F5 SSL ORCHESTRATOR

WHAT'S INSIDE

3 Centralize SSL decryption across multiple security tools

3 Inspect next-generation encryption protocols

3 Simplify change management through security stack orchestration

3 Improve scalability and availability of your existing security tools

4 Configure dynamic service chaining based on context

5 Deploy with flexible options that ease integration

5 Partners

6 Features

11 More information

KEYS TO ENCRYPTED THREAT PROTECTION: VISIBILITY INTO AND ORCHESTRATION OF ENCRYPTED TRAFFIC

The ever-increasing volume of encrypted traffic is hampering the ability of IT and security operations (SecOps) teams to protect their applications, customer data, and intellectual property. Traditional security gateways, network firewalls—even next-generation firewalls (NGFWs)—and intrusion prevention systems (IPS) are increasingly running blind to SSL/TLS traffic. Attackers commonly hide threats within links to encrypted websites or encrypted payload attachments in phishing and spear phishing emails, and they use encrypted channels to evade detection during data exfiltration. They will select specific cipher primitives based on known security product gaps to force bypass of encrypted malicious traffic. The growth in SSL/TLS encryption is a challenge for enterprises, because without security tools able to inspect inbound and outbound SSL/TLS traffic efficiently at scale, encrypted attacks go undetected and expose your applications and data to breaches.

Visibility into and inspection of SSL/TLS traffic only scratches the security surface, though. Most organizations lack the ability to centrally control and implement decryption policies across the multiple existing and deployed security inspection devices commonly found in an organization's security stack. Many organizations resort to daisy-chaining devices or tedious, manual configurations to support inspection across the security stack—increasing latency, complexity, and risk.

F5® SSL Orchestrator® was designed and purpose-built to enhance SSL/TLS infrastructure, provide security solutions with visibility into SSL/TLS encrypted traffic, and optimize and maximize your existing security investments. SSL Orchestrator delivers dynamic service chaining and policy-based traffic steering, applying context-based intelligence to encrypted traffic handling to allow you to intelligently manage the flow of encrypted traffic across your entire security stack, ensuring optimal availability. Designed to easily integrate with existing architectures and to centrally manage the SSL/TLS decrypt/encrypt function, F5 SSL Orchestrator delivers the latest SSL encryption technologies across your entire security infrastructure. With SSL Orchestrator's high-performance encryption and decryption capabilities, your organization can quickly discover hidden threats and prevent attacks at multiple stages, leveraging your existing security solutions.

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, you can maximize your 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.

KEY BENEFITS

Enables visibility into SSL/TLS traffic with centralized decryption/encryption function for inspection across multiple security tools.

Provides high-performance decryption of inbound and outbound SSL/TLS traffic, enabling security inspection to expose threats and stop attacks such as phishing, spear phishing, and ransomware.

Dynamically chains security devices, independently monitors and scales them, and intelligently manages decryption across the entire security chain via a contextual classification engine, reducing administrative costs while utilizing security resources more efficiently.

Delivers a single platform for unified inspection of next-generation encryption protocols, providing unparalleled flexibility, minimizing architectural changes, and preventing new security blind spots.

Shortens the typically cumbersome, time-consuming change management process by orchestrating the security stack, simplifying equipment changes and mitigating their detrimental impact.

Flexibly integrates into even the most complex architectures, centralizing SSL decrypt/encrypt functions and delivering the latest encryption technologies across the entire security infrastructure.

Scales security services with high availability, leveraging F5's best-in-class load balancing, health monitoring, and SSL offload capabilities.

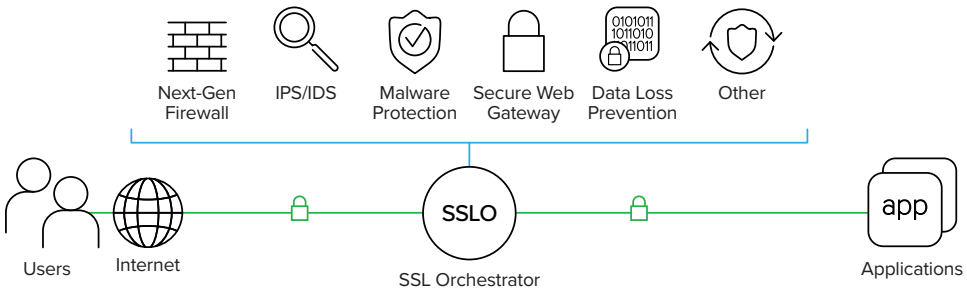


Figure 1: F5 SSL Orchestrator maximizes efficiency and performance for a wide range of inspection devices while maintaining optimal security.

CENTRALIZE SSL DECRYPTION ACROSS MULTIPLE SECURITY TOOLS

F5 SSL Orchestrator provides decryption and re-encryption of user traffic bound to the Internet and web-based applications, enabling security inspection. The solution supports policy-based management and steering of traffic flows to third-party security devices such as firewalls, IPSs, anti-malware, DLPs, secure web gateways (HTTP proxy services), and forensics tools. Centralizing the SSL/TLS decrypt/encrypt function enables you to realize the full value of your security investments. This multi-vendor ecosystem approach allows the inspection of all traffic inbound and outbound for malware and exfiltration.

INSPECT NEXT-GENERATION ENCRYPTION PROTOCOLS

Next-generation encryption protocols are evolving with industry best practices for increased security and privacy. New emerging standards encourage rapid adoption of SSL forward secrecy for improved network security. The transition to next-generation encryption breaks passive SSL devices, bypassing your security controls and putting you, your network, your apps, and your data at risk. Diverse cipher support by F5 SSL Orchestrator prevents new blind spots by enabling greater flexibility without requiring architectural changes.

SIMPLIFY CHANGE MANAGEMENT THROUGH SECURITY STACK ORCHESTRATION

Making necessary equipment changes or swaps in daisy-chained security stacks are difficult and time-consuming. Changes or swaps increase operational and business costs, cause delays, and can create unintended encrypted traffic bypasses, expanding risks and the threat threshold for your applications and data. Security stack orchestration with F5 SSL Orchestrator simplifies equipment changes, lessens change time, cost, and impact, and alleviates prospective traffic bypass and potential exploitation.

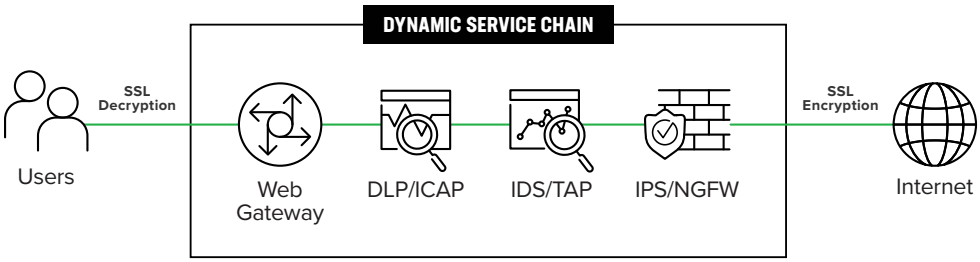
IMPROVE SCALABILITY AND AVAILABILITY OF YOUR EXISTING SECURITY TOOLS

Enterprises with substantial traffic loads will optimize security deployments by leveraging the health monitoring, load-balancing, and SSL offload capabilities of F5 SSL Orchestrator. These capabilities enable your security investments to better scale and protect through multi-layered security, even in the most demanding environments. Scaling your existing, deployed security devices with failover protection achieves better utilization and service availability.

CONFIGURE DYNAMIC SERVICE CHAINING BASED ON CONTEXT

SSL Orchestrator dynamically chains security services, including anti-virus/malware products, intrusion detection systems (IDS), IPSs, NGFWs, secure web gateways (HTTP proxy services), and DLPs. It leverages classification metrics such as domain name, content category, geolocation, IP reputation, and other policies that determine whether to decrypt traffic and which services traffic should be sent to. The policy-based traffic steering capabilities of SSL Orchestrator also increase administrative efficiency and reduce administrative cost by removing key and certificate management from your security infrastructure.

Figure 2: SSL Orchestrator enables the creation of dynamic security service chains.



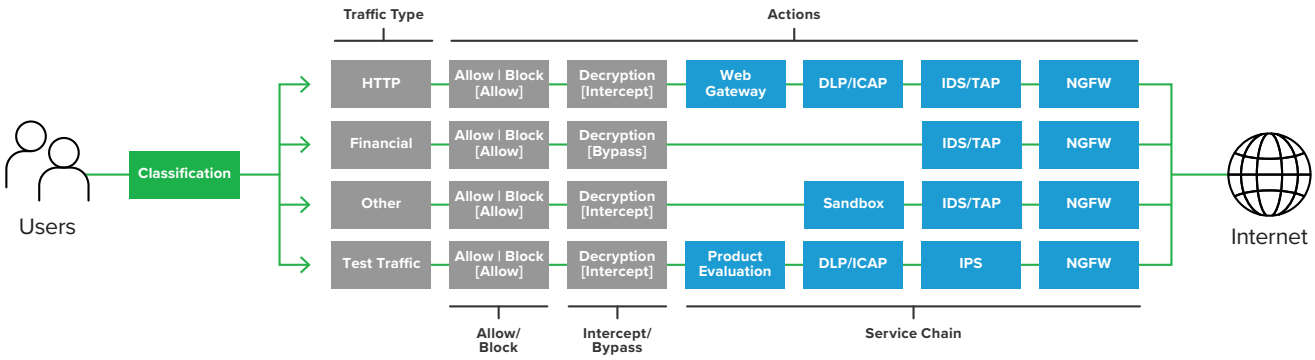


Figure 3: Leveraging its context-aware policy engine, SSL Orchestrator steers decrypted traffic to the appropriate security service chain and can perform an intelligent bypass on sensitive user traffic, such as financial or health-care related traffic.

DEPLOY WITH FLEXIBLE OPTIONS THAT EASE INTEGRATION

SSL Orchestrator supports multiple deployment modes, easily integrating into even the most complex of architectures. This centralizes SSL/TLS decrypt/encrypt services and delivers the latest encryption technologies across your entire security infrastructure. It eliminates your organization's need to re-architect the network to enable visibility into encrypted traffic, orchestrating and effectively routing traffic to the appropriate security services—in addition to dynamically chaining the appropriate security services. That helps to better utilize, preserve, and future-proof your security solution investments. In addition, SSL Orchestrator includes a step-by-step Guided Configuration to help your IT or SecOps teams logically walk through the deployment within your existing architecture and with your existing security solutions. The Guided Configuration simplifies deployment of SSL Orchestrator and enables you and your organization to be better protected, sooner, against the onslaught of encrypted threats.

PARTNERS

F5 has developed—and continues to develop—an ever-expanding security solution ecosystem for SSL Orchestrator. While SSL Orchestrator is vendor and product agnostic, F5 has optimized integration solutions for leading tools from partners such as Cisco, FireEye, Palo Alto Networks, and others.

The following Recommended Practices Guides, with reference architectures, provide granular, prescriptive guidance for deployment:

- Broadcom Symantec Data Loss Prevention (DLP)
- Cisco Firepower Threat Defense
- Cisco Web Security Appliance (WSA)
- FireEye NX
- McAfee Data Loss Prevention (DLP)
- McAfee Web Gateway
- Menlo Security Web Isolation Platform
- Palo Alto Networks NGFW

FEATURES

F5 SSL Orchestrator enables your security team to streamline security service deployment, delivering greater agility, control, and visibility into encrypted traffic.

SSL visibility

- High performance SSL/TLS decryption/re-encryption
- Inspection of inbound and outbound encrypted traffic
- Supports L3 (routed) and L2 (transparent) modes
- Forward and reverse proxy architecture
- SSL/TLS decryption independent of TCP port

Dynamic service chaining

- Policy-based steering of decrypted traffic
- Decoupled from physical interface, port, or VLANs
- Simplified security service insertion
- Service resiliency
- Service monitoring
- Load balancing of multiple security devices

Contextual policy engine

- Source and destination IP and subnet port
- Protocol
- Domain
- IP geolocation
- IP reputation (subscription)
- URL categorization (subscription)
- Policy-based block, bypass, and forward for inspection actions

Granular control

- Header changes
- Support for port translation

Robust cipher and protocol support

- TLS 1, 1.1, 1.2, 1.3
- Forward secrecy/perfect forward secrecy encryption
- RSA/ECDSA/DHE/ECDHE
- AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA/SHA2 (SHA256/384), Chacha20-Poly1305
- Proxy-level control over ciphers and protocols

Deployment modes

- Outbound layer 3 explicit proxy
- Outbound layer 3 transparent proxy
- Inbound layer 3 reverse proxy
- Outbound layer 2
- Inbound layer 2
- High availability with TCP session resiliency

Supported service types

- HTTP proxy services
- Inline layer 3 services
- Inline layer 2 services
- ICAP/DLP services
- TAP services

Reporting and logging

- On-board analytics dashboard

Network hardware security module (HSM)

- Thales (Gemalto, SafeNet)
- Atos
- AWS CloudHSM
- Equinix SmartKey (Fortanix)
- Entrust (nCipher)

Add-ons

- IP Intelligence Services (subscription feed)
- URL filtering
- Network HSM
- F5 BIG-IP Access Policy Manager (APM)
- F5 Secure Web Gateway Services

SPECIFICATIONS	i15800	i11800/i11800-DS*
Processor:	Two 14-Core Intel Xeon processors (total 56 hyperthreaded logical processor cores)	One 18-Core Intel Xeon processor (total 36 hyperthreaded logical processor cores)
Memory:	512 GB DDR4	256 GB DDR4
Hard Drive:	1x 1.6 TB Enterprise Class SSD	1x 960 GB Enterprise Class SSD (i11800) Dual SSD 2x 960 GB Enterprise Class SSD (i11800-DS)
Gigabit Ethernet CU Ports:	N/A	Optional SFP
Gigabit Fiber Ports (SFP):	N/A	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	N/A	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	8 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	6 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
100 Gigabit Fiber Ports (QSFP28)	4 SR4/LR4 (sold separately) QSFP28	N/A
SSL Orchestrator Throughput (Maximum):		
Receive Only:	22.7 Gbps	18.9 Gbps (i11800); 30.5 Gbps (i11800-DS)
L3 Inline Service:	22.9 Gbps	19.1 Gbps (i11800); 31.5 Gbps (i11800-DS)
L3 Inline + (1) L2 Service:	22.9 Gbps	17.9 Gbps (i11800); 27.1 Gbps (i11800-DS)
L3 Inline + (2) L2 Services:	22.8 Gbps	16.9 Gbps (i11800); 13.2 Gbps (i11800-DS)
For each additional L2 service:	-1.3 Gbps	-1.9 Gbps (i11800); -5.1 Gbps (i11800-DS)
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
Receive Only:	41.8 K	24.7 K (i11800); 31.7 K (i11800-DS)
L3 Inline Service:	41.2 K	25.0 K (i11800); 30.9 K (i11800-DS)
L3 Inline + (1) L2 Service:	37.3 K	24.0 K (i11800); 27.2 K (i11800-DS)
L3 Inline + (2) L2 Services:	34.3 K	23.2 K (i11800); 24.5 K (i11800-DS)
For each additional L2 service:	-2.9 K	-2.9 K (i11800); -2.5 K (i11800-DS)
L3 Inbound Topology:		
Receive Only:	76.7 K	45.8 K (i11800); 57.5 K (i11800-DS)
L3 Inline Service:	74.0 K	45.5 K (i11800); 56.4 K (i11800-DS)
L3 Inline + (1) L2 Service:	65.4 K	45.2 K (i11800); 47.4 K (i11800-DS)
L3 Inline + (2) L2 Services:	57.8 K	39.4 K (i11800); 41.0 K (i11800-DS)
For each additional L2 service:	-7.0 K	-3.6 K (i11800); -5.9 K (i11800-DS)
SSL Orchestrator Concurrent Sessions:		
L3 Outbound	5500 K (5.5 M)	3100 K (3.1 M)
L3 Inbound	6200 K (6.2 M)	3400 K (3.4 M)

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System datasheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. Please refer to the Platform Guide: i15000 Series or Platform Guide: i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

*More information on additional dedicated cryptographic hardware on the DS Series is available in the BIG-IP System datasheet, which also provides complete specifications on all BIG-IP iSeries platforms.

SPECIFICATIONS	i10800	i7800
Processor:	One 8-core Intel Xeon processor (total 16 hyperthreaded logical processor cores)	One 6-core Intel Xeon processor (total 12 hyperthreaded logical processor cores)
Memory:	128 GB DDR4	96 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD Model with dual SSDs in RAID 1 also available	1x 480 GB Enterprise Class SSD Model with Dual SSDs in RAID 1 also available
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR/LR (sold separately); optional 10G copper direct attach	8 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	6 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10 GB ports)	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
SSL Orchestrator Throughput (Maximum):		
Receive Only:	18.2 Gbps	10.9 Gbps
L3 Inline Service:	19.0 Gbps	11.1 Gbps
L3 Inline + (1) L2 Service:	16.2 Gbps	11.0 Gbps
L3 Inline + (2) L2 Services:	13.2 Gbps	9.1 Gbps
For each additional L2 service:	-2.2 Gbps	-1.3 Gbps
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
Receive Only:	17.0 K	12.1 K
L3 Inline Service:	16.7 K	13.0 K
L3 Inline + (1) L2 Service:	15.0 K	12.3 K
L3 Inline + (2) L2 Services:	13.6 K	11.1 K
For each additional L2 service:	-1.3 K	-0.9 K
L3 Inbound Topology:		
Receive Only:	36.1 K	23.0 K
L3 Inline Service:	35.2 K	23.0 K
L3 Inline + (1) L2 Service:	28.5 K	22.6 K
L3 Inline + (2) L2 Services:	24.3 K	19.7 K
For each additional L2 service:	-4.1 K	-2.0 K
SSL Orchestrator Concurrent Sessions:		
L3 Outbound	1400 K (1.4 M)	1000 K (1.0 M)
L3 Inbound	1600 K (1.6 M)	1200 K (1.2 M)

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System datasheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. SFP+ ports in i10800 are compatible with F5 SFP modules. Please refer to the Platform Guide for i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

SPECIFICATIONS	i5800	i4800
Processor:	One 4-core Intel Xeon processor (total 8 hyperthreaded logical processing cores)	One 4-core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
Memory:	48 GB DDR4	32 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD	1x 500 GB Enterprise Class HDD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	8 SX or LX (sold separately)
10 Gigabit Fiber Ports (SFP+):	8 SR or LR (sold separately); optional 10G copper direct attach	4 SR/LR (sold separately); optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	N/A
SSL Orchestrator Throughput (Maximum):		
Receive Only:	10.1 Gbps	6.2 Gbps
L3 Inline Service:	10.7 Gbps	6.4 Gbps
L3 Inline + (1) L2 Service:	9.1 Gbps	5.9 Gbps
L3 Inline + (2) L2 Services:	7.6 Gbps	4.7 Gbps
For each additional L2 service:	-1.3 Gbps	-0.8 Gbps
SSL Orchestrator Transactions/ Second (TPS):		
L3 Outbound Topology:		
Receive Only:	9.3 K	5.8 K
L3 Inline Service:	9.2 K	5.7 K
L3 Inline + (1) L2 Service:	8.2 K	4.7 K
L3 Inline + (2) L2 Services:	7.5 K	4.6 K
For each additional L2 service:	-0.8 K	-0.5 K
L3 Inbound Topology:		
Receive Only:	19.4 K	12.3 K
L3 Inline Service:	18.9 K	12.2 K
L3 Inline + (1) L2 Service:	15.4 K	8.3 K
L3 Inline + (2) L2 Services:	13.1 K	8.4 K
For each additional L2 service:	-2.3 K	-1.5 K
SSL Orchestrator Concurrent Sessions:		
L3 Outbound	500 K	300 K
L3 Inbound	610 K	375 K

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System datasheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. Please refer to the Platform Guide for i5000/i7000/i10000/i11000 Series or Platform Guide for i2000/i4000 for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

SPECIFICATIONS	i2800^
Processor:	One 2-core Intel Xeon processor (total 4 hyperthreaded logical processor cores)
Memory:	16 GB DDR4
Hard Drive:	1x 500 GB Enterprise Class HDD
Gigabit Ethernet CU Ports:	Optional SFP
Gigabit Fiber Ports (SFP):	4 SX or LX (sold separately)
10 Gigabit Fiber Ports (SFP+):	2 SR or LR (sold separately); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	N/A
SSL Orchestrator Throughput:	2.8 Gbps
SSL Orchestrator Transactions/ Second (TPS):	3800
SSL Orchestrator Concurrent Sessions:	150 K

For complete specifications on the BIG-IP iSeries platforms, please refer to the BIG-IP System datasheet.

Notes: Cipher string used: ECDHE-RSA-AES128-AES-GCM-SHA256. Only optics provided by F5 are supported. Please refer to the Platform Guide for i2000/i4000 for the latest power ratings for your specific configurations (number of PS, highline input voltage, DC, etc.).

^Supports a maximum of one additional service.

SPECIFICATIONS	VIPRION 4450 Blade	VIPRION 4340N/4300 Blade	VIPRION 2250 Blade
Processor:	2 Intel 12-core processors (48 hyperthreaded logical processor cores total)	2 Intel hex 6-core processors (total 24 hyperthreaded logical processor cores)	Single Intel 10-core Xeon processor (total 20 hyperthreaded logical processor cores)
Memory:	256 GB	96 GB (4340N); 48 GB (4300)	64 GB
Hard Drive Capacity:	1.2 TB SSD	600 GB hard drive	One 800 GB solid state drive

For complete specifications on all the VIPRION platforms, please refer to the VIPRION datasheet.

Notes: L2 virtual wire mode is only supported on the VIPRION 2250 and VIPRION 4450 blades. L2 virtual wire mode is *not* supported in any vCMP configuration. Inline layer 2 services are *not* supported in the following conditions: VIPRION 2250 blade on VIPRION 2400 chassis, VIPRION 4300 blade on VIPRION 4800 chassis, and VIPRION 4450 blade on VIPRION 4480 chassis.

HIGH PERFORMANCE VIRTUAL EDITION (VE)

SPECIFICATIONS	16vCP**	8vCP**
SSL Orchestrator Throughput:	9.3 Gbps**	7.1 Gbps**
SSL Orchestrator Transactions/Second (TPS):	8500**	4800**
SSL Orchestrator Concurrent Sessions:	330,000**	150,000**

** High Performance VE tests were run on a single dedicated host with SR-IOV enabled.

MORE INFORMATION

To learn more about F5 SSL Orchestrator, visit f5.com to find these and other resources.

Web page

F5 SSL Orchestrator

Solution overview

F5 SSL Orchestrator

Recommended practices guides

Broadcom Symantec Data Loss Prevention
Cisco Firepower Threat Defense
Cisco Web Security Appliance (WSA)
FireEye NX
McAfee Data Loss Prevention (DLP)
McAfee Web Gateway
Menlo Security Web Isolation Platform
Palo Alto Networks NGFW

DC1020 | DS-SEC-562428117