Nemertes

Better data. Better decisions.

# The Intelligent Interconnect

The Case for AI in SD-WAN

**February 2022**

**By John Burke, CTO**

**Nemertes**

# Table of Contents

## The Issue: The WAN is Exploding

In what seems like the deep past, and what was surely another world, the WAN was a simple thing to understand (even if it was not always simple to implement): The WAN was the network that connected a company's locations to each other. Employees working from company computers in company offices used the WAN to reach company resources in a few company data centers.

Of course, the revolutions in mobility, cloud, and remote work have upended pretty much every assumption underlying that description. Even before the pandemic, more than 54% of the average enterprise's workloads were running in a cloud of some sort, and only 37% of WAN traffic was fitting that classic model of connecting internal sources to internal destinations. In the wake of COVID-19, even more work has shifted to clouds, and even less traffic is inside-to-inside.

So, far from the classic model of inside users on inside systems reaching inside resources, the modern enterprise has users anywhere, working from anything, to reach services that can be anywhere. The number of service providers involved is steadily increasing. The pace of change in who is using what and from where is also increasing.

In this context, the WAN has to be redefined: The WAN is the network the company controls that interconnects things not in the same geographic location. The WAN is not a thing, but a locus of control—the physical and logical networks as well as the network services over which the enterprise can exert control. The WAN provides the enterprise with both visibility into and control over what traffic passes among resources and users in different places in the same way LANs and data center networks do for resources on premises.

For larger organizations the scale of activities and rate of change in them is growing past the point of robust operation by unaided humans, and even of traditional SD-WAN. Adding AI to the SD-WAN is the logical and necessary next step. AI is what will enable SD-WAN to stay relevant for large and complex environments.

## Steering Clear: AI for traffic routing intelligence and resilience

The primary reason SD-WAN exists is to make it simpler and easier for IT to provide resilient connectivity among locations with best-possible performance. Job 1 for any SD-WAN AI will be to supercharge that functionality by improving traffic routing.

A good SD-WAN will already have been capable of intelligently probing available paths from one location to another, or to a cloud-hosted service, to establish current traffic flow characteristics and watch for degradation of performance or link failure. This is how it knows when to fail traffic over from current to alternate paths.

The more complex the environment, the trickier it will get to make sure user sessions are using the connectivity that will not just keep a connection alive but provide the best user experience. As more sites go to multiple Internet links from different ISPs, the number of possible paths from user to service or user to user will grow, and the problem of selecting the best path will get exponentially harder. Complicating the picture further are differences in application traffic types: at

any given moment, one path may do better delivering lots of small packets and another do better at delivering smaller numbers of larger packets. AI should help address the complexities of finding the best path at any given moment for the traffic users are driving at that moment. The ability to provide machine learning tools with event, user, network, service, and application data, and not just from the WAN but also the LAN and data center networks, will make such tools more effective.

### Forward Looking Statements: AI for Traffic Prediction

AI can take the analysis and direction of traffic to the next level. Beyond monitoring what *has been* happening and what *is* happening now, AI can make SD-WANs predictive—they can base actions on what traffic *will be*. For example, an AI-powered SD-WAN might see a pattern in the Internet "weather" for one provider suggesting it is in the first moments of an oncoming performance crash, and preemptively redirect traffic through alternate routes. Beyond dealing with rerouting traffic in the event of cable cuts or similar wholesale disruptions of service, an intelligent SD-WAN can work with what's available to maintain performance—and therefore user satisfaction—to the fullest extent possible. It may normally not deploy high-overhead traffic conditioning functionality such as forward error correction or packet multipathing, but might proactively switch them on for specific traffic streams not to address what is happening now but in anticipation of an event it sees on the horizon.

## Guardrails and Traffic Cops: AI for Security

A robust SD-WAN is foundational to securing cloud access and enforcing enterprise policies, based on its deep visibility into traffic flows among users and services, the ability to partition traffic arbitrarily into virtual WANs based on a variety of factors, and the ability to reshape those vWANs on the fly. (For this reason, SD-WAN is foundational to most definitions of the SASE—Secure Access Service Edge—market category.)

Given the reaction speed required to spot and shut down bad actors and network-borne contagions in time to limit and mitigate damage, an SD-WAN solution needs intelligence to bolster security functionality. SD-WAN with AI—and ideally seeing data from the rest of the network as well—could ideally understand baseline normal traffic, spot anomalous behaviors, attribute them to specific entities (whether human, hardware, or software) wherever located, alert the SOC and the NOC to issues, and take automated actions in response.

### Intelligent Lack of Trust

Looking beyond SASE and "business as usual" network and security operations, enterprises are beginning to embrace zero-trust thinking. Contrary to what the name implies, a zero-trust architecture strives only to remove all implicit trust from the environment.

At its base, this means no entity gets access to anything else based solely on where it is on the network—there is no trusted "inside" where everything is assumed trustworthy. Instead, the default assumption is that no access will be provided, and only traffic flows that are explicitly sanctioned will be allowed to pass. Anything not sanctioned explicitly is blocked.

Zero-trust thinking goes further than this basic limitation of trust to explicitly sanctioned interactions. It also denies implicit trust over *time*: that is, a zero-trust environment does not assume that an entity that was granted access to a service 5 minutes ago should still have access for the next flow it tries to initiate. Instead, each new attempt to connect is freshly checked against the trust map. A zero-trust architecture seeks to have a unified policy set, a single dynamic trust map that can control access anywhere: into, out of, and among services running within a data center; across campus LANs; and on the WAN.

The intelligent SD-WAN plays two crucial roles here. It can be a policy enforcement point, passing or blocking traffic based on policy. And, it can play an active role in *shaping* the trust map, by providing dynamic feedback on entity behavior in real time. In applying AI techniques to behavioral threat analytics, an intelligent SD-WAN solution helps spot incursions and lateral attacks, and can help shut down lateral movements from successful breaches.

## Smart Hands to Assist: AI for operations

In IT operations, a more intelligent SD-WAN (and really, an AI-assisted network in any domain) could expand its role in hands-on management of network operations, security operations, and service delivery management.

An AI SD-WAN should be able to proactively alert the network operations team earlier in the lifecycle of events that hurt service delivery, based on the ability to spot and flag anomalous behavior, and to engage in predictive analytics. It could even be empowered to make some kinds of mitigating or corrective changes on the fly, like disconnecting sites generating too much anomalous traffic in too short a time, dynamically engaging optimizations to improve performance in the face of increasing demand, or throttling down less important traffic to make more room for critical business functions.

These same capabilities help on the security operations side. An SD-WAN can enforce security policy and push it out to all WAN segments automatically. An *intelligent* SD-WAN can go further, reacting to anomalous or malicious behavior by dynamically reassigning to sandbox and honeypot networks entities behaving badly, for closer scrutiny. Or it could block traffic from them, and the sites they are in, entirely, if the situation warrants it.

AI in SD-WAN can even help in the deployment phase, providing for more robust, secure, and flexible zero-touch provisioning of SD-WAN nodes, for example by alerting on anomalous attempts to connect new sites or services to the system, and tweaking policy definitions based on the behavior of newly added sites.

With intelligence added, an SD-WAN should do more than just throw up a dashboard of performance metrics and report on whether SLAs are being met. It should apply predictive modeling to project future delivery trends and thereby highlight foreseeable problems in the offing and even, ideally, suggest preemptive actions to head them off, such as increasing bandwidth at or adding a redundant link to a given site. It should do all this using data from every part of the organization that can be fed into it.

## Recommendations

Network teams should seek SD-WAN solutions that apply artificial intelligence techniques to the problems of operating and securing high-performing, highly reliable wide-area networks that interconnect all their users and services. An intelligent WAN can play a key role in implementing zero trust, reduce operational costs, and improve service performance and availability.

When replacing a legacy WAN or updating a first-generation SD-WAN deployment, IT professionals should:

- Explore SD-WAN solutions that meaningfully incorporate AI techniques in deployment, configuration, management, monitoring, and security contexts – help day 0, day 1, and day 2 and beyond
- Look for solutions that can use data from other domains (LAN, data center) to further enrich the analysis
- Generate a short list and do proof of concept deployments on at least two solutions
- Evaluate based on improvements to user experience, reductions in management effort, and strengthened security posture
- Integrate AI-driven alerting and automation into NOC operations
- Integrate AI-driven alerting and automation into SOC operations, threat hunting, and threat response, to improve mean time to contain attacks, and reduce the percentage of severe security incidents