CLOUDFLARE

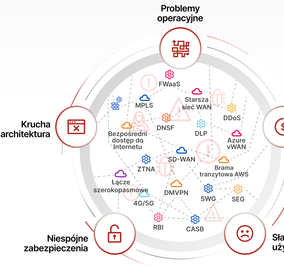
Każda ścieżka ma znaczenie

Czy nadszedł czas na zmianę tras przepływów sieciowych?

Starsze sieci korporacyjne koncentrowały się wyłącznie na łączności wewnętrznej i bezpieczeństwie. Jednak praca hybrydowa, aplikacje wdrażane w chmurze oraz szybkie inwestycje w modernizację cyfrową drastycznie zmieniły miejsce i sposób przepływu ruchu sieciowego.

Co się stanie, jeśli infrastruktura sieciowa nie będzie gotowa na dzisiejsze wymagania biznesowe?

Starsze sieci korporacyjne często doświadczają następujących problemów:



52% menedżerów wyższego szczebla twierdzi, że **złożoność jest największą przeszkodą** w prowadzeniu operacji bezpieczeństwa[1]

70% prezesów firm na całym świecie twierdzi, że poziom **dojrzałości sieciowej negatywnie wpływa** na realizację celów biznesowych[2]

101% to średni **zwrot z inwestycji (ROI) w organizacjach opartych na modelu platformowym,** w porównaniu do 28% ROI w przypadku tych, które nie przyjęły tego modelu[1]

W tradycyjnych architekturach stosowanie dziesiątek różnych rozwiązań do obsługi czterech rodzajów przepływów sieciowych dodatkowo zwiększa złożoność

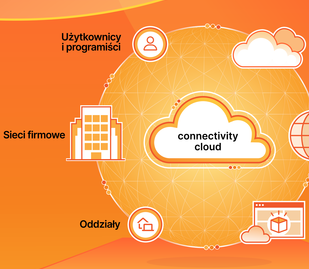
Przepływ ruchu	Wymagane produkty	Wyzwania
Ruch przychodzący z Internetu	Tradycyjnie obsługiwany przez zapory lokalne, połączenia VPN, infrastrukturę DMZ oraz filtrowanie dostawców usług internetowych	• Ataki typu DoS i DDoS • Wykorzystanie luk typu zero-day • Phishing • Złośliwe oprogramowanie
Ruch wychodzący do Internetu i aplikacji w chmurze	Tradycyjnie obsługiwany przez zapory lokalne i serwery proxy	• Ruch boczny • Narażenie danych • Propagacja oprogramowania typu ransomware • Uczestnictwo w sieci botów
Sieci WAN łączące kampusy i oddziały	Tradycyjnie obsługiwane przez połączenia fizyczne/wirtualne, SD-WAN, prywatne połączenia międzysieciowe oraz MPLS	• Wyższe koszty CapEx/OpEx • Opóźnienia sieciowe • Ograniczenia przepustowości • Słabe doświadczenia użytkownika
Obsługa wielu chmur dla aplikacji w wielu chmurach	Tradycyjnie obsługiwane przez produkty DIY	• Problemy z widocznością i egzekwowaniem zasad • Złożoność regulacyjna

Co musi się zmienić?

Tradycyjne sieci	Nowoczesne sieci
• Wstawiane urządzenia w celu dodania nowej funkcjonalności lub obsługi kolejnych lokalizacji, powodujące przestoje i zakłócenia w działaniu usług • Zabezpieczeni użytkownicy i oddziały połączeni z aplikacjami hostowanymi w centrum danych • Domyślnie „zaufany" ruch wewnątrz obwodu • Zoptymalizowane pod kątem obsługi pracowników biurowych	• Wdrażanie komponowalnych usług zamiast urządzeń, co zmniejsza złożoność i zakłócenia • Wymagana obsługa aplikacji w chmurze, SaaS oraz w chmurach prywatnych — w każdym miejscu • Należy założyć, że każda jednostka, w tym rozproszeni użytkownicy, urządzenia, aplikacje i dane, jest „niezaufana" • Nie można zakładać lokalizacji użytkownika, a system musi zapewniać obsługę użytkowników pracujących z dowolnego miejsca

Jak sprostać współczesnym wymaganiom, jednocześnie uwzględniając wszystkie przepływy ruchu sieciowego?

Platforma connectivity cloud nie stosuje rozproszonych rozwiązań dla każdej ścieżki ruchu, lecz podchodzi całościowo do modernizacji sieci.



Ruch przychodzący

Chroń sieć i aplikacje przed atakami DDoS i innymi zagrożeniami pochodzącymi z Internetu

Ruch wychodzący

Chroń użytkowników i biura przed zagrożeniami, egzekwuj spójne zasady oraz kontroluj dane w aplikacjach

Sieci WAN

Połącz i zabezpiecz biura, użytkowników, urządzenia, centra danych oraz infrastrukturę

Ruch wielochmurowy

Zapewnij sieć umożliwiającą łączenie, zabezpieczanie i tworzenie aplikacji w środowiskach chmury publicznej/hybrydowej

Oferowane przez Cloudflare rozwiązanie connectivity cloud charakteryzuje się komponowalną, programowalną architekturą, aby zapewnić usługi sieciowe i bezpieczeństwa zarówno użytkownikom, jak i całej infrastrukturze biznesowej oraz aplikacjom działającym w środowiskach chmurowych.

- Wyeliminuj konieczność rozbudowy lub rozszerzania prywatnych centrów danych
- Korzystaj z usług sieciowych i bezpieczeństwa opartych na chmurze zamiast z urządzeń fizycznych
- Ogranicz nadmierne „zaufanie" w sieci dzięki modelowi Zero Trust

Dowiedz się więcej o tym, jak wykorzystać rozwiązania Cloudflare do uproszczenia i przyspieszenia modernizacji sieci

Dowiedz się więcej

1. Al, Mohamad, Jenkins, BJ. „Capturing the cybersecurity dividend". IBM. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyrfnet-cybersecurity platform. Dostęp: 26 czerwca 2025 r.

2. „70% Of CEOs Say Their Network Is Slowing Business Growth, New NTT Study Finds". Business Wire, 20 października 2022 r., https://www.businesswire.com/news/home/20221020005120/en/70-Of-CEOs-Say-Their-Network-Is-Slowing-Business-Growth-New-NTT-Study-Finds (komunikat prasowy).

+44 20 3514 6970 | enterprise@cloudflare.com | Cloudflare.com

CLOUDFLARE

REV:BDES-7841.2025JUL31