

Integrate McAfee Firewall Enterprise *EventTracker Enterprise*

Abstract

This guide provides instructions to configure McAfee Firewall Enterprise to send the syslog events to EventTracker Enterprise.

Scope

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

Audience

McAfee Firewall Enterprise users, who wish to forward syslog events to EventTracker Manager.

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
Overview	3
Prerequisites	3
Integrate EventTracker with McAfee Firewall Enterprise	4
Configure McAfee Firewall Enterprise to forward logs to EventTracker.....	4
Configure McAfee Firewall Enterprise (Sidewinder) v6.1.....	4
Configure McAfee Firewall Enterprise (Sidewinder) v 6.2.x	5
Configure McAfee Firewall Enterprise (Sidewinder) version 7.0.....	6
EventTracker Knowledge Pack (KP)	7
Categories	7
Alerts.....	9
Reports	9
Import McAfee Firewall Enterprise (Sidewinder) Knowledge Pack in EventTracker	10
Import Category.....	10
Import Alerts.....	11
Import Flex Reports.....	13
Verify McAfee Firewall Enterprise (Sidewinder) knowledge pack in EventTracker.....	14
Verify Categories.....	14
Verify Alerts	14
Verify Flex Reports	15
Create Dashboards in EventTracker	16
Schedule Reports.....	16
Create Dashlets	19
Sample Dashboards	23
Sample Reports	25

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

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

Prerequisites

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

- EventTracker v7.x should be installed.
- Secure Computing McAfee Firewall Enterprise appliances running version 6.1, 6.2.x, 7.0.
- Proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.
- McAfee Firewall Enterprise (Sidewinder) appliances running version 7.0.

Integrate EventTracker with McAfee Firewall Enterprise

Configure McAfee Firewall Enterprise to forward logs to EventTracker

Configure McAfee Firewall Enterprise (Sidewinder) 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:

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

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

Configure McAfee Firewall Enterprise (Sidewinder) 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 daemon restart agent=syslog
cf daemon 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) monitoring.

Categories

- **McAfee Sidewinder: Access violation** - This category based report provides information related to the access violation.
- **McAfee Sidewinder: ACL modifications** - This category based report provides information related to ACL modifications.
- **McAfee Sidewinder: Application defense log** - This category based report provides information related to application defense log.
- **McAfee Sidewinder: Attack detection** - This category based report provides information related to attack detection.
- **McAfee Sidewinder: Blackhole message detection** - This category based report provides information related to blackhole message detection.
- **McAfee Sidewinder: DNS requests log** - This category based report provides information related to DNS requests log.
- **McAfee Sidewinder: Generic messages** - This category based report provides information related to generic messages.
- **McAfee Sidewinder: Hardware/Software failure** - This category based report provides information related to Hardware/Software failure.
- **McAfee Sidewinder: Health monitoring** - This category based report provides information related to the health monitoring.
- **McAfee Sidewinder: HTTP requests** - This category based report provides information related to HTTP requests.
- **McAfee Sidewinder: IP filter traffic** - This category based report provides information related to IP filter traffic.
- **McAfee Sidewinder: License exceeded** - This category based report provides information related to license exceeded.

- **McAfee Sidewinder: Log overflow** - This category based report provides information related to log overflow.
- **McAfee Sidewinder: Mail messages rejected** - This category based report provides information related to mail messages rejected.
- **McAfee Sidewinder: MIME/Virus detected** - This category based report provides information related to MIME/Virus detected.
- **McAfee Sidewinder: Network access control allowed** - This category based report provides information related to network access control being allowed or not.
- **McAfee Sidewinder: Network access control violation** - This category based report provides information related to network access control violation.
- **McAfee Sidewinder: Network traffic log** - This category based report provides information related to network traffic log.
- **McAfee Sidewinder: Protocol violation** - This category based report provides information related to protocol violation.
- **McAfee Sidewinder: Proxy flooded** - This category based report provides information related to proxy flooded.
- **McAfee Sidewinder: Proxy/Server authentication** - This category based report provides information related to Proxy/Server authentication.
- **McAfee Sidewinder: SNMP trap alert log** - This category based report provides information related to SNMP trap alert log.
- **McAfee Sidewinder: SWEDE configuration change** - This category based report provides information related to SWEDE configuration change.
- **McAfee Sidewinder: UDP traffic dropped** - This category based report provides information related to UDP traffic dropped.
- **McAfee Sidewinder: UPS logs** - This category based report provides information related to UPS logs.
- **McAfee Sidewinder: User database modifications** - This category based report provides information related to User database modifications.
- **McAfee Sidewinder: VPN traffic log** - This category based report provides information related to VPN traffic log.

Alerts

- **McAfee Sidewinder: Access violation** - This alert is generated when access violation occurs.
- **McAfee Sidewinder: ACL modifications** - This alert is generated when ACL modifications occur.
- **McAfee Sidewinder: Attack detection** - This alert is generated when attack detection occurs.
- **McAfee Sidewinder: Hardware/Software failure** - This alert is generated when Hardware/Software failure occurs.
- **McAfee Sidewinder: License exceeded** - This alert is generated when license is exceeded.

Reports

- **Mcafee Sidewinder: ACL Allowed:** This report provides information related to Access Control List which includes Source Address, Source Port, Destination Address, Destination Port, User Name, Authentication Method and Access List ID and other fields.
- **Mcafee Sidewinder: ACL Denied:** This report provides information related to Access Control List which includes Source Address, Source Port, Destination Address, Destination Port, User Name, Authentication Method and Access List ID and other fields.
- **Mcafee Sidewinder: Authentication Allowed:** This report provides information related to Authentication allowed which includes Domain, Edomain, Hostname, Eventname, Authentication method, Information and other fields.
- **Mcafee Sidewinder: Authentication Denied:** This report provides information related to Authentication denied which includes Domain, Edomain, Hostname, Eventname, Authentication method, Domain, Edomain, Hostname, Eventname,
- **Mcafee Sidewinder: Authentication Lockout:** This report provides information related to Authentication allowed which includes Domain, Edomain, Hostname, Eventname, Authentication method, Information and other fields.
- **Mcafee Sidewinder: Configuration Changes:** This report provides information related to Configuration Changes whether is it modified, restored and apply which includes Domain, Edomain, Hostname, Eventname, Information and other fields.


- **McAfee Sidewinder: IP Filter:** This report provides information related to IP filter whether it is open, close and timeout which includes Source Address, Source Port, Destination Address, Destination Port, User Name and other fields.
- **McAfee Sidewinder: Spam Attack:** This report provides information related to Spam attacks which includes Source Address, Source Port, Domain, Edomain, Hostname, Eventname, Attack IP and other fields.

Import McAfee Firewall Enterprise (Sidewinder) Knowledge Pack in EventTracker

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

Import **Category** and **Alert** as given below.

Import Category

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

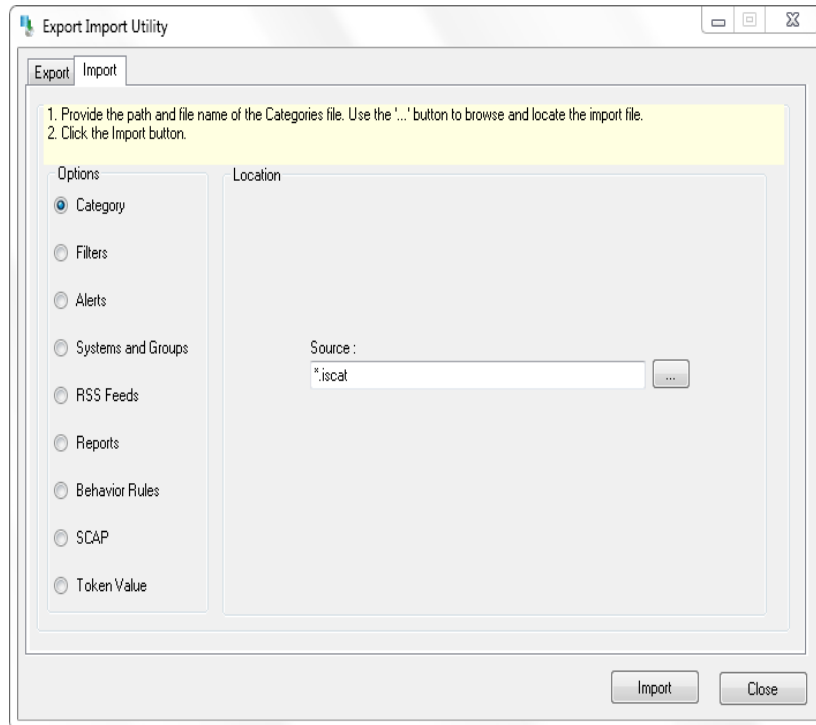


Figure 1

2. Locate **All McAfee Sidewinder group of Categories.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

EventTracker displays success message.

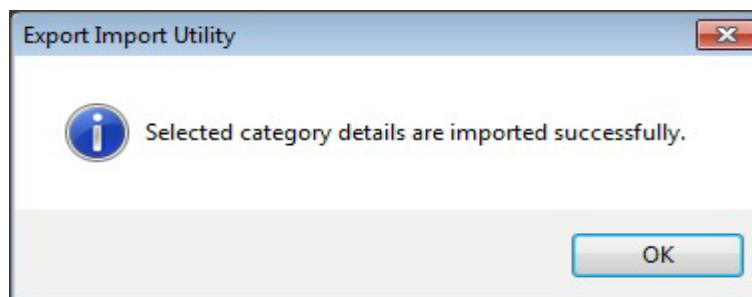


Figure 2

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

Import Alerts

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

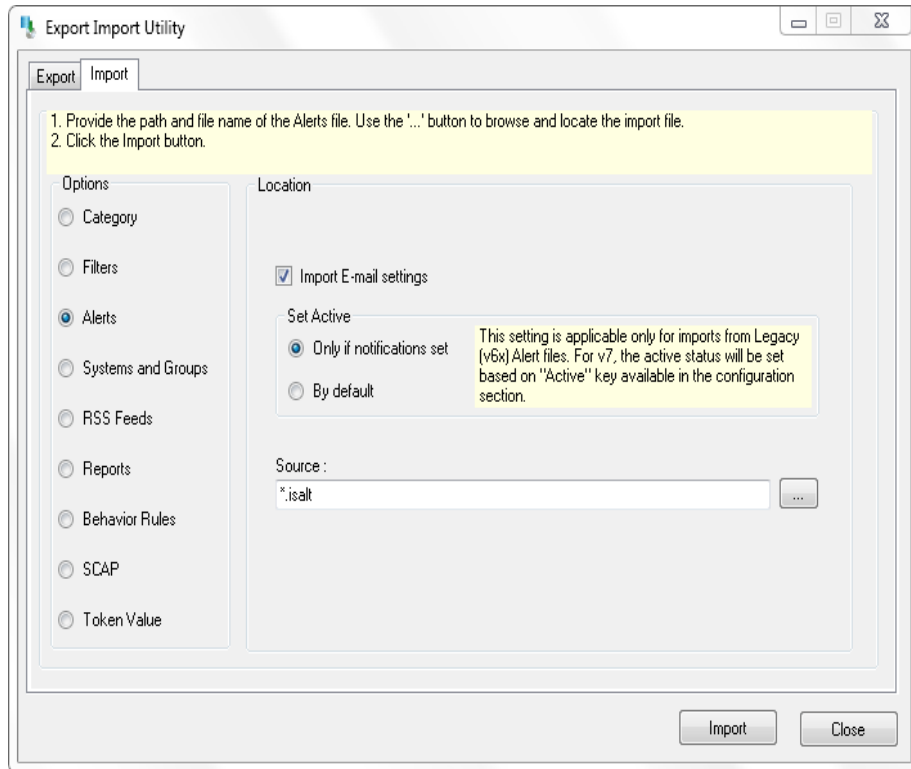


Figure 3

2. Locate **All McAfee Sidewinder group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

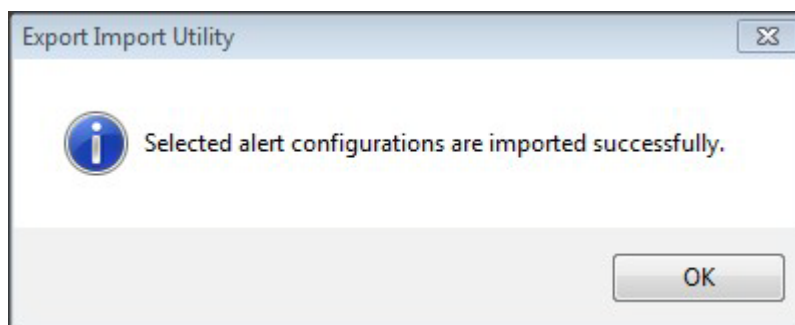



Figure 4

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

Import Flex Reports

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

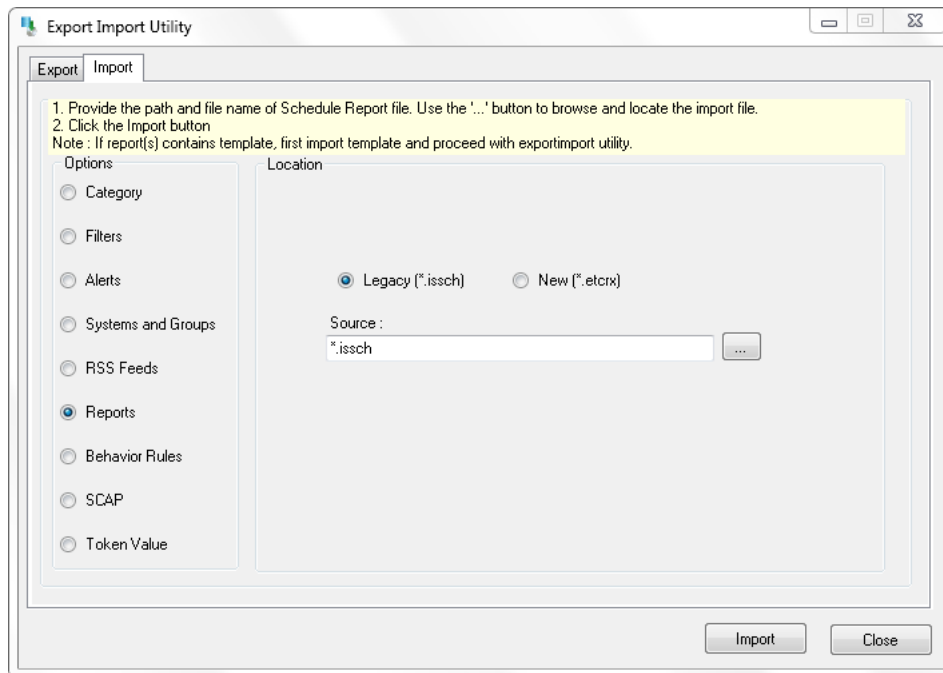


Figure 5

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

EventTracker displays success message.

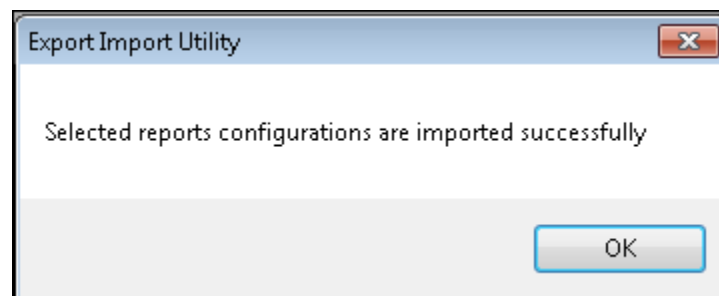


Figure 6

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

Verify McAfee Firewall Enterprise (Sidewinder) knowledge pack in EventTracker

Verify Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In **Category Tree**, expand **McAfee Sidewinder Firewall** group folder to view imported categories.

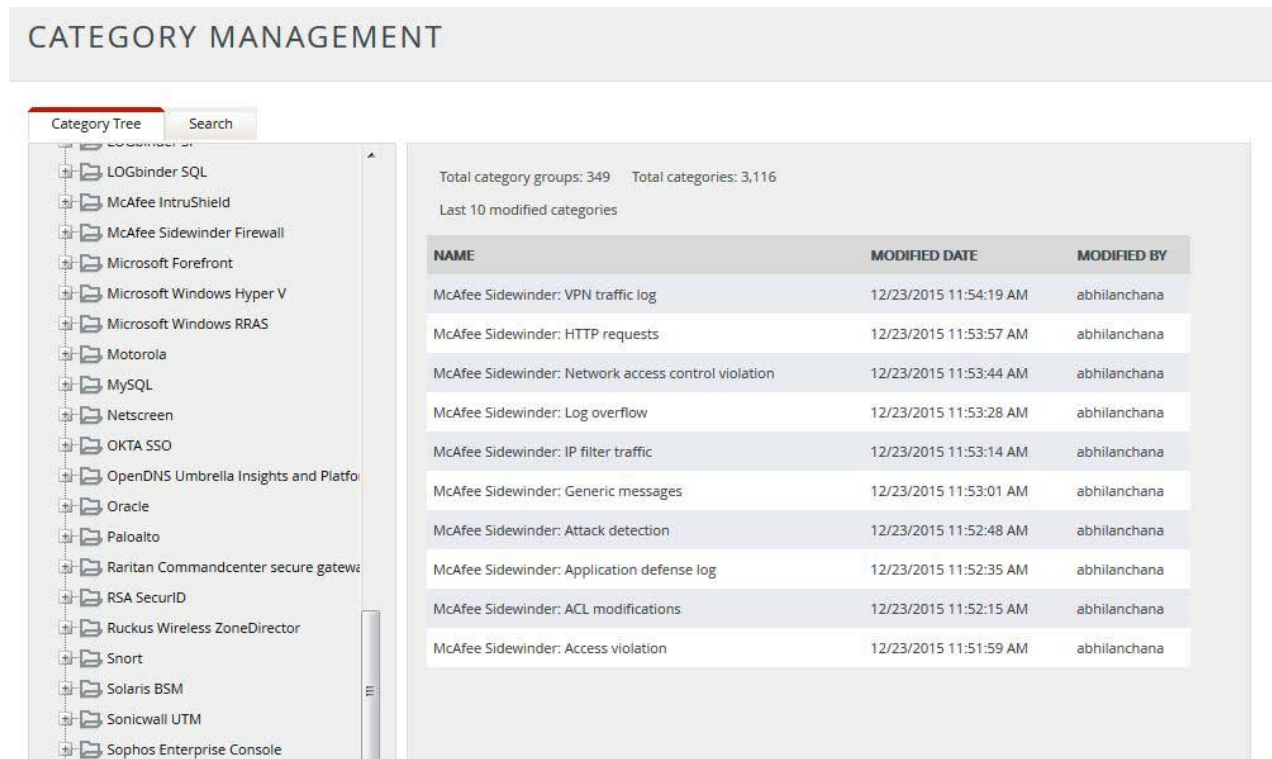


Figure 7

Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.

3. In **Search** field, type '**McAfee Sidewinder Firewall**', and then click the **Go** button.

Alert Management page will display all the imported McAfee Sidewinder Firewall alerts.

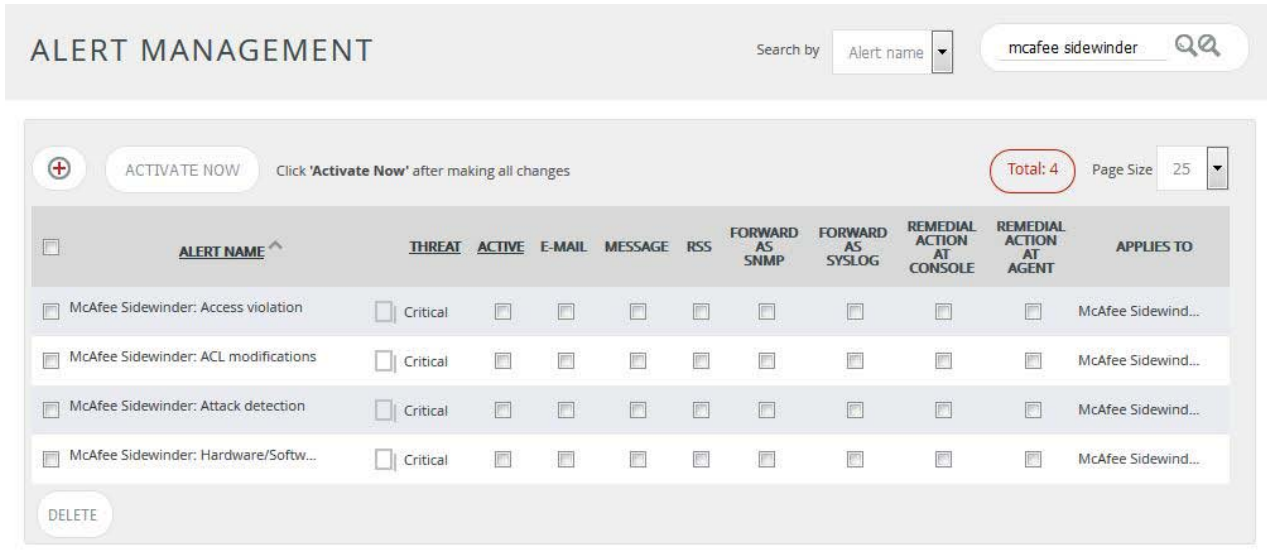


Figure 8

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

EventTracker displays message box.

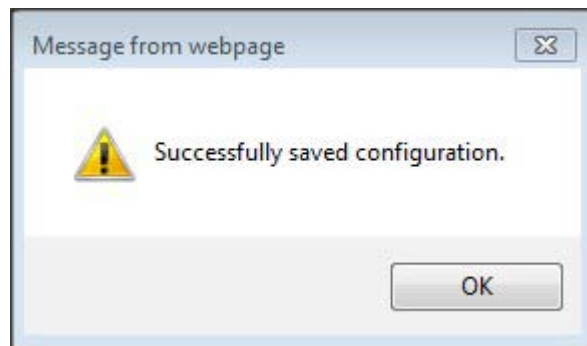


Figure 9

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

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** group folder.

Scheduled Reports are displayed in the Reports configuration pane.

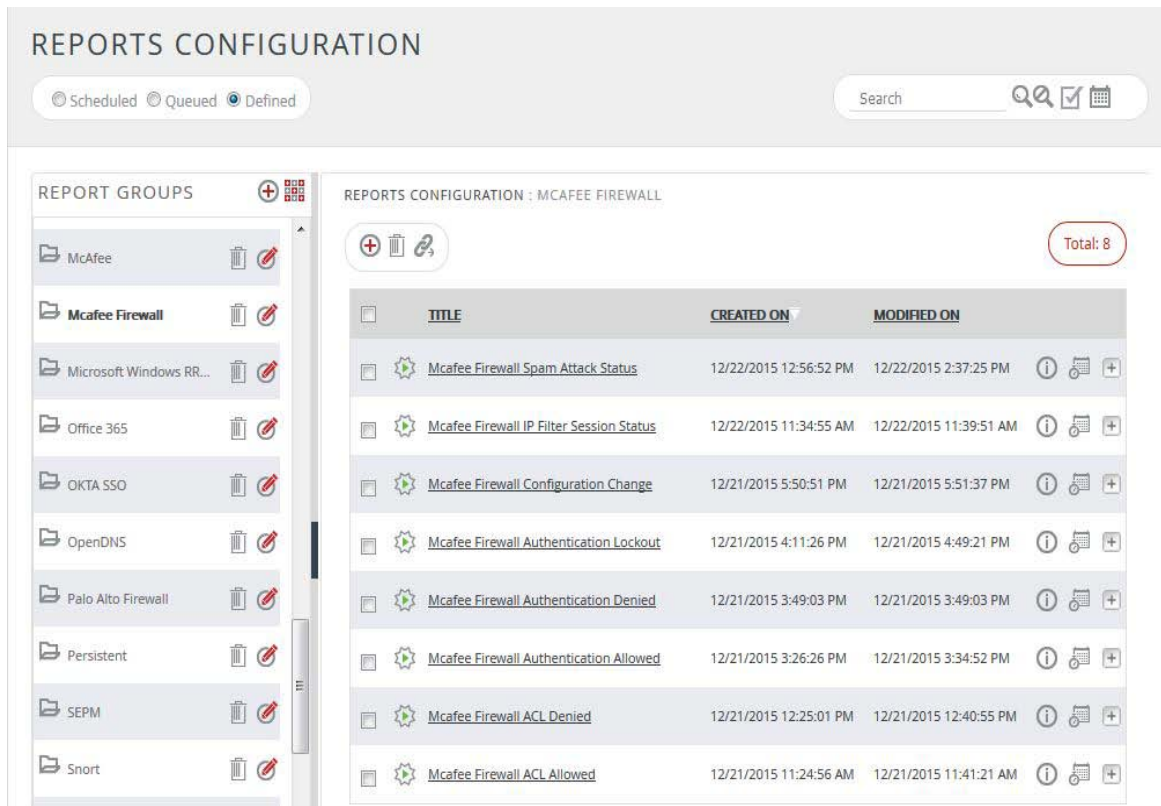


Figure 10

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.

Create Dashboards in EventTracker

Schedule Reports

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

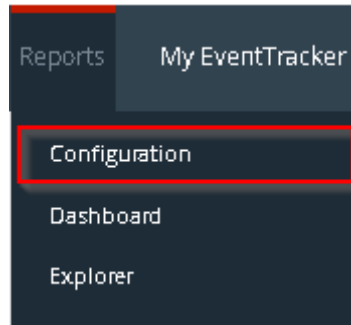


Figure 11

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

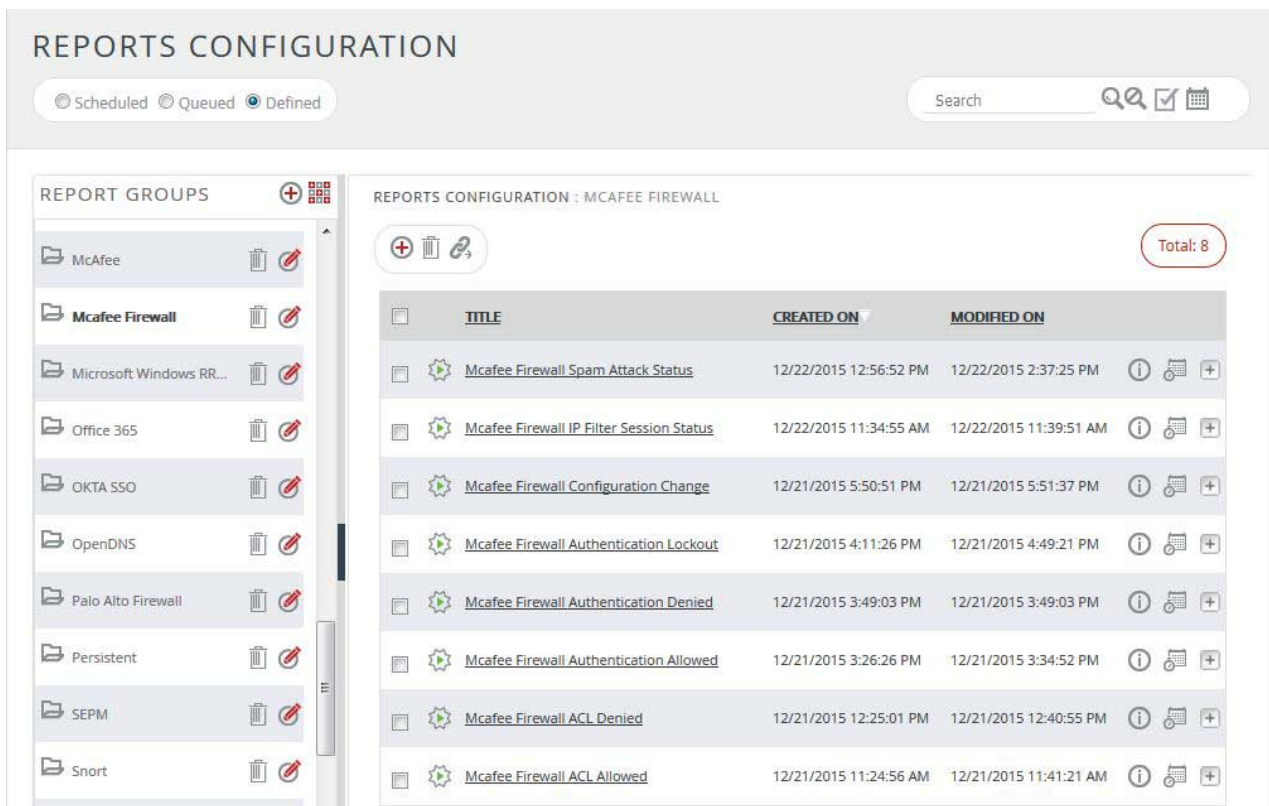


Figure 12

3. Select **McAfee Sidewinder Firewall** in report groups. Check **defined** dialog box.

4. Click on 'schedule' to plan a report for later execution.

REPORT WIZARD

CANCEL < BACK NEXT >

LOGS

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

DISK COST ANALYSIS

Estimated time for completion: 00:00:36(HH:MM:SS)
Number of cab(s) to be processed: 3
Available disk space: 197 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 13

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

REPORT WIZARD

TITLE: FORTIGATE-TRAFFIC ALLOWED
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"/>
Source Address	<input checked="" type="checkbox"/>
Source Port	<input checked="" type="checkbox"/>
Source Location	<input checked="" type="checkbox"/>
Destination Address	<input checked="" type="checkbox"/>

Figure 14

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.

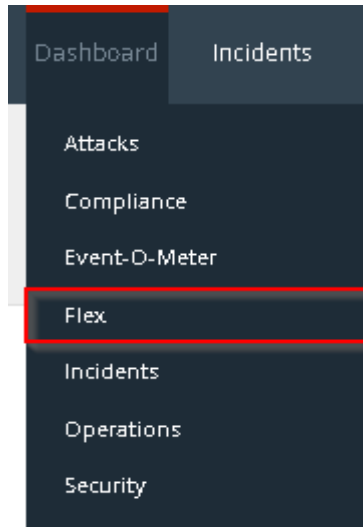


Figure 15

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

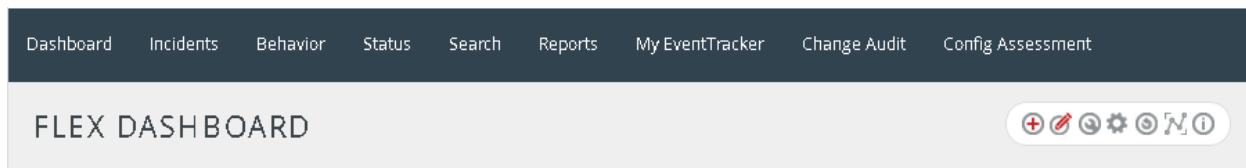



Figure 16

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

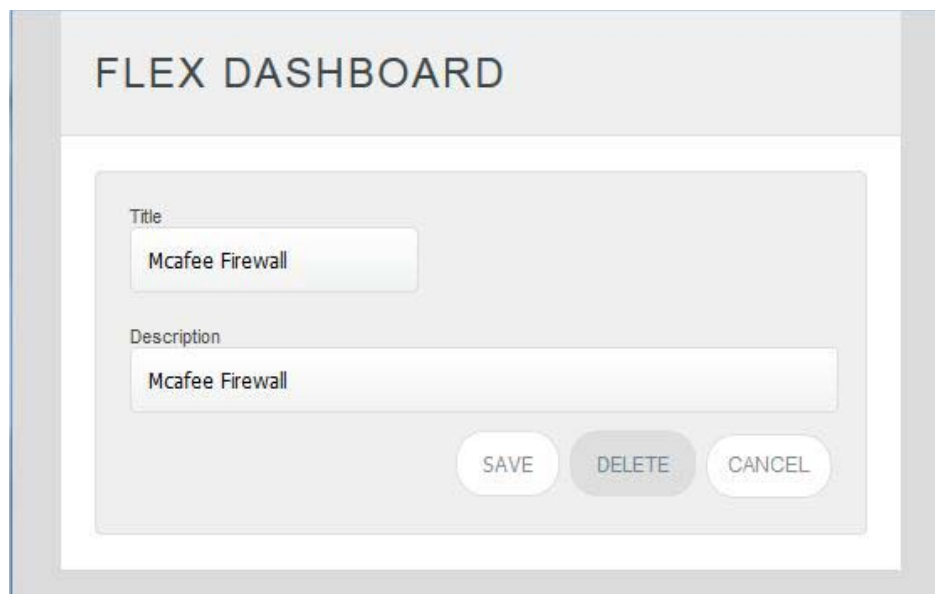


Figure 17

WIDGET CONFIGURATION

WIDGET TITLE: McAfee Firewall Configuration Change

NOTE:

DATA SOURCE: McAfee Firewall Configuration Change

CHART TYPE: None

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: Select column

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

FILTER VALUES:

LEGEND [SERIES]: Select column

SELECT: All

TEST CONFIGURE CLOSE

Figure 18

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.

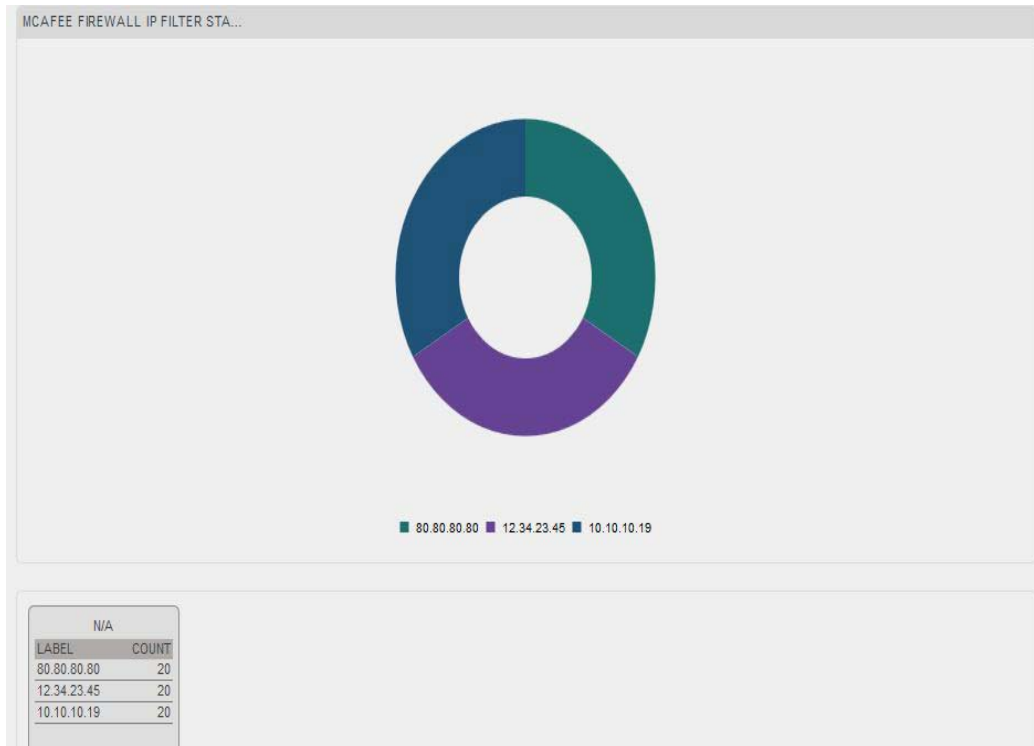



Figure 19

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



Figure 20

15. Click 'customize'  to locate and choose created dashlet.

16. Click  to add dashlet to earlier created dashboard.

Sample Dashboards

1. McAfee Firewall Configuration Change(Modify/Restore/Apply)

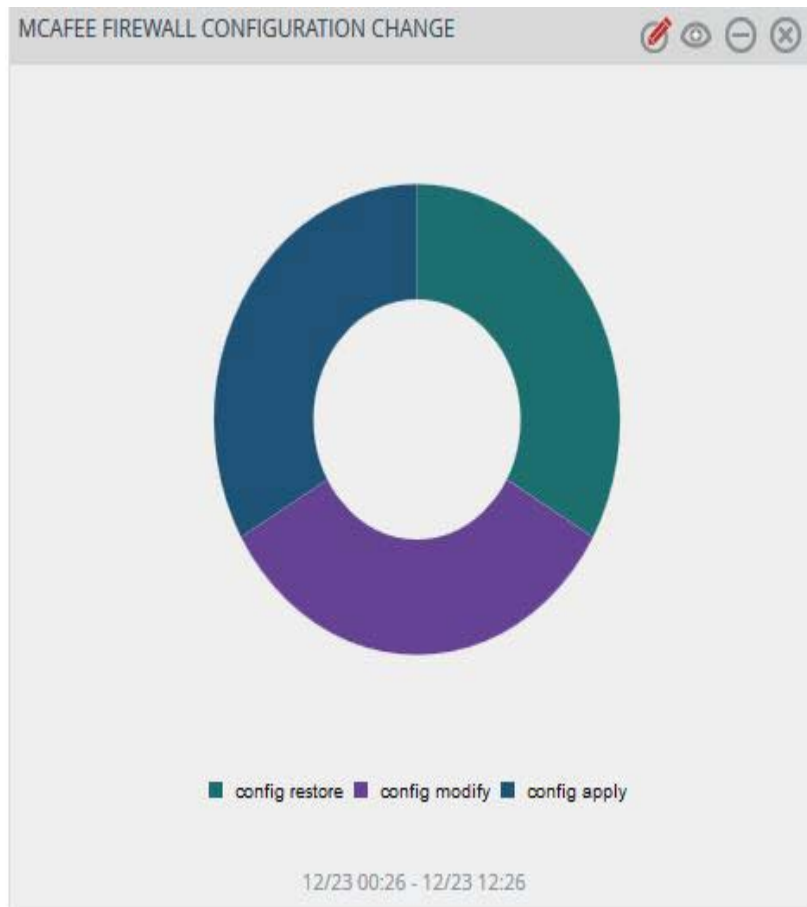


Figure 21

2. McAfee Firewall IP Filter Status(Open/Closed/Timeout)



Figure 22

Sample Reports

1. McAfee Firewall IP Filter Status(Open/Closed/Timeout)

McAfee Firewall IP Filter Session Status									
LogTime	Computer	Type	Domain Name	EDomain	Host name	Source Address	Source Port	Destination Address	Destination Port
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	twitter.com	10.10.10.19	1345	70.12.34.45	9234
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	twitter.com	10.10.10.19	1345	70.12.34.45	9234
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	hi5.com	12.34.23.45	1612	12.34.45.56	9345
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	twitter.com	10.10.10.19	1345	70.12.34.45	9234
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	hi5.com	12.34.23.45	1612	12.34.45.56	9345
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	twitter.com	10.10.10.19	1345	70.12.34.45	9234
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	hi5.com	12.34.23.45	1612	12.34.45.56	9345
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	twitter.com	10.10.10.19	1345	70.12.34.45	9234
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	hi5.com	12.34.23.45	1612	12.34.45.56	9345
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	twitter.com	10.10.10.19	1345	70.12.34.45	9234
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	Facebook.com	80.80.80.80	1662	70.70.70.70	9003
12/23/2015 12:15:14 PM	MFFIP1	t_ipfttraffic	wert	wert	hi5.com	12.34.23.45	1612	12.34.45.56	9345

2. McAfee Firewall Configuration Change(Modify/Restore/Apply)

McAfee Firewall Configuration Change											
LogTime	Computer	Type	PID	Domain Name	EDomain	Host name	Event Name	User Name	Information	LogLevel	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11349	CARW	CARW	hi5.com	config apply	johnathan	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11349	CARW	CARW	hi5.com	config apply	johnathan	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11349	CARW	CARW	hi5.com	config apply	johnathan	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11349	CARW	CARW	hi5.com	config apply	johnathan	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11349	CARW	CARW	hi5.com	config apply	johnathan	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11349	CARW	CARW	hi5.com	config apply	johnathan	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11234	CARW	CARW	twitter.com	config restore	raechel	Changed ACLD	3	
12/23/2015 12:15:15 PM	MFCC	t_cfg_change	11589	CARW	CARW	Facebook.com	config modify	michel	Changed ACLD	3	