Problèmes de coexistence de sécurité DNS globale avec Broadcom WSS sur macOS

Table des matières

Problème

Le module Umbrella n'intercepte pas le trafic DNS sur macOS lorsqu'il coexiste avec Broadcom WSS (Web Security Service). Lorsque l'agent WSS est configuré pour intercepter des ports Web spécifiques tels que 80 et 443, la fonctionnalité de sécurité Umbrella DNS ne parvient pas à capturer toutes les requêtes DNS. Cependant, lorsque WSS est désactivé, Umbrella reprend l'interception du trafic DNS comme prévu. Seules certaines requêtes DNS sont traitées par Umbrella lorsque WSS est activé, plutôt que tout le trafic DNS intercepté.

Environnement

- Système d'exploitation : macOS
- Module de sécurité DNS Cisco Umbrella
- Agent Broadcom WSS (Web Security Service)
- Agent WSS configuré pour intercepter les ports Web 80 et 443

Résolution

Ce problème a été analysé et déterminé comme étant une limitation architecturale de macOS où la sécurité DNS ne peut pas coexister avec WSS dans l'architecture macOS actuelle. Cette limitation s'applique aux solutions de sécurité DNS Infoblox et Cisco Umbrella.

Analyse technique

La cause principale est liée aux limitations du proxy DNS macOS :

- Un seul proxy DNS à la fois peut être actif dans le système en raison des limitations de macOS
- Si les résolveurs DNS sont liés à des interfaces UTUNX ou à des résolveurs par proxy, macOS résout le DNS à l'intérieur du tunnel, et non via Umbrella
- Lorsqu'un autre NEDnsProxyProvider est actif sur le système sur macOS, Umbrella n'intercepte pas le trafic DNS

Commandes de diagnostic

Pour vérifier quel résolveur DNS est prioritaire sur macOS, utilisez la commande suivante :

```
scutil --dns
```

Cette commande affiche le résolveur marqué comme : Étendue, supplémentaire ou interface : utunX, qui permet d'identifier les conflits de proxy DNS.

Options de contournement

Pour les environnements macOS, WSS continuera à intercepter DNS sans agent DNS distinct. Pour aller de l'avant avec la couverture de sécurité DNS, une option serait de mettre en oeuvre pour prendre en charge une architecture de contournement passif. Avec cette approche, le fournisseur contournerait complètement le flux, permettant au trafic d'être traité comme si le fournisseur n'était pas actif.

Motif

Le problème est causé par les limitations architecturales de macOS où un seul NEDnsProxyProvider peut être actif sur le système à la fois. Lorsque la sécurité DNS Umbrella et Broadcom WSS sont toutes deux installées, elles rivalisent pour le contrôle de proxy DNS, ce qui a pour conséquence que WSS est prioritaire et empêche Umbrella d'intercepter le trafic DNS. Il s'agit d'une limitation fondamentale de la pile réseau macOS et elle affecte toutes les solutions de sécurité DNS, pas seulement Cisco Umbrella.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

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.