INVESTMENT IN CUSTOM SECURITY PROCESSING UNITS PAYS OFF HUGE DIVIDENDS FOR FEDERAL SECURITY

INDUSTRY PERSPECTIVE

INTRODUCTION

Federal agencies are a natural target for cyber criminals and nation-state actors due to the services they perform along with the troves of information their systems may hold. According to a 2016 Ponemon Cost of Data Breach Study: Global Analysis security study, government was the fourth most popular hacking target in 2016, preceded by the fields of healthcare, manufacturing, and financial services. A successful attack against the government has the potential to disrupt public services, expose classified information, and steal the personally identifiable information (PII) of millions of citizens. One need only look as far as the 2015 hack against the Office of Personnel Management (OPM) databases, in which the information, including in some cases highly detailed security clearance applications, of as many as 22 million people was stolen.

Encryption is an essential tool that federal agencies must employ to protect their networks and both the transient and maintained data on said networks.

Encryption works like this: Conversion of digital data into a code that requires a key or passcode to decipher, which ensures the authenticity of the sender and nonrepudiation, and Establishment of an encrypted link between two parties. However, cyber criminals and hackers are increasingly exploiting encryption to conceal malware as benign messages to circumvent established security perimeters, hiding in plain sight from intrusion-protection systems; gaining access to networks, sensitive data, and command and control functions while trusted insiders are using it for the exfiltration of stolen PII and internal IP addresses; and all the while putting personal, proprietary, and other sensitive information at risk.

With web-based transactions, the primary issue continues to be the trustworthy, longtime standard for securing our online communications, Secure Sockets Layer (SSL) encryption, most notably identified by the “s” in “HTTPS” at the beginning of a URL. Utilizing SSL, all transmitted information is encrypted and thereby protected. Without its utilization, information such as names, social security numbers, and credit card information is exposed in plain, readable text.

The question is, then, how can the government effectively implement encryption to protect federal networks and data while simultaneously blunting its use by malicious actors?

“The answer lies in decrypting and inspecting both incoming and outgoing SSL Web traffic to identify threats,” said Matthew Miller, U.S. Federal Channel Manager at Fortinet, in an interview with GovLoop. “With the right tools, any agency can implement this process, closing a developing gap in network defenses and avoiding false choices between security and privacy.”

However, the encryption/decryption and inspection of incoming and outgoing SSL web traffic places a tremendous burden on the network security infrastructure. Traditionally, network security products were reliant on shared CPU resources and the network administrator was required to “over buy” to actualize the performance required to meet demands from users and of applications.

Fortinet has taken a distinct approach to addressing the SSL challenge with the development of the security processing unit (SPU) for hardware acceleration of SSL encryption/decryption traffic. In recognizing general-purpose hardware was not sufficient to address the most difficult and upcoming security challenges, Fortinet reached a strategic decision to invest in custom hardware application-specific integrated circuit (ASIC) research and development to pioneer SPU technology. The dividends of the investment have been realized as Fortinet offers groundbreaking performance for SSL encryption/decryption at a low cost, removing the necessity to “over buy” that administrators had encountered.

In this industry perspective, created in partnership with Fortinet, you will learn more about the ASIC SPU chip; how hackers are using encryption to subvert edge defenses; and how governmental agencies may utilize the newly created SPU technology for a cybersecurity solution that can be employed for SSL decryption and inspection to thwart cyberattacks.

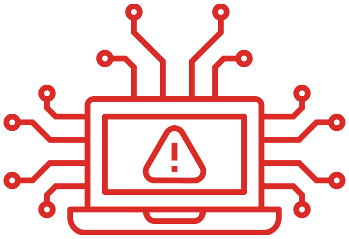
USING ENCRYPTION TO THWART EDGE DEFENSE

Encryption has become an increasingly popular way for cyber criminals to conceal their attempts to access federal networks. A recent Ponemon Institute survey determined 77% of public-sector respondents reported being the victim of some form of cyberattack in the previous year, and 43% of those attacks exploited encryption to sidestep detection.

Whether it is cyber criminals looking for monetary gain or hackers acting on behalf of a nation-state, the appeal is evident: The encryption used ostensibly to protect organizations, users, and their data is doing the hackers' work for them, concealing their attempts to get inside, and masking any data they might remove or replace.

The problem is certain to intensify with government agencies' increasing use of web-based interactions and cloud services in its varying manifestations, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Websites and cloud-based operations currently host items/documents such as permit applications to email services to an Amazon Web Services cloud infrastructure shared by the 17 agencies within the intelligence community. With no decrease in cloud-based operations on the horizon, by at least one estimate as much as 92% of online activity will be processed by cloud services by 2020. This means, in addition to formal online transactions, applications, or email, the increasingly popular user-generated content and custom applications will also be able to become exploited to introduce encrypted malware into a system.

Meanwhile, a June 2015 mandate from the White House established HTTPS as a requirement for all public-facing federal websites. While this improves security from one perspective, it also puts greater strain on essential cyberdefenses.



77%

of public-sector respondents reported being the victim of some form of cyberattack in the previous year

REDUCING NEW ENCRYPTED ATTACKS

A solid defense against these tactics is Secure Inspection at the Edge, which is an analysis of decrypted packets of information to ensure they do not pose a threat prior to re-encryption with allowance to traverse the network, allowing for the identification and handling of both valid and malicious traffic. However, it must be noted, tough choices must be made by many agencies, federal and civilian alike, due to the degradation of performance when employing this solution. It is not necessarily a case of viewing SSL encryption as a set it and forget it security blanket but rather an outgrowth of the complicating factors of running and maintaining a safe and secure network.

Shortages in qualified, knowledgeable personnel and limited funds to apply critical network defense while juggling ever-present security concerns, along with users' requirement for near constant uptime and dependable network performance, constantly plague federal IT administrators and engineers.

With the wrong equipment, decrypting and inspecting traffic strains network resources, slowing performance. The volume and sophistication of SSL security places a burden on the tools in a comprehensive security system, such as intrusion prevention and threat detection to maintain the pace.

In addition to hiding malware within web transactions, hackers and cyber criminals can also gain network access through the theft of SSL certificate keys, the electronic documents issued by credible certificate authorities and designed to ensure the authenticity of the sender. The certificate keys—and therefore the contents of a message—are trusted by the parties involved, allowing a stolen one to be used to encrypt malicious code in emails, websites, or applications. The process of managing many certificates may be cumbersome to some organizations, which ultimately may lead to complacency.

While HTTPS increases cyber security from one perspective, it has the potential to undermine a fundamental security strategy that is used and highly valued by the highest-end security organizations in the world.

THE TOOLS NEEDED FOR BETTER SSL INSPECTIONS AND SPUs

The biggest challenge is in meeting the seemingly contradictory goals of decrypting and inspecting web traffic without slowing down performance, by somehow adding speed, efficiency, and cyber safety to the process. Meeting that challenge is not as implausible and insurmountable as it might initially seem.

> *“Too many network operators are left with the false choice between performance and security, when it comes to SSL Inspection. The solution is hardware acceleration of networking and security functions, so that this fundamental secure inspection strategy can take place at cyber-relevant speed. Fortinet has pioneered hardware-based Security Processing Units in its products to ensure that high-end security keeps up with high-volume encryption.”*
>
> Phil Quade, CISO for Fortinet

Organizations can take two important steps to begin the process:

1. **SIMPLIFY** the processes by implementing tools, such as a web filter, that can granularly categorize traffic into specific types. Organizations can then efficiently and correctly determine which encrypted data to inspect.

2. **IMPLEMENT** technologies that can decrypt, inspect, and re-encrypt data at high speeds using dedicated components, such as SPUs.

Both steps would ideally be performed within the same tool, such as a Fortinet’s FortiGate Next-Generation Firewall (NGFW), which is a set of appliances that can come in several configurations, from entry level to high end, and provide a single, high-speed platform capable of handling physical, virtual, and cloud environments.

NGFW, encrypted with these SPUs, centralizes the inspection process while providing ways to limit the strain on network resources, enabling the use of Application Control, which identifies the data and functions specific to an application regarding input, output, and processing, thus helping ensure their accuracy and authenticity.

Guided by strong security policies, Application Control can identify and block traffic that cannot be inspected. For example, it is with Application Control that IPsec tunneling would only be enabled for authenticated users and validated systems, while nonstandard encryption tunnels and proxy avoidance-type tunnels would be blocked outright.

At times, inspecting and confirming the identity of an SSL certificate can be enough to ensure security, rather than digging through an entire email, application, or website. The FortiGate NGFW can be configured to verify the web server used in a message's transport and ensure HTTPS has not been used to circumvent a web filter. Both the time and effort saved during the inspection could significantly lighten the burden on network performance. Organizations could also carefully employ HTTP Public Key Pinning, which allows for the whitelisting of certificate authorities deemed trustworthy. An example of this is Google initiating the practice of pinning its own websites, which removed them from the decryption and inspection process.

If the decryption, inspection, and re-encryption of the data stream does not occur transparently or quickly, it will not benefit users. Web traffic and SSL encryption may take place within software, but the key to speeding up the decryption and inspection process lies in hardware, specifically hardware acceleration. Without hardware acceleration, SSL decryption could be running on a general-purpose processor, which will undoubtedly introduce debilitating latency into the network, greatly impacting the productivity of users and the speed of system-to-system communication. Furthermore, systems without ASIC acceleration often sacrifice most of their processing capacity to enable SSL inspection, which can severely diminish network performance.

FortiGate appliances address these problems with hardware specialized to handle the load. At the root of those appliances are specialized SPUs with the FortiASIC System-on-a-Chip architecture. FortiASIC chips offer up to 100 Gbps of throughput, far exceeding the secure networking performance of enterprise CPUs in other security solutions, making it the most powerful in its class. Perhaps most importantly, Fortinet can offer this throughput at a price to fit within most agencies' budgets.

Additionally, for times when inspecting the identity of an SSL certificate or whitelisting an issuing authority is not sufficient and all SSL-encrypted content must be inspected, the FortiGate can be configured to perform deep, or full, SSL inspection at industry-leading throughputs. Deep SSL inspection, as the name suggests, goes beyond a cursory look at a message or application; it can examine any sub-applications in use, allowing for enablement of Application Control. The FortiGate decrypts the content, inspects it, and then re-encrypts it using a certificate stored within FortiGate.

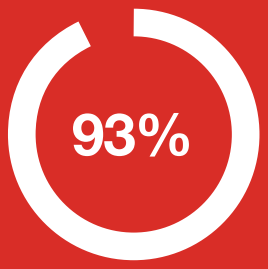
Fortinet appliances include SPU acceleration hardware designed to offload resource-intensive processing from main CPU resources, separating security processes from network performance. It is important to note that Fortinet's SPUs are not limited to SSL challenges. The FortiGate units include specialized content SPU processors that accelerate a wide range of security processes, including virus scanning, attack detection, encryption, and decryption. Many FortiGate models feature security processors that speed up processing for specific security features, to include intrusion-prevention systems and network processors that offload the processing of high-volume network traffic.

FORTIFYING THE GATES WHILE LETTING TRAFFIC FLOW

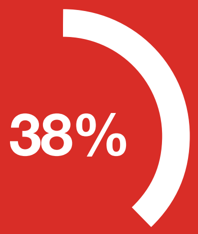
Encrypted web traffic is ubiquitous, as is the hackers' usage of encryption within malicious attacks, thus the implementation of decryption, inspection, and re-encryption has become a mutual inevitability and prerequisite to safely traversing the world wide web. The challenge we must meet is effectively and efficiently performing decryption, inspection, and re-encryption seamlessly and transparent of the end-user and applications used.

In the Ponemon survey, 93% of respondents in the public sector rated SSL inspection as important or essential, with only 38% admitting to its implementation. The trade-offs in network performance required by decryption and inspection have kept more than half of federal agencies from employing best practices. Therefore, the threat of encryption being used in attacks is real, and sure to grow.

Employment of the best tools, industry-standard techniques, and safety measures can streamline inspection without crippling performance. Tools such as the FortiGate NGFW line can centralize and simplify the procedure while speeding up processes and minimizing the drain on other resources, providing an effective counter against what has become a serious and emergent threat.



93% of respondents in the public sector rated SSL inspection as important or essential



But only 38% admitted to its implementation

ABOUT FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. We empower our customers with intelligent, seamless protection across the expanding attack surface, and with the ability to take on ever-increasing performance requirements of the borderless network - today and into the future. Our federal solutions protect the classified and unclassified systems used by 12 of 15 cabinet-level agencies, and those of numerous independent agencies, utilizing Fortinet's specially configured USG product line. These platforms comply with federal certification requirements including NIST FIPS 140-2, NIAP Common Criteria certification, and are on the Commercial Solutions for Classified Programs (CSfC) approved Components List.

Learn more at www.FortinetFederal.com.

ABOUT TVAR SOLUTIONS

TVAR Solutions was founded in 2006 and is headquartered in McLean, VA. TVAR Solutions is a small business information technology value added reseller that markets exclusively to the Federal Government and its system integrator partners. TVAR Solutions aims to provide innovative solutions that address complex computing infrastructure challenges.

For more information, please visit www.tvarsolutions.com.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop