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

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

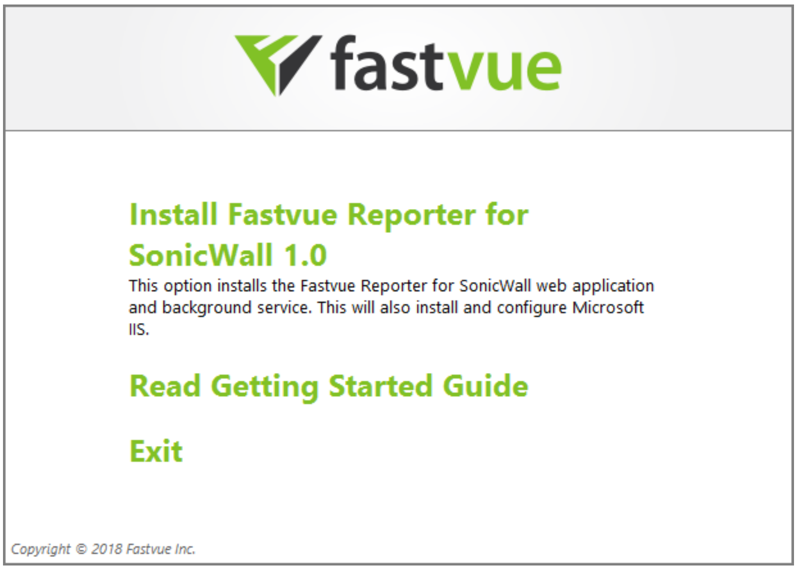
- Fastvue Reporter
- SonicOS 6.2.6 and above, SonicOS 5.8/5.9
- Windows Server 2008 R2 and above (x64 Windows Operating Systems)
- .NET 4.6, Microsoft IIS, Open JDK and Elasticsearch are automatically installed and configured
- Minimum CPU and RAM recommendations: Less than 500 users - 4 CPUs/Cores,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



Install Fastvue Reporter for SonicWall 1.0

This option installs the Fastvue Reporter for SonicWall web application and background service. This will also install and configure Microsoft IIS.

Read Getting Started Guide

Exit

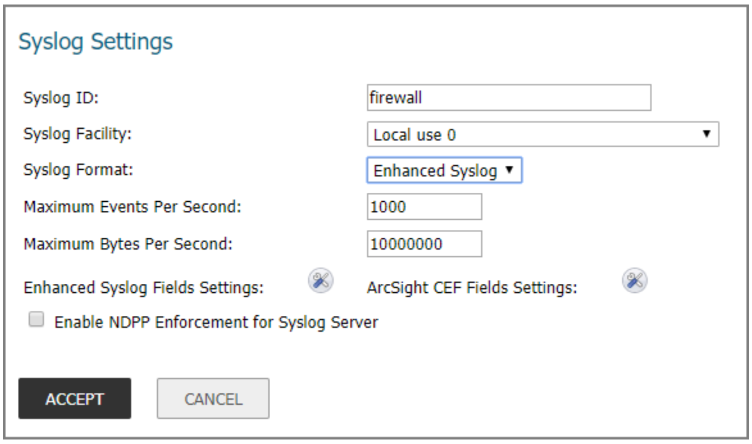
Copyright © 2018 Fastvue Inc.

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

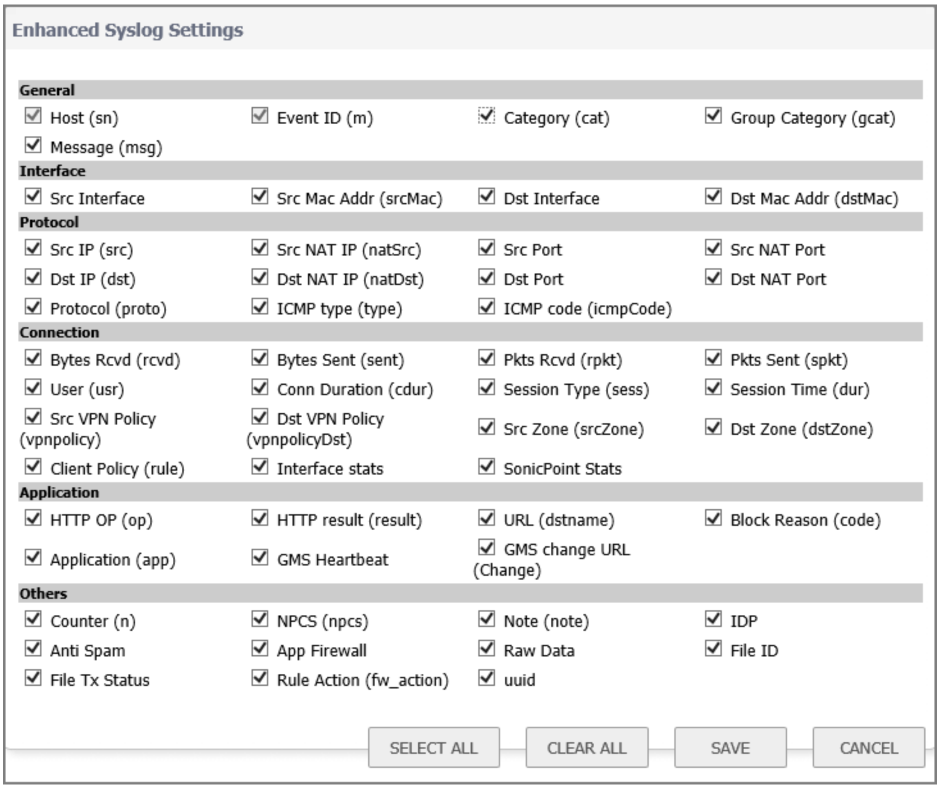
Maximum Events Per Second: 1000

Maximum Bytes Per Second: 10000000

Enhanced Syslog Fields Settings:
ArcSight CEF Fields Settings:
☐ Enable NDPP Enforcement for Syslog Server
ACCEPT
CANCEL

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.

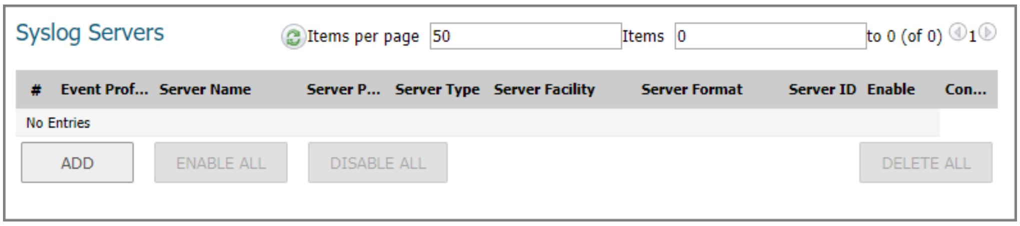


Enhanced Syslog Settings

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	

5 Click **SAVE**.

6 Under **Syslog Servers**, click **ADD** to add your Fastvue Reporter server.

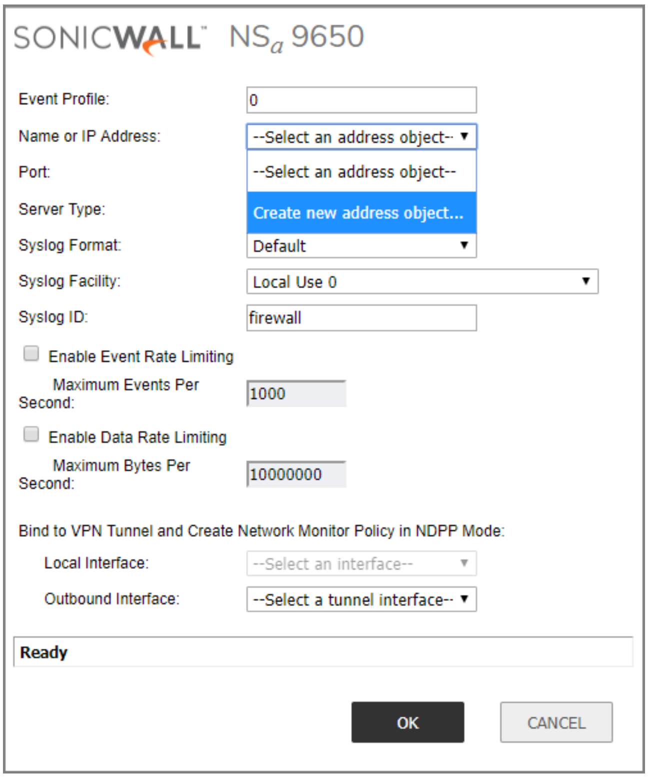


Syslog Servers

Items per page 50 Items 0 to 0 (of 0) 1

#	Event Prof...	Server Name	Server P...	Server Type	Server Facility	Server Format	Server ID	Enable	Con...
No Entries									

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--

--Select an address object--

Create new address object...

Port:

Server Type:

Syslog Format: Default

Syslog Facility: Local Use 0

Syslog ID: firewall

□ Enable Event Rate Limiting

Maximum Events Per Second: 1000

□ Enable Data Rate Limiting

Maximum Bytes Per Second: 10000000

Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode:

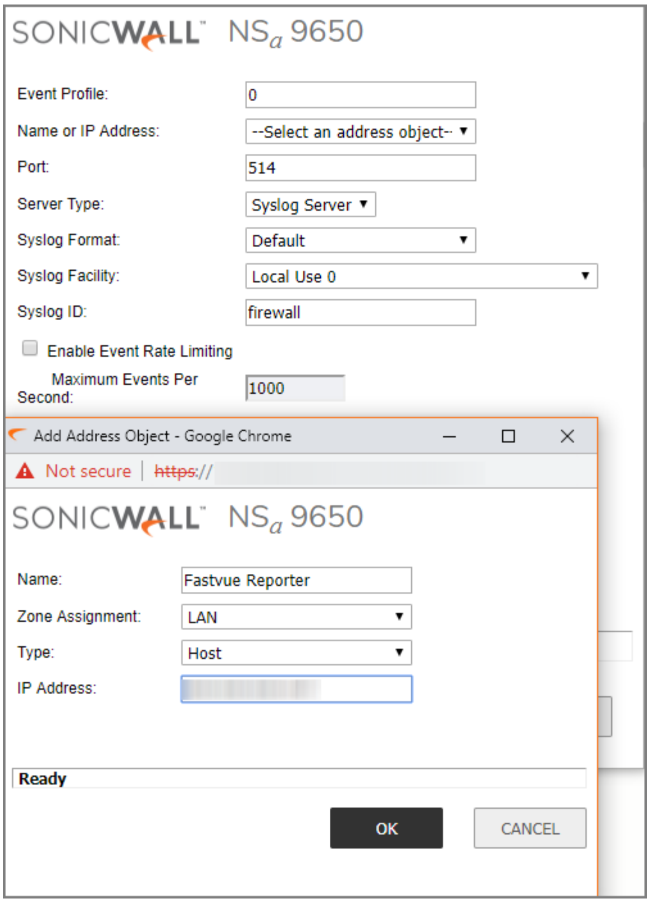
Local Interface: --Select an interface--

Outbound Interface: --Select a tunnel interface--

Ready

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.


SONICWALL NS$_a$ 9650

Event Profile: 0

Name or IP Address: --Select an address object--

Port: 514

Server Type: Syslog Server

Syslog Format: Default

Syslog Facility: Local Use 0

Syslog ID: firewall

□ Enable Event Rate Limiting

Maximum Events Per Second: 1000

Add Address Object - Google Chrome

Not secure | ~~https~~:// [redacted]

SONICWALL NS$_a$ 9650

Name: Fastvue Reporter

Zone Assignment: LAN

Type: Host

IP Address: [redacted]

Ready

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

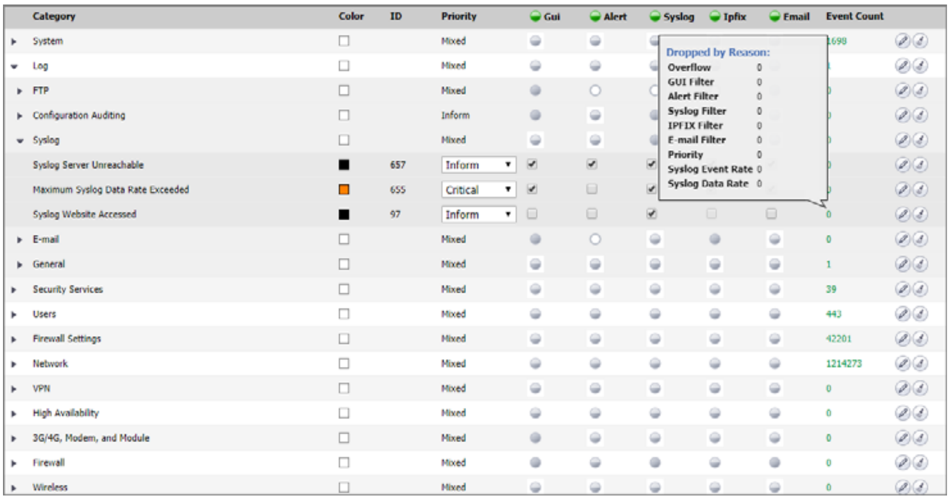
10 Go to **MANAGE | Logs & Reporting | Log Settings > Base Setup.**

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	Syslog	Ipfix	Email	Event Count
▸ System	☐		Mixed	◐	◐	◐			1698
▾ Log	☐		Mixed	◐	◐	◐			
▸ FTP	☐		Mixed	◐	○	○			
▸ Configuration Auditing	☐		Inform	◐	◐	◐			
▾ Syslog	☐		Mixed	◐	◐	◐			
Syslog Server Unreachable	■	657	Inform ▾	☑	☑	☑			
Maximum Syslog Data Rate Exceeded	■	655	Critical ▾	☑	☐	☑			
Syslog Website Accessed	■	97	Inform ▾	☐	☐	☑	☐	☐	0
▸ E-mail	☐		Mixed	◐	○	◐	◐	◐	0
▸ General	☐		Mixed	◐	◐	◐	◐	◐	1
▸ Security Services	☐		Mixed	◐	◐	◐	◐	◐	39
▸ Users	☐		Mixed	◐	◐	◐	◐	◐	443
▸ Firewall Settings	☐		Mixed	◐	◐	◐	◐	◐	42201
▸ Network	☐		Mixed	◐	◐	◐	◐	◐	1214273
▸ VPN	☐		Mixed	◐	◐	◐	◐	◐	0
▸ High Availability	☐		Mixed	◐	◐	◐	◐	◐	0
▸ 3G/4G, Modem, and Module	☐		Mixed	◐	◐	◐	◐	◐	0
▸ Firewall	☐		Mixed	◐	◐	◐	◐	◐	0
▸ Wireless	☐		Mixed	◐	◐	◐	◐	◐	0

Dropped by Reason:

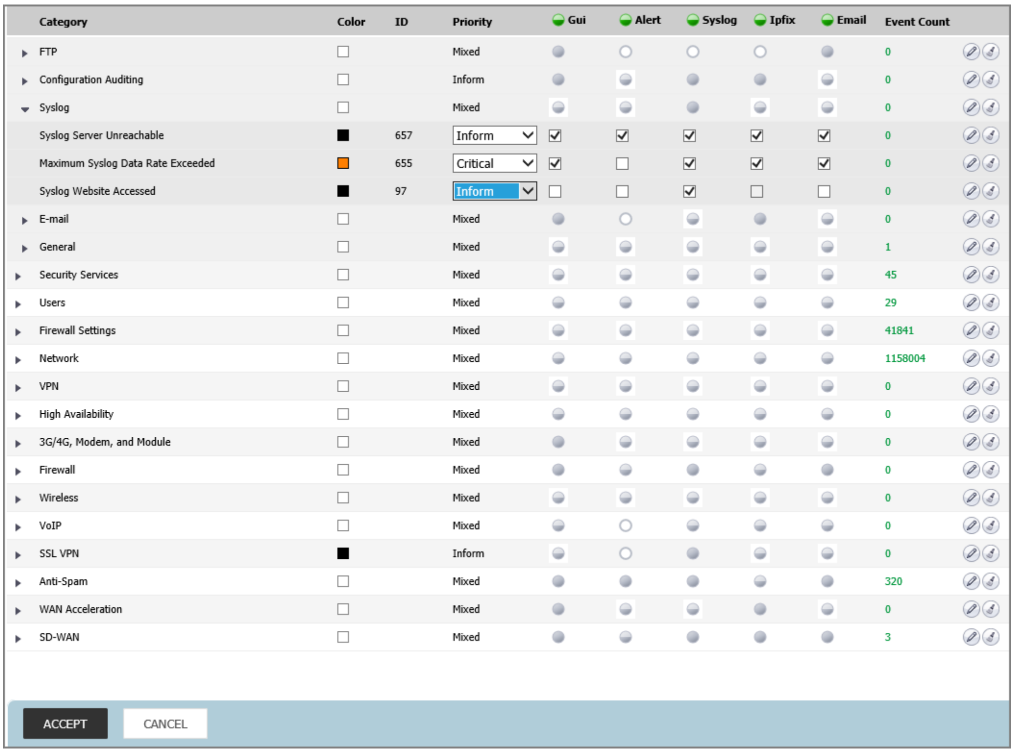
Overflow	0
GUI Filter	0
Alert Filter	0
Syslog Filter	0
IPFIX Filter	0
E-mail Filter	0
Priority	0
Syslog Event Rate	0
Syslog Data Rate	0

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**.

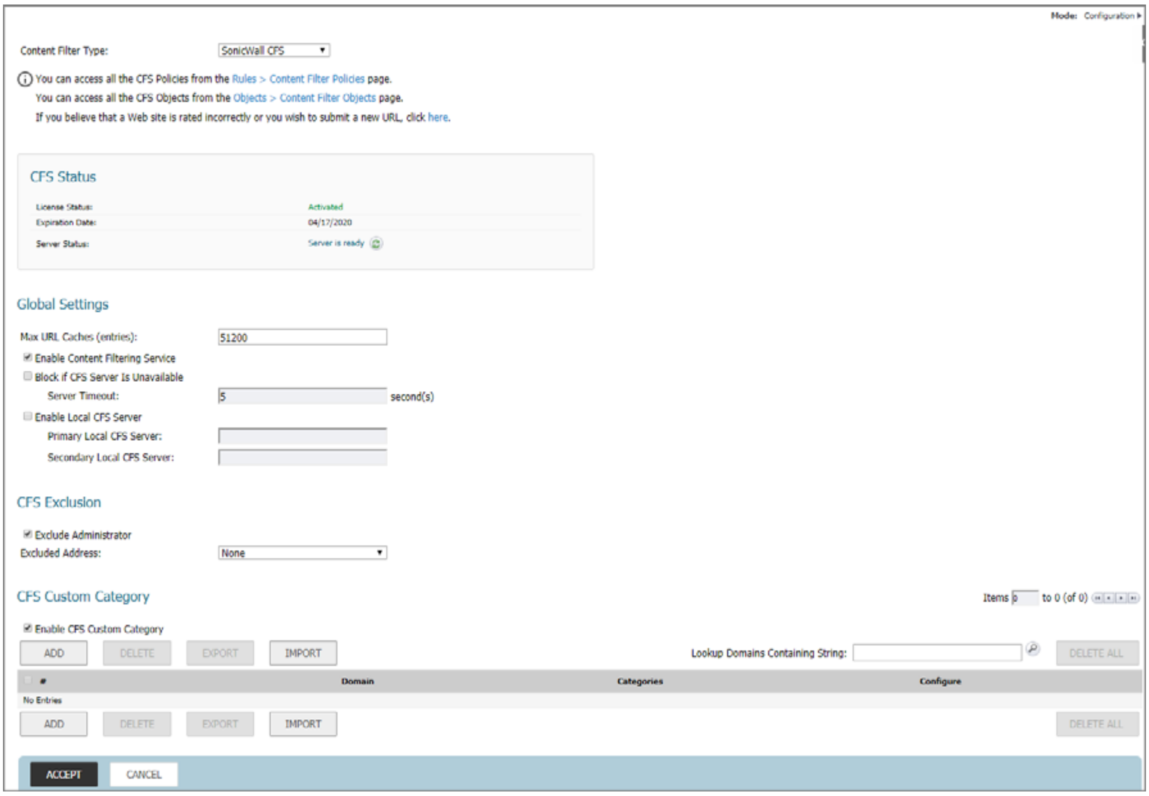


	Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
▸	FTP	□		Mixed	●	○	○	○	●	0
▸	Configuration Auditing	□		Inform	●	●	●	●	●	0
▾	Syslog	□		Mixed	●	●	●	●	●	0
	Syslog Server Unreachable	■	657	Inform	☑	☑	☑	☑	☑	0
	Maximum Syslog Data Rate Exceeded	■	655	Critical	☑	□	☑	☑	☑	0
	Syslog Website Accessed	■	97	Inform	□	□	☑	□	□	0
▸	E-mail	□		Mixed	●	○	●	●	●	0
▸	General	□		Mixed	●	●	●	●	●	1
▸	Security Services	□		Mixed	●	●	●	●	●	45
▸	Users	□		Mixed	●	●	●	●	●	29
▸	Firewall Settings	□		Mixed	●	●	●	●	●	41841
▸	Network	□		Mixed	●	●	●	●	●	1158004
▸	VPN	□		Mixed	●	●	●	●	●	0
▸	High Availability	□		Mixed	●	●	●	●	●	0
▸	3G/4G, Modem, and Module	□		Mixed	●	●	●	●	●	0
▸	Firewall	□		Mixed	●	●	●	●	●	0
▸	Wireless	□		Mixed	●	●	●	●	●	0
▸	VoIP	□		Mixed	●	○	●	●	●	0
▸	SSL VPN	■		Inform	●	○	●	●	●	0
▸	Anti-Spam	□		Mixed	●	●	●	●	●	320
▸	WAN Acceleration	□		Mixed	●	●	●	●	●	0
▸	SD-WAN	□		Mixed	●	●	●	●	●	3

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

ⓘ You can access all the CFS Policies from the Rules > Content Filter Policies page.
You can access all the CFS Objects from the Objects > Content Filter Objects page.
If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click 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 CFS Server
Primary Local CFS Server:
Secondary Local CFS Server:

CFS Exclusion

☑ Exclude Administrator
Excluded Address: None

CFS Custom Category

Items 0 to 0 (of 0)

☑ Enable CFS Custom Category

Lookup Domains Containing String:

#	Domain	Categories	Configure
No Entries			

22 Click **ADD** and then click **ACCEPT**.

Create a CFS policy for your LAN network or zone:

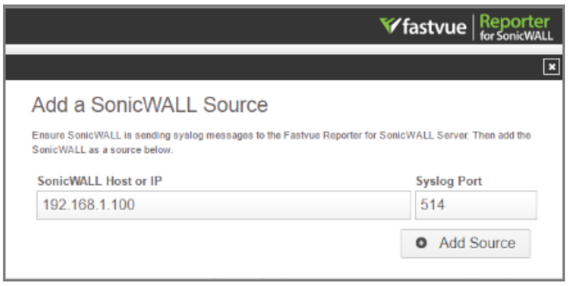
In the CFS Policy dialog box, enter the following from the drop-down choices:

- **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:
> 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**.



Add a SonicWALL Source

Ensure SonicWALL is sending syslog messages to the Fastvue Reporter for SonicWALL Server. Then add the SonicWALL as a source below.

SonicWALL Host or IP: 192.168.1.100

Syslog Port: 514

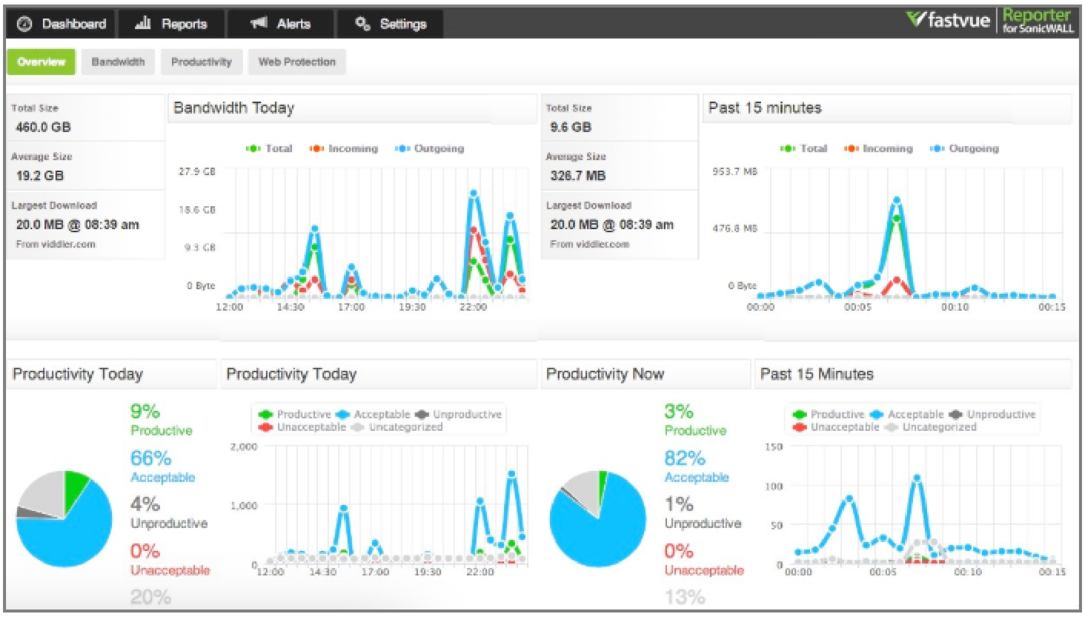
> **NOTE:** Ensure SonicWall is sending syslog messages to the Fastvue Reporter from the SonicWall server. Then add the SonicWall as a source.

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.



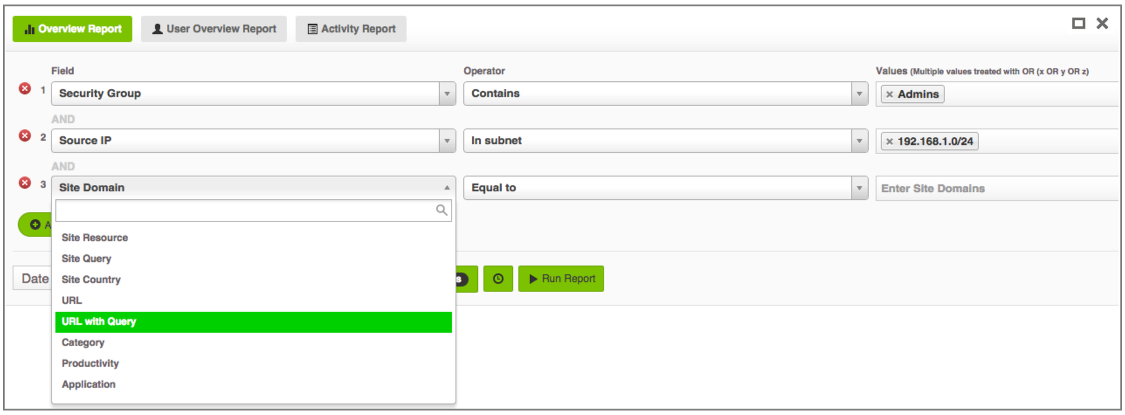
Total Size
460.0 GB
Average Size
19.2 GB
Largest Download
20.0 MB @ 08:39 am
From viddler.com

Total Size
9.6 GB
Average Size
326.7 MB
Largest Download
20.0 MB @ 08:39 am
From viddler.com

Productivity Today: 9% Productive, 66% Acceptable, 4% Unproductive, 0% Unacceptable, 20%

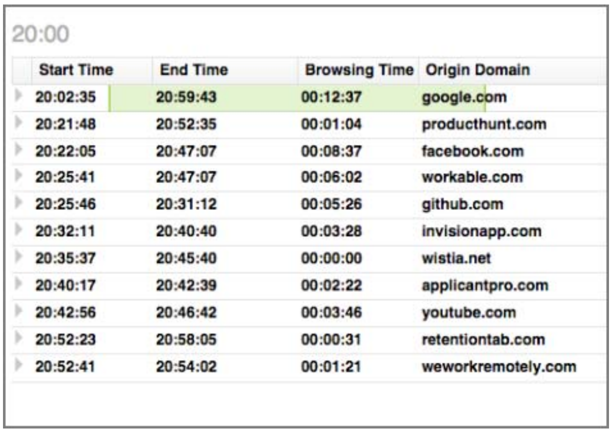
Productivity Now: 3% Productive, 82% Acceptable, 1% Unproductive, 0% Unacceptable, 13%

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



	Field	Operator	Values (Multiple values treated with OR (x OR y OR z)
1	Security Group	Contains	× Admins
	AND		
2	Source IP	In subnet	× 192.168.1.0/24
	AND		
3	Site Domain	Equal to	Enter Site Domains

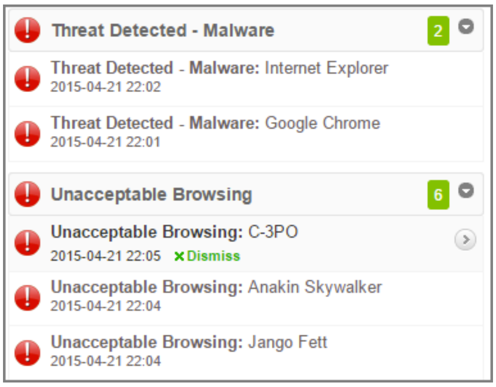
5 Under **Activity Report**, see the **Start Time**, **End Time**, **Browsing Time**, and **Origin Domain** of your activity.



20:00

Start 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.



Threat Detected - Malware 2

Threat Detected - Malware: Internet Explorer
2015-04-21 22:02

Threat Detected - Malware: Google Chrome
2015-04-21 22:01

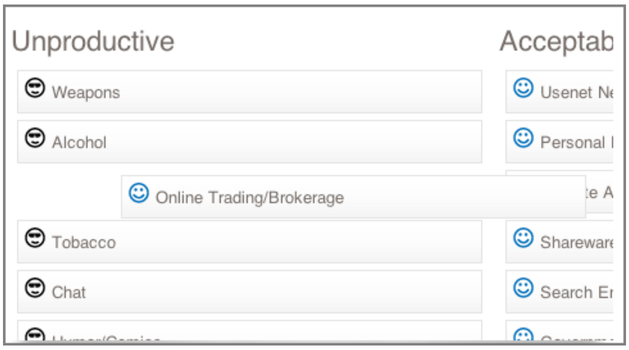
Unacceptable Browsing 6

Unacceptable Browsing: C-3PO
2015-04-21 22:05 ✕Dismiss

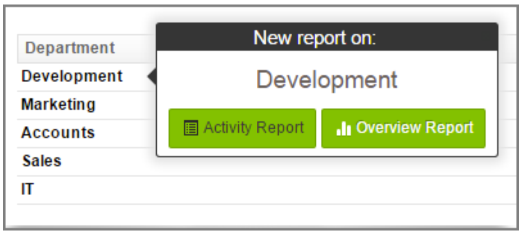
Unacceptable Browsing: Anakin Skywalker
2015-04-21 22:04

Unacceptable Browsing: Jango Fett
2015-04-21 22:04

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**.



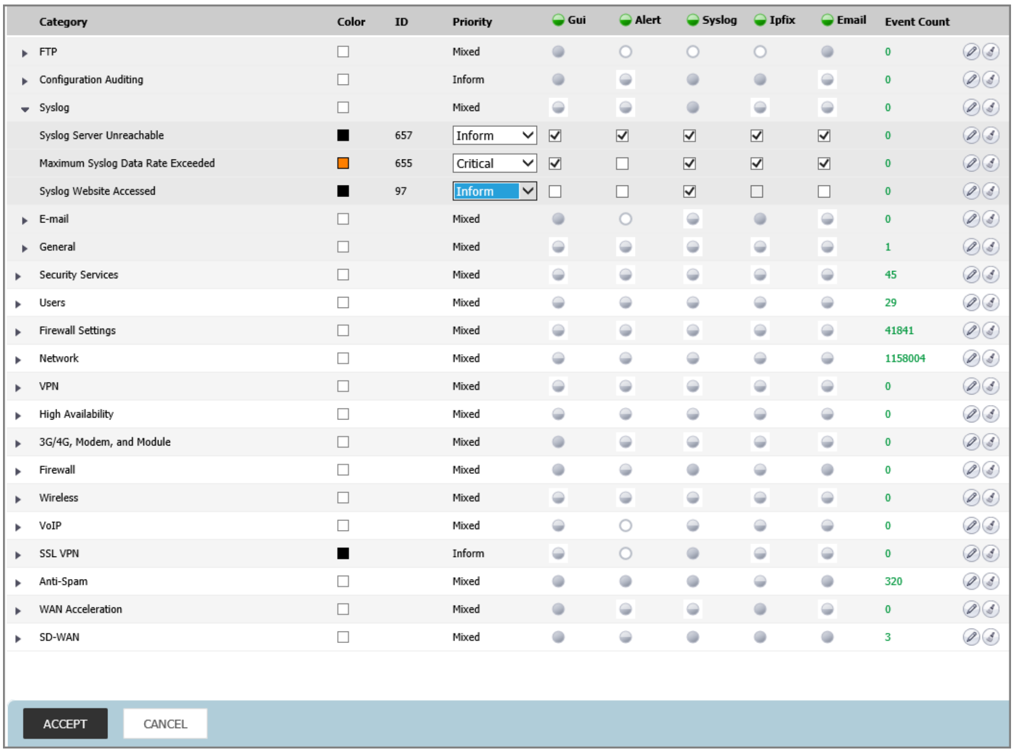
8 Share your Fastvue reports with others using **Scheduled Reports** or by clicking the **Share** button at the top of each report.



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
FTP	□		Mixed	●	○	○	○	●	0
Configuration Auditing	□		Inform	●	◐	●	●	◐	0
Syslog	□		Mixed	◐	◐	●	◐	◐	0
Syslog Server Unreachable	■	657	Inform	☑	☑	☑	☑	☑	0
Maximum Syslog Data Rate Exceeded	🟧	655	Critical	☑	□	☑	☑	☑	0
Syslog Website Accessed	■	97	Inform	□	□	☑	□	□	0
E-mail	□		Mixed	●	○	◐	●	◐	0
General	□		Mixed	◐	◐	◐	◐	◐	1
Security Services	□		Mixed	◐	◐	◐	◐	◐	45
Users	□		Mixed	◐	◐	◐	◐	◐	29
Firewall Settings	□		Mixed	◐	◐	◐	◐	◐	41841
Network	□		Mixed	◐	◐	◐	◐	◐	1158004
VPN	□		Mixed	◐	◐	◐	◐	◐	0
High Availability	□		Mixed	◐	◐	◐	◐	◐	0
3G/4G, Modem, and Module	□		Mixed	●	◐	◐	◐	◐	0
Firewall	□		Mixed	●	◐	●	◐	●	0
Wireless	□		Mixed	◐	◐	◐	◐	◐	0
VoIP	□		Mixed	◐	○	◐	◐	◐	0
SSL VPN	■		Inform	◐	○	●	◐	◐	0
Anti-Spam	□		Mixed	●	●	●	◐	●	320
WAN Acceleration	□		Mixed	●	◐	◐	●	◐	0
SD-WAN	□		Mixed	●	◐	●	●	●	3

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.

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