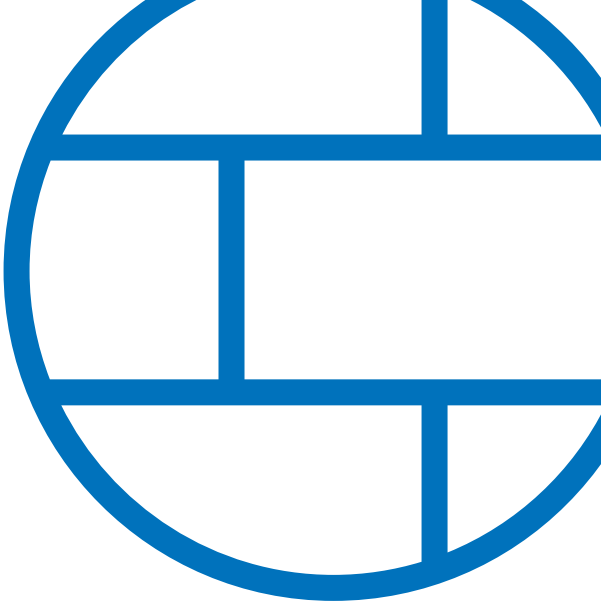
SOPHOS
Cybersecurity made simple.



Next-Gen Firewall Buyer's Guide

In a recent survey, we asked IT network managers to name their top issues with their existing firewall. Here are problems they cited:

- My firewall requires I spend time digging to get the information I need
- My firewall does not automatically identify threats or isolate infected systems
- My firewall has lots of features but it makes it difficult to figure out how to use them
- My firewall is missing key features I wish it had
- My network does not identify potentially risky users or apps on my network

If any of these sound familiar, you're not alone. The fact is, most firewalls today are incredibly complex, lacking in essential features, and provide little if any visibility into what's happening on your network.

It can be challenging to even know where to start. You'll want to begin by identifying your key requirements, but once you've established those, it's a daunting task to wade through vendor websites and datasheets in an effort to determine which firewall can best meet your needs.

How to use this guide

This buyer's guide is designed to help you choose the right solution for your organization so that you don't end up with regrets like the firewall buyers above. This guide covers all the features and capabilities you should consider when evaluating your next firewall purchase. We've also included a number of important questions to ask your IT partner or vendor to determine if their product will meet your needs. And on the last page, we've added a convenient time-saving chart that can help you create a shortlist of suitable firewall vendors.

Next-generation firewall awareness and control

While firewalls started life simply protecting networks from outside hacks and attacks, the role of the firewall has greatly evolved to take on additional duties, such as compliance and risk management. While most modern next-gen firewalls provide basic visibility and control over user activity, they often fall far short when it comes to providing any kind of risk assessment or insights. These days, you need all the help you can get, which means a firewall solution that not only makes it easy to setup and enforce acceptable use policies, but also one that can identify risky users and apps before they become a problem.

There are four key technologies your firewall must include to provide adequate next-generation user awareness and control:

- **Application Control** – Application control enables you to prioritize important network traffic like VoIP, while limiting or blocking unwanted traffic like streaming media. Even if you don't enforce any app control policies, you need to be aware of what applications are putting your network and organization at risk. Ensure your next firewall has full user and group-based application control with traffic shaping options by application, user, category, or rule.
- **Web Control** – URL filtering policies are important for compliance to ensure a safe environment for all your users. While this has become a staple of nearly every firewall, there are important differences in the ease with which sophisticated user and group-based policies can be implemented and maintained on a daily basis. Make sure your next firewall offers a simple yet flexible set of policy tools to make day-to-day maintenance of this important area easy and less time-consuming.
- **Risk Visibility** – Insights into your riskiest users and applications are critical to ensuring proper policies are enforced before there's a serious incident. Ensure your next firewall provides a risk assessment report for users that correlates their network activity to identify your riskiest users. Also, look for an assessment of overall application risk level on your network that can guide you into taking action if and when high-risk application usage starts to become evident.
- **HTTPS Scanning** – With most internet traffic now encrypted, compliance enforcement is challenging unless you have adequate HTTPS scanning. Since HTTPS scanning can be invasive and disruptive, make sure your next firewall includes selective scanning and easy solutions for managing exceptions.

Capability to look for	Description	Questions to ask your vendor
Application Visibility and Control	When you have visibility into the applications being used, you're enabled to make educated decisions about what to allow, what to prioritize, and what to block, so your bandwidth is used to best effect and you don't waste time blocking applications that aren't a problem. If you look into the reports from most firewalls, the majority of network traffic will show as 'unclassified' or 'general Internet, as there are many apps which are custom, obscure, evasive, or simply using generic HTTP or HTTPS and therefore, remain unidentified.	› Does your app control provide per-user and group-level visibility and policy enforcement? › Does it provide application control by category, risk level, technology, or characteristics (such as misuse, low productivity, etc.) › Does your firewall have a way to introduce visibility for otherwise unclassified apps, such as those using generic HTTP? › Can you provide a sample firewall report showing what traffic is actually identified?
Web and App Traffic Shaping	Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared	› Does your solution enable traffic shaping or QoS based on app, category, user, group, or rule?
URL filtering	Controls web usage to prevent non-compliant surfing and keep inappropriate content and malware off the network.	› Does your firewall contain a inheritance-based web gateway policy engine - for example, if you need to do something just a little different for a user, do you need to create a whole new web policy, or can you define just what you want to do different, and let it inherit the rest? Are there pre-configured policies for workplaces, CIPA compliance (etc.)? › Beyond blocking, can it also warn about potentially inappropriate websites allowing the user to proceed? › Does your firewall include web keyword monitoring and can I upload my own lists, as relevant to my sector or region?
Web Compliance Features	Ensures compliance when searching or using Google Apps.	› Can your web control solution enforce our Google Apps domain? › Does it enforce SafeSearch on major search engines? › Can it enforce additional image filtering such as only those with a Creative Commons license?
User Risk Assessment	Provides an overview of riskiest users based on their network activity and recent history.	› Does your firewall provide insights into high-risk users based on their recent network behavior and activity? › Is there a widget on the dashboard? › Is there a full, detailed report?
Application Risk Assessment	Provides an overall risk metric for your organization's network.	› Does your firewall provide an overall application risk assessment? › Is there detailed historical reporting on application's usage?
HTTPS scanning	Provides visibility into encrypted web traffic to ensure compliance.	› Does your firewall offer HTTPS man-in-the-middle decryption? › Exceptions handling options? › Does it block unrecognized SSL protocols and invalid certs?

The importance of a layered threat defense

Cybercriminals are continually changing their attack methods to avoid detection. These days, nearly every malware instance is a new zero-day variant that hasn't been seen before and is more sophisticated, stealthy, and targeted than the one that came before it. This makes traditional signature-based detection obsolete. You need multi-layered defense across several vectors, each using behavioral analysis and working better together to provide adequate protection.

There are seven key technologies your network perimeter requires to provide an adequate defense against modern threats.

- **Advanced Threat Protection** – Advanced threat protection is important to identify bots, APTs, and other threats already operating on your network. Ensure your next firewall has malicious traffic detection, botnet detection, and command and control (C&C) call-home traffic detection. The firewall should use a collaborative approach that combines IPS, DNS, and web telemetry to identify call-home traffic.
- **Identify and Isolate Compromised Systems** – To prevent data loss and further infections, and to accelerate remediation, your firewall should immediately identify not only the infected host, but the user and process in the event of an incident, and ideally, it should also automatically block or isolate compromised systems until they can be investigated and cleaned up (preferrably automatically by your endpoint protection).
- **Intrusion Prevention** – Intrusion prevention systems (IPS) can detect hackers attempting to breach your network resources. Ensure your firewall has a next-gen IPS that's capable of identifying advanced attack patterns on your network traffic to detect hacking attempts and malware moving laterally across your network segments. Also consider a solution that offers the capability to block entire GeoIP ranges for regions of the world you don't do business with to further reduce your surface area of attack.
- **Sandboxing** – Sandboxing can easily catch the latest evasive malware and advanced threats like ransomware and botnet malware before it makes its way onto your computers. Ensure your firewall offers advanced sandboxing that can identify suspicious web or email files and detonate them in a safe sandbox environment to determine their behavior before allowing them into your network.
- **Web Protection** – Effective web protection can prevent botnet-recruiting malware from getting onto your network in the first place. Ensure your firewall has dual antivirus engines and behavioral-based web protection that can actually emulate or simulate JavaScript code in web content to determine intent and behavior before it's passed to the user's browser.
- **Email Protection** – Email is still one of the primary entry points for threats and social engineering exploits. Be sure that your next firewall or email filtering solution has top-shelf anti-spam and anti-phishing technology to detect the latest malware lurking in emails and their attachments.
- **Web Application Firewall** – A WAF can protect your servers, devices, and business applications from being hacked. If you manage any servers or business applications in-house that require access from the internet, ensure your firewall offers full WAF protection. A web application firewall should provide a reverse proxy, offload authentication, and should also harden systems from being hacked.

Capability to look for	Description	Questions to ask your vendor
Advanced Threat Protection	Identifies bots and other advanced threats and malware attempting to call home or communicate with command and control servers.	‣ What level of advanced threat protection does your firewall offer? ‣ Does it coordinate information from a variety of sources to detect malicious traffic or is it just a simple botnet database?
Compromised System Detection	Identifies infected systems on your network.	‣ Can your firewall pinpoint the exact host, user and process infected? ‣ Is your firewall aware of the health status of endpoints? ‣ Does it provide instant visibility into the health status of your endpoints?
Compromised System Isolation	Use firewall rules to isolate compromised systems until they can be cleaned up.	‣ Can your firewall automatically isolate infected or potentially compromised systems on the network without user or admin intervention? ‣ Will it automatically restore normal access when the endpoints are cleaned up?
Sandboxing	Protects from zero day threats by sending potentially harmful files to the cloud sandbox to be detonated and observed in a safe environment.	‣ Do you need to buy additional hardware to get additional layer of security? ‣ How much time does your solution take to analyze suspected files?
Web Protection	Provides protection from web-based malware, compromised websites and web downloads.	‣ Does your web protection engine offer signatureless behavioral analysis of web code like JavaScript? ‣ Does your web protection offer multiple antivirus engines? ‣ Are live updates available?
HTTPS scanning	Provides visibility into encrypted web traffic to protect the network against threats that can be transmitted via HTTPS.	‣ Does your firewall offer HTTPS man-in-the-middle decryption? ‣ Exceptions handling options? ‣ Block unrecognized SSL protocols and invalid certs?
Email Anti-Spam and Anti-Phishing	Stops spam, phishing, and other unwanted email from being delivered to employees' inboxes.	‣ What are your spam detection and false-positive rates? ‣ What techniques do you use to identify spam and phishing? ‣ Does your email solution offer domain-based routing and a full MTA mode to store and forward messages? ‣ Does it offer a user portal for quarantine management?
Web Application Firewall	Provides protection for servers and business applications exposed to the internet	‣ Does your firewall include a WAF? ‣ Does it provide templates? ‣ Does it provide protection from hacks and attacks with form hardening, URL hardening, cookie tamper protection and cross-site scripting protection? ‣ Does it provide a reverse proxy with authentication offloading?

Comparing firewall solutions

When comparing firewall solutions there are a number of other factors you should consider alongside security and control features.

VPN and wireless connectivity

Site-to-site and remote access VPN is a critical component of any firewall solution. Make sure your next firewall includes all the standards-based VPN connectivity you need and see what other options they offer for connecting users to internal resources or securing your remote locations. Make sure these other options are lightweight and dead simple.

With wireless becoming a staple in every network, consider a firewall that integrates a full-featured wireless controller with support for a wide range of high performance wireless access points to meet your wireless networking needs.

Deployment options

When selecting your next firewall solution, make sure it will fit your business, and not the other way around. Consider not only your current topology and infrastructure, but where you might be next year or a few years from now. Be sure to select a firewall that offers a flexible choice of deployment both on-premises and in the cloud, with management tools to match. If you have several small remote locations, consider how you can securely connect those into your network simply and affordably.

Performance

It's important to consider your network performance needs not only today, but down the road as the demands on your network grow. Users all have multiple devices, and an increasing number of services are moving to the cloud, putting unprecedented demands on network bandwidth and firewall throughput.

Choose a solution that allows you to scale easily, and adapt to your changing needs with features like high availability and multiple WAN link balancing for redundancy or performance. Also, look at firewalls with performance enhancing technologies like FastPath packet optimization that puts known traffic on the fast path through the firewall stack to accelerate performance.

Integration with other IT security solutions

Integrating your IT security solutions like your firewall and endpoints can provide significant benefits such as coordinated protection, immediate identification of infected systems on your network, enhanced app control capabilities, and an automated response by isolating infected systems until they can be cleaned up. While this is a relatively new way of synchronizing security, it has been extremely effective and is quickly becoming a key requirement for many organizations. Consider a vendor that has leading technology in both firewalls and other IT security areas such as endpoint, server, encryption, and mobile protection, and enables them to work better together in a coordinated and synchronized fashion.

Reporting and alerting

As outlined at the beginning of this document, visibility and insight into what's happening on the network is one of the top complaints with firewalls today. Make sure this isn't one of your problems by selecting a firewall that includes rich historical reporting with the option to add centralized reporting across all your firewalls if you need it. And be sure to check the level of insights the firewall provides on the dashboard and throughout important areas of the firewall. Don't let your firewall make you go digging for the information you need.

Ease-of-use

Configuring and maintaining your firewall can range from easy to infuriating. You don't have to be one of the many who struggle to figure out how to setup your firewall properly because your vendor made it too complex. Find a solution that thinks the way you do from a vendor that is focused on making your day-to-day management as streamlined and easy as possible.

Another time-saving feature that's often overlooked is making sure your users can help themselves. Look for a firewall that offers a secure self-help portal for users to download VPN clients and manage their email quarantine.

Try XG Firewall online for free.
sophos.com/demo

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

18-08-07 BG-NA (3074-DD)

SOPHOS