



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com

Phone: +47 22 02 81 00



Configuring BIG-IP AFM: Advanced Firewall Manager v16.1

CODE:	LENGTH:	PRICE:
F5N_BIG-AFM	16 Hours (2 days)	kr16,500.00

Description

This 2-day course uses lectures and hands-on lab exercises to give participants real-time experience in setting up and configuring the BIG-IP® Advanced Firewall Manager system.

Students are introduced to the AFM user interface, stepping through various options that demonstrate how AFM is configured to build a network firewall and to detect and protect against DoS (Denial of Service) attacks. Reporting and log facilities are also explained and used in the course labs.

Further Firewall functionality and additional DoS facilities for DNS and SIP traffic are discussed. Course Topics

- Configuration and management of the BIG-IP AFM system
- AFM Network Firewall concepts
- Network firewall options and modes
- Network firewall rules, policies, address/port lists, rule lists and schedules
- IP Intelligence facilities of dynamic black and white lists, IP reputation database and dynamic IP shunning
- Detection and mitigation of DoS attacks
- Event logging of firewall rules and DoS attacks
- Reporting and notification facilities
- DoS Whitelists
- DoS Sweep/Flood
- DNS Firewall and DNS DoS
- SIP DoS
- Port Misuse
- Network Firewall iRules
- Various AFM component troubleshooting commands

Objectives

Introducing the BIG-IP System
Initially Setting Up the BIG-IP System
Archiving the BIG-IP Configuration
Leveraging F5 Support Resources and Tools
Chapter Resources

v13 Course Outline Chapter 1: Setting up the BIG-IP System BIG-IP System Setup Labs

- AFM Overview
- AFM Release History
- AFM Availability
- What do you see?
- Terminology
- Network Firewall
- AFM Contexts
- AFM Modes
- AFM Packet Processing
- AFM Rules and Direction
- Rules Contexts and Processing
- Configuring Network Firewall
- Network Firewall Rules
- Geolocation
- Redundant and Conflicting Rules
- Stale Rules
- Lists and Schedules
- Rule Lists
- Address Lists
- Port Lists
- Schedules
- Policies
- Policy Status and Firewall Policy Management
- Inline Rule Editor
- Send to Virtual

Chapter 2: AFM Overview and Network Firewall Packet Tester

Chapter 3: Logs

- Overview
- Event Logs
- Logging Profiles
- Log Throttling
- Logging and Logging Profiles
- BIG-IP Logging Mechanisms
- Publisher
- Log Destination
- Custom Search
- Logging Global Rule Events
- Log Configuration Changes
- QKView and Log Files
- SNMP MIB
- SNMP Traps

- Overview
- Feature 1 Dynamic Black and White Lists
- Black List Categories
- Feed Lists
- IP Intelligence Policies
- IP Intelligence Log Profile
- IP Intelligence Reporting
- Troubleshooting IP Intelligence Lists
- Feature 2 IP Intelligence Database
- Licensing
- Installation
- Configuration
- Troubleshooting

Chapter 4: IP Intelligence IP Intelligence iRule

Chapter 5: Device DoS

- Denial of Service and DoS Protection Overview
- Device DoS
- Configuring Device DoS
- Variant 1
- Variant 2
- Auto-Threshold Configuration
- Variant 3
- Bad Actor and Blacklist Address
- Device DoS Profiles
- DoS Protection Profile
- Dynamic Signatures
- DoS iRules

- Reports
- Reporting
- General Reporting Facilities
- Time Series Chart
- Details
- Report Export
- DoS Screens
- Dashboard
- Analysis
- Custom Page
- Settings
- Scheduled Reports
- Troubleshooting Scheduled Reports
- Overview
- Summary
- Widgets
- Custom Widgets
- Deleting and Restoring Widgets

Chapter 6: Reports Firewall Manager

- White Lists
- Configuration
- tmsh

Sweep Flood

Chapter 7: DoS White Lists Source Address List Chapter 8: DoS Sweep Flood Protection Configuration

	IP Intelligence Shun Manual Configuration Dynamic Configuration IP Intelligence Policy tmsh Extending the Shun Feature Remotely Triggered Black Hole		DNS Firewall Configuration DNS Query DNS Opcodes Logging
Chapter 9: IP Intelligence Shun	Scrubber	Chapter 10: DNS Firewall	Troubleshooting
			Session Initiation Protocol (SIP) Transactions and Dialogs SIP DoS Configuration DoS Protection Profile Device DoS
	DNS DoS Configuration DoS Protection Profile	Chapter 11: DNS DoS	Device DoS
		Chapter 12: SIP DoS	SIP iRules
	Network Firewall iRules iRule Events Configuration Recommended Practice		Port Misuse Port Misuse Policy Attaching a Service Policy
Chapter 13: Network Firewall iRules	More Information	Chapter 14: Port Misuse	Log Profile

Audience

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 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 v12 Course Outline Chapter 1: Setting up the BIG-IP System

Introducing the BIG-IP System

Initially Setting Up the BIG-IP System

Archiving the BIG-IP Configuration

Leveraging F5 Support Resources and Tools **Chapter 2: AFM Overview and Network Firewall**

DoS iRules
iRule Events
Use Cases
More Information
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

Further Information

Course Changes since v15

Updates for the v16.1 release are minor. Course material including student guide and labs steps have been updated to reflect the version change and for any product changes to GUI appearance and screen options.

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
30 May 2024	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		kr16,500.00

Tilleggsinformasjon

[Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.](#)