radware

DefensePro X
Version 10.x

Training Lab Manual
Administration

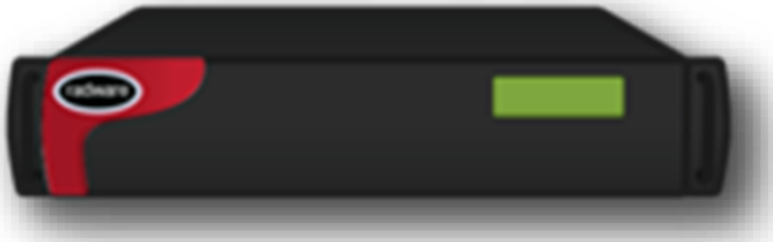


Table of Contents

Contents

Administration

Overview

Radware DefensePro X labs are maintained and kept up to date by Radware lab managers. This lab introduces DefensePro device administration for information only.

Exercises in this lab are viewed from the MONITORING and CONFIGURATION perspectives.

After reviewing these lab exercises, retain the information for future use.

Updating DefensePro X Software Version

Since the device is already upgraded to the version of the lab manual, you should not upgrade it and just review the options. If you update the device, the screens can be different than in the lab manual.

1. In **Cyber Controller**, select DefensePro X **Configuration** perspective. Select **Setup → Software Version Management** on the navigation tree. Here you can see the software versions which are on the device. Only one version can be active (see status column). In this table you can also select a different version to be activce, if you do so the DefensePro X will reboot using the selected version with the configuration file, which was active at this version. There will be a popup window to validate that you want to select this version and reboot.
2. To update the software select **Upload Software Version** below the **Software Version Management**
3. In the dialog you have the option to upload the software version and activate it imediately or just upload without activation.
4. Each software version needs a password, which can be generated automatically, if Cyber Controller has access to the internet to validate the support contract of the device, or can be generated on the Radware portal.

View License Informaton

1. In **Cyber Controller**, select DefensePro **Configuration** perspective and select **Setup → Global Parameters → License Upgrade**
2. In the License Upgrade window, you can review the current licenses and update them in case it's needed.
3. NOTE: In our lab we use a virtual DefensePro X, this platform has an additional license called **vCPU license**
   In regular hardware platforms you will only have the **Throughput License**.

Export Configuration Files

1. In **Cyber Controller**, select DefensePro X **Operations → Export Configuration File** to export a configuration file saved on the local client or on the cyber controller server.
2. Select Client and check Include Private Keys to make sure all keys and certificates (WebUI, SSL inspection) will be saved as well. Type **radware** as passphrase and click OK
3. Save the file at a location you remember.

Import Configuration Files

1. **NOTE (optional step)**: If you import a configuration file, the DefensePro X will reboot. It's **not** necessary to import configuration at this step. This is for your reference only.
2. To be able to monitor the reboot process, open the **vDP Console** in **mRemoteNG**
3. In **Cyber Controller**, select DefensePro X **Operations → Import Configuration File** to import a configuration file saved on the local client or on the Cyber Controller server.
4. Select the configuration you saved and don't forget to add the passphrase (**radware**) and click on **Import**
5. On the vDP Console you can now review the boot process. After the proccess is finished the device will be available again in Cyber Controller.
6. You should see a "**Upload File succeed**" yellow message.
7. Click **Close** to close the Import Configuration File window.

Updating The Signature Database

1. Before we do the update, check first which version is currently on the device
2. In Cyber Controller select DefensePro X **Monitoring** perspective. Select **Operational Status → Overview** in the navigation tree and in the Overview window see the **Signature File Update → Radware Signature File Version**
3. In Cyber Controller select DefensePro X **Operations → Update Security Signatures**
4. Signatures can be updated direclty from Radware.com web site, or from a local client. In case Cyber Controller has no access to the internet, the update file can be downloaded from Radware Portal.
5. Keep the defaults and click on **Update** to start the proccess from Radware.com
6. You should get a succeed message after the update is finished.
7. Click on **Close** to close the Update Security Signatures window.
8. Repeat step 2 to see the current version.

Using the Scheduler

1. Cyber Controller has the **Scheduler** to automate some recuring tasks.
2. The first task we add, is to daily update the attack description file for the Signature protection to make sure each time a new attack is added in the attack details window we can see the details.
3. In the left menu select the **Scheduler** icon 📅
4. Click **+** to add a new Task and use the information as follows:

Parameters	
Task Type	Update Attack Description File
Name	SUS Description File Update
Description	Update Signature Description File
Schedule	Daily
Time	08:00:00

5. Click **Submit** to add the new task
6. The second task we add is to daily update the security signature file

7. Click **+** to add a new Task and use the information as follows:

Parameters	
Task Type	Update Security Signatures Files
Name	SUS File Update
Description	Update Security Signatures
Schedule	Daily
Time	08:05:00
Target Device List	Highlight your device name and use the **>** button to add it to the Selected Device list

8. Click **Submit** to add the new task

9. The third task we add is a weekly backup of the configuration file
10. Click **+** to add a new Task and use the information as follows:

Parameters	
Task Type	Device Configuration Backup
Name	Configuration Backup
Description	Backup DefensePro X
Schedule	Weekly
Time	09:00:00
Day	Select **Sunday**
Parameters	Select **Include Private Keys** Pasphrase: **radware**
Destination	Cyber Controller Server
Target Device List	Highlight your device name and use the > button to add it to the Selected Device list

11. Click **Submit** to add the new task
12. You can start an task at every time by highlighting the Task and use the **Run Now** ➤ button
13. For each task you can see the last execution date and status
14. Run each task and check that all tasks finished successfully.

Exporting A TechSupport File

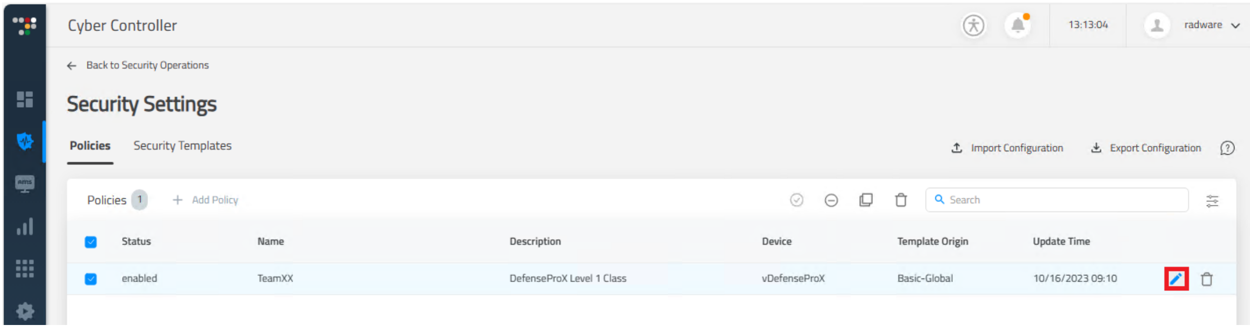
1. In **Cyber Controller**, select DefensePro X **Configurartion** perspective and select **Operations → Export Technical Support File** to create and export a technical support file, which is often need to open a support case.
2. Save the file at a location you remember or open it direclty to review it's content.

Interface Walkthrough

We will modify a basic policy to demonstrate the Cyber Controller Interface.

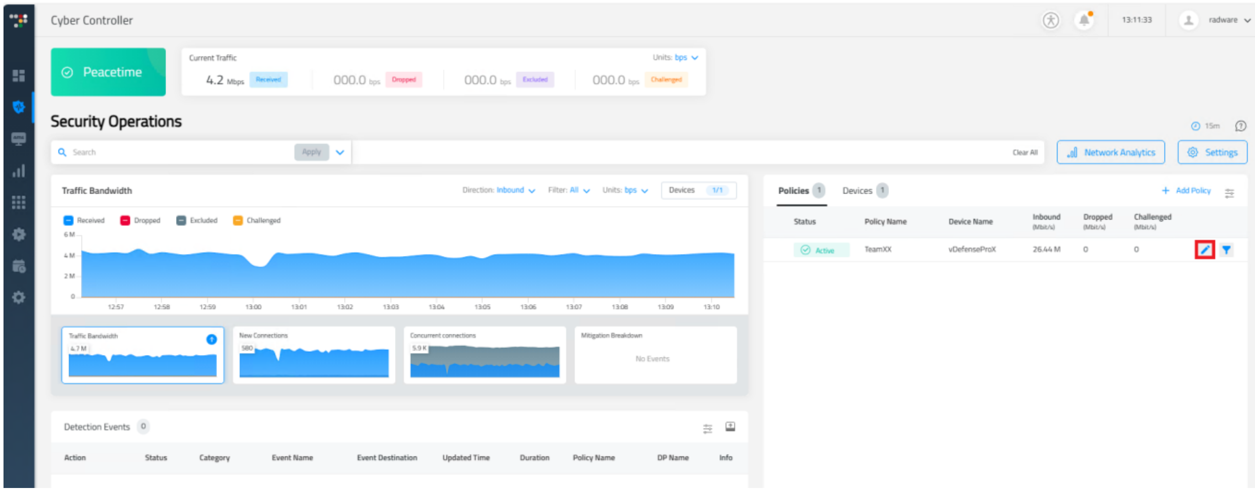
Modify a base policy

To modify a base policy we created in a previous lab, go to **Security Operations → Security Settings →** select **TeamXX** policy you created and click on edit (pencil) icon.



	Status	Name	Description	Device	Template Origin	Update Time
☑	enabled	TeamXX	DefenseProX Level 1 Class	vDefenseProX	Basic-Global	10/16/2023 09:10

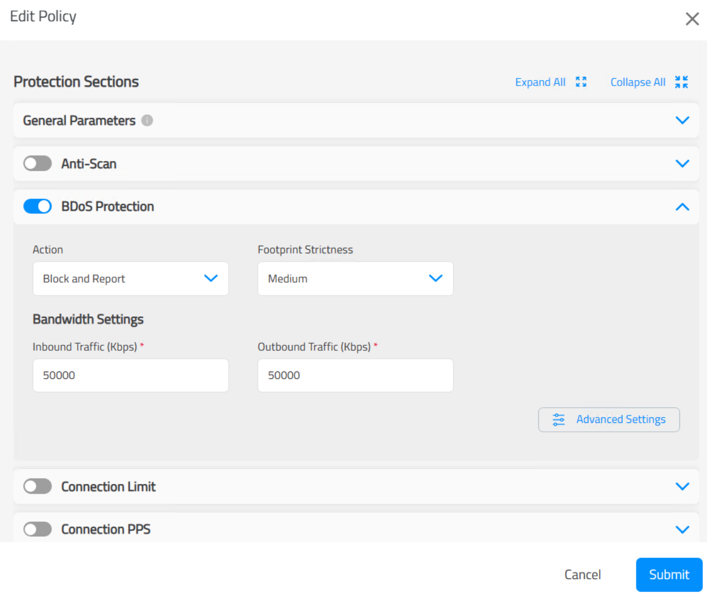
Or use the **Security Operations → Real-Time Monitoring** select **TeamXX** policy you created and click on edit (pencil) icon.



Status	Policy Name	Device Name	Inbound (Mbit/s)	Dropped (Mbit/s)	Challenged (Mbit/s)
Active	TeamXX	vDefenseProX	26.44 M	0	0

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info

Click to enable **BDoS Protection** and keep default settings.



Edit Policy

Protection Sections

General Parameters

Anti-Scan

BDoS Protection

Action: Block and Report

Footprint Strictness: Medium

Bandwidth Settings

Inbound Traffic (Kbps) *: 50000

Outbound Traffic (Kbps) *: 50000

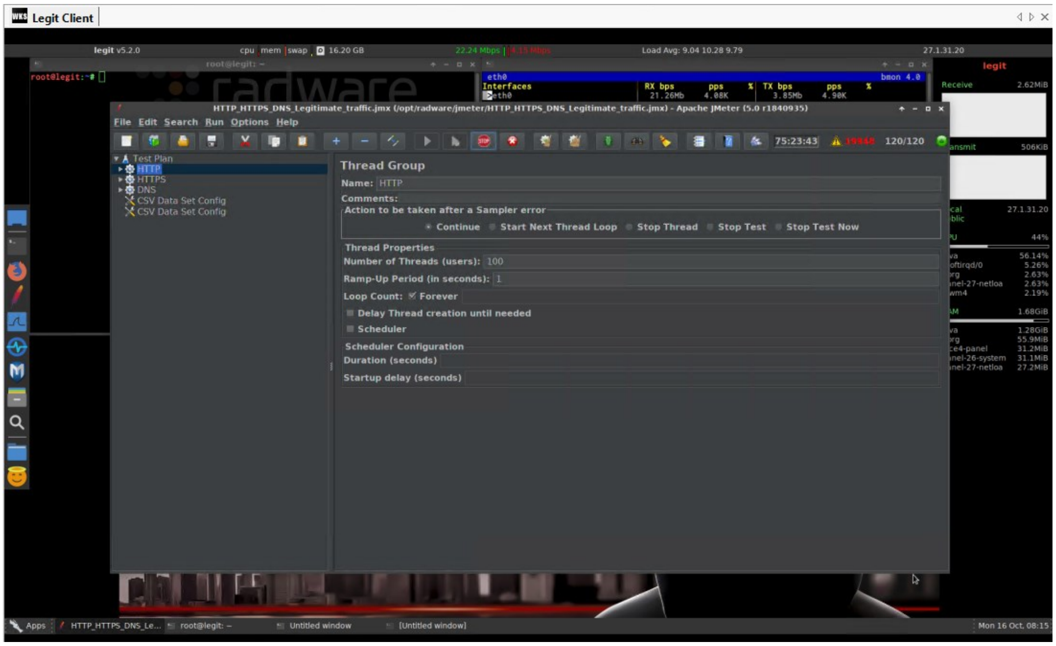
Connection Limit

Connection PPS

Click **Submit**.

Run the baseline traffic

If you haven’t done it already, open the mRemoteNG **Legit Client** from the Connections part of already running mRemoteNG. In the **JMeter** window click on the green play button to start running a legitimate traffic load. Wait a few minutes to see the traffic in the **Real-Time Monitoring**.



HTTP_HTTPS_DNS_Legitimate_traffic.jmx (/opt/radware/jmeter/HTTP_HTTPS_DNS_Legitimate_traffic.jmx) - Apache JMeter (5.0 r1840935)

Test Plan
- HTTP
- HTTPS
- DNS
- CSV Data Set Config
- CSV Data Set Config

Thread Group

Name: HTTP

Comments:

Action to be taken after a Sampler error

● Continue ○ Start Next Thread Loop ○ Stop Thread ○ Stop Test ○ Stop Test Now

Thread Properties

Number of Threads (users): 100

Ramp-Up Period (in seconds): 1

Loop Count: ☑ Forever

□ Delay Thread creation until needed

□ Scheduler

Scheduler Configuration

Duration (seconds)

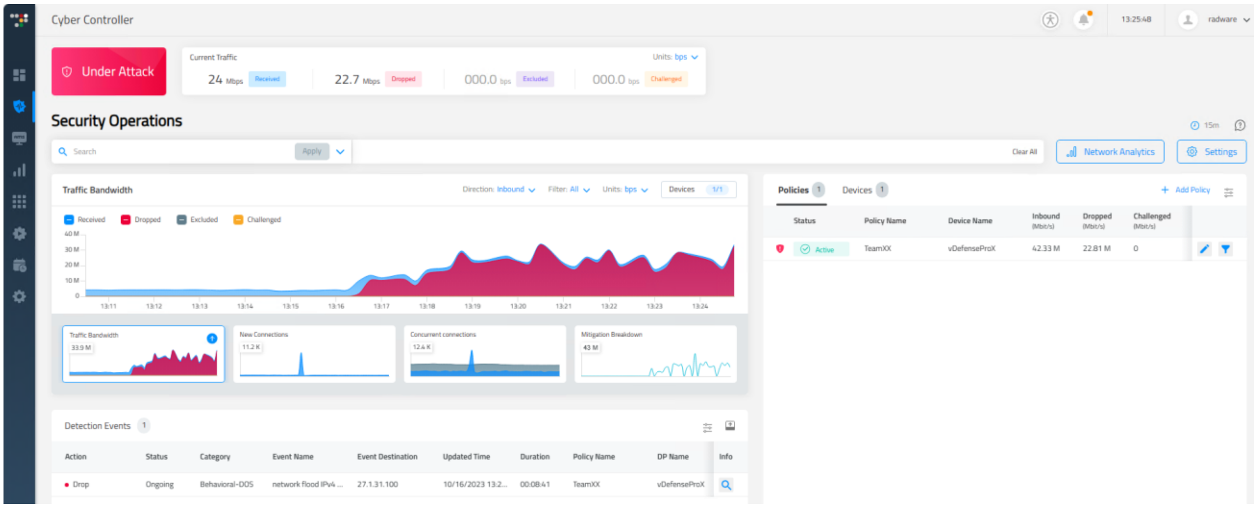
Startup delay (seconds)

```
eth0                                                       bmon 4.0
Interfaces          RX bps       pps     %  TX bps       pps     %
>eth0                21.26Mb     4.08K       3.85Mb      4.90K
```

Run an attack

If you you haven’t done it already, open the mRemoteNG **Attacker** from the Connections part of already running mRemoteNG. In Raptor (blue window) launch an attack **Network Attacks → Floods → Multiple Sources → TCP → RST Attack**. Enter **27.1.31.100** as an attack destination.

Go to Cyber Controller **Security Operations → Real-Time Monitoring**. Explore the GUI.



Current Traffic — Units: bps

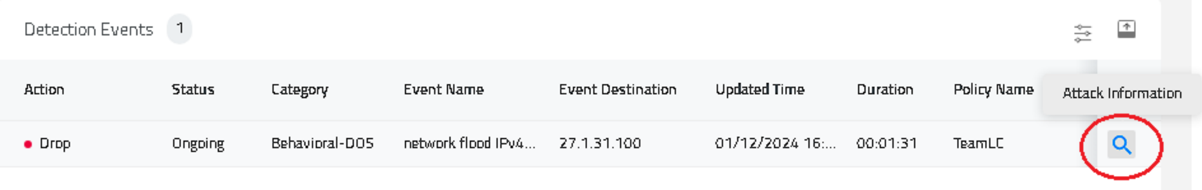
24 Mbps Received | 22.7 Mbps Dropped | 000.0 bps Excluded | 000.0 bps Challenged

Status	Policy Name	Device Name	Inbound (Mbit/s)	Dropped (Mbit/s)	Challenged (Mbit/s)
Active	TeamXX	vDefenseProX	42.33 M	22.81 M	0

Detection Events 1

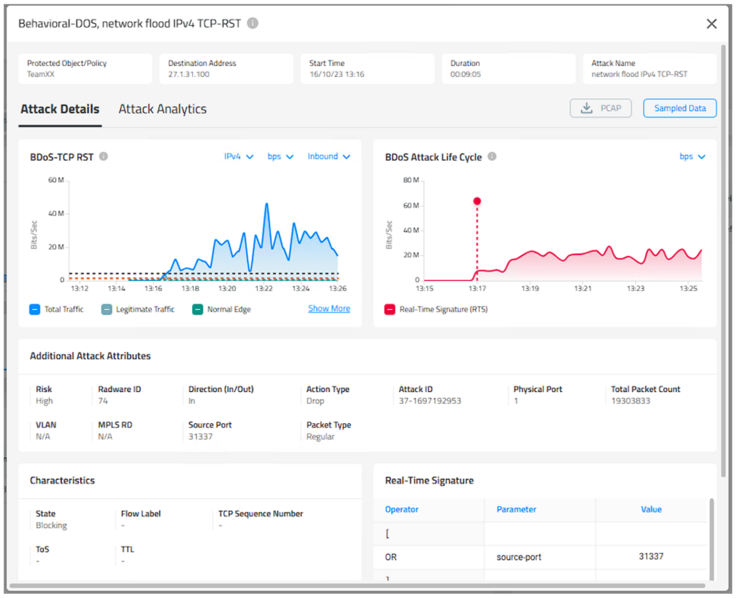
Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
● Drop	Ongoing	Behavioral-DOS	network flood IPv4 ...	27.1.31.100	10/16/2023 13:2...	00:08:41	TeamXX	vDefenseProX	🔍

If the attack is detected use the magnifying glass icon to see the details. Attack Analytics information will be available around two minutes after the attack was detected.



Detection Events 1

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	Attack Information
● Drop	Ongoing	Behavioral-DOS	network flood IPv4...	27.1.31.100	01/12/2024 16:...	00:01:31	TeamLC	🔍



Behavioral-DOS, network flood IPv4 TCP-RST

Protected Object/Policy: TeamXX
Destination Address: 27.1.31.100
Start Time: 16/10/23 13:16
Duration: 00:09:05
Attack Name: network flood IPv4 TCP-RST

Additional Attack Attributes

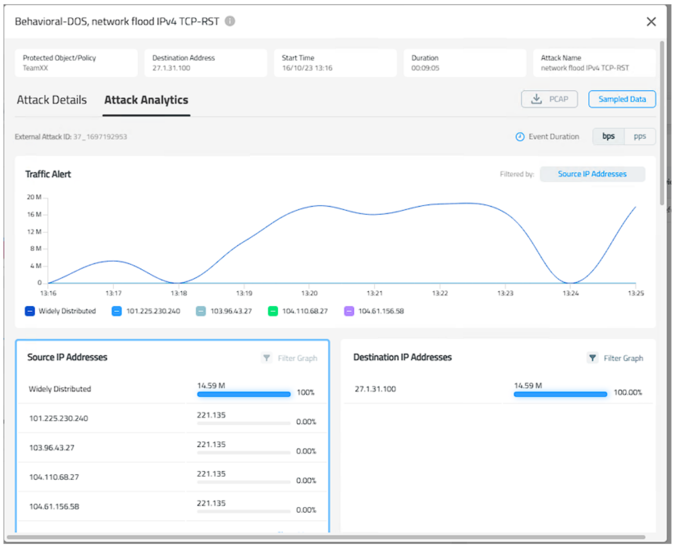
Risk: High
Radware ID: 74
Direction (In/Out): In
Action Type: Drop
Attack ID: 37-1697192953
Physical Port: 1
Total Packet Count: 19303833
VLAN: N/A
MPLS RD: N/A
Source Port: 31337
Packet Type: Regular

Characteristics

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

Real-Time Signature

Operator	Parameter	Value
[		
OR	source-port	31337
]		



Behavioral-DOS, network flood IPv4 TCP-RST

Protected Object/Policy: TeamXX
Destination Address: 27.1.31.100
Start Time: 16/10/23 13:16
Duration: 00:09:05
Attack Name: network flood IPv4 TCP-RST

External Attack ID: 37_1697192953

Source IP Addresses

Widely Distributed	14.59 M	100%
101.225.230.240	221.135	0.00%
103.96.43.27	221.135	0.00%
104.110.68.27	221.135	0.00%
104.61.156.58	221.135	0.00%

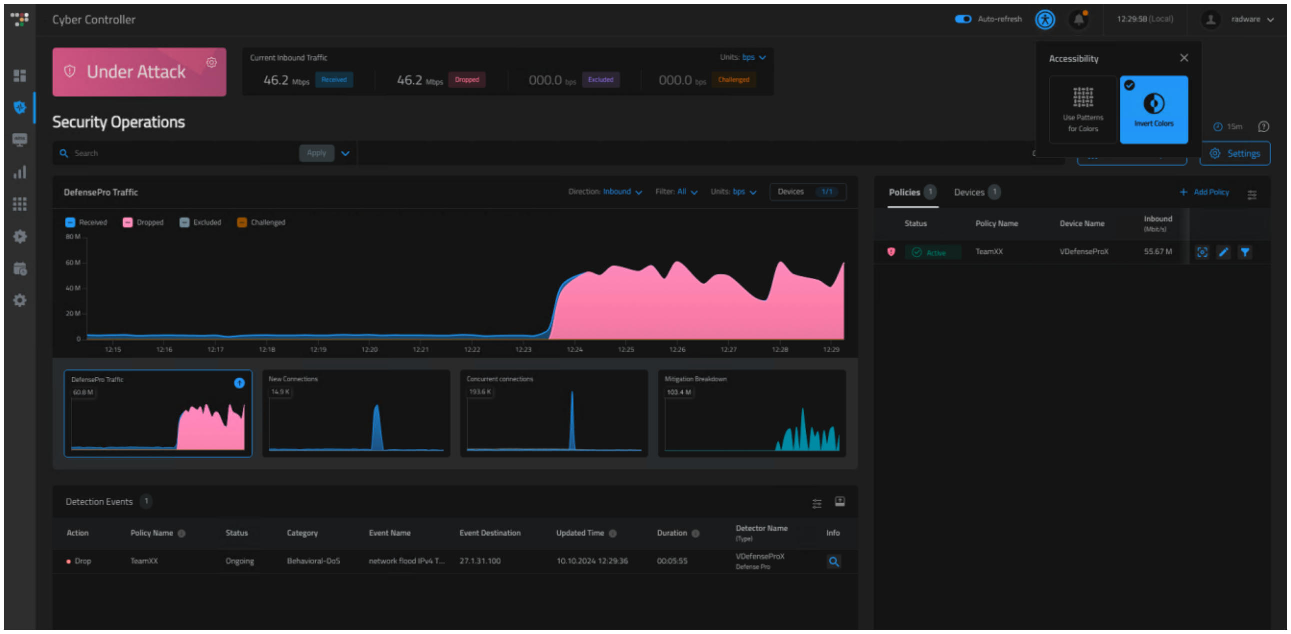
Destination IP Addresses

27.1.31.100	14.59 M	100.00%

Starting Cyber Controller version 10.7 you can also use a dark mode for the user interface.

Click the **Accessibility** ⓘ icon next to the bell symbol and click on **Invert Colors**.

The UI will be in dark mode:



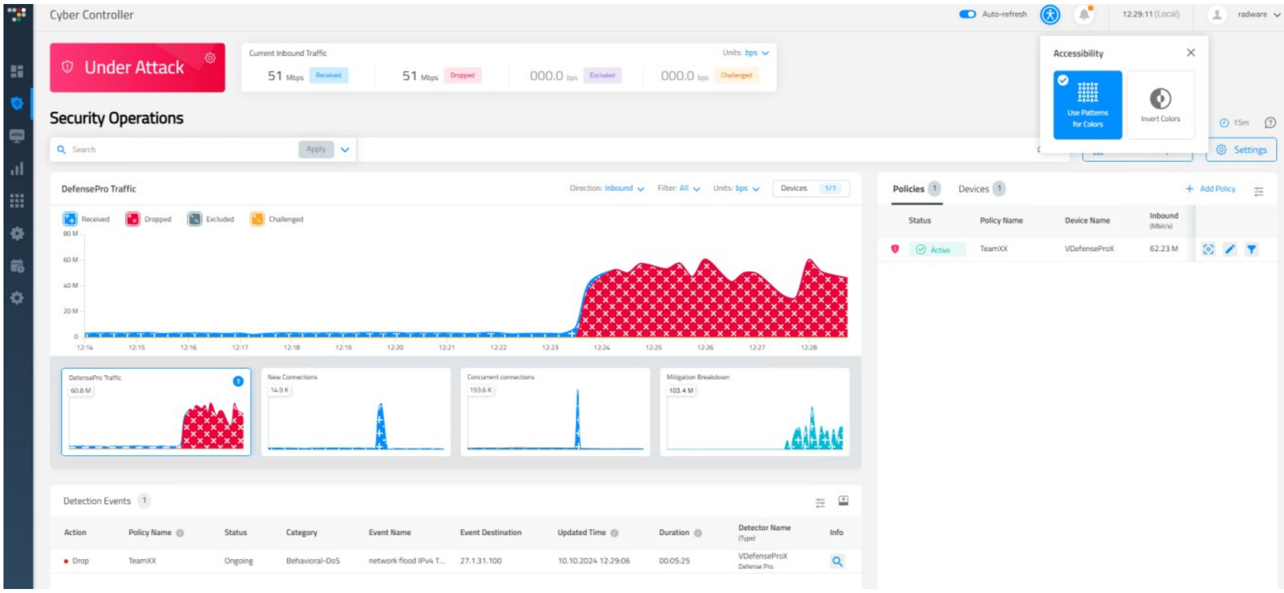
Accessibility: Invert Colors ☑

Status	Policy Name	Device Name	Inbound (Mbit/s)
Active	TeamXX	VDefenseProX	55.67 M

Detection Events 1

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 12:29:36	00:05:55	VDefenseProX Defense Pro	

In addition you can use patterns instead of color, in case you have problems seeing colors:



Accessibility: Use Patterns for Colors ☑

Status	Policy Name	Device Name	Inbound (Mbit/s)
Active	TeamXX	VDefenseProX	62.23 M

Detection Events 1

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 12:29:06	00:05:25	VDefenseProX Defense Pro	

Stop the attack and wait until you see Peacetime on the Security Operations dashboard.

Save the configuration file as ***dpX-Maintenance-config.txt*** in DefensePro X Operations and ***dpX-Maintenance-config.zip*** (in Cyber Controller Security Settings).

For questions, contact training@Radware.com