



**Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

---

**Du kan nå os her**

Email: [training.ecs.dk@arrow.com](mailto:training.ecs.dk@arrow.com)  
Phone: +45 7025 4500



# Configuring BIG-IP AFM: Advanced Firewall Manager

CODE:	LENGTH:	PRICE:
F5N_BIG-AFM	16 Hours (2 dage)	kr 14,900.00

## 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.

### Major Course Changes since v17.1

The Configuring AFM v14 course broadly follows the chapter structure of the previous version of this course, with edits for changes in creating and editing network firewall rules and configuring DoS detection and protection. The Intrusion Protection System chapter has been removed awaiting feature changes in a future release.

## 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 basis 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

## 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 v14.1 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

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

**Chapter 3: Logs** SNMP Traps

**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

**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
<b>Chapter 6: Reports</b>	Firewall Manager	<b>Chapter 7: DoS White Lists</b>	Source Address List
			IP Intelligence Shun
			Manual
			Dynamic
			IP Intelligence Policy
			tmsh
	Sweep Flood		
<b>Chapter 8: DoS Sweep Flood Protection</b>	Configuration	<b>Chapter 9: IP Intelligence Shun</b>	Troubleshooting
	DNS Firewall		
	DNS Query		DNS DoS
	DNS Opcodes		DoS Protection Profile
<b>Chapter 10: DNS Firewall</b>	Troubleshooting	<b>Chapter 11: DNS DoS</b>	Device 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	<b>Chapter 13: Network Firewall iRules</b>	More Information
	DoS iRules		
	iRule Events		<b>Chapter 14: DoS iRules</b>
	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
16 Oct 2025	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		kr 14,900.00

## Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.