



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 v16.1

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

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

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	
	DNS DoS Configuration DoS Protection Profile Device DoS		Session Initiation Protocol (SIP) Transactions and Dialogs SIP DoS Configuration DoS Protection Profile Device DoS SIP iRules
Chapter 11: DNS DoS		Chapter 12: SIP DoS	
	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		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 Rules		Publisher
Lists and Schedules		Log Destination
Rule Lists		Custom Search
Address Lists		Logging Global Rule Events
Port Lists		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
Overview		Chapter 4: IP Intelligence
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
		tmsh
Chapter 8: DoS Sweep Flood Protection	Sweep Flood 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
	Session Initiation Protocol (SIP)	Chapter 12: SIP DoS
	Transactions and Dialogs	
	SIP DoS	Network Firewall iRules
	DoS Protection Profile	iRule Events
	Device DoS	Use Cases
	SIP iRules	Recommended Practice
	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	Type	Guaranteed	PRICE
26 Sep 2024	Virtual Classroom (CET)	CEDT	English	Instructor Led Online		kr19,500.00
28 Nov 2024	Virtual Classroom (CET)	CET	English	Instructor Led Online		kr19,500.00

Ytterligare information

[Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.](#)