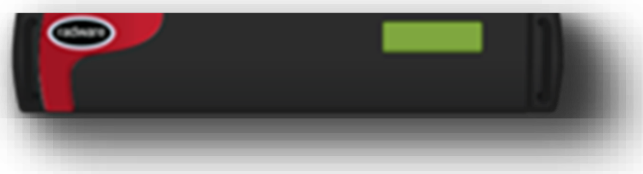
radware

DefensePro X
Version 10.x

# Training Lab Manual
# Configure BDoS



# Table of Contents

## Contents

# Objectives

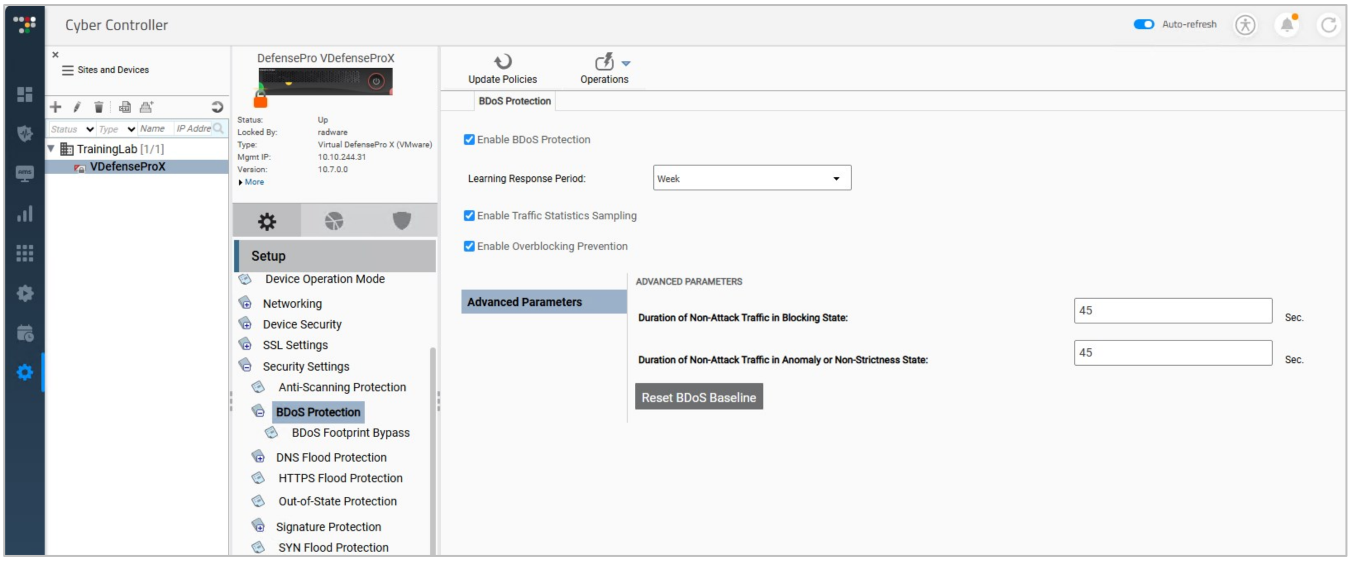
After reviewing the BDoS training module and completing this lab, you should be able to configure and monitor Behavioral DoS (BDoS) protection.

## 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.

# Global Setup Configuration

1. Access DefensePro via **Cyber Controller**.
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: ***Week***



Status: Up
Locked By: radware
Type: Virtual DefensePro X (VMware)
Mgmt IP: 10.10.244.31
Version: 10.7.0.0

☑ Enable BDoS Protection

Learning Response Period: Week

☑ Enable Traffic Statistics Sampling

☑ Enable Overblocking Prevention

ADVANCED PARAMETERS

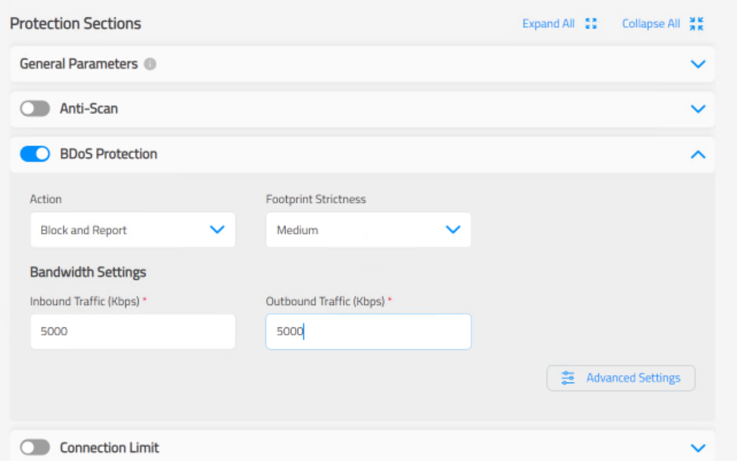
Duration of Non-Attack Traffic in Blocking State: 45 Sec.

Duration of Non-Attack Traffic in Anomaly or Non-Strictness State: 45 Sec.

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

# Edit BDoS Protection

1. Select the **Security Operations** in Cyber Controller.
2. Highlight existing **TeamXX** policy and click **pencil** icon to edit.
3. Expand the **BDoS Protection** and edit the inbound and outbound traffic to **5000 Kbps.**



Protection Sections — Expand All — Collapse All

General Parameters

○ Anti-Scan

● BDoS Protection

Action: Block and Report

Footprint Strictness: Medium

Bandwidth Settings

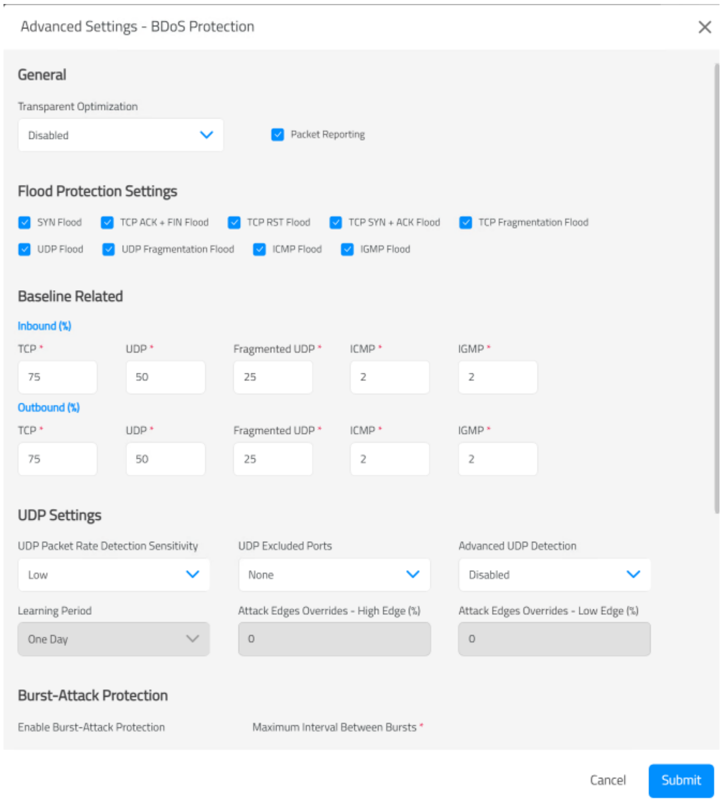
Inbound Traffic (Kbps) *: 5000

Outbound Traffic (Kbps) *: 5000

Advanced Settings

○ Connection Limit

4. Click on **Advance Settings**. Review the settings. There is no need to change the defaults in this lab.



Advanced Settings - BDoS Protection

General

Transparent Optimization: Disabled

☑ Packet Reporting

Flood Protection Settings

☑ SYN Flood ☑ TCP ACK + FIN Flood ☑ TCP RST Flood ☑ TCP SYN + ACK Flood ☑ TCP Fragmentation Flood

☑ UDP Flood ☑ UDP Fragmentation Flood ☑ ICMP Flood ☑ IGMP Flood

Baseline Related

| | TCP * | UDP * | Fragmented UDP * | ICMP * | IGMP * |
|---|---|---|---|---|---|
| Inbound (%) | 75 | 50 | 25 | 2 | 2 |
| Outbound (%) | 75 | 50 | 25 | 2 | 2 |

UDP Settings

UDP Packet Rate Detection Sensitivity: Low

UDP Excluded Ports: None

Advanced UDP Detection: Disabled

Learning Period: One Day

Attack Edges Overrides - High Edge (%): 0

Attack Edges Overrides - Low Edge (%): 0

Burst-Attack Protection

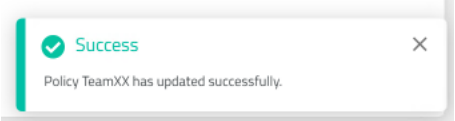
Enable Burst-Attack Protection

Maximum Interval Between Bursts *

Cancel Submit

5. Click **Submit** in **Advanced Settings** and **Submit** again in the **Edit Policy**.

6. You should see a Success message in the bottom right.



Success

Policy TeamXX has updated successfully.

7. Open **Alerts Table** and watch changes.

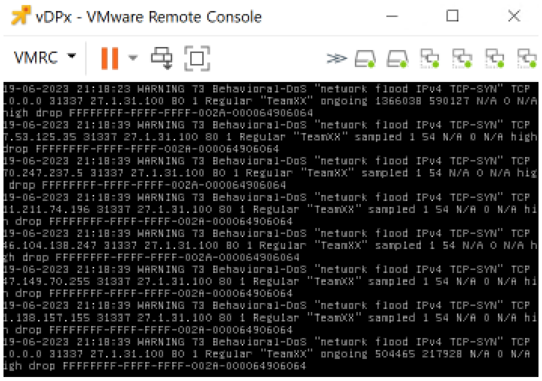
# Test and Monitor the Configuration

## 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 → Multiple Sources → 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.

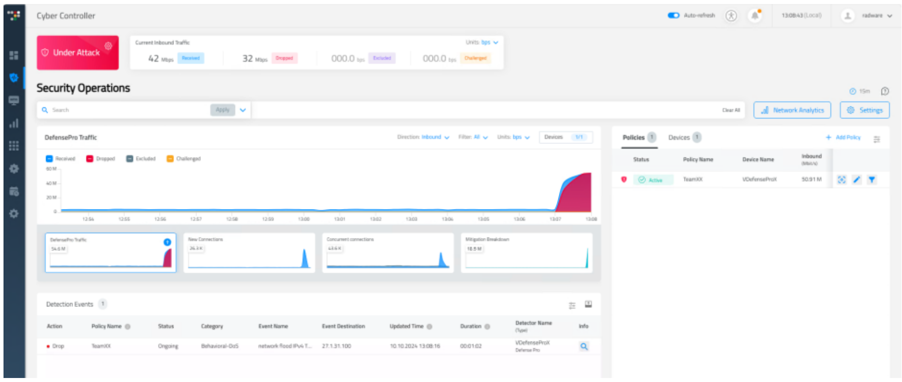
After the attack is initiated from the Attack-PC, you should see traps in the CLI/Syslog.
To view traps,

1. Open **vDP Console** tab in mRemoteNG.



```
19-06-2023 21:18:23 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
10.0.0 31337 27.1.31.100 80 1 Regular "TeamXX" ongoing 1366038 590127 N/A 0 N/A
high drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
7.53.125.35 31337 27.1.31.100 80 1 Regular "TeamXX" sampled 1 54 N/A 0 N/A high
drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
70.247.237.5 31337 27.1.31.100 80 1 Regular "TeamXX" sampled 1 54 N/A 0 N/A hig
 drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
11.211.74.196 31337 27.1.31.100 80 1 Regular "TeamXX" sampled 1 54 N/A 0 N/A hi
h drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
46.104.138.247 31337 27.1.31.100 80 1 Regular "TeamXX" sampled 1 54 N/A 0 N/A h
gh drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
47.149.70.255 31337 27.1.31.100 80 1 Regular "TeamXX" sampled 1 54 N/A 0 N/A hi
h drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
1.138.157.155 31337 27.1.31.100 80 1 Regular "TeamXX" sampled 1 54 N/A 0 N/A hi
h drop FFFFFFFF-FFFF-FFFF-002A-000064906064
19-06-2023 21:18:39 WARNING 73 Behavioral-DoS "network flood IPv4 TCP-SYN" TCP
10.0.0 31337 27.1.31.100 80 1 Regular "TeamXX" ongoing 504465 217928 N/A 0 N/A
igh drop FFFFFFFF-FFFF-FFFF-002A-000064906064
```

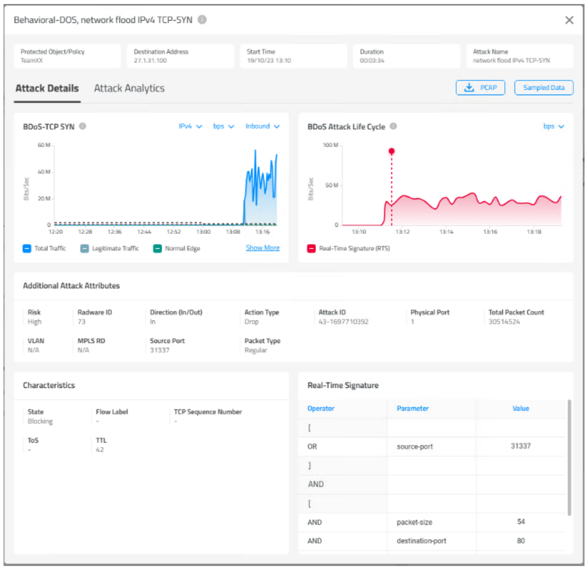
2. In Cyber Controller, select the **Security Operations → Real-Time Monitoring** perspective.
3. Explore the **Real-Time Monitoring** page.



| Status | Policy Name | Device Name | Inbound (Mbit/s) |
|---|---|---|---|
| Active | TeamXX | VDefenseProX | 50.91 M |

| Action | Policy Name | Status | Category | Event Name | Event Destination | Updated Time | Duration | Detector Name (Type) | Info |
|---|---|---|---|---|---|---|---|---|---|
| Drop | TeamXX | Ongoing | Behavioral-DoS | network flood IPv4 T... | 27.1.31.100 | 10.10.2024 13:08:16 | 00:01:02 | VDefenseProX<br>Defense Pro | |

4. Select the attack in **Detection Events** section and click on the maginfying glass/info icon.



Behavioral-DOS, network flood IPv4 TCP-SYN

Protected Object/Policy: TeamXX
Destination Address: 27.1.31.100
Start Time: 19/10/23 13:10
Duration: 00:03:34
Attack Name: network flood IPv4 TCP-SYN

Additional Attack Attributes

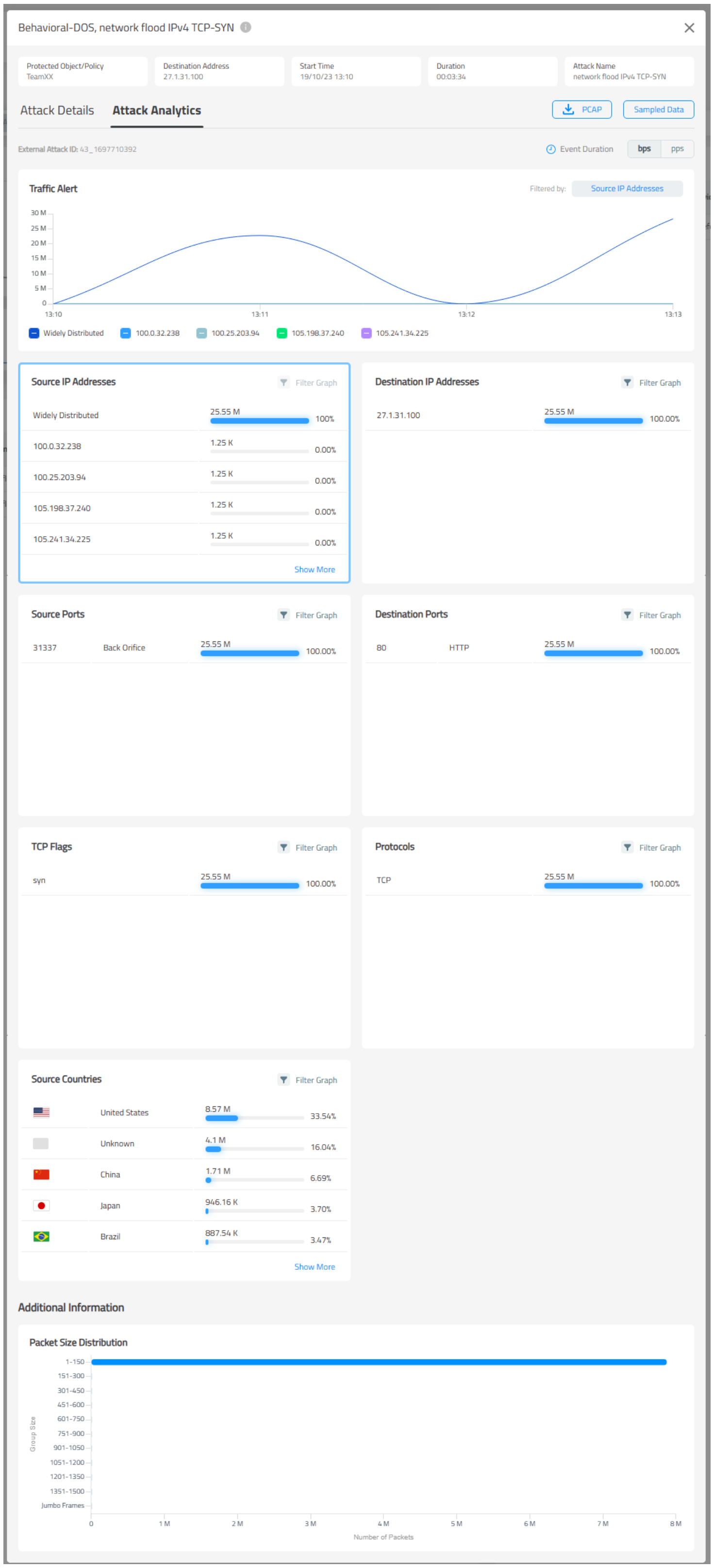
Risk: High
Radware ID: 73
Direction (In/Out): In
Action Type: Drop
Attack ID: 43-1697710392
Physical Port: 1
Total Packet Count: 30514524
VLAN: N/A
MPLS RD: N/A
Source Port: 31337
Packet Type: Regular

Characteristics

State: Blocking
Flow Label: -
TCP Sequence Number: -
ToS: -
TTL: 42

Real-Time Signature

| Operator | Parameter | Value |
|---|---|---|
| [ | | |
| OR | source-port | 31337 |
| ] | | |
| AND | | |
| [ | | |
| AND | packet-size | 54 |
| AND | destination-port | 80 |



Behavioral-DOS, network flood IPv4 TCP-SYN

Protected Object/Policy: TeamXX
Destination Address: 27.1.31.100
Start Time: 19/10/23 13:10
Duration: 00:03:34
Attack Name: network flood IPv4 TCP-SYN

External Attack ID: 43_1697710392

Source IP Addresses

| | | |
|---|---|---|
| Widely Distributed | 25.55 M | 100% |
| 100.0.32.238 | 1.25 K | 0.00% |
| 100.25.203.94 | 1.25 K | 0.00% |
| 105.198.37.240 | 1.25 K | 0.00% |
| 105.241.34.225 | 1.25 K | 0.00% |

Destination IP Addresses

| | | |
|---|---|---|
| 27.1.31.100 | 25.55 M | 100.00% |

Source Ports

| | | | |
|---|---|---|---|
| 31337 | Back Orifice | 25.55 M | 100.00% |

Destination Ports

| | | | |
|---|---|---|---|
| 80 | HTTP | 25.55 M | 100.00% |

TCP Flags

| | | |
|---|---|---|
| syn | 25.55 M | 100.00% |

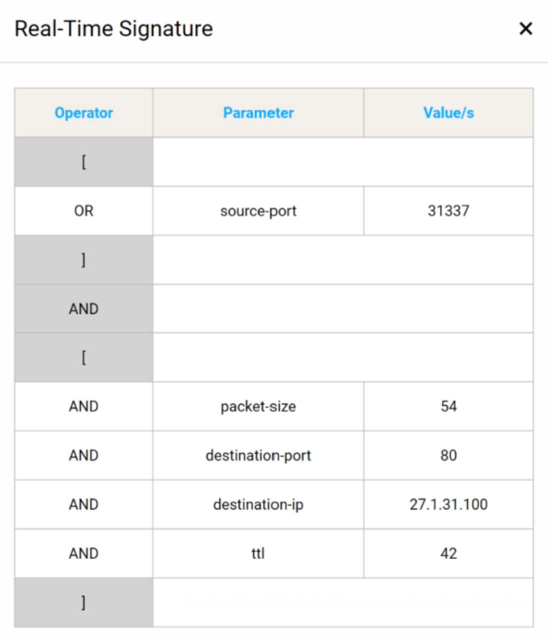
Protocols

| | | |
|---|---|---|
| TCP | 25.55 M | 100.00% |

Source Countries

| | | |
|---|---|---|
| United States | 8.57 M | 33.54% |
| Unknown | 4.1 M | 16.04% |
| China | 1.71 M | 6.69% |
| Japan | 946.16 K | 3.70% |
| Brazil | 887.54 K | 3.47% |

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

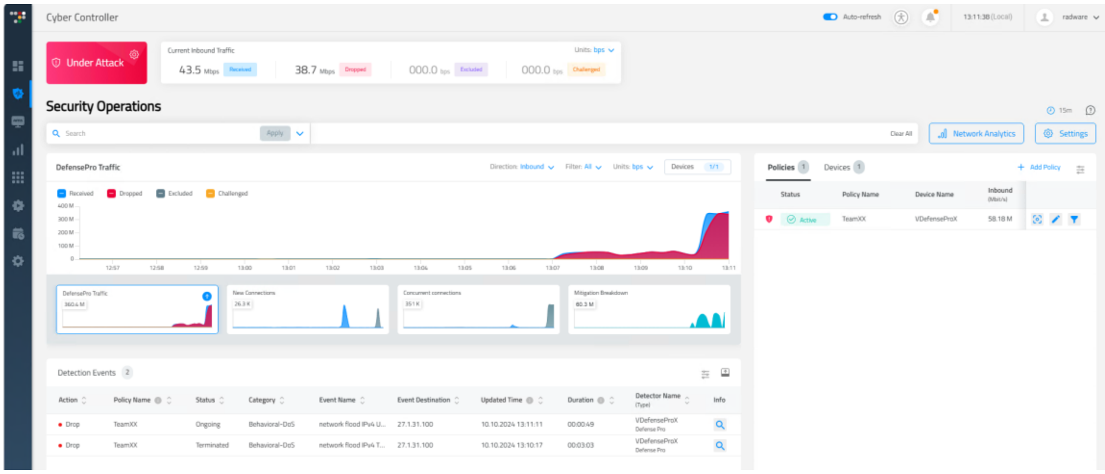


Real-Time Signature ✕

| 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 | ttl | 42 |
| ] | | |

## Use Raptor to send an UDP Flood Attack

1. Access Attacker-PC Raptor main menu.
2. Stop the current TCP SYN Attack.
3. Select **Network Attacks → Floods → Multiple Sources → UDP → Data Flood**.
4. 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.
5. Wait a few minutes. Click **Stop** button.
6. Use Cyber Controller to View UDP Flood Attack.
   a. Select the **Security Operations → Real-Time Monitoring** and explore the new attack.



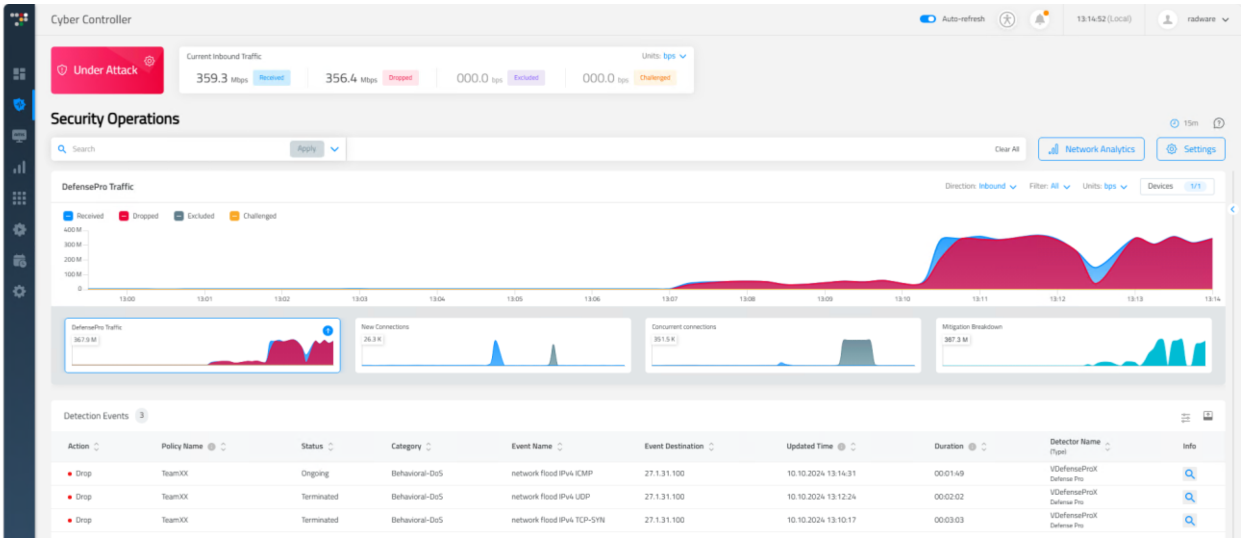
| Status | Policy Name | Device Name | Inbound (Mbit/s) |
|---|---|---|---|
| Active | TeamXX | VDefenseProX | 58.18 M |

Detection Events 2

| Action | Policy Name | Status | Category | Event Name | Event Destination | Updated Time | Duration | Detector Name (Type) | Info |
|---|---|---|---|---|---|---|---|---|---|
| ● Drop | TeamXX | Ongoing | Behavioral-DoS | network flood IPv4 U... | 27.1.31.100 | 10.10.2024 13:11:11 | 00:00:49 | VDefenseProX<br>Defense Pro | |
| ● Drop | TeamXX | Terminated | Behavioral-DoS | network flood IPv4 T... | 27.1.31.100 | 10.10.2024 13:10:17 | 00:03:03 | VDefenseProX<br>Defense Pro | |

## Use Raptor to Send ICMP Flood Attack.

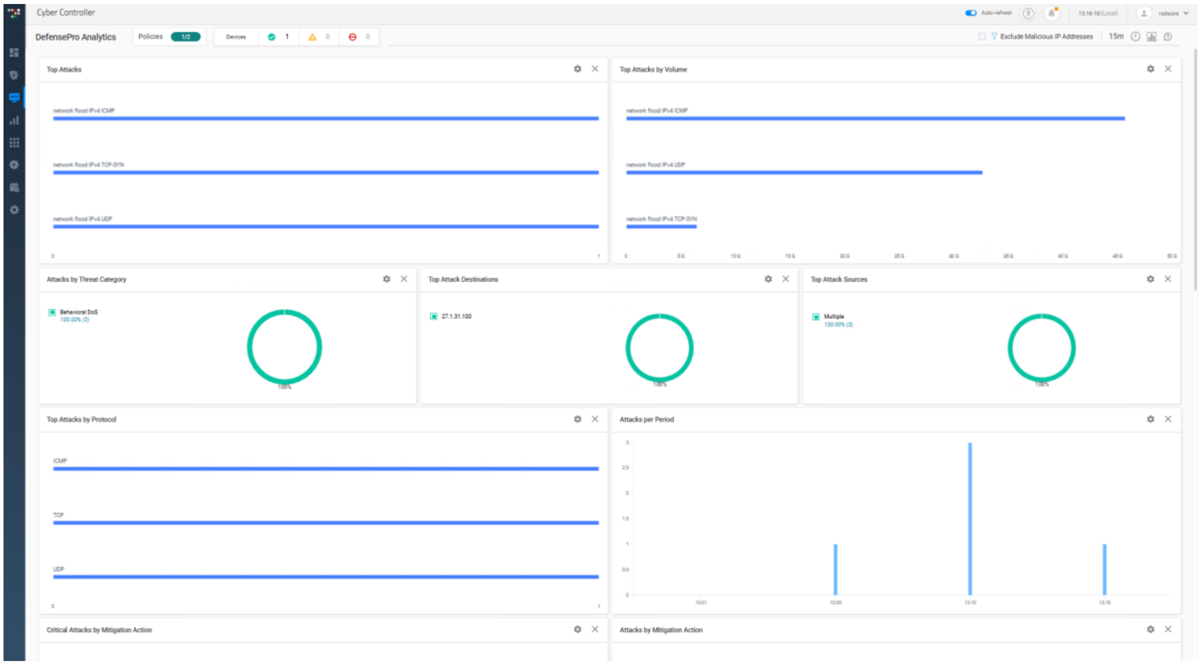
1. Access Attacker-PC Raptor main menu and select **Network Attacks → Floods → Multiple Sources → ICMP → Echo Request Flood**.
2. Verify Destination IP address: **27.1.31.100**
   Soon after the attack is initiated from the Attack-PC, you'll see traps in the CLI/Syslog.
3. Wait a few minutes. Click **Stop** button.
4. In Cyber Controller monitor the attack details as already done for the TCP and UDP floods.
   a. To see more details click on the event with the and you can drill down to see all the attack information



Detection Events 3

| Action | Policy Name | Status | Category | Event Name | Event Destination | Updated Time | Duration | Detector Name (Type) | Info |
|---|---|---|---|---|---|---|---|---|---|
| ● Drop | TeamXX | Ongoing | Behavioral-DoS | network flood IPv4 ICMP | 27.1.31.100 | 10.10.2024 13:14:31 | 00:01:49 | VDefenseProX<br>Defense Pro | 🔍 |
| ● Drop | TeamXX | Terminated | Behavioral-DoS | network flood IPv4 UDP | 27.1.31.100 | 10.10.2024 13:12:24 | 00:02:02 | VDefenseProX<br>Defense Pro | 🔍 |
| ● Drop | TeamXX | Terminated | Behavioral-DoS | network flood IPv4 TCP-SYN | 27.1.31.100 | 10.10.2024 13:10:17 | 00:03:03 | VDefenseProX<br>Defense Pro | 🔍 |

5. Explore the **Analytics AMS → DefensePro Analytics** dashboard.



6. **Do not forget to stop the attack after completing this lab.**
7. Save the configuration as **dpX-BDOSLab-config**.

radware

For questions, contact training@Radware.com