POINT OF VIEW

Requirements for a Security-Driven Networking Strategy, from SD-WAN to SASE

Digital innovation forces all organizations to redesign their networks and provide a better user experience for employees and customers. The perimeter, once a narrow point of access for the network edge, now extends across the entire IT infrastructure, and introduces new requirements across the data center, wide-area network (WAN), local-area network (LAN), and Cloud Edge. More recently, the COVID-19 pandemic has highlighted the need for business continuity plans that include flexible, anywhere, anytime, secure remote access—at scale.

At the same time, security threats aren't getting any less sophisticated, or less frequent. Over a third of data breaches in 2020 were the result of social engineering.[1] That's just one example of why providing better security along with re-designing the network is becoming critical for all businesses.

A **security-driven networking strategy** accelerates the convergence of networking and security across the connected environment—all edges and users—from the core, out to the branch, and into the cloud. This strategy enables organizations to effectively defending today's highly dynamic environments while preserving an excellent user experience for employees and customers.

With security at their core, networks can evolve, expand, and adapt to digital innovations with ease, at the levels the next-generation of computing—including hyperscale, multi-cloud, 5G, and other fast-arriving trends—so significantly needs. Converged networking and security means security that is flexible, anytime and anywhere.

Key Elements of a Security-Driven Networking Strategy

A security-driven networking strategy accomplishes three needs overall:

- The ability to manage external and internal risk for on-network users
- The ability to provide flexible, cloud-native security for off-network users
- The ability to improve the overall user experience while reducing WAN costs

The first step to achieving security-driven networking is to **apply custom security processing units**, or ASICs, that allow teams to run networking and security very fast, and enable the **consolidation of all security features**, including application control, firewalling, and intrusion prevention system (IPS), into solutions like network firewalls without compromising functionality or performance. Required use cases include Secure software-defined WAN (SD-WAN), next-generation firewall (NGFW), IPS, secure sockets layer (SSL) inspection, app control, web filtering, antivirus and anti-malware, sandboxing, and accelerated segmentation. (That last item is especially important for a security-driven network strategy because a lot of firewalls can't handle the processing overhead required to support dynamic internal segmentation.)

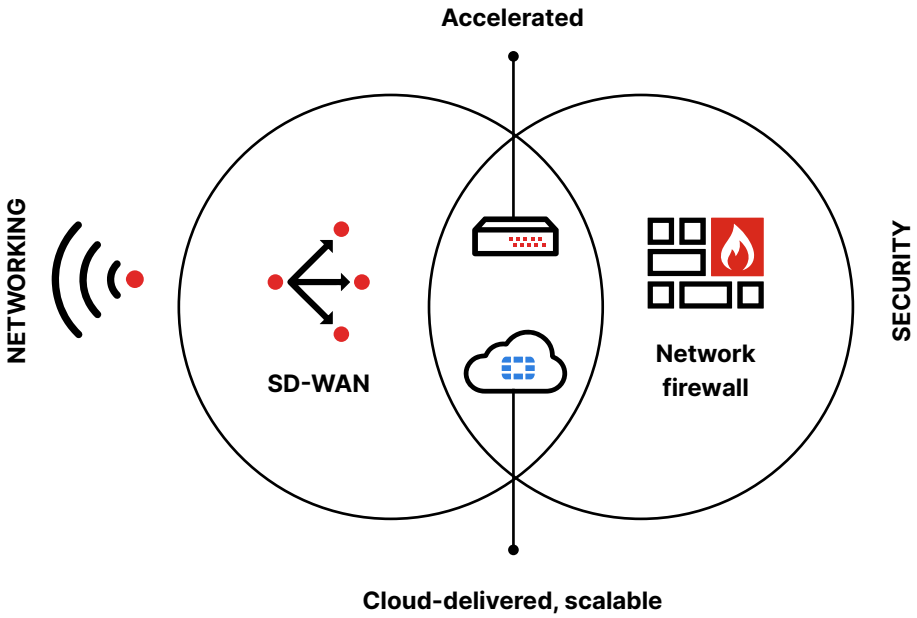
Purpose-built cloud architecture enables convergence of security and networking for organizations that are either cloud-first, or looking for flexibility when deploying solutions.

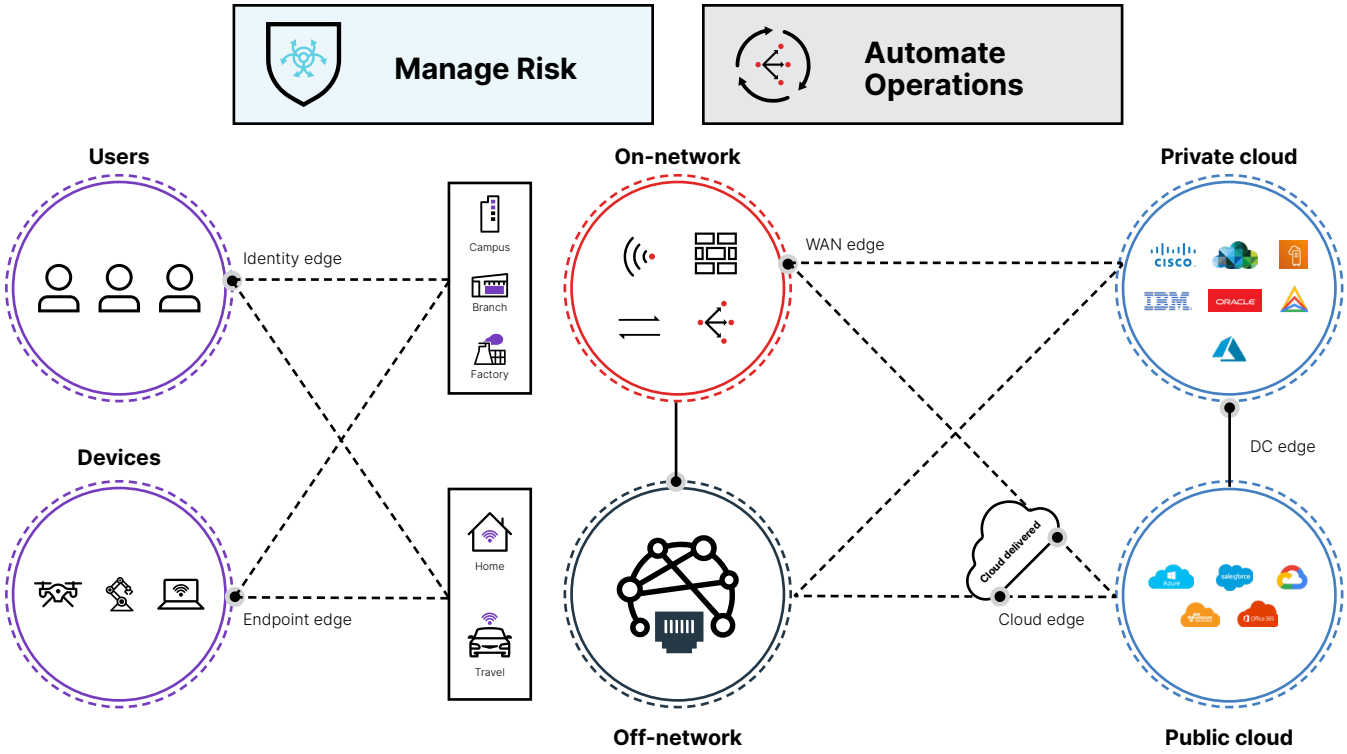
Going forward, network firewall solutions will also need to **support hybrid and hyperscale data centers and the performance requirements of 5G**. New, high-performance innovations—such as elephant flows, edge computing, protection of high-definition television (HDTV) and other rich media traffic, 5G networks, and dynamic core segmentation will require unprecedented performance levels from a next-generation firewall. But because they were not designed with this performance in mind, some solutions will simply be unable to meet these demands of tomorrow without an enormous price tag—and in many cases, not even then.

A security-driven networking strategy transforms WAN edges with enterprise-class SD-WAN, which is fully integrated into an NGFW device. This integration helps make **SD-WAN** truly secure, instead of SD-WAN technology that needs security as an overlay. A robust approach to SD-WAN also includes artificial intelligence (AI)-powered predictive analytics, intuitive orchestration, and the ability to self-heal.

Finally, organizations need to extend security into the wired and wireless network edges through deep integration, enabling consistent and pervasive security enforcement for LAN edges. These are **the conditions for health-aware, responsive networks** that extend security to the access edge and network edges.

All of these edges also require **centralized management** to reduce complexity and enable automation to make the network more agile.





The Right Foundation for Securing the Cloud Edge: SASE

In 2020 and beyond, a discussion of security-driven networking unavoidably includes Secure Access Service Edge (SASE). SASE is an emerging enterprise framework that combines network security functions with WAN capabilities to support the dynamic, secure access needs of today's organizations—right in line with a security-driven networking strategy. SASE plays a critical role in ensuring that security can be delivered anywhere, especially at the Cloud Edge, and for securing remote and mobile users.

SASE is generally classified in terms of cloud computing, but there are common circumstances that may require a combination of physical and cloud-based solutions for SASE to be effectively integrated into the network. This may include combining SASE connectivity with network access controls and edge security devices, supporting a physical SD-WAN device— especially one that contains a full stack of security—or even needing to integrate with technologies such as wireless LAN controllers or WiFi access points at branch offices. Critically, SASE enables organization **to secure remote users** with always-on security—regardless of their location—creating a better user experience and improved productivity as they are using purpose-built cloud edge for optimized, low-latency paths.

A SASE offering and a complete security-driven networking strategy are not the same thing. In addition to the essential cloud-based protections described in SASE's popular definition , a robust SASE solution also needs to support such things as network segmentation and compliance requirements that cloud-based security can't address without shuttling traffic out to the cloud for inspection.

It's then when SASE becomes the basis for a complete, security-driven networking strategy—delivering the kind of security and performance required by organizations everywhere.

[1] "2020 Data Breach Investigations Report," Verizon, May 2020.

[2] "The Future of Network Security Is in the Cloud," Gartner, September 13, 2019.

FORTINET

www.fortinet.com

May 13, 2021 10:39 PM
745599-A-0-EN