Protecting Against Encrypted Threats

Encrypting user and corporate data to maintain privacy has great merit, but there is a nefarious downside: attackers have realized encrypted traffic is also a fabulous—and stealthy—way to spread malware and other malicious content *to* users and throughout organizations, and to surreptitiously exfiltrate stolen data *from* users and organizations.

Challenge

These days, most traffic traversing the web, clouds, and networks is encrypted. And the majority of Internet traffic is protected by SSL/TLS encryption. The need to keep user and sensitive corporate data private has helped drive the explosion in encrypted traffic. While not mandating that traffic be encrypted, government regulations—such as the European Union's General Data Protection Regulation (GDPR)—and industry standards—such as Payment Card Industry (PCI) Data Security Standard (DSS)—have prompted organizations to protect user and corporate data via encryption. The record adoption of Microsoft Office 365 and other cloud-based application services has also driven the meteoric rise in encrypted traffic, as has the continued increase in the growth and use of social networks.

Encryption helps to keep user and corporate data protected and private. However, it also creates security challenges when it comes to the proliferation of malware infections and other malicious content: when traffic is encrypted, organizations are unable to see what is *inside* the traffic.

It has become a struggle for organizations to gain visibility into encrypted traffic, while preserving necessary user and data privacy. Attackers know that they can hide malware and other threats in encrypted traffic, creating security blind spots. This lack of visibility makes it easier for attackers to launch attacks on the organization and its data. For this reason, organizations require a level of visibility into encrypted traffic, at a minimum, to determine whether or not hidden, malicious payloads are lurking behind the encryption.

SSL/TLS visibility is a minimum requirement today. Many organizations leverage solutions in their existing security stacks to handle the decryption, inspection, and re-encryption of encrypted traffic. Often, these organizations manually connect security point products, creating a daisy-chained security stack consisting of multiple security devices. But statically configured security

stacks are complex and can fail to adapt to changing network conditions. In addition, existing security solutions can be inefficient, costly, and may be vulnerable when dealing with encrypted traffic. A daisy chain of security point products may be able to decrypt, inspect, and re-encrypt traffic; but the redundancy of each point product having to perform the same steps and functions can create latency and a poor user experience. Also, removing a security device from the chain for any reason—for example, it needs to be updated or swapped out, or it stops working—can create a break in the chain. This means that any encrypted traffic can bypass the remaining security devices in the chain, which can lead to malware infections and data exfiltration.

In addition, new encryption protocols and ciphers can—and many times do—break passive SSL inspection by security devices. Another challenge arises when newer encryption ciphers are not supported by certain security devices. Attackers know which devices are unable to support specific encryption ciphers and use that knowledge to their advantage. If an inline device does not support a particular cipher or encryption protocol, it may cause a break in the chain, allowing malicious encrypted traffic to slip through unchecked. With unsupported ciphers, the security devices that do not support the ciphers are forced to bypass the malicious encrypted traffic and *voilà*—an organization's network, cloud, and/or applications are infected, and its data is being stolen, corrupted, or held for ransom.

How to securely, cost-effectively, and efficiently halt incoming threats or outgoing data exfiltration when traffic is encrypted is already a major challenge for organizations. At the same time, they must keep up with the array of new encryption protocols and ciphers being introduced, forcing them to perform the difficult, costly, and time-consuming task of updating existing security solutions.

Solution

Visibility into and inspection of inbound encrypted traffic is vital, but it is just a start. A true solution to the challenge requires greater insight and protection.

Visibility and inspection of encrypted outbound traffic can protect organizations from malware that may already be present and laying nascent in their networks, clouds, or applications, waiting for the appropriate time or calls to strike. When it does unleash its malevolent payload, the already-present malware may attempt to exfiltrate sensitive user or corporate data from the networks, clouds, or applications. Or, it may attempt to communicate with a command-and-control (CnC) server that will attempt to distribute and launch additional or different types of malware attacks on an organization. These actions are halted when outbound encrypted traffic—that is, traffic emanating from an organization's network, cloud, or application, or from a user's web browser—is decrypted, inspected, and, if safe, re-encrypted as it attempts to access a server outside of the network.

Centralizing the management of encryption, as well as protocol and cipher updates, can be a relief for most organizations. The cost, time, and potential for error can be great when managing new or updated encryption protocols and ciphers across multiple daisy-chained point security devices responsible for the organization's SSL/TLS visibility. Centrally managing and administering encryption protocols and ciphers alleviates a potentially expensive and dangerous headache for organizations.

Also, the ability to deploy a single platform for unified inspection of encrypted devices helps to stop the potential for performance drain of existing security devices. It enables point security products to focus on the function for which they were purchased: to keep the organization's network, cloud, and apps—and user data—safe.

Statically chained security point products are inefficient when it comes to SSL/TLS decryption and re-encryption. To increase protection from encrypted threats while reducing the cost of security, organizations need a solution that can: 1) route encrypted traffic to a centralized point for decryption, then 2) use policy and context-based intelligence to dynamically steer decrypted traffic to an appropriate security service chain, and 3) simultaneously prevent that traffic from redundantly running the same gauntlet of security devices each time.

F5 SSL Orchestrator

F5® SSL Orchestrator™ is a dedicated offering that centralizes encryption, dynamically steers decrypted traffic to policy-based security service chains while intelligently bypassing sensitive encrypted data, and secures the balance and health of security services. SSL Orchestrator lowers security total cost of ownership (TCO) while enhancing security, control, and visibility into today's encrypted threats.

Mitigates Encrypted Traffic Risks

SSL Orchestrator breaks the encrypted attack chain. It alleviates encrypted traffic threats by holistically enabling SSL/TLS traffic visibility, intelligently steering and orchestrating the handling of encrypted traffic, and unifying encrypted traffic inspection services.

By centralizing the decrypt and encrypt functions for encrypted traffic inspection, SSL Orchestrator helps to reveal the security blind spots and hidden threats associated with inbound encrypted traffic. Additionally, it helps to eliminate malware infections, exfiltration of stolen sensitive data, and CnC communications found in outbound encrypted traffic.

F5 SSL Orchestrator goes beyond encrypted traffic visibility, living up to its name: it orchestrates the handling of encrypted and decrypted traffic by applying context-based intelligence.

SSL Orchestrator also supports new, diverse protocols and ciphers, which prevents security blind spots from occurring with encrypted traffic. It also enables greater flexibility in how encrypted traffic is handled, without necessitating any architectural changes.

Provides More Than Visibility

SSL Orchestrator enhances encrypted threat protection *and* privacy, both of which are paramount in today's networks, clouds, and applications. SSL Orchestrator stops encrypted threats while maintaining privacy through its intelligent routing, dynamic service chaining, and standards support.

Instead of manually creating redundant, static service chains with security point products in their stack, organizations can dynamically, logically chain security services using SSL Orchestrator, leveraging its classification metrics to create focused, appropriate security service chains based on the traffic. SSL Orchestrator then decrypts the traffic, and steers it to the appropriate dynamic security service chain or chains via policy and context-based intelligence, ensuring that the right security solutions are deployed against the right decrypted traffic, helping to uncover and eliminate threats hidden in encrypted traffic.

SSL Orchestrator includes robust cipher management, ensuring that the latest encryption protocols and ciphers are supported. But even if they are not supported, SSL Orchestrator can—through its full-proxy architecture—negotiate an appropriate handshake between the different encryption protocols or ciphers. This ensures that the encrypted traffic will be decrypted and inspected, and not bypassed as it would be if it were handled in a chain of security point products or by a half-proxy environment.

SSL Orchestrator also supports Federal Information Processing Standard (FIPS) Publication 140-2 and as well as network hardware security modules (HSMs). The strength of supporting FIPS is in its cryptographic key and security parameter protection and in its inherent threat defense. FIPS delivers multi-layered, physical, and logical security, and protects data against theft and attacks at layer 7 (such as SSL and HTTP attacks), in addition to layers 3 and 4 (including network and DNS attacks). An HSM secures the cryptographic operations and protects critical cryptographic keys—segregating administrative and security domains and enforcing policies over key usage. Both FIPS support and HSMs enable SSL Orchestrator to deliver enhanced security and encryption key protection, while delivering superior cost efficiency.

SSL Orchestrator centralizes and enables consistent encryption policies, which strengthens SSL infrastructure security. It also supports Perfect Forward Secrecy (PFS), assuring against compromise. And, SSL Orchestrator enables smart, dynamic bypass of sensitive traffic, such as user personal financial or personal healthcare information (PHI), without conceding security or user privacy.

Lowers Security TCO

SSL Orchestrator optimizes and maximizes the efficacy of an organization's existing security solutions. It ensures encrypted threat protection while enhancing the effectiveness, economics, and lifecycle of deployed solutions in an organization's security stack.

SSL Orchestrator accomplishes this through its intelligent decrypted traffic steering and dynamic service chaining. Security against encrypted threats is enhanced by intelligently steering decrypted traffic—based on traffic awareness and context—to an appropriate security service chain leveraging policy. This subsequently reduces the over-subscription of security devices. Because SSL Orchestrator allows security solutions to work smarter and without a deluge of traffic being steered to them, organizations no longer require bigger and more costly versions of security solutions, which means performance increases. These factors lower security costs.

SSL Orchestrator provides centralized encryption management and administration, manages encryption keys with a single solution, increases security, and decreases human error. It also helps organizations save time and cost by relieving each security device in an organization of the need to perform these same functions, in some cases redundantly.

SSL Orchestrator monitors the health of existing, deployed security devices, balances traffic to the devices in an organization's existing security stack, and delivers unparalleled scalability for those devices—providing resilience in case of inspection device failure. By load balancing and health monitoring devices in the security stack, SSL Orchestrator reduces downtime, helping to alleviate a security service failure that could allow encrypted traffic bypassing the failed service and result in potential malware infiltration.

Running on F5 full proxy architecture, SSL Orchestrator enables architectural flexibility. It also includes access to powerful F5 iRules® programmability, enabling an organization to address specific requirements of its particular environment which increases security extensibility.

Encrypted traffic—and the need to decrypt, inspect, and re-encrypted checked and safe traffic—is significantly complex on its own. But it becomes exponentially more complex and challenging if each service handles those tasks independent of other services. Organizations may need to hire additional, trained personnel to handle the more complex and brittle architecture of an encrypted daisy chain which definitely increases costs.

With SSL Orchestrator offloading the computationally intensive task of decrypting and re-encrypting traffic—while also efficiently and smartly steering decrypted traffic to appropriately load balanced, scaled, and monitored security devices in an intelligent, context-based service chain—organizations require fewer security devices. And, the security devices that are necessary can be smaller and not over-subscribed. This significantly reduces security TCO.

Conclusion

Encryption is pervasive—and most security devices are not designed to perform SSL/TLS decryption at scale. Because attackers leverage this knowledge, it is common for threats to be hidden within encrypted payloads and for encrypted channels to be used to evade detection during data exfiltration. Solutions that only offer greater visibility into encrypted traffic aren't enough to defend data against these critical threats, and more robust protection can exhaust security investments and increase costs.

F5 is a proven and trusted leader in encryption, and particularly SSL. F5 SSL Orchestrator breaks the encrypted attack chain—ending encryption blind spots and halting exploitation, callback, and data exfiltration. SSL Orchestrator centralizes encryption, dynamically steering decrypted traffic to policy-based security service chains while intelligently bypassing sensitive encrypted data. It also optimizes and maximizes the effectiveness of an organization's existing security solutions by balancing security traffic loads and monitoring the health of security services, enabling optimal security performance and efficiency, eliminating security over-subscription, lowering TCO, and maximizing ROI without sacrificing data security and privacy.

DC0219 | OV-SEC-318179746