F5 Networks Configuring BIG-IP AFM v13: Advanced Firewall Manager

Course Summary

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.

Topics

- Setting up the BIG-IP System
- AFM Overview and Network Firewall
- Logs
- IP Intelligence
- Device DoS
- Reports
- DoS White Lists
- DoS Sweep Flood Protection

- IP Intelligence Shun
- DNS Firewall
- DNS DoS
- SIP DoS
- Network Firewall iRules
- Port Misuse
- Additional Training and Certification

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

Administering BIG-IP, OSI model, TCP/IP addressing and routing, WAN, LAN environments, and server redundancy concepts; or having achieved TMOS Administration Certification

Duration

Two days

F5 Networks Configuring BIG-IP AFM v13: Advanced Firewall Manager

Course Outline

I. Setting up the BIG-IP System
A. Introducing the BIG-IP System
B. Initially Setting Up the BIG-IP System
C. Archiving the BIG-IP Configuration
D. Leveraging F5 Support Resources and Tools
E. Chapter Resources
F. BIG-IP System Setup Labs

G. AFM Overview and Network Firewall
H. AFM Overview
I. AFM Release History
J. AFM Availability
K. What do you see?
L. Terminology
M. Network Firewall
N. AFM Contexts
O. AFM Modes
P. AFM Packet Processing
Q. AFM Rules and Direction
R. Rules Contexts and Processing
S. Configuring Network Firewall
T. Network Firewall Rules
U. Geolocation
V. Redundant and Conflicting Rules
W. Stale Rules
X. Lists and Schedules
Y. Rule Lists
Z. Address Lists
AA. Port Lists
BB. Schedules
CC. Policies
DD. Policy Status and Firewall Policy Management
EE. Inline Rule Editor
FF. Send to Virtual
GG. Packet Tester

II. Logs
A. Overview
B. Event Logs
C. Logging Profiles
D. Log Throttling
E. Logging and Logging Profiles
F. BIG-IP Logging Mechanisms
G. Publisher

H. Log Destination
I. Custom Search
J. Logging Global Rule Events
K. Log Configuration Changes
L. QKView and Log Files
M. SNMP MIB
N. SNMP Traps

III. IP Intelligence
A. Overview
B. Feature 1 Dynamic Black and White Lists
C. Black List Categories
D. Feed Lists
E. IP Intelligence Policies
F. IP Intelligence Log Profile
G. IP Intelligence Reporting
H. Troubleshooting IP Intelligence Lists
I. Feature 2 IP Intelligence Database
J. Licensing
K. Installation
L. Configuration
M. Troubleshooting
N. IP Intelligence iRule

IV. Device DoS
A. Denial of Service and DoS Protection Overview
B. Device DoS
C. Configuring Device DoS
D. Variant 1
E. Variant 2
F. Auto-Threshold Configuration
G. Variant 3
H. Bad Actor and Blacklist Address
I. Device DoS Profiles
J. DoS Protection Profile
K. Dynamic Signatures
L. DoS iRules

F5 Networks Configuring BIG-IP AFM v13: Advanced Firewall Manager

Course Outline (cont'd)

V. Reports
- A. Reports
- B. Reporting
- C. General Reporting Facilities
- D. Time Series Chart
- E. Details
- F. Report Export
- G. DoS Screens
- H. Dashboard
- I. Analysis
- J. Custom Page
- K. Settings
- L. Scheduled Reports
- M. Troubleshooting Scheduled Reports
- N. Overview
- O. Summary
- P. Widgets
- Q. Custom Widgets
- R. Deleting and Restoring Widgets
- S. Firewall Manager

VI. DoS White Lists
- A. White Lists
- B. Configuration
- C. tmsh
- D. Source Address List

VII. DoS Sweep Flood Protection
- A. Sweep Flood
- B. Configuration

VIII. IP Intelligence Shun
- A. IP Intelligence Shun
- B. Manual Configuration
- C. Dynamic Configuration
- D. IP Intelligence Policy
- E. tmsh
- F. Extending the Shun Feature
- G. Remotely Triggered Black Hole
- H. Scrubber

IX. DNS Firewall
- A. DNS Firewall
- B. Configuration
- C. DNS Query
- D. DNS Opcodes
- E. Logging
- F. Troubleshooting

X. DNS DoS
- A. DNS DoS
- B. Configuration
- C. DoS Protection Profile
- D. Device DoS

XI. SIP DoS
- A. Session Initiation Protocol (SIP)
- B. Transactions and Dialogs
- C. SIP DoS Configuration
- D. DoS Protection Profile
- E. Device DoS
- F. SIP iRules

XII. Network Firewall iRules
- A. Network Firewall iRules
- B. iRule Events
- C. Configuration
- D. Recommended Practice
- E. More Information

XIII. Port Misuse
- A. Port Misuse
- B. Port Misuse Policy
- C. Attaching a Service Policy
- D. Log Profile

XIV. Additional Training and Certification
- A. Getting Started Series Web-Based Training
- B. F5 Instructor Led Training Curriculum
- C. F5 Professional Certification Program