

Dynamic Security for the Global Network

NETWORK SECURITY

SonicWALL Features and Capabilities

A Vision for Dynamic Security for the Global Network

Our vision is simple: we believe security solutions should be “smart” enough to adapt as organizations evolve and as threats evolve, dynamically, globally. We believe customers around the world should have the ability to control, manage and protect their global network easily and automatically. We believe our customers should be able to receive and share threat and defense data around the world so they can anticipate and stop attacks before they happen. We want our customers to be able to secure any user, any device, using any application from anywhere so they can collaborate securely across different networks. All this needs to be achieved with maximum ease of deployment and at the best economic value and in a compliant framework.

The following summarizes key enterprise-class features, attributes, and certifications for our network security solutions:

Enterprise-Class Features/Attributes

- **Application Intelligence:** Extends the protection of SonicWALL's network security appliances beyond blocking traditional network threats to the management and control of data and applications that pass through the network security appliance. This extended capability provides application-level bandwidth management access controls, data leakage control functionality, restrictions on the transfer of specific files and documents, and much more. This configurable set of granular application-specific policies can be based on user, application, schedule, or IP subnet. These policies can be used to restrict transfer of specific files and documents, scan email attachments using user-configurable criteria, automate application bandwidth, control and inspect both internal and external Web access, and enable administrators to create custom signatures.
- **SSL Inspection (DPI SSL):** Transparently decrypts and scans both inbound and outbound SSL traffic regardless of port and protocol. Once decrypted, this traffic can be sent through SonicWALL's Reassembly-Free Deep Packet Inspection engine and can be scanned for threats and vulnerabilities. Should DPI SSL discover no threats or vulnerabilities, it re-encrypts the traffic and sends it to its destination.
- **Active/Active UTM:** Active/Active Unified Threat Management (UTM) optimizes concurrent processing of Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention (IPS) and Application Intelligence services on both the primary and failover UTM firewalls deployed in a stateful high availability (HA) pair, providing maximum security and network throughput. It delivers comprehensive network protection along with up to a 75% performance increase¹ which allows certain customers to consolidate their protection onto one device without network performance degradation.
 - **Stateful Active/Passive High Availability:** In Active/Passive mode, the active firewall deployed in stateful high availability (HA) pair performs all traffic processing until a failover occurs, at which time all traffic is instantly and automatically routed through the secondary firewall where it seamlessly takes over all traffic processing.
- **Route-based VPN with Dynamic Routing:** Dynamic Routing over VPN allows network administrators to provide greater redundancy and resiliency on their VPN networks. OSPF and RIP protocols are used to determine the best and alternate, if necessary, paths for network traffic over VPN.
- **Single Sign-on:** Single Sign-On (SSO) enables automated reuse of user credentials across multiple authentication checkpoints to provide user based policy enforcement and user based reporting using ViewPoint or SonicWALL Global Management System (GMS).
- **Citrix® and Terminal Services Support:** Provides transparency authentication of users in environments running Terminal Services or Citrix within their network environment. This user authentication allows for policy enforcement and user-based reporting.
- **Gateway Security Services:** The SonicWALL Comprehensive Gateway Security Suite (CGSS) offers Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service, Application Intelligence, Content Filtering and more to businesses of all sizes.
- **PCI Compliance:** Configurations using SonicWALL UTM appliances and SonicWALL GMS are backed and approved by an independent PCI Qualified Security Assessor (QSA), ensuring their capacity to serve as technological control components in any network striving to achieve PCI compliance.

¹UTM throughput measured using industry standard Spirent WebAvalanche HTTP Performance test.



PROTECTION AT THE SPEED OF BUSINESS™

Certifications

SonicWALL's Network Security solutions secure some of the largest government agencies worldwide from the latest security threats and vulnerabilities. Use of SonicWALL's Global Management System enables these agencies to manage thousands of appliances from a central location, providing real-time monitoring and reporting. SonicWALL's Secure Remote Access (SRA) solutions allows government employees to work from any location, securely, while providing end-point control to limit access for non-trusted systems like hand held or mobile devices. SonicWALL solutions also help government agencies comply with mandates and legislation such as the Homeland Security Act of 2002 and National Strategy to Secure Cyberspace.

Additionally SonicWALL complies with:

- Common Criteria Evaluation Assurance Level (EAL)
- Federal Information Processing Standard (FIPS)

SonicWALL firewalls are certified for :

- EAL 4+¹
- FIPS 140-2²



¹ NSA Series and E-Class NSA Series

² NSA E7500, NSA E6500, NSA E5500, NSA 4500 and NSA 3500. Pending on TZ 210, TZ 200 and TZ 100

Coming Soon

- **IPv6:** Provides networking, security and Virtual Private Networking (VPN) support for the next generation Internet Protocol version 6 (IPv6) networks. The feature set that SonicWALL has developed for IPv6 will allow organizations to migrate from IPv4 to IPv6 while providing the highest level of security, network connectivity and encryption. (IPv6 ready addendum: Current NSA products are IPv6 ready and will only require a software upgrade.
- **Application Visibility:** Provides network administrators a current view of the applications running on the network. This information can be used to provide user-based policy enforcement, to block or limit bandwidth intensive and non-business related applications.
- **Active/Active Clustering:** Allows two or more SonicWALL Network Security Appliances to be clustered together so they can process network traffic in Active/Active high-availability cluster configuration. This clustering configuration provides greater network redundancy and can increase over-all network security performance.

SonicWALL's line-up of comprehensive protection



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB AND E-MAIL SECURITY



BACKUP AND RECOVERY



POLICY AND MANAGEMENT

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com



PROTECTION AT THE SPEED OF BUSINESS™