SONICWALL

Advanced Gateway Security Suite

Complete network security and firewall management in a single integrated package

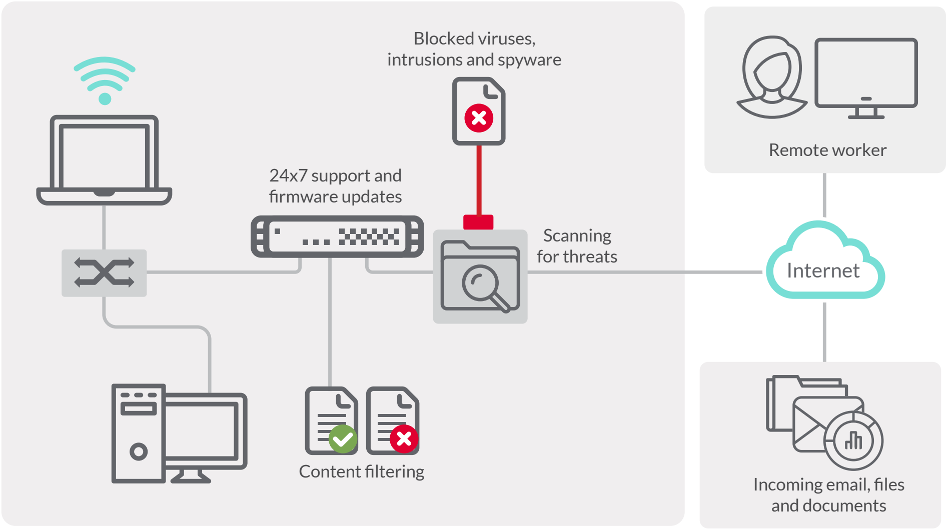
Understanding and managing effective network security is challenging and complex. Fortunately, there is a simple solution to block advanced attacks, assess and mitigate risk, and ease firewall management.

SonicWall Advanced Gateway Security Suite (AGSS) integrates comprehensive network security and firewall management services into a convenient, affordable package. AGSS is available as an add-on services for all physical and virtual SonicWall firewalls, including our NSsp, NSa, TZ and NSv Series.

Features and benefits

AGSS keeps 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 every SonicWall firewall is a patented Reassembly-Free Deep Packet Inspection® (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. It integrates everything you need for firewall management and protection from threats such as ransomware, viruses, spyware, worms, Trojans, adware, keyloggers, malicious mobile code (MMC) and other dangerous applications and web content.

Capture Advanced Threat Protection (ATP) Service revolutionizes advanced threat detection and sandboxing with a cloud-based, multi-engine solution for stopping unknown and zero-day attacks


Blocked viruses, intrusions and spyware
24x7 support and firmware updates
Scanning for threats
Content filtering
Remote worker
Internet
Incoming email, files and documents

Benefits:

- Complete network security solution
- ICSA-certified gateway anti-virus and anti-spyware protection
- Cutting-edge IPS technology
- Application intelligence and control
- Content filtering
- Capture Security Center (CSC)
- Universal dashboard
- Risk meters
- Configuration & change management
- 7-day reporting
- Shadow IT Visibility
- 24x7 support with firmware updates and hardware replacement
- Multi-engine network sandbox featuring SonicWall RTDMI
- Cloud-based single pane of glass management

ICSA labs CERTIFIED ANTI-VIRUS

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, analyze a broad range of file types, and rapidly and automatically deploy remediation signatures to other network security appliances.

Capture ATP features SonicWall's Real-Time Deep Memory Inspection (RTDMI) technology which detects and blocks malware that does not exhibit any malicious behavior or hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, never-before-seen threats and unknown malware, accurately utilizing real-time memory-based inspection techniques.

ICSA-certified gateway anti-virus and anti-spyware protection combines network-based anti-malware with a dynamically updated cloud database of tens of millions of malware signatures. This adds deep security protection against advanced modern threats continuously in real time. 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.

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. Website ratings cached locally on SonicWall firewalls make response time to frequently visited sites virtually instantaneous. Dynamically updated rating architecture cross-references all requested websites against a database in the cloud containing millions of URLs, IP addresses and domains and then compares each rating to the local policy setting.

Additionally, with the SonicWall Content Filtering Client, you can extend security and productivity by enforcing Internet use policies on endpoint devices located outside the firewall. This is available as a separate subscription service for Windows, Mac OS and Chrome endpoints.

Capture Security Center (CSC) delivers unified management, analytics and reporting for network, web, endpoint, email and cloud security through a single pane of glass. It enhances visibility, agility and capacity to help you govern your entire SonicWall security ecosystem with greater clarity, precision and speed — all from one simple cloud interface.

CSC Zero-Touch Deployment enables administrators to have pre-configured firewalls shipped to their remote sites with minimal interaction required to start up and manage the device.

CSC 7-Day Reporting gives comprehensive security and operational KPIs for doing proactive security strategizing and planning. This includes network events, user activities, threat, operation and performance metrics, compliance and audit readiness and post-mortem analysis.

Shadow IT Visibility discovers usage of risky SaaS applications, track user activity, and set allow/block policies on sanctioned and unsanctioned applications.

24x7 Support with firmware updates and hardware replacement protects your business and your SonicWall investment. Software and firmware updates and upgrades maintain network security to keep your solution as good as new. 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. You also receive an annual subscription to SonicWall Service Bulletins and access to electronic support tools and moderated discussion groups.

Feature	CGSS	AGSS
Gateway Anti-Virus	Y	Y
Intrusion Prevention	Y	Y
Application Control	Y	Y
Content Filtering	Y	Y
24 x 7 Support	Y	Y
CSC Unified Dashboard & Risk Meters	Y	Y
CSC Firewall Management	Y	Y
CSC 7-Day Reporting	Y	Y
Capture ATP	N	Y
Shadow IT Visibility	N	Y

AGSS is an upgrade over Comprehensive Gateway Security Suite (CGSS) that adds multi-engine sandboxing and Shadow IT Visibility for superior protection.

Advanced Gateway Security Suite	SKU
NSsp 12800 (1-year)	01-SSC-6591
NSsp 12400 (1-year)	01-SSC-6588
NSa 9650 (1-year)	01-SSC-2036
NSa 9450 (1-year)	01-SSC-0414
NSa 9250 (1-year)	01-SSC-0038
NSa 6650 (1-year)	01-SSC-8761
NSa 5650 (1-year)	01-SSC-3674
NSa 4650 (1-year)	01-SSC-3493
NSa 3650 (1-year)	01-SSC-3451
NSa 2650 (1-year)	01-SSC-1783
TZ600 Series (1-year)	01-SSC-1460
TZ500 Series (1-year)	01-SSC-1450
TZ400 Series (1-year)	01-SSC-1440
TZ350 Series (1-year)	02-SSC-1773
TZ300 Series (1-year)	01-SSC-1430
SOHO 250 Series (1-year)	02-SSC-1726
NSv 1600 (1-year)	01-SSC-5787
NSv 800 (1-year)	01-SSC-5737
NSv 400 (1-year)	01-SSC-5681
NSv 300 (1-year)	01-SSC-5584
NSv 200 (1-year)	01-SSC-5306
NSv 100 (1-year)	01-SSC-5219
NSv 50 (1-year)	01-SSC-5194
NSv 25 (1-year)	01-SSC-5165
NSv 10 (1-year)	01-SSC-5008

Multi-year SKUs are available.
To access SKUs for the complete line of SonicWall firewalls, please visit www.sonicwall.com.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award-winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

SONICWALL®