Features

Intrusion prevention	
Feature	Description
Signature-based scanning	Tightly integrated, signature-based intrusion prevention scans packet payloads for vulnerabilities and exploits that target critical internal systems.
Automatic signature updates	Dell SonicWALL's Research Team continuously updates and deploys an extensive list of over 5,400 IPS signatures covering 52 attack categories. These signatures take immediate effect and do not require reboots or any other interruption in service.
Outbound threat prevention	The ability to inspect both inbound and outbound traffic ensures that the network will not unwittingly be used in Distributed Denial of Service attacks and will prevent any Command and Control Botnet communication.
Intra-zone IPS protection	Intrusion prevention can be deployed between internal security zones to protect sensitive servers and to prevent internal attacks.
VPN	
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the firewall to connect remote branch offices to a central location.
SSL VPN or IPSec client remote access	Utilize clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure by seamlessly re-routing traffic between endpoints through alternate routes.
Clean VPN	Dell SonicWALL Clean VPN™ both secures the integrity of VPN access and decontaminates malicious threats before they can enter the corporate network.
Gateway threat prevention	
Gateway anti-malware	Dell SonicWALL's patented RFDPI engine scans all ports and protocols for viruses without file size or stream length limitation. SonicLabs Researchers constantly provide updated threat protection, providing faster response times and threat prevention.
Reassembly-Free Deep Packet (RFDPI)	Reassembly-Free Deep Packet Inspection keeps track of malware regardless of the order or inspection timingwith which the packets arrive. This allows for extremely low latency while eliminating file and stream size limitations. This provides greater performance and security than outdated proxy designs which reassemble contents using sockets bolted to traditional anti-virus programs and are plagued with inefficiencies and the overhead of memory thrashing leading to high latency, low performance and size limitations.
Cloud anti-virus	Using the built-in RFDI engine, Dell SonicWALL can leverage the power of the cloud to provide the most comprehensive set of anti-malware signatures available, while minimizing latency or delay. The Dell SonicWALL Cloud Anti-Virus Service provides millions of additional malware signatures for inspection of executable files using the most up-to-date information available.
Bi-directional Inspection	RFDPI can be performed on both inbound and outbound connections to provide protection in all networktraffic directions.
24x7 signature updates	SonicLabs Research Team team creates and updates signature databases that are propagated automatically to the firewalls in the field, with those signatures taking immediate effect without any reboot or service interruption required.
Firewall and networking	
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DOS attack protection	SYN Flood protection provides defense against DOS attacks using both layer 3 SYN proxy and layer 2 SYN blacklisting technologies.
Flexible deployment	Can be deployed in traditional NAT and Layer 2 Bridge modes.
Policy-based routing	Create routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail backto a secondary WAN in the event of an outage.
High availability	Supports Active/Passive failover to ensure increased reliability by protecting against hardware or software faults.
WAN load balancing	Load balance up to four WAN interfaces using Round Robin, Spillover or Percentage based methods.
WAN acceleration	WAN Acceleration decreases latency and increases transfer speeds between remote sites for even higher network efficiency gains.