Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

Configuring F5 SSL Orchestrator v.16.1

CODE:	LENGTH:	PRICE:
F5N_BIG-SSLO	16 Hours (2 days)	£1,850.00

Description

Learn how to deploy and operate F5 SSL Orchestrator to maximize infrastructure investments, efficiencies, and security with dynamic, policy-based encryption, decryption, and traffic steering through multiple inspection devices. Combining hands-on lab exploration with instructor-led lectures, gain practical experience implementing comprehensive encrypted traffic protection using SSL Orchestrator Guided Configuration. Build deployments for transparent and explicit forward proxies, gateway reverse proxies and existing application protecting inbound enterprise traffic, then modify those deployments changing a gateway to application mode and applying TLS v1.3 requirements. Incorporate multiple security devices at layer 2 and layer 3 with ICAP and receive-only devices in varying topology deployments.
Explore interception rules and context-based policies allowing for targeted SSL visibility based on context engine steering using geolocation, IP reputation and URL categorization. Implement dynamic service chaining of security devices to provide service insertion, service resiliency, service monitoring, and load balancing in hands-on lab scenarios. Discuss the essentials of PKI and certificates with lab practice to import certificates and private keys, then incorporate into security configurations for each topology deployment.

Objectives

- 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
  Course Topics
    - 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

Audience

This course is intended for network administrators and Security Operations responsible for installation, setup, configuration, and administration of the F5 SSL Orchestrator system.

Prerequisites

The following free Self-Directed Training (SDT) courses, although optional, are helpful for any student with limited BIG-IP administration and configuration experience:
• Getting Started with BIG-IP
• Getting Started with SSL Orchestrator (SSLO)
General network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course, including OSI model encapsulation, routing and switching, Ethernet and ARP, TCP/IP concepts, IP addressing and subnetting, NAT and private IP addressing, NAT and private IP addressing, default gateway, network firewalls, and LAN vs. WAN.
The following course-specific knowledge and experience is suggested before attending this course:
• HTTP, HTTPS, FTP, and SSH 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)

Programme

Chapter 1: Introducing SSL Orchestrator
• Internet Security and SSL Visibility
• Introducing SSL Orchestrator and its role in network security
• SSL Orchestrator Placement on the Network
• Platform and Licensing Requirements
Chapter 2: Certificate Fundamentals
• Overview of Internet Security Model
• Understanding Certificate Use
• Managing Certificates on SSL Orchestrator (BIG-IP)
Chapter 3: Architecture Overview
• Inbound and outbound inspection
• Cipher diversity
• Broad topology and inspection device support
• Dynamic service chaining and policy-based traffic steering
• Advanced monitoring
• Dynamic scaling and evaluation
Chapter 4: Guided Configuration
• Reviewing the Landing Page
• Selecting a Topology
• Making SSL Certificate Configurations
• Creating Services and Service Handling
• Constructing a Service Chain
• Building a Security Policy
• Defining an Interception Rule
• Examining Egress settings
• Reviewing the Summary Page and Deployment
• Exploring the SSL Orchestrator Dashboard
Chapter 5: Services
• Relationship of devices to services
• Inline layer 2, layer 3 and HTTP inspection services
• ICAP and TAP passive inspection services
Chapter 6: Topologies
• Selecting the appropriate topology
• Benefits and limitations of topologies
• Existing application integration
• Layer 2 virtual wire concepts
Chapter 7: Components
• Initial and subsequent forward proxy flow
• Flow and header based signaling
• Access components
• Appropriate naming of service objects
• Authentication
• Tee connector design and flow
Chapter 8: Managing Security Policy
• Creating security policies
• Reviewing per-request policy for an outbound topology
• Navigating Visual Policy Editor
Chapter 9: Solving SSL Orchestrator Problems
• Collecting system information
• Solving traffic flow issues
• Guided Configuration and iAppLX issues
• Troubleshooting with cURL
• Traffic captures with tcpdump
• Cleanup and deleting configurations
Chapter 10: SSL Orchestrator High Availability
• Review BIG-IP High Availability
• SSL Orchestrator High Availability (HA) Requirements
• Installation and Upgrade Cautions
• SSL Orchestrator in Scaled Mode
• Troubleshooting SSL Orchestrator HA

Follow on courses

F5N_BIG-LTM-CFG-3, Configuring BIG-IP LTM: Local Traffic Manager v.16.1
F5N_BIG-DNS-I, Configuring BIG-IP DNS (formerly GTM) v.16.1
F5N_BIG-AWF-CFG, Configuring F5 Advanced WAF (previously licensed as ASM) v16.1
F5N_BIG-EGW-APM, Configuring BIG-IP APM: Access Policy Manager v.16.1

F5N_BIG-IRULE-CFG, Developing iRules for BIG-IP v.16.1
F5N_BIG-TRBL-INT2, Troubleshooting BIG-IP v.16.1

Further Information

Course Changes since v15

- Changes to the presentation and student guide materials reflect feature updates and new software SSL Orchestrator version v8.3.
- Key feature updates include Improved HA behavior, Remediation Dashboard, Strictness Improvements and Data group security policy support.
- Content for Topologies, Services and Components are separated out, placed into dedicated lessons and additional labs created for each lesson.
- The Troubleshooting lesson is re-organized and received additional content. Local Traffic Management review chapter has been removed.

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.