radware

DefensePro
Version 8.x

Training Lab Manual
Configure SYN Protection

Table of Contents

Overview

A SYN Flood Attack is a type of DoS attack that attemps to fill or overflow the session table used by a server another stateful network device such as firewall to track TCP connections. SYN Packets are small, making it easier to generate them in large volumes.

Typical SYN Attacks involve: incomplete TCP 3-way handshakes, random source addresses, fully-open connections, and participation of large number of unknowing participante, i.e. Bots (zombies). SYN flood protection is a more efficient use of the DefensePro resources for known SYN flood attacks.

Since this attack could also be detected by BDoS you need to disable BDoS for this lab to ensure SYN Flood is used for mitigation. In real life you would have both enabled. Depending on the attack, lower or higher amount of flood, steep or lower increase of attack select the best suitable DefensePro mitigation.

Remove BDoS Protection

Because BDoS protection might start protecting in the lab and we will not see how the SYN protection works, please remove BDoS protection profile from the policy.

1. In APSolute Vision select the vDefensePro **Configuration → Protections → Protection Policies** double click (or select and click pencil button/**Edit Protection Policy**) your protection policy.
2. Go to **Profiles** tab.
3. Select drop down in **BDoS Profile** and select blank.
4. Click **Submit**.
5. Click **Update Policies Required**.
6. Watch status message "**Upload Policies succeeded**" at bottom line of Vision window.

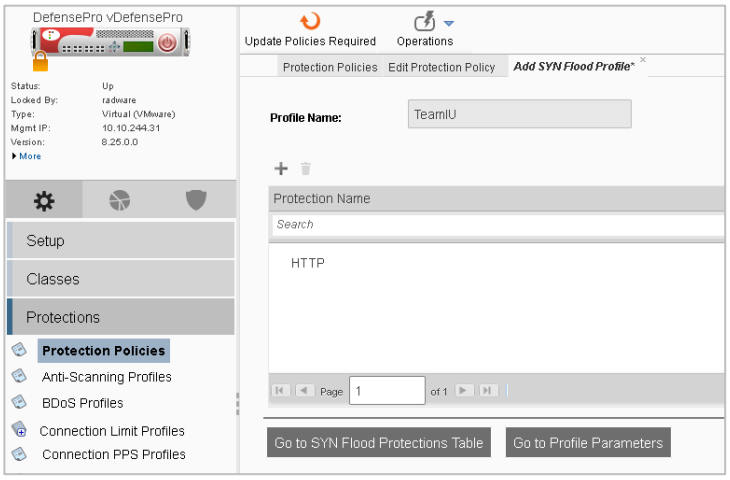
Setup SYN Flood

1. Select the DefensePro **Configuration** perspective.
2. In **Setup** section, select **Security Settings** and then **SYN Flood Protection**.
   By default this feature is enabled.
   Only tracking time can configured. The time, in seconds, during which the number of SYN packets directed to a single protected destination must be lower than the Termination Threshold to cause the attack state to terminate for that destination. Keep default values.

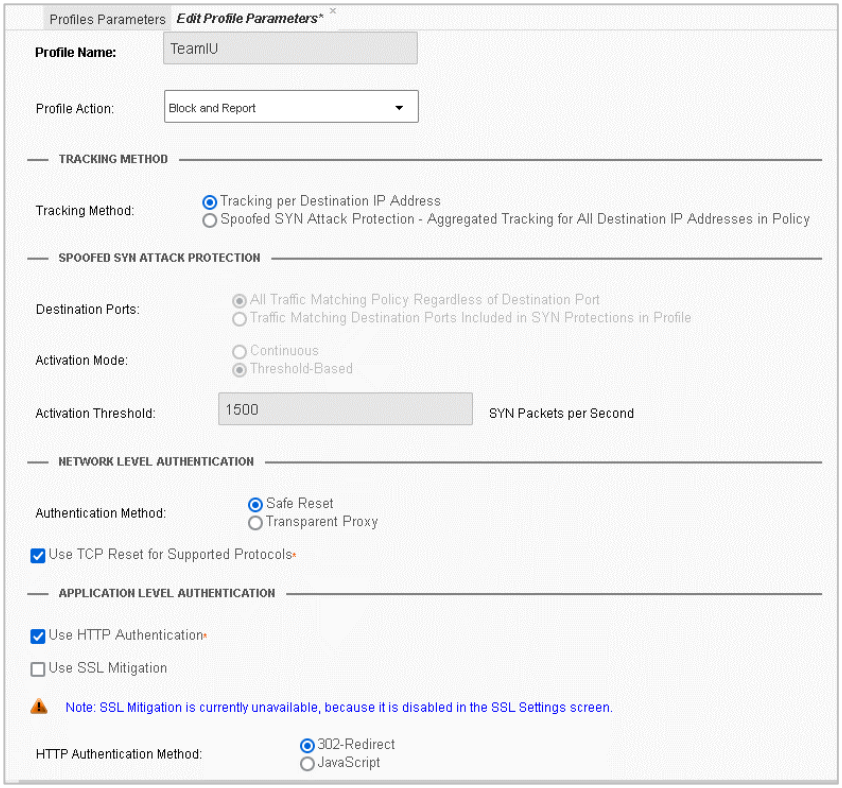
Configure SYN Flood

1. Select the **Configuration** perspective.
2. In the **Protections** section, select **Protection Policies** on navigation tree.
3. In the **Protection Policies** tab double-click your protection policy to edit.
4. Select the **Profiles** section → **SYN Flood Profile**
5. Click **+** to **add** SYN Flood Profile.
6. In **Add SYN Flood Profile** tab type the **Profile Name**: ***TeamXX*** (where XX are your initials)

7. Click **+** to **Add** SYN Flood Protection select **HTTP**
8. If protection for other application/port is required, add additional or create your own SYN Flood Protection Table. You can add as many profiles as required. Activate ONLY ports you really need to protect!
9. Click **Submit** button to add protection to profile.



10. Click **Close**.
11. Go to **Configuration → Protections → SYN Flood Protection Profiles → Profie Parameters**.
12. Double click your profile or select profile and click pen to edit.
    Since we want protect HTTP, under **Network Level Authentication** section select ***Use TCP Reset for Supported Protocols*** and under **Application Level Authentication** section select ***Use HTTP Authentication*** with default ***302-Redirect***.



13. Save option by click on **Submit.**
14. At the **Configuration → Protections → Protection Policies** edit your policy and under **Profiles** select **SYN Flood Protection Profile TeamXX** (where XX are your initials)
15. Make sure NO BDoS profile is selected, since we want SYN Flood protection to identify the SYN attack.
16. Click on **Submit** and **Update Policies Required** buttons.

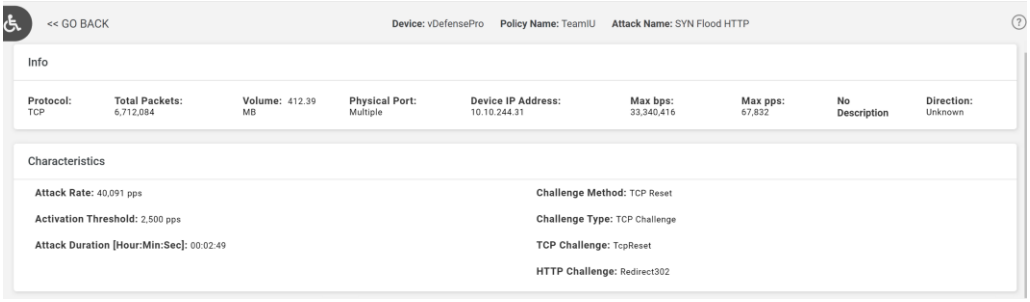
Test the Configuration

Use Raptor to send TCP SYN Flood Attack

1. Access **Attacker-PC Raptor** main menu → select **Network Attacks → Floods → Multiple Source → TCP → SYN Attack**.
2. Verify **Destination IP** address: ***27.1.31.100***

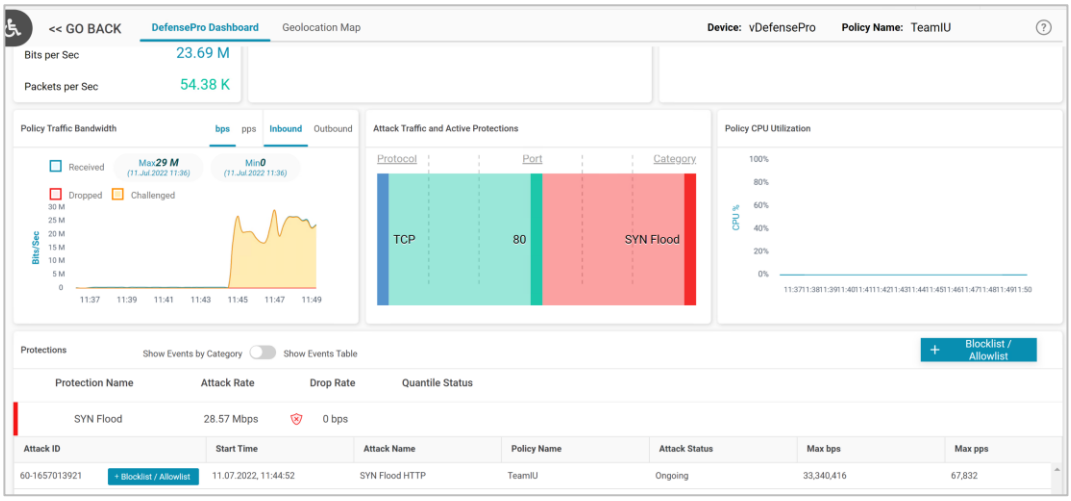
   Soon after the attack is initiated from the Attack-PC, you see traps in the CLI/Syslog.

3. If you did not follow our advice, remove BDoS profile you get this attack detected as BDOS or SYN-Flood.
4. Use Vision to View SYN Flood Attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.
5. View your policy under **Protection Policies**, select **SYN Flood** in the **Protection** section**,** select the ongoing SYN Flood HTTP attack to open Attack Details.

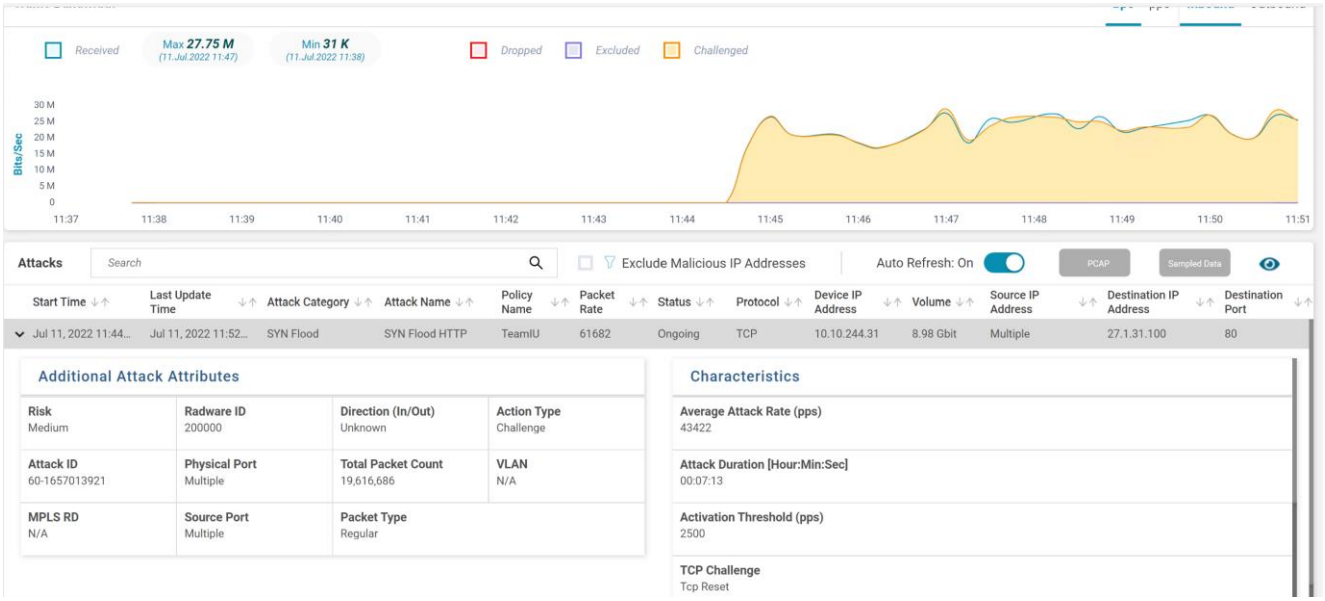


For SYN flooding DP does not record sorce IP information!

6. The graph display in **DefensePro Dashboard** displays **Challenged** because this is a challenge mechanism.



7. You can view on the **Analytics AMS → DefensePro Attacks** select the ongoing SYN Flood HTTP attack to see details.



8. At Raptor **Stop** the attack.
9. **Export** and save configuration file as **dp8-SYNLab-config.txt**.

For questions, contact training@Radware.com