Exhibit C

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 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:

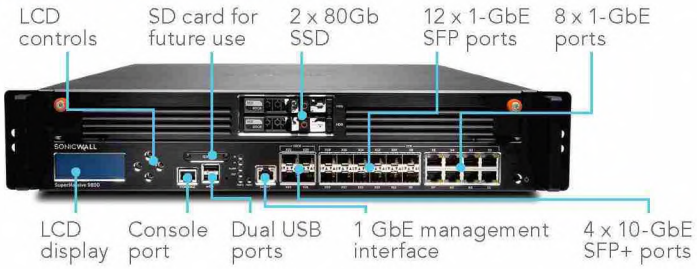
- Get complete breach prevention including high performance intrusion prevention, low latency malware protection and cloud-based sandboxing
- Gain full granular application identification, control and visualization
- Find and block hidden threats with decryption and inspection of TLS/SSL and SSH encrypted 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

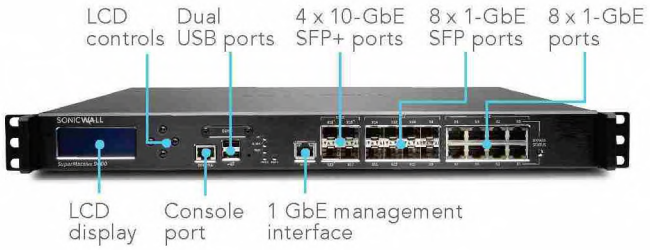
*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

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



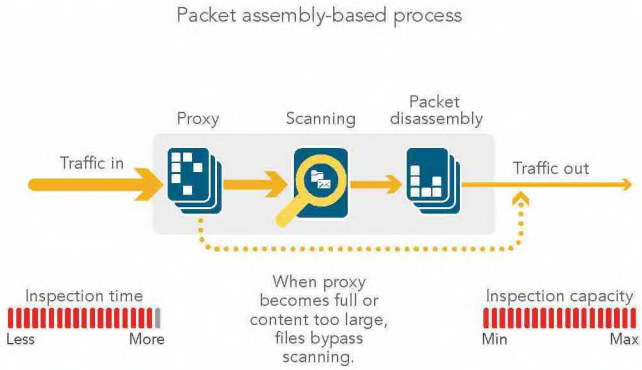


Capability	9200	9400	9600	9800
Processing cores	24	32	32	64
Firewall throughput	15 Gbps	20 Gbps	20 Gbps	31.8 Gbps
Application inspection throughput	5 Gbps	10 Gbps	11.5 Gbps	23 Gbps
Intrusion prevention system (IPS) throughput	5 Gbps	10 Gbps	11.5 Gbps	21.3 Gbps
Anti-malware inspection throughput	3.5 Gbps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

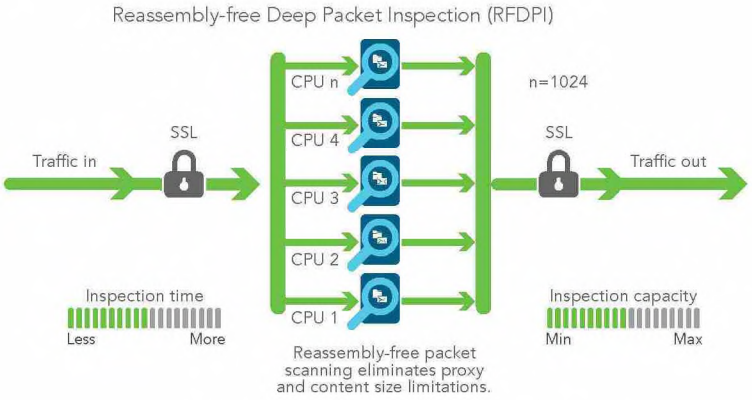
Reassembly-Free Deep Packet Inspection engine

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

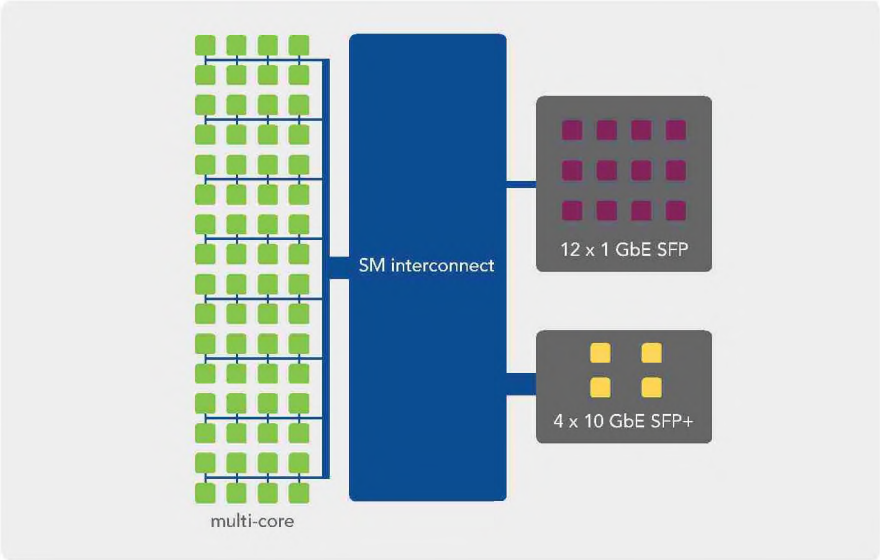


SonicWall stream-based architecture

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.



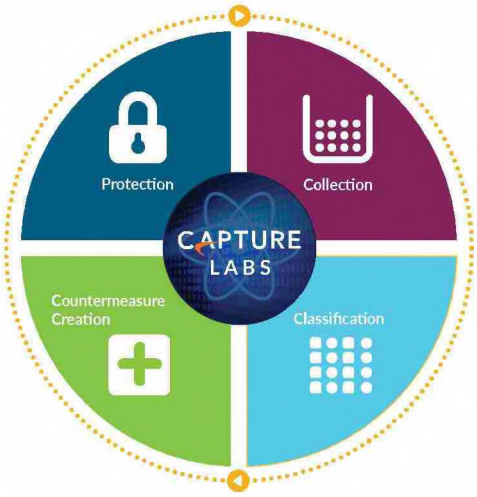
SONICWALL®

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.



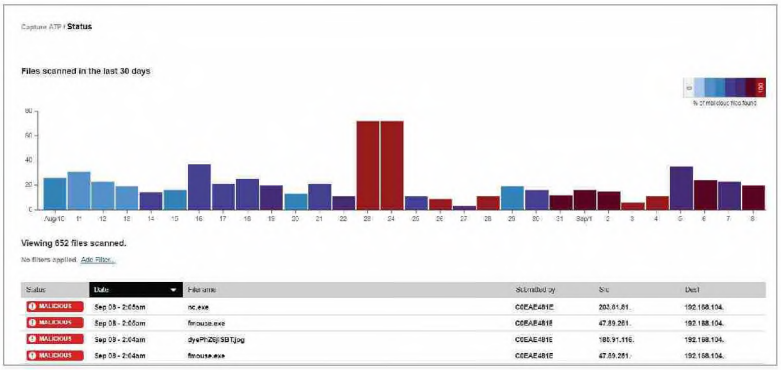
[1] *Requires added subscription*

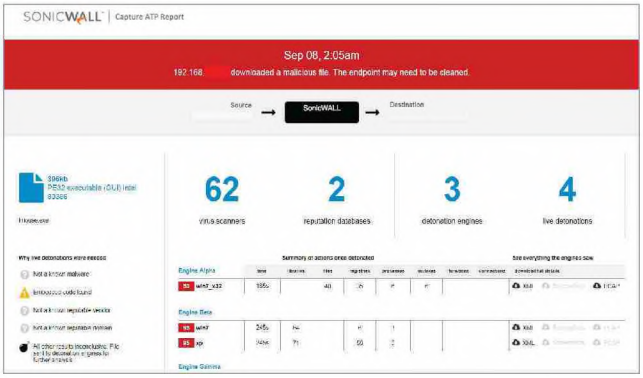
Advanced threat protection

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.





DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.