

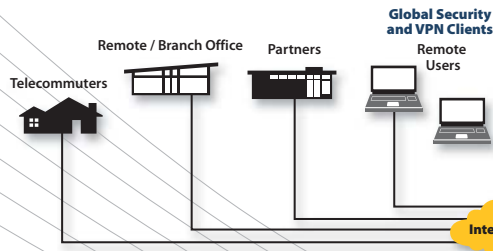
Applications

Central-site Primary Gateway

The PRO 5060 is ideal as a security gateway for critical, centralized networks. Its high-performance and advanced networking features allow seamless deployment into virtually any environment.

Features

- Suite of advanced security services for comprehensive multi-layer protection
- Zone security for segmenting internal groups
- Object-based management for easy administration
- Enhanced workforce productivity with Content Filtering Service
- DHCP server and DHCP relay ability
- Hardware and WAN/WAN Fail-over with round-robin, percent-based and spill-over load balancing

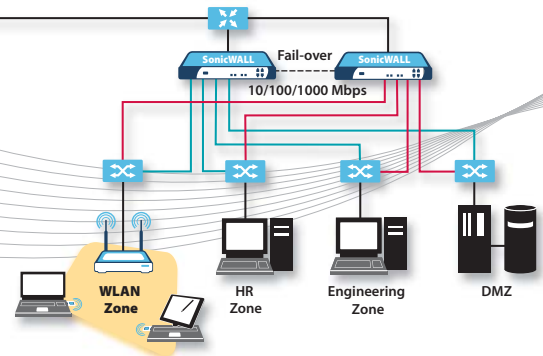


Distributed Office and Remote User Security

With its powerful VPN performance and enhanced NAT modes, the PRO 5060 is ideal for securely and easily linking remote/branch offices, partner sites and remote workers.

Features

- 500 Mbps hardware-accelerated IPSec VPN
- Advanced NAT modes for flexible site-to-site connectivity and management
- Compatibility with most major security and VPN appliance manufacturers
- Secondary VPN gateway support with "Dead Peer Detection" for automatic VPN Fail-over
- Easy-to-use Global Security Client/Global VPN Clients for remote users
- Third-party CA certificate support
- Flexible application of firewall rules for VPN traffic on a user or group basis
- DHCP over VPN capability for centralized IP management
- Award-winning Global Management System (GMS) and SonicWALL ViewPoint® for comprehensive management and reporting

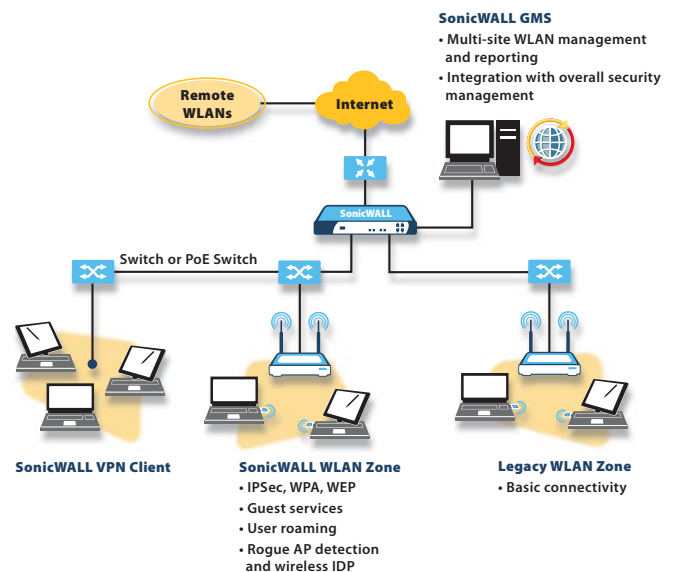


Distributed WLAN Security and Management

The PRO 5060's distributed WLAN capabilities rival those of the most sophisticated WLAN switch vendors on the market. With SonicWALL, you can easily integrate advanced WLAN services within the organization's existing network and security architectures. And with over 500 Mbps of IPSec VPN throughput, the PRO 5060 can aggregate a massive number of access points (APs) for large WLAN deployments.

Features

- Complete integration of WLAN security into overall network security management and reporting system
- Centrally manage and configure SonicPoints™ from PRO 5060 security appliances
- SonicPoints are intelligent, 802.11a/b/g satellite APs that allow wireless intrusion detection, secure wireless roaming, wireless guest services and more
- Standards-based WEP, WPA and IPSec encryption options
- Automatic discovery and provisioning enabled by the SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP)
- Utilizes SonicWALL's easy-to-use Global VPN Client software for secure IPSec wireless communications



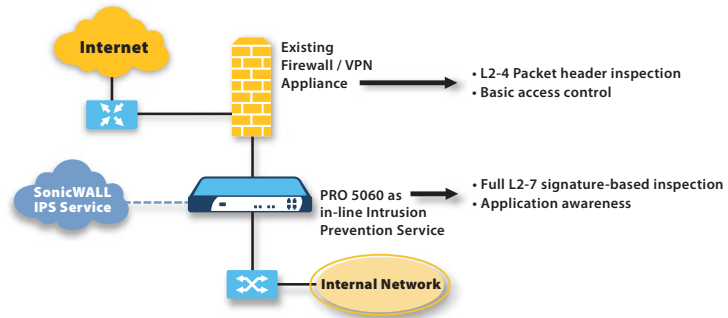
One of the
industry's most
comprehensive
intrusion
prevention
solutions

PRO 5060 In-Line Intrusion Prevention Mode for Legacy Firewall Deployments

The SonicWALL PRO 5060 is the industry's most comprehensive security and intrusion prevention solution, combining a dynamically updated database of over 1,800 attack and vulnerability signatures with a lightning-fast deep packet inspection engine that guarantees high levels of performance under load conditions. The PRO 5060 is ideal as an integrated security appliance, or as a stand-alone intrusion prevention appliance for legacy firewall deployments.

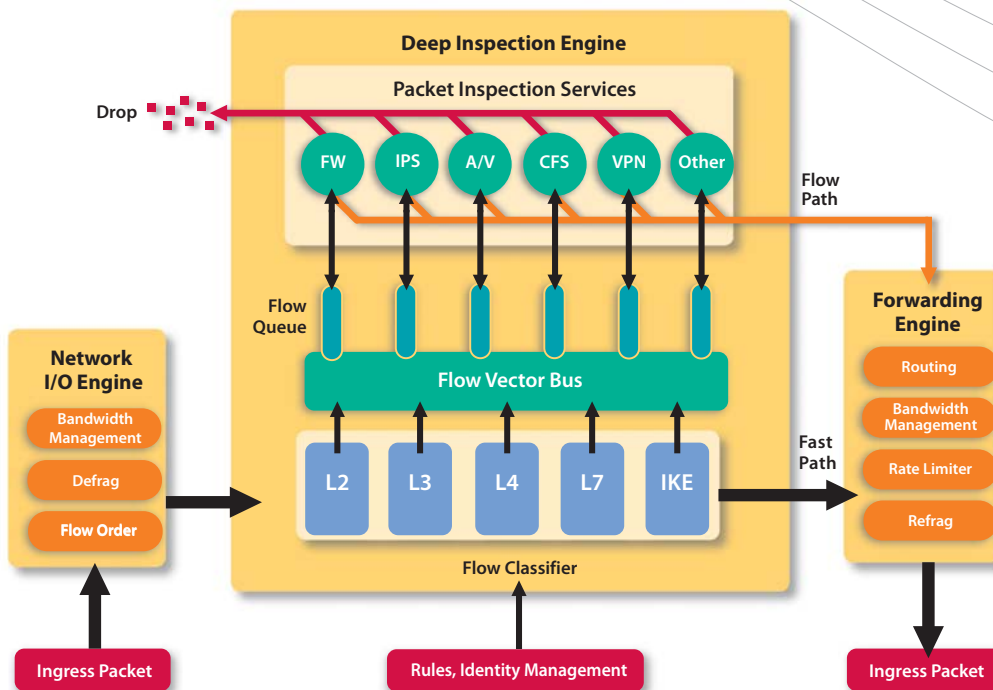
Features

- 1,800+ attack and vulnerability signature database is constantly updated to protect against the latest threats
- Maximum protection from Trojans, worms, DoS/DDoS attacks, and blended threats—even sophisticated polymorphic attacks
- Protection against threats carried by and management of instant messaging and peer-to-peer applications
- Inter-zone intrusion prevention protects against internal attacks targeting network segments
- Transparent-mode capability allows seamless integration into most existing network topologies



The nature of network security threats has evolved. While basic L2-4 firewall functionality is still a mandatory element of network security, new breeds of dynamic attacks are wreaking more havoc than ever before. Not only can these attacks render a traditional firewall useless, they also require a constantly updated attack database that guarantees protection. And they absolutely must have a hardware platform that can withstand the rigors of real-time intrusion prevention while maintaining high levels of performance.

SonicWALL Deep Inspection Architecture



SonicWALL's **Deep Inspection Architecture** is a highly scalable approach to multi-layer network security. Combining parallel stream processing with our custom-developed flow classification and flow vector bus technology, SonicWALL appliances deliver exceptional levels of performance under the most demanding of security requirements.

