Protecting Every Edge To Make Hackers' Jobs Harder, Not Yours
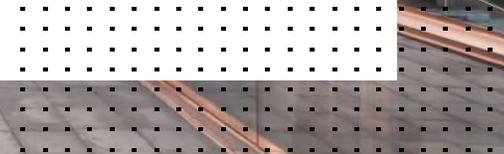
Table of Contents

Executive Summary

Today's users need a network that allows them to connect to any resource from any location using any device. At the same time, data center and campus networks need to operate in a hybrid IT architecture, working alongside next-generation branch offices, private and public multi-cloud networks, remote workers, and cloud-based SaaS services. As a result, enterprise security is under enormous pressure to provide complete visibility across a moving and distributed network environment to secure and track every user and device accessing data, applications, and workloads.

Unfortunately, most traditional security tools, like legacy firewalls, were never designed for this sort of challenge. They were designed for static network checkpoints where workflows and data were highly predictable. But those days are gone.
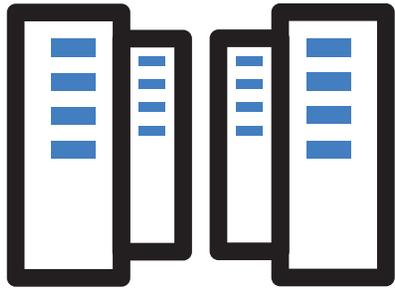
New Problems

The data center, though essential, is no longer the primary location for corporate applications. Instead, applications can be deployed anywhere. Because a transaction or workflow may span multiple environments and applications, the source, destination, and data path can sometimes change several times, making it impossible to track and secure a transaction end to end.

5G adoption has also left traditional firewalls struggling to keep up—especially when 95% of all traffic is now encrypted. Encrypted traffic, especially secure sockets layer/transport layer security (SSL/TLS) tunnels, is widely used to secure remote access and transactions. However, cyber criminals also use encryption to hide malicious activities, such as stealing company data and secrets and to launch ransomware attacks. Most firewalls cannot decrypt and inspect encrypted traffic without seriously impacting performance and user experience. So, most encrypted traffic—especially data traveling at very high speeds—goes uninspected.

Multi-cloud environments and a hybrid workforce are also rewriting security requirements. The cloud enables agile application development and scale-out/scale-up functionality to accommodate growing application access by remote workers. However, numerous business-critical applications still need to be housed in the on-premises data center for reasons such as compliance, privacy, or the need to protect intellectual property. However, most traditional firewalls cannot support hybrid data center use cases, including user-to-data center, data center-to-cloud, user-to-cloud, and data center-to-data center interconnect models.

The data center, though essential, is no longer the primary location for corporate applications. Instead, applications can be deployed anywhere.
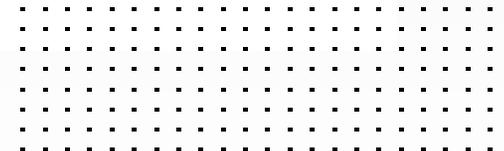
New Solutions

Supporting and securing hybrid architectures requires single-lens visibility across the entire distributed network. This includes knowledge of every user and device on the network, the applications and resources they are accessing, and identifying anomalous behavior and malicious activity anywhere. It also requires marshaling all necessary security resources to direct a timely, coordinated response. To support today's expanding networks and their numerous edges, many businesses have begun adopting disparate secure access service edge (SASE), solid-state wide-area network (SD-WAN), and zero-touch network access (ZTNA) solutions creating complexity while fracturing visibility, compromising user experience, and limiting the ability to respond effectively to attacks.

What's needed is a new next-generation firewall (NGFW) approach that integrates these functions into a unified platform providing contextually coordinated security across the network.

Fortunately, regardless of where security needs to be deployed—whether a campus or data center environment, multi-cloud network, branches, or home offices—use cases are remarkably similar. Addressing them requires breaking down security into three primary functions: Protect, Consolidate, and Scale. By understanding these three concepts, you can implement a security strategy designed to deliver a seamless user experience and protection aligned with business goals.

Protect

An NGFW needs to be aware of the entire application life cycle, including interoperating with tools to accelerate application access and use. This includes providing essential web filtering augmented with advanced image recognition and video content filtering to ensure acceptable use and compliance.

An NGFW solution also needs to provide advanced security solutions to prevent known, zero-day, and unknown attacks with integrated intrusion prevention system (IPS) and anti-malware. It needs to support constantly shared threat-intelligence feeds from complementary products like email security and sandboxes to detect and prevent the latest threats.

And it needs to interoperate with other solutions, such as endpoint detection and response (EDR), web application firewalls (WAFs), and other security systems. This combination of native threat protection and integration with other technologies ensures that the network is effectively protected against all current and emerging threats.

Consolidate

An NGFW should also provide full visibility into sophisticated attacks that hide in secure HTTPS channels to steal data and load ransomware. It should also seamlessly integrate essential networking and security functions into a unified solution—whether delivered directly from an on-premises NGFW or through a cloud-delivered SASE—that combines advanced routing and connectivity functions with dynamic security solutions.

It also needs to identify any user, device, or application requesting access and automatically assign it to its appropriate network segment. This requires natively integrated proxy services. When a device makes its initial access request, the firewall needs to work with endpoint clients (for users and servers) and network access control (for Internet-of-Things [IoT]/Industrial-Internet-of-Things [IIoT] devices) solutions. It also needs to support multi-factor authentication to determine the role of a user or device, link it to associated policies, and only grant access to the application or segment of the network required to do its job.

For applications and workflows that move from one environment to another, an NGFW needs to understand, implement, and enforce the same policy everywhere. This consistent orchestration and enforcement approach, built with single-pane-of-glass management, allows security to follow applications, workflows, and other transactions end to end.
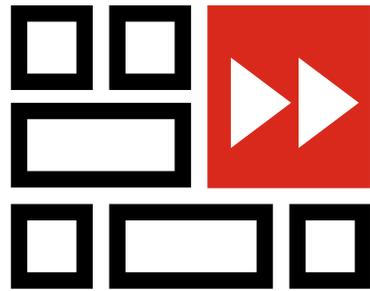
For applications and workflows that move from one environment to another, an NGFW needs to understand, implement, and enforce the same policy everywhere.
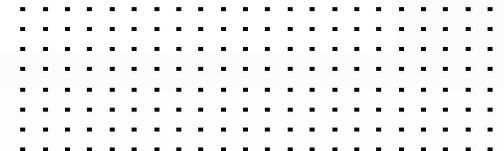
Scale

Regardless of where a firewall is deployed, one thing remains true: It needs to be fast. And it will need to be even faster tomorrow. Today's data centers generate and process massive amounts of data at transactional speeds—whether it's big data for advanced modeling, low latency for high-speed financial transactions, or hyperperformance for massive multiuser environments.

Speed refers to how quickly a firewall can inspect data and its ability to support automation. An NGFW needs to effectively protect the network from high-speed attacks with advanced and coordinated security as well as not be bogged down with time-consuming manual provisioning efforts. Manual operations slow things down, and configuration errors can be compromised by ransomware and other attacks.

The challenge is that most traditional firewalls are already running at capacity—which means they can't scale to match growing business demands. That's because they were never designed with hyperperformance in mind. Their biggest problem is they rely on off-the-shelf processors in an age when everything—whether graphics cards, smartphones, or cloud servers—runs on custom chips. Security is a processor-intensive activity. Scaling to meet today's performance demands requires delivering full firewall functionality without sacrificing performance— or overwhelming limited IT and security budgets.

www.fortinet.com

September 6, 2022 2:14 PM

1161971-0-0-EN