SOPHOS
Security made simple.

Pocket Guide

Synchronized Security in Bridge Mode

Product: Sophos XG Firewall

Contents

Overview

This document describes how to deploy Sophos XG Firewall in Bridge mode, and install Sophos Central Endpoint Advanced protection (CEA) with Intercept X (CIX) on endpoint computers to gain synchronized security and network visibility on the Admin Console of XG Firewall:

- **Security Heartbeat** provides visibility into the health status and identity information of Sophos Endpoints based on the Security Heartbeat sent by them to XG Firewall. Bringing anti-exploit zero-day defense, anti-ransomware CryptoGuard technology and root cause analysis through signature-less technologies on top of traditional endpoint security, Intercept X with Sophos Endpoint Advanced protection scans Sophos Endpoints for threats and vulnerabilities, based on which it sends Security Heartbeat.

- **Synchronized Application Control** provides visibility into all previously unknown applications, which are identified and automatically categorized by Sophos Synchronized Security based on users, hosts, and destination countries. This consists of application information from Sophos Endpoints for traffic that does not match current application control signatures or which is using generic HTTP or HTTPS connections.

Prerequisites

- You must have read-write permissions on the SFOS Admin Console and Command Line Interface for the relevant features.
- Choose the endpoint computers on which you wish to install the following:
  - Sophos Endpoint Advanced (CEA)
  - Intercept X (CIX)
- Set IPS Max Packets to the default 8 packets. (CLI command: **set ips maxpkts default**)
- XG Firewall must be able to reach all Sophos Endpoints.

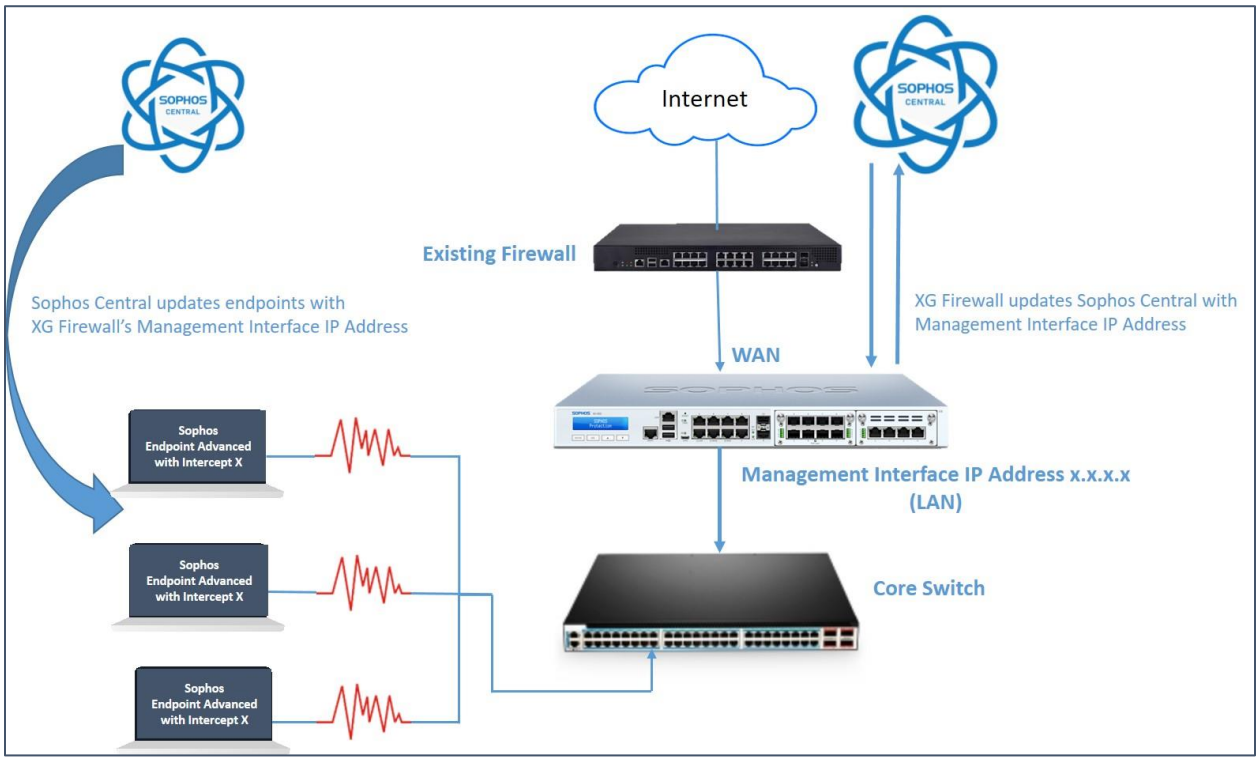
Note:

- SAC works only in active-passive high availability mode. It does not support active-active mode.
- The bridge interface of XG Firewall cannot support multicast routing, IPsec VPN, VLAN and PPPoE.
- In Bridge mode, XG Firewall cannot support dynamic DNS, DHCP client functions.

Network Diagram

In Bridge mode, XG Firewall can act as a Layer 2 bridge (Transparent mode) or Layer 3 bridge (NAT/Route mode). The device works in-line with any existing firewall, and performs deep packet inspection, IPS, malware scanning, and email content scanning without displacing or disrupting existing IT security infrastructure.

You can use Bridge mode when you wish to enhance network protection without changing the network configuration.



Deploy Synchronized Security

Step 1: Deploy XG Firewall

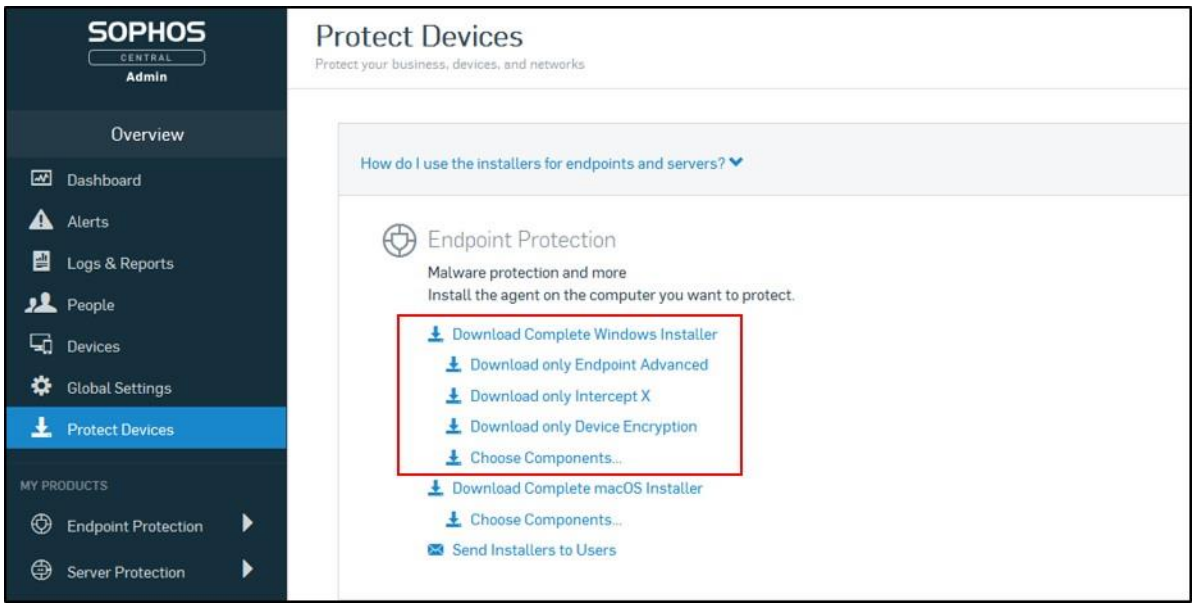
For details of how to deploy XG Firewall in Bridge mode, click Deploy in Pure Bridge Mode.

Note:

- You require subscription to Network Protection and Web Protection modules for the analysis of IPS, Web Filter and Application Filter policies. Trial version gives you access to these modules.
- You can create custom categories for Web and Application Filter to receive reports specific to your network.

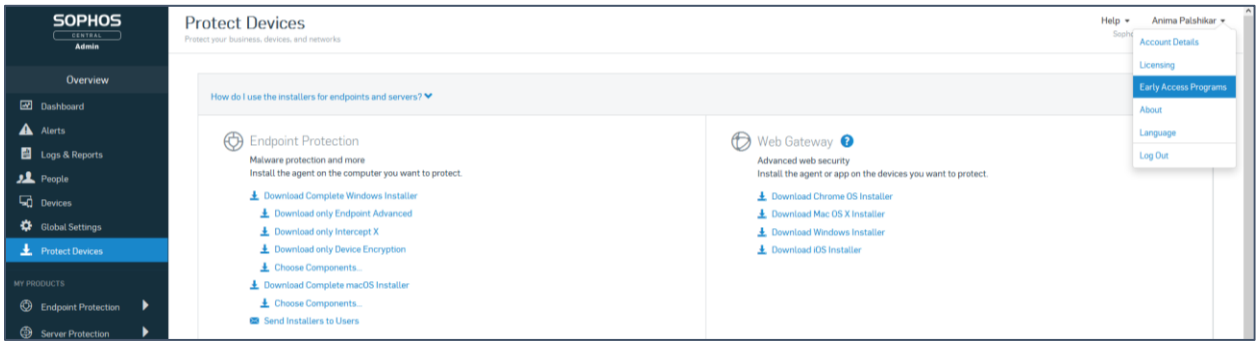
Step 2: Install CEA and CIX

- Log in to your Sophos Central account (https://central.sophos.com). If you do not have one, take a 30-day trial of Sophos Central. It will give you access to the trial version of all modules available from Sophos Central.
- On the left menu, click **Protect Devices**.
- Click **Download Complete Windows Installer** or click **Choose Components** and select **Endpoint Advanced** and **Intercept X**. Click **Download Installer** and save the file.

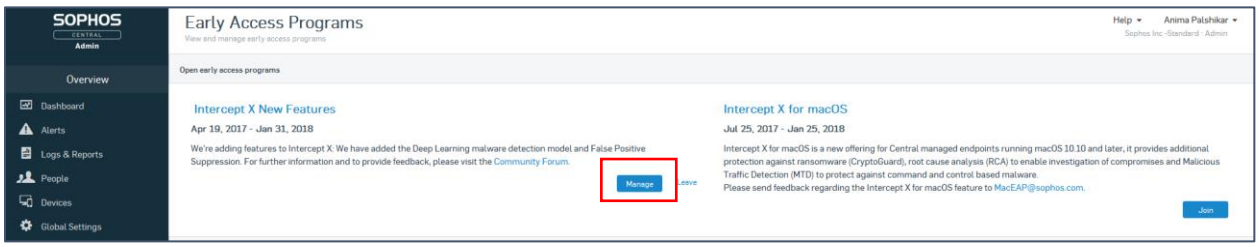


Note:

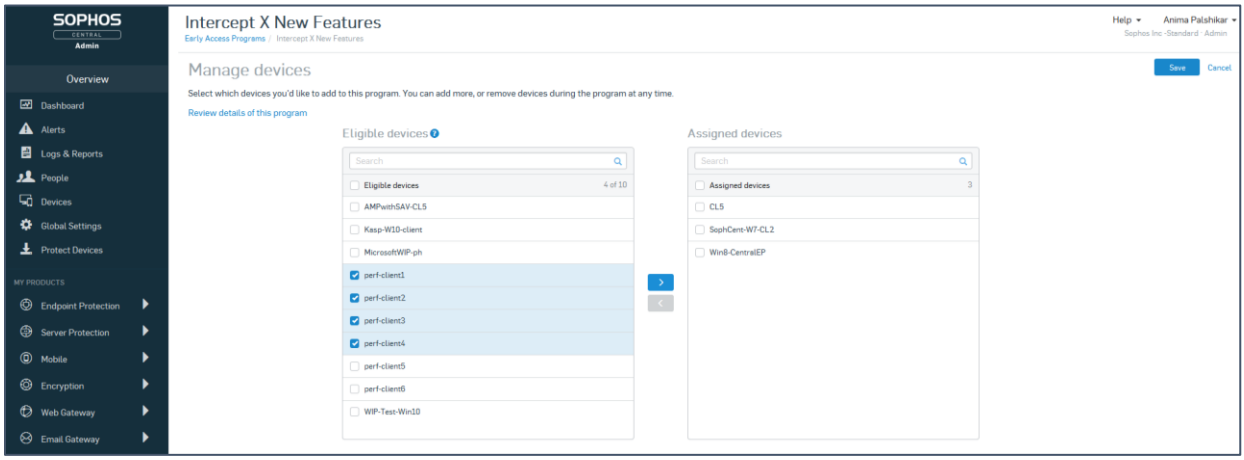
- Installing Sophos CEA protection will uninstall your current anti-virus.
- To enable Security Heartbeat and Synchronized Application Control, you require Sophos CEA and CIX of version 11.x.
- Go to the upper-right corner, click the tab next to your name. Click **Early Access Programs**.



- Under **Intercept X New Features**, click **Manage**.



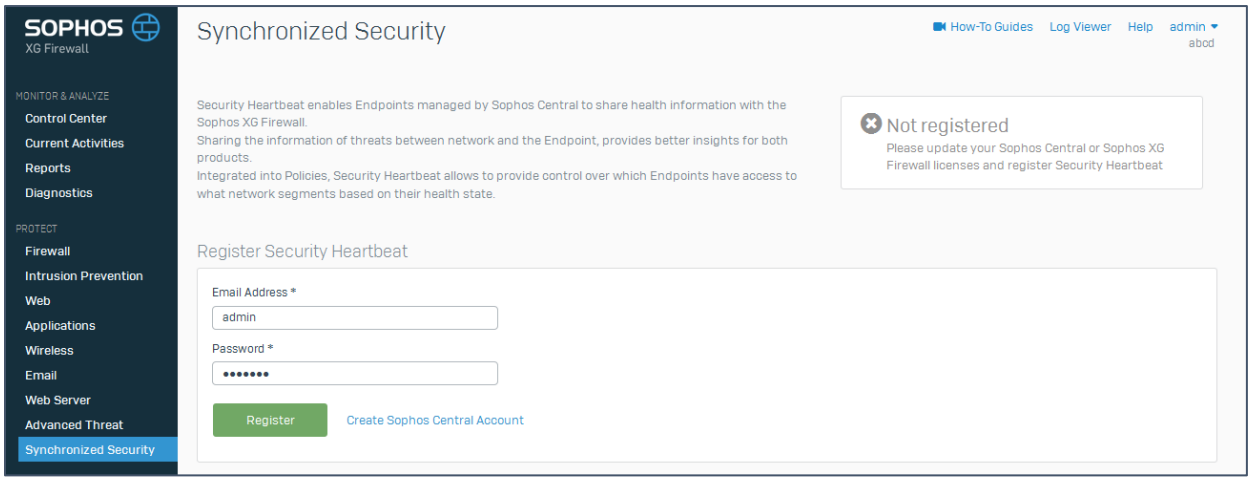
- Under **Eligible devices**, select the endpoint computers and add them to **Assigned devices**.
- On the upper-right corner, click **Save**.



Result: You have installed Sophos Endpoint Advanced and Intercept X on the **Assigned devices**.

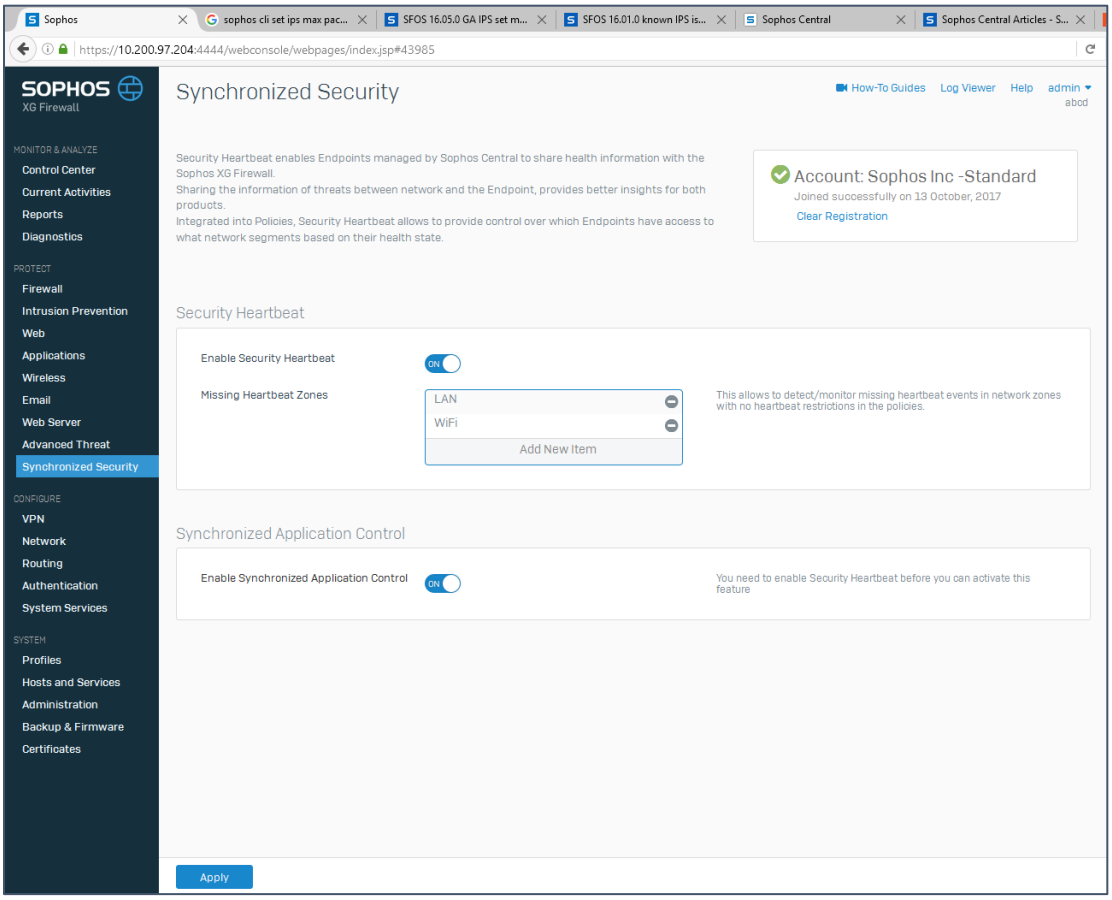
Step 3: Connect XG Firewall to Sophos Central and Enable Security Heartbeat

- Log in to the Admin Console of XG Firewall. Go to **Protect > Synchronized Security** and enter the Sophos Central admin credentials to register the XG Firewall with Sophos Central.



- Turn on **Enable Security Heartbeat**.
- For **Missing Heartbeat Zones**, select the zones in which you wish to monitor the endpoint Heartbeats.
- Turn on **Enable Synchronized Application Control**.

- Click **Apply**.



Result

- XG Firewall device will become visible in Sophos Central.
- XG Firewall will update its LAN management interface IP address on all the endpoints in the heartbeat.xml file via Sophos Central.
- Once the endpoint receives this updated information, it will initiate Security Heartbeat with the management interface of XG Firewall.
- The following health status will appear on the XG Firewall dashboard:
    - **Green:** Endpoint is healthy.
    - **Yellow:** A 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.

Note: Additionally, Sophos Central dashboard displays the endpoint health status.

- XG Firewall also identifies network intrusions, web and application usage by users and hosts, and automatically categorizes the information.

What you can Monitor and control in Bridge Mode

A. Create Synchronized Security Policies

You can configure the following synchronized security policies from XG Firewall based on Security Heartbeat and synchronized applications:

- Restrict Access from Sophos Endpoints with Yellow Security Heartbeat
- Customize Category of Synchronized Applications Captured by Sophos Endpoints

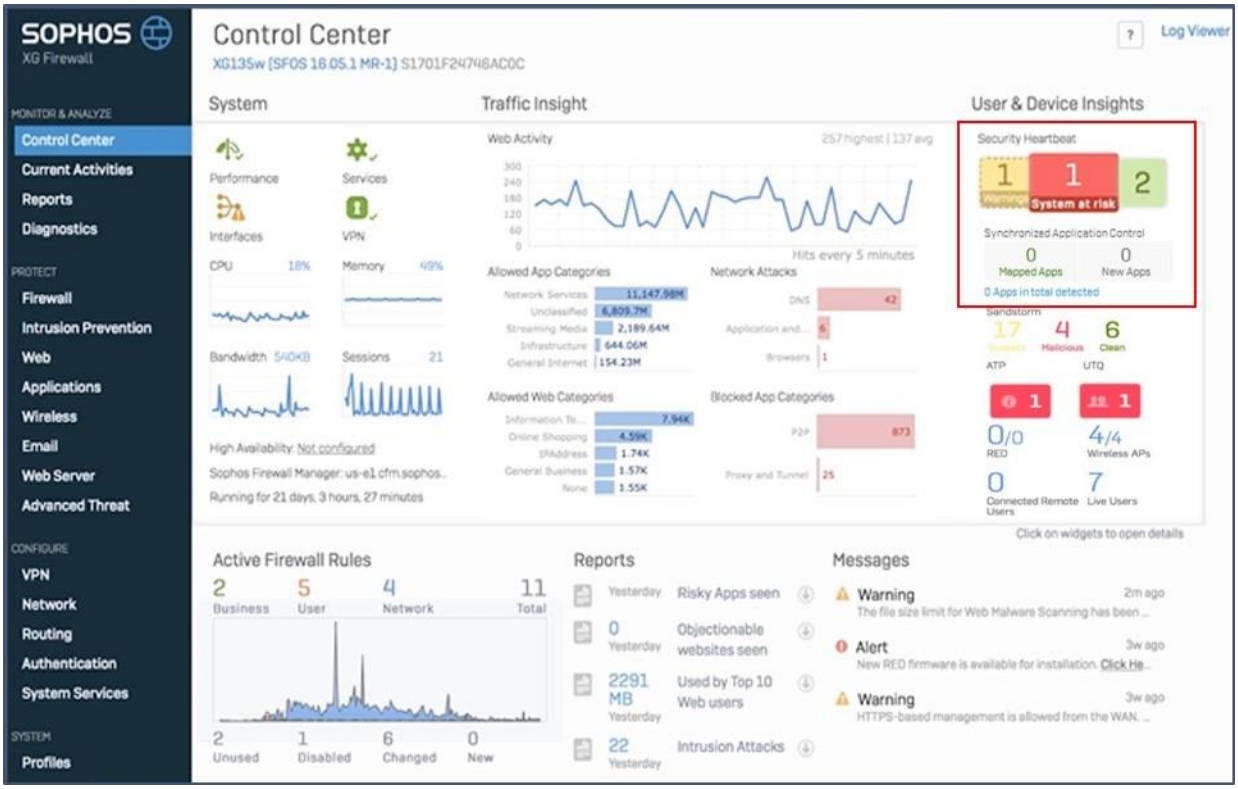
B. View Synchronized Security Reports

You can view synchronized security reports on XG Firewall:

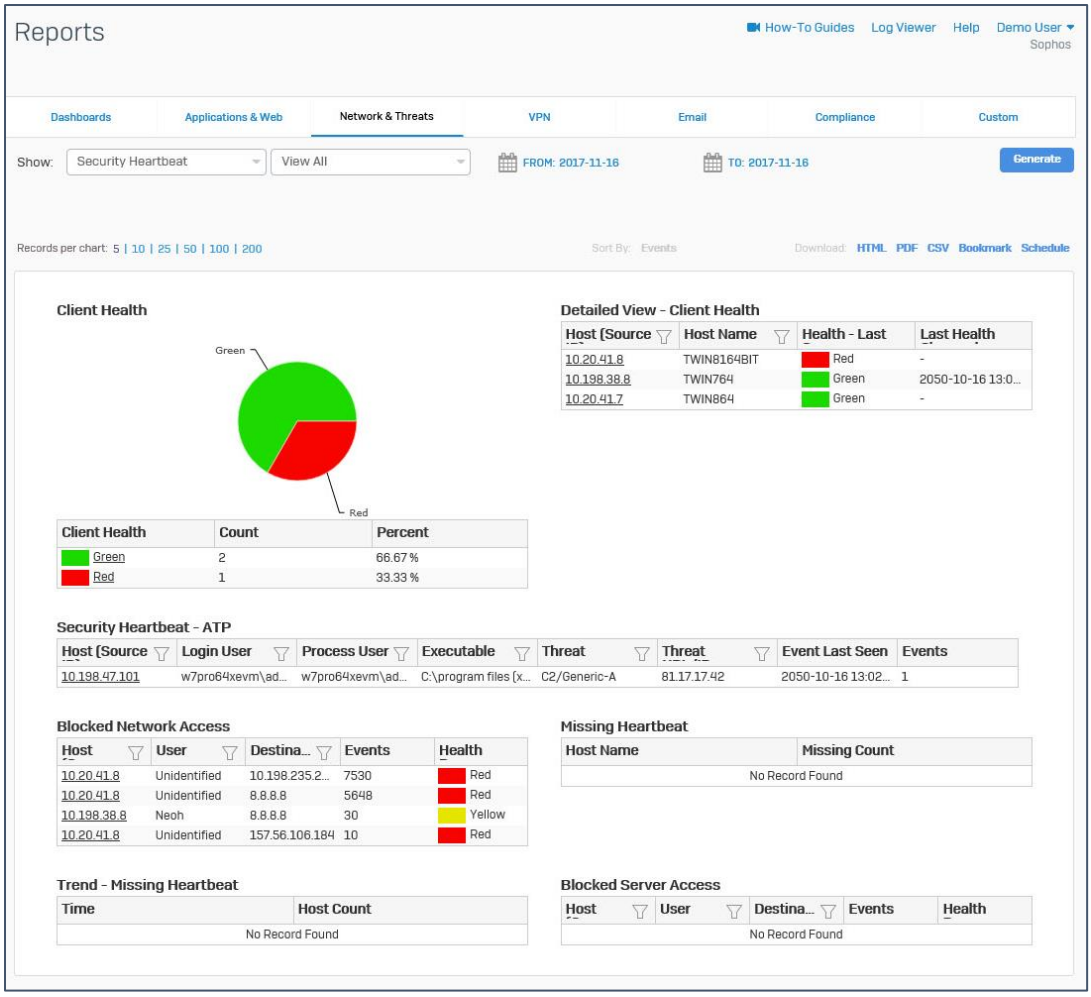
- Security Heartbeat
- Synchronized Applications

Security Heartbeat

On the XG Firewall dashboard (**Monitor & Analyze > Control Center**), the Sophos Security Heartbeat widget displays the health status of all your Sophos Central-managed endpoints.


SOPHOS
XG Firewall
Control Center
XG135w (SFOS 16.05.1 MR-1) S1701F24746AC0C
Log Viewer
MONITOR & ANALYZE
Control Center
Current Activities
Reports
Diagnostics
PROTECT
Firewall
Intrusion Prevention
Web
Applications
Wireless
Email
Web Server
Advanced Threat
CONFIGURE
VPN
Network
Routing
Authentication
System Services
SYSTEM
Profiles
System
Performance
Services
Interfaces
VPN
CPU 18%
Memory 49%
Bandwidth 540KB
Sessions 21
High Availability: Not configured
Sophos Firewall Manager: us-e1.cfm.sophos...
Running for 21 days, 3 hours, 27 minutes
Traffic Insight
Web Activity
257 highest | 137 avg
Hits every 5 minutes
Allowed App Categories
Network Attacks
Allowed Web Categories
Blocked App Categories
User & Device Insights
Security Heartbeat
System at risk
Synchronized Application Control
Mapped Apps
New Apps
0 Apps in total detected
Sandstorm
ATP
UTQ
RED
Wireless APs
Connected Remote Users
Live Users
Click on widgets to open details
Active Firewall Rules
Business
User
Network
Total
Unused
Disabled
Changed
New
Reports
Risky Apps seen
Objectionable websites seen
Used by Top 10 Web users
Intrusion Attacks
Messages
Warning
Alert
Warning

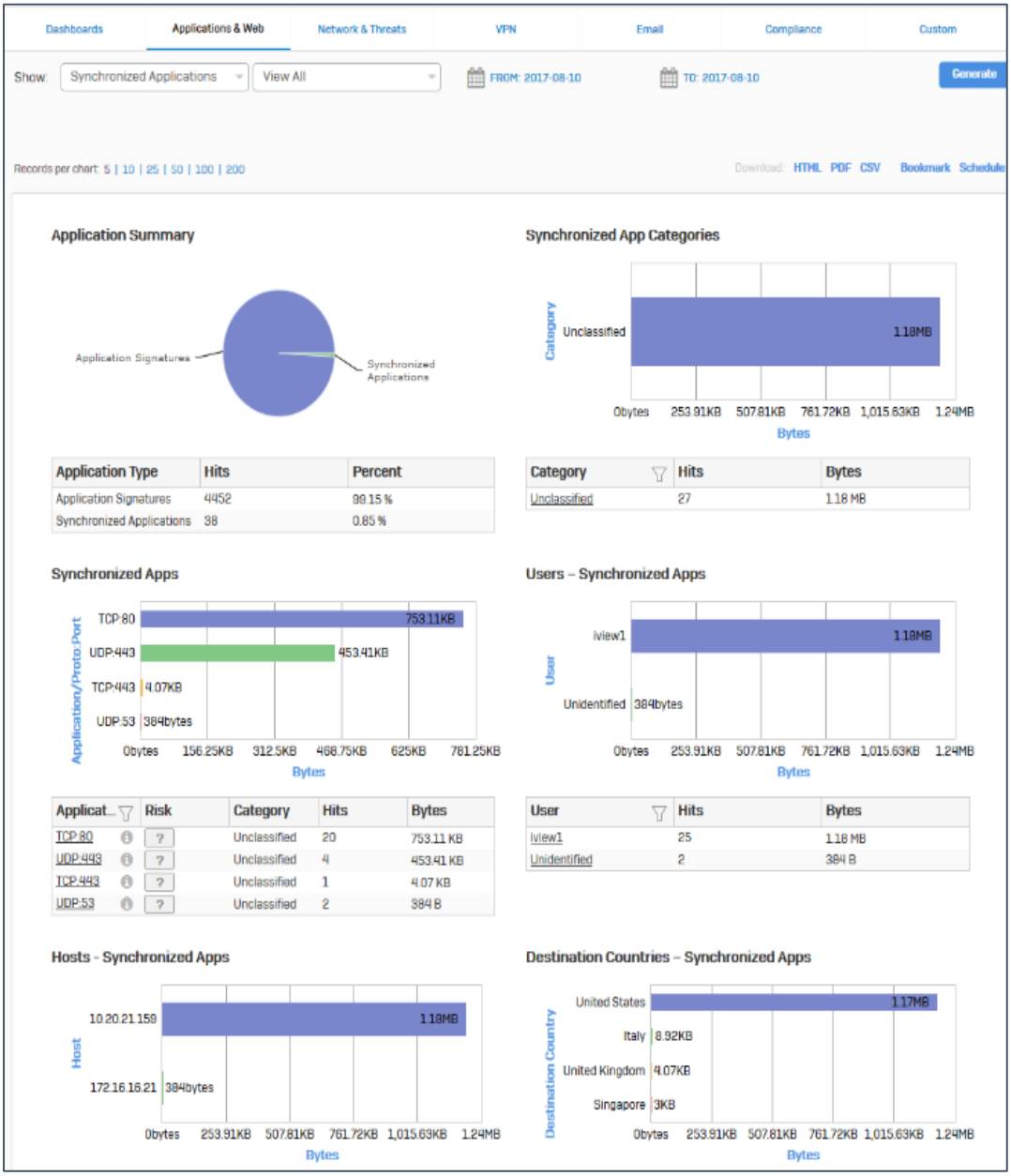
Dashboard



Security Heartbeat

Synchronized Applications

Synchronized Applications reports offer complete historical reporting of all applications, which are identified by Sophos Endpoints. These applications appear based on users, hosts, destination countries.



Synchronized Applications

Suggested Reading

Synchronized Security in Discover (TAP) Mode

Copyright Notice