SONICWALL

EXECUTIVE BRIEF: THE DARK SIDE OF ENCRYPTION

Why your network security needs to decrypt traffic to stop hidden threats

Abstract

Most of your users' web sessions are likely now encrypted with Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, or HTTPS. This is because there is a huge trend in the industry today that wants to move towards an all-encrypted Internet to achieve two key objectives:

- Make it more difficult for cyber-criminals to eavesdrop on web connections
- Keep personal information secure and private

As the good guys increase their use of encryption protocol, encryption has become a favorite threat vector for hackers to mask their attacks, evade defense systems and ultimately open backdoors directly into your network. After all, your security controls cannot stop what they cannot see. If left untreated, any attacks utilizing SSL/TLS will have a 100 percent success rate in compromising your network, leading to loss of classified data, IP and reputation.

Encryption is everywhere

SSL/TLS is commonly used for everything from e-commerce to online banking. SSL/TLS secures a growing amount of enterprise traffic and makes up the majority of network traffic in some verticals. SSL protects data-in-motion by creating an encrypted channel over the public Internet or private networks, which keeps data from being captured or compromised.

In addition, SSL verifies that the data's final destination is not with a hacker spoofing a trusted destination. Crucial and sensitive data such as credit card information, user names and passwords are transported in a way that makes it difficult for anyone but the intended recipient to access that data. While websites and FTP and telnet servers were the original users of

Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic or their performance is so low that they become unusable when conducting the inspection.

SSL, today a wide variety of applications use the protocol, including Java-based applications, application management services and cloud-based services. Facebook and Twitter are two of the most popular SSL-enabled applications. Browser add-ons that can force the use of SSL via HTTPS are also available.

In the fourth quarter of 2015, HTTPS connections (SSL/TLS) made up an average of 64.6 percent of web connections, outpacing the growth of HTTP throughout most of the year. In January 2015, HTTPS connections were 109 percent higher than in January 2014. Furthermore, each month of 2015 saw an average of a 53 percent increase over the corresponding month in 2014.

Firewalls can be challenged when inspecting encrypted traffic

Using SSL/TLS, skilled attackers can cipher command and control communications and malicious code to evade intrusion prevention systems (IPS) and anti-malware inspection systems. These attacks can be extremely effective, simply because most organizations do not have the right infrastructure to detect them. Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic or their performance is so low that they become unusable when conducting the inspection. HTTPS traffic inspection by a next-generation firewall (NGFW) requires six additional compute processes compared to plain-text traffic inspection.

The two processes that affect performance most are:

- Establishing a secure connection
- Decrypting and re-encrypting the traffic for a secured data exchange

The performance penalty can be high in some cases, effectively prohibiting SSL/TLS inspection for companies operating on legacy security systems.

A majority of cyberattacks are opportunistic and most are financially motivated. This means that all organizations are at risk of becoming compromised.

What this can mean to your organization

Throughout this year, attackers have taken full advantage of the growth of HTTPS traffic and the lack of visibility. One attack leveraged an advertisement on Yahoo in precisely this way, exposing as many as 900 million users to malware. This campaign redirected Yahoo visitors to a site that was infected by the Angler exploit kit. An additional 10 million users were likely affected in the weeks prior by accessing ads placed by a marketing company called "E-planning."

Conclusion

Encryption is everywhere and is now a favorite threat vector for hackers. Your network security needs to decrypt traffic to stop hidden threats.

Learn more. Read our solution brief, "Best practices for stopping 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