DATA SHEET

SonicWall Protection Security Suites

Comprehensive and simplified network security and firewall management packages

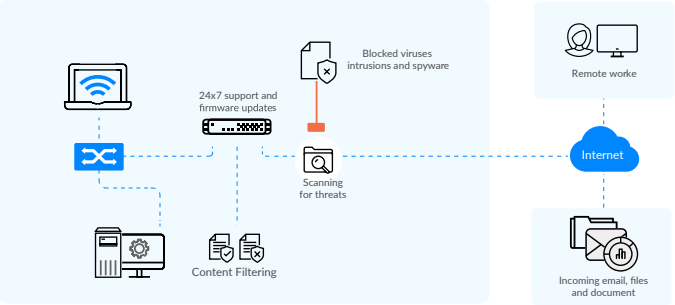
Understanding and managing effective network security is challenging and complex. Fortunately, there is a simple solution to block advanced attacks, assess and mitigate risk, and ease firewall management.

SonicWall Advanced Protection Security Suite (APSS) and SonicWall Managed Protection Security Suite (MPSS) are simplified packages of comprehensive security services for your business needs.

APSS includes advanced threat protection services, Capture ATP, cloud-based network management, reporting and analytics plus 24/7 Support to keep your business protected and ahead of the threat landscape.

MPSS simplifies firewall management by putting it in the hands of SonicWall experts. In addition to all the services in APSS, it includes 24/7 monitoring, configuration management, scheduled firmware updates, and monthly health check reports outlining threat activity and protection status.

Both packages include an industry-first firewall cyber warranty to help mitigate financial loss from security breaches, and promote peace of mind.



BENEFITS

- Simplified, comprehensive security solution
- Gateway anti-virus and anti-spyware protection
- Comprehensive Anti-Spam Service
- Cutting-edge IPS technology
- Application intelligence and control
- DNS Filtering
- Content filtering
- 24/7 support with firmware updates and hardware replacement
- Cloud-based advanced management, reporting and analytics
- Multi-engine network sandbox featuring SonicWall's patented Real-Time Deep Memory Inspection (RTDMI™)
- Option for managed firewall services
- No cost, embedded cyber warranty

sonicwall.com

SONICWALL®

Features and benefits

Threat protection services keep your network safe from viruses, intrusions, botnets, spyware, trojans, worms and other malicious attacks. As soon as new threats are identified and often before software vendors can patch their software, SonicWall firewalls and Capture Cloud database are automatically updated with signatures that protect against these threats. Inside these firewalls resides patented RTDMI™ engine that scans traffic against multiple application types and protocols, ensuring your network has around-the-clock protection from internal and external attacks and application vulnerabilities.

Cloud based **Network Security Manager (NSM)**, a centralized firewall management solution that delivers scalable and simplified management of firewall operations including multi-tenant administration. **Advanced Reporting and Analytics** give single-pane visibility and let you monitor and uncover threats by unifying and correlating logs across all firewalls.

Capture ATP Service revolutionizes advanced threat detection and sandboxing with a cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway. Capture ATP blocks zero-day attacks before they enter your network. It lets you establish advanced protection against the changing threat landscape and analyze a broad range of file types.

Gateway Anti-Virus protection combines network-based anti-malware with a dynamically updated cloud database of tens of millions of malware signatures. Dynamic spyware protection blocks the installation of malicious spyware and disrupts existing spyware communications.

Cutting-edge IPS technology protects against worms, trojans, software vulnerabilities and other intrusions by scanning all network traffic for malicious or anomalous patterns, thereby increasing network reliability and performance.

Application intelligence and control is a set of granular, application-specific policies providing application classification and policy enforcement to help administrators control and manage both business and non-business related applications.

Comprehensive Anti-Spam Service offers small- to medium sized businesses >99% effectiveness against spam, dropping >80% of spam at the gateway, while utilizing advanced anti-spam techniques like Adversarial Bayesian™ and machine-learning filtering.

Content Filtering Services (CFS) lets you enforce Internet use policies and control internal access to inappropriate, unproductive and potentially illegal web content with comprehensive content filtering. Reputation-based **CFS 5.0** provides a reputation score that forecasts the security risk of a URL across 93 web categories.

DNS filtering blocks malicious websites or applications at the DNS layer to filter out harmful or inappropriate content without enabling TLS decryption and adversely affecting performance.

SonicWall's highly secure **access points** can be managed via the cloud using SonicWall Wireless Network Manager (WNM) on SonicWall Unified Management, or through SonicWall firewalls, offering ease of management and seamless integration with SonicWall wireless products.

Network access control integration provides network access control for SonicWall customers by integrating with Aruba ClearPass, giving you comprehensive and precise profiling, authentication, and authorization for systems and devices trying to access your IT resources. SonicOS provides a RESTful API that will support Aruba ClearPass as NAC to integrate with SonicWall NGFW. This architecture will turn static security into contextual security to provide more flexible and advanced security protection.

24/7 Support with firmware updates and hardware replacement protects your business and your SonicWall investment. Support includes around-the-clock access to telephone and web-based support for basic configuration and troubleshooting assistance, as well as hardware replacement in the event of failure.

Managed Protection Security Suite (MPSS) makes firewall management even easier by leaving it to the SonicWall team. Our team will monitor your firewall and notify you of downtime or local changes, and will manage all firmware updates for you on your schedule. MPSS includes a $200K cyberwarranty.

Embedded warranty by Cysurance is offered as part of your security services to mitigate costs of security breach, meet compliance requirements and promote peace of mind.

SONICWALL®

FEATURE	ADVANCED PROTECTION SECURITY SUITE	MANAGED PROTECTION SECURITY SUITE
24/7 Support	●	●
IPS	●	●
Application Control	●	●
Content Filtering Service	●	●
Gateway Anti-Virus	●	●
DNS Security including Advanced DNS Filtering**	●	●
Network Access Control (NAC) Integration with Aruba ClearPass	●	●
Wi-Fi 6 integration	●	●
Deep Packet TLS/SSL for Decryption & Inspection	●	●
GeoIP Country Traffic Identification	●	●
Botnet Service	●	●
Comprehensive Anti-Spam Service	●	●
Capture ATP - Sandboxing (Static, RTDMI, Memory, Hypervisor, Emulation)	●	●
NSM (Cloud) Management	●	●
Advanced Reporting and Analytics (Cloud)***	7-Day Included	30-day included
Firewall Configuration Management		●
After Hours Critical Support		●
Embedded Warranty****	Up to $100,000	Up to $200,000

** DNS Filtering is not supported on WireMode interfaces
*** Reporting and analytics can be extendable to 30, 90 or 365 days.
**** Only for firewalls sold & registered after November 1, 2024

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.