Point of View

Is the Network the Security?

What is a network and infrastructure professional to do?

Well, for starters, let's not overthink the terminology. SASE is the Secure Access Service Edge, a term coined by researcher Gartner[1] in 2019 to describe an architectural framework … OK, a useful way of setting up the network and security infrastructure to satisfy a cloud-first future. What does that mean? Well, we're all in the cloud now, accessing critical company data from our homes, our local coffee shops, and our mobile devices. We're all increasingly remote, and the global pandemic means we're all adjusting to a new normal where remote is Option A, not an occasional deviation from "going to the office."

Despite what various technology vendors would have you believe, SASE does not mean using old or retrofitted technology to try to meet these data access requirements. SASE does not mean various pockets of products that can't operate in an integrated, easy-to-manage fashion. SASE does not mean buy more stuff, hire more people, or look at more logs. SASE does not mean throw enough security at your network to effectively destroy the performance of that network in the name of safety.

With Powers Combined…

SASE, if properly implemented, means network and security services that we once knew as totally separate or at least, discrete, in terms of technologies and job roles are integrated so tightly into a single-platform approach that … wait for it … the network is the security.

Facts

90%

Nearly 90% of enterprises are either actively working on a digital transformation project or have just completed one.

Digital transformation can't happen without security and networking transformation.

In the rush to market "SASE," many vendors are trickling water on you and telling you it's raining.

[1] "Invest Implications: 'The Future of Network Security Is in the Cloud,'" September 13, 2019

When your network is the security:

- **You get speed. You get scale. You get performance**. No business seeking digital transformation benefits—meaning all businesses—can afford to trade security for network performance, or vice versa, allowing onerous security controls to degrade network performance and keep users from being productive as they use cloud applications for day-to-day business.
- **You get more for your money and work with fewer technology vendors.** Gartner says it best: by 2024, nearly one-third of enterprises will adopt cloud-delivered Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access, and branch office Firewall-as-a-Service capabilities from the same vendor, up from less than 5% in 2020. SASE is more efficient. SASE is ultimately a more favorable total cost of ownership. SASE means fewer vendors on your line card.[2]
- **Your infrastructure provides continuous adaptive trust to protect your data.** Security goes beyond merely controlling who has access to information and moves toward a state of not just "Zero Trust," but continuous adaptive trust, in which real-time access and policy controls adapt on an ongoing basis based on a number of factors, including the users themselves, the devices they're operating, the apps they're accessing, the threats that are present, and the context with which they're attempting to access data.

How did we get here?

Consider:

- Workforces now demand the ability to work from anywhere.
- More than 90% of devices sold today are mobile, and those devices are being used to access business systems somewhere off-premises in at least half of all cases.
- The average enterprise-level business also now has more than 1,200 SaaS applications in use—dwarfing the number of on-premises applications, and indicating that the sheer volume of critical business data and the number of locations from which it can be accessed have greatly expanded the available attack surface.
- More than 50% of Internet traffic related to SaaS and cloud apps contains essential business information.
- At the same time, cloud-delivered malware is now responsible for more than 65% of all malware delivery—increasing every quarter where it was less than 20% of all malware less than 18 months ago.

Now, that's a lot of data thrown at you. The simplest way to think about all of these shifts and what they collectively mean is that more businesses are using more cloud applications, enabling more remote access to more critical data, and seeing heightened security risks as a result. **But what's often missed in the rush to apply proper security measures to cloud access—and get you closer to that SASE ideal—are the companion networking needs**. Straight up: if the network performance degrades because of security, the user experience degrades as a result, and business productivity slows to a crawl. Users need fast, direct access to their apps and data, and they need it from anywhere.

Security and networking can't be trade-offs, and teams are misaligned if coverage and performance can't match the security controls necessarily applied when accessing data using cloud apps. Here are some things to think about when it comes to designing networking and security for an exceptionally well-operating converged architecture.

---

[2] "Gartner Forecasts 51% of Global Knowledge Workers Will be Remote by the End of 2021," June 22, 2021

Prevent the "Backhaul Blues"

You wouldn't travel to San Francisco from Los Angeles by way of Cairo, would you? Well, many businesses today use an architecture that relies heavily on traffic backhauling, also known as "hairpinning."

Hairpinning, in a networking context, is the method where a packet travels to an interface, goes out towards the internet but instead of continuing on, makes a "hairpin turn" and comes back in on the same interface. But one doesn't need to be a network engineer to realize this approach is going to impact user experience, adding latency and slowing things down significantly. Putting user experience and ultimately business productivity aside, this approach also puts a greater burden on the expensive and hard-to-maintain private WAN links, like MPLS connections, that enterprises have relied on for a long time for bridging together their distributed enterprise.

Most networking vendors still haven't solved this, and many are repeating the mistakes seen in traditional enterprise WAN design by replicating them inside a cloud form factor. The classic example of this is the virtual point of presence (or vPOP), which provides a misleading view both of total network coverage, and where traffic processing occurs within the vendor's network.

At the most simplistic level, vPOPs provide an entry and exit point for traffic. But if a remote user in, say, Kenya, is connecting to a vPOP in Johannesburg, South Africa, only to have their traffic sent to Frankfurt, Germany, for processing, and then back to Johannesburg before the user's request would head out to the internet and the web, cloud, or SaaS app they are trying to access, imagine the latency introduced with this back and forth, routing across huge distances, over multiple networks, ultimately slowing the user experience to a crawl. The conundrum is that vPOPs are literally traffic hairpinning all over again with the same implications for complexity, latency, and potentially, cost.

Critical Questions to Ask:

- ☐ What can be done to slash my WAN costs and reduce reliance on MPLS circuits?
- ☐ How can I steer more traffic direct-to-net to address the cloud generation?
- ☐ What role does SD-WAN have in my digital transformation journey?
- ☐ How can I remove network latency to improve application performance?

Phase Out the VPN

Ask enough IT people what they'd simply love to be able to do in the next few years, and chances are more than a few will respond, "Get rid of my VPN." It's easy to understand why: many VPNs exist as appliances within an enterprise's on-premises security stack. As the traditional perimeter disappears, and the security stack follows suit into cloud services, there's no sense in paying for the upkeep of a costly VPN appliance, especially when Zero Trust Network Access (ZTNA) approaches are much more aligned to cloud-first environments and are proven to significantly reduce capital expenses over several years.

Quite a few enterprises still require users to be on VPN and, as noted earlier, backhaul all traffic through the data center, even if they are using cloud-destined applications. The problem is that they are relying on equipment they deployed pre-pandemic when only a very small proportion of the workforce was offsite. Their systems are not sized appropriately for this volume of remote work. They might manage this discrepancy by kicking anyone who's idle off the VPN, but then an employee who steps away to refill a cup of coffee might have to launch a new VPN session. This is another example of security undermining user experience and business productivity. When that happens, enterprise employees are tempted to find workarounds—which is perhaps why more than 97% of cloud apps in use in the enterprise are unmanaged by a central security or IT function (effectively, "shadow IT").

Critical Questions to Ask:

- ☐ How can I reduce the cost and complexity of managing my legacy VPNs?
- ☐ What alternatives are available to extend access to business partners or contractors?
- ☐ How can I better support DevOps by simplifying their access to cloud workloads?
- ☐ What is the best approach to implement zero trust and improve my security posture?

Determine the Right Role for SD-WAN

One of the buzziest of buzz words in networking these days is the software-defined wide-area-network, which you know more colloquially as "SD-WAN." SD-WAN technology uses a virtualized network overlay to connect branch offices, allowing organizations to better tap the public Internet and low-cost broadband to save on expensive, legacy MPLS connections. Along with cost-cutting—which can be as significant as 65% compared with traditional alternatives—SD-WAN benefits also include increased network availability, better traffic prioritization, and more intelligent path selection. (Not an inveterate networker? Well, just know that these are good things.)

In recent years, SD-WAN's role in SASE has been rightly described as important, but it has also been significantly overstated. SD-WAN allowed for a near-total transformation of the WAN back when security could be centralized. But guess what? Security is no longer centralized.The role of SASE is to deliver the right security where and when it's needed—ideally at the Internet edge, which is also where most SaaS apps and websites live. That leaves only one connection left for SD-WAN to optimize in most scenarios: the one from the users to the security stack at the Internet edge.

The number one concern of networking professionals is whether the network is up and running. Then they focus on its performance, wanting to ensure it is fast, responsive, and able to handle their critical business traffic. But what good is the very best SD-WAN solution paired with cloud security if this new SASE-ready WAN edge doesn't perform? What if it slows down business processes, impacts user productivity, or in a worst-case scenario drives users to exploit workarounds to get the speed and experience they demand? And even worse, what if this cloud security approach then fails to adequately protect valuable data, achieve compliance objectives, or guard against threats?

Performance, coverage, and connectedness matter. The right support for SD-WAN is a security private cloud that can apply Zero Trust Network Access to data and resources, provide seamless and direct access to public clouds, provide protection for private applications, and simplify IT operations overall. Forward-thinking organizations have already cast aside the idea that SD-WAN alone makes them ready for SASE, or that SD-WAN with security bolted-on will be sufficient. The right SD-WAN isn't some hastily assembled combination of networking smarts with security parts, it's a robust, best-of-breed combination of SD-WAN with a cloud-native security stack.

Critical Questions to Ask:

- ☐ What are the key security considerations as I look to adopt SD-WAN?
- ☐ How can I avoid duplicating my security stack at every branch and leverage the cloud?
- ☐ Is your solution flexible, so I can integrate between best-of-breed solutions?
- ☐ When outside the branch, how can I provide fast, secure remote access to my users?

Understand Why Peering Matters

Let's talk about peering. Network peering is when one internet network connects to another directly, enabling a faster throughput and better exchange of information. In successful peering, no additional charges are incurred and no third-party network is required. The modern network should peer with leading cloud infrastructure providers such as Microsoft and Google in every data center. This is a critical, but sometimes-overlooked aspect of coverage. Vendors might like to talk about the extent of their "peering relationships," but caveat emptor when it comes to so much of the marketing that occurs in this regard: peering in one city only benefits users connecting to the data center in that city.

Interconnections that are critical to delivering a truly world-class service, especially without making performance trade-offs. Delivering the lowest possible latency–typically measured in single-digit milliseconds–that translates to the highest throughput, is what's meant by cloud security that can do what it needs to without network performance trade-offs.

Critical Questions to Ask:

- ☐ How can I ensure a good user experience for web, cloud, and SaaS traffic?
- ☐ What can be done to reduce costly private connections, like Microsoft Express Route?
- ☐ What is your peering and interconnection strategy to ensure the best performance?
- ☐ Do you partner with the cloud and SaaS providers my business depends on?

Critical Questions to Ask:

- ☐ What can be done to lower TCO and accelerate ROI on my IT investments?
- ☐ How does your solution aid my organization in its digital transformation journey?
- ☐ How can my firm become more agile, cut costs, and gain business efficiencies?
- ☐ What is the best approach to SASE that supports security and network convergence?

Create More Effective Cross-Functional Teams

Believe it or not, enterprise technology planning can be terribly short-sighted, especially if it focuses only on the "T" in "people, processes, and technology." Team dynamics are important, and the success of a SASE architecture depends on how well networking and security teams, and the products and services they manage, converge into a shared set of priorities tied to business objectives.

This isn't easy. But more than 50% of CIOs today believe that a lack of collaboration between these teams stops organizations from realizing the benefits of digital transformation. It isn't just better team relations, either; with an estimated $6.8T to be spent on digital transformation projects through 2023, the absence of collaboration starts to cost teams real money when projects stall, budget line items go wasted, and infrastructure gets more complicated. Your network won't be your security if you have separate networking and security teams mis-aligned on objectives and key results.

At Netskope we're focused on delivering world-class security, without trade-offs. Our industry-leading fast, low latency on-ramps to NewEdge deliver a superior user experience and world-class app performance. Discover the typical network performance you can expect from the Netskope Security Cloud and find out how we compare to the competition.

netskope

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything, visit netskope.com.