SOPHOS
Cybersecurity evolved.

Next-Gen Firewall Buyer's Guide

In recent surveys, network administrators and IT managers cite the following top issues with their existing firewall:

- Poor visibility into network applications, risks, and threats
- Concerns about protection from the latest ransomware and attacks
- Lack of any response or assistance when there is a threat on the network

If any of this sounds familiar, you're not alone. The problem 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.

When selecting a shortlist for your next firewall, 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 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 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.

The perfect storm in network security: encryption

Ever-increasing encrypted traffic flows have created a perfect storm – with dire consequences. Consider these important facts:

- 90% of internet traffic is now TLS encrypted
- 50% of malware, PUA, and hacker servers are utilizing encryption to avoid detection
- The vast majority of organizations are not inspecting encrypted traffic

When we ask organizations why they are not inspecting encrypted traffic, they cite performance as the number one reason. TLS inspection is simply too resource intensive for most firewalls to keep up with the huge volume of encrypted traffic. The second major reason for not inspecting encrypted traffic. It tends to cause usability issues; it breaks the internet.

This fundamental challenge with encryption and an inability to address it by most firewalls is creating a variety of other issues: visibility into risky behavior and content, compliance, and protection from ransomware, attacks, and breaches. In effect, encryption is the root cause of many of today's top network security challenges. Unfortunately, most networks are simply turning a blind eye to the vast majority of traffic passing through them. This is no longer necessary. There is a very effective way to deal with this challenge.

To learn more, check out: Has Encryption Made Your Current Firewall Irrelevant?

Top critical capabilities

To solve your top challenges with network visibility, protection, and response to threats, here are four must-have critical capabilities you need in your next firewall that are likely missing today:

TLS 1.3 inspection – 90% of internet traffic now encrypted and that number is growing, so it's absolutely critical that your next firewall include TLS 1.3 inspection. Perhaps more importantly, it must provide the intelligence and performance to do it efficiently, without becoming a bottleneck or forcing you to buy a much more expensive firewall than you really need. Not all encrypted traffic requires inspection, and not all encrypted traffic supports it. Your next firewall must support all the latest standards and cipher-suites. It must also have intelligent exceptions built in to be more selective in what traffic to inspect, while also providing tools to easily identify potential issues and add exceptions on the fly to avoid them. It should also offer adequate performance to deal with an ever increasing volume of encryption – both today and into the future.

Zero-day threat protection – Threats are constantly evolving. The ransomware variant used to attack an organization tomorrow will almost certainly be different from the one used yesterday. This is the nature of the current threat landscape. Your next firewall must have artificial intelligence based on multiple machine learning models, plus sandboxing with advanced exploit detection and crypto-guard ransomware detection to identify the latest zero-day threats and stop them before they get on your network.

FastPath application acceleration – About 80% of the traffic on your network likely comes from approximately 20% of your apps. These elephant flows are typical of meeting and collaboration tools, streaming media, and VoIP. These large traffic flows are both resource intensive to inspect and require optimal performance for a great user experience, creating an enormous challenge. Your next firewall should be able to adequately handle these trusted traffic flows and offload them to provide optimal performance and create added performance headroom for traffic that actually needs deeper packet inspection.

Integration with other cybersecurity products – It's no longer enough for IT security products to work in isolation. Today's sophisticated attacks require multiple layers of protection, all working in coordination and sharing information to provide a synchronized response. Your next firewall should integrate with other systems like your endpoint AV protection to share important threat intelligence and telemetry. This will allow both systems to work better together to coordinate a defense when you come under attack. These systems should also share a common management interface to make deployment, day-to-day management, as well as cross-product threat hunting and reporting easier.

These four capabilities will ensure the top problems with your current firewall will be a thing of the past, and power your network protection well into the future.

Critical capabilities	Questions to ask your vendor
TLS 1.3 inspection Provides visibility into the growing volume of encrypted traffic traversing networks	‣ 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?
Zero-day threat protection Protection from the latest unknown threats using machine learning and sandboxing	‣ 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?
FastPath application acceleration Offloading trusted application traffic to a FastPath to improve performance and reduce overhead	‣ Does your firewall support FastPath acceleration of trusted traffic and elephant flows? ‣ Is it done in software or hardware? ‣ How are applications identified for FastPath acceleration? ‣ What policy tools are provided to admins to control which applications are offloaded? ‣ Are any signatures provided out of the box to accelerate and FastPath some applications? ‣ Are your FastPath packet flow processors programmable, upgradable, and futureproof?
Integration with other security products Integration is essential to provide adequate layered protection and sharing of information across products for a response to threats or for forensic investigations and threat hunting	‣ Does your firewall integrate with an endpoint technology? ‣ What information is shared between the two products? ‣ Is a threat identified by one product shared with the other? ‣ What is the response when a threat is detected? Can it automatically isolate threats? How does it do this? ‣ Does the endpoint provide any information on users or application usage to the firewall? ‣ Can the firewall and endpoint be managed from the same console? Is it cloud-based? ‣ Can you do cross-product threat hunting (XDR)? ‣ Does the vendor offer a fully-managed network monitoring and threat response service? ‣ Does the firewall integrate with any other products such as WiFi, ZTNA, edge devices, or network switches?

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?
Web protection and URL filtering Provides protection from web-based malware, compromised websites, and web downloads	‣ Does your firewall support FastPath acceleration of trusted traffic and elephant flows? ‣ Is it done in software or hardware? ‣ How are applications identified for FastPath acceleration? ‣ What policy tools are provided to admins to control which applications are offloaded? ‣ Are any signatures provided out of the box to accelerate and FastPath some applications? ‣ Are your FastPath packet flow processors programmable, upgradable, and futureproof?
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?
VPN and SD-WAN Site-to-site and remote access VPN capabilities, SD-WAN overlays, and managing multiple WAN connections	‣ Does your firewall integrate with an endpoint technology? ‣ What information is shared between the two products? ‣ Is a threat identified by one product shared with the other? ‣ What is the response when a threat is detected? Can it automatically isolate threats? How does it do this? ‣ Does the endpoint provide any information on users or application usage to the firewall? ‣ Can the firewall and endpoint be managed from the same console? Is it cloud-based? ‣ Can you do cross-product threat hunting (XDR)? ‣ Does the vendor offer a fully-managed network monitoring and threat response service? ‣ Does the firewall integrate with any other products such as WiFi, ZTNA, edge devices, or network switches?

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?

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 will it 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

	Sophos	Cisco	Fortinet	PAN	SW	WG
Core Firewall Capabilities						
Firewall rule and web policy test simulator	✓		✓	✓		✓
FastPath packet optimization	✓		✓	✓		
Intrusion protection system	✓	✓	✓	✓	✓	✓
Application control	✓	Partial	✓	✓	✓	✓
Dual AV engines	✓					✓
Shadow IT cloud app visibility	✓		✓	✓	✓	✓ - OEM
Block Potentially Unwanted Applications (PUAs)	✓		✓	✓	✓	
Web protection and control	✓	✓	✓	✓	✓	✓
Web keyword monitoring and enforcement	✓		✓	✓	✓	✓
DPI engine: streaming, proxy or both?	✓	Flow	✓	Flow	Stream	Proxy
User and app risk visibility (User Threat Quotient)	✓		Limited			
Advanced threat protection	✓	✓	✓	✓	✓	✓
On-box logging and historical reporting	✓		Limited	Limited		

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

	Sophos	Cisco	Fortinet	PAN	SW	WG
Core VPN and SD-WAN						
Unlimited free full-featured remote access VPN	✓	Extra*	✓	Extra*	Extra*	Extra*
IPSEC and SSL site-to-site VPN	✓	✓	✓	✓	✓	✓
SD-RED Layer-2 site-to-site VPN	✓					
SD-WAN cloud multi-site VPN orchestration	Soon	✓	Extra*			
SD-WAN routing and link management	✓	✓	✓	✓	✓	✓

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

* These capabilities are available at extra cost

	Sophos	Cisco	Fortinet	PAN	SW	WG
Zero-Day Threat Protection						
Multiple ML model analysis of suspicious files	✓	✓	✓	✓	✓	
Dynamic sandboxing of suspicious files	✓	✓	✓	✓	✓	✓
Cloud-based file analysis	✓	✓	✓	✓	✓	✓
Extensive on-box threat analysis reporting	✓	✓			✓	
SD-WAN routing and link management	✓	✓	✓	✓	✓	✓

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

	Sophos	Cisco	Fortinet	PAN	SW	WG
Endpoint Protection Integration Features						
Identify compromised hosts	✓	✓	Extra*	✓	✓	✓
Auto isolate hosts at the firewall from other parts of the network	✓					✓
Auto isolate hosts at the EP level to prevent lateral movement	✓			Extra*		✓
Identify unknown network applications (Synchronized App Control)	✓			✓		
Enable cross-product threat hunding (XDR)	✓			✓		
Enable a fully managed threat response service	✓			✓		

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

* These capabilities are available at extra cost

	Sophos	Cisco	Fortinet	PAN	SW	WG
Cloud Management						
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*		✓	✓
Cloud firewall reporting	✓	✓	✓		✓	✓
Cloud managed cross-product threat hunting (XDR)	Extra*			Extra*		

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

* These capabilities are available at extra cost

Sophos Firewall

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

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

21-06-10 EN (DD)

SOPHOS