Course Code: 300-x01

DefenseFlow

Training Course Outline

Version 5.0

1 Introduction

Cyberassaults against networks of service providers can include multiple vectors with vaqrious characteristics, thereby threatening network infrastructure elements and requiring multiple methods of mitigation. **DefenseFlow** is a network detection and cybercontrol application designed to automate and orchestrate the detection and mitigation of network, multivector attacks. Radware's DefenseFlow supports always-on/SmartTap and hosted customer protection use cases for service providers to provide the widest attack detection combined with real-time attack mitigation.

2 Purpose and Scope

This course, **DefenseFlow**, is a structured 2-day training.

It consists of a *practical* and a *theoretical* part.

In this course we will focus on the features used in all different DefenseFlow deployments.

The course begins by explaining the benefits of DefenseFlow. We continue with the basics required to set up a DefenseFlow from scratch and walk through the various installation tasks. In this training we will discuss attack detection with FlowDetector, DefensePro and external detectors. We explain how you can monitor attacks in Vision Analytics and examine various parameters before and during an attack. It also explains how the Managed Security Service Providers (MSSP) portal works. We also cover DefenseFlow in redundancy mode. Our final topic is troubleshooting. We explain the different commands and options to get information to correct incorrect values.

3 Target Audience and Prerequisites

A prerequisite for this course is DefensePro Level 1 training.

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

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

Product	Version
DefenseFlow	4.x
FlowDetector	2.x
DefensePro	8.x
APSolute Vision	5.x

4 Course Objectives

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

5 DefenseFlow Presentations and Hands on Labs

5.1 Day 1

Presentations:

- Introduction to DefenseFlow
- DefenseFlow Technical Overview
- DefenseFlow Attack Walkthrough
- Security Templates

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: DefensePro as Detector and IP-Mode DP as Scrubber
- Configure DefenseFlow to use a DefensePro as detector
- Run an attack to see the delegation from DefensePro to DefensePro in IP-Mode

Configure Use Case: DefensePro as Detector and transparent DP as Scrubber
- Configure DefenseFlow to use a DefensePro as detector
- Run an attack to see the delegation from DefensePro to DefensePro

5.2 Day 2

Presentations:

- FlowDetector
- MSSP Portal
- BGP Flowspec and Filters
- High Availability
- Best Practice SmartTAP

Hands on Labs:

Configure Use Case: FlowDetector as Detector and transparent DP as Scrubber

- Configure DefenseFlow to use a FlowDetector as detector
- Run an attack to see the detection from FlowDetector

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

MSSP Portal

Review the capabilities of the MSSP portal

Exercise configure multi step diversion

- Configure DefenseFlow to use a DefensePro as detector and divert the traffic to different devices according to the attack bandwidth
- Run an attack to see the delegation from DefensePro to DefensePro

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