OVERVIEW

Decreasing Security Total Cost of Ownership with F5 SSL Orchestrator

Challenge

Attacks are increasing, and are becoming more sophisticated and complex. Addressing the onslaught and ferocity of attacks today, and in the future, is bound to increase the cost of securing your network, cloud, and applications. You'll need different security solutions that address specific attacks and breaches because "good enough" security never stops all attacks. Attackers only need to be good enough once to infiltrate your network, cloud, and applications to steal user credentials or data, making your company tomorrow's embarrassing headline.

The tip of the spear for the increase in attacks—and one of the core reasons security is going to cost you more—is the ever-increasing amount of encrypted traffic. It drives up costs for protecting user and customer data, as well as your intellectual property. Attackers commonly use encrypted payloads and channels to deliver malware and evade detection during data exfiltration. They even research and use specific ciphers that can exploit security product gaps that force a bypass of encrypted, malicious traffic.

While visibility into and inspection of SSL and TLS encrypted traffic should be required for any secure network, cloud, or application, it's only the starting point. Without the ability to centrally control, optimize, and implement decryption policies across the solutions in your security chain, not only will your costs increase exponentially, but so will successful attacks.

Solution

F5 SSL Orchestrator is specifically designed to enhance SSL/TLS infrastructure, provide security solutions with visibility into SSL/TLS encrypted traffic, and optimize your existing security investments. Through its dynamic service chaining and policy-based traffic steering, SSL Orchestrator applies context-based intelligence to encrypted traffic handling and lets you effectively manage the encrypted traffic flow across your security chain, while also ensuring optimal availability.

Designed to easily integrate with existing architectures and to centrally manage SSL/ TLS decryption and encryption, SSL Orchestrator delivers the latest SSL encryption technologies across your security infrastructure, maximizing and future-proofing your security service investments and lowering your total cost of ownership (TCO).

Decrypted SSL Load Balancing and Health Monitoring

SSL Orchestrator leverages F5 Networks' best-in-class load balancing, health monitoring, and SSL offload capabilities to scale your security services with high availability. Even if your organization handles substantial traffic loads, SSL Orchestrator is equipped to best optimize your security solutions. Through its built-in load balancing capabilities, SSL Orchestrator enables your security investments to scale and protect your network, clouds, applications, and data with multi-layered security, even in the most demanding environments. SSL Orchestrator optimizes your security services by dynamically scaling and intelligently routing encrypted traffic to an appropriate security service chain, defined and enforced by policy.

SSL Orchestrator also intelligently monitors the health and availability of the solutions in your organization's security chain, fortifying your network, cloud, application, and data security. Adding failover protection via SSL Orchestrator increases your security solution and services availability. SSL Orchestrator decreases the total cost of ownership of your security solutions while increasing your ability to better secure your network, clouds, and applications.

Encryption Management and Centralization

Most organizations don't have the ability to centrally control encryption and the ciphers that are its instruction sets. This lack of centralized management and control increases organizational security costs because ciphers need to be managed on a per solution basis. Plus, next-generation encryption protocols are evolving, along with industry best practices, toward increased security and privacy.

These new standards are driving the rapid adoption of SSL forward secrecy to improve network security. However, the migration to next-generation encryption can break passive SSL devices and bypass security controls, increasing your organization's risk of attack. SSL Orchestrator simplifies this complex situation by centrally managing encryption and its ciphers across your existing security infrastructure, lessening the burden on existing security solutions and on the staff responsible for managing them.

SSL Orchestrator's diverse cipher support prevents new security blind spots caused by encrypted traffic, delivering greater flexibility without requiring changes in network architecture. SSL Orchestrator supports Federal Information Processing Standards (FIPS) 140-2 requirements required by many government agencies and industries worldwide, which demand the highest standards in information, application, and data security. SSL Orchestrator also supports a variety of hardware security modules (HSM), providing an additional layer of encryption protection.

Privacy and Policy Enforcement

The concerns about user and data privacy are accelerating quickly. There's been an increase in national and state regulatory activity emphasizing the security of user, customer, and patient data, its use and misuse, and the need to maintain its privacy. For example, while the General Data Protection Regulation (GDPR) in the European Union (EU) doesn't require the encryption of user data, many organizations already are (or are beginning to) encrypt it. In addition, U.S. states are introducing legislation to protect user data, and the U.S. federal government may follow.

It's becoming clear that while visibility into encrypted traffic is vital, so is the ability to intelligently bypass decryption of some user data. SSL Orchestrator, with its full-proxy architecture, helps ensure that organizational policies on visibility into encrypted traffic, as well as those on privacy for user, customer, or patient data, are enforced. But SSL Orchestrator goes a step further: instead of blindly bypassing encrypted traffic, policy-enforced bypass is accomplished in a way that complies with legal and privacy expectations. By applying specific policies to visibility and inspection or intelligently bypassing decryption for select data, organizations are able to deliver confirmation of the intelligent policy actions taken—including logs and reports. These provide proof of adherence to corporate privacy policies and any industry or government regulations overseeing privacy, providing an audit trail and transparency into the privacy process followed.

Diverse Cipher and Protocol Management

Many security solutions and services rely on a store-and-forward, or client-side (referred to as a half-proxy) method of managing ciphers and protocols for encryption. That means those solutions and services rely on the client and server to directly negotiate the protocol and ciphers. If the client and server agree on a protocol or cipher that your security solutions and services don't support, then your security chain is broken. Or, the security solution or service that doesn't support the protocol or cipher must allow the encrypted traffic to bypass its security check. This can leave your organization open to threats from unchecked, encrypted traffic.

Attackers know which devices are unable to support which protocols or ciphers and how to sneak in malware and other malicious software via bypass. SSL Orchestrator's full-proxy architecture delivers robust, independent control of client- and server-side ciphers and protocols. The client negotiates the connection with SSL Orchestrator, which then negotiates the connection with the server. SSL Orchestrator's full-proxy architecture optimizes both the client and server connection based on their unique needs.

Because SSL Orchestrator manages the SSL negotiation, it can reduce or eliminate bypass events caused by new ciphers, addressing any necessary protocol transition. SSL Orchestrator not only protects the network, cloud, and applications via its cipher and protocol management, it also decreases the cost of managing ciphers and protocols for each security solution and service in your service chain, further reducing security TCO.

To learn more on how F5 SSL Orchestrator can trim your security TCO, please contact an F5 sales representative at sales@f5.com.

DC0119 | OV-SEC-306090294 | 0119