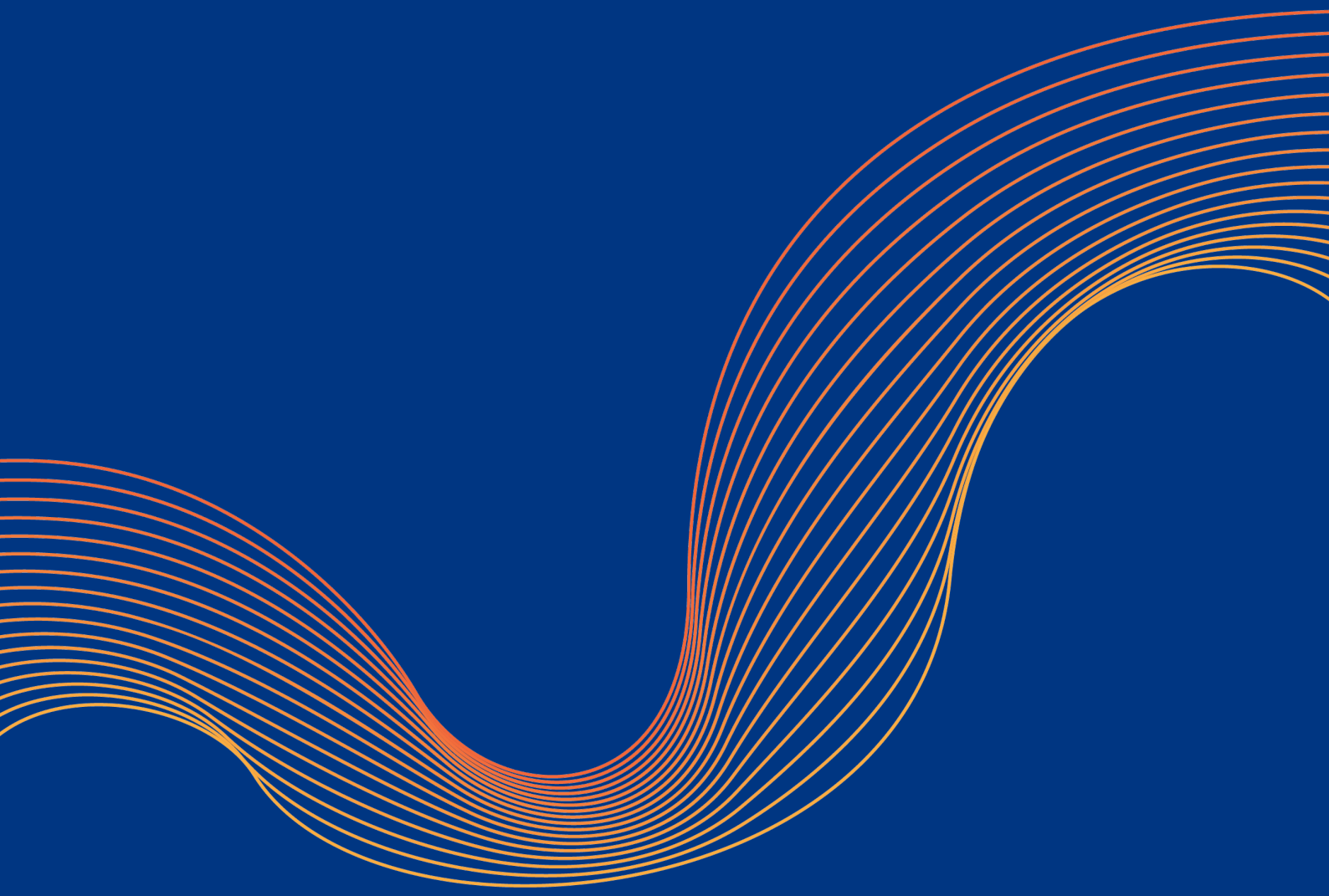
ARTIGO TÉCNICO

CLOUDFLARE

O ZTNA pode substituir sua VPN? Compare 3 abordagens de acesso remoto



+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

ÍNDICE

INTRODUÇÃO

O acesso remoto seguro e contínuo é um facilitador de negócios — aumentando a produtividade do usuário remoto e reduzindo o tempo gasto pelas equipes de TI para integrar e manter a conectividade do usuário para o aplicativo com agilidade e resiliência. E, no entanto, o acesso remoto continua sendo um desafio para muitas organizações.

Antigamente, as VPNs ofereciam uma maneira simples de conectar alguns usuários remotos a redes corporativas por breves períodos de tempo. No entanto, à medida que as forças de trabalho se tornaram mais distribuídas — e as organizações precisavam manter os usuários remotos conectados com segurança por mais tempo — as falhas nessa abordagem se tornaram evidentes, desde performance lenta e aumento dos riscos de segurança até preocupações de escalabilidade.

À medida que as necessidades de acesso remoto crescem, as organizações estão se afastando cada vez mais das implementações de VPNs tradicionais e indo em direção a soluções de acesso remoto mais seguras e de alta performance. O acesso à rede Zero Trust, ou ZTNA, cria limites seguros em torno de aplicativos específicos, IPs privados e nomes de host, substituindo conexões VPN de permissão padrão por políticas de negação padrão que concedem acesso com base em identidade e contexto.

Em 2020, aproximadamente 5% de todo o uso de acesso remoto foi predominantemente fornecido pelo ZTNA. Devido às limitações do acesso da VPN tradicional e à necessidade de fornecer acesso e controle de sessão mais precisos, espera-se que esse número salte para 40% até 2024.[1]

Embora o ZTNA ofereça às empresas várias vantagens claras — e funcionalidades expandidas — sobre as VPNs, muitas organizações o consideraram um substituto incompleto para a infraestrutura de VPN. Mas à medida que os ZTNAs se tornam mais robustos e as VPNs se tornam mais problemáticas, isso está mudando rapidamente. Este artigo contrasta as soluções de acesso remoto de VPNs e ZTNA para esclarecer seus benefícios e limitações, ao mesmo tempo em que esclarece as considerações mais importantes para projetos de migração. Ele explica como a Cloudflare oferece o ZTNA e recomenda um conjunto de etapas de ação para fazer a transição da infraestrutura de VPN ultrapassada para uma conectividade Zero Trust mais rápida e segura para usuários remotos.

[1] *Riley, Steve, MacDonald, Neil, and Orans, Lawrence. "Market Guide for Zero Trust Network Access." Pesquisa da Gartner, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. Acessado em 21 de junho de 2021. Consulte a tabela 1 para mais detalhes.*

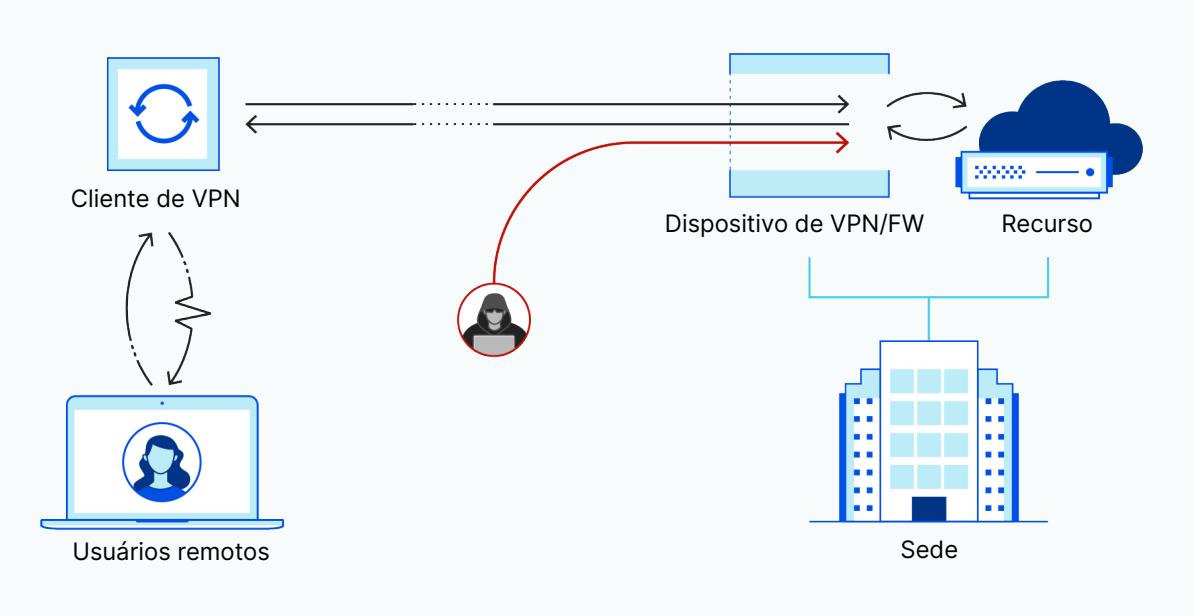
ABORDAGEM Nº 1: VPN ULTRAPASSADA

Durante décadas, as VPNs permitiram que as organizações conectassem seus usuários remotos a redes corporativas com alguma privacidade e segurança. Em vez de acessar informações sensíveis pela internet pública, onde qualquer invasor pode espionar ou roubar dados, as VPNs permitem que os usuários acessem recursos internos com segurança por meio de uma conexão criptografada.

Os dois modos mais comuns de implementação de VPN são VPNs baseadas em cliente e VPNs sem cliente VPN-SSL. Cada um vem com seus próprios benefícios e desafios:

VPNs baseadas em cliente conectam usuários remotos a um rede privada através de um túnel criptografado. Essa conexão é estabelecida por meio de um aplicativo de software, ou cliente, que exige que os usuários se autentiquem uma vez com um nome de usuário e senha para obter acesso contínuo a qualquer recurso dentro dessa rede.	**Benefício:** uma vez conectado, o movimento lateral livre facilita o acesso rápido dos usuários a vários recursos, acessando aplicativos e conectando-se a hosts internos. **Desafios:** • **Não projetado para usuários de roaming e dispositivos móveis**. À medida que os usuários circulam, seus laptops e dispositivos móveis se reconectam perfeitamente à medida que as redes sem fio mudam de local para local. No entanto, os clientes VPN não são adeptos de lidar com fluidez com essas reconexões, exigindo que os usuários forcem repetidamente o cliente VPN a reiniciar e reautenticar — causando perda de produtividade e criando tíquetes de TI. • **Visibilidade ruim.** Com esse método, a infraestrutura da VPN encerra o túnel criptografado do cliente VPN atrás do firewall interno do data center. Embora essas conexões sejam registradas, não há registros centralizados específicos do aplicativo que revelem quais aplicativos os usuários acessaram ou as ações que realizaram no aplicativo.

Portais VPN-SSL sem cliente permitem que alguns usuários remotos se conectem a alguns aplicativos baseados em navegador dentro de uma rede privada. Essa conexão é possível usando um servidor web integrado ao dispositivo de rede que executa o serviço de VPN.	**Benefício:** Em vez de usar um cliente em um dispositivo, qualquer navegador web pode usar o certificado SSL do portal para estabelecer uma conexão HTTPS criptografada para oferecer suporte a contratados em dispositivos não gerenciados. **Desafios:** • **Preocupações com a segurança.** A maioria das configurações de VPN dentro do data center concede acesso total aos usuários, o que representa um problema para as organizações que não querem que não funcionários, como contratados, obtenham acesso irrestrito a recursos e aplicativos sensíveis. • **Não construída para oferecer suporte a um grande número de usuários simultâneos.** Ao contrário dos serviços de nuvem modernos, o servidor web do portal não pode ser dimensionado de forma elástica para atender a uma demanda maior. Em vez disso, mais dispositivos de rede devem ser instalados e ter balanceamento de carga para escalar o portal, o que geralmente é caro, complexo e ineficaz, pois o restante da funcionalidade do dispositivo pode ser subutilizado. • **Os portais VPN-SSL sem cliente expõem portas de firewall e servidores web a ataques.** Para permitir que o servidor web que hospeda o portal alcance aplicativos internos, os administradores devem abrir portas de firewall de entrada, expondo-as a ataques externos. Tanto as portas abertas quanto o próprio servidor web devem ser protegidos contra ataques DDoS e de aplicativos da web, o que requer configuração mais complexa e custos mais altos para proteger esse método de conectividade.



Embora as VPNs forneçam um nível básico de privacidade para usuários remotos, elas não foram projetadas com segurança ou escalabilidade em mente. Tradicionalmente, as organizações usam as VPNs para conectar alguns usuários remotos à rede corporativa por curtos períodos de tempo. À medida que o trabalho remoto se torna mais prevalente, no entanto, os problemas de VPN começam a se multiplicar:

- **Os usuários experimentam uma performance lenta.** Se a infraestrutura da VPN não tiver capacidade para lidar com a taxa de transferência de tráfego e conexões simultâneas criadas por sua força de trabalho, os usuários experimentarão uma lentidão em sua conexão com a internet. Além disso, quando as VPNs estão localizadas a uma grande distância do usuário e do servidor dos aplicativos que estão tentando acessar, o tempo de viagem resultante cria latência.
- **Redes corporativas ficam vulneráveis a ataques.** As VPNs normalmente usam um modelo de castelo e fosso, no qual um usuário recebe acesso irrestrito a todos os recursos corporativos assim que se conecta a uma rede. Sem nenhum método integrado para restringir o acesso à infraestrutura e aos dados críticos, as organizações são forçadas a configurar serviços de segurança caros e complexos, como firewalls de próxima geração e controle de acesso à rede — ou ficam vulneráveis a movimentos laterais maliciosos, resultando em violações de dados maiores.

O desafio dos serviços de VPN hospedados

Alguns fornecedores mudaram o dispositivo de rede que executa o serviço de VPN para a nuvem pública, onde ele é executado como uma máquina virtual em um ou mais data centers. A VPN pode ou não ser agrupada (ou encadeada) a serviços de segurança adicionais.

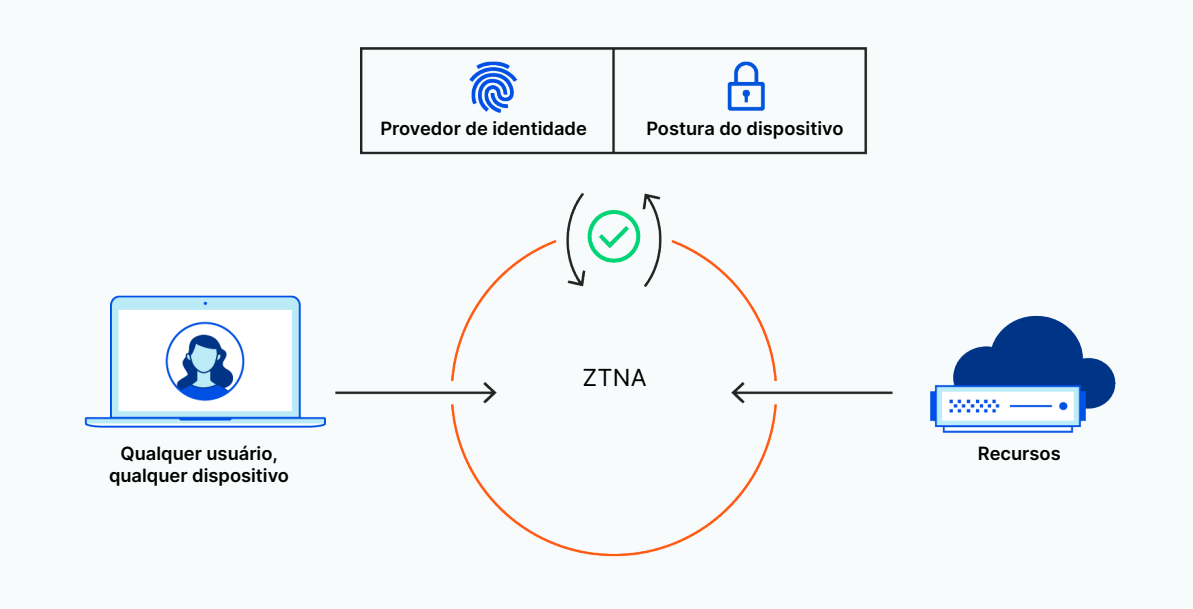
Colocar uma VPN na nuvem pode parecer resolver alguns dos problemas de escalabilidade inerentes aos dispositivos de VPN de hardware. No entanto, isso também apresenta alguns desafios significativos de segurança e escalabilidade.

Por exemplo, considere uma organização que hospeda um NGFW (firewall de próxima geração)completo, que combina a VPN com um firewall e funcionalidades de segurança adicionais. Como o NGFW é oferecido como um serviço agrupado, é impossível dimensionar independentemente qualquer funcionalidade específica sob demanda. A ampliação de uma função requer a ampliação de todo o serviço; para fazer isso, mais VMs devem ser ativadas para fazer o balanceamento de carga de uma pequena quantidade de computação que está sendo executada em cada VM. Essa não é apenas uma solução impraticável e difícil de manejar, mas provavelmente incorrerá em altos custos à medida que as necessidades de acesso remoto da organização continuam a se expandir.

ABORDAGEM Nº 2: ACESSO À REDE ZERO TRUST

A segurança Zero Trust contorna muitos dos desafios inerentes às VPNs. Baseia-se no princípio de que nenhum usuário ou dispositivo dentro ou fora de uma rede pode ser confiável por padrão. Para reduzir o risco e o impacto de violações de dados, ataques internos e outras ameaças, uma abordagem Zero Trust...

- autentica e registra cada login e solicitação,
- requer verificação rigorosa de todos os usuários e dispositivos,
- limita as informações que cada usuário e dispositivo pode acessar com base na identidade e no contexto
- e adiciona criptografia de ponta a ponta para isolar aplicativos e dados dentro da rede.



Assim como nas VPNs, há várias maneiras de configurar o ZTNA:

1. **O ZTNA Sem cliente (ou iniciado por serviço)** usa o navegador existente, em vez de um cliente , para criar uma conexão segura e autenticar os dispositivos do usuário. Tradicionalmente, o ZTNA sem cliente era limitado a aplicativos com protocolos HTTP/HTTPS, mas a compatibilidade está evoluindo rapidamente.[2]
   - **Benefício:** O ZTNA sem cliente usa uma conexão de proxy reverso para evitar o acesso direto a aplicativos, bloqueando os usuários de acessar aplicativos e dados que eles podem não ter permissão para visualizar e permitindo aos administradores maior controle e flexibilidade na gestão.
2. **O ZTNA baseado em cliente (ou iniciado por endpoint)** instala o software em um dispositivo de usuário antes que uma conexão criptografada possa ser estabelecida entre o agente de controle e os aplicativos autorizados.
   - **Benefício:** O ZTNA baseado em cliente permite que os administradores tenham mais informações sobre a postura do dispositivo, localização e contexto de risco dos usuários que acessam aplicativos, para que políticas mais granulares possam ser criadas e aplicadas. E, como esse método não é restrito a HTTP/HTTPS, ele pode ser usado para acessar uma variedade maior de aplicativos não HTTP — como aqueles que dependem de SSH, RDP, VNC, SMB e outras conexões TCP.

[2] A partir de junho de 2021, a solução ZTNA da Cloudflare oferece suporte ao acesso sem cliente a aplicativos SSH e VNC, com suporte para RDP planejado no futuro.

Desafios da implementação do ZTNA

Embora o ZTNA ofereça vantagens claras sobre as VPNs tradicionais, não é uma abordagem perfeita para proteger o acesso à rede para usuários remotos. À medida que as empresas avaliam os prós e os contras da adoção do Zero Trust, elas podem se deparar com um ou mais dos seguintes desafios:

As soluções não são realmente nativas em nuvem.

Se um fornecedor não oferece ZTNA baseado em nuvem — o que significa que seus clientes precisam implantar o software em seus próprios data centers —, os usuários perdem os principais benefícios, como escalabilidade instantânea e taxa de transferência ilimitada.

Os fornecedores podem não oferecer opções de ZTNA com e sem cliente.

Isso limita o valor para organizações que precisam conectar usuários a aplicativos não HTTP, como áreas de trabalho remotas, aplicativos SSH ou compartilhamentos de arquivos.

A configuração pode ser complexa e demorada.

Os fornecedores que não oferecem suporte para orquestração e automação de políticas (por meio de ferramentas como o Terraform) podem introduzir mais trabalho manual para os administradores — além da configuração que já ocorre em um provedor de identidade.

ABORDAGEM DA CLOUDFLARE PARA O ACESSO REMOTO

Proteger e escalar o acesso remoto deve ser um processo contínuo, que não utilize camadas de soluções de segurança desajeitadas, crie compensações de performance ou incorra em custos desnecessários. A Cloudflare capacita as equipes a lidar com todos os casos de uso de acesso remoto, com os seguintes benefícios:

- **Integração fácil e sem riscos para usuários e administradores.** A Cloudflare integra-se facilmente a provedores de identidade e plataformas de proteção de endpoints existentes para aplicar políticas Zero Trust que limitam o acesso a aplicativos e recursos corporativos.
- **Flexibilidade para implantações ZTNA baseadas em cliente e sem cliente**. A Cloudflare oferece suporte sem cliente para conexões com aplicativos web, SSH, VNC (e em breve, RDP) e suporte baseado em cliente para aplicativos não HTTP e roteamento privado para IPs internos.

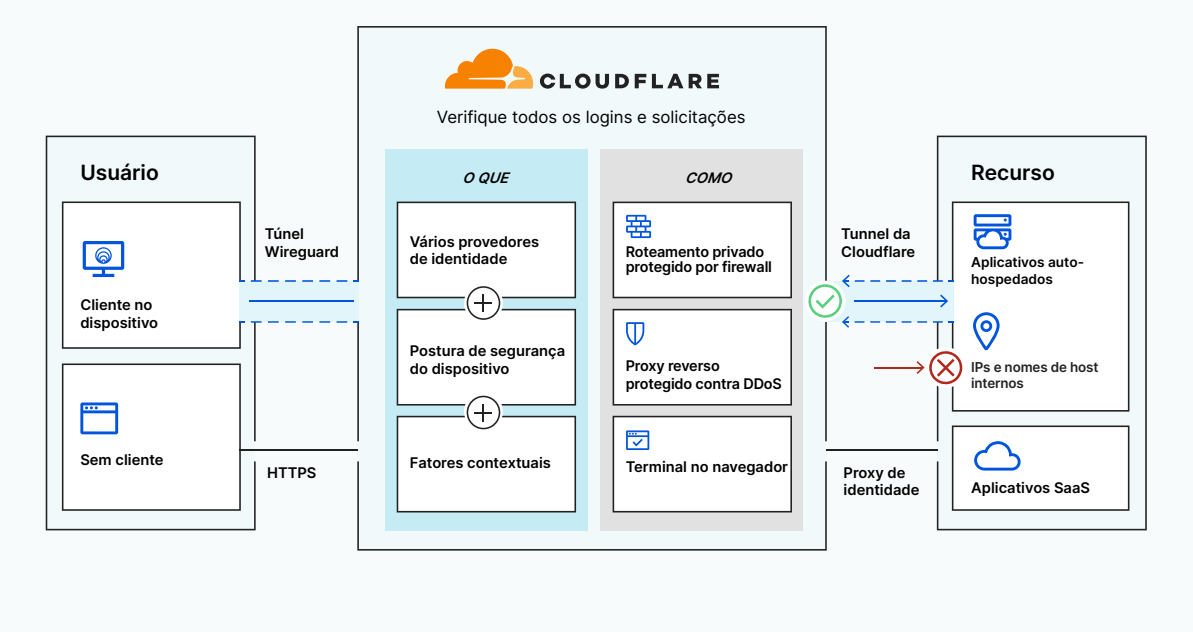


Tabela 1: Como a Cloudflare aborda os desafios do acesso remoto

⚠ Problema	✓ Solução	⚙ Implementação da Cloudflare
Difícil de escalar	Rede de borda global	Problemas de escalabilidade afetam VPNs e serviços de ZTNA que não são nativos em nuvem, dificultando o acesso de usuários remotos a aplicativos e dados. A Rede Anycast global da Cloudflare não apenas torna as conexões dos usuários mais rápidas do que uma VPN, mas também garante que as forças de trabalho remotas de qualquer tamanho possam se conectar com segurança e rapidez aos recursos corporativos conforme necessário — sem exigir configuração adicional demorada por parte dos administradores.
Pouca compatibilidade com dispositivos móveis	Cliente leve	As soluções de VPNs e ZTNA que utilizam protocolos IPSec e SSL geralmente apresentam baixa performance em dispositivos móveis e em roaming. O cliente WARP da Cloudflare utiliza o protocolo Wireguard mais moderno, que é executado no espaço do usuário para oferecer suporte a um conjunto mais amplo de opções de SO com experiência do usuário mais rápida do que as opções tradicionais. O cliente WARP da Cloudflare pode ser configurado em dispositivos Windows, MacOS, iOS, Android e, em breve, Linux.
Proteção contra DDoS não integrada ou fraca	Proteção contra DDoS líder do setor integrada	Sem a proteção contra DDoS integrada, as organizações geralmente são forçadas a encadear serviços de segurança adicionais que podem criar problemas de configuração, problemas de escalabilidade e desafios de segurança. A rede de mais de 67 Tbps da Cloudflare oferece proteção contra DDoS integrada para qualquer modo ZTNA, defendendo as redes contra os maiores ataques volumétricos.
Limitações de protocolo	Compatibilidade com aplicativos não web	✓ Compatibilidade de modo: ZTNA sem cliente para aplicações SSH/VNC; ZTNA baseado em cliente para todos os outros aplicativos não web.
Sem firewall de rede integrado	Firewall de rede incorporado	À medida que as redes corporativas crescem, o mesmo acontece com a pilha de hardware de segurança que as organizações precisam equilibrar — causando compensações em custo, performance e segurança. A Cloudflare permite que os administradores apliquem políticas de firewall de rede na borda, dando a eles um controle refinado sobre quais dados podem entrar e sair de sua rede e melhorando a visibilidade de como o tráfego flui por ela. ✓ Compatibilidade de modo: ZTNA baseado em cliente
Falta de controle refinado	Gateway seguro da web (SWG) integrado	O uso não autorizado de aplicativos pode causar problemas de segurança significativos para as organizações; sem políticas rigorosas em vigor, os usuários podem acessar e adulterar dados sensíveis e outros recursos corporativos. Combinando o ZTNA com o SWG, a Cloudflare permite que os administradores exerçam um controle mais refinado sobre os direitos de acesso de usuários e dispositivos dentro dos aplicativos, para que usuários e grupos baseados em funções tenham acesso apenas aos recursos de que precisam. ✓ Compatibilidade de modo: ZTNA baseado em cliente

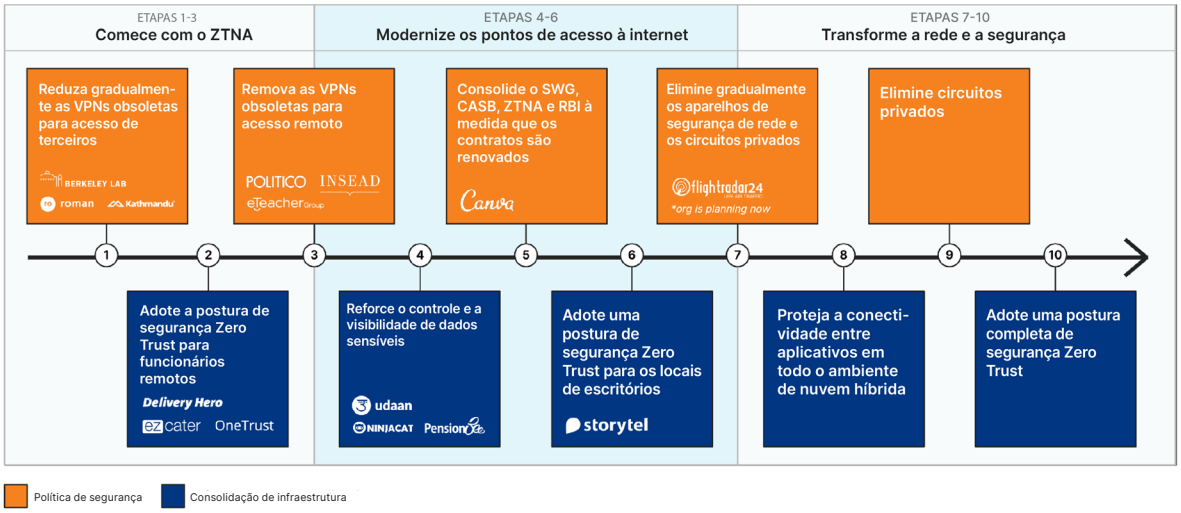
SUBSTITUA SUA VPN ULTRAPASSADA POR ACESSO À REDE ZERO TRUST

As promessas do Zero Trust podem parecer vazias para os líderes de segurança de TI em meio a uma longa e complicada transição para a segurança sem VPN. Mas é possível substituir sua VPN pelo Acesso à Rede Zero Trust sem fazer concessões na compatibilidade ou na funcionalidade do protocolo.

O caminho de migração recomendado varia de acordo com as prioridades da empresa que orientam seu projeto:

- se a conectividade mais rápida com aplicativos for sua prioridade, implante **primeiro o ZTNA baseado em cliente para aplicativos** não web.
- se aumentar a segurança de suas regras de acesso a aplicativos for mais importante, comece com **aplicativos web**.

Substituir sua VPN é apenas o primeiro passo para uma transformação completa da rede. Como a transição para um modelo SASE pode ser muito complicada, dividimos um caminho comum para a segurança Zero Trust com base na abordagem adotada por nossos clientes:



Saiba mais sobre como a plataforma Zero Trust da Cloudflare pode ajudá-lo a reduzir a dependência de sua VPN e, eventualmente, substituí-la.

Saiba mais

Veja uma comparação do mundo real entre VPN e ZTNA e como o Cloudflare Access aprimora a segurança para acesso a aplicativos.

Assista à demonstração

ANEXO

Modernize seus pontos de acesso à internet

A implementação do ZTNA é uma etapa importante na implantação de um modelo SASE (Serviço de Acesso Seguro de Borda). O **Cloudflare One** é uma solução abrangente de rede como serviço (NaaS) que simplifica e protege a rede corporativa para equipes de todos os tamanhos. Com o Cloudflare One, as organizações podem:

- **Adotar o acesso Zero Trust.** Substituir amplos perímetros de segurança por uma verificação individualizada de cada solicitação para cada recurso. Aplicar regras de Zero Trust em todas as conexões com seus aplicativos corporativos, não importa onde ou quem são seus usuários.
- **Proteger o tráfego da internet.** Quando as ameaças na internet se movem rapidamente, as defesas que você usa para detê-las precisam ser mais proativas. O Cloudflare One protege funcionários remotos contra ameaças na internet e aplica políticas que evitam que dados valiosos saiam de sua organização, impondo o isolamento do navegador Zero Trust a qualquer site — com uma experiência do usuário regular e rápida.
- **Proteger e conectar escritórios e data centers.** A rede corporativa tornou-se excessivamente complicada, o que significa que o tráfego de usuários geralmente precisa percorrer vários saltos para chegar onde precisa ir. Com o Cloudflare One, as empresas podem proteger escritórios e data centers por meio de uma plataforma em nuvem consistente e unificada.

Para saber mais sobre o Cloudflare One, assista a uma apresentação de 10 minutos e uma demonstração.

Transforme sua rede

Em breve, as ofertas Zero Trust e WAN como serviço da Cloudflare se tornarão uma só, permitindo que seus funcionários acessem recursos corporativos de forma consistente — onde quer que estejam trabalhando.

Hoje, seus produtos VPN e WAN permitem que seus funcionários acessem recursos localizados em sua rede corporativa privada, mas forçam você a gerenciar as políticas de conectividade e segurança de maneira diferente.

Agora, a Cloudflare fornece um plano de controle unificado, dando a você mais flexibilidade para aplicar as mesmas políticas de segurança Zero Trust a toda a sua força e local de trabalho sem precisar fazer malabarismos com vários produtos pontuais.

Para saber mais, visite https://www.cloudflare.com/pt-br/cloudflare-one/.