SETTING UP F5 ADVANCED WAF
DURATION - 1 DAYS

COURSE OVERVIEW

Do you need to secure your applications quickly from today's threats such as those from automated agents, bots, and common vulnerabilities? Are you limited by time, resources, and knowledge of your web applications? Do you need protection against CVEs without thinking too deeply about them?

In this 1 day course, participants identify and mitigate common web application vulnerabilities on the client and application sides of the threat spectrum. Participants use F5 Advanced WAF to quickly configure advanced protection against common Layer 7 vulnerabilities (OWASP Top Ten) and bot defense.

This course is intended for users who wish to rapidly deploy a basic web application security policy with minimal configuration.

PREREQUISITES

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

COURSE OBJECTIVES

- Provision the Application Security Manager and Fraud Protection Service modules
- Define a web application firewall
- Deploy F5 Advanced WAF using the Guided Configuration for Application Security
- Define learn, alarm, and block settings as they pertain to configuring F5 Advanced WAF
- Define attack signatures and explain why attack signature staging is important
- Contrast positive and negative security policy implementation and explain benefits of each
- Tune a policy manually by reviewing learning suggestions
- Deploy a Threat Campaign
- Mitigate Credentials Stuffing attacks
- Secure a URL from client-side fraud using DataSafe encryption and obfuscation
- Deploy F5 Advanced WAF using the Guided Configuration for L7 Denial of Service Protection
- Use the automated L7 Behavioral Denial of Service feature to detect and mitigate DoS attacks

WHAT YOU'LL LEARN

- Differentiating between client-side and application-side web vulnerabilities
- Categorizing Attack Techniques
- Use the Guided Configuration to deploy a Web Application Security Policy
- Defining the key parts of a Web Application Security Policy
- Understanding request logging options
- Identifying HTTP headers and methods
- Defining attack signatures, attack signature staging, and violations
- Overview of the OWASP Top Ten
- Review learning suggestions and basic policy tuning

- Deploy Threat Campaign
- Mitigate Credentials Stuffing
- Secure a URL from client-side fraud using DataSafe encryption and obfuscation
- Use the automated L7 Behavioral Denial of Service feature to detect and mitigate DoS attacks

WHO SHOULD ATTEND?

This course is intended for security and network administrators who will be responsible for the deployment of F5 Advanced Web Application Firewall to secure web applications from common vulnerabilities and denial of service.