



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Arrow ECS Internet Security AG, Richtistrasse 11, CH-8304 Wallisellen

Email: trainings.ecs.ch@arrow.com
Phone: +41 43 222 80 00



Configuring F5 Advanced WAF (previously licensed as ASM) v14

CODE:

F5N_BIG-AWF-CFG

LENGTH:

32 Hours (4 days)

PRICE:

CHF5,550.00

Description

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 as web scraping, Layer 7 Denial of Service, brute force, bots, code injection, and zero day exploits.

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.

Prerequisites

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)
- 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

Programme

- Setting Up the BIG-IP System
- Traffic Processing with BIG-IP
- Web Application Concepts
- Common Web Application Vulnerabilities
- Security Policy Deployment
- Policy Tuning and Violations
- Attack Signatures
- Positive Security Policy Building
- Cookies and Other Headers
- Reporting and Logging
- Lab Project 1
- Advanced Parameter Handling
- Policy Diff and Administration
- Automatic Policy Building
- Web Application Vulnerability Scanner Integration
- Layered Policies
- Login Enforcement, Brute Force Mitigation, and Session Tracking
- Web Scraping Mitigation and Geolocation Enforcement
- Layer 7 DoS Mitigation and Advanced Bot Protection
- F5 Advanced WAF and iRules
- Using Content Profiles
- Review and Final Labs

Further Information

- Bitte beachten Sie, dass diese Kurse direkt beim Hersteller stattfinden und Arrow ECS Education nur als Vermittler auftritt.
- Die Verfügbarkeit von freien Plätzen können wir trotz Ihrer Online-Buchung/Bestellung leider nicht gewährleisten.
- Installation und Kursunterlagen sind Englisch.
- Dieser Kurs ist nicht rabatt- und prämienprogrammfähig!

Session Dates

Auf Anfrage. Bitte [kontaktieren Sie uns](#)

Zusätzliche Information

[Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.](#)