Comprendre pourquoi les requêtes de domaines internes ne sont pas connectées à Umbrella Insights

Table des matières

Introduction

Ce document explique pourquoi les requêtes pour les domaines internes ne sont pas consignées.

Aperçu

Lors de l'utilisation d'Umbrella Insights, qui inclut l'appliance virtuelle (VA), tous les postes de travail doivent uniquement disposer de leurs paramètres de serveur DNS pointant vers les VA. Les serveurs virtuels doivent être configurés pour utiliser vos serveurs DNS internes préexistants. Le tableau de bord vous permet d'entrer une liste de 'Domaines internes' de sorte que lorsque le client effectue une requête DNS pour une ressource interne, l'AV transfère la requête à l'un des serveurs DNS internes. Parfois, on nous demande pourquoi aucune de ces requêtes internes n'apparaît dans la journalisation.

Explication

Comme indiqué ci-dessus, les requêtes DNS internes reçues par l'appliance virtuelle sont transmises à l'un des serveurs DNS internes configurés sur l'appliance virtuelle au cours de la configuration. Elles sont visibles sur la console. Le serveur DNS interne émet alors une réponse et l'appliance virtuelle la relaie au client.

Lorsque le client effectue une requête DNS pour une ressource qui ne figure PAS dans la liste des domaines internes, il la transfère aux adresses IP Umbrella Anycast. Cette requête inclut des données supplémentaires dans la requête DNS vers nos résolveurs, ce qui permet de lier la requête à une origine. L'origine peut être, par exemple, un hachage UserID, une adresse IP source ou un certain nombre d'autres facteurs d'identification inclus dans ce paquet DNS étendu. Ces données supplémentaires peuvent être vues en exécutant une requête DNS spécifique à partir d'une ligne de commande :

```
nslookup -server=208.67.222.222 -type=txt debug.opendns.com.
```

La journalisation réelle des requêtes DNS a lieu sur nos résolveurs. La journalisation repose sur l’ajout de ces informations uniques au paquet DNS. L'appliance virtuelle n'enregistre pas les requêtes DNS qu'elle transfère. Il s'agit avant tout d'un serveur DNS récursif. Une fois que nos résolveurs publics reçoivent une requête DNS, ils utilisent les données étendues envoyées avec la requête réelle pour identifier la source, appliquer la stratégie appropriée et consigner les informations de la requête et si elle a été autorisée ou bloquée, qui apparaît ensuite dans le tableau de bord. Comme les requêtes DNS internes ne voient jamais nos résolveurs, leur journalisation n'est pas possible.

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.