Appliquer le DNS parapluie et empêcher le contournement avec les règles de pare-feu

Table des matières

Introduction

Ce document décrit comment empêcher le contournement DNS et appliquer les protections Umbrella DNS à l'aide de règles de pare-feu et de politiques réseau.

Conditions préalables

- Pare-feu réseau
- Privilèges d'accès au pare-feu
- Connaissance de la configuration du pare-feu

Mise en oeuvre de Umbrella DNS : méthode la plus courante

La plupart des routeurs et des pare-feu vous permettent d'appliquer tout le trafic DNS sur le port 53, ce qui oblige tous les périphériques réseau à utiliser les paramètres DNS définis sur le routeur, qui doit pointer vers les serveurs DNS Umbrella.

L'approche privilégiée consiste à transférer toutes les requêtes DNS provenant d'adresses IP autres que Umbrella aux adresses IP de DNS Umbrella répertoriées ci-dessous. Cette méthode transfère les requêtes DNS de manière transparente et empêche la configuration DNS manuelle d'échouer.

Vous pouvez également créer une règle de pare-feu pour autoriser uniquement DNS (TCP/UDP)

aux serveurs DNS parapluie et bloquer tout autre trafic DNS vers d’autres adresses IP.

Exemple de règle de pare-feu

1. Ajoutez cette règle au pare-feu de périphérie :
    - Autoriser TCP/UDP en entrée et en sortie vers **208.67.222.222** ou **208.67.220.220** sur le port 53.
    - Bloquez TCP/UDP en entrée et en sortie vers toutes les adresses IP sur le port 53.

La règle d'autorisation pour le DNS Umbrella est prioritaire sur la règle de blocage. Les requêtes DNS vers Umbrella sont autorisées, tandis que toutes les autres requêtes DNS sont bloquées.

Selon l’interface de configuration de votre pare-feu, configurez une règle distincte pour chaque protocole ou une règle unique couvrant à la fois TCP et UDP. Appliquez la règle sur le périphérique de périphérie du réseau. Vous pouvez également appliquer une règle similaire aux pare-feu logiciels sur les stations de travail, comme le pare-feu intégré dans Windows ou macOS.

Si vous utilisez le client d'itinérance et la stratégie de groupe Active Directory, reportez-vous à la documentation relative au verrouillage du client d'itinérance d'entreprise à l'aide de la stratégie de groupe.

Application contre DNS sur HTTPS (DoH)

Configuration recommandée

1. Dans Umbrella, activez les catégories Proxy / Anonymizer et DoH / DoTcontent.
2. Bloquez les adresses IP des fournisseurs DoH connus sur votre pare-feu.

Détails et contexte

Umbrella prend en charge le`use-application-dns.net`domaine, tel que défini par Mozilla, pour empêcher Firefox d'activer le DoH par défaut. Pour plus d'informations sur Firefox et DoH, reportez-vous à la documentation associée.

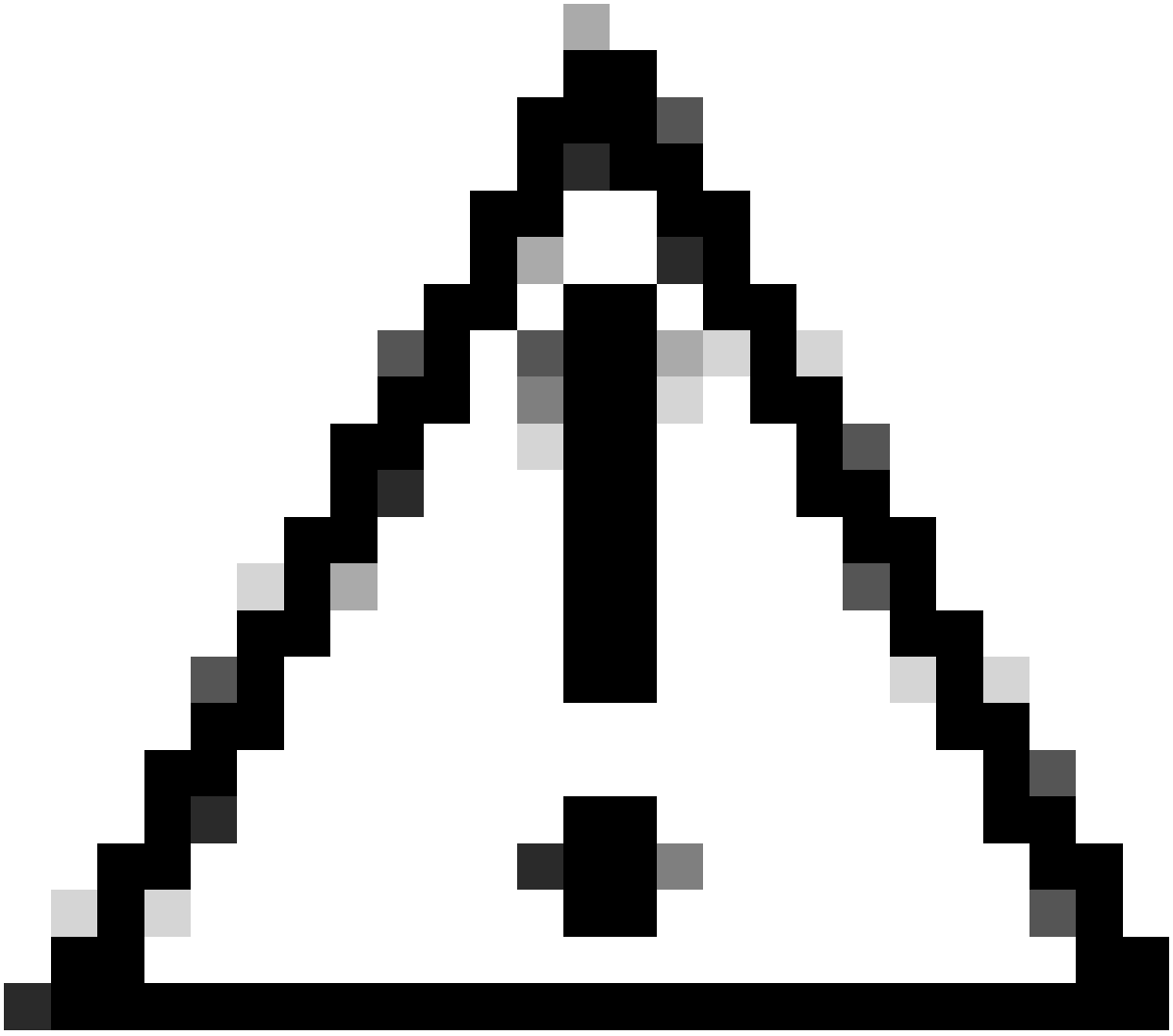
Même après le blocage d'autres fournisseurs DNS, le DNS peut toujours être contourné avec le DoH. Un résolveur DNS local traduit les requêtes DNS en HTTPS et les envoie à un terminal à l'aide de JSON ou POST/GET. Ce trafic évite généralement l’inspection DNS.

Comme le DoH peut être utilisé pour contourner Umbrella, Umbrella inclut les serveurs DoH connus dans la catégorie de contenu Proxy / Anonymizer. Ce mécanisme présente certaines limitations :

- Il ne peut pas bloquer les fournisseurs de DoH flambant neufs qui ne sont pas encore connus.
- Il ne peut pas bloquer le DoH utilisé directement via une adresse IP.

Pour répondre aux nouveaux fournisseurs de DoH, surveillez les mises à jour et bloquez les domaines nouvellement vus pour une couverture améliorée.

Pour le DoH via l'adresse IP, les scénarios sont limités. Firefox avec CloudFlare en est un exemple frappant.



Mise en garde : N'ajoutez pas de domaines de commutateur de suppression Mozilla à la liste de blocage. Le blocage de ces domaines génère un enregistrement A pour les pages de blocage, et Firefox considère cela comme valide et met automatiquement à niveau son

---

utilisation DoH.

Application contre DNS sur TLS (DoT)

Même après le blocage d'autres fournisseurs DNS et du DoH, DNS peut être contourné sur TLS, qui utilise RFC7858 sur le port 853. Par exemple, CloudFlare est un fournisseur DoT.

Exemple d'application

- Bloquez les adresses1.1.1.1IP et1.0.0.1sur le port 853 (CloudFlare).

Avertissement de support pare-feu

Ce document aide les administrateurs réseau à mettre en oeuvre le système Umbrella DNS. Cisco Umbrella Support ne fournit pas d'assistance pour les configurations individuelles des pare-feu ou des routeurs, car chaque périphérique dispose d'une interface de configuration unique. Consultez la documentation de votre routeur ou de votre pare-feu ou contactez le fabricant du périphérique pour vérifier si ces configurations sont possibles.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.