F5 NETWORKS CONFIGURING BIG-IP AFM: ADVANCED FIREWALL MANAGER

Course Code: 100337

Learn 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.

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.

What You'll Learn

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.

Who Needs to 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.

Prerequisites

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

F5 NETWORKS CONFIGURING BIG-IP AFM: ADVANCED FIREWALL MANAGER

Course Code: 100337

CLASSROOM LIVE	$2,420 USD	2 Day

Classroom Live 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
- 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

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

F5 NETWORKS CONFIGURING BIG-IP AFM: ADVANCED FIREWALL MANAGER

Course Code: 100337

VIRTUAL CLASSROOM LIVE	$2,420 USD	2 Day

Virtual Classroom Live 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
- 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

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

Jun 26 - 27, 2025 | 7:00 AM - 3:30 PM PDT

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/2/2025 5:20:27 PM