

# Integrate Meraki Firewall

---

*EventTracker Enterprise*

Publication Date: April 5, 2016

EventTracker  
8815 Centre Park Drive  
Columbia MD 21045  
[www.eventtracker.com](http://www.eventtracker.com)

# Abstract

This guide provides instructions to configure a Meraki Firewall to report its logs to EventTracker Enterprise.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and **Meraki security appliance MX series**.

## Audience

Administrators, who wish to monitor Meraki Firewall using EventTracker Enterprise.

*The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

|  |    |
|--|----|
| Abstract.....  | 1  |
| Scope.....   | 1  |
| Audience.....  | 1  |
| Introduction .....   | 3  |
| Pre-requisites.....  | 3  |
| Enable syslog logging.....                                     | 3  |
| EventTracker Knowledge Pack (KP).....                          | 4  |
| Reports.....   | 4  |
| Categories .....   | 7  |
| Alerts.....  | 8  |
| Knowledge Object.....  | 8  |
| Import Meraki Firewall Knowledge Pack into EventTracker.....   | 8  |
| Import Token Templates.....                                    | 9  |
| Import Categories .....  | 11 |
| Import Alerts.....   | 12 |
| Import Flex Reports.....                                       | 13 |
| Import Knowledge Object.....                                   | 14 |
| Verifying Meraki Firewall knowledge pack in EventTracker ..... | 16 |
| Token Templates.....   | 16 |
| Categories .....   | 17 |
| Alerts.....  | 18 |
| Flex Reports.....  | 19 |
| Knowledge Object.....  | 20 |
| Create Dashboards in EventTracker.....                         | 21 |
| Schedule Reports.....  | 21 |
| Create Dashlets.....   | 24 |
| Sample Dashboards.....   | 28 |

# Introduction

Meraki Firewalls are cloud-managed network security appliances designed to make distributed networks fast, secure, manageable by employing stateful inspection and auto-configuring VPN options.

EventTracker amasses and examines logs generated by Meraki Firewall to help an administration to monitor ids, alerts, VPN sessions, web traffic etc.

## Pre-requisites

- Administrative access to Meraki Dashboard.

## Enable syslog logging

To configure a Meraki Firewall to forward logs to a syslog server;

1. Logon to Meraki Dashboard and select firewall device. From there, click on **Alerts & administration**.
2. At the **Alerts & administration** page scroll down to the Logging section.

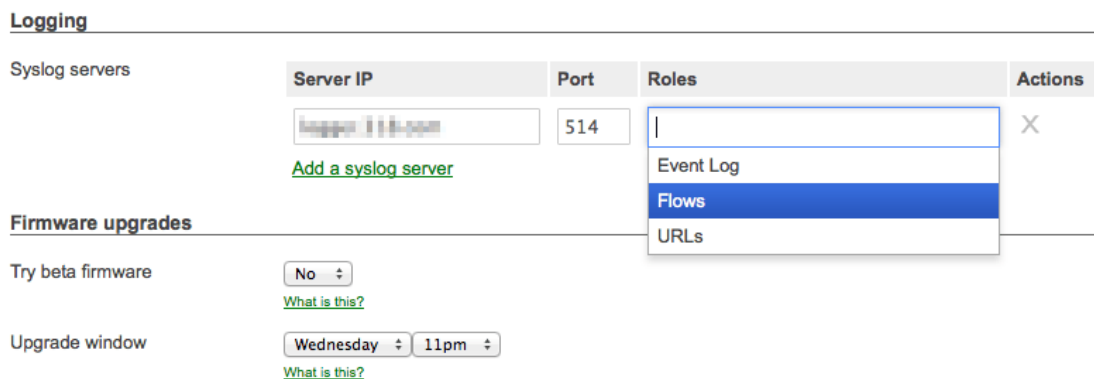


Figure 1

3. Click on the **Add a syslog server** link and type the IP address or name of **EventTracker Manager** in **Server IP** field.
4. Type **514** in the **Port** field.
5. Choose **Event Log, IDS Alerts, Flows and URLs**; in **Roles** field. Mentioned log types are detailed below:

| Log Type   | Log Details                                  |
|------------|--|
| Event Log  | Messages under <b>Monitor &gt; Event log</b> |
| Flows      | Inbound and outbound traffic flows           |
| URL        | HTTP/HTTPS GET requests                      |
| IDS Alerts | Alerts generated by IDS                      |

Table 1

Sample configuration is shown below.



Figure 2

Integrated device can be verified in systems pane of EventTracker advanced log search.

## EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker; Categories, Alerts, Reports and Dashboards can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Meraki Firewall monitoring.

### Reports

- **Meraki Firewall- Blocked web content details**  
This report provides information related to web content blocked by content filter.

| LogTime                | Device Name | Server Address | Server Port | Blocked Category                | Blocked URL   |
|------------------------|-------------|----------------|-------------|---------------------------------|---|
| 03/30/2016 07:53:40 PM | MX64        | 174.76.226.93  | 80          | User-defined Blacklist          | http://img2.imagesbn.com/p/2940043877833_p0_v2_s600_e404.png;                         |
| 03/30/2016 07:53:49 PM | MX64        | 184.105.82.3   | 443         | User-defined Blacklist          | https://*.cloudmosa.com/...   |
| 03/30/2016 07:54:01 PM | MX64        | 67.215.65.130  | 80          | Proxy Avoidance and Anonymizers | http://q99.info/wp-content/uploads/2013/12/posted-the-wizard-saturday-july-48090.jpg; |
| 04/01/2016 04:54:48 PM | MX64        | 52.86.88.235   | 443         | Dating                          | https://api.gotinder.com/...  |
| 04/04/2016 10:30:07 AM | MX64        | 174.76.226.93  | 80          | User-defined Blacklist          | http://img2.imagesbn.com/p/2940043877833_p0_v2_s600_e404.png;                         |

Figure 3

```
Apr 01 05:31:08 192.168.1.58 1 1392859657.308826035 Meraki_Security_Appliance events content_filtering_block url='http://img2.imagesbn.com/p/2940043877833_p0_v2_s600_e404.png'; category0='User-defined Blacklist' server='174.76.226.93:80'
```

- **Meraki Firewall- VPN session details**

This report provides information related to VPN sessions establishment, connection or disconnection.

| LogTime                | Device Name | VPN Type         | VPN Status     | User Name | Source IP      | Source Port | Destination IP  | Destination Port |
|------------------------|-------------|------------------|----------------|-----------|----------------|-------------|-----------------|------------------|
| 03/30/2016 07:10:26 PM | MX60        | Site-to-site VPN | established    |           | 24.249.102.115 | 4500        | 70.168.64.32    | 4500             |
| 03/30/2016 07:10:36 PM | MX60        | client_vpn       | vpn_connect    | astaubin  | 70.168.64.32   |             | 192.168.251.122 |                  |
| 03/30/2016 07:10:45 PM | MX60        | client_vpn       | vpn_disconnect | astaubin  | 70.168.64.32   |             | 192.168.251.122 |                  |

Figure 4

```
Apr 01 05:31:08 192.168.1.58 1 1392808395.669667263 Meraki_Security_Appliance events Site-to-site VPN: IPsec-SA established: ESP/Transport 24.249.102.115[4500]->70.168.64.32[4500] spi=120847356(0x733fbfc)
```

```
Apr 01 05:31:08 192.168.1.58 1 1392808392.258224600 Meraki_Security_Appliance events client_vpn_disconnect user id 'astaubin' local ip 192.168.251.122 connected from 70.168.64.32
```

```
Apr 01 05:31:08 192.168.1.58 1 1459444533.502384019 Meraki_Security_Appliance events type=route_connection_change peer_type='l3_vpn' peer='00:18:0A:86:86:4C' connection_status='connected'
```

- **Meraki Firewall- User authentication details**

This report provides information related to local user authentication attempt.

| LogTime                | Device Name | Host MAC          | User Name | User Details   | Group Details   |
|------------------------|-------------|-------------------|-----------|--|---|
| 03/30/2016 03:36:30 PM | MX64        | 00:1E:0B:3E:42:DD | TTobey    | CN=Tami Tobey,OU=Teachers,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org        | CN=Teachers,OU=Teachers,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org             |
| 03/30/2016 03:36:43 PM | MX64        | 90:B1:1C:79:1C:50 | JWolfe    | CN=Janet Wolfe,OU=Administration,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org | CN=Administration,OU=Administration,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org |
| 03/30/2016 03:36:54 PM | MX64        | 00:0B:DB:73:F1:78 | student   | CN=Student Guest,OU=Students,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org     | CN=Students,OU=Students,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org             |

Figure 5

Apr 01 05:31:08 192.168.1.58 1 1 1392792900.051011956 Meraki\_Security\_Appliance events authentication on 00:1E:0B:3E:42:DD for user TTobey as CN=Tami Tobey,OU=Teachers,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org with policy for group CN=Teachers,OU=Teachers,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org

- Meraki Firewall- DHCP IP lease details**

This report provides information related to IPs leased by DHCP.

| LogTime                | Device Name | Server MAC        | Client MAC        | Leased IP     | Allocated DNS            | Router IP  |
|------------------------|-------------|-------------------|-------------------|---------------|--------------------------|------------|
| 03/31/2016 06:03:47 PM | MX60        | 00:18:0A:02:85:88 | 00:18:0A:76:F9:79 | 172.16.37.220 | 172.16.1.200, 172.16.1.1 | 172.16.1.2 |
| 03/31/2016 06:08:20 PM | MX60        | 00:18:0A:02:85:88 | 00:18:08:06:9F:88 | 172.16.37.210 | 172.16.1.200, 172.16.1.1 | 172.16.1.2 |

Figure 6

Apr 01 05:31:08 192.168.1.58 1 1392793111.469320128 Meraki\_Security\_Appliance events dhcp lease of ip 172.16.37.220 from server mac 00:18:0A:02:85:88 for client mac 00:18:0A:76:F9:79 from router 172.16.1.2 on subnet 255.255.0.0 with dns 172.16.1.200, 172.16.1.1

- Meraki Firewall- IDS alert details**

This report provides information related to threats detected by IDS.

| LogTime                | Device Name | Source MAC        | Source IP       | Source Port | Destination MAC   | Destination IP | Destination Port | Protocol Type | Alert Priority | Alert Direction | Alert Details                          |                                   |
|------------------------|-------------|-------------------|-----------------|-------------|-------------------|----------------|------------------|---------------|----------------|-----------------|--|-----------------------------------|
| 03/29/2016 05:45:12 PM | MX60        | 03:99:9D:3B:F7:C5 | 192.168.251.122 | 61724       |                   | 172.16.1.90    | 22               | tcp/ip        | 2              | egress          | (spp_ssh) Protocol mismatch            |                                   |
| 03/29/2016 05:45:23 PM | MX60        |                   | 70.168.64.32    | 64697       | 00:1B:21:A2:73:C9 | 172.16.1.70    | 6690             | tcp/ip        | 3              | ingress         | Data sent on stream not accepting data |                                   |
| 03/29/2016 05:45:34 PM | MX60        |                   | 24.249.102.115  | 46865       |                   | 6.0.0.2        | 3128             | tcp/ip        | 2              |                 | (http_inspect) NON-RFC DEFINED CHAR    |                                   |
| 03/29/2016 05:45:43 PM | MX60        |                   | 72.246.55.50    | 80          | 04:15:52:5B:60:CC | 172.16.25.241  | 50449            | tcp/ip        | 2              | ingress         | Bad segment, adjusted size <= 0        |                                   |
| 03/29/2016 05:45:53 PM | MX60        | 20:C9:D0:BC:66:A3 |                 |             |                   |                |                  |               | 34525          | 3               | egress                                 | (spp_frag3) Fragmentation overlap |

Figure 7

Apr 01 05:31:08 192.168.1.58 1 1392812405.977854011 Meraki\_Security\_Appliance ids-alerts signature=128:4:1 priority=2 timestamp=1392812405.977656 shost=03:99:9D:3B:F7:C5 direction=egress protocol=tcp/ip src=192.168.251.122:61724 dst=172.16.1.90:22 message: (spp\_ssh) Protocol mismatch

- Meraki Firewall- Web traffic details**

This report provides information related to web traffic.

| LogTime                | Device Name | Source MAC        | Source IP  | Source Port | Destination IP | Destination Port | Request Type | Requested URI  |
|------------------------|-------------|-------------------|------------|-------------|----------------|------------------|--------------|--|
| 03/29/2016 12:40:56 PM | MX60        | 00:18:0A:77:1B:D7 | 172.16.0.1 | 1           | 192.168.0.1    | 80               | GET          | http://192.168.3.12/fog/service/servicemodule-active.php?mac=00:0F:20:FE:CA:A8&moduleid=snapiin' nc -v -u -w 0 172.16.1.90 552; done |
| 03/29/2016 12:41:07 PM | MX60        | 00:18:0A:77:1B:D7 | 172.16.4.6 | 52436       | 173.194.115.45 | 80               | GET          | http://testuser:testpassword@pagead2.googleadsyndication.com/simgad/2675983589122411580  |
| 03/29/2016 12:41:18 PM | MX60        | 00:18:0A:82:4E:26 | 172.16.4.3 | 41805       | 74.50.59.38    | 443              | UNKNOWN      | http://dsfsd.sdf   |

Figure 8

Apr 01 05:31:08 192.168.1.58 1 1392339100.728804745 Meraki\_Security\_Appliance urls src=172.16.4.6:52436 dst=173.194.115.45:80 mac=00:18:0A:77:1B:D7 request: GET http://testuser:testpassword@pagead2.googleadsyndication.com/simgad/2675983589122411580

- Meraki Firewall- Traffic flow details**  
 This report provides information related to inbound and outbound traffic flow.

| LogTime                | Device Name | Source MAC        | Source IP      | Source Port | Destination IP | Destination Port | Protocol Type | Rule Name |
|------------------------|-------------|-------------------|----------------|-------------|----------------|------------------|---------------|-----------|
| 03/29/2016 11:56:40 AM | MX10        |                   | 17.173.254.223 | 16387       | 24.249.102.115 | 1072             | udp           | 1 all     |
| 03/29/2016 11:56:50 AM | MX10        | 00:18:0A:77:1B:D7 | 172.16.4.21    | 53336       | 74.125.193.138 | 443              | tcp           | allow all |
| 03/29/2016 11:57:00 AM | MX60        |                   | 39.41.41.56    | 13943       | 114.18.74.11   | 16329            | udp           | 1 all     |
| 03/29/2016 11:57:08 AM | MX60        | 00:18:0A:98:L9:U7 | 192.168.10.254 | 9562        | 8.8.8.8        | 53               | udp           | allow all |

Figure 9

Apr 01 05:31:08 192.168.1.58 1 1392793163.700257235 Meraki\_Security\_Appliance flows src=17.173.254.223 dst=24.249.102.115 protocol=udp sport=16387 dport=1072 pattern: 1 all

## Categories

- Meraki Firewall: Content filtering** - This category provides information related to web content blocked by content filter.
- Meraki Firewall: DHCP IP leased** - This category provides information related to IPs leased by DHCP.
- Meraki Firewall: IDS alert detected** - This category provides information related to threats detected by IDS.
- Meraki Firewall: Traffic flow** - This category provides information related to ingress and egress traffic flow.
- Meraki Firewall: Web traffic** - This category provides information related to inbound and outbound web traffic.
- Meraki Firewall: User authentication attempt** - This category provides information related to local user authentication attempt.
- Meraki Firewall: VPN session** - This category provides information related to VPN sessions establishment, connection or disconnection.



## Alerts

- **Meraki Firewall: IDS alert detected** - This alert is generated when unusual traffic is detected by IDS.
- **Meraki Firewall: Suspicious web content blocked** - This alert is generated when suspicious content is blocked by content filter.

## Knowledge Object

- **Meraki Firewall** - This KO aids an administrator to analyze and visualize all the logs generated by Meraki Firewall.

# Import Meraki Firewall Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**, and then click the **Import** tab.

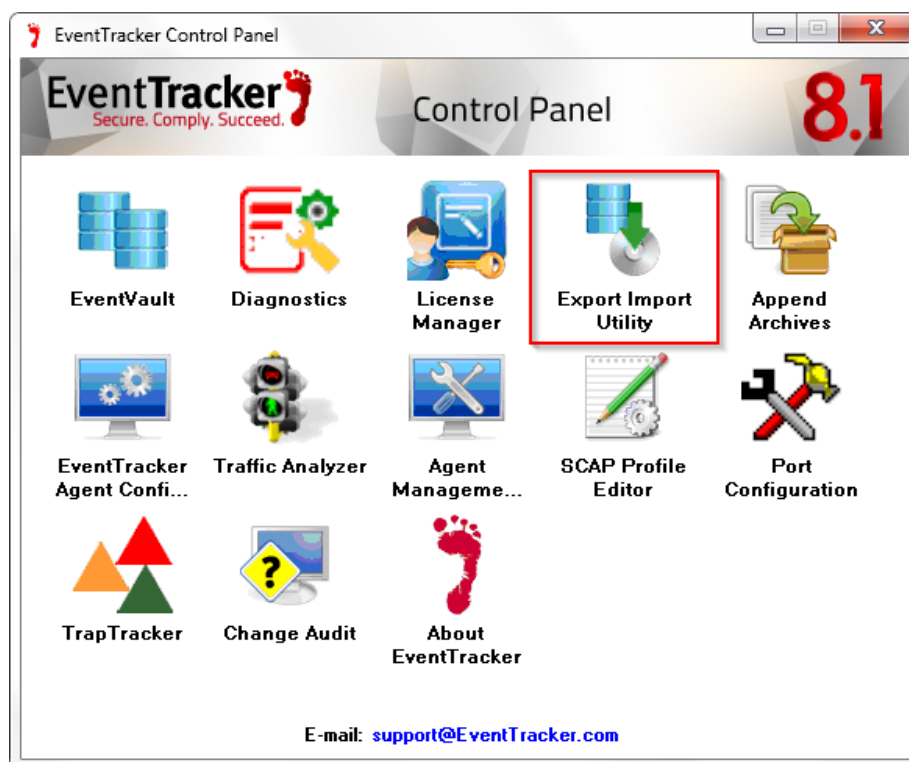



Figure 10

Please import KP items in the following sequence:

- **Token Templates**
- **Categories**
- **Alerts**
- **Reports**
- **Knowledge Objects**

Import **Token Templates, Categories, Alerts, Reports and Knowledge Objects** as given below.

## Import Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

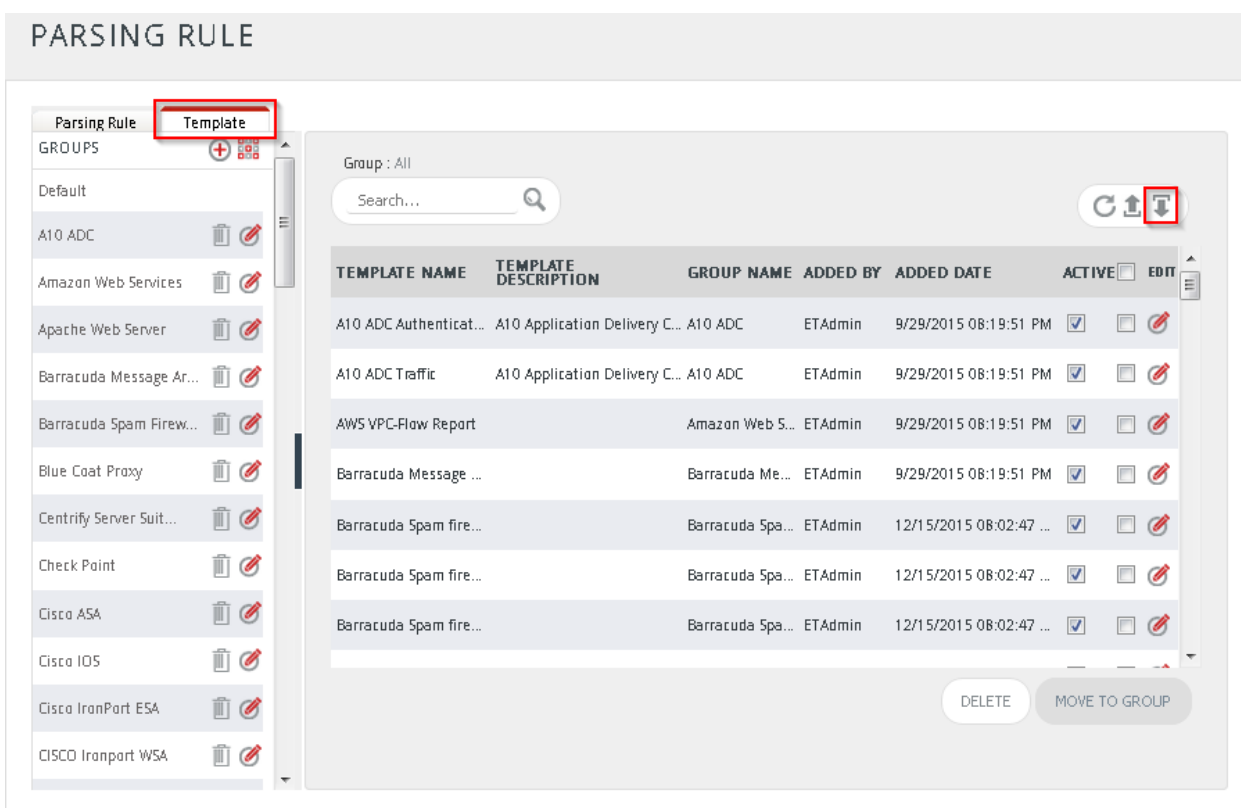


Figure 11

3. Click on **Browse** button.

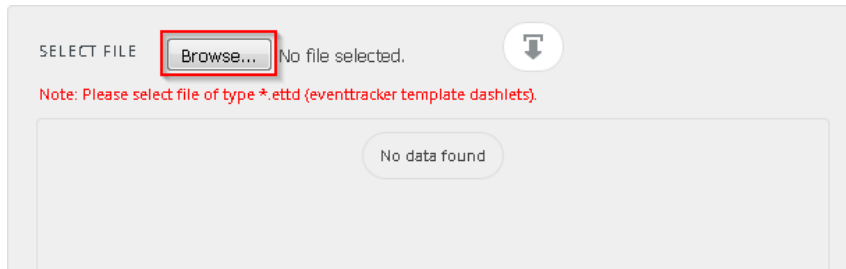


Figure 12

4. Locate **All Meraki Firewall token template.ettd** file, and then click the **Open** button.

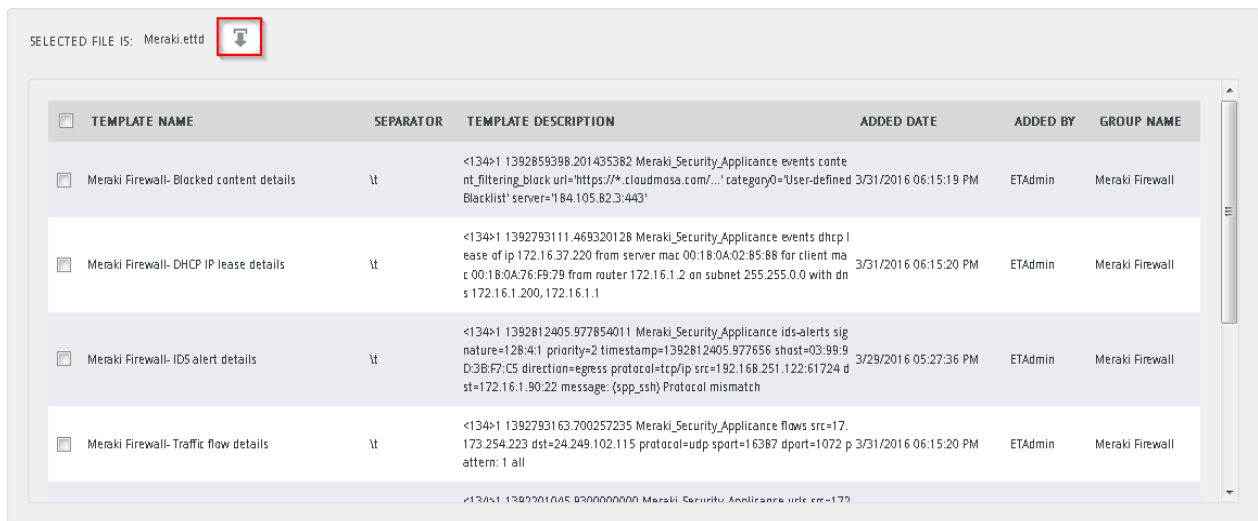


Figure 13

5. Now select the corresponding check boxes and then click on **Import** option.

EventTracker displays success message.

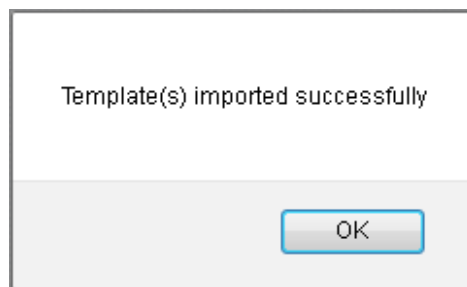



Figure 14

6. Click on **OK** button.

## Import Categories

1. Click **Category** option, and then click the **browse**  button.

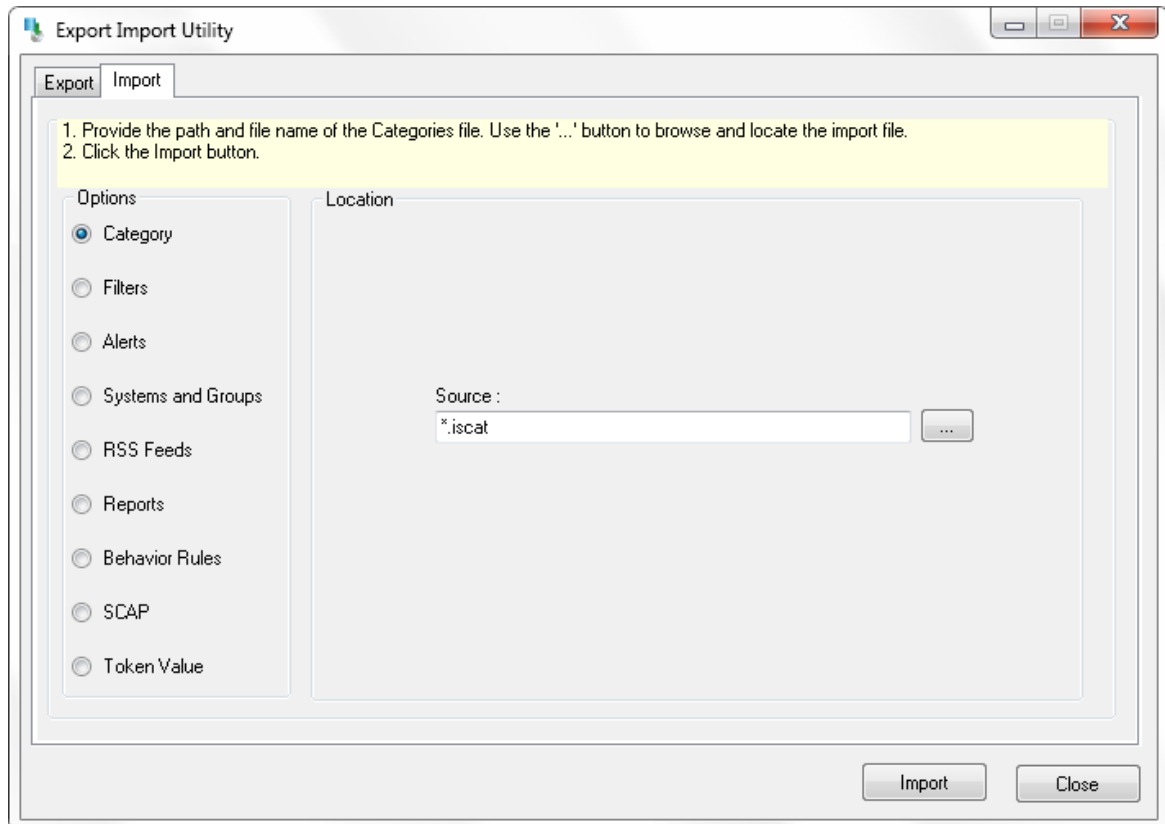


Figure 15

2. Locate **All Meraki Firewall categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

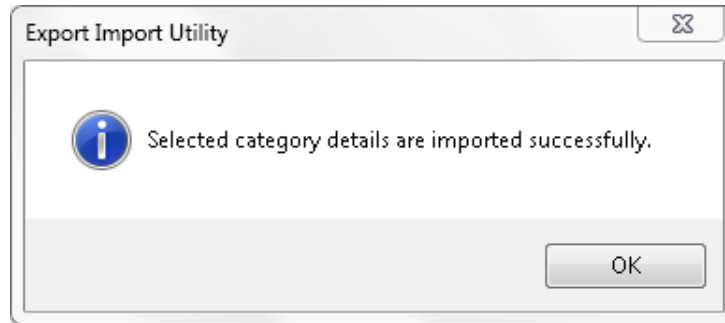



Figure 16

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

## Import Alerts

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

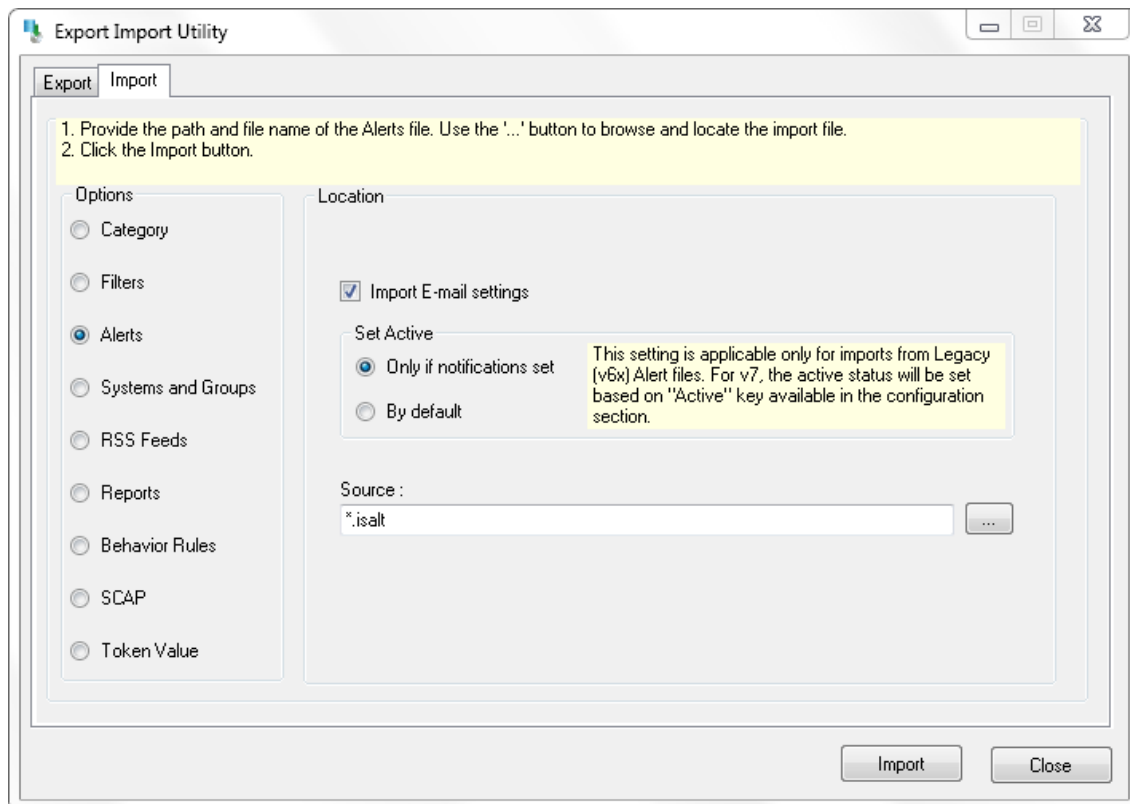


Figure 17

3. To import alerts, click the **Import** button.

EventTracker displays success message.

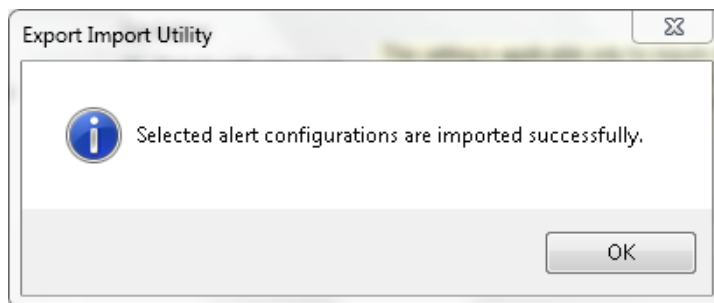



Figure 18

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

## Import Flex Reports

1. Click **Reports** option, and then click the '**browse**'  button.
2. Locate **All Meraki Firewall reports.issch** file, and then click the **Open** button.

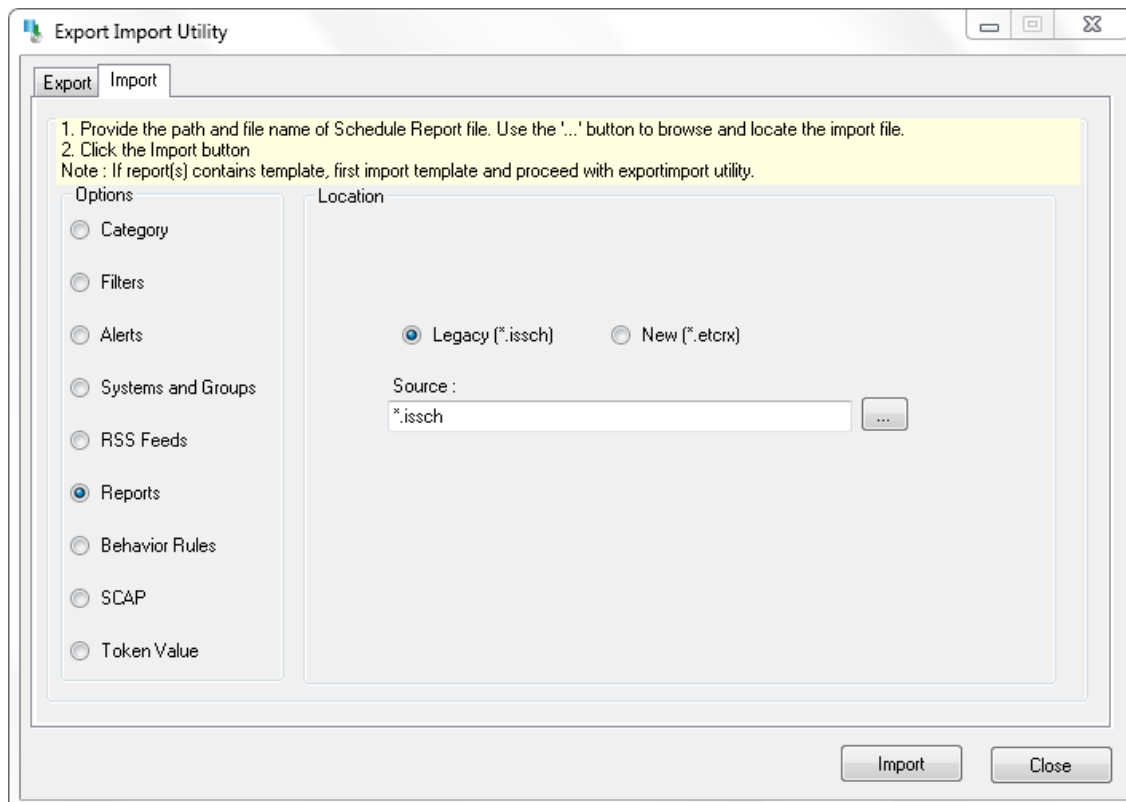


Figure 19

3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

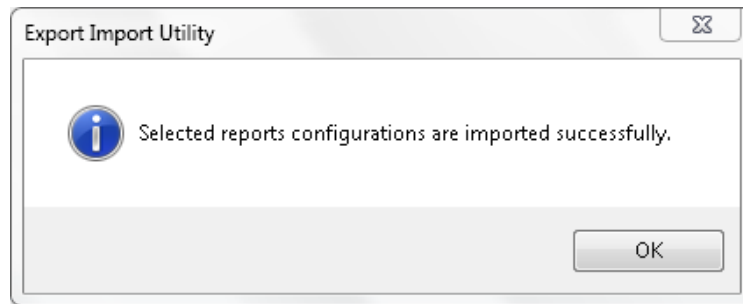


Figure 20

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

## Import Knowledge Object


1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on  'Import' option.



Figure 21

3. In **IMPORT** pane click on **Browse** button.

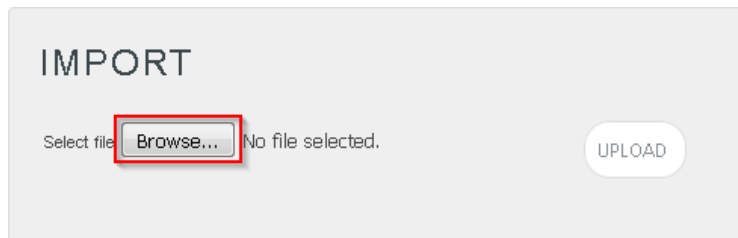


Figure 22

4. Locate **All Meraki Firewall KO.etko** file, and then click the **UPLOAD** button.

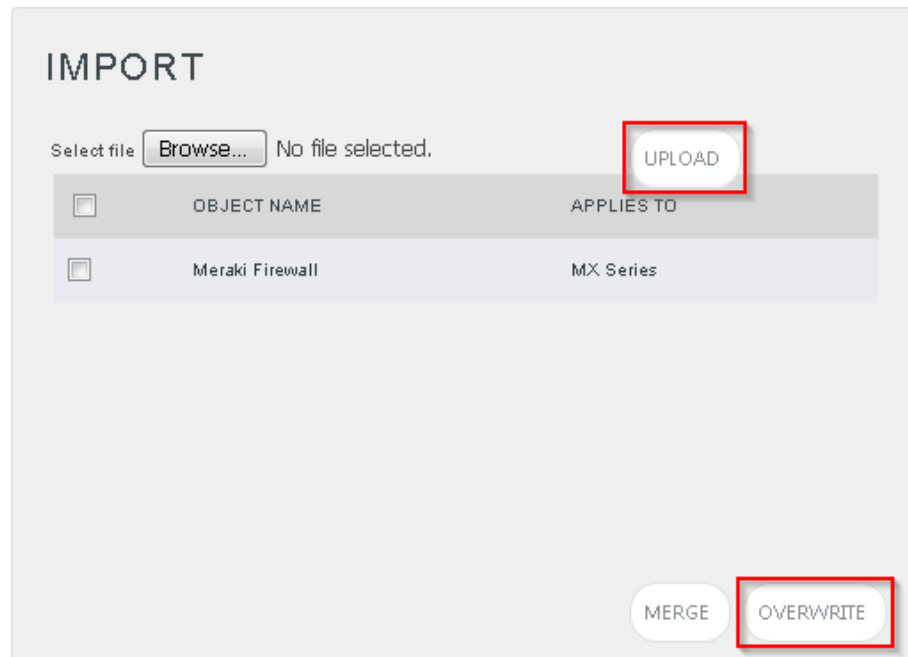


Figure 23

5. Now select the check box and then click on '**OVERWRITE**' option.

EventTracker displays success message.



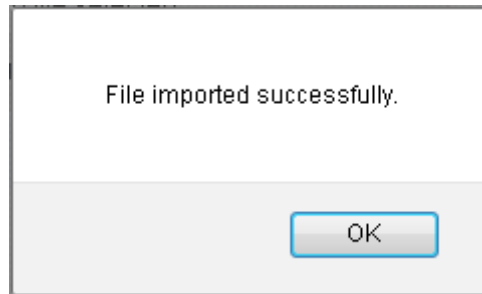


Figure 24

6. Click on **OK** button.

## Verifying Meraki Firewall knowledge pack in EventTracker

### Token Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing rule**.
3. Select **Template** tab.
4. In **Token Templates Groups Tree**, select **Meraki Firewall group** folder.

Imported token templates are shown on the right pane.

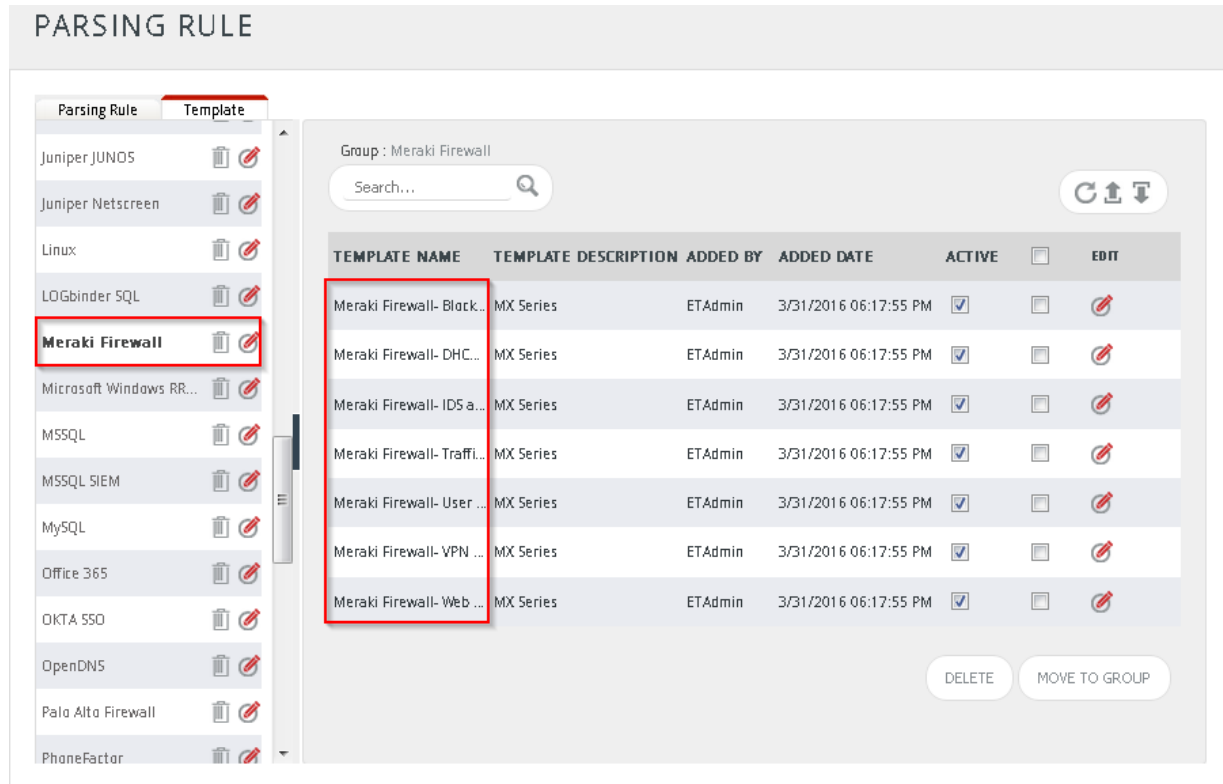


Figure 25

## Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. In the **Category Tree**, navigate to **Meraki->Meraki Firewall** group folder.

## CATEGORY MANAGEMENT

Category Tree Search

- Linux
  - Linux Cracking
  - Linux Violation
  - LOGbinder SP
  - LOGbinder SQL
  - McAfee IntruShield
  - McAfee Sidewinder Firewall
  - Meraki**
    - Meraki Firewall**
      - Meraki Firewall: Content filtering
      - Meraki Firewall: DHCP IP leased
      - Meraki Firewall: Ids-alerts detect
      - Meraki Firewall: Traffic flow
      - Meraki Firewall: User authenticat
      - Meraki Firewall: VPN session
      - Meraki Firewall: Web traffic
  - Microsoft Forefront
  - Microsoft Windows Hyper V
  - Microsoft Windows RRAS
  - Motorola
  - MySQL
  - Netscreen
  - OKTA SSO
  - OpenDNS Umbrella Insights and Platform


Total category groups: 361 Total categories: 3,118

Last 10 modified categories

| NAME   | MODIFIED DATE         | MODIFIED BY |
|--|-----------------------|-------------|
| Meraki Firewall: Web traffic                 | 4/1/2016 03:50:07 PM  | ETAdmin     |
| Meraki Firewall: DHCP IP leased              | 3/31/2016 06:55:44 PM | ETAdmin     |
| Meraki Firewall: Content filtering           | 3/31/2016 06:54:55 PM | ETAdmin     |
| Meraki Firewall: Ids-alerts detected         | 3/31/2016 06:20:18 PM |             |
| Meraki Firewall: Traffic flow                | 3/31/2016 06:20:18 PM |             |
| Meraki Firewall: User authentication attempt | 3/31/2016 06:20:18 PM |             |
| Meraki Firewall: VPN session                 | 3/31/2016 06:20:18 PM |             |
| FortiGate(4.0): Activex script removed       | 1/11/2016 03:56:53 AM |             |
| FortiGate(4.0): Admin account locked         | 1/11/2016 03:56:53 AM |             |
| FortiGate(4.0): Admin account timed out      | 1/11/2016 03:56:53 AM |             |

Figure 26

## Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and select **Alerts**.
3. In **Search** field, type '**Meraki Firewall**', and then click the  button.

Alert Management page will display all the imported Meraki Firewall alerts.

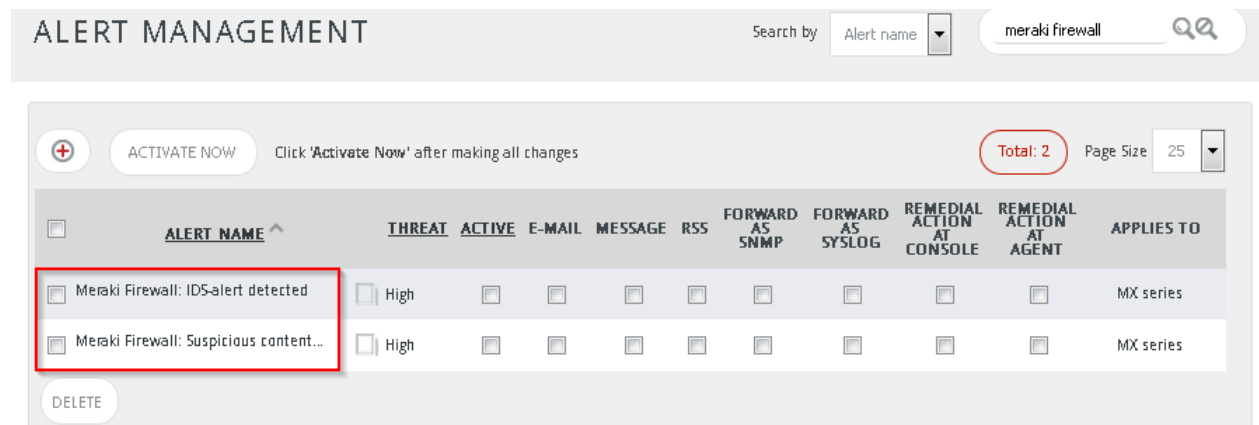


Figure 27

- To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

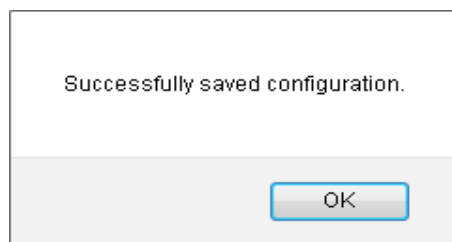


Figure 28

- Click **OK**, and then click the **Activate Now** button.

**NOTE:** Please specify appropriate **systems** in **alert configuration** for better performance.

## Flex Reports

- Logon to **EventTracker Enterprise**.
- Click the **Reports** menu and select **Configuration**.
- Select **Defined** in report type.
- In **Report Groups Tree**, select **Meraki Firewall group** folder.

Imported reports are displayed on the right pane.

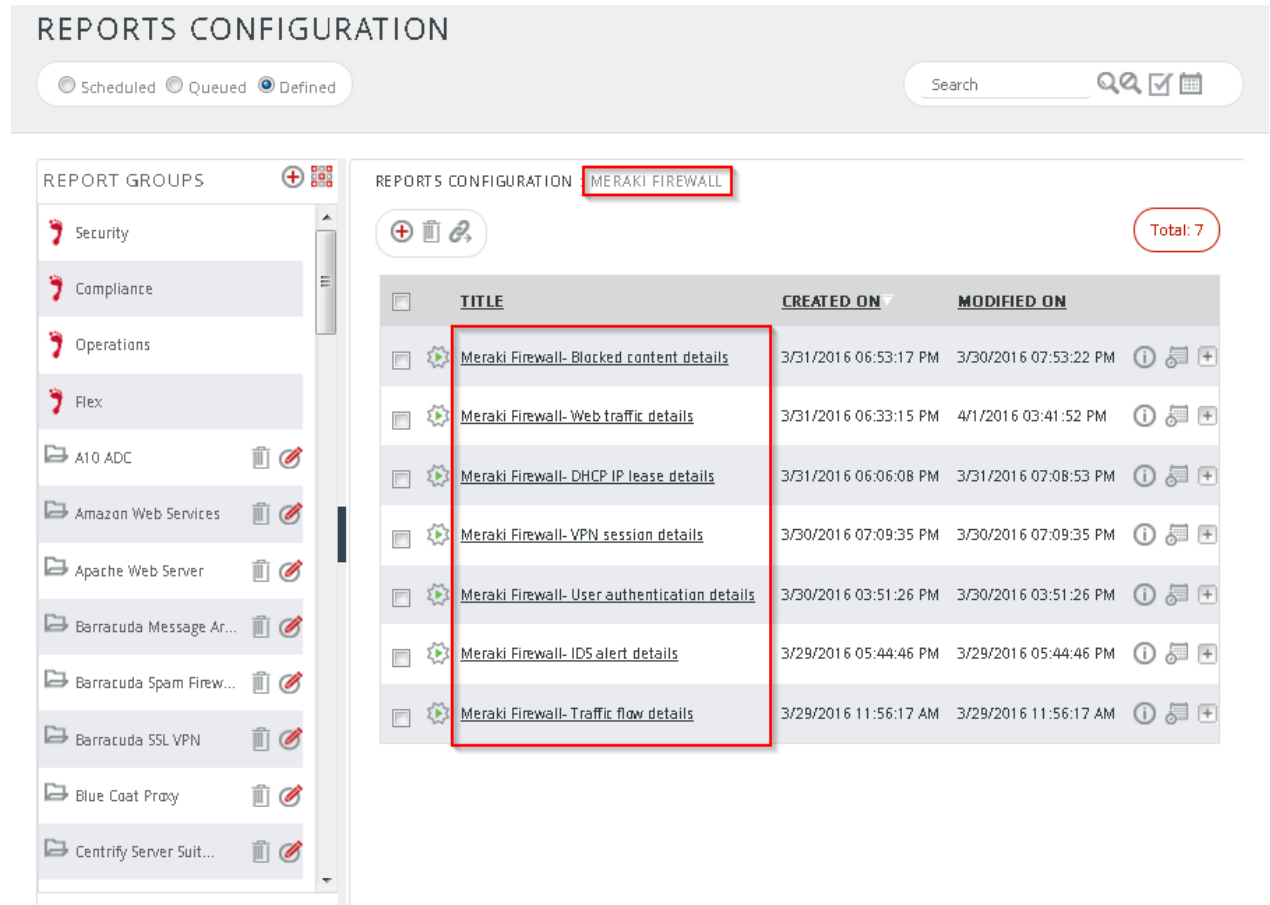


Figure 29

## Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Objects**.
3. In **Objects Tree**, select **Meraki Firewall** group folder.

Imported **Meraki Firewall** objects are shown on the right pane.



2. Navigate to **Reports>Configuration**.

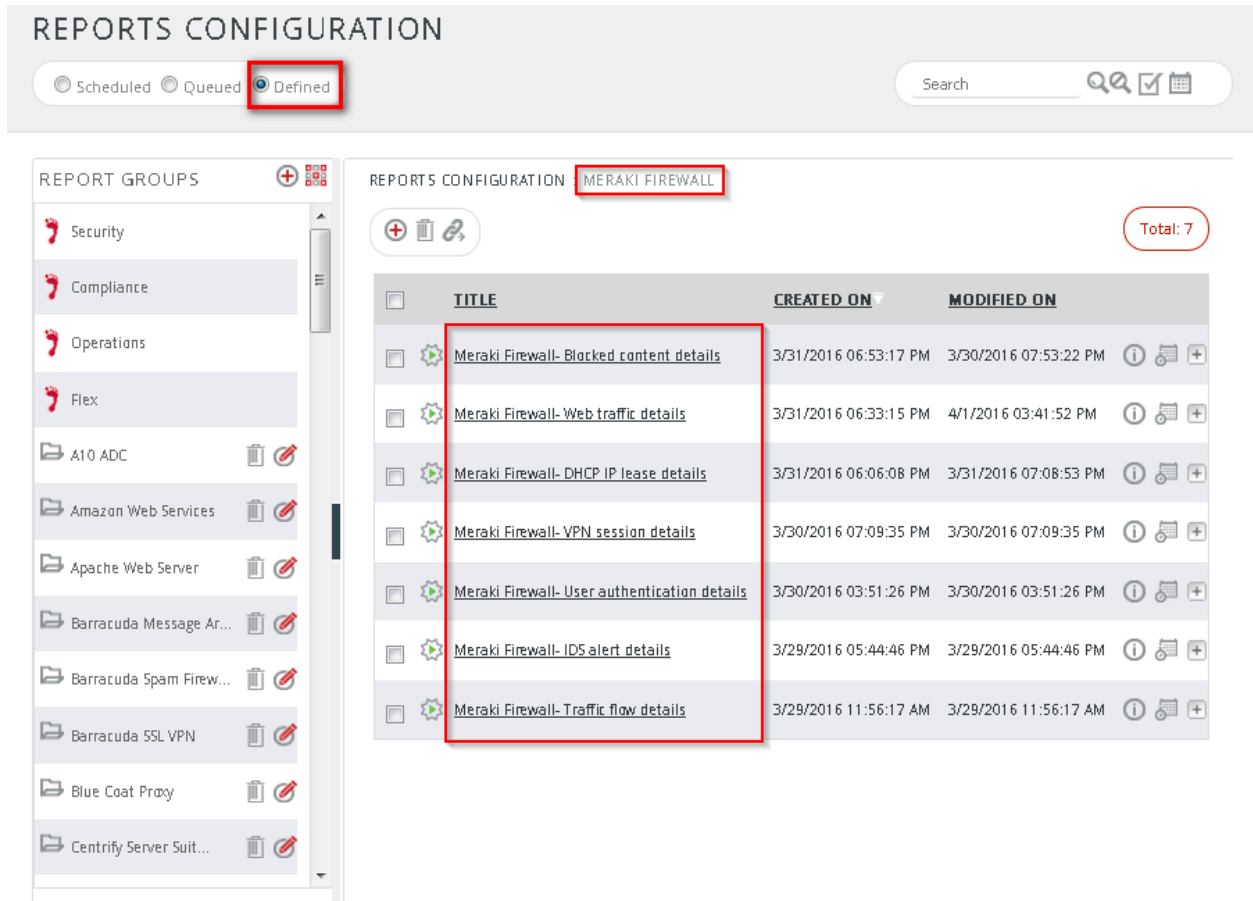



Figure 32

3. Select 'Meraki Firewall' in report groups. Check **defined** dialog box.
4. Click on 'schedule'  to plan a report for later execution.

## REPORT WIZARD

TITLE: MERAKI FIREWALL- BLOCKED CONTENT DETAILS

LOGS

CANCEL < BACK NEXT >

Review cost details and configure the publishing options. Step 8 of 10

### DISK COST ANALYSIS

Estimated time for completion: 00:01:12(HH:MM:SS)  
Number of cab(s) to be processed: 21  
Available disk space: 177 GB  
Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)  
 Deliver results via E-mail  
 Notify results via E-mail

To E-mail:  [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:  ▼

Show in:  ▼

Persist data in Eventvault Explorer

Figure 33

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault Explorer** box.



## REPORT WIZARD

TITLE: MERAKI FIREWALL- BLOCKED CONTENT DETAILS  
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist Step 9 of 10

### RETENTION SETTING

Retention period:  days ⓘ

Persist in database only *[Reports will not be published and will only be stored in the respective database]*

### SELECT COLUMNS TO PERSIST

| COLUMN NAME      | PERSIST                             |
|------------------|-------------------------------------|
| Device Name      | <input checked="" type="checkbox"/> |
| Host Address     | <input checked="" type="checkbox"/> |
| Host Port        | <input checked="" type="checkbox"/> |
| Blocked Category | <input checked="" type="checkbox"/> |
| Blocked URL      | <input checked="" type="checkbox"/> |

Figure 34

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

## Create Dashlets

1. **EventTracker 8 or later** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

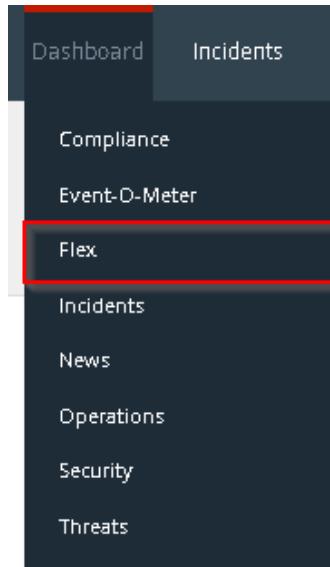


Figure 35

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

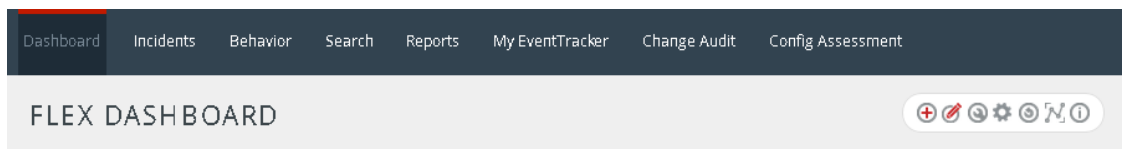



Figure 35

4. Click  to add a new dashboard.  
Flex Dashboard configuration pane is shown.


FLEX DASHBOARD

Title  
Meraki Firewall

Description  
MX Series

SAVE DELETE CANCEL

Figure 37

5. Fill appropriate title and description and click **Save** button.
6. Click  to configure a new flex dashlet.  
Widget configuration pane is shown.

WIDGET CONFIGURATION

WIDGET TITLE: Meraki blocked web contents today

NOTE: [Empty]

DATA SOURCE: Meraki Firewall- Blocked content details

CHART TYPE: Donut | DURATION: 24 Hours | VALUE FIELD: COUNT | AS OF: Recent

AXIS LABELS [X-AXIS]: Blocked URL | LABEL TEXT: [Empty]

VALUES [Y-AXIS]: Select column | VALUE TEXT: [Empty]

FILTER: Select column | FILTER VALUES: [Empty]

LEGEND [SERIES]: Blocked Category | SELECT: All

User-defined Blacklist |  Proxy Avoidance and Anonym...

TEST CONFIGURE CLOSE

Figure 38

7. Locate earlier scheduled report in **Data Source** dropdown.

8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.

Evaluated chart is shown.

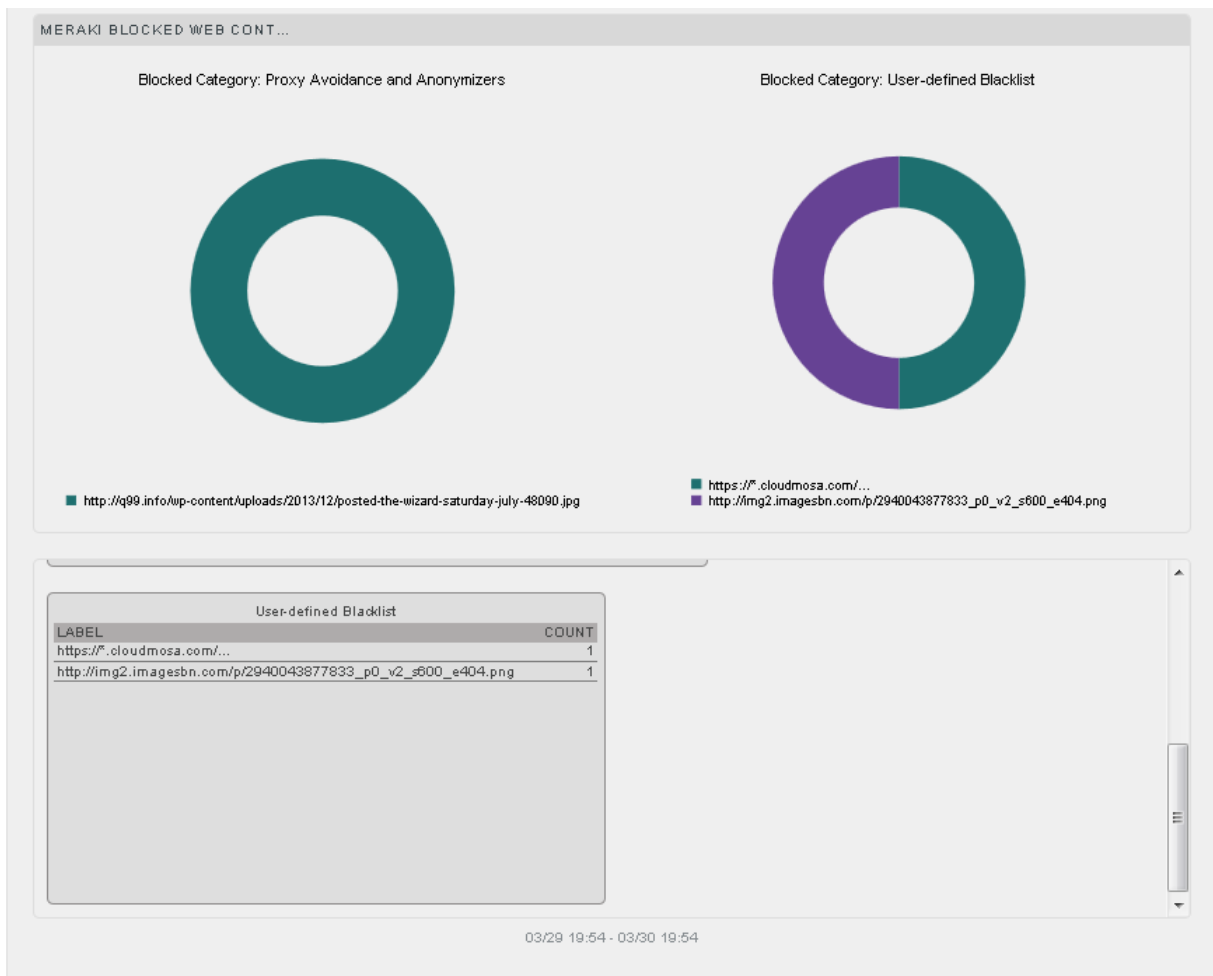




Figure 39

16. If satisfied, Click **Configure** button.



Figure 40

17. Click 'customize'  to locate and choose created dashlet.
18. Click  to add dashlet to earlier created dashboard.

## Sample Dashboards

- **Meraki Firewall-Blocked web content today**

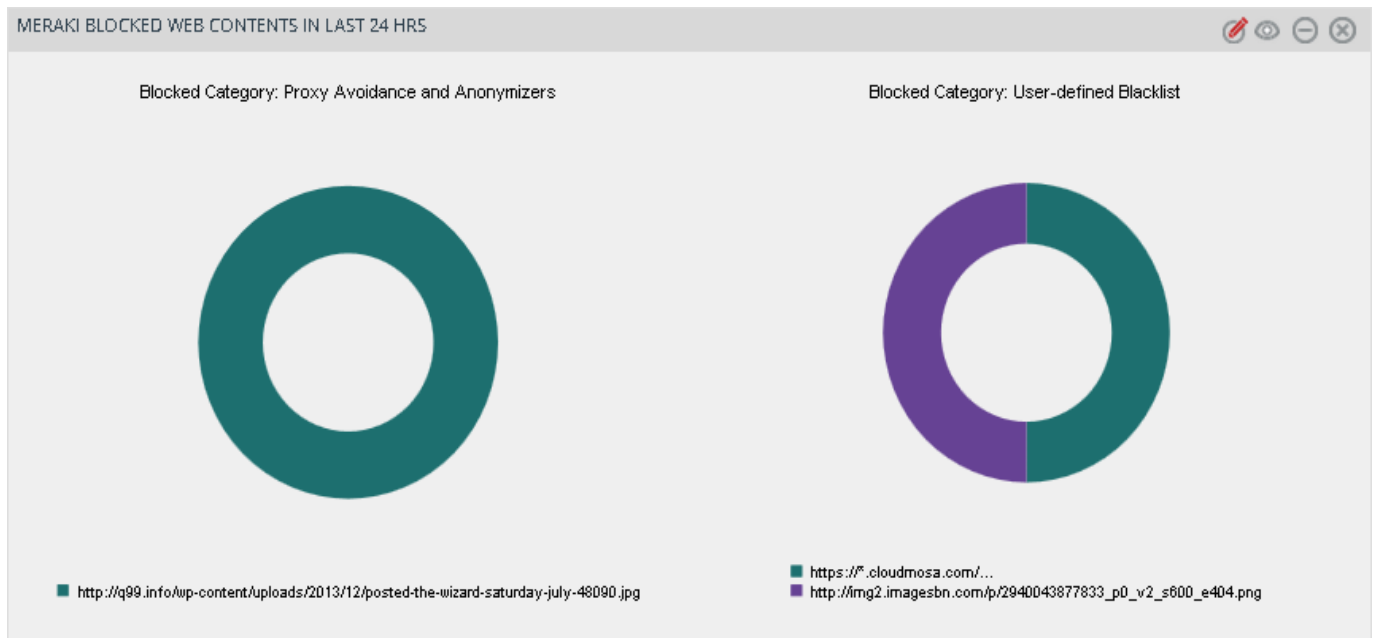


Figure 41

- Meraki Firewall-VPN sessions today

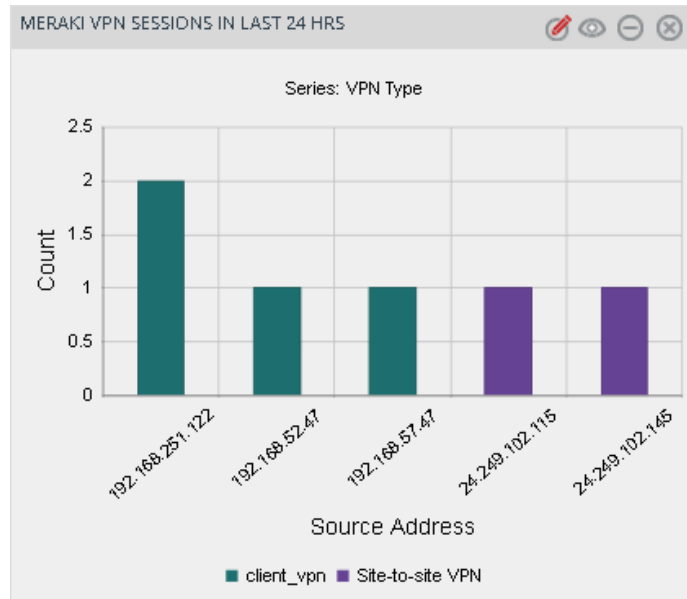


Figure 42

- Meraki Firewall-IDS alert pattern

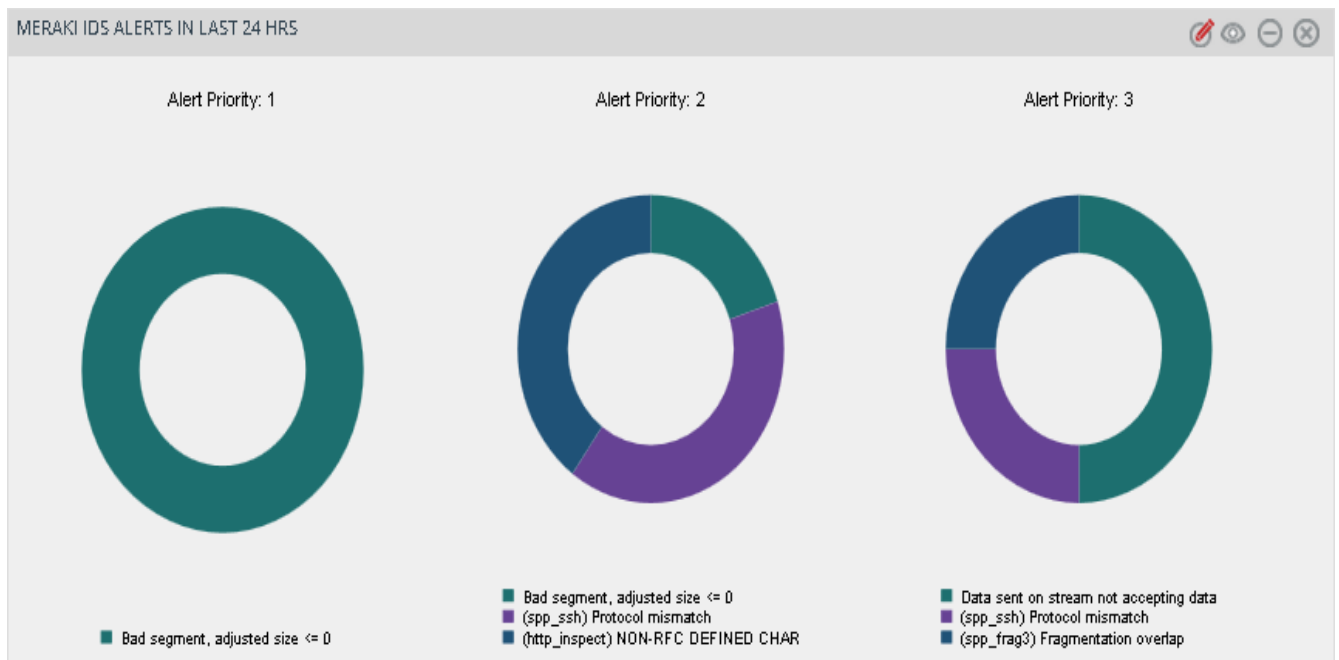


Figure 43

<-|->