SonicOS Platform

The SonicOS architecture is at the core of every SonicWall firewall from the SuperMassive™ E10800 to the TZ SOHO. SonicOS uses deep packet inspection technology in combination with multi-core specialized security microprocessors to deliver effective breach prevention, application identification, control, and real-time visualization, high-speed virtual private networking (VPN) technology and other robust security features.

Firewall features

Reassembly-Free Deep Packet Inspection (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 intocompliance with firewall access policies.
High availability/clustering	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	Firewall 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.

Firewall and networking cont.	
Feature	Description
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.
Integrated 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 SuperMassive 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.
Management and reporting	
Feature	Description
Global Management System	SonicWall GMS monitors, configures and reports on multiple SonicWall appliances through a single management console with an intuitive interface, reducing management costs and complexity.
Powerful single device management	A continuously updated database of over 17 million threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Scrutinizer or other tools that support IPFIX and NetFlow with extensions.
Virtual private networking (VPN)	
Feature	Description
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
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. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

Breach prevention subscription services

Capture Advanced Threat Protection	
Feature	Description
Multi-Engine Sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
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 OSX 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.
Block Until Verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Encrypted Threat Protection	
Feature	Description
SSL decryption and inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in SSL encrypted traffic. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspects data traversing over SSH tunnels to prevent attacks that leverage SSH.
Intrusion prevention	
Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect 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	Identifies and blocks attacks that abuse protocols as they attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.
Threat prevention	
Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
CloudAV malware protection	A continuously updated database of over 17 million threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.

Threat prevention cont.	
Feature	Description
Bi-directional raw TCP inspection	The RFDPI engine scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbond threats.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP. Decodes payloads for malware inspection, even if they do not run on standard, well-known ports.
Application intelligence and control	
Feature	Description
Application control	Controls applications, or individual application features that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures. This increases network security and enhances network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. This helps gain further control over the network.
Application bandwidth management	Application bandwidth management granularly allocates and regulates available bandwidth for critical applications (or application categories), while inhibiting nonessential application traffic.
On-box/off-box traffic visualization	Identifies bandwidth utilization and analyzes network behavior with real-time, on-box application traffic visualization and off-box application traffic reporting via NetFlow/IPFix.
Granular control	Controls applications (or specific components of an application) based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.
Content filtering	
Feature	Description
Inside/outside content filtering	Uses Content Filtering Service to enforce acceptable use policies and block access to websites containing information or images that are objectionable or unproductive.
Enforced content filtering client	Extends policy enforcement to block internet content for Windows, Mac and Android devices located outside the firewall perimeter.
Granular controls	Blocks content using 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	
Feature	Description
Multi-layered protection	Utilizes the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block viruses entering the network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensures every computer accessing the network has the most recent version of anti-virus and anti-spyware signatures installed and active, eliminating the costs commonly associated with desktop anti-virus and anti-spyware management.
Automated deployment and installation 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.

SonicOS 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

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

Capture Advanced Threat Protection

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

Intrusion prevention

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection engine
- Granular IPS rule capability
- GeoIP/Botnet filtering
- Regular expression matching

Anti-malware

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

Application identification

- Application control
- Application 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

- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth manage CFS rating 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)

Networking

- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (not on TZs an NSA 2600)
- Layer-2 QoS
- Port security
- Dynamic routing
- SonicPoint wireless controller[1]
- Policy-based routing
- NAT
- DHCP server
- Bandwidth management
- Link aggregation
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire mode, tap mode, NAT mode
- 3G/4G WAN failover (not on SuperMassive 9800)
- Asymmetric routing
- Common Access Card (CAC) support

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
- Single sign-on (SSO)
- Terminal service/Citrix support[1]
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)
- LCD management screen
- Dell X-Series switch management (not on SM 9800)

IPv6

- IPv6 filtering
- 6rd (rapid deployment)
- DHCP prefix delegation
- BGP

Wireless (TZ Series only)

- Dual-band (2.4 GHz and 5.0 GHz)
- 802.11 a/b/g/n/ac wireless standards
- Wireless intrusion detection and prevention
- Wireless guest services
- Lightweight hotspot messaging
- Virtual access point segmentation
- Captive portal
- Cloud ACL

[1] *Supported on SonicOS 6.1 and 6.2. Not supported on SonicOS 6.2.1.*
[2] *Requires added subscription.*

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

Datasheet-SonicOSplatform-US-VG-27296

SONICWALL™