Dell SonicWALL product lines

Table of contents

Overview

Deeper Network Security

Not all next-generation firewalls are the same. To start, Dell™ SonicWALL™ NGFWs are the only firewalls capable of providing organizations of any size with a deeper level of network security because they are designed using a scalable, multi-core hardware architecture and a patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine that scans all traffic regardless of port or protocol. Dell NGFWs ensure that every byte of every packet is inspected while maintaining the high performance and low latency that busy networks require. Additionally, in order to combat emerging threats effectively and address rising productivity concerns, organizations require a deeper level of security and control that includes an IPS with advanced anti-evasion capabilities, the ability to decrypt and inspect every SSL-encrypted connection crossing the network (on any port), granular control over and visibility into application and user activity across the network, and network-based malware protection that leverages the power of the cloud.

Secure Mobile Access

The proliferation of mobile devices in the workplace, both employer issued and personally owned, has increased the demand on organizations to enable secure mobile access to company applications, data and resources. To address mobile workforce needs, Dell™ delivers a secure mobile access solution that combines its SonicWALL™ Mobile Connect application with its Secure Remote Access or next-generation firewall appliances. The solution enables you to easily provision secure mobile access and role based privileges for managed and unmanaged devices. You can provide mobile workers with fast, simple access to the organization's applications, data and resources that they demand. At the same time, you can ensure that the network is protected from mobile security threats, such as unauthorized access to data and malware attacks, without affecting personal data and apps.

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

2014 NSS Labs NGFW and
2013 IPS Security Value Maps

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	28 Gbps	15 Gbps	7.5 Gbps
Firewall throughput	40 Gbps	20 Gbps	10 Gbps
Application inspection throughput	28 Gbps	15 Gbps	7.5 Gbps
Threat-prevention throughput	12 Gbps	6.0 Gbps	3.0 Gbps
Max connections (SPI)	12.0M	6.0M	3.0M
Max connections (DPI)	10.0M	5.0M	2.5M
SSO User	60,000	40,000	
Upgrade path	—	Field upgradeable to the E10800	Field upgradeable to the E10400, E10800

	SuperMassive 9800	SuperMassive 9600	SuperMassive 9400	SuperMassive 9200
Cores	64	32		24
IPS throughput	24 Gbps	11.5 Gbps	10 Gbps	5 Gbps
Firewall throughput	40 Gbps	20 Gbps	20 Gbps	15 Gbps
Application inspection throughput	24 Gbps	11.5 Gbps	10 Gbps	5 Gbps
Threat-prevention throughput	10 Gbps	5 Gbps	4.5 Gbps	3.5 Gbps
Max connections (SPI)	3.0M	1.5M	1.25M	1.0M
Max connections (DPI)	2.5M	1.5M	1.25M	
SSO User	110,000	100,000	90,000	80,000

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

SuperMassive E10000 Series

	E10400	E10800
Operating system	SonicOS	
Security Processing Cores	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)	32 GB	64 GB
Storage	80 GB SSD, Flash	
Firewall inspection throughput	20 Gbps	40 Gbps
Application inspection throughput	15 Gbps	28 Gbps
IPS throughput	15 Gbps	28 Gbps
Anti-malware inspection throughput	6.0 Gbps	12 Gbps
SSL-DPI performance	3 Gbps	5 Gbps
VPN throughput	10 Gbps	20 Gbps
Latency	24µs	
Connections per second	200,000/sec	400,000/sec
Maximum connections (SPI)	6.0M	12.0M
Maximum connections (DPI)	5.0M	10.0M
SSO User	40,000	60,000
VPN	**E10400**	**E10800**
Site-to-site tunnels	10,000	
IPSec VPN clients	2,000	
Encryption	DES, 3DES, AES (128, 192, 256-bit)	
Authentication	MD5, SHA-1, Common Access Card (CAC)	
Key exchange	Diffie Hellman Groups 1, 2, 5, 14	
Route-based VPN	RIP, OSPF	
Networking	**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	1024	2048
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	FIPS 140-2, Common Criteria NDPP, IPv6 Phase 2, VPAT, VPNC	
Third party verification	NSS NGFW Recommended and NSS IPS Recommended	
Hardware	**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)	550	750
Form factor	4U Rack Mountable	
Dimensions	17x18x7 in (43x43.5x17.8 cm)	
Weight	61 lb (27.7 kg)	67 lb (30.3 k
WEEE weight	62 lb (28.1 kg)	68 lb (30.8 kg)
Shipping weight	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	9800
Operating system	SonicOS			
Security Processing Cores	24	32		64
10 GbE interfaces	4 x 10-GbE SFP+			
1 GbE interfaces	8 x 1-GbE SFP, 8 x 1 GbE (1 LAN Bypass pair)			12 x 1-GbE SFP, 8 x 1 GbE
Management interfaces	1 GbE, 1 Console			
Memory (RAM)	8 GB	16 GB	32 GB	64GB
Storage	Flash			2x 80GB SSD, Flash
Expansion	1 Expansion Slot (Rear)*, SD Card*			
Firewall inspection throughput	15 Gbps	20 Gbps		40 Gbps
Application inspection throughput	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
IPS throughput	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
Anti-malware inspection throughput	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps
IMIX Performance (Gbps)	4.0 Gbps	6.2 Gbps		9 Gbps
SSL-DPI	1 Gbps	2 Gbps	2 Gbps	5 Gbps
VPN throughput	5.0 Gbps	10 Gbps	12 Gbps	18 Gbps
Latency	17µs			
Connections per second	110,000/sec	150,000/sec		280,000/sec
Maximum connections (SPI)	1.25M		1.5M	3M
Maximum connections (DPI)	1.0M		1.25M	2.5M
SSO User	80,000	90,000	100,000	110,000
SonicPoints Supported (Maximum)	128			-
VPN	**9200**	**9400**	**9600**	**9800**
Site-to-site tunnels	6,000	10,000		25,000
IPSec VPN clients (Maximum	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)	2,000 (10,000)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Common Access Card (CAC)			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14			
Route-based VPN	RIP, OSPF			
Networking	**9200**	**9400**	**9600**	**9800**
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	FIPS 140-2, Common Criteria NDPP			
Certifications	ICSA Enterprise Firewall, IPv6 Phase 2, VPNC, VPAT, USGv6			
Hardware	**9200**	**9400**	**9600**	**9800**
Power supply	Dual, redundant, hot swappable, 300 W			Dual, redundant, hot swappable, 500 W
Fans	Dual, redundant, hot swappable			
Display	Front LED display			
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	300			350
Form factor	1U Rack Mountable			2U Rack Mountable
Dimensions	17x19.1x1.75 in (43.3x48.5x4.5 cm)			17x24x3.5 in (9x60x43 cm)
Weight	18.1 lb (8.2 kg)			40.5 lb (18.38 kg)
WEEE weight	23 lb (10.4 kg)			49.5 lb (22.4 kg)
Shipping weight	29.3 lb (13.3 kg)			65 lb (29.64 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			15-40 deg C
Humidity	10-90% non-condensing			10-95% 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
SonicOS supported	SonicOS 5.9	
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
Power supply	External 36W	
Cooling system (fans)	No Fan/1 Fan	2 Fans
VLAN interfaces	25	35
High availability	Active/Passive with Optional State Sync	
Stateful throughput[1]	600 Mbps	750 Mbps
3DES/AES throughput[2]	150 Mbps	200 Mbps
Gateway anti-virus throughput[3]	115 Mbps	140 Mbps
Intrusion prevention throughput[3]	195 Mbps	250 Mbps
Full DPI performance[3]	110 Mbps	130 Mbps
IMIX performance[3]	180 Mbps	210 Mbps
New connections per second	2,200	3,000
Maximum connections	85,000	110,000
Maximum DPI connections	32,000	64,000
Site-to-site VPNs	25	50
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	
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	
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	10	20
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 Intrusion Prevention

The Dell SonicWALL Intrusion Prevention System (IPS) Service provides network protection around the clock — including the critical periods between patches. Dell's award-winning IPS Service is activated as a license on SonicWALL TZ, NSA and SuperMassive Series appliances, and integrates a high-performance, deep-packet inspection architecture with dynamically updated countermeasures for complete protection from application exploits and other malicious traffic. The Dell IPS Service is scalable to support virtually any size organization. It also provides enforcement between each network zone and the internet, and between internal zones for added security. In addition, the Dell IPS Service is powered by an industry-leading threat research team with deep experience in vulnerability analysis and countermeasure creation. The team gathers threat intelligence from over one million connected sensors around the world, so Dell IPS subscribers benefit from a nimble and fast response to new attacks, regular security updates and out-of-band updates when necessary.

2013 NSS Labs IPS Security Value Map

Dell SonicWALL Malware Prevention

The Dell SonicWALL Threat Research team has nearly 10 years of experience in malware analysis and countermeasure creation. Thanks to over one million connected sensors deployed around the world, the Dell SonicWALL Threat Research Team receives tens of thousands of new samples every day. Businesses can benefit from the expertise of the Dell SonicWALL Threat Research Team by subscribing to the Dell Malware Prevention Service, a cost-effective, comprehensive threat protection service that stops APTs, RATs, viruses, key loggers, spyware, and other nasty things from entering networks. The service is available by annual subscription and works with Dell SonicWALL TZ, NSA and SuperMassive Series next-generation firewalls. And because Dell is an industry leader in developing malware signatures that are highly-effective, low-maintenance, automated and scalable, the service ensures that networks are protected against emerging threats 24 hours a day, 365 days a year.

Dell SonicWALL NGFW are tested and certified monthly by ICSA Labs for Malware Prevention

Dell SonicWALL Application Intelligence and Control

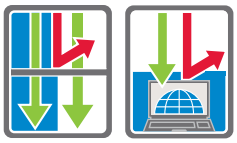
The Application Intelligence and Control Service for Dell SonicWALL next-generation firewalls provides context-aware application control and administrators with the tools they need to easily manage privileges and bandwidth for applications, users, groups or devices. The policies are then updated automatically as new users and applications are added to IT systems. In addition, application traffic analytics provide administrators with real-time insights that allow them to troubleshoot network outages and security threats quickly and efficiently.

Dell SonicWALL SSL Inspection

Organizations can safeguard their networks from these tactics with Dell SonicWALL SSL Decryption and Inspection, an add-on service to Dell SonicWALL next-generation firewall appliances. Available as a one-time license, the service provides advanced protection against SSL threats. Dell's patented Reassembly-Free Deep Packet Inspection® engine, full-stack stream inspection technology, inspects SSL-encrypted traffic — including HTTPS and FTPS — and regardless of the port being used. The service decrypts SSL traffic, scans it for threats and then re-encrypts it, sending it along to its destination if no threats or vulnerabilities are found.

*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 Content Filtering Service and Content Filtering Client

Content Filtering Service (CFS) and Content Filtering Client (CFC) are powerful protection and productivity solutions that deliver unequalled content filtering enforcement for educational institutions, businesses, libraries and government agencies. Using Dell SonicWALL CFS, organizations can create and apply web use policies that control access to web sites containing information or images that are inappropriate, unproductive or even illegal. Extend enforcement of internal web use policies to block objectionable and unproductive internet content for devices located outside the firewall perimeter with the Content Filtering Client. 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 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.

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.

SonicWALL Mobile Connect™

Mobile Connect, a single unified client app for iOS, OS X, Android, Kindle Fire 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 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 SuperMassive 9000, 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 a bootable linux software image.

Dell SonicWALL WXA 500 Software
The WXA 500 Live CD supports flexible deployment via a bootable linux software image.

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.

Dell SonicWALL WXA 6000 software
The WXA 6000 software running on Dell PowerEdge R320 hardware supports higher scale deployments.

Features	WXA 500 Software	WXA 2000	WXA 4000	WXA 5000 Virtual Appliance	WXA 6000 Software
Platform	Software[5]	Hardware Appliance		Virtual Appliance (VMWare)	Software[5]
Maximum users[1]	20	120	240	360	2,000
Maximum connections	100	600	1,200	1,800[3]	10,000
Included/maximum concurrent WXA client licenses[4]	2/20	2/50	2/125	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 Software Only
Dell Hardware	Dell OptiPlex 3010 Dell Inspiron 660s Dell Vostro 270s

	WXA 6000 Software Only
Dell Hardware	Dell PowerEdge R320 Server

	WXA 5000 Virtual Appliance Only
Hypervisor	ESX and ESXi (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. [5] The WXA 500 and 6000 software can be downloaded from www.mysonicwall.com and requires specific Dell hardware in order operate.

Dell Secure Mobile Access delivers fast, easy, policy-enforced access to mission-critical applications, data and resources without compromising security.

Dell Secure Mobile Access solutions

The proliferation of mobile devices in the workplace, both personally owned and employer issued, has created a requirement to enable secure mobile access to corporate data and resources. Often, mobile workers want to use personal mobile devices for business use, resulting in the intermingling of business and personal data and applications. With this, enterprises are at increased risk of:

- Security breaches caused by unauthorized users gaining access to company networks and systems from lost or stolen devices.
- Interception of company data in-flight on unsecured public WI-Fi networks.
- Loss of business data at-rest on devices.
- Malware infected devices or personal apps acting as a conduit to infect company systems.

Mobile workers are also concerned about personal privacy, and in some countries, employers are legally prohibited from tampering with employee personal data and can be held liable for damages.

To enable access for mobile workers while protecting data from threats, enterprises must implement solutions that take a new approach focused on managing and securing business apps, data and usage, while coexisting with personal apps and respecting personal data privacy. IT needs to safeguard corporate data and resource access to ensure only authorized users, business applications and validated devices that meet security policy are granted corporate network access, and that personal content is excluded from corporate network access. Also, company data in-flight and at-rest on mobile devices must be kept secure, and personal data must not be tampered with.

Unfortunately, this often involves proprietary mobile applications, custom application development and complex multi-box solutions from multiple vendors to support VDI and container applications that add significantly to the complexity and total cost of ownership.

With Dell™ Secure Mobile Access solutions, including Secure Remote Access (SRA) appliances and the Mobile Connect app, you can offer mobile and remote workers using smartphones, tablets or laptops — whether managed or unmanaged — policy-enforced SSL VPN access to mission-critical applications, data and resources without compromising security.

Dell SonicWALL provides solutions to fit organizations of all sizes—from small-to medium-sized businesses to large global enterprises. The Dell SonicWALL E-Class Secure Remote Access (SRA) and the 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 E-Class SRA Series at-a-glance

Dell SonicWALL E-Class Secure Remote Access (SRA) with the new Secure Mobile Access (SMA) OS 11.0 enables administrators to easily provision secure mobile access and role based privileges for managed and BYOD unmanaged devices. You can provide mobile workers with policy-enforced per app SSL VPN access to the allowed enterprise data and resources that they demand, while protecting the corporate network from mobile security threats. With SMA, only authorized users, mobile apps and trusted devices are permitted access to resources. Also, corporate VPN access can be restricted to the set of mobile apps trusted by the administrator while unauthorized mobile apps are prevented from accessing VPN resources. SMA is the only solution that requires no modification of mobile apps for per app VPN access. Any mobile app or secure container can be supported with no modifications, app wrapping or SDK development. The solution also helps enforce and track mobile worker acceptance of device authorization policy terms, reducing legal risk. For mobile device users, the solution includes the intuitive SonicWALL Mobile Connect™ app that, in combination with the E-Class SRA, provides iOS, Mac OS X, Android, Kindle Fire or Windows 8.1 devices with fast, easy per-app VPN access to permitted resources, including shared folders, client server applications, intranet sites, email and virtual desktop applications such as Citrix, VMware view, RDP and Dell vWorkspace. For multi-layer threat protection, when integrated with a Dell SonicWALL next-generation firewall as a Clean VPN™, the solution decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment and the combined solution delivers centralized access control, malware protection, web application control and content filtering.

Secure Mobile Access Solutions — Dell SonicWALL E-Class SRA Series

Dell SonicWALL E-Class SRA EX9000

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 E-Class SRA EX7000

The 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 E-Class SRA EX6000

The 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 E-Class SRA Virtual Appliance

The 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 E-Class SRA add-on features

SonicWALL Mobile Connect

Mobile Connect, a single unified client app for iOS, OS X, Android, Kindle Fire 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 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 Advanced Reporting

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

Dell SonicWALL Native Access Modules

Native Access Modules provide native protocol access to Citrix®, Windows® Terminal Services and VMWare® View via a secure Dell SonicWALL 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 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 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	
Cache cleaner	Add-on		Included	
End-user device registration and authorizationpolicy acceptance, management and reporting (requires SMA OS 11.0)	Add-on		Included	
Mobile application VPN access control (requires SMA OS 11.0)	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 tablet and 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, OS X)	Included			
Mobile Connect (Android, Kindle Fire)	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 SRA Series offers affordable, easy-to-use and manage secure remote access.

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

The Dell SonicWALL Secure Remote Access (SRA) Series provides mobile and remote workers using smartphones, tablets or laptops — whether managed or unmanaged BYOD — with fast, easy, policy-enforced access to mission critical applications, data and resources without compromising security. For mobile devices, the solution includes the intuitive SonicWALL Mobile Connect™ application that provides iOS, Android,Kindle Fire, Windows, and Mac OSX devices secure access to allowed network resources, including shared folders, client-server applications, intranet sites and email. Users and IT administrators can download the SonicWALL Mobile Connect application via the Apple AppStore, Google Play and the Kindle store. New with Windows 8.1, Windows tablets and laptops ship pre-installed with the Mobile Connect application. For PCs and laptops, including Windows®, Mac OS and Linux® computers, the solution supports clientless, secure browser access and thin-client VPN access. To protect from rogue access and malware, the SRA Series appliance connects only authorized users and trusted devices to permitted resources. When integrated with a Dell SonicWALL next-generation firewall as a Clean VPN™, the combined solution delivers centralized access control, malware protection, application control and content filtering. The multi-layered protection of Dell SonicWALL Clean VPN™ decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment.

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. Users can easily and securely access email, files, intranets, applications, remote desktops, servers and other resources on the corporate LAN from more smartphone, tablet and laptops including iOS, Mac OS X, Android, Kindle, Windows, and Linux devices. 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. Users can easily and securely access email, files, intranets, applications, remote desktops, servers and other resources on the corporate LAN from more smartphone, tablet and laptops including iOS, Mac OS X, Android, Kindle, Windows and Linux devices. 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

SonicWALL Mobile Connect

With the SonicWALL Mobile Connect application, in combination with Dell SonicWALL Secure Remote Access (SRA) or next-generation firewall appliances, you can give your employees safe, easy access to the data and resources they need to be productive from a range of devices, including iOS, OS X, Android™, Kindle Fire and Windows 8.1, while ensuring that the corporate network is protected from mobile security threats. With the Dell solution, mobile workers simply install and launch the Mobile Connect application on their iOS, OS X or Android mobile device, or simply launch it from their Windows 8.1 device, to establish a secure connection to an SRA or next-generation firewall appliance. The encrypted SSL VPN connection will protect traffic from being intercepted and keep in-flight data secure.

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, iOS, Mac OS, Android 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 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.

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 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[1]	Add-on		
Botnet Filtering[1]	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		
RDP/VNC over HTML5	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	
Mobile Connect (iOS, OS X)	Included		
Mobile Connect (Android, Kindle Fire)	Included		
Mobile Connect (Windows 8.1/RT)	Included		

[1] Geolocation and Botnet filtering protection require a valid support contract on the SRA appliance.

Dell SonicWALL Email Security provides superior email protection from email threats and compliance violations.

Dell SonicWALL Email Security

Email is crucial for your business communication, but it can also expose your business to sabotage and productivity drains if email-based threats such as spam, phishing, viruses and zombies flood your mail servers and user inboxes. What's more, government regulations now hold your business accountable for protecting confidential data, ensuring it is not leaked and ensuring secure exchange of email containing sensitive customer data or confidential information. Whether your organization is a growing small- to midsize business (SMB), a large distributed enterprise, or managed service provider (MSP), you need a cost-effective way to deploy email security and encryption for your IT infrastructure, and the scalability to easily grow capacity for—and delegate management across— organizational units and domains.

Dell SonicWALL Email Security provides superior email protection from email threats and compliance violations. Multiple proven, patented* threat detection techniques deliver real-time protection from spam, phishing attacks and viruses. Compliance scanning and management prevent confidential data leaks and regulatory violations.

With integrated email encryption, policies may be configured to scan outbound email content and attachments for sensitive data. When detected, the email is encrypted for secure email exchange with customers and partners. Encrypted email can be tracked to confirm the time of receipt and time opened. Intuitive for the recipient, a notification email is delivered to the recipient's inbox with instructions to simply log into a secure portal to read or securely download the email. The service is cloud based with no additional client software necessary and unlike competitive solutions; the encrypted email may be accessed and read from mobile devices or laptops.

Easy to set-up and administer, the solution is architected to cost-effectively scale from 10 to 100,000 mailboxes, and may be deployed as a hardware appliance, virtual appliance, or windows server software to best meet your infrastructure requirements. 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, multitenancy 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.

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

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.

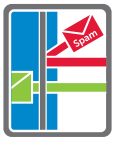
Dell SonicWALL Email Security Virtual Appliance

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.

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.

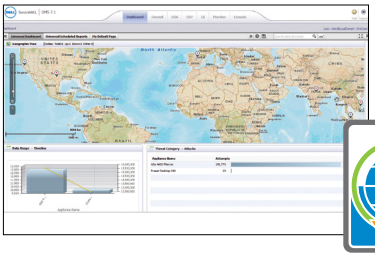
Dell SonicWALL Email Anti-Virus Subscription
Email Anti-Virus Subscription provides protection from the time a virus outbreak occurs until the time a signature update is available through Dell SonicWALL Time Zero Technology. Dell SonicWALL provides additional layers of protection by partnering with McAfee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

Dell SonicWALL Email Compliance and Encryption Subscription
Dell SonicWALL Email Compliance and Encryption Subscription services work with the Dell SonicWALL Email Security solution to provide organizations of all sizes with a powerful framework for stopping email threats, managing compliance requirements, and providing mobile-ready secure email exchange. Adding Email Compliance and Encryption subscription services to the Email Security solution enables organizations to meet both regulatory and corporate requirements. The joint solution enables organizations to identify email for compliance policy enforcement; apply multiple email governance policies; monitor and report on email traffic; and ensure the secure exchange of sensitive and confidential information.

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	Windows Server 2008 x64 and above

Email Security Virtual Appliance	
Hypervisor	ESXi™ and ESX™ (version 5.0 and newer)

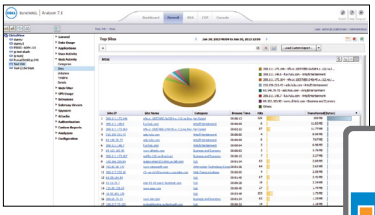


Dell SonicWALL policy management and reporting solutions

Dell SonicWALL Global Management System

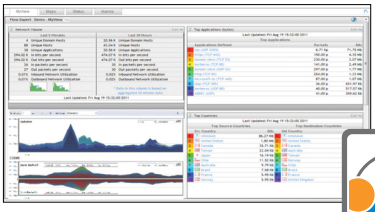
The Global Management System (GMS) provides organizations, distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy Dell SonicWALL firewall, anti-spam, and secure remote access solutions. Flexible deployment options include software, 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.

Network Security and Secure Mobile Access

Dell 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 signatures and dynamic updates that defeat the latest threats. Patented* Reassembly-Free Deep Packet Inspection technology, combined with multi-core parallel architecture, enables simultaneous full stack 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 secure mobile access 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, and SC Magazine for easy to use, high quality, and high performance appliances and services. Gartner named Dell SonicWALL in the Leaders Quadrant in their 2013 Unified Threat Management Magic Quadrant. In both the NSS Labs 2013 Next-Generation Firewall and Intrusion Prevention System 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 mobile 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.

Brochure-SonicWALL-ProductLines-US-KS-25046