



PRODUCT LINE

Dynamic Security for the Global Network

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Overview2

Network Security Solutions

Network Security Solution Summary3

E-Class Solutions.....3

Branch Office and SMB Solutions.....5

Wireless Enablers10

Subscription Services, Licenses and Firmware.....11

Secure Remote Access Solutions

Secure Remote Access Solution Summary13

E-Class Solutions.....13

Add-on Features.....14

SMB and Branch Office Solutions.....15

Add-on Features.....16

Anti-Spam/Email and Web Security Solutions

Email Security Solution Summary.....17

E-Class Solutions.....17

SMB Solutions.....18

Subscription Services.....18

Web Solutions19

Backup and Recovery Solutions

Backup and Recovery Solution Summary.....20

SMB Solutions.....21

Licenses and Services.....21

Policy and Management Solutions

Global Management System.....23

ViewPoint.....23

MySonicWALL.....23

Global Support Services

E-Class Support 24x7.....24

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

Comprehensive Global Management System Support.....24

Focused Technical Support.....24

Remote Start-up and Configuration Service.....25

Customer Advantage Program

Secure Upgrade Plus25

Customer Loyalty Bundle25

Dynamic Security for the Global Network Our vision is simple: we believe security solutions should be “smart” enough to adapt as organizations evolve and as threats evolve, dynamically, globally. We believe customers around the world should have the ability to control, manage and protect their global network easily and automatically. We believe our customers should be able to receive and share threat and defense data around the world so they can anticipate and stop attacks before they happen. We want our customers to be able to secure any user, any device, using any application from anywhere so they can collaborate securely across different networks. All this needs to be achieved with maximum ease of deployment and at the best economic value and in a compliant framework.

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, and Web and email 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 Application Intelligence extends control over nonproductive applications like online trading, instant messaging/chat, peer-to-peer sharing and streaming video sites. SonicWALL Email Security completes the offering with effective protection against spam and phishing attacks so employees only read legitimate emails and are not exposed to fraudulent emails. 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 or secure remote access using IPSec or SSL VPN. Combining these appliances with self-configuring SonicPoints instantly provides provisional temporary networks with secure wireless hotspot connectivity. The SonicWALL TZ 200 and TZ 210 allows temporary sites to establish secure 3G wireless broadband virtually anywhere in an instant without a fixed Internet connection. Additionally, SonicWALL dedicated 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 VPN solutions also offer unsurpassed levels of granular control.

Business Continuity Whether triggered by a major disaster, a flu outbreak 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 and flexible disaster recovery options for servers, laptops and PCs. The SonicWALL Continuous Data Protection (CDP) Series protects files locally as well as at offsite locations to ensure data can be recovered instantly.

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 emails, robust monitoring and reporting tools, and a range of remediation options. And, SonicWALL Content Security Manager 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.

Virtual Appliances SonicWALL's Virtual Appliances bring together the cost and management advantages of virtualization plus the security of hardened appliance OS to offer improved choice and flexibility for SMBs, enterprises, and Managed Service Providers (MSPs). SonicWALL Virtual Appliances enable the enterprise to fully capitalize on security solutions while channel partners can deliver virtualized solutions and related benefits to their customers.

Converged Network Security Solutions As customers IP networks continue to grow by adding voice and video, along with high bandwidth data applications, the need for security and control becomes critical. The SonicWALL Converged Network Security Solution delivers the highest-performance multi-function VoIP Firewall, offering greater access, control and security. Customers of any size understand that the more information and process' that reside on their network, the more it becomes a critical company asset. SonicWALL's solutions allow customers of any size to protect this asset.

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 patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology* in combination with multi-core specialized security microprocessors to deliver gateway anti-virus, anti-spyware, intrusion prevention and Application Intelligence 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 E-Class 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 their class. Taking protection to new levels of control is Application Intelligence, a set of customizable protection tools that affords administrators precise control over network traffic. To meet the operational reliability enterprise-class networks demand, the E-Class NSA Series incorporates a suite of high availability features at the hardware and system levels 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 E-Class 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 Intelligence 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
- Flexible yet secure virtual private networking (VPN) technologies include IPSec VPN for site-to-site connectivity and both SSL VPN and IPSec VPN client connectivity to enable secure remote access
- Uncompromising business continuity and high availability protection

*U.S. Patent 7,310,815–A method and apparatus for data stream analysis and blocking.

SonicWALL ECLASS

Network Security Solutions—SonicWALL E-Class NSA Series

SonicWALL NSA E8500

The SonicWALL E-Class Network Security Appliance (NSA) E8500 offers Dynamic Security for the Global Network by providing powerful application intelligence and control along with network intrusion detection and prevention. With the patented SonicWALL® Reassembly-Free Deep Packet Inspection™ (RFDPI) engine and sophisticated application intelligence capabilities, the NSA E8500 can analyze and control over 1,100 unique applications, whether they are encrypted with SSL or are unencrypted. This exceptional combination of software sophistication and incredibly powerful hardware leaves little room for application traffic to hide on the network, since SonicWALL's RFDPI engine is capable of inspecting hundreds of thousands of connections simultaneously across all 65,535 ports equally, with nearly zero latency and without stream size limitations.

SonicWALL NSA E7500

The SonicWALL E-Class Network Security Appliance (NSA) E7500 is designed to be the most scalable, high-performance, reliable multi-function threat appliance in its class. This protection is enabled through the NSA E7500's 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 Intelligence, 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 takes advantage of specialized multi-core processing technology, providing parallel traffic processing, in conjunction with SonicWALL's Reassembly-Free Deep Packet Inspection engine. Now enterprise administrators have a high-performance secure platform to combat the changing threat landscape. Using tools such as Application Intelligence, network administrators can take advantage of customizable protection tools that empower 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 a high-performance, multi-service network security platform engineered to be the workhorse of the enterprise network environment. Taking advantage of SonicWALL's Reassembly-Free Deep Packet Inspection engine and eight-core processor technology providing parallel traffic processing, the NSA E5500 delivers exceptional deep packet inspection performance for enterprise networks. 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.





SonicWALL SMB and Branch Office Solutions: NSA Series At-A-Glance
SonicWALL Network Security Appliance 4500

The SonicWALL Network Security Appliance (NSA) 4500 is a next-generation Unified Threat Management (UTM) firewall designed to meet the demands of corporate central-site and large distributed environments. Built upon a breakthrough Reassembly-Free Deep Packet Inspection engine and eight-core hardware platform for corporate networks and distributed environments, the NSA 4500 delivers real-time internal and external network protection without compromising network performance. The NSA 4500 combines high-speed intrusion prevention, file and content inspection and powerful Application Intelligence capabilities with an extensive array of advanced networking, stateful high availability and configuration flexibility. With six configurable gigabit Ethernet (GbE) interfaces and SonicWALL Clean VPN™ technology, the NSA 4500 is an ideal solution for corporate perimeter protection and remote access connectivity. The NSA 4500 also supports virtual local area networks (VLANs), enterprise-class routing and QoS features, further extending security and performance throughout the network.



SonicWALL Network Security Appliance 3500

The SonicWALL Network Security Appliance (NSA) 3500 is a next-generation Unified Threat Management firewall designed to meet the needs of corporate, branch office and distributed environments. Utilizing a breakthrough Reassembly-Free Deep Packet Inspection engine and multi-core hardware design with four cores and six gigabit Ethernet (GbE) interfaces, the NSA 3500 delivers real-time internal and external network protection without compromising network performance. The NSA 3500 combines high-speed intrusion prevention, file and content inspection and powerful Application Intelligence capabilities with 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. With its intuitive Web management interface and easy-to-use wizards, the NSA 3500 simplifies set-up and configuration. The NSA 3500 also supports virtual local area networks (VLANs), enterprise-class routing and QoS features, further extending security and performance throughout the network.



SonicWALL Network Security Appliance 2400

The SonicWALL Network Security Appliance (NSA) 2400 is a next-generation Unified Threat Management firewall platform, utilizing a breakthrough multi-core hardware design and Reassembly-Free Deep Packet Inspection technology with six gigabit Ethernet (GbE) interfaces to deliver real-time network protection without compromising performance. Designed for small-to-midsize corporate and branch office networks, the NSA 2400 offers best-in-class threat prevention, rapid deployment and lowered TCO. The NSA 2400 combines high-speed intrusion prevention, file and content inspection and powerful Application Intelligence capabilities with an extensive array of advanced network and configuration flexibility features in an accessible, affordable platform that is easy to deploy and manage in a wide variety of environments.



SonicWALL Network Security Appliance 240

The SonicWALL NSA 240 delivers next-generation high-performance Unified Threat Management firewall for small- to medium-sized businesses and branch offices, integrating gigabit Ethernet (GbE), multi-core hardware and SonicWALL's Reassembly-Free Deep Packet Inspection engine for network protection without compromising performance. The NSA 240 combines Clean VPN™ threat prevention, file and content inspection, Application Intelligence, future-proofed extensibility and high availability. Ideal for distributed environments requiring high security, performance, rapid implementation, and lower TCO, the NSA 240 offers advanced networking, multiple WAN redundancy and flexible configuration features in a cost-effective solution that is easy to deploy and manage.



SonicWALL SMB and Branch Office Solutions: NSA 2400MX
SonicWALL Network Security Appliance 2400MX

The all-new NSA 2400MX delivers robust, high-performance security on a next-generation Unified Threat Management (UTM) platform that features a breakthrough Reassembly-Free Deep Packet Inspection™ technology and multi-core hardware design to deliver real-time comprehensive network protection, high-speed intrusion prevention, file and content inspection, and powerful Application Intelligence capabilities, all without compromising performance. At the same time, the NSA 2400MX also provides flexible, intelligent switching capabilities with its unique PortShield architecture, increased port density with 26 interfaces, and advanced switching, routing, networking and connectivity features. The NSA 2400MX also supports integrated virtual private networks (VPNs), virtual local area networks (VLANs), standards-based Voice over IP (VoIP), dynamic routing and Quality of Service (QoS) features, further extending security and performance through the network environment.

Feature			
SonicOS Supported	SonicOS Enhanced 5.7 (or higher)	Object-based Management	Yes
Users and Nodes	Unrestricted	Policy-based NAT	Yes
Network Interfaces	(16) 10/100, (10) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB, 2 Module Slots (For Future Use)	Multi-WAN	Yes
Power Supply	Single 180W ATX	Multiple ISP Failover	Yes
Cooling System (Fans)	2 Fans	Load Balancing	Yes
VLAN Interfaces	25	Integrated Wireless Switch and Controller	Yes
High Availability	Optional Active/Passive with State Sync	Policy-based Routing	Yes
Stateful Throughput¹	775 Mbps	3G Wireless Technology	Yes
3DES/AES Throughput²	300 Mbps	Comprehensive Anti-Spam Service	Optional
Gateway Anti-Virus Throughput³	160 Mbps	Voice over IP (VoIP)	Yes
Intrusion Prevention Throughput³	275 Mbps	IKEv2 VPN	Yes
UTM Performance³	150 Mbps	Secure Remote Management (SSHv2 Support)	Yes
IMIX Performance³	235 Mbps	SSL VPN and IPSec VPN Remote Access Clients	Yes
New Connections Per Second	4,000	Virtual Assist Technicians	Yes
Maximum Connections⁴	225,000	Route-based VPN	Yes
Maximum UTM Connections	125,000	Multiple SSIDs using VAP	Yes
Switching Features	VLAN Trunking, Rapid Spanning Tree, Layer 2 Discovery, Link Aggregation, Port Mirroring, Layer 2 QoS, Rate Control, Port Security	Dynamic Address Objects	Yes
Site-to-Site VPNs	75	Terminal Services User Authentication	Yes
Bundled Global VPN Client Licenses (Maximum)	10 (250)	802.1q VLANs	Yes
Bundled SSL VPN Licenses (Maximum)	2 (25)	RIPv2 and OSPF Routing	Yes
Bundled Virtual Assist Technicians (Maximum)	1 (5)	Single Sign-On (SSO)	Yes
Zone Security	Yes	Application Intelligence	Optional
		SSL Control	Yes
		IPv6 Ready	Yes

¹Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

²VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.

³UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.

⁴Actual maximum connection counts are lower when UTM services are enabled.

**The TZ Series
is the ultimate
total security
platform for distributed
environments,
including remote
and branch offices,
SMBs, and retail/POS
deployments.**



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

The all new SonicWALL TZ Series changes the game for distributed enterprises and small- to medium-sized businesses (SMBs) with a major breakthrough in higher-performance network protection. Leveraging advanced fifth-generation processing technology honed in SonicWALL’s NSA Series, the TZ Series dramatically expands the comprehensive protection critical for securing distributed environments and SMBs, at a performance level that doesn’t compromise network throughput. The TZ Series achieves this level of higher-performance protection by integrating SonicWALL’s high-speed Reassembly-Free Deep Packet Inspection™ firewall technology, Gigabit Ethernet, and a specialized security processor capable of delivering up to 200 Mbps of stateful packet throughput and up to 50 Mbps of deep packet inspection capability on the TZ 210.

The all new SonicWALL TZ Series revolutionizes protection for the distributed enterprise and SMB by adding new Comprehensive Anti-Spam Service and integrated SSL VPN capabilities, to complement the Unified Threat Management (UTM) portfolio of gateway anti-virus, anti-spyware, intrusion prevention, Application Intelligence, enforced client anti-virus, and content filtering. This new comprehensive level of protection is vital for securing any network against the new, more advanced Web 2.0 based threats. Additionally, the TZ Series offers Clean Wireless protection by incorporating UTM with 802.11n wireless in the firewall, extendable through the addition of multiple 802.11a/b/g/n SonicPoint smart access points. The TZ Series also provides continuous network access by offering USB-based 3G or analog failover.

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 210, TZ 200 and TZ 100 Series and an optional upgrade on the TZ 180 Series, 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, route-based VPN and more.

TZ Series appliances are 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).

Every TZ Series appliance is available as a SonicWALL TotalSecure™ solution, a convenient and affordable solution that combines the hardware and all the services needed for comprehensive network protection from a wide range of network threats including viruses, spyware, worms, Trojans, keyloggers and other malicious threats. Together, these components form a Unified Threat Management (UTM) solution that delivers exceptional security to protect against emerging threats.

SonicWALL TZ 210 Series

The flagship of the revolutionary TZ Series, the new TZ 210 Series builds upon the TZ 200 and delivers our most sophisticated and future-proofed TZ Series offering. The TZ 210 infrastructure offers dual Gigabit Ethernet interfaces for the WAN and the primary LAN that can act independently or as part of the five-port 10/100 switch. Activating the Comprehensive Gateway Security Suite on the TZ Series enables the powerful Application Intelligence to provide application-level access control over Web 2.0 applications such as social networking sites, application inspection, bandwidth management and throttling, data leakage control functionality, and the ability to create pure custom signatures. The TZ 210 delivers the extraordinary redundancy and flexibility of dual USB ports for 3G and analog modem failover, integrated SSL VPN capabilities, as well as the future-proofed speed and powerful protection of 50 Mbps of full Unified Threat Management performance, 40% faster¹ than the TZ 200. The TZ 210 Wireless-N also integrates ultra-fast 802.11n wireless LAN capabilities. The TZ 210 is the most comprehensive network security appliance available to SMBs at a price point under \$1,000.



SonicWALL TZ 200 Series

The new TZ 200 Series builds upon the TZ 100 delivering critical business continuity and flexibility through a host of advanced features. The TZ 200 adds critical failover capabilities that can provide 24x7 access to keep your organization up and running, with support for USB-based 3G and analog failover and box-to-box failover. Like the TZ 100, the TZ 200 comes pre-bundled with a single concurrent SSL VPN tunnel and is upgradeable to 10. The TZ 200 also adds SonicWALL Comprehensive Anti-Spam Service including sophisticated per-user mailbox quarantine capabilities as a complement to UTM, adding customization at a lower cost. The higher-performance TZ 200 significantly boosts memory and processor power to support all these additional features while running 40% faster¹ than the TZ 100. The TZ 200 Wireless-N version incorporates high-speed 802.11n. The entire TZ 200 Series delivers powerful, enterprise-class features that are normally only found in enterprise-priced offerings, all available for a low total cost of ownership.



SonicWALL TZ 100 Series

The new TZ 100 is the entry point of the fifth-generation TZ Series, making high performance Unified Threat Management available and affordable for everyone. It features a powerful Stateful Packet Inspection Firewall plus an advanced Reassembly-Free Deep Packet Inspection engine capable of delivering SonicWALL's newly expanded comprehensive protection. The TZ 100 completely revolutionizes SMB and distributed enterprise protection with the introduction of a new enterprise-class Comprehensive Anti-Spam Service to complement the existing UTM protection lineup of gateway anti-virus, anti-spyware, intrusion prevention, and advanced content filtering. The new TZ 100 Series provides secure remote access by including a single SSL VPN tunnel that is upgradeable to five along with five configurable 10/100 interfaces. The TZ 100 performs two-and-a-half times faster¹ than the TZ 180 and TZ 150, easily expanding comprehensive protection without compromising network throughput. The TZ 100 Wireless-N version adds high-speed 802.11n. Plus, all TZ Series appliances support an integrated wireless switch controller to add managed distributed wireless to any network.



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 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 robust 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.

¹ UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.

Feature	TZ 180 Series	TZ 100 Series	TZ 200 Series	TZ 210 Series
Nodes	10/25	Unrestricted	Unrestricted	Unrestricted
Interfaces	7 Fast Ethernet	5 Fast Ethernet	5 Fast Ethernet	2 Gigabit Ethernet 5 Fast Ethernet
USB Ports	N/A	N/A	1	2
SonicOS Standard/Enhanced	Standard	Enhanced	Enhanced	Enhanced
Upgrade to SonicOS Enhanced	Yes	N/A	N/A	N/A
Stateful Packet Inspection Throughput	90 Mbps	100 Mbps	100 Mbps	200 Mbps
UTM Throughput	10 Mbps	25 Mbps	35 Mbps	50 Mbps
3DES/AES Throughput	30 Mbps	75 Mbps	75 Mbps	75 Mbps
Maximum Connections	6,000	6,000	8,000	10,000
Site-to-Site VPN Tunnels	10 Node = 2 25 Node = 10	5	10	15
Remote Access IPsec VPN Tunnels (Max)	5/50	5	10	25
Remote Access IPsec VPN Tunnels (Bundled)	Optional Upgrade/1	Optional Upgrade	2	2
Remote Access SSL VPN Tunnels (Max)	N/A	5	10	10
Remote Access SSL VPN Tunnels (Bundled)	N/A	1	1	2
Virtual Assist Technicians (Max)	N/A	N/A	1	2
Virtual Assist Technicians (Bundled)	N/A	N/A	0	0
Zone Security	Yes*	Yes	Yes	Yes
Object-based Management	Yes*	Yes	Yes	Yes
Policy-based NAT	Yes*	Yes	Yes	Yes
Multiple ISP Failover	Yes*	Yes	Yes	Yes
ISP Failover	Yes*	Yes	Yes	Yes
Hardware Failover	No	No	Active/Passive	Active/Passive
Load Balancing	Yes*	Yes	Yes	Yes
Layer 2 Wireless Bridging	N/A	Yes	Yes	Yes
Wireless Switch and Controller	Yes*	Yes	Yes	Yes
Virtual Access Points (VAPs)	Yes*	Yes ¹	Yes ¹	Yes ¹
Integrated Access Point	Optional 802.11a/b/g	Optional 802.11n	Optional 802.11n	Optional 802.11n
Configurable Ports	OPT Port	All LAN ports	All LAN ports	All LAN ports
Comprehensive Anti-Spam Service	N/A	Optional	Optional	Optional
Voice over IP (VoIP)	Yes	Yes	Yes	Yes
PortShield Security	Yes*	Yes	Yes	Yes
Route-based VPN	N/A	Yes	Yes	Yes
3G Wireless Technology	N/A	N/A	Yes	Yes
Bandwidth Management	Yes*	Yes	Yes	Yes

¹Virtual Access Points (VAPs) are supported on the integrated wireless radio only.

*With SonicOS Enhanced upgrade.



SonicWALL Clean Wireless Solution

SonicWALL's Clean Wireless solution combines 802.11n wireless controller functionality available in SonicOS 5.2 or higher for the TZ 100, TZ 200, TZ 210 Series and NSA firewall appliances with the new SonicPoint-N Dual-Band managed access point. In addition to basic wireless encryption, all wireless traffic is scanned through the firewall's Reassembly-Free Deep Packet Inspection™ engine. The SonicWALL Clean Wireless solution goes beyond mere secure wireless solutions by making wireless networks as secure as wired networks using deep packet inspection, delivering dual protection to secure the wireless network by encrypting wireless traffic and decontaminating it from network threats while also protecting the network from wireless attacks. The SonicPoint-N Dual-Band is a dependent access point that is utilized to provide seamless, secure wireless LAN (WLAN) connectivity as well as advanced features and services. SonicPoints receive 802.3af power over Ethernet (PoE) for convenient deployment in any network. The Clean Wireless Solution is built around the SonicWALL award-winning TZ, NSA and E-Class NSA Series firewall 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.



Advanced Security Services for Network Security Solutions
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service with Application Intelligence

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 email, Web, file transfer and stream-based protocols as well as instant messaging (IM) and peer-to-peer (P2P) applications. Application Intelligence delivers a suite of configurable tools to prevent data leakage while providing granular application level controls.



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 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.



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.



Software for Network Security Appliance
SonicWALL VPN Clients

For remote client-to-host secure access, SonicWALL offers both SSL VPN and IPSec VPN connectivity options. For SSL VPN, SonicWALL NetExtender allows for clientless remote access for Windows, Mac and Linux-based systems utilizing a Web portal to provide connectivity and access. For IPSec VPN, SonicWALL Global VPN Client enables the client system to download the VPN client for a more traditional client-based VPN experience.



SonicWALL Comprehensive Anti-Spam Service

SonicWALL Comprehensive Anti-Spam Service enables SonicWALL's fully-featured, market-leading protection against spam, phishing, viruses and malware with one simple check box. Using the same technology behind SonicWALL's award-winning email security product portfolio, provides a 98% effectiveness rate against spam, and reduced bandwidth consumption by eliminating up to 80% of threats at the connection level. Any remaining email is processed using SonicWALL's cloud-based Advanced Content Management service, which applies proven spam detection techniques. With no additional hardware, software or servers to purchase, you'll benefit from an integrated, single point of management, configuration and reporting.



SonicWALL Virtual Assist

SonicWALL® Virtual Assist is a 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. The easy-to-use customer Web portal provides a familiar look and feel for both Windows and Mac customers. Furthermore, the technician and standalone client facilitates the management and scheduling of the support queue. SonicWALL Virtual Assist allows tight integration by leveraging existing network and authentication infrastructures.

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 medium-sized businesses to large global enterprises. SonicWALL Aventail E-Class SSL VPNs and SonicWALL SSL VPNs for the SMB deliver flexible solutions for secure remote access, disaster recovery, wireless networking and secure extranets.

SonicWALL ^ECLASS

SonicWALL Aventail E-Class SRA Series At-A-Glance

SonicWALL Aventail E-Class Secure Remote Access (SRA) solutions 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 SRA appliances deliver robust solutions by providing:

- Secure remote access to mission-critical applications and resources from a wide range of endpoint 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
- Even greater control over portal access, content and design with the newly-enhanced SonicWALL Workplace Portal
- Enhanced security that detects inherent risks of an endpoint prior to authentication; protects resources with granular policy based on that user and endpoint; and then connects the user only to authorized resources
- Recurring EPC endpoint scans at user login and administrator-defined intervals to ensure ongoing endpoint integrity
- 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.
- A solid foundation for Network Access Control (NAC) today and in the future

Secure Remote Access Solutions — SonicWALL Aventail E-Class SRA Series SonicWALL Aventail E-Class EX7000

The SonicWALL Aventail E-Class SRA EX7000 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 EX7000 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 EX6000

The SonicWALL Aventail E-Class SRA EX6000 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 EX6000 provides easy secure access to more applications from more devices 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 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	EX6000	EX7000
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
Connect Tunnel (Windows, Mac and Linux access to TCP or UDP based applications)	Included	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 Secure Remote Access Solutions for SMB and Branch Offices At A Glance**

SonicWALL's Secure Remote Access (SRA) provides organizations of any size with an affordable, easy-to-use and manage secure clientless remote network and application access solutions that require no pre-installed client software. Utilizing only a standard Web browser, users can easily and securely access email, 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.

- Clientless connectivity removes the need for a pre-installed VPN client, thus freeing administrators from a tedious and costly task
- Seamless integration behind virtually any firewall enables organizations to leverage the existing network infrastructure
- Remote support using SonicWALL Virtual Assist enables technicians to provide secure on-demand assistance to customers while leveraging the existing infrastructure
- 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 email address, with the user's network user name and password
- Mobile device support to access an entire intranet as well as Web-based applications provides greater flexibility for a remote workforce
- Application offloading allows users to securely access Web applications while leveraging strong authentication and granular access policy features
- Clean VPN 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 SRA 4200

The SonicWALL SRA 4200 provides medium 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.



Optional SonicWALL SSL VPN Add-on Features

SonicWALL Virtual Assist

SonicWALL® Virtual Assist is a 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. The easy-to-use customer Web portal provides a familiar look and feel for both Windows and Mac customers. Furthermore, the technician and standalone client facilitates the management and scheduling of the support queue. SonicWALL Virtual Assist allows tight integration by leveraging existing network and authentication infrastructures.

Deployment	SSL-VPN 200	SRA 4200	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	SRA 4200	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
email threat
protection**

SonicWALL Email Security

Every organization needs protection from both inbound and outbound email 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 email security solution.

SonicWALL Email Security delivers the highest level of protection from inbound and outbound email threats. Leveraging a unique worldwide attack identification and monitoring network called SonicWALL Global Response Intelligent Defense (GRID) Network and combined with our continuously innovative protection techniques, SonicWALL delivers superior protection today and stands ready to stop the new attacks of tomorrow. Additionally, SonicWALL GRID Anti-Virus provides integrated SonicWALL anti-virus and anti-spyware. Protection 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 email 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 integration across multiple LDAP servers, robust reporting, automatic software updates, automatic protection updates, an integrated Junk button for Outlook® 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 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 Appliance ES6000 and ES8300 Series

SonicWALL E-Class Email Security Appliance (ESA) ES6000 and ES8300 offers comprehensive, effective and scalable email 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 email 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 appliance on a software platform. This email security solution combines best protection with effortless control and high-performance.



SonicWALL Anti-Spam SMB Solutions At-A-Glance

SMB Solutions Appliance: SonicWALL Email Security 300 and 500 Series

Ideal for small- to medium-sized organizations, SonicWALL Email Security appliances are easy-to-install and extremely effective at stopping all email 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 email 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 email.

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 email 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 email threats through an easy-to-use, Web-based administrative interface.

SonicWALL Email Security for Windows® Small Business Server (SBS) is designed to install directly on the SBS server hardware to ease installation and lower cost of ownership. It integrates with SBS to deliver superior anti-spam, anti-phishing, and anti-virus protection, and prevents DHA, DOS attacks using advanced connection management before mail traffic reaches SBS.



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 email threat protection by providing real-time anti-spam, anti-phishing and anti-virus 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 email usage. The features include detailed attachment scanning, compliance dictionaries, approval boxes, record ID matching, encryption routing, email archiving, pre-defined policies and compliance reports. By intelligently identifying emails that violate compliance policies, monitoring and reporting the problem and applying multiple enforcement options, SonicWALL can help organizations take the next step towards email compliance.

Email Security Appliances	SMB		E-Class	
	300	500	ES6000	ES8300
Model	300	500	ES6000	ES8300
Rackmount Chassis	1U Mini	1U Mini	1U Mini	2RU
CPU	2.66 GHz	2.66 GHz	3.2 GHz	Quad Core Xeon
RAM	1 GB	1 GB	2 GB	4 GB
Hard drive	80 GB	2x80 GB	2x160 GB	4x750 GB
Redundant Disk Array (RAID)	No	Yes	Yes	RAID 5
Hot Swappable Drives	No	No	No	Yes
Redundant Power Supply	No	No	No	Yes
Email Security Software				
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

SonicWALL® Continuous Data Protection (CDP) offers the only complete end-to-end backup and recovery solution for SMBs. SonicWALL CDP takes the complexity out of safeguarding your data by automating tedious tasks to provide a true low-touch solution, with flexible Offsite Data Backup, Site-to-Site Data Backup, Local Archiving and Bare Metal Recovery options to address any disaster recovery scenario. Policy-driven CDP is transparent to the end-user, ensuring that data, applications and systems are reliably protected. Because most recovery involves a single file, CDP's self-directed restore helps meet service levels while reducing burden on IT support. CDP ensures that all files are available in multiple historic versions, and that all servers and their applications—including Exchange, SQL and Active Directory databases—are protected with multiple-point-in-time versions for disaster recovery. With capacity up to 9 TB at typical compression, GbE connectivity, RAID 5, and field-replaceable components, CDP is designed to meet today's demanding requirements for performance and reliability. CDP provides foolproof, intuitive, continual protection. CDP ensures reliability and speeds recovery by automatically generating email alerts on any compromised connectivity and regularly-scheduled reports on backup activity. Extensible across multiple platforms including Windows® and Linux®, CDP can instantly recover data, applications or entire workstation or server systems onto original, new or virtual devices. CDP secures data using industry-standard encryption anytime it is transmitted offsite, offering complete business information availability for servers, desktops and mobile laptops. No other solution offers such comprehensive protection while still being so easy-to-manage.



SonicWALL Backup and Recovery Solutions At-A-Glance SonicWALL CDP 6080

The SonicWALL Continuous Data Protection (CDP) 6080 is ideal for medium size organizations demanding higher performance and capacity, offering automatic disk-based backup and recovery for multiple workstations and server applications, capacity from 4.5-9 TB (at 2:1 compression), flexible disaster recovery options, RAID 5, and replaceable drives and power supplies. The low-touch CDP 6080 automatically enforces policy-driven, user-transparent backups of multiple versions of files and applications—including Exchange and SQL databases. The CDP 6080 offers flexible disaster recovery options for Local Archiving, Offsite Data Backup, Site-to-Site Data Backup, and Bare Metal Recovery of entire systems onto original, virtual or new Windows or Linux devices.

SonicWALL CDP 5040

The SonicWALL Continuous Data Protection (CDP) 5040 is ideal for small-to-medium size organizations demanding high-performance and capacity. The CDP 5040 offers automatic disk-based backup and recovery for multiple workstations and server applications, capacity of up to 4.5 TB (at standard 2:1 compression ratios), flexible disaster recovery options, RAID 5 and replaceable drives. The low-touch CDP 5040 automatically enforces policy-driven, user-transparent backups of multiple versions of files and applications—including Exchange and SQL databases. The CDP 5040 offers flexible disaster recovery options for Local Archiving, Offsite Data Backup, Site-to-Site Data Backup, and Bare Metal Recovery of entire systems onto original, virtual or new Windows or Linux devices.



SonicWALL CDP 210

The SonicWALL Continuous Data Protection (CDP) 210 is ideal for small distributed environments and remote or branch offices requiring complete end-to-end disk-based backup and recovery for multiple workstations and servers with a capacity of up to 2 TB (at standard 2:1 compression ratios). The low-touch CDP 210 automatically enforces policy-driven, user-transparent backups of multiple versions of files and applications—including Exchange and SQL databases. The CDP 210 offers flexible disaster recovery options for Local Archiving, Offsite Data Backup, Site-to-Site Data Backup, and Bare Metal Recovery of entire systems onto original, virtual or new Windows or Linux devices.

SonicWALL CDP 110

The SonicWALL Continuous Data Protection (CDP) 110 is ideal for smaller distributed environments and remote or branch offices requiring complete end-to-end disk-based backup and recovery for multiple workstations and servers with a capacity of up to 800 GB (at standard 2:1 compression ratios). The low-touch CDP 110 automatically enforces policy-driven, user-transparent backups of multiple versions of files and applications—including Exchange and SQL databases. The CDP 110 offers flexible disaster recovery options for Local Archiving, Offsite Data Backup, Site-to-Site Data Backup, and Bare Metal Recovery of entire systems onto original, virtual or new Windows or Linux devices.

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.

Backup and Recovery Solutions

Feature	CDP 110	CDP 210	CDP 5040	CDP 6080
Appliance Characteristic				
Form Factor	Desktop	Desktop	1U	2U
RAID Support	-	-	RAID 5	RAID 5
Total Capacity (Raw)	400 GB	1 TB	3 TB	3 TB (6 TB max.)
Total Capacity (Useable Uncompressed)	400 GB	1 TB	2.25 TB	2.25TB (4.5 TB max.)
Total Capacity (Useable@Typical 2:1 Compression)	800 GB	2 TB	4.5 TB	4.5 TB (9 TB max.)
Network Interface	100baseT	100baseT	1 GbE	1 GbE
Hot-swappable and Redundant Power Protection	-	-	-	Yes
Replaceable Hard Drive	-	-	Yes	Yes
Users (Recommended)	<15	<25	<60	<100
Servers (Recommended)	<5	<5	<10	<15
Backup and Recovery				
Continuous Data Protection (CDP)	Yes	Yes	Yes	Yes
Transparent, Automated Backup	Yes	Yes	Yes	Yes
User Directed Recovery	Yes	Yes	Yes	Yes
Flexible Disaster Recovery options	Yes	Yes	Yes	Yes
Direct backup of server, laptop and desktop	Yes	Yes	Yes	Yes
Application Support – Exchange, SQL, AD	Yes	Yes	Yes	Yes
Central Administration				
Enforced Policy-base Backup	Yes	Yes	Yes	Yes
Reporting and Alerting	Yes	Yes	Yes	Yes
AES 256-bit Encryption	Yes	Yes	Yes	Yes
Auto-discovery of Database for backup	Yes	Yes	Yes	Yes
Disaster Recovery				
Site-to-Site Backup	Yes	Yes	Yes	Yes
Local Archiving	Yes	Yes	Yes	Yes
Online Backup (Offsite Datacenter)	Yes	Yes	Yes	Yes
Bare Metal Recovery with Universal Restore	Yes	Yes	Yes	Yes
Bare Metal Recovery – Server	Yes	Yes	Yes	Yes

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 (GMS)

SonicWALL Global Management System (GMS) provides organizations of any size, distributed enterprises and service providers with a flexible, powerful and intuitive tool to centrally manage and rapidly deploy SonicWALL firewall, anti-spam, backup and recovery, secure remote access solutions and security policy configurations. Flexibly deployed as software, hardware—in the form of the Universal Management Appliance (UMA)—or a virtual appliance. 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™ also provides centralized real-time monitoring, and comprehensive policy and compliance reporting. SonicWALL GMS' intuitive Web-based user interface easily allows for complete life cycle control of thousands of SonicWALL firewall, anti-spam, secure remote access, and backup and recovery appliances and services—from initial configuration to complex policy changes and remote updates. For enterprises, GMS simplifies the complexity of network management by offering a single management interface, thereby reducing administration time, complexity and the overall total cost of ownership (TCO). Service providers benefit from its multi-organizational management capabilities where it consolidates, groups and classifies thousands of individual customers' managed appliances and their respective security policies. Through an integrated reporting architecture, administrators can customize and schedule reports individually tailored to meet the needs of managed customers, executives and regulatory compliance audits for corporate departments.



- **GMS Software** – SonicWALL GMS can be flexibly deployed as a software application on a third party Windows® server, leveraging existing infrastructure.
- **Universal Management Appliance** – The UMA, leveraging a hardened high-performance appliance, simplifies and automates multi-level policy management, monitoring and compliance reporting with flexible, powerful and intuitive tools. Multiple UMA devices, when deployed in a cluster, can scale to manage up to thousands of SonicWALL security appliances.
- **GMS Virtual Appliance** – Appliance provides a hardened, performance-optimized virtual appliance agent for the SonicWALL Global Management System. In the past, under the “one server, one application” model, administrators often underutilized hardware resources and spent considerable time on server management.



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 helps organizations of all sizes track network utilization, monitor security activity and view Web usage. Available as software or virtual appliance, SonicWALL ViewPoint can be deployed as a software application on a third party Windows® server or as a SonicWALL GMS Virtual Appliance in a VMware® environment.



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, email security appliances and data backup and recovery installations spread across the enterprise.



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.

E-Class Support 24x7

Designed for customers with SonicWALL E-Class solutions, SonicWALL E-Class Support 24x7 delivers the enterprise-class support features and quality of service that enterprise organizations require to keep their networks running smoothly and efficiently.

- 24x7 direct access to a team of highly-trained Senior Support Engineers for telephone, email and Web-based technical support
- Subscription to firmware updates and upgrades
- Advance Exchange hardware replacement in the event of failure

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:

- Subscription to firmware updates and upgrades
- Access to telephone, email and Web-based technical support
- Advance Exchange hardware replacement in the event of failure

Comprehensive Global Management System Support (CGMS Support)

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

- All the services and advantages of an E-Class Support 24x7 contract
- Support and software updates for the GMS application itself
- One expiration date for everything, simplifying management and administration

Focused Technical Support

Mission critical customers need mission critical support. SonicWALL Focused Technical Support (FTS) is designed to provide our most important customers the highest-quality, most responsive support services available in the industry. This premium support offering includes a comprehensive suite of proactive services, all of which are managed by a designated SonicWALL Security Engineer (SSE) who understands your technical requirements and your business.

- A customized service for organizations who need high-end enterprise-class support with a designated resource
- Available in 8x5 (FTS Standard and Lite) or 24x7 (FTS Ultra)
- Immediate access to subject matter experts (SMEs) and a fast-track into SonicWALL for enhanced escalation and new feature processing



SonicWALL Remote Start-up and Configuration Service

SonicWALL Remote Start-up and Configuration Service provides businesses of all sizes with rapid, secure configuration and deployment of their SonicWALL appliance into a new or existing network. The remote configuration is performed by CSSA-certified technicians using SonicWALL’s proven methodology, ensuring the solution is properly configured and ready for deployment. The service minimizes costs associated with configuring and deploying new appliances while enhancing productivity by freeing up valuable resources to focus on other critical needs. With Remote Configuration Service, your SonicWALL appliance will be up and running in a matter of hours, allowing you to realize a faster return on your SonicWALL investment.

Customer Advantage Program

The Customer Advantage Program provides two key mechanisms for keeping your infrastructure up to date—Secure Upgrade Plus and Customer Loyalty Bundle:

Secure Upgrade Plus

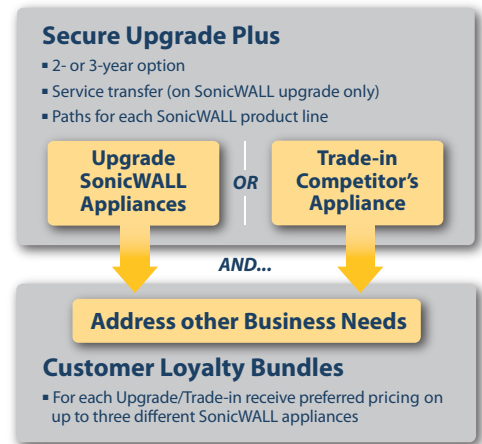
Whether you are upgrading older SonicWALL appliances or trading-in products from a competitor, Secure Upgrade Plus recognizes your past investments and enables you to upgrade easily and affordably. Save up to 50% on the total annual cost of most solutions (compared with purchasing hardware separately and only one year of services separately).

This option now covers all SonicWALL product categories, including Continuous Data Protection (CDP), Email Security (ES), Secure Remote Access (SSL VPN) and Network Security/firewall (UTM) appliances. For the complete listing of eligible SonicWALL and competitive products, see the Secure Upgrade Program Terms and Conditions. Customers who participate in Secure Upgrade Plus also qualify to receive preferred Customer Loyalty Bundle pricing on the purchase of additional products.

Customer Loyalty Bundle

The SonicWALL Customer Loyalty Bundle acknowledges our customers’ trust and reflects our commitment to them by rewarding customers who deploy multiple SonicWALL product lines. Qualified customers can save up to 30% off MSRP on appliances from each of SonicWALL’s other product lines. For each upgrade or trade-in purchase, customers can purchase as many as one additional product from each of the other product lines at this preferred price. The Customer Loyalty Bundle is available to those who participate in Secure Upgrade Plus and is available only at the time of an upgrade or trade-in purchase.

SonicWALL designed the Customer Advantage Program to serve you better by removing the cost and complexity of owning the most effective, up-to-date, enterprise-class network security and data protection systems available.



A Vision for Dynamic Security for the Global Network

Our vision is simple: we believe security solutions should be “smart” enough to adapt as organizations evolve and as threats evolve, dynamically, globally. We believe customers around the world should have the ability to control, manage and protect their global network easily and automatically. We believe our customers should be able to receive and share threat and defense data around the world so they can anticipate and stop attacks before they happen. We want our customers to be able to secure any user, any device, using any application from anywhere so they can collaborate securely across different networks. All this needs to be achieved with maximum ease of deployment and at the best economic value and in a compliant framework.

Built upon a shared network of millions of global touch points, Dynamic Security begins by leveraging the SonicWALL GRID Network and the SonicWALL Threat Center that provide continuous communication, feedback, and analysis regarding the nature and changing behavior of threats worldwide. SonicWALL Research Labs continuously processes this information, proactively delivering defenses and dynamic updates that defeat the latest threats. Utilizing behavioral analysis, our innovative malware identification signature language can detect blended malware to help secure organizations in advance of many of the most malicious cyber attacks.

SonicWALL further leverages technological innovation with its patented Reassembly-Free Deep Packet Inspection (RFDPI) technology—the foundation for all SonicWALL network security products. By combining our single engine with a high speed, multi-core, parallel hardware architecture, we enable simultaneous, multi-threat scanning and analysis at wire speed. Importantly, this also provides the technical framework that allows the entire solution to scale for deployment in high bandwidth networks. Finally, by integrating advanced networking and remote access technologies, SonicWALL verifies and defends the security of traditional and mobile wireless networks, users and applications—and their endpoint devices—while scanning and disinfecting the entire data stream across platforms and perimeters. Along with the technological scalability, SonicWALL’s policy and administration management scales easily as your organization grows.

More and more, customers everyday are seeing SonicWALL as the partner who understands the technology, business, social and security challenges ahead and has the long term vision for a secure future matched with an innovative technological and business approach. SonicWALL drives the cost and complexity out of building and running secure infrastructures, thus enabling organizations of all sizes to achieve greater productivity and IT efficiencies.

SonicWALL’s financial, operational and technological excellence makes it the right partner to help you secure your business with **Dynamic Security for the Global Network**.

Award-winning Leadership

Established in 1991, SonicWALL is the global leader of dynamic network security and data protection solutions for small, mid-sized through large enterprise organizations. SonicWALL’s global network of strategic partners, resellers and distributors are some of the best-known names in information technology. Earning high recognition from key industry publications, SonicWALL products have been recognized with seven 5-Star reviews from SC Magazine over the past year. Other awards include: 2009 InfoWorld Technology of the Year for Networking and Security, SC Magazine 2010 Award finalists, eWeek’s Channel Insider 2008 Products of the Year, and SearchNetworking.com’s 2008 Product Leadership. With over 15,000 resellers and distributors worldwide, SonicWALL has won top honors in the VAR Business Annual Report Card in the security appliance category in four out of the past 5 years. SonicWALL is rated among the top three brands among U.S. resellers according to CMP’s VAR Business.

SonicWALL Inc. has shipped over one million appliances through its global network of channel partners to keep tens of millions of worldwide business computer users safe and in control of their data. SonicWALL’s award-winning solutions include network security, secure remote access, content security, backup and recovery, and policy and management technology. For more information, visit the company web site at <http://www.sonicwall.com/>.

SonicWALL’s line-up of comprehensive protection



NETWORK
SECURITY



SECURE
REMOTE ACCESS



WEB AND E-MAIL
SECURITY



BACKUP
AND RECOVERY



POLICY AND
MANAGEMENT

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com



PROTECTION AT THE SPEED OF BUSINESS™