

# Training Lab Manual AMS Analytics



# Table of Contents

OVERVIEW.....	3
DEFENSEPRO MONITORING DASHBOARD .....	3
DEFENSEPRO ATTACKS DASHBOARD.....	7
DEFENSEPRO ANALYTICS DASHBOARD .....	9
DEFENSEPRO BEHAVIORAL PROTECTIONS DASHBOARD .....	10
FORENSICS .....	11
ALERTS.....	13
REPORTS.....	14

## Overview

The APSolute Vision Analytics AMS dashboards display monitoring and reporting metrics. These metrics enable you to view and track real-time and historical information on selected AMS devices as well as security information on the traffic that the devices protect.

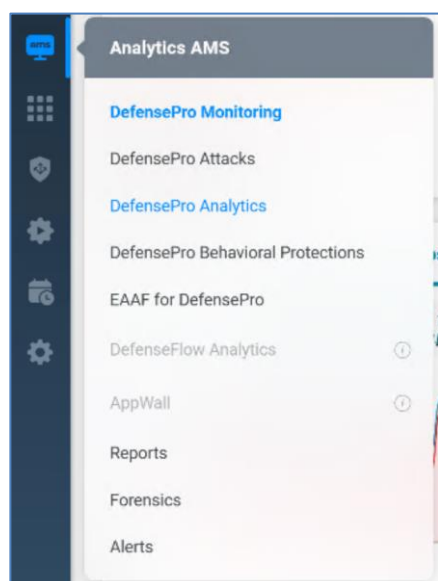
Exercises in this lab are viewed from the AMS Analytics perspectives.

Before you start make sure you have done the other labs generating attacks, so the database of the Analytics is filled with data to show.

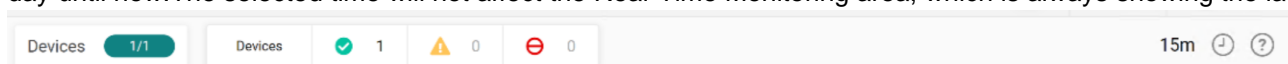
The screenshots are based on APSolute Vision version 5.3.0. For more details read the AVA User guide for the version you are using, available from the Radware customer portal.

## DefensePro Monitoring Dashboard

1. In **APSolute Vision**, select **Analytics AMS** → **DefensePro Monitoring**



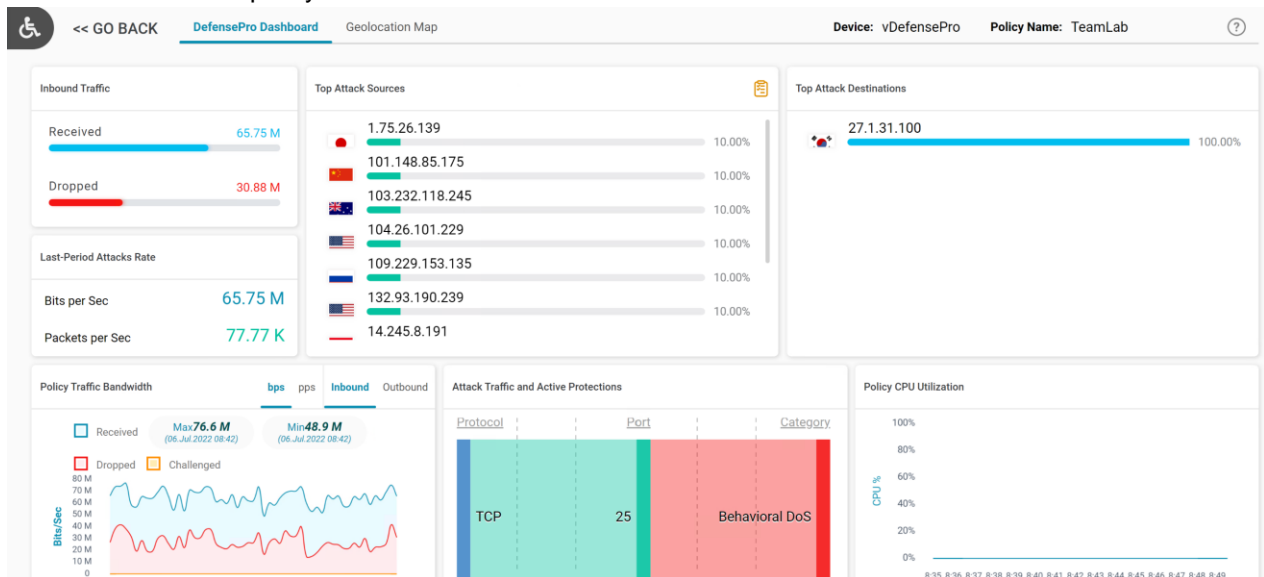
2. By default you will see monitoring information from all DefensePro v8 devices. Clicking on Devices, you can select a specific device and protection policy, in case you want to see only specific data. In our lab, we only have one device, so no need to do any specific selection
3. In the Dashboard Toolbar you can select the device/policy, see information about problematic devices (high cpu, license issues, down...) and select the time frame you want to see the information. There are preconfigured quick ranges (15-30Minutes/1-3-6-12-24Hours) or you can select a specific time range you are interested. For this exercise make sure you select a time frame, you have generated attacks, for example starting from you lab start day until now. The selected time will not affect the Real-Time Monitoring area, which is always showing the last 90s



- In the Traffic Bandwidth graph you can select between bps/pps and inbound/outbound traffic information.

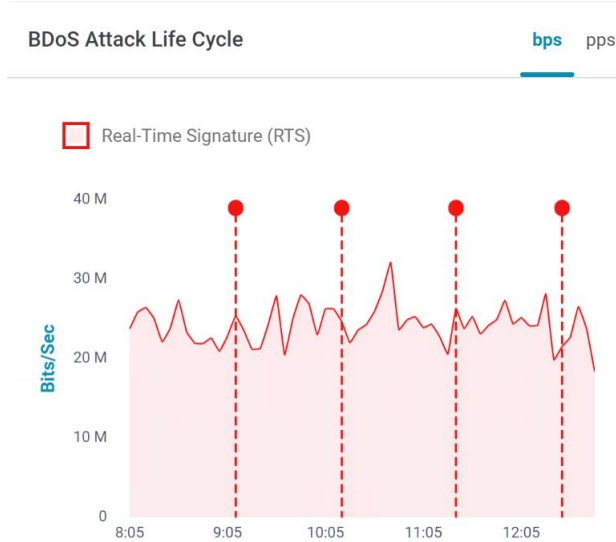


- If you click on the gear icon, you can select in the device/policy for which you want to see the information.
- If you click on the protection policy you can see the DefensePro Dashboard, which gives you information on the current status of the policy.



- In Protections view you can toggle between Show Events by Category or Show Events Table view, depending on your preferences and requirements.
- If you click on the Category, it will show the attack events.
- If you click on any event you will see it's details.

10. If event is protected by Behavioral DoS you will see BDoS Attack Life Cycle graph.



11. If you click on red dot you can see Real-Time Signature.

Real-Time Signature ×

Operator	Parameter	Value/s
[		
OR	source-port	31337
]		
AND		
[		
AND	packet-size	54
AND	destination-port	25
AND	destination-ip	27.1.31.100
AND	ttd	42
]		

12. If you click on **Geolocation Map**, you can see there the attacks are coming from and see if any country is blocked or block a country for a given time

DefensePro Dashboard **Geolocation Map**

13. In the attack view you can use the **+Black/White List** button to quickly block or allow certain traffic, based on the information you see in the table.

Protections

Show Events by Category ☒ Show Events Table

Attack ID	Start Time	Attack Name
41-1657013921	06.07.2022, 08:02:29	network flood IPv4 TCP-RST

+ Blacklist / Allowlist

Add IP Address to Blocklist or Allowlist – run

Target Devices: \*

vDefensePro

Add array elements...

Rule Type: \*

Blocklist Rule

Allow Updates During Attacks: \*

☒

Name Prefix: \*

Source IP Address: \*

IP address

Source Port:

31337

Destination IP Address:

27.1.31.100

Destination Port:

25

Cancel

Run

14. If you click on a BDoS event, you see the attack details.

Info

Protocol: TCP

Total Packets: 144,612,432

Volume: 8 GB

Physical Port: 1

Device IP Address: 10.10.244.31

Max bps: 64,297,984

Max pps: 145,350

Description

Direction: In

Characteristics

Edit Threshold

Attack Identification Statistics

Type	SYN In	SYN Out	RST In	RST Out	
Normal (Kbps)	245	245	491	491	2
Anomaly (Kbps)	295	0	7367	0	4
Normal (Packets/Sec)	480	480	1024	1024	5
Anomaly (Packets/Sec)	616	0	23023	0	1

BDoS Attack Life Cycle

bps pps

Real-Time Signature (RTS)

BDoS-TCP RST

IPv4 IPv6 bps pps Inbound Outbound

Legitimate ... Total ... Norma... Suspecte... Attac...

State: Real-Time Sianature Blocking



15. From here you can use the **Edit Threshold** button to change the bandwidth settings of the relevant BDoS Profile, in case tuning is needed.

Edit Profile Threshold -- run
✕

Target Device: \*

vDefensePro

Profile Type:

BDoS
✕

Profile Name:

TeamLab

Inbound Traffic (Kbit/s):

5000

Outbound Traffic (Kbit/s):

5000

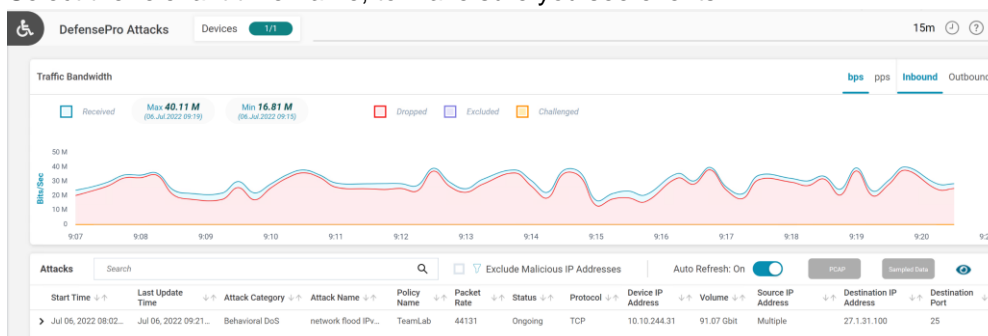
Cancel

Run

## DefensePro Attacks Dashboard

Starting APSolute Vision version 4.60 the DefensePro Attacks dashboard can be used to see the current attacks or attacks for a specific time frame with it's details.

1. In **APSolute Vision**, select **AMS Analytics → DefensePro Attacks**
2. Select the relevant time frame, to make sure you see events.



3. If you see a peak of attacks, you can mark the relevant time range in the Traffic Bandwidth graph to see the attacks from that specific range, or use the Search option to search for a specific attack.
4. The Auto Refresh can be disabled if needed.
5. You can sort on any row like **Volume**

Start Time	Last Update Time	Attack Category	Attack Name	Policy Name	Packet Rate	Status	Protocol	Device IP Address	Volume	Source IP Address	Destination IP Address	Destination Port
Jul 06, 2022 08:02...	Jul 06, 2022 09:22...	Behavioral DoS	network flood IPv...	TeamLab	53869	Ongoing	TCP	10.10.244.31	92.41 Gbit	Multiple	27.1.31.100	25

6. Depending on the type of attack you will see different information and you will see if a pcap or/and sampled data is available for the attack.

## 7. BDoS Example

Attacks

Search

Q

Exclude Malicious IP Addresses

Auto Refresh: On

PCAP

Sampled Data

Start Time

Last Update Time

Attack Category

Attack Name

Policy Name

Packet Rate

Status

Protocol

Device IP Address

Volume

Source IP Address

Destination IP Address

Destination Port

Jul 06, 2022 08:02:...

Jul 06, 2022 09:27:...

Behavioral DoS

network flood IPv...

TeamLab

36674

Ongoing

TCP

10.10.244.31

96.74 Gbit

Multiple

27.1.31.100

25

Additional Attack Attributes

Risk

High

Radware ID

74

Direction (In/Out)

In

Action Type

Drop

Attack ID

41-1657013921

Physical Port

1

Total Packet Count

234,823,018

VLAN

N/A

MPLS RD

N/A

Source Port

31337

Packet Type

Regular

Characteristics

State

Blocking

Flow Label

-

TCP Sequence Number

-

ToS

-

TTL

42

Real-Time Signature

Operator

Parameter

Value

[

OR

source-port

31337

]

AND

[

Sampled Data

X

Time

Source IP Address

Source Port

Destination IP Address

Destination Port

VLAN Tag

Protocol

06.07.2022 08:02:40

153.141.109.130

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:41

192.41.239.153

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:41

150.215.241.40

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:41

197.192.1.213

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:41

41.246.221.98

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:41

207.12.135.87

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:58

148.160.100.171

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:58

66.197.83.67

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:58

66.249.65.176

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:02:58

207.130.239.209

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:12:54

97.197.111.87

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:12:54

243.144.222.91

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:12:54

14.245.8.191

31337

27.1.31.100

25

N/A

TCP

06.07.2022 08:12:54

4.4.75.231

31337

27.1.31.100

25

N/A

TCP

## 8. Syn Flood example

Attacks

Search

Auto Refresh: Off

PCAP

Sampled Data

Start Time	End Time	Attack Category	Attack Name	Policy Name	Packet Rate	Status	Protocol	Device IP Address	Volume	Source IP Address	Destination IP Address	Destination Ports
Jun 19, 2020 01:48:20	Jun 19, 2020 01:48:41	SYN Flood	SYN Flood HTTP	NWRule_Tea...	0	Terminated	TCP	10.10.244.31	66.71 MB	Multiple	27.1.31.100	80

Additional Attack Attributes

Risk Medium	Radware ID 200000	Direction (In/Out) Unknown	Action Type Challenge
Attack ID 66-1592289343	Physical Port Multiple	Total Packet Count 1,111,913	VLAN N/A
MPLS RD N/A	Source Port Multiple		

Characteristics

Average Attack Rate (pps) 5155
Attack Duration [Hour:Min:Sec] 00:00:21
Activation Threshold 2500
TCP Challenge Tcp Reset
TCP Auth. List (%) 0
HTTP Challenge Redirect 302



## 9. Anti-Scanning example

Start Time	End Time	Attack Category	Attack Name	Policy Name	Packet Rate	Status	Protocol	Device IP Address	Volume	Source IP Address	Destination IP Address	Destination Ports
Jun 19, 2020 01:51:16	Jun 19, 2020 01:52:39	Anti-Scanning	TCP IP Scan	NWRule_Tea...	0	Terminated	TCP	10.10.244.31	5.65 MB	27.1.31.10	Multiple	80

Additional Attack Attributes			
Risk Medium	Radware ID 350	Direction (In/Out) In	Action Type Drop
Attack ID 72-1592288343	Physical Port 1	Total Packet Count 108,282	VLAN N/A

Real-Time Signature		
Operator	Parameter	Value
[		
OR	Destination Port	80
]		
AND		

Characteristics	
Avg. Time Between Probes [sec]	< 0 ms
Number of Probes	0
Action Reason	-
Blocking Duration [Sec]	40
Estimated Release Time	Jun 19, 2020 01:51:16

Scan Details		
Destination IP Addr...	Destination L4 Port	TCP Flag/Protocol
27.1.31.100	443	SYN
27.1.31.100	80	SYN
27.1.32.127	80	SYN
27.1.32.69	80	SYN
27.1.32.234	80	SYN
27.1.32.85	80	SYN
27.1.32.190	80	SYN
27.1.32.57	80	SYN
27.1.32.49	80	SYN
27.1.32.165	80	SYN

## 10. Signature protection example

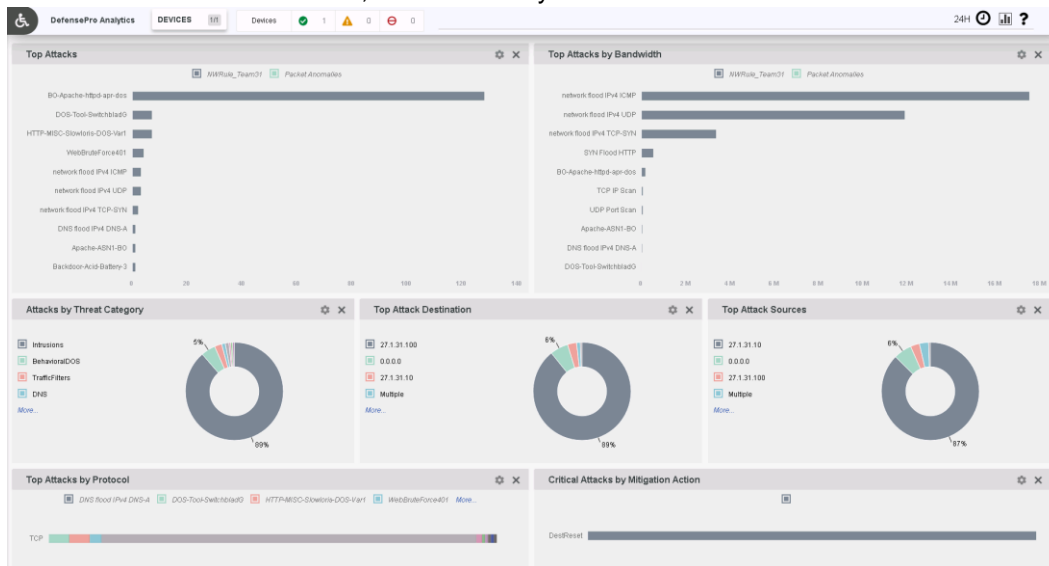
Start Time	End Time	Attack Category	Attack Name	Policy Name	Packet Rate	Status	Protocol	Device IP Address	Volume	Source IP Address	Destination IP Address	Destination Ports
Jun 19, 2020 01:56:26	Jun 19, 2020 01:56:41	Intrusions	DOS-Tool-SwitchblatdG	NWRule_Tea...	99	Occurred	TCP	10.10.244.31	400.39 KB	27.1.31.10	27.1.31.100	80

Additional Attack Attributes			
Risk Medium	Radware ID 16676	Direction (In/Out) In	Action Type DestReset
Attack ID 82-1592288343	Physical Port 1	Total Packet Count 1,501	VLAN N/A
MPLS RD N/A	Source Port Multiple		

## DefensePro Analytics Dashboard

1. In **APSolute Vision**, select **AMS Analytics** → **DefensePro Analytics**
2. Select the relevant time frame, to make sure you see events.

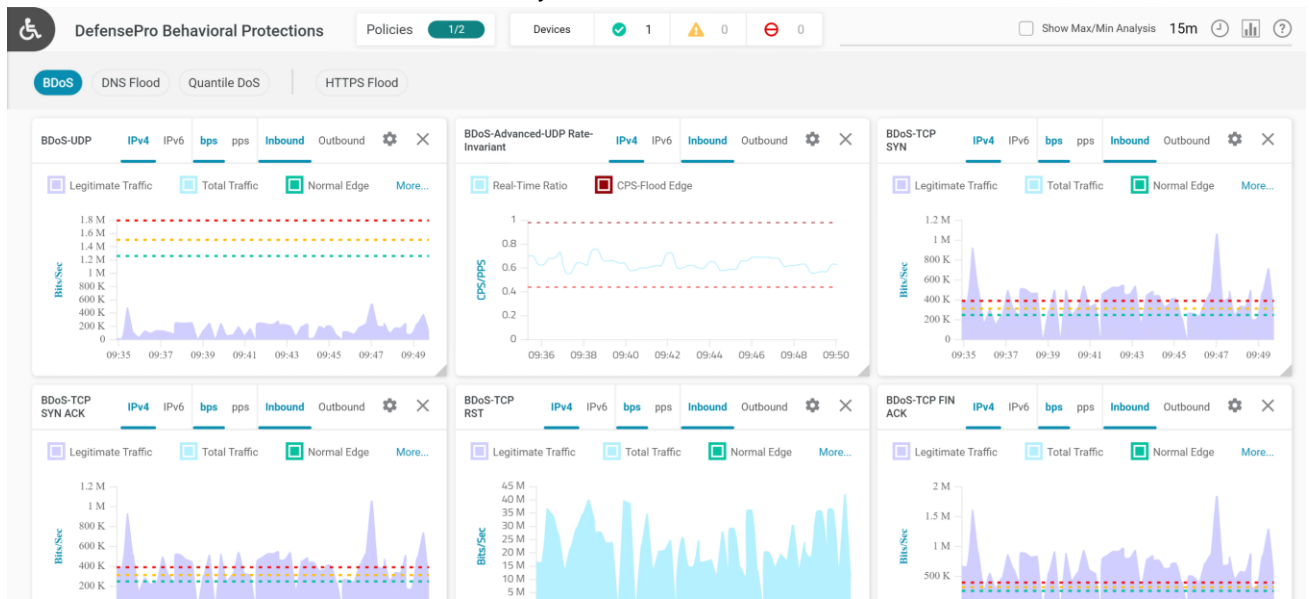


3. This dashboard can be customized, by using the widgets icon
4. Each widget can be changed to show only data from a specific device or/and policy using the gear symbol. So you can add the same widget twice and show content from different devices/policies.

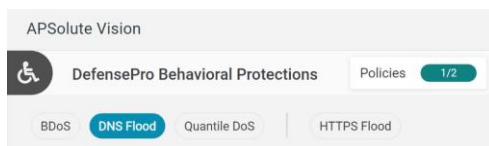
## DefensePro Behavioral Protections Dashboard

This dashboard is used to see the BDoS and DNS protection learning information for a specific policy on a specific device.

1. In **APSolute Vision**, select **AMS Analytics** → **DefensePro Behavioral Protections**
2. Click on **Policies** to select a specific protection policy on a device to see its details. Make sure you have a BDoS or/and a DNS protection profile in the selected policy.
3. Select the relevant time frame, to make sure you see events Dashboard



4. You can also select **DNS Flood**, **Quantile DoS**, and **HTTPS Flood** behavioral protection tabs in this section.



## Forensics

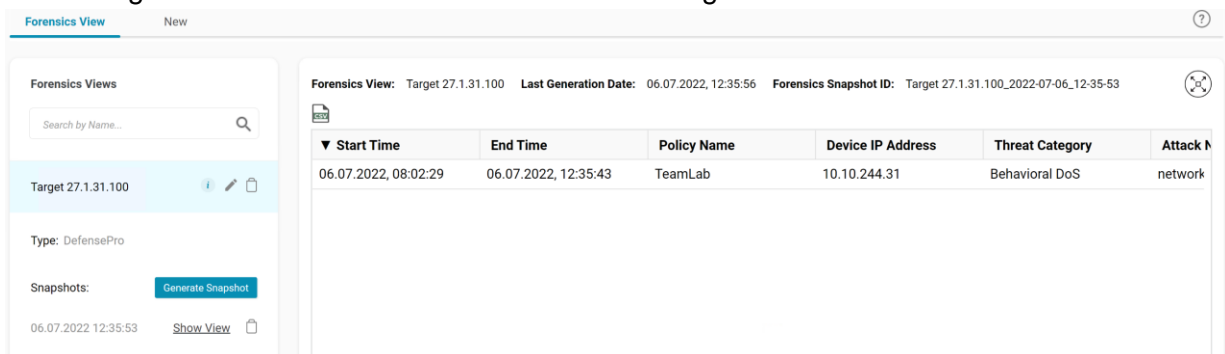
Use the **Forensics** module to analyze and discover the source of security attacks, attack methods and trends, or other problem incidents.

When the Forensics module generates an iteration of a forensics-view, it is referred to as a forensicsview *snapshot*. Each forensics-view snapshot can contain a maximum of 10,000 entries.

1. In **APSolute Vision**, select **AMS Analytics → Forensics**
2. Click on the **New** tab to create a new view
3. Use the following information for the new Forensics View:

Parameter	Value
<b>Forensics Name</b>	Target 27.1.31.100
<b>Product</b>	DefensePro
<b>Devices</b>	vDefensePro
<b>Time</b>	Today
<b>Criteria</b>	Destination IP Equals IPv4 27.1.31.100 - click <b>Add Condition</b> to use the criteria
<b>Criteria &gt; Apply To</b>	Any Condition (OR)
<b>Output</b>	Select all fields (click <b>Add All</b> in the Available Fields)
<b>Format</b>	HTML
<b>Schedule</b>	Run Report / Once

4. Click **Submit**
5. Select the **Forensic View** and click on **Generate Snapshot**
6. After it is generated click on the **Show View** that was generated.



The screenshot shows the 'Forensics View' interface. On the left, there's a sidebar with a search bar and a list of views. The main panel displays a table of generated snapshots.

Start Time	End Time	Policy Name	Device IP Address	Threat Category	Attack N
06.07.2022, 08:02:29	06.07.2022, 12:35:43	TeamLab	10.10.244.31	Behavioral DoS	network

## 7. Click on an event to see it's details

### Attack Details


[Refine View](#)
[Sampled Data](#)
[Close](#)

Action	Drop	Attack Packet Rate (pps)	48636
Attack ID	41-1657013921	Physical Port	1
Threat Category	Behavioral DoS	Protocol	TCP
Destination IP Address	27.1.31.100	Radware ID	74
Destination Port	25	Risk	High
Device IP Address	10.10.244.31	Policy Name	TeamLab
Direction	In	Source IP Address	Multiple
Duration	16394	Source Port	31337
End Time	2022/07/06 12:35:43	Start Time	2022/07/06 08:02:29
Attack Name	network flood IPv4 TCP-RST	Status	Ongoing
Total Mbits Dropped	336357.91	VLAN Tag	N/A
Total Packets Dropped	797293944	Packet Type	Regular

## 8. Use can use the icon to enlarge the view.

## Alerts

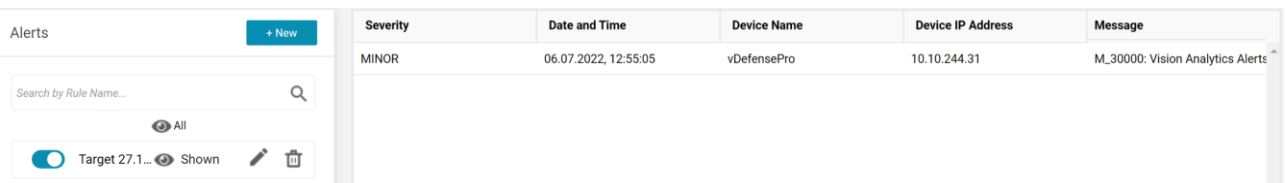
Use the Alerts module to create rules for alerts that Analytics generates. The Alerts screen displays the alert rules. You can turn alert rules on and off, as you require.

The right side of the Alerts screen can show the alerts from the alert rules. Alerts from alert rules that are turned go to the APSolute Vision Alerts Table pane. You can also configure alert rules to send alerts via email.

1. In **APSolute Vision**, select **AMS Analytics → Alerts**
2. Click on the **+New** button to create a new alert
3. Use the following information for the new Forensics View:

Parameter	Value
<b>Alert Name</b>	Target 27.1.31.100
<b>Select Product</b>	DefensePro
<b>Scope</b>	Devices/vDefensePro
<b>Criteria</b>	Destination IP Equals IPv4 27.1.31.100 - click <b>Add New Condition</b> to use the criteria
<b>Criteria → Apply To</b>	Any Condition
<b>Threshold → Run Alert</b>	Send an alert any time the criteria match

4. Click **Submit**
5. Run a new attack against the target server to trigger the alert
6. When the alert gets triggered, you can see it. You might need to click on the “Shown/Hidden” eye icon to show the alert.



Severity	Date and Time	Device Name	Device IP Address	Message
MINOR	06.07.2022, 12:55:05	vDefensePro	10.10.244.31	IM_30000: Vision Analytics Alerts

7. If you click on the event, you can see more details.

Alert details ×

Rule name: Target 27.1.31.100			
Start Time	End Time	Threat Category	Attack Name
06.07.2022 08:02:29	06.07.2022 12:54:48	Behavioral DoS	network f

## Reports

We will return to this section at the end of the training so the report will show enough activities.

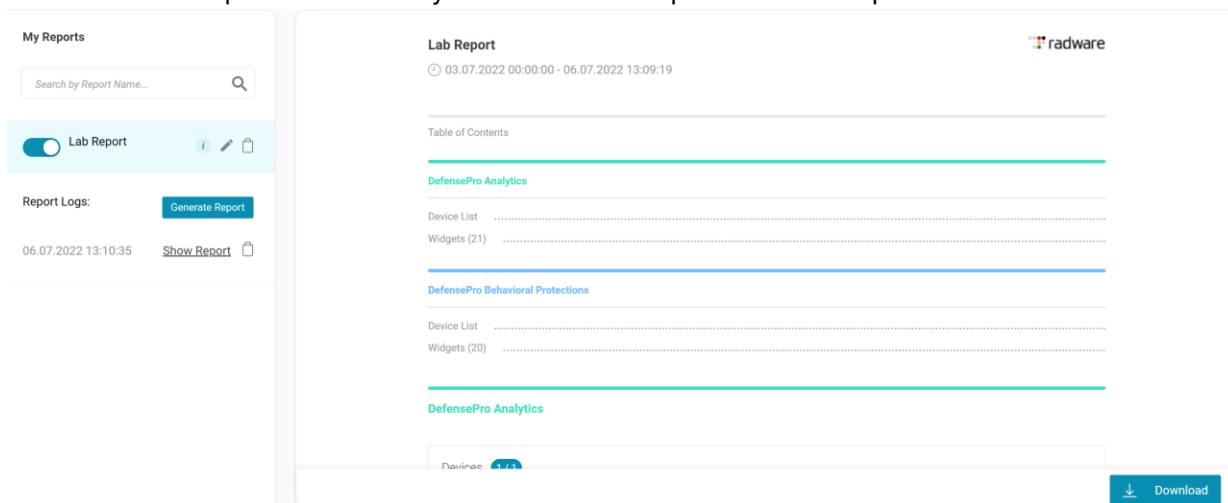
Use the Reports module to create and generate a report and view a single query on the fly. This is helpful when you want to quickly view data for a single query..

1. In **APsolute Vision**, select **AMS Analytics** → **Reports**
2. Click on the **New Report** tab to create a new report

3. You can select between several different templates, create two reports one using the DefensePro Analytics and one using the DefensePro Behavioral Protections (use TeamXX policy) as template. Make sure you select a **time** range, there you have data to show (i.e. **This Week**). And select your device and policy for Behavioral template you need to select the device and the relevant protection policy.
4. Reports can be as well **Scheduled** and **Shared** via Email, so this would be useful, if you need to automatically generate a weekly/monthly report.
5. The **Format** of the report output can be PDF, HTML or CSV, depending on the purpose
6. After you created the report, we need to generate the report. Click on the Generate Report button.



7. You will see the report after it's ready. Click on Show Report to see the report.



8. Use the **Download File** button to export the report.



For questions, contact [training@Radware.com](mailto:training@Radware.com)

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.