DefensePro X
Version 10.x

Training Lab Manual
Configure BDoS DNS

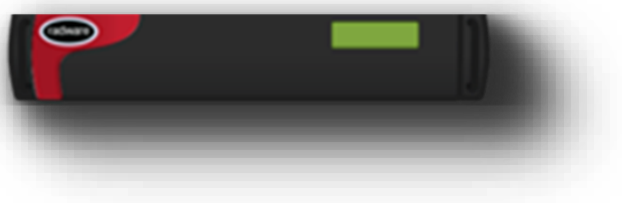


Table of Contents

Contents

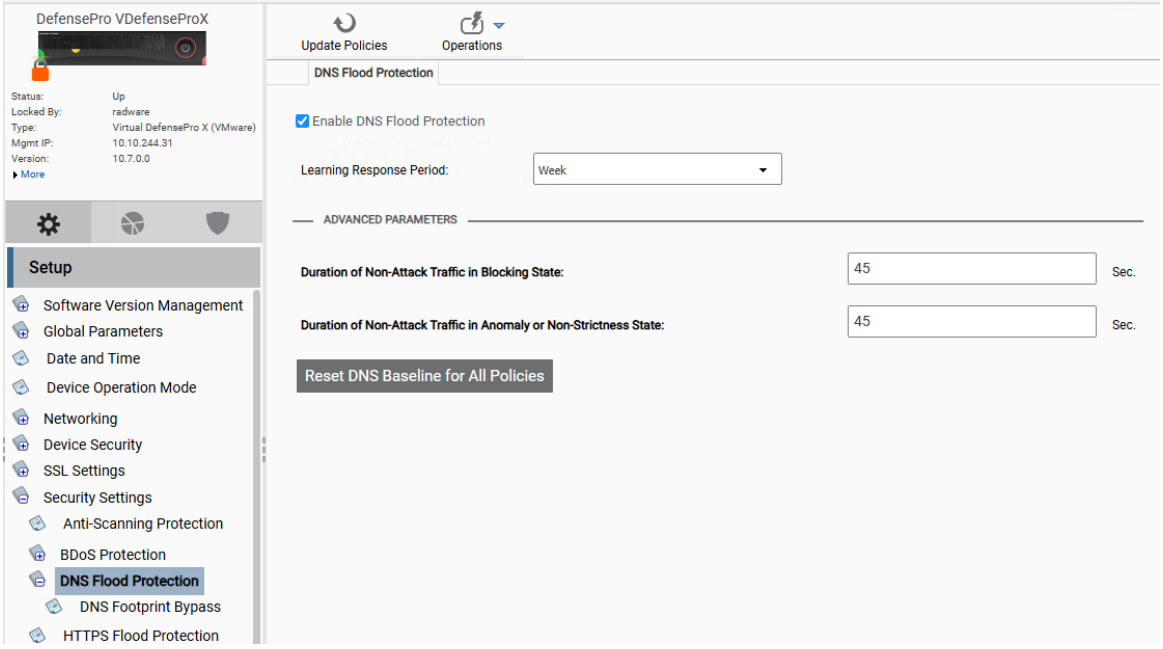
Overview

Radware DefensePro X 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 X device.
This guide is for DefenseProX 10.5 and later, since in 10.5 the DNS protection was updated.

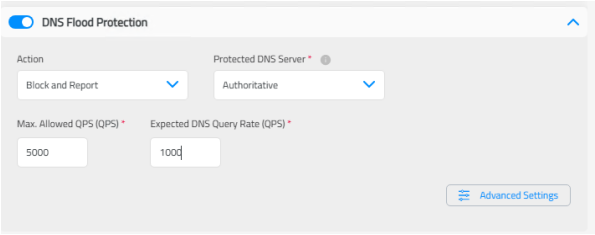
Setup DNS Flood Protection

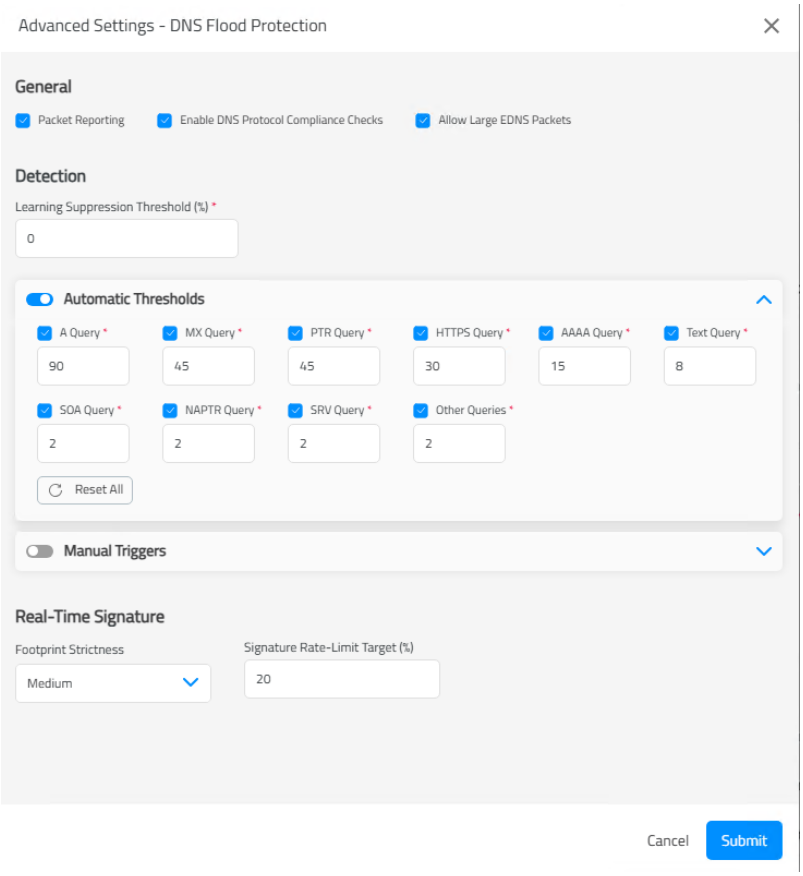
1. Access **Cyber Controller**
2. Select the DefensePro **Configuration** perspective.
3. In **Setup** section, select **Security Settings → DNS Flood Protection** on navigation tree
4. In the **DNS Flood Protection** tab verify that the **Enable DNS Flood Protection** checkbox is checked.
5. Configure **Learning Response Period** as: ***Week***
6. Set Duration of **Non-attack Traffic in Blocking State**: ***45*** and **Duration of Non-attack Traffic in Anomaly or Non-Strictness State**: ***45***
   Depending on software version this is the default.
7. Click **Submit** button to save changes.



Configure DNS Flood Protection

1. Select in the CyberController left menu the **Security Operations → Security Settings** perspective or use the **Security Operations Dashboard (Real-Time Monitoring)**.
2. Edit the ***TeamXX*** policy.
3. Enable **DNS Flood Protection**.
4. Expand the DNS Flood Protection section.
5. Configure:
    - **Protected DNS Server**: ***Authoritative***
    - **Max Allowed QPS**: ***5000*** QPS
    - **Expected DNS Query Rate**: ***1000*** QPS
    - **Advanced Settings** → enable **Automatic Thresholds and enable all query types**
    - **Advanced Settings → Footprint Strictness:** ***Medium***
    - **Advanced Settings → Signature Rate-Limit Target**: ***20%***
6. Click **Submit** button to close the Advanced Settings.
7. Click **Submit** button to apply the changes.
8. Make sure on the Legit client the jMeter is running with the background traffic including DNS traffic.





Add a Manual Allowlist Entry

The DefensePro is learning during peacetime the regular queried DNS entries, but in some situations we need to manually add entries to the 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++). The m marks this entry as a manual entry.
2. Go to DefensePro **Configuration perspective Protections → Protection Policies** and edit your policy containing the DNS Flood profile.
3. In the **DNS Handling** tab click **Browse** at *DNS Subdomains Allowlist to Import*.
4. Select your **allowlist.txt** and click **Import**.

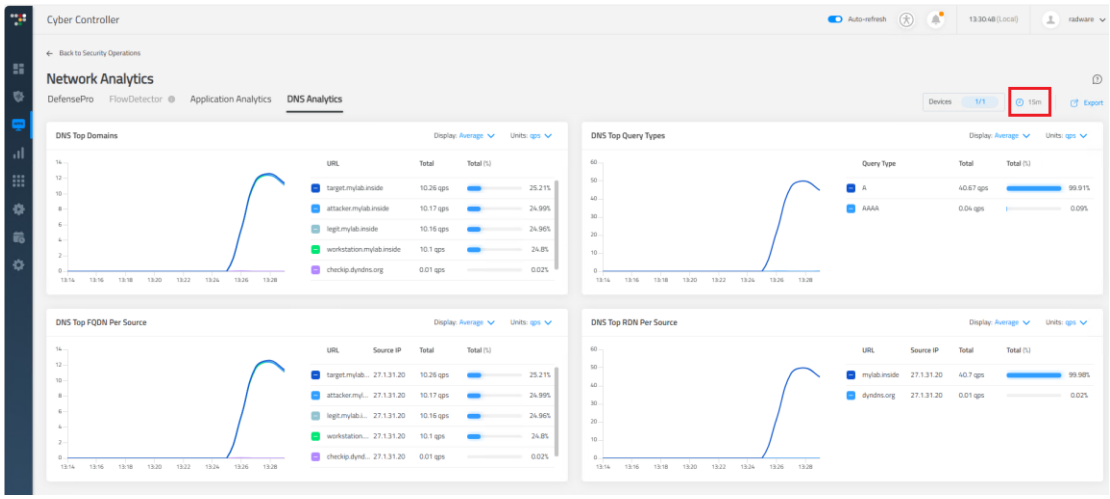
Note: Importing a Subdomains Allowlist file is performed without having to run the Update Policies command.

5. Wait a few minutes before you continue.
6. At the DNS Handling tab and click on **Export > All Entries** to see the entry you generated and also the already learned values. You only will see values if you have started the legitimate traffic in the initial lab, since part of it are DNS queries. If you didn't performed that, start the legitimate traffic now (see initial lab guide how to do it) and wait a few minutes and export the file again.

   You should see the following entries
   a. www.mydomain.com,m
   b. target.mylab.inside,a
   c. attacker.mylab.inside,a
   d. legit.mylab.inside,a
   e. workstation.mylab.inside,a

Check DNS Analytics

1. Select in the CyberController left menu the **AMS Analytics → Network Analytics**.
2. Select DNS Analytics and change the time to the last 15 minutes, you should see the DNS names.



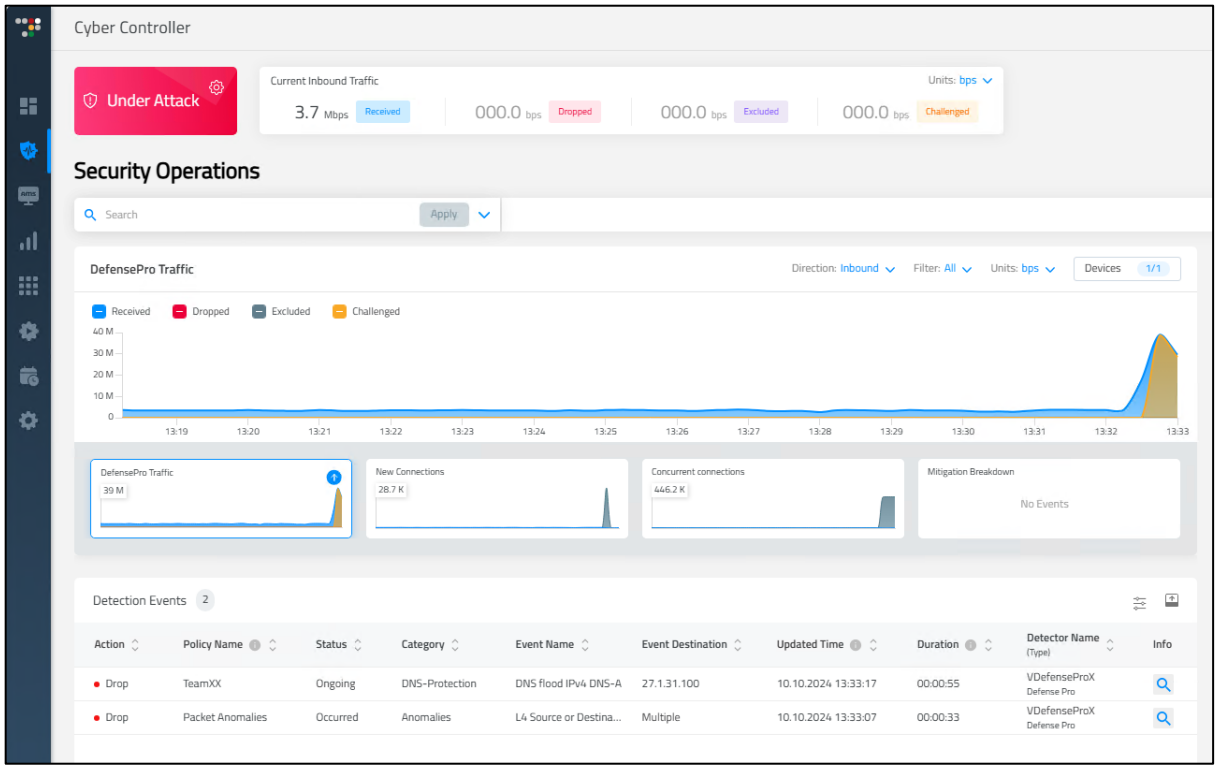
Test the Configuration

Use Raptor to send DNS Flood Attack

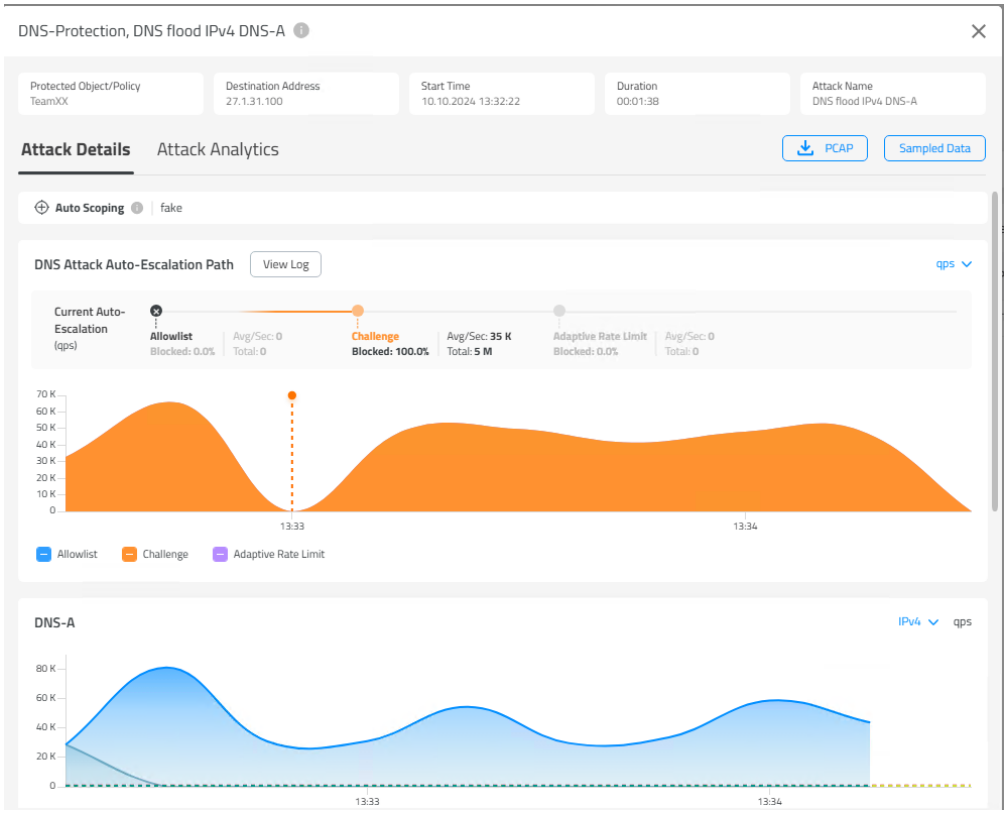
1. Access **Attacker-PC Raptor** main menu select **Services Attacks → DNS → Flooding**.
2. Verify/Enter Destination IP address: **27.1.31.100** Keep default domain name (i.e. **example.fake**)
3. Click **OK** to start attack.

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.

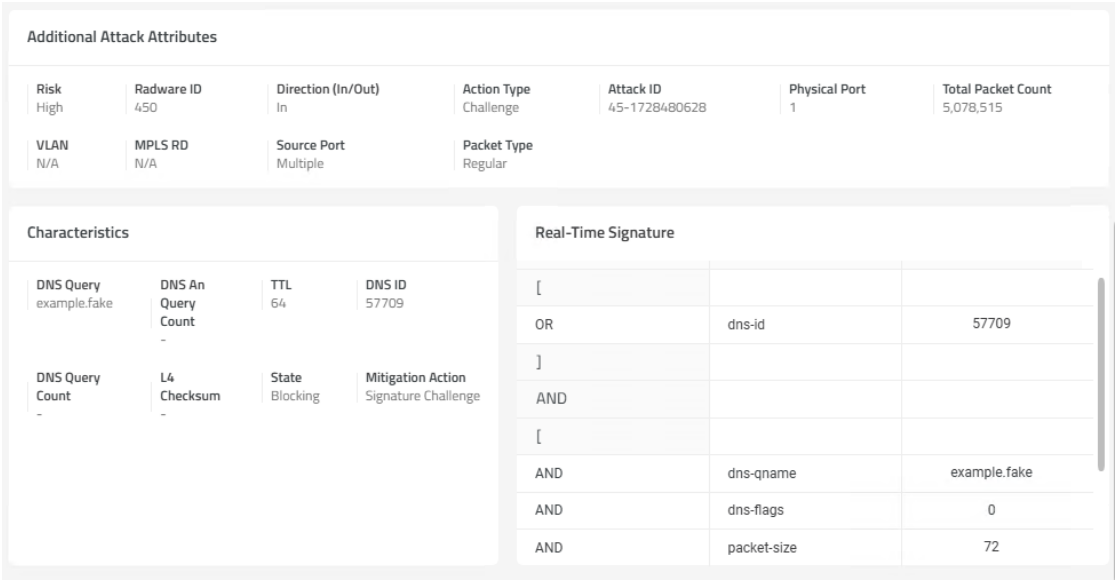
4. Use Cyber Controller to View DNS Flood Attack. Select the **Security Operations → Real-Time Monitoring**..



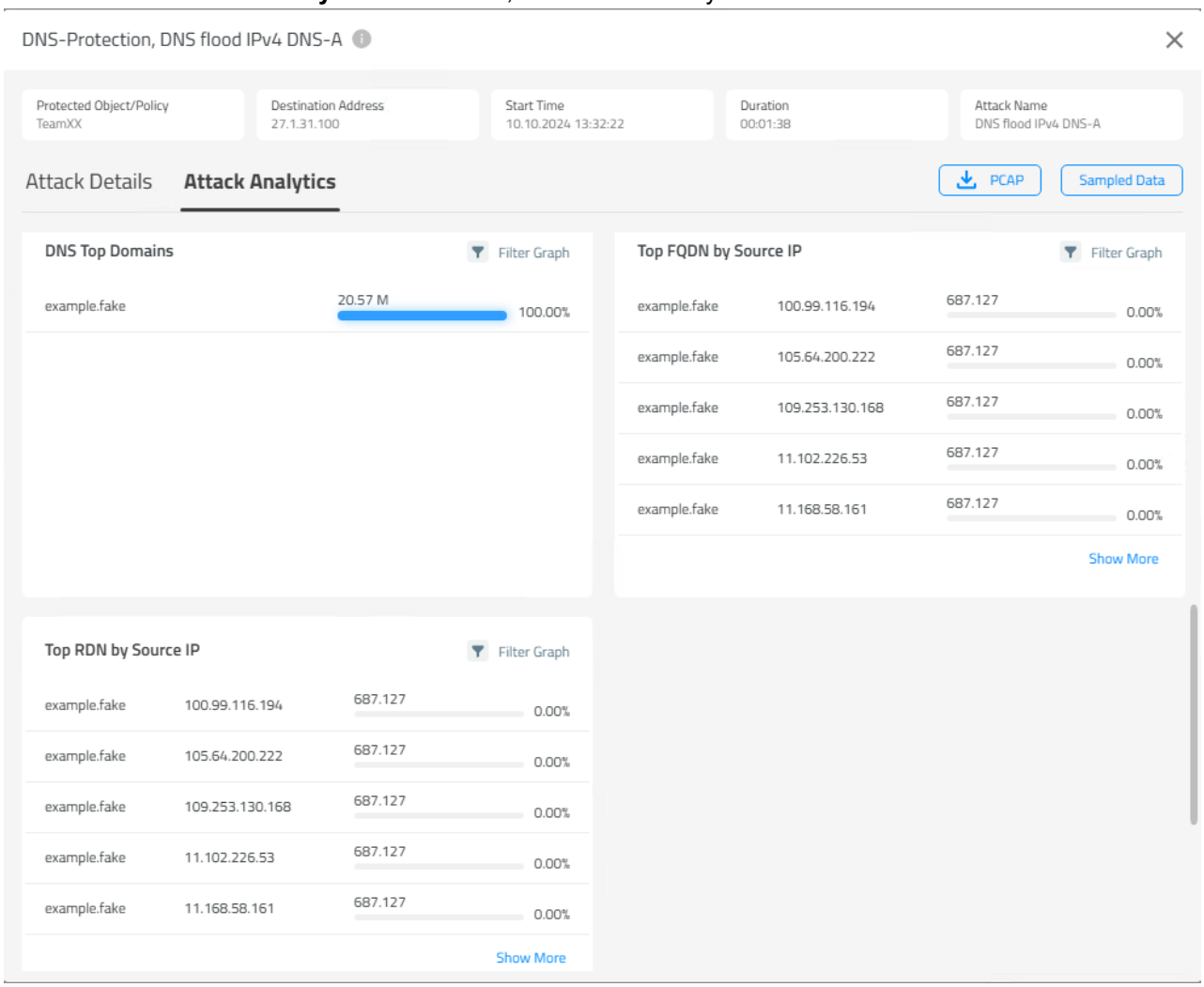
5. Select your event in **Detected Events** section and click on info/maginfying glass icon. Notice the DNS-A attack traffic is challenged and the protection is focused/scoped on the domain called **fake**, which we attack.



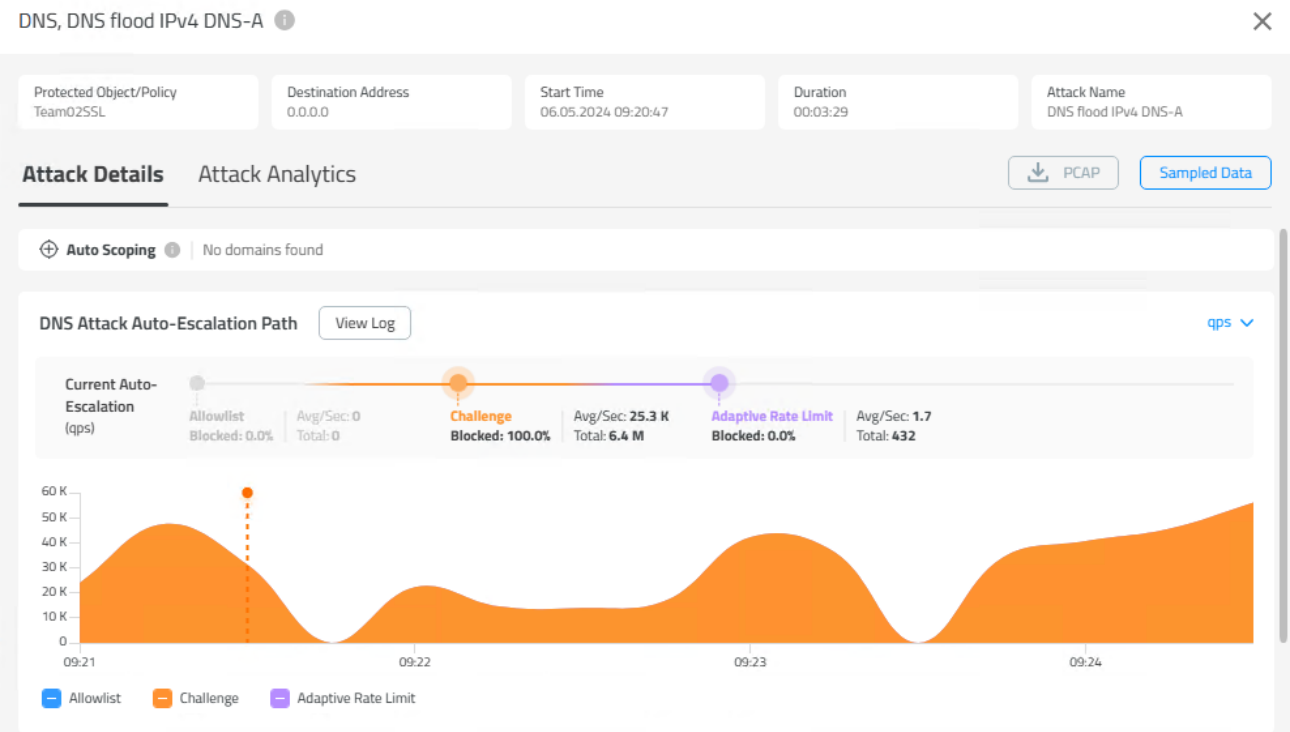
6. Scroll down to see the Real-Time Signature and other attack details.



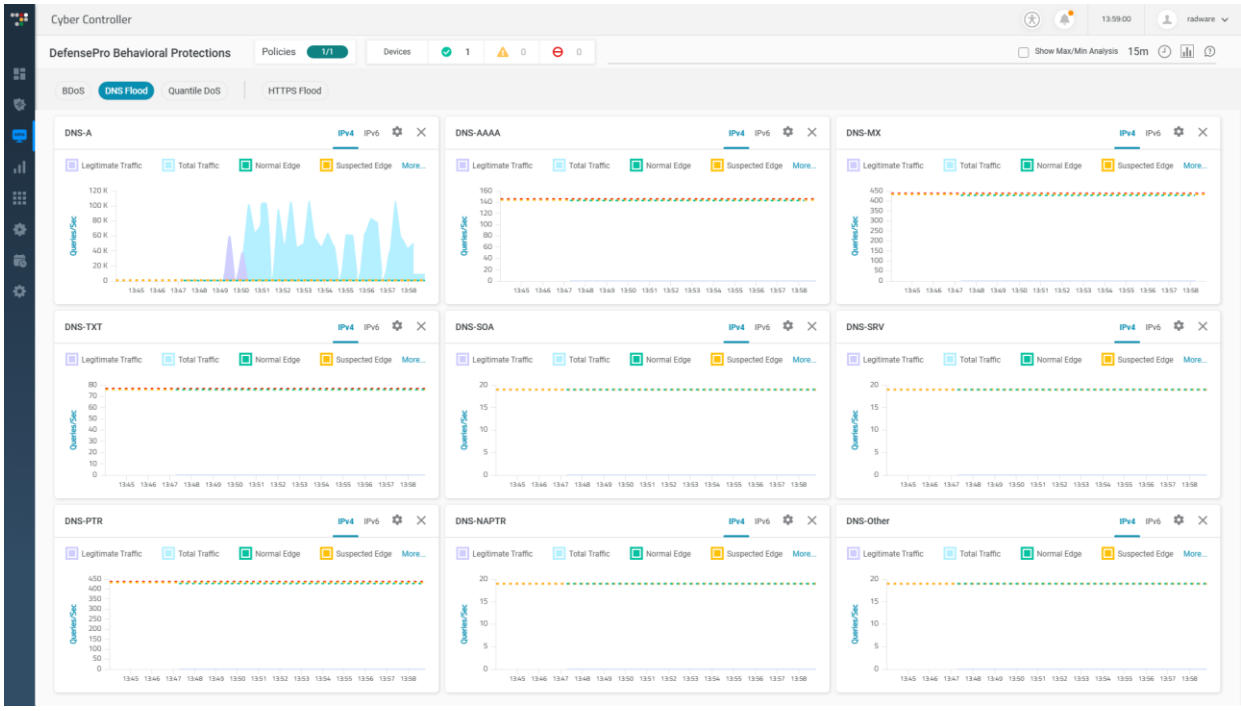
7. Also review the **Attack Analytics** information, scroll down until you see the DNS related information collected



8. Wait a few minutes and click on the attack again, you will see if it went to the next excalation phase (not in our lab):



9. Select **Analytics AMS → DefensePro Behavioral Protections → DNS Flood**
10. Select your policy under the **Policies** to see the details. In our lab we only see DNS-A records, since the attack and the legit traffic is only DNS-A record requests.



11. At Raptor **Stop** the attack.

Import The Allowlist Via Zone Transfer

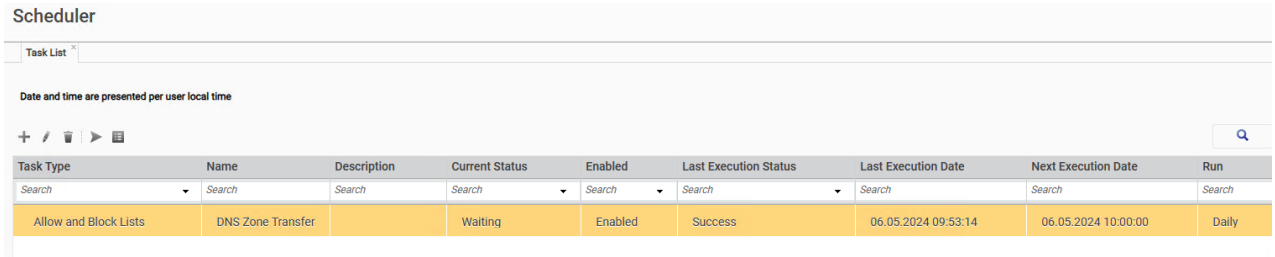
Now we want to see how to use the scheduler in the Cyber Controller, to grep the allowed DNS entries from a DNS server and use it in the DNS allow list.

1. At the Legit Client stop the jMeter so the system don't learn any entries.
2. Go to DefensePro **Configuration perspective Protections → Protection Policies** → Select your policy → **DNS Handling** → **Delete** and click on ***All Entries***
3. Now export all entries, to see the list is empty.
4. Go to the Schedular in Cyber Controller

5. Create a new entry using the below information:

Configure Allow and Block Lists Scheduler Task	
Point	**Value**
Task Type	Allow and Block Lists
Name	DNS Zone Transfer
Subtype	DNS Allowlist
Schedule	Run → Daily 10:00:00
Manual Entries	Add Manual Entries: www.radware.com
Remote Server Settings	Format: **DNS Zone Transfer** DNS Server: **27.1.31.100** Domain Names: mylab.inside radware.inside
Target List	Select your DP and your DNS policy

6. Click **Submit**
7. We don't want to wait until the next day. Select your task and click the run button .
8. Check if you see the Last Excution Status is Success



9. Now let's see if the transfer was really successful by exporting the list.
   Go to DefensePro **Configuration perspective Protections → Protection Policies** → Select your policy → **DNS Handling** go to Export → All Entries.

10. The exported file should be like:

VDefenseProX_Team02SSL_dns_allowlist_06052024_095523 - Notepad

File Edit Format View Help

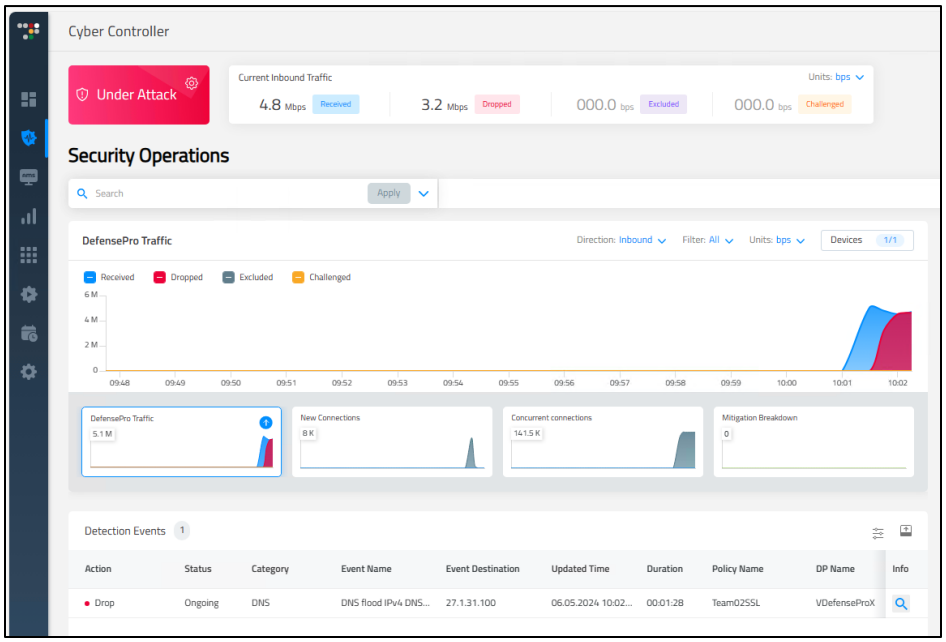
```
workstation.radware.inside,m
workstation.mylab.inside,m
exchange.radware.inside,m
attacker.radware.inside,m
attacker.mylab.inside,m
target.radware.inside,m
target.mylab.inside,m
legit.radware.inside,m
legit.mylab.inside,m
mail.radware.inside,m
kali.radware.inside,m
kali.mylab.inside,m
www.radware.inside,m
www.radware.com,m
```

Test the Configuration

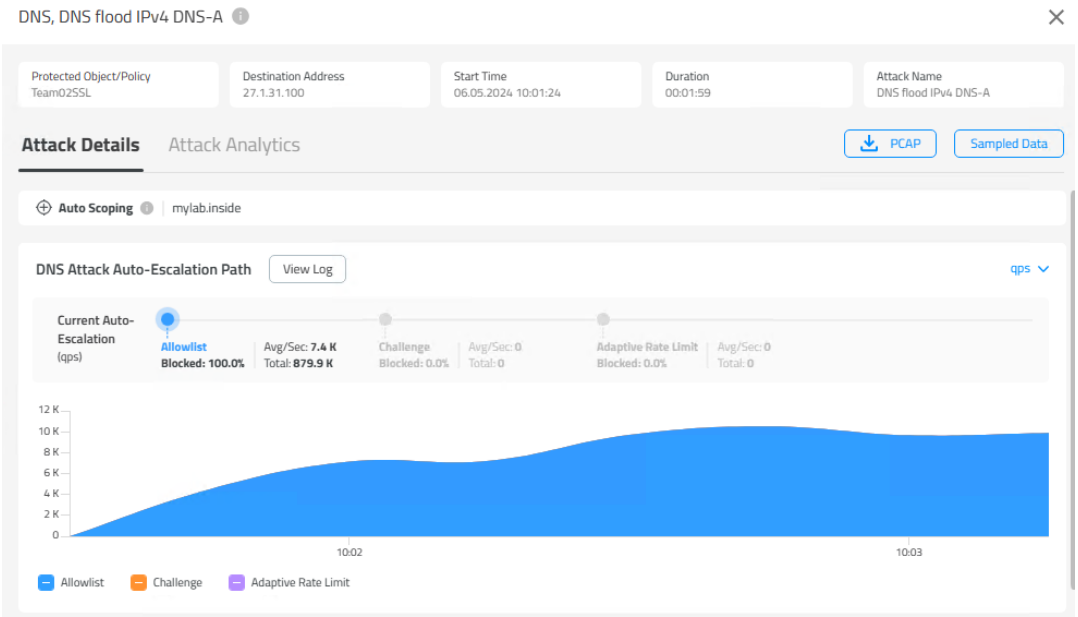
Use Raptor to send DNS Flood Attack

1. At the attacker use the command prompt to type the follwoing commands, which will run a water tourture attack.
```
cd  /opt/radware/attacks
python3 DNS_Subdomain_Attack_python3.py -i 27.1.31.100 -r -d mylab.inside
```

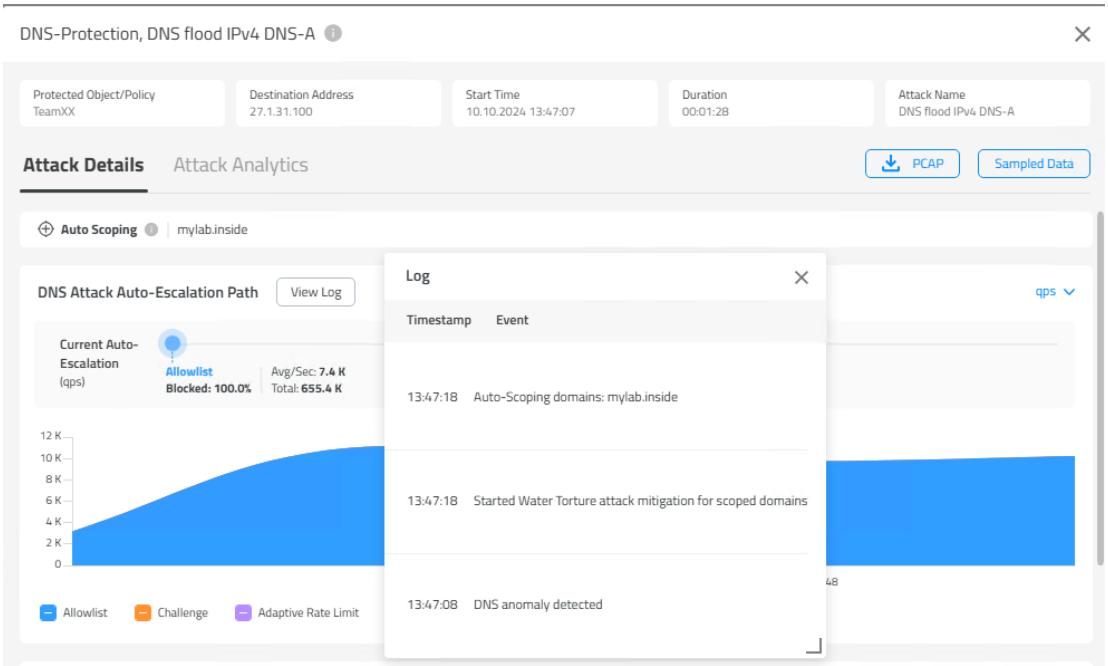
2. Use Cyber Controller to View DNS Flood Attack. Select the **Security Operations → Real-Time Monitoring**..



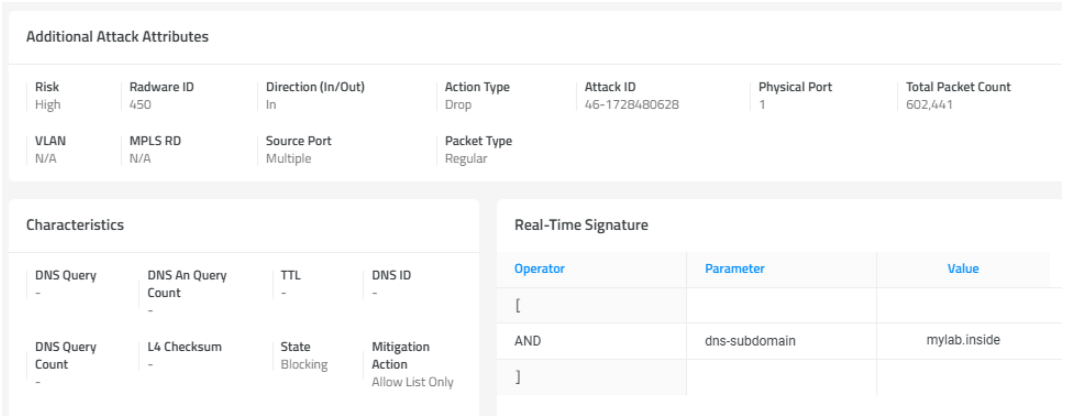
3. Check the Attack Details, the attack is mitigated using the allow list we imported.



4. Click on the View Log icon to see that the Water Torture attack was identified.

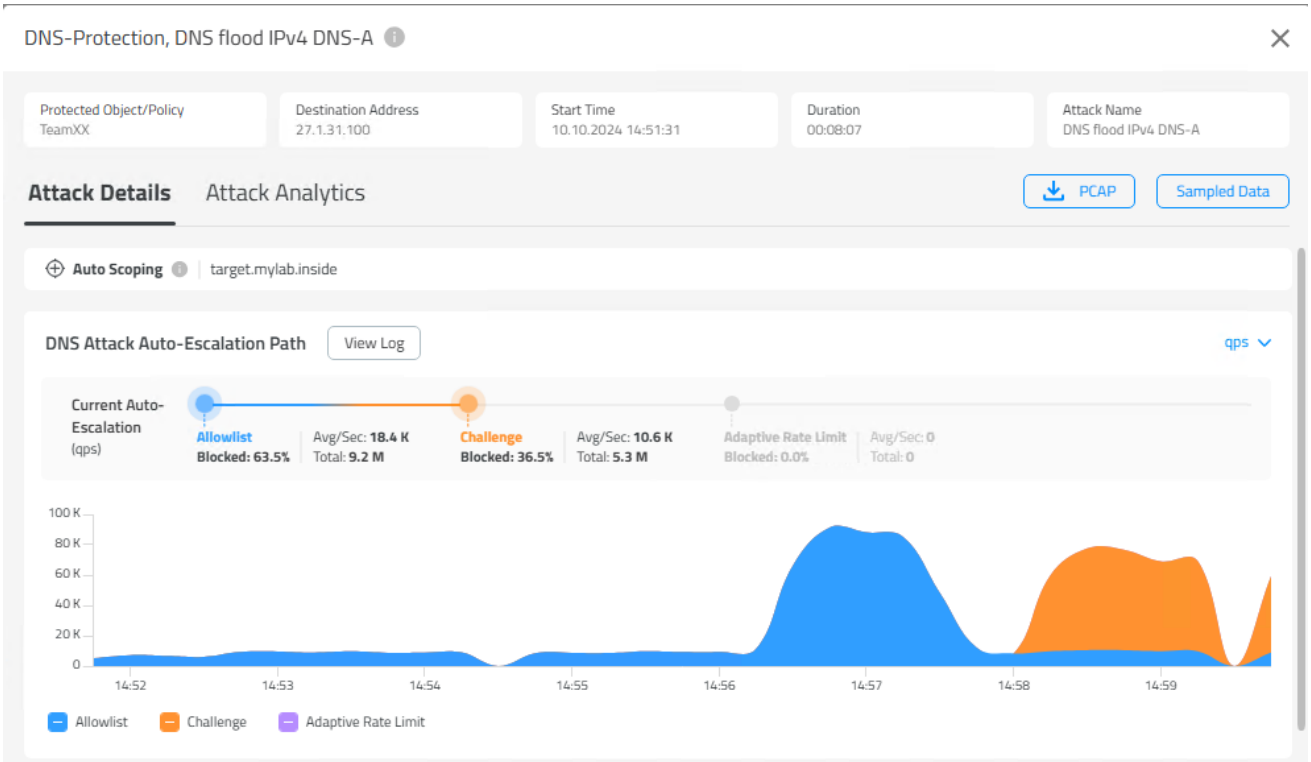


5. Scroll down to see the Characteristics

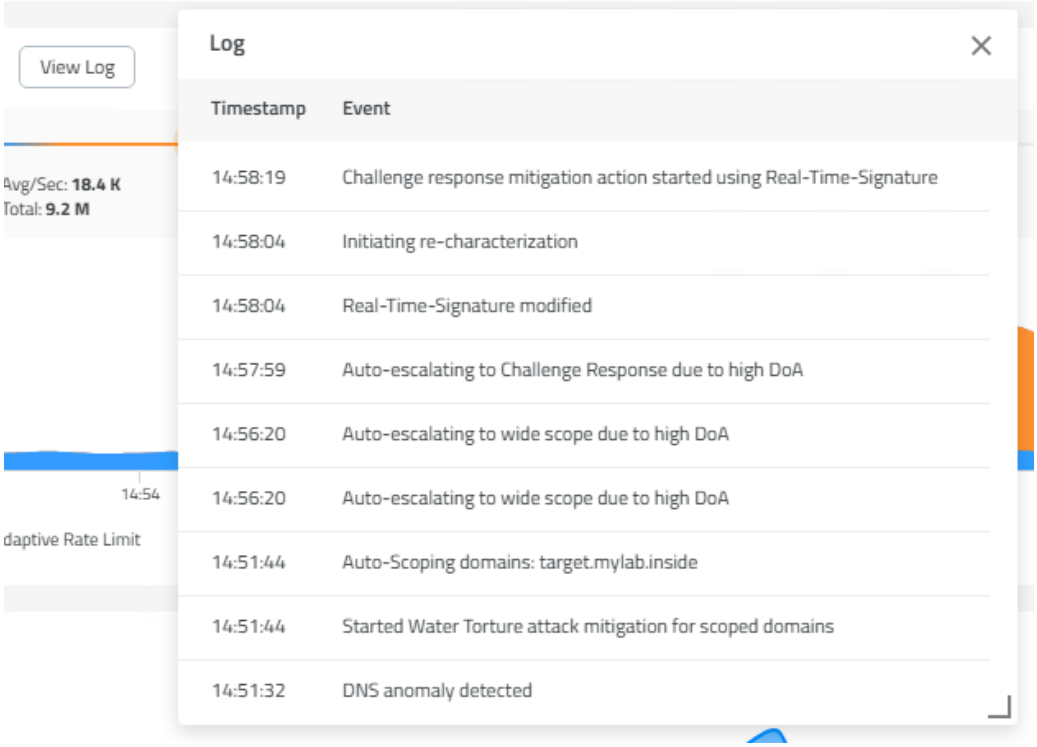


6. Now let's change the attack.
7. Go to the attacker and use the raptor to run a DNS flooding attack to target.mylab.inside, which is part of the allow list.

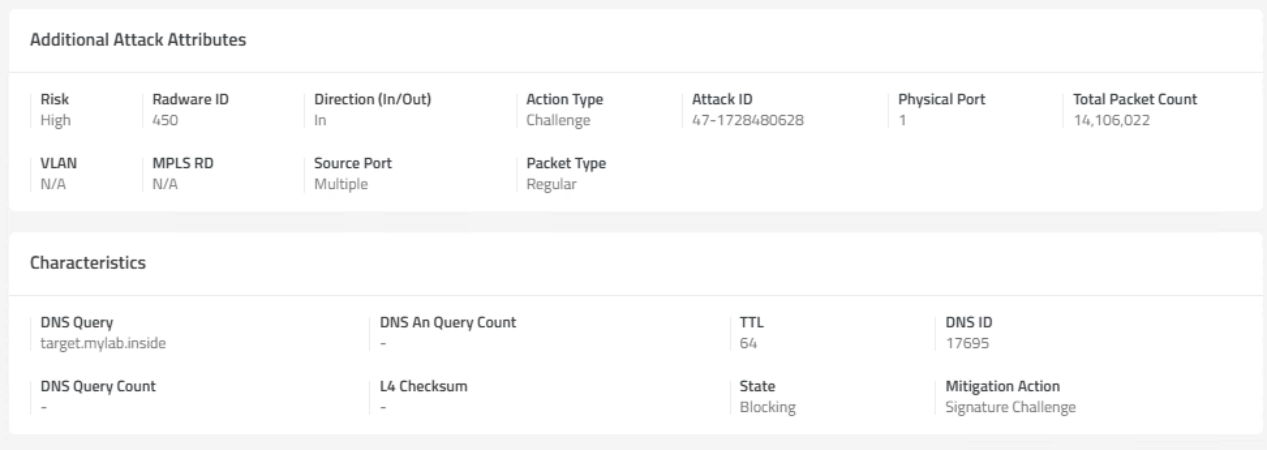
8. The attack should now be escalated to the Challenge phase.
   Check the attack details now



9. Check the Log file as well and expand to make sure you can read all lines using



10. And also the Additional Attack Attributes and Characteristics



Additional Attack Attributes

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	450	In	Challenge	47-1728480628	1	14,106,022

VLAN	MPLS RD	Source Port	Packet Type
N/A	N/A	Multiple	Regular

Characteristics

DNS Query	DNS An Query Count	TTL	DNS ID
target.mylab.inside	-	64	17695

DNS Query Count	L4 Checksum	State	Mitigation Action
-	-	Blocking	Signature Challenge

11. Stop the attacks and after a few minutes you should see Peacetime again.
12. Save the DP configuration if you want.

13.

For questions, contact training@Radware.com