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

Setting up F5 Advanced WAF v15.1

CODE:	LENGTH:	PRICE:
F5N_BIG-AWF-SU1	8 Hours (1 day)	€905.00

Description

Do you need to secure your applications quickly from today's threats such as those from automated agents, bots, and common vulnerabilities? Are you limited by time, resources, and knowledge of your web applications? Do you need protection against CVEs without thinking too deeply about them?
In this 1 day course, participants identify and mitigate common web application vulnerabilities on the client and application sides of the threat spectrum. Participants use F5 Advanced WAF to quickly configure advanced protection against common Layer 7 vulnerabilities (OWASP Top Ten) and bot defense.

Objectives

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 courseorF5 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 trainingGetting 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 encapsulationRouting and switchingEthernet and ARPTCP/IP conceptsIP addressing and subnetting
NAT and private IP addressingDefault gatewayNetwork firewallsLAN vs. WAN

Audience

This course is intended for users who wish to rapidly deploy a basic web application security policy with minimal configuration; deploy a DoS Protection Profile to detect server stress, and block bad actors.

Programme

Provision resources for F5 Advanced Web Application FirewallRapidly deploy a security policy using the Guided Configuration
Configure learn, alarm, and block settings to ensure valid users can access your applicationDefine attack signatures
Contrast positive and negative security policy implementationReview learning suggestions for policy tuning
Mitigate Credentials Stuffing attacksSecure a URL from client-side fraud using DataSafe encryption and obfuscation
Use the automated L7 Behavioral Denial of Service feature to detect and mitigate DoS attacks

Session Dates

On request. Please contact us

Additional Information

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