SONICWALL®

DEFEATING ENCRYPTED THREATS

State of encrypted traffic

Hackers have expanded their craft to use SSL traffic to obfuscate their attacks and malware from security systems.

97% of surveyed enterprises are seeing an increase in encrypted web traffic[1]

130% increase in threats using TLS/SSL connections in 2016 over 2014[1]

41% of malware is hidden in SSL traffic[2]

80% of those surveyed were victims of a cyber attack[2]

[1]*Research Study, NSS Labs, June 2016*
[2]*Research Study, Ponemon Study 2016*

Understanding the malicious use of encryption

Page Visit: User machine (victim A) visits a compromised good site.

Exploit Kit Execution: As the web content is served to the client, a small piece of software is downloaded to the user's device where a sequence of commands is executed to exploit software vulnerabilities on the client machine.

Malware Request: Once the exploit kit operator gets control of that machine, a request command is made to a malware hosting website that delivers the malware.

Malware Infection: Victim A now has malware installed.

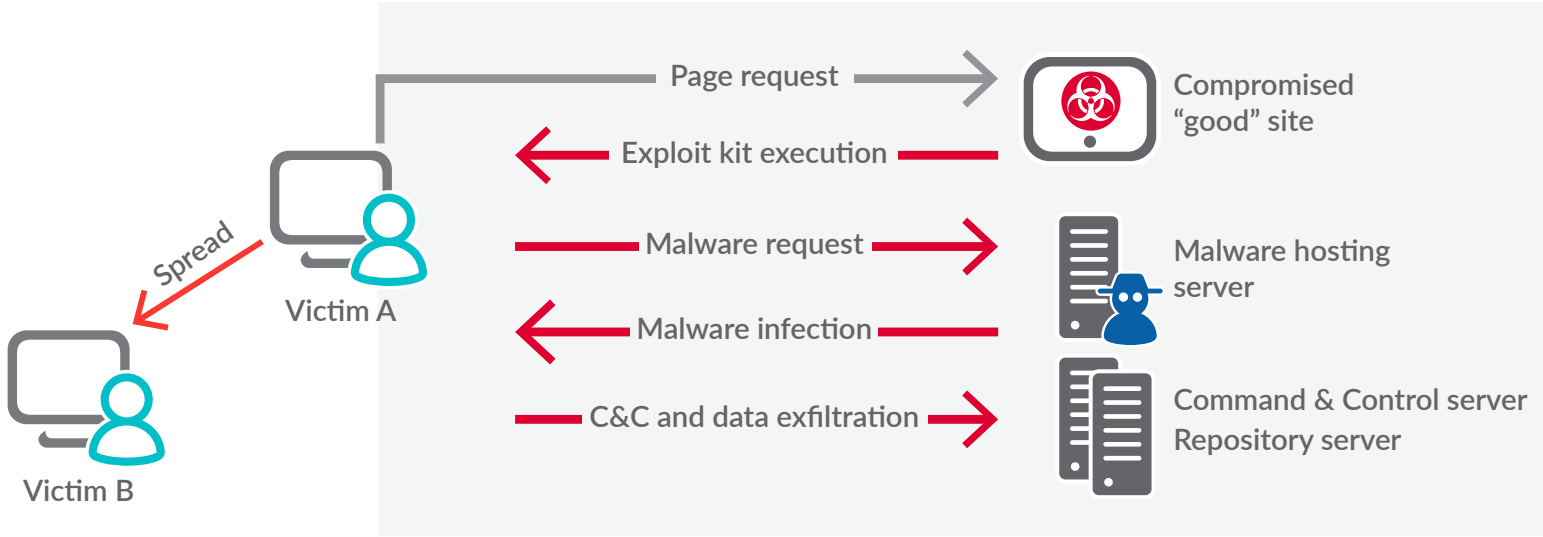
C&C: The malware communicates back to a Command and Control infrastructure for more instructions.

Data Exfiltration: Data from Victim A's machine is copied to an external server for processing.

Victim B: Attackers often elevate their access rights at this stage allowing them to move laterally within the network and infect other endpoints.

Encryption: The new reality is that encryption can be implemented at any phase of this attack to evade detection.

Encryption can be implemented at any phase of an attack



SONICWALL®

The challenges of encrypted traffic

Three common barriers for not inspecting SSL traffic

Lack of enabling security tools

Insufficient resources

Performance degradation

Source: Research Study, Ponemon Study 2016

SONICWALL®

Performance impact is a big concern

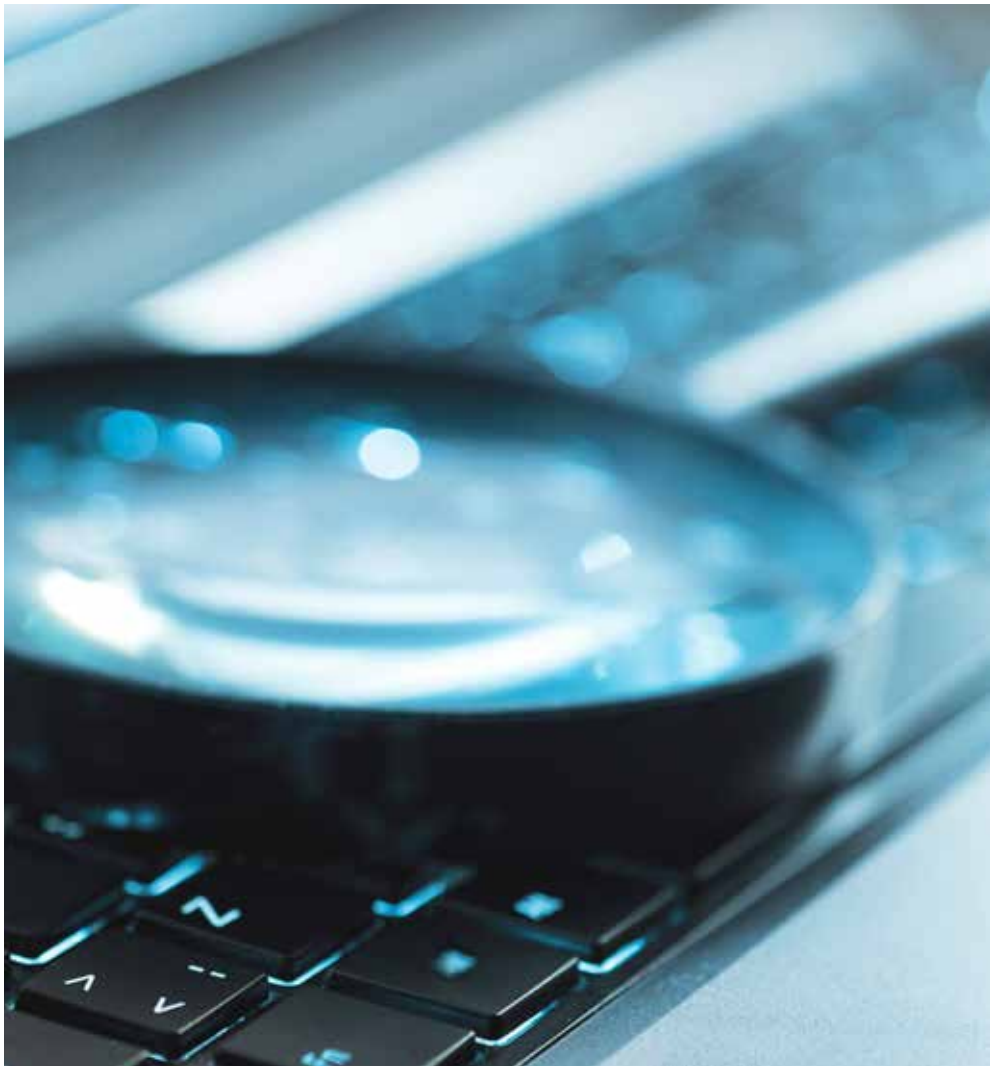
- Performance penalty on a security system when SSL inspection is active can be as high as **81%**[1]
- **61%** say lack of performance is a concern for organizations that don't decrypt SSL traffic[2]
- **83%** say decryption results in some type of degradation within organizations currently decrypting and inspecting SSL traffic[2]

[1]*Source: SSL Performance Problems NSS Labs, June 2013*
[2]*Source: Research Study, Ponemon Study 2016*

Ask tough questions

3 tough questions you MUST ask about SSL encrypted traffic

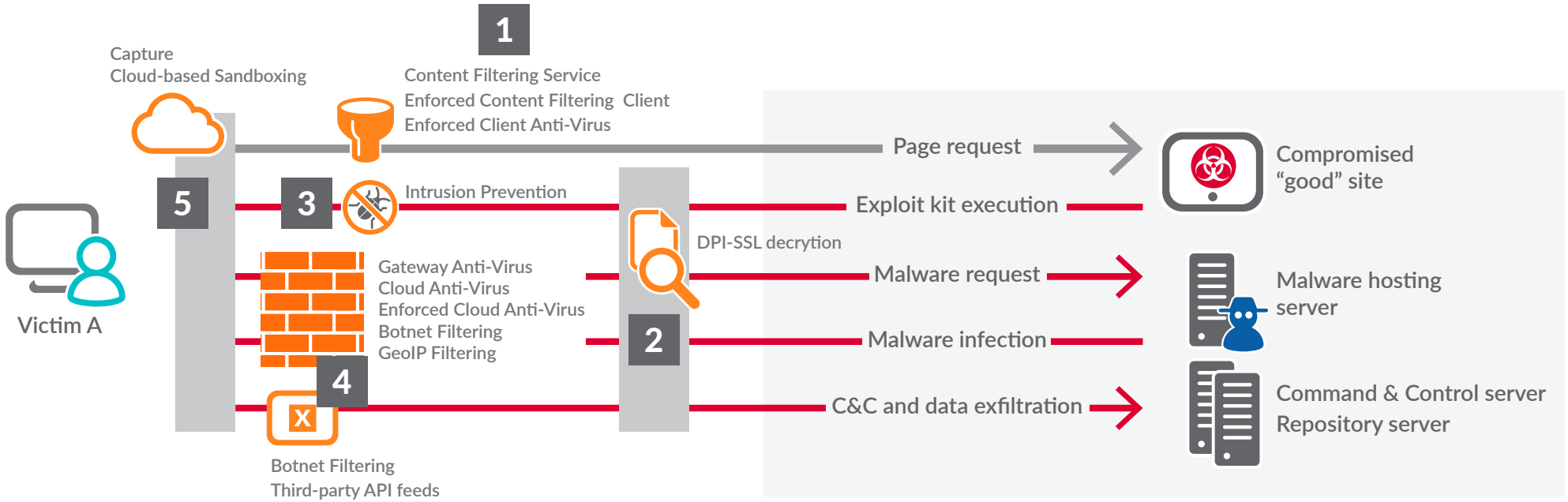
- Do you know whether or not your organization's firewall is inspecting HTTPS traffic?
- Has your organization experienced frequent network service disruptions or downtime as a result of a total collapse of your firewall performance when inspecting HTTPS traffic?
- How are you scaling firewall protection to prevent performance degradation, lag and latency of your network when inspecting HTTPS traffic?




The SonicWall solution

The SonicWall solution:
Breaking the malware cycle operating inside encrypted traffic

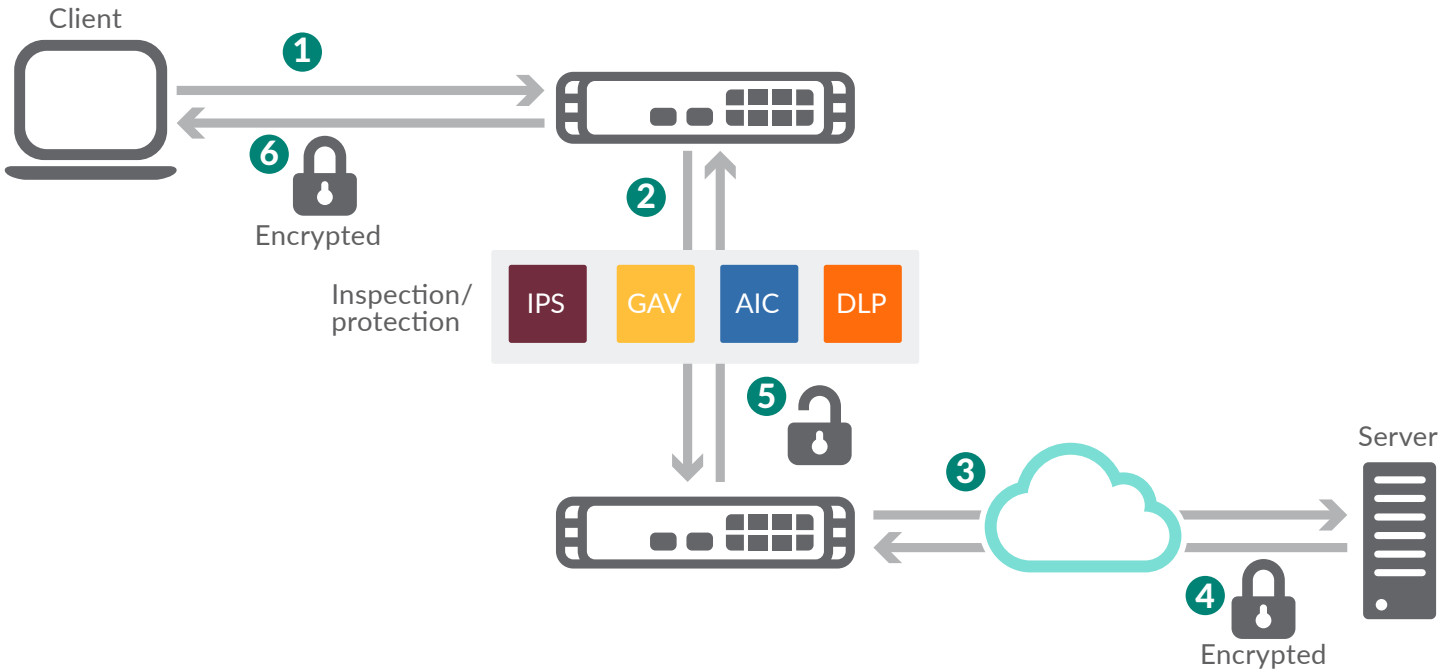
1. SonicWall protects endpoint systems inside or outside the firewall perimeter from visiting inappropriate, illegal and malicious URLs with the firewall's Web Content Filtering and Enforced Content Filtering Client.
2. The unique SonicWall Deep Packet Inspection of SSL (DPI-SSL) technology decrypts encrypted internet traffic between clients and web servers.
3. The SonicWall Intrusion Prevention Service scans the unencrypted traffic to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits.
4. SonicWall threat prevention security services, including Gateway Anti-Virus, Cloud Anti-Virus, Botnet and GeoIP Filtering and third-party threat information, further break the malware infection cycle.
5. SonicWall Capture ATP, a multi-engine sandbox platform, executes and examines suspicious files to discover and stop zero-day threats.



SONICWALL®

The SonicWall Solution:
How DPI-SSL decrypts and inspects encrypted traffic

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



SONICWALL®

The customer outcomes

- Gain visibility into SSL/TLS encrypted traffic
- Block malware downloads hiding inside encrypted traffic
- Thwart command and control communications and data exfiltration
- Enhance security, application control and data leak prevention capabilities
- Maintain highest level of network and resource quality of service and availability as the system load increases without performance problems

Learn more. Visit www.sonicwall.com/encrypted-threats.

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 global businesses in over 150 countries, so you can do more business with less fear.

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