SOPHOS
Cybersecurity delivered.

Sophos Firewall

Solution Brief

Contents

Sophos Firewall

Sophos Firewall has been designed right from the start to address today's top problems with existing existing firewalls while also providing a true next-gen platform to tackle the modern encrypted internet and evolving threat landscape.. Sophos Firewall brings a fresh approach to the way you identify hidden risks, protect against threats, and respond to incidents while providing optimal performance. Our Xstream Architecture for Sophos Firewall utilizes a packet processing architecture that delivers extreme levels of visibility, protection, and performance.

Sophos 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, Sophos 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 Firewall has four key advantages over other network firewalls:

1. **Exposes hidden risks** – Sophos 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** – Sophos 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** – Sophos 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.
4. **Optimizes your SD-WAN network** – the Xstream SD-WAN capabilities in Sophos Firewall enable setting up complex SD-WAN overlay networks a simple point-and-click exercise. You can also take advantage of automatic performance-based WAN link selection with instant zero-impact transitions between links to optimize your application performance, network resliancy, and business continuity while reducing connectivity costs.

Exposing Hidden Risks

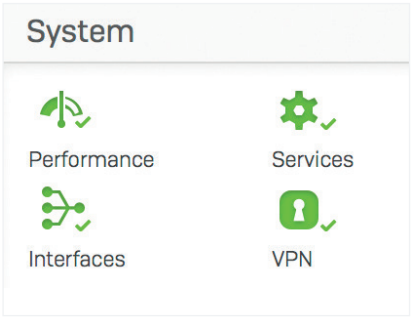
It's critically important for a modern firewall to parse through the mountain of information it collects, correlate data where possible, and highlight only the most important information requiring action – ideally before it's too late.

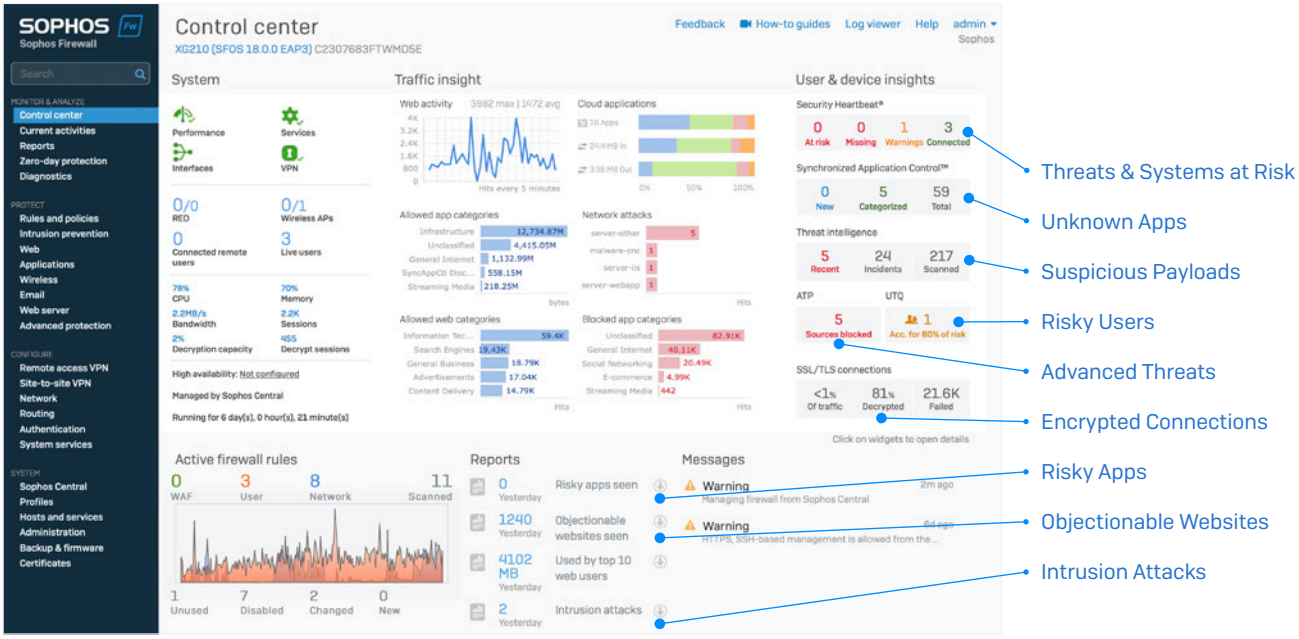
Control Center

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

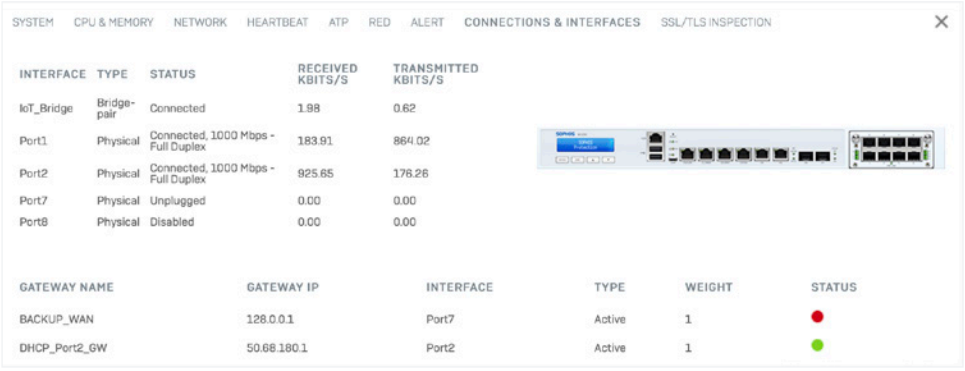
It uses "traffic light" style indicators to focus your attention on what's most important to you.

If something's red, it requires immediate attention. Yellow indicates a potential problem. And if everything is green, no further action is required.

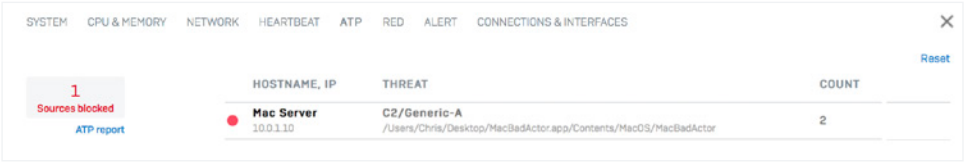




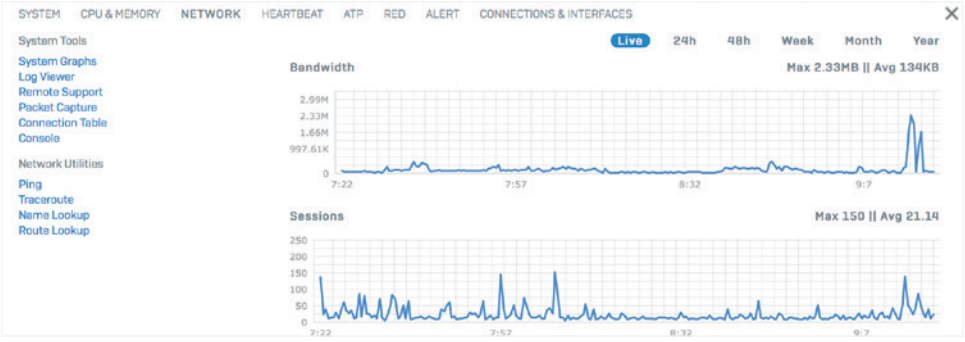
Every widget on the Control Center offers additional information that is easily revealed simply by clicking that widget. For example, the status of interfaces on the device can be obtained by clicking the "Interfaces" widget on the Control Center.



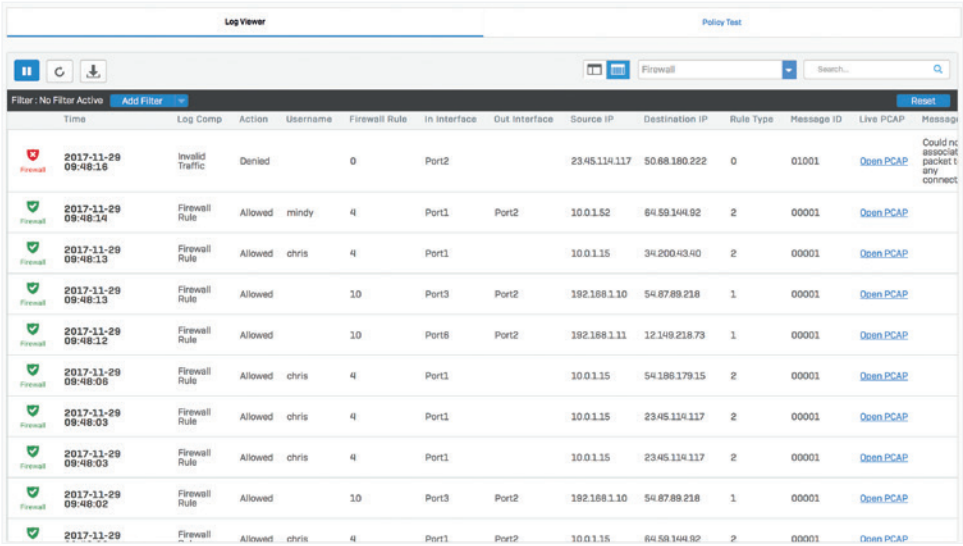
The host, user, and source of an advanced threat are also easily determined simply by clicking the ATP (advanced threat protection) widget in the dashboard.



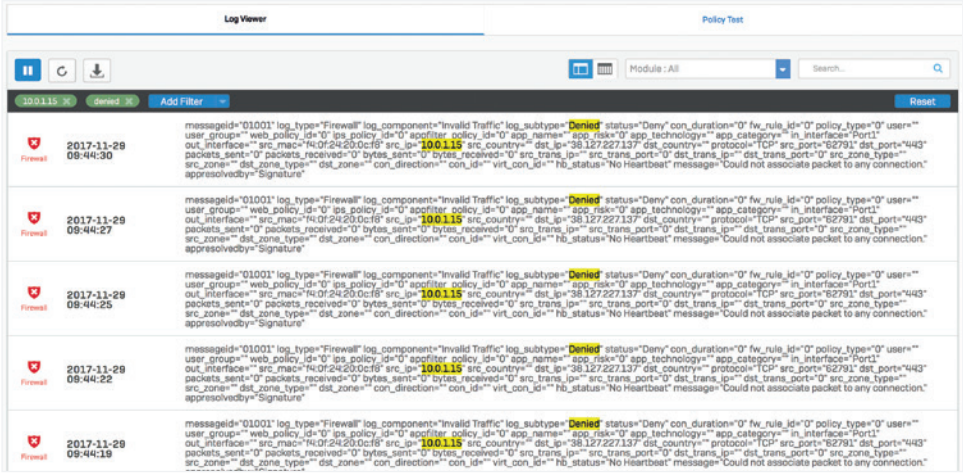
System graphs also show performance over time with selectable timeframes, whether you want to look at the last two hours to the last month or year. And they provide quick access to commonly used troubleshooting tools to resolve potential issues.



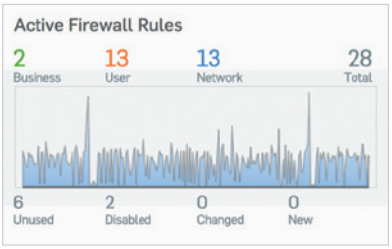
The live log viewer is available from every screen with just a single click. You can open it in a new window to keep one eye on the relevant log while working on the console. It provides two views: a simpler column-based format by firewall module, as well as a more detailed unified view with powerful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



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 Firewall, you don't need to wonder anymore.



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.

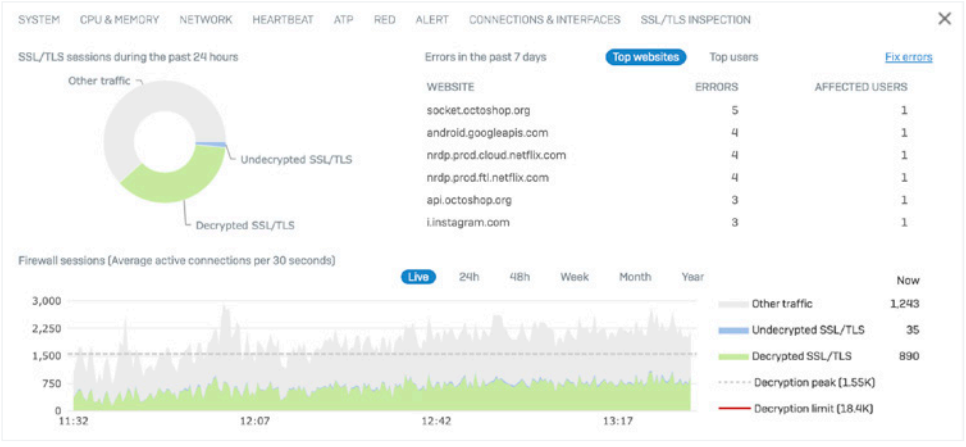


Xstream TLS Inspection

There's a perfect storm brewing around encrypted traffic. According to Google, the volume of encrypted traffic on networks has grown to over 90%. 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.

Sophos 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. Sophos 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. Sophos 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.



Sophos Firewall provides insights into encrypted traffic flows and any issues arising from TLS inspection right from the Control Center

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.

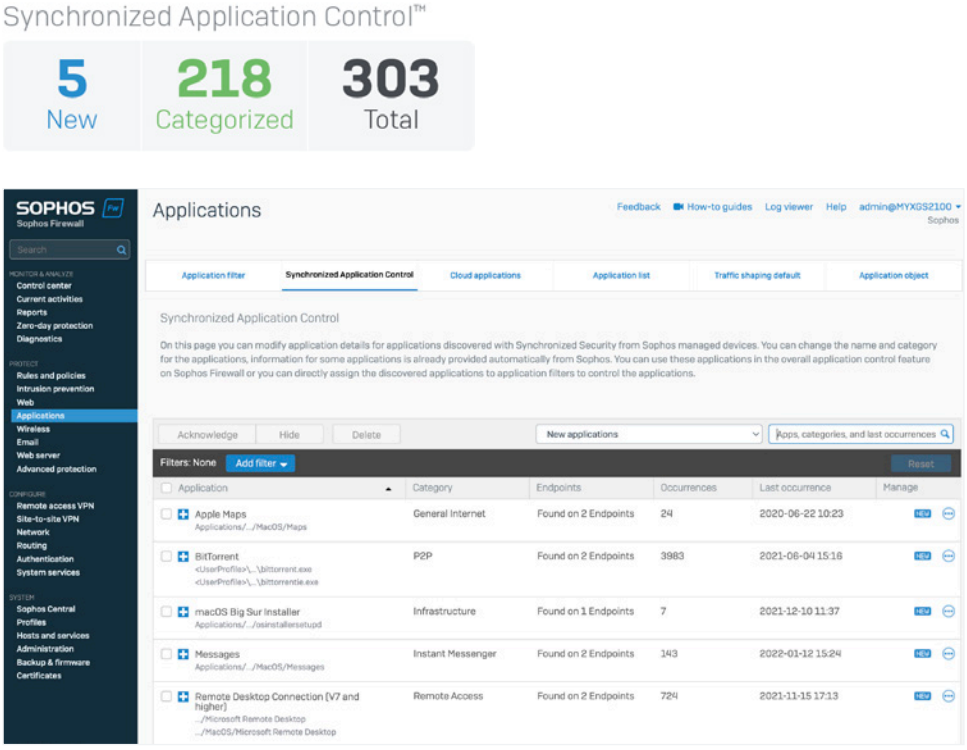
Synchronized Application Control

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.

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 Sophos Firewall sees application traffic it can't identify with signatures, it asks the endpoint which application is generating that traffic.



Unknown applications that have been discovered by Synchronized Application Control can be automatically or manually categorized.

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 this information to classify and control the application automatically in most situations.

If Sophos Firewall can't determine the appropriate application category automatically, the administrator can set the desired category or assign the app to an existing policy.

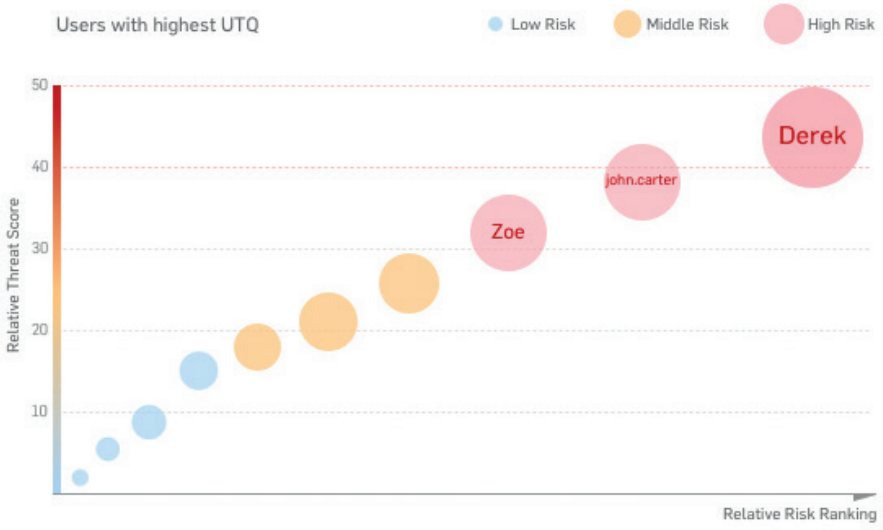
Once an application is classified, either automatically or by the network administrator, the application is subject to the same policy controls as all other applications in that category, making it very easy to block all the unidentified apps you don't want, and prioritize the apps you do want.

Synchronized Application Control is a breakthrough in application visibility and control, providing absolute clarity over 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.

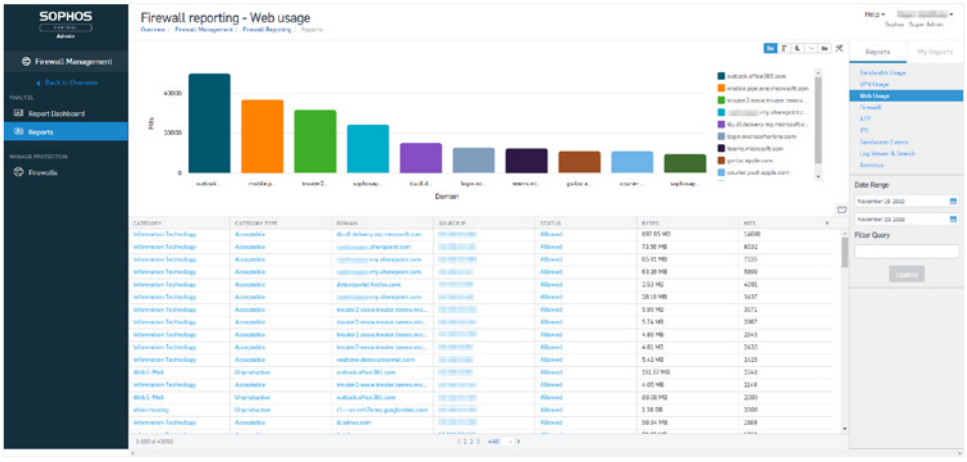


Sophos Firewall highlights your top-risk users at a glance.

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

Sophos 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.



Sophos Firewall provides extensive on-box and central cloud-based reporting options.

Sophos 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.

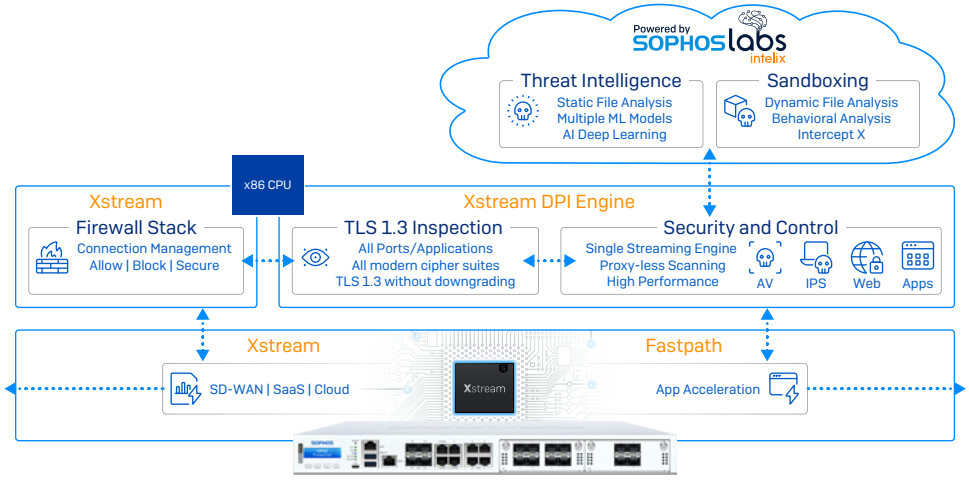
At Sophos, not only do we believe you need the most advanced protection technology available, we also understand it needs to be simple to configure, deploy, and manage day-to-day because misconfigured protection is often worse than having no protection at all.

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.

Sophos Firewall does things differently that make a big difference.

Xstream Protection and Performance

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 Sophos 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.



Sophos Firewall's Xstream Architecture with programable Xstream Flow Processors provides powerful protection and performance.

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.

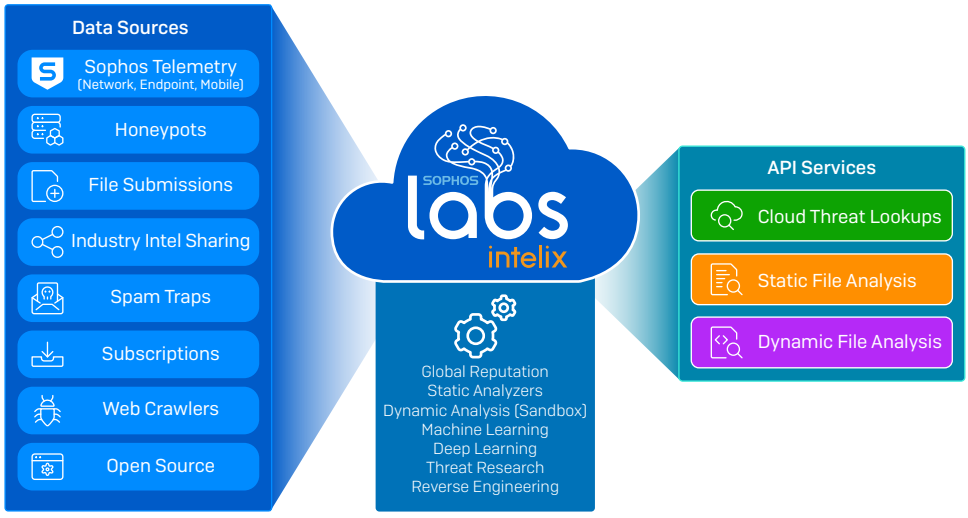
Then, if the stream is considered secure and no longer requires further inspection, the DPI engine can completely offload the flow to the Sophos Network Flow FastPath which provides an accelerated path for trusted traffic. This boosts performance dramatically by freeing up other resources from inspecting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

Zero-Day Threat Protection

With advanced threats like ransomware becoming more targeted and evasive, there's a critical need for predictive zero-day threat identification and protection. The ultimate solution to this is two-fold:

1. **Static Machine Learning Analysis** – This provides predictive analysis and detection through multiple artificial neural network machine learning models, combined with global reputation and deep file scanning, all without needing to execute the file in real time.
2. **Dynamic Run-time Sandbox Analysis** – This detonates malware real-time in a cloud sandbox environment for unmatched insights into file activity to reveal the true nature and capabilities of an unknown threat.

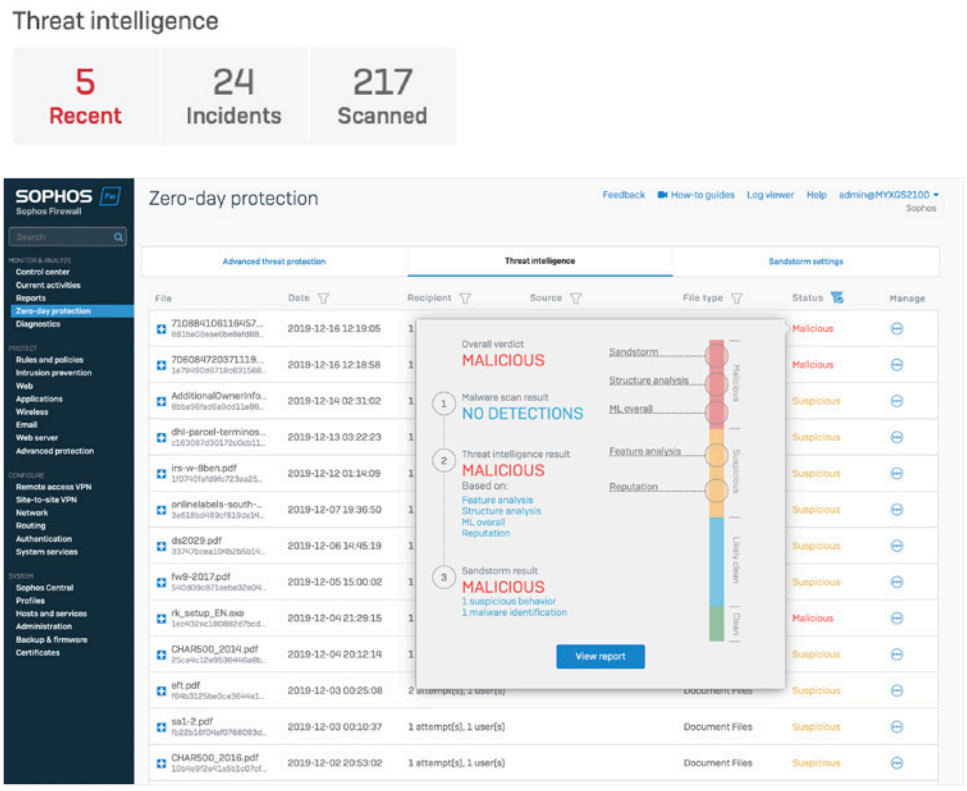
Sophos Firewall includes both of these important protection technologies, powered by SophosLabs Intelix. SophosLabs, our critically acclaimed Tier-1 Cybersecurity threat research lab has developed the ultimate threat analysis and intelligence platform in SophosLabs Intelix. It utilizes the latest machine learning technology, decades of threat research, and petabytes of intelligence, providing unmatched protection against the latest previously unseen threats.



Sophos Firewall's zero-day protection is powered by SophosLabs Intelix machine learning analysis.

When the Sophos Firewall Xstream DPI engine performs AV analysis on a file entering the network and determines there is active code, it holds the file temporarily and sends the file to SophosLabs Intelix service in the cloud for both static and dynamic file analysis. It then provides a summary of the results on the Sophos Firewall Control Center via the Threat Intelligence widget and this click-through report (below) and only releases the file to the downloader or email recipient if the file is clean.

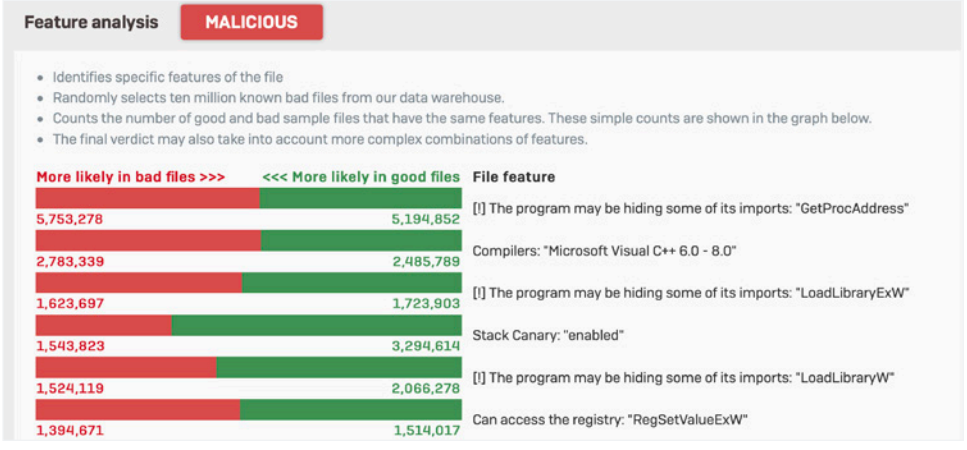
This last step is important, as many firewall advanced malware solutions often release the file to the end user before the analysis is complete, possibly resulting in a messy and costly cleanup if the file was ultimately convicted as a threat.



Sophos Firewall's Zero-Day Protection identifies new previously unseen threats before they get on your network.

Static Machine Learning Analysis

Static file analysis utilizes multiple machine learning models to analyze various characteristics, features, genetics and reputation elements of the file, comparing it with millions of known good and bad files in SophosLabs database to render a verdict in seconds on any new and previously unseen file. It's remarkably fast and effective at identifying new threats and new variants of existing threats, particularly threats that are not easily sandboxed, such as password protected documents containing malware.



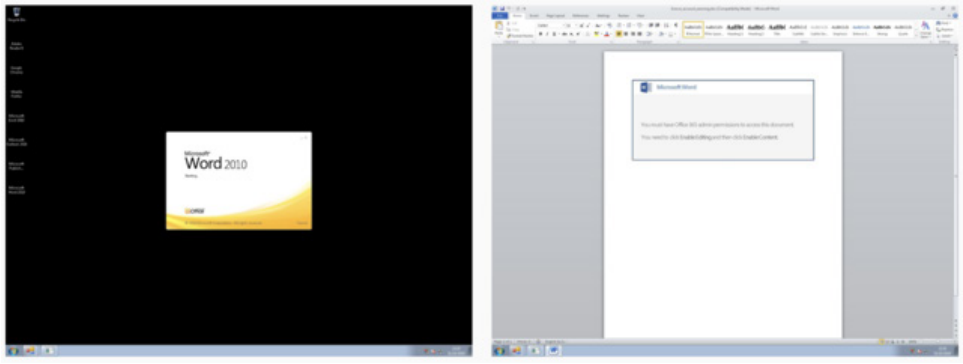
Multiple machine learning models are used to analyze suspicious files for zero day threats.

Dynamic Runtime Sandboxing Analysis

When sandboxing technology first emerged, it 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.

Because it's cloud-based there's no additional software or hardware required, and no impact on firewall performance. Any file determined by the Xstream DPI Engine to contain active code, such as an email attachment or web download is automatically uploaded and detonated in SophosLabs Intelix cloud sandbox in parallel with the Static analysis (above) to determine its runtime behavior before being allowed onto your network.

To identify threats, SophosLabs have 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 (to detect active ransomware encrypting files in real time). It also monitors all file, memory, registry and network activity for characteristics of malicious intent to render a verdict. No other firewall offers this kind of run-time analysis with the world's best threat protection – Intercept X. And no other firewall offers the level of insights and reporting that Sophos Firewall provides, including a full set of screen shots of what transpired as the file was run.

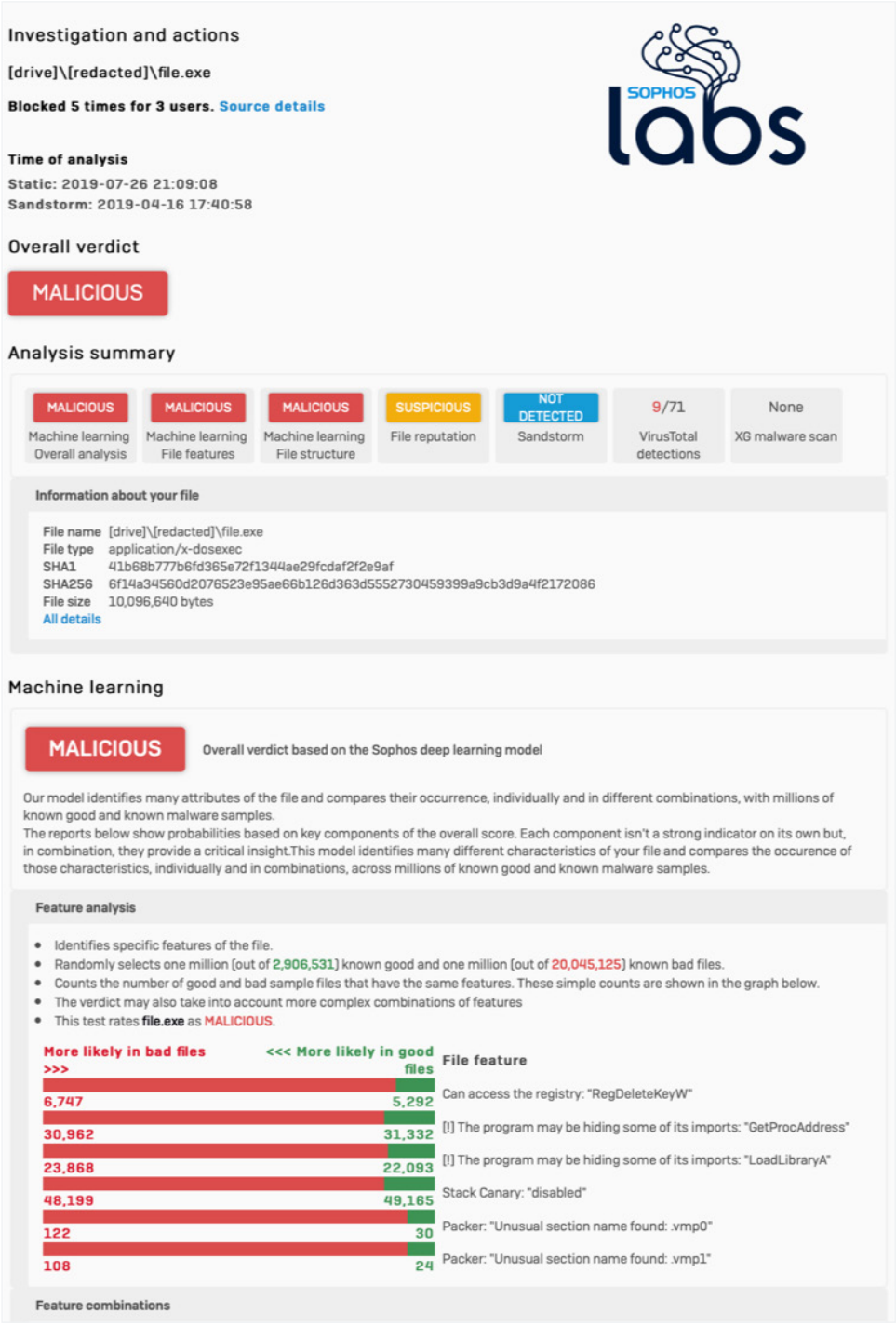


Sandboxing run-time analysis detonates files in a safe environment to determine behaviour and provides screen shots for your review.

Sandboxing is particularly effective at detecting threats that lurk in normally benign files that may not have any obvious malicious characteristics. Office files with macros, or benign executables or application updates that have been subverted.

Threat Protection Reporting

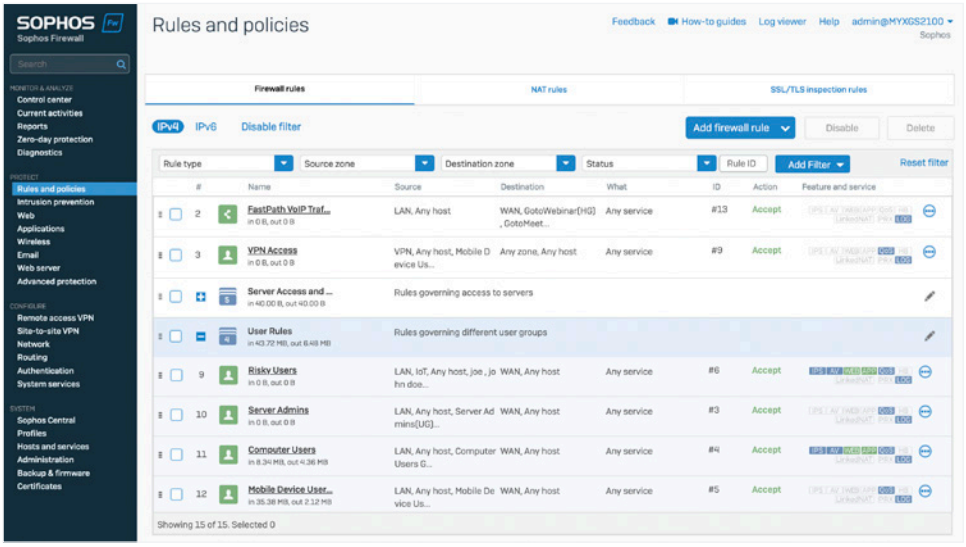
Every file analyzed by Sophos Firewall has an accompanying report that provides full details on the results of the various analysis and the verdicts. There are six different elements of the report, including the various machine learning analysis, file reputation, sandboxing, and even third-party VirusTotal data.



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 Sophos 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.



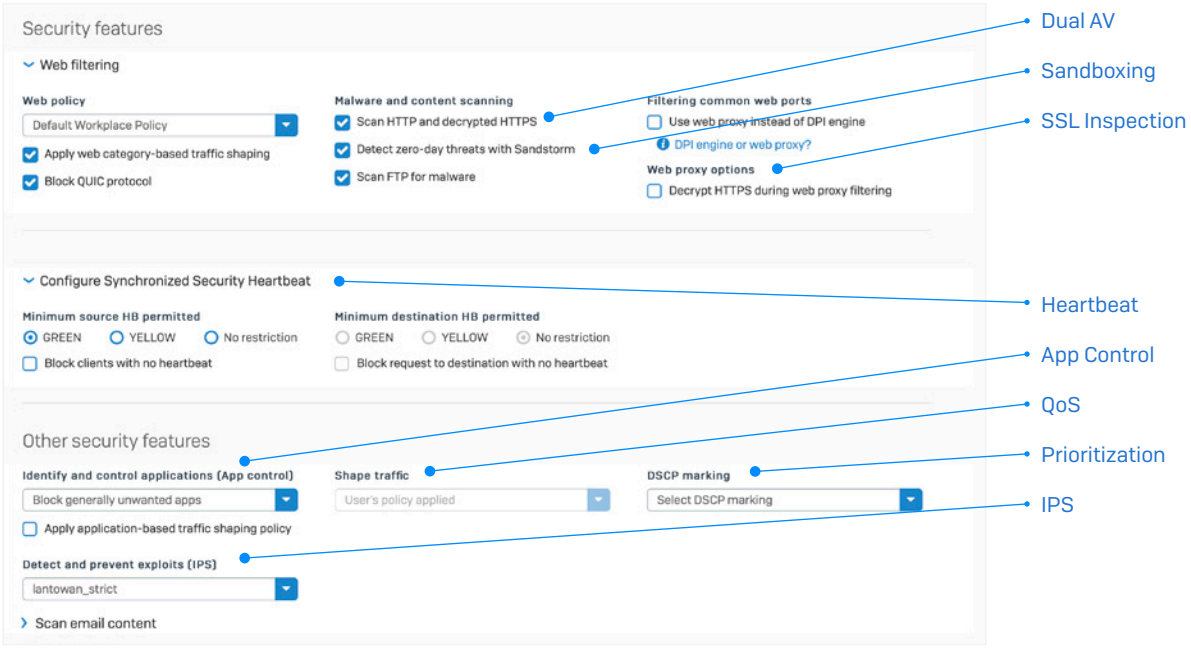
Sophos Firewall puts all your rules for access policy, NAT and TLS inspection together in one-place making it easy to manage.

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

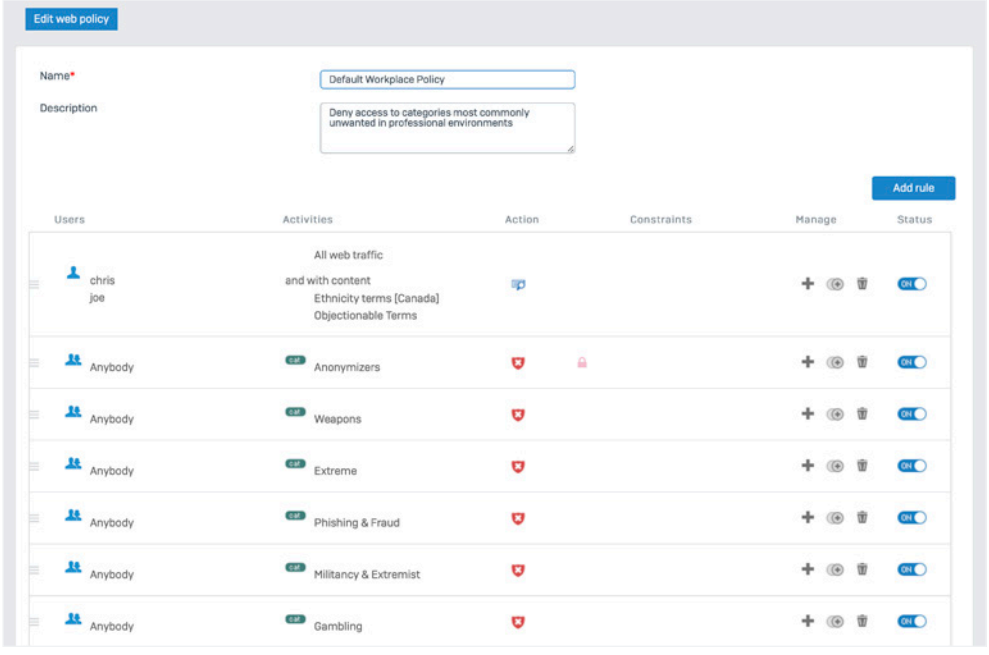
Whether through your Sophos Central account in the cloud or the Sophos Firewall user interface, Sophos makes it incredibly easy to configure and manage everything needed for modern protection and do it all from a single screen.



Configure your full security posture on one screen using pre-defined or custom policies.

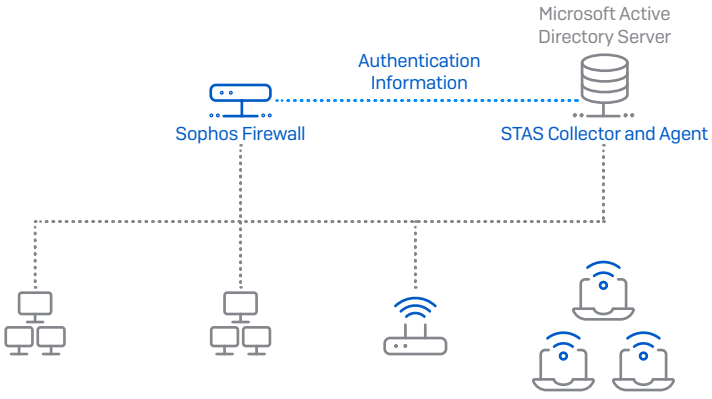
You can set up and snap in security and control for antivirus, TLS/SSL inspection, sandboxing, IPS, traffic shaping, web and app control, Security Heartbeat, NAT, routing, and prioritization all in one place — and all on a rule by rule, user by user, or group by group basis.

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.



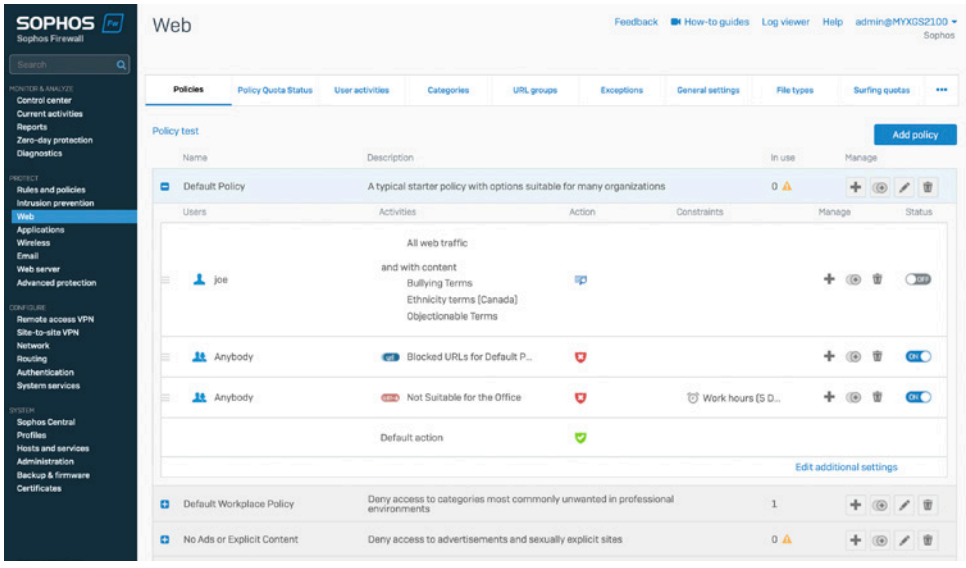
View policy details at a glance and make changes without leaving the firewall rule screen.

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, 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.



Powerful enterprise-grade web polices offer granular controls.

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

Sophos 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.

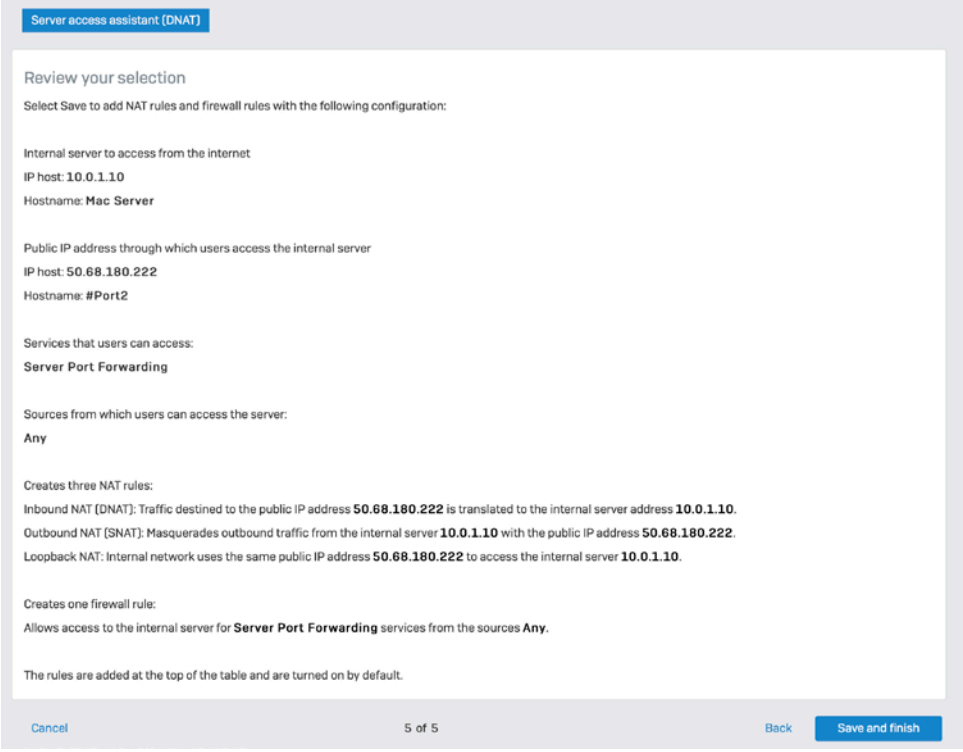
Sophos Firewall helps with CIPA policy compliance right out of the box, enabling quick compliance. It also offers flexible and powerful controls over SafeSearch and YouTube restrictions on a user/group policy basis. And teachers can be granted the option to set up and manage their own policy overrides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

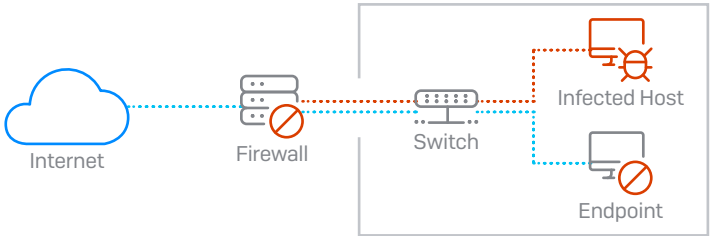


Take advantage of the powerful but intuitive NAT rule wizard to create complex access controls with just a few clicks.

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 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.



Sophos Firewall and Security Heartbeat can automatically isolated infected hosts on your network.

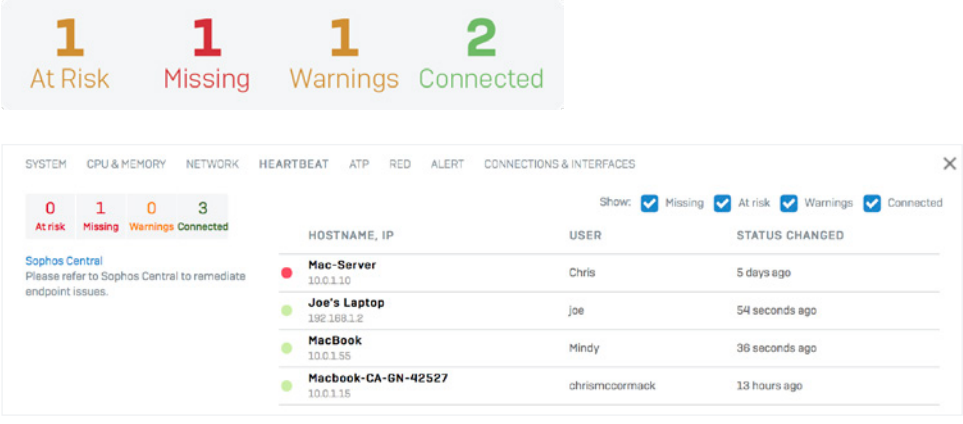
Sophos Firewall uniquely integrates the health of connected hosts into your firewall rules, enabling you to automatically limit access to sensitive network resources from any compromised system until it's decontaminated.

Not only can Sophos 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 Sophos Firewall. This simple step of synchronizing security products that previously operated independently creates more effective protection against advanced malware and targeted attacks.



Security Heartbeat™ status for your network is visible on the Control Center.

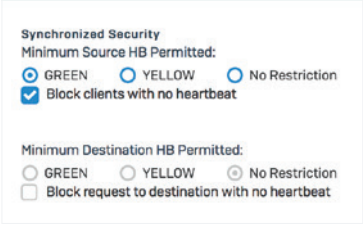
Security Heartbeat not only identifies the presence of advanced threats instantly, it can also be used to communicate important information about the nature of the threat, the host system, and the user. And perhaps most importantly, Security Heartbeat can also automatically act to isolate or limit access 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.

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.



Set Security Heartbeat requirements as part of any firewall rule.

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 – The world's most trusted cybersecurity platform puts these disparate and complementary technologies into a single cloud management console to help you orchestrate and monitor your zero trust network.

Synchronized Security – Cybersecurity that continuously shares information between endpoint, ZTNA, firewall, and other systems, providing insight and visibility to one another.

Sophos ZTNA – Provides a true zero-trust network access solution for securely connecting users to applications and data.

Sophos 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.

Optimizing your SD-WAN Network

Few terms in networking have generated as much buzz as SD-WAN (or Software Defined Networking in a Wide Area Network). All that buzz has been accompanied by equal doses of useful information and confusing rhetoric. As a result, SD-WAN has grown to mean different things to different people, while some are still trying to figure out exactly what it means.

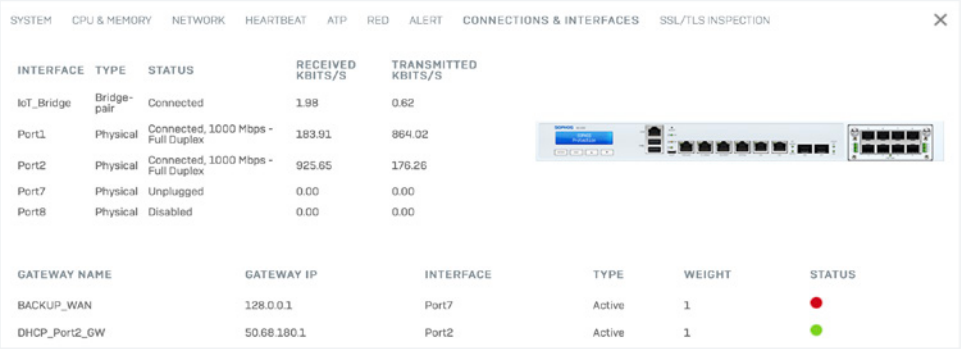
Fundamentally, SD-WAN is often about achieving one or more of these four networking objectives:

- **Reduce connectivity costs** – Traditional MPLS (Multi-Protocol Label Switching) connections are expensive so organizations are shifting to more affordable broadband WAN options such as cable, DSL, and 3G/4G/LTE
- **Business continuity** – Organizations require solutions that provide redundancy, routing, failover, and session preservation in the event of a WAN failure or outage
- **Quality of critical applications** – Organizations are seeking real-time visibility into application traffic and performance in order to maintain session quality of mission-critical business apps
- **Simpler branch office VPN orchestration** – VPN orchestration between locations is often complex and time consuming, which is why having the tools to simplify and automate deployment and setup is critical

Sophos Firewall with Xstream SD-WAN enables you to achieve even your most ambitious SD-WAN goals simply and affordably with a comprehensive set of SD-WAN orchestration, management, and peformance and reliability optimization options.

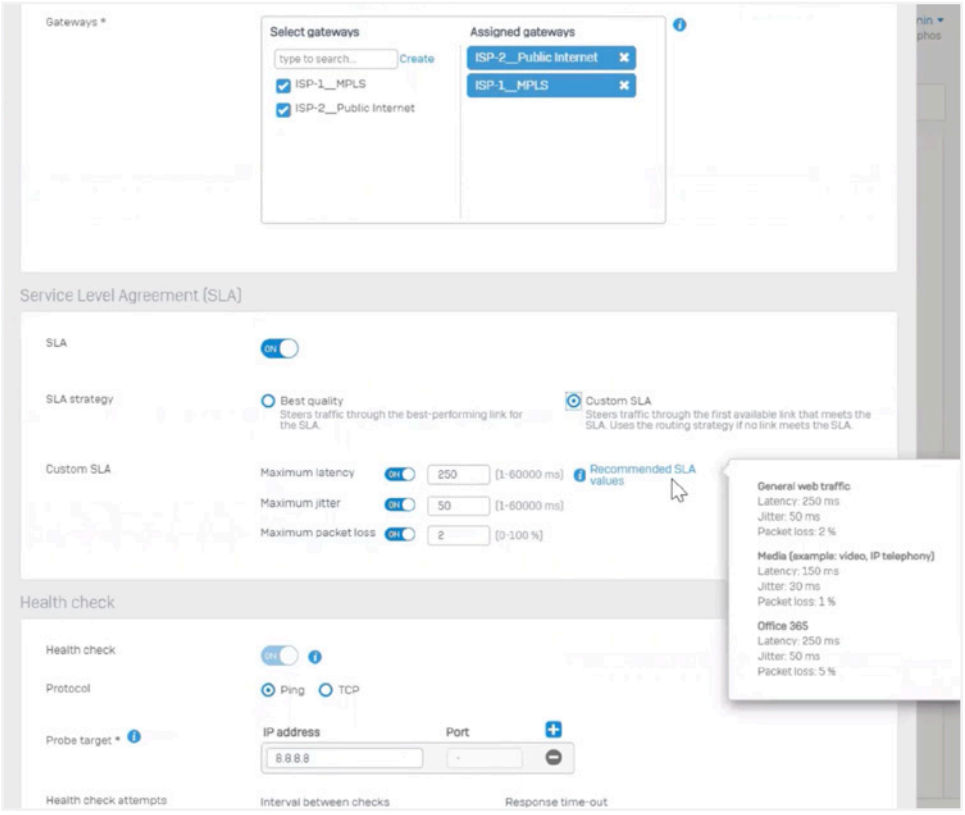
Xstream SD-WAN

Managing routing of application traffic over multiple WAN links is a key tenet of SD-WAN, and Sophos Firewall with Xstream SD-WAN provides a powerful and flexible link management solution whether you are using multiple MPLS, DSL, Cable, or cellular connections.



WAN Link Status is shown in the bottom of this interface status widget available via the dashboard.

SD-WAN profiles define a routing strategy across multiple WAN link gateways enabling seamless and efficient rerouting of application connections based on WAN Link performance. Transitions between links happen instantaneously with zero impact to application sessions and no disruption providing seamless continuity, application performance, and the best end-user experience in even the most disruptive or unstable ISP environments.



Setting up performance-based SD-WAN profiles is intuitive and easy.

SD-WAN profile routing strategies can be based on first available or performance-based link criteria. Performance monitoring criteria includes jitter, latency, and packet loss and can utilize multiple probe targets for PING and TCP probes.

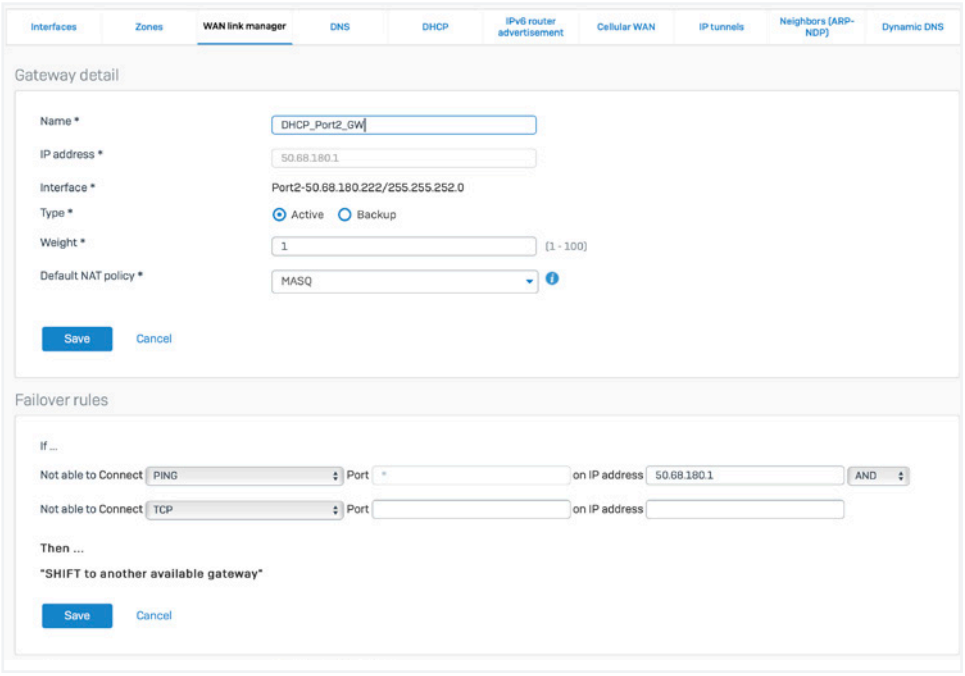
SD-WAN profiles can automatically select the best link based on performance or according to your custom SLA policies that define specific values for maximum acceptable jitter, latency, or packet loss before re-routing over a better performing link with absolutely zero impact to any active connections.

Monitoring the performance of your SD-WAN network is easy with real-time and historical graphs for latency, jitter, and packet loss. Timeline selections include real-time, the last 24 or 48 hours, or over the last week or month as well. Advanced logging of SD-WAN performance and routing is also included.

Monitor the performance of your various WAN links in real time.

Xstream FastPath Acceleration of SD-WAN VPN Traffic

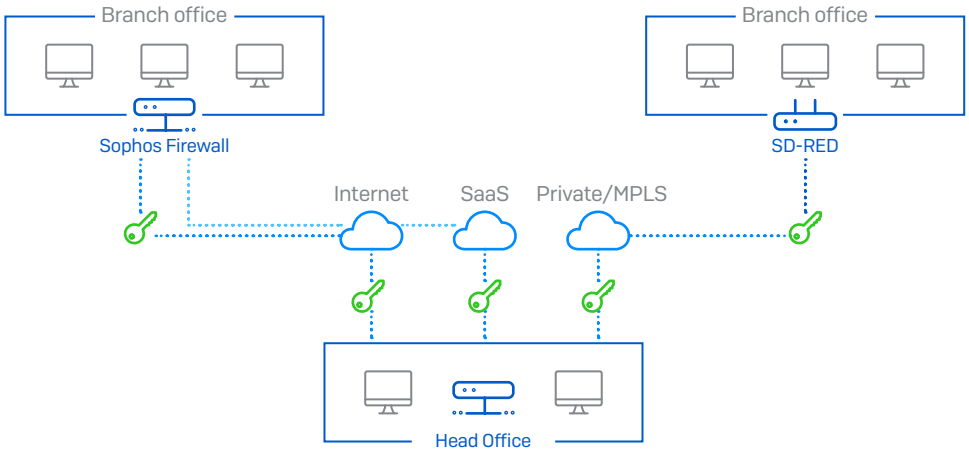
Sophos Firewall utilizes the integrated Xstream Flow Processors in XGS Series appliances to provide hardware acceleration of IPsec VPN tunnel traffic. This dramatically improves performance, moving some of the CPU-intensive processing required for IPsec tunnels to the Xstream Flow Processor such as ESP-encapsulation/encryption and decapsulation/decryption. This new feature takes full advantage of the hardware crypto capabilities within the Xstream Flow Processor and has the added benefit of freeing up CPU resources for other tasks like deep-packet inspection of traffic that needs it. Xstream FastPath Acceleration for IPsec traffic works for both site-to-site and remote access VPN traffic.



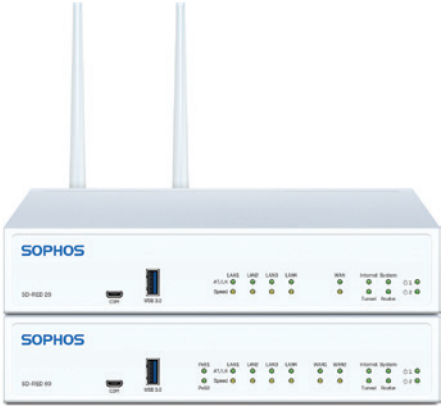
Sophos Firewall WAN Link Management, including balancing and failover rules.

SD-Branch Office Connectivity

Sophos has long been a pioneer in the area of zero-touch branch office deployment and connectivity with our unique SD-RED devices. These affordable devices are extremely easy for a non-technical person to deploy, and provide a robust secure Layer 2 tunnel between the device and a central firewall.

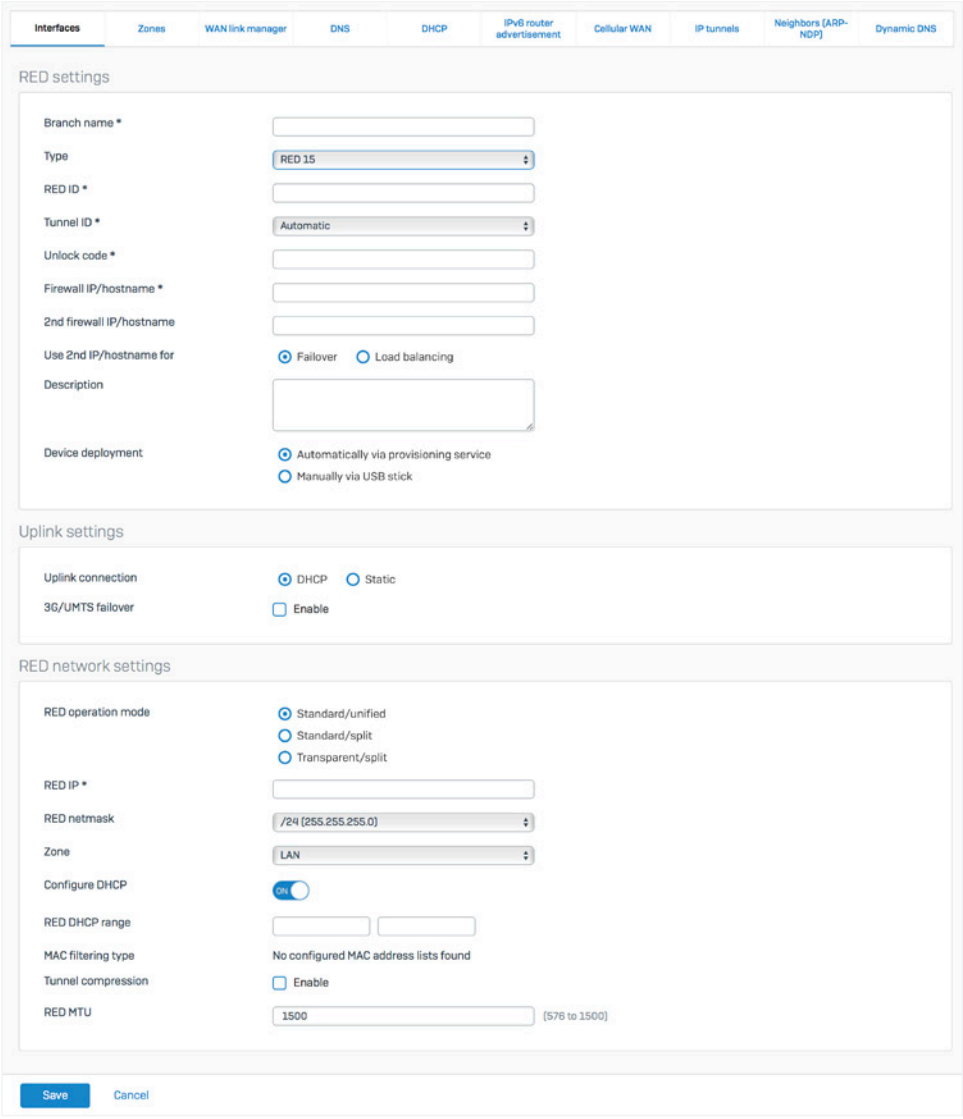


Sophos Firewall and SD-RED devices offer tunnel options to simply and affordably connect branch offices via SD-WAN.



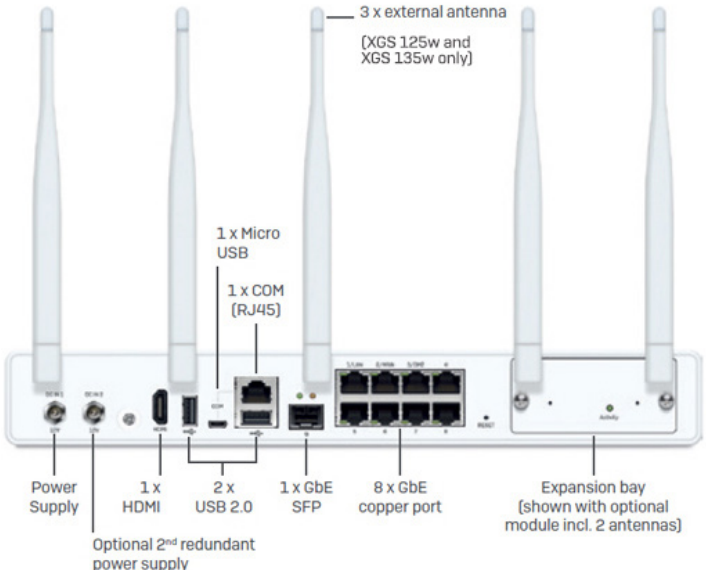
Sophos SD-RED devices offer an affordable, zero-touch solution to SD-WAN branch connectivity.

Deploying SD-RED devices couldn't be easier: You simply note the serial number of the device in your firewall and ship the device to the remote location. Any non-technical person at the remote site simply connects the device and it will contact our cloud-provisioning service automatically to establish a secure tunnel connection with your Sophos Firewall.



Sophos SD-RED offers a flexible, secure, and affordable SD-WAN branch office connectivity solution.

Our desktop XGS Series appliances also make excellent branch office SD-WAN connectivity solutions with flexible connectivity options including VDSL and cellular in addition to copper and fiber interfaces, and support for our robust SD-RED tunnels.

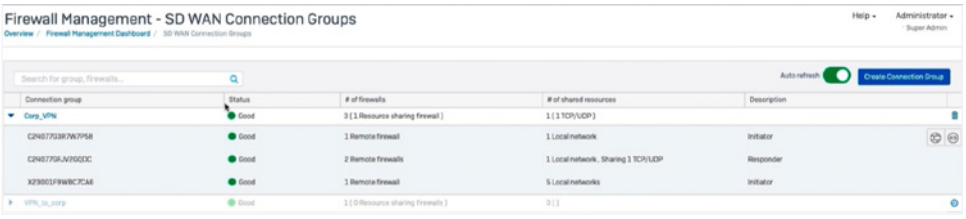


Select desktop models like the XGS 135w shown here come with options for LTE/ cellular, VDSL, copper, or fiber WAN connectivity options.

VPN Support and Orchestration

If you've ever set up more than a couple of VPN tunnels between different firewalls, you know how time consuming and tedious this process can be. Sophos Firewalls supports rich SD-WAN orchestration in Sophos Central which makes interconnecting multiple tunnels between several firewalls a quick and easy task.

You simply select the firewalls you have under management that you wish to participate in the SD-WAN connection group, and then select the network resources you wish every site to have access to. With the flip of a switch, you essentially watch your SD-WAN VPN overlay network come to life as all the necessary firewall access rules and tunnels, including redundancy, are created for you automatically.



Quickly setup complex SD-WAN overlay networks with just a few clicks and monitor them from Sophos Central.

Whether you need a full mesh network, hub-and-spoke topology, or something in between, Sophos Central will automatically take care of all the necessary tunnel and firewall setup on the backend to enable your SD-WAN overlay network.

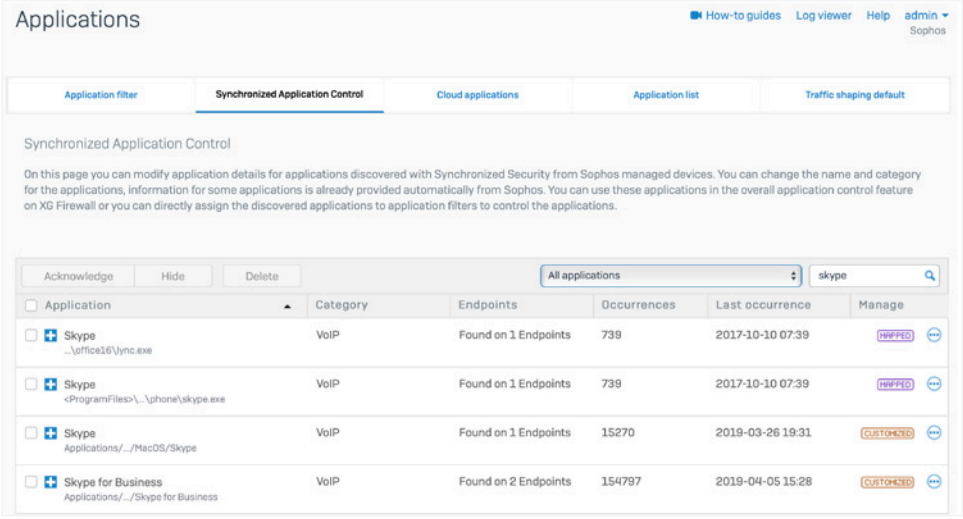
Of course, Sophos Firewall supports all the standard site-to-site VPN options you expect, including IPsec and SSL. We even offer our own unique SD-RED Layer 2 tunnel with routing that's extremely robust and proven reliable in high-latency situations such as over satellite links.

Application Visibility and Routing

Another important feature for achieving SD-WAN objectives is application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP.

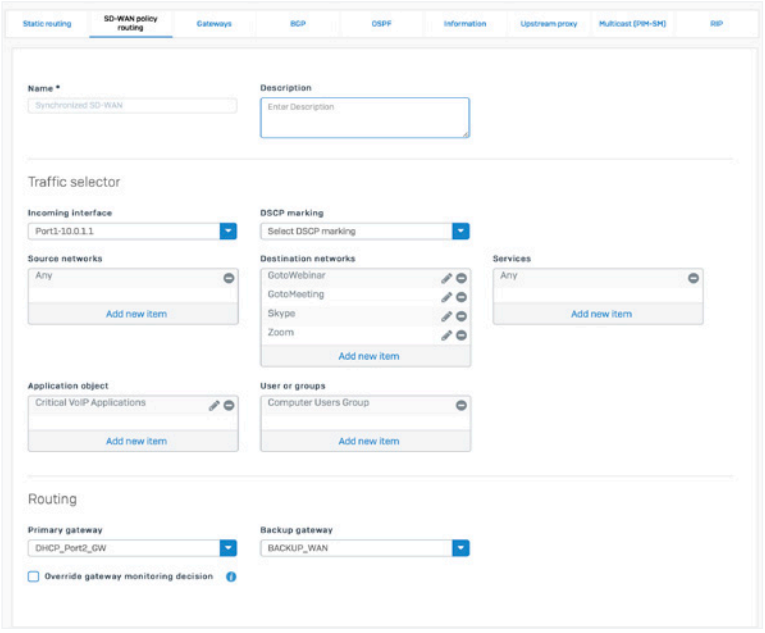
Of course, you can't route what you can't identify, so accurate, reliable application identification and visibility is critical. This is one area where Sophos Firewall and Sophos Synchronized Security provide an incredible advantage. Synchronized Application Control provides 100% clarity and visibility into all networked applications, providing a significant advantage in identifying mission-critical applications, especially obscure or custom applications.

Synchronized SD-WAN, a Synchronized Security feature, offers additional benefits with SD-WAN application routing. Synchronized SD-WAN leverages the added clarity and reliability of application identification that comes with the sharing of Synchronized Application Control information between Sophos-managed endpoints and Sophos Firewall. Now, previously unidentified applications can also be added to SD-WAN routing policies, providing a level of application routing control and reliability that other firewalls can't match.



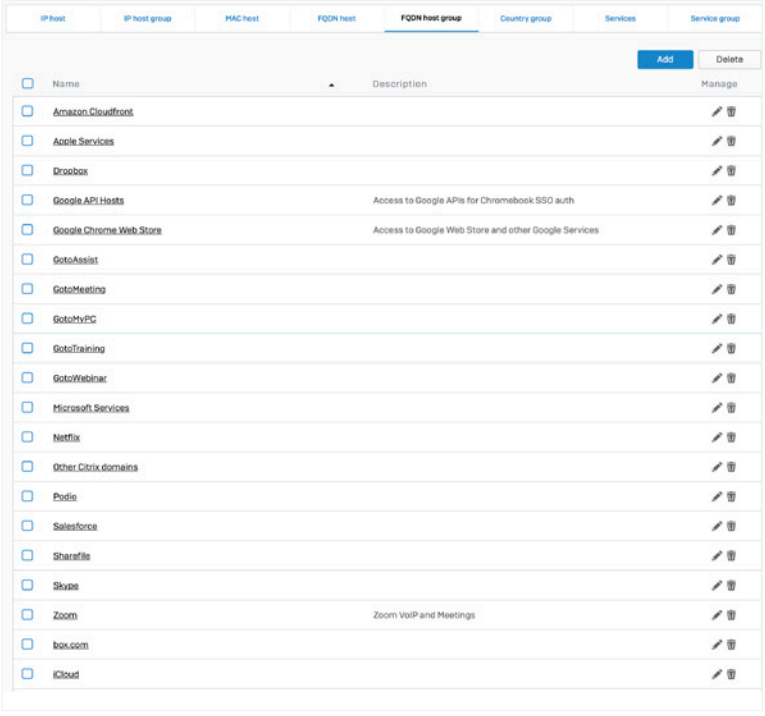
Synchronized Application Control identifies 100% of all networked applications, making it easy to prioritize and route mission critical applications.

Sophos Firewall also enables application-based routing and path selection in every firewall rule, including by user and group. Granular policy-based routing (PBR) controls provide the ability to define routing through either the primary or backup gateway WAN connection and configure for replay direction. Together, these features make it easy to direct important application traffic out the optimal WAN interface.



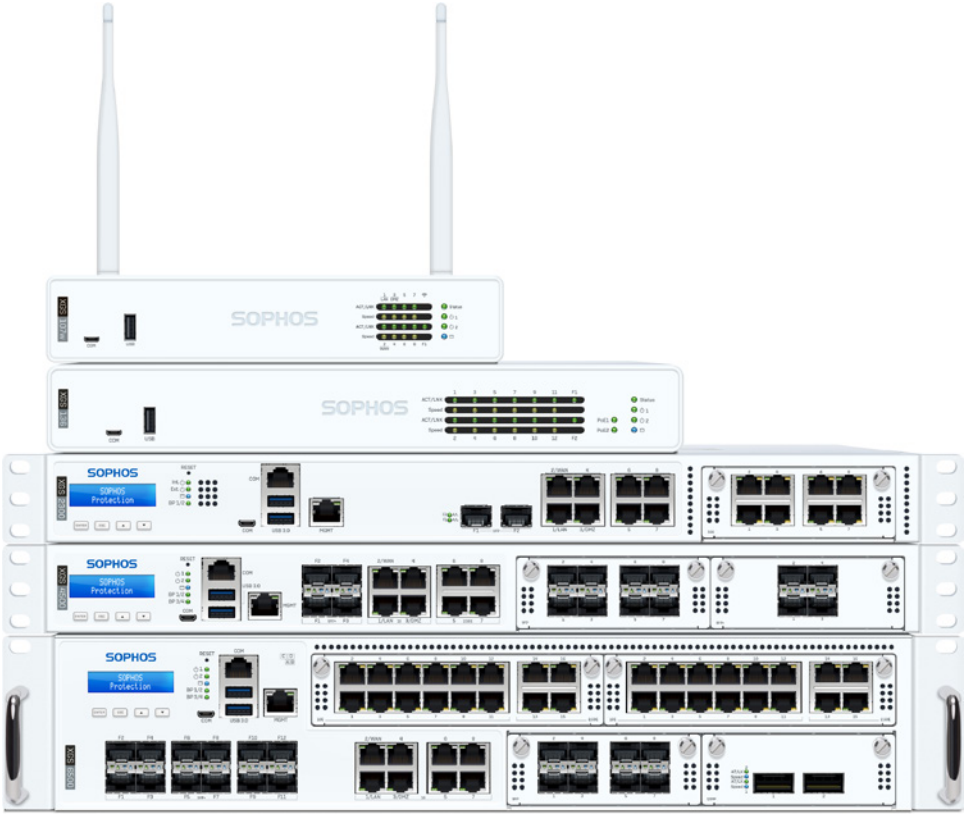
SD-WAN policy-based routing provides flexible tools for routing critical application traffic.

Sophos Firewall also includes predefined Fully Qualified Domain Name (FQDN) objects for popular SaaS cloud services, with thousands of FQDN hosts definitions included right out of the box and the option to easily add more.



Pre-defined FQDN Host Objects simplify path selection and application-based routing.

Add Sophos Firewall to Any Network – Simply



Sophos Firewall 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 Sophos Firewall to be installed in bridge mode in line with existing firewalls. If the Sophos 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 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 American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

22-03-30 EN (DD)