WHITEPAPER

Netzwerkschutz und höhere Performance mit Cloudflare Magic Transit

Cloudflare Magic Transit bietet Schutz vor DDoS-Angriffen und eine Beschleunigung des Traffic für lokale, cloudbasierte und hybride Netzwerke. Mit Rechenzentren in 200 Städten und einer DDoS-Abwehrkapazität von mehr als 51 Tbit/s kann Magic Transit Angriffe in der Nähe ihres Ursprungs in durchschnittlich weniger als drei Sekunden erkennen und eindämmen – wobei sich gleichzeitig auch noch die Performance verbessert.

In diesem Whitepaper stellen wir die Ergebnisse von Catchpoint-Tests vor, die wir über unser Netzwerk durchgeführt haben, um die Auswirkungen von Magic Transit auf die Latenz zu messen. Festgestellt wurde, dass sich die Netzwerk-Performance (im Hinblick auf Latenz und Paketverlust) für den Testkunden beim Routing des Datenverkehrs über Cloudflare Magic Transit verbesserte. Insbesondere zeigte sich, dass die Latenz um drei Millisekunden abnahm und der Paketverlust nahezu bei Null lag.

Wie schützt Magic Transit die Netzwerkinfrastruktur, ohne dabei die Performance zu beeinträchtigen?

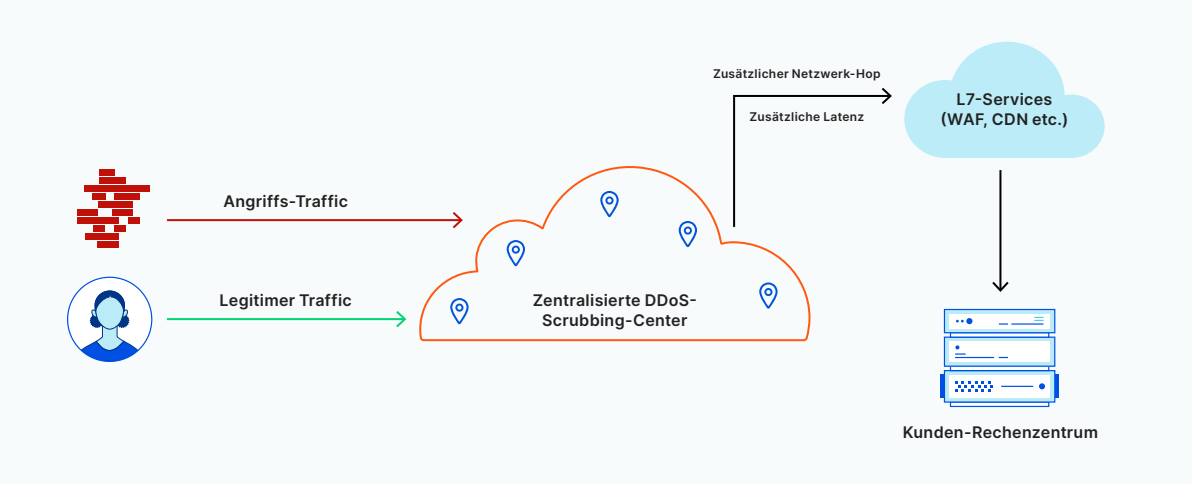
Vor Magic Transit gab es im Wesentlichen zwei Möglichkeiten, Netzwerkinfrastruktur vor DDoS-Angriffen zu schützen: lokale Hardware-DDoS-Appliances und cloudbasierte Scrubbing-Lösungen.

Lokale Hardware-Appliances leisten durchaus gute Arbeit beim Schutz der Infrastruktur – zumindest in einem gewissen Umfang. Doch ihre Bandbreite ist begrenzt und sie können unter der Last größerer oder parallel ablaufender Angriffe zusammenbrechen. Zudem erfordert die Hardware eine große Vorabinvestition und hohen Ressourcenaufwand für Verwaltung und Wartung.

Cloudbasierte Scrubbing-Center sind als einfachere Alternative entstanden, über die Datenverkehr geroutet werden kann, um Angriffs-Traffic herauszufiltern. Dadurch wurden die mit lokaler Hardware verbundenen hohen Kosten und Wartungsprobleme beseitigt.

Allerdings entstand auch ein neues Problem: erhebliche Latenz.

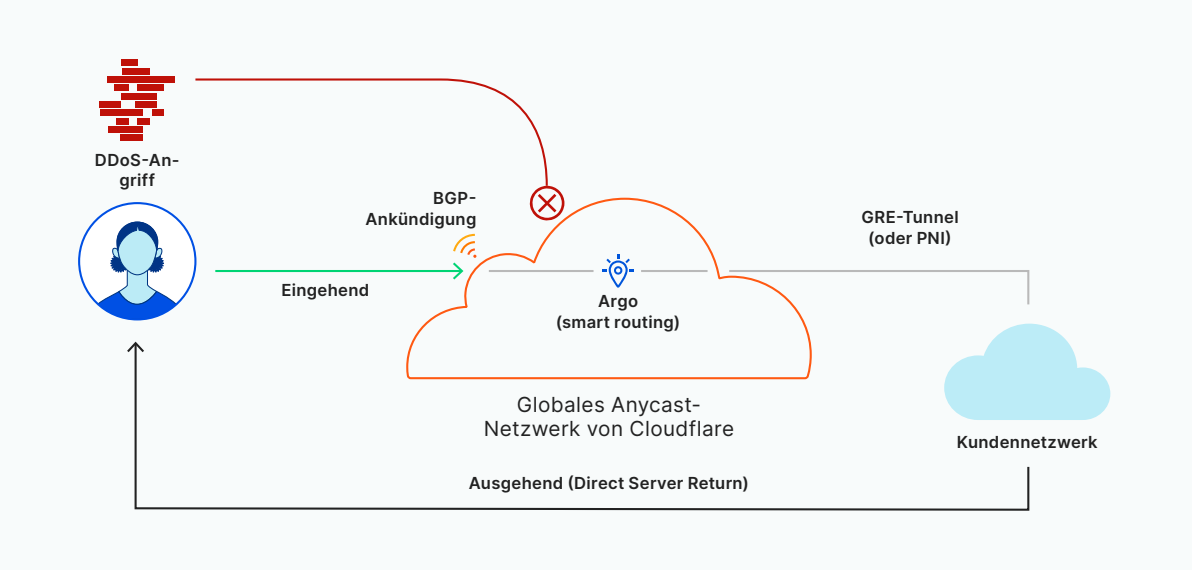
Da diese Cloud-Provider nur über eine begrenzte Anzahl geografisch ungleich verteilter Scrubbing-Center verfügen, muss der Traffic für das Bereinigen unter Umständen einen langen Umweg nehmen, bevor er schließlich sein eigentliches Ziel erreicht. Cloud-Provider betreiben in der Regel nur eine Handvoll Scrubbing-Center, und wenn Sie oder Ihre Endbenutzer sich nicht in der Nähe eines dieser Zentren befinden, muss Ihr Traffic selbst bei geringer Entfernung des Endziels eine weite Strecke zurücklegen. Dies führt oft zu spürbaren und ärgerlichen Verzögerungen.



Es gibt nur wenige und weit entfernte Scrubbing-Center, die sich der DDoS-Abwehr widmen. Darum muss Netzwerk-Traffic für jede weitere Verarbeitung in Layer 4-7 zu einem alternativen Rechenzentrum geleitet werden, wodurch sich die Datenübertragung zusätzlich verlängert.

In dem oben dargestellten Fall muss der Datenverkehr auf Layer 3-4 sowie für Layer 7-Dienste (wie WAF, Bot Management usw.) verarbeitet werden. Dabei wird er zunächst für die Layer 3-DDoS-Abwehr zu einem entfernten Layer 3-Scrubbing-Center und anschließend zur weiteren Layer 7-Verarbeitung an ein sekundäres Rechenzentrum weitergeleitet. Somit muss der Datenverkehr einen zusätzlichen Hop nehmen, was die Latenz unnötig erhöht. Die Latenz ist besonders ausgeprägt, wenn der Cloud-Provider nur über eine begrenzte Anzahl von Scrubbing-Centern verfügt und die Quelle des Netzwerk-Traffic weit davon entfernt ist.

Magic Transit bietet eine bessere Lösung. Anstelle von dedizierten Scrubbing-Centern lassen wir jedes Rechenzentrum im globalen Netzwerk von Cloudflare das Scrubbing übernehmen. Tatsächlich wird in jedem Cloudflare-Rechenzentrum das gesamte Spektrum unserer Dienste ausgeführt. Somit muss Ihr Datenverkehr nur zu einem der Cloudflare-Rechenzentren geleitet werden, die sich in der Nähe befinden. Da diese auf mehr als 200 Städte in über 100 Ländern verteilt sind, dürfte der Weg nicht allzu weit sein.

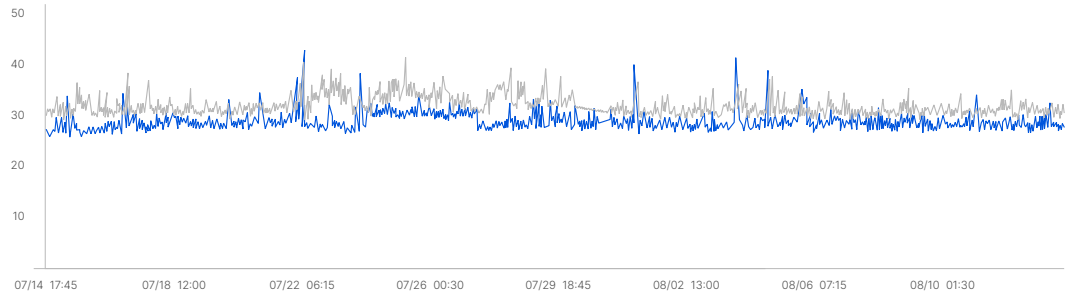


In jedem Cloudflare-Rechenzentrum wird das gesamte Spektrum der Layer 3-7-Dienste ausgeführt, sodass der Netzwerk-Traffic am gleichen Standort verarbeitet wird.

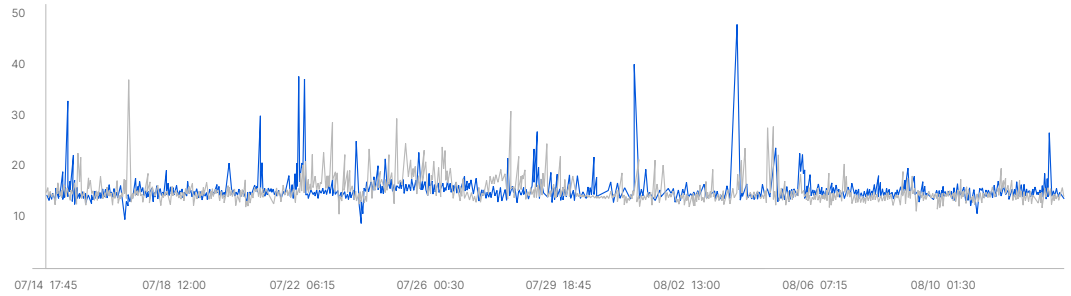
So muss der Datenverkehr keine Umwege mehr nehmen und die Latenz ist äußerst gering. Bei der Entwicklung von Magic Transit wurde besonderes Augenmerk auf die Netzwerk-Performance gelegt. Wir wollten sicher sein, dass unsere Benutzer diese nicht um der Sicherheit willen opfern müssen.

Catchpoint-Tests

Wir wollten dies überprüfen und die Auswirkungen der Verwendung von Magic Transit auf die Leistungsfähigkeit des Netzwerks untersuchen. Daher haben wir mit Catchpoint global verteilt ICMP-Ping-Tests durchgeführt, die sich an zwei IP-Adressen richteten. Beide wurden auf derselben Netzwerkinfrastruktur gehostet, wobei die eine durch Magic Transit geschützt wurde, die andere hingegen nicht. Auf diese Weise konnten wir zum Vergleich der Performance Latenz, Paketverlust und Jitter gleichzeitig messen.



Latenz (Paketumlaufzeit) Leistung (ms) mit Magic Transit (blau) und ohne Magic Transit (grau)



Jitter (ms) mit Magic Transit (blau) und ohne Magic Transit (grau)

Paketverlust (in Prozent) mit Magic Transit (blau) und ohne Magic Transit (grau)

In dem oben veranschaulichten Test bildet die blaue Linie die Performance mit Magic Transit und die graue die Performance ohne Magic Transit ab.

Testergebnisse

Performance	Mit Magic Transit (blau)	Ohne Magic Transit (grau)
Latenz	28,96 ms	31,98 ms
Jitter	15,61 ms	15,24 ms
Paketverlust	0,52 %	5,26 %

Wichtigste Ergebnisse im Überblick

- Rückgang der Latenz um 3 ms mit Magic Transit
- Zunahme des Jitter um 0,36 ms mit Magic Transit
- Paketverlust fast bei Null (bei 0,52 %) mit Magic Transit und bei 5,26 % ohne Magic Transit

Einordnung der Ergebnisse

Latenz: die Zeitspanne, die Datenpakete benötigen, um innerhalb des Netzwerks von einem Punkt zu einem anderen zu gelangen. In unserem Test haben wir über das Cloudflare-Netzwerk eine geringere Latenz gemessen.

Cloudflare optimiert die Traffic-Routen laufend entsprechend dem Zustand der verschiedenen Netzwerkpfade. Daher funktionieren die Pfade, die Pakete von Cloudflare zum Kundennetzwerk nehmen, oft besser als diejenigen, die sie ohne die Optimierung durch Cloudflare nehmen würden.

So wird sichergestellt, dass die Netzwerklatenz nicht erhöht und in vielen Fällen – wie in unseren Testergebnissen zu sehen – sogar verringert wird. Dies ist vor allem bei (Echtzeit-)Anwendungen wie Online-Spielen und Voice-over-IP (VoIP) wichtig, bei denen Latenz eine besonders große Relevanz hat.

Jitter: das Ausmaß der Verzögerung bei der Paketzustellung über ein Netzwerk. Den Jitter niedrig zu halten, ist bei Anwendungen wie VoIP besonders wichtig. Mit Magic Transit stieg der Jitter jedoch nur um 0,36 ms. Das gilt selbst für Anwendungen als vernachlässigbar, die empfindlich auf höheren Jitter reagieren.

Paketverlust: wenn ein oder mehrere Pakete bei einer Netzwerkübertragung ihren Bestimmungsort nicht erreichen. Je nach Protokoll kann der Paketverlust dazu führen, dass mehr Zeit für die erneute Übertragung benötigt wird oder die Qualität sich verschlechtert. Für Übertragungen wie Videokonferenzen, bei denen der Zeitfaktor eine besonders große Rolle spielt, gilt ein Paketverlust von weniger als 1 % als vertretbar*. In unseren Tests haben wir festgestellt, dass der Paketverlust über das Netzwerk von Cloudflare fast auf Null zurückgegangen ist (während ohne Magic Transit ein Paketverlust von mehr als 5 % verzeichnet wurde).

Zusammenfassend lässt sich sagen, dass die Auswirkungen von Magic Transit auf Latenz, Jitter und Paketverlust die Benutzererfahrung nicht beeinträchtigen und in vielen Fällen sogar verbessern können. Mit anderen Worten: Cloudflare-Kunden müssen bei der Verwendung von Magic Transit keine Abstriche bei der Netzwerk-Performance machen.

Darüber hinaus lässt sich Cloudflare Magic Transit mit dem gesamten Spektrum an Cloudflare-Produkten für Sicherheit, Performance und Zuverlässigkeit integrieren, damit Websites noch besser funktionieren.

Sie erhalten weitere Informationen zu Cloudflare Magic Transit unter www.cloudflare.com/de-de/magic-transit oder auf Anfrage bei sales@cloudflare.com.

*https://web.archive.org/web/20131010010244/http://sdu.ictp.it/pinger/pinger.html