



Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com

Phone: +420 597 488 811



Configuring F5 Advanced WAF (previously licensed as ASM)

Kód:	DÉLKA:	CENA:
F5N_BIG-AWF-CFG	32 Hours (4 DENNÍ)	Kč bez DPH 68,000.00

Description

Kurz Configuring F5 Advanced Web Application Firewall poskytne účastníkům znalosti a praktické dovednosti k tomu, aby byli schopni nasadit, nastavit a provozovat F5 Advanced Web Application Firewall (včetně modulu ASM, který je součástí AWAf). Naučí účastníky zásady a principy jak chránit webové aplikace před útoky založenými na protokolu HTTP. Součástí školení s lektorem jsou rozsáhlé praktické laby a diskuse k tématům o detekci a zmírnění hrozeb na Layer7 jako je: Denial of Service, brute force, bots, code injection, and zero day exploits.

Cíle

- 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

Určeno pro

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.

Vstupní znalosti

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. WA

Program

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

Termíny školení

Datum	Místo konání	Časové pásmo	Jazyk	Typ	Garance termínu	CENA
08 Jun 2026	Virtual Classroom	CEDT	Čeština	Instructor Led Online		Kč bez DPH 68,000.00
19 Oct 2026	Virtual Classroom	CEDT	Čeština	Instructor Led Online		Kč bez DPH 68,000.00

Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)