Netsurion | EventTracker®

Integrate Barracuda NextGen Firewall F-Series

EventTracker v8.x and above

Publication Date: September 18, 2020

Abstract

This guide provides instructions to configure **Barracuda NG Firewall F-Series** to send the syslog to EventTracker. Once syslog is being configured to send to EventTracker manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 8.x and later, **Barracuda NG Firewall F-Series** (F18, F80, F180, F280, F380, F400, F600, F800, F900, f1000).

Audience

Administrators who are responsible for monitoring **Barracuda NG Firewall F-Series** which are running using EventTracker Manager.

Table of Contents

1. Barracuda NG Firewall F-Series

The **Barracuda NextGen Firewall F-Series** is a family of hardware, virtual, and cloud-based appliances that protect and enhance your dispersed network infrastructure. They deliver advanced security by tightly integrating a comprehensive set of next-generation firewall technologies, including layer 7 application profiling, intrusion prevention, web filtering, malware and advanced threat protection, antispam protection, and network access control.

In addition, the F-Series combines highly resilient VPN technology with intelligent traffic management and WAN optimization capabilities. This lets you reduce line costs, increase overall network availability, improve site-to-site connectivity, and ensure uninterrupted access to applications hosted in the cloud. Scalable centralized management helps you reduce administrative overhead while defining and enforcing granular policies across your entire dispersed network.

1.1 Prerequisites

- EventTracker v8.x should be installed.
- **Barracuda NG Firewall F-Series** (F18, F80, F180, F280, F380, F400, F600, F800, F900, f1000) should be installed and configured.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

2. Configuring Barracuda NextGen Firewall to send syslog to EventTracker

2.1 Logging into the Barracuda NextGen Firewall F-Series

1. Launch NextGen Admin.
2. Enter the Management IP, Username, and Password.

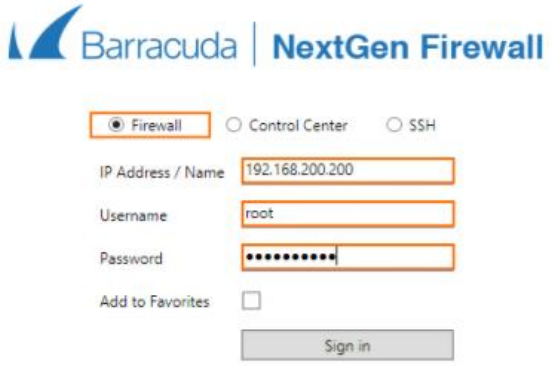

Figure 1

3. Click Sign In.

2.2 Configuring the Logstream Destinations

1. Configure the data transfer settings for the EventTracker server. You can optionally choose to send all the syslog data via SSL-encrypted connection.
2. Go to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming.
3. In the left menu, select Logstream Destinations.
4. Click Lock.
5. Click + in the Destinations table. The Destinations window opens.
6. Configure the EventTracker server logstream destination.
7. Enter the name “e.g. EventTracker”.
8. Remote Loghost – Select explicit-IP
9. Loghost IP Address – Enter the IP address of the EventTracker server.
10. Loghost Port – EventTracker server port.

2.3 Configuring Logdata Filters

Define profiles specifying the log file types to be transferred / streamed.

1. Go to **CONFIGURATION** > **Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata** Filters.
3. Click **Lock**.
4. Click the **+** icon to add a new filter.
5. Enter a **Name** “e.g. FILT01” and click **OK**. The **Filters** window opens.
6. Click + in the **Data Selection** table and select **Firewall_Audit_Log**.
7. In the **Affected** Box **Logdata** section, select **Selection** from the **Data Selector** dropdown.
8. Click **+** to add a **Data Selection**. The **Data Selection** window opens.
9. Enter a **Name** and click **OK**.
10. In the **Log Groups** table, click **+** and select **Firewall-Activity-Only** from the list.

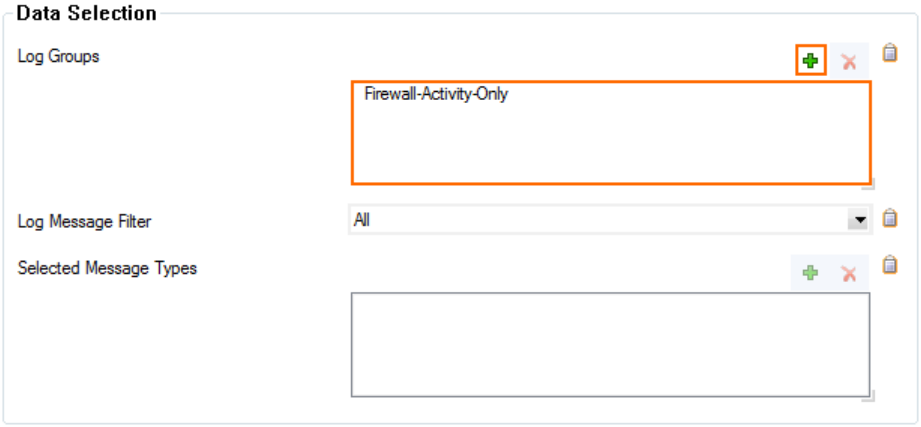

Figure 2

11. In the **Data Selection Table**, from the log message filter select the following filters.
    - Auth
    - Config
    - Firewall
    - Network
    - virscan
    - wi-fi
    - Watchdog
12. Click **OK**.
13. In the **Affected Service Logdata** section, select **None** from the **Data Selector** dropdown.
14. Click **OK**.

2.4 Enabling the syslog Service

1. Go to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming.

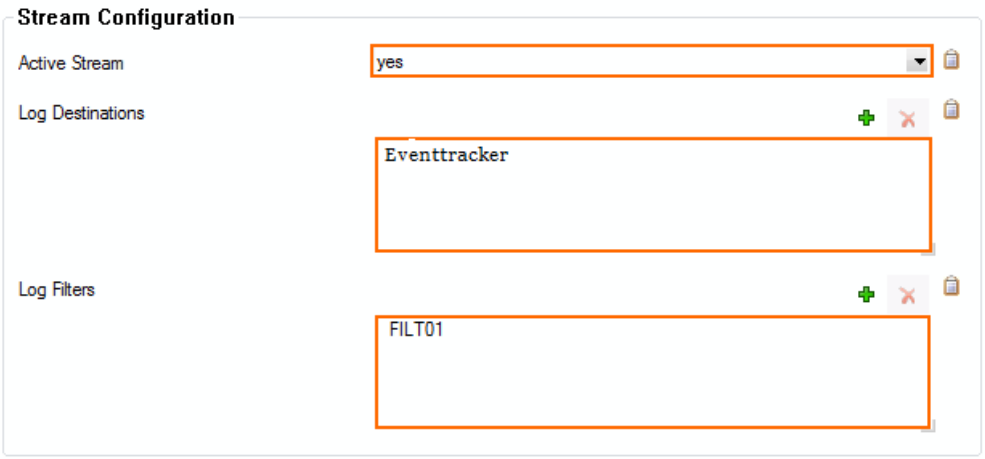

Figure 3

2. Set Enable the Syslog service to yes.
3. Click on + on log destination and select the Log Destination which we configured in the section Configuring the Logstream Destinations
4. Click on + on log filter and select the filter which we configured in the section Configuring Logdata Filters
5. Click Send Changes and Activate.

3. EventTracker Knowledge Pack

Once logs are received into EventTracker, categories, reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Windows.

3.1 Alerts

- **Barracuda NG Firewall-Login failures:** This alert is generated when a login failure by a user is done on Barracuda Firewall console.
- **Barracuda NG Firewall-Attacks detection:** This alert is generated when any Security events has been triggered by a user.
- **Barracuda NG Firewall-IDS alerts:** This alert is generated when any IDS/IPS is detected.
- **Barracuda NG Firewall-Virus detection:** This alert is generated when any virus or malware is detected by the Barracuda NG firewall.

3.2 Flex Reports

- **Barracuda NG Firewall-Allowed traffic-** This report provides details about all the traffic that is allowed to pass by the NG Firewall.

LogTime	Computer	Source MAC Address	Source IP Address	Destination IP Address	Action	Activity Type	Rule Name	Protocol	Count
06/20/2017 12:20:52 PM	BARRACUDA-NG	55:e3:ca:45:c3:e1	192.168.1.111	121.227.12.153	Allow	FWD	Pass	TCP	1
06/20/2017 12:20:52 PM	BARRACUDA-NG	a1:8c:cc:e3:f1:ff	192.168.1.111	121.227.12.153	Allow	cumulative	Pass	TCP	6
06/20/2017 12:20:52 PM	BARRACUDA-NG	55:e3:ca:45:c3:e1	192.168.1.111	121.227.12.153	Allow	LIN	Pass	TCP	1

Figure 4

- **Barracuda NG Firewall-Denied traffic-** This report provides details about all the traffic that is denied to pass by the NG Firewall.

LogTime	Computer	Source MAC Address	Source IP Address	Destination IP Address	Action	Activity Type	Protocol	Rule Name	Rule Description	Count
06/20/2017 12:20:52 PM	BARRACUDA-NG	55:e3:ca:45:c3:e1	192.168.1.111	121.227.12.153	Drop	LIN	UDP	DROPALL	Drop by Rule	1
06/20/2017 11:45:32 AM	BARRACUDA-NG	a1:8c:cc:e3:f1:ff	192.168.1.111	121.227.12.153	Block	cumulative	TCP	BLOCKALL	Block by Rule	6
06/20/2017 11:45:32 AM	BARRACUDA-NG	55:e3:ca:45:c3:e1	192.168.1.111	121.227.12.153	Block	FWD	UDP	BLOCKALL	Block by Rule	1
06/20/2017 12:20:53 PM	BARRACUDA-NG	55:e3:ca:45:c3:e1	192.168.1.111	130.22.69.141	Drop	LOUT	TCP	DROPALL	Drop by Rule	1

Figure 5

- **Barracuda NG Firewall-Login success-** This report provides details on all the successful logon that is done in the NG Firewall console.

LogTime	Computer	Device IP Address	User Name	Client IP address
06/29/2017 03:46:59 PM	PNPL-6-KP	192.168.105.1	root	192.168.1.13
06/29/2017 03:46:59 PM	PNPL-6-KP	192.168.105.1	Steven	192.168.112.191
06/29/2017 03:46:59 PM	PNPL-6-KP	192.168.105.1	kevin	192.168.32.96

Figure 6

- **Barracuda NG Firewall-Login failures-** This report provides details about all the login failures that is done in the NG Firewall console.

LogTime	Computer	Device IP Address	User Name	Client IP address	Reason
06/29/2017 03:46:59 PM	PNPL-6-KP	192.168.105.1	katie	192.168.10.94	No Access from this ip address (192.168.1.125).
06/29/2017 03:46:59 PM	PNPL-6-KP	192.168.105.1	root	192.168.11.124	Invalid Password.
06/29/2017 03:47:21 PM	PNPL-6-KP	192.168.105.1	katie	192.168.10.94	No Access from this ip address (192.168.1.125).
06/29/2017 03:47:21 PM	PNPL-6-KP	192.168.105.1	root	192.168.11.124	Invalid Password.

Figure 7

- **Barracuda NG Firewall-IDS alerts:** This report provides details about all the IDS/IPS attacks that is attempted to compromise the NG Firewall.

LogTime	Computer	Source IP Address	Threat Url	Threat File	Origin	Risk	Hash	Threat Hits	Blocked	Start Time
06/29/2017 02:18:53 PM	PNPL-6-KP	192.168.105.1	http://cache\ytisf-thezoo-v0.60-74-gc4cdcd9\ytisf-thezoo-c4cdcd9\malwares\binaries\equationgroup.pdf	equationgroup.pdf	http/https	High	db1dg8weg52fv5eg98e2g39	6	1	06.29.2017 17.22.40.
06/29/2017 02:18:53 PM	PNPL-6-KP	192.168.105.1	http://eicar_com.apk	eicar_com.apk	http/https	High	e5h6e5her598r98w2h2w35j	2	4	06.29.2017 07.14.59.
06/29/2017 02:18:53 PM	PNPL-6-KP	192.168.105.1	http://cache\ytisf-thezoo-v0.60-74-gc4cdcd9\ytisf-thezoo-c4cdcd9\malwares\binaries\eqinoxone.exe	eqinoxone.exe	http/https	High	5bs47rg5gweqq6q6ayikje	1	2	06.28.2017 15.02.00.
06/29/2017 02:18:53 PM	PNPL-6-KP	192.168.105.1	http://10.17.33.114/virus/9/uno.zip	uno.zip	http/https	Medium	h5wrh1bsd12g9h2gw92v32v4	1	4	06.28.2017 13.01.00.

Figure 8

- **Barracuda NG Firewall-Attack detection-** This report provides details about on all the security events that is triggered by the user.

LogTime	Computer	Source IP Address	Attack Detected	Count	Attack Details
06/20/2017 11:45:32 AM	BARRACUDA-NG	192.168.1.111	Address-Port Scan	13	13 unallowed requests for source IP 192.168.1.111 within 60 seconds
06/20/2017 11:45:32 AM	BARRACUDA-NG	192.168.1.68	Address-Port Scan	15	15 unallowed requests for source IP 192.168.1.68 within 60 seconds

Figure 9

- **Barracuda NG Firewall-Virus detection-** This report provides details on all the Virus/malware that is detected by the Barracuda Anti-Virus scan.

LogTime	Computer	Activity Type	User Name	Source IP Address	Destination IP Address	Protocol	Scan Type	Application Context	Action Info	Risk/Severity	Attack Count	Last Observed
06/30/2017 11:51:43 AM	PNPL-6-KP	LOUT	Katie	192.168.105.104	172.217.12.142	TCP	Virus Scan	Eicar.com.exe	Virus Blocked(Eicar-Test Virus)	High	12	3d 12hr.03m.00s.
06/30/2017 11:51:43 AM	PNPL-6-KP	LIN	Bane	192.168.105.104	172.119.45.1	TCP	Virus Scan	cncrover-guard.exe	Virus Blocked(Trojan Detected)	Critical	28	6d 1hr.17m.11s
06/30/2017 11:51:43 AM	PNPL-6-KP	LIN	Donald	192.112.34.10	172.14.161.22	TCP	Virus Scan	miranda-im-v.0.12.rar	Virus Blocked(ADWARE)	Critical	6	1d 12hr.12.44
06/30/2017 11:51:43 AM	PNPL-6-KP	LOUT	Trunx	172.1.15.141	10.111.35.14	TCP	Virus Scan	ServiceChecker-2.5.13.exe	Malicious File Blocked by Rule	High	11	3d 12hr.03m.00s
06/30/2017 11:51:43 AM	PNPL-6-KP	LOUT	Pierce	172.168.11.72	172.217.12.142	TCP	Virus Scan	ophcrack-win32-installer.bat	Malicious Content Detected	Critical	2	10d 7hr.41m.15s

Figure 10

- **Barracuda NG Firewall-Wi-fi authentication-** This report provides details about all Wi-fi authentication that are done by use.

LogTime	Computer	Device IP Address	User Name	Client IP address
06/29/2017 04:22:28 PM	PNPL-6-KP	10.17.133.103	Leon	172.12.111.77.
06/29/2017 04:22:29 PM	PNPL-6-KP	10.17.133.103	Sophie	172.19.1.23.

Figure 11

4. Importing Barracuda NG Firewall knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Alerts
- Token templates
- Flex Reports

NOTE: Export knowledge pack items in the following sequence:

- Alerts
- Token templates
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

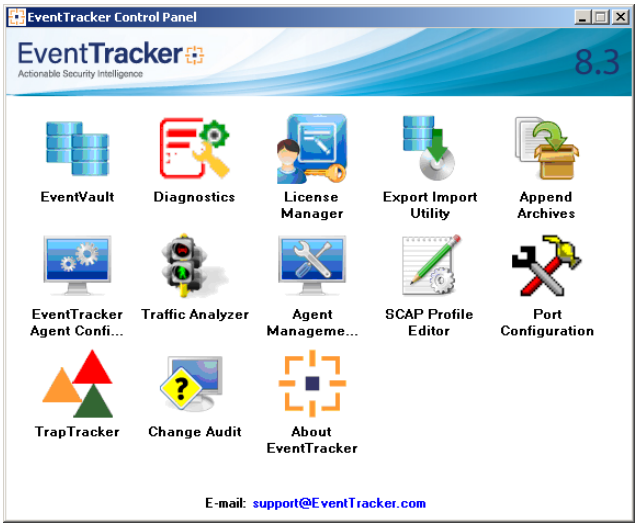

Figure 12

3. Click the **Import** tab.

4.1 Alerts

1. Click **Alerts** option, and then click the browse  button.
2. Locate the **Barracuda NG Firewall alerts.isalt** file, and then click the **Open** button.

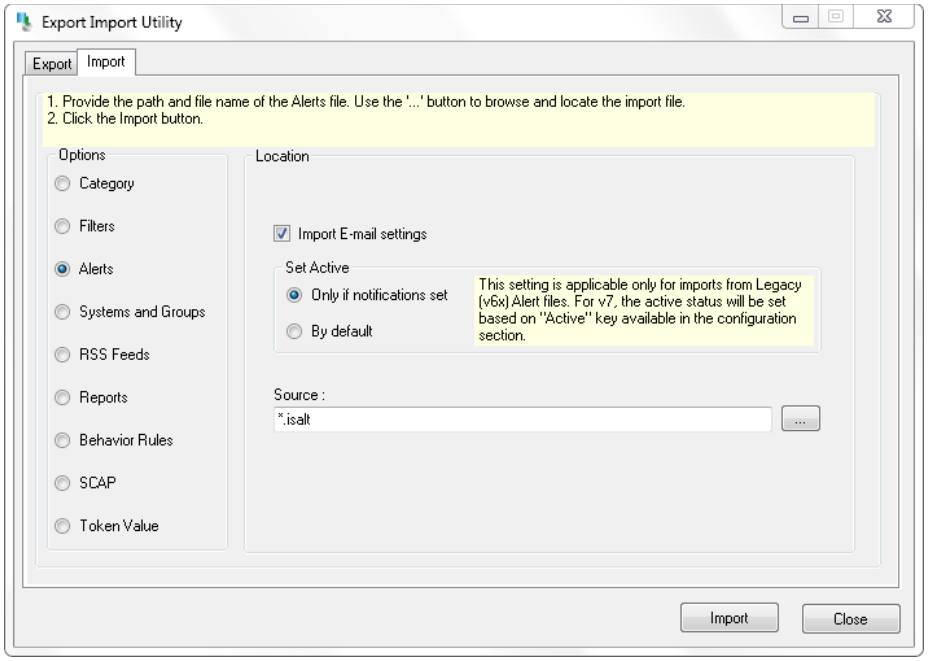

Figure 13

3. To import alerts, click the **Import** button.
   EventTracker displays success message.

Figure 14

4. Click **OK**, and then click the **Close** button.

4.2 Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on ‘**Import**’ option.
3. Click on **Browse** button.

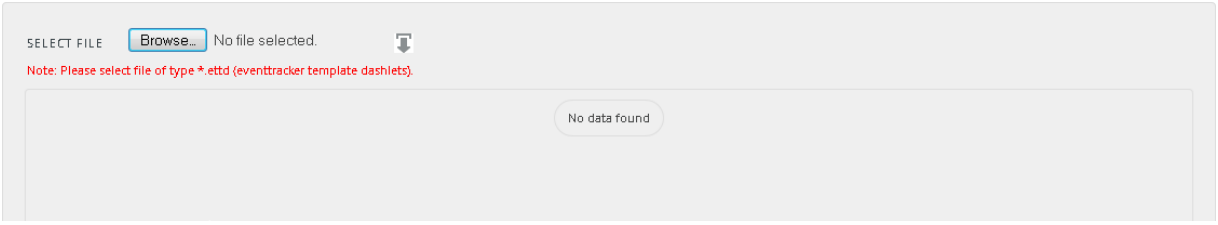

Figure 15

4. Locate **Barracuda NG Firewall.ettd** file, and then click the **Open** button.

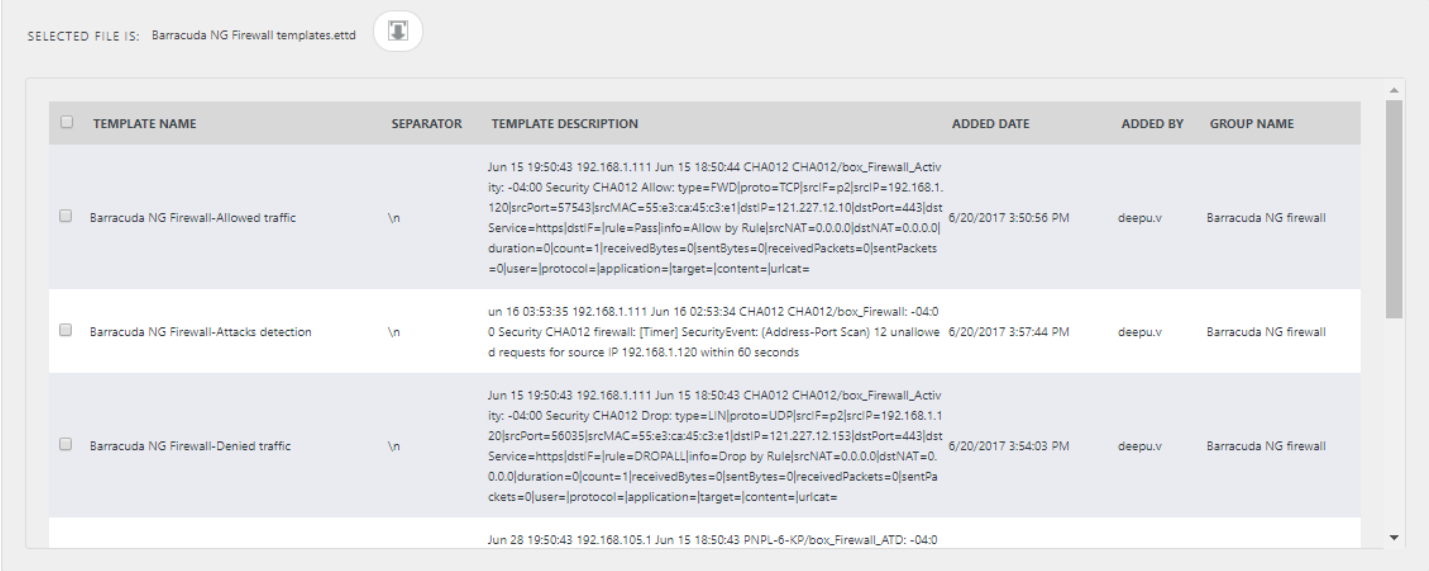

Figure 16

5. Now select the check box and then click on ‘**Import**’ option. EventTracker displays success message.

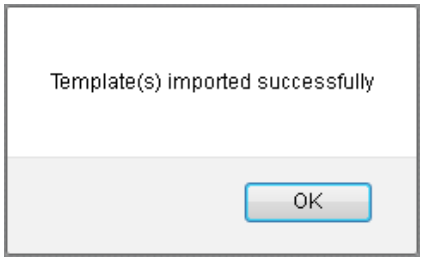

Figure 17

6. Click on OK button.

4.3 Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **Barracuda NG Firewall.etcrx** file, and then click the **Open** button.

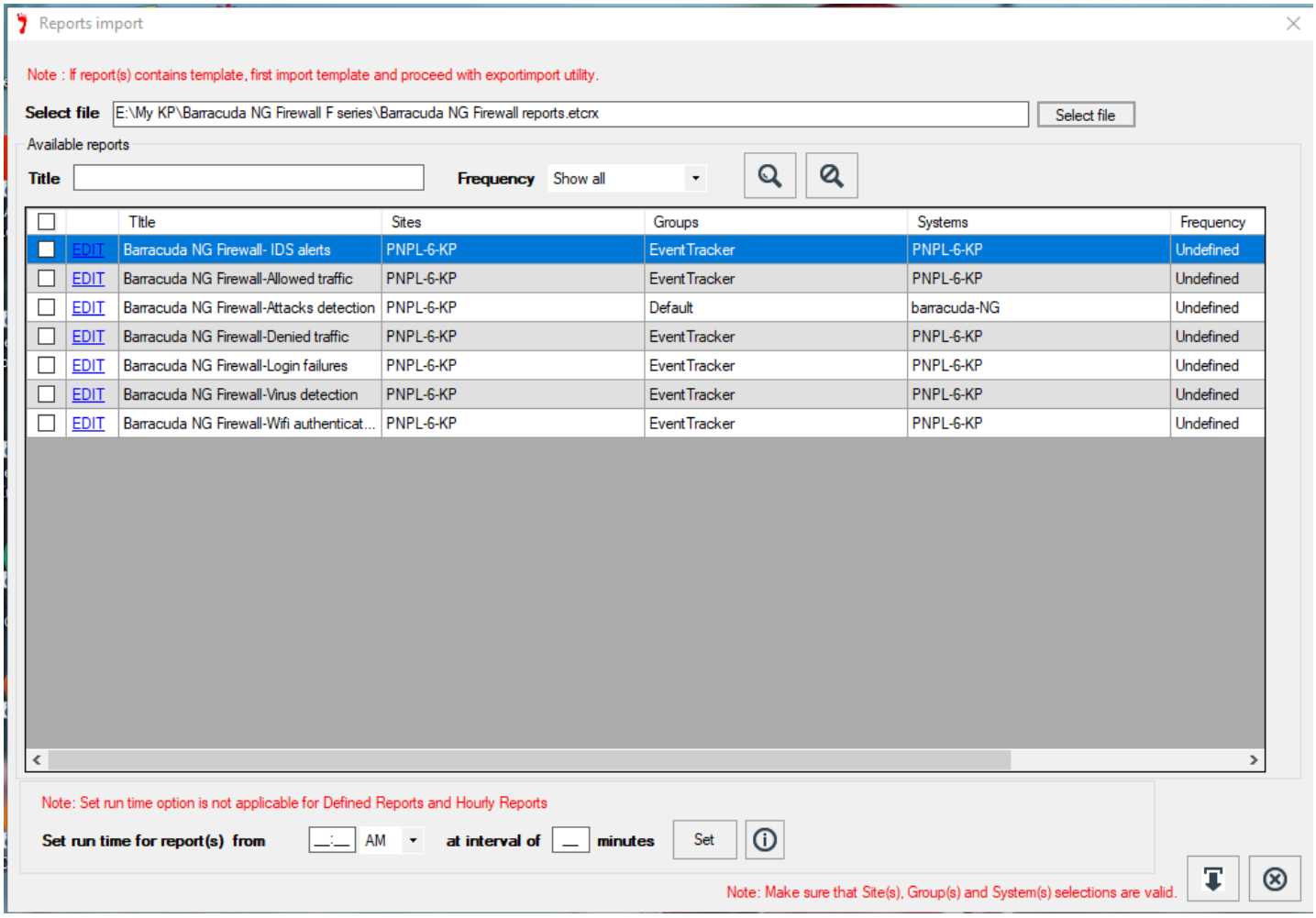

Figure 18

3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

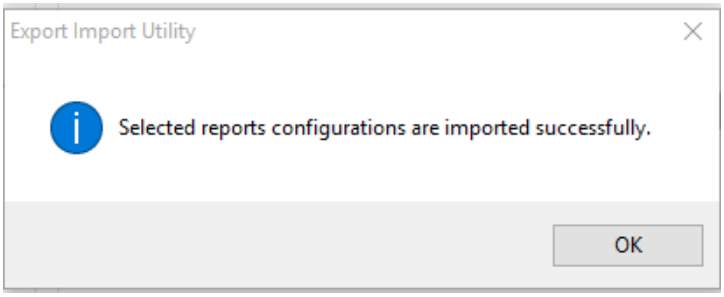

Figure 19

5. Verifying Barracuda NG Firewall knowledge pack in EventTracker

5.1 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **Barracuda NG Firewall**, and then click **Go**.
   Alert Management page will display the imported Barracuda NG Firewall alert.

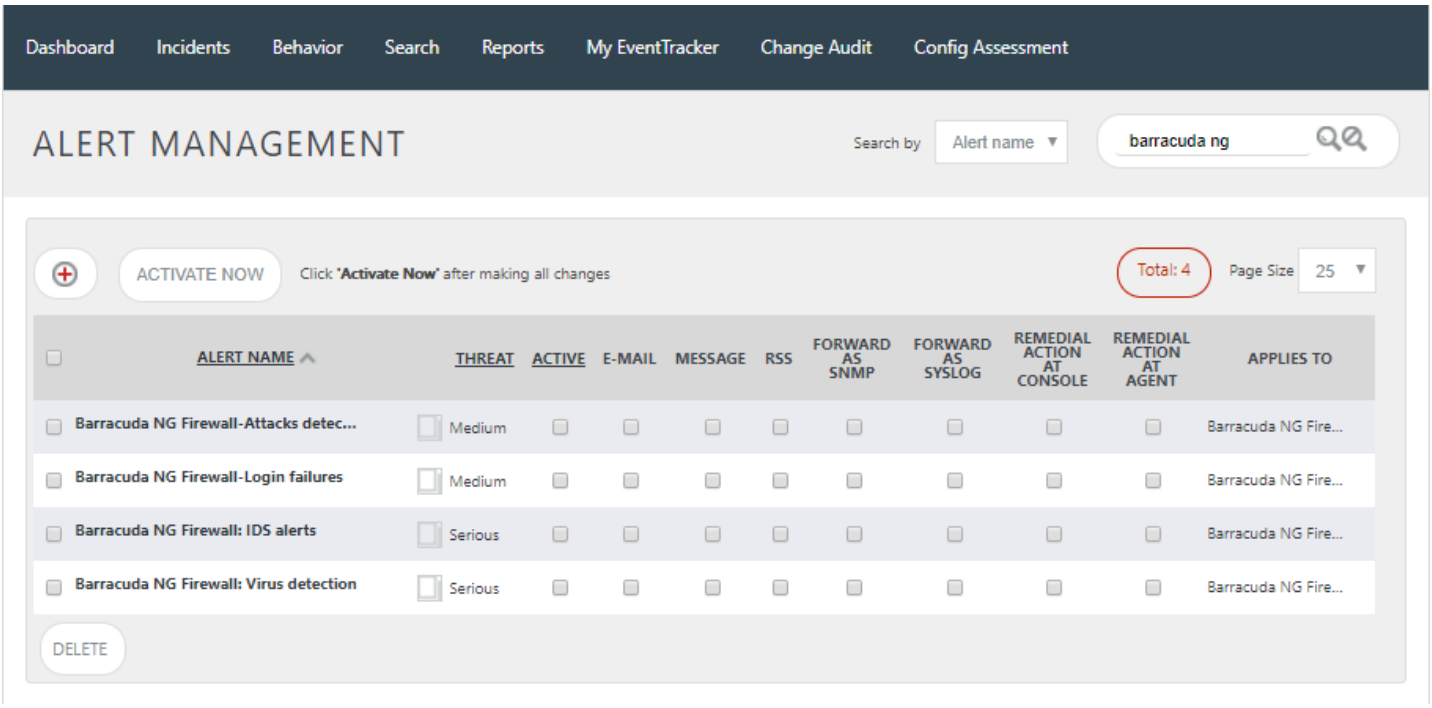

Figure 20

3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

Figure 21

4. Click the **OK** button, and then click the **Activate now** button.

NOTE:

- You can select alert notification such as beep, email, and message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

5.2 Token Template

1. Logon to **EventTracker** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.
3. Click on **Barracuda NG Firewall** group option.

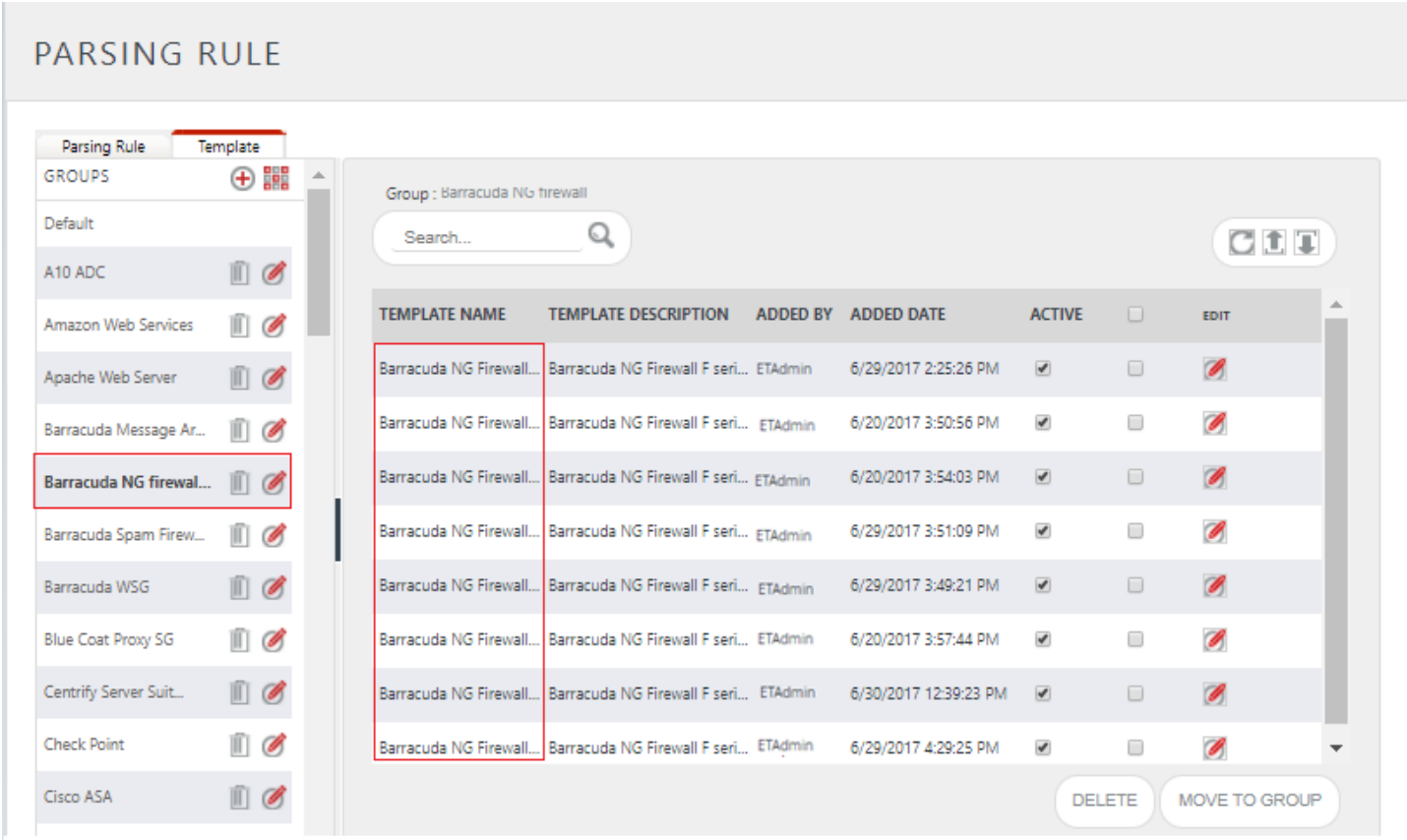

Figure 22

5.3 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**Barracuda NG Firewall**, and then click the **Search** button.

EventTracker displays Flex reports of '**Barracuda NG Firewall.**

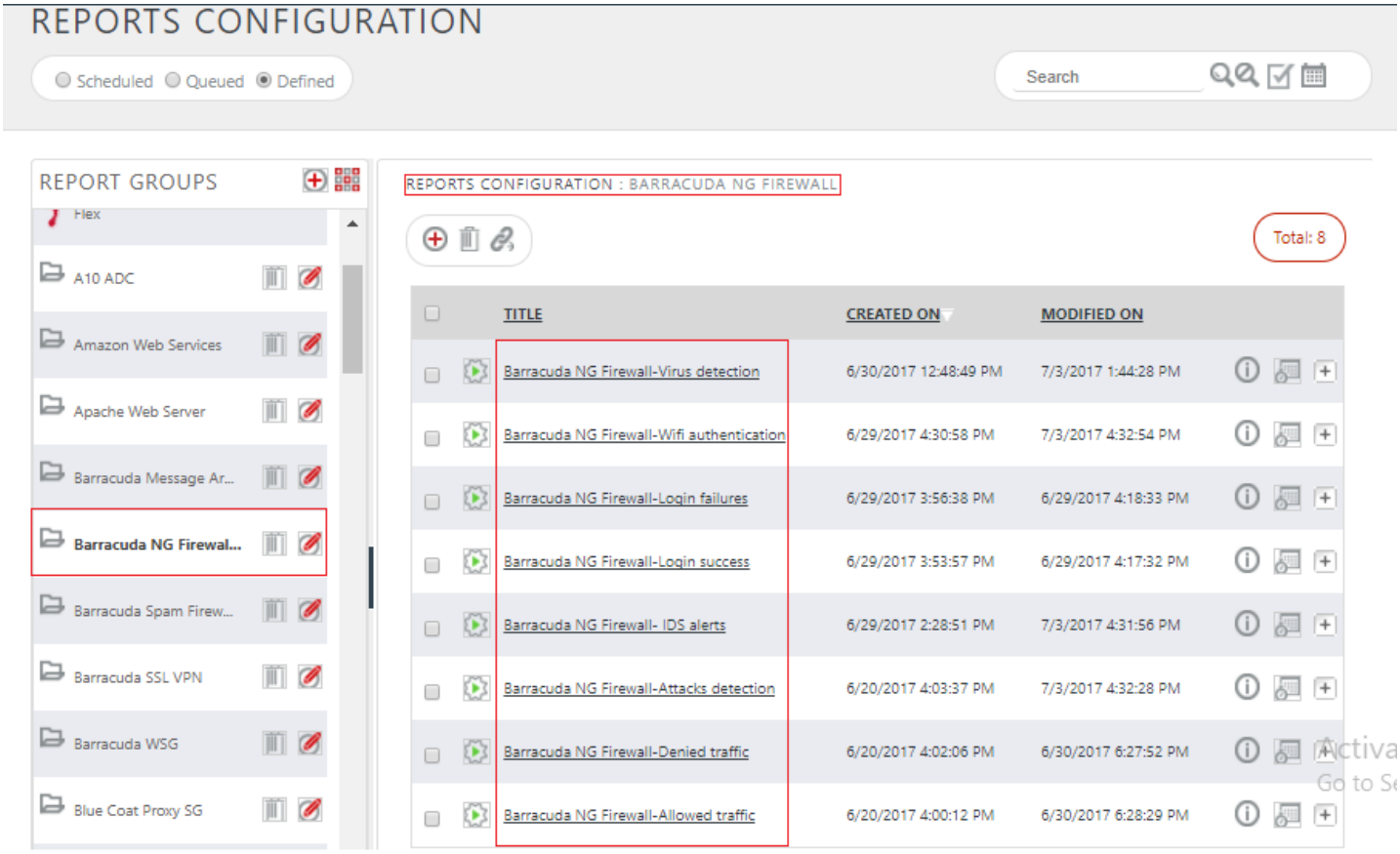

Figure 23

6. Creating Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker v8.0.

6.1 Schedule Reports

1. Open **EventTracker** in browser and logon.

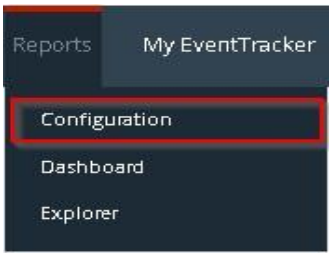

Figure 24

2. Navigate to **Reports>Configuration**.
3. Select **Barracuda NG Firewall** in report groups. Check **Defined** dialog box.

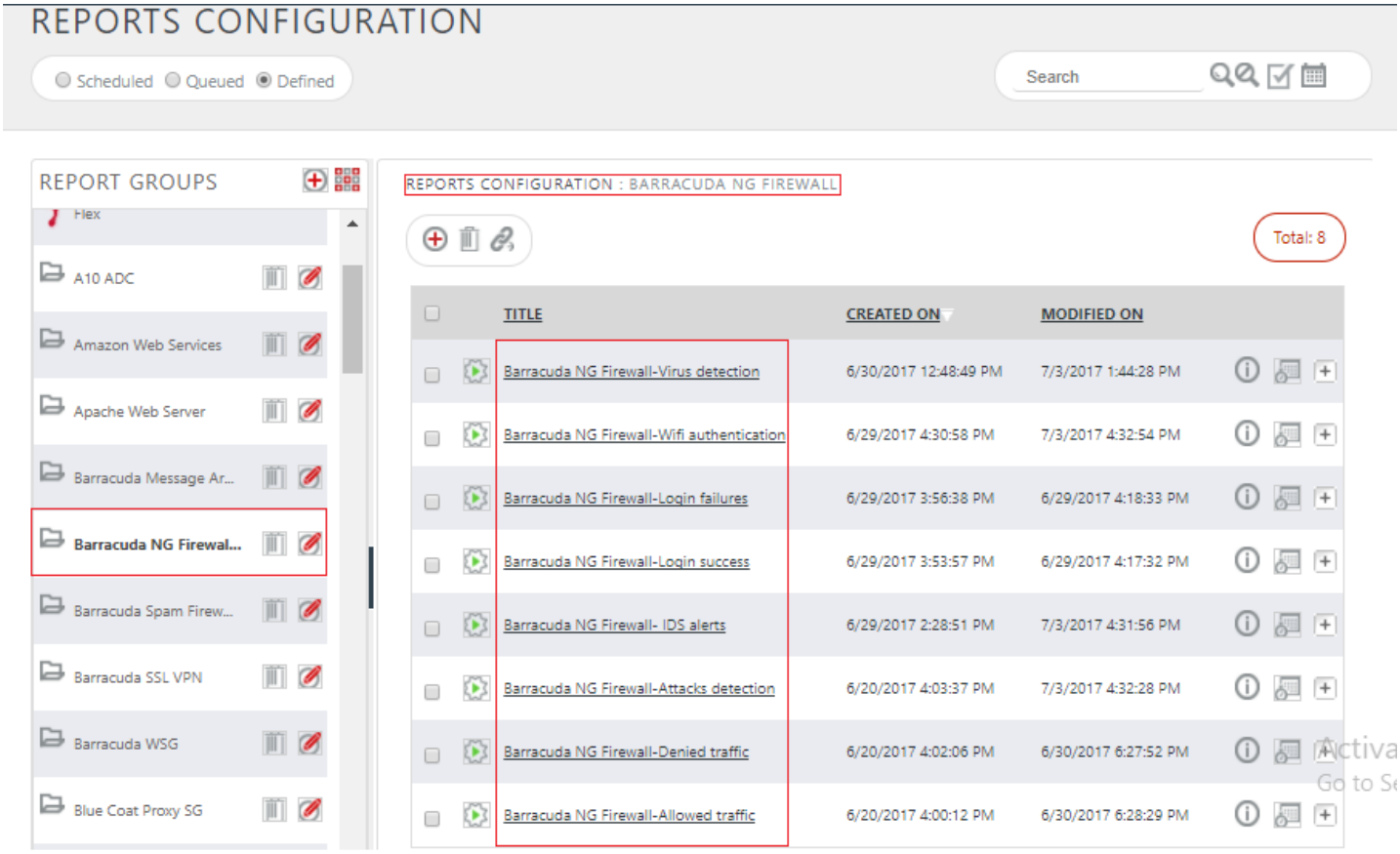

Figure 25

4. Click on '**schedule**'  to plan a report for later execution.
5. Click **Next** to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

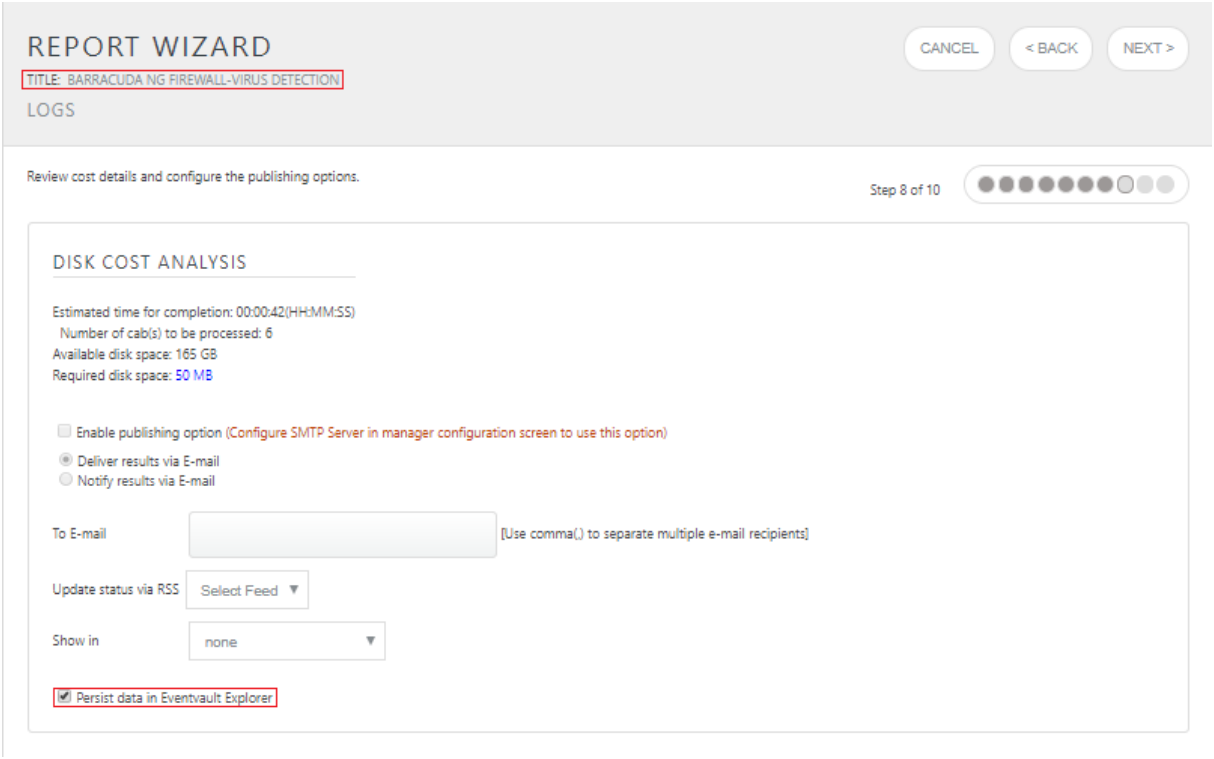

Figure 26

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

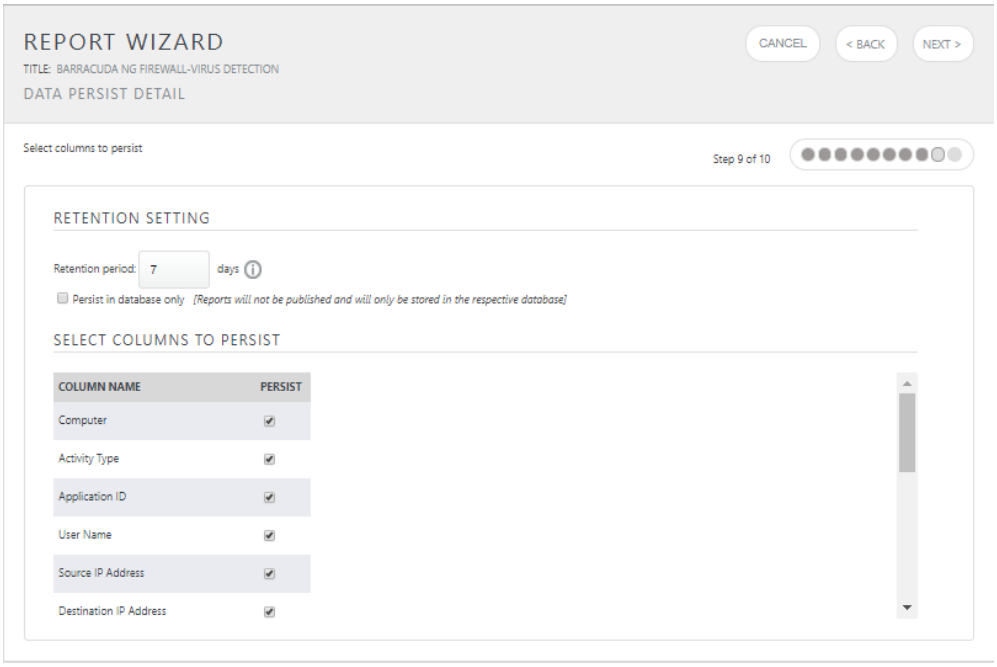

Figure 27

8. Proceed to next step and click **Schedule**.
9. Wait till the reports get generated.

6.2 Create Dashlets

1. Open **EventTracker** in browser and logon.

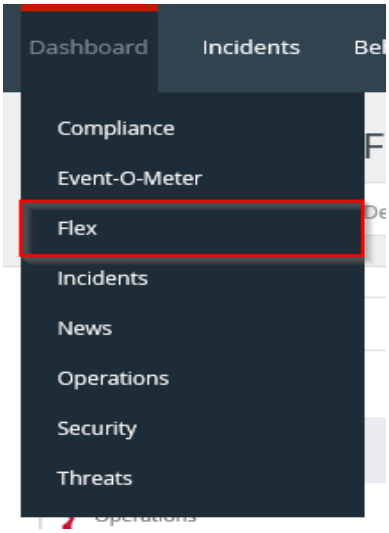

Figure 28

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

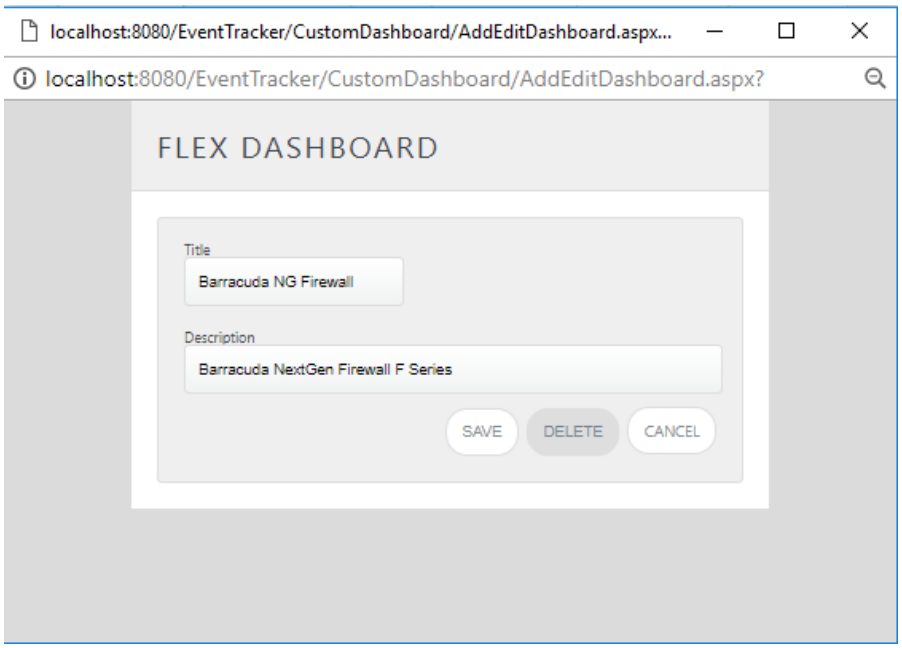

Figure 29

3. Fill suitable title and description and click **Save**.
4. Click to configure a new flex dashlet. Widget configuration pane is shown.

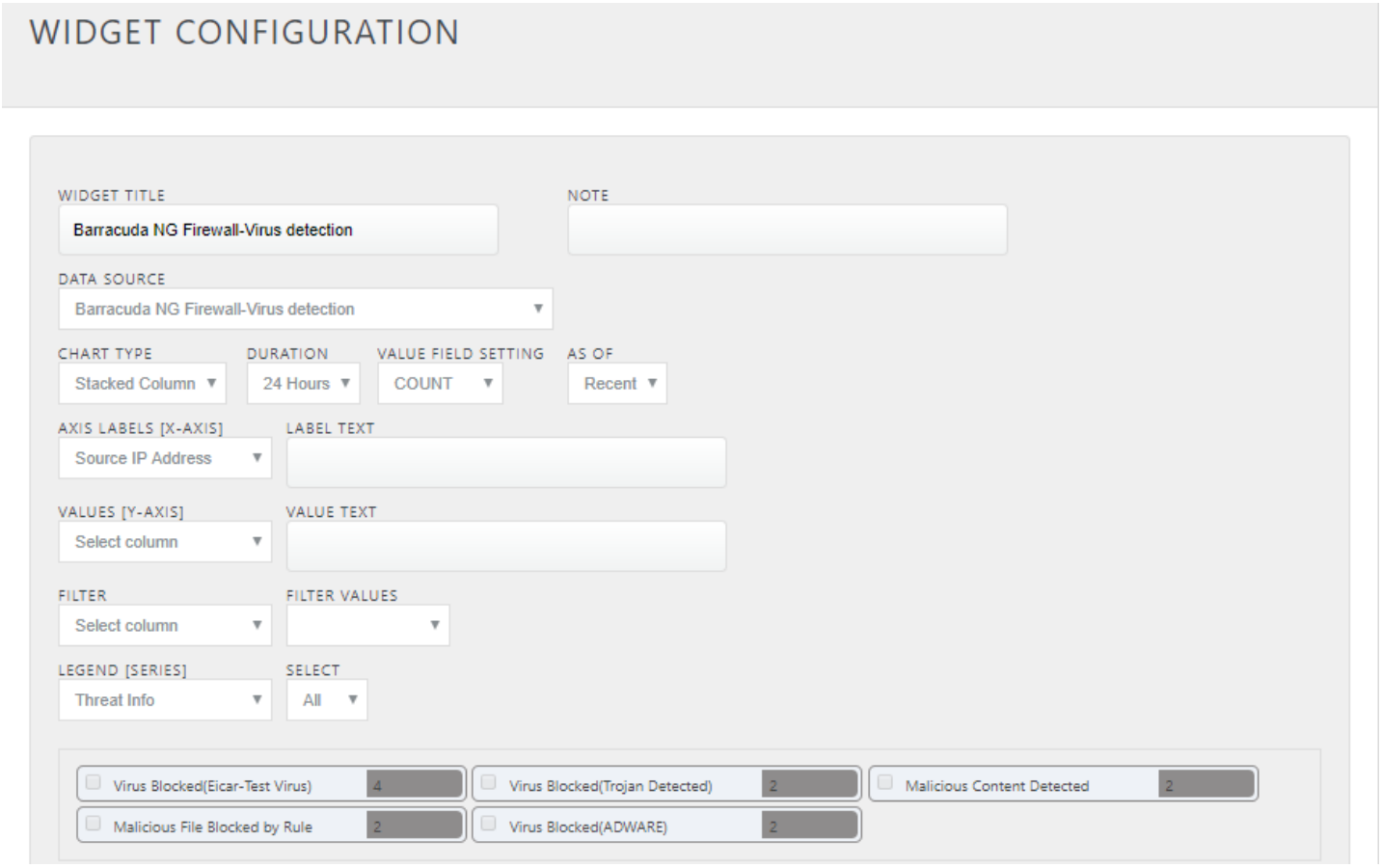

Figure 30

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** to evaluate. Evaluated chart is shown.

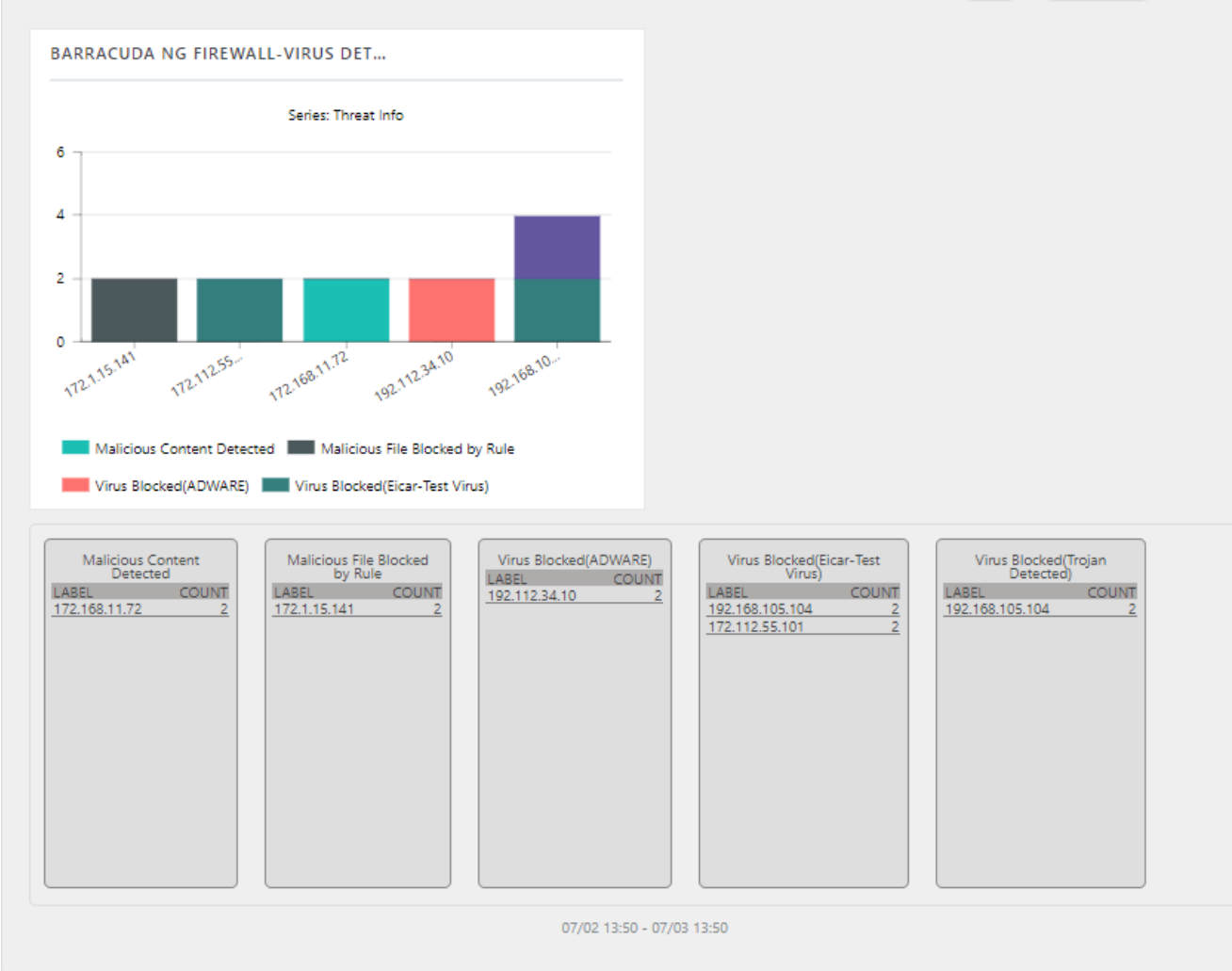

Figure 31

14. If satisfied, click **Configure**.

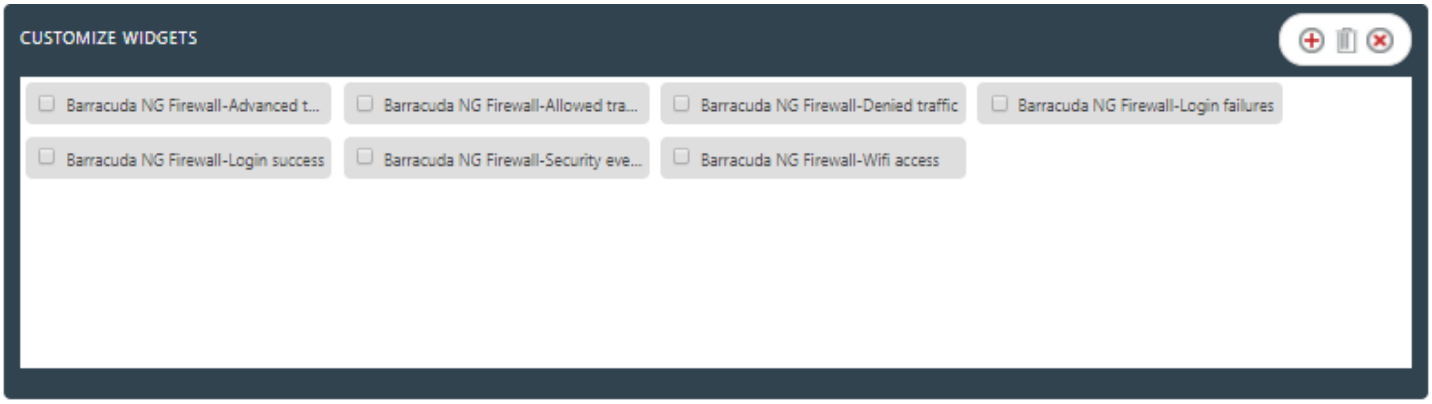

Figure 32

15. Click 'customize' to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

6.3 Sample Flex Dashboards

- **REPORT: Barracuda NG Firewall-Allowed traffic**
  WIDGET TITLE: Barracuda NG Firewall-Allowed traffic
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND[SERIES]: Activity Type

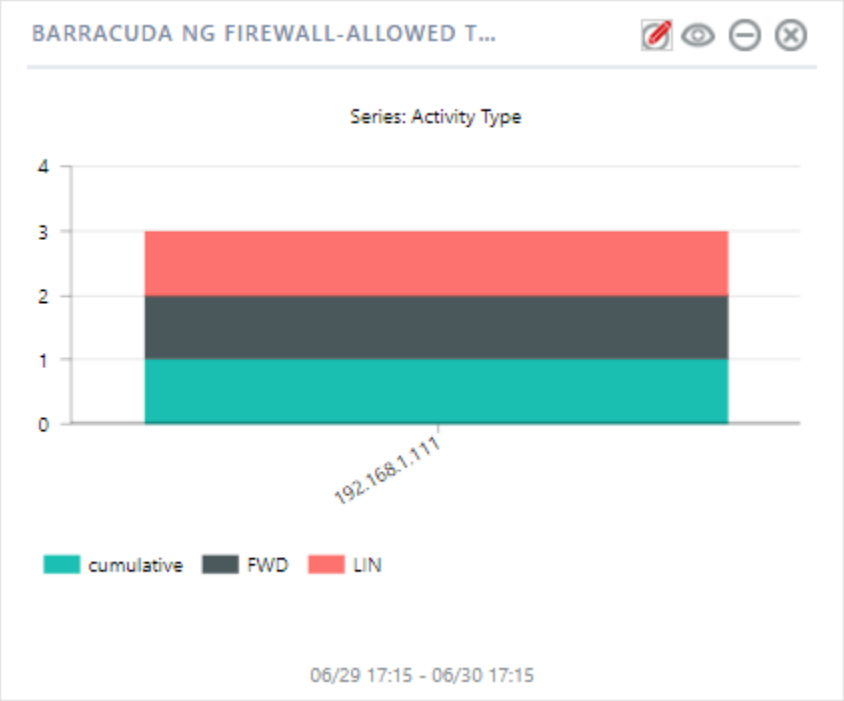

Figure 33

- **REPORT: Barracuda NG Firewall-Denied traffic**
  WIDGET TITLE: Barracuda NG Firewall-Denied traffic
  CHART TYPE: PIE
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND[SERIES]: Rule Description

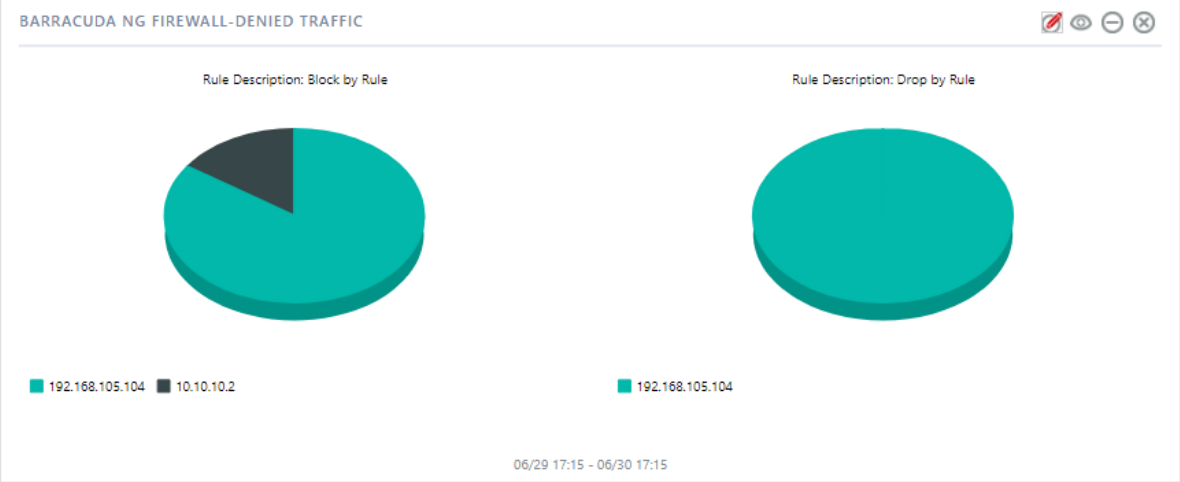

Figure 34

- **REPORT: Barracuda NG Firewall-Login success**
  WIDGET TITLE: Barracuda NG Firewall-Login success
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: User-Name
  LEGEND[SERIES]: Action

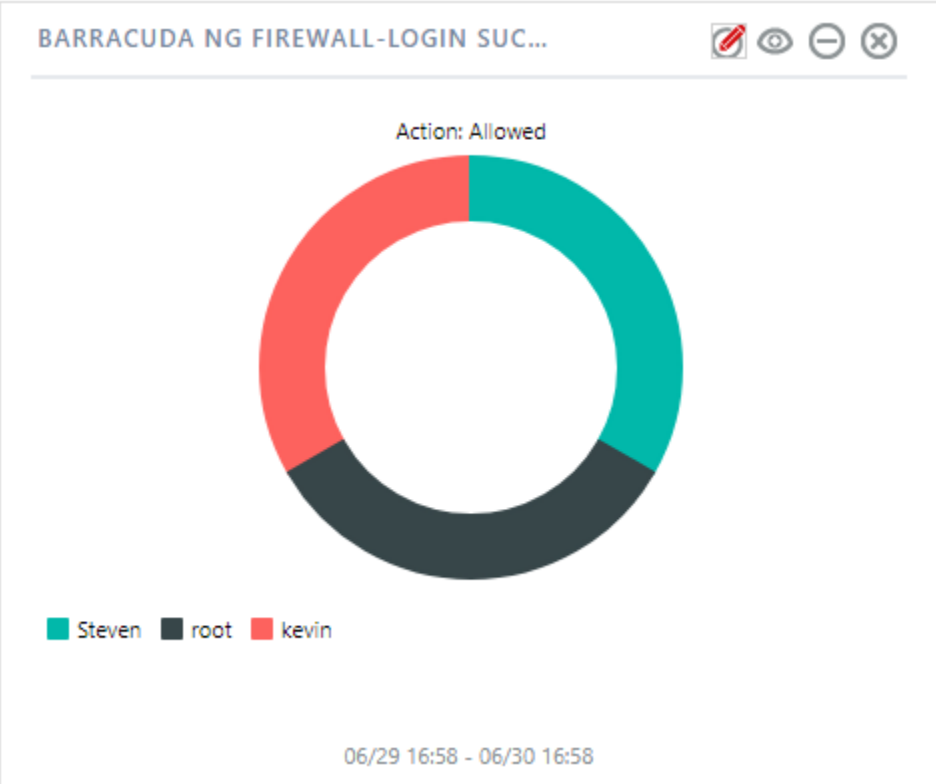

Figure 35

- **REPORT: Barracuda NG Firewall-Login failures**
  WIDGET TITLE: Barracuda NG Firewall-Login failures
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: User-Name
  LEGEND[SERIES]: Reason

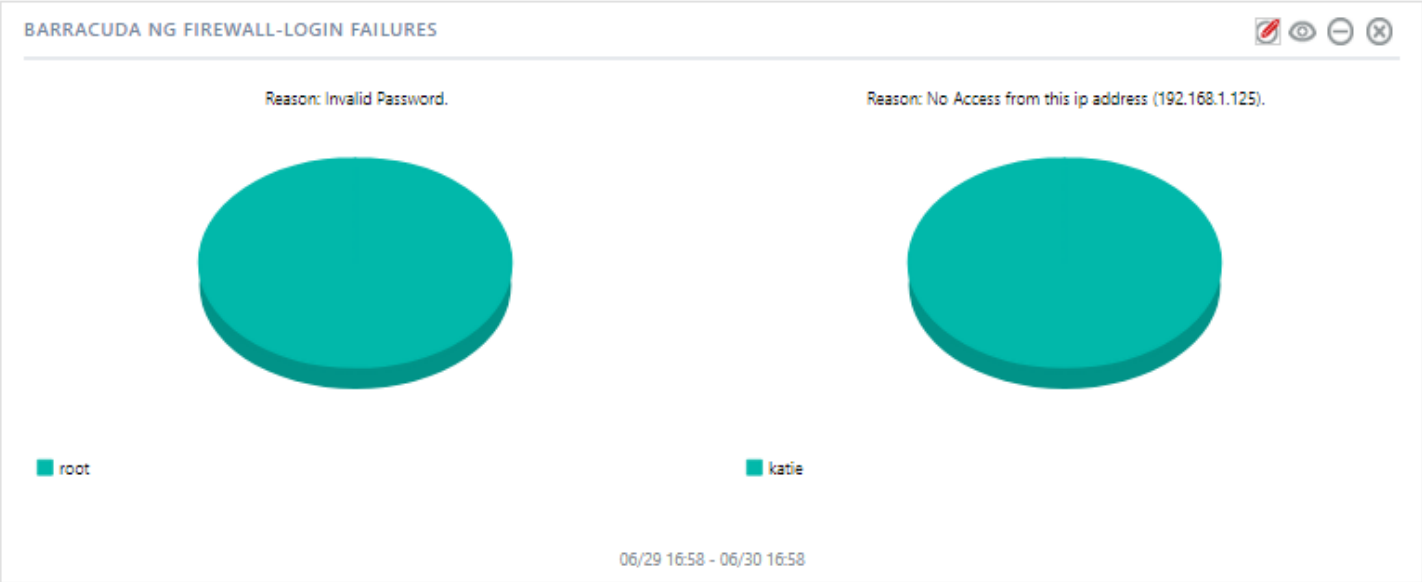

Figure 36

- **REPORT: Barracuda NG Firewall-IDS alerts**
  WIDGET TITLE: Barracuda NG Firewall-IDS alerts
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Threat File
  LEGEND: Risk

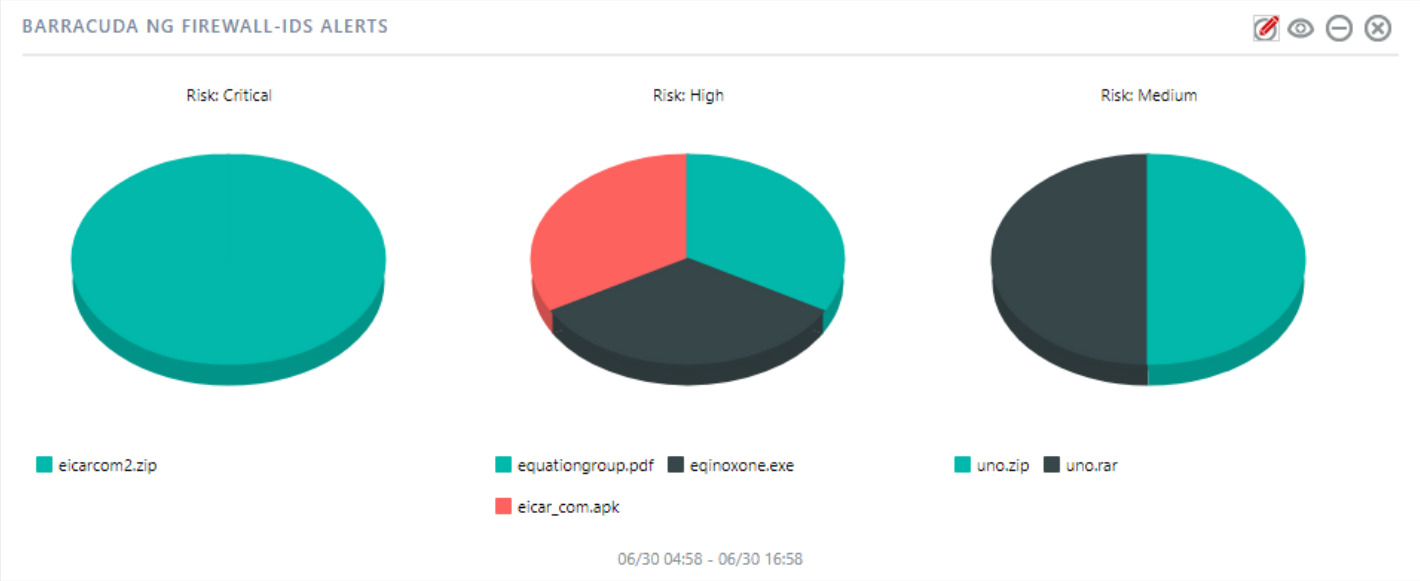

Figure 37

- **REPORT: Barracuda NG Firewall-Wi-fi authentication**
  WIDGET TITLE: Barracuda NG Firewall-Wi-fi authentication
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: User-Name
  LEGEND[SERIES]: Client IP Address

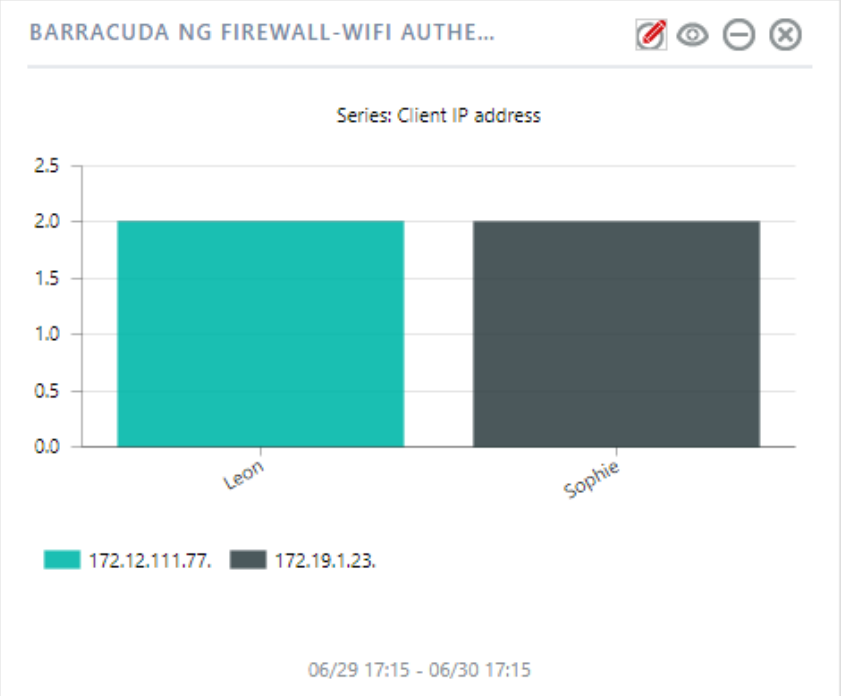

Figure 38