DECRYPTION AND INSPECTION OF ENCRYPTED TRAFFIC

High-performance protection from malicious use of encryption

According to the 2018 SonicWall Threat Report, encrypted traffic now accounts for almost seventy percent of an organization's total web communication. Although there are many benefits to encrypting internet sessions such as protecting the privacy and integrity of personal information for data exchange, we are also seeing a less positive trend emerge as malware writers exploit this encryption capability as a way of hiding their attacks from firewalls. Not only can attackers bypass firewalls and capitalize on blind spots to sneak in malware that opens doors directly into any network, they are also using TLS/SSL to hide command and control traffic to manipulate compromised systems from virtually anywhere. Organizations not inspecting encrypted traffic are missing a lot of the value of their firewall systems. They are unable to view what is inside that traffic, spot malware downloads, identify harmful files or see unauthorized transmission of privileged information to external systems.

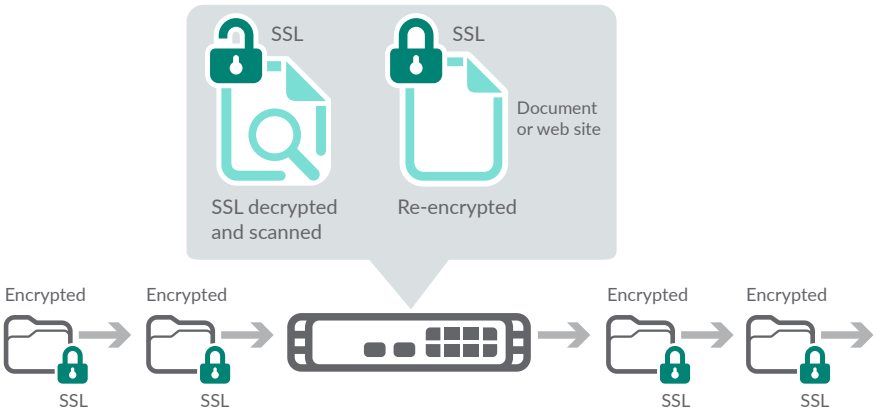
Organizations can safeguard their networks from these security risks with SonicWall Deep Packet Inspection of SSL (DPI-SSL), an add-on service that is available on all SonicWall Next-Generation Firewall (NGFW) and Unified Threat Management (UTM) network security appliances. DPI-SSL provides advanced protection against encrypted threats using SonicWall's patented Reassembly-Free Deep Packet Inspection engine, a full-stack stream inspection technology that scans a broad array of encryption protocols — including HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS, and POPS, regardless of the port being used.

The service decrypts TLS/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 also for preventing data leakage.

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

Benefits:

- Gain visibility into TLS/SSL encrypted traffic
- Block hidden malware downloads
- Thwart C&C communication and data exfiltration
- Customize inclusion and exclusion lists for compliance or legal requirements



System requirements

SSL Inspection is available with the following SonicWall firewalls:
SOHO / SOHO W
TZ300 / TZ300 W
TZ400 / TZ400 W
TZ500 / TZ500 W
TZ600
NSa 2650
NSa 3650
NSa 4650
NSa 5650
NSA 6600
SuperMassive 9200
SuperMassive 9400
SuperMassive 9600
SuperMassive 9800

Features

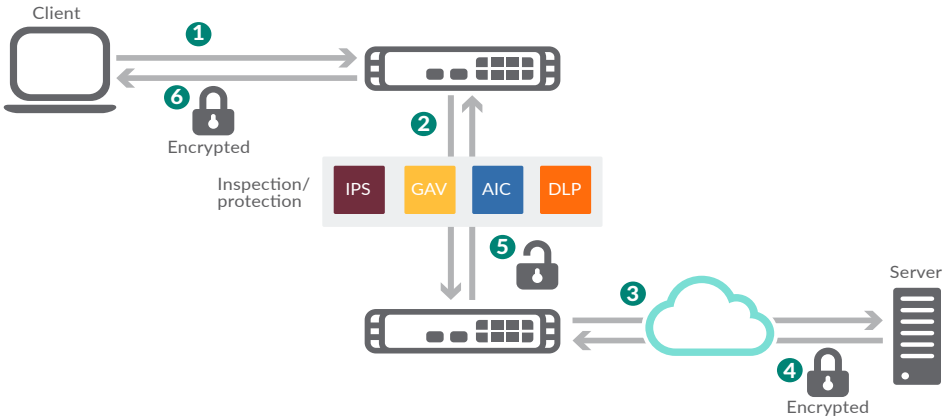
Secure and simple setup — DPI-SSL decryption and inspection service protects users on the network with minimal configuration and complexity.

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

Client deployment mode — Inspects TLS/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 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 TLS/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 TLS/SSL connections to the address object, it presents the paired certificate and negotiates TLS/SSL with the connecting client. In this scenario, the owner of the 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 prevention of malware command and control communication.



TLS/SSL Inspection — Client Deployment Mode

1. Client initiates TLS/SSL handshake with server
2. NGFW intercepts request and establishes session using its own certificates in place of server
3. NGFW initiates TLS/SSL handshake with server on behalf of client using admin defined TLS/SSL certificate
4. Server completes handshake and builds a secure tunnel between itself and NGFW
5. NGFW re-encrypts traffic and sends along to client
6. NGFW decrypts and inspect all traffic coming from or going to client for threats and policy violations

System requirements

TLS/SSL Inspection is available with the following SonicWall next-generation firewalls:

FIREWALL	ONE-TIME LICENSE
SOHO / SOHO W	01-SSC-0723
TZ300 / TZ300 W	Included with Security Services Subscription
TZ400 / TZ400 W	Included with Security Services Subscription
TZ500 / TZ500 W	Included with Security Services Subscription
TZ600	Included with Security Services Subscription
NSa 2650	Included with Security Services Subscription
NSa 3650	Included with Security Services Subscription
NSa 4650	Included with Security Services Subscription
NSa 5650	Included with Security Services Subscription
NSA 6600	Included with Security Services Subscription
SuperMassive 9200	Included with Security Services Subscription
SuperMassive 9400	Included with Security Services Subscription
SuperMassive 9600	Included with Security Services Subscription
SuperMassive 9800	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

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear..

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

DataSheet-DecryptionAndInspection-US-VG-MKTG1925

SONICWALL®