Dynamic Service Chaining with F5 SSL Orchestrator

KEY BENEFITS

Gain visibility into SSL traffic with centralized SSL decryption across multiple security tools.

Dynamically chain services based on context-based policy to efficiently deploy security.

Choose from flexible deployment options for ease of integration with unique network topologies.

Protect existing investments in security infrastructure with better availability and utilization.

Provisioning network and security services—such as firewalls and security gateways—can be time-intensive and error-prone when deploying SSL inspection. F5® SSL Orchestrator™ reduces the risk through dynamic service chaining, which enables automatic insertion of physical or virtual security service appliances.

Challenge

Privacy concerns are driving a growth in encrypted traffic, which is expected to represent 70 percent of all Internet traffic this year. This growth in secure socket layer (SSL) encryption presents a challenge for enterprises, because without security tools to inspect SSL traffic, attacks can go undetected. In several cases, attackers have cleverly installed web shells on servers that used SSL encryption. As result, all requests to and from the back door were encrypted with the server's own legitimately installed private key. Because the network architectures had not been configured to permit inspection of SSL traffic, the attackers' actions went undetected.

Solution

F5 SSL Orchestrator provides high-performance decryption and encryption of outbound SSL/TLS traffic, enabling traffic inspection to reveal and stop hidden threats. The device also supports policy-based management and steering of traffic flows to third-party security solutions so organizations can apply context-based intelligence to the handling of encrypted traffic flows.

Leveraging the URL filtering and SSL inspection capabilities of F5 platforms and technologies, SSL Orchestrator ensures that select traffic can be decrypted, inspected by third-party solutions, and then re-encrypted, delivering enhanced visibility to threats traversing the network. As a result, organizations can prevent attacks at multiples stages, including exploitation, callback, and data exfiltration.

Service chaining to maximize security investments and lower TCO

Typical security stacks often begin with a firewall but almost never stop there. To solve specific security challenges, security administrators are accustomed to manually chaining multiple point products, creating a bare-bones security stack consisting of multiple services. A typical stack may include components such as data loss prevention (DLP) scanners, web application firewalls, intrusion prevention systems (IPS), malware analysis tools, and more.

All user sessions are applied with the same level of security because the chain is statically configured. SSL Orchestrator can dynamically chain security services (including anti-virus/malware products, intrusion detection systems (IDS), IPS, next-generation firewalls, and DLP) by matching the URL and policies that determine whether traffic should bypass or be decrypted and sent to one service or another. This policy-based traffic steering capability reduces administrative costs and enables organizations to gain more value from the investments they've made in these security services.

Higher availability and flexible deployment options

SSL Orchestrator supports multiple deployment modes, easily integrating into even complex architectures to centralize the SSL decrypt/encrypt function and deliver the latest encryption technologies across the entire security infrastructure. The solution enhances flexibility through the programmability of F5 iApps® Templates, integrated network address translation, and single or two-box physical modes. At the same time, SSL Orchestrator's service chaining and load balancing increase availability for connected security solutions.

Features

SSL Orchestrator features enable security 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 one and two-box deployments

Dynamic Service Chaining
Service insertion
Service resiliency
Service monitoring
Load balancing

Context Engine
Geolocation
IP reputation
URL categorization
Source and destination

Multi-Layer Context
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

OV-SEC-93160422-ssli 0616