Enterprise Computing Solutions - Education Services

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

Setting up F5 Advanced WAF v14.1

CODE:	LENGTH:	PRICE:
F5N_BIG-AWF-SU1	1 day	£830.00

Description

F5 Advanced Web Application Firewall (Advanced WAF) is a new offering including BIG-IP Application Security Manager (ASM) and additional anti-fraud features which can secure the entire Layer 7 threat spectrum, with client-side protection on one end and application-side protection on the opposite end.
Due to the complexity of traditional ASM implementations, F5 devised Advanced WAF as a solution for customers who want quick configuration for advanced protection against common layer 7 application vulnerabilities, layer 7 denial of service attacks, and client-side fraud defense.
Advanced WAF is not a different product from ASM. It is a new licensing model of existing ASM features, additional defense capabilities, paid add-on features, and paid subscription features.

Objectives

• Differentiating between client-side and application-side web vulnerabilities
• Categorizing Attack Techniques
• Use the Guided Configuration to deploy a Web Application Security Policy
• Defining the key parts of a Web Application Security Policy
• Understanding request logging options
• Identifying HTTP headers and methods
• Defining attack signatures, attack signature staging, and violations
• Overview of the OWASP Top Ten
• Review learning suggestions and basic policy tuning
• Deploy Threat Campaign
• Mitigate Credentials Stuffing
• Secure 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

Audience

This course is intended for security and network administrators who will be responsible for the deployment of F5 Advanced Web Application Firewall to secure web applications from common vulnerabilities and denial of service.

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 (https://university.f5.com):

? Getting Started with BIG-IP web-based training
? Getting Started with BIG-IP Application Security Manager (ASM)

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

Chapter 1: Setting Up the BIG-IP System

? Introducing the BIG-IP System
? Initially Setting Up the BIG-IP System
? Archiving the BIG-IP System Configuration
? Leveraging F5 Support Resources and Tools

Chapter 2: Threat Overview and Guided Configuration

? Classifying Attack Types
? Differentiating Benign and Malicious Clients
? Categorizing Attack Techniques
? Defining the Layer 7 Web Application Firewall
? Defining Traffic Processing Objects
? Introducing F5 Advanced WAF
? Using Guided Configuration for Web Application Security

Chapter 3: Exploring HTTP Traffic

? Exploring Web Application HTTP Request Processing
? Overview of Application-Side Vulnerabilities
? Defining Attack Signatures
? Defining Violations

Chapter 4: Securing HTTP Traffic

? Defining Learning
? Defining Attack Signature Staging
? Defining Attack Signature Enforcement

Chapter 5: Mitigating Credential Stuffing

? Defining Credential Stuffing Attacks
? The Credential Stuffing Mitigation Workflow

Chapter 6: Using BIG-IP DataSafe

? What Elements of Application Delivery are Targeted?
? Exploiting the Document Object Model
? Protecting Applications Using DataSafe
? Configuring a DataSafe Profile

Chapter 7: Deploying Threat Campaigns

? Defining Threat Campaigns
? Differentiate from Attack Signatures
? Staging and Threat Campaigns
? Live Update for Threat Campaigns

Chapter 8: Using Layer 7 Behavioral Analysis to Mitigate DoS

? Defining Behavioral Analysis
? Defining the DoS

Session Dates

On request. Please contact us

Additional Information

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