WHITEPAPER

So many ways to WAN

How the most essential technology for distributed enterprises has evolved—and where it's headed

One of the most critical components to the success of any growth-oriented enterprise is its wide area network (WAN), which is essential to delivering an exemplary customer and employee experience across all locations.

From data access via mobile devices to e-commerce platforms, the WAN is fundamental to ensuring that applications are available and functioning 24x7, with sufficient bandwidth and security, across the entire organization.

WAN quality is an ongoing issue for IT managers. They want to improve network performance and uptime, as well as provide better support to real-time applications. At the same time, they are also concerned about costs.

In fact, over the past few years, many organizations have looked at changing their network design to Internet-based networks to reduce cost and improve access for their business-critical cloud-based applications.

90% of WAN decision makers cite their network as important or critically important to the success of their company's digital transformation.[1]

88% of WAN decision makers regard reliability, resilience and low latency as critically/very important features of their network.[2]

85% of WAN decision makers regard high bandwidth capacity as critically/very important to their network performance.[2]

Let's look at the various types of WANs in use today and how wide area networking is evolving to support new applications and better performance now and in the future.

Striking the right balance for your network from a wide array of options

While one type of network can work for some companies, most enterprises are best served by selecting a flexible network design that includes MPLS IP VPN, Switched Ethernet, IPSec VPN, MPLS IPSec and—increasingly—connectivity to the cloud.

The goal is to strike the right balance of network options, realizing that business-critical applications can, and should, be handled differently from less essential functions.

The impact of this multifaceted network architecture can be quite significant, as the organization no longer needs to trade performance for cost and can satisfy the needs of all the sites on the network. Common questions to consider for many multi-location companies include:

How important is voice and data traffic?

Is redundancy required?

Is additional bandwidth needed for Internet traffic and non-real-time applications?

Is security required to avoid data breaches that could devastate the company's business?

To determine the best network design for a growth-oriented enterprise, it's important to understand and evaluate all available options based on requirements for scalability, availability, Quality of Service (QoS) and security.

Multiprotocol label switching (MPLS VPN)

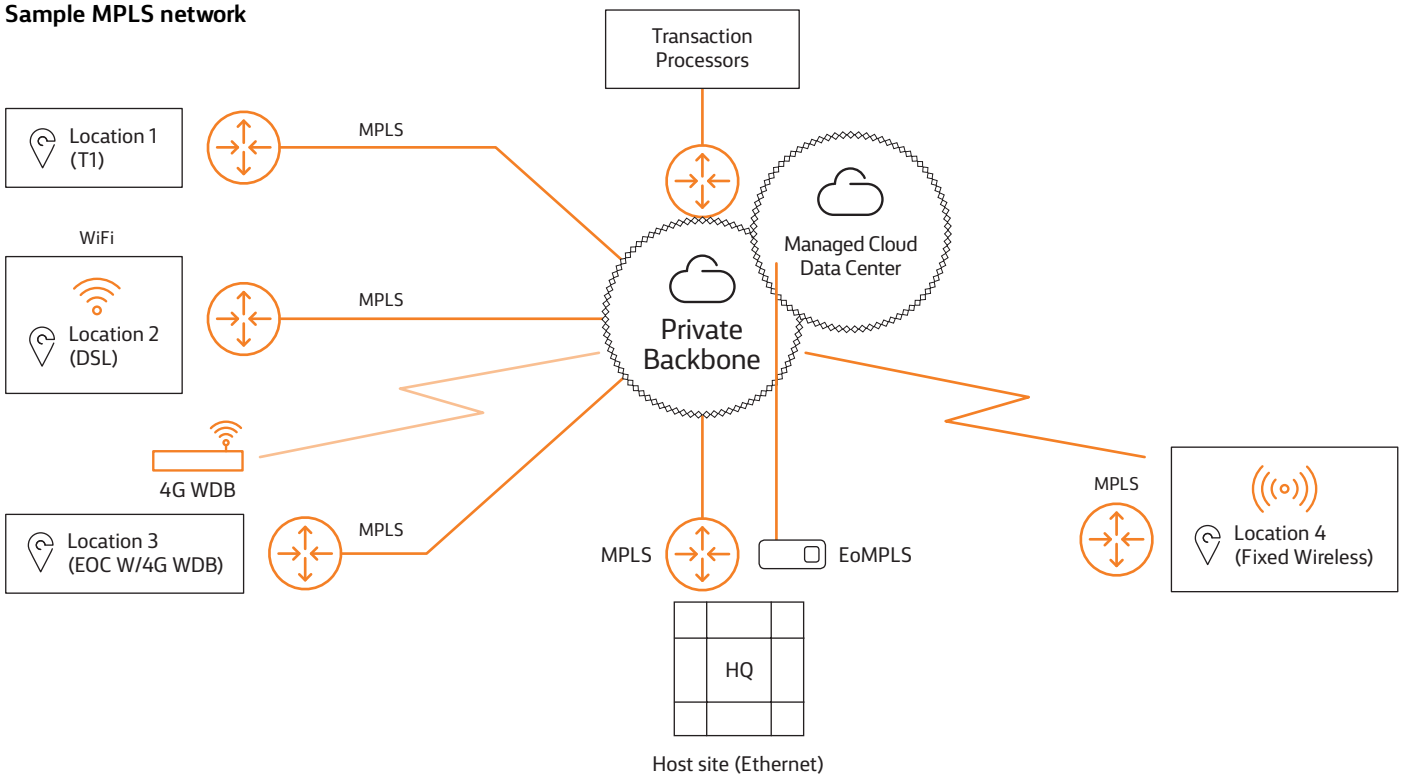
Traditional Layer 2 Ethernet over MPLS (EoMPLS) or Layer 3 MPLS VPNs are operated and managed by a single carrier, with connections that are isolated from the public Internet. Because the traffic within the MPLS network is kept private, the carrier is able to enforce QoS and Class of Service (CoS) policies on individual traffic flows.

From its introduction, MPLS has been a good option for organizations that run multiple business-critical applications and need control over application performance.

Voice and data traffic can converge into one network infrastructure, and this enables cost-effective management by right-sizing connectivity at each location.

Over the years, many larger companies have chosen to add a back-up MPLS VPN from a different service provider to enable redundancy and achieve greater availability. While MPLS has been the network of choice from a security perspective, it's also the most expensive option. What's more, the explosion in bandwidth demand driven by cloud-based apps has put a strain on MPLS designs. To enable cost-effective bandwidth, many businesses have begun to augment their MPLS networks with hybrid WANs and SD-WANs.

Sample MPLS network



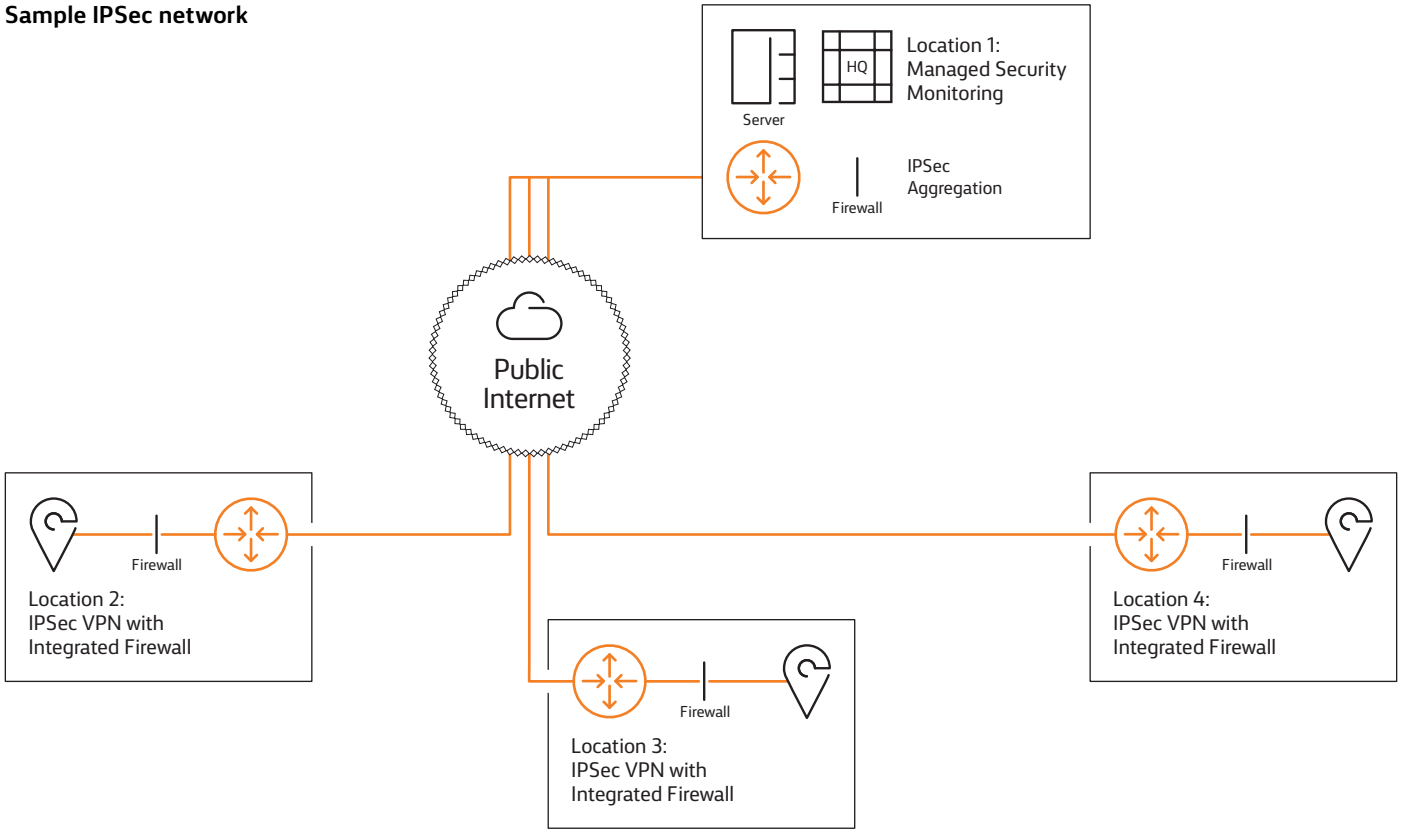
IPSec VPN

As an alternate solution, IPSec VPN securely connects multiple locations via the public Internet, thus requiring that traffic move across networks operated by multiple carriers.

Because this design can create challenges in keeping traffic private, the data is encrypted and the Internet port at each location should be secured with a firewall.

IPSec VPN is a better option if high bandwidth is more important than traffic prioritization and if flexibility to select access providers is desired as a cost-containment strategy. This network allows IT to obtain the bandwidth needed at an affordable price. Since an IPSec VPN uses encryption protocols and firewalls to shield sensitive corporate and customer information, it is much more secure than a direct Internet connection.

Sample IPSec network



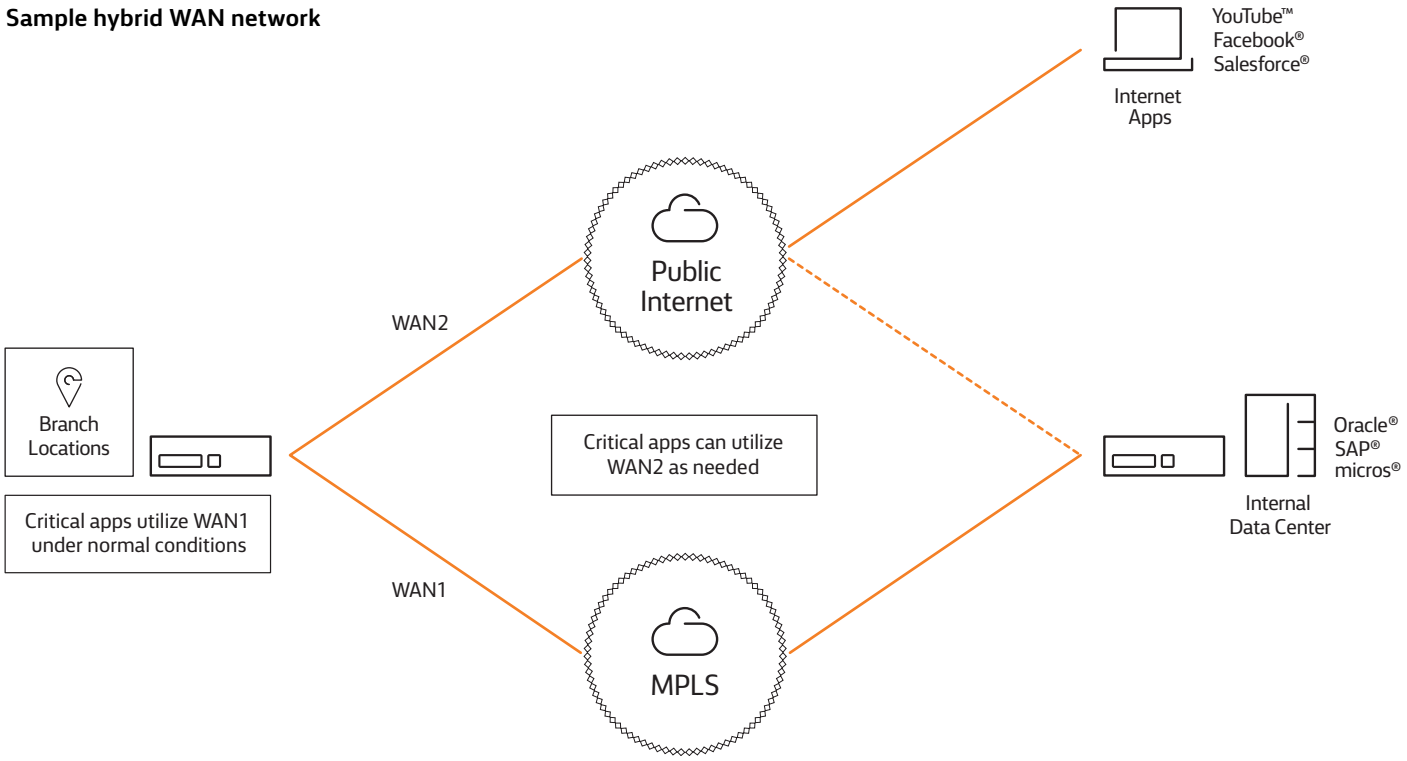
Hybrid WAN

Over time, the hybrid WAN has evolved to combine features of both MPLS IP VPN and IPSec VPN to leverage the benefits of each network. With this network architecture, IT can deploy the MPLS network to run real-time applications, such as voice and video with built-in CoS, as well as use IPSec VPN with broadband access at smaller remote sites or less critical locations.

Not only does this approach strike a balance between cost and performance requirements, but having two networks also enables one—most likely, the IPSec VPN—to serve as a redundant option for backup connectivity. In this design, the primary MPLS network connection would carry all of the private traffic, while all traffic destined for the Internet would flow through a separate Internet connection. In the event where access to the MPLS network fails, the private traffic would flow through an encrypted IPSec VPN tunnel back into the customer's MPLS network.

A hybrid WAN is an improvement over having a primary and passive secondary backup network design, because both connections can be simultaneously used to deliver traffic. However, a hybrid WAN will not provide the application visibility and intelligent dynamic routing to maximize application performance.

Sample hybrid WAN network



SD-WAN

As the latest entry in wide area networking, SD-WAN is an application-aware service that intelligently routes traffic in real time based on the established business policies, along with network quality and availability.

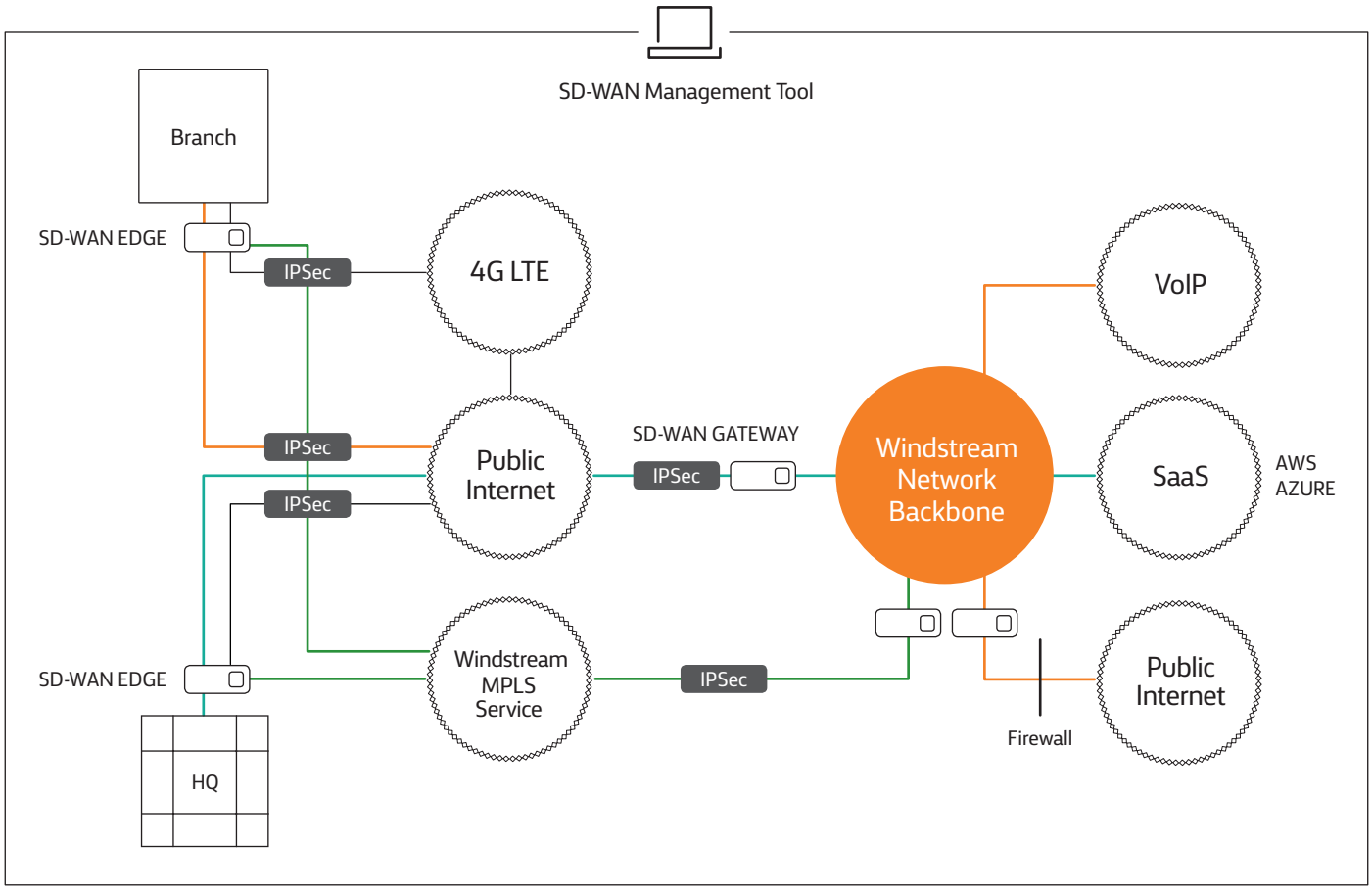
Cloud-based application traffic no longer needs to be backhauled through a private network. Instead, it's dynamically routed through the best link to deliver optimal performance. SD-WAN is designed to optimize application performance, reduce costs and simplify network management.

As a software-defined overlay network, SD-WAN works on top of the other types of networks, using elements from them.

Network management is centralized, allowing simplified visibility and control from a single pane of glass. IT personnel can view application performance and set network, security and applications policies across all locations according to their specific goals. New sites can rapidly be turned up with zero-touch deployment, dramatically reducing the need for on-site IT support.

Adding WiFi, video and cloud-based applications such as VoIP, O365, Salesforce, and others drives the need for more bandwidth. As part of the SD-WAN solution, additional low-cost broadband connections can be installed rapidly—without the need to reconfigure edge devices.

Sample SD-WAN network



Other considerations in choosing the right WAN

Service level agreements (SLAs)

Businesses want maximum uptime from their networks so all traffic gets to the right destinations, quickly. While both IPSec and MPLS IP VPNs can offer excellent availability, the private nature of MPLS gives it more stringency in this regard. The active-active design of SD-WAN enables providers to offer 100% availability SLAs and performance metrics that are much higher than Internet-only networks.

Class of Service (CoS)

IP transport is by nature subject to jitter, packet loss and latency. The collective measure of these characteristics across a connection forms the definition of Quality of Service (QoS). With an MPLS network, CoS is used to prioritize different types of traffic (e.g., voice, data and video) according to the relative importance of QoS to each. CoS is inherent in MPLS networks, while IPSec VPNs don't offer CoS prioritization. New SD-WAN technology can prioritize specific applications on a location or end-user basis, providing much more granularity and control than setting priorities for an entire class of service.

Network security

IPSec VPNs, MPLS VPNs and SD-WANs all keep data private: IPSec with encryption and firewalls; MPLS by being a dedicated network that doesn't touch the Internet; and SD-WAN by encrypting all traffic with IPSec so that any access type becomes a secure connection. Service providers employ a number of additional methods to protect business data from being accessed by unauthorized users. In some industries, this is necessary to demonstrate regulatory compliance. For businesses that transmit card data over their VPNs, some IPSec VPN providers offer the built-in convenience of PCI compliance, which helps to reduce the burden on the business.

Visibility and control

The ability to determine traffic prioritization across the entire WAN is essential. SD-WAN offers an advantage in this regard. Since it utilizes an overlay network to separate the networking hardware from the network control layer, SD-WAN relies on a centralized controller to set policies. SD-WAN then acts on these policies in concert with the real-time performance of the network connections to determine the best path for each application's traffic. This ensures that application performance meets service level agreements (SLAs).

What to look for in a WAN provider

While enterprises now have a wealth of WAN options available, choosing the right WAN design for an organization can nevertheless be tricky. That is especially true for IT leaders seeking to leverage the newest options, like SD-WAN technology.

Select a provider who:

Helps you take the guesswork out of network capacity planning and design so you can right-size your network to meet current needs and support your applications' innovation roadmap of the future.

Enables the flexibility to provide the best available access options to satisfy unique location requirements while keeping costs down by paying only for the access and capacity needed.

Offers tools to provide application visibility and control to maximize bandwidth utilization for a cost-optimized WAN to drive the customer experience initiatives that will help the business succeed.

Specializes in managed network, security and cloud solutions for multi-location businesses.

Provides experts to offer guidance in selecting the appropriate technologies that will achieve the organization's business goals and differentiate it from the competition.

Delivers an outstanding customer experience, every time.

Offers a reliable and secure WAN network foundation, along with years of experience, to allow for a custom-fit design to match the operational demands of the organization—which means maximizing the performance of all applications, all the time.

1. "SD-WAN Networks Enable Modern Digital Business Ecosystems." Windstream Enterprise, Forrester Consulting commissioned by Windstream Enterprise, Aug. 2017, https://www.windstreamenterprise.com/insights/sd-wan/sd-wan-networks-enable-modern-digital-business-ecosystems/, p.2. Accessed 12 Feb. 2018.
2. "SD-WAN Networks Enable Modern Digital Business Ecosystems." p.3. Accessed 12 Feb. 2018.

About Windstream Enterprise

Windstream Enterprise collaborates with businesses across the U.S. to drive digital transformation by delivering solutions that solve today's most complex networking and communication challenges.

To learn more about SD-WAN, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE

CONNECT. TRANSFORM. ELEVATE.