

Szkozenie: F5 Networks Configuring BIG-IP F5 Advanced WAF



DOSTĘPNE TERMINY

2024-08-19	4 dni	Virtual Classroom
2024-08-19	4 dni	Warszawa / Wirtualna sala (Termin gwarantowany)
2024-09-23	4 dni	Kraków / Wirtualna sala
2024-09-23	4 dni	Virtual Classroom
2024-10-21	4 dni	Virtual Classroom
2024-10-21	4 dni	Warszawa / Wirtualna sala
2024-11-12	4 dni	Kraków / Wirtualna sala
2024-11-12	4 dni	Virtual Classroom
2024-12-16	4 dni	Virtual Classroom
2024-12-16	4 dni	Warszawa / Wirtualna sala

Cel szkolenia:

In this 4 day course, students are provided with a functional understanding of how to deploy, tune, and operate F5 Advanced Web Application Firewall to protect their web applications from HTTP-based attacks.

The course includes lecture, hands-on labs, and discussion about different F5 Advanced Web Application Firewall tools for detecting and mitigating threats from multiple attack vectors such web scraping, Layer 7 Denial of Service, brute force, bots, code injection, and zero-day exploits.

Course Objectives

- Describe the role of the BIG-IP system as a full proxy device in an application delivery network
- Provision F5 Advanced Web Application Firewall resources
- Define a web application firewall
- Describe how F5 Advanced Web Application Firewall protects a web application by securing file types, URLs, and parameters
- Deploy F5 Advanced Web Application Firewall using the Rapid Deployment template (and other templates) and define the security checks included in each
- Define learn, alarm, and block settings as they pertain to configuring F5 Advanced Web Application Firewall
- Define attack signatures and explain why attack signature staging is important
- Contrast positive and negative security policy implementation and explain benefits of each
- Configure security processing at the parameter level of a web application

- Use an application template to protect a commercial web application
- Deploy F5 Advanced Web Application Firewall using the Automatic Policy Builder
- Tune a policy manually or allow automatic policy building
- Integrate third party application vulnerability scanner output into a security policy
- Configure login enforcement and session tracking
- Configure protection against brute force, web scraping, and Layer 7 denial of service attacks
- Implement iRules using specific F5 Advanced Web Application Firewall events and commands
- Use Content Profiles to protect JSON and AJAX-based applications
- Implement Bot Signatures
- Implement Proactive Bot Defense

Audience:

this course is intended for security and network administrators who will be responsible for the installation, deployment, tuning, and day-to-day maintenance of the F5 Advanced Web Application Firewall.

Plan szkolenia:

- 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
- Traffic Processing with BIG-IP
 - Identifying BIG-IP Traffic Processing Objects
 - Overview of Network Packet Flow
 - Understanding Profiles
 - Overview of Local Traffic Policies
 - Visualizing the HTTP Request Flow
- Web Application Concepts
 - Overview of Web Application Request Processing
 - Web Application Firewall: Layer 7 Protection
 - F5 Advanced WAF Layer 7 Security Checks
 - Overview of Web Communication Elements
 - Overview of the HTTP Request Structure
 - Examining HTTP Responses
 - How F5 Advanced WAF Parses File Types, URLs, and Parameters
 - Using the Fiddler HTTP Proxy

- Common Web Application Vulnerabilities
 - A Taxonomy of Attacks: The Threat Landscape
 - What Elements of Application Delivery are Targeted?
 - Common Exploits Against Web Applications
- Security Policy Deployment
 - Defining Learning
 - Comparing Positive and Negative Security Models
 - The Deployment Workflow
 - Policy Type: How Will the Policy Be Applied
 - Policy Template: Determines the Level of Protection
 - Policy Templates: Automatic or Manual Policy Building
 - Assigning Policy to Virtual Server
 - Deployment Workflow: Using Advanced Settings
 - Selecting the Enforcement Mode
 - The Importance of Application Language
 - Configure Server Technologies
 - Verify Attack Signature Staging
 - Viewing Requests
 - Security Checks Offered by Rapid Deployment
 - Defining Attack Signatures
 - Using Data Guard to Check Responses
- Policy Tuning and Violations
 - Post-Deployment Traffic Processing
 - Defining Violations
 - Defining False Positives
 - How Violations are Categorized
 - Violation Rating: A Threat Scale
 - Defining Staging and Enforcement
 - Defining Enforcement Mode
 - Defining the Enforcement Readiness Period
 - Reviewing the Definition of Learning
 - Defining Learning Suggestions
 - Choosing Automatic or Manual Learning
 - Defining the Learn, Alarm and Block Settings
 - Interpreting the Enforcement Readiness Summary
 - Configuring the Blocking Response Page

- Attack Signatures
 - Defining Attack Signatures
 - Attack Signature Basics
 - Creating User-Defined Attack Signatures
 - Defining Simple and Advanced Edit Modes
 - Defining Attack Signature Sets
 - Defining Attack Signature Pools
 - Understanding Attack Signatures and Staging
 - Updating Attack Signatures
- Positive Security Policy Building
 - Defining and Learning Security Policy Components
 - Defining the Wildcard
 - Defining the Entity Lifecycle
 - Choosing the Learning Scheme
 - How to Learn: Never (Wildcard Only)
 - How to Learn: Always
 - How to Learn: Selective
 - Reviewing the Enforcement Readiness Period: Entities
 - Viewing Learning Suggestions and Staging Status
 - Violations Without Learning Suggestions
 - Defining the Learning Score
 - Defining Trusted and Untrusted IP Addresses
 - How to Learn: Compact
- Cookies and Other Headers
 - F5 Advanced WAF Cookies: What to Enforce
 - Defining Allowed and Enforced Cookies
 - Configuring Security Processing on HTTP headers
- Reporting and Logging
 - Overview: Big Picture Data
 - Reporting: Build Your Own View
 - Reporting: Chart based on filters
 - Brute Force and Web Scraping Statistics
 - Viewing F5 Advanced WAF Resource Reports
 - PCI Compliance: PCI-DSS 3.0
 - The Attack Expert System
 - Viewing Traffic Learning Graphs

- Local Logging Facilities and Destinations
- How to Enable Local Logging of Security Events
- Viewing Logs in the Configuration Utility
- Exporting Requests
- Logging Profiles: Build What You Need
- Configuring Response Logging
- Lab Project 1
- Advanced Parameter Handling
 - Defining Parameter Types
 - Defining Static Parameters
 - Defining Dynamic Parameters
 - Defining Dynamic Parameter Extraction Properties
 - Defining Parameter Levels
 - Other Parameter Considerations
- Policy Diff and Administration
 - Comparing Security Policies with Policy Diff
 - Merging Security Policies
 - Restoring with Policy History
 - Examples of F5 Advanced WAF Deployment Types
 - ConfigSync and F5 Advanced WAF Security Data
 - ASMQVIEW: Provide to F5 Support for Troubleshooting
- Automatic Policy Building
 - Overview of Automatic Policy Building
 - Defining Templates Which Automate Learning
 - Defining Policy Loosening
 - Defining Policy Tightening
 - Defining Learning Speed: Traffic Sampling
 - Defining Track Site Changes
- Web Application Vulnerability Scanner Integration
 - Integrating Scanner Output into F5 Advanced WAF
 - Will Scan be Used for a New or Existing Policy?
 - Importing Vulnerabilities
 - Resolving Vulnerabilities
 - Using the Generic XML Scanner XSD file
- Layered Policies
 - Defining a Parent Policy

- Defining Inheritance
- Parent Policy Deployment Use Cases
- Login Enforcement, Brute Force Mitigation, and Session Tracking
 - Defining Login Pages
 - Configuring Automatic Detection of Login Pages
 - Defining Session Tracking
 - What Are Brute Force Attacks?
 - Brute Force Protection Configuration
 - Defining Source-Based Protection
 - Source-Based Brute Force Mitigations
 - Defining Session Tracking
 - Configuring Actions Upon Violation Detection
 - Session Hijacking Mitigation Using Device ID
- Web Scraping Mitigation and Geolocation Enforcement
 - Defining Web Scraping
 - Mitigating Web Scraping
 - Defining Geolocation Enforcement
 - Configuring IP Address Exceptions
- Layer 7 DoS Mitigation and Advanced Bot Protection
 - Defining Denial of Service Attacks
 - The General Flow of DoS Protection
 - Defining the DoS Profile
 - Overview of TPS-based DoS Protection
 - Applying TPS mitigations
 - Create a DoS Logging Profile
 - Defining DoS Profile General Settings
 - Defining Bot Signatures
 - Defining Proactive Bot Defense
 - Defining Behavioral and Stress-Based Detection
 - Defining Behavioral DoS Mitigation
- F5 Advanced WAF and iRules
 - Common Uses for iRules
 - Identifying iRule Components
 - Triggering iRules with Events
 - Defining F5 Advanced WAF iRule Events
 - Defining F5 Advanced WAF iRule Commands

- Using F5 Advanced WAF iRule Event Modes
- Using Content Profiles
 - Defining Asynchronous JavaScript and XML
 - Defining JavaScript Object Notation (JSON)
 - Defining Content Profiles
 - The Order of Operations for URL Classification
- Review and Final Labs
 - Final Lab Project (Option 1) – Production Scenario
 - Final Lab Project (Option 2) – JSON Parsing with the Default JSON Profile
 - Final Lab Project (Option 3) – Managing Traffic with L7 Local Traffic Policies

Wymagania:

There are no F5-technology-specific prerequisites for this course. However, completing the following before attending would be very helpful for students with limited BIG-IP administration and configuration experience:

- Administering BIG-IP instructor-led course

-or-

- F5 Certified BIG-IP Administrator

The following free web-based training courses, although optional, will be very helpful for any student with limited BIG-IP administration and configuration experience. These courses are available at [F5 University](#):

- [Getting Started with BIG-IP](#) web-based training
- [Getting Started with BIG-IP Application Security Manager \(ASM\)](#) 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

Poziom trudności



Certyfikaty:

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

Prowadzący:

Certified F5 Networks Trainer.