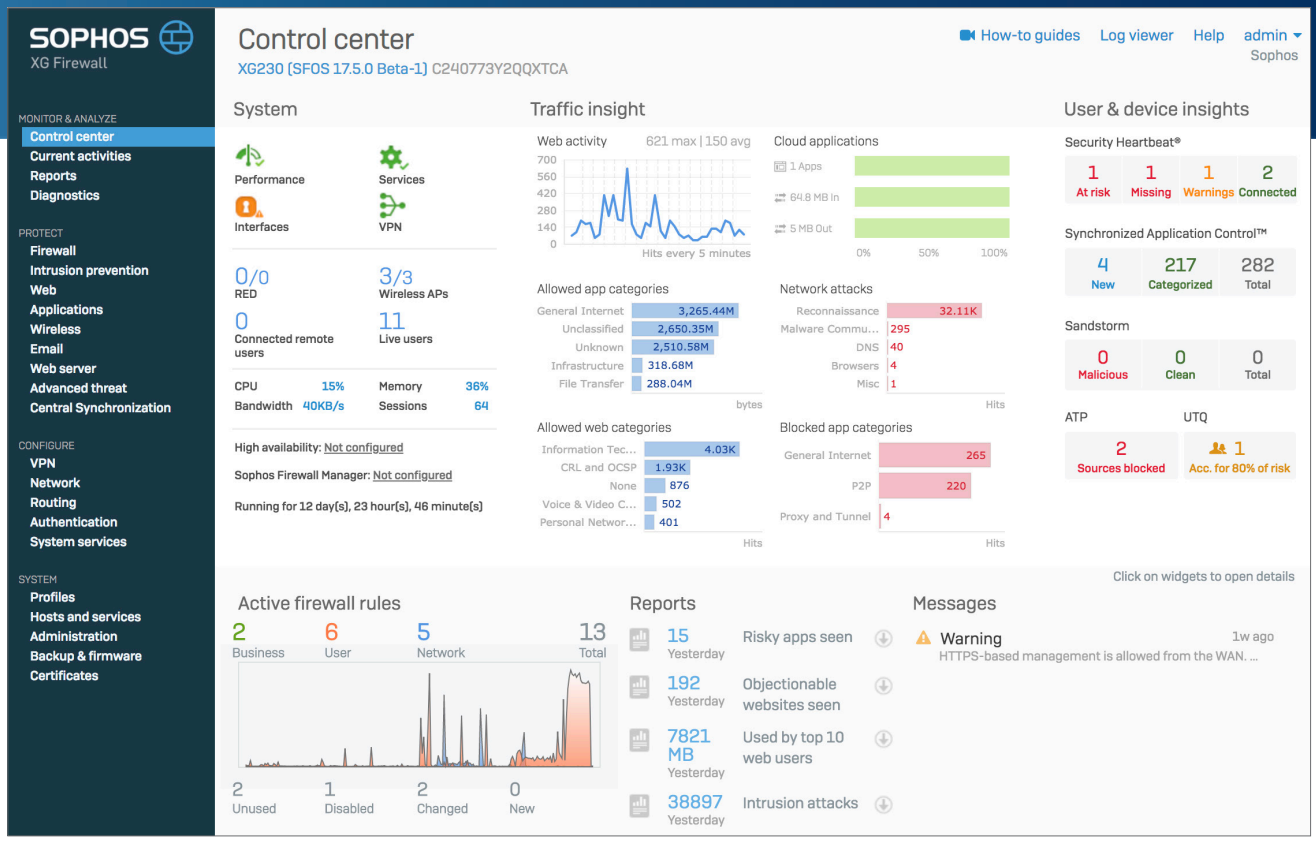
SOPHOS
Cybersecurity made simple.

XG Firewall

What's New in v17.5



Key New Features in XG Firewall v17.5

Sophos Central Management

The addition of XG Firewall management to Sophos Central is a significant milestone as customers now have the option to manage the entire portfolio of Sophos Synchronized Security products in Sophos Central. This includes: Endpoint, Server, Mobile, Device Encryption, Wireless, Email and now XG Firewall.

Firewalls can be joined to Sophos Central quickly and easily and managed from within Sophos Central securely from anywhere without having to enable HTTPS login access from the WAN on the firewall. All your XG Firewall devices will appear in Sophos Central and they can be managed individually as if you were logged onto the actual device. Sophos Central displays the actual user interface from the device in Sophos Central so there is no synchronization of settings or configuration between Central and the device required.

Backup Management: Additional features that Sophos Central management provides include the option to store regularly scheduled backup files in Central automatically for safe keeping along with easy and convenient access to your historic backup files should they be required.

Alerting: XG Firewall alerts will appear on the main Sophos Central dashboard including connectivity alerts for interfaces and VPN, resource utilization, licensing notifications, and security events.

Firmware Updates: You can manage firmware updates for XG Firewall from within Sophos Central – enabling an easy one-click update to the latest firmware.

Light-Touch Deployment: This feature enables even a non-technical person to connect and configure a remote XG Firewall and get it connected into Sophos Central. An administrator can add the new firewall in central and step through the initial setup wizard before the XG device is installed. They can then download the configuration or email it to another location, so it can be copied to a USB stick. The stick is then plugged into the XG Firewall device when it is first fired up, setting its initial configuration, after which it can be fully managed from Sophos Central. For power users, the config file can be edited and customized further.

Synchronized Security – Synchronized Application Control Enhancements

Synchronized App Control, introduced in v17 has proven to offer a breakthrough in network visibility with its ability to identify, classify and control previously unknown applications active on the network. It uses Synchronized Security to obtain information from the Endpoint about applications that don't have signatures or that 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 "generic HTTP" or, "SSL" or even "unknown" or "unclassified".

This feature has been so successful in identifying hundreds of new applications on most networks, that several additional enhancements have been requested since launch to better manage and organize the newly discovered applications. In addition to the enhancements provided in v17.1, Synchronized App Control adds the much-requested ability to display Windows and Mac system applications in a separate list, to better focus on user-driven applications. You can also hide applications, then use a new filter option to view hidden applications and unhide apps. There's also a new option to mark applications as seen to remove them from the "new" list. Enhancements have also been made to how path names are displayed.

Synchronized Security – Lateral Movement Protection

When Synchronized Security was first introduced with XG Firewall, Security Heartbeat™ settings in firewall rules allowed unhealthy endpoints with RED or YELLOW heartbeat status to be denied or blocked by these firewall rules. This effectively ensures compromised systems can be isolated from other parts of the network such as other zones, segments, or even the internet depending on the firewall rule configuration. In this way, Security Heartbeat™ helps isolate infected endpoints to prevent a threat moving or spreading to other parts of the network or communicating out to the internet.

In v17.5, this feature is enhanced further with the ability to isolate unhealthy endpoints even from other endpoints on the same broadcast domain or network segment. This is elegantly accomplished by the firewall automatically informing all healthy endpoints to ignore any traffic coming from any unhealthy endpoints, effectively isolating them on the network until they can be cleaned up. Once cleaned up, its Security Heartbeat status will return to GREEN and connectivity with other systems on the network will be automatically restored.

In addition, IPS detections from compromised endpoints can now trigger a RED heartbeat condition and lateral movement protection as well, further enhancing protection from threats on the network.

Synchronized Security – Synchronized User ID

User authentication is critically important for all next-gen firewalls to provide user-based visibility, reporting and policy enforcement. In a typical Active Directory environment, transparent user identity at the firewall is achieved either by installing an agent on the Directory Server to relay user identity information to the Firewall or on the endpoint to share user identification. These agent solutions can be problematic to deploy in some situations and environments. With v17.5, Endpoints on an Active Directory Domain, can now share user identity with the Firewall through the Security Heartbeat™ connection. This makes user identification seamless and easy without having to deploy agents on the domain controllers. This feature can be very helpful in many situations, but particularly where inline deployment of XG with other firewalls is desired.

Note this solution is not a replacement for SATC which provides a user identification agent for multi-user systems like terminal services hosts. SATC is still the best solution in these situations. This solution also doesn't support non-managed devices such as Linux hosts.

Web Policy Enhancements

A few enhancements to web policy enforcement are included in v17.5 that have been highly requested by many customers, particularly those in the education sector. Web policies have been expanded to include many settings that were previously global configuration options. Search engine enforcement, including SafeSearch and YouTube restrictions, along with download file size limits, and Google App domain restrictions are all set on a per-policy basis now providing much greater flexibility in how these controls are applied.

Web Policy Overrides

Web policy overrides is another top requested feature. It allows authorized users to override blocked sites on user devices – temporarily allowing access. Administrators define which users (e.g. teachers) have the option to authorize policy overrides. Those users can then create their own override codes, like simple passwords, in the XG Firewall User Portal and define rules about which sites they can be used for. Codes can be shared with End-users, who enter them directly into the block page to allow access to a blocked site. Override code rules can be broad – allowing any traffic or whole categories – or more narrow – allowing only individual sites or domains – and can also be limited by time and day. And to avoid abuse, codes can easily be changed or cancelled. Administrators can see a full list of all override codes created and disable or delete them, as well as defining sites or categories that can never be overridden. There is also a new report providing full historical insight into web override use.

Chromebook Authentication

Chromebooks are increasingly popular in education and some corporate environments, but they create a unique set of challenges for user identification with network firewalls. XG Firewall v17.5 provides a Chromebook extension that shares Chromebook user IDs with the Firewall to enable full user-based policy enforcement and reporting. Pre-requisites include an on-premise Active Directory Server synced to Google Gsuite. The Chrome extension is pushed from the Gsuite admin console providing easy and seamless deployment that is transparent to users.

Client Authentication

The XG Firewall Client Authentication Agent is a very popular authentication method and in v17.5 it gets a number of important enhancements including per-machine (rather than per-user) installation support, an option to hide on startup, an option for the user to explicitly logout, automatic reconnection on wake from sleep, MAC address telemetry sharing to support MAC address filtering as well as a new icon and support for Windows XP.

Log Viewer Enhancements

An all-new XG Firewall Log Viewer was launched with v17 and in this release it gets further enhancements. The filter list is now sorted in alphabetical order and now all rule ID's in log entries are hyperlinked that will open the related firewall rule in the main window when clicked. In the standard column view, there is a new option to customize the columns displayed in the log viewer. Up to 17 different columns can be selected from the full set of fields that are available based on the selected module being monitored.

Firewall Rule Group Enhancements

Firewall rule group enhancements add an option to select a group when creating a firewall rule, including the option to assign the rule to a group automatically. The rule will be assigned to a group based on matching criteria defined as part of the group configuration.

IPSec and SD-WAN Link Fail-over and Restore

You can now set redundancy groups for your IPSec tunnels that will handle fail-over automatically in the event of a disruption and restore once the primary link is available. There is now a similar option for WAN link restoration following a fail-over as well that will either assign only new connections to the restored link or all connections.

IPS Enhancements

Over time we have been enhancing protection and performance of the IPS engine by adding the Talos commercial IPS signature library from Cisco. We augment the Talos library with additional signatures as required to ensure optimal intrusion protection. The Talos library includes more granular categories, and in v17.5 we are making those available in the IPS policy tool, making it easier to tune your policies for optimal protection and performance. Like SophosLabs, Talos is a highly respected network security analysis group working around the clock to respond to the latest trends in hacking, intrusions, and malware.

Note: All new categories have been carefully mapped to previous categories, but admins are encouraged to use this as an opportunity to double-check your IPS policies and ensure they are optimized under the new category structure.

Email Enhancements

XG Firewall email enhancements include verification of the recipient using Active Directory and Sender Policy Framework (SPF) spoofing protection. The Mail Transfer Agent (MTA) is also being updated to Exim. Together these enhancements address our top requested email features from our SG UTM customers and partners.

Wireless Enhancements

Support for Radius server failover with multiple servers.

Improved documentation

Enhanced online help now centers around the user's current task and needs with a learning content approach that suggests context specific actions, related information and links to relevant Knowledgeable articles.

Airgap Support (Coming in a v17.5 MR)

Enables updates for XG Firewalls deployed in environments that are physically isolated from the internet (an "airgap"). Protection pattern updates, licenses, and firmware updates can be downloaded from Sophos and uploaded via USB storage device to XG Firewall.

New Wireless APX Access Point Support (Coming in v17.5 MR1)

Support for the latest Wave 2 APX Series wireless access points will be provided in a follow-on maintenance release shortly after the release of v17.5.

Sophos Connect IPSec VPN Client (Entering EAP)

At the same time as v17.5 we are launching the Early Access Program (EAP) for Sophos Connect, a new IPSec VPN Client that makes VPN connections easy to deploy and seamless for end-users to utilize. It also supports Synchronized Security for remote connected clients providing all the benefits of application visibility and health monitoring and response for remote users. Connection profiles can be easily deployed or added at any time. The application runs as a system try or menu bar item on Windows and Macs respectively. It is freely available for all XG Firewall customers from within the XG Firewall management console under VPN > Sophos Connect.

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

18-11-01 WPNA (MP)