Magic WAN

Magic WAN vereinfacht den Weg zu SASE mit Any-to-Any-Konnektivität

Die Weiterentwicklung der Netzwerkarchitektur

Das Internet als neues Firmennetzwerk

Hybrides Arbeiten ist heute Normalität und Anwendungen wandern zunehmend in die Cloud. Das stellt IT-Abteilungen vor Herausforderungen:

- **Netzwerkkomplexität:** Die Bereitstellung per MPLS und die Anpassung von Einzellösungen kostet zu viel Zeit
- **Sicherheitslücken:** Direkte Verbindungen mit dem Internet umgehen Sicherheitsvorkehrungen und Richtlinien zur akzeptablen Nutzung, was Anwender und Daten Risiken aussetzt
- **Hohe Kosten:** MPLS-Links und Sicherheits-Einzellösungen verursachen unnötige Ausgaben
- **Schlechte Nutzererfahrung:** Die Umleitung des Traffic zu einem perimeterbasierten Sicherheitsstack steigert die Latenz

Magic WAN vereinfacht die Netzwerkanbindung von Zweigstellen, Multi-Virtual Private Clouds oder Rechenzentren an die SASE-Plattform Cloudflare One. Die Lösung ermöglicht eine sichere, leistungsstarke und kosteneffiziente Konnektivität. So können IT-Abteilungen die mit hybridem Arbeiten und Multi-Cloud-Architekturen verbundenen Herausforderungen meistern.

Im Gegensatz zu unflexiblen und teuren MPLS-Netzwerken oder komplizierten SD-WAN-Implementierungen, die sich auf lokale Firewalls stützen, folgt Magic WAN einem „Light Branch, Heavy Cloud“-Ansatz zur Verstärkung bzw. zum Ersatz der aktuellen Architektur. Die Lösung bietet integrierte Sicherheit, lässt sich leicht einführen und ist im Einklang mit den geschäftlichen Anforderungen skalierbar.

Magic WAN verbindet physische oder virtuelle Netzwerkstandorte mit der SASE-Plattform von Cloudflare. Physische Standorte können beispielsweise Zweigstellen, Fabrikhallen, Einzelhandelsfilialen, Hauptgeschäftsstellen oder Rechenzentren sein. Beispiele für virtuelle Standorte sind Public Cloud-Dienste wie AWS, Azure, GCP und OCI.

Größere betriebliche Flexibilität

Netzwerksicherheit und -konnektivität werden über eine einzige Verwaltungskonsole gesteuert. Der Traffic kann binnen Minuten per Zero Touch-Konfiguration eingebunden werden.

Integrierte, nicht nachträglich hinzugefügte Sicherheit

Cloudnativer DDoS-Schutz, Netzwerk-Firewall, SSE und Zero Trust-Funktionen – alles tief integriert und im „As a Service“-Modell bereitgestellt.

Geringere Netzwerkkosten

Eine Verkleinerung des Fußabdrucks von Zweigstellen und die Verlagerung von Netzwerkfunktionen in die Cloud verringern die Abhängigkeit von teurem MPLS und ermöglichen die Abschaffung von SD-WAN.

Die wichtigsten Anwendungsfälle für Magic WAN

Optimierung der Netzwerkkonnektivität

- **Anbindung von Zweigstellen vereinfachen**: Um den Datenverkehr zwischen Zweigstellen und Rechenzentren sicher zu übermitteln, wird ein Flickwerk aus firmeneigenen Leitungen und Netzwerkgeräten ersetzt. Anycast-IPSec erleichtert die Verbindung zwischen Standorten.
- **Hybrid- und Multi-Cloud-Anbindungen vereinfachen**: Unternehmen betreiben Anwendungen in Cloud-Instanzen verschiedener Anbieter (z. B. AWS, GCP, Azure, Oracle, IBM) *und* in lokalen Rechenzentren. Zur Absicherung und Übermittlung von Datenverkehr in diesen unterschiedlichen Umgebungen können zentrale Kontrollen genutzt werden.

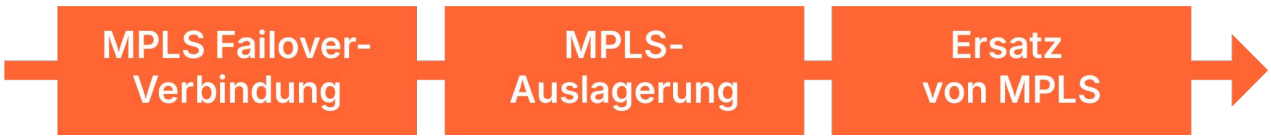
Mehr Sicherheit ohne Abstriche bei der Performance

- **Geschützte WAN-Verbindungen**: Ermöglicht wird dies durch die Durchsetzung von Richtlinien zur Netzwerksicherheit an verschiedenen Standorten (Zweigstellen, Rechenzentren usw.) mit Kontrollmöglichkeiten für Firewalls und SWG über die Cloud.
- **Skalierung der WAN-Leistung**: MPLS-Implementierungen sind teuer, unflexibel und langsam. Ein Wechsel zu Cloudflare ermöglicht Kostensenkungen sowie eine agilere Bereitstellung mit integrierter Sicherheit.

So klappt die Einführung von Magic WAN

Eine Netzwerktransformation ist ein längerer Prozess

Magic WAN bietet ebenso leistungsstarke wie zuverlässige Internetverbindungen und unterstützt beim Wechsel von alten Netzwerkarchitekturen. Durch die schrittweise Implementierung von Magic WAN gelingt die Umstellung in mehreren Etappen. Die Cloudflare-Kombination aus Konnektivität auf der letzten Meile und Performance, Zuverlässigkeit und Sicherheit auf der mittleren Meile nach dem Prinzip „Light Branch, Heavy Cloud“ hilft bei der besseren Vernetzung und Absicherung hybrider Arbeit. Unsere Architektur unterstützt die Implementierung parallel zu bereits bestehender Infrastruktur für eine Migration in Ihrem eigenen Tempo.



Cloudflare One, MPLS und SD-WAN im Vergleich

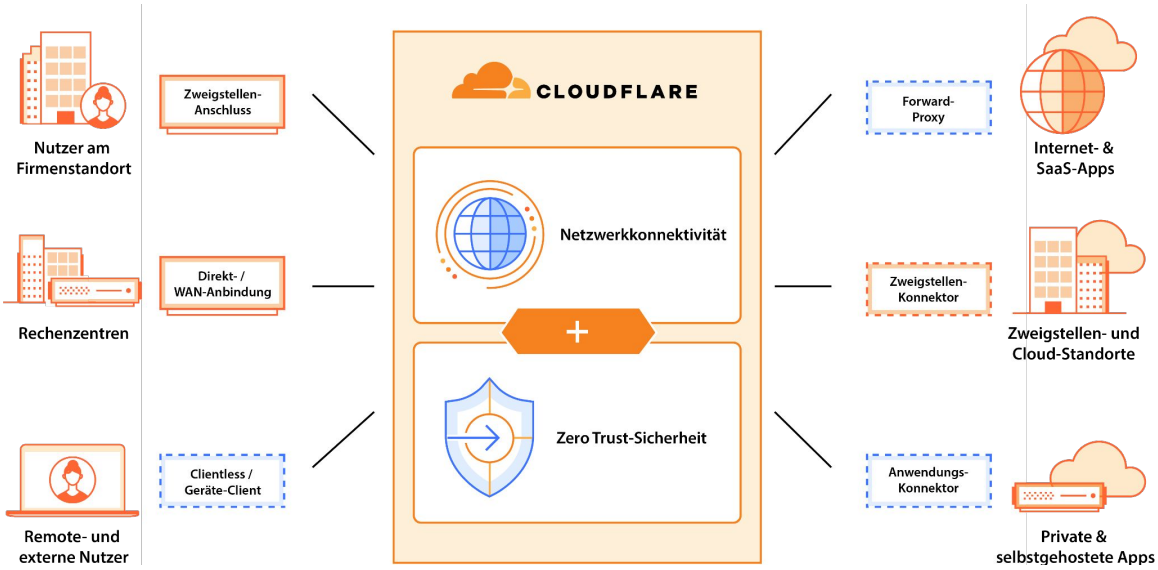
Die Verlagerung von Anwendungen in die Cloud und die Verbreitung hybrider Arbeit beeinträchtigen die Leistung und das Sicherheitsniveau herkömmlicher Netzwerkarchitekturen. Das Umleiten von Traffic für Sicherheitsprüfungen verschlechtert Performance und Nutzererfahrung. Zugleich werden Sicherheitsmaßnahmen durch lokale Breakouts verwässert. Nichts davon ist erstrebenswert. Infolgedessen werden bei der Gestaltung von Netzwerken Kompromisse gemacht, die weder Unternehmen noch Anwender zufriedenstellen.

In der jüngsten Zeit wurden dem SD-WAN überlagernde Netzwerke hinzugefügt, um den Traffic zu verwalten und nach Möglichkeit eine MPLS-Alternative zu bieten. Allerdings ist SD-WAN zur Implementierung von Sicherheitsmaßnahmen überwiegend auf Edge-Geräte angewiesen. Das bedeutet, dass Hardware, virtualisierte und cloudbasierte Tools mehr schlecht als recht miteinander in Einklang gebracht werden. Die erhöhte Komplexität, die dies mit sich bringt, macht die angestrebten Vorteile zu einem nicht unerheblichen Teil zunichte.

Die SASE-Plattform von Cloudflare führt Sicherheits- und Netzwerkdienste in unserer Connectivity Cloud zusammen und erlaubt es Unternehmen, unser Netzwerk als Verlängerung ihres eigenen zu nutzen. Vereinfachte Verwaltung, zuverlässige Performance, moderne Zero Trust-Sicherheit und niedrigere Gesamtbetriebskosten sind zusammen nur möglich, wenn SASE völlig neu gedacht wird.

Kriterien	MPLS/VPN-Dienst	SD-WAN	SASE mit Cloudflare One
Konfiguration Einrichtung, Konfiguration und Verwaltung neuer Standorte	Durch Managed Service Provider über Service-Anfrage	Vereinfachte Orchestrierung und Verwaltung über eine zentrale Steuerung	Automatisierte Orchestrierung über SaaS-Portal; zentrales Dashboard
Traffic-Kontrolle auf der letzten Meile Verteilung des Traffic, QoS und Failover	Abgedeckt durch MPLS-SLA	Auswahl des besten Pfads in SD-WAN-Appliance verfügbar	Minimale Implementierung vor Ort zur Kontrolle der lokalen Entscheidungsfindung
Traffic-Kontrolle auf der mittleren Meile Traffic-Lenkung bei Überlastung der mittleren Meile	Abgedeckt durch MPLS-SLA	Tunnel-Chaos und keine Kontrolle auf der mittleren Meile	Integrierte Traffic-Verwaltung und private Backbone-Kontrollen über dieselbe Benutzeroberfläche
Cloud-Integration Konnektivität für Cloud-Migration	Zentraler Breakout	Dezentraler Breakout	Native Konnektivität mit Cloud Network Interconnect
Sicherheit Filterung des ein- und ausgehenden Internettraffics auf Malware	Flickwerk aus verschiedenen Hardware-Kontrollen	Flickwerk aus Hardware- und/oder Software-Kontrollen	Native Integration mit Tools für Nutzer-, Daten-, Anwendungs- und Netzwerksicherheit
Kosten Nutzenmaximierung von Netzwerkinvestitionen	Hohe Kosten für Hardware und Konnektivität	Optimierung der Konnektivitätskosten, zugleich aber Steigerung der Hardware- und Softwarekosten	Geringere Hardware- und Konnektivitätskosten für maximalen Nutzen

Datenverkehr wird zur SASE-Plattform von Cloudflare geleitet



Mit dem Magic WAN Connector lassen sich Netzwerkstandorte ganz leicht mit Cloudflare verbinden. Die Software für den Zweigstellenanschluss kann vorinstalliert und bereits konfiguriert auf einer Cloudflare-zertifizierten Hardware-Appliance für eine reibungslose Bereitstellung eingesetzt werden. Alternativ lässt sie sich auf physischen oder virtuellen Linux-Appliances innerhalb einer Umgebung installieren.

Teil einer wachsenden Zahl von flexiblen Einbindungsmöglichkeiten

Der erste Schritt zur Einführung von SASE besteht darin, eine Verbindung herzustellen, d. h. einen sicheren Pfad vom bestehenden Netzwerk zum nächstgelegenen Standort zu schaffen, an dem Zero Trust-Sicherheitsrichtlinien angewendet werden können. Cloudflare bietet zur Ermöglichung dieser Anbindung eine breite Palette von Zugangsmöglichkeiten („On-Rampings“) an. Dazu gehören auch clientbasierte und clientlose Zugriffsoptionen für Nutzer hybrider Arbeitsumgebungen, Tunnel auf Anwendungsschicht, die mithilfe eines schlanken Software-Daemons eingerichtet werden, Konnektivität auf Netzwerkschicht mit Anycast-fähigen GRE- oder IPsec-Tunneln sowie physische oder virtuelle Interconnection für private Rechenzentren und öffentliche Clouds.

Um die Einführung von SASE noch weiter zu erleichtern, kann der Magic WAN Connector an jedem beliebigen physischen oder cloudbasierten Netzwerkstandort eingesetzt werden, um eine automatische Verbindung zu dem am besten geeigneten Cloudflare-Rechenzentrum herzustellen. Dabei wird die bestehende Internetverbindung auf der letzten Meile genutzt und die IT-Teams müssen zur Herstellung einer Verbindung die Netzwerkgeräte nicht mehr manuell konfigurieren.

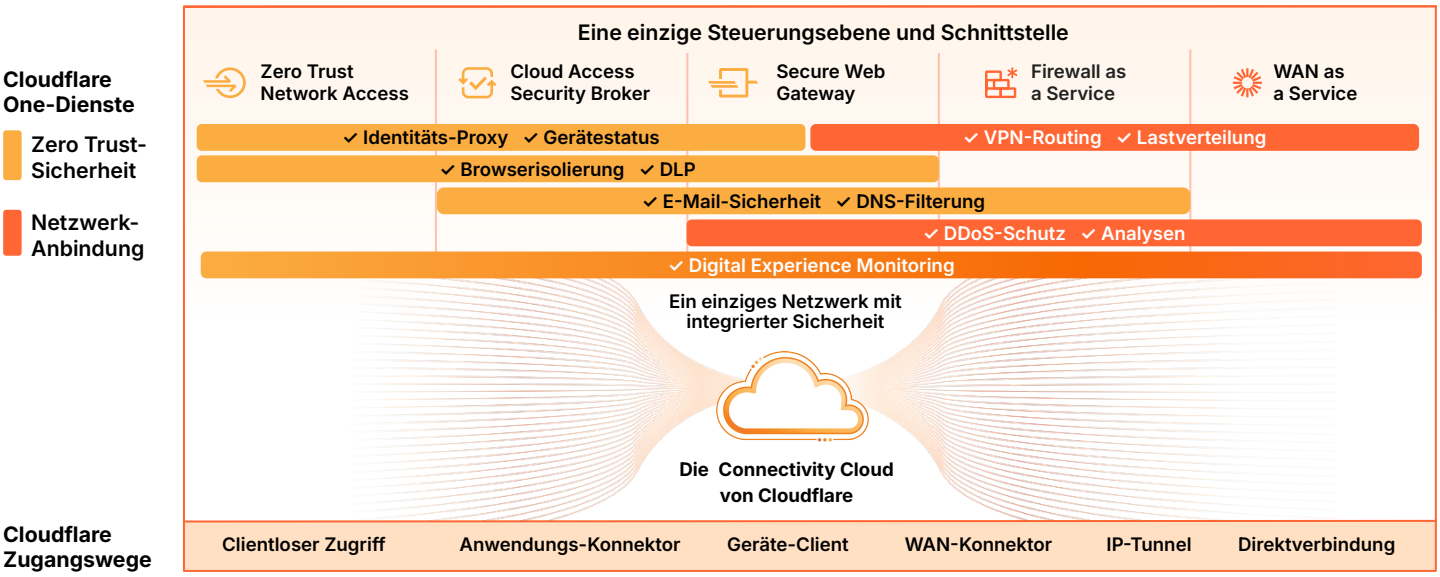
Softwarefunktionen und Hardwarespezifikationen

Funktionen der Magic WAN-Software[1]	
Einrichtung des WAN-Anschlusses	Plug-and-Play, Zero Touch-Bereitstellung von Teilnehmernetz-Geräten, die zentral über das Dashboard/die API von Cloudflare verwaltet werden. Automatische Einrichtung von IPsec-Tunneln und Routen für die Weiterleitung des Datenverkehrs an das Cloudflare-Netzwerk zur Anwendung von Konnektivitäts- und Sicherheitsdiensten. Automatische Software-Upgrades (innerhalb des vom Kunden definierten Servicefensters).
WAN-Connector-Standortkonfiguration	WAN/LAN-Unterstützung für statische IP- oder DHCP-Konfigurationen. Unterstützung von VLAN und lokaler Netzwerksegmentierung.
„Light Branch, Heavy Cloud"-Ansatz	Hochverfügbarer, schlanker WAN-Connector mit Lastverteilung und Failover über mehrere WAN-Verbindungen auf Grundlage von Zustandsprüfungen. Sicherheitsdienste wie Firewall- und Zero Trust-SSE-Funktionen werden von der Connectivity Cloud von Cloudflare bereitgestellt.
Integration von Drittanbietern	Anycast IPsec- oder GRE-Tunnel-Endpunkte können mit bestehenden VPC wie Amazon AWS Transit Gateway oder kundeneigener Ausrüstung wie SD-WAN-, Firewall- und Router-Geräten konfiguriert werden. Statische Routen sind mit ECMP-Paketweiterleitung an das Cloudflare-Netzwerk konfigurierbar.
Integrierte Sicherheit	Integrierte L3-Firewall und Erkennung von Eindringlingen; nahtlose Integration in andere SSE-/Sicherheitsfunktionen und On-Ramping-Möglichkeiten wie Secure Web Gateway auf L4–7, Geräte-Client, Anwendungs-Anschluss usw.
Überblick und Kontrolle	Erkennung und Routing von Traffic auf Anwendungsgrundlage. Bandbreitenkontrolle. Übersicht über/Analysen für Tunnel, Kennzahlen für Traffic und Geräte über das Dashboard, API, Protokolle oder GraphQL verfügbar. Verwaltung über das Cloudflare-Dashboard, API oder Terraform.
Spezifikationen der Magic WAN Connector-Hardware-Option[2]	
Geräte-Spezifikationen	• **Ports:** (6× 1G Copper RJ45) + (2× 10G SFP+) + (2x USB 3.0 Typ A) • **Abmessungen:** 8.1×7.9×2.0 Zoll; 1.5RU; **Gewicht:** ca. 1,3 kg • **Montageoptionen:** Tischaufstellung, Wandmontage oder Rackmontage (mit Ablage) • **TPM:** 2.0, weltweit außer China • **CPU:** Denverton 4 Core C3558 • **Festplatte:** M.2 120 SSD mit 16G eMMC Flash • **RAM:** 8 GB DDR4 • **WLAN und Bluetooth:** 802.11ac, 2×2 MIMO, max. PHY-Rate: 866,7 Mbit/s • **Lüfterzahl:** 1

[1] Die gesamten Unterlagen zu den Magic WAN-Funktionen finden Sie in der Cloudflare Dokumentation.
[2] Cloudflare-zertifizierte Hardware mit vorinstallierter Magic WAN-Software: Dell VEP 1425 erhältlich über Partner (mit Rackmontage)

Netzwerkkonnektivität und der Weg zu SASE

Die Connectivity Cloud von Cloudflare bietet die einfache Bereitstellung, Netzwerkstabilität und Innovationsgeschwindigkeit, die Sie benötigen, um bei der Konsolidierung von Einzelprodukten und der Konvergenz zu einer einheitlichen IT-Strategie die Nase vorn zu haben.



Cloudflare One ermöglicht Unternehmen jeder Größe den Wechsel zu SASE: Jeder Traffic-Quelle kann mit jedem Ziel verbunden werden. Das geschieht über ein sicheres, schnelles und zuverlässiges weltumspannedes Netzwerk, in dem alle Sicherheitsfunktionen durchgesetzt werden und der Datenverkehr auf dem Weg zu seinem Ziel optimiert wird, ob innerhalb eines privaten Netzwerks oder im öffentlichen Internet.

Unabhängig davon, ob Ihr Unternehmen den Datenverkehr aus ausgereiften MPLS- oder SD-WAN-Implementierungen auslagert oder zum ersten Mal eine Netzwerkmodernisierung in Angriff nimmt, kann Magic WAN zur Vereinfachung beitragen. Cloudflare One bietet sowohl Zero Trust-Sicherheit als auch WAN as a Service, um ein SASE-Modell aus einer Hand zu ermöglichen. Unsere Lösung kann aber auch eine Multi-Vendor-Strategie ergänzen, um bei der Umstellung auf das SASE-Konzept zu unterstützen.

Netzwerkanbindung für Ihr Unternehmen

Für Workshop anmelden

CLOUDFLARE

Noch nicht bereit für ein persönliches Gespräch?

In unserer SASE-Referenzarchitektur **erfahren Sie mehr.**