Inside Out and Upside Down

Redefining What the WAN Is In The Age of Hybrid Multicloud and the Remote Workforce

John Burke

Principal Research Analyst and CIO

Nemertes Research

Q4 2020

Table of Contents

Inside Out and Upside Down 1

Executive Summary 3

COVID-19 Has Exposed A Flaw In Our Understanding Of The WAN 4

What the WAN Isn't, Anymore 5

What the WAN Now Is 5

The New Backbone 6

SD-WAN: from Anywhere, to Anywhere 6

Cloud Access Security Broker and Beyond 7

WAN-Cloud Exchanges and Direct Cloud Connects 8

Spectrum of Options, DIY to Fully Managed 9

Pros and Cons 9

Recommendations 10

Executive Summary

COVID-19 has only accelerated a definitive shift in WAN traffic that was already well under way. Even before the pandemic, the majority of WAN traffic was coming from or going to the Internet. Work from Home (WFH) has only deepened and accelerated that shift.

As this paradigm shift becomes more pronounced, the WAN must be understood differently, because it no longer means what we always thought it meant: "the network connecting my users in my company sites to my data centers." Today's WANs take on a new definition as the locus of enterprise control over every type of access--no matter its starting place or ending place. While the modern WAN certainly encompasses the traditional use cases of connecting the data center, it also fully embraces other use cases for today's multi-cloud businesses:

- connecting and optimizing performance for on-premise staff using resources in external clouds;
- connecting users off premises (especially at home) to resources in both private and public clouds (and to each other, for that matter); and
- connecting resources in one cloud to resources in other clouds e.g. for application integrations.

Beyond just redefining WAN behavior, the cloud is altering the WAN fundamentally. SD-WAN (including in home office and mobile deployments), Cloud-Access Security Brokers (CASBs), cloud exchanges and secure cloud access technologies form the new technological backbone of the WAN, and shift the center of gravity technologically from on-premises networking to cloud- and managed-services offerings. This pivot reflects the realities of handling fully distributed access scalably, seamlessly, and with the best performance when resources could be anywhere, not just in the data center. The new WAN backbone is critical to sustaining success in the hybrid multicloud and WFH world.

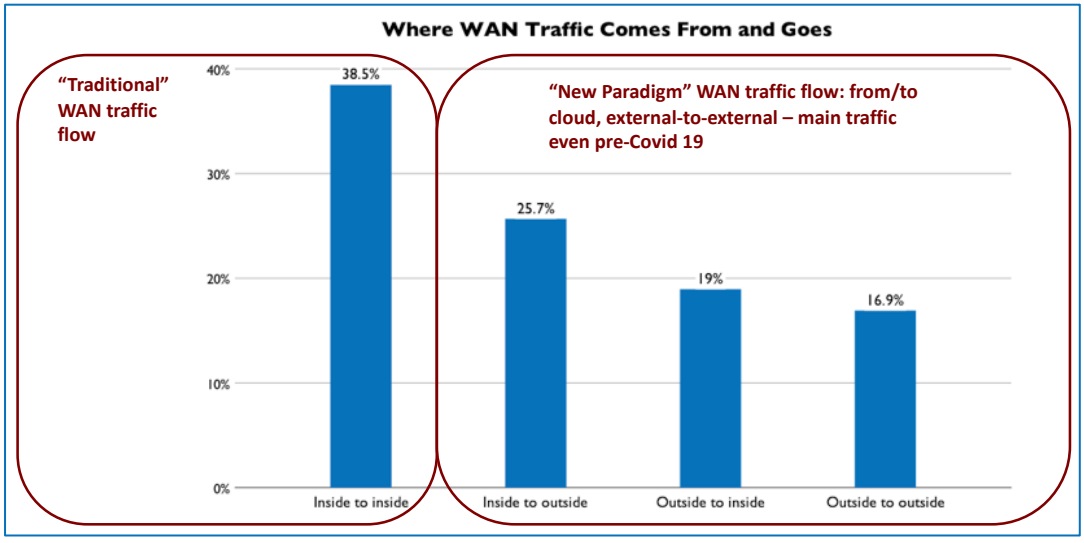
IT professionals should:

- Review WAN strategies and roadmaps to root out plans and policies built on the false assumption that the WAN is for connecting inside users to inside resources;
- Evaluate SD-WAN solutions, from several places along the spectrum, from fully DIY to fully managed, to find the core of their new WAN;
- With SD-WAN integration in their roadmap, evaluate CASB options;
- Ensure that network, application, and security teams are engaged in evaluating CASB and SD-WAN solutions, including their ability to provide or integrate with firewall functionality, on premises or via cloud services;
- Explore the available complementary solutions for connecting to and among clouds, including DCCs, WAN-CXes, and cloud networks.

COVID-19 Has Exposed A Flaw In Our Understanding Of The WAN

When the WAN was invented, it had a single and clear purpose: connecting the different sites of an organization to each other. However, since the widespread embrace of the Internet for business in the 2000s, the corporate WAN has had to accommodate traffic ultimately bound for, or starting from, places outside the enterprise itself. IT teams at the core still think of the WAN as "inside" though, and use cases touching the outside are an add-on to the prime use case.

Over time, the balance has shifted, driven largely by the embrace of SaaS and IaaS. When Nemertes began collecting data on cloud use in 2009, just 2% of organizations were using IaaS, with 42% using SaaS. Only a few percent of the overall IT portfolio was running on external clouds. A decade later, Nemertes Cloud and Cybersecurity 2019-2020 Research Study found the average company for the first time running the *majority* of its IT work in external clouds; only 40% remained in the data centers.



In light of that shift, it makes sense that just 38.5% of the average WAN's traffic was running "inside to inside" in the month immediately pre-COVID-19. The subsequent massive shift to work-from-home has accelerated this realignment, cratering inside-to-inside traffic and driving massive growth in outside-to-inside and outside-to-outside.

The fall back post-COVID will not be to the *status quo ante,* though. The new equilibrium will leave inside-to-inside lower than it was as many initially temporary WFH arrangements are made permanent, and because the shift to WFH has been broadening and accelerating the shift of work to the cloud, as well.

> The fundamental change in WAN thinking has to be giving up any connection to the physical incarnation of the enterprise.

Layer onto this human-centered shift some other critical aspects of enterprise wide-area networking: cloud-to-cloud traffic, DC-to-cloud traffic, and traffic originating not with people but with things—sensors, controllers, drones, etc. The spread of workloads among clouds is complicated by the integration of workloads across clouds: workloads in IaaS environments cooperating with those running in data centers or in other clouds, for example, or integrating SaaS platforms with other SaaS applications, or apps in IaaS or a data center. Further, the WAN has to ensure both good performance and resilient security for systems increasingly entrusted with control of the physical environment. The explosion of IoT systems for monitoring and controlling manufacturing plants, logistics facilities, and offices, or for powering autonomous vehicles in a corporate fleet, can all exert enormous pressure on enterprise networking. IoT endpoints *en masse* generate floods of traffic to monitoring and control systems in distant data centers and, more often, clouds.

What the WAN Isn't, Anymore

With the majority of the WAN's job now and in the future being to convey and secure traffic starting or ending outside the enterprise's physical boundaries, it's time to acknowledge that when we say "WAN" we no longer mean what we used to. The WAN isn't the network that connects users in corporate sites to resources in corporate data centers, since that is only a (thinning) slice of what it does now.

So, what *should* the new enterprise understanding of WAN be, to take the place of "sites-to-datacenters" in IT minds?

The fundamental change in WAN thinking has to be giving up any connection to the physical incarnation of the enterprise. The WAN may serve an enterprise's sites—if there are any—but that can no longer be all it does, so it cannot define what a WAN is.

What the WAN Now Is

Enterprises have gradually eroded their borders by moving work out of data centers and into clouds, and users out of company sites and into home offices and travel spaces. They have interpenetrated their own systems with those of partners, customers, suppliers, and service partners

In this enlarged context, enterprises need a broader mission definition for the WAN. They need the WAN to:

- secure and optimize the network from anywhere, company site or not, to any company resource, on premises or not (encompassing the roles of traditional WAN and VPN);
- secure network usage, taking on functions of firewalls, secure web gateways, IDS, IPS, and more;
- secure cloud resource usage.

In sum, they need to reimagine the WAN as "the network we control that connects things we care about that are not co-located." What defines and limits the scope of the WAN is control over what traffic goes where, including that coming from sources outside enterprise

control, and heading out to same, a security perimeter wrapping and filtering communications amongst widely distributed entities.

Thus the WAN encompasses the traditional job of delivering, controlling, and optimizing traffic flowing from "inside" sources to "inside" destinations. But, it is equally focused on connecting to destinations in external clouds, and in connecting up sources "outside" the enterprise's walls to destinations inside or outside. "Sources" is not users, not people, and covers connectivity for IoT use cases, as well as workloads running in one cloud (public or private) seeking to communicate with workloads running in some other cloud.

The New Backbone

A WAN uncoupled from physical sites still needs some kind of infrastructure. In the next generation WAN this means mainly virtualized infrastructure running on generic silicon. That is, the new WAN looks more like the data center or a cloud environment, at an infrastructure level, and can be provisioned with heavy emphasis on cloud for infrastructure.

The key technologies are:

- SD-WAN
- CASB
- Physical and virtual direct cloud connects

The key technologies are SD-WAN, for the optimized connectivity; Cloud Access Security Brokers (CASBs), for control and policy enforcement; and cloud networking for interconnecting back-end transactions, direct cloud connects both physical and, via a WAN-cloud exchange, virtual.

SD-WAN: from Anywhere, to Anywhere

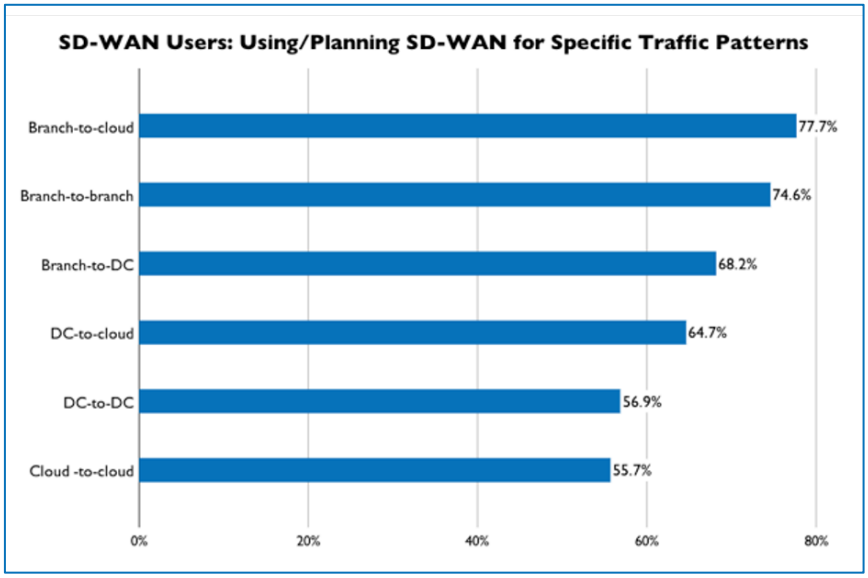
Software-defined WAN is the core of the new enterprise WAN. Its centralized, policy-driven management allows application-, location-, and sometimes device- and user-sensitive control over how traffic is allowed to flow. It can control flows among endpoints both physical and virtual, wherever located, including, increasingly, home offices, as pandemic-driven work from home morphs into a more permanent relocation of workers. SD-WAN also controls where and how traffic heads to or enters from the Internet, a key capability for optimizing the performance of SaaS applications and other cloud resources.

Bringing all those pathways under the same policy control mechanism eliminates the challenge of getting policy consistent across them all.

We see nearly two-thirds of companies (61.7%) having begun their deployments of SD-WAN. Another 14% plan to begin deploying before the end of 2021. In mid-pandemic interviews, some organizations have accelerated deployments while shifting attention to work-from-home installations;

others have slowed roll-outs, as they figure out how many locations will still be in use post-pandemic, and which and how many staff will still be using them.

One key change in enterprise use of SD-WAN in the last few years has been the expansion beyond SD-WAN's original use cases (connecting branches to each other, or the data center, or the Internet). Enterprises now use SD-WAN in multiple back-end-focused scenarios as well: connecting data center to data center, data center to cloud, and cloud to cloud. A majority now use SD-WAN in those scenarios, or plan to within the next 18 months.



Bringing all those pathways under the same policy control mechanism eliminates the challenge of getting policy consistent across them all.

Cloud Access Security Broker and Beyond

Wrapped around enterprise users as they reach out for cloud resources, CASBs do two things central to the reimagined WAN: they manage access authorizations across clouds, and provide visibility into staff use of cloud-based systems, illuminating blind spots created by workloads migrating to SaaS and IaaS. Some CASBs also provide user authentication in the form of Single Sign-On (SSO) as a service, others simply integrate with available SSO services. CASBs are a key element of the new WAN, rounding out the capabilities needed to control traffic.

Combined with an SD-WAN and on-premises and/or cloud-based firewalling, and applied to on-premises workloads as well as cloud ones, CASBs begin to function like a Software-Defined Perimeter (SDP). SD-WAN plus CASB allows an enterprise to create a highly granular "trust map" controlling what kinds of network traffic flows are allowed, based on the identities of the entities communicating (whether human, software, or hardware). An SDP is a zero-trust architecture, meaning that if traffic is not specifically sanctioned by that trust map it is not allowed to flow: a network entity with an SDP around it will only be sent traffic

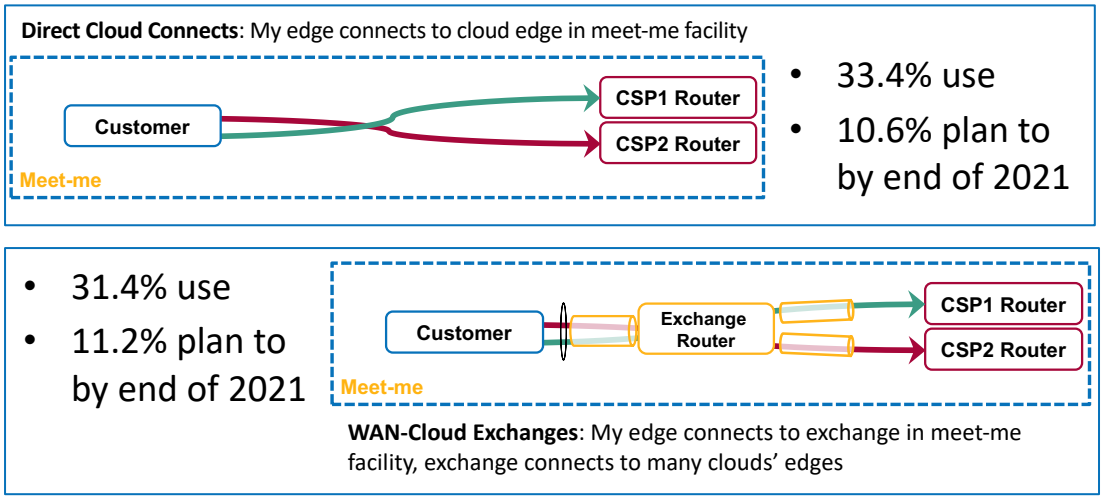
it is supposed to see. Enterprise security is moving towards zero-trust broadly: already, 34% of organizations have begun deploying a zero-trust security architecture, and another 35% plan to begin by the end of 2020, though it will be a multi-year effort in almost all cases.

> A Software Defined Perimeter is a zero-trust architecture: if traffic is not green-lit by a trust map, it is blocked. An entity wrapped in an SDP will only be sent traffic it is supposed to see.

WAN-Cloud Exchanges and Direct Cloud Connects

One function of an SD-WAN is to optimize performance for applications, and a big and growing piece of that is to manage the egress and ingress of Internet- and especially cloud-bound traffic. Two technologies enterprises deploy more frequently in a next-generation WAN bypass the Internet for some flavors of cloud access: physical direct cloud connects (DCC), and WAN-Cloud exchanges (WAN-CX).

A DCC connects the enterprise WAN directly to the cloud service provider's network in a place where both have infrastructure (a "meet-me" facility). It is a high-capacity link and provides the absolute maximum in performance, minimizing latency, loss, and jitter, all of which are very deleterious to application performance when the application is dispersed across clouds. A WAN-CX connects the WAN to an exchange service, which is in turn connected directly to multiple cloud service providers, allowing enterprises to spin up virtual DCCs to any of those providers. Performance is almost that of a DCC, but an enterprise can spin up virtual links more quickly and easily, at any bandwidth needed.



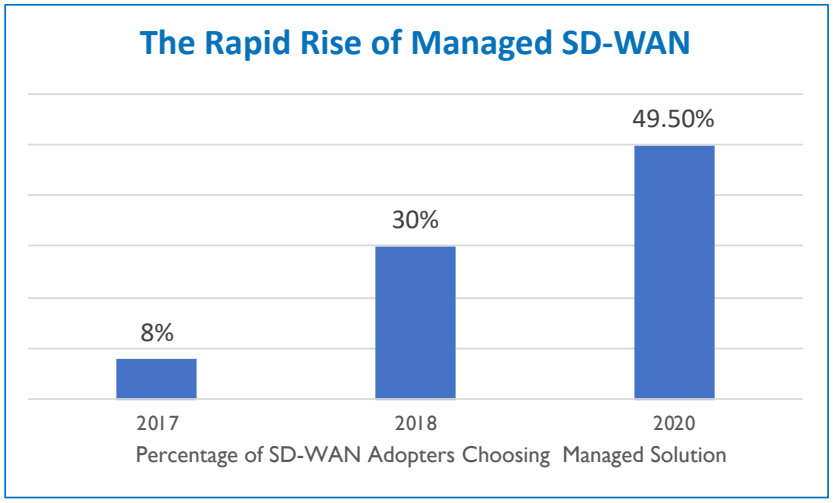
DCCs and WAN-CXes expand the SD-WAN's range of options for application traffic paths by adding ultra-low-latency and -loss options. The SD-WAN can then evaluate which path is going to give the best performance for a given packet stream and choose accordingly. It may route all traffic generated in a data center and heading to AWS out through the DCC or

WAN-CX serving AWS, for example, but send a remote branch office's AWS-bound traffic through the Internet instead, if Amazon's on-ramp is closer and performing well enough.

Spectrum of Options, DIY to Fully Managed

Enterprises have a full range of options in deploying SD-WAN, from complete do-it-yourself overlay networks (DIY) to co-managed to fully-managed, network-based options.

In the DIY model, the enterprise buys or leases, installs, and manages the endpoints (physical and/or virtual) that comprise the SD-WAN's infrastructure. At the other end of the spectrum, in the fully managed, in-net model, the service provider installs and manages any needed endpoints, and provides some or most SD-WAN functionality using its own service cloud. In between are an enormous number of variations, from cloud-based consoles on otherwise DIY solutions to enterprise co-management of an otherwise fully managed in-network solution.



Nemertes' data shows a dramatic and rapid shift toward enterprise embrace of managed options. In Nemertes' 2017-2018 study, just 8% of organizations chose a managed offering; in the 2018-2019 study, 30% did. In the 2020-2021 study, 49.5% of enterprises chose a managed solution.

Pros and Cons

Benefits and risks come with whatever choice IT makes.

DIY solutions are the most mature, technologically, and enjoy the broadest adoption. IT controls everything about the rollout, the mix and providers of connectivity options at each site, and the configurations and upgrade schedules. However, complete control equals complete responsibility, and IT has to rely on its own resources to roll out, manage, and troubleshoot, upgrade, and eventually refresh the tool. IT also has to manage the portfolio of connectivity providers, which can grow very large in a WAN of any size. Each provider added incurs real costs for both engineering and administrative management.

With managed solutions, the main trade-offs are on cost and control. The enterprise can rely on provider expertise and staff for deployment, operation, and troubleshooting. This is a significant burden offloaded: on average, enterprises devote about 17% of their network staff's time to WAN management, roughly four full-time staff out of an IT department of 100. But, the enterprise necessarily loses some control of how and when things get done.

Any good managed service provider seeks to deliver predictable and appropriately responsive services, but the meaning of "appropriate" is context sensitive, and negotiated response times may not be context-aware. And, an enterprise typically can't control which staff serve it, and often sees skilled staff rotated off to other jobs, replaced by less-skilled colleagues. And, some providers with their own network services portfolio limit enterprises to specific connectivity options, while others embrace a flexible, "BYO networks" approach.

Co-managed solutions provide a middle ground (like cloud-managed DIY solutions). IT teams can retain some degree of access and control, ranging from handling most day-to-day operations with the provider as a backstop to reserving the right to jump in to make emergency adjustments (in the event of a malware outbreak, for example) but otherwise staying hands-off. Co-management allows the enterprise to drive knowledge transfer and so develop expertise of its own as a hedge against staff rotation or slow response to emergencies. But, of course, it requires an ongoing commitment to staffing for WAN management instead of completely outsourcing it.

Recommendations

Even before COVID-19, the legacy WAN was no more; COVID-driven WFH has just pushed the old picture we had of it in our heads even further away from current reality. IT leadership needs to let go of that old mental model of the WAN to embrace the new paradigm: the WAN is a locus of control, the network for connecting enterprise users and resources that are not all in the same place.

With that in mind, SD-WAN is the logical organizing concept and technology for what replaces that old model, and along with complementary solutions like direct cloud connects and cloud exchanges and CASBs, it forms the core of the next generation WAN.

IT professionals should:

- Review WAN strategies and roadmaps to root out plans and policies built on the false assumption that the WAN is for connecting inside users to inside resources;
- Evaluate SD-WAN solutions, from several places along the spectrum, from fully DIY to fully managed, to find the core of their new WAN;
- With SD-WAN integration in their roadmap, evaluate CASB options;
- Ensure that network, application, and security teams are engaged in evaluating CASB and SD-WAN solutions, including their ability to provide or integrate with firewall functionality, on premises or via cloud services;
- Explore the available complementary solutions for connecting to and among clouds, including DCCs, WAN-CXes, and cloud networks.