Configuring BIG-IP AFM: Advanced Firewall Manager

Length 2 Days

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.

Participants

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.

Objectives

- Installation and setup 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

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 Resources
- BIG-IP System Setup Labs

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
- Send to Virtual
- Packet Tester

Chapter 3: Logs
- 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

Chapter 4: IP Intelligence
- 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

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
- 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
- Firewall Manager

Chapter 7: DoS White Lists
- White Lists
- Configuration
- tmsh
- Source Address List

Chapter 8: DoS Sweep Flood Protection
- Sweep Flood
- Configuration

Chapter 9: IP Intelligence Shun
- IP Intelligence Shun
- Manual Configuration
- Dynamic Configuration
- IP Intelligence Policy
- tmsh
- Extending the Shun Feature
- Remotely Triggered Black Hole
- Scrubber

Chapter 10: DNS Firewall
- DNS Firewall
- Configuration
- DNS Query
- DNS Opcodes
- Logging
- Troubleshooting

Chapter 11: DNS DoS
- DNS DoS
- Configuration
- DoS Protection Profile
- Device DoS

Chapter 12: SIP DoS
- Session Initiation Protocol (SIP)
- Transactions and Dialogs
- SIP DoS Configuration
- DoS Protection Profile
- Device DoS
- SIP iRules

Chapter 13: Network Firewall iRules
- Network Firewall iRules
- iRule Events
- Configuration
- Recommended Practice
- More Information

Chapter 14: Port Misuse
- Port Misuse
- Port Misuse Policy
- Attaching a Service Policy
- Log Profile

Chapter 15: Additional Training and Certification
- Getting Started Series Web-Based Training
- F5 Instructor Led Training Curriculum
- F5 Professional Certification Program

Appendix A: Troubleshooting
- Support Requirements
- tmsh commands
- Tools
- Log and Other Files

Appendix B: Lab Scripts
- Scripts
- Installation