Course Outline

F5 Networks Configuring BIG-IP AFM v14: 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.

Objectives

After taking this course, students will be able to:

- 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

Course Outline

F5 Networks Configuring BIG-IP AFM v14: Advanced Firewall Manager

Course Summary

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.

Prerequisite

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

Course Outline

F5 Networks Configuring BIG-IP AFM v14: 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 Lab

II. ***AFM Overview and Network Firewall***
- A. AFM Overview
- B. AFM Release History
- C. AFM Availability
- D. What do you see?
- E. Terminology
- F. Network Firewall
- G. AFM Contexts
- H. AFM Modes
- I. AFM Packet Processing
- J. AFM Rules and Direction
- K. Rules Contexts and Processing
- L. Configuring Network Firewall
- M. Network Firewall Rules
- N. Geolocation
- O. Redundant and Conflicting Rules
- P. Stale Rules
- Q. Lists and Schedules
- R. Rule Lists
- S. Address Lists
- T. Port Lists
- U. Schedules
- V. Policies
- W. Policy Status and Firewall Policy Management
- X. Inline Rule Editor
- Y. Send to Virtual
- Z. Packet Tester

III. ***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

IV. ***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

V. ***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

VI. ***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

Course Outline

F5 Networks Configuring BIG-IP AFM v14: Advanced Firewall Manager

Course Outline (cont.)

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

VII. ***DoS White Lists***
A. White Lists
B. Configuration
C. tmsh
D. Source Address List

VIII. ***DoS Sweep Flood Protection***
A. Sweep Flood
B. Configuration

IX. ***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

X. ***DNS Firewall***
A. DNS Firewall
B. Configuration
C. DNS Query
D. DNS Opcodes
E. Logging
F. Troubleshooting

XI. ***DNS DoS***
A. DNS DoS
B. Configuration
C. DoS Protection Profile
D. Device DoS

XII. ***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

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

XIV. ***Port Misuse***
A. Port Misuse
B. Port Misuse Policy
C. Attaching a Service Policy
D. Log Profile

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