F5-TRG-BIG-AFM-CFG
Configuring BIG-IP AMF: Advanced Firewall Manager v15.1

Overview

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.

Course Length

2 days

Topics covered in this course Include

- 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
- Network Firewall iRules
- Port Misuse
- Various AFM component troubleshooting commands

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:

- 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

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

- HTTP and DNS protocols

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
  - 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

- 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
  - Filtering Logs with the Custom Search Facility
  - 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 Black and White Lists
  - 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 IP Intelligence Policy
  - Troubleshooting
  - IP Intelligence iRule
- 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 Schedule 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