

Training Lab Manual Configure BDoS



Table of Contents

Contents

OBJECTIVES.....	3
OVERVIEW	3
DISABLE PROTECTION POLICY.....	3
GLOBAL SETUP CONFIGURATION	3
CREATE BDOS PROFILE	5
TEST AND MONITOR THE CONFIGURATION.....	6
OPEN THE ATTACKER MACHINE AND SEND A TCP FLOOD ATTACK.....	6
USE RAPTOR TO SEND AN UDP FLOOD ATTACK.....	8
USE RAPTOR TO SEND ICMP FLOOD ATTACK.....	8

Objectives

After reviewing the BDoS training module and completing this lab, you should be able to configure and monitor Behavioral DoS (BDoS) protection.

Overview

Radware DefensePro can be configured to protect against Behavioral DoS flood attacks that misuse network bandwidth resources including: TCP Floods, UDP floods, ICMP floods, IGMP floods and fragmented attacks. Radware's Network Behavioral Analysis (NBA) module employs patented behavioral-based, real-time signature technology. It creates baselines of normal network, application, and user behavior; then analyzes traffic in real-time to create signatures to mitigate attacks.

Disable Protection Policy

Before continuing with this please disable the policy you loaded in a previous lab.

1. Select **vDefensePro** in the **Sites and Devices**
2. **Configuration → Protection → Protection Policies** select the policy (TeamLab)
3. Double click and uncheck the Enabled option.
4. Click **Submit**

Protection Policies *Edit Protection Policy**

☐ Enabled

Policy Name: TeamLab

Action: Block and Report

Classification

CLASSIFICATION

Priority: 100

SRC Network: any

DST Network: TeamLab

Port Group:

Direction: One Way

Context:

Submit Cancel

5. Click **Update Policies Required**

Global Setup Configuration

1. Access DefensePro via **APSolute Vision**.
2. Select the DefensePro **Configuration** perspective

3. In the **Setup** section, select **Security Settings**
4. In the **BDoS Protection** tab, verify that **Enable BDoS Protection** checkbox is checked
5. For **Learning Response Period** select: **Day**

Update Policies Operations

BDoS Protection*

☒ Enable BDoS Protection

Learning Response Period:

☒ Enable Traffic Statistics Sampling

☒ Enable Overblocking Prevention

Advanced Parameters

ADVANCED PARAMETERS

Duration of Non-Attack Traffic in Blocking State:

Duration of Non-Attack Traffic in Anomaly or Non-Strictness State:

[Reset BDoS Baseline](#)


These settings are for lab configuration; for other environments different setups may be required.

6. Click **Submit** button to save changes.

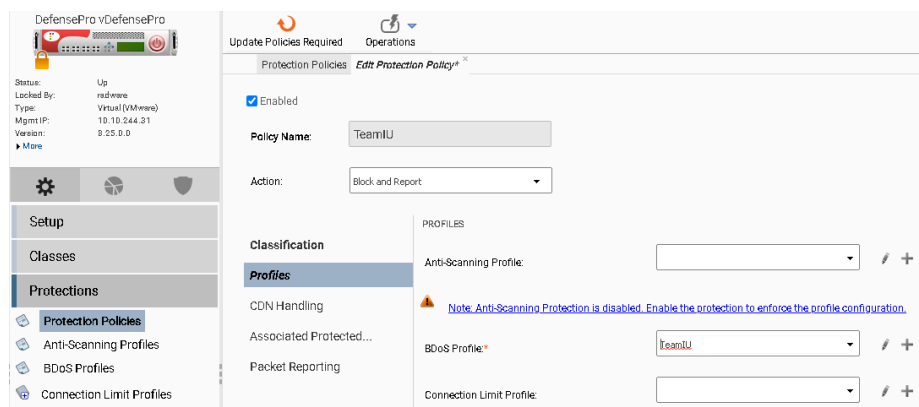
Create BDoS Profile

1. Select the **Configuration** perspective.
2. In **Protections** section, select **BDoS Profiles** in the navigation tree.
3. In **BDoS Profiles** tab, click **Add** to add profile.
4. In the **Add New BDoS Profile** tab, type the **Profile Name**: **TeamXX** (where XX are your initials)
5. Check **Select All Flood Protection Types** checkbox; for other installations select the protection types according to need.

6. Select **Bandwidth Settings** section and set **Inbound Traffic** and **Outbound Traffic** to **5000 Kbps**. Always use the same Kbps settings for both inbound and outbound if not instructed otherwise by the ERT team.

7. In **Quota Settings** section click **Revert to Default Quotas** button.
 Default values are filled in the **Quota** fields. Keep values of all other sections as default.
8. **Advanced Settings** now allows to determine footprint strictness per policy.
9. Click **Submit** button to accept configuration settings.

10. Add the created BDoS to **Protection Policies**. In **Protection Policies** select the existing policy (TeamXX) and add your BDoS profile at profiles.



11. Click **Submit**
12. Click on **Update Policies Required** button for activation. Wait for completion.
13. Open **Alerts Table** and watch changes.

Test and Monitor the Configuration

Open the Attacker machine and send a TCP Flood Attack.

1. Access **Attacker-PC** select and use the **Raptor Attacker** to launch attacks. Once window is selected you can use your mouse or cursor arrow to navigate. Confirm by pressing **↵** or click on **<Select>** or **<OK>** buttons
2. Select **Network Attacks** → **Floods** → **Single Source** → **TCP** → **SYN Attack**.
3. Verify Destination IP address: **27.1.31.100** then **<OK>**
4. Window eth0 at Attack-PC display now outgoing traffic (TX) from the vDP.

After the attack is initiated from the Attack-PC, you should see traps in the CLI/Syslog.

To view traps,

1. Open **vDP_Serial** tab in mRemoteNG.

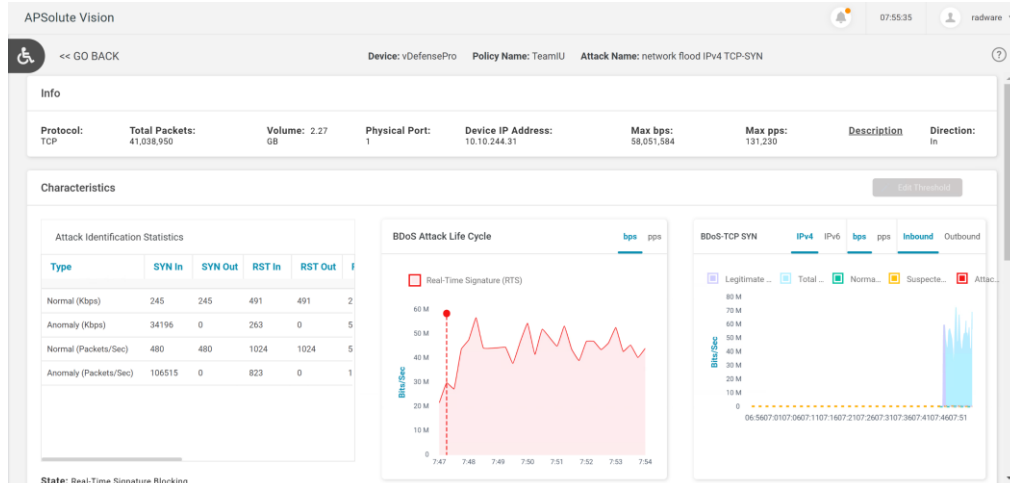
```

drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:02 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 140.11.19.118 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled 1
drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:02 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 30.192.105.143 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled
drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:02 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 40.140.147.84 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled 1
drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:02 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 72.31.162.146 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled 1
drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:02 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 0.0.0.0 31337 27.1.31.100 80 1 Regular "NWRule_Team31" ongoing 3144905
high drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:17 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 165.78.225.133 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled
drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:17 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 96.94.153.182 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled 1
drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F
7:17 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP 155.191.188.177 31337 27.1.31.100 80 1 Regular "NWRule_Team31" sampled
high drop FFFFFFFF-FFFF-FFFF-0029-00005E1B491F

```

2. In APSolute Vision, select the **Analytics AMS** → **DefensePro Monitoring** perspective.
3. Explore the **DefensePro Monitoring** page.

4. Select your policy in **Protection Policies** section.
5. Explore the DefensePro Dashboard.
6. Select the TeamXX policy in **Protection Policies** section.
7. Select the **Behavioral DoS** in the **Protections** section.
8. Select an ongoing attack from the list.
9. Explore the attack characteristics such as **Attack Identification Statistics**, **Real-Time Signature** (footprint), attack graph etc.
10. In **Dashboard View** section, select **Current Attacks Table** and then **Ongoing Attacks Monitor**.



11. Click on the red dot in BDoS Attack Life Cycle graph to show Real-Time Signature (RTS)

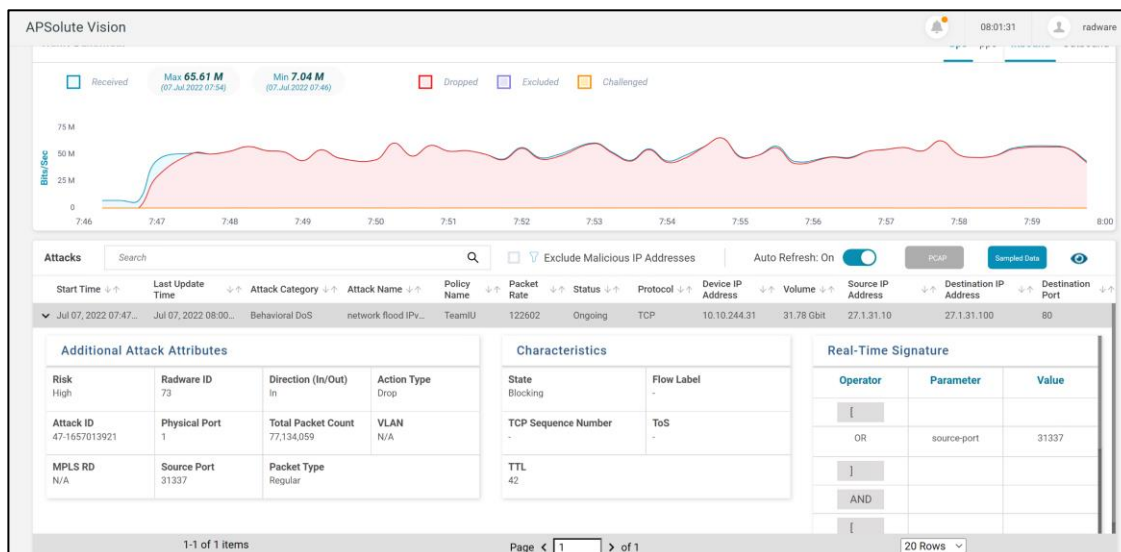
Real-Time Signature



Operator	Parameter	Value/s
[
OR	source-port	31337
]		
AND		
[
AND	packet-size	54
AND	destination-port	80
AND	destination-ip	27.1.31.100
AND	ttd	42
]		

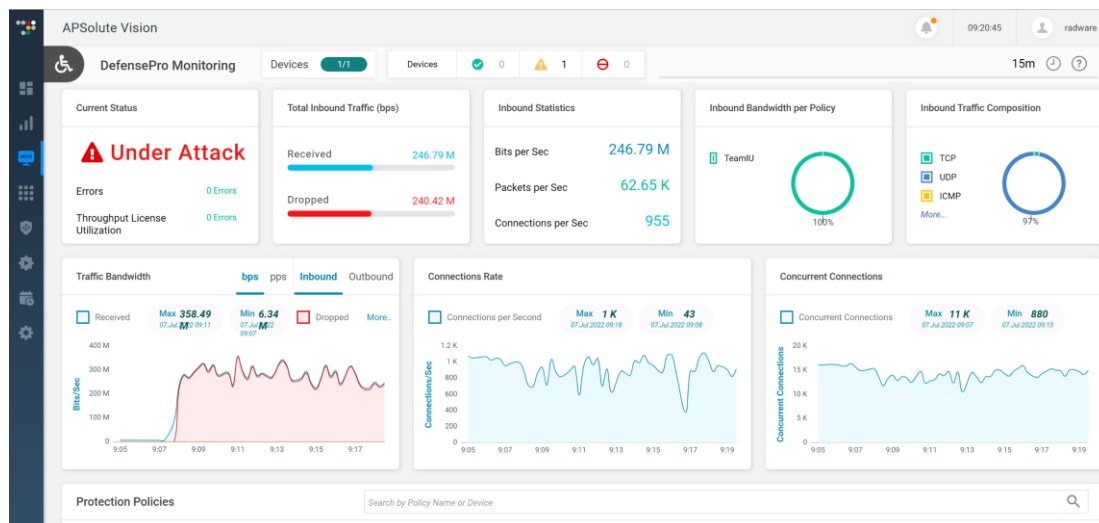
12. Click **Go Back** button to go back to the **DefensePro Dashboard**.

13. In **Analytics AMS** select **DefensePro Attacks**. Click on the attack and explore the screen.



Use Raptor to send an UDP Flood Attack

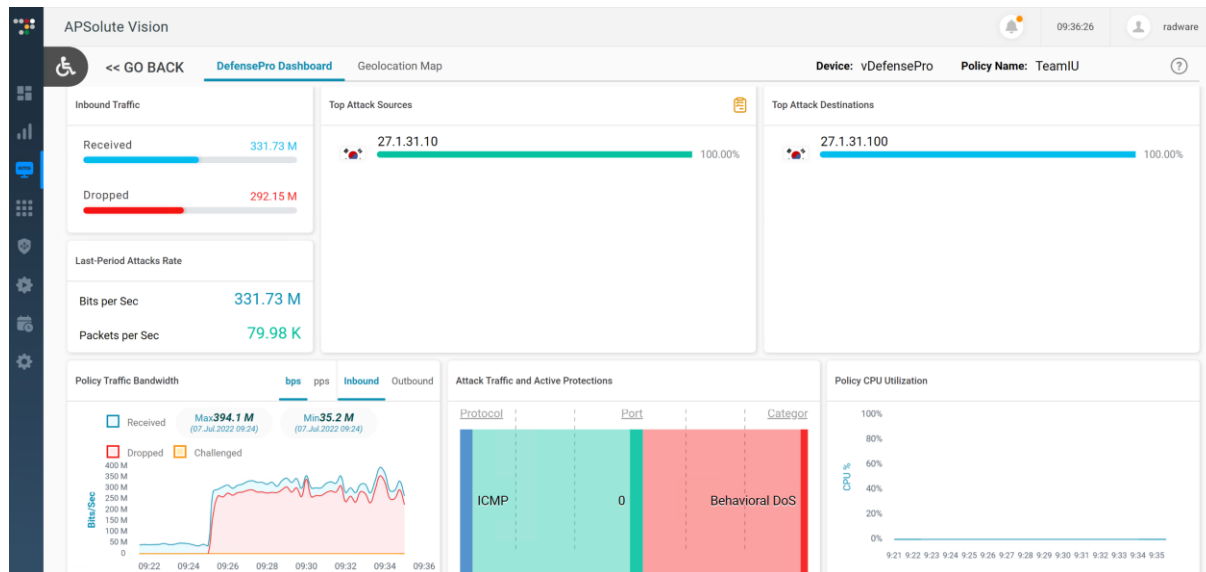
1. Access Attacker-PC Raptor main menu and select **Network Attacks** → **Floods** → **Single Source** → **UDP** → **Data Flood**.
2. Verify Destination IP address: **27.1.31.100**
Soon after the attack is initiated from the Attack-PC, you'll see traps in the CLI/Syslog.
3. Wait a few minutes. Click **Stop** button.
4. Use Vision to View UDP Flood Attack.
 - a. Select the **Analytics AMS** → **DefensePro Monitoring** and explore the new attack.



Use Raptor to Send ICMP Flood Attack.

1. Access Attacker-PC Raptor main menu and select **Network Attacks** → **Floods** → **Single Source** → **ICMP** → **Echo Request Flood**.
2. In Vision monitor the attack details as already done for the TCP and UDP floods.

- a. To see more details click on the policy with the symbol and you can drill down to see all the attack information



Do not forget to stop the attack after completing this lab.

Export and save configuration file. After the file is saved, change the name to **dp8-BDosLab-config**



For questions, contact training@Radware.com

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.