

Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com Phone: +46 8 555 188 00



Configuring BIG-IP AFM: Advanced Firewall Manager v17.1

CODE: LENGTH: PRICE:

F5N BIG-AFM 16 Hours (2 days) kr21,500.00

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

v17.1 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 Packet Tester Chapter 3: Logs

Overview Overview

Event Logs Feature 1 Dynamic Black and White Lists

Logging Profiles Black List Categories

Log Throttling Feed Lists

Logging and Logging ProfilesIP Intelligence PoliciesBIG-IP Logging MechanismsIP Intelligence Log ProfilePublisherIP Intelligence Reporting

Log Destination Troubleshooting IP Intelligence Lists
Custom Search Feature 2 IP Intelligence Database

Logging Global Rule EventsLicensingLog Configuration ChangesInstallationQKView and Log FilesConfigurationSNMP MIBTroubleshooting

SNMP Traps Chapter 4: IP Intelligence IP Intelligence iRule Chapter 5: Device DoS

Reports Reporting

Details

General Reporting Facilities

Time Series Chart

Report Export DoS Screens Dashboard Analysis

Denial of Service and DoS Protection Overview
Device DoS
Configuring Device DoS
Variant 1
Dashboard
Analysis
Custom Page
Settings

Variant 2 Scheduled Reports

Auto-Threshold Configuration Troubleshooting Scheduled Reports

Variant 3 Overview
Bad Actor and Blacklist Address Summary
Device DoS Profiles Widgets
DoS Protection Profile Custom Widgets

Dynamic Signatures Deleting and Restoring Widgets

DoS iRules 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 Configuratio

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
DNS DoS SIP DoS Configuration
Configuration DoS Protection Profile

DoS Protection Profile Device DoS

Chapter 11: DNS DoS Device DoS Chapter 12: SIP DoS SIP iRules

Network Firewall iRules

iRule EventsPort MisuseConfigurationPort Misuse PolicyRecommended PracticeAttaching 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

AFM Overview
AFM Release History
AFM Availability
What do you see?
Terminology
Network Firewall
AFM Contexts

AFM Packet Processing

AFM Modes

AFM Rules and Direction Event Logs
Rules Contexts and Processing Logging Profiles
Configuring Network Firewall Log Throttling
Network Firewall Rules Traffic Flow Statistics

Geolocation Logging and Logging Profiles
Redundant and Conflicting Rules BIG-IP Logging Mechanisms

Stale RulesPublisherLists and SchedulesLog DestinationRule ListsCustom Search

Address Lists

Port Lists

Logging Global Rule Events

Log Configuration Changes

Schedules QKView
Policies Other Log Files
Policy Status and Firewall Policy Management SNMP MIB

Inline Rule Editor Chapter 3: Logs SNMP Traps Chapter 4: IP Intelligence

Overview

Feature 1 Dynamic Black and White Lists

Black List Categories

Feed Lists Denial of Service and DoS Protection Overview

IP Intelligence Policies Configuring Device DoS
IP Intelligence Log Profile Configuring Device DoS Vectors

IP Intelligence Reporting Variant 1

Troubleshooting IP Intelligence Lists Rate and Leak Limit

Feature 2 IP Intelligence Database Variant 2

Licensing Auto-Threshold Configuration

Installation Variant 3

Configuration Bad Actor and Blacklist Attacking Address

Troubleshooting Device DoS Profiles
IP Intelligence iRule Chapter 5: Device DoS DoS Protection Profile

Reports Reporting

General Reporting Facilities

Charts
Details
Report Export
Network Screens
DoS Screens
Settings
Overview

Summary White Lists Widgets Configuration

Time Periods, Settings, Export, and Delete Options tmsh

Chapter 6: Reports Firewall Manager

Chapter 7: DoS White Lists Source Address List
IP Intelligence Shun

Manual Dynamic

IP Intelligence Policy

Sweep Flood tmsh

Chapter 8: DoS Sweep Flood Protection Configuration Chapter 9: IP Intelligence Shun Troubleshooting

DNS Firewall

DNS Query DNS DoS

DNS Opcodes DoS Protection Profile

Chapter 10: DNS Firewall Troubleshooting Chapter 11: DNS DoS Device DoS Chapter 12: SIP DoS

Session Initiation Protocol (SIP)

Transactions and Dialogs Network Firewall iRules

SIP DoS iRule Events
DoS Protection Profile Use Cases

Device DoS Recommended Practice

SIP iRules Chapter 13: Network Firewall iRules More Information 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

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	Туре	Guaranteed	PRICE
25 Sep 2025	Virtual Classroom (CET)	CEDT	English	Instructor Led Online		kr21,500.00
27 Nov 2025	Virtual Classroom (CET)	CET	English	Instructor Led Online		kr21,500.00

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.