Aplique o DNS do Umbrella e evite o desvio com regras de firewall

Contents

Introdução

Este documento descreve como impedir o desvio de DNS e aplicar as proteções de DNS Umbrella usando regras de firewall e políticas de rede.

Pré-requisitos

- Firewall de rede
- Privilégios de acesso ao firewall
- Conhecimento de configuração de firewall

Aplicação do Umbrella DNS — método mais comum

A maioria dos roteadores e firewalls permite que você aplique todo o tráfego DNS na porta 53, exigindo que todos os dispositivos de rede usem as configurações DNS definidas no roteador, que devem apontar para servidores DNS Umbrella.

A abordagem preferida é encaminhar todas as solicitações de DNS de endereços IP que não são de guarda-chuva para os IPs de DNS de guarda-chuva listados abaixo. Esse método encaminha solicitações DNS de forma transparente e evita que a configuração DNS manual simplesmente falhe.

Como alternativa, crie uma regra de firewall para permitir o DNS (TCP/UDP) somente para

servidores DNS Umbrella e bloquear todo o tráfego DNS para qualquer outro endereço IP.

Exemplo de regra de firewall

1. Adicionar esta regra ao firewall de borda:
    - Permita entrada e saída TCP/UDP na porta ou **208.67.222.222** **208.67.220.220** na porta 53.
    - Bloquear entrada e saída TCP/UDP para todos os endereços IP na porta 53.

A regra de permissão para o DNS do Umbrella tem prioridade sobre a regra de bloqueio. As solicitações DNS para o Umbrella são permitidas, enquanto todas as outras solicitações DNS são bloqueadas.

Dependendo de sua interface de configuração de firewall, configure uma regra separada para cada protocolo ou uma única regra que cubra o TCP e o UDP. Aplique a regra no dispositivo de borda de rede. Você também pode aplicar uma regra semelhante a firewalls de software em estações de trabalho, como o firewall integrado no Windows ou no macOS.

Se você estiver usando o cliente de roaming e a Diretiva de Grupo do Ative Diretory, consulte a documentação sobre como bloquear o Cliente de Roaming Corporativo usando a Diretiva de Grupo.

Imposição contra DNS sobre HTTPS (DoH)

Configuração recomendada

1. No Umbrella, habilite as categorias Proxy / AnonymizerandDoH / DoTcontent.
2. Bloqueie os endereços IP de provedores DoH conhecidos em seu firewall.

Detalhes e histórico

O Umbrella suporta o use-application-dns.netdomínio, conforme definido pelo Mozilla, para impedir que o Firefox habilite o DoH por padrão. Para obter informações sobre o Firefox e o DoH, consulte a documentação relacionada.

Mesmo depois de bloquear provedores DNS alternativos, o DNS ainda pode ser ignorado com DoH. Um resolvedor de DNS local converte solicitações de DNS em HTTPS e as envia para um endpoint usando JSON ou POST/GET. Esse tráfego normalmente evita a inspeção de DNS.

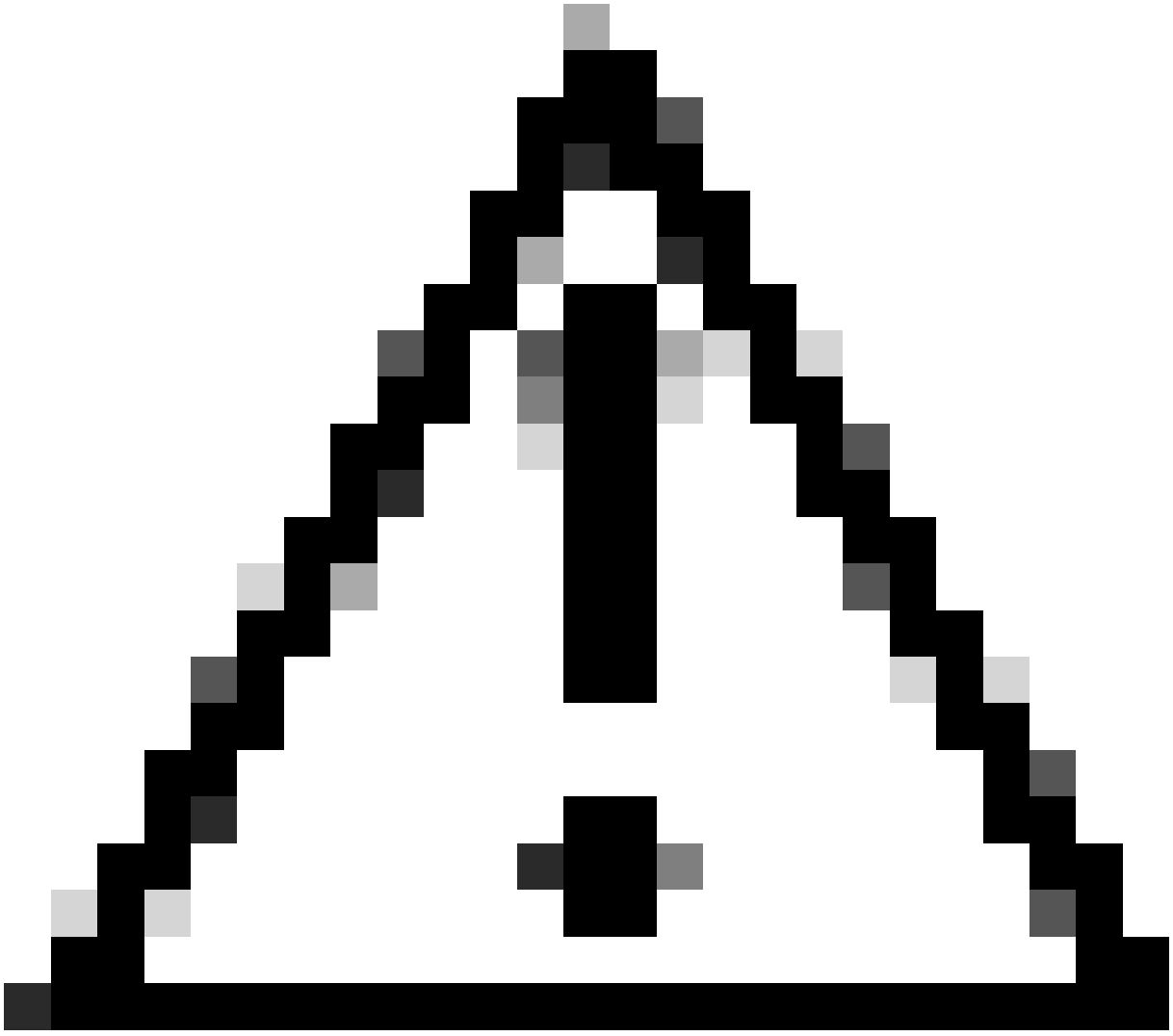
Como o DoH pode ser usado para ignorar o Umbrella, o Umbrella inclui servidores DoH conhecidos na categoria de conteúdo Proxy / Anonymizer. Esse mecanismo tem algumas

limitações:

- Ele não pode bloquear provedores DoH totalmente novos que ainda não são conhecidos.
- Ele não pode bloquear o DoH usado diretamente via endereço IP.

Para lidar com os novos provedores do DoH, monitore atualizações e bloqueie domínios vistos recentemente para melhorar a cobertura.

Para DoH via endereço IP, os cenários são limitados. O Firefox com CloudFlare é um exemplo proeminente.



Caution: Não adicione domínios do Mozilla Kill Switch à lista de bloqueios. O bloqueio desses domínios resulta em um registro A para páginas bloqueadas, e o Firefox trata isso como válido e atualiza automaticamente seu uso do DoH.

Imposição contra DNS sobre TLS (DoT)

Mesmo depois de bloquear provedores DNS alternativos e DoH, o DNS pode ser ignorado sobre TLS, que usa RFC7858 sobre a porta 853. Por exemplo, CloudFlare é um provedor DoT.

Exemplo de aplicação

- Bloqueie os endereços1.1.1.1IP e1.0.0.1na porta 853 (CloudFlare).

Isenção de responsabilidade do suporte de firewall

Este documento ajuda os administradores de rede na aplicação do Umbrella DNS. O Cisco Umbrella Support não oferece assistência com configurações individuais de firewall ou roteador, pois cada dispositivo tem uma interface de configuração exclusiva. Consulte a documentação do roteador ou firewall ou entre em contato com o fabricante do dispositivo para confirmar se essas configurações são possíveis.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.