Configuring BIG-IP AFM: Advanced

Firewall Manager v15

Chapter 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

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
- Filtering Logs with the Custom Search Facility
- 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
- Black List Categories
- Feed Lists
- Applying 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 P Intelligence Policy
- Troubleshooting
- IP Intelligence iRule

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 List

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 Traffic 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 Traffic Flow
- 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