

F5 Networks Configuring BIG-IP Advanced WAF: Web Application Firewall (BIG-IP WAF v14)

Course Summary

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 web scraping, Layer 7 Denial of Service, brute force, bots, code injection, and zero day exploits.

Objectives

After taking this course, students will be able to:

- Describe the role of the BIG-IP system as a full proxy device in an application delivery network
- Provision the Application Security Manager
- Define a web application firewall
- Describe how ASM protects a web application by securing file types, URLs, and parameters
- Deploy ASM 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 ASM
- Define attack signatures and explain why attack signature staging is important
- Contrast positive and negative security policy implementation and explain benefits of each
- Configure security processing at the parameter level of a web application
- Use an application template to protect a commercial web application
- Deploy ASM 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 and session tracking
- Configure protection against brute force, web scraping, and Layer 7 denial of service attacks
- Implement iRules using specific ASM events and commands
- Use Content Profiles to protect JSON and AJAX-based applications
- Implement Bot Signatures
- Implement Proactive Bot Defense

Topics

- Setting Up the BIG-IP System
- Traffic Processing with BIG-IP
- Web Application Concepts
- Common Web Application Vulnerabilities
- Security Policy Deployment
- Policy Tuning and Violations
- Attack Signatures
- Positive Security Policy Building
- Cookies and Other Headers
- Reporting and Logging
- Lab Project 1
- Advanced Parameter Handling
- Policy Diff and Administration
- Automatic Policy Building
- Web Application Vulnerability Scanner Integration
- Layered Policies

F5 Networks Configuring BIG-IP Advanced WAF: Web Application Firewall (BIG-IP WAF v14)

Course Summary (cont.)

- Login Enforcement, Brute Force Mitigation, and Session Tracking
- Web Scraping Mitigation and Geolocation Enforcement
- Layer 7 DoS Mitigation and Advanced Bot Protection
- F5 Advanced WAF and iRules
- Using Content Profiles
- Review and Final Labs

Audience

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.

Prerequisite

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

Duration

Four Days

F5 Networks Configuring BIG-IP Advanced WAF: Web Application Firewall (BIG-IP WAF v14)

Course Outline

- I. **Setting Up the BIG-IP System**
 - A. Introducing the BIG-IP System
 - B. Initially Setting Up the BIG-IP System
 - C. Archiving the BIG-IP System Configuration
 - D. Leveraging F5 Support Resources and Tools
- II. **Traffic Processing with BIG-IP**
 - A. Identifying BIG-IP Traffic Processing Objects
 - B. Overview of Network Packet Flow
 - C. Understanding Profiles
 - D. Overview of Local Traffic Policies
 - E. Visualizing the HTTP Request Flow
- III. **Web Application Concepts**
 - A. Overview of Web Application Request Processing
 - B. Web Application Firewall: Layer 7 Protection
 - C. F5 Advanced WAF Layer 7 Security Checks
 - D. Overview of Web Communication Elements
 - E. Overview of the HTTP Request Structure
 - F. Examining HTTP Responses
 - G. How F5 Advanced WAF Parses File Types, URLs, and Parameters
 - H. Using the Fiddler HTTP Proxy
- IV. **Common Web Application Vulnerabilities**
 - A. A Taxonomy of Attacks: The Threat Landscape
 - B. What Elements of Application Delivery are Targeted?
 - C. Common Exploits Against Web Applications
- V. **Security Policy Deployment**
 - A. Defining Learning
 - B. Comparing Positive and Negative Security Models
 - C. The Deployment Workflow
 - D. Policy Type: How Will the Policy Be Applied
 - E. Policy Template: Determines the Level of Protection
 - F. Policy Templates: Automatic or Manual Policy Building
 - G. Assigning Policy to Virtual Server
 - H. Deployment Workflow: Using Advanced Settings
 - I. Selecting the Enforcement Mode
 - J. The Importance of Application Language
 - K. Configure Server Technologies
 - L. Verify Attack Signature Staging
 - M. Viewing Requests
 - N. Security Checks Offered by Rapid Deployment
 - O. Defining Attack Signatures
 - P. Using Data Guard to Check Responses
- VI. **Policy Tuning and Violations**
 - A. Post-Deployment Traffic Processing
 - B. Defining Violations
 - C. Defining False Positives
 - D. How Violations are Categorized
 - E. Violation Rating: A Threat Scale
 - F. Defining Staging and Enforcement
 - G. Defining Enforcement Mode
 - H. Defining the Enforcement Readiness Period
 - I. Reviewing the Definition of Learning
 - J. Defining Learning Suggestions
 - K. Choosing Automatic or Manual Learning
 - L. Defining the Learn, Alarm and Block Settings
 - M. Interpreting the Enforcement Readiness Summary
 - N. Configuring the Blocking Response Page

F5 Networks Configuring BIG-IP Advanced WAF: Web Application Firewall (BIG-IP WAF v14)

Course Outline (cont.)

VII. *Attack Signatures*

- A. Defining Attack Signatures
- B. Attack Signature Basics
- C. Creating User-Defined Attack Signatures
- D. Defining Simple and Advanced Edit Modes
- E. Defining Attack Signature Sets
- F. Defining Attack Signature Pools
- G. Understanding Attack Signatures and Staging
- H. Updating Attack Signatures

VIII. *Positive Security Policy Building*

- A. Defining and Learning Security Policy Components
- B. Defining the Wildcard
- C. Defining the Entity Lifecycle
- D. Choosing the Learning Scheme
- E. How to Learn: Never (Wildcard Only)
- F. How to Learn: Always
- G. How to Learn: Selective
- H. Reviewing the Enforcement Readiness Period: Entities
- I. Viewing Learning Suggestions and Staging Status
- J. Violations Without Learning Suggestions
- K. Defining the Learning Score
- L. Defining Trusted and Untrusted IP Addresses
- M. How to Learn: Compact

IX. *Cookies and Other Headers*

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

X. *Reporting and Logging*

- A. Overview: Big Picture Data
- B. Reporting: Build Your Own View
- C. Reporting: Chart based on filters

- D. Brute Force and Web Scraping Statistics
- E. Viewing F5 Advanced WAF Resource Reports
- F. PCI Compliance: PCI-DSS 3.0
- G. The Attack Expert System
- H. Viewing Traffic Learning Graphs
- I. Local Logging Facilities and Destinations
- J. How to Enable Local Logging of Security Events
- K. Viewing Logs in the Configuration Utility
- L. Exporting Requests
- M. Logging Profiles: Build What You Need
- N. Configuring Response Logging

XI. *Lab Project 1*

XII. *Advanced Parameter Handling*

- A. Defining Parameter Types
- B. Defining Static Parameters
- C. Defining Dynamic Parameters
- D. Defining Dynamic Parameter Extraction Properties
- E. Defining Parameter Levels
- F. Other Parameter Considerations

XIII. *Policy Diff and Administration*

- A. Comparing Security Policies with Policy Diff
- B. Merging Security Policies
- C. Restoring with Policy History
- D. Examples of F5 Advanced WAF Deployment Types
- E. ConfigSync and F5 Advanced WAF Security Data
- F. ASMQVIEW: Provide to F5 Support for Troubleshooting

F5 Networks Configuring BIG-IP Advanced WAF: Web Application Firewall (BIG-IP WAF v14)

Course Outline (cont.)

XIV. *Automatic Policy Building*

- A. Overview of Automatic Policy Building
- B. Defining Templates Which Automate Learning
- C. Defining Policy Loosening
- D. Defining Policy Tightening
- E. Defining Learning Speed: Traffic Sampling
- F. Defining Track Site Changes

XV. *Web Application Vulnerability Scanner Integration*

- A. Integrating Scanner Output into F5 Advanced WAF
- B. Will Scan be used for a New or Existing Policy?
- C. Importing Vulnerabilities
- D. Resolving Vulnerabilities
- E. Using the Generic XML Scanner XSD file

XVI. *Layered Policies*

- A. Defining a Parent Policy
- B. Defining Inheritance
- C. Parent Policy Deployment Use Cases

XVII. *Login Enforcement, Brute Force Mitigation, and Session Tracking*

- A. Defining Login Pages
- B. Configuring Automatic Detection of Login Pages
- C. Defining Session Tracking
- D. What Are Brute Force Attacks?
- E. Brute Force Protection Configuration
- F. Defining Source-Based Protection
- G. Source-Based Brute Force Mitigations
- H. Defining Session Tracking
- I. Configuring Actions Upon Violation Detection
- J. Session Hijacking Mitigation Using Device ID

XVIII. *Web Scraping Mitigation and Geolocation Enforcement*

- A. Defining Web Scraping
- B. Mitigating Web Scraping
- C. Defining Geolocation Enforcement
- D. Configuring IP Address Exceptions

XIX. *Layer 7 DoS Mitigation and Advanced Bot Protection*

- A. Defining Denial of Service Attacks
- B. The General Flow of DoS Protection
- C. Defining the DoS Profile
- D. Overview of TPS-based DoS Protection
- E. Applying TPS mitigations
- F. Create a DoS Logging Profile
- G. Defining DoS Profile General Settings
- H. Defining Bot Signatures
- I. Defining Proactive Bot Defense
- J. Defining Behavioral and Stress-Based Detection
- K. Defining Behavioral DoS Mitigation

XX. *F5 Advanced WAF and iRules*

- A. Common Uses for iRules
- B. Identifying iRule Components
- C. Triggering iRules with Events
- D. Defining F5 Advanced WAF iRule Events
- E. Defining F5 Advanced WAF iRule Commands
- F. Using F5 Advanced WAF iRule Event Modes

XXI. *Using Content Profiles*

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

XXII. *Review and Final Labs*