New Horizons®
An Educate 360 Brand

F5 Networks Configuring BIG-IP AFM: Advanced Firewall Manager

Price	Duration	Delivery Methods
$2,310.00	2 Days	VILT, Private Group

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.

Who Should Attend

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.

Agenda

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

2 - AFM OVERVIEW

- AFM Overview
- AFM Availability
- AFM and the BIG-IP Security Menu

3 - NETWORK FIREWALL

- AFM Firewalls
- 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

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

5 - IP INTELLIGENCE

- Overview
- IP Intelligence Policy

- Feature 1 Dynamic White and Black Lists
- Black List Categories
- Feed Lists
- IP Intelligence Log Profile
- IP Intelligence Reporting
- Troubleshooting IP Intelligence Lists
- Feature 2 IP Intelligence Database
- Licensing
- Installation
- Configuration
- Troubleshooting
- IP Intelligence iRule

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

7 - 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

8 - DOS WHITE LISTS

- Bypassing DoS Checks with White Lists
- Configuring DoS White Lists
- tmsh options

- Per Profile Whitelist Address List

9 - DOS SWEEP FLOOD PROTECTION

- Isolating Bad Clients with Sweep Flood
- Configuring Sweep Flood

10 - 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

11 - DNS FIREWALL

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

12 - DNS DOS

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

13 - SIP DOS

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

14 - PORT MISUSE

- Overview
- Port Misuse and Service Policies
- Building a Port Misuse Policy
- Attaching a Service Policy

- Creating a Log Profile

15 - NETWORK FIREWALL IRULES

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

16 - RECAP

- BIG-IP Architecture and Traffic Flow
- AFM Packet Processing Overview