

SonicWALL/Aventail Whitepaper

SSL-VPN Combined With Network Security

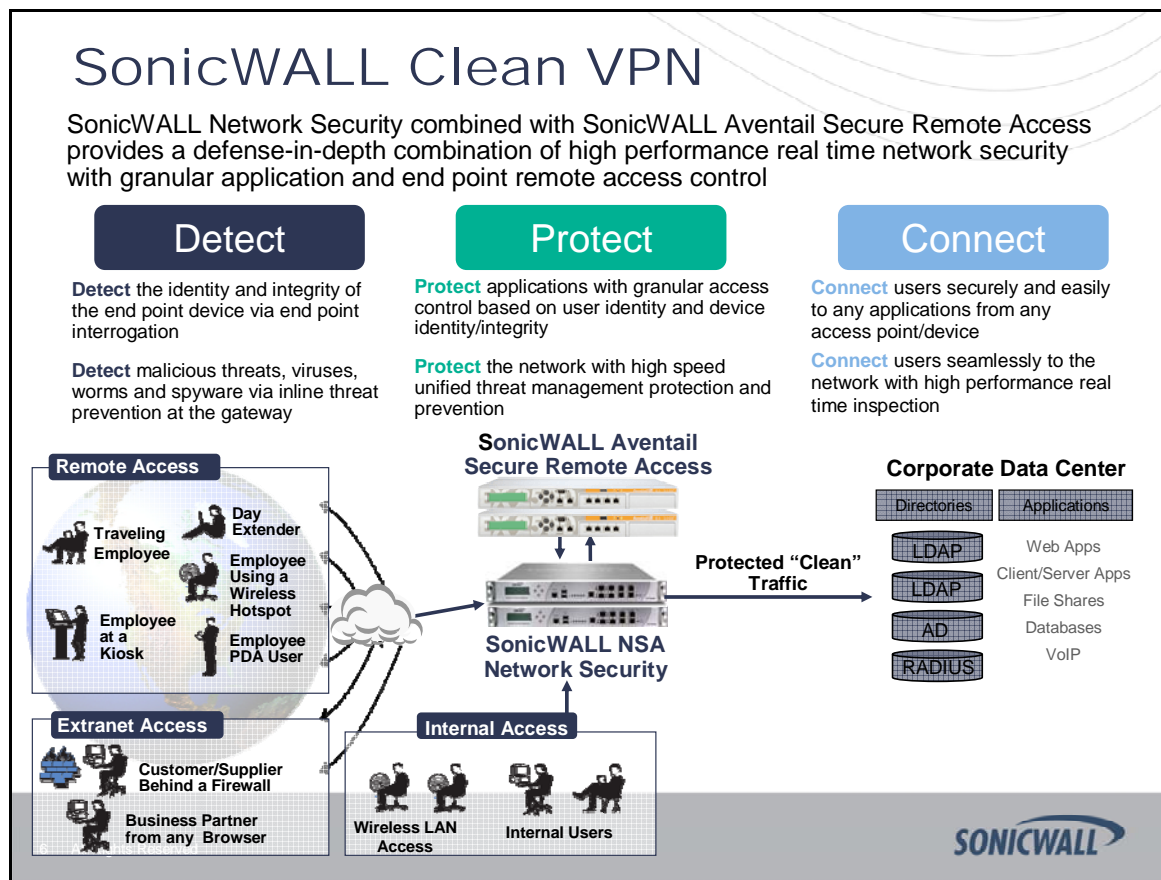
SonicWALL Clean VPN

Introducing SonicWALL Clean VPN

A popular feature of the SonicWALL® Aventail® SSL VPN appliances is called End Point Control (EPC). This allows the administrator to define specific criteria or attributes which an endpoint must meet to adhere to the company security policy. EPC can check for running applications, domain membership, certificates, files, and common anti-virus, anti-spyware, and personal firewall applications. Even with these checks though, it is still possible for malicious packets to enter the corporate network over the SonicWALL Aventail SSL VPN connection. This is especially true when connections are established from untrusted endpoints like home computers or kiosks where specific security applications can not be enforced.

To provide another layer of network protection, the SonicWALL Network Security Appliance (NSA) product can be deployed in conjunction with a SonicWALL Aventail SSL VPN appliance to provide SonicWALL® Clean VPN solution. This protection is enabled through the NSA multi-core architecture which provides ultra high-speed Deep Packet Inspection, Intrusion Prevention Service (IPS), Gateway Anti-Virus, Gateway Anti-Spyware, Content Filtering, and Application Firewall capabilities. The NSA ensures that all VPN traffic is scanned in real-time and decontaminated before it is placed on the internal network.

The combination of SonicWALL Aventail SSL VPN and SonicWALL NSA products provides organizations with a single solution for defense-in-depth security. The Clean VPN configuration allows organizations to establish trust for users, devices, and traffic before allowing a connection to any sensitive information on the network. The addition of SonicWALL Global Management System (GMS) means administrators can configure and manage their Secure Remote Access solution and their Network Security solution all from a single management interface.



SonicWALL/Aventail Whitepaper

NSA Overview

The SonicWALL Network Security Appliance (NSA) is an industry first: a multi-core Unified Threat Management (UTM) appliance that delivers enterprise-class deep packet inspection without significantly impacting network throughput. Combining a powerful deep packet inspection firewall, with multiple layers of protection technology and a suite of high-availability features, the NSA is the ultimate choice for a variety of enterprise deployments including distributed environments, campus networks and data centers.

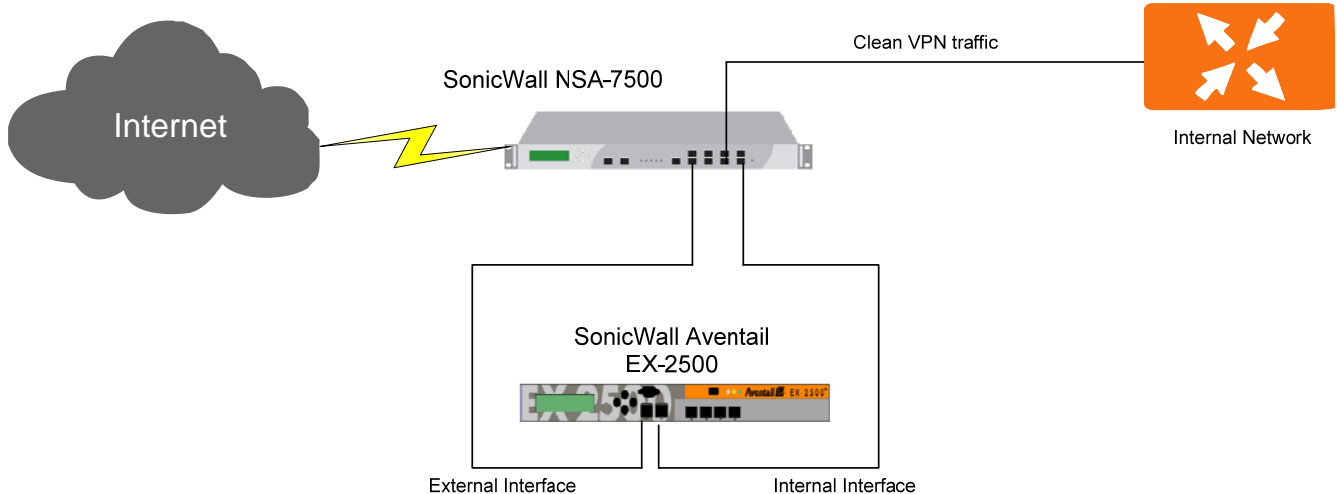
Key Features:

- **Multi-core Performance Architecture** – At the heart of the NSA is the SonicWALL multi-core performance architecture designed to provide breakthrough deep packet inspection and granular network intelligence without impacting network throughput. The SonicWALL NSA can effectively deliver ultra high-speed performance through the combined use of up to sixteen specialized security processing cores. Using the processing power of multiple cores in unison dramatically increases throughput and simultaneous inspection capabilities while lowering overhead impact.
- **Highly Redundant Security and Connectivity Platform** - The NSA delivers a highly redundant security and connectivity platform purpose-built for high-speed internal and external network protection, virtual private network (VPN) implementations, and deployment flexibility. SonicWALL NSA integrates real-time gateway antivirus, anti-spyware, and intrusion prevention to secure the network against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans, phishing attacks and software vulnerabilities. With built-in secure wireless switch functionality, dual power supplies and fans, the NSA is an ideal solution for a host of wired and wireless applications requiring high-speed access, highly redundant operation and heavy workgroup segmentation.
- **24x7 Dynamic Protection** - The NSA integrates dynamic threat protection, content filtering and application control to maximize security and decrease cost. These services are continually updated on a 24x7 basis to provide the latest in protection and control, improving overall network reliability and increasing IT productivity while eliminating the requirement of ad-hoc patch management for servers and workstations.
- **Deep Packet Inspection Signature Service** - Comprehensive signature database. Peer-to-peer and instant messaging control and signature updates through Distributed Enforcement Architecture.
- **Content Filtering Service** - HTTP URL, HTTPS IP, keyword and content scanning, ActiveX, Java Applet, and Cookie blocking
- **Gateway-enforced Client Anti-Virus and Anti-Spyware** - HTTP/S, SMTP, POP3, IMAP and FTP, Enforced Client Anti-Virus

Configuration Scenario 1: Firewall & Unified Threat Management (UTM)

The SonicWALL NSA can be placed in front of a SonicWALL Aventail appliance to provide both firewall and UTM capabilities. Utilizing the security zone capabilities of the NSA (which is a logical method of grouping one or more firewall interfaces), all VPN traffic from the SonicWALL Aventail appliance to the internal network can be scanned. In this configuration, network traffic from the Internet passes through the NSA firewall to the external interface of the SonicWALL Aventail appliance. If permitted by the Aventail access control rules, traffic is then proxied to the internal interface of the SonicWALL Aventail appliance back into the NSA where the traffic is then scanned for malicious content before being passed to the internal network, as depicted below:

SonicWALL/Aventail Whitepaper



Note: this same configuration can also be used for a single-homed SonicWALL Aventail appliance

Application Firewall

In addition to the UTM capabilities, another important NSA security feature for SonicWALL Aventail deployments is the Application Firewall. Application Firewall is a set of application-specific policies that gives granular control over network traffic on the level of users, email users, schedules, and IP-subnets.

Application Firewall advantages:

- Provides application access control and bandwidth management
- Regulates web traffic, email, email attachments and file transfers
- Allows scanning of files and documents for keywords and specified content
- Flexible configuration to allow creation of custom IDS/IPS signatures

Application Firewall's digital rights management component provides the ability to scan files and documents for content and keywords. Using application firewall, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. Based on SonicWALL Deep Packet Inspection technology, Application Firewall also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include:

- Disabling an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel
- Bandwidth throttling for file types when using the HTTP or FTP protocols

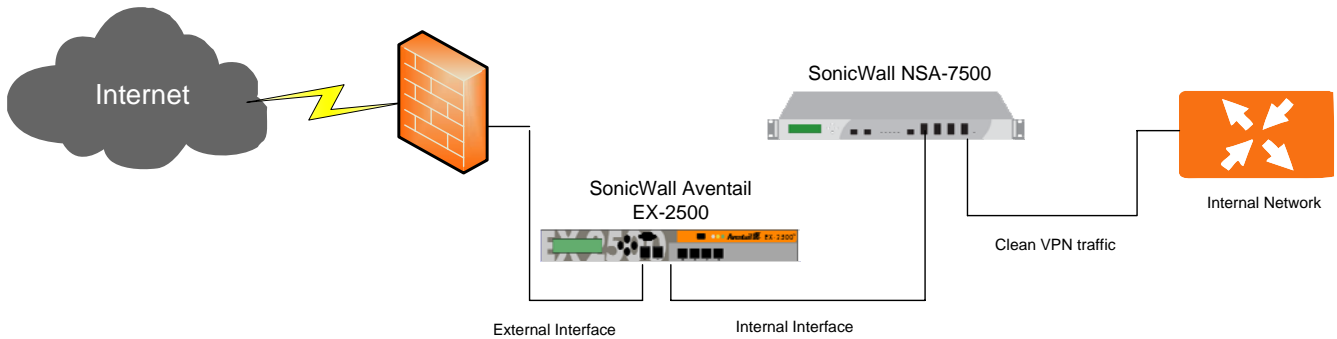
Examples of Application Firewall usage:

- Provide bandwidth management of BitTorrent applications
- Restrict user access of internet radio and video streaming sites like www.youtube.com
- Restrict outgoing "confidential" data using watermarks
- Restrict email send/receive for temps and contractors
- Manage bandwidth or block file downloads and uploads
- and much more.....

SonicWALL/Aventail Whitepaper

Configuration Scenario 2: Unified Threat Management (UTM)

SonicWALL NSA appliances can also be placed behind a SonicWALL Aventail appliance to provide only Unified Threat Management (UTM) capabilities. In this configuration, traffic from the internal interface of the SonicWALL Aventail appliance passes through the NSA before being placed on the internal network as depicted below:

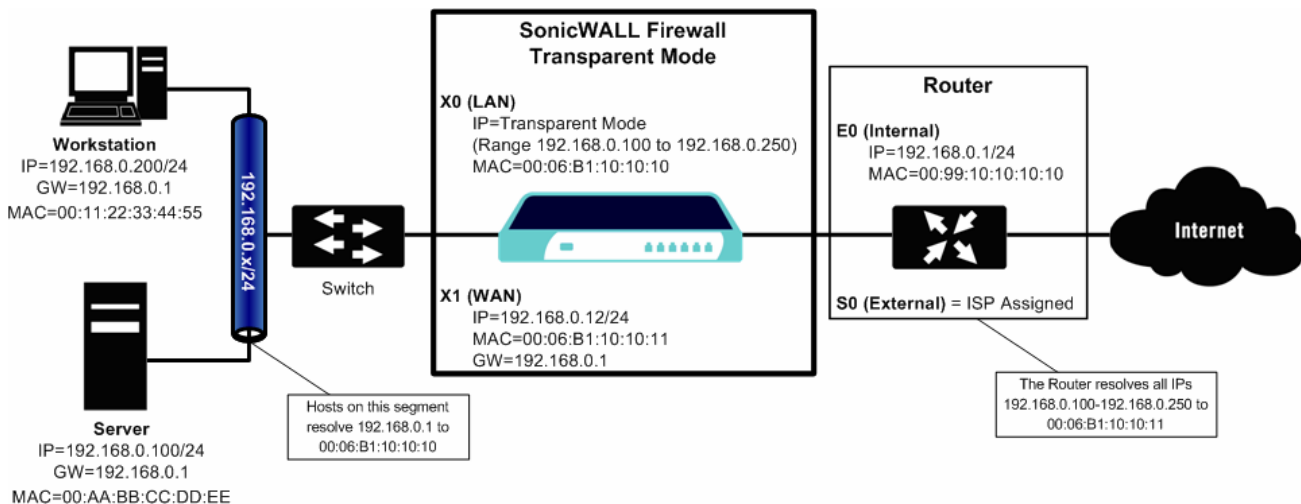


Layer 2 Bridge Mode

The SonicWALL NSA firmware has a feature called L2 (Layer 2) Bridge Mode which makes it very simple to deploy the NSA behind a SonicWALL Aventail appliance to implement a Clean VPN.

L2 (Layer 2) Bridge Mode enables a SonicWALL NSA to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic. It employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration.

Using L2 Bridge Mode, a SonicWALL NSA can be nondisruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.



SonicWALL/Aventail Whitepaper

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWALL Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti Virus, and Gateway Anti Spyware.