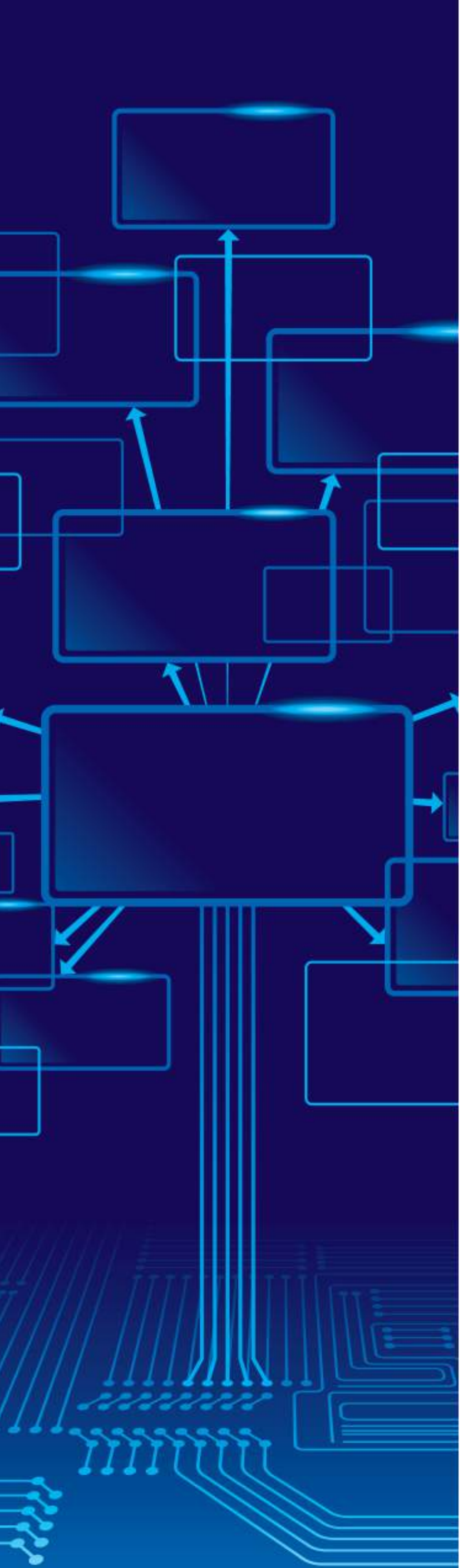


How SD-WAN for Home Offices Supports Remote Work

In this handbook:

How SD-WAN for Home Offices Supports Remote Work

JOHN BURKE, CTO AND RESEARCH ANALYST

Many workers no longer travel to the office five days a week. Instead, a new normal has emerged, where large numbers of staff work remotely every day or every couple days.

That shift has fueled new ways to connect these remote workers to the resources they need. VPNs -- the traditional method to provide corporate access -- are not well suited to enabling such a hybrid environment. In response, companies have expanded their use of cloud-based zero-trust network access (ZTNA) services. Others have turned to software-defined WAN for home offices, directly extending their network edge -- specifically, their SD-WAN edge -- to employee residences.

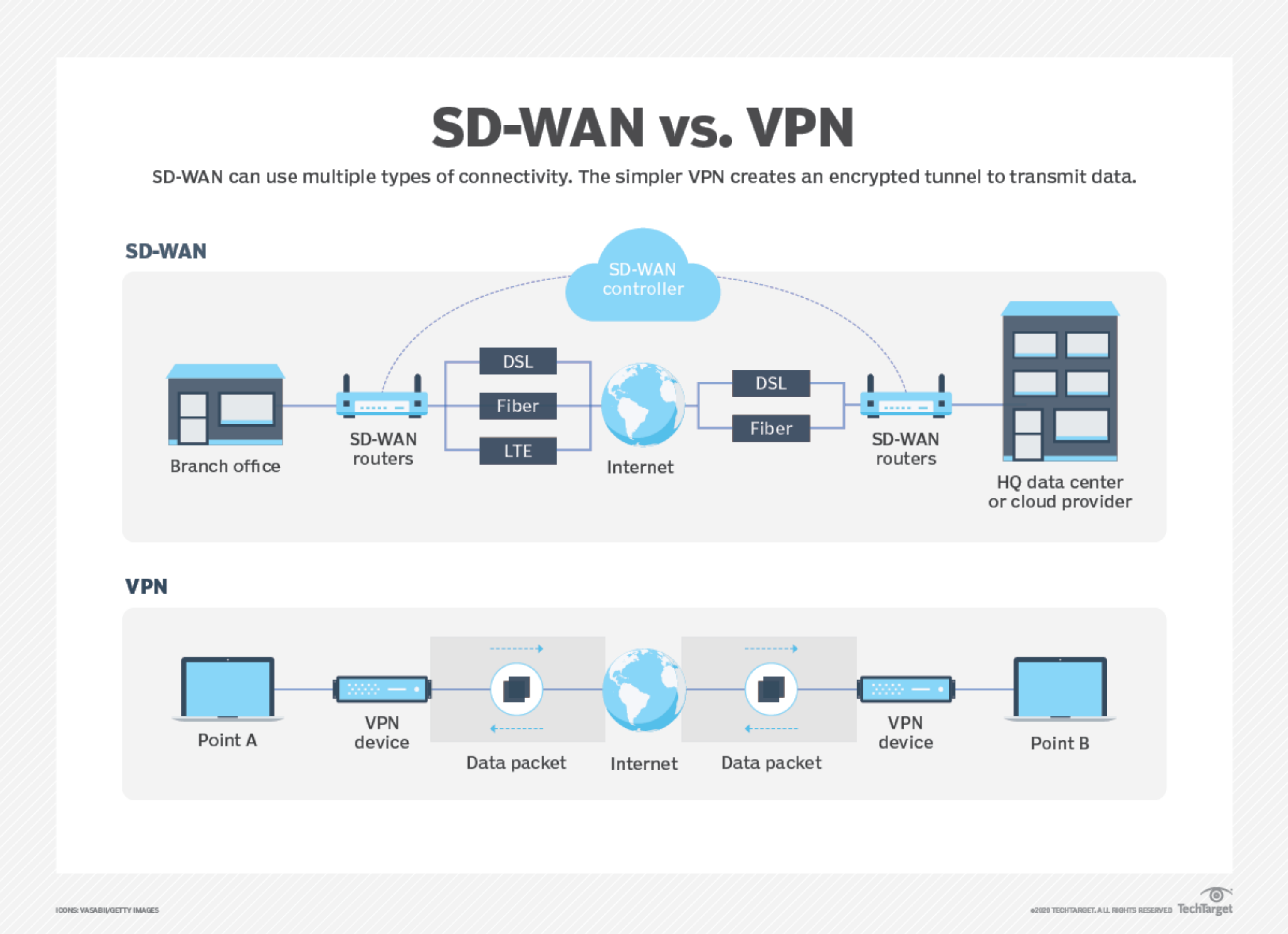
VPNs vs. SD-WAN

In the days before cloud, enterprises used VPNs to give remote workers access to network segments and resources protected by corporate firewalls. VPNs build network tunnels between the remote computer and a VPN head-end device -- called a *VPN concentrator* -- on a segment of the company's network. To some extent, the VPN puts the remote computer on the same network segment, or segments. This enables remote users to reach systems not reachable via the internet directly or to use protocols not allowed to pass through corporate firewalls.

VPNs are a fine option for small numbers of remote users -- primarily travelers and IT support staff -- who only infrequently and briefly need access to corporate resources. But VPNs can be notoriously high maintenance and fragile, as well as expensive when gauging how much it costs to support a user each time a session initiates.

Another conventional option is router-to-router VPNs. Enterprises can use these to support internet-based branch connectivity to corporate networks. A branch router establishes a VPN connection into one or more other locations, and company traffic travels through those tunnels onto the company WAN.

In this handbook:



SD-WAN vs. VPN

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

ICONS: VASABII/GETTY IMAGES

In the 2010s, SD-WAN emerged as a way to improve how branches could use internet connectivity to link to the corporate WAN. SD-WAN centralizes and automates the process of configuring tunnels among branches. It also enables traffic load balancing across multiple connections and bandwidth allocation based on policy. Finally, it supports the free mixing of multiple connection types, such as MPLS, wired internet and cellular data, from multiple providers.

The economics of SD-WAN work well for a branch office with multiple users. But, for the first several years of SD-WAN's existence, it was too expensive for most companies to extend SD-WAN to individual users. Remote access continued to rely on VPNs. Then came the COVID-19 pandemic and the subsequent shift to remote work.

Due to the technology's maturation and market competition, SD-WAN is an intriguing option for connecting remote users to corporate assets. Small-office SD-WAN appliances and soft clients can be a viable alternative for locations where users need access to sensitive or critical systems and data or especially large data files, all day, every day. SD-WAN has the potential to manage these remote users with lower overhead and better reliability and performance than traditional VPNs, even as they support full network-level access, unlike ZTNA gateways.

SD-WAN for home

Residential SD-WAN provides more flexible security than a VPN, making it a better choice for a persistent connection. Also, SD-WAN can route work-related cloud traffic, such as Microsoft 365 or Salesforce traffic, directly to those services over the internet instead of backhauling it through a company data center. It can do the same for nonwork traffic to the internet, which a VPN sends into the company network, preventing that traffic from consuming company resources.

The zero-touch provisioning of most SD-WAN endpoints means IT can send appliances directly to a remote worker for installation. Once plugged in to the internet, such devices can self-provision and connect back to headquarters with little or no interaction on the employee's part.

Does SD-WAN at home make sense for your business?

Enterprises likely don't need to deploy residential SD-WAN devices to all their employees. Pinpoint the users who could benefit from the reliability and security of SD-WAN, and then weigh the

If the company doesn't already have SD-WAN, remote user access is not the use case to drive deployment.

pros and cons of extending the organization's network edge to those remote employees. In the evaluation process, consider these three key questions:

1. **How does the employee work?** Most productivity-type applications, such as word processing, spreadsheets and CRM, don't require an SD-WAN connection. But data-intensive applications that move a lot of data across the network, such as computer-aided design for architects and engineers, can benefit from the better-quality SD-WAN connection.
2. **How much does the employee cost?** It's easier to make the case for pricier connectivity in support of pricier employees, if SD-WAN can enable higher productivity to offset its higher cost.
3. **What is the current state of WAN and remote access?** If the company doesn't already have SD-WAN, remote user access is not the use case to drive deployment. If the company already has a satisfactory work-from-home environment via VPN or ZTNA, why bother with migrating? But, if the VPN infrastructure is strained by work-from-home rules or loads and SD-WAN is already deployed, then extending the SD-WAN edge to key employees or groups might make sense.

Editor's note: *This article was originally written by John Fruehe and expanded by John Burke. It was updated to reflect industry changes.*

John Burke is CTO and principal research analyst with Nemertes Research. With nearly two decades of technology experience, he has worked at all levels of IT, including end-user support specialist, programmer, system administrator, database *specialist, network administrator, network architect and systems architect. His focus areas include AI, cloud, networking, infrastructure, automation and cybersecurity.*

John Fruehe is an independent enterprise technology analyst with more than 25 years of experience. He has specialized in enterprise networking and data center markets with a focus on product marketing.