Configuring BIG-IP AFM: Advanced Firewall Manager (TRG-BIG-AFM-CFG)

ID TRG-BIG-AFM-CFG **Price** US $ 2,640.—(excl. VAT) **Duration** 2 days

Who should attend

This course is intended for network operators, network administrators, network engineers, network architects, security administrators, and security architects responsible for installation, setup, configuration, and administration of the BIG-IP AFM system.

Prerequisites

Students must complete one of the following F5 prerequisites before attending this course:

- Administering BIG-IP (TRG-BIG-OP-ADMIN) instructor-led course
  or
- F5 Certified BIG-IP Administrator

The following free web-based courses, although optional, will be very helpful for any student with limited BIG-IP administration and configuration experience. These courses are available at F5 University:

- Getting Started with BIG-IP web-based training
- Getting Started with BIG-IP Local Traffic Manager (LTM) web-based training
- Getting Started with BIG-IP Advanced Firewall Manager (AFM) web-based training

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

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

- HTTP and DNS protocols

Course Objectives

- Configure and manage an AFM system
- Configure AFM Network Firewall in a positive or negative security model
- Configure Network Firewall to allow or deny network traffic using rules based on protocol, source, destination, geography, and other predicate types
- Prebuild firewall rules using lists and schedule components
- Enforce firewall rules immediately or test them using policy staging
- Use Packet Tester and Flow Inspector features to check network connections against your security configurations for Network Firewall, IP intelligence and DoS features
- Configure various IP Intelligence features to identify, record, allow or deny access by IP address
- Configure the Device DoS detection and mitigation feature to protect the BIG-IP device and all applications from multiple types of attack vectors
- Configure DoS detection and mitigation on a per-profile basic to protect specific applications from attack
- Use DoS Dynamic Signatures to automatically protect the system from DoS attacks based on long term traffic and resource load patterns
- Configure and use the AFM local and remote log facilities
- Configure and monitor AFM’s status with various reporting facilities
- Export AFM system reports to your external monitoring system directly or via scheduled mail
- Allow chosen traffic to bypass DoS checks using Whitelists
- Isolate potentially bad clients from good using the Sweep Flood feature
- Isolate and re-route potentially bad network traffic for further inspection using IP Intelligence Shun functionality
- Restrict and report on certain types of DNS requests using DNS Firewall
- Configure, mitigate, and report on DNS based DoS attacks with the DNS DoS facility

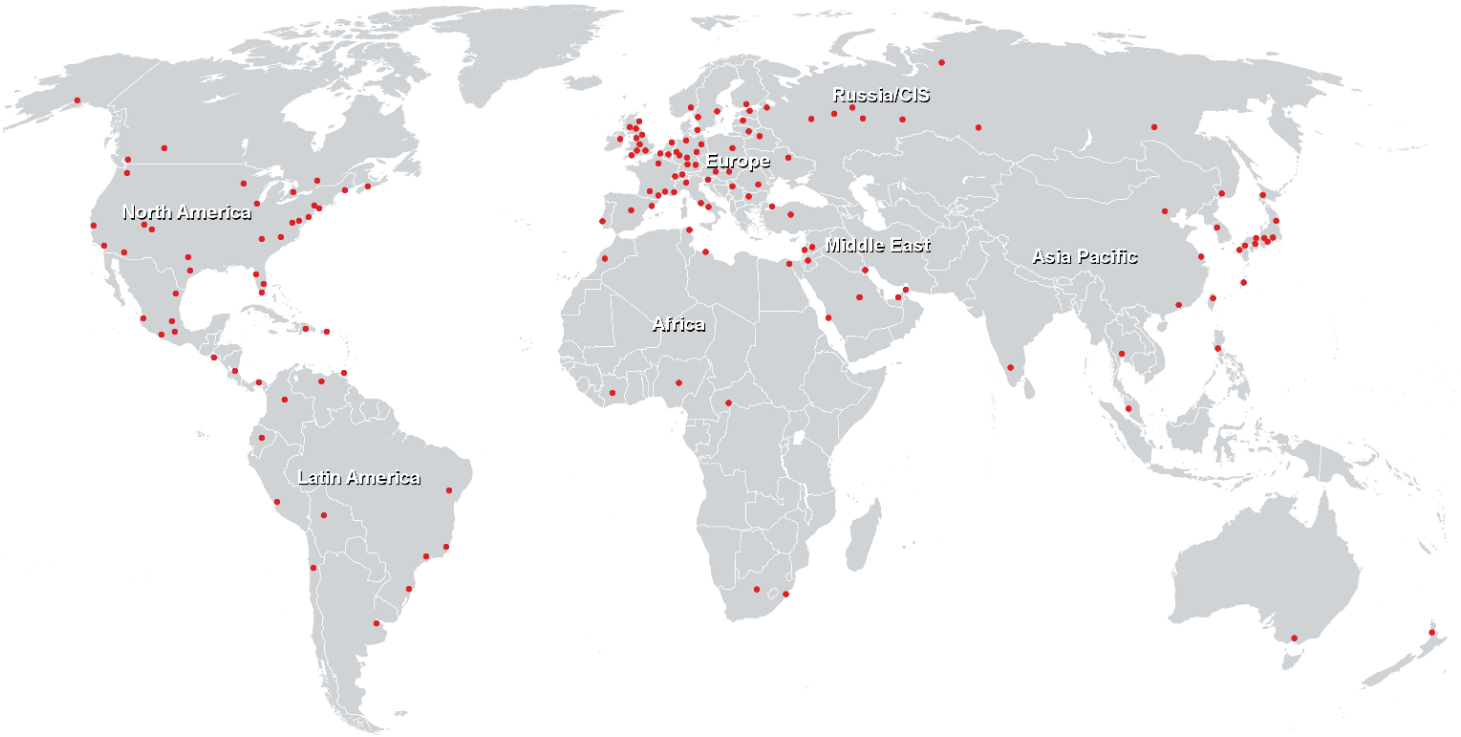
- Configure, mitigate, and report on SIP based DoS attacks with the SIP DoS facility
- Configure, block, and report on the misuse of system services and ports using the Port Misuse feature
- Build and configure Network Firewall rules using BIG-IP iRules
- Be able to monitor and do initial troubleshooting of various AFM functionality

Course Content

- Setting up the BIG-IP System
- AFM Overview
- Network Firewall
- Logs
- IP Intelligence
- DoS Protection
- Reports
- DoS White Lists
- DoS Sweep Flood Protection
- IP Intelligence Shun
- DNS Firewall
- DNS DoS
- SIP DoS
- Port Misuse
- Network Firewall iRules
- Recap
- Additional Training and Certification

Configuring BIG-IP AFM: Advanced Firewall Manager (TRG-BIG-AFM-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