fastvue

Web Reporting. Solved.

Fastvue Reporter intelligently interprets Sophos (SG, XG and SWA) log files to deliver *useful* web activity reports to HR, Department Managers, IT and You!

SOPHOS

Turn Sophos into a Reporting and Alerting Powerhouse!

You don't need to become a log analysis expert. That's our job. We've created dedicated, streamlined reporting applications for the major web gateways and firewalls. All you need to do is read the reports!
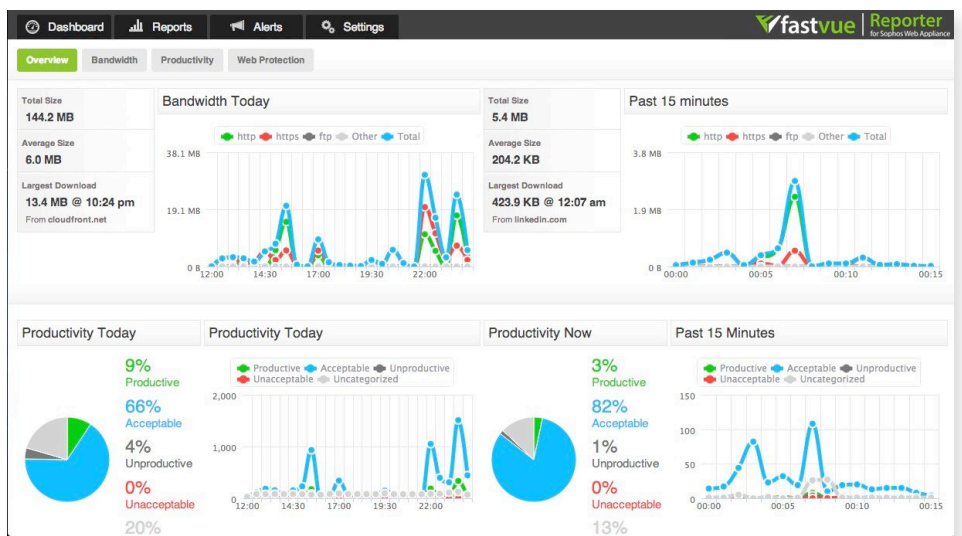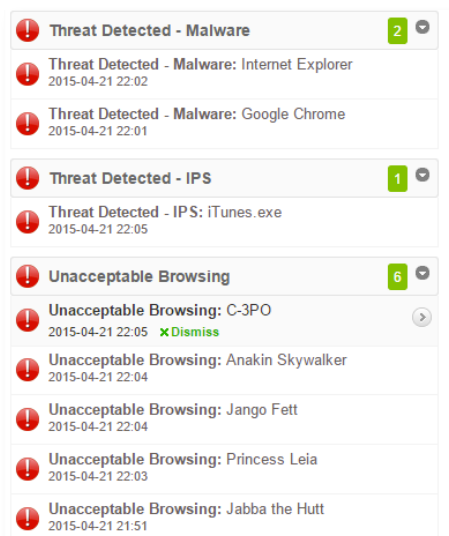

Real-time Alerts

- People accessing unacceptable or extremist material.
- Search terms and URL keywords.
- Large downloads.
- Viruses, threats and more.

Awesome Reports

- Simple, interactive web usage reports non-technical people can understand.
- Seamless Active Directory integration for user or group reporting.
- Report scheduling and distribution.
- Automatic removal of background sites such as google-analytics.com.
- Substitution of CDNs such as akamaihd.net with the real site visited.

---

www.fastvue.co/sophos
sales@fastvue.co

United States: +1 888 885 6711
United Kingdom: +44 (0)203 575 1178
Australia: +61 2 8003 3707

SOPHOSReporter

Powerful Reporting : Zero Learning Curve

Who said enterprise software should be hard to deploy and use? Simply install Fastvue Reporter, pull in the data, and you're ready to enjoy these powerful and incredibly easy to use features:

Overview Reports & Detailed Investigations

Fastvue's Overview Reports highlight the information you need to know such as productivity, bandwidth or network issues.

Need more detail? Fastvue's innovative Activity Reports include timestamps and full URLs intuitively grouped into browsing sessions, with green bars showing exactly when browsing started and stopped.

Intelligent Alerts

Send instant alerts to the right people including searches for extermist or violent content, enormous downloads, unacceptable web activity and network threats. All the detail they need, sent straight to their inbox!

Productivity Reporting

Fastvue Reporter assesses web productivity according to your guidelines to highlight unproductive or unacceptable browsing.

See exactly what is being allowed (or blocked) that shouldn't be, and adjust your Content Filter policies accordingly.

Active Directory Integration

Seamless (zero config) AD integration, enables simple reporting across AD Departments, Offices, Companies and Security Groups.
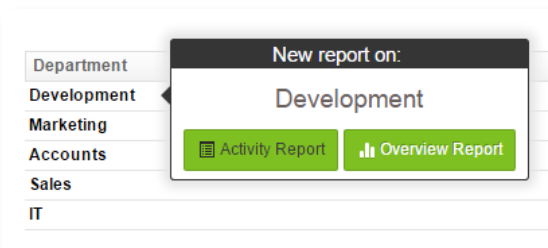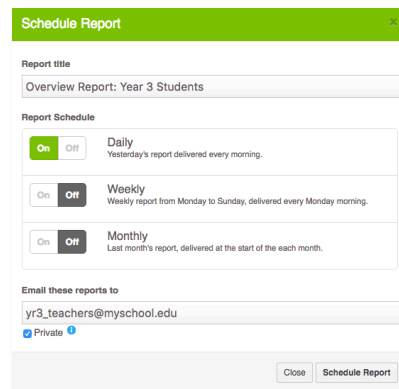
Site Clean

Fastvue Reporter's Site Clean engine automatically removes most Junk URLs and background noise such as fbcdn.net, akamaihd.net and google-analytics.com from your web reports.

Simple Report Scheduling

Automatically send reports to the right person each day, week or month.

Live Dashboards

Fastvue Reporter is always ready to show you what is happening on your network right now. Real-time dashboards focus on the trifecta of network concerns: Bandwidth, Productivity and Security.

Advanced Filtering

Fastvue Reporter's advanced filtering engine narrows down your reports and alerts by anything you can dream up. Subnets, Departments, Keywords, Unproductive traffic, and more!

www.fastvue.co/sophos
sales@fastvue.co

United States: +1 888 885 6711
United Kingdom: +44 (0)203 575 1178
Australia: +61 2 8003 3707
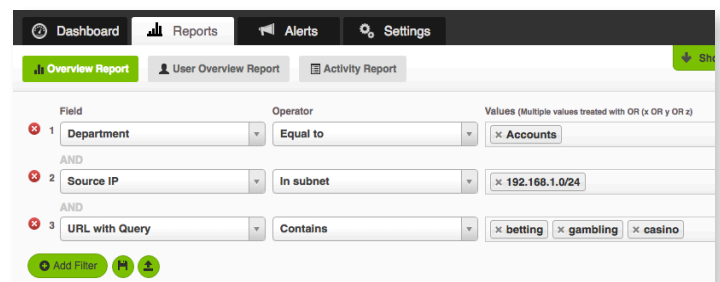
SOPHOS Reporter

Sophos Reporting Made Awesome

There are a few option available when it come to reporting on your Sophos devices.
So what makes Fastvue Sophos Reporter so special?

Sophos On-Box Reports

- Designed for the Sophos UTM Administrators
- Reports mainly on UTM and network performance
- Only basic information about web usage (top users, domains and categories)

Sophos iView Appliance

- Designed for the Sophos UTM Administrators
- Reports mainly on UTM and network performance
- Basic information about web usage (top users, domains and categories)
- Collates data from multiple UTMs
- Provides easy access to the log records that built each report

Fastvue Sophos Reporter

- Designed for *everyone else* concerned about Internet usage
- Also very useful for Sophos Administrators
- Goes beyond simple log aggregation to provide *sensible and useful* information around web usage and productivity and the UTM's policies
- Collates data from multiple UTMs into single dashboards, reports and alerts
- Real-time alerts for any type of traffic or network issue

Feature	Sophos On-Box	Sophos iView	Fastvue Sophos Reporter
Department and Security Group Reports	Limited	X	√
'Sensible' Web Reports (Fastvue Site Clean)	X	X	√
'Readable' Time-Based Activity Reports	X	X	√
Report on Web Policies	X	X	√
Report on Allowed Undesirable Sites/Apps	X	X	√
Report on Blocked Acceptable Sites/Apps	X	X	√
Subnet Reports	X	X	√
Flexible Report Filtering	Limited	Limited	√
Import Historical Logs	N/A	X	√
Fill in Missed Syslog Messages	N/A	X	√
Supports older UTMs	N/A	X	√
Easy to deploy, setup and use	X	X	√

Independent, Honest Reporting

Fastvue is not affiliated with Sophos in anyway, so our reports are not focused on showing you how excellent your Sophos is. Our reports may highlight traffic being allowed when it shouldn't, blocked when it should, mis-categorized websites, ineffective policies and more.

Fastvue Reporter gives you the information you need to make your network efficient, productive and secure, getting the most out of your Sophos investment.

Getting Started

Fastvue Sophos Reporter is simple to install, easy to configure and a joy to use.
Get started in less than 10 minutes.

Download Fastvue Sophos Reporter

Sophos SG and XG UTM:
http://www.fastvue.co/Sophos/download
Sophos Web Appliance:
http://www.fastvue.co/Sophos/SWA/download

For Sophos (SG) UTM Users:

Ensure Sophos UTM has the Web Filtering feature enabled and applied to your network, with at least one category set to block or warn. Then go to **Web Admin | Logging and Reporting | Log Settings | Remote Syslog**, and add the Fastvue server as a syslog server with these settings:
Server = Fastvue Reporter Server IP (add a new host object if necessary)
Port = Drag in the predefined SYSLOG protocol. If you already have a syslog application installed on the Fastvue machine, then use a custom port such as 50514.

Then check the 'Web Filtering' checkbox in the Remote Syslog Log Selection section and click Apply.

For Sophos (XG) UTM Users:

On your XG Firewall, ensure you have a firewall rule with a 'Web Policy' applied and the 'Log Traffic' checkbox checked.

Then go to **Configure | System Services | Log** and add the Fastvue server as a syslog server with these settings:
Server = Fastvue Reporter Server IP
Port = Any unused port on Fastvue machine (514 is the default)
Facility = Daemon
Severity = Information
Format = Device Standard Format.

Then check the 'syslog' checkbox for the 'Content Filtering' log events (Web Filter and Application Filter).

For Sophos Web Appliance Users:

On the Sophos Web Appliance, go to **Configuration | System | Alerts and Monitoring | Syslog**. Check 'Enable Syslog transfer of web traffic (Sophos log)' and enter these settings:
Hostname/IP = Fastvue Reporter Server IP
Port = Any unused port on Fastvue machine (514 is the default)
Protocol = UDP

Note: Sophos Web Appliance only supports a single syslog server. If you already have a syslog server defined, Fastvue Sophos Reporter for Web Appliance includes a syslog forwarder so you can forward the messages on to your existing syslog server.

Add a Source to Fastvue Reporter

Add the Sophos UTM, or the Sophos Web Appliance as a Source in Sophos Reporter. This can be done on the start page that is presented after installation, or in **Settings | Sources | Add Source**. You can also choose to import historical logs, or forward syslog messages at this stage.

Enjoy!

It may take 10-20 seconds before the first records are imported. You can watch the records and dates imported in **Settings | Sources**. Once records start importing, you can go to the Dashboard tab to see your live network traffic.

Now you can explore all the features of Fastvue Reporter such as:

• Live Dashboards (Bandwidth, Productivity and Web Protection).
• Simple, Powerful Reporting.
• Fastvue Site Clean.
• Schedule Reports for anyone in your organization
• Real time alerts.
• Seamless Active Directory integration
• + Many more!

Operating System Requirements

• **Windows Server 2008 R2 or above** (x64 Windows Operating Systems)
• The **Web Server** and **Application Server Roles** (.NET 3.5 and IIS) will be automatically installed and configured.

Take care installing Fastvue Reporter on existing web servers. Do not install to sites or direcories where existing applications are already running (E.g Outlook Web Access).

CPU & RAM Recommendations

Network Size	Recommended Server specification
Less than 500 Users	4 CPUs/Cores, 6 GB RAM
500 – 1000 Users	4 CPUs/Cores, 8 GB RAM
1000 – 3000 Users	8 CPUs/Cores, 12 GB RAM
3000 – 5000 Users	8 CPUs/Cores, 16 GB RAM
5000+ Users	16 CPUs/Cores, 24 GB RAM

Data Storage

The default data retention policy in Fastvue Reporter is 90 days or 50 GB, whichever comes first. This can be adjusted in **Settings | Data Storage**.

The amount of data stored per day will vary depending on the amount of traffic flowing through your SonicWall. Check the amount of data in **Settings | Data Storage** after one day of installing to see if you need to make adjustments to the data retention policy.

www.fastvue.co/sophos
sales@fastvue.co

United States: +1 888 885 6711
United Kingdom: +44 (0)203 575 1178
Australia: +61 2 8003 3707

SOPHOSReporter