TRENDS | Academy
Learning | Evolving | Empowering

F5 Configuring BIG-IP AFM: Advanced Firewall Manager

Duration: 2 Days

Prerequisites:

The following course-specific knowledge and experience is suggested before attending this course:

- HTTP and DNS protocols

Course Description:

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

Course Objectives:

- Configure and manage an AFM system
- Configure AFM Network Firewall in a positive or negative security model
- Configure Network Firewall to allow or deny network traffic using rules based on protocol, source, destination, geography, and other predicate types
- Prebuild firewall rules using lists and schedule components
- Enforce firewall rules immediately or test them using policy staging
- Use Packet Tester and Flow Inspector features to check network connections against your security configurations for Network Firewall, IP intelligence and DoS features
- Configure various IP Intelligence features to identify, record, allow or deny access by IP address
- Configure the Device DoS detection and mitigation feature to protect the BIG-IP device and all applications from multiple types of attack vectors
- Configure DoS detection and mitigation on a per-profile basic to protect specific applications from attack
- Use DoS Dynamic Signatures to automatically protect the system from DoS attacks based on long term traffic and resource load patterns

- Configure and use the AFM local and remote log facilities
- Configure and monitor AFM's status with various reporting facilities
- Export AFM system reports to your external monitoring system directly or via scheduled mail
- Allow chosen traffic to bypass DoS checks using Whitelists
- Isolate potentially bad clients from good using the Sweep Flood feature
- Isolate and re-route potentially bad network traffic for further inspection using IP Intelligence Shun functionality
- Restrict and report on certain types of DNS requests using DNS Firewall
- Configure, mitigate, and report on DNS based DoS attacks with the DNS DoS facility
- Configure, mitigate, and report on SIP based DoS attacks with the SIP DoS facility
- Configure, block, and report on the misuse of system services and ports using the Port Misuse feature
- Build and configure Network Firewall rules using BIG-IP iRules
- Be able to monitor and do initial troubleshooting of various AFM functionalitysolutions on AskF5, submitting a problem ticket to F5 Technical Support, and view traffic flow using tcpdump

Intended Audience:

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 Outlines:

- Configuration and management 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
- Port Misuse
- Network Firewall iRules
- Various AFM component troubleshooting
- commands

REGISTER NOW!
training@trends.com.ph
(+632) 8863-2123
www.trendsacademy.com.ph