GUIA DE DESIGN

CLOUDFLARE

Cloudflare One
nossa plataforma SASE

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

ÍNDICE

Sobre este guia **3**

Transformação: uma comparação entre o antes e o depois da Cloudflare **4**

- Conectividade segura, rápida, confiável e privada para qualquer usuário 5
- Simplificando a conectividade e a segurança para recursos públicos 6-7
- Simplificando a conectividade e a segurança para recursos privados 8-9
- Simplificando a conectividade e a segurança para qualquer recurso 10
- Uma plataforma para conectividade e segurança mais simples 11

Caso de uso 1: acesso seguro para aplicativos web **12**

- Design legado - à primeira vista 13
- Design legado - falhas de segurança 14
- Design legado - complementos de segurança necessários 15
- Design do Cloudflare One 16
- Comparação de diagrama 17
- Comparação de tabela 18

Caso de uso 2: filtragem de DNS **19**

- Design legado - à primeira vista 20
- Design legado: falhas operacionais 21
- Design legado - modificações necessárias na rede 22
- Design do Cloudflare One 23
- Comparação de diagrama 24
- Comparação de tabela 25

Observação: serão adicionados mais casos de uso

Sobre este guia

Este guia de design se destina a profissionais técnicos e fornece exemplos ilustrativos de como as organizações podem simplificar e reforçar a arquitetura de rede e segurança com o Cloudflare One, nossa plataforma SASE. O Cloudflare One unifica serviços de conectividade de rede com os serviços de segurança Zero Trust. Todos são entregues na Rede global da Cloudflare.

A primeira seção deste guia de design trata da transformação e da modernização holísticas. Ela ilustra todos os elementos de conectividade e segurança possíveis alinhados à rede de entrada, rede de saída e aplicativos antes e depois da Cloudflare. Compara a abordagem de perímetro de segurança centralizada legada que conta com soluções de vários fornecedores com a abordagem da Rede global da Cloudflare que utiliza uma arquitetura de plataforma composta.

As próximas seções contêm casos de uso técnico comuns — primeiro, como esse problema é normalmente resolvido com uma abordagem legada e, em seguida, como o Cloudflare One resolve o mesmo problema com maior eficiência e experiência aprimorada.

Dois casos de uso foram priorizados com base na popularidade entre os clientes, mas de forma alguma representam todo o escopo dos recursos do Cloudflare One.

- Acesso seguro para aplicativos web privados e públicos
- Filtragem de DNS para funcionários locais e remotos

Continuaremos a expandir este guia com casos de uso adicionais, incluindo acesso seguro a redes privadas, proteção avançada de dados/contra ameaças e muito mais.

Transformação: Uma comparação entre o antes e o depois da Cloudflare

Conectividade segura, rápida, confiável e privada para qualquer usuário

Qualquer usuário

As organizações precisam permitir conectividade segura, rápida, confiável e privada para dois grupos de usuários.

Os **usuários gerenciados** são funcionários que acessam um recurso usando um dispositivo corporativo ou pessoal, seja em casa, no escritório ou em outro local.

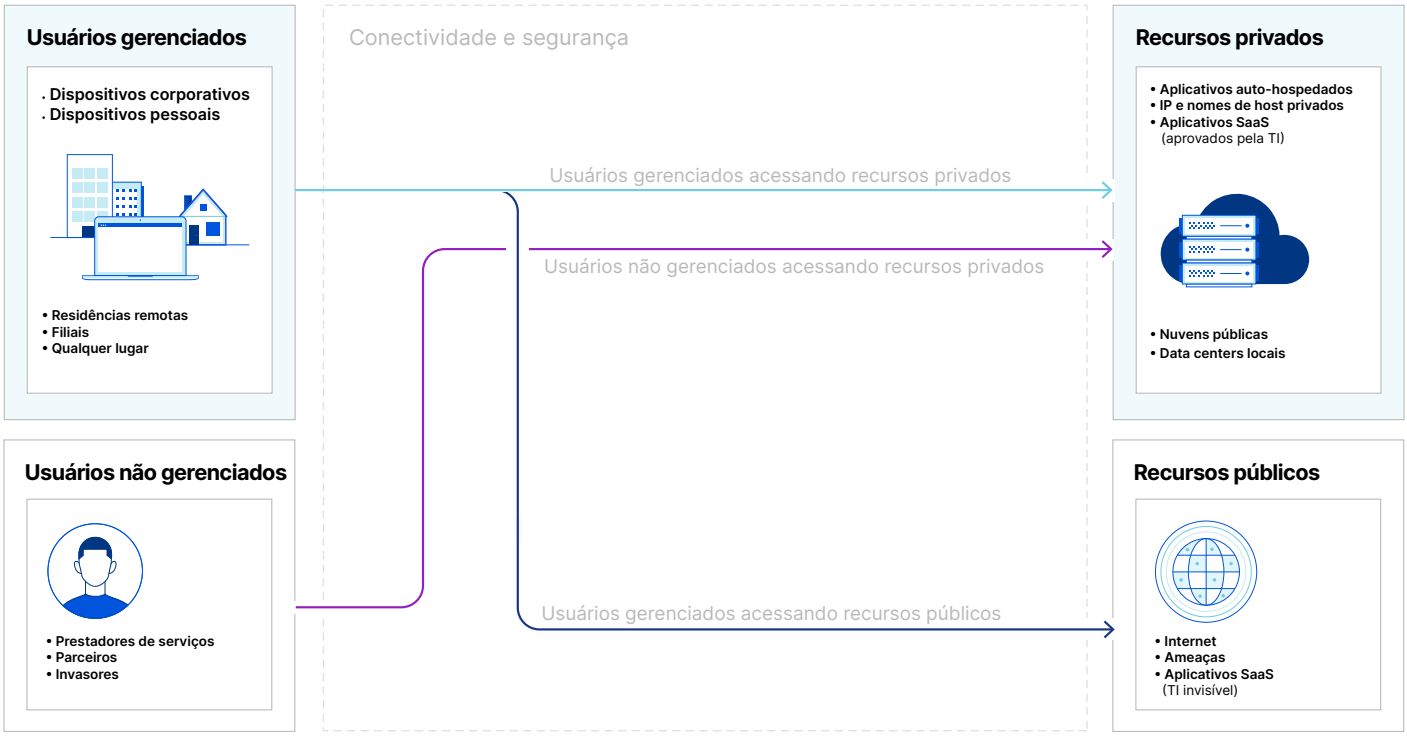
Os **usuários não gerenciados** incluem prestadores de serviços ou parceiros autorizados a usar um recurso, bem como invasores não autorizados.

Qualquer recurso

As organizações precisam habilitar o gerenciamento de acesso com proteção de dados e contra ameaças para dois grupos de recursos.

Os **recursos privados** incluem aplicativos auto-hospedados e IPs ou nomes de host privados em nuvens públicas e data centers locais, além de aplicativos SaaS aprovados pela TI.

Os **recursos públicos** na internet incluem aplicativos SaaS não sancionados e ameaças.



Comparação da conectividade e da segurança antes e depois da Cloudflare

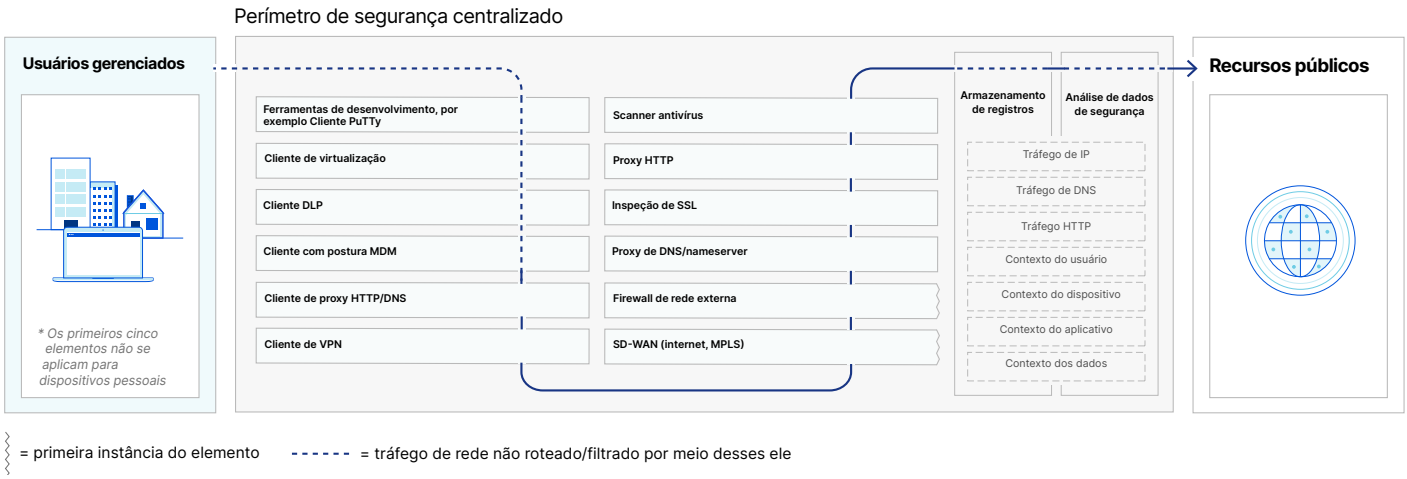
Nas próximas seis páginas, uma série de diagramas de antes e depois apresenta, de forma incremental, detalhes em camadas sobre todos os elementos de conectividade e segurança possíveis que sua organização exige para usuários gerenciados que acessam recursos públicos e usuários gerenciados ou não gerenciados que acessam recursos privados.

O primeiro diagrama “antes” ilustra a computação de endpoint e os dispositivos de rede implantados em um perímetro de segurança centralizado.

O segundo diagrama “depois” ilustra os serviços de nuvem comparáveis fornecidos por meio da Rede global da Cloudflare.

1a. Simplificando a conectividade e a segurança para recursos públicos

Depois da Cloudflare



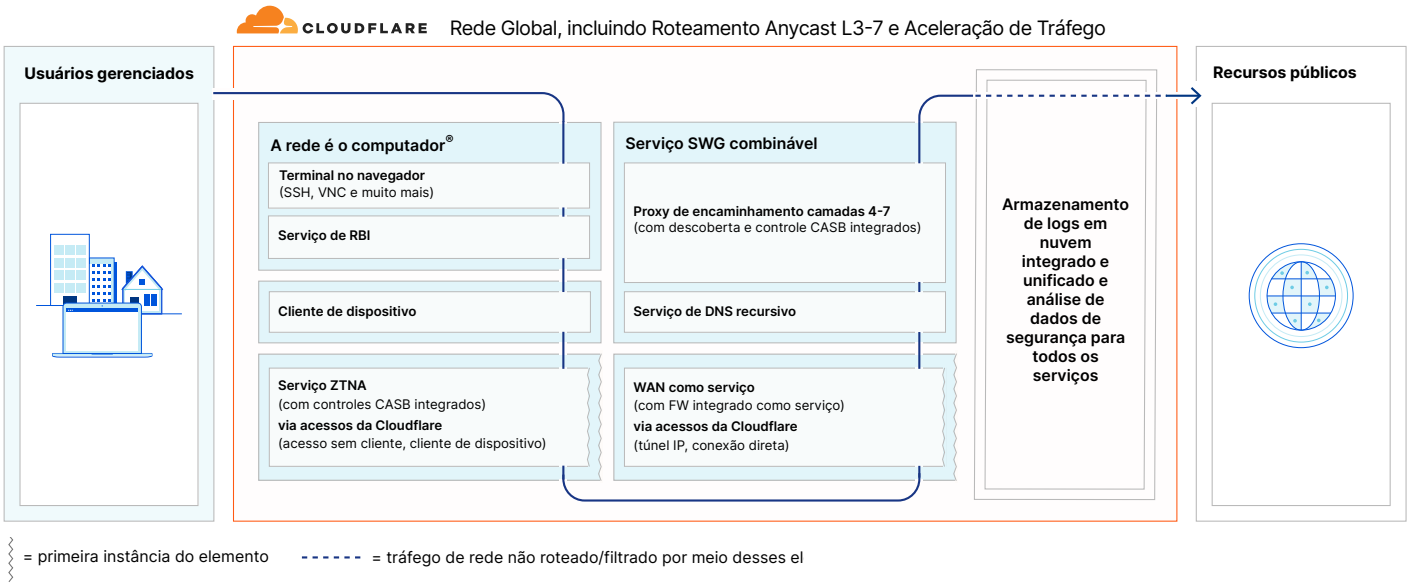
Usuários gerenciados (para recursos públicos e privados)

As equipes de TI tinham que gerenciar muitos clientes para verificar conectividade e segurança — ou pior, não conseguiam fazer isso para dispositivos pessoais. Ferramentas de desenvolvimento e VPN para acesso privado. Proxy HTTP/DNS para acesso público. Virtualização, DLP e MDM para uma melhor proteção.

Recursos públicos

As equipes de segurança dependiam do cliente de VPN ou SD-WAN para rotear o tráfego de usuários remotos ou do escritório através do firewall de rede, proxy DNS, inspeção de SSL, proxy HTTP e dispositivos de verificação antivírus para proteger o acesso a recursos públicos.

Depois da Cloudflare



Usuários gerenciados (para recursos públicos e privados)

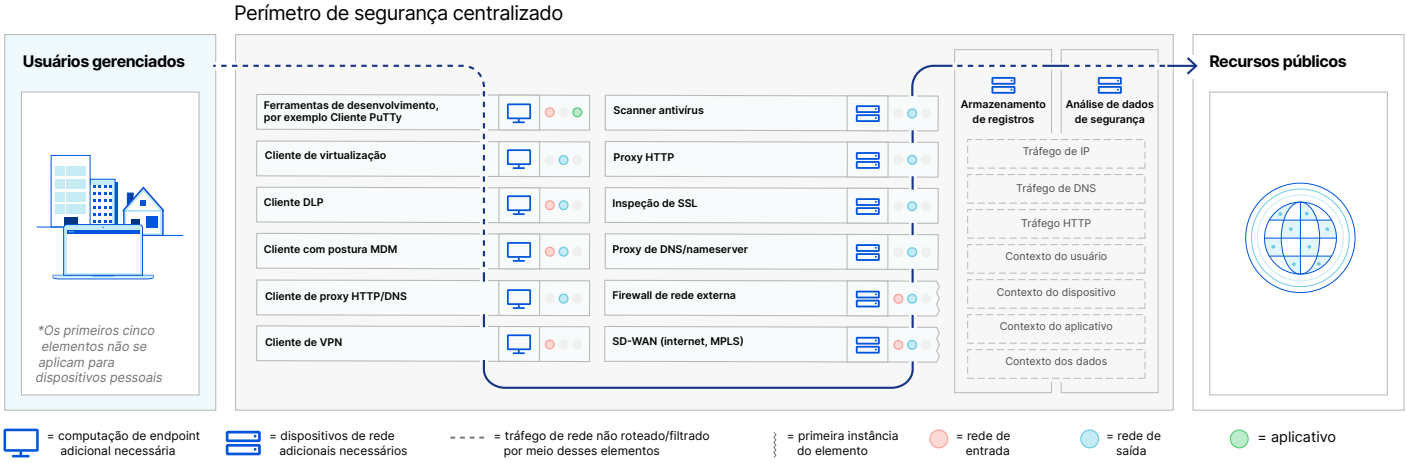
A rede remove muitas funções do computador ou um cliente consolida muitas funções.

Recursos públicos

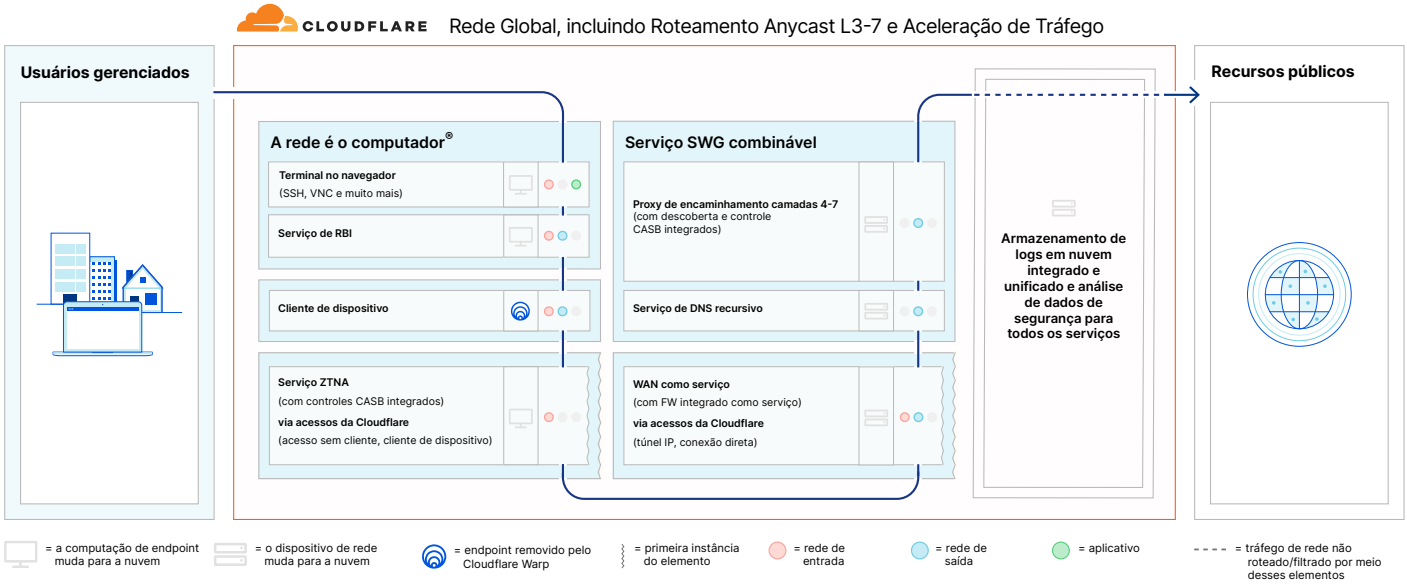
Nosso serviço SWG combinável inspeciona o tráfego em uma única passagem antes ou depois de adotar nossa WAN como serviço e/ou serviço ZTNA com segurança integrada.

1b. Simplificando a conectividade e a segurança para recursos públicos

Depois da Cloudflare



Depois da Cloudflare



Serviços nativos em nuvem

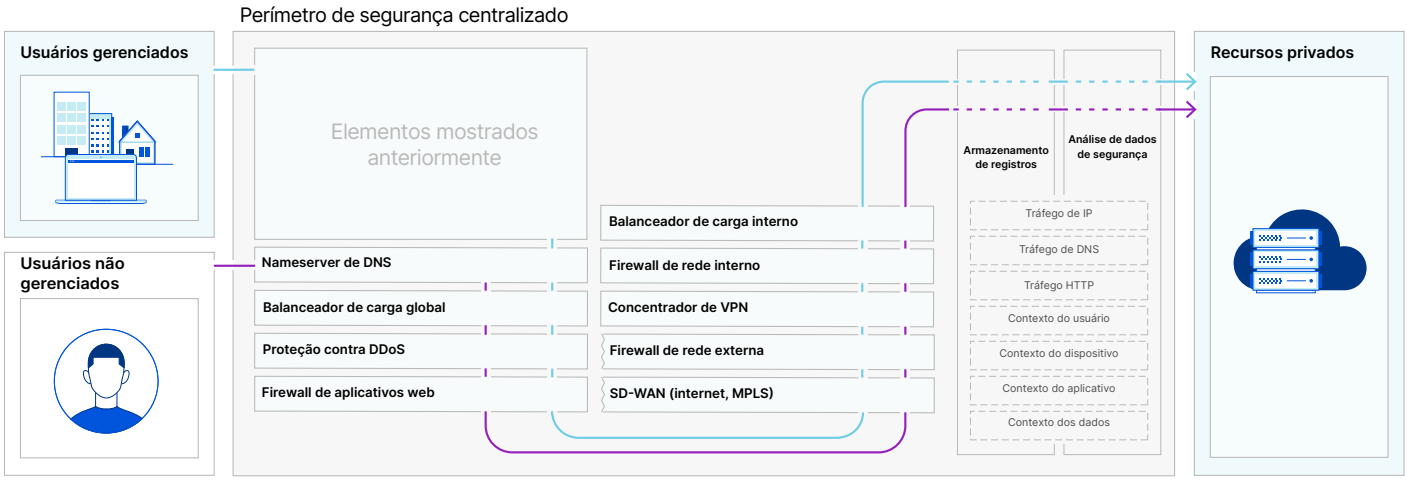
Os requisitos de computação de endpoint e dispositivo de rede são reduzidos.

Arquitetura combinável

As pilhas de rede de entrada e saída são unificadas com a pilha de aplicativos para segurança e performance de ponta a ponta.

2a. Simplificando a conectividade e a segurança para recursos privados

Depois da Cloudflare



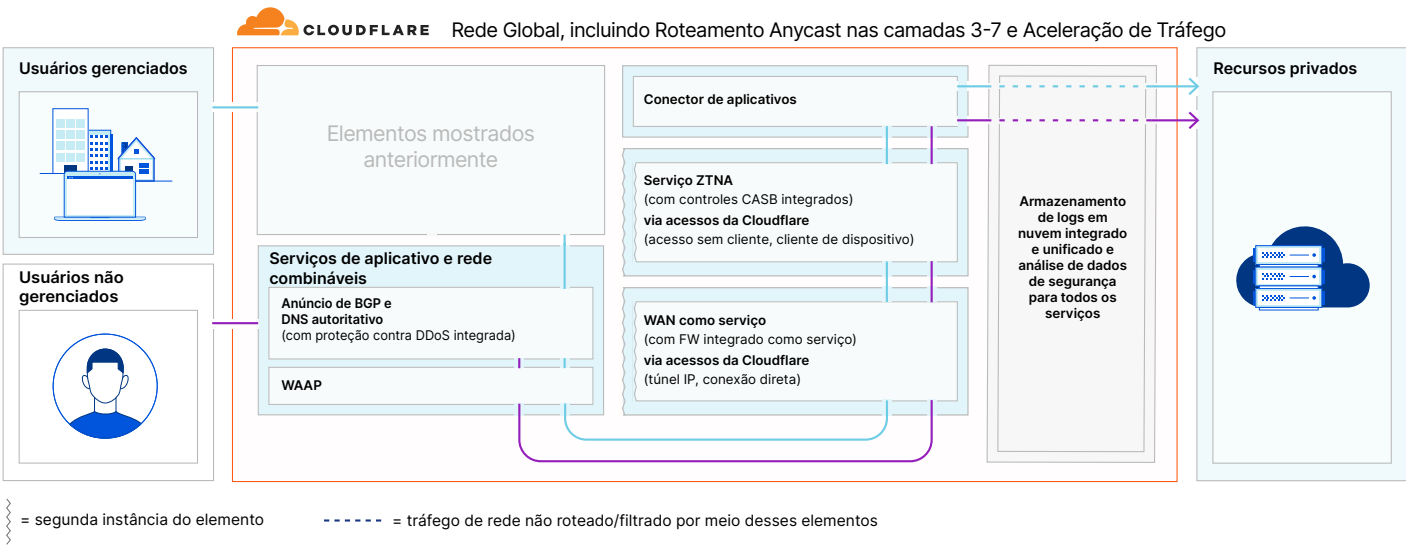
Usuários não gerenciados

As equipes de rede precisavam anunciar publicamente a disponibilidade de recursos privados para prestadores de serviços e parceiros e se proteger contra DDoS ou exploração por invasores.

Recursos privados (de usuários gerenciados e não gerenciados)

As equipes de segurança dependiam do cliente de VPN ou SD-WAN para rotear o tráfego dos usuários através dos firewalls de rede, concentradores de VPN e balanceadores de carga para proteger o acesso a recursos privados.

Depois da Cloudflare



Usuários não gerenciados

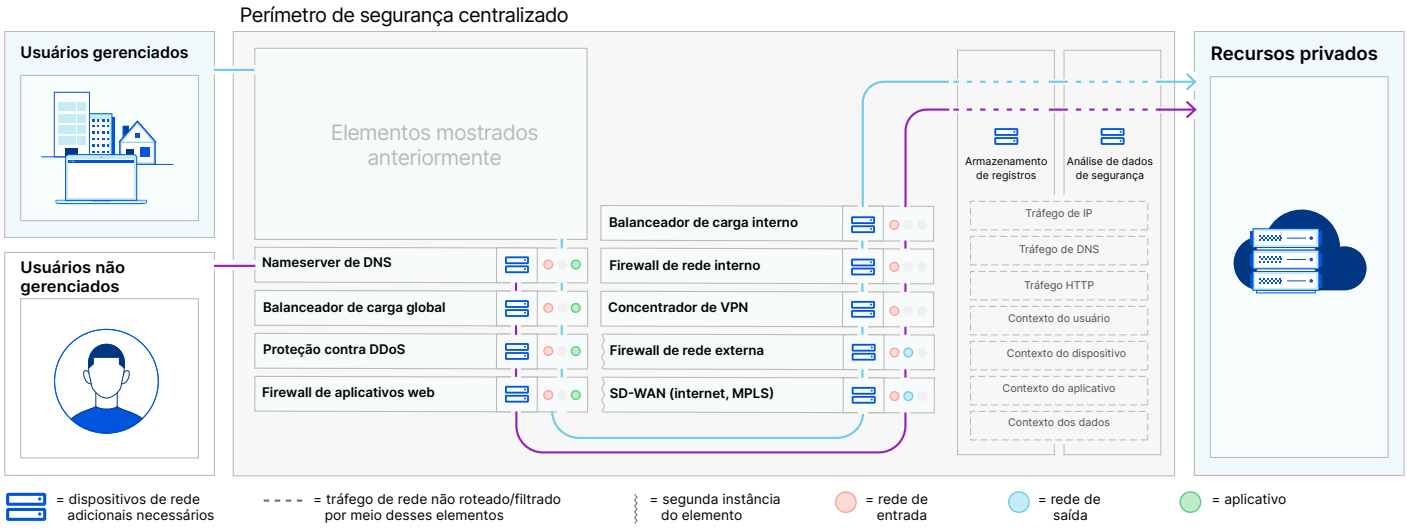
Nossos aplicativos e serviços de rede combináveis eliminam esse fardo antes ou depois de adotar nosso serviço ZTNA ou WAN como serviço com segurança integrada.

Recursos privados (de usuários gerenciados e não gerenciados)

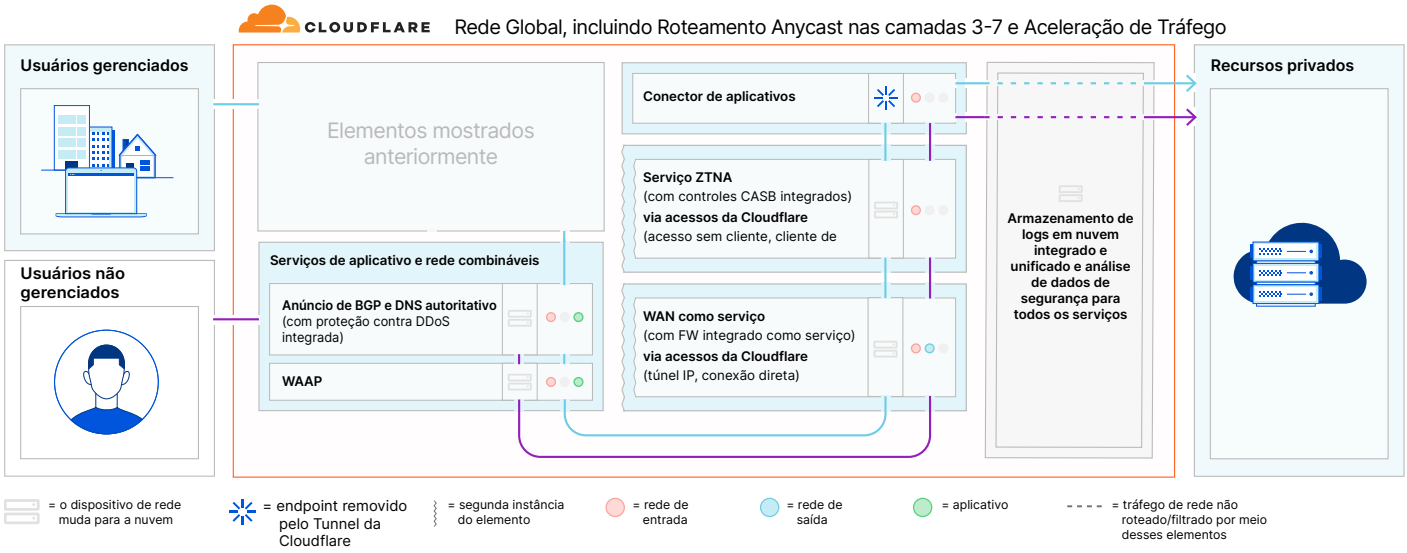
Nosso serviço ZTNA e/ou WAN como serviço com segurança integrada simplifica o acesso usando nosso conector de aplicativos.

2b. Simplificando a conectividade e a segurança para recursos privados

Depois da Cloudflare



Depois da Cloudflare



Serviços nativos em nuvem

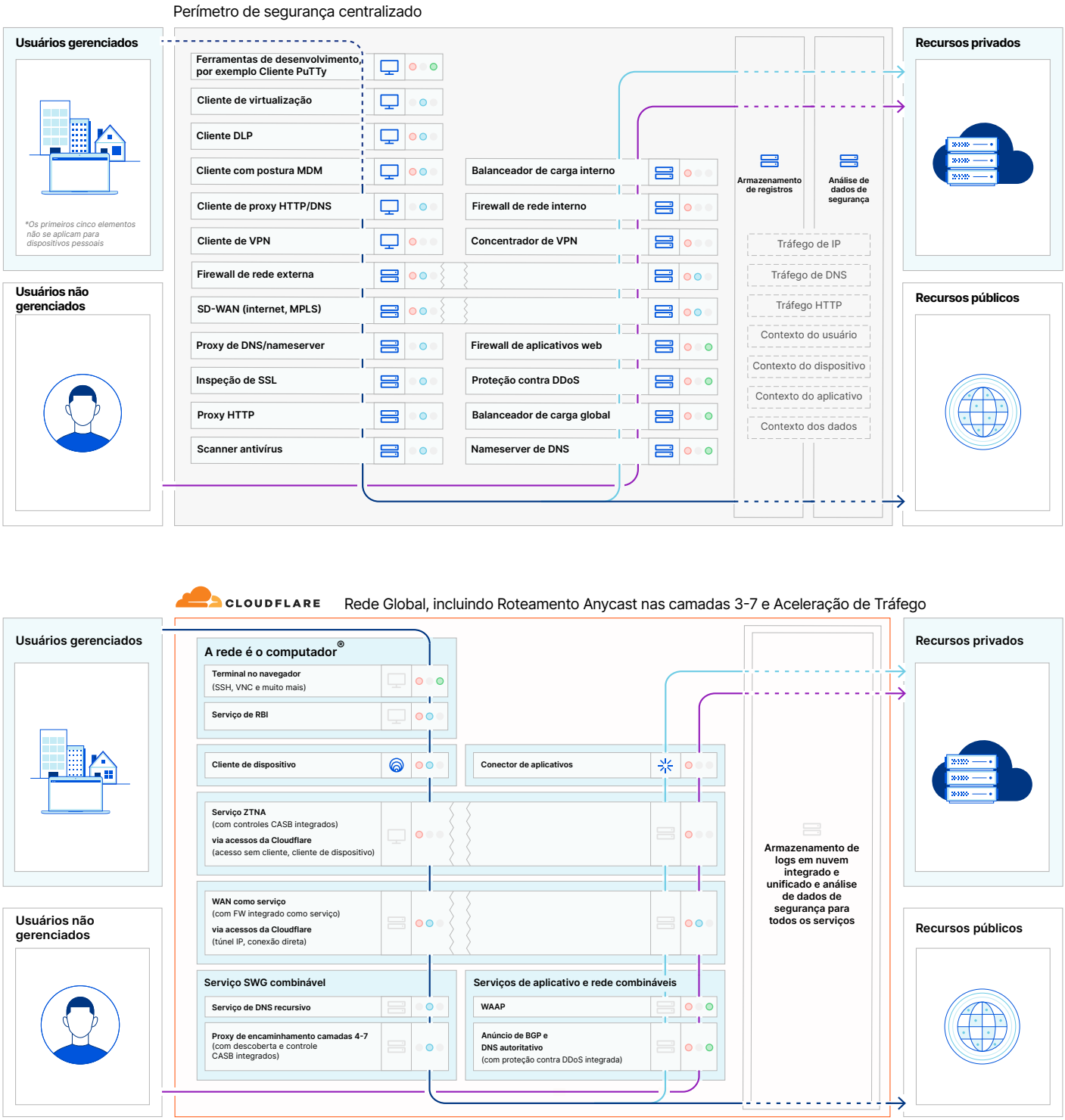
Os requisitos de computação de endpoint e dispositivo de rede são reduzidos.

Arquitetura combinável

As pilhas de rede de entrada e saída são unificadas com a pilha de aplicativos para segurança e performance de ponta a ponta.

Simplificando a conectividade e a segurança para qualquer recurso

Esta visualização reúne os diagramas 1 e 2.



Depois

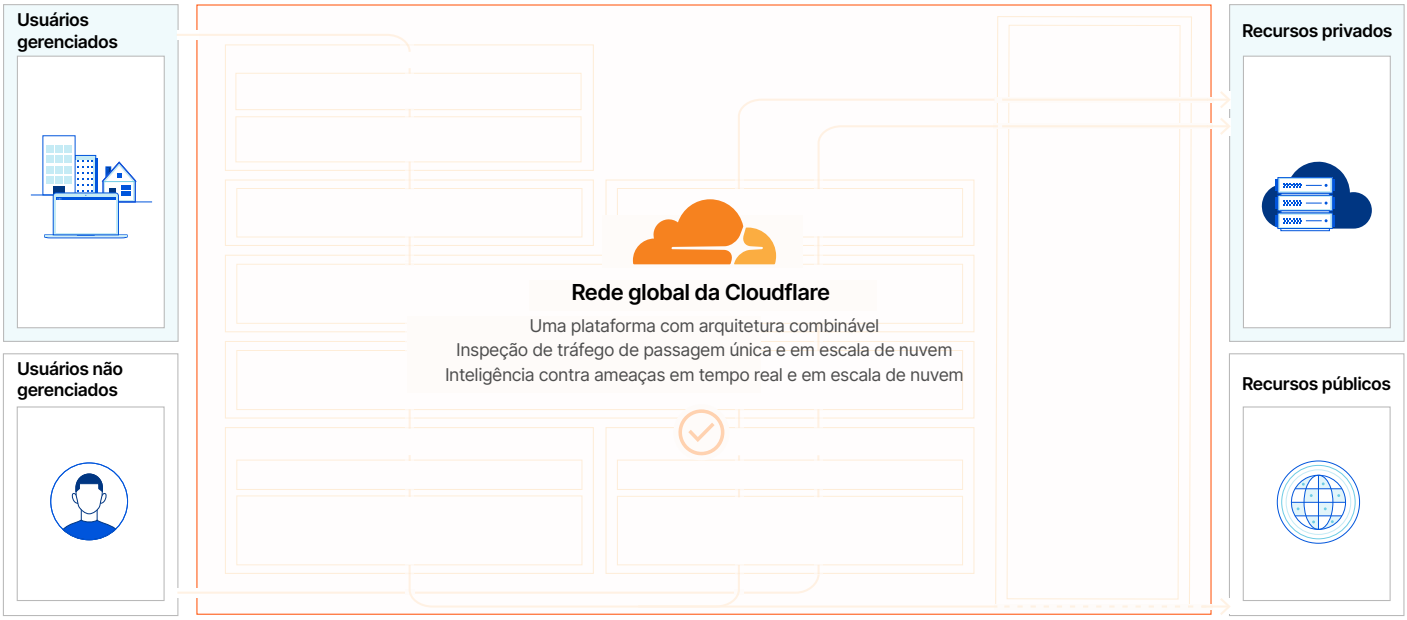
Os elementos de conectividade e segurança são reutilizados quando qualquer usuário acessa qualquer recurso, o que melhora a eficiência e a experiência. Além disso, nosso serviço ZTNA e a WAN como serviço abrangem elementos que eram tradicionalmente gerenciados separadamente nas equipes de TI, rede e segurança.

Uma plataforma para a conectividade e a segurança mais simples

Comparação entre perímetro de segurança centralizado e a Rede global da Cloudflare

Antes

As equipes de TI, rede e segurança dependiam de soluções de muitos fornecedores, cada uma com uma arquitetura diferente, de modo que as integrações ponto a ponto geravam falhas de conectividade e segurança com performance limitada.



Depois

Todas as equipes utilizam uma plataforma com a mesma arquitetura combinável para eliminar lacunas e perdas na performance. Nossa plataforma inteira funciona em todos os lugares e é construída para se adequar ao seu mundo e não o contrário. Você pode implantar qualquer número de serviços, em qualquer sequência e eles ainda funcionarão uniformemente juntos.

Caso de uso 1: Acesso seguro para aplicativos web

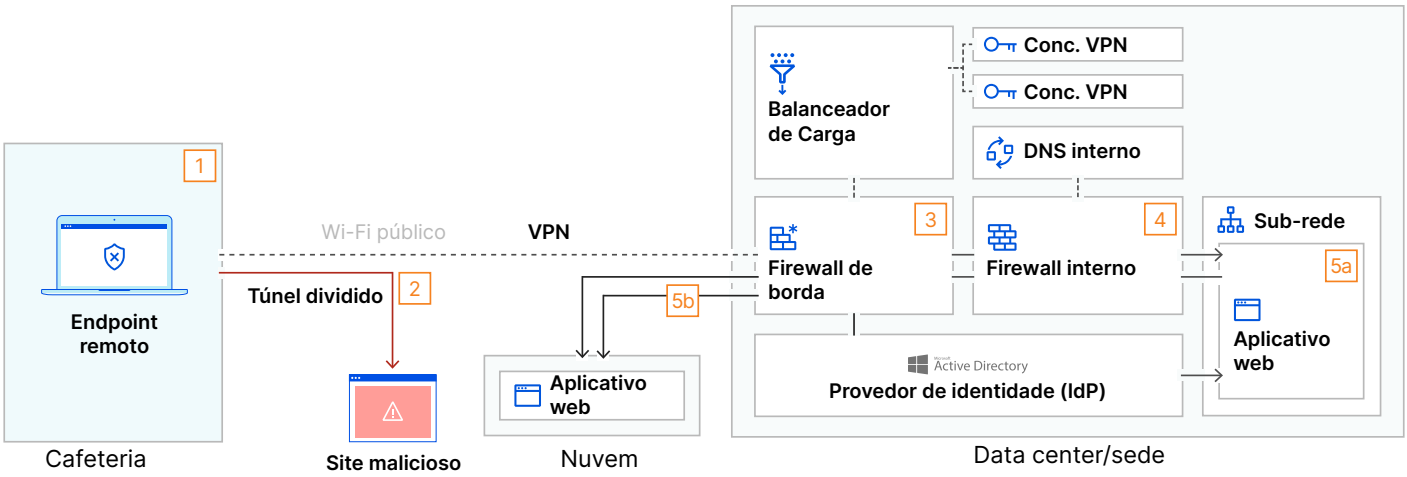
Design legado - à primeira vista

Este gráfico representa um método tradicional de fornecer acesso remoto a aplicativos web. Aqui, um funcionário remoto acessa recursos corporativos, especificamente um aplicativo web privado (auto-hospedado) e público (baseado em nuvem).

Incluímos algumas das medidas de segurança mais comuns que qualquer organização razoável adotaria, incluindo um firewall de borda, um firewall interno para segmentação e uma VPN.

Da esquerda para a direita, esse cenário ilustra a existência de uma sessão quando um usuário faz login em um local público — um cenário sobre o qual os gráficos de design subsequentes serão construídos.

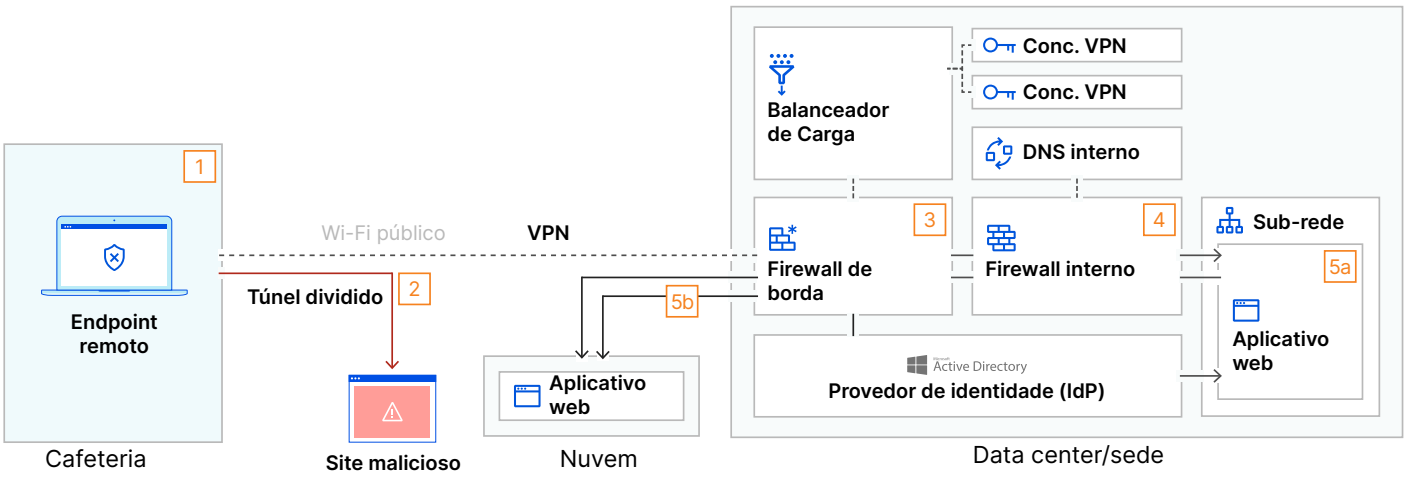
Observação: este gráfico mostra apenas os dispositivos, ferramentas e fluxos de tráfego envolvidos nessa transação de rede específica. Ele não representa um instantâneo abrangente de todas as tecnologias que estariam presentes em uma arquitetura de rede legada.



	Ação na rede/de segurança
1	Um dispositivo remoto se conecta a recursos corporativos via Wi-Fi público
2	O dispositivo remoto alcança a borda corporativa via cliente de VPN, mas divide outros túneis de tráfego
3	A VPN termina no firewall de borda ou no concentrador de VPN atrás do firewall
4	A política de firewall concede acesso de usuários remotos à sub-rede com aplicativo web privado
5	O usuário acessa o aplicativo da web por IP/URL privado **[5a]** ou URL público **[5b]** depois de autenticar no IDP

Design legado - falhas de segurança

Este gráfico adiciona outra coluna à tabela abaixo, destacando problemas de falhas de segurança associados a cada etapa específica neste cenário e que deixam uma organização vulnerável.

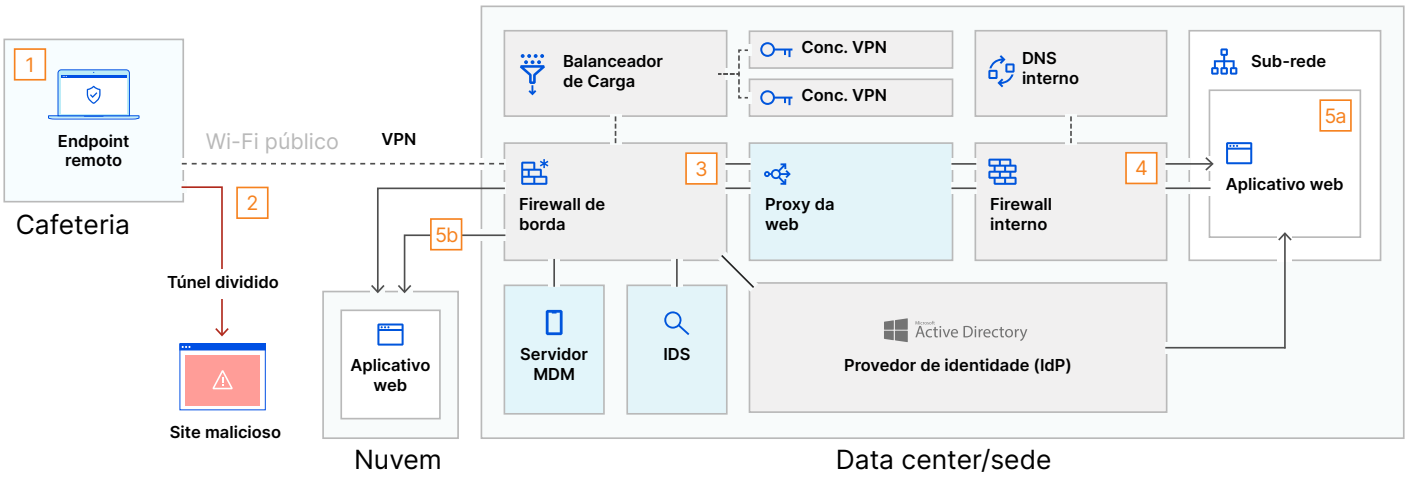


	Ação na rede/de segurança	Solução legada relevante	Falha no design legado
1	Um dispositivo remoto se conecta a recursos corporativos via Wi-Fi público	Cliente de VPN corporativa	Um dispositivo desprotegido em uma rede Wi-Fi pública é alvo de agentes mal-intencionados
2	O endpoint remoto alcança a borda corporativa via cliente de VPN, mas divide outros túneis de tráfego	Cliente de VPN corporativa	A segurança específica da VPN não protegerá o tráfego dividido em túneis
3	A VPN termina no firewall de borda ou no concentrador de VPN atrás do firewall	Balanceador de Carga Firewall de borda Concentrador de VPN	As regras de FW/VPN de entrada podem expor portas/protocolos à internet, expandindo a superfície de ataque em potencial
4	A política de firewall concede acesso de usuários remotos à sub-rede com aplicativo web privado	Firewall interno	O usuário tem acesso a recursos fora de sua função de trabalho
5	O usuário acessa o aplicativo da web por IP/URL privado **[5a]** ou URL público **[5b]** depois de autenticar no IDP	Diretório ativo DNS interno (privado)	Se o endpoint for comprometido, o aplicativo/rede empresarial fica em risco

Design legado - complementos de segurança necessários

Para abordar as falhas de design destacadas na página anterior, a organização agora precisa modificar a arquitetura de rede existente. Este gráfico adiciona outra coluna à tabela abaixo, detalhando soluções típicas para proteger usuários e recursos.

O uso de vários complementos de segurança adiciona complexidade e custos de gerenciamento contínuos entre vários fornecedores prováveis para ambiente legado.



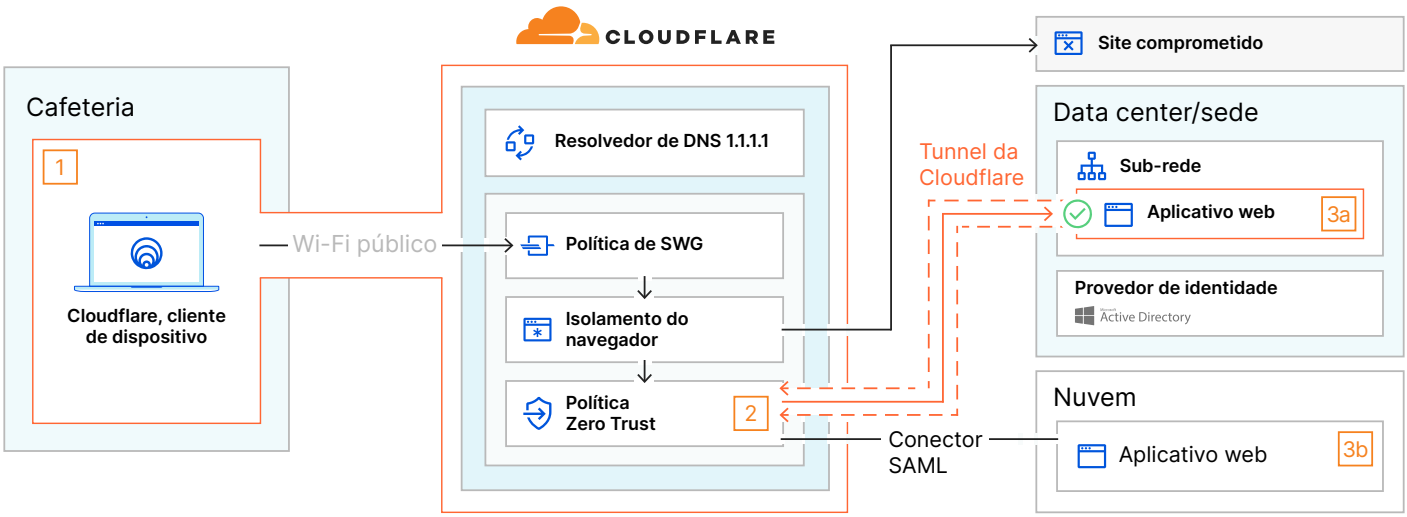
	Ação na rede/de segurança	Solução legada relevante	Falha no design legado	Complemento de segurança necessário
1	Um dispositivo remoto se conecta a recursos corporativos via Wi-Fi público	Cliente de VPN corporativa	Um dispositivo desprotegido em uma rede Wi-Fi pública é alvo de agentes mal-intencionados	Plataforma de proteção de endpoints (EPP)
2	O dispositivo remoto alcança a borda corporativa via cliente de VPN, mas divide outros túneis de tráfego	Cliente de VPN corporativa	A segurança específica da VPN não protegerá o tráfego dividido em túneis	Desativar o túnel dividido
3	A VPN termina no firewall de borda ou no concentrador de VPN atrás do firewall	Balanceador de Carga Firewall de borda Concentrador de VPN	As regras de FW/VPN de entrada podem expor portas/protocolos à internet, expandindo a superfície de ataque em potencial	Sistema de detecção de intrusão (IDS)
4	A política de firewall concede acesso de usuários remotos à sub-rede com aplicativo web privado	Firewall interno	O usuário tem acesso a recursos fora de sua função de trabalho	Proxy da web
5	O usuário acessa o aplicativo da web por IP/URL privado **[5a]** ou URL público **[5b]** depois de autenticar no IDP	Diretório ativo DNS interno (privado)	Se o endpoint for comprometido, o aplicativo/rede empresarial fica em risco	Servidor de gerenciamento de dispositivo móvel (MDM)

Design do Cloudflare One

O gráfico abaixo destaca como uma organização pode adotar uma abordagem mais simples e eficiente para proteger o acesso a aplicativos implementando o Cloudflare One.

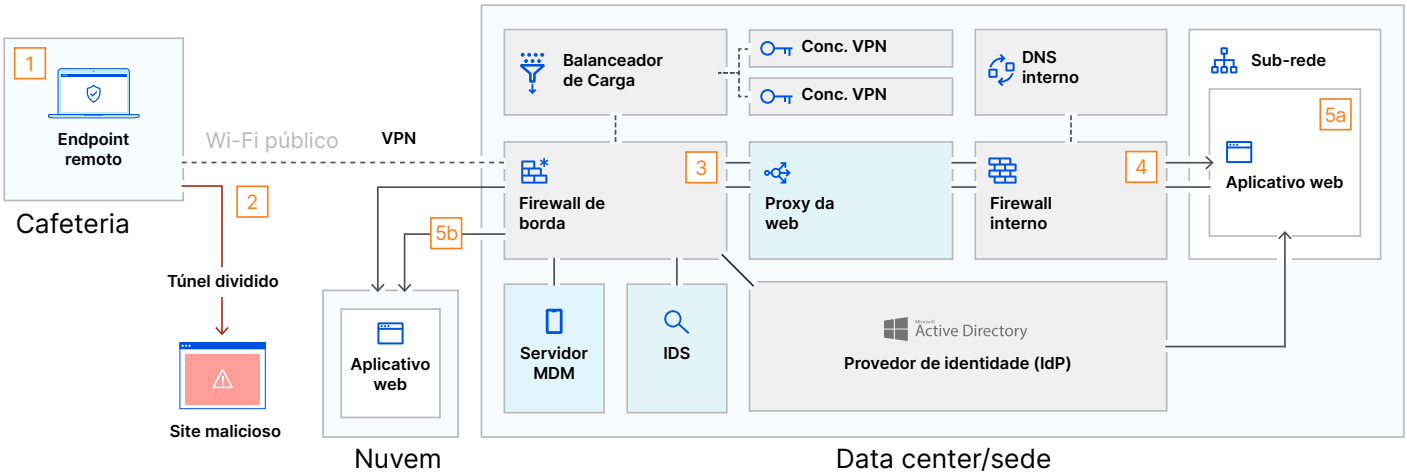
Aqui, grande parte da arquitetura de rede legada, mostrada anteriormente, é transferida para a Cloudflare. Muitas das falhas de design existentes são corrigidas sem a necessidade de soluções adicionais.

Com o Cloudflare One, o tráfego entre o usuário remoto e os recursos da organização acontece ao longo da Rede global da Cloudflare com inspeção de passagem única. Todos os serviços mostrados abaixo são executados em todos os data centers da Cloudflare, localizados em mais de 250 cidades em mais de 100 países.

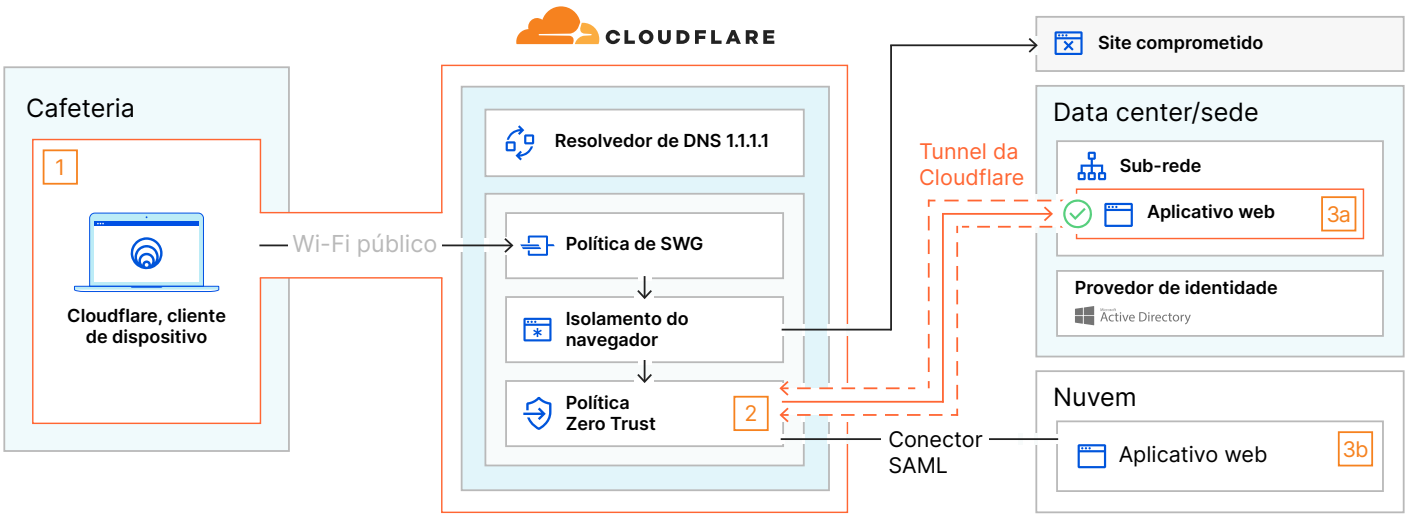


	Ação na rede/de segurança	Elemento relevante do Cloudflare One	Correção das falhas de design
1	Um dispositivo remoto se conecta a recursos corporativos e à internet via Cloudflare	**Cliente de dispositivo da Cloudflare** **Política de gateway seguro da web** **Isolamento do navegador**	O cliente do gateway seguro da web local permite que o Cloudflare One filtre o tráfego de DNS/HTTP/rede para o dispositivo do usuário por meio da política de gateway O isolamento do navegador absorve/isola o impacto de ataques de malware bem-sucedidos de sites
2	O usuário passa por verificações de IDP e postura do dispositivo na Cloudflare	**Política Zero Trust**	A política Zero Trust realiza a verificação da postura do dispositivo antes de permitir o acesso, mitigando o risco de dispositivos comprometidos A política Zero Trust autentica o usuário no recurso em vez de na rede subjacente, evitando o movimento lateral
3	Acessar o aplicativo da web [privado | público] diretamente pelo [Tunnel da Cloudflare | Conector SAML]	**Tunnel da Cloudflare** **Resolvedor de DNS 1.1.1.1**	O Tunnel da Cloudflare faz a intermediação com segurança de uma conexão com o aplicativo web e elimina o uso de regras explícitas de FW

Design legado - complementos de segurança necessários



Design do Cloudflare One



Design legado - complementos de segurança necessários

	Ação na rede/de segurança	Solução legada relevante	Falha no design legado	Complemento de segurança necessário
1	Um dispositivo remoto se conecta a recursos corporativos via Wi-Fi público	Cliente de VPN corporativa	Um dispositivo desprotegido em uma rede Wi-Fi pública é alvo de agentes mal-intencionados	Plataforma de proteção de endpoints (EPP)
2	O dispositivo remoto alcança a borda corporativa via cliente de VPN, mas divide outros túneis de tráfego	Cliente de VPN corporativa	A segurança específica da VPN não protegerá o tráfego dividido em túneis	Desativar o túnel dividido
3	A VPN termina no firewall de borda ou no concentrador de VPN atrás do firewall	Balanceador de Carga Firewall de borda Concentrador de VPN	As regras de FW/VPN de entrada podem expor portas/protocolos à internet, expandindo a superfície de ataque em potencial	Sistema de detecção de intrusão (IDS)
4	A política de firewall concede acesso de usuários remotos à sub-rede com aplicativo web privado	Firewall interno	O usuário tem acesso a recursos fora de sua função de trabalho	Proxy da web
5	O usuário acessa o aplicativo da web por IP/URL privado **[5a]** ou URL público **[5b]** depois de autenticar no IDP	Diretório ativo DNS interno (privado)	Se o endpoint for comprometido, o aplicativo/rede empresarial fica em risco	Servidor de gerenciamento de dispositivo móvel (MDM)

Design do Cloudflare One

	Ação na rede/de segurança	Elemento relevante do Cloudflare One	Correção das falhas de design
1	Um dispositivo remoto se conecta a recursos corporativos e à internet via Cloudflare	**Cliente de dispositivo da Cloudflare** **Política de gateway seguro da web** **Isolamento do navegador**	O cliente do gateway seguro da web local permite que o Cloudflare One filtre o tráfego de DNS/HTTP/rede para o dispositivo do usuário por meio da política de gateway O isolamento do navegador absorve/isola o impacto de ataques de malware bem-sucedidos de sites
2	O usuário passa por verificações de IDP e postura do dispositivo na Cloudflare	**Política Zero Trust**	A política Zero Trust realiza a verificação da postura do dispositivo antes de permitir o acesso, mitigando o risco de dispositivos comprometidos A política Zero Trust autentica o usuário no recurso em vez de na rede subjacente, evitando o movimento lateral
3	Acessar o aplicativo da web [privado | público] diretamente pelo [Tunnel da Cloudflare | Conector SAML]	**Tunnel da Cloudflare** **Resolvedor de DNS 1.1.1.1**	O Tunnel da Cloudflare faz a intermediação com segurança de uma conexão com o aplicativo web e elimina o uso de regras explícitas de FW

Caso de uso 2: Filtragem de DNS

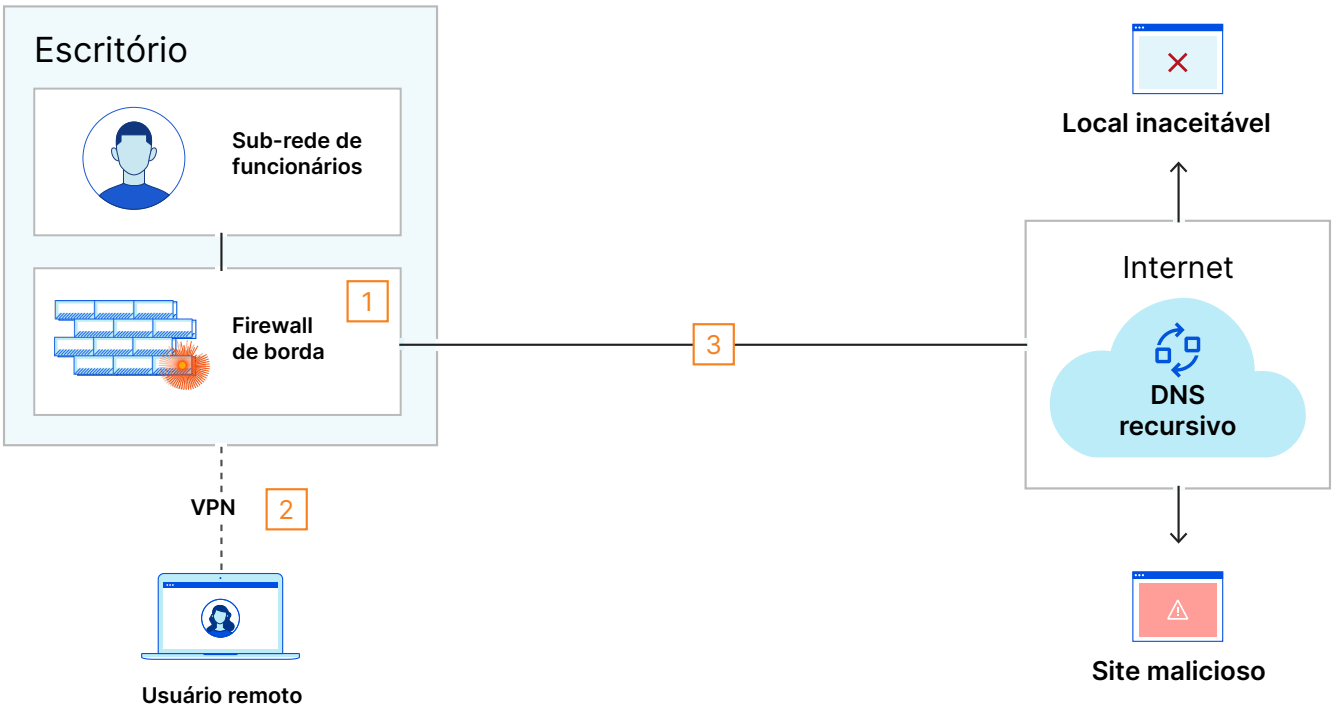
Design legado - à primeira vista

Este gráfico representa como as organizações implementam a filtragem de DNS para funcionários locais e remotos em um ambiente legado.

Normalmente, a filtragem de DNS para organizações é realizada por meio de recursos integrados de soluções locais, como um firewall. Os usuários remotos enviam solicitações por meio desse firewall primeiro fazendo backhaul de tráfego por meio de uma VPN de túnel completo.

Para resolver sites, a organização envia suas consultas de DNS para um DNS recursivo (como o 8.8.8.8 do Google).

Observação: assim como em outras seções deste guia, esse ambiente legado não representa todas as tecnologias dentro de um escritório, mas apenas as envolvidas nesse caso de uso específico.



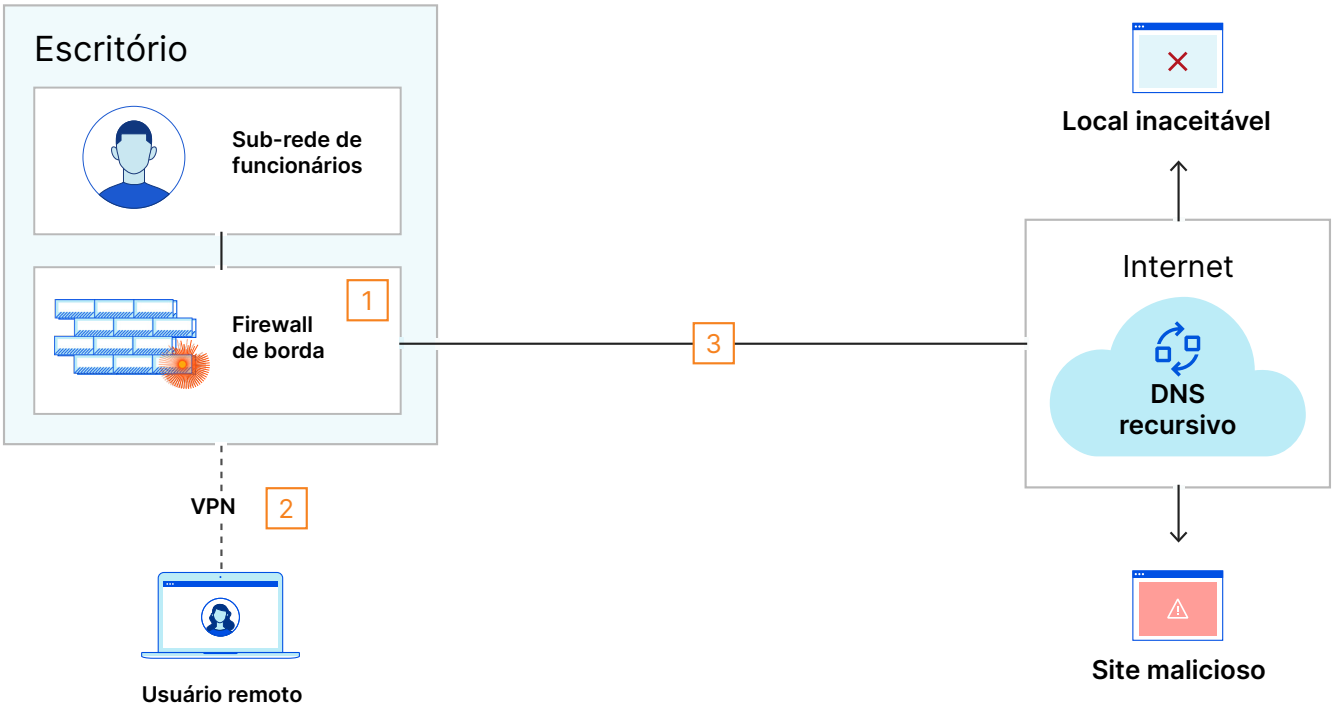
	Evento relacionado a DNS
1	Um usuário local tem seu conteúdo de solicitações de DNS filtrado para segurança pelo recurso integrado no firewall de borda
2	Um usuário remoto tem suas solicitações de DNS filtradas após se conectar à VPN de túnel completo da organização
3	As solicitações de DNS de saída são transmitidas sem problemas.

Design legado: falhas operacionais

Este próximo gráfico adiciona uma coluna à tabela abaixo articulando os desafios associados a esse design tradicional.

O desafio mais urgente é que confiar no hardware local para realizar a filtragem de DNS em escala acabará por afunilar a performance para todos os usuários, especialmente quando esse hardware também for responsável por outros serviços críticos (como terminar a VPN de usuários remotos).

Além disso, o envio de consultas de DNS sem criptografia (o que ocorre por padrão) cria um novo vetor de ataque com risco desconhecido.



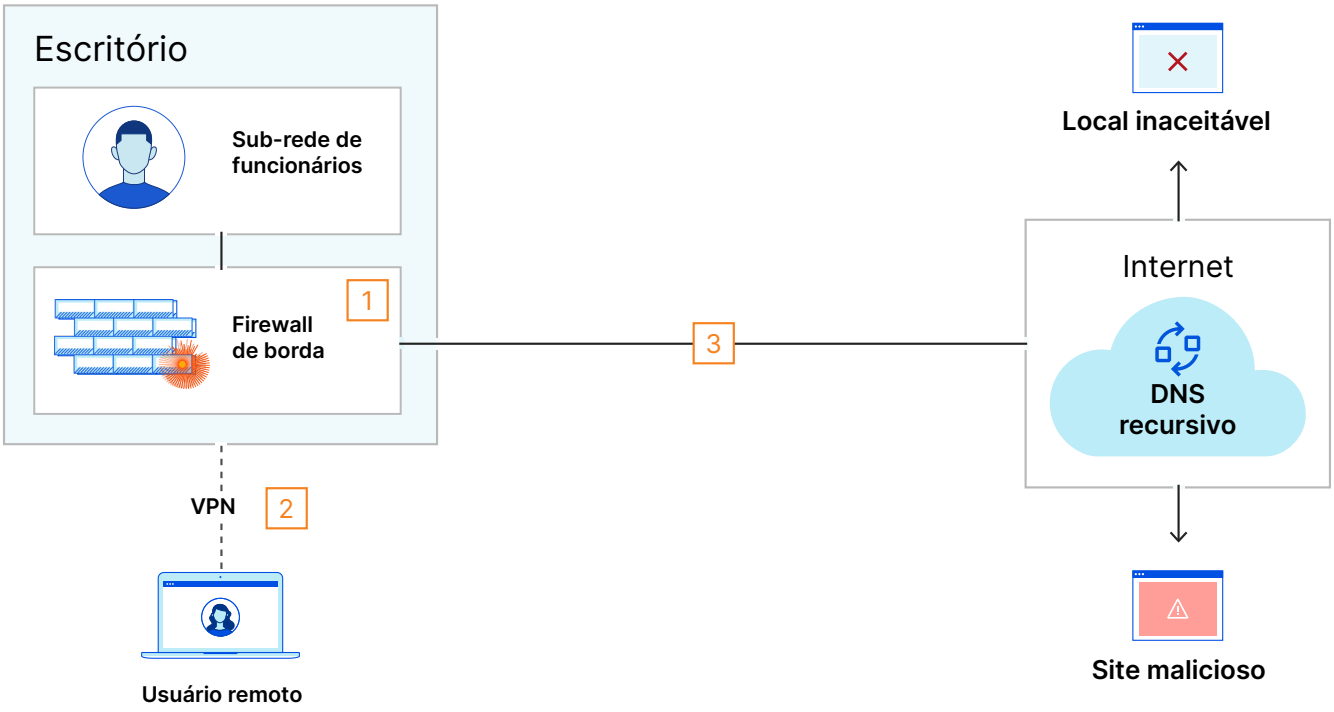
	Evento relacionado a DNS	Elementos relevantes	Falha de design
1	Um usuário local tem seu conteúdo de solicitações de DNS filtrado para segurança pelo recurso integrado no firewall de borda	Firewall de borda	Confiar no Edge FW para muitas operações essenciais pode prejudicar a performance em toda a organização
2	Um usuário remoto tem suas solicitações de DNS filtradas após se conectar à VPN de túnel completo da organização	Concentrador de VPN Firewall de borda	Uma VPN de túnel completo cria uma “taxa dupla” de pacotes de internet, o que pode criar um gargalo de performance para todo o tráfego em túnel da organização
3	As solicitações de DNS de saída são transmitidas sem problemas.	UDP53	O DNS na porta UDP 53 não é criptografado e, portanto, não é privado. Qualquer um que veja isso pode reconhecer o comportamento do usuário na web

Design legado - modificações necessárias na rede

Para resolver as falhas de design destacadas na página anterior, a organização agora precisa modificar a arquitetura de rede existente. Este gráfico adiciona outra coluna à tabela abaixo, destacando soluções comuns e suas desvantagens.

Aqui, comprar novo hardware para lidar com mais usuários ou aumentar o consumo de largura de banda resultará em maiores despesas operacionais e de capital ao longo do tempo.

As organizações que tentam ampliar essa abordagem muitas vezes enfrentam problemas de crescimento consideráveis. De fato, muitas organizações evitam a filtragem de DNS inteiramente devido a essas preocupações operacionais.



	Evento relacionado a DNS	Elementos relevantes	Falha de design	Solução que não é da Cloudflare
1	Um usuário local tem seu conteúdo de solicitações de DNS filtrado para segurança pelo recurso integrado no firewall de borda	Firewall de borda	Confiar no Edge FW para muitas operações essenciais pode prejudicar a performance em toda a organização	Filtro de DNS discreto
2	Um usuário remoto tem suas solicitações de DNS filtradas após se conectar à VPN de túnel completo da organização	Concentrador de VPN Firewall de borda	Uma VPN de túnel completo cria uma "taxa dupla" de pacotes de internet, o que pode criar um gargalo de performance para todo o tráfego em túnel da organização	Aumentar a largura de banda do provedor Upgrade de hardware Ativar o túnel dividido*
3	As solicitações de DNS de saída são transmitidas sem problemas.	UDP53	O DNS na porta UDP 53 não é criptografado e, portanto, não é privado. Qualquer um que veja isso pode reconhecer o comportamento do usuário na web	DNS sobre TLS/HTTPS

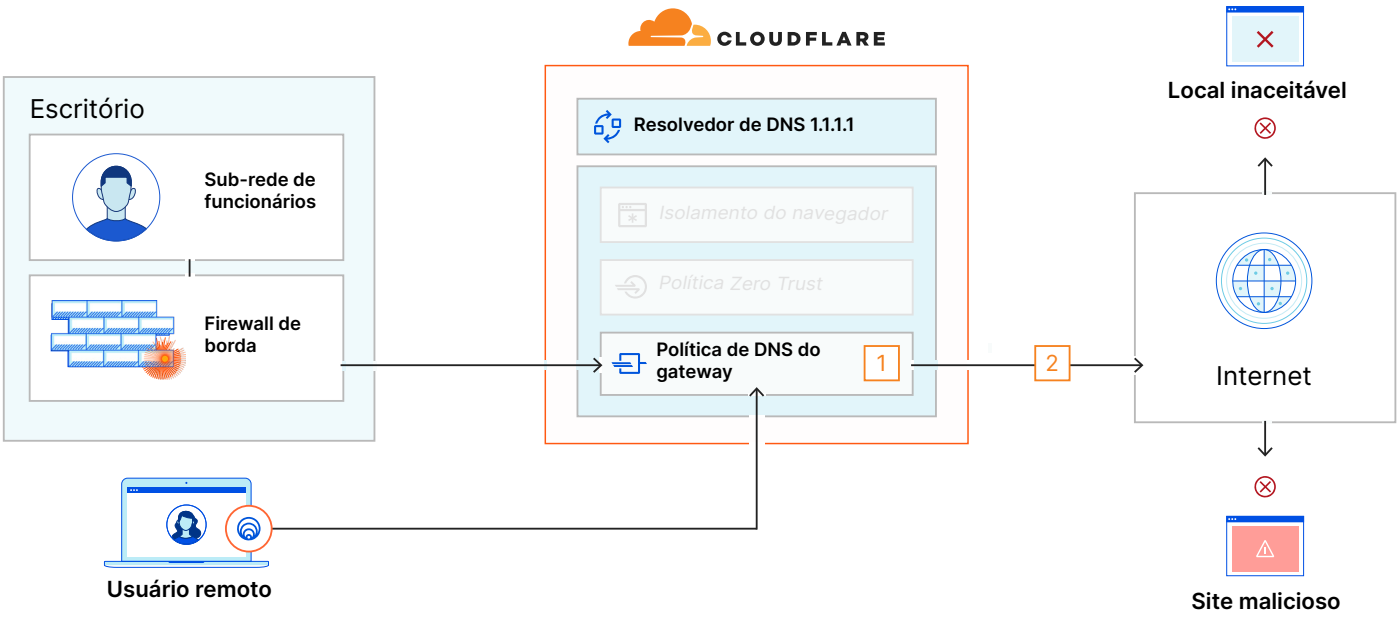
Design do Cloudflare One

As organizações que adotam o Cloudflare One direcionam seu tráfego para a Rede global da Cloudflare e podem realizar a filtragem de DNS para toda a força de trabalho sem se preocupar com os limites operacionais do hardware local.

O DNS filtrado da Cloudflare é fácil de implantar para usuários locais e remotos:

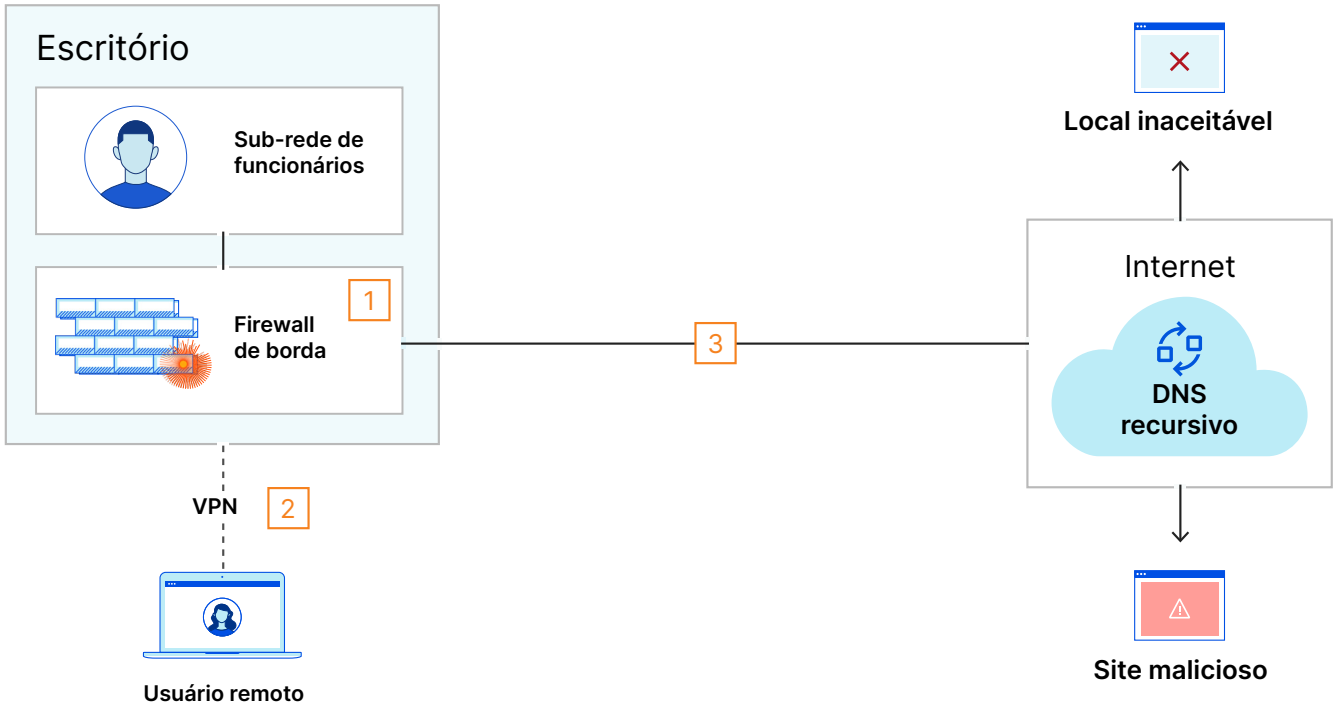
- O tráfego de usuários do escritório é enviado para a Cloudflare com base no IP de saída do firewall de borda
- O tráfego de usuários remotos é enviado para a Cloudflare a partir do cliente de dispositivo

Além disso, o resolvedor de DNS 1.1.1.1 da Cloudflare é compatível com o DNS sobre TLS/HTTPs, o que resolve o problema de segurança detalhado no ambiente legado.

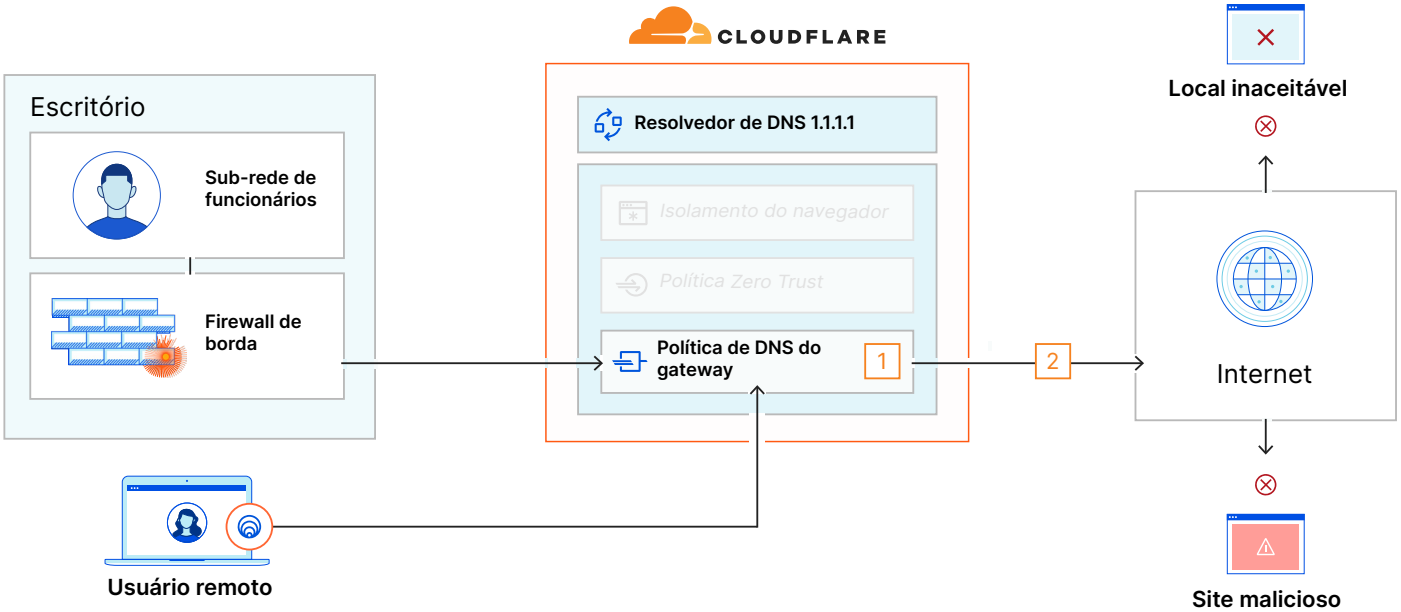


	Evento relacionado a DNS	Elemento relevante do Cloudflare One	Correção das falhas de design
1	Tanto os usuários locais quanto os remotos têm o conteúdo de suas solicitações de DNS filtrado pela Cloudflare	Gateway seguro da web	As políticas de DNS do gateway descarregam a filtragem de DNS do hardware local (ou a fornecem pela primeira vez)
2	As solicitações de DNS da organização são criptografadas antes de serem enviadas.	Resolvedor de DNS 1.1.1.1	O resolvedor de DNS 1.1.1.1 da Cloudflare é compatível com DNS sobre TLS/HTTPs, criptografando solicitações de DNS e dificultando o reconhecimento hostil

Design legado



Design do Cloudflare One



Design legado

	Evento relacionado a DNS	Elementos relevantes	Falha de design	Solução que não é da Cloudflare
1	Um usuário local tem seu conteúdo de solicitações de DNS filtrado para segurança pelo recurso integrado no firewall de borda	Firewall de borda	Confiar no Edge FW para muitas operações essenciais pode prejudicar a performance em toda a organização	Filtro de DNS discreto
2	Um usuário remoto tem suas solicitações de DNS filtradas após se conectar à VPN de túnel completo da organização	Concentrador de VPN Firewall de borda	Uma VPN de túnel completo cria uma "taxa dupla" de pacotes de internet, o que pode criar um gargalo de performance para todo o tráfego em túnel da organização	Aumentar a largura de banda do provedor Upgrade de hardware Ativar o túnel dividido*
3	As solicitações de DNS de saída são transmitidas sem problemas.	UDP53	O DNS na porta UDP 53 não é criptografado e, portanto, não é privado. Qualquer um que veja isso pode reconhecer o comportamento do usuário na web	DNS sobre TLS/HTTPS

Design do Cloudflare One

	Evento relacionado a DNS	Elemento relevante do Cloudflare One	Correção das falhas de design
1	Tanto os usuários locais quanto os remotos têm o conteúdo de suas solicitações de DNS filtrado pela Cloudflare	**Gateway seguro da web**	As políticas de DNS do **gateway** descarregam a filtragem de DNS do hardware local (ou a fornecem pela primeira vez)
2	As solicitações de DNS da organização são criptografadas antes de serem enviadas.	**Resolvedor de DNS 1.1.1.1**	O **resolvedor de DNS 1.1.1.1 da Cloudflare** é compatível com DNS sobre TLS/HTTPs, criptografando solicitações de DNS e dificultando o reconhecimento hostil