radware

DefensePro
Version 8.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.

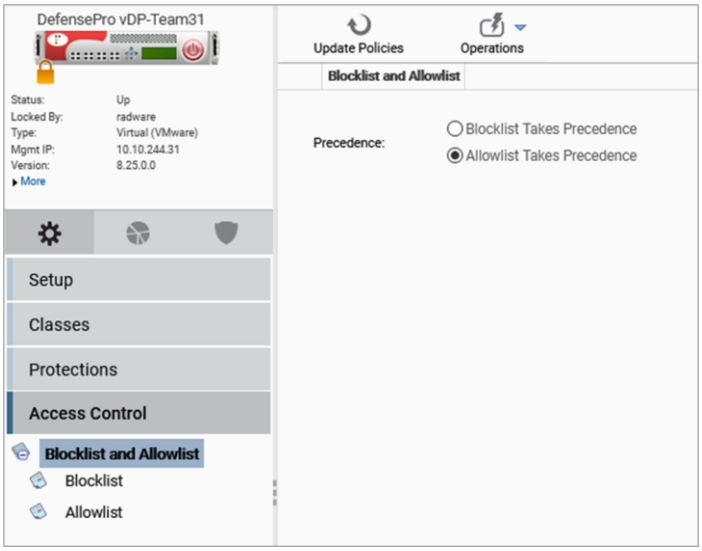
Preparations

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

1. Edit your protection policy and add the BDoS profile from the BDoS lab and update policies.
2. Go to the attacker and launch a TCP RST attack (**Network Attacks → Floods → Single Source → TCP → RST Attacks**, destination **IP 27.1.31.100**)
3. Find out the source IP and destination port of the attack by examining the attack **in Analytics AMS**. (In this example it is 27.1.31.10 and 25 respectively, however in your case it might differ).

Setup Blocklist and Allowlist

1. Select the **Configuration** perspective.
2. In **Configuration → Access Control → Blocklist and Allowist** select which one takes precedence.



3. By default **Default Allowlist Takes Precedence**.

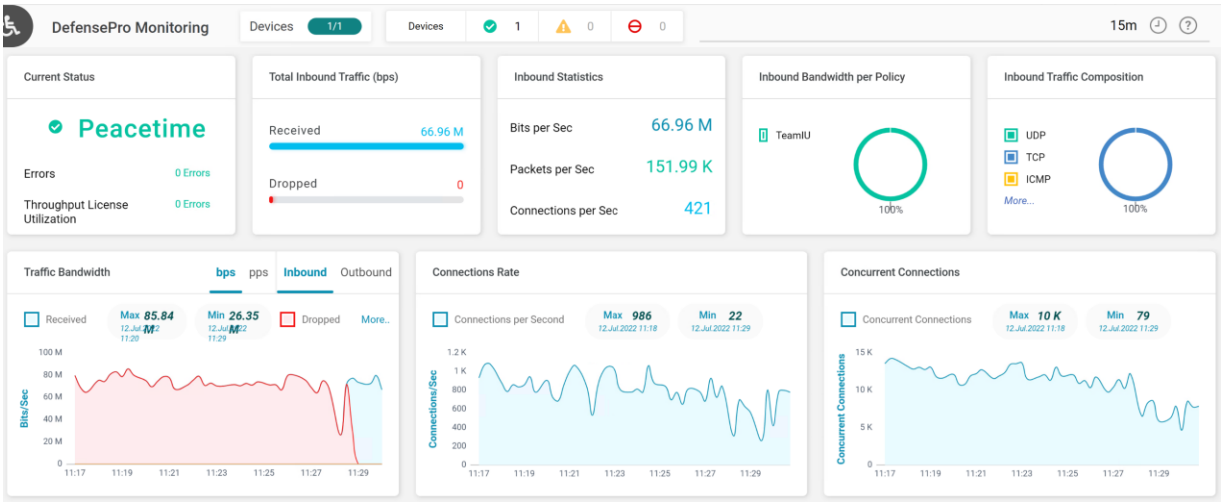
Configure Allowlist

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** (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**.

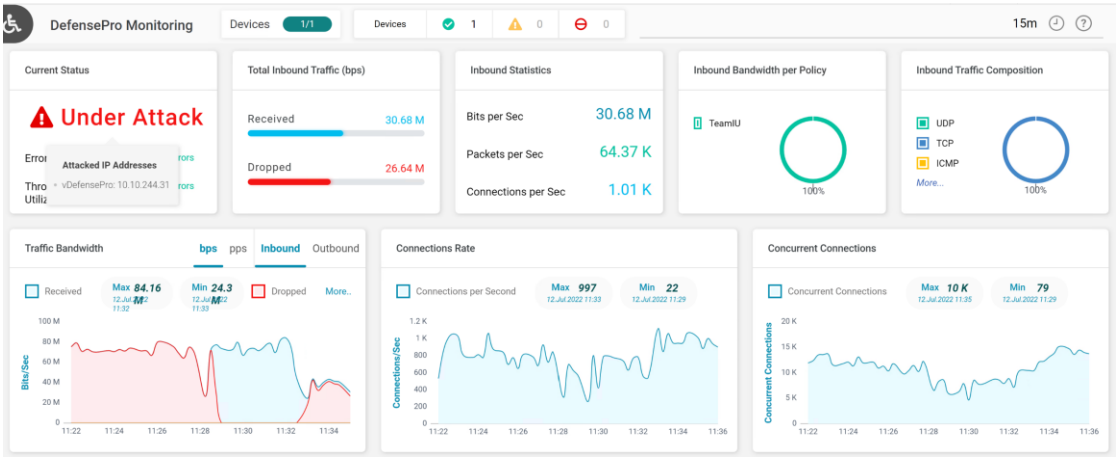
Test the Configuration

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



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**)

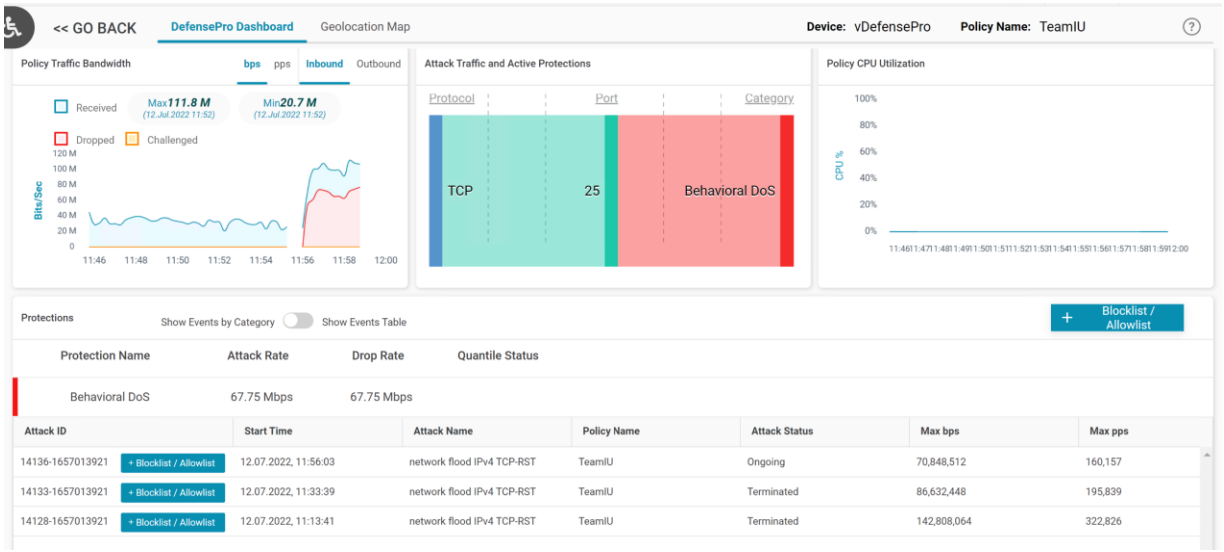
3. Use Vision analytics to view the attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.



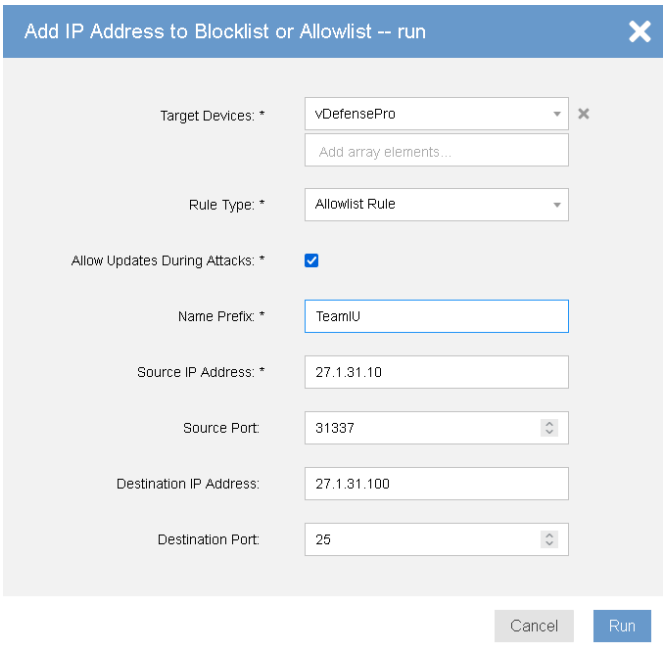
4. At Attacker Raptor **Stop** the attack. (CTRL-C).

Configure Allowlist using Vision Analytics AMS

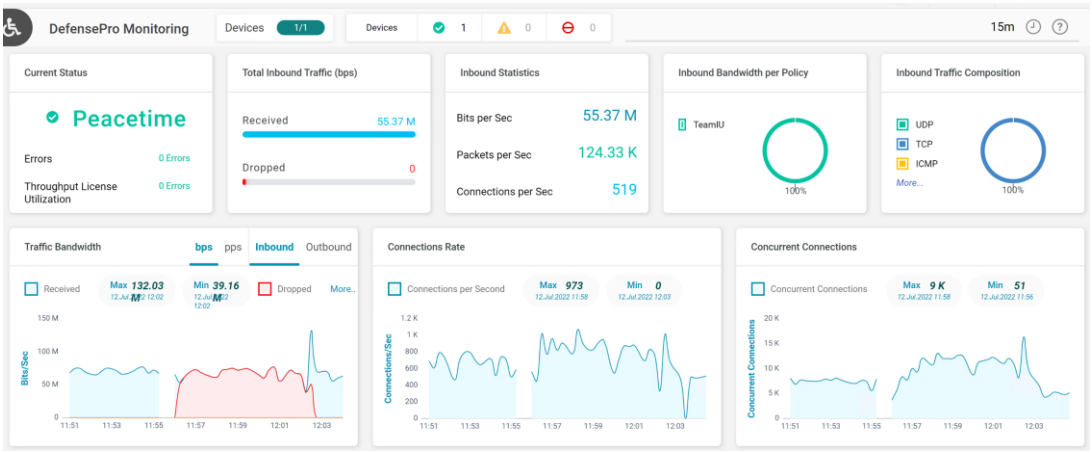
1. Launch a single source TCP RST attack again.
2. Disable the existing Allowlist **Configuration → Access Control → Blocklist and Allowlist → Allowlist**. Double click on the existng allowlist and uncheck **Enable**.
3. Click on the **Update Policies Required**.
4. Use Vision analytics to view the attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.
5. Select your policy in the **Protection Policies** section.
6. Select **Behavioral DoS** in the **Protections** section.
7. Click on the **+Blocklist / Allowlist** button on the **Ongoing** attack.



8. Change **Rule Type** to **Allowlist Rule**, **Name Prefix** to **TeamXX** (where XX are your initials) leave rest as default.Then click on **Run**.



9. You will notice the DefensePro will stop detecting an attack.

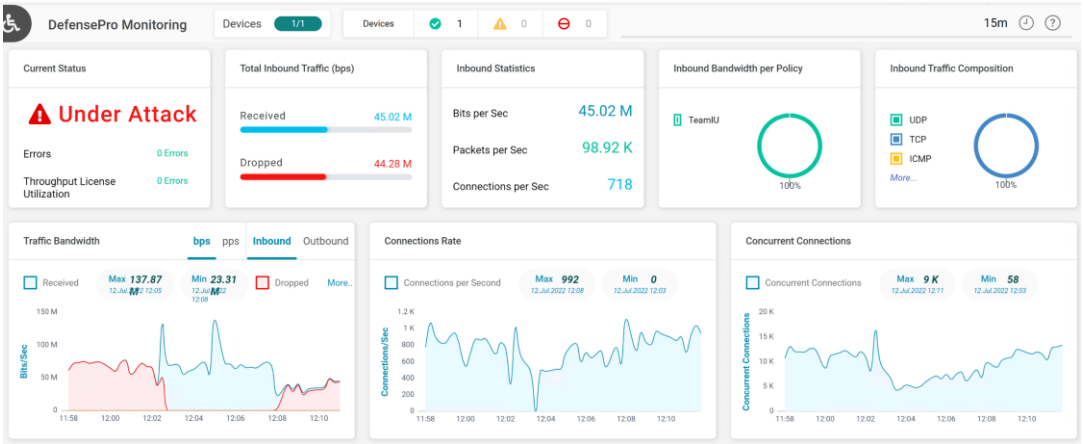


10. Go to the Attacker and stop the single source attack and start a multiple sources TCP RST attack and observe the DefensePro blocking new attack.
11. Stop the attack.
12. Go to DefensePro **Configuration** and disable the new **Allowlist** and click on the **Update Politices Required**.

Configure Blocklist

Configure Blocklist using DefensePro configuration

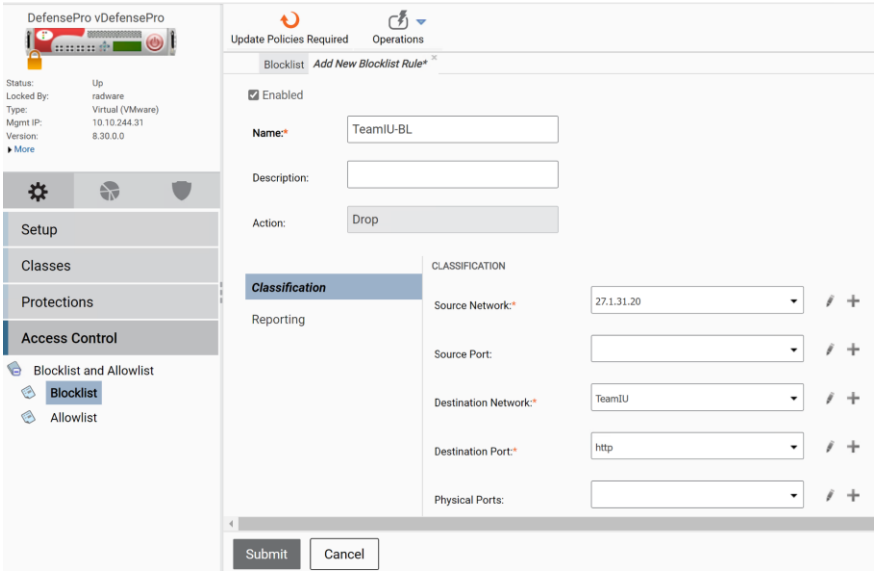
1. Select the **Configuration → Access Control → Blocklist and Allowlist → Blocklist.**
2. To add or modify an Blocklist rule, do one of the following:
    a. To add a rule, click + (Add) button
    b. To edit a rule, double-click the entry in the table.
3. Configure Blocklist rule **Classification** parameters.



    a. Check **Enabled**
    b. Name: **TeamXX-BL** (where XX are your initials)

c. Source Network: **<IP of the legitimate client>** (example: 27.1.31.20)
d. Destination Network: **TeamXX** (where XX are your initials)
e. Destination Port: **http**
f. Protocol: **TCP**

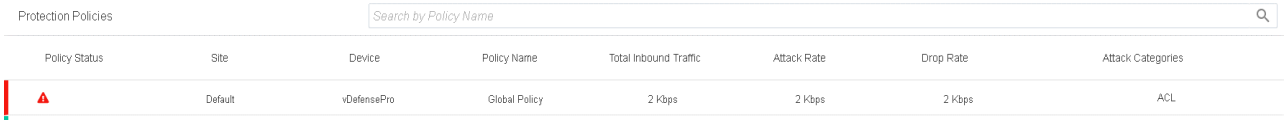
4. Click **Submit**.
5. Click **Update Policies Required**.



Test the Configuration

Once you configured the Blocklist, go to the Legitimate Client

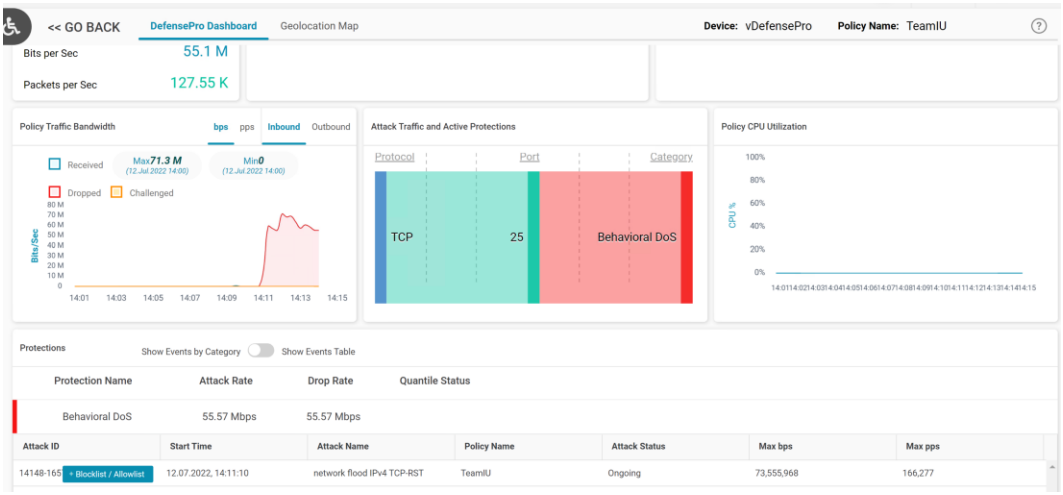
1. Open a browser in the Legitimate Client
2. URL: http://target.mylab.inside
3. Notoce that browser times out.
4. Use Vision analytics to view the attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.



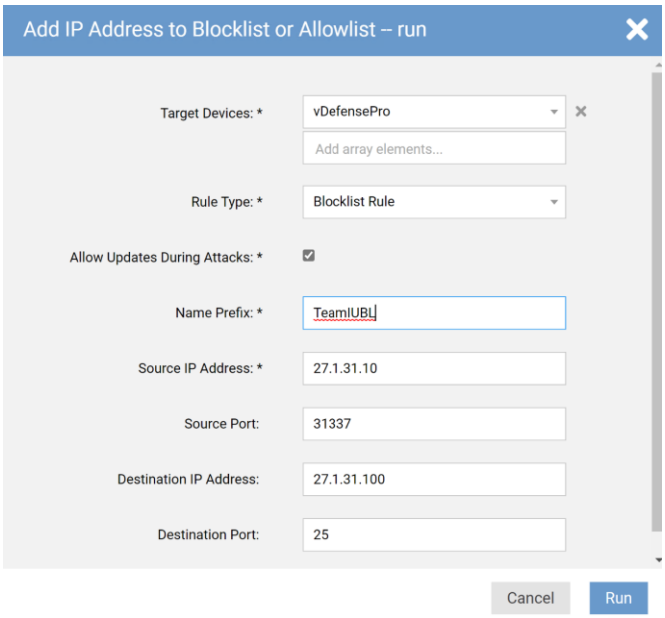
5. Disable the existing Blocklist **Configuration → Access Control → Blocklist and Allowlist → Blocklist**. Double click on the existing blocklist and uncheck **Enable**.
6. Click on the **Update Policies Required**.
7. Open a browser in the Legitimate Client and notice the page is loading.

Configure Blocklist using Vision Analytics AMS

1. Launch a single source TCP RST attack again.
2. Use Vision analytics to view the attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.
3. Select your policy in the **Protection Policies** section.
4. Select **Behavioral DoS** in the **Protections** section.
5. Click on the **+Blocklist / Allowlist** button on the **Ongoing** attack.

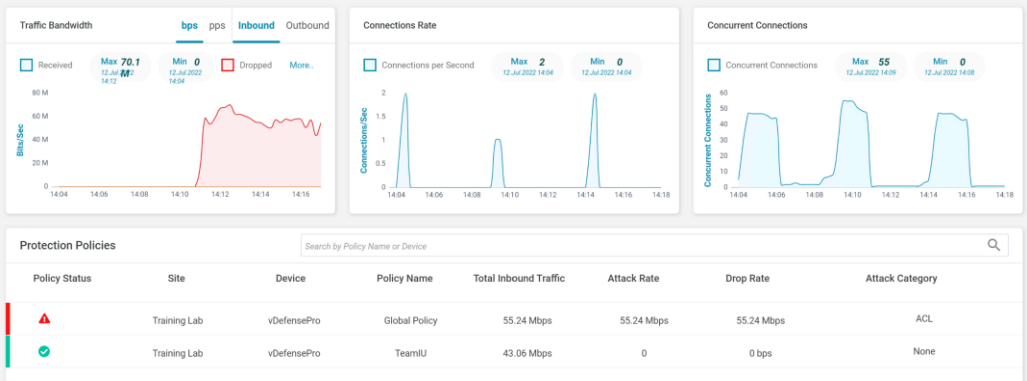


6. Use **Rule Type** to **Blocklistist Rule**, **Name Prefix** to **TeamXXBL** (where XX are your initials) leave rest as default.



7. You will notice the DefensePro will stop detecting an attack as **a Behavioral DoS** and display **ACL attack**.

8. Go to the Attacker and stop the single source.



9. Stop the attack.
10. Go to DefensePro configuration and disable the new **Blocklist** and click on the **Update Politices Required**.

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

For questions, contact training@Radware.com