SonicWall Enforced Client Anti-Virus and Anti-Spyware Software

Automated and enforced anti-virus and anti-spyware protection

When you are facing multiple threats from multiple locations, you need multiple layers of protection. A firewall's gateway anti-virus solution provides the first layer of defense at the perimeter, stopping most attacks before they enter the network. But viruses can still enter the network through multiple entry points. While protection at multiple layers is the best defense, deploying, maintaining and enforcing the right security software on the endpoint devices can strain IT resources and budgets. This has created the need for a manageable, enforced network-wide solution that ensures all endpoints have the latest security software updates.

SonicWall™ firewalls provide an innovative multi-layered anti-malware strategy consisting of its proprietary Reassembly Free Deep Packet Inspection® (RFDPI) anti-malware solution at the gateway and enforced anti-virus solution at the endpoints. When a non-complaint endpoint within the network tries to connect to the Internet, the firewall will redirect the user to a web page to install the latest SonicWall Enforced Client Anti-Virus and Anti-Spyware software. The firewall further ensures that all the endpoint clients are automatically updated with the latest anti-virus and anti-spyware signatures without end-user intervention. The software is easily deployed, automatically enforced and updated network-wide on Microsoft® Windows® devices through a powerful but easy-to-use policy-driven engine. Because it is client-based and maintained across the network, it protects against threats

regardless of whether the endpoint is inside the corporate network or outside connected via VPN. Virus and spyware signatures are updated automatically, thus simplifying ongoing administration and ensuring reliability. SonicWall Enforced Client Anti-Virus and Anti-Spyware software is available for purchase with the McAfee® or SentinelOne anti-virus engine.

Features and benefits

Automated installation and deployment of anti-virus and anti-spyware clients machine-by-machine across the network is enforced by the firewall thus minimizing administrative overhead.

Automated by the SonicWall firewall, anti-virus and anti-spyware client enforcement verifies that 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 policy management.

Always on, automatic virus protection keeps end-user productivity high and security management low by providing frequent anti-virus and anti-spyware updates transparently to all desktops and file servers.

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.

Benefits:

- Automated/enforced installation and deployment

- Automated anti-virus and anti-spyware client enforcement

- Always on, automatic virus protection

- Always on, automatic spyware protection

- On-demand and scheduled scanning

- Comprehensive web-based reporting

- License sharing

On-demand and scheduled scanning provides administrators with the customization flexibility to choose when additional scans are performed and how frequently the software checks for anti-virus and anti-spyware signature updates.

Comprehensive web-based reporting provides information about the state of each user, historical data on past infection detections, and information on each computer's operating system.

License sharing enables organizations with distributed networks of multiple SonicWall firewall appliances to allocate Enforced Client Anti-Virus and Anti-Spyware licenses to meet changing conditions.

Centralized anti-virus management and reporting

SonicWall anti-virus policy management and reporting can be accessed through the web interface of the SonicWall firewall appliance. It reports detailed enterprise-wide information such as coverage status summary, machines updated, viruses cleaned, and spyware detected, deleted and quarantined, as well as the currency of .DAT, engine and product versions.
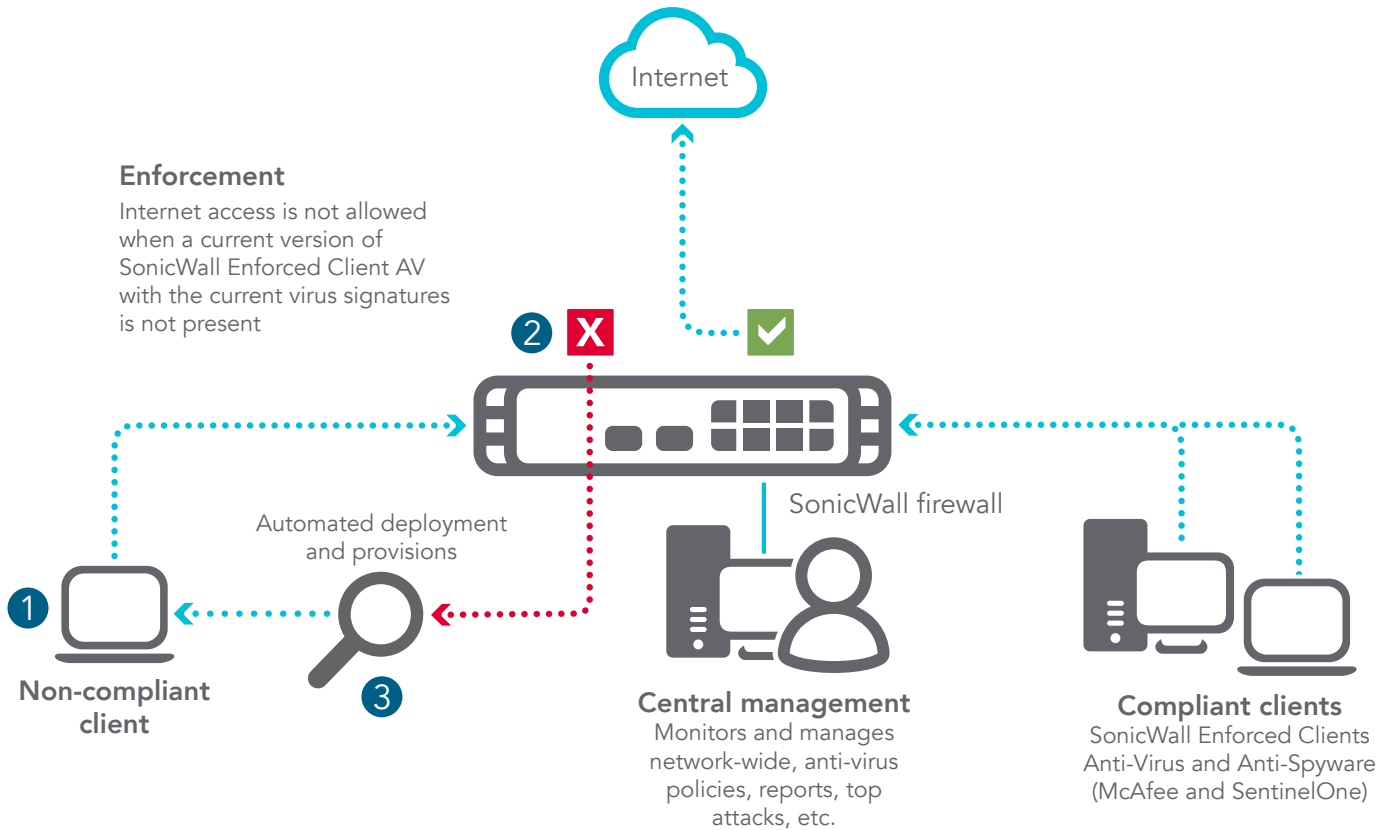
Policy-based management

- Scheduled and manual scan settings
- Configurable spyware protection mode

- Excluded files and folders
- Manage approved programs list
- Granularly configurable virus and spyware protection settings

Top reports

- Systems out-of-date
- Systems up-to-date
- Viruses found and spyware detected
- Most-infected machines
- Detailed system reporting of each machine

Enforcement

Internet access is not allowed when a current version of SonicWall Enforced Client AV with the current virus signatures is not present

Internet

② ✗ ✓

SonicWall firewall

Automated deployment and provisions

Non-compliant client

Central management
Monitors and manages network-wide, anti-virus policies, reports, top attacks, etc.

Compliant clients
SonicWall Enforced Clients Anti-Virus and Anti-Spyware (McAfee and SentinelOne)

① Non-compliant client attempts to access the Internet

② Access is denied and client is notified

③ SonicWALL Enforced Client Anti-Virus and Anti-Spyware (McAfee and SentinelOne) is installed and client becomes compliant

SONICWALL®

Specifications

Solution	Supported platforms	Features
McAfee Enforced Client	• Windows XP Home or Professional (with Service Pack 2 or later) • Windows Vista • Windows 7.1 • Windows 8.1	• Can be deployed in enforced and/or in stand-alone mode • Enforced through all SonicWall firewalls (E-Class Network Security Appliance (NSA), NSA and TZ Series)
SonicWall Server Anti-Virus (McAfee)*	• Windows 2000 (with Service Pack 2 or later) • Windows 2003 • Windows Server 2008 • Microsoft Exchange 2000/2003/2007/2010	• Not enforceable; can be deployed in stand-alone mode and/or managed using McAfee ePolicy Orchestrator (not sold by SonicWall)

Sold as part of SonicWall Server Anti-Virus/Enforced Client Anti-Virus and Anti-Spyware Suite McAfee which includes SonicWall Enforced Client Anti-Virus and Spyware (McAfee)

Enforced Client Anti-Virus and Anti-Spyware

McAfee	
Number of users	SKU
5 user license (1 yr)	01-SSC-2743
10 user license (1 yr)	01-SSC-2740
25 user license (1 yr)	01-SSC-2745
50 user license (1 yr)	01-SSC-2741
100 user license (1 yr)	01-SSC-2742
250 user license (1 yr)	01-SSC-6948
500 user license (1 yr)	01-SSC-6949
1,000 user license (1 yr)	01-SSC-6950

SonicWall Server Anti-Virus/ Enforced Client Anti-Virus and Anti-Spyware Suite

McAfee	
Number of users	SKU
5 user license (1 yr)	01-SSC-3419
10 user license (1 yr)	01-SSC-3420
25 user license (1 yr)	01-SSC-3421
50 user license (1 yr)	01-SSC-3422
100 user license (1 yr)	01-SSC-3423
250 user license (1 yr)	01-SSC-6975
500 user license (1 yr)	01-SSC-6976
1,000 user license (1 yr)	01-SSC-6977

McAfee: 2-year SKUs available. Visit sonicwall.com for more information.

For more information on SonicWall's suite of value-added security services including gateway anti-virus, anti-spyware and intrusion prevention service, application intelligence and control, comprehensive anti-spam service, enforced client anti-virus and anti-spyware and content filtering service, please visit our web site at sonicwall.com.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

SONICWALL®