



The SonicWALL PRO 4100

PRO SERIES

Real-time threat protection and internal security

- **Powerful re-assembly free deep packet inspection engine**
- **Real-time gateway anti-virus, anti-spyware and intrusion prevention**
- **Innovative SonicWALL Clean VPN**
- **Comprehensive application control**
- **Integrated high availability and load balancing**
- **Standards-based Voice over IP**
- **Secure distributed wireless LAN services**
- **Onboard Quality of Service (QoS) features**
- **Advanced security and networking features**

Organizations of all sizes rely on their networked infrastructure as the primary means of communication and productivity. These same networks are under attack from a continually-evolving array of dynamic threats. Securing data from external as well as internal threats across distributed, often highly-complex architectures is challenging. Today's organizations need a solution that not only provides high-speed threat protection at the gateway, but also the flexibility and port density to segment the network into workgroups for extended internal security.

The SonicWALL® PRO 4100 solves these issues with the first real-time unified threat management firewall appliance utilizing 10 gigabit interfaces to deliver high-speed internal and external network protection for corporate central sites, distributed environments and data centers. The PRO 4100 is based on a dynamically updateable platform that includes an extensive array of advanced networking and configuration flexibility features in an accessible, affordable platform that is easy to deploy and manage in a wide variety of environments.

Features and Benefits

Powerful re-assembly free deep packet inspection engine eliminates threats over unlimited file sizes and unrestricted concurrent connections, offering ultimate scalability.

Real-time gateway anti-virus, anti-spyware anti-SPAM and intrusion prevention secures the network against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans, phishing attacks and software vulnerabilities such as buffer overflows.

Innovative SonicWALL Clean VPN™ deep packet inspection architecture assures mobile user connections and branch office traffic are decontaminated to prevent vulnerabilities and malicious code from being introduced into the corporate network from remote connections.

Comprehensive application control prevents non-business traffic such as peer-to-peer and instant messaging applications at the administrator's discretion.

Integrated high availability and load balancing features maximize total network bandwidth and maintain network uptime, ensuring uninterrupted access to critical resources.

Standards-based Voice over IP capabilities provide the highest levels of security for every element of the VoIP infrastructure, from communications equipment to VoIP-ready devices such as SIP Proxies, H.323 Gatekeepers and Call Servers.

Secure distributed wireless LAN services enable the appliance to function as a secure wireless switch and controller that automatically detects and configures SonicPoints™, SonicWALL wireless access points, for secure remote access in distributed network environments.

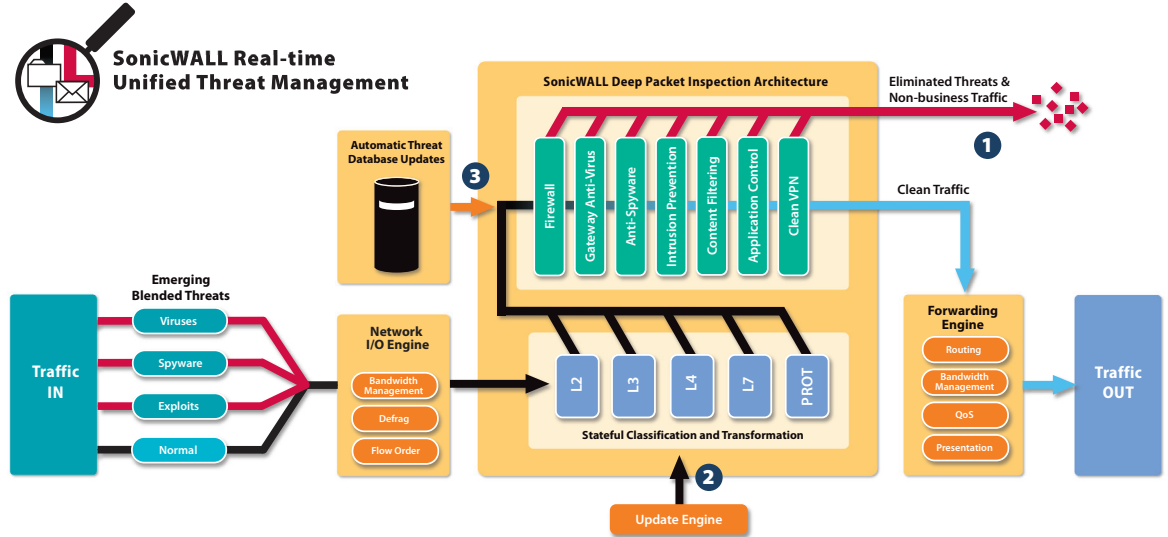
Onboard Quality of Service (QoS) features use industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators to provide powerful and flexible bandwidth management that is vital for Voice over IP (VoIP), multimedia content and business-critical applications.

Advanced security and networking features include 802.1q VLANs, enterprise routing support, WAN/WAN failover, zone and object-based management, load balancing, advanced NAT modes and more, providing granular configuration flexibility and comprehensive protection.



Robust Internal Security

Network security and control is accomplished through a robust and flexible platform



*Real-time
unified threat
management
protection
in an affordable,
easy-to-manage
platform*

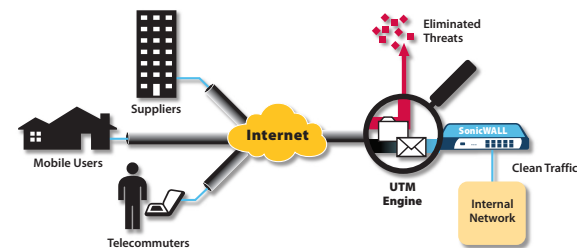
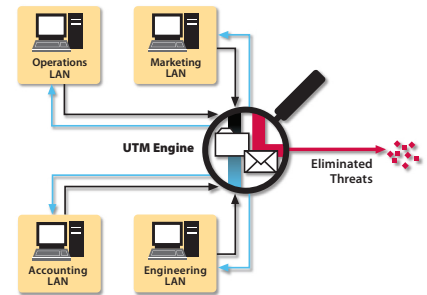
- 1 The SonicWALL deep packet inspection architecture inspects traffic to ensure network risks such as viruses, worms, Trojans, spyware, phishing attacks, emerging threats and Internet misuse are properly prevented.
- 2 The uniquely scalable approach scans traffic in real-time as it moves through the engine without having to stall traffic in memory. This allows threats to be identified and eliminated over unlimited file sizes and

unrestricted concurrent connections without any interruptions. No other solution offers the same scalability and limitless protection.

- 3 Because threats are always evolving, dynamic network protection is accomplished through automated and continuous security updates, ensuring the PRO 4100 can prevent emerging threats without requiring any administrator intervention.

Internal Security

The PRO 4100 delivers robust “trusted network” protection across 10 gigabit Ethernet interfaces. Inter-departmental traffic is inspected to prevent the spread of threats and attacks that occur on the internal network. The high-speed prevention engine detects threats over both virtual and connected wireless LANs, delivering end-to-end protection throughout the network.

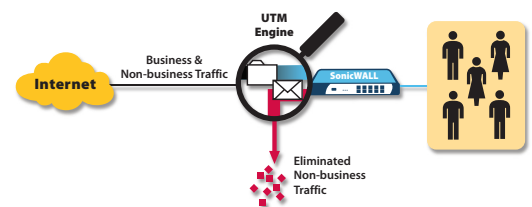


SonicWALL Clean VPN

The PRO 4100 includes innovative SonicWALL Clean VPN technology that prevents vulnerabilities and malicious code by decontaminating mobile user connections and branch office traffic before they enter the corporate network. Based on a real-time deep packet inspection engine, the PRO 4100 eliminates viruses, worms, Trojans, spyware and malicious code without any user intervention.

Intelligent Application Control

Business applications are sensitive to bandwidth, speed and compatibility. The PRO 4100 optimizes business critical traffic such as VoIP and corporate server traffic for complete end-to-end bandwidth and speed management. Other applications such as instant messaging, peer-to-peer and multimedia pose both productivity and security issues. The PRO 4100 affords administrators complete control over the usage of these non-business applications.

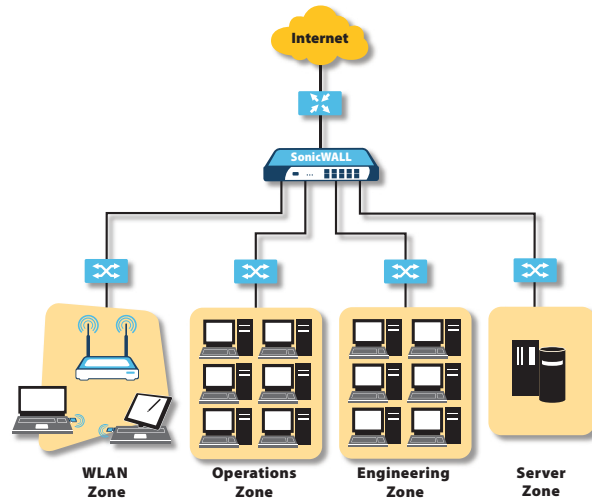


Central-site Primary Gateway

The PRO 4100 is ideal as a security gateway for central site deployments and distributed environments with a focus on both external as well as internal security. Advanced networking features allow seamless deployment into virtually any environment.

Features

- Suite of advanced security services for comprehensive multi-layered protection
- Zone security for segmenting internal groups and eliminating threats between network groups
- Granular QoS features prioritize business-critical traffic and applications over non-essential functions
- SonicWALL Clean VPN ensures remote users do not infect the corporate site location
- Secondary VPN gateway support with automatic VPN failover

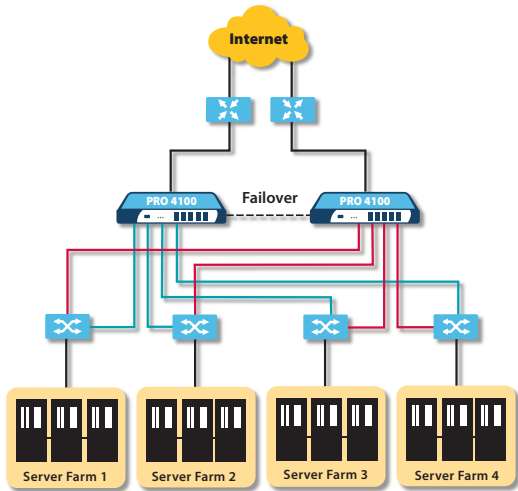


Data Center Environments

With its powerful VPN performance and enhanced NAT modes, the PRO 4100 is ideal for segmenting high-speed data center environment traffic.

Features

- 800 Mbps stateful packet inspection firewall throughput
- Suite of advanced security services for comprehensive multi-layered protection
- Zone security for segmenting internal groups and eliminating threats between internal groups
- Object-based management for easy administration
- Granular QoS features prioritize server traffic to meet the most demanding service level agreements
- Integrated high availability (HA) and load balancing features guarantee network uptime and maximize total network bandwidth

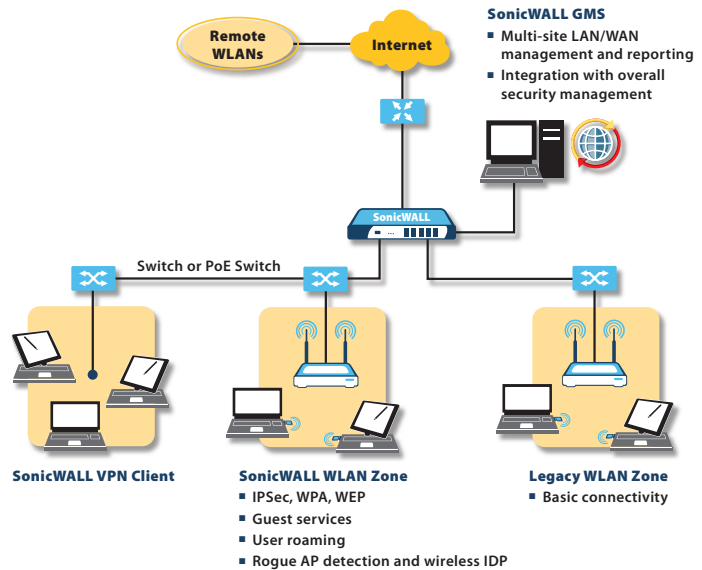


Secure WLAN Security and Management

The PRO 4100 features secure distributed WLAN capabilities that rival those of the most sophisticated WLAN switch vendors on the market.

Features

- Complete integration of WLAN security into overall network security management and reporting system
- Centrally manage and configure SonicPoints, 802.11a/b/g and 802.11n/b/g dependent access points from PRO 4100 security appliances to enable wireless intrusion detection, secure wireless roaming, wireless guest services and more
- Zone security for segmenting internal groups and eliminating threats between internal segments
- Standards-based WEP, WPA and IPSec encryption options



Specifications

SonicWALL PRO 4100

Firewall

Nodes Supported	Unrestricted
Stateful Throughput*	800 Mbps
Deep Packet Inspection	Protection from viruses, spyware, worms, Trojans and application layer attacks. Requires Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service for signature updates
Gateway Anti-Virus Throughput**	300 Mbps
Intrusion Prevention Throughput**	300 Mbps
Connections	600,000
Policies	10,000
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks

VPN

3DES/AES Throughput***	350 Mbps (MDS, 168-bit)
Site-to-Site VPN	3,500 tunnels max
Remote Access VPN	5,000 tunnels max (1,500 clients bundled)
Encryption	DES, 3DES, AES (128, 192, 256-bit)
Authentication	MDS, SHA-1
Key Exchange	Manual Key, PKI (X.509), IKE
XAUTH/RADIUS	Yes
L2TP/IPSec	Yes
Flexible VPN Termination	Any port for site-to-site and remote access tunnels
Certificate Support	Verisign®, Thawte, Baltimore, RSA Keon, Entrust® and Microsoft® CA for SonicWALL-to-SonicWALL VPN
Dead Peer Detection	Yes
DHCP Over VPN	Yes
IPSec NAT Traversal	Yes, NAT_Tv00 and v03
Redundant VPN Gateway	Yes
Single-arm VPN	Yes

Deep Inspection Security Services

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention	Dynamic signature database prevents intrusions, worms, spyware and application exploits. Peer-to-peer and instant messaging control and signature updates through Distributed Enforcement Architecture ¹
Content Filtering Service (CFS) Standard Edition	URL, keyword and content scanning; ActiveX, Java Applet and Cookie Blocking ²
Gateway-enforced Network Anti-Virus	HTTP/S, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients ³ ; E-mail attachment blocking

* Testing Methodologies: Maximum performance based on RFC 2544 (for firewall)
Actual performance may vary depending on network conditions and activated services

** Throughput measured using HTTP throughput test

*** VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544

1) 30-day service included 2) 30-day service included 3) 30-day 50-user service included

Networking

DHCP	Relay, internal server (4,096 leases)
NAT Modes	1:1, 1:many, many:1, flexible NAT (overlapping IPs), PAT, transparent mode
VLANs Supported	300
Authentication	Internal user database, RADIUS, LDAP, Microsoft Active Directory
VoIP	Full H.323v1-5, SIP, gatekeeper support, inbound/outbound bandwidth management, call tracking and monitoring, full interoperability with most VoIP gateway and communications devices
Routing Protocols	OSPF (Open Shortest Path First) and RIP (Router Information Protocol)

System

Zone Security	Yes
Object-based Management	Yes
Management	Local CLI, Web GUI, SNMP v2; WebTrends, Global Management with SonicWALL GMS
Reporting	Comprehensive reporting and graphing, automated scheduling, bandwidth monitoring with SonicWALL ViewPoint™ reporting suite
WAN/WAN Failover	Yes, with percent-based, round-robin and spill-over load balancing
Hardware Failover Standards	Active/Passive TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS

Hardware

Interfaces	(10) 10/100/1000 auto-sensing Ethernet, (1) Serial Port
Fans	Redundant, high-capacity fans
Power Supply	250 W
Power Input	100-240 VAC, 60-50 Hz, 6-3 A
Max Power Consumption	163 W
Total Heat Dissipation	556 BTU
Processors	Intel® Pentium main processor, Cavium Nitrox cryptographic accelerator
Dimensions	17.00 x 16.25 x 1.75 in 43.18 x 41.23 x 4.45 cm
Weight	15.05 lbs (6.83 kg)
Major Regulatory Compliance	FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, BSMI Class A, MIC, NOM, UL, cUL, TUV/GS, CB
Environment	40-105° F, 5-40° C
Humidity	10-90% non-condensing
MTBF	7.0 years



SonicWALL PRO 4100 (US/Canada)
01-SSC-5400

SonicWALL Content Filtering Premium Business Edition for PRO 4100
01-SSC-5653

SonicWALL Content Filtering Premium Gov/Ed Edition for PRO 4100
01-SSC-5663

SonicWALL Complete Anti-Virus (100 User License)
01-SSC-3423

SonicWALL SonicPoint (US/Canada)
01-SSC-5522

SonicWALL SonicPoint G (US/Canada)
01-SSC-5536

SonicWALL Support 8x5 for PRO 4100
01-SSC-5638

SonicWALL Support 24x7 for PRO 4100
01-SSC-5639

NOTE: PRO 4100 ships with 1 year of free Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service.

PRO 4100 Front



Console port
10 10/100/1000 gigabit Ethernet interfaces

PRO 4100 Rear



Redundant, high-capacity fans

SonicWALL Value-added Security Services

SonicWALL Internet security appliances integrate seamlessly with an expanding array of value-added security services to provide a comprehensive security solution. Gateway anti-virus, anti-spyware, intrusion prevention, desktop-enforced anti-virus and content

filtering can be enforced over both the wired and wireless LANs. For more information on SonicWALL security services, please visit our Web site at <http://www.sonicwall.com/products/vpnsoft.html>.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

