SSL Inspection

High-performance protection for SSL-encrypted threats

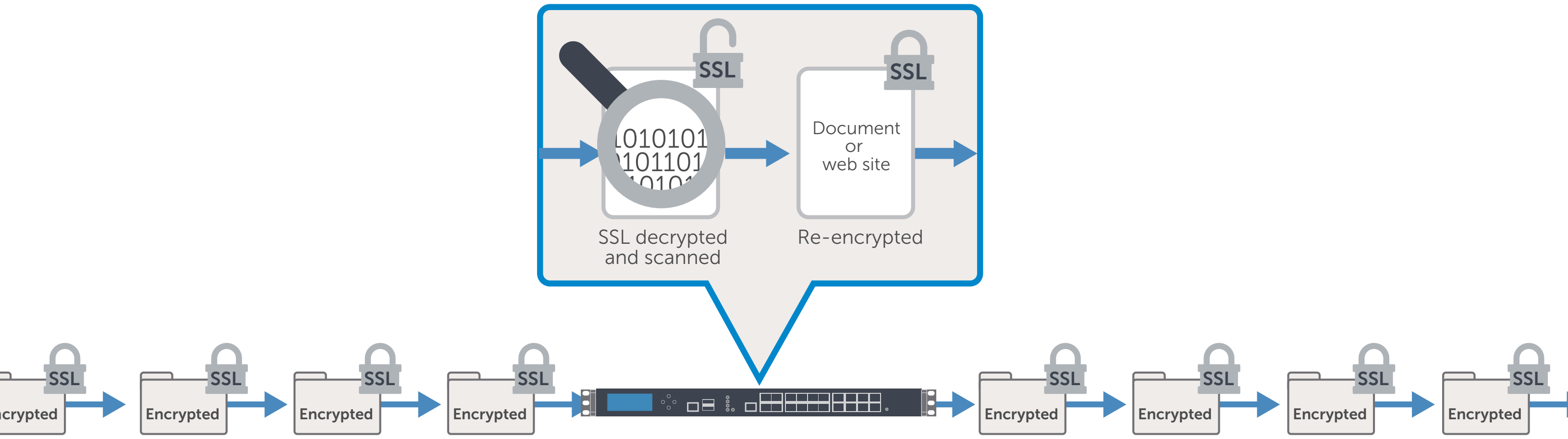
Today, more enterprise traffic is secured using the Secure Sockets Layer (SSL) protocol — up to 35 percent, according to industry analysts, and even more in some vertical industries. Cybercriminals know this, which is why they have begun to use SSL to hide their attacks. Not only are they bypassing firewalls and capitalizing on blind spots to sneak in malware that opens doors directly into corporate networks, they are also using SSL to hide command and control traffic so they can manipulate compromised systems from virtually anywhere.

Organizations can safeguard their networks from these tactics with Dell SonicWALL SSL Inspection, an add-on service to Dell SonicWALL Network Security Appliance (NSA) and SuperMassive Series next-generation firewall appliances. SSL Inspection provides advanced protection against SSL threats. Dell's patented Reassembly-Free Deep Packet Inspection® engine, a full-stack stream inspection technology scans SSL-encrypted traffic — including HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS, and POPS — and regardless of the port being used. The service decrypts SSL traffic, inspects it for threats and then re-encrypts it, sending it along to its destination if no threats or vulnerabilities are found. It is an invaluable service for providing critical security and application control, and for preventing data leakage.

This service provides critical security, application control and data leakage prevention for analyzing HTTPS and other SSL-encrypted traffic.

Benefits:

- Gain peace of mind with advanced SSL threat protection
- Simplify SSL security with easy set-up and automated scanning and threat identification
- Customize your security needs with inclusion and exclusion lists
- Avoid costly attacks and security incidents with a service designed to help you maximize protection from your Dell SonicWALL next-generation firewall



System requirements

SSL Inspection is available for all Network Security Appliance and SuperMassive Series appliances. It is not supported on the TZ Series.

SSL Inspection is available with the following Dell SonicWALL firewalls:

- NSA 220 / NSA 220W
- NSA 250M / NSA 250MW
- NSA 2600
- NSA 3600
- NSA 4600
- NSA 5600
- NSA 6600
- SuperMassive 9200
- SuperMassive 9400
- SuperMassive 9600
- SuperMassive E10200
- SuperMassive E10400
- SuperMassive E10800

Features

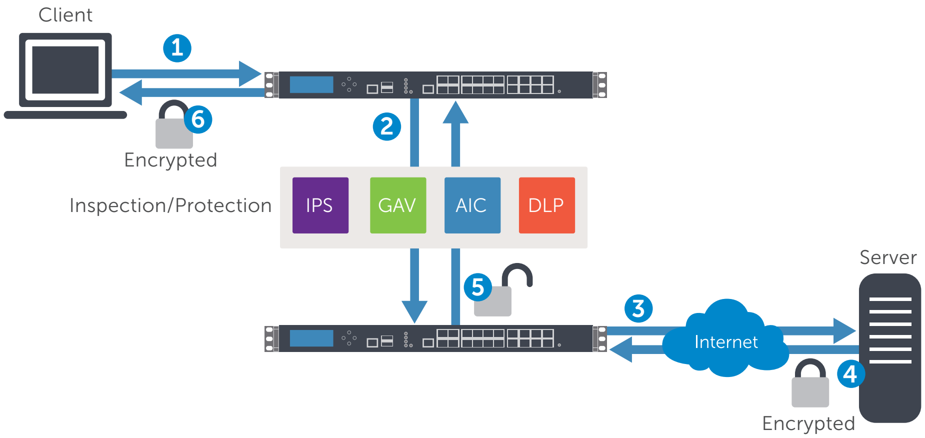
Secure and simple setup—Dell SSL Decryption and Inspection service protects users on the network with minimal configuration and complexity.

Inclusion/exclusion list—For high-traffic deployments, administrators can exclude trusted sources to maximize network performance. Additionally, administrators can target specific traffic for SSL inspection by customizing a list that specifies address, service or user objects or groups.

Client deployment mode—Inspects SSL traffic when the client is on the firewall's LAN and accesses content located on the WAN. After the appliance has decrypted and inspected the SSL-encrypted traffic, it re-writes the certificate sent by the remote server and signs the newly-generated certificate with the user-specified certificate. By default, this is the appliance certificate authority (CA), although a different certificate can be selected.

Server deployment mode—Inspects SSL traffic when remote clients connect over the WAN to access content located on the firewall's LAN, allowing the administrator to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client. In this scenario, the owner of the Dell SonicWALL next-generation firewall owns the certificates and private keys of the origin content servers.

Comprehensive support—Support includes intrusion prevention, malware prevention, application control, content/URL filtering, and preventing malware command and control communication.



SSL Inspection – Client Deployment Mode

1 Client initiates SSL handshake with server

2 NGFW intercepts request and establishes session using its own certificates in place of server

3 NGFW initiates SSL handshake with server on behalf of client using admin defined SSL certificate

4 Server completes handshake and builds a secure tunnel between itself and NGFW

5 NGFW decrypts and inspect all traffic coming from or going to client for threats and policy violations

6 NGFW re-encrypts traffic and sends along to client

System requirements

SSL Inspection is available with the following Dell SonicWALL next-generation firewalls:

	One-Time License
NSA 220 / NSA 220W	01-SSC-8933
NSA 250M / NSA 250MW	01-SSC-8933
NSA 2600	01-SSC-8933
NSA 3600	01-SSC-8934
NSA 4600	01-SSC-8934
NSA 5600	01-SSC-8680
NSA 6600	01-SSC-8680
SuperMassive 9200	Included with Security Services Subscription
SuperMassive 9400	Included with Security Services Subscription
SuperMassive 9600	Included with Security Services Subscription
SuperMassive E10200	Included with Security Services Subscription
SuperMassive E10400	Included with Security Services Subscription
SuperMassive E10800	Included with Security Services Subscription

SSL Inspection is also available for the following Dell SonicWALL Next-Generation Firewalls:

- NSA 240
- NSA 2400
- NSA 2400MX
- NSA 3500
- NSA 4500
- NSA 5000
- NSA E5500
- NSA E6500
- NSA E7500
- NSA E8500
- NSA E8510

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

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information about Dell Connected Security, please visit Software.Dell.com/solutions/security

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.