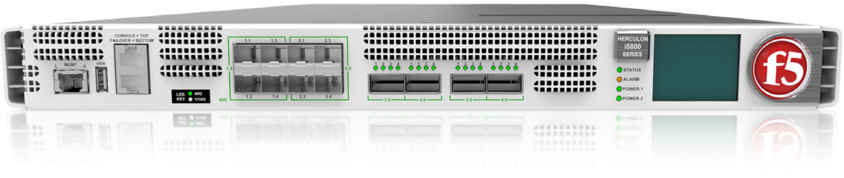
F5 Herculon SSL Orchestrator

DATASHEET

What's Inside



Visibility into Encrypted Traffic Is Key to Securing Your Data

Rising amounts of encrypted traffic are hampering the ability of IT security teams to protect customer data and intellectual property. Traditional security gateways, network firewalls, and intrusion prevention systems are increasingly running blind to SSL/TLS traffic. The growth in SSL encryption presents a challenge for enterprises, because without security tools to inspect SSL traffic, encrypted attacks go undetected and expose your data to breaches.

F5® Herculon™ SSL Orchestrator™ is an all-in-one appliance designed to optimize the SSL infrastructure, provide security solutions with visibility into SSL/TLS encrypted traffic, and maximize the use of your existing security investment. Herculon SSL Orchestrator supports policy-based management and steering of traffic flows to existing security solutions, and applies context-based intelligence to the handling of encrypted traffic. It is designed to easily integrate into existing architectures and centralize the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. With Herculon SSL Orchestrator's high-performance encryption and decryption capabilities, your organization can discover hidden threats and prevent attacks at multiple stages.

Key benefits

Gain visibility into SSL traffic with centralized decryption for inspection across multiple security tools. Re-encrypt user traffic bound to the Internet and web-based applications, enabling security inspection.

Use a single platform for unified inspection of next-generation encryption protocols. This allows for the greatest flexibility in minimizing architectural changes to prevent new blind spots from emerging.

Scale security services with high availability using best-in-class load balancing, health monitoring, and SSL offload capabilities.

Dynamically chain services to efficiently deploy security tools with context-based policies that reduce administrative costs and utilize security resources more effectively.

Integrate flexible deployment options into even the most complex architectures. Centralize the SSL decrypt/encrypt function and deliver the latest encryption technologies across the entire security infrastructure.

Centralized SSL Decryption Across Multiple Security Tools

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 (IPSs), anti-malware, data loss prevention (DLP), and forensics tools. Centralizing the SSL decrypt/encrypt function allows you to realize the full value of your security investments. This multi-vendor ecosystem approach enables the inspection of all your traffic for malware and exfiltration.

Inspect Next-Generation Encryption Protocols

Next-generation encryption protocols are evolving with industry best practices for better security and privacy. New emerging standards like TLS 1.3 and Apple Transport Security (ATS) encourage the rapid adoption of SSL forward secrecy for improved network security. The transition to next-generation encryption breaks passive SSL devices, which bypass your security controls, leaving you at risk. Diverse cipher support allows for the greatest flexibility in preventing new blind spots—without the need for architectural changes.

Improve Scalability and Availability for Your Security Tools

Enterprises with substantial traffic loads can optimize security deployments by using health monitoring, load-balancing, and SSL offload capabilities. This enables your security investments to scale and protect with multi-layered security in the most demanding environments. Scale your security devices with failover protection to achieve better utilization and service availability.

Dynamic Service Chaining Based on Context

Herculon SSL Orchestrator can dynamically chain security services including anti-virus/malware products, intrusion detection systems (IDSs), IPSs, next-generation firewalls, and DLP. It leverages classification metrics such domain name, content category, geolocation, IP reputation, and other 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 by removing the key and certificate management from your security infrastructure.

Flexible Deployment Options Provide Ease of Integration

Herculon 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. It eliminates your organization’s need to re-architect the network to provide visibility into encrypted traffic and preserves your investment in security solutions.

Partners

Herculon SSL Orchestrator has been designed to interoperate with leading tools from partners such as Cisco, Symantec, FireEye, 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

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

SSL visibility

High performance SSL decryption/re-encryption
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

Policy context engine

Source and destination IP and Subnet
Port
Protocol
Domain
IP Geolocation
IP reputation (subscription)
URL categorization (subscription)
Policy-based Block, Bypass, Forward for Inspection actions

Robust cipher and protocol support

TLS 1/1.1/1.2, DTLS1
RSA/DHE/ECDHE with Forward Secrecy support
SHA, SHA2, AES, AES-GCM
Proxy-level control over ciphers and protocols

Deployment modes

Inline routed layer 3
Inline layer 2
ICAP service to DLP and antivirus/antimalware devices
Receive-only
Support for one and two-box deployments
High availability with TCP session resiliency
Load balancing of multiple security devices

Network 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	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)
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, i10600, i7800, i7600, i5800, and i5600 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
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.).

More Information

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

Web page

Herculon SSL Orchestrator

Solution overview

Herculon 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

Solutions for
an application world.