XG Firewall Reviewers Guide

Contents

Welcome to XG Firewall 2
  Documentation and How-To Videos 3
  Enabling Synchronized Security 3
  Add XG Firewall to Any Network – Simply 3

Exposing Hidden Risks 4
  Control Center 4
  Synchronized Application Control 6
  Top Risk Users 8
  Rich On-Box Reporting 9

Blocking Unknown Threats 10
  Unified Rule Management 10
  Managing Your Security Posture at a Glance 11
  Enterprise-Grade Secure Web Gateway 12
  Educational Features 12
  Business Application and NAT Rule Templates 13
  Sandstorm Sandboxing 14
  Advanced Threat Protection 15

Automatic Response to Incidents 16
  Security Heartbeat 16

Add XG Firewall to Any Network – Simply 18
Welcome to XG Firewall

Thank you for choosing to review or evaluate Sophos XG Firewall. This guide provides an overview of some of the many features that differentiate XG Firewall from other firewall products available on the market and will provide a helpful aid in exploring and evaluating XG Firewall in your own network.

XG Firewall has been developed right from the start to address some of today’s top problems with existing firewalls. These are the top complaints we hear about most firewalls today:

- Lack of visibility into risks and activity on the network. Most firewalls make it too difficult to get important information and do a terrible job of surfacing what’s important.
- Lack of protection, features, or overwhelming complexity in setting them up. Most firewalls either don’t provide all the necessary technology to block the latest advanced threats, or they make it cumbersome to configure, which dramatically reduces the chances it is setup optimally.
- Lack of response to incidents on the network when they do occur. Most firewalls don’t provide any kind of insight into the presence of threats on the network and don’t offer any kind of automated response when they do.

Sophos XG Firewall has three key advantages over other network firewalls:

1. **Exposes hidden risks:** XG Firewall does a much better job at exposing hidden risks than competitors with a visual dashboard, rich on-box reporting, and unique risk insights.

2. **Blocks unknown threats:** XG Firewall makes blocking unknown threats easier and more effective than other firewalls with a full suite of advanced protection that’s very easy to setup and manage.

3. **Automatically responds to incidents:** XG Firewall with Synchronized Security automatically responds to incidents on the network thanks to Security Heartbeat™.

This guide will help you explore and evaluate the benefits of XG Firewall first hand. However, before you get started, here are some other important sources of information that will help you get set up and configured to make the most out of your XG Firewall experience.
XG Firewall Reviewers Guide

Documentation and How-To Videos

Our library of documentation and links to How-To videos to help get you setup are available here at sophos.com/get-started-xg. Extensive context-sensitive online help is also available by clicking the “Help” option in the upper right corner of the XG Firewall console.

Enabling Synchronized Security

To explore and review the benefits of Synchronized Security, here are some additional considerations:

- If you don’t already have a Sophos Central account, you can sign up for a trial at https://central.sophos.com.
- Once you have a Sophos Central Account, be sure to protect one or more of the computers on your network with either Central Endpoint Advanced or Intercept X. Either of these products on both Windows and Mac will enable Security Heartbeat with your XG Firewall. In Sophos Central, go to “Protect Devices” and download the Endpoint Protection installer for your platform of choice.
- Log in to your XG Firewall and click the “Central Synchronization” menu option to connect your Firewall with Sophos Central. You simply need to enter your Sophos Central credentials to register your XG Firewall with Sophos Central, enabling Security Heartbeat, Synchronized Application Control, and even management of your XG Firewall from Sophos Central.

Add XG Firewall to Any Network – Simply

Our latest XG Series hardware appliances offer more flexible deployment with fail-open bypass ports now standard on all 1U models and available in new FleXi Port Modules. This enables this feature on our latest 2U appliances as well. The new bypass ports enable XG Firewall to be installed in bridge mode in line with existing firewalls, and if the XG Firewall needs to be shutdown or rebooted to update the firmware, the bypass ports will allow traffic to continue to flow, ensuring no disruptions to the your network. This is a unique feature to the XG Series and enables new deployment options that are completely risk free and easy without replacing any existing network infrastructure. And what’s more, our next-gen endpoint protection, Intercept X, runs alongside any existing desktop antivirus product, enabling a complete Sophos Synchronized Security solution to be deployed in any network without replacing anything.
Exposing Hidden Risks

It's critically important for a modern firewall to parse through the mountain of information it collects, correlate data where possible, and highlight only the most important information requiring action – ideally before it's too late.

Control Center

XG Firewall’s Control Center provides an unprecedented level of visibility into activity, risks, and threats on your network.

It uses “traffic light” style indicators to focus your attention on what’s most important.

If something’s red, it requires immediate attention. If something is yellow, that’s an indication of a potential problem. And if everything is green, no further action is required.

And every widget on the Control Center offers additional information that is easily revealed simply by clicking that widget. For example, the status of interfaces on the device can be easily obtained by simply clicking the “Interfaces” widget on the Control Center.
The host, user, and source of an advanced threat is also easily determined simply by clicking the ATP [advanced threat protection] widget in the dashboard.

System graphs also show performance over time with selectable timeframes, whether you want to look at the last two hours to the last month or year. And they provide quick access to commonly used troubleshooting tools.

The live log viewer is available from every screen with just a single click. You can open it in a new window so you can keep one eye on the relevant log while working on the console. It provides two views, a simpler column based format by firewall module, as well as a more detailed unified view with powerful filter and sort options that aggregates logs from across the system into a single real-time view.
XG Firewall Reviewers Guide

If you’re like most network admins, you’ve probably wondered whether you have too many firewall rules, and which ones are really necessary versus which ones are not actually being used. With Sophos XG Firewall, you don’t need to wonder anymore.

The Active Firewall Rules widget shows a real-time graph of traffic being processed by the firewall by rule type: Business Application, User, and Network Rules. It also shows an active count of rules by status, including unused rules where you could have an opportunity to do some housekeeping. As with other areas of the Control Center, clicking any of these will drill down, in this case, to the firewall rule table sorted by the type or status of rule.

Synchronized Application Control

The problem with application control today in every next-generation firewall is that the majority of application traffic is going unidentified: it’s unclassified, unknown, generic HTTP, or generic HTTPS.

There’s a simple reason for this: all firewall app control engines rely on signatures and patterns to identify applications. And as you might expect, any custom vertical market application, like medical or financial apps, will never have signatures, and some evasive apps like bittorrent clients or VoIP and messaging apps are constantly changing their behavior and signature to evade detection and control. Many applications now use encryption to escape detection, while others have simply resorted to using generic web browser-like connections to communicate out through the firewall because port 80 and 443 are generally unblocked on most firewalls.

The end result is a complete lack of visibility into apps on the network, and you can’t control what you can’t see.

The solution to this is very elegant yet effective: Synchronized Application Control, which uses our unique Synchronized Security connection with Sophos managed endpoints.
When the firewall sees application traffic it can’t identify with signatures, it can ask the endpoint what application is generating that traffic. The endpoint can then share the executable, the path, and often its category, and pass that information back to the firewall. The firewall can then use that information to classify and control the application automatically in most situations.

If XG Firewall can’t determine the appropriate application category automatically, the admin can set the desired category or assign the app to an existing policy.

Once an application is classified – either automatically, or by the network administrator – the application is subject to the same policy controls as all other applications in that category, making it very easy to block all the unidentified apps you don’t want, and prioritize the apps you do want.

Synchronized Application Control is a breakthrough in application visibility and control, providing absolute clarity over all the applications that were previously operating on the network and going unidentified and uncontrolled.
Top Risk Users

Studies have proven that users are the weakest link in the security chain, and patterns of human behavior can be used to predict and prevent attacks. Also, usage patterns can help illustrate how efficiently corporate resources are utilized and if user policies need to be fine-tuned.

User Threat Quotient (UTQ) helps a security administrator spot users who pose a risk based on suspicious web behavior and threat and infection history. A user’s high UTQ risk score could be an indication of unintended actions due to lack of security awareness, a malware infection, or intentional rogue actions.

Knowing the user and the activities that caused risk can help the network security administrator take required actions and either educate their top risk users or enforce stricter or more appropriate policies to get their behavior under control.
Rich On-Box Reporting

XG Firewall is unique among firewall and UTM products, providing comprehensive, rich on-box reporting at no extra charge. Of course, we also offer a centralized off-box reporting platform, Sophos iView, if you prefer to do your reporting on a separate server or appliance. But most small and mid-sized organizations appreciate the ability to get full historical reporting on a single appliance without paying extra.

XG Firewall provides a comprehensive set of reports, conveniently organized by type, with several built-in dashboards to choose from. There are literally hundreds of reports with customizable parameters across all areas of the firewall, including traffic activity, security, users, applications, web, networking, threats, VPN, email, and compliance. You can easily schedule periodic reports to be emailed to you or your designated recipients, and save reports as HTML, PDF, or CSV.
Blocking Unknown Threats

Protection from the latest network threats requires a symphony of technologies all working together, and orchestrated by a master conductor – the network administrator. Unfortunately, most firewall products are more like playing a one-man-band while juggling throwing knives, with firewall rules setup in one area, web policy in another, SSL inspection somewhere else, and App Control in a whole different part of the product.

At Sophos, we not only believe you need the most advanced protection technology available, we also believe it needs to be simple to configure and manage day-to-day because misconfigured protection is often worse than having no protection.

A commitment to simplicity has always been a key part of the Sophos DNA. But perhaps more importantly, Sophos has a rare willingness to embrace change and take bold steps to do things differently in the interest of providing both better protection and a better user experience.

XG Firewall does a few things differently that make a big difference.

Unified Rule Management

Managing a firewall can be incredibly challenging, with multiple rules, policies, and security settings spread across a variety of functional areas – often with several different rules required to provide the necessary protection.

With the new XG Firewall, we took the opportunity to completely re-think the way firewall rules are organized and how your security posture is managed. Instead of having to hunt around the management console looking for the right policies, we collected all firewall rule and enforcement management into a single unified screen. You can now view, filter, search, edit, add, modify, and organize all your firewall rules in one place.

Rules for users, business applications, NAT, and networking make it easy to view only the policies you need while providing a single convenient screen for management.

Indicator icons provide important information about policies such as their type, status, enforcement, and much more.
Managing Your Security Posture at a Glance

XG Firewall makes it super easy to configure and manage all of the modern protection required and all on a single screen.

You can set up and snap in security and control for antivirus, SSL inspection, sandboxing, IPS, traffic shaping, web and app control, Heartbeat, NAT, routing, and prioritization all in one place — and all on a rule by rule, or user by user, or group by group basis.

And if you want to see exactly what any of your snap-in policies are doing, or even make changes, you can edit them in place without having to leave the firewall rule and visit another part of the product.

Flexible authentication options enable you to easily know who’s who, and include directory services such as Active Directory, eDirectory, and LDAP, as well as NTLM, RADIUS, TACACS+, RSA, client agents, or a captive portal. And Sophos Transparent Authentication Suite (STAS) provides integration with directory services like Microsoft Active Directory for easy, reliable, transparent single sign-on authentication.
XG Firewall Reviewers Guide

Enterprise-Grade Secure Web Gateway

Web protection and control is a staple in any firewall, but unfortunately, it feels like an afterthought in most firewall implementations. Our experience building enterprise-grade web protection solutions has provided us with the background and know-how to implement the kind of web policy control you would normally only find in enterprise SWG solutions costing ten times as much. We’ve implemented an all-new, top-down inheritance policy model, which makes building sophisticated policies easy and intuitive. Pre-defined policy templates, available right out of the box, are included for most common deployments – such as typical workplace environments, education CIPA compliance, and much more. It means you can be up and compliant immediately with easy fine-tuning and customization options at your fingertips.

In fact, we know that web policy is one of the most frequently changed elements on a day-to-day basis in your firewall, which is why we’ve invested heavily in making it easy for you to manage and tweak based on your user and business needs. You can easily customize users and groups, activities [comprised of URLs, categories, content filters, and file types], actions [to block, allow, or warn], and add or adjust time-of-day and day-of-week constraints.

Education Features

XG Firewall offers several features ideally suited for education environments where web policy and compliance are critical requirements. Education specific features include:

- Pre-packaged web policies for CIPA
- Content filtering and reporting on keywords
- SafeSearch and YouTube Restriction settings on a user/group policy basis
- Blockpage overrides that can be managed by teachers
- Comprehensive built-in reporting to identify potential issues early
XG Firewall Reviewers Guide

Web policies now include the option to log and monitor or even enforce policy related to dynamic content based on 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.

XG Firewall comes with CIPA compliance policy ready to go out of the box, enabling quick compliance. It also offers flexible and powerful controls over SafeSearch and YouTube restrictions on a user/group policy basis. And teachers can be granted the option to set up and manage their own policy overrides to enable their classrooms to access websites that would normally be blocked as part of their curriculum.

It's powerful web policy made simple.

Business Application and NAT Rule Templates

Anyone who's tried to set up web application firewall rules for something like Exchange, SharePoint, or a web server knows how challenging and issue-prone it can be. The range and number of settings is bewildering. But pre-defined policy templates can help you protect common business application servers quickly, easily, and with confidence. Simply select your desired server type from the drop-down list.

Once you select one of the common business applications you need to protect with your firewall, the configuration screen is prepopulated with the appropriate fields to make your job a lot simpler. You then simply enter a few details like the domain, path, and server information, and you're done.

Compare this with having to set up a WAF policy in any other product, which usually requires several screens. It’s complex and confusing. Not with XG Firewall.
Sandstorm Sandboxing

With advanced threats like ransomware becoming more targeted and evasive, there’s a dire need for behavior-based payload analysis. Up until recently, the sandboxing technology required to provide this protection was only affordable for the largest enterprises. But now, thanks to cloud-based sandboxing solutions like Sophos Sandstorm, it’s incredibly affordable for even the smallest businesses. For the first time, small and mid-size organizations are getting access to sandboxing with deep learning technology that goes well beyond the kinds of dedicated on-premises sandboxing solutions that enterprises were deploying for millions of dollars only a few years ago.

Sophos Sandstorm provides the ultimate cloud sandboxing solution, one that is simple and affordable, while providing essential protection with deep learning from the latest zero-day threats lurking in email and web payloads. It’s tightly integrated into XG Firewall and incredibly simple to setup, but because it’s cloud-based there’s no additional software or hardware required, and no impact on performance of your firewall. Suspicious email attachments and web downloads are automatically analyzed and detonated in a cloud sandbox to determine their behavior before they are allowed onto your network.

Sophos Sandstorm includes the latest protection technologies from our Intercept X next-gen endpoint product such as deep learning, exploit detection, and CryptoGuard to identify the latest threats before they get on the network.

Sophos Sandstorm provides an at-a-glance account of payload analysis on the XG Firewall Control Center and rich detailed reporting on all the files and threats analyzed and processed by your firewall.

While sandboxing technology is becoming more commonplace, XG Firewall and Sophos Sandstorm deliver the best protection made simple, at a very aggressive price, making it affordable and effective for everyone.
Advanced Threat Protection

Advanced threat protection is essential for identifying APTs, bots, and other malware lurking on your network. XG Firewall uses a sophisticated mix of malicious traffic detection, botnet detection, and command and control (C and C) call-home traffic detection. It combines IPS, DNS, and URL analysis to identify call-home traffic and immediately identify not only the infected host, but the user and process.

This sophisticated underlying protection technology provides a very simple but helpful view of advanced threats on the network. As mentioned earlier, the XG Firewall Control Center presents a simple traffic-light style indication of advanced threats on the network. When it’s red, that means the firewall has identified and blocked an advanced threat. And if you’re using Sophos Synchronized Security with your XG Firewall, it can go one step further and isolate that compromised system until it’s cleaned up to prevent any data leakage or further communication with hacker’s servers.
Automatic Response to Incidents

One of the most requested firewall features from network administrators is the ability to automatically respond to security incidents on the network.

Sophos XG Firewall is the only network security solution that is able to fully identify the source of an infection on your network and automatically limit access to other network resources in response. This is made possible with our unique Sophos Security Heartbeat that shares telemetry and health status between Sophos endpoints and your firewall.

XG Firewall uniquely integrates the health of connected hosts into your firewall rules, enabling you to automatically limit access to sensitive network resources from any compromised system until it’s cleaned up.

Not only can XG Firewall isolate endpoints from accessing other parts of the network at the firewall, it can also enlist the aid of all the healthy endpoints on the network to further isolate a compromised host and isolate it at the endpoint level.

This Lateral Movement Protection, as we call it, isolates and prevents threats or attackers from moving laterally across the network to other systems, even if they are on the same network segment or broadcast domain where the firewall can’t normally intervene. It’s an extremely simple and effective solution to the challenge of active adversaries operating on your network. And it’s only possible if your endpoint and firewall are working on a coordinated or synchronized defense.

Security Heartbeat

Sophos Security Heartbeat shares intelligence in real time using a secure link between your endpoints and your firewall. This simple step of synchronizing security products that previously operated independently creates more effective protection against advanced malware and targeted attacks.
Security Heartbeat can not only identify the presence of advanced threats instantly, it can also be used to communicate important information about the nature of the threat, the host system, and the user. And perhaps most importantly, Security Heartbeat can also be used to automatically take action to isolate or limit access to compromised systems until they can be cleaned up. It’s exciting technology that is revolutionizing the way IT security solutions identify and respond to advanced threats.

Security Heartbeat for managed endpoints behind your firewall can be in one of three states:

**Green Heartbeat** status indicates the endpoint system is healthy and will be allowed to access all appropriate network resources.

**Yellow Heartbeat** status indicates a warning that a system may have a potentially unwanted application (PUA), is out of compliance, or is experiencing other issues. You can choose which network resources a yellow heartbeat is allowed to access until the issue is resolved.

**Red Heartbeat** status indicates a system that is at risk of being infected with an advanced threat and may be attempting to call home to a botnet or command and control server. Using the Security Heartbeat policy settings in your firewall, you can easily isolate systems with a red heartbeat status until they can be cleaned up to reduce the risk of data loss or further infection.

Only Sophos can provide a solution like Security Heartbeat because only Sophos is a leader in both endpoint and network security solutions. While other vendors are starting to realize this is the future of IT security and are scrambling to implement something similar, they are all at a distinct disadvantage: they don’t own both an industry leading endpoint solution and an industry leading firewall solution to integrate together.