



Cloudflare Magic Transit chrání síť, a přitom zvyšuje výkon

Cloudflare Magic Transit zajišťuje ochranu před DDoS útoky a rychlejší přenos dat pro lokální, cloudové i hybridní síť. Díky datovým centřům umístěným ve 200 městech a přes 42 Tb/s kapacity pro eliminaci DDoS útoků dovede Magic Transit detekovat a eliminovat útoky blízko jejich zdrojů do 10 sekund (a v průměru za méně než 3 sekundy) – a to vše spolu s integrovanými výkonnostními výhodami.

V tomto článku představujeme výsledky testů Catchpoint, které jsme prováděli přes naši síť s cílem kvantifikace dopadů Magic Transit na přenosové zpoždění. Výsledky těchto testů ukazují, že výkonnost sítě (zpoždění a ztrátovost paketů) se pro testovacího uživatele zlepšily, když byl provoz směrován přes Cloudflare Magic Transit. Konkrétně jsme pozorovali ve výsledcích našich testů, že když byl provoz směrován přes Magic Transit, zpoždění se snížilo o 3 ms a ztrátovost paketů byla blízka nule.

Jak Magic Transit chrání síťovou infrastrukturu bez blokování výkonu sítě?

Před příchodem Magic Transit existovaly pro ochranu síťové infrastruktury před DDoS útoky dvě primární strategie: lokální hardwarové DDoS appliance a cloudová čistící řešení.

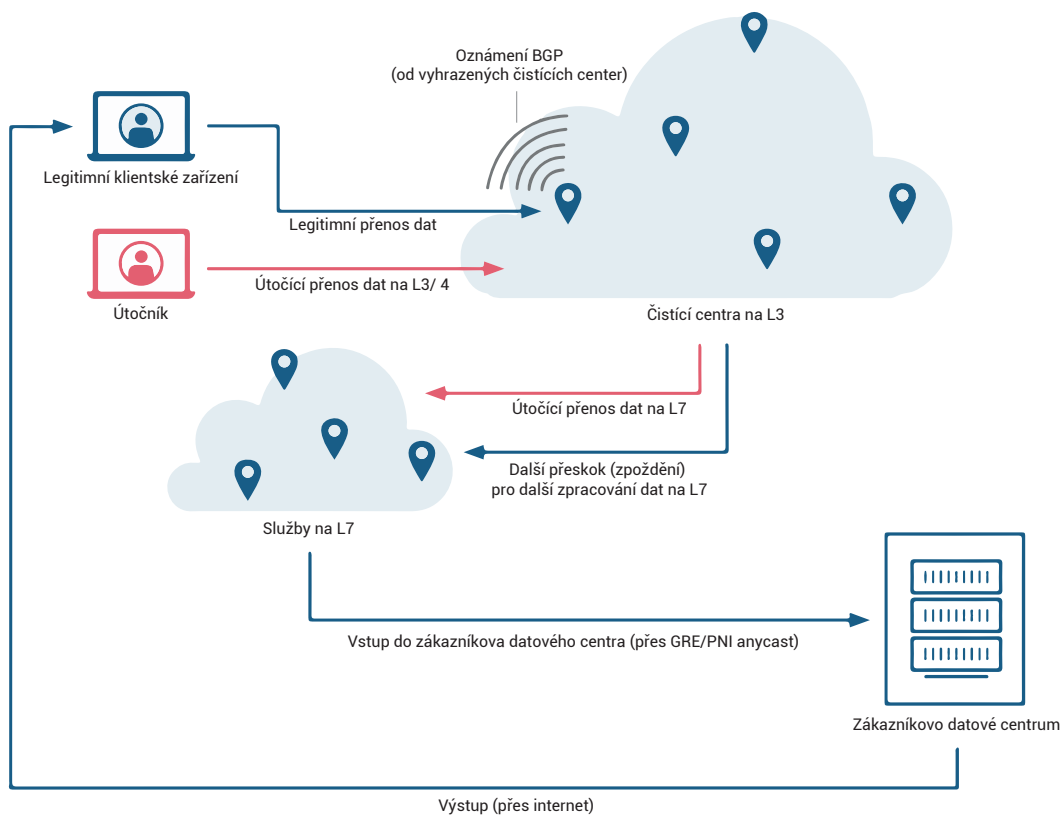
Hardwarové appliance v lokalitě uživatele dělají dobrou práci při ochraně Vaší infrastruktury – do jisté míry. Tyto boxy mají omezenou přenosovou kapacitu. a tak se mohou při větších souběžných útocích zahltit. Hardware také vyžaduje velké investice předem a také vyžaduje mnoho prostředků pro účely správy a údržby.

Cloudová čistící centra přispěla s nabídkou jednoduché alternativy: směřovat svůj provoz přes jejich čistící centra, kde jsou útoky odfiltrovány. Tím se vyřešilo finanční zatížení a problémy s údržbou související s on premise boxy.

Ale také se tím vytvořil nový problém: významné zpoždění.

Protože tito cloudoví poskytovatelé mají omezenou a geograficky nesourodou množinu čistících center, znamená to, že provoz někdy musel cestovat velkou vzdálenost mimo svou cestu, aby byl vyčištěn předtím, než se dostal do koncového místa určení. Cloudoví poskytovatelé obvykle mají pouze hrstku čistících center, a pokud Vy nebo Vaši koncoví uživatelé nejste blízko jednoho z nich, bude muset Váš provoz cestovat na velké vzdálenosti, i když jeho cílové místo určení je nablízku. Toto je takzvaný trombónový jev, který často způsobuje ztlačení a nepříjemná zpoždění. (Tento jev je nazván ‚trombónový,‘ protože když ilustrujete dlouhou obousměrnou přenosovou cestu, kterou musí Váš provoz urazit, na mapě, výsledný tvar připomíná trombón).

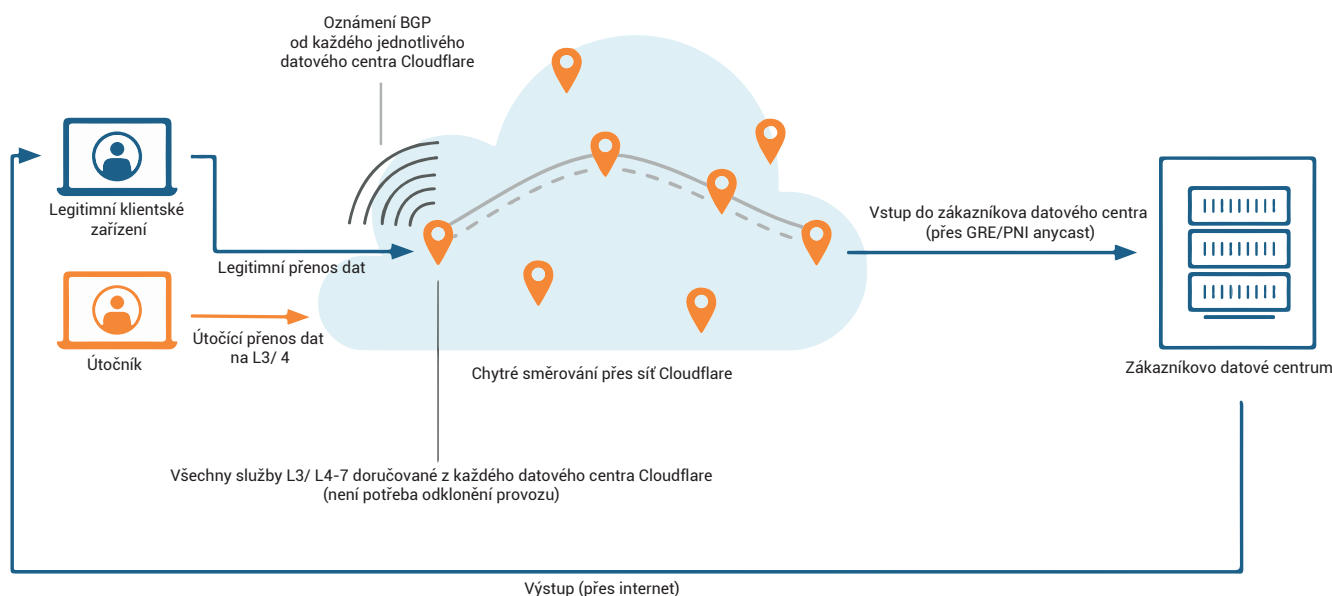
‘Čistící centra’ jsou vzdálená a je jich málo a jsou vyhrazená pro eliminaci DDoS útoků. To vyžaduje, aby síťový provoz cestoval do alternativního datového centra kvůli každému dodatečnému zpracování na L4-7, což způsobuje další zpoždění



Uvažujte scénář výše, kde potřebujete, aby Váš provoz byl zpracováván jak ve službách na vrstvách 3-4, tak na vrstvě 7 (jako např. WAF, správa botů, atd.). V tomto případě nejprve Váš provoz projde přes vzdálené L3 čistící centrum, kde se provede eliminace DDoS na L3, a pak bude poslán k jakémukoli dalšímu zpracování na 7. vrstvě do sekundárního datového centra, čímž se přidává do provozu mezi odesílatelem a příjemcem další síťový přeskok; to zavádí zpoždění, které není nutné. Zpoždění je zvláště zřetelné, pokud má cloudový dodavatel omezenou množinu čistících center a zdroj Vašeho síťového provozu je daleko od nich.

Magic Transit zavádí lepší řešení. Namísto dedikovaných čistících center umožňujeme, aby každé datové centrum v celosvětové síti Cloudflare provádělo čištění. Ve skutečnosti v každém datovém centru Cloudflare běží úplná sada služeb Cloudflare. To znamená, že Vašemu provozu stačí se pouze dostat do nejbližšího datového centra Cloudflare; díky tomu, že datová centra jsou ve více než 200 městech ve více než 100 zemích, je pravděpodobné, že to bude blízko.

V každém datovém centru Cloudflare běží úplná sada služeb na L3-7, takže síťový provoz je zpracováván na stejném místě

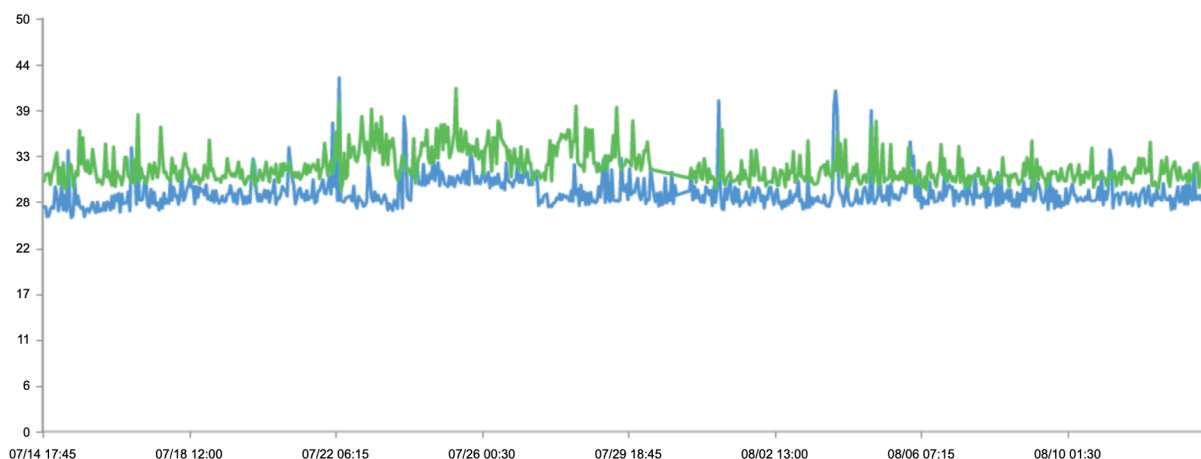


Znamená to žádný trombónový jev a velmi minimální zpoždění. Výkonnost sítě byla při vývoji Magic Transit nejdůležitějším kritériem; chtěli jsme si být jistí, že naši uživatelé neobětují výkonost na oltář bezpečnosti.

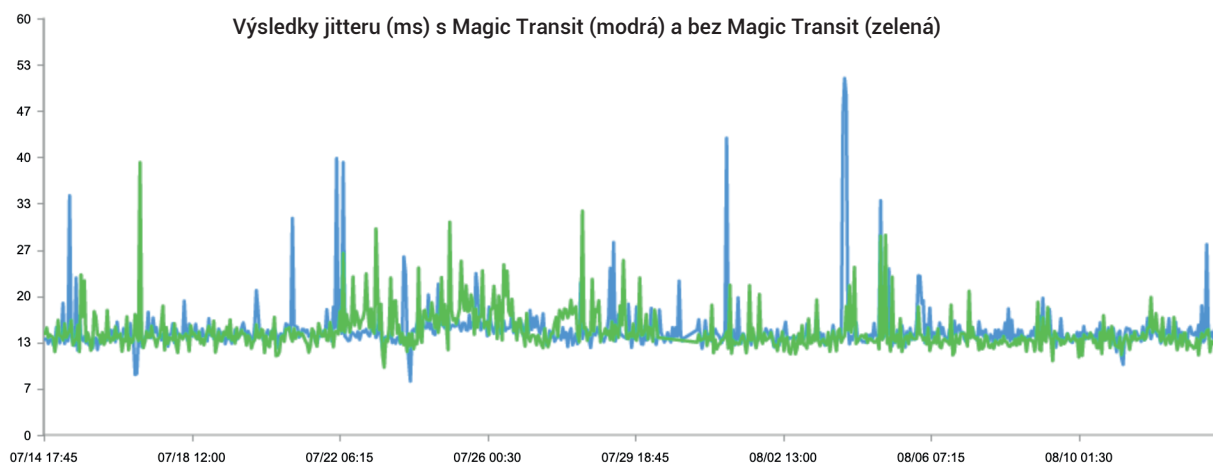
Testy Catchpoint

Abychom si to ověřili, použili jsme Catchpoint pro spuštění určitých testů, abychom mohli určit dopady používání Magic Transit na celkovou síťovou výkonnost. Pomocí sond rozložených po celém světě jsme spustili testy ICMP ping na IP adresu za Magic Transit, a na druhou mimo Magic Transit, přičemž obě byly hostována na stejné síťové infrastruktuře. To umožnilo změřit zpoždění, ztrátu paketů a jitter souběžně a určit tak rozdíl ve výkonnosti.

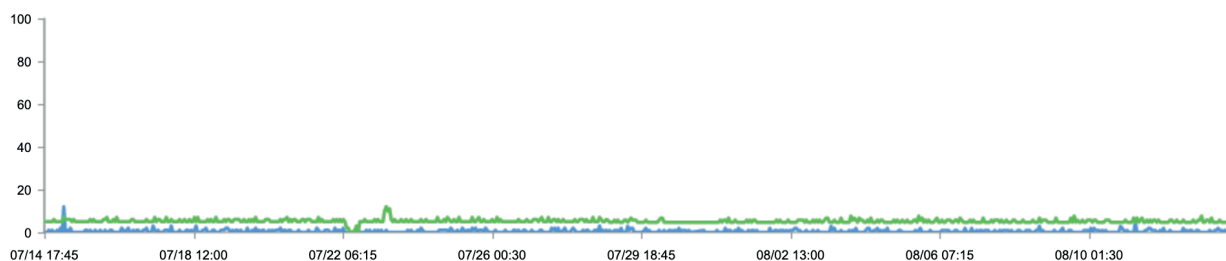
Výsledky latence (obousměrná cesta pingu) (ms) s Magic Transit (modrá) a bez Magic Transit (zelená)



Výsledky jitteru (ms) s Magic Transit (modrá) a bez Magic Transit (zelená)



% Ping Packet Loss Výsledky ztrátovosti paketů (v procentech) s Magic Transit (modrá) a bez Magic Transit (zelená)



V testu ilustrovaném výše představuje modrá čára výkonnost s pomocí Magic Transit, zatímco zelená čára představuje totéž bez Magic Transit.

Výsledky testů:

Výkonnost	S Magic Transit (modrá)	Bez Magic Transit (zelená)
Latence (zpoždění)	28.96 ms	31.98 ms
Jitter	15.61 ms	15.24 ms
Ztráta paketů	0.52%	5.26%

Hlavní závěry z těchto testů:

- Zpoždění se při používání Magic Transit zkrátilo o 3 ms.
- Jitter se při používání Magic Transit zvýšil o 0,36ms.
- Ztrátovost paketů byla při používání Magic Transit téměř nulová (0,52 %), v porovnání se ztrátou paketů 5,26% bez Magic Transit.

Co tyto výsledky znamenají?

Zpoždění: Zpoždění (latence) je množství času, který uplyne při přenosu datových paketů z jednoho místa v síti do jiného. V našich testech jsme pozorovali, nižší zpoždění přes síť Cloudflare.

Cloudflare průběžně optimalizuje směrování provozu v reakci na stav různých síťových tras, takže cesty, které odchozí pakety používají ze sítě Cloudflare do sítě zákazníka, jsou často efektivnější než ty, které pakety použijí bez optimalizace Cloudflare.

Tím se zajišťuje, že síťové zpoždění se nezvýší a v mnohých případech –jak je vidět na výsledcích našich testů –se dokonce sníží. To je zvláště důležité pro aplikace citlivé na zpoždění (pracující v reálného času) jako např. online hry a přenos hlasu před datovou sítí (Voice over IP - VoIP).

Jitter: Síťový jitter je kolísání zpoždění mezi doručení paketů přes síť. Udržování jitteru na nízké hodnotě je zvláště důležité pro aplikace jako VoIP. Při používání Magic Transit se jitter zvýšil o 0,36 ms. To lze považovat za zanedbatelné, dokonce i pro aplikace citlivé na jitter.

Ztrátovost paketů: Ke ztrátě paketů dochází, když jeden nebo více paketů při přenosu přes síť nedojde do svého cíle. V závislosti na protokolu může ztráta paketů způsobit prodloužení času kvůli opakovanému přenosu, nebo snížení kvality. Pro časově velmi citlivé přenosy, jako jsou videokonferenční hovory, se považuje za přijatelnou ztrátovost paketů nižší než 1 %. V našich testech jsme pozorovali, že ztrátovost paketů se snížila téměř na nulu přes síť Cloudflare (v porovnání s více než 5 % ztracených paketů bez použití Magic Transit).

Shrnuto, vliv Magic Transit na zpoždění, jitter a ztrátovost paketů nezhorší zkušenost uživatelů, a v mnoha případech ho může dokonce zlepšit. Jinými slovy, zákazníci Cloudflare se nemusí bát ‚kompromisů‘ ve výkonnosti sítě, když používají Magic Transit.

Navíc Cloudflare Magic Transit je integrován s úplnou sadou produktů Cloudflare pro zajištění bezpečnosti, výkonnosti a spolehlivosti pro další optimalizaci výkonnosti internetových sídel.

Chcete-li se o Cloudflare Magic Transit dovědět víc, otevřete si stránku www.cloudflare.com/magic-transit, nebo nám napište na adresu: cloudflare@zebra.cz

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



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

© 2020 Cloudflare Inc. All rights reserved.

The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.