Szkolenie: F5 Networks
Configuring BIG-IP AFM Advanced Firewall Manager

<table>
<thead>
<tr>
<th>FORMA SZKOLENIA</th>
<th>MATERIAŁY SZKOLENIOWE</th>
<th>CENA</th>
<th>CZAS TRWANIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacjonarne</td>
<td>Tradycyjne</td>
<td>8700 PLN NETTO*</td>
<td>2 dni</td>
</tr>
<tr>
<td>Stacjonarne</td>
<td>Tablet CTAB</td>
<td>9100 PLN NETTO*</td>
<td>2 dni</td>
</tr>
<tr>
<td>Metoda dlearning</td>
<td>Tradycyjne</td>
<td>8700 PLN NETTO*</td>
<td>2 dni</td>
</tr>
<tr>
<td>Metoda dlearning</td>
<td>Tablet CTAB</td>
<td>8700 PLN NETTO*</td>
<td>2 dni</td>
</tr>
</tbody>
</table>

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE
Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00
Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

DOSTĘPNE TERMINY
2019-12-16  | 2 dni  | Warszawa
2019-12-16  | 2 dni  | Warszawa
2020-01-13  | 2 dni  | Warszawa
2020-01-13  | 2 dni  | Warszawa
2020-03-30  | 2 dni  | Kraków
2020-03-30  | 2 dni  | Kraków

Cel szkolenia:
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** 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.

Audience:
This course is intended for system administrators, network administrators, security administrators, and security architects responsible for installation, setup, configuration, and administration of the **BIG-IP Advanced Firewall Manager (AFM)** system.

Course is based on the system version v14.
Plan szkolenia:

- 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
- AFM Overview and Network Firewall
  - AFM Overview
  - AFM Release History
  - AFM Availability
  - What do you see?
  - Terminology
  - Network Firewall
  - AFM Contexts
  - AFM Modes
  - AFM Packet Processing
  - AFM Rules and Direction
  - Rules Contexts and Processing
  - Configuring Network Firewall
  - Network Firewall Rules
  - Geolocation
  - Redundant and Conflicting Rules
  - Stale Rules
  - Lists and Schedules
  - Rule Lists
  - Address Lists
  - Port Lists
  - Schedules
  - Policies
  - Policy Status and Firewall Policy Management
  - Inline Rule Editor
- Logs
  - Event Logs
  - Logging Profiles
  - Log Throttling
Traffic Flow Statistics
Logging and Logging Profiles
BIG-IP Logging Mechanisms
Publisher
Log Destination
Custom Search
Logging Global Rule Events
Log Configuration Changes
QKView
Other Log Files
SNMP MIB
SNMP Traps
IP Intelligence
Overview
Architecture
Feature 1 Dynamic Black and White 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
Device DoS
Policies
Policy Status and Firewall Policy Management
Inline Rule Editor
Reports
Reports
Reporting
General Reporting Facilities
- Charts
- Details
- Report Export
- Network Screens
- DoS Screens
- Settings
- Overview
- Summary
- Widgets
- Time Periods, Settings, Export, and Delete Options
- Firewall Manager
  - DoS White Lists
    - White Lists
    - Configuration
    - tmsh
  - DoS Sweep Flood Protection
    - Sweep Flood
    - Configuration
  - IP Intelligence Shun
    - IP Intelligence Shun
    - Manual
    - Dynamic
    - IP Intelligence Policy
    - tmsh
    - Troubleshooting
  - DNS Firewall
    - DNS Firewall
    - DNS Query
    - DNS Opcodes
    - Troubleshooting
  - DNS DoS
    - DNS DoS
    - DoS Protection Profile
    - Device DoS
  - SIP DoS
    - Session Initiation Protocol (SIP)
Transactions and Dialogs
- SIP DoS
- DoS Protection Profile
- Device DoS
- SIP iRules

Network Firewall iRules
- Network Firewall iRules
- iRule Events
- Use Cases
- Recommended Practice
- More Information

DoS iRules
- DoS iRules
- iRule Events
- Use Cases
- More Information

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

Wymagania:

Before attending the Troubleshooting, ASM, DNS, APM, AAM, AFM, VIPRION or iRules courses is mandatory:

- to take part in the BIG-IP Admin or LTM course
- or possession of F5-CA or F5-CTS LTM certification
- or pass special assessment test with score 70% or greater.

To take assessment test:
**Step 1:** get an account on F5 University [https://university.f5.com](https://university.f5.com)
**Step 2:** goto My Training and find Administering BIG-IP Course Equivalency Assessment
Take the test. Pass mark is 70%
**Step 3:** take a screen shot as proof of results
If this prerequisite is not met, F5 Networks have the right to refuse entry to the class.
Poziom trudności

Certyfikaty:

The participants will obtain certificates signed by F5 Networks (course completion).

Prowadzący:

Certified F5 Networks Trainer.