

Tips and Tricks for XG firewall



Per Söderqvist

Team Leader – Sales Engineer Nordics

Top Performing Protection – New XG Series Appliances



Performance

Increase in throughput across the board to add to our already outstanding price-per-protected Mbps



High Availability

Redundant power supplies across the entire line



Connectivity

Great WiFi, LTE, and DSL Modules as well as huge selection of PoE, copper, and fiber Flexi Ports modules and bypass ports



Management

Manage via micro USB or COM
Connect monitor via HDMI



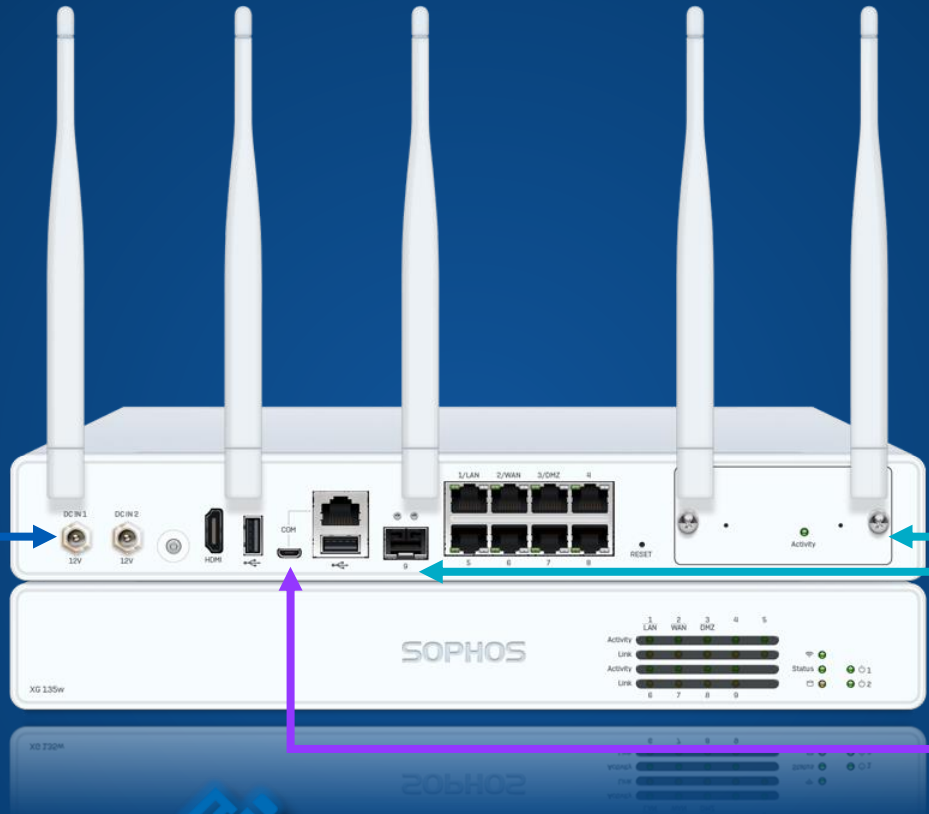
New SG/XG Desktop Units – Highlights



High Availability
Redundant power supply option*



Performance
Increase in throughput
New Apollo Lake/Denverton CPUs
Built-in high-speed Wi-Fi



Connectivity
802.11ac Wi-Fi for every w model
Add 3G/4G module or 2nd radio*
Connect DSL Modem via SFP*



Management
Manage via micro USB or COM
Connect monitor via HDMI



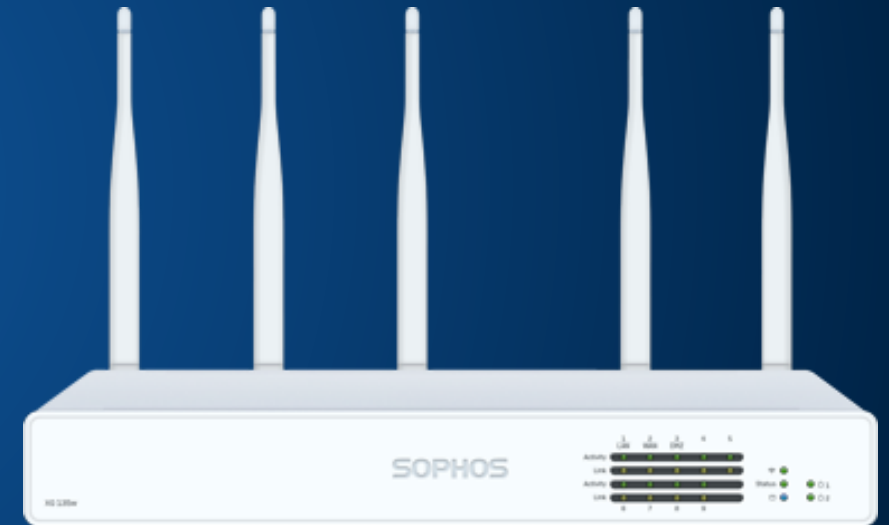
New XG Brand Experience
Modern hardware design
Great unboxing experience
QR code direct to setup

Image shows XG model – SG has a different design
*Not all features are available on every model

Many Ways To Add Value to Your Desktop Deals

XG 135w – with integrated Wi-Fi

1. Add optional 3G/4G module
 - ✓ Connectivity failover
 - ✓ Better coverage in all areas
2. Add redundant power
 - ✓ Power failover
3. Add further access points if better Wi-Fi coverage and performance needed
4. Add rackmount kit
 - ✓ Put it in the datacenter along with other equipment



Three Options for Enabling Sync Security in Any Environment

Firewall
Replacement



Security Heartbeat™ &
Synchronized App Control



Inline



Security Heartbeat™ &
Synchronized App Control



Discover
Mode



Security Heartbeat™ &
Synchronized App Control



Three Options for Enabling Sync Security in Any Environment

Firewall Replacement



Inline



Discover Mode



SOPHOS
Security made simple.

Adding Sophos Synchronized Security to Your Network

For Unrivalled Insight and Protection
Easily add Synchronized Security to gain deeper insights into what's happening on your network and automatically identify and respond to threats.

Highlights

- Bring rich network visibility to your network
- Unlock the full potential of your Sophos Endpoints
- Discover Mode makes it easy with no disruption
- Inline deployment gives you automatic response with zero risk

Unlock the full potential of your Sophos Endpoints

If you already have or are considering Sophos Central managed Endpoint Protection like Central Endpoint Advanced or Intercept X, Synchronized Security enables a whole new level of visibility and protection. Utilize our unique Security Heartbeat™ to get instant insights into endpoint health status, with the option to automatically respond to security incidents by isolating infected systems until they can be cleaned up. Or take advantage of the rich insights and control that Synchronized Application Control provides by identifying hundreds of applications that are currently going undetected on your network. A Synchronized Security Appliance unlocks the full potential of your Sophos Endpoints without disrupting your existing network.

Expose hidden risks

Sophos Synchronized Security provides unprecedented visibility into top risk users, unknown apps, advanced threats, suspicious payloads, and much more. Traffic light-style indicators on the Control Center instantly identify what needs your attention on the most, and rich on-box reporting provides deep forensic and analytics capabilities into users, threats, applications, web usage, and other activity on your network.

Automatically respond to incidents

Synchronized Security can instantly identify the source of an infection on your network and automatically limit access to important network resources in response. This is made possible with the Security Heartbeat™, sharing telemetry and health status between Sophos Endpoints and the Synchronized Security Appliance to provide a coordinated response.

Synchronized Security made simple

Synchronized Security has been designed to fit your network, any way you want. We make it easy to add deeper insights and visibility to your existing network protection without any risk or disruption to your network. Our appliance can be deployed either in Discover Mode (also known as TAP mode) by simply connecting it to your network switch, or it can be deployed inline with your firewall using our always-on bypass ports to provide rich visibility and added control.

Get the Synchronized Security Deployment Datasheet

SG to XG Migration Assistant

Now Available as a VM for you to offer Migration Services



CATEGORY	SUB-CATEGORY	WHAT'S MIGRATED
Definitions & Users	Network Definitions	Hosts, Group, Network, Range, MAC Address Definitions
	Service Definitions	TCP, UDP, TCP/UDP, ICMP, ICMPv6, IP, Group
	Time Period Definitions	Time Period Definitions
	Authentication Services	Authentication Servers, STAS
Interfaces & Routing	Interfaces	Ethernet, Alias, VLAN, PPPoE
	Static Routing	Static Routes, Policy Routes [Interface Route, Gateway Route]
Network Services	DNS	Request Routing, Forwarders, DyDNS
	DHCP	IPv4 - Relay, Servers, Options
Network Protection	Firewall	Basic Network Firewall Rules
Site-to-site VPN	IPsec	Connections, Policies
	Certificate Management	Certificate Management
Remote Access	PPTP	Global settings
	L2TP over IPsec	Global settings
	IPsec	Connections, Policies
Management	System Settings	Hostname, Time and Date





XG Firewall v17.5 Key Pillars



Threat Protection

Lateral Movement Protection

Automatic isolation at every point in your network

Sandstorm Sandboxing

Now the best protection from zero-day threats with the best technology from Intercept X

IPS Enhancements

Talos Signature integration



Central Management

Sophos Central Management

XG Firewall Joins Sophos Central

Wireless

Cloud Managed or On-premise firewall controller

Education Vertical

Flexible User-Based Policy Tools

Chromebook support, classroom policy overrides and new user-based policy options



Networking

APX Wireless Access Points

WAVE 2 Performance:

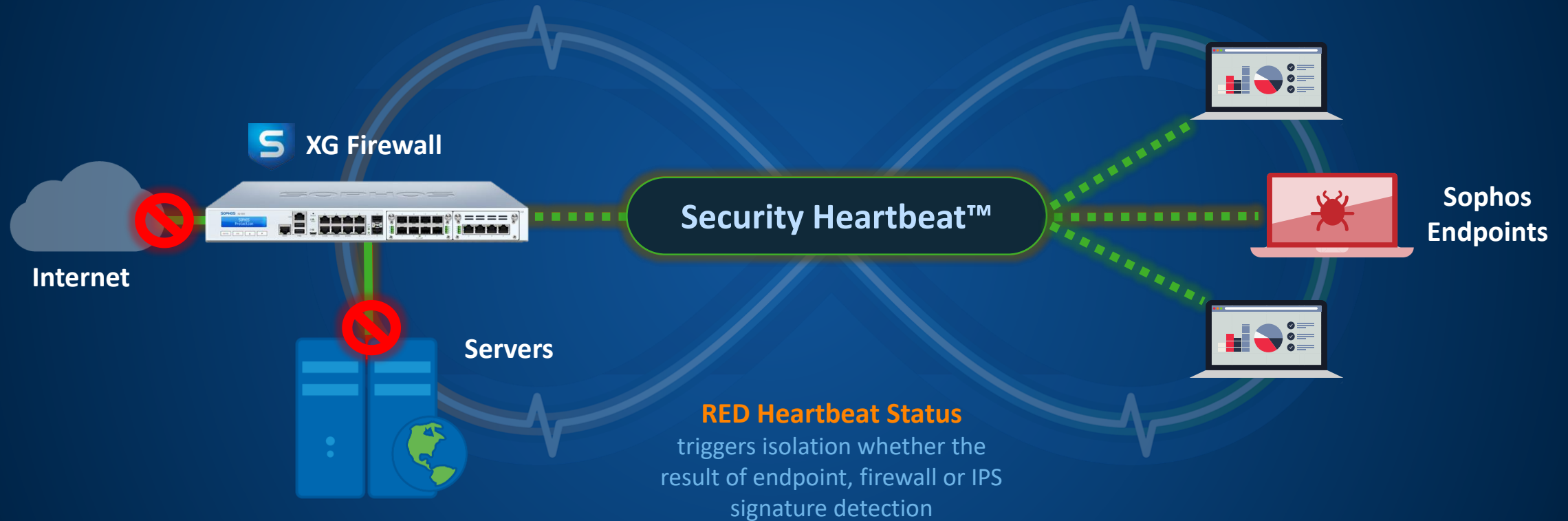
Faster connectivity, higher capacity and optimal performance

IPSec Client

New IPSec Client for easy end-user VPN

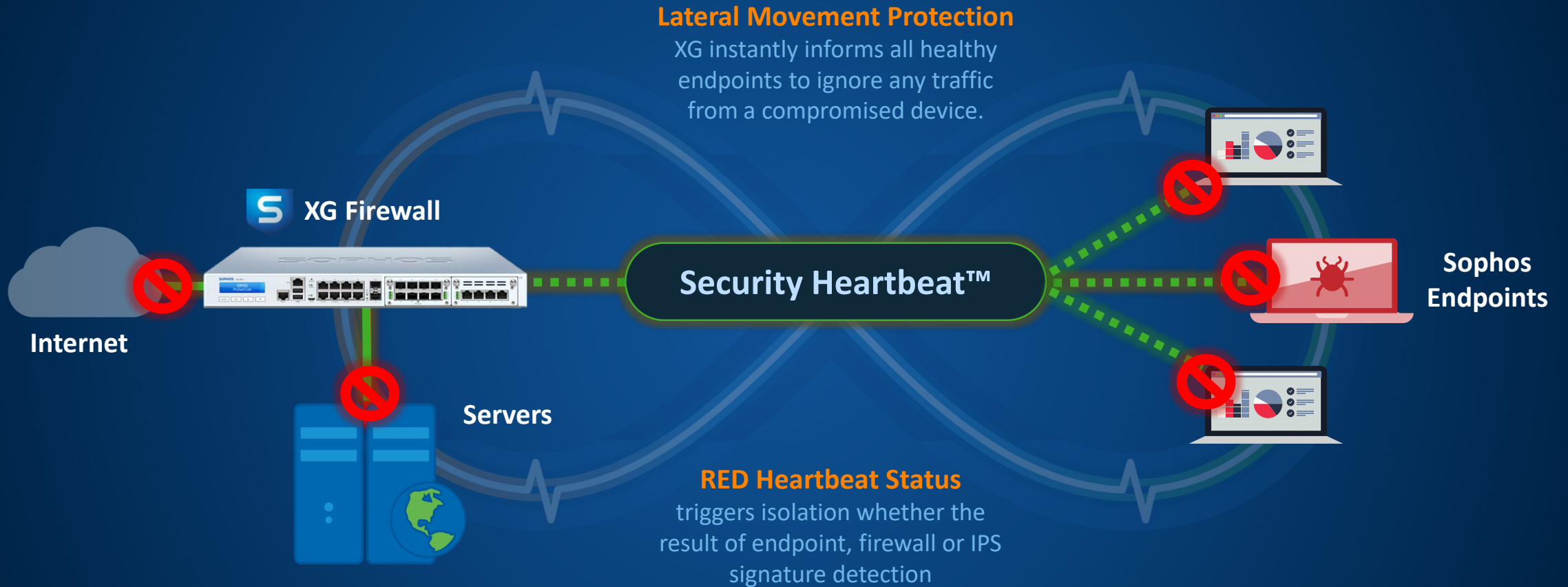
Endpoint Isolation & Security Heartbeat

Automatic system isolation at the firewall



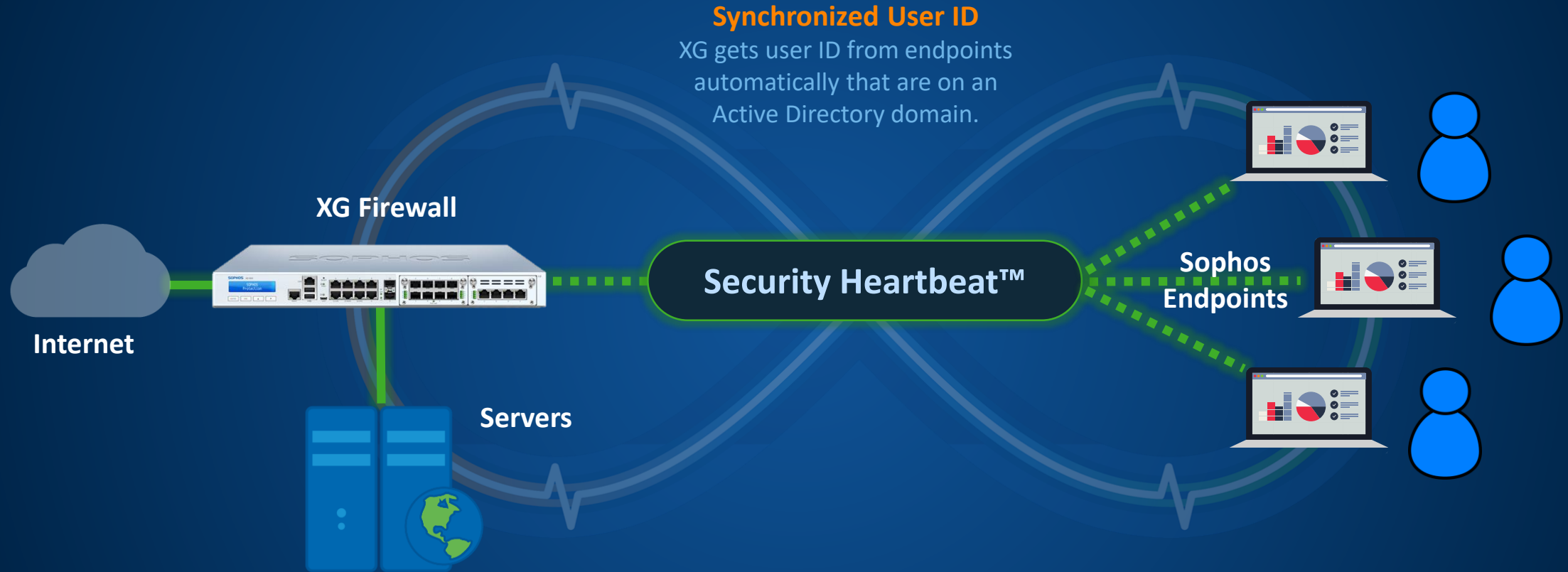
Lateral Movement Protection

Automatic system isolation at the endpoint - even on the same broadcast domain



Synchronized User ID

Eliminates the need for an authentication agent



Full Network User Identification – Without AD Integration

IPS Enhancements

Enterprise pattern integration

What's New

- Bolstered our IPS patterns with Enterprise categories
- Deeper, broader, granular coverage
- 60 Categories (up from 21)
- Increased granularity in policies

SOPHOS
XG Firewall

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion prevention**
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced threat
- Central Synchronization

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Profiles

Intrusion prevention

DoS attacks | **IPS policies** | Custom IPS si

Category: browser | Severity: | Platform: | Target: | Individual signature

SID	Category	Severity	Platform
2200304	Server-Webapp	2 - Major	Windows
9000495	Os-Windows	4 - Minor	Windows
9000496	Os-Windows	1 - Critical	Windows
1000070	Policy-Other	4 - Minor	

List of matching signatures [1 - 50 of 11206]

Action: Drop packet

Sandstorm Deep Threat Prevention

The best protection from zero day threats

Deep Memory Analysis

01010000101001010011
10011010010000001010
01010010010010010100

Initial & Post
Execution Memory
Inspection &
Analysis

Frequent &
Aggressive Run-Time
Analysis

Deep Behavioural Analysis



Sandbox Evasion
Techniques,
API & File System
Behavior

Intercept X Exploit
Detection &
CryptoGuard

Deep Network Analysis



Full port and
protocol analysis

IPS detections
coming soon

Deep Learning Analysis



Analysis of all
dropped
executables

Continuously
adaptive learning
model


Real-time Threat Intelligence from Sophos Labs



Sandstorm prevention goes beyond endpoint or firewall

JavaScript CryptoJacking Protection

One-Click Protection



SOPHOS
XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web**
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat
- Synchronized Security

CONFIGURE

- VPN
- Network
- Routing
- Authentication

Web

[Policies](#)[User Activities](#)[Categories](#)[URL Groups](#)[Exceptions](#)[General Settings](#)[File Types](#)[Surfing Quotas](#)[User Notifications](#)[Content Filters](#)

XG Firewall protects you by scanning HTTP and HTTPS traffic for unwanted content or malware, and enforcing SafeSearch restrictions. Use this page to modify protection settings, as well as settings for the proxy and web cache.

Protection

Malware and Content Scanning

Scan Engine Selection

Single Engine (Optimal Performance)

Single scan engine is set to [Sophos](#).

Sandstorm and content filters require use of the Sophos engine, either as the single scan engine or in Dual Engine mode.

Scanning Mode

Batch (Maximum Protection)

Real-time mode improves performance by allowing parts of a file to be downloaded before the scan is complete.

Action on Malware Scan Failure

Block (Best Protection)

Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats.

Do not scan files larger than

10 MB

Authorized PUAs

Search / Add

Advanced Settings

[How-To Guides](#)[Log Viewer](#)[Help](#)[Demo User](#)
Sophos Inc

Networking

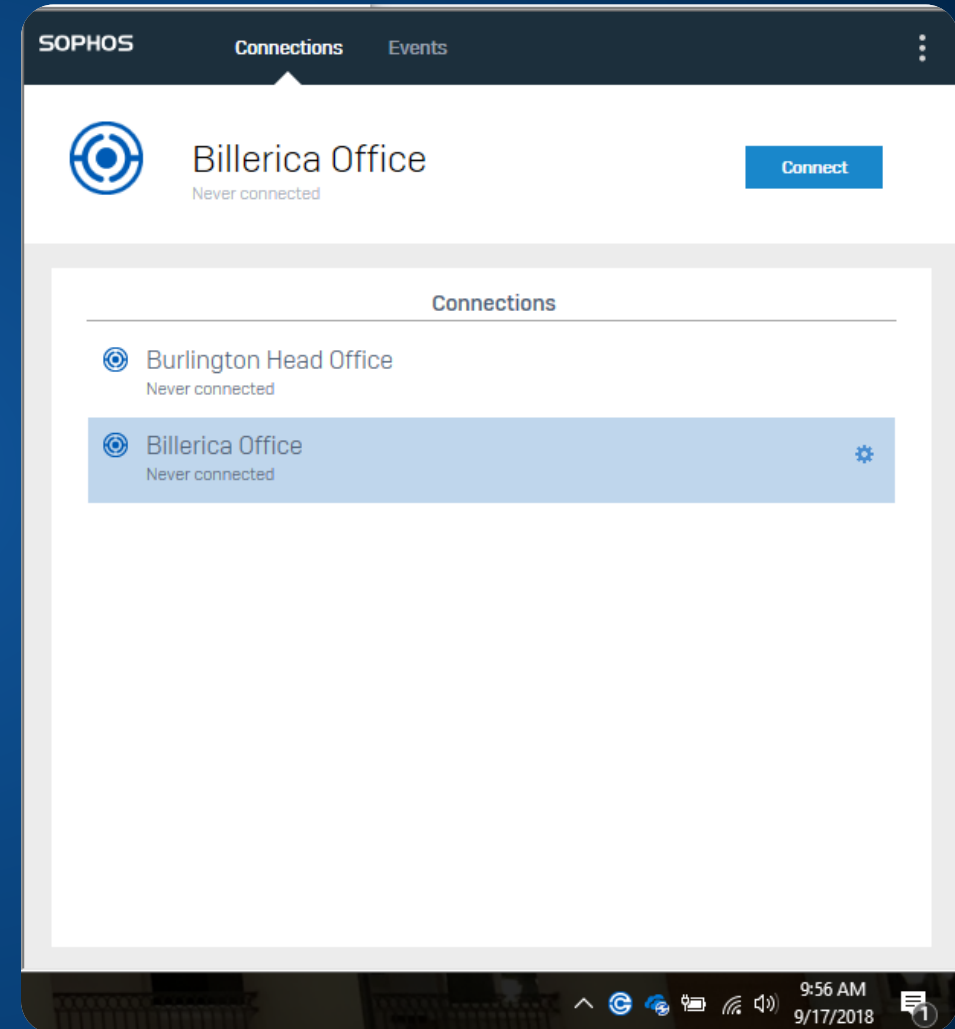
Synchronized Security via Remote VPN

Free client for easy, reliable remote connections

What's New

- IPSec VPN client for Windows/Mac
- Supports Synchronized Security for remote users
- Easy deployment and maintenance
- Simple operation requires no user education

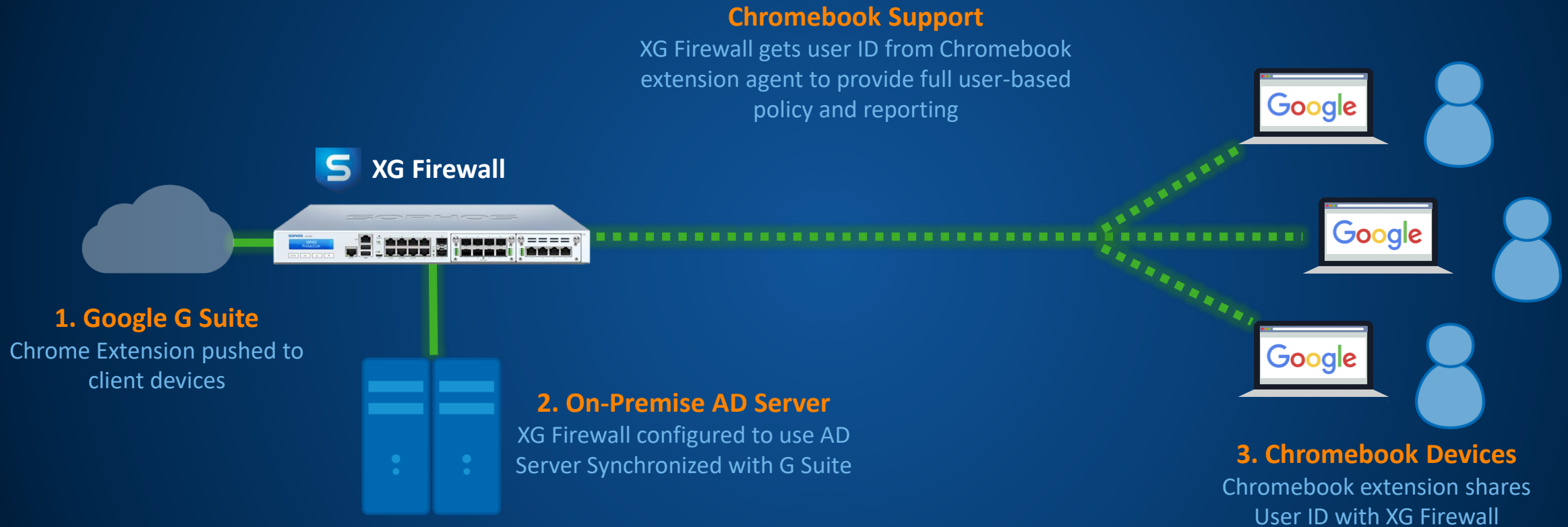
Free for partners and customers!



Education

Chromebook User ID

Enables user-based policy and reporting with Chromebooks

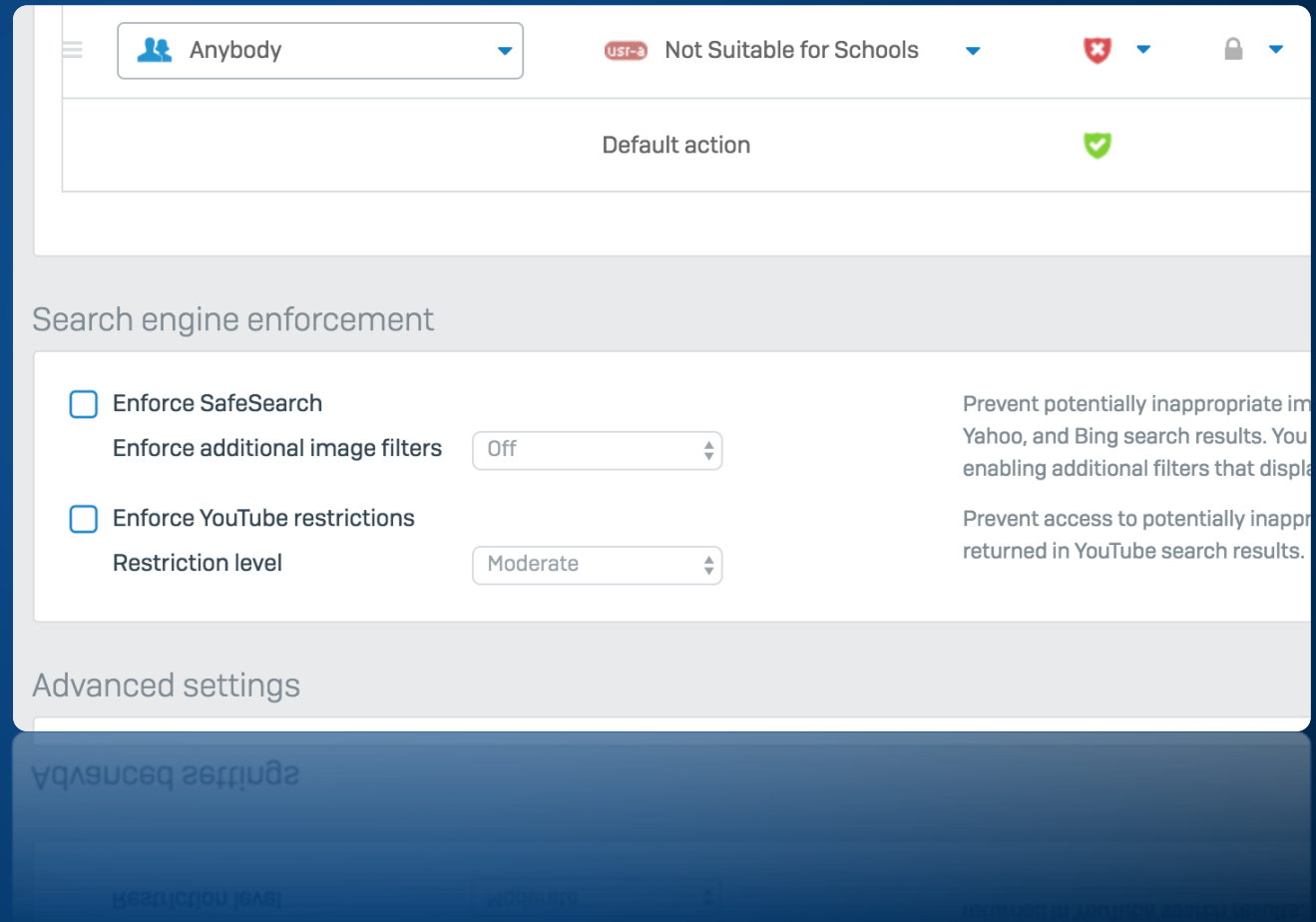


New Web Policy Options

Greater flexibility for SafeSearch, YouTube and unblocking sites for education

What's New

- SafeSearch and YouTube restrictions are now part of web filtering policy settings – enabling user/group based control of these features

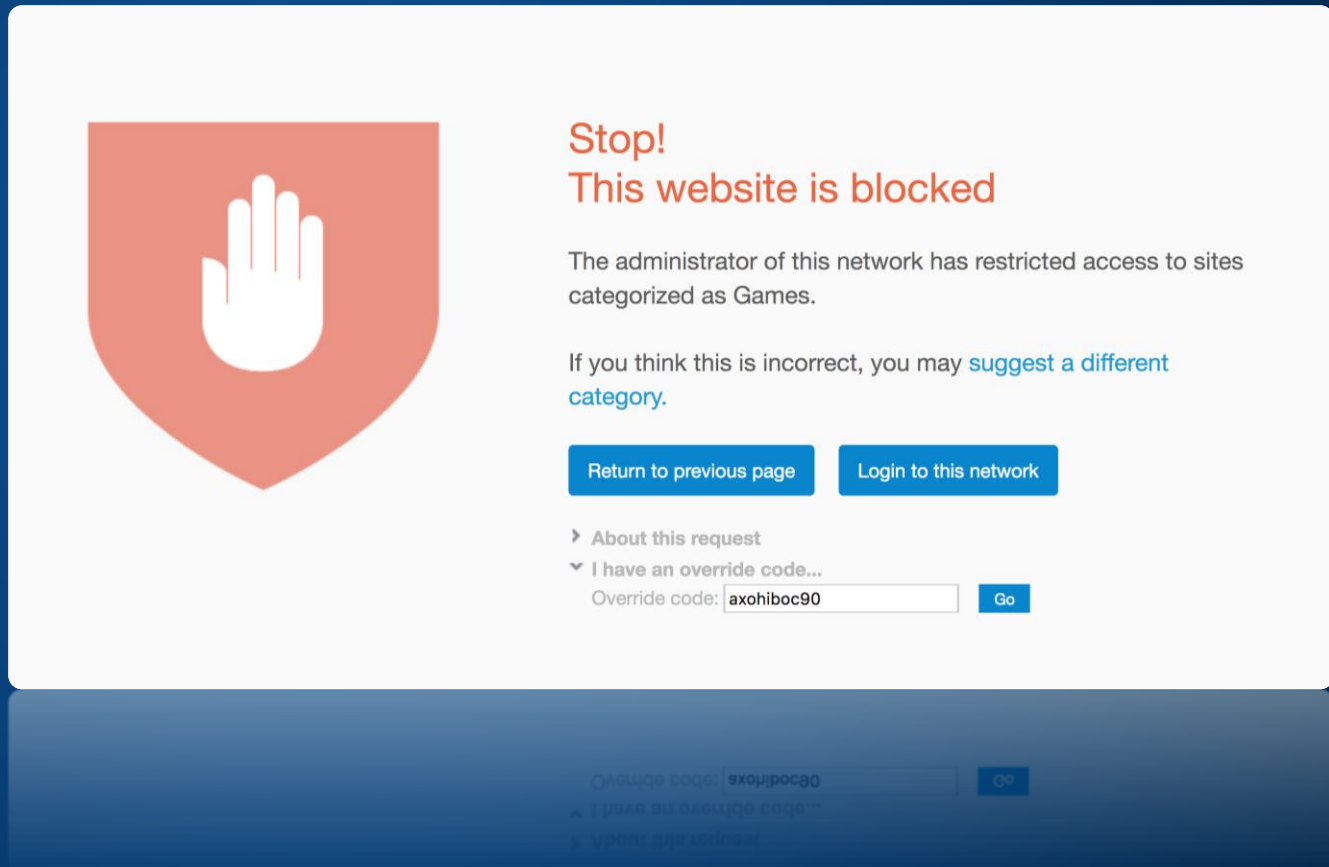


New Web Policy Options

Greater flexibility for SafeSearch, YouTube and unblocking sites for education

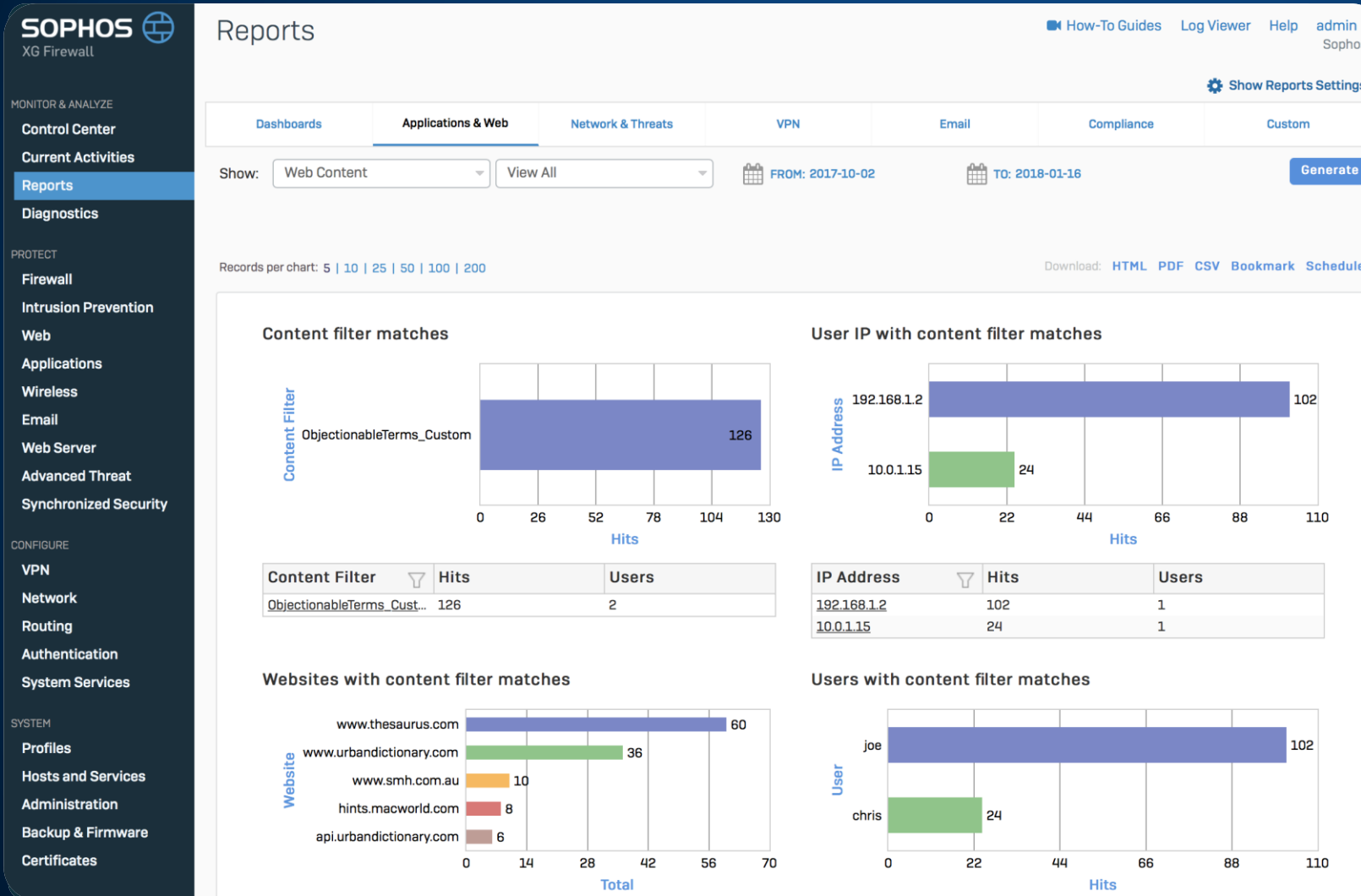
What's New

- SafeSearch and YouTube restrictions are now part of web filtering policy settings – enabling user/group based control of these features
- Override codes for blocked websites which can be configured/managed by teachers through the user portal



Web Content Filtering (v17)

Enabling child safety in education



Dynamic Content Monitoring & Filtering

- Quickly identify signs of bullying, radicalization, abuse or self-harm before they become a problem
- Dynamically block websites based on content regardless of their category

Management & Trouble-shooting

Firewall Rule Grouping

Ideal for larger firewall rule sets

What's New

- Setup matching criteria as part of the group definition for auto group assignment

Edit group

Group name *

Traffic to Internal Zones

Group description

To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis

Rule type

Any

Source zone

Any

Add new item

Destination zone

LAN

DMZ

VPN

WiFi

Add new item

Cancel Update

Firewall Rule Grouping

Ideal for larger firewall rule sets

What's New

- Setup matching criteria as part of the group definition for auto group assignment
- Select a group when creating a rule or set to automatically be assigned a group

Add User/network rule

How-to guides Log viewer Help admin ▼ Sophos

Rule name *
Enter Rule name

Description
Enter Description

Rule position
Bottom ▼

Action
Accept Drop Reject

Rule group
Create new
None
Automatic
User Traffic to DMZ
Traffic to DMZ
Traffic to WAN
Traffic to Internal Zones

Source

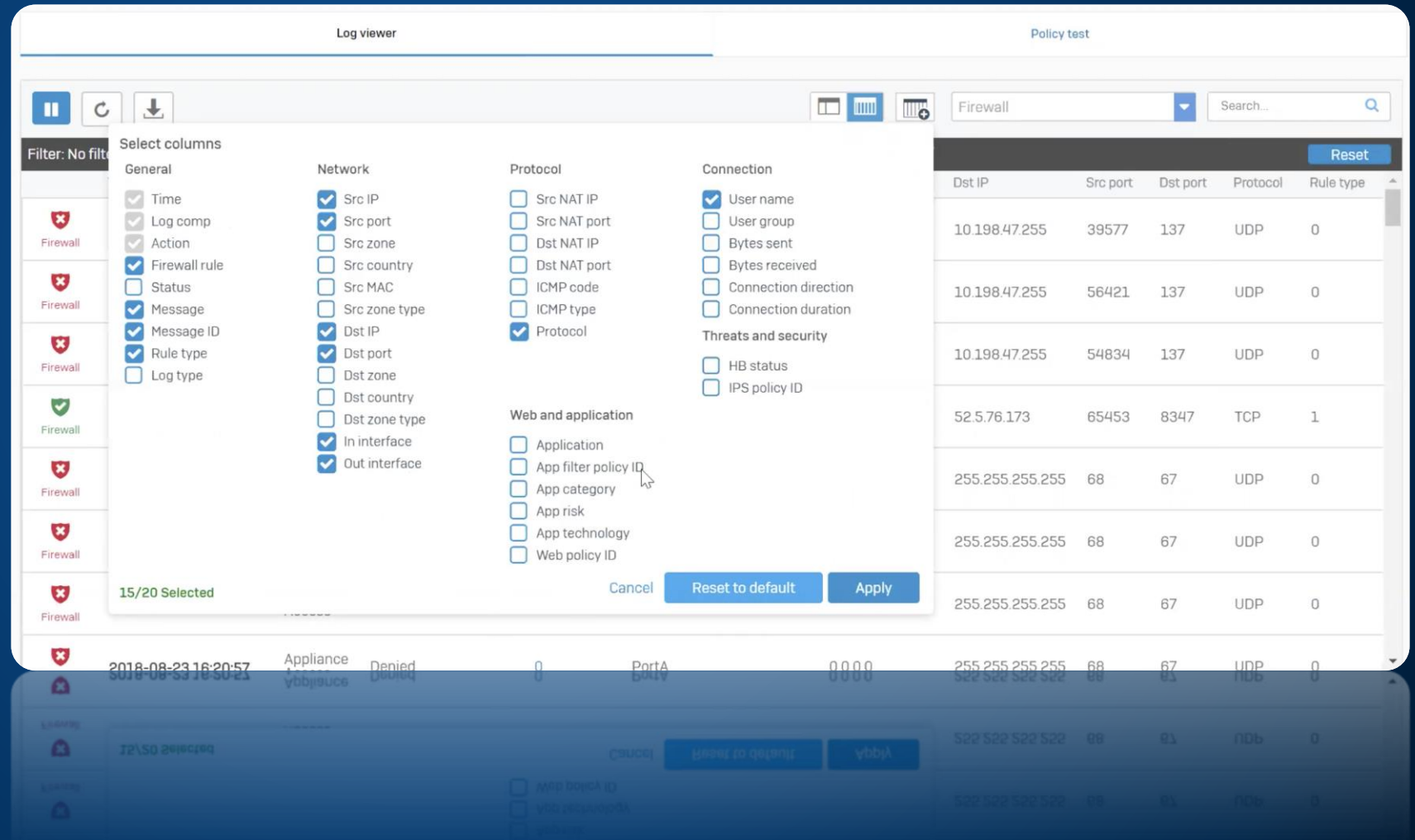
Can't add the rule to an existing group based on the selected criteria.

Log Viewer Enhancements

More powerful and streamlined trouble-shooting

What's New

- Column selector - select any 17 columns from a list of 44 possible fields
- Rule IDs referenced in logs are hyperlinked to open the related rule in the main console window
- Filters sorted alphabetically



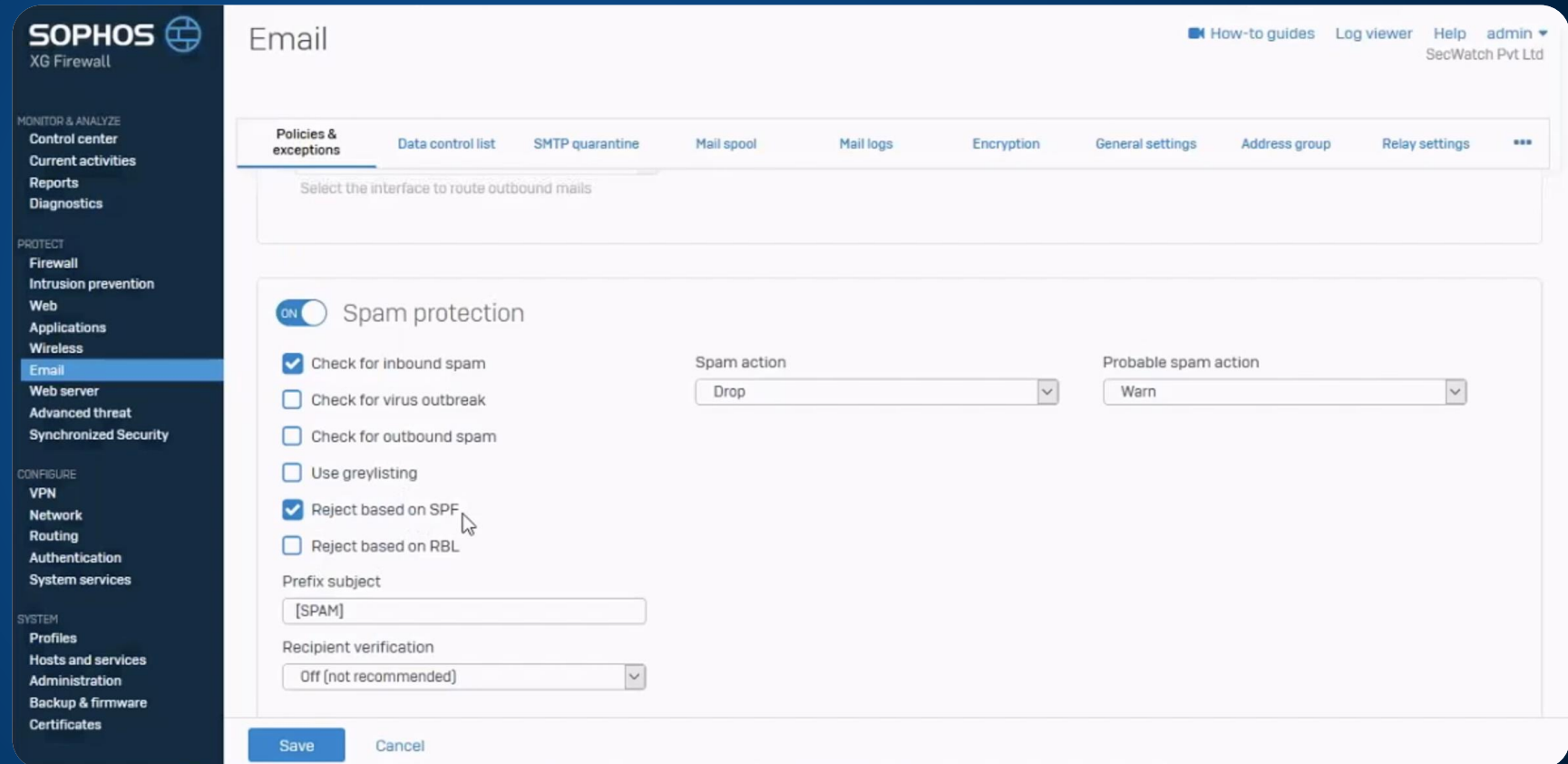
Email

Email Enhancements

Closing top requested feature gaps with SG UTM

What's New

- Recipient verification using Sender Policy Framework (SPF) for spoofing protection
- MTA update to Exim



Coming Soon

SOPHOS

Sophos Central Management for XG Firewall

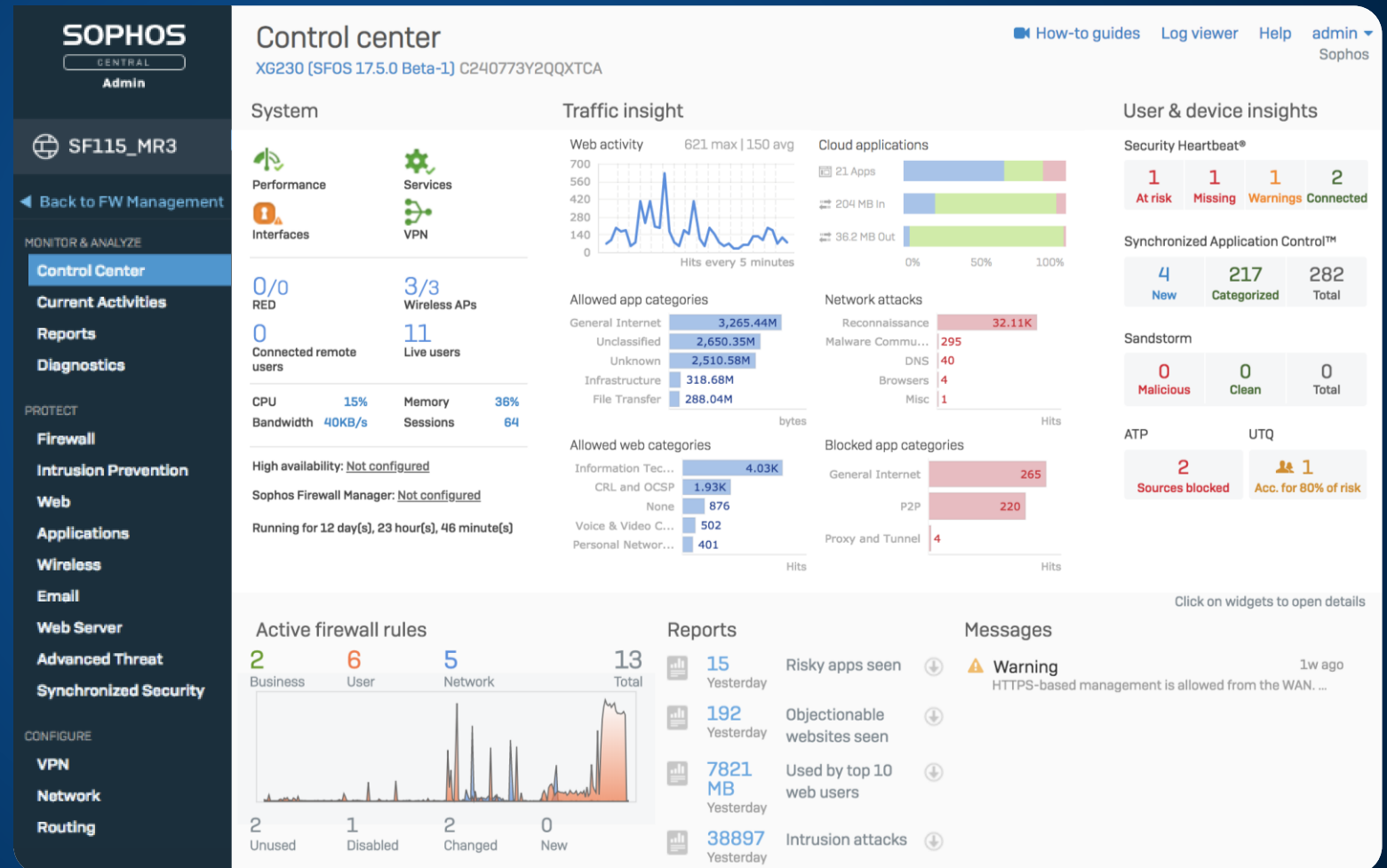
XG Firewall Joins Sophos Central

One Console

- View status and manage XG alongside all other Sophos Central products
- Full device management via SSO
- Secure remote access to all your XG devices via Sophos Central
- Alerting and status for availability, license, performance, and security
- Manage firmware updates
- Option to store/maintain backups in Central
- Zero-touch setup of new appliances

Free for partners and customers!

No Additional License Required



XG Firewall in Sophos Central – Available Soon

See all of your firewalls under management

SOPHOS
CENTRAL
Admin

Firewall Management

Back to Overview

ANALYZE

Dashboard

Alerts

Backup

MANAGE

Firewalls

CONFIGURE

Settings

Firewall Management - Firewalls

Overview / Firewall Management Dashboard / Firewalls

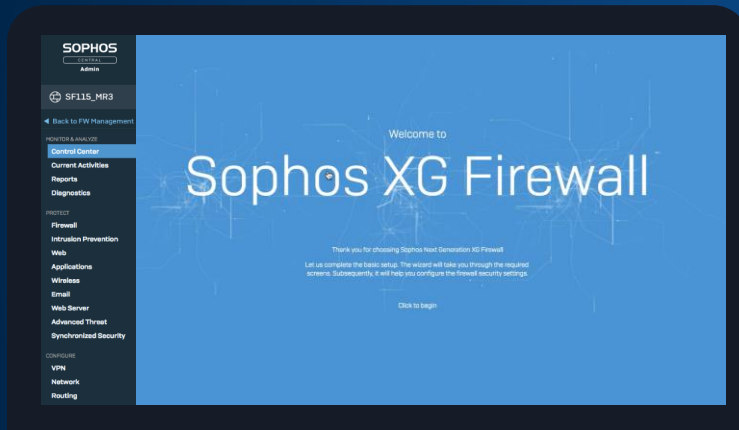
Add Firewall

	FW Name, IP	OS Version, Model, Serial Number
CONNECTED	C0100139BBHDVD6 108.7.62.118	SN: C0100139BBHDVD6
CONNECTED	Burlington Lab VM 198.144.101.86	SN: C010016J436YT20
CONNECTED	Billerica Lab VM 1 108.7.62.118	SN: C01001CY9K2YPE0

Rapid Deployment –Coming Early Next Year

Remote device deployment without an on-site engineer

**1. Use the Setup Wizard in
Sophos Central**



**2. (Optional) Email the Config File
to the remote site**



**3. Transfer the Config File to a
USB Stick**



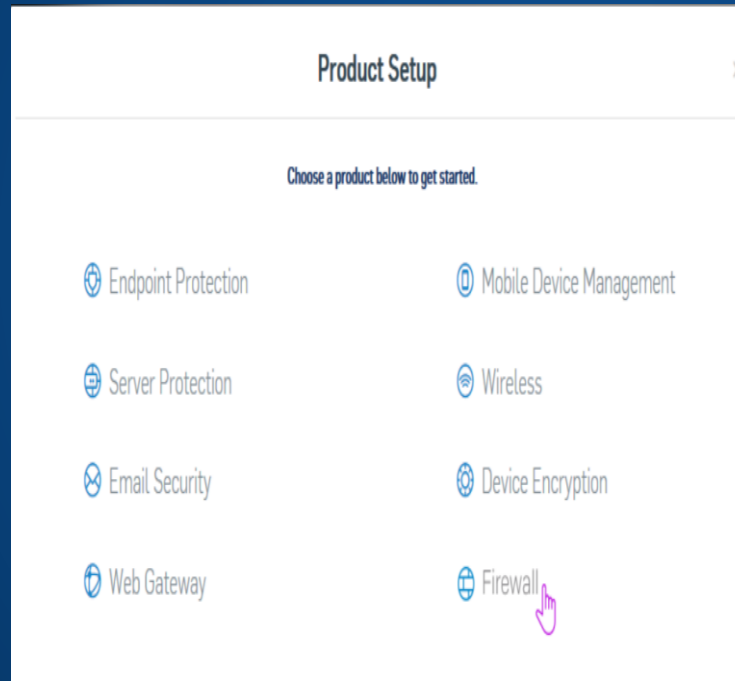
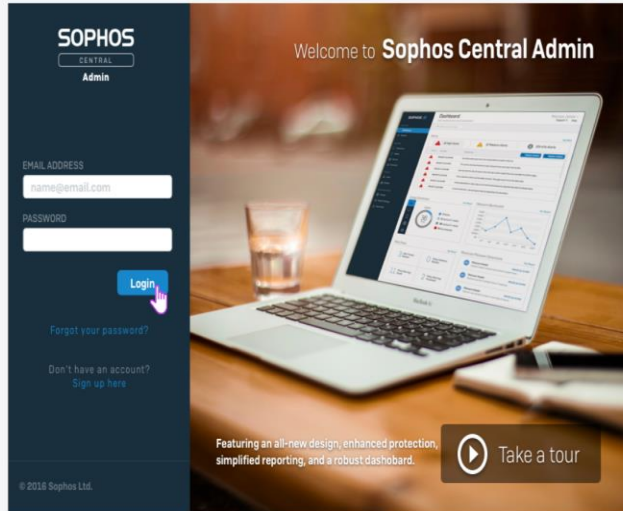
**4. Start the device with the USB
stick connected**

Workflow

Add Firewall



Steps on Central



The product setup page appears automatically upon initial access

- Clicking firewall opens the welcome /branding page if no firewall is added.
- If one has already trialed or added firewall - clicking Firewall will open the firewall Dashboard.
- Tentative sequence of products given
- a. Endpoint
- b. Server
- c. Encryption
- d. Phish Threat
- e. Mobile
- f. Firewalls
- g. Email
- h. Wireless
- i. Web

Workflow

Add Firewall



Steps on Central

Add Your Firewall

Add a fresh firewall



I want to add a fresh new firewall which is not configured yet, to provision and manage it via Sophos Central.

Join a firewall that is configured or deployed



I want to join my firewall that is already deployed or configured to manage it via Sophos Central.

Initiate adding firewall

- o Choose if the firewall is fresh (new) or already configured / deployed
- o If fresh (new) ask for Serial number. Enter serial number
- o Validate serial number, and if firewall is already claimed or managed via CFM or managed via Central
- o Register firewall (if not already registered)
- o Accept EULA

Try

- o Links to virtual firewall trial

Request Pricing

- o Redirect to find partners

Workflow

Add Firewall



Steps on Central

Note

o XG can only be managed from either SFM, CFM or Central

Add a firewall that is already deployed or configured x

If your firewall is already deployed or configured, you can join it to Sophos Central for management from your Firewall WebAdmin. Please note that a firewall can be managed at any point of time either via Sophos Central or Sophos Firewall Manager (SFM) or Sophos Central Firewall Manager (CFM).

- Register your firewall to this Sophos Central account [Show me how](#)
- Enable firewall management via Sophos Central [Show me how](#)

[Finish without waiting](#)

- Clicking [Show me how](#) opens a KB article or guide
- Finish without waiting takes to welcome page if no firewall in Central a/c. If a firewall already exists in Central a/c then take to firewalls list page
- On attempting to close the screen display msg to check if user does not want to wait on this screen. If user still continues then take to screens as defined for 'Finish without waiting'

Join your firewall to this Sophos Central account.
Enable Central Firewall Management from Firewall UI

Steps

Display steps as in progress with spinners.

['show me how'](#) takes to KB article or guide

Clicking [Finish](#) without waiting will take to screen 'Accept firewall in Central from FW list page'

[Canceling](#) the flow prompts user to confirm if they want to cancel this process. If user proceeds they land on firewall list page if a firewall is already connected to Central account, if no firewall then land on welcome to firewall page

Workflow

Add Firewall



Steps on Central

Add a firewall that is already deployed or configured

If your firewall is already deployed or configured, you can join it to Sophos Central for management from your Firewall WebAdmin. Please note that a firewall can be managed at any point of time either via Sophos Central or Sophos Firewall Manager (SFM) or Sophos Central Firewall Manager (CFM).

- ☒ Register your firewall to this Sophos Central account SN: xxx-xxxx-xxxx
- ☐ Enable firewall management via Sophos Central [Show me how](#)

[Finish without waiting](#)

- While user is on this screen and if a firewall is registered to this Central a/c that wasn't initiated through zero touch, then show a green check and display serial number of firewall. Show tooltip on hover over SN: xx, that this is the serial number of firewall that has joined to Central a/c
- Clicking finish without waiting in this case will take user to firewall list page

Add a firewall that is already deployed or configured

- ☒ **Congratulations!**
Your firewall is now joined to Sophos Central. Proceed to approve this firewall for management from the Firewalls page.
- ☒ Register your firewall to this Sophos Central account SN: xxx-xxxx-xxxx
- ☒ Enable firewall management via Sophos Central

[Next](#)

- When same FW reaches out to Central for approval of mgmt then turn both checks to green and display serial number
- Change the upper section of screen to reflect congratulations
- Clicking next takes to firewall list page

Line 2 of the text will be
You can now manage this firewall from the firewall list.

Steps

- Once the firewall is **registered** to Central and detected the check against first step turns green
- Clicking **Finish** without waiting will take to screen 'Accept firewall in Central from FW list page'
- No cancel** link or cross on screen

Steps


- If user is on this screen when firewall mgmt via Central is turned on the firewall, and if the serial number of firewall trying to join to Central matches the serial number displayed against step 1, then turn the 2nd step status to **green**
- Replace **Finish** without warning to Next button

Workflow "Fresh Install"




Add Your Firewall

Add a fresh firewall



Join a firewall that is configured or deployed



I want to add a fresh new firewall which is not configured yet, to provision and manage it via Sophos Central.

I want to join my firewall that is already deployed or configured to manage it via Sophos Central.

Register Firewall

You must register the firewall to manage license(s) and record registration date. A MySophos account is needed to register the firewall.

This firewall will be registered to

Primary SuperAdmin (email id)

Paul 2 (email)
Super Administrator 3 (email)
Administrator 1 (email)
Administrator 2 (email)
Administrator 3 (email)

Change

Model: <XG105>

Back

Register and Proceed

Register

Register the firewall for 30-days trial

Zero Touch

SOPHOS

Zero Touch Workflow

Initial Config On
Central



Loading to XG..

Download Zero Touch Configuration file



Download the zero touch configuration file after making the below settings and provide to the administrator who will deploy the firewall. The local administrator needs to add this file to a USB and plug it in the firewall before powering on the firewall. [Learn more.](#)

If the firewall does not detect a valid zero touch configuration file the firewall cannot be auto-provisioned from Sophos Central and one has to configure the firewall manually to join it to Sophos Central.

If the network environment or placement where the firewall will be deployed, won't allow the firewall to automatically connect to Internet on bootup, you need to configure the Internet settings.

Manually configure Internet Settings

☐ Email the Zero Touch configuration file to

(enter multiple emails with semi colon as separator)

[Previous](#)

[Download & Email Zero Touch file](#)

Zero Touch Config File

Email sample pending
XML format file, not encrypted
reusable across multiple
firewalls

Zero Touch Workflow


Steps on Firewall


Prep USB Drive


- <https://wiki.sophos.net/display/NSG/Format+USB+Pen+drive+for+Zero+touch+configuration>
- Local administrator receives the firewall. Copies the zero touch config file in USB


On XG

- Power on the firewall with USB plugged in. If no zero touch configuration is detected, starts with regular wizard
- Detects zero touch configuration file on bootup
- Accepts Internet settings if in the file reaches out to check for zero touch service

 No auto-provision details for firewall on contacting Sophos Central

 Internet Connected


 Unable to contact Sophos Central for auto-provisioning details

 No Internet found

The firewall detected a USB with a zero touch configuration file plugged in.

But the firewall could not find Internet to connect to Sophos Central for the auto-provisioning details. The firewall will keep trying again for some time.

[Manually configure Internet Settings](#)

 Connected to Internet

This firewall is provisioned to be managed by Sophos Central.

Sophos Central a/c details:
Company: <ABC Technologies>
Email: <sanket.handa@sophos.com>
Firewall provisioned by: Sanket Handa

You can login to Sophos Central to finish setting up this firewall or notify your Central Administrator.

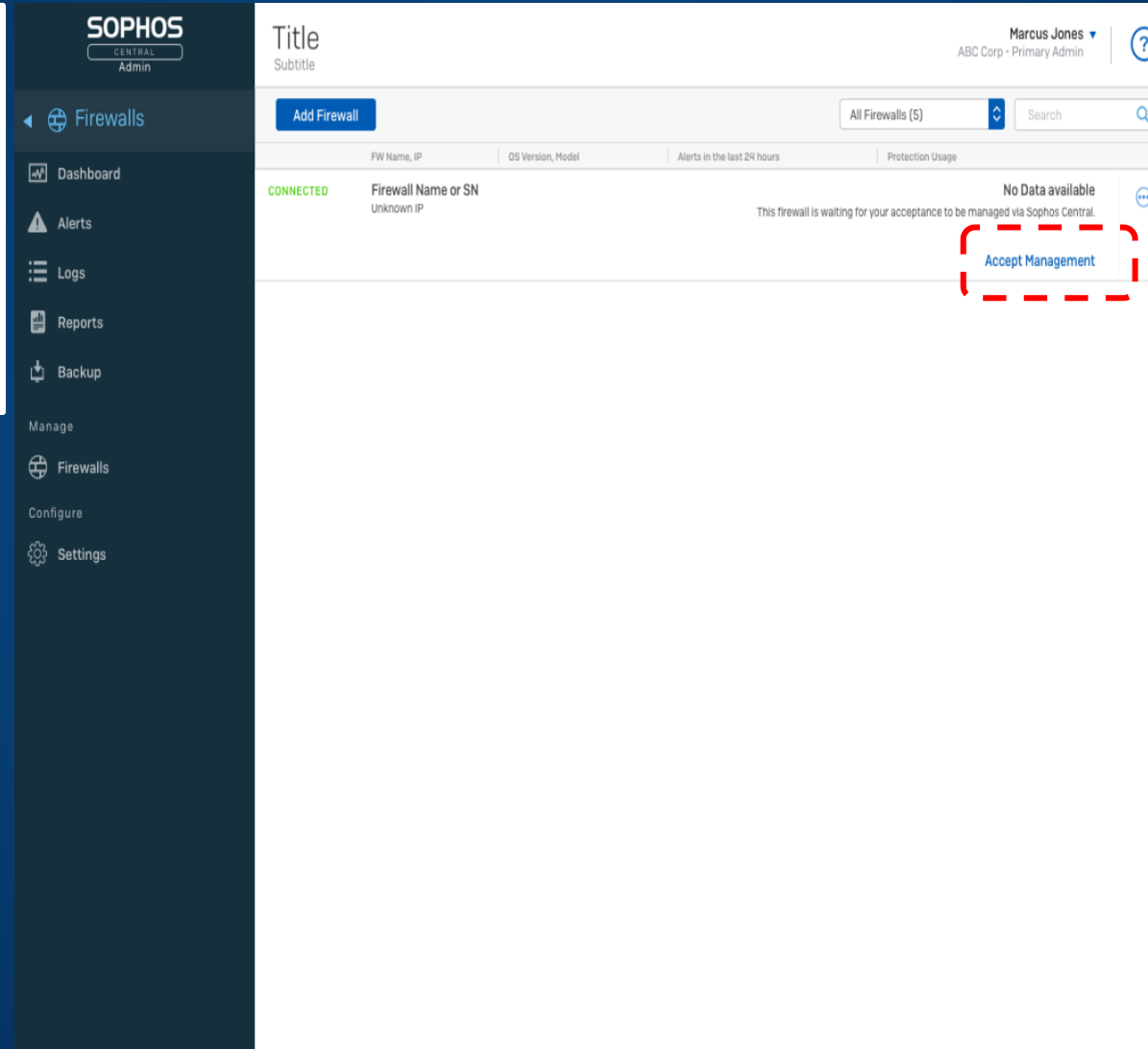
Steps on Sophos Central

Status

Connected when firewall is connected to Central

Firewall name - Serial number

Accept Management



Zero Touch Config

- Connection gets established
- Pre-configuration settings (stored on firewall from USB) are applied on firewall.
- Data from firewall starts coming into Central

Note On Central

- When SuperAdministrator opens firewall, display popup on control center to set password of firewall.
- A Section in firewall UI that allows to set password of admin user without having to enter previous password. (applies only for SuperAdministrator)

Note On Local XG

If user opens firewall webadmin after firewall is accepted in Central. Local control Center with a popup informing that firewall is managed via Central.

APX – Wave 2 Access Points – Coming in MR1

Faster, Better WiFi



Faster Connectivity – up to 2.3Gbps

High density – high capacity

Optimized performance – per device

APX 740

Flagship 4x4:4 for the mid-market enterprise
(at load*, 3x the throughput of AP100)

APX 530

High performance 3x3:3 for all business
(at load*, 2x the throughput of AP100)

APX 320

2x2:2 Medium performance 2x2:2 for all orgs
(at load*, 2x throughput of AP55)

SOPHOS
Security made simple.