BLACKBIRD FOR TRAINING

FortiWeb Web Application Firewall (WAF) Administration and Security

24 – 28 January 2027
Online



FortiWeb Web Application Firewall (WAF) Administration and Security

Ref: 3255871_354365 **Date:** 24 – 28 January 2027 **Location:** Online **Fees:** 2700 GBP

Introduction

As organizations continue to expand their digital services, web applications have become essential for delivering business operations, online services, customer engagement, and critical enterprise functions. However, the growing dependence on web-based technologies has also increased exposure to sophisticated cyber threats targeting web applications. Attacks such as SQL Injection, Cross-Site Scripting XSS, command injection, malicious file inclusion, and denial-of-service attacks can compromise sensitive information, disrupt business operations, and damage organizational reputation.

A Web Application Firewall WAF plays a critical role in protecting web applications by monitoring, filtering, and securing HTTP and HTTPS traffic before it reaches application servers. Among the leading WAF solutions, FortiWeb provides advanced security capabilities that help organizations detect, prevent, and respond to web application attacks while maintaining application availability, performance, and regulatory compliance.

The FortiWeb Web Application Firewall WAF Administration and Security course provides participants with a comprehensive understanding of web application security principles and the deployment, configuration, administration, and optimization of FortiWeb in enterprise environments. The course covers security policy configuration, application protection profiles, traffic inspection, attack prevention, event monitoring, log analysis, performance optimization, troubleshooting, and security best practices for protecting modern web applications.

Participants will also gain insight into the latest web application threats, the OWASP Top 10 security risks, cyberattack mitigation strategies, security monitoring, compliance requirements, and the integration of FortiWeb with enterprise cybersecurity infrastructures. By the end of the course, participants will be equipped with the knowledge required to strengthen web application security, improve operational resilience, and enhance the overall cybersecurity posture of their organizations.

Course Objectives

By the end of this training course, participants will be able to:



- Understand the principles and architecture of Web Application Firewalls WAFs.
- Explain the architecture, components, and deployment models of FortiWeb.
- Deploy and configure FortiWeb within enterprise environments.
- Understand the OWASP Top 10 web application security risks and their impact on business operations.
- Develop and manage Web Application Firewall security policies.
- Configure and maintain application security profiles.
- Monitor and analyze HTTP and HTTPS traffic to identify abnormal activities.
- Implement access control policies to protect web applications and users.
- Protect web applications against SQL Injection, Cross-Site Scripting XSS, command injection, malicious file inclusion, and other common web attacks.
- Monitor security events, analyze system logs, and generate security reports.
- Troubleshoot FortiWeb operational issues and optimize system performance.
- Apply industry best practices to strengthen enterprise web application security.

Course Outlines

Day 1: Web Application Security Fundamentals and FortiWeb Architecture

- Fundamentals of web application security.
- Common web application threats and vulnerabilities.
- Understanding the OWASP Top 10 security risks.
- FortiWeb architecture, components, and deployment models.
- Deploying FortiWeb in enterprise environments.
- Initial system installation and configuration.
- System administration and management interface overview.

Day 2: Security Policies and Application Protection Profiles

- Creating and managing Web Application Firewall security policies.
- Configuring application protection profiles.
- HTTP and HTTPS traffic inspection techniques.
- URL access control and application access management.
- User authentication and access control mechanisms.
- Session security and user protection.
- Reviewing and optimizing security policy effectiveness.



Day 3: Web Application Threat Protection

- Protecting applications against SQL Injection attacks.
- Preventing Cross-Site Scripting XSS attacks.
- Protecting against command injection and malicious file inclusion attacks.
- Detecting and managing malicious bot traffic.
- Protecting applications against DoS and DDoS attacks.
- Security signatures and attack detection mechanisms.
- Security event analysis and alert management.

Day 4: Monitoring, Logging, and Security Reporting

- Log management and security event analysis.
- Continuous monitoring of application security events.
- Security alert configuration and management.
- Security dashboards and operational visibility.
- Security reporting and compliance requirements.
- Security incident investigation techniques.
- Integration with Security Information and Event Management SIEM platforms.

Day 5: Performance Optimization, Advanced Administration, and Best Practices

- Troubleshooting common FortiWeb issues.
- Performance tuning and operational optimization.
- High Availability HA configuration and management.
- Backup and disaster recovery procedures.
- System maintenance and software updates.
- Industry best practices for Web Application Firewall administration.
- Developing a comprehensive web application security strategy for enterprise environments.



Why Attend this Course: Wins & Losses!

- Develop a comprehensive understanding of Web Application Firewall WAF technologies and their role in enterprise cybersecurity.
- Gain in-depth knowledge of the FortiWeb architecture, deployment models, and administration capabilities.
- Strengthen the ability to configure and manage Web Application Firewall security policies.
- Improve skills in protecting web applications against the most common cyber threats, including the **OWASP Top 10** security risks.
- Enhance the ability to inspect and analyze web application traffic to identify malicious activities.
- Learn how to configure application protection profiles and user access control mechanisms.
- Improve security monitoring through effective log analysis, event management, and security reporting.
- Strengthen troubleshooting capabilities to resolve operational issues and improve FortiWeb performance.
- Understand High Availability HA, backup, recovery, and business continuity considerations.
- Apply internationally recognized best practices for securing enterprise web applications and maintaining regulatory compliance.

Conclusion

Protecting web applications has become a critical component of modern cybersecurity strategies as organizations increasingly rely on web-based services to support business operations, customer engagement, and digital transformation initiatives. Implementing an effective Web Application Firewall is essential for defending against evolving cyber threats, safeguarding sensitive information, maintaining application availability, and ensuring regulatory compliance.

The FortiWeb Web Application Firewall WAF Administration and Security course provides participants with a comprehensive understanding of Web Application Firewall technologies and the administrative, operational, and security capabilities of FortiWeb. Throughout the course, participants explore web application security fundamentals, security policy management, application protection profiles, threat detection, attack prevention, event monitoring, log analysis, performance optimization, High Availability, and enterprise security best practices.

By combining internationally recognized cybersecurity practices with FortiWeb-specific administration techniques, this course enables participants to strengthen their ability to deploy, manage, monitor, and optimize Web Application Firewall solutions within enterprise environments. Upon completion, participants will be better equipped to improve web application security, enhance operational resilience, support compliance requirements, and contribute to building a stronger and more secure cybersecurity infrastructure for their organizations.

