

# F5 AWAf Modern Application (formerly Configuring F5 Advanced WAF)

Learn to deploy and operate F5 Advanced WAF to protect web applications from the most critical security risks as described in the OWASP Top 10 list, from bots and other automated agents, and from Denial of Service (DoS) attacks operating at the HTTP layer of the web application delivery ecosystem. Through a combination of lecture, hands-on labs, and discussion, secure applications from the majority of common attacks by the end of the first day. Take technical deep dives into mitigating web scraping, account aggregation, account creation, ad fraud, CAPTCHA defeat, card cracking, carding, cashing out, credential stuffing, and other unwanted automated application abuse as described in the OWASP automated threats list.

Observe various vulnerability mitigations in real time by playing the role of an attacker in lab exercises. Gain context for securing applications, including analysis of HTTP and the elements of both modern and traditional web applications such as file types, parameters, URLs, and login pages. Learn to recognize client and server-side technologies such as JSON and AJAX, and learn to address vulnerabilities that might be present in common application development tools such as PHP, AngularJS, and others.

Review recommended practices for reporting, security event logging, and integration with third-party web application vulnerability scanners in detail. Follow prescribed step-by-step directions for activities initially, and gradually gain proficiency so that, by the end of class, little or no instruction is needed to complete simple to more complex configurations.

## Course Contents

- Introducing the BIG-IP System
- Traffic Processing with BIG-IP
- Overview of Web Application Processing
- Overview of Web Application Vulnerabilities
- Security Policy Deployments: Concepts and Terminology
- Policy Tuning and Violations
- Using Attack Signatures and Threat Campaigns
- Positive Security Policy Building
- Securing Cookies and other Header Topics
- Visual Reporting and Logging
- Lab Project 1
- Advanced Parameter Handling
- Automatic Policy Building
- Integrating with Web Application Vulnerability Scanners
- Deploying Layered Policies
- Login Enforcement and Brute Force Mitigation
- Reconnaissance with Session Tracking
- Layer 7 Denial of Service Mitigation
- Advanced Bot Defense
- Final Projects

## Target Group

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 and prior WAF knowledge are not required.

## Prerequisites

The following free Self-Directed Training (SDT) courses, although optional, are helpful for any student with limited BIG-IP administration and configuration experience:

- Getting Started with BIG-IP
- Getting Started with Local Traffic Manager (LTM)
- Getting Started with F5 Advanced WAF

These courses are available at F5 University

General network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course, including OSI model encapsulation, routing and switching, Ethernet and ARP, TCP/IP concepts, IP addressing and subnetting, NAT and private IP addressing, NAT and private IP addressing, default gateway, network firewalls, and LAN vs. WAN.

## Course Target

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.

## This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

[www.experteach-training.com/go/FWAF](http://www.experteach-training.com/go/FWAF)

## Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

## Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

## Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
<b>Classes in Germany</b>	<b>4 Days</b>	<b>€ 4,400</b>
<b>Online Training</b>	<b>4 Days</b>	<b>€ 4,400</b>
<b>Date/course venue</b>	Course language English 	
15/09-18/09/25 	17/11-20/11/25	

Status 05/25/2025

# Table of Contents

## F5 AWAF Modern Application (formerly Configuring F5 Advanced WAF)

### 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
- Overview of Network Packet Flow
- 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
- F5 Advanced WAF 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: Common Web Application Vulnerabilities

- A Taxonomy of Attacks: The Threat Landscape
- What Elements of Application Delivery are Targeted?
- Common Exploits Against Web Applications

### Chapter 5: Security Policy Deployment

- Defining Learning
- Comparing Positive and Negative Security Models
- The Deployment Workflow
- Policy Type: How Will the Policy Be Applied
- Policy Template: Determines the Level of Protection
- Policy Templates: Automatic or Manual Policy Building
- Assigning Policy to Virtual Server
- Deployment Workflow: Using Advanced Settings
- Selecting the Enforcement Mode
- The Importance of Application Language
- Configure Server Technologies
- Verify Attack Signature Staging
- Viewing Requests
- Security Checks Offered by Rapid Deployment
- Defining Attack Signatures
- Using Data Guard to Check Responses

### Chapter 6: Policy Tuning and Violations

- Post-Deployment Traffic Processing
- Defining Violations
- Defining False Positives
- 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

- 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

### 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
- Violations Without Learning Suggestions
- Defining the Learning Score
- Defining Trusted and Untrusted IP Addresses
- How to Learn: Compact

### Chapter 9: Cookies and Other Headers

- F5 Advanced WAF Cookies: What to Enforce
- Defining Allowed and Enforced Cookies
- Configuring Security Processing on HTTP headers

### Chapter 10: Reporting and Logging

- Overview: Big Picture Data
- Reporting: Build Your Own View
- Reporting: Chart based on filters
- Brute Force and Web Scraping Statistics
- Viewing F5 Advanced WAF Resource Reports
- PCI Compliance: PCI-DSS 3.0
- The Attack Expert System
- Viewing Traffic Learning Graphs
- Local Logging Facilities and Destinations
- How to Enable Local Logging of Security Events
- Viewing Logs in the Configuration Utility
- Exporting Requests
- Logging Profiles: Build What You Need
- Configuring Response Logging

### Chapter 11: Lab Project 1

### Chapter 12: Advanced Parameter Handling

- Defining Parameter Types
- Defining Static Parameters
- Defining Dynamic Parameters
- Defining Dynamic Parameter Extraction Properties
- Defining Parameter Levels
- Other Parameter Considerations

### Chapter 13: Policy Diff and Administration

- Comparing Security Policies with Policy Diff
- Merging Security Policies
- Restoring with Policy History
- Examples of F5 Advanced WAF Deployment Types
- ConfigSync and F5 Advanced WAF Security Data
- ASMQKVIEW: Provide to F5 Support for Troubleshooting

### Chapter 14: 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 15: Web Application Vulnerability Scanner Integration

- Integrating Scanner Output into F5 Advanced WAF
- Will Scan be Used for a New or Existing Policy?
- Importing Vulnerabilities
- Resolving Vulnerabilities
- Using the Generic XML Scanner XSD file

### Chapter 16: Layered Policies

- Defining a Parent Policy
- Defining Inheritance
- Parent Policy Deployment Use Cases

### Chapter 17: Login Enforcement, Brute Force Mitigation, and Session Tracking

- Defining Login Pages
- Configuring Automatic Detection of Login Pages
- Defining Session Tracking
- What Are Brute Force Attacks?
- Brute Force Protection Configuration
- Defining Source-Based Protection
- Source-Based Brute Force Mitigations
- Defining Session Tracking
- Configuring Actions Upon Violation Detection
- Session Hijacking Mitigation Using Device ID

### Chapter 18: Web Scraping Mitigation and Geolocation Enforcement

- Defining Web Scraping
- Mitigating Web Scraping
- Defining Geolocation Enforcement
- Configuring IP Address Exceptions

### Chapter 19: Layer 7 DoS Mitigation and Advanced Bot Protection

- Defining Denial of Service Attacks
- The General Flow of DoS Protection
- Defining the DoS Profile
- Overview of TPS-based DoS Protection
- Applying TPS mitigations
- Create a DoS Logging Profile
- Defining DoS Profile General Settings
- Defining Bot Signatures
- Defining Proactive Bot Defense
- Defining Behavioral and Stress-Based Detection
- Defining Behavioral DoS Mitigation

### Chapter 20: F5 Advanced WAF and iRules

- Common Uses for iRules
- Identifying iRule Components
- Triggering iRules with Events
- Defining F5 Advanced WAF iRule Events
- Defining F5 Advanced WAF iRule Commands
- Using F5 Advanced WAF iRule Event Modes

### Chapter 21: Using Content Profiles

- Defining Asynchronous JavaScript and XML
- Defining JavaScript Object Notation (JSON)
- Defining Content Profiles
- The Order of Operations for URL Classification

### Chapter 22: Review and Final Labs

- Final Lab Project (Option 1) – Production Scenario
- Final Lab Project (Option 2) – JSON Parsing with the Default JSON Profile
- Final Lab Project (Option 3) – Managing Traffic with L7 Local Traffic Policies

