

300-101 Defense Pro Level 1

Overview

Learn how to isolate, block and prevent application-level attacks, coupling unmatched security performance with advanced security intelligence. Understand how to securely connect and protect all mission-critical applications by thwarting viruses, intrusions, Trojans, worms and Denial of Service attacks. Learn how to eliminate security tool vulnerabilities and bottlenecks across all combined security architectures, overcoming the security vs. performance trade-off for fault-tolerant and highly scalable defense.

Please bring your laptop to complete the hands-on lab exercises. Students will use well-known applications such as PDF Reader, VNC, Telnet, SSH and possibly other Radware-proprietary apps. Therefore, it is also important to have administrative rights on your laptop.

Course Length

3 days

Objectives

- Install and deploy a DefensePro based on deployments guidelines
- Understand the different Attack Protection capabilities and how to configure them
- Navigate and use APSolute Vision
- Understand fundamentals of Vision Reporter.

Prerequisites

Familiarity with common network terminology, TCP/IP addressing & routing, and Internetworking concepts is required.

Delegates should also be proficient in basic PC operation and application, including skilled at operating a keyboard, mouse and Windows OS as well as basic Web browser operation (Internet Explorer used in class).

Certification

To earn the Radware Certified Security Specialist (RCSS) accreditation, candidates must successfully complete Defense Pro Level 1 training, pass the hands-on Practical Exam, and successfully complete the online certification exam.



Day 1

Presentations

- Security Landscape Overview
- Introduction to AMS
- Introduction to DefensePro
- Hardware to Connectivity
- Administration and Security Policies
- Behavioral Dos

Hands on Labs:

- Administration and Configuration
- Lab 1a- Initial DefensePro Setup
- Lab 1b- Connecting to your DefensePro Using APSolute Vision
- Lab 2- Administering DefensePro
 - Network Flood Protection
- Lab 3- Behavioral DoS Protection

Day 2

Presentations

- Netx Generation DNS Protection
- SYN Flood Protection
 - DefenseSSL
- Out State Protection
- Connection Limits

Hands on Lab

Network Flood Protection:

- Lab 4- DNS Flood Protection
- Lab 5- SYN Flood Protection
- Lab 6- SYN Flood SSL Protection
- Lab 7- Out of State Protection
- Lab 8- Connection Limits



Day 3

- Signature Protections
 - Signature Profiles
 - Custom Signatures
- Policy Exceptions (Black & White Lists)
- Vision and Vision Reporter
- Deployment Guidelines

Hands on Lab

- Signature Protection
 - Lab 10- Signature Protection
 - Lab 11- Custom Signatures
- Additional Components
 - Lab 12- Policy Exceptions (Black & White lists)
 - Lab 13- Administration
 - Lab 14- Vision Reporter

