FortiWeb 5.0, Web Application Firewall

Course #251

Course Overview

Through this 1-day instructor-led classroom or online virtual training, participants learn the basic configuration and administration aspects of the most commonly used features on the FortiWeb Web Application Firewall Appliance. Through interactive modules, participants explore server policies, web protection profiles, DoS protection policies, load balancing, authentication offloading, SSL offloading, auto learn, web vulnerability scan, and more. This training provides a solid understanding of how to implement, administrate and troubleshot a FortiWeb solution in a corporate environment.

Course Objectives

At the conclusion of this course, participants will be able to:

- Identify the most common web application attacks
- Understand the benefits of using a web application firewall
- Describe the main FortiWeb characteristics and features
- Understand the differences between the different operation modes
- Configure serve policies and web protection profiles to protect a web application
- Describe the most important settings inside web protection rules and policies
- Implement SSL offloading, authentication offloading, compression offloading, SSL inspection and load balancing
- Import and manage certificates for FortiWeb use
- Configure the FortiWeb device to protect web applications against DoS attacks
- Use auto-learn to create ad hoc web protection profiles
- Describe the OSWASP top 10 guidelines
- Configure the FortiWeb device to comply with each of the OSWASP top 10 guidelines
- Analyze the data from a web vulnerability scan report
- Know the basic commands and tools to start a troubleshooting process

Products Used in This Course

- FortiWeb Appliance

Prerequisites

- Extensive experience administrating web applications
- Basic understanding of web security
- Basic understanding of firewall concepts

System Requirements

If performing this training online, students will require the following:

- A high-speed Internet connection
- A Web browser that supports the Adobe Flash Player to launch the Virtual Classroom
- Speakers or a headset to follow along with the audio portion of the presentation
- Adobe Reader to view on-line class materials

Who Should Attend

This course is intended for networking professionals involved in the installation, administration, management and troubleshooting of a web security infrastructure using FortiWeb appliances.

AGENDA

Module 1: Functional Overview

In this module students review the types of web application attacks and why Web Application Firewalls are needed. This module also provides a quick overview of the FortiWeb features and product family. Finally, students learn the different FortiWeb deployment options.

Objectives

At the conclusion of this module, participants will be able to:

- Describe the FortiWeb deployment options
- Explain the importance of using Web Application Firewall (WAF) to protect web applications

Topics

- Introduction to web application attacks
- Most common categories of web application attack techniques
- Benefits of using a Web Application Firewall
- FortiWeb characteristics and features
- FortiWeb family of appliances and Virtual Machines
- Operation modes

Module 2: System Configuration

In this module students learn to access the unit, configure the initial device settings, and create custom admin accounts. The module also explains how to implement a high availability solution using 2 FortiWeb devices.

Objectives

At the conclusion of this module, participants will be able to:

- Access the unit's Graphical User Interface (GUI) and Command Line Interface (CLI)
- Configure the initial FortiWeb device settings
- Test the FortiWeb network connectivity

Topics

- Accessing the Graphical User Interface (GUI) and the Command Line Interface (CLI)
- Real-time Dashboard
- Context Sensitive On-Line Help
- Configuring the network interfaces and V-zones
- FortiWeb routing
- IP-based forwarding
- Creating admin accounts and access profiles
- Introduction to FortiGuard subscription services
- Fail-open configuration
- High-availability (HA)
- Upgrading the firmware

Module 3: Policies and Profiles

In this module students learn to create server policies and objects, such as virtual and physical servers, server farms and custom services. The module also describes the SSL offloading, SSL inspection and load balancing features.

Objectives

At the conclusion of this module, participants will be able to:

- Configure a serve policy to protect a web application
- Configure application load balancing between two physical web servers
- Check that the load balancing feature is working properly
- Generate a certificate signing request
- Import a signed certificate into the FortiWeb device
- Implement SSL offloading

Topics

- Server policies
- Web protection profiles
- Configuration steps
- Policy behavior by operational mode
- Virtual server
- Physical server
- Server farm
- Load balancing
- Certificate management
- SSL offloading
- SSL inspection
- Customized services
- Protected host groups

Module 4: Web Protection

This module explains some of the most important Web protection rules and policies. Students also learn to disable and create exception for specific policies.

.

Objectives

At the conclusion of this module, participants will be able to:

- Describe the most important settings inside the web protection rules and policies
- Configure a web protection profile to protect a web application

Topics

- Standalone and shared IP
- IP list
- Brute force
- Cookie poison detection
- HTTP protocol constraints
- Start page and page order rules
- Parameter validation
- Upload restriction
- IP reputation
- Signature polices
- Anti-defacement
- URL access
- Known search engines
- Cross site scripting (XSS)
- SQL injection
- Bad robots
- Credit card detection
- AV scanning
- Generic attacks and known exploits
- Tuning the signature policy

Module 5: Application Delivery and DoS

In this module, students learn how to do authentication offloading and configure the FortiWeb device to protect web applications against DoS attacks.

Objectives

At the conclusion of this module, participants will be able to:

- Describe the most important settings inside the authentication, file compress and DoS protection policies
- Configure and test authentication offloading

Topics

- Authentication offloading
- Local users
- Remote authentication servers
- File compression offloading
- Introduction to DoS protection
- HTTP access limit
- Real browser enforcement
- Malicious IPs
- HTTP flood prevention
- TCP flood prevention
- SYN cookie

Module 6: Auto-Learning

This module explains how to configure, monitor and use the auto-learn feature to create ad-hoc web protection profiles.

Objectives

At the conclusion of this module, participants will be able to:

- Configure the auto-learn functionality
- Analyze the auto-learn results
- Use auto-learn to create ad hoc web protection profiles

Topics

- Introduction to auto-learning
- Data type group
- Suspicious URL
- Application policy
- Auto-learn profile
- Auto-learn report overview
- Generating the web protection profile from the auto-learn report
- Auto-learn best practices

Module 7: PCI DSS Compliance and Vulnerability Assessment

This module lists the two PCI DSS (Payment Card Industry Data Security Standard) requirements that are specific for web applications. Additionally, it explains how to set up the FortiWeb to adhere to the OWASP top 10 guidelines.
Students also learn to run a web vulnerability scan and analyze its results.

Objectives

At the conclusion of this module, participants will be able to:

- Describe the OSWASP top 10 guidelines
- Describe how FortiWeb can be configured to comply with each of the OSWASP top 10 guidelines
- Configure the FortiWeb to run a web vulnerability scan
- Analyze the data from a web vulnerability scan report

Topics

- Overview of the Payment Card Industry Data Security Standard (PCI DSS)
- PCI DSS Requirements for web application firewalls
- Introduction to the Open Web Application Security Project (OWASP)
- Using the FortiWeb device to protect web applications from the OWASP top 10 vulnerabilities
- Web vulnerability scan preparation and execution
- Understanding the web vulnerability scan Report

Module 8: Troubleshooting

In this module, students learn some basic commands and procedures to troubleshoot technical problems.

Objectives

At the conclusion of this module, participants will be able to:

- Know the basic commands to start any troubleshooting process
- Use the attack console to solve false-positive issues
- Understand how FortiGuard works

Topics

- FortiWeb unit storage structure
- Storage Maintenance
- FortiGuard troubleshooting
- Checking the system status
- Monitoring the system performance
- Network interface statistics
- Checking the ARP table
- Connectivity test commands
- Packet sniffer
- Event logs
- Attack logs
- Integration with FortiAnalyzer
- Data analytics
- Bot analysis
- Blocked IPs
- Troubleshooting false-positive issues
- UDP and TCP port for outgoing and incoming connections