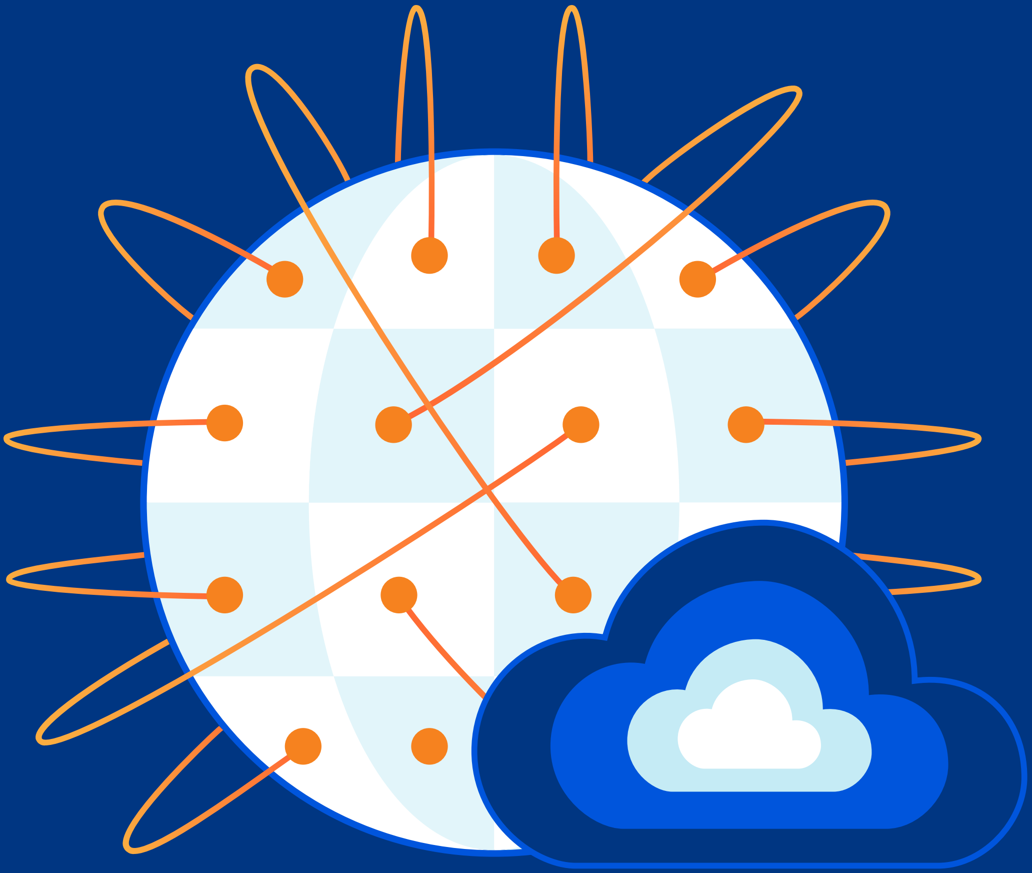
WHITEPAPER

CLOUDFLARE®

WAN-as-a-Service enables networks to respond to evolving IT needs



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Introduction

Enterprises have long relied on multiprotocol label switching (MPLS) services or IPSec VPNs over broadband Internet to build wide area networks (WANs). Both of these methods have always had their challenges. MPLS is a reliable way to establish a virtual private network (VPN) across private data centers, offices, retail stores, and other locations, but it is expensive to establish. IPSec VPNs over broadband are cheaper, but are inherently unreliable.

In addition, both of these WAN models were designed for a world where apps lived in a private data center and users were mostly in offices. Fast forward to the present day — with more data-rich applications, more applications running in the cloud, and entire workforces enabled to work from home — and we see conventional WANs struggling to keep up.

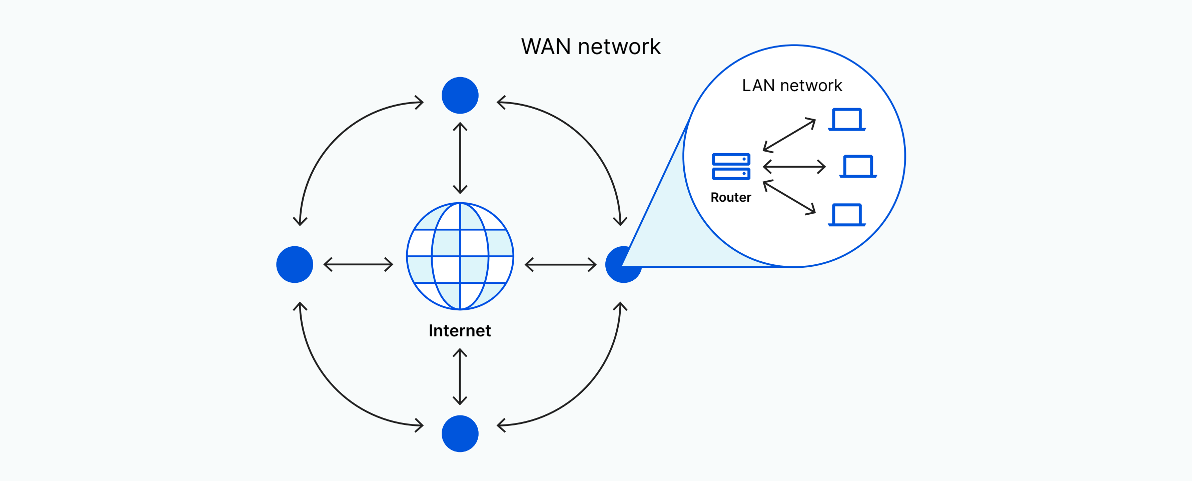
The industry responded to these challenges with the development of the software-defined WAN (SD-WAN). SD-WANs simplify network policy configuration and management while orchestrating traffic over multiple paths and WAN architectures, such as broadband and MPLS. Thanks to these benefits, enterprises have been able to evolve their WANs and take advantage of cheaper connectivity options. The global SD-WAN market size is expected to grow from USD 1.9 billion in 2020 to USD 8.4 billion by 2025.

Despite the incremental improvement of SD-WAN over traditional network architectures, fundamental challenges remain. While some deployments have addressed today's evolving traffic patterns, cloud adoption and the explosive growth of remote work strain many SD-WAN architectures. Security is another key challenge, since decentralized networks are harder to secure.

To meet these new challenges, enterprises need a new WAN architecture — with built-in security, speed, and reliability — that can evolve quickly. WAN-as-a-Service is this model. It promises to transform enterprise network architectures and provide significant cost and performance advantages.

Challenges with traditional WAN architectures

A WAN is a large network that connects individual locations — like offices, data centers, retail stores, and more — over long distances. Often, each of these locations has its own local area network (LAN), which connects individual devices using methods like Ethernet or WiFi. Meanwhile, WAN connections use methods like VPNs, MPLS, or IPSec tunnels.



WANs enable employees to securely access business applications and tools. They also enable machines to communicate with each other over a private network. However, the methods traditionally used to provide this interconnection provide several challenges:

MPLS VPN Challenges

MPLS VPNs let enterprises connect multiple data center and office locations over a wide geographic area. MPLS speeds up data transit by directing data from one node to the next using labels along predetermined network paths, rather than having each core router independently compute the path using IP addresses.

This approach allows for a faster, simpler core network that can carry traffic for multiple enterprise WANs at the same time. It also provides tighter control over the traffic paths to ensure reliability and quality of service. MPLS often includes multiple classes of service that give latency-sensitive applications like voice and video priority over less sensitive apps like database backups.

While MPLS offers speed and reliability, deployments are expensive to build and slow to scale since they require specialized routers and up-front provisioning. Additionally, encryption for data privacy and other perimeter firewall protections must be set up separately at each location. Organizations may also experience difficulty extending their MPLS network connections to cloud servers, making it hard to reach the places their data and applications live.

MPLS pros:	MPLS cons:
Highly reliable service with SLAs	Slow to deploy and scale
Multiple classes of service	No native encryption
Less vulnerable to threats like DDoS	Not optimized for SaaS or public cloud

IPSec VPN over Broadband Internet Challenges

Enterprises may also build VPNs over the public Internet using encrypted tunnels, which ensure data privacy while taking advantage of cheaper broadband Internet connections. Many VPNs use the IPsec protocol suite to establish these tunnels. IPSec VPNs are typically available as a service from carriers.

Since traffic traverses the public Internet — which has no quality of service guarantees — this WAN architecture is inherently less reliable. Public Internet congestion, outages, routing errors, and other obstacles can hurt IPSec VPN performance and connectivity. Also, even though quality of service can be enforced at the network edge using specialized routers, all traffic is treated the same once it hits the Internet. Voice and video calls will not be prioritized over less-sensitive traffic like backups.

In addition, IPSec VPNs typically follow a hub and spoke model, in which traffic from remote branch offices is brought back to a central data center — the 'hub.' The hub-and-spoke model worked well when most network traffic involved business applications hosted in a centralized data center. However, the growth of public cloud, SaaS, and IoT creates inefficiencies. For example, a user in a Singapore office trying to access corporate email might have their traffic backhauled to the US, even though the email provider has data centers in Singapore. These long round trips hurt application performance.

IPSec VPN pros:

- Inexpensive compared to MPLS
- More operationally agile
- Native encryption

IPSec VPN cons:

- Less reliable than MPLS
- Inefficient hub and spoke architecture
- Single class of service

Hybrid MPLS and Broadband Internet Challenges

Some companies implement a hybrid WAN using MPLS and IPSec over broadband Internet simultaneously. This allows them to integrate additional sites that may not be served by the MPLS vendor or that have simpler requirements, like small retail stores.

This hybrid MPLS-broadband approach, while improving bandwidth allocation, does not mitigate the shortcomings inherent to either technique. Enterprises are still left with the increased administrative overhead of installing and managing leased lines and broadband Internet from multiple service providers. Plus, they must string together a series of security and performance appliances at each office location to overcome the shortcomings of each connectivity model.

In addition, traditional WAN architectures don't include security services natively, forcing enterprises to purchase, install, and manage equipment (such as network firewalls, DDoS mitigation, WAN optimization, and load balancers) at each location for the security, performance, and reliability business applications need today. This network hardware contributes to increased complexity, cost, technical debt, and a tangled web of dependencies.

Lastly, traditional WANs provide limited visibility into traffic flows. With fragmented performance data from LANs, vendor MPLS networks, and the public Internet, insights remain elusive. For example, what are users doing while online? How well is a security policy working? And what apps are using the most bandwidth?

Hybrid WAN pros:

- Better bandwidth allocation
- Reliability (when MPLS is used)
- Cost-efficiency (when IPSec VPNs are used)

Hybrid WAN cons:

- No native security
- Hardware management overhead
- Fragmented visibility

SD-WAN benefits and challenges

An SD-WAN uses software at enterprise sites and a centralized controller to overcome some of the limitations of traditional WAN architectures. It enables enterprises to manage traffic across multiple connection types — including broadband Internet, leased line and MPLS — from a single software platform. It can also automate network monitoring tasks, make real time traffic steering decisions, and optimize access to public cloud and SaaS applications using direct connections and split tunneling.

SD-WANs can reduce costs for an organization by simplifying administration and providing MPLS-like reliability and performance over cheaper broadband Internet connections. However, SD-WANs face their own challenges.

Security still needs to be bolted on

While SD-WANs allow direct access to the public cloud and SaaS services from a branch office, they lack the full suite of perimeter security controls most enterprises require. Some SD-WAN vendors include basic firewall and VPN capabilities, but these are typically not enough to provide robust protection.

As a result, most organizations are unable to take advantage of these enhancements and still have to backhaul traffic to the data center locations with firewall, intrusion detection, data loss prevention, and secure web access enabled.

End-user latency

When traffic must be backhauled to centralized locations, data-rich applications like video and telephony will suffer as a result.

Poor quality of service end-to-end

While SD-WANs simplify management and reduce costs, they still rely on the unpredictable public Internet to deliver traffic between sites. This means that latency-sensitive and bandwidth-hungry apps like video conferencing may operate poorly during periods of network congestion. While some SD-WAN vendors operate their own backbone networks, most are edge technologies that cannot guarantee a good application experience end-to-end.

Does not extend to remote work

Employees across many industries now work from home, in the office, and on the road, often interchangeably. SD-WANs do not readily extend to the remote work use case. While home office LANs can theoretically be integrated into the corporate network, it is impractical to do so for many reasons. Most SD-WAN technologies are not designed to accommodate individual laptops connecting to the corporate WAN. Employees expect the same level of access regardless of location and this requires additional zero trust network access solutions to be layered on.

SD-WAN Pros:	SD-WAN Cons
Simplified WAN management	Security is a bolt-on
Reduced operational costs	Poor end-to-end quality of service
Improved application performance	Harder to accommodate remote workers

WAN-as-a-Service meets the demands of modern networks

WAN-as-a-Service is a WAN model that addresses all of the previous challenges. It enables organizations to build upon the benefits of SD-WANs, and also responds to SD-WAN deficiencies for improved operational agility and lower total costs of ownership.

A WAN-as-a-Service deployment has the following features:

- **Global network:** WAN-as-a-Service uses a large global network of many data centers as the WAN's connective tissue.
- **Interconnectivity:** This network is deeply interconnected with ISPs, cloud vendors, and private corporate networks.
- **Integrated security:** The network runs a full suite of network security services, including a firewall, DDoS mitigation, and zero trust security.
- **Unified architecture:** All WAN functionality and security services operate in every server in every data center in the network.
- **Single dashboard:** All of these services are manageable in-browser from a single dashboard.

Using these features, WAN-as-a-Service offers the following solutions to common WAN and SD-WAN challenges:

Challenge	WAN-as-a-Service advantage
Patchwork of expensive legacy services and network appliances	Optimized application performance over an interconnected global network with integrated security.
Proprietary hardware appliances at each site	Fully software-defined and cloud-native, which eliminates the need for custom physical or virtual appliances.
Slow MPLS scaling	Scales rapidly to accommodate new office locations and thousands of remote access requests over an existing globally distributed, interconnected network.
Management cost & resource drain	As-a-service means network management is now a centralized line item operating expense that covers the entire WAN. Expensive, remote on-site maintenance costs are eliminated.
Exposure to public Internet congestion	WAN-as-a-Service approaches send traffic across the public Internet, but use their network scale to find fast network paths and avoid congestion.
Latency due to data backhauling	Using hundreds of network locations around the world, WAN-as-a-Service brings workloads closer to users and eliminates the need to backhaul data. This improves performance, especially for real-time, data heavy applications.

Challenge	WAN-as-a-Service advantage
Security holes & bolt-on solutions	From a single unified control plane, WAN-as-a-Service applies tightly integrated network-wide security (such as a built-in, software-defined network firewall) from every network location. Traffic filters can be applied based on IP, port, packet length, and bit field match. Rules apply instantly across all locations. Additional security functionality can be layered in for DNS filtering, SWG with remote browser isolation, and DDoS protection.
Fragmented network analytics and visibility	With WAN-as-a-Service, enterprises can view their entire WAN traffic flow on a unified analytics dashboard and gain insights into how the network is being utilized and by whom.
Does not extend to remote work	WAN-as-a-Service can accommodate remote users and endpoints. Instead of funneling all remote traffic through a single choke point (such as VPN concentrators at a corporate network “perimeter”), traffic is routed to the nearest edge location and directed over the most optimal path. This enables superior application performance and an improved end user experience from any location.

Magic WAN

The administrative burden of maintaining both MPLS and Internet circuits along with an SD-WAN controller and in-line routers saps resources and hurts performance. Cloudflare’s Magic WAN provides as-a-service convenience and functionality.

Cloudflare operates one of the world’s largest networks with data centers strategically located in over 200 cities in 100 countries. Our network is carrier-agnostic, and has over 9500 interconnections with major ISPs, cloud services, and enterprises. And every security and performance service is available from every server in every data center in our network.

Magic WAN replaces legacy WAN architectures with Cloudflare’s network, providing global connectivity, integrated security, and high performance through one simple user interface.

To learn more, visit cloudflare.com/magic-wan