



TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com

Phone: 0870 251 1000



Configuring F5 Advanced WAF (previously licensed as ASM) v16.1

| CODE: | LENGTH: | PRICE: |
|-----------------|-------------------|-----------|
| F5N_BIG-AWF-CFG | 32 Hours (4 days) | £3,545.00 |

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.

- Resource provisioning for F5 Advanced Web Application Firewall
- Traffic processing with BIG-IP Local Traffic Manager (LTM)
- Web application concepts
- Mitigating the OWASP Top 10 and other vulnerabilities
- Security policy deployment
- Security policy tuning
- Deploying Attack Signatures and Threat Campaigns
- Positive security building
- Securing cookies and other headers
- Reporting and logging
- Advanced parameter handling
- Using Automatic Policy Builder
- Integrating with web vulnerability scanners
- Login enforcement for flow control
- Brute force and credential stuffing mitigation
- Session tracking for client reconnaissance
- Using Parent and Child policies
- Layer 7 DoS protection
 - Transaction Per Second-based DoS protection
 - Layer 7 Behavioral DoS Protection
- Configuring Advanced Bot Defense
 - Web Scraping and other Microservice Protection
 - Working with Bot Signatures

Topics Covered • Using DataSafe to Secure the client side of the Document Object Model

Objectives

At the end of this course, the student will be able to:

- Describe the role of the BIG-IP system as a full proxy device in an application delivery network
- Provision the F5 Advanced Web Application Firewall
- 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
- Deploy Threat Campaigns to secure against CVE threats
- Contrast positive and negative security policy implementation and explain benefits of each
- Configure security processing at the parameter level of a 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 for flow control
- Mitigate credential stuffing
- Configure protection against brute force attacks
- Deploy Advanced Bot Defense against web scrapers, all known bots, and other automated agents
- Deploy DataSafe to secure client-side data

Audience

This course is intended for SecOps personnel responsible for the deployment, tuning, and day-to-day maintenance of F5 Adv. WAF. Participants will obtain a functional level of expertise with F5 Advanced WAF, including comprehensive security policy and profile configuration, client assessment, and appropriate mitigation types.

- Experience with LTM is not required.
- Prior WAF knowledge is not required.
- This course is on the list of approved study resources for the F5 ASM 303 certification exam.

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 LearnF5 (<https://www.f5.com/services/training>):

- ? 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

- ? Introducing the BIG-IP System
- ? Initially Setting Up the BIG-IP System
- ? Archiving the BIG-IP System Configuration

Chapter 1: Setting Up the BIG-IP System ? Leveraging F5 Support Resources and Tools Chapter 2: Traffic Processing with BIG-IP

? Identifying BIG-IP Traffic Processing Objects

? Understanding Profiles

? Overview of Local Traffic Policies

? Visualizing the HTTP Request Flow

Chapter 3: Web Application Concepts

| | |
|---------------------------------------------------------------|-------------------------------------------------------------------|
| ? Overview of Web Application Request Processing | |
| ? Web Application Firewall: Layer 7 Protection | |
| ? 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 | Chapter 4: Web Application Vulnerabilities |
| ? A Taxonomy of Attacks: The Threat Landscape | |
| ? Common Exploits Against Web Applications | Chapter 5: Security Policy Deployment |
| ? Defining Learning | |
| ? Comparing Positive and Negative Security Models | |
| ? The Deployment Workflow | |
| ? Policy Templates: Protection Starting Point | |
| ? Deployment Workflow: Using Advanced Settings | |
| ? Defining Logging Profiles | |
| ? Security Checks Offered by Rapid Deployment | |
| ? Defining Data Guard | Chapter 6: Policy Tuning and Violations |
| ? Post-Deployment Traffic Processing | |
| ? How Violations are Categorized | |
| ? Violation Rating: A Threat Scale | |
| ? Defining Staging and Enforcement | |
| ? Defining Enforcement Mode | |
| ? Defining the Enforcement Readiness Period | |
| ? Defining the Learn, Alarm and Block Settings | |
| ? Defining Learning Suggestions | |
| ? Interpreting the Enforcement Readiness Summary | |
| ? Configuring the Blocking Response Page | Chapter 7: Attack Signatures and Threat Campaigns |
| ? Defining Attack Signatures | |
| ? Creating User-Defined Attack Signatures | |
| ? Defining Simple and Advanced Edit Modes | |
| ? Defining Attack Signature Sets | |
| ? Understanding Attack Signatures and Staging | |
| ? Updating Attack Signatures | |
| ? Defining Threat Campaigns | Chapter 8: 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 | |
| ? Defining the Learning Score | |
| ? Defining Trusted and Untrusted IP Addresses | |
| ? How to Learn: Compact | Chapter 9: Securing Cookies and Other Headers |
| ? The Purpose of F5 Advanced WAF Cookies | |
| ? Defining Allowed and Enforced Cookies | |
| ? Securing HTTP headers | Chapter 10: Visual Reporting and Logging |
| ? Viewing Application Security Summary Data | |
| ? Building Application Security Reports Using Filters | |
| ? Viewing F5 Advanced WAF Resource Consumption | |
| ? Ensuring PCI Compliance: PCI-DSS 3.0 | |
| ? Using the OWASP Compliance Dashboard | |
| ? Analyzing Requests using the Attack Expert System | |
| ? Local Logging Facilities and Destinations | |
| ? Viewing Logs in the Configuration Utility | |
| ? Defining the Logging Profile | |
| ? Configuring Response Logging | Chapter 11: Lab Project 1 Chapter 12: Advanced Parameter Handling |

- ? Understanding the Need for Parameter Protections
- ? Understanding Where Parameters Appear
- ? Understanding Parameter Types and Definitions
- ? Understanding Parameter Levels
- ? Understanding Parameter Properties
- ? Understanding Static Content Value Parameters
- ? Understanding User Input Parameters
- ? Defining Dynamic Parameters
- ? Defining Dynamic Parameter Extraction Properties
- ? Defining Positional Parameters
- ? Understanding Sensitive Parameters Chapter 13: Automatic Policy Building
- ? Overview of Automatic Policy Building
- ? Identifying Templates Which Automate Learning
- ? Defining Policy Loosening
- ? Defining Policy Tightening
- ? Defining Learning Speed: Traffic Sampling
- ? Defining Track Site Changes Chapter 14: Web Application Vulnerability Scanner Integration
- ? Integrating Scanner Output ? Defining a Parent and Child Policies
- ? Importing and Resolving Vulnerabilities Chapter 15: Deploying Layered Policies ? Layered Policy Deployment Use Cases
 - ? Defining Login Pages for Flow Control
 - ? Defining Brute Force Attacks
- Chapter 16: Login Enforcement and Brute Force Mitigation ? Defining Credential Stuffing
 - ? Defining Session Tracking
- Chapter 17: Reconnaissance with Session Tracking ? Configuring Actions Upon Violation Detection
 - ? Defining Denial of Service Attacks
 - ? Defining the DoS Protection Profile
 - ? Overview of TPS-based DoS Protection
 - ? Configuring Stress-based Mitigation
 - ? Defining Behavioral DoS Mitigation
- Chapter 18: Layer 7 DoS Mitigation ? Mitigate Attacks Starting with the TLS Handshake Chapter 19: Advanced Bot Defense
 - ? Classifying Clients with the Bot Defense Profile
 - ? Defining Bot Signatures
 - ? Defining F5 Fingerprinting
 - ? Defining Browser Verification
 - ? Defining Device ID
 - ? Defining Bot Defense Profile Templates
 - ? Defining Microservices protection
 - ? Mitigating Web Scraping Chapter 20: Form Encryption using DataSafe
 - ? What Elements of Application Delivery Are Targeted?
 - ? Exploiting the Document Object Model
 - ? Protecting Applications Using DataSafe
 - ? Configuring a DataSafe Profile Chapter 21: Review and Final Labs
 - ? Final Lab Project (Option 1) – Production Scenario
 - ? Final Lab Project (Option 2) – Managing Traffic with Layer 7 Local Traffic Policies

Follow on courses

- F5N_BIG-OP-ADMIN, Administering BIG-IP v.15.1
- F5N_BIG-LTM-CFG-3, Configuring BIG-IP LTM: Local Traffic Manager v.15.1
- F5N_BIG-DNS-I, Configuring BIG-IP DNS (formerly GTM) v.15.1
- F5N_BIG-EGW-APM, Configuring BIG-IP APM: Access Policy Manager v.15.1
- F5N_BIG-IRULE-CFG, Developing iRules for BIG-IP v.15.1

Other courses available: F5N_BIG-TRBL-INT2, Troubleshooting BIG-IP v.15.1

Test and Certification

Exam 303 – BIG-IP ASM Specialist

Prerequisites: Valid F5-CA, BIG-IP Certification

Upon passing Exam 303, candidates receive their F5 Certified Technology Specialist, BIG-IP ASM certification. This certification verifies that a candidate is fully qualified to design, implement, and maintain BIG-IP ASM, integrating BIG-IP ASM with other platforms and products in a manner that is application-specific and appropriate to organizational policies, needs, and requirements. Receiving the F5-CTS, BIG-IP ASM certification is a prerequisite for the Security Solutions Expert certification track.

[View Exam 303 study materials on AskF5](#)

Exam vouchers can be purchased from Arrow ECS at an additional charge. Vouchers can be used at www.vue.com/f5 to schedule exams at a time and location convenient to the attendee.

Session Dates

| Date | Location | Time Zone | Language | Type | Guaranteed | PRICE |
|-------------|-----------------------------|-----------|----------|-----------|------------|-----------|
| 18 Dec 2023 | Virtual Training Class - TP | GMT | English | Classroom | | £3,545.00 |

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)