Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

Configuring BIG-IP AFM: Advanced Firewall Manager v.16.1

CODE:	LENGTH:	PRICE:
F5N_BIG-AFM	16 Hours (2 days)	£1,850.00

Description

Configuring BIG-IP Advanced Firewall Manager (AFM) Duration: 2 days
Learn how to deploy and operate BIG-IP Advanced Firewall Manager to protect a data center against incoming threats that enter the network at layers 3 and 4 on common protocols including HTTP, SIP, SSH, SSL, and others. Using a mix of lectures and hands-on lab exploration, gain experience implementing comprehensive protection against attacks from rapidly changing IP addresses by applying the latest threat intelligence, and by anticipating, detecting, and responding to attacks before they hit data center targets. Practice using hardware-based DDoS mitigation that scales to prevent high-volume, targeted, network flood attacks—while allowing legitimate traffic to flow without compromising performance or degrading the user experience. Observe malicious network activity in real time as you assume the role of an attacker.

F5 recognizes the importance of visibility, analytics, and reporting regarding attack evolution, attack mitigation, and overall firewall health. Plenty of time is dedicated to analyzing reports. Learn how to retrieve clear, concise, and actionable information highlighting attacks and trends with detailed drill-down and page-view capabilities.

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 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 (ILT)

- F5 Certified BIG-IP Administrator

Suggested Prework
The following free Self-Directed Training (SDT) courses, although optional, are helpful for any student with limited BIG-IP administration and configuration experience:

- Getting Started with BIG-IP
- Getting Started with Local Traffic Manager (LTM)
- Getting Started with BIG-IP Advanced Firewall Manager (AFM)

General network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course, including OSI model encapsulation, routing and switching, Ethernet and ARP, TCP/IP concepts, IP addressing and subnetting, NAT and private IP addressing, NAT and private IP addressing, default gateway, network firewalls, and LAN vs. WAN.

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 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 Firewalls
- 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

Chapter 4: Logs

- Event Logs
- Logging Profiles
- Limiting Log Messages with Log Throttling
- Enabling Logging in Firewall Rules
- BIG-IP Logging Mechanisms
- Log Publisher

- Log Destination
- Logging Global Rule Events
- Log Configuration Changes
- QKView and Log Files
- SNMP MIB
- SNMP Traps

Chapter 5: IP Intelligence

- Overview
- IP Intelligence Policy
- Feature 1: Dynamic White and Blacklists
- Blacklist 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 IP Intelligence Policy
- Troubleshooting
- IP Intelligence iRules

Chapter 6: DoS Protection

- 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
- DoS iRules

Chapter 7: Reports

- 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
- Dashboards

Chapter 8: DoS White Lists

- Bypassing DoS Checks with White Lists
- Configuring DoS White Lists
- tmsh options
- Per Profile Whitelist Address List

Chapter 9: DoS Sweep Flood Protection

- Isolating Bad Clients with Sweep Flood
- Configuring Sweep Flood

Chapter 10: IP Intelligence Shun

- Overview
- Manual Configuration
- Dynamic Configuration
- IP Intelligence Policy
- tmsh options
- Troubleshooting
- Extending the Shun Feature
- Route this Traffic to Nowhere - Remotely Triggered Black Hole
- 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

Chapter 12: DNS DoS

- Overview
- DNS DoS
- Configuring DNS DoS
- DoS Protection Profile
- 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

Chapter 14: Port Misuse

- Overview
- Port Misuse and Service Policies
- Building a Port Misuse Policy
- Attaching a Service Policy
- Creating a Log Profile

Chapter 15: Network Firewall iRules

- Overview
- iRule Events
- Configuration
- When to use iRules
- More Information

Chapter 16: Recap

- BIG-IP Architecture and Traffic Flow
- AFM Packet Processing Overview

Chapter 17: Additional Training and Certification

- Getting Started Series Web-Based Training
- F5 Instructor Led Training Curriculum
- F5 Professional Certification Program

Follow on courses

F5N_BIG-LTM-CFG-3, Configuring BIG-IP LTM: Local Traffic Manager v.16.1
F5N_BIG-DNS-I, Configuring BIG-IP DNS (formerly GTM) v.16.1
F5N_BIG-AWF-CFG, Configuring F5 Advanced WAF (previously licensed as ASM) v16.1
F5N_BIG-EGW-APM, Configuring BIG-IP APM: Access Policy Manager v.16.1
F5N_BIG-IRULE-CFG, Developing iRules for BIG-IP v.16.1
Other courses available: F5N_BIG-TRBL-INT2, Troubleshooting BIG-IP v.16.1

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

On request. Please Contact Us

Additional Information

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