WHITEPAPER

CLOUDFLARE

Cloudflare Magic Transit protects networks while improving performance

Cloudflare Magic Transit provides DDoS protection and traffic acceleration for on-premise, cloud, and hybrid networks. With data centers spanning 200 cities and over 51 Tbps in DDoS mitigation capacity, Magic Transit can detect and mitigate attacks close to their source of origin in less than 3 seconds on average—all with integrated performance benefits.

In this paper, we present results of Catchpoint tests we've run over our network to quantify the impact of latency with Magic Transit. These test results demonstrate that network performance (latency and packet loss) improved for the test customer when traffic was routed over Cloudflare Magic Transit. Specifically, we observed in our test results that the latency decreased by 3 ms and packet loss was nearly zero when traffic was routed over Magic Transit.

How does Magic Transit protect network infrastructure without impeding network performance?

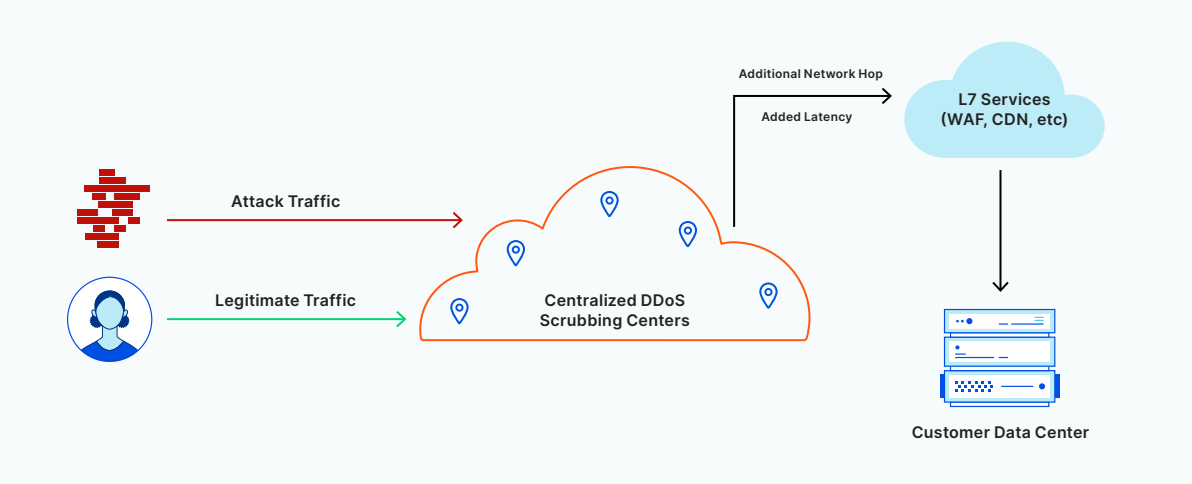
Before Magic Transit, there were two primary strategies for protecting network infrastructure from DDoS attacks: on-premise hardware DDoS appliances and cloud-based scrubbing solutions.

On-premise hardware appliances do a fine job of protecting your infrastructure—to an extent. These boxes have limited bandwidth and they can become overwhelmed by larger or simultaneous attacks. Hardware also requires a large up-front investment and requires a lot of resources to manage and maintain.

Cloud-based scrubbing centers came along to offer a simpler alternative: route your traffic through their scrubbing centers, where attack traffic is filtered out. This solved the financial burden and maintenance headaches that came with on-premise boxes.

But it also created a new problem: significant latency.

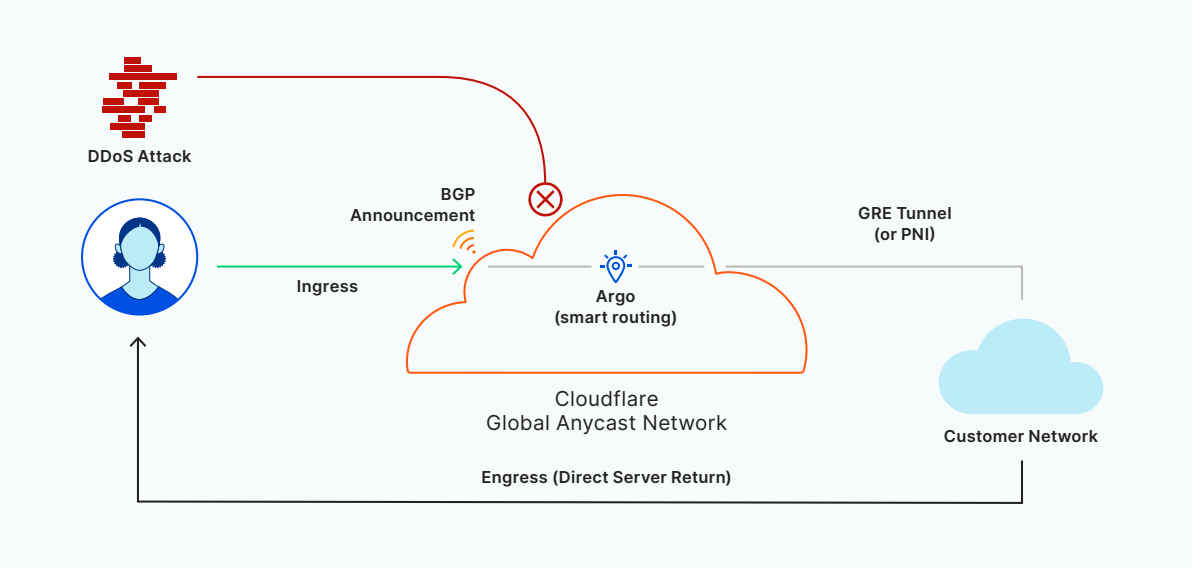
Since these cloud providers have a limited and geographically disparate set of scrubbing centers, this means traffic may have to travel a long distance out of its way to get scrubbed before reaching its final destination. Cloud providers usually only have a handful of scrubbing centers, and if you or your end users are not near one of them, your traffic will have to travel a long distance, even if its final destination is nearby. This is the so-called trombone effect, and it often creates noticeable and painful delay. (It's called the 'trombone effect' because if you illustrate the long round-trip path your traffic is taking on a map, the shape resembles a trombone).



'Scrubbing centers' are distant and few and dedicated to DDoS mitigation. This requires network traffic to travel to an alternate data center for any additional L4-7 processing incurring additional delay.

Consider the scenario above, where you need your traffic to be processed at Layers 3-4 as well as for Layer 7 services (such as WAF, Bot Management, etc.) In this case, first your traffic hits a distant L3 scrubbing center for L3 DDoS mitigation and is then sent for any additional L7 processing to a secondary data center, adding a network hop to the end-to-end traffic; this introduces unnecessary latency. The latency is especially pronounced if the cloud vendor has a limited set of scrubbing centers and the source of your network traffic is far away from it.

Magic Transit introduces a better solution. Instead of dedicated scrubbing centers, we let every data center in Cloudflare's global network handle the scrubbing. In fact, every Cloudflare data center runs the full stack of Cloudflare services. This means your traffic only needs to go to the nearest Cloudflare data center; with data centers in over 200 cities across more than 100 countries, it's likely to be a short distance.

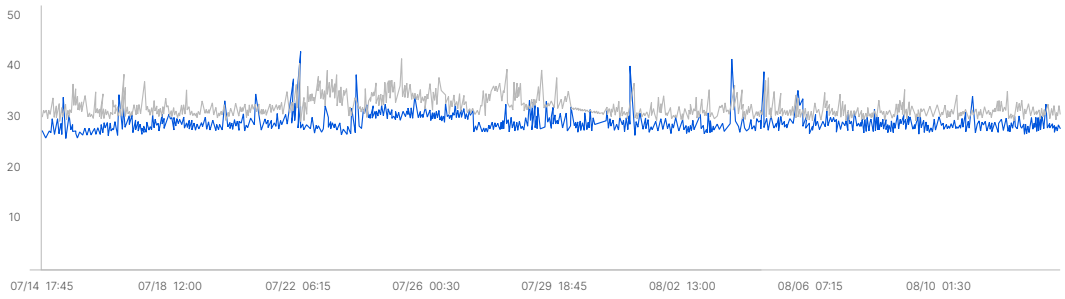


Every Cloudflare data center runs the full stack of L3-7 services, so network traffic is processed at the same location.

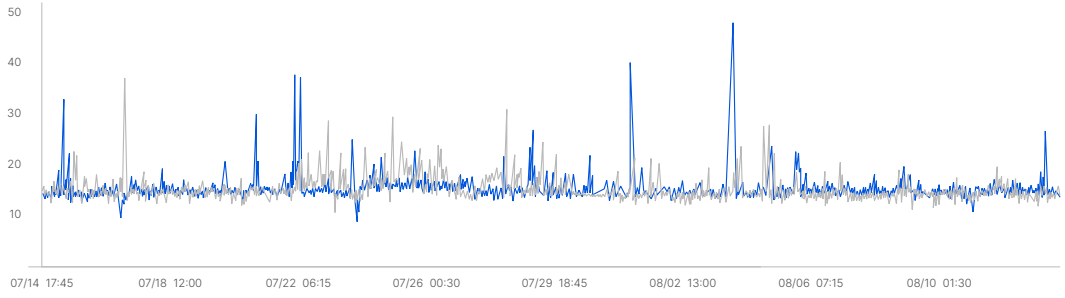
This means no trombone effect and very minimal latency. Network performance was a top concern in how we developed Magic Transit; we wanted to be sure that our users weren't sacrificing performance for the sake of security.

Catchpoint Tests

To verify this, we used Catchpoint to run some tests to determine the effects of using Magic Transit on overall network performance. With a global distribution of probes, we ran ICMP ping tests to an IP address behind Magic Transit and another off of Magic Transit, both hosted on the same network infrastructure. This allowed us to measure latency, packet loss, and jitter concurrently to see the difference in performance.



Latency (ping round trip) performance (ms) with Magic Transit (blue) and without Magic Transit (gray)



Jitter performance (ms) with Magic Transit (blue) and without Magic Transit (gray)

Packet loss performance (percentage) with Magic Transit (blue) and without Magic Transit (gray)

In the test illustrated above, the blue line represents the performance using Magic Transit, while the gray line represents the same without Magic Transit.

Test results

Performance	With Magic Transit (blue)	Without Magic Transit (gray)
Latency	28.96 ms	31.98 ms
Jitter	15.61 ms	15.24 ms
Packet Loss	0.52%	5.26%

Key takeaways from these tests

- Latency decreased by 3 ms when using Magic Transit
- Jitter increased by 0.36 ms when using Magic Transit
- Packet Loss was almost zero (at 0.52%) when using Magic Transit when compared to 5.26% packet loss without Magic Transit

What do these results mean?

Latency: Latency is the amount of time it takes for data packets to travel from one point to another point on the network. In our tests, we observed lower latency over Cloudflare's network.

Cloudflare is constantly optimizing traffic routes in response to the state of different network paths, so the outgoing paths packets take from Cloudflare to the customer network are often more efficient than the one those packets would take without Cloudflare's optimization.

This ensures that network latency is not increased and in many cases—as seen in our test results—it is even decreased. This is especially important to latency sensitive (real-time) applications such as online gaming and Voice over IP (VoIP).

Jitter: Network jitter is the amount of delay between packet delivery over a network. Keeping jitter low is especially important for applications such as VoIP. With Magic Transit, the jitter increased by 0.36 ms. This is considered negligible, even for jitter-sensitive applications.

Packet loss: Packet loss happens when one or more of the packets in a network transmission fail to reach their destination. Depending on the protocol, packet loss can result in time added for retransmission or degradation in quality. For extremely time-sensitive transmissions like video conferencing, less than 1% packet loss is considered to be acceptable*. In our tests, we observed that the packet loss decreased to nearly zero over Cloudflare's network (compared to over 5% packet loss without Magic Transit)

In summary, Magic Transit's effects on latency, jitter, and packet loss will not impair the user experience, and in many cases, can even improve it. In other words, Cloudflare customers do not have to worry about a 'trade-off' in network performance when using Magic Transit.

In addition, Cloudflare Magic Transit integrates with the full stack of Cloudflare's security, performance, and reliability products to further optimize the performance of Internet properties.

To learn more about Cloudflare Magic Transit, go to www.cloudflare.com/magic-transit or contact us as: sales@cloudflare.com

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