Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Configuring BIG-IP AFM: Advanced Firewall Manager v.15.1

CODE:	LENGTH:	PRICE:
F5N_BIG-AFM	16 Hours (2 days)	€1,795.00

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.

Topics Covered
- Configuration and management of the BIGIP 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

After completing this course, participants will be able to complete the following tasks: • 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 basic 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 system and network administrators responsible for the configuration and ongoing administration of a BIG-IP Advanced Firewall Manager (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 LearnF5 (https://www.f5.com/services/training):
• 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
• NAT and private IP addressing
• Default gateway
• Network firewalls
• LAN vs. WAN
• HTTP and DNS protocols

The following course-specific knowledge and experience is suggested before attending this course:

Programme

Chapter 1: Setting up the BIG-IP System
• Introducing the BIG-IP System
• Initially Setting Up the BIG-IP System
• Archiving the BIG-IP System Configuration
• Leveraging F5 Support Resources and Tools

Chapter 2: AFM Overview
• AFM Overview
• AFM Availability
• AFM and the BIG-IP Security Menu

Chapter 3: Network Firewall
• AFM Overview
• Contexts
• Modes
• Packet Processing
• Rules and Direction
• Rules Contexts and Processing
• Inline Rule Editor
• Configuring Network Firewall
• Network Firewall Rules and Policies
• Network Firewall Rule Creation
• Identifying Traffic by Region with Geolocation
• Identifying Redundant and Conflicting Rules
• Identifying Stale Rules
• Prebuilding Firewall Rules with Lists and Schedules
• Rule Lists
• Address Lists
• Port Lists
• Schedules
• Network Firewall Policies
• Policy Status and Management
• Other Rule Actions
• Redirecting Traffic with Send to Virtual
• Checking Rule Processing with Packet Tester
• Examining Connections with Flow Inspector

- Event Logs
- Logging Profiles
- Limiting Log Messages with Log Throttling
- Enabling Logging in Firewall Rules
- BIG-IP Logging Mechanisms
- Log Publisher
- Log Destination
- Filtering Logs with the Custom Search Facility
- Logging Global Rule Events
- Log Configuration Changes
- QKView and Log Files
- SNMP MIB

Chapter 4: Logs
- SNMP Traps

Chapter 5: IP Intelligence
- Overview
- IP Intelligence Policy
- Feature 1 Dynamic White and Blacklists
- Black List Categories
- Feed Lists
- Applying an IP Intelligence Policy
- IP Intelligence Log Profile
- IP Intelligence Reporting
- Troubleshooting IP Intelligence Lists
- Feature 2 IP Intelligence Database
- Licensing
- Installation
- Linking the Database to the P Intelligence Policy
- Troubleshooting
- IP Intelligence iRule
- Denial of Service and DoS Protection Overview
- Device DoS Protection
- Configuring Device DoS Protection
- Variant 1 DoS Vectors
- Variant 2 DoS Vectors
- Automatic Configuration or Automatic Thresholds
- Variant 3 DoS Vectors
- Device DoS Profiles
- DoS Protection Profile
- Dynamic Signatures
- Dynamic Signatures Configuration

Chapter 6: DoS Protection
- DoS iRules
- AFM Reporting Facilities Overview
- Examining the Status of Particular AFM Features
- Exporting the Data
- Managing the Reporting Settings
- Scheduling Reports
- Troubleshooting Scheduled Reports
- Examining AFM Status at High Level
- Mini Reporting Windows (Widgets)
- Building Custom Widgets
- Deleting and Restoring Widgets

Chapter 7: Reports
- Dashboards

Chapter 8: DoS White Lists
- Bypassing DoS Checks with White Lists
- Configuring DoS White Lists
- tmsh options
- Isolating Bad Clients with Sweep Flood
- Per Profile Whitelist Address List

Chapter 9: DoS Sweep Flood Protection
- Configuring Sweep Flood
- Overview
- Manual Configuration
- Dynamic Configuration
- IP Intelligence Policy
- tmsh options
- Troubleshooting
- Extending the Shun Feature
- Route this Traffic to Nowhere - Remotely Triggered Black Hole

Chapter 10: IP Intelligence Shun
- Route this Traffic for Further Processing – Scrubber

Chapter 11: DNS Firewall
- Filtering DNS Traffic with DNS Firewall
- Configuring DNS Firewall
- DNS Query Types
- DNS Opcode Types
- Logging DNS Firewall Events
- Troubleshooting
- Overview
- DNS DoS
- Configuring DNS DoS
- DoS Protection Profile

Chapter 12: DNS DoS
- Device DoS and DNS

Chapter 13: SIP DoS
- Session Initiation Protocol (SIP)
- Transactions and Dialogs
- SIP DoS Configuration
- DoS Protection Profile
- Device DoS and SIP
- Overview
- Port Misuse and Service Policies
- Building a Port Misuse Policy
- Attaching a Service Policy
- Creating a Log Profile

Chapter 14: Port Misuse
- Overview
- iRule Events
- Configuration
- When to use iRules
- More Information

Chapter 15: Network Firewall iRules
- BIG-IP Architecture and Traffic Flow
- AFM Packet Processing Overview

Chapter 16: Recap

Follow on courses

F5N_BIG-LTM-CFG-3, Configuring BIG-IP LTM: Local Traffic Manager v.15.1
F5N_BIG-DNS-I, Configuring BIG-IP DNS (formerly GTM) v.15.1
F5N_BIG-AWF-CFG, Configuring F5 Advanced WAF (previously licensed as ASM) v15.1
F5N_BIG-EGW-APM, Configuring BIG-IP APM: Access Policy Manager v.15.1
F5N_BIG-IRULE-CFG, Developing iRules for BIG-IP v.15.1

Other courses available: F5N_BIG-TRBL-INT2, Troubleshooting BIG-IP v.15.1

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
30 May 2024	Virtual Classroom (CET / UTC+1)	CEDT	English	Instructor Led Online		€1,795.00

Additional Information

This training is also available as onsite training. Please contact us to find out more.