Configuring F5 Advanced WAF (previously licensed as ASM) v14.1

Category: Networking & Security | **Vendor:** F5

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

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.

About This Course

- 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
- Using DataSafe to Secure the client side of the Document Object Model
- Certification
- 303 ASM Specialist

Prerequisites & Entry Requirements

General Prerequisites:

Prerequisite – Students must complete ONE of these:

- Attend an Administering BIG-IP (TRG-BIG-OP-ADMIN) class
- Achieve F5 Certified BIG-IP Administrator certification
- Pass the free Administering BIG-IP Course Equivalency Assessment with a score of 70% or higher

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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Students should 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

Detailed Course Outline

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: 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

- Assigning Policy to Virtual Server

- Deployment Workflow: Using Advanced Settings
- Configure Server Technologies
- Defining Attack Signatures
- Viewing Requests
- Security Checks Offered by Rapid Deployment
- Defining Attack Signatures
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
- Reviewing the Definition of Learning
- Defining Learning Suggestions
- Choosing Automatic or Manual Learning
- Defining the Learn, Alarm and Block Settings
- Interpreting the Enforcement Readiness Summary
- Configuring the Blocking Response Page
Chapter 7: Attack Signatures and Threat Campaigns

- Defining Attack Signatures
- Attack Signature Basics
- Creating User-Defined Attack Signatures
- Defining Simple and Advanced Edit Modes
- Defining Attack Signature Sets
- Defining Attack Signature Pools
- Understanding Attack Signatures and Staging
- Updating Attack Signatures

- Defining Threat Campaigns

- Deploying 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

- Reporting: Build Your Own View

- Reporting: Chart based on filters

- Brute Force and Web Scraping Statistics

- Viewing Resource Reports

- PCI Compliance: PCI-DSS 3.0

- Analyzing Requests

- 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

- Defining Parameter Types

- Defining Static Parameters

- Defining Dynamic Parameters

- Defining Parameter Levels

- Other Parameter Considerations

Chapter 13: Automatic Policy Building

- Overview of Automatic Policy Building

- Defining 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

- Importing Vulnerabilities

- Resolving Vulnerabilities

- Using the Generic XML Scanner XSD file

Chapter 15: Deploying Layered Policies

- Defining a Parent Policy

- Defining Inheritance

- Parent Policy Deployment Use Cases

Chapter 16: Login Enforcement and Brute Force Mitigation

- Defining Login Pages for Flow Control

- Configuring Automatic Detection of Login Pages

- Defining Brute Force Attacks

- Brute Force Protection Configuration

- Source-Based Brute Force Mitigations

- Defining Credential Stuffing

- Mitigating Credential Stuffing

Chapter 17: Reconnaissance with Session Tracking

- Defining Session Tracking

- Configuring Actions Upon Violation Detection

Chapter 18: Layer 7 DoS Mitigation

- Defining Denial of Service Attacks

- Defining the DoS Protection Profile

- Overview of TPS-based DoS Protection

- Creating a DoS Logging Profile

- Applying TPS Mitigations

- Defining Behavioral and Stress-Based Detection

Chapter 19: Advanced Bot Defense

- Classifying Clients with the Bot Defense Profile

- Defining Bot Signatures

- Defining F5 Fingerprinting

- Defining Bot Defense Profile Templates

- Defining Microservices protection

Chapter 20: Form Encryption using DataSafe

- Targeting Elements of Application Delivery

- Exploiting the Document Object Model

- Protecting Applications Using DataSafe

- The Order of Operations for URL Classification

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

Skills You Will Learn:

- Students should 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

Frequently Asked Questions

Q: What delivery options are available for Configuring F5 Advanced WAF (previously licensed as ASM) v14.1?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 4-day Configuring F5 Advanced WAF (previously licensed as ASM) v14.1 course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Configuring F5 Advanced WAF (previously licensed as ASM) v14.1 training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Configuring F5 Advanced WAF (previously licensed as ASM) v14.1?

Yes, we provide corporate training, dedicated training, and closed classes for Configuring F5 Advanced WAF (previously licensed as ASM) v14.1. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Configuring F5 Advanced WAF (previously licensed as ASM) v14.1, F5 Networks, TRG-BIG-AWF-CFG

Q: Why choose Nexus Human for Configuring F5 Advanced WAF (previously licensed as ASM) v14.1?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Configuring F5 Advanced WAF (previously licensed as ASM) v14.1 training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 19/10/2026.