

Comprendre les meilleures pratiques d'installation d'OpenDNS Umbrella avec Websense

Table des matières

[Introduction](#)

[Aperçu](#)

[1\) Le proxy sur site résout les requêtes DNS initiées par les serveurs Web](#)

[2\) Le proxy cloud résout les requêtes DNS initiées par les serveurs Web](#)

[3\) Le proxy local résout les requêtes DNS pour le compte des clients](#)

Introduction

Ce document décrit les meilleures pratiques pour installer OpenDNS Umbrella avec Websense.

Aperçu

Pour vous assurer de voir tout le potentiel d'OpenDNS pendant votre évaluation (et après), tout le trafic DNS non interne doit pointer vers le réseau global OpenDNS. Trois environnements Websense font manquer du trafic DNS à OpenDNS :

1. Le proxy local résout les requêtes DNS initiées par les serveurs Web (plus courant)
2. Le proxy cloud résout les requêtes DNS initiées par les serveurs Web (pour les clients hybrides utilisant des agents de point de terminaison Web)
3. Le proxy local résout les requêtes DNS pour le compte des clients (moins fréquent)

1) Le proxy local résout les requêtes DNS initiées par les serveurs Web

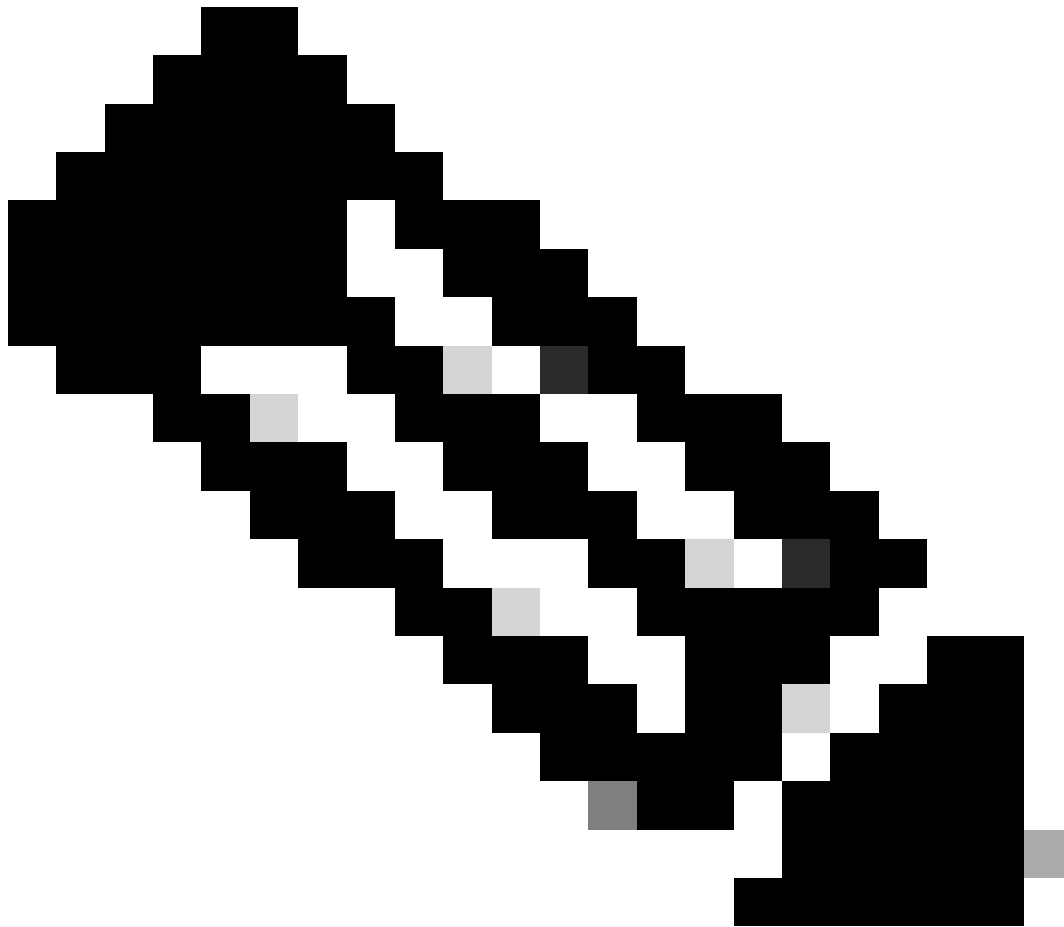
- Les passerelles de contenu Websense, déployées en mode proxy explicite ou transparent, peuvent résoudre les requêtes DNS initiées après une connexion avec un serveur Web ; selon sa configuration.
- Si ces requêtes DNS sont résolues à partir de la mise en cache de proxy DNS intégrée à Websense ou d'un service DNS récursif différent, OpenDNS est contourné.
- Reportez-vous aux documents d'assistance de Websense (liés ici pour plus de commodité) pour vous assurer que Websense est configuré pour toujours résoudre les requêtes DNS non internes à l'aide d'OpenDNS.

2) Le proxy cloud résout les requêtes DNS initiées par les serveurs Web

- Malheureusement, Websense ne permet pas à ses clients de modifier directement les paramètres du serveur DNS.
- Nous ne savons pas si vous pouvez demander à Websense de modifier manuellement les paramètres pour pointer vers OpenDNS.

3) Le proxy local résout les requêtes DNS pour le compte des clients

- Cela se produit si l'option de [cache de proxy DNS](#) est activée, mais que la [configuration de la cache de proxy DNS](#) est uniquement possible avec un commutateur L4 ou un périphérique Cisco WCCPv2, de sorte qu'il ne s'agit pas d'un environnement commun.
- Le proxy DNS répond uniquement aux demandes d'entrées DNS A et CNAME. Les autres types de demandes ne reçoivent pas de réponse.
- Si le mappage du nom d'hôte sur l'adresse IP ne se trouve pas dans le cache DNS, Content Gateway contacte le serveur DNS spécifié dans le fichier /etc/resolv.conf. (Remarque: Seule la première entrée du fichier resolv.conf est utilisée. Il se peut que ce ne soit pas le même serveur DNS que celui auquel la requête DNS était initialement destinée.)



Remarque : L'option « Toujours interroger la destination » [réduit le nombre de recherches DNS](#), et peut être activée si la passerelle de contenu ne s'exécute pas en mode proxy explicite et transparent. Il configure le proxy pour toujours obtenir l'adresse IP de destination d'origine des requêtes entrantes à partir du module ARM (Adaptive Redirection Module). Et utilisez cette adresse IP pour déterminer le serveur d'origine, au lieu d'effectuer une recherche DNS sur le nom d'hôte de la requête. Comme le client a déjà effectué une recherche DNS, le proxy n'a pas à le faire.

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.