

# **DefensePro X v1.5.1**

## **Demo Lab Guide**

*Last Update: 12.05.2024*

## TABLE OF CONTENTS

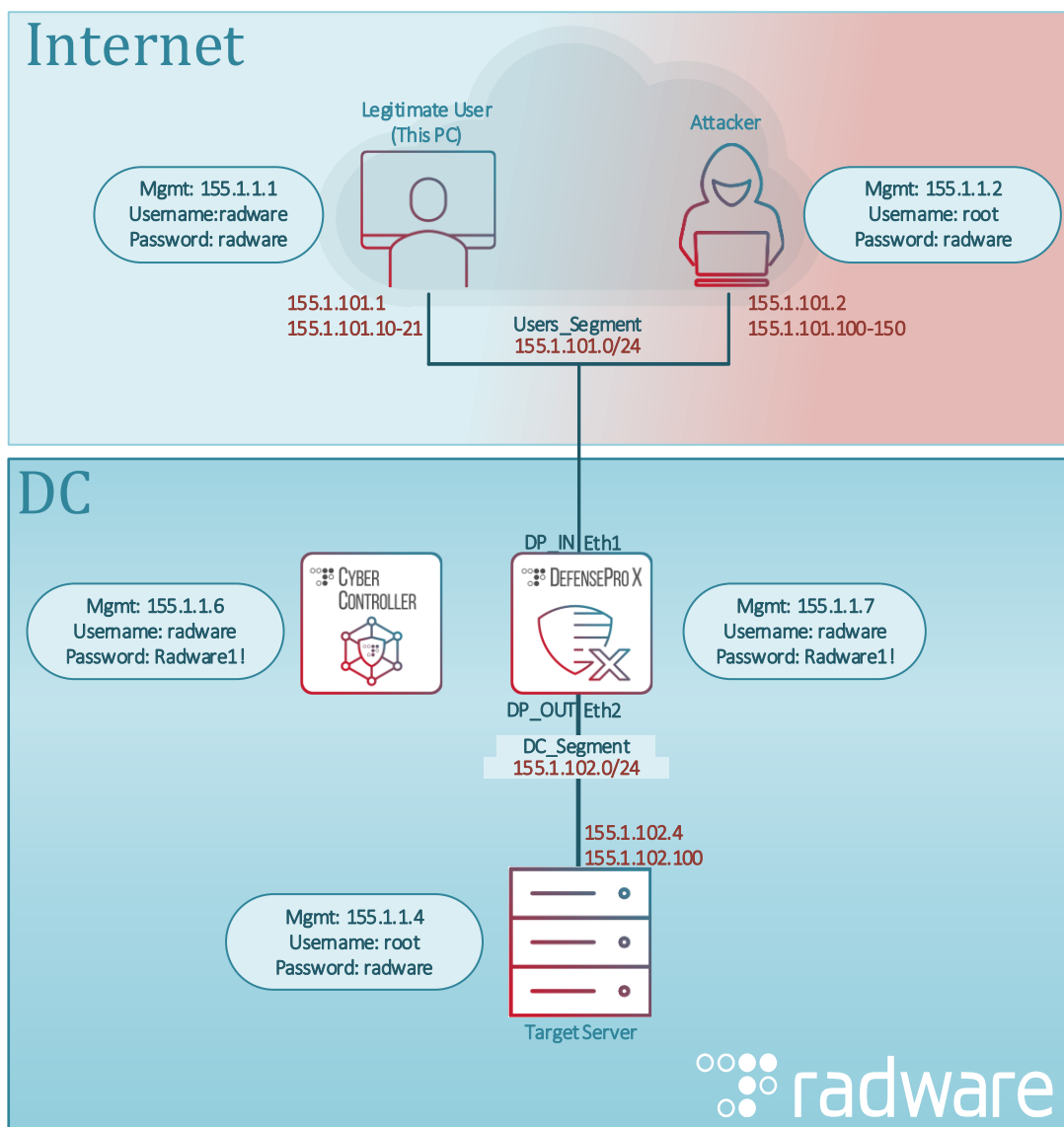
<b>TABLE OF CONTENTS</b> .....	<b>2</b>
<b>LAB ENVIRONMENT</b> .....	<b>5</b>
<b>Topology Data Segment</b> .....	<b>5</b>
<b>Topology Management Segment</b> .....	<b>6</b>
<b>Lab Environment Credentials</b> .....	<b>6</b>
<b>Management (MGT) Station</b> .....	<b>7</b>
Connecting the environment devices and running attacks .....	7
<b>Legitimate Traffic Generation</b> .....	<b>8</b>
Generating Traffic with JMeter .....	8
Verify legit traffic on the Cyber Controller Dashboards.....	9
<b>Attack Generation Tool</b> .....	<b>12</b>
<b>DefensePro X High-Level Configuration Overview</b> .....	<b>12</b>
DefensePro X Network Protection Policies .....	12
<b>DEFENSEPRO X DEMO LAB SCENARIOS</b> .....	<b>14</b>
<b>DNS Authoritative Protection</b> .....	<b>14</b>
Scenario Topology.....	15
Running Legitimate Traffic .....	16
DNS Attacks .....	17
Packet Capture .....	23
<b>TLS Fingerprint Protection</b> .....	<b>25</b>
Legit Traffic & Baseline Adjustment .....	25
TLS Attacks .....	27
<b>HTTPS Protection</b> .....	<b>31</b>
HTTPS Baseline Adjustment .....	31
Start the HTTPS Flood Attack from Kali and Verify Detection .....	33
Attack Mitigation .....	34

<b>Traffic Filters .....</b>	<b>39</b>
Create an HTTP Page Scanning Attack from Kali and Verify Detection .....	39
Attack Mitigation .....	40
<b>ERT Active Attacker Feed Protection.....</b>	<b>43</b>
Start a UDP Flood Attack and Verify Detection.....	43
Attack Mitigation .....	44
<b>Spoofed Syn Attack Protection.....</b>	<b>46</b>
Start a Spoofed Syn Flood Attack And verify Detection .....	46
Attack Mitigation .....	47
<b>BDoS Protection .....</b>	<b>49</b>
Create a UDP Flood Attack and Verify Detection .....	49
Attack Mitigation .....	50
<b>BDoS Advanced UDP Protection .....</b>	<b>54</b>
Start Legitimate Traffic.....	54
Start a UDP Flood Attack .....	54
Attack Mitigation .....	56
Start a UDP Flood Flash Crowded Legit Traffic .....	59
Verify Flash Crowded Isn't Getting Blocked .....	60
<b>DNS Flood Protection .....</b>	<b>61</b>
Start DNS Legitimate Traffic .....	61
Start a DNS NX Domain Flood Attack and Verify Detection .....	64
Attack Mitigation .....	65
<b>APPENDIX 1 - HTTPS PROTECTION (ADDITIONAL INFO) .....</b>	<b>68</b>
<b>Protection Overview.....</b>	<b>68</b>
<b>Scenario Steps Overview .....</b>	<b>68</b>
<b>Configurations .....</b>	<b>70</b>
<b>APPENDIX 2 - TRAFFIC FILTERS (ADDITIONAL INFO).....</b>	<b>71</b>
<b>Protection Overview.....</b>	<b>71</b>
<b>Scenario Steps Overview .....</b>	<b>72</b>

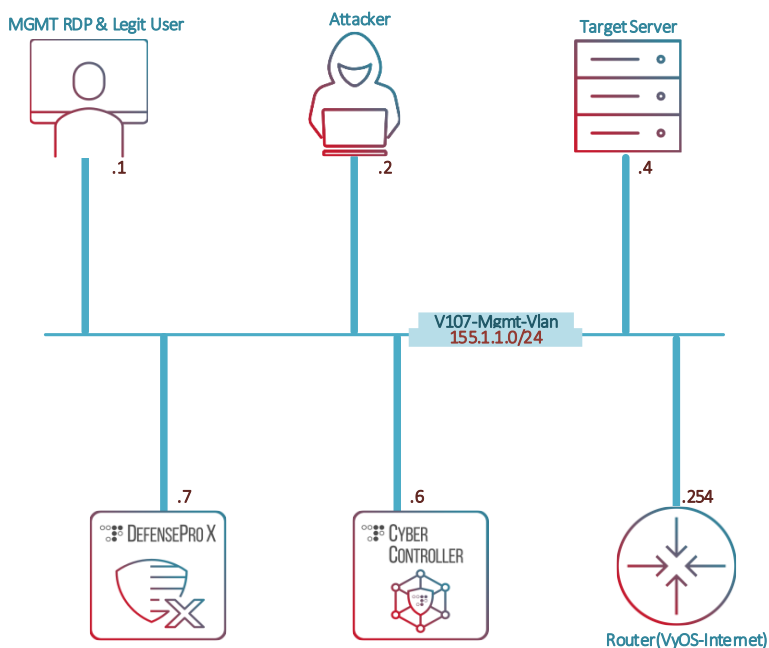
Configurations .....	73
<b>APPENDIX 3 - ERT ACTIVE ATTACKER FEED PROTECTION (ADDITIONAL INFO).....</b>	<b>77</b>
Protection Overview.....	77
Scenario Steps Overview .....	77
Configuration .....	78
<b>APPENDIX 4 - SPOOFED SYN ATTACK PROTECTION (ADDITIONAL INFO) .....</b>	<b>80</b>
Protection Overview.....	80
Scenario Steps Overview .....	80
Configurations .....	82
<b>APPENDIX 5 - BDOS PROTECTION (ADDITIONAL INFO).....</b>	<b>84</b>
Protection Overview.....	84
Scenario Steps Overview .....	84
Configurations .....	86
<b>APPENDIX 6 - BDOS ADVANCED UDP PROTECTION (ADDITIONAL INFO).....</b>	<b>89</b>
Protection Overview.....	89
Scenario Steps Overview .....	89
Configurations .....	91
<b>APPENDIX 7 - DNS FLOOD PROTECTION (ADDITIONAL INFO) .....</b>	<b>94</b>
Protection Overview.....	94
Scenario Steps Overview .....	94
Configurations .....	95
<b>APPENDIX 8 - HTTPS TRAFFIC GENERATION TEMPLATE (ADDITIONAL INFO) .....</b>	<b>97</b>

## LAB ENVIRONMENT

### Topology Data Segment



## Topology Management Segment



## Lab Environment Credentials

Device	User	Password	MGMT IP
Cyber Controller	radware	Radware1!	Internal MGMT: 155.1.1.6
DefensePro X	radware	Radware1!	Internal MGMT: 155.1.1.7
Attacker	root	radware	Internal MGMT: 155.1.1.2
Target Server	radware	radware	Internal MGMT: 155.1.1.4
Grafana	radware	Radware1!	Internal MGMT: 155.1.1.4

## Management (MGT) Station

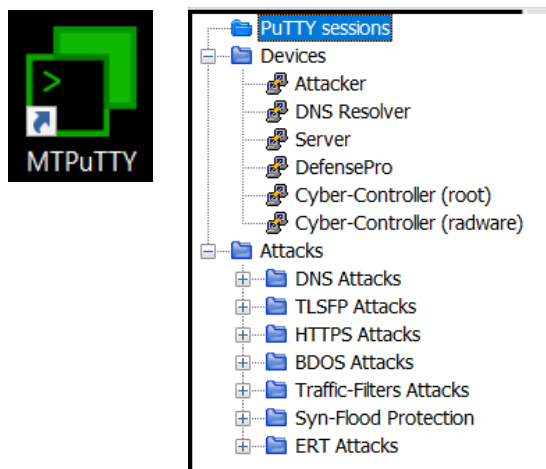
The demonstration is performed from the management station, which includes:

- Access to Cyber Controller
- Access to environment devices
- Legitimate traffic generation
- Attack traffic generation (via remote to attacker station)

The management station includes two network interfaces: one interface connects to the lab data segment, and the second interface connects to the management segment.

### ***Connecting the environment devices and running attacks***

We use the Management station to connect the rest of the lab devices with the help of Multi PuTTY Manager tool. To access the Multi PuTTY click the black icon in the task bar.



## Legitimate Traffic Generation

To generate legitimate traffic in the demo environment, use the management station. The management station uses the **JMeter** tool for HTTPS and DNS traffic generation.

Note: certain attacks have their own legit traffic, described in the relevant scenarios.

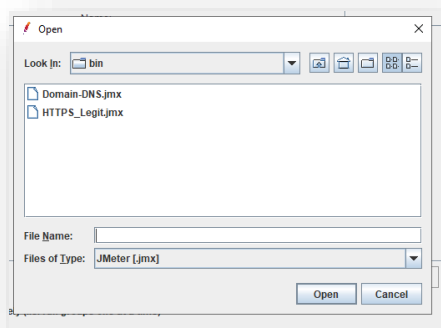
### Generating Traffic with JMeter

JMeter is a Java-based stress tool that is used in the demo lab to generate DNS and HTTPS requests from the legitimate host (management station) to the protected object in the policy, and for simulated HTTPS requests from authenticated and unauthenticated sources (Attackers) in the HTTPS protection scenario.

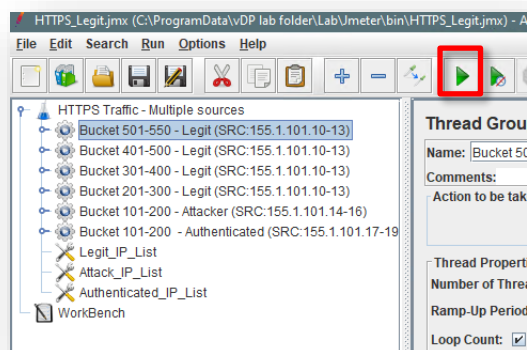
For more information regarding the buckets used in the HTTPS protection scenario [click here](#).

To load the profile template, do the following:

1. From the management station, click **JMeter**, which is located on the desktop.
2. Open the file menu → click on “open”.
3. Select the **JM legit script** folder:



4. Select the **HTTPS\_Legit.jmx** script.
5. To start the test traffic, after loading the template, click **Play**.





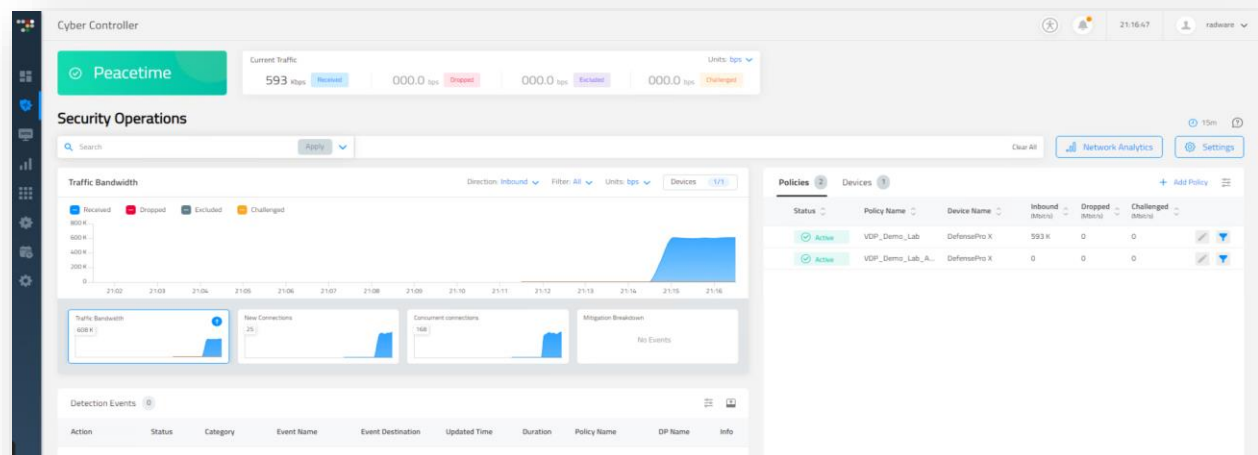
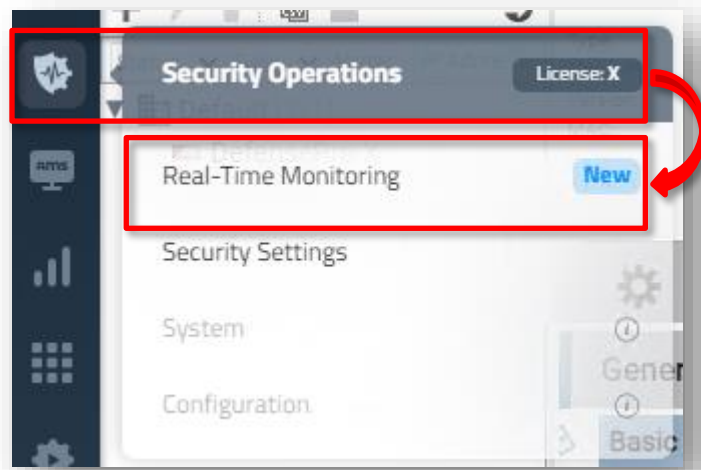
6. After the test runs, the number of running users displays at the upper right of the pane.
7. To stop the test traffic, click the red **x** button.

**Note:** some of the attacks includes specific legit traffic generation

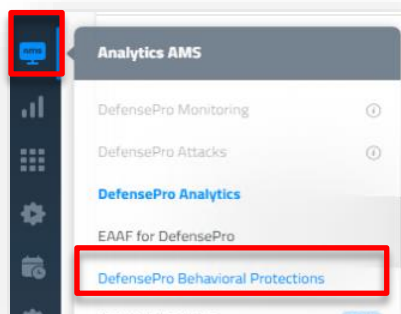
For the scenario of [DNS Flood Protection](#) and [BDoS Advanced UDP Protection](#), there is a different legit traffic, which is mentioned on the scenario section.

### **Verify legit traffic on the Cyber Controller Dashboards**

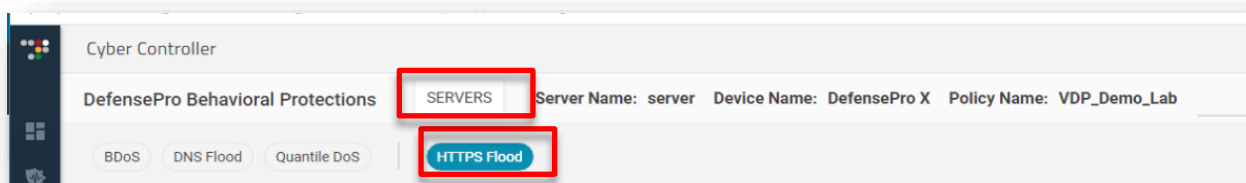
1. Once the legitimate traffic has started, it is displayed in the **Analytics AMS > DefensePro X Monitoring:**



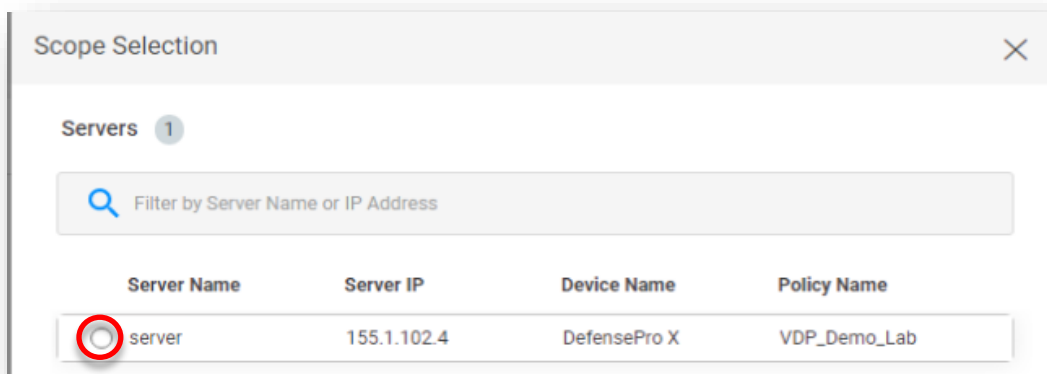
2. Verify the data on the HTTPS Flood dashboard. Go to **Analytics AMS > DefensePro X Behavioral Protections**:



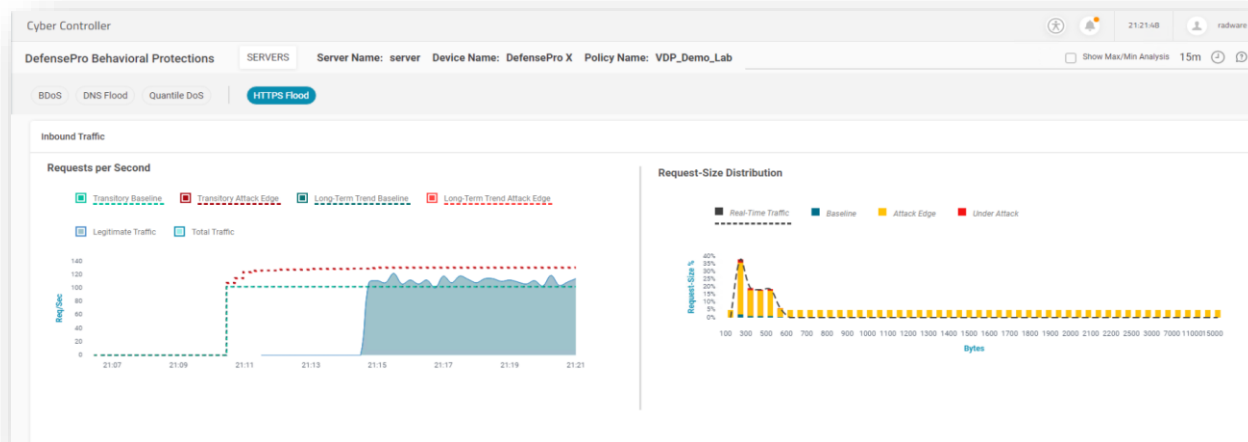
3. On the “**DefensePro Behavioral Protections**” page click on the “**HTTPS Flood**” button and then click on the “**Server**” button and choose “**Change Scope**”.



- On the “**Scope Selection**” window, choose the server with the IP “155.1.102.4” and click “Submit”.



- The HTTPS Flood dashboard includes a graph with all the buckets with more detailed information (such as attack edge, real-time traffic, baselines, and so on):



## Attack Generation Tool

The DefensePro X Demo lab includes the Kali Linux client as the attacking tool for all attack scenarios:

Kali is a well-known penetration machine that runs various types of attacks. The demo lab uses Kali to execute HTTPS, DNS, UDP floods, and page scanning attacks.

## DefensePro X High-Level Configuration Overview

### *DefensePro X Network Protection Policies*

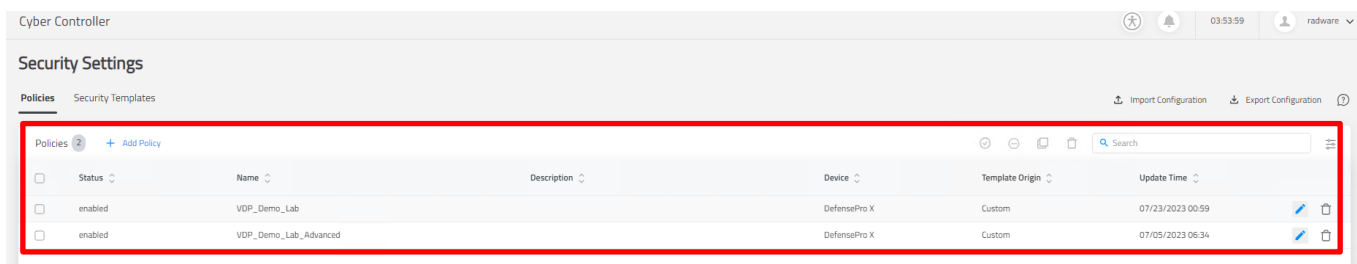
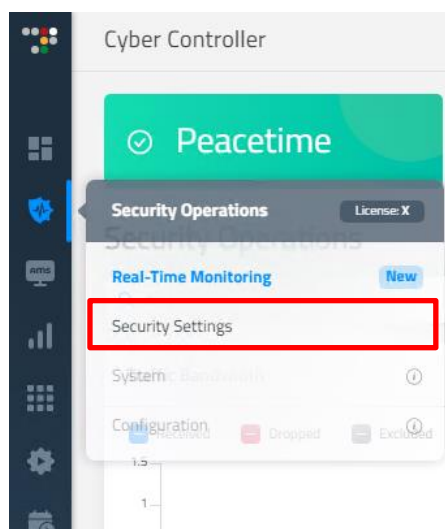
The following table provides a high-level overview of the DefensePro X demo lab configurations:

Protection Policy Name	Priority	Protected Object	Protections Profiles
VDP_Demo_Lab_Advanced	10	udp_server (155.1.102.100 /32)	<ul style="list-style-type: none"> <li>• BDoS (for the advanced UDP)</li> </ul>
VDP_Demo_Lab	5	Protected Webserver (155.1.102.4/32)	<ul style="list-style-type: none"> <li>• HTTPS</li> <li>• Traffic Filter</li> <li>• TLS Fingerprint</li> <li>• ERT Attacker Feed</li> <li>• Spoofed Syn Flood</li> <li>• DNS Flood</li> <li>• BDoS</li> </ul>

DefensePro X configurations include two major network protection.

To view the network protection configurations in Cyber Controller:

1. Go to **Security Operations > Security Setting**:



## DEFENSEPRO X DEMO LAB SCENARIOS

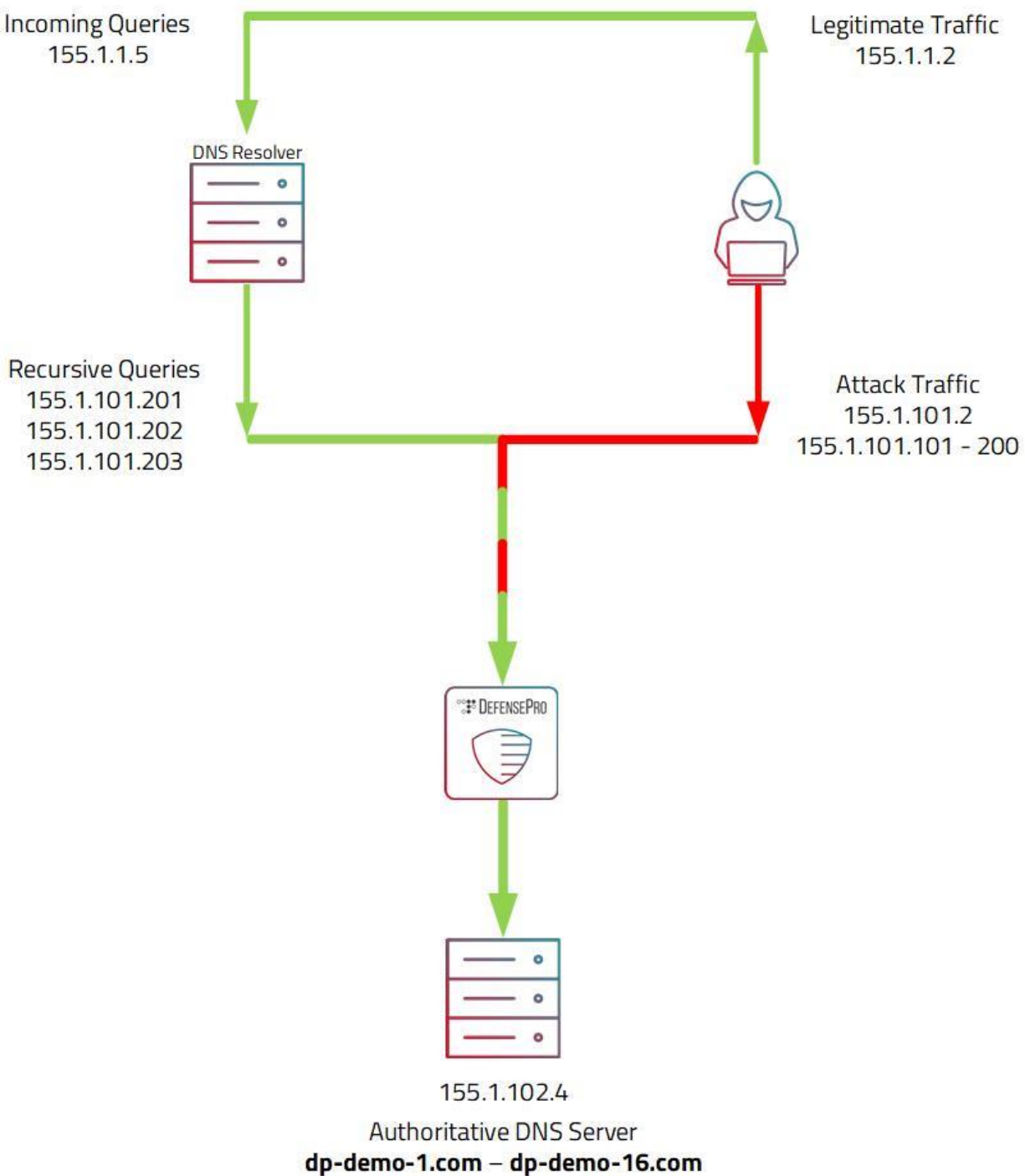
### DNS Authoritative Protection

In this scenario, we'll delve into the new protection for authoritative name servers, introduced in DefensePro X version 10.5. The updated DNS protection now encompasses two types of modes: Recursive, the familiar DNS protection from previous versions, and Authoritative, a new protection specifically designed for authoritative name servers which we will focus on.

Our scenario comprises of several components:

1. **Server:** This is our Authoritative DNS server, housing 16 zone files from **dp-demo-1.com** to **dp-demo-16.com**.
2. **Resolver** (newly introduced server): The resolver plays a crucial role in serving legitimate traffic and navigating the challenge/response mechanism introduced in the new Authoritative protection. This allows the protection to distinguish between legitimate resolvers and attackers. It's important to note that the resolver in our demo is configured to forward all requests to our Authoritative server when doing recursive lookups, and caching has been disabled, ensuring it performs recursive lookups for each request.
3. **Attacker:** responsible for generating both attack and legitimate traffic. Attack traffic is directed straight to the authoritative server, targeting the **dp-demo-1.com** domain exclusively. Legitimate traffic, on the other hand, is sent directly to the resolver, with queries distributed across all 16 domains on our authoritative server.
4. **Cyber-Controller:** configured with a scheduled task to retrieve all 16 zone files from our authoritative server and automatically configure them on the DNS Protection allow list. The new protection uses the DNS allow list first, it's essential to maintain a one-to-one representation of the zone files in the DefensePro allow list for proper mitigation without false positives.
5. **Grafana:** available in chrome bookmarks bar a link to Grafana dashboard. The dashboard displays graphs that offer insights into the types of queries and responses received by both the authoritative and resolver servers.

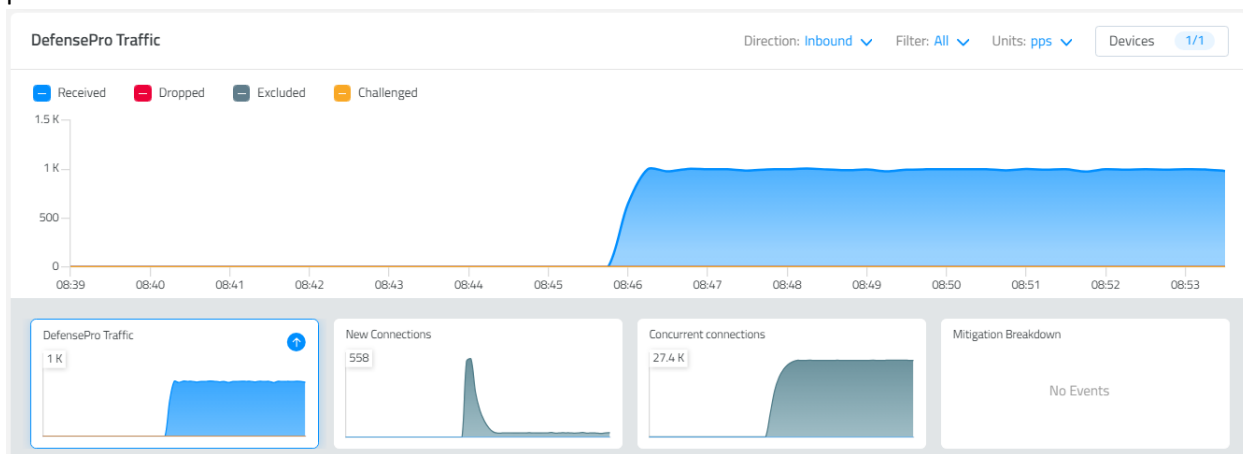
## Scenario Topology



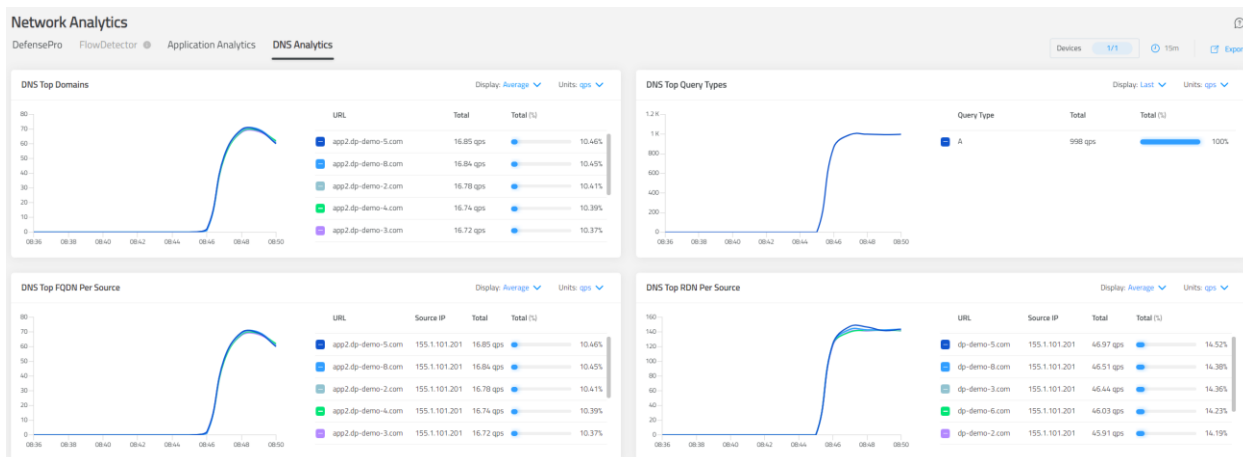
## Running Legitimate Traffic

To start legitimate traffic, open **MTPutty** and double-click on "**Start DNS Legit Traffic**". Our legitimate traffic is configured to run at a rate of 1000 Queries per Second and includes queries from all existing domains. This traffic is sent directly to the resolver, which then performs recursive lookups through our authoritative server.

When observing the Real-Time Monitoring screen and the units are displayed in PPS (Packets per Second), we can observe that we are receiving 1000 Packets per Second, equivalent to our 1000 Queries per Second.



Since Cyber-Controller 10.5, DNS Analytics has been added and can be accessed via the Network Analytics feature. Here, we can gain valuable insights into our legitimate traffic. We observe that we are sending only A queries from a single source, which is our resolver with IP address 155.1.101.201. Additionally, we can see that these queries span across all of our domains.





Accessing the Grafana dashboard (available in Chrome bookmarks), we can access information about both our Authoritative and Resolver servers. The Authoritative server receives A type queries and responds successfully at a rate of 1000 queries per second (QPS). Similarly, our resolver receives 1000 QPS from our legitimate clients and performs recursive lookups at the same rate of 1000 QPS.



## DNS Attacks

In this scenario, we will demonstrate three different DNS attack types, each corresponding to a mitigation method used by the new Authoritative protection. We will run the attacks in the same order in which the protection escalates, starting from Allow-List, then proceeding to Challenge/Response, and finally, Adaptive Rate-Limit.

### 1. DNS Water Torture Attack

To start the attack open **MTPutty** and double click on "**Start Water Torture Attack**".

Water Torture attacks are basically a random sub-domain query, in our attack we are generating a random string for **dp-demo-1.com** domain in the form of **<random>.dp-demo-1.com**. this attack generates 7000 QPS.

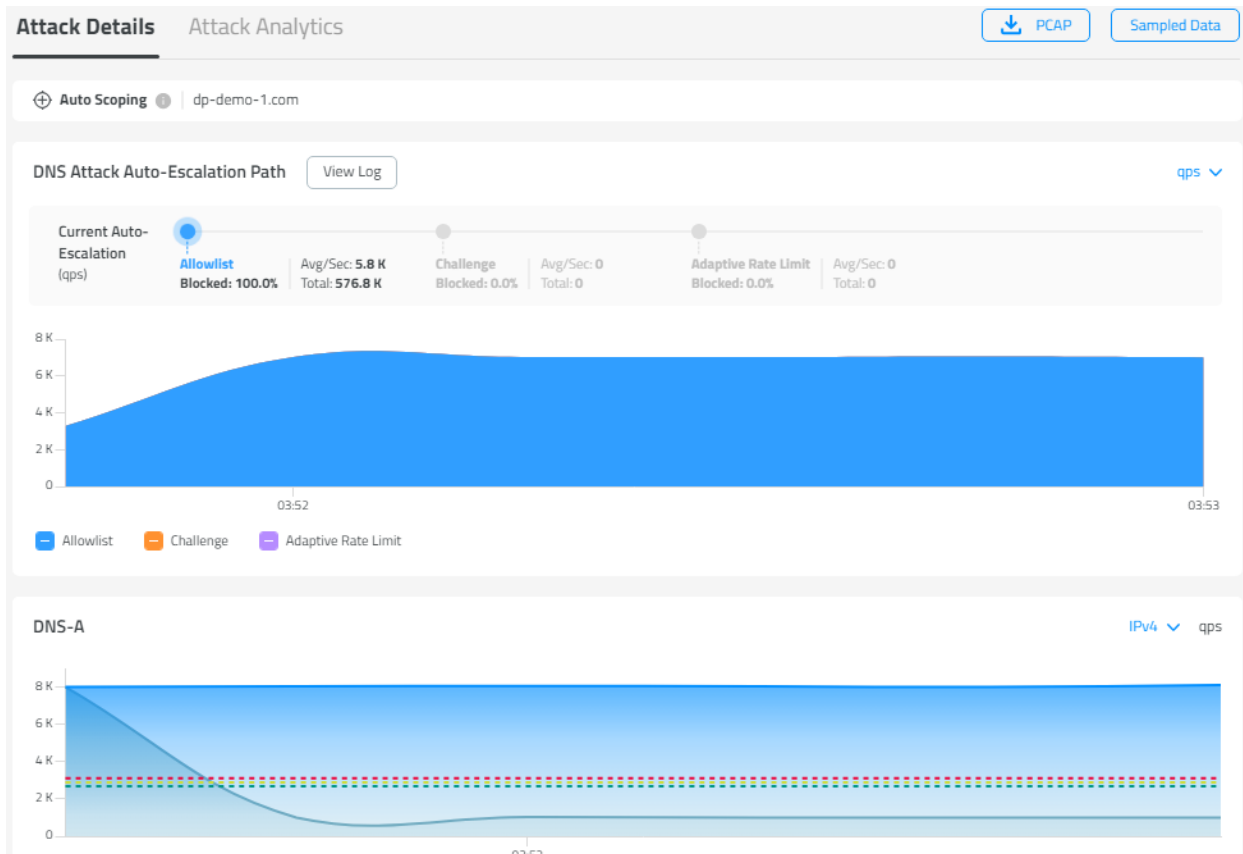
Once the attack is running, we will be able to see a DNS event detected, clicking on the magnifying glass will take us to the attack details.

Detection Events 1									
Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
Drop	Ongoing	DNS	DNS flood IPv4 DNS...	155.1.102.4	18.04.2024 10:19...	00:03:10	VDP_Demo_Lab	DefensePro X	<a href="#">Info</a>

In the attack details we can see multiple items from top to bottom:

- Auto Scoping – Identifying that the attack is currently targeting the **dp-demo-1.com** domain.
- Escalation Path – Currently utilizing the Allow-List method for mitigation.
- Escalation Path Graph – Illustrating the mitigation of 7000 QPS using the Allowlist method.

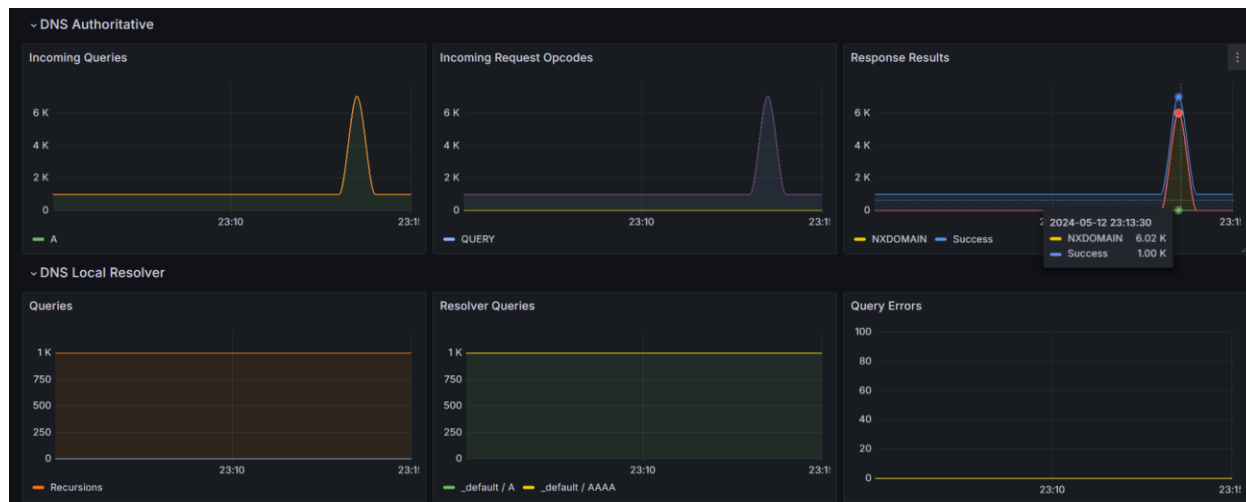
- DNS-A Graph – showing A query mitigation along with the legit traffic not impacted, which maintains its rate of 1000 QPS.



In the Escalation Path, we can also click on the 'View Log' to examine the events that triggered the Allowlist mitigation. In our case, upon reviewing the log, we observe that a Water Torture attack was detected, and the Auto-Scoping feature identified the attacked domain as **dp-demo-1.com**, thereby limiting the allowlist mitigation to this specific domain.

Log		X	
Timestamp	Event		
10:16:18	Auto-Scoping domains: dp-demo-1.com		
10:16:18	Started Water Torture attack mitigation for scoped domains		

While the Water Torture attack is running, you can switch to the Grafana dashboard and observe the Authoritative DNS responses. Since the attack generates nonexistent domains, you'll notice an increase in NXDOMAIN responses from the server, as a real-world attack would.



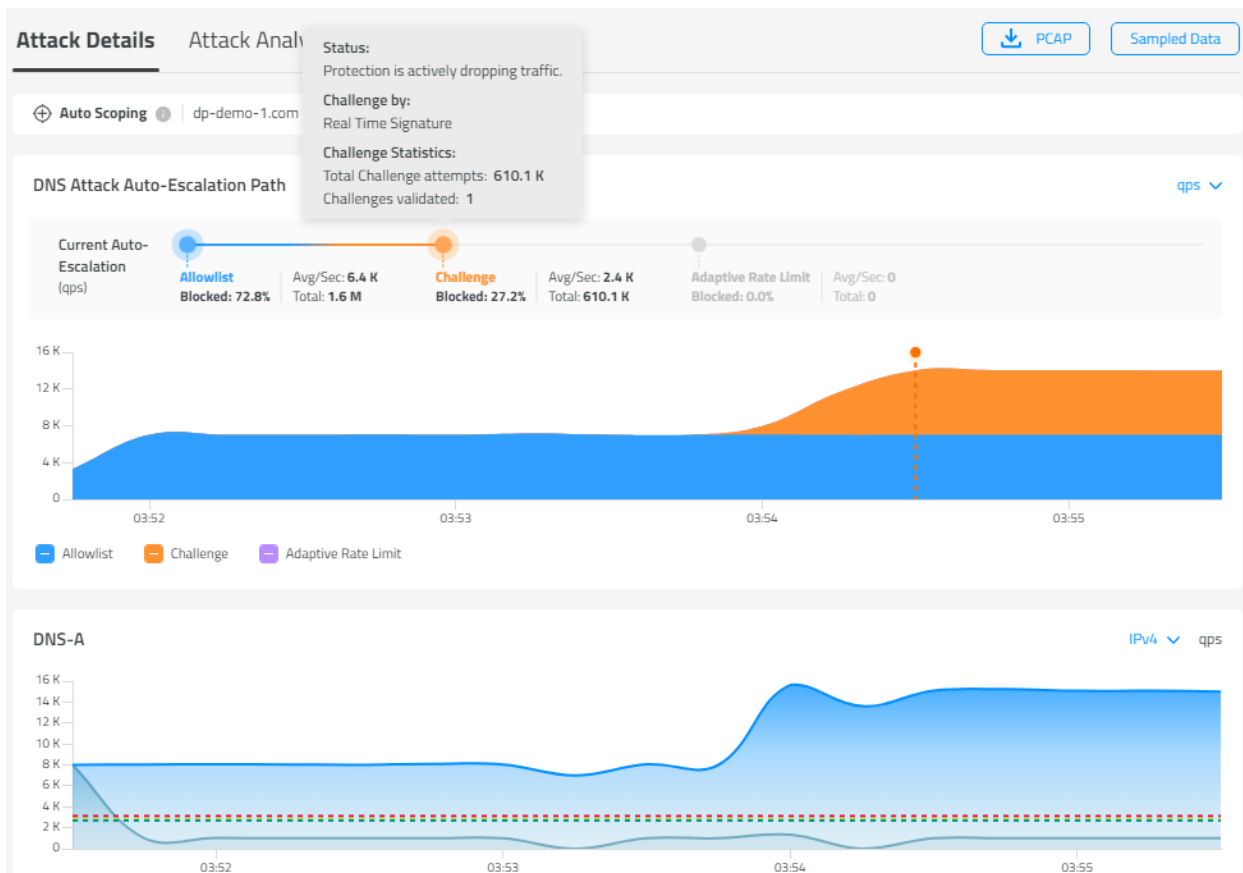
## 2. Dictionary Attack

To start the attack open **MTPutty** and double click on "**Start Dictionary Attack**".

This attack involves flooding by sending an A query for **app1.dp-domain-1.com** at a rate of 7000 QPS. It's important to note that this FQDN is included in our allow list.

Once the attack is running, it will continue from the same event as detected by the Water Torture attack. Looking at the attack details we can see that the Escalation Path has escalated to the next mitigation approach, challenge.

Hovering over the challenge dot in the escalation path will reveal a popup showing that we have sent 600k challenge attempts and only 1 has been validated. The one validated attempt is from our resolver, which successfully passes the challenge. This ensures that legitimate traffic continues to flow without interruption.



Scrolling down the Attack Details, we'll find the signature calculated by the DefensePro. It's essential to understand that this signature isn't used to block traffic; instead, it's used to identify the queries that will receive the challenge.

Additional Attack Attributes						
Risk High	Radware ID 450	Direction (In/Out) In	Action Type Drop	Attack ID 66-1713350764	Physical Port 1	Total Packet Count 1,520,474
VLAN N/A	MPLS RD N/A	Source Port Multiple	Packet Type Regular			

Characteristics				Real-Time Signature		
DNS Query -	DNS An Query Count -	TTL 64	DNS ID -	Operator	Parameter	Value
				[		
				OR	dns-flags	0,256
				]		
				AND		
				[		
				AND	destination-ip	155.1.102.4
				AND	dns-subdomain	dp-demo-1.com

Examining the attack log, we notice that the Real-Time Signature has been calculated and is currently utilized for the Challenge\Response mitigation action.

Log		×
Timestamp	Event	
10:22:56	Real-Time-Signature modified	
10:22:56	Challenge response mitigation action started using Real-Time-Signature	
10:22:51	Real-Time-Signature modified	
10:22:47	Real-Time-Signature modified	
10:16:18	Auto-Scoping domains: dp-demo-1.com	
10:16:18	Started Water Torture attack mitigation for scoped domains	

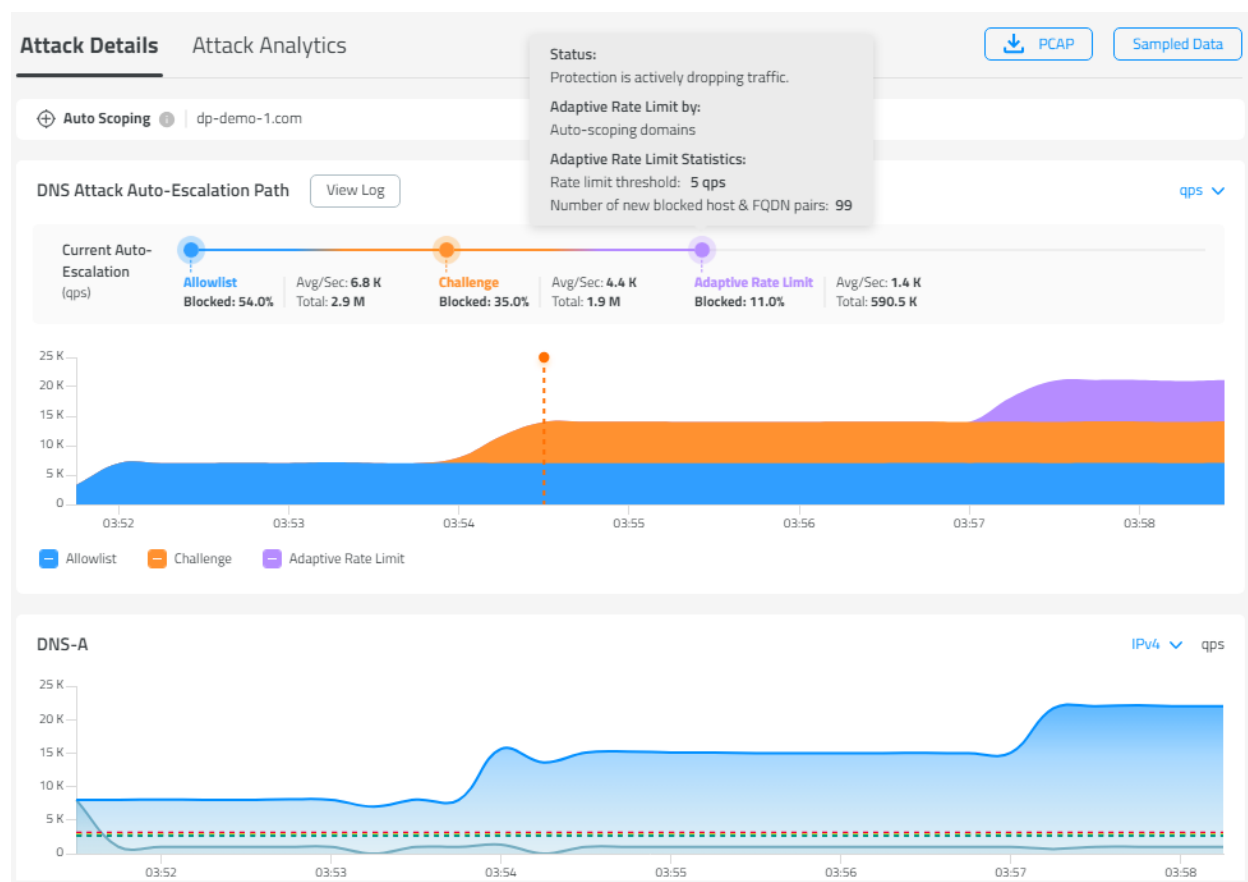
### 3. Authenticated Resolvers Dictionary Attack

To start the attack open **MTPutty** and double click on " **Start Authenticated Resolvers Dictionary Attack**".

This attack involves flooding by sending an A query for **app1.dp-domain-1.com** at a rate of 7000 QPS. It's essentially the same attack as the Dictionary Attack, with the only difference being that the source IPs are authenticated. This simulates a dictionary attack through real resolvers that can pass the challenge.

Once the attack is active, we'll notice that the Escalation Path has progressed to the next mitigation approach, Adaptive Rate-Limit. With the Adaptive Rate-Limit, DefensePro tracks sources that request the same FQDN at a rate of 5 QPS or higher. These sources will be added to the suspend table along with the suspended FQDN. It's important to note that in this mitigation approach, the Real-Time Signature is not used, all queries that match the domains found by the Auto Scoping are considered eligible for suspension.

As observed by hovering over the Adaptive Rate-Limit in the Escalation Path, we have 99 Sources & FQDN pairs in the suspend table. At this point, our legitimate traffic is not impacted as we ensured that queries to **dp-demo-1.com** will not exceed 5 QPS.



Examining the attack log, we can observe that due to the high Degree of Attack during the challenge event, we escalated to Adaptive Rate-Limit.

Log		X	
Timestamp	Event		
10:36:00	Auto-escalating to Adaptive Rate Limit due to high DoA		
10:36:00	Adaptive Rate Limit mitigation action started for scoped domains		
10:22:56	Real-Time-Signature modified		
10:22:56	Challenge response mitigation action started using Real-Time-Signature		
10:22:51	Real-Time-Signature modified		
10:22:47	Real-Time-Signature modified		
	Auto-Escaping domains: do.domo		

In our demo we are simulating 99 authenticated sources by authenticating the entire 155.1.101.0/24. Typically, resolvers will pass the challenge and enter the authentication table with a /32. However, in cases where a resolver receives a challenge with one source and responds with a second source IP, DefensePro authenticates the entire /24. We utilize this by authenticating 155.1.101.0/24 and execute the attack with source IPs from this range.

To observe the source in the authentication table, execute the following command in the DefensePro CLI: "system internal security dns challenge auth-table". Then, using WinSCP, access the file located at "/mnt/applData/debug\_dns\_cr\_authentication\_table.txt" on DefensePro. This file contains the authenticated source IPs.

## Packet Capture

At this stage, while all attacks are running, we can demonstrate our unique packet capture capabilities by initiating a packet capture for our policy "VDP\_Demo\_Lab". Simply click on the icon indicated below.

Policies2

Devices1

+ Add Policy

Status	Policy Name	Device Name	Inbound (Mbit/s)	Dropped (Mbit/s)	Challenged (Mbit/s)	Packet Capture
<div><div></div><div>Active</div></div>	VDP_Demo_Lab	DefensePro X	8.28 M	5.07 M	2.5 M	<div><div></div><div></div><div></div></div>
<div><div></div><div>Active</div></div>	VDP_Demo_Lab_Advanced	DefensePro X	0	0	0	<div><div></div><div></div><div></div></div>

Once clicked, you'll be presented with the packet viewer. Pressing the Play button will initiate the packet capture, which will automatically stop after capturing 5000 packets. At this point you should be able to observe multiple types of packets (Dropped, Passed, Matched and Challenged) marked by different colors as shown below.

Packet Viewer ⓘ ×

**Capture Settings**  
 Device: DefensePro X  
 Capture Filter: policy == VDP\_Demo\_Lab

**Display Settings**  
 Match Filter: Type and press enter to filter  
 Display Filter: Type and press enter to filter

**Packets**

🔴 Dropped
🟢 Passed
🔵 Match
🟡 Challenge
▶ Start
🗑 Delete
📄 Export
📄 Import

Time	Device	SRC IP Address	SRC Port	DST IP Address	DST Port	Protocol	Length	Reason
0.000	DefensePro X	155.1.101.125	32727	155.1.102.4	53	DNS	78	Dropped due to DNS Protection
0.000	DefensePro X	130.5.13.239	5559	155.1.102.4	53	DNS	78	-
0.000	DefensePro X	155.1.102.4	53	130.5.13.239	5559	DNS	148	DefensePro challenge request
0.000	DefensePro X	130.50.111.239	5559	155.1.102.4	53	DNS	78	-
0.000	DefensePro X	155.1.102.4	53	130.50.111.239	5559	DNS	148	DefensePro challenge request
0.000	DefensePro X	164.40.222.85	37049	155.1.102.4	53	DNS	79	Dropped due to DNS Protection
0.000	DefensePro X	155.1.101.126	47616	155.1.102.4	53	DNS	78	Dropped due to DNS Protection

Capture Elapsed Time: 5.75 Seconds    Passed Packets: 3461 (out of 5000)

For each packet, you can expand the DNS payload to view additional information. Below, we can see a challenge sent by the DefensePro in the form of an NS response along with its cookie.

Packet Viewer ⓘ ×

IPv4

UDP

DNS

ID: 0x927b  
 QR: Response  
 OPCODE: 0 (Query)  
 Authoritative Answer: True  
 Truncated: False  
 Recursion Desired: False  
 Recursion Available: False  
 Reserved Bit: 0  
 Authentic Data: False  
 Checking Disabled: False  
 RCODE: 0 (No Error)  
 QDCOUNT: 1  
 ANCOUNT: 0  
 NSCOUNT: 1

ARCOUNT: 0  
 Question:  
 QNAME: App1.Dp-Demo-1.Com  
 QTYPE: 1 (A (Host Address))  
 QCLASS: 1 (Internet (IN))  
 Authority:  
 NAME: App1.Dp-Demo-1.Com  
 TYPE: 2 (NS (Authoritative Name Server))  
 CLASS: 1 (Internet (IN))  
 TTL: 0  
 RDLLENGTH: 40  
 RDATA:  
 NS RDATA:  
 NSDNAME: Ck01-76e895b6d4-81c44617.Dp-Demo-1.Com

```

0040 65 6D 6F 2D 31 03 63 6F 6D 00 00 01 00 01 04 61  EMO-1.COM...A
0050 70 70 31 09 64 70 2D 64 65 6D 6F 2D 31 03 63 6F  PP1.DP-DEMO-1.CO
0060 6D 00 00 02 00 01 00 00 00 00 28 18 63 6B 30  M...Ck0
0070 31 2D 37 36 65 38 39 35 62 36 64 34 2D 38 31 63  1-76E895B6D4-81C
0080 34 34 36 31 37 09 64 70 2D 64 65 6D 6F 2D 31 03  44617.DP-DEMO-1.
0090 63 6F 6D 00                                     COM.
  
```



## TLS Fingerprint Protection

### Legit Traffic & Baseline Adjustment

**Note: make sure JMeter is not running when demoing this protection.**

The TLS Fingerprint protection needs a learning time between 6 hours to 3 days . To quickly set up a baseline, we use a script that automatically resets it and generates the necessary legit traffic for the demo.

To execute the script, open the Multi Putty and double-click on "TLSFP\_Legit\_and\_Baseline\_Start".

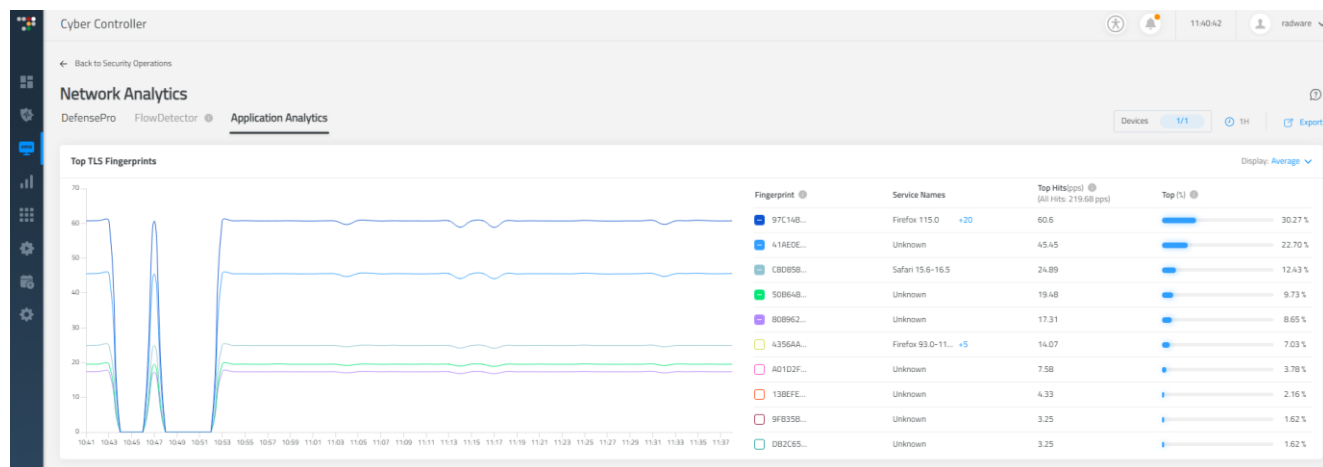
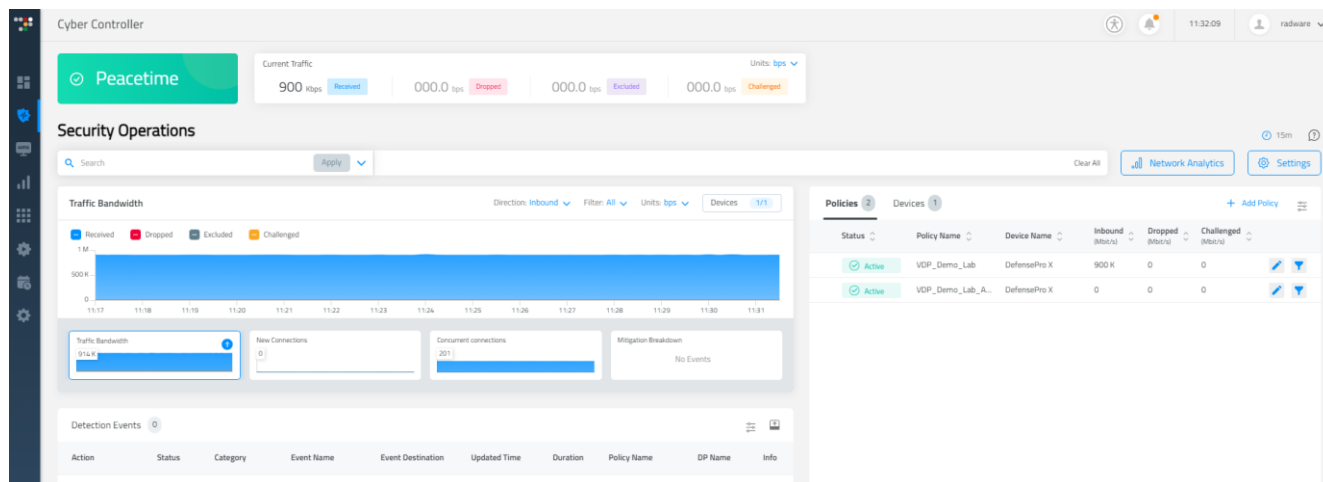
Here's a high-level overview of the script's actions:

1. Initiate legit traffic using a packet capture containing "Client Hello" from various legit clients.
2. Reduce the learning period to 120 seconds.
3. Reset the baseline.
4. Pause for 160 seconds.
5. Apply the learned baseline.
6. Restore the learning period to 60000.
7. Print the baseline.

To verify the script's successful execution, check that the printed baseline state is "**Detect**", and all the thresholds are populated with numbers as seen below.

```
# Policy Name # State # Learning # RT BL R # RT Thre # BL Rate # BL Thre # Current # Current # Active # Learning # Suspend # Start Time #
# # # Hits # ate # shold # # shold # Rate # RI val # Attacks # Duration # # #
#####
# VDP_Demo_Lab # Detect # 28246 # 2192.52 # 87.43 # 2189.36 # 87.43 # 2202 # 0.08 # 0 # 130 # 0 # 11-11-23 19:13:51 #
#####
```

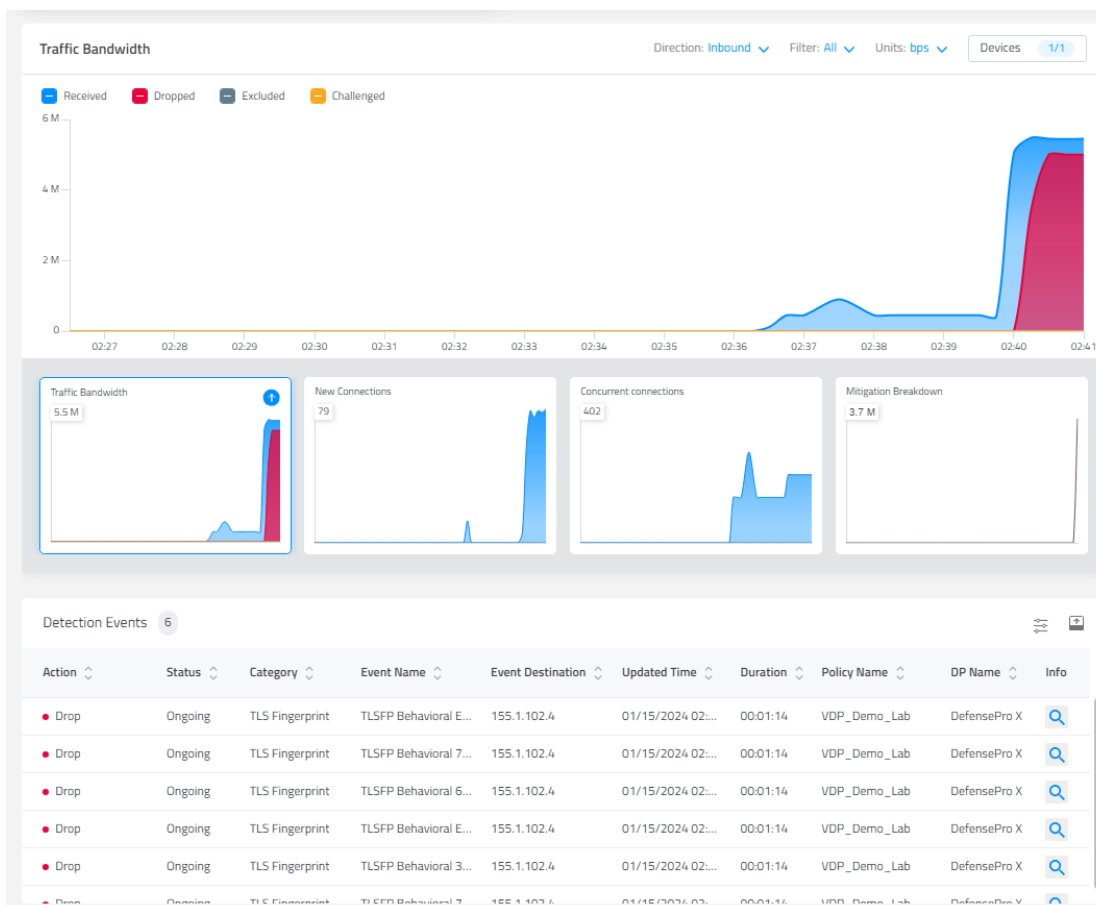
Additionally, in the Real-Time Monitoring and Network Analytics section of Cyber-Controller, confirm that the legitimate traffic is visible, resembling the captures below:



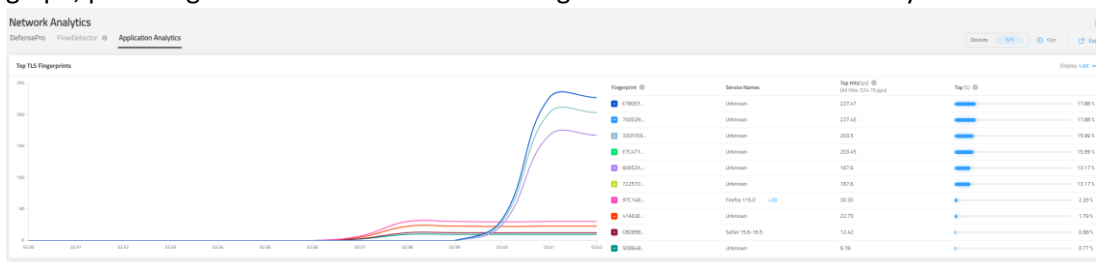
## TLS Attacks

The TLS Fingerprint Scenario includes 3 different attacks:

1. **Six fingerprint attack** – this attack is using a packet capture to send TLS Client-Hellos taken from actual real-world attack. To initiate the attack, open Multi Putty and double-click on “TLS\_6\_Finger\_Attack\_Start”. Once the attack is running you should be able to observe 6 detected events in the Real-Time Monitoring screen as shown below:



By examining the Application Analytics, you can easily identify the six fingerprints responsible for the attack. It's important to note that we manually selected the lower four fingerprints to display in the graph, providing a clear distinction between legitimate and malicious activity.



2. **Non-Citizen attack** – this attack is using a packet capture as well to send TLS Client-Hellos, the aim with this scenario is to show an attack on a fingerprint that existed during peace time and is considered non-Citizen as its traffic is significantly low, meaning it can be used for mitigation even though the TLS profile mitigation scope is configured for ‘*Unknown Fingerprints*’ as shown below.

BEHAVIOURAL TLS FINGERPRINT

☒ Behavioral Detection State

Mitigation Scope: ☒ Unknown Fingerprints ☐ All Fingerprints

Detection Sensitivity:

Learning Period:

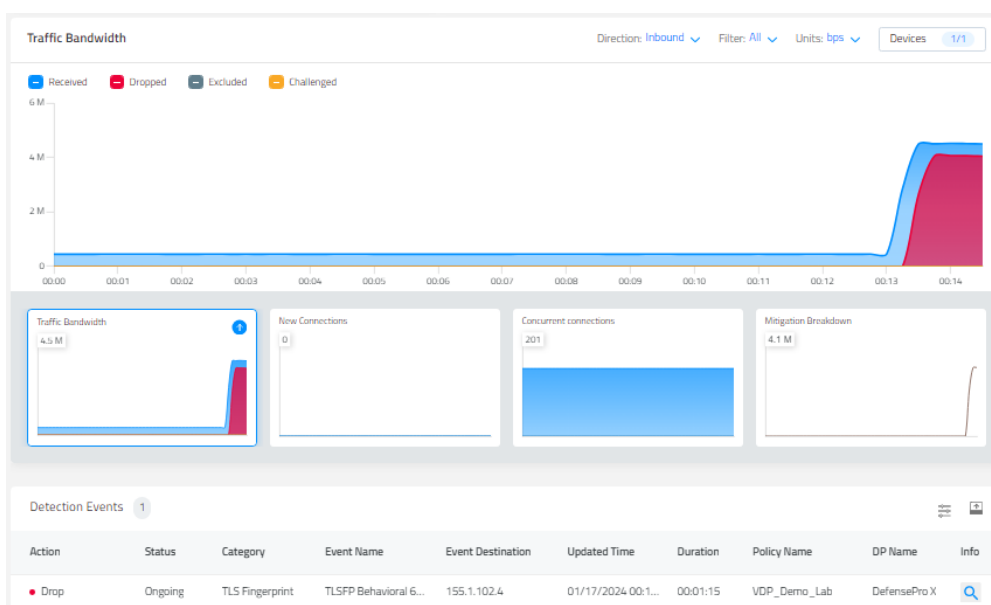
During peacetime you can observe the non-Citizen fingerprint highlighted below using the command “*system internal security tls-fingerprint behavioral fingerprint-data \* -c 50*”.

For Policies in Learning State: 25 For Policies in all other States:

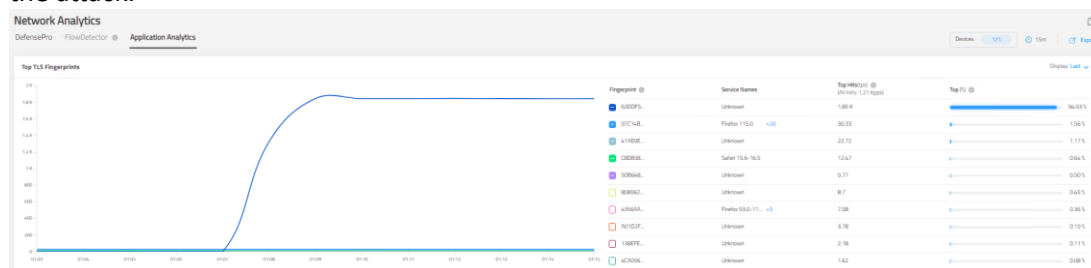
Total Fingerprints: 25  
Citizens: 11  
Under Attack: 0

Policy Name	Fingerprint	Policy State	FP State	Current hits	Current Portion	Moving hits	Baseline hits	Baseline Portion	Citizen	Attack-on Edge	Attack-off Edge	Attack Off	Idle Time	Under Attack
				hits/sec		hits/sec	hits/sec			hits/sec	hits/sec	(sec)	(sec)	
VDP_Demo_Lab	97C14B3455A004FF08BA1D1F5A05CA	Detect	Active	30.5	0.277273	29.130	29.129	0.276681	Yes	50,000	43,494	0	0	No
VDP_Demo_Lab	41A0E5757CC603C2B3C6C4E319A6A6	Detect	Active	23.0	0.209091	21.834	21.833	0.204633	Yes	50,000	32,750	0	0	No
VDP_Demo_Lab	C8D58FFBC9737086A4A401FF5920F9	Detect	Active	12.7	0.115455	11.970	11.970	0.113282	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	50B441BDC53B18C70ABD3119C02056F	Detect	Active	1.7	0.001882	9.406	9.406	0.003021	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	80896224B8C7C597D350951E1A5458	Detect	Active	0.6	0.079182	0.329	0.329	0.078828	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	4356A126F0958C472384159F77297F	Detect	Active	7.0	0.043636	6.787	6.787	0.044230	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	AC1D2F03E576618A10F9F5011607746	Detect	Active	1.6	0.032727	3.451	3.451	0.034554	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	138FE246F8B02015787A18A2CA41	Detect	Active	1.2	0.020000	2.084	2.084	0.019720	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	4A0546760F10B8A2F0C2732656C53	Detect	Active	1.6	0.014545	1.563	1.563	0.014793	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	9F93BAC74F752FFB3F7A0B90C6A8E	Detect	Active	1.6	0.014545	1.551	1.551	0.014677	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	D82C55E176348E1C9618AAB49D4C0	Detect	Active	1.5	0.013636	1.551	1.551	0.014677	Yes	50,000	20,000	0	0	No
VDP_Demo_Lab	288FA3C3D3C2C74F2820E8F4146093	Detect	Active	1.0	0.009091	1.042	1.042	0.009660	No	50,000	20,000	0	0	No
VDP_Demo_Lab	4771B4630A091D8F905031E4D66F9F	Detect	Active	0.6	0.005455	0.527	0.527	0.004989	No	50,000	20,000	0	0	No
VDP_Demo_Lab	99826652CA2791EEF55941B3CF6A6AD	Detect	Active	0.5	0.004545	0.527	0.527	0.004989	No	50,000	20,000	0	0	No
VDP_Demo_Lab	00CF0F3A1D4731875751048A8A03	Detect	Active	1.5	0.004545	0.527	0.527	0.004989	No	50,000	20,000	0	0	No
VDP_Demo_Lab	428A968C2CAF8906835920C45E3C	Detect	Active	0.5	0.004545	0.527	0.527	0.004989	No	50,000	20,000	0	0	No
VDP_Demo_Lab	AS6A18E419C9C2C47023515833AC	Detect	Active	0.5	0.004545	0.521	0.521	0.004927	No	50,000	20,000	0	0	No
VDP_Demo_Lab	218F96E403178275620F7A2C080540	Detect	Active	0.5	0.004545	0.521	0.521	0.004927	No	50,000	20,000	0	0	No
VDP_Demo_Lab	7930A7550406970558D84318F66889	Detect	Active	0.5	0.004545	0.521	0.521	0.004927	No	50,000	20,000	0	0	No
VDP_Demo_Lab	C0420F18F38C9068A0717110A040	Detect	Active	0.5	0.004545	0.521	0.521	0.004927	No	50,000	20,000	0	0	No
VDP_Demo_Lab	5049C546F6C7036C786C77A193083	Detect	Active	0.6	0.005455	0.519	0.519	0.004918	No	50,000	20,000	0	0	No
VDP_Demo_Lab	130F3F3F3A8A267C8FF7F9067934	Detect	Active	0.6	0.005455	0.515	0.515	0.004972	No	50,000	20,000	0	0	No
VDP_Demo_Lab	8A86F98A010F0F0C83F08A17A80F	Detect	Active	0.6	0.005455	0.515	0.515	0.004972	No	50,000	20,000	0	0	No
VDP_Demo_Lab	DA9FD97102A6D624A4A9C0568F2B1F	Detect	Active	0.5	0.004545	0.515	0.515	0.004972	No	50,000	20,000	0	0	No
VDP_Demo_Lab	FE3CF77C8B7853E394A3C44F90802	Detect	Active	0.6	0.005455	0.513	0.513	0.004954	No	50,000	20,000	0	0	No

To initiate an Attack, open Multi Putty and double-click on “*TLS\_Non\_Citizen\_Attack*”. Looking at the Real-Time Monitoring screen you should be able to observe a single event detected.

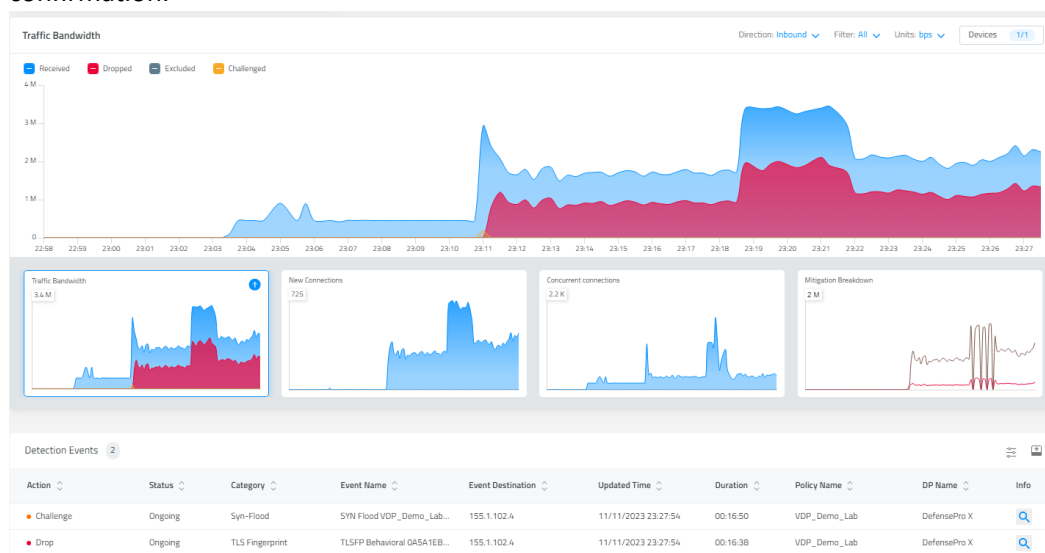


By examining the Application Analytics, you can identify the non-Citizen fingerprints responsible for the attack.

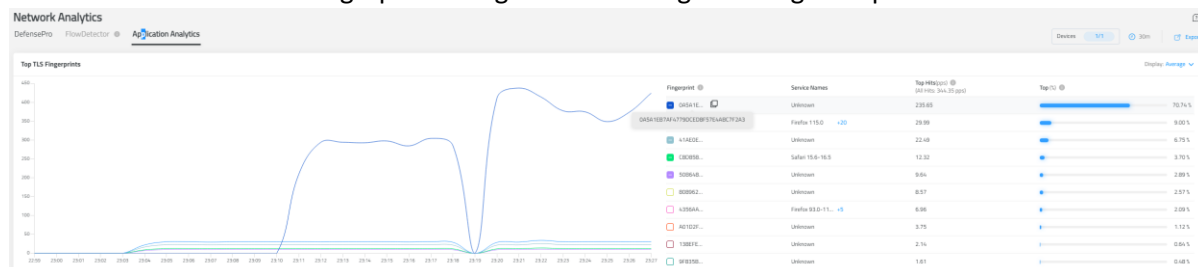


3. **Python script attack** – this script is used to create an HTTP attack involving a complete TCP connection followed by TLS handshake, unlike the previous two attacks that relied on packet captures with only TLS Client-Hello. The script establishes numerous HTTPS connections intentionally exceeding the learned baseline triggering a detection and subsequent mitigation by the TLSFP protection. To initiate the attack, open Multi Putty and double-click on "*TLSFP\_Attack\_Start*".

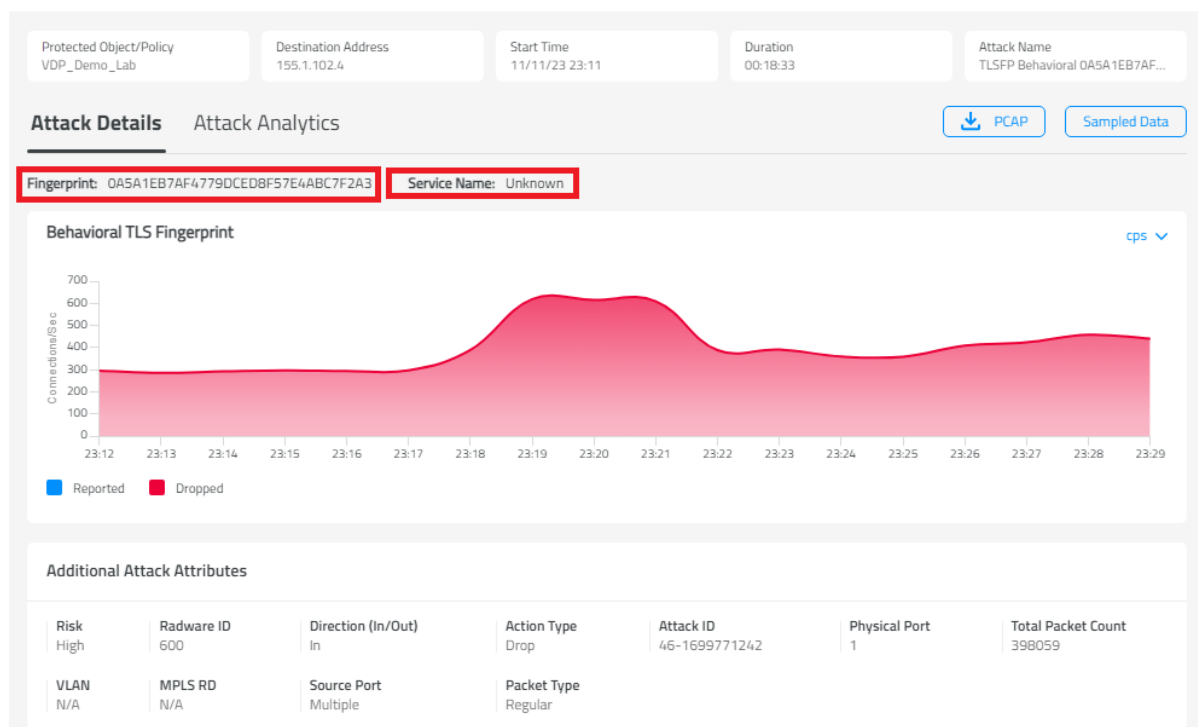
Once the attack is running, you'll be able to see two detection events on the Real-Time Monitor screen of Cyber-Controller, Syn-Flood and TLS Fingerprint, as seen in the screen capture below. Please be aware that while Syn-Flood detection occurs due to an excess of SYN packets surpassing the threshold, the mitigation is carried out by TLSFP. "Client Hello" packets are dropped before the Challenge/Response phase can occur. To validate this, examine the mitigation breakdown for further confirmation.



Additionally, examining Network-Analytics will reveal the primary fingerprint behind most requests, specifically the attack initiated by the Python script. Refer to the TLSFP attack details for accurate information on the exact fingerprint being blocked during the mitigation process.



TLS Fingerprint, TLSFP Behavioral 0A5A1EB7AF4779DCED8F57E4ABC7F2A3



## HTTPS Protection

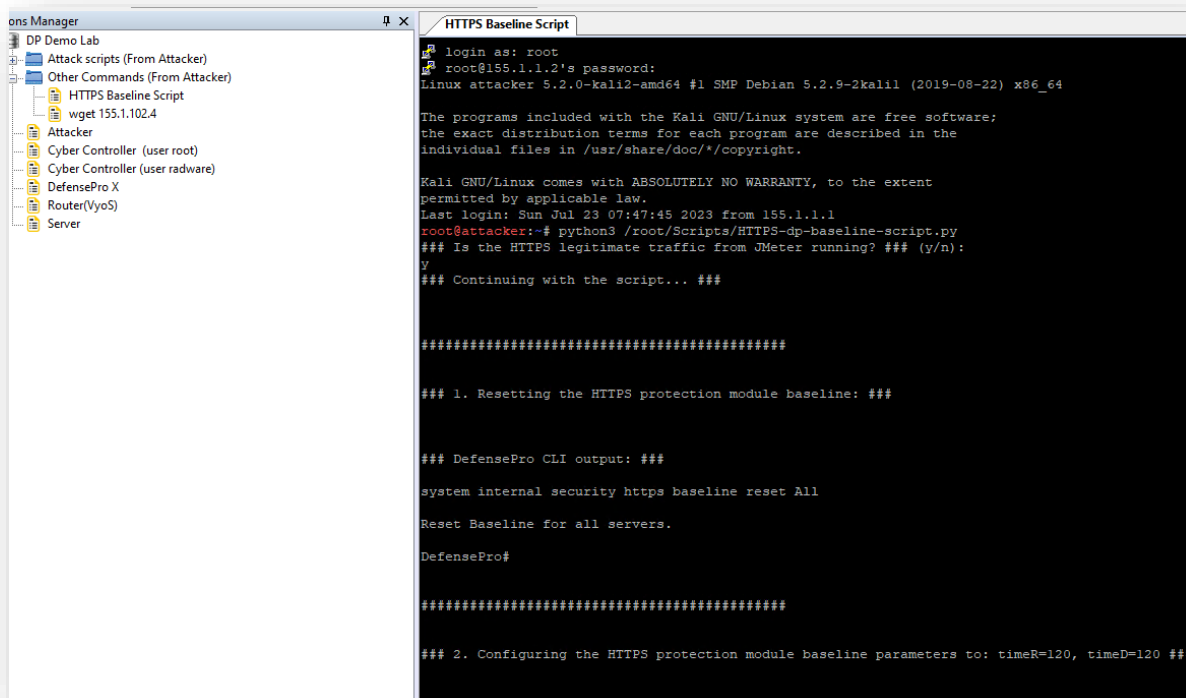
For more additional information about this scenario, please refer to the [“Appendix 1 - HTTPS Protection \(Additional Info\)”](#) section.

### HTTPS Baseline Adjustment

HTTPS protection requires baselining (default 7 days). As this is not possible during Demo, we suggest adjusting baseline learning period to 120 seconds.

#### Use the following script for adjusting the HTTPS baseline:

1. Open the Multi Putty Manager.
2. Double click on the “**HTTPS Baseline Script**” session, which is in:  
Sessions Manager à DP Demo Lab à Other Commands (From Attacker)
3. When the script opens, press “y” if the legit HTTPS traffic is running (the HTTPS legit traffic must be running at this point!).



```

ons Manager
DP Demo Lab
  Attack scripts (From Attacker)
  Other Commands (From Attacker)
    HTTPS Baseline Script
    wget 155.1.102.4
  Attacker
  Cyber Controller (user root)
  Cyber Controller (user radware)
  DefensePro X
  Router(VyoS)
  Server

HTTPS Baseline Script
login as: root
root@155.1.1.2's password:
Linux attacker 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 23 07:47:45 2023 from 155.1.1.1
root@attacker:~# python3 /root/Scripts/HTTPS-dp-baseline-script.py
### Is the HTTPS legitimate traffic from JMeter running? ### (y/n):
y
### Continuing with the script... ###

#####

### 1. Resetting the HTTPS protection module baseline: ###

### DefensePro CLI output: ###

system internal security https baseline reset All

Reset Baseline for all servers.

DefensePro#

#####

### 2. Configuring the HTTPS protection module baseline parameters to: timeR=120, timeD=120 ###
  
```

4. Now wait for the step number 9 on the script, which will tell you that you can start the attack:

```
#####
```

```
### 9. Now you can start the attack! ###
```

```
root@attacker:~#
```

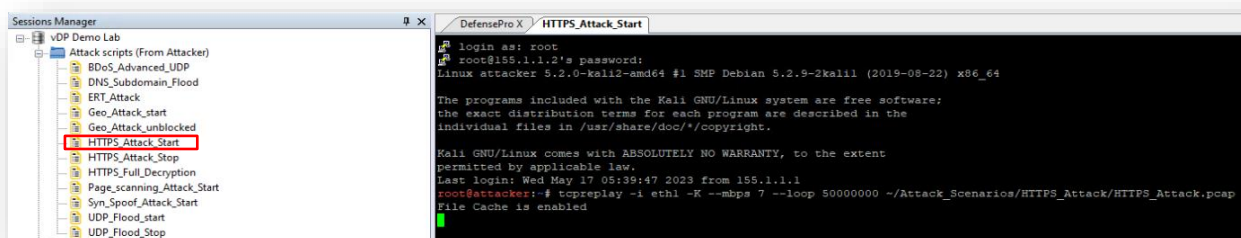


## Start the HTTPS Flood Attack from Kali and Verify Detection

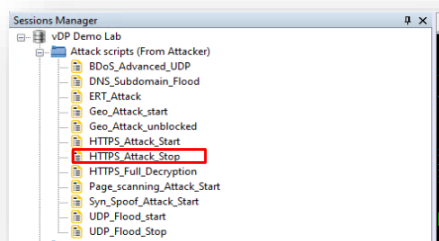
1. From the session manager, select the **HTTPS\_Attack\_Start**.

This script activates HTTPS flooding towards a specific bucket (101-200), which initiates the detection and mitigation phases.

While the script is running, the following screen displays:



2. In order to **stop** the attack, double click on **HTTPS\_Attack\_Stop**:

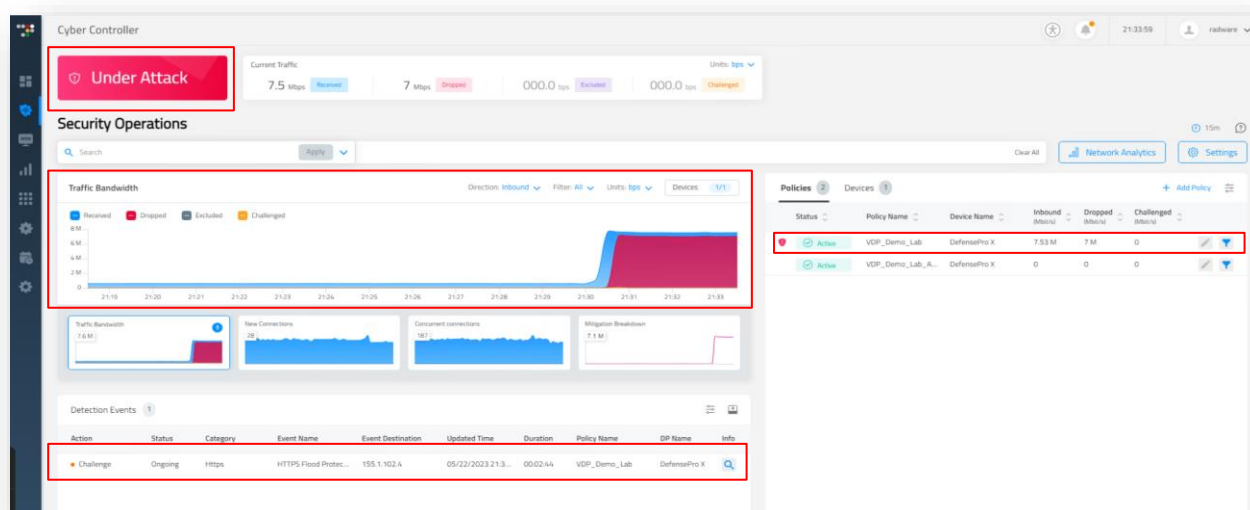


## Attack Mitigation


While the attack is running, the HTTPS protection module begins the characterization process of the malicious sources.

In this phase, all sources whose destinations match the attacked bucket and their HTTPS requests rate towards the attacked bucket are above 80%, are challenged with a 302-redirection cookie challenge, those who do not pass the challenge are considered as attackers.

1. Verify the attack in Cyber Controller. Go to the **Security Operations -> Real-Time Monitoring**:



2. On the detection events section, you will find the event attack. You can verify the attack details by clicking on the magnifying glass button:

Detection Events 1									
Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
Challenge	Ongoing	Https	HTTPS Flood Protec...	155.1.102.4	05/22/2023 21:3...	00:05:46	VDP_Demo_Lab	DefensePro X	

3. Verify the number of authenticated and attacker sources:

Protected Object/Policy

VDP\_Demo\_Lab

Destination Address

155.1.102.4

Start Time

22/05/23 21:30

Duration

00:04:14

Attack Name

HTTPS Flood Protection

Details

PCAP

Sampled Data

Additional Attack Attributes

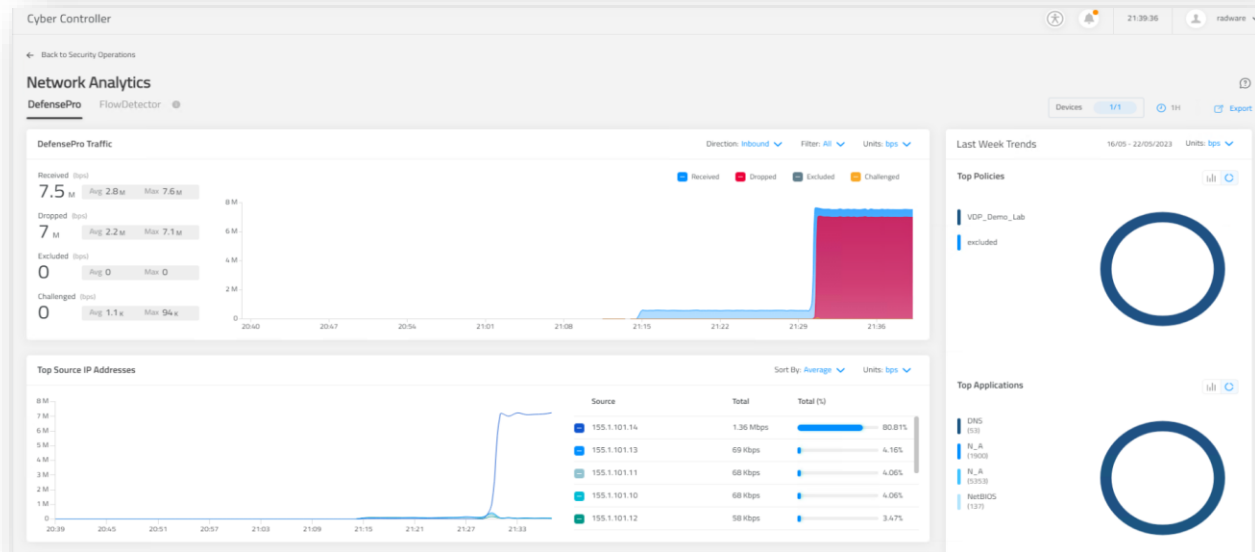
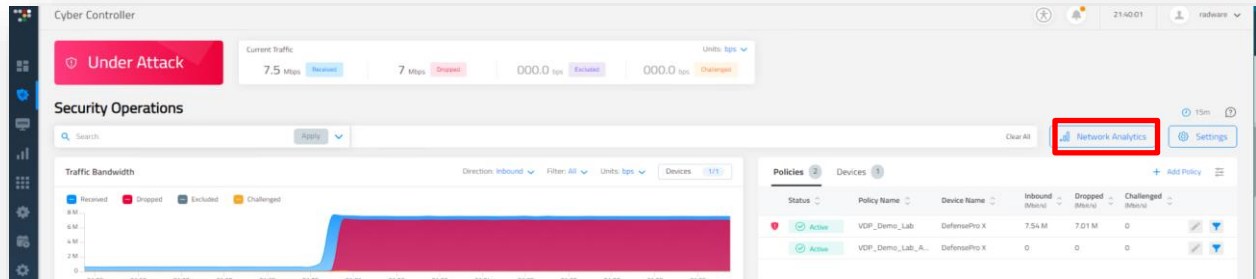
Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	700	In	Challenge	37-1684815078	1	1087749
VLAN	MPLS RD	Source Port	Packet Type			
N/A	N/A	Multiple	Regular			

Characteristics

Detection Method	Mitigation Method	Authentication Method	Total Suspect Sources	Total Req. Challenged	Total Sources Challenged
By Rate of HTTPS Requests	Challenge Suspected Attackers	302 Redirect	8	156	8
Total Sources Authenticated	Total Attackers Sources	Auth List Util.	Req. Per Sec	Transitory Baseline Value	Transitory Attack Edge Value
5	3	1%	4,460	107 RPS	128 RPS
Long Term Trend Baseline Value	Long Term Trend Attack Edge Value				
110 RPS	138 RPS				

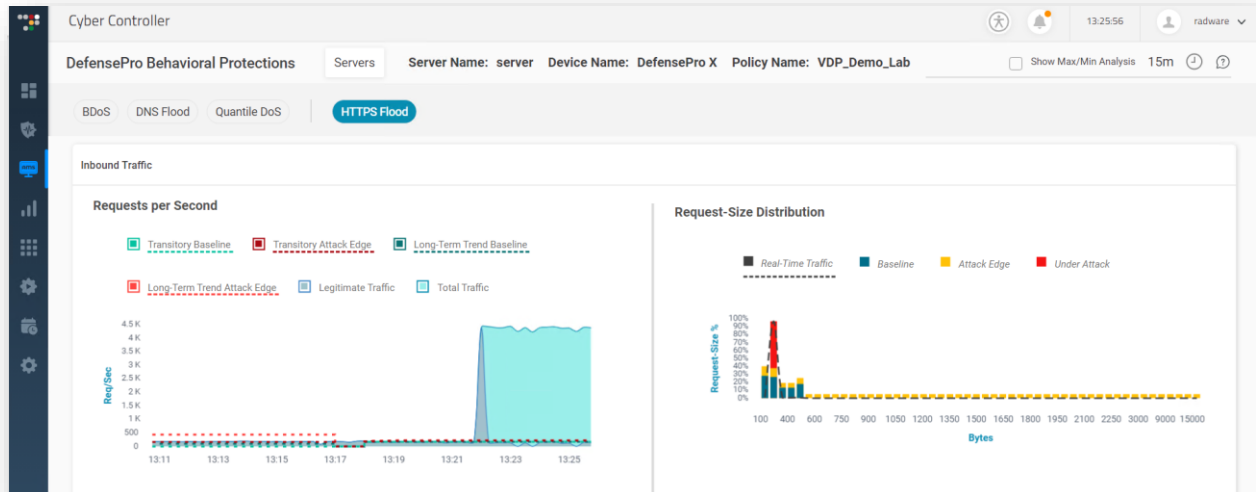
4. Close the detect event detail by clicking on the “x” button, so you will return back the real-time monitoring dashboard.

5. Click on the “Network Analytics” button:



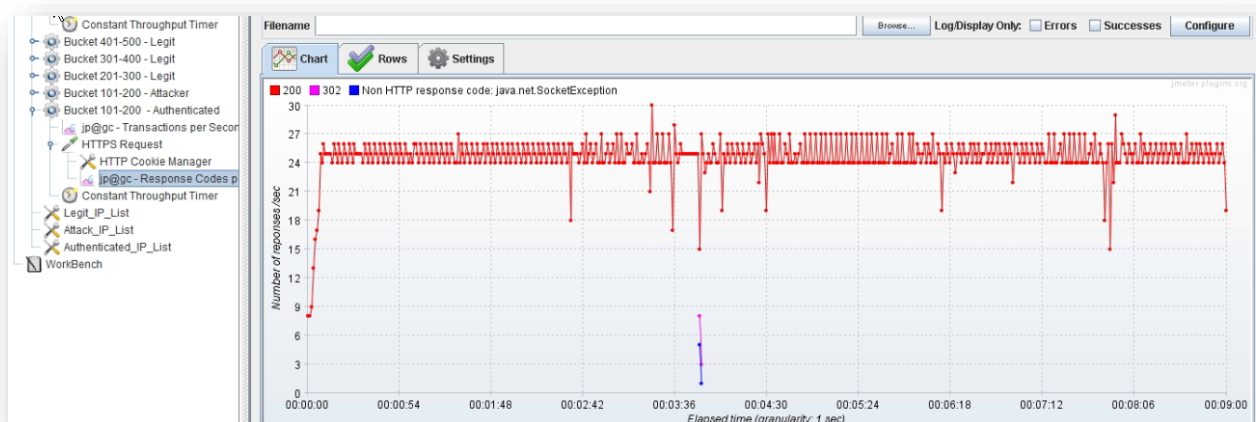
- Verify the data on the HTTPS Flood dashboard. Go to **Analytics AMS > DefensePro Behavioral Protections > HTTPS Flood (make sure the server is selected)**:

In the following screen, you should see a graph that includes all the buckets together. While under attack, a deviation in one or more of the buckets should occur. In this output, the deviation occurs in bucket 101-200:

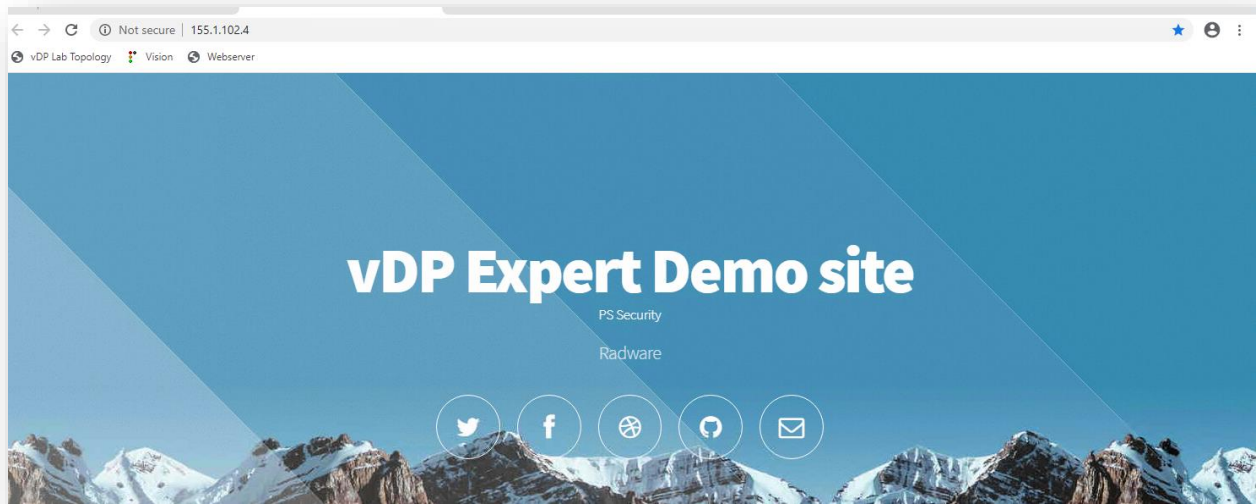


- Open the *JMeter* pane and view the 302 results in the *Response code per second* pane:

Open the bucket 101-200 – Authenticated (these sources are the legitimate traffic that has been passed the challenge):



8. Verify connectivity towards the attacking destination. Open the browser and select the **Webserver** bookmark (URL: <http://155.1.102.4>):



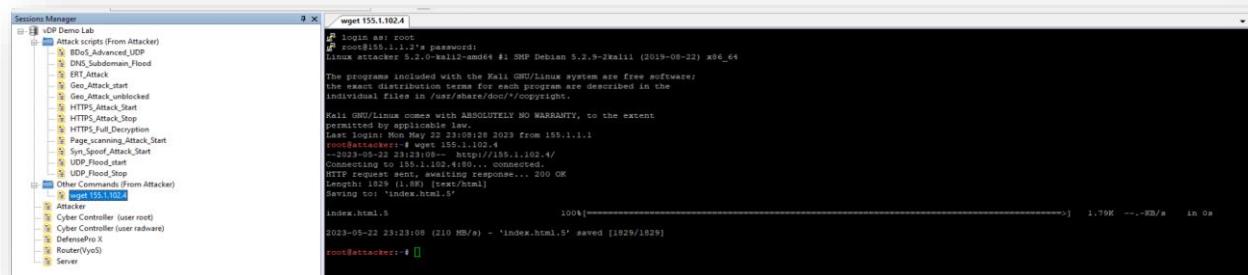
## Traffic Filters

For more additional information about this scenario, please refer to the [“Appendix 2 - Traffic Filters \(Additional Info\)”](#) section.

### Create an HTTP Page Scanning Attack from Kali and Verify Detection

1. Check if the Webserver is reachable from the attacker *before* running the attack.

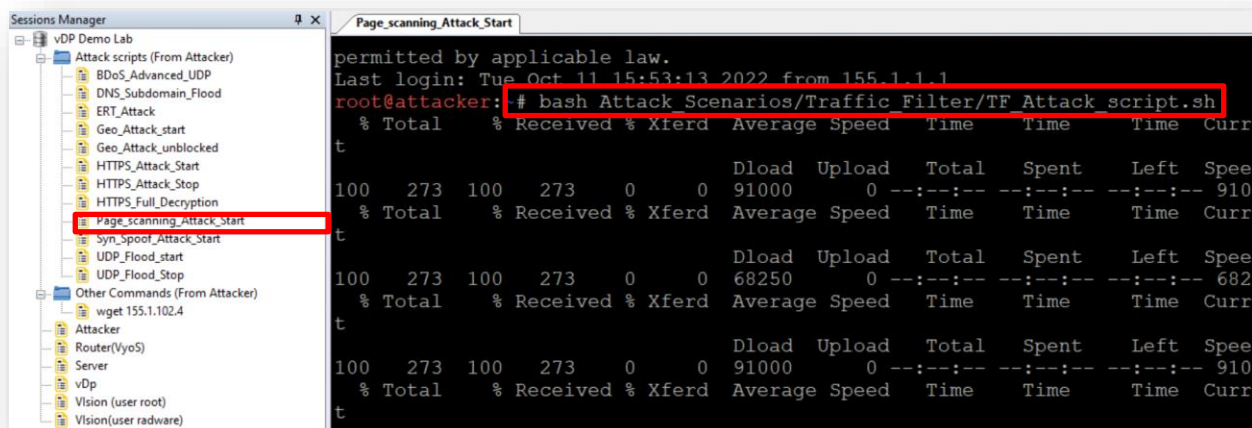
Select the **wget 155.1.102.4** icon located in the **Other Commands (From Attacker)** folder on the Session Manager.



2. Click on the **Page\_scanning\_Attack\_start** icon located in the **Attack scripts** folder on the Session Manager.

This script activates an HTTP Page scanning attack towards the Webserver with a URL that does not exist on the Webserver.

While the script is running, the following screen displays:

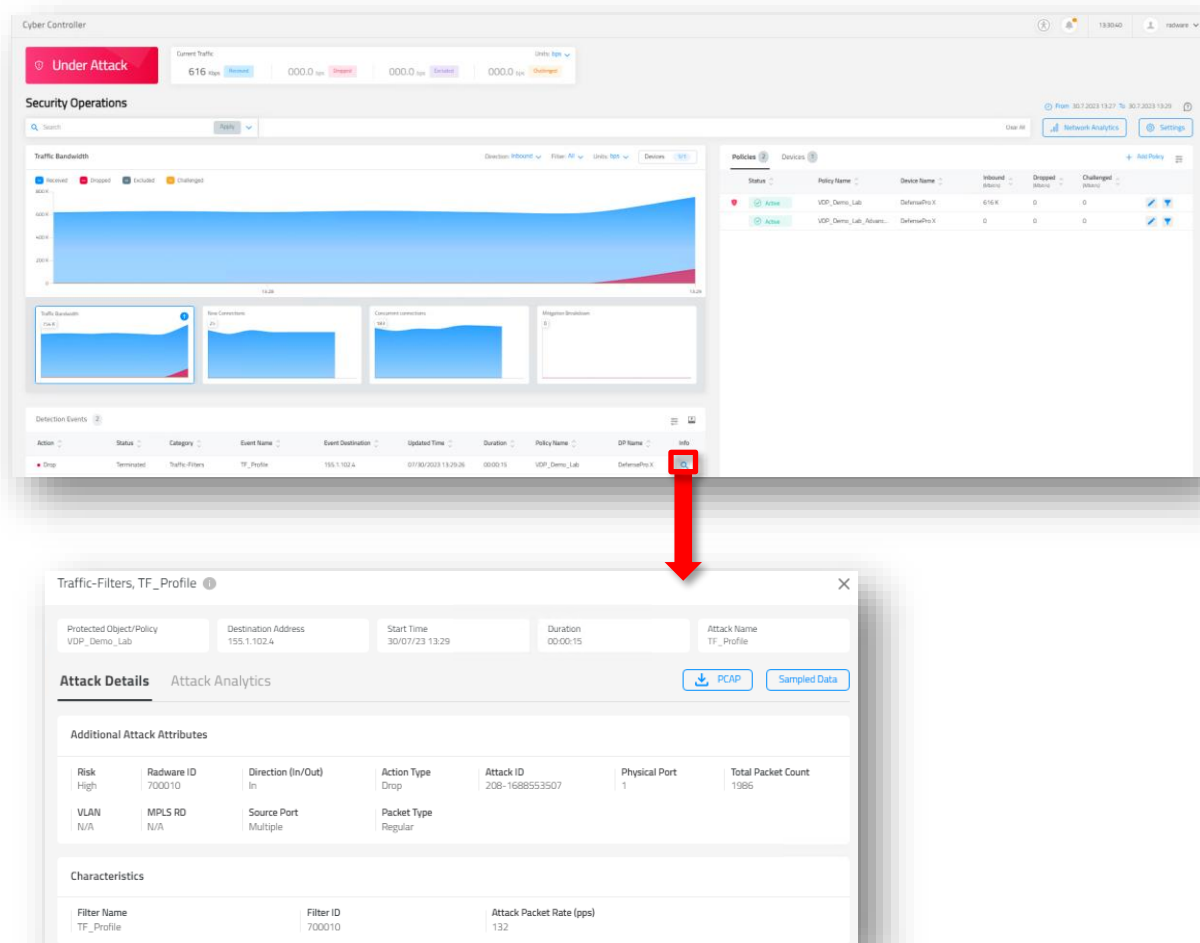




3. To stop the attack, press **Ctrl +C**

## Attack Mitigation

1. Verify the attack in Cyber Controller. Go to the **Security Operations -> Real-Time Monitoring**:



The screenshot shows the Cyber Controller Security Operations interface. At the top, there's a 'Under Attack' status bar with traffic statistics: 616 Mbps, 000.0 kbps, 000.0 kbps, and 000.0 kbps. Below this, the 'Security Operations' section displays a 'Traffic Bandwidth' chart and a table of 'Detection Events'. A red arrow points from the 'Info' icon in the 'Detection Events' table to a detailed view of the 'Traffic-Filters, TF\_Profile' event.

**Detection Events Table:**

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
Drop	Terminated	Traffic Filters	TF_Profile	155.1.102.4	07/30/2023 13:29:38	00:00:15	VDP_Demo_Lab	DefensePro X	Info

**Traffic-Filters, TF\_Profile Details:**

Protected Object/Policy: VDP\_Demo\_Lab  
Destination Address: 155.1.102.4  
Start Time: 30/07/23 13:29  
Duration: 00:00:15  
Attack Name: TF\_Profile

**Attack Details** | Attack Analytics

Additional Attack Attributes

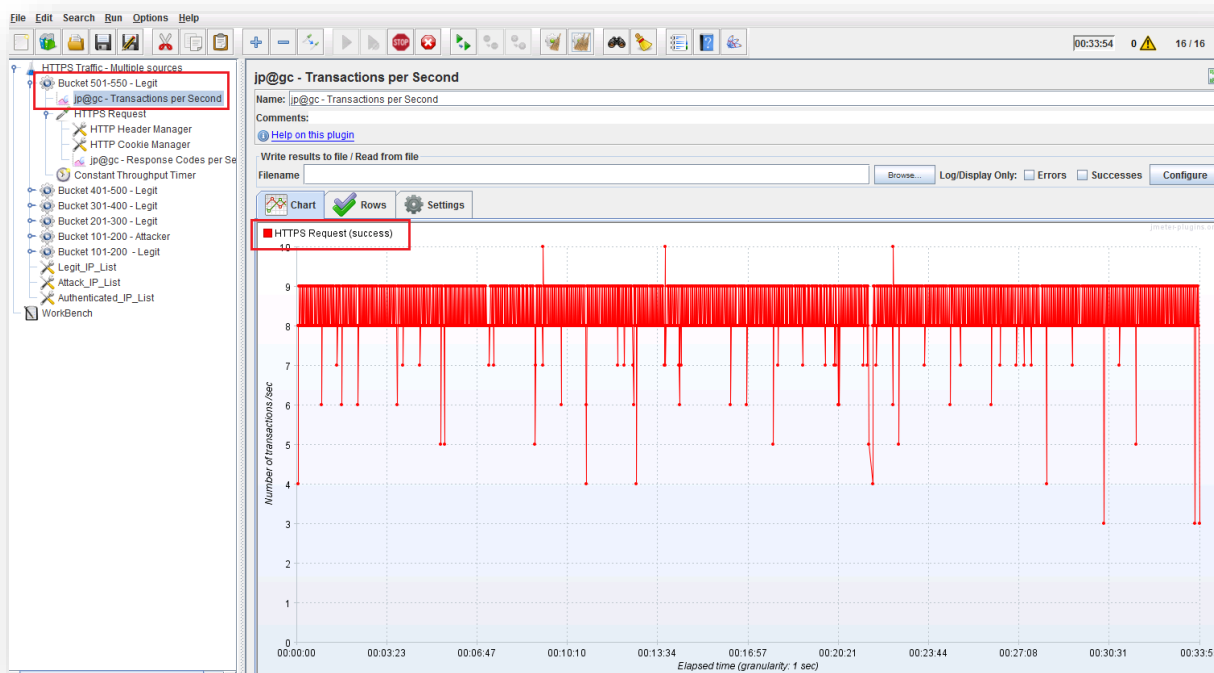
Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	700010	In	Drop	208-1688553507	1	1986
VLAN	MPLS RD	Source Port	Packet Type			
N/A	N/A	Multiple	Regular			

**Characteristics**

Filter Name	Filter ID	Attack Packet Rate (pps)
TF_Profile	700010	132

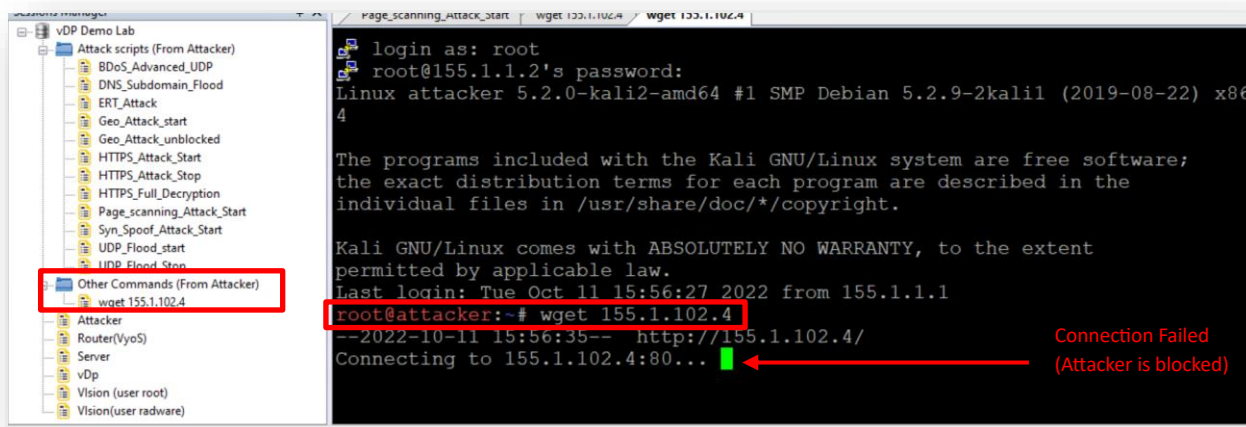


2. Open **JMeter** on the legitimate client and verify the information on the *Transactions Per Second* graph, select one of the legit buckets.

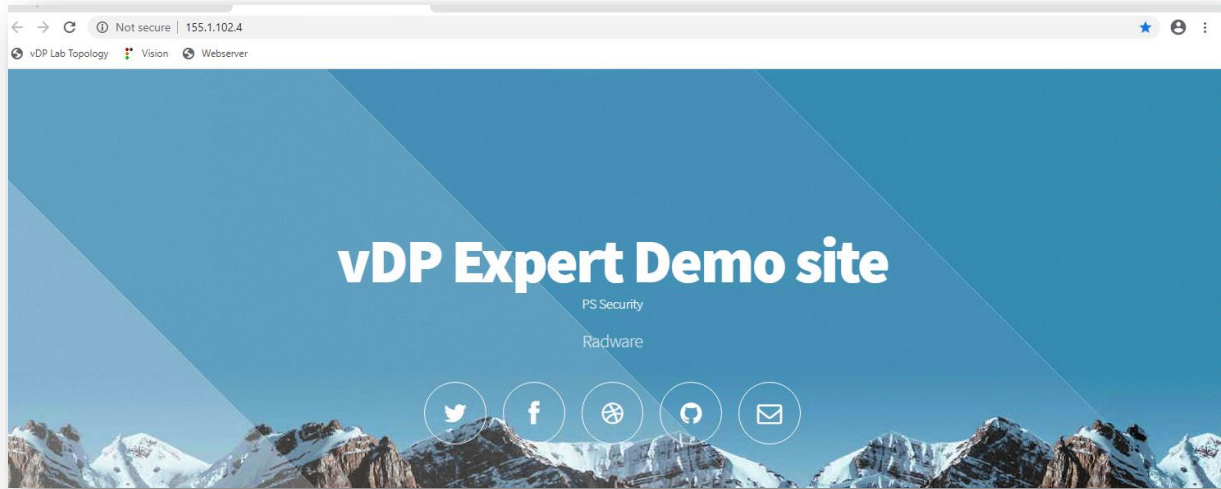


3. Check if the Attacker client can log in to the Webserver.

Select the **wget 155.1.102.4** icon located in the **Other Commands (From Attacker)** folder on the Session Manager:



4. Verify connectivity towards the attacking destination. Open the browser and select the **Site(155.1.102.4)** bookmark (URL: <http://155.1.102.4>):



## ERT Active Attacker Feed Protection

For more additional information about this scenario, please refer to the [“Appendix 3 - ERT Active Attacker Feed Protection \(Additional Info\)”](#) section.

**Before running the test: Verify if the last ERT Attacker feed schedule was run successfully by clicking the Scheduler button in Cyber Controller:**

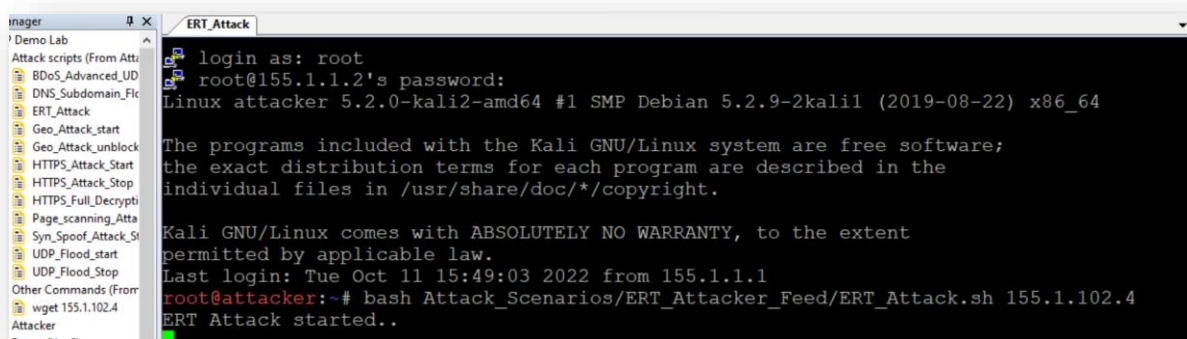
Scheduler

Task List

Task Type	Name	Description	Current Status	Enabled	Last Execution Status	Last Execution Date	Next Execution Date	Run
ERT Active Attackers Feed for DefensePro	ERT		Waiting	Enabled	Success	23.05.2023 09:38:59	23.05.2023 10:38:51	Minutes
Update Security Signature Files	Signature		Waiting	Enabled	Success	22.05.2023 23:40:46	29.05.2023 14:36:00	Weekly
Geolocation Feed	GEO		Waiting	Enabled	Success	22.05.2023 23:41:00	29.05.2023 12:00:00	Weekly

### Start a UDP Flood Attack and Verify Detection

- From the session manager, select the **ERT\_Attack\_start**.  
This script activates UDP flood attacks towards the Webserver from multiple sources that are on the ERT list.  
While the script is running, the following screen displays:



```

login as: root
root@155.1.1.2's password:
Linux attacker 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64

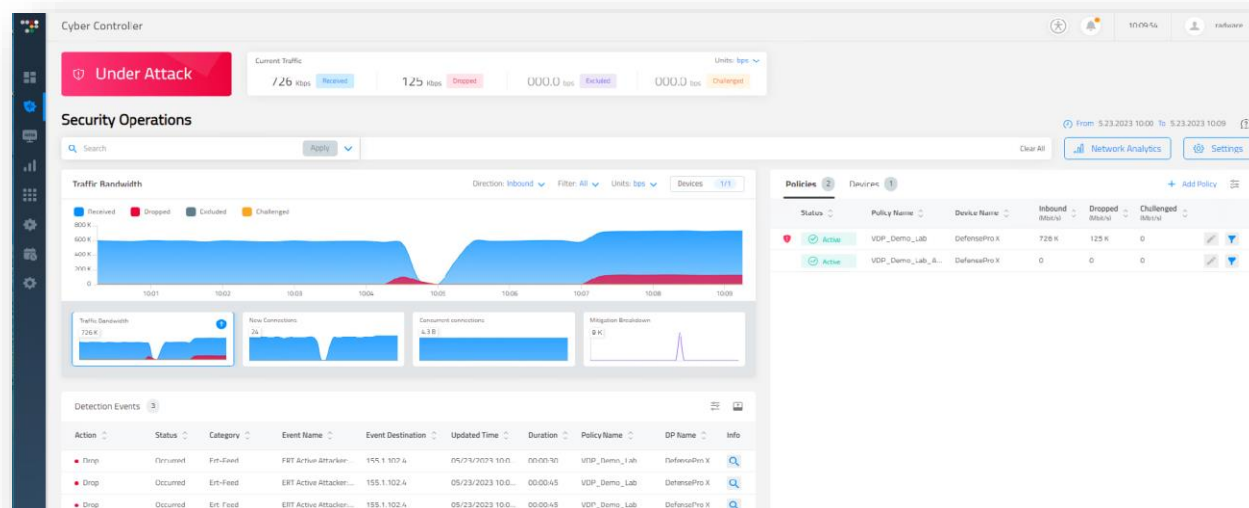
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 11 15:49:03 2022 from 155.1.1.1
root@attacker:~# bash Attack_Scenarios/ERT_Attacker_Feed/ERT_Attack.sh 155.1.102.4
ERT Attack started..
  
```

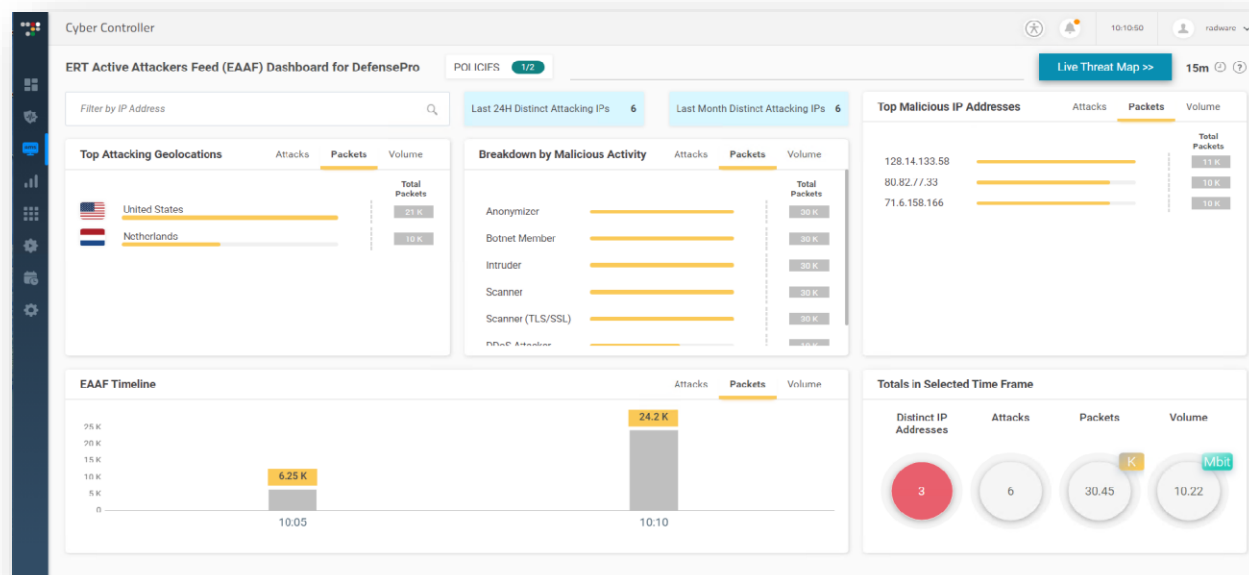
- In order to **stop** the attack, press **Ctrl +C**.

## Attack Mitigation

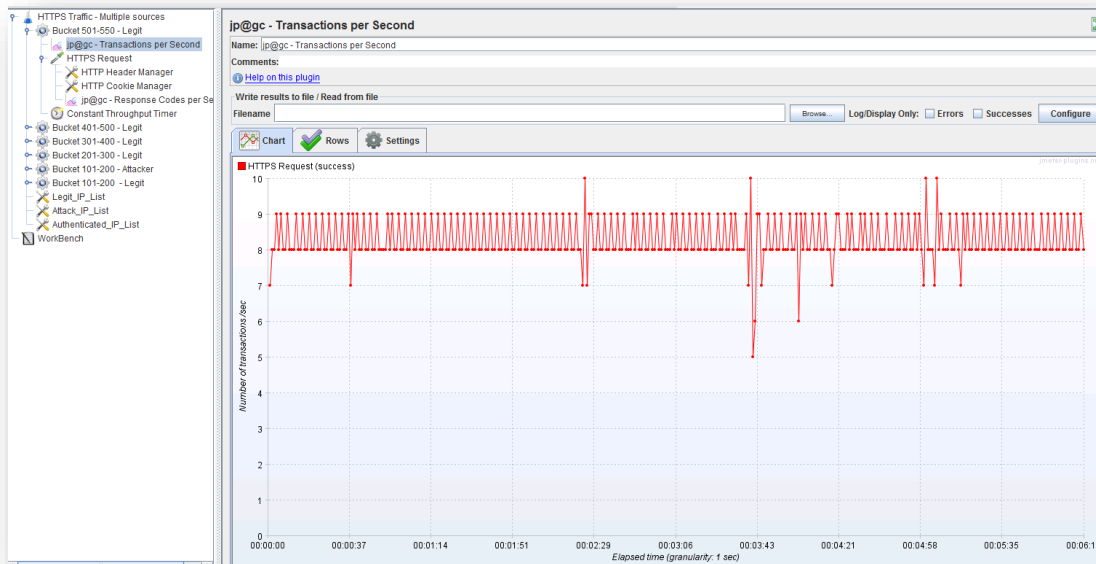
1. Verify the attack in Cyber Controller. Go to **Security Operations** -> **Real-Time Monitoring**:



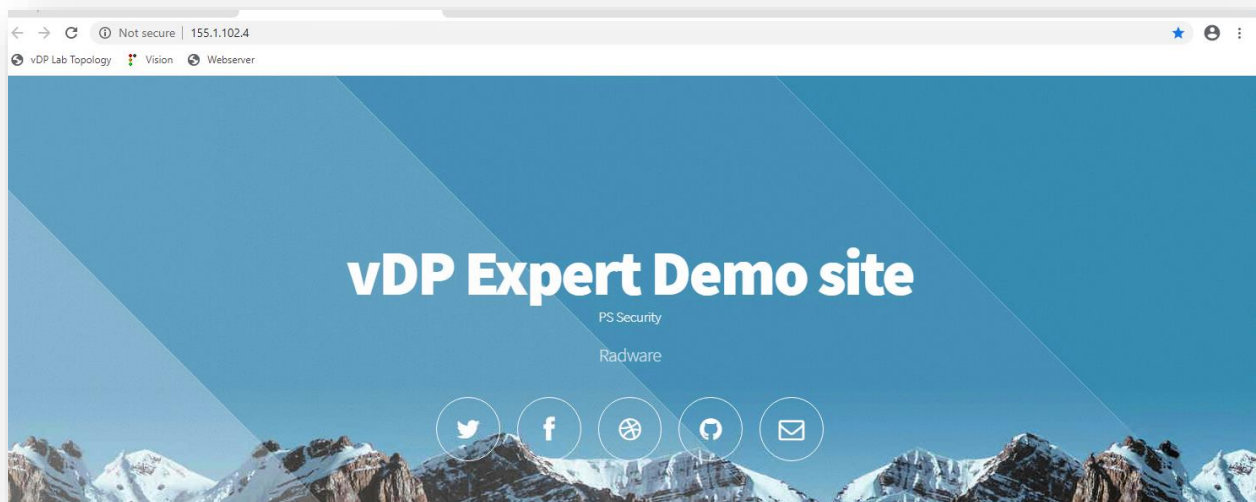
2. Verify the attack details on the **AMS > EAAF Dashboard**:



- Open **JMeter** on the legitimate client and verify the information on the *Transactions per Second* graph:



- Verify connectivity towards the attacking destination. Open the browser and select the **Webserver** bookmark (URL: <http://155.1.102.4>):

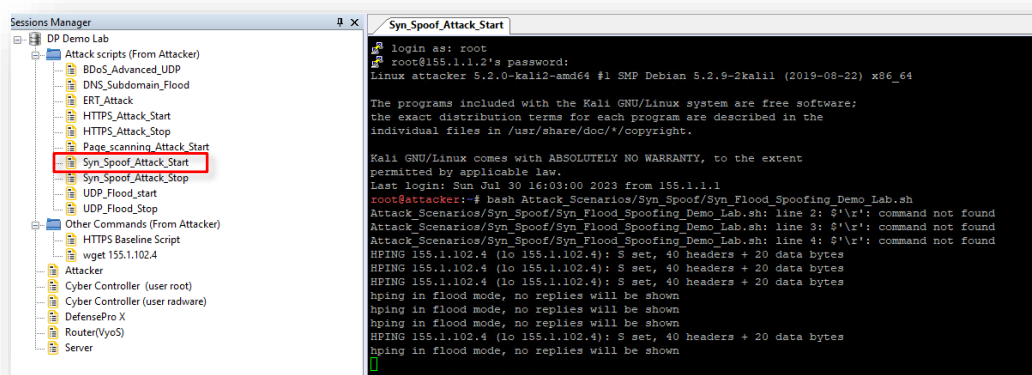


## Spoofed Syn Attack Protection

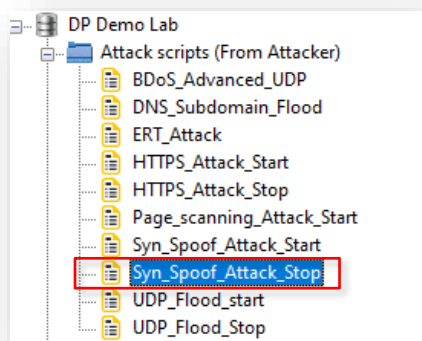
For more additional information about this scenario, please refer to the [“Appendix 4 – Spoofed Syn Attack Protection \(Additional Info\)”](#) section.

### Start a Spoofed Syn Flood Attack And verify Detection

1. From the session manager, select the **Syn\_Spoofed\_Attack\_start** .  
This script activates Spoofed Syn flood attacks towards the Webserver from multiple sources.  
While the script is running, the following screen displays:



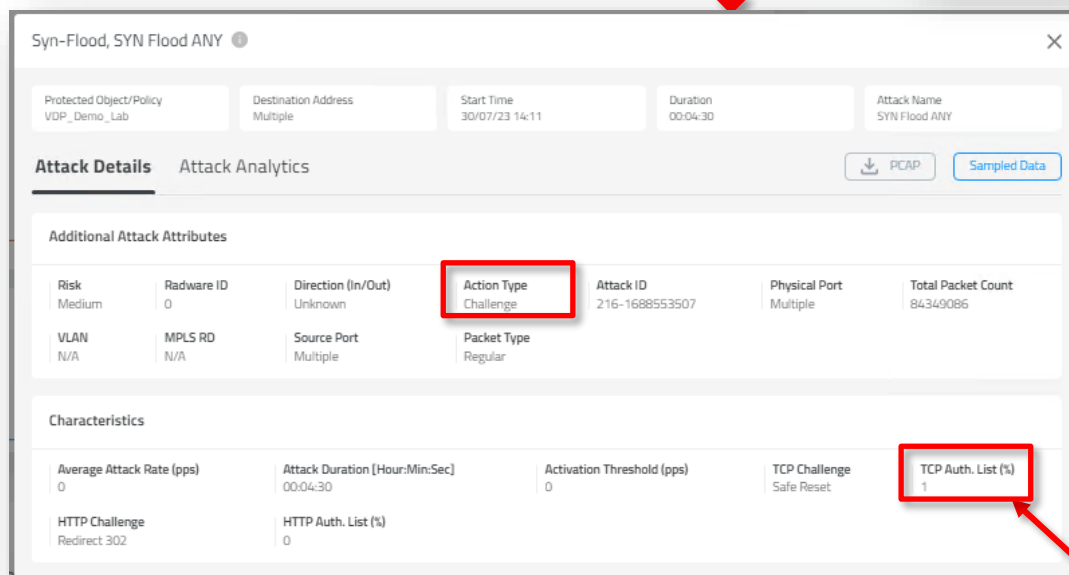
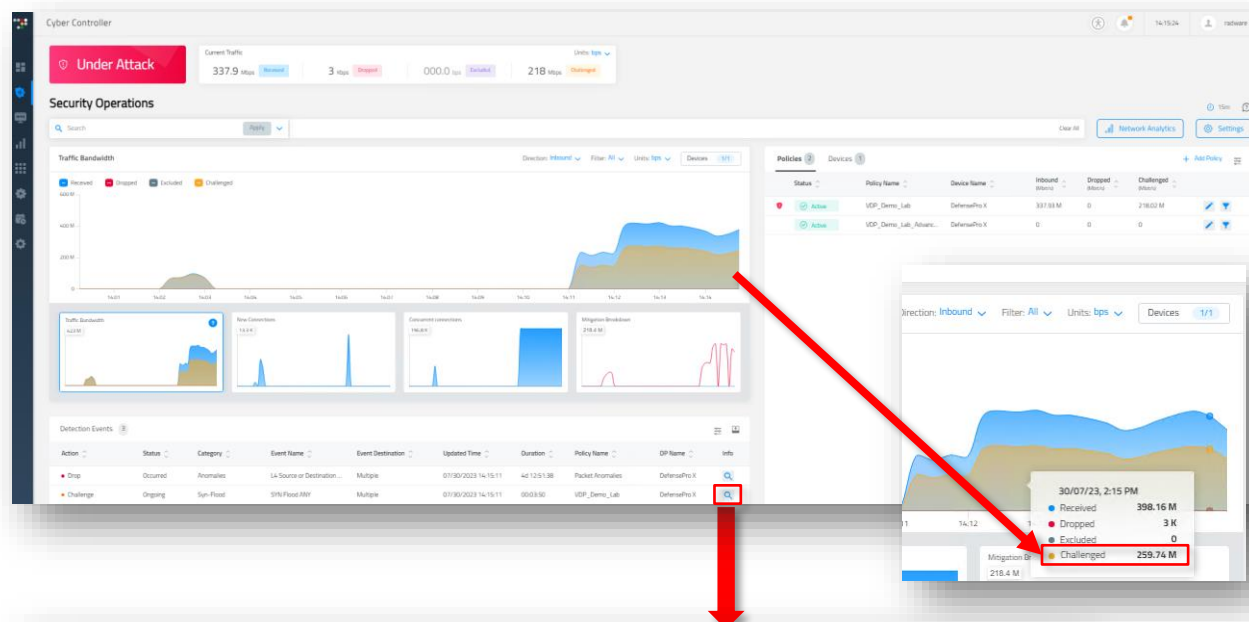
2. In order to **stop** the attack, double-click on **Syn\_Spoofed\_Attack**:





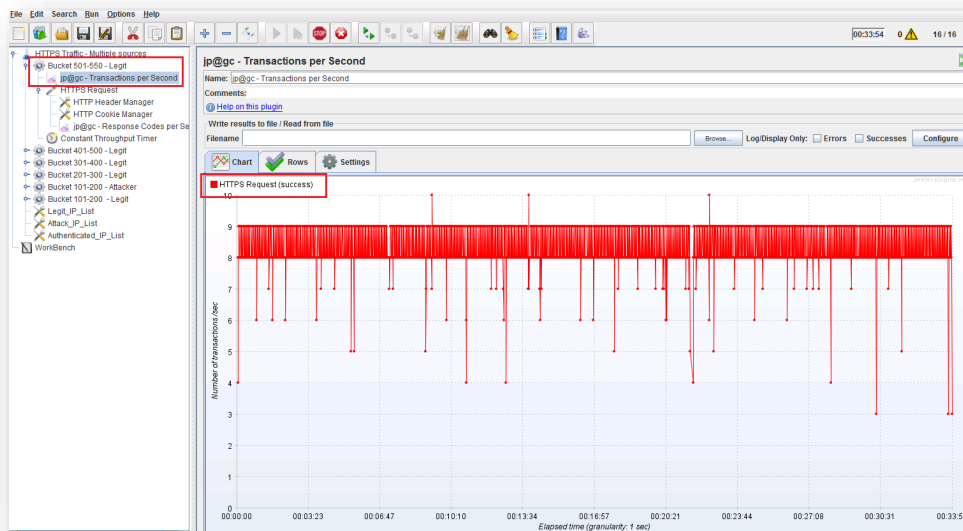
## Attack Mitigation

1. Verify the attack in Cyber Controller. Go to the **Security Operations -> Real-Time Monitoring**:

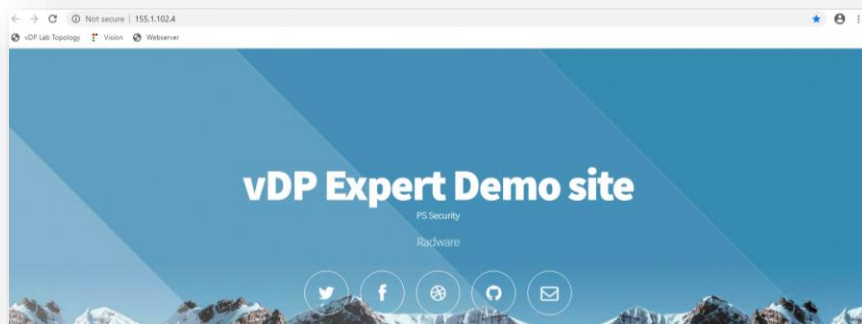


The **legit** user passed the challenge and get into the TCP authentication list.

2. Open **JMeter** on the legitimate client and verify the information on the *Transactions Per Second* graph, select one of the legit buckets.



3. Verify connectivity towards the attacking destination. Open the browser and select the **Webserver** bookmark (URL:http://155.1.102.4):



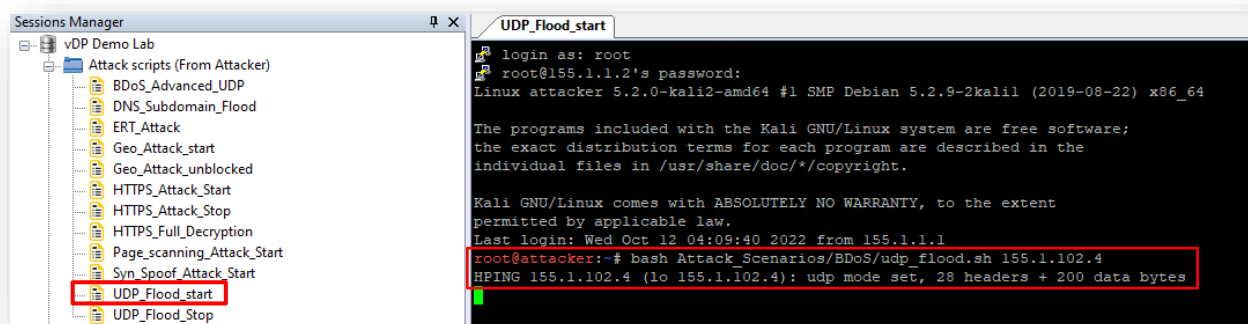


## BDoS Protection

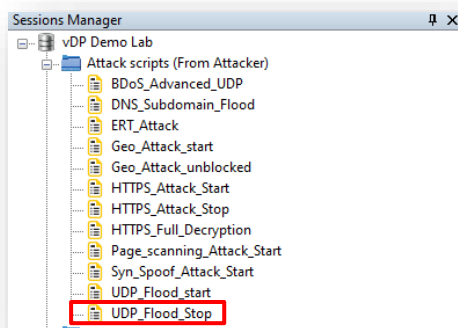
For more additional information about this scenario, please refer to the [“Appendix 5 - BDoS Protection \(Additional Info\)”](#) section.

### Create a UDP Flood Attack and Verify Detection

1. From the session manager, select the **UDP\_Flood\_start**.  
This script activates UDP flood attacks towards the web server from multiple sources.  
**The attack vectors are change after 100 seconds.**  
While the script is running, the following screen displays:

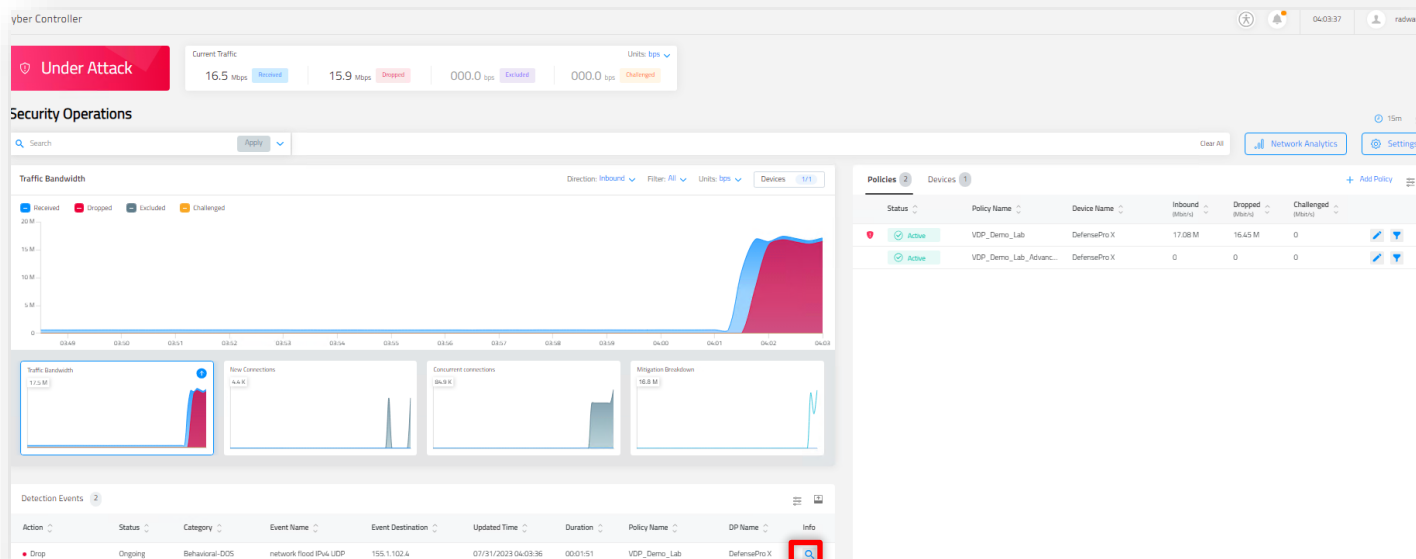


2. In order to **stop** the attack, double-click on **UDP\_Flood\_Stop**:

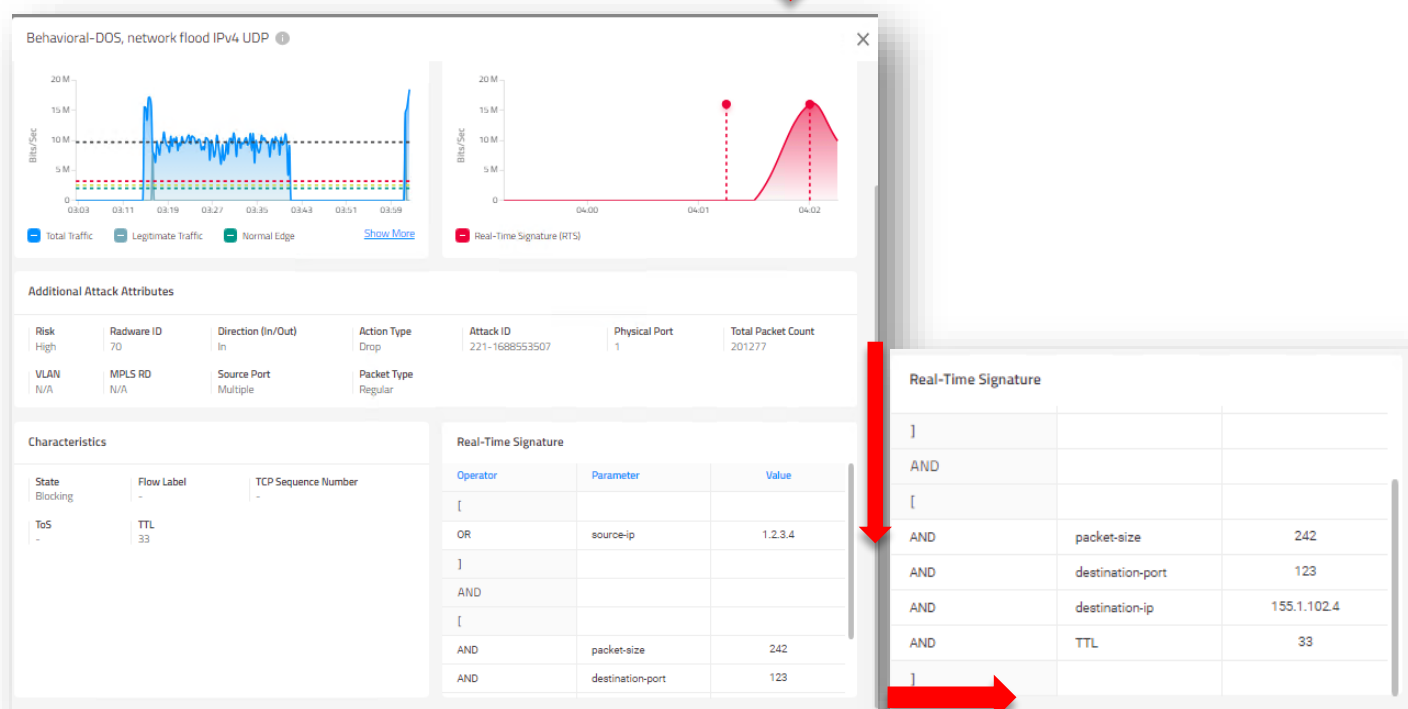


## Attack Mitigation

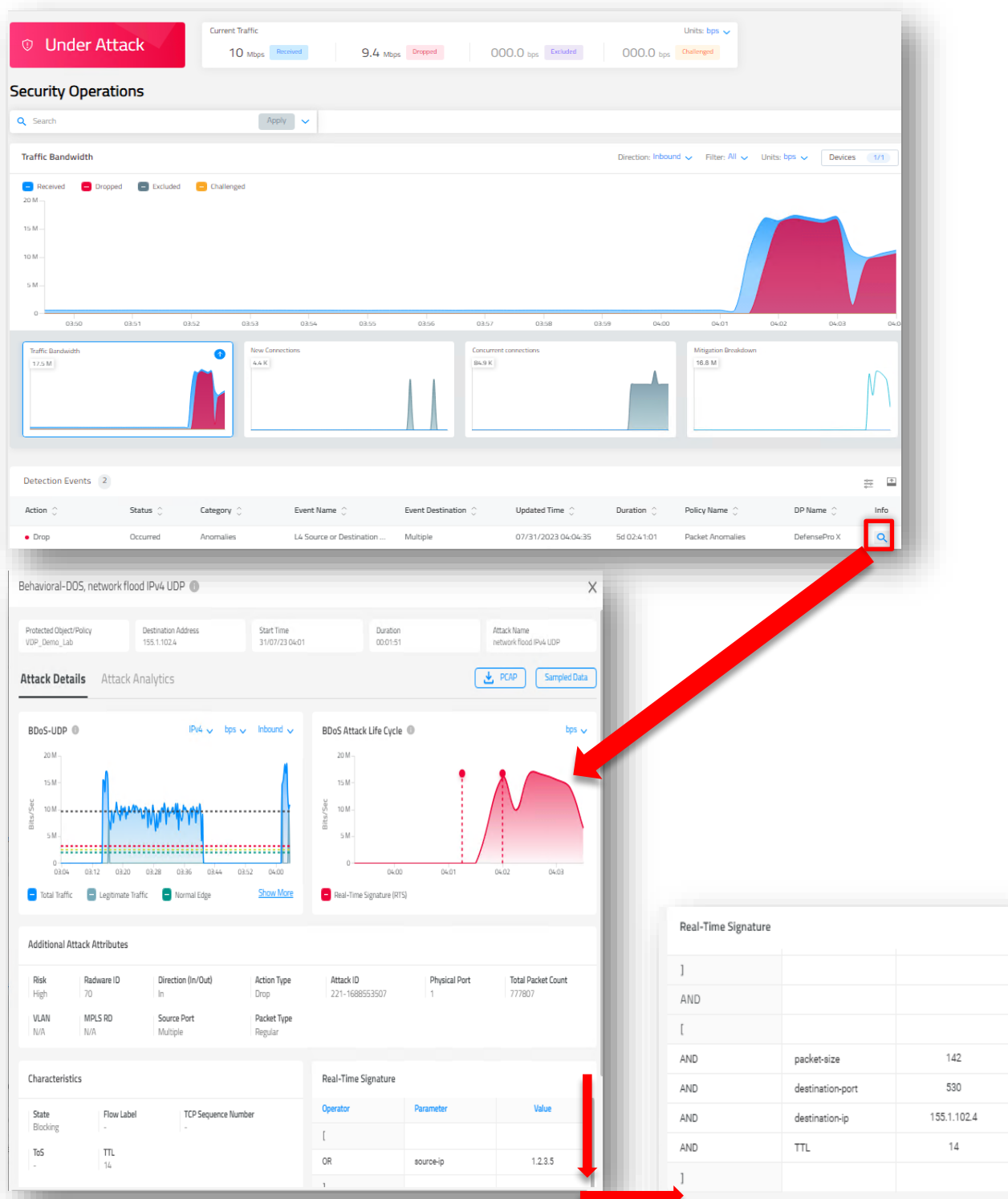
1. Verify the attack in Cyber Controller. Go to the **Security Operations -> Real-Time Monitoring**:



2. Verify the signature which DefensePro X generates for the first attack vectors:



3. Verify the signature which DefensePro X generates for the second attack vectors:



The screenshot displays the DefensePro X interface. At the top, a 'Current Traffic' summary shows 10 Mbps Received, 9.4 Mbps Dropped, 000.0 tps Excluded, and 000.0 tps Challenged. Below this, the 'Security Operations' section includes a 'Traffic Bandwidth' graph showing a significant spike in traffic around 04:02. A red arrow points from the 'Info' icon in the 'Detection Events' table to the 'Attack Details' panel.

The 'Detection Events' table shows a single event:

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
Drop	Occurred	Anomalies	L4 Source or Destination ...	Multiple	07/31/2023 04:04:35	5d 02:4:101	Packet Anomalies	DefensePro X	<a href="#">Info</a>

The 'Attack Details' panel for 'Behavioral-DOS, network flood IPv4 UDP' shows the following information:

- Protected Object/Policy:** VDP\_Demo\_Lab
- Destination Address:** 155.1.102.4
- Start Time:** 31/07/23 04:01
- Duration:** 00:01:51
- Attack Name:** network flood IPv4 UDP

The 'Attack Details' section includes two graphs: 'BDOS-UDP' and 'BDOS Attack Life Cycle'. A red arrow points from the 'Real-Time Signature (RTS)' link in the 'BDOS Attack Life Cycle' graph to the 'Real-Time Signature' table.

**Additional Attack Attributes:**

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	70	In	Drop	221-1686553507	1	777807

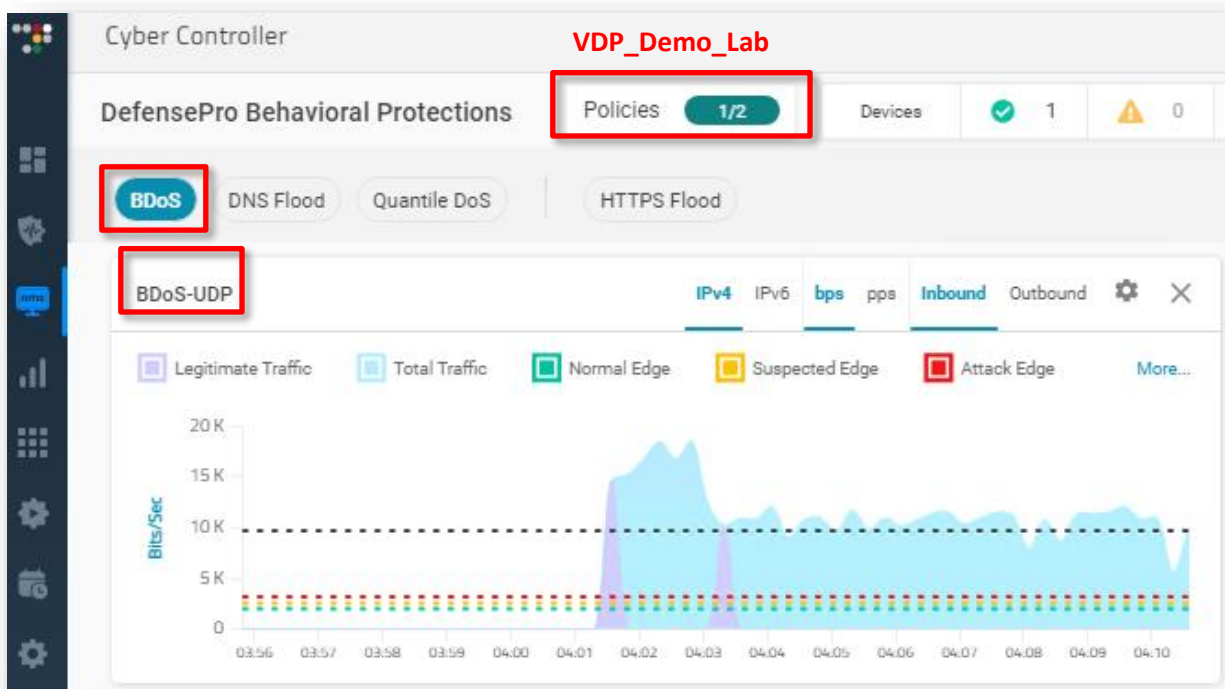
**Characteristics:**

State	Flow Label	TCP Sequence Number
Blocking	-	-

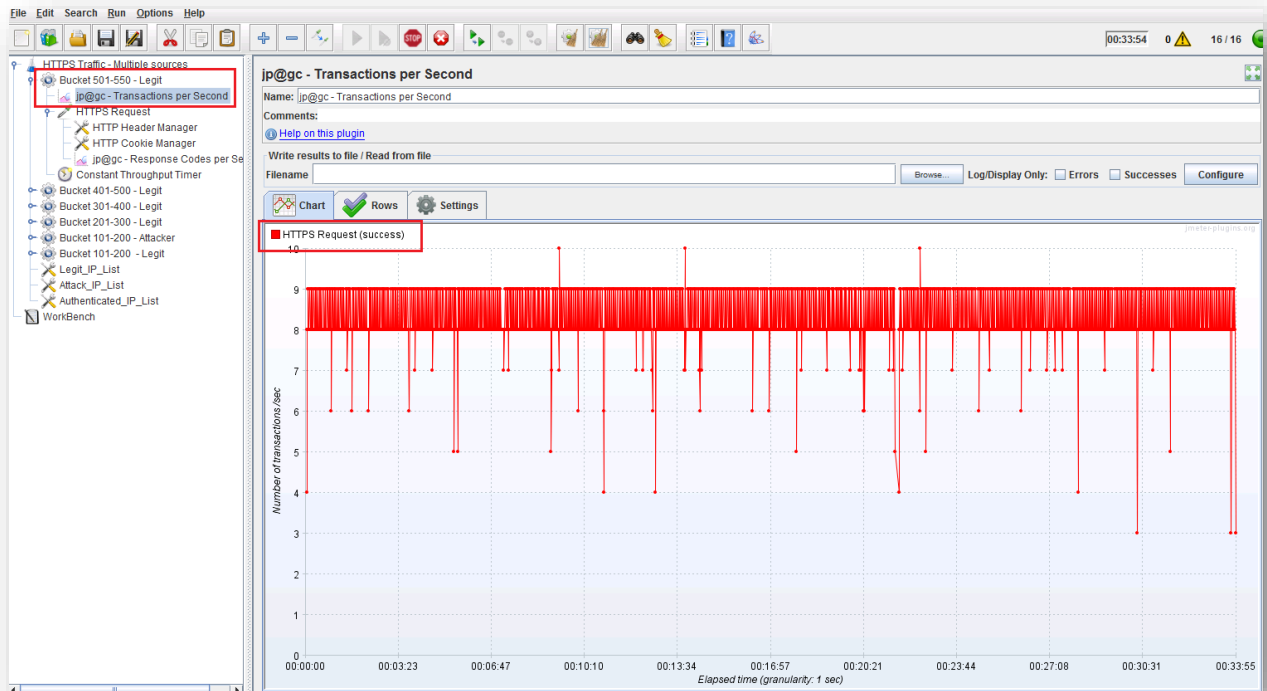
**Real-Time Signature:**

Operator	Parameter	Value
[		
AND	packet-size	142
AND	destination-port	530
AND	destination-ip	155.1.102.4
AND	TTL	14
]		

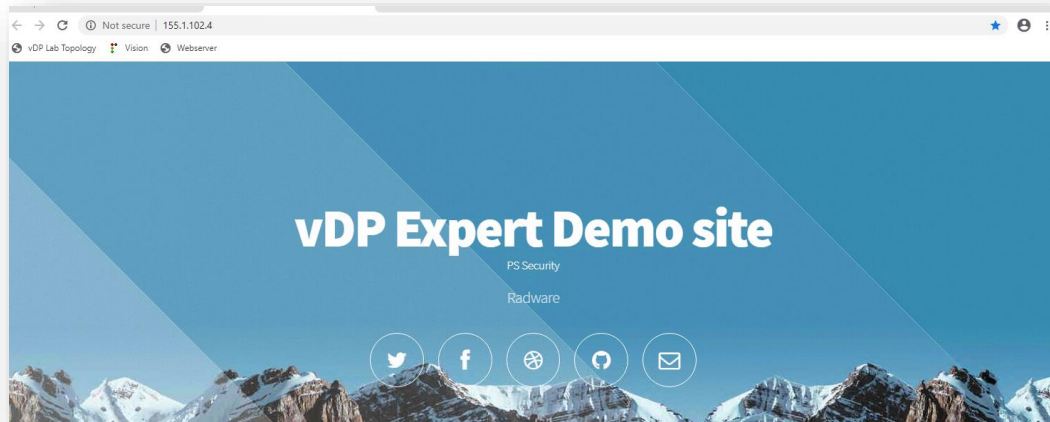
2. Check the current baselines of each BDoS controller in the **AMS > DefensePro Behavioral Protections** dashboard:



- Open **JMeter** on the legitimate client and verify the information on the *Transactions per Second* graph:



- Verify connectivity towards the attacking destination. Open the browser and select the **Webserver** bookmark (URL: <http://155.1.102.4>):



## BDoS Advanced UDP Protection

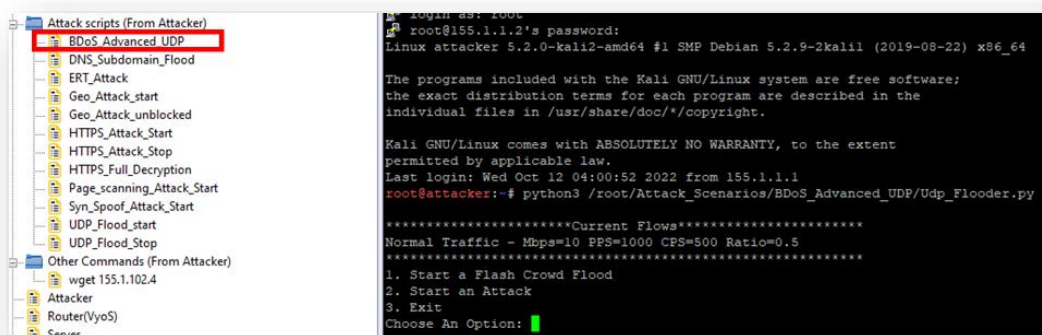
For more additional information about this scenario, please refer to the [“Appendix 6 - BDoS Advanced Protection \(Additional Info\)”](#) section.

### Start Legitimate Traffic

From the session manager, select the **BDoS\_Advanced\_UDP**.

The script **automatically** starts with 10 Mbps of a legitimate UDP traffic once activated.

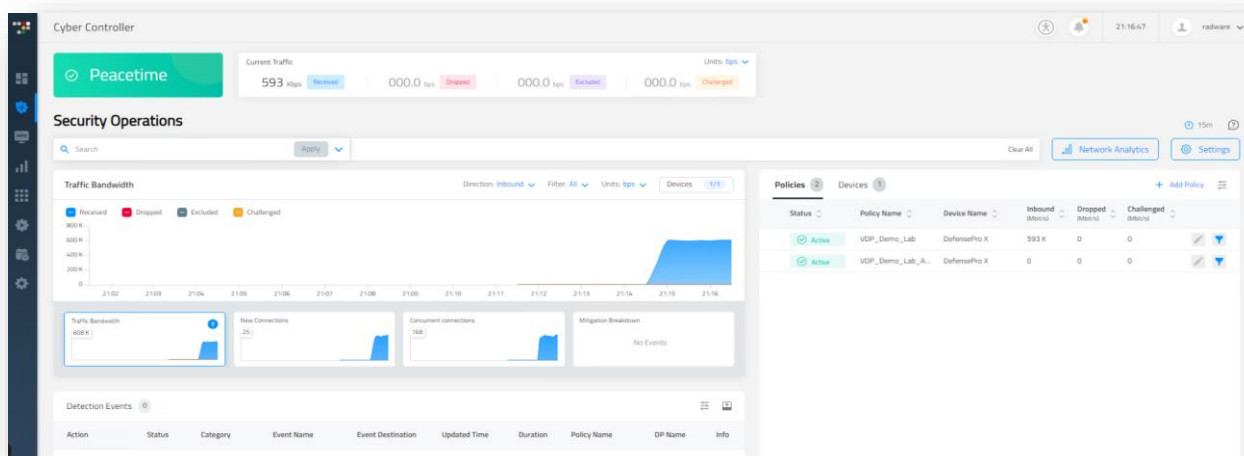
**Note:** The following output shows the current flows and the configured parameters.



```

root@kali:~# python3 /root/Attack_Scenarios/BDoS_Advanced_UDP/Udp_Flooder.py
*****Current Flows*****
Normal Traffic - Mbps=10 PPS=1000 CPS=500 Ratio=0.5
*****
1. Start a Flash Crowd Flood
2. Start an Attack
3. Exit
Choose An Option: 1
  
```

1. Once the legitimate traffic has started, it is displayed in the **Security Operations -> Real-Time Monitoring**:



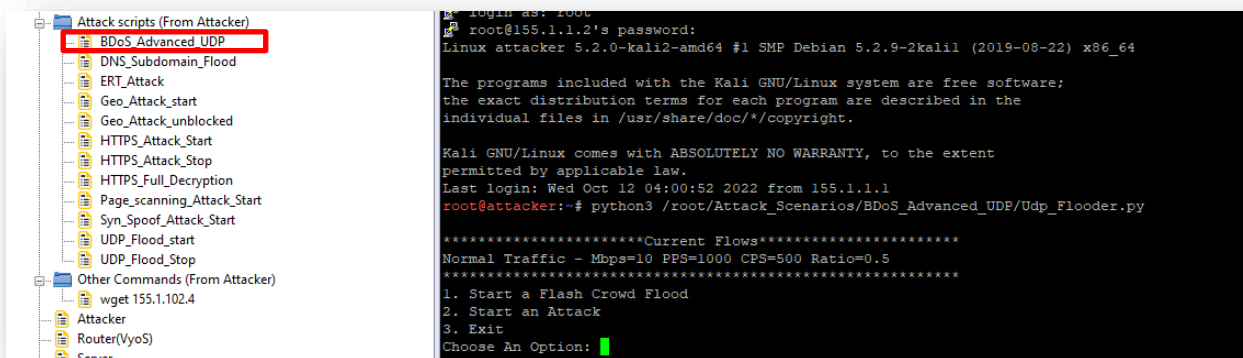
### Start a UDP Flood Attack



1. Select again the **BDoS\_Advanced\_UDP** icon located in the **Attack scripts** folder on the Session Manager.

The script runs 10 Mbps of a legitimate UDP traffic once activated.

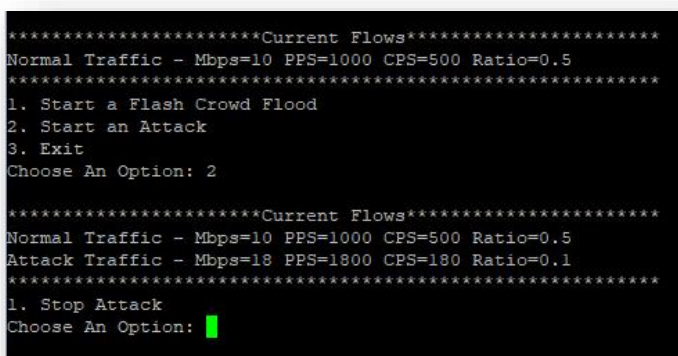
**Press 2**, in order to activate UDP Flood attack.



The script runs two different flows.

1. Normal Traffic
2. UDP Flood Attack

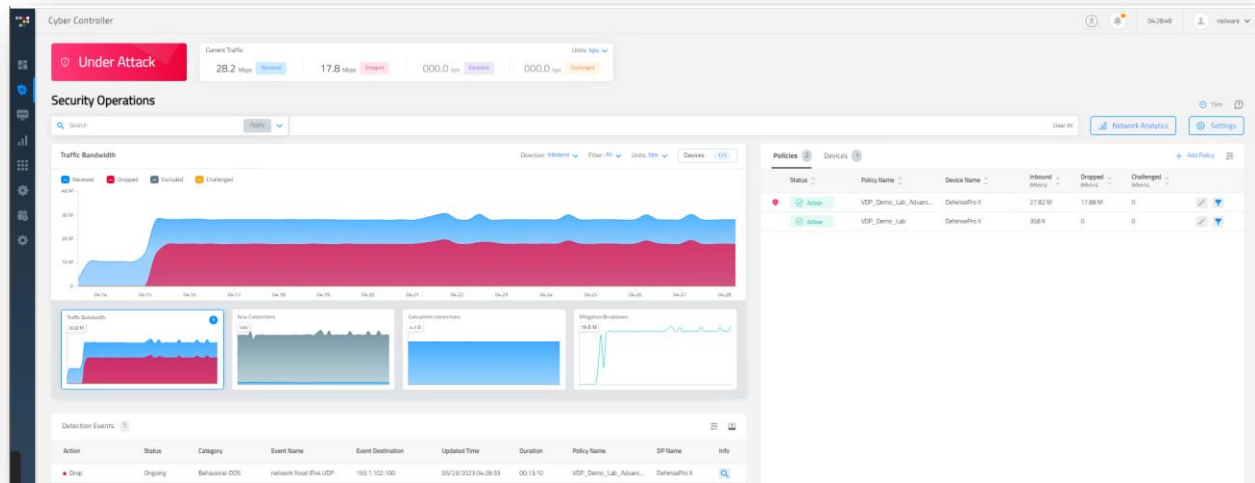
While the script is running, the following screen displays:



2. In order to **stop** the attack traffic, press **1**.

## Attack Mitigation


1. Verify the attack in Cyber Controller. Go to the **Security Operations -> Real-Time Monitoring**:





2. Verify the attack details and the BDoS fingerprint that the DefensePro X generated:

Detection Events 1

Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
Drop	Ongoing	Behavioral-DOS	network flood IPv4 UDP	155.1.102.100	05/23/2023 04:29:59	00:14:37	VDP_Demo_Lab_Advanc...	DefensePro X	

**Behavioral-DOS, network flood IPv4 UDP**

Protected Object/Policy: VDP\_Demo\_Lab\_Advanced Destination Address: 155.1.102.100 Start Time: 26/07/23 23:40 Duration: 00:01:43 Attack Name: network flood IPv4 UDP

**Attack Details** **Attack Analytics** [Download PCAP](#) [Sampled Data](#)

**BDoS-UDP** **BDoS Attack Life Cycle**

**Additional Attack Attributes**

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	70	In	Drop	114-1688553507	1	152840

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

**Characteristics**

State	Flow Label	TCP Sequence Number
Blocking	-	-
ToS	TTL	
-	255	

**Real-Time Signature**

Operator	Parameter	Value
[		
OR	id-number	123
]		

**Additional Attack Attributes**

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	70	In	Drop	99-1684815078	1	1725480

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

**Characteristics**

State	Flow Label	TCP Sequence Number
Blocking	-	-
ToS	TTL	
-	255	

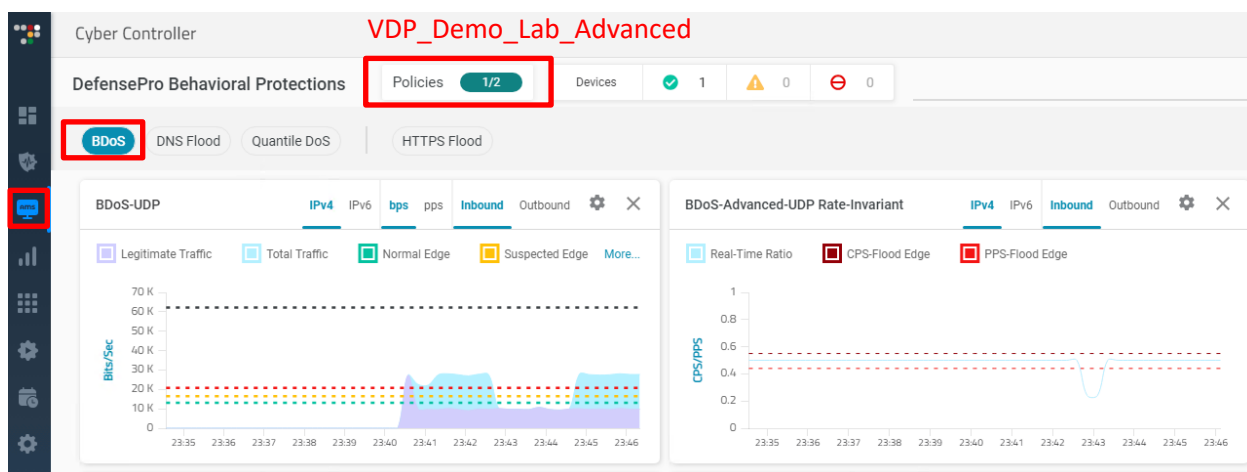
**Real-Time Signature**

Operator	Parameter	Value
[		
OR	id-number	123
]		
AND		
[		
AND	packet-size	1242
AND	destination-port	123
AND	destination-ip	155.1.102.100
AND	TTL	255
]		

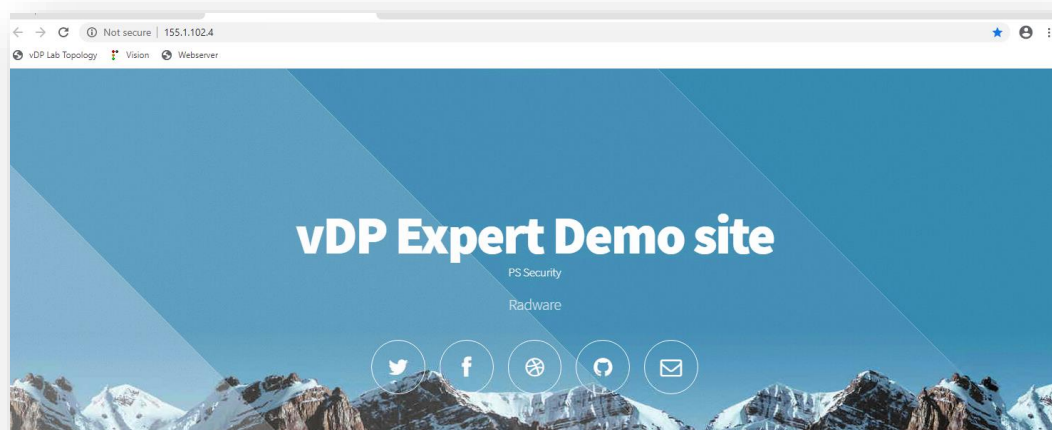
**Real-Time Signature**

]		
AND		
[		
AND	packet-size	1242
AND	destination-port	123
AND	destination-ip	155.1.102.100
AND	TTL	255
]		

- Verify the BDoS UDP graph on the **AMS > DefensePro Behavioral Protections** (choose the VDP\_Demo\_Lab\_Advanced policy):



- Verify connectivity towards the attacking destination. Open the browser and select the **Site (155.1.102.100)** bookmark (URL: <http://155.1.102.100>):



### ***Start a UDP Flood Flash Crowded Legit Traffic***

1. Select again the **BDoS\_Advanced\_UDP** icon located in the **Attack scripts** folder on the Session Manager.

The script runs 10 Mbps of a legitimate UDP traffic once activated.

**Press 1**, in order to activate Flash-Crowded traffic.

The script runs two different flows.

1. Normal Traffic
2. Flash-Crowded traffic.

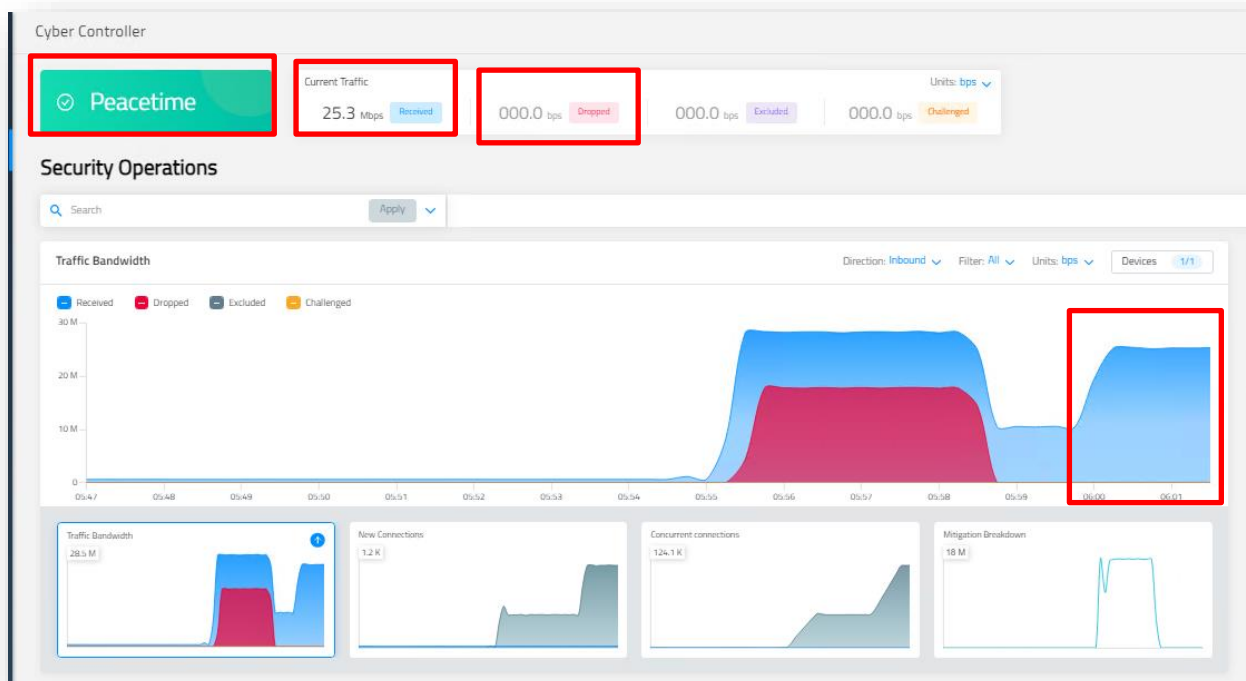
```
*****Current Flows*****
Normal Traffic - Mbps=10 PPS=1000 CPS=500 Ratio=0.5
*****
1. Start a Flash Crowd Flood
2. Start an Attack
3. Exit
Choose An Option: 1

*****Current Flows*****
Normal Traffic - Mbps=10 PPS=1000 CPS=500 Ratio=0.5
Flash Crowd Traffic - Mbps=15 PPS=1500 CPS=750 Ratio=0.5
*****
1. Stop Flash Crowd
Choose An Option: 1
```

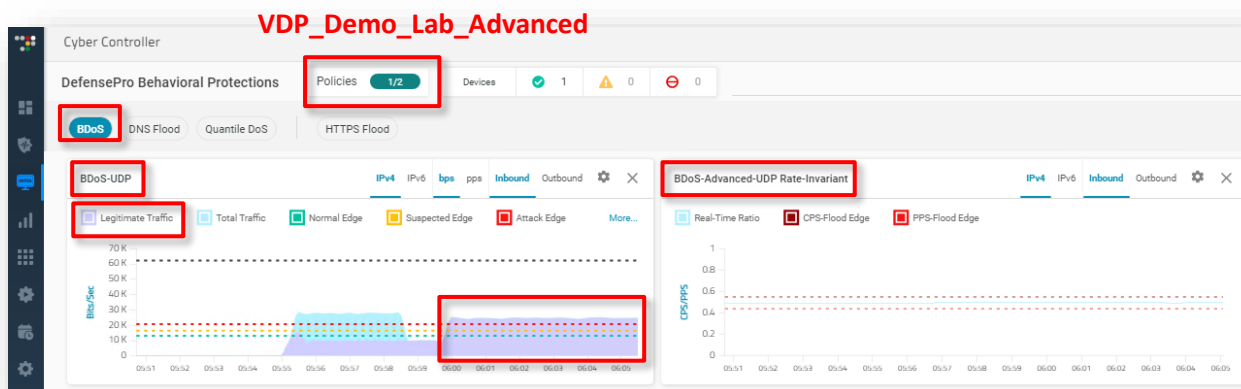
2. In order to **stop** the Flash-Crowded traffic, press **1**.

## Verify Flash Crowd Isn't Getting Blocked

1. Verify that all the traffic (legit traffic with the flash crowd traffic) **isn't** getting blocked and that there **isn't** any attack detection. You can verify it on:



2. Verify the BDoS UDP graph on the **AMS > DefensePro Behavioral Protections** (choose the VDP\_Demo\_Lab\_Advanced policy):



## DNS Flood Protection

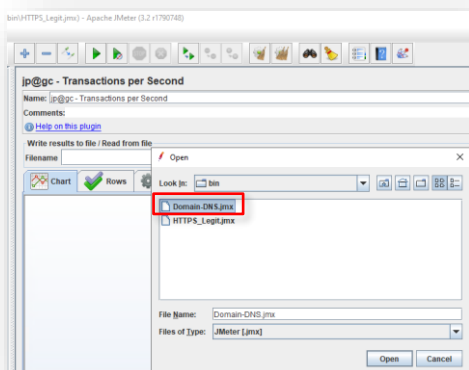
For more additional information about this scenario, please refer to the [“Appendix 7 - DNS Flood Protection \(Additional Info\)”](#) section.

### Start DNS Legitimate Traffic

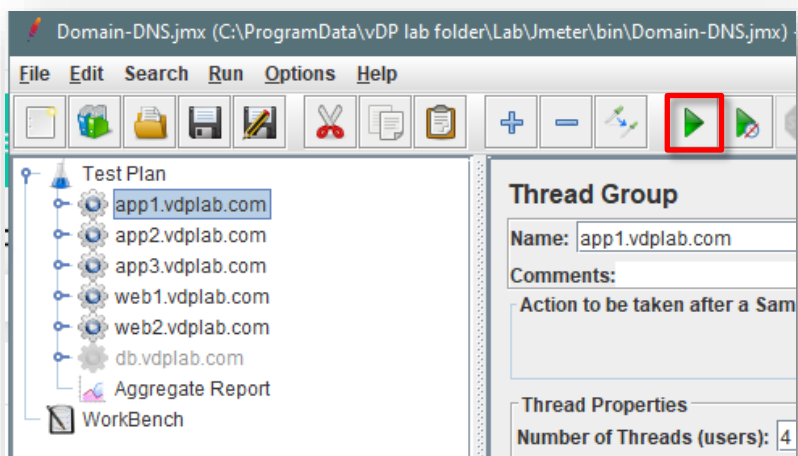
**Before start this scenario, you need first to stop the HTTPS legitimate traffic** (running two JMeters on parallel, can cause issue with resources of the nested ESXI of the demo lab).

1. Open the DNS legitimate traffic on the JMeter:

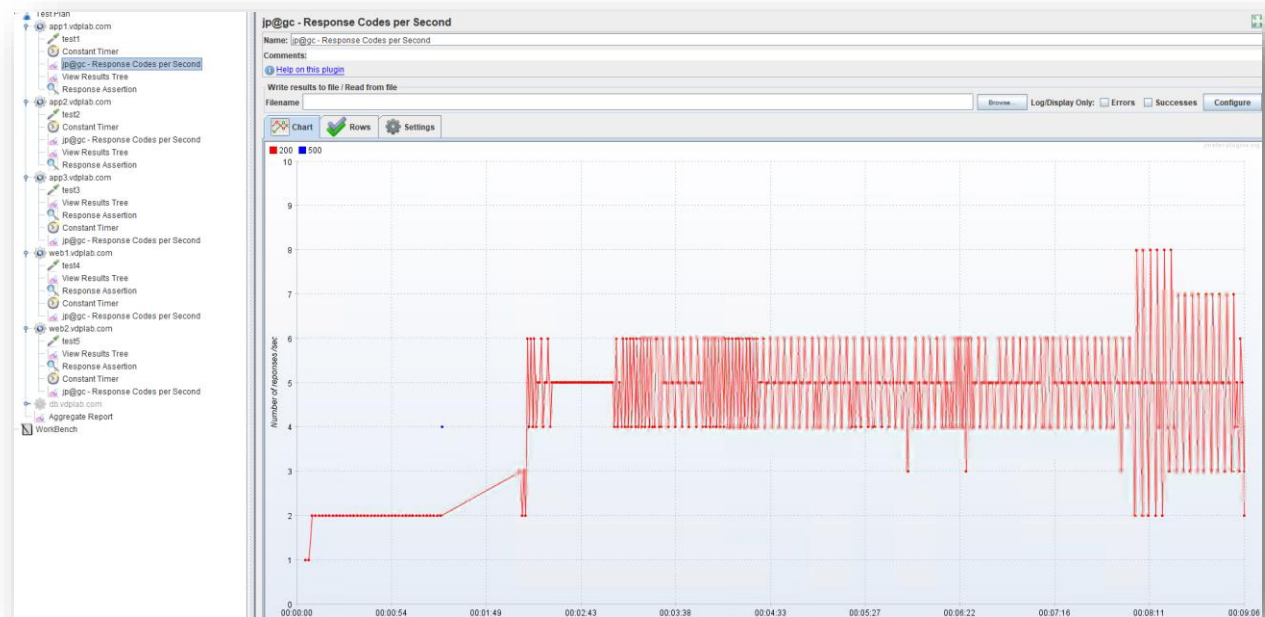
Legitimate script location: **Desktop\Lab\Jmeter\JM legit script\bin\Domain-DNS.jmx**



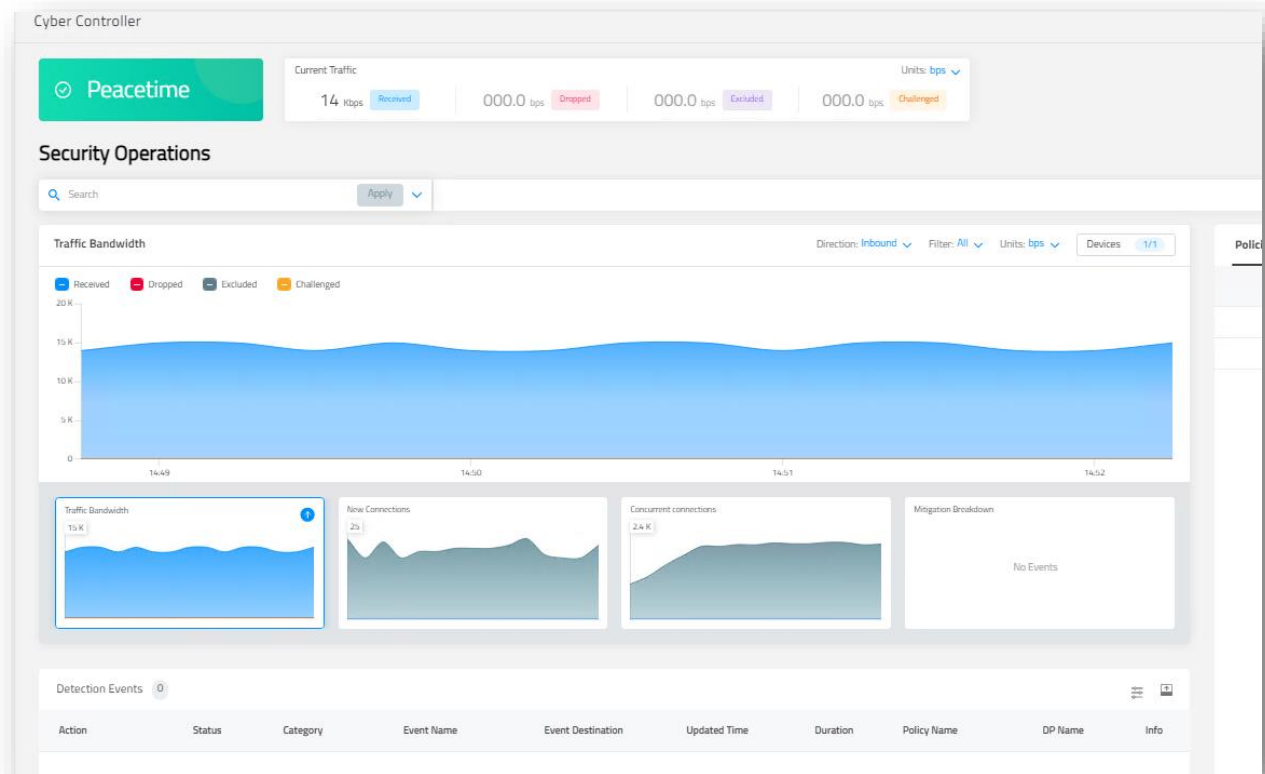
2. Press start.



### 3. Verify the legitimate queries response code:



4. Once the legitimate traffic has started, it is displayed in the **Security Operations -> Real-Time Monitoring**:



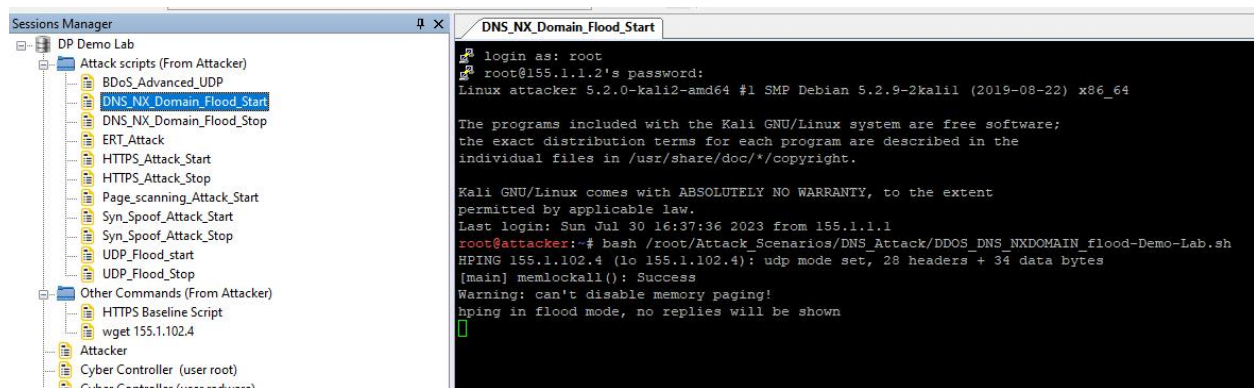


## Start a DNS NX Domain Flood Attack and Verify Detection

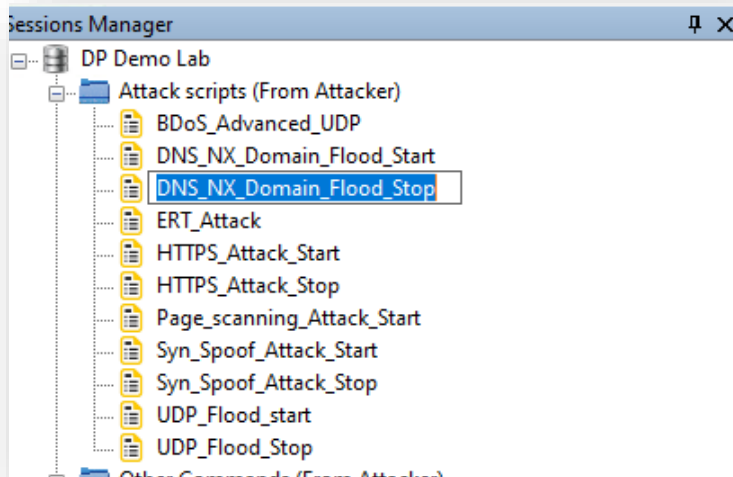
1. From the session manager, select the **DNS\_NX\_Domain\_Flood\_Start**.

This script activates NX Domain flood attacks towards the DNS server from multiple sources.

While the script is running, the following screen displays:



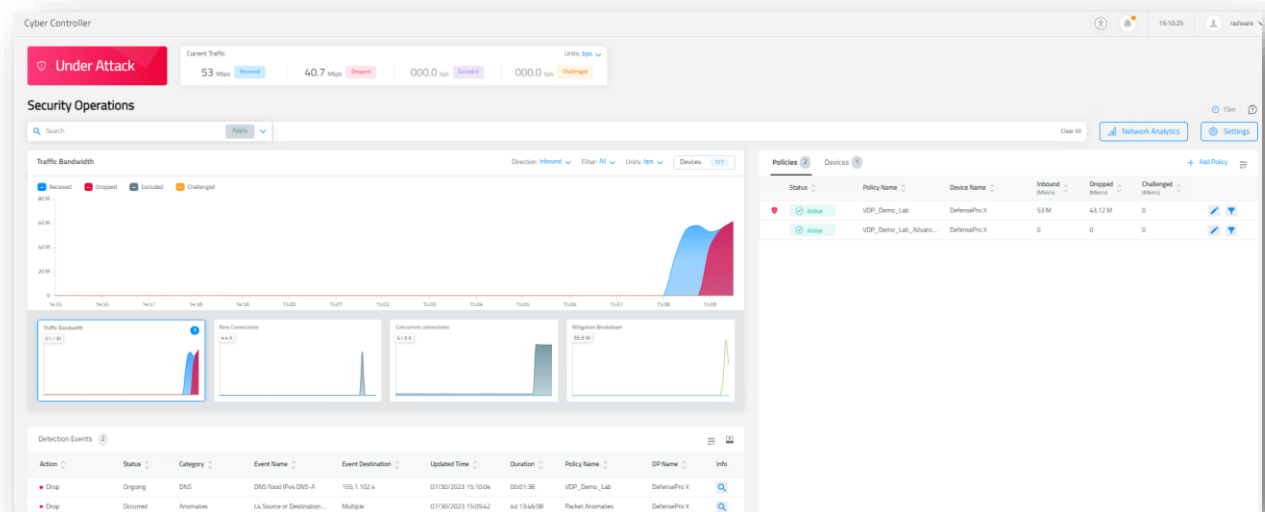
2. In order to **stop** the attack, double-click on **DNS\_NX\_Domain\_Flood\_Stop**.



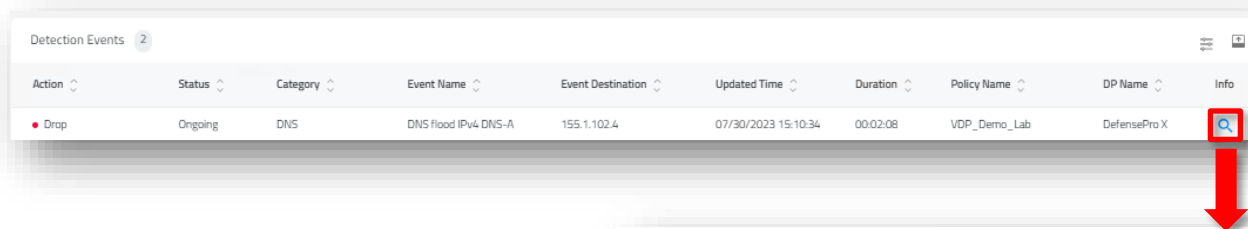


## Attack Mitigation

1. Verify the attack in Cyber Controller. Go to the **Security Operations -> Real-Time Monitoring**:



- On the detection events section, you will find the event attack. You can verify the attack details by clicking on the magnifying glass button:



The screenshot shows the 'Detection Events' section with a table of events. The event 'DNS flood IPv4 DNS-A' is selected. A red arrow points to the magnifying glass icon in the 'Info' column.

The event details are displayed in a modal window titled 'DNS, DNS flood IPv4 DNS-A'. The modal contains the following sections:

- Attack Details:**
  - Protected Object/Policy: VDP\_Demo\_Lab
  - Destination Address: 155.1.102.4
  - Start Time: 30/07/23 15:08
  - Duration: 00:02:30
  - Attack Name: DNS flood IPv4 DNS-A
- Attack Analytics:**
  - DNS-A: A line graph showing traffic volume over time.
  - DNS Attack Life Cycle: A line graph showing the attack's progression.
- Additional Attack Attributes:**

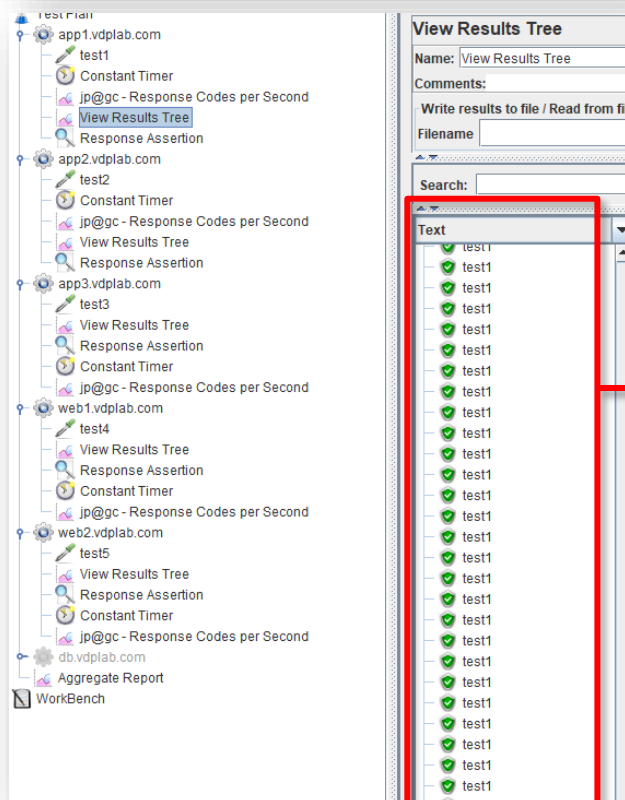
Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	450	In	Drop	218-1688553507	1	155,281,776
VLAN	MPLS ID	Source Port	Packet Type			
N/A	N/A	Multiple	Regular			
- Characteristics:**

DNS Query	DNS An Query Count	TTL	DNS ID
www.mylab.inside	-	64	9611
DNS Query Count	L4 Checksum	State	Mitigation Action
-	-	Blocking	Signature Rate Lim
- Real-Time Signature:**

Operator	Parameter	Value
[		
OR	dns-id	9611
]		
[		
AND	dns-qname	www.mylab.inside
AND	dns-flags	0

A red arrow points to the 'Real-Time Signature' table, indicating the next step in the verification process.

3. Open **JMeter** on the legitimate client and verify the information on the *Transactions per Second* graph and check the *results tree*:

After the attack get blocked, we can see that the DNS Queries from legit users don't get blocked, and they keep receiving DNS responses from the DNS server.

## APPENDIX 1 - HTTPS PROTECTION (ADDITIONAL INFO)

### Protection Overview

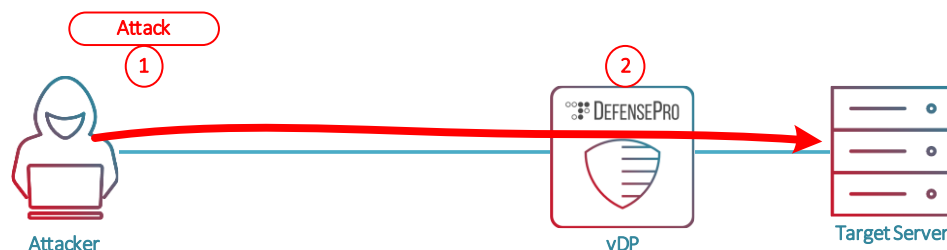
The HTTPS Flood mechanism introduced in DefensePro8 version 8.18.0.0 aims to stop denial of service (DoS) attacks on HTTPS servers by effectively blocking malicious traffic towards an attacked server.

By using the number of requests per second and outbound size per second, DefensePro X can create a baseline of the legitimate traffic behaviour and identify the case where the ratio of the request/response is increased significantly (above the baseline) and at the same time the average response size is also increased high above the baseline, which means the server is under attack.

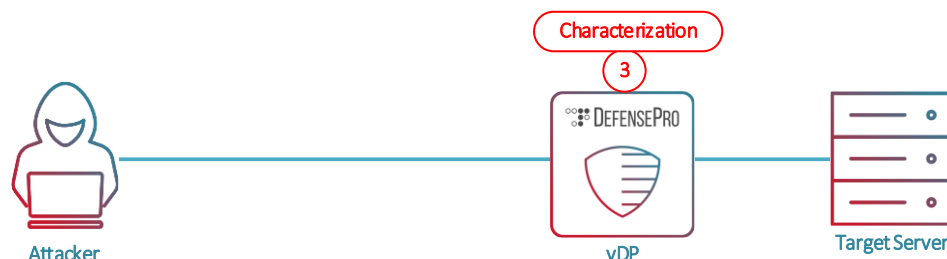
Inbound request rate learning is based on the rate of packets with an SSL record header of Content type: "Application Data (23)"

### Scenario Steps Overview

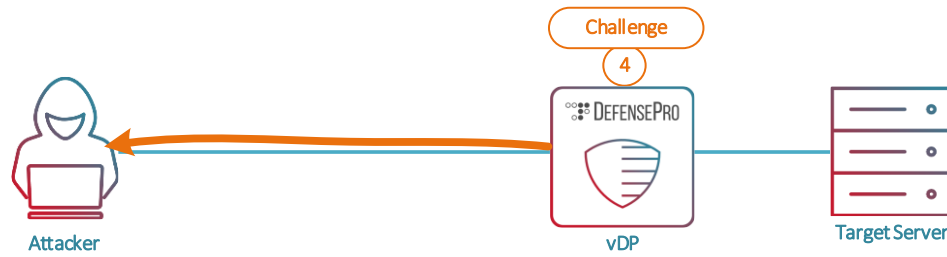
1. The attacker generates HTTPS Flood traffic from different sources towards the Webserver.
2. Detection on DefensePro begins:



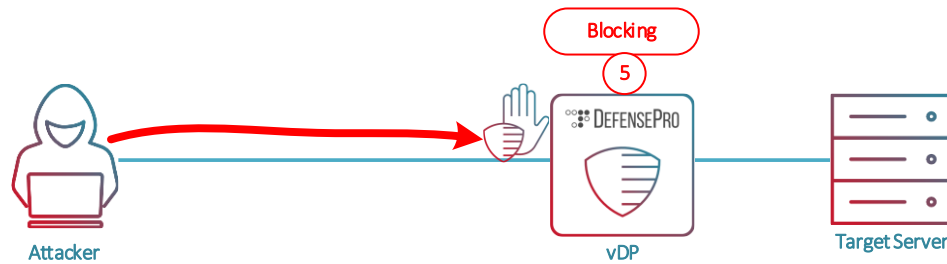
3. The attacker traffic rate goes above the Attack Edge baselines. The Detection phase begins HTTPS protection and enters the characterization stage:



4. While in the characterization stage, DefensePro challenges all the suspected sources:



5. When the attacker is not able to pass the challenge, all the traffic coming from this source is blocked:



## Configurations

HTTPS Protection

Action

Block and Report

▼

☒

Packet Reporting

Mitigations Actions

☒

First Request Mitigation on Suspect Sources

Use HTTPS Authentication on Suspect Sources.

☐

First Request Mitigation on All Sources

Use HTTPS Authentication on All Sources

☐

Keyless Mitigation

Rate-Limit Traffic from Suspect Sources Limit

100

Packed per Second per Source

☒

Selective Full Inspection

Perform Full-Session Decryption and Inspection by Full-Session Mitigations on Attacked PSSLOs

Authentication Methods

HTTP Authentication Method

302-Redirect

▼

☐

Out-of-State Protection

Cancel

Submit

## APPENDIX 2 - TRAFFIC FILTERS (ADDITIONAL INFO)

### Protection Overview

A traffic filter is a filter rule-based mitigation mechanism, which lets you mitigate an attack by a particular property, similar to an advanced ACL.

Moreover, Traffic filter can be used for mitigation of HTTP brute force, and SIP flood attacks.

To mitigate an attack, there are some filtering parameters that can be applied, such as:

- Source and destination network
- Packet size
- Source and destination ports
- TCP flags, and more
- Regex

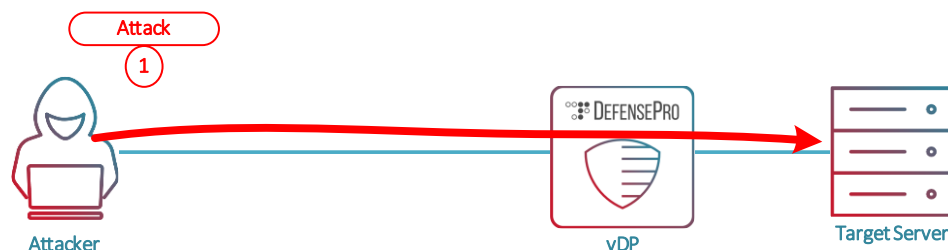
Traffic filter mitigation is performed by using a rate limit for the attacker traffic (in PPS, by default)

Some of the advantages of this protection are:

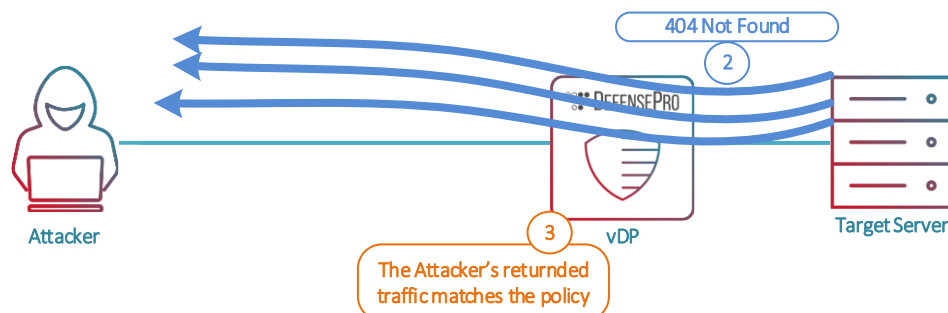
- Manual, more granular control
- Flexibility to meet unique needs

## Scenario Steps Overview

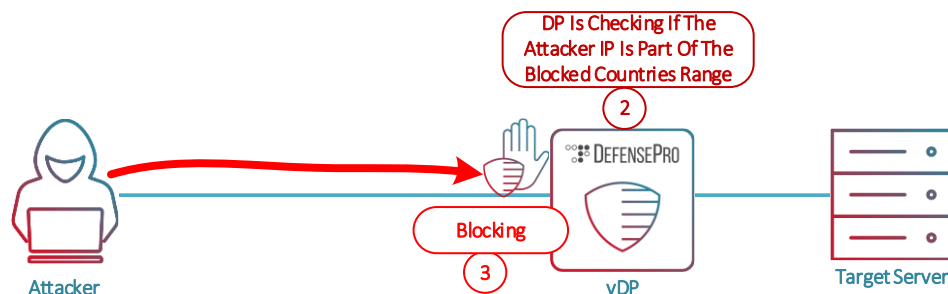
1. The attacker starts with an HTTP page scanning attack toward the Webserver.



2. The Webserver responds with **404 page not found**.
3. The attacker's return traffic matches the configured traffic-filter profile (matches all returning traffic which includes a 404 error code):



4. The attacker's IP address is added to the suspend – table and is blocked:





## Configurations

Cyber Controller

Security Settings

Policies Security Templates

Import Configuration Export Configuration

Status	Name	Description	Device	Template Origin	Update Time	
enabled	VDP_Demo_Lab_Advanced		DefensePro X	Custom	06/19/2023 09:13	
enabled	VDP_Demo_Lab		DefensePro X	Custom	06/19/2023 08:05	

Edit Policy

General and Networks

☒ Enable

Policy Name \* VDP\_Demo\_Lab

Device \* DefensePro X

Description

Type Here

Network Table + Add New

Classification *	Type *	Network Address *	Prefix *	
Destination	IPv4	155.1.102.0	27	

Security Policy

Priority \* 5

Copy from Template \* custom-10.0.0.0

Protection Sections

Expand All Collapse All



☒ Traffic Filters

Action

Block and Report

Traffic Filters List

[+ Add New](#)

Filter Name	Traffic Filter	Protocol	Other Protocols	Source Port	
TF_Profile	Matching Traffic	TCP		Any	 

Cancel

Submit

## Edit Traffic Filters List



### Filter Threshold

Filter Name \*

TF\_Profile

Apply Traffic Filter To

Matching Traffic

### Basic Filter

Source Network

As in Policy

Destination Network

As in Policy

Protocol

TCP

Other Protocol Number(s)

Type Here

Source Port

Any

Destination Port

http

Packet Size (Bytes)

Type Here

### Advanced Filter

- ☐ TCP Flags - SYN
 ☐ TCP Flags - ACK
 ☐ TCP Flags - RST
 ☐ TCP Flags - SYN+ACK
 ☐ TCP Flags - FIN+ACK
   
☐ TCP Flags - PSH+ACK

Time To Live(TTL)

Type Here

TCP Sequence Number

Type Here

Context Tag

Any

Type of Service (ToS) - DSCP

Type Here

Fragment Offset

Fragment ID

Regular Expression

Cancel

Submit

Add Traffic Filters List
×

Packet Size (Bytes)

**Advanced Filter**  
☐ TCP Flags - SYN   
☐ TCP Flags - ACK   
☐ TCP Flags - RST   
☐ TCP Flags - SYN+ACK   
☐ TCP Flags - FIN+ACK  
☐ TCP Flags - PSH+ACK

Time To Live(TTL)   
TCP Sequence Number   
Context Tag

Type of Service (ToS) - DSCP   
Fragment Offset   
Fragment ID

Regular Expression

**Filter Action**  
Threshold Units   
Threshold \*   
Tracking Mode

IPv4 Source Prefix Length   
IPv6 Source Prefix Length   
IPv4 Destination Prefix Length   
IPv6 Destination Prefix Length

☒ Packet Reporting

Cancel

## APPENDIX 3 - ERT ACTIVE ATTACKER FEED PROTECTION (ADDITIONAL INFO)

### Protection Overview

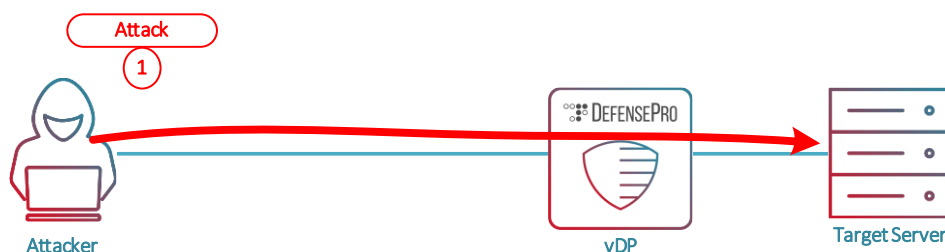
The ERT Attacker feed provides protection against well-known attackers' IP addresses that were recently actively involved in a DDoS attack.

The feed update process can be scheduled by the user per week/day.

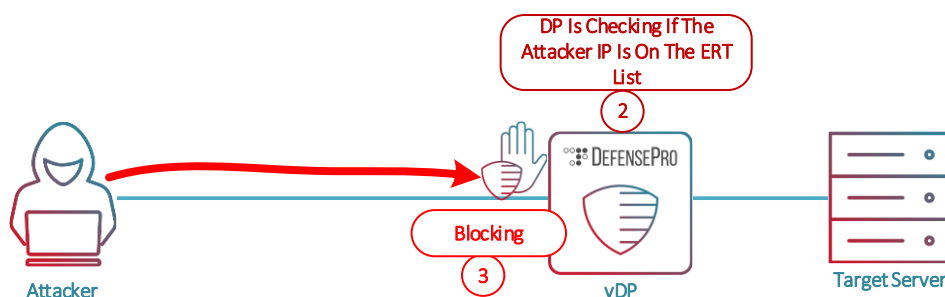
The ERT Active Attackers Feed focuses on unique, real-time intelligence against emerging DDoS-specific threats including evolving IoT botnets and new DNS attack vectors.

### Scenario Steps Overview

1. An attacker with a malicious IP address (located on the ERT list) begins a UDP flood attack towards the Webserver.



2. DefensePro checks if the IP address of the attacker is contained in the ERT file and mitigates the attack immediately.
3. The IP address of the attacker is blocked immediately by DefensePro.



## Configuration

Cyber Controller





Security Settings

Policies Security Templates

Import Configuration Export Configuration

Policies 2 + Add Policy

Search

<input type="checkbox"/>	Status	Name	Description	Device	Template Origin	Update Time	
<input type="checkbox"/>	enabled	VDP_Demo_Lab_Advanced		DefensePro X	Custom	06/19/2023 09:13	 
<input type="checkbox"/>	enabled	VDP_Demo_Lab		DefensePro X	Custom	06/19/2023 08:09	 

### Edit Policy

#### General and Networks

☒ Enable


Policy Name \*

Device \*

Description

#### Network Table

+ Add New

Classification *	Type *	Network Address *	Prefix *	
Destination	IPv4	155.1.102.0	27	

#### Security Policy

Priority \*

Copy from Template \*

#### Protection Sections

Expand All Collapse All

☒ EAAF

ERT Active Attackers Core

High	Medium	Low
Block and Report	Block and Report	No Action

TOR Exit Nodes

High	Medium	Low
Block and Report	Block and Report	Report Only

Web Attackers

High	Medium	Low
Block and Report	Block and Report	No Action

### Examples from the ERT file:

```

80.82.77.33; high; [ERT Active Attackers, Web Attackers]
89.248.167.131; high; [ERT Active Attackers, Web Attackers]
93.174.95.106; high; [ERT Active Attackers, Web Attackers]
77.247.108.119; high; [ERT Active Attackers, Web Attackers]
80.82.77.139; high; [ERT Active Attackers]
122.228.19.79; high; [ERT Active Attackers]
66.249.88.3; high; [Web Attackers]
66.249.88.46; high; [Web Attackers]

185.220.101.0; medium; [Tor Exit Nodes]
185.220.101.1; medium; [Tor Exit Nodes]
185.220.101.21; medium; [Tor Exit Nodes]
    
```

**Note:** The ERT file can be exported from DefensePro X, located at:  
/mnt/applData/EaafFeed/EaafFeed-imp



## APPENDIX 4 - SPOOFED SYN ATTACK PROTECTION (ADDITIONAL INFO)

### Protection Overview

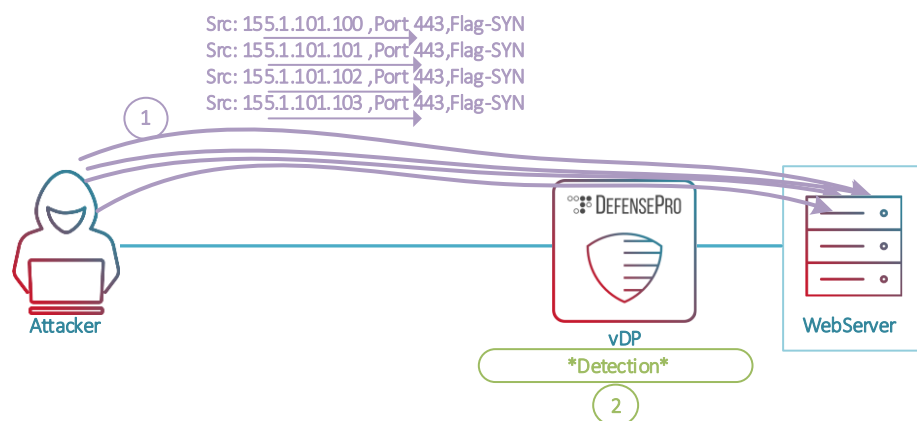
Spoofed SYN Attack protection is a new feature which allows mitigation of spoofed syn attacks targeting a wide range of IP's from the customer network.

With this new feature, syn protection can track the number of syn packet for the whole protected subnet together and not only for a specific server.

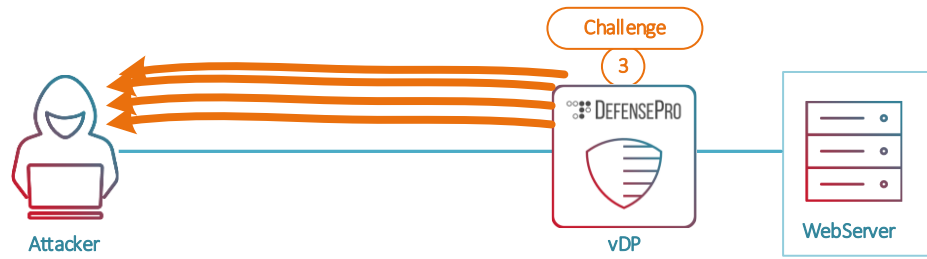
By using this kind of tracking technique, attacks like carpet bomb and others can be mitigated easily by DefensePro X.

### Scenario Steps Overview

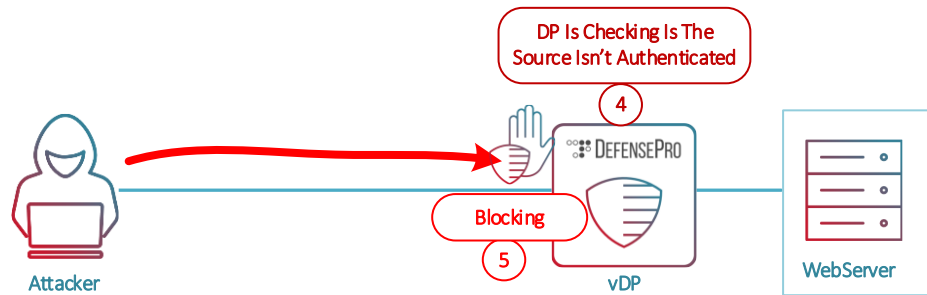
1. The attacker generates SYN flood attack using hping3 tool from different sources towards a web server.
2. Detection on DefensePro begins:



3. If the number of syn packets rate goes above the configured threshold. The DefensePro will begin challenging every source.

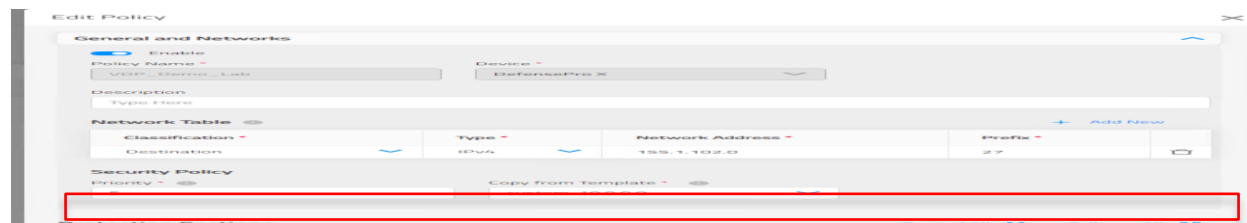
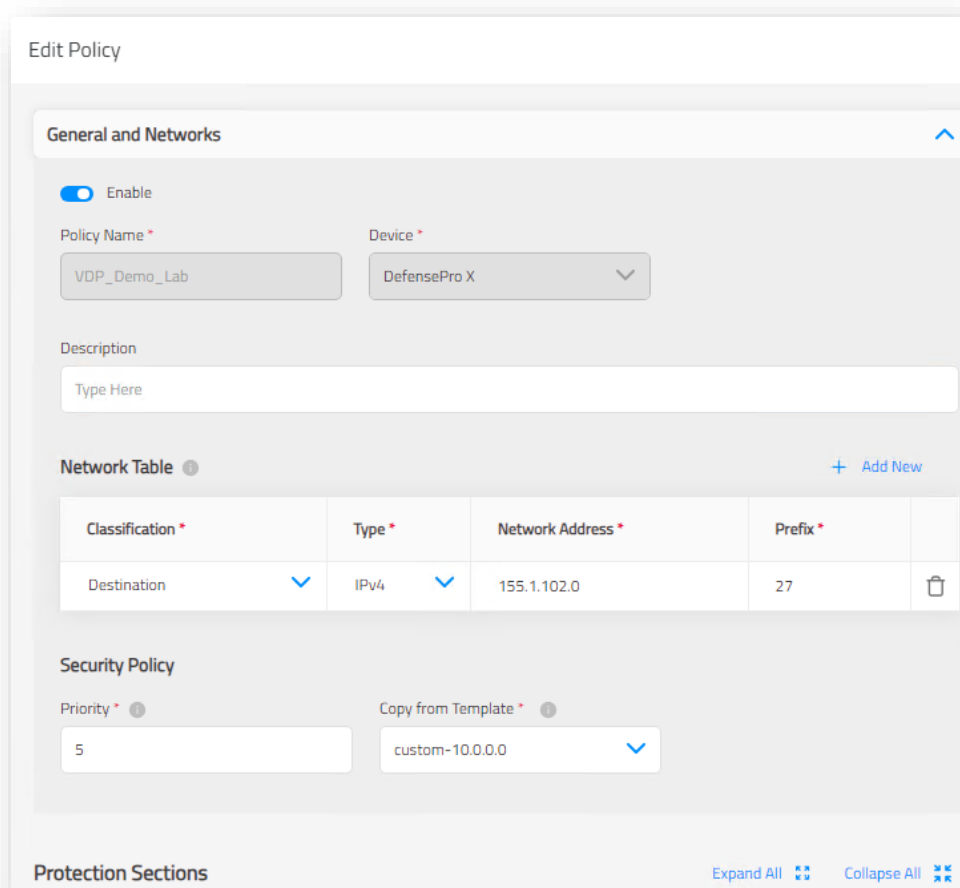


4. Every traffic from sources which didn't pass the challenge will be blocked by DefensePro X.



## Configurations

With the configuration given below, while under attack, if the number of the total syn packets per second get above 50, DefensePro X starts challenge every source:

SYN Flood Protection

Action

Block and Report

Protection Table

+ Add New

Use	Protection Name	Application Port Group	Activation Threshold	Termination Threshold	Risk	
<input checked="" type="checkbox"/>	HTTPS-SYN	https	50	20	Medium	

Advanced Settings

Advanced Settings - SYN Flood Protection

Tracking Method

Action

Spoofed SYN Attack Protectio...

Spoofed SYN Attack Protection

Destination Ports

Traffic Matching Destination ...

Activation Mode

Threshold Based

Activation Threshold

50

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

Cancel

Submit

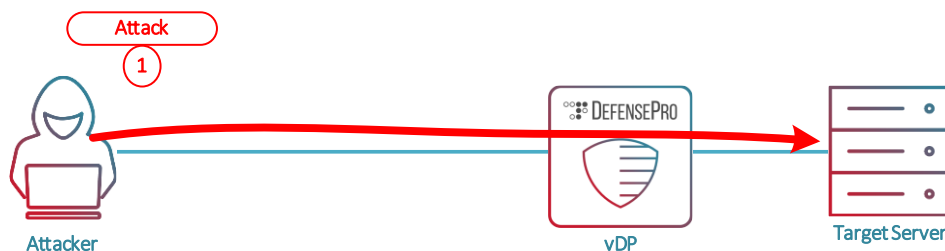
## APPENDIX 5 - BDOS PROTECTION (ADDITIONAL INFO)

### Protection Overview

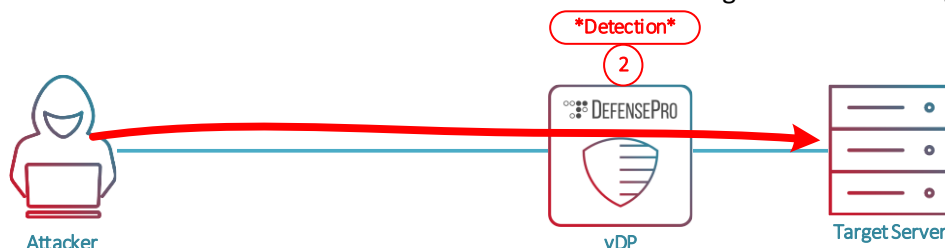
The BDoS module provides a behavior-based DoS protection that meets the detection and prevention challenge raised by the most sophisticated DDoS attack methods. Through an adaptive behavioral approach, based on analysis methods such as an adaptive Fuzzy Logic decision engine, probability theory and Closed-Feedback mechanism, the system provides a natural dynamic DoS protection system that is able to answer current and future needs. This system auto-mitigates DoS and DDoS flood attacks, and no human intervention is needed.

### Scenario Steps Overview

1. The Attacker begins a UDP flood attack towards the web server and changes the vector of the attack after 100 seconds.

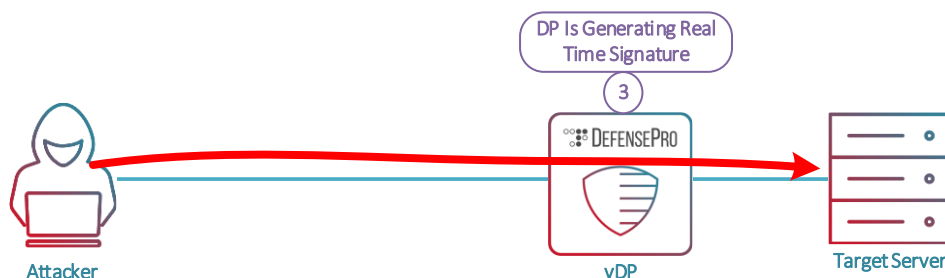


2. DefensePro checks if the UDP rate is above the attack edge baseline and begins the detection phase.

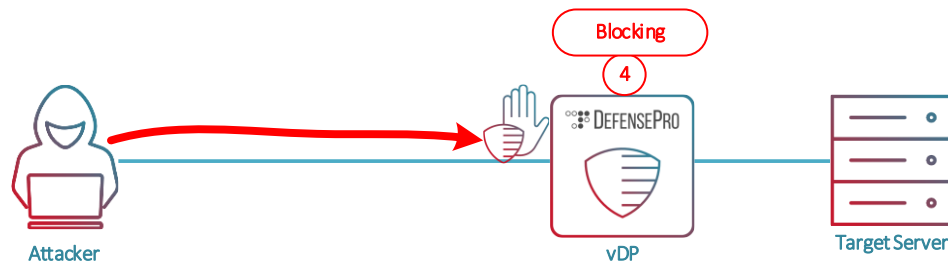


3. DefensePro generates a real time signature which will be used to mitigate the UDP Flood.

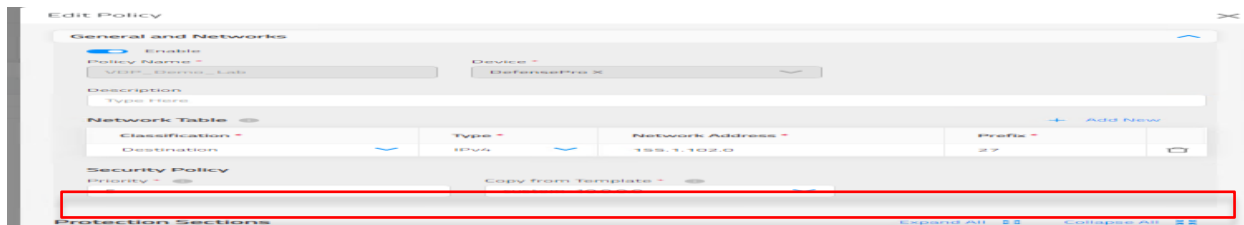
When the attack vector changes, DefensePro generates a new signature.



4. The UDP Flood is being blocked by DefensePro.



## Configurations



**Edit Policy**

**General and Networks**

☒ Enable

Policy Name \*

Device \*

Description  
Type Here

**Network Table** + Add New

Classification *	Type *	Network Address *	Prefix *
Destination	IPv4	155.1.102.0	27

**Security Policy**

Priority \*

Copy from Template \*

**Protection Sections** Expand All Collapse All



BDoS Protection

Action

Block and Report

Footprint Strictness

Medium

Bandwidth Settings

Inbound Traffic (Kbps) \*

10000

Outbound Traffic (Kbps) \*

10000

Advanced Settings

Advanced Settings - BDoS Protection

General

Transparent Optimization

Disabled

Packet Reporting

☒

Flood Protection Settings

☐ SYN Flood
 ☐ TCP ACK + FIN Flood
 ☐ TCP RST Flood
 ☒ TCP SYN + ACK Flood
 ☒ TCP Fragmentation Flood

☒ UDP Flood
 ☐ UDP Fragmentation Flood
 ☒ ICMP Flood
 ☒ IGMP Flood

Baseline Related

Inbound (%)

TCP \*

75

UDP \*

50

Fragmented UDP \*

25

ICMP \*

9

IGMP \*

9

Outbound (%)

TCP \*

75

UDP \*

50

Fragmented UDP \*

25

ICMP \*

9

IGMP \*

9

UDP Settings

UDP Packet Rate Detection Sensitivity

Low

UDP Excluded Ports

None

Advanced UDP Detection

Disabled

Learning Period

One Day

Attack Edges Overrides - High Edge (%)

0

Attack Edges Overrides - Low Edge (%)

0

Burst-Attack Protection

Enable Burst-Attack Protection

Maximum Interval Between Bursts \*

Cancel

Submit

Advanced Settings - BDoS Protection
×

**Outbound (%)**

TCP \*

UDP \*

Fragmented UDP \*

ICMP \*

IGMP \*

75

50

25

9

9

**UDP Settings**

UDP Packet Rate Detection Sensitivity

UDP Excluded Ports

Advanced UDP Detection

Low

None

Disabled

Learning Period

Attack Edges Overrides - High Edge (%)

Attack Edges Overrides - Low Edge (%)

One Day

0

0

**Burst-Attack Protection**

Enable Burst-Attack Protection

Maximum Interval Between Bursts \*

Enabled

30

**Overblocking Settings**

Overblocking Prevention

Overblocking Prevention Threshold (%)

Disabled

25

**Advanced**

Learning Suppression Threshold (%) \*

BDoS Rate Limit

0

Limit To Suspect Edge

User-Defined Rate Limit

Rate Limit Units

0

Kbps

Cancel
Submit

## APPENDIX 6 - BDoS ADVANCED UDP PROTECTION (ADDITIONAL INFO)

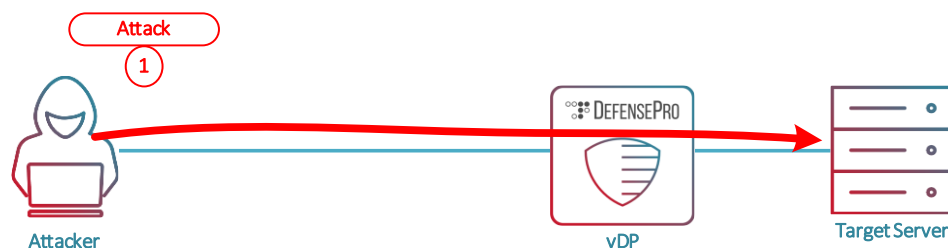
### Protection Overview

The UDP Settings help the BDoS module detect UDP-flood DoS attacks, ensure good mitigation of such attacks, limit false positives, and reduce leakage of attack traffic.

The Advanced UDP Detection engine relies on rate and rate-invariant traffic statistics — including UDP bandwidth, packet rate, and connection rate — to ensure accurate detection of UDP floods. This engine can detect different types of UDP floods, based on high packet rate (PPS) or high connection rate (CPS).

### Scenario Steps Overview

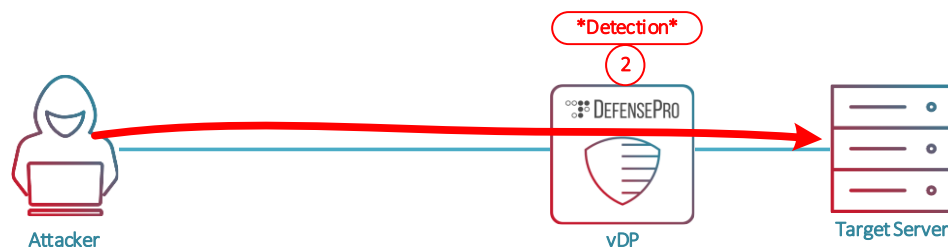
1. The Attacker begins a UDP flood attack towards the web server.



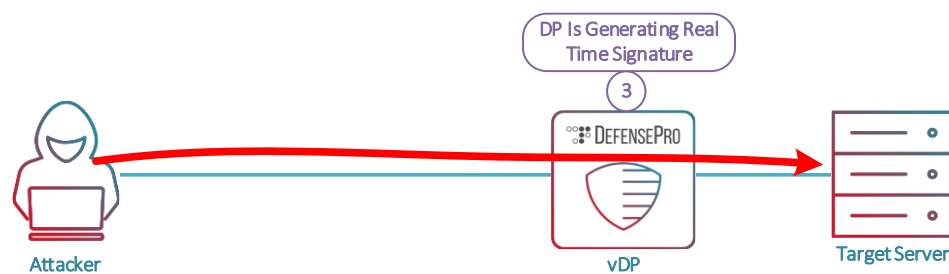
2. DefensePro checks if the UDP rate is above the Attack-Edge baseline:

If the rate-invariant remains the same (the ratio between cps and pps) means it is a “Flash-Crowd” event and no detection will occur.

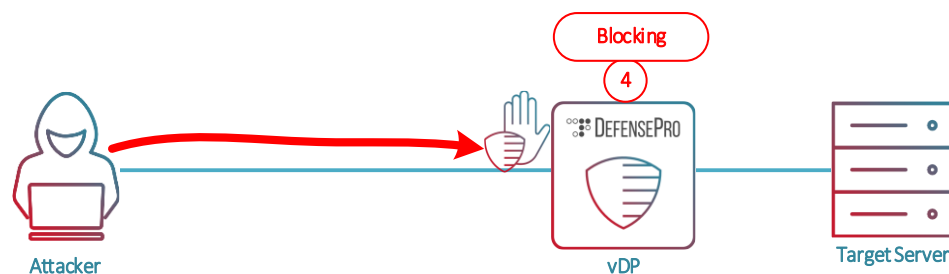
If the rate-invariant changes, DefensePro begins the Detection phase.



3. DefensePro generates a real time signature which will be used in order to mitigate the UDP Flood.



4. The UDP Flood is being blocked by DefensePro.







## Configurations

Cyber Controller

Security Settings

Policies Security Templates

Import Configuration Export Configuration

Status	Name	Description	Device	Template Origin	Update Time	
enabled	VDP_Demo_Lab_Advanced		DefensePro X	Custom	06/19/2023 09:13	 
enabled	VDP_Demo_Lab		DefensePro X	Custom	06/19/2023 08:09	 

Edit Policy

General and Networks


☒ Enable


Policy Name \* VDP\_Demo\_Lab\_Advanced

Device \* DefensePro X

Description

Type Here

Network Table  [+ Add New](#)



Classification *	Type *	Network Address *	Prefix *	
Destination	IPv4	155.1.102.100	32	



Security Policy


Priority \* 10


Copy from Template \* custom-10.0.0.0

Protection Sections

Expand All  Collapse All 

General Parameters  

☐ Anti-Scan 

☒ BDoS Protection 

Cancel Submit

BDoS Protection

Action

Block and Report

Footprint Strictness

Medium

Bandwidth Settings

Inbound Traffic (Kbps) \*

40000

Outbound Traffic (Kbps) \*

40000

Advanced Settings

Advanced Settings - BDoS Protection

General

Transparent Optimization

Disabled

☒ Packet Reporting

Flood Protection Settings

☐ SYN Flood
 ☐ TCP ACK + FIN Flood
 ☐ TCP RST Flood
 ☐ TCP SYN + ACK Flood
 ☐ TCP Fragmentation Flood
 ☒ UDP Flood
 ☐ UDP Fragmentation Flood
 ☐ ICMP Flood
 ☐ IGMP Flood

Baseline Related

Inbound (%)

TCP *	UDP *	Fragmented UDP *	ICMP *	IGMP *
75	80	25	3	3

Outbound (%)

TCP *	UDP *	Fragmented UDP *	ICMP *	IGMP *
75	80	25	3	3

UDP Settings

UDP Packet Rate Detection Sensitivity

Medium

UDP Excluded Ports

None

Advanced UDP Detection

Enabled

Learning Period

Six Hrs

Attack Edges Overrides - High Edge (%)

0

Attack Edges Overrides - Low Edge (%)

0

Burst-Attack Protection

Enable Burst-Attack Protection

Maximum Interval Between Bursts

Cancel

Submit

Advanced Settings - BDoS Protection

Outbound (%)

TCP \*

75

UDP \*

80

Fragmented UDP \*

25

ICMP \*

3

IGMP \*

3

UDP Settings

UDP Packet Rate Detection Sensitivity

Medium

UDP Excluded Ports

None

Advanced UDP Detection

Enabled

Learning Period

Six Hrs

Attack Edges Overrides - High Edge (%)

0

Attack Edges Overrides - Low Edge (%)

0

Burst-Attack Protection

Enable Burst-Attack Protection

Disabled

Maximum Interval Between Bursts

30

Overblocking Settings

Overblocking Prevention

Disabled

Overblocking Prevention Threshold (%)

25

Advanced

Learning Suppression Threshold (%) \*

0

BDoS Rate Limit

Disable

User-Defined Rate Limit

0

Rate Limit Units

Kbps

Cancel

Submit



## APPENDIX 7 - DNS FLOOD PROTECTION (ADDITIONAL INFO)

### Protection Overview

The DNS Flood module provides protection against DNS Flood attacks.

DNS module can be configured in two modes, Behavioral or Manual.

When using the behavioral mode, DefensePro X learns the legitimate traffic in peacetime and builds baseline for each DNS query (A, AAA, PTR, NS, etc.)

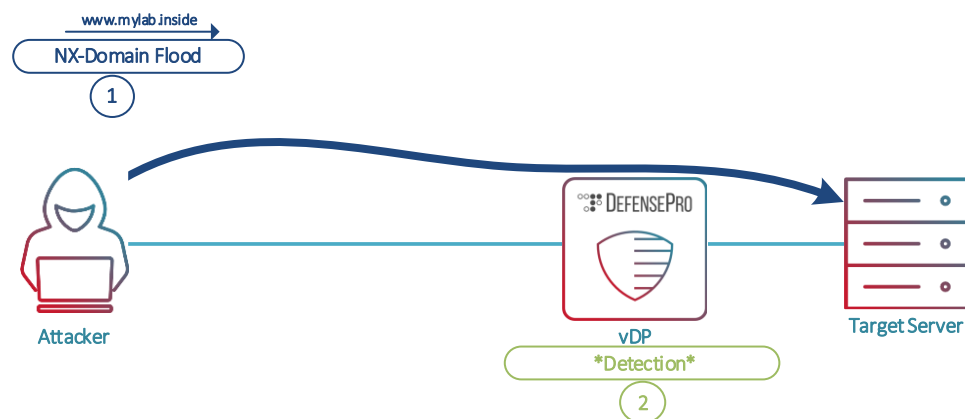
When under attack, DefensePro X will generate a Real-Time signature that matches the attack traffic pattern and use it to mitigate the attack while allows the legitimate queries to pass in.

In Manual mode, the user can specify explicit quires thresholds.

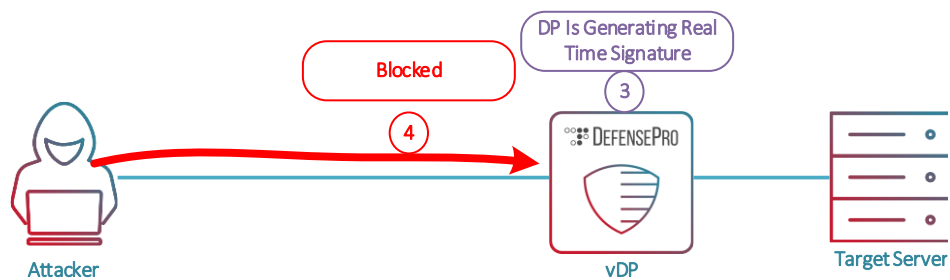
DNS protection can mitigate DNS sub-domain flood attacks while allowing only legitimate queries to pass.

### Scenario Steps Overview

1. The attacker begins a DNS NX-Domain flood attack towards the DNS server.

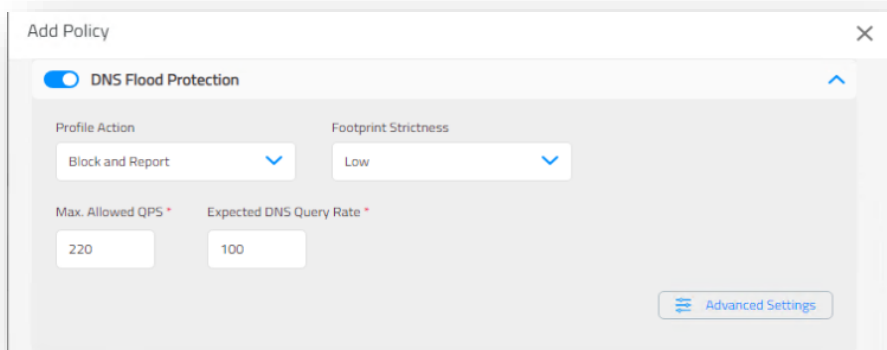


2. DefensePro X checks if the DNS queries rate is above the attack edge baseline.
3. DefensePro X generates a real time signature which will be used to mitigate the DNS NX domain flood attack.



## Configurations

DNS Flood profile configured as follows:



Advanced Settings - DNS Flood Protection
✕

### General

☒ Packet Reporting

### Flood Protection Settings

☒ A Query
☒ MX Query
☒ PTR Query
☒ AAAA Query
☒ Text Query
☒ SOA Query

☒ NAPTR Query
☒ SRV Query
☒ Other Queries

### Baseline Related

A Query *	MX Query *	PTR Query *	AAAA Query *	Text Query *
<input type="text" value="90"/>	<input type="text" value="45"/>	<input type="text" value="45"/>	<input type="text" value="15"/>	<input type="text" value="8"/>
SOA Query *	NAPTR Query *	SRV Query *	Other Queries *	
<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="2"/>	

### Other Rate Settings

Signature Rate-Limit Target \*

### Manual Triggers

Use Manual Triggers

Disabled
▼

### Advanced

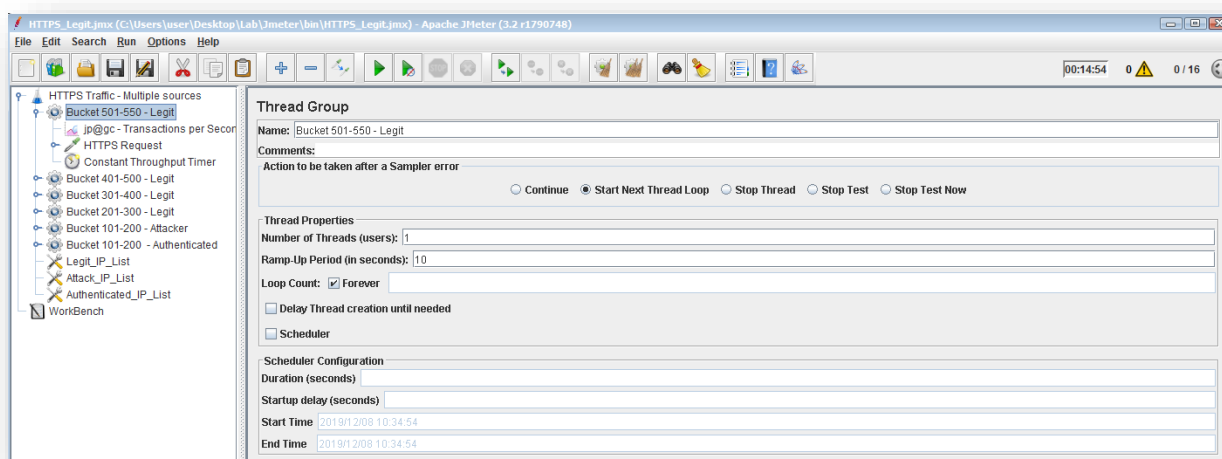
Learning Suppression Threshold \*

Cancel
Submit

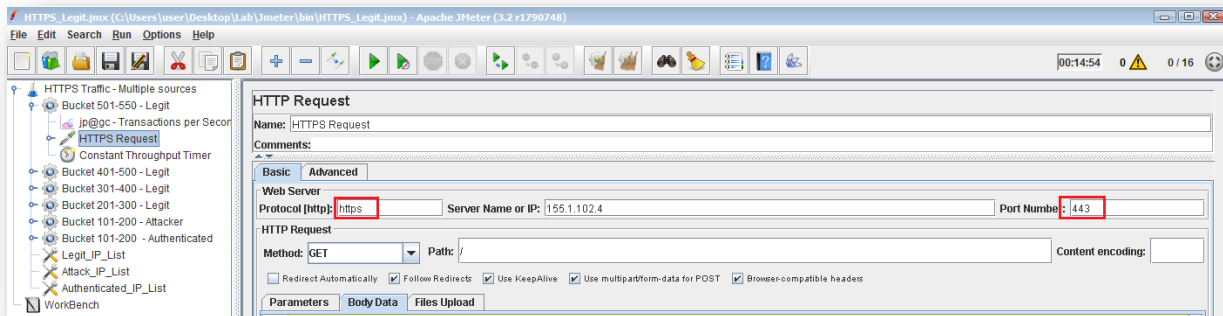
## APPENDIX 8 - HTTPS TRAFFIC GENERATION TEMPLATE (ADDITIONAL INFO)

The HTTPS traffic template configured as follows:

1. Bucket # – The HTTPS request to the specific bucket size:
  - **Number of Threads** – Control the number of simultaneous users for the test.
  - **Ramp-Up Period** – The time to start all users.
  - **Loop Count** – Select **Forever** for an endless loop, or **manual** configuration.

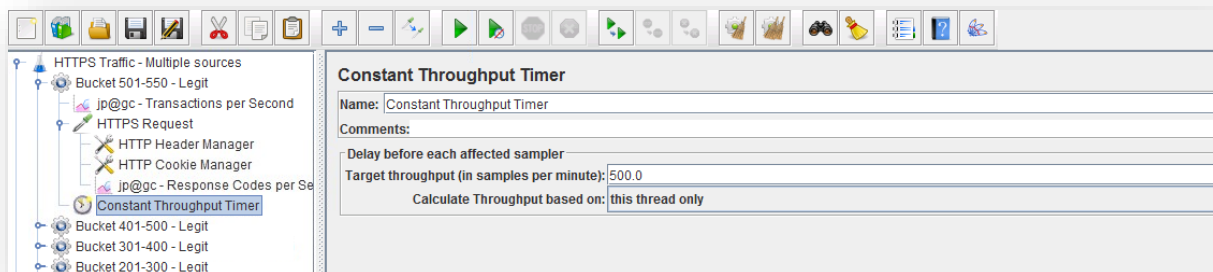


2. HTTP Request – The HTTPS header configuration:
  - **Server Name or IP** – The test destination.
  - **Port Number** – The test destination port
  - **Protocol** – Select HTTP or HTTPS. A blank value indicates HTTP.
  - **Path** – The request path.



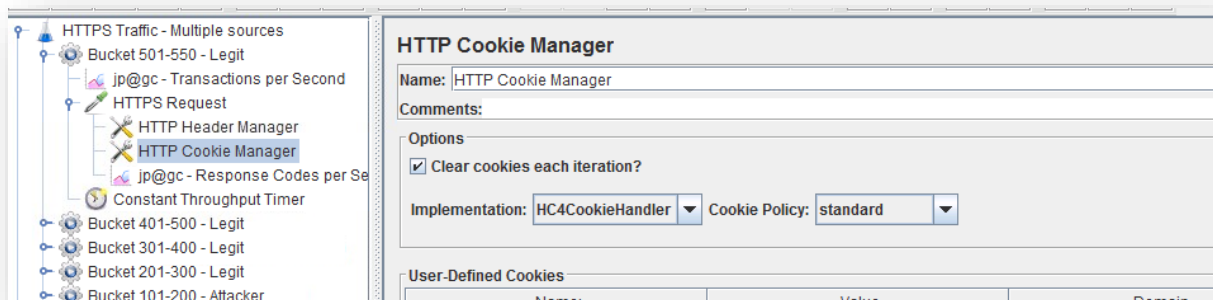
### 3. Set the Constant Throughput Timer:

- **Thread Delay** – Test delay.

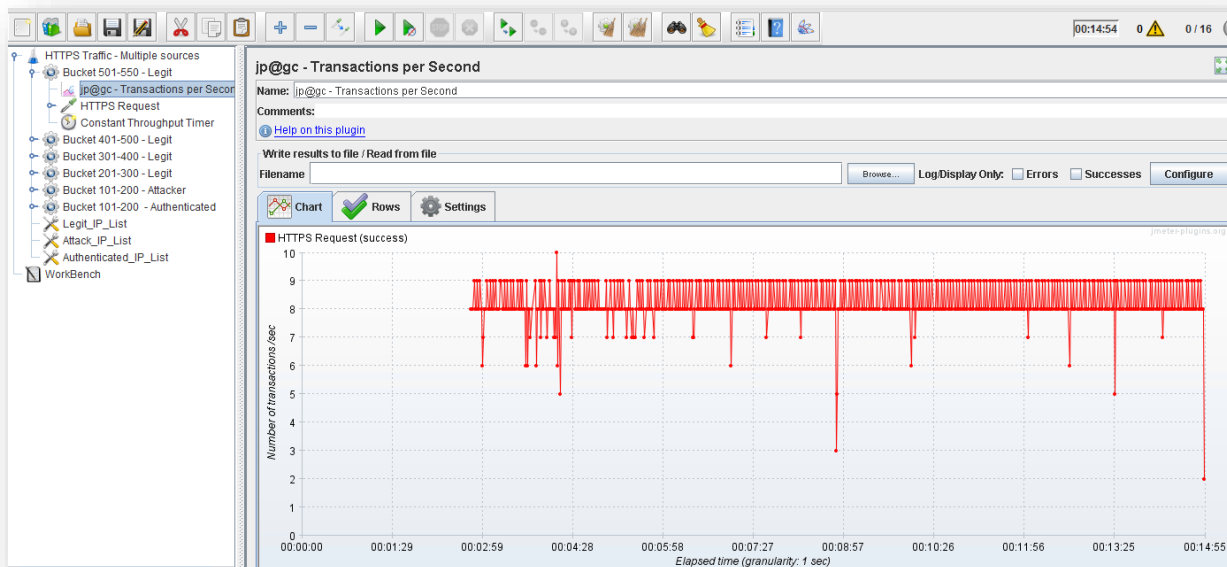


### 4. Set the HTTP Cookie Manager:

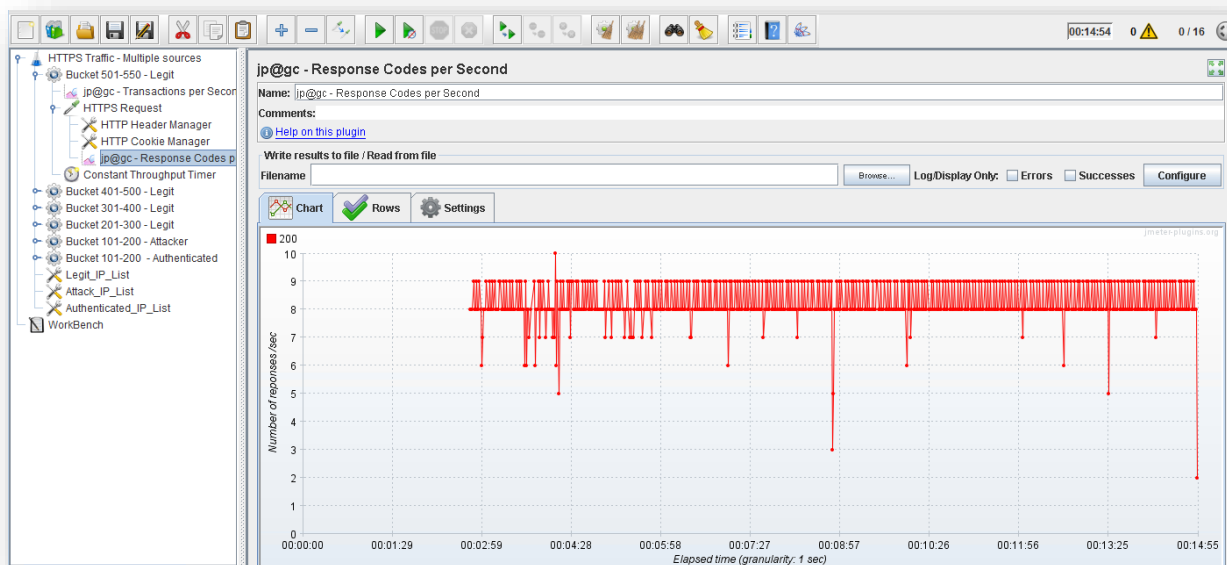
- Used for a 302-cookie challenge



5. Set the Transactions per Second:



6. Set the Response Codes per Second:

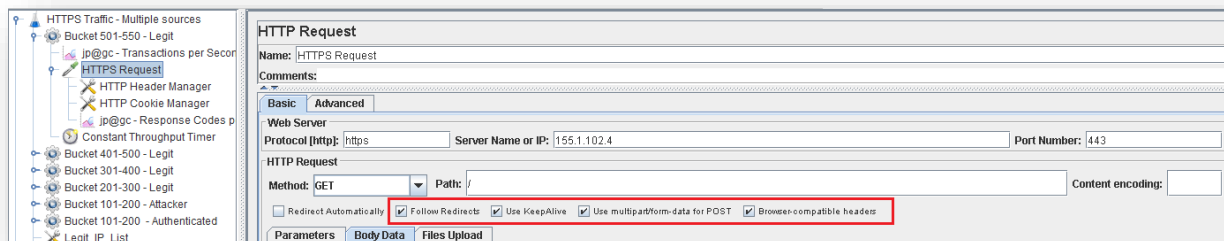


7. To clear statistics and graphs, click the **Brush** icon:

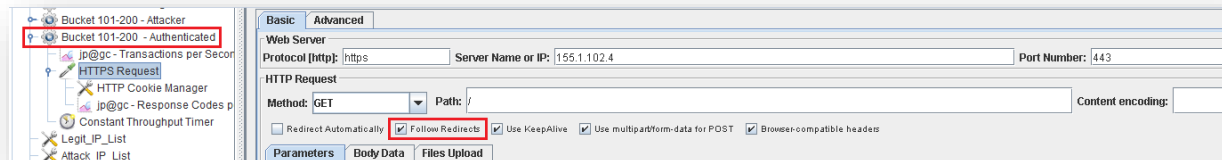


8. Buckets Type:

- Legit – Simulates traffic from legitimate users:



- Authenticated – Simulates traffic from legitimate users that passes the challenge:



9. Attacker – Simulate traffic from attacking users that do not pass the challenge: (**Follow redirect is disabled**):

