



Dell SonicWALL product lines

Table of contents

Overview	4
Network security/firewall solutions	
Network security solution summary	6
SuperMassive solutions	7
Wireless enablers	14
Subscription services, licenses and firmware	17
WAN acceleration solutions	
WAN acceleration solutions	19
Secure remote access solutions	
Secure remote access solution summary	21
E-Class solutions	21
Add-on features	22
SMB and branch office solutions	24
Add-on features	26
Anti-spam/email security solutions	
Email security solution summary	28
Email security solutions	28
Subscription services	30
Policy management and reporting solutions	
Global Management System	31
Scrutinizer	31
Analyzer	31
Global support services	
Platinum Support for the SuperMassive E10000 Series	32
Gold Support	32
Silver Support	32
E-Class Support	33
Dynamic Support	33
Comprehensive Global Management System Support	33
Focused Technical Support	33
Remote Start-up and Configuration Service	33



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 (NGFW) 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 4G/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 NGFWs, 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 4,600 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.

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.

Dell SonicWALL firewall/network security

Dell SonicWALL is one of the leading providers of next-generation firewalls (NGFWs). When deployed as a NGFWs 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 NGFWs 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 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 E10000 and 9000 Series. SuperMassive E10800 with SonicOS earned the recommended rating by NSS Labs for the second consecutive year. 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, 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.

Deep security, high performance and low latency next-generation firewall for the data center and enterprise



Dell SonicWALL SuperMassive Series at-a-glance

The SuperMassive E10000 and 9000 Series is the Dell SonicWALL 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 is ideal for securing enterprise networks, data centers and service providers. Combining massively scalable multi-core design and the patented RFDPI* technology, the SuperMassive delivers industry-leading application control, intrusion prevention, malware protection and SSL inspection.

	SuperMassive E10800	SuperMassive E10400	SuperMassive E10200
Cores	96	48	24
IPS throughput	30 Gbps	15 Gbps	7.5 Gbps
Firewall throughput	40 Gbps	20 Gbps	10 Gbps
Application inspection throughput	30 Gbps	15 Gbps	7.5 Gbps
Threat-prevention throughput	12 Gbps	6.0 Gbps	3.0 Gbps
Max connections	12.0M	6.0M	3.0M
Upgrade path	—	Field upgradeable to the E10800	Field upgradeable to the E10400, E10800

	SuperMassive 9600	SuperMassive 9400	SuperMassive 9200
Cores	32		24
IPS throughput	12 Gbps	10 Gbps	7.5 Gbps
Firewall throughput	20 Gbps	20 Gbps	15 Gbps
Application inspection throughput	12 Gbps	10 Gbps	7.5 Gbps
Threat-prevention throughput	5 Gbps	4.5 Gbps	3.5 Gbps
Max connections	1.5M	1.25M	

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



SuperMassive E10000 Series

	E10200	E10400	E10800
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 inspection 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	E10200	E10400	E10800
Site-to-site tunnels	10,000		
IPSec VPN clients	2,000		
SSL VPN licenses	50		
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	E10200	E10400	E10800
IP address assignment	Static (DHCP PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay		
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode		
VLAN interfaces	512		
Routing protocols	BGP, OSPF, RIPv1/v2, 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		
VoIP	Full H323-v1-5, SIP		
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certifications pending	FIPS 140-2, Common Criteria EAL4+, NEBS, ICSA Firewall		
Certifications	NSS NGFW Recommended and NSS IPS Recommended		
Common Access Card (CAC) support	Pending		
Hardware	E10200	E10400	E10800
Power supply	Dual, redundant, hot swappable, 850 W		
Fans	Dual, redundant, hot swappable		
Display	Front LED display		
Input power	100-240 VAC, 60-50 Hz		
Maximum power consumption (W)	400	550	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 k)
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, RoHS, WEEE		
Environment	40-105 F, 5-40 deg C		
Humidity	10-90% non-condensing		

All specifications, features and availability are subject to change.

SuperMassive 9000 Series

	9200	9400	9600
Operating system	SonicOS		
Cores	24	32	
10 GbE interfaces	4 x 10-GbE SFP+		
1 GbE interfaces	8 x 1-GbE SFP, 8 x 1 GbE (1 LAN Bypass pair)		
Management interfaces	1 GbE, 1 Console		
Memory (RAM)	8 GB	16 GB	32 GB
Expansion	1 Expansion Slot (Rear)*, SD Card*		
Firewall inspection throughput	15 Gbps	20 Gbps	
Application inspection throughput	7.5 Gbps	10 Gbps	12 Gbps
IPS throughput	7.5 Gbps	10 Gbps	12 Gbps
Anti-malware inspection throughput	3.5 Gbps	4.5 Gbps	5 Gbps
IMIX Performance (Gbps)	4.0 Gbps	6.2 Gbps	
VPN throughput	5.0 Gbps	10 Gbps	12 Gbps
Connections per second	110,000/sec	150,000/sec	
Maximum connections (SPI)	1.25M		1.5M
Maximum connections (DPI)	1.0M		1.25M
SonicPoints Supported (Maximum)	96	128	
VPN	9200	9400	9600
Site-to-site tunnels	6,000	10,000	
IPSec VPN clients (Maximum)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)
SSL VPN licenses (Maximum)	2 (50)		50 (50)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1		
Key exchange	Diffie Hellman Groups 1, 2, 5, 14		
Route-based VPN	RIP, OSPF		
Networking	9200	9400	9600
IP address assignment	Static (DHCP PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay		
NAT modes	:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode		
VLAN interfaces	512		
Routing protocols	BGP, OSPF, RIPv1/v2, 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		
VoIP	Full H323-v1-5, SIP		
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certifications pending	FIPS 140-2, Common Criteria EAL4+, NEBS, ICSA Firewall		
Common Access Card (CAC) support	Pending		
Hardware	9200	9400	9600
Power supply	Dual, redundant, hot swappable, 300 W		
Fans	Dual, redundant, hot swappable		
Display	Front LED display		
Input power	100-240 VAC, 60-50 Hz		
Maximum power consumption (W)	300		
Form factor	1U Rack Mountable		
Dimensions	17x19.1x1.75 in (43.3x48.5x4.5 cm)		
Weight	18.1 lb (8.2 kg)		
WEEE weight	23 lb (10.4 kg)		
Shipping weight	29.3 lb (13.3 kg)		
Major regulatory	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TUV/GS, CB, RoHS, WEEE, ANATEL, BSMI		
Environment	32-105 F, 0-40 deg C		
Humidity	10-90% non-condensing		

*Future use. All specifications, features and availability are subject to change.

Dell SonicWALL NSA Series at-a-glance

The Dell™ SonicWALL™ Network Security Appliance (NSA) Series is the one of the most secure, highest performing next-generation firewall lines. It delivers business-class security and performance without compromise, using the same architecture as the flagship SuperMassive NGFW line—initially developed for the world’s most demanding carriers and enterprises. At the same time, it offers Dell SonicWALL’s acclaimed ease of use and high value. Based on years of research and development, the NSA Series is designed from the ground-up for distributed enterprises, small- to medium-sized businesses, branch offices, school campuses and government agencies. The NSA Series combines a revolutionary multi-core architecture with a patented* Reassembly-Free Deep Packet Inspection® (RFDPI) single-pass threat-prevention engine in a massively scalable design. This offers industry-leading protection, performance, and scalability, with the highest number of concurrent connections, lowest latency, no file size limitations and superior connections-per-second in its class. Highly respected independent third-party testing firms have evaluated and/or certified the technology for your confidence and assurance.



Dell SonicWALL Network Security Appliance 6600

The Dell SonicWALL NSA 6600 NGFW is ideal for large distributed and corporate central site environments requiring high throughput protection and performance.



Dell SonicWALL Network Security Appliance 5600

The Dell SonicWALL NSA 5600 NGFW is ideal for distributed, branch office and corporate environments needing significant protection and performance.



Dell SonicWALL Network Security Appliance 4600

The Dell SonicWALL NSA 4600 NGFW is ideal for branch office and small- to medium-sized corporate environments concerned about throughput network protection and performance.



Dell SonicWALL Network Security Appliance 3600

The Dell SonicWALL NSA 3600 NGFW is ideal for branch office sites in distributed enterprise, small- to medium-sized businesses and retail environments.



Dell SonicWALL Network Security Appliance 2600

The Dell SonicWALL NSA 2600 NGFW is designed to address the needs of growing small organizations, branch offices and school campuses.

*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 NGFW offer branch offices and small to mid-size organizations in-depth frontline security and optional 802.11n 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 NGFWs offer branch offices and small to mid-size organizations 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
SonicOS supported	SonicOS 5.8.1.1		SonicOS Enhanced 5.6 (or higher)
Users and nodes	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)
Power supply	External 36W		Single 180W ATX
Cooling system (fans)	No Fan/1 Fan	2 Fans	
VLAN interfaces	25	35	25
High availability	Active/Passive with Optional State Sync		
Stateful throughput ¹	600 Mbps	750 Mbps	775 Mbps
3DES/AES throughput ²	150 Mbps	200 Mbps	300 Mbps
Gateway anti-virus throughput ³	115 Mbps	140 Mbps	160 Mbps
Intrusion prevention throughput ³	195 Mbps	250 Mbps	275 Mbps
Full DPI performance ³	110 Mbps	130 Mbps	150 Mbps
IMIX performance ³	180 Mbps	210 Mbps	235 Mbps
New connections per second	2,200	3,000	4,000
Maximum connections	85,000	110,000	225,000
Maximum DPI connections	32,000	64,000	125,000
Site-to-site VPNs	25	50	75
Zone security	Yes		
Object-based management	Yes		
Policy-based NAT	Yes		
Multiple ISP failover	Yes		
Load balancing	Yes		
Integrated wireless switch and controller	Yes		
3G wireless failover	Yes		—
Policy-based routing	Yes		
Comprehensive Anti-Spam Service	Optional		
Voice over IP (VoIP)	Yes		
IKEv2 VPN	Yes		
Secure remote management (SSHv2 support)	Yes		
SSL VPN and IPSec VPN remote access clients	Yes		
Secure Virtual Assist technicians	30-day trial		Yes
Route-based VPN	Yes		
TSA User authentication	Yes		
Dynamic address objects	Yes		
Layer 2 bridge mode	Yes		
Layer 2 wireless bridging	Yes		
Wireless switch and controller	Yes		
802.1q VLANs	Yes		
RIPv2 and OSPF routing	Yes		
Single Sign-On (SSO)	Yes		
Application intelligence and control	Optional		
Deep Packet Inspection SSL	Optional		
SSL control	Yes		
IPv6 ⁴	No		Yes
Application visualization	Yes		
NetFlow/IPFIX	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.



Network Security Appliances Series

Feature	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
SonicOS supported	SonicOS 6.1.2	SonicOS 6.1.1			
Users and nodes	Unrestricted				
Network interfaces	8 x 1 GbE	(2) 10-GbE SFP+, (4) 1GbE SFP, (12) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB			(4) 10-GbE SFP+, (8) 1GbE SFP, (8) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB
Power supply	Single, Fixed 200W	Single, Fixed 250W			
Cooling system (fans)	2 Fans				
VLAN interfaces	50		200	400	500
High availability	Active/Passive with Optional State Sync*		Active/Passive with Optional State Sync		
Stateful throughput ¹	1.9 Gbps	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
3DES/AES throughput ²	1.1 Gbps	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
Gateway anti-virus throughput ³	300 Mbps	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
Intrusion prevention throughput ³	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
Full DPI performance ³	300 Mbps	500 Mbps	800 Mbps	1.6 Gbps	3.0 Gbps
IMIX performance ³	600 Mbps	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
New connections per second	15,000	20,000	40,000	60,000	90,000
Maximum connections	225,000	325,000	400,000	750,000	
Maximum DPI connections	125,000	175,000	200,000	500,000	
Site-to-site VPNs	75	800	1,500	5,000	6,000
Zone security	Yes				
Object-based management	Yes				
Policy-based NAT	Yes				
Multiple ISP failover	Yes				
Load balancing	Yes				
Integrated wireless switch and controller	Yes				
3G wireless failover	—	Yes		—	Yes
Policy-based routing	Yes				
Comprehensive Anti-Spam Service	Optional				
Voice over IP (VoIP)	Yes				
IKEv2 VPN	Yes				
Secure remote management (SSHv2 support)	Yes				
SSL VPN and IPSec VPN remote access clients	Yes				
Secure Virtual Assist technicians	Yes				
Route-based VPN	Yes				
TSA User authentication	Yes				
Dynamic address objects	Yes				
Layer 2 bridge mode	Yes				
Layer 2 wireless bridging	Yes			No	
Wireless switch and controller	Yes			No	
802.1q VLANs	Yes				
RIPv2 and OSPF routing	Yes				
Single Sign-On (SSO)	Yes				
Application intelligence and control	Optional				
Deep Packet Inspection SSL	Optional				
SSL control	Yes				
IPv6 ⁴	Future release				
Application visualization	Yes				
NetFlow/IPFIX	Yes				
Link aggregation	Yes ⁵				
Port redundancy	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 SMBs, and retail/ POS deployments.

Dell SonicWALL SMB solutions: TZ Series at-a-glance

The Dell SonicWALL TZ Series is 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 ensures that bandwidth is available for business-critical applications while throttling or blocking unproductive applications. The TZ 215 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 iOS, Android, Windows, Windows 8.1/RT, 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 Series

The Dell SonicWALL TZ 215 is one of 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. TZ 215 also provides application control to ensure bandwidth for critical applications, while throttling nonproductive ones.



Dell SonicWALL TZ 205 Series

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.



Dell SonicWALL TZ 105 Series

The Dell SonicWALL TZ 105 delivers proven, 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		
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	
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	
Remote access SSL VPN tunnels (max)	5	10	
Remote access SSL VPN tunnels (bundled)	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		
Object-based management	Yes		
Policy-based NAT	Yes		
Multiple ISP failover	Yes		
ISP failover	Yes		
Hardware failover	No	Active/Passive	
WAN load balancing	Yes		
Layer 2 wireless bridging	Yes		
Wireless switch and controller	Yes		
Virtual Access Points (VAPs)	Yes ⁴		
Integrated access point	Optional 802.11n		
Comprehensive Anti-Spam Service	Optional		
Dual band wireless-N	Yes	Yes (2x2)	Yes (3x3)
Voice over IP (VoIP)	Yes		
PortShield security	Yes		
Route-based VPN	Yes		
3G wireless failover	Yes		
Bandwidth management	No	Yes	
Application intelligence and control	No	Yes	
Application visualization	No	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. 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. 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).



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.

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



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 service 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) is a powerful protection and productivity solution that delivers unequalled content filtering enforcement for educational institutions, businesses, libraries and government agencies. Using Dell SonicWALL CFS, organizations can control access to web sites containing information or images that are inappropriate, unproductive or even illegal. Granular controls provide administrators with the tools to create and apply policies that allow or deny access to sites based on individual or group identity, or by time of day for over 56 pre-defined categories. CFS also dynamically caches web site ratings locally on the Dell SonicWALL firewall for near-instantaneous response times.



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 SSL Decryption and Inspection

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 iOS, Android, and Windows 8.1/RT, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections. It also 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, and secure remote access devices while leveraging application traffic analytics for security event reports.



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, 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.

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, HTTP (web) caching and data-in-flight compression.

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 a Dell SonicWALL NGFW running 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 makes it easy for you to add a WXA solution into your network by providing a variety of platform options including both hardware and virtual appliances as well as Live CD software



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 acceleration connections.

Dell SonicWALL WXA 4000

The WXA 4000 accelerates network performance for up to 240 users and 1,200 WAN acceleration connections.

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		Virtual Appliance (VMWare)
Maximum users ¹	20	120	240	360
Maximum connections	100	600	1,200	1,800 ³
Included/maximum concurrent WXA client licenses ⁴	2/20	2/50	2/125	2/125
Byte caching	Yes			
Web (HTTP) caching	Yes			
Compression	Yes			
Signed SMB support	Yes			
Management	Requires SonicOS 5.8.1 or later			
CIFS/SMB 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
Dell Hardware	Dell OptiPlex 3010 Dell Inspiron 660s Dell Vostro 270s

	WXA 5000 Virtual Appliance Only
Hypervisor	ESX and ESXi (version 4.0, 5.0 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 connections being generated per user. ² CIFS/SMB 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. ⁴ NetExtender is required in order to use the WXA client software. Please refer to the WXA release notes for supported operating systems.



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 proliferation of mobile devices has increased the demand for secure access to mission critical applications, data and resources. In parallel, a growing mobile malware threat has caused mobile protection to become a business imperative. Because legacy, client-based VPNs can be cumbersome for mobile workers to use and manage, IT professionals are looking for easy-to-use, cost-effective and secure mobile access solutions that address the needs of their increasingly mobile workforces. Dell SonicWALL provides scalable secure mobile access solutions to fit organizations of all sizes—from small-to medium-sized businesses to large global enterprises. Dell SonicWALL Aventail™ E-Class Secure Remote Access (SRA) and Dell SonicWALL Secure Remote Access (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. And unlike other device management solutions, Dell solutions can easily provision secure mobile access and role-based privileges so end-users get fast, simple access to the enterprise applications, data and resources they demand. At the same time, organizations can institute secure BYOD policies to protect their corporate networks from rogue access and malware.

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

The Dell SonicWALL E-Class Secure Remote Access (SRA) appliance provides large enterprise remote workers using smartphones, tablets or laptops, whether managed or unmanaged, fast, easy, policy-enforced access to mission critical applications, data and resources without compromising security. Dell SonicWALL SRA appliances deliver robust solutions by providing:

- Secure remote access to mission-critical applications and resources from a wide range of endpoint devices running a variety of operating system, including Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux®, and 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 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 enforce 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 8.1/RT, Apple Mac OS, iOS, Linux, and Android devices.

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 8.1/RT, Apple Mac OS, iOS, Linux, and 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 8.1/RT, Apple Mac OS, iOS, Linux, and 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 5,000 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 8.1/RT, Apple Mac OS, iOS, Linux, and 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. Advanced EPC simplifies endpoint protection with a comprehensive checklist of anti-virus, personal firewall and anti-spyware products that even verifies versions and signature file updates. Advanced EPC adds the encrypted virtual desktop functionality of Secure Desktop for the easiest, most robust remote access control on the market.



Dell SonicWALL Aventail Advanced Reporting

Advanced Reporting delivers powerful analysis of remote access to your resources. Dell SonicWALL Aventail Advanced Reporting[™] provides powerful analysis of remote access to resources. Advance Reporting is a robust hierarchical log analysis tool that can track and evaluate all remote user access to enterprise resources over the E-Class SRA appliance.



SonicWALL Mobile Connect

Mobile Connect, a single unified client app for iOS, Android and Windows 8.1/RT, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.



Dell SonicWALL Aventail Native Access Modules

Dell SonicWALL Aventail® Native Access Modules™ provide native protocol access to Citrix®, Windows® Terminal Services and VMWare® View via a secure Dell SonicWALL Aventail E-Class Secure Remote Access appliance. Native Access Modules deliver access to server-based sessions without any additional configuration. Using a single portal link, remote users receive an easy, seamless experience while accessing all Citrix applications, including support for load-balance Citrix farms.



Dell SonicWALL Aventail Spike License

Spike License is a disaster recovery “insurance policy” for future increases in remote users. The Spike License Pack is a temporary-capacity add-on license providing flexibility to increase their remote user count immediately in the event of a disaster or other business disruption. It is ideal as part of a company’s overall disaster recovery plan as well as for firms that experience seasonal spikes.



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.

Feature	Virtual Appliance	EX6000	EX7000	EX9000
Concurrent user license	up to 5,000	up to 250	up to 5,000	up to 20,000
Basic End Point Control (EPC) interrogation	Included			
Advanced EPC (anti-virus, personal firewall, anti-spyware)	Add-on		Included	
Aventail Secure Desktop/ cache cleaner	Add-on		Included	
Allow, deny and quarantine zones based on EPC interrogation	Included			
Granular access control (user and group, source IP, service/port, destination URL, host name/ip address, IP range, subnet, domain)	Included			
Advanced reporting	Add-on			
Analyzer	Add-on			
WorkPlace portal	Included			
WorkPlace Mobile (optimized portal for mobile phone browsers)	Included			
Native Access Modules (Citrix, Windows Terminal Services and VMWare View)	Add-on		Included	
Connect Tunnel (Windows, Mac OS and Linux)	Included			
Mobile Connect (iOS)	Included			
Mobile Connect (Android)	Included			
Mobile Connect (Windows 8.1/RT)	Included			
IPv6 client side support	Included			
ADA 508 support	Included			
At-a-glance status dashboard	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 a hardware or 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, Android and Windows 8.1/RT 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®, Mac OS® or Linux® devices 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 makes it easy for employees to get the support they need by enabling technicians to assume control of a Windows, Mac OS or Linux device remotely to diagnose and fix problems
- Secure Virtual Access helps to ensure a seamless workflow by making it easy for employees to gain secure access to their Windows® computers from any location
- 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 remote collaboration
- Spike licensing allows for the administrator to prepare a disaster recovery plan to support a temporary spike in the number of licensed users
- Clean VPN is enabled when a Dell SonicWALL SRA Series appliance is deployed alongside a Dell SonicWALL next-generation firewall utilizing powerful deep packet inspection technology to scan traffic and remove malware threats before they enter into the network



Dell SonicWALL Secure Remote Access 4600

The Dell SonicWALL Secure Remote Access (SRA) 4600 provides medium-size organizations with a powerful, easy-to-use and cost-effective secure remote access solution that requires 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 more devices and operating systems including Windows, Windows 8.1/RT, Mac OS, Linux, Apple iOS and Android. Additional value-added services allow remote PC support, access and collaboration while Web Application Firewall adds a further layer of security for web applications. High Available (HA) on the SRA 4600 provides an Active/Passive configuration to enable increased reliability in the event of failure.



Dell SonicWALL Secure Remote Access 1600

For small- to medium-sized businesses, the Dell SonicWALL Secure Remote Access (SRA) 1600 provides a powerful, easy-to-use and cost-effective secure remote access solution that requires 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 more devices and operating systems including Windows, Windows 8.1/RT, Mac OS, Linux, Apple iOS and Android. Additional value-added services allow remote PC support and access while Web Application Firewall adds a further layer of security for web applications.

Secure Remote Access Virtual Appliance

The Dell SonicWALL Secure Remote Access (SRA) Virtual Appliance offers clientless and tunnel access for Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux, and Android. Additional value-added services allow remote PC support, access and collaboration while Web Application Firewall adds a further layer of security for web applications. 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).

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" in order to protect against day-zero web application threats. Additionally, administrators can use Geolocation and Botnet filtering to create and enforce policies to block connections from a specific geographic region or from systems known to be infected with malware. 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 iOS, Android and Windows RT/8.1, 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 a user's PC or laptop running Windows, Mac OS 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 to send support staff on-site to debug problems.



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 Secure 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 through the SRA web portal. 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 calendar scheduling systems such as Microsoft Outlook™.



Dell SonicWALL End Point Control for SRA Series

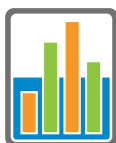
End Point Control (EPC) for the Secure Remote Access (SRA) Series delivers enterprise-class device identification and interrogation features to small and medium-sized businesses. EPC for the SRA Series uniquely identifies Windows, Mac OS and Linux endpoints to tie them to authorized users. It also enforces granular security posture by checking for essential components such as anti-virus, anti-spyware and personal firewall software to ensure device integrity before allowing the devices to connect to the network. 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 for a temporary period of time due to a disaster or other business disruption.



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.

Deployment	SRA 1600	SRA 4600	SRA Virtual Appliance
Type and size of deployment environment	Small organizations with fewer than 50 employees	Mid-size organizations with 250 or fewer employees	Small organizations with fewer than 50 employees
Included/maximum (recommended) number of licensed users	5/50 (25)	25/500 (100)	5/50
Virtual Access/Virtual Assist included/maximum licensed connections	30-day trial/10	30-day trial/25	

Features	SRA 1600	SRA 4600	SRA Virtual Appliance
Secure Virtual Access		Add-on	
Secure Virtual Assist		Add-on	
Secure Virtual Meeting	–		Add-on
End Point Control for SRA Series		Add-on	
Analyzer		Add-on	
Web Application Firewall		Add-on	
Spike Licensing		Add-on	
Geolocation-based policies		Add-on	
Botnet Filtering		Add-on	
One time password (OTP) authentication		Included	
Dell Quest Defender two-factor authentication support		Included	
Citrix (ICA) support		Included	
NetExtender: Support for multiple IP ranges and routes		Included	
Optional client certificate support		Included	
Graphical usage monitoring		Included	
Option to create system backup		Included	
Reverse proxy: OWA premium version and Lotus Domino Access		Included	
RADIUS test function		Included	
Active directory groups support		Included	
Virtual host/domain name support		Included	
FileShares Java applet		Included	
Diagnostics: DNS lookup and traceroute		Included	
SNMPv2		Included	
Layer-7 load balancing		Included	
High Availability (HA)	–	Included	–
SSL hardware-assisted offload	–	Included	Depends on underlying hardware
Mobile Connect (iOS)		Included	
Mobile Connect (Android)		Included	
Mobile Connect (Windows 8.1/RT)		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 patented¹ 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 Email Security Series

Dell SonicWALL Email Security appliances

Dell SonicWALL Email Security appliances offer comprehensive, effective and scalable email security for SMB, enterprise and MSSP 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 Email Security Software

For organizations 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 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.

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

Dell SonicWALL Hosted Email Security

Dell SonicWALL Hosted Email Security offers superior cloud-based protection from inbound and outbound threats, including spam, phishing, zombie 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 Global Response Intelligent Defense (GRID) Anti-Virus, Dell SonicWALL Time Zero, and premium anti-virus technologies, to deliver best-in-class email security. The Dell SonicWALL GRID Network 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, premium anti-virus technology from industry leading anti-virus partners provides 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	ES8300
Rackmount chassis	1RU		2RU
CPU	Intel 2.0GHz	Intel Dual Core 2.0GHz	Quad Core Xeon
RAM	2 GB	4 GB	
Hard drive	250 GB	2 x 250 GB	4 x 750 GB
Redundant Disk Array (RAID)	No	Yes	RAID 5
Hot swappable drives	No	Yes	
Redundant power supply	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 policy management and reporting 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, 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.

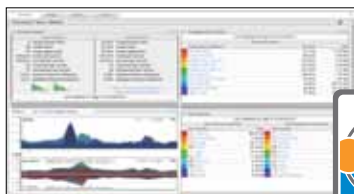


- GMS Software – Dell SonicWALL GMS can be flexibly deployed as a software application on a third party Windows server, leveraging existing infrastructure.
- GMS Virtual Appliance – The Dell SonicWALL GMS Virtual Appliance provides a hardened, performance-optimized virtual appliance agent for the Dell 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.
- 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.



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, 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 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 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 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)

Gold Support

Exclusive to NSA 5600, NSA 6600 and SuperMassive 9000 Series next-generation firewalls, Gold Support provides the advanced support features enterprise organizations need to keep their networks running reliably and securely. With Gold Support, you have around-the-clock access to seasoned support engineers at a Dell SonicWALL Enterprise TAC plus the latest firmware features and Advance Exchange hardware replacement, all of which combine to protect and maximize your Dell SonicWALL investment.

- Software and firmware updates and upgrades
- 24x7 access to a team of season support engineers located at a Dell SonicWALL Enterprise TAC for telephone, email and web-based technical assistance
- Advance Exchange hardware replacement (RMA)

Silver Support

More than a traditional break-fix service, Dell SonicWALL Silver Support is a multi-layered security offering that provides you with access to critical firmware updates and upgrades plus expert technical assistance to keep your Dell SonicWALL solution performing optimally. Services include:

- Subscription to firmware updates and upgrades
- 8x5 or 24x7 access to chat, email, web and telephone technical support
- Advance Exchange Next Business Day hardware replacement in the event of failure

E-Class Support

For 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 located at a Dell SonicWALL Enterprise TAC 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

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) 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.

Dell SonicWALL

Dell SonicWALL provides intelligent network security 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 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 2013 Unified Threat Management Magic Quadrant. In the NSS Labs 2013 Next-Generation Firewall Security Value Map™, the Dell SonicWALL SuperMassive E10800 running SonicOS earned the recommended rating for the second consecutive year. This proven SonicOS architecture is at the core of every Dell SonicWALL firewall.

Dell SonicWALL offers a comprehensive lineup of industry-leading network security solutions, including firewall, secure remote access/SSL VPN, anti-spam/email security 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



For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com

T +1 408.745.9600

F +1 408.745.9300

Dell Software

5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.

© 2013 Dell, Inc. ALL RIGHTS RESERVED. Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

