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

Prerequisite – Students must complete ONE of these:

- Attend an Administering BIG-IP (TRG-BIG-OP-ADMIN) class
- Achieve F5 Certified BIG-IP Administrator certification
- Pass the free Administering BIG-IP Course Equivalency Assessment with a score of 70% or higher

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
- Network firewalls
- 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

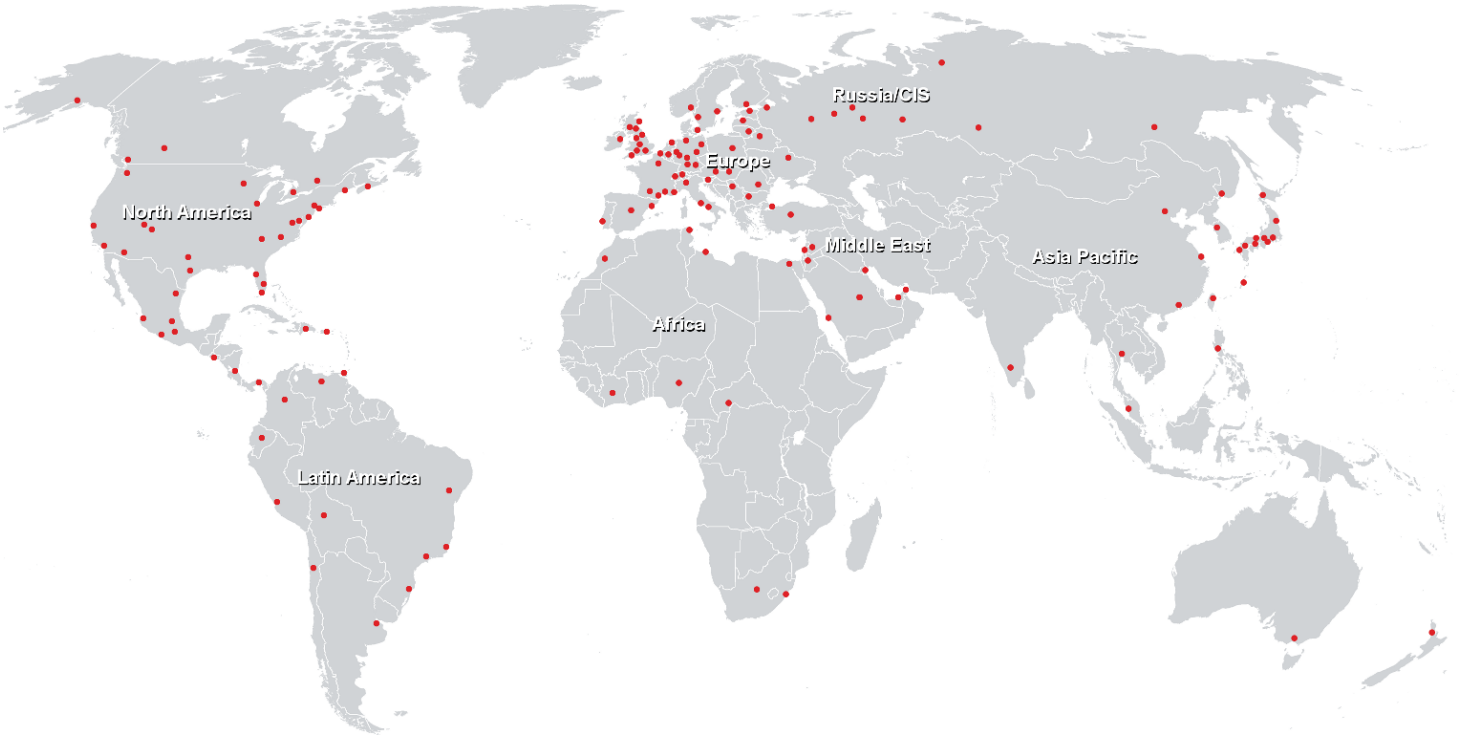
- Resource provisioning for F5 Advanced Web Application Firewall
- Traffic processing with BIG-IP Local Traffic Manager (LTM)
- Web application concepts
- Mitigating the OWASP Top 10 and other vulnerabilities
- Security policy deployment
- Security policy tuning
- Deploying Attack Signatures and Threat Campaigns
- Positive security building
- Securing cookies and other headers
- Reporting and logging
- Advanced parameter handling
- Using Automatic Policy Builder
- Integrating with web vulnerability scanners
- Login enforcement for flow control
- Brute force and credential stuffing mitigation
- Session tracking for client reconnaissance
- Using Parent and Child policies
- Layer 7 DoS protection
- Transaction Per Second-based DoS protection
- Layer 7 Behavioral DoS Protection
- Configuring Advanced Bot Defense
- Web Scraping and other Microservice Protection
- Working with Bot Signatures
- Using DataSafe to Secure the client side of the Document Object Model
- Certification

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

- 303 ASM Specialist

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