Red Education

F5 CONFIGURING BIG-IP AFM: ADVANCED FIREWALL MANAGER

DURATION - 2 DAYS
COURSE LEVEL : CORE

Description

Learn how to deploy and operate BIG-IP Advanced Firewall Manager to protect a data center against incoming threats that enter the network at layers 3 and 4 on common protocols, including HTTP, SIP, SSH, SSL, and others. Using a mix of lectures and hands-on lab exploration, gain experience implementing comprehensive protection against attacks from rapidly changing IP addresses by applying the latest threat intelligence, and by anticipating, detecting, and responding to attacks before they hit data center targets. Practice using hardware-based DDoS mitigation that scales to prevent high-volume, targeted, network flood attacks—while allowing legitimate traffic to flow without compromising performance or degrading the user experience. Observe malicious network activity in real time as you assume the role of an attacker.

F5 recognizes the importance of visibility, analytics, and reporting regarding attack evolution, attack mitigation, and overall firewall health. Plenty of time is dedicated to analyzing reports. Learn how to retrieve clear, concise, and actionable information highlighting attacks and trends with detailed drill-down and page-view capabilities.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.

Course Outline:

Chapter 1: Setting Up the BIG-IP System

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

Chapter 2: AFM Overview

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

Chapter 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

Chapter 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
- Logging Global Rule Events
- Log Configuration Changes
- QKView and Log Files
- SNMP MIB
- SNMP Traps

Chapter 5: IP Intelligence

- Overview
- IP Intelligence Policy
- Feature 1: Dynamic White and Blacklists
- Blacklist Categories
- Feed Lists
- Applying for an IP Intelligence Policy
- IP Intelligence Log Profile
- IP Intelligence Reporting
- Troubleshooting IP Intelligence Lists
- Feature 2: IP Intelligence Database
- Licensing

- Installation
- Linking the Database to the IP Intelligence Policy
- Troubleshooting
- IP Intelligence iRules

Chapter 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 Configuration or Automatic Thresholds
- Variant 3 DoS Vectors
- Device DoS Profiles
- DoS Protection Profile
- Dynamic Signatures
- Dynamic Signatures Configuration
- DoS iRules

Chapter 7: Reports

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

Chapter 8: DoS White Lists

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

Chapter 9: DoS Sweep Flood Protection

- Isolating Bad Clients with Sweep Flood
- Configuring Sweep Flood

Chapter 10: IP Intelligence Shun

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

Chapter 11: DNS Firewall

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

Chapter 12: DNS DoS

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

Chapter 13 : SIP DoS

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

Chapter 14: Port Misuse

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

Chapter 15: Network Firewall iRules

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

Chapter 16: Recap

- BIG-IP Architecture and TraƯic FlowConfiguring DNS Firewall
- AFM Packet Processing Overview

Chapter 17: Additional Training and Certification

- Getting Started Series Web-Based Training
- F5 Instructor-Led Training Curriculum
- F5 Professional Certification Program