# F5 Networks Configuring BIG-IP Advanced WAF: Web Application Firewall Training

BILGINC
IT Academy
info@bilginc.com
bilginc.com

Duration: **4 Day**

**New - Explore functional understanding of how to deploy, tune, and operate F5 Advanced Web Application Firewall to protect their web applications from HTTP-based attacks.**

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.

**Who Should Attend?**

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

Administering BIG-IP; basic familiarity with HTTP, HTML and XML; basic web application and security concepts.

## What You Will Learn

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.

## Training Outline

**Module 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

**Module 2: Traffic Processing with BIG-IP**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Identifying BIG-IP Traffic Processing Objects
- Overview of Network Packet Flow
- Understanding Profiles
- Overview of Local Traffic Policies
- Visualizing the HTTP Request Flow

**Module 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

**Module 4: Common Web Application Vulnerabilities**

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

**Module 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

**Module 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

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- 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

**Module 7: Attack Signatures & 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

**Module 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

**Module 9: Cookies and Other Headers**

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

**Module 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

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Viewing Logs in the Configuration Utility
- Exporting Requests
- Logging Profiles: Build What You Need
- Configuring Response Logging

**Module 12: Advanced Parameter Handling**

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

**Module 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

**Lesson 14: Web Application Vulnerability Scanner Integration**

- Integrating Scanner Output
- Importing Vulnerabilities
- Resolving Vulnerabilities
- Using the Generic XML Scanner XSD file

**Lesson 15: Deploying Layered Policies**

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

**Lesson 16: Login Enforcement and Brute Force Mitigation**

- Defining Login Pages for Flow Control
- Configuring Automatic Detection of Login Pages
- Defining Session Tracking
- Brute Force Protection Configuration
- Source-Based Brute Force Mitigations
- Defining Credentials Stuffing
- Mitigating Credentials Stuffing

**Lesson 17: Reconnaissance with Session Tracking**

- Defining Session Tracking
- Configuring Actions Upon Violation Detection

**Lesson 18: Layer 7 DoS Mitigation**

- Defining Denial of Service Attacks

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- 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

**Lesson 19: Advanced Bot Protection**

- Classifying Clients with the Bot Defense Profile
- Defining Bot Signatures
- Defining Proactive Bot Defense
- Defining Behavioral and Stress-Based Detection
- Defining Behavioral DoS Mitigation

**Lesson 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