

Setting up F5 Advanced WAF (TRG-BIG-AWF-SU1)

ID TRG-BIG-AWF-SU1 Preis US\$ 995,- (exkl. MwSt.) Dauer 1 Tag

Kursüberblick

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; deploy a DoS Protection Profile to detect server stress, and block bad actors.

Voraussetzungen

There are no F5-technology-specific prerequisites for this course. However, completing the following before attending would be very helpful for students with limited BIG-IP administration and configuration experience:

- [Administering BIG-IP \(TRG-BIG-OP-ADMIN\)](#)

or

- F5 Certified BIG-IP Administrator

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

Kursziele

- Provision resources for F5 Advanced Web Application Firewall
- Rapidly deploy a security policy using the Guided Configuration
- Configure learn, alarm, and block settings to ensure valid users can access your application
- Define attack signatures
- Contrast positive and negative security policy implementation
- Review learning suggestions for policy tuning
- Mitigate Credentials Stuffing attacks
- 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

Kursinhalt

- 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