

## 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.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2019 Netsurion. 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	. 4
Prerequisites	. 4
Configure syslog forwarding to EventTracker	. 4
EventTracker Knowledge Pack (KP) Categories	. 6 . 7
Alerts	. 7
Reports	. 8
Import Knowledge Pack into EventTracker Import Category	. 9 10
Import Alerts	12
Import Parsing Rules	13
Import Template	14
Import Flex Reports	15
Import Knowledge Object	16
Verify Knowledge Pack in EventTracker Verify Categories	18 18
Verify Alerts	19
Verify Flex Reports	20
Verify Parsing Rule	21
Verify Templates	22
Verify Knowledge Object	23
Sample Reports & Logs WatchGuard XTM–User authentication failed	24 24
Sample Report	24
Relevant Log	24
WatchGuard XTM-Attack detected	24
Sample Report	24

# Netsurion. EventTracker

Relevant Log	25
NatchGuard XTM–Device configuration change details	25
Sample Report	25
Relevant Log	25
NatchGuard XTM-User logon and logout success	26
Sample Report	26
Relevant Log	26
NatchGuard XTM–Traffic details	26
Sample Report	26
Relevant Log	26

# Netsurion... EventTracker

## 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.



#### Integrate WatchGuard XTM

IREWALL	Washington Line Province		(BARLANS)
BSCRIPTION SERVICES	watchobard Log Server	Systog Server	settings
THENTICATION	Send log messages to the s	yslog server at this IP	address
N	IP Address	10.201.30.5	
STEM			
nformation	Port	514	
eature Key		-	
ITP	Log Format	Syslog	
INMP			
Managed Device	Select the details to include in s	syslog messages:	
Vetwork Scan	The serial number of the de	evice	
ogging	The syslog header		
Diagnostic Log	Suclea Cottings		
Slobal Settings	Systog Settings		
Certificates	Alarm	Local0	
Proxy Auto-Configuration		F	
Jpgrade OS	Traffic	Local1	
Backup Image	-		
Restore Image	Event	Local2	
JSB Drive	Disaportio	Line	
Jsers and Roles	Diagnostic	Local3	
Configuration File	Performance	Locald	_
ogon Disclaimer	r enviniance	LOC314	
e Serre and and the			

#### 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.



Integrate WatchGuard XTM

FIREWALL	Diagnostic Log Level		
SUBSCRIPTION SERVICES	Authentication	-	1
AUTHENTICATION	Addition	Error	•
VPN	FireCluster	Error	*
SYSTEM	Cluster Management	Error	
Information	Custer Operation	Error	•
Feature Key	Custer Event Monitoring	Error	
NTP	Custer Transport	Error	
SNMP		End	
Managed Device	Firewall	Error	
Network Scan	FQDN	Error	
Logging	Management	Error	
Diagnostic Log	Maturalities	Line	
Global Settings	Networking	Error	¥
Certificates	DHCP Client	Error	*
Proxy Auto-Configuration	DHCP Server	Error	
Upgrade OS	PPP	Error	
Backup Image	DEDat	- Line	
Restore Image	PPPOE	Error	*
USB Drive	Dynamic Routing	Error	•
Users and Roles	IPv6 Router Advertisement	Error	-
Configuration File	Gateway Wireless Controller		
Logon Disclaimer		Error	
About	Proxy	Error	

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 (<u>support@eventtracker.com</u>).

#### 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**.



**Netsurion** EventTracker



3. Click the **Import** tab.

Figure 3

- 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

10

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

1. Provide the path and file na	ame of the Categories file. Use the '' button to browse and locate the import file.
Click the Import button.     Options     Category     Filters	Location
<ul> <li>Alerts</li> <li>Systems and Groups</li> </ul>	Source :
<ul> <li>RSS Feeds</li> <li>Reports</li> </ul>	*.iscat
Behavior Rules	
<ul> <li>Token Value</li> </ul>	

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.

🖖 Export Import Utility		
Export Import		
<ol> <li>Provide the path and file name</li> <li>Click the Import button.</li> </ol>	e of the Alerts file. Use the '' button	to browse and locate the import file.
Options	Location	
Category		
◎ Filters	☑ Import E-mail settings	
Alerts	Set Active	
Systems and Groups	<ul> <li>Only if notifications set</li> <li>Bv default</li> </ul>	Inis setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section
RSS Feeds	0 1, 1111	SCUUT.
Reports	Source :	
Behavior Rules	JSGIL	
SCAP		
Token Value		
		Import Close

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.

🖖 Export Import Utility		
Export Import		
	me of token value file. Use the "" button to browse and locate the import file.	
<ul> <li>Systems and Groups</li> <li>RSS Feeds</li> </ul>	*.istoken	
Reports		
Behavior Rules		
SCAP		
Token Value		
	Import	Close



- 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.

PARSING R	ULE									
Parsing Rule Ter GROUPS Default	mplate	Group : All	0					~	A	1
A10 ADC	1		_~	CROUPNANT			ACTRE	G	I I	J L
Amazon Web Services	1		TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY		ACTIVE		EDII	î
Apache Web Server	1	A 10 ADC Authenticati.	A10 Application Delivery C	ATO ADC	ETAdmin	9/29/2015 8:19:51 PM	M		ø	
Barracuda Message Ar	1	A10 ADC Traffic	A10 Application Delivery C	A10 ADC	ElAdmin	9/29/2015 8:19:51 PM	V		0	
Barracuda Spam Firew	Ü Ø	AWS VPC-Flow Report		Amazon Web	ETAdmin	9/29/2015 8:19:51 PM	✓		0	
Centrify Server Suit	Ü 🧭	Barracuda Message		Barracuda Me	ETAdmin	9/29/2015 8:19:51 PM	$\checkmark$		Ø	
Check Point	Ü 🏉	Barracuda Spam fire		Barracuda Spa	. ETAdmin	12/15/2015 8:02:47 PM	$\checkmark$		0	
Cisco ASA	Ū 🏈	Barracuda Spam fire		Barracuda Spa	ETAdmin	12/15/2015 8:02:47 PM	$\checkmark$		0	
Cisco IOS	Ü 🏉	Barracuda Spam fire		Barracuda Spa	. ETAdmin	12/15/2015 8:02:47 PM	✓		0	
Cisco IronPort ESA	1	Barracuda Spam fire		Barracuda Spa	ETAdmin	12/15/2015 8:02:47 PM	~		0	~
CISCO Ironport WSA	Ü 🏉					DELETE	моч	E TO	GROUP	

3. Click on Browse button.

Figure 10

SELECT FILE Browse. No file selected.	
	No data found

Figure 11

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



CTED FILE IS: All WatchGuard XTM Templates.ettd					
TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
WatchGuard XTM-Attack detected	\t	Jun 19 11:19:11 192.168.90.9 Jun 19 11:20:17 CADM-XTM-520 (2015-06-19T15: 20:17) packet filter-firewall[2127]: msg_id="3000-0154" ICMP flood attack agai nst 10.0.1.51 from 216.3.21.4 detected.	7/29/2016 4:06:30 PM	ETAdmin	WatchGuard XTM
□ WatchGuard XTM-IP spoofing and blocked site traffic detected	\t	Jun 19 11:19:11 192.168.90.9 Jun 19 11:20:17 CADM-XTM-520 (2015-06-19T15: 20:17) packet filter-firewall[2127]: msg_id="3000-0168" Blocked site: Traffic de tected from 10.0.1.2 to 61.231.45.165.	7/29/2016 4:06:30 PM	ETAdmin	WatchGuard XTM
UWatchGuard XTM-IPS traffic detected	\n	Jul 06 14:22:14 192.168.90.9 Jul 6 14:22:14 NFMC-XTM-520 (2016-07-06T18:22: 14) firewali: msg.id="3000-0150" Deny 1-Trusted 0-External 1440 tcp 20 61 10. 0.1.2 192.168.130.126 55810 80 offset 5 A 447868619 win 54 signature_name ="EXPLOIT Apple QuickTime FLIC Animation file buffer overflow -1-2" signatur e_cate"Misc" signature_Id="1112464" severity="4" msg="IPS detected" (HTTP-0 0)	7/29/2016 4:05:51 PM	ETAdmin	WatchGuard XTM
WatchGuard XTM-Traffic details	\n	Jul 11 09:22:25 192.168.90.9 Jul 11 09:22:25 NFMC-XTM-520 (2016-07-11T13:2 2:25) firewall: msg_id="3000-0149" Allow 1-Trusted 6-External main 40 tcp 20 124 192.168.15.41 13.107.5.80 63241 80 offset 5 AF 2896757907 win 257 app_ mame="Microsoft Internet Explorer" cat name="Web" app beh name="acces	7/29/2016 4:05:51 PM	ETAdmin	WatchGuard XTM



5. Now select the check box and then click on <sup>↓</sup> **'Import**' option. EventTracker displays success message.

Template(s) imported successfully
ОК
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.



Provide the path and file na Click the Import button	ame of Schedule Report file. Use the "" button to browse and locate the import file.
ote : If report(s) contains ten Options Category	nplate, first import template and proceed with exportimport utility. Location
) Filters	
) Alerts	Legacy (*.issch)
Systems and Groups	Source :
RSS Feeds	
Reports	
Behavior Rules	
SCAP	
<b>Token Value</b>	

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 I 'Import' option.



KNOWLEDGE O	3JECTS	
Search objects QQ		OBJECTS 🕀 Ţ 🟦
GROUPS 🕀 🏈 🗓		
Hapache Web Server   ArrayOS SPX   Barracuda Message   Barracuda Spam Fir   Barracuda SSL VPN   Centrify AD client   Check Point   Cisco ACE   Cisco ASA   Cisco IOS   Clavister   Cyberoam UTM   Dell FORCE 10 Swit   Ezproxy	SELECT OBJECT FROM THE LEFT PANEL.	

Figure 16

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

IMPORT	
Select file <b>Browse</b> No file selected.	UPLOAD
Figure 17	

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



IMPORT							
Select file Br	owse No file selected.		UPLOAD				
	OBJECT NAME	APF	PLIES TO				
	WatchGuard	XTM	1				
			MERGE	OVERWRITE			
		10					

Figure 18

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

EventTracker displays success message.

File imported successfully.				
ОК				
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.





#### Verify Alerts

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

Alert Management page will display all the imported alerts.



ALERT MANAGEMENT Search by Alert name 🔍 Watchguard QQ										
ACTIVATE NOW Click 'Activa	<b>te Now'</b> after mak	ing all cha	inges						Total: 10	Page Size 25 💌
ALERT NAME ^	THREAT	<u>ACTIVE</u>	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
WatchGuard XTM: Attack detected	Serious									WatchGuard Fire
WatchGuard XTM: Authentication ser	🔄 High									WatchGuard Fire
WatchGuard XTM: Customized certifi	High									WatchGuard Fire
WatchGuard XTM: Device configurati	🔄 High									WatchGuard Fire
WatchGuard XTM: Feature expiration	High									WatchGuard Fire
WatchGuard XTM: Feature key downl	- High									WatchGuard Fire
WatchGuard XTM: Feature key expired	High									WatchGuard Fire
WatchGuard XTM: Shutdown request	Serious									WatchGuard Fire
WatchGuard XTM: User authenticatio	High									WatchGuard Fire
WatchGuard XTM: User logon failed	High									WatchGuard Fire

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.



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.

REPORTS CO	NFIGUR	ATION			
O Scheduled O Queued	Optimized		s	earch (	2010
REPORT GROUPS	$\oplus$	REPORTS CONFIGURATION : WATCHGUARD XTM			
Syslog	Ū Ø 🔨	⊕ Ĩ <i>∂</i> ,			Total: 10
🔁 Teradata Database	1		CREATED ON	MODIFIED ON	^
Terminal Services	1	U WatchGuard XTM-System management details	7/29/2016 2:29:12 PM	7/29/2016 4:01:12 PM	() 🚑 🛨
Trend Micro Deep Sec	1	U 🗱 WatchGuard XTM-Device configuration change deta	<u>ails</u> 7/29/2016 2:22:41 PM	7/29/2016 4:01:30 PM	() <i>[</i> ] ∃
Trend Micro InterSca	1	¥			
Trend Micro OfficeSc	Ē 🏈	U WatchGuard XTM-IPS traffic detected	7/28/2016 3:40:06 PM	7/28/2016 3:40:06 PM	() 💭 🛨
VMware	1	U KatchGuard XTM-Traffic details	7/28/2016 3:01:44 PM	8/4/2016 12:01:31 PM	🛈 💭 🗉
WatchGuard XTM	1	U XXX WatchGuard XTM-IP spoofing and blocked site traff	i 7/23/2016 5:13:35 PM	7/29/2016 4:28:56 PM	() 🖉 🕂
🕞 Websense WSG	1	U XXX WatchGuard XTM-User logon failed	7/18/2016 2:47:19 PM	7/29/2016 4:35:08 PM	() 🗦 Ŧ

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.



PARSING R	ULE					
Parsing Rule Ter	mplate					
Snort IDS	1 Ø <	Token-Value Display name	•	QQ	roup : WatchGuard XTM	(?)
Sonicwall UTM Sophos Enterprise Co			TOKEN NAME	TAG	SEPARATOR	TERMINATOR
Sophos UTM	Ē Ø	+ 🗌 Message Details	msg_id=		\s	\n
Suricata IDS	Ĩ Ø					
Symantec Endpoint Pr	1					
Syslog	1					
Terminal Services	1					
Trend Micro	1		ADD RULE EDIT	DELETE MOV	E TO GROUP TOKEN	VALUE WIZARD
Trend Micro Deep Sec	Ü 🧭					
Trend Micro InterSca	1					
VMware	1					
WatchGuard XTM	1					
Websense WSG	1				Act	ivate Wind



## Verify Templates

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



#### PARSING RULE

Parsing Rule Ter	mplate									
Sophos UTM	1	^	Group : WatchGuard X	TM						
Suricata IDS	1 🧭		Search	Q					CIT	
Symantec Endpoint Pr	Ü 🧭		TEMPI ATE NAME	TEMPI ATE DESCRIPTION			ACTIVE		EDIT	
Syslog	İ 🧭			ILMPLATE DESCRIPTION	ADDLD DI	ADDED DATE	ACTIVE		LDII	Î
Terminal Services	iii 🧭		WatchGuard XTM-Att	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:06:30 PM	$\checkmark$		1	
Trend Micro	Ē Ø		WatchGuard XTM-IP	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:06:30 PM	$\checkmark$		1	
Trend Mirro Door Coo			WatchGuard XTM-IPS	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:05:51 PM	$\checkmark$		1	
Trend Micro Deep Sec	······································		WatchGuard XTM-Tr	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:05:51 PM	~		1	
Trend Micro InterSca		11	WatchGuard YTM LIs	WatchGuard Eireware 11.1	FTAdmin	7/20/2016 4-05-11 PM				
VMware	Ü 🧭		watchouard x1w-os	watchouard Pileware 11.1	LIAUIIII	772572010 4.03.11 PW	V		<b></b>	
WatchGuard XTM	İ 🏈		WatchGuard XTM-Us	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:05:11 PM	$\checkmark$		1	
Websense WSG	Ē Ø		WatchGuard XTM-Us	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:05:11 PM	$\checkmark$		1	
Windows	1		WatchGuard XTM-Us	WatchGuard Fireware 11.1	ETAdmin	7/29/2016 4:05:11 PM	$\checkmark$		1	~
Windows DNS Server	1 0						DELE	TE	OVE TO GROUP	•)



## Verify Knowledge Object

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

KNOWLEDGE O	BJECIS				
Search objects QQ				0	BJECTS 🕀 Ҭ 👤
GROUPS 🕀 🏈 🗓	OBJECT NAME XTM Authentica APPLIES TO XTM 5 series or	tion later			1.0
⊕Pulse Secure MAG S	RULES				
	TITLE	LOG TYPE	EVENT SOURCE	EVENT ID EVENT TYPE	
	XTM Authentication		syslog*		Ø 🕑 🗉 🖏
€Snort	MESSAGE SIGNATURE	(Authentication)sof(s([))	w/s]#)/s/[( #)/]/sfrom/s/[/d -	+)/sis/s(/w+) //s[/w/s]+))/(Authen	tication\sof\s([\w\s]*)\s\
	MESSAGE SIGNATORE.	(Autoritication Son S() #	raj jan. janomalia.	.)636(w.c)(6[w6].))[(Addie	incention being (investigation
	MESSAGE EXCEPTION				
. ● Teradata	EXERCICIONS				
Trend Micro Deep S	EXPRESSIONS				
Trend Micro Office	EYDDESSION TYDE	FORMAT STRING	EXDRESSION 1	EVIDESSION 2	
€Vmware	LAFRESSION ITTE	FORMATSTRING	LAFRESSION	EAFRESSION 2	
€VOIP	Regular Expression		(?>Authentication\sof	\s(? <usr< td=""><td>🖸 🔟</td></usr<>	🖸 🔟
⊡WatchGuard					
XTM Authentication 🖉 🗓					
XTM Management 🛛 🖉 🗓					
XTM Threat 🖉 🗓					

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:0 370:7344
07/23/2016 04:19:42 PM	WATCHTEST	ICMP flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0 370:7344
07/23/2016 04:19:56 PM	WATCHTEST	UDP flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0 370:7344
07/23/2016 04:20:14 PM	WATCHTEST	IPSEC flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0 370:7344
07/23/2016 04:20:28 PM	WATCHTEST	IKE flood	FF01::101	2001:0db8:85a3:08d3:1319:8a2e:0 370:7344

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 filterfirewall [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) dnsproxy[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

