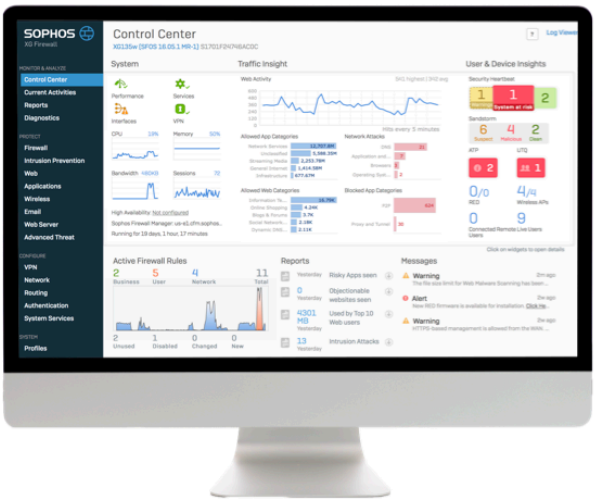
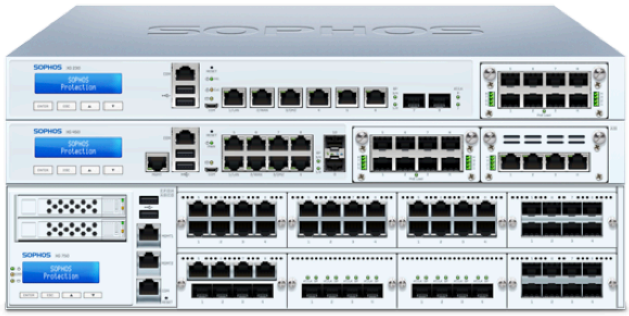
SOPHOS
Security made simple.

# XG Firewall

## What's New in v17



## Setup, Control Center and Navigation

### Initial Setup Wizard

Introduced in a Maintenance Release, a new initial setup wizard enables quick and easy out-of-the-box setup. In addition to a new user-friendly setup wizard, the new process also allows the initial license registration process to be bypassed during initial setup to streamline the process. The wizard has been carefully crafted to provide both maximum assistance to new XG Firewall customers without requiring documentation, while also enabling expert users to breeze through the setup process quickly and efficiently. It also includes an option to update the firmware to the latest release as part of the setup process which ensures customers will be on the latest-and-greatest firmware when they deploy.

### Synchronized App Control Widget

A new widget on the Control Center associated with the new Synchronized App Control feature provides at-a-glance indication of unidentified applications that have been matched.

### How-to Guides

Introduced in a Maintenance Release, a new option at the top of every screen provides one-click access to the XG Firewall How-To Library with videos and guides on how to perform common tasks in XG Firewall.

# Security and Control

## Synchronized App Control

Synchronized App Control is a breakthrough in network visibility. It can identify, classify and control previously unknown applications active on the network utilizing Synchronized Security to obtain information from the Endpoint about applications that don't have signatures or are using generic HTTP or HTTPS connections. This 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.

XG Firewall can now positively identify all applications being utilized on Sophos Endpoints. Where possible, XG Firewall will automatically classify the application and control it using existing app control policies. Administrators can also manually assign categories to discovered applications to enable app control enforcement to block or prioritize the application as desired. Discovered applications can also be added directly to existing App Control Policies.

Full interactive drill-down reporting on Synchronized Applications is also included providing insights into how applications are identified, what categories they belong to, specific applications in use, by user, host, destination country, policy, and more.

## Web Keyword Monitoring and Enforcement

Web policies now include the option to log and monitor or even enforce policy related to keyword lists. This feature is particularly important in education environments to ensure online child safety and provide insights into students using keywords related to self-harm, bullying, radicalization or otherwise inappropriate content. Keyword libraries can be uploaded to the Firewall and applied to any web filtering policy as an added criteria with actions to log and monitor, or block search results or websites containing the keywords of interest.

Comprehensive reporting is provided to identify keyword matches and users that are searching or consuming keyword content of interest, enabling proactive intervention before an at-risk user becomes a real problem.

## IPS Policy Enhancements and Smart Filters

Creating custom IPS polices is greatly improved with a powerful but intuitive new policy editor that enables quick and easy selection of desired IPS patterns by category, severity, platform, and target type, with support for persistent smart filter lists that will automatically update as new patterns are added that match the selected criteria.

For example, an IPS policy designed specifically for protecting Linux servers and devices can easily be created simply by selecting "Linux" for the "Platform" and then as new patterns are added to address newly discovered vulnerabilities in Linux, the firewall will automatically protect against them.

## App Control Policy Enhancements and Smart Filters

Identical to the IPS Policy Enhancements mentioned above, Custom App Control Policies are also greatly improved with a powerful but intuitive new policy editor that enables quick and easy selection of

applications by category, risk, characteristics, and technology, with support for persistent smart filter lists that will automatically update as new applications are added that match the selected criteria.

For example, an App Control policy designed specifically for blocking Peer-to-Peer file sharing applications can easily be created simply by selecting "P2P" for the "Category" and then as new BitTorrent or other Peer-to-Peer applications are added to that category, the firewall will automatically enforce policy for those new apps.

### Web Filtering Enhancements

An option is now available as part of web protection to block Potentially Unwanted Applications from being downloaded.

SafeSearch enforcement has been enhanced for Bing, Google, and YouTube (Restricted Mode) to use a DNS enforcement mechanism that now enables enforcement during SSL encrypted browser sessions even if HTTPS is not being decrypted.

End user block pages have new styling and added detail, allowing users and administrators to better understand the reasons behind any blocked content.

### Streaming Media Enhancements

Streaming media applications that previously may not have functioned properly with AV scanning enabled are now handled more intelligently providing better support for services that stream audio and video.

## Management and Troubleshooting

### Firewall Rule Management

Firewall rule management is more powerful and streamlined in v17 that will make working with firewall rules easier, particularly in environments with large numbers of firewall rules.

Firewall rules are now more compact yet offer more information at-a-glance - more than doubling the number of rules that can be viewed together while also making it easier to identify what each rule is doing. Rules can now be easily grouped together and collapsed, expanded, and moved as a single object.

Each rule provides a complete overview of the source, destination, service details, and security and enforcement features governed by that rule. A mouse-over pop-up window provides even more information including basic instructions for editing rules, moving rules, or creating groups.

Groups are easily created from the action menu and providing a name and description for the group. Adding additional rules to the group can be done when creating a rule, or by selecting the group from the action menu for existing rules. Groups can be moved up and down the rule list simply by dragging-and-dropping.

Filtering and searching are fully supported and present results in a way that maintains the group structure.

### Unified Log Viewer and More Granular Logging

The amount and type of events and details being logged has greatly improved, providing better real-time visibility into firewall activity through the new unified log viewer that now aggregates all logs into a single view.

As before, the log viewer opens in a pop-up window that enables easy monitoring while working in other parts of the console. New to v17 is an aggregate real-time live view that combines all log entries together into a single view. Log entries also offer richer detail and information. You can easily switch between this new view and the previous default column view by functional area.

Powerful search allows you to instantly focus on log entries of interest simply by entering desired search criteria.

Blocked traffic is still clearly identified with red indicator to quickly identify enforcement at work.

Log data now persists across restarts and can be downloaded as a CSV file in one-click.

### Firewall Rule and Policy Test Simulator

An all-new feature in XG Firewall v17 is the new firewall rule and policy test simulator that enables instant and effortless simulation of firewall rules and web filtering policy based on user, protocol, source, destination, and time of day. This tool provides a quick and easy way to verify a policy or rule is working as expected and can be a valuable troubleshooting tool in the event users or traffic are being unexpectedly blocked.

The results of the policy or rule simulation test will indicate whether the traffic is allowed or blocked and identify the rule or web policy that's governing the traffic.

## Reporting

### Synchronized Applications Report

Get complete historical reporting on all applications identified through the Synchronized App Control feature with details on the app classifications, users, hosts, policies, and destination countries.

### Web Keyword Content Report

Identify users who are matching keyword content so you can take preventive action before a potential issue turns into a serious problem.

### Security Audit Report (SAR)

This report which is part of a Discover Mode (TAP mode) deployment, now includes a report on applications discovered by Synchronized App Control as well as additional details on client health and Security Heartbeat.

### Report Scheduling

New options for the daily reporting period of the "previous day" or the current day "since midnight" are now part of the scheduled reporting choices.

# Networking and VPN

## IKEv2 Support

IPSec VPN connections now support Internet Key Exchange (IKE) v2 enabling better interoperability with other systems. An IKEv2 IPsec profile is included out-of-the-box for convenience, enabling quick setup of IKEv2 IPsec VPN connections.

## VPN UI Enhancements

Both the IPsec Profile Configuration and IPsec Connection setup screens have been enhanced with a new more intuitive layout and automatic field validation checking to streamline setup and reduce errors.

## Wildcard Support for Domain Name Host Objects

Fully qualified domain name (FQDN) host objects now support wildcards making these objects significantly more powerful. In addition, there are a number of popular cloud service host objects fully defined out-of-the-box that can be easily applied to firewall rules and web policies with no effort.

## NAT Rule Enhancements

Business rules are now fully object-based that support forwarding of multiple ports and services in a single rule. For example, you can now forward RDP, Web and VoIP to a single server in a single business application rule. This reduces the number of rules required to support the same services and makes inbound NAT rules much more intuitive.

# Email Protection

## Smart Host

Improve the reliability of your email delivery with smart host outbound relays, allowing you to route email via an alternate set of servers (a smart host), rather than directly to the recipients server. Perfect in environments that are more complex and where email is not directly routed via the Sophos gateway.

## Greylisting

Block more spam at the gateway with Greylisting. As most spam and viruses only attempt to deliver the message once, Greylisting temporarily denies the first attempt, telling the sending mail server to try again. On the next attempt, the message is accepted and scanned as usual. If a mail server passes this test enough times it is added to the whitelist automatically, alternatively the admin can update whitelist records manually or use inbuilt presets for common senders.

## Recipient Verification

Reduce the load on XG Firewall email processing and provide senders, including customers and valued partners, with an instant response if they mis-type your email address. Recipient Verification allows XG Firewall to query the recipient's directory service via SMTP to check that a valid mailbox exists. If it does, the message is processed for spam and viruses as normal, if not the email is rejected and a bounce back is sent to the sender.

# Synchronized Security

## Synchronized Security in Discover (TAP) Mode Deployments

XG Firewall can now support Security Heartbeat™ visibility and threat identification when deployed in Discover (TAP) mode – simply connected to a mirror port on a switch. This enables XG Firewall to work alongside a customer's existing firewall, providing added visibility into threats and the health status of Sophos Endpoints on the network.

While not new, Synchronized Security and the new Synchronized App Control features are also fully supported when XG Firewall is deployed in line with an existing firewall. This delivers all the great benefits of visibility and protection that Synchronized Security provides, with the existing network infrastructure. The new fail-open bypass ports that are included with all new XG Series 1U appliances make this simple and risk free.

Together, Intercept X (which can be deployed alongside existing 3rd party endpoint protection) and XG Firewall running in line, provide a full Synchronized Security solution that can be deployed without displacing or disrupting any of the existing IT security infrastructure.

## Synchronized App Control

As mentioned in the Security and Control section of this document, Synchronized App Control is a breakthrough new Synchronized Security feature that can identify, classify and control previously unknown applications.

It utilizes Synchronized Security to solicit application information from the Endpoint for traffic that does not match any app control signature. This 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.

XG Firewall can now positively identify all applications being utilized on Sophos Endpoints. Where possible, XG Firewall will automatically classify the application and control it using existing app control policies. Administrators can also manually assign categories to discovered applications to enable app control enforcement to block or prioritize the application as desired.

# Deployment and Hardware

## Microsoft Azure High Availability

Microsoft Azure provides flexibility and global scale that provides customers immediate redundancy and business continuity benefits. New in v17, customers can further benefit from these features by deploying XG in High Availability (HA) scenarios on Azure.

Using Azure Resource Manager (ARM) templates created by Sophos, customers can deploy XG on Azure and use Azure Load Balancer Probes to determine the health status of XG and automatically failover when needed. Check out our ARM templates in our GitHub repository or take XG for a test drive and let us know what you think.

### New Hardware Support

Support for the latest XG Series hardware connectivity and features, including the new fail-open bypass ports that are standard on all new XG Series 1U appliances that make in line deployments with an existing firewall simple and risk free.

### Central Management

Firewall configuration for Central Management by Sophos Firewall Manager or Sophos Central Firewall Manager have been redesigned to be much simpler and more intuitive.

## Issues Addressed

### Open Issues Addressed

In addition to new features, this release and the previous 2017 maintenance releases have significantly improved the overall performance, reliability, and stability of XG Firewall across all areas of the product

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