EventTracker

Actionable Security Intelligence

Integrate McAfee Firewall Enterprise VPN

Publication Date: January 06, 2016

Abstract

This guide provides instructions to configure McAfee Firewall Enterprise (Sidewinder) VPN to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 6.X, 7.X and later, and McAfee Firewall Enterprise (Sidewinder) VPN 7.x and later.

Audience

McAfee Firewall Enterprise (Sidewinder) VPN users, who wish to forward syslog events to EventTracker Manager.

Table of Contents

Overview

McAfee Firewall (also known as Secure Firewall) is a hardware appliance that contains the following features:

- Application-layer firewall
- VPN functionality
- Web filtering
- Anti-spam/Anti-fraud functionality
- Anti-virus/Anti-spyware filtering engines

The logs produced by McAfee Firewall Enterprise (Sidewinder) VPN include events from all its application functions (i.e., firewall, VPN, Web filtering, etc.) as well as local auditing of the McAfee Firewall Enterprise (Sidewinder) VPN appliance itself (e.g., appliance configuration changes, logins, daemon errors, etc.). McAfee Firewall Enterprise (Sidewinder) VPN appliances can generate audit log messages via Syslog using a variety of log formats.

The EventTracker supports Syslog Sidewinder firewall events using the McAfee Firewall Enterprise (Sidewinder) VPN Export Format (SEF). EventTracker acts as the Syslog Server for Sidewinder, and Sidewinder sends SEF-formatted Syslog messages via UDP or TCP to the EventTracker's Syslog Listener. The configuration procedures for Sidewinder and the EventTracker depend upon your environment.

Prerequisites

Prior to configuring McAfee Firewall Enterprise (Sidewinder) VPN and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker v7.x should be installed.
- Secure Computing Sidewinder appliances running version 6.x, 7.x and later.
- Proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.
- McAfee Firewall Enterprise (Sidewinder) VPN appliances running version 7.0.

Integrate EventTracker with McAfee Firewall Enterprise (Sidewinder) VPN

Configure McAfee Firewall Enterprise (Sidewinder) VPN to forward logs to EventTracker

Configure McAfee Firewall Enterprise (Sidewinder) VPN v6.1

1. Make sure that the auditing and syslog daemons are stopped on the Sidewinder host machine.
2. On Sidewinder, navigate to the location **/etc/sidewinder/**
3. Open **auditd.conf** file in a text editor and add the following line to end of the file:**syslog(**facility **filters["**filter**"]** format**)** where,

    - **facility** - Facility level associated with the Syslog message (e.g., local0-local7)
    - **filter** - Name of the sacap filter to use for all the events. If this parameter is set to NULL, then all audit events are reported to the log.
    - **format** - Event output format. Make sure this is set to SEF (Sidewinder Export Format used by Sidewinder G2 Security Reporter). For example, syslog(local0 filters["NULL"] SEF)

4. Open the **syslogd.conf** file in a text editor and modify the default burb entry (log_burb[0]) to the correct burb.
5. Navigate to the location **/etc/.**
6. Open the syslog.conf file in a text editor and add the following line to the file:

    facility**.* @**x.x.x.x where,

    - **facility** - Facility level you specified in same facility as mentioned above
    - **x.x.x.x** - IP address of the remote Syslog Server (i.e., EventTracker's Machine IP)

    For example, local0.* @10.2.1.149

7. Restart the auditing and syslog daemons by completing the following steps:

    - Find the **Syslog Process Identifier** (PID) using the **pss** syslog command.
    - Restart the syslogd and audit processes by using the following commands:

    kill syslogpid
    ind Slog /usr/sbin/syslogd –
    l cf server restart auditd

Configure McAfee Firewall Enterprise (Sidewinder) VPN v 6.2.x

1. Make sure that the auditing and syslog daemons are stopped on the Sidewinder host machine.
2. Navigate to the location **/etc/sidewinder/.**
3. Open **auditd.conf** file in a text editor and add the following line to the end of the file: **syslog(**facility **filters["**filter**"]** format**)** where,

    - **facility** - Facility level associated with the Syslog message (e.g., local0-local7)
    - **filter** - Name of the sacap filter to use for all the events. If this parameter is set to NULL, then all audit events are reported to the log.
    - **format** - Event output format. Make sure this is set to SEF (Sidewinder Export Format used by Sidewinder G2 Security Reporter). For example, syslog(local0 filters["NULL"] SEF)

4. Navigate to the location **/etc/.**
5. Open the **syslog.conf** file in a text editor and add the following line to the file: facility**.*** **@**x.x.x.x where,

    - **facility** - Facility level you specified in same facility as mentioned above
    - **x.x.x.x** - IP address of the remote Syslog Server (i.e., EventTracker's Machine IP)

    For example, local0.* @10.2.1.149

6. Restart the auditing and syslog daemons by completing the following steps:

    - Find the **Syslog Process Identifier (PID)** using the **pss** syslog command.
    - Restart the **syslogd** and audit processes by using the following commands:

    kill -HUP syslogpid **i nd Slog**
    /usr/sbin/syslogd -l cf server restart
    auditd

Configure McAfee Firewall Enterprise (Sidewinder) VPN v 7.0

1. Make sure that auditing and syslog daemons are stopped on Sidewinder host machine.
2. Navigate to the location **/secureos/etc/.**
3. Open **auditd.conf** file in a text editor and add the following line to the end of the file **syslog(**facility **filters["**filter**"]** format**)** where,

    - **facility** - Facility level associated with the Syslog message (e.g., local0-local7)
    - **filter** - Name of the sacap filter to use for all the events. If this parameter is set to NULL, then all audit events are reported to the log.
    - **format** - Event output format. Make sure this is set to SEF (Sidewinder Export Format used by Sidewinder G2 Security Reporter). For example, syslog(local0 filters["NULL"] SEF)

4. Navigate to the location **/etc/.**
5. Open the syslog.conf file in a text editor and add the following line to the file: facility**.*** **@**x.x.x.x where,

    - **facility** - Facility level you specified in same facility as mentioned above
    - **x.x.x.x** - IP address of the remote Syslog Server (i.e., EventTracker's Machine IP) For example, local0.* @10.2.1.149

6. Within the **syslog.conf** file by changing this line from

    ***.notice;auth,...uucp.none /var/logmessages**
    to
    ***.notice;auth,...uucp,facility.none /var/logmessages**
    Changing this line prevents redundant logging.

7. Restart auditing and syslog daemons using the following commands:

    cf daemond restart agent=syslog cf daemond restart agent=auditd

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker, Alerts and reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7.x to support McAfee Firewall Enterprise (Sidewinder) VPN monitoring.

Reports

- **Mcafee Sidewinder: IKE Authentication Status:** This report provides information related to IKE Authentication Status which includes VPN Name, Message ID, Hostname, Local Gateway, Remote Gateway, Remote ID Information and other fields.
- **Mcafee Sidewinder VPN: Tunnel Establishment Attempt:** This report provides information related to Tunnel Establishment Attempt which includes Pid, VPN Name, Hostname, Local Gateway, Remote Gateway, Information and other fields.
- **Mcafee Sidewinder VPN: IPSec Session Status:** This report provides information related to IPSec Session Status which includes Hostname, Eventname, VPN Name, Local Gateway, Remote Gateway, Local Network, Remote Network, Information and other fields.

Import McAfee Firewall Enterprise (Sidewinder) VPN Knowledge Pack in EventTracker

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

Import Flex Reports

1. Click **Reports** option, and then click the '**browse**'  button.
2. Locate applicable **McAfee Sidewinder Firewall VPN.issch** file, and then click the **Open** button.

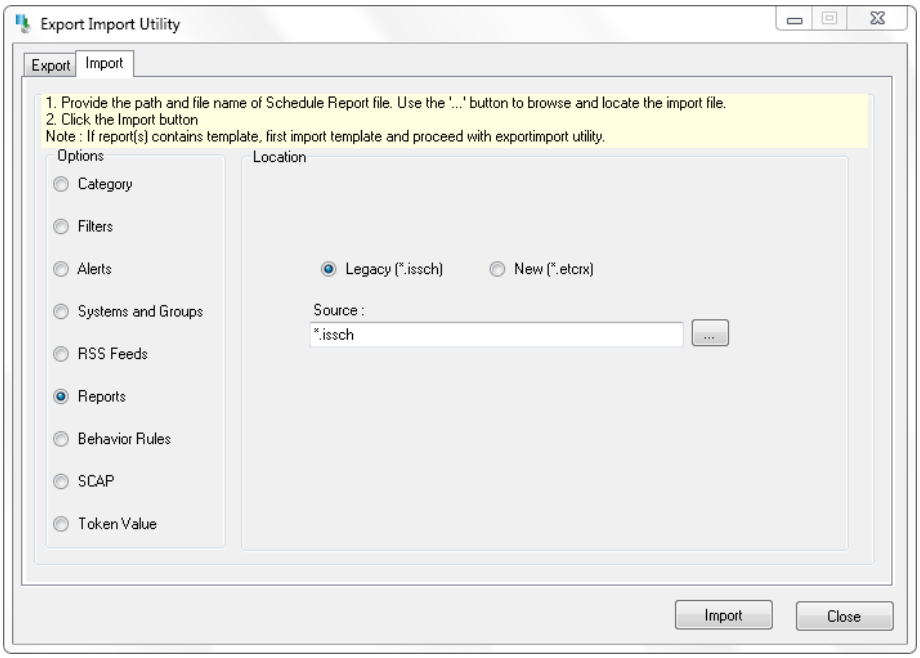

Figure 1

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

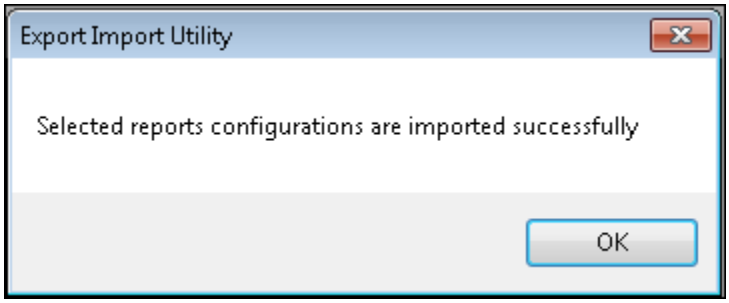

Figure 2

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

Verify McAfee Firewall Enterprise (Sidewinder) VPN knowledge pack in EventTracker

Verify Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click McAfee Sidewinder Firewall VPN group folder.

   Scheduled Reports are displayed in the Reports configuration pane.

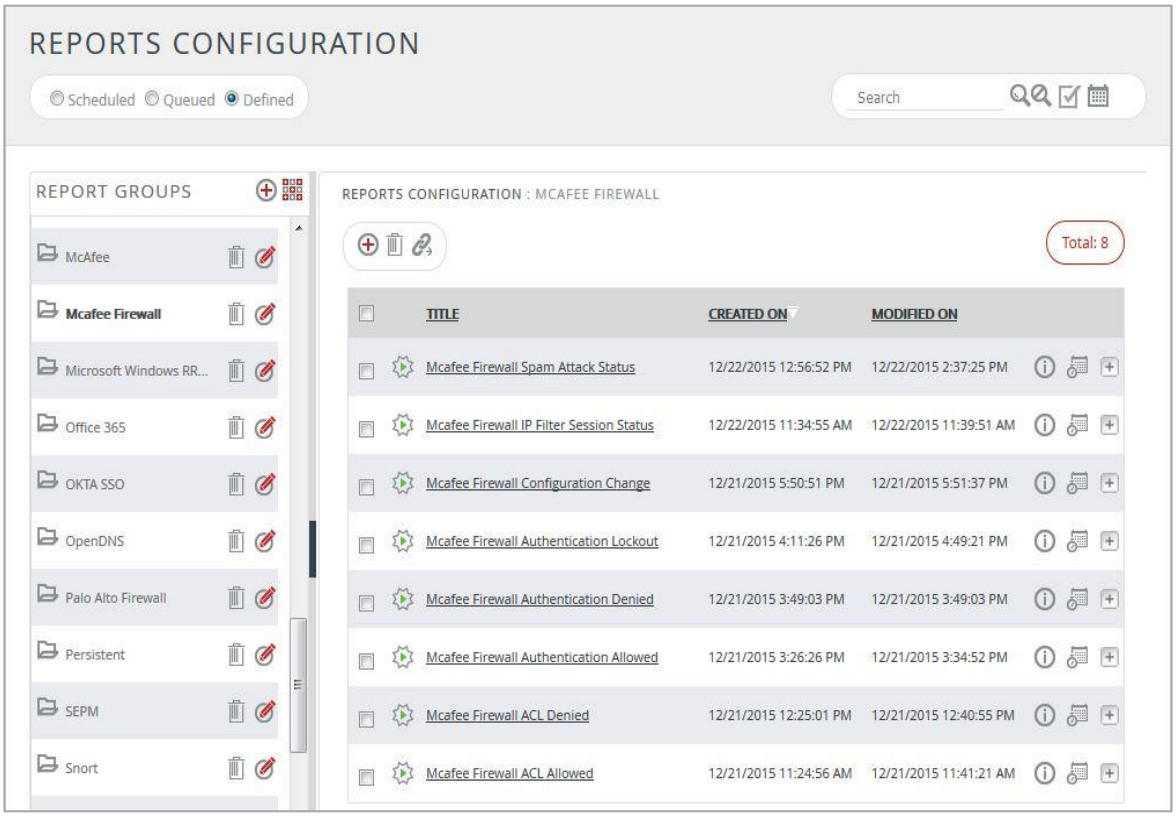

Figure 3

Create Dashboards in EventTracker

Schedule Reports

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

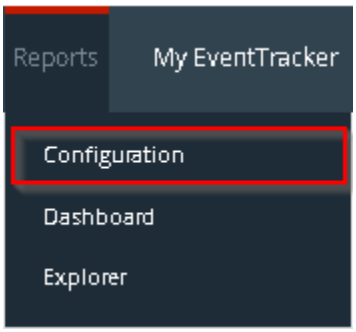

Figure 4

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

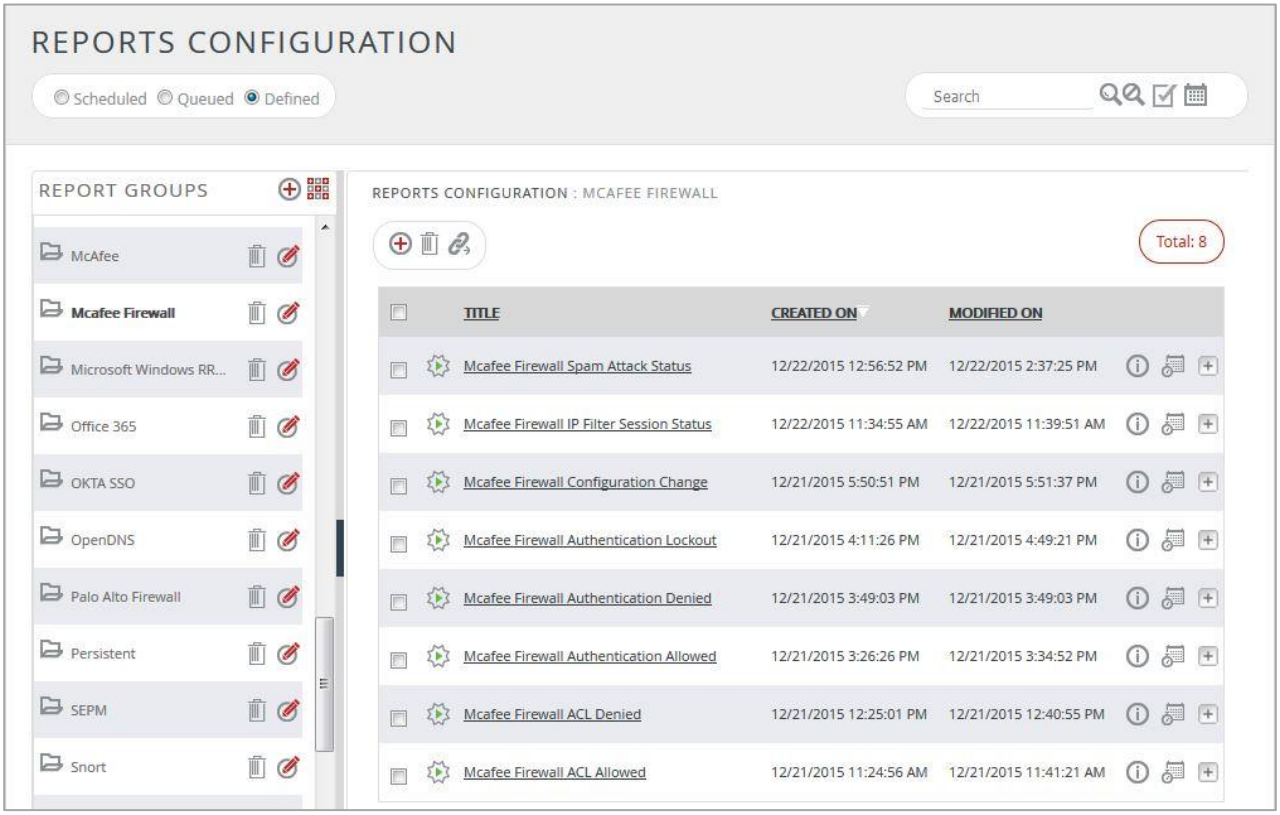

Figure 5

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

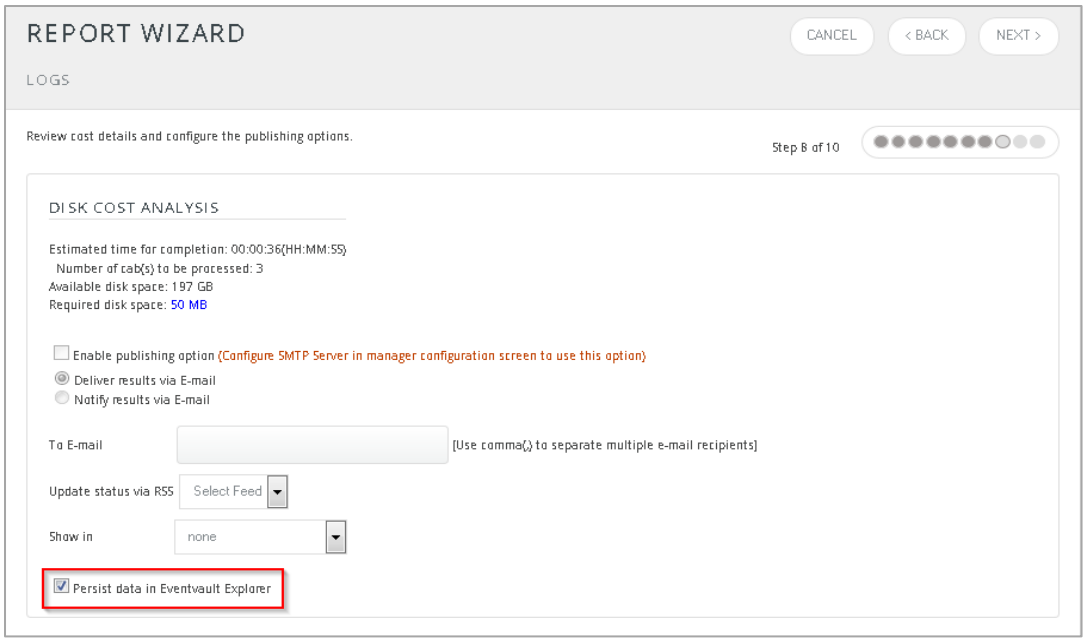

Figure 6

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

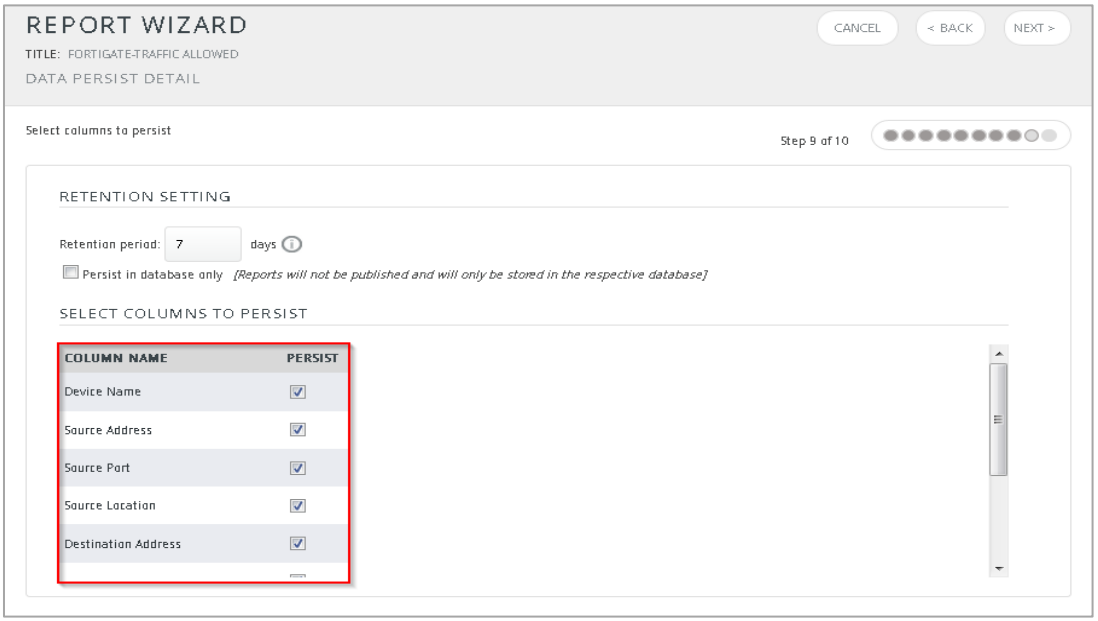

Figure 7

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** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

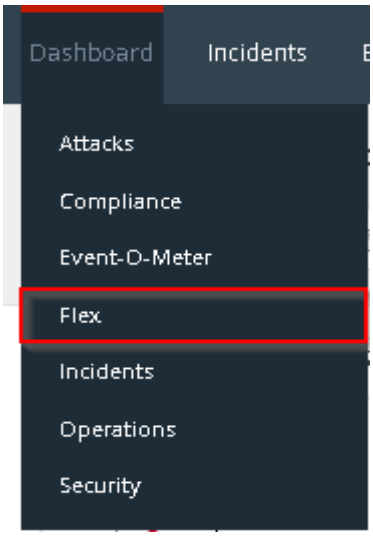

Figure 8

3. Navigate to **Dashboard>Flex**.

   Flex Dashboard pane is shown.

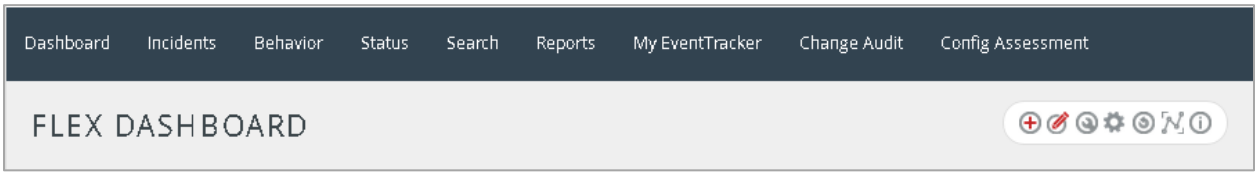

Figure 9

4. Click ⊕ to add a new dashboard.

Flex Dashboard configuration pane is shown.

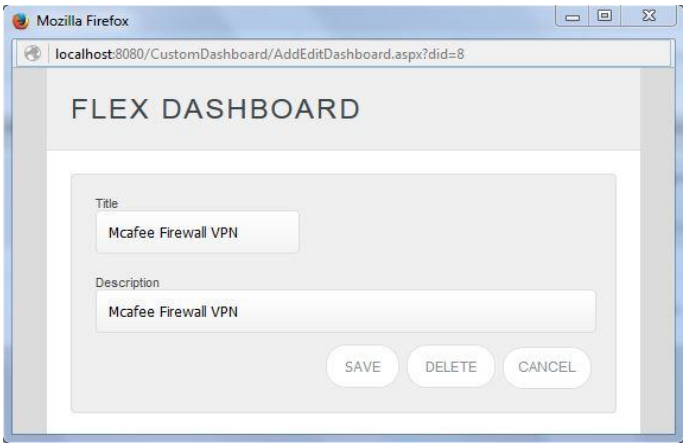

Figure 10

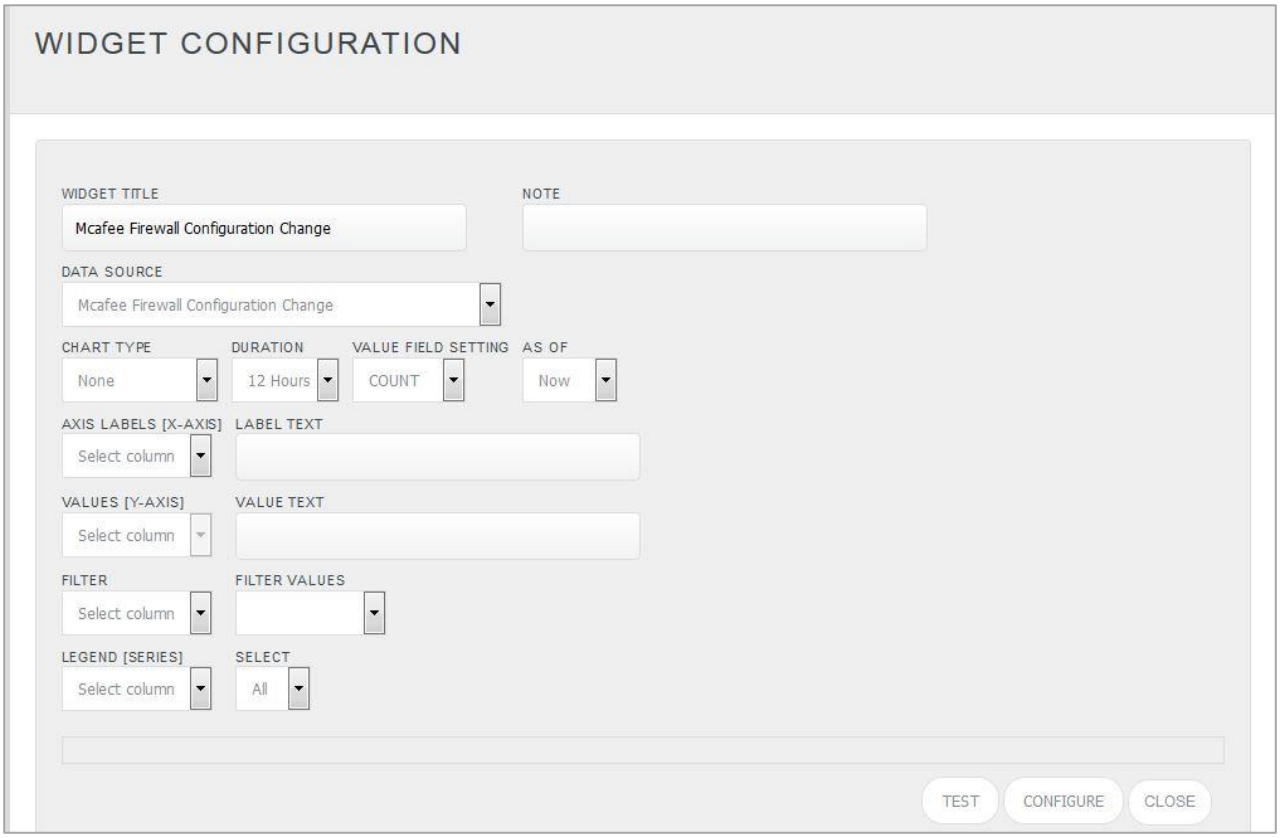

Figure 11

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 button to evaluate.
    Evaluated chart is shown.

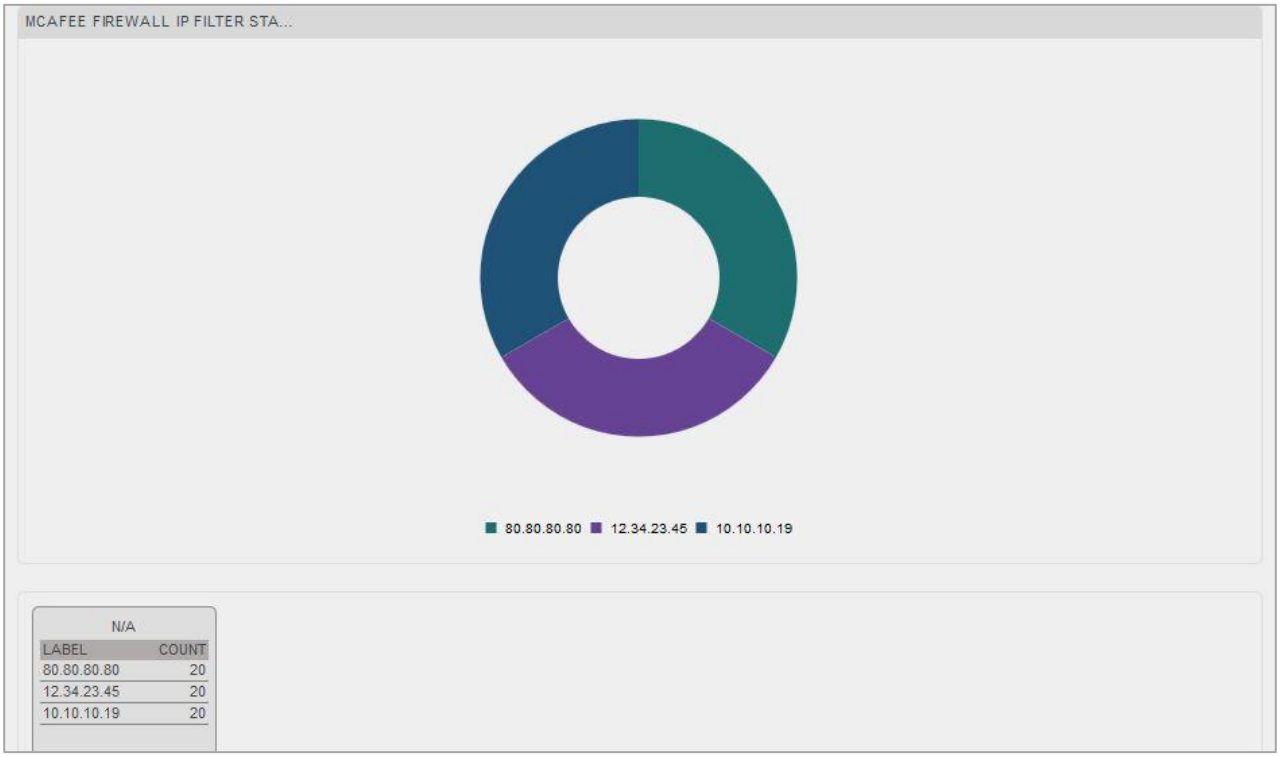

Figure 12

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

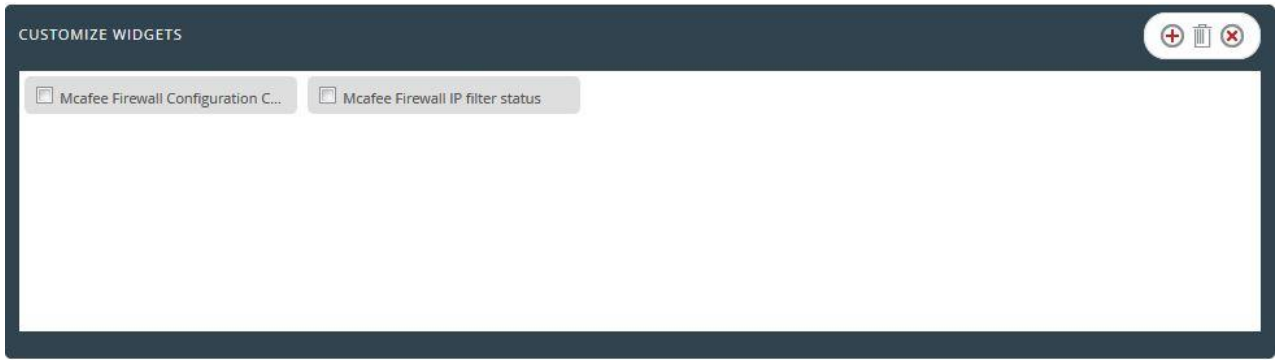

Figure 13

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

Sample Dashboards

1. Mcafee Firewall VPN IKE Authentication Status

Figure 14

2. Mcafee Firewall VPN IPSec Session Status

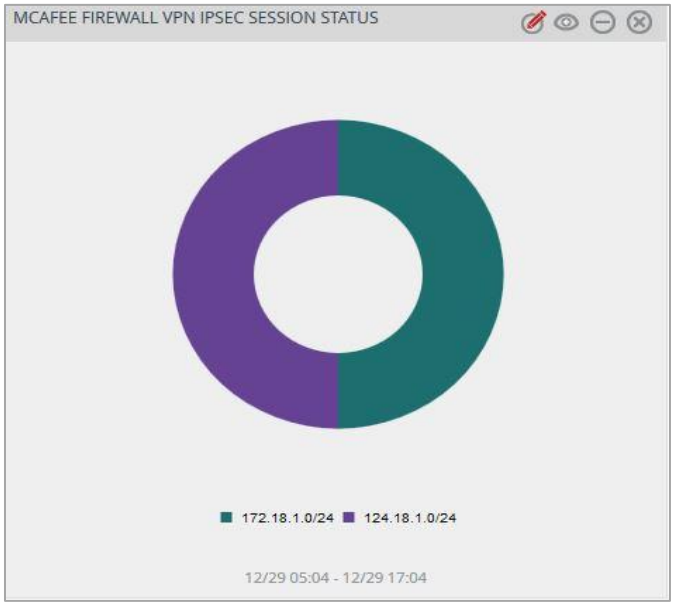

Figure 15

Sample Reports

1. Mcafee Firewall VPN IKE Authentication Status

Mcafee Firewall VPN IKE Authentication status

LogTime	Computer	Host Name	VPN Name	Local Gateway	Gateway	Remote ID	Information
12/28/2015 05:20:36 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:36 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:36 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:36 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:36 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:36 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:36 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:36 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:36 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:37 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:37 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:37 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:37 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:37 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:37 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:38 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:38 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:38 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:38 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established
12/28/2015 05:20:38 PM	IKEA	a.a.local	werf	10.0.0.245	10.0.0.222	10.0.0.244	IKE_AUTH exchange terminated
12/28/2015 05:20:40 PM	IKEA	a.a.local	ngfw	10.0.0.239	10.0.0.254	10.0.0.254	IKE_AUTH exchange established

Figure 16

2. Mcafee Firewall VPN IPSec Session Status

Mcafee Firewall VPN IPsec Session Status

LogTime	Computer	Host Name	Event Name	VPN Name	Local Gateway	Remote Gateway	Local Network	Remote Network
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session closed	mnbh	10.0.0.222	10.0.0.232	192.142.2.0/24	124.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:22 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24
12/29/2015 09:29:27 AM	IPSECS	a.a.local	IPsec session begin	ngfw	10.0.0.239	10.0.0.254	192.168.2.0/24	172.18.1.0/24

Figure 17