-Vrus* Standards CTP/IPI, IPI, SPEs, ISAK-MIKKE, SNIP, DHCP, PPFD, L2TP, PEPT, RADUS, IEEE B02.3 Certifications UC API, 'LCSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2'. Common Criteria NDPP', ICSA Anti-Vrus* HARDWARE 9200 9800 9800 Power supply Dual, redundant, hot-swappable, 300 W 9801 9801 Ipit power 100-240 VAC, 50-60 Hz 100-41 9801 9801 Ipit power 100-240 VAC, 50-60 Hz 100-42 <t< td=""><td>Encryption/authentication</td><td></td><td></td><td>DES, 3DES, AES (128, 192, 256-bit</td><td>/MD5, SHA-1, Suite B, Common Acces</td><td>s Card (CAC)</td></t<>	Encryption/authentication			DES, 3DES, AES (128, 192, 256-bit	/MD5, SHA-1, Suite B, Common Acces	s Card (CAC)	
NEWORKING 9200 9400 9600 9800 IP addres assignment Static, DHCP, PIPP, L2TP, and PIPT e linet, internal DHCP server, DHCP relay' NAT modes 1:1, many, 1, imany, 1, Rubik 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), XAUTHRADUS, SSO, Novell, internal user database, Terminal Socies*, Citra' VoP CETFILITY Standards TCP/IPI, ICMP, HTTP, HTTPS, IPSec, ISAKMPI/KE, SNMP, DHCP, PPDE, L2TP, PPTP, RADIUS, IEE 802.3 Certifications UC APL*, ICSA Enterprise Frevail, IPS 40-2*, Common Criteria NDPP', ICSA Anti-Virus* HABDWARE 9200 960 960 Power supply Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W S00 W Fars Dual, redundant, hot-swappable, 300 W S00 W S00 W Marimu power consumption (W) 2153 21.43 21.43 21.43 MBF @25°C in hours 186,719 120.44 14.40	Key exchange			Diffie He	llman Groups 1, 2, 5, 14v		
IP address assignment Static, DHCP, PPPoE, L2TP and PPTP client, internal DHCP server, DHCP relay' NAT modes 1:1, many, flexible NAT (overlapping IPs), PAT, transparent mode VLAN interfaces 512 Routing protocols BGP, OSPF, RIPV1/A2, static routes, policy-based routing, multicast QoS Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p Authentication LDAP (multi-domaing, XAUTHARDIUS, SSO, Novell, internal user database, Terminal Services*, Citrix* Stadards TCPI/P, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPP6, L2TP, PPTP, RADIUS, IEEE 802.3 Certifications UC APL*, ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2*, Common Criteria NDPP*, ICSA Anti-Virus* HARDWARE 9200 9400 9800 9800 Power supply Dual, redundant, hot-swappable 501 multi-redundant, hot-swappable 501 multi-redundant, hot-swappable Display Front LED display 100-240 VAC, 50-60 Hz 500 multi-redundant, 500 multi-redund	Route-based VPN				RIP, OSPF		
NAT model 1:1, many: 1, 1:many: flexible NAT (overlapping IPs), PAT, transparent mode VLAN interfaces 512 Routing protocols BGP, OSPF, RIV-1/V2, static routes, policy-based routing, multicast QoS Bandhwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p Authentication LDAP (multi-domains), XAUTH/RADIUS, SSO, Noveli, internal user database, Terminal Services*, Clitrik* VolP Full H323-v1-5, SIP Standards TCP/IPI (CNP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPe, L2TP, PTP, RADIUS, IEEE 802.3 Certifications UC APL*, ICSA Enterprises Freewall, IPV6 Phase, ZVPR, CVPAT, FIPS 140-2*, Commo Criteria NDPP*, ICSA Anti-Vrus* HARDWARE 9200 9400 9600 9800 Power supply Dual, redundant, hot-swappable, 300 W Dual redundant, hot-swappable, 500 W Dual redundant, hot-swappable Input power 1000 200 350 350 350 Marine power consumption (W) 200 350 350 350 350 350 MTBF @25°C in hours 188.719 187.702 186.451 126.144 360 360 Dimension 17.324.324.55.45.65.45.cfm 127.8	NETWORKING	9200		9400	9600	9800	
VLAN interfaces 512 Routing protocols BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast QoS Bandwidth priority, max bandwidts, guaranteed bandwidth, DSCP marking, 802.1p Authentication LDAP (multi-domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services ⁵ , Citrix ³ VoIP Full H323-v1-5, SIP Standards TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMPI/KE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 Certifications UC APL ¹ , ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2 ⁴ , Common Criteria NDPP ¹ , ICSA Anti-Virus ⁴ HARDWARE 9200 9600 9600 Power supply Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W S00 W Fans Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W S00 W S00 W Input power 100-240 VAC, 50-60 Hz Input power S00 S00 MTBF @25°C in hours 188,719 187,702 186,451 126,144 MTBF @25°C in hours 188,719 147,702 186,451 126,144 Dimensions 17,19,11,175 in (43,344,85,45,65) 17,24,43,5 in (9,600,43 cm) 14,400 <td< td=""><td>IP address assignment</td><td></td><td></td><td>Static, DHCP, PPPoE, L2TP and</td><td>PPTP client, internal DHCP server, DH</td><td>CP relay⁴</td></td<>	IP address assignment			Static, DHCP, PPPoE, L2TP and	PPTP client, internal DHCP server, DH	CP relay ⁴	
Routing protocols BGP, OSPF, RIPV1/v2, static routes, policy-based routing, multicast QoS Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p Authen functication LDAP (multi-domains), KXUTH/RADIUS, SSO, Novell, internal user database, Terminal Services ⁶ , Citrix ⁴ VolP Full H323-v1-5, SIP Standards TCP/IP, ICMP, HTTP, IPTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPOE, LZTP, PPTP, RADIUS, IEEE 802.3 Certifications UC APL ¹ , ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2 ¹ , Common Criteria NDPP ⁴ , ICSA Anti-Virus ⁴ HADWARE 920 940 960 980 Power supply Dual, redundant, hot-swapable, 300 W Dual, redundant, hot-swapable, 300 W S00	NAT modes			1:1, many:1, 1:many, flexible N	NAT (overlapping IPs), PAT, transparent	mode	
QoS Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p Authentication LDAP (multi-domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services [*] , Citrix ⁹ VolP Full H323-v1-5, SIP Standards TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PTPT, RADIUS, IEEE 802.3 Certifications UC APL ⁴ (SCA Entreprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2 ⁴ , Common Criteria NDPPP, ICSA Anti-Virus ⁴ HARDWARE 9200 9400 9600 980 Power supply Dual, redundant, hot-swappable, 300 W S000 Photomath Fans Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W S00 W Fans Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W S00 W S00 W Maximu power consumption (W) 200 S00 W <	VLAN interfaces				512		
Authentication LDAP (multi-domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services ⁸ , Citrix ⁴ VolP 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 Frewall, 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 Dual, redundant, hot-swappable Fins Dual, redundant, hot-swappable Stopping Stopping Stopping Maximum power consumption (W) 200 350 Stopping Stopping Stopping Form factor 1U rack-mountable 2U rack-mountable 2U rack-mountable 2U rack-mountable 2U rack-mountable Displat 17x19.1x175 in (43.3x48.5x4.5 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) MTBF @25*C in years 21.53 21.43 21.28 40.5 Ib (18.3 kg) 40.	Routing protocols			BGP, OSPF, RIPv1/v2, sta	tic routes, policy-based routing, multic	ast	
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, 300 W Standards Fans Dual, redundant, hot-swappable, 300 W Standards Standards Maximum power consumption (W) 200 350 350 Matife Q25°C in hours 188,719 187,702 186,451 126,144 Dimensions 117243.3 x145.54.5 cm) 1724243.5 in (936043 cm) WEEE weight 213 di 13.3 x345.54.5 cm) 1724243.5 in (936043 cm) WEEE weight 233 bi [13.3 kg) 651 b(23.4 kg) 49.5 bi [23.4 kg) Shipping weight 29.3 bi [13.3 kg) 51.6 (36.4 kg) 40.5 bi [23.4 kg] Shipping weight 29.3 bi [13.3 kg) 651 b(23.4 kg) 40.5 bi [23.4 kg] Shipping weight 29.3 bi [13.3 kg) 651 b(23.6 kg) 40.5 bi [23.4 kg]	QoS			Bandwidth priority, max bandwid	th, guaranteed bandwidth, DSCP marki	ng, 802.1p	
Standards TCP/IP, ICMP, HTTP,, IPTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPE, L2TP, PPTP, RADIUS, IEEE 802.3 Certifications UC APL ¹ , ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2 ⁴ , Common Criteria NDPP ¹ , ICSA Anti-Virus ⁴ HARDWARE 9200 9400 9600 9800 Power supply Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 500 W Fans Dual, redundant, hot-swappable Torn LED display Input power Input power 100-240 VAC, 50-60 Hz S00 W 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 Dimensions 17x19x11/5 in (43,3x48,5x45 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) Weight 23.b (10.4 kg) 40.5 b (12.8 kg) 40.5 b (12.8 kg) 40.5 b (12.8 kg) Shipping weight 23.b (10.4 kg) 23.b (10.4 kg) 45.5 b (22.4 kg) 55.5 b (22.4 kg) 55.5 b (22.4 kg) Shipping weight 29.3 b (13.3 kg) FCC Class A, ICES Class A, CEE (EMC, LVD, ROHS), CTICk, VCCI Class A, UL/CUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSM, KCC/MSIP, ANATEL	Authentication		LDA	AP (multi-domains), XAUTH/RADIUS, SS	60, Novell, internal user database, Term	inal Services ⁵ , Citrix ⁵	
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, 300 W Dual, redundant, hot-swappable, 500 W Fans Display Front LED display Input power 350 Input power 100-240 VAC, 50-60 Hz 350 350 MARIF @25°C in hours 188,719 187,702 186,451 126,144 MTBF @25°C in hours 188,719 127,23 21,28 14,40 Obmensions 17x19,11,751 rig (43,3x48,5x4.5 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) Weight 23 lb (10,4 kg) 40.5 lb (E2,4 kg) 40.5 lb (E2,4 kg) 40.5 lb (E2,4 kg) 40.5 lb (E2,4 kg) Shipping weight 29.3 lb (13,3 kg) 65 lb (22,6 kg) 65 lb (22,6 kg) 65 lb (22,6 kg) Maior regulatory FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	VoIP			Fu	III H323-v1-5, SIP		
HARDWARE 9200 9400 9600 9800 Power supply Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 300 W Soo W So	Standards		TCP/	IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP,	/IKE, SNMP, DHCP, PPP₀E, L2TP, PPTF	, RADIUS, IEEE 802.3	
Power supply Dual, redundant, hot-swappable, 300 W Dual, redundant, hot-swappable, 500 W Fans Dual, redundant, hot-swappable 500 W Display Front LED display 100-240 VAC, 50-60 Hz 100-240 VAC, 50-60 Hz 100-240 VAC, 50-60 Hz 350 Maximup power consumption (W) 200 350 350 350 MTBF @25°C in years 186,719 186,451 126,144 MTBF @25°C in years 21.53 21.43 21.28 14.40 Form factor 10 rack-mountable 20 rack-mountable 20 rack-mountable 20 rack-mountable 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) 10 rack-mountable 20 rack-mountable 23 lb (10.4 kg) 49.5 lb (22.4 kg) 49.5 lb (23.4 kg) 49.5	Certifications		UC APL ⁴ , IC	SA Enterprise Firewall, IPV6 Phase 2, VI	PNC, VPAT, FIPS 140-2 ⁴ , Common Crite	eria NDPP ⁴ , ICSA Anti-Virus ⁴	
Proven suppy Dual, redundant, not-swappable, sol W 500 W Fans Dual, redundant, hot-swappable Display Front LED display Input power 100-240 VAC, 50-60 Hz Maximum power consumption (W) 200 MTBF @25°C in hours 188,719 1RBF @25°C in years 21.53 21.43 21.28 10rack-mountable 2U rack-mountable Dimensions 17x19.1x1.75 in (43.3x48.5x4.5 cm) VietEE weight 23.1b (10.4 kg) Shipping weight 23.3 b (13.3 kg) MSEE weight 55.b (29.64 kg) Major regulatory FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	HARDWARE	9200		9400	9600	9800	
Display Front LED display Input power 100-240 VAC, 50-60 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 2U rack-mountable Dimensions 17x19.1x1.75 in (43.3x48.5x4.5 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) Weight 618.1 lb (8.2 kg) 40.5 lb (18.3 kg) 40.5 lb (18.3 kg) VEEE weight 23 lb (10.4 kg) 49.5 lb (22.4 kg) 65 lb (29.64 kg) Shipping weight 29.3 lb (13.3 kg) 65 lb (29.64 kg) 65 lb (29.64 kg) Major regulatory FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	Power supply			Dual, redundant, hot-swappable,	300 W	Dual, redundant, hot-swappable, 500 W	
Input power 100-240 VAC, 50-60 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 2U rack-mountable Dimensions 17x19.1x1.75 in (43.3x48.5x4.5 cm) 17x24x3.5 in (9x60x43 cm) Weight Weight 18.1 lb (8.2 kg) 40.5 lb (18.3 kg) Weight Shipping weight 29.3 lb (13.3 kg) 65 lb (29.64 kg) MIST (9x60x45 CC) Major regulatory FCC Class A, CEC (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment	Fans			Dual, red	dundant, hot-swappable		
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 2U rack-mountable Dimensions 17x19.1x1.75 in (43.3x48.5x4.5 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) Weight 18.1 lb (8.2 kg) 40.5 lb (18.38 kg) 40.5 lb (18.38 kg) WEEE weight 23 lb (10.4 kg) 49.5 lb (22.4 kg) 51bipping weight Shipping weight 29.3 lb (13.3 kg) 65 lb (29.64 kg) 65 lb (29.64 kg) Major regulatory FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	Display			F	ront LED display		
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 2U rack-mountable Dimensions 17x19.1x1.75 in (43.3x48.5x4.5 cm) 17x24x3.5 in (9x60x43 cm) 17x24x3.5 in (9x60x43 cm) Weight 18.1 lb (8.2 kg) 40.5 lb (18.38 kg) 40.5 lb (18.38 kg) WEEE weight 23 lb (10.4 kg) 49.5 lb (22.4 kg) 51b(22.4 kg) Shipping weight 29.3 lb (13.3 kg) 65 lb (29.64 kg) 65 lb (29.64 kg) Major regulatory FCC Class A, ICE SC lass A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment	Input power	100-240 VAC, 50-60 Hz					
MTBF @25°C in years 21.53 21.43 21.28 14.40 Form factor 1U rack-mountable 2U rack-mountable 2U rack-mountable 2U rack-mountable 2U rack-mountable 2U rack-mountable 2U rack-mountable 20 rack-mountable	Maximum power consumption (W)			200		350	
Form factorU rack-mountable2U rack-mountableDimensions17x19.1x1.75 in (43.3x48.5x4.5 cm)17x24x3.5 in (9x60x43 cm)Weight18.1 lb (8.2 kg)40.5 lb (18.38 kg)WEEE weight23 lb (10.4 kg)49.5 lb (22.4 kg)Shipping weight29.3 lb (13.3 kg)65 lb (29.64 kg)Major regulatoryFCC Class A, ICE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATELEnvironment15-40 deg C	MTBF @25°C in hours		188,719	187,702	186,451	126,144	
Dimensions17x19.1x1.75 in (43.3x48.5x4.5 cm)17x24x3.5 in (9x60x43 cm)Weight18.1 lb (8.2 kg)40.5 lb (18.38 kg)WEEE weight23 lb (10.4 kg)49.5 lb (22.4 kg)Shipping weight29.3 lb (13.3 kg)65 lb (29.64 kg)Major regulatoryFCC Class A, ICE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATELEnvironment15-40 deg C	MTBF @25°C in years		21.53	21.43	21.28	14.40	
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, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico Coc by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	Form factor			1U rack-mountable		2U rack-mountable	
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, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	Dimensions			17x19.1x1.75 in (43.3x48.5x4.	5 cm)	17x24x3.5 in (9x60x43 cm)	
Shipping weight 29.3 lb (13.3 kg) 65 lb (29.64 kg) Major regulatory FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	Weight			18.1 lb (8.2 kg)		40.5 lb (18.38 kg)	
Major regulatory FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL Environment 15-40 deg C	WEEE weight			23 lb (10.4 kg)		49.5 lb (22.4 kg)	
Environment 15-40 deg C	Shipping weight	29.3 lb (13.3 kg) 65 lb (29.64 kg)					
	Major regulatory	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL					
Humidity 10-90% non-condensing	Environment	15-40 deg C					
	Humidity			10-9	0% non-condensing		

¹Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. ²Threat Prevention/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and kin its test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled. ³VPN throughput measured using UDP traffic at 1280 byte packet. ⁴Applies to SuperMassive 9200, 9400 and 9600. SuperMassive 9800 UC APL certification is pending. ⁸Supported on SonicOS 6.1 and 6.2. ⁶For 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.



SuperMassive 9000 Series ordering information

PRODUCT	SKU
SuperMassive 9800 Total Secure Advance Edition (1-year)	01-SSC-0312
SuperMassive 9600 Total Secure Advance Edition (3-year)	02-SSC-0410
SuperMassive 9400 Total Secure Advance Edition (3-year)	02-SSC-0409
SuperMassive 9200 Total Secure Advance Edition (3-year)	02-SSC-0408
SUPERMASSIVE 9200 SUPPORT AND SECURITY SUBSCRIPTIONS	SKU
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, 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, Firewall management and reporting, Shadow IT Visibility, 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, Firewall management and reporting, Shadow IT Visibility, 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, Firewall management and reporting, Shadow IT Visibility, 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 10-houe software incense 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
Somewan Scraamizer with how Analytics module software needs for up to 5 hours (includes one year of 24x7 Software Support)	01-330-4002

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

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit <u>www.sonicwall.com</u>

SonicWall, Inc. 1033 McCarthy Boulevard | Milpitas, CA 95035 Refer to our website for additional information. www.sonicwall.com © 2020 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. Datasheet-SuperMassive-US-COG-2465

