DefensePro X
Version 10.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 X 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 X 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 Cyber Controller **Security Operations → Security Settings** edit the TeamXX policy.
2. Disable the **BDoS Protection** by toggling the button.
3. Click **Submit**.

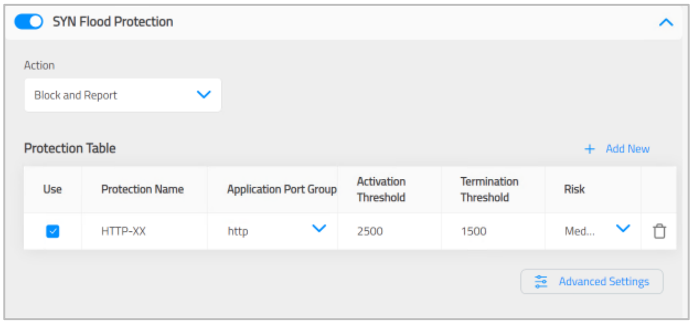
Setup SYN Flood

1. Select the DefensePro X **Configuration** perspective.
2. In **Setup** section, select **Security Settings** and then **SYN Flood Protection**.
   Check, if this feature is enabled, note: by default this feature is enabled.

   Only the 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 **Security Operations → Security Settings** and edit the TeamXX policy.
2. Enable **SYN Flood Protection** and expand it
3. Add new entry into the **Protection Table** by clicking on **"+ Add New**".
4. Add **HTTP** protection:
   - Use: **Checked**
   - Protection Name: **HTTP-XX** (where XX are your initials)
   - Application Port Group: **http**
   - Activation Threshold" **2500**
   - Deactivation Threshold: **1500**
   - Risk: **Medium**



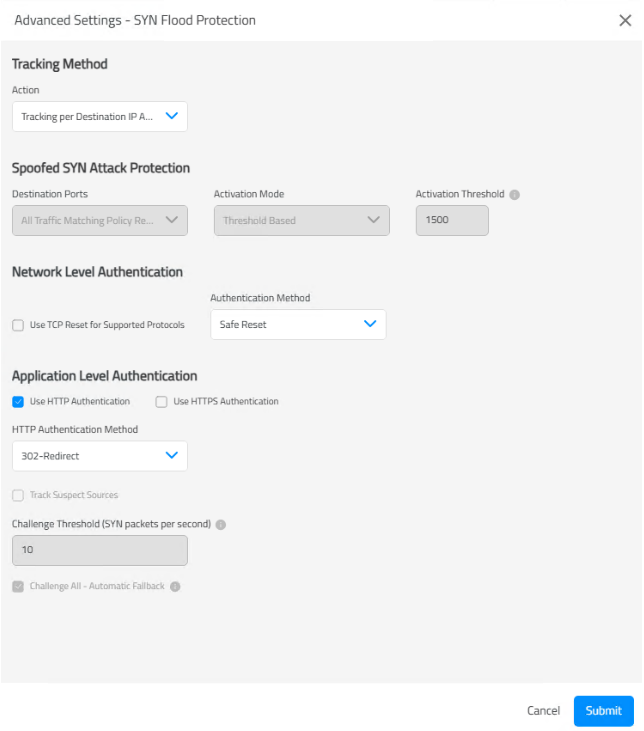
SYN Flood Protection

Action: Block and Report

Protection Table

Use	Protection Name	Application Port Group	Activation Threshold	Termination Threshold	Risk
☑	HTTP-XX	http	2500	1500	Med...

5. Since we want protect HTTP also on the application layer we activate the http authentication. Under **Advanced Settings** section select ***Use TCP Reset for Supported Protocols*** and under **Application Level Authentication** section select ***Use HTTP Authentication*** with default ***302-Redirect***.



Advanced Settings - SYN Flood Protection

Tracking Method

Action: Tracking per Destination IP A...

Spoofed SYN Attack Protection

Destination Ports: All Traffic Matching Policy Re...

Activation Mode: Threshold Based

Activation Threshold: 1500

Network Level Authentication

□ Use TCP Reset for Supported Protocols

Authentication Method: Safe Reset

Application Level Authentication

☑ Use HTTP Authentication

□ Use HTTPS Authentication

HTTP Authentication Method: 302-Redirect

□ Track Suspect Sources

Challenge Threshold (SYN packets per second): 10

☑ Challenge All - Automatic Fallback

6. Click two times **Submit**

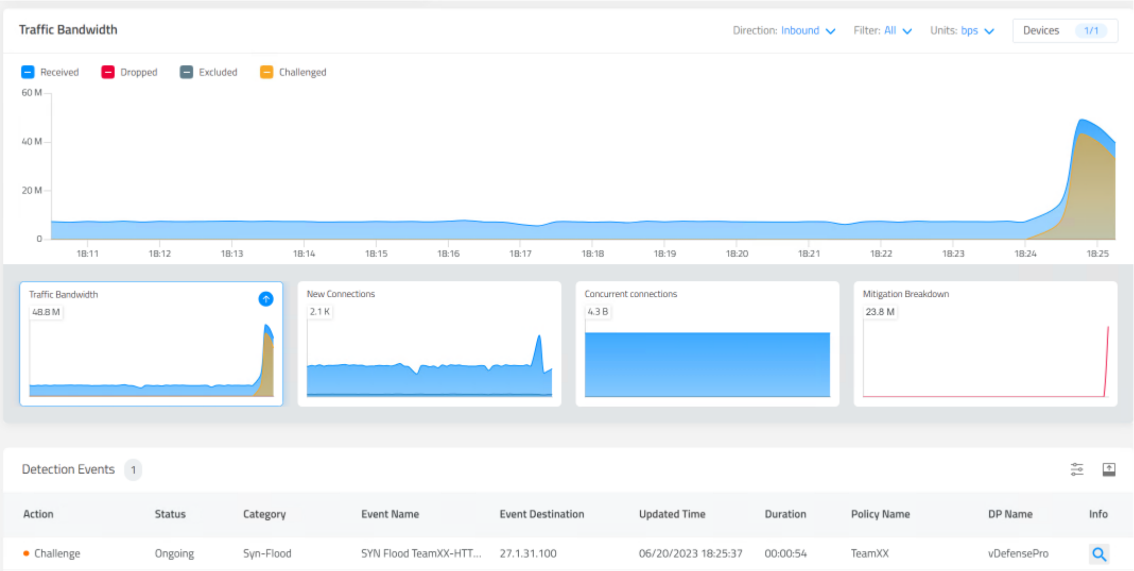
Test the Configuration

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.

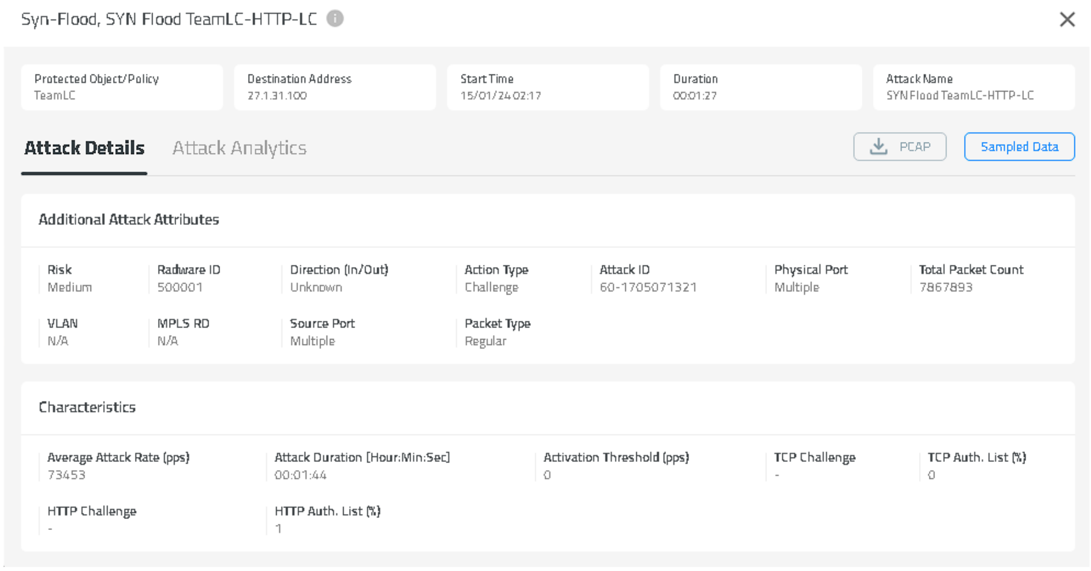
3. If you did not follow our advice, remove BDoS profile you get this attack detected as BDOS or SYN-Flood.
4. Use Cyber Controller to View SYN Flood Attack. Select the **Security Operations → Real-Time Monitoring** perspective.



Detection Events 1

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
● Challenge	Ongoing	Syn-Flood	SYN Flood TeamXX-HTT...	27.1.31.100	06/20/2023 18:25:37	00:00:54	TeamXX	vDefensePro	🔍

5. View the Detection Event by clicking to the Info/Magnifying glass icon.



Syn-Flood, SYN Flood TeamLC-HTTP-LC

Protected Object/Policy	Destination Address	Start Time	Duration	Attack Name
TeamLC	27.1.31.100	15/01/24 02:17	00:01:27	SYN Flood TeamLC-HTTP-LC

Attack Details Attack Analytics

Additional Attack Attributes

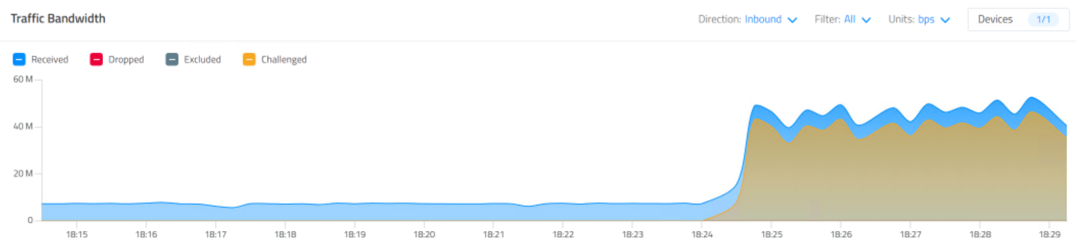
Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
Medium	500001	Unknown	Challenge	60-1705071321	Multiple	7867893
VLAN	MPLS RD	Source Port	Packet Type			
N/A	N/A	Multiple	Regular			

Characteristics

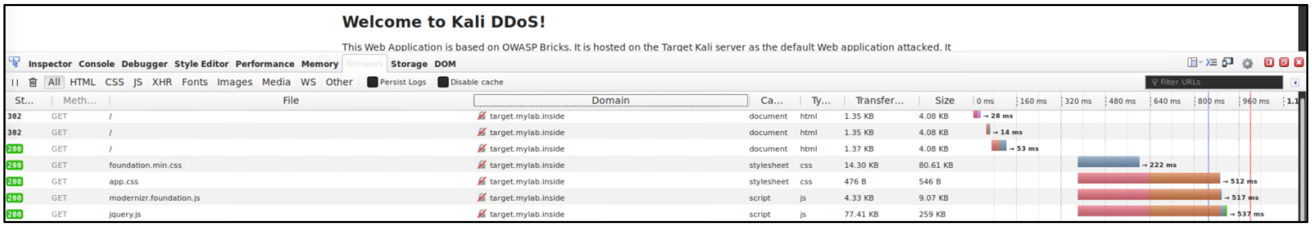
Average Attack Rate (pps)	Attack Duration [Hour:Min:Sec]	Activation Threshold (pps)	TCP Challenge	TCP Auth. List (%)
73453	00:01:44	0	-	0
HTTP Challenge	HTTP Auth. List (%)			
-	1			

For SYN flooding DP does not record source IP information!

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



7. Now let's experience the redirect on a legitimate client.
   Connect to the **Legit Client** and start the FireFox browser
8. Open the developer tools (F12) and surf to the target server using the bookmark in the favorites toolbar called "Bricks HTTP".

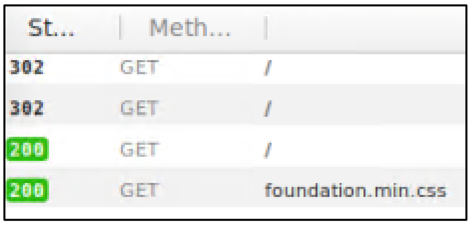


Welcome to Kali DDoS!

This Web Application is based on OWASP Bricks. It is hosted on the Target Kali server as the default Web application attacked. It

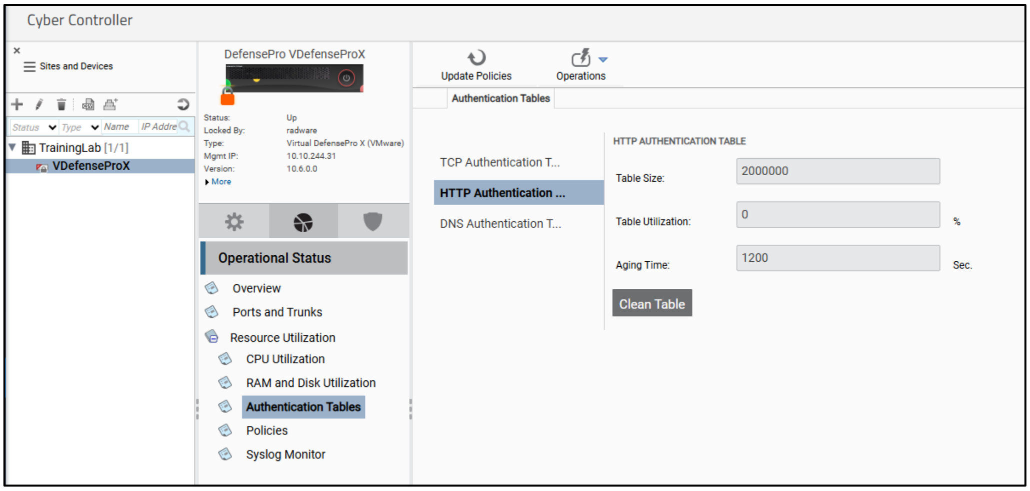
St...	Meth...	File	Domain	Ca...	Ty...	Transfer...	Size	
302	GET	/	target.mylab.inside	document	html	1.35 KB	4.08 KB	→ 28 ms
302	GET	/	target.mylab.inside	document	html	1.35 KB	4.08 KB	→ 14 ms
200	GET	/	target.mylab.inside	document	html	1.37 KB	4.08 KB	→ 53 ms
200	GET	foundation.min.css	target.mylab.inside	stylesheet	css	14.30 KB	80.61 KB	→ 222 ms
200	GET	app.css	target.mylab.inside	stylesheet	css	476 B	546 B	→ 512 ms
200	GET	modernizr.foundation.js	target.mylab.inside	script	js	4.33 KB	9.07 KB	→ 517 ms
200	GET	jquery.js	target.mylab.inside	script	js	77.41 KB	259 KB	→ 537 ms

The two 302 redirects are part the http challenge we enabled.



St...	Meth...	
302	GET	/
302	GET	/
200	GET	/
200	GET	foundation.min.css

9. If you want to see the redirect challenge again, connect on to the **DP configuration > Monitoring > Operational Status > Resource Utilization > Authentication Tables > HTTP Authentication** and click on **Clean Table**.



DefensePro VDefenseProX

Status: Up
Locked By: radware
Type: Virtual DefensePro X (VMware)
Mgmt IP: 10.10.244.31
Version: 10.6.0.0
More

HTTP AUTHENTICATION TABLE

Table Size: 2000000

Table Utilization: 0 %

Aging Time: 1200 Sec.

10. At Raptor **Stop** the attack.
11. **Export** and save configuration file as **dpx-SYNLab-config**.

For questions, contact training@Radware.com