Solution Brief

XG Firewall

v18

SOPHOS
Cybersecurity evolved.

Contents

Solution Brief: XG Firewall

Network firewalls are evolving, and the latest generation is very different from its predecessors. We continue to see a shift in the threat landscape, and a dramatic rise in the number and complexity of security systems that protect against cyberattacks. These changes, combined with the overwhelming amount of data produced, have created a dangerous situation that requires a much different approach to network security, one that makes it essential security systems work together, simplify and streamline workflows, and parse through enormous volumes of data to focus attention on exactly what's important without negatively impacting performance. It also requires new approaches to security integration, new management systems, and new ways of identifying and responding to risks and threats.

The Evolution of Firewalls

Early firewalls operated at lower layers of the network stack, providing basic routing and packet filtering based on port and protocol inspection to forward or drop traffic. These firewalls were effective at stopping very basic attempts by hackers to infiltrate the network.

Network security has been forced to evolve as threats have shifted from attacking the network directly to infecting systems and spreading to others on the network. For most of the past decade, cybercriminals have built up a vast repertoire of automation, coupled with exploitable vulnerabilities, to rapidly attack targets and evade security measures or protection at the network and endpoint levels. This use of automation has taken on myriad forms, from exploit kits that trap browsers and weaponized MS Office files to malicious spam email that thoroughly obfuscates the threat it poses to victims and their technology. Over time, organizations have been forced to add additional network security appliances to their network perimeter for intrusion prevention, web filtering, anti-spam, remote access (VPN), and web application firewalls (WAF). The UTM (Unified Threat Management) appliance evolved out of the burden of managing an array of network security products – UTM solutions allowed organizations to consolidate everything into a single appliance.

Firewall technology has evolved as well, moving up the stack to Layer 7 and beyond to identify and control specific application traffic. Firewalls also grew to incorporate technologies to more deeply inspect the contents of network packets and hunt for threats. They also gained the ability to control traffic based on the originating user or application, not just by traffic type . This shift from ports and protocols to applications and users spawned a category of network protection known as “next-generation firewalls" (NGFWs).

A next-generation firewall is one that provides traditional stateful firewall inspection along with deep packet inspection that includes intrusion prevention, application awareness, user-based policies, and the ability to inspect encrypted traffic.

Network security continues to change and grow to meet the ever-evolving threat landscape. Modern threats such as ransomware, cryptojacking, and botnet malware are more advanced, evasive, and targeted than ever before. These advanced persistent threats (APTs) use techniques that create a new zero-day threat with every instance, and can be extremely challenging for signature-based systems to detect until it’s too late.

Most organizations at any given time have compromised systems on their network that are victims either of an APT or botnet, and in many cases, they’re not even aware of these infections. Unfortunately, it’s a pervasive problem.

The threat landscape is currently undergoing yet another major transformation. Sophisticated attackers are turning to more targeted and inherently unpredictable manual network hacks, using brute force to gain a foothold on the network, and striking out from there as if they were a resident network administrator. In some respects, we’ve come full circle with attacks now taking advantage of age-old security issues like weak passwords.

The nature of the current threat and network landscape is creating the need for fundamental changes in the approach to network security.

First Network security systems must now integrate new technologies to identify malicious behavior in network payloads without the use of traditional antivirus signatures. Technologies such as sandboxing and machine learning that, until recently, were a solution only large enterprises could afford have become extremely affordable for small and mid-sized organizations, and are now an essential part of an effective defense against modern malware and zero-day attacks.

Second Security systems that used to be isolated and independent, such as the firewall and endpoint, now need to be integrated and work together to detect, identify, and respond to advanced threats quickly and efficiently before they can cause significant damage.

Third New dynamic application control technologies are required to properly identify and manage unknown applications, given the growing ineffectiveness of signature-based engines to identify the latest app protocols, custom apps, and apps increasingly reliant on generic HTTP/HTTPS protocols.

Fourth The use of HTTPS encryption to secure web sessions continues to grow. So too does cybercriminal use of encryption to disguise malware attacks, which can create an enormous blind spot that hackers can exploit. This makes it essential that modern network security systems be able to scan encrypted traffic for hidden threats.

Fifth The traditional model for security has been "Trust, but verify." However, it assumes everything inside the network is good and everything outside is bad. Zero Trust directs us to never trust something blindly. Instead, we must verify anything and everything that is trying to connect to our systems before granting access.

To make matters worse, most modern firewalls have become increasingly complicated, often leveraging several separate but loosely integrated products to tackle different threat vectors and compliance requirements. As a result, the management burden for the typical network administrator has reached unsustainable levels while the amount of information and data these systems produce is simply indigestible.

In fact, in a Firewall Satisfaction Survey of IT administrators, several common issues were identified with most firewalls in use today:

- They make it difficult and time-consuming to identify and locate necessary information
- They do not provide adequate visibility into threats and risks on the network
- They suffer a substantial performance decrease when inspecting encrypted traffic for threats
- They have plenty of features but make it too difficult to figure out how to use them

Sophos XG Firewall

Sophos XG Firewalls are developed right from the start to address today's top problems that plague existing firewalls while also providing a platform designed specifically to tackle the evolving threat and network landscape. XG Firewall brings a fresh approach to the way you identify hidden risks, protect against threats, and respond to incidents without taking a performance hit. Our Xstream Architecture for XG Firewall utilizes a packet processing architecture that delivers extreme levels of visibility, protection, and performance.

XG Firewall provides unrivaled visibility into risky users, unwanted applications, suspicious payloads, and persistent threats. It tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain. And unlike legacy firewalls, XG Firewall communicates with other security systems on the network, enabling it to become your trusted enforcement point to contain threats and block malware from spreading or exfiltrating data out of the network – automatically – in real time.

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

1. Exposes hidden risks XG Firewall does a far better job exposing hidden risks than other solutions through a visual dashboard, rich on-box and cloud reporting, and unique risk insights.

2. Blocks unknown threats XG Firewall makes blocking unknown threats faster, easier and more effective than other firewalls with 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.

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't 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 un-decryptable 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.

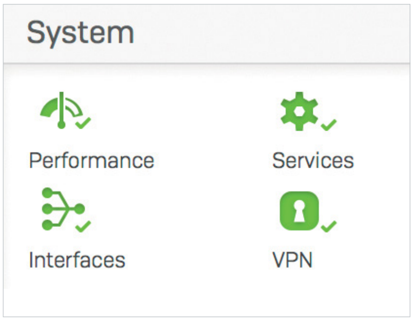
Administrators can also pop up a detailed window to see exactly which sites are problematic, and why, as well as users experiencing issues. From there, they can take action directly to exclude the application or site from decryption to prevent further issues. No other SSL inspection solution offers the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

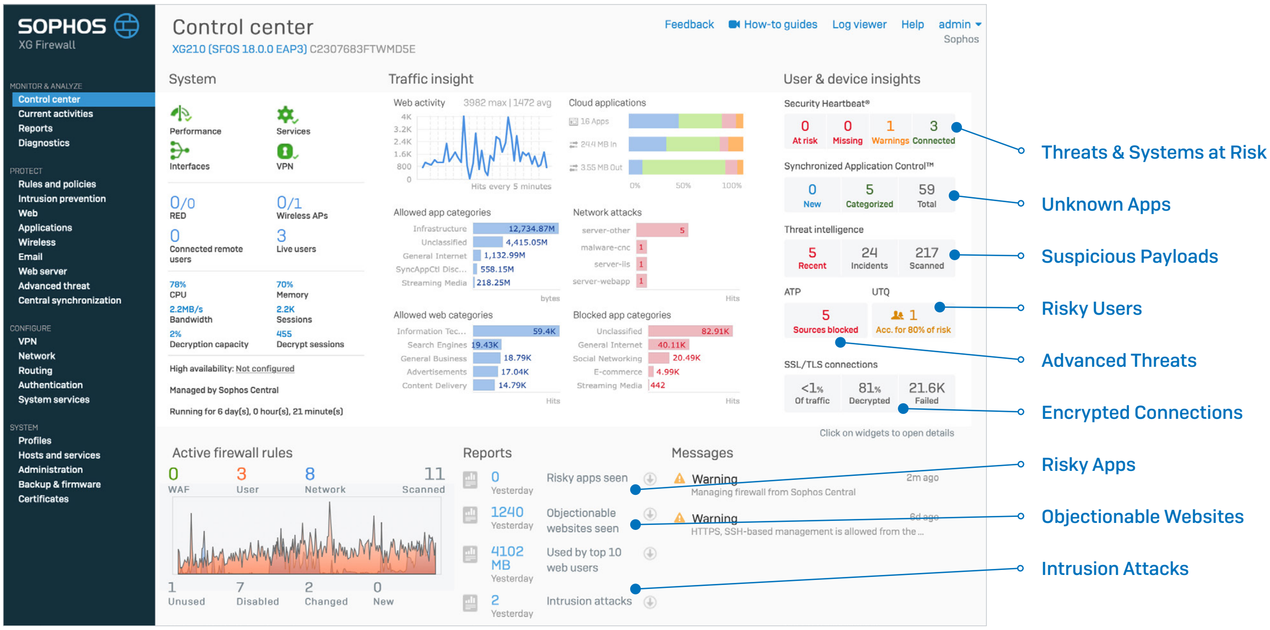
Control Center

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. Yellow indicates a potential problem. And if everything is green, no further action is required.





Threats & Systems at Risk

Unknown Apps

Suspicious Payloads

Risky Users

Advanced Threats

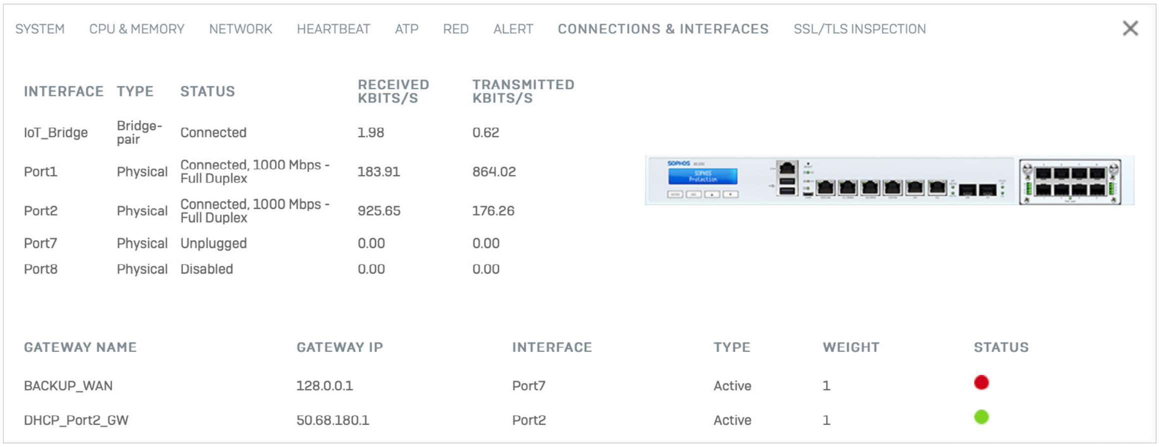
Encrypted Connections

Risky Apps

Objectionable Websites

Intrusion Attacks

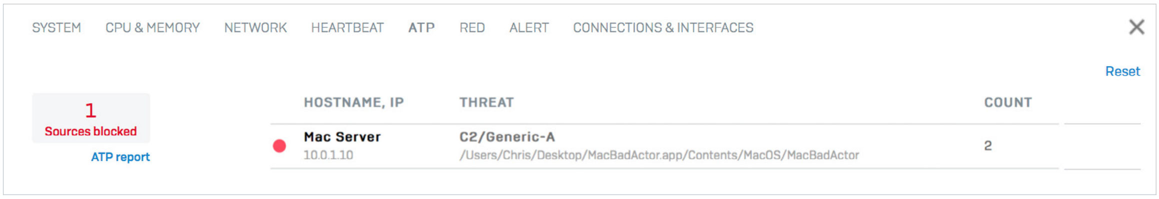
Every widget on the Control Center offers additional information that is easily revealed simply by clicking that widget. For example, the status of interfaces on the device can be obtained by clicking the "Interfaces" widget on the Control Center.



INTERFACE	TYPE	STATUS	RECEIVED KBITS/S	TRANSMITTED KBITS/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	176.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

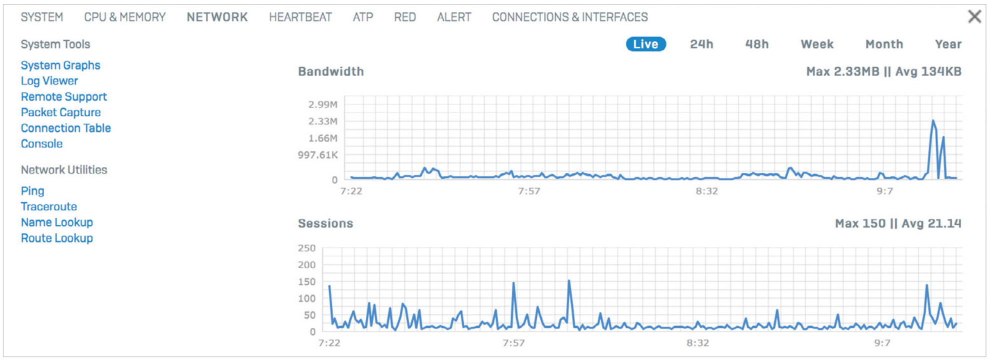
GATEWAY NAME	GATEWAY IP	INTERFACE	TYPE	WEIGHT	STATUS
BACKUP_WAN	128.0.0.1	Port7	Active	1	🔴
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	🟢

The host, user, and source of an advanced threat are also easily determined simply by clicking the ATP (advanced threat protection) widget in the dashboard.

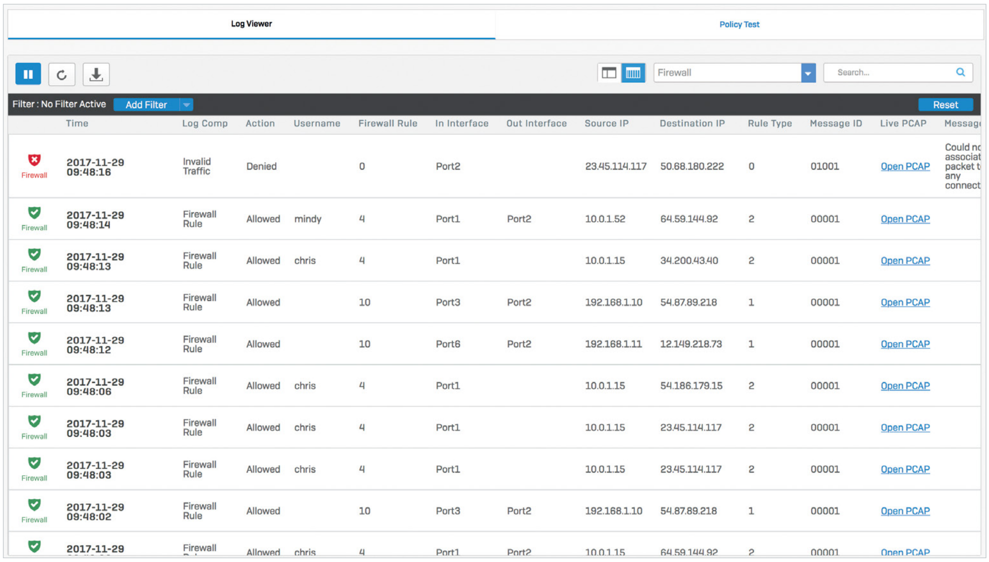


	HOSTNAME, IP	THREAT	COUNT
🔴	Mac Server 10.0.1.10	C2/Generic-A /Users/Chris/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2

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 to resolve potential issues.

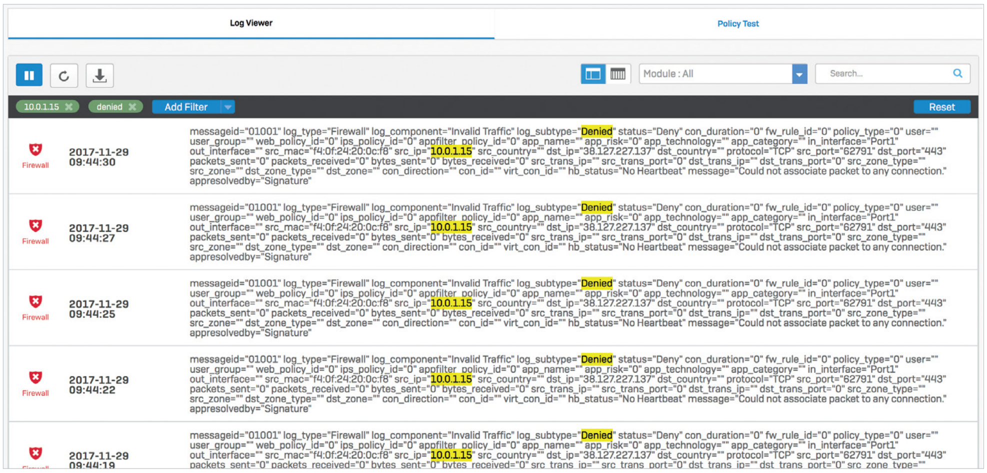


The live log viewer is available from every screen with just a single click. You can open it in a new window to keep one eye on the relevant log while working on the console. It provides two views, a simpler column-based format by firewall module, as well as a more detailed unified view with powerful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



	Time	Log Comp	Action	Username	Firewall Rule	In Interface	Out Interface	Source IP	Destination IP	Rule Type	Message ID	Live PCAP	Messag
Firewall	2017-11-29 09:48:16	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could nc associat packet t any connect
Firewall	2017-11-29 09:48:14	Firewall Rule	Allowed	mindy	4	Port1	Port2	10.0.1.52	64.59.144.92	2	00001	Open PCAP	
Firewall	2017-11-29 09:48:13	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	34.200.43.40	2	00001	Open PCAP	
Firewall	2017-11-29 09:48:13	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.89.218	1	00001	Open PCAP	
Firewall	2017-11-29 09:48:12	Firewall Rule	Allowed		10	Port6	Port2	192.168.1.11	12.149.218.73	1	00001	Open PCAP	
Firewall	2017-11-29 09:48:06	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	54.186.179.15	2	00001	Open PCAP	
Firewall	2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
Firewall	2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
Firewall	2017-11-29 09:48:02	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.89.218	1	00001	Open PCAP	
	2017-11-29	Firewall	Allowed	chris	4	Port1	Port2	10.0.1.15	64.59.144.92	2	00001	Open PCAP	

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



Firewall 2017-11-29 09:44:30

```
messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user=""
user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="" app_risk="0" app_technology="" app_category="" in_interface="Port1"
out_interface="" src_mac="f4:0f:24:20:0c:f8" src_ip="10.0.1.15" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="62791" dst_port="443"
packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone_type=""
src_zone="" dst_zone_type="" dst_zone="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection."
appresolvedby="Signature"
```

Firewall 2017-11-29 09:44:27

```
messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user=""
user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="" app_risk="0" app_technology="" app_category="" in_interface="Port1"
out_interface="" src_mac="f4:0f:24:20:0c:f8" src_ip="10.0.1.15" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="62791" dst_port="443"
packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone_type=""
src_zone="" dst_zone_type="" dst_zone="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection."
appresolvedby="Signature"
```

Firewall 2017-11-29 09:44:25

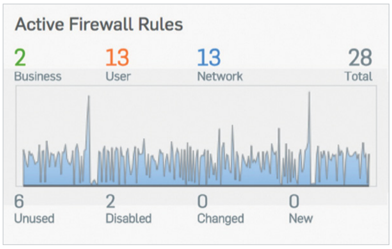
```
messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user=""
user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="" app_risk="0" app_technology="" app_category="" in_interface="Port1"
out_interface="" src_mac="f4:0f:24:20:0c:f8" src_ip="10.0.1.15" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="62791" dst_port="443"
packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone_type=""
src_zone="" dst_zone_type="" dst_zone="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection."
appresolvedby="Signature"
```

Firewall 2017-11-29 09:44:22

```
messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user=""
user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="" app_risk="0" app_technology="" app_category="" in_interface="Port1"
out_interface="" src_mac="f4:0f:24:20:0c:f8" src_ip="10.0.1.15" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="62791" dst_port="443"
packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone_type=""
src_zone="" dst_zone_type="" dst_zone="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection."
appresolvedby="Signature"
```

2017-11-29 09:44:19

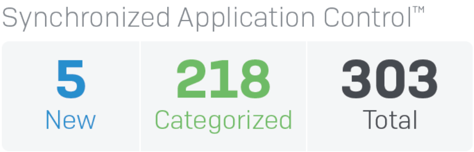
```
messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user=""
user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="" app_risk="0" app_technology="" app_category="" in_interface="Port1"
out_interface="" src_mac="f4:0f:24:20:0c:f8" src_ip="10.0.1.15" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="62791" dst_port="443"
packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone_type=""
```



The Active Firewall Rules widget shows a real-time graph of traffic 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, providing you with 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 rules table sorted by the type or status of rule.

Synchronized Application Control

The problem with application control in today's next-generation firewalls is that most application traffic goes unidentified: it's either unclassified or labelled as unknown, generic HTTP, or generic HTTPS.

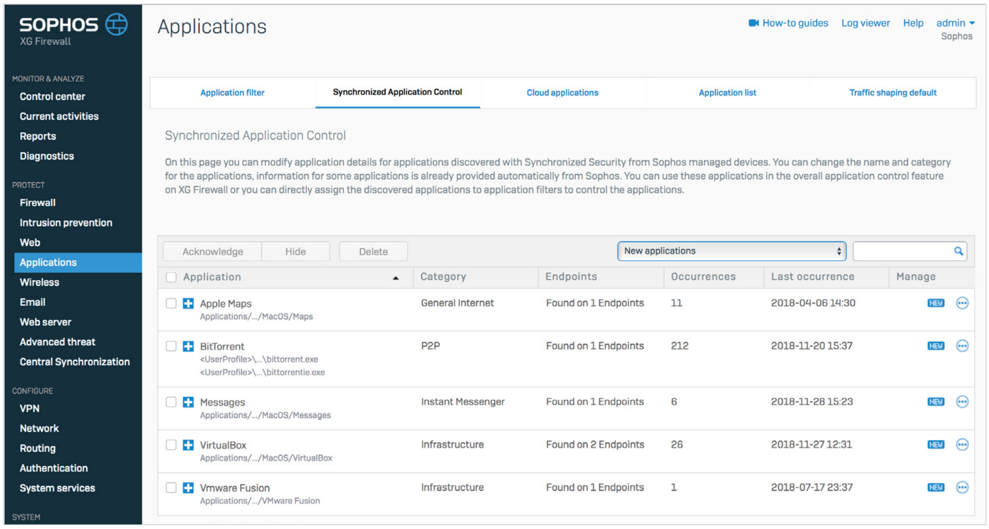

Synchronized Application Control™

5	218	303
New	Categorized	Total

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, custom vertical market applications such as medical and financial apps will never have signatures. Other evasive apps like BitTorrent clients and VoIP as well as messaging apps are constantly changing their behavior and signature to evade detection and control. Many of them 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 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: Sophos Synchronized Application Control, which uses our unique Synchronized Security connection with Sophos managed endpoints.

Here's how it works. When the XG 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



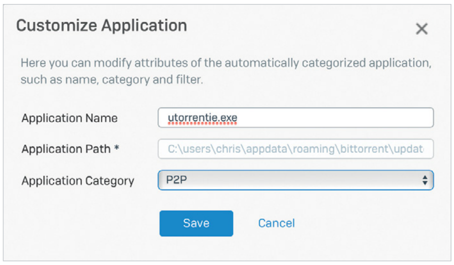
Synchronized Application Control

On this page you can modify application details for applications discovered with Synchronized Security from Sophos managed devices. You can change the name and category for the applications, information for some applications is already provided automatically from Sophos. You can use these applications in the overall application control feature on XG Firewall or you can directly assign the discovered applications to application filters to control the applications.

☐ Application	Category	Endpoints	Occurrences	Last occurrence	Manage
☐ Apple Maps Applications/.../MacOS/Maps	General Internet	Found on 1 Endpoints	11	2018-04-06 14:30	NEW
☐ BitTorrent <UserProfile>\...\bittorrent.exe <UserProfile>\...\bittorrentie.exe	P2P	Found on 1 Endpoints	212	2018-11-20 15:37	NEW
☐ Messages Applications/.../MacOS/Messages	Instant Messenger	Found on 1 Endpoints	6	2018-11-28 15:23	NEW
☐ VirtualBox Applications/.../MacOS/VirtualBox	Infrastructure	Found on 2 Endpoints	26	2018-11-27 12:31	NEW
☐ Vmware Fusion Applications/.../VMware Fusion	Infrastructure	Found on 1 Endpoints	1	2018-07-17 23:37	NEW

pass that information back to the firewall. The firewall can then use this information to classify and control the application automatically in most situations.

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.



Customize Application

Here you can modify attributes of the automatically categorized application, such as name, category and filter.

Application Name: utorrentie.exe

Application Path *: C:\users\chris\appdata\roaming\bittorrent\updat

Application Category: P2P

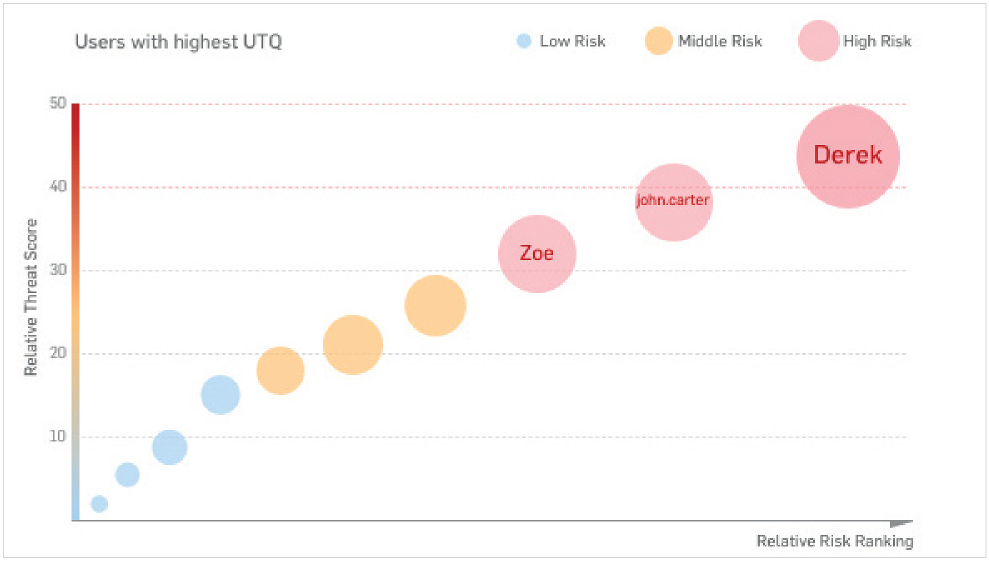
Once an application is classified – either automatically or by the network administrator – the application is subject to the same policy controls as all other applications in that category, making it very easy to block all the unidentified apps you don't want, and prioritize the apps you do want.

Synchronized Application Control is a breakthrough in application visibility and control, providing absolute clarity over every application in use on the network including those that were previously unidentified or uncontrolled.

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 and used 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.

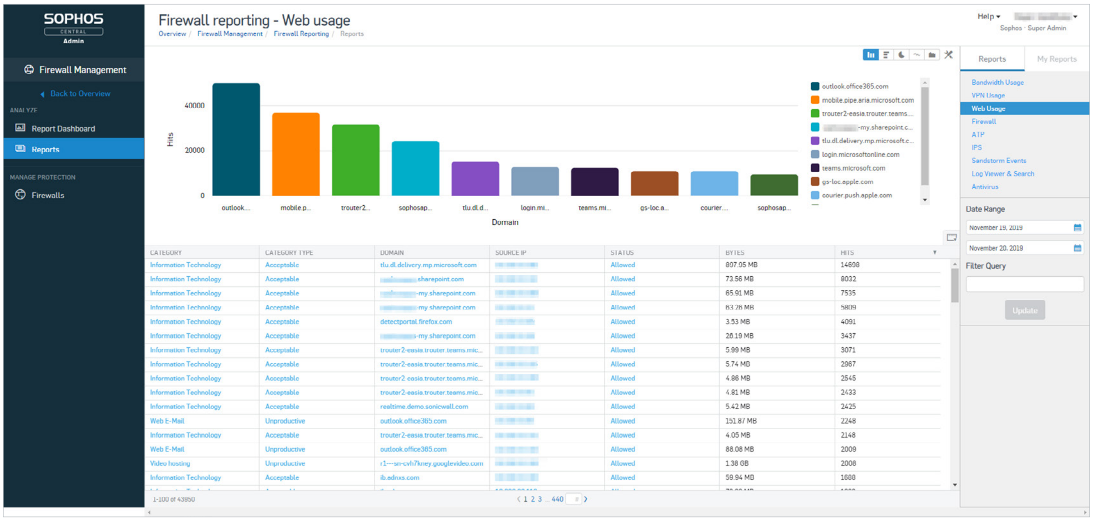
Sophos User Threat Quotient (UTQ) helps security administrators spot users who pose a risk based on suspicious web behavior and threat and infection history. A user's high UTQ risk score may indicate unintended actions due to a lack of security awareness, a malware infection, or intentional rogue actions.



Knowing the user and the activities that caused a risk helps network security administrators take required actions and either educate top risk users or enforce stricter or more appropriate policies to get user behavior under control.

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.



CATEGORY	CATEGORY TYPE	DOMAIN	SOURCE IP	STATUS	BYTES	HITS
Information Technology	Acceptable	tlu.dl.delivery.mp.microsoft.com	[redacted]	Allowed	897.95 MB	14698
Information Technology	Acceptable	[redacted].sharepoint.com	[redacted]	Allowed	73.56 MB	8032
Information Technology	Acceptable	[redacted]-my.sharepoint.com	[redacted]	Allowed	65.91 MB	7535
Information Technology	Acceptable	[redacted]-my.sharepoint.com	[redacted]	Allowed	63.26 MB	5809
Information Technology	Acceptable	detectportal.firefox.com	[redacted]	Allowed	3.53 MB	4091
Information Technology	Acceptable	[redacted]-my.sharepoint.com	[redacted]	Allowed	26.19 MB	3437
Information Technology	Acceptable	trouter2-easia.trouter.teams.mic...	[redacted]	Allowed	5.99 MB	3071
Information Technology	Acceptable	trouter2-easia.trouter.teams.mic...	[redacted]	Allowed	5.74 MB	2967
Information Technology	Acceptable	trouter2-easia.trouter.teams.mic...	[redacted]	Allowed	4.86 MB	2545
Information Technology	Acceptable	trouter2-easia.trouter.teams.mic...	[redacted]	Allowed	4.81 MB	2433
Information Technology	Acceptable	realtime.demo.sonicwall.com	[redacted]	Allowed	5.42 MB	2425
Web E-Mail	Unproductive	outlook.office365.com	[redacted]	Allowed	151.87 MB	2248
Information Technology	Acceptable	trouter2-easia.trouter.teams.mic...	[redacted]	Allowed	4.05 MB	2148
Web E-Mail	Unproductive	outlook.office365.com	[redacted]	Allowed	88.08 MB	2009
Video hosting	Unproductive	r1---sn-cvh7kney.googlevideo.com	[redacted]	Allowed	1.38 GB	2008
Information Technology	Acceptable	ib.adnxs.com	[redacted]	Allowed	59.94 MB	1688

1-100 of 43950 ‹ 1 2 3 ... 440 ›

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 firewalls 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 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 proxy-less, single-pass security scanning for IPS, Web, AV, and App Control as well as our Xstream SSL inspection.

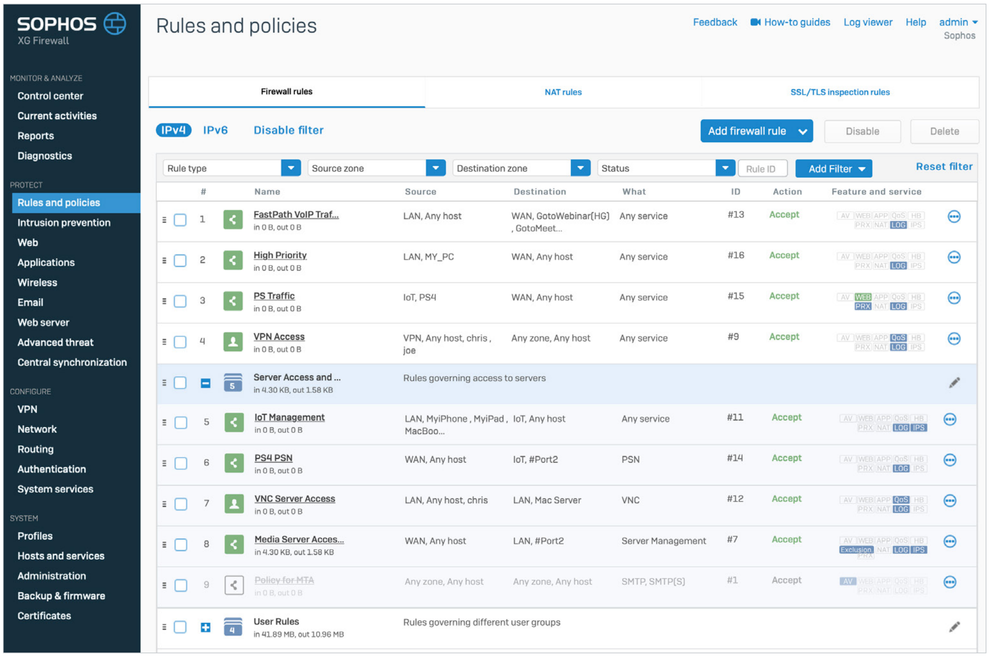
When a new connection is established, it is processed by the firewall stack which makes decisions about whether to allow, block, or scan the traffic for threats. If the traffic requires security scanning, it forwards the packets on to the proxy-less high-performance streaming DPI engine which scans the 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, there's a lot to do.

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 and policies

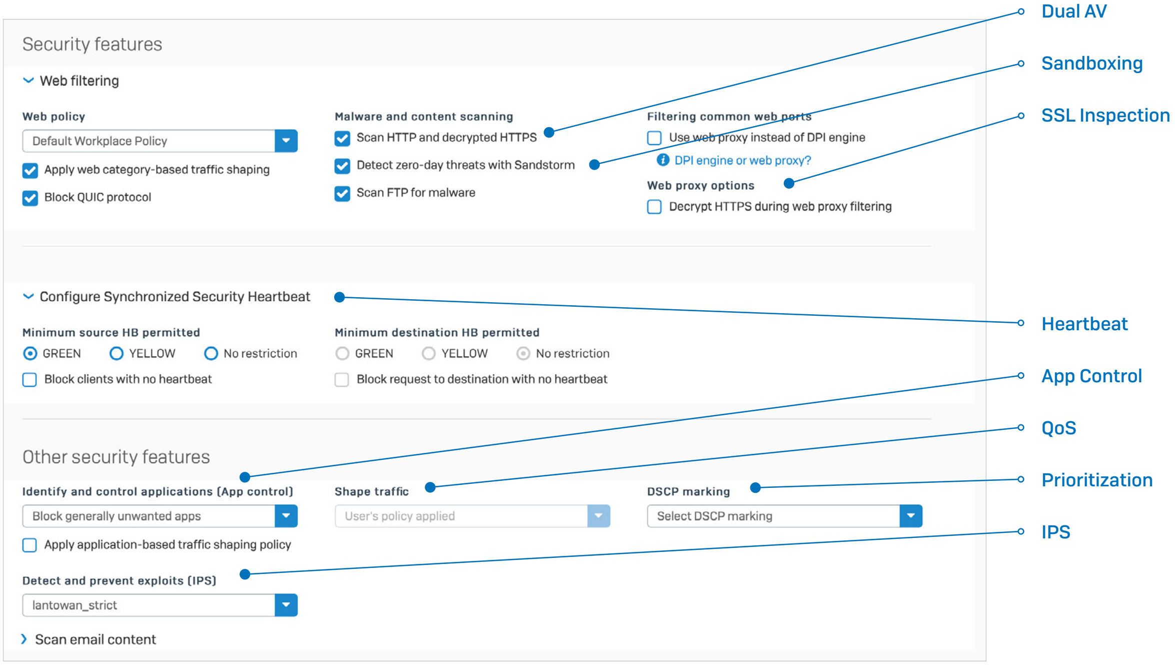
#	Name	Source	Destination	What	ID	Action	Feature and service
1	FastPath VoIP Traf... in 0 B, out 0 B	LAN, Any host	WAN, GotoWebinar(HG), GotoMeet...	Any service	#13	Accept	AV WEB APP QoS HB PRX NAT **LOG** IPS
2	High Priority in 0 B, out 0 B	LAN, MY_PC	WAN, Any host	Any service	#16	Accept	AV WEB APP QoS HB PRX NAT **LOG** IPS
3	PS Traffic in 0 B, out 0 B	IoT, PS4	WAN, Any host	Any service	#15	Accept	AV **WEB** APP QoS HB **PRX** NAT **LOG** IPS
4	VPN Access in 0 B, out 0 B	VPN, Any host, chris, joe	Any zone, Any host	Any service	#9	Accept	AV WEB APP **QoS** HB PRX NAT **LOG** IPS
	Server Access and ... in 4.30 KB, out 1.58 KB	Rules governing access to servers					
5	IoT Management in 0 B, out 0 B	LAN, MyiPhone, MyiPad, MacBoo...	IoT, Any host	Any service	#11	Accept	AV WEB APP QoS HB PRX NAT **LOG** **IPS**
6	PS4 PSN in 0 B, out 0 B	WAN, Any host	IoT, #Port2	PSN	#14	Accept	AV WEB APP QoS HB PRX NAT **LOG** IPS
7	VNC Server Access in 0 B, out 0 B	LAN, Any host, chris	LAN, Mac Server	VNC	#12	Accept	AV WEB APP **QoS** HB PRX NAT **LOG** IPS
8	Media Server Acces... in 4.30 KB, out 1.58 KB	WAN, Any host	LAN, #Port2	Server Management	#7	Accept	AV WEB APP QoS HB **Exclusion** PRX NAT **LOG** **IPS**
9	~~Policy for MTA~~ in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	**AV** WEB APP QoS HB PRX NAT LOG IPS
	User Rules in 41.89 MB, out 10.96 MB	Rules governing different user groups					

Rules for users, business applications, NAT, TLS/SSL 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 all from a single screen.



Security features

Web filtering

Web policy: Default Workplace Policy

☑ Apply web category-based traffic shaping

☑ Block QUIC protocol

Malware and content scanning

☑ Scan HTTP and decrypted HTTPS

☑ Detect zero-day threats with Sandstorm

☑ Scan FTP for malware

Filtering common web ports

☐ Use web proxy instead of DPI engine

DPI engine or web proxy?

Web proxy options

☐ Decrypt HTTPS during web proxy filtering

Configure Synchronized Security Heartbeat

Minimum source HB permitted: ● GREEN ○ YELLOW ○ No restriction

☐ Block clients with no heartbeat

Minimum destination HB permitted: ○ GREEN ○ YELLOW ○ No restriction

☐ Block request to destination with no heartbeat

Other security features

Identify and control applications (App control): Block generally unwanted apps

☐ Apply application-based traffic shaping policy

Shape traffic: User's policy applied

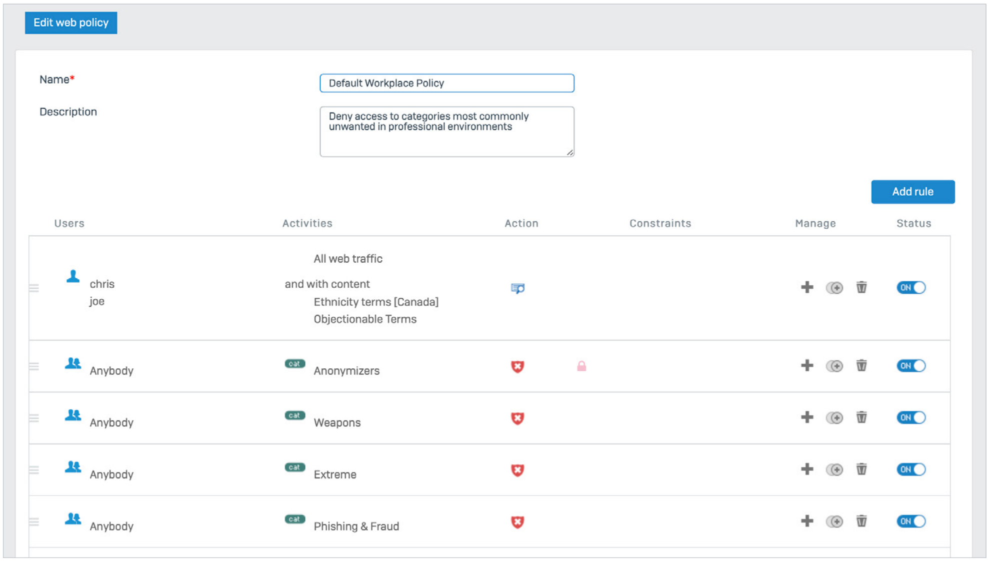
DSCP marking: Select DSCP marking

Detect and prevent exploits (IPS): lantowan_strict

Scan email content

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.



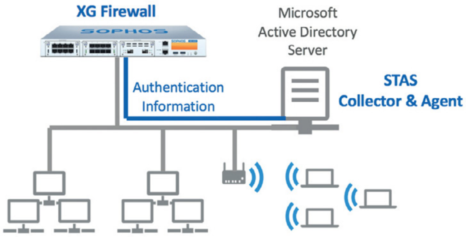
Edit web policy

Name*: Default Workplace Policy

Description: Deny access to categories most commonly unwanted in professional environments

Users	Activities	Action	Constraints	Manage	Status
chris joe	All web traffic and with content Ethnicity terms [Canada] Objectionable Terms				ON
Anybody	cat Anonymizers				ON
Anybody	cat Weapons				ON
Anybody	cat Extreme				ON
Anybody	cat Phishing & Fraud				ON

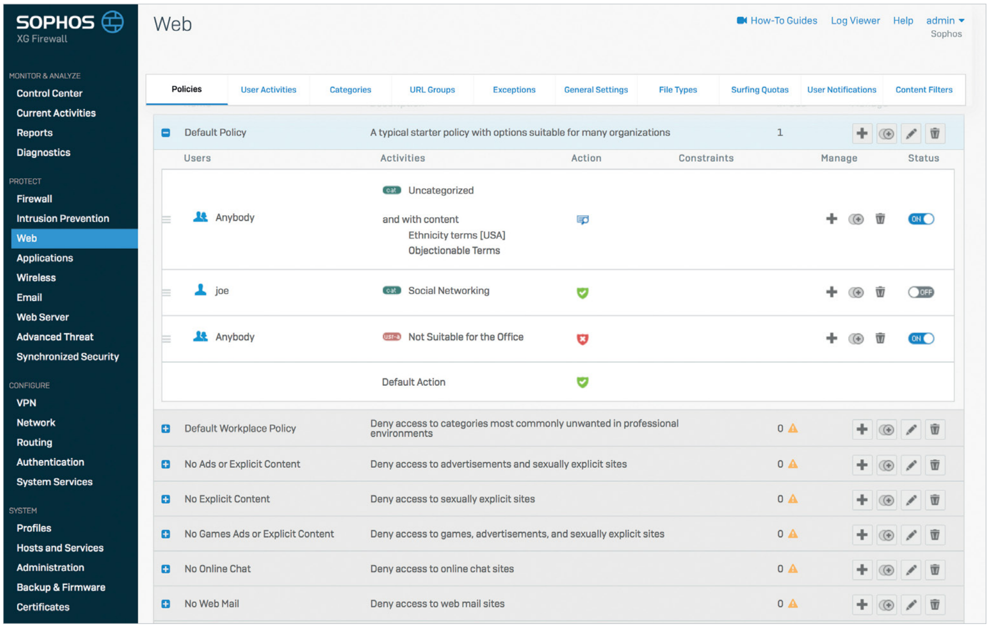
Flexible authentication options enable you to easily know who's who, and include directory services such as Active Directory, eDirectory, and LDAP, as well as NTLM, Kerberos, RADIUS, TACACS+, RSA, client agents, or a captive portal. And Sophos Transparent Authentication Suite (STAS) provides integration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



No client required on devices for SSO!

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, 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, 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.



Web

Default Policy	A typical starter policy with options suitable for many organizations	1

Users	Activities	Action	Constraints	Manage	Status
Anybody	cat Uncategorized and with content Ethnicity terms [USA] Objectionable Terms				ON
joe	cat Social Networking	✓			OFF
Anybody	usr-a Not Suitable for the Office	✗			ON
	Default Action	✓			

Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	0 ⚠
No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites	0 ⚠
No Explicit Content	Deny access to sexually explicit sites	0 ⚠
No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites	0 ⚠
No Online Chat	Deny access to online chat sites	0 ⚠
No Web Mail	Deny access to web mail sites	0 ⚠

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
- Blockpage 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, 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.

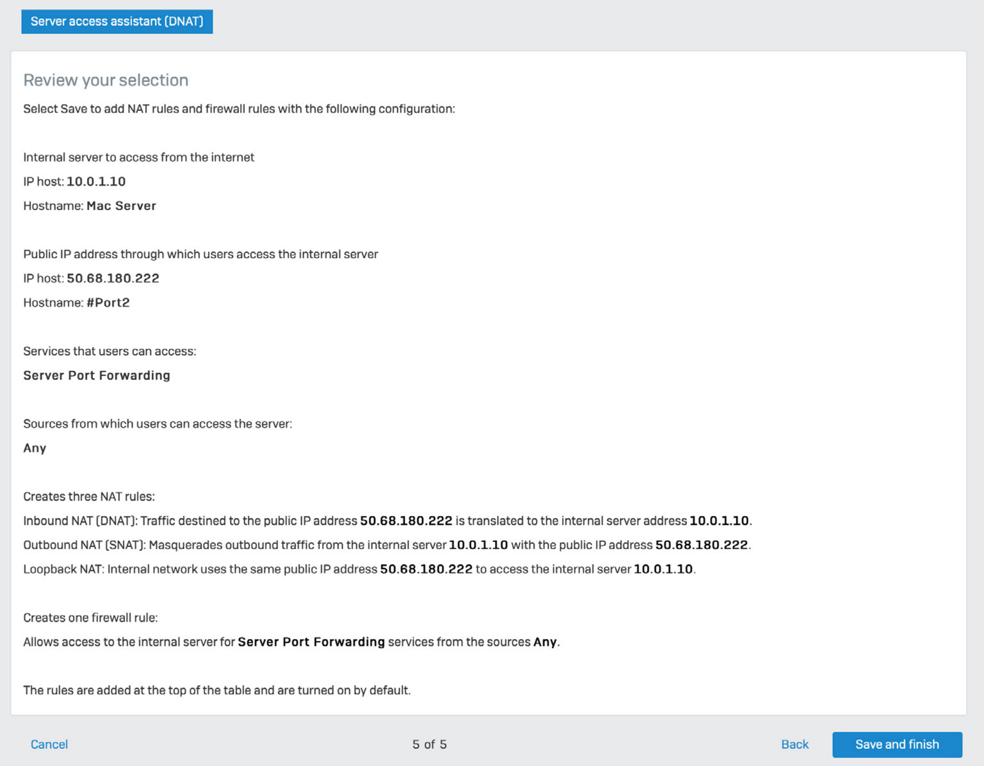
XG Firewall helps with CIPA policy compliance right out of the box, enabling quick compliance. It also offers flexible and powerful controls over SafeSearch and YouTube restrictions on a user/group policy basis. And teachers can be granted the option to set up and manage their own policy overrides to 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.



Review your selection

Select Save to add NAT rules and firewall rules with the following configuration:

Internal server to access from the internet
IP host: **10.0.1.10**
Hostname: **Mac Server**

Public IP address through which users access the internal server
IP host: **50.68.180.222**
Hostname: **#Port2**

Services that users can access:
Server Port Forwarding

Sources from which users can access the server:
Any

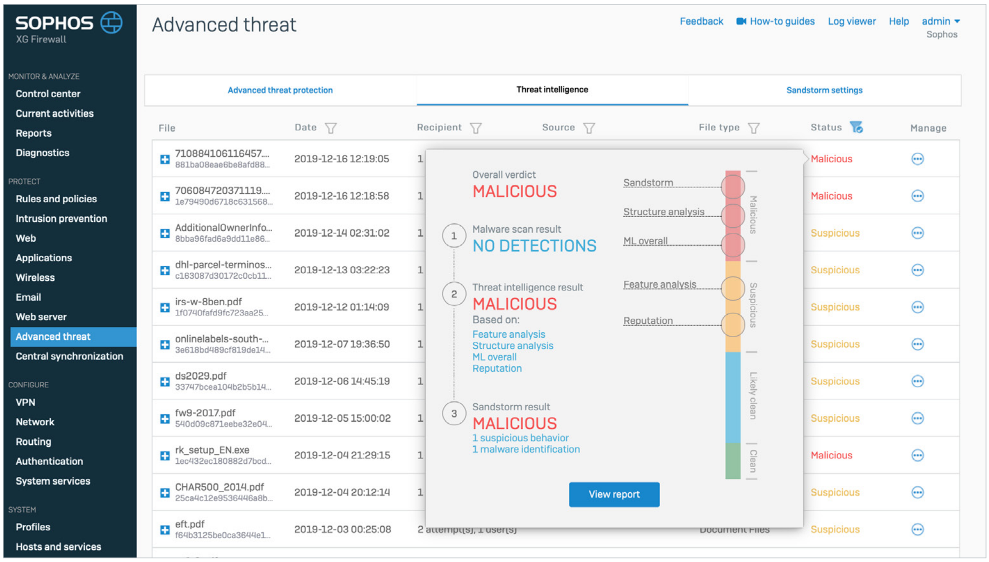
Creates three NAT rules:
Inbound NAT (DNAT): Traffic destined to the public IP address **50.68.180.222** is translated to the internal server address **10.0.1.10**.
Outbound NAT (SNAT): Masquerades outbound traffic from the internal server **10.0.1.10** with the public IP address **50.68.180.222**.
Loopback NAT: Internal network uses the same public IP address **50.68.180.222** to access the internal server **10.0.1.10**.

Creates one firewall rule:
Allows access to the internal server for **Server Port Forwarding** services from the sources **Any**.

The rules are added at the top of the table and are turned on by default.

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.



Advanced threat

File	Date	Recipient	Source	File type	Status	Manage
710884106116457.... 881ba08eae6be8afd88...	2019-12-16 12:19:05	1			Malicious	⋯
706084720371119.... 1e79490d6718c631568...	2019-12-16 12:18:58	1			Malicious	⋯
AdditionalOwnerInfo... 8bba96fad6a9dd11e86...	2019-12-14 02:31:02	1			Suspicious	⋯
dhl-parcel-terminos... c163087d30172c0cb11...	2019-12-13 03:22:23	1			Suspicious	⋯
irs-w-8ben.pdf 1f0740fafd9fc723aa25...	2019-12-12 01:14:09	1			Suspicious	⋯
onlinelabels-south-... 3e618bd489cf819de14...	2019-12-07 19:36:50	1			Suspicious	⋯
ds2029.pdf 33747bcea104b2b5b14...	2019-12-06 14:45:19	1			Suspicious	⋯
fw9-2017.pdf 540d09c871eebe32e04...	2019-12-05 15:00:02	1			Suspicious	⋯
rk_setup_EN.exe 1ec432ec180882d7bcd...	2019-12-04 21:29:15	1			Malicious	⋯
CHAR500_2014.pdf 25ca4c12e9536446a8b...	2019-12-04 20:12:14	1			Suspicious	⋯
eft.pdf f64b3125be0ca3644e1...	2019-12-03 00:25:08	2 attempt(s), 1 user(s)		Document Files	Suspicious	⋯

Overall verdict
MALICIOUS

1 Malware scan result
NO DETECTIONS

2 Threat intelligence result
MALICIOUS
Based on:
Feature analysis
Structure analysis
ML overall
Reputation

3 Sandstorm result
MALICIOUS
1 suspicious behavior
1 malware identification

Sandstorm
Structure analysis
ML overall
Feature analysis
Reputation

Sophos Sandstorm is the ultimate cloud sandboxing solution, one that is simple and affordable, while providing essential protection through 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 set up. Because it's cloud-based there's no additional software or hardware required, and no impact on firewall performance. 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 newest threats, we integrated the latest protection technologies from our industry-leading Intercept X next-gen endpoint product 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.

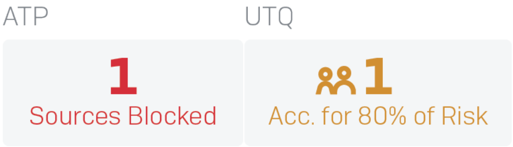
Threat Intelligence

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 in 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 a high level of 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 also the user and process.



ATP

1

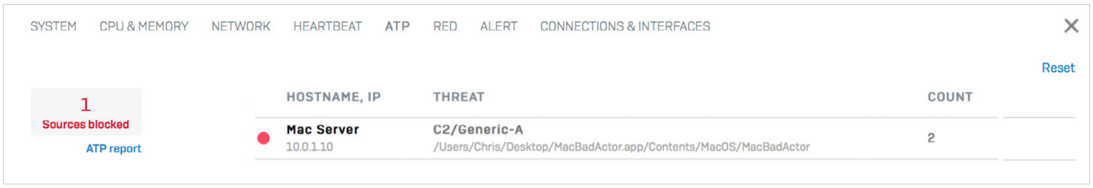
Sources Blocked

UTQ

1

Acc. for 80% of Risk

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 straightforward 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 hacker's servers.



1

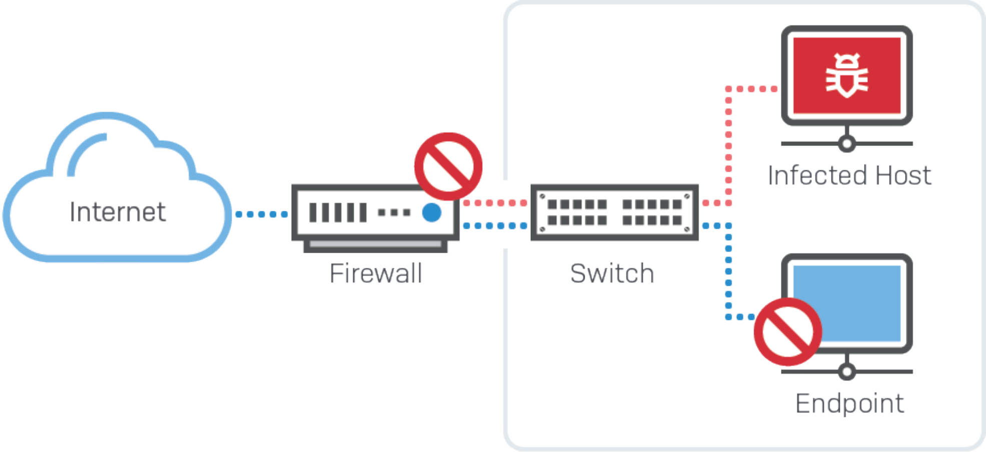
Sources blocked

	HOSTNAME, IP	THREAT	COUNT
●	Mac Server 10.0.1.10	C2/Generic-A /Users/Chris/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2

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.



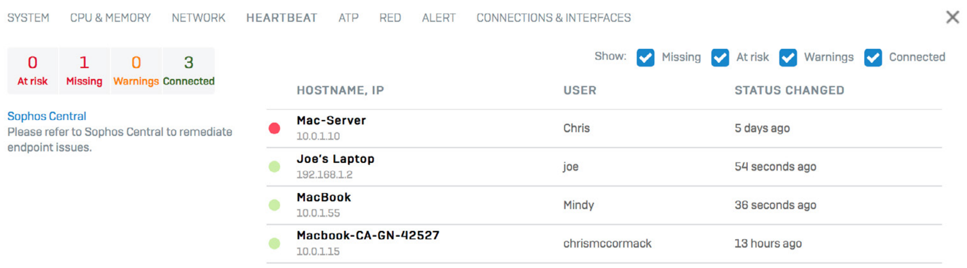
XG Firewall uniquely integrates the health of connected hosts into your firewall rules, enabling you to automatically limit access to sensitive network resources from any compromised system until it's decontaminated.

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 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 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 XG Firewall. This simple step of synchronizing security products that previously operated independently creates more effective protection against advanced malware and targeted attacks.



0 At risk | 1 Missing | 0 Warnings | 3 Connected

Sophos Central
Please refer to Sophos Central to remediate endpoint issues.

Show: ☑ Missing ☑ At risk ☑ Warnings ☑ Connected

	HOSTNAME, IP	USER	STATUS CHANGED
🟥	Mac-Server 10.0.1.10	Chris	5 days ago
🟩	Joe's Laptop 192.168.1.2	joe	54 seconds ago
🟩	MacBook 10.0.1.55	Mindy	36 seconds ago
🟩	Macbook-CA-GN-42527 10.0.1.15	chrismccormack	13 hours ago

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 act 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.

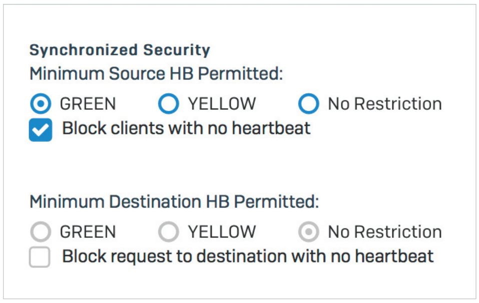
1 At Risk | 1 Missing | 1 Warnings | 2 Connected

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.



Synchronized Security
Minimum Source HB Permitted:
● GREEN ○ YELLOW ○ No Restriction
☑ Block clients with no heartbeat

Minimum Destination HB Permitted:
○ GREEN ○ YELLOW ● No Restriction
□ Block request to destination with no heartbeat

Only Sophos can provide a solution like the 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.

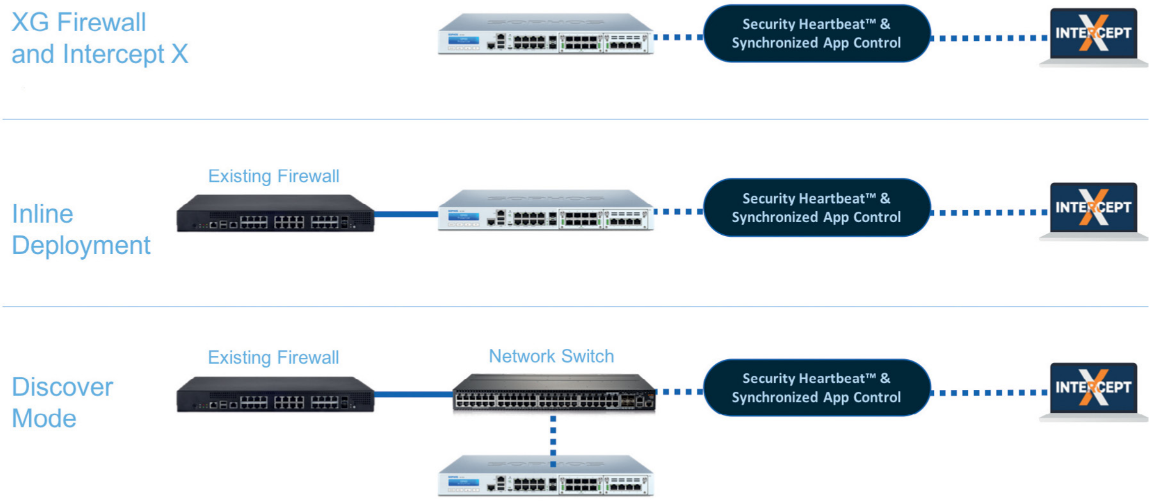
Synchronized Security Cybersecurity that continuously shares information between systems, providing insight and visibility to one another.

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) service Monitors all user activity across the network and identifies potentially compromised user credentials.

Add XG Firewall to Any Network – Simply


XG Firewall and Intercept X
Security Heartbeat™ & Synchronized App Control
INTERCEPT X
Existing Firewall
Inline Deployment
Security Heartbeat™ & Synchronized App Control
INTERCEPT X
Existing Firewall
Network Switch
Discover Mode
Security Heartbeat™ & Synchronized App Control
INTERCEPT X

XG Series hardware appliances offer flexible deployment options with fail-open bypass ports standard on all 1U models and available in FleXi Port Modules to enable this feature on our 2U appliances as well. The bypass ports enable XG Firewall to be installed in bridge mode in line with existing firewalls. 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 the network. This feature enables new deployment options that are completely risk free 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.

Sophos XG Firewall: It's cybersecurity made simple.

Request Pricing

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

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

North America 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