F5 SSL Orchestrator

DATASHEET

What's Inside

The Keys to Securing Data: Visibility into and Orchestration of Encrypted Traffic

The rising volume of encrypted traffic is hampering the ability of IT security teams to protect 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 encrypted payloads and 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 to inspect inbound and outbound SSL/TLS traffic, encrypted attacks go undetected and expose your 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 chain. Most organizations resort to daisy-chaining devices or tedious, manual configurations to support inspection across the security chain—increasing latency, complexity, and risk.

F5® SSL Orchestrator™ is purpose-built and designed to enhance SSL/TLS infrastructure, provide security solutions with visibility into SSL/TLS encrypted traffic, and optimize and maximize your existing security investments. F5 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 chain, 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 F5 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.

F5 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.

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.

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.

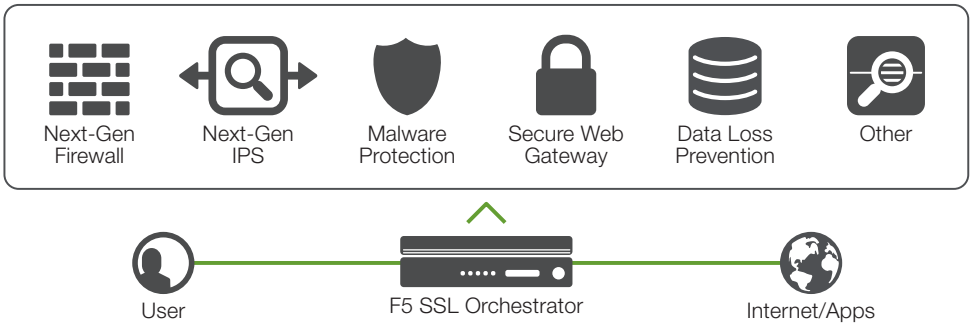

Figure 1: F5 SSL Orchestrator maximizes the efficiency and performance for a wide range of inspection devices while maintaining optimal security.

Centralized 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, intrusion prevention systems (IPS), anti-malware, data loss prevention (DLP), 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 leaving you, your network, and your data at risk. Diverse cipher support prevents new blind spots by enabling greater flexibility without requiring architectural changes.

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. This enables 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.

Dynamic service chaining based on context

F5 SSL Orchestrator dynamically chains security services, including anti-virus/malware products, intrusion detection systems (IDS), IPS, next-generation firewalls (NGFWs), secure web gateways (HTTP proxy services), and DLP. It leverages classification metrics such as domain name, content category, geolocation, IP reputation, and other policies that determine whether or not to decrypt, and to which services to send traffic. The policy-based traffic steering capabilities of F5 SSL Orchestrator also reduces administrative costs by removing key and certificate management from your security infrastructure.

Flexible deployment options provide ease of integration

F5 SSL Orchestrator supports multiple deployment modes, easily integrating into even the most complex of architectures. This centralizes SSL/TLS decrypt/encrypt 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—helping to better utilize, preserve, and future-proof your security solution investments.

Partners

F5 SSL Orchestrator has developed—and continues to develop—an ever-expanding security solution ecosystem. F5 SSL Orchestrator has been designed to interoperate with leading tools from partners such as Cisco, Symantec, FireEye, Palo Alto Networks, and others. The following Recommended Practices Guides provide granular, prescriptive guidance for deployment:

FireEye NX
Palo Alto Networks NGFW
Cisco ASA FirePOWER
Symantec DLP

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

Support for L2

Forward 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

Forward secrecy/perfect forward secrecy

RSA/DHE/ECDHE with forward secrecy support

SHA, SHA2, AES, AES-GCM

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

Network Hardware Security Module (HSM)

Thales

Gemalto

Add-ons

F5 IP Intelligence Services

URL filtering

Network HSM

F5 BIG-IP Access Policy Manager (APM)

F5 Secure Web Gateway Services

Specifications	i15800	i11800
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
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)
SSL Orchestrator Throughput:	24 Gbps	20 Gbps
SSL Orchestrator Transactions/Second (TPS):	53000	33000
SSL Orchestrator Concurrent Sessions:	7200K (7.2M)	3700K (3.7M)
Power Supply:	2x 1500W Platinum AC PSU	2x 650W Platinum AC PSU (2x 650W DC PSU Optional) 2x
Typical Consumption:	885W (dual power supply, 110V input)**	455W (dual power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	3020 BTU/hour (dual power supply, 110V input)*	1555 BTU/hour (dual power supply, 110V input)*
Dimensions:	3.45” (8.76 cm) H x 17.9” (45.47 cm) W x 30.2” (76.71 cm) D 2U industry standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis
Weight:	76 lbs. (34.47 kg) (Dual power supply)	36 lbs. (16.3 kg) (dual power supply)
Operating Temperature:	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Operational Relative Humidity:	5 to 85% at 40° C	5 to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.

* Maximum throughput.

** 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.).

Specifications	i10800	i5800
Processor:	One 8-Core Intel Xeon processor (total 16 hyperthreaded logical processor cores)	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processing cores)
Memory:	128 GB DDR4	48 GB DDR4
Hard Drive:	1x 480 GB enterprise class SSD	1x 480 GB enterprise class SSD
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 gigabit ports)	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
SSL Orchestrator Throughput:	15 Gbps	7.8 Gbps
SSL Orchestrator Transactions/Second (TPS):	20500	10600
SSL Orchestrator Concurrent Sessions:	1700K (1.7M)	600K
Power Supply:	2x 650W Platinum AC PSU (2x 650W DC PSU optional)	1x 650W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU optional)
Typical Consumption:	415W (dual power supply, 110V input)*	265W (single power supply, 110V input)*
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1420 BTU/hour (dual power supply, 110V input)*	905 BTU/hour (single power supply, 110V input)*
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industrial standard rack-mount chassis	1.72” (4.37 cm) H x 17.4” (44.2 cm) W x 30.6” (77.72 cm) D 1U industry standard rack-mount chassis
Weight:	36 lbs. (16.3 kg) (dual power supply)	26 lbs. (11.8 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5 to 85% at 40° C	5 to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A; EN 61000-3-2:2014 EN 61000-3-3:2013; EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported. SFP+ ports in i10800 are compatible with F5 SFP modules.

* Please refer to the Platform Guide: i10000 Series or i5000 Series for the latest power ratings for your specific configurations (SSL, SSD, 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:	150K
Power Supply:	1x 250W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU optional)
Typical Consumption:	95W (single power supply, 110V input)*
Input Voltage:	100–240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	325 BTU/hour (single power supply, 110V input)*
Dimensions:	1.72” (4.37 cm) H x 17.4” (44.2 cm) W x 22.5” (57.15 cm) D 1U industry standard rack-mount chassis
Weight:	20 lbs. (9.07 kg) (single power supply)
Operating Temperature:	32°F to 104°F
Operational Relative Humidity:	5% to 85% @ 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A: EN 61000-3-2:2014 EN 61000-3-3:2013: EN 55024:2010 FCC Class A (Part 15), IC Class A, VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
* Please refer to the Platform Guide: i2000 Series for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

Specifications	High Performance Virtual Edition (VE) 8vCP**	16vCP*
SSL Orchestrator Throughput:	7.1 Gbps**	9.3 Gbps**
SSL Orchestrator Transactions/Second (TPS):	4800**	8500**
SSL Orchestrator Concurrent Sessions:	150000**	330000**

** 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

FireEye NX
Symantec DLP
Palo Alto Networks NGFW
Cisco ASA FirePOWER

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com