Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Configuring BIG-IP AFM: Advanced Firewall Manager v.15.1

CODE:	LENGTH:	PRICE:
F5N_BIG-AFM	16 Hours (2 days)	€1,795.00

Description

This 2 day course uses lectures and hands-on lab exercises to give participants real-time experience in setting up and configuring the BIG-IP® Advanced Firewall Manager 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.

- Configuration and management of the BIGIP 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

Topics Covered• Various AFM component troubleshooting commands

Objectives

After completing this course, participants will be able to complete the following tasks: • 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 functionality

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.

Prerequisites

Students must complete one of the following F5 prerequisites before attending this course:
• Administering BIG-IP instructor-led course or
• F5 Certified BIG-IP Administrator
The following free web-based courses, although optional, will be very helpful for any student with limited BIG-IP administration and configuration experience. These courses are available at LearnF5 (https://www.f5.com/services/training):
• Getting Started with BIG-IP web-based training
• Getting Started with BIG-IP Local Traffic Manager (LTM) web-based training
• Getting Started with BIG-IP Advanced Firewall Manager (AFM) web-based training
The following general network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course:
• OSI model encapsulation
• Routing and switching
• Ethernet and ARP
• TCP/IP concepts
• IP addressing and subnetting
• NAT and private IP addressing
• Default gateway
• Network firewalls
• LAN vs. WAN   The following course-specific knowledge and experience is suggested before attending this course:
• HTTP and DNS protocols

Programme

                         • Introducing the BIG-IP System
                         • Initially Setting Up the BIG-IP System
                         • Archiving the BIG-IP System Configuration
Chapter 1: Setting up the BIG-IP System• Leveraging F5 Support Resources and ToolsChapter 2: AFM Overview
                         • AFM Overview
                         • 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
• AFM Overview   • Redirecting Traffic with Send to Virtual
• AFM Availability   • Checking Rule Processing with Packet Tester
• AFM and the BIG-IP Security MenuChapter 3: Network Firewall• Examining Connections with Flow Inspector

Follow on courses

F5N_BIG-LTM-CFG-3, Configuring BIG-IP LTM: Local Traffic Manager v.15.1
F5N_BIG-DNS-I, Configuring BIG-IP DNS (formerly GTM) v.15.1
F5N_BIG-AWF-CFG, Configuring F5 Advanced WAF (previously licensed as ASM) v15.1
F5N_BIG-EGW-APM, Configuring BIG-IP APM: Access Policy Manager v.15.1
F5N_BIG-IRULE-CFG, Developing iRules for BIG-IP v.15.1
Other courses available:F5N_BIG-TRBL-INT2, Troubleshooting BIG-IP v.15.1

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
30 May 2024	Virtual Classroom (CET / UTC+1)	CEDT	English	Instructor Led Online		€1,795.00

Additional Information

This training is also available as onsite training. Please contact us to find out more.