Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

ID TRG-BIG-AWF-CFG **Price** US $ 5,280.—(excl. VAT) **Duration** 4 days

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 Local Traffic Manager (LTM)
- Getting Started with F5 Advanced WAF

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.

Course Objectives

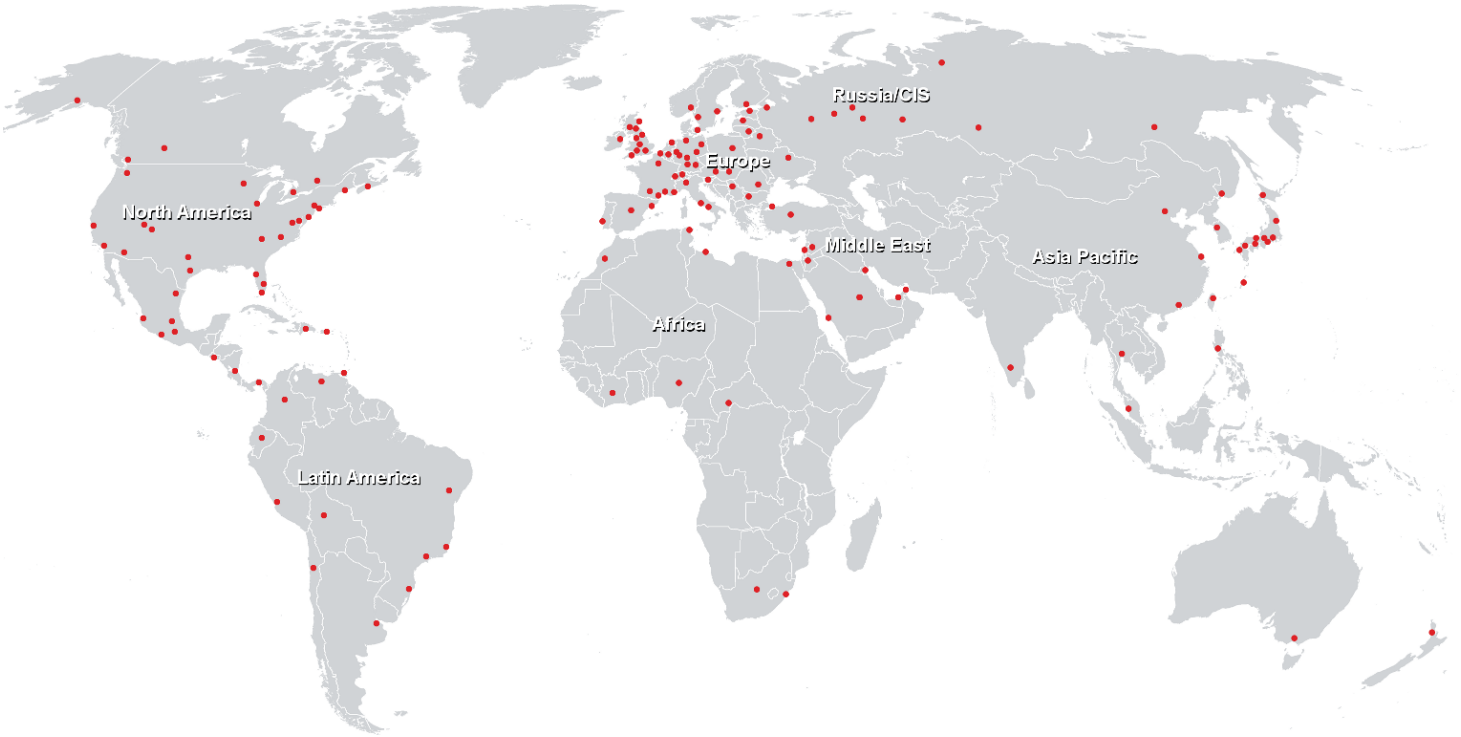
- Students should be able to:
- Describe the role of the BIG-IP system as a full proxy device in an application delivery network
- Provision the F5 Advanced Web Application Firewall
- Define a web application firewall
- Describe how F5 Advanced Web Application Firewall protects a web application by securing file types, URLs, and parameters
- Deploy F5 Advanced Web Application Firewall using the Rapid Deployment template (and other templates) and define the security checks included in each
- Define learn, alarm, and block settings as they pertain to configuring F5 Advanced Web Application Firewall
- Define attack signatures and explain why attack signature staging is important
- Deploy Threat Campaigns to secure against CVE threats
- Contrast positive and negative security policy implementation and explain benefits of each
- Configure security processing at the parameter level of a web application
- Deploy F5 Advanced Web Application Firewall using the Automatic Policy Builder
- Tune a policy manually or allow automatic policy building
- Integrate third party application vulnerability scanner output into a security policy
- Configure login enforcement for flow control
- Mitigate credential stuffing
- Configure protection against brute force attacks
- Deploy Advanced Bot Defense against web scrapers, all known bots, and other automated agents
- Deploy DataSafe to secure client-side data

Course Content

- Introducing the BIG-IP System
- Traffic Processing with BIG-IP
- Overview of Web Application Processing
- Overview of Web Application Vulnerabilities
- Security Policy Deployments: Concepts and Terminology
- Policy Tuning and Violations
- Using Attack Signatures and Threat Campaigns
- Positive Security Policy Building
- Securing Cookies and other Header Topics
- Visual Reporting and Logging
- Lab Project 1
- Advanced Parameter Handling
- Automatic Policy Building
- Integrating with Web Application Vulnerability Scanners
- Deploying Layered Policies
- Login Enforcement and Brute Force Mitigation
- Reconnaissance with Session Tracking
- Layer 7 Denial of Service Mitigation
- Advanced Bot Defense
- Final Projects

Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

Training Centres worldwide





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch