

DefensePro X v1.5.1

Demo Lab Guide

TABLE OF CONTENTS

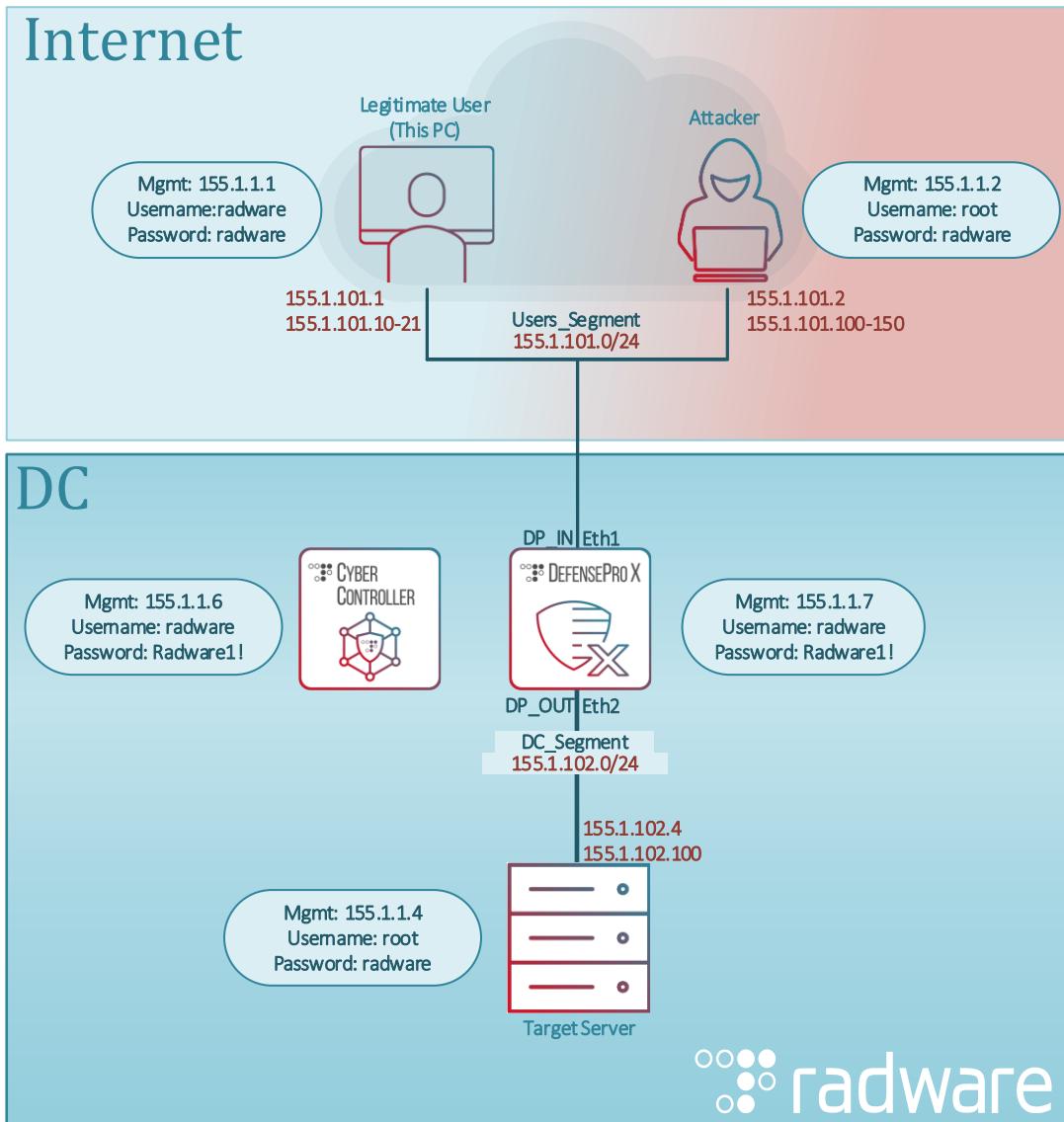
TABLE OF CONTENTS	2
LAB ENVIRONMENT	5
Topology Data Segment	5
Topology Management Segment	6
Lab Environment Credentials	6
Management (MGT) Station	7
Connecting the environment devices and running attacks	7
Legitimate Traffic Generation	8
Generating Traffic with JMeter	8
Verify legit traffic on the Cyber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

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

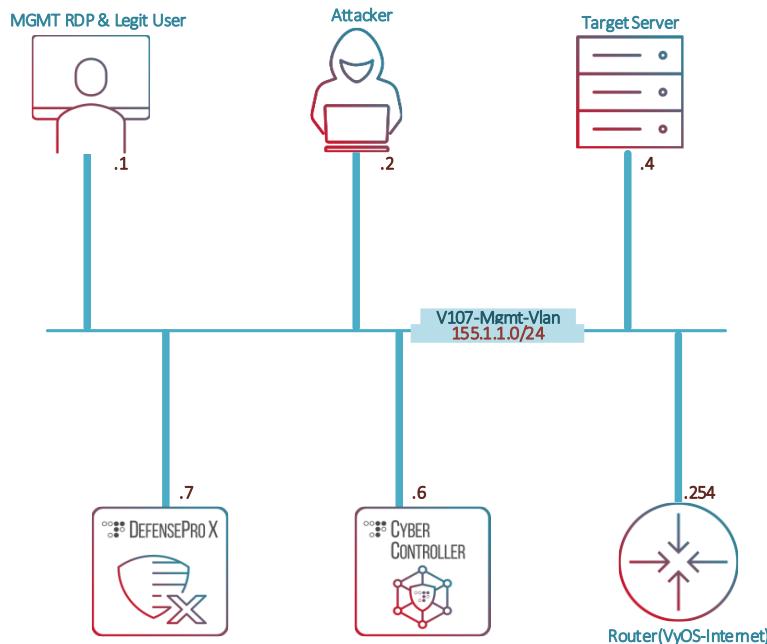
Configurations	73
APPENDIX 3 - ERT ACTIVE ATTACKER FEED PROTECTION (ADDITIONAL INFO).....	77
Protection Overview.....	77
Scenario Steps Overview	77
Configurations	78
APPENDIX 4 - SPOOFED SYN ATTACK PROTECTION (ADDITIONAL INFO)	80
Protection Overview.....	80
Scenario Steps Overview	80
Configurations	82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

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.

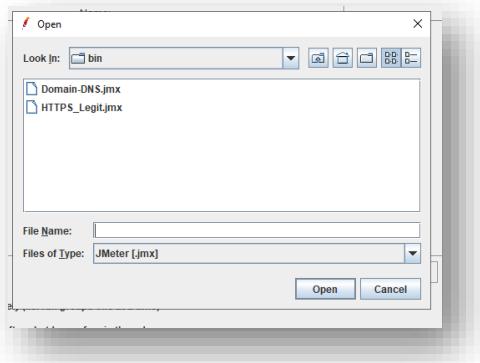
Generating Traffic with JMeter

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.

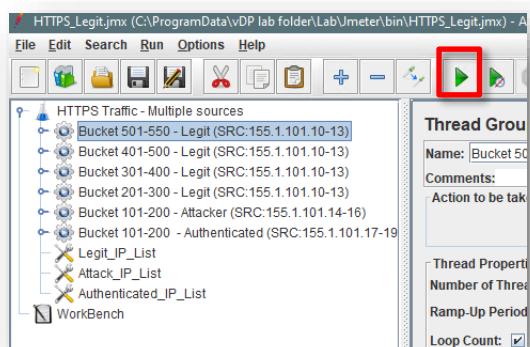
For more information regarding the buckets used in the HTTPS protection scenario [click here](#).

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**.



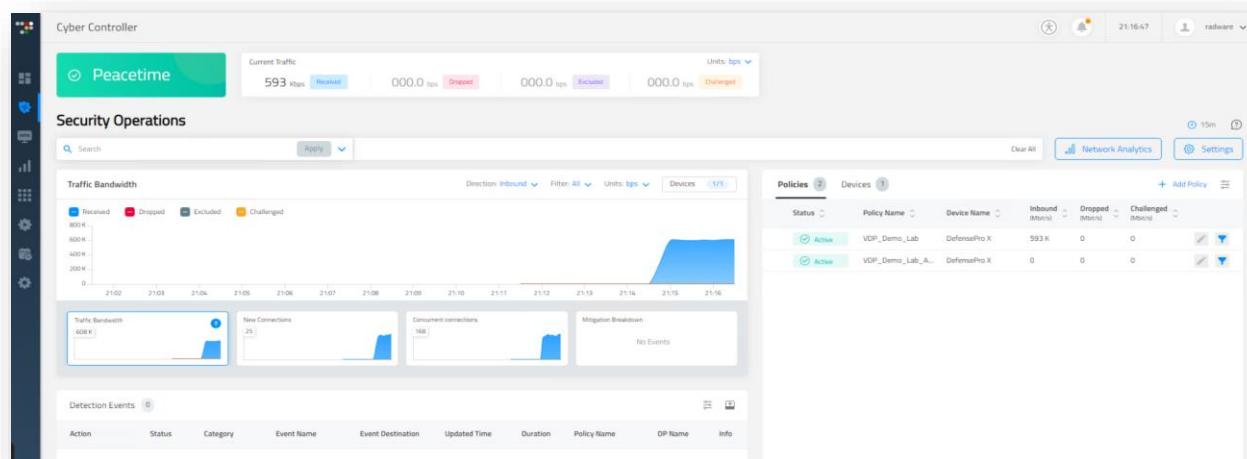
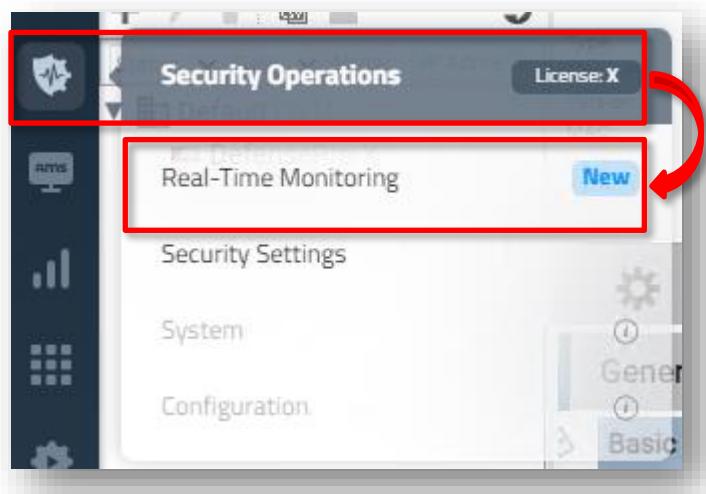
6. After the test runs, the number of running users displays at the upper right of the pane.
7. To stop the test traffic, click the red x button.

Note: some of the attacks includes specific legit traffic generation

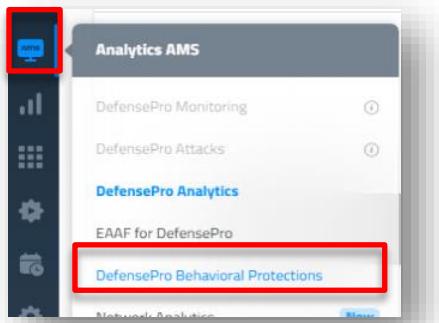
For the scenario of [DNS Flood Protection](#) and [BDoS Advanced UDP Protection](#), there is a different legit traffic, which is mentioned on the scenario section.

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**:



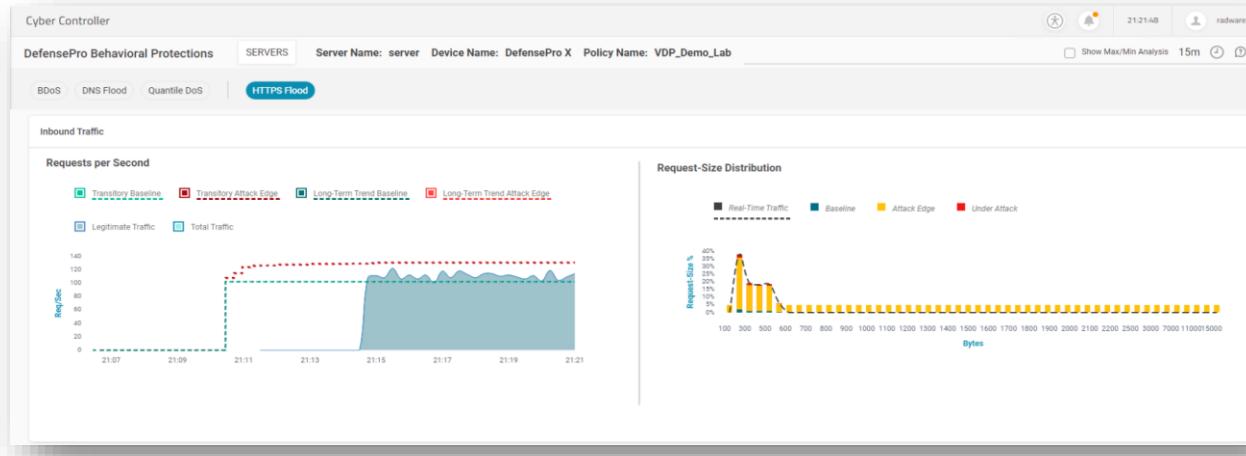
3. On the “DefensePro Behavioral Protections” page click on the “HTTPS Flood” button and then click on the “Server” button and choose “Change Scope”.



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



5. 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

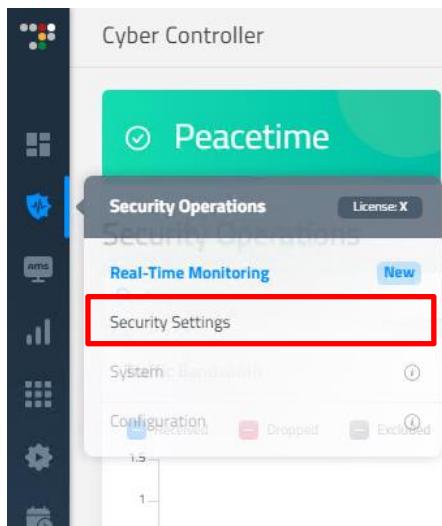
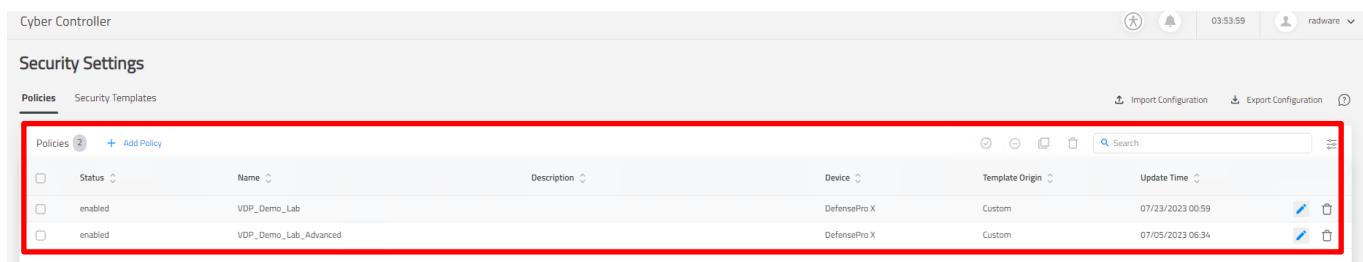
The following table provides a high-level overview of the DefensePro X demo lab configurations:

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">• BDoS (for the advanced UDP)
VDP_Demo_Lab	5	Protected Webserver (155.1.102.4/32)	<ul style="list-style-type: none">• HTTPS• Traffic Filter• TLS Fingerprint• ERT Attacker Feed• Spoofed Syn Flood• DNS Flood• BDoS

DefensePro X configurations include two major network protection.

To view the network protection configurations in Cyber Controller:

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

Policies	Status	Name	Description	Device	Template Origin	Update Time
<input type="checkbox"/>	enabled	VOP_Demo_Lab		DefensePro X	Custom	07/23/2023 00:59
<input type="checkbox"/>	enabled	VOP_Demo_Lab_Advanced		DefensePro X	Custom	07/05/2023 06:34

DEFENSEPRO X DEMO LAB SCENARIOS

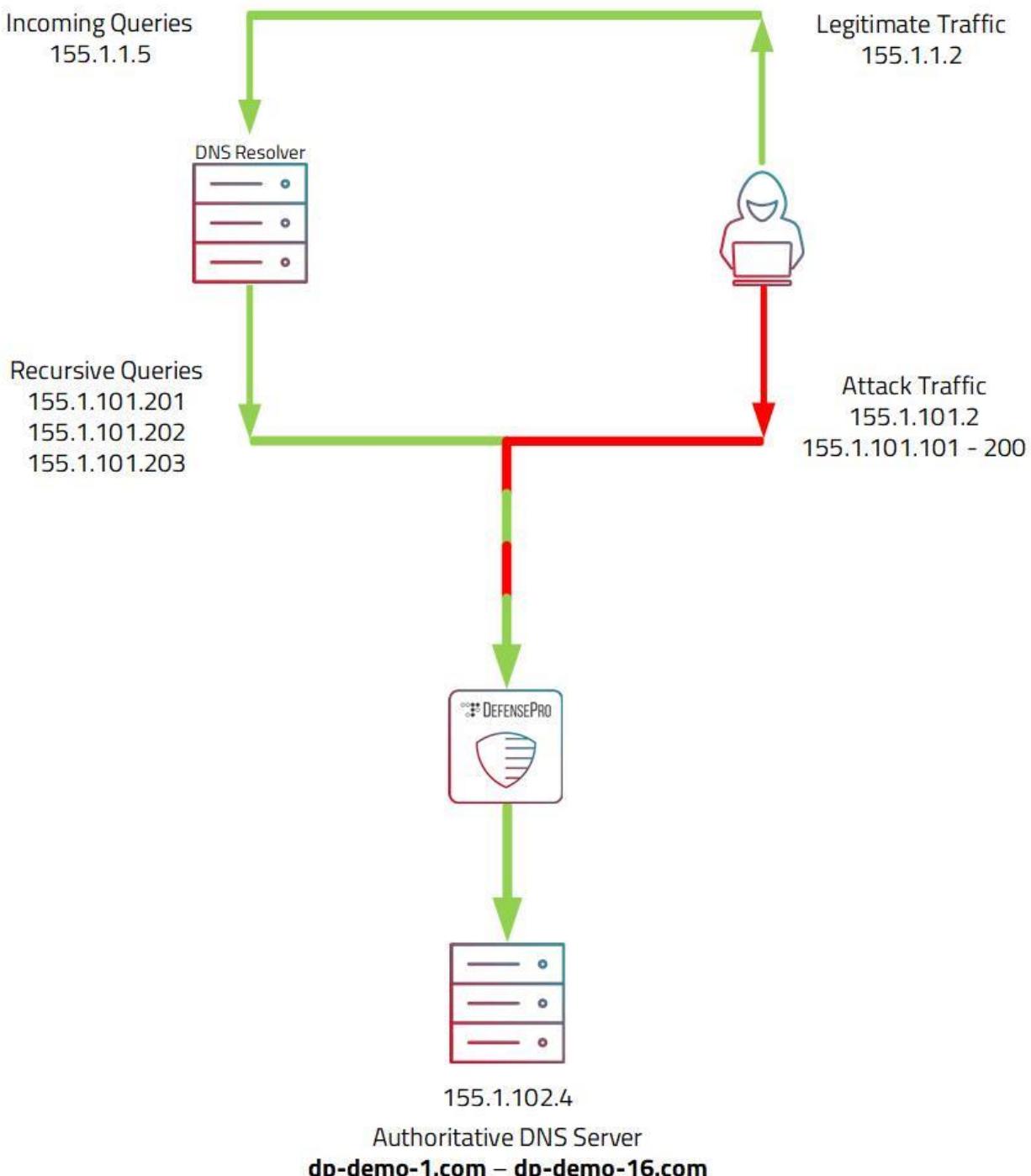
DNS Authoritative Protection

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



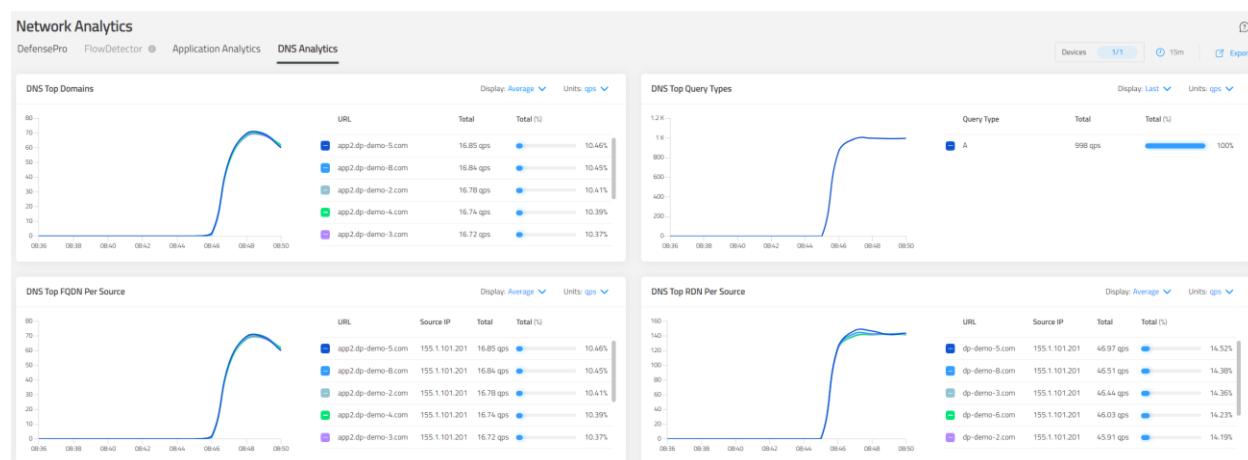
Running Legitimate Traffic

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.

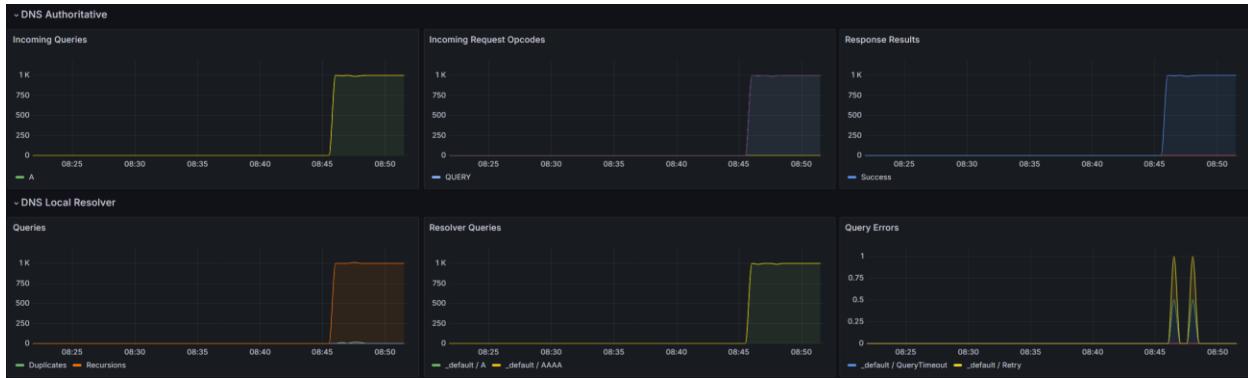
When observing the Real-Time Monitoring screen and the units are displayed in PPS (Packets per Second), we can observe that we are receiving 1000 Packets per Second, equivalent to our 1000 Queries per Second.



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.

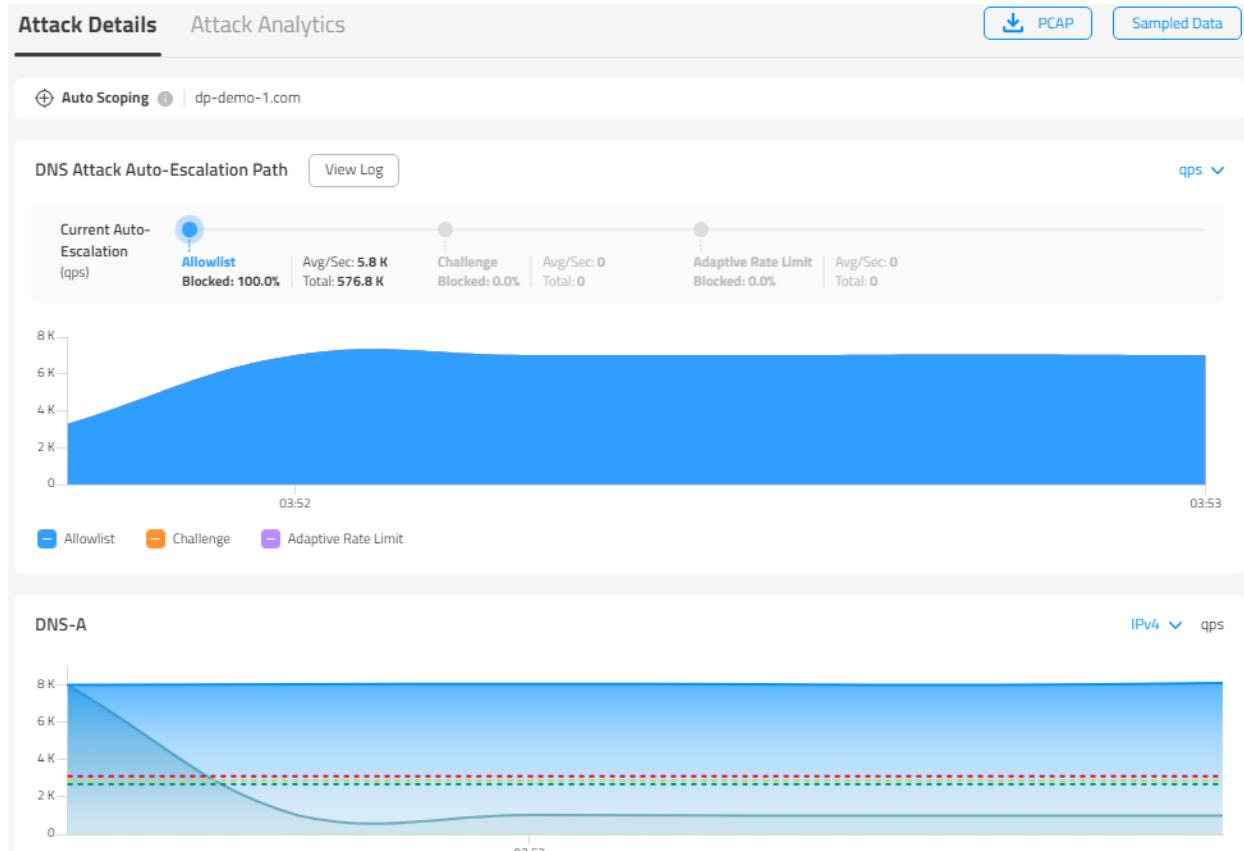
Once the attack is running, we will be able to see a DNS event detected, clicking on the magnifying glass will take us to the attack details.

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	

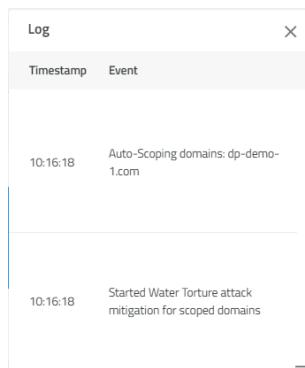
In the attack details we can see multiple items from top to bottom:

- 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.

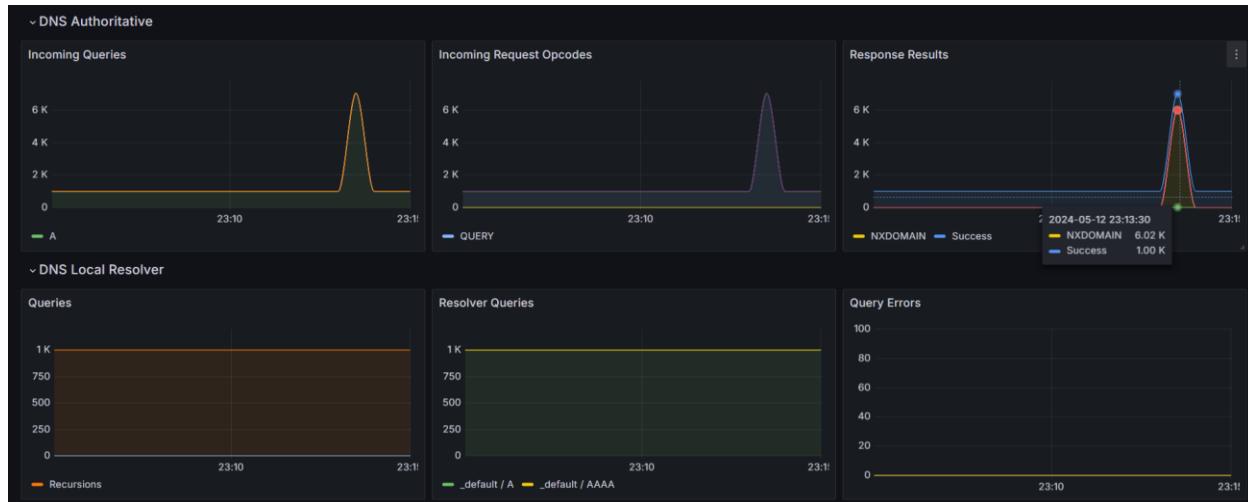
- DNS-A Graph – showing A query mitigation along with the legit traffic not impacted, which maintains its rate of 1000 QPS.



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.



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.



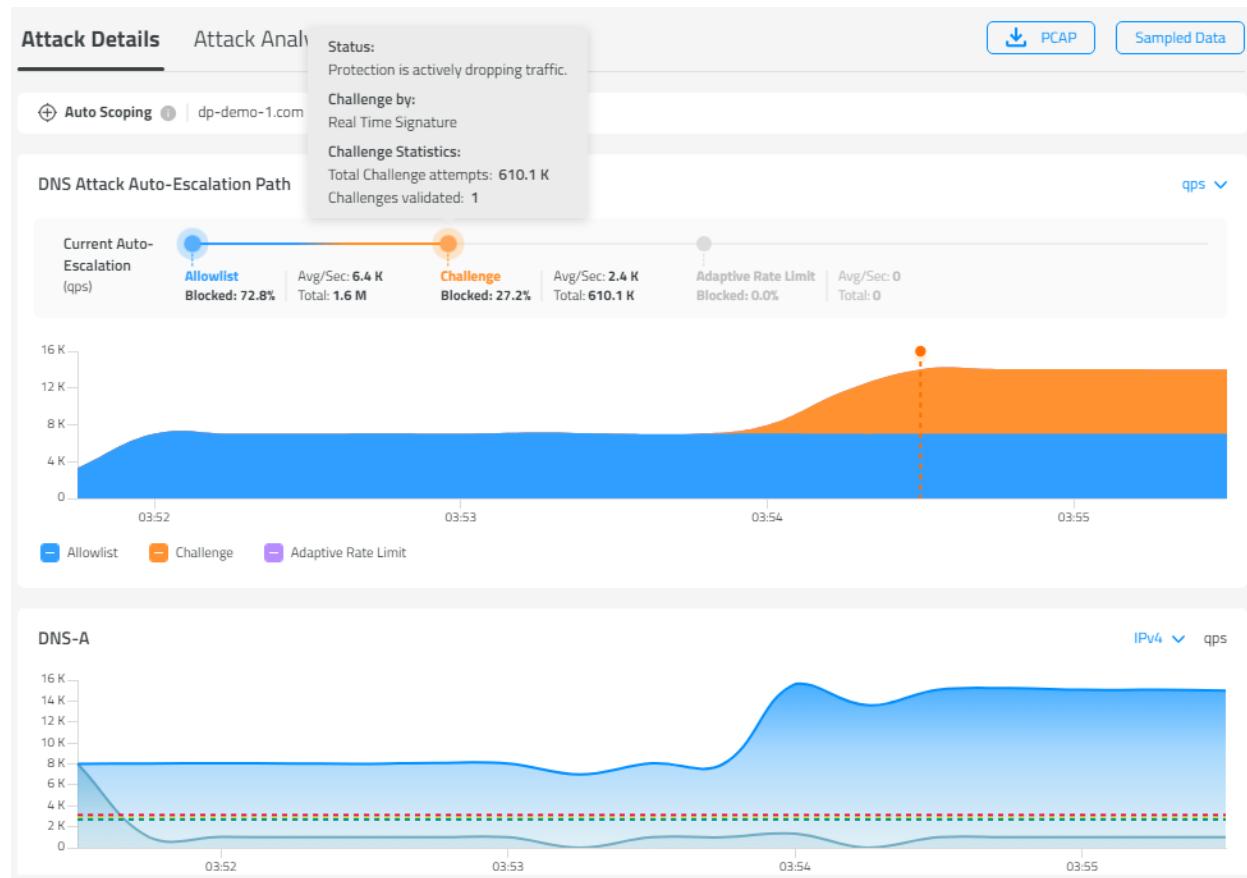
2. Dictionary Attack

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						
DNS Query -	DNS An Query Count -	TTL 64	DNS ID -			
DNS Query Count -	L4 Checksum -	State Blocking	Mitigation Action Signature Challenge			
Real-Time Signature						
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		X
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	

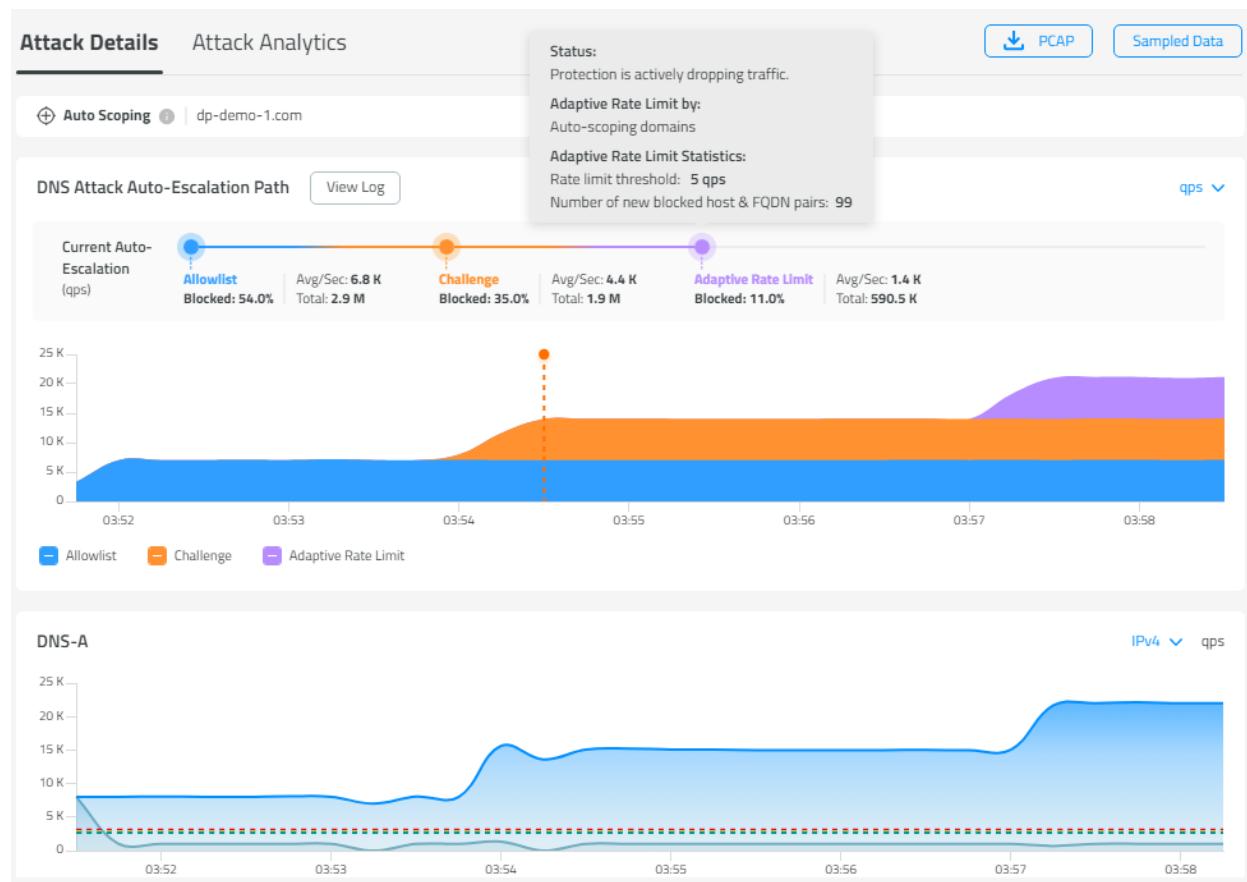
3. Authenticated Resolvers Dictionary Attack

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	
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- Creating domains do domain	

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/appData/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.

Policies 2		Devices 1						+ Add Policy
Status	Policy Name	Device Name	Inbound (Mbit/s)	Dropped (Mbit/s)	Challenged (Mbit/s)	Packet Capture		
! Active	VDP_Demo_Lab	DefensePro X	8.28 M	5.07 M	2.5 M			
✓ Active	VDP_Demo_Lab_Advanced	DefensePro X	0	0	0			

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

Legend: Dropped (red), Passed (green), Match (blue), Challenge (purple)

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

RDLENGTH: 40

RDATAt:

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 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 36 31 37 09 64 70 2D 64 65 6D 6F 2D 31 03  44617.DP-DEMO-1.
0090 63 6F 6D 00
    
```

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**".

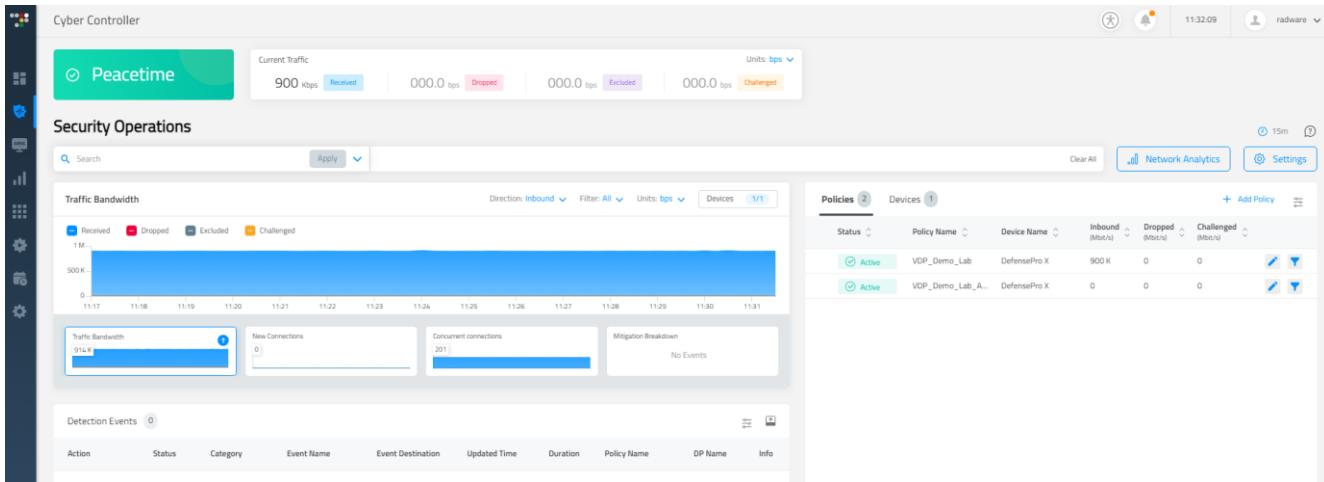
Here's a high-level overview of the script's actions:

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      # RT 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:



The screenshot shows the Cyber Controller interface under the 'Security Operations' tab. At the top, a green banner indicates 'Peacetime' with '900 Kbps Received' and '000.0 bps Dropped'. Below this, a 'Traffic Bandwidth' chart shows a single blue bar for 'Received' traffic from 11:17 to 11:31, peaking at 900 Kbps. To the right, a table lists 'Policies' and 'Devices'. The 'Policies' table shows two entries: 'VDP_Demo_Lab' and 'VDP_Demo_Lab_A...'. The 'Devices' table shows one entry: 'DefensePro X'. At the bottom, a 'Detection Events' table is partially visible.



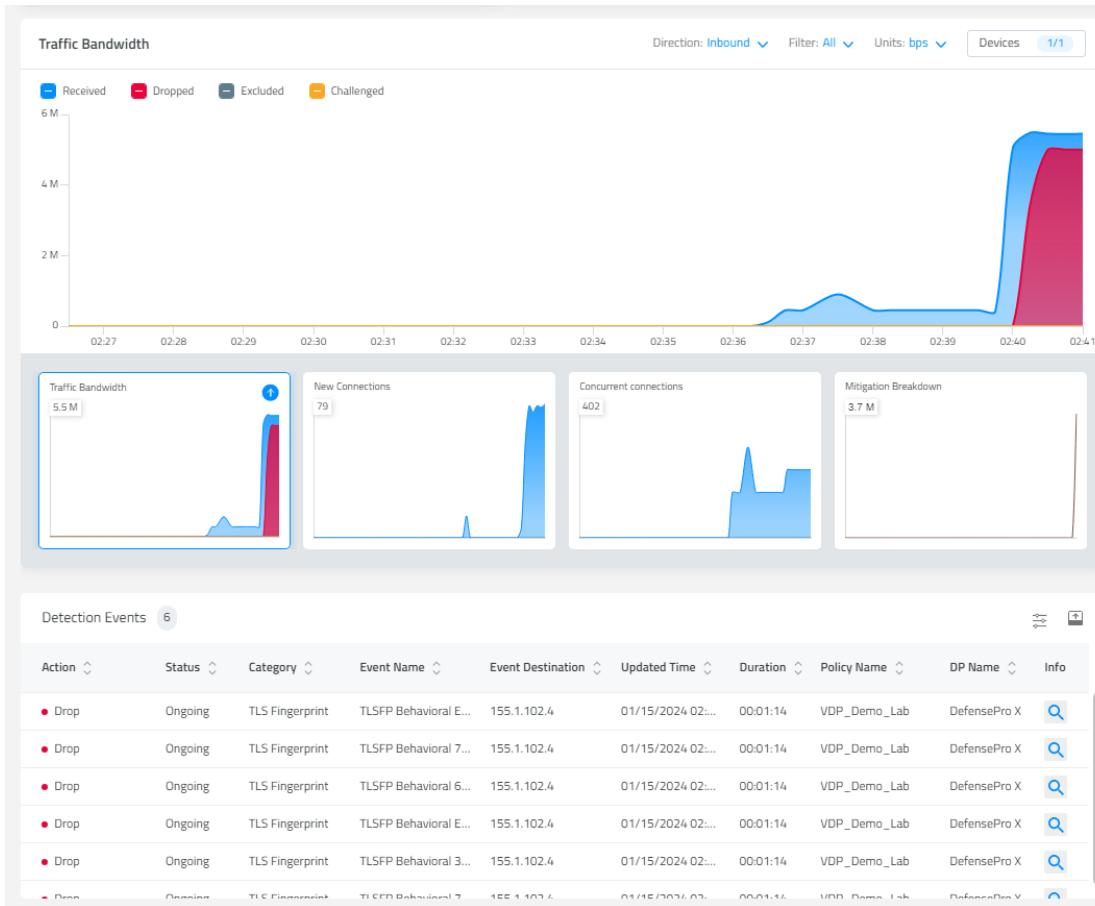
The screenshot shows the Cyber Controller interface under the 'Network Analytics' tab. It displays 'Top TLS Fingerprints' with a line chart showing the count of hits over time. The chart shows a significant spike in hits around 10:45. To the right, a table lists 'Fingerprint', 'Service Names', 'Top Hits(pps)', and 'Top (%)'. The table data is as follows:

Fingerprint	Service Names	Top Hits(pps)	Top (%)
97C14B...	Firefox 115.0	60.6	30.27 %
41A0E0...	Unknown	45.45	22.70 %
C80858...	Safari 15.6-16.5	24.89	12.43 %
50B648...	Unknown	19.48	9.73 %
80E962...	Unknown	17.31	8.65 %
4356AA...	Firefox 93.0-11...	14.07	7.03 %
A0102F...	Unknown	7.58	3.78 %
13B0FE...	Unknown	4.33	2.16 %
9F8358...	Unknown	3.25	1.62 %
0B2C65...	Unknown	3.25	1.62 %

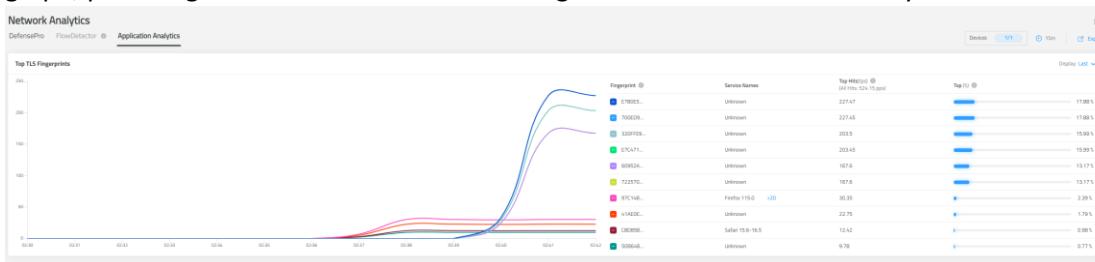
TLS Attacks

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.



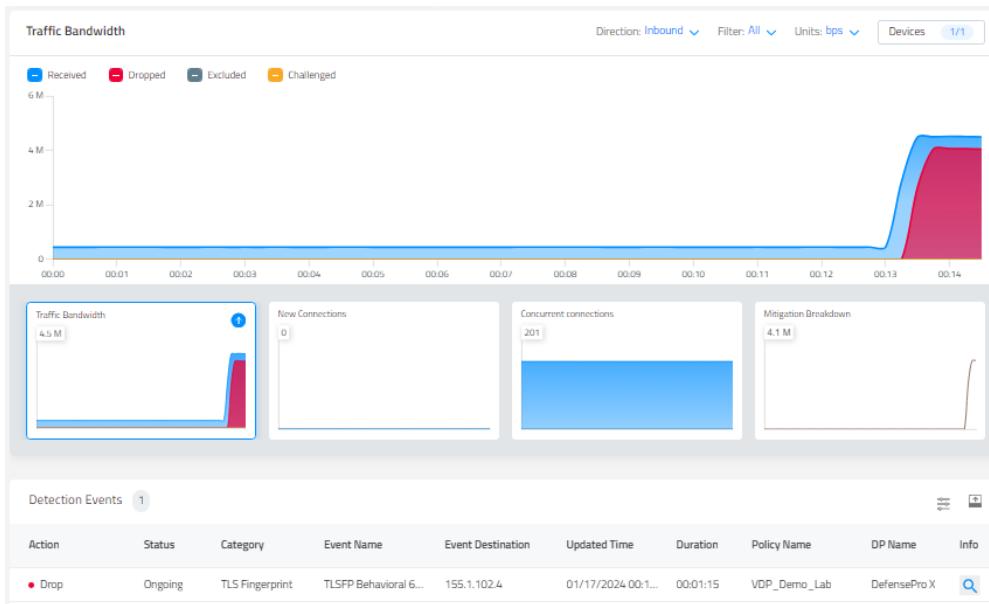
2. **Non-Citizen attack** – this attack is using a packet capture as well to send TLS Client-Hellos, the aim with this scenario is to show an attack on a fingerprint that existed during peace time and is considered non-Citizen as its traffic is significantly low, meaning it can be used for mitigation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



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

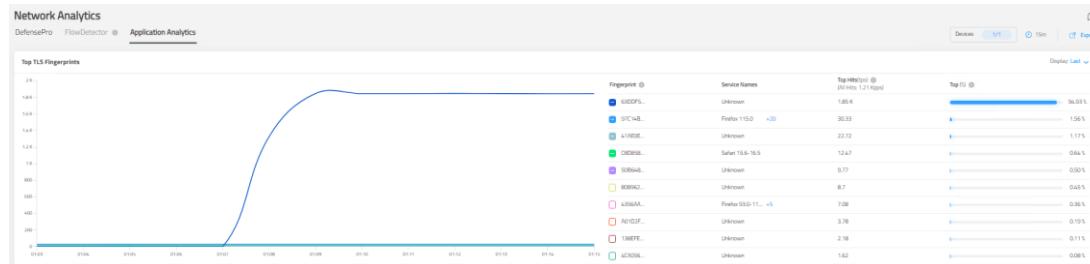
For Policies in Learning State: 25 For Policies in all other States														
Total Fingerprints: 25	Citizens : 11	Under Attack : 0												
Policy Name	Fingerprint	Policy State	FP State	Current Hits	Current Portion	Moving Hits	Baseline Hits	Baseline Portion	Citizen	Attack-on Edge	Attack-off Edge	Attack Off	Idle Time	Under Attack
VDP_Demo_Lab	97C148335356004F0F00A101F5405CA	Detected	Active	30.5	0.277273	29.130	29.128	0.275681	Yes	50.250	43.694	0	0	No
VDP_Demo_Lab	41AA0E5797CC630C2B38C04E83196A6	Detected	Active	23.0	0.209091	21.834	21.833	0.206433	Yes	50.000	32.750	0	0	No
VDP_Demo_Lab	CB05087F0C70C57704A54401FF5209F	Detected	Active	12.7	0.115020	11.470	11.470	0.113222	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	803962244B0C7C5B7D350951E1A5458	Detected	Active	0.7	0.000000	0.400	0.400	0.000000	Yes	50.000	0.000	0	0	No
VDP_Demo_Lab	803962244B0C7C5B7D350951E1A5458	Detected	Active	0.6	0.079182	0.329	0.329	0.079126	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	4356AA12F6958C4723B419599FT2F7	Detected	Active	7.0	0.063636	6.787	6.787	0.064230	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	4356AA12F6958C4723B419599FT2F7	Detected	Active	6.9	0.063636	6.787	6.787	0.064230	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	138F8E448FB020218579TA1EAC441	Detected	Active	2.2	0.020000	2.084	2.084	0.019720	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	4CA05667E0F30B802F6217C3656053	Detected	Active	1.6	0.014545	1.563	1.563	0.014793	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	9E7358AC24C0752F901E76A950A6E	Detected	Active	1.6	0.014545	1.553	1.553	0.014677	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	288F8A5C3D13C3C274F232D0EYF4164093	Detected	Active	1.5	0.014545	1.524	1.524	0.014640	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	288F8A5C3D13C3C274F232D0EYF4164093	Detected	Active	1.0	0.009091	1.042	1.042	0.009060	Yes	50.000	20.000	0	0	No
VDP_Demo_Lab	477178430A0191FB9531E406469F	Detected	Active	0.6	0.050455	0.527	0.527	0.049688	No	50.000	20.000	0	0	No
VDP_Demo_Lab	477178430A0191FB9531E406469F	Detected	Active	0.5	0.050455	0.527	0.527	0.049688	No	50.000	20.000	0	0	No
VDP_Demo_Lab	00CF0F0A1A1D9479218370157004B403	Detected	Active	0.5	0.004545	0.527	0.527	0.004688	No	50.000	20.000	0	0	No
VDP_Demo_Lab	423A9368EFC2CA6F690633920A583C	Detected	Active	0.5	0.004545	0.527	0.527	0.004688	No	50.000	20.000	0	0	No
VDP_Demo_Lab	A59A13E44FC9C3D04270235105813AC	Detected	Active	0.5	0.004545	0.521	0.521	0.004627	No	50.000	20.000	0	0	No
VDP_Demo_Lab	7930A75504697C555064E4210F66080	Detected	Active	0.5	0.004545	0.521	0.521	0.004627	No	50.000	20.000	0	0	No
VDP_Demo_Lab	C0D4200F1B13BFC7C0EAE11F710B40	Detected	Active	0.5	0.004545	0.521	0.521	0.004627	No	50.000	20.000	0	0	No
VDP_Demo_Lab	477178430A0191FB9531E406469F	Detected	Active	0.4	0.050455	0.521	0.521	0.049688	No	50.000	20.000	0	0	No
VDP_Demo_Lab	477178430A0191FB9531E406469F	Detected	Active	0.6	0.050455	0.515	0.515	0.049472	No	50.000	20.000	0	0	No
VDP_Demo_Lab	A59A13E44FC9C3D04270235105813AC	Detected	Active	0.6	0.050455	0.515	0.515	0.049472	No	50.000	20.000	0	0	No
VDP_Demo_Lab	DA9F7E97102A2E0244AA9C0568F2B1F	Detected	Active	0.5	0.004545	0.515	0.515	0.004672	No	50.000	20.000	0	0	No
VDP_Demo_Lab	FE3C77C9B97B7B530C944FF9082	Detected	Active	0.6	0.050455	0.513	0.513	0.050454	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.



Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
• Drop	Ongoing	TLS Fingerprint	TLSFP Behavioral 6...	155.1.102.4	01/17/2024 00:1...	00:01:15	VDP_Demo_Lab	DefensePro X	

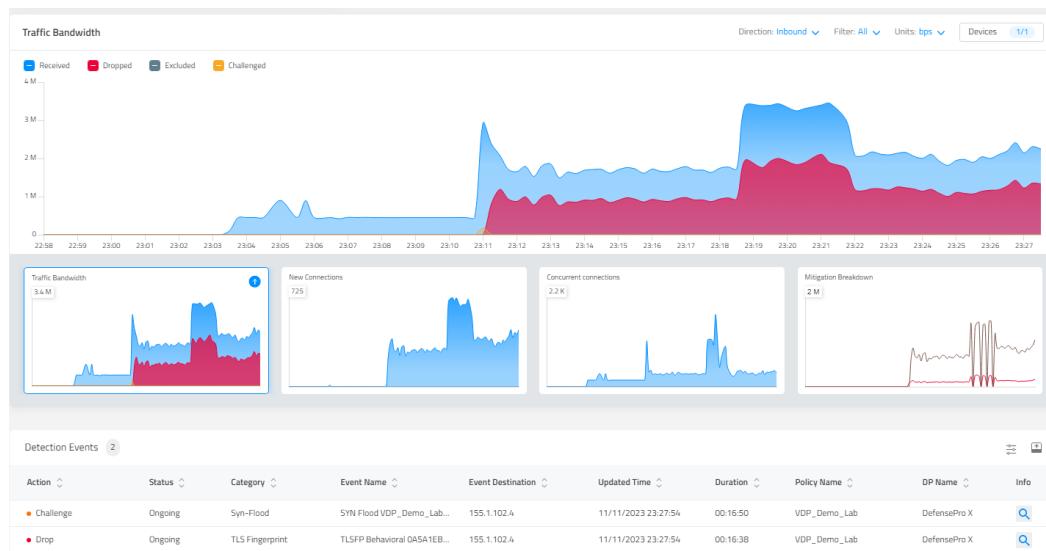
By examining the Application Analytics, you can identify the non-Citizen fingerprints responsible for the attack.



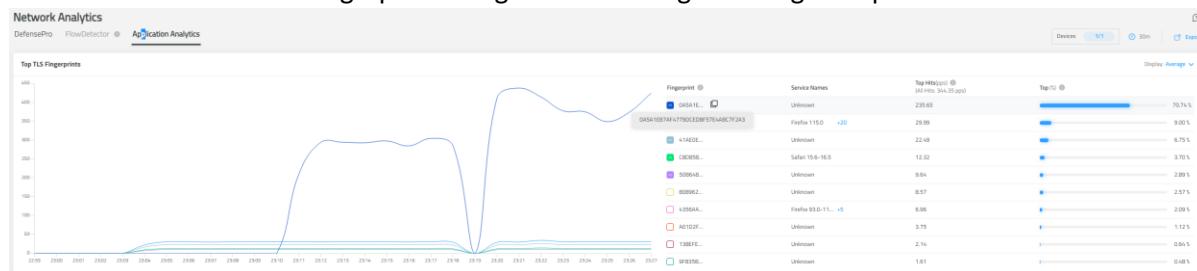
3. **Python script attack** – this script is used to create an HTTP attack involving a complete TCP connection followed by TLS handshake, unlike the previous two attacks that relied on packet captures with only TLS Client-Hello. The script establishes numerous HTTPS connections intentionally exceeding 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.



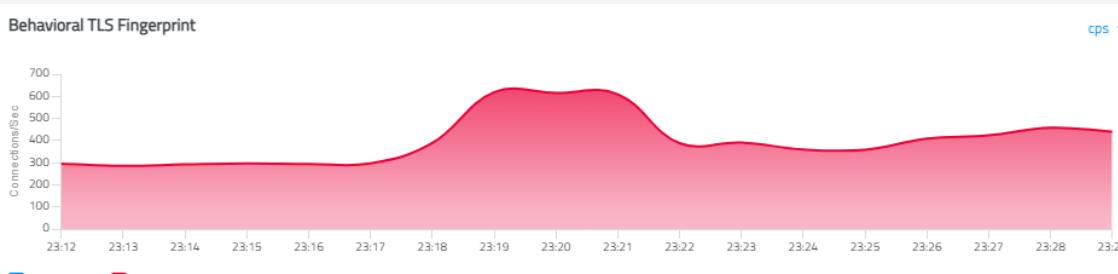
TLS Fingerprint, TLSFP Behavioral 0A5A1EB7AF4779DCED8F57E4ABC7F2A3 ⓘ

Protected Object/Policy: VDP_Demo_Lab Destination Address: 155.1.102.4 Start Time: 11/11/23 23:11 Duration: 00:18:33 Attack Name: TLSFP Behavioral 0A5A1EB7AF...

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

Fingerprint: 0A5A1EB7AF4779DCED8F57E4ABC7F2A3 **Service Name:** Unknown

Behavioral TLS Fingerprint



The chart shows 'Connections/Sec' on the Y-axis (0 to 700) and time on the X-axis (23:12 to 23:29). A red area represents 'Dropped' connections, which remains relatively flat until 23:18, then rises sharply to a peak of about 600 cps before gradually declining. A legend indicates 'Reported' (blue) and 'Dropped' (red) connections.

Additional Attack Attributes

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	600	In	Drop	46-1699771242	1	398059
VLAN	MPLS RD	Source Port	Packet Type			
N/A	N/A	Multiple	Regular			

HTTPS Protection

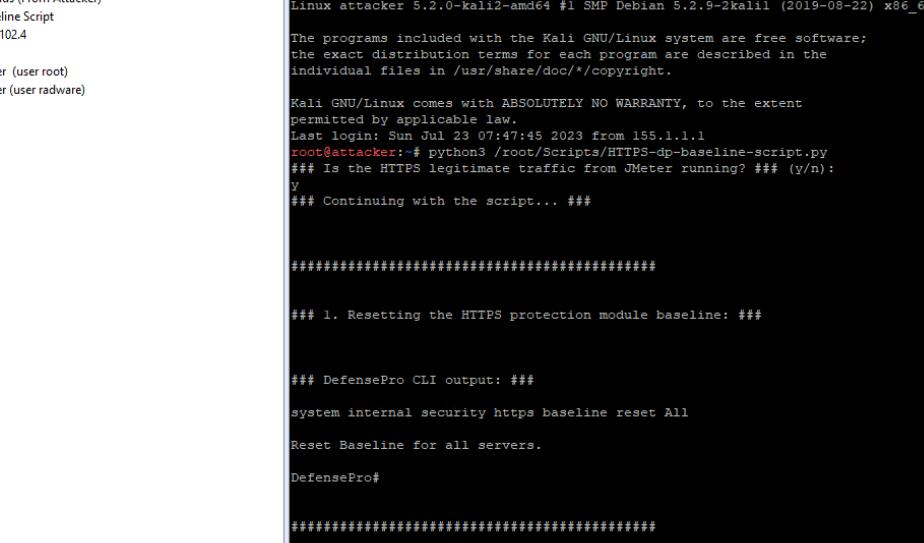
For more additional information about this scenario, please refer to the “[Appendix 1 - HTTPS Protection \(Additional Info\)](#)” section.

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 àDP Demo Labà 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!).



The screenshot shows the ONS Manager interface with a terminal window open. The terminal window title is "HTTPS Baseline Script". The terminal content shows a series of commands and their outputs, indicating the setup of an HTTPS baseline on a Kali Linux system, followed by configuration steps for DefensePro and a final configuration step for the HTTPS module.

```
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 radmin)
DefensePro X
Router(Vyo5)
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:



```

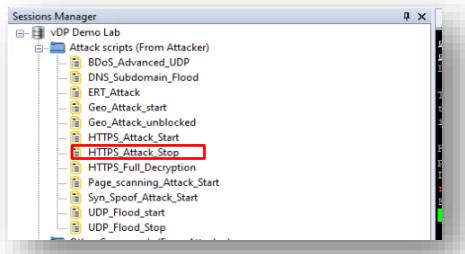
Sessions Manager
vDP Demo Lab
Attack scripts (From Attacker)
  BDOS_Advanced_UDP
  DNS_Subdomain_Flood
  ERT_Attack
  Geo_Attack_start
  Geo_Attack_unblocked
  HTTPS_Attack_Start (highlighted)
  HTTPS_Attack_Stop
  HTTPS_Full_Decryption
  Page_scanning_Attack_Start
  Syn_Spoof_Attack_Start
  UDP_Flood_Start
  UDP_Flood_Stop

DefensePro X / HTTPS_Attack_Start
login as: root
root@155.1.1.2's password:
Linux attacker 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali2 (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: Wed May 17 05:39:47 2023 from 155.1.1.1
root@attacker:~# tcpreplay -i eth1 -K --mbps 7 --loop 50000000 ~/Attack_Scenarios/HTTPS_Attack/HTTPS_Attack.pcap
File Cache is enabled

```

2. In order to **stop** the attack, double click on **HTTPS_Attack_Stop**:

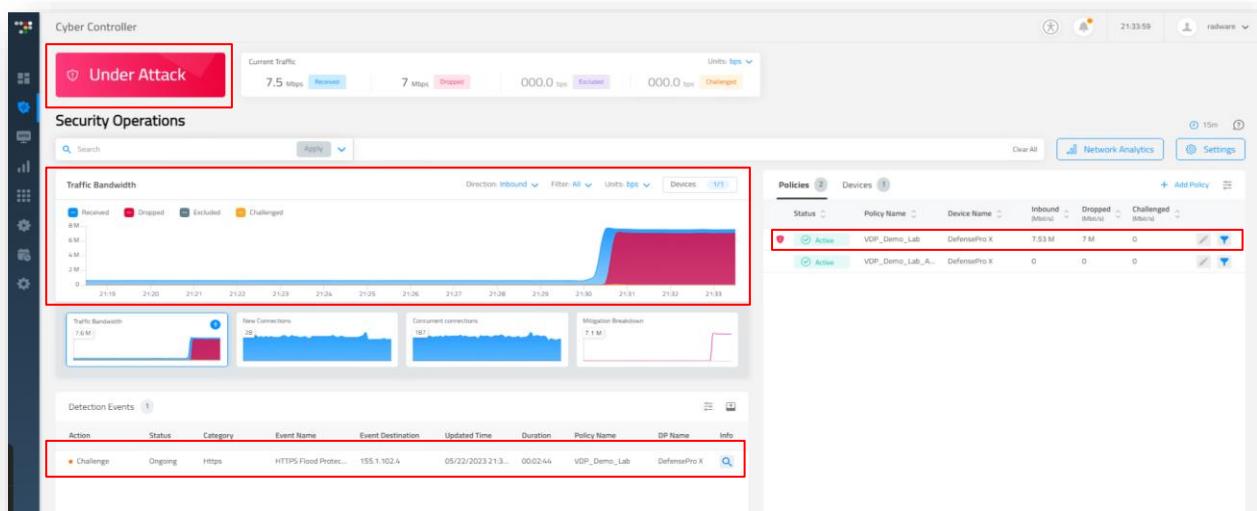


Attack Mitigation

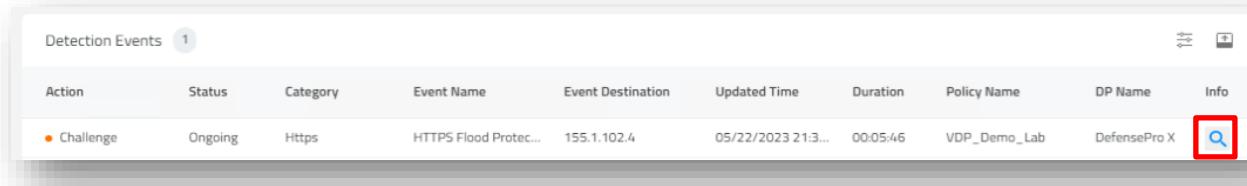
While the attack is running, the HTTPS protection module begins the characterization process of the malicious sources.

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**:

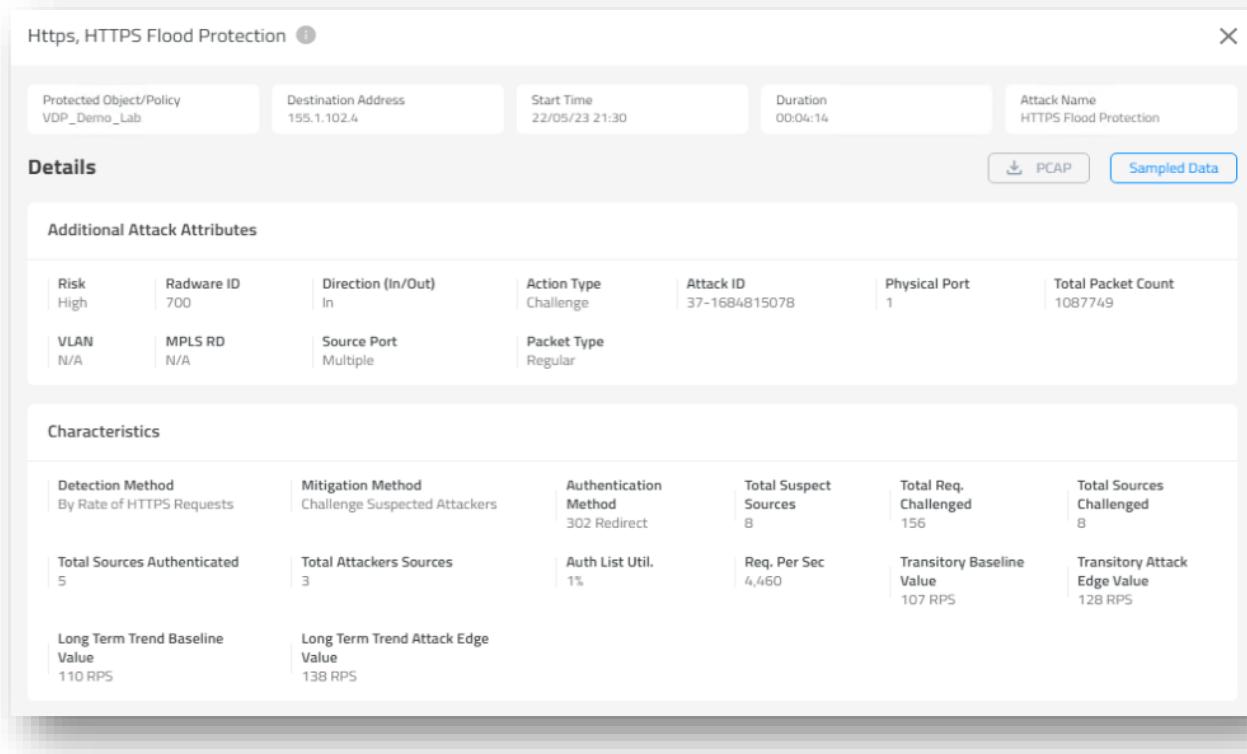


2. On the detection events section, you will find the event attack. You can verify the attack details by clicking on the magnifying glass button:



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:

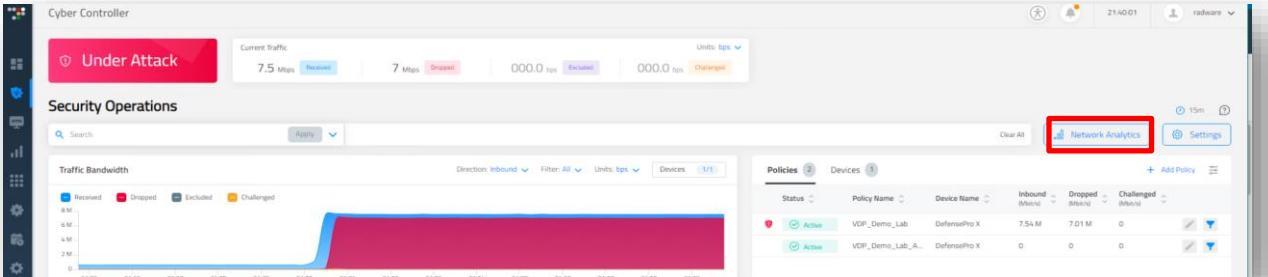


Protected Object/Policy		Destination Address		Start Time	Duration	Attack Name
VDP_Demo_Lab		155.1.102.4		22/05/23 21:30	00:04:14	HTTPS Flood Protection

Details																								
Additional Attack Attributes <table border="1"> <tr> <td>Risk High</td> <td>Radware ID 700</td> <td>Direction (In/Out) In</td> <td>Action Type Challenge</td> <td>Attack ID 37-1684815078</td> <td>Physical Port 1</td> <td>Total Packet Count 1087749</td> </tr> <tr> <td>VLAN N/A</td> <td>MPLS RD N/A</td> <td>Source Port Multiple</td> <td>Packet Type Regular</td> <td colspan="3"></td> </tr> </table>							Risk High	Radware ID 700	Direction (In/Out) In	Action Type Challenge	Attack ID 37-1684815078	Physical Port 1	Total Packet Count 1087749	VLAN N/A	MPLS RD N/A	Source Port Multiple	Packet Type Regular							
Risk High	Radware ID 700	Direction (In/Out) In	Action Type Challenge	Attack ID 37-1684815078	Physical Port 1	Total Packet Count 1087749																		
VLAN N/A	MPLS RD N/A	Source Port Multiple	Packet Type Regular																					
Characteristics <table border="1"> <tr> <td>Detection Method By Rate of HTTPS Requests</td> <td>Mitigation Method Challenge Suspected Attackers</td> <td>Authentication Method 302 Redirect</td> <td>Total Suspect Sources 8</td> <td>Total Req. Challenged 156</td> <td>Total Sources Challenged 8</td> </tr> <tr> <td>Total Sources Authenticated 5</td> <td>Total Attackers Sources 3</td> <td>Auth List Util. 1%</td> <td>Req. Per Sec 4,460</td> <td>Transitory Baseline Value 107 RPS</td> <td>Transitory Attack Edge Value 128 RPS</td> </tr> <tr> <td>Long Term Trend Baseline Value 110 RPS</td> <td>Long Term Trend Attack Edge Value 138 RPS</td> <td colspan="4"></td> </tr> </table>							Detection Method By Rate of HTTPS Requests	Mitigation Method Challenge Suspected Attackers	Authentication Method 302 Redirect	Total Suspect Sources 8	Total Req. Challenged 156	Total Sources Challenged 8	Total Sources Authenticated 5	Total Attackers Sources 3	Auth List Util. 1%	Req. Per Sec 4,460	Transitory Baseline Value 107 RPS	Transitory Attack Edge Value 128 RPS	Long Term Trend Baseline Value 110 RPS	Long Term Trend Attack Edge Value 138 RPS				
Detection Method By Rate of HTTPS Requests	Mitigation Method Challenge Suspected Attackers	Authentication Method 302 Redirect	Total Suspect Sources 8	Total Req. Challenged 156	Total Sources Challenged 8																			
Total Sources Authenticated 5	Total Attackers Sources 3	Auth List Util. 1%	Req. Per Sec 4,460	Transitory Baseline Value 107 RPS	Transitory Attack Edge Value 128 RPS																			
Long Term Trend Baseline Value 110 RPS	Long Term Trend Attack Edge Value 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:



The screenshot shows the Cyber Controller interface. At the top, a red banner displays the message "Under Attack". Below it, the "Security Operations" section shows a "Traffic Bandwidth" chart with a sharp peak in traffic around 21:30. To the right, a table lists "Policies" and "Devices". The "Network Analytics" button is highlighted with a red box. The main content area shows the "Network Analytics" dashboard with sections for "DefensePro Traffic", "Top Source IP Addresses", and "Last Week Trends".

Network Analytics

DefensePro Traffic

Received (bps)	7.5 M	Avg 2.8 M	Max 7.6 M
Dropped (bps)	7 M	Avg 2.2 M	Max 7.1 M
Excluded (bps)	0	Avg 0	Max 0
Challenged (bps)	0	Avg 1.1 k	Max 94 k

Top Source IP Addresses

Source	Total	Total (%)
155.1.101.14	1.36 Mbps	80.81%
155.1.101.13	69 Kbps	4.16%
155.1.101.11	68 Kbps	4.06%
155.1.101.10	68 Kbps	4.06%
155.1.101.12	58 Kbps	3.47%

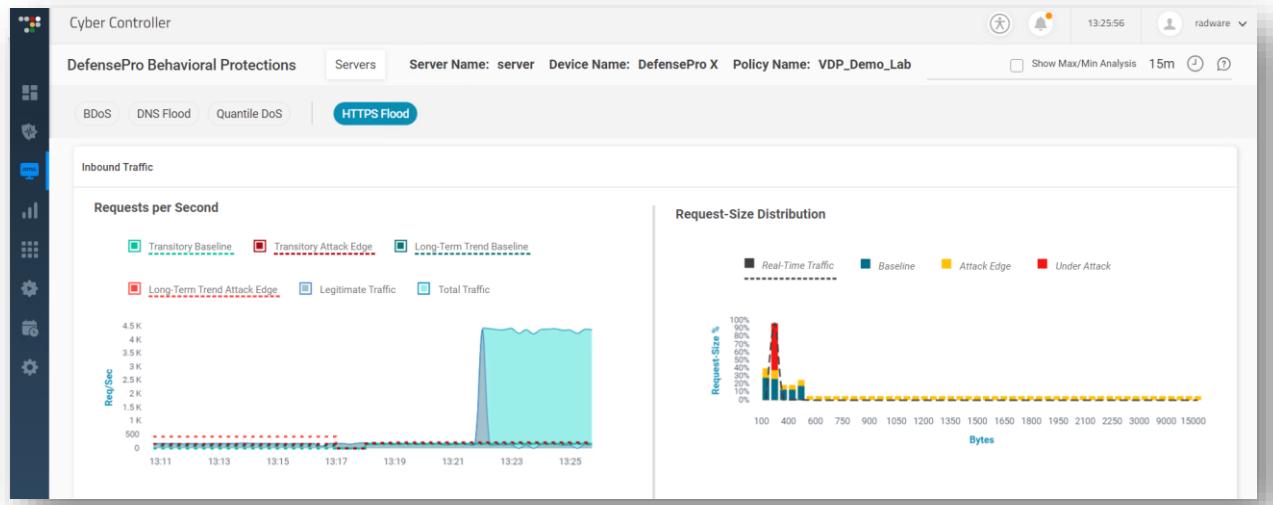
Last Week Trends

Top Policies: VDP_Demo_Lab, excluded

Top Applications: DNS (10), N_A (1900), N_A (5353), NetBIOS (137)

6. 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:

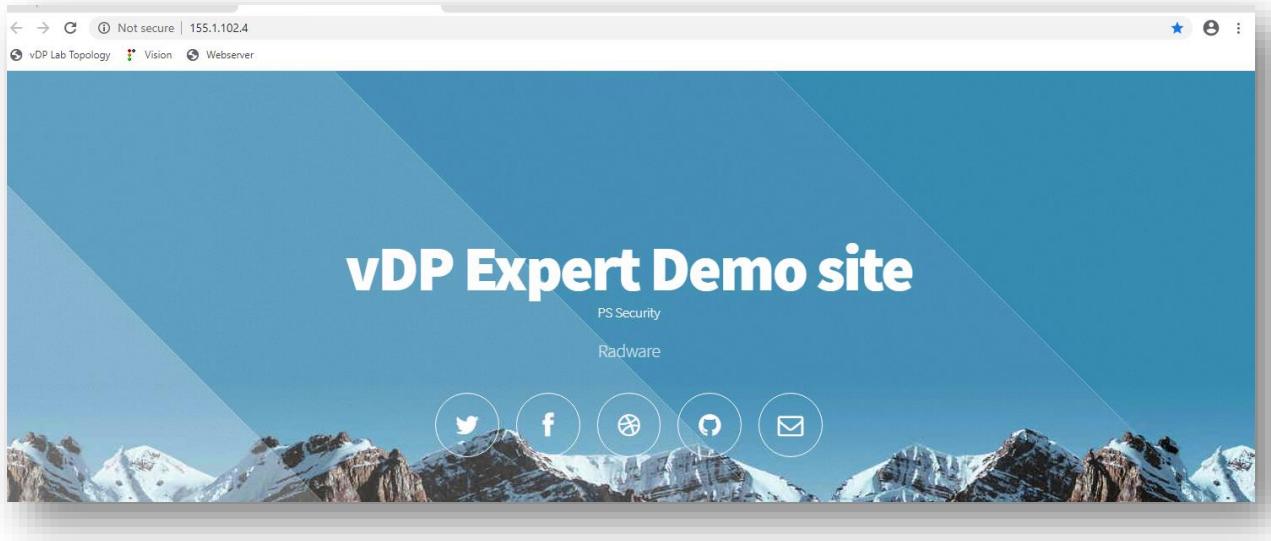


7. Open the *JMeter* pane and view the 302 results in the *Response code per second* pane:

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>):



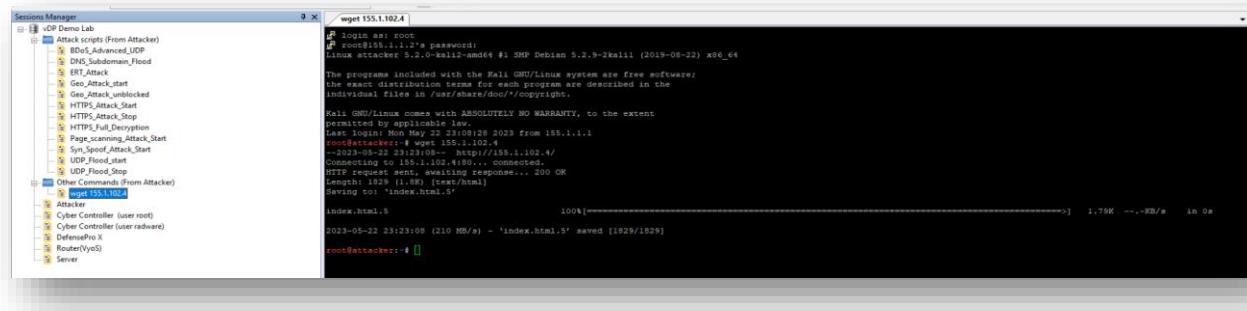
Traffic Filters

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.

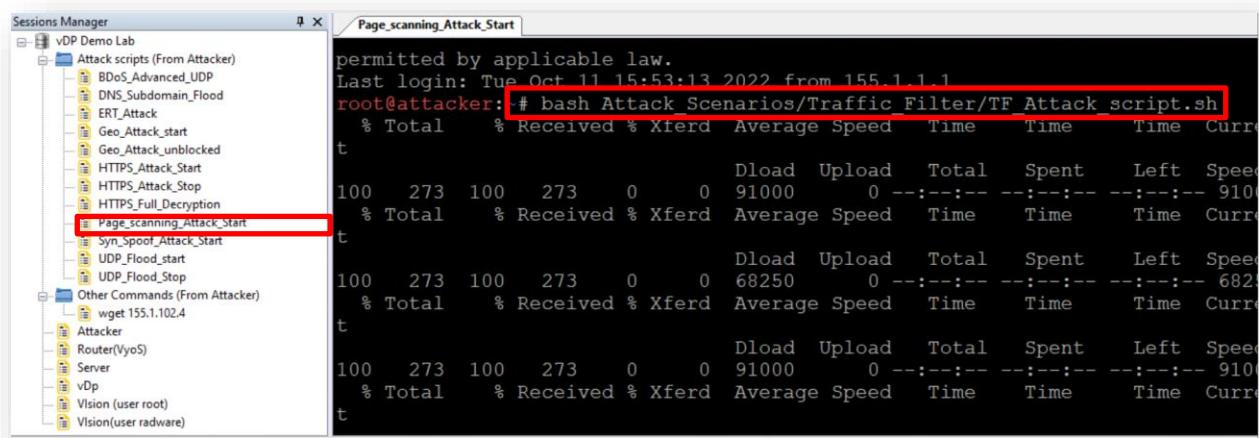
Select the **wget 155.1.102.4** icon located in the **Other Commands (From Attacker)** folder on the Session Manager.



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.

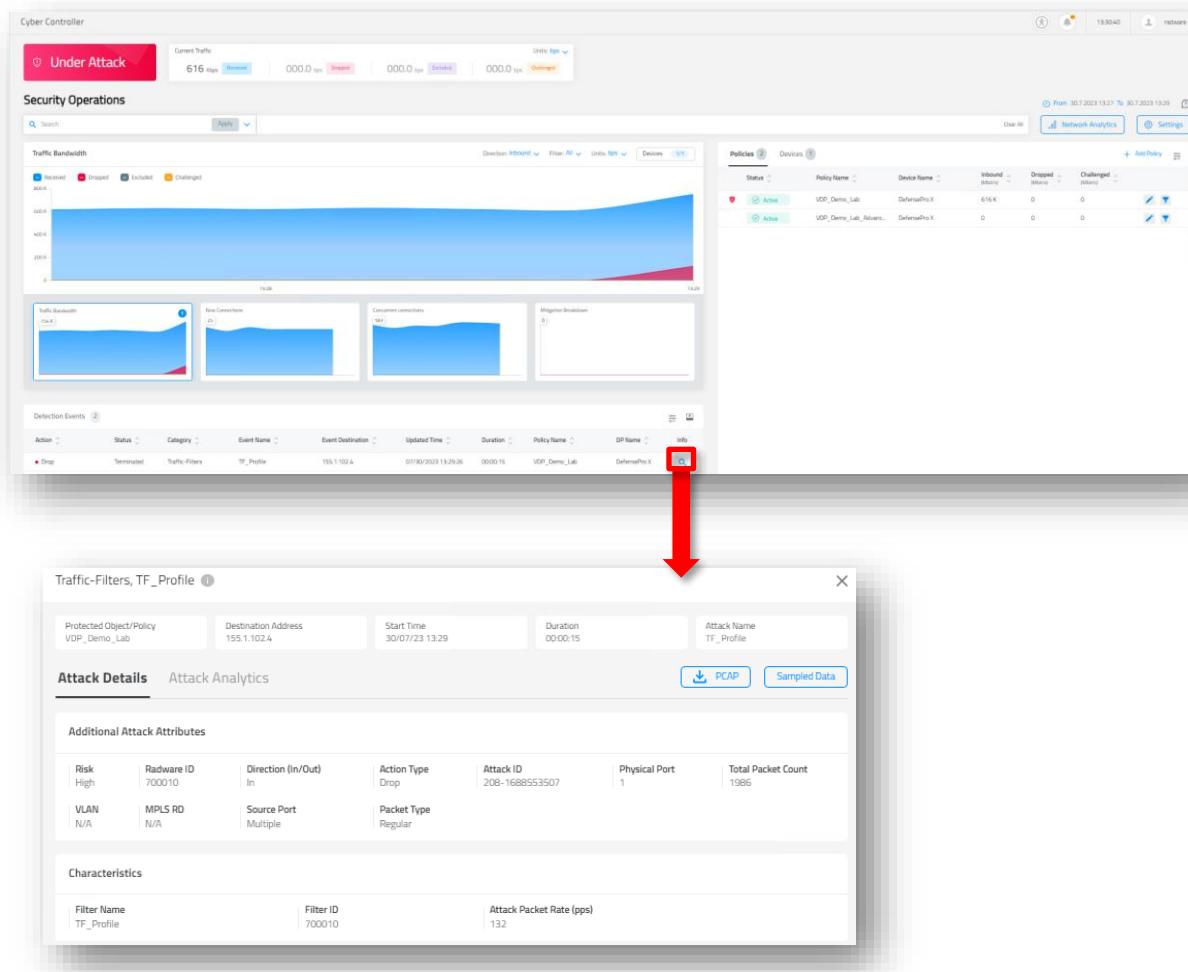
While the script is running, the following screen displays:



- To stop the attack, press **Ctrl +C**

Attack Mitigation

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



The screenshot shows the Cyber Controller's Real-Time Monitoring interface. At the top, a red banner indicates "Under Attack" with a current traffic count of 616 Kbps. The main dashboard displays traffic bandwidth, new connections, concurrent connections, and mitigation breakdown. Below this, a table shows policies and devices. A red arrow points from the "Info" button in the policy table to a detailed "Traffic-Filters, TF_Profile" modal window.

Traffic-Filters, TF_Profile

Protected Object/Policy	Destination Address	Start Time	Duration	Attack Name
VDP_Demo_Lab	155.1.102.4	30/07/23 13:29	00:00:15	TF_Profile

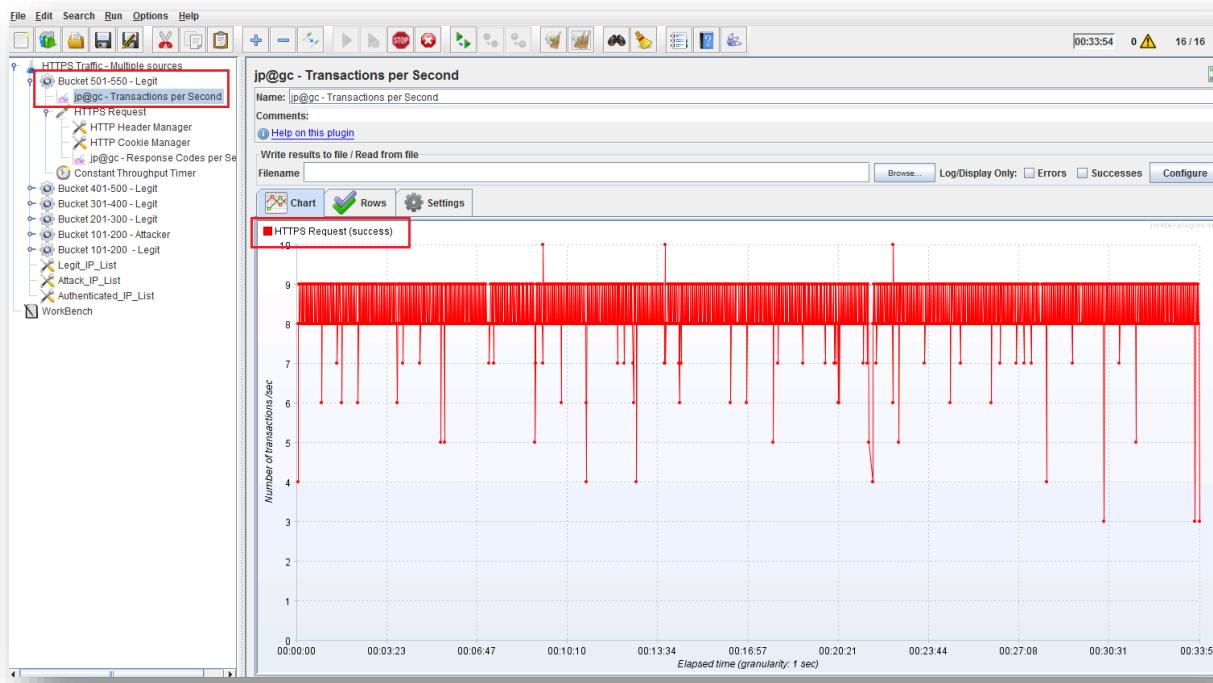
Attack Details

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

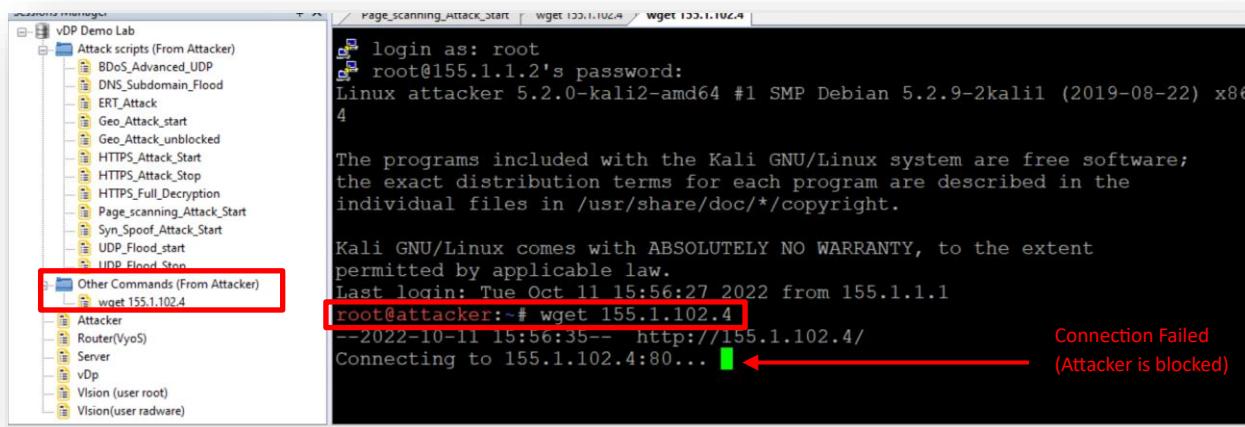
Filter Name	Filter ID	Attack Packet Rate (pps)
TF_Profile	700010	132

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

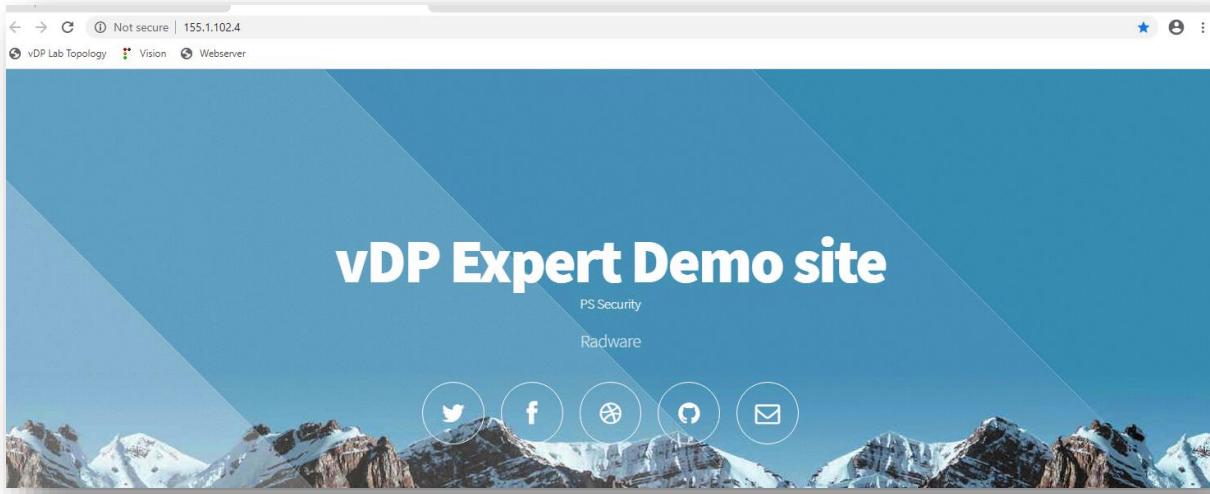


3. Check if the Attacker client can log in to the Webserver.

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



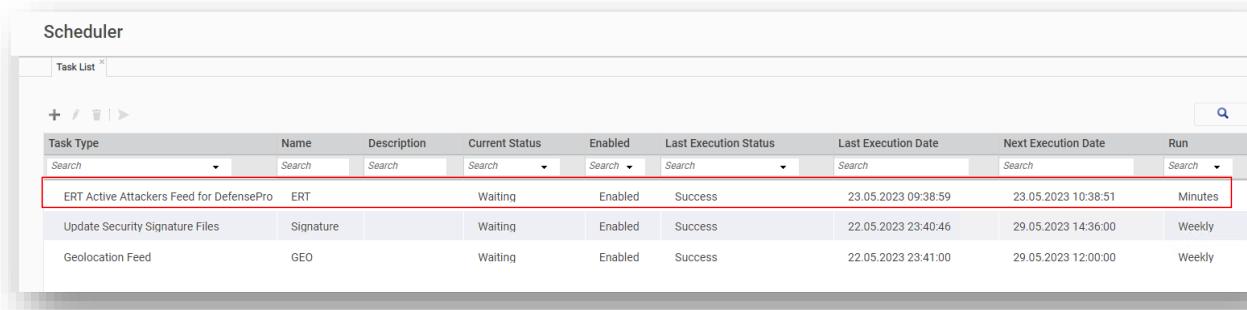
4. Verify connectivity towards the attacking destination. Open the browser and select the **Site(155.1.102.4)** bookmark (URL: <http://155.1.102.4>):



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:



The screenshot shows the 'Scheduler' interface in the Cyber Controller. The 'Task List' tab is selected. A table displays the following tasks:

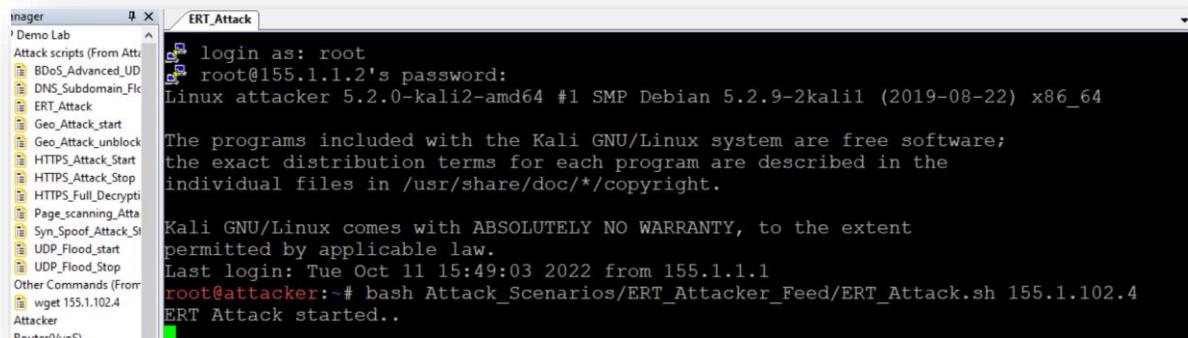
Task Type	Name	Description	Current Status	Enabled	Last Execution Status	Last Execution Date	Next Execution Date	Run
Search	Search	Search	Search	Search	Search	Search	Search	Search
ERT Active Attackers Feed for DefensePro	ERT		Waiting	Enabled	Success	23.05.2023 09:38:59	23.05.2023 10:38:51	Minutes
Update 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

1. 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:



The terminal window title is 'ERT_Attack'. The session is running as root on a Kali Linux system. The output of the script is as follows:

```

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.

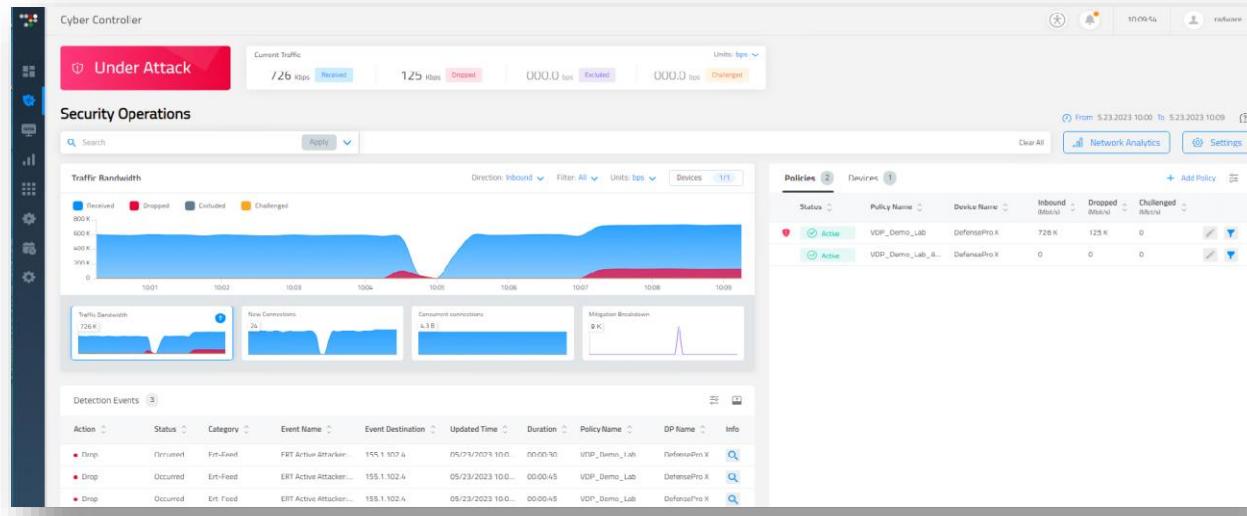
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 11 15:49:03 2022 from 155.1.1.1
root@attacker:~# bash Attack_Scenarios/ERT_Attacker_Feed/ERT_Attack.sh 155.1.102.4
ERT Attack started..

```

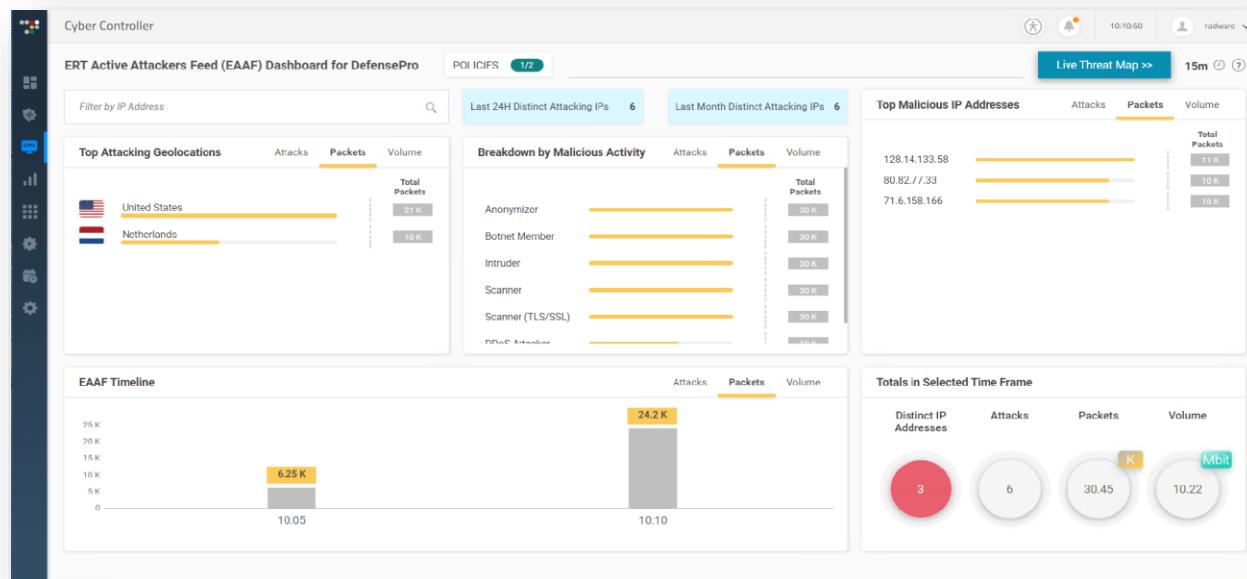
2. In order to stop the attack, press **Ctrl +C**.

Attack Mitigation

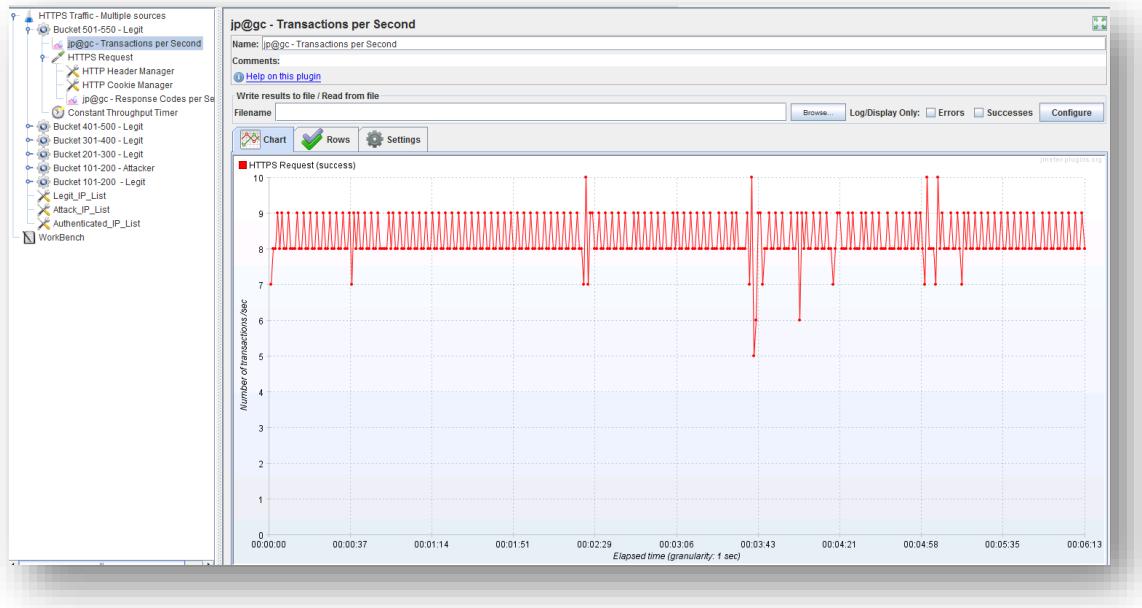
1. Verify the attack in Cyber Controller. Go to **Security Operations** -> **Real-Time Monitoring**:



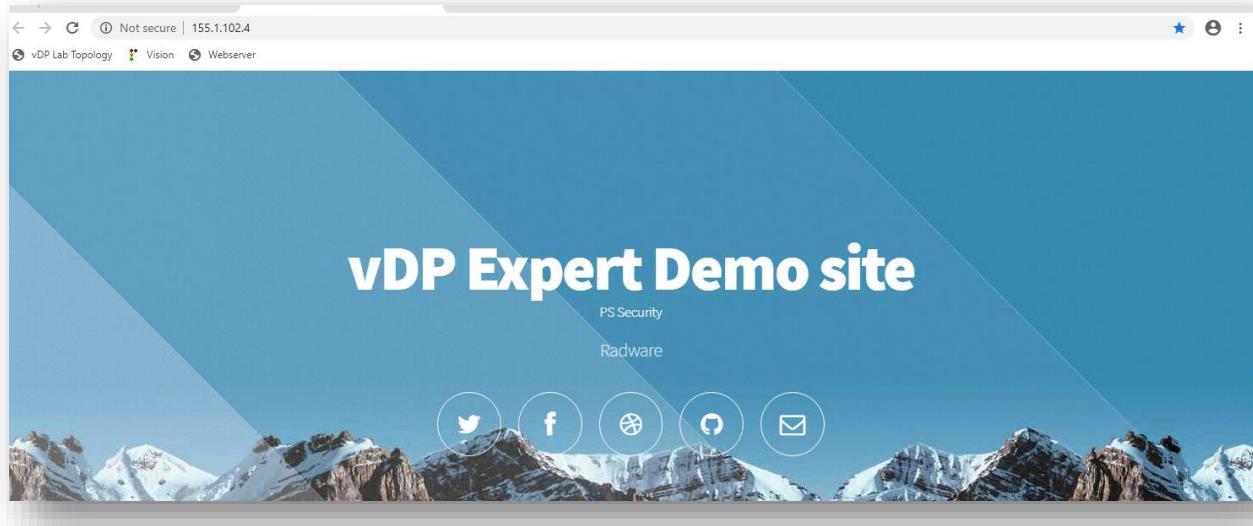
2. Verify the attack details on the **AMS > EAAF Dashboard**:



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



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



Spoofed Syn Attack Protection

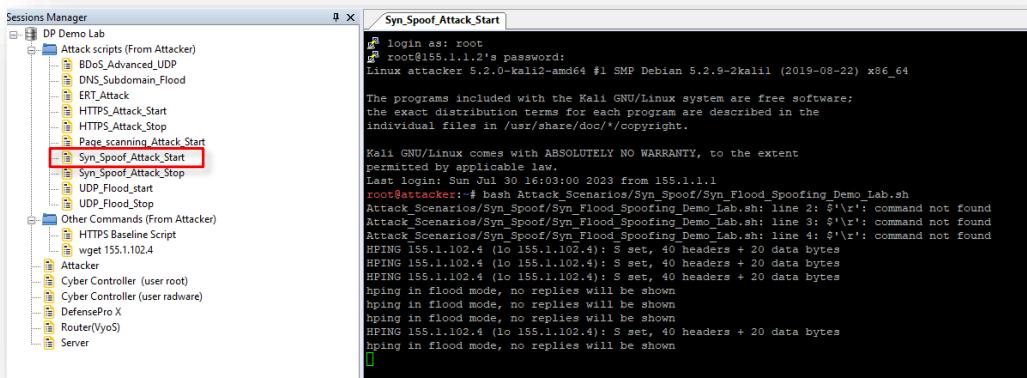
For more additional information about this scenario, please refer to the "[Appendix 4 – Spoofed Syn Attack Protection \(Additional Info\)](#)" section.

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:



```

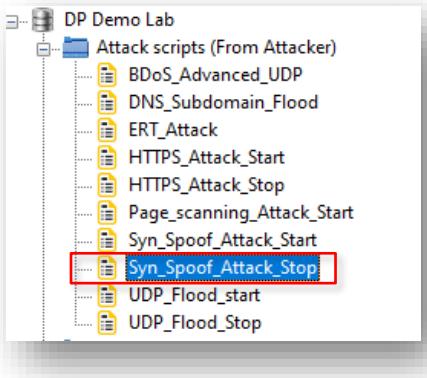
Sessions Manager
DP Demo Lab
  Attack scripts (From Attacker)
    BDOS_Advanced_UDP
    DNS_Subdomain_Flood
    ERT_Attack
    HTTPS_Attack_Start
    HTTPS_Attack_Stop
    Page_scanning_Attack_Start
    Syn_Spoof_Attack_Start (highlighted)
    Syn_Spoof_Attack_Stop
    UDP_Flood_Start
    UDP_Flood_Stop
  Other Commands (From Attacker)
    HTTPS Baseline Script
    wget 155.1.102.4
  Attacker
  Cyber Controller (user root)
  Cyber Controller (user radware)
  DefensePro X
  Router(yoS)
  Server

Syn_Spoof_Attack_Start
login as: root
root@155.1.1.2's password:
Linux attacker 5.2.0-kali2-amd64 #1 SMP Debian 5.2.5-2kali1 (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 30 16:03:00 2023 from 155.1.1.1
root@attacker: ~ bin/Attack_Scenarios/Syn_Spoof/Syn_Flood_Spoofing_Demo_Lab.sh
root@attacker: ~ bin/Attack_Scenarios/Syn_Spoof/Syn_Flood_Spoofing_Demo_Lab.sh: line 2: $'\r': command not found
root@attacker: ~ bin/Attack_Scenarios/Syn_Spoof/Syn_Flood_Spoofing_Demo_Lab.sh: line 3: $'\r': command not found
root@attacker: ~ bin/Attack_Scenarios/Syn_Spoof/Syn_Flood_Spoofing_Demo_Lab.sh: line 4: $'\r': command not found
Hping 155.1.102.4 (to 155.1.102.4); S set, 40 headers + 20 data bytes
Hping 155.1.102.4 (to 155.1.102.4); S set, 40 headers + 20 data bytes
Hping 155.1.102.4 (to 155.1.102.4); S set, 40 headers + 20 data bytes
hping in flood mode, no replies will be shown
hping in flood mode, no replies will be shown
hping in flood mode, no replies will be shown
hping 155.1.102.4 (to 155.1.102.4); S set, 40 headers + 20 data bytes
hping in flood mode, no replies will be shown

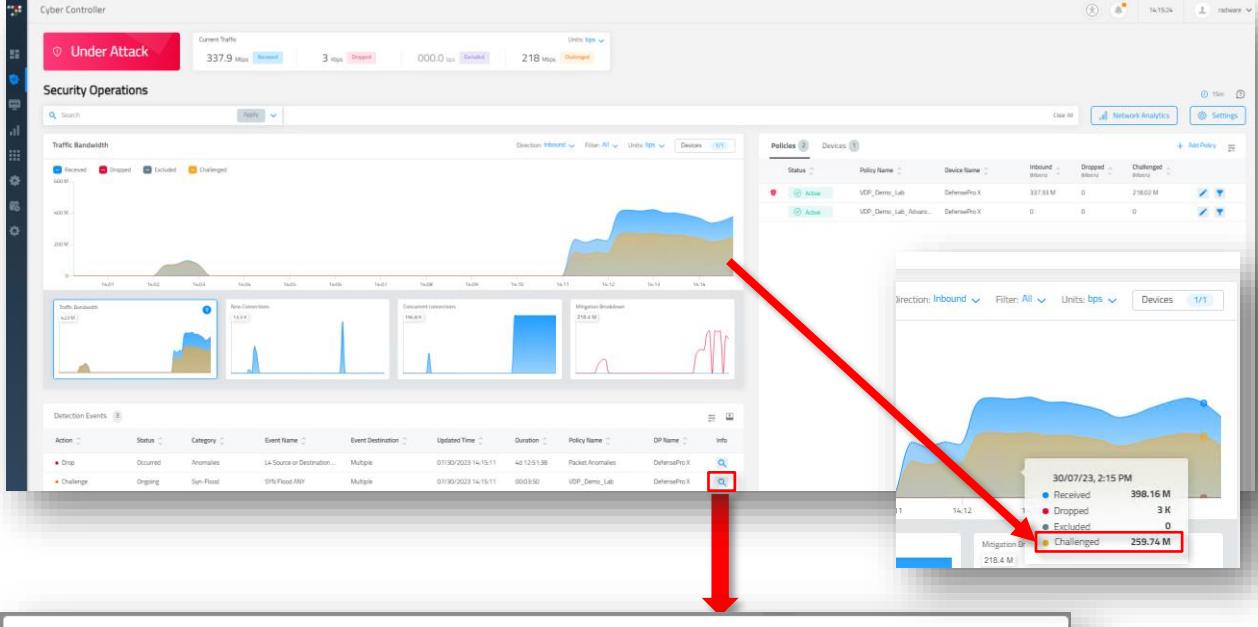
```

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 screenshot shows the Cyber Controller's Security Operations interface. A prominent red banner at the top left says "Under Attack". Below it, the "Traffic Bandwidth" section shows a chart with four stacked areas: Received (blue), Dropped (red), Excluded (green), and Challenged (orange). The total bandwidth is 337.9 Mbit/s. A red arrow points from the "Challenged" area in the main chart to a detailed tooltip for the "Mitigation Breakdown" chart, which shows 218.4 Mbit/s. Another red arrow points from this tooltip to a detailed "Syn-Flood, SYN Flood ANY" attack analysis window.

Attack Details (Syn-Flood, SYN Flood ANY):

Parameter	Value
Protected Object/Policy	VDP_Demo_Lab
Destination Address	Multiple
Start Time	30/07/23 14:11
Duration	00:04:30
Attack Name	SYN Flood ANY

Attack Details (Attack Analytics):

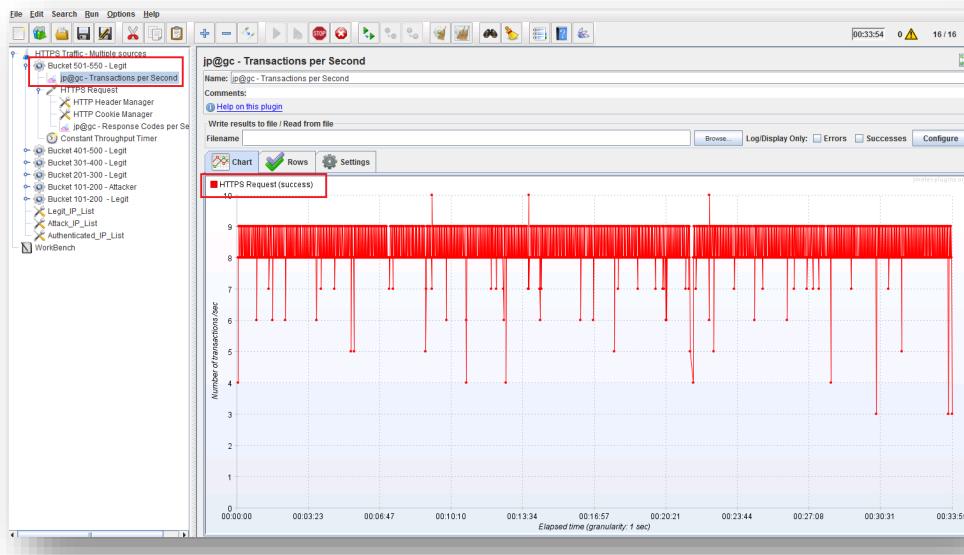
Attribute	Value
Risk	Medium
Radware ID	0
Direction (In/Out)	Unknown
Action Type	Challenge
VLAN	N/A
MPLS RD	N/A
Source Port	Multiple
Packet Type	Regular
Attack ID	216-1688553507
Physical Port	Multiple
Total Packet Count	84349086

Characteristics:

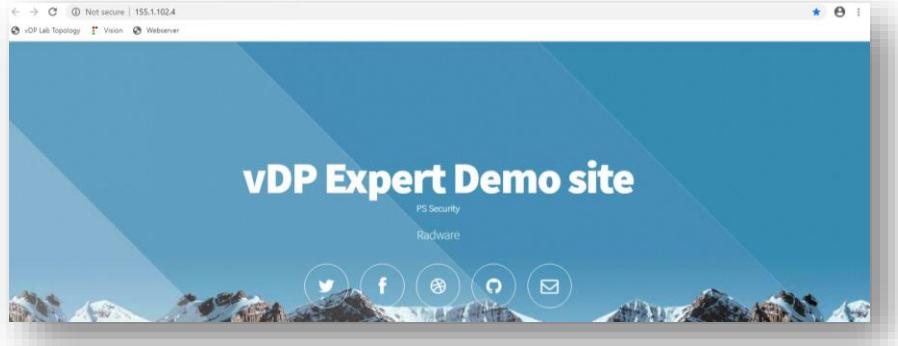
Characteristic	Value
Average Attack Rate (pps)	0
Attack Duration [Hour:Min:Sec]	00:04:30
Activation Threshold (pps)	0
TCP Challenge	Safe Reset
TCP Auth. List (%)	1
HTTP Challenge	Redirect 302
HTTP Auth. List (%)	0

Annotation: 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.

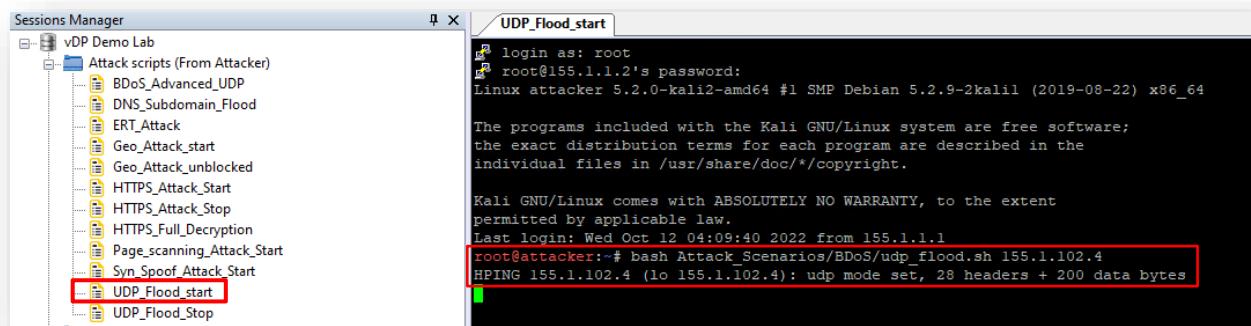
Create a UDP Flood Attack and Verify Detection

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:



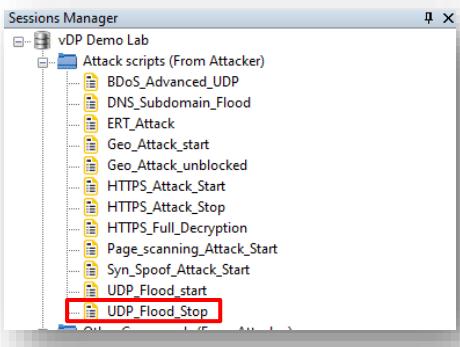
```

Sessions Manager
vDP Demo Lab
  Attack scripts (From Attacker)
    BDoS_Advanced_UDP
    DNS_Subdomain_Flood
    ERT_Attack
    Geo_Attack_start
    Geo_Attack_unblocked
    HTTPS_Attack_Start
    HTTPS_Attack_Stop
    HTTPS_Full_Decryption
    Page_scanning_Attack_Start
    Syn_Spoof_Attack_Start
    UDP_Flood_start
    UDP_Flood_Stop

  UDP_Flood_start
  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: Wed Oct 12 04:09:40 2022 from 155.1.1.1
  root@attacker:~# bash Attack_Scenarios/BDoS/udp_flood.sh 155.1.102.4
  HPING 155.1.102.4 (lo 155.1.102.4): udp mode set, 28 headers + 200 data bytes

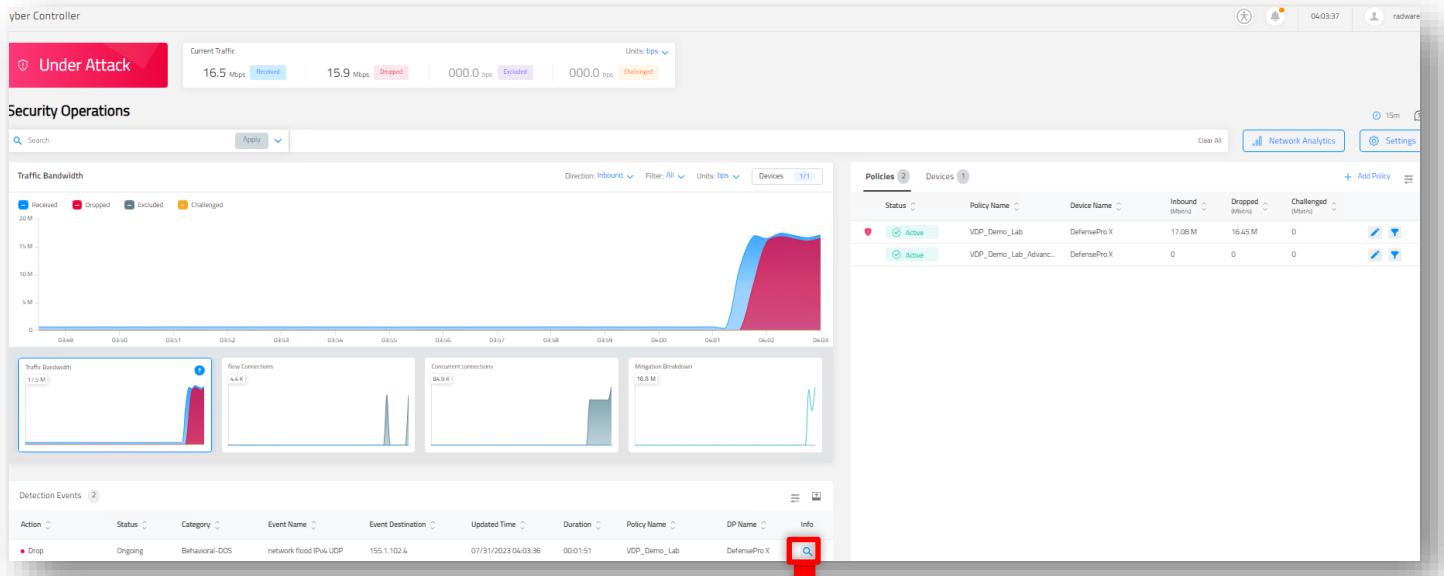
```

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**:

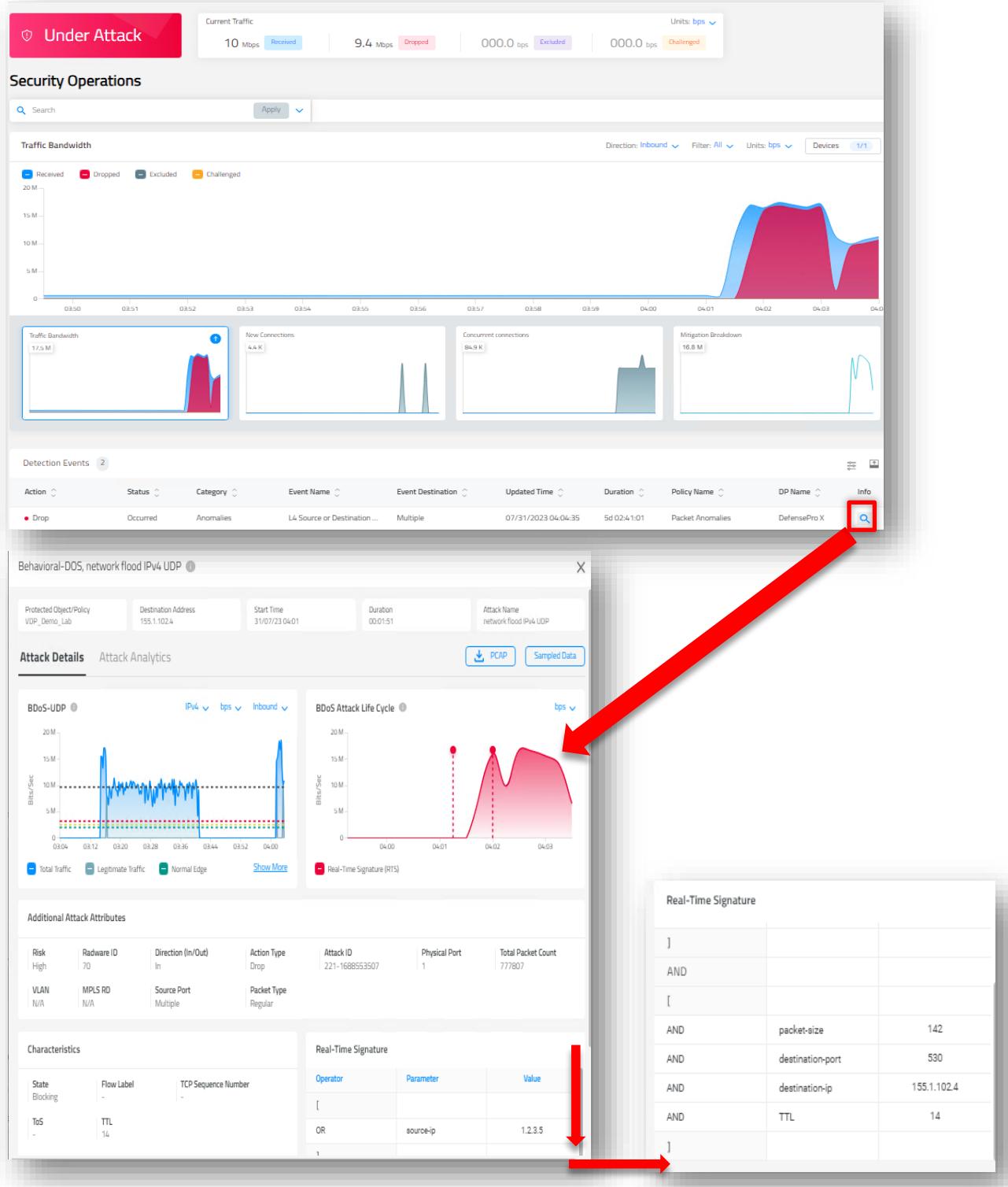


2. Verify the signature which DefensePro X generates for the first attack vectors:

Operator	Parameter	Value
[
OR	source-ip	1.2.3.4
]		
AND		
[
AND	packet-size	242
AND	destination-port	123
]		

 A red arrow points from the end of this table to the right edge of the interface.
 " data-bbox="68 525 932 865"/>

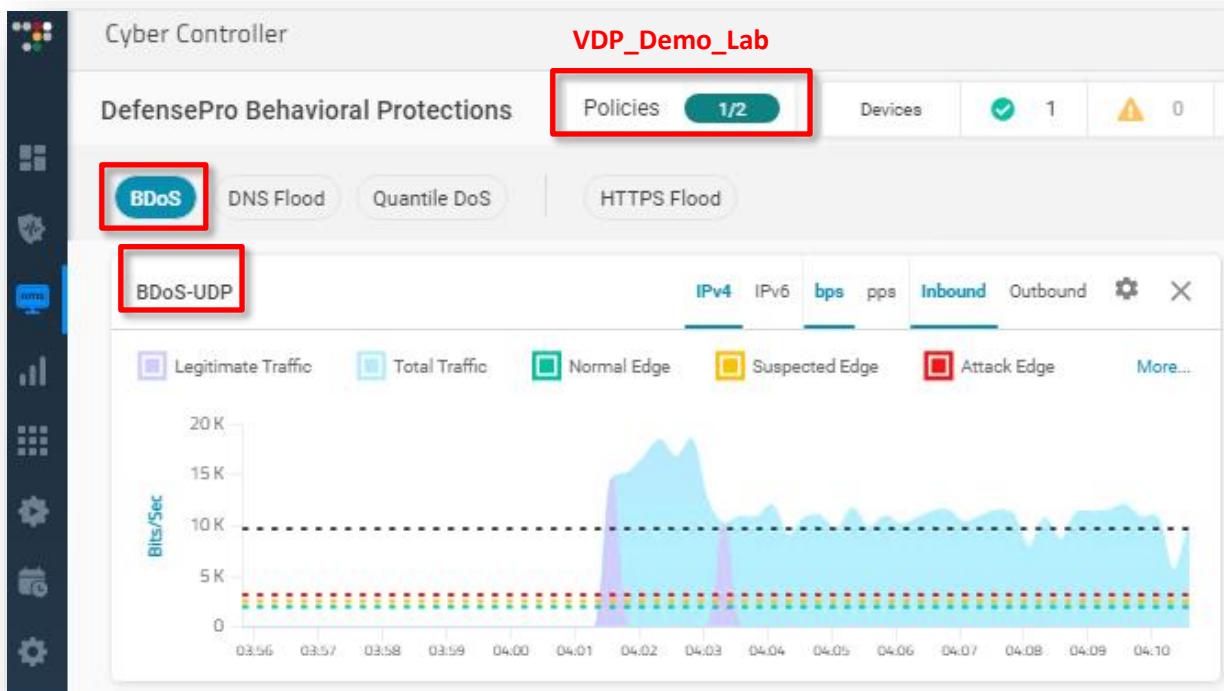
3. Verify the signature which DefensePro X generates for the second attack vectors:



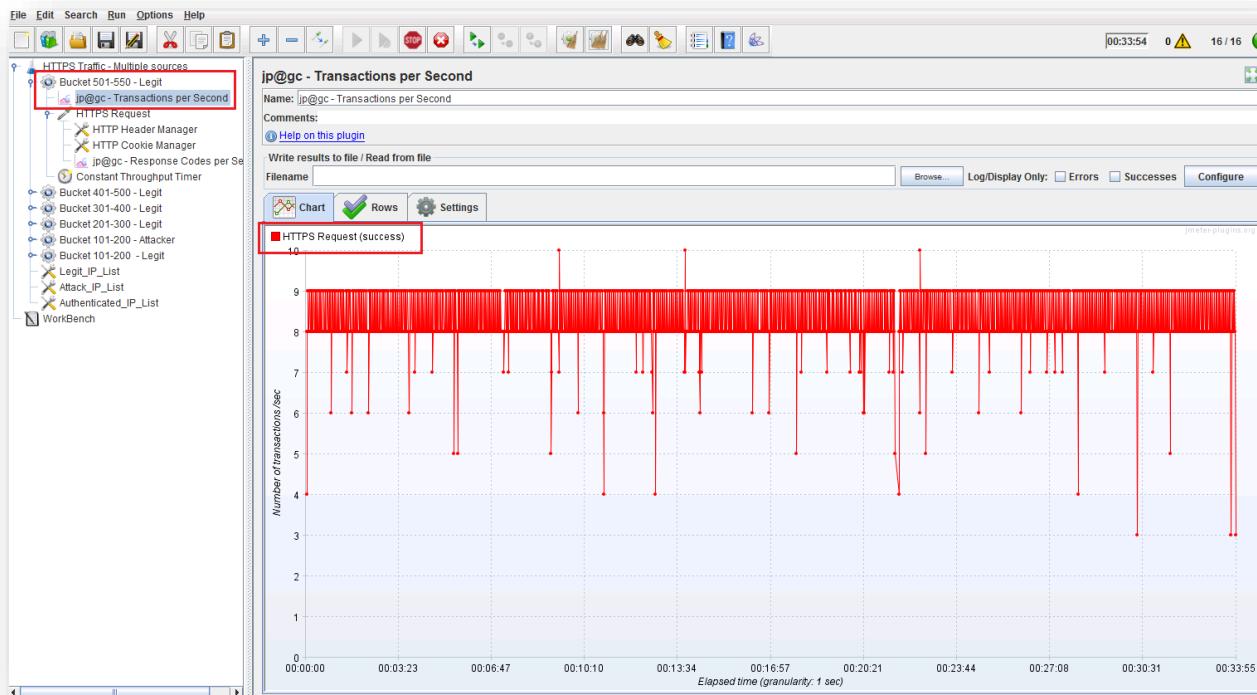
The screenshot shows the DefensePro X Security Operations interface. At the top, a pink banner indicates "Under Attack" with current traffic statistics: 10 Mbps Received, 9.4 Mbps Dropped, 000.0 bps Excluded, and 000.0 bps Challenged. Below this is a "Traffic Bandwidth" chart showing a sharp increase in traffic around 04:01. The "Detection Events" table shows a single entry for a "Drop" event, with a red box highlighting the search icon. A modal window for a "Behavioral-DOS, network flood IPv4 UDP" attack is open, displaying "Attack Details" and "Attack Analytics" tabs. The "Attack Analytics" tab shows two charts: "BDoS-UDP" and "BDoS Attack Life Cycle". A red arrow points from the search icon in the "Attack Details" table to the "Real-Time Signature" table on the right. The "Real-Time Signature" table lists the generated signature rules:

Operator	Parameter	Value
[
OR	source-ip	1.2.3.5
1		
AND	packet-size	142
AND	destination-port	530
AND	destination-ip	155.1.102.4
AND	TTL	14
]		

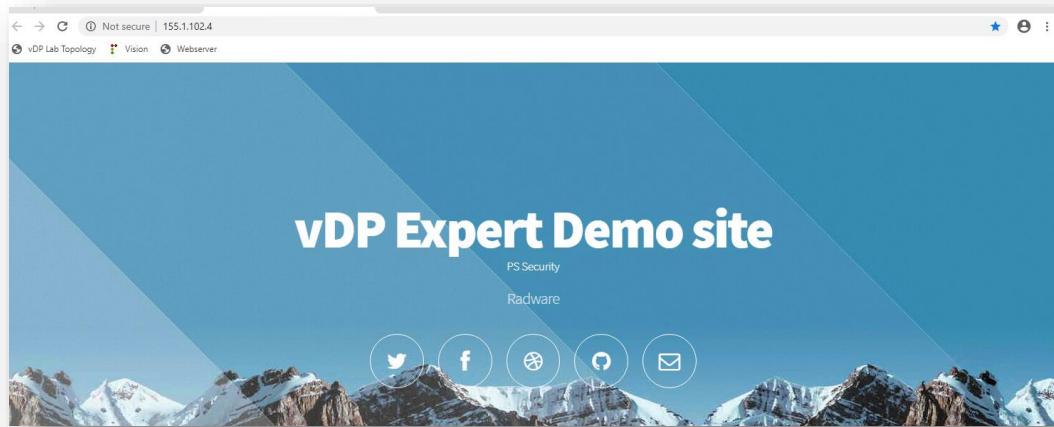
2. Check the current baselines of each BDoS controller in the **AMS > DefensePro Behavioral Protections** dashboard:



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



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



BDoS Advanced UDP Protection

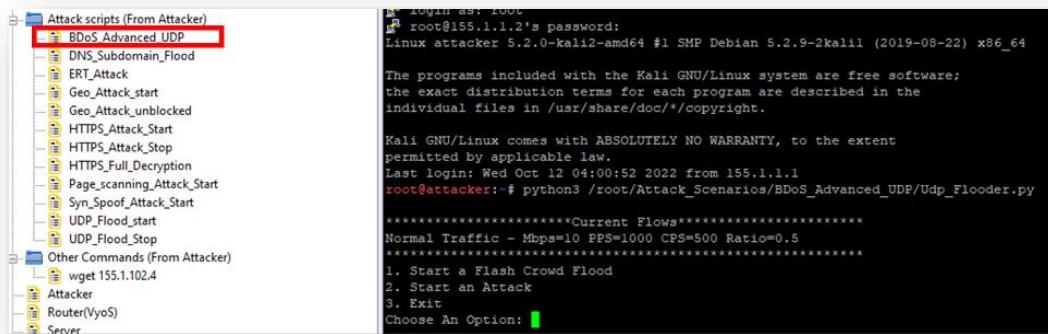
For more additional information about this scenario, please refer to the ["Appendix 6 - BDoS Advanced Protection \(Additional Info\)"](#) section.

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.



```

[+] Attack scripts (From Attacker)
  [+] BDoS_Advanced_UDP
    DNS_Subdomain_Flood
    ERT_Attack
    Geo_Attack_start
    Geo_Attack_unblocked
    HTTPS_Attack_Start
    HTTPS_Attack_Stop
    HTTPS_Full_Decryption
    Page_scanning_Attack_Start
    Syn_Spoof_Attack_Start
    UDP_Flood_Start
    UDP_Flood_Stop
  [+] Other Commands (From Attacker)
    wget 155.1.102.4
  Attacker
  Router(VyOS)
  Server

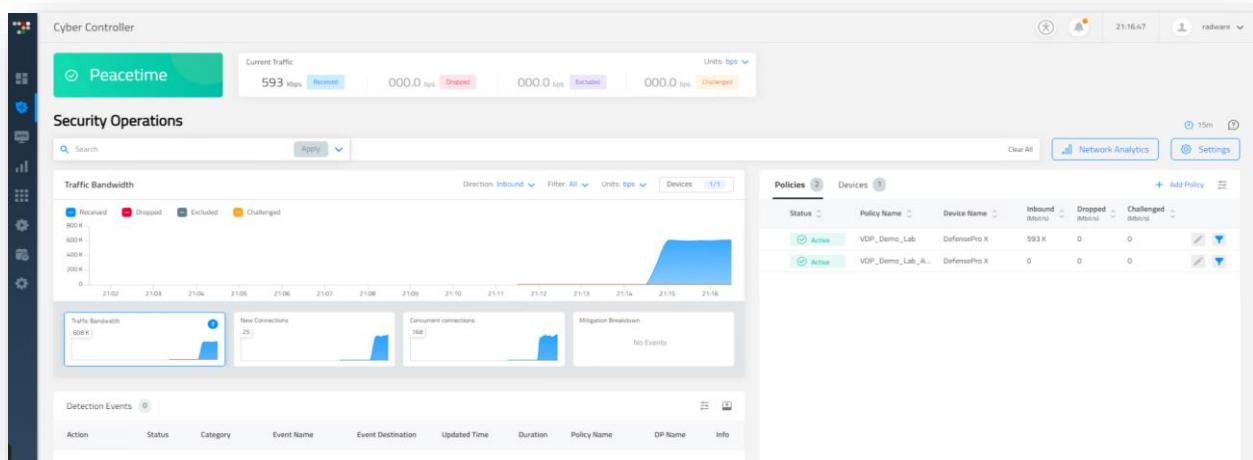
[+] root@155.1.1.2:~# root@155.1.1.2's password:
Linux attacker 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 12 04:00:52 2022 from 155.1.1.1
root@attacker:~# python3 /root/Attack_Scenarios/BDoS_Advanced_UDP/Udp_Flood.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: [green bar]

```

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

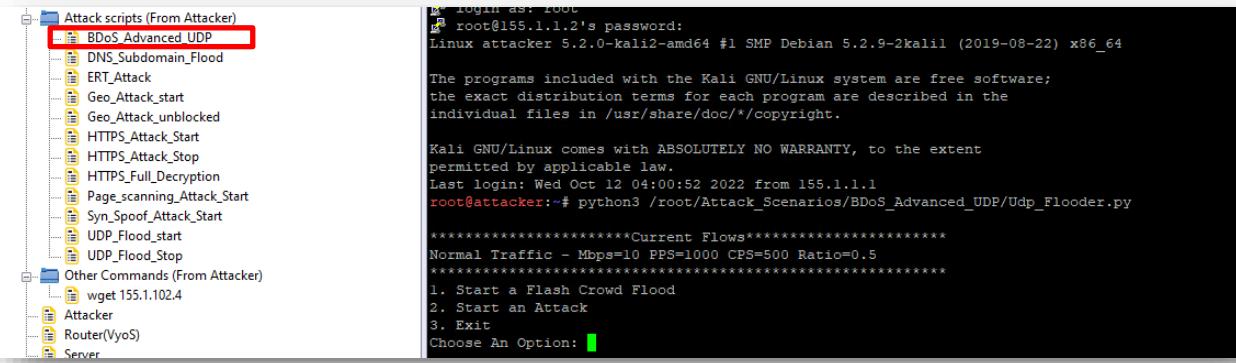


Start a UDP Flood Attack

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.

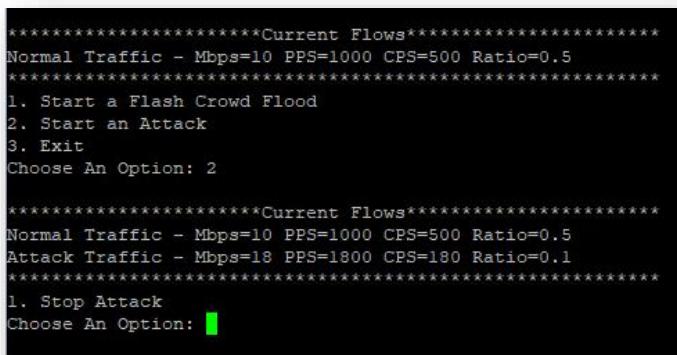
Press **2**, in order to activate UDP Flood attack.



The script runs two different flows.

1. Normal Traffic
2. UDP Flood Attack

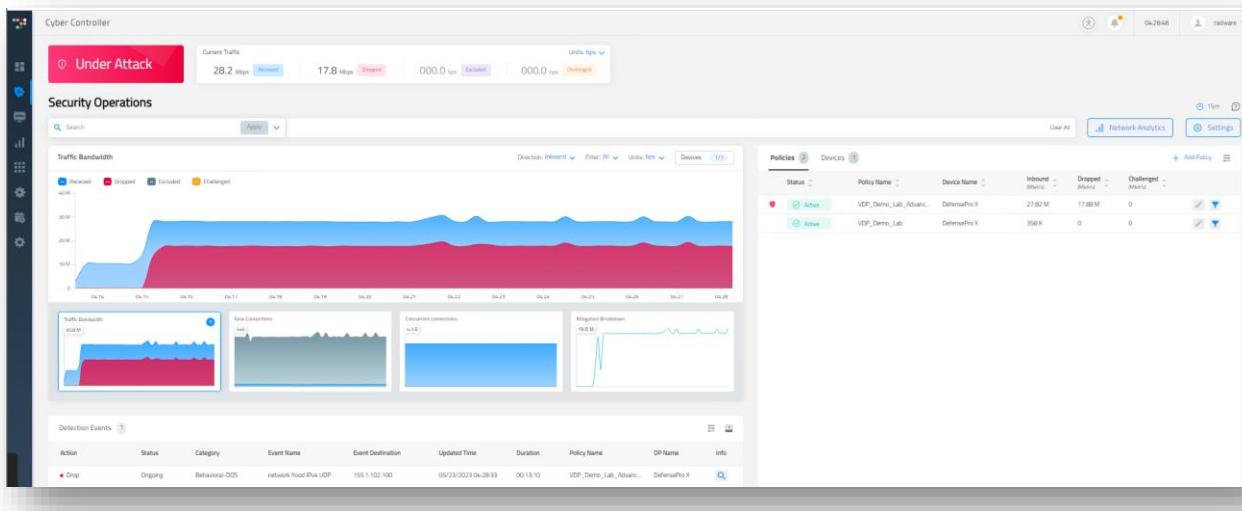
While the script is running, the following screen displays:



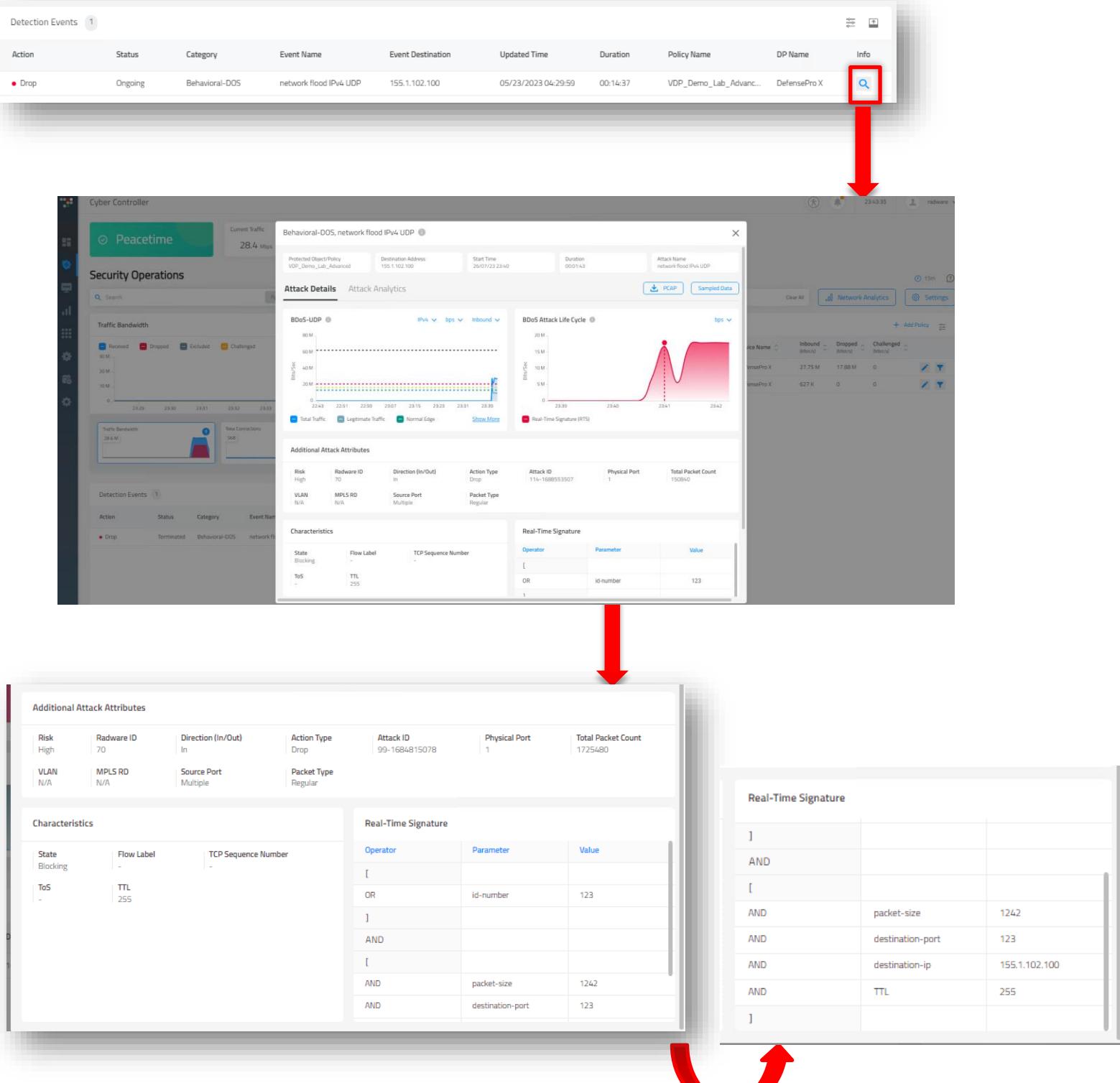
2. In order to **stop** the attack traffic, press **1**.

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:



Attack Details and Real-Time Signature

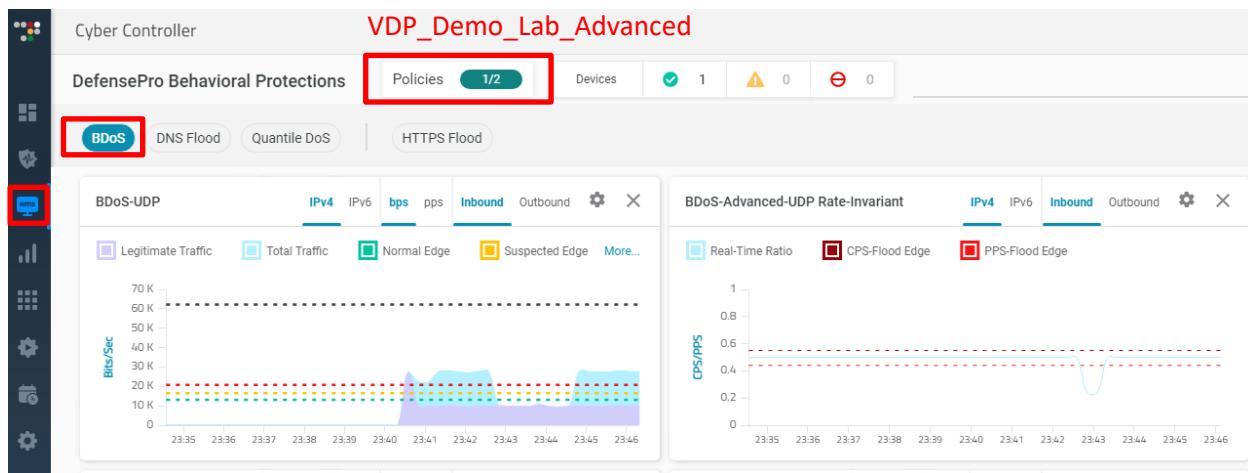
Attack Details:

- 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

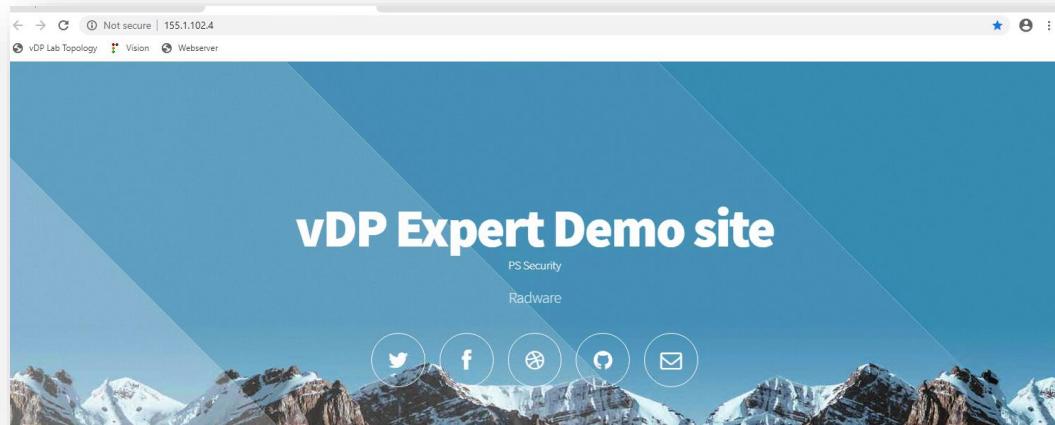
Real-Time Signature:

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

3. Verify the BDoS UDP graph on the **AMS > DefensePro Behavioral Protections** (choose the **VDP_Demo_Lab_Advanced** policy):



4. 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 Crowed 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-Crowed traffic.

The script runs two different flows.

1. Normal Traffic
2. Flash-Crowed traffic.

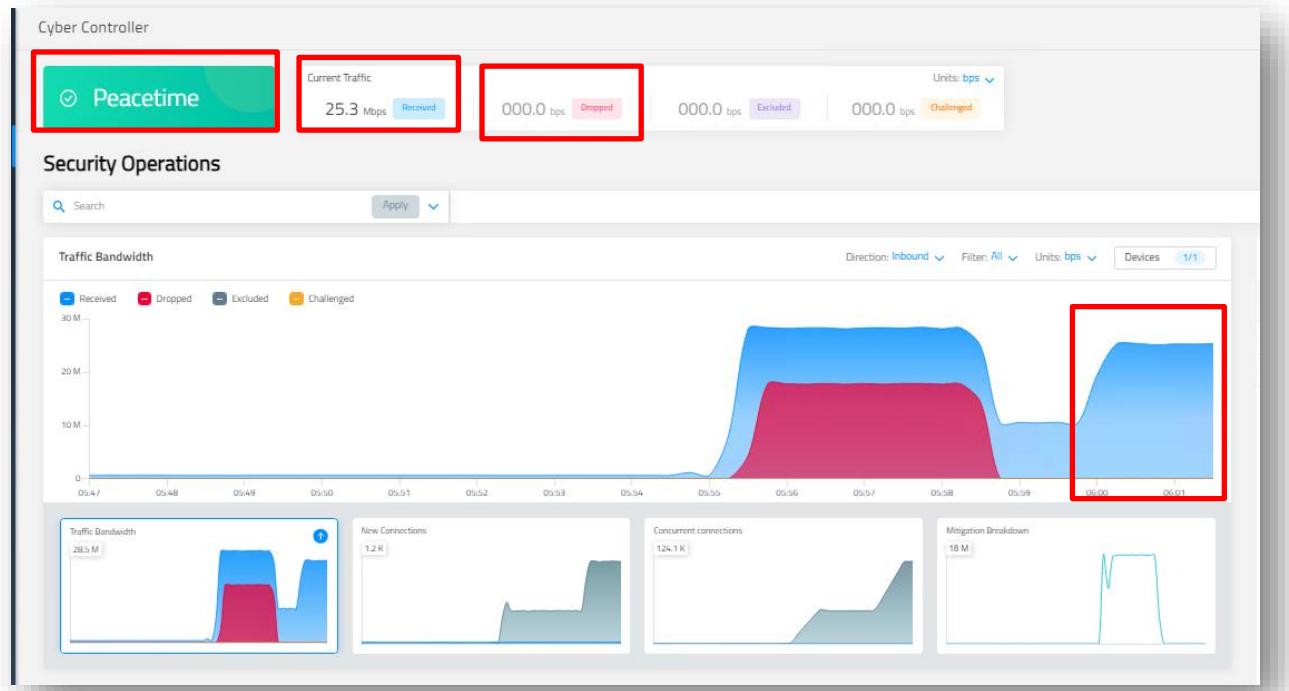
```
*****Current Flows*****
Normal Traffic - Mbps=10 PPS=1000 CPS=500 Ratio=0.5
*****
1. Start a Flash Crowd Flood
2. Start an Attack
3. Exit
Choose An Option: 1

*****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
```

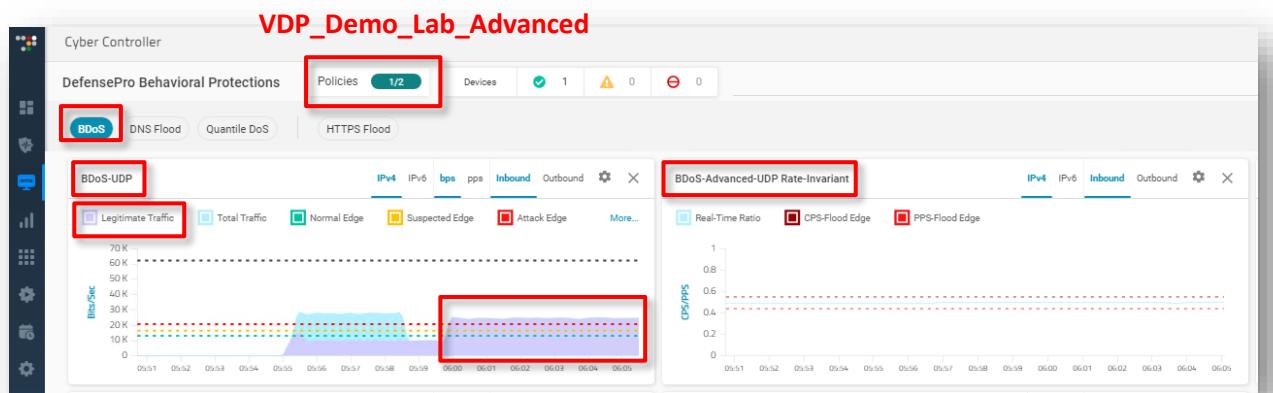
2. In order to **stop** the Flash-Crowed traffic, press **1**.

Verify Flash Crowd Isn't Getting Blocked

- 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:



- Verify the BDoS UDP graph on the **AMS > DefensePro Behavioral Protections** (choose the **VDP_Demo_Lab_Advanced** policy):



DNS Flood Protection

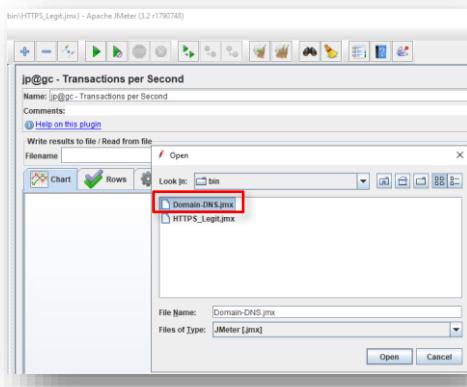
For more additional information about this scenario, please refer to the "[Appendix 7 - DNS Flood Protection \(Additional Info\)](#)" section.

Start DNS Legitimate Traffic

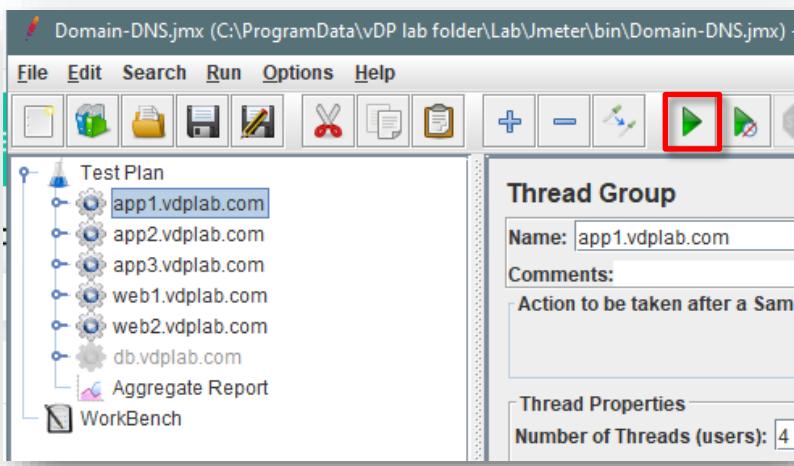
Before start this scenario, you need first to stop the HTTPS legitimate traffic (running two JMetrics on parallel, can cause issue with resources of the nested ESXi of the demo lab).

1. Open the DNS legitimate traffic on the JMeter:

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



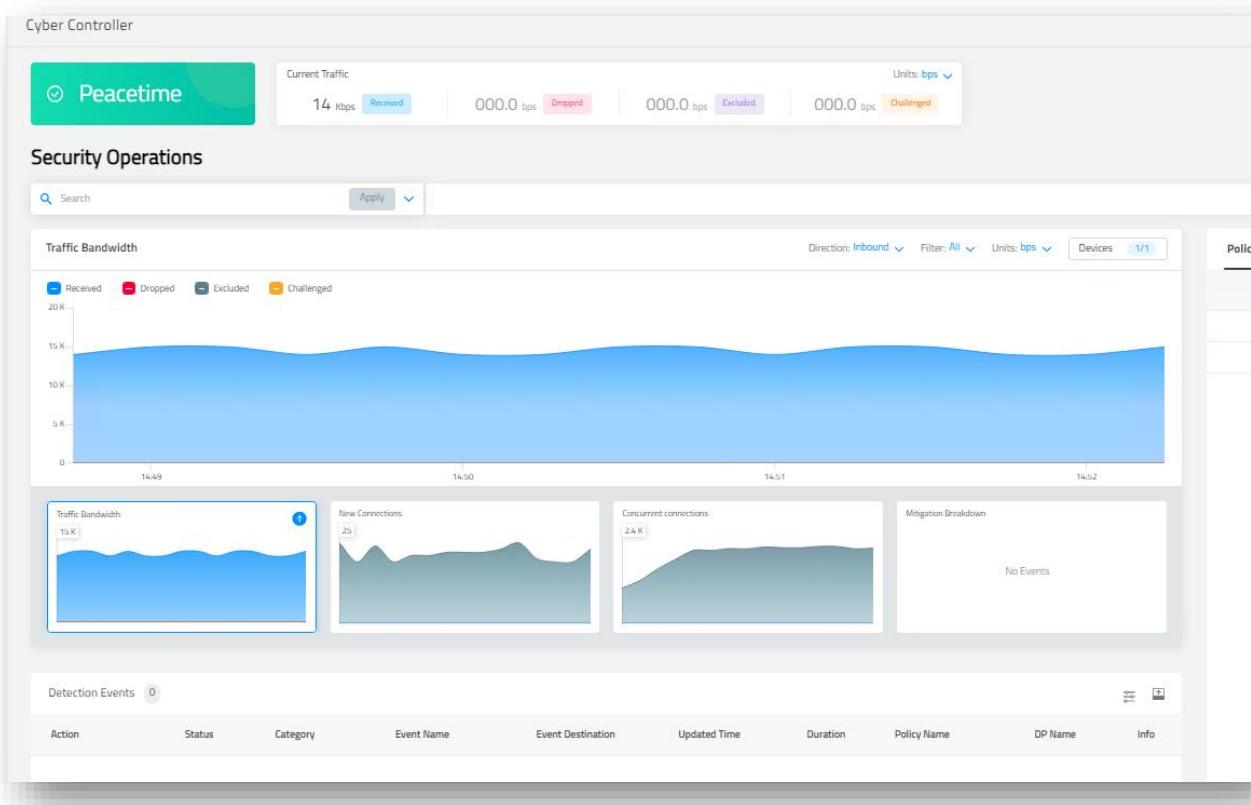
2. Press start.



3. Verify the legitimate queries response code:



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

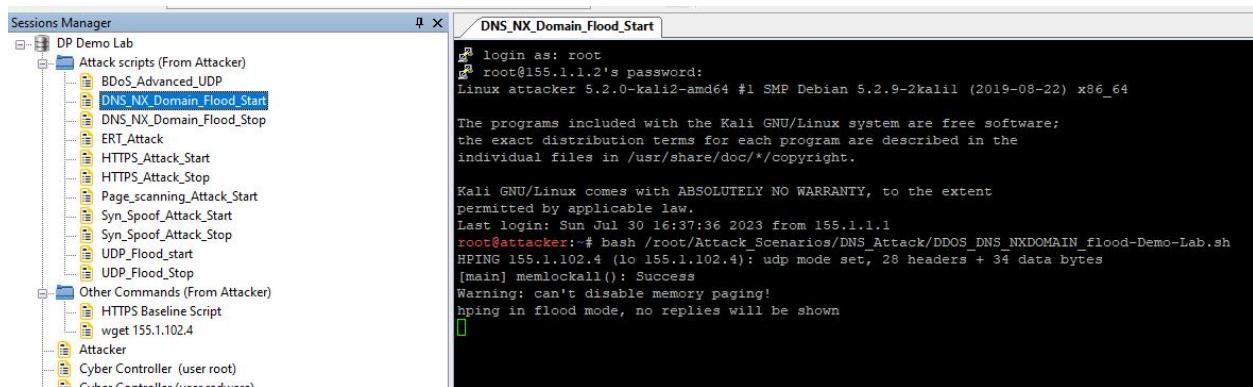


Start a DNS NX Domain Flood Attack and Verify Detection

- 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:



```

Sessions Manager
DP Demo Lab
  Attack scripts (From Attacker)
    BDOS_Advanced_UDP
    DNS_NX_Domain_Flood_Start
    DNS_NX_Domain_Flood_Stop
    ERT_Attack
    HTTPS_Attack_Start
    HTTPS_Attack_Stop
    Page_scanning_Attack_Start
    Syn_Spoof_Attack_Start
    Syn_Spoof_Attack_Stop
    UDP_Flood_Start
    UDP_Flood_Stop
  Other Commands (From Attacker)
    HTTPS Baseline Script
    wget 155.1.102.4
  Attacker
  Cyber Controller (user root)
    Cyber Controller (user root)

```

DNS_NX_Domain_Flood_Start

```

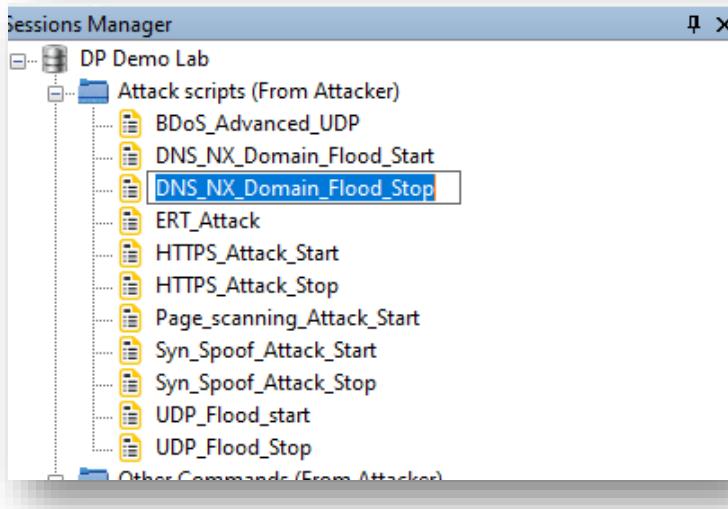
login as: root
root@155.1.1.2's password:
Linux attacker 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64

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 30 16:37:36 2023 from 155.1.1.1
root@attacker:~# bash /root/Attack_Scenarios/DNS_Attack/DDOS_DNS_NXDOMAIN_flood-Demo-Lab.sh
HPING 155.1.102.4 (to 155.1.102.4): udp mode set, 28 headers + 34 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
hpPing in flood mode, no replies will be shown

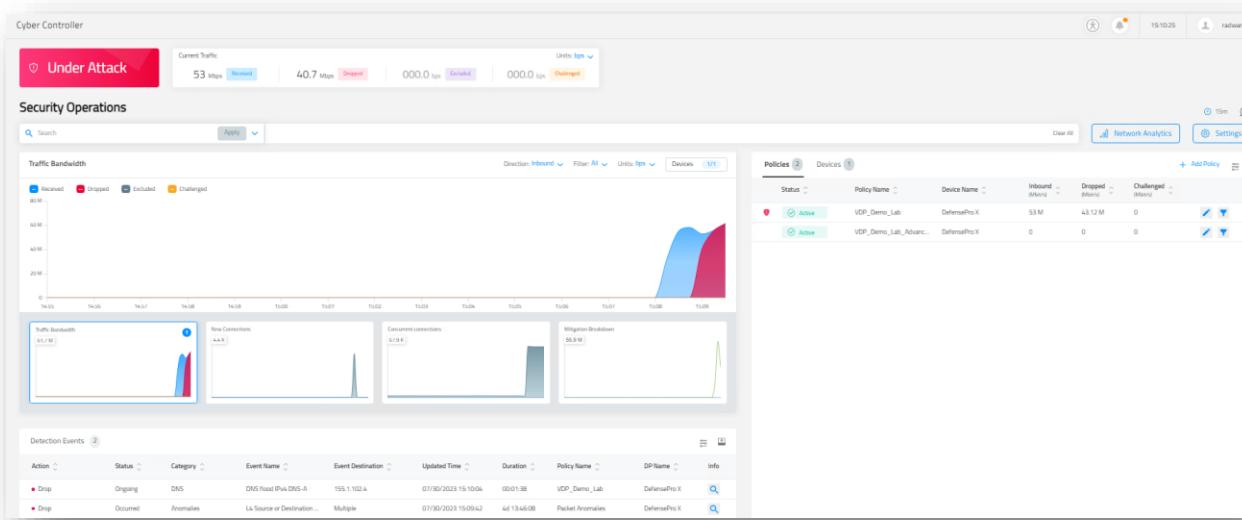
```

- In order to **stop** the attack, double-click on **DNS_NX_Domain_Flood_Stop**.

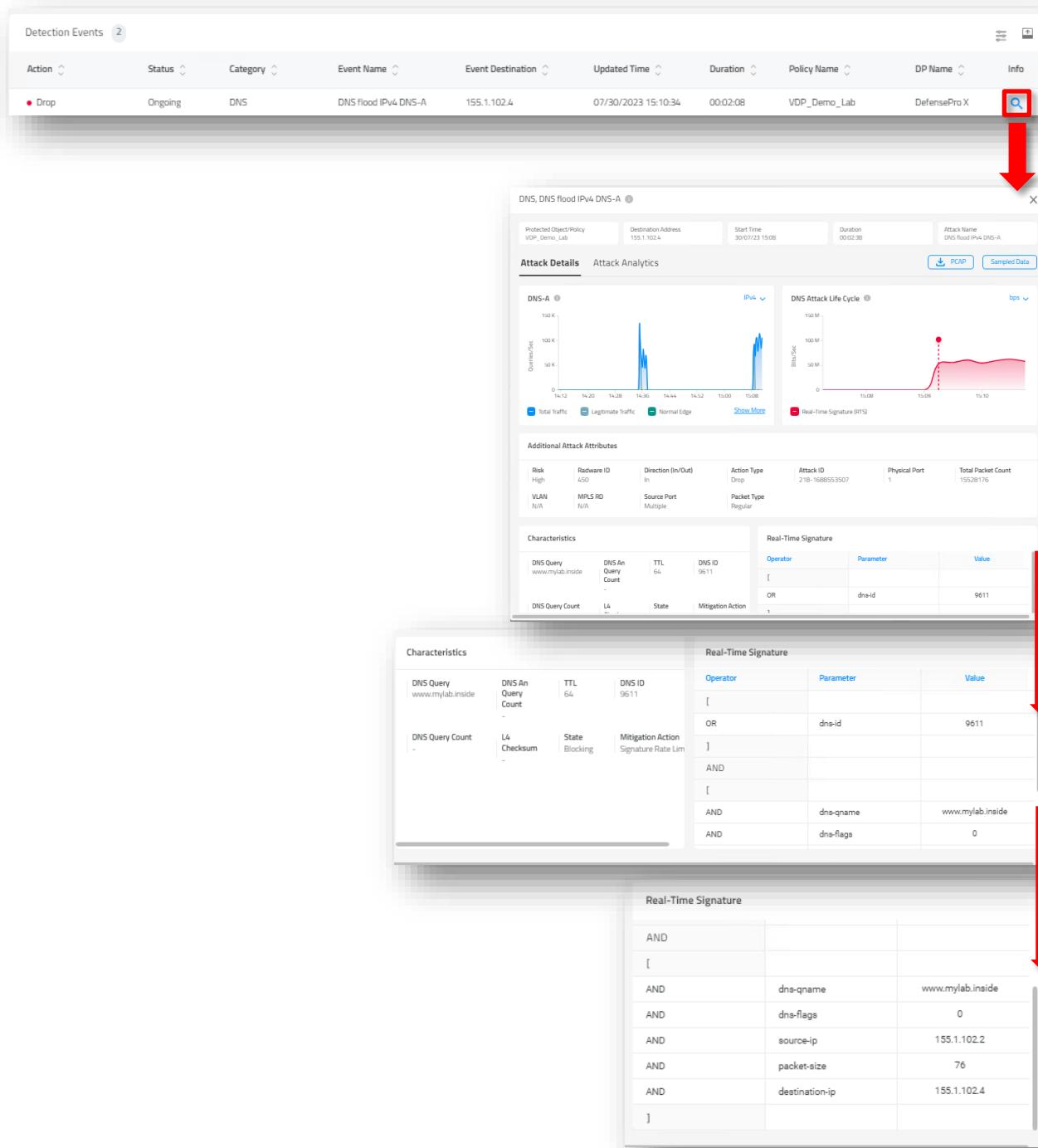


Attack Mitigation

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



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:



The screenshot illustrates the DefensePro X interface for monitoring and responding to network attacks. The main window displays a list of 'Detection Events' with a single entry highlighted: 'Drop' status, 'DNS' category, 'Event Name' 'DNS flood IPv4 DNS-A', 'Event Destination' '155.1.102.4', 'Updated Time' '07/30/2023 15:10:34', 'Duration' '00:02:08', 'Policy Name' 'VDP_Demo_Lab', 'DP Name' 'DefensePro X'. A magnifying glass icon is overlaid on the 'Info' column for this event, with a red arrow pointing to it from the top right.

Clicking the magnifying glass icon opens a detailed analysis window for the 'DNS-A' attack. This window includes:

- Attack Details:** Shows a timeline of DNS traffic (OverheadSec) from 14:12 to 15:08, with a sharp peak around 14:35. It also displays the 'DNS Attack Life Cycle' (bps) from 10:08 to 15:10, showing a significant increase in traffic volume.
- Additional Attack Attributes:** Lists the following parameters:

Risk: High	Radware ID: 450	Direction (In/Out): In	Action Type: Drop
VLAN: N/A	MPLS RD: N/A	Source Port: Multiple	Packet Type: Regular
- Characteristics:** Shows DNS query details for 'www.my.lab.inside' with a TTL of 64 and a DNS ID of 9611. It also lists 'DNS Query Count' and 'L4 Checksum'.
- Real-Time Signature:** Displays a table of operators, parameters, and values used for real-time detection, including 'dns-id' and '9611'.
- Characteristics:** (Reappears in the lower section) Shows DNS query details for 'www.my.lab.inside' with a TTL of 64 and a DNS ID of 9611. It also lists 'DNS Query Count' and 'L4 Checksum'.
- Real-Time Signature:** (Reappears in the lower section) Displays a table of operators, parameters, and values used for real-time detection, including 'dns-qname' and 'www.my.lab.inside'.

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



APPENDIX 1 - HTTPS PROTECTION (ADDITIONAL INFO)

Protection Overview

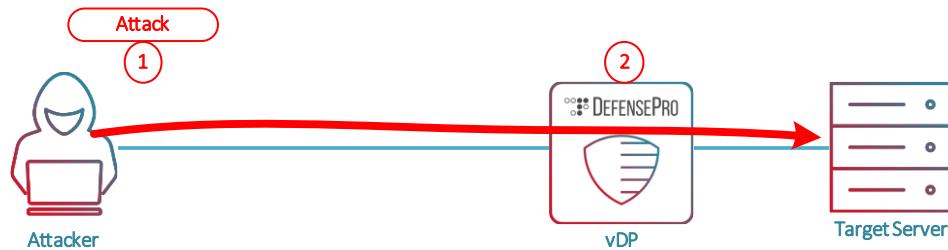
The HTTPS Flood mechanism introduced in DefensePro8 version 8.18.0.0 aims to stop denial of service (DoS) attacks on HTTPS servers by effectively blocking malicious traffic towards an attacked server.

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.

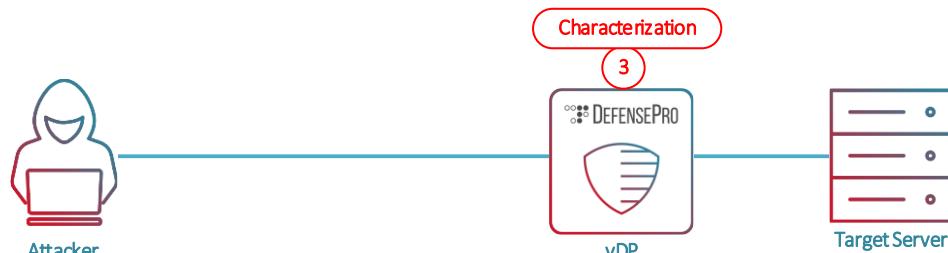
Inbound request rate learning is based on the rate of packets with an SSL record header of Content type: "Application Data (23)"

Scenario Steps Overview

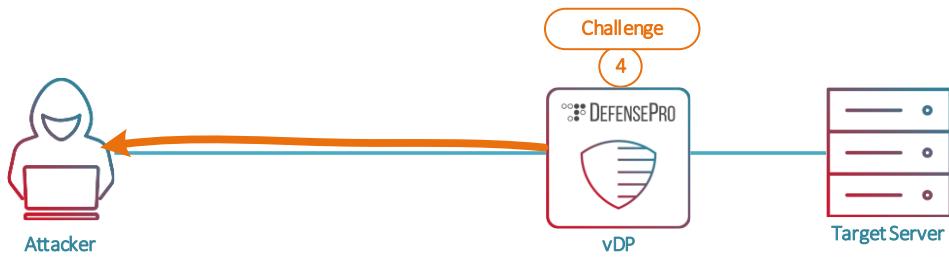
1. The attacker generates HTTPS Flood traffic from different sources towards the Webserver.
2. Detection on DefensePro begins:



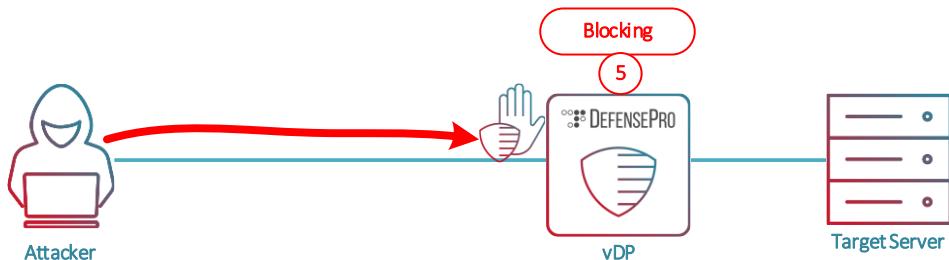
3. The attacker traffic rate goes above the Attack Edge baselines. The Detection phase begins HTTPS protection and enters the characterization stage:



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.

Keyless Mitigation
Rate-Limit Traffic from Suspect Sources Limit
100 Packets per Second per Source

First Request Mitigation on All Sources
Use HTTPS Authentication on All Sources

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

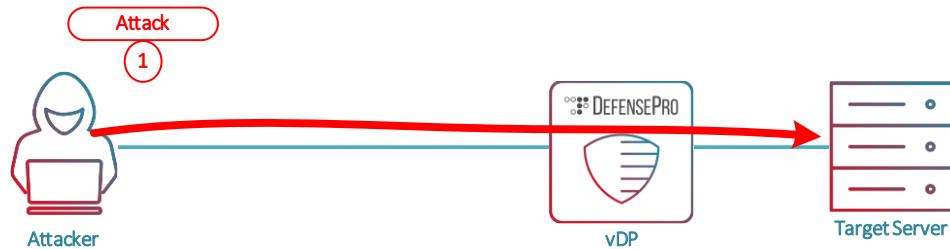
Traffic filter mitigation is performed by using a rate limit for the attacker traffic (in PPS, by default)

Some of the advantages of this protection are:

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

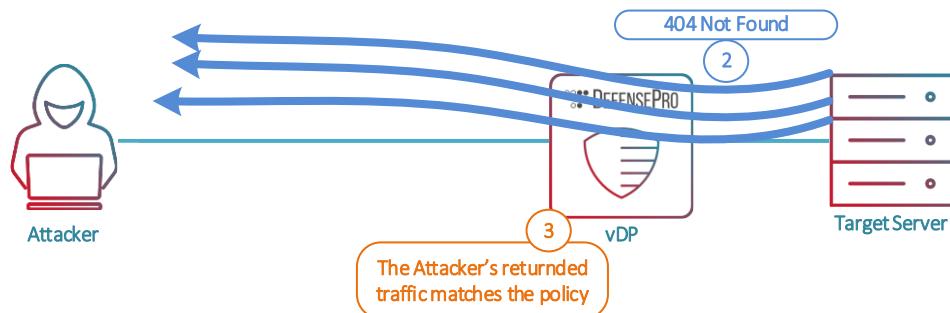
Scenario Steps Overview

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

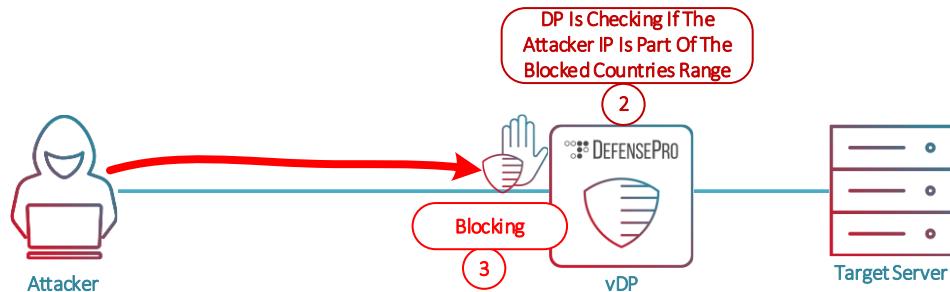


2. The Webserver responds with **404 page not found**.

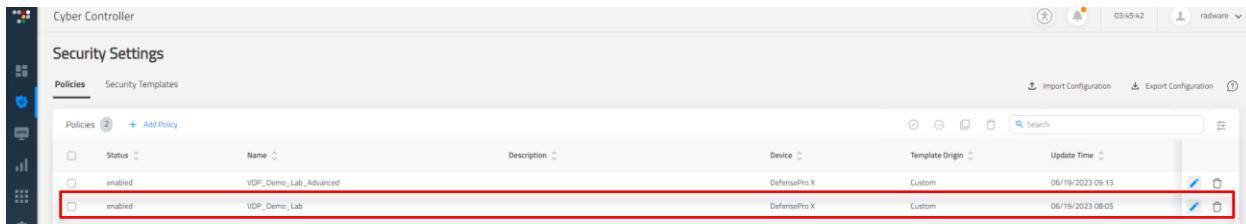
3. The attacker's return traffic matches the configured traffic-filter profile (matches all returning traffic which includes a 404 error code):



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

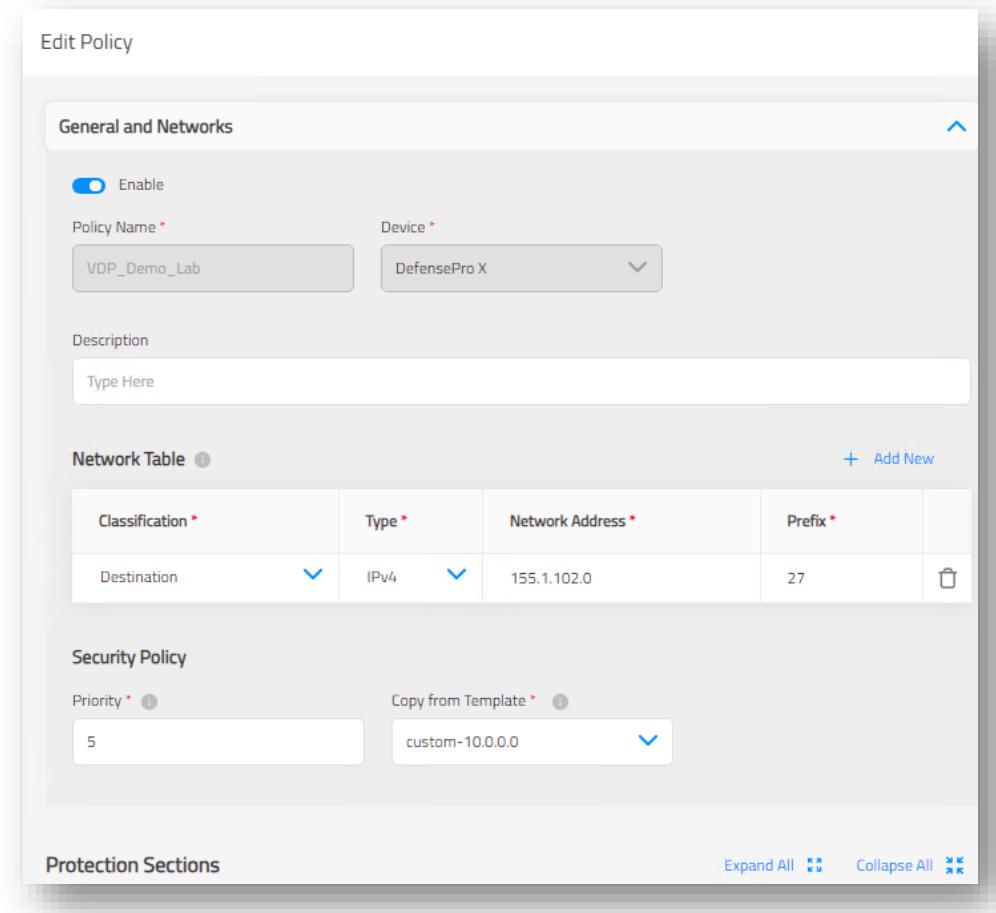


Configurations



Policies

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



General and Networks

Enable

Policy Name *: VDP_Demo_Lab

Device *: DefensePro X

Description: Type Here

Network Table

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	Edit Delete

Cancel Submit

Edit Traffic Filters List X

Filter Threshold

Filter Name * Apply Traffic Filter To ▼

Basic Filter

Source Network <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="As in Policy"/> ▼	Destination Network <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="As in Policy"/> ▼	Protocol <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="TCP"/> ▼
Other Protocol Number(s) <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="Type Here"/>	Source Port <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="Any"/> ▼	Destination Port <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="http"/> ▼
Packet Size (Bytes) <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="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) <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="Type Here"/>	TCP Sequence Number <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="Type Here"/>	Context Tag <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="Any"/>
Type of Service (ToS) - DSCP <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value="Type Here"/>	Fragment Offset <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value=""/>	Fragment ID <input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; padding: 2px 10px;" type="text" value=""/>

Regular Expression

Cancel Submit

Add Traffic Filters List

X

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

404

Filter Action

Threshold Units

Packet Per Second

Threshold *

5

Tracking Mode

Returning Traffic From De...

IPv4 Source Prefix Length

32

IPv6 Source Prefix Length

128

IPv4 Destination Prefix Length

32

IPv6 Destination Prefix Length

128

Packet Reporting

Cancel
Submit

DefensePro X v1.5.1 Demo Lab Guide Page 76

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

Protection Overview

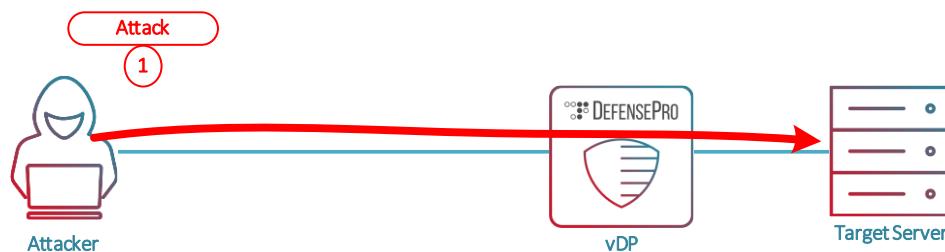
The ERT Attacker feed provides protection against well-known attackers' IP addresses that were recently actively involved in a DDoS attack.

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

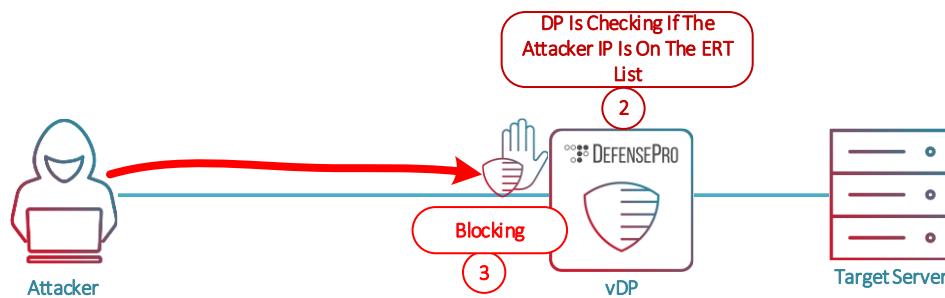
The ERT Active Attackers Feed focuses on unique, real-time intelligence against emerging DDoS-specific threats including evolving IoT botnets and new DNS attack vectors.

Scenario Steps Overview

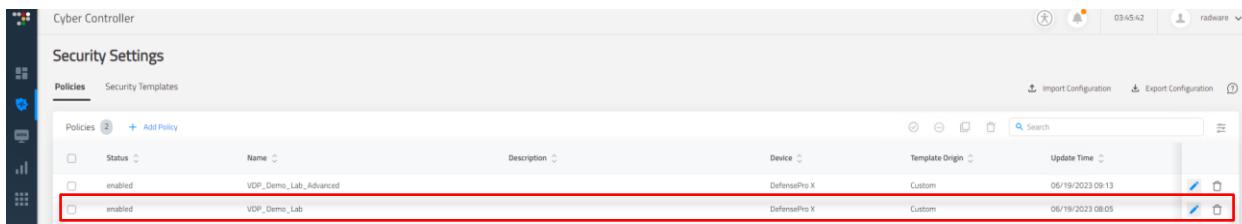
1. An attacker with a malicious IP address (located on the ERT list) begins a UDP flood attack towards the Webserver.



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



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:

Device:

Description:

Network Table (1 item) [+ Add New](#)

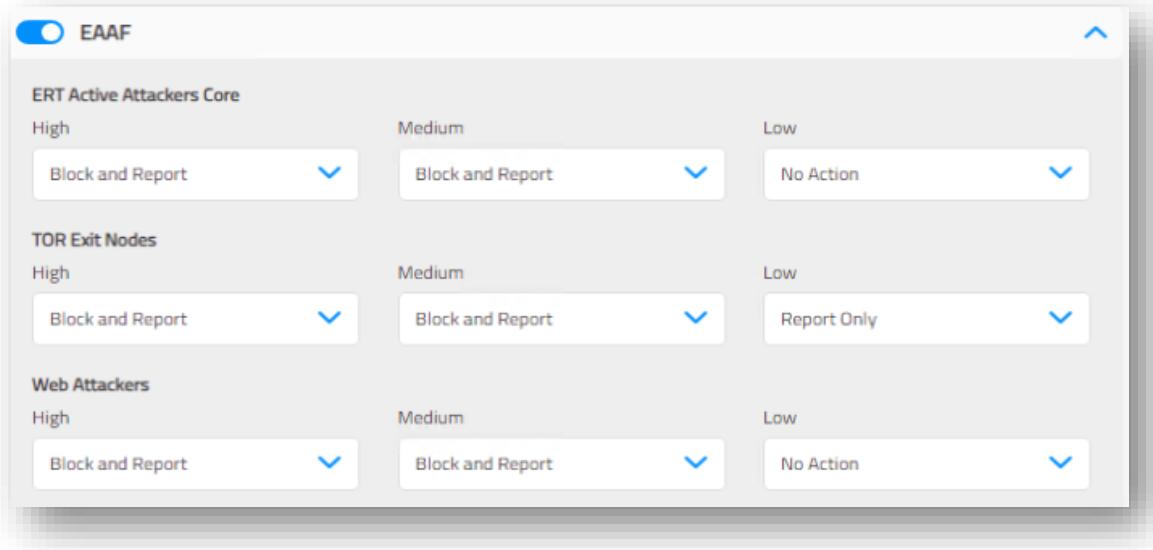
Classification *	Type *	Network Address *	Prefix *	
Destination	IPv4	155.1.102.0	27	

Security Policy

Priority:

Copy from Template:

Protection Sections [Expand All](#) [Collapse All](#)


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/appData/EaaffFeed/EaaffFeed-imp

APPENDIX 4 - SPOOFED SYN ATTACK PROTECTION (ADDITIONAL INFO)

Protection Overview

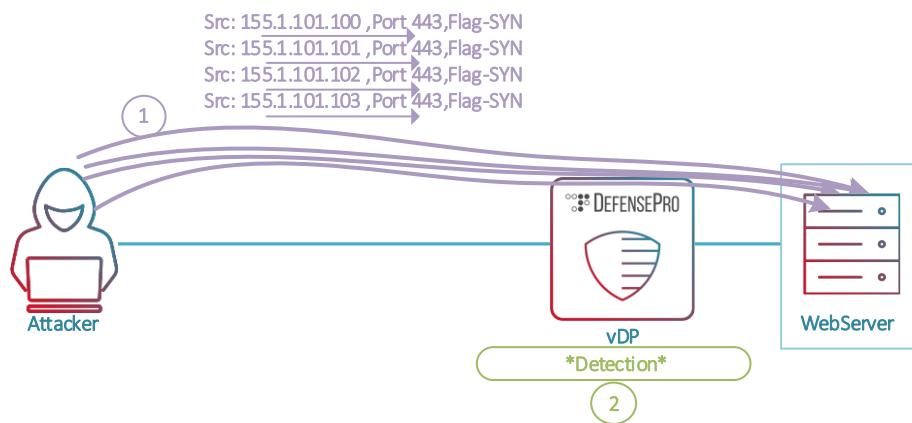
Spoofed SYN Attack protection is a new feature which allows mitigation of spoofed syn attacks targeting a wide range of IP's from the customer network.

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.

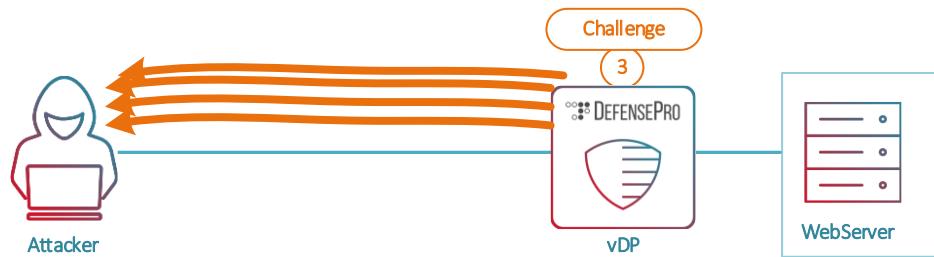
By using this kind of tracking technique, attacks like carpet bomb and others can be mitigated easily by DefensePro X.

Scenario Steps Overview

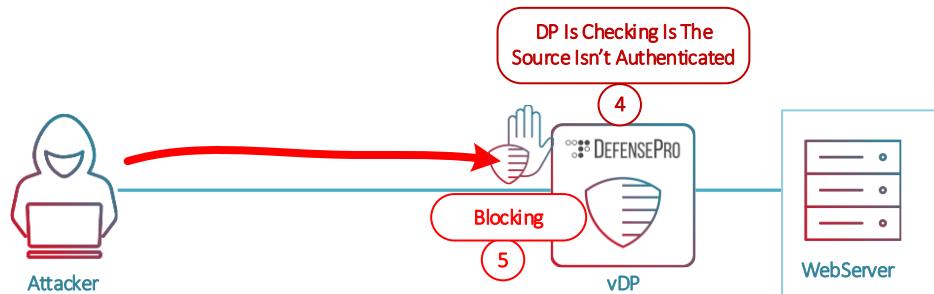
1. The attacker generates SYN flood attack using hping3 tool from different sources towards a web server.
2. Detection on DefensePro begins:



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

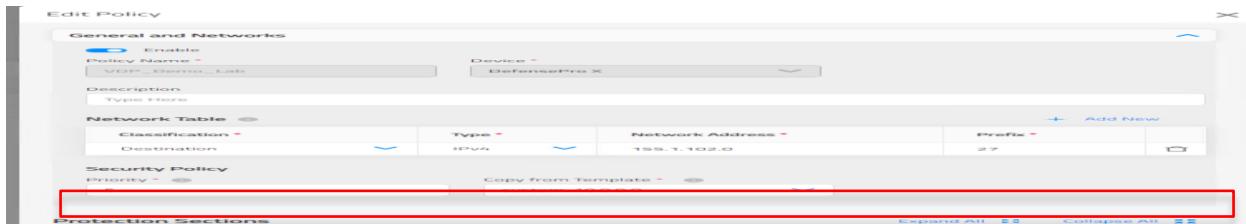


4. Every traffic from sources which didn't pass the challenge will be blocked by DefensePro X.



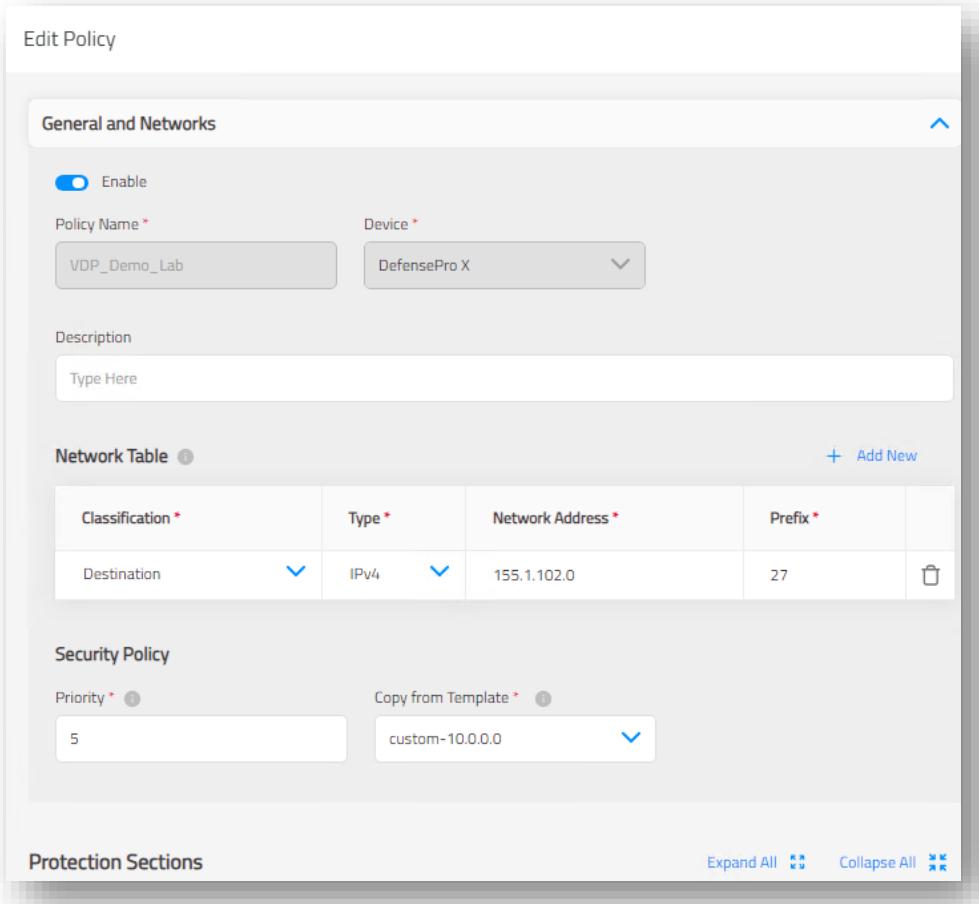
Configurations

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:



The screenshot shows the 'Edit Policy' interface for DefensePro X. The configuration includes:

- General and Networks:** Policy Name: VDP_Demo_Lab, Device: DefensePro X.
- Network Table:** A single entry for Destination 155.1.102.0, Type IPv4, Network Address 155.1.102.0, and Prefix 27.
- Security Policy:** Priority: 5, Copy from Template: custom-10.0.0.0.
- Protection Sections:** This section is highlighted with a red box.



The screenshot shows the 'Edit Policy' interface for DefensePro X. The configuration includes:

- General and Networks:** Policy Name: VDP_Demo_Lab, Device: DefensePro X.
- Network Table:** A single entry for Destination 155.1.102.0, Type IPv4, Network Address 155.1.102.0, and Prefix 27.
- Security Policy:** Priority: 5, Copy from Template: custom-10.0.0.0.
- Protection Sections:** This section is visible at the bottom of the configuration screen.

SYN Flood Protection

Action
Block and Report

Protection Table

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 Protection

Destination Ports
Traffic Matching Destination ...

Activation Mode
Threshold Based

Activation Threshold 50

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
Safe Reset

Application Level Authentication

Use HTTP Authentication Use HTTPS Authentication

HTTP Authentication Method
302-Redirect

Cancel **Submit**

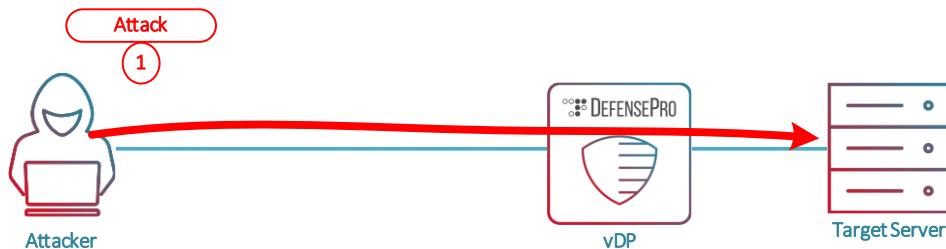
APPENDIX 5 - BDOS PROTECTION (ADDITIONAL INFO)

Protection Overview

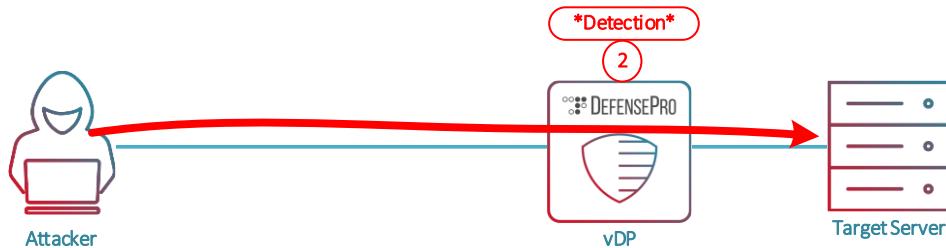
The BDOS module provides a behavior-based DoS protection that meets the detection and prevention challenge raised by the most sophisticated DDoS attack methods. Through an adaptive behavioral approach, based on analysis methods such as an adaptive Fuzzy Logic decision engine, probability theory and Closed-Feedback 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.

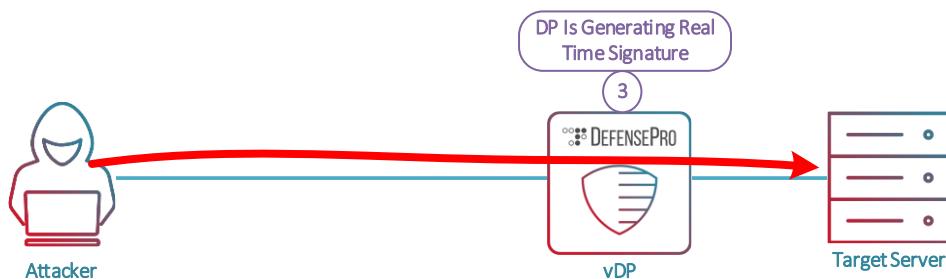


2. DefensePro checks if the UDP rate is above the attack edge baseline and begins the detection phase.

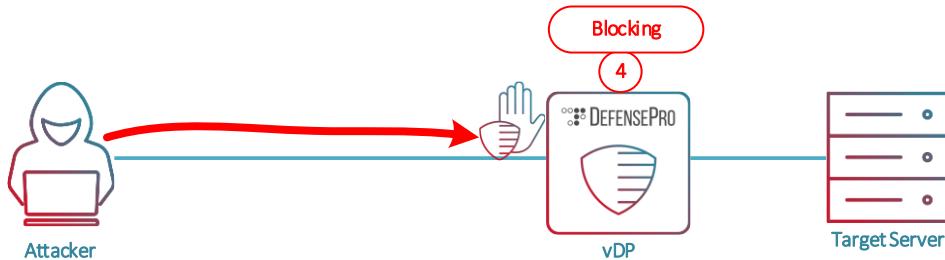


3. DefensePro generates a real time signature which will be used to mitigate the UDP Flood.

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:

Network Table 

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

Security Policy

Priority: Copy from Template:

Protection Sections  

Edit Policy

General and Networks

Enable: Policy Name: Device:

Description:

Network Table 

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

Security Policy

Priority: Copy from Template:

Protection Sections  

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 *	UDP *	Fragmented UDP *	ICMP *	IGMP *
75	50	25	9	9

Outbound (%)

TCP *	UDP *	Fragmented UDP *	ICMP *	IGMP *
75	50	25	9	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)

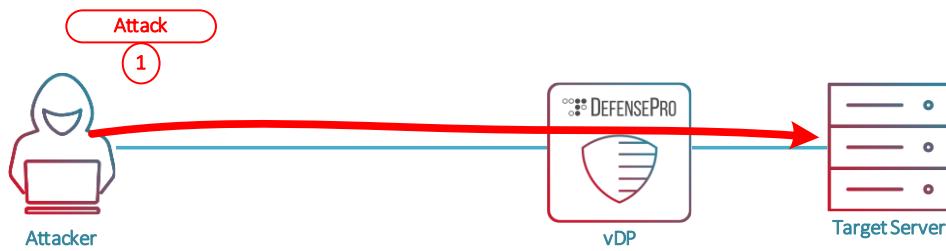
Protection Overview

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

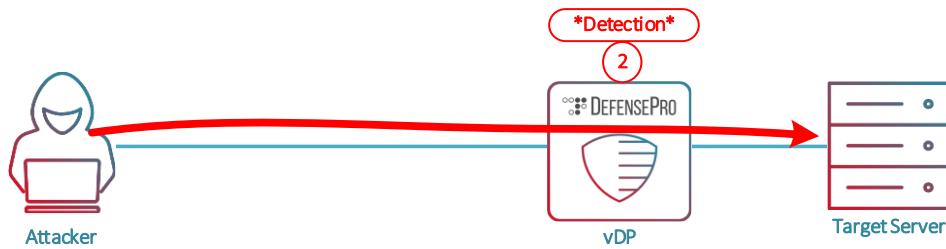
1. The Attacker begins a UDP flood attack towards the web server.



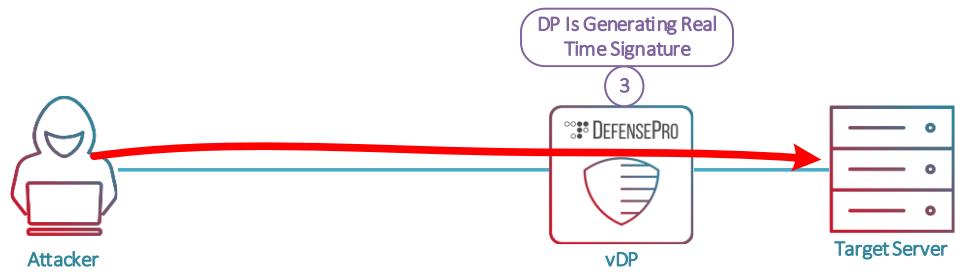
2. DefensePro checks if the UDP rate is above the Attack-Edge baseline:

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

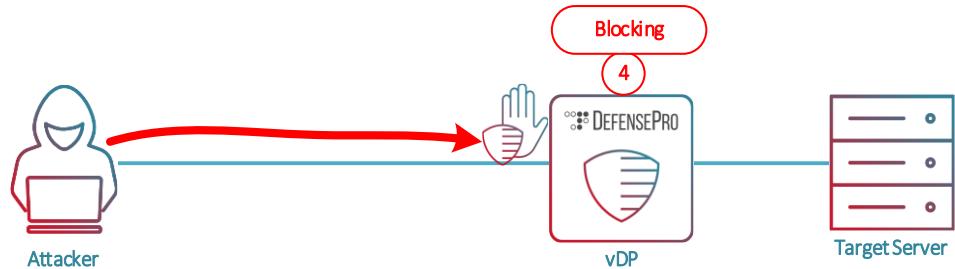
If the rate-invariant changes, DefensePro begins the Detection phase.



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** **Search**

Policy Name **Device** **Template Origin** **Update Time**

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 *** **Device ***

Description **Type Here**

Network Table **Add New**

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

Security Policy

Priority * **Copy from Template ***

Protection Sections **Expand All** **Collapse All**

General Parameters

Anti-Scan **BDoS Protection**

Cancel **Submit**

BDoS Protection

Action	Footprint Strictness
Block and Report	Medium

Bandwidth Settings

Inbound Traffic (Kbps) *	Outbound Traffic (Kbps) *
40000	40000

[Advanced Settings](#)

Advanced Settings - BDoS Protection

General

Transparent Optimization: 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	UDP Excluded Ports	Advanced UDP Detection
Medium	None	Enabled

Learning Period: Attack Edges Overrides - High Edge (%): Attack Edges Overrides - Low Edge (%):

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	80	25	3	3

UDP Settings

UDP Packet Rate Detection Sensitivity	UDP Excluded Ports	Advanced UDP Detection
Medium	None	Enabled
Learning Period	Attack Edges Overrides - High Edge (%)	Attack Edges Overrides - Low Edge (%)
Six Hrs	0	0

Burst-Attack Protection

Enable Burst-Attack Protection	Maximum Interval Between Bursts
Disabled	30

Overblocking Settings

Overblocking Prevention	Overblocking Prevention Threshold (%)
Disabled	25

Advanced

Learning Suppression Threshold (%) *	BDoS Rate Limit
0	Disable
User-Defined Rate Limit	Rate Limit Units
0	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.)

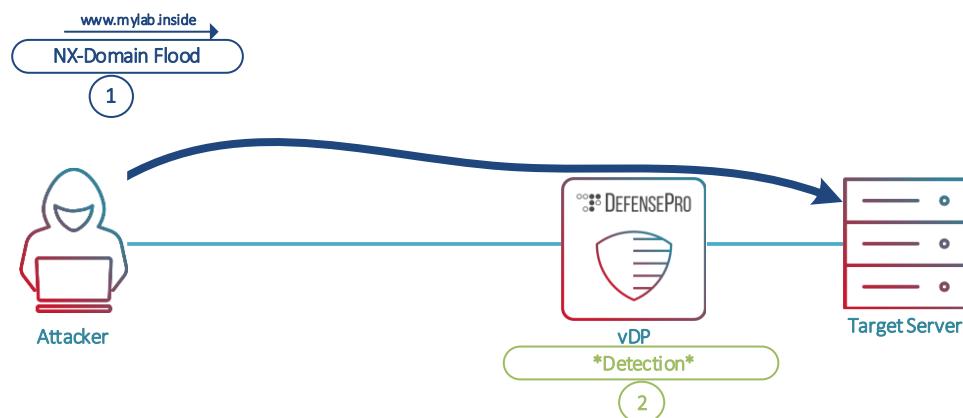
When under attack, DefensePro X will generate a Real-Time signature that matches the attack traffic pattern and use it to mitigate the attack while allows the legitimate queries to pass in.

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

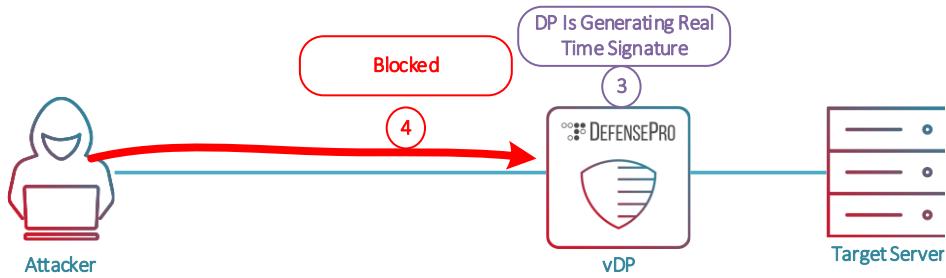
DNS protection can mitigate DNS sub-domain flood attacks while allowing only legitimate queries to pass.

Scenario Steps Overview

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

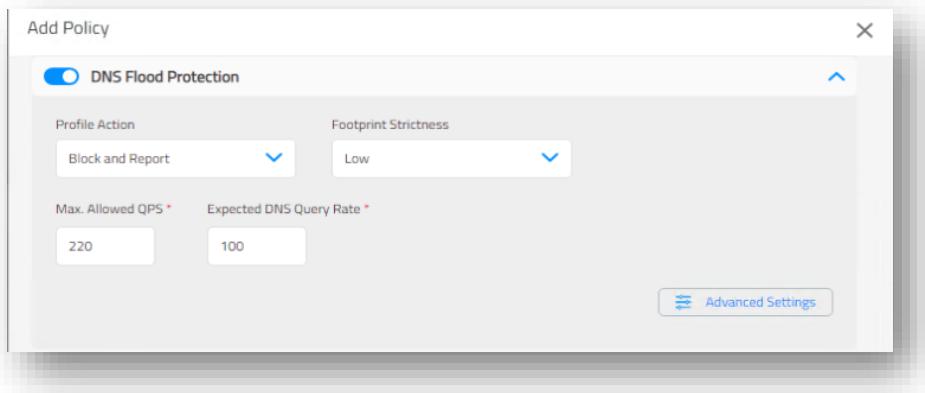


2. DefensePro X checks if the DNS queries rate is above the attack edge baseline.
3. DefensePro X generates a real time signature which will be used to mitigate the DNS NX domain flood attack.



Configurations

DNS Flood profile configured as follows:



Advanced Settings - DNS Flood Protection X

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 *
90	45	45	15	8
SOA Query *	NAPTR Query *	SRV Query *	Other Queries *	
2	2	2	2	

Other Rate Settings

Signature Rate-Limit Target *

0

Manual Triggers

Use Manual Triggers

Disabled ▼

Advanced

Learning Suppression Threshold *

0

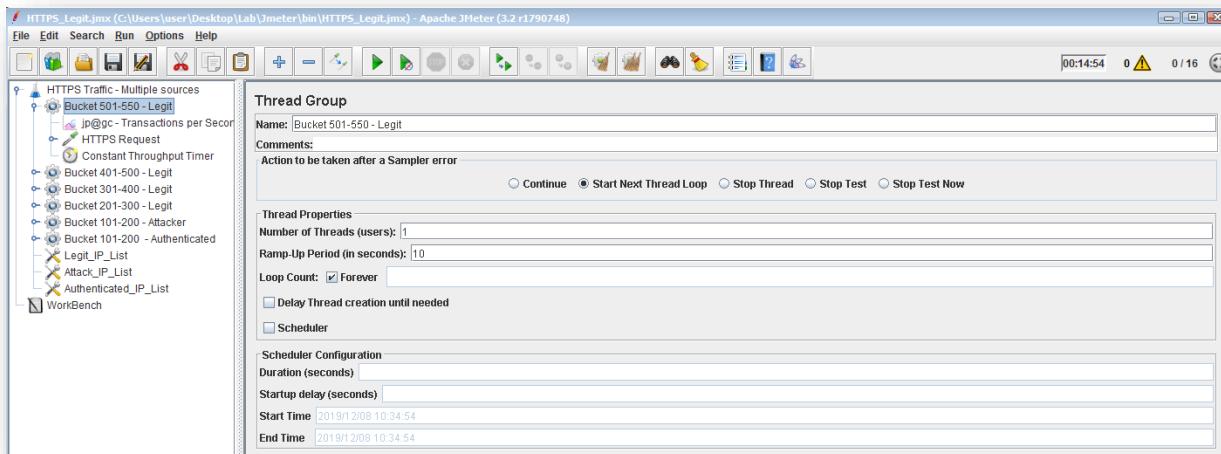
Cancel Submit

APPENDIX 8 - HTTPS TRAFFIC GENERATION TEMPLATE (ADDITIONAL INFO)

The HTTPS traffic template configured as follows:

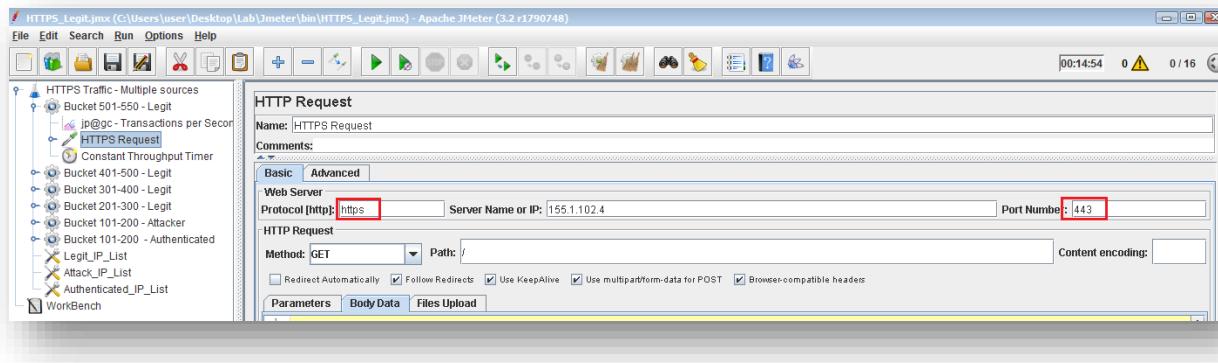
1. Bucket # – The HTTPS request to the specific bucket size:

- **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.



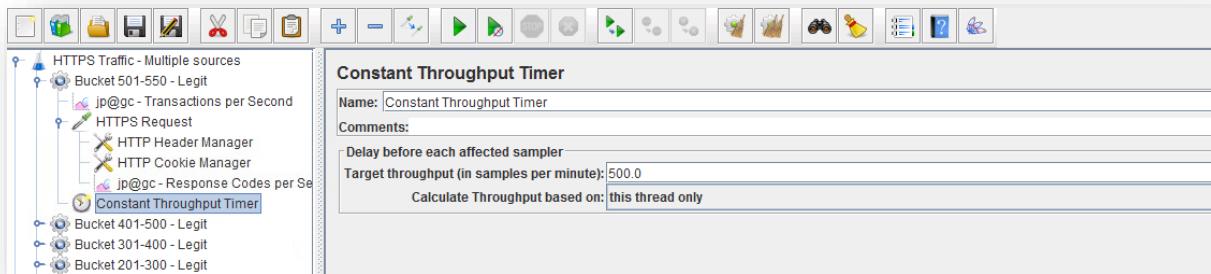
2. HTTP Request – The HTTPS header configuration:

- **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.

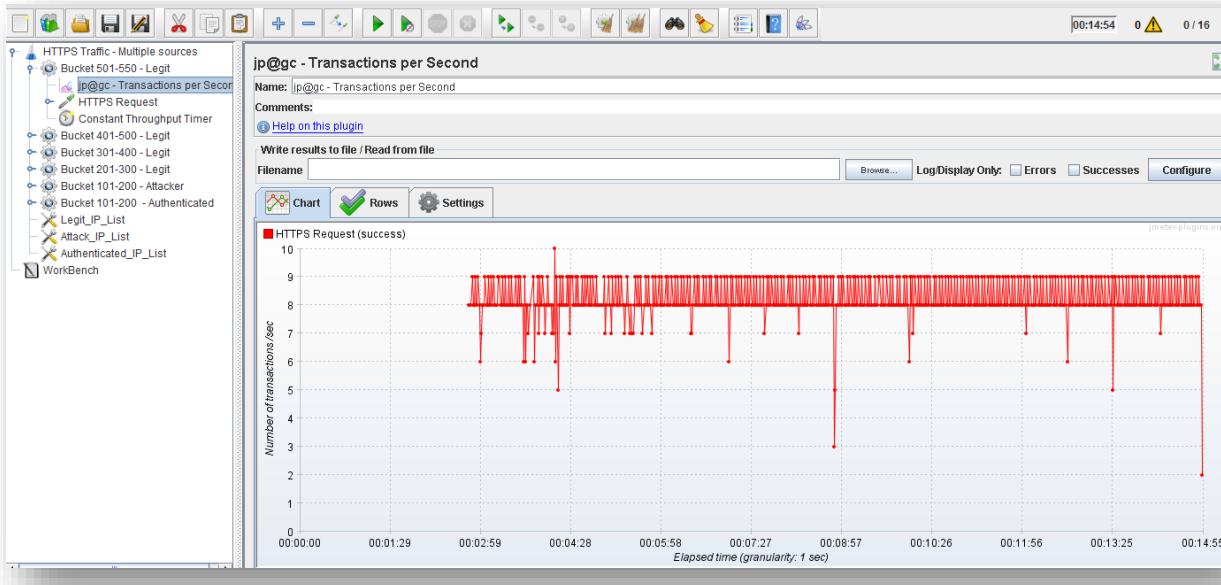


4. Set the HTTP Cookie Manager:

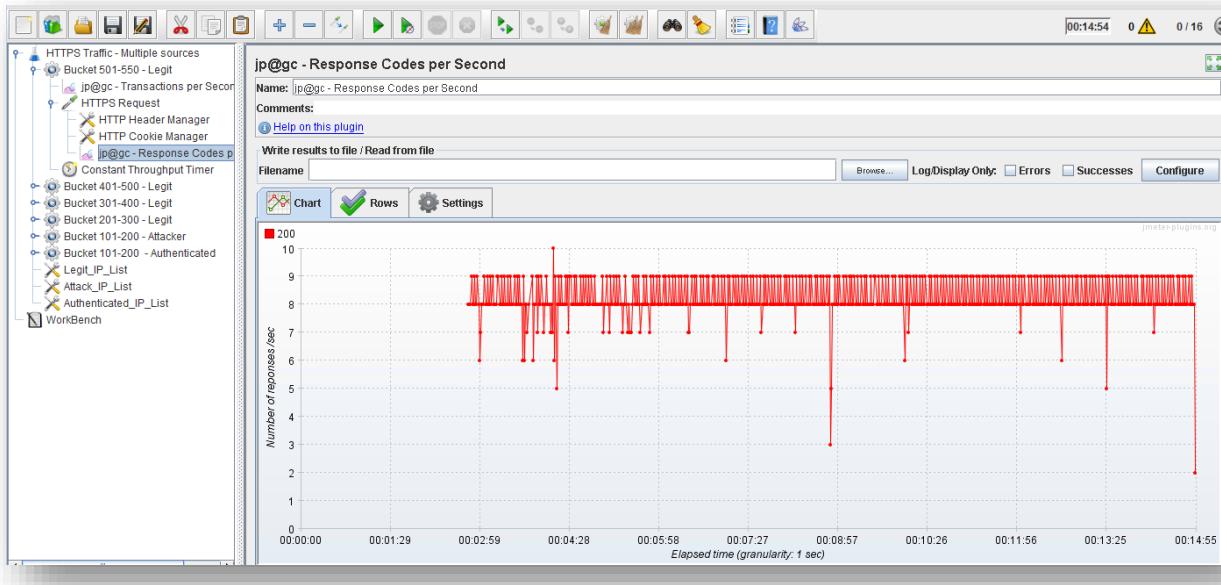
- Used for a 302-cookie challenge



5. Set the Transactions per Second:



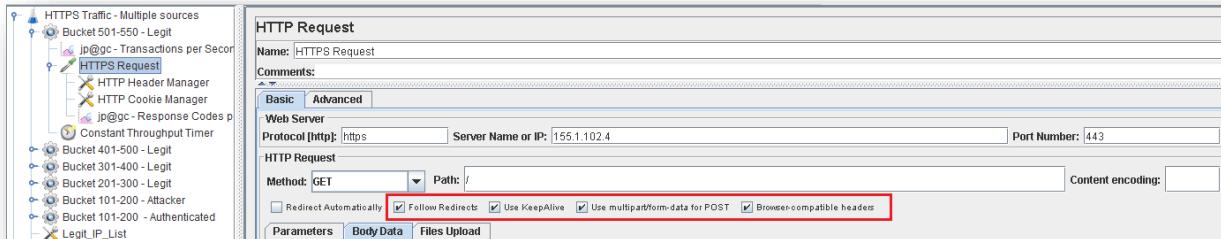
6. Set the Response Codes per Second:



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

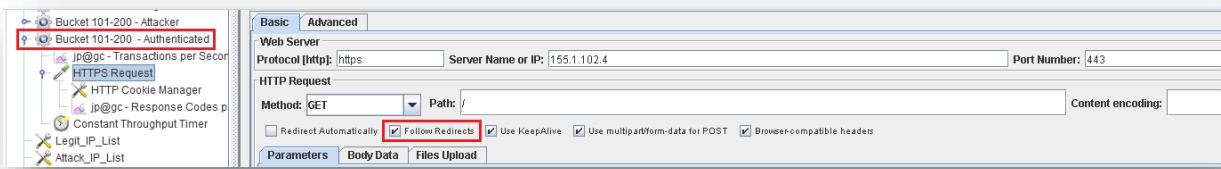
8. Buckets Type:

- Legit – Simulates traffic from legitimate users:



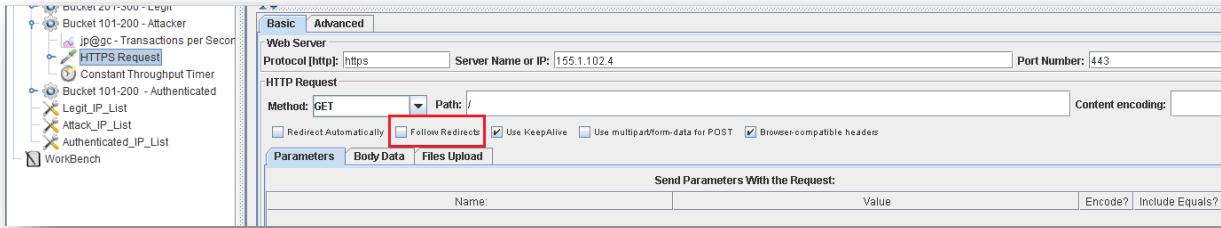
The screenshot shows the DefensePro X interface. On the left, a tree view shows 'Bucket 501-550 - Legit' selected. The main panel is titled 'HTTP Request' with the sub-tab 'Basic' selected. The 'Web Server' section shows 'Protocol [https]: https' and 'Server Name or IP: 155.1.102.4' with 'Port Number: 443'. The 'HTTP Request' section shows 'Method: GET' and 'Path: /'. Under 'HTTP Request' settings, the 'Follow Redirects' checkbox is checked (highlighted with a red box). Other checked checkboxes include 'Use KeepAlive', 'Use multipart/form-data for POST', and 'Browser-compatible headers'. The 'Content encoding' field is empty. Below the main panel are tabs for 'Parameters', 'Body Data', and 'Files Upload'.

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



The screenshot shows the DefensePro X interface. On the left, a tree view shows 'Bucket 101-200 - Authenticated' selected. The main panel is titled 'HTTP Request' with the sub-tab 'Basic' selected. The 'Web Server' section shows 'Protocol [http]: http' and 'Server Name or IP: 155.1.102.4' with 'Port Number: 443'. The 'HTTP Request' section shows 'Method: GET' and 'Path: /'. Under 'HTTP Request' settings, the 'Follow Redirects' checkbox is checked (highlighted with a red box). Other checked checkboxes include 'Use KeepAlive', 'Use multipart/form-data for POST', and 'Browser-compatible headers'. The 'Content encoding' field is empty. Below the main panel are tabs for 'Parameters', 'Body Data', and 'Files Upload'.

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



The screenshot shows the DefensePro X interface. On the left, a tree view shows 'Bucket 201-300 - Legit' selected. The main panel is titled 'HTTP Request' with the sub-tab 'Basic' selected. The 'Web Server' section shows 'Protocol [https]: https' and 'Server Name or IP: 155.1.102.4' with 'Port Number: 443'. The 'HTTP Request' section shows 'Method: GET' and 'Path: /'. Under 'HTTP Request' settings, the 'Follow Redirects' checkbox is unchecked (highlighted with a red box). Other checked checkboxes include 'Use KeepAlive', 'Use multipart/form-data for POST', and 'Browser-compatible headers'. The 'Content encoding' field is empty. Below the main panel are tabs for 'Parameters', 'Body Data', and 'Files Upload'. A 'Send Parameters With the Request' section is visible at the bottom.