

# **Arrow ECS Finland Oy - Education Services**

# **TRAINING OFFERING**

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com Phone: 0870 251 1000



# Configuring F5 Advanced WAF (previously licensed as ASM) v17.1

CODE: LENGTH: PRICE:

F5N BIG-AWF-CFG 32 Hours (4 days) €3,595.00

# **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 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

-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

#### **Programme**

- •Resource provisioning for F5 Advanced Web Application Firewall
- •Traffic processing with BIG-IP Local Traffic Manager (LTM)
- •Web application concepts
- •Web application vulnerabilities
- Security policy deployment
- Security policy tuning
- Attack signatures
- Positive security building
- Securing cookies and other headers
- Reporting and logging
- ·Policy Diff, merging, and exporting
- Advanced parameter handling
- Using application templates
- •Using Automatic Policy Builder
- •Integrating with web vulnerability scanners
- Login enforcement
- •Brute force mitigation
- Session tracking
- •Web scraping detection and mitigation
- •Geolocation Enforcement and IP Address Exceptions
- •Using Parent and Child policies
- •Layer 7 DoS protection
- •F5 Advanced Web Application Firewall and iRules
- •Using Content Profiles for AJAX and JSON applications
- Advanced Bot Detection and Defense
- •Proactive Bot Defense

### **Session Dates**

Date	Location	Time Zone	Language	Туре	Guaranteed	PRICE
09 Mar 2026	Virtual Classroom (CET / UTC +1)		English	Instructor Led Online		€3,595.00
09 Mar 2026	Espoo Arrow Classroom (CET / UTC +1)		English	Classroom		€3,595.00
04 May 2026	Virtual Classroom (CET / UTC +1)		English	Instructor Led Online		€3,595.00
04 May 2026	Espoo Arrow Classroom (CET / UTC +1)		English	Classroom		€3,595.00

# **Additional Information**

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