Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Sophos Firewall to Forward Logs to EventTracker

EventTracker v9.2 and later

Publication Date:

April 9, 2021

Abstract

This guide provides instructions to configure Sophos SG/UTM and XG Firewall to send crucial events to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2X and later, and Sophos SG/UTM 9 or Sophos XG Firewall version 15.01.0-17.1.2 and later.

Table of Contents

1 Overview

Sophos Firewall combines the best of both Sophos and Cyberoam technology delivering an unprecedented level of innovation to next-generation firewalls. With all new user interface, new security heartbeat technology, and a powerful new unified policy model, it introduces many important innovations that take simplicity, protection, and performance, to a whole new level.

EventTracker collects and analyses firewall events and notifies an administrator about security violations, user behavior, and traffic anomalies.

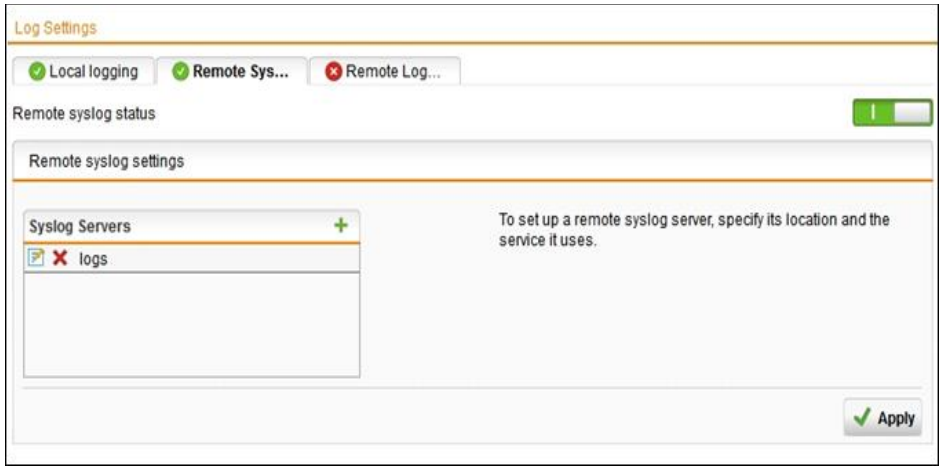
2 Prerequisites

- **EventTracker Agent 9.2x** and above should be installed.
- **Sophos SG/UTM 9** or **Sophos XG Firewall** version **15.01.0-16.5** and later should be installed and configured.

3 Integrating EventTracker with Sophos SG/UTM and XG Firewall

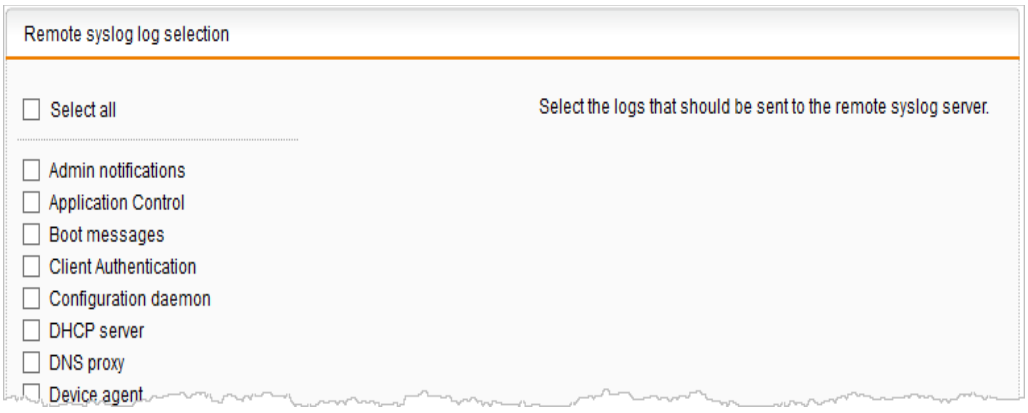
3.1 Enabling syslog forwarding in Sophos SG/UTM firewall

1. Logon to the WebAdmin of the SG/UTM.
2. Navigate to **Logging & Reporting > Log Settings > Remote Syslog Server.**
3. Activate the **Remote Syslog status.**
4. Configure a Syslog server by clicking on **+** button.
   - **Name:** Freely selectable.
   - **Server:** IP or hostname of your **EventTracker Manager IP/EventTracker syslog relay IP.**
   - **Port:** UDP **514.**
5. Click **Apply**.



If syslog messages cannot be delivered, they will be buffered, and re-sends it. By default, up to 1000 logs will be buffered.

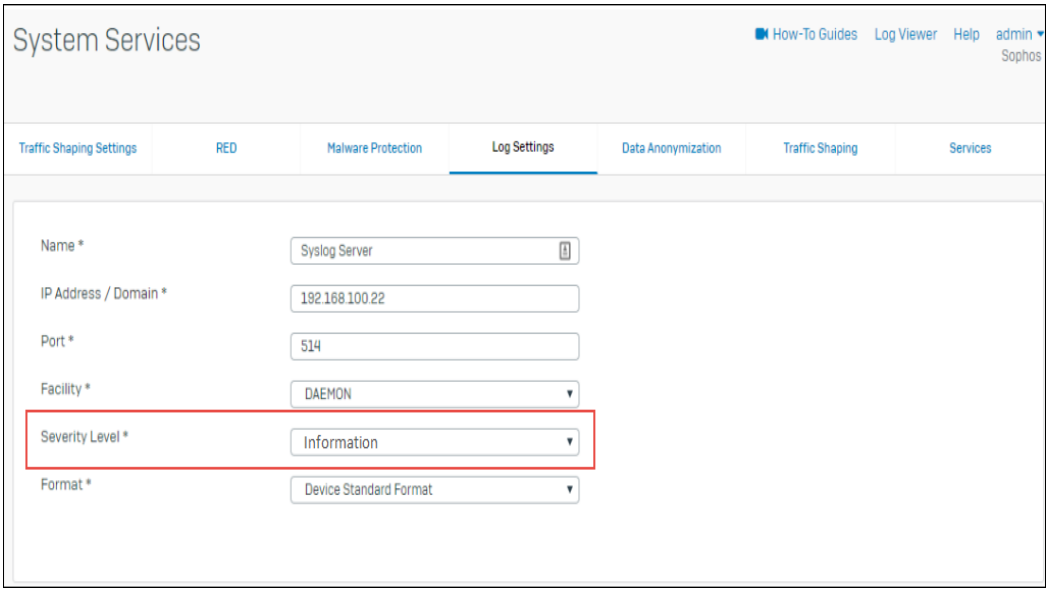
Once syslog targets have been configured, the logs to be send via syslog must also be selected on the same screen. By default, none is selected. Select the desired logs and click **Apply**.



To determine which logs are desired, you can view complete log contents and watch logs in real-time, under **Logging & Reporting > View Log Files**.

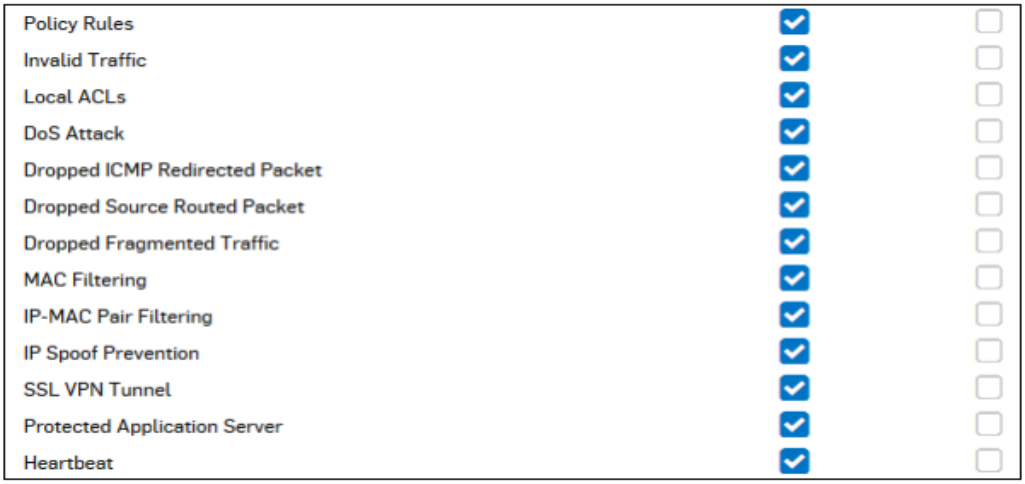
3.2 Enabling syslog forwarding in Sophos XG firewall

1. Navigate to **System** > **System Services** > **Log Settings** and click **Add** under the **Syslog Servers** section.
2. Enter server details.
   - **Name**
     - Enter a unique name for the syslog server.
   - **IP Address / Domain**
     - Enter the **EventTracker Manager IP Address/EventTracker syslog relay IP**.
   - **Port**
     - Enter Port number **514**, **UDP** protocol.
   - **Facility**
     - Select syslog facility for logs to be sent to the syslog server. Facility indicates to the syslog server the source of a log such as operating system, the process, or an application. It is defined by the syslog protocol. The device supports several syslog facilities for received log.
     - In the **Severity** field, select **Information** from the dropdown options.

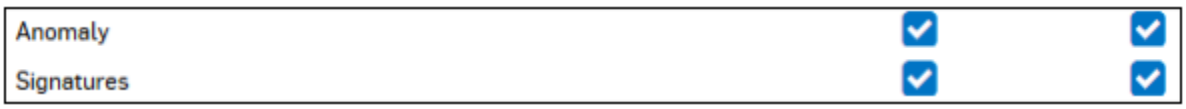


Note: You can configure maximum five syslog servers.

3. Click **Save**.
   - Once you add the server, go to the **System** > **System Services** > **Log Settings** page and enable all those logs, which are to be sent to the syslog server in the section Log Settings.



IPS



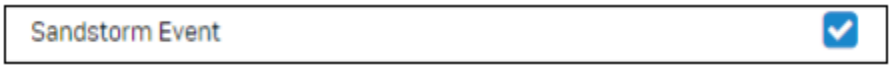
Anti-Virus

Anti-Spam

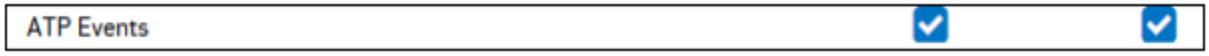
Content Filtering

Events

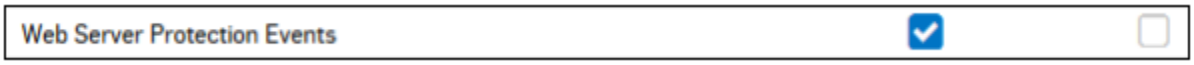
Sandbox



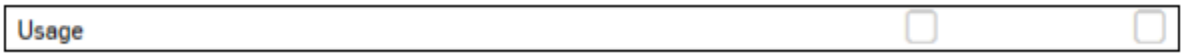
ATP



Web Server Protection



System Health



3.3 Monitoring Systems and User Behavior

- User behavior and activity analysis
- Event correlation
- 400-day searchable log retention
- Monitor file and app changes
- Threat dashboard

3.4 Detecting Cyber Attacks Instantly

- Removable media inserts and file copying
- Group security policy changes
- Abnormal network or system activity
- Abnormal user activity or remote access
- Application installs.

Target Audience	Example	Core Product(s)	Key Messages	Reach/Influence/Media
IT MSP	CMIT	SIEMphonic Essentials Connect SD-WAN	Endpoint security Compliance Secure Connectivity	ConnectWise IT Nation Kaseya Connect Continuum Navigate
Network MSP Secure the edge; secure connectivity	Masergy Triton	Connect SD-WAN SIEMphonic Essentials	Above, plus: Edge Management Bundling	Informa properties Channel Partners Online Tier 1 Master Agent events PlanetOne, Telarus, Avant, Intelisys
Telco Master Agents	Telarus	Connect SD-WAN SIEMphonic Essentials	Above, plus: Ease of deployment	Same as above

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

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