Key Considerations in Deploying an SSL Solution

Introduction

As social animals, humans struggle to keep secrets. We survive—and thrive—through the sharing of information. However, some information needs to remain private, which is why cryptography has been around in one form or another since the Spartan army used a transposition cipher to protect military information during their wars with the Greeks.

But while the science of keeping private data private was once the purview of government intelligence agencies, the ubiquity of the Internet has made privacy a concern for everyone. In the face of a steady stream of data breaches, the question of how to safeguard personal and corporate data online has become paramount to businesses around the world.

The rise of SSL and the current security landscape

Only a decade ago, large financial institutions and government agencies were the primary organizations employing the cryptographic protocol historically known as the Secure Sockets Layer (SSL) and now called Transport Layer Security (TLS). Today, SSL is everywhere. Analysts predict that encrypted traffic will jump to nearly 64 percent of all North American online traffic in 2016, up from just 29 percent in 2015.[1] Organizations are scrambling to encrypt the majority of traffic, including everything from email and social media to streaming video. This evolution adds security to web traffic, but at a price. The growth of SSL traffic has put a burden on organizations to implement an efficient SSL solution that allows their network infrastructure to respond to the increased workload demanded by strong security.

an everywhere, all-the-time security protocol. At the same time, SSL has become a vulnerability vector as attackers have started using SSL as a way to hide malware from security devices that cannot see encrypted traffic. Distributed denial-of-service (DDoS) attacks are particularly troublesome, as they take advantage of the relatively large computational costs associated with hosting SSL server traffic. In addition, implementation issues such as the Heartbleed incident can result in security breaches.

Properly deploying SSL is daunting even for seasoned administrators. However, it is possible to stay in front of changes—choosing proactive strategies instead of reactive tactics—by learning about the most current options and trends in deploying SSL across sites.

Fundamental Considerations When Adopting an SSL Strategy

Data protection and privacy

The primary goal of SSL is to secure data in transit between applications. When secured by SSL, communications between a client such as a web browser and a server will be private, and the identities of the two parties can be authenticated. However, all traffic that is encrypted with a private key is subject to potential future decryption, as learned during the high-profile U.S. National Security Agency (NSA) leaks from Edward Snowden. Securing all web communications is not enough.

Implement perfect forward secrecy

SSL has a passive surveillance countermeasure called perfect forward secrecy (PFS) protection, which adds an additional exchange to the key establishment protocol between the two sides of the SSL connection. By generating a unique session key for each session the user initiates, PFS guarantees that an attacker cannot simply recover a single key and decrypt millions of previously recorded conversations.

It's seemingly simple to adopt PFS; just activate it within the SSL termination device such as an Application Delivery Controller (ADC). However, organizations using passive security devices such as an intrusion prevention system (IPS) or intrusion detection system (IDS) will run into trouble, as those devices often require that they be configured with a persistent private key, which PFS does not use. Thus, organizations are faced with a choice: turn off their IPS/IDS or turn off PFS. Either choice compromises their overall security posture.

There is another way. Allow the IDS/IPS to do the job it was made for by offloading all the SSL traffic to a reverse proxy, such as a web application firewall or ADC. The reverse proxy can then handle the ciphers before passing the decrypted traffic on to the IDS/IPS for inspection and sanitization.

SSL traffic and optimize the work of network security devices.

Use HTTP Strict Transport Security

Enabling HTTP Strict Transport Security (HSTS) is one of the easiest and most powerful ways to improve the security posture of applications. By inserting a header into HTTPS traffic, HSTS provides a layer of protection against several common attack vectors, including cookie hijacking, man-in-the-middle, and downgrade attacks. All major browsers now support HSTS, making its use a good way to ensure that all traffic stays encrypted.

What you can do: Ensure that all pages for all domains have the HSTS header by enabling HSTS for subdomains. Be sure that those subdomains are able to support the use of SSL. Double-check that the SSL solution permits quick and easy configuration of system-wide HSTS parameters. Ensure that the HSTS header has a duration of six months or more.

Visibility and control

Managing applications and ensuring their security requires visibility into traffic—or the ability to provide that visibility to security devices such as a web application firewall (WAF), an IPS/IDS, or a next-generation firewall (NGFW)—so that it may be screened for known threats. By definition, however, SSL hides the data being communicated, even from security solutions, but several approaches maintain security while effectively revealing malicious traffic.

Employ SSL offload and transformation

Encrypting and decrypting SSL traffic consumes additional computational power. With the growth of SSL, network and user experiences can be affected by latency and sluggish performance. In addition, some computationally intense protocols are not supported by some security devices in use today. An ADC can ease that computational burden by serving as a full proxy for TCP, HTTP, and SSL, meaning the ADC creates one connection to the client (browser) and a separate connection to the server. The transformational nature of an SSL proxy allows a site to provide SSL features that are decoupled from the capabilities of the application servers.

What you can do: Deploy a solution that can scale. Offloading SSL termination work to an ADC simplifies enforcing a consistent SSL policy without compromising performance, key protection, or visibility. This increases flexibility by allowing the ADC to transform the interface to the web servers into any protocol the ADC supports, regardless of the back-end transport options. This allows business-critical legacy devices and applications on the back end to continue operating without changes while maintaining a robust public-facing security posture.

vulnerabilities. Finally, with a hybrid architecture, look for a solution that allows offloading SSL processing from virtual machines (VMs) to a hardware device in order to reduce computational demands on the infrastructure and get the most from a virtual deployment.

Neutralize malware with SSL intercept

Security analysts estimate that by 2017, 100 percent of new malware will use SSL to hide its tracks from the security devices designed to identify and neutralize it. Enterprises need to monitor and sanitize their outbound web traffic to mitigate advanced persistent threats (APTs) such as spear phishing and malware activity.

New security devices are constantly being developed to assist administrators in detecting these threats. Implementing what is known as a defense-in-depth strategy, many administrators deploy security devices in a chain so they can support each other. However, SSL operations hinder the efficiency, security, and performance of these devices. Many of these new technologies are either blind to encrypted traffic or suffer significant performance degradation when tasked with inspecting encrypted traffic. Next-generation firewalls, for example, can experience up to 80 percent performance loss with SSL enabled. Malware and spear phishing authors know this and are quickly moving to encrypt all communication between their malware and the outside world.

What you can do: One way to battle these encrypted threats is to deploy an SSL air gap solution, which consists of placing an ADC on either side of the visibility chain. The ADC closest to the users decrypts outbound traffic and sends the decrypted communications through the security devices. These devices, which can now see the content, apply policy and controls, detecting and neutralizing malware. At the other end of the chain, another ADC re-encrypts the traffic as it leaves the data center. Deploying this solution provides the flexibility of keeping security devices in line, while ensuring that they can do the job they were built for.

One more note: When employing a visibility scanner such as FireEye or Cisco Sourcefire to protect the network from zero-day exploits and other malicious attacks, make sure the SSL solution works closely with these security products to maximize efficiency.

Mitigate brute-force DDoS attacks

The complexity of deploying SSL, combined with the difficulty many network devices experience in gaining visibility into encrypted traffic, make SSL the perfect target for DDoS attacks—a fact attackers understand all too well. As the overall volume of legitimate SSL traffic rapidly increases, malicious DDoS traffic becomes ever more difficult for security devices to identify.

SSL solution that can efficiently identify suspect DDoS traffic and prevent it from impacting the availability of websites. Consider investigating cloud-based DDoS services that can help mitigate the impact of SSL-based DDoS attacks.

Check Your Security Now

So how do you know whether your SSL security posture is up to snuff? Qualys SSL Labs offers an invaluable tool that lets you test your sites' certificates and configuration—before you face an attack. You can also evaluate your browser's SSL implementation and see how other sites—and your competitors—are doing in the face of these rapidly evolving SSL challenges.

Cipher agility

Since the beginning of the SSL protocol in the 1990s, the RSA cryptosystem has been the main choice for key exchange. Over time, as brute-force attacks became more feasible, RSA key lengths had to become longer. Today, RSA keys are so large that the key exchange is a very computationally intensive operation.

To reduce that computational load while maintaining stringent privacy controls, new cryptographic protocols are gaining popularity. For instance, elliptic curve cryptography (ECC) offers the same level of security as previous algorithms while requiring less processing, which also means that it's much friendlier to the battery life of mobile devices. While these cryptographic options are promising, organizations are rightfully concerned about having to reconfigure hundreds of servers to offer these new protocols.

What you can do: It is not uncommon to have to switch algorithms over time, so ensure that the SSL solution has cipher agility—the ability of an SSL device to offer multiple cryptographic protocols such as ECC, RSA2048, and DSA at the same time, even in the same web application. In addition, with increasing cipher diversity, it's essential that the SSL solution demonstrates a proven track record of staying up to date with cipher support.

Key management

SSL keys are among an organization's most prized assets. An attacker who gains possession of private SSL keys could impersonate the target's applications and create the ultimate phishing portal. However, there are several ways to protect these all-important keys.

Keep high-value keys safe

A hardware security module (HSM) is a separate software and hardware security device that follows the strict FIPS 140-2 cryptographic design guidelines to safeguard and manage

like the Heartbleed bug.

What you can do: The most secure way to safeguard SSL keys is by using an HSM. There are several possibilities, such as purchasing an internal HSM like the one included in some ADCs. Some organizations consolidate their key management by using HSM devices as centralized key stores (for example, one pair per data center). These network HSMs are accessible over the internal network to services that need key decryption, which means that many SSL termination points can use the same network HSM. One caveat: Just make sure that the SSL solution can tie seamlessly into the network HSM.

Organizations implement enterprise key and certificate management (EKCM) best practices to ensure the security of SSL keys. Consider using a hardware-secured encrypted key storage system, which allows passphrases to be stored in an encrypted form in the network file system.

Manage SSL certificates efficiently

The foundation of effective EKCM best practices is creating a comprehensive inventory of all enterprise certificates, their locations, and the people responsible for managing them. Each SSL-enabled website has its own certificate, and each certificate has its own expiration date. In any given week, one or more certificates may expire, which will cause the associated website or application to become unavailable. Managing all these certificates can be a laborious undertaking, but it is essential to ensure the high availability of critical sites. In addition, SSL certificates should also be audited for key length (2048-bit or more), digital signing (SHA2 or better), and rogue certificates not generated within internal PKI or by a public root CA. Finally, compliance with PCI DSS requires a documented certificate and key management process.

What you can do: Most administrators of medium to large organizations prefer an external certificate management system because the organization has keys and certificates in many locations. In particular, many have had success with two external solutions: Venafi and Symantec. It is important that whatever solution chosen has open APIs to automate management and decrease the operational load.

Comprehensive compliance

Compliance is often *the* driving force behind SSL adoption. Applications that comply with the PCI DSS specification will need to discontinue use of SSLv3 and TLSv1 over the next two years to remain in compliance with PCI 3.0. New PCI DSS deployments must already be disabling SSL 3.0 and TLS 1.0.

services provide the ability to maintain compliance with an Internet-facing SSL policy without the need to enforce that policy on individual servers. Ensure that the SSL solution is ready for the upcoming TLS 1.3. In addition, real operational efficiency gains can be made by centralizing compliance through a network service offloaded to an ADC rather than attempting to solve it for each individual application.

Conclusion

Like it or not, the online world is a dangerous place, and protecting sensitive corporate information from would-be attackers has become a top priority for enterprises of all sizes. With privacy breaches becoming increasingly common, many organizations look to SSL as a way to protect the integrity of their data online. However, the implementation of a comprehensive SSL strategy comes with its own challenges of visibility, performance, and scale.

Through proper planning and deployment, a strong SSL strategy mitigates the risk of breaches. Once the strategy is in place, the site will be positioned for future security, scalability, and reliability, putting the focus where it really matters—moving business forward.

[1] Sandvine, Global Internet Phenomena Spotlight: Internet Traffic Encryption (https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf), 2015.

PUBLISHED MAY 26, 2016

F5 NEWSROOM

News, F5 blogs, and more.

Go to the newsroom

Secure and Deliver Extraordinary Digital Experiences

F5's portfolio of automation, security, performance, and insight capabilities empowers our customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users. Learn more ›

WHAT WE OFFER

RESOURCES

SUPPORT

PARTNERS

COMPANY

CONNECT WITH US

Chat with Codey