CLOUDFLARE

BIAŁA KSIĘGA

Odporność sieci i usług Cloudflare

Spis treści

Omówienie

Internet bazuje na niedoskonałych systemach, które zaprojektowano w taki sposób, aby priorytetem — ponad wszystko inne — był dla nich czas działania. Protokoły takie jak TCP i BGP opierają się na zasadach systemów rozproszonych — przewidując awarie i uwzględniając je — a Internet został odpowiednio do tego zaprojektowany. Jednak punkty awarii nadal istnieją i mogą mieć negatywny wpływ na działanie. Dostawcy sieci muszą być w stanie planować możliwość pojawienia się awarii, wykrywać je w momencie wystąpienia oraz łagodzić skutki, których doświadczają użytkownicy.

Ze względu na charakter wielu aplikacji internetowych działających w czasie rzeczywistym sieci muszą nie tylko obejmować jak największą część Internetu, ale także reagować i łagodzić skutki w czasie rzeczywistym. Przestoje rzędu kilku minut są nie do zaakceptowania — klienci oczekują rozwiązania problemu w ciągu zaledwie kilku sekund.

Cloudflare dostarcza kluczowe usługi infrastruktury sieciowej, aby wspierać organizacje we wdrażaniu zabezpieczeń i komunikowaniu się w Internecie. Opracowaliśmy naszą sieć i świadczone przez nią usługi w taki sposób, aby utrzymać najwyższy poziom doskonałości operacyjnej. Cloudflare przetwarza średnio 84 miliony żądań HTTP i 61 milionów zapytań DNS na sekundę, świadcząc usługi milionom zasobów internetowych i użytkowników.

W jaki sposób Cloudflare zapewnia niezawodną obsługę na taką skalę, biorąc pod uwagę nieprzewidywalność Internetu?

Odpowiedzią jest tu architektura sieci Cloudflare, która współdziała z funkcjami odporności zaprojektowanymi z myślą o niezależnym funkcjonowaniu i wytrzymywaniu całego spektrum zakłóceń. Nasze możliwości obliczeniowe, sieciowe i magazynowe, a także procesy operacyjne, zostały zaprojektowane w taki sposób, aby niezawodność rozwiązań Cloudflare był tak samo wysoka, jak obecność sygnału wybierania w starej sieci telefonicznej. Cloudflare zapewnia, metaforycznie, „sygnał wybierania chmury” dla usług sieciowych i związanych z bezpieczeństwem, na których polegają klienci, niezależnie od warunków panujących w Internecie w dowolnym momencie.

W niniejszym dokumencie analizujemy wyzwania związane z działaniem w czasie rzeczywistym w Internecie oraz wyjątkowe możliwości firmy Cloudflare pozwalające im sprostać.

Funkcjonowanie w niedoskonałym świecie

Chociaż Internet to niedoskonałe miejsce, organizacje potrzebują go do rozwijania swojej działalności i prowadzenia organizacji łączących rozproszonych użytkowników, dane i urządzenia z aplikacjami w chmurze. Każde zakłócenie świadczenia usług ma poważne konsekwencje. Na przestrzeni lat firma Cloudflare informowała o wielu poważnych zakłóceniach usług Internetu na całym świecie, od wypadków po ataki DDoS, klęski żywiołowe i nie tylko.

Internet to zróżnicowana sieć, która została zbudowana jako luźno powiązany zbiór tysięcy sieci o różnej wielkości i pojemności. Sieci te charakteryzują się różnymi poziomami usług: niektóre działają najlepiej, jak to możliwe, w geście dobrej woli, a inne w powiązaniu ze swoimi usługami komercyjnymi. Dzięki dwustronnym umowom operatorów dotyczącym wymiany ruchu, który może, ale nie musi być kierowany do hostów w ich własnej sieci, Internet funkcjonuje jako globalna tkanka, opierając się na dobrowolnym udziale regionalnych i lokalnych centrów wymiany ruchu internetowego oraz dostawców usług.

Taka różnorodność wiąże się jednak z pewnym stopniem nieprzewidywalności. Ścieżka, jaką obiera każdy pakiet w drodze do miejsca przeznaczenia, bazuje na sekwencji najlepszych domysłów i starań. Brak dostępnych w czasie rzeczywistym danych lub modeli predykcyjnych dotyczących rzeczywistych warunków sieciowych występujących w danym momencie powoduje zazwyczaj, że pakiet wykonuje swój następny skok, korzystając z tras domyślnych lub przypuszczalnej najkrótszej ścieżki. Żadna z tych opcji nie uwzględnia stanu usługi sieciowej w decyzjach dotyczących routingu. W wyniku tego pakiety często doświadczają różnych problemów:

- Na najbardziej podstawowym poziomie sieci mogą występować tymczasowe zakłócenia i awarie, które zmniejszają przepustowość i powodują utratę pakietów.
- W miarę nasycania się sieci zatory negatywnie wpływają na wydajność i doświadczenia użytkownika.
- Chociaż tego rodzaju spowolnienia mogą wystąpić w normalnych warunkach działania, coraz większa liczba zakłóceń jest celowo powodowana przez cyberprzestępców, którzy złośliwie zużywają dostępne zasoby.

Misją Cloudflare jest budowanie lepszego Internetu. W tym celu tworzymy infrastrukturę, dzięki której Internet staje się szybszy, bardziej niezawodny i bezpieczniejszy. Jest to możliwe dzięki usługom świadczonym przez sieć Cloudflare i za jej pośrednictwem. To jedna z największych sieci na świecie, która działa z wykorzystaniem naszych własnych serwerów (bez wirtualizacji), prywatnej sieci szkieletowej oraz ogromnej globalnej obecności zapewniającej średnią osiągalność na poziomie 50 ms dla 95% światowej populacji.[1]

Klienci często chcą zrozumieć, w jaki sposób się to odbywa. Jak to możliwe, że Cloudflare realizuje usługi na taką skalę bez kompromisów między bezpieczeństwem a wydajnością, jednocześnie zapewniając niezawodność której potrzebują organizacje? Odpowiedzią jest zestaw celów North Star, które określają, w jaki sposób budujemy naszą infrastrukturę, aby zachowywać wydajność pomimo działań zakłócających — zarówno zewnętrznych, jak i wewnętrznych.

Jak Cloudflare projektuje odporność?

Wiele organizacji koncentruje się na poprawie dostępności, próbując szybciej lub lepiej reagować na awarie. Wymaga to ciągłego inwestowania w systemy i procesy przełączania awaryjnego oraz testowania ich skuteczności. Chociaż są to uzasadnione cele, podejście Cloudflare jest inne: nasze zespoły ds. odporności wkładają ogromny wysiłek w minimalizowanie scenariuszy, w których odzyskiwanie awaryjne jest w ogóle potrzebne.

Inżynieria odporności Cloudflare zaczyna się od prostego pytania: **jak zbudować krytyczną infrastrukturę, która pozostanie operacyjna przy założeniu, że awarie są nieuniknione?**

W momencie wystąpienia awarii usługi Cloudflare zapewniają jej wykrycie i izolację, tak aby nie miała ona wpływu na dostępność. Awarie są usuwane niezależnie od świadczenia usług. Dążymy do tego, aby pojawiające się problemy nie wpływały na dostarczanie naszych rozwiązań.

Aby zrozumieć zasady zapewniania odporności, warto najpierw zdefiniować kluczowe pojęcia dotyczące ścieżek ruchu w Cloudflare oraz cele projektowe dla kluczowych systemów. Na najbardziej abstrakcyjnym poziomie architekturę Cloudflare można podzielić na dwa segmenty: **płaszczyznę sterowania i płaszczyznę danych.** Każdy z nich charakteryzuje się unikalną odpornością i podejściem do awarii.

Odporność płaszczyzny sterowania

Płaszczyzna sterowania zapewnia interfejs zarządzania definiujący źródło prawdy dla konfiguracji usług sieciowych i bezpieczeństwa w środowisku klienta. Sama płaszczyzna sterowania nie przetwarza ruchu (jest to rolą płaszczyzny danych), lecz informuje płaszczyznę danych, które zasady należy egzekwować, i zarządza konfiguracjami w różnych centrach danych.

Usługi płaszczyzny sterowania Cloudflare są zazwyczaj wdrażane w bardziej tradycyjnej, scentralizowanej topologii, w trzech logicznie powiązanych, ale niezależnych centrach danych w regionie podstawowym (np. USA). Te trzy centra danych są replikowane z równoważną pojemnością do regionu dodatkowego (np. UE). Usługi płaszczyzny sterowania zaprojektowano tak, aby były odporne i zapewniały spójne świadczenie usług w przypadku awarii dowolnego centrum danych w lokalizacji podstawowej. Utrata dodatkowych centrów danych w lokalizacji podstawowej spowodowałaby przełączenie awaryjne na centra danych z innego regionu (np. w Europie zamiast w USA).

Zgodnie z filozofią firmy Cloudflare, która koncentruje się na odporności, a nie odzyskiwaniu, stale inwestujemy w pogłębianie naszej odporności.

Na przykład:

- Coraz częściej używamy dwóch regionów płaszczyzny sterowania w konfiguracji aktywny-aktywny, co zwiększa zarówno naszą przepustowość/reaktywność, jak i tolerancję na awarie. W rezultacie możemy wytrzymać więcej rodzajów awarii bez zakłóceń w świadczeniu usług czy konieczności przełączania awaryjnego.
- Zwiększamy również szczegółowość sposobu przenoszenia usług między różnymi lokalizacjami płaszczyzny sterowania, co pozwala nam reagować z większą precyzją na lokalne problemy z infrastrukturą.

Testowanie chaosu

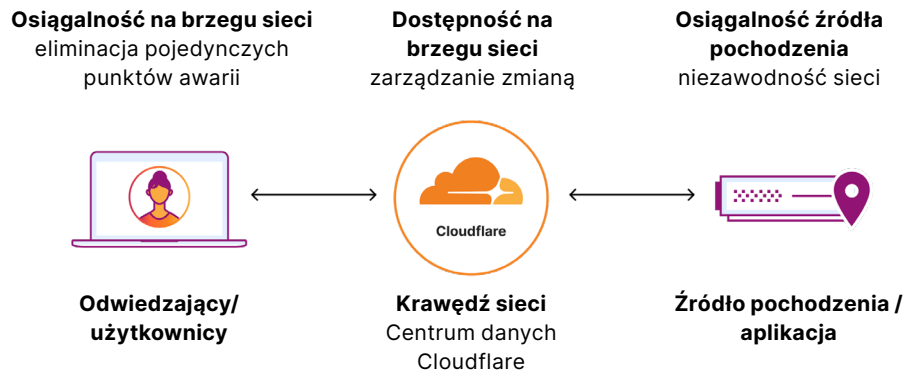
Odporność nie jest kwestią typu „ustaw i zapomnij”. Nawet najbardziej niezawodne plany dotyczące odporności mogą okazać się nieskuteczne z powodu „dryfowania” systemu — powolnej, często niezauważalnej akumulacji zmian, które mogą pogarszać zamierzone zachowania i wprowadzać nieprzewidziane kategorie awarii. Aby proaktywnie zaradzić temu ryzyku, Cloudflare regularnie przeprowadza testy chaosu, systematycznie wyszukując potencjalne luki związane z dryfowaniem.

Odporność płaszczyzny danych

Płaszczyzna danych przetwarza ruch klientów Cloudflare zgodnie z zasadami określonymi w płaszczyźnie sterowania. Chociaż usługi płaszczyzny danych otrzymują instrukcje od płaszczyzny sterowania, nie są one od niej zależne w zakresie funkcjonowania. Wszystkie zasady są utrzymywane w naszym globalnie rozproszonym magazynie typu „klucz-wartość”, Quicksilver, co pozwala zagwarantować, że usługi pozostaną operacyjne i poprawnie skonfigurowane w przypadku wystąpienia zakłóceń komunikacji z płaszczyzną sterowania.

Ważną rolę w redundancji centrów danych odgrywa Anycast. Centra danych Cloudflare, zlokalizowane w ponad 330 miastach, są lokalnie autonomiczne, a jednocześnie wzajemnie wymienne za pośrednictwem Anycast i BGP. Dzieje się tak dzięki temu, że każde centrum danych może lokalnie przetwarzać dowolne usługi, bez współzależności od usług w innym centrum danych. Dzięki Anycast każde centrum danych jest faktycznie nadmiarowe w stosunku do innych. Ponieważ każde centrum danych uczestniczy w Anycast, nie ma potrzeby zlecania klientowi przełączania się do alternatywnego centrum danych pod innym adresem IP.

Niezależnie od tego, który scenariusz jest realizowany — konsument odwiedzający witrynę chronioną przez Cloudflare, pracownik uzyskujący dostęp do aplikacji połączonych z Internetem, czy też biuro łączące się ze swoją siecią WAN — protokół BGP umożliwia znalezienie najbliższego centrum danych Cloudflare Anycast. Jeśli wybrane centrum danych staje się niedostępne, protokół BGP automatycznie przekierowuje do kolejnego najlepszego centrum danych Cloudflare.



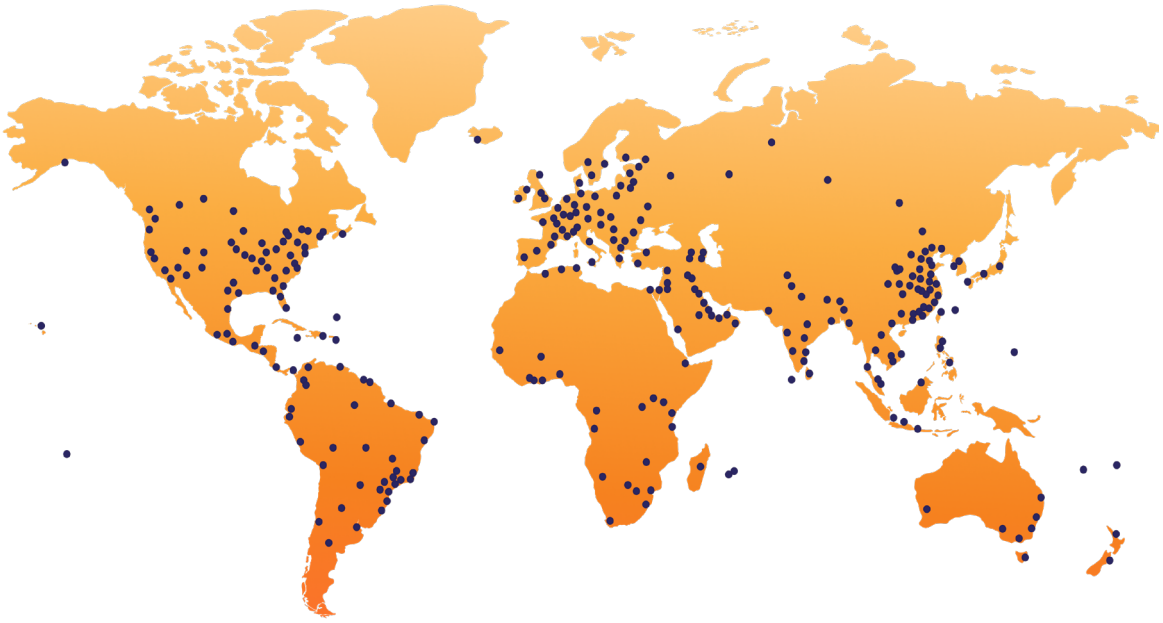
Cloudflare utrzymuje odporność płaszczyzny danych, rozwiązując trzy różne problemy:

- Osiągalność na brzegu sieci: zapewnienie, że ruch użytkowników końcowych może dotrzeć do centrów danych, i wyeliminowanie pojedynczych punktów awarii w ruchu przychodzącym
- Dostępność na brzegu sieci: utrzymywanie jakości kodu i dostępności oprogramowania poprzez rygorystyczne zarządzanie zmianami
- Osiągalność źródła pochodzenia: adaptacyjny routing do aplikacji klienta dla zapewnienia, że nie ma strat na ścieżkach wychodzących

Osiągalność na brzegu sieci

Osiągalność na brzegu sieci to możliwość łączenia się użytkowników końcowych z siecią Cloudflare. Jest to prawdopodobnie najważniejszy element w obszarze problemów związanych z odpornością. W przypadku awarii dostawców usług internetowych (ISP) lub centrów danych osiągalność na brzegu sieci jest ograniczona lub pogorszona, co uniemożliwia lub spowalnia dostęp użytkowników do potrzebnych im zasobów w Internecie. Cloudflare rozwiązuje problemy z osiągalnością na brzegu sieci na cztery kluczowe sposoby:

1. Sieć Anycast



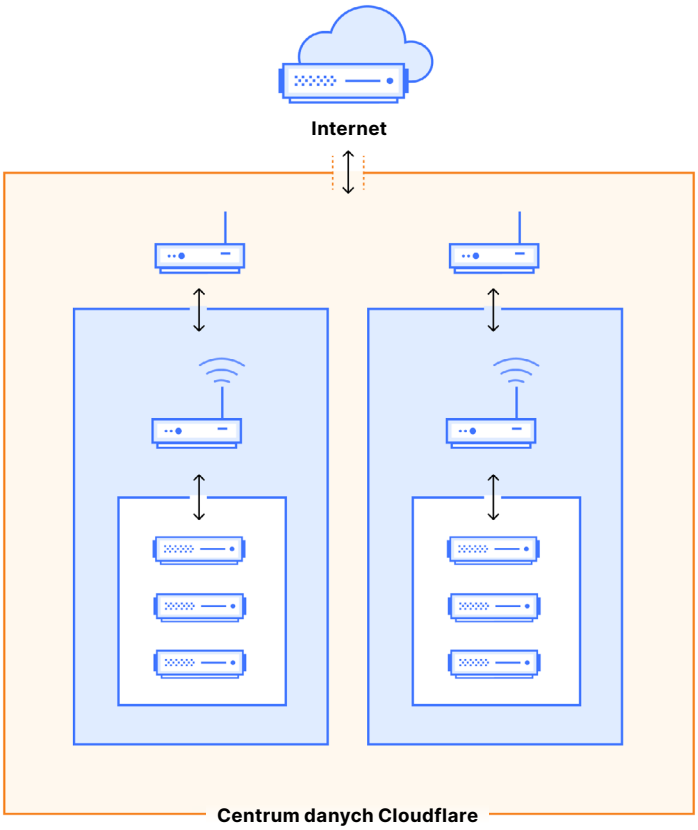
Lepsza wydajność sieci wraz z jej odpornością jest wbudowana w naszą architekturę sieciową, która w dużej mierze opiera się na technologii Anycast. Rozwiązanie Anycast — inżynieryjne osiągnięcie Cloudflare — powoduje, że przestrzeń IP jest reklamowana wszędzie. Jeśli którykolwiek z naszych punktów obecności (PoP) stanie się nieaktywny, ruch będzie po prostu kierowany do innych lokalizacji zamiast odrzucenia. Fakt, że Cloudflare jest obecne w tylu miastach na całym świecie i ma komunikację równorzędną z lokalnymi sieciami, oznacza, że przetwarzamy ruch klientów tak blisko użytkownika, jak to tylko możliwe. Jeśli na przykład tranzyt dostawcy usług internetowych zostanie odłączony lub centrum danych utraci zasilanie, ruch pozostanie nienaruszony.

2. Każda usługa Cloudflare działa w każdej lokalizacji

Oprócz zastosowania Anycast centra danych Cloudflare są zaprojektowane w taki sposób, aby mogły przetwarzać ruch lokalnie, bez współzależności od łańcuchów proxy dla innych zasobów obliczeniowych. Na każdym urządzeniu uruchamiamy niemal każdą usługę. To oznacza, że centrum danych może zostać przełączone w tryb offline bez wpływu na klientów. Urządzenia w centrum danych można wzajemnie zastępować, ponieważ setki z nich obsługują tę samą usługę i są w stanie przejąć jej działanie w przypadku awarii jednego z nich.

3. Wielokolokacyjne punkty PoP

Projekt i lokalizacje centrów danych Cloudflare odzwierciedlają potrzeby naszych klientów. Sieć Anycast umożliwia nam dodawanie i usuwanie centrów danych według uznania, ale musimy stale monitorować wydajność klientów. Dostosowaliśmy topologie naszych centrów danych, aby sekcje mocy obliczeniowej (kolokacje) mogły ulegać awarii niezależnie od siebie. Te centra danych (z wieloma kolokacjami) nazywane są wielokolokacyjnymi punktami obecności lub inaczej lokalizacjami MCP (multi-collocation points of presence).



Takie lokalizacje oddzielają łączność z Internetem od wewnętrznej łączności obliczeniowej, aby umożliwić indywidualne wyłączanie kolokacji. Oznacza to, że nawet w przypadku problemu z kolokacją cały punkt PoP w regionie może pozostać online, zapewniając klientowi dłuższy czas pracy bez przestojów i lepszą wydajność. Ten typ centrum danych eliminuje również pojedyncze punkty awarii dzięki redundantnym urządzeniom w warstwie ukierunkowanej na Internet (na krawędzi): jeśli jeden router brzegowy ulegnie awarii, drugi router brzegowy może przejąć ruch i zapewnić ciągłość działania lokalizacji.

Ten model operacyjny pomaga lokalizacjom MCP unikać przenoszenia ruchu, chyba że jest to absolutnie konieczne, a dodatkowo zwiększa czas pracy bez przestojów dla klientów Cloudflare.

4. Menedżer ruchu Cloudflare

Centra danych MCP współpracują ze sobą, tworząc szerszą sieć Cloudflare. Wykorzystuje ona usługę Anycast, aby zapewnić obsługę ruchu klientów. Usługa Anycast została wzbogacona o deterministyczne zarządzanie ruchem, dzięki któremu żądania klientów są obsługiwane tam, gdzie możemy je obsłużyć z najlepszą możliwą wydajnością. Ten system zarządzania ruchem (menedżer ruchu) działa na zasadzie ciągłego sondowania sieci Cloudflare i automatycznie przekierowuje ruch z centrów danych, które doświadczają przeciążenia procesora. Pozwala to uniknąć zatorów w centrach danych o dużym ruchu. Zamiast tego ruch jest inteligentnie kierowany do innego centrum danych, które może go obsłużyć.

Dostępność na brzegu sieci

Dostępność na brzegu sieci odnosi się do zdolności Cloudflare do przetwarzania ruchu po dotarciu do naszej sieci. Gdy modyfikacje wprowadzane w narzędziach sieciowych lub oprogramowaniu skutkują niezamierzonymi zmianami, dostępność może się zmniejszyć i negatywnie wpływać na komfort użytkowania. Aby zapobiec incydentom wynikającym ze zmian w kodzie, Cloudflare zainwestowała znaczne środki w następujące mechanizmy kontroli wdrażania:

1. Lejek wdrożeniowy

Podczas wdrażania oprogramowania zapewnianie jakości kodu zaczyna się od śledzenia i ograniczania możliwości programistów i klientów do wprowadzania zmian w ekosystemie. Cloudflare ogranicza liczbę sposobów, na jakie można wprowadzać zmiany w naszej infrastrukturze, dzięki czemu możemy ściśle monitorować każdą zmianę i upewnić się, że przejdą one szereg testów przed wdrożeniem produkcyjnym.

2. Zarządzanie zakresem oddziaływania zmian

Innym sposobem, w jaki Cloudflare wspiera dostępność na brzegu sieci podczas wdrażania, jest ograniczenie ich do testowych centrów danych lub grup testowych, zanim zostaną wdrożone na szeroką skalę. Nazywamy to zarządzaniem zakresem oddziaływania.

Wdrożone zmiany w sieci mogą zacząć działać globalnie w ciągu kilku minut. Ograniczanie zmian do środowiska wdrożeniowego oraz wdrażanie kolejnych zmian w sposób kaskadowy umożliwia nam monitorowanie skutków zmiany pod kątem jej zamierzonych i niezamierzonych konsekwencji, zanim wpłynie to na większe obszary geograficzne lub populacje użytkowników.

Mamy dwa sposoby na ograniczenie wpływu zmian w kodzie:

- Ograniczenie liczby lokalizacji, do których wprowadzane są zmiany
- Ograniczenie liczby użytkowników otrzymujących zmiany

Ograniczając liczbę lokalizacji i urządzeń, które otrzymują zmiany, możemy zagwarantować prawidłowe testy A/B kodu w jednej lokalizacji, aby ocenić jego stan przed kontynuowaniem. Ograniczając liczbę użytkowników, którzy otrzymują zmiany, możemy najpierw przetestować poprawki na mniejszych grupach użytkowników.

3. Wdrożenie uzależnione od kondycji

Wdrożenie zależne od kondycji to system programowo oceniający przydatność wydania na podstawie wstępnie ustawionych wskaźników, które dają sygnał „zgody” lub „braku zgody” w zależności od potencjalnego wpływu. Ta seria zautomatyzowanych kontroli może nie tylko zapobiec wprowadzeniu szkodliwego wydania, ale także wycofać je po wykryciu problemów.

Każdy produkt i usługa wdrożone za pośrednictwem Cloudflare muszą mieć docelowy poziom usługi (SLO), który obejmuje zarówno wskaźnik przedstawiający kondycję produktu, jak i poziom docelowy, poniżej którego produkt zostałby uznany za działający nieprawidłowo.

Wskaźnik SLO ma określone akceptowalne progi awarii. W ramach scalania zmiany, która ma zostać wdrożona, każda usługa z wdrożeniem uzależnionym od kondycji przekazuje wartości wskaźnika SLO do zautomatyzowanego systemu. W każdym zdefiniowanym zakresie wdrożenia (plany bezpłatne, podgrupa urządzeń w Ashburn itp.) zautomatyzowany system realizuje następujące działania:

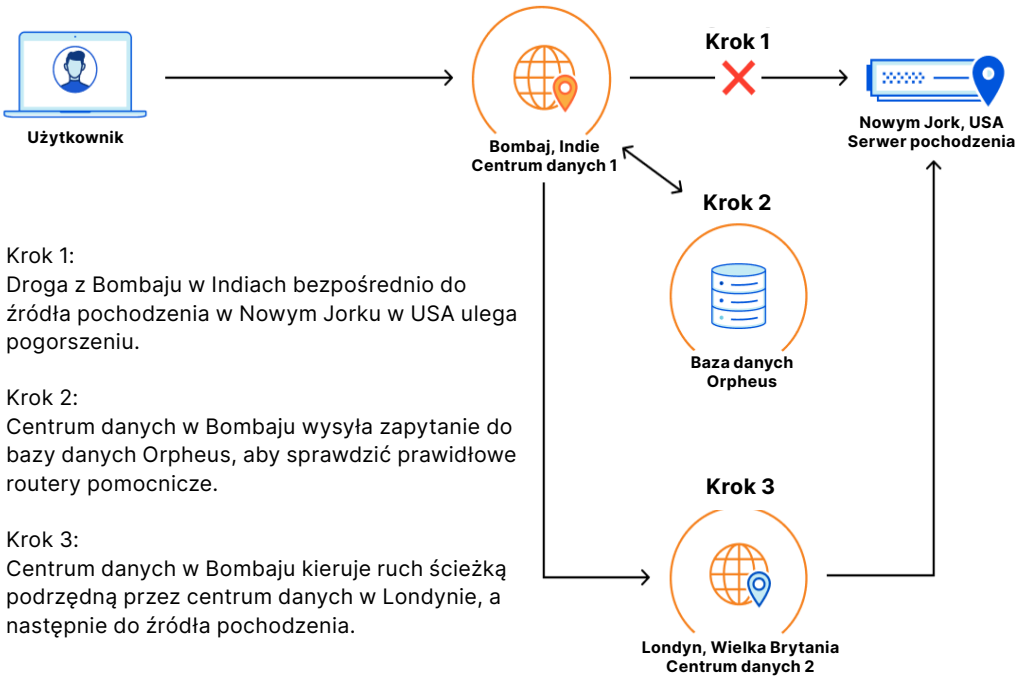
- System monitoruje w pierwszej kolejności wskaźnik SLO usługi przez określony czas, aby upewnić się, że kondycja nie spada poniżej progu.
- Jeśli wskaźnik SLO pozostaje w akceptowalnym zakresie przez ustawiony okres próbny, system automatycznie przechodzi do etapu większego wdrażania.
- Jeśli jednak poziom wskaźnika SLO zostaje naruszony, system samoczynnie wstrzymuje wdrożenie i wycofuje zmiany, aby automatycznie złagodzić skutki.

Te kroki gwarantują, że wdrożenia kodu nie będą miały wpływu na kondycję klienta, a czas trwania problemów będzie jak najkrótszy.

Osiągalność źródła pochodzenia

Osiągalność źródła pochodzenia odnosi się do zdolności Cloudflare do dotarcia do miejsc docelowych, niezależnie od tego, czy jest to źródło klienta, witryna SaaS czy publiczny Internet za pośrednictwem Cloudflare Gateway. Routing żądań tam, gdzie powinny trafić, ma kluczowe znaczenie dla użytkowników uzyskujących dostęp do sieci Cloudflare. Na przykład Argo Smart Routing, narzędzie Cloudflare, które optymalizuje wydajność (tj. czas do pierwszego bajtu (TTFB)), nieustannie sonduje sieć Cloudflare, aby znaleźć najszybszą ścieżkę do źródła pochodzenia.

Orpheus, odpowiednik Argo, ma podobną filozofię, ale inną funkcję. Jego zadaniem jest nawiązywanie niezawodnych połączeń z serwerami pochodzenia. Orpheus analizuje zdolność firmy Cloudflare do dotarcia do źródła (w przeciwieństwie do najszybszej ścieżki do źródła) i znajduje ścieżki, które minimalizują utratę pakietów bez wpływu na stabilność wydajności. Oznacza to, że w przypadku wystąpienia problemów ruch jest automatycznie kierowany z pominięciem lokalizacji z wykrytymi błędami.



Krok 1:
Droga z Bombaju w Indiach bezpośrednio do źródła pochodzenia w Nowym Jorku w USA ulega pogorszeniu.

Krok 2:
Centrum danych w Bombaju wysyła zapytanie do bazy danych Orpheus, aby sprawdzić prawidłowe routery pomocnicze.

Krok 3:
Centrum danych w Bombaju kieruje ruch ścieżką podrzędną przez centrum danych w Londynie, a następnie do źródła pochodzenia.

Przed wydaniem rozwiązania Orpheus przez firmę Cloudflare w 2021 roku byliśmy w stanie z powodzeniem korzystać z routingu do źródeł w 99,9% przypadków. Po jego wdrożeniu nasza zdolność do kierowania do źródeł wzrosła do 99,99%. W nadchodzącym roku będziemy rozbudowywać rozwiązanie Orpheus, aby chronić więcej rodzajów ruchu, reagować na więcej scenariuszy awarii i pracować szybciej w celu skrócenia czasu, przez który jakikolwiek użytkownik pozostaje dotknięty skutkami problemów.

Zobowiązanie do przejrzystości operacyjnej

Awarie mogą wystąpić nawet w najbardziej odpornych i innowacyjnych sieciach. Gdy pojawiają się incydenty i mają one wpływ na klientów, Cloudflare stosuje się do procedury ich komunikowania, która obejmuje dokładne dochodzenie, wewnętrzny i zewnętrzny raport dotyczący incydentu oraz, w razie potrzeby, aktualizacje statusu przez cały okres trwania incydentu.

W niektórych przypadkach, gdy incydenty mają taki wpływ — lub mogą być podstawą innowacji — analizy przypadku są publikowane w blogu Cloudflare.

Wnioski

Wysiłki inżynieryjne stojące za działaniem sieci Cloudflare są złożone, ale jest to praca, którą z dumą wykonujemy dla naszych klientów. Nagrodą jest zbudowanie platformy sieciowej, która przynosi korzyści naszym klientom i całej społeczności internetowej.

Traktując odporność nie tylko jako kwestię techniczną, ale także jako kluczową filozofię operacyjną, robimy coś więcej niż tylko wzmacnianie zabezpieczeń — aktywnie budujemy firmę, która z natury jest gotowa na przyszłe wyzwania. Proaktywne podejście polegające na ciągłym testowaniu i dostosowywaniu oznacza, że możemy płynnie ewoluować wraz ze stale zmieniającymi się wymaganiami naszych klientów i dynamicznym krajobrazem samego Internetu.

Rozumiemy, że wiele kwestii przedstawionych w tym dokumencie dotyczy koncepcji sieciowych, z którymi duża część przedsiębiorstw nie ma styczności, ponieważ wiążą się one z wewnętrzną architekturą globalnego środowiska chmurowego klasy operatorskiej.

W celu poznania szczegółowego omówienia tych zagadnień oraz uzyskania dodatkowych informacji na temat inżynierii odporności Cloudflare zapraszamy do skontaktowania się ze swoim przedstawicielem Cloudflare.

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/pl-pl/

REV:BDES-8251.2025OCT28