SOPHOS
Security made simple.

Pocket Guide

Restrict Access from Sophos Endpoints with Yellow-Red Security Heartbeat

Product: Sophos XG Firewall

Contents

Overview

This document describes how to configure XG Firewall to automatically block access to sensitive sites from Sophos Endpoints with yellow or red Security Heartbeat.

Endpoints with Sophos Central Endpoint Advanced (CEA) protection with Intercept X (CIX) installed on them send Security Heartbeat to XG Firewall through Sophos Central, providing visibility into their health status and identity information.

On the XG Firewall dashboard, the Sophos Security Heartbeat widget indicates the health status of Sophos Endpoints:

- **Green:** Endpoint is healthy.
- **Yellow:** Potentially unwanted application (PUA) was detected, or inactive malware was found on the endpoint.
- **Red:** Active malware or ransomware was found on the endpoint and one or more Sophos Endpoint Services are not running or are missing.
- **Missing Heartbeat:** Endpoint is no longer sending Heartbeat, but XG Firewall still receives traffic from the endpoint.

For detailed Heartbeat reports, go to **Monitor & Analyze > Reports > Network & Threats**, and select **Security Heartbeat** from the **Show** list.

Prerequisites

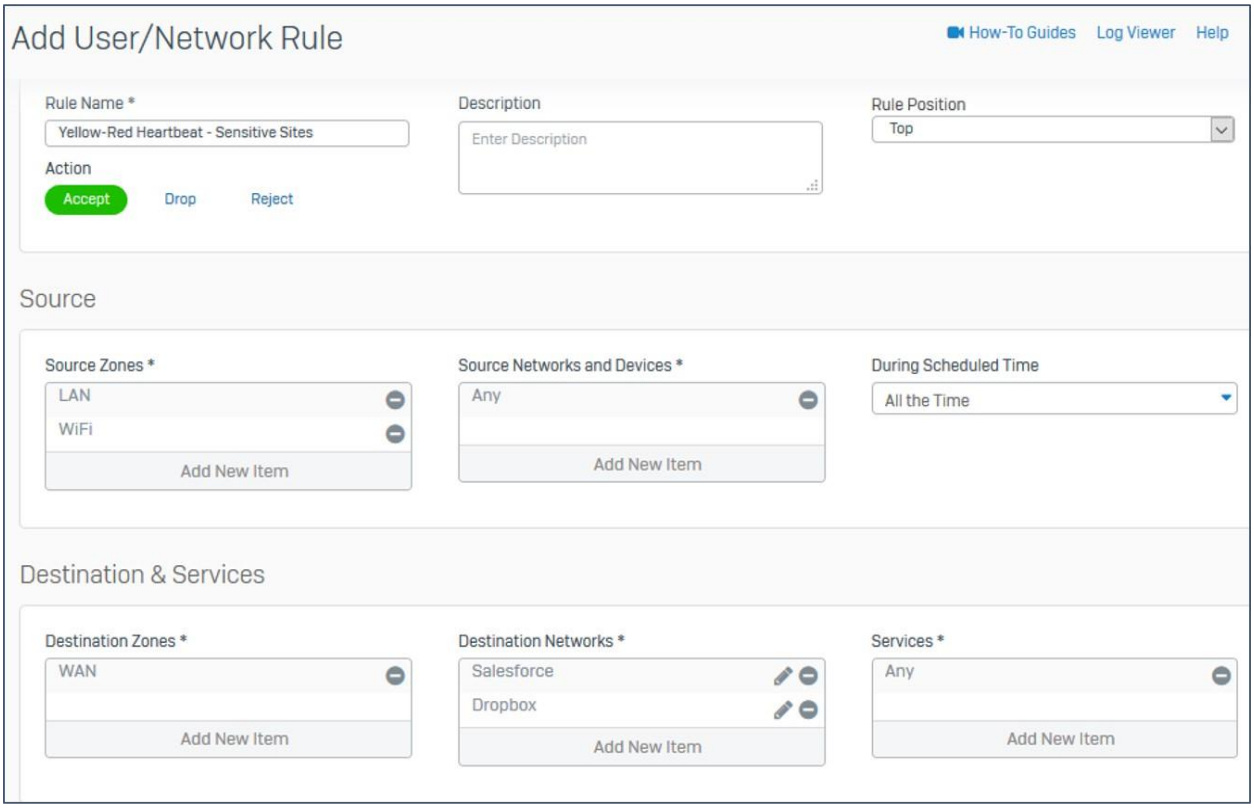
- You must have read-write permissions on the SFOS Admin Console for the relevant features.
- You must have access to Sophos Central Admin Console.
- You must install the following on endpoint computers whose Security Heartbeat you wish to monitor:
  - Sophos Central Endpoint Advanced (CEA)
  - Intercept X (CIX)
- To enable Security Heartbeat, you require Sophos Endpoint Advanced and Intercept X of version 11.x.
- You must enable Security Heartbeat on XG Firewall (**Protect > Synchronized Security**).
- XG Firewall must receive a valid Heartbeat from Sophos Endpoints.

Configuration

Create firewall rule to restrict access from Sophos Endpoints with yellow or red security Heartbeat

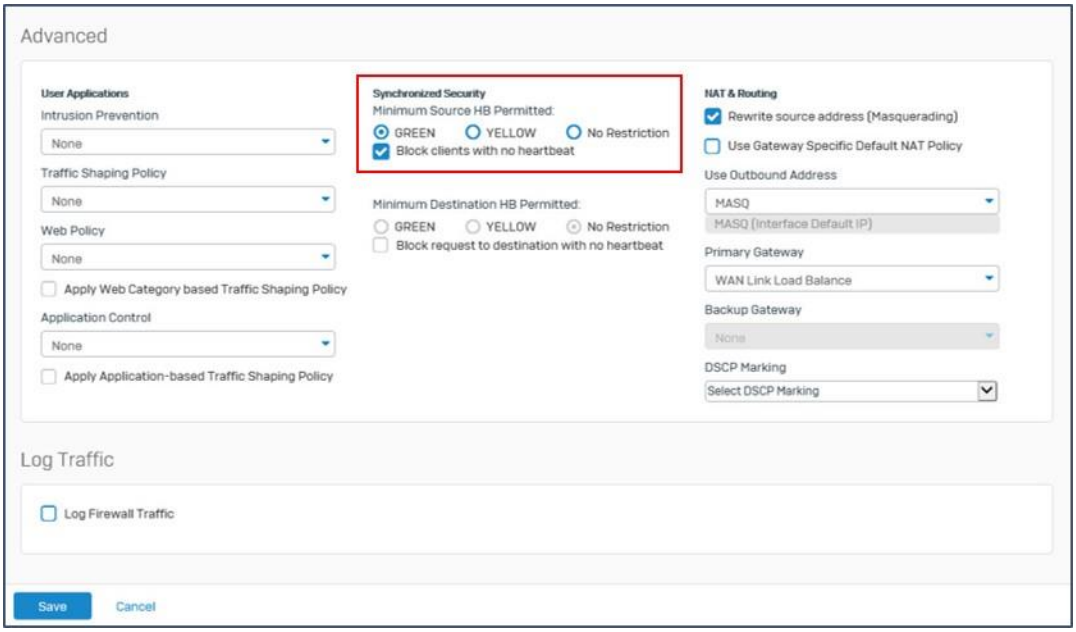
- Go to Protect > Firewall. **Click Add Firewall Rule** and click **User/Network Rule**.
- Create a Source Security Heartbeat rule.
- Set **Action** to Accept.
- Set **Rule Position** to Top.
- Set **Source Zones** to LAN, Wi-Fi and **Destination Zones** to WAN.
- For **Destination Networks**, select from **FQDN Host Groups**. If the site which you wish to block is not available in the default list, you can create the FQDN host (**System > Hosts and Services > FQDN Host**).

Note: To block access to specific sub-domains, you can create a URL Group and Web Policy.

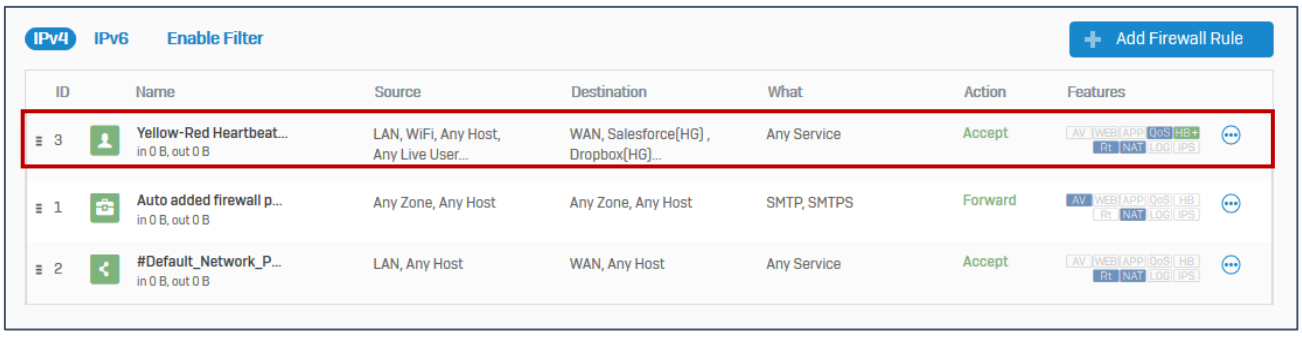


- Set **Minimum Security HB Permitted** to Green. Endpoints with yellow or red Heartbeats will not be able to access the sites listed in the FQDN Host Group. Only endpoints with green Heartbeats will be allowed to access these sites.

Note: You can select **Block Clients with no heartbeat** to block endpoints which are generating traffic, but have stopped sending Heartbeat to XG Firewall.



You have configured Security Heartbeat in XG Firewall.



Result

You have created a firewall rule to block access to sensitive sites from Sophos Endpoints with yellow or red Heartbeats.

Copyright Notice