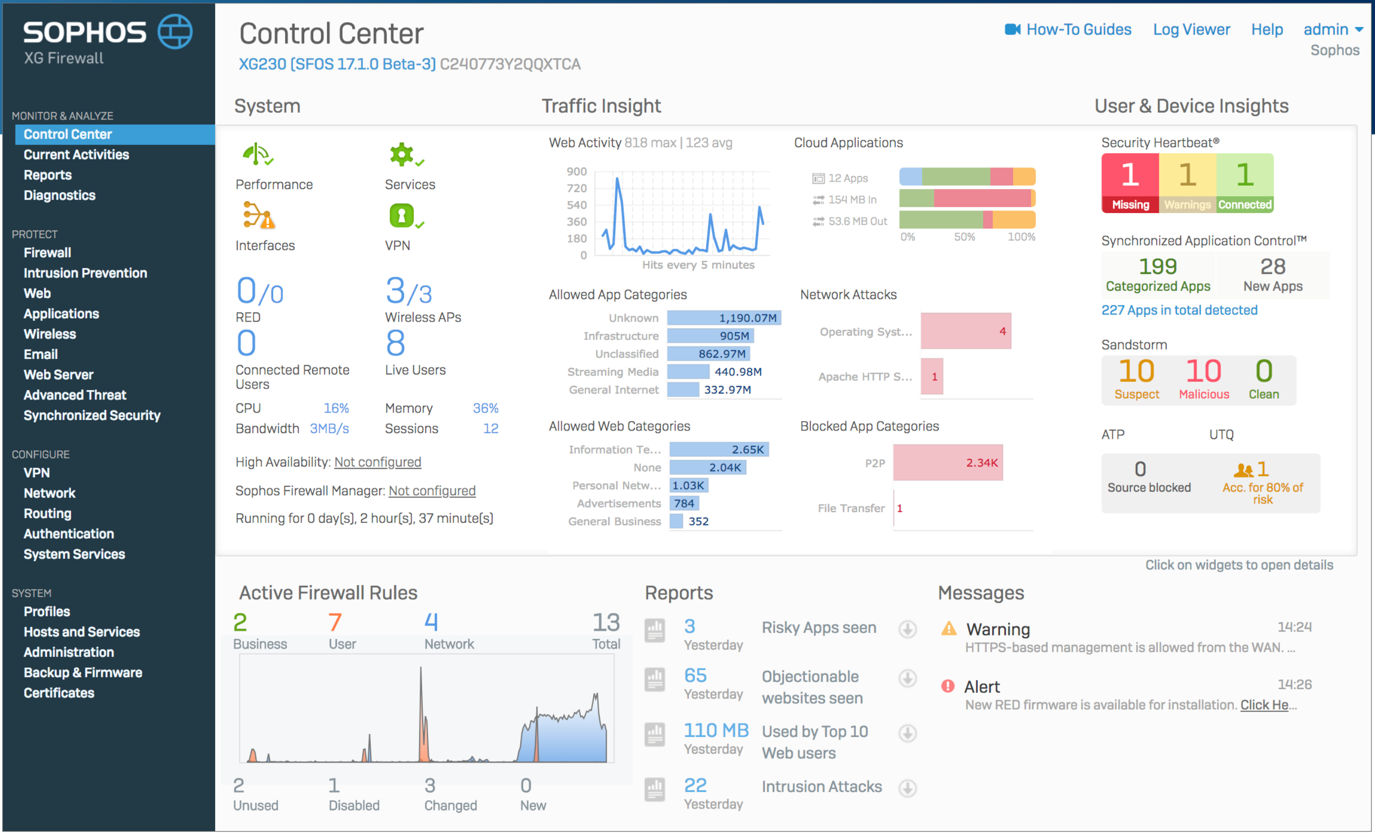
SOPHOS
Cybersecurity made simple.

What's New in Sophos XG Firewall

Key New Features in XG Firewall v17.1


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
System Services

SYSTEM
Profiles
Hosts and Services
Administration
Backup & Firmware
Certificates

Control Center
XG230 (SFOS 17.1.0 Beta-3) C240773Y2QQXTCA

How-To Guides | Log Viewer | Help | admin Sophos

System
Performance | Services | Interfaces | VPN
0/0 RED | 3/3 Wireless APs
0 Connected Remote Users | 8 Live Users
CPU 16% | Memory 36%
Bandwidth 3MB/s | Sessions 12
High Availability: Not configured
Sophos Firewall Manager: Not configured
Running for 0 day(s), 2 hour(s), 37 minute(s)

Traffic Insight
Web Activity 818 max | 123 avg

Cloud Applications

Allowed App Categories
Unknown 1,190.07M
Infrastructure 905M
Unclassified 862.97M
Streaming Media 440.98M
General Internet 332.97M

Network Attacks
Operating Syst... 4
Apache HTTP S... 1

Allowed Web Categories
Information Te... 2.65K
None 2.04K
Personal Netw... 1.03K
Advertisements 784
General Business 352

Blocked App Categories
P2P 2.34K
File Transfer 1

User & Device Insights
Security Heartbeat®
1 Missing | 1 Warnings | 1 Connected
Synchronized Application Control™
199 Categorized Apps | 28 New Apps
227 Apps in total detected
Sandstorm
10 Suspect | 10 Malicious | 0 Clean
ATP | UTQ
0 Source blocked | 1 Acc. for 80% of risk

Click on widgets to open details

Active Firewall Rules
2 Business | 7 User | 4 Network | 13 Total
2 Unused | 1 Disabled | 3 Changed | 0 New

Reports
3 Yesterday — Risky Apps seen
65 Yesterday — Objectionable websites seen
110 MB Yesterday — Used by Top 10 Web users
22 Yesterday — Intrusion Attacks

Messages
Warning 14:24
HTTPS-based management is allowed from the WAN. ...
Alert 14:26
New RED firmware is available for installation. Click He...

CASB (Cloud Access Security Broker) – Cloud App Visibility

With the tremendous number of cloud application and storage services available, organizations require visibility to expose any hidden risks related to what services are being used and where data is being stored. XG Firewall v17.1 delivers shadow IT discovery and cloud app visibility as the first phase of our CASB solution. This feature includes a new widget on the Control Center that provides valuable usage information on new, sanctioned, unsanctioned, and tolerated cloud-based applications and services. It also provides insights into inbound and outbound traffic by type. Drill down to detailed reporting on individual cloud apps and services that provides details on users, traffic, uploads, and downloads with options to classify, filter, or traffic shape individual apps or services. Further drill downs provide additional information on individual user traffic and data usage for each cloud application, so you can identify risky usage patterns quickly and easily.

Synchronized App Control Enhancements

Synchronized App Control, introduced in v17, has proven to provide a breakthrough in network visibility being able to identify, classify and control previously unknown applications active on the network. It utilizes Synchronized Security to obtain information from the endpoint about applications that don't have signatures or are using generic HTTP or HTTPS connections. It solves a significant problem that affects signature-based app control on all firewalls today where many applications are being classified as "unknown," "unclassified," "generic HTTP," or "SSL," for example.

In addition to the filtering options provided in v17, Synchronized App Control gets a few additional enhancements that streamline large application list management, such as the ability to search for applications and the option to delete or remove discovered applications from the list that are not relevant to you. The application category is also now displayed in the application list, making it easy to see what category an application is associated with at a glance.

Firewall Enhancements

Enhancements have been made to the firewall and rule management to improve flexibility and streamline management even further. You can now double-click a firewall rule in the list to open it for editing. There's a new option to block Google QUIC's HTTPS over UDP, forcing a fallback to TCP, enabling full SSL inspection of the traffic. And there is now added flexibility in defining ACL exceptions to restrict access to services, such as the User Portal from a single alias, for example.

Email Protection Enhancements

User management over individual SMTP block and allow lists is now provided via the User Portal. Domains or email addresses added to the Allow list will bypass policies (except for malware or sandboxing enforcement) and adding domains or addresses to the block list will automatically quarantine emails from those senders.

In addition, more flexible and granular SMTP policy exceptions are supported to provide parity with Sophos SG UTM and reduce false positives. Exceptions can be defined based on sources/hosts, sender address domains, or recipients (with support for wildcards).

Wireless Enhancements

XG Firewall v17.1 provides wireless networking enhancements, including the option to set the channel width for wireless radios in the GUI, as well
as Radius Accounting.

SSL VPN Port Customization

A top requested feature: the SSL VPN Port for remote access can now be customized.

IPSec VPN IKEv2 Enhancements

XG Firewall v17 introduced new IKEv2 support for IPSec VPN connections and all stability and reliability enhancements, included in subsequent maintenance releases, are included with v17.1.

New Hardware Support

Support for the latest XG Series desktop hardware connectivity and features, unveiled in an earlier maintenance release, is also included in XG Firewall v17.1.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS