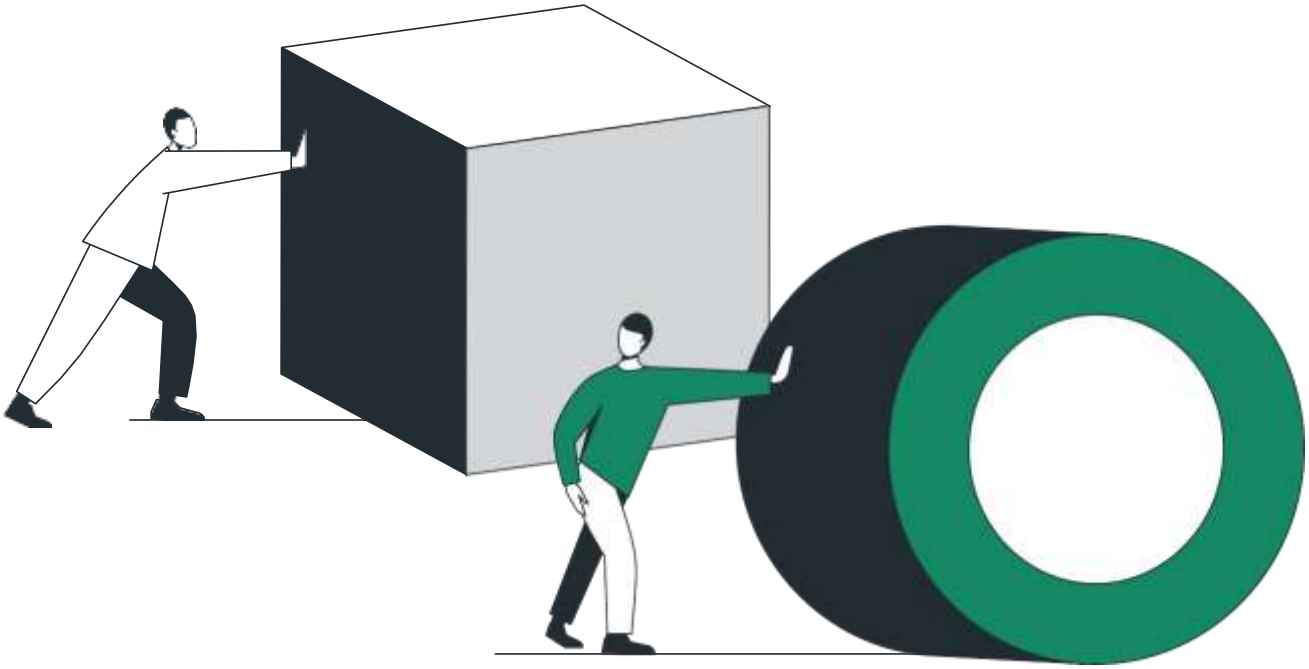
CATO NETWORKS

CLOUDTIVITY CONSULTING SERVICES

MPLS, SD-WAN, and SASE

Understanding the Trade-offs for Your New WAN

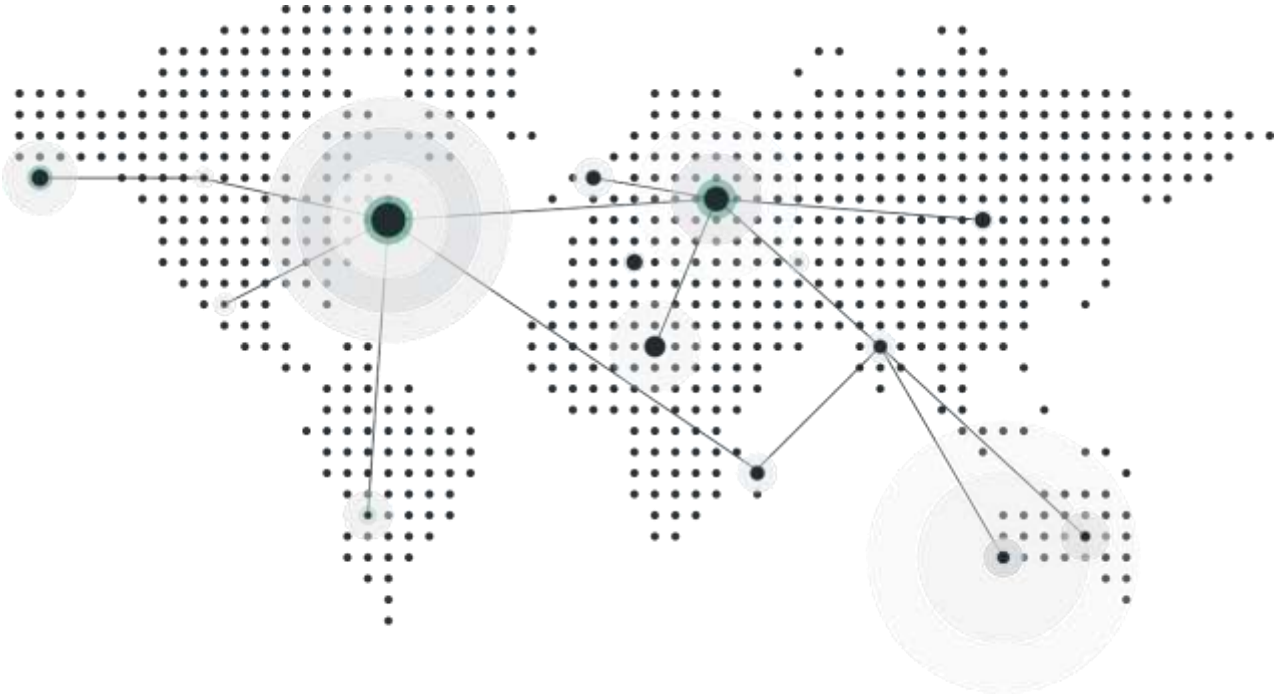


Executive Summary

The WAN is the backbone of the business. It ties together the remote locations, headquarters and data centers into an integrated network. Yet, the role of the WAN has evolved in recent years. Beyond physical locations, we now need to provide optimized and secure access to cloud-based resources for a global and mobile workforce. The existing WAN optimization and security solutions, designed for physical locations and point-to-point architectures, are stretched to support this transformation.

This paper discusses the different connectivity, optimization and security options that are needed when building a network for the digital business. A new architecture is needed, one that addresses the dynamics of cloud and mobility.

Both are new to the WAN that traditionally only connected remote offices and other business locations to the applications and resources hosted in the company's datacenter. Let's take a look at how the WAN is evolving.



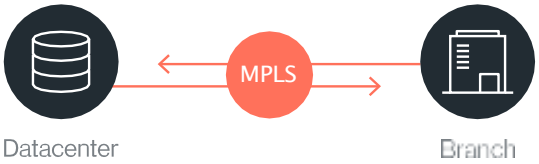
First Generation

Legacy WAN Connectivity

Currently, there are two WAN connectivity options, which balance cost, availability, and latency:

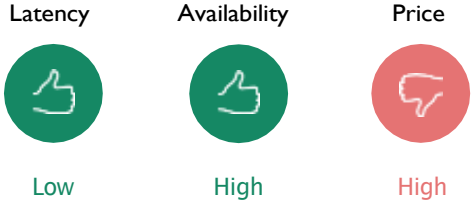
MPLS

SLA-Backed Service at Premium Price



With MPLS, a telecommunication provider provisions two or more business locations with a managed connection and routes traffic between these locations over their private backbone. In theory, since the traffic does not traverse the Internet, encryption is optional. Because the connection is managed by the telco, end to end, it can commit to availability and latency SLAs. This commitment is expensive and is priced by bandwidth. Enterprises choose MPLS if they need to support applications with stringent up-time requirements and minimal quality of service (such as Voice over IP (VoIP).

To maximize the usage of MPLS links, WAN optimization equipment is deployed at each end of the line, to prioritize and reduce different types of application traffic. The effectiveness of such optimizations is protocol and application specific (for example, compressed streams benefit less from WAN optimization).

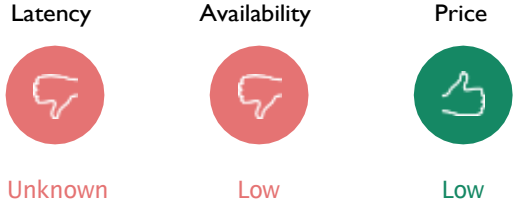


Internet

Best-Effort Service at a Discounted Price

Internet connections procured from the ISP, typically offers nearly unlimited last mile capacity for a low monthly price. An unmanaged Internet connection doesn't have the high availability and low-latency benefits of MPLS but it is inexpensive and quick to deploy. IT establishes an encrypted VPN tunnel between the branch office firewall and the headquarters/data center firewall. The connection itself is going through the Internet, with no guarantee of service levels because it is not possible to control the number of carriers or the number of hops a packet has to cross. This can cause unpredictable application behavior due to increased latency and packet loss.

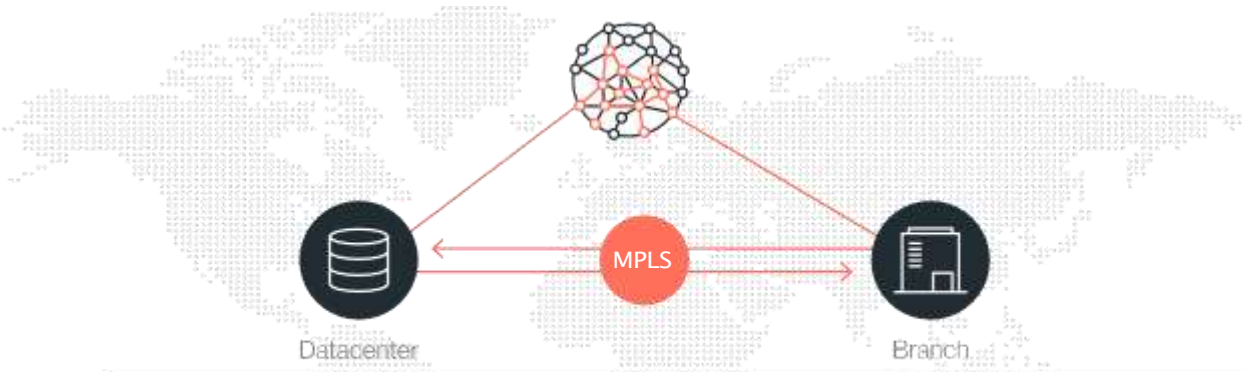
Internet-based connectivity forces customers to deploy and manage branch office security equipment.



Second Generation

Appliance-based SD-WAN

The cost/performance trade off between Internet and MPLS, gave rise to SD-WAN. SD-WAN is using both MPLS and Internet links to handle WAN traffic. Latency sensitive apps are using the MPLS links, while the rest of the traffic is using the Internet link. The challenge customers face is to dynamically assign application traffic to the appropriate link.



Augmenting MPLS with Internet Links

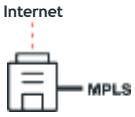
SD-WAN solutions offer the management capabilities to direct the relevant traffic according to its required class of service, offloading MPLS links and delaying the need to upgrade capacity. SD-WAN solutions, however, are limited in a few key aspects:

Footprint

Similar to WAN optimization equipment, SD-WAN solutions must have a box deployed at each side of the link.

Connectivity

SD-WAN can't replace the MPLS link because its Internet "leg" is exposed to the unpredictable nature of an unmanaged Internet connection (namely, its unpredictable latency, packet drops and availability).



Deployment

SD-WAN, like the other WAN connectivity options, is agnostic to the increased role of Internet, cloud and mobility within the enterprise network. It focuses, for the most part on optimizing the legacy, physical WAN.

Third Generation

Secure Access Service Edge (SASE)

With the rapid migration to cloud applications (e.g., Office 365), cloud infrastructure (e.g. Amazon AWS) and a mobile workforce, the classic WAN architecture is severely challenged. It is no longer sufficient to think in terms of physical locations being the heart of the business. Here is why:

Limited end-to-end link control for the cloud

With public cloud applications, organizations can't rely on optimizations that require a box at both ends of each link. In addition, cloud infrastructure (servers and storage) introduces a new production environment that has its own connectivity and security requirements. Existing WAN and security solutions don't naturally extend to cloud-based environments.

Limited service and control to mobile users

Securely accessing corporate resources requires, mobile users to connect to a branch or HQ firewall VPN which could be very far from their location. This causes user experience issues, and encourages compliance violations (for example, direct access to cloud services that bypasses corporate security policy). Ultimately, the mobile workforce is not effectively covered by the WAN.

SASE is aiming to address these challenges. It is based on the following principles:

The perimeter moves to the cloud

The notorious dissolving perimeter is re-established in the cloud. The cloud delivers a managed WAN backbone with reduced latency and optimal routing. This ensures the required quality of service for both internal and cloud-based applications.

The network "democratic" and all-inclusive

All network elements plug into the cloud WAN with secure tunnels including physical locations, cloud resources and mobile users. This ensures all business elements are integral part of the network instead of being bolted on top of a legacy architecture.

Security is integrated into the network

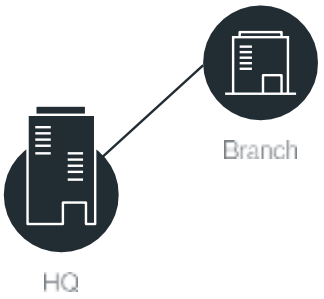
Beyond securing the backbone itself, it is possible to directly secure all traffic (WAN and Internet) that crosses the perimeter - without deploying distributed firewall.

WAN Connectivity and Security Use Cases

Options and Tradeoffs

Option A

Branch to HQ Connectivity



MPLS

PROS

- Guaranteed SLA (latency, uptime)
- No need for a branch FW (if Internet access isn't required)

CONS

- High cost per bit
- Long time to provision (weeks to months)
- Limited global coverage (requires multiple carriers)
- Performance impact with backhaul for Internet access ("Trombone Effect")

Internet Link

PROS

- Low cost (vs. MPLS)
- Ad-hoc provisioning
- Ability to create Any site-to-any site mesh

CONS

- No SLA for Internet routing
- Susceptible to unpredictable latency/packet loss
- Requires branch firewall (capex, management/ support overhead)
- Requires local ISP/connection contract

Appliance-based SD-WAN

PROS

- Dynamic link selection (MPLS or IPVPN)
- Reduce need to increase expensive MPLS capacity
- Redundancy/availability

CONS

- MPLS is still a costly requirement because IPVPN link subject to unpredictable Internet latency/line quality
- Requires local ISP/connection contracts
- Requires branch firewall or cloud-based Secure Web Gateway
- Limited optimization for branch-to-cloud access

Secure Access Service Edge (SASE)

PROS

- MPLS-like SLA-backed latency
- Multi-ISP/LTE support for last mile redundancy
- Automated secure office mesh
- No need to backhaul
- No need for branch firewall

CONS

- Requires local ISP connection/contract (two for resiliency)
- SASE provider must have a PoP in region

Option B

Secure and Optimized Branch Access to the Internet/cloud

MPLS

PROS

- Direct connection to cloud service providers

CONS

- Expensive transport for Internet traffic
- Slow time-to-upgrade
- Limited security access control to the Internet/cloud (requires 3rd party point solutions)

Internet Link

PROS

- Secure direct access to the Internet with branch firewall

CONS

- Requires to deploy and maintain branch firewall
- Limited security access control to the Internet/ cloud, often requiring a Cloud Access Security Broker (CASB)

Appliance-based SD-WAN

PROS

- Secure and optimize cloud access with 3rd party partnerships

CONS

- Designed mostly for WAN connectivity and not as a cloud-focused optimization and security solution

Secure Access Service Edge (SASE)

PROS

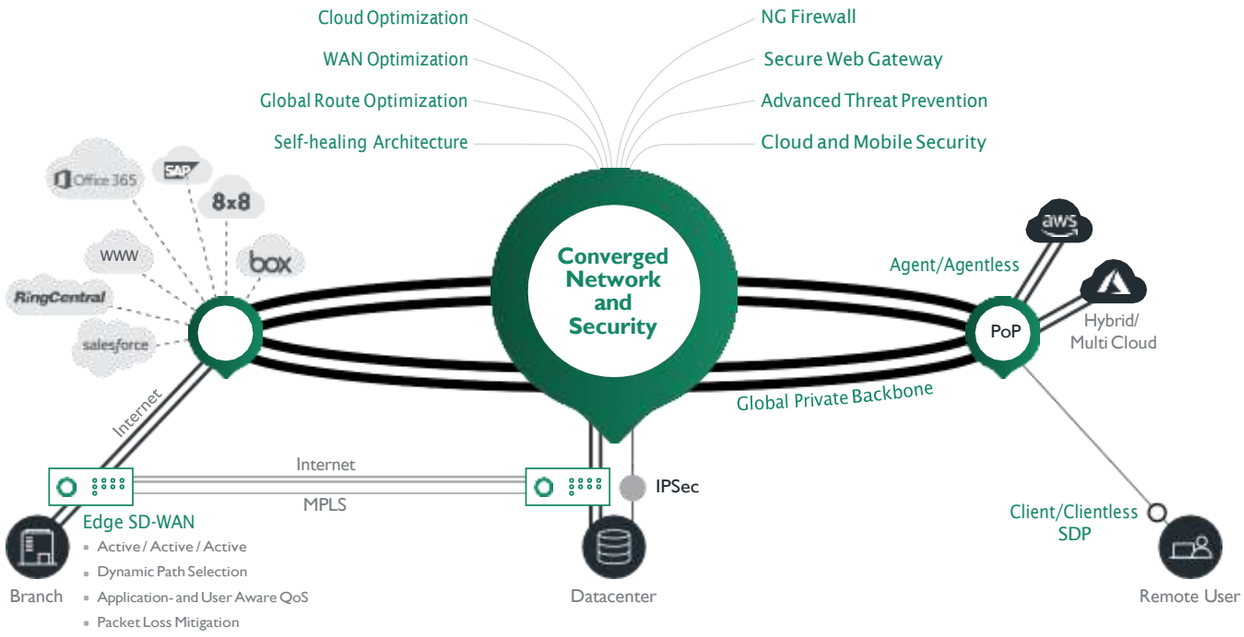
- No need for a branch firewall
- Integrated branch-to-cloud optimization, cloud access control
- Automated secure office mesh
- One solution to handle both WAN, Internet and cloud traffic

CONS

- Depends on a cloud security service availability
- SASE provider must have a PoP in region

About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero trust architecture.



For more details, please contact us

Cloudtivity Consulting Services, LLC
(770) 833-6371
info@cloudtivityconsulting.com
https://cloudtivityconsulting.com/

Cato.
The Network for Whatever's Next.

Cato Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Mobile Access Optimization
- Cato Management Application

Managed Services

- Managed Threat Detection and Response (MDR)
- Intelligent Last-Mile Management
- Hands-Free Management
- Site Deployment