FORTINET

Keeping Hackers Off Every Edge

Table of Contents

Executive Overview

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 must operate in a hybrid IT architecture, working alongside next-generation branch offices, private and public multi-cloud networks, remote workers, and cloud-based Software-as-a-Service (SaaS) solutions. As a result, enterprise security teams are 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. This gives cybercriminals an excellent opportunity to infiltrate your network from the edge. And once they are in, they can wreak havoc.

Unfortunately, most traditional security tools, like legacy firewalls, were not designed for this challenge. They were designed to be static network checkpoints with highly predictable workflows and data. What's needed now is unified network security designed for today's hybrid infrastructure with integrated next-generation firewalls (NGFWs) across the network and form factors, centralized management, and coordinated response to threats. This unification of security needs to protect assets and users located anywhere, converge and consolidate distributed solutions to reduce overhead, simplify management, enable automation, and dynamically scale services and bandwidth to meet your constantly evolving business requirements.

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.[1] Encrypted traffic, especially secure sockets layer/transport layer security (SSL/TLS) tunnels, is widely used to secure remote access and transactions. However, cybercriminals 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, the need to protect intellectual property, or the need to secure sensitive records. 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.

Ultimately, organizations end up creating complex workarounds to get disparate solutions to loosely work together. This is causing the data center infrastructure to become more complex as the number of devices, servers, switches, routers, firewalls, load balancers, and other interconnected components attempt to provide a seamless flow of data between various systems and applications. As the number of devices and the volume of data traffic increases, network complexity also increases, making it more challenging to manage, monitor, and troubleshoot issues.

Though essential, the data center 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 and the applications and resources they are accessing. Plus, it's necessary to identify anomalous behavior and malicious activity everywhere. Marshaling all the required security resources to direct a timely, coordinated response is also vital to stopping threats. To support today's expanding networks and their numerous edges, many businesses have begun adopting disparate secure access service edge (SASE), software-defined wide area network (SD-WAN), and zero-trust network access (ZTNA) solutions. This creates complexity while fracturing visibility, compromising user experience, and limiting the ability to respond effectively to attacks.

Integrating NGFWs with these functions can offer both strong defense and network resilience. With centralized management to enforce unified policy in real time, this combination can help mitigate risks from both internal failures and external attacks across all surfaces. Because of its native interoperability, this approach simplifies operations, ensures compliance, reduces complexity, and enables broad automation to increase operational efficiency for today's hybrid business models. It doesn't matter if you have all on-premises firewalls, all cloud firewalls, or a mix of both. The enhanced value lies in centralized and unified management across all firewall deployments.

Fortunately, use cases are remarkably similar regardless of where security needs to be deployed, whether a campus or data center environment, multi-cloud network, branches, or home offices. Addressing them requires breaking down security into three primary functions: **protect, converge,** 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

The main objective is to prevent any threat from entering the network. But if that should happen, the next step is to minimize business disruptions as fast as possible. An NGFW must 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, such as an integrated intrusion prevention system (IPS) and anti-malware, to prevent known, zero-day, and unknown attacks. It needs to support constantly shared threat-intelligence feeds from complementary products like email security and sandboxes to detect and prevent the latest threats.

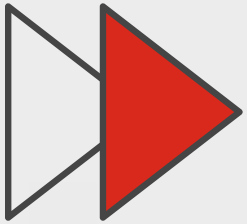
It must also interoperate with other solutions, such as endpoint detection and response (EDR), web application firewalls (WAFs), and other security systems. This combination of native threat protection and integration with other technologies ensures the network is effectively protected against all current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

Converge

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 must also 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 must 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 must also 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 hyper-performance 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 and 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 hyper-performance 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.

AI-Powered Secure Networking for the Modern World

Firewalls are the first line of defense to keep hackers off the networks. Fortinet's patented security processing unit (SPU), with the industry's only converged security and networking, is a critical component of its AI-powered NGFW architecture, designed to enhance security performance and network efficiency. By leveraging Fortinet's unified security platform, businesses can manage their entire security infrastructure at scale from a single interface, regardless of firewall form factors and deployment locations. This integration approach allows for better coordination and faster threat detection and response across all attack edges.

[1] "HTTPS encryption on the web," Google Transparency Report.

FORTINET

www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

December 27, 2024 2:24 PM / 2170366-A-0-EN