F5 SSL Orchestrator and Cisco Firepower NGFW

The Challenge

About 80% of all network traffic is now encrypted. Much of this encrypted traffic passes through enterprise networks without being inspected, creating major security blind spots. Organizations must be able to inspect traffic to protect against data loss, malware, viruses, trojans, and other potential security threats. Inspecting traffic that is encrypted means it must be decrypted prior to inspection and re-encrypted after inspection. But, visibility into—and decryption and re-encryption of—SSL/TLS traffic is only part of the solution. Orchestrating the decrypted SSL/TLS traffic and routing it to the appropriate, existing security infrastructure for inspection, ensuring security, is also a requirement.

Security stacks—including firewalls, intrusion prevention systems (IPS), data loss prevention (DLP), and web proxies—are typically not designed to efficiently decrypt SSL/TLS encrypted traffic at the scale and speed necessary for modern businesses. Decryption and encryption are computationally intensive tasks and performing decryption of SSL/TLS traffic on each device in a security stack can tremendously degrade the performance and cost-efficiency of those devices. This performance concern becomes even more challenging in the face of ever stronger ciphers and more complex encryption keys, creating serious risk for businesses.

Additional challenges are emphasized by the role businesses now must play in maintaining data privacy; see the European Union's General Data Protection Regulation (GDPR) as a prime example. IT administrators must balance the need to defend against threats with the need to ensure that private data remains private—and in most cases that means that private data must remain encrypted. Although challenging, identifying private data among all the encrypted traffic is a requirement.

The Cisco and F5 Joint Solution

In the face of modern threats, Cisco Firepower Next-Generation Firewall (NGFW) is a leading next-generation firewall and next-generation IPS. Cisco Firepower NGFW is built to block more threats and quickly mitigate those that do breach defenses with hardware and software options that combine Cisco's proven network firewall with the industry's most effective next-gen IPS and advanced malware protection (AMP).

With the Firepower series (named a Gartner Peer Insights Customers' Choice for enterprise network firewall), Cisco has delivered the industry's first fully integrated, threat-focused next-generation firewall with unified management. When working together with F5 SSL Orchestrator, the Cisco Firepower series' threat mitigation and performance capabilities can be fully utilized. F5 SSL Orchestrator performs the computationally heavy workload to decrypt traffic *before* distributing it to other devices in the security stack. This enables security stack devices to cost efficiently scale and perform the work that they are meant to do, and that they do best: ensuring security.

When Cisco Firepower NGFW is a part of your F5 SSL Orchestrator service chain, F5 centralizes decryption and re-encryption using best-in-class hardware acceleration with modern cipher implementations and software orchestration. This enables Cisco Firepower NGFW to focus on providing advanced threat protection before, during, and after attacks.

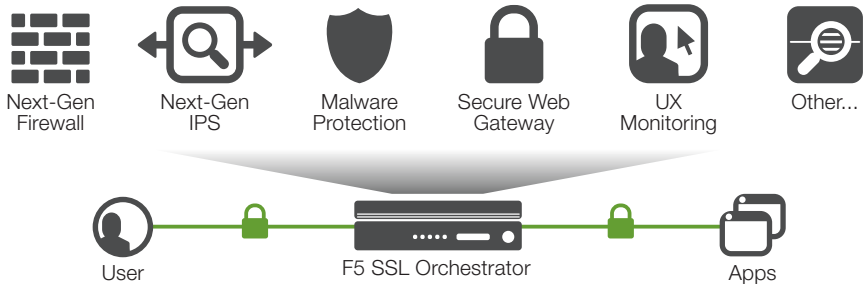

Diagram 1: F5 SSL Orchestrator is key to maximizing the efficiency and performance of a wide range of inspection devices—including Cisco Firepower NGFW—while maintaining optimal security.

As part of its traffic orchestration, F5 SSL Orchestrator identifies and categorizes encrypted traffic so that it is handled according to policy. This helps to ensure compliance with regulations and business practices. The orchestration capability enables policy-based steering of traffic. For example, privacy can be fully maintained for sensitive or regulated data without impacting inspection capabilities of other traffic.

Joint Solution Benefits

F5 SSL Orchestrator helps improve overall speed and efficiency of the security devices in your network's security stack, improving both cost efficiency and the user experience. While Cisco Firepower NGFW has onboard SSL decryption capabilities, many organizations choose to offload this work to F5 SSL Orchestrator so that all of the considerable horsepower of Cisco Firepower NGFW can be dedicated where it counts: to protecting your network.

The joint solution benefits include:

- **Actionability:** Combining the power of two actionable solutions, F5 SSL Orchestrator intelligently and automatically applies policies to act on your data by decrypting what is appropriate, routing it to other devices in the security stack, and then re-encrypting it afterwards. Cisco Firepower NGFW identifies and blocks threats, protecting data and mitigating harm.
- **Availability:** As scalability and uptime rely foremost on availability, F5 SSL Orchestrator increases availability by maximizing efficiency (taking the computational load off of Cisco Firepower NGFW). This ability to offload work from across the security stack is particularly critical for ensuring that your network is not overwhelmed by high volumes of traffic or distributed denial-of-service (DDoS) attacks.

- **Orchestration:** SSL Orchestrator excels at context- and policy-based visibility to maximize productivity of your security stack and protect against revenue loss, brand degradation, and other negative impacts. A powerful intelligence engine discerns context (i.e., the nature of the traffic based on server mapping, as well as other contextual awareness regarding which traffic originates where) and gives you the ability to implement policy based on this context. Its orchestration capabilities efficiently optimize the abilities of Cisco Firepower NGFW and other security devices (web proxies, IPS, DLP, etc.). Intelligent organization and management improves network performance, security, and the user experience.
- **Investment protection:** A divide-and-conquer approach protects your existing investments in firewall, IPS, and other security devices by ensuring that even as traffic volume grows and encryption becomes more complex these devices are not overwhelmed with de-/re-encryption functions. These duties are capably handled by F5 SSL Orchestrator.
- **Ease of use:** Without F5 SSL Orchestrator, setting up decryption zones is difficult and often requires the security team to resort to manual daisy-chaining or tedious configuration to manage decryption/encryption across the entire security stack. F5 SSL Orchestrator supports multiple deployment models simultaneously (inline layer 3, inline layer 2, ICAP, receive-only, *and* HTTP security services such as web proxy and/or secure web gateway) and delivers high levels of automation to ensure speedy deployments and ongoing utility.

To find out how our joint solutions can help your business please contact info@f5.com or partnering-csta@cisco.com, or visit f5.com/products/security/ssl-orchestrator.

Resources:

The F5 SSL Orchestrator and Cisco Firepower Solution: SSL Visibility with Service Chaining for Advanced Malware Protection (recommended development practices)

Cisco Firepower NGFW

Cisco Firepower Support Documentation and Software

DC1018 | OV-SEC 280003352 | 1018