THE RAPID GROWTH OF SSL ENCRYPTION

The Dark Side of SSL That Today's Enterprise Can't Ignore

SSL ENCRYPTION: GROWING IN LEAPS AND BOUNDS

We're in the midst of a transition that is often referred to as "always-on SSL." Secure Sockets Layer (SSL)—or more specifically Transport Layer Security (TLS), the successor of SSL—is now a requisite for anyone wishing to transmit email and data over the Internet safely and securely.

A sharp increase in SSL traffic occurred in 2015, as organizations moved to encrypt—and thus protect—their Internet traffic. Though reports vary, between 35 and 50 percent of traffic is now encrypted, and that number continues to rise.[1] Indeed, with 20 percent year-over-year growth, SSL encrypted traffic is predicted to increase to 75 percent by 2019.[2] This makes a lot of sense, considering that 97 percent of organizations reported an increase in encrypted traffic over the past year.[3]

There are a number of factors behind this rapid growth:

1. Websites. Another factor driving SSL encryption are websites, which are increasingly implementing HTTPS by default. Over 40 percent of the most popular websites today have implemented SSL encryption,[4] though only about 25 percent of the top 100 websites use HTTPS; the remainder still employ HTTP. As these additional top-traffic sites adopt HTTPS, the overall percentage of SSL traffic will concurrently increase.[5]

So why are websites opting to use HTTPS? Using HTTPS active by default, websites can protect sensitive information sent over the Internet that is passed from computer to computer to get to the destination. Without SSL encryption (viz., those using HTTP), any computer or server between the user and the server can see confidential data such as

ENCRYPTION CATEGORIES

Encryption is applied to data that is *at rest*, such as databases, desktops and laptops, mobile devices, and servers. It also is used for data *in motion*, such as that moving across virtual private networks, and communications between browsers and web servers. SSL encryption refers to *encrypted web communications*—network traffic such as email and web applications, among others, using HTTPS.

credit card numbers, usernames, passwords, and other private information. Further, the entire URL and page content are visible to anyone on the network between the user and the website, revealing everything from every page visited on that site, any search terms, and what content is being read or watched. Websites that use SSL ensure that those communications are only read by the server to which the information is being sent.

2. Cloud Adoption. Cloud adoption is another reason for the increase, with 85 percent of enterprises reporting they have multi-cloud strategies.[6] Yet, the cloud still comprises less than 15 percent of total IT spend. What this means is that the majority of cloud adoption is still ahead of us. The global cloud market is growing at an annual rate of 22 percent, topping $146 billion this year,[7] and it is forecast to exceed 50 percent of IT budgets by 2019.[8]

Regardless of the cloud model, service delivery modes vary, with most enterprises embracing a wide range of services: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). A new wave of adoption is certainly on the way: by 2020, 92 percent of workloads will be processed in the cloud versus 8 percent by traditional data centers.[9]

In particular, as many SaaS applications such as Salesforce, Dropbox, and Microsoft Office 365 embrace the need to protect customer data by enabling SSL encryption on their platforms, the cloud has become a significant factor in SSL traffic growth. SaaS providers relying on SSL encryption do so to protect customer data while it is in transit to and from the cloud.

3. Compliance. Organizations across various industry segments are required to use SSL encryption on certain types of sensitive data that is in transit in order to remain in compliance with regulations such as PCI DSS (Payment Card Industry Data Security Standard) and HIPAA (Health Information Portability and Accountability Act). Regardless of the communications method (email, websites, SaaS applications, etc.), SSL encryption is a requirement when data that is transmitted falls underneath these regulations.

4. Internet of Things (IoT). IoT is quickly becoming a huge opportunity as well as a challenge for enterprises. Many industry segments are seeing the number of IoT devices connected to the network grow 50 percent annually. Growth forecasts are gigantic. For example, IHS predicts the IoT market will double to 30.7 billion devices by 2020. This will more than double in another five years to 75.4 billion in 2025![10] Revenue forecasts are comparable; IoT devices will generate $300 billion by 2020, with a global economic impact of $1.9 trillion.[11]

IoT devices are proving to be transformative in certain industry segments. In healthcare, IoT devices enable doctors and caregivers to deliver better patient care while improving efficiencies. Doctors can maintain real-time monitoring of patients when they are discharged to home. Transportation and distribution is another industry segment where IoT is making a big difference. Shipping companies can track everything from vehicle fuel and consumption to monitoring and control shipping containers.

As organizations increasingly recognize the threat that IoT devices present, they elect to activate SSL encryption on them. Yet, just as SSL-enabled applications are increasing SSL traffic, so does the growth in IoT devices.

5. Email. When Google started flagging unencrypted emails to Gmail users last year, the number of inbound emails using SSL encryption spiked 25 percent.[12] Protecting sensitive information in email—both content, attachments, and links—is one of the top use cases. This enables organizations to prevent eavesdropping (everything is encrypted), message modifications (uses message digests), message replay (timestamps included on signatures), repudiation (signatures enable proof of who sent a message), and unprotected backups (everything is always encrypted).

TOP REASONS FOR INCREASED INBOUND SSL ENCRYPTION[13]

- IoT/Connected Devices, 32%
- SaaS Applications, 29%
- Managed Services Partners Connections, 28%
- Webmail and Social Media, 27%
- Custom Web Applications, 25%

GROWTH IN INBOUND AND OUTBOUND ENCRYPTED TRAFFIC[14]

Outbound Traffic

- Will Increase, 85%
- Will Remain Flat or Decrease, 15%

Inbound Traffic

- Will Increase, 79%
- Will Remain Flat or Decrease, 21%

The percentage of Internet traffic that is encrypted is growing at a **20 percent** annual rate.[15]

HTTPS

The number of websites using HTTPS (SSL encryption) **nearly doubled** from 2015 to 2016.[16]

THE “DARK SIDE” OF SSL ENCRYPTION

Despite the list of benefits associated with SSL encryption, there is a dark side. Just as confidential communications using email, websites, SaaS applications, and custom applications are protected with SSL encryption, cybercriminals also use it to hide malware and ransomware embedded in applications and links that enable them to infiltrate company networks. In doing so, these bad actors are able to communicate with command and control systems.

The biggest challenge is that traditional cybersecurity solutions such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) are trained to trust encrypted traffic. So, what is the result? Ninety percent of CIOs indicate they have experienced or experience a network attack using SSL encryption, and 87 percent say their security defenses are less effective today due to cybercriminals using encryption to hide their attacks.[17]

The following are some of the more prevalent ways that cybercriminals use SSL encryption:

1. **Hiding the Initial Infection.** Cybercriminals encrypt their malware and send it through an approved port; users click on embedded links that take them to sites containing the payload or as an attached file.
2. **Hiding Command and Control.** Certain malware families use encryption to hide command and control communications.
3. **Hiding Data Exfiltration.** Many malware families also use encryption to hide network information such as passwords and stolen information (e.g., bank accounts and passwords).

Eighty-seven percent of CIOs feel SSL encryption puts their organizations at greater risk of cyberthreats.[23]

In addition to the above, cybercriminals are becoming increasingly adept at stealing SSL certificate keys that allow them to encrypt malicious emails, websites, and applications typically tagged to a whitelist. In these instances, SSL inspection may identify them as valid due to the identity of the SSL certificate. However, in reality, they are not what they purport to be. Cybercriminals certainly have the attention of IT leaders: 86 percent of them are concerned about stolen certificates and encryption keys.[18]

Part of the problem related to SSL certificates is that some enterprises lack comprehensive management processes. Less than half indicate they routinely review their SSL configuration.[19] Key management for SSL certificates is subpar for the majority of enterprises. The average organization has more than 23,000 certificate keys, and 54 percent of IT leaders admit they do not know where all of their keys and certificates are located.[20]

With more than three-quarters of enterprises indicating they manage between 10 and 19 certificate keys, the importance of maintaining a cohesive process around key management becomes heightened even further.[21] The number and complexity of certificate keys is expected to grow, with multiple development teams and the rise of DevOps and containerization that automatically generate their own keys. Seventy-nine percent of IT leaders say this makes it more difficult for organizations to manage their certificates and keys.[22]

DIFFERENT TYPES OF SSL CERTIFICATES

1. *Domain Validation.* These certificates are checked against domain registry. As there is no identifying organizational information for these certificates, they should not be used for commercial purposes (best used for internal systems and where security is not a concern).
2. *Organizational Certificates*. Organizations are authenticated by real agents against government business registry databases. Certificates contain legitimate business information and are used as a standard verification on a commercial or public-facing website.
3. *Extended Validation Certificates*. These require companies to undergo vetting with a Certificate Authority before an SSL certificate is granted. Successful SSL connections on websites result in the padlock icon appearing in the browser bar. Cybercriminals steal Extended Validation Certificates to add perceived credibility to their websites.

Over 75 percent of enterprises manage 10 to 19 SSL certificate keys.

Only **1 in 20** websites with HTTPS have it correctly deployed. **Ninety-five percent** are at risk of man-in-the-middle attacks.[24]

WHY ENTERPRISES ELECT NOT TO INSPECT SSL TRAFFIC

Enterprises can address the cybersecurity challenges that come with SSL encryption by implementing SSL decryption and traffic inspection systems. These allow them to pinpoint traffic that is valid versus instances where a bad actor is attempting to infiltrate a network by hiding their malicious attack via communications. Yet, for enterprises with security appliances deployed, less than half of them have SSL decryption and inspection enabled.

So, what is holding them back from implementing SSL decryption and inspection? One of the primary factors is the performance impact to their networks. Studies show performance can be impacted by nearly 75 percent.[25] Couple this with 20 percent year-over-year increases in network traffic and over three-quarters of IT leaders indicating they need to upgrade their existing IT networks for enhanced bandwidth and capabilities,[26] and it makes a lot of sense why many IT security leaders have been reluctant to activate SSL traffic inspection. Not only will this have a detrimental impact on traffic throughput and inspection performance but also on user productivity.

SSL decryption and inspection can also increase the complexity of managing their network security by introducing additional hardware and software to manage as well as security policies and workflows. Organizations need to develop and maintain whitelists, build and manage rules, and resolve false positives. But this is a problem, as many security solutions do not actively manage whitelists, and their management becomes a huge overhead.

In addition to the above, certain websites enable HTTP Public Key Pinning to prevent man-in-the-middle attacks. However, a number of things can go wrong. Certificate authorities can change their issuance practices without notice, and new certificates may not use the same chain of trust as old ones. If the new certificate chain no longer includes the pinned keys, the website will not be accessible until the HTTP Public Key Pinning policy expires. Mistakes or oversights could result in a business being without a website for weeks or months.

USERNAME

✱✱✱✱✱

SSL inspection and cryptography can degrade network performance by as much as **75 percent**.

PUTTING A SUCCESSFUL SSL ENCRYPTION (AND INSPECTION) STRATEGY IN PLACE

With the average cost of a cybersecurity breach now pinned at $3.5 million and the number growing 15 percent annually, enterprises need to pay heed.[27] SSL encryption is at a critical crossroads for protection and hacking. Organizations without an SSL encryption strategy are at much greater risk of cyberthreats. And it is not simply encrypting email, websites, and applications. Because bad actors are tapping SSL encryption to execute over half of their attacks today, a number that will continue to rise, enterprises must simultaneously have an SSL decryption and inspection strategy.

When assembling an SSL encryption strategy, enterprises should account for the following:

1. **Network Performance.** SSL decryption and inspection impact network performance. But there are ways to minimize the impact, such as consolidating all network security activity into one appliance. Further, look for a solution with accelerated purpose-built security processors that include intensive functions such as packet forwarding and pattern matching. This offloads workload and processing, thereby increasing performance fivefold to tenfold.[28] Organizations should also look for security appliances with parallel path processors specifically designed to meet the unique requirements of cybersecurity. In particular, they need to enable heavy content processing such as SSL inspection and cryptography to occur outside the direct flow of network traffic.
2. **Comprehensive Cipher List.** The list of SSL certificates continues to grow. The embedded cryptography within them is also evolving. Organizations using SSL decryption and inspection require a comprehensive list of ciphers. Cybercriminals typically use the most advanced—and newest—ciphers, thereby necessitating that organizations remain on the cusp of ongoing cryptography changes used for encryption.
3. **Avoid Complexity.** Minimize the complexity of SSL decryption and inspection. For example, in some instances, it may not be necessary to inspect the entire contents of an email, website, or web application, but rather only the identity of the SSL certificate. This streamlines the inspection process and reduces the impact to network performance. Enterprises will also be wise to implement efficient ways of dealing with potential HTTP Public Key Pinning conflicts. For example, organizations can institute processes to categorize a list of all certificate authorities that are whitelisted and remove those from SSL cryptography and inspection.
4. **Known and Unknown Threats.** Traditional cybersecurity technologies simply cannot keep pace with the changes in the cybersecurity landscape today. Threat prevention inspection for SSL must look for both known and unknown threats. Whitelisting is a great starting point, though a multipronged intrusion detection and threat prevention approach is also needed. Whitelisting also has a secondary impact in that it offloads specified domains and websites from packet decryption and inspection, thereby minimizing the impact to network performance.
5. **Web Browsing.** Websites and social networks use user-generated content that may be protected using SSL encryption. Cybercriminals use this encryption to hide malware payloads. Decryption and inspection of SSL web application traffic are requisites for organizations that want to protect users from introducing malware, bots, and ransomware into their environments.
6. **SaaS Application Monitoring.** As the security of SaaS traffic is not controlled by the end-user, it needs to be decrypted and inspected to ensure it does not contain hidden malware. Cloud Access Security Inspection, which leverages predetermined policies, enables organizations to achieve granular control of the most popular cloud applications such as YouTube, Dropbox, Salesforce, and Amazon, among others.
7. **Custom Applications.** Just like SaaS applications, custom applications over the web and via partners must be given the same level of attention when it comes to decryption and inspection.
8. **Email: Inbound and Outbound.** It is critical to encrypt outbound email to protect sensitive information. But with cybercriminals concealing command and control and exfiltrating locked and pilfered data using outbound email, it is just as important to decrypt and inspect all outbound email. The same is true for inbound email, with cybercriminals concealing their initial malware entry with encryption.

[1] See, e.g., J. Michael Butler, "SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL," November 2013; Johnnie Konstantas, "SSL Encryption: Keep Your Head in the Game," Security Week, March 15, 2016.

[2] "NSS Predicts 75% of Web Traffic Will Be Encrypted by 2019," NSS Labs, November 9, 2016.

[3] Ibid.

[4] Brian Barrett, "Most Top Websites Still Don't Use a Basic Security Feature," Wired, March 17, 2016.

[5] Brian Barrett, "Most Top Websites Still Don't Use a Basic Security Feature," Wired, March 17, 2016.

[6] "State of the Cloud Report: Public Cloud Adoption Grows as Private Cloud Wanes," RightScale, January 2017.

[7] Clint Boulton, "6 Trends That Will Shape Cloud Computing in 2017," CIO.com, November 2, 2016.

[8] Fredric Paul, "Cloud to Consume Almost Half of IT Infrastructure Sales by 2019," Network World, July 7, 2015.

[9] Joe McKendrick, "With Internet of Things and Big Data, 92% of Everything We Do Will Be in the Cloud," Forbes, November 13, 2016.

[10] Louis Columbus, "Roundup of Internet of Things Forecasts and Market Estimates, 2016," Forbes.com, November 27, 2016.

[11] Gil Press, "Internet of Things by the Numbers: Market Estimates and Forecasts," Forbes, August 22, 2014.

[12] Ashley Carman, "Gmail's Encryption Warning Spurs 25 Percent Increase in Encrypted Inbound Emails," The Verge, March 24, 2016.

[13] Robert Westervelt, "The Blind State of Rising SSL/TLS Traffic: Are Your Cyber Threats Visible?" IDC, July 2016.

[14] Westervelt, "The Blind State of Rising SSL/TLS Traffic."

[15] Jason Pappalexis, "TLS/SSL: Where Are We Today? The Encrypted Web: Part 1—An Upward Trajectory," NSS Labs, accessed February 14, 2017.

[16] Ibid.

[17] Jai Vijayan, "When Encryption Becomes the Enemy's Best Friend," Dark Reading, March 5, 2016.

[18] Ben Rossi, "CIOs Admit to Wasting Millions on Security Technology that Doesn't Work," Information Age, February 24, 2016.

[19] Robert Westervelt, "The Blind State of Rising SSL/TLS Traffic: Are Your Cyber Threats Visible?" IDC, July 2016.

[20] Rossi, "CIOs Admit to Wasting Millions."

[21] Westervelt, "The Blind State of Rising SSL/TLS Traffic."

[22] Rossi, "CIOs Admit to Wasting Millions."

[23] Vijayan, "When Encryption Becomes the Enemy's Best Friend."

[24] "95% of HTTPS Websites Are Vulnerable to Trivial Man-in-the-Middle Attacks," Netcraft, March 17, 2016.

[25] Westervelt, "The Blind State of Rising SSL/TLS Traffic."

[26] "Cyber Threat Assessment Report," Fortinet, accessed February 14, 2017.

[27] "Cyber Threat Assessment Report."

[28] "Cyber Threat Assessment Report."

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990