SOPHOS
Security made simple.

Firewall Buyers Guide

Looking to replace your network firewall? Whether you want to consolidate everything into a unified solution or add next-generation features, this guide is for you. It provides an overview of what to consider when selecting your next network firewall, including information on the features available and questions to ask your vendors. Use it to identify the right solution for your organization.

Firewall comparison check list

This table summarizes the main capabilities that you should consider when evaluating network security solutions. Use it to help you decide which solution fits your needs.

Read the full report for information on the factors that influence the usage experience, protection and performance of a solution, as well as a deep dive into specific protection features.

Feature	Sophos UTM	Fortinet FG 20-90	Dell SonicWALL TZ Series	WatchGuard XTM Series	The Sophos advantage
Network Firewall/ Protection	✔	✔	✔	✔	Automatically updated IPS, checkbox configuration
Advanced Threat Protection	✔	✔	✔	✔	All-in-one solution
Site to site and remote user VPN	✔	✔	✔	✔	Easy set up with Sophos RED
Secure web gateway	✔	✔	✔	✔	Easy policy builder
Spam protection	✔	✗*	✗*	✔	No separate appliance needed
Email encryption and DLP	✔	✗	✗	✗*	Automated encryption, no extra infrastructure needed
Endpoint protection	✔	✔	✔	✗	Sophos is Gartner Leader***
Dual anti-virus	✔	✗	✗	✗	Choose your scanner or use both
Mobile network access control	✔**	✗	✗	✗	Simple policy deployment
WiFi	✔	✔	✔	✔	Simple, elegant mesh networks
Reverse Proxy	✔	✔	✗	✗	Complete Reverse Proxy capabilities
Web application firewall	✔	✗*	✗*	✗	No separate appliance needed
User portal	✔	✔	✗	✗	Free up IT resources
Full reporting	✔	✗*	✗*	✗*	On-box, using built-in hard drive
Integrated 2 factor authentication	✔	✗	✗	✗	FREE and no additional infrastructure required
FREE Central management	✔	✗	✗	✗	FREE and no separate appliance needed
Best TMG feature parity	✔	✗	✗	✗	Independent experts recommend Sophos†
Deployment options					
Choice of Hardware, Software, Virtual or Cloud deployment	✔	✗	✗	✗	All features available for all deployment options
Active/Active Cluster with integrated load balancing	✔	Larger models	✔	Limited	Cluster up to 10 appliances for a fully scalable solution
Consistent feature set on all models	✔	✗	✗	✗	No need to buy a bigger appliance just to get key features
Ability to add license modules as and when required	✔	Larger models	✔	✔	Flexible licensing, no hardware upgrade necessary to support additional features
Additional requirements					

Refers to functionality included in a unified solution only

* Comparable functionality with separate appliance only

** Requires Sophos Mobile Control subscription

*** Sophos is a Leader in the Gartner Magic Quadrants for UTM, Endpoint Protection Platforms and Mobile Data Protection.

† www.sophos.com/tmg

Introduction

How to use this guide

This guide is intended to provide you with useful advice on what to consider when evaluating firewall solutions, including specific protection features to help you identify which capabilities your network firewall or UTM solution will need to deliver.

It also includes a comparison between selected Sophos, Dell SonicWALL, WatchGuard and Fortinet products.

Whether you're looking for an alternative to a network firewall to add enhanced functionality, want to reduce the number of network security products you currently manage, or are looking for more visibility and granular control over your web users, this guide is written for you.

Independent product performance tests

We recently commissioned an independent testing facility, Miercom Labs, to compare firewall products from Sophos with those of other vendors. They tested one of our SG Series appliances, the SG 210.

The competitor products were selected based upon their suitability for a typical 50-100 user organization:

- DELL SonicWALL NSA 2600
- Fortinet FortiGate 100D
- WatchGuard XTM 525

Please note that for all appliances sizing is an average guideline as factors such as type of user, infrastructure, etc. can influence the individual requirements. We would always recommend that customers contact their vendor or a qualified reseller to identify the right appliance model for their individual needs.

UTM vs Next-Gen Firewall

What constitutes a UTM and what is a next-generation firewall? Although many believe it's a case of semantics, there are differences.

In the majority of cases, a UTM consolidates security solutions into a single platform. Those security solutions can include network, web, email, endpoint, wireless management and more.

A next-generation firewall, on the other hand, will probably have fewer core features and require additional security solutions such as an email gateway or endpoint protection.

A next-generation firewall, or NGFW, has a strong focus on granular web controls and application-based security with core capabilities for application visibility and control, optimization of the use of Internet connections, clear, understandable Intrusion Prevention Systems (IPS), and seamless VPN to connect to remote sites and provide remote access.

Whatever you call it, it is more important to understand what you want to protect and evaluate solutions based upon your individual business requirements.

Part 1: Evaluating solutions

The five key areas to consider when choosing your next firewall are:

1. Ease of use
2. Performance
3. Security features
4. Reporting
5. Proven protection

1. Ease of use

A network firewall used to be something you configured once and then rarely touched again. In some organizations, the person with the knowledge to do that setup is long gone. That leaves many businesses with that 'thing' in the server room which nobody dare touch for fear of breaking something.

If you've been used to configuring your firewall using a command line interface, then a security gateway product with a decent GUI will probably be a treat for you in terms of usability. Network security has come a long way, and vendors have learned that products that are simpler to use can also be more effective. Advanced features are of little value if they are too complex to actually use.

The user interface of any solution will need well-defined workflows to avoid you having to repeat configuration steps for different modules of the product.

Also, with today's distributed workforces, the need to do any installation on the end user clients is no longer a feasible option for many organizations. For example, a firewall which offers full transparent mode without the need to configure proxies or set up NAT rules, can save any IT administrator a lot of time. A management interface accessible from any location and on any device ensures that ad-hoc or emergency administrative tasks do not mean a drive to the office.

By the same token, policy setup for users in the office should be equally applicable to those who are working remotely. Web filtering rules, for example, need to protect users outside the realms of the corporate network. And in order to support the different devices your users have, authentication should provide the best user experience.

Some things to consider:

- How quickly can you get to the information you need to troubleshoot user problems (blocked websites, etc.)?
- How easy is it to update the solution?
- How many steps are required to do the most common tasks, e.g. create web filtering policies?
- Can you tailor the dashboard view to suit your needs?

2. Performance

Whether you're looking for a unified solution for a small business, or enterprise-grade next-generation firewall features, one of the first points of comparison you will make is generally performance.

Vendors offer sizing guidelines, but it is always advisable to consider your individual infrastructure. Look at how your users work, their individual usage patterns, which applications and servers you need to protect, and which features of your firewall you will have switched on.

Beware of blindly trusting any kind of online sizing tool: one vendor may say you need 1 Mbps firewall throughput per user, the next may say anything up to 20 Mbps, and so on. Even some of the most network-savvy experts have made mistakes by undersizing an appliance – eventually leading to performance problems – or oversizing the appliance and pricing the solution way outside of the available budget.

Performance is also influenced by the architecture used in any hardware appliance and how the software and the hardware work together. Whereas an appliance with ASICs chips can produce good throughput results for a specific purpose, it places limits on upgradability and often requires the appliance to be connected in a particular way. Also, performance numbers for ASICs hardware differ greatly from virtual installations from the same vendor.

Third-party tests, such as the ones that follow from Miercom Labs, generally offer a more accurate picture of the actual throughput you will see in a productive environment. Here it is important to check the test methodology.

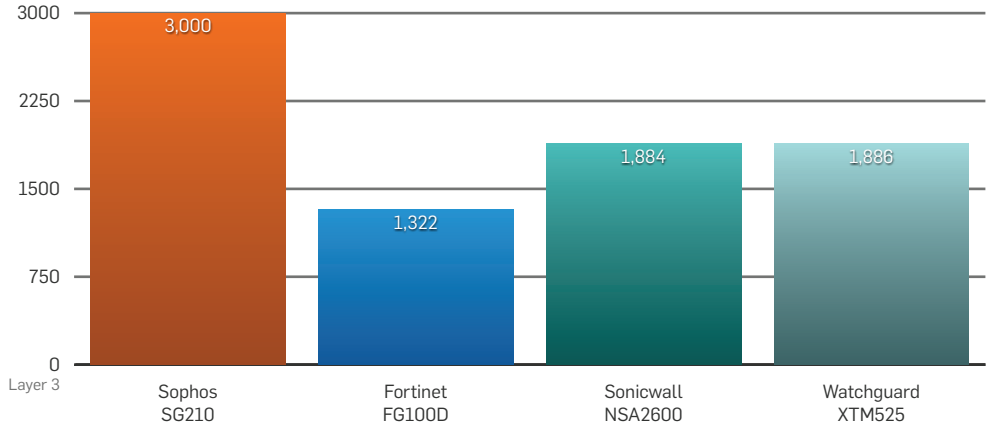
Test results can be influenced greatly by:

- The architecture used in the hardware e.g., ASICs vs. standard multi-core processors such as Intel
- The number of ports on an appliance – line speed will be shown in round numbers
- Type of traffic measured – bi-directional or uni-directional
- How comparable the tests are, e.g., proxy-based antivirus (slower but more secure) vs. flow-based (faster but less effective)

Miercom test: Firewall Throughput

The firewall is the most fundamental function of your UTM. Any slowdown here impacts all traffic passing through the device. Therefore firewall throughput should ideally allow line rate for your connections. This test was conducted with three 1Gbps ports giving a theoretical maximum of 3Gbps/3,000Mbps.

Unidirectional Firewall Throughput (Mbps)



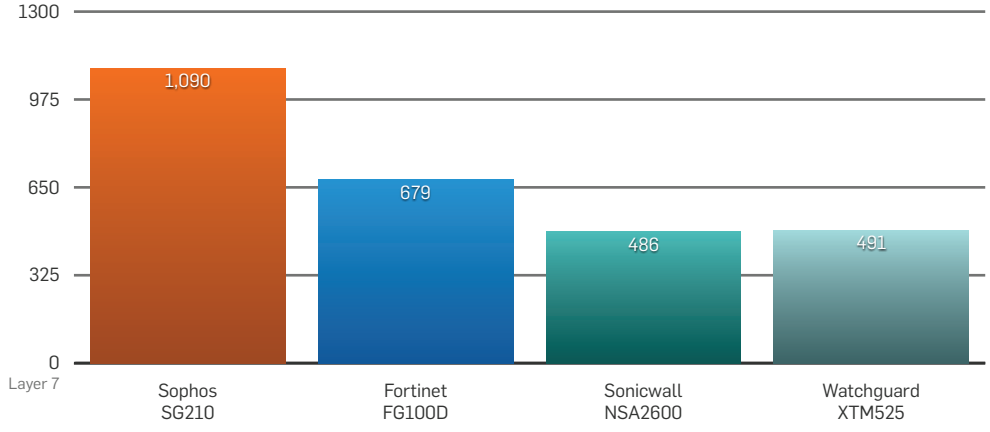
Source: Miercom, June 2014

As the first firewall throughput test did not stretch the Sophos SG210 to its limits, it was re-tested using more ports and sending traffic in both directions at the same time. The Sophos SG210 reached maximum throughput of 10,441 Mbps.

Miercom test: Application Control Throughput

Application Control allows you to effectively monitor and manage different types of traffic going through your gateway such as VPN, YouTube or Facebook without having to block traffic completely. This test looks at Layer 7 (Application layer) throughput.

Application Control Throughput (Mbps)

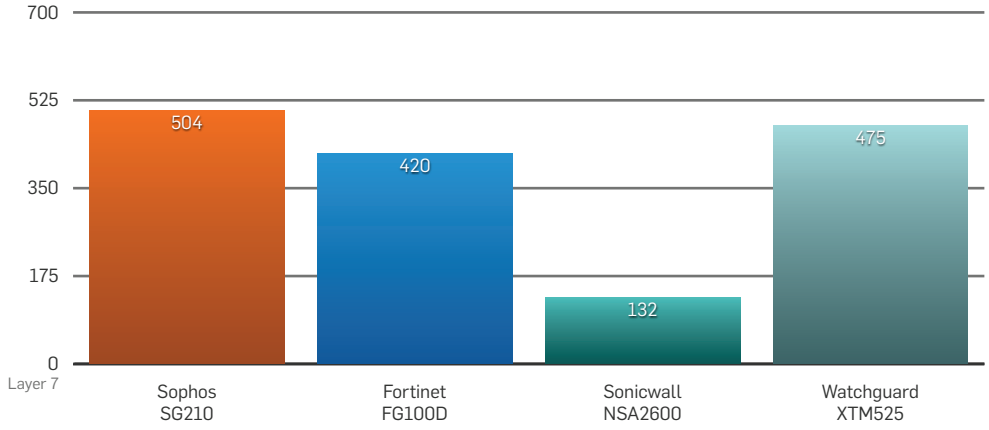


Source: Miercom, June 2014

Miercom test: IPS Throughput

Intrusion Prevention Systems monitor the network for suspicious traffic and can block exploits of known vulnerabilities. Similar to application control, this is a resource intensive process where packets are assembled and inspected.

Firewall + IPS Throughput (Mbps)



Source: Miercom, June 2014

For more information on the Miercom independent testing report visit www.sophos.com/miercom

Deployment options

Some vendors offer value in the form of deployment flexibility – hardware, software, virtual environment (such as VMware, Hyper-V and Citrix Xen), or cloud-based.

Should you choose a software and virtual installation, it is important to note if it will run on any dedicated Intel X86-compatible hardware or if it requires purpose-built hardware components. Obviously, you have greater flexibility with standard hardware which can be easily upgraded.

Also depending on the architecture a vendor uses, you may see substantial differences in performance between the firewall appliance a vendor offers and a virtual installation from the same vendor on standard hardware.

Alternatively, you may choose to deploy your network security solution in the cloud. This can often be done by using Amazon Web Services, or a data center of your choice.

Not all vendors offer all deployment options as the table below shows. Select the deployment scenario which best suits your requirements and offers you the flexibility to grow.

Deployment	Sophos UTM	Fortinet FG 20-70	Dell SonicWALL TZ Series	WatchGuard XTM Series
Hardware	✔	✔	✔	✔
Software	✔	✗	✗	✗
Virtual	✔	✔	✗	✔
Cloud	✔	✔	✗	✗

3. Security features

If your goal is to consolidate your existing infrastructure into a single solution, you likely want the same security features you're accustomed to having. Should you be considering a UTM solution for email protection, for example, don't forfeit features such as anti-spam, email encryption and DLP.

If a vendor on your shortlist doesn't offer comparable features to your email gateway, then perhaps they shouldn't be on that list.

The same goes for web protection. A unified solution should offer equivalent features to a web security gateway. Even if you don't use every feature your chosen network security product offers, you have the functionality you need to support and enable your business.

If you're trying to replace a retired product such as Microsoft Forefront Threat Management Gateway (TMG), you can find a UTM with superior features to your End-of-Life solution. If your TMG replacement can offer you network, web and email protection features as well, that will save you money and administrative effort.

The comparison check list on page 2 lists features and functionalities you may look for in a network security gateway. This comparison shows which vendors offer functionalities as part of a unified solution (UTM).

Although most vendors can offer almost all of the features, in many cases they can only do so with multiple appliances or security solutions. Also many vendors do not offer the full breadth of features on all appliances.

So if you are a small business looking to secure a limited number of users, look to purchase a solution that isn't over-dimensioned for your purposes just to get the features you need.

For a detailed look at individual protection capabilities please see **part 2** of this guide.

4. Reporting

Reports give you visibility into what's happening with your network, so you can make informed decisions to support your business.

If a large amount of bandwidth is being used by a particular application, it could slow down other operations. In addition, reporting gives visibility into infections on your system.

It's important to have real-time data to make ad-hoc decisions and ensure you are providing the quality of service your users need. Reporting on web usage in real-time lets you adapt your solution dynamically, removing bottlenecks caused by particular usage patterns; or free up more resources for certain departments when peaks can be expected.

Solutions which only offer reports in set intervals aren't adequate for some organizations. For example, many school districts require data immediately and cannot wait until the next report is available.

You may also want to access historical data to make more informed decisions about the optimal setup or to analyze particular incidents. Having some kind of storage on-box lets you access that data.

Any reporting module needs to be adaptable to your needs and give you the data you want – and not store what you don't want.

Consolidated reports spanning multiple features can be beneficial in some areas. Not all attacks are necessarily just from one designated source and having a single view, e.g., for command and control, can allow you to quickly remediate a problem.

If you are worried about the effect reporting can have on performance, consider a solution with an integrated solid-state drive rather than a rotating hard drive. Having no moving parts not only makes them robust but also fast and with minimum impact on your solution performance, even for complex reporting.

Feature	Sophos UTM	Fortinet FG 20-90	Dell SonicWALL TZ Series	WatchGuard XTM Series
Reporting – included as standard	1000s	Few	Few	Few
On-box storage for local quarantine, log files and reports	Complete	Limited	Limited	Limited

5. Proven protection

When choosing a firewall, you also need to look at the quality of protection; third-party endorsements can give you a good idea of which vendors have the best protection from various threats.

For many organizations, the Gartner Magic Quadrant is the benchmark in selecting which vendors to consider.

But with many network firewalls now providing complete security, the technology as a whole needs to be considered and if the vendor has the experience in which you can place your full confidence.

Part 2: Evaluating security capabilities

We will now look in depth as the different security features available. Use this to identify the capabilities that are important to you and what questions you should ask your vendors.

Network protection

This section looks in-depth at the different security features available. Use this to identify the capabilities that are important to you and the questions you should ask your vendors.

Your network security product should provide a solid security foundation even before you add network protection subscriptions or licenses. At a basic level it should include static routing, DNS proxy services, DHCP server options, NTP functionality, stateful firewall, network address translation, basic remote access VPN, local user authentication, local logging and daily reports, and basic management functionality.

Capability to look for	Description	Questions to ask your vendor
IPS	Bolsters your firewall's security policy by inspecting approved traffic for malicious packets. Can drop packets that match a signature list of threat patterns.	‣ What kind of expertise is needed to properly use the system? ‣ How are rules delivered and configured? ‣ Is IPS easy to tailor to your individual network infrastructure?
Advanced Threat Protection / Command-and-Control / Botnet Detection	Checks outbound traffic to detect and block attempts to communicate with malicious hosts such as command-and-control and Botnet servers	‣ What expertise is needed to use the system? ‣ Does it include the detection of threats via the Web? ‣ Does it offer consolidated reporting for all sources?
Bandwidth control/Quality of service	Prioritizes traffic based on the rules you set and allows you to control how a fixed resource is used during different conditions.	‣ How many WAN connections can you support on a single appliance? ‣ How easy is it to identify and control the bandwidth applications use?
Site-to-site VPN options	Links remote sites with the main office, allowing users to send and receive information via a secure connection. Also allows employees to use devices such as file servers and printers that are not in the same office.	‣ What protocols does your VPN support? ‣ How much experience or VPN knowledge is required to set up a VPN?
Remote access options	Allows users to securely connect to the network security appliance from any location.	‣ Do you offer multiple remote access options including clientless VPN? ‣ Is remote access supported from any OS and/or device? ‣ Is the clientless VPN truly clientless or are applets required on end-user devices? ‣ Are additional licenses required?
Remote office support	Connects remote office networks to the network security appliance to protect them with the same policies and capabilities.	‣ How easy is it to connect remote offices? ‣ Technician required? ‣ Can remote offices be centrally managed? ‣ Are additional subscriptions or licenses needed?
Detailed reports	Provides detailed real-time and historical statistics and reports on network/bandwidth usage, network security, etc.	‣ Does it contain a built-in hard drive? ‣ What kind of reports are available without a separate application?

Web protection

You need web protection that allows you to apply terms and conditions to where and how users spend their time online, and stops spyware and viruses before they can enter the network. Detailed reports should show you how effective your policy is so you can make adjustments.

Capability to look for	Description	Questions to ask your vendor
URL filtering	Controls employee web usage to prevent casual surfing and to keep inappropriate content and malware off the network.	› Are live updates available? › How many web surfing profiles can be created and used? › Can it just block or also warn about potentially inappropriate websites?
Spyware protection	Prevents malicious software from installing on employees' computers, consuming bandwidth and sending sensitive data out of the network.	› Are live updates available?
Antivirus scanning	Scans content before it enters the network to prevent viruses, worms and other malware from infecting computers on the network.	› Are live updates available?
HTTPS scanning	Provides visibility into encrypted web traffic to protect the network against threats that can be transmitted via HTTPS.	› Can HTTPS traffic be inspected and checked against policies?
Application control	Provides visibility into how employees are using the web and controls which applications they can use and how.	› Are live updates available?
Interactive web reporting	Provides flexible reporting capabilities to allow administrators to build their own reports.	› Are real-time and historical usage reports available? › Can reports be scheduled for delivery? › Is a third-party reporting application required?

Next-generation firewall protection

NGFW is an evolution of the traditional port-based protections used in most network security approaches. Rather than simply allowing traffic through on ports like HTTP or HTTPS, NGFWs have application signatures that can identify traffic on a much more granular level. For example, administrators can choose to block Facebook Messaging while still allowing access to Facebook.

NGFWs also do deep packet inspection at a high speed, identifying and blocking exploits, malware and other threats with high levels of precision. Because many attacks are now web-based, traditional firewalls filtering only by port are of limited effectiveness in defending you against these threats.

A NGFW also allows organizations to be more strategic by prioritizing their network usage with powerful shaping rules. For example, you can choose to allow VOIP phone calls or prioritize Salesforce.com traffic while the throughput or blocking outright applications like Bittorrent.

Capability to look for	Description	Questions to ask your vendor
Application visibility and control	Having visibility of the applications being used enables you 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.	› Can you prioritize and control access to applications and see in real-time how your Internet connection is being used, and by whom? › How easy is it to set a policy from a live view of your current activity?
Optimizing the use of the internet connection(s)	Bandwidth is a limited commodity and you need to make sure that you make best use of it, like ensuring business-critical applications like salesforce.com have priority.	› How easy is it to shape bandwidth? › Do you have a Quality-of-Service (QoS) toolkit?
Clear, understandable IPS	Many web-based attacks are now able to masquerade as legitimate traffic. Effective IPS enables you to see what web traffic actually does, rather than just what it is.	› How easy it is to manage IPS? › What level of expertise is required – for example, do you need to understand different types of threats?
Seamless VPN for remote connections	Remote and mobile working are becoming increasingly common. Organizations need quick, easy and secure VPN so users can connect to the network and be productive from any location.	› How easy is it to set up client VPNs for your remote workers? › Which devices can you use to connect to the network? › Do you offer a clientless HTML5 solution?

Email protection

Protecting email against spam and viruses isn't a new problem. But, email security threats continually evolve, making email protection a full-time job that never ends. You need email protection so that common email problems like spam, viruses and the leaking of confidential information don't affect your business.

Capability to look for	Description	Questions to ask your vendor
Anti-spam	Stops spam 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?
Antivirus scanning	Scans and blocks malicious content at the gateway to stop viruses and other malware from infecting computers.	› How many antivirus engines does your solution use? › How often does your solution scan content?
Email encryption	Renders email illegible to prevent eavesdroppers and other unintended recipients from obtaining sensitive and confidential information.	› What does a user have to do to encrypt and decrypt email? › How is encryption managed? › What infrastructure is required for key management?
Data Loss Prevention (DLP)	Prevents sensitive data from being intentionally or unintentionally sent by email	› How is it triggered, automatically or manually? › Does it integrate with the email encryption? › Which data types can be detected?
User portal	Gives employees control over their email, including spam quarantine and message activity.	› Can end users handle their own email quarantine?

Webserver protection

Webserver protection stops hackers from using attacks like SQL injection and cross-site scripting from stealing sensitive information like credit card data and personal health information. And it should help you achieve regulatory compliance when a web application firewall is required.

A web application firewall scans activity and identifies attempts to exploit web applications, preventing network probes and attacks.

Capability to look for	Description	Questions to ask your vendor
Form hardening	Inspects and validates the information submitted by visitors via forms on your websites. Prevents invalid data from damaging or exploiting your server as it is processed.	› Is a complete form analysis performed? › Can the system detect tampered forms?
Reverse proxy authentication	Provides exploit-free authentication for users by integrating with your backend DMZ services like Exchange. Often requested when looking for an alternative to Microsoft TMG.	› What systems will it integrate with seamlessly? › What forms of authentication are supported?
Antivirus scanning	Scans and blocks malicious content at the gateway to stop viruses and other malware from infecting computers.	› How many antivirus engines does your solution use? › How often does your solution scan content?
URL hardening	Prevents your website visitors from accessing content they aren't allowed to see.	› Do I have to enter the structure of my website manually, or can it be done automatically with dynamic updates?
Cookie protection	Protects from tampering the cookies given to your website visitors.	› Does the system protect my ecommerce site against manipulation of product prices?

Wireless protection

Wireless networks require the same security policies and protection as the main corporate network. Unfortunately, they are often operated by network administrators as two separate networks. Wireless protection from your network security vendor should reduce if not eliminate the problem of enforcing consistent security policies across your organization. Make sure your wireless protection extends your network security security features to your wireless networks. And it should provide a way for you to centrally manage the wireless network.

Capability to look for	Description	Questions to ask your vendor
Plug-and-play deployment	Provides fast and simple set-up because access points are configuration-less.	• How long does it take to set up and deploy access points and policies?
Central management	Simplifies management of the wireless network by centralizing configuration, logging and troubleshooting within a single console.	• Do I have to configure the access points one-by-one in the local GUI or command line?
Integrated security	Offers instant protection to all wireless clients through complete UTM security.	• Can all wireless traffic be forwarded directly to the security gateway?
WPA/WPA 2 encryption options	Enterprise-level encryption that prevents data loss and theft by rendering data illegible to unauthorized recipients.	• Are multiple encryption and authentication methods supported? • Is an interface to my RADIUS server available?

Guest Internet access	Protects multiple wireless zones, each with different authentication and privacy settings. Enables and supports wireless hot spots.	• How many different wireless network zones are supported?
		• What type of hot spots are supported?
		  ◦ terms-of-use acceptance
		  ◦ password of the day
		  ◦ voucher-based

Detailed reporting	Provides information about connected wireless clients and network usage.	• Is there built-in reporting? • Is a separate tool required for reports?

Endpoint protection

To maintain a secure network, you need endpoint protection that checks connecting devices for current updates and security policies. Your endpoint protection also needs to protect company-owned devices on and off the network. Reduce your management effort and save money by integrating your endpoints directly into your network security appliance. This also helps to achieve regulatory compliance when different antivirus engines are running at the gateway and on the endpoint.

Capability to look for	Description	Questions to ask your vendor
Ease of deployment	Gives the organization the ability to easily deploy and manage endpoint clients to prevent malware and data loss.	• How is the endpoint client deployed? • Is it possible to integrate an existing Endpoint solution?
Antivirus scanning	Scans the endpoint for viruses and other malware to prevent it from entering the network.	• How many different antivirus engines are used? • Does the solution provide live updates via the cloud?
Device control	Allows the organization to prevent the use of modems, Bluetooth, USB ports, CD/DVD drives, etc.	• What devices can be controlled through your solution? • Does endpoint protection only work if endpoints are in the domain or connected through a VPN tunnel?
Real-time reporting	Provides visibility into endpoints with up-to-date statistics.	• Is real-time reporting built in?
Support for remote workers	Provide the same protection for workers whether on or off the corporate network	• How are endpoints protected when they are off the corporate network?

Conclusion

Buying your next firewall is a big decision. You will probably keep it for three years or more, so it has to meet your needs both now and in the future. This Firewall Buyers Guide helps you identify what is important to you and your business and then evaluate solutions based on third party tests.

About Sophos

Sophos began producing antivirus and encryption products nearly 30 years ago. Today our products help secure the networks used by 100 million people in 150 countries and 100,000 businesses, including enterprises such as Pixar, Xerox, Ford, Avis, and Toshiba but also many small and medium businesses around the globe.

Our products allow you to secure every endpoint of your network, from laptops to virtual desktops and servers, to web and email traffic and mobile devices. At Sophos we know that the solution to complexity is not more complexity. That's why we focus on making things simple without compromising on functionality, performance or protection - simple security is better security.

Try it now for free

Get a free 30-day evaluation
at sophos.com/firewall

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

Oxford, UK | Boston, USA

1192.07.13DD.bgna.simple

SOPHOS