Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Configuring BIG-IP ASM: Application Security Manager (replaced with F5N_BIG-AWF-CFG, Configuring F5 Advanced WAF (previously licensed as ASM) v14.1.)

CODE:	LENGTH:	PRICE:
F5N_BIG-ASM-ESS	32 Hours (4 days)	€3,635.00

Description

This course gives participants a functional understanding of how to deploy, tune, and operate BIG-IP Application Security Manager (ASM) to protect their web applications from HTTP-based attacks.
The course includes lecture, hands-on labs, and discussion about different ASM components 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

• Provisioning ASM
• Traffic processing with BIG-IP Local Traffic Manager (LTM)
• Web application concepts
• Web application vulnerabilities
• Security policy deployment
• Security policy tuning
• Attack signatures
• Positive security building
• Securing cookies and other headers
• Reporting and logging
• Policy Diff, merging, and exporting
• Advanced parameter handling
• Using application templates
• Using Automatic Policy Builder
• Integrating with web vulnerability scanners
• Login enforcement
• Brute force mitigation
• Session tracking
• Web scraping detection and mitigation
• Geolocation Enforcement and IP Address Exceptions
• Using Parent and Child policies
• Layer 7 DoS protection
• ASM and iRules
• Using Content Profiles for AJAX and JSON applications
• NEW — Advanced Bot Detection and Defense
• NEW — Proactive Bot Defense
• NEW — Simple Edit Mode for Attack Signatures

Audience

This course is intended for system and network administrators responsible for the installation, deployment, tuning, and day-to-day maintenance of the Application Security Manager.

Prerequisites

Students must complete one of the following F5 prerequisites before attending this course:

• 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 (http://university.f5.com):
• Getting Started with BIG-IP
• 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

• Introducing the BIG-IP System
• Initially Setting Up the BIG-IP System
• Archiving the BIG-IP System Configuration
Chapter 1: Setting Up the BIG-IP System• Leveraging F5 Support Resources and ToolsChapter 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
• ASM Layer 7 Security Checks
• Overview of Web Communication Elements
• Overview of the HTTP Request Structure
• Examining HTTP Responses
• How ASM 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
• 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

Chapter 8: Positive Security Policy Building
• How to Learn: Compact

Chapter 9: Cookies and Other Headers

• ASM 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 ASM 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
• Editing and Exporting Security Policies
• Restoring with Policy History
• Examples of ASM Deployment Types
• ConfigSync and ASM Security Data
• ASMQKVIEW: Provide to F5 Support for Troubleshooting

Chapter 14: Using Application-Ready Templates

• Application Templates: Pre-Configured Baseline Security

Chapter 15: 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 16: Web Application Vulnerability Scanner Integration

• Integrating Scanner Output Into ASM
• Will Scan be Used for a New or Existing Policy?
• Importing Vulnerabilities
• Resolving Vulnerabilities
• Using the Generic XML Scanner XSD file

Chapter 17: Layered Policies
• Defining a Parent Policy
• Defining Inheritance
• Parent Policy Deployment Use Cases
• 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

Chapter 18: Login Enforcement, Brute Force Mitigation, and Session Tracking
• Session Hijacking Mitigation Using Device ID
• Defining Web Scraping
• Mitigating Web Scraping
• Defining Geolocation Enforcement

Chapter 19: Web Scraping Mitigation and Geolocation Enforcement
• Configuring IP Address Exceptions
• 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

Chapter 20: Layer 7 DoS Mitigation and Advanced Bot Protection
• Defining Behavioral DoS Mitigation
• Common Uses for iRules
• Identifying iRule Components
• Triggering iRules with Events
• Defining ASM iRule Events
• Defining ASM iRule Commands

Chapter 21: ASM and iRules
• Using ASM iRule Event Modes

Chapter 22: Using Content Profiles
• Defining Asynchronous JavaScript and XML
• Defining JavaScript Object Notation (JSON)
• Defining Content Profiles
• The Order of Operations for URL Classification

Chapter 23: 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 Layer 7 Local Traffic Policies

Session Dates

On request. Please contact us

Additional Information

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