# Magic WAN

Magic WAN upraszcza drogę do modelu SASE, oferując łączność typu każdy z każdym

## Ewolucja architektur sieciowych

**Internet jako nowa sieć firmowa**

W sytuacji, gdy praca hybrydowa staje się nową normalnością, a aplikacje są przenoszone do chmury, zespoły ds. IT muszą stawiać czoła wielu problemom:

- **Złożoność sieci:** zapewnianie połączeń MPLS oraz dostosowywanie rozwiązań punktowych zajmuje zbyt dużo czasu
- **Luki w zabezpieczeniach:** bezpośrednie połączenia z Internetem omijają zabezpieczenia i polityki akceptowalnego użytkowania, co stwarza ryzyko dla użytkowników i danych
- **Wysokie koszty:** łącza MPLS oraz punktowe rozwiązania z zakresu bezpieczeństwa generują niepotrzebne wydatki
- **Słabe doświadczenie użytkownika:** przekazywanie ruchu do granicznego stosu rozwiązań z zakresu bezpieczeństwa powoduje opóźnienia

Usługa Magic WAN upraszcza łączność sieciową między lokalizacjami oddziałów, wieloma wirtualnymi chmurami prywatnymi (VPC) lub centrami danych a platformą SASE Cloudflare One, zapewniając bezpieczną, wydajną i tanią łączność umożliwiającą zespołom ds.
IT uporanie się z wyzwaniami związanymi z pracą hybrydową i rozwiązaniami wielochmurowymi.

W przeciwieństwie do nieelastycznych, kosztownych sieci MPLS lub złożonych wdrożeń sieci SD-WAN opartych na zaporach lokalnych, w ramach usługi Magic WAN stosowane jest podejście „light branch, heavy cloud" w celu rozbudowy lub zastąpienia obecnej architektury. Charakteryzuje się ono łatwością wdrożenia, skalowalnością wraz ze zmieniającymi się wymaganiami biznesowymi, jak również wbudowanymi zabezpieczeniami.

Magic WAN łączy fizyczne lub wirtualne lokalizacje sieciowe z platformą SASE Cloudflare. Przykładami lokalizacji fizycznych mogą być oddziały firmy, hale produkcyjne, punkty sprzedaży detalicznej, główne biura czy centra danych. Z kolei przykładami lokalizacji wirtualnych są usługi w chmurze publicznej, takie jak AWS, Azure, GCP i OCI.

**Większa elastyczność operacyjna**

Centralne zarządzanie bezpieczeństwem sieci i łącznością z jednej konsoli administracyjnej. Ruch dotyczący rozwiązań typu on-ramp w ciągu kilku minut dzięki konfiguracji bezdotykowej.

**Wbudowane, a nie dobudowane zabezpieczenia**

Uzyskaj natywną ochronę chmurową przed atakami DDoS, zaporę sieciową oraz rozwiązania SSE i Zero Trust — wszystko to głęboko zintegrowane i świadczone jako usługa.

**Niższe koszty dotyczące sieci**

Zminimalizuj ślad swojego oddziału i przenieś funkcje sieciowe do chmury, aby zmniejszyć zależność od drogich rozwiązań MPLS i odejść od sieci SD-WAN.

## Główne przypadki użycia dotyczące usługi Magic WAN

### Usprawnienie łączności sieciowej

- **Uproszczenie łączności oddziałów** — zastąp mozaikę autorskich obwodów i urządzeń sieciowych, aby bezpiecznie przekierowywać ruch między oddziałami i centrami danych. Usprawnij łączność między lokalizacjami za pomocą tuneli Anycast IPSec.
- **Uproszczenie łączności hybrydowej i wielochmurowej** — organizacje posiadają aplikacje w instancjach chmurowych różnych dostawców (np. AWS, GCP, Azure, Oracle, IBM) *oraz* w lokalnych centrach danych. Użyj scentralizowanych narzędzi kontrolnych do przekierowywania i zabezpieczania ruchu w tych zróżnicowanych środowiskach.

### Zwiększenie bezpieczeństwa bez poświęcania wydajności

- **Bezpieczna łączność WAN** — zabezpiecz połączenia poprzez egzekwowanie polityki bezpieczeństwa sieci między lokalizacjami (oddziałami, centrami danych itp.) za pomocą dostarczanych w chmurze środków bezpieczeństwa, takich jak zapora i SWG.
- **Skalowanie wydajności WAN** — wdrożenia MPLS są kosztowne, nieelastyczne i powolne. Przejście na rozwiązania Cloudflare zapewnia obniżkę kosztów oraz bardziej elastyczne wdrożenie z wbudowanymi zabezpieczeniami.

## Przystępowanie do wdrożenia Magic WAN

### Transformacja sieci jest podróżą

Magic WAN zapewnia wydajność i niezawodność połączenia internetowego, pomagając organizacjom w migracji ze starszych architektur sieciowych. Rozpocznij od stopniowego wdrażania usługi Magic WAN, realizując przejście w dłuższym czasie. Oferowana przez Cloudflare kombinacja „light branch, heavy cloud", obejmująca łączność na ostatniej mili oraz wydajność, niezawodność i bezpieczeństwo na środkowej mili, pozwala poprawić komunikację i bezpieczeństwo pracy hybrydowej. Nasza architektura umożliwia przeprowadzenie wdrożenia obok istniejącej infrastruktury, dzięki czemu migracja będzie przebiegała w tempie wskazanym przez Ciebie.

# Porównanie architektury Cloudflare One z rozwiązaniami MPLS i SD-WAN

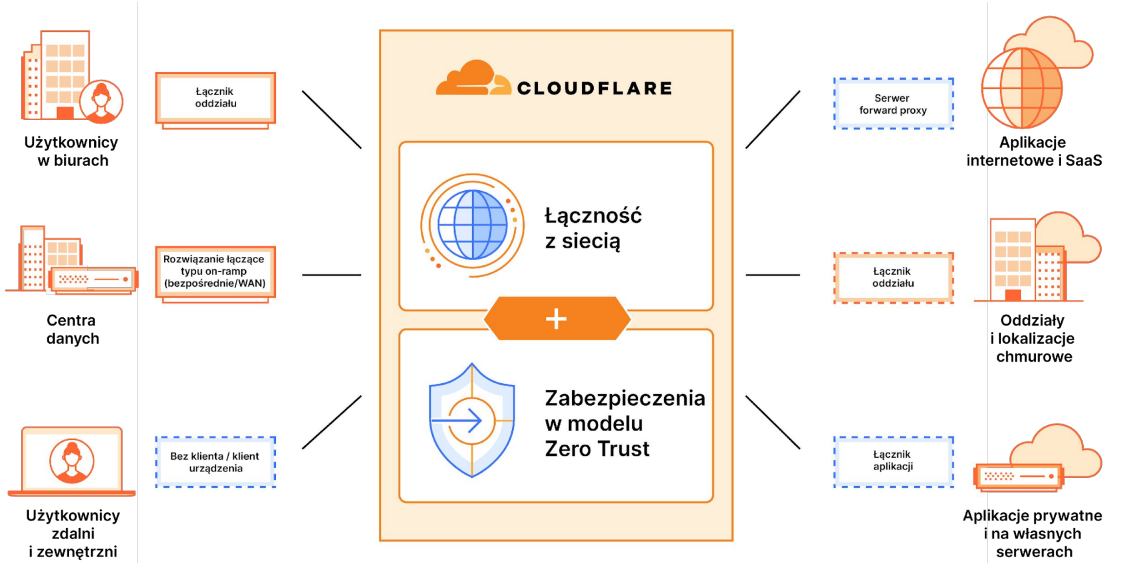
Wraz z przenoszeniem aplikacji do chmury oraz upowszechnianiem się pracy hybrydowej w organizacjach maleje wydajność i bezpieczeństwo działania tradycyjnych architektur sieciowych. Przekazywanie ruchu skutkuje pogorszeniem wydajności i doświadczenia użytkownika, a zezwalanie na lokalne połączenia z sieciami zewnętrznymi obniża spójność i skuteczność zabezpieczeń. Żaden z tych efektów nie jest pożądany, a ustępstwa przy projektowaniu sieci sprawiają, że potrzeby organizacyjne i indywidualne pozostają niezaspokojone.

W ostatnim czasie w sieciach SD-WAN wprowadzono nakładki umożliwiające zarządzanie ruchem, w nadziei, że stworzy to alternatywę dla sieci MPLS. W kwestiach bezpieczeństwa sieci SD-WAN polegają jednak w dużej mierze na urządzeniach brzegowych, co skutkuje koniecznością łączenia przez zespoły ds. IT różnorodnych elementów, takich jak narzędzia sprzętowe, wirtualne i oparte na chmurze. Ta dodatkowa złożoność niweluje wiele z zamierzonych korzyści.

Platforma SASE firmy Cloudflare umożliwia bezpieczną współpracę sieciową w ramach naszej chmury connectivity cloud, pozwalając organizacjom korzystać z naszej sieci jako rozszerzenia ich własnej. Uproszczone zarządzanie, niezawodne działanie, bezpieczeństwo dzięki modelowi Zero Trust oraz niższe całkowite koszty użytkowania to korzyści, których jednoczesne osiąganie jest możliwe wyłącznie dzięki prawdziwie nowatorskiemu podejściu do SASE.

| Kryteria | Usługa MPLS/VPN | SD-WAN | SASE z Cloudflare One |
|---|---|---|---|
| **Konfiguracja**<br>Konfiguracja nowej lokalizacji i zarządzanie nią | Przez dostawcę usług zarządzanych (MSP), przy użyciu żądania usługi | Uproszczona orkiestracja i zarządzanie za pośrednictwem scentralizowanego kontrolera | Automatyczna orkiestracja za pośrednictwem portalu SaaS; scentralizowany pulpit nawigacyjny |
| **Kontrola ruchu na ostatniej mili**<br>Równoważenie ruchu, jakość usługi (QoS) oraz przełączanie awaryjne | Objęte umowami SLA dotyczącymi MPLS | Wybór najlepszej ścieżki dostępny w urządzeniu SD-WAN | Minimalne wdrożenie lokalne w celu kontrolowania lokalnego podejmowania decyzji |
| **Kontrola ruchu na środkowej mili**<br>Omijanie zatorów ruchu na środkowej mili | Objęte umowami SLA dotyczącymi MPLS | „Tunnel spaghetti” i brak kontroli nad środkową milą | Zintegrowane zarządzanie ruchem i elementy kontrolne prywatnej sieci szkieletowej w tym samym interfejsie |
| **Integracja w chmurze**<br>Łączność na potrzeby migracji do chmury | Scentralizowane tworzenie połączeń z sieciami zewnętrznymi | Zdecentralizowane tworzenie połączeń z sieciami zewnętrznymi | Łączność natywna dzięki Cloud Network Interconnect |
| **Bezpieczeństwo**<br>Filtrowanie przychodzącego i wychodzącego ruchu internetowego pod kątem złośliwego oprogramowania | Mozaika sprzętowych elementów kontrolnych | Mozaika sprzętowych i/lub programowych elementów kontrolnych | Natywna integracja z narzędziami bezpieczeństwa dotyczącymi użytkowników, danych, aplikacji i sieci |
| **Koszty**<br>Maksymalizacja zwrotu z inwestycji w sieć | Wysoki koszt sprzętu i łączności | Zoptymalizowane koszty łączności za cenę wzrostu kosztów sprzętu i oprogramowania | Niższe koszty sprzętu i łączności w celu maksymalizacji zwrotu z inwestycji |

# Kierowanie ruchu na platformę Cloudflare SASE




Łącznik Magic WAN ułatwia połączenie Twoich lokalizacji sieciowych z Cloudflare. Użyj oprogramowania łącznika oddziału, które jest wstępnie zainstalowane i skonfigurowane na sprzęcie certyfikowanym przez Cloudflare w celu uproszczenia wdrożenia, bądź zainstaluj oprogramowanie na fizycznych lub wirtualnych urządzeniach z systemem Linux w swoim środowisku.

**Część powiększającej się rodziny elastycznych rozwiązań łączących typu on-ramp**

Pierwszym krokiem na drodze do przyjęcia modelu SASE jest nawiązanie połączenia — ustanowienie bezpiecznej ścieżki z istniejącej sieci do najbliższej lokalizacji, w której mogą być stosowane polityki bezpieczeństwa Zero Trust. Cloudflare oferuje szeroki zestaw „ramp" umożliwiających taką łączność, w tym opcje dostępu w trybach z klientami i bez klientów na potrzeby użytkowników pracujących hybrydowo, tunele w warstwie aplikacji ustanowione w wyniku wdrożenia lekkich łączników programowych, łączność w warstwie sieci z tunelami GRE lub IPsec korzystającymi z Anycast, jak również fizyczne lub wirtualne połączenia międzysystemowe na potrzeby prywatnych centrów danych oraz chmur publicznych.

Aby jeszcze bardziej ułatwić przyjęcie SASE, w dowolnej fizycznej lub chmurowej lokalizacji sieciowej może zostać wdrożony łącznik Magic WAN zapewniający automatyczną łączność z optymalnym centrum danych Cloudflare, co pozwala wykorzystać istniejące łącze internetowe ostatniej mili oraz wyeliminować konieczność ręcznej konfiguracji sprzętu sieciowego przez zespoły ds. IT w celu nawiązania połączenia.

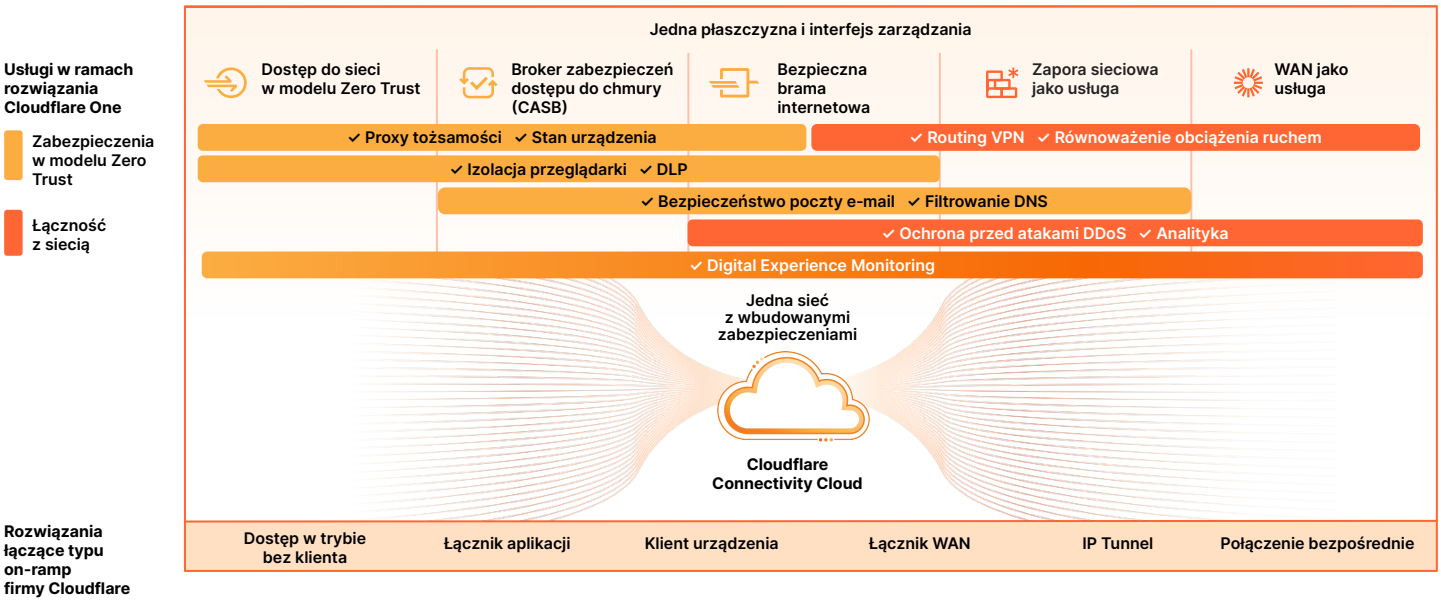
# Możliwości oprogramowania i specyfikacje sprzętowe

| Możliwości oprogramowania Magic WAN[1] | |
|---|---|
| **Konfiguracja łącznika WAN** | Urządzenia infrastruktury lokalnej klienta typu plug-and-play, skonfigurowane automatycznie bez ingerencji użytkownika, które są zarządzane centralnie z pulpitu nawigacyjnego Cloudflare lub interfejsu API. Automatyczne konfigurowanie tuneli i tras IPsec pod kątem kierowania ruchu do sieci Cloudflare na potrzeby funkcji łączności i bezpieczeństwa. Automatyczne uaktualnienia oprogramowania (w ramach okna serwisowego zdefiniowanego przez klienta). |
| **Konfiguracja w lokalizacji łącznika WAN** | Pomoc techniczna dotycząca konfiguracji statycznego adresu IP lub DHCP w sieciach WAN/LAN. Pomoc techniczna dotycząca wirtualnych sieci LAN oraz segmentacji sieci lokalnych. |
| **Podejście „Light branch, heavy cloud”** | Lekki łącznik WAN o dużej dostępności, z funkcjami równoważenia obciążenia ruchem oraz przełączania awaryjnego między wieloma obwodami WAN na podstawie kontroli kondycji. Usługi bezpieczeństwa, takie jak zapora i funkcje SSE Zero Trust, dostarczane z chmury Cloudflare Connectivity Cloud. |
| **Integracja z rozwiązaniami podmiotów zewnętrznych** | Skonfiguruj punkty końcowe tuneli Anycast IPsec lub GRE z istniejącymi chmurami VPC, takimi jak Amazon AWS Transit Gateway, lub infrastrukturą lokalną klienta, taką jak SD-WAN, zapora i routery. Skonfiguruj trasy statyczne z przekazywaniem pakietów ECMP do sieci Cloudflare. |
| **Wbudowane zabezpieczenia** | Wbudowana zapora warstwy L3 i wykrywanie włamań; bezproblemowa integracja z innymi funkcjami SSE/bezpieczeństwa oraz rampami, takimi jak bezpieczna brama internetowa warstw L4–7, klient urządzenia, łącznik aplikacji itp. |
| **Widoczność i kontrola** | Wykrywanie ruchu i routing na podstawie aplikacji. Kontrola przepustowości. Widoczność/analizy danych statystycznych dotyczących tunelu, ruchu i urządzenia dostępne za pośrednictwem pulpitu nawigacyjnego, interfejsu API, dzienników lub języka GraphQL. Zarządzanie z wykorzystaniem pulpitu nawigacyjnego Cloudflare, interfejsu API lub rozwiązania Terraform. |
| **Dane techniczne opcji sprzętowych łącznika Magic WAN[2]** | |
| **Dane techniczne urządzenia** | • **Porty:** (6× 1 Gb/s, miedziane, RJ45) + (2× 10 Gb/s SFP+) + (2x USB 3.0, typ A)<br>• **Wymiary:** 8,1 × 7,9 × 2,0 cala; 1,5 RU; **Waga:** 2,87 funta<br>• **Opcje montażu:** umieszczenie na biurku, montaż na ścianie lub w szafie (z półką)<br>• **TPM:** 2.0, cały świat z wyjątkiem Chin<br>• **Procesor:** Denverton 4 Core C3558<br>• **Dysk:** M.2 120 GB SSD z 16 Gb/s pamięci Flash eMMC<br>• **RAM:** 8 GB DDR4<br>• **Wi-Fi i Bluetooth:** 802.11ac, 2×2 MIMO, maksymalna przepustowość PHY: 866,7 Mb/s<br>• **Wentylator:** jeden |

[1] Cała dokumentacja na poziomie funkcji Magic WAN znajduje się w dokumentach Cloudflare
[2] Sprzęt certyfikowany przez Cloudflare, ze wstępnie zainstalowanym oprogramowaniem Magic WAN: Dell VEP 1425, sprzedawany przez partnera (z montażem w szafie)

# Łączność z siecią i droga do modelu SASE

**Rozwiązanie Cloudflare Connectivity Cloud zapewnia prostotę wdrożenia, odporność sieci oraz szybkość wprowadzania innowacji, które są potrzebne, aby utrzymać przewagę podczas konsolidowania rozwiązań punktowych oraz opracowywania jednolitej strategii IT.**




Cloudflare One umożliwia organizacjom każdej wielkości przejście na architekturę SASE: łączy dowolne źródła i miejsca docelowe ruchu z bezpieczną, szybką i niezawodną siecią globalną, w której egzekwowane są wszystkie funkcje bezpieczeństwa, a ruch jest optymalizowany po drodze do miejsca docelowego — zarówno w sieci prywatnej, jak i w publicznym Internecie.

Niezależnie od tego, czy Twoja organizacja przekierowuje ruch ze starszych wdrożeń MPLS lub SD-WAN, czy też po raz pierwszy podchodzi do modernizacji sieci, rozwiązanie Magic WAN może pomóc uprościć ten proces. Architektura Cloudflare One zapewnia zarówno bezpieczeństwo w modelu Zero Trust, jak i WAN jako usługę, co pozwala wdrożyć model SASE od jednego dostawcy, ale może również uzupełniać strategię bazującą na wielu dostawcach, wspierając Cię w drodze do modelu SASE.

## Przeanalizujmy łączność z siecią w przypadku Twojej organizacji

Umów się na warsztaty

CLOUDFLARE

Dowiedz się więcej na temat platformy SASE firmy Cloudflare.