radware

DefensePro
Version 8.x

Training Lab Manual
Configure BDoS DNS

Table of Contents

Contents

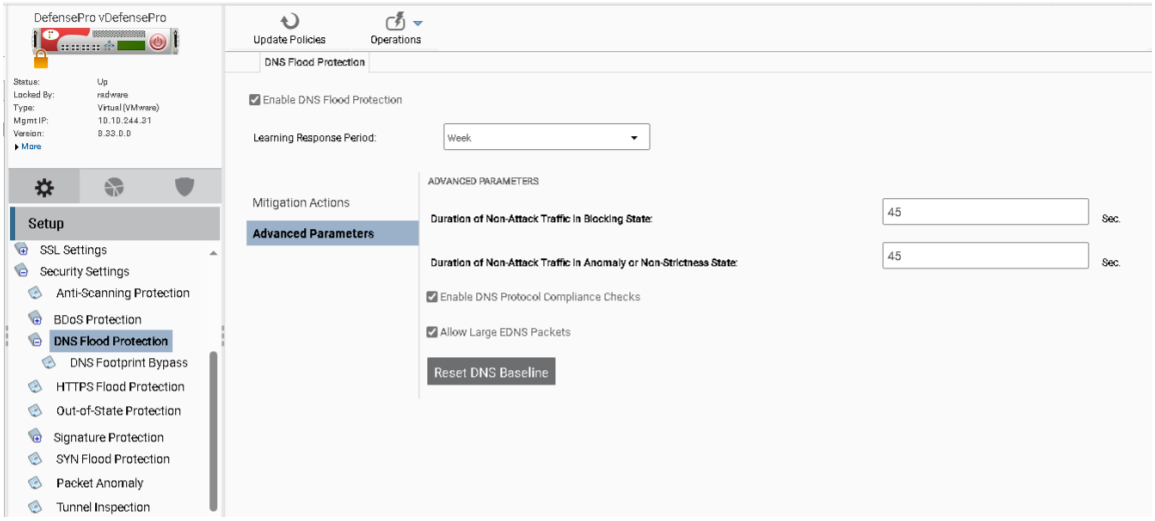
Overview

Radware DefensePro can be configured to protect public DNS server against DNS flood attacks.
A DNS Flood is an application-specific variant of a UDP flood.
Since DNS servers use UDP traffic for name resolution, sending a massive number of DNS requests to a DNS server can consume its resources, resulting in significantly slower response times for legitimate DNS requests.

In the Radware virtual lab environment, DNS Flood Protection is enabled on your DefensePro device.

Setup DNS Flood Protection

1. Access **APSolute Vision**
2. Select the DefensePro **Configuration** perspective.
3. In **Setup** section, select **Security Settings → DNS Flood Protection** on navigation tree
4. In the **DNS Flood Protection** tab verify that the **Enable DNS Flood Protection** checkbox is checked.
5. Configure **Learning Response Period** as: ***Day***
6. In **Mitigation Actions**, enable all available mitigation actions, since the challenges are disabled by default.
7. Click **Advanced Parameters** section
8. Set Duration of **Non-attack Traffic in Blocking State**: ***50*** and **Duration of Non-attack Traffic in Anomaly or Non-Strictness State**: ***50***



Depending on software version this is the default.

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

Configure DNS Flood Protection

1. Select the **Configuration** perspective.
2. In **Protections** section, select ***Protection Policies***.
3. In **Protection Policies** tab double-click ***TeamXX*** (where XX are your initials) to edit.
4. In **Edit Network Protection Policy** tab select ***Profiles*** section.
5. For **DNS Flood Protection Profile** click ***Add*** button.
6. For **Profile Name** type: ***TeamXX*** (where XX are your initials)
7. In **Query Protections and Quotas** section:
   Check the "Select All Query Types" check box and leave the values empty. The device will use the default quotas.
8. Select **Rate Settings** and configure:
   - **Expected DNS Query Rate**: ***1000*** QPS
   - **Max Allowed QPS**: ***5000*** QPS
   - **Signature Rate-Limit Target**: ***20%***
9. Click **Submit** button to Add DNS Profile.
   This new Profile is automatically selected at Policy Profiles menu.
10. Click **Submit** button to save changes to Network Protection Policy.
11. Click **Update Policies Required** button and wait for completion.

Add a Manual Allowlist Entry

Sometimes we need to manually add Allowlist for particular fully qualified domain name (FQDN) query.

1. Create a text file allowlist.txt with the following entry **www.mydomain.com,m** (using Notepad++)
2. Go to DefensePro **Configuration → Protection Policies** and edit your policy containing the DNS Flood profile.
3. In the **DNS Subdomains Allowlist** tab click **Browse**.
4. Select your **allowlist.txt** and click **Import**.

Note: Importing a Subdomains Allowlist file is performed without having to run the Update Policies command.

5. Enable the **DNS Subdomains Allowlist** checkbox (When enabled, the DNS Flood Protection policy uses the imported user-defined allowlist as a mitigation method against subdomain attacks. During subdomain attacks, the DNS Flood Protection policy drops all DNS queries that do not match any user-defined entry in the subdomains allowlist).
6. Click **Submit**
7. Click **Update Policies Required**

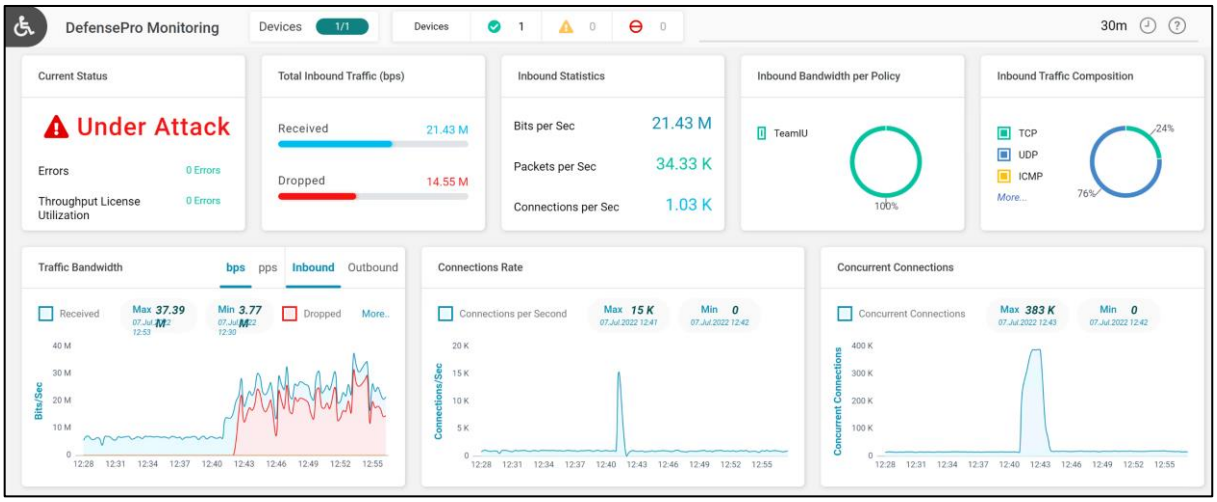
Test the Configuration

Use Raptor to send DNS Flood Attack

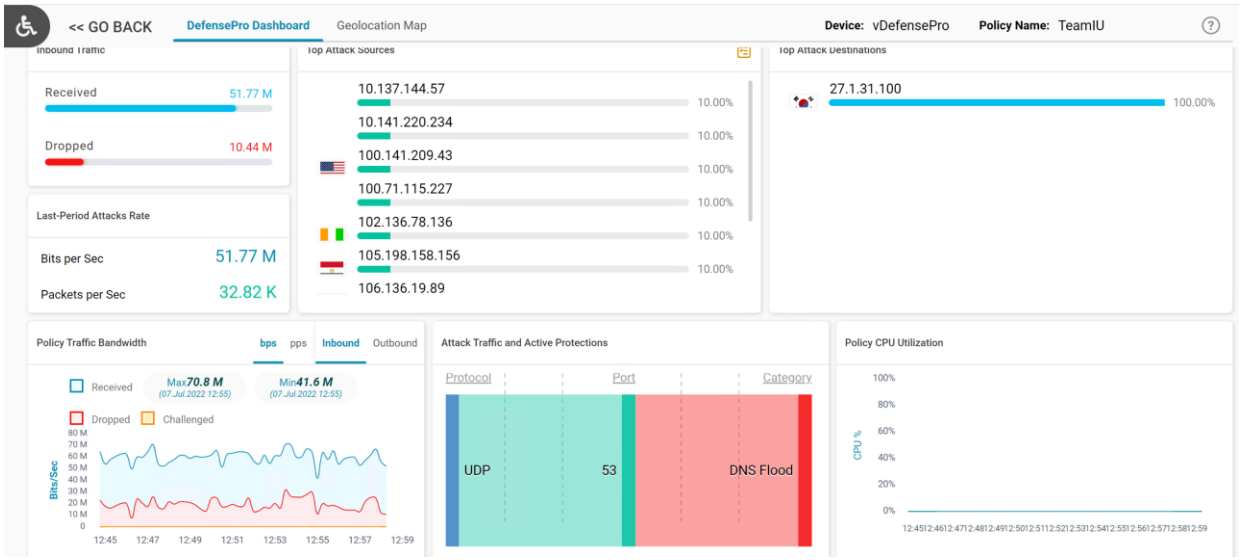
1. Access **Attacker-PC Raptor** main menu select **Services Attacks → DNS → Flooding**.
2. Verify/Enter Destination IP address: **27.1.31.100** Keep default domain name (i.e. **example.fake**)
3. Click **OK** to start attack.

After the attack is initiated from the Attack-PC, you should see traps in the CLI/Syslog. DNS flood attacks and Anomalies are detected by DP.

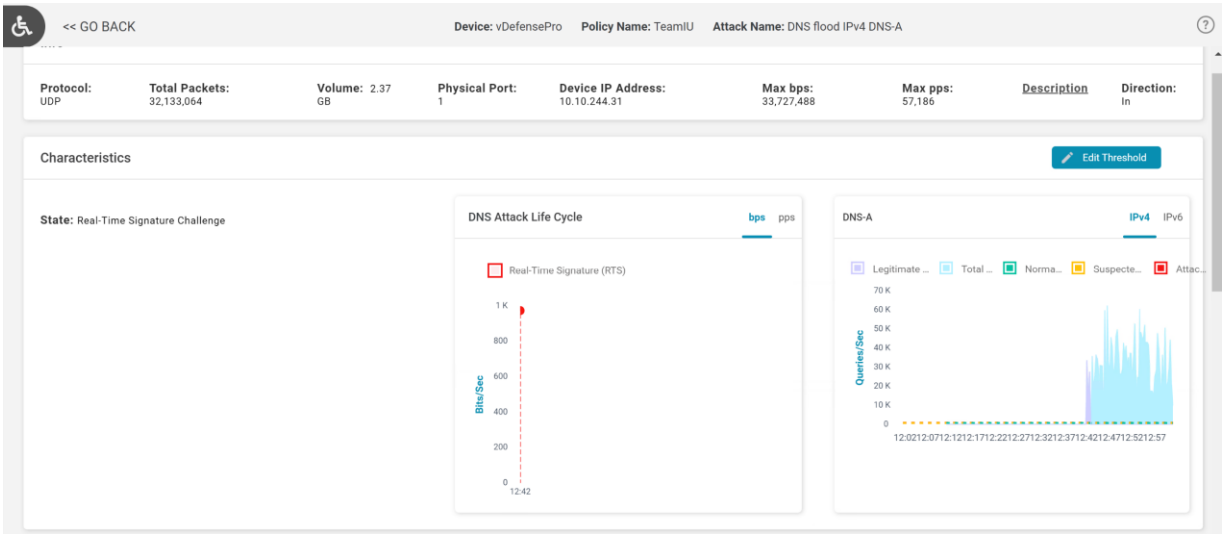
4. Use Vision to View DNS Flood Attack. Select the **Analytics AMS → DefensePro Monitoring**.



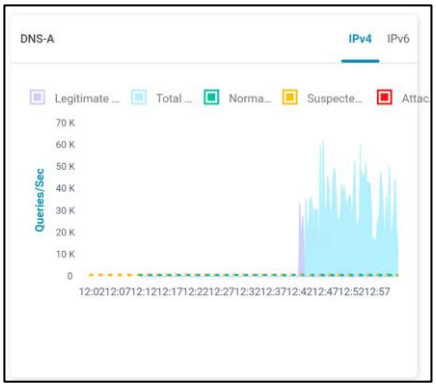
5. Select your policy under attack in **Protection Policies** section.



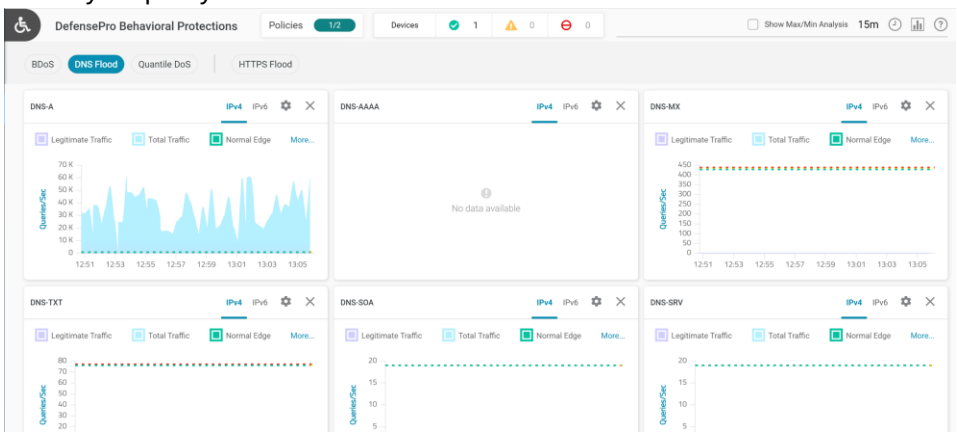
6. Select **DNS Flood** under **Protections** section and click on the ongoing attack.



7. You should see that the type A record is under attack



8. Select **Analytics AMS → DefensePro Behavioral Protections**
9. Select your policy under the **Policies** and select **DNS Flood**.



10. At Raptor **Stop** the attack.
11. **Export** and save configuration file as **dp8-DNS-BDoSLab-config.txt**.

For questions, contact training@Radware.com