DefenseProX
Version 10.x

Training Lab Manual
Configure Blocklist and Allowlist

Table of Contents

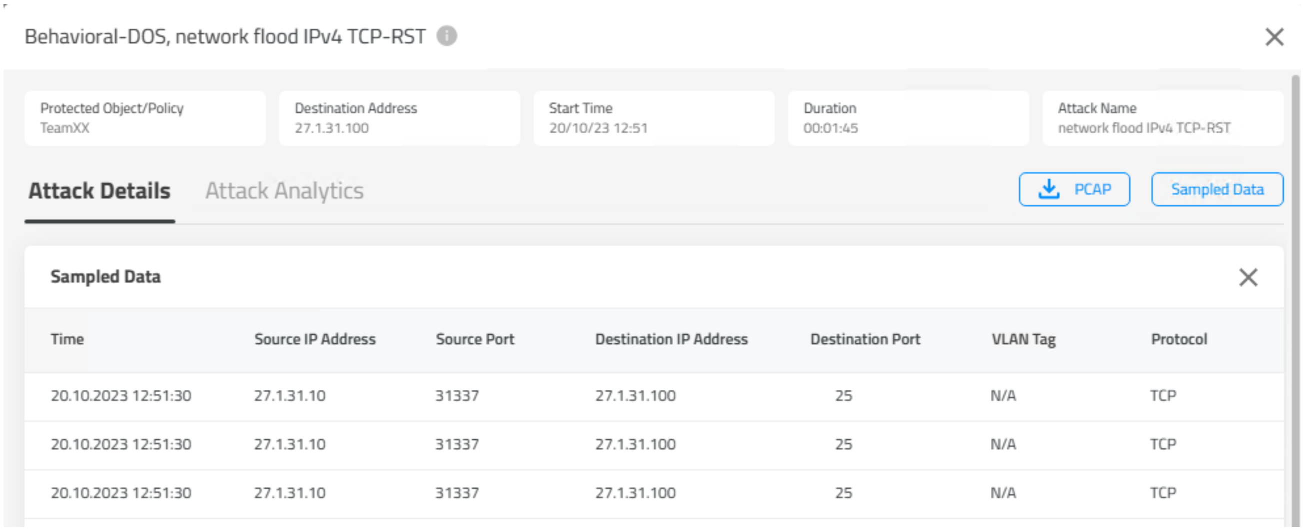
Overview

The Blocklist comprises the traffic that the device always blocks without inspection. You use the Blocklist as policy exceptions for security policies.
The Allowlist determines the traffic that is exempt from DefensePro security inspection.
An Allowlist rule can use explicit values or predefined classes to classify the traffic. The classes are displayed in the Classes tab.

Preparations

In order to prepare for the next exercise, please complete the following:

1. In **Cyber Controller**, select **Security Operations → Security Settings**. Select and edit the TeamXX policy.
2. Enable **BDoS Protection** and click **Submit**.
3. Go to the attacker and launch a TCP RST attack (**Network Attacks → Floods → Single Source → TCP → RST Attacks**, destination **IP 27.1.31.100**)
4. Find out the source IP and destination port of the attack by examining the attack in the **Detection Events**. (In this example it is 27.1.31.10 and 25 respectively, however in your case it might differ).



Behavioral-DOS, network flood IPv4 TCP-RST

Protected Object/Policy: TeamXX
Destination Address: 27.1.31.100
Start Time: 20/10/23 12:51
Duration: 00:01:45
Attack Name: network flood IPv4 TCP-RST

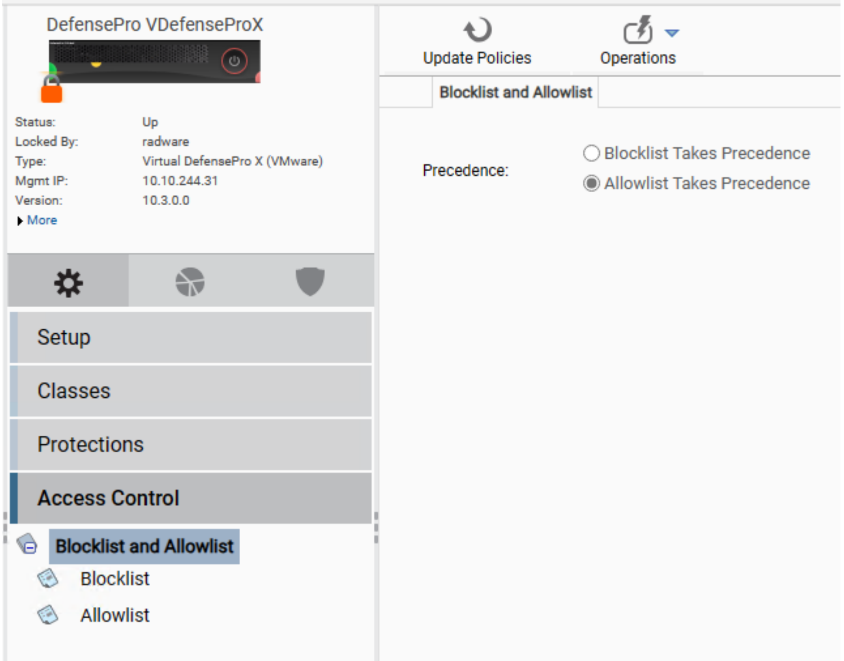
Sampled Data

Time	Source IP Address	Source Port	Destination IP Address	Destination Port	VLAN Tag	Protocol
20.10.2023 12:51:30	27.1.31.10	31337	27.1.31.100	25	N/A	TCP
20.10.2023 12:51:30	27.1.31.10	31337	27.1.31.100	25	N/A	TCP
20.10.2023 12:51:30	27.1.31.10	31337	27.1.31.100	25	N/A	TCP

Setup Blocklist and Allowlist

Block- and Allowlists are not part of the Cyber Controller protection policy and will be configured at the Access List part of the system configuration.

1. Select the **Configuration** perspective.
2. In **Access Control → Blocklist and Allowlist** select which one takes precencense.
3. By default **Default Allowlist Takes Precedence**.



Status: Up
Locked By: radware
Type: Virtual DefensePro X (VMware)
Mgmt IP: 10.10.244.31
Version: 10.3.0.0
More

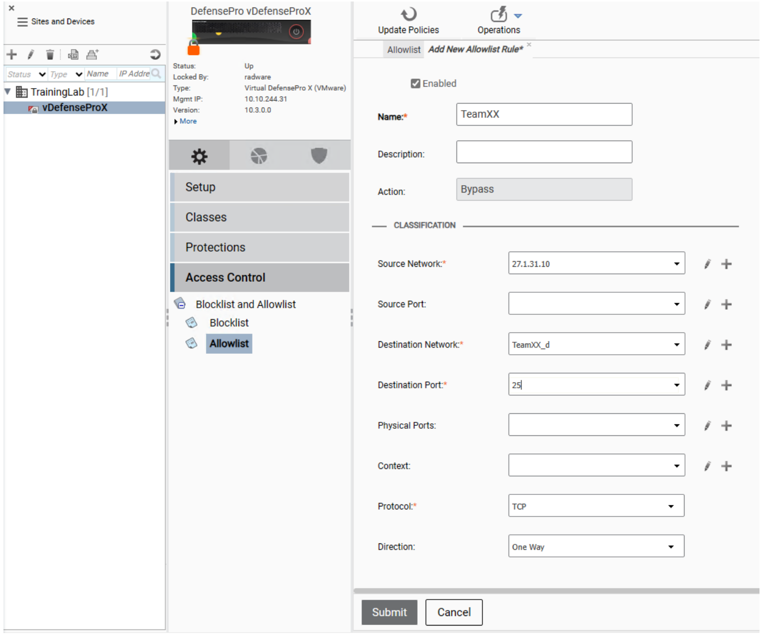
Precedence: ○ Blocklist Takes Precedence
● Allowlist Takes Precedence

Configure Allowlist

Configure Allowlist using DefensePro configuration

1. Select the **Configuration → Access Control → Blocklist and Allowlist → Allowlist.**
2. To add or modify an Allowlist rule, do one of the following:
   a. To add a rule, click + (Add) button
   b. To edit a rule, double-click the entry in the table.
3. Configure Allowlist rule parameters.
   a. Check **Enabled**
   b. Name: **TeamXX** (where XX are your initials)
   c. Source Network: **<IP from preparations section>** (example: 27.1.31.10)
   d. Destination Network: **TeamXX_d** (select existing network where XX are your initials)
   e. Destination Port: **<port from the preparations section>** (example: 25)
   f. Protocol: **TCP**
4. Click **Submit**.

5. Click **Update Policies Required**.



Status:	Up
Locked By:	radware
Type:	Virtual DefensePro X (VMware)
Mgmt IP:	10.10.244.31
Version:	10.3.0.0

☑ Enabled

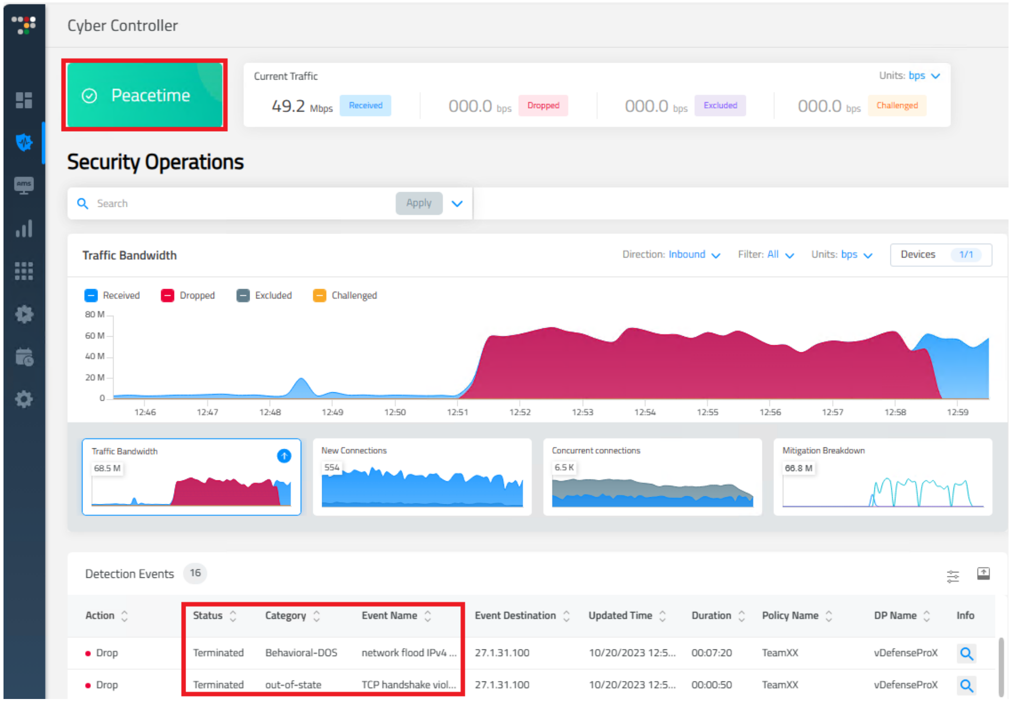
Name:*	TeamXX
Description:	
Action:	Bypass

CLASSIFICATION

Source Network:*	27.1.31.10
Source Port:	
Destination Network:*	TeamXX_d
Destination Port:*	25
Physical Ports:	
Context:	
Protocol:*	TCP
Direction:	One Way

Test the Configuration

Once you configured the Allowlist, the DefensePro should stop detecting the single source RST attack.



Cyber Controller

Peacetime

Current Traffic — Units: bps

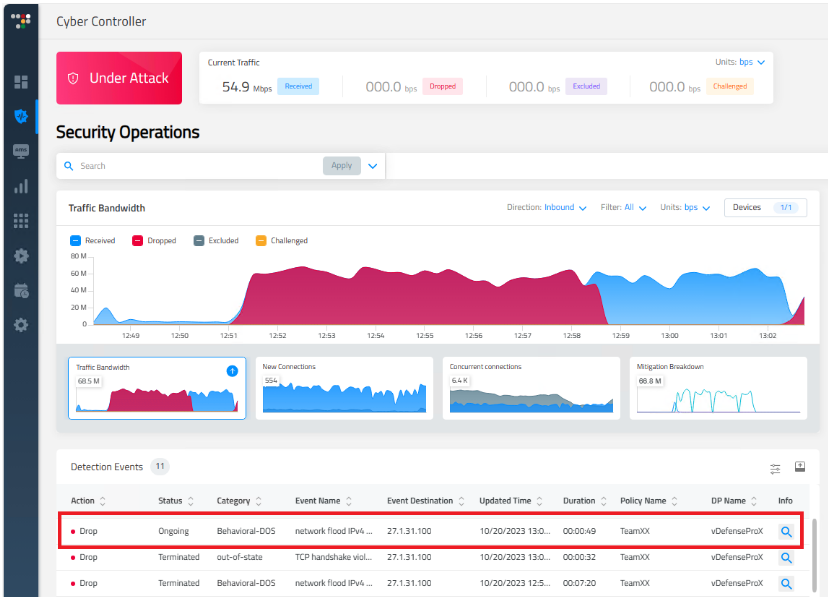
49.2 Mbps Received | 000.0 bps Dropped | 000.0 bps Excluded | 000.0 bps Challenged

Security Operations

Detection Events 16

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
● Drop	Terminated	Behavioral-DOS	network flood IPv4 ...	27.1.31.100	10/20/2023 12:5...	00:07:20	TeamXX	vDefenseProX	
● Drop	Terminated	out-of-state	TCP handshake viol...	27.1.31.100	10/20/2023 12:5...	00:00:50	TeamXX	vDefenseProX	

1. Go to the attacker and stop the attack.
2. Launch a TCP RST attack (**Network Attacks → Floods → Multiple Sources → TCP → RST Attacks**, destination **IP 27.1.31.100**)



Cyber Controller

Under Attack

Current Traffic — Units: bps

54.9 Mbps Received | 000.0 bps Dropped | 000.0 bps Excluded | 000.0 bps Challenged

Security Operations

Detection Events 11

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	10/20/2023 13:0...	00:00:49	TeamXX	vDefenseProX	
● Drop	Terminated	out-of-state	TCP handshake viol...	27.1.31.100	10/20/2023 13:0...	00:00:32	TeamXX	vDefenseProX	
● Drop	Terminated	Behavioral-DOS	network flood IPv4 ...	27.1.31.100	10/20/2023 12:5...	00:07:20	TeamXX	vDefenseProX	

3. You should see that since this attack is coming from spoofed source IPs it is detected and mitigated.

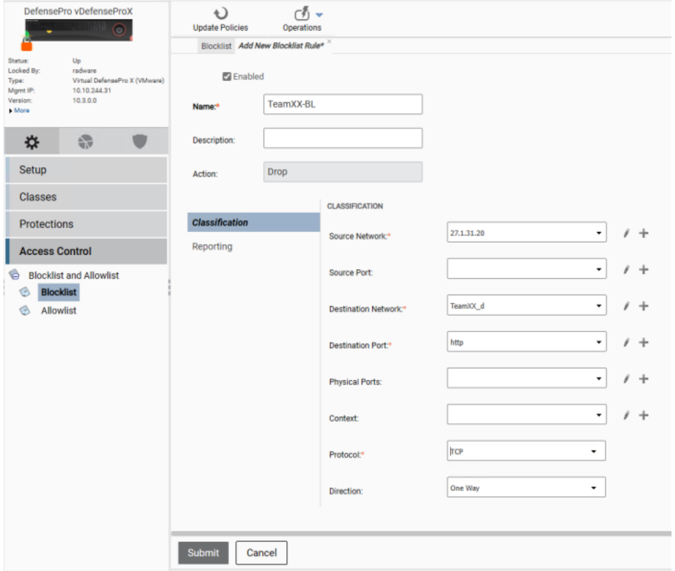
4. At Attacker Raptor Stop the attack.

Configure Blocklist

Configure Blocklist using DefensePro configuration

Before you begin, be sure to stop JMeter app generating legitimate traffic from a legitimate client.

1. Select the **Configuration → Access Control → Blocklist and Allowlist → Blocklist.**
2. To add or modify an Blocklist rule, do one of the following:
    a. To add a rule, click + (Add) button
    b. To edit a rule, double-click the entry in the table.
3. Configure Blocklist rule **Classification** parameters.
    a. Check **Enabled**
    b. Name: **TeamXX-BL** (where XX are your initials)
    c. Source Network: **27.1.31.20** (IP of the legitimate client)
    d. Destination Network: **TeamXX_d** (select existing network where XX are your initials)
    e. Destination Port: **http**
    f. Protocol: **TCP**
4. Click **Submit**.
5. Click **Update Policies Required**.



Status: Up
Locked By: radware
Type: Virtual DefensePro X (VMware)
Mgmt IP: 10.10.244.31
Version: 10.3.0.0
▸ More

☑ Enabled

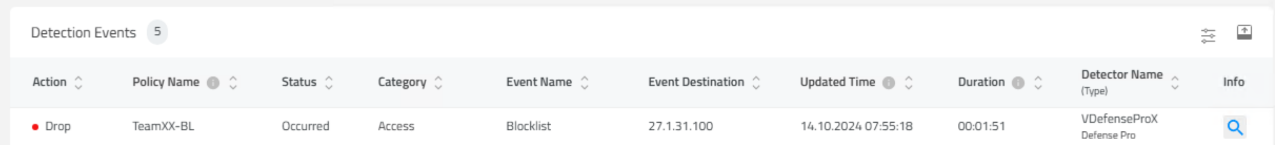
Name:* TeamXX-BL
Description:
Action: Drop

Source Network:* 27.1.31.20
Source Port:
Destination Network:* TeamXX_d
Destination Port:* http
Physical Ports:
Context:
Protocol:* TCP
Direction: One Way

Test the Configuration

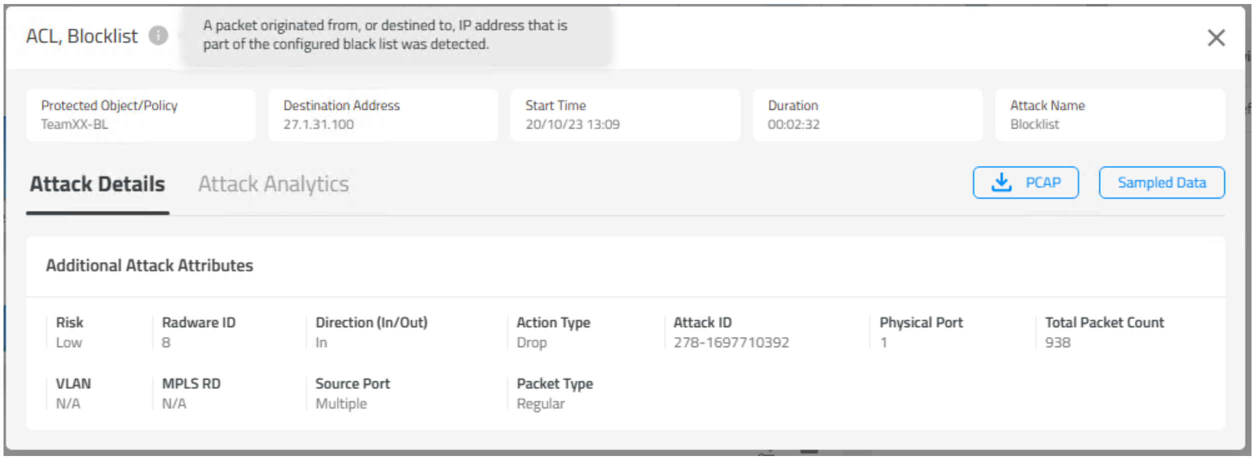
Once you configured the Blocklist, go to the Legitimate Client

1. Open a browser in the Legitimate Client
2. URL: http://target.mylab.inside
3. Notice that browser times out.
4. Check the Detection Events at the Real-Time Monitoring dashboard.
5. See as well the attack details:



Detection Events 5

Action	Policy Name	Status	Category	Event Name	Event Destination	Updated Time	Duration	Detector Name (Type)	Info
● Drop	TeamXX-BL	Occurred	Access	Blocklist	27.1.31.100	14.10.2024 07:55:18	00:01:51	VDefenseProX Defense Pro	🔍



ACL, Blocklist

A packet originated from, or destined to, IP address that is part of the configured black list was detected.

Protected Object/Policy	Destination Address	Start Time	Duration	Attack Name
TeamXX-BL	27.1.31.100	20/10/23 13:09	00:02:32	Blocklist

Additional Attack Attributes

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
Low	8	In	Drop	278-1697710392	1	938

VLAN	MPLS RD	Source Port	Packet Type
N/A	N/A	Multiple	Regular

6. Disable the existing Blocklist **Configuration → Access Control → Blocklist and Allowlist → Blocklist and Allowlist**. Double click on the existing blocklist and uncheck **Enable**.
7. Click on the **Update Policies Required**.
8. Open a browser in the Legitimate Client and notice the page is loading.

Export and save configuration file as **dp8-BlockAllow-config.txt**.

For questions, contact training@Radware.com