

**Integration Guide** 

# Integrating SonicWALL UTM

**Publication Date:** 

March 20, 2022



## Abstract

This guide provides instructions to configure SonicWALL UTM (Unified Threat Management) to send the syslog events to EventTracker.

## Audience

The SonicWALL UTM users, who wish to forward the syslog events to the EventTracker Manager.

## Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and later, and SonicOS 5.8 and later for SonicWALL NSA and TZ Series.

## Table of Contents

Та	ble (	of Contents	3
1.	0	verview	5
2.	Ρ	rerequisites	5
3.	Ir	tegrating SonicWALL UTM with EventTracker	5
	3.1	Configuring the Syslog Settings	5
	3.2	Configuring the Syslog Server	8
4.	S	vslog Send Receive Verification	9
	4.1	Verifying the Ping from SonicWALL UTM to EventTracker	9
	4.2	Verifying the Syslog messages forwarding on SonicWALL UTM	10
	4.3	Verifying the Syslog messages in EventTracker	12
5.	E١	ventTracker Knowledge Pack (KP)	13
	5.1	Categories	13
	5.2	Alerts	18
	5.3	Reports	19
6.	In	nporting SonicWALL UTM Knowledge pack into EventTracker	22
	6.1	Templates	22
	6.2	Importing Categories	24
	6.3	Importing Alerts	25
	6.4	Importing Tokens	26
	6.5	Importing Flex Reports	27
7.	V	erifying the SonicWALL UTM Knowledge Pack in EventTracker	29
	7.1	Template	29
	7.2	Verifying the SonicWALL UTM Categories	29
	7.3	Verifying the SonicWALL UTM Alerts	30
	7.4	Verifying the SonicWALL UTM Tokens	31
	7.5	Verifying the SonicWALL UTM Flex Reports	32
8.	С	reating Dashboards in EventTracker	32
	8.1	Scheduling Reports	32
	8.2	Creating Dashlets	34
9.	Sa	ample Reports	38
10	).	Sample Dashboards	39

# **Netsurion**<sub>®</sub>

About Netsurion	40
Contact Us	40

## 1. Overview

SonicWALL's approach to the Unified Threat Management (UTM) is the best security approach for Small- to Medium-sized Businesses (SMBs) bringing a new level of efficiency to the security field. EventTracker gathers and examines acquired logs to identify malicious traffic, fatal threats, configuration changes, VPN activity, and user behavior.

## 2. Prerequisites

- EventTracker Agent 9.x and later should be installed.
- SonicOS 5.8 and later should be installed.
- Port 514 must be allowed on SonicWALL UTM.
- An exception should be added to the Windows Firewall on the EventTracker Manager system for Syslog port 514.

## 3. Integrating SonicWALL UTM with EventTracker

To forward the logs from SonicWALL UTM to EventTracker follow the below steps:

### 3.1 Configuring the Syslog Settings

- 1. Login to **SonicWALL UTM** using the Web browser.
- 2. Click the Log option at the bottom left of the SonicWALL UTM screen.



Figure 1

3. Select the **Syslog** option.

SonicWALL Netwo	ork Security Appliance			
<ul> <li>▶</li></ul>	Syslog Accept Cancel Syslog Settings			
<ul> <li>SSL VPN</li> <li>Virtual Assist</li> <li>Users</li> <li>High Availability</li> <li>Security Services</li> <li>WAN Acceleration</li> <li>AppFlow</li> <li>Log</li> </ul>	Syslog Facility: Syslog Facility: Syslog Event Redundancy Filter (seconds): Syslog Format: Syslog ID: Enable Event Rate Limiting	Local Use 0 are Settings 0 Default • firewall	•	
View Categories Syslog Automation Name Resolution Benorts	Maximum Events Per Second: Tenable Data Rate Limiting Maximum Bytes Per Second: Syslog Servers	1000		
Analyzer	Server Name No Entries Add		Server Port	Configure



- 4. Under the **Syslog Setting** configure the following.
  - **Syslog Facility** Select the Syslog Facility you want or keep it as default.
  - **Override Syslog Settings with Reporting Software Settings** Uncheck this box to override the Syslog settings.

	Syslog			
VoIP Anti-Spam	Accept     Cancel      Suchas Sattings			
SSL VPN	Syslog Facility:	Local Use 0	•	
Users	Override Syslog Settings with Reporting Software	ire Settings		
🗄 High Availability	Syslog Event Redundancy Filter (seconds):	0		
Security Services	Syslog Format:	Default 👻		
AppFlow	Syslog ID:	firewall		
Log	Enable Event Rate Limiting	# CESEDONIE		
View	Maximum Events Per Second:	1000		
Categories	Enable Data Rate Limiting			
Syslog	Maximum Bytes Per Second:	1000000		
Automation		1		
Reports	Syslog Servers			
Analyzer	Server Name		Server Port	Configure
	No Entries			



5. From the **Syslog Format** menu list, select the **Enhanced Syslog format**.

### 6. Click the Configure icon stress of the Enhanced Syslog Settings configuration window appears.

General			
Host (sn)	Event ID (m)	Category (cat)	Group Category (gcat)
Message (msg)			
Interface			
✓ Src Interface	🗹 Src Mac Addr (srcMac)	Dst Interface	🗹 Dst Mac Addr (dstMac)
Protocol			
Src IP (src)	Src NAT IP (natSrc)	Src Port	Src NAT Port
🔽 Dst IP (dst)	🗷 Dst NAT IP (natDst)	Dst Port	Dst NAT Port
Protocol (proto)	ICMP type (type)	ICMP code (icmpCode)	
Connection			
Bytes Rcvd (rcvd)	Bytes Sent (sent)	Pkts Rcvd (rpkt)	Pkts Sent (spkt)
User (usr)	Conn Duration (cdur)	Session Type (sess)	Session Time (dur)
Src VPN Policy (vpnpolicy)	Dst VPN Policy (vpnpolicyDst)	Src Zone (srcZone)	🗹 Dst Zone (dstZone)
Client Policy (rule)	Interface stats	SonicPoint Stats	
Application			
HTTP OP (op)	HTTP result (result)	URL (dstname)	Block Reason (code)
Application (app)	GMS Heartbeat	GMS change URL (Change)	
Others			
Counter (n)	NPCS (npcs)	Note (note)	IDP IDP
Anti Spam	App Firewall		
		Select All Clear All	Save Cancel

#### Enhanced Syslog Settings

#### Figure 4

- 7. Select the **Enhanced Syslog** options you want to log into. To select all options, click **Select All**. To deselect all the options, click **Clear All**.
- 8. Click the Save button.
- 9. In the **Syslog ID** box, enter the Syslog ID that you want.

A **Syslog ID** field is included in all the generated Syslog messages, prefixed by "id=". Thus, for the default value, firewall, all Syslog messages include "id=firewall." The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

10. **(Optional)** Select **Enable Event Rate Limiting** if required. This control allows you to enable the rate limiting of the events to prevent the internal or external logging mechanism from being overwhelmed by the log events. Specify the maximum number of events in the Maximum Events per Second field; the minimum number is 0, the maximum is 1000, and the default is 1000 per second.

**NOTE:** Event rate and data rate limiting are applied regardless of the Log Priority of individual events.

11. **(Optional)** Select the Enable Data Rate Limiting if required. This control allows you to enable the rate limiting of the data to prevent the internal or external logging mechanism from being overwhelmed



by the log events. Specify the maximum number of bytes in the **Maximum Bytes per Second** field; the minimum is 0, the maximum is 1000000000, and the default is 100000000 bytes per second.

12. (Optional) Select Enable NDPP Enforcement for the Syslog Server if required.

### **3.2** Configuring the Syslog Server

1. Under the Syslog Servers heading, click the Add button.

SonicWALL   Netw	ork Security Appliance				Wizards   Help   Close
					Mode: Non-Config >
Firewall	Log / Syslog				
Firewall Settings					
DPI-SSL	Accept Cancel				4
🕨 🍻 VoIP					
Anti-Spam	Syslog Settings				
🕨 🐻 VPN		1			
SSL VPN	Sysiog Facility:	Local Use U	•		
🕨 🔒 Virtual Assist	Override Syslog Settings with Reporting Software	e Settings			
🕨 🤐 Users	Syslog Format:	Enhanced Syslog 👻			
🕨 📰 High Availability	Syslog ID:	firewall	]		
Security Services	Enable Event Rate Limiting				
WAN Acceleration	Maximum Events Der Second	1000			
AppFlow		1000			
🕶 🖾 Log	Enable Data Rate Limiting				
Log Monitor	Maximum Bytes Per Second:	1000000			
Settings	Enable NDPP Enforcement for Syslog Server				
Syslog	Curles Comme				
Automation	Sysiog Servers				
Name Resolution	Server Name	Server Port		Configure	
Reports	No Entries				
Analyzer	Add				Delete All



The Add Syslog Server window display.

SonicWALL   N	letwork Security Appliance
Name or IP Address:	
Port:	514
	OK Cancel
_	



2. Type the **EventTracker Agent** machine name or IP address in the **Name or IP Address** field. Type the port number in the **Port Number** field. The Syslog default port is 514.



10.10.1.29	
514	
OK	Cancel
	10.10.1.29 514 ОК

Figure 7

3. Click OK.

The Syslog server **EventTracker Agent** machine IP address would be added under the **Syslog Servers** section.

4. Click the **Accept** button to **Save** the settings.

PI-SSL	Log /	
IP	Syslog	
iti-Spam		
N	Accept     Cancel	
. VPN	System Settings	
tual Assist	Sysicy Sectings	
rs	Syslog Facility:	Local Use 0 🗸
h Availability	Override Syslog Settings with Reporting Software	are Settings
curity Services	Syslog Event Redundancy Filter (seconds):	0
	Syslog Format:	Default 👻
	Svelog ID:	firewall
iew		in orda
ategories	Enable Event Rate Limiting	4000
yslog	Maximum Events Per Second:	1000
utomation	Enable Data Rate Limiting	
Name Resolution	Maximum Bytes Per Second:	10000000

## 4. Syslog Send Receive Verification

## 4.1 Verifying the Ping from SonicWALL UTM to EventTracker

1. Login to SonicWALL UTM using the **Web** browser.



- 2. Click System->Diagnostics.
- 3. Select **Ping** from the **Diagnostic Tool** menu.

SonicWALL   Netwo	ork Security Appliance
Dashboard      System      Status      Licenses      Administration      SNMP      Certificates	System / Diagnostics @ Accept Cancel Refresh Tech Support Report
Time Schedules Settings Packet Monitor	Include: VPN Keys ARP Cache DHCP Bindings IKE Info SonicPointN Diagnostics Current users Include inactive users Detail of users Geo-IP/Botnet Cache
Diagnostics Restart Second Point Firewall Firewall Diagnostics Pirewall Diagnostics Pirewall Diagnostics Dia	Download Report       Send Diagnostic Reports         Image: Comparison of Diagnostic Reports to Support       Send Diagnostic Reports to Support         Time Interval (minutes)       1440         Include raw flow table data entries when sending diagnostic report
<ul> <li>▶ 9 VoIP</li> <li>▶ 20 Anti-Spam</li> <li>▶ 8 VPN</li> <li>▶ 9 VPN</li> <li>▶ 9 VPN</li> </ul>	Diagnostic Tools Diagnostic Tool: Ping  Multi-Core Monitor

Figure 9

- 4. Enter the IP address or hostname of the EventTracker Manager system and click Go.
- 5. In the **Interface** pulldown menu, select the interface you want to test the ping from. Selecting the option **ANY** allows the appliance to choose among all the interfaces—including those that are not listed in the pulldown menu.
- 6. If the test is successful, SonicWALL UTM returns a message saying that the IP address is alive, and the time taken to return in milliseconds (ms).

### 4.2 Verifying the Syslog messages forwarding on SonicWALL UTM

- 1. Login to the SonicWALL Network Security using the Web browser.
- 2. Navigate to the **System-> Packet Monitor** page in the GUI and click **Configure**.



System Status Licenses Administration SNMP Certificates Time Schedules Settings Modules Packet Monitor	Packet Monito Configure Packet Monito Packet Monito Trace of Trace of Remote Remote Remote FTP logg Current Buffer S Current Configure	Monitor All Monitor All Monito	Click "Configur Monitor Di KB, 0 Packets or ng to interface:N illiroring to: 0.0. Receiving from: ( er Pass/Failure or ed, 0 Forwarded General	e" option efault Clear aptured, Buffer is 0° IONE, 0 packets mirro J.0.0.0, 0 packets mirro J.0.0.0, 0 mirror pac punt: 0 / 0, FTP Three , 0 Consumed, 0 Gen Logging i Mir	Refresh % full, 0 MB of Buffer lost ored, 0 pkts skipped, 0 pkt ed, 0 pkts skipped, 0 pkts kets rcvd, 0 mirror packets r ad is Idle, Buffer status OK erated roring	s exceeded rate exceeded rate cvd but skipped	
Diagnostics	Start Capture	Stop Capture	Start Mirro	r Stop Mirror	Log to FTP server	Export as:	•
Restart           Restart           Network           Restart	Captured Pack	e <mark>ts `</mark>					
B 3G/AG/Modem	Sec. Second	Thoraca	Foress	Source IP	Destination TP	Ether Type	Packet

- 3. In the **Monitor Filter** tab, specify the following information.
- Ether Type(s): IP Address
- IP Type(s): UDP
- Destination Port(s): 514
- Enable the check box Enable Bidirectional Address and Port Matching.

Settings Mo	nitor Filter Display Filter	Logging	Advanced Monitor Filter	Mirror
Ionitor Filter (Used	for both mirroring and pa	icket capture	)	
Enable filter based or	n the firewall/app rule			
nterface Name(s):	5			
ther Type(s):	IP.			
P Type(s):	UDP		•	
ource IP Address(es):			•	
ource Port(s):			•	
estination IP Address(es	;):		•	
estination Port(s):	514		•	
Cashla Ridicactional A	ddross and Dect Matching			
Enable Bidirectional A	doress and Port Matching			

#### Figure 11

- 4. In the Advanced Monitor Filter tab, enable the check boxes.
- Monitor the Firewall Generated Packets. (This will bypass interface filter).
- Monitor the Intermediate Packets.



Settings	Monitor Filter	Display Filter	Logging	Advanced Monitor Filter	Mirror
lvanced Filt	er				
Z Monitor Firew	all Generated Packets	. (This will bypass inter	rface filter)		
🗾 Monitor Inter	mediate Packets. 🎙				
Monitor i	ntermediate multicast	traffic.			
Monitor i	ntermediate IP helper	traffic.			
Monitor i	ntermediate reassemb	led traffic.			
Monitor i	ntermediate fragment	ed traffic.			
Monitor i	ntermediate remote m	rrored traffic.			
Monitor i	ntermediate IPsec traf	fic.			
Monitor i	ntermediate SSL decry	pted traffic.			
Monitor i	ntermediate decrypted	LDAP over TLS packe	ts. •		
Manitari	ntermediate decrupter	Single Sign On agent	massager 1		



- 5. Click **OK** to save the packet capture setup.
- Click Start Capture in the Packet Monitor page to see the UDP 514 packets getting generated from SonicWALL destined for syslog server IP address as shown below.

Pa	cket Monitor									
	Configure Monitor All	Monitor Defaul	t C	ear Refresh						
Paci O O Curre Curre Sta Capl	wet Monitor         If Trace active,       Buffer size 500 KB         If Local mirroring off,       Mirroring to         If Remote mirroring Tx off,       Mirroring to         If PIploging off,       FTP Server Part         Int Buffer Statistics:       0 Dropped,         Int Configurations:       Filters         Int Capture       Stop Capture         wared Packets       *	, 10 Packets ci interface:NONE ing to: 0.0.0, ving from: 0.0.0 ss/Failure count Forwarded, 0 ( General 0 L Start Mirror Sonick	aptured, Bu ; 0 packets 0 packets r .0,0 0 mirror :0 / 0, FT :0 / 0, FT	ffer is 0% full, 0 MB of B mirrored, 0 pkts skipped, packets rcvd, 0 mirror p Thread is Idle, Buffer sta 0 Generated Mirroring Tor Log to FTP s interface IP ss	uffer lost 1, 0 pkts exceeded rate 0 pkts exceeded rate ackets rovd but skipped tus OK Export as: Sysl	▼ ` og Server's IP a	ddress		Items 1	to 10 (of 10)
#	Time	Ingress	Egress	vurce IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	10/16/2014 07:19:53.832	X0*(s)		192, 168, 168, 168	192.168.168.169	IP	UDP	514,514	GENERATED	275[275]
2	10/16/2014 07:19:53.832		X0*(s)	192.168.168.168	192.168.168.169	IP	UDP	514,514	GENERATED	275[275]
3	10/16/2014 07:19:53.832	X0*(s)		192, 168, 168, 168	192.168.168.169	IP	UDP	514,514	GENERATED	322[322]
4	10/16/2014 07:19:53.832		X0*(s)	192.168.168.168	192.168.168.169	IP	UDP	514,514	GENERATED	322[322]
5	10/16/2014 07:19:53.848	X0*(s)	10.77	192.168.168.168	192.168.168.169	IP	UDP	514,514	GENERATED	302[302]
6	10/16/2014 07:19:53.848		X0*(s)	192.168.168.168	192.168.168.169	IP	UDP	514,514	GENERATED	302[302]
-	tale barran ta pa ana	VAP/ 1		100 100 100 100		-	100			antant
					Figure	13				

## 4.3 Verifying the Syslog messages in EventTracker

- 1. Login to the EventTracker Web Application.
- 2. Perform the Log Search for SonicWALL UTM device.

 Log Search would display the syslog messages which EventTracker is receiving from SonicWALL UTM.

## 5. EventTracker Knowledge Pack (KP)

After the logs are received in EventTracker; categories, alerts, reports, and dashboards can be configured to provide valuable insight.

The following Knowledge Packs are available in EventTracker v7 and later to support the SonicWALL UTM monitoring.

### **5.1 Categories**

- **SonicWALL UTM: Application block** This category gives information related to the applications blocked on SonicWALL UTM.
- **SonicWALL UTM: Application control detection** This category gives information related to the application control, detected on SonicWALL UTM.
- **SonicWALL UTM: Application control prevention** This category gives information related to the application control, prevented on SonicWALL UTM.
- **SonicWALL UTM: Application detection -** This category gives information related to the applications, detected on SonicWALL UTM.
- SonicWALL UTM: Administrator logged out This category gives information related to the administrator logged out on SonicWALL UTM.
- **SonicWALL UTM: Administrator login failed** This category gives information related to the administrator login fail on SonicWALL UTM.
- **SonicWALL UTM: User authentication failed -** This category gives information related to the user authentication fail on SonicWALL UTM.
- **SonicWALL UTM: User authentication success** This category gives information related to the user whose authentication is a success on SonicWALL UTM.
- SonicWALL UTM: User logged out This category gives information related to the user who tries to log out on SonicWALL UTM.
- SonicWALL UTM: User login failed This category gives information related to the user whose login fails on SonicWALL UTM.
- **SonicWALL UTM: Website access allowed -** This category gives information related to the website access which is allowed on SonicWALL UTM.
- **SonicWALL UTM: Website access denied** This category gives information related to the website access which is denied on SonicWALL UTM.
- **SonicWALL UTM: DHCP lease dropped -** This category gives information related to the DHCP lease dropped on SonicWALL UTM.
- **SonicWALL UTM: DHCP lease expired -** This category gives information related to the DHCP lease expired on SonicWALL UTM.

- SonicWALL UTM: DHCP lease received This category gives information related to the DHCP lease received on SonicWALL UTM.
- **SonicWALL UTM: DHCP request received -** This category gives information related to the DHCP request received on SonicWALL UTM.
- **SonicWALL UTM: DHCP Server IP address conflict detected** This category gives information related to the DHCP server IP address conflict which was detected on SonicWALL UTM.
- SonicWALL UTM: DHCP Server received DHCP decline from client This category gives information related to the DHCP server received on the DHCP client, declined on SonicWALL UTM.
- **SonicWALL UTM: Connection closed** This category gives information related to the connection closed on SonicWALL UTM.
- **SonicWALL UTM: Connection dropped** This category gives information related to the connection dropped on SonicWALL UTM.
- **SonicWALL UTM: Connection established** This category gives information related to the connection established on SonicWALL UTM.
- **SonicWALL UTM: Connection opened -** This category gives information related to the connection open on SonicWALL UTM.
- **SonicWALL UTM: Connection timed out** This category gives information related to the connection time out on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule added** This category gives information related to the rules added to the firewall access on SonicWALL UTM.
- SonicWALL UTM: Firewall access rule deleted This category gives information related to the rules deleted to firewall access on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule modified** This category gives information related to the rules modified to firewall access on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule restored to default** This category gives information related to rules restored by default on firewall access on SonicWALL UTM.
- **SonicWALL UTM: FTP connection dropped** This category gives information related to the FTP connection dropped on SonicWALL UTM.
- SonicWALL UTM: FTP logon failure This category gives information related to the FTP logon failure on SonicWALL UTM.
- **SonicWALL UTM: FTP successful logons -** This category gives information related to the FTP, which is successfully logged on, on the SonicWALL UTM.
- **SonicWALL UTM: Packet dropped** This category gives information related to the packet dropped on SonicWALL UTM.
- **SonicWALL UTM: Back orifice attack dropped -** This category gives information related to the back orifice attack dropped on SonicWALL UTM.
- SonicWALL UTM: DNS rebind attack detected This category gives information related to the attack detected on the DNS rebind on SonicWALL UTM.
- SonicWALL UTM: DOS protection on WAN This category gives information related to the WAN protected by DOS on SonicWALL UTM.

- **SonicWALL UTM: FIN-Flooding machine blacklisted -** This category gives information related to the FIN-flooding machine blacklisted on SonicWALL UTM.
- **SonicWALL UTM: Forbidden email attachment disabled** This category gives information related to the forbidden email attachment disabled on SonicWALL UTM.
- **SonicWALL UTM: FTP port bounce attack dropped** This category gives information related to the FTP port bounce attack dropped on SonicWALL UTM.
- **SonicWALL UTM: ICMP flood attack detected** This category gives information related to the ICMP flood attack detected on SonicWALL UTM.
- **SonicWALL UTM: Ini killer attack dropped -** This category gives information related to ini killer attack dropped on SonicWALL UTM.
- **SonicWALL UTM: Initiator from country blocked** This category gives information related to the initiator from the country blocked on SonicWALL UTM.
- **SonicWALL UTM: Intrusion detection -** This category gives information related to the intrusion detection on SonicWALL UTM.
- SonicWALL UTM: IPS alert This category gives information related to the IPS alert on SonicWALL UTM.
- **SonicWALL UTM: Land attack dropped -** This category gives information related to the land attack dropped on SonicWALL UTM.
- SonicWALL UTM: MAC IP anti spoof check enforced for hosts This category gives information related to the MAC IP anti spoof check enforced for hosts on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from FINflood blacklist** This category gives information related to the FINflood blacklist, removed by the machine on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from RSTflood blacklist** This category gives information related to the RSTflood blacklist, removed by the machine on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from SYNflood blacklist** This category gives information related to the SYNflood blacklist, removed by the machine on SonicWALL UTM.
- SonicWALL UTM: Malformed DNS packet detected This category gives information related to the malformer DNS packet detected on SonicWALL UTM.
- **SonicWALL UTM: Malformed or unhandled IP packet dropped** This category gives information related to the malformed or the unhandled IP packet dropped on SonicWALL UTM.
- **SonicWALL UTM: NetBus attack dropped -** This category gives information related to the netbus attack dropped on SonicWALL UTM.
- SonicWALL UTM: Ping of death dropped This category gives information related to the ping of death dropped on SonicWALL UTM.
- SonicWALL UTM: Port scan detected This category gives information related the port scan detected on SonicWALL UTM.
- **SonicWALL UTM: Responder from country blocked** This category gives information related to the responder from the country blocked on SonicWALL UTM.
- **SonicWALL UTM: Suspected botnet initiator blocked** This category gives information related to the suspected botnet initiator blocked on SonicWALL UTM.
- SonicWALL UTM: SYN flood detected on WAN This category gives information related to the SYN flood detected on the WAN on SonicWALL UTM.

- SonicWALL UTM: TCP SYN packet dropped This category gives information related to the TCP SYN packet dropped on SonicWALL UTM.
- **SonicWALL UTM: UDP Flood attack detected** This category gives information related to the UDP flood attack detected on SonicWALL UTM.
- **SonicWALL UTM: WLAN IDS** This category gives information related to the WLAN IDS on SonicWALL UTM.
- **SonicWALL UTM: Backup firewall transitioned to active** This category gives information related to the backup firewall transitioned to active on SonicWALL UTM.
- **SonicWALL UTM: Backup firewall transitioned to idle -** This category gives information related to the backup firewall transitioned to idle on SonicWALL UTM.
- **SonicWALL UTM: Interface link down** This category gives information related to the interface link down on SonicWALL UTM.
- SonicWALL UTM: Interface link up This category gives information related to the interface link up on SonicWALL UTM.
- **SonicWALL UTM: Multicast policy list added** This category gives information related to the multicast policy added to the list on SonicWALL UTM.
- **SonicWALL UTM: Multicast policy list deleted** This category gives information related to the multicast policy deleted from the list on SonicWALL UTM.
- **SonicWALL UTM: Network monitoring -** This category gives information related to the network monitoring on SonicWALL UTM.
- **SonicWALL UTM: Network security appliance activated** This category gives information related to the network security appliance activated on SonicWALL UTM.
- SonicWALL UTM: PC card device not detected This category gives information related to the PC card device not detected on SonicWALL UTM.
- SonicWALL UTM: PC card inserted This category gives information related to the PC card inserted on SonicWALL UTM.
- SonicWALL UTM: PC card removed This category gives information related to the PC card removed on SonicWALL UTM.
- **SonicWALL UTM: Primary firewall transitioned to active** This category gives information related to the Primary firewall transitioned to active on SonicWALL UTM.
- **SonicWALL UTM: Primary firewall transitioned to idle -** This category gives information related to the primary firewall transitioned to idle on SonicWALL UTM.
- SonicWALL UTM: System fan failure This category gives information related to the system fan failure on SonicWALL UTM.
- **SonicWALL UTM: System shutdown by administrator** This category gives information related to the shutting down of the system by the administrator on SonicWALL UTM.
- SonicWALL UTM: WAN failover This category gives information related to the WAN failover on SonicWALL UTM.
- SonicWALL UTM: WAN failure This category gives information related to the WAN failure on SonicWALL UTM.

- SonicWALL UTM: Antispam service disabled This category gives information related to the antispam service disabled on SonicWALL UTM.
- **SonicWALL UTM: Antispam service enabled** This category gives information related to the antispam service enabled on SonicWALL UTM.
- **SonicWALL UTM: DSL device down** This category gives information related to the DSL device down on SonicWALL UTM.
- SonicWALL UTM: DSL device up This category gives information related to the DSL device up on SonicWALL UTM.
- SonicWALL UTM: DSL WAN connected This category gives information related to the DSL WAN connected on SonicWALL UTM.
- **SonicWALL UTM: DSL WAN initialized -** This category gives information related to the DSL WAN initialized on SonicWALL UTM.
- **SonicWALL UTM: Dynamic DNS configuration error** This category gives information related to the dynamic DNS configuration error on SonicWALL UTM.
- SonicWALL UTM: SSO agent down This category gives information related to the SSO agent which is down on SonicWALL UTM.
- **SonicWALL UTM: Terminal Services agent down** This category gives information related to the terminal services agent which is down on SonicWALL UTM.
- SonicWALL UTM: Spam detected This category gives information related to the spam detected on SonicWALL UTM.
- SonicWALL UTM: Maximum events per second threshold exceeded This category gives information related the maximum events per second threshold exceeded on SonicWALL UTM.
- SonicWALL UTM: Maximum syslog data per second threshold exceeded This category gives information related to the maximum syslog data per second threshold exceeded on SonicWALL UTM.
- **SonicWALL UTM: No firewall rule associated with VPN policy -** This category gives information related to no firewall rule associated with the VPN policy on SonicWALL UTM.
- SonicWALL UTM: Real time blacklist error This category gives information related to the real time blacklist error on SonicWALL UTM
- **SonicWALL UTM: Unhandled multicast IPv6 packet dropped** This category gives information related to the packet dropped for unhandled multicast IPv6 on SonicWALL UTM.
- SonicWALL VPN: Client activity This category gives information related to the VPN client activities on SonicWALL UTM.
- SonicWALL VPN: IKE activity This category gives information related to the VPN IKE activities on SonicWALL UTM.
- SonicWALL VPN: IPsec activity This category gives information related to the VPN IPsec activities on SonicWALL UTM.
- SonicWALL VPN: IPsec tunnel status changed This category gives information related to the VPN IPsec tunneling status changed on SonicWALL UTM.
- SonicWALL VPN: PKI error This category gives information related to the PKI error on SonicWALL UTM.



### **5.2** Alerts

- **SonicWALL UTM: Administrator login failed** This alert is generated when the administrator login has failed.
- SonicWALL: Antispam service disabled This alert is generated when the antispam service disable.
- **SonicWALL: Antispam service expired -** This alert is generated when the antispam service expires.
- **SonicWALL: Application control detection** This alert is generated when the application control was detected.
- **SonicWALL: Application control prevention** This alert is generated when the application control was prevented.
- **SonicWALL: Application filter blocked** This alert is generated when the application filter has been blocked.
- SonicWALL: Authentication failed This alert is generated when the authentication was failed.
- SonicWALL: Back orifice attack dropped This alert is generated when the back orifice attack was dropped.
- **SonicWALL: Backup firewall transitioned to active** This alert is generated when the backup of firewall was transited to active mode.
- SonicWALL: Bad CRL format This alert is generated when the bad CRL was formatted.
- SonicWALL: Certificate import failed This alert is generated when the certificate import was failed.
- SonicWALL: Connectivity error This alert is generated when the connectivity generated an error.
- SonicWALL: CRL validation failure This alert is generated when the CRL validation is failed.
- SonicWALL: DHCP lease expired This alert is generated when the DHCP lease has been expired.
- **SonicWALL: DHCP Server IP conflict detected** This alert is generated when the DHCP server IP address conflict has been detected.
- **SonicWALL: DHCP Server sanity check failed** This alert is generated when the DHCP server sanity check has been failed.
- **SonicWALL: DNS rebind attack detected** This alert is generated when the DNS rebind attack has been detected.
- SonicWALL: DSL device down This alert is generated when the DSL device is down.
- SonicWALL: DSL WAN connected This alert is generated when the DSL WAN is connected.
- SonicWALL: DSL WAN initialized This alert is generated when the DSL WAN initialized.
- SonicWALL: Failed to get CRL This alert is generated when it fails to get the CRL.
- SonicWALL: Failed to process CRL This alert is generated when it fails to process the CRL.
- SonicWALL: Firewall access rule added This alert is generated when the Firewall access rule is added.
- SonicWALL: Firewall access rule deleted This alert is generated when the Firewall access rule is deleted.
- SonicWALL: Firewall access rule modified This alert is generated when the Firewall access rule is modified.
- **SonicWALL: FTP connection dropped -** This alert is generated when the FTP connection is dropped.
- SonicWALL: FTP logon failure This alert is generated when the FTP logon failure occurs.
- SonicWALL: Interface link down This alert is generated when the Interface link is down.
- SonicWALL: Intrusion detection This alert is generated when the Intrusion detection occurs.
- SonicWALL: IPS alert This alert is generated when the IPS alert occurs.
- SonicWALL: Issuer match failed This alert is generated when the issuer match fails.
- SonicWALL: L2TP error This alert is generated when the L2TP error occurs.

- SonicWALL: Multicast policy list deleted This alert is generated when the Multicast policy list deleted.
- SonicWALL: NetBus attack dropped This alert is generated when the NetBus attack is dropped.
- SonicWALL: NetSpy attack dropped This alert is generated when the NetSpy attack is dropped.
- SonicWALL: Outbound access blocked This alert is generated when the outbound access is blocked.
- SonicWALL: Ping of death dropped This alert is generated when the Ping of death is dropped.
- **SonicWALL: PPP Dial-Up dialing failed -** This alert is generated when the PPP Dial-Up dialing is failed.
- SonicWALL: SIM detection failure This alert is generated when the SIM detection failure occurs.
- SonicWALL: Spam detected This alert is generated when the Spam is detected.
- SonicWALL: SSO agent down This alert is generated when the SSO agent is down.
- SonicWALL: System fan failure This alert is generated when the System fan failure occurs.
- SonicWALL: User login failed This alert is generated when the User login fails.
- SonicWALL: Website access denied This alert is generated when the Website access is denied.
- SonicWALL Firewall: VPN User authentication failed This alert is generated when the user authentication is failed.

### 5.3 Reports

- SonicWALL Firewall-Network access report: This report provides information related to the network access which includes the Source IP Address, Source Port, Destination IP Address, Destination Port, WAN Address and Message Column.
- **SonicWALL UTM-WLAN IDS report:** This report provides information related to the WLAN IDS which includes the Source IP address and Message Column.
- **SonicWALLUTM-FTP logon details:** This report provides information related to the FTP logon details which include the Username, Source IP address and Message Column.
- **SonicWALL UTM-Website access allowed:** This report provides information related to website access allowed which includes the Username, Source IP address, URL Category and URL Name.
- **SonicWALL Firewall-access rule change:** This report provides information related to the firewall access rule change which includes the Username, Source IP address and Message Column.
- **SonicWALL UTM-User activity:** This report provides information related to the user activity which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Anti-Spyware detected:** This report provides information related to the antispyware detected which includes Event generated time and the Source IP address Column.
- **SonicWALL UTM-DSL activity:** This report provides information related to the DSL activity which includes the Username, Source IP address and Messages Column.
- **SonicWALLUTM-Attacks detection:** This report provides information related to the attack detection which includes the Source IP address and Messages Column.

- **SonicWALL UTM-Application control prevention:** This report provides information related to application control prevention which includes the Source IP address and Messages Column.
- **SonicWALL UTM-Application control detection:** This report provides information related to application control detection which includes which includes the Source IP address and Messages Column.
- **SonicWALL UTM-Admin login failed:** This report provides information related to the admin login failed which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Authentication failed:** This report provides information related to the authentication failed which includes Username, Source IP address and Messages Column.
- **SonicWALL UTM-Authentication success:** This report provides information related to the authentication success which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Interface link status**: This report provides information related to the interface link status which includes the interface name and its status (UP OR DOWN).
- **SonicWALLUTM-Connection closed dropped or terminated**: This report provides information related to the connection status which includes the source and the destination IP address, ports and connection status (closed, dropped and terminated) with protocol used during the connection.
- SonicWALL UTM-Connection opened or established: This report provides information related to the connection opened and established which includes the source and the destination IP address, ports and interface, application used for making connection and protocol details.
- SonicWALL UTM-Terminal services or SSO Agent: This report provides information related to the terminal and the SSO services status which includes the service name (terminal or SSO) and its status and by whom these services are enabled and disabled.
- SonicWALL UTM-Website access denied: This report provides information related to the websites whose access are denied which includes the source and the destination IP address, port and interface and the URL and its category.
- SonicWALL UTM-Intrusion detection: This report provides information related to the intrusion detected by the SonicWALL firewall which includes the source details, victim details and the attack name.
- SonicWALL UTM-Multicast policy list: This report provides information related to the addition or deletion of the multicast policy list in interface or VPN SPI, which includes the interface Name and the VPN SPI value in which the multicast policy is added or deleted.
- **SonicWALLUTM-Antispam service:** This report provides information related to the antispam service which includes the status of the service and by whom it is enabled or disabled.



- SonicWALL UTM-System Shutdown by Administrator: This report provides information related to the system shutdown by the administrator which includes the user details i.e., by whom the firewall is shutdown.
- SonicWALL UTM-Configuration change details: This report provides information related to the configuration change. It shows the Username, the Source IP address and the Destination IP address and also what have been changed.
- SonicWALL Firewall-VPN User authentication failed: This report provides information related to the User authentication failure which includes the Source address and Port, Destination address and Port, Additional Information and Reason for failure.
- SonicWALL Firewall-VPN User authentication success: This report provides information related to the User authentication success which includes the Source address and Port, the Destination address and Port, Additional Information and the Reason for success.
- SonicWALL Firewall-VPN activity: This report provides information related to the VPN activity that contains the VPN Client, VPN IPsec, VPN IKE, and the VPN PKI which includes the Source address and Port, Destination address and Port, Additional Information and message.
- SonicWALL Firewall-VPN IPsec tunnel status changed: This report provides information related to the IPsec tunnel status that is changed to up or down which includes the Source Range, Destination Range, Gateway, Reason, Status and the VPN Details.
- **SonicWALL Firewall- Traffic flow:** This report provides information related to the traffic flow. It gives information regarding where the traffic connected is opened or closed.
- **SonicWALL UTM-Administrator login status**: This report provides information related to the administrator login status.
- **SonicWALL UTM-Application management**: This report provides information related to the application activities that have occurred.
- **SonicWALL UTM-Connection status**: This report provides information related to the connection status.
- **SonicWALL UTM-DHCP lease status**: This report provides information related to the DHCP lease status.
- **SonicWALL Firewall-Access rule change**: This report provides information related to the firewall access rule changes.
- **SonicWALL Firewall-IDS attacks**: This report provides information related to the IDS attacks that occur in the system.
- SonicWALL UTM-FTP logon status: This report provides information related to the FTP logon status.

- SonicWALL-User admin login status: This report provides information related to the user admin login status.
- **SonicWALL UTM-User authentication status**: This report provides information related to the user authentication status.
- SonicWALL UTM-Website access status: This report provides information related to the website access status.

## 6. Importing SonicWALL UTM Knowledge pack into EventTracker

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





Import the following in the same order as mentioned below.

- Template
- Category
- Alert
- Tokens
- Flex Reports

### 6.1 Templates

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

2. Select the **Template** tab, and then click the Import option.

Parsing Rule Te	emplate	*						
Default		Group : All					Gi	Ŧ
10 ADC	1	E TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	EDIT
mazon Web Services	Ū Ø	A10 ADC Authentica	t A10 Application Delivery C	. Default	ETAdmin	9/25/2015 07:56:59 PM		1
.pacheWeb Server	11 🧭	A10 ADC Traffic	A10 Application Delivery C	. Default	ETAdmin	9/25/2015 07:56:59 PM	<b>V</b>	1
entrify Server Suit	Ū 🧭	Cisco IOS-Access De	n	Cisca IOS	ETAdmin	10/17/2015 03:32:42	<b>V</b>	1
heckPaint	1 🧭	Cisco IOS-Configurat	i	Cisca IOS	ETAdmin	10/17/2015 06:48:45		0
isca ACS	11 🧭	Cisco IOS-Port Statu	5	Cisco 105	ETAdmin	10/16/2015 06:27:54		
isca ASA	11 🧭							•
lisca IOS	Ē 🏉	HP PraCurve-Part Sta	a HP 2520G,HP 2520,HP 253	Default	ETAdmin	9/16/2015 04:16:51 PM		Ø
iisca IranPart ESA	İ 🧭	HP ProCurve-Security	y HP 2520G,HP 2520,HP 253	Default	ETAdmin	9/16/201505:33:25 PM		0
EISCO Iranpart WSA	Ū Ø							-
Cisca ISE	Ē 🏉					DELETE	IVE TO GRO	UP
Ilavister firewall	1 🧭							

#### PARSING RULE



3. Click the **Browse** button.

SELECT FILE Browse No file selected.	
	No data found

Figure 16

4. Locate the All SonicWALL UTM group of the Template.ettd file, and then click Open.

SELEC	TED FILE IS: All SonicWALL UTM group o	f Template.ettd	Ţ				
	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME	Â
	Sonicwall: Application management	\n	May 25 22:36:14 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-26 02:36:14 UTC" fw=75.147.154.153 pri=1 c=0 m=649 msg="Application Filters BI ock Alert: facebook.com" sid=5148 appcat=PROTOCOLS appid=1277 sess=Aut o n=2673709 usr="VLC ech2" src=10.0.105.86:62016:X0:VLC-TECH2 dst=72.3.2 09.232:80:X1:us11.systemmonitor.us	7/13/2016 3:28:24 PM	abhilanchana	Sonicwall UTM	
	Sonicwall: DHCP lease status	\n	May 27 18:30:12 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-27 18:30:12 UTC" fw=75.147.154.153 pri=6 c=32 m=222 msg="DHCP RELEASE rela yed to Central Gateway" sess=Web n=6 usr="john" src=10.0.105.202:0:X0:VLC- ADMIN dst=10.0.105.130:443:X0:	7/14/2016 5:00:09 PM	abhilanchana	Sonicwall UTM	
	Sonicwall: Firewall access rule change	\n	May 25 12:00:59 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-25 16:00:59 UTC" fw=75.147.154.153 pri=3 c=4 m=443 msg="Access rules restore d to defaults" sess=Auto n=16253 usr="ucknorth" src=10.0.105.40:53177:X0:VL C-TRUCK-N dst=184.51.207.65:80:X1: dstname=static-p-a.comcast.net arg=/api /assets/cimed-20120712/nbc.png code=4 Category="Pornography"	7/14/2016 6:12:19 PM	abhilanchana	Sonicwall UTM	
			May 21 12:26:08 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-21 16:26:08 UTC" fw=75.147.154.153 ori=1 c=32 m=79 mse="Priority attack droop				¥

#### Figure 17

5. Select the check box and then click the **Import** option. EventTracker displays a success message.

Template(s) imported successful	ly
ОК	



6. Click the **OK** button.

## 6.2 Importing Categories

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

Export       Import         1. Provide the path and file name of the Categories file. Use the '' button to browse and locate the import file.         2. Click the Import button.         Options       Location         © Category         Filters         Alerts         Systems and Groups       Source :         ".iscat         RSS Feeds         Behavior Rules         SCAP         Token Value	🖖 Export Import Utility		
1. Provide the path and file name of the Categories file. Use the '' button to browse and locate the import file.         2. Click the Import button.         Options       Location         • Category         • Filters         • Alerts         • Systems and Groups         Surce :         * iscat         • RSS Feeds         • Reports         • Behavior Rules         • SCAP         • Token Value	Export Import		
Category     Category     Filters     Alerts     Systems and Groups     Source :     *.iscat     RSS Feeds     Reports     Behavior Rules     SCAP     Token Value	1. Provide the path and file name 2. Click the Import button.	of the Categories file. Use the '' button to browse and locate the import file.	
<ul> <li>Filters</li> <li>Alerts</li> <li>Systems and Groups</li> <li>Source :         <ul> <li>*.iscat</li> <li>RSS Feeds</li> <li>Reports</li> <li>Behavior Rules</li> <li>SCAP</li> <li>Token Value</li> </ul> </li> </ul>	Category	Location	
<ul> <li>Alerts</li> <li>Systems and Groups</li> <li>Source :         <ul> <li>*.iscat</li> <li>RSS Feeds</li> <li>Reports</li> <li>Behavior Rules</li> <li>SCAP</li> <li>Token Value</li> </ul> </li> </ul>	<ul> <li>Filters</li> </ul>		
Systems and Groups Source :   RSS Feeds   Reports   Behavior Rules   SCAP   Token Value	Alerts		
<ul> <li>RSS Feeds</li> <li>Reports</li> <li>Behavior Rules</li> <li>SCAP</li> <li>Token Value</li> </ul>	Systems and Groups	Source :	
<ul> <li>Reports</li> <li>Behavior Rules</li> <li>SCAP</li> <li>Token Value</li> </ul>	RSS Feeds	*.iscat	
<ul> <li>Behavior Rules</li> <li>SCAP</li> <li>Token Value</li> </ul>	Reports		
<ul> <li>SCAP</li> <li>Token Value</li> </ul>	Behavior Rules		
💿 Token Value	SCAP		
	🔘 Token Value		
Import Close		Import	Close

Figure 19

- 2. Locate the All SonicWALL UTM group of the Categories.iscat file, and then click Open.
- To import the categories, click the Import button. EventTracker displays a success message.



Figure 20

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

## 6.3 Importing Alerts

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

🖖 Export Import Utility		
Export Import		
Export       Import         1. Provide the path and file na         2. Click the Import button.         Options         ① Category         ③ Filters         ④ Alerts         ③ Systems and Groups         ③ RSS Feeds         ④ Reports         ④ Behavior Rules         ⑤ SCAP	me of the Alerts file. Use the '' button Location  Import E-mail settings Set Active Only if notifications set By default Source : *.isalt	to browse and locate the import file. This setting is applicable only for imports from Legacy (ν6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.
Token Value		
		Import Close

Figure 21

- 2. Locate the All SonicWALL UTM group of the Alerts.isalt file, and then click Open.
- 3. To import the alerts, click the **Import** button. EventTracker displays a success message.



Figure 22

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

### 6.4 Importing Tokens

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

Export Import Utility		
xport Import		
<ol> <li>Provide the path and file na</li> <li>Click the Import button</li> </ol>	me of token value file. Use the '' button to browse and locate the import file.	
Options	Location	
Category		
─ Filters		
Alerts		
Systems and Groups	Source : 	
RSS Feeds		
Reports		
Behavior Rules		
SCAP		
Token Value		
	Import	Close

Figure 23

- 2. Locate the All SonicWALL UTM group of the Tokens.istoken file, and then click Open.
- 3. To import the tokens, click the **Import** button.
  - EventTracker displays a success message.



Figure 24

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

## 6.5 Importing Flex Reports

1. Click the **Report** option, and then click the Browse button.

🖖 Export Import Utility		- • ×
Export Import		
1. Provide the path and file nam         2. Click the Import button         Note : If report(s) contains temple         Options         O Category         Filters         Alerts         Systems and Groups         RSS Feeds         Reports         Behavior Rules         SCAP         Token Value	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility. Location Legacy (".issch) New (".etcrx) Source : *.issch	
	Import	Close

Figure 25

- 2. Locate the All SonicWALL UTM group of the Flex Report.issch file, and then click Open.
- 3. To import the scheduled reports, click the **Import** button. EventTracker displays a success message.



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

## 7. Verifying the SonicWALL UTM Knowledge Pack in EventTracker

### 7.1 Template

- 1. Logon to the **EventTracker** web interface.
- 2. Click the Admin menu, and then click Parsing Rules and click Template.

PARSING R	ULE						
Parsing Rule Tem Snort IDS Sonicwall UTM	nplate	Group : Sonicwall UTM					CIT
Sophos Antivirus	1	TEMPLATE NAME TEMPLATE D	DESCRIPTION ADDED BY	ADDED DATE	ACTIVE		EDIT
Sophos Enterprise Co	1	Sonicwall: Application Sonicwall: Ap	oplication man abhilancha	7/13/2016 3:28:24 PM			0
Suricata	1	Sonicwall: DHCP lease Sonicwall: Dł	HCP lease status abhilancha	7/14/2016 5:00:09 PM	$\checkmark$	$\checkmark$	0
Symantec Endpoint Pr	1	Sonicwall: Firewall acc Sonicwall: Fir	rewall access r abhilancha	7/14/2016 6:12:19 PM		$\checkmark$	8
Syslog		Sonicwall: Firewall IDS Sonicwall: Fir	rewall IDS attac abhilancha	7/15/2016 3:32:11 PM		$\checkmark$	8
Syslog login failure		Sonicwall: FTP logon s Sonicwall: FT	P logon status abhilancha	7/14/2016 6:34:33 PM			0
Trend Micro		Sonicwall: Traffic status Sonicwall: Tr	affic status abhilancha	7/15/2016 11:16:18 AM			Ø
Trend Micro InterSca		Sonicwall: User admin Sonicwall: Us	ser admin login abhilancha	7/14/2016 4:34:57 PM		$\checkmark$	1
VMware		Sonicwall: User login s Sonicwall: Us	ser login status abhilancha	7/13/2016 5:15:10 PM			ø 🗸
WatchGuard XTM Websense WSG	U Ø				DELETE	MOVE	TO GROUP



## 7.2 Verifying the SonicWALL UTM Categories

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Categories.
- 3. In the **Category Tree**, expand the **SonicWALL UTM** group folder to view the imported categories.

ashboard	Incidents	Behavior	Status	Search	Reports	My EventTracker	Change Audit	Config Asses	sment
CATEG	ORY MA	NAGE	MEN	Т					
Category Tre	ee Search								
Sol Con Con Con Con Con Con Con Con Con Con	aris BSM nicwall UTM Sonicwall Antispa	m	*	Total categ Last 10 mo	ory groups: 349 dified categorie	Total categories: 3,104			
ΨD	Sonicwall Applicat	tion		NAME	ł		MODIFIE	D DATE	MODIFIED BY
₽ <b>₽</b>	Sonicwall Attacks			Sonicwall: N	letBus attack dr	opped	8/17/2015	10:28:37 AM	shalendra
	Sonicwall Authent	tication		Sonicwall: V	Vebsite access a	llowed	8/17/2015	10:28:24 AM	shalendra
	Sonicwall Content	Filtering		Sonicwall: A	.RP request rest	oonse	8/17/2015	10:28:13 AM	shalendra
<b>40</b>	Sonicwall DHCP	Ū		Soniowall: F	lackup firewall t	transitioned to active	8/17/2015	10-27-59 AM	shalendra
	Sonicwall Firewall Sonicwall IDS			Sonicwall: C	onnection esta	blished	8/17/2015	i 10:27:47 AM	shalendra
	Sonicwall L2TP			Sonicwall: E	OOTP configur	ation error	8/17/2015	10:27:32 AM	shalendra
<b>₽</b> ₽	Sonicwall Network	< No.		Sonicwall: A	dministrator lo	gin failed	8/17/2015	10:27:16 AM	shalendra
	Sonicwall PPP Dia	lup	E	Sonicwall: E	ad CRL format		8/17/2015	10:27:00 AM	shalendra
-@	Sonicwall: 802.11	management	sen	Sonicwall: E	ack orifice atta	ck dropped	8/17/2015	10:26:30 AM	shalendra
-8	Sonicwall: All ever Sonicwall: Backup	nts firewall trans	itio	Sonicwall: A	ntispam service	e disabled	8/17/2015	10:26:16 AM	shalendra



## 7.3 Verifying the SonicWALL UTM Alerts

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.
- 3. In the **Search** field, type **SonicWALL**, and then click the **Go** button.

The Alert Management page will display all the imported SonicWALL UTM alerts.

Dashboard Incidents Behavior	Status	Search	Report	s MyE	ventTr	acker C	hange Audit	Config /	Assessment	
ALERT MANAGEME	NT								Sonicwall	્ર
ACTIVATE NOW     Click 'Activate Now' after making all changes     Page Size 25										
ALERT NAME ^	THREA		E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
Sonicwall: Administrator login failed	Serious									SonicOS 5.8 and I
Sonicwall: Antispam service disabled	Serious									SonicOS 5.8 and I
Sonicwall: Antispam service expired	Serious									SonicOS 5.8 and I
Sonicwall: Application control detect	Serious									SonicOS 5.8 and I
Sonicwall: Application control preve	Serious									SonicOS 5.8 and I
Sonicwall: Application filter blocked	Serious									SonicOS 5.8 and I
Sonicwall: Authentication failed	Serious									SonicOS 5.8 and I
Sonicwall: Back orifice attack dropped	Serious									SonicOS 5.8 and I
Sonicwall: Backup firewall transition	Serious									SonicOS 5.8 and I
				Figure	29					

© Copyright Netsurion. All Rights Reserved.



4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays a message box.



Click the OK button, and then click the Activate Now button.
 NOTE: You can select the 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.

## 7.4 Verifying the SonicWALL UTM Tokens

- 1. Logon to **EventTracker**.
- Click the Admin menu, and then click the Parsing rule.
   The imported SonicWALL UTM tokens are added to the Token-Value Groups list.

Dashboard Incide	ents Be	ehavior	Status	Search	Reports	My EventTracker	Change Au	dit Confi	ig Assessmer	ıt	
PARSING F	RULE										
Parsing Rule T	Template	*	Token-Vali	IP Diselar			QQ	Group :	Sonicwall UTM	1	?
Linux	Ē Ø					EN NAME	TAC	5 !	SEPARATOR	TERMINATOR	× E
LOGbinder SQL Microsoft Windows RR.	<sup>™</sup> <sup>™</sup> <sup>™</sup>		+ • A	pplication Nat	msg=	ame=			1	"	
MySQL Netscreen	Ü Ø		+ 🗖 De	estination	dst				-	\s	
OpenDNS RRAS	Ū Ø		+ 🗖 In	terface	Interf	ADD RULE EDIT	DELETE	MOVE TO GRO	Ns DUP TOKE	\s N-VALUE WIZA	<b>₽</b>
Sonicwall UTM	. () () () () () () () () () () () () () (										
Symantec Endpoint Pr.	🔟 🧭				Fig	gure 31					

## 7.5 Verifying the SonicWALL UTM Flex Reports

- 1. Logon to EventTracker.
- 2. Click the **Reports** menu, and then select **Configuration**.
- 3. In **Reports Configuration**, select the **Defined** option.
- 4. In the search box enter **SonicWALL**, and then click the **Search** button. EventTracker displays a Flex report of SonicWALLUTM.

ashboard Incidents Be	havior Status	Search Reports	My EventTracker	Change Audit	Config Assessment	
Scheduled © Queued © D		N			Sonicwall	
REPORT GROUPS	REPOR	TS CONFIGURATION				
	•					
Juniper Netscreen		Sonicwall-Terminal Service	e and SSO agent	8/14/2015 5:45:28 P	M 8/14/2015 5:45:28 PM	
		Sonicwall-Connection op	ened or established	8/14/2015 5:34:58 P	M 8/14/2015 6:21:10 PM	() / +
McAfee	as 🗆 🔅	Sonicwall-Connection clo	osed, dropped or terminate	d 8/14/2015 3:32:47 P	M 8/14/2015 6:22:06 PM	() 🖉 🗉
OKTA SSO     Persistent		Sonicwall-Interface Link	Up and Down	8/14/2015 3:18:46 P	M 8/14/2015 3:18:46 PM	() ∰ ⊕ =
SEPM		Sonicwall Firewall-Netwo	irk access report	4/24/2015 3:00:11 P	M 4/24/2015 3:00:11 PM	⊙ ⁄⊒ 🗉
Sonicwall UTM	nsole	Sonicwall-WLAN IDS repo	ort	7/8/2014 7:59:52 PN	1 7/8/2014 7:59:52 PM	() / +
		Fi	gure 32			

## 8. Creating Dashboards in EventTracker

### 8.1 Scheduling Reports

1. Open EventTracker in browser and logon.





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

#### **REPORTS CONFIGURATION** O Scheduled O Queued O Defined QQVI Search **+** REPORT GROUPS REPORTS CONFIGURATION : ALL Total: 450 🕀 🗓 ) Sonicwall UTM 1 0 ^ TITLE CREATED ON MODIFIED ON Sophos Enterprise Co... İ 🖉 ~ Sophos UTM 1 0 🗌 🛞 SonicWALL Firewall-VPN User authentication failed 12/10/2015 6:22:11 PM 12/10/2015 6:34:01 PM () 🖉 🛨 Syslog Ü Ø 🗌 🔅 SonicWALL Firewall-VPN IPSec tunnel status changed 12/10/2015 2:55:19 PM 12/10/2015 7:04:03 PM () 🖉 王 🔁 Teradata Database 1 0 SonicWALL Firewall-VPN activity 12/9/2015 3:26:42 PM 12/10/2015 6:05:37 PM () 🚝 🛨 Trend Micro Ê Ø VMware 🗆 🔅 SonicWALL Firewall-VPN User authentication success 12/9/2015 2:04:13 PM 🛛 12/10/2015 6:18:27 PM 🛈 👼 🖭 1 0 WatchGuard XTM 1 0 SonicWALL Firewall VPN-IKE Activity 12/8/2015 11:17:32 AM 12/8/2015 5:19:11 PM 🕕 🗐 🚝 🛨 Websense WSG 11 0

#### Figure 34

- 3. Select SonicWALL UTM in report groups. Check the **Defined** dialog box.
- 4. Click **Schedule** to plan a report for later execution.
- 5. Choose the appropriate time for the report execution and in **Step 8** check **Persist data in the Event vault explorer** box.

	ZARD			CANC	EL < BACK NEXT >
E: SONICWALL FIREWA	LL-VPN USER AUTHEN	TICATION SUCCESS			
GS					
iew cost details and cor	nfigure the publishing o	options.		Step 8 of 10	
DISK COST AN	ALYSIS				
Estimated time for con	npletion: 00:00:52(HH:N	MM:SS)			
Available disk space: 2	61 GB				
Required disk space: 5	0 MB				
Enable publishing	option (Configure SMTF	P Server in manager	configuration screen to use this option)		
Enable publishing     Opeliver results via I	option (Configure SMTF E-mail	P Server in manager	configuration screen to use this option)		
<ul> <li>Enable publishing</li> <li>Deliver results via l</li> <li>Notify results via E</li> </ul>	option (Configure SMTF E-mail -mail	P Server in manager	configuration screen to use this option)		
Enable publishing (     Deliver results via l     Notify results via E     To E-mail	option (Configure SMTF E-mail mail	P Server in manager	Configuration screen to use this option) [Use comma(,) to separate multiple e-mail recipients]		
Enable publishing (     Deliver results via [     Notify results via E     To E-mail	E-mail mail	P Server in manager	Configuration screen to use this option)		
Enable publishing (     Deliver results via       Notify results via E     To E-mail     Update status via RSS     Show in	poption (Configure SMTF E-mail mail Select Feed V none	P Server in manager	Configuration screen to use this option) [Use comma(,) to separate multiple e-mail recipients]		

Figure 35

REPORT WIZARD TITLE: INFOBLOX-USER LOGON DETAILS DATA PERSIST DETAIL			CANCEL < BACK NE	XT >
Select columns to persist			Step 9 of 10	
RETENTION SETTING Retention period: 7 day Persist in database only <i>(Repor</i> ) SELECT COLUMNS TO PER COLUMN NAME Device Address User Name Saurce Address Cansole Type Lagan Status	IS IST	ublished and will only be stored in the respective database]		

Figure 36

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

### 8.2 Creating Dashlets

- 1. EventTracker 8 is required to configure the Flex dashboard.
- 2. Open EventTracker in browser and logon.







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



Click ⊕ to add a new dashboard.
 Flex Dashboard configuration pane display.

http://localhost:8080/CustomDashboard/Addl	ditDashboard.aspx?did=14 - Inter
FLEX DASHBOAR	RD
Title SonicWALL Firewall VPN U: Description SonicWALL Firewall VPN-User Au	thentication failed

#### Figure 39

- 5. Fill in the title and description and click **save**.
- Click settings to configure a new Flex dashlet. The Widget configuration pane display.

### WIDGET CONFIGURATION

WIDGET TITLE NOTE	
SonicWALL Firewall-VPN User authentication success	
DATA SOURCE	
SonicWALL Firewall-VPN User authentication success	
CHART TYPE DURATION VALUE FIELD SETTING AS OF	
Donut V 12 Hours V COUNT V Now V	
AXIS LABELS [X-AXIS] LABEL TEXT	
Additional Information	
VALUES [Y-AXIS] VALUE TEXT	
Select column	
FILTER FILTER VALUES	
Select column	
LEGEND [SERIES] SELECT	
Select column 🔽 All 🔽	

#### Figure 40

- a. Locate the earlier scheduled report in the Data Source dropdown.
- b. Select **Chart Type** from the dropdown.
- c. Select the extent of data to be displayed in the **Duration** dropdown.
- d. Select the computation type in the Value Field Setting dropdown.
- e. Select the evaluation duration in the As Of dropdown.
- f. Select the comparable values in the **X-Axis** with a suitable label.
- g. Select the numeric values in the **Y-Axis** with a suitable label.
- h. Select the comparable sequence in Legend.
- i. Click the **Test** button to evaluate.

Evaluated chart display.

SONICWALL FIREWALL-VPN A	
Sophie Clara ammy ajay	

#### Figure 41

j. Once done, click the **Configure** button.

CUSTOMIZE WIDGETS		⊕ 🗓 😣
Cisco IronPort ESA-User authenti	SonicWALL VPN-User authentica	

Figure 42

- 7. Click **Customize** to locate and choose created dashlet.
- 8. Click 🕀 to add dashlet to earlier created dashboard.

## 9. Sample Reports

#### • SonicWALL Firewall - Configuration Change Details

LogTime	Computer	Username	Source IP Address	Destination IP Address	Message
10/12/2015 12:15:39 PM	SONIC	mike	10.20.2.100	10.20.2.1	High Availability is disabled
10/12/2015 12:15:39 PM	SONIC	john	10.20.2.110	10.20.2.1	High Availability is enabled
10/12/2015 12:15:40 PM	SONIC	robin	10.20.2.45	10.20.2.1	User created
10/12/2015 12:15:40 PM	SONIC	james	10.20.2.78	10.20.2.1	logging configured

Figure 43

#### • SonicWALL Firewall-VPN IPsec tunnel status changed

LogTime	Computer	Source Range	Destination Range	Gateway	Reason	Status	VPN Details
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPSec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPSec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPSec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPSec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPSec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPSec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPSec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPSec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPSec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPSec SaNode	Tunnel Down	policy 39(DataVai/VPN218)

#### Figure 44

#### • SonicWALL Firewall – Network Access Report

LogTime	Source Address	Source Port	Destination Address	<b>Destination Port</b>	Wan Address	Message
04/26/2015 11:17:06 AM	1.214.119.227	55499	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 11:17:03 AM	1.214.119.227	55499	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:47 PM	1.214.119.227	56995	98.191.208.24	80	98.191.208.24	Web access request dropped
04/26/2015 12:32:47 PM	1.214.119.227	57658	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 12:32:47 PM	1.214.119.227	56603	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 12:32:47 PM	1.214.119.227	56239	98.191.208.24	80	98.191.208.24	Web access request dropped
04/26/2015 12:32:47 PM	1.214.119.227	55788	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 12:32:44 PM	1.214.119.227	58256	98.191.208.24	80	98.191.208.24	UDP packet dropped
04/26/2015 12:32:44 PM	1.214.119.227	57658	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:43 PM	1.214.119.227	56995	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:43 PM	1,214.119.227	56603	98.191.208.24	80	98.191.208.24	Web access request dropped
04/26/2015 12:32:42 PM	1.214.119.227	56239	98.191.208.24	80	98.191.208.24	UDP packet dropped
04/26/2015 12:32:42 PM	1.214.119.227	137	98.191.208.24	137	98.191.208.24	Connection Closed
04/26/2015 12:32:42 PM	1.214.119.227	137	98.191.208.24	137	98.191.208.24	ICMP packet dropped due to policy
04/26/2015 12:32:42 PM	1.214.119.227	55788	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:47 PM	1.214.119.227	58256	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 05:37:36 AM	1.30.20.148	137	98.191.208.24	137	98.191.208.24	Connection Closed
04/26/2015 05:37:36 AM	1.30.20.148	137	98.191.208.24	137	98.191.208.24	ICMP packet dropped due to policy
04/26/2015 05:37:35 AM	1.30.20.148	12238	98.191.208.24	22	98.191.208.24	UDP packet dropped
04/26/2015 05:37:35 AM	1.30.20.148	12238	98.191.208.24	22	98.191.208.24	Connection Opened

Figure 45

## 10. Sample Dashboards

• SonicWALL Firewall-VPN user authentication success



Figure 46



### **About Netsurion**

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion <u>Managed Threat Protection</u> combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion <u>Secure Edge Networking</u> delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guid ing hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>.

#### **Contact Us** Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

#### **Contact Numbers**

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support