

# Proteger WiFi público e para visitantes com filtragem de DNS

Defender contra ameaças cibernéticas, aplicar o uso aceitável e otimizar as experiências dos usuários em todos os locais.

## A melhor proteção para WiFi da categoria

### Navegação mais segura, melhores experiências

Restrinja o acesso a conteúdos e atividades perigosos ou inapropriados na internet em redes WiFi de visitantes e públicas, com a filtragem de DNS do Cloudflare Gateway.

Proteja ambientes de varejo, de hotelaria, de educação, da área da saúde, de transporte e públicos para:

- **Impor políticas de uso aceitável** bloqueando conteúdo ofensivo ou ilegal
- **Proteger a reputação da rede e os espaços de trabalho de usuários visitantes** bloqueando phishing, ransomware e outros domínios maliciosos
- **Otimizar o desempenho da rede** bloqueando atividades que exigem muita largura de banda, como streaming
- **Melhorar as experiências dos visitantes** com acesso à internet seguro, rápido e confiável

Como um dos [maiores resolvedores de DNS autoritativos e recursivos do mundo](#), a Cloudflare está posicionada de forma única para impor proteções em escala global de maneira econômica.



**Companhia aérea global**

A Cloudflare complementa o serviço de internet de alta velocidade da Starlink para impor o uso aceitável para passageiros e tripulação



**Educação pública**

129 escolas secundárias na região de Seine-et-Marne, na França protegidas com a filtragem de DNS

[Ler o estudo de caso](#)



**Marca global de café**

Substituiu o Cisco Umbrella pela Cloudflare para proteger o WiFi de convidados em locais de varejo na América do Norte

## A diferença da Cloudflare



### Implantações simples e flexíveis

Filtre consultas de DNS por escritório, loja ou qualquer entidade física.

Direcione roteadores ou pontos de acesso para a Cloudflare para resolução de DNS upstream a fim de aplicar [políticas baseadas em localização](#), sem necessidade de software cliente.



### Velocidade e privacidade globais

Escale proteções consistentes em todos os lugares, apoiadas por uma rede global que abrange mais de 300 locais em mais de 125 países.

Construído em um dos resolvedores de DNS [mais rápidos \(1.1.1.1\)](#), projetado para garantir a [privacidade](#) sem retenção de IPs de origem.



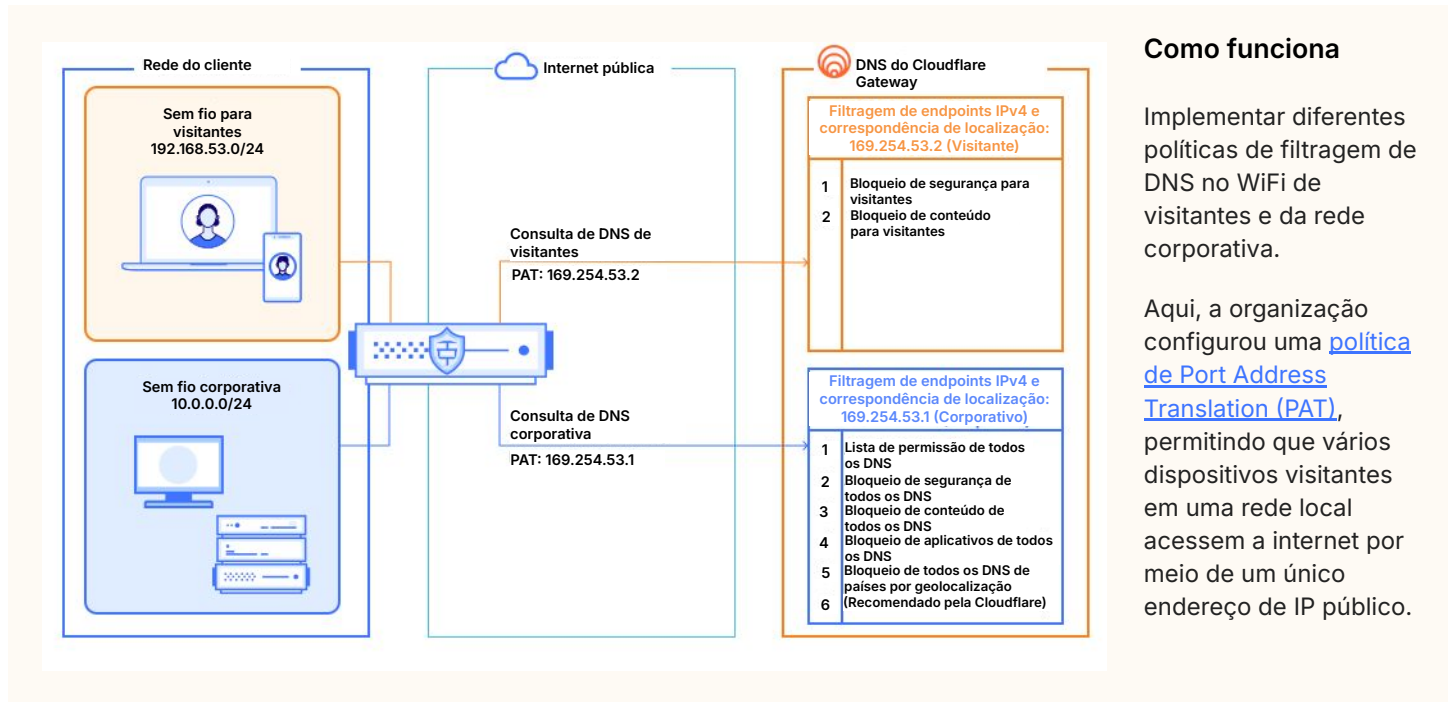
### Inteligência contra ameaças apoiada por IA

A Cloudflare resolve cerca de 49 milhões de consultas de DNS por segundo, ou mais de 4 trilhões de consultas por dia.

Essa visibilidade em tempo real de domínios recém-vistos e arriscados alimenta os modelos de caça a ameaças apoiados por IA/ML.

Quer se aprofundar nesse caso de uso? Analise nossa [arquitetura de referência](#), ou [solicite uma conversa](#).

## Proteção do tráfego da rede corporativa e rede de visitantes



## Exemplos de recursos

Defesa contra ameaças e acesso seguro	
<b>Categorias de segurança e aplicativos</b>	<a href="#">Cobertura abrangente</a> de ransomware, phishing, domínios DGA, tunelamento de DNS, domínios novos e recém-vistos, C2 e botnets e outros riscos de segurança. Cobertura do CASB in-line de 25 <a href="#">categorias de aplicativos</a> , incluindo IA.
<b>Filtragem de DNS recursivo</b>	<a href="#">Permitir ou bloquear</a> domínios e endereços de IP por categorias de segurança ou conteúdo e dentro de <a href="#">durações de tempo específicas</a> . Definir políticas de <a href="#">substituição</a> de DNS para redirecionar consultas para páginas de destino seguras, portais cativos, página de política de uso aceitável, sites pré-aprovados específicos e mais. Os filtros de DNS podem ser gerenciados por meio de nossa <a href="#">Tenant API</a> para configurabilidade pai-filho.
<b>Inteligência contra ameaças integrada</b>	A inteligência contra ameaças é baseada nos nossos próprios modelos de IA/ML e em feeds de terceiros. A inteligência primária é derivada da telemetria global como um dos maiores resolvers de DNS autoritativos e recursivos (mais de 4T de consultas/dia). <a href="#">Feeds de ameaças personalizados</a> e assinaturas (IPs, URLs e domínios, etc.) também são suportados.
Administração e capacidade de personalização	
<b>Via de acesso ao local:</b> Endereços IPv4 e IPv6	Usar os endereços <a href="#">IPv4 ou IPv6</a> do resolver de DNS que a Cloudflare atribui à sua conta. Clientes Enterprise podem solicitar <a href="#">IPs de resolvers de DNS dedicados</a> ou <a href="#">trazer seus próprios IPs de resolvers de DNS</a> .
<b>Via de acesso ao local:</b> Endpoints de DoH ou DoT	É atribuído um hostname exclusivo para <a href="#">DNS sobre HTTPS (DoH)</a> ou <a href="#">DNS sobre TLS (DoT)</a> para cada local de DNS. Este método criptografa o tráfego e reduz a dependência de IPs estáticos.
<b>Políticas de resolver</b>	Para clientes Enterprise, <a href="#">rotear e aplicar controles granulares</a> em consultas de DNS a partir das vias de acesso acima (por exemplo, roteamento de <a href="#">subdomínios específicos de DoH</a> para resolvers personalizados).
<b>IPs de saída dedicados e políticas de saída</b>	<a href="#">Faixa de IPs estáticos dedicada</a> (IPv4 ou IPv6) que pode ser usada para criar listas de permissões de tráfego com base no IP de origem. Usar <a href="#">políticas de saída</a> para selecionar qual IP de saída será usado, com base em atributos como identidade, geolocalização ou postura do dispositivo. Cada IP de saída é exclusivo de uma conta individual e não é usado por outros clientes.
<b>Automação</b>	<a href="#">APIs intuitivas</a> e <a href="#">provedor Terraform</a> disponíveis para gerenciar todos os serviços da Cloudflare de forma programática.