



PRODUCT LINE

High-performance Solutions that Engineer the Cost Out of Secure Networking

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[™]

A Recognized Leader From our founding in 1991, SonicWALL, Inc. has been dedicated to our customers' needs, believing solutions can and should perform multiple functions—especially those that sit at the gateway. SonicWALL was the first to integrate additional capabilities into a firewall appliance, including VPN and content filtering.

Today, we are a leader in network security, secure remote access, Web and e-mail security and backup and recovery with offerings like our market leading Unified Threat Management solutions, with enterprise-class, appliance-based products and services that provide anti-virus, anti-spyware and Intrusion prevention, for wired and wireless networks of all sizes, in a single package. More than one million SonicWALL network security and data protection solutions have shipped to protect millions of computer users in small, medium and distributed networks, enterprise, e-commerce, education, healthcare, retail/point-of-sale and government markets from a wide range of security and data threats, while improving network productivity.

SonicWALL's commitment to this market is about more than products: it encompasses all the resources and ongoing vision necessary to keep network security and data protection solutions ahead of ever-evolving threats. SonicWALL strategic partners are some of the best-known names in information technology and serve the global market with over 15,000 qualified, customer-focused resellers and distributors. SonicWALL also provides comprehensive technical support, and maintains the finest team of security and data protection professionals in the industry, devoted to continuous innovation in integrated network security, secure remote access, Web and e-mail security, backup and recovery and policy and management solutions.

Overview2

Network Security Solutions

Network Security Solution Summary3

E-Class Solutions.....4

SMB and Branch Office Solutions.....6

Wireless Enablers10

Subscription Services, Licences and Firmware11

Secure Remote Access Solutions

Secure Remote Access Solution Summary12

E-Class Solutions.....12

Add-on Features.....13

SSL VPN SMB and Branch Office Solutions14

Add-on Features.....15

Email and Web Security Solutions

E-mail Security Solution Summary16

E-Class Solutions.....16

SMB Solutions.....17

Subscription Services.....17

Web Solutions18

Backup and Recovery Solutions

Backup and Recovery Solution Summary.....19

SMB Solutions.....19

Subscription Services.....20

Policy and Management Solutions

Global Management System.....21

SonicWALL ViewPoint.....21

MySonicWALL.....21

Global Support Services

Dynamic Support 8x5 and 24x7.....22

Comprehensive Global Management System22

Deep Protection The vision of SonicWALL® is to relentlessly engineer the costs and complexity out of high-performance secure networking, freeing business resources to be more productive. A recognized innovation leader, SonicWALL creates elegant solutions that provide dynamic high-performance protection while simultaneously driving down costs of acquisition, deployment and administration. Easy to use and manage, SonicWALL appliance-based solutions and subscription services scale to enhance the productivity and performance of any sized organization from small businesses to large enterprises, including government, retail point-of-sale, healthcare and service providers. SonicWALL safeguards networks—and organizations—with a comprehensive portfolio of scalable and interoperable solutions that provide threat management, secure mobility, business continuity and regulatory compliance.

Threat Management Internet threats have transformed from mere annoyances to sophisticated malicious attacks that can dramatically impede business. SonicWALL® solutions offer comprehensive protection against these intricate and evolving threats by seamlessly integrating network security, Web and e-mail security. SonicWALL Network Security provides deep protection against viruses, worms, Trojans, spyware and intrusions while delivering enterprise-levels of network performance at load conditions. SonicWALL Web Security provides greater control to block inappropriate and illegal Web sites as well as to control the use of instant messaging and peer-to-peer applications. SonicWALL Email Security completes the offering with effective protection against spam and phishing attacks so employees only read legitimate e-mails and are not exposed to fraudulent e-mails. SonicWALL all-in-one solutions greatly simplify the centralized management of local, remote and mobile network services while protecting key information and communications resources in a cost-effective manner.

Mobility The ubiquity of mobile technology, the increasingly distributed workforce, and the demand for business continuity have made mobility a business imperative. SonicWALL provides organizations of all sizes with mobility solutions over broadband, wireless and dial-up connections. Integrated with SonicWALL Unified Threat Management protection, SonicWALL network security provides secure site-to-site connections using IPSec VPN. Combining these appliances with self-configuring SonicPoints instantly provides provisional temporary networks with secure wireless hotspot connectivity. The SonicWALL TZ 190 allows temporary sites to establish secure 3G wireless broadband virtually anywhere in an instant without a fixed Internet connection. Additionally, SonicWALL SSL VPNs extend secure mobile access to virtually any remote location over standard Web browsers or mobile devices including wireless PDAs and smartphones. SonicWALL SSL VPNs also offer unsurpassed levels of granular control.

Business Continuity Whether triggered by a major disaster or a neighborhood power outage, any disruption to normal business operations can mean missed opportunities, lost revenue, and a damaged reputation. SonicWALL offers business continuity and recovery solutions for any size organization. With SonicWALL SSL VPN solutions, isolated workers can remain as productive from home or other contingent locations as if they were in the office. SonicWALL Backup and Recovery solutions provide automatic, real-time, hands-free disk-based data backup for servers, laptops and PCs. The SonicWALL Continuous Data Protection (CDP) Series protects files locally as well as to an offsite location to ensure they can be recovered instantly and from any point in time.

Compliance Security threats exist within a network as well. Whether intentionally or accidentally, employees can transmit inappropriate content, intellectual property or confidential data, resulting in significant damage or breach of industry or government regulations like HIPAA or Sarbanes-Oxley. Noncompliance may result in fines, executive liability and a damaging loss of credibility. SonicWALL can help any organization meet mandated regulations, with best-in-class encryption technology and deep packet inspection to ensure “Clean VPN,” connectivity. SonicWALL SSL VPN solutions offer data encryption and authentication, granular access control, policy management, logging capability, and flexible authentication architecture. SonicWALL Email Security provides easy creation of outbound policies, intelligent identification of noncompliant e-mails, robust monitoring and reporting tools, and a range of remediation options. And, SonicWALL Content Security appliances protect your network from illicit or unproductive Web content. Finally, the award-winning SonicWALL Global Management System (GMS) provides comprehensive audit trails with centralized real-time monitoring, and comprehensive policy and compliance reporting.

SonicWALL's enterprise level E-Class Network Security Appliance (NSA) uses a multi-core microprocessor that can run deep packet inspection full throttle without compromising network speed.

SonicWALL Network Security

Other existing network security solutions can be technologically limited, notoriously expensive or painful to deploy and use. SonicWALL eliminates these concerns by focusing on engineering the cost and complexity out of a high performance security infrastructure. This frees business resources to be more productive. SonicWALL Network Security solutions incorporate multiple security technologies in a single platform to provide high-speed threat protection, reliable communications, low total cost of ownership and flexible connectivity options.

SonicWALL *E*CLASS

SonicWALL Enterprise Solutions: E-Class NSA Series At-A-Glance

The SonicWALL E-Class Network Security Appliance (NSA) Series is an industry first—using a re-assembly free deep packet inspection engine in combination with multi-core specialized security microprocessors to deliver gateway anti-virus, anti-spyware and intrusion prevention at high-speed so you don't have to sacrifice network performance. Combining a powerful deep packet inspection firewall with multiple layers of protection technology and a suite of high-availability features, the NSA Series offers the ultimate choice for a variety of enterprise deployments including distributed environments, campus networks and data centers.

The E-Class NSA appliances are engineered to be the most scalable, high performance and reliable multi-function threat appliances in class. Taking protection to new levels of control is Application Firewall, a set of customizable protection tools that affords administrators precise control over network traffic. To meet the operational reliability enterprise-class network demand, the E-Class NSA Series incorporates a suite of high availability features at the hardware and system level to maximize uptime and improve security coverage. The E-Class NSA Series lowers management complexity by providing an extensive array of advanced network configuration features that ease deployment and integration. This makes NSA an ideal solution for organizations that require high performance network security deployed across a wide variety of environments. The E-Class NSA Series delivers:

- Enterprise-class deep packet inspection (DPI) and Application Firewall for every packet, every protocol, over every interface
- Revolutionary multi-core performance utilizing up to 16 cores for ultra high-speed multi-layer threat protection over both external and internal networks
- Ultimate scalability in eliminating threats of unlimited file size and unrestricted concurrent connections by utilizing a reassembly-free deep packet inspection engine
- Dynamically updateable and customizable security defense
- Uncompromising business continuity and high availability protection



SonicWALL ECLASS

Network Security Solutions—SonicWALL E-Class NSA Series

SonicWALL NSA E7500

The SonicWALL E-Class Network Security Appliance (NSA) E7500 is the flag ship of the E-Class NSA product family designed to be the most scalable, high performance and reliable multi-function threat appliance in its class. It protects against a vast spectrum of network attacks with unprecedented speed and reliability. This protection is enabled through the NSA E7500 16-core architecture, a parallel performance design for ultra high-speed threat protection and deployment scalability. Taking protection to new levels of control is Application Firewall, a set of customizable protection tools that empowers administrators with precise control and inspection over network traffic. The NSA E7500 comes standard with four gigabit copper Ethernet ports, four expandable SFP ports for deployment flexibility and an LCD management screen for instant configuration access. Operational reliability is delivered through a suite of high availability features at the hardware level with dual power supplies and fans and at the system level with Stateful failover to dramatically improve uptime. The NSA E7500 offers enterprise customers an extensive array of advanced network and deployment flexibility features for use in large scale enterprise network deployments.



SonicWALL NSA E6500

The SonicWALL E-Class Network Security Appliance (NSA) E6500 is engineered to meet the needs of the expanding enterprise network by providing a high performance, scalable, multifunction threat prevention appliance. The NSA E6500 has been engineered to take advantage of specialized multi-core processing technology, providing parallel traffic processing, in conjunction with SonicWALL's re-assembly free deep packet inspection engine. The NSA E6500 provides enterprise administrators a high performance secure platform to combat the changing threat landscape. Using tools such as Application Firewall network administrators can take advantage of customizable protection tools that empower network administrator's precise control and inspection over network traffic. The NSA E6500 comes standard with eight gigabit copper Ethernet ports for deployment flexibility and includes a management LCD screen for ease of deployment.



SonicWALL NSA E5500

The SonicWALL E-Class Network Security Appliance (NSA) E5500 is high performance, multi-service network security platform engineered to be the work horse of the enterprise network environment. Taking advantage of SonicWALL's re-assembly free deep packet inspection engine and an 8-core processor technology providing parallel traffic processing, the NSA E5500 delivers exceptional deep packet inspection performance for the enterprise network environment. The NSA E5500 comes standard with eight gigabit copper Ethernet ports for deployment flexibility and includes a management LCD screen for ease of deployment. This solutions offers enterprise network administrators an array of enterprise networking features, designed to provide lowered management complexity, and unrivalled value.

Network Security Solutions

Feature	NSA 5500	NSA 6500	NSA 7500
SonicOS Supported	SonicOS Enhanced 5.0 (or higher)	SonicOS Enhanced 5.0 (or higher)	SonicOS Enhanced 5.0 (or higher)
Users and Nodes	Unrestricted	Unrestricted	Unrestricted
Network Interfaces	(8) 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface	(8) 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface	(4) 10/100/1000 Copper Gigabit Ports and (4) SFP Ports, 1Gbe HA Interface, 1 Console Interface
CPU Cores	8	16	16
Power Supply	Single 250W ATX	Single 250W ATX	Dual 250W ATX, Hot Swappable
Cooling System (Fans)	Dual Fans, Hot Swappable	Dual Fans, Hot Swappable	Dual Fans, Hot Swappable
VLAN Interfaces	256	256	512
High Availability	Active/Standby Statesync	Active/Standby Statesync	Active/Standby Statesync
Stateful Throughput¹	2 Gbps	3 Gbps	5.5 Gbps
3DES/AES Throughput¹	1.5 Gbps	2.5 Gbps	4 Gbps
Gateway Anti-Virus Throughput²	750 Mbps	900 Mbps	1.8 Gbps
Intrusion Prevention Throughput²	550 Mbps	850 Mbps	1.2 Gbps
UTM Performance²	400 Mbps	750 Mbps	1.0 Gbps
New Connections Per Second	10,000	19,000	25,000
Total Concurrent Connections	700,000	750,000	1,000,000
Site-to-Site VPNs	4,000	6,000	10,000
Zone Security	Yes	Yes	Yes
Object-based Management	Yes	Yes	Yes
Policy-based NAT	Yes	Yes	Yes
WAN/WAN Failover	Yes	Yes	Yes
Load Balancing	Yes	Yes	Yes
Integrated Wireless Switch and Controller	Yes	Yes	Yes
Spam Blocking	Yes	Yes	Yes
Voice over IP (VoIP)	Yes	Yes	Yes
IKEv2 VPN	Yes	Yes	Yes
Secure Remote Management (SSHv2 Support)	Yes	Yes	Yes
Multiple SSIDs using VAP	Yes	Yes	Yes
Dynamic Address Objects	Yes	Yes	Yes
Layer 2 Bridge Mode	Yes	Yes	Yes
802.1q VLANs	Yes	Yes	Yes
RIPv2 and OSPF Routing	Yes	Yes	Yes
Single Sign On (SSO)	Yes	Yes	Yes
Application Firewall	Yes	Yes	Yes
SSL Control	Yes	Yes	Yes

¹Firewall and VPN throughput measured using UDP traffic adhering to RFC 2544

²Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP Performance test

**Real-time
unified threat
management
provides deep
protection for
SMB and Branch
Offices**



SonicWALL SMB and Branch Office Solutions: PRO Series At-A-Glance

The SonicWALL PRO Series is a multi-service security platform for companies requiring rock solid network protection coupled with fast, secure VPN access for remote employees. Built on the innovative SonicWALL deep packet inspection architecture, the PRO Series combines gateway anti-virus, anti-spyware, intrusion prevention, anti-spam, content filtering and secure wireless capabilities with a deep packet inspection firewall and IPSec VPN for real-time, granular protection against malicious application layer attacks. With six distinct, highly integrated security appliances, the PRO Series delivers the scalability and performance growing networks require.

Every PRO Series appliance packs the benefits of the SonicWALL SonicOS operating system into an affordable, rack-mount appliance, providing enterprise-class performance, advanced features and configuration flexibility. Standard on the PRO 4060/4100/5060 and an optional upgrade on the PRO 1260/2040/3060, feature-rich SonicWALL SonicOS Enhanced adds a suite of redundancy, management and wireless LAN features typically associated with more expensive appliances including Quality of Service (QoS), ISP failover, WAN redundancy, load balancing, object/zone-based management, policy-based NAT, wireless guest services and more.

PRO Series appliances are ICSA-certified and can be easily managed remotely as part of a multi-firewall and VPN environment through a Web interface or using the industry-leading SonicWALL Global Management System (GMS).

SonicWALL PRO 5060

The PRO 5060, SonicWALL's flagship PRO Series appliance, provides an enterprise-class, multi-service, gigabit network security platform that protects users and critical network resources from the dynamic, sophisticated threats that put today's corporate networks at risk. Available in 10/100/1000 copper and copper/fiber interface configurations, the PRO 5060 incorporates advanced networking and security features such as 802.1q virtual LANs, dynamic RIP and OSPF routing, Quality of Service (QoS) and more, making it an ideal solution for data-intensive network environments. The PRO 5060 includes SonicWALL ViewPoint® reporting software, one year of Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service and 2,000 Global VPN Client licenses for secure remote access.

SonicWALL PRO 4100

The PRO 4100 is an enterprise-class unified threat management platform that delivers real-time internal and external network protection to corporate networks, distributed environments and data centers. The PRO 4100 combines high-speed gateway anti-virus, anti-spyware, intrusion prevention and powerful deep packet inspection capabilities with an extensive array of advanced networking and configuration flexibility features in an accessible, affordable platform that is easy to deploy and manage. With 10 configurable gigabit Ethernet interfaces, SonicWALL Clean VPN technology and built-in secure wireless LAN functionality, the PRO 4100 is an ideal solution for a host of wired and wireless applications requiring high-speed access and heavy workgroup segmentation. The PRO 4100 includes SonicWALL ViewPoint reporting software and 1,000 Global VPN Client licenses for secure remote access.

SonicWALL PRO 4060

The PRO 4060 is a high-performance, multi-service network security platform designed to meet the critical security requirements of medium-to-large sized networks. With 190 Mbps of hardware-accelerated VPN performance, enhanced VPN capabilities and 1,000 Global VPN Client licenses, the PRO 4060 is the ideal solution for even the most complex remote connectivity environments. Six configurable 10/100 Ethernet interfaces allow administrators to create multiple LANs, WANs, WLANs, DMZs and custom-defined zones for greater network configuration flexibility. The PRO 4060 includes SonicWALL ViewPoint reporting software and 1,000 Global VPN Client licenses for secure remote access.

SonicWALL PRO 3060

The PRO 3060 is a high-performance, network security platform designed to meet the business continuity needs of mid-sized networks. Powered by the SonicWALL next-generation SonicOS operating system, the PRO 3060 delivers powerful firewall throughput and 3DES/AES VPN concentration. An upgrade on the PRO 3060, SonicOS Enhanced unlocks critical redundancy features such as hardware failover, WAN/ISP failover and the ability to fail over to a secondary VPN gateway, ensuring continuous network uptime. Six configurable 10/100 Ethernet interfaces allow administrators to create multiple LANs, WANs, WLANs, DMZs and custom-defined zones for greater network configuration flexibility.



SonicWALL PRO 2040

The PRO 2040 is an award-winning network security platform designed to meet the business continuity needs of small-to-mid sized networks. Optimized for networks of up to 200 nodes or 50 network locations, the PRO 2040 delivers powerful firewall throughput and 3DES/AES VPN concentration. An upgrade on the PRO 2040, SonicOS Enhanced provides hardware failover, WAN/ISP failover and the ability to fail over to a secondary VPN gateway, ensuring continuous network uptime. Four configurable 10/100 Ethernet interfaces allow administrators to create multiple LANs, WANs, WLANs, DMZs and custom-defined zones for greater network configuration flexibility.

SonicWALL PRO 1260

The PRO 1260 is a total security and switching platform for small network applications. The PRO 1260 combines deep packet inspection firewall and IPSec VPN capabilities with an intelligent, wire-speed, 24-port auto-sensing MDIX switch in a single, convenient network security and LAN switching platform. This unique appliance can be configured either as an unmanaged switch under SonicOS Standard or as an intelligent managed LAN switching platform through the powerful SonicWALL PortShield architecture enabled in SonicOS Enhanced. The innovative PortShield architecture allows all 24 ports on the PRO 1260 to be independently and easily configured into custom security zones (PortShield groups), each with its own “virtual firewall,” along with granular rate limiting on each interface.

Feature	PRO 1260	PRO 2040	PRO 3060	PRO 4060	PRO 4100	PRO 5060
Nodes	Unrestricted					
Interfaces	27 Ethernet	3/4* Ethernet	3/6* Ethernet	6 Ethernet	10 Gigabit	6 Gigabit
SonicOS Standard/Enhanced	Standard	Standard	Standard	Enhanced	Enhanced	Enhanced
Upgrade to SonicOS Enhanced	Yes	Yes	Yes	N/A	N/A	N/A
Stateful Throughput¹	90 Mbps	200 Mbps	300 Mbps	300+ Mbps	800 Mbps	2.4 Gbps
Gateway Anti-Virus Throughput²	8 Mbps	40 Mbps	99 Mbps	182 Mbps	300 Mbps	339 Mbps
Intrusion Prevention Throughput²	8 Mbps	39 Mbps	98 Mbps	170 Mbps	300 Mbps	279 Mbps
Connections	6,140	32,000	128,000	500,000	600,000	750,000
Policies	150/300*	150/1,000*	300/3,000*	5,000	10,000	15,000
3DES/AES Throughput³	30+ Mbps	50 Mbps	75 Mbps	190 Mbps	350 Mbps	700 Mbps
Site-to-Site VPN Tunnels	25	50	500/1,000*	3,000	3,500	4,000
Remote Access VPN Tunnels (Max)	50	100	500	3,000	4,500	6,000
Remote Access VPN Tunnels (Bundled)	5	10	25	1,000	1,500	2,000
Zone Security	Yes*	Yes*	Yes*	Yes	Yes	Yes
Object-based Management	Yes*	Yes*	Yes*	Yes	Yes	Yes
Policy-based NAT	Yes*	Yes*	Yes*	Yes	Yes	Yes
WAN/WAN Failover	Yes*	Yes*	Yes*	Yes	Yes	Yes
Load Balancing	Yes*	Yes*	Yes*	Yes	Yes	Yes
Hardware Failover	No	Yes*	Yes*	Yes	Yes	Yes
Stateful Hardware Failover	No	No	Yes**	Yes**	Yes**	Yes**
Integrated Wireless Switch and Controller	Yes*	Yes*	Yes*	Yes	Yes	Yes
Spam Blocking	Yes*	Yes*	Yes*	Yes	Yes	Yes
Voice over IP (VoIP)	Yes	Yes	Yes	Yes	Yes	Yes
IKEv2 VPN	Yes*	Yes*	Yes*	Yes	Yes	Yes
Secure Remote Management (SSHv2 Support)	Yes*	Yes*	Yes*	Yes	Yes	Yes
Multiple SSIDs using VAP	No	Yes**	Yes**	Yes**	Yes**	Yes**
Dynamic Address Objects	Yes**	Yes**	Yes**	Yes**	Yes**	Yes**
Layer 2 Bridge Mode	No	Yes**	Yes**	Yes**	Yes**	Yes**
802.1q VLANs	No ¹	Yes*	Yes*	Yes	Yes	Yes
RIPv2 and OSPF Routing	Yes*	Yes*	Yes*	Yes	Yes	Yes
Single Sign On (SSO)	Yes**	Yes**	Yes**	Yes**	Yes**	Yes**
Application Firewall	No	No	Yes**	Yes**	Yes**	Yes**
SSL Control	Yes**	Yes**	Yes**	Yes**	Yes**	Yes**

*With SonicOS Enhanced upgrade

**4.0.0 Enhanced required

¹Firewall throughput measured using UDP traffic at 1518 byte packet size adhering to RFC 2544

²Gateway AV/Anti-Spyware/IPS throughput measured using HTTP traffic

³VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544

⁴PRO 1260 supports PortShield Technology

**The TZ Series
is the ultimate
total security
platform for
small networks,
including remote
and branch offices
and retail/POS
deployments**



SonicWALL SMB and Branch Office Solutions: TZ Series At-A-Glance

The SonicWALL TZ Series is the ideal total security platform for home, small and remote/branch offices, providing a compelling blend of ease-of-use for basic networks and unsurpassed flexibility for more complex networks. Integrating deep packet inspection firewall, 802.11b/g secure wireless, failover/failback, gateway anti-virus, anti-spyware, intrusion prevention, content filtering and IPSec VPN capabilities into an affordable solution, the TZ Series scales to protect your investment as your organization grows. Available in multiple hardware and node configurations, the TZ Series allows you to add features and functionality when your network needs them.

Every TZ Series appliance packs the benefits of SonicWALL's SonicOS operating system into an affordable desktop appliance, providing business-class performance, advanced features and configuration flexibility. Standard on the TZ 190 Series and TZ 170 SP Wireless and an optional upgrade on all other TZ 170 SP and TZ 180 Series appliances, feature-rich SonicOS Enhanced adds a suite of redundancy, management and wireless LAN features typically associated with more expensive appliances including ISP failover, load balancing, object/zone-based management, policy-based NAT, wireless guest services and more.

TZ Series appliances are ICSA-certified and can be easily managed remotely as part of a multi-firewall and VPN environment through a Web interface or using the industry-leading SonicWALL Global Management System (GMS).

SonicWALL TZ 190 Series

Optimized for powerful Unified Threat Management (UTM) performance, the TZ 190 Series is a multi-layered network security platform that enables organizations to establish 3G wireless broadband network access in an instant without the need for a fixed Internet connection. The solution integrates Type II PC Card* based 3G wireless broadband support, automated failover/failback technologies and a deep packet inspection firewall along with optional 802.11b/g Wireless LAN access. Built on SonicWALL's powerful SonicOS Enhanced operating system, the TZ 190 Series delivers advanced business continuity and networking features including ISP failover, policy-based NAT, object-based management and DDNS. The TZ 190 Series offers a deeper level of network security through integration of real-time gateway anti-virus, anti-spyware, intrusion prevention and anti-spam capabilities for complete protection against malicious threats that originate either internally or from the Internet.

*PC Card sold separately. See <http://www.sonicwall.com/us/tz190cards.html> for supported cards.

SonicWALL TZ 180 Series

Designed as a complete Unified Threat Management (UTM) platform, the TZ 180 Series delivers business-class wired and wireless protection to small, remote and branch office networks through a deep packet inspection firewall and secure 802.11b/g wireless in a cost-effective, easy-to-use solution. The compact form factor includes a single Ethernet WAN port and five-port auto-MDIX LAN switch, allowing multiple devices to connect safely to the network. The TZ 180 Wireless provides network administrators with the ability to create multiple zones of access—for wired and wireless workers as well as guest wireless users—offering an unprecedented level of control without compromising network security. Advanced features such as enforced VPN encryption on the wireless LAN, plus wireless intrusion and rogue access point detection, deliver impenetrable wireless security. Upgrading to SonicOS Enhanced enables the optional port to be configured as a workport for telecommuters, a second WAN for ISP failover and load balancing, a second LAN or another custom-defined zone for added network flexibility.



SonicWALL TZ 170 SP Wireless

The TZ 170 SP Wireless is a total wired and wireless security platform ensuring continuous network uptime through integrated and automated failover and failback technologies. Dual broadband WAN connections plus an integrated analog modem and secure 802.11b/g wireless make the TZ 170 SP Wireless the first appliance to offer automated broadband-to-broadband-to-analog WAN redundancy for unparalleled uptime on both wired and wireless networks. The TZ 170 SP Wireless comes standard with the feature-rich SonicWALL SonicOS Enhanced firmware which includes advanced networking and security features including ISP failover, zone and object-based management, policy-based routing, NAT, spam blocking and more.

SonicWALL TZ 170 SP

The TZ 170 SP is a total security platform for telecommuters and point-of-sale businesses that ensures continuous network uptime for critical, secure data connectivity through integrated and automated failover and failback technologies. With an integrated analog modem and an optional port that can be configured as a second WAN through SonicOS Enhanced, the TZ 170 SP offers automated broadband-to-broadband-to-analog WAN redundancy for unparalleled network uptime.

SonicWALL TZ 150 Series

The TZ 150 Series is a complete layered security platform for home and small offices, integrating a deep packet inspection firewall and secure 802.11b/g wireless LAN access in an easy-to-use, low cost platform. The compact form factor includes a single Ethernet WAN port and four-port auto-MDIX LAN switch, allowing multiple devices to connect safely to the network. The TZ 150 Wireless includes advanced features such as enforced VPN encryption on the wireless LAN and wireless intrusion detection and prevention services for impenetrable wireless security. Utilizing the wireless guest services feature, network administrators can create multiple zones of access—for wired and wireless workers as well as guest wireless users—offering an unprecedented level of control without compromising network security. The TZ 150 Series supports hardware-accelerated IPSec 3DES and AES encryption as well as SonicWALL Global VPN Client upgrades for secure remote access to critical network resources.

Feature	TZ 150 Series	TZ 170 SP	TZ 170 SP Wireless	TZ 180 Series	TZ 190 Series
Nodes	10	10	10	10/25	Unrestricted
Interfaces	5 Ethernet	7 Ethernet	7 Ethernet	7 Ethernet	10 Ethernet
SonicOS Standard/Enhanced	Standard	Standard	Enhanced	Standard	Enhanced
Upgrade to SonicOS Enhanced	No	Yes	N/A	Yes	N/A
Stateful Throughput ¹	30 Mbps	90 Mbps	90 Mbps	90 Mbps	90 Mbps
Gateway Anti-Virus Throughput ²	8 Mbps	8 Mbps	8 Mbps	10 Mbps	10 Mbps
Intrusion Prevention Throughput ²	8 Mbps	8 Mbps	8 Mbps	8 Mbps	8 Mbps
Gateway Anti-Spyware Throughput	5 Mbps	5 Mbps	5 Mbps	6 Mbps	6 Mbps
Connections	2,000	6,000	6,000	6,000	6,000
Policies	20	100/250*	100/250*	100/250*	250
3DES/AES Throughput ³	10+ Mbps	30+ Mbps	30+ Mbps	30+ Mbps	30+ Mbps
Site-to-Site VPN Tunnels	2	2	2	2/10	15
Remote Access VPN Tunnels (Max)	2	5	5	5/50	25
Remote Access VPN Tunnels (Bundled)	Optional Upgrade	Optional Upgrade	Optional Upgrade	Optional Upgrade/1	2
Zone Security	No	Yes*	Yes	Yes*	Yes
Object-based Management	No	Yes*	Yes	Yes*	Yes
Policy-based NAT	No	Yes*	Yes	Yes*	Yes
WAN/WAN Failover	No	Yes*	Yes	Yes*	Yes
ISP Failover	No	Yes*	Yes	Yes*	Yes
Load Balancing	No	Yes*	Yes	Yes*	Yes
Wireless Switch and Controller	No	Yes*	Yes	Yes*	Yes
Integrated Access Point	Optional	No	Yes	Optional	Optional
Receive Power over Ethernet	No	No	Yes	No	No
Integrated Analog Modem	No	Yes	Yes	No	No
Optional Port	No	Yes	Yes	Yes	Yes
Spam Blocking	No	Yes*	Yes	Yes*	Yes
Voice over IP (VoIP)	Yes	Yes	Yes	Yes	Yes
PortShield Architecture	No	No	No	Yes	Yes
3G Wireless Technology	No	No	No	No	Yes
Modular PC Card Slot	No	No	No	No	Yes
Bandwidth Management	No	Yes*	Yes	Yes*	Yes

*With SonicOS Enhanced upgrade

¹Firewall throughput measured using UDP traffic at 1518 byte packet size adhering to RFC 2544

²Gateway AV/Anti-Spyware/IPS throughput measured using HTTP traffic

³VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544



SonicWALL Secure Distributed Wireless Solution

The SonicWALL Secure Distributed Wireless Solution is the first wireless networking security solution that integrates 802.11a/b/g wireless management and security enforcement into an enterprise-class firewall/VPN appliance. The innovative SonicWALL Secure Distributed Wireless Solution scales to fit virtually any network deployment by simply distributing SonicPoints™ at optimal locations throughout the building. Available in IEEE 802.11a/b/g and 802.11b/g options, SonicPoints are dependent access points that are utilized to provide seamless, secure wireless LAN (WLAN) connectivity as well as advanced features and services. SonicPoints can receive 802.3af power over Ethernet (PoE) to aid in their convenient deployment in any network. The Secure Distributed Wireless Solution is built around the SonicWALL award-winning TZ 170 and PRO Series network security appliances which function as secure wireless switches and controllers, automatically detecting and configuring SonicPoints as they are added to the network while simultaneously enforcing security policies on all wired and wireless traffic.

SonicWALL



GAV/
Anti-Spyware/
IPS

Advanced Security Services for Network Security Solutions

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent, real-time network security protection against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows, as well as backdoor exploits and other malicious code. As an added layer of security, this powerful solution provides application layer attack protection not only against external threats, but also against those originating inside the network. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service closes potential backdoors by inspecting over a multitude of e-mail, Web, file transfer and stream-based protocols as well as instant messaging (IM) and peer-to-peer (P2P) applications.

SonicWALL



Content
Filtering
Service

SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) provides businesses and schools with greater control to transparently enforce productivity and protection policies and block inappropriate, illegal and dangerous Web content. Featuring a dynamic rating and caching architecture, SonicWALL CFS blocks multiple categories of objectionable Web content, providing the ideal combination of control and flexibility to ensure the highest levels of productivity and protection.

SonicWALL



Enforced Client
Anti-Virus and
Anti-Spyware

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

SonicWALL Enforced Client Anti-Virus and Anti-Spyware provides comprehensive virus and spyware protection with little administrative overhead. Developed in partnership with McAfee®, this product delivers enforced and auto-updated endpoint protection through automatic system-wide updates of virus definitions and software, eliminating machine-by-machine deployments. Combining the enforced client product with advanced server protection, SonicWALL Client/Server Anti-Virus Suite leverages the award-winning McAfee VirusScan Enterprise for Windows® and GroupShield for Exchange anti-virus protection for Windows-based file, print, message and exchange servers. SonicWALL anti-virus solutions reduce the time and costs associated with administering an anti-virus policy throughout your entire network.

SonicWALL



SonicOS
Enhanced

Firmware for Network Security Appliance

SonicOS Enhanced Firmware

SonicOS Enhanced is the powerful next-generation operating system from SonicWALL, integrating a host of advanced features to meet the business continuity, configuration flexibility and management requirements of complex networks today and into the future. Available as an optional upgrade on the PRO 3060, PRO 2040, PRO 1260, TZ 170 Wireless, TZ 170 SP and TZ 170, SonicOS Enhanced comes factory installed on the PRO 5060, PRO 4100, PRO 4060, PRO 1260 Enhanced, TZ 190 and TZ 170 SP Wireless, providing superior networking and security features to maximize the capabilities of your SonicWALL appliance.

SonicWALL Secure Remote Access delivers granular access control while remaining easy-to-use and manage for the enterprise.



SonicWALL Secure Remote Access Solutions

The traditional corporate LAN is evolving into a distributed global network that connects employees, partners and customers over multiple Internet, intranet, extranet and VoIP channels. The modern mobile workforce demands more solutions for secure access to more resources from more remote devices and platforms than ever before. SonicWALL provides scalable Secure Remote Access solutions to fit every organization—from small- to mid-sized businesses to large global enterprises. SonicWALL Aventail E-Class SSL VPNs and SonicWALL SSL VPNs deliver flexible solutions for secure remote access, disaster recovery, wireless networking and secure extranets.

SonicWALL ^ECLASS

SonicWALL Aventail E-Class SSL VPN Series At-A-Glance

SonicWALL Aventail E-Class SSL VPNs increase productivity with its easy-to-use access capability and reduce IT overhead costs by enforcing granular control while being easy to manage. Recognized by top analysts as an industry leader, SonicWALL Aventail's award-winning SSL VPNs answer the secure remote access needs of today's increasingly mobile enterprise. Offering a single, centrally-managed gateway to control access to network resources, SonicWALL Aventail SSL VPNs deliver robust solutions by providing:

- Secure remote access to mission-critical applications and resources from a wide range of end point device platforms, including Macintosh, Linux, Microsoft® Vista and Microsoft® Windows Mobile
- Clientless browser access or Web-delivered thin client access for an "in-office" experience
- Business continuity and disaster recovery during unexpected disruptions
- Centralized secure access control for wireless networks supporting multiple device platforms
- Secure access to business partner extranets to enhance collaborative productivity
- Policy enforcement across disparate entry points, allowing granular access control
- A solid foundation for Network Access Control (NAC) today and in the future
- Enhanced security that detects inherent risks of an end point prior to authentication; protects resources with granular policy based on that user and end point; and then connects the user only to authorized resources
- Unsurpassed levels of granular control that enforces access based on the trust for the user, the trust for the device used for access and the applications that the user needs to access.

Secure Remote Access Solutions— SonicWALL Aventail E-Class SSL VPN Series SonicWALL Aventail E-Class EX-2500

The SonicWALL® Aventail E-Class EX-2500 is a clientless SSL VPN solution that delivers secure, easy-to-manage remote access control for the mobile enterprise, supporting up to 2,000 concurrent users from a single appliance. The EX-2500 increases user productivity and maximizes IT control by providing authorized access to any application from a broad range of cross-platform devices.

SonicWALL Aventail E-Class EX-1600

The SonicWALL® Aventail E-Class EX-1600 is a clientless SSL VPN solution that delivers secure, easy-to-manage remote access control for mid-size companies and enterprise departments that require up to 250 concurrent users. The EX-1600 provides easy secure access to a broad range of applications from an extensive number of device types and locations, while ensuring easy administrative control through one gateway, reducing deployment and management costs.

SonicWALL Aventail E-Class EX-750

The SonicWALL® Aventail E-Class EX-750 is a full-featured, clientless SSL VPN solution that delivers secure, easy-to-manage remote access for organizations supporting up to 50 concurrent users. Organizations can easily provide anywhere access to mobile employees and business partners from a broad set of end point devices with granular access control rules.

Optional SonicWALL Aventail E-Class Add-on Features

SonicWALL Aventail Advanced End Point Control (EPC)[™]

Advanced EPC combines the most advanced end point detection with the most advanced data protection.

SonicWALL Aventail Advanced Reporting[™]

Advanced Reporting delivers powerful analysis of remote access to your resources.

SonicWALL Aventail Connect Mobile[™]

Connect Mobile offers true “in-office” experience for PDA devices.

SonicWALL Aventail Connect Tunnel[™]

Connect Tunnel provides an “in-office” experience for IT-managed devices.

SonicWALL Aventail Host Access Modules[™]

Host Access Modules support best-of-breed terminal emulation over SSL VPN.

SonicWALL Aventail Native Access Modules[™]

Native Access Modules allow native protocol access to server-based applications.

SonicWALL Aventail Spike License[™]

Spike License is a disaster recovery “insurance policy” for future increases in remote users.

Feature	EX-750	EX-1600	EX-2500
Concurrent User License	10 to 50	25 to 250	50 to 2,000
Basic End Point Control (EPC) Interrogation	Included	Included	Included
Advanced EPC (Anti-Virus, Personal Firewall, Anti-Spyware)	Add-On	Add-On	Included
Aventail Secure Desktop	Add-On	Add-On	Included
Allow, Deny and Quarantine Zones based on EPC interrogation	Included	Included	Included
Granular Access Control (User & Group, Source IP, Service/Port, Destination URL, Host Name/IP Address, IP range, Subnet, Domain)	Included	Included	Included
Advanced Reporting	Add-On	Add-On	Add-On
WorkPlace Portal	Included	Included	Included
WorkPlace Mobile (optimized portal for mobile phone browsers)	Included	Included	Included
Native Access Modules (Citrix and Windows Terminal Services)	Add-On	Add-On	Included
Host Access Modules (Terminal Emulation Access)	Add-On	Add-On	Add-On
Connect Tunnel (Windows, Mac and Linux access to TCP or UDP based applications)	Add-On	Included	Included
Connect Mobile (Windows Mobile)	Add-On	Add-On	Included

SonicWALL SSL VPN

**offers affordable,
easy-to-use and
manage secure
remote access.**

**SonicWALL SSL VPN SMB and Branch Office Solutions At-A-Glance**

The SonicWALL SSL VPN Series provides organizations of any size with an affordable, easy-to-use and manage secure clientless remote network and application access solution that requires no pre-installed client software. Utilizing only a standard Web browser, users can easily and securely access e-mail, files, intranets, applications, remote desktops, servers and other resources on the corporate LAN from any location. SonicWALL SSL VPN solutions integrate seamlessly into virtually any wired or wireless network topology to deliver powerful, scalable and affordable remote access to corporate resources.

- Unrestricted concurrent user tunnels, unlike per-tunnel licensing, significantly reduces the costs associated with deploying a scalable secure remote access solution
- Clientless connectivity removes the need for a pre-installed or "fat" VPN client, thus freeing administrators from the tedious and costly task of installing and updating a client on users' PCs
- Seamless integration behind virtually any firewall enables organizations to leverage the existing network infrastructure without the need to purchase additional hardware
- Granular policy configuration controls enable network administrators to create policies that "lock down" a user to specific applications/resources and prevent unauthorized access to them
- Tokenless two-factor authentication provides enhanced protection against key loggers by combining a unique one-time password, generated by the SSL VPN appliance and sent to a remote user's mobile device or e-mail address, with the user's network user name and password
- Enhanced layered security is enabled when deployed alongside a SonicWALL network security appliance which utilizes powerful deep packet inspection technology to scan traffic for malicious threats such as viruses, worms, Trojans and spyware

SonicWALL SSL-VPN 4000

The SSL-VPN 4000 provides medium-to-large organizations with an enterprise-class remote access solution offering rock solid security, high performance and great flexibility.

SonicWALL SSL-VPN 2000

The SonicWALL SSL-VPN 2000 provides mid-size organizations with a powerful, easy-to-use and cost-effective secure remote access solution that requires no pre-installed client software.

SonicWALL SSL-VPN 200

The SonicWALL SSL-VPN 200 provides small organizations with an affordable, secure remote access solution that requires no pre-installed client software and is easy-to-deploy, manage and use.

SonicWALL



Virtual Assist

Optional SonicWALL SSL VPN Add-on Features SonicWALL Virtual Assist

SonicWALL® Virtual Assist is a clientless remote support tool that enables a technician to assume control of a customer's PC or laptop in order to provide technical assistance. With the customer's permission, the technician can gain instant access to the computer using a Web browser, making it easy to diagnose and fix a problem remotely without the need for a pre-installed "fat" client. Furthermore, SonicWALL Virtual Assist allows tight integration by leveraging existing network and authentication infrastructures.

Deployment	SSL-VPN 200	SSL-VPN 2000	SSL-VPN 4000
Type and Size of Deployment Environment	Small organizations up to 50 employees	Mid-size organizations up to 500 employees	Mid-size organizations over 500 employees
Recommended Maximum Number of Concurrent Users	10	50	200
Concurrent User License	Unrestricted	Unrestricted	Unrestricted

Feature	SSL-VPN 200	SSL-VPN 2000	SSL-VPN 4000
Tokenless Two-factor Authentication	Included	Included	Included
Vasco Support	Included	Included	Included
RSA Support	—	Included	Included
Citrix (ICA) Support	—	Included	Included
NetExtender: Support for Multiple IP Ranges and Routes	—	Included	Included
Optional Client Certificate Support	—	Included	Included
Graphical Usage Monitoring	—	Included	Included
Option to Create System Backup	—	Included	Included
Reverse Proxy: OWA Premium Version and Lotus Domino Access	—	Included	Included
RADIUS Test Function	—	Included	Included
Active Directory Groups Support	—	Included	Included
Virtual Host/Domain Name Support	—	Included	Included
FileShares Java Applet	—	Included	Included
Diagnostics: DNS Lookup and Traceroute	—	Included	Included
SonicWALL Virtual Assist	—	Add-on	Add-on
ViewPoint	—	Add-on	Add-on

**Powerful and
easy-to-use
e-mail threat
protection**

SonicWALL Email Security

Every organization needs protection from both inbound and outbound e-mail threats including spam, phishing, viruses, zombies as well as compliance violations. SonicWALL Email Security delivers a highly-effective, easy-to-use solution from 10 to 100,000 mailboxes which dramatically reduces the time and expense of owning and managing an e-mail security solution.

SonicWALL Email Security delivers the highest level of protection from inbound and outbound e-mail threats. Leveraging a unique worldwide attack identification and monitoring network called SonicWALL Global Response Intelligent Defense (GRID) and combined with our continuously innovative protection technique, SonicWALL delivers superior protection today and stand ready to stop the new attacks of tomorrow. Protections include anti-spam, anti-phishing, anti-virus and Time-Zero technology (responsive and predictive), policy management, connection management, zombie detection, compliance and content filtering—regulatory and corporate as well as e-mail auditing.

With SonicWALL Email Security, administration takes less than 10 minutes a week. There are no rules to write, no scores to set, and no pulling user messages out of quarantine. Designed and built to be intuitive and easy to use for the administrator and the end-user, simplicity means quick configuration, end-user spam management, seamless LDAP integration, robust reporting, automatic software updates, automatic protection updates and an intuitive and streamlined interface.

SonicWALL Email Security ensures peak system performance and throughput through its unique preemptive scanning MTA and extensive Connection Management capabilities. This results in breakthrough message analysis that is 40-290% faster than the competition.

SonicWALL Email Security is available as an appliance or as Windows software. Each appliance includes fully functional inbound and outbound capabilities.



SonicWALL ECLASS

SonicWALL E-Class Email Security Solutions At-A-Glance

E-Class Email Security Appliance:

SonicWALL Email Security 6000 and 8000 Series

SonicWALL E-Class Email Security 6000 and 8000 offers comprehensive, effective and scalable e-mail security for enterprise environments. This powerful yet easy-to-manage solution combines anti-spam, anti-virus and anti-phishing capabilities with content filtering and outbound e-mail management, preventing leaks of confidential information and violations of regulatory compliance laws. Its unique pre-emptive scanning Mail Transfer Agent (MTA) offers breakthrough message analysis and industry-leading message delivery rates, providing high-performance and enterprise-wide scalability.

E-Class Email Security Software:

SonicWALL Email Security Software – Enterprise

For enterprises that standardize on specific hardware, have existing monitoring and backup systems or just want the ultimate in deployment flexibility, SonicWALL E-Class Email Security Software provides all the functionality of SonicWALL E-Class Email Security 6000 and 8000 Series on a software platform. This e-mail security solution combines best protection with effortless control and high performance.



SonicWALL Email Security SMB Solutions At-A-Glance

SMB Solutions Appliance: SonicWALL Email Security 200, 300, 400 and 500 Series

Ideal for small- to medium-sized organizations, SonicWALL Email Security appliances are easy-to-install and extremely effective at stopping all e-mail threats at the SMTP gateway. This powerful solution protects organizations against threats including spam, phishing, viruses, Denial-of-Service and Directory Harvest Attacks, and compromised Zombie machines. These appliances also provide robust outbound e-mail management for policy and regulatory compliance. Based on a hardened SonicWALL OS, these plug-and-play appliances install in less than an hour to securely protect your e-mail.

Software Solutions: SonicWALL Email Security Software – Small-to-Medium Business

SonicWALL Email Security Software is ideal for small- to medium-sized organizations that want to implement a software e-mail security solution on their existing hardware. With all the available features of the SMB appliances, SonicWALL Email Security Software secures organizations from all inbound and outbound e-mail threats through an easy-to-use, Web-based administrative interface.

SonicWALL



Email Protection

SonicWALL



Email Anti-Virus

SonicWALL



Email Compliance

SonicWALL Email Security Services

SonicWALL Email Protection Subscription and Dynamic Support (8x5 or 24x7)

SonicWALL Email Protection Subscription and Dynamic Support is a required subscription service for Email Security appliances and software as it completes the comprehensive e-mail threat protection by providing real-time anti-spam and anti-phishing updates as well as software/firmware updates. The subscription includes either 8x5 or 24x7 technical support with advanced RMA for the appliance and warranty for repair or replacement of any defective product due to manufacturer’s defects.

SonicWALL Email Anti-Virus Subscription

SonicWALL Email Anti-Virus Subscription provides protection from the time a virus outbreak occurs until the time a signature update is available through SonicWALL Time Zero Technology. SonicWALL provides additional layers of protection by partnering with best-of-breed companies McAfee™ and Kaspersky Lab™ for signature updates.

SonicWALL Email Compliance Subscription

SonicWALL Email Compliance Subscription enables organizations to adhere to regulatory compliance requirements and the implementation of best practices with e-mail usage. The features include detailed attachment scanning, compliance dictionaries, approval boxes, record ID matching, encryption routing, e-mail archiving, pre-defined policies and compliance reports. By intelligently identifying e-mails that violate compliance policies, monitoring and reporting the problem and applying multiple enforcement options, SonicWALL can help organizations take the next step towards e-mail compliance.

Email Security Appliances	SMB				E-Class		
	Model	200	300	400	500	6000	8000
Users Licensed		50	250	750	2000	5000	Over 5000
Rackmount Chassis		1U Mini	1U Mini	1U Mini	1U Mini	1U Mini	1U Fullsize
CPU		2.66 GHz	2.66 GHz	2.66 GHz	2.66 GHz	3.2 GHz	2x3.2 GHz
RAM		1 GB	1 GB	1 GB	1 GB	2 GB	2 GB
Hard drive		80 GB	80 GB	2x80 GB	2x80 GB	2x160 GB	2x146 GB
Redundant Disk Array (RAID)		No	No	Yes	Yes	Yes	Yes
Hot Swappable Drives		No	No	No	No	No	Yes
Redundant Power Supply		No	No	No	No	No	Yes
Email Security Software							
Users Licensed		25	50	250	750	2000	5000
Software Platforms		Windows 2000 Server, Windows 2003 Server					

SonicWALL Content Security Manager Series At-A-Glance

The SonicWALL Content Security Manager (CSM) Series is an appliance-based Internet threat protection solution that integrates real-time gateway anti-virus, anti-spyware, intrusion prevention and advanced content filtering to deliver maximum network protection from today's sophisticated Web-based threats. Combining dynamic threat management capabilities with precise control over Internet usage in an affordable, appliance-based solution, the CSM appliance boosts network security and employee productivity, optimizes network utilization and mitigates legal liabilities. This unique solution integrates seamlessly into virtually any network topology for powerful, scalable and cost-effective threat protection.

- Granular controls for managing access to Web sites containing unproductive and potentially illegal Web content
- Blocks continually-evolving threats including viruses, worms, Trojans, spyware, keyloggers, phishing and malicious mobile code (MMC)
- Instant messaging, peer-to-peer and multimedia application controls enhance bandwidth utilization
- Dynamically updated signature and ratings databases ensure vulnerabilities are blocked before they can be exploited
- Advanced reporting and analysis tool provides insight into network usage through custom reports



SonicWALL CSM 3200

SonicWALL Content Security Manager 3200 provides protection against inbound and outbound Web-based threats, designed for networks with up to 1000 users.

SonicWALL CSM 2200

SonicWALL Content Security Manager 2200 provides protection against inbound and outbound Web-based threats, designed for networks with up to 250 users.

SonicWALL Continuous Data Protection (CDP) Series

The SonicWALL Continuous Data Protection (CDP) Series is a disk-based data backup and recovery solution that provides deep protection for businesses and remote offices. The solution reduces business downtime from days and hours to minutes and seconds, allowing organizations to meet rigorous Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). By combining the advantages of instant data recovery (local disk-based backup) with protection against disaster events (offsite backup), the SonicWALL backup and recovery solution is the first to eliminate, not just mitigate, exposure to threats of data loss. The solution also includes central management and remote administration features that enable IT administrators to more effectively and efficiently protect an organization's data.



SonicWALL Backup and Recovery Solutions At-A-Glance

SonicWALL CDP 4440i

The CDP 4440i is a robust 2U rack-mountable backup and recovery solution for branch offices and mid-size organizations. Offering a 1.2 TB compressed capacity with RAID 5 along with accelerated throughput and AES 256-bit encryption for offsite data security, along with all the features of the CDP 3440i, it provides continuous real-time data protection for unlimited servers, laptops, PCs, databases and business applications. IT Administrators benefit from central management and file-level visibility into every client machine connected to the SonicWALL CDP appliance, enabling enforcement of consistent backup policies and control features available to individual end users.

SonicWALL CDP 3440i

The CDP 3440i offers enterprise-class data backup protection for small-to-medium organizations and remote offices. The high-performance 1U rack-mountable solution is optimized for up to 75 users and unlimited servers. Offering 600 GB compressed capacity with RAID 1 along with accelerated throughput and AES 256-bit encryption for offsite data security; it provides continuous real-time data protection for servers, laptops and PCs using policy-based backup, central administration and open file backup. It supports most small business databases and applications such as Microsoft Exchange, SQL-Server, Quickbooks, PeachTree, Great Plains, etc.

SonicWALL CDP 2440i

The CDP 2440i is ideal for small organizations and remote offices. Featuring a 300 GB compressed capacity along with standard throughput and AES 256-bit encryption for offsite data security, it provides continuous real-time data protection for servers, laptops and PCs. Differentiating this solution from many of its competitors is its seamless support of most small business databases and applications such as SQL-Server and Microsoft Exchange without the need to integrate additional software packages.

SonicWALL CDP 1440i

The CDP 1440i is a disk-based backup and recovery appliance that offers real-time end-to-end data protection for small organizations. It includes unique features such as instant data recovery and central administration. The CDP 1440i supports servers, PCs and laptops for small business networks and is recommended for up to 15 users, 192 GB compressed capacity and AES 256-bit encryption for offsite data security.

SonicWALL



Offsite Data Backup

SonicWALL



Site-to-Site Data Backup

SonicWALL



Bare Metal Recovery

SonicWALL Backup and Recovery Licenses and Services

SonicWALL offers hands-free offsite backup and recovery solutions that store data to enable organizations to be up and running quickly after a disaster event. Data can be transmitted to either an offsite datacenter or to a managed CDP appliance. All data is transmitted and stored with an AES 256-bit encryption key that is only known to the end-user. Data can be restored directly to a CDP appliance via a simple point and click interface. SonicWALL’s dedicated support organization will always be there to help with the recovery process as well.

SonicWALL CDP Offsite Data Backup Service

SonicWALL CDP Offsite Data Backup Service provides a fully managed offsite data solution for hassle-free disaster protection. Data is restored directly to a CDP appliance with point and click functionality in the event of a disaster. The datacenters feature uninterruptible power supply (UPS) systems, emergency diesel generators, earthquake protection, redundant fire prevention, flood control, HVAC and 24-hour on-site security.

SonicWALL CDP Site-to-Site Backup

SonicWALL CDP Site-to-Site Backup is for customers and resellers who want to manage their disaster protection solution. Site-to-Site Backup allows any CDP appliance to be used for offsite backup. A single offsite appliance can provide disaster protection for multiple downstream CDP appliances. In the event of a disaster, data can quickly be restored to a new CDP appliance using SonicWALL’s Enterprise Manager software.

SonicWALL CDP Bare Metal Recovery/Local Archiving

Bare Metal Recovery (BMR) software creates an exact image of an entire server or workstation, including operating system files, programs, databases and settings. An entire system can be recovered in minutes through an easy-to-use wizard-driven graphical user interface. Additionally, the BMR software provides local archiving capabilities that allow organizations to store snapshots of their data for extended periods of time to meet industry and government compliance regulations.

Feature	CDP 1440i	CDP 2440i	CDP 3440i	CDP 4440i
Core Compression Technology	Standard	Standard	Enhanced	Enhanced
Encryption	AES 256-bit	AES 256-bit	AES 256-bit	AES 256-bit
Throughput	Standard	Standard	Accelerated	Accelerated
Users (recommended)	15 or fewer	30 or fewer	75 or fewer	Unlimited
Servers (recommended)	3	5	Unlimited	Unlimited
Base Capacity¹	160 GB	250 GB	400 GB	600 GB
Compressed Capacity²	192 GB	300 GB	800 GB	1.2 TB
Chassis	Mini	Mini	1U Rack	2U Rack
RAID	N/A	N/A	RAID 1	RAID 5
Interface	1 x 10/100 Base-T Ethernet	1 x 10/100 Base-T Ethernet	10/100/1000 GIG LAN	10/100/1000 GIG LAN
Continuous Data Protection	Yes	Yes	Yes	Yes
File Versions	Yes	Yes	Yes	Yes
Central Administration	Yes	Yes	Yes	Yes
Desktop Laptop, Server Backup	Yes	Yes	Yes	Yes
Remote Administration	Yes	Yes	Yes	Yes
Open Files Backup	Yes	Yes	Yes	Yes
Policy Based Backup	Yes	Yes	Yes	Yes
Active Directory Backup	No	Yes	Yes	Yes
SQL Server Support	No	Yes	Yes	Yes
MS Exchange Server Support	No	Yes	Yes	Yes
Bare Metal Recovery/Local Archiving - Workstation	Yes (1 license bundled)	Yes (2 licenses bundled)	Yes (5 licenses bundled)	Yes (10 licenses bundled)
Bare Metal Recovery/Local Archiving - Server	No	No	Yes (1 license bundled)	Yes (2 licenses bundled)

¹Product capacity specified in gigabytes (GB) are terabytes (TB) where 1 GB = 1,000,000,000 bytes and 1 TB = 1,000,000,000,000 bytes.

²Compressed capacity assumes 1.2:1 for standard data compression and 2:1 for enhanced data compression. Capacity may vary and is data dependent.

SonicWALL

Global
Management
System

Global Management System (GMS)

SonicWALL Global Management System (GMS) provides organizations, distributed enterprises and service providers with a flexible, powerful and intuitive tool to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations. Organizations can globally manage and collect detailed information from security applications such as gateway anti-virus, anti-spyware, intrusion prevention and content filtering, all from a single console. SonicWALL GMS enables organizations to reduce staffing requirements, speed up deployment and lower costs.

- Simplifies configuration and enforcement of global security and VPN policies
- Offers centralized reporting and monitoring of security appliances and user activity
- Scales to support growing deployments

SonicWALL

ViewPoint

SonicWALL ViewPoint

SonicWALL ViewPoint™ is an easy-to-use Web-based reporting tool that fully compliments and extends SonicWALL's security products and services. Using both a customized dashboard and a variety of historical reports, ViewPoint provides administrators insight into the health of their network including network utilization, security activity and Web usage.

- Graphical, easy-to-interpret reports on network and security activities
- On-demand reporting saves administrative overhead
- Web interface simplifies deployment and access from a local or remote system

SonicWALL

MySonicWALL

MySonicWALL

MySonicWALL delivers a convenient, centralized way to register and manage SonicWALL network security and data protection appliances and associated services. MySonicWALL is an easy-to-use online customer portal that enables organizations to manage their entire SonicWALL relationship in a single location. Busy IT managers can save time by using MySonicWALL to track firmware versions, existing software licenses and security service subscriptions.

- MySonicWALL helps prevent unanticipated service expirations, which can lead to crippling and costly security breaches and business interruptions
- MySonicWALL makes it easy for managers to renew existing security services and to subscribe to additional levels of security and data protection
- MySonicWALL allows customers to manage multiple discrete product installations, including network security appliances, e-mail security appliances and data backup and recovery installations spread across the enterprise.

SonicWALL



**Dynamic
Support
Services**

SonicWALL Global Support Services

SonicWALL offers a robust portfolio of global support services that not only help keep your network security and data backup and recovery infrastructure current, but also swiftly resolve any problem that may occur. However that's not enough to keep your network safe these days. So, SonicWALL's support services also include crucial software and firmware updates and upgrades, the finest technical support, timely hardware replacement and access to extensive electronic tools.

Dynamic Support 8x5 and 24x7

Designed for customers who need continued protection through on-going firmware updates and advanced technical support, SonicWALL Dynamic Support is available during normal business hours, or 24x7, depending on your needs. Services include:

- Annual subscription to firmware updates and upgrades
- Access to telephone and Web-based support for basic configuration and troubleshooting assistance
- Advance Exchange hardware replacement in the event of failure

Comprehensive Global Management System (GMS)

For customers using SonicWALL Global Management System (GMS) to manage their distributed networks, there's SonicWALL Comprehensive GMS. This umbrella support service delivers all the benefits of an 8x5 or 24x7 support contract for every appliance managed through a SonicWALL GMS deployment. Comprehensive GMS includes:

- All the services and advantages of a Dynamic Support 8x5 or 24x7 contract
- Support and software updates for the GMS application itself
- One expiration date for everything, simplifying management and administration

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™