Contents

Welcome to XG Firewall 3
   Documentation and How-To Videos 4
   Enabling Synchronized Security 4

Exposing Hidden Risks 5
   Control Center 6
   Synchronized Application Control 8
   Top Risk Users 10
   Flexible Reporting Options 11

Blocking Unknown Threats 12
   High-speed Security 12
   Unified Rule Management 13
   Managing Your Security Posture at a Glance 14
   Enterprise-Grade Secure Web Gateway 15
   Educational Features 16
   Simplified NAT Configuration 17
   Sandstorm Sandboxing 18
   Threat Intelligence 19
   Advanced Threat Protection 19

Automatic Response to Incidents 20
   Security Heartbeat 21
   It’s a Zero Trust World 22

Add XG Firewall to Any Network – Simply 23
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 poor job surfacing what’s important.
- Lack of protection and 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 set up optimally.
- Lack of response to incidents on the network when they do occur. Most firewalls provide little, if any, insight into the presence of threats on the network. They also don’t respond automatically 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 exposing hidden risks than other firewalls by providing a visual dashboard, rich cloud-based reporting, and unique risk insights.

2. **Blocks unknown threats**: XG Firewall makes blocking unknown threats faster and more effective than other firewalls through a full suite of advanced protection capabilities that are very easy to set up and manage.

3. **Automatically responds to incidents**: XG Firewall with Synchronized Security automatically responds to incidents on the network thanks to Sophos Security Heartbeat™ which shares real-time intelligence between your endpoints and your firewall.

This guide will help you explore and evaluate the benefits of XG Firewall firsthand. 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.
Documentation and How-To Videos

Our library of documentation and links to How-To videos to help you set up 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 Sophos Intercept X, which 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 into 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.
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.

Xstream SSL Inspection

There’s a perfect storm brewing around encrypted traffic. According to Google, the volume of encrypted traffic on networks has grown to over 80%. This increase represents an opportunity for cybercriminals to launch attacks that are hidden and therefore difficult to detect. After all, you can stop what you can’t see. Unfortunately, most organizations are powerless to do anything about it because their current firewall lacks the performance necessary to utilize TLS/SSL inspection without slowing down dramatically.

XG Firewall, with its new Xstream SSL inspection engine, has a much higher capacity for concurrent connections and offers flexible policy tools to make intelligent decisions about what should and can be scanned, offloading where appropriate. Using the SSL policy tools, organizations can create enterprise-grade TLS/SSL policies related to undecryptable traffic, certificates, protocols, cipher enforcement options, and more. XG Firewall supports TLS 1.3 and all modern crypto suites across every port and application in the system.

Additional tools available right on the dashboard enable administrators to see exactly how much network traffic is encrypted, and how it’s being handled. XG Firewall does a much better job at surfacing this information than other solutions, particularly with how it highlights errors that are encountered due to certificate validation or websites that don’t support the latest encryption standards.

Administrators can also pop up a detailed window to see exactly which sites are problematic, and why, as well as users experiencing issues. From there, they can take action directly to exclude the application or site from decryption to prevent further issues. No other SSL inspection solution offers the same accessibility to this information.
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 to you.

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.

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 obtained by clicking the “Interfaces” widget on the Control Center.
The host, user, and source of an advanced threat can also be determined by clicking the ATP (advanced threat protection) widget in the dashboard.

System graphs show performance over time with selectable timeframes, whether you want to look at the last two hours, the last month or the past 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 to 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.
If you’re like most network admins, you’ve probably wondered whether you have too many firewall rules, and which ones are necessary versus those that 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 according to rule type: Business Application, User, and Network Rules. It also shows an active count of rules by status, including unused rules that you may want to remove. 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 every next-generation firewall faces with application control today is that most application traffic goes unidentified: it’s categorized as 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 such as medical or financial apps will never have signatures. 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 simply resort to using generic web browser-like connections to communicate out through the firewall because most don’t block ports 80 and 443.

The 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.
Here’s how it works. When the firewall sees application traffic it can’t identify with signatures, it asks the endpoint which 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 then uses the information to classify and control the application automatically in most situations.

![Applications](image)

If XG Firewall can’t determine the appropriate application category automatically, the administrator 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 unidentified and uncontrolled applications that were previously operating on the network.
Top Risk Users

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

Sophos 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 may indicate unintended actions due to a lack of security awareness, a malware infection, or intentional rogue actions.

Knowing the user and the activities that cause risk can help network security administrators take required actions and either educate top risk users or enforce stricter or more appropriate policies to change their behavior.
Flexible Reporting Options

XG Firewall is unique among NGFW and UTM products, providing flexible cloud-based and on-box reporting options with a high degree of customization at no extra charge. Sophos Central Firewall Reporting (CFR) enables organizations to gain deeper insight into network activity through analytics. With its comprehensive set of built-in reports and the tools to create hundreds of variations, CFR offers actionable intelligence on user behavior, application usage, security events, and more. Interactive reports and an at-a-glance report dashboard enable administrators to drill down into the syslog data stored in your Sophos Central account for a granular view that is presented in a visual format for easy understanding. The data can then be analyzed for trends that could identify gaps in the security posture and highlight the need for potential policy change.

XG Firewall also provides on-box reporting. Choose from a comprehensive set of reports, conveniently organized by type, with several built-in dashboards. There are 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 operate more like a one-man-band who plays while juggling throwing knives, with firewall rules set up in one area, web policies in another, TLS/SSL inspection somewhere else, and App Control in a completely different part of the product.

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

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 the necessary steps to do things differently in the interest of providing both better protection and ultimately a better user experience.

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

High-speed Security

Firewall performance shouldn’t slow down when you turn on the security you need to keep your network safe from threats. One of the core components of XG Firewall’s Xstream packet processing architecture is a high-speed Deep Packet Inspection (DPI) engine. The DPI engine provides proxyless, single-pass security scanning for IPS, web, antivirus, and App Control as well as our Xstream SSL inspection.

When a new connection is established, it is processed by the firewall stack, which makes decisions about whether to allow, block, or scan the traffic for threats. If the traffic requires security scanning, it forwards the packets on to the proxyless high-performance streaming DPI engine which scans the packets, even if they’re encrypted. This is only used for the initial few packets. After that, the firewall stack steps out of the way and offloads the processing completely to the DPI engine. This significantly improves latency and performance.

Then, if the stream is considered secure and no longer requires further inspection, the DPI engine can completely offload the flow to the Sophos Network Flow FastPath, which provides an accelerated path for trusted traffic. This boosts performance dramatically by freeing up other resources from inspecting traffic that doesn’t need it.
Unified Rule Management

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

With 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, SSL/TLS inspection, 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, and enforcement, plus much more.
Managing Your Security Posture at a Glance

Whether through your Sophos Central account in the cloud or the XG Firewall user interface, Sophos makes it incredibly easy to configure and manage everything needed for modern protection and do it from on a single screen.

You can set up and snap in security and control for antivirus, TLS/SSL inspection, sandboxing, IPS, traffic shaping, web and app control, Security Heartbeat, NAT, routing, and prioritization all in one place — and all on a rule by rule, 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, Kerberos, RADIUS, TACACS+, RSA, client agents, or a captive portal. And Sophos Transparent Authentication Suite (STAS) provides integration with directory services such as Microsoft Active Directory for easy, reliable, and transparent single sign-on authentication.

**Enterprise-Grade Secure Web Gateway**

Web protection and control is a staple of 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 knowhow to deploy the kind of web policy control you would normally only find in enterprise secure web gateway (SWG) solutions costing 10 times as much. We’ve implemented a top-down inheritance policy model that 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, CIPA compliance for education, 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 policies 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 compliance
- Content filtering and reporting on keywords
- SafeSearch and YouTube Restriction settings on a user/group policy basis
- Block page overrides that can be managed by teachers
- Comprehensive built-in reporting to identify potential issues early

Web policies now include the option to log, monitor, and 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 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 helps with CIPA compliance right 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 the curriculum.

It’s powerful web policy made simple.
Simplified NAT Configuration

Anyone who’s tried to configure NAT (Network Address Translation) rules knows how challenging this can be. However, it doesn’t have to be. XG Firewall includes full enterprise NAT capabilities for powerful and flexible NAT configurations including Source NAT (SNAT) and Destination NAT (DNAT) in a single rule with granular selection criteria. To make complex DNAT simpler, an easy-to-use wizard walks you through the process of creating a full NAT configuration in just a few clicks. Administrators can also take advantage of the convenient Linked NAT option when creating a firewall rule. Linked NAT will automatically create a corresponding NAT configuration rule, further reducing time spent creating and configuring NAT rules.
Sandstorm Sandboxing

With advanced threats like ransomware becoming more targeted and evasive, there’s a dire need for behavior-based payload analysis. 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 have access to sandboxing with deep learning technology that goes well beyond the capabilities of dedicated on-premises sandboxing solutions that enterprises were deploying for millions of dollars only a few years ago.

Sophos Sandstorm is 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.

To identify the latest threats, we integrated the latest protection technologies from our industry-leading next-gen endpoint product, Intercept X, into Sophos Sandstorm, including deep learning, exploit detection, and CryptoGuard.

Sophos Sandstorm also 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. In parallel with full sandbox analysis, all suspicious files are subject to threat intelligence analysis. Files are checked against SophosLabs’ massive threat intelligence database and subjected to our industry-leading deep learning, which identifies new and unknown malware quickly and efficiently – often rendering a verdict in seconds – to stop the latest zero-day threats before they get on the network.

While sandboxing technology has become more commonplace, XG Firewall with Sophos Sandstorm delivers the best protection made simple, at a very aggressive price, making it effective and affordable for everyone.
Threat Intelligence

As we’ve discussed, when the Xstream DPI engine performs AV analysis on a file and determines there is active code, it sends the file to Sophos Sandstorm for dynamic run-time analysis in the cloud. In parallel, the file is sent to SophosLabs for immediate threat intelligence analysis using our industry-leading deep learning technology where it conducts a thorough analysis on the file to identify any threat indicators. And just like Sophos Intercept X, it identifies previously unseen malware and threats almost instantly. When combined with Sophos Sandstorm, the level of protection against the latest zero-day threats is incredible, enabling XG Firewall to secure the network from the latest email and web-based attacks.

The results for both Threat Intelligence and Sandstorm analysis are provided together on a Threat Intelligence widget on the Control Center. A full detailed view is available with a single click that takes you to the Threat Intelligence tab of the XG Firewall console. Here you can see the result of every file analyzed along with its verdict – suspicious, malicious, known clean, or likely clean – with high confidence.

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 & C) call-home traffic detection. It combines IPS, DNS, and URL analysis to recognize 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 yet 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. A red light indicates 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 been cleaned to prevent any data leakage or further communication with the 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 fully identifies the source of an infection on your network and automatically limits the infected device’s access to other network resources in response. This is made possible with our unique Sophos Security Heartbeat, which shares telemetry and health status between Sophos-managed 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 decontaminated.

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 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 normally can’t intervene. It’s an extremely intuitive 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 together on a coordinated or synchronized defense.
Security Heartbeat

Sophos Security Heartbeat shares intelligence in real time using a secure link between your Sophos-managed endpoints and your XG Firewall. This simple step of synchronizing security products that previously operated independently creates more effective protection against advanced malware and targeted attacks.

Security Heartbeat not only identifies 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 automatically take action to isolate or limit access to compromised systems until they are free of malware. It’s exciting technology that has revolutionized 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 device is healthy and allowed to access all appropriate network resources.

**Yellow Heartbeat** status indicates a warning that a device 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 can access until the issue is resolved.

**Red Heartbeat** status indicates a device 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 to reduce the risk of data loss or stop the infection from spreading.

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 that integrate together.
It’s a Zero Trust World

Trust has become a dangerous word in IT, especially when that trust is implicit. Creating a large, sealed-off corporate perimeter and trusting everything inside has proven to be a flawed design.

Zero trust is a holistic approach to security that addresses these changes and how organizations work and respond to threats. It’s a model and a philosophy for how to think about and do security.

No one and no thing should be automatically trusted, whether inside or outside of the corporate network. Eventually, however, something needs to be trusted. With Zero trust, this trust is temporary and established from multiple sources of data, and it’s constantly re-evaluated.

Zero trust enables us to control our entire estate, from inside the office out to the cloud platforms we use. No more lack of control outside the corporate perimeter, or struggles with remote users.

How do we move towards Zero trust and take advantage of all the benefits it offers? While no one can provide Zero trust as a singular solution, Sophos has a wide portfolio of security technologies and controls that accelerates and simplifies your journey to Zero trust.

**Sophos Central:** Our cloud-based cybersecurity platform puts these disparate and complementary technologies into a single hub to help you orchestrate and monitor your Zero trust network.

**Synchronized Security:** Cybersecurity that continuously shares information between systems, providing insight and visibility to one another.

**XG Firewall:** Create segments or micro-perimeters around users, devices, apps, networks, and more.

**Server Protection and Intercept X:** Assign a Device Health status for every device so that, in the event one is compromised, the devices can be automatically isolated and blocked from connecting with other devices.

**Managed Threat Response (MTR):** A service that monitors all user activity across the network and identifies potentially compromised user credentials.
Add XG Firewall to Any Network – Simply

Our XG Series hardware appliances offer flexible deployment options with fail-open bypass ports now standard on all 1U models and available in FleXi Port modules. It’s also enabled on our 2U appliances as well. The new bypass ports allow XG Firewall to be installed in bridge mode in line with existing firewalls, and if the XG Firewall needs to be shut down or rebooted to update the firmware, the bypass ports provide business continuity by allowing traffic to continue to flow, ensuring no disruptions to your network.

This feature is unique to the XG Series and enables new deployment options that are free of risk and easy to install without replacing any existing network infrastructure. And what’s more, our next-gen Intercept X endpoint protection runs alongside any existing desktop antivirus product, enabling a complete Sophos Synchronized Security solution to be deployed in any network without replacing anything.

Sophos XG Firewall: It’s cybersecurity made simple.

---

Request Pricing

Request a no-obligation quote customized to your needs at sophos.com/firewall-quote