POINT OF VIEW

Five Mistakes To Avoid When Securing a Hybrid Network

Most organizations today now operate on a hybrid network. According to Gartner, the recent shift to a remote workforce has had a lasting impact on networks. "Through 2024, organizations will be forced to bring forward digital business transformation plans by at least five years as a survival plan to adapt to a post-COVID-19 world that involves permanently higher adoption of remote work and digital touchpoints."[1]

However, today's hybrid networks make centralized visibility and control increasingly difficult to achieve, especially when an organization does not have a central security strategy in place. Instead, organizations have deployed an average of more than 45 security tools across their network, most from different vendors. And each incident they respond to requires coordination across 19 different solutions. Such complexity inevitably leads to poor visibility, limited control, and exploitable security gaps.[2]

Consolidation and integration of networking and security are the best strategies for addressing such overly complex environments. Deploying a common next-generation firewall (NGFW) platform as the backbone of a unified security strategy enables end-to-end visibility, ease of management and control, and consistent enforcement across the network. But selecting the right solution can be daunting, and there are several critical mistakes IT leaders need to avoid.

Five Common Mistakes When Securing Hybrid Networks

Mistake 1—Over-rotating to a cloud-based solution. Some organizations are considering replacing their traditional security with a secure access service edge (SASE) solution. However, few organizations have a cloud-only environment in place. The reality is, most have—and will continue to own and operate—a hybrid network. Over-pivoting to a cloud-only security strategy ignores the needs of those users working on-premises in local campuses.

According to Gartner, "Classic datacenter edge firewall designs are not obsolete and must be maintained in support of traditional inbound data flow patterns and residual outbound connections from internal users that remain on-site in campus environments or at large branches."[3]

Mistake 2—Ignoring the importance of the on-premises data center. For a variety of reasons, many organizations simply can't move critical services from the data center to the cloud. But many of its applications need to remain available for external customers and corporate users, reinforcing the importance of traditional, on-premises firewalls.

The Gartner report confirms this approach, as well as acknowledges challenges related to cloud provider security solutions. "A significant minority of organizations consider these offerings to be immature when compared to third-party vendor solutions and sometimes deploy network virtual appliance (NVA) versions of these third-party solutions directly in public cloud IaaS instances." "Private and public cloud operators offer native solutions for firewall, WAF, distributed denial of service (DDoS) and ADC."[4,5]

> "For public-facing applications hosted in private data centers, it is recommended that IT leaders consider the traditional enterprise firewall edge design."[6]

Hybrid networks need a security solution designed to operate natively in any environment—protecting all edges consistently, seeing and sharing threat intelligence across the network, and delivering coordinated security enforcement anywhere. That starts with a common network firewall platform deployed at every network edge: campus, data center, branch, private and public clouds, and as a cloud-based service for remote and mobile workers.

Mistake 3—The "Best-of-Breed" myth. There is a mistaken belief that a best-of-breed approach provides better security at the edge. Instead, such an approach usually leads to product sprawl, resulting in an overly complex network and isolated security architectures that can't effectively share threat intelligence. This defeats the very purpose of building a strong security posture—point solutions can never provide the same level of visibility and security as those designed to work together. Only integrated security ecosystems, built around the premise of sharing actionable threat intelligence, can provide robust, coordinated, and timely responses to cyber events.

A unified system is always more secure than the sum of its components. For example, how would a best-of-breed approach handle the case of a user with a compliant laptop who then inserts an unauthorized USB thumb drive? Most isolated network security devices have no way to detect or respond. But an endpoint detection and response (EDR) solution designed to collaborate with other security systems can inform the NGFW about this policy violation, which can then provide policy enforcement, such as isolating the device or removing it from the network. This is only possible with a security ecosystem approach built around a common security platform, where actionable threat intelligence is shared across all security devices, and policy can be enforced wherever it is most effective.

Mistake 4—Not thinking holistically. Evolving hybrid architectures expand the attack surface, reducing visibility and increasing risks. Compounding the problem further, the volume of encrypted traffic is estimated to soon reach 95%.[5] However, most network firewalls are unable to inspect encrypted traffic while maintaining the performance levels today's applications require. So how do you secure a network when you only have real visibility into 5% of your traffic? IT leaders need to choose an NGFW solution that can operate at scale across the network without getting bogged down with compute-intensive operations like secure sockets layer (SSL) decryption, threat detection, and automated remediation.

This begins with a solution designed to support the latest encryption standards, like TLS 1.3, while ensuring existing TLS 1.2-based communications are not broken. Beyond visibility, the real challenge in future-proofing your security is selecting a solution able to learn about the state of dynamically changing resources scattered across the network and then adapt in real time. This is especially challenging when your security strategy needs to include multi-cloud. Not considering how various clouds are built and configured can pose a nightmare for normalizing security policy across different cloud providers. Therefore, reasonable care must be taken to select an NGFW solution capable of learning about the ever-changing state of private and public cloud resources and then delivering consistent end-to-end security across this hybrid IT architecture for a strong and consistent security posture.

Mistake 5—The risk of implicit trust. Traditionally flat networks focus on preventing attacks from the outside but give attackers lots of latitude once the perimeter has been breached. Organizations need to consider an NGFW solution able to provide security beyond the edge by reducing the attack surface through network segmentation to prevent the lateral propagation of north-south threats and microsegmentation to prevent east-west proliferation.

In addition to dynamically segmenting the network to prevent lateral movement, an NGFW must also dynamically adjust levels of trust by monitoring behavior through tools like user and entity behavior analytics (UEBA). And it must be able to reduce or revoke trust if a user or device begins to behave suspiciously.

It must also integrate with zero-trust access (ZTA) and zero-trust network access (ZTNA) solutions to control access to network resources, down to granular per-application segmentation. And it must also manage the proliferation of headless devices, like Internet of Things (IoT) or Industrial Internet of Things (IIoT), by seamlessly integrating with a network access control (NAC) solution to ensure that every device, application, and transaction is accounted for and secured.

Hybrid Networks Need a Network Firewall Designed for Today's Digital World

Hybrid networks require an NGFW designed to provide consistent protection, visibility, and control across even the most distributed and dynamic environments. This requires selecting a solution designed to operate at any edge, in any form factor, to seamlessly integrate networking and provide consistent policy enforcement, centralized policy orchestration, real-time intelligence sharing, and correlated threat response. By enabling security policies and enforcement to follow applications and workflows end to end, organizations can enjoy broad visibility and control across their continually changing networks while ensuring optimal user experience for today's work-from-anywhere reality.

[1] Gartner, "Forecast Analysis: Remote and Hybrid Workers, Worldwide," Ranjit Atwal, et al., June 2, 2021. (P1).

[2] Kim Samra, "IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue," IBM, June 30, 2020.

[3] Gartner, "How the Shift From Firewall Appliances to Hybrid Cloud Firewalling Will Change Selection Criteria," Aaron McQuaid, March 10, 2021. (P1).

[4] Ibid (P5).

[5] Ibid (P5).

[6] Ibid (P11).

FORTINET®

www.fortinet.com

June 23, 2021 5:09 AM
745599-A-0-EN