

FORTIWEB WEB APPLICATION FIREWALL (WAF) ADMINISTRATION AND SECURITY



GENTEX[®]
TRAINING CENTER



Introduction

Web applications now carry the core of most business operations, which makes them a prime target for attackers. The FortiWeb Web Application Firewall (WAF) Administration and Security Training Course prepares security professionals to protect these applications using Fortinet's dedicated WAF platform. Participants learn to deploy FortiWeb, build protection policies, and defend against threats such as SQL injection, cross-site scripting, and application-layer denial of service. The course combines theoretical foundations with hands-on configuration on FortiWeb appliances and virtual machines. Furthermore, it covers tuning, monitoring, and troubleshooting so that defenses stay accurate and reliable. As a result, teams leave with the practical ability to reduce risk, meet compliance expectations, and keep critical web services available.

FortiWeb Web Application Firewall (WAF) Administration and Security Course Objectives

- Deploy FortiWeb in reverse proxy, transparent, and offline inspection modes.
- Configure server policies, protection profiles, and HTTP content routing rules.
- Build and maintain web application firewall signatures and custom attack rules.
- Use machine learning to detect anomalies and reduce false positives.
- Apply protection against the OWASP Top 10 web application risks.
- Configure bot mitigation, threat feeds, and IP reputation controls.
- Manage SSL/TLS offloading and certificate inspection.
- Implement API protection and JSON payload validation.
- Monitor events through logs, alerts, and the FortiWeb dashboard.
- Automate tasks using the CLI, REST API, and FortiManager integration.

Course Methodology



LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Instructor-led sessions that combine concept delivery with live demonstrations.
- Guided hands-on labs on FortiWeb appliances and virtual instances.
- Real attack simulations against a controlled vulnerable web application.
- Scenario-based exercises in policy tuning and false-positive analysis.
- Group discussion and troubleshooting clinics using actual log data.
- Continuous knowledge checks and a final practical assessment.

Who Should Take This Course

- Web application security engineers and WAF administrators.
- Network security analysts and SOC team members.
- Security architects responsible for application protection.
- IT infrastructure engineers managing web-facing services.
- Network administrators moving into application security roles.
- Consultants and auditors assessing web security controls.

FortiWeb Web Application Firewall (WAF) Administration and Security Course Outlines

Day 1: FortiWeb Fundamentals and Deployment

- Common web application attack types and their business impact.
- FortiWeb architecture and hardware and virtual form factors.
- Deployment modes: reverse proxy, transparent, and offline.
- Initial setup, licensing, and administrative access.
- Network interfaces, routing, and virtual servers.
- Server policy structure and basic traffic flow.



LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Lab: first deployment and administrative hardening.

Day 2: Policy Configuration and Traffic Management

- Server pools, health checks, and load balancing.
- HTTP content routing and URL rewriting.
- SSL/TLS offloading and certificate management.
- Client authentication and access control options.
- HTTP protocol constraints and header validation.
- Virtual server versus server policy relationships.
- Lab: building a multi-server policy for a web farm.

Day 3: Threat Protection and Attack Signatures

- Signature-based detection and attack signature sets.
- Protection against SQL injection and cross-site scripting.
- Cookie security, CSRF tokens, and session protection.
- Machine learning for anomaly and bot detection.
- Bot mitigation, IP reputation, and threat feeds.
- Custom signatures and exception handling.
- Lab: blocking live attacks against a test application.

Day 4: Tuning, API Protection, and Compliance

- False positive analysis and policy tuning workflow.
- Parameter validation and JSON payload inspection.
- API gateway protection and schema enforcement.
- DDoS and application-layer rate limiting.



LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- PCI DSS and OWASP Top 10 alignment.
- Change management and policy version control.
- Lab: tuning a policy and securing a REST API.

Day 5: Monitoring, Automation, and Troubleshooting

- Dashboards, log repositories, and report configuration.
- Alerting, syslog, and SIEM integration.
- CLI command structure and configuration backup.
- REST API automation for routine tasks.
- FortiManager and FortiAnalyzer integration.
- Diagnosing performance and false-negative issues.
- Lab: end-to-end monitoring and automation exercise.

Conclusion

By successfully completing the FortiWeb Web Application Firewall (WAF) Administration and Security Training Course, participants will have acquired the ability to deploy FortiWeb, build layered protection policies, block real application attacks, and tune defenses for accuracy. They will also gain confidence in monitoring, automating, and troubleshooting the platform in live environments. In addition, the course strengthens compliance readiness and incident response skills. Gentex Training Center delivers this program with an emphasis on practical, job-ready application security competence.

FAQs





Q1 What is the "FortiWeb Web Application Firewall (WAF) Administration and Security" course about?

It is a hands-on program on deploying and managing FortiWeb to protect web applications. Participants learn policy creation, attack signature configuration, SSL inspection, API protection, and monitoring, using FortiWeb appliances and virtual machines in guided labs.

Q2 What are the key benefits of the "FortiWeb Web Application Firewall (WAF) Administration and Security" course?

Participants gain the practical confidence to stop SQL injection, cross-site scripting, and bot traffic before it reaches applications. They learn to tune policies that reduce false positives, improve compliance alignment with PCI DSS and OWASP guidance, and strengthen the availability of customer-facing web services.

Q3 What skills will I gain from the "FortiWeb Web Application Firewall (WAF) Administration and Security" course?

FortiWeb deployment and configuration, web attack mitigation, security policy tuning and false-positive analysis, and log-based monitoring and troubleshooting.



Q4 What tools, methods, or standards are covered in the "FortiWeb Web Application Firewall (WAF) Administration and Security" course?

The course covers the FortiWeb platform, FortiManager and FortiAnalyzer integration, the FortiWeb REST API and CLI, machine learning attack detection, bot mitigation and threat feeds, and standards such as the OWASP Top 10 and PCI DSS requirements.

Q5 How is the "FortiWeb Web Application Firewall (WAF) Administration and Security" course applied in real-world practice?

Graduates apply it by placing FortiWeb in front of production web and API services, building protection profiles for each application, reviewing logs daily for tuning, and automating configuration tasks. SOC and security teams use the same skills for incident triage and audits.