Publication date : 12/05/2024

Course : F5 - Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

Official F5-TRG-BIG-AWF-CFG course, preparation for F5 certifications

Practical course - 4d - 28h00 - Ref. WA1

Avec cette formation, vous disposerez d'une compréhension fonctionnelle de la manière de déployer, de régler et d'utiliser F5 Advanced Web Application Firewall pour protéger vos applications web contre les attaques basées sur le protocole HTTP. Entre théorie et mise en pratique, vous aborderez les différents outils de F5 Advanced Web Application Firewall pour détecter et atténuer les menaces provenant de multiples vecteurs d'attaque tels que le web scraping, le déni de service de la couche 7, la force brute, les bots, l'injection de code et les exploits de type "zero day".

PARTICIPANTS

Security and network administrators who will be responsible for the installation, deployment, optimization and day-to-day maintenance of the F5 Advanced Web Application Firewall.

PREREQUISITES

F5 Certified BIG-IP Administrator" or equivalent level of knowledge. General knowledge or experience of network technologies is recommended.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Describe the role of the BIG-IP system as a complete proxy in an application distribution network
- ✓ Dimensioning the F5 Advanced Web Application Firewall
- ✓ Define a Web application firewall
- ✓ Explain how F5 Advanced WAF protects web applications through file, URL and parameter security
- ✓ Deploy F5 Advanced Web Application Firewall using the rapid deployment model
- ✓ Define the security controls included in each of them
- ✓ Define learning, alarm and blocking parameters as part of F5 Advanced WAF configuration
- ✓ Define attack signatures and explain the importance of staging attack signatures
- ✓ Deploy anti-threat campaigns to protect against CVE threats
- ✓ Compare positive and negative safety policies and detail the distinct advantages of each approach
- ✓ Configure security handling in web application parameters
- ✓ Deploy F5 Advanced Web Application Firewall using the automatic policy editor
- ✓ Adjust a policy manually or enable automatic policy creation
- ✓ Integrate the results of a third-party application vulnerability scanner into a security policy
- ✓ Configure connection application for flow control
- ✓ Mitigate credential stuffing
- ✓ Configuring protection against brute force attacks
- ✓ Deploy advanced defense against robots and other automated agents
- ✓ Deploy DataSafe to secure client-side data

Intended audience

Security and network administrators who will be responsible for the installation, deployment, optimization and day-to-day maintenance of the F5 Advanced Web Application Firewall.

Prerequisites

F5 Certified BIG-IP Administrator" or equivalent level of knowledge. General knowledge or experience of network technologies is recommended.

Certification

This course prepares you for certification as a "F5 Certified Technology Specialist, BIG-IP ASM".
Comment passer votre examen ?

Practical details

Teaching methods

Training in French. Official course material in digital format and in English. Good understanding of written English.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.
Assessment by the participant, at the end of the training course, of the skills acquired during the training course.
Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.
At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.
An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

Course schedule

1 BIG-IP system configuration

- Introducing the BIG-IP system.
- Initial configuration of the BIG-IP system.
- Archiving of BIG-IP system configuration.
- Use of resources and support tools F5.

2 Traffic processing with BIG-IP

- Identification of BIG-IP traffic processing objects.
- Comprendre les profils.
- Overview of local traffic strategies.
- View the HTTP request flow.

3 Web application concepts

- Overview of web application request processing.
- Layer 7 protection.
- Layer 7 security controls.
- Overview of Web communication elements.
- Overview of HTTP request structure.
- Examination of HTTP responses.
- Analyzes file types, URLs and parameters.
- Using the Fiddler HTTP proxy.

4 Web application vulnerabilities

- Threat overview.
- Common exploits against Web applications.

5 Deploying security strategies

- Defining learning.
- Comparison of positive and negative safety models.
- The deployment process.
- Assign a policy to the virtual server.
- Using advanced settings.
- Configure server technologies.
- Definition of attack signatures.
- Display requests.
- Safety checks offered by rapid deployment.
- Definition of attack signatures.

6 Optimizing strategies and offenses

- Post-deployment traffic handling.
- Categories of offence.
- Threat scale.
- Define staging and application.
- Define application mode.
- Define the application preparation period.
- Review the definition of apprenticeship.
- Define learning suggestions.
- Choose automatic or manual learning.
- Definition of learning, alarm and blocking parameters.
- Interpret the application readiness summary.
- Blocking response page configuration.

7 Attack signatures and threat campaigns

- Definition of attack signatures.
- Basics of attack signatures.
- Create user-defined attack signatures.
- Definition of simple and advanced editing modes.
- Definition of attack signature sets.
- Definition of attack signature pools.
- Understand attack signatures and how attacks are staged.
- Update attack signatures.
- Defining campaigns against threats.
- Deployment of campaigns against threats.

8 Developing a positive safety strategy

- Defining and learning security strategy components.
- Wildcard definition.
- Define the entity's life cycle.
- Choose your learning program.
- How to learn: Never (joker only), always and selectively.
- Review of the application preparation period.
- Display of learning suggestions and progress.
- Definition of the learning score.
- Definition of approved and unapproved IP addresses.
- How to learn: Compact.

9 Securing cookies and other headers

- Purpose of F5 Advanced WAF cookies.
- Definition of authorized and applied cookies.
- Secure HTTP headers.

10 Visual reporting and logging

- Displays application security summary data.
- Reports: create your own view.
- Reports: filter-based graphics.
- Statistics on brute force and Web Scraping.
- Display resource reports.
- PCI compliance : PCI-DSS 3.0.
- Analysis of requests.
- Installation and destination of local logging.
- Display logs in the configuration utility.
- Define logging profile.
- Configure response logging.

11 Advanced parameter management

- Definition of parameter types.
- Define static parameters.
- Define dynamic parameters.
- Definition of parameter levels.
- Other parameter considerations.

12 Automatic strategy generation

- Overview of automatic strategy development.
- Definition of models that automate learning.
- Defining strategy relaxation.
- Defining the tightening of strategies.
- Definition of learning speed.
- Definition of follow-up site modifications.

13 Integration of web application vulnerability scanner

- Integration of scanner output.
- Import vulnerabilities.
- Vulnerability resolution.
- Use of the generic XML scanner XSD file.

14 Layered strategy deployment

- Define a parent strategy.
- Define inheritance.
- Parent strategy deployment use case.

15 Connection enforcement and brute force mitigation

- Definition of connection pages for flow control.
- Configure automatic detection of login pages.
- Defining brute force attacks.
- Configuration of brute force protection.
- Source-based brute force mitigation.
- Definition of how to fill in identification information.
- Reduce the need to fill in identification information.

16 Recognition with session tracking

- Definition of session tracking.
- Configure actions in the event of violation detection.

17 Layer 7 DoS mitigation

- Definition of denial-of-service attacks.
- DoS protection profile definition.
- Introducing TPS-based DoS protection.
- Create a DoS logging profile.
- Application of GST rebates.
- Definition of behavioral and stress-based detection.

18 Advanced Defense Bots

- Classification of customers with the Bot Defense profile.
- Definition of bot signatures.
- Fingerprint definition F5.
- Definition of Bot Defense profile templates.
- Defining protection for microservices.

19 Encrypting forms with DataSafe

- Targeting application delivery elements.
- Use the document object model.
- Application protection with DataSafe.
- The order of operations for URL classification.