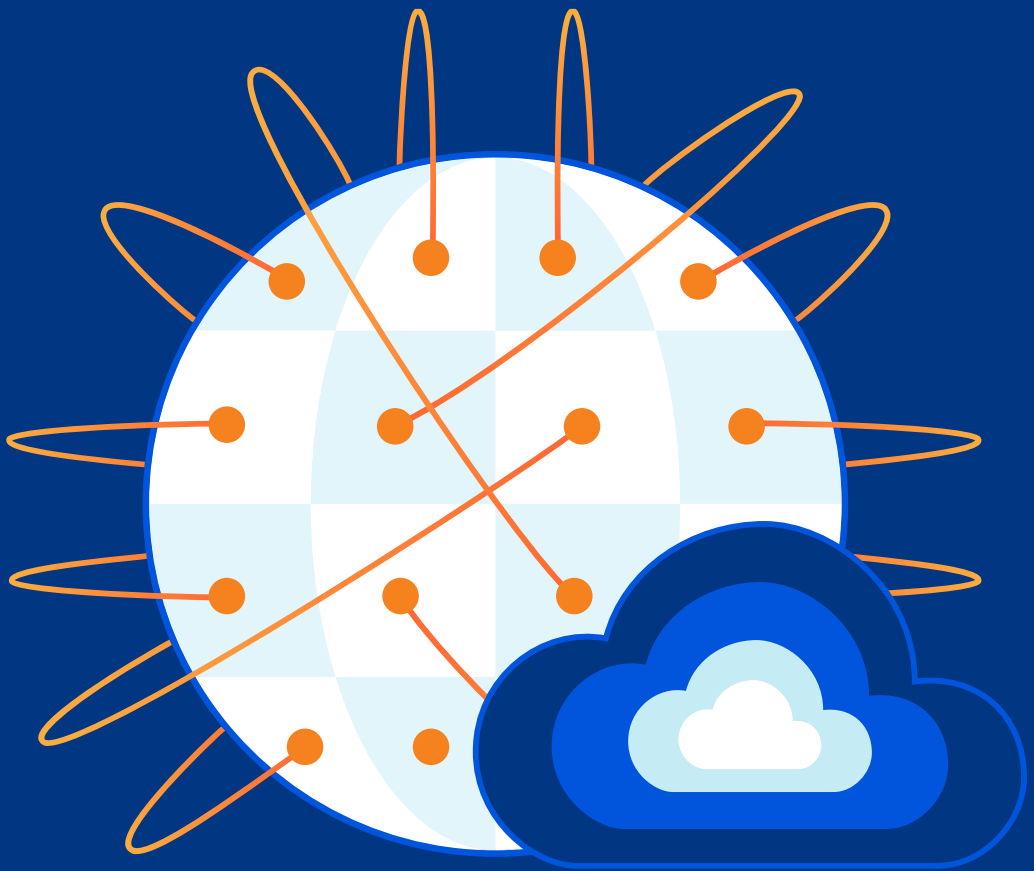
WHITEPAPER

CLOUDFLARE

WAN as a Service macht Netzwerke für neue IT-Anforderungen fit



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

Was ist Cloudflare?

Cloudflare ist ein globales Netzwerk an der Internet-Edge. Wir bringen Sie Ihren Kunden, Mitarbeitern und Partnern näher, indem wir dafür sorgen, dass Sie sich sicher, vertraulich, schnell und zuverlässig mit dem Internet verbinden können. Ungefähr 25 Millionen Websites – darunter 17 % der Fortune 1000 – nutzen Cloudflare, um öffentlich zugängliche Websites zu schützen und zu beschleunigen, interne Abläufe zu sichern und neue Anwendungen auf unserer Serverless-Plattform zu erstellen.

Unser Netzwerk verfügt über Rechenzentren in über 200 Städten. 99 % aller Internetnutzer können mit einer Latenzzeit von weniger als 100 Millisekunden erreicht werden. Zudem werden durchschnittlich 57 Milliarden Bedrohungen pro Tag blockiert, darunter auch einige der größten DDoS-Angriffe. Jede einzelne Anmeldung, Anfrage und Antwort stärkt die Machine Learning-Modelle, mit denen wir Bedrohungen am Netzwerkrand erkennen und blockieren, bevor sie Ihr Unternehmen überhaupt erreichen.

Zudem ist das Cloudflare-Netzwerk mit Blick auf Datenschutz entwickelt worden. Weil das für uns an erster Stelle steht, setzen wir Ende-zu-Ende Verschlüsselung ein. Wir halten uns an die örtlichen Gesetzesvorgaben zur Datenlokalisierung und -speicherung. Da wir keine Einnahmen aus Werbung erzielen, verzichten wir auf die Erfassung und Speicherung von personenbezogenen Daten, die wir in Ihrem Auftrag verarbeiten.

Der Hauptsitz von Cloudflare befindet sich in San Francisco (Kalifornien). Das Unternehmen unterhält Niederlassungen in Lissabon, London, München, Paris, Peking, Singapur, Sydney, Tokio, Austin (Texas), Champaign (Illinois), Seattle (Washington), New York (New York), San Jos (Kalifornien) und Washington, D.C.

Mehr als 25 Millionen Websites setzen auf die intelligenten Lösungen von Cloudflare. Diese Websites stammen von Unternehmen und Organisationen aus diversen Branchen.

Einleitung

Lange haben Unternehmen für den Aufbau von Wide Area Networks (WANs) auf Multiprotocol Label Switching (MPLS)-Services oder IPSec-VPNs auf Basis von Breitband-Internetverbindungen gesetzt. Doch beide Methoden hatten von jeher ihre Tücken. Mit MPLS lässt sich ein zuverlässiges Virtual Private Network (VPN) schaffen, dass private Rechenzentren, Büros, Geschäfte und andere Standorte abdeckt, allerdings hat das seinen Preis. IPSec-VPNs auf Basis von Breitbandverbindungen sind demgegenüber zwar weniger kostspielig, aber leider auch notorisch unzuverlässig.

Hinzu kommt, dass beide WAN-Modelle für eine Welt entwickelt wurden, in der Apps über private Rechenzentren zur Verfügung gestellt wurden und die Nutzer hauptsächlich an Firmenstandorten arbeiteten. Heute stellt sich die Lage aber anders da: Anwendungen sind inzwischen nicht nur datenintensiver, sondern werden auch häufiger über die Cloud betrieben, und mittlerweile sitzen komplette Belegschaften im Homeoffice. Konventionelle WANs haben Mühe, mit dieser Entwicklung Schritt zu halten.

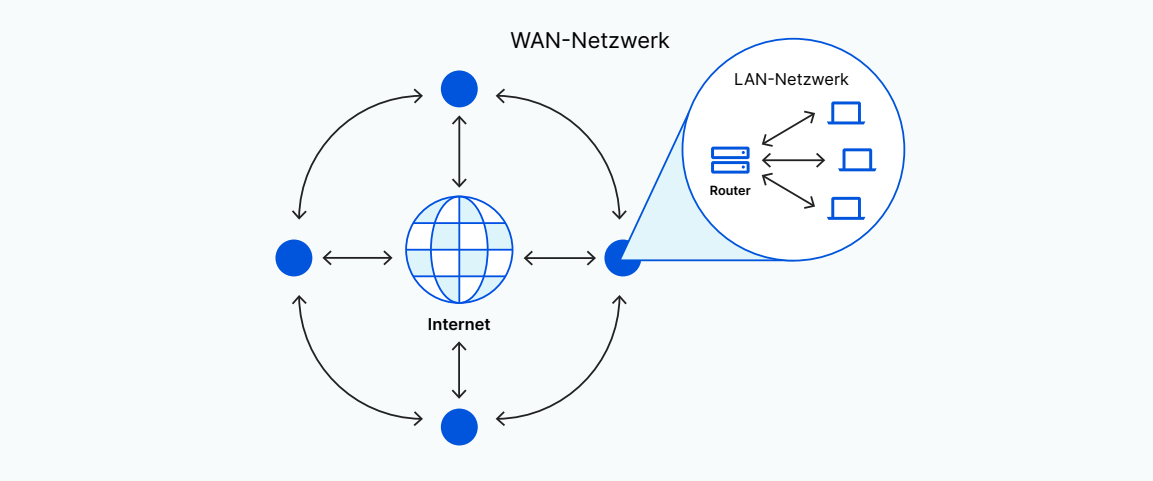
Deshalb hat die Branche das Modell des softwaredefinierten WAN (SD-WAN) entwickelt. SD-WANs erleichtern die Konfiguration und Verwaltung von Netzwerkrichtlinien und organisieren gleichzeitig den Datentransfer über verschiedene Pfade und WAN-Architekturen wie Breitband und MPLS. Dadurch konnten Unternehmen ihre WANs weiterentwickeln und auf günstigere Verbindungslösungen zurückzugreifen. Prognosen zufolge wird der globale Markt für SD-WAN von 1,9 Milliarden US-Dollar im Jahr 2020 auf 8,4 Milliarden im Jahr 2025 wachsen.

SD-WAN stellt gegenüber herkömmlichen Netzwerkarchitekturen durchaus eine gewisse Verbesserung dar, doch grundlegende Probleme bleiben bestehen. Einige Unternehmen haben zwar Lösungen gefunden, um der Wandelbarkeit der heutigen Datenverkehrsmuster Rechnung zu tragen, doch der Umzug in die Cloud und die explosionsartige Verbreitung von Remote-Arbeit bringen weiterhin viele SD-WAN-Architekturen an ihre Grenzen. Ein weiterer wichtiger Knackpunkt ist die Sicherheitsfrage, denn es ist schwieriger, dezentrale Netzwerke zu schützen.

Um diese neuen Herausforderungen zu bewältigen, brauchen Unternehmen eine neue Art der WAN-Architektur, die hochgradig anpassungsfähig ist und die nötige Sicherheit, Geschwindigkeit und Zuverlässigkeit von Anfang an bieten kann. WAN as a Service erfüllt all diese Bedingungen. Die Lösung hat nicht nur das Potenzial, die Architekturen von Firmennetzwerken auf eine ganz neue Grundlage zu stellen, sondern verspricht auch große Vorteile hinsichtlich Kosten und Performance.

Die Schwächen herkömmlicher WAN-Architekturen

Ein WAN ist ein umfangreiches Netzwerk, das Einzelstandorte wie Büros, Rechenzentren oder Geschäfte über große Entfernungen miteinander verbindet. Häufig verfügt jeder dieser Standorte über ein eigenes Local Area Network (LAN), das einzelne Geräte über Ethernet, per WLAN oder auf andere Weise miteinander vernetzt. WAN-Verbindungen wiederum nutzen Verfahren wie VPN, MPLS oder den IPSec-Tunnelmodus.



Mit WANs können Beschäftigte sicher auf Geschäftsanwendungen und -Tools zugreifen. Außerdem ermöglichen sie die Kommunikation zwischen Geräten über ein privates Netzwerk. Die traditionell für diese Vernetzung eingesetzten Methoden bringen jedoch gleich mehrere Probleme mit sich:

Die Schwächen von MPLS-VPN

Mit MPLS-VPNs können Unternehmen mehrere Rechenzentren und Firmenstandorte über große Entfernungen hinweg vernetzen. MPLS leitet Daten mithilfe von Kennzeichnungen (Labels) entlang vordefinierter Netzwerkpfade von einem Knoten zum nächsten, anstatt jeden Router im Netzwerkzentrum den Pfad anhand von IP-Adressen unabhängig bestimmen zu lassen. Auf diese Weise wird die Datenübertragung beschleunigt.

Da das zentrale Netzwerk dadurch schneller arbeitet und eine weniger komplexe Struktur aufweist, ist es in der Lage, den Datenverkehr mehrerer Firmen-WANs gleichzeitig abzuwickeln. Außerdem können zur Gewährleistung von Zuverlässigkeit und Quality of Service die genutzten Traffic-Pfade strenger kontrolliert werden. Häufig stehen bei MPLS mehrere Serviceklassen zur Verfügung, um etwa Sprach- und Video-Anwendungen Vorrang einräumen zu können, weil diese durch eine hohe Latenz stärker beeinträchtigt werden als beispielsweise Datenbank-Backups.

Für MPLS sprechen die Geschwindigkeit und Zuverlässigkeit, die diese Methode bietet. Entsprechende Lösungen sind aber kostspielig in der Entwicklung und können nur langsam skaliert werden, weil sie spezielle Router und Vorabinvestitionen erforderlich machen. Darüber hinaus müssen an jedem Standort eigene Verschlüsselungen zur Sicherstellung des Datenschutzes eingerichtet und weitere Firewall-Maßnahmen zum Schutz des Perimeters durchgeführt werden. Unter Umständen fällt es Unternehmen außerdem schwer, ihre MPLS-Netzwerkverbindungen auf Cloud-Server auszuweiten, was die Erreichbarkeit ihrer Daten und Anwendungen beeinträchtigt.

Die Vorteile von MPLS:

- Höchste, durch SLAs garantierte Zuverlässigkeit
- Mehrere Serviceklassen
- Weniger anfällig für DDoS-Angriffe und andere Bedrohungen

Die Nachteile von MPLS:

- Zeitaufwendige Implementierung und Skalierung
- Keine native Verschlüsselung
- Nicht für SaaS oder Public Clouds optimiert

Die Schwächen von IPSec-VPN auf Basis von Breitband-Internetverbindungen

VPNs können auch über das öffentliche Internet aufgebaut werden. Dabei wird der Datenschutz mit verschlüsselten Tunneln gewährleistet, zugleich profitieren die Unternehmen von den Kostenvorteilen von Breitband-Internetverbindungen. Viele VPNs greifen zum Aufbau dieser Tunnel auf die Protokollsuite IPSec zurück. Normalerweise zählen IPSec-VPNs zu den von Netzbetreibern angebotenen Services.

Da der Traffic über das öffentliche Internet befördert wird, das keine Dienstgütegarantien bietet, ist diese Art der WAN-Architektur naturgemäß weniger zuverlässig. Überlastungen, Ausfälle und Routingfehler sind nur einige der Faktoren, die bei der Nutzung des öffentlichen Internets die Performance und Konnektivität von IPSec-VPNs beeinträchtigen können. Die Quality of Service lässt sich zwar am Netzwerkrand mit speziellen Routern sicherstellen, doch sobald der Datenverkehr das Internet erreicht, wird nicht mehr zwischen den verschiedenen Traffic-Arten unterschieden. Das heißt beispielsweise, dass keine Priorisierung von Sprach- und Videoanrufen gegenüber weniger sensiblem Traffic, wie er etwa bei Backups anfällt, stattfindet.

Obendrein sind IPSecs-VPNs normalerweise nach dem Speichenmodell (Hub and Spoke) aufgebaut, bei dem Traffic aus verschiedenen Firmenstandorten an ein zentrales Rechenzentrum, den „Hub“, zurückgeleitet wird. Diese sternförmige Anordnung funktionierte solange gut, wie sich der Netzwerk-Traffic im Wesentlichen auf Geschäftsanwendungen beschränkte, die in einem zentralen Rechenzentrum gehostet wurden. Durch die Verbreitung von Public Cloud, SaaS und IoT sind allerdings ineffiziente Datenwege entstanden. Wenn beispielsweise ein Nutzer aus einem Büro in Singapur auf seine Firmen-E-Mails zugreifen möchte, muss der damit einhergehende Traffic unter Umständen selbst dann den Umweg über die USA nehmen, wenn der E-Mail-Provider Rechenzentren in Singapur betreibt. Diese langen Datenwege beeinträchtigen die Performance der Anwendung.

Die Vorteile von IPSec-VPN:

- Erschwinglich im Vergleich zu MPLS
- Größere betriebliche Agilität
- Native Verschlüsselung

Die Nachteile von IPSec-VPN:

- Weniger zuverlässig als MPLS
- Ineffiziente Hub and Spoke-Architektur
- Nur eine Serviceklasse

Die Schwächen eines hybriden Modells mit MPLS und Breitband-Internetverbindung

Manche Unternehmen entscheiden sich für ein hybrides WAN, indem sie sowohl MPLS als auch IPSec auf Breitband-Internetbasis einsetzen. Dadurch lassen sich auch Standorte einbinden, die von dem MPLS-Anbieter vielleicht nicht abgedeckt werden oder deren Anforderungen möglicherweise weniger komplex sind, zum Beispiel kleinere Einzelhandelsgeschäfte.

Bei diesem hybriden Ansatz wird zwar die Zuteilung der Datenrate optimiert, doch die Schwächen des jeweiligen Verfahrens werden damit nicht ausgemerzt. Die Installation und Verwaltung von Standleitungen und Breitbandanschlüssen verschiedener Service-Provider bringt weiterhin einen erhöhten Aufwand mit sich. Außerdem müssen an jedem Firmenstandort unterschiedliche Appliances für Sicherheit und Performance mühsam miteinander kombiniert werden, um die Mängel der beiden Verbindungsmodelle zum kompensieren.

Darüber hinaus bieten klassische WAN-Architekturen keine nativen Sicherheitsdienste, sodass bei jeder Firmenzweigstelle Lösungen wie Netzwerk-Firewalls, DDoS-Abwehr, WAN-Optimierung und Load Balancer angeschafft, installiert und verwaltet werden müssen, um die für moderne Geschäftsanwendungen benötigte Sicherheit, Performance und Zuverlässigkeit zu gewährleisten. Diese zusätzliche Netzwerk-Hardware bringt höhere Komplexität, Kosten, technische Schulden und ein unübersichtliches Netz an Abhängigkeiten mit sich.

Last, but not least: Man erhält man mit herkömmlichen WANs nur begrenzten Überblick über den Datenverkehr. Bruchstückhafte Performancezahlen aus LANs, Netzwerken von MPLS-Anbietern und dem öffentlichen Internet ergeben ein allenfalls lückenhaftes Bild. Was tun beispielsweise die Nutzer, wenn sie online sind? Wie wirksam ist eine bestimmte Sicherheitsrichtlinie? Und welche Apps benötigen die größte Bandbreite?

Die Vorteile hybrider WANs:

- Bessere Bandbreitenzuteilung
- Zuverlässiger (bei Einsatz von MPLS)
- Kosteneffizient (bei Einsatz von IPSec-VPNs)

Die Nachteile hybrider WANs:

- Keine native Sicherheitslösung
- Aufwendige Hardware-Verwaltung
- Lückenhafte Kontrolldaten

Die Vorzüge und Schwächen von SD-WANs

Um bestimmte Defizite herkömmlicher WAN-Architekturen auszugleichen, kombiniert SD-WAN eine Software an Firmenstandorten mit einem zentralen Controller. Auf diese Weise lässt sich Traffic, der vielfältige Datenwege nutzt – von Breitband-Internetverbindung über Standleitung bis hin zu MPLS –, über eine einzige Software-Plattform verwalten. Außerdem können Aufgaben im Rahmen der Netzwerküberwachung automatisiert und in Echtzeit Entscheidungen zur Steuerung des Traffics getroffen werden. Darüber hinaus lässt sich mit Direktverbindungen und Split Tunneling der Zugriff auf Public Cloud- und SaaS-Anwendungen optimieren.

Mit SD-WANs können Unternehmen ihre Kosten drücken, weil sich ihr Verwaltungsaufwand verringert und sie mit günstigeren Breitband-Internetverbindungen eine Zuverlässigkeit und Performance erreichen, wie man sie sonst nur von MPLS kennt. SD-WANs bringen aber ihre eigenen Probleme mit sich.

Ergänzender Sicherheitsdienst weiterhin erforderlich

SD-WANs erlauben zwar den Direktzugriff auf Public Cloud- und SaaS-Services von einem Firmenstandort, bieten aber nicht die volle Bandbreite an Sicherheitskontrollen, die von den meisten Unternehmen zum Schutz ihrer Perimeter benötigt werden. Das Angebot einiger Provider von SD-WAN-Lösungen umfasst grundlegende Firewall- und VPN-Funktionen, diese bieten aber normalerweise keinen wirklich belastbaren Schutz.

Die meisten Unternehmen können deshalb die Vorzüge der Lösung gar nicht nutzen, weil sie den Datenverkehr immer noch über diejenigen Rechenzentren leiten müssen, bei denen eine Firewall, ein Angriffserkennungs- und Data Loss Prevention-System sowie eine Lösung für den sicheren Webzugang aktiv sind.

Latenz bei Endnutzern

Wenn der Traffic einen Umweg über zentrale Standorte nehmen muss, leidet darunter die Qualität von datenintensiven Anwendungen wie Video- und Telefonieangeboten.

Durchgängig schlechte Dienstgüte

Durch SD-WANs sinken zwar Verwaltungsaufwand und Kosten, sie sind für die Datenübermittlung zwischen Standorten aber immer noch auf das unzuverlässige öffentliche

Internet angewiesen. Videokonferenzlösungen und andere Anwendungen, die empfindlich auf hohe Latenz reagieren und eine große Datenrate benötigen, funktionieren unter Umständen schlecht, wenn das Netzwerk gerade stark beansprucht wird. Einige SD-WAN-Provider unterhalten zwar eigene Backbone-Netzwerke, in den meisten Fällen handelt es sich aber um Edge-Lösungen, die keine durchgängig gute Anwendungserfahrung gewährleisten können.

Remote-Arbeit ist nicht abgedeckt

Inzwischen wird in vielen Branchen sowohl im Homeoffice als auch am Standort und im Außendienst gearbeitet; oft werden die verschiedenen Optionen auch kombiniert. Doch SD-WANs lassen sich nicht ohne Weiteres auf Remote-Arbeitsplätze ausweiten. Zwar können die Heim-LANs der Mitarbeiter theoretisch in das Firmennetzwerk integriert werden, das ist jedoch aus vielerlei Gründen nicht praktikabel. Die meisten SD-WAN-Technologien sind nicht darauf ausgelegt, dass sich einzelne Laptops mit dem Firmen-WAN verbinden. Die Mitarbeiter erwarten jedoch, die gleichen Zugriffsmöglichkeiten zu haben, wo auch immer sie sich befinden. Dafür müssen dem System Lösungen für einen Zero Trust-Netzwerkzugang hinzugefügt werden.

Die Vorteile von SD-WANs:

- Einfachere WAN-Verwaltung
- Geringere Betriebskosten
- Verbesserte Anwendungsperformance

Die Nachteile von SD-WANs:

- Ergänzende Sicherheitslösung erforderlich
- End-to-End-Dienstgüte nicht zufriedenstellend
- Schwierigere Einbindung von Remote-Mitarbeitern

WAN as a Service erfüllt die Anforderungen moderner Netzwerke

WAN as a Service ist ein Modell, mit dem man all der bisher geschilderten Probleme Herr werden kann. Es macht sich nicht nur die Vorzüge von SD-WANs zunutze, sondern bietet auch Lösungen für deren Defizite und erzielt so größere operative Flexibilität und niedrigere Gesamtbetriebskosten.

WAN as a Service umfasst folgende Funktionen:

- **Globales Netzwerk:** WAN as a Service greift auf ein weltumspannendes Netzwerk mit zahlreichen Rechenzentren zurück.
- **Vernetzung:** Dieses Netzwerk ist eng mit mit Internetdienstleistern, Cloud-Anbietern und privaten Firmennetzwerken verzahnt.
- **Integrierte Sicherheit:** Auf dem Netzwerk läuft die ganze Palette an Netzwerksicherheitsdiensten, darunter eine Firewall, DDoS-Abwehr und Zero Trust-Sicherheit.
- **Einheitliche Architektur:** Sämtliche WAN-Funktionen und Sicherheitsdienste werden auf jedem Server in jedem Rechenzentrum des Netzwerks ausgeführt.
- **Zentrales Dashboard:** Alle diese Services können über ein einziges Dashboard im Browser verwaltet werden.

Dank dieser Funktionen bietet WAN as a Service die folgenden Lösungen für typischerweise im Zusammenhang mit WAN und SD-WAN auftretende Probleme:

Schwäche	Vorteil von WAN as a Service
Flickwerk aus teuren althergebrachten Diensten und Netzwerk-Appliances	Bessere Performance von Anwendungen dank eines globalen Netzwerks mit integrierter Sicherheit
Firmeneigene Hardware-Appliances an jedem Standort nötig	Vollständig softwaredefiniert und cloudnativ, was maßgeschneiderte physische oder virtuelle Appliances überflüssig macht
Langsame MPLS-Skalierung	Kann schnell skaliert werden, um neue Bürostandorte und Tausende von Fernzugriffsanfragen über ein bestehendes, global verteiltes Netzwerk abzudecken
Höhere Verwaltungskosten und Ressourcenbeanspruchung	Die Bereitstellung als Service bedeutet, dass die Netzwerkverwaltung nun für das gesamte WAN als ein einziger Posten bei den Betriebskosten erscheint Kostspielige, remote oder vor Ort durchgeführte Wartungen entfallen
Von Engpässen im öffentlichen Internet betroffen	Bei WAN as a Service-Lösungen wird der Traffic zwar über das öffentliche Internet übermittelt, sie nutzen jedoch die Größe des ihnen zur Verfügung stehenden Netzwerks, um schnelle Datenwege ausfindig zu machen und überlastete Pfade zu umgehen
Längere Übertragungswege steigern Latenz	Dank Hunderter Netzwerkstandorte auf der ganzen Welt können mit WAN as a Service Workloads näher am Nutzer ausgeführt und durch Umleitung von Daten entstehende Verzögerungen vermieden werden. Dadurch verbessert sich insbesondere bei datenintensiven Echtzeit-Anwendungen die Performance
Sicherheitslücken und Ergänzungslösungen	Über eine einzige zentrale Steuerungsschnittstelle wird bei WAN as a Service eine tief integrierte und das gesamte Netzwerk schützende Sicherheitslösung (etwa eine softwaredefinierte Netzwerk-Firewall) an jedem Netzwerkstandort ausgeführt. Der Traffic kann nach IP, Port, Paketlänge und Bitfeld-Treffer gefiltert werden. Neue Regeln werden an allen Standorten sofort angewandt. Zur DNS-Filterung, für sichere Web-Gateways (SWG) mit Remote Browser Isolation und für den DDoS-Schutz können zusätzliche Sicherheitsfunktionen eingebunden werden
Fragmentierte Netzwerk-Analytics und Kontrolldaten	Mit WAN as a Service steht Unternehmen ein zentrales Analytics-Dashboard zur Verfügung, mit dem sie sich einen Überblick über den gesamten WAN-Datenverkehr verschaffen können und das Ihnen Erkenntnisse darüber liefert, wie und von wem das Netzwerk genutzt wird
Remote-Arbeit ist nicht abgedeckt	WAN as a Service kann auch Remote-Nutzer und -Endpunkte einbinden. Anstatt den gesamten Traffic aus Remote-Quellen durch ein einziges Nadelöhr (wie VPN-Konzentratoren im „Perimeter“ eines Firmennetzwerks) zu routen, gelangt er zum nächstgelegenen Edge-Standort und wird über optimierte Datenwege weitergeleitet. Das ermöglicht eine überragende Anwendungsperformance und verbessert standortunabhängig die Benutzererfahrung

Der Verwaltungsaufwand für die gleichzeitige Aufrechterhaltung von MPLS- und Internetverbindungen mit einem SD-WAN-Controller und internen Routern bindet Ressourcen und schmälert die Performance. Demgegenüber ist Komfort und Funktionstüchtigkeit bei der Magic WAN-Lösung von Cloudflare ein integraler Bestandteil des gebotenen Service.

Cloudflare betreibt eines der größten Netzwerke der Welt, mit Rechenzentren an mehr als 200 strategisch günstig gelegenen Standorten in 100 Ländern. Unser Netzwerk ist betreiberunabhängig und unterhält Verbindungen zu über 9.500 großen Internetdienstanbietern, Cloud-Service-Providern und Unternehmen. Jeder Sicherheits- und Performancedienst ist über jeden Server in jedem Rechenzentrum unseres Netzwerks verfügbar.

Magic WAN ersetzt althergebrachte WAN-Architekturen durch das Cloudflare-Netzwerk und kombiniert dabei ein einfaches und zentrales Nutzerinterface mit globalen Verbindungsmöglichkeiten, integrierter Sicherheit und hoher Performance.

Weitere Informationen finden Sie unter cloudflare.com/de-de/magic-wan