

How-To Guide

Configuring SonicWALL UTM to Forward Logs to EventTracker

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

Table	of Contents	3
1. C	Dverview	4
2. F	Prerequisites	4
3. I	ntegrating SonicWALL UTM with EventTracker	4
3.1	Configuring the Syslog Settings	4
3.2	Configuring the Syslog Server	7
4. S	syslog Send Receive Verification	8
4.1	Verifying the Ping from SonicWALL UTM to EventTracker	8
4.2	Verifying the Syslog messages forwarding on SonicWALL UTM	9
4.3	Verifying the Syslog messages in EventTracker	11
Abo	out Netsurion	12
Cor	ntact Us	12

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 Netw	ork Security Appliance			
▶ 🐻 DPI-SSL	Syslog			
VoIP				
Anti-Spam	Accept Cancel			
► 🚳 VPN	Svslag Settings			
SSL VPN	Sysicg Settings			
Virtual Assist	Syslog Facility:	Local Use 0	-	
Users	Override Syslog Settings with Reporting Software	are Settings		
High Availability	Syslog Event Redundancy Filter (seconds):	0		
Security Services	Surlag Formati	Dofault -		
WAN Acceleration	Systog Pormat:			
AppFlow	Syslog ID:	firewall		
V 🖳 Log	Enable Event Rate Limiting			
View	Maximum Events Per Second:	1000		
Categories	Enable Data Rate Limiting			
Automation	Maximum Bytes Per Second:	1000000		
Name Resolution				
Reports	Syslog Servers			
Analyzer	Server Name		Server Port	Configure
	No Entries			
	Add			



- 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.

amma	Syslog		
N Syslog Settings Assist Syslog Fadilty: Local Use 0 Valability Override Syslog Settings with Reporting Software Settings valability Syslog Event Redundancy Filter (seconds): 0 y Services Syslog Format: Default Syslog Di: Inferwall Image: Signed Setting Settings Inferwall Image: Signed Setting Sett	am Cancel		
Asist Sydog Facility: Local Use 0 Valability Sydog Event Redundancy Filter (seconds): 0 Sydog Event Redundancy Filter (seconds): 0 Sydog Format: Default Sydog Format: Default Sydog Format: I Default Maximum Events Per Second: I 000 Maximum Events Per Second: I 000 Maximum Bytes Per Second: I 000000 Resolution Resolution Sydog Servers Syd	Syslog Settings		
s Image: Coverride Sysiog Settings with Reporting Software Settings Availability Sysiog Event Redundancy Filter (seconds): 0 rity Services Sysiog Format: Default i Acceleration Sysiog ID: firewall How Sysiog ID: firewall I Enable Event Rate Limiting Image: Coverride Sysiog ID: 1000 tepories Image: Coverride Sysiog ID: firewall Ideximum Events Per Second: 10000 temation Maximum Bytes Per Second: 10000000 storation Sysiog Servers	al Assist Syslog Facility:	Local Use 0	
Availability Syslog Event Redundancy Filter (seconds): 0 inty Services Syslog Format: Default • How Syslog ID: firewall Flow Enable Event Rate Limiting Image: Services Image: Services Image: Services Image: Services Image: Services Image: Services Syslog Event Redundancy Filter (seconds): Image: Services Image: Services Image: Services Syslog Event Redundancy Filter (seconds): Image: Services	s 📝 Override Syslog Settings with Reporting S	oftware Settings	
Unity Services Sysiog Format: Default N Acceleration Sysiog Format: Default Flow Sysiog ID: firewall Image: Im	n Availability Syslog Event Redundancy Filter (seconds)): 0	
Filow Syslog ID: firewall Filow Enable Event Rate Limiting Image: Syslog ID: 1000 ategories Enable Data Rate Limiting utumation Maximum Bytes Per Second: 10000000 ame Resolution Syslog Servers	urity Services Syslog Format:	Default 👻	
ew Cable Event Rate Limiting Maximum Events Per Second: I000 Cable Data Rate Limiting Atomation Maximum Bytes Per Second: Cable Data Rate Limiting System Events Cable Data Rate Limiting System Events Cable Data Rate Limiting System Events Cable Data Rate Limiting Cable Data Rate Rate Data Rate Limiting Cable Data Rate Rate Data Rate Data Rate Limiting Cable Data Rate Data Rate Limiting Cable D	Flow Syslog ID:	firewall	
ew Maximum Events Per Second: 1000 tegories Image: Enable Data Rate Limiting stomation Maximum Bytes Per Second: 10000000 me Resolution Systog Servers	Enable Event Rate Limiting		
Image: Set	ew Maximum Events Per Second:	1000	
utomation Maximum Bytes Per Second: 10000000 ame Resolution ame Resolution Syslog Servers	ategories Enable Data Rate Limiting		
me Resolution Syslog Servers	Itomation Maximum Bytes Per Second:	1000000	
ports	me Resolution System Servers		
	vorts		



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

6. Click the Configure icon 🕙 . 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
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 10000000 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				.
► 🈡 VoIP					
Anti-Spam	Syslog Settings				
🕨 🐻 VPN		1			
SSL VPN	Systog 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 Commen				
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.



SonicWALL	Network Security A	Appliance
Name or IP Address:	10.10.1.29	
Port:	5 <mark>1</mark> 4	
	ОК	Cancel

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.

	Lances .		
SSL	Log /		
1	Syslog		
-Spam			
	Accept Cancel		
VPN			
ial Assist	Syslog Settings		
s	Syslog Facility:	Local Use 0	
Availability	Ouerride Surles Settings with Departing Setting	en Cattinga	
rity Services	Overnue sysiog setungs with Reporting Software	resetungs	
I Acceleration	Syslog Event Redundancy Filter (seconds):	0	
Flow	Syslog Format:	Default 🔹	
	Syslog ID:	firewall	
ew	Enable Event Pate Limiting		
ategories		1000	
slog	Maximum Events Per Second:	1000	
Itomation	Enable Data Rate Limiting		
ame Resolution	Maximum Bytes Per Second:	1000000	

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	System / Diagnostics
Certificates Time Schedules Settings Packet Monitor Diagnostics	Tech Support Report Indude: VPN Keys ARP Cache DHCP Bindings IKE Info SonicPointN Diagnostics V Current users Include inactive users Geo-IP/Botnet Cache
Restart Second Point Firewall Firewall Settings Firewall Settings No DPI-SSL Second Point No DPI-SSL Second Point No DPI-SSL Second Point No DPI-SSL Second Point No DPI-SSL No DPI-SSL Second Point No DPI-SSL Second Point Second Point S	Enable Periodic Secure Backup of Diagnostic Reports to Support Time Interval (minutes) 1440 Include raw flow table data entries when sending diagnostic report Diagnostic Tools
Anti-Spam O VPN VPN	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**.

Netsurion®

t Configurations: Filters 😈 General 🛈 Logging 🛈 Mirroring 🔞
Capture Stop Capture Start Mirror Stop Mirror Log to FTP server Export as:
red Packets

- 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	Monitor Filter	Display Filter	Logging	Advanced Monitor Filt	er Mirror
Ionitor Filter (Us	ed for both m	virroring and pa	cket capture		
		,	cher cupture,	,	
Enable filter based	l on the firewall/a	op rule			
nterface Name(s):					
ther Type(s):	IP.			•	
P Type(s):	UDI	2		•	
ource IP Address(es):				•	
ource Port(s):					
estination IP Address	(es):			•	
estination Port(s):	514			•	
Enable Bidirectiona	Address and Por	t 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.

Netsurion®

Settings	Monitor Filter	Display Filter	Logging	Advanced Monitor Filter	Mirror
wanced Filt					
vanceu rin	er				
Monitor Firev	vall Generated Packets	. (This will bypass inte	rface filter)		
Monitor Inter	mediate Packets.				
Monitor i	ntermediate multicast	traffic.			
Monitor i	ntermediate IP helper	traffic.			
Monitor i	ntermediate reassemb	ed traffic.			
Monitor i	ntermediate fragmente	ed traffic.			
Monitor i	ntermediate remote mi	rrored traffic.			
Monitor i	ntermediate IPsec traf	fic.			
Monitor i	ntermediate SSL decry	pted traffic.			
Monitor i	ntermediate decrypted	LDAP over TLS packe	ts. T		
Monitor i	ntermediate decrynter	Single Sign On agent	messages.		

5. Click **OK** to save the packet capture setup.

Packet Monitor

 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.

i u												
	Configure	Monitor All	Monitor Default	С	lear Refresh							
Pack	et Monitor											
0	🕴 Trace active	e, Buffer size 500	KB, 10 Packets ca	ptured, Bu	iffer is 0% full, 0 MB of Bi	uffer lost						
0	Local mirror	ing off, Mirroring	to interface:NONE,	0 packets	mirrored, 0 pkts skipped,	0 pkts exceeded rate						
	Remote min	roring Tx off, Min	roring to: 0.0.0.0,	0 packets r	mirrored, 0 pkts skipped,	0 pkts exceeded rate						
	FTP logging	off. ETP Server	Pass/Failure count:	0/0. FTP	Thread is Idle. Buffer stat	us OK						
Curre	nt Buffer Stati	istics: 0 Dropped	, 0 Forwarded, 0 C	onsumed, 1	0 Generated							
Curre	nt Configuratio	ons: Filters 🛈	General 🛈 Lo	igging 🛈	Mirroring 🛈							
Sta	rt Capture	Stop Capture	Start Mirror	Stop Mir	Tor Log to FIP se	erver Export as:	•					
Captured Packets			SonicW	ALL's X0/ addre	interface IP ss	Syslog Server's IP address				Items 1	to 10 (of 10) 🕡	
#	Time		Ingress	Egress	urce 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)	1000	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)		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]	
-			UAP/ 1			100 100 100 100	-	100			07510751	
						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.
- 3. Log Search would display the syslog messages which EventTracker is receiving from SonicWALL UTM.



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 guiding han d 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