F5 SSL ORCHESTRATOR AND CISCO WSA JOINT SOLUTION

While encryption helps keep our information and data private, it also increases the risk of attacks and data breaches. The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS) have been widely adopted by organizations worldwide to secure IP communications, and their usage continues to rise rapidly. While SSL/TLS provides data privacy and secure communications, it also creates challenges in the security stack when inspecting encrypted traffic.

With over 80% of global traffic encrypted, it's now easier for attackers to hide malicious payloads in encrypted traffic and launch their attacks. However, it makes it more difficult for IT teams to protect their organizations from those attacks.

Decrypting SSL/TLS encrypted traffic on security inspection devices via native decryption support takes a lot of computing power. Instead of burdening best-of-breed security solutions with decrypting traffic, it makes more sense to offload decryption and encryption management tasks to a dedicated solution. The F5 and Cisco integrated solution addresses SSL/TLS challenges while also ensuring web security and high performance.

THE CISCO AND F5 SOLUTION

F5® SSL Orchestrator™ and Cisco Web Security Appliance (WSA) integrate to deliver centralized visibility, orchestration, security, and control of web traffic, optimizing protection from web-based threats against any device.

Cisco® WSA combats advanced web security threats, provides strong protection and consistent control across all endpoints and everywhere in between. That includes mobile devices, web-enabled and mobile applications, and web browsers addressing the challenges of securing and controlling web traffic easily and quickly.

Cisco WSA combines Advanced Malware Protection (AMP), Cognitive Threat Analytics (CTA), and Application Visibility and Control (AVC), augmented with enhanced file reputation, continuous file analysis acceptable-use policies, insightful reporting, and highly secure mobility—all available on a single, easy-to-manage platform. Cisco WSA also has the sophistication required to stay one step ahead of cyber threats, as well as the ability to scale to meet the demands of today's business.

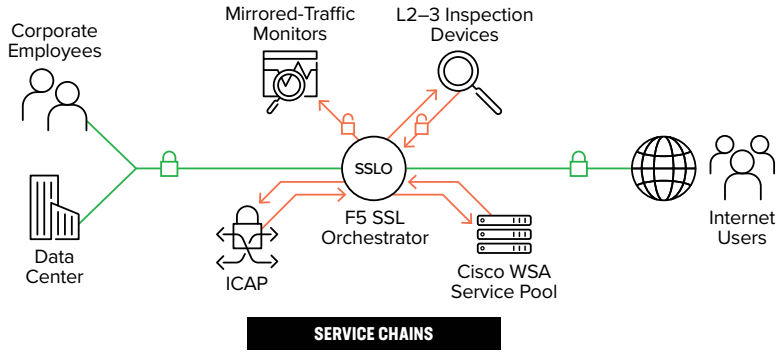

Figure 1: Traffic flow for the integrated F5 SSL Orchestrator with Cisco WSA in the service chain.

F5 SSL Orchestrator provides SSL/TLS offloading, visibility, and intelligent steering through the creation of dynamic service chains. A service chain is a defined, ordered set of security services, deployed in various configurations (L2, L3, Proxy, ICAP, TAP), and supports a wide range of common configurations.

Once traffic is decrypted using SSL Orchestrator, a steering decision is applied based on a number of criteria including source and destination IP, geolocation, and many others. Once the steering is determined, the traffic will be sent, unencrypted, through the optimal service chain and security stack. Then, it'll be re-encrypted and sent on to its destination.

SSL Orchestrator uses hardware acceleration and performs health monitoring, load balancing, and other services to make sure security inspection devices, including Cisco WSA, are running at optimum efficiency. Personal data, including financial- and health-related information, can be intelligently bypassed based on policy, allowing it to circumvent service chaining or not, depending on policy.

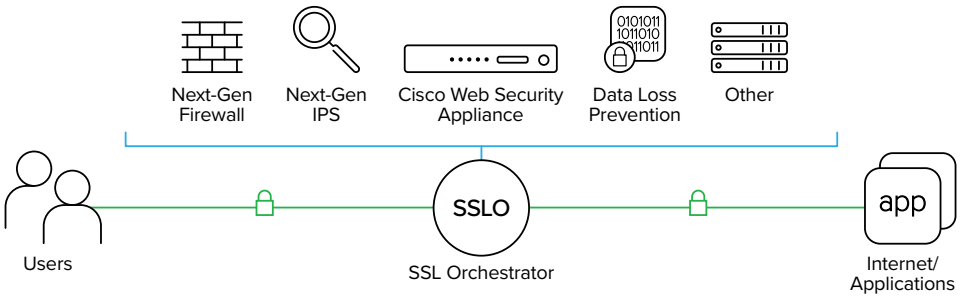

Figure 2: F5 SSL Orchestrator and Cisco WSA working together to provide advanced web security that maximizes efficiency and performance.

KEY SOLUTION BENEFITS

The F5 and Cisco integrated solution enhances security against hidden threats that attackers use to exploit vulnerabilities, establish command-and-control channels, and steal data. The F5 and Cisco solutions work together to intelligently manage SSL/ TLS and optimize—even enhance—security capabilities.

THESE SOLUTIONS WORK TOGETHER TO ENABLE ADVANCED WEB SECURITY WITH MAXIMUM EFFICIENCY AND PERFORMANCE

Some of the key benefits of the F5 and Cisco integrated solution include:

- **Optimal web security:** The integrated F5 and Cisco solution optimizes security while maximizing efficiency. Offloading computationally intensive decryption and re-encryption (including encryption management) tasks onto SSL Orchestrator ensures that the web security threat mitigation, malware protection, threat analytics, and application visibility and control of Cisco WSA operates at peak performance and efficiency.
- **Enhanced protection:** Combining Cisco WSA's enhanced protection from web threats with SSL Orchestrator's visibility into encrypted traffic and intelligent traffic steering, better and more quickly secures organizations against attacks that can lead to lost data and revenue, regulatory fines, loss of brand reputation, and other negative business impacts.

- **Cost-efficiency:** The real and virtual costs of traffic decryption and re-encryption continue to rise as new encryption ciphers become more sophisticated and complex. By deploying the integrated F5 SSL Orchestrator and Cisco WSA solution, organizations can enjoy a decrease in security total cost of ownership (TCO) and a quicker security return on investment (ROI) via complete, optimal web security without the burden of computationally intense decryption and re-encryption, centralized encryption management, and health monitoring, load balancing, and scale over multiple devices.

To find out how our joint solutions can help your business please contact Sales@f5.com or Partnering-csta@cisco.com or visit: f5.com/cisco.

ADDITIONAL RESOURCES

F5 SSL Orchestrator Web Page

The F5 SSL Orchestrator and Cisco WSA Recommended Practices Guide