CLOUDFLARE

RESUMO DA SOLUÇÃO

Proteger locais de trabalho distribuídos

Proteção consistente em um plano de controle unificado para todas as solicitações, de qualquer escritório

Migre a segurança para a nuvem

Reduza a complexidade e o risco para escritórios com a Cloudflare

Com funcionários trabalhando em escritórios e remotamente, muitas organizações estão reavaliando como protegem os escritórios hoje, quer dependam de dispositivos em data centers ou permitam acesso direto e não seguro à internet.

Seu novo foco é fornecer proteção e experiências consistentes para os usuários dentro e fora da rede. Na maioria das vezes, isso significa mudar os controles de ferramentas diferentes, como VPNs, proxies e firewalls da web, para uma única plataforma de segurança fornecida em nuvem.

A Cloudflare observa organizações que modernizam a segurança do escritório com dois casos de uso comuns.

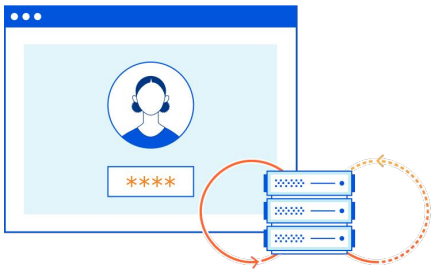
> "Combinar filiais e acesso remoto em uma única implementação para garantir políticas consistentes e minimizar o número de fornecedores necessários. Implantar o ZTNA para aumentar ou substituir a VPN legada para limitar o investimento em tecnologia ultrapassada."[1]
>
> Gartner

Caso de uso recomendado:

acesso seguro a aplicativos com Zero Trust para substituir VPNs

Aplique políticas granulares com reconhecimento de identidade por aplicativo, em vez de permitir movimentação lateral pela rede corporativa.

- **Etapa 1:** integração com seus provedores de identidade.
- **Etapa 2**: proteger qualquer aplicativo web por meio de um navegador
- **Etapa 3**: proteger ambientes SSH, VNC e RDP por meio de um navegador

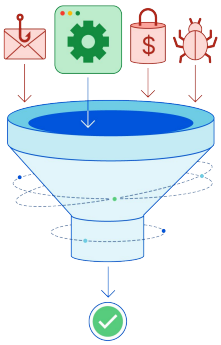


Caso de uso recomendado:

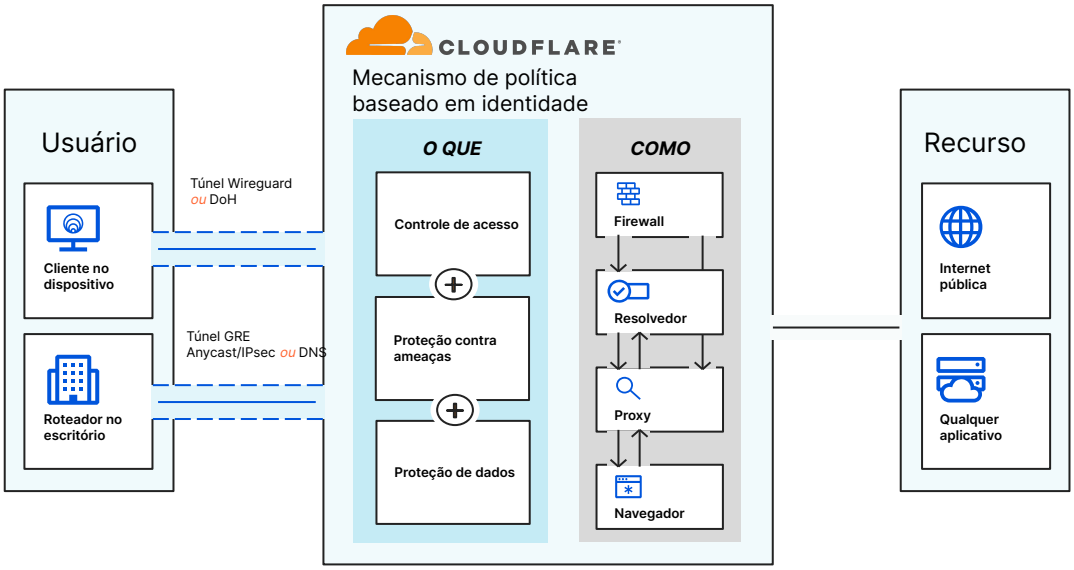
filtrar o acesso à internet para obter segurança consistente com tempo de valorização rápido

Proteja os usuários do escritório primeiro com filtragem de DNS e, posteriormente, com inspeções mais abrangentes em todos os locais. Sem tráfego de backhaul por meio de dispositivos de segurança locais em data centers.

- **Etapa 1:** apontar o tráfego de DNS para a rede global da Cloudflare.
- **Etapa 2**: configurar a filtragem de DNS baseada em localização para proteger contra ransomware, phishing e outras ameaças da internet.
- **Etapa 3**: controlar os fluxos de dados aplicando regras de isolamento de HTTP, rede e navegador com inspeção TLS 1.3 ilimitada.



Como funciona



Implantação sem cliente
para verificar o acesso e filtrar consultas de DNS de escritórios.

Implantação com o cliente de dispositivo da Cloudflare
para desbloquear visibilidade e controles aprimorados por usuário e dispositivo.

Figura: Verificar, filtrar, isolar e inspecionar o tráfego do escritório em uma única passagem com Zero Trust da Cloudflare

Acessos flexíveis a partir de qualquer origem

Comece usando a Cloudflare para resolução de DNS por meio de roteadores de rede. Com o tempo, envie o tráfego da camada 3 para nossa rede global por meio de seus túneis GRE ou IPsec, ou use seu método de roteamento SD-WAN existente.

Como alternativa, implante o cliente Cloudflare para filtragem e inspeção de DNS e HTTP em dispositivos gerenciados.

Aplicação de políticas rápida, desenvolvida para escalar globalmente

Todas as funções de segurança, desempenho e confiabilidade são criadas para que sejam executadas em todos os servidores e em todos os data centers em mais de 275 locais e mais de 100 países.

Nossa escala de rede significa que as proteções são sempre aplicadas perto de escritórios e usuários finais, onde quer que estejam, em alta velocidade com inspeção de passagem única.

Outros casos de uso que vão ser explorados nos próximos seis a doze meses

Recuperar o controle sobre aplicativos SaaS

Descubra e reduza os riscos da TI invisível que os funcionários usam nos escritórios e em casa.

Evite vazamentos de dados e violações de conformidade com políticas CASB habilitadas no mesmo e único painel de controle da Cloudflare. Saiba como.

Descarregar o tráfego MPLS

Substitua conexões MPLS privadas caras, antigas e lentas.

Simplifique a arquitetura WAN legada usando a rede global da Cloudflare para gerenciar o tráfego entre filiais, data centers e serviços em nuvem pública. Saiba como.

[1] *Gartner Hype Cycle for Network Security, 2021* | GARTNER e HYPE CYCLE são marcas registradas e marcas de serviços da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, sendo usadas no presente documento mediante permissão. Todos os direitos reservados.