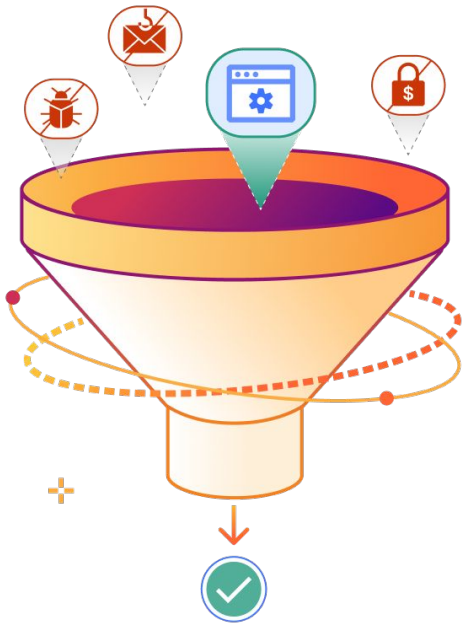
Gateway seguro da web (SWG)

O Cloudflare Gateway, um serviço combinável do Cloudflare One, protege usuários e dados contra ameaças cibernéticas com filtragem de internet com reconhecimento de identidade.



Defesa simples e moderna contra ameaças

Substitua a segurança da web legada complexa

As ameaças cibernéticas estão por toda parte e continuam a explorar as lacunas na crescente superfície de ataque de sua organização. Fazer malabarismos com várias soluções pontuais (como resolvedores de DNS, gateways da web e firewalls de rede) só aumenta o custo, a complexidade e o risco.

O Cloudflare Gateway simplifica a segurança com proteções consistentes e visibilidade para acesso à internet e a recursos internos. Reduza o risco cibernético com políticas com reconhecimento de identidade que ajudam sua organização a:

- **Deter as ameaças da internet** como ransomware, phishing, comando e controle e outras
- **Controlar e monitorar o tráfego das camadas 4 e 7** com regras de DNS, HTTP, rede e isolamento do navegador
- **Aplicar políticas de uso aceitável** para funcionários remotos e no escritório

Em uma arquitetura de passagem única, o tráfego é verificado, filtrado, inspecionado e isolado das ameaças.

SWG hoje, Serviços de segurança de borda (SSE) no futuro

A modernização dos controles SWG é uma etapa comum para consolidar a segurança com uma arquitetura SSE e adotar as práticas recomendadas de Zero Trust.

Descubra como pode ser essa jornada com a Cloudflare.

Por que a Cloudflare?

Segurança unificada

Uma rede

e plano de controle para todos os serviços de Serviços de segurança de borda (SSE), proteção de aplicativos web e APIs (WAAP), segurança de e-mails e outros domínios.

Inteligência contra ameaças em grande escala

2 trilhões

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

Criada para escalar

mais de 310

locais de rede em mais de 120 países. Todas as funções SWG e Zero Trust/SSE estão disponíveis para os clientes executarem em todos os locais, de modo que a aplicação seja sempre rápida e consistente.

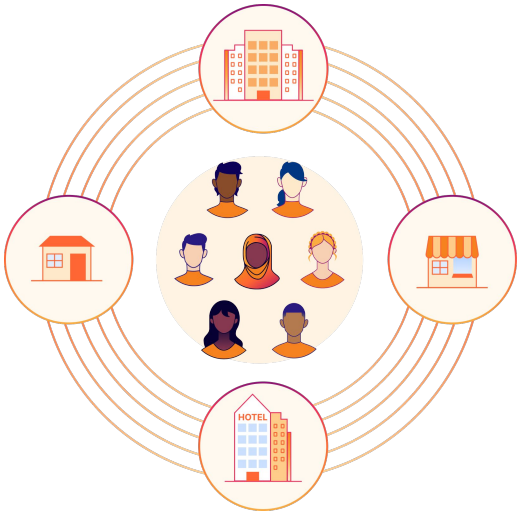
Caso de uso: defesa contra ameaças para trabalhadores remotos e locais de escritório

Problema

O trabalho híbrido expandiu sua superfície de ataque, e as lacunas de segurança decorrentes do gerenciamento de ferramentas distintas tornam mais fácil para ransomware, phishing e outras ameaças cibernéticas prejudicarem sua carteira e a reputação da marca.

Solução

O SWG da Cloudflare oferece segurança da web consistente para funcionários remotos e no escritório. A maioria das organizações começa com a filtragem de DNS para obter um tempo de retorno rápido, antes de realizar inspeções e controles mais abrangentes em toda a atividade na internet.



Comece a usar

Enviar tráfego para a rede da Cloudflare primeiro para resolução de DNS (e depois para inspeção HTTP completa)

Implementar filtragem de DNS por identidade/dispositivo para funcionários remotos ou por local para escritórios

Adicionar controles mais granulares, incluindo HTTP, rede e regras de isolamento do navegador.

Implantar segurança de e-mail em nuvem in-line como MX, via API ou ambas (multimodo)

Em primeiro lugar, navegação segura na web para usuários dentro e fora da rede

Em seguida, adicionar segurança de e-mail

Reduzir o risco e, ao mesmo tempo, melhorar a produtividade da equipe

Implantações simples e flexíveis

Usar roteadores de rede para a resolução de DNS. Enviar tráfego da camada 3 por meio de túneis GRE/IPsec, conector WAN ou SD-WAN existente.

Ou implantar nosso cliente de dispositivo para encaminhar o tráfego de proxy.

Proteção rápida e consistente

Inspeção de passagem única em toda a nossa rede para uma aplicação de políticas rápida e consistente em qualquer lugar.

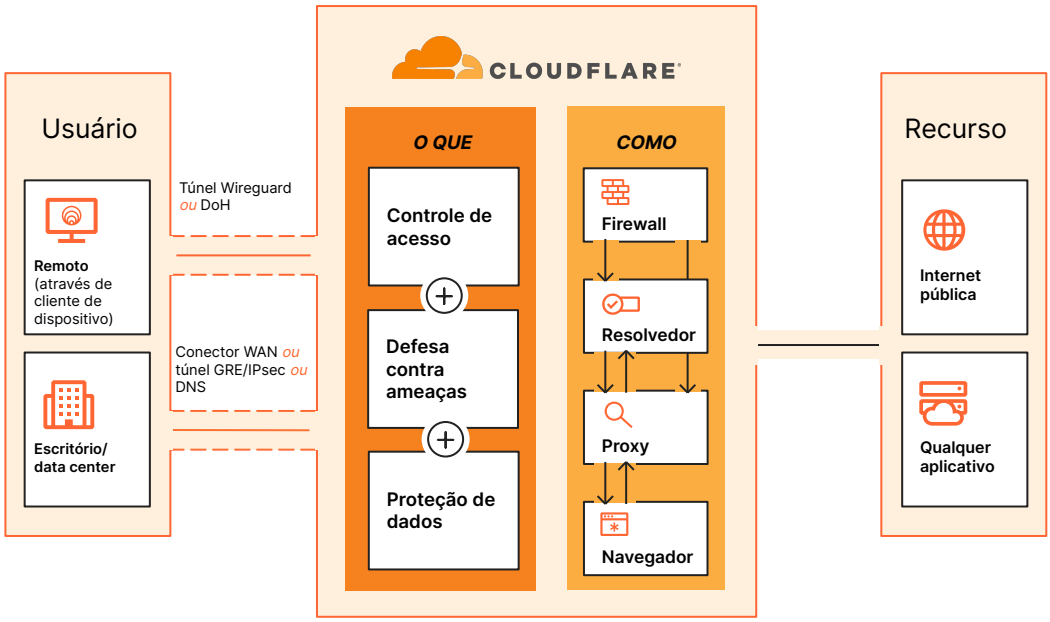
Comprovadamente mais rápida do que fornecedores como Zscaler, Netskope e Palo Alto Networks.

Acelerar a adoção do Zero Trust

Um plano de controle unificado com um gerenciador de políticas entre serviços SSE/SASE combináveis.

Comece com segurança na web e e-mail e aplique outros controles Zero Trust em seu próprio ritmo.

Como funciona o SWG



Simplifique a segurança.

Aplique controles de firewall, resolvedor, proxy e navegador ao tráfego de recursos internos e vinculados à internet.

Crie políticas a partir de um único gerenciador de políticas.

Adicionar controles SSE na sua base de SWG

Ao encaminhar o tráfego de proxy por meio do SWG da Cloudflare, sua organização pode ampliar ainda mais os controles de segurança e a visibilidade ao aproveitar os recursos em nossos serviços SSE combináveis e integrados nativamente.

Proteger a atividade na web e em aplicativos com o isolamento do navegador remoto

- Isolar os dispositivos locais de malware executando todo o código do navegador na rede global da Cloudflare com baixa latência.
- Isolar aplicativos para proteger os dados com verificações de DLP e controles do navegador (por exemplo, bloquear copiar e colar, restringir upload/download, impressão) com ou sem um cliente de dispositivo.

Proteger dados com DLP multimodo e CASB

- Evitar vazamentos de dados detectando e bloqueando dados confidenciais no tráfego HTTP(S) e arquivos com regras predefinidas (por exemplo, dados financeiros/de saúde) ou perfis personalizados (por exemplo, correspondência exata de dados).
- Verificar se há configurações incorretas em suítes SaaS com detecções DLP integradas para dados confidenciais e adotar medidas prescritivas para corrigir.

Ampliar as políticas de acesso com reconhecimento de identidade com o ZTNA

- Aplique regras Zero Trust que limitam o acesso a aplicativos corporativos auto-hospedados, aplicativos SaaS e IPs ou hostnames de redes privadas.
- Integrar provedores de proteção de identidade e endpoints uma única vez e aplicar verificações de postura na internet e em regras de acesso a aplicativos usando o mesmo criador de regras.

Aumento da visibilidade

- Manter logs de auditoria detalhados em dispositivos gerenciados e não gerenciados (no plano contratual, os logs de DNS são armazenados por 6 meses e os logs de HTTP e de rede por 30 dias).
- Fazer logpush para seu SIEM preferido para correlação e análise adicional.

Recursos do gateway

Defesa contra ameaças e acesso seguro	
Categorias de segurança e de aplicativos	Cobertura abrangente de ransomware, phishing, domínios DGA, tunelamento de DNS , domínios novos e recém-vistos, C2 e botnet e outros riscos de segurança. Cobertura do CASB in-line de 25 categorias de aplicativos, incluindo IA.
Filtragem de DNS recursivo	Permitir/bloquear/substituir domínios e endereços de IP por categorias de segurança ou de conteúdo. A filtragem de DNS pode ser gerenciada por meio de nossa Tenant API para configurabilidade de pai-filho.
Filtragem e inspeção de HTTP(S)	Controlar o tráfego com base na origem, no destino, em domínios, em métodos HTTP, em URLs e em muito mais. A inspeção HTTP1/2/3 permite verificações AV e DLP , controles de arquivos, postura do dispositivo, locatários, isolamento do navegador remoto e muito mais.
Inspeção TLS 1.3 ilimitada	Inspeção ilimitada de TLS 1.3 por padrão. Todo o tráfego HTTPS é descriptografado, as políticas são aplicadas e as solicitações são recriptografadas com nosso certificado ou seu certificado personalizado, tudo com baixa latência líder de mercado. Padrões de DNS sobre TLS (DoT) e DNS sobre HTTP (DoH) compatíveis. Habilitar apenas conjuntos de cifras compatíveis com FIPS 140-2.
FWaaS na camada 4	As políticas de rede na camada 4 se aplicam a todos os pacotes TCP/UDP públicos/privados, controlando o acesso a recursos não HTTP por protocolo detectado, geolocalização, domínio SNI e muito mais. Auditar o tráfego SSH na porta 22. (Recursos de FWaaS na camada 3 integrados aos serviços de rede WAN).
Inspeção antivírus	Examinar uploads/downloads de arquivos de todos os tipos (PDFs, ZIP, RAR etc.) em busca de vírus.
Verificações de identidade e postura do dispositivo	Definir políticas com base em todos os principais provedores de identidade corporativa, identidades sociais ou padrões SAML e OIDC. Verificar a postura do dispositivo por meio do cliente do dispositivo ou de seu provedor de proteção de endpoints de terceiros.
Inteligência contra ameaças integrada	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 resolvedores de DNS autoritativos e recursivos (mais de 2T de consultas/dia). Nosso web crawler também indexa toda a web (mais de 8 bilhões de páginas) a cada poucas semanas para descobrir infraestrutura de campanhas emergentes. Feeds e assinaturas de ameaças personalizadas (IPs, URLs e domínios, etc.) também são suportados.
Acessos de entrada e saída	
Com cliente de dispositivo	Encaminhar o tráfego proxy por meio de nosso cliente de dispositivo (WARP) através de túneis WireGuard completos ou DoH. Autocadastramento ou implantação via MDM. Permitir verificações de postura do dispositivo. Detectar se o dispositivo está na rede.
Opções sem cliente	As opções incluem: consultas de DNS roteadas na rede a partir de locais do cliente, Túneis Anycast GRE/IPsec, conector WAN, endpoints de proxy por meio de arquivos PAC e isolamento da web sem cliente por meio de um URL reescrito.
Compatibilidade com IPv4 e IPv6	Todas as funcionalidades disponíveis para conectividade IPv4 e IPv6 (seja apenas IP6 ou pilha dupla).
Roteamento de tráfego	
IPs de saída dedicados e políticas de saída	Faixa de IPs estáticos dedicada (IPv4 ou IPv6) que pode ser usada para criar lista de permissões de tráfego com base no IP de origem. Usar políticas de saída 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.
Políticas de resolvedores	Encaminhar as solicitações de DNS para resolvedores de DNS personalizados de modo a alcançar domínios que não podem ser roteados publicamente, como serviços de rede privada e aplicativos internos. (Por padrão, as solicitações de DNS usam o resolvedor de DNS público da própria Cloudflare , o 1.1.1.1, um dos mais rápidos e mais confiáveis do mundo).
Tunelamento dividido	Excluir/incluir endereços de IP ou domínios para redes privadas ou em execução junto com uma VPN.
Visibilidade e extensibilidade	
Registro	Registro abrangente para todas as consultas de DNS, pacotes de rede da camada 4 e solicitações HTTP inspecionados em qualquer porta. Usar logpush ou API para integração com ferramentas de SIEM, orquestração e análise existentes. Os administradores podem optar por excluir e/ou editar a coleta de informações de identificação pessoal entre os usuários.
Detecção de TI Invisível	Rastrear, analisar e aprovar origens de SaaS e de redes privadas que seus usuários finais visitam por meio do CASB in-line.
Personalização de página	Fazer upload de páginas de bloqueio HTTP personalizadas para se adequar à sua marca ou transmitir instruções para uma melhor experiência do usuário.
Automação	APIs intuitivas e provedor Terraform disponíveis para gerenciar programaticamente todos os aspectos de uma implementação Zero Trust. Também oferece suporte a token de serviço sem usuário para serviços automatizados.

Como os clientes utilizam nosso SWG

A Cloudflare e a Accenture protegem o acesso à internet para a Agência de Segurança Cibernética e de Infraestrutura (CISA) dos EUA

+ de 100 **Agências civis dos EUA**
com escritórios protegidos pela filtragem de DNS da Cloudflare
Saiba mais

bouvet

Consultoria escandinava de TI e comunicações digitais

"Dependemos da Cloudflare para reduzir nossa superfície de ataque, protegendo nossas portas, filtrando ameaças e limpando nosso tráfego."

— Victor Persson, Security Operations Lead
Leia o estudo de caso

classmethod

Integrador e consultoria de nuvem do Japão

4 mil **solicitações bloqueadas por semana**
de conteúdo prejudicial e indesejado na internet entre centenas de funcionários
Leia o estudo de caso

Exemplo de comparação competitiva com a Zscaler

Critérios	Cloudflare Gateway	Acesso à internet da Zscaler
Arquitetura	Uma plataforma em nuvem, um único plano de controle	Nuvem fragmentada, Muitos planos de controle
Interface de gerenciamento	Uma interface para todos os serviços	Separado para SWG e ZTNA
Inspeção de passagem única	SIM para todos os serviços SSE	NÃO
Compatível apenas com IPv6	SIM	NÃO
SLA de tempo de atividade	100% para todos os serviços	99,999% para a maioria dos serviços 99,9% para o resolvedor de DNS

Continue comparando Cloudflare e Zscaler

Proteção mais rápida

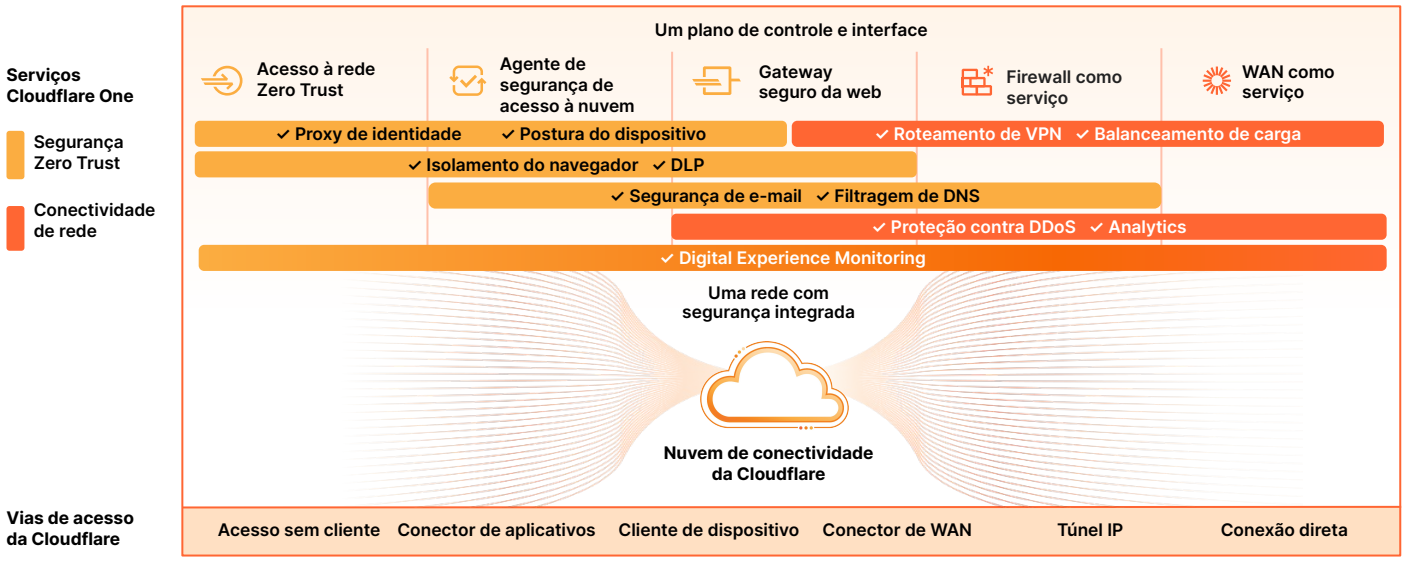
13-58%
mais rápida para gateway seguro da web (SWG)

45-64%
mais rápida para isolamento do navegador remoto

Com base em testes primários e testes de terceiros

Modernizar a segurança com a plataforma SSE da Cloudflare

O Cloudflare Gateway é um serviço combinável dentro do Cloudflare One, nossa plataforma SSE. Crie a partir de sua base SWG e amplie a visibilidade e os controles com os recursos de segurança interoperáveis do Cloudflare One em ambientes web, SaaS e de aplicativos privados.



Uma plataforma unificada

- **Acesso seguro** ao verificar e segmentar qualquer usuário para qualquer recurso
- **Defesa contra ameaças** ao cobrir todos os canais com IA/ML alimentados por rede e inteligência contra ameaças
- **Proteção de dados** ao aumentar a visibilidade e o controle dos dados em trânsito, em repouso e em uso

Uma rede programável

- **Mais eficaz** ao simplificar a conectividade e o gerenciamento de políticas
- **Mais produtivo** ao garantir UX rápida, confiável e consistente em todos os lugares
- **Mais ágil** ao inovar rapidamente para atender aos seus requisitos de segurança em constante evolução

Ainda não está pronto para uma conversa ao vivo?

Continue aprendendo mais sobre nossa arquitetura de referência SASE, ou veja como ela funciona em um tour interativo de nossa plataforma Zero Trust.