Configuring BIG-IP AFM:

Advanced Firewall Manager

LANTEC
OF LOUISIANA, LLC
CORPORATE TRAINING CENTER

Days: 2

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.

- 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

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.

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.

Configuring BIG-IP AFM:

Advanced Firewall Manager

Course 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

OUTLINE:

LESSON 1: SETTING UP THE BIG-IP SYSTEM

- Introducing the BIG-IP System
- Initially Setting Up the BIG-IP System
- Archiving the BIG-IP System Configuration
- Leveraging F5 Support Resources and Tools

LESSON 2: AFM OVERVIEW AND NETWORK FIREWALL

- AFM Overview
- AFM Availability
- AFM and the BIG-IP Security Menu
- Explaining F5 Terminology
- Network Firewall
- Contexts
- Modes
- Packet Processing
- Rules and Direction

Configuring BIG-IP AFM:

Advanced Firewall Manager

- 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

LESSON 3: 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

LESSON 4: IP INTELLIGENCE

- Overview
- Feature 1 Dynamic White and Black 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

LESSON 5: 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 Threshold Configuration
- Variant 3 DoS Vectors
- Device DoS Profiles
- DoS Protection Profile
- Dynamic Signatures
- Dynamic Signatures Configuration
- DoS iRules

LESSON 6: REPORTS

- AFM Reporting Facilities Overview
- Examining the Status of Particular AFM Features
- Exporting the Data
- Managing the Reporting Settings
- Scheduling Reports
- Examining AFM Status at High Level
- Mini Reporting Windows (Widgets)
- Building Custom Widgets
- Deleting and Restoring Widgets
- Dashboards

LESSON 7: DOS WHITE LISTS

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

LESSON 8: DOS SWEEP FLOOD PROTECTION

- Isolating Bad Clients with Sweep Flood
- Configuring Sweep Flood

Configuring BIG-IP AFM:

Advanced Firewall Manager

LESSON 9: IP INTELLIGENCE SHUN

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

LESSON 10: DNS FIREWALL

- Filtering DNS Traffic with DNS Firewall
- Configuring DNS Firewall
- DNS Query Types
- DNS Opcode Types
- Logging DNS Firewall Events
- Troubleshooting

LESSON 11: DNS DOS

- Overview
- DNS DoS
- Configuring DNS DoS
- DoS Protection Profile
- Device DoS and DNS

LESSON 12: SIP DOS

- Session Initiation Protocol (SIP)
- Transactions and Dialogs
- SIP DoS Configuration
- DoS Protection Profile
- Device DoS and SIP

LESSON 13: PORT MISUSE

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

LESSON 14: NETWORK FIREWALL IRULES

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