DefensePro
Version 8.x

Training Lab Manual
Configure Location Based and EAAF Protection

Table of Contents

Overview

A Geolocation profile can do one of the following:

- Permanently block traffic from/to selected geolocations.
- Permanently allow traffic from/to selected geolocations, and block all other geolocations.

To identify the geolocation that traffic originates from, the Geolocation feature uses the *Geolocation feed*.
APSolute Vision manages the Geolocation subscription and the Geolocation feed.
If the DefensePro device has a valid Geolocation subscription and a user-defined scheduled task of type *Geolocation Feed*, the task uploads the feed to the Geolocation database on the DefensePro device.

ERT Active Attackers Feed (EAAF) profiles use the EAAF subscription service to identify and block source IP addresses involved in major attacks in real-time to provide preemptive protection from known attackers. The feed is generated by Radware's Threat Research Center.
Each IP address in the EAAF may belong to one, two, or all three of the following categories:

- **ERT Active Attackers Core** — An IP address that has been correlated and determined to be malicious from multiple sources. Reported events use ERT to identify an ERT Active Attackers address.
- **Tor Exit Nodes** — An IP address that is a Tor exit node, regardless of whether it has been seen performing malicious activity. Block these only if you wish to block all Tor exit nodes by default. Note that ERT Active Attackers category will contain Tor exit nodes that have recently been seen performing malicious activities. Reported events use TOR to identify a Tor Exit Nodes address.
- **Web Attackers** — An IP address that has been seen performing Web violations. Note that the ERT Active Attackers category will contain Web attackers that have recently been seen performing other malicious activities in addition to Web violations. Reported events use WEB to identify a Web Attackers address.

Setup Scheduler for Geolocation Feed and ERT Active Attackers Feed

Create a scheduler for the Geolocation feed.

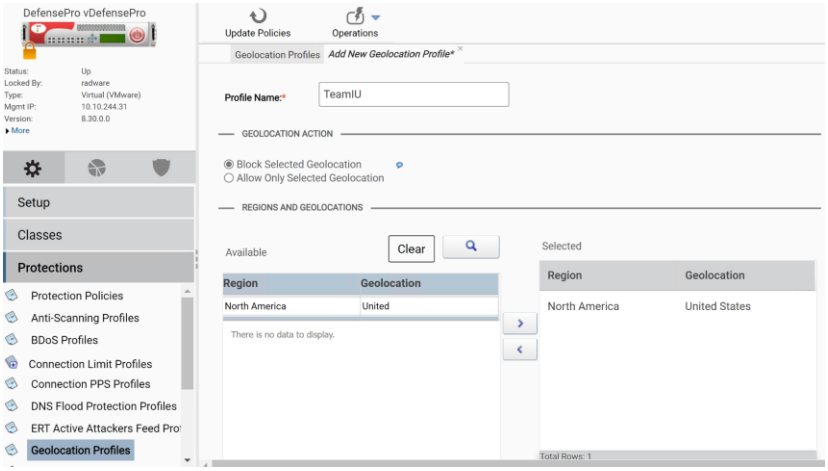
1. In Vision click on the scheduler and verify that the **Geolocation Feed** is scheduled and executed successfully.
2. If it is not scheduled, create a schedule.
    a. Task Type: **Geolocation Feed**
    b. Name: **Geolocation Update**
    c. Schedule → Run: **Daily**
    d. Schedule → Time: **9:00:00**
    e. Target Device List → Selected: **vDefensePro**
3. Select the Geolocation Feed task and click **Run** icon and make sure it completes successfully

Create an ERT Active Attackers Feed schedule.

1. In scheduler verify that the **ERT Active Attackers Feed for DefensePro** is scheduled and executed successfully.
2. If it is not scheduled, create a schedule.
    a. Task Type: **ERT Active Attackers Feed for DefensePro**
    b. Name: **ERT AAF**
    c. Schedule → Run: **12 Hours**
    d. Target Device List → Selected: **vDefensePro**
3. Select the ERT Active Attackers Feed task and click **Run Now** icon and make sure it completes successfully.

Configure Permanent Block

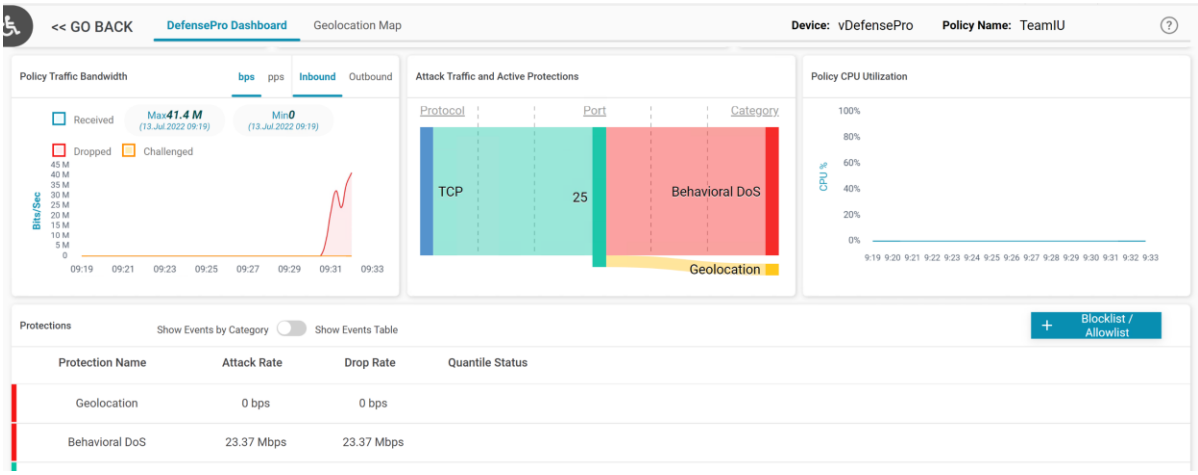
1. Select the DefensePro **Configuration → Protections → Geolocation Profiles.**
2. Click on **+** (Add Geolocation Profile)
3. Enter Profile Name: **TeamXX** (where XX are your initials)
4. Select **North America / United States** in the Regions and Geolications section



5. Click **Submit**.
6. Edit your protection policy and add **Geolocation Profile**.
7. Click **Submit**.
8. Click **Update Policies Required**.

Test the Configuration

1. Launch a TCP RST attack (**Network Attacks → Floods → Multiple Sources → TCP → RST Attacks**, destination **IP 27.1.31.100**)
2. Use Vision analytics to view the attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.



3. Select **Analytics AMS → DefensePro Monitoring → Geolocation Map**
4. Locate a country that is marked red.

5. Click on the country and select **Block Duration 3H**.

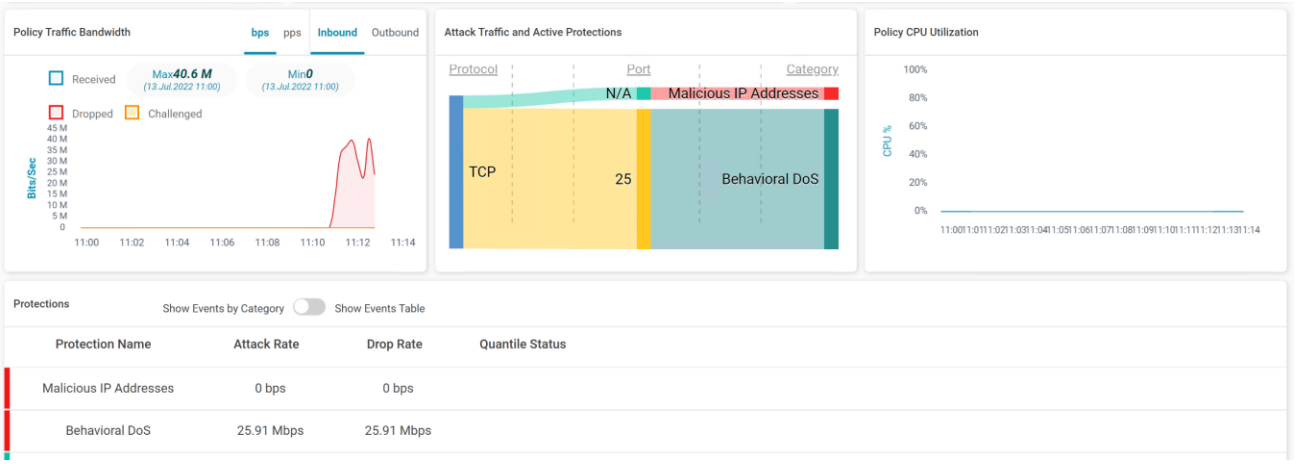
6. Go to DefensePro **Monitoring → Networking → Location-Based Suspended Traffic** to see temporarily suspended Geolocation traffic.
7. Go back to the **Geolocation Map** and click on the same country and click **Block Duration 3H** to unblock the country.

Configure ERT Active Attackers Feed

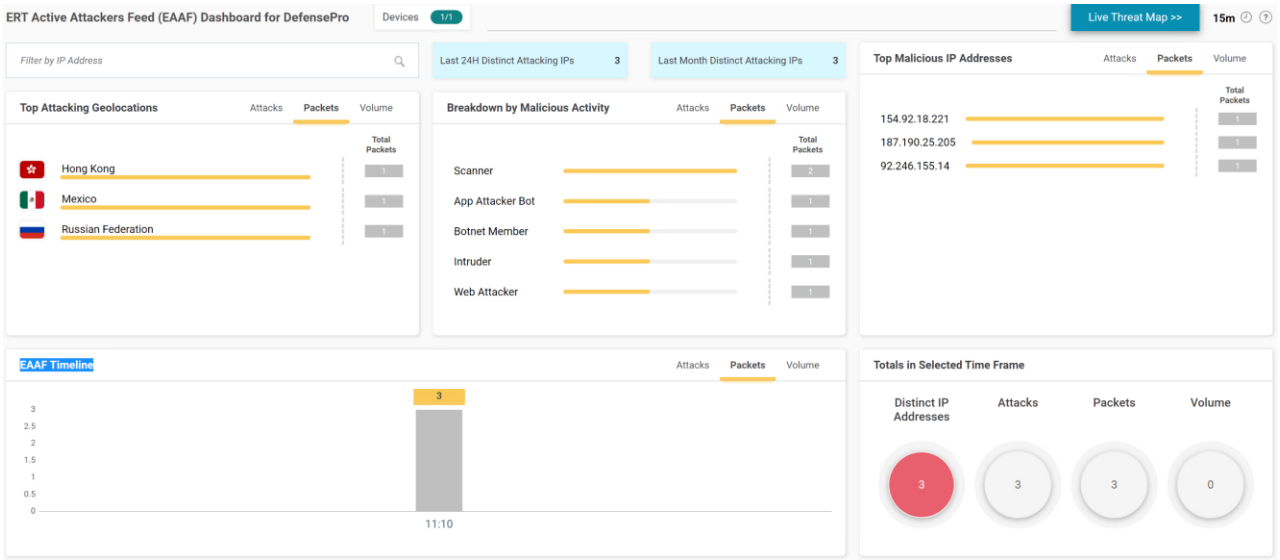
1. Select the DefensePro **Configuration → Protections → ERT Active Attackers Feed Profiles**
2. Click + (Add ERT Attackers Feed Profile)
3. Enter Profile Name: **TeamXX** (where XX are your initials)
4. In the **Feed Categories and Action Per Level** change all to **Block and Report** (in production your settings should be different).
5. Click **Submit**.
6. Add the **ERT Active Attackers Feed Profile** to your **Protection Policy**.
7. Remove the **Geolocation Profile** from your **Protection Policy**.
8. Click **Submit**.
9. Click **Update Policies Required**.

Test the Configuration

1. Launch a TCP RST attack (**Network Attacks → Floods → Multiple Sources → TCP → RST Attacks**, destination **IP 27.1.31.100**)
2. Use Vision analytics to view the attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.



3. Select **Analytics AMS → EAAF for DefensePro**



4. Stop the attack.

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

For questions, contact training@Radware.com