[OVERVIEW]

TO ENCRYPT, OR NOT TO ENCRYPT: WHAT IS THE REGULATION?

Regulations in many countries require organizations to secure and encrypt any communications with their customers. The downside: those organizations now have to grapple with threats that hide within encrypted traffic.

People have long used cryptography to hide secret communications. The use of codes and ciphers to protect sensitive information began thousands of years ago—the well-known “Caesar cipher” is named for Julius Caesar, who used shift-cipher when writing messages containing sensitive military information. In the early 1970s, IBM introduced crypto into its business practices when it designed a block cipher to protect its customers’ data. In 1976, the United States adopted the Data Encryption Standard (DES) as a national standard.

In the early 1990s the Internet moved into the commercial realm, and the need to “scramble” data became a requirement. Netscape developed the Secure Sockets Layer (SSL) protocol in 1994 to secure communications between the client and server on the web. Over the years, SSL–and its recent replacement Transport Layer Security (TLS)–have undergone many improvements; and with that, widespread adoption. Today, close to 90% of web traffic is encrypted, according to F5 Labs.

While some adoption of encryption-in-transit (SSL/TLS) can be credited to organizations’ desire to maintain security and privacy, a lot can be attributed to regulation or mandatory compliance standards.

REGULATIONS & COMPLIANCE IN THE U.S.

VIOLATING ANY OF THE UNITED STATES’ PRIVACY LAWS CAN LEAD TO HEFTY FINES–AND POTENTIAL JAIL TIME.

Depending on the type of data, the protection of U.S. residents’ data is defined by various laws or contractual obligations. Federal statutes are primarily aimed at specific sectors, such as financial or health care, while state laws focus on protecting individual consumers’ personally identifiable information (PII). And then there are industry mandated protection frameworks, such as PCI, which prescribes the exact measures required to protect credit card data.

Most U.S. states’ privacy laws only determine the consequences of a breach of PII, rather than defining how to protect it in the first place. In any case, a data breach can lead to hefty fines—and potential jail time. The California Consumer Privacy Act of 2018 goes into effect in January 2020, and greatly expands the rights of individuals in ways that are similar to the EU GDPR. Likewise, the federal healthcare industry law, HIPAA, mandates fines based on the number of patients that are involved in a breach. Such fines are categorized in one of two categories: “Reasonable Cause” carries lower fines (between $100-$50,000) and no jail time, whereas “Willful Neglect” leads to higher fines ($10,000-$50,000) with potential jail time and criminal charges.

There are several entities that maintain network security guidelines for TLS. Listed below are the four most adopted:

- **The Health Insurance Portability and Accountability Act (HIPAA)**
- **NIST’s SP 800-52r1 guidelines**
- **Payment Card Industry (PCI) Data Security Standard (DSS)**
- **The Gramm–Leach–Bliley Act**

REGULATIONS IN EUROPE

In Europe, GDPR is a broad-reaching regulation meant to protect the private data of Europeans in IT systems. It mandates that regulated information must be protected with “appropriate technical and organizational measures,” including encryption of personal data and the ability to ensure the ongoing confidentiality of systems and services. GDPR defines “personal data” as any personally identifiable information (PII), personal health information (PHI), web usage information, and a set of personal characteristics such as race, sexual orientation, and political opinion. Violating GDPR can be an expensive mistake. Lower level fines can be up to €10 million, or 2% of the worldwide annual revenue of the prior financial year and upper level fines can be up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. EU GDPR requires encryption with up-to-date technology, so only TLS 1.2 or higher is acceptable. Failing to provide this minimum of security compromises the communications security of all correspondents.

GDPR DEFINES “PERSONAL DATA” AS ANY OF THE FOLLOWING:

PII
Personally identifiable information such as a name, an identification number, location data, or an online identifier; or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

PHI
Personal Health Information

Web Usage Information
Personal data that has been collected during web transactions, such as cookies and ad trackers.

Personal Characteristics
Race, sexual orientation and political opinion

In Europe, the GDPR requires encryption with up-to-date technology, so only TLS 1.2 or higher is acceptable.

REGULATIONS IN APAC

In APAC, Japan’s Personal Information Protection Act protects individuals’ rights in regard to their personal data. The act’s definition of “personal data” is so broad that it even applies to information that could be found in a public directory. It states that you must describe as specifically as possible the purpose of the personal data you're collecting, and you must obtain prior consent to share the personal data with any third party (such as an email newsletter service). However, Japan has no laws or policies that address a general right to encryption.

South Korea's Act on Promotion of Information and Communications Network Utilization and Data Protection states that all information and communications service providers need to obtain a user's consent before collecting their personal information. For the consent to be valid, you must provide the user with specific information, including your name and contact information, the purpose of the data collection, and the user's rights concerning their own data.

In Japan, you must describe the purpose of the personal data you're collecting, and obtain prior consent to share it with any third party (such as an email newsletter service).

GOOD NEWS, BAD NEWS

All of these regulations and requirements mean that organizations must secure and encrypt any communications with their customers—along with internal data such as trade secrets and employee information. This is the good news, because encryption already protects our data, keeping our private info private and ensuring the integrity of encrypted data. TLS prevents eavesdropping, tampering or message forgery and provides endpoint authentication.

68%

OF MALWARE WEBSITES LEVERAGE ENCRYPTION CERTIFICATES.

93%

OF PHISHING DOMAINS OFFER A SECURE WEBSITE VERSION.

ORGANIZATIONS NOW HAVE TO GRAPPLE WITH THREATS THAT HIDE WITHIN ENCRYPTED TRAFFIC.

The bad news? Organizations now have to grapple with threats that hide within encrypted traffic. Encryption limits visibility into incoming traffic, and attackers are taking advantage of this security blind spot by sending malware/malicious payloads via encrypted connections. According to F5 Labs, 68% of malware websites leverage encryption certificates, and 93% of phishing domains offer a secure website version. This means that organizations should decrypt and inspect traffic to ensure nothing malicious is hiding in that transmission.

All this elevates the security risks associated with encryption, and elevates the risk of non-compliance with privacy regulations. So, where should a company place its focus? On protecting the organization from malware by decrypting and inspecting traffic? Or on adhering to privacy regulations by letting encrypted traffic pass through?

YOU CAN DO BOTH

With the availability of advanced security solutions, you don't need to settle for an "either-or" situation. F5's SSL Orchestrator's Policy Based Traffic Steering can decrypt and steer to service chain based on a policy match. The contextual classification engine has a rich set of traffic selectors to determine which traffic gets inspected and which traffic requires bypass. Your security service chain might include inspection devices such as an NGFW, a DLP device, an IPS/IDS device, or even a http/https web proxy.

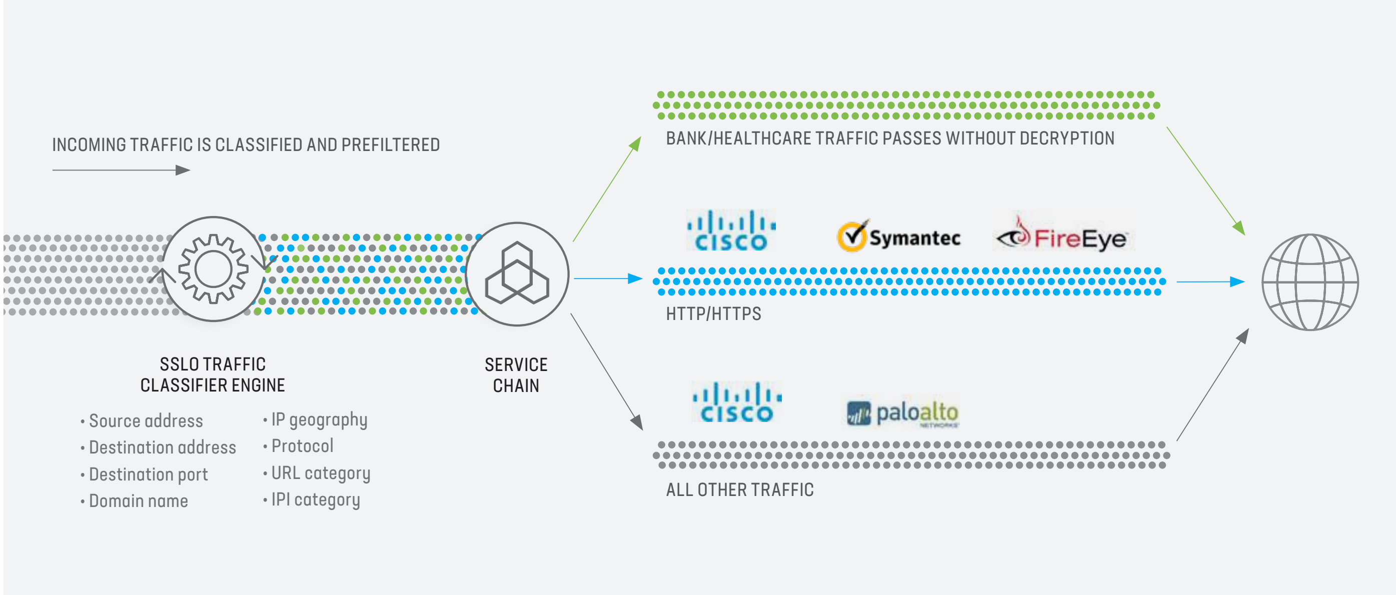

Figure 1: *Policy Based Traffic Steering* allows organizations to determine what types of traffic get decrypted/inspected and what types get bypassed.

Based on traffic classification—URL, domain name, protocol, source/destination address, geolocation and others—SSLO takes the appropriate action necessary to decrypt and inspect that traffic, or allow the traffic to bypass untouched to adhere to regulatory standards. This means organizations can stop encrypted threats while maintaining privacy through intelligent routing, dynamic service chains, and standards support. SSLO balances security and privacy in a single high-performance solution.

F5 SSL Orchestrator provides an all-in-one solution designed specifically to optimize your SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution supports policy-based management and steering of traffic flows to existing security devices, is designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure.

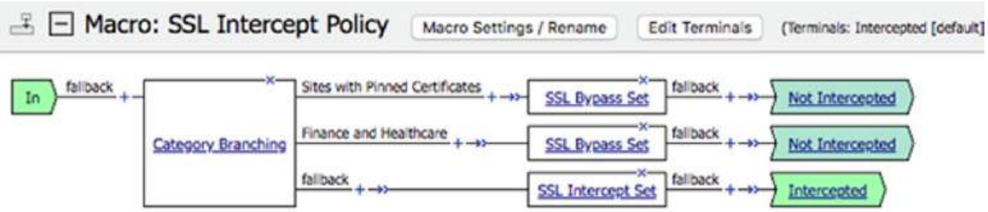

Figure 2: The Visual Policy Editor (VPE) allows administrators to follow the flow chart and determine what happens to the output of that individual element, which is then fed into the next element's macro.

You can configure SSL Orchestrator in an array of topologies that define the type of traffic (transparent or explicit) and the direction of the traffic flow (inbound or outbound) you wish to inspect. These deployment settings can be modified as needed without re-deploying a configuration. They're complemented by SSL management settings that help you define inbound decryption and outbound decryption. These SSL management settings also help you set your service types, and create service policies by defining per-request and per-session policy settings. These can then be managed through a virtual policy editor. SSL Orchestrator can install default outbound interception rules, providing greater support for defining your listeners and the flexibility to create your own outbound and inbound interception rules.

SECURE COMPLIANCE

Privacy is an important part of business strategy. It's critical for companies to balance user privacy concerns and regulations with the need for data, and a desire to provide a customized browsing experience. Businesses that successfully manage this can improve customer satisfaction, build trust, and avoid negative press coverage and the costs of legal action.

F5's SSL Orchestrator can help by enhancing your organizations privacy and security with improved efficiencies—plus features that lower total cost of ownership, eliminate security blind spots, comply with privacy regulation, and meet the performance challenges of today's encrypted world.

AS TECHNOLOGY EVOLVES OVER TIME, IT'S ALSO IMPORTANT TO KEEP UP TO DATE WITH CHANGES AND AMENDMENTS TO THE LAWS.

But technology is only half the solution. Privacy and compliance laws vary by region, and you need to know which ones apply to your organization and which ones don't. As technology evolves over time, it's also important to keep up to date with changes and amendments to these laws. Noncompliance can be quite costly—in money and reputation. It's better for the bottom line to stay on the right side of regulations.

To learn more about F5 SSL Orchestrator, visit f5.com/SSLO