DefensePro X Level 1 Training Course Outline

Version 10.x

1 Introduction

DefensePro provides automated DDoS protection from fast-moving, high-volume, encrypted or very-short-duration threats and is part of Radware's attack mitigation solution. It defends against IoT-based, Burst, DNS and TLS/SSL attacks to secure organizations against emerging network multi-vector attacks, ransom DDoS campaigns, IoT botnets, phantom floods, and other types of cyberattacks.

2 Target Audience and Prerequisites

This course is designed for technicians with a solid knowledge of networking in the areas of switching and routing.

Additionally, knowing how applications and network protocols are working (like TCP, HTTP, HTTPS) is a key asset for setting up signatures and traffic filters. Knowledge of penetration testing is very useful.

3 Purpose and Scope

This course, DefensePro X Level 1, is a structured 3-day certification training.

It consists of a practical and a theoretical part.

In this course we focus on the advanced features used in many different DDoS protection deployments.

The course starts with a short basics overview of different DoS attacks. Flood detection with SSL protected data are our next topics. For behavioral protection, we have several different protective measures on our agenda; Anti-Scanning, UDP Advanced Protection and troubleshooting and providing a well working setup for it. We have prepared different DDoS attacks; students are required to find out the attacking parameters and set up suitable protection on DefensePro.

The features and functions of Radware devices discussed in this document are based on the following firmware version.

Product	Version
DefensePro X	10.x
Cyber Controller	10.x

4 Course Duration and Objectives

This comprehensive 3-day instructor-led program is designed to provide participants with a deep understanding of the full capabilities of the DefensePro X platform. Through a structured blend of theoretical instruction and immersive hands-on labs, attendees will explore the system's core features, configuration options, and advanced protection mechanisms.

Key highlights of the course include:

- **In-depth exploration** of DefensePro X functionalities and architecture
- **Interactive lab sessions** simulating real-world threat scenarios
- **Step-by-step guidance** on deploying and managing security policies
- **Best practices** for optimizing performance and ensuring robust protection

By the end of the training, participants will be equipped with the practical skills and technical knowledge needed to confidently operate and maintain DefensePro X in dynamic network environments.

4.1 Objectives

- Install and deploy a DefensePro X based on deployments guidelines.
- Understand the different Attack Protection capabilities and how to configure them.
- Learn how to use BDoS attack detections
- Detect SSL encrypted attacks and configure how to protect against
- Navigate and use central management system, Cyber Controller
- Understand fundamentals of AMS Analytics

5 DefensePro X Presentations and Hands on Labs

5.1 Day 1 – Getting Started with DefensePro X

Presentations:

- Introduction to DefensePro X
  - Overview of the solution, its role in network protection, and how it fits into the overall security ecosystem.
- Hardware and Connectivity
  - A closer look at the system architecture, hardware components, and how the device connects to the network.
- Administration and Security Policies
  - Understanding how to manage the platform, defining user roles, and implementing core security policies.
- Basic Protections:
  - Covering AccessList, Rate Limit, Geolocation based protection and ERT Active Attacker Feed

Hands on Labs:

Administration and Initial Configuration:

- Practical exercises including:
  - Setting up DefensePro X for the first time
  - Connecting the system to Cyber Controller for management
  - Performing basic administrative tasks
  - Configure Block and Allow lists
  - Configure Geolocation and ERT Active attacker feed protection
  - Configure Connection Limits

5.2 Day 2

Presentations:

- Behavioral DoS module
  - Exploring how the system detects and mitigates abnormal traffic patterns.
- DNS Protection
  - Safeguarding critical DNS services from flood and amplification attacks.
- SYN Flood Protection
  - Techniques to block SYN flood attacks that attempt to overwhelm servers.
- SSL Protection
  - Providing an overview of SSL attack protection and explaining the first request protection using the SYN flood protection on SSL traffic

Hands on Labs:

- **Network Flood Protection – Step-by-step practice with:**
  - Creating and using Behavioral DoS Protection
  - Creating and using DNS Flood Protection
  - Configuring and testing SYN Flood Protection
  - Configuring and testing SSL Protection

5.3 Day 3

Presentations:

- Out of State Protection
  - Understanding TCP state tracking and how to protect against invalid traffic.
- Signature Protections
  - Detecting and blocking attacks based on known signatures and patterns.
- AMS Analytics for DefensePro X
  - Introduction to the integrated monitoring and analytics tool that provides visibility and insights into security events.
- Troubleshooting
  - Key tools and techniques to diagnose and resolve common issues.

Hands on Labs:

- Configure and test Out of State Protection
- Signature Protection – Step-by-step practice with:
  - Applying and managing signature protections
  - Creating and using block/allow lists
  - Configuring and testing connection limits
- Use the AMS Analytics to get insight on attacks
  - Creating reports
  - Creating alerts
  - Reviewing Forensic data

6 Certification

To earn certification, participants must successfully complete both a theoretical and a practical examination. These assessments are designed to validate a solid understanding of the DefensePro X system and the ability to apply its features in real-world scenarios. Exams are delivered online and can be accessed from any location—only a stable internet connection is required, offering maximum flexibility for learners worldwide.

For both exam parts the minimum passing grade is 75%.

When you pass both parts, you will be recognized as:
Radware Certified Security Specialist (RCSS)

6.1 Hands-On Practical Exam

As part of the certification process, candidates are required to configure a DefensePro X system based on a set of realistic customer requirements. This task reflects scenarios covered during the hands-on portion of the training and is designed to assess the participant's ability to apply their knowledge in a practical, solution-oriented context.

The exam is proctored remotely and evaluated by Radware's Technical Training Team, ensuring a fair and consistent assessment process. Participants are expected to demonstrate proficiency in system setup, policy implementation, and threat mitigation strategies aligned with best practices.

6.2 Online Certification Exam

The online theoretical exam consists of carefully crafted multiple-choice questions that assess the participant's comprehension of the concepts and technologies presented during the classroom sessions.

Designed to test both foundational knowledge and solution-specific understanding, the exam ensures that candidates can confidently interpret and apply the principles behind DefensePro X's architecture and functionality.

Accessible from anywhere with an internet connection, the exam offers a flexible and convenient way to validate learning outcomes while maintaining rigorous standards.

North America
Radware Inc.
575 Corporate Drive, Lobby 1
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: +972 3 766 8666