Small Business Firewall Guide

The Top Three Requirements for Your Next Firewall Purchase

Introduction

As businesses of all sizes embrace digital transformation, remote work and mobile devices accessing sensitive data, they are increasingly susceptible to cybersecurity threats. Reports of ransomware attacks and data breaches grow with each passing week. While small and medium-sized enterprises (SMEs) face many of the same cyber threats as larger enterprises, they carry a higher security risk due to lack of IT resources and a heavier financial burden if attacked.

It's critical that these businesses are secured with the same level of protection as large enterprises and data centers. But what are the most critical firewall capabilities to effectively secure your network and business as you grow? Read on for the top three considerations for selecting the right firewall and management solution that addresses the challenges of your business—today and tomorrow.

paloalto® NETWORKS | STRATA™ BY PALO ALTO NETWORKS

Next-Generation Firewall Requirements for Small Businesses

The requirements you have for your security functions correspond to the size and business needs of your organization, as well as the number of applications traversing your network. Managing risk has to be balanced with keeping your business running at top speed. For example, the policies you set for accessing and utilizing business applications should be easy to adopt, simple to manage and tightly integrated.

Here are the three things to consider when evaluating whether a firewall can fully protect your business: security functions, management, and performance.

Small businesses need the same enterprise-grade protection as the Fortune 500

Key Firewall Considerations

Security Functions | Management | Performance

1. Security Functions

Identify Users and Enable Appropriate Access

The Challenge

Employees, customers, and partners connect to different repositories of information within your business network and online, accessing data from different physical locations, multiple devices, applications, and operations systems. It's important to identify your users beyond IP addresses and understand the inherent risks of the devices they're using—especially if and when security policies have been circumvented or new threats have been introduced to your network.

The Solution

User and group information must be directly integrated into the technology platforms that secure modern businesses. Your firewall must be able to pull user identity from multiple sources, including virtual private networks (VPNs), wireless local area network (WLAN) access controllers, directory servers, email servers, and captive portals. By knowing who is using the applications on your network and who may be transmitting a threat or transferring files, you can strengthen security policies and improve incident response times. User-based policies will follow users no matter where they go—to your primary business location, remote offices, or home—and on any devices they use. You should be able to dynamically change user access based on changes in circumstances, whether due to new indicators of compromise or a business need, such as granting temporary access to a set of users.

Prevent Theft and Abuse of Corporate Credentials

The Challenge

Users and their credentials are among the weakest links in any organization's security infrastructure. According to Gartner, "Over 80% of security breaches are caused by weak or reused passwords."[1] With stolen credentials, attackers' chances of successfully breaching your systems increase, and their risk of getting caught decreases substantially. They can use these credentials to gain access to your network, move laterally, and escalate their privileges to gain unauthorized access to applications and data.

You need a firewall with machine learning-based analysis to better identify websites that steal credentials.

The Solution

You need a firewall with machine learning-based analysis to better identify websites that steal credentials. If the machine-learning analysis identifies a site as malicious, your firewall should be updated in real time and block it. There will always be new, never-before-seen phishing sites that are treated as "unknown." Your next firewall must allow you to block submission of your business' credentials to unknown sites and protect sensitive data and applications by enforcing multi-factor authentication (MFA) to prevent attackers from abusing stolen credentials.

Safely Enable All Apps and Control Functions

The Challenge

More and more applications, such as instant messaging applications, peer-to-peer file sharing, or Voice over Internet Protocol (VoIP), are capable of operating on nonstandard or hopping ports. Users access diverse and software-as-a-service (SaaS) apps from varying devices and locations. While these applications can provide users with a rich set of functions that ensure user loyalty, they can also represent different risk profiles. For example, once users sign in to Gmail®, which may be allowed by policy, they can easily switch to YouTube®, which may not be allowed. Your business network needs complete control over the usage of these apps and policies that allow or control certain types of applications and their functions while denying others.

The Solution

Your firewall must, by default, classify traffic by application on all ports and provide complete visibility into application usage and capabilities to understand and control their use (see figure 1). For example, the firewall should verify usage of application functions, such as audio streaming, remote access, and posting documents, and enforce granular controls over that usage, such as upload versus download permissions or chat versus file transfer. Traditional "one-and-done" traffic classification ignores the fact that these commonly used applications share sessions and support multiple functions. If a different function or feature is introduced in the session, the firewall must perform another policy check. Continuous state tracking to understand the functions each application may support—and the different associated risks—is a must for your next firewall.

1. David Chase, "Integrating Password Management Software in Your Enterprise's SSO," Gartner, January 7, 2021, https://www.gartner.com/en/documents/3945609.

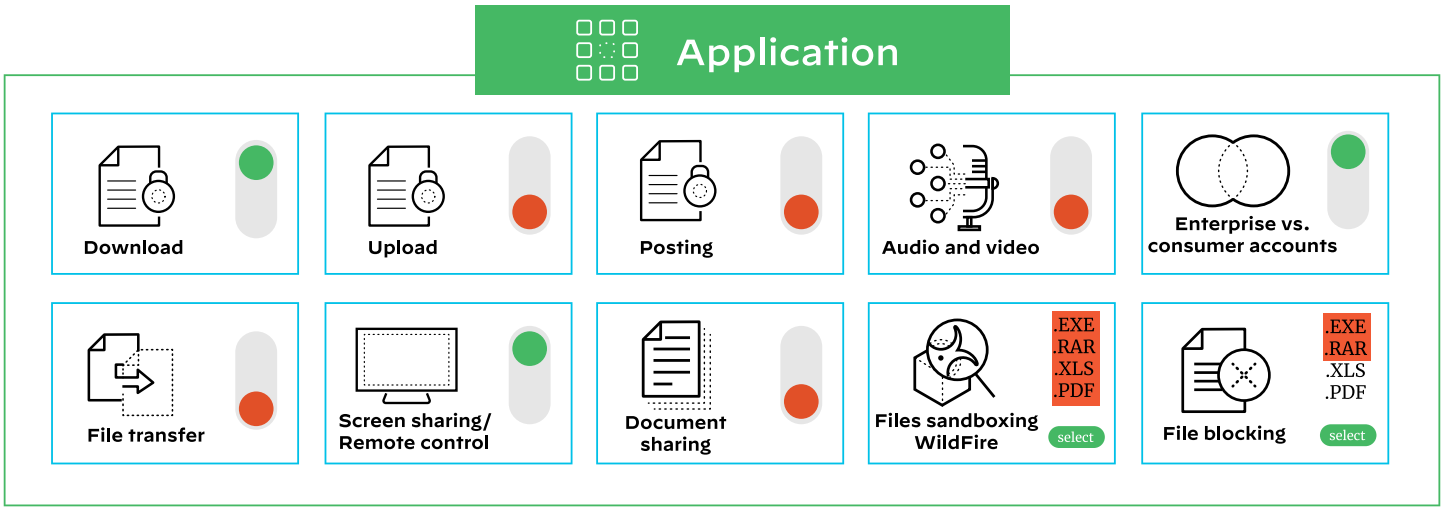

Figure 1: Easily control application usage with continual tracking and monitoring tools.

Secure Encrypted Traffic

The Challenge

Attackers can exploit encryption to hide threats from security surveillance. Even businesses with mature, comprehensive security measures can be breached if encrypted traffic is not monitored. In addition, TLS/SSL encryption is used nearly universally and end users can easily configure it to hide non-work-related activity.

The ability to decrypt TLS/SSL-encrypted traffic is a foundational security function.

The Solution

The ability to decrypt TLS/SSL-encrypted traffic is a vital security function. Firewalls should include recognition and decryption on any port, inbound or outbound; policy control over decryption; and the necessary hardware and software elements to perform decryption across simultaneous SSL connections without compromising performance. However, your firewall must be flexible enough to easily decrypt certain types of encrypted traffic via policy (e.g., HTTPS from unclassified websites), while other types are left alone in compliance with privacy standards (e.g., web traffic from known financial services organizations.) A next-generation firewall should apply security and load balancing to decrypted flows across multiple stacks of security devices for additional enforcement.

Stop Advanced Threats to Prevent Successful Cyberattacks

The Challenge

Most modern malware uses advanced techniques to transport attacks or exploits through network security devices and tools, such as wrapping malicious payloads in legitimate files or packing files to avoid detection. With readily available exploit kits and subscription models like phishing-as-a-service, threat actors now have access to a wide array of sophisticated attacks. This presents a huge problem for organizations that rely on siloed legacy security technologies to combat advanced threats.

Don't overlook DNS Security. It can be almost impossible to identify and stop DNS threats.

Domain Name System (DNS) is a massive, often overlooked channel that can be used for malware delivery, C2, and data exfiltration. According to Palo Alto Networks Unit 42 threat research team, almost 80% of malware uses DNS to establish communication with a C2 server.[2] Unfortunately, security teams lack basic visibility into how threats use DNS to maintain control of infected devices. It's almost impossible to keep up with the high volume of malicious domains, let alone advanced tactics for stealthy data theft.

2. Stop Attackers from Using DNS Against You, p.2, Palo Alto Networks, June 11, 2020, https://www.paloaltonetworks.com/resources/whitepapers/stop-attackers-from-using-dns-against-you.

The Solution

Your firewall, integrated with security services and using machine learning (ML), should automatically prevent known threats. Having cloud-based inline ML enables security tools to analyze traffic in real time and protect against advanced file- or web-based threats often cloaked from crawlers. This significantly closes the window of time for attackers to exploit vulnerabilities or penetrate networks.

It's also critical to contextualize behaviors through robust analytics and integration with other parts of your security infrastructure. This helps identify threats at all points within the cyberattack lifecycle—not just when they first enter your network. By integrating security services, your firewall can provide evasive countermeasures that prevent the most sophisticated and evasive attacks from being successful without requiring you to manage or maintain multiple single-function appliances. This ensures that your security posture is proactive against advanced threats.

2. Security Management

The Challenge

New firewalls, as with any technology, are not typically simple to deploy, configure, and manage. Many businesses may not have in-house expertise to provision the device or make day-to-day changes, but the security of your business relies on a properly configured device.

The Solution

Businesses should look for firewall solutions that offer simplified onboarding, automated deployment processes, and streamlined operations. Low or no-touch provisioning allows you to automate the onboarding of new firewalls to all of your locations and then remotely configure and manage your firewalls with a centralized management tool. In addition, centralized visibility across the network is key to gaining comprehensive insights into your network traffic, logs, and threats.

3. Security Performance

The Challenge

Organizations of all sizes need high network speeds to stay efficient and competitive. Slow connections and network outages can reduce productivity, sales, and customer experience. Because businesses need cost-effective security, IT teams sometimes choose low-cost appliances, not realizing they aren't getting predictable performance. Alternatively, some IT teams disable security features on their firewall to increase throughput, putting their organization at risk for cyberattacks. Businesses should not need to trade security for performance.

The Solution

Businesses do not need to choose between low cost and high performance when it comes to network security appliances. In recent testing, Miercom, an independent network and security testing organization, found that businesses can expect predictable throughput with security services enabled on certain firewalls at a competitive price. There is no reason to compromise on your network security for any of your locations.

Figure 2: PA-400 Series

Conclusion

As you research your next firewall, it's important to consider three areas: security functions, operations, and performance. Attackers can often see smaller businesses as easy targets, so it's important to adopt best-in-class security with Level 7 enterprise-grade protection similar to what is available for data centers and large office locations.

The Palo Alto Networks PA-400 Series Next-Generation Firewalls offer the same comprehensive security we provide to the Fortune 500, tailored to small and medium businesses. Their uncompromising performance, packed into a small desktop form factor, makes them ideal for securing small and medium enterprises. Learn more about the latest ML-Powered Next-Generation Firewalls for small businesses.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com