

WAN como serviço

O Magic WAN simplifica o caminho para o SASE com conectividade any-to-any

Evolução das arquiteturas de rede

A internet como a nova rede corporativa

Com o trabalho híbrido como o novo normal e os aplicativos migrando para a nuvem, as equipes de TI estão tendo dificuldades com:

- **Complexidade da rede:** o provisionamento de MPLS e o ajuste de soluções pontuais levam muito tempo.
- **Lacunas de segurança:** usuários distribuídos e dispositivos pessoais aumentam o risco para os dados corporativos.
- **Altos custos:** links MPLS e soluções pontuais de segurança geram gastos desnecessários.
- **Experiência do usuário abaixo do ideal:** o backhauling do tráfego para reforçar a segurança introduz latência.

O Magic WAN simplifica a conectividade de rede de filiais, VPCs multinuvem ou de data centers para a plataforma [Cloudflare One](#) SASE, permitindo conectividade segura, de alto desempenho e econômica para resolver desafios de trabalho híbrido e multinuvem para equipes de TI.

Ao contrário das redes [MPLS](#) rígidas e caras ou das implantações [SD-WAN](#) inchadas construídas em firewalls locais, o Magic WAN adota uma abordagem de “light branch, heavy cloud” para aumentar ou eventualmente substituir sua arquitetura atual. É mais fácil implantar, gerenciar, consumir e escalar de acordo com as mudanças nos requisitos da empresa, com segurança integrada.



O Magic WAN conecta locais de rede físicos ou virtuais à plataforma SASE da Cloudflare. Exemplos de locais físicos incluem filiais, fábricas, lojas, sedes ou data centers. Exemplos de locais virtuais incluem serviços em nuvem pública como AWS, Azure, GCP e OCI.



Melhor agilidade operacional

Gerencie centralmente a segurança e a conectividade da rede a partir de uma interface. Tráfego nas vias de acesso em minutos com configuração sem toque.



Segurança integrada, não complementar

Obtenha proteção contra DDoS nativa de nuvem, firewall de rede, SSE e funcionalidade Zero Trust, tudo profundamente integrado e fornecido como serviço.



Custos de rede reduzidos

Minimize a pegada da sua filial e transfira as funções de rede para a nuvem para reduzir a dependência de implantações caras de MPLS ou SD-WAN.

Principais casos de uso do Magic WAN

Simplificar a conectividade de rede

- ★ **Simplificar a conectividade das filiais** — Substituir uma colcha de retalhos de circuitos proprietários e dispositivos de rede para rotear com segurança o tráfego entre filiais e data centers. Facilitar a conectividade site a site entre locais com Anycast IPSec.
- **Simplificar a conectividade híbrida e multinuvem** — As organizações têm aplicativos em instâncias de nuvem de diferentes provedores (por exemplo, AWS, GCP, Azure, Oracle, IBM) e data centers no local. Usar controles centralizados para rotear e proteger o tráfego nesses ambientes variados.

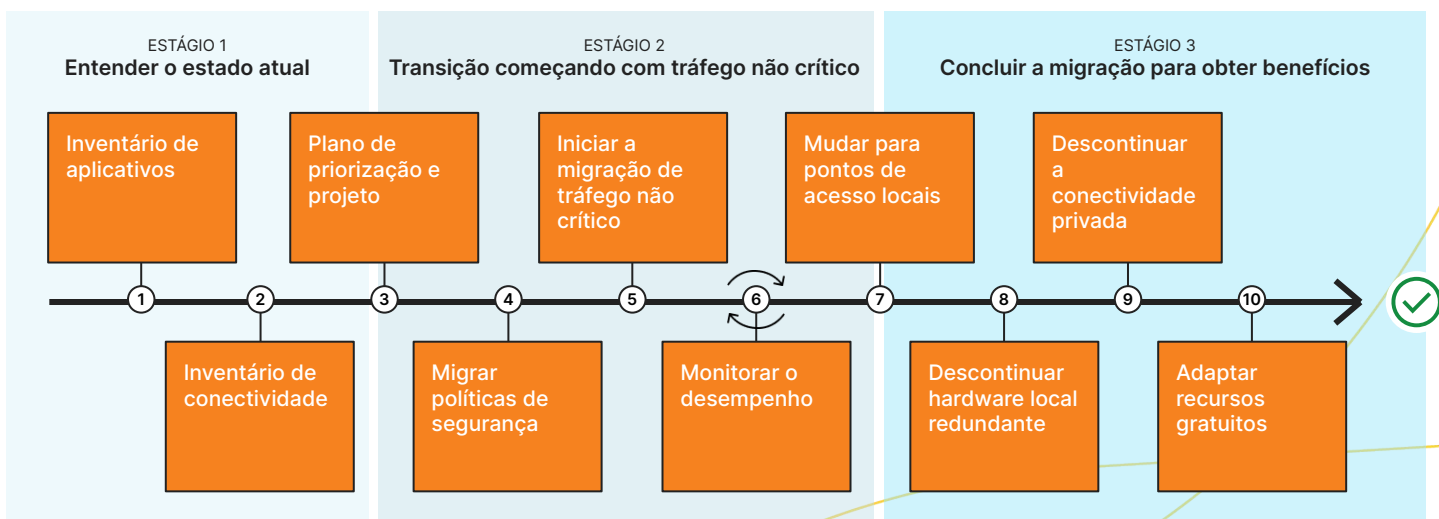
Aumentar a segurança sem abrir mão do desempenho

- **Conectividade WAN segura** — Proteger conexões aplicando filtros e inspeções de tráfego entre locais (filiais, data centers, etc.) e de/para esses locais dentro/fora da internet mais ampla, colocando firewalls e controles SWG na WAN.
- **Escalar o desempenho da WAN** — As implantações de MPLS são caras para construir e lentas para escalar. A remoção do MPLS e a mudança para WAN fornecida em nuvem oferece custo mais baixo, implantação mais ágil e segurança integrada.

Como abordar a implantação do Magic WAN

A transformação da rede é um processo de longo prazo, com muitas pequenas vitórias ao longo do caminho

O Magic WAN traz desempenho e confiabilidade semelhantes aos do MPLS para a internet pública para fornecer um caminho de migração de arquiteturas de rede legadas. Comece aos poucos com um piloto de migração de tráfego não crítico e descarregue gradualmente mais tráfego ao longo do tempo. A combinação de “light branch, heavy cloud” da Cloudflare de conectividade de última milha e desempenho, confiabilidade e segurança de meia milha, ajuda a conectar e proteger melhor o trabalho híbrido. Nossa arquitetura nativa da internet pode ser implantada junto com as implementações de SD-WAN existentes quando necessário ou substituir totalmente a necessidade de novas implementações de SD-WAN.



Comparação entre MPLS e SD-WAN

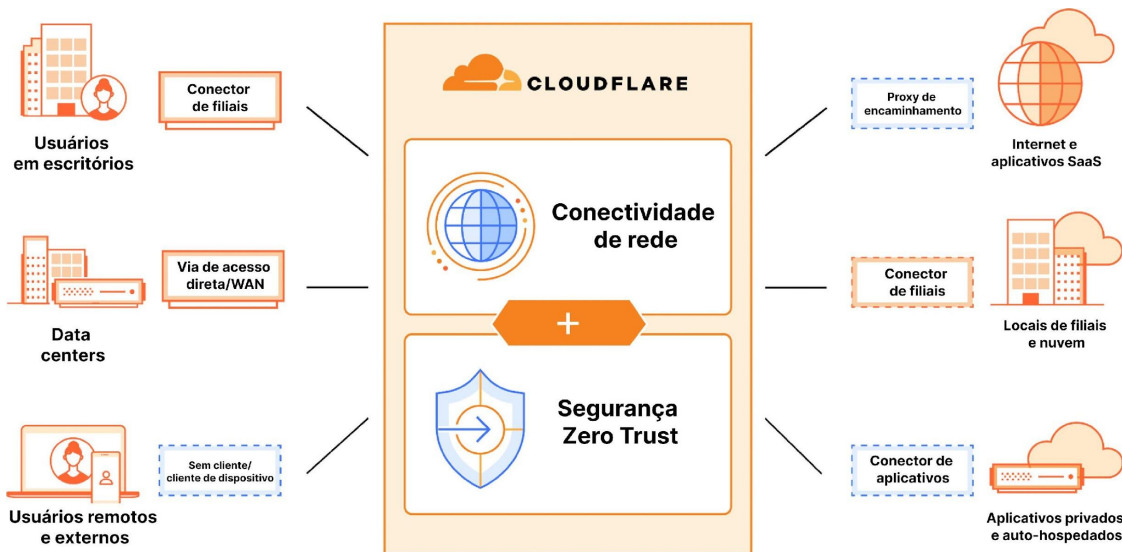
As organizações tradicionalmente dependiam de circuitos MPLS para conectividade WAN confiável e de alto desempenho. À medida que os aplicativos migraram para a nuvem e os usuários têm opções de trabalho mais flexíveis, esse modelo está se rompendo. Mesmo que o tráfego tenha se tornado mais distribuído, as equipes de segurança ainda impõem o controle com locais de “ponto de acesso” centralizados, fazendo backhauling de todo o tráfego por meio de uma colcha de retalhos de dispositivos de segurança. Especialmente porque seus custos aumentam para implantações maiores, o MPLS não consegue atender com eficiência às necessidades modernas de conectividade.

Mais recentemente, a SD-WAN ajudou a melhorar os problemas de orquestração com interfaces web intuitivas e centralizadas, e recursos de roteamento inteligente foram implementados localmente para tomar melhores decisões instantâneas para direcionar e moldar o tráfego na última milha. No entanto, os dispositivos SD-WAN geralmente ainda não possuem controles de segurança incorporados, deixando as equipes juntando uma colcha de retalhos de hardware, ferramentas virtualizadas e baseadas em nuvem para cobertura. Embora os custos devessem diminuir com a promessa de encerrar os contratos de MPLS, as organizações normalmente não conseguiram isso devido a novos custos de hardware, licença ou manutenção, ou por não serem capazes de substituir o MPLS devido às deficiências de segurança e confiabilidade da SD-WAN.

A plataforma SASE da Cloudflare reúne segurança e rede em nossa nuvem de conectividade para atender todo o tráfego por meio de uma abordagem de “light branch, heavy cloud”, permitindo que as organizações migrem dos circuitos privados legados e usem nossa rede como uma extensão própria. Gerenciamento simplificado, desempenho confiável, segurança Zero Trust moderna e custo total de propriedade reduzido só são possíveis simultaneamente com uma abordagem verdadeiramente reinventada, que a arquitetura de design SASE pretende ser para organizações em processo de modernização digital.

Aspecto	Exemplo	Serviço MPLS/VPN	SD-WAN	SASE com Cloudflare One
Configuração	Configuração, implantação e gerenciamento de novo site	Por MSP através de solicitação de serviço	Orquestração e gerenciamento simplificados por meio de controlador centralizado	Orquestração automatizada via portal SaaS; painel centralizado
Controle de tráfego na última milha	Balanceamento de tráfego, QoS e failover	Coberto por SLAs de MPLS	Melhor seleção de caminho disponível no dispositivo SD-WAN	Implantação mínima no local para controlar a tomada de decisões locais
Controle de tráfego de meia milha	Direção de tráfego em torno do congestionamento de meia milha	Coberto por SLAs de MPLS	Complexidade de túneis e ainda sem controle sobre a meia milha	Gerenciamento de tráfego integrado e controles de backbone privado na mesma interface
Integração de nuvens	Conectividade para migração para nuvem	Ponto de acesso centralizado	Ponto de acesso descentralizado	Conectividade nativa com Cloud Network Interconnect
Segurança	Filtrar o tráfego de entrada e saída da internet em busca de malware	Colcha de retalhos de controles de hardware	Colcha de retalhos de hardware e/ou controles de software	Integração nativa com ferramentas de segurança de usuários, dados, aplicativos e rede
Custo	Maximizar o ROI para investimentos em rede	Alto custo de hardware e conectividade	Custos de conectividade otimizados em detrimento do aumento dos custos de hardware e software	Custos reduzidos de hardware e conectividade para maximizar o ROI

Tráfego de vias de acesso para a plataforma SASE da Cloudflare



O Magic WAN Connector facilita a conexão de seus locais de rede à Cloudflare. Adquira o software do conector de filiais pré-instalado e configurado em um dispositivo de hardware certificado pela Cloudflare para uma implantação de menor atrito ou instale o software em dispositivos Linux físicos ou virtuais em seu ambiente.

Parte de uma família crescente de vias de acesso flexíveis

O primeiro passo para adotar o [SASE](#) é conectar-se, estabelecendo um caminho seguro da sua rede existente até o local mais próximo onde as políticas de segurança Zero Trust possam ser aplicadas. A Cloudflare oferece um amplo conjunto de “vias de acesso” para permitir essa conectividade, incluindo opções de acesso baseadas em cliente e sem cliente para usuários de trabalho híbrido, túneis na camada de aplicação estabelecidos através da implantação de um daemon de software leve, conectividade de camada de rede com GRE habilitado para Anycast ou túneis IPsec e interconexão física ou virtual para data centers privados e nuvens públicas.

Para tornar esse primeiro passo para o SASE ainda mais fácil, o Magic WAN Connector pode ser implantado em qualquer local de rede física ou em nuvem para fornecer conectividade automática ao local de rede da Cloudflare mais próximo, aproveitando sua conectividade de internet de última milha existente e eliminando a necessidade de as equipes de TI configurarem manualmente o equipamento de rede para se conectar.

Capacidades de software e especificações de hardware

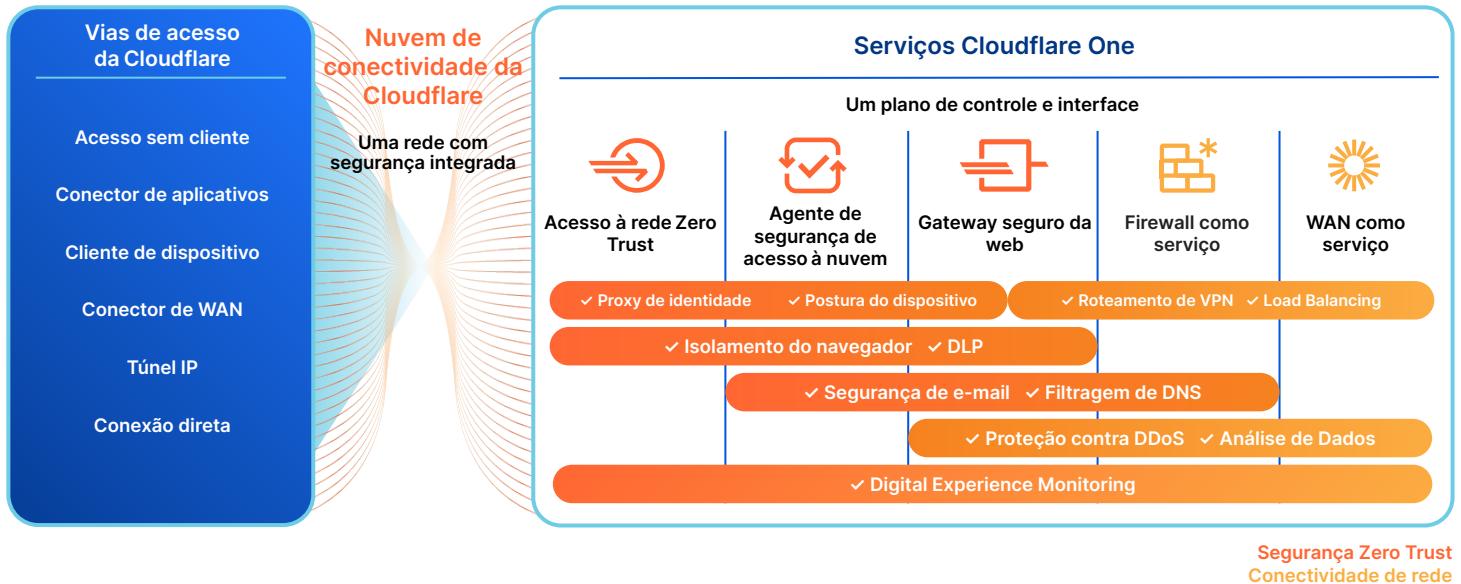
Recursos do software Magic WAN ¹	
Configuração do WAN Connector	Dispositivos CPE plug-and-play provisionados sem toque que são gerenciados centralmente por meio do painel/API da Cloudflare. Configure automaticamente túneis e rotas IPsec para direcionar o tráfego para a rede da Cloudflare para funções de conectividade e segurança. Atualizações automáticas de software ao longo do tempo (dentro da janela de serviço definida pelo cliente).
Configuração do site do WAN Connector	Suporte WAN/LAN para configurações de IP estático ou DHCP que existem em cada site. Suporte para VLANs e segmentação de rede local.
Abordagem "light branch, heavy cloud"	Balanceamento de carga e failover do WAN Connector no local em vários circuitos WAN com base em verificações de integridade. Recursos de firewall e SSE Zero Trust que consomem mais capacidades fornecidos pela nuvem de conectividade da Cloudflare na meia milha.
Integração de terceiros	Configure endpoints de túnel Anycast IPsec ou GRE com suas VPCs de nuvem existentes, como Amazon AWS Transit Gateway ou equipamentos nas instalações do cliente, como SD-WAN, firewall e dispositivos roteadores. Configure rotas estáticas com encaminhamento de pacotes ECMP para a rede da Cloudflare.
Segurança integrada	Firewall na camada 3 integrado e detecção de intrusão; integração perfeita com outros recursos de SSE/segurança e vias de acesso, como gateway seguro da web nas camadas 4 e 7, cliente de dispositivo, conector de aplicativos, etc.
Visibilidade e controle	Métricas de visibilidade/análise de dados de túnel, tráfego e dispositivo disponíveis através do painel, API, logs ou GraphQL. Controle através do painel ou da API da Cloudflare ou Terraform.
Especificações da opção de hardware do Magic WAN Connector ²	
Especificações do dispositivo	• Portas: (6× 1G Copper RJ45) + (2× 10G SFP+) + (2x USB 3.0 Tipo A) • Dimensões: 8,1×7,9×2,0 polegadas; 1.5RU; Peso: 2,87 lbs • Opções de montagem: desktop, montagem em parede ou montagem em rack (com bandeja) • TPM: 2.0, em todo o mundo, exceto na China • CPU: Denverton 4 Core C3558 • Drive: M.2 120 SSD com 16G eMMC Flash • RAM: 8 GB DDR4 • WiFi e Bluetooth: 802.11ac, 2×2 MIMO, max. phy rate: 866.7 Mbps • Ventilador: um

¹ Toda a documentação de nível de recurso do Magic WAN pode ser encontrada no [Cloudflare Docs](#)

² Hardware certificado pela Cloudflare com software Magic WAN pré-instalado: [Dell VEP 1425](#) vendido por parceiro (vem com montagem em rack)

Conectividade de rede e o caminho para o SASE

A nuvem de conectividade da Cloudflare oferece a simplicidade de implantação, a resiliência de rede e a velocidade de inovação necessárias para permanecer à frente conforme você consolida produtos pontuais e converge para uma estratégia de TI unificada.



O Cloudflare One permite que organizações de todos os tamanhos façam a [transição para o SASE](#): conectando qualquer origem e destino de tráfego a uma rede global segura, rápida e confiável, onde todas as funções de segurança são aplicadas e o tráfego é otimizado no caminho até seu destino, tanto dentro de uma rede privada ou na internet pública.

Esteja sua organização descarregando o tráfego de implantações maduras de MPLS ou SD-WAN ou abordando a transformação da rede pela primeira vez, o Magic WAN pode ajudar na modernização. O Cloudflare One oferece segurança Zero Trust e WAN como serviço para alcançar o SASE de fornecedor único, mas também pode complementar uma estratégia de vários fornecedores por meio de seus componentes para atender sua empresa onde quer que esteja em sua jornada SASE.

Vamos conversar sobre conectividade de rede para sua organização

Solicite um workshop



Ainda não está pronto para uma conversa ao vivo?

Continue aprendendo mais sobre [a plataforma SSE e SASE da Cloudflare](#)