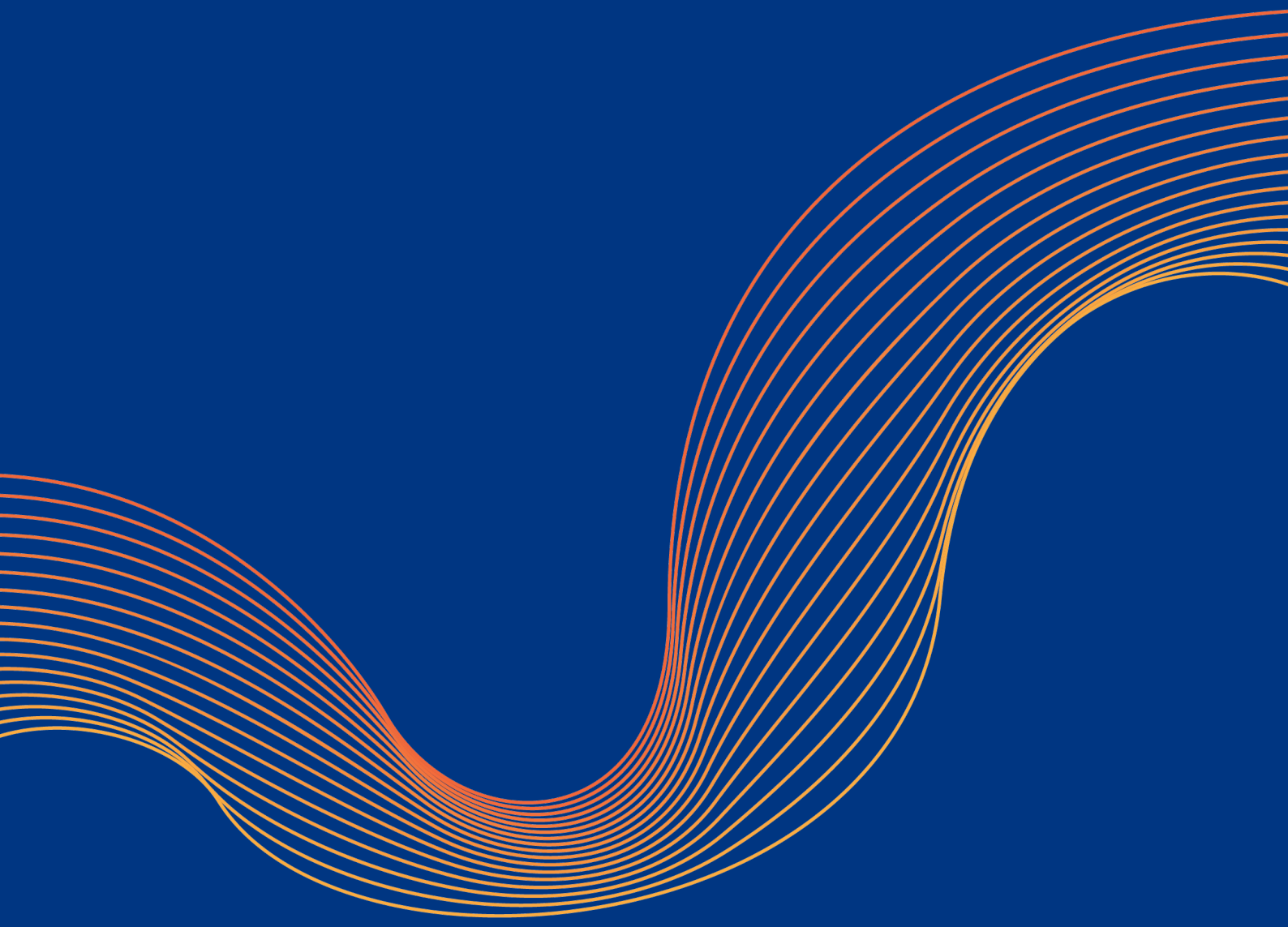
WHITEPAPER

CLOUDFLARE®

Magic Transit: Anwendungsfälle und Referenzarchitektur



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

INHALT

Einleitung

In diesem Dokument werden die Hauptarchitektur, die Funktionalitäten und die Netzwerkeinsatzoptionen von Cloudflare Magic Transit beschrieben. Magic Transit ist ein BGP-basierter DDoS-Schutz- und Traffic-Beschleunigungsdienst für die Netzwerkinfrastruktur im Internet.

KAPITEL ZWEI

Was ist Magic Transit?

Um die Netzwerkinfrastruktur vor DDoS-Angriffen zu schützen, bedarf es einer einzigartigen Kombination aus Stärke und Geschwindigkeit. Volumetrische Angriffe können Hardware-Boxen und deren bandbreitenbeschränkte Internetverbindungen leicht überfordern. Die meisten cloudbasierten Lösungen leiten den Datenverkehr an zentralisierte Scrubbing-Zentren um, was die Performance des Netzwerks erheblich beeinträchtigt.

Cloudflare Magic Transit bietet Schutz vor DDoS-Angriffen und eine Beschleunigung des Traffic für lokale, cloudbasierte und hybride Netzwerke. Mit Rechenzentren in 250 Städten und mehr als 100 Tbit/s Abwehrkapazität kann Magic Transit weltweit in durchschnittlich weniger als 3 Sekunden Angriffe in der Nähe ihres Ursprungs erkennen und neutralisieren. Zugleich wird der Traffic schneller geroutet als über das öffentliche Internet.

Im Wesentlichen funktioniert Magic Transit folgendermaßen:

Connect: Durch die Verwendung von Border-Gateway-Protocol-(BGP)-Routenankündigungen an das Internet und das Anycast-Netzwerk von Cloudflare wird der Kunden-Traffic in einem Cloudflare-Rechenzentrum in der Nähe der Quelle erfasst.

Schützen und Verarbeiten: Der gesamte Kunden-Traffic wird auf Angriffe überprüft. Fortgeschrittene und automatisierte Schadensbegrenzungstechniken werden unmittelbar nach dem Erkennen eines Angriffs angewendet. Zusätzliche Funktionen wie Lastverteilung, Next-Generation-Firewall, Content Caching und Serverless Computing sind als Dienst verfügbar.

Beschleunigen: Der saubere Traffic wird für einen optimalen Durchsatz über die latenzarmen Netzwerkverbindungen von Cloudflare geroutet und über IP-Tunnel (GRE oder IPsec) oder private Netzwerkverbindungen (PNI) an das Ursprungsnetzwerk weitergeleitet. Magic Transit verwendet Anycast-IP-Adressen für die Tunnelendpunkte von Cloudflare, was bedeutet, dass jeder Server in jedem Rechenzentrum in der Lage ist, Pakete für denselben Tunnel zu integrieren und zu desintegrieren. Weitere Einzelheiten zu Tunneln und Integration finden Sie hier.

Mit Anycast bringen wir Ausfallsicherheit in unser Netzwerk:

Magic Transit verwendet Anycast-IP-Adressen für seine Endpunkte des Netzwerktunnels. Ein einziger Tunnel, der vom Netzwerk eines Kunden zu Cloudflare konfiguriert wird, verbindet sich also mit allen globalen Rechenzentren von Cloudflare (mit Ausnahme des China-Netzwerks). Für den Router stellt das keine zusätzliche Belastung dar, denn aus seiner Sicht handelt es sich um einen einzigen Tunnel zu einem einzigen IP-Endpunkt.

Das funktioniert, weil der Tunnelendpunkt zwar an eine IP-Adresse gebunden ist, aber nicht an ein bestimmtes Gerät. Jedes Gerät, das die äußeren Header entfernen und anschließend das sich darunter befindliche Datenpaket weiterleiten kann, ist auch in der Lage, jedes beliebige über den Tunnel gesendete Paket zu verarbeiten.

Bei einem Netzwerkausfall oder anderen Problemen werden die Tunnel automatisch umgeschaltet (Failover), ohne dass die Performance des Kundennetzwerks beeinträchtigt wird.

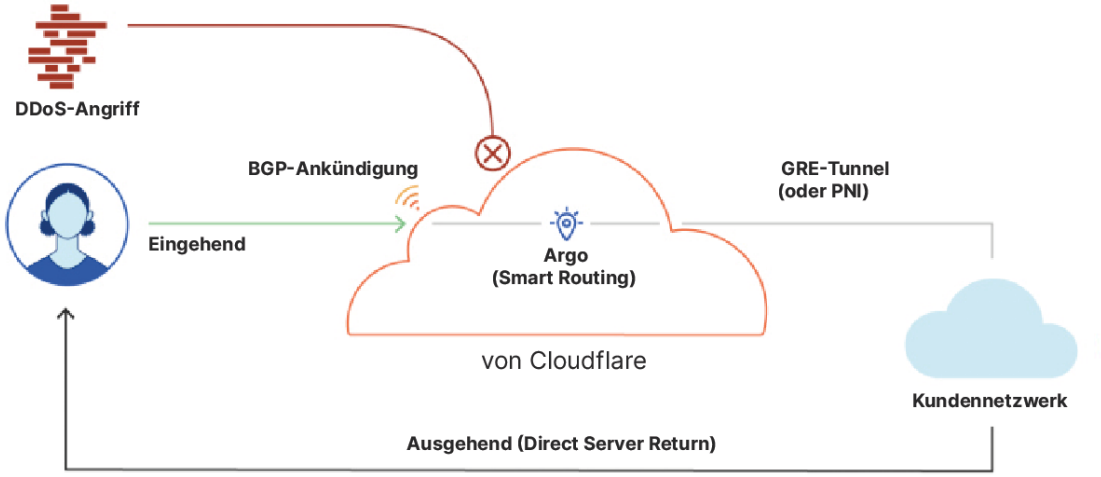


Abbildung 1: Magic Transit – Überblick

3.1. Bereitstellungsarchitekturen für Magic Transit

3.1 Standardkonfiguration (nur Ingress, Direct-Server-Return)

Standardmäßig verarbeitet Magic Transit nur eingehenden Traffic (Ingress; vom Internet zum Kundennetzwerk). Der Server-Return-Traffic zu den Clients wird vom RZ-Edge-Router des Kunden über seine Uplinks zum Internet/ISP auf der Grundlage der Standard-Routing-Tabelle des Edge-Routers geroutet. Dieser Server-Return-Traffic wird nicht durch Cloudflare über Tunnel geleitet. Dies wird als Direct Server Return (DSR) bezeichnet.

Das Netzwerkdiagramm in Abbildung 2 veranschaulicht eine solche Magic Transit-Implementierung und den Ende-zu-Ende-Paketfluss des durch Magic Transit geschützten Datenverkehrs. Der Tunnel in dieser Konfiguration verwendet für die Integration GRE.

- Cloudflare stellt dem Kunden ein Paar Anycast-IP-Adressen für das Cloudflare-Ende der Tunnelendpunkte zur Verfügung. Dies sind öffentlich routbare IP-Adressen aus dem Cloudflare-eigenen Adressraum. Das Paar von Anycast-IP-Adressen kann verwendet werden, um zwei Tunnel für die Netzwerkredundanz zu konfigurieren, obwohl nur einer für eine Grundkonfiguration erforderlich ist. Die obige Konfiguration zeigt einen einzelnen Tunnel, wobei die Adresse des Cloudflare-Endpunkts 192.0.2.1 lautet.
- Das kundenseitige Ende des Anycast GRE-Tunnels muss eine öffentlich routbare Adresse sein. Es handelt sich in der Regel um die IP-Adresse der WAN-Schnittstelle auf dem Edge-Router des Kunden. In diesem Beispiel ist es 192.0.2.153.
- Die IP-Adressen der Tunnelschnittstellen sind private RFC1918-Adressen. Sie sind im Tunnelheader integriert und werden nur von den beiden Endpunkten des Tunnels gesehen, sobald sie von ihnen integriert wurden (d.h. von den Cloudflare-Servern und dem Edge-Router des Kunden), nachdem die integrierten Pakete über das Internet transportiert wurden.

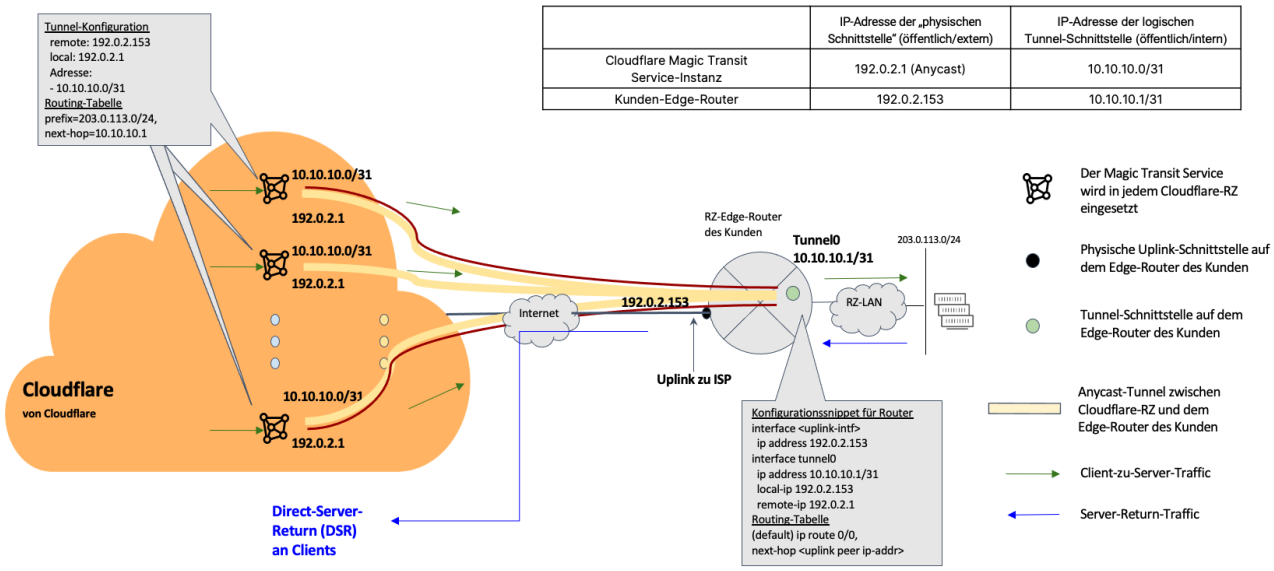


Abbildung 2: Referenzkonfiguration von Magic Transit Anycast Tunnel (GRE) mit Standard-DSR-Option

- Diese Tunnelschnittstellenadressen sind nur innerhalb der jeweiligen Magic Transit-Service-Instanz, zu der sie gehören, „lokal signifikant“. Daher kann der Kunde beliebige RFC1918-Adressen auswählen, solange sie sich nicht mit denen anderer Tunnel überschneiden, die innerhalb derselben Magic Transit Service-Instanz konfiguriert sind.
- Da es sich bei den Tunneln um Punkt-zu-Punkt-Verbindungen handelt, ist ein /31-Subnetz für die Zuweisung der 2 IP-Adressen, die für einen bestimmten Tunnel benötigt werden, ausreichend. Im obigen Beispiel wird das 10.10.10.0/31 Subnetz gewählt, wobei das Cloudflare-Ende der Tunnelschnittstelle 10.10.10.0/31 und die Seite des DC-Edge-Routers des Kunden 10.10.10.1/31 ist.
- Sobald der/die Tunnel konfiguriert ist/sind, wird/werden in der Magic Transit Service-Instanz eine statische Route konfiguriert, um den für ein bestimmtes Kundenpräfix bestimmten Traffic an den richtigen Tunnel weiterzuleiten.
- Der für das Kundenpräfix 203.0.113.0/24 bestimmte Traffic wird über den Tunnel geleitet, dessen entferntes Ende (d.h. das Ende des Kunden aus Sicht des Cloudflare-Netzwerks) der Tunnelschnittstelle 10.10.10.1 ist.
- Da es sich um eine DSR-Implementierung (Direct Server Return) handelt, folgt der Server-Return-Traffic der Standardroute (ip route 0/0), die auf dem Edge-Router des Kunden konfiguriert ist, und wird an seinen Uplink-Peer (d.h. den Router des ISP des Kunden) gesendet, auf dem Weg zurück zu den Clients aus dem Internet.

Hinweis: Die kleinste IP-Präfixgröße (d.h. mit der längsten IP-Subnetzmaske), die die meisten ISPs in ihren BGP-Ankündigungen gegenseitig akzeptieren, ist /24; z.B. sind x.x.x.0/24 oder y.y.y.0/23 in Ordnung, aber z.z.z.0/25 nicht. Daher ist die kleinste IP-Präfixgröße, die Cloudflare Magic Transit im Namen der Kunden ankündigen kann, /24.

3.2 Magic Transit mit aktivierter Egress-Option

Wenn Magic Transit mit aktivierter Egress-Option bereitgestellt wird, fließt der Egress-Traffic aus dem Kundennetzwerk ebenfalls über das Cloudflare-Netzwerk. Diese Art der Bereitstellung sorgt für einen symmetrischen Traffic-Fluss, bei dem sowohl der Client-zu-Server- als auch der Server-Return-Traffic durch das Cloudflare-Netzwerk fließt. Diese Implementierung bietet zusätzliche Sicherheit und Zuverlässigkeit für den Server-Return-Traffic, die durch das Cloudflare-Netzwerk gewährleistet werden.

Das folgende Netzwerkdiagramm veranschaulicht den End-to-End-Paketfluss zwischen dem Endkunden und dem Kundennetzwerk, wenn die Option Magic Transit Egress aktiviert ist.

- Der Traffic-Fluss beim eingehenden Traffic ist der gleiche wie in Anwendungsfall 3.1.
- Damit der ausgehende Traffic von Magic Transit empfangen und verarbeitet werden kann, müssen die Quell-IP-Adressen des Datenverkehrs im Bereich der von Magic Transit geschützten IP-Präfixe liegen und die Ziel-IP-Adressen müssen im öffentlichen Internet routbar sein, d.h. Nicht-RFC1918-Adressen.

Für Kunden, die ihre eigenen öffentlichen IP-Adressen (BYOIP) für in der Cloud gehostete Dienste mitbringen, kann die Magic Transit Egress-Option einen zusätzlichen Mehrwert bieten. Für sie entfällt die Notwendigkeit, BYOIP-Dienste bei ihren Cloud-Anbietern zu erwerben und zu implementieren, was ihre Cloud-Rechnung senkt und die Betriebskosten verringert.

Um dies zu erreichen, werden die IP-Tunnel, die zu Magic Transit führen, zwischen den VPCs der Cloud-Anbieter und dem Cloudflare-Netzwerk konfiguriert. Mit der Egress-Option von Magic Transit würde der Client-Server-Traffic in beide Richtungen durch diese(n) Tunnel fließen. Die BYOIP-Adressen in den getunnelten Paketen werden hinter den äußeren Tunnelendpunkt-IP-Adressen und dem Tunnelheader versteckt. Damit werden sie für die zugrunde liegenden Cloud-Provider-Netzwerkelemente zwischen den VPCs und dem Cloudflare-Netzwerk „unsichtbar“.

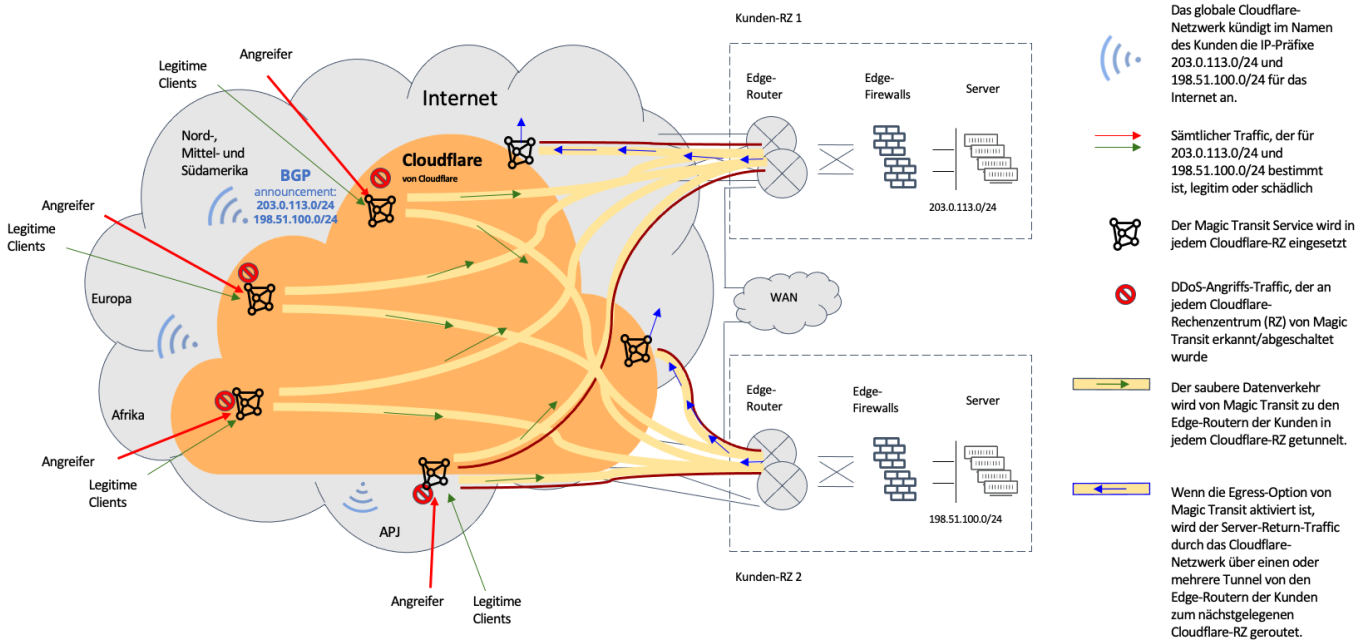


Abbildung 3: Magic Transit mit aktivierter Egress-Option

3.3 Magic Transit über Cloudflare Network Interconnect (CNI)

Cloudflare Network Interconnect (CNI) ermöglicht es Kunden, ihre Netzwerkinfrastruktur direkt mit Cloudflare zu verbinden. Sie umgehen damit das öffentliche Internet und erhalten eine zuverlässigere, performantere und sicherere Verbindung. Weitere Einzelheiten zu CNI finden Sie hier.

- CNI wird von den Cross-Connect-Anbietern als eine Reihe von Layer-2-Verbindungen bereitgestellt. Cloudflare weist für jede Verbindung ein Paar IP-Adressen aus dem eigenen Internet-routbaren IP-Adressblock von Cloudflare zu.
- Während des CNI-Onboardings koordiniert Cloudflare mit dem Kunden die Konfiguration dieser Links und den Aufbau einer BGP-Peering-Sitzung über die Links.
- Sobald die BGP-Sitzung zwischen dem Cloudflare-Netzwerk und dem Edge-Router des Kunden, die über CNI verbunden sind, aufgebaut ist, werden Cloudflare-eigene Präfixe über diese CNI-Verbindung an den Edge-Router des Kunden angekündigt.

Abbildung 4 zeigt eine Referenzkonfiguration für Magic Transit über CNI und den damit verbundenen Paketfluss.

Hinweis: Das hier gezeigte Beispiel bezieht sich auf den standardmäßigen Magic-Transit-Service ohne aktivierte Egress-Option. Wie in früheren Abschnitten beschrieben, wird der Server-Return-Traffic im Magic Transit Direct Server Return-Modus (d.h. nur Ingress) vom Edge-Router des Kunden über das öffentliche Internet zu den Clients über deren ISP geroutet.

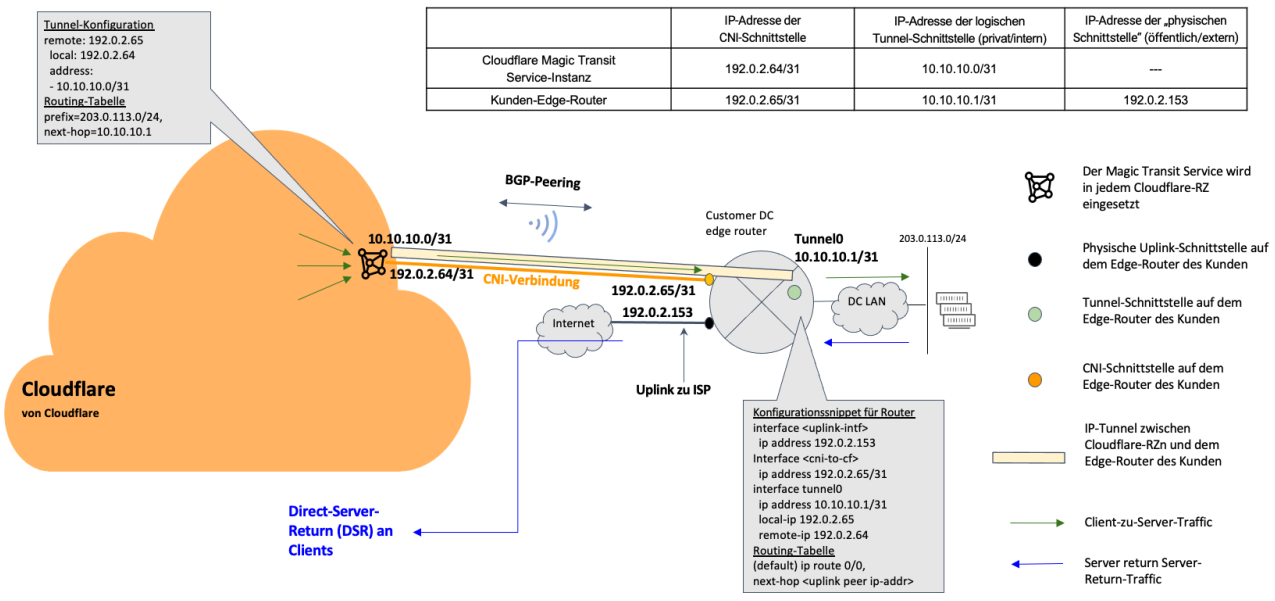


Abbildung 4: Referenzkonfiguration von Magic Transit über CNI (Standard-DSR-Option)

Wenn die Egress-Option von Magic Transit aktiviert ist und genutzt wird, kann der Server-Return-Traffic über das Cloudflare-Netzwerk an die Clients zurückgesendet werden. Dies erfolgt über die IP-Tunnel, die über die CNI-Verbindungen konfiguriert sind. Abbildung 5 zeigt ein solches Beispiel.

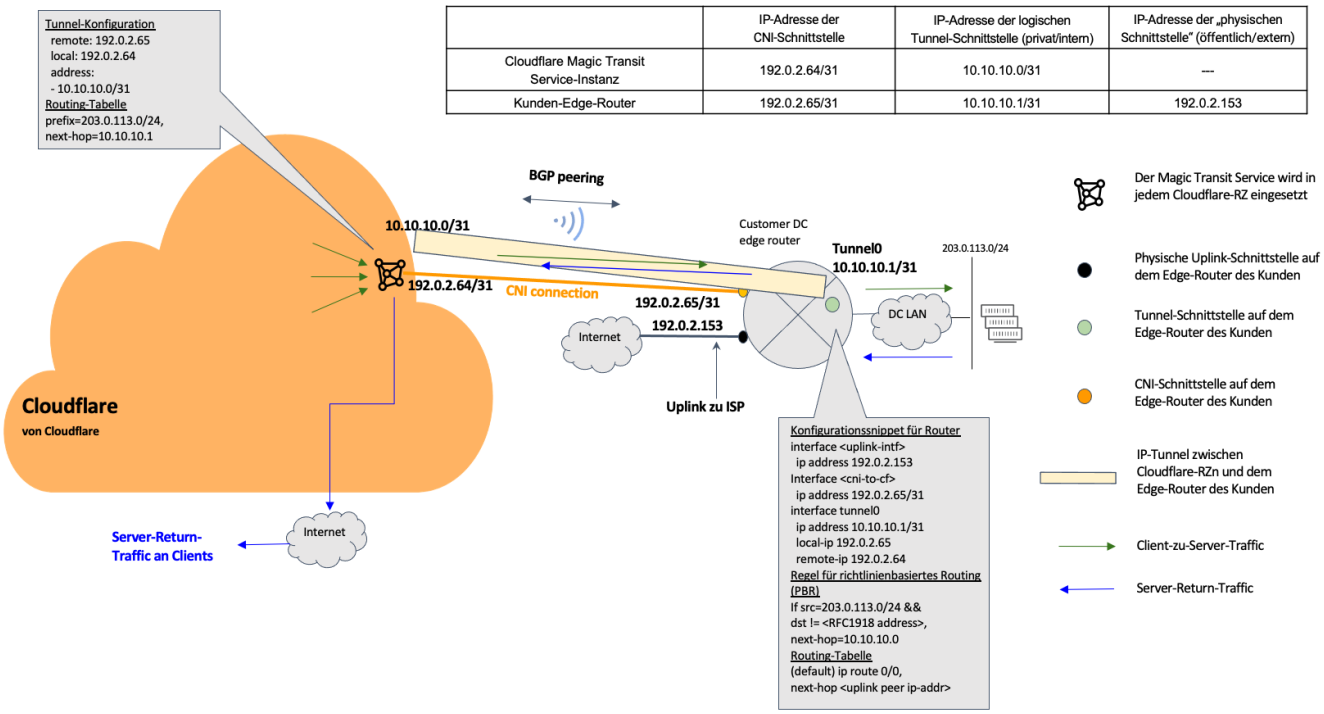


Abbildung 5: Referenzkonfiguration von Magic Transit über CNI mit aktivierter Egress-Option

3.4 Magic Transit zum Schutz von in einer Public Cloud-gehosteten Services

Magic Transit schützt sowohl lokal als auch in der Cloud gehostete Dienste. Dieser Anwendungsfall veranschaulicht die Konfiguration für eine in der Cloud gehostete Bereitstellung.

- In diesem Beispiel hat ein Kunde zwei Cloud VPC-Bereitstellungen bei zwei verschiedenen Cloud-Anbietern und in zwei verschiedenen geografischen Regionen.
- In diesem Beispiel wird das Präfix /24 oder größer des Kunden in mehrere kleinere (d.h. längere Subnetzmaskenlänge) Präfixe (z.B. /26) und den verschiedenen VPCs an unterschiedlichen Standorten zugewiesen. Nachdem die Tunnel vom Cloudflare-Netzwerk zu den einzelnen VPCs eingerichtet wurden, kann der Kunde zentral in der Magic Transit-Konfiguration statische Routen konfigurieren, um den Traffic zu den jeweiligen VPCs zu routen. Diese Konfiguration kann über die API oder das UI-Dashboard vorgenommen werden.

Beachten Sie, dass der Kunde mit der Egress-Option von Magic Transit die BYOIP-Services der einzelnen Cloud-Anbieter, die damit verbundenen Gebühren und die Komplexität der Verwaltung und des Betriebs umgehen kann, indem er den Egress-Traffic (d.h. Server-Return- oder Server-zu-Internet-Traffic) durch das globale Cloudflare-Netzwerk über die Magic Transit-Tunnel schickt.

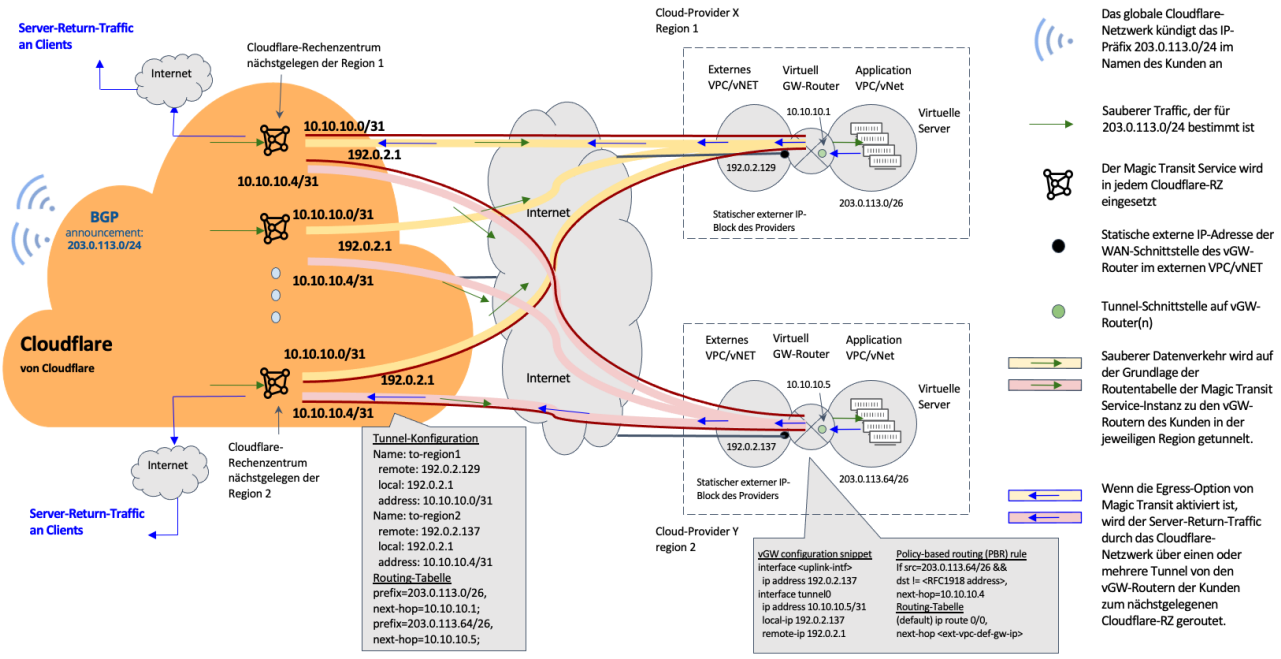


Abbildung 6: Schützen Sie Multi-Cloud-basierte Dienste mit Magic Transit (Egress-Option aktiviert)

3.5 Magic Transit und Magic WAN

Zusätzlich zum Schutz und zur Weiterleitung des Traffic für externe Dienste eines Unternehmens (d.h. von Norden nach Süden über das Internet routbarer Traffic) mit dem Cloudflare Magic Transit-Service können Kunden mit Cloudflare Magic WAN den internen Ost-West-Traffic (z.B. RFC1918-Privatadressen) schützen, der alle Standorte eines Unternehmens miteinander verbindet.

Magic WAN ersetzt veraltete WAN-Architekturen durch das Cloudflare-Netzwerk, das globale Konnektivität, cloudbasierte Sicherheit, hohe Performance und Steuerung über eine einfache Benutzeroberfläche bietet.

Die Cloudflare Magic Transit- und Magic WAN-Services bieten zusammen eine ganzheitliche, sichere, zuverlässige und performante globale Netzwerk-as-a-Service-Lösung für ein ganzes Unternehmen, die sowohl den Nord-Süd- als auch den Ost-West-Traffic schützt und beschleunigt.

Beide Dienste können in derselben Service-Instanz bereitgestellt werden. Für Kunden, die die Verwaltung und den Traffic-Fluss von externen, dem Internet zugewandten Netzwerken und internen Unternehmensnetzwerken völlig getrennt halten möchten, können für Magic Transit und Magic WAN unterschiedliche Service-Instanzen bereitgestellt werden.

Abbildung 7 zeigt ein Beispiel für die Bereitstellung von Magic Transit- und Magic WAN-Services in separaten Service-Instanzen.

- In diesem Beispiel werden GRE-Tunnel verwendet, um die verschiedenen Standorte des Kunden über das globale Anycast-Netzwerk von Cloudflare zu verbinden. Die Cloudflare Anycast IP-Adresse für die Magic Transit Service-Instanz lautet 192.0.2.1, die für die Magic WAN Service-Instanz 192.0.2.2. Der Magic Transit-Dienst ist mit der Egress-Option aktiviert.
- Der Magic Transit-Dienst schützt und leitet den nach außen gerichteten Front-End-Client-Server-Traffic weiter. Der Magic WAN-Service schützt und leitet den unternehmensinternen Datenverkehr, z. B. den von internen Anwendungen, Backend-Datenbanksynchronisationen und den Datenverkehr zwischen den Niederlassungen.

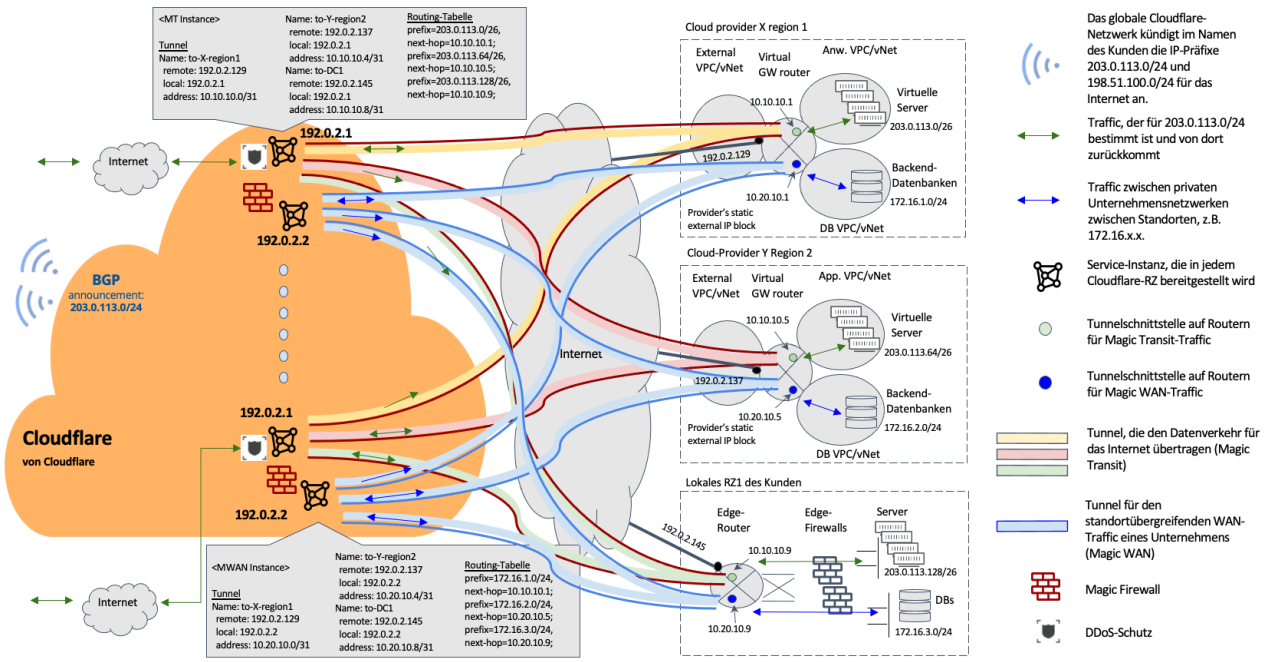


Abbildung 7: Magic Transit + Magic WAN bieten Network-as-a-Service für das gesamte Unternehmen

3.6 Magic Firewall: Kontrollieren und Filtern von unerwünschtem Traffic, bevor er das Unternehmensnetzwerk erreicht

Magic Transit schützt die Dienste der Kunden vor DDoS-Angriffen. Viele Netzwerkadministratoren möchten jedoch auch anderen unerwünschten oder potenziell bösartigen Datenverkehr kontrollieren und blockieren können. Cloudflare Magic Firewall sorgt für konsistente Netzwerksicherheitsrichtlinien im gesamten WAN des Kunden, einschließlich des Hauptsitzes, der Zweigstellen und der virtuellen privaten Clouds, und ermöglicht es den Kunden, präzise Filterregeln global in weniger als 500 ms zu implementieren – und das alles über ein gemeinsames Dashboard.

Magic Firewall wird als Teil von Magic Transit bereitgestellt und konfiguriert. Der gesamte eingehende Traffic, der durch die Edge-Rechenzentren von Cloudflare fließt und dessen Ziel-Präfixe durch Magic Transit geschützt sind, kann von Magic Firewall gefiltert werden.

Mit Magic Firewall-Regeln können Administratoren den Netzwerk-Traffic nicht nur auf der Grundlage der typischen 5-Tupel-Informationen (Quell-/Ziel-IP, Quell-/Ziel-Port, Protokoll) im IP-Paket-Header abgleichen und filtern, sondern auch auf der Grundlage anderer Paketinformationen wie IP-Paketlänge, IP-Headerlänge, TTL usw. Darüber hinaus können geografische Informationen wie der Name des Cloudflare-Rechenzentrums/Colo, die Region und das Land, in dem sich die Rechenzentren befinden, bei der Konfiguration von Magic Firewall-Regeln (Geoblocking) verwendet werden.

Weitere Informationen zur Magic Firewall und ihrer Konfiguration finden Sie in diesem Blog-Beitrag und unserer Dokumentation für Entwickler.

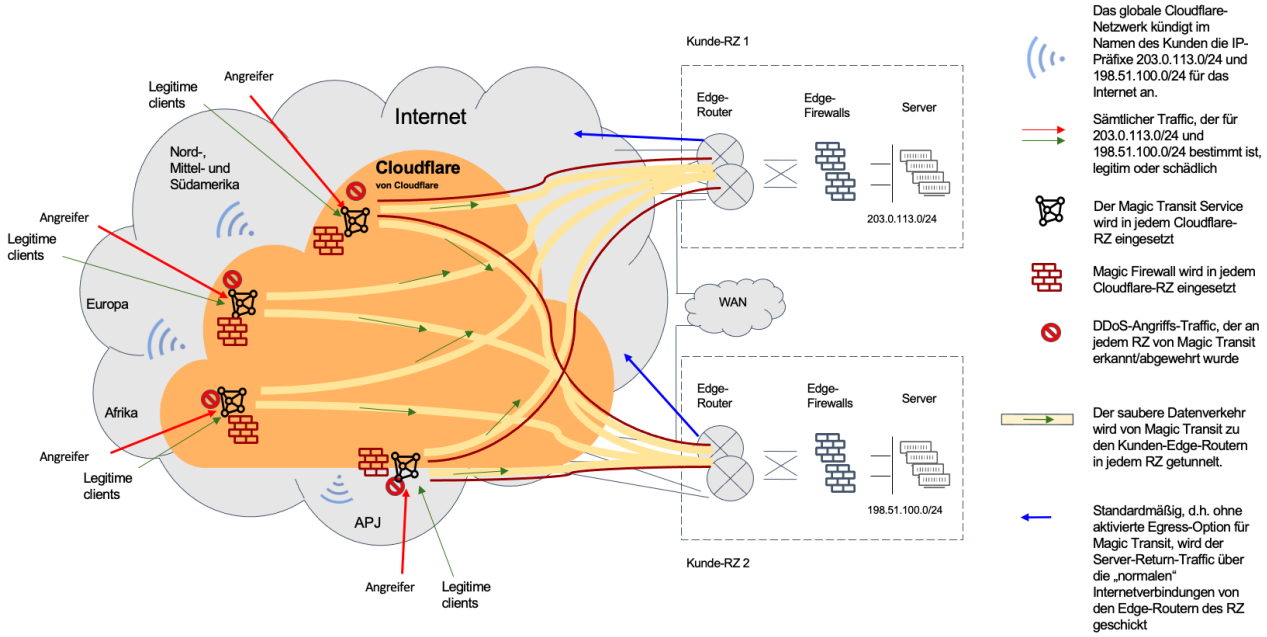


Abbildung 8: Magic Firewall blockiert unerwünschten und schädlichen Traffic an der Internet-Edge

KAPITEL VIER

Ein Hinweis zu Always-On- und On-Demand-Einsätzen

Ein cloudbasierter Anbieter von DDoS-Abwehr kann den Datenverkehr rund um die Uhr auf Bedrohungen untersuchen (Always-on) oder den Datenverkehr nur dann umleiten, wenn ein Angriff erkannt wurde (On-Demand). Die Entscheidung für die eine oder andere Lösung beeinflusst sowohl die Reaktions- als auch die Abwehrzeit. Unter Umständen wirkt sie sich auch auf die Latenz aus.

Das On-Demand-Bereitstellungsmodell sieht vor, dass der eingehende Traffic am Netzwerkrand überwacht und gemessen wird, um volumetrische Angriffe zu erkennen. Im Normalbetrieb – quasi in „Friedenszeiten" – erreicht der gesamte Datenverkehr die Anwendungen und Infrastruktur direkt und ohne Verzögerungen oder Umleitungen. Erst wenn festgestellt wird, dass ein DDoS-Angriff im Gange ist, wird der Traffic der cloudbasierten Scrubbing-Lösung zugeführt. In vielen Fällen muss ein Kunde den Dienstanbieter anrufen, um den Traffic umzuleiten, wodurch sich die Reaktionszeit verlängert.

Der „Always-on"-Modus ist ein vollautomatischer Ansatz zur DDoS-Abwehr, bei dem der Kunde im Falle eines Angriffs nichts tun muss. Der Traffic des Unternehmens wird stets – auch in „Friedenszeiten" – über die Rechenzentren des Cloud-Anbieters geleitet und dort auf Bedrohungen überprüft. Damit vergeht zwischen Aufdeckung und Abwehr eines Angriffs weniger Zeit und die Dienste bleiben ununterbrochen verfügbar.

Unter allen Ansätzen und Bereitstellungsoptionen bietet die Always-on-Methode den umfassendsten Schutz.

Je nach Anbieter können allerdings geschäftskritische Anwendungen durch Latenz beeinträchtigt werden, wenn der gesamte Datenverkehr die Cloud des DDoS-Abwehranbieters durchlaufen muss. Die Netzwerkarchitektur von Cloudflare sorgt dafür, dass unseren Kunden auch bei Angriffen eine höhere Latenz erspart bleibt – und das gilt auch für Always-on-Bereitstellungen. Die Analyse des Datenverkehrs am Netzwerkrand ist die einzige Möglichkeit, selbst große Angriffe ohne Beeinträchtigung der Performance abzuwehren.

Der Grund dafür ist, dass die Aufnahme des Datenverkehrs über Anycast sicherstellt, dass der Datenverkehr nur an das nächstgelegene Cloudflare-Rechenzentrum zur Prüfung weitergeleitet wird. Und weil wir Rechenzentren in über 250 Städten und mehr als 100 Ländern betreiben, müssen die Daten in der Regel wahrscheinlich nur eine kurze Entfernung zurücklegen. Ein langwieriges Hin und Her der Daten wird vermieden.

In vielen Fällen wird mit Cloudflare eine höhere Datengeschwindigkeit erreicht als über das öffentliche Internet. Wir finden, dass unsere Kunden umfassende Sicherheit nicht mit Performanceeinbußen bezahlen sollten.

KAPITEL FÜNF

Zusammenfassung

Cloudflare bietet umfassende Netzwerkdienste für die Verbindung und den Schutz von lokalen, in der Cloud gehosteten und hybriden Unternehmensnetzwerken. Cloudflare bietet verschiedene Konnektivitäts- und Bereitstellungsoptionen, um den individuellen Architekturen der Kunden gerecht zu werden.

- Cloudflare Magic Transit ist eine cloudnative Netzwerksicherheitslösung, die die Leistungsfähigkeit des globalen Cloudflare-Netzwerks nutzt, um Unternehmen vor DDoS-Angriffen zu schützen.
- Magic Transit ist mit einer integrierten Netzwerk-Firewall ausgestattet, die Kunden dabei hilft, lokale Firewalls abzuschaffen und skalierbare Netzwerksicherheit als Service bereitzustellen.
- Zusätzlich zum Schutz und zur Weiterleitung des Traffic für externe Dienste eines Unternehmens (d.h. über das Internet leitbarer Nord-Süd-Traffic) können Kunden mit Cloudflare Magic WAN auch den internen Ost-West-Traffic „innerhalb des Unternehmens“ schützen.

Sie möchten mehr erfahren über Magic Transit, Magic WAN oder Magic Firewall? Dann kontaktieren Sie uns jetzt, um eine Demo zu erhalten.