Netsurion™ | EventTracker

Integrate WatchGuard XTM

EventTracker v9.x or above

Publication Date: July 24, 2019

Abstract

This guide provides instructions to configure WatchGuard XTM to send the event logs to EventTracker. Once events are configured to send to EventTracker alerts, dashboard and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and later, and WatchGuard XTM Fireware v12.5

Audience

WatchGuard XTM users, who wish to forward event logs to EventTracker and monitor events using EventTracker.

Table of Contents

Overview

WatchGuard XTM Series appliances combine firewall/VPN with powerful security services and a suite of flexible management tools.

EventTracker continually collects firewall events and leverages machine learning to identify possible attacks, suspicious network traffic and user behavior analytics.

Prerequisites

- EventTracker v9.x and later should be installed.
- Fireware OS v12.5 or later should be deployed and configured.
- User must have device Administrator access credentials for the WatchGuard XTM and EventTracker.
- Port 514 must be opened on WatchGuard XTM.
- Port 514 must not be used by other services of WatchGuard XTM.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.

Configure syslog forwarding to EventTracker

To collect events from Fireware OS, you must configure your Firebox to send events to EventTracker. You can use Policy Manager or Fireware Web UI to make the changes. In this Integration Guide, we are using Web UI.

Follow the below steps to configure syslog forwarding to EventTracker.

1. Login to Fireware Web UI.
2. Select **System** from left side pane.
3. Select **Logging** and then click the **Syslog Server** tab.

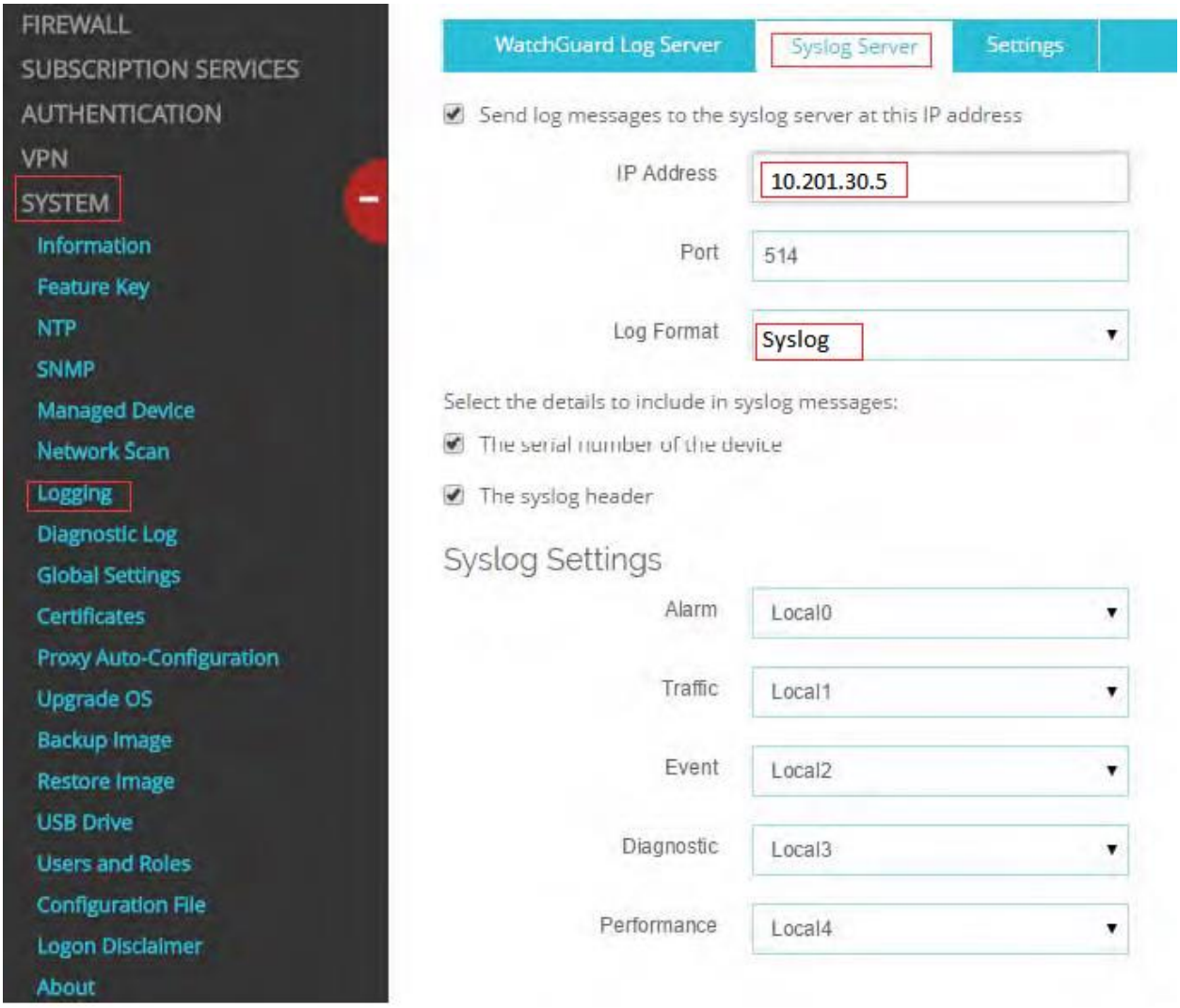

Figure 1

4. In the Syslog Server section, select the **Send log messages to the syslog server at this IP address** check box.
5. In the **IP Address** text box, type the IP address of the EventTracker machine.
6. In the **Port** text box, type 514.
7. From the **Log Format** drop-down list, select "**Syslog**".
8. Select both check boxes '**The serial number of the device'** and '**The syslog header**'.
9. In the Syslog Settings section, ensure each log level is assigned a facility.
10. Click **Save**.
11. Go to **Diagnostic Log** under **System.**

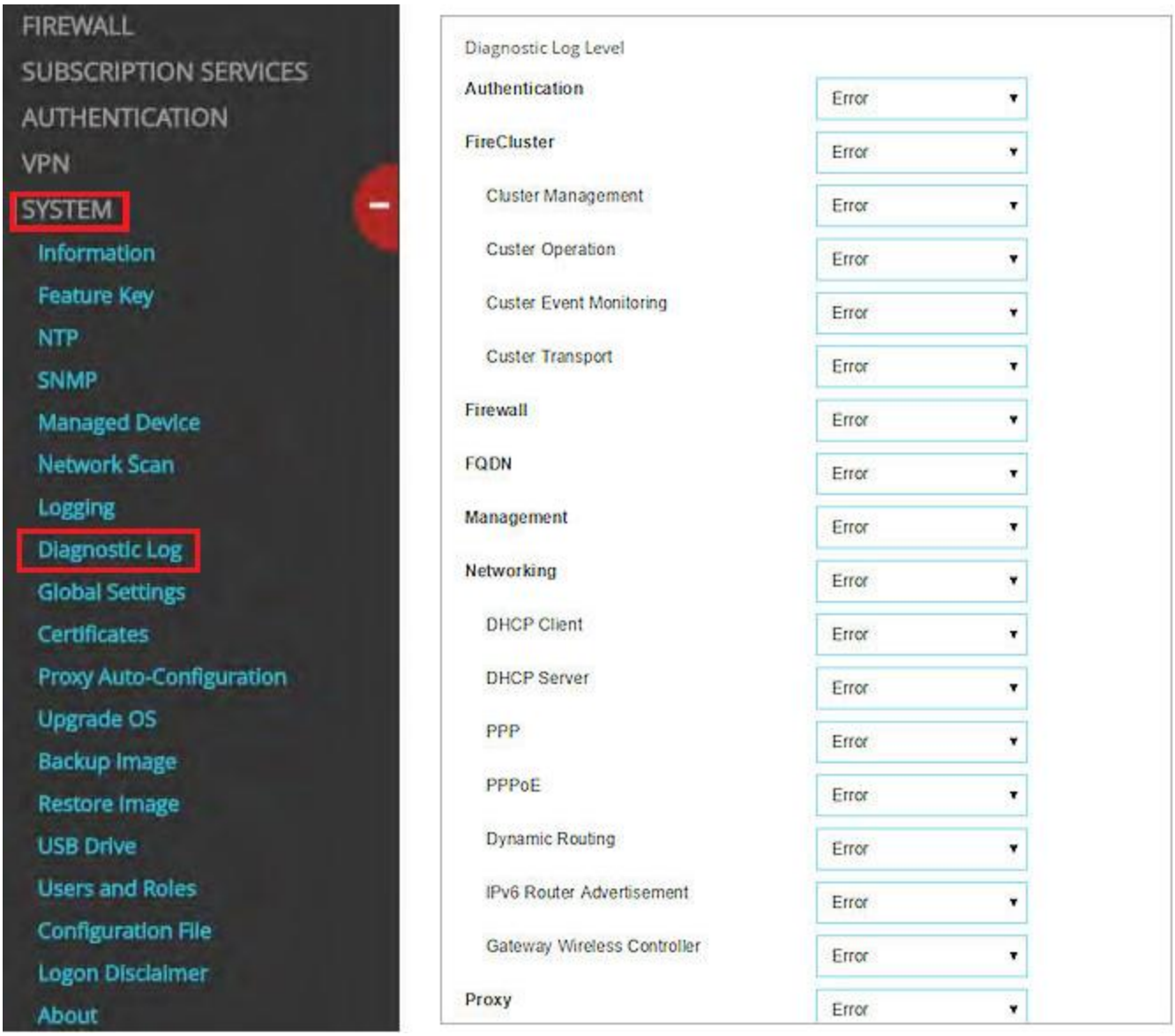

Figure 2

12. In **Diagnostic Log Level**, select **Information** from the drop-down list for each log type.
13. Click **Save**.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; Categories, Alerts, Reports and Dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7.x and later to support WatchGuard XTM monitoring:

NOTE: The EventTracker Knowledge Pack files (Category, Alert, Report, Knowledge Object, etc.) for WatchGuard Fireware v12.5 and earlier version can be collected from the EventTracker support (support@eventtracker.com).

Categories

- **WatchGuard XTM: Authentication failure -** This category provides information related to user authentication failure.
- **WatchGuard XTM: Authentication success -** This category provides information related to user authentication success.
- **WatchGuard XTM: Configuration changed -** This category provides information related to configuration change.
- **WatchGuard XTM: DHCP activity -** This category provides information related to DHCP activity.
- **WatchGuard XTM: Firewall allowed traffic -** This category provides information related to traffic allowed by firewall.
- **WatchGuard XTM: Firewall denied traffic -** This category provides information related to traffic denied by firewall.
- **WatchGuard XTM: Interface status -** This category provides information related to change in interface status.
- **WatchGuard XTM: IPS attack detected -** This category provides information related to attacks detected by IPS.
- **WatchGuard XTM: PPOE session details -** This category provides information related to PPOE sessions.
- **WatchGuard XTM: Proxy policy allowed traffic -** This category provides information related to traffic allowed by proxy policy.
- **WatchGuard XTM: Proxy policy denied traffic -** This category provides information related to traffic denied by proxy policy.
- **WatchGuard XTM: Security services error -** This category provides information related to security services error.
- **WatchGuard XTM: VPN session details -** This category provides information related to VPN sessions.

Alerts

- **WatchGuard XTM**: **Attack detected**- This alert is generated when any attack is detected by WatchGuard XTM firewall.
- **WatchGuard XTM**: **Authentication server unavailable**- This alert is generated when authentication server is unavailable for authentication.
- **WatchGuard XTM**: **Customized certificate generation error**- This alert is generated when customized certificate generation error occurs.

- **WatchGuard XTM**: **Device configuration changed**-This alert is generated when device configuration is changed by a user.
- **WatchGuard XTM: Feature expiration reminder**- This alert is generated when particular feature is about to expire and so WatchGuard XTM generates a reminder event. EventTracker captures it and shows on the Incident dashboard.
- **WatchGuard XTM: Feature key download failed**- This alert is generated when a particular feature key is downloaded.
- **WatchGuard XTM**: **Feature key expired**- This alert is generated when a feature key is expired.
- **WatchGuard XTM**: **Shutdown requested by system**- This alert is generated when shutdown is requested by system.
- **WatchGuard XTM**: **User authentication failed**- This alert is generated when user tries to authenticate and it fails.
- **WatchGuard XTM: User logon failed**- This alert is generated when user tries to logon and it fails.

Reports

- **WatchGuard XTM-Device configuration change details:** This report provides information related to device configuration change, when a user performs any changes in WatchGuard XTM. This report captures the changed item information in column called message details and also shows what time and which firewall device configuration changes have been done.

- **WatchGuard XTM-System management details:** This report provides information related to system management like system is shutdown, system is restarted, system is upgraded, system is backed up etc. This report has a column called message details which contains the information about what have been performed by user or system. It also shows what time and on which firewall device it has happened.

- **WatchGuard XTM-User logon and logout success:** This report provides information related to user logons. This report captures at what time a particular user has logged in or logged out from specific IP address and what IP address has been assigned to him.

- **WatchGuard XTM-User authentication failed:** This report provides information related to user authentication failure event. When a user tries to authenticate and it fails, it gives the reason why the authentication failed.

- **WatchGuard XTM-User authentication success:** This report provides information related to authentication success event, when a user tries to authenticate and it gets success. This report has the columns LogTime, Computer or Device name, Username, User Type and Source Address.

- **WatchGuard XTM-User logon failed:** This report provides information related to user logon failure event i.e. when a user tries to login and it fails. It has the column LogTime, Computer or Device name, Username, User Type and Source Address and Assigned Virtual Client IP Address.

- **WatchGuard XTM-Attack detected:** This report provides information related to attack detected by WatchGuard XTM. It contains the columns LogTime, Computer or Device name, Attack Type, Source Address and Target Address.

- **WatchGuard XTM-IP spoofing and blocked site traffic detected:** This report provides information related to IP spoofing and blocked site traffic detection. It has the column LogTime, Computer or Device name, Traffic Type, Source Address and Target Address.

- **WatchGuard XTM-Traffic details:** This report provides information related to inbound and outbound traffic. It has the column LogTime, Computer or Device name, Status, In Interface Name, Out Interface Name, Source IP Address, Source Port, Destination IP Address, Destination Port, Application Behavior Name, Application Category ID, Application ID, Application Name, Category Name, Message, Policy Name.

- **WatchGuard XTM-IPS traffic detected:** This report provides information related to IPS traffic detection. It has the column LogTime, Computer or Device name, Status, Message, In Interface Name, Out Interface Name, Source IP Address, Source Port, Destination IP Address, Destination Port, Policy Name, Signature Category, Signature ID, Signature Name.

Import Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.

2. Double click **Export/Import Utility**.

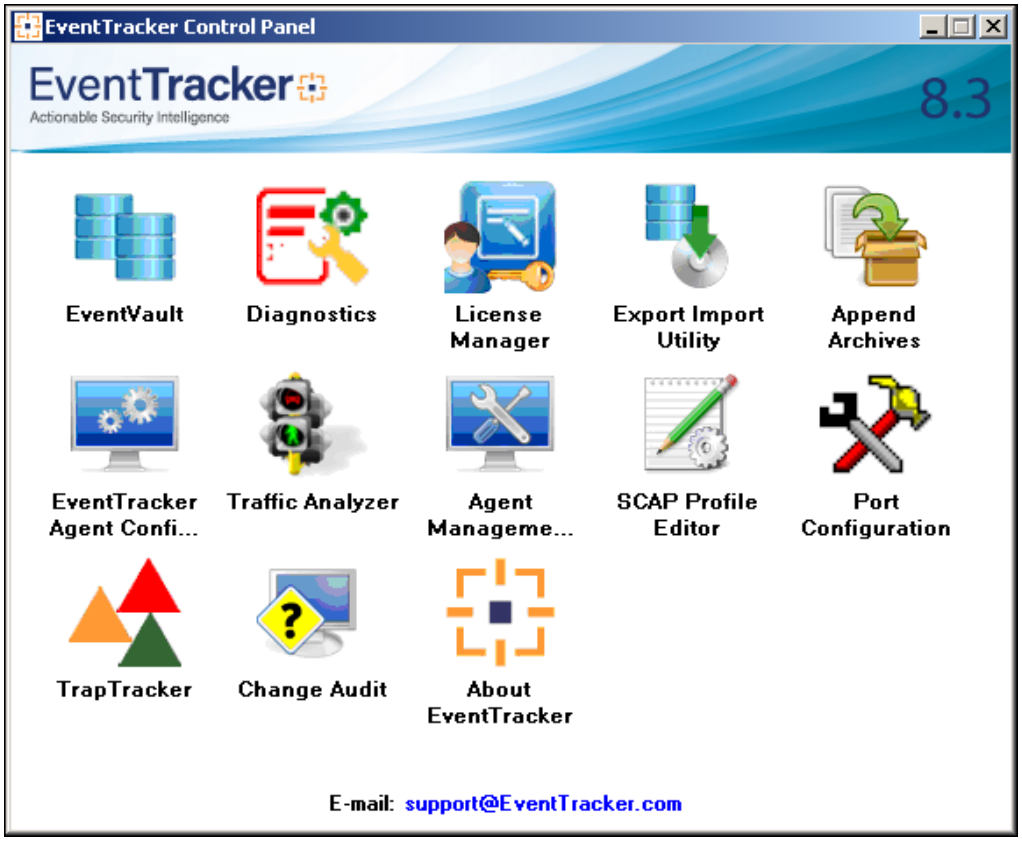

Figure 3

3. Click the **Import** tab.

NOTE: Import the following KP items in the specified sequence.

a. **Category**
b. **Alerts**
c. **Parsing Rules**
d. **Templates**
e. **Reports**
f. **Knowledge Object**

Import Category

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

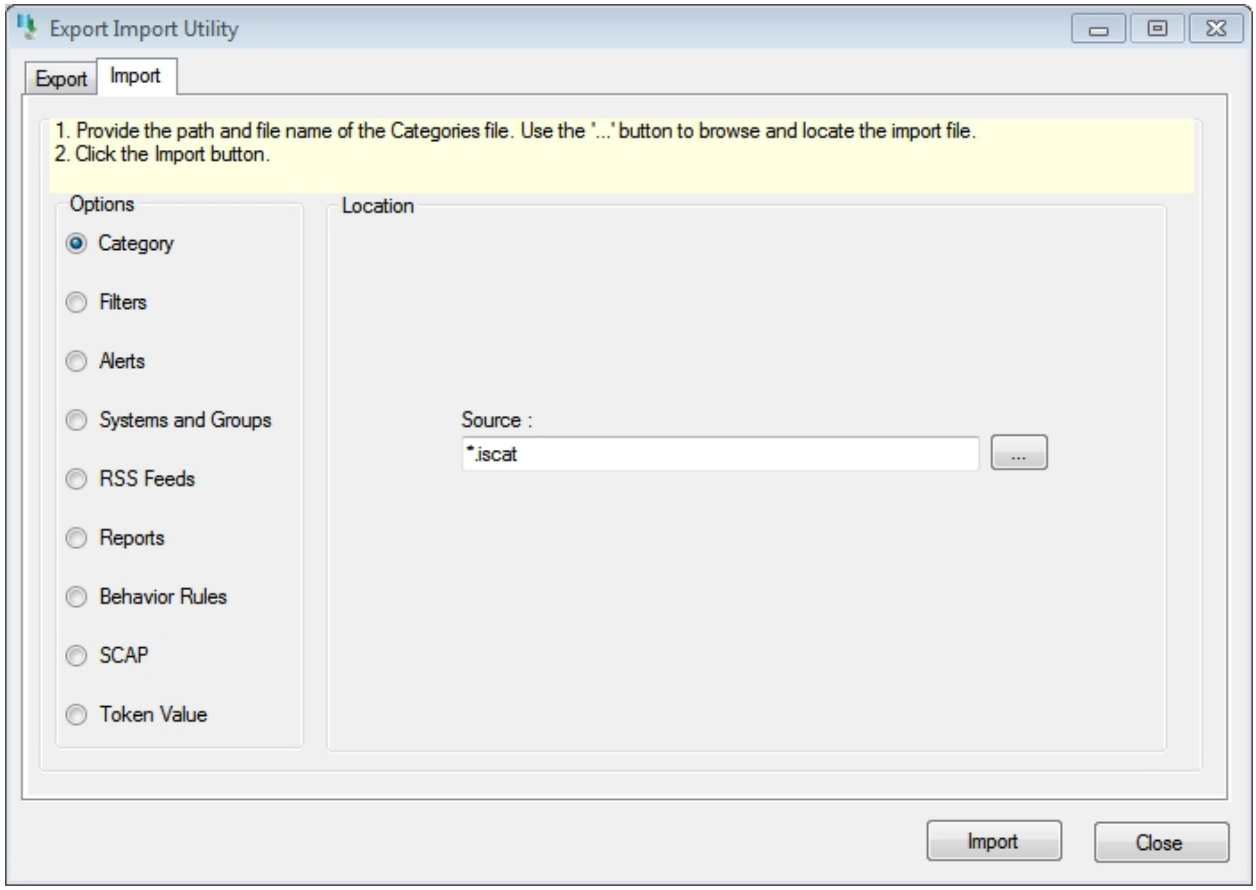

Figure 4

2. Locate **All WatchGuard XTM group categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

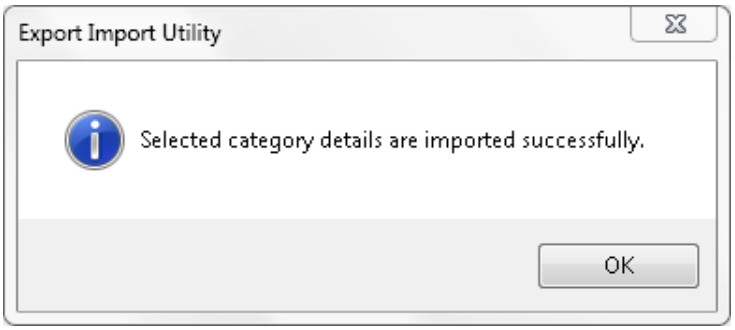

Figure 5

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

Import Alerts

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

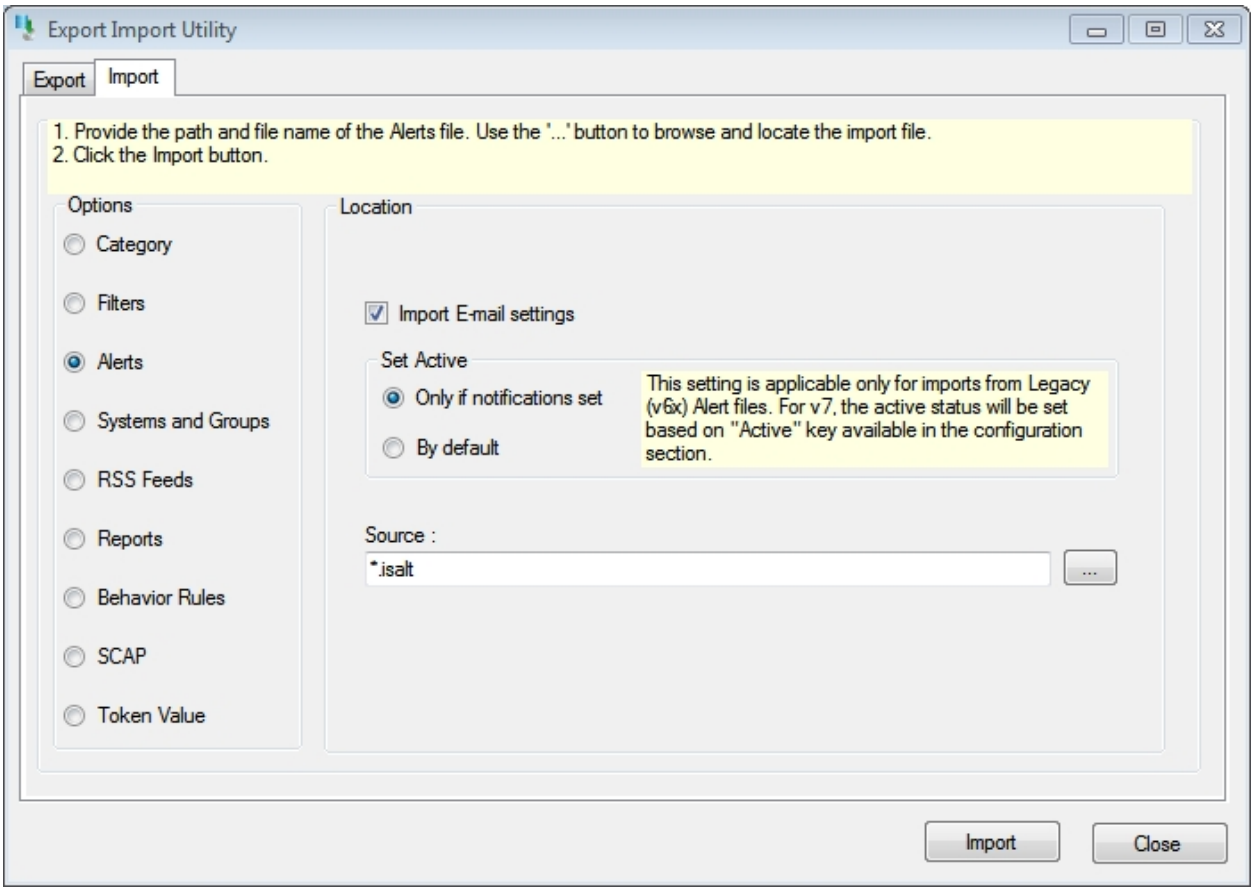

Figure 6

2. Locate **All WatchGuard XTM group alerts.isalt** file, and then click the **Open** button.

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

EventTracker displays success message.

Figure 7

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

Import Parsing Rules

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

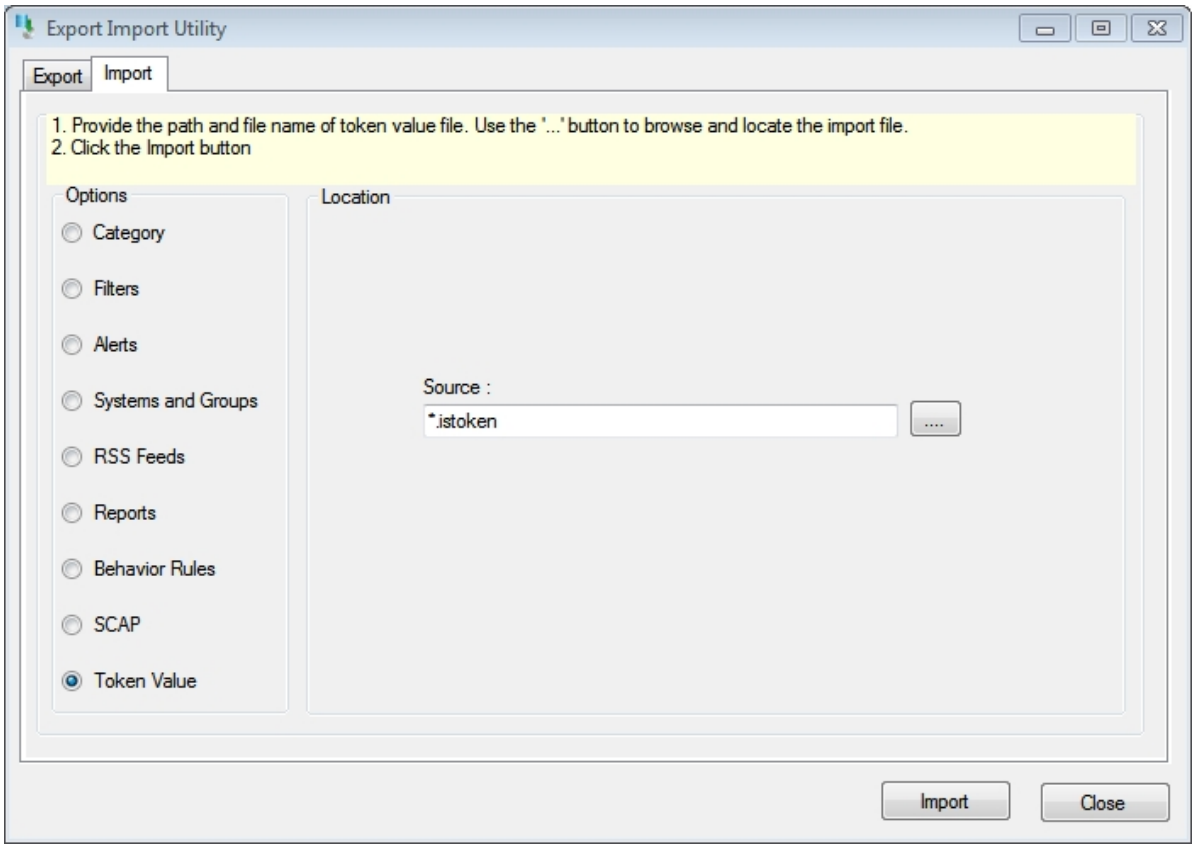

Figure 8

2. Locate the **All Malwarebytes group of parsing rules.istoken** file, and then click the **Open** button.
3. To import tokens, click the **Import** button.
   EventTracker displays success message.

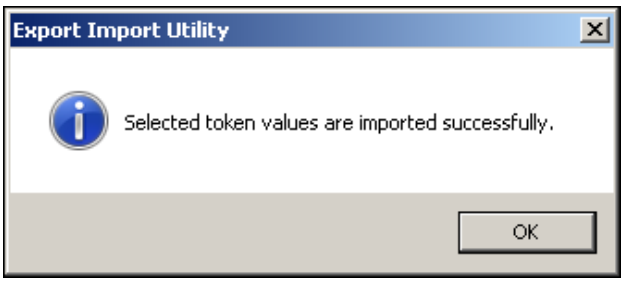

Figure 9

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

Import Template

1. Login to EventTracker, click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ‘**Import**’ option.

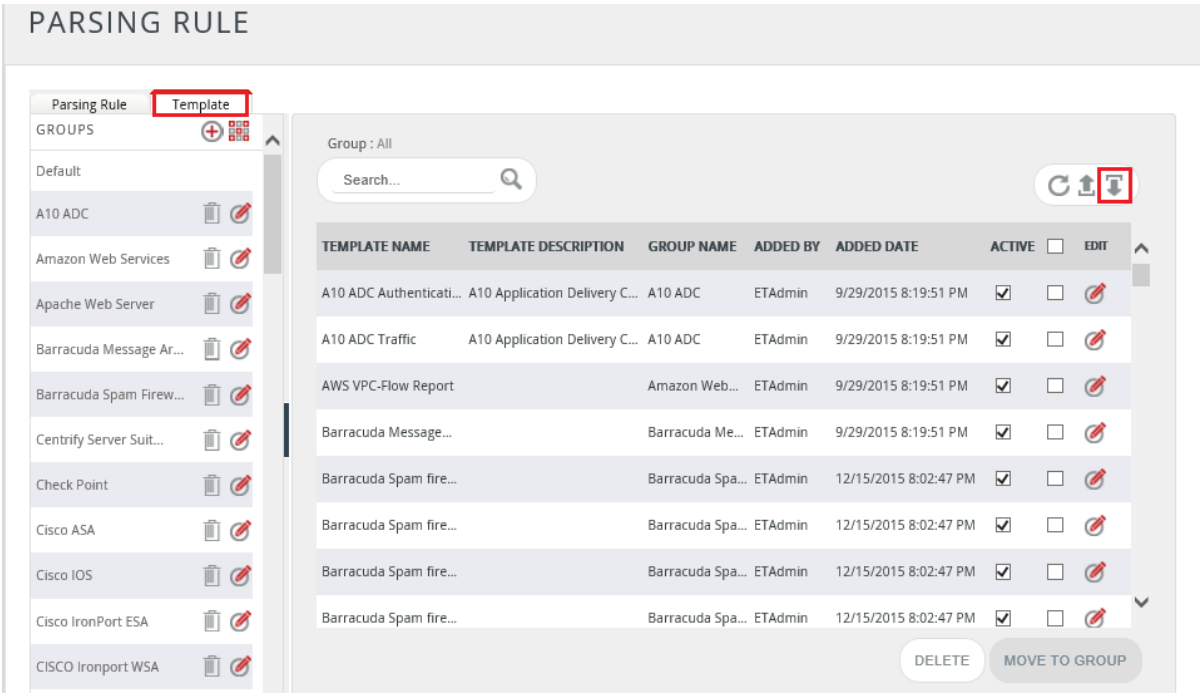

Figure 10

3. Click on **Browse** button.

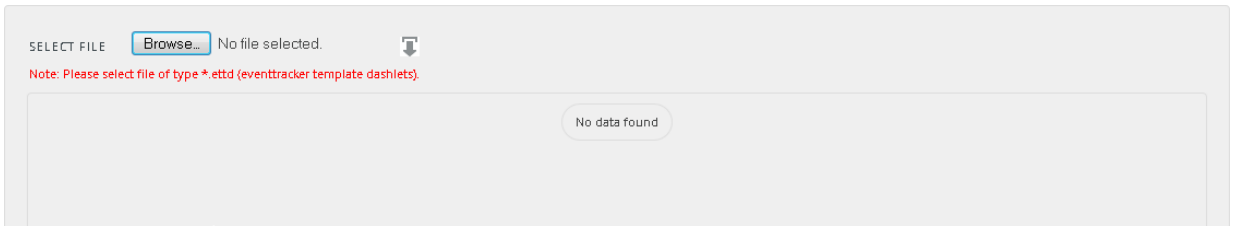

Figure 11

4. Locate **WatchGuard XTM group template.ettd** file, and then click the **Open** button.

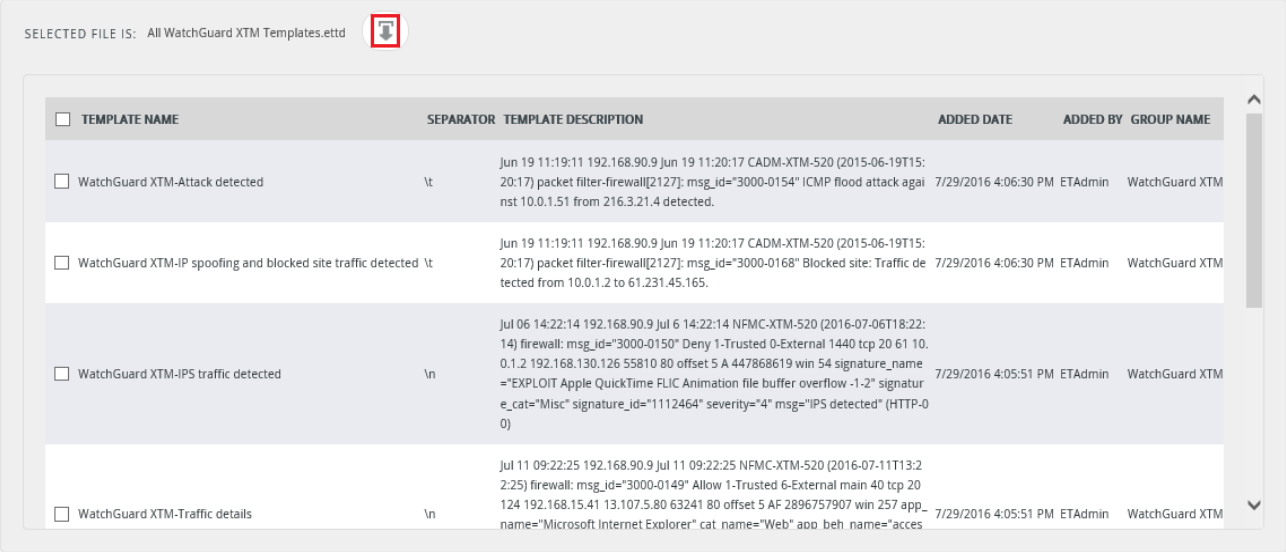

Figure 12

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

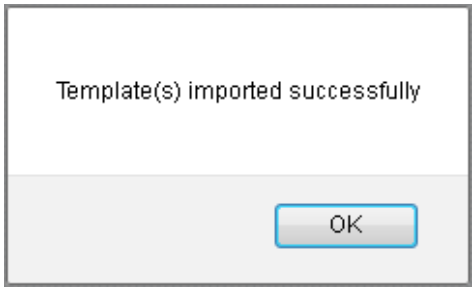

Figure 13

6. Click on **OK** button.

Import Flex Reports

1. Click **Reports** option, and then click the browse ... button.
2. Locate **All WatchGuard XTM group reports.issch** file, and then click the **Open** button.

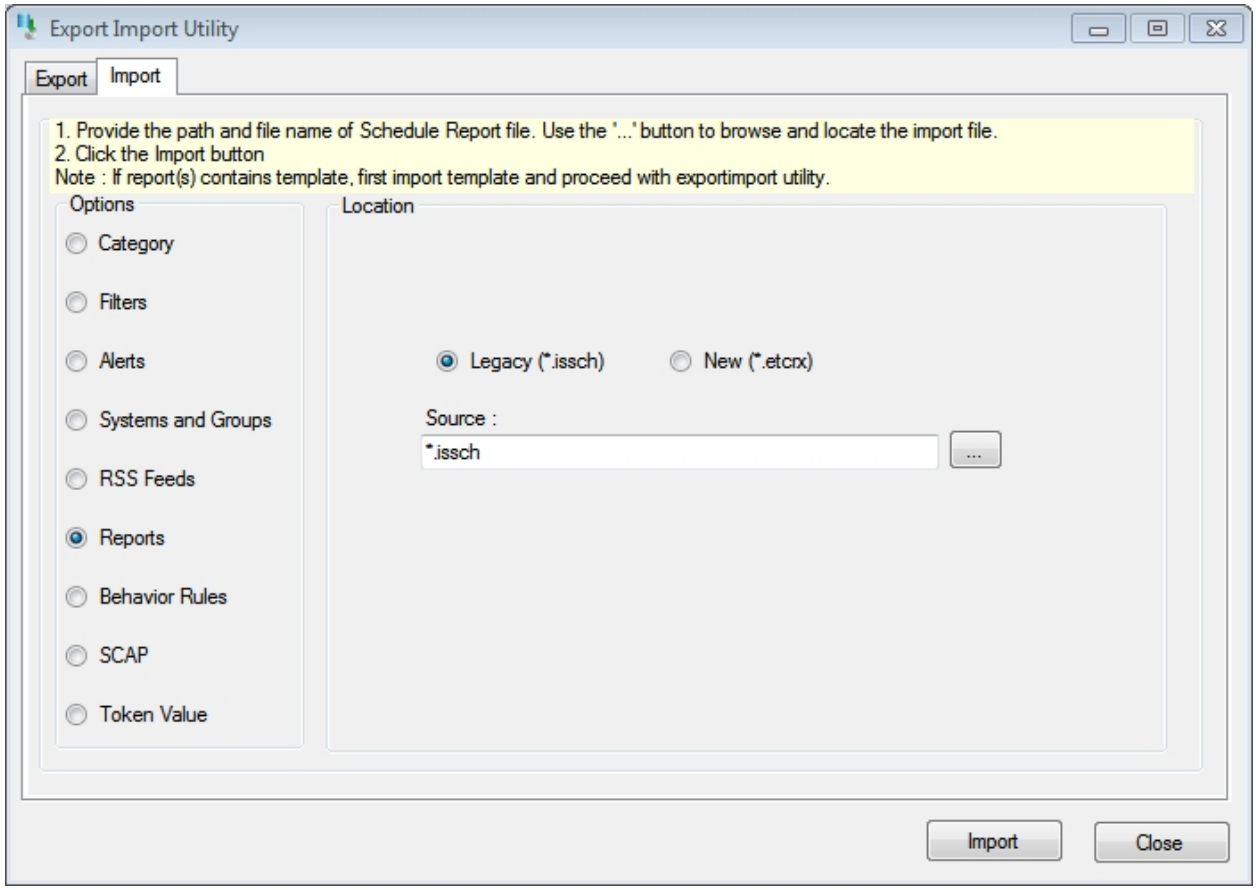

Figure 14

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

   EventTracker displays success message.

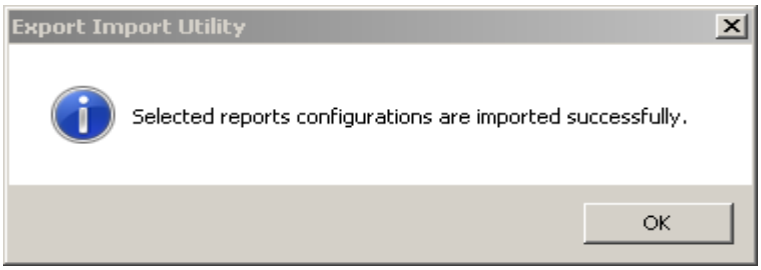

Figure 15

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.

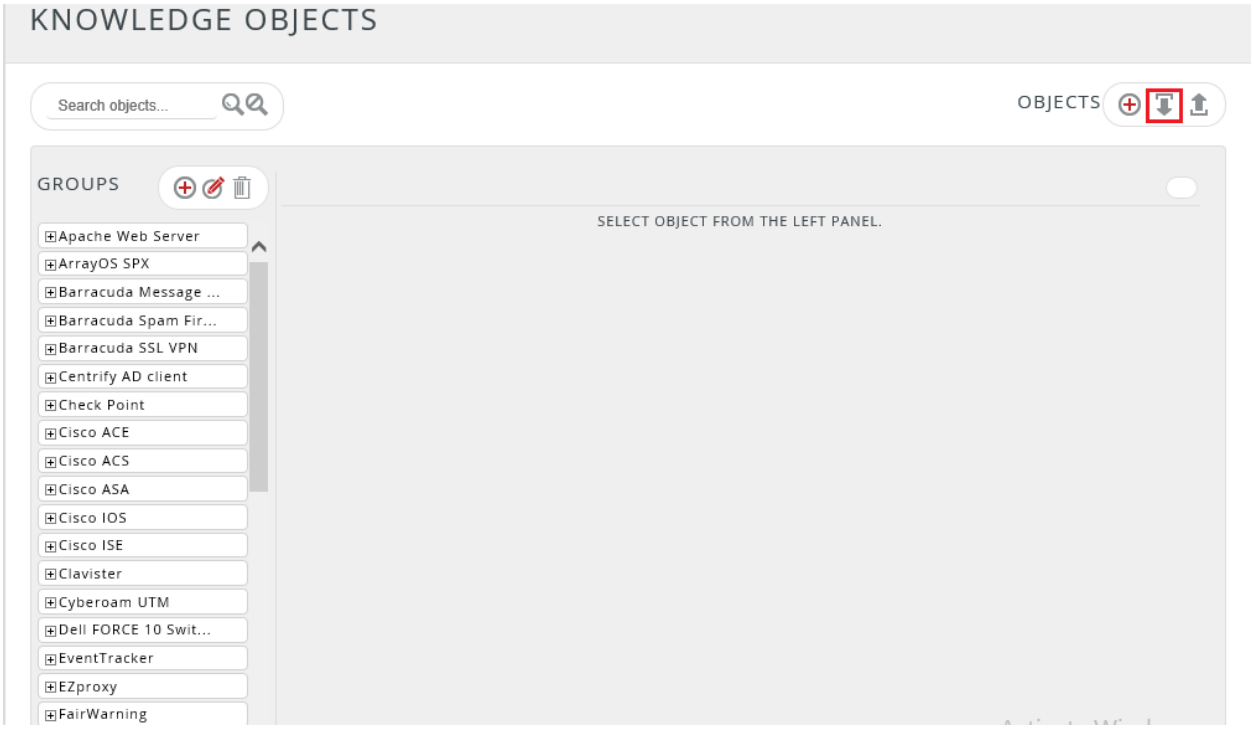

Figure 16

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

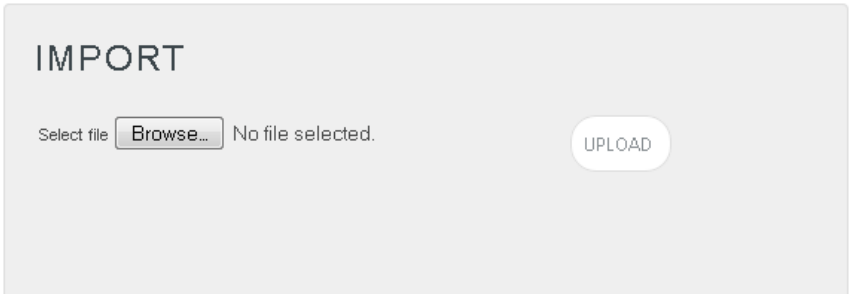

Figure 17

4. Locate **WatchGuard XTM group KO.etko** file, and then click the **UPLOAD** button.

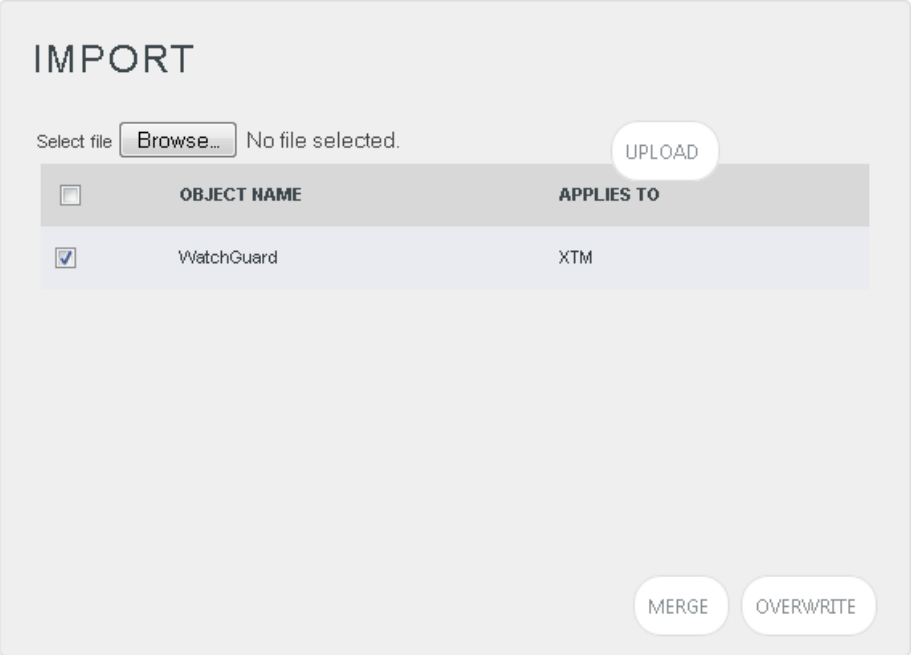

Figure 18

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

   EventTracker displays success message.

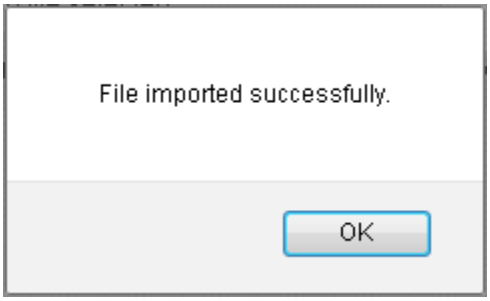

Figure 19

6. Click on **OK** button.

Verify Knowledge Pack in EventTracker

Logon to **EventTracker**

Verify Categories

1. Click the **Admin** menu, and then click **Categories**.

2. To view the imported categories, in the **Category Tree**, expand **WatchGuard XTM** group folder.

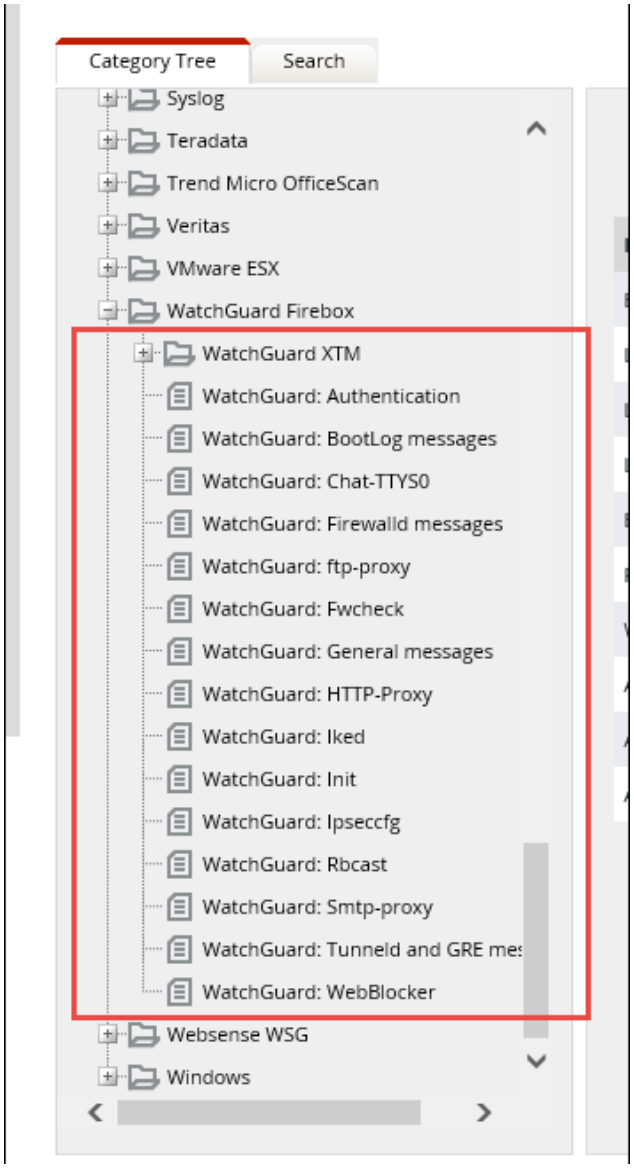

Figure 20

Verify Alerts

1. Click the **Admin** menu, and then click **Alerts**.
2. In the **Search** box, type '**WatchGuard**', and then click the '**search**' button.

   Alert Management page will display all the imported alerts.

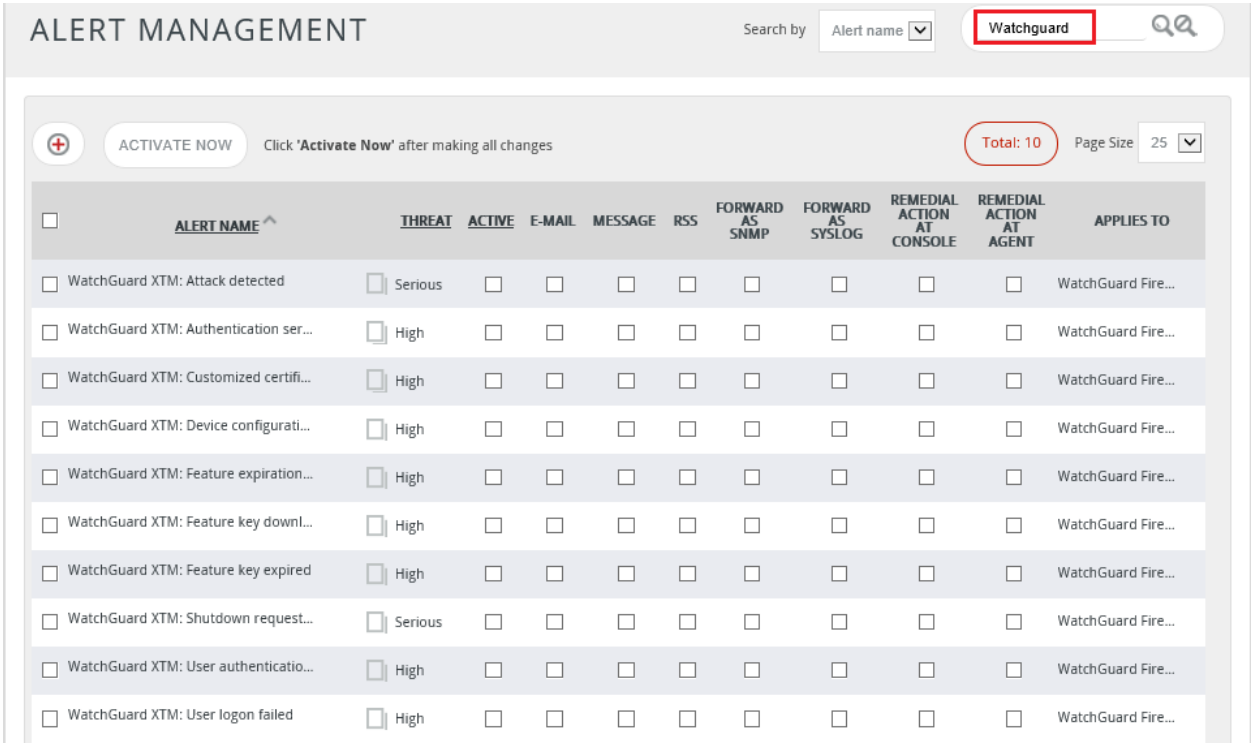

Figure 21

3. To activate the imported alerts, select the respective checkbox in the **Active** column and then click the **Activate Now** button.

   EventTracker displays message box.

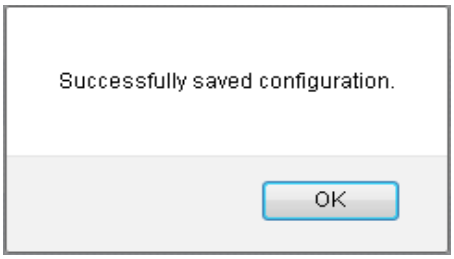

Figure 22

4. Click **OK**.

Verify Flex Reports

1. Click the **Reports** menu, and then **Configuration**.
2. Select **Defined** in report type.
3. In **Report Groups Tree** to view imported Reports, scroll down and click **WatchGuard XTM** group folder.

- The Reports are displayed in the Reports configuration pane. The imported reports can further be scheduled as per requirement.

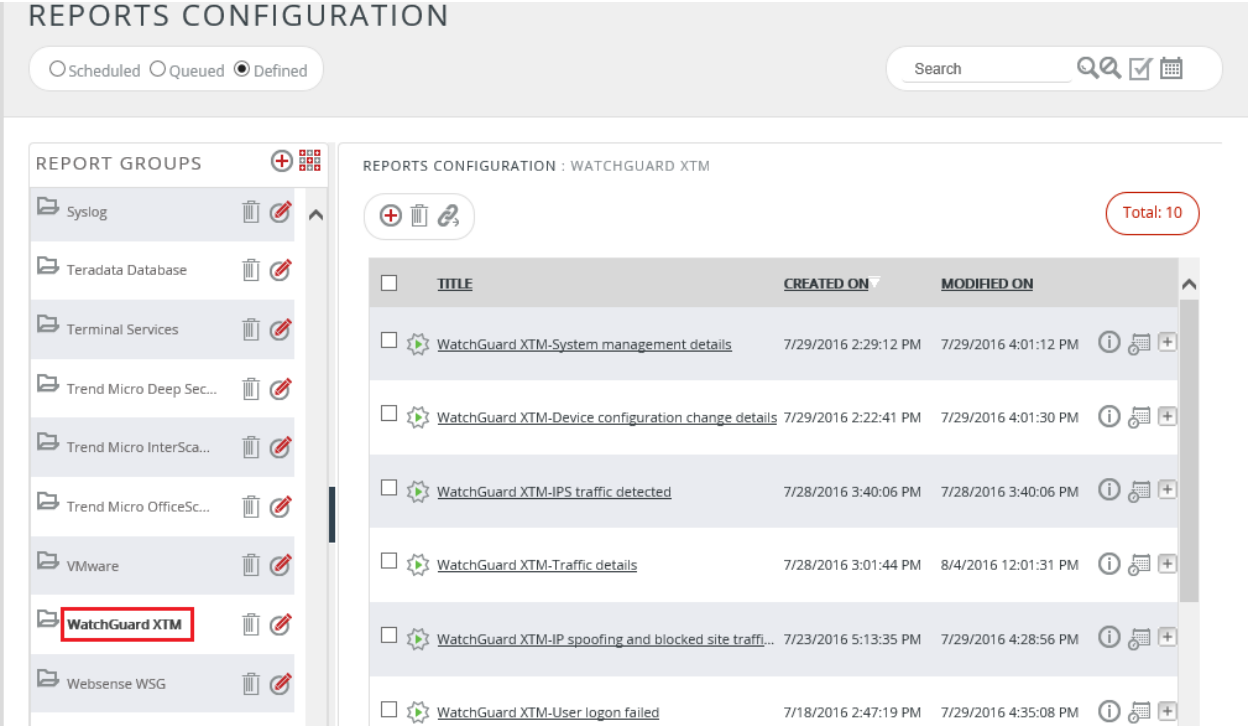

Figure 23

Verify Parsing Rule

1. Click the **Admin** menu, and then click **Parsing rule**.

   The imported WatchGuard XTM Parsing rules are added in Token-Value Groups list.

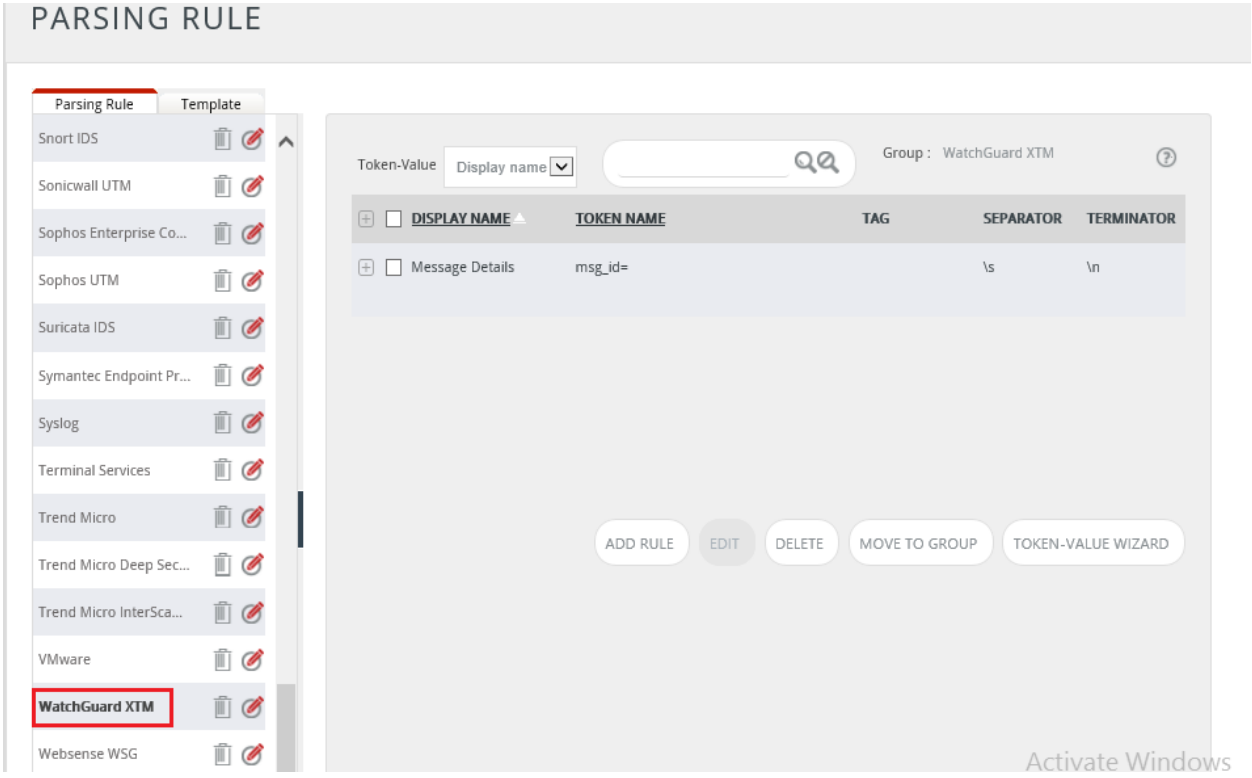

Figure 24

Verify Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab.
3. Scroll and find imported **WatchGuard XTM** templates.

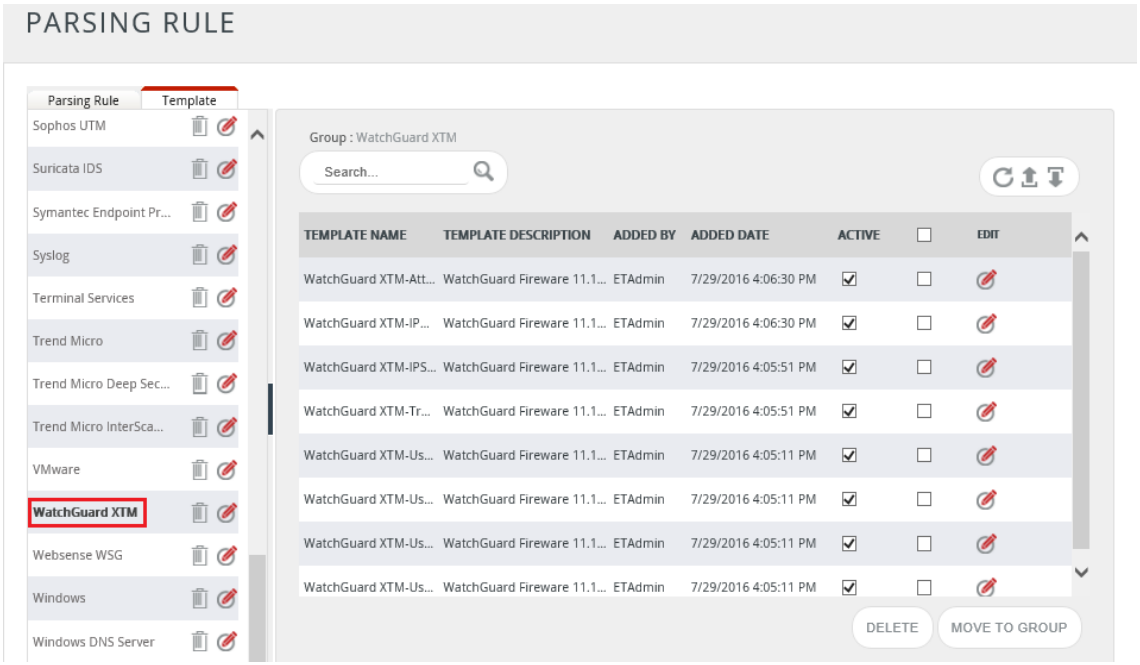

Figure 25

Verify Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects.**
2. Scroll down and select **WatchGuard** in Groups pane.
   Imported WatchGuard object details are shown.

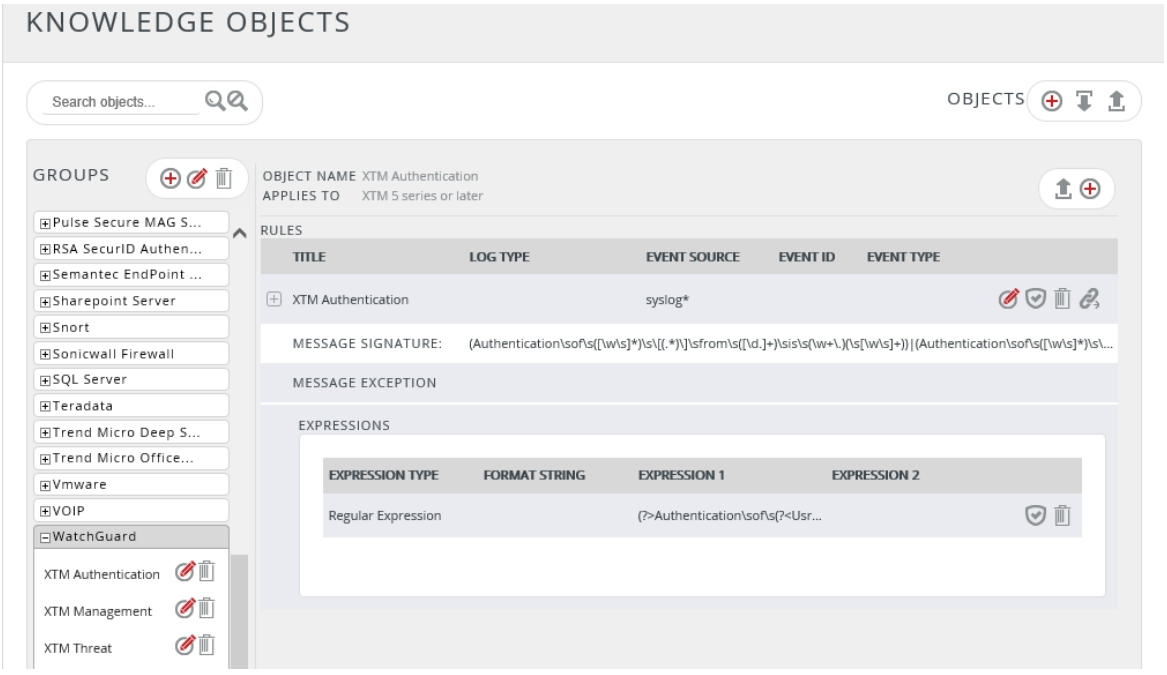

Figure 26

Sample Reports & Logs

WatchGuard XTM–User authentication failed

Sample Report

WatchGuard XTM-User authentication failed

LogTime	Computer	Username	User Type	Source Address	Reason
07/20/2016 06:10:11 PM	WATCHTEST	user@Firebox-DB	PPTP	192.168.9.2	The user is in the wrong group
07/20/2016 06:10:29 PM	WATCHTEST	robert@example.com			Both primary and secondary servers are unavailable
07/20/2016 06:10:58 PM	WATCHTEST	mike@RADIUS	firewall		RADIUS authentication method MSCHAP_V1 is not supported
07/20/2016 06:11:13 PM	WATCHTEST	jack			Domain not found
07/20/2016 07:10:23 PM	WATCHTEST	smith@Firebox-DB	PPTP	192.168.9.2	The user is in the wrong group

Figure 27

Relevant Log

Jun 19 09:17:14 192.168.90.9 Jun 19 09:18:19 CADM-XTM-520 (2015-06-19T13:18:19) authentication-management [2021]: Authentication of firewall user [user1@RADIUS] failed. RADIUS authentication method MSCHAP_V1 is not supported.
Jun 30 06:52:53 172.17.1.6 Jun 30 06:52:53 WVSAO-1-810 80B502F579BAE WVSAO-810-Cluster (2016-06-30T10:52:53) sessiond[1588]: msg_id="1100-0005" Authentication of PPTP user [user1@Firebox-DB] from 192.168.9.2 is rejected. The user is in the wrong group.

Table 1

WatchGuard XTM-Attack detected

Sample Report

WatchGuard XTM-Attack detected

LogTime	Computer	Attack Name	Source Address	Target Address
07/23/2016 04:17:05 PM	WATCHTEST	IPv4 source route	10.0.1.34	
07/23/2016 04:17:21 PM	WATCHTEST	SYN flood	216.3.21.4	10.0.1.51
07/23/2016 04:17:32 PM	WATCHTEST	ICMP flood	216.3.21.4	10.0.1.51
07/23/2016 04:17:44 PM	WATCHTEST	UDP flood	12.34.23.67	32.21.56.8
07/23/2016 04:17:56 PM	WATCHTEST	IPSEC flood	12.34.23.67	32.21.56.8
07/23/2016 04:18:20 PM	WATCHTEST	IKE flood	12.34.23.67	32.21.56.8
07/23/2016 04:18:33 PM	WATCHTEST	IP scan	12.34.23.67	32.21.56.8
07/23/2016 04:18:47 PM	WATCHTEST	PORT scan	12.34.23.67	32.21.56.8
07/23/2016 04:19:11 PM	WATCHTEST	SYN flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
07/23/2016 04:19:42 PM	WATCHTEST	ICMP flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
07/23/2016 04:19:56 PM	WATCHTEST	UDP flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
07/23/2016 04:20:14 PM	WATCHTEST	IPSEC flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
07/23/2016 04:20:28 PM	WATCHTEST	IKE flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Figure 28

Relevant Log

Jun 19 11:19:11 192.168.90.9 Jun 19 11:20:17 Nyt-XTM-520 (2015-06-19T15:20:17) packet filter-firewall [2127]: IPSEC flood attack against 32.27.56.78 from 127.34.243.67 detected.
Feb 08 09:33:52 172.17.1.6 Feb 8 09:33:51 Crows-2-810 80B502F5EBE2E Crows-810-Cluster (2016-02-08T14:33:51) firewall: msg_id="3000-0150" Deny tun0 1-Trusted 820 tcp 20 62 192.168.16.79 172.16.14.34 51870 445 offset 5 A 2325226339 win 8003 signature_name="SMB Microsoft DLL Planting Remote Code Exectution Vulnerability" signature_cat="Misc" signature_id="1130527" severity="4" msg="IPS detected" src_user="Leo@Production" (Allow SSLVPN-Users-00)

Table 2

WatchGuard XTM–Device configuration change details

Sample Report

WatchGuard XTM-Device configuration change details

LogTime	Computer	Message Details
07/29/2016 01:08:15 PM	WATCHTEST	Management user admin@Firebox-DB from 10.139.36.22 {modified | added | deleted } Blocked Sites Exceptions
07/29/2016 01:08:29 PM	WATCHTEST	Administrative accounts were reset to the default settings
07/29/2016 01:08:37 PM	WATCHTEST	admin added feature key '883B25CCF32949EE'
07/29/2016 01:08:47 PM	WATCHTEST	admin removed feature key '883B25CCF32949EE'
07/29/2016 01:08:59 PM	WATCHTEST	Device default configuration was loaded in safe mode
07/29/2016 01:09:07 PM	WATCHTEST	Device auto restore from USB drive image initiated, reboot needed
07/29/2016 01:09:20 PM	WATCHTEST	System upgrade failed: 'LIVESECURITY' feature expired
07/29/2016 01:09:32 PM	WATCHTEST	Upload of logo succeeded
07/29/2016 01:09:47 PM	WATCHTEST	Upload of logo succeeded
07/29/2016 01:10:08 PM	WATCHTEST	The configuration file and feature key for the device were successfully updated after a request from admin from the Management Server at 10.139.44.88. Revision: dummy_config_rev_id. Comments: update tcp segment.
07/29/2016 01:10:17 PM	WATCHTEST	Device configuration file was successfully updated. Configuration file retrieved from the Management Server at 10.139.44.88.
07/29/2016 01:10:30 PM	WATCHTEST	During a system downgrade, the configuration reset failed

Figure 29

Relevant Log

Nov 06 11:19:11 192.168.90.9 Jun 19 11:20:17 CADM-XTM-520 (2015-06-19T15:20:17) configd[758]: msg_id="0101-0001" admin deleted Blocked_Sites Exceptions
Jun 19 11:19:11 192.168.90.9 Jun 19 11:20:17 CADM-XTM-520 (2015-06-19T15:20:17) configuration-management[2127]: admin deleted Blocked Sites Exceptions

Table 3

WatchGuard XTM-User logon and logout success

Sample Report

WatchGuard XTM-User logon and logout success

LogTime	Computer	Username	User Type	Source Address	Status	Assigned Virtual Client IP
07/20/2016 06:10:11 PM	WATCHTEST	louis@wvauditor.com	SSL VPN	182.156.92.60	logged in	192.168.113.2
07/20/2016 06:10:29 PM	WATCHTEST	mike@wvauditor.com	SSL VPN	182.156.92.18	logged out	192.168.113.2
07/20/2016 06:10:58 PM	WATCHTEST	john@wvauditor.com	management	182.156.92.198	logged in	
07/20/2016 06:11:13 PM	WATCHTEST	jack@wvauditor.com	management	182.156.92.80	logged out	

Figure 30

Relevant Log

Jun 19 09:17:14 192.168.90.9 Jun 19 09:18:19 CADM-XTM-520 (2015-06-19T13:18:19) accounting-management [2021]: Management user admin from 10.0.1.2 log in attempt was rejected.
Jun 30 06:52:53 172.17.1.6 Jun 30 06:52:53 local-1-810 80B502F579BAE local-810-Cluster (2016-06-30T10:52:53) sessiond[1588]: msg_id="3E00-0002" SSL VPN user et_support@wvauditor.com from 182.156.92.138 logged in assigned virtual IP is 192.168.113.2

Table 4

WatchGuard XTM–Traffic details

Sample Report

WatchGuard XTM-Traffic details

LogTime	Computer	Status	In Interface Name	Out Interface Name	Source IP Address	Source Port	Destination IP Address	Destination Port
07/28/2016 02:43:14 PM	WATCHTEST	Deny	1-Trusted	6-External	192.168.90.38	59136	37.252.230.28	5938
07/28/2016 02:43:24 PM	WATCHTEST	Allow	1-Trusted	6-External	192.168.90.242	26937	199.30.234.34	443
07/28/2016 02:43:34 PM	WATCHTEST	Allow	1-Trusted	6-External	192.168.90.166	64678	192.204.82.136	80
07/28/2016 02:43:46 PM	WATCHTEST	Allow	2-LAN	1-FPL	192.168.100.27	51894	23.239.26.89	123

Figure 31

Relevant Log

Jul 11 09:23:33 192.168.90.9 Jul 11 09:23:33 NFMC-XTM-520 (2016-07-11T13:23:33) firewall: msg_id="3000-0148" Allow 1-Trusted 6-External main 52 tcp 20 127 192.168.90.242 199.30.234.34 26937 443 offset 8 S 352333572 win 32 (HTTPS-00)

Jun 19 11:19:35 192.168.90.9 Jun 19 11:20:41 Nrty-XTM-520 (2015-06-19T15:20:41) firewall: Allow 1-Trusted 6-External main 60 tcp 20 63 192.168.90.20 208.70.74.8 59109 443 offset 10 S 2730632788 win 61690 (HTTPS-00)
Jun 19 11:19:33 192.168.90.9 Jun 19 11:20:39 NFMC-XTM-520 (2015-06-19T15:20:39) dns-proxy[2128]: Allow 1-Trusted 6-External main udp 192.168.90.4 205.171.3.26 51235 53 msg="DNS Request" proxy_act="DNS-Outgoing.4" query_type="PTR" question="25.66.17.96.in-addr.arpa" (DNS-proxy-00)
Jun 19 11:19:22 192.168.90.9 Jun 19 11:20:28 CADM-XTM-520 (2015-06-19T15:20:28) Allow Firebox 0-External 52 tcp 20 127 10.0.1.2 125.156.60.25 62443 80 offset 8 S 832026162 win 8192 (HTTP-00)

Table 5