radware Smart Network. Smart Business.

Course Code: 300-x01

DefenseFlow

Training Course Outline

Version 1.0

1 Purpose

This document is protected by United States and International copyright laws.

Neither this document nor any material contained within it may be duplicated, copied or reproduced, in whole or part, without the expressed written consent of Radware, Inc.

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

Product	Version
DefenseFlow	2.9.x
DefensePro	7.x or 8.x
APSolute Vision	3.95

2 Course Duration and Objectives

The DefenseFlow class is a structured 2-day course that is meant to highlight all the features and functions used on the DefenseFlow along with hands on labs to illustrate the protection mechanics.

2.1 Objectives

- Install and deploy a DefenseFlow 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

3 DefenseFlow Presentations and Hands on Labs

3.1 Day 1

Presentations:

- Introduction to DefenseFlow
- DefenseFlow Technical Overview

Hands on Labs:

Administration and Initial Configuration:
Configure Management IP and Gateway
Configure NTP server and time zone
Register DefenseFlow to APSolute Vision

Configure DefenseFlow
Check relevant licensing
Adapt BDOS learning and attack grace period
Configure IP settings to manage and control
Add Router as Network Element
Add DefensePro as Mitigation Device

Configure Use Case Netflow based Attack detection with Radware Flow-Collector and BDOS on DefenseFlow
Add the Flow-Collector as Control Element
Configure the security settings and the Protected Object
Start legitimate traffic to create the base line on the BDOS
Run Attack using automatic protection flow
Run Attack using semi-automatic protection flow
Run Attack and start protection manually

3.2 Day 2

Presentations:

- DefenseFlow Attack Walkthrough
- Radware Flow Collector
- Security Templates
- BGP Flowspec and Filters

Hands on Labs:

Configure Use Case: DefensePro as Detector
Configure DefenseFlow to use a DefensePro as detector
Run an attack to see the delegation from DefensePro to DefensePro

Configure Use Case: External Detector signaling an attack
Configure DefenseFlow to use an external device as detector
Run an attack to see the traffic diversion to the DefensePro in the Scrubbing center based on the attack signaled from the external detector

Filter, Tuning during a live attack
Change security policy during an attack
Blacklist an IP address during an attack
Use Filters to Blacklist/Whitelist traffic during an attack

Mahwah, NJ 07430
Tel: +1-888-234-5763

Tel Aviv 69710, Israel
Tel: +972 3 766 8666