netskope DELL'ORO GROUP

Got the WAN Backhaul Blues? There's a Better Way to Network!

Excerpts from Dell'Oro Group's whitepaper, "Network Considerations in the Age of Secure Access Service Edge (SASE)."

Traditional Approaches Fail As The Network Perimeter Dissolves

For decades, enterprises favored the hub-and-spoke network topology (Figure 1). The hub—the corporate headquarters and data center—was at the center of the network. The spokes emanating from the central hub were the network's connections to individual branch offices and remote users.

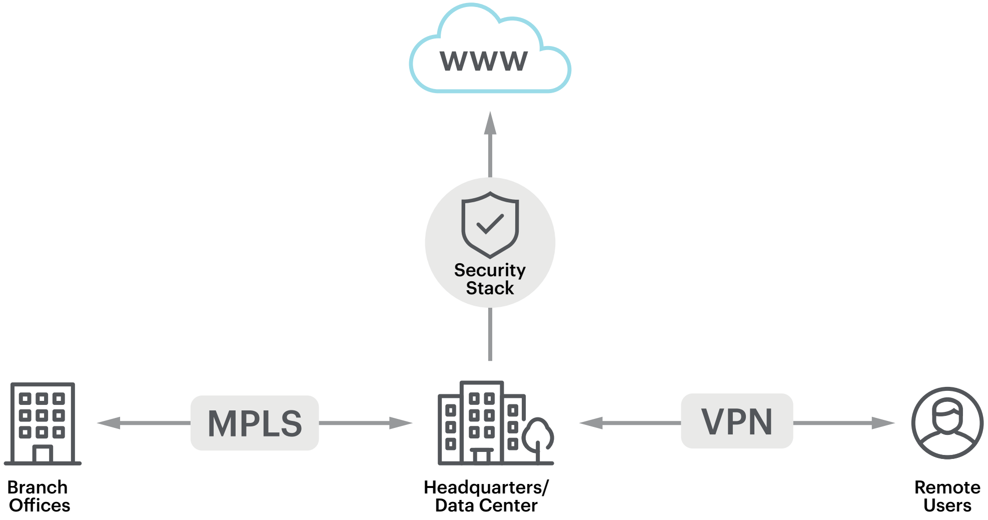

Figure 1: Legacy Network Topology

Historically, enterprises have used WANs to connect geographically dispersed locations to each other, to data centers, and, more recently, to cloud-based services. The preferred network technology for WANs has been multiprotocol layer switching (MPLS) due to its reliability and scalability. However, MPLS commands premium prices and is generally difficult to upgrade or Expand. In the legacy network topology, remote users relied on VPN agents. These were based on internet protocol security (IPsec) or a Secure Sockets Layer (SSL) located on each endpoint to connect over the Internet back to VPN concentrator devices at corporate headquarters.

Legacy WAN And VPN Are Outmoded In The Work From Anywhere Era

As the popularity of Software as a Service (SaaS) applications and highly distributed workforces has grown, so, too, have the limitations of the hub-and-spoke topology. There is a new confluence of cost, application experience, and security problems:

High Cost of MPLS

MPLS spending for branch offices became untenable as network bandwidth requirements increased appreciably in order to service SaaS applications that required significantly more bandwidth.

Poor Application Experience

Application experience suffered because traffic from branch offices or remote users to an Internet-based SaaS application first had to be backhauled to the Internet gateway in the corporate headquarters.

Perimeter Security Circumvention

As Internet-based SaaS apps became popular, some remote users began to skip the enterprise network altogether by using the Internet to go directly to those apps. This created enormous security blind spots. Thus, it became impossible for IT teams to enforce corporate security.

IT Staff Pressure

Many IT teams find themselves lacking the necessary skillset to manage the new cloud- and mobile-centric IT environment, which further amplifies the cost, application, and security problems noted above.

Over the last ten years, new networking technologies, such as software-defined WAN (SD-WAN), and new security technologies, such as cloud-based secure web gateways (SWGs), were developed. They individually addressed the deficiencies of legacy WANs and VPNs. However, they lacked substantive integration.

Why networking and security need to unify

To better understand the needs of enterprises, we interviewed three organizations, two end-users, and a consulting firm, at the forefront of transforming their or their clients' organizations.

- Stuart Walters, Chief Information Officer at BDO UK (United Kingdom), the UK member firm with 6,000 employees. BDO UK is part of the $10 Billion International network of public accounting, tax, consulting, and business firms operating under the BDO name.
- Mark Mahovlich, Vice President of Strategy and Execution at ICM Cyber, a cybersecurity consulting firm headquartered in Jackson, Mississippi with 500 clients across 40 U.S. states.
- A senior cybersecurity executive at a global accounting firm with nearly 400,00 employees who has requested to remain anonymous. This leader is responsible for specifying his company's data-protection strategy across more than 35 global regions.

The unanimous consensus of the group was that legacy architectures are outmoded, inadequate, and overly restrictive. All agreed on the need for a cloud- and mobile-first IT strategy in which security and network are viewed not as individual silos but as a larger, intertwined system. Security and network must be collectively addressed. For many organizations, including some in the group we interviewed, undertaking such significant change is daunting. A best practice voiced by our interviewees was the importance of ensuring strong relationships between, and a sense of collective ownership by the security and network teams.

Download the entire Dell'Oro Group's whitepaper, "Network Considerations in the Age of Secure Access Service Edge (SASE)".

netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

To learn more visit, https://www.netskope.com.