Acesso à Rede Zero Trust com roteamento privado

Evite o movimento lateral e reduza a dependência da VPN

A confiança em controles baseados em rede (como VPNs e restrição de localização de IP) para o acesso a aplicativos pode aumentar sua superfície de ataque, limitar a visibilidade e frustrar os usuários finais. O Acesso à Rede Zero Trust da Cloudflare trabalha com seus provedores de identidade e plataformas de proteção de endpoints para aplicar regras de negação padrão e Zero Trust que limitam o acesso a aplicativos corporativos, espaços de IP privados e nomes de host. Com a tecnologia da Rede Anycast da Cloudflare, que é ampla e de excelente performance, ele torna as conexões dos usuários mais rápidas que em uma VPN.

Desde que implantou o Acesso à Rede Zero Trust internamente, a Cloudflare viu os seguintes benefícios:

- 91% de redução na superfície de ataque[1]
- Economia de custos duplicada e esforços de TI reduzidos
- 80% de redução do tempo gasto atendendo a chamados relacionados à VPN
- 70% de redução no volume de tickets
- +300 horas anuais de produtividade desbloqueadas durante a integração de novos funcionários

O que você pode fazer com o Access

Proteger qualquer aplicativo

A Cloudflare é independente de identidade e de aplicativos, permitindo que você proteja qualquer aplicativo, SaaS, na nuvem ou no local, com seu provedor de identidade preferido.

Conectar os usuários de maneira flexível, com ou sem um cliente

Facilite as conexões de aplicativos web e SSH sem necessidade de um software cliente ou configuração do usuário final. Para aplicativos não web, conexões RDP e roteamento privado, utilize um cliente abrangente na internet e casos de uso de acesso a aplicativos.

Habilitar a federação de identidade em diversos provedores de identidade

Integre todos os seus provedores de identidade corporativa (Okta, Azure AD e outros) para migrações, aquisições e acesso de usuários de terceiros mais seguros. Habilite pins de uso único para acesso temporário ou incorpore fontes de identidade social, como LinkedIn e GitHub.

Restringir o movimento lateral entre recursos corporativos

Aplique métodos de autenticação fortes e consistentes até mesmo para aplicativos obsoletos com o firewall de IP e regras de Zero Trust.

Implementar acesso com reconhecimento de dispositivo

Antes de conceder acesso a um recurso, avalie a postura do dispositivo, incluindo a presença do cliente de Gateway, número de série e certificado mTLS, garantindo que apenas dispositivos conhecidos e seguros possam se conectar aos seus recursos. Integre a postura do dispositivo de provedores de Plataforma de Proteção de Endpoints (EPP), incluindo Crowdstrike, Carbon Black, Sentinel One e Tanium.

Registrar a atividade do usuário em qualquer aplicativo

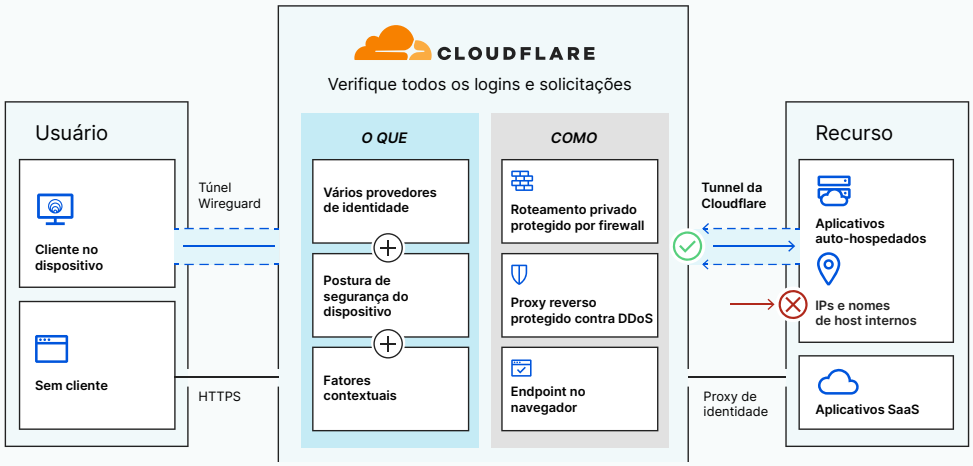
Registre todas as solicitações feita em seus aplicativos protegidos — não apenas login e logout. Agregue os registros de atividades na Cloudflare ou os exporte para seu provedor de SIEM.

[1]Quando o Acesso à Rede Zero Trust é combinado com navegação na internet

O diferencial da Cloudflare

- A **performance incomparável** roteia solicitações mais rapidamente com roteamento otimizado e baseado em inteligência na Rede Anycast da Cloudflare. Em média, os aplicativos web são acessados de forma 30% mais rápida e as conexões TCP veem uma diminuição de 17% no tempo de ida e volta. Nossa inteligência se baseia em analisar dados da rede de 25 milhões de solicitações HTTP/segundo e 39 mil novas conexões TCP/segundo.
- O **gerenciamento mais simples** combina Acesso à Rede Zero Trust, Gateway Seguro da Web, Isolamento do Navegador Remoto e muito mais em um plano de controle com experiência de administração construída desde o início, não adquirida e modificada a partir de vários fornecedores.
- A **Inspeção de Passagem Única** verifica, filtra, isola e inspeciona o tráfego de forma rápida e consistente em todo o mundo, porque todos os serviços da Cloudflare são implantados em todos os data centers em nossos mais de 250 locais no mundo todo.

Como funciona



Em vez de uma VPN, os usuários se conectam aos recursos corporativos por meio de um cliente ou navegador web. À medida que são roteadas e aceleradas por meio da borda da Cloudflare, as solicitações são avaliadas frente às regras Zero Trust que incorporam sinais de seus provedores de identidade, dispositivos e outros contextos. Nos casos em que o software de RDP, visualizadores de arquivos SMB e outros programas clientes densos costumavam exigir uma VPN para conectividade de rede privada, as equipes agora podem rotear qualquer tráfego TCP ou UDP de forma privada pela Rede da Cloudflare, onde ele é acelerado, verificado e filtrado em uma passagem única, favorecendo a segurança e uma performance aprimoradas.

"Graças ao Cloudflare Access, não precisamos desenvolver nosso próprio sistema de Gerenciamento de Identidade e Acesso (IAM). Não precisamos integrar funções de permissão de usuário nos aplicativos que o Access protege. Entramos com tudo. Todos na empresa têm um lugar".

Jim Tyrell
Diretor de Infraestrutura, Canva

"Na Delivery Hero, sempre nos esforçamos para proporcionar uma experiência incrível aos nossos clientes. O Cloudflare Access nos ajuda a fazer o mesmo para nossas equipes internas: oferecer-lhes um ambiente de trabalho seguro e eliminar a necessidade de uma VPN para acessar todos os nossos aplicativos em todo o mundo".

William Carminato
Diretor Sênior de Engenharia, Delivery Hero

Integrações de gerenciamento de identidade e acesso (IAM)

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

Integrações da plataforma de proteção de endpoints (EPP)

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

Principais recursos

Política consistente	
Aplicativo personalizado, rede privada e políticas de acesso à internet	**Ilimitado**
Autenticação via IdPs corporativos e sociais	✔
Postura do dispositivo usando integrações de terceiros e a Cloudflare	✔
Importação em massa baseada em CSV para listas de números de série de dispositivos corporativos	✔

Aumento da visibilidade	
Retenção do registro de atividades	**6 meses**
Visualizações de país, estado e detalhes do dispositivo com base na identidade	✔
Envio de registros para armazenamento em nuvem ou SIEMs	✔

Conectividade segura	
Conexões criptografadas com a internet baseadas no cliente (cliente WARP)	**Win, Mac, iOS, Android**
Acesso seguro sem cliente a aplicativos auto-hospedados e SaaS	✔
Conexões privadas para aplicativos auto-hospedados, IPs e nomes de host internos (Tunnel da Cloudflare)	✔

Interoperabilidade simples	
Integrações de endpoints e gerenciamento de mobilidade	✔
Tunelamento dividido para conectividade local ou de VPN	✔
Autocadastramento do cliente para dispositivos não gerenciados	✔
Inicializador de aplicativos personalizável	✔
Autenticação compatível com vários provedores de identidade simultaneamente	✔
Conectores genéricos e personalizados para compatibilidade com SAML e OIDC	✔
Autenticação com token para serviços automatizados	✔
Autenticação baseada em certificado para IoT e outros casos de uso de mTLS	✔

Sem abrir mão da performance	
SLA de tempo de atividade	**100%**
Uma das redes mais rápidas (<50ms de distância de mais de 250 PoPs)	✔
Resolvedor de DNS mais rápido, privacidade em primeiro lugar (7-31ms via mais de 250 PoPs)	✔
Atualizações de política extremamente rápidas (<500ms em mais de 250 PoPs)	✔
Navegador remoto extremamente rápido (sem pixel pushing — executado em nossa Rede; sem nuvem de terceiros)	**Add on**

Interessado em saber mais?

Visite www.cloudflare.com/pt-br/products/zero-trust/access/ para iniciar uma conta. Grátis para até 50 usuários.