Comprendre le DNS parapluie avec la minimisation QNAME

Table des matières

Introduction

Ce document décrit comment utiliser Cisco Umbrella Domain Name System (DNS) avec la minimisation QNAME.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

En juin 2019, Cisco Umbrella a ajouté la prise en charge de la minimisation des noms de requêtes (RFC7816). La minimisation QNAME est une fonctionnalité orientée confidentialité dans DNS qui vise à limiter l'envoi de la destination de domaine complet aux serveurs de noms racine. En conséquence, le flux de requêtes DNS pour déterminer la réponse à la requête DNS est modifié.

QNAME Minimization est un sujet mondial. L'Internet Systems Consortium propose un article d'introduction sur la minimisation de QNAME. Mozilla Firefox exige que les résolveurs utilisent la minimisation QNAME pour les implémentations DNS sur HTTPS et a un article sur ce sujet.

Comprendre la minimisation des requêtes

La minimisation des requêtes est une nouvelle approche axée sur la confidentialité des données des requêtes DNS faisant autorité. Pour découvrir ce qu'est la minimisation des requêtes, commencez par expliquer le fonctionnement actuel d'une requête DNS.

Comme la plupart des interactions humaines avec Internet commencent par une requête DNS, le Big Data sur l'endroit où les utilisateurs vont est une information inestimable, qui peut être considérée comme des données privées.

Pour cet exemple, vous souhaitez visiter le site umbrella.cisco.com. Vous avez besoin d'une requête DNS pour déterminer l'emplacement de ce serveur. Par conséquent, Umbrella envoie cette requête à un serveur DNS récursif pour trouver la réponse de l'autorité en procédant comme suit :

1. Requête utilisateur vers le résolveur DNS récursif : umbrella.cisco.com

2. Le serveur DNS récursif interroge la réponse à partir des serveurs de noms racine : où puis-je trouver umbrella.cisco.com à root > répondre pour .com

3. Requête sur les serveurs de noms .com : umbrella.cisco.com à .com > obtient l'emplacement des serveurs de noms cisco.com

4. Effectuez une requête vers les serveurs de noms cisco.com : umbrella.cisco.com à cisco.com > Réponse fournie

Dans de nombreux cas, cela peut continuer avec plusieurs itérations vers différents serveurs de noms jusqu'à ce qu'un enregistrement A soit localisé. Dans les étapes 1 et 2, Umbrella recherche uniquement l'emplacement des serveurs de noms .com. Cependant, le domaine umbrella.cisco.com complet est envoyé au serveur racine et au serveur de noms .com. Il en va de même pour le serveur de noms cisco.com qui reçoit la requête complète.

Avec la minimisation de la requête, l'algorithme passe à demander uniquement le niveau de détail requis dans les requêtes en amont :

1. Requête utilisateur vers le résolveur DNS récursif : umbrella.cisco.com

2. Le serveur DNS récursif interroge les serveurs de noms racine : où puis-je trouver .com > répondre pour .com

3. Requête sur les serveurs de noms .com : cisco.com vers .com > emplacement de cisco.com

4. Effectuez une requête sur les serveurs de noms cisco.com pour umbrella.cisco.com > Réponse

Cela fonctionne très bien dans la plupart des cas et permet de localiser la réponse sans révéler la requête unique effectuée sur les serveurs de noms racine ou TLD.

Cette confidentialité est encore plus importante pour les domaines qui utilisent le sous-réseau client EDNS, où l'autorité DNS est informée du bloc C source de l'utilisateur (/24) lors de

l'interrogation. Sans la minimisation de QNAME, les serveurs de noms racine et .com (dans cet exemple) connaissent votre emplacement général ainsi que l'endroit exact où vous allez. Avec QNAME Minimization, les racines savent seulement que quelqu'un recherche .com et la confidentialité du demandeur est maintenue. Ils n'ont pas besoin du niveau de détail qui leur est fourni aujourd'hui sans protection de la vie privée QMIN.

Effets secondaires potentiels

La minimisation de QNAME fonctionne sans problème dans la plupart des cas. Cependant, elle est sujette à des sources d'échec supplémentaires par rapport à une requête directe. Comme la destination complète n'est révélée qu'à la dernière étape du processus au serveur de noms faisant autorité, les ruptures dans la chaîne DNS peuvent interrompre la résolution du domaine. Par exemple, voici un nom fictif long : umbrellas.in.the.rain.umbrella.cisco.com. Cela peut entraîner les requêtes suivantes :

1. Quels sont les serveurs de noms pour .com vers les serveurs racine .

2. Quels sont les serveurs de noms pour cisco.com vers les serveurs .com ?

3. Quels sont les serveurs de noms umbrella.cisco.com vers les serveurs de noms cisco.com ?

4. Quels sont les serveurs de noms pour rain.umbrella.cisco.com vers les serveurs de noms umbrella.cisco.com ?

5. Quels sont les serveurs de noms the.rain.umbrella.cisco.com vers les serveurs de noms rain.umbrella.cisco.com ?

6. Quels sont les serveurs de noms pour in.the.rain.umbrella.cisco.com vers les serveurs de noms rain.umbrella.cisco.com : DÉFAILLANCE DE SERVICE

7. Quels sont les serveurs de noms pour umbrellas.in.the.rain.umbrella.cisco.com vers les serveurs de noms rain.umbrella.cisco.com (non interrogés en raison de SERVFAIL précédemment) ?

8. Quelle est la réponse de umbrellas.in.the.rain.umbrella.cisco.com aux serveurs de noms umbrellas.in.the.rain.umbrella.cisco.com précédemment trouvés (non interrogés en raison de SERVFAIL) ?

Étant donné que les racines ne reçoivent pas la requête complète, si l'un des niveaux du domaine renvoie un NXDOMAIN, SERVFAIL, l'IP d'un serveur de noms interne RFC-1918 ou une autre mauvaise réponse, la requête peut échouer à recevoir une réponse faisant autorité en amont. Par exemple, si la sixième étape (gras, souligné) échouait, la résolution de la requête pour umbrellas.in.the.rain.umbrella.cisco.com peut échouer. Pour résoudre ces problèmes, le propriétaire du domaine doit s'assurer que chaque niveau dispose d'une réponse publique valide.

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.