Dell SonicWALL product lines

SonicWALL

Table of contents

DELL SonicWALL

Overview

Threat management

Internet threats have transformed from mere annoyances to sophisticated malicious attacks that can dramatically impede business. Dell™ SonicWALL™ solutions offer intelligent protection against these intricate and evolving threats by seamlessly integrating network security, and web and email security. Dell SonicWALL Network Security provides deep protection against viruses, worms, Trojans, spyware and intrusions while delivering enterprise-levels of network performance without compromising performance. Dell 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. Dell SonicWALL Application Intelligence, Control and Visualization extends control over nonproductive applications like online trading, instant messaging/chat, peer-to-peer sharing and streaming video sites. Dell 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. Dell SonicWALL's intelligent 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, smartphones and tablets accessing the corporate network, and the demand for business continuity have made mobility a business imperative. Dell SonicWALL provides organizations of all sizes with mobility solutions over broadband, and cellular connections. Integrated with Dell SonicWALL Next-Generation Firewall protection, Dell SonicWALL network security provides secure site-to-site connections or secure remote access using IPSec or SSL VPN. Combining these appliances with self-configuring SonicPoint access points instantly provides provisional temporary networks with secure wireless hotspot connectivity. Dell SonicWALL firewalls can establish secure 3G wireless broadband virtually anywhere in an instant without a fixed Internet connection. Additionally, Dell SonicWALL dedicated SSL VPNs extend secure mobile access to virtually any remote location over standard web browsers or mobile devices including wireless smartphones and tablets. Dell SonicWALL SSL VPN solutions also offer unsurpassed levels of granular access control.

Application control

Dell SonicWALL Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. A tightly integrated feature of Dell SonicWALL Next-Generation Firewalls, it uses the patented Dell SonicWALL Reassembly-Free Deep Packet Inspection® (RFDPI)* to identify and control applications, regardless of port or protocol. With a continuously expanding signature database currently recognizing over 3,500 applications and millions of malware threats, it can maintain granular control over applications, prioritize or throttle bandwidth and deny web site access. The Dell SonicWALL Application Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active web site connections and user activity.

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. Dell SonicWALL can help any organization meet mandated regulations, with best-in-class encryption technology and deep packet inspection to ensure "Clean VPN," connectivity. Dell SonicWALL SSL VPN solutions offer data encryption and authentication, granular access control, policy management, logging capability and flexible authentication architecture. Dell 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, Dell SonicWALL Content Filtering Service protects your network from illicit or unproductive web content. Finally, the award-winning Dell SonicWALL Global Management System (GMS®) provides comprehensive audit trails with centralized real-time monitoring, and comprehensive policy and compliance reporting.

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. Dell SonicWALL offers business continuity and recovery solutions for any size organization. With Dell SonicWALL SSL VPN solutions, isolated workers can remain as productive from home or other contingent locations as if they were in the office. The Dell SonicWALL Backup and Recovery solution provides automatic, real-time data backup and flexible disaster recovery options for servers, laptops and PCs. The Dell SonicWALL Continuous Data Protection (CDP) Series protects files locally as well as at offsite locations to ensure data can be instantly recovered.

Application traffic analytics

Dell SonicWALL Application Traffic Analytics solutions provide organizations with powerful insight into application traffic, bandwidth utilization and security threats while providing powerful troubleshooting and forensics capabilities. The Dell SonicWALL Global Management System and Analyzer leverage application traffic analytics data from Dell SonicWALL firewalls for powerful insight into the network. Dell SonicWALL Scrutinizer offers additional compatibility with third-party routers and switches.

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Dell SonicWALL firewall/network security

Dell SonicWALL is one of the leading providers of Next-Generation Firewalls. When deployed as a Next-Generation Firewall solution, Dell SonicWALL firewalls tightly integrate RFDPI to deliver superior intrusion prevention, malware protection, application intelligence, control and real-time visualization, and inspection for SSL encrypted sessions. Essential to an intelligent and highly adaptive security system, Dell SonicWALL Next-Generation Firewalls scan every byte of every packet for the deepest level of protection. Unlike competitive offerings, the single-pass RFDPI engine enables simultaneous, multi-threat and application scanning and analysis of unlimited files sizes and connections, without packet reassembly. This enables Dell SonicWALL firewalls to massively scales to extend state-of-the-art security to growing and distributed enterprise networks. Dell SonicWALL network security appliances can also be deployed as Unified Threat Management (UTM) firewalls that offer comprehensive security combining gateway content filtering, anti-spam, anti-virus, anti-spyware, intrusion prevention, and application intelligence and control.

Dell SonicWALL's patented* Reassembly-Free Deep Packet Inspection (RFDPI) technology enables simultaneous, multi-threat and application scanning and analysis of unlimited files sizes and connections at extremely high speeds. Going far beyond simple stateful inspection, the RFDPI engine scans against multiple application types and protocols to ensure your network is protected from internal and external attacks. This single code base is at the core of every Dell SonicWALL firewall, from the TZ 105 to the Dell SonicWALL SuperMassive E10800. SuperMassive E10800 with SonicOS is the highest overall protection Next-Generation Firewall to earn the NSS Labs Recommend rating. RFDPI is tightly integrated into the firewall platform, streamlining management of granular firewall policies, directly via the firewall interface or via the Dell SonicWALL Global Management System. Organizations can choose from an entire line of proven Dell SonicWALL firewalls with SonicOS, which massively scale to meet the needs of the highest performance networks. Moreover, by leveraging the unique Dell SonicWALL Global Response Intelligent Defense (GRID) Network worldwide attack identification and monitoring network, Dell SonicWALL firewalls deliver superior protection today and stands ready to stop the new attacks of tomorrow.

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Highest Overall Protection Next-Generation Firewall "Recommended" by NSS Labs

SuperMasssive E10800 Running SonicOS 6.0

Dell SonicWALL SuperMassive E10000 Series at-a-glance

The SuperMassive E10000 Series is Dell SonicWALL's Next-Generation Firewall platform designed to deliver scalability, reliability and deep security at multi-gigabit speeds for large networks. Built to meet the needs of enterprise, government, university, and service provider deployments, the SuperMassive E10000 Series is ideal for securing enterprise networks, data centers and server farms. Combining massively scalable multi-core design and the patented RFDPI* technology, the SuperMassive E10000 Series delivers industry-leading application control, intrusion prevention, malware protection and SSL inspection.

SuperMassive E10800
- Cores: 96
- IPS throughput: 30 Gbps
- Firewall throughput: 40 Gbps
- Max connections: 12.0M
- Application inspection throughput: 30 Gbps
- Threat-prevention throughput: 12 Gbps

SuperMassive E10400
- Cores: 48
- Max connections: 6.0M
- Firewall throughput: 20 Gbps
- Upgrade path: field upgradeable to the E10800
- Application inspection throughput: 15 Gbps
- IPS throughput: 15 Gbps
- Threat-prevention throughput: 6.0 Gbps

SuperMassive E10200
- Cores: 24
- Max connections: 3.0M
- Firewall throughput: 10 Gbps
- Upgrade path: field upgradeable to the E10400, E10800
- Application inspection throughput: 7.5 Gbps
- Threat-prevention throughput: 3.0 Gbps
- IPS throughput: 7.5 Gbps

SuperMassive E10000 Series

Feature	E10200	E10400	E10800
System specifications			
Operating system		SonicOS	
Cores	24	48	96
10 GbE interfaces		6 x 10-GbE SFP+	
1 GbE interfaces		16 x 1-GbE SFP	
Management interfaces		1 GbE, 1 Console	
Memory (RAM)	16 GB	32 GB	64 GB
Storage		80 GB SSD, Flash	
Firewall throughput	10 Gbps	20 Gbps	40 Gbps
Application inspection throughput	7.5 Gbps	15 Gbps	30 Gbps
IPS throughput	7.5 Gbps	15 Gbps	30 Gbps
Anti-malware inspection throughput	3.0 Gbps	6.0 Gbps	12 Gbps
VPN throughput	5.0 Gbps	10 Gbps	20 Gbps
Connections per second	160,000/sec	320,000/sec	640,000/sec
Maximum connections (SPI)	3.0M	6.0M	12.0M
Maximum connections (DPI)	2.5M	5.0M	10.0M
VPN			
Site-to-site tunnels	10,000 (20,000)*	10,000 (40,000)*	10,000 (80,000)*
IPSec VPN clients	2,000 (4,000)*	2,000 (8,000)*	2,000 (16,000)*
SSL VPN licenses	50 (2,000)*	50 (4,000)*	50 (8,000)*
Encryption		DES, 3DES, AES (128, 192, 256-bit)	
Authentication		MD5, SHA-1	
Key exchange		Diffie Hellman Groups 1, 2, 5, 14	
Route-based VPN		RIP, OSPF	
Networking			
IP address assignment		Static (DHCP PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay	
NAT modes		1:1, many:1, 1:many, many:many, flexible NAT (overlapping Ips), PAT, transparent mode	
VLAN interfaces		512	
Routing protocols		OSPF, RIPv1/v2, BGP*, static routes, policy-based routing, multicast	
QoS		Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p	
Authentication		XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, terminal services, Citrix	
IPv6		Yes	
VoIP		Full H323-v1-5, SIP	
Standards		TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
Hardware			
Power supply		Dual, Redundant, Hot Swappable, 850W	
Fans		Dual, Redundant, Field Replaceable	
Display		Front LCD Display	
Input power		100-240 VAC, 60-50 Hz	
Maximum power consumption (W)	400	500	750
Form factor		4U Rack Mountable	
Dimensions		17x18x7 in (43x43.5x17.8 cm)	
Weight	58 lb (26.3 kg)	61 lb (27.7 kg)	67 lb (30.3 kg)
WEEE weight	59 lb (26.8 kg)	62 lb (28.1 kg)	68 lb (30.8 kg)
Shipping weight	79 lb (35.8 kg)	82 lb (37.2 kg)	88 lb (39.9 kg)
Major regulatory		FCC Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE	
Environment		40-105 F, 5-40 deg C	
Humidity		10-90% non-condensing	

*Available with expanded license.
All specifications, features and availability are subject to change.

Dell SonicWALL's enterprise- level E-Class NSA Series uses a multi-core microprocessor that can run RFDPI full throttle without compromising network speed.

Dell SonicWALL enterprise solutions: E-Class NSA Series at-a-glance

Dell SonicWALL E-Class Network Security Appliance (NSA) Series Next-Generation Firewalls provide enterprise-performance featuring tightly integrated intrusion prevention, anti-malware protection and application intelligence, control and visualization. Combining Dell SonicWALL's patented Reassembly-Free Deep Packet Inspection (RFDPI)* technology with a powerful multi-core hardware platform, E-Class NSA Series solutions can analyze and control thousands of unique applications, even if encrypted with SSL. Integrated application traffic analytics reporting provides the E-Class NSA Series with powerful insight into network usage.

The E-Class NSA Series are engineered to be the most scalable, high-performance and reliable multi-function threat appliances in their class. Gateway anti-virus, anti-spyware and intrusion prevention deliver real-time network security protection against sophisticated application layer and content-based attacks including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows. Taking protection to new levels of control, application intelligence, control and visualization capabilities offer a complete view into network traffic and a set of customizable policies affording administrators highly granular control over applications and users on the network. 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. In addition, the E-Class NSA Series addresses the multifunction security needs of federal, state and local governments and to meet certification requirements such as Federal Information Processing Standards (FIPS) and Common Criteria for Information Technology Security Evaluation Assurance Levels (Common Criteria 3.1 EAL 4+). The E-Class NSA Series delivers:

- Enterprise-class RFPDI with intrusion prevention, malware protection and application intelligence, control and visualization for every packet, every protocol, over every interface
- Revolutionary multi-core performance utilizing up to 16 cores for high-speed multi-layered threat protection over both external and internal networks
- Ultimate scalability in eliminating threats across unlimited file sizes and unrestricted concurrent connections by utilizing the RFDPI 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. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

ICSA labs CERTIFIED FIREWALL - CORPORATE

Dell SonicWALL E-Class Network Security Appliance E8510 and E8500

The Dell SonicWALL NSA E8510 and E8500 Next-Generation Firewalls are designed for enterprise networks requiring full deep packet inspection protection and application control without compromising performance. The NSA E8510 combines tightly integrated intrusion prevention, sophisticated malware protection, and powerful application intelligence, control and visualization. With the patented Dell SonicWALL RFDPI* engine, these firewalls can analyze and control thousands of applications, even if they are encrypted with SSL. This exceptional combination of software sophistication and incredibly powerful hardware leaves little room for application traffic to hide on the network, since Dell SonicWALL RFDPI engine is capable of inspecting hundreds of thousands of connections simultaneously across all ports, with nearly zero latency and without file size limitations.

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED FIREWALL - ENTERPRISE

Dell SonicWALL E-Class Network Security Appliance E6500 and E5500

The Dell SonicWALL NSA E6500 and E5500 Next-Generation Firewalls are engineered to meet the needs of the expanding enterprise network by providing high-performance, scalable solutions. These firewalls take advantage of specialized multi-core processing technology, providing parallel traffic processing, in conjunction with the patented Dell SonicWALL RFDPI* engine to deliver deep packet inspection performance for enterprise networks. Now enterprise administrators have a high-performance secure platform to combat the changing threat landscape. Taking protection to new levels of control, Dell SonicWALL's Application Intelligence, Control and Visualization offers a real-time view into network traffic and a set of customizable policies affording administrators highly granular control over applications and users on the network. These firewalls come standard with eight gigabit copper Ethernet ports for deployment flexibility and include a management LCD screen for ease of deployment.

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED FIREWALL - ENTERPRISE

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Dell SonicWALL SMB and branch office solutions: NSA Series at-a-glance

The Dell SonicWALL Network Security Appliance (NSA) Series combines the patented Dell SonicWALL RFDPI* engine with a powerful and massively scalable multi-core architecture to deliver intrusion prevention, gateway anti-virus, gateway anti-spyware, and application intelligence and control for businesses of all sizes. By integrating automated and dynamic security capabilities into a single platform, the NSA Series provides comprehensive protection without compromising performance. The NSA Series delivers high-speed intrusion prevention, file and content inspection and powerful application intelligence, control and visualization capabilities. It offers 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 Series simplifies set-up and configuration. The NSA Series also supports virtual local area networks (VLANs), enterprise-class routing and QoS features, further extending security and performance throughout the network. In addition, the NSA series enables compliance with certification requirements such as FIPS and Common Criteria EAL 4+

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

Dell SonicWALL Network Security Appliance 4500

The Dell SonicWALL NSA 4500 is a Next-Generation Firewall designed to meet the demands of corporate central-site and large distributed environments, built upon an eight-core hardware platform. With six configurable gigabit Ethernet (GbE) interfaces, the NSA 4500 is an ideal solution for corporate perimeter protection and remote access connectivity.

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

Dell SonicWALL Network Security Appliance 3500

The Dell SonicWALL NSA 3500 is a Next-Generation Firewall utilizing four cores and six gigabit Ethernet (GbE) interfaces.

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

Dell SonicWALL Network Security Appliance 2400

The Dell SonicWALL NSA 2400 is a Next-Generation Firewall that utilizes multi-core hardware and six gigabit Ethernet (GbE) interfaces.

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Dell SonicWALL Network Security Appliance 250M Series

The Dell SonicWALL NSA 250M Series modular Next-Generation Firewalls offer branch offices and distributed enterprises in-depth frontline security and optional 802.11 dual-band wireless. The NSA 250M can be extended with a variety of modules, such as T1/E1, DSL and SFP Modules, in order to provide deployment flexibility and additional failover capabilities, as well as reduce acquisition and maintenance costs.

Dell SonicWALL Network Security Appliance 220 Series

The Dell SonicWALL NSA 220 Series Next-Generation Firewalls offer branch offices and distributed enterprises easy-to-manage in-depth frontline security, and optional 802.11 dual-band wireless.

Network Security Appliances Series

Feature	NSA 220/W-N	NSA 250M/W-N	NSA 2400	NSA 3500	NSA 4500
SonicOS supported	SonicOS 5.8.1.1	SonicOS 5.8.1.1	SonicOS Enhanced 5.6 (or higher)	SonicOS Enhanced 5.6 (or higher)	SonicOS Enhanced 5.6 (or higher)
Users and nodes	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Network interfaces	(7) 10/100/1000 Gigabit Ports, 2 USB, 1 Console Interface	(5) 10/100/1000 Gigabit Ports, 2 USB, 1 Console Interface, Module Slot	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB (Future Use)	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB	(6) 10/100/1000 Copper GigabitPorts, 1 Console Interface, 2 USB
Power supply	External 36W	External 36W	Single 180W ATX	Single 180W ATX	Single 180W ATX
Cooling system (fans)	No Fan/1 Fan	2 Fans	2 Fans	2 Fans	2 Fans
VLAN interfaces	25	35	25	50	200
High availability	Active/Passive with Optional State Sync	Active/Passive with Optional State Sync	Active/Passive with Optional State Sync	Active/Passive with Optional State Sync	Active/Passive with State Sync
Stateful throughput[1]	600 Mbps	750 Mbps	775 Mbps	1.5 Gbps	2.75 Gbps
3DES/AES throughput[2]	150 Mbps	200 Mbps	300 Mbps	625 Mbps	1.0 Gbp
Gateway anti-virus throughput[3]	115 Mbps	140 Mbps	160 Mbps	350 Mbps	690 Mbps
Intrusion prevention throughput[3]	195 Mbps	250 Mbps	275 Mbps	750 Mbps	1.4 Gbps
Full DPI performance[3]	110 Mbps	130 Mbps	150 Mbps	240 Mbps	600 Mbps
IMIX performance[3]	180 Mbps	210 Mbps	235 Mbps	580 Mbps	700 Mbps
New connections per second	2,200	3,000	4,000	7,000	10,000
Maximum connections	85,000	110,000	225,000	325,000	500,000
Maximum DPI connections	32,000	64,000	125,000	175,000	250,000
Site-to-site VPNs	25	50	75	800	1,500
Zone security	Yes	Yes	Yes	Yes	Yes
Object-based management	Yes	Yes	Yes	Yes	Yes
Policy-based NAT	Yes	Yes	Yes	Yes	Yes
Multiple ISP failover	Yes	Yes	Yes	Yes	Yes
Load balancing	Yes	Yes	Yes	Yes	Yes
Integrated wireless switch and controller	Yes	Yes	Yes	Yes	Yes
3G wireless failover	Yes	Yes	—	Yes	Yes
Policy-based routing	Yes	Yes	Yes	Yes	Yes
Comprehensive Anti-Spam Service	Optional	Optional	Optional	Optional	Optional
Voice over IP (VoIP)	Yes	Yes	Yes	Yes	Yes
IKEv2 VPN	Yes	Yes	Yes	Yes	Yes
Secure remote management (SSHv2 support)	Yes	Yes	Yes	Yes	Yes
SSL VPN and IPSec VPN remote access clients	Yes	Yes	Yes	Yes	Yes
Secure Virtual Assist technicians	30-day Trial	30-day Trial	Yes	Yes	Yes
Route-based VPN	Yes	Yes	Yes	Yes	Yes
TSA User authentication	Yes	Yes	Yes	Yes	Yes
Dynamic address objects	Yes	Yes	Yes	Yes	Yes
Layer 2 bridge mode	Yes	Yes	Yes	Yes	Yes
Layer 2 wireless bridging	Yes	Yes	No	No	No
Wireless switch and controller	Yes	Yes	No	No	No
802.1q VLANs	Yes	Yes	Yes	Yes	Yes
RIPv2 and OSPF routing	Yes	Yes	Yes	Yes	Yes
Single Sign-On (SSO)	Yes	Yes	Yes	Yes	Yes
Application intelligence and control	Optional	Optional	Optional	Optional	Optional
Deep Packet Inspection SSL	Optional	Optional	Optional	Optional	Optional
SSL control	Yes	Yes	Yes	Yes	Yes
IPv6[4]	No	No	Yes	Yes	Yes
Application visualization	Yes	Yes	Yes	Yes	Yes
NetFlow/IPFIX	Yes	Yes	Yes	Yes	Yes

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.
[3] Full DPI/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.
[4] IPv6 functionality requires separate firmware.
*With Stateful HA and Expansion Upgrade.

E-Class Network Security Appliances Series

Feature	NSA E5500	NSA E6500	NSA E8500	NSA E8510
SonicOS supported	SonicOS Enhanced 5.6 (or higher)	SonicOS Enhanced 5.6 (or higher)	SonicOS Enhanced 5.6 (or higher)	SonicOS Enhanced 5.81 (or higher)
Users and nodes	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Network interfaces	(8) 10/100/1000 Copper Gigabit Ports, 1 GbE HA Interface, 1 Console Interface, 2 USB	(8) 10/100/1000 (4) 10/100/1000 GbE, 1 GbE HA Interface, 1 Console Interface, 2 USB	(4) SFP (SX, LX or TX), (4) 10/100/1000 GbE, 1GbE HA Interface, 2 USB, 1 Console Interface	(2) SFP+ 10GbE, (4) 10/100/1000 GbE, 1 GbE HA Interface, 2 USB, 1 Console Interface
Power supply	Single 250W ATX	Single 250W ATX	Dual 250W ATX, Hot Swappable	Dual 250W ATX, Hot Swappable
Cooling system (fans)	Dual Fans, Hot Swappable	Dual Fans, Hot Swappable	Dual Fans, Hot Swappable	Dual Fans, Hot Swappable
VLAN interfaces	400	500	512	512
High availability	Active/Passive with State Sync, Active/Active DPI with State Sync	Active/Passive with State Sync, Active/Active DPI with State Sync	Active/Passive with State Sync, Active/Active DPI with State Sync	Active/Passive with State Sync, Active/Active DPI with State Sync
Stateful throughput[1]	3.9 Gbps	5.0 Gbps	8.0 Gbps	8.0 Gbps
3DES/AES throughput[2]	1.7 Gbps	2.7 Gbps	4.0 Gbps	4.0 Gbps
Gateway anti-virus throughput[3]	1.0 Gbps	1.69 Gbps	2.25 Gbps	2.25 Gbps
Intrusion prevention throughput[3]	2.0 Gbps	2.3 Gbps	3.7 Gbps	3.7 Gbps
Full DPI performance[3]	850 Mbps	1.59 Gbps	2.2 Gbps	2.2 Gbps
IMIX performance[3]	1.1 Gbps	1.4 Gbps	2.0 Gbps	2.0 Gbps
New connections per second	30,000	60,000	85,000	85,000
Maximum connections	750,000	1,000,000	1,500,000	1,500,000
Maximum DPI connections	500,000	600,000	1,250,000	1,250,000
Site-to-site VPNs	4,000	6,000	10,000	10,000
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
Load balancing	Yes	Yes	Yes	Yes
Integrated wireless switch and controller	Yes	Yes	Yes	Yes
3G wireless failover	Yes	Yes	Yes	Yes
Policy-based routing	Yes	Yes	Yes	Yes
Comprehensive Anti-Spam Service	Optional	Optional	Optional	Optional
Voice over IP (VoIP)	Yes	Yes	Yes	Yes
IKEv2 VPN	Yes	Yes	Yes	Yes
Secure remote management (SSHv2 support)	Yes	Yes	Yes	Yes
SSL VPN and IPSec VPN remote access clients	Yes	Yes	Yes	Yes
Secure Virtual Assist technicians	Yes	Yes	Yes	Yes
Route-based VPN	Yes	Yes	Yes	Yes
TSA User authentication	Yes	Yes	Yes	Yes
Dynamic address objects	Yes	Yes	Yes	Yes
Layer 2 bridge mode	Yes	Yes	Yes	Yes
802.1q VLANs	Yes	Yes	Yes	Yes
RIPv2 and OSPF routing	Yes	Yes	Yes	Yes
Single Sign-On (SSO)	Yes	Yes	Yes	Yes
Application intelligence and control	Optional	Optional	Yes	Ye
Deep Packet Inspection SSL	Optional	Optional	Yes	Yes
SSL control	Yes	Yes	No	No
IPv6[4]	Yes	Yes	Yes	Yes
Application visualization	Yes	Yes	Yes	Yes
NetFlow/IPFIX	Yes	Yes	Yes	Yes
Link aggregation	Yes[5]	Yes[5]	Yes[5]	Yes[5]
Port redundancy	Yes	Yes	Yes	Yes

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.
[3] Full DPI/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.
[4] IPv6 functionality requires separate firmware.
[5] Static Link Aggregation.
*With Stateful HA and Expansion Upgrade.

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

Dell SonicWALL branch office and SMB solutions: TZ Series at-a-glance

The Dell SonicWALL TZ Series is the among most secure Unified Threat Management (UTM) firewalls for small businesses, retail deployments, government organizations, remote sites and branch offices. Unlike consumer-grade products, the TZ Series delivers highly effective anti-malware, intrusion prevention, content/URL filtering and application control capabilities along with broad mobile platform support for laptops, smartphones and tablets. It provides full deep packet inspection (DPI) at very high performance levels, eliminating the network bottleneck that other products introduce, and enabling organizations to realize increased productivity gains. The TZ Series is one of the most secure, sophisticated and widely-deployed security platform on the market today.

Additionally, the Dell SonicWALL Application Intelligence and Control feature in the TZ 215 and TZ 205 ensures that bandwidth is available for business-critical applications while throttling or blocking unproductive applications. The TZ 215 and the TZ 205 also offers advanced application traffic analytics and reporting for deep insight into bandwidth utilization and security threats.

The TZ Series includes additional advanced networking features such as IPSec and SSL VPN, multiple ISP failover, load balancing, optional integrated 802.11n wireless and network segmentation, and also enables PCI compliance. Unlike other UTM firewalls, the TZ Series provides a native VPN remote access client for Apple® iOS, Google® Android™, Windows, Mac OS and Linux. This unique client also supports Clean VPN™, which decontaminates threats from VPN traffic. The new TZ Series is an elegant and simple integration of multiple point products, combined into a single solution providing greater value and less complexity.

Dell SonicWALL TZ 215

The Dell SonicWALL TZ 215 is the most secure, highest performance Unified Threat Management (UTM) firewall available for small businesses and branch offices. Designed for small businesses, distributed enterprises, branch offices and retail deployments, the TZ 215 integrates anti-malware, intrusion prevention, application control and URL filtering, driving down cost and complexity. It provides a dual-core architecture delivering full deep packet inspection (DPI) without diminishing network performance, thus eliminating bottlenecks that other products introduce, enabling businesses to realize increased productivity gains. The TZ 215 also provides application control to ensure bandwidth for critical applications, while throttling nonproductive ones. Advanced networking features include multiple ISP failover and load balancing, optional dual-band secure wireless, IPSec VPN support, network segmentation and PCI compliance capabilities.

Dell SonicWALL TZ 205

Small businesses, retail deployments, government organizations, remote sites and branch offices can benefit from the powerful security and business-class performance of the Dell SonicWALL TZ 205. Unlike consumer grade products, this powerful Unified Threat Management (UTM) firewall combines the most effective intrusion prevention, anti-malware and content/URL filtering with the broadest, most secure mobile platform support for laptops, smartphones and tablets. By providing full deep packet inspection (DPI) at very high performance levels, it eliminates the tradeoff between comprehensive security and performance.

DELL SonicWALL

Dell SonicWALL TZ 105 Series

The Dell SonicWALL TZ 105 is the one of the most secure Unified Threat Management (UTM) firewall available for small offices, home offices and small retail deployments. Unlike consumer-grade products, the TZ 105 delivers the proven, most effective intrusion prevention, anti-malware and content/URL filtering, along with the broad mobile platform support for laptops, smartphones and tablets. It provides full deep packet inspection (DPI) at very high performance levels, eliminating the network bottleneck that other products introduce, and enabling organizations to realize increased productivity gains without the increased cost.

Feature	TZ 105 Series	TZ 205 Series	TZ 215 Series
Nodes	Unrestricted	Unrestricted	Unrestricted
Network interfaces	(5) 10/100 Fast Ethernet, 1 USB, 1 Console	(5) 10/100/1000 Copper Gigabit, 1 USB, 1 Console	(7) 10/100/1000 Copper Gigabit, 2 USB, 1 Console
Stateful packet inspection throughput[1]	200 Mbps	500 Mbps	500 Mbps
UTM throughput[3]	25 Mbps	40 Mbps	60 Mbps
3DES/AES throughput[2]	75 Mbps	100 Mbps	130 Mbps
Maximum connections	8,000	12,000	48,000
Maximum UTM connections	8,000	12,000	32,000
Site-to-site VPN tunnels	5	10	20
Remote access IPSec VPN tunnels (max)	5	10	25
Remote access IPSec VPN tunnels (bundled)	Optional Upgrade	2	2
Remote access SSL VPN tunnels (max)	5	10	10
Remote access SSL VPN tunnels (bundled)	1	1	2
Secure Virtual Assist technicians (max)	N/A	1	2
Secure Virtual Assist technicians (bundled)	N/A	0	30-day trial
VLAN interfaces	5 , PortShield	10 , PortShield	20, PortShield
Zone security	Yes	Yes	Yes
Object-based management	Yes	Yes	Yes
Policy-based NAT	Yes	Yes	Yes
Multiple ISP failover	Yes	Yes	Yes
ISP failover	Yes	Yes	Yes
Hardware failover	No	Active/Passive	Active/Passive
WAN load balancing	Yes	Yes	Yes
Layer 2 wireless bridging	Yes	Yes	Yes
Wireless switch and controller	Yes	Yes	Yes
Virtual Access Points (VAPs)	Yes[4]	Yes[4]	Yes[4]
Integrated access point	Optional 802.11n	Optional 802.11n	Optional 802.11n
Comprehensive Anti-Spam Service	Optional	Optional	Optional
Dual band wireless-N	Yes	Yes (2x2)	Yes (3x3)
Voice over IP (VoIP)	Yes	Yes	Yes
PortShield security	Yes	Yes	Yes
Route-based VPN	Yes	Yes	Yes
3G wireless failover	Yes	Yes	Yes
Bandwidth management	No	Yes	Yes
Application intelligence and control	No	Yes	Yes
Application visualization	No	Yes	Yes
NetFlow/IPFIX	No	Yes[5]	Yes

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.
[3] 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.
[4] Virtual Access Points (VAPs) are supported on the integrated wireless radio only.
[5] Please consult latest release notes for availability.

Dell SonicWALL Clean Wireless solution: SonicPoints at-a-glance

Dell SonicWALL makes wireless networking secure, simple and affordable with the innovative Dell SonicWALL Clean Wireless Solution—the first total security solution that integrates 802.11n and 802.11a/b/g wireless management with best-in-class Next-Generation Firewall security and application intelligence, control and visualization to provide application based policy control. Dell SonicWALL SonicPoint-N Series wireless access point devices and Dell SonicWALL Power over Ethernet (PoE) Injectors complement our award-winning line of firewall appliances to flexibly extend comprehensive security across wireless networks. The Dell 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-Ni and SonicPoint-Ne Dual-Band and the SonicPoint-N Dual-Radio are access points that are utilized to provide seamless, secure wireless LAN (WLAN) connectivity as well as advanced features and services. Dell SonicWALL lowers TCO by enabling administrators avoid implementing and separately managing an expensive wireless-specific solution that runs in parallel to their existing wired network.

Dell SonicWALL-N Dual-Radio

Dell SonicWALL SonicPoint-N Dual-Radio provides secure 802.11a/g/b/n wireless networking across the 2.4 GHz and 5 GHz bands through its two discrete radios. Dell SonicWALL's Clean Wireless™ technology with SonicPoints provides integrated access point management with the security provided by the patented Dell SonicWALL RFDPI* technology on the firewall to remove threats from wireless traffic. SonicPoint-N Dual-Radio delivers a combined throughput of up to 600 Mbps, for greater security and productivity.

SonicPoint-Ne Dual-Band

Dell SonicWALL SonicPoint-Ne Dual-Band access points integrate 802.11a/b/g/n management and enforcement features with the patented Dell SonicWALL RFDPI* technology, for flexible deployment into Dell SonicWALL Clean Wireless networks. Flexible deployment options include both 802.3af Power over Ethernet (PoE), where an electrical outlet is not readily available, and direct power through an AC adapter. Ideal for hospitals or clinics, professional offices and other deployment scenarios that require discreet wireless deployment with light and logo covers, silent operation and controllable LED (except power).

SonicPoint-Ni Dual-Band

Dell SonicWALL SonicPoint-Ni Dual-Band access points integrate 802.11a/b/g/n management and enforcement features with the patented Dell SonicWALL RFDPI* technology, to secure highly discreet Dell SonicWALL Clean Wireless network environments. Ideal for hospitals or clinics, professional offices and other deployment scenarios that require discreet wireless deployment with internal antennas, light and logo covers silent operation and controllable LED (except power).

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

PoE Injector

The Dell SonicWALL PoE Injector is an IEEE 802.3af or IEEE 802.3at (SonicPoint-N Dual Radio) compliant power injector featuring an advanced auto-sensing algorithm that automatically detects the presence of PoE-compatible devices and "injects" the appropriate power into the data cable. A plug-and-play device, the PoE Injector fits easily into wireless Ethernet infrastructures and requires no configuration or management.

Advanced security services for network security solutions

Dell SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control Service

Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control 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. Dell 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. Dell SonicWALL Application Intelligence and Control Service provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity.

Dell SonicWALL Content Filtering Service

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, Dell 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.

Dell SonicWALL Enforced Client Anti-Virus and Anti-Spyware

Enforced Client Anti-Virus and Anti-Spyware, working in conjunction with Dell SonicWALL firewalls provides comprehensive enforced virus and spyware protection for desktops and laptops from the gateway. Dell SonicWALL firewalls confirm that all computers have the latest version of anti-virus and anti-spyware software installed and active before authorizing their access to the network. Automated updates of virus and spyware signatures eliminate the need for time-consuming machine-by-machine anti-virus deployments. Dell SonicWALL Enforced Client Anti-Virus and Anti-Spyware software is available for purchase with the McAfee® anti-virus engine.

Dell SonicWALL Comprehensive Anti-Spam Service

Comprehensive Anti-Spam Service (CASS) offers small- to medium-sized businesses comprehensive protection from spam and viruses, instantly deployed over existing Dell SonicWALL network security appliances. CASS speeds deployment, eases administration and reduces overhead by consolidating solutions, providing one-click anti-spam services, with advanced configuration in just ten minutes.

Dell SonicWALL DPI-SSL

Deep Packet Inspection of SSL-encrypted traffic (DPI-SSL) transparently decrypts and scans both inbound and outbound HTTPS traffic using Dell SonicWALL RFDPI. The traffic is then re-encrypted and sent to its original destination if no threats or vulnerabilities are discovered.

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Dell SonicWALL Secure Virtual Assist

Secure 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. Dell SonicWALL Virtual Assist allows tight integration by leveraging existing network and authentication infrastructures.

Software for network security appliance

Dell SonicWALL VPN Clients

For remote client-to-host secure access, Dell SonicWALL offers both SSL VPN and IPSec VPN connectivity options. For SSL VPN, Dell 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, Dell SonicWALL Global VPN Client enables the client system to download the VPN client for a more traditional client-based VPN experience.

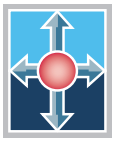
SonicWALL Mobile Connect™

Mobile Connect, a single unified client app for Apple iOS and Google Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections. When deployed on a Dell SonicWALL Next-Generation Firewall, it creates a Clean VPN to remove malware from communications relayed through mobile devices.

Dell SonicWALL Analyzer Reporting Software

Analyzer is an easy-to-use web-based application traffic analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the network. Analyzer supports Dell SonicWALL firewalls, backup/recovery appliances, and secure remote access devices while leveraging application traffic analytics for security event reports.

Firmware for network security solutions



SonicOS Enhanced Firmware

SonicOS Enhanced is the powerful next-generation operating system, integrating a host of advanced features to meet the business continuity, configuration flexibility and management requirements of complex networks today and into the future.

Dell SonicWALL WAN acceleration solutions: WXA Series at-a-glance

The Dell SonicWALL WAN Acceleration Appliance (WXA) Series reduces application latency and conserves bandwidth, significantly enhancing WAN application performance and user experience for small- to medium-sized organizations with remote and branch offices. After initial data transfer, the WXA Series dramatically reduces all subsequent traffic by transmitting only new or changed data across the network. The WXA de-duplicates data traversing the WAN, remembers previously transferred data, and replaces repeated byte sequences with an identifier, thus reducing application latency and conserving bandwidth. Other acceleration features include data caching, file de-duplication, metadata caching and data-in-flight compression.

The WXA Series is comprised of the WXA 500 Live CD, WXA 2000 and WXA 4000 hardware appliances, and WXA 5000 Virtual Appliance. Unlike standalone WAN acceleration products, WXA solutions are integrated add-ons to Dell SonicWALL E-Class NSA, NSA and TZ Series appliances that are deployed as Next-Generation Firewalls. This integrated solution streamlines the placement, deployment, configuration, routing, management and integration of the WXA with other components, such as VPNs. When deployed in conjunction with Dell SonicWALL Application Intelligence and Control Service, the WXA offers the unique combined benefit of both prioritizing application traffic and minimizing traffic between sites, resulting in optimal network performance.

Dell SonicWALL WXA 500 Live CD
The WXA 500 Live CD supports flexible deployment via a bootable Live CD.

Dell SonicWALL WXA 2000
The WXA 2000 accelerates network performance for up to 120 users and 600 WAN optimization flows.

Dell SonicWALL WXA 4000
The WXA 4000 accelerates network performance for up to 240 users and 1,200 WAN optimization flows.

Dell SonicWALL WXA 5000 Virtual Appliance
The WXA 5000 supports flexible virtual machine deployments in VMWare® environments.

Features	WXA 500 Live CD	WXA 2000	WXA 4000	WXA 5000 Virtual Appliance
Platform	Software/CD	Hardware Appliance	Hardware Appliance	Virtual Appliance (VMWare)
Maximum users[1]	20	120	240	360
Maximum connections	100	600	1,200	1,800[3]
Byte caching		Yes		
Compression		Yes		
Management		Requires SonicOS 5.8.1 or later		
WFS acceleration	Yes[2]	Yes		
TCP/WFS visualization		Yes		
SNMP		Yes		
Syslog		Yes		
Operating system		Hardened Dell SonicWALL Linux OS		
Rack-mount chassis	—	1 RU		—
CPU	—	Intel 2.0GHz	Intel Dual Core 2.0GHz	—
RAM	—	2 GB	4 GB	—
Hard drive	—	250 GB	2x250 GB	—
Redundant Disk Array (RAID)	—	—	RAID 1	—
Dimensions		17.0 x 16.4 x 1.7 in/43.18 x 41.59 x 4.44 cm		
Weight	—	16 lbs/7.26 kg		—
WEEE weight	—	16 lbs/7.37 kg		—
Power consumption (Watts)	—	86	101	—
BTUs	—	293	344	—
MTBF (Years)		14.27		

	WXA 500 Live CD Only
Minimum CPU	Pentium 4 or higher
External storage	CD/DVD ROM Bay
Allocated memory	Minimum of 2 GB RAM
Allocated storage	Minimum of 80 GB Hard Disk
Storage controller	SATA Controller with Support for IDE Emulation
Additional requirements	Monitor/Keyboard

	WXA 5000 Virtual Appliance Only
Hypervisor	ESX and ESXi (version 4.0 and newer)
Operating system installed	Hardened SonicLinux
Minimum CPU	2 x 1.6 GHz
Allocated memory	4 GB
Applied disk size	250 GB
VMware Hardware Compatibility Guide	http://vmware.com/resources/compatibility/search.php

[1] Maximum users may vary depending on the number of flows being generated per user.
[2] WFS Acceleration is available only when the Live CD image is installed on the provided hardware.
[3] The max number of flows is dependent on the hardware specifications and may vary depending on the hardware configuration. The specifications provided are the minimum requirements to run the WXA Virtual Appliance.

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

Dell SonicWALL Secure Remote Access solutions

The traditional corporate LAN boundary is evolving into a distributed global network that connects employees, partners and customers over the Internet, intranets and extranet networks. The modern mobile workforce demands anytime access to resources from more devices including smartphones and tablets than ever before. Dell SonicWALL provides scalable Secure Remote Access (SRA) solutions to fit organizations of all sizes—from small-to medium sized businesses to large global enterprises. Dell SonicWALL Aventail™ E-Class SRA Series and Dell SonicWALL SRA Series for the SMB deliver flexible SSL VPN solutions for secure remote access, disaster recovery, secure wireless networking and secure extranets, and can be deployed as hardware or virtual appliances.

Dell SonicWALL Aventail E-Class SRA Series at-a-glance

Dell SonicWALL Aventail E-Class Secure Remote Access (SRA) Series increases 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, Dell 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 or a virtual appliance in a VMWare environment to control access to network resources, Dell 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 Windows, Windows Mobile, Apple Mac OS, iOS, Linux®, and Google Android
- 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 Dell 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 End Point Control 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 — Dell SonicWALL Aventail E-Class SRA Series
Dell SonicWALL Aventail E-Class SRA EX9000
Dell SonicWALL Aventail E-Class Secure Remote Access (SRA) Series delivers full-featured, easy-to-manage, clientless or thin-client "in-office" connectivity for up to 20,000 concurrent mobile-enterprise users from a single appliance. E-Class SRA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android devices.

Secure Remote Access Solutions — Dell SonicWALL Aventail E-Class SRA Series
Dell SonicWALL Aventail E-Class SRA EX7000
The Dell SonicWALL Aventail SRA EX7000 delivers full-featured, easy-to-manage, clientless or thin-client "in-office" connectivity for up to 5,000 concurrent mobile-enterprise users from a single appliance. E-Class SRA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android devices.

Dell SonicWALL Aventail E-Class SRA EX6000
The Dell SonicWALL Aventail E-Class SRA EX6000 delivers full-featured, easy-to-manage, clientless or thin-client "in-office" connectivity for up to 250 concurrent mobile-enterprise users from a single appliance. E-Class SRA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android devices.

Dell SonicWALL Aventail E-Class SRA Virtual Appliance
The Dell SonicWALL Aventail E-Class SRA Virtual Appliance is a hardened, performance-optimized virtual server for full-featured and easy-to-manage clientless secure remote access for mobile enterprise organizations, supporting up to 250 concurrent users from a single virtual appliance. E-Class SRA Virtual Appliance enhances productivity and business continuity with policy-enforced remote access to network resources from Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android devices.

Optional Dell SonicWALL Aventail E-Class add-on features

Dell SonicWALL Aventail Advanced End Point Control (EPC)™
Advanced EPC combines the most advanced end point detection with the most advanced data protection.

Dell SonicWALL Aventail Advanced Reporting™
Advanced Reporting delivers powerful analysis of remote access to your resources.

SonicWALL Mobile Connect
Mobile Connect, a single unified client app for Apple iOS and Google Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.

Dell SonicWALL Aventail Connect Mobile™
Connect Mobile offers true "in-office" experience for smartphone devices.

Dell SonicWALL Aventail Native Access Modules™
Native Access Modules allow native protocol access to server-based applications.

Dell SonicWALL Aventail Spike License™
Spike License is a disaster recovery "insurance policy" for future increases in remote users.

Dell SonicWALL Secure Virtual Assist
A remote support tool enabling remote technical assistance.

Dell SonicWALL Analyzer
An easy-to-use application traffic analytics and reporting tool that provides real-time and historical insight into the performance and security of the network. For Dell SonicWALL Aventail E-Class SRA appliances, Analyzer delivers reporting on remote user connections. Analyzer also provides reporting for Dell SonicWALL firewalls and CDP appliances.

Feature	Virtual Appliance	EX6000	EX7000	EX9000
Concurrent user license	5 to 250	25 to 250	50 to 5,000	100 to 20,000
Basic End Point Control (EPC) interrogation	Included	Included	Included	Included
Advanced EPC (anti-virus, personal firewall, anti-spyware)	Add-on	Add-on	Included	Included
Aventail Secure Desktop/ cache cleaner	Add-on	Add-on	Included	Included
Allow, deny and quarantine zones based on EPC interrogation	Included	Included	Included	Included
Granular access control (user and group, source IP, service/port, destination URL, host name/ip address, IP range, subnet, domain)	Included	Included	Included	Included
Advanced reporting	Add-on	Add-on	Add-on	Add-on
Analyzer	Add-on	Add-on	Add-on	Add-on
WorkPlace portal	Included	Included	Included	Included
WorkPlace Mobile (optimized portal for mobile phone browsers)	Included	Included	Included	Included
Native Access Modules (Citrix, Windows Terminal Services and VMWare View)	Add-on	Add-on	Included	Included
Connect Tunnel (Windows, Mac and Linux access to TCP or UDP based applications)	Included	Included	Included	Included
Connect Mobile (Windows Mobile, Google Android)	Included	Included	Included	Included
Mobile Connect (iOS)	Included	Included	Included	Included
Mobile Connect (Android)	Included	Included	Included	Included

Dell SonicWALL SSL VPN offers affordable, easy-to-use and manage secure remote access.

Dell SonicWALL Secure Remote Access Series for the SMB at-a-glance

Dell SonicWALL's SRA Series 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. Dell 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. Dell SonicWALL Secure Remote Access Series is available as an appliance or as a virtual appliance in a VMWare environment.

- Seamless integration behind virtually any firewall enables organizations to leverage the existing network infrastructure
- 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 for iOS and Google Android to access an entire intranet as well as web-based applications provides greater flexibility for a remote workforce.
- 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
- Application offloading allows users to securely access web applications while leveraging strong authentication and granular access policy features
- Dell SonicWALL's Web Application Firewall Service detects and protects web applications (including the SSL VPN appliance itself) from web-based attacks, reducing potential losses and adhering to data protection compliance mandates such as PCI-DSS
- End Point Control (EPC) for SRA Series allows for the unique identification of Windows-based endpoints to tie them to the authorized user as well as the ability to assess the security posture of the device by looking for security components such as anti-virus and anti-spyware software
- Remote support using Dell SonicWALL Secure Virtual Assist enables technicians to provide secure on-demand assistance to customers while leveraging the existing infrastructure
- Secure Virtual Access enables authorized end users in distributed enterprises and service provider organizations to gain secure remote access to their unattended Windows-based computers from anywhere
- Secure Virtual Meeting incorporates all of the security of the SRA for SMB Series to comprehensively protect sensitive and proprietary communications, while enabling cost-effective collaboration
- Spike licensing allows for the administrator to prepare a disaster recovery plan to support a spike in the number of licensed users
- Clean VPN is enabled when deployed alongside a Dell SonicWALL network security appliance which utilizes powerful deep packet inspection technology to scan traffic for malicious threats such as viruses, worms, Trojans and spyware

Dell SonicWALL Secure Remote Access 4200

The Dell SonicWALL SRA 4200 provides medium-sized organizations with a powerful, easy-to-use and cost-effective secure remote access solution that requires no pre-installed client software for Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android, plus optional Web Application Firewall and multi-platform remote support. 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. The SRA 4200 with its hardware assisted SSL offload functionality can support a large number of remote access users, as well as supporting value-added services for allowing remote PC support, remote PC access and Web Application Firewall. High Availability (HA) on the SRA 4200 allows for an Active/Passive configuration to enable businesses to have reliable and secure remote access even in the event of the failure of one of the two units.

Dell SonicWALL Secure Remote Access 1200

The Dell SonicWALL SRA 1200 provides small- to medium-sized businesses easy-to-use secure remote access to corporate email, files and web-based applications without pre-installed clients for Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android, plus optional Web Application Firewall and multi-platform remote support. Integrating seamlessly into virtually any network topology, the SRA 1200 delivers affordable yet powerful remote access, remote support, remote PC control and Web Application Firewall.

Secure Remote Access Virtual Appliance

The Dell SonicWALL SRA Virtual Appliance provides small- to medium-sized businesses with a |hardened, performance-optimized virtual server for clientless remote access to business applications and resources, including email, files, intranets, web-based and legacy applications, desktops and servers from more OS platforms, including Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android. The SRA Virtual Appliance can be rapidly deployed in a virtualized environment as a cost effective solution to help lower the Total Cost of Ownership (TCO) objectives of small-to-medium organizations.

Optional Dell SonicWALL SSL VPN add-on features

Dell SonicWALL Web Application Firewall Service

Dell SonicWALL's award winning Web Application Firewall Service (WAF), a complete, affordable, out-of-box compliance solution, leverages your existing infrastructure as a licensable add-on module to the Dell SonicWALL Secure Remote Access platform. Utilizing a dynamically updated signature database to detect sophisticated web-based attacks and protect web applications including SSL VPN portals, Dell SonicWALL WAF Service applies reverse proxy analysis of Layer 7 traffic against known signatures, denies access upon detecting web application malware, and redirects users to an explanatory error page. Dell SonicWALL's WAF also provides the ability to plug in custom rule chains and use automatic Application Profiling to do "virtual patching" so as to protect against zero day web application threats. Dell SonicWALL WAF is a critical component towards achieving PCI compliance as well as providing web-based DLP (Data Leakage Protection) capabilities to block or mask sensitive information such as Credit Cards and SSN's from falling into the wrong hands.

Optional Dell SonicWALL SRA for SMB add-on features

SonicWALL Mobile Connect

Mobile Connect, a single unified client app for Apple iOS and Google Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections. When deployed with a Dell SonicWALL Next-Generation Firewall, it creates a Clean VPN to remove malware from communications relayed through mobile devices.

Dell SonicWALL Secure Virtual Assist

Secure Virtual Assist is a remote support tool that enables a technician to assume control of an end customer's PC or laptop running Windows, Mac or Linux, for the purpose of providing remote technical assistance. With the customer's permission, the technician can gain instant access to a computer using a web browser, making it easy to diagnose and fix a problem remotely without the need for a pre-installed "fat" client.

Dell SonicWALL Secure Virtual Access

Secure Virtual Access is a remote PC control tool that enables authorized end users to gain secure remote access to their unattended Windows-based computers from anywhere. Users simply need to install the Virtual Access agent onto a Windows PC with Internet access and, as long as that PC has a connection to the Dell SonicWALL SSL VPN, the user can connect to that PC from anywhere they have an Internet connection. This is especially useful for remote employees who have the need to connect back to a home office computer or small branch office PC that is not normally connected to the LAN.

Dell SonicWALL Secure Virtual Meeting

Secure Virtual Meeting allows for secure and cost-effective collaboration, eliminating the need for unnecessary travel expenses. Unlike other virtual meeting solutions, Dell SonicWALL Secure Virtual Meeting incorporates all of the security of the SRA for SMB Series to comprehensively protect sensitive and proprietary communications. Secure Virtual Meeting integrates with existing authentication infrastructure as well as with calendar scheduling systems such as Microsoft Outlook™.

Dell SonicWALL End Point Control for SRA Series

End Point Control (EPC) for the Secure Remote Access (SRA) Series delivers enterprise-class device identification and interrogation features to small and medium-sized businesses. EPC for the SRA Series uniquely identifies Windows-based endpoints to tie them to authorized users. It also enforces granular security posture by checking for essential components such as anti-virus and anti-spyware software to ensure device integrity before admitting users of Windows-based devices via the Dell SonicWALL NetExtender client. The device interrogation list includes supported anti-virus, anti-spyware and personal firewall solutions from leading vendors such as McAfee, Kaspersky Lab, Symantec®, Computer Associates®, Sophos® and many others. This greatly reduces the chance of malware entering the network from non-IT-managed devices.

Optional Dell SonicWALL SRA for SMB add-on features

Dell SonicWALL Spike License

Spike License offers customers the ability to immediately increase the remote user count in preparation for business disruptions because of emergencies such as riots, earthquakes and snowstorms.

Dell SonicWALL Analyzer

Analyzer is an easy-to-use application traffic analytics and reporting tool that provides real-time and historical insight into the performance and security of the network. For SRA devices Analyzer delivers reporting on remote user connections and web application firewall activity. Analyzer also provides reporting for Dell SonicWALL firewalls and CDP appliances.

Deployment	SRA 1200	SRA 4200	SRA Virtual Appliance
Type and size of deployment environment	Small organizations up to 50 employees	Mid-size organizations up to 500 employees	Organizations of any size
Included/maximum number of concurrent users	5/50	25/500	5/50
Virtual Access/Virtual Assist maximum number of concurrent users	10	25	25

Features	SRA 1200	SRA 4200	SRA Virtual Appliance
Secure Virtual Access	Add-on	Add-on	Add-on
Secure Virtual Assist	Add-on	Add-on	Add-on
Secure Virtual Meeting	Add-on	Add-on	Add-on
End Point Control for SRA Series	Add-on	Add-on	Add-on
Analyzer	Add-on	Add-on	Add-on
Web Application Firewall	Add-on	Add-on	Add-on
Spike Licensing	Add-on	Add-on	Add-on
One time password (OTP) authentication	Included	Included	Included
Vasco support	Included	Included	Included
RSA support	Included	Included	Included
Citrix (ICA) support	Included	Included	Included
NetExtender: Support for multiple IP ranges and routes	Included	Included	Included
Optional client certificate support	Included	Included	Included
Graphical usage monitoring	Included	Included	Included
Option to Create System backup	Included	Included	Included
Reverse proxy: OWA premium version and Lotus Domino Access	Included	Included	Included
RADIUS test function	Included	Included	Included
Active directory groups support	Included	Included	Included
Virtual host/domain name support	Included	Included	Included
FileShares Java applet	Included	Included	Included
Diagnostics: DNS lookup and traceroute	Included	Included	Included
SNMPv2	Included	Included	Included
Layer-7 load balancing	Included	Included	Included
High Availability (HA)	–	Included	–
SSL hardware-assisted offload	–	Included	Depends on underlying hardware
Mobile Connect (iOS)	Included	Included	Included
Mobile Connect (Android)	Included	Included	Included

Powerful and easy-to-use email threat protection

Dell SonicWALL Email Security

Protect your business from inbound and outbound email threats and compliance violations with Dell SonicWALL Email Security. Achieve superior, real-time protection from spam, phishing, viruses, zombies, directory harvest (DHA), Denial of Service (DoS) and other attacks by leveraging multiple proven and patented[1] Dell SonicWALL threat detection techniques and unique worldwide attack identification and monitoring network. In addition, Email Security prevents confidential data leaks and regulatory violations with advanced compliance scanning and management.

You can easily and cost-effectively scale your email security deployment from 10 to 100,000 mailboxes. Flexibly deploy Dell SonicWALL Email Security as a scalable hardware appliance, virtual appliance, or software including software optimized for Microsoft Windows® Server or Small Business Server (SBS), to best meet to your budget and infrastructure requirements and receive greatest return on your long-term investment. Configure for high availability and scalable split mode and centrally and reliably manage enterprise-class deployments. Administration is intuitive, quick and simple. Safely delegate spam management to end users while still retaining ultimate control over security enforcement. Easily manage user and group accounts with seamless multi-LDAP synchronization. In large distributed environments, new multi-tenancy support lets you delegate sub-administrators to manage settings at multiple organizational units (such as enterprise divisions or MSP customers) within a single email security deployment.

Dell SonicWALL E-Class Email Security Series

Dell SonicWALL E-Class Email Security Appliance Series

Dell 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 MTA offers breakthrough message analysis and industry-leading message delivery rates, providing high-performance and enterprise-wide scalability.

Dell SonicWALL E-Class Email Security Software

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

Dell SonicWALL E-Class Email Security Virtual Appliance

The Dell SonicWALL Email Security Virtual Appliance provides a hardened, performance-optimized virtual server for Dell SonicWALL Email Security. In the past, under the "one server, one application" model, administrators often underutilized hardware resources and spent considerable time on server management. Dell SonicWALL Virtual Appliances significantly improve the efficiency and availability of resources and applications. To support larger deployments and scalability, administrators can use Split-Config Mode to deploy multiple virtual appliances within a single physical server or across multiple physical servers.

[1] U.S. Patents 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348

Dell SonicWALL Email Security Series for the SMB

Dell SonicWALL Email Security Appliance Series

Ideal for small- to medium-sized organizations, Dell 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 Dell SonicWALL OS, these plug-and-play appliances install in less than an hour to securely protect your email..

Dell SonicWALL Email Security Software

Dell 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, Dell SonicWALL Email Security Software secures organizations from all inbound and outbound email threats through an easy-to-use, web-based administrative interface.

Dell 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.

Dell SonicWALL Email Security Virtual Appliance

The Dell SonicWALL Email Security Virtual Appliance provides a hardened, performance-optimized virtual server for Dell SonicWALL Email Security. In the past, under the "one server, one application" model, administrators often underutilized hardware resources and spent considerable time on server management. Dell SonicWALL Virtual Appliances significantly improve the efficiency and availability of resources and applications. To support larger deployments and scalability, administrators can use Split-Config Mode to deploy multiple virtual appliances within a single physical server or across multiple physical servers.

Dell SonicWALL Hosted Email Security

Dell SonicWALL Hosted Email Security offers small- to medium-sized businesses (SMBs) superior cloud-based protection from spam, phishing attacks and malware at an affordable, predictable and flexible monthly or annual subscription price. At the same time, it minimizes upfront deployment time and costs, as well as ongoing administration expenses. Dell SonicWALL Hosted Email Security is the only hosted solution to integrate multiple anti-virus technologies, including Dell SonicWALL GRID Anti-Virus, Time Zero Anti-Virus and Kaspersky Labs technologies, to deliver best-in-class email security.
The Dell SonicWALL GRID Network technology and Threat Research Team performs rigorous testing and evaluation of millions of emails every day, and then reapplies this constantly updated analysis to provide exceptional spam blocking results and anti-virus and anti-spyware protection. Dell SonicWALL Time Zero Virus Protection uses predictive and responsive technologies to protect organizations from virus infections before anti-virus signature updates are available. The suspect emails are identified and immediately quarantined, safeguarding the network from the time a virus outbreak occurs until the time an anti-virus signature update is available. Moreover, Kaspersky Labs technology adds an additional layer of anti-virus protection, resulting in protection superior to that provided by solutions that rely on a single anti-virus technology.

Dell SonicWALL Email Security Services

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

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

Dell SonicWALL Email Compliance Subscription
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, Dell SonicWALL can help organizations take the next step towards email compliance.

Email Security Appliances	SMB		E-Class	
Model	**3300**	**4300**	**ES6000**	**ES8300**
Rackmount chassis	1RU	1RU	1U Mini	2RU
CPU	Intel 2.0GHz	Intel Dual Core 2.0GHz	3.2 GHz	Quad Core Xeon
RAM	2 GB	4 GB	2 GB	4 GB
Hard drive	250 GB	2 x 250 GB	2x160 GB	4x750 GB
Redundant Disk Array (RAID)	No	Yes	Yes	RAID 5
Hot swappable drives	No	Yes	No	Yes
Redundant power supply	No	No	No	Yes

Email Security Software	
Software platforms	Microsoft Windows 2003 Server or Windows 2008 Server

Email Security Virtual Appliance	
Hypervisor	ESXi™ and ESX™ (version 4.0 and newer)

Dell SonicWALL backup and recovery solutions

Built from the ground up with an entirely new architecture, Dell SonicWALL Continuous Data Protection (CDP) v.6 revolutionizes the backup and recovery process. Easy to deploy, configure, manage and use with an intuitive graphical user interface, CDP transparently and automatically preserves and protects business-relevant data assets against loss from file, device, and location-based disasters. One-touch user-directed recovery cuts IT overhead while boosting user satisfaction and productivity.

CDP's unmatched flexibility offers the multiple disaster recovery options of Site-to-Site Backup, Offsite Backup, Local Archiving and Universal System Recovery. CDP can back up and recover Mac OS, Linux, or Windows platforms on local or remote laptops, desktops and servers. And CDP supports Microsoft SQL®, Exchange®, SharePoint®, Active Directory® and Small Business Server®.

With CDP's granular protection, administrators can reliably back up only business-related data. CDP also lets administrators enforce global policies and schedules, or allow users to set their own. Data de-duplication technology optimizes storage efficiency by handling more data with less disk space. Plus it optimizes bandwidth efficiency by sending less traffic over the network during backups.

Dell SonicWALL Continuous Data Protection (CDP) Series

Dell SonicWALL CDP 6080B

The Dell SonicWALL CDP 6080B offers larger organizations with multiple workstations and server applications a flexible, high capacity data backup and disaster recovery solution that automatically protects business assets from loss. Supporting Windows, Linux and Mac OS platforms through a single web GUI, it provides granular, globally enforced policy controls over the entire backup operation. Sophisticated fileset backup and agent-based de-duplication speeds backups and optimizes bandwidth, while maintaining data continuity and multiple revisions. The CDP 6080B offers powerful comprehensive protection for vigilant data backup and disaster recovery, with RAID 5 and a capacity of up to 20 TB (at standard 2:1 compression ratios).

Dell SonicWALL CDP 5040B

The Dell SonicWALL CDP 5040B offers small-to-medium sized organizations with multiple workstations and multiple server applications a flexible, high capacity data backup and disaster recovery solution that automatically protects business assets from loss. Supporting Windows, Linux and Mac OS platforms through a single web GUI, it provides granular, globally enforced policy controls over the entire backup operation. Sophisticated fileset backup and agent-based de-duplication speeds backups and optimizes bandwidth, while maintaining data continuity and multiple revisions. The CDP 5040B offers powerful comprehensive protection for vigilant data backup and disaster recovery, with RAID 5 and a capacity of up to 10 TB (at standard 2:1 compression ratios).

Dell SonicWALL CDP 220

The Dell SonicWALL CDP 220 offers small, remote or branch offices and distributed environments with multiple workstations and servers a flexible data backup and disaster recovery solution that automatically protects business assets from loss. Supporting Windows, Linux and Mac OS platforms through a single web GUI, it provides granular, globally enforced policy controls over the entire backup operation. Sophisticated fileset backup and agent-based de-duplication speeds backups and optimizes bandwidth, while maintaining data continuity and multiple revisions. The CDP 220 offers powerful, comprehensive protection for vigilant data backup and disaster recovery, with a capacity of up to 3.4 TB (at standard 2:1 compression ratios).

Dell SonicWALL CDP 210

The Dell SonicWALL CDP 210 offers small, remote or branch offices with workstations a flexible data backup and disaster recovery solution that automatically protects business assets from loss. Supporting Windows, Linux and Mac OS platforms through a single web GUI, it provides granular, globally enforced policy controls over the entire backup operation. Sophisticated fileset backup and agent-based de-duplication speeds backups and optimizes bandwidth, while maintaining data continuity and multiple revisions. The CDP 210 offers powerful comprehensive protection for vigilant data backup and disaster recovery, with a capacity of up to 1.7 TB (at standard 2:1 compression ratios).

Dell SonicWALL backup and disaster recovery licenses and services

Dell SonicWALL CDP Offsite Data Backup Service
CDP Offsite Data Backup Service provides a fully managed offsite data solution for hassle-free disaster protection. In the event the local CDP appliance is no longer viable, IT administrators can easily recover any stored revision of data through the replacement CDP appliance using an easy-to-use user interface. The datacenters feature uninterruptible power supply systems (UPS), emergency diesel generators, earthquake protection, redundant fire prevention, flood control, HVAC and 24-hour onsite security.

Dell SonicWALL CDP Site-to-Site Backup
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, IT administrators can easily recover any stored revision of data through an easy-to-use user interface.

Dell SonicWALL CDP Universal System Recovery
Universal System Recovery 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, it 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.

Dell SonicWALL CDP Local Archiving
CDP Local Archiving capability allows IT to store the latest version of business-critical data to a USB drive. Designed to help organizations meet regulatory compliance, Local Archiving enables administrators to browse archives and restore individual files. Local archiving is available on both upstream and downstream CDP appliances.

Dell SonicWALL CDP Recovery Manager for Microsoft Exchange
CDP Recovery Manager for Microsoft Exchange lets administrators search, compare and restore individual, criteria-specific items—including single messages, multiple mailboxes and public folders—from unmounted .edb files, without setting up a dedicated recovery server. Recovery Manager saves money by eliminating the need for a dedicated recovery server. It also saves time by performing fast searches based on sender, recipient, date, subject, message keyword or attachment keyword and saves critical data by granularly searching backed-up attachment content, public folders and public folder hierarchies in Exchange and Lotus® Domino.

Dell SonicWALL Analyzer
Analyzer is an easy-to-use application traffic analytics and reporting tool that provides real-time and historical insight into the performance and security of the network. For CDP devices Analyzer delivers reporting on agent backup activity and device capacity utilization and health. Analyzer also provides reporting for Dell SonicWALL firewalls and secure remote access appliances."

Feature	CDP 210	CDP 220	CDP 5040B	CDP 6080B
Appliance characteristic				
Users (recommended max)[1]	50	50	100	250
Servers (recommended max)[1]	5	5	10	15
Microsoft Application Licenses included (Additional Can be Purchased)[2]	0	1	3	3
File Server Agent License included (Windows, Apple and Linux)[3]	1	1	1	1
Workstation Agent License included (Windows and Apple)[3]	10	50	100	250
Form factor	Desktop	Desktop	1U	2U
RAID support	-	-	RAID 5	RAID 5
RAM included	512 MB	512 MB	2 GB	4 GB
Internal drives included (Number of drive bays)	1	1	4	4 (8 max)
Disk drive capacity, type	1 TB SATA	2 TB SATA	2 TB SATA	2 TB SATA
Total capacity (with Expansion Disk Pack)[4]	1 TB	2 TB	6 TB	6 TB (12 TB max)[4]
Total usable capacity (with Expansion Disk Pack)[4]	860 GB	1.7 TB	5 TB	5 TB (10 TB)[4]
Total usable capacity (Typical 2:1 compression)	1.7 TB	3.4 TB	10 TB	10 TB (20 TB)[4]
Network interface	100baseT	100baseT	1 GbE	1 GbE
Hot-swappable and redundant power protection	–	–	–	Yes
Field Replaceable hard drive	–	–	Yes	Yes
Backup and recovery				
Continuous Data Protection (CDP)	Yes	Yes	Yes	Yes
Volume shadow copy service (Snapshot)	Yes	Yes	Yes	Yes
Highly efficient fileset backup methodology	Yes	Yes	Yes	Yes
Global policy-enforced backup	Yes	Yes	Yes	Yes
Chronological data versioning	Yes	Yes	Yes	Yes
Version trimming	Yes	Yes	Yes	Yes
Agent-based data de-duplication	Yes	Yes	Yes	Yes
Granular discovery and recovery of exchange data	Yes	Yes	Yes	Yes
Flexible disaster recovery options	Yes	Yes	Yes	Yes
AES-256 bit encryption for data in-flight and at-rest	Yes	Yes	Yes	Yes
User Self-directed restore	Yes	Yes	Yes	Yes
Administration and data management (Policy and control)				
Web and agent-based management interface	Yes	Yes	Yes	Yes
Global management using Dell SonicWALL Global Management System	Yes	Yes	Yes	Yes
Object-based backup policy and control	Yes	Yes	Yes	Yes
Backup data rules	Yes	Yes	Yes	Yes
Version control	Yes	Yes	Yes	Yes
Version trimming rule	Yes	Yes	Yes	Yes
Offsite rule	Yes	Yes	Yes	Yes\
Quota provisioning	Yes	Yes	Yes	Yes
Bandwidth management	Yes	Yes	Yes	Yes
Reporting, logging and notifications	Yes	Yes	Yes	Yes
Dell SonicWALL Analyzer	Add-on	Add-on	Add-on	Add-on
Application Support				
Microsoft Exchange 2003, 2007 and 2010	Yes	Yes	Yes	Yes
Individual Mailbox Backup Support	Yes	Yes	Yes	Yes
Microsoft SQL Server 2005 and 2008	Yes	Yes	Yes	Yes
Microsoft SharePoint 2010	Yes	Yes	Yes	Yes
Active Directory	Yes	Yes	Yes	Yes
System state	Yes	Yes	Yes	Yes
Microsoft Outlook 2003, 2007 and 2010	Yes	Yes	Yes	Yes
Multi-platform system support				
Windows Server 2003 and 2008 R2 (SE and EE)	Yes	Yes	Yes	Yes
Small Business Server 2003 and 2008 R2 (Standard and Premium)	Yes	Yes	Yes	Yes
Windows XP, Vista and Win 7 (All Versions)	Yes	Yes	Yes	Yea
Apple Mac OS X – Leopard, Snow Leopard and Server	Yes	Yes	Yes	Yes
Linux (Debian, SuSE, Fedora, Red Hat and Ubuntu)	Yes	Yes	Yes	Yes

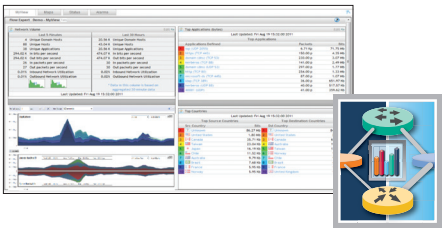
[1] These are estimated values and are subject to change without notice. The maximum supported configuration can be more or less depending on your backup and network load and offsite upload.
[2] The licenses can be applied to the following Microsoft applications: Microsoft Exchange 2003, 2007 and 2010 (includes individual mailbox support), Microsoft SQL Server 2005 and 2008, Microsoft SharePoint 2010, Microsoft Active Directory, Microsoft Small Business Server. Additional licenses may also be purchased to the maximum limits indicated above
[3] Additional licenses may also be purchased to the maximum limits indicated
[4] Requires purchase of Dell SonicWALL 4 Disk Pack Upgrade Kit (01-SSC-9301)

Dell SonicWALL policy and management solutions

Dell SonicWALL Global Management System

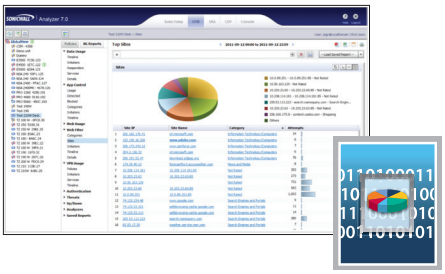
The Global Management System (GMS) provides organizations, distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy Dell SonicWALL firewall, anti-spam, backup and recovery, and secure remote access solutions. Flexible deployment options include software, hardware or as a virtual appliance; Dell SonicWALL GMS also provides centralized real-time monitoring, and comprehensive policy and compliance reporting. For enterprise customers, Dell SonicWALL GMS streamlines security policy management and appliance deployment, minimizing administration overhead. For Service Providers, Dell SonicWALL GMS simplifies the security management of multiple clients and creates additional revenue opportunities. For added redundancy and scalability, GMS system can be deployed in a cluster configuration.

- GMS Software – Dell SonicWALL GMS can be flexibly deployed as a software application on a third party Windows server, leveraging existing infrastructure.
- Universal Management Appliance EM5000 – The award-winning 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 Dell SonicWALL security appliances.
- GMS Virtual Appliance – The Dell SonicWALL GMS Virtual Appliance provides a hardened, performance-optimized virtual appliance agent for the Dell 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. Dell SonicWALL Virtual Appliances significantly improve the efficiency and availability of resources and applications.



Dell SonicWALL Scrutinizer

Scrutinizer is a multi-vendor, flow-based application traffic flow analytics visualization and reporting tool to measure and troubleshoot network performance and utilization while increasing productivity for enterprises and service providers. Scrutinizer supports a wide range of routers, switches, firewalls, and data-flow reporting protocols, providing unparalleled insight into application traffic analysis from IPFIX/NetFlow data exported by Dell SonicWALL firewalls. Scrutinizer easily identifies top applications, conversations, flows, protocols, domains, countries, and subnets, and alerts on suspicious behavior. Scrutinizer features deep packet application traffic analysis, proactive jitter/latency monitoring, automated reporting and customizable dashboards. Scrutinizer also provides historical and advanced reporting, role-based administration, advanced analysis, and threshold-based alerts, in addition to numerous special features for MSPs and ISPs. Dell SonicWALL Scrutinizer is available as a Windows application.



Dell SonicWALL Analyzer

Analyzer is an easy to use web-based traffic analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the network. Analyzer supports Dell SonicWALL firewalls, backup/recovery appliances, and secure remote access devices while leveraging application traffic analytics for security event reports. Organizations of all sizes benefit from enhanced employee productivity, optimized network bandwidth utilization increased security awareness. Dell SonicWALL is the only firewall vendor that provides a complete solution combining off-box application traffic analytics combined with granular statistical data generated by Dell SonicWALL firewalls. Dell SonicWALL Analyzer is available as a Windows application and as a virtual appliance.

Dell SonicWALL global support services

Dell 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, Dell 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.

Dell SonicWALL Platinum Support for the SuperMassive E10000 Series

Platinum Support and Professional Services combine the technical support and custom services IT needs to attain the greatest return on its Dell SonicWALL investment. Dell SonicWALL Platinum Support is a custom support offering that includes a comprehensive suite of services to ensure operational effectiveness and efficiency, all of which are managed and delivered by a team of senior support engineers who understand an enterprise's business and technical requirements. Built upon a proactive service and support lifecycle, Dell SonicWALL Platinum Support establishes a solid operational foundation, anticipates emerging security demands, and dynamically adapts and evolves to support an enterprise's business goals. In addition, Platinum Professional Services offer onsite installation and configuration services, training and education services and system migration from either an existing Dell SonicWALL solution or a product from another vendor.

- 24x7 support provided by a team of senior support engineers
- Software and firmware updates and upgrades
- Advance Exchange hardware replacement (RMA)

E-Class Support 24x7

Designed for customers with Dell SonicWALL E-Class solutions, Dell 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 Next Business Day 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, Dell 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 chat, email, web and telephone technical support
- Advance Exchange Next Business Day hardware replacement in the event of failure

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

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

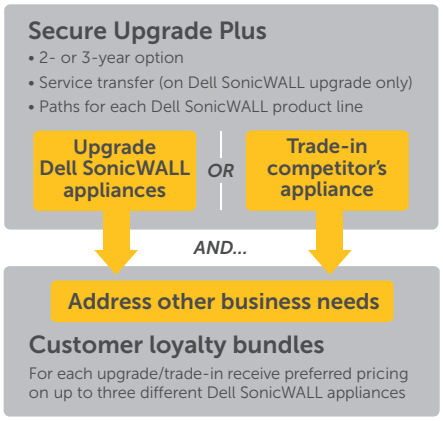
Focused Technical Support
Mission critical customers need mission critical support. Dell SonicWALL Focused Technical Support (FTS) is designed to provide our most important customers the highest-quality, most responsive support services available in the industry. This premium support offering includes a comprehensive suite of proactive services, all of which are managed by a designated Dell 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 Dell SonicWALL for enhanced escalation and new feature processing

Dell SonicWALL Remote Start-up and Configuration Service
Remote Start-up and Configuration Service provides businesses of all sizes with rapid, secure configuration and deployment of their Dell SonicWALL appliance into a new or existing network. The remote configuration is performed by CSSA-certified technicians using Dell 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 Dell SonicWALL appliance will be up and running in a matter of hours, allowing you to realize a faster return on your Dell 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 Dell 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).

Secure Upgrade Plus now features more Dell SonicWALL firewall products, including the new Network Security Appliance (NSA) 220 and NSA 250M Series, as well as other specified Dell SonicWALL product lines, including Secure Remote Access (SSL VPN) and Email Security (ES). For the complete listing of eligible Dell 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 Dell SonicWALL Customer Loyalty Bundle acknowledges our customers' trust and reflects our commitment to them by rewarding customers who deploy multiple Dell SonicWALL product lines. Qualified customers can save up to 30% off MSRP on appliances from each of Dell 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.

Dell 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.

Dell SonicWALL

Dell SonicWALL provides intelligent network security and data protection solutions that enable customers and partners to dynamically secure, control, and scale their global networks. Using input from millions of shared touch points in the Dell SonicWALL Global Response Intelligent Defense (GRID) Network, the Dell SonicWALL Threat Center provides continuous communication, feedback, and analysis on the nature and changing behavior of threats. Dell SonicWALL Research Labs continuously processes this information, proactively delivering countermeasures and dynamic updates that defeat the latest threats. Patented* Reassembly-Free Deep Packet Inspection technology, combined with multi-core parallel architecture, enables simultaneous multi-threat scanning and analysis at wire speed and provides the technical framework that allows the entire solution to scale for deployment in high bandwidth networks. Dell SonicWALL network security and data protection solutions, available for the SMB through the Enterprise, are deployed in large campus environments, distributed enterprise settings, government, retail point-of-sale and healthcare segments, as well as through service providers.

Dell SonicWALL has been hailed by industry publications such as Network World, InfoWorld, PC Magazine, and SC Magazine for easy to use, high quality, and high performance appliances and services. Gartner named Dell SonicWALL in the Visionaries Quadrant in the SSL VPN Magic Quadrant 2011, and most recently named Dell SonicWALL in the Leaders Quadrant in their 2012 Unified Threat Management Magic Quadrant. In the NSS Labs 2012 Next-Generation Firewall Security Value Map™, the Dell SonicWALL SuperMassive E10800 running SonicOS earned recognition as the Highest Overall Protection Next-Generation Firewall Recommended by NSS Labs. This proven SonicOS architecture is at the core of every Dell SonicWALL firewall.

Dell SonicWALL offers a comprehensive lineup of industry-leading network security and data protection solutions, including firewall, secure remote access/SSL VPN, anti-spam/email security, and continuous backup and recovery, plus centralized management and reporting, and 24x7 technical support.

Originally founded in 1991, SonicWALL was acquired by Dell in 2012.

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723