WHITE PAPER

How To Pick the Right Small Business Firewall

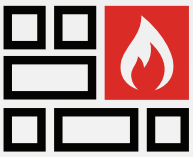
Executive Summary

While it's impossible to know for sure how growth and expansion will affect your networking and security requirements over time, it's still possible to make a wise investment for the future. The right firewall will help you prepare your business for growth by consolidating your product portfolio, increasing operational efficiency, reducing costs, and making the overall management of your network infrastructure more effortless and cost-efficient.

Taking systems offline while infrastructure is retooled is an expense few businesses competing in today's digital marketplace can afford. Your firewall selection, and the vendor behind it, should not only set up your business with the tools you need to be successful in the short term but provide the capabilities and performance needed to prevent complexity and a costly and laborious shift down the line.

Whether you're new to network administration and security or an experienced professional with an opportunity to refresh and architect smarter, this white paper will help explain where complexity and failure occur, why they happen, and help lead you down a path of simplicity and scalability without sacrificing the critical functionality on which your business depends.

76% of U.S. SMBs and 66% of SMBs globally reported a cyberattack in 2018.[1]



Throughput

A measure of how much traffic a firewall can handle when security and other functionality are activated. This differs from bandwidth, which measures the baseline amount of traffic that can pass through without impacting performance. Few security vendors provide throughput numbers with full security functions enabled.

Identifying Key Capabilities

Firewalls 101

The firewall serves as the critical inspection point for all network traffic for many network designs, making it the cornerstone of a business's security architecture. But not all firewalls are up to the challenge of delivering the deep inspection and performance today's networks and applications require. As the volume and maturity of users, devices, and applications increase and more applications run from the cloud rather than from the office, bandwidth demands intensify. A firewall's ability to process and secure network traffic is known as "throughput," and how many users and applications it can analyze simultaneously is known as "concurrent sessions." The higher the performance, the higher the throughput and number of concurrent sessions that can be analyzed and routed simultaneously.

Even though most SMBs expect their technology to last two to four years, in reality, 51% introduce new tools and workarounds every one to two years.[2] Fully understanding what your firewall and the vendor delivering it can—and can't—do is essential to getting the investment out of the technology you're expecting.

Effectively analyzing network traffic for threats centers around the basic security concept of comparison. Network traffic must be compared against known malicious (bad) traffic and behaviors, with artificial intelligence based on billions of samples to accurately assess unknown traffic. How much, how fast, and how accurate this comparison is before a device and network are brought to a standstill comes down to performance. And that is determined by the device's central processing unit (CPU) and its alignment with its underlying operating system.

As a result, understanding how a vendor has developed and engineered their firewall can be very telling, especially regarding performance capabilities and limitations.

Why Are Firewalls So Expensive?

Given the increasingly sophisticated technologies and tactics used by today's cyber criminals, effectively analyzing traffic for threats requires a much more specialized and intensive process. And it will only continue to grow in intensity over time, so evaluating a firewall requires understanding your needs today as well as those in the future.

Most small and midsize business (SMB) firewall vendors rely on generic CPUs working serially, one process after another, to perform analysis. Serial analysis sufficed when firewalls began, and threats were relatively straightforward (versus today's modern threats). But as technology has advanced and network traffic and threats have become more complex, devices built using this approach quickly become overwhelmed.

To fix this, some vendors selling into SMB began developing firewalls capable of parallel path processing, splitting the load across multiple specialized (albeit still largely generic) CPUs. While this increased processing power and performance, these high-end CPUs were, and continue to be, in incredibly high demand because they power many of today's advanced technology systems. And with that demand comes low availability and a hefty price tag—the higher the performance needed of a chip, the higher its price, forcing smaller companies to decide between performance or security at a time when attackers are turning more downmarket than ever before.

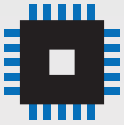
In addition to the high price demanded of these generic chips, they were also designed for the masses, which means that they were never developed to perform the sort of specialized inspection, analysis, correlation, and response tasks modern firewalls need to deliver. To deliver the services modern users demand, many of the world's leading technology companies realized they could never truly optimize their proprietary innovations using these generic chips, let alone deliver a price point people could afford. That's why leading innovators like Apple, Google, Microsoft, and Tesla, among others, began to develop custom processors designed to perfectly marry with and optimize their proprietary operating systems and perform specific tasks to achieve new speeds and availability at a more affordable price.

The need for advanced processing power for security is no different than for video processing, smartphones, cloud servers, or smart cars. But taking on the cost, risk, and burden of proprietary chip design is no simple task. Because of that, very few security vendors (let alone ones supporting SMB) have opted to take on the burden of designing their own chips.

But for those that have made that investment, taking a security-first approach has paid off. Specialized security processing units (SPUs) designed to optimize their underlying code not only run at exponentially higher speeds but a significantly reduced price compared to generic chips. This approach reduces the burden of implementing advanced security in the near term while future-proofing those investments long into the future. This is especially critical now as businesses of all sizes need to inspect encrypted data and other performance-intensive data transfers, like streaming video, that are becoming commonplace—something very few security solutions can do.

Multivendor vs. Single Vendor?

By definition, a multivendor, best-of-breed strategy is more complex, especially when systems need to be managed and configured using separate consoles. It's not necessarily the wrong approach. But deploying, managing, and correlating data across multiple devices—many of which were never designed to interoperate—does require more resources to implement and maintain that need to be considered, especially if one of your goals is to avoid complexity in the short and long term.



Security Processing Units (SPUs)

Specialized security chipsets designed to optimize their underlying code not only run at exponentially higher speeds but a significantly reduced price compared to generic chips. This reduces the burden of implementing advanced security now and while future-proofing those investments long into the future.

Security-first vs. Networking-first Approach

Networking-first vendors attempt to layer security onto basic networking routers not designed for intense security. On the other hand, a security-first approach means a vendor has designed their firewall from the ground up to handle the intense security analysis and basic routing required of the device. While both systems can perform networking and security functions, networking-first solutions struggle to perform when security functions are enabled, such as inspecting encrypted traffic.

Is Being Proactive and Improving the Business Worth the Risk of Change?

To penetrate a business's defenses, hackers are constantly on the lookout for security gaps, vulnerabilities, and other areas of weakness to exploit. Such gaps are most commonly due to misconfigurations and a lack of interoperability and deep integration between security products. Operationally, a system with multiple vendors requires more time to manage and cross-reference disparate systems, aggregate and normalize reports, and ensure that any gaps—especially surrounding privacy and compliance mandates—are closed.

Discovering threats is also harder when systems aren't natively integrated. When disparate products determine and treat threats differently, you need someone or something to normalize it all. That means that your team must make manual assessments after researching alerts and digging through disconnected logs. And in all that noise, issues that should be addressed can be easy to miss. This complex process is why the average time to detect a threat is 228 days and a further 80 days to contain a breach.[4] It's also why companies operate in a constant reactive state rather than being proactive because, by the time a threat has been discovered, the damage has already been done.

What's needed is a security framework where every component was designed to work together as an integrated fabric from the beginning. Sharing threat intelligence and indicators of compromise to detect and automatically respond to a threat quickly and accurately to deliver the goal you initially set out to achieve. Even when every piece of the fabric may not be the leading product in their category, the ability to have true deep integration and automation across your business is more than enough to make up for it.

When operating with limited budgets and small teams, choosing a firewall as part of a natively integrated security fabric with a common operating system capable of automatically managing multiple pieces of the equation gives growing businesses a distinct advantage in security and operational efficiency. Centralization reduces deployment time, enables broad automation for instant threat remediation, and significantly reduces the potential for human error—the leading cause of successful attacks.

The same logic applies to visibility, logs, and reporting. When systems speak the same language, operations and management are dramatically simplified while strengthening security.

Over 30% of each day is lost managing workarounds and fixes when deploying a multivendor approach.[3]

Over 60% of enterprises admit they wished they had focused on a single vendor rather than multivendor approach.[3]

Even when products are purchased from the same vendor, you must stay vigilant. The "growth through acquisition" strategy of many network and security vendors can leave customers holding a bag of poorly integrated products that don't work together and broken promises of future integration. This could leave you building the deep integration and automation you need using custom workarounds that will need to be continually maintained.

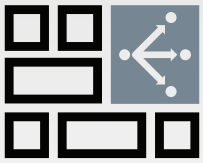
What Should a Firewall Do?

By consolidating visibility and control of disparate solutions directly into a single firewall platform, businesses eliminate the need to run multiple point solutions. This improves operational efficiency, visibility, and control across the network by removing the need to duplicate efforts multiple times. Security services—such as advanced threat protection, intrusion prevention, content filtering, and Domain Name System (DNS)—as well as advanced networking capabilities—like SD-WAN and zero trust—can all be converged into a single offering and then pushed down through the connecting pieces of the fabric.

Decrypting Network Traffic

To inspect traffic, a firewall must be able to read it. Which means it must be decrypted. Current assessments peg the level of encrypted network traffic in the realm of 90%, including most application traffic. This makes a firewall's ability to decrypt traffic in real-time critical. The recent rise in virtual private network (VPN) traffic to support hybrid work environments has further increased this need.

Again, the firewall's ability to inspect such traffic without creating a bottleneck depends entirely on performance, and buyers should pay attention to how much throughput a firewall can handle with encryption enabled. Without rapid decryption, your firewall cannot analyze incoming traffic, which means data ends up being sent straight through to the end-user and onto the network rather than slow down mission-critical applications and workflows—risk and all.



Few modern firewalls can perform a full inspection of encrypted traffic without severely undermining their its. However, "the percentage of encrypted web traffic on the internet has steadily increased, from around 50% in 2014 to around 95% today."[5]

Antivirus (AV), Advanced Threat Protection, Intrusion Prevention

In addition to the more sophisticated threats businesses face, today's cyber criminals often use older attacks in the hope that the firewall doesn't have the memory to still include them in its inspection database. To combat this, firewalls need to combine threat-matching signatures with machine-learning capabilities—commonly called "advanced threat protection"—to identify all threats, new or old, to successfully fight today's attackers. But while many vendors may market their security as advanced malware protection, it is not uncommon for basic protections, such as AV, to be mislabeled as "advanced." To truly understand the solutions embedded in a modern firewall, one should look to third-party reports and testing services to determine the true efficacy of their protection.

And the battle keeps escalating. Over time, mature malware and attacks "as-a-service" have begun to increase on the dark web, making advanced threats even more challenging to hunt down. They increasingly require deep packet inspection (DPI) to identify malicious markers and indicators. Advanced intrusion prevention/detection services (IPS/IDS) should be part of the threat prevention services your firewall utilizes.

But once again, a firewall's ability to perform DPI effectively—especially without slowing down the firewall—rests predominately on its level of performance. Firewalls lacking advanced processors often leave off this critical capability when making throughput claims. Or they assert things like only companies being targeted by state-sponsored attackers need it—a dangerous fallacy. An attacker's ability to hide an attack that requires DPI is table stakes today. And while purchasing a separate IPS system isn't unheard of, the use case is often only seen in the largest companies due to the staggering amount of data they must analyze. At the SMB level, this simply isn't the case.

Content Filtering

The most effective way to prevent users from being infected by malicious websites (such as drive-by downloads) is to prevent them from going there in the first place. Content filtering performs a check on URLs based on URL categories, such as pornography, gambling, malicious content, and file sharing, while building exemptions for approved traffic. But in today's world of hybrid workforces that don't have an integrated endpoint and network solution, such enforcements performed by the firewall often fall away when a user is offline, or they require the manual updating of the endpoint to match changes on the network side. An integrated solution, however, that ensures endpoint and network security are in constant communication without manual intervention fixes this.

Endpoint Hygiene

Integrated endpoint and network security have additional advantages beyond keeping agents updated. Traditionally, understanding what is running on an endpoint, identifying vulnerabilities, and implementing patching had to be run from an endpoint product's management console. However, when firewall and endpoint solutions are built using the same operating system, this visibility can be obtained directly from the firewall. This enables network access control to be enforced based on endpoint risk and hygiene assessments, forcing the end-user to update and patch their system appropriately before being allowed on the network. This significantly reduces network risk from employees who have been offline working remotely for long periods.

Domain Name System (DNS)

While URLs are designed to be interpreted by humans to ease internet navigation, the underlying code used to navigate to sites can be hijacked to obscure and hide malicious intent while still offering the same superficial URL—a process known as Domain Name System (DNS) hijacking. Ensuring you work with a vendor that provides DNS security as part of their threat subscriptions provides an additional layer of web security against a rising threat.

Sandboxing

When new files are introduced to the network, AV usually checks them against a database of known attacks to block their entry. But this approach is ineffective against unknown threats. In that case, a "sandbox" is used to open and "detonate" files and attachments unknown to AV inspection to determine if they are malicious.

Once again, depth of integration and inherent performance will determine how fast this process can occur. Here, single-vendor solutions have another advantage. Each element of the security fabric operates using the same underlying code and leverages the same specialized security processors, including the sandbox. As a result, risks can be quickly determined, and threat intelligence automatically shared across the security fabric in near real-time without manual intervention. Additionally, thanks to deep integration and automation capabilities, automated playbooks and threat responses can immediately kick in, including quarantine, alerting, and remediation—precisely what you want out of an intelligent, proactive cybersecurity system.

When new files are introduced to the network, AV usually checks them against a database of known attacks to block their entry. But this approach is ineffective against unknown threats. In that case, a "sandbox" is used to open and "detonate" files and attachments unknown to AV inspection to determine if they are malicious.

IoT Visibility and Control

The Internet of Things (IoT) ranges from smart appliances in the home to sophisticated operational technology (OT) sensors and monitors on manufacturing floors, in inventory rooms, and in hospital ICUs. The challenge for most administrators is the lack of standardization across these devices, making it extremely difficult to accurately discover all the devices on the network and appropriately control them.

Hackers have been quick to exploit the lack of security surrounding IoT and use their vulnerabilities to gain a foot in the door of many networks. While some vendors sell a separate solution to address the IoT challenge, some innovative security vendors have begun integrating the ability to track IoT devices and identify those compromised into the underlying operating system of the firewall. Some even offer this free of charge, helping businesses future-proof their business without added complexity or cost.

Network Control of Switching and Wireless Access

Unfortunately, no platform is 100% secure, especially in the face of ongoing digital innovation. Network segmentation prevents ransomware and similar threats from moving freely across your network, enabling the firewall to inspect and control traffic moving across the network (east-west) at critical checkpoints.

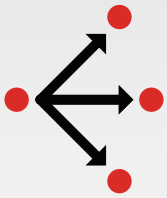
This is the starting point for building a "zero trust" network framework—the leading cybersecurity approach of successful enterprises. Teams can further increase their flexibility and limit their attack surface by only allowing specific people or departments access to applications or application abilities, known as granular application control. This prevents threats from using less inspected or newly deployed application protocols to avoid detection. They can also control access to applications on a per-user or per-session basis, a technique known as zero trust network access (ZTNA).

However, all this additional inspection adds extra load, making the firewall's application control services' performance, depth, and flexibility even more critical. And when the various devices in the ecosystem (firewall, switch, wireless access point) aren't from the same vendor, managing these policies is also much more complex. This is also why a single vendor capable of pushing and maintaining these policies from a centralized source streamlines operations and strengthens security.

Secure SD-WAN

SD-WAN is deployed by businesses looking to replace fixed multiprotocol label switching (MPLS) connections, optimize user experience for cloud applications, reduce onboarding time for new locations, and better use local internet access. The challenge is that few standalone SD-WAN solutions include security. Fortunately, an SD-WAN device optimizes traffic using much of the same routing information the firewall uses, which has led some innovative vendors to consolidate the two devices.

However, even when conjoined, SD-WAN capabilities can vary significantly between firewalls. Some include advanced routing functionality and innovations like self-healing networks, while others only provide the bare minimum to claim they offer SD-WAN. But as business plans increasingly include significant shifts to the cloud, paying close attention to a firewall's SD-WAN capabilities, along with the vendor's pace of innovation, is an excellent way to enable growth and avoid unnecessary investments down the road.



As business plans increasingly include significant shifts to the cloud, paying close attention to a firewall's SD-WAN capabilities, along with the vendor's pace of innovation, is an excellent way to enable growth and avoid unnecessary investments down the road.

Avoiding Complexity as You Grow

Dealing with growth is an exciting and stressful time for companies of any size. Apparent demand for your products and services proves that your go-to-market strategy was successful, and there was a need for your solutions. But maintaining that growth while avoiding complexity down the road can be a massive challenge. More users mean more connected devices, new locations must be onboarded, and new technologies to support business and customer demands must be implemented. While some IT projects can be easily ripped and replaced, that's simply not the case when it comes to essential networking and security.

Once established and intertwined into businesses' processes, replacing an underlying infrastructure is neither quick nor inexpensive. Rarely can everything be done at once. This leaves the IT team struggling to manage multiple vendors and disparate solutions while constantly troubleshooting issues as components are added, replaced, or updated. The process is so painful that many businesses build workarounds and implement long-term band-aids to provide temporary relief, further exacerbating complexity.

Managing Multiple Locations

As businesses scale, new locations must be brought on board and synced with the main office. Staff must be hired to oversee these locations, managing multiple firewalls, switches, access points, and security solutions to ensure permissions and configurations remain consistent regardless of where a user is located.

Vendors that have integrated SD-WAN into their firewalls are at a unique advantage. "Zero touch deployment and provisioning" allows devices to be sent to a remote location and "phone home" once there and plugged in. Without the need for an on-site IT person, the devices receive preconfigured templates and configurations, thereby minimizing, if not eliminating, errors that stem from manual configuration. This not only decreases risk but also minimizes onboarding time and costs arising from travel and lodging for IT staff.

But once operational, businesses must still manage these devices over the long term. Selecting a vendor with centralized cloud management significantly simplifies this task. Centralized cloud management gives IT teams visibility over the entire ecosystem—users, devices, application usage, threats, and network utilization. This helps them identify and quickly troubleshoot potential problems from anywhere the internet is available, even from their phone.

And once again, single-vendor solutions are at an advantage. But this requires proper solution integration. Vendors that have grown through mergers and acquisitions often still need multiple management consoles to oversee their supposedly "integrated platform." In contrast, vendors who maintain and develop solutions around a common operating system can easily aggregate management, reporting, and analysis into a single portal.

Third-party Integrations

Integrating third-party products can be challenging, and not all vendors do it well. Most vendors offer "open" application programming interface (API) integrations, but quality and updates can still vary widely. If not well-maintained, "tight integration" with third-party solutions can quickly become outdated.

Understanding a vendor's relationship with their technology alliance partners is key to understanding their integration story. Are they able to develop turnkey solutions together? How easy are the integrations to deploy, and how deep do they run? What is their track record of integration? If these issues are not considered, integration with third-party tools can quickly become a source of pain and complexity.

Don't Get Caught With Buyer's Remorse

As our thirst for digital innovation grows, so too do the challenges that stem from cybersecurity. The consumerization of IT has made once unaffordable technologies accessible to lean IT teams. But this growth is double-sided. Even smaller businesses have shifted from a safe, clearly defined office perimeter to a much riskier scenario. Users now work from anywhere, accessing private information through multiple devices and locations across a technology stack similar to small enterprises but growing much more quickly. And while it would be easy for a smaller business to claim, "We're too small to be attacked," the data suggests otherwise. Attackers have also taken advantage of the consumerization of technology and use "as-a-service" attacks just like legitimate businesses use Software-as-a-Service.

So, who do you trust? While large businesses can run their networking and security investments through extensive real-world testing, this is a luxury for many. Meanwhile, many vendors claim they provide all the functionality we have discussed, but the reality is often far different from sales pitches. So, how do you know which solutions work and which don't?

Luckily, there are numerous industry analysts and testing businesses whose role is to provide third-party validation. Even those with a focus on leading industry players are an advantage. A vendor's absence from such reports should raise the question of whether their solution can genuinely protect your business or has the commitment and resources to be a long-term partner.

Businesses need to select a firewall designed to support a fully integrated security fabric—one with the performance required to drive critical functionality and defend against cyberattacks at every stage of your business growth. The right solution provides the peace of mind that comes from not only knowing that your security works now but will continue to protect and sustain your business in the future, even as technologies and business strategies continue to evolve. Additionally, working with a vendor who understands your needs now and tomorrow ensures longevity, prevents unnecessary workarounds, and avoids the rip and replace conversations down the road that can derail a business.

[1] 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses, Ponemon Institute, October 8, 2019.

[2] "Avoiding Complexity: The Impact Complexity Has on Organizations Over Time and How SMBs Can Prevent It," Fortinet and Vanson Bourne, October 2021.

[3] Ibid.

[4] "2020 Cost of a Data Breach Report," IBM Security, July 2020.

[5] "HTTPS encryption on the web," Google Transparency Report, accessed September 28, 2021.

October 7, 2021 9:42 PM

1266277-0-0-EN