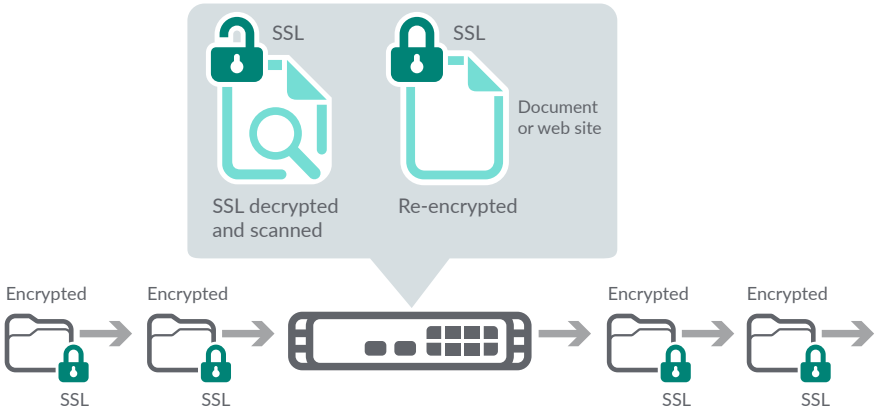
SONICWALL

Decryption and inspection of encrypted traffic

According to the 2018 SonicWall Cyber 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 through a combination of cloud-based and on-box threat prevention technologies. Enhancing SonicWall's multi-engine Capture Advanced Threat Protection (ATP) service is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. In combination, SonicWall's patented* single-pass Reassembly-Free Deep Packet Inspection (RFDPI) engine examines every byte of every packet, inspecting both inbound and outbound traffic on the firewall. As an additional layer or protection, SonicWall Deep Packet Inspection of



DPI-SSL 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
- Get cutting-edge threat prevention with Real-Time Deep Memory Inspection and Reassembly-Free Deep Packet Inspection technologies
- Block hidden malware downloads
- Thwart C&C communication and data exfiltration
- Customize inclusion and exclusion lists for compliance or legal requirements

TLS/SSL (DPI-SSL), provides advanced protection against encrypted threats using SonicWall's patented Reassembly-Free Deep Packet Inspection engine which scans a broad array of encryption protocols — including HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS, and POPS, regardless of the port being used.

DPI-SSL 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 invaluable for providing critical security and application control and also for preventing data leakage.

Features

High performance and connection count — SonicWall next-generation firewalls leverage an advanced processor architecture and a very high number of connections to enhance DPI-SSL performance and protection across all connected devices.

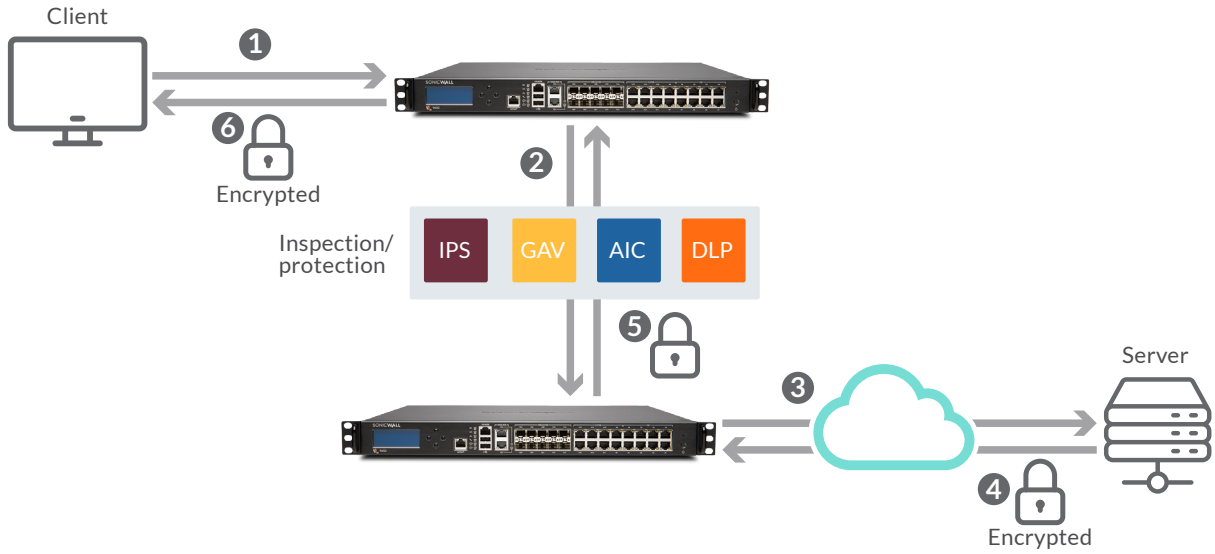
Secure and simple setup — DPI-SSL decryption and inspection protects users on the network with minimal configuration and complexity.

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
SOHO 250 / SOHO 250 W	Included with Security Services Subscription
TZ300 / TZ300 W / TZ300P	Included with Security Services Subscription
TZ350 / TZ350 W	Included with Security Services Subscription
TZ400 / TZ400 W	Included with Security Services Subscription
TZ500 / TZ500 W	Included with Security Services Subscription
TZ600 / TZ600P	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 6650	Included with Security Services Subscription
NSa 9250	Included with Security Services Subscription
NSa 9450	Included with Security Services Subscription
NSa 9650	Included with Security Services Subscription
SuperMassive 9800	Included with Security Services Subscription
NSsp 12400	Included with Security Services Subscription
NSsp 12800	Included with Security Services Subscription
NSv 10	Included with Security Services Subscription
NSv 25	Included with Security Services Subscription
NSv 50	Included with Security Services Subscription
NSv 100	Included with Security Services Subscription
NSv 200	Included with Security Services Subscription
NSv 300	Included with Security Services Subscription
NSv 400	Included with Security Services Subscription
NSv 800	Included with Security Services Subscription
NSv 1600	Included with Security Services Subscription

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

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

DataSheet-DecryptionAndInspection-US-KJ-MKTG5190