ZTEdge™
By Ericom Software

The Cloud Area Network Reinvents LANs for an All-Local World

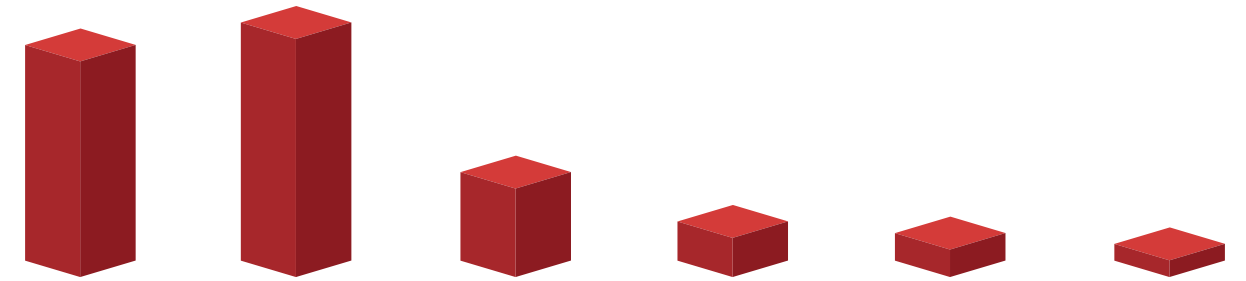
Contents

Today, "Access" Means "Cloud"

Today, more than two years into the sudden acceleration of rapid digital transformation triggered by the COVID pandemic, networking advancements have leapfrogged over connectivity models that seemed cutting-edge just a short while ago. The secure access service edge (SASE) capabilities at the heart of that model, such as zero trust network access (ZTNA) and isolation-powered secure web gateways (SWGs), are increasingly being adopted. And in a decidedly positive step, numerous access scenarios, such as connecting users from within or outside traditional office environments to applications and resources located within private datacenters or increasingly, the public cloud are now being provided by a single cloud-delivered platform. This represents a huge step forward.

Enterprise SASE Adoption Status, 2021

ESG 2021 SASE Trends



37%	41%	14%	5%	3%	1%
We've begun to implement SASE	We're actively planning for SASE and will start implementing over the next 12-24 months	We're planning to implement SASE, but do not have a timeframe	We're interested but would have to learn more	We have no current plans for SASE	Don't know

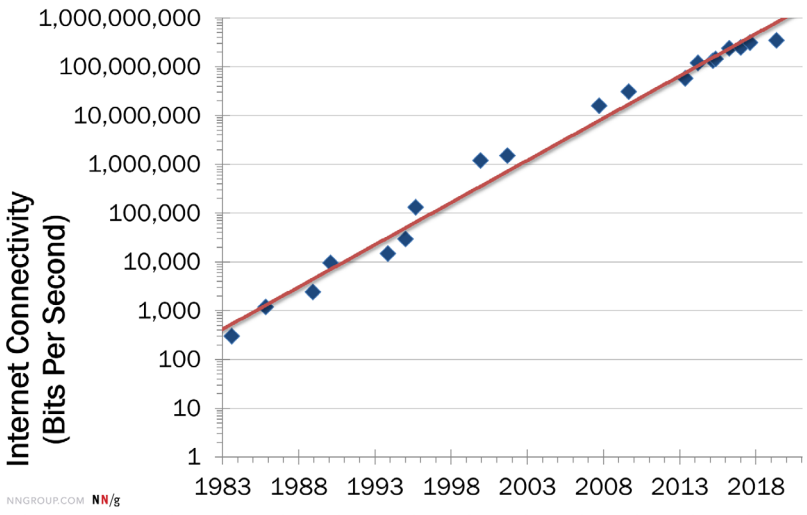
Can We Get Simpler than SASE?

But what if everyone-and-everything access to everyone and everything else could be simplified further? What if a single modality could provide that access in keeping with zero trust security principles, with no need for a menu of connectivity options? And what if all users – employees, 3rd party contractors and gig workers – could get to the connections, resources and apps that they needed and were authorized to use, securely and without increasing risk of cyberattack or data loss? In short, what if we could consolidate WAN Edge Services, the connectivity side of SASE platforms, in a single simple solution that would enable granular, efficient, policy-controlled connections between users, devices, endpoints and apps?

Imagine a vast, cloud-age version of the good old reliable LAN, upgraded for our perimeter-less age. The cloud, along with internet access, serves to make every location local. Rather than physical switches, policies could be used to enable each user, anywhere, to simply and securely access any data center servers they're authorized to use and to prevent unauthorized users from doing the same. Access to cloud services, corporate apps and websites, and to other users could be provided in the same way. Needless to say, users could connect via any device that organization policies permit for that user.

The steady move to the cloud kicked off by AWS a decade ago has turned into a flood. Available bandwidth has been growing by 50% annually, making cloud access less costly than ever before and in most cases, instantaneous. The shortage of networking and cybersecurity professionals is further accelerating the move to the cloud, as organizations seek solutions that are simple to deploy and operate remotely, and eliminate the need for on-premises equipment.

Two factors, however, are still keeping organizational networking somewhat earthbound. The first is that users in headquarters and branch locations still need fast, reliable access to data and apps in on-premises corporate data centers. And of course, cybersecurity is the second.

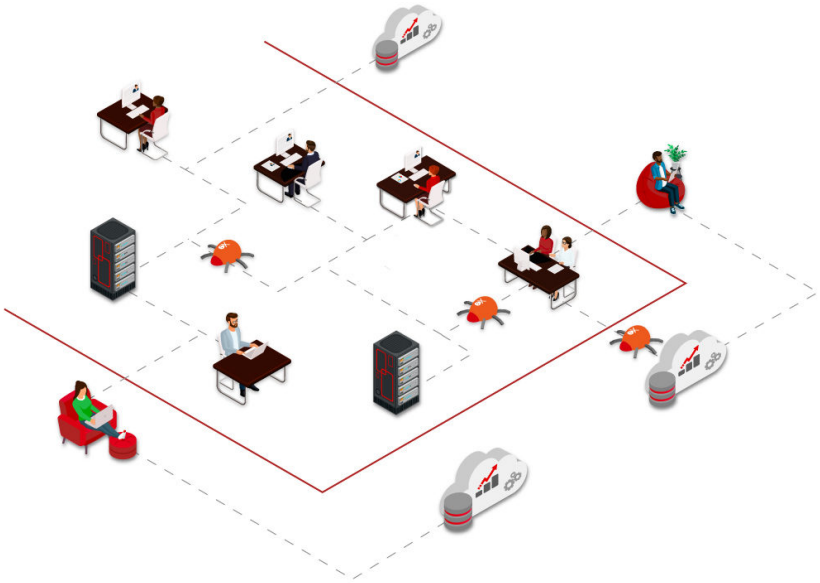


Nielsen's Law of Internet Bandwidth

Imagine a vast, cloud-age version of the good old reliable LAN, upgraded for our perimeter-less age. The cloud, along with internet access, serves to make every location local. Rather than physical switches, policies could be used to enable each user, anywhere, to simply and securely access any data center servers they're authorized to use and to prevent unauthorized users from doing the same.

Magical (Networking) History Tour

The traditional wide area network (WAN), which has long been essential for distributed organizations, is way more costly than today's public internet, yet often not much more reliable. With bandwidth plentiful, costly multiprotocol label switching (MPLS) circuits are no longer required to ensure the quality of service (QoS) that organizations need.



WANs are also problematic in that they cannot secure all types of access that today's organizations require. Because the internet and SaaS apps are perhaps the most essential tools of virtually every organization, secure internet access from branch offices is indispensable – yet not natively provided by WANs. To secure web access, organizations can opt to have branch office users bypass centralized cybersecurity stacks and directly access the websites they need with only minimal antivirus inspection to protect them from cyber risks. Or they can backhaul internet traffic via WAN MPLS circuits to the secure web gateways, firewalls and other on-premises cybersecurity solutions at the main data center for centralized scanning – a costly process that adds latency to each interaction. In essence, for internet access, WANs force organizations into a devil's choice between risk and inefficiency.

Today's bandwidth abundance has tipped the scales toward organizations leveraging internet protocol security (IPsec) encryption and tunneling technologies to create private networks over the public internet. Instead of depending on service level agreements (SLAs) to ensure that bandwidth and speeds are sufficient for their needs, they rely on redundant connections via multiple internet service providers (ISPs) and employ bandwidth controls to prioritize app traffic.

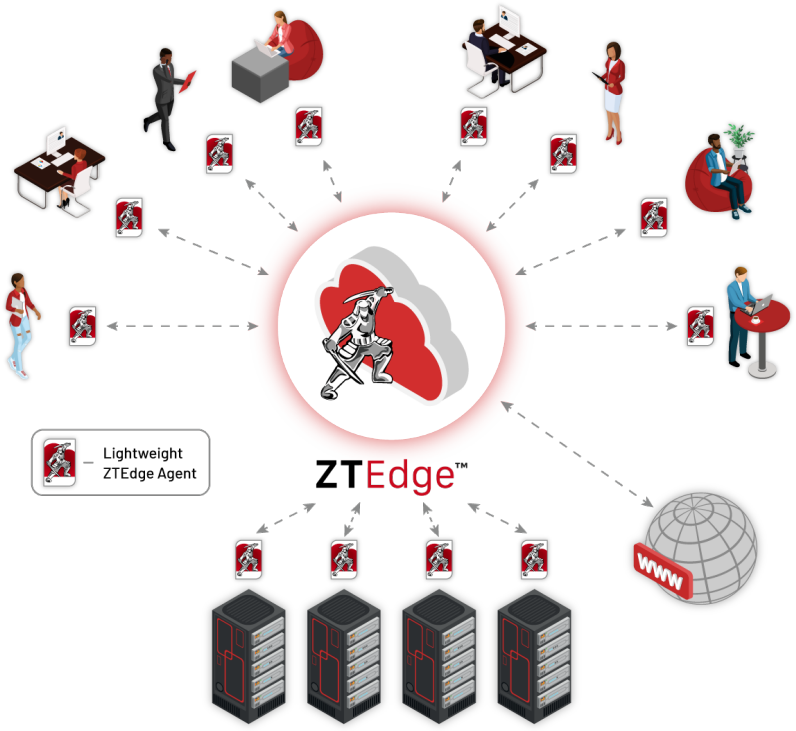
These internet-based, software-defined WANs (SD-WANs) require routers to be installed at the corporate office as well as at each branch. Routers often integrate web cybersecurity tools, including remote browser isolation, SWGs and firewalls, enabling secure internet access direct from branch offices, and increasingly, are software-based. Compared to traditional WANs, SD-WANs are much less costly and enable greater cybersecurity, particularly for internet and cloud use.

The Internet is Your New Corporate Network

Once we move to SD-WANs that operate over the public internet, with only software-based routers required at branch offices, a reasonable (and obvious) next question becomes, "Can we get better service with less redundancy? Less complexity? Fewer restrictions? And at lower cost?" With private cloud infrastructure capacity increasing rapidly and costs falling, it's worth considering whether swapping in "private cloud backbone" network infrastructure available from some internet-as-a-service (IaaS) providers instead of redundant public internet services would allow organizations to respond to all the above questions with a confident "Yes."

> Can we get better service with less redundancy? Less complexity? Fewer restrictions? And at lower cost?

Conceptually, replacing SD-WANs that use the public internet with cloud-based networks that primarily leverage private global backbones as "cloud overlay mesh networks" would create a next-generation form of networking. What would it look like?



Because this new type of network is delivered in the cloud, cybersecurity could be baked directly in. Functions such as policy-based controls, malware scanning and data loss prevention (DLP) checks would be applied en route in real time, removing the traditional divide between networking connectivity and cybersecurity.

In this new type of Cloud Area Network, every person or device would represent an individual node, with its own permanent, location-agnostic IP address. Each node could connect directly to every other IT resource via a mesh security fabric of secure tunnels, restricted only by relevant authorization policies. A small lightweight software agent would connect each device or node to the network, functioning, in effect, as a modern-day version of the Ethernet cables that connect laptops, printers and servers to LAN routers. With this approach, only "last mile" connectivity, from where the private backbone ends to the location of the user device, would need to be through private secure tunnels on the public internet.

Because this new type of network is delivered in the cloud, cybersecurity could be baked directly in. Functions such as policy-based controls, malware scanning and data loss prevention (DLP) checks would be applied en route in real time, removing the traditional divide between networking connectivity and cybersecurity.

Of course, technology vendors will have to make this transition simple and affordable for enterprises. Imagine a new breed of managed service networking providers who leverage a globally available multitenant platform to create multiple instances of overlay networks – that is, multiple virtual LANs. Each customer organization could have its own private network, including the access and cybersecurity policies it requires, provided as a customized, no-hassle and cost-effective service.

Conclusion

The long-touted move to a native cloud world is in high gear. The technology is ripe, and bandwidth is abundant. Now, the network – both connectivity and cybersecurity – just needs to catch up. When it does, we'll see that all networks can be both private and local.

See for yourself how ZTEdge Web Isolation can protect your organization from ransomware, phishing and other web-based attacks.

Contact us now

www.zerotrustedge.com
info@zerotrustedge.com
US: (201) 767-2210
Europe: +44 (0) 1905 777970
ROW: +972-2-591-1700