SOPHOS

2025 NEXT-GEN FIREWALL BUYER'S GUIDE

Top issues with Network Security and Next-Gen Firewalls today:

- Too many products, vendors, and management consoles.
- Unforeseen cost and complexity.
- Lack of security and protection best practices built-in.

If you're experiencing any of these issues, you're not alone. Most organizations share the same frustrations and are seeking a solution that allows them to consolidate, simplify, and save, while improving their protection and security posture.

How to use this guide

This buyers guide is designed to help you choose the right solution so 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 and network security purchase.

We've also included important questions to ask your IT partner or vendor to ensure the product will meet your needs. And on the last few pages, we've added a convenient time-saving chart that can help you create a shortlist of suitable firewall vendors.

Imagine your ideal solution

Consider items you won't find on any feature checklist.

Imagine if you could:

- Use a single cloud management console for all your firewalls, network security infrastructure, and the rest of your cybersecurity portfolio.
- Deal with only a single vendor with transparent licensing, affordable pricing, and great support for all your cybersecurity needs.
- Have cybersecurity products that were secure by design and if any new vulnerabilities we're discovered they could be patched over-the-air without scheduling downtime.
- Your day-to-day management was easy, with no blind spots, amazing insights, and all the information you need at your fingertips with deep drill-down reporting that didn't cost you extra.
- Your firewall got better protection AND performance with every update.
- You got all this tremendous value at a very competitive and affordable price.

The thing is, you won't find these items on most product feature lists. But don't settle for less! Look at solutions that allow you to consolidate, simplify, and save while enhancing your network security best practices.

Network Security Best Practices

It's critically important that your next firewall and broader network security portfolio implement best practices to better protect your network from threats and attacks.

Best practices generally fall into one of these three areas:

01 Mitigation tools and technology to reduce the surface area of attack - including hardening your infrastructure.

02 Protection to block threats and attacks before they get on the network.

03 Detection and response capabilities that can identify and stop an active adversary operating on the network.

The problem is that most next-gen firewalls out there are failing to implement best practices in these three areas effectively. Most firewall products are focused only on "protection"- or blocking threats or attacks at the gateway. Very few vendors are making their products a tough target or looking inside the network for an attacker that's already there.

Mitigation

Mitigation is about ensuring your internet-facing network infrastructure is minimized, secure by design, hardened against attack, and tightly controlled, all while ensuring any newly discovered vulnerabilities are patched quickly.

Most firewalls are running on aging platforms that have unpatched vulnerabilities that are increasingly being targeted by attackers to get a foothold on your network. That's partly because most firewalls require scheduling downtime to fix any newly discovered vulnerability, and most organizations don't have time or resources to continually manage this.

What to look for in your next firewall:

- **Consolidation**: Look for a firewall that consolidates remote access VPN and Zero-Trust (MFA and ZTNA) into the firewall to minimize exposed infrastructure.
- **Secure by Design:** Look for a vendor that is committed to building products that are more secure, hardened, and have tight access controls.
- **Over-the-Air Updates:** Look for a firewall that offers easy over-the-air security patches without downtime.
- **Proactive Monitoring:** Look for a vendor that is continually monitoring their customer's firewalls for signs of attack and swiftly taking action in the event you are targted – without requiring an extra subsciption.

Protection

Protection is all about catching threats as they attempt to enter the network using the latest AI and machine learning technology to catch the latest zero-day attacks.

What to look for in your next firewall:

- **TLS 1.3 Inspection:** With the vast majority of internet traffic now encrypted, this is a critical capability. However, not all TLS inspection solutions are created equal. Look for a solution that is easy to manage, provides granular controls over what to inspect and what not to, supports the latest standards and cipher suites, and provides valuable insights into potential incompatibilities. Most importantly, choose a solution that won't slow down your network.

- **Zero-day threat protection:** Your next firewall must have artificial intelligence based on multiple machine learning models, plus sandboxing with advanced exploit and ransomware detection to identify the latest zero-day threats and stop them before they get on your network.

- **Programmable architecture:** Many firewall products include custom silicon to accelerate the processing of various network traffic flows. Make sure you're buying a future-proof solution that doesn't rely on custom ASIC chips that cannot be upgraded without a full hardware upgrade. Get a firewall with a programmable flow processor architecture that allows additional protection and performance to be unlocked down the road.

Detection and Response

Detection and response is all about identifying active adversaries that somehow got on the network and shutting them down before they cause a real problem. This is where most next-gen firewalls fail miserably. If you have an active attack on your network, it's very unlikely your firewall will know, and even more unlikely that it will be able to do anything to help stop it. But there is a very elegant and effective solution out there: only available from Sophos.

What to look for in your next firewall:

- **Integrated Network Detection and Response:** NDR is a category of network security products that has been around for many years, but only one vendor has integrated NDR with their firewall: Sophos. This provides an enormous advantage in detecting active adversaries operating on the network early so they can be shut down before they become a real problem.

- **Automated response to active attacks:** Only one vendor has implemented an automated response mechanism to help isolate and contain an active attack: Sophos. Sophos Active Threat Response enables the firewall to respond to threat feeds from a variety of sources, including Sophos X-Ops, an MDR or XDR analyst, or a third-party feed, and kick off a Synchronized Security response automatically that coordinates between various Sophos products, including endpoints, wireless, switches, and email products to isolate a compromised deivce until it can be cleaned up. This can reduce response times from hours or days, to mere seconds. And it doesn't require any extra products, licenses or management consoles. It just works!

Best Practices	Questions to Ask Your Vendor
Consolidation	▸ Do you have a single cloud management console for firewalls, switches, wireless, email, ZTNA, and other cybersecurity products? ▸ Is ZTNA and remote access VPN included at no extra charge? ▸ Is dashboarding and reporting included at no extra charge? ▸ Is point-and-click SD-WAN orchestration included? ▸ Are multiple threat feeds included? ▸ Is MDR/XDR integration included? ▸ Do products share information (e.g. firewall and endpoint)?
Secure By Design and Proactive Monitoring	▸ In the event a new vulnerability is discovered and a patch is required can it be applied over-the-air without scheduling down time for a firmware update? ▸ Is your product hardened from attack? How? ▸ Do you actively monitor your customer install base remotely for signs of attack and respond if there is an attack?
Protection	▸ Do you support TLS 1.3 and the latest standards for inspecting encrypted traffic? ▸ What type of technology are you using with AI and machine learning to catch zero-day threats? ▸ Does your sandboxing technology run in the cloud or on-box and what endpoint technology is it using to detect threats in the sandbox?
Programmable Architecture	▸ Does your firewall platform offer FastPath or other techniques to offload certain traffic flows for optimized protection and performance? ▸ Does your architecture use ASICs or is it upgradable via firmware without having to upgrade the hardware?
Integrated NDR	▸ Does your firewall offer an integrated NDR solution? ▸ Is it included at no extra charge? ▸ Is it cloud-based to eliminate any performance impact on the firewall? ▸ Is it easy to manage? ▸ Does it catch encrypted malware traffic without using man-in-the-middle TLS decryption?
Automated Response	▸ When an active adversary or attack is discovered, what does your firewall do to respond? ▸ Is it automatic – how long does it take? ▸ Does it coordinate the response with other products? ▸ What is required to make it work?

Core firewall capabilities

The following technologies are also essential components of any firewall solution. Most of these capabilities are mature, well-established staples in any firewall, so vendors are often differentiated based on ease of management and the level of actionable visibility they provide.

Be sure that your next firewall not only includes these features, but provides easy management – and more importantly, greater visibility into risks and issues in each of these areas.

Core capabilities	Questions to Ask Your Vendor
Deep packet inspection and intrusion prevention Provides decryption and inspection for threats and exploits	▸ Does your TLS inspection support the latest 1.3 standard? ▸ Does it work across all ports and protocols? ▸ Is it streaming based or proxy based? ▸ What is the performance impact? ▸ Does it provide dashboard visibility into encrypted traffic flows? ▸ Does it provide dashboard visibility into sites that don't support decryption? ▸ Does it provide simple tools to add exceptions for problematic sites? ▸ Does it come with a comprehensive exclusion list? ▸ Who maintains the list and is it updated periodically?
Advanced threat protection Identifies bots and other advanced threats and malware attempting to call home or communicate with command and control servers	▸ Does your firewall include technology to detect previously unseen threats? ▸ Does it use machine learning to analyze files? ▸ How many machine learning models are applied? ▸ Does your solution include sandboxing? ▸ Does the sandboxing allow the file through while it's being analyzed? ▸ Does the sandboxing solution run on-premises or in the cloud? ▸ Does the sandboxing solution include leading endpoint protection technology to identify threats like ransomware in the sandbox environment? ▸ What endpoint technology is used to assist in sandboxing? ▸ What kind or reporting is provided on-box (versus a separate reporting product)? ▸ What kind of dashboard visibility is provided?
Deep packet inspection and intrusion prevention Provides decryption and inspection for threats and exploits	▸ Does your TLS inspection support the latest 1.3 standard? ▸ Does it work across all ports and protocols? ▸ Is it streaming based or proxy based? ▸ What is the performance impact? ▸ Does it provide dashboard visibility into encrypted traffic flows? ▸ Does it provide dashboard visibility into sites that don't support decryption? ▸ Does it provide simple tools to add exceptions for problematic sites? ▸ Does it come with a comprehensive exclusion list? ▸ Who maintains the list and is it updated periodically?
Application control Visibility and control over application traffic to shape or block unwanted traffic and accelerate and prioritize essential application traffic	▸ What sources of information are used to identify applications? ▸ Can the application engine use information obtained from the endpoint to greatly enhance application identification, or is it limited to only what the firewall can glean from the packet? ▸ Can applications be assigned to the FastPath and routed out preferred WAN links using policy rules? ▸ Does the system provide dashboard insights into cloud apps and shadow IT?

Complimentary firewall products

The following complimentary products may be important to extend your network and protection where it's needed. Make sure your vendor of choice offers these additional products and makes them easy to integrate with your firewall, either managed directly from the firewall and/or through the same central management console as the firewall.

Complimentary products	Questions to Ask Your Vendor
Branch office SD-WAN edge devices Affordable, easy-to-deploy devices for connecting small remote branch offices	▸ Do you offer a device for connecting remote locations via a dedicated VPN back to the main firewall? ▸ Is it zero-touch to deploy? ▸ How much does it cost? ▸ Does it support both a dedicated and split-tunnel? ▸ What modular connectivity options does it support such as Wi-Fi or LTE?
Wireless access points Extend the network to include wireless	▸ Does the firewall include a built-in wireless controller? ▸ How much does it cost? ▸ Are your wireless access points plug and play? ▸ Do they support multiple radios and SSIDs? ▸ Do they support mesh networking?
ZTNA Zero-trust network access for connecting remote users securely to applications and data	▸ Do you offer a ZTNA solution? ▸ Is it integrated in any way with your firewall and/or endpoint? ▸ Is it managed from the same central management console as the firewall? ▸ Does the ZTNA agent deploy alongside your endpoint agent? ▸ How is device health integrated into your ZTNA solution?
Email protection Protection for email from spam, phishing, and unwanted email	▸ Do you offer an integrated on-box email protection solution? ▸ Do you offer cloud-managed email protection? ▸ Does it include sandboxing of suspicious attachments? ▸ Does it support email encryption and DLP? ▸ Does it provide domain-based routing and a full MTA mode? ▸ Does it offer a user portal for quarantine management?
WAF Web Application Firewall for reverse proxy protection of on-premises servers exposed to the internet	▸ Do you offer an integrated on-box WAF capability? ▸ Does it make setup easy with pre-defined templates for common server hosted applications? ▸ Does it provide hardening, CSS, and cookie tamper protection? ▸ Does it provide reverse proxy authentication offloading?
NDR Network Detection and Response for detecting active adversaries and attacks	▸ Do you offer an integrated NDR capability? ▸ Is it included with the firewall for no extra charge? ▸ Is it cloud based to eliminate any performance impact on the firewall? ▸ Is it easy to manage? ▸ Does it catch encrypted malware traffic without using man-in-the-middle TLS decryption?

Management capabilities

Firewall products are often differentiated by how easy they are to manage. Many firewalls that have been on the market for decades suffer from having new capabilities bolted onto the product over time using different user interface concepts that make every section of the product seem like a completely different product. The following capabilities can make a huge difference in the deployment and day-to-day management.

Management capabilities	Questions to Ask Your Vendor
Central management Managing multiple firewalls or IT security products	▸ Do you offer a cloud management solution? ▸ How are multiple firewalls managed through this solution? ▸ What other products are managed from the same cloud console? ▸ Is threat intelligence shared across products and is cross-product threat hunting possible?
Reporting What reporting capabilities are offered	▸ Does the firewall include on-box storage for log data? How much? ▸ Is on-box reporting included? How much does it cost? ▸ Is cloud reporting supported? How much does it cost? ▸ Can custom reports be created, saved, exported, scheduled? ▸ Is syslog export supported? ▸ Is cross-product reporting and threat hunting supported?
Management experience How well does the firewall simplify day-to-day management and highlight what's important	▸ Does your product offer a rich dashboard with drill-down capabilities? ▸ Are policies for web, app control, IPS, and traffic shaping all together in one place, or do I need to set these components up in different areas of the product? ▸ Is the user experience consistent from one part of the product to the next? ▸ Is there extensive built-in context sensitive help, documentation, videos and other content for a new firewall owner?
User portal Portal for users to help themselves	▸ Does your firewall offer a user portal for users to download VPN clients or settings and manage quarantined emails?

Deployment options

Another important consideration for your next firewall is how easily it will integrate into your network both today and down the road. You want a firewall that fits your network, not one that demands your network fit the firewall. Ensure your vendor offers a variety of deployment options including public cloud platform support such as AWS and Azure, as well as popular virtualization platforms, and flexible, modular hardware appliance options.

Deployment options	Questions to Ask Your Vendor
Hardware appliances Ensure your next firewall is as futureproof as possible	▸ How many models of appliances do you offer that suit my needs? ▸ What connectivity options are included? ▸ What modular connectivity options are included? ▸ Are redundant power supplies available? ▸ What high-availability options are available? ▸ Are firmware upgrades included in the licensing? ▸ What is the hardware warranty?
Cloud, virtual, software Public cloud and virtual support for hybrid networks that may be important today or in the future	▸ Is your firewall available in the marketplace for public cloud platforms such as AWS and Azure? ▸ Do you support all popular virtualization platforms? ▸ Is your appliance available as a software solution to run on X86 hardware?

Firewall Feature Checklist

It's critically important that your next firewall and broader network security portfolio implement best practices to better protect your network from threats and attacks.

Core Firewall Capabilities	Sophos	Meraki	Fortinet	PAN	SW	WG
Firewall rule and web policy test simulator	✓		✓	✓		✓
FastPath packet optimization	✓		✓	✓		
Intrusion protection system	✓	✓	✓	✓	✓	✓
Application control	✓	Limited	✓	✓	✓	✓
Application IDs from managed endpoints	✓					
Dual AV engines	✓					✓
Shadow IT cloud app visibility	✓		✓	✓	✓	✓ - OEM
Block Potentially Unwanted Applications (PUAs)	✓		✓	✓	✓	
DNS Protection	✓		✓	Extra*	✓	✓
Web keyword monitoring and enforcement	✓		✓	✓	✓	✓
User and app risk visibility (User Threat Quotient)	✓		Limited			
Advanced threat protection	✓	✓	✓	✓	✓	✓
On-box logging and historical reporting	✓		Limited	Limited	Limited	Limited

Server and Email Protection	Sophos	Meraki	Fortinet	PAN	SW	WG
On-box full-featured WAF	✓		Extra*			
On-box email: antivirus, anti-spam, encryption, DLP	✓		Limited		Limited	Limited

SD-WAN and VPN	Sophos	Meraki	Fortinet	PAN	SW	WG
Unlimited free full-featured remote access VPN	✓	Extra*	✓	Extra*	Extra*	Extra*
IPSEC and SSL site-to-site VPN	✓	✓	No SSL	✓	✓	✓
SD-RED Layer-2 site-to-site VPN	✓					
SD-WAN cloud-managed orchestration	✓	✓	Extra*		✓	
SD-WAN routing and link management	✓	✓	✓	✓	✓	✓
SD-WAN zero-impact fail-over transitions	✓		✓	✓		
SD-WAN identification and routing of unknown or custom app traffic	✓			✓		
Hardware acceleration and offloading of VPN traffic	✓		✓			
Zero-touch affordable VPN tunnel devices	✓					

TLS Inspection	Sophos	Meraki	Fortinet	PAN	SW	WG
TLS 1.3 inspection	✓		✓	✓	✓	✓
Dashboard visibility into encrypted traffic issues	✓					
Create TLS exceptions from dashboard	✓					

* These capabilities are available at extra cost

Zero-Day Threat Protection	Sophos	Meraki	Fortinet	PAN	SW	WG
Multiple ML model analysis of suspicious files	✓	✓	✓	✓		✓
Dynamic sandboxing of suspicious files	✓	✓	✓	✓	✓	
Cloud-based file analysis	✓	✓	✓	✓	✓	✓
Extensive on-box threat analysis reporting	✓	✓		✓		✓

FastPath Packet Optimization	Sophos	Meraki	Fortinet	PAN	SW	WG
Fastpath offloading of SD-WAN, cloud, SaaS traffic	✓		✓	✓		
Policy and automatic FastPath offloading	✓		✓	✓		
Hardware offloading and acceleration	✓		✓	✓		
Programmable architecture and packet flow processors	✓			✓		

Detection and Response	Sophos	Meraki	Fortinet	PAN	SW	WG
NDR Integration	✓					✓
Pre-configured automatic threat response across product portfolio included at no extra cost	✓					

Network Access Portfolio Integration	Sophos	Meraki	Fortinet	PAN	SW	WG
Integrated wireless controller and access point solution	✓	✓	✓		✓	✓
Integrated ZTNA Gateway in the Firewall	✓		✓		✓	
Integrates with network switch products	✓	✓	✓		✓	
Integrates with remote service access edge devices (SD-RED)	✓					

Cloud Management	Sophos	Meraki	Fortinet	PAN	SW	WG
Full-featured firewall management from the cloud - no extra charge	✓	✓	Extra*	✓	Extra*	✓
Single cloud console for EP, server, mobile, email, encryption, and firewall	✓					✓
Group firewall management from the cloud	✓	✓	Extra*	✓	✓	
Schedule firmware updates from the cloud	✓	✓	✓	✓	✓	✓
Deploy new firewalls from the cloud (zero-touch)	✓	✓	Extra*	Limited	✓	✓
Cloud firewall reporting	✓	✓	Extra*	Limited	✓	✓
Cloud managed cross-product threat hunting (XDR)	Extra*			Extra*		

Cloud and Virtual Deployment Options	Sophos	Meraki	Fortinet	PAN	SW	WG
AWS	✓	✓	✓	✓	✓	✓
Azure	✓	✓	✓	✓	✓	✓
Google	Future	✓	✓	✓		
Nutanix	✓		✓	✓	✓	
Virtual platforms	✓	✓	✓	✓	✓	✓
Software appliance (x86)	✓					

* These capabilities are available at extra cost

Sophos Firewall Resources

If you're interested in learning about the capabilities and features of Sophos Firewall, be sure to check out these resources:

- Sophos Firewall Solution Brief
- Sophos Firewall Features List
- Sophos Firewall Brochure

SOPHOS

Try Sophos Firewall online for free:
www.sophos.com/demo

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

2025-07-17 EN (MP)