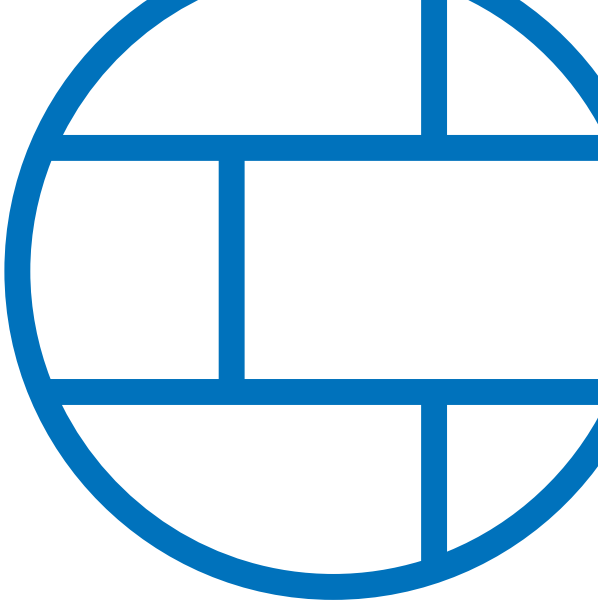
SOPHOS



Next-Gen Firewall Buyer's Guide

We surveyed IT network managers to name their top issues with their existing firewall. Here are problems they cited:

- Visibility into application traffic, risks, and threats
- Protection from the latest threats
- No response or assistance when there is a threat on the network

If any of these sound familiar, you're not alone. The fact is, most next-generation firewalls today are failing to do their job. They are not able to provide adequate visibility, appropriate protection, or any kind of response.

It can be challenging to even know where to start. You'll want to begin by identifying your key requirements. 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 not only meet your needs, but actually do what it claims.

How to use this guide

This buyers guide is designed to help you choose the right solution for your organization so that you don't end up with firewall buyer's remorse. It covers all the features and capabilities you should consider when evaluating your next firewall purchase. We've also included 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

Next-gen firewalls have long promised to deliver visibility into application traffic and user activity on the network. Today, however, most are failing at this basic task. The problem lies with the old-school signature-based application identification technology modern firewalls use. It is no longer effective at identifying encrypted, evasive, and custom apps, or even those apps masquerading as web browsers using generic HTTP and HTTPS. As a result, applications such as peer-to-peer, VPN tunneling clients, and games are going completely undetected on most networks. New techniques and technologies are required to solve this 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 mission-critical application traffic while blocking or limiting unwanted apps. Most next-gen firewalls fail to provide adequate application visibility and control due to limitations with signature-based application identification. Make sure your next firewall uses the latest techniques to address this problem and reveal the hundreds of apps that are likely going unidentified on your network.

Web Control – URL filtering policies are important for compliance to ensure a safe environment for all your users, especially if you're in education. 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. Be 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. Make certain your next firewall provides a risk assessment report for users that correlates their network activity to identify your riskiest users. Also, look for clear indicators of suspicious cloud application usage, shadow IT, risky downloads, objectionable websites, and the presence of threats.

HTTPS Scanning – With more than 80% of internet traffic now encrypted, compliance enforcement is challenging unless you have adequate HTTPS scanning. Since HTTPS scanning can be invasive and resource-intensive, make sure your next firewall includes selective scanning and easy solutions for managing exceptions without negatively impacting performance.

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 able 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 firewall integrate with the hosts on the network to identify all evasive and unknown applications generating encrypted or HTTP type traffic? ‣ Can you provide a sample firewall report showing what traffic is actually identified? ‣ 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)?
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 an 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 differently, 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 and identifies risky behavior when browsing, searching or using Google Apps.	‣ Can your web control solution enforce our Google Apps domain? ‣ Does it enforce SafeSearch and YouTube restrictions on a user or group policy basis? ‣ Can it enforce additional image filtering such as only those with a Creative Commons license? ‣ Can it identify potentially problematic behavior related to bullying, self-harm, or radicalization based on dynamic content filtering and keyword monitoring? ‣ Does it allow staff members such as teachers to set up temporary policy exceptions for users or groups?
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 for easy access to information? ‣ 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 usage?
HTTPS Scanning	Provides visibility into encrypted web traffic to ensure compliance and identify hidden threats.	‣ Does your firewall offer HTTPS man-in-the-middle decryption? ‣ Does it offer exceptions handling options? ‣ Does it block unrecognized SSL/TLS protocols and invalid certs? ‣ Does it support scanning of traffic that is encrypted using the the latest encryption protocols?

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 a multi-layered defense across multiple vectors, each using behavioral analysis, deep learning, and other next-gen techniques 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 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. It should also integrate and interact with hosts on the network to understand their health and state of compromise.

Identify and Isolate Compromised Systems – To prevent data loss and the spread of infections to other systems on the network, and to accelerate remediation, your firewall should immediately identify not only the infected host, but also the user and process in the event of an incident. Ideally, it should also automatically block or isolate compromised systems until they can be investigated and cleaned.

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. To further reduce your attack surface area, consider a solution that offers the capability to block entire GeoIP ranges for regions of the world where you don't conduct business.

Sandboxing – Sandboxing can easily catch the latest evasive malware and advanced threats like ransomware and botnet malware before they make their way onto your computers. Ensure your firewall offers advanced sandboxing with the latest technologies such as deep learning, exploit detection, ransomware detection, analysis of behavior, network activity, and memory utilization.

Web Protection – Effective web protection can prevent the latest web threats such as cryptojacking and 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 remains 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 technologies to detect the latest malware lurking in emails and their attachments.

Web Application Firewall (WAF) – A WAF protects your servers, devices, and business applications from being hacked. If you manage any servers or business applications in-house that require access to the internet, ensure your firewall offers full WAF protection. A web application firewall should provide a reverse proxy, offload authentication, and 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? ‣ Does your firewall integrate with hosts on the network to understand if they have any signs of compromise even if there is no network evidence?
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 connected 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.	‣ Can your firewall automatically isolate infected or potentially compromised systems on the network without user or admin intervention? ‣ Will it automatically restore normal access once the endpoints are cleaned?
Sandboxing	Protects against 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 extra layers of security? ‣ How much time does your solution take to analyze suspected files? ‣ What next-gen technologies does your sandbox solution employ to reveal zero-day threats such as the latest ransomware? For example, deep learning, exploit detection, and encryption detection?
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? ‣ Does your firewall support the latest TLS standard for inspecting encrypted traffic? ‣ Does it provide exceptions handling options? ‣ Does it 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 several other factors you should consider alongside security and control features.

SD-WAN, VPN, and wireless connectivity

SD-WAN capabilities are increasingly important considerations when purchasing a new firewall. Make sure your firewall supports multiple WAN links including options for prioritization, routing, and failover. Using a firewall solution with integrated SD-WAN will enable you to connect remote sites, deliver applications, and share data for a lot less than the price of MPLS.

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

Wireless has become a staple in every network, so 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 researching your next firewall solution, make sure it fits your business, and not the other way around. Consider not only your current topology and infrastructure, but also where you might be next year or a few years from now. Select a firewall that offers a flexible choice of deployment options including both on-premises and in the cloud, with management tools to match. If you have several small remote locations, consider technologies such as SD-WAN to securely connect those sites into your network simply and affordably.

Performance

It's important to consider your network performance needs not only today, but also 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 such as high availability and multiple WAN link balancing for redundancy and performance. Also, look at firewalls with performance-enhancing technologies like FastPath packet optimization which 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 including 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. While this is a relatively new way of synchronizing security, it is extremely effective and has quickly become 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, enabling 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 network activity 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 flexibility 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 set up 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-service portal for users to download VPN clients and manage their email quarantine.

Side-by-side comparison

Use our product comparison checklist on the next page to see which solutions make your shortlist. Once you find some that meet your criteria, try them and price them out.

Product comparison checklist

After reviewing the previous sections to identify your minimum requirements, use this table to evaluate different solutions to determine which meet your shortlist for evaluation. Of course, you can also add any additional requirements you may have to meet the specific needs of your organization.

	Sophos XG	Cisco Meraki	Fortinet FortiGate	SonicWall NSa	WatchGuard Firebox
NEXT-GEN FIREWALL FEATURES					
Firewall Rule and Web Policy Test Simulator	✓		✓		✓
Dual Antivirus Engines	✓				✓
FastPath Packet Optimization	✓		✓		
Intrusion Protection System	✓	✓	✓	✓	✓
Application Control	✓	Partial	✓	✓	✓
Synchronized App Control (using Endpoint telemetry)	✓				
Shadow IT Cloud App Visibility	✓		✓	✓	
Block Potentially Unwanted Applications (PUAs)	✓		✓	✓	
Web Protection and Control	✓	✓	✓	✓	✓
Web Keyword Monitoring and Enforcement	✓		✓	✓	✓
User and App Risk Visibility (User Threat Quotient)	✓		Partial		
Filtering of HTTPS Data	✓	✓	✓	✓	✓
SSL Inspection Mode – TLS 1.3 Version Support	✓		IPS engine only		✓
ADVANCED THREAT PROTECTION					
Advanced Threat Protection	✓	✓	✓	✓	✓
Compromised System Detection	✓		+1Box *		✓
Compromised System Isolation	✓		+1Box *		✓
Lateral Movement Protection	✓				✓
Sandboxing	✓	✓	✓	✓	✓

	Sophos XG	Cisco Meraki	Fortinet FortiGate	SonicWall NSa	WatchGuard Firebox
SERVER AND EMAIL PROTECTION					
Full-Featured WAF	✓		+1Box *	+1Box *	
Complete Email: Antivirus, Anti-Spam, Encryption, DLP	✓		+1Box *	+1Box *	
CONNECTING USERS/REMOTE OFFICES					
IPSec and SSL VPN	✓	No SSL VPN	✓	✓	✓
Wireless Mesh Networks	✓	✓	✓	✓	✓
Plug and Protect Remote Office Security (RED)	✓				
SD-WAN	✓	✓	✓	✓	✓
EASE OF DEPLOYMENT AND USE					
Flexible Deployment (HW,SW,VM,IaaS)	✓	HW Only	No SW	No SW	No SW
Integrates with Other IT Security Products (e.g. Endpoint)	✓		✓	✓	
Synchronized Security in Discover (TAP) Mode Deployments	✓				
Free Historical Reporting	✓		+1Box *	+1Box *	+1Box *
Free Central Management	✓	✓	Partial		
Central Management for Partners	✓	✓	✓	✓	
User Self-Serve Portal	✓		✓	✓	

* These features require an additional product/device adding cost and complexity.

Statements contained in this document are based on publicly available information as of January, 2020. This document has been prepared by Sophos and not the other listed vendors. The features or characteristics of the products under comparison, which may directly impact the accuracy or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own purchasing decision based on their individual requirements, and should also research original sources of information and not rely only on this comparison while selecting a product. Sophos makes no warranty as to the reliability, accuracy, usefulness, or completeness of this document. The information in this document is provided "as is" and without warranties of any kind, either expressed or implied. Sophos retains the right to modify or withdraw this document at any time.

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

2019-12-19 BG-NA (RP)