Configurer le filtre Web Umbrella et BlueCoat/K9

Table des matières

Introduction

Ce document décrit comment configurer la compatibilité entre le client d'itinérance Umbrella et BlueCoat Webfilter/K9.

Aperçu

Cet article concerne les ordinateurs sur lesquels le client d'itinérance Umbrella et BlueCoat sont installés. Cet article fait référence à l'utilisation d'un agent de filtrage BlueCoat installé sur la machine. Cela peut coïncider avec une configuration PAC ou proxy.

Le client d'itinérance Umbrella et le module de sécurité d'itinérance Umbrella d'AnyConnect ne sont actuellement pas compatibles avec le filtrage basé sur le logiciel BlueCoat qui tente de contrôler DNS.

Logiciels affectés :

- Module de sécurité Cisco AnyConnect Umbrella Roaming
- Client d'itinérance Umbrella

Symptômes

Module d'itinérance AnyConnect et client d'itinérance antérieur à 2.2.150

Lorsque le client ou le module d'itinérance est actif, tous les DNS semblent échouer. Cela entraîne une perte apparente de convivialité sur la machine et une perte de la capacité à accéder aux ressources Web. Plus précisément, toute requête DNS à un enregistrement A échoue ; cependant, d'autres types d'enregistrement tels que AAAA ou TXT réussissent.

Lorsque le client itinérant est désinstallé ou temporairement arrêté, le comportement normal du réseau est rétabli.

Le client d'itinérance ne reconnaît pas le DNS défaillant, car seuls les enregistrements A échouent. Par conséquent, le client reste actif et chiffré.

Client itinérant 2.2.150 et versions ultérieures

Lorsque le client en itinérance est actif, il bascule en état ouvert avec le message

"nous avons détecté une interférence potentielle avec les requêtes DNS A et/ou AAAA ; il se peut que certains logiciels sur le système posent des problèmes. »

Il s'agit d'une nouvelle méthode de détection pour les logiciels qui remplace A-Records mais ne modifie pas les enregistrements TXT. Nous marquons ce comportement et le désactivons pour empêcher la perte de DNS.

Dépannage

Pour vérifier si vous observez actuellement ce problème, vérifiez que les conditions suivantes sont remplies :

- Ces scénarios entraînent l'échec du DNS (ou la désactivation du mode enregistrement A)
  - BlueCoat actif et :
    - Client ou module itinérant protégé et chiffré
    - Client ou module itinérant protégé et non chiffré
  - Processus BlueCoat manuellement tué (non désinstallé). La redirection est active, mais le proxy sous-jacent est hors ligne.
    - Client ou module itinérant protégé
    - Client itinérant désinstallé ou arrêté
- Cela n'entraîne aucun problème
  - Client ou module itinérant actif avec BlueCoat désinstallé (après un redémarrage)
  - Le filtre Web BlueCoat est installé et aucun client d'itinérance n'est exécuté

Lorsque DNS échoue, tous les enregistrements A échouent, mais les enregistrements TXT ne sont toujours pas redirigés par BlueCoat et sa fonction.

Cause première et solution

La cause première de ce problème de compatibilité est double.

1. Le logiciel BlueCoat redirige les requêtes d'enregistrement A (les enregistrements DNS les plus courants pour l'affichage des pages Web) de sorte que seul il peut répondre à ces requêtes. Ce DNS peut quitter le réseau, mais il ne peut pas répondre au système. Le client itinérant n'a aucun moyen de remplacer cela.
2. Le client d’itinérance détermine la disponibilité DNS en vérifiant les réponses d’enregistrement TXT qui sont uniques aux résolveurs Umbrella. Étant donné que BlueCoat n'applique pas les enregistrements TXT, les tests du client d'itinérance continuent de réussir même après que tous les enregistrements A commencent à échouer. Cet échec

d'enregistrement A et le succès d'enregistrement TXT font que le client d'itinérance reste chiffré, perpétuant ainsi un état cassé avec le logiciel BlueCoat.

L'application sélective de proxy DNS de BlueCoat à un niveau bas dans le système entraîne un problème de compatibilité directe avec le client d'itinérance. L'impact sur l'utilisateur est une perte de DNS et de la capacité de navigation Web basée sur DNS.

La seule solution pour le moment est de cesser d'utiliser le logiciel de station de travail BlueCoat qui redirige DNS et d'utiliser à la place des restrictions de contenu basées sur Umbrella. BlueCoat peut ajouter la possibilité de désactiver l'application DNS à une date ultérieure.

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.