SONICWALL®

Integration Guide: SonicOS and Fastvue Reporter

May 2019

This document describes how SonicOS is integrated with Fastvue Reporter. Such integration allows Fastvue Reporter to interpret SonicWall firewall log files giving real-time web activity reports. It also integrates with SonicWall's Content Filtering System (CFS) and its authentication tools for security and protection.

Topics:

- About Fastvue
- Requirements
- Installing Fastvue Reporter
- Configuring Your SonicWall Syslog
- References

About Fastvue

Fastvue helps businesses and schools deliver useful Internet usage reports to human resources personnel, teachers, department managers and information technology staff. You can use Fastvue Reporter for SonicWall to:

- Send scheduled reports to department managers and HR detailing their staff's Internet usage.
- Safeguard students by monitoring access to self-harm, extremist, or inappropriate content.
- Monitor and troubleshoot your network in real-time to uncover the firewall features and policies responsible for allowing or blocking specific traffic.

Requirements

- Fastvue Reporter
- SonicOS 6.2.6 and above, SonicOS 5.8/5.9
- Windows Server 2008 R2 and above (x64 Windows Operating Systems)
- .NET 4.6, Microsoft IIS, Open JDK and Elasticsearch are automatically installed and configured
- Minimum CPU and RAM recommendations: Less than 500 users 4 CPUs/Cores, 6 GB RAM

Installing Fastvue Reporter

- 1 Go to https://www.fastvue.co/sonicwall/ and click DOWNLOAD.
- 2 In the **Download Fastvue Reporter for SonicWall** popup window enter your contact details, and click **DOWNLOAD** again.

3 Install Fastvue Reporter for SonicWall on a machine (or virtual machine) that meets the recommended requirements for your network size.



() NOTE: Installing Fastvue Reporter for SonicWall also installs and configures .NET 4.6, Microsoft IIS, and Open JDK and Elasticsearch.

V fastvue							
Inst Son This opt and bac IIS. Read	all Fastvue Reporter for icWall 1.0 ion installs the Fastvue Reporter for SonicWall web application kground service. This will also install and configure Microsoft d Getting Started Guide						
Exit							
Copyright © 2018 Fastvue In	۵.						

Configuring Your SonicWall Syslog

Configure SonicWall to send network and web traffic events via Syslog to the Fastvue Reporter machine.

- 1 Go to MANAGE | Logs & Reporting | Log Settings | SYSLOG.
- 2 Under Syslog Settings, set the Syslog Format to Enhanced Syslog from the drop-down list.

Syslog Settings	
Syslog ID:	firewall
Syslog Facility:	Local use 0
Syslog Format:	Enhanced Syslog 🔻
Maximum Events Per Second:	1000
Maximum Bytes Per Second:	1000000
Enhanced Syslog Fields Settings: 🛞	ArcSight CEF Fields Settings:
Enable NDPP Enforcement for Syslog Ser	ver
ACCEPT	

- 3 Click ACCEPT to apply the settings to all Syslog Servers except for GMS and Analyzer.
- 4 Click the Enhanced Syslog Fields Settings button to the right and check all the available fields.

Enhanced Syslog Setting	gs		
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	🗹 Raw Data	✓ File ID
File Tx Status	✓ Rule Action (fw_action)	🗹 uuid	
	SELECT A	LL CLEAR ALL	SAVE CANCEL

- 5 Click SAVE.
- 6 Under **Syslog Servers**, click **ADD** to add your Fastvue Reporter server.

Syslog	Server	S	Items per	page 50		Items 0		to 0 (of 0)@ 1 D
# Ever	nt Prof	Server Name	Server P	Server Type	Server Facility	Server Format	Server ID	Enable	Con
ADD)	ENABLE ALL	DISABL	E ALL				DELETE	E ALL

7 In the popup dialog window that displays, choose **Select an address object** next to **Name or IP Address**.

SONICWALL" NS _a 9650							
Event Profile:	0						
Name or IP Address:	Select an address object 🔻						
Port:	Select an address object						
Server Type:	Create new address object						
Syslog Format:	Default 🔻						
Syslog Facility:	Local Use 0						
Syslog ID:	firewall						
Enable Event Rate Limiting Maximum Events Per	1000						
Second:							
Maximum Bytes Per Second:	1000000						
Bind to VPN Tunnel and Create	Network Monitor Policy in NDPP Mode:						
Local Interface:	Select an interface						
Outbound Interface:	Select a tunnel interface v						
Ready							
	OK CANCEL						

- 8 In the popup dialog window that displays, enter the **Name**, **Zone Assignment**, **Type**, and **IP Address** of your Fastvue Reporter server.
- 9 Click **OK** when done.

SONIC	LL" N	NS _a 9650				
Event Profile:		0				
Name or IP Address:		Select an address ol	oject ▼			
Port:		514				
Server Type:		Syslog Server 🔻				
Syslog Format:		Default	T			
Syslog Facility:		Local Use 0			۲	
Syslog ID:		firewall				
Enable Event Rat Maximum Events Second:	te Limiting 8 Per	1000				
Add Address Objec Anot secure + SONICWA Name:	t - Google (ttps:// LL" N Fastvue	Chrome $VS_a 9650$ Reporter	-		×	
Zone Assignment:	LAN	•				
Туре:	Host	•				
IP Address:						
Ready						-
		ок		CANC	EL	

After this step you see the Fastvue Reporter IP Address listed under the Server Name column of the Syslog Servers section.

- 10 Go to MANAGE | Logs & Reporting | Log Settings > Base Setup.
- 11 Under the **Category** column, expand the **Log** > **Syslog** section.
- 12 Under the Syslog section, check the Syslog Website Accessed events.
- 13 Check the Syslog box, in the Syslog Website Accessed row, and ensure the Priority is set to Inform.
- 14 In the Event Count column, check to see if the number of Syslog Website Accessed events are increasing. If not, ensure Content Filtering Services is licensed and configured.

	Category	Color	ID	Priority	🝚 Gui	🝚 Alert	🝚 Sysl	og 🤤 Ipfix	👄 Email	Event Count	
۲	System			Mixed			Dee	oped by Reaco		1698	Øð
•	Log			Mixed			G Ove	erflow (0		Øð
+	FTP			Mixed	•	0	GU	t Filter 0		9	Øð
+	Configuration Auditing			Inform	•		Sys	log Filter 0		5	Øð
-	Syslog			Mixed			E-n	sail Filter 0		0	Øð
	Syslog Server Unreachable	•	657	Inform •			✓ Pris Sys	log Event Rate 0		0	Øð
	Maximum Syslog Data Rate Exceeded		655	Critical •			Sys	log Data Rate		9	Øð
	Syslog Website Accessed	•	97	Inform •			₹			20	Øð
	E-mail			Mixed		0	۲			0	Øð
	General			Mixed						1	Øð
×	Security Services			Mixed						39	Øð
۲	Users			Mixed					•	443	Øð
۲	Firewall Settings			Mixed						42201	Øð
	Network			Mixed						1214273	Øð
۲	VPN			Mixed						0	Øð
۲	High Availability			Mixed						0	Øð
Þ	3G/4G, Modem, and Module			Mixed						0	Øð
۲	Firewall			Mixed						0	Øð
Þ	Wireless			Mixed						0	Øð

- 15 In the Category column, expand Network and check the Syslog boxes for Connection Closed, Web Request Receiver, and Web Request Drop, and ensure the Priority is set to Inform.
- 16 In the Category column, expand Security Services and check the Syslog boxes for Website Accessed, and Website Blocked, and ensure the Priority is set to Inform.
- 17 Check the Syslog boxes for the Website Accessed and Website Blocked rows.
- 18 Click ACCEPT.

	Category	Color	ID	Priority	🝚 Gui	🝚 Alert	🝚 Syslog	🝚 Ipfix	🝚 Email	Event Count	
►	FTP			Mixed	•	0	0	0	•	0	
•	Configuration Auditing			Inform	•		٠	•		0	
-	Syslog			Mixed	-		•	•	-	0	
	Syslog Server Unreachable		657	Inform 🗸	\checkmark	\checkmark	\checkmark		\checkmark	0	
	Maximum Syslog Data Rate Exceeded		655	Critical 🗸	✓		\checkmark	\checkmark	~	0	
	Syslog Website Accessed		97	Inform 🗸			\checkmark			0	
►	E-mail			Mixed	•	0	•	•	•	0	
►	General			Mixed	9					1	
•	Security Services			Mixed						45	
►	Users			Mixed					9	29	
•	Firewall Settings			Mixed						41841	
•	Network			Mixed	•	-	•	•	-	1158004	
►	VPN			Mixed	•					0	
•	High Availability			Mixed	•	•	•	•	9	0	
•	3G/4G, Modem, and Module			Mixed	•			•		0	
•	Firewall			Mixed	•	-	•	•	•	0	
•	Wireless			Mixed	•	•			•	0	
•	VoIP			Mixed	9	0	•		9	0	
►	SSL VPN			Inform	•	0	٠	•		0	
►	Anti-Spam			Mixed	•	۲	٠		۲	320	
►	WAN Acceleration			Mixed	•			•		0	
►	SD-WAN			Mixed	•		•	•	٠	3	
	ACCEPT CANCEL										

19 Go to MANAGE | Security Configuration | Security Services > Content Filter.

20 Choose SonicWall CFS, from the drop-down choices, next to Content Filter Type.

21 Under Global Settings, check Enable Content Filtering Service.

						Mode: Configuration
Content Filter Type:	SonicWall CFS V					
(i) You can access all the CFS Policies f	from the Rules > Content Filter Policies pag	je.				
You can access all the CFS Objects f	from the Objects > Content Filter Objects p	page.				
If you believe that a Web site is rate	ed incorrectly or you wish to submit a new	URL, dick here.				
CFS Status						
License Status:	Activated					
Expiration Date:	04/17/2020					
Server Status:	Server is ready @					
Global Settings						
Max URL Caches (entries):	51200]				
Enable Content Filtering Service						
Block if CFS Server Is Unavailable						
Server Timeout:	5	second(s)				
Enable Local CPS Server						
Primary Local CFS Server:						
Secondary Local CPS Server:						
CFS Exclusion						
Exclude Administrator						
Excluded Address:	None					
CFS Custom Category					Items	p to 0 (of 0)
Enable CFS Custom Category						
ADD DELETE	EXPORT			Lookup Domains Containing String:		DELETE ALL
•	Domain		Categories		Configure	
No Entries						
ADD DELETE	EXPORT IMPORT					DELETE ALL
CANCEL						

22 Click ADD and then click ACCEPT.

Create a CFS policy for your LAN network or zone:

In the CFS Policy dialog box, enter the following from the drop-down choices:

- . Name
- Source Zone
- **Destination Zone**
- Source Address Included
- Source Address Excluded •
- User/Group Included
- **User/Group Excluded** •
- Schedule
- Profile
- Action
- NOTE: Report quality improves when using the following SonicWall features: (i)

Enabling CFS Enabling Authentication Enabling DPI-SSL (Decryption Services) **Enabling Name Resolution** Logging Referrer URLs Blocking QUIC

Add Your SonicWall as a Source in Fastvue Reporter

- 1 Add SonicWall as a Source in Fastvue Reporter on the Start Page after your installation, or in the top navigation section of Fastvue Reporter in Settings | Sources | Add Source.
- 2 Enter the **SonicWall Host or IP** address and **Syslog Port** in the fields provided.
- 3 Click Add Source or Let's Go on the Start Page.

	V fastvue Reporter
	×
Add a SonicWALL Source	
Ensure SonicWALL is sending syslog messages to the Fa SonicWALL as a source below.	stvue Reporter for SonicWALL Server. Then add the
SonicWALL Host or IP	Syslog Port
192.168.1.100	514
	Add Source

NOTE: Ensure SonicWall is sending syslog messages to the Fastvue Reporter from the SonicWall server. Then add the SonicWall as a source. (i)

Explore Fastvue Reporter for SonicWall

- 1 Go to Dashboard | Overview to see the Bandwidth Today, Productivity Today, Productivity Now, and Past 15 minutes charts.
- 2 Go to **Dashboard | Overview** to choose from the three Fastvue dashboards in the top navigation menu: **Bandwidth**, **Productivity**, and **Web Protection**.
- 3 Go to the **Reports**, **Alerts**, and **Settings** pages in the top navigation for more services.

② Dashboard	Reports الله	rel Alerts 9, Settings		
Overview Bandwid	th Producti	wity Web Protection		
Total Size 460.0 GB	Bandy	width Today	Total Size 9.6 GB	Past 15 minutes
Average Size 19.2 GB	27.9 GE	••• Total ••• Incoming ••• Outgoing	Average Size 326.7 MB	••• Total ••• Incoming ••• Outgoing 953.7 MB
Largest Download 20.0 MB @ 08:39 an	18.6 GB	. A A	Largest Download 20.0 MB @ 08:39 am	476.8 MS
Productivity Toda	у	Productivity Today	Productivity Now	Past 15 Minutes
Productivity Toda	y 9% Productive	Productivity Today Productive Acceptable Unproductive Productive Acceptable Uncelegorized	Productivity Now	Past 15 Minutes
	66% Acceptable	2,000	82 Act	2%
	1% Jnproductive	1,000	19 Uni	% productive so
			00	
	0% Inacceptable	0 _{12:00} 14:30 17:00 19:30 22:00	Un	acceptable 0 00:00 00:05 00:10 00:15

4 Under Reports, choose between Overview Report, User Overview Report and Activity Report.

di Ov	User Overview Report	Activity Report		□ ×
0.1	Field		Operator	Values (Multiple values treated with OR (x OR y OR z)
	Security Group	•	Contains	Admins
<mark>8</mark> 2	Source IP	•	In subnet	× 192.168.1.0/24
1 3 3	Site Domain		Equal to	Enter Site Domains
0 4		٩	· · · · · · · · · · · · · · · · · · ·	
	Site Resource Site Query	-		
Date	Site Country	6	Bun Report	
	URL URL with Query			
	Category			
	Application			

5 Under Activity Report, see the Start Time, End Time, Browsing Time, and Origin Domain of your activity.

St	art Time	End Time	Browsing Time	Origin Domain
20	:02:35	20:59:43	00:12:37	google.com
20	21:48	20:52:35	00:01:04	producthunt.com
20	22:05	20:47:07	00:08:37	facebook.com
20	25:41	20:47:07	00:06:02	workable.com
20	25:46	20:31:12	00:05:26	github.com
20	32:11	20:40:40	00:03:28	invisionapp.com
20	35:37	20:45:40	00:00:00	wistia.net
20	40:17	20:42:39	00:02:22	applicantpro.com
20	42:56	20:46:42	00:03:46	youtube.com
20	52:23	20:58:05	00:00:31	retentiontab.com
20	52:41	20:54:02	00:01:21	weworkremotely.com

6 Under Alerts, choose categories such as **Threat Detected - Malware** or **Unacceptable Browsing** to receive instant notifications regarding your security concerns.



7 Under Settings | Productivity Reporting, adjust your organization's web productivity by dragging and dropping SonicWall's URL categories onto the desired list such as Unproductive or Unacceptable Browsing.

Unproductive	Acceptab			
🕏 Weapons	🙂 Usenet Ne			
C Alcohol	🙂 Persona			
Online Trading/Brokerage	te A			
🔁 Tobacco	C Shareware			
Chat	🙂 Search Er			
	@			

8 Share your Fastvue reports with others using **Scheduled Reports** or by clicking the **Share** button at the top of each report.

Department		New report on:					
Development 📢		Development					
Marketing			·				
Accounts		Activity Report	II Overview Report				
Sales							
п							

9 Configure all your SonicWall devices to send Syslog messages to Fastvue Reporter to achieve centralized reporting.



- 10 Go to Settings | Data Storage to see your data usage.
- 11 Go to **Settings | Data Storage | Settings** to set your **Data Retention Policy** and how large Fastvue Reporter should be for SonicWall's log database.

	Category	Color	ID	Priority	🝚 Gui	🝚 Alert	🝚 Syslog	🝚 Ipfix	🝚 Email	Event Count	
Þ	FTP			Mixed	•	0	0	0	•	0	
•	Configuration Auditing			Inform	•	•	•	•	•	0	
	Syslog			Mixed	•	•	•	•	•	0	
	Syslog Server Unreachable		657	Inform 🗸	v	\checkmark	\checkmark		\checkmark	0	
	Maximum Syslog Data Rate Exceeded		655	Critical 🗸	v		\checkmark	\checkmark	\checkmark	0	
	Syslog Website Accessed		97	Inform 🗸			\checkmark			0	
►	E-mail			Mixed	•	0		•	9	0	
Þ	General			Mixed	•	9			•	1	ØI
۲	Security Services			Mixed						45	ØI
۲	Users			Mixed	9	•	•	•	9	29	ØI
۲	Firewall Settings			Mixed				•		41841	ØI
۲	Network			Mixed	9	•	•	9	9	1158004	ØI
۲	VPN			Mixed						0	ØI
۲	High Availability			Mixed	9	9	9	9	9	0	
۲	3G/4G, Modem, and Module			Mixed	•					0	ØI
۲	Firewall			Mixed	•	-	•	9	•	0	ØI
۲	Wireless			Mixed						0	
۲	VoIP			Mixed	9	0	•	•	9	0	ØI
۲	SSL VPN			Inform		0	•	•		0	ØI
۲	Anti-Spam			Mixed	•	٠	•	•	•	320	ØI
۲	WAN Acceleration			Mixed	•			•		0	ØI
۲	SD-WAN			Mixed	•	9	۲	•	۲	3	
	ACCEPT CANCEL										

References

For more information on using Fastvue Reporter for SonicWall, go to https://www.fastvue.co/sonicwall, or contact Fastvue at https://www.fastvue.co/support.

Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/eupa.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

() IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 5/17/19