SONICWALL

# SOLUTION BRIEF: BEST PRACTICES FOR STOPPING ENCRYPTED THREATS

**Safeguard your network from cybercriminals who use SSL/TLS**


## Abstract

Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, or HTTPS traffic, has become a ubiquitous means of securing sensitive data in flight over the Internet. The question is, how can you keep the integrity and privacy of SSL communication intact while ensuring security of the network and the data that's being exchanged? This brief examines considerations and presents best practices for protecting against encrypted threats.


### Introduction

The key is to decrypt encrypted traffic entering your network in order to allow your network security firewall to scan the traffic and identify hidden threats. To do so, today's firewalls apply deep packet inspection of secure socket layer (DPI SSL) technology.

However, even firewall vendors that claim to offer SSL decryption and inspection may not have the processing power to handle the level of SSL traffic moving across a network today. When considering a DPI SSL solution, it is advisable to conduct a proof-of-concept trial.

The best solution utilizes full-stack inspection engine technology to scan SSL-encrypted traffic for threats and then send the traffic along to its destination if no threats or vulnerabilities are found. It is also important to have a secure and simple setup that minimizes configuration overhead and complexity.

### Deployment considerations

For high-traffic deployments, it is necessary to exclude trusted sources in order to maximize network performance. Additionally,

With the right firewall combination, you can recover the lost performance of inspecting SSL on existing or standalone firewalls and scale DPI-SSL up to 80 Gbps.

you want the capability to target specific traffic for SSL inspection by customizing a list that specifies address as well as either service or user objects or groups.

It's also crucial to inspect SSL traffic, whether it is coming from behind the firewall's LAN to access content on the WAN or vice versa. This level of inspection protects all users on the LAN from dangerous intrusion, viruses, Trojans and other network attacks hidden by encryption. It also protects all users on the WAN — including remote clients — from hidden encrypted attacks as well.

Another consideration is a firewall security hardware solution that can scale affordably to provide server-side and client-side DPI-SSL, without compromising security effectiveness. The answer is a "firewall sandwich."

A firewall sandwich is a configuration based on next-generation firewalls (NGFWs) that can scale up with inbound and outbound DPI-SSL. The firewall sandwich is highly effective because it scales out in a linear fashion. It contains network-based architecture that relies on NGFWs in a single layer instead of additional appliances for content filtering or SSL decryption. This approach adds protection without hampering throughput and avoids the poor scalability and costs of chasing the next big chassis.

Note that firewalls used for this approach must be engineered with multicore processors to scale when run in parallel with one another. Many NGFW brands may not scale in a linear fashion, which can lead to performance degradation if one component in this configuration maxes out. With the right firewall combination, you can recover the lost performance of inspecting SSL on existing or standalone firewalls and scale DPI-SSL up to 80 Gbps.

### Best practices for protection

The good news is that there are ways to enjoy the security benefits of SSL/TLS encryption without providing a tunnel for attackers:

1. If you haven't conducted a security audit recently, undertake a comprehensive risk analysis to identify your risks and needs.
2. Upgrade to a capable, extensible NGFW with an integrated IPS and SSL-inspection design that can scale performance to support future growth.
3. Update your security policies to defend against a broader field array of threat vectors and establish multiple security defense methods to respond to both HTTP and HTTPS attacks.
4. Continually train your staff to be aware of the danger of social media, suspicious social engineering websites and downloads, and various spam and phishing scams.
5. Inform users never to accept a self-signed, non-valid certificate.
6. Make sure all your software is up-to-date. This will help protect you from older SSL exploits that have already been neutralized.

## Conclusion

There are effective ways to retain the integrity and privacy of SSL communication while securing the network and the data being exchanged. Learn more about how SonicWALL can help your organization stop hidden threats at www.sonicwall.com/solutions/security-solutions.

## About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
**www.sonicwall.com**