



Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com

Phone: 0870 251 1000



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

CODE:	LENGTH:	PRICE:
F5N_BIG-AFM	16 Hours (2 days)	€1,995.00

Description

This course uses lectures and hands-on exercises to give participants real-time experience in setting up and configuring the BIG-IP Advanced Firewall Manager (AFM) 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.

Topics covered in this course include: v14.1 Course Topics

- Installation and setup 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
- Network Firewall iRules
- Port Misuse
- 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

v14.1 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

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

Packet Tester

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 3: Logs

Chapter 4: IP Intelligence

IP Intelligence iRule

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 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

Chapter 6: Reports

Firewall Manager

White Lists
 Configuration
 tmsb

Sweep Flood

Chapter 7: DoS White Lists

Chapter 8: DoS Sweep Flood Protection

Source Address List Configuration

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

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**

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

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
IP Intelligence iRule

Reports
Reporting
General Reporting Facilities
Charts
Details
Report Export
Network Screens
DoS Screens
Settings
Overview
Summary
Widgets
Time Periods, Settings, Export, and Delete Options

Chapter 6: Reports Firewall Manager

Chapter 8: DoS Sweep Flood Protection Configuration

DNS Firewall
DNS Query
DNS Opcodes

Chapter 10: DNS Firewall Troubleshooting

Session Initiation Protocol (SIP)
Transactions and Dialogs
SIP DoS
DoS Protection Profile
Device DoS
SIP iRules

Chapter 13: Network Firewall iRules More Information

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

Chapter 3: Logs

Chapter 4: IP Intelligence

Denial of Service and DoS Protection Overview
Configuring Device DoS
Configuring Device DoS Vectors
Variant 1
Rate and Leak Limit
Variant 2
Auto-Threshold Configuration
Variant 3
Bad Actor and Blacklist Attacking Address
Device DoS Profiles
DoS Protection Profile

Chapter 7: DoS White Lists Source Address List

IP Intelligence Shun
Manual
Dynamic
IP Intelligence Policy
tmsh

Chapter 9: IP Intelligence Shun Troubleshooting

DNS DoS
DoS Protection Profile

Chapter 11: DNS DoS Device DoS

Chapter 12: SIP DoS

Network Firewall iRules
iRule Events
Use Cases
Recommended Practice

Chapter 14: DoS iRules

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

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
20 Apr 2023	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		€1,995.00
20 Apr 2023	Espoo	EEST	English	Classroom		€1,995.00
07 Jun 2023	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		€1,995.00
07 Jun 2023	Espoo	EEST	English	Classroom		€1,995.00

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)