Configuring F5 SSL Orchestrator

Category: Networking & Security | **Vendor:** F5

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

In this 2 day course, students are provided with a functional understanding of how to deploy, test and maintain F5 SSL Orchestrator to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment.

The course includes lecture, hands-on labs, and discussion about the importance of SSL visability, how F5 SSL Orchestrator supports policy-based management, steering of traffic flows to existing security devices and centralizes the SSL decrypt/encrypt function through multi-layered security, dynamic service chaining, topology selections and security policies.

About This Course

- Compare F5 SSL Orchestration to manual “daisy chaining” of security services
- Learn essentials of PKI and certificates, how to create a certificate signing request, and how to import certificates and private keys into BIG-IP
- Implement certificate forging in an SSL Forward Proxy deployment
- Understand HTTP, ICAP, L3/L2, and TAP security services
- Configure traffic classification and URL bypass within a security policy
- Define security services to include in a dynamic service chain
- Use the Guided Configuration to deploy an outbound Layer 3 transparent forward proxy
- Use the Guided Configuration to deploy an outbound Layer 3 explicit forward proxy
- Use the Guided Configuration to deploy an inbound Layer 3 reverse proxy
- Use the Guided Configuration to deploy an SSL Orchestration for an existing application
- Configure High Availability for SSLO devices
- Troubleshoot SSLO and traffic flow issues

Prerequisites & Entry Requirements

General Prerequisites:

The following general network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course:

- OSI model encapsulation
- Routing and switching
- Ethernet and ARP
- TCP/IP concepts
- IP addressing and subnetting
- NAT and private IP addressing
- Default gateway

The following course-specific knowledge and experience is suggested before attending this course:

- HTTP, HTTPS protocols
- TLS/SSL
- Security services such as malware detection, data loss/leak prevention (DLP), next-generation firewalls (NGFW), intrusion prevention systems (IPS), and Internet Content Adaptation Protocol (ICAP)

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Understand basic use cases for decryption and re-encryption of inbound and outbound SSL/TLS network traffic
- Create dynamic service chains of multiple security services
- Configure security policies to enable policy-based traffic steering
- Add SSL visibility to existing applications
- Deploy SSL Orchestrator configurations based on topology templates
- Troubleshoot an SSL Orchestrator deployment

Detailed Course Outline

Chapter 1: Introducing SSL Orchestrator

- Why is SSL Visibility Needed?
- SSL Visibility without SSL Orchestrator
- The SSL Orchestrator Solution
- SSLO Placement on the Network
- Platform and Licensing Requirements
- Leveraging F5 Support Resources and Tools

Chapter 2: Reviewing Local Traffic Configuration

- Reviewing Nodes, Pools, and Virtual Servers
- Reviewing Address and Port Translation
- Reviewing Routing Assumptions
- Reviewing Application Health Monitoring
- Reviewing Traffic Behavior Modification with Profiles
- Reviewing the TMOS Shell (TMSH)

- Reviewing Managing BIG-IP Configuration Data

Chapter 3: Certificate Fundamentals

- Overview of Internet Security Model
- Understanding how Certificates are Used
- Using a Certificate in Profiles
- SSL Forward Proxy
- SSLdump

Chapter 4: SSLO Traffic Flow

- SSL Orchestration is more than Visibility
- Inbound/Outbound Inspection
- Flow Support and Cipher Diversity
- Broad Topology and Device Support
- Dynamic Service Chaining and Policy-based Traffic Steering
- Advanced Monitoring
- Dynamic Scaling
- Dynamic Evaluation
- Selecting the Appropriate Topology

Chapter 5: Using SSLO Guided Configuration

- Introducing Guided Configuration
- Reviewing the Landing Page
- Differentiating Topologies
- SSL Configuration
- Services and Service Handling
- Constructing Service Chains
- Creating a Security Policy
- Defining an Interception Rule

- Examining Egress
- Applying Log Settings
- Summary page and Deployment
- Exploring the Dashboard

Chapter 6: SSLO Deployment Scenarios

- Transparent Forward Proxy
- Explicit Forward Proxy
- Classroom Lab Environment
- Gateway Reverse Proxy (L3 Inbound)
- Existing Application

Chapter 7: Managing the SSLO Security Policy

- Review creating Security Policies
- View Security Policies
- Viewing Per-Request Policies

Chapter 8: Troubleshooting SSLO

- Solving Traffic Flow Issues
- Solving Guided Configration(UI) and iAppLX issues
- Determining SSLO Version
- Troubleshooting using cURL
- Viewing Log Files
- Capturing Traffic using tcpdump
- Backing up SSLO
- Deleting a SSLO Configuration

Chapter 9: SSLO High Availability

- Deploying BIG-IP Systems to Achieve High Availability
- Establishing Device Trust
- Establishing a Sync-Failover Device Group
- Synchronizing Configuration Data
- SSLO High Availability (HA) Requirements
- Installation and Upgrade Cautions
- Troubleshooting HA

Skills You Will Learn:

- Understand basic use cases for decryption and re-encryption of inbound and outbound SSL/TLS network traffic
- Create dynamic service chains of multiple security services
- Configure security policies to enable policy-based traffic steering
- Add SSL visibility to existing applications
- Deploy SSL Orchestrator configurations based on topology templates
- Troubleshoot an SSL Orchestrator deployment

Frequently Asked Questions

Q: What delivery options are available for Configuring F5 SSL Orchestrator?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day Configuring F5 SSL Orchestrator course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Configuring F5 SSL Orchestrator training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Configuring F5 SSL Orchestrator?

Yes, we provide corporate training, dedicated training, and closed classes for Configuring F5 SSL Orchestrator. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Configuring F5 SSL Orchestrator, F5 Networks, SSLO

Q: Why choose Nexus Human for Configuring F5 SSL Orchestrator?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Configuring F5 SSL Orchestrator training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.