



SD-WAN HEADS HOME

Network technology becomes a possible solution in ‘branch of one’ deployments

By *Martin Vilaboy*

Before the pandemic struck, software-defined wide area networking (SD-WAN) was arguably the hottest technology in networking. Adoption was robust, as the technology had past its “peak of expectations” on the Gartner networking hype cycle and was rapidly climbing to its “plateau of productivity.” Then suddenly, when home-based workers were geographically separated from centralized work resources, enterprises looking to connect those remote employees fell back to the more familiar virtual private networks (VPNs) that SD-WAN in many cases had been

replacing. VPN sales returned with a vengeance. According to a recent survey by Cybersecurity Insiders, more than seven in 10 organizations said they had increased their VPN capacity in response to the response to the COVID-19 pandemic.

During the initial rush to go remote, SD-WAN still was positioned as a solution for the branch office and was seen as less cost-effective for individual workers in their homes. But as SD-WAN vendors tweak their offerings, and the cost of on-premises devices come down, an increasingly strong case can be made for utilizing SD-WAN

to connect the “branch of one” remote worker.

Certainly, the benefits SD-WAN-to-the-home provide network administrators are interesting enough. SD-WAN clearly is more flexible, more controllable, and provides a better user experience for today’s workers who must securely access not only internal assets but approved cloud-based resources, as well. As technology analyst John Fruehe describes things, VPNs create a type of session-based tunnel into IT resources. The user initiates a connection that punches in behind the firewall and then disconnects when done. SD-WAN, meanwhile, effectively creates a new network edge that’s always connected and granted access to everything that’s available to workers at the office.

For network administrators and IT departments, specifically, SD-WANs provide a level of control, visibility, and flexibility – in terms



Top VPN Challenges for Remote Access

Lack of visibility into user activity taking place	24%
High cost of security appliances/infrastructure	23%
Requires giving employees and third-parties access to corporate network	19%
Poor user experience due to backhauls to VPN gateways	16%
Complexity of managing existing remote access across public cloud environments	14%
Inability to scale to meet user demand	4%

Source: *Cybersecurity Insiders 2021 survey*

apps including VoIP, collaboration tools, or video conferencing, or prioritizing certain roles or power users, all while deprioritizing or blocking less-important traffic, such as Facebook or YouTube, so as not to constrain company bandwidth and infrastructure. This type of optimization and prioritization is particularly important to remote work, as home users' ISP networks are becoming more congested with more work traffic. And in cases where the home internet service is simply inadequate for work, SD-WAN appliances often can be outfitted with cellular LTE connectivity as an alternate connection. Another benefit over a VPN is that an SD-WAN can route cloud traffic directly to cloud services instead of backhauling the data through a data center.

Ultimately, as explained by Jean-Luc Valente, vice president of product management for Cisco's SD-WAN and edge routing division, SD-WAN appliances in the home means employees' homes can be treated similar to any other

branch office, allowing IT teams to apply policy consistently across various business segments, extend security beyond company-issued devices to the LAN, and enable application-level quality of service.

For the individual users, SD-WAN to the home can be relatively simple and transparent. The zero-touch provisioning of most SD-WAN gateways, explained Fruehe, means IT can send SD-WAN appliances directly to a remote worker for installation, and when plugged in, the device can self-provision and connect back to headquarters with little or no interaction on the employee's end.

"Even VoIP can be configured, enabling calls from the headquarters to route directly to the employee," Fruehe continued.

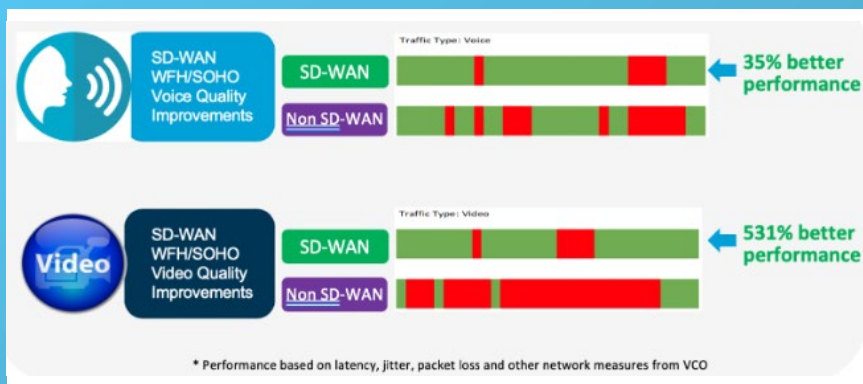
Not that an SD-WAN deployment makes sense across the entire WHF spectrum, at least in the near term. Fruehe suggests companies consider the specific role or duties of the individual home-based employee when deciding where to go with SD-WAN. Those utilizing intensive or expensive applications or who have specific

of security, traffic, and applying policies – that VPNs typically do not. In most cases, VPNs handle most users in the same way and typically route all traffic over the established connection, "so even nonwork traffic ends up running through the headquarters' gateways out to the internet," explained Fruehe. VPNs also do little to mitigate slow, congested, or over-provisioned broadband connections.

"But, with an SD-WAN home office, IT can take a more fine-grained approach to managing users, access, security, and the other aspects of connectivity back to the main headquarters," argued Fruehe.

Even in a home office set-up with a single link, the dynamic optimization capabilities of SD-WAN can adjust and prioritize traffic for a better user experience, such as maintaining quality for bandwidth-sensitive

Quality of Experience Improvements of SD-WAN in WFH Environment



Source: AT&T

licensing requirements, such as people working in CAD design remotely, for example, represent situations where the investment in SD-WAN can be justified. Much the same can be said for those in higher-level or mission-critical roles such as engineers, developers, lawyers, or C-suite occupants that are largely working from home.

On the other hand, employees who live in the world of PowerPoint, email clients, Excel and Word, said Fruehe, can run those applications at home rather inexpensively and can be adequately served by a VPN connection. But as the price points for SD-WAN premises equipment drop below \$1,000, it starts to make sense to look at home-based marketing and HR managers or folks working in finance to see if the improvements wrought by SD-WAN in user experience, connectivity, and security can be justified.

Ben Niernberg, executive vice president at MNJ Technologies, a managed service provider with experience providing SD-WAN solutions to clients, believes this time will come sooner than later. Many OEMs in the space have been working on “branch of one” solutions, he said, and Nierenberg has already seen devices that combine security with some level of routing and switching, if not full SD-WAN capabilities, all for around the same price of set-

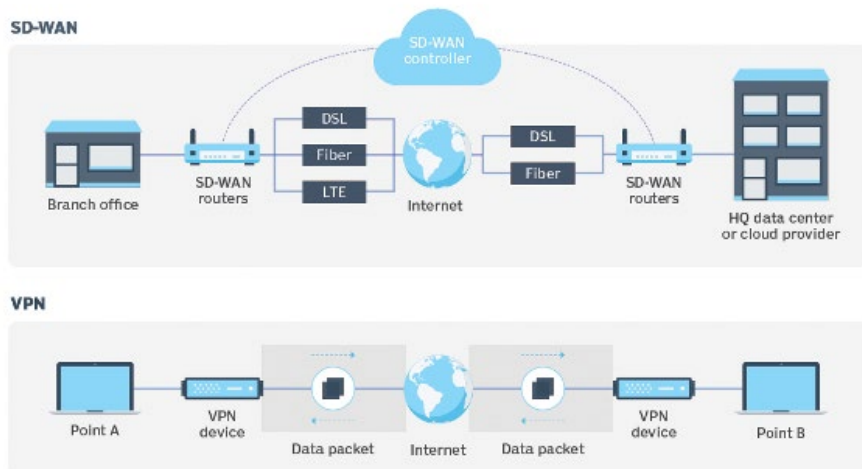
SD-WAN Desired Features

Cloud and SaaS connectivity	35%
WAN optimization acceleration capabilities	32%
Advanced security features SASE	32%
Support for remote and mobile employees	32%
Better alignment with cloud tech operational models	30%
Private connectivity that can replace MPLS	28%
Fully managed service	28%
NFV at branch to replace appliances	26%

Source: Aryaka Networks 2021 survey

SD-WAN vs. VPN

SD-WAN can use multiple types of connectivity. The simpler VPN creates an encrypted tunnel to transmit data.



Source: TechTarget

ting up a remote office with a nice laptop or a PC and monitor.

“If you get your connectivity and security all in a box, where you can protect the company, I think that changes the financial posture of what is and what isn’t acceptable,” said Niernberg, speaking as part of a podcast on SD-WAN and WFH by Frankly MSP.

And even if the cost to connect the at-home workers goes up slightly, “there is probably some savings on the backside, whether it be through real estate or through trying to enable an entire office,” he continued. “I’m not sure that it doesn’t become widespread yet; I think that is where we

are: trying to learn what is that threshold where it makes both financial and business sense.”

SD-WAN to the “branch of one” only make sense if remote work is clearly part of organizations long-term plans and culture. If the idea is that eventually everyone is coming back to the office, even if that is a year or two down the road, advised Fruehe, “you are probably not willing to go down the path of putting all the infrastructure in place.”

Even if a company already is committed to SD-WAN in some capacity in its wide area network, the decision to push it down to home-based workers should be made separately. But if cost and cultural factors align, “SD-WAN makes a lot of sense,” Fruehe continued.

Niernberg suggests on organization starts with an understanding of the key applications or problems it is trying to solve and then consider the possible appliances and solutions that might be able to help.

“Not all SD-WAN is created equal,” he warned. “An [MSP or SD-WAN channel partner] that knows not just one SD-WAN product but multiple SD-WAN products can help you find the right solution and not just the solution they sell.” ♦