F5 Networks Configuring BIG-IP AFM v12: Advanced Firewall Manager (F5-AFM-12)

Modality: Virtual Classroom

Duration: 2 Days

About this course:

The course ware of F5 Networks Configuring BIG-IP AFM v12: Advanced Firewall Manager (F5-AFM-12) is a combination of theory and practical. It is designed by subject experts to provide an authentic learning experience to students, starting from the installation to effectively using the firewall, and protect against Denial of service attacks.

Lab work is also part of the cyber security classes to facilitate practical learning experience. It allows students to utilize theoretical knowledge o working with a firewall. They learn and practice on real life interface to not only configure and build AFM network firewall, but also to detect and protect against potential threats of DoS for DNS and SIP traffic. Students also get to learn about reporting and log facilities.

A Network Engineer makes up to **$77,484** per year.

Course Objective:

After completing this course, students will be able to:

- 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 and DoS iRules
- Various AFM component troubleshooting commands

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 Advanced Firewall Manager (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

Suggested prerequisites courses:

- F5 Networks Administering BIG-IP v12 (F5-NetAdmin-v12)

Course 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

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

Lesson 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

Lesson 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

Lesson 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

Lesson 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

Lesson 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

Lesson 8: DoS White Lists

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

Lesson 9: DoS Sweep Flood Protection

- Isolating Bad Clients with Sweep Flood
- Configuring Sweep Flood

Lesson 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

Lesson 11: DNS Firewall

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

Lesson 12: DNS DoS

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

Lesson 13: SIP DoS

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

Lesson 14: Port Misuse

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

Lesson 15: Network Firewall iRules

- Overview
- iRule Events

- Configuration
- When to use iRules
- More Information

Lesson 16: Recap

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