F5 SSL Orchestrator and Dynamic Service Chains

KEY BENEFITS

Gain visibility into encrypted traffic.
Expose hidden threats with centralized decryption for the whole network stack.

Maximize security investment.
Optimize performance with efficient management of inbound and outbound encrypted traffic.

Improve risk management and privacy.
Implement policies to effectively balance security and privacy.

Organizations need to protect critical assets from threats that originate both outside and inside the corporate environment. However, most traffic is now encrypted, and existing security controls are unable to perform decryption at the scale required to enable inspection, leaving critical assets vulnerable. F5 SSL Orchestrator provides policy-based orchestration to enable cost-effective visibility across the full security chain for any network topology, device, or application.

Challenge

Privacy concerns have driven growth in encrypted traffic, with over 80% of page loads now encrypted with SSL/TLS. This growth presents a challenge: attackers commonly hide threats within encrypted payloads and use encrypted channels to evade detection during data exfiltration. They select specific cipher primitives based on known security product gaps to force encrypted bypass. Most organizations lack a central control to implement decryption policies across the multiple security inspection devices commonly found in the security chain. Security teams must resort to daisy-chaining devices or tedious manual configuration to support inspection across the security chain, increasing latency, complexity, and risk.

Solution

F5 SSL Orchestrator provides high-performance decryption of inbound and outbound SSL/TLS traffic, enabling security inspection to expose threats and stop attacks. Dynamic service chaining and policy-based traffic steering allow organizations to intelligently manage encrypted traffic flows across the entire security chain with optimal availability.

SSL Orchestrator ensures encrypted traffic can be decrypted, inspected by security controls, then re-encrypted, delivering enhanced visibility to mitigate threats traversing the network. As a result, organizations maximize their security services investment for malware, data loss prevention (DLP), ransomware, and next-generation firewalls (NGFW), thereby preventing inbound and outbound threats, including exploitation, callback, and data exfiltration.

FEATURES

SSL Orchestrator enables teams to streamline security service deployment, delivering greater agility, control, and visibility for encrypted environments.

SSL Visibility

- SSL decryption/re-encryption
- Strong cipher support
- Support for inbound and outbound encrypted traffic
- Support for L2

Dynamic Service Chaining

- Service insertion
- Service resiliency
- Service monitoring
- Load balancing

Context Engine

- Geolocation
- IP reputation
- URL categorization
- Source and destination

Granular Control

- Header changes
- Support for port translation
- Robust proxy-level control over ciphers and protocols

Deployment Modes

- Inline layer 3
- Inline layer 2
- ICAP services
- Receive-only
- Tap

Deploy in any environment

SSL Orchestrator supports multiple deployment modes, easily integrating into complex architectures to centralize decryption functions for both inbound and outbound traffic. SSL Orchestrator supports multiple inbound and outbound topology modes, including inbound layer 2/3, outbound L2, and outbound explicit/transparent proxy, along with multiple security devices, including inline layer 2/3, Tap, web proxies, receive-only, and ICAP-based devices.

Optimize operational efficiencies

Security teams are accustomed to manually connecting point products, creating a daisy-chained security stack consisting of multiple components. A typical stack may include components such as NGFW, DLP scanners, web application firewalls (WAF), intrusion prevention systems (IPS), malware analysis tools, and more.

Statically configured security chains are operationally inefficient and fail to adapt to changing network conditions. SSL Orchestrator can dynamically chain security devices, independently monitor and scale them, and intelligently manage decryption across the entire security chain with a contextual classification engine. Dynamic service chaining and policy-based traffic steering reduces operational costs and transforms daisy-chained security devices into highly available security services.

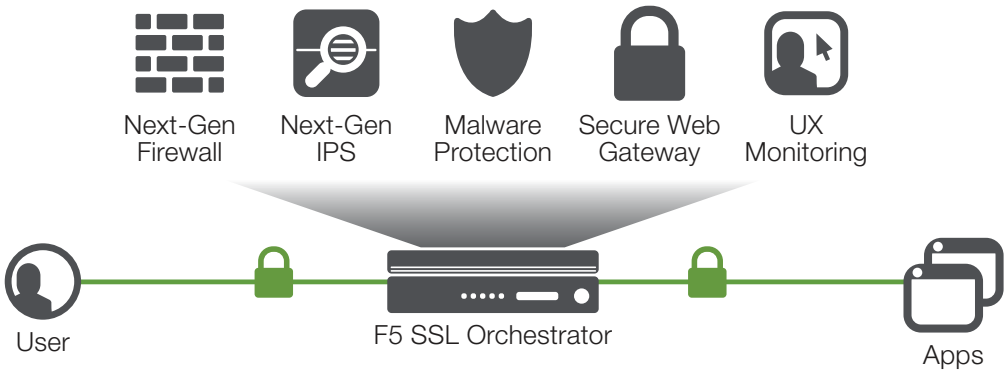

Figure 1: F5 SSL Orchestrator dynamic service chaining.

To learn more about SSL Orchestrator and other security solutions, contact an F5 sales representative at sales@f5.com.

DC0718 | OV-SEC 247943687 | 0718