CLOUDFLARE

ARTIGO TÉCNICO

# Entender o papel da proteção de rede fornecida pela nuvem

# Conteúdo

# Entender o papel da proteção de rede fornecida pela nuvem

Toda organização tem infraestrutura de rede voltada para o público. Essa infraestrutura hospeda vários aplicativos, incluindo aqueles que dão suporte a funcionários, clientes e parceiros de negócios. Ela pode incluir serviços de gateway que fornecem conectividade de rede, como VPNs, servidores de desktop virtual ou jump servers. Essa infraestrutura também fornece serviços críticos de TI e rede, como e-mail, servidores de arquivo, DNS, acesso remoto e comunicações como VoIP.

A infraestrutura voltada para o público é um desafio para proteger, pois é acessível a qualquer pessoa na internet. Como consequência, ela é vulnerável a vários vetores de ameaças diferentes. Por exemplo, os invasores podem explorar a infraestrutura para inventariar aplicativos e serviços detectáveis. Se os invasores encontrarem uma vulnerabilidade no sistema operacional, no dispositivo ou no software no futuro, eles poderão tirar vantagem da janela explorável antes que uma correção seja desenvolvida ou instalada.

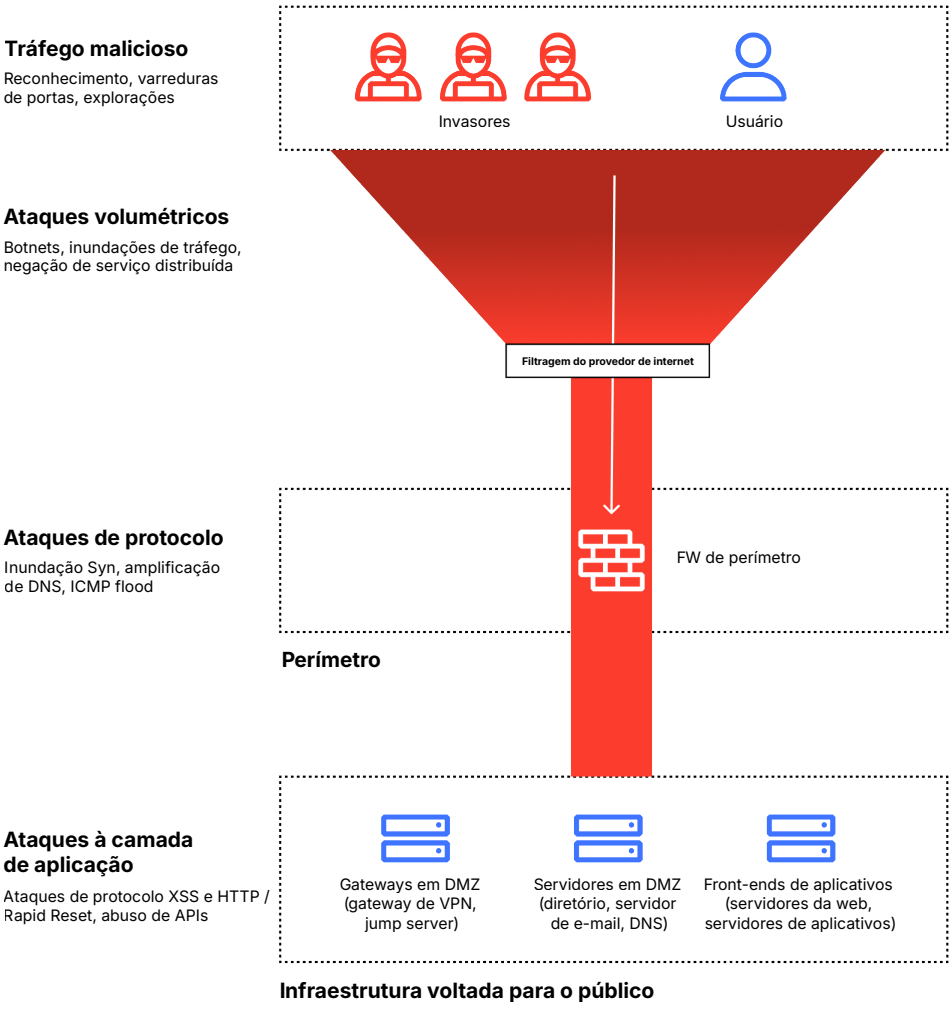
Os ataques também podem assumir outras formas. Por exemplo, ataques de negação de serviço distribuída (DDoS) são uma ameaça de longa data à infraestrutura voltada para o público que pode causar diretamente perdas financeiras e danos à marca. Esses ataques podem facilmente sobrecarregar o limite das proteções convencionais, e as equipes de segurança ficam sabendo dos problemas somente depois que o ataque já está em andamento.

Em decorrência desses desafios de rede, as organizações implantam uma longa lista de auxiliares de firewall, como dispositivos de rede adicionais, e serviços de filtragem. As funcionalidades adicionais têm um custo, pois muitas tornam a rede ineficiente, e as proteções ainda são ineficazes contra a crescente sofisticação do cenário de ameaças.

Firewalls de rede convencionais, juntamente com vários auxiliares de firewall, simplesmente não são suficientes. O momento para a mudança de arquitetura é agora, mas o caminho para a mudança nem sempre é claro. Neste artigo, ilustramos os tipos de ataques que são empregados contra a infraestrutura voltada para o público, destacamos os problemas que as organizações enfrentam e defendemos a implementação de proteções fornecidas em nuvem por meio de uma nuvem de conectividade.

# Desafios na proteção da infraestrutura voltada para o público

As equipes de segurança e rede usam firewalls de rede para estabelecer a demarcação entre a rede confiável (interna), a rede voltada para o público ou zona desmilitarizada (DMZ) e a internet. Essa é uma função perfeitamente válida para um firewall.  No entanto, a infraestrutura voltada para o público está sujeita a uma série de ataques que não podem ser detidos por firewalls.




Uma arquitetura de rede tradicional voltada para o público.

**DDoS:** os firewalls fornecem recursos de filtragem, e muitos fornecem proteção contra tipos de ataques DDoS. No entanto, os firewalls nem sempre podem proteger contra variantes em técnicas de DDoS. Como resultado, a eficácia de suas proteções integradas deixa muito a desejar em relação ao que é necessário hoje.

**Ataques DDoS volumétricos:** ataques volumétricos (às vezes chamados de ataques DDoS à camada 3) distribuem uma quantidade enorme de tráfego para processar, medido em gigabits por segundo (Gbps). Para distribuir esse tráfego, esses ataques normalmente usam botnets com a assistência de uma vulnerabilidade de amplificação. Com tráfego suficiente, um ataque volumétrico satura a linha e sobrecarrega a interface do firewall. Para lidar com essas ameaças, as organizações empregam um auxiliar de firewall, como filtragem upstream com centros de depuração de tráfego ou filtragem do provedor de internet. Mas ambos apresentam seus próprios conjuntos de problemas, como latência adicional. A filtragem do provedor de internet também tem limites acima do que pode processar, o que significa que ela descarta o que não pode lidar e bloqueia o acesso a usuários legítimos.

**Ataques DDoS de protocolo:** ataques DDoS baseados em protocolo (às vezes chamados de ataques DDoS nas camadas 3 e 4) tentam sobrecarregar o número de sessões por meio de técnicas como inundações SYN. Os ataques de protocolo são medidos em tamanho por pacotes por segundo (pps). Os firewalls modernos têm a capacidade de reconhecer um ataque de protocolo, mas os firewalls só podem descartar ataques de protocolo se tiverem recursos suficientes para reconhecer, analisar e descartar o ataque que já está em andamento. Os fornecedores de firewall às vezes usam esses recursos para dar suporte às suas alegações de que oferecem proteção contra DDoS, sem esclarecer que os ataques de protocolo ainda podem sobrecarregar o firewall e não são claros em relação a outros tipos de ataques DDoS que não podem impedir. Para resolver as deficiências de um firewall, as organizações às vezes empregam centros de depuração ou filtragem do provedor de internet como auxiliares para descartar o tráfego upstream do firewall.

**Ataques DDoS à camada de aplicação:** os ataques DDoS à camada de aplicação (às vezes chamados de ataques DDoS à camada 7) diferem dos ataques volumétricos e baseados em protocolo, pois usam a comunicação com os protocolos da camada de aplicação para causar a negação de serviço. Como tal, eles são medidos em solicitações por segundo (rps). Como esse tipo de ataque opera na camada de aplicação, ele pode ter sucesso usando um número menor de hosts. Os firewalls (mesmo firewalls com inspeção de camada 7) não entendem a interação entre um host e um servidor e, portanto, exigem outro conjunto de auxiliares de firewall, como o firewall de aplicativos web (WAF) e os dispositivos contra DDoS projetados para filtrar ameaças de interação com a infraestrutura voltada para o público.

**Exploração de interfaces HTTP:** tanto os aplicativos quanto a infraestrutura de rede frequentemente fornecem interfaces na web. Por exemplo, um dispositivo VPN tem interfaces na web para funções como VPN sem cliente, que está exposta publicamente. Esses aplicativos estão sujeitos a ataques pré-autenticados que exploram uma vulnerabilidade e, portanto, as organizações devem empregar proteções para filtrar e bloquear o abuso de aplicativos.

**Escalar proteções de firewall:** os firewalls têm capacidade finita e não são elásticos. Quando as organizações compram um firewall, elas devem comprar um modelo com capacidade suficiente. Sua capacidade de escalar as proteções de firewall é limitada por essa decisão de compra. A escala costuma ser um problema porque a decisão mais econômica é comprar apenas a capacidade necessária. Mas quando as organizações compram capacidade insuficiente para a vida útil do firewall, elas podem não conseguir operar proteções computacionalmente pesadas, como a descriptografia TLS. É caro comprar capacidade adicional para lidar com volumes de tráfego atípicos. Portanto, a capacidade é quase sempre um desafio: não há cenário que seja perfeito e muitos estão abaixo do ideal.

| | | | Controles de auxiliares de firewall | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Tipos de ataques** | **Exemplos** | **Firewall** | **IP S/IDS** | **WAF** | **Segurança de APIs** | **Dispositivo contra DDoS** | **Filtragem do provedor de internet** | **Centro de depuração** |
| **Tráfego malicioso** | Reconhecimento, varreduras de portas, explorações | ✔ | ✔ | | | | | |
| **Ataques DDoS volumétricos (Camada 3)** | Botnets, inundações de tráfego, negação de serviço distribuída | | | | | | ✔ | ✔ |
| **Ataques DDoS de protocolo (Camadas 3/4)** | Inundação Syn, amplificação de DNS, ICMP flood | ✔ | | | | | ✔ | ✔ |
| **Ataques à camada de aplicação** | Abuso de aplicativos: XSS, bots, injeção de SQL | | | ✔ | | | | |
| | DDoS na camada de aplicação (camada 7): ataques de protocolo HTTP/Rapid Reset | | | | | ✔ | | |
| | Abuso de APIs: exploração de vulnerabilidades, MITM, preenchimento de credenciais | | | | ✔ | | | ✔ |

As organizações usam “controles auxiliares” para abordar funcionalidades que os firewalls não executam.

# O problema com os auxiliares de firewall

Para fornecer proteções suplementares, as organizações empregam uma série de auxiliares de firewall, como proteções específicas da camada de aplicação (incluindo WAF e filtragem de DDoS), centros de depuração e filtragem do provedor de internet. Essas proteções existem em grande parte porque as necessidades da organização vão além do que seu firewall pode fazer e, além disso, as proteções introduzem problemas por si mesmas.

**Dispositivos adicionais no local:** no passado, a única maneira de adicionar mais proteção de rede era adicionar mais dispositivos na rede. Inserir um dispositivo na rede não é uma questão simples, pois a rede efetivamente precisa ser reprojetada para cada novo recurso que a organização precisa. A inserção de dispositivos para proteções in-line causa tempo de inatividade da rede, redundância e a disputa entre o tempo de atividade da rede e a exposição ao risco de segurança ao decidir entre falha fechada ou falha aberta.

**Centros de depuração:** um centro de depuração promete filtrar o tráfego antes que ele chegue à organização. No entanto, o desvio de tráfego por meio de um centro de depuração introduz um impacto no desempenho, já que a localização do centro de depuração de um fornecedor provavelmente não corresponde 1:1 à infraestrutura de destino do cliente. Nos piores casos, pode levar a ineficiências como o "efeito trombone", que faz com que o tráfego tome um caminho indesejável e danifica a experiência geral do usuário. Na verdade, a arquitetura dos centros de depuração amplifica as diferenças filosóficas entre segurança e rede, pois a proteção tem um custo para os caminhos de rede ideais.

**Filtragem do provedor de internet:** a filtragem do provedor de internet promete fornecer um caminho de rede mais eficiente para filtragem upstream do que um centro de depuração. Isso porque o provedor de internet fica na frente da infraestrutura voltada para o público da organização. No entanto, embora a filtragem do provedor de internet forneça mais capacidade do que o firewall da organização, a filtragem do provedor de internet tem suas próprias limitações. Os provedores de internet absorvem todo o tráfego do ataque, o que torna o filtro altamente vulnerável aos limites superiores de ataques volumétricos e de protocolo. O pior é que a filtragem do provedor de internet apenas observa tipos específicos de ataques e, portanto, requer outro auxiliar de firewall para atender às necessidades não atendidas.

# Definir requisitos para a mudança de arquitetura

A essência do problema é que é extremamente difícil e caro absorver um ataque dinâmico com recursos estáticos. Além disso, dar suporte ao firewall com auxiliares cria seus próprios problemas de arquitetura e gerenciamento.  O que é necessário é uma arquitetura que possa abordar as necessidades funcionais e a escala global do cenário de ameaças com proteção dinâmica.

A nuvem fornece um modelo para computação e rede elásticas, mas nem todas as nuvens são iguais.  Uma rede em nuvem projetada para fornecer segurança dentro da rede é necessária. O caminho a seguir é uma “nuvem de conectividade”, capaz de fornecer uma rede global para conectar qualquer usuário ou escritório a qualquer aplicativo. Uma nuvem de conectividade também pode fornecer um conjunto de serviços combináveis projetados para reconhecer e neutralizar as atividades de ameaças.

Para abordar as proteções de rede, os serviços de segurança necessários devem incluir:

**Cobertura global:** com a base de clientes aumentando e um número crescente de trabalhadores híbridos, as empresas devem ser capazes de fornecer proteções em geografias cada vez maiores. Como tal, há pressões para fornecer uma cobertura mais ampla do que o que é convencionalmente viável com uma estratégia no local.

**Serviços de firewall de perímetro:** para proteger a infraestrutura voltada para o público, uma nuvem de conectividade deve fornecer serviços de firewall de perímetro projetados para impor inspeções de tráfego de entrada e aplicação de políticas.

**Proteções contra DDoS:** a nuvem de conectividade também deve oferecer proteções de passagem única contra ataques DDoS volumétricos, de protocolo e à camada de aplicação. Qualquer modelo diferente da aplicação de passagem única introduz latência indesejada.

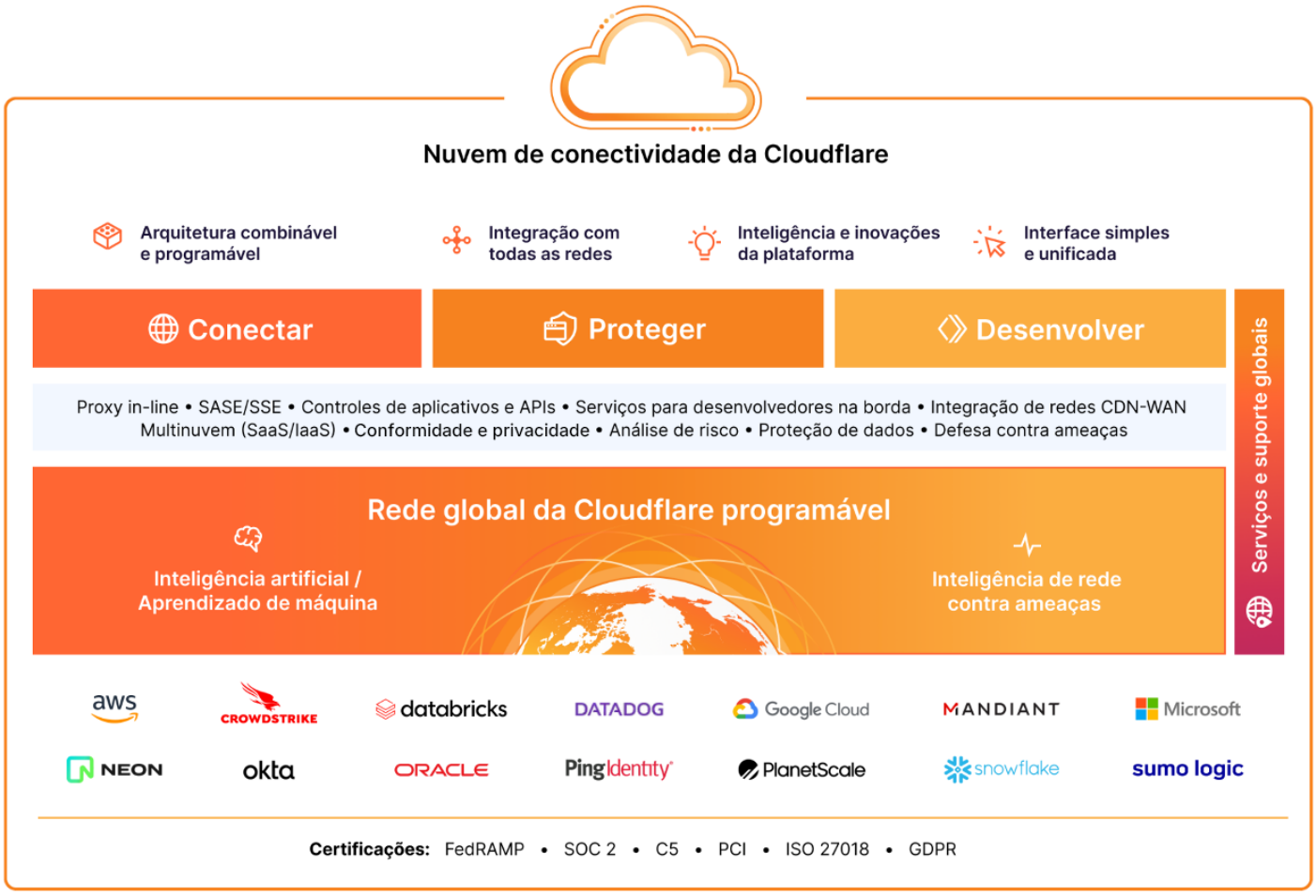
**Observabilidade:** a nuvem de conectividade deve fornecer visibilidade sobre o estado atual, comportamento e desempenho da rede, o que permite melhor solução de problemas, análise e otimização.

# Nuvem de conectividade da Cloudflare

A nuvem de conectividade da Cloudflare pode ajudar as organizações a modernizar suas redes e proteger melhor a infraestrutura voltada para o público. Construída em uma arquitetura programável e combinável, ela fornece serviços de rede e segurança em toda a infraestrutura e aplicativos empresariais habilitados para a nuvem. Como resultado, a nuvem de conectividade pode atender às necessidades atuais e futuras em sua jornada de modernização.

Com a Cloudflare, sua organização pode facilmente adicionar funcionalidades e dar suporte a novos casos de uso habilitando serviços em vez de inserir dispositivos. Com uma conexão a um data center Anycast da Cloudflare, você pode configurar e implantar serviços a partir da interface de gerenciamento unificada para processar o tráfego. Você pode atender às necessidades atuais e, ao mesmo tempo, implementar uma plataforma para acomodar casos de uso futuros e dar suporte a toda a sua jornada de modernização de rede.

Em vez de construir uma infraestrutura global, você pode se beneficiar do desempenho extremamente rápido da rede global da Cloudflare. Com conexões diretas com quase todos os provedores de serviços e provedores de nuvem, a rede da Cloudflare está a 50 ms de 95% da população mundial conectada à internet.




A nuvem de conectividade da Cloudflare pode ajudar organizações a se conectar, proteger e desenvolver em qualquer lugar.

# Como a Cloudflare oferece proteção de rede

A Cloudflare usa uma combinação de serviços de nuvem de conectividade para fornecer proteção de rede. Para proteger a infraestrutura voltada para o público, a nuvem de conectividade combina serviços em locais de rede ao redor do mundo.

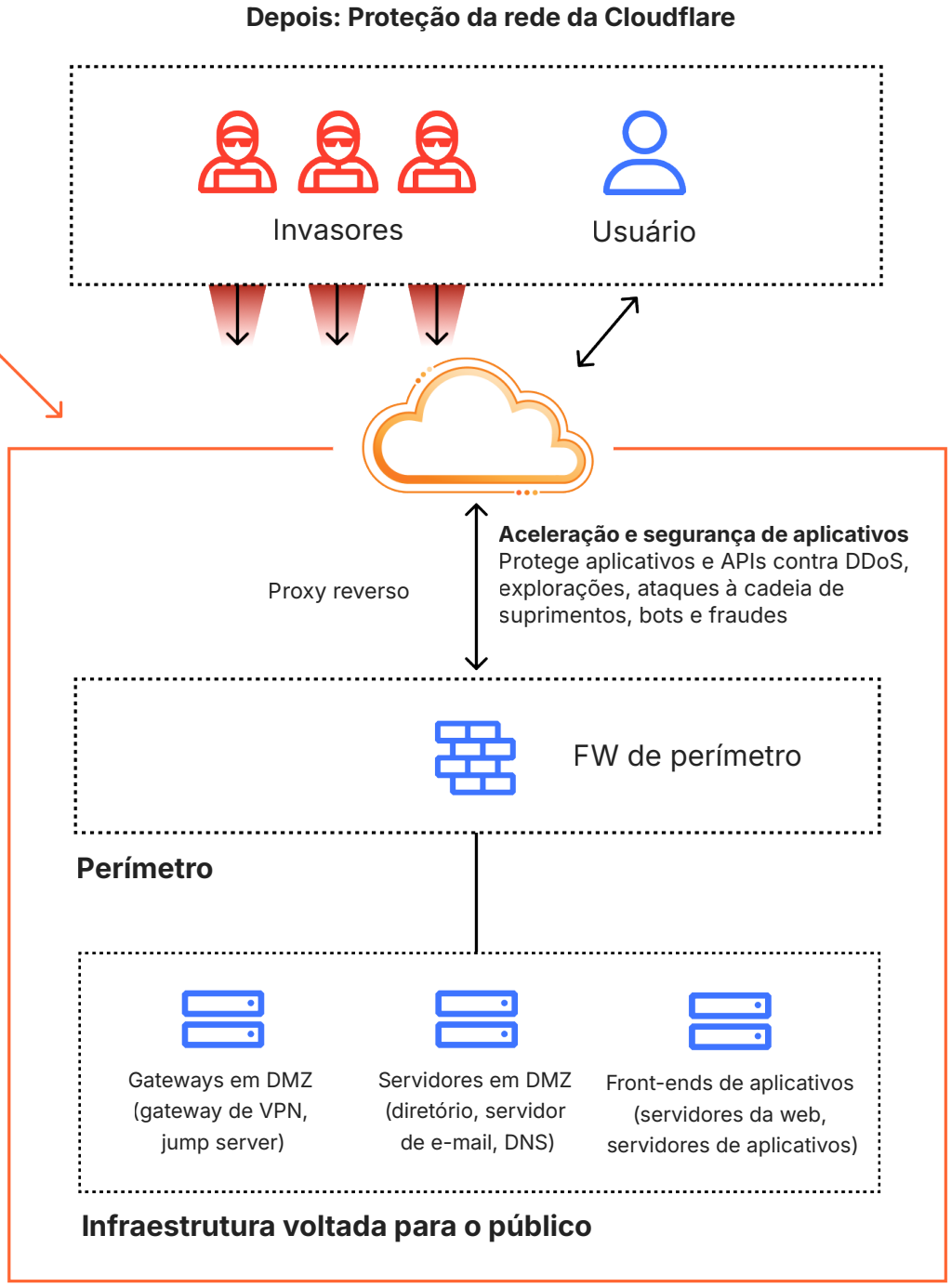
## Nuvem de conectividade da Cloudflare

**Ataques volumétricos**

- Absorve ataques volumétricos, difundindo o tráfego pela rede da Cloudflare

**Proteção de rede**

- Aplicação de firewall com atualizações de políticas globais em segundos
- Filtragem de DDoS para ataques volumétricose de protocolo




A nuvem de conectividade da Cloudflare oferece um novo modelo para proteger a infraestrutura voltada para o público.

Para fornecer proteções in-line, todo o tráfego de entrada para a infraestrutura voltada para o público passa primeiro por um data center da Cloudflare. A Cloudflare oferece diversas maneiras de se conectar à rede da Cloudflare. Um dos conceitos subjacentes por trás de muitos métodos de direcionamento de tráfego é um conceito chamado Anycast. A rede Anycast da Cloudflare (que cobre mais de 330 cidades e continua crescendo) atua como a porta de entrada para a infraestrutura voltada para o público de uma organização.

Todos os data centers da Cloudflare operam em grande escala com recursos de computação intercambiáveis. Esses data centers operam muito acima da capacidade que qualquer organização poderia construir sozinha. Com a rede Anycast, toda essa capacidade é amplificada, porque todos os data centers da Cloudflare ajudam a filtrar e difundir ataques.

Considere, por exemplo, como as botnets distribuem tráfego malicioso.  As botnets usam números gigantescos de hosts distribuídos e comprometidos para gerar quantidades avassaladoras de tráfego, pacotes ou solicitações. O tráfego visa o mesmo destino. Com a rede Anycast, os participantes da botnet veem o data center da Cloudflare mais próximo que está no caminho em direção à infraestrutura voltada para o público de sua vítima pretendida. A escala da rede da Cloudflare “espalha” o volume de tráfego enquanto aplica simultaneamente proteção contra DDoS nas camadas 3, 4 e 7. Na verdade, a Cloudflare usa a resiliência da rede distribuída como uma contramedida contra um ataque.

O Cloudflare Magic Firewall fornece a linha de frente de inspeções que ajudam as organizações a definir o que é ou não permitido. Ele remove o lixo que sua infraestrutura existente não precisa processar, usando recursos elásticos para liberar os recursos estáticos limitados do firewall no local para outras funções. Ele ajuda as organizações a usar uma estratégia de defesa em profundidade para desbloquear com eficiência um valor que, de outra forma, não seria obtido devido à alta utilização do firewall no local.

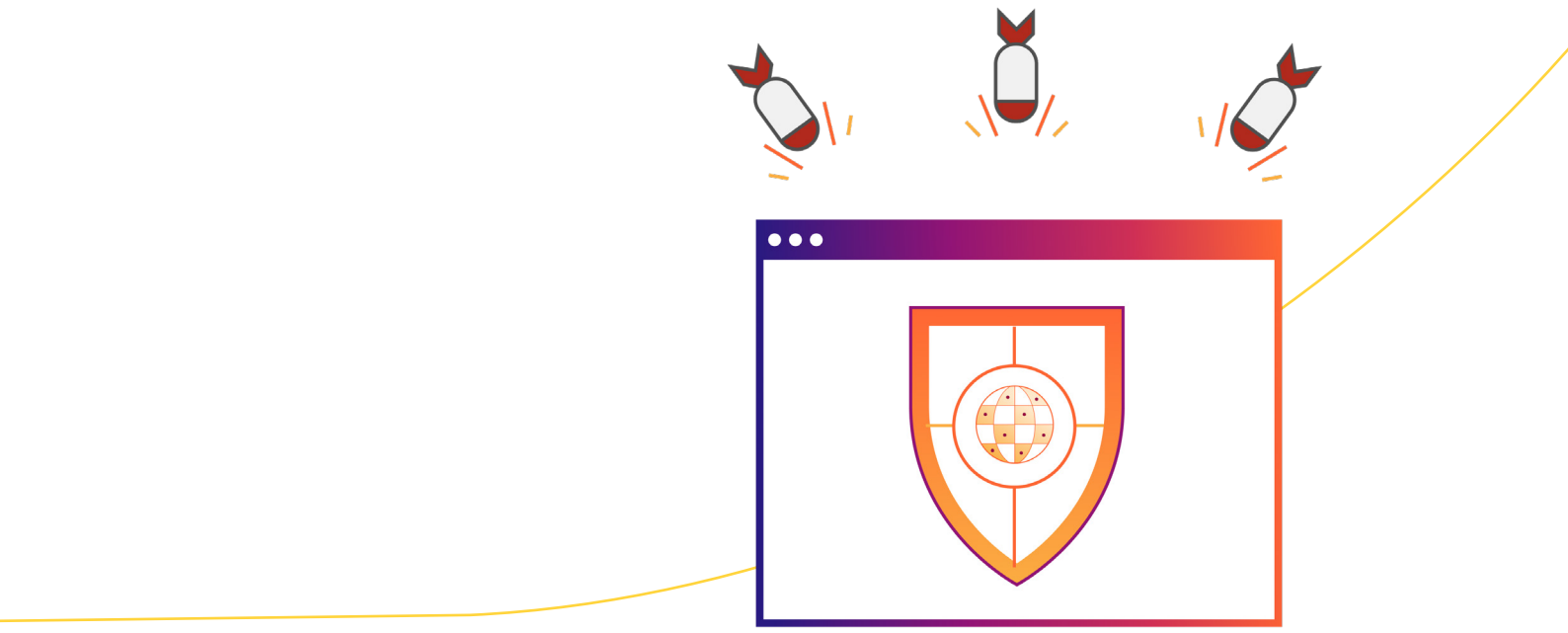
Como os ataques DDoS afetam diferentes camadas, as organizações devem implementar proteções em cada uma delas. A nuvem de conectividade da Cloudflare fornece proteções multicamadas por meio dos seguintes serviços:

- **Cloudflare Magic Transit:** oferece proteção contra DDoS contra ataques volumétricos na camada 3.
- **Cloudflare Spectrum:** fornece proteção contra DDoS contra ataques baseados em protocolo nas camadas 3 e 4.
- **Cloudflare DDoS:** protege contra ataques DDoS à camada de aplicação na camada 7.

Essas proteções funcionam juntas e são todas distribuídas e gerenciadas a partir do mesmo plano de controle da Cloudflare.  Elas eliminam a necessidade de auxiliares de firewall e complementam a estratégia de defesa em profundidade de uma organização, ajudando a garantir que as operações possam ser mantidas diante do cenário de ameaças atual.

A nuvem de conectividade da Cloudflare também fornece uma série de serviços adicionais para operar a infraestrutura voltada para o público, como:

- **Cloudflare Network Interconnect** para conectar diretamente sua infraestrutura voltada para o público à rede da Cloudflare. Pense na Cloudflare como a entrada e a saída para o seu tráfego.
- **Aceleração de aplicativos** para otimizar o desempenho da distribuição de seus aplicativos.
- **Segurança de aplicativos** para implementar proteções como um firewall de aplicativos web (WAF) para o tráfego que passa pela Cloudflare.



# Próximas etapas

Essa arquitetura de defesa em profundidade usando a nuvem de conectividade da Cloudflare é fácil de implantar, muito mais fácil do que as etapas operacionais para inserção de dispositivos tradicionais. Depois de estabelecer o caminho do tráfego para a Cloudflare, as proteções podem ser habilitadas com políticas implantadas globalmente em minutos.

Para saber mais sobre o Magic Transit, visite a arquitetura de referência.

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

REV:BDES-6349.2024AUG30