Comprendre OpenDNS FamilyShield

Table des matières

Introduction

Ce document décrit ce qu'est OpenDNS FamilyShield, ce qu'il fait et comment l'utiliser sur un réseau.

Aperçu

OpenDNS FamilyShield est un service de filtrage de contenu basé sur DNS qui permet de bloquer l'accès aux sites Web généralement classés comme des contenus pour adultes à l'aide de paramètres de filtrage prédéfinis.

Quand utiliser FamilyShield ?

Utilisez FamilyShield lorsque vous avez besoin d'une méthode simple basée sur DNS pour appliquer le filtrage de contenu de base :

- Réseaux domestiques
- Petits environnements de bureau
- Réseaux invités
- Périphériques de laboratoire ou de kiosque nécessitant des contrôles simplifiés

FamilyShield est généralement utilisé lorsqu'une configuration rapide est préférable à la gestion de stratégies de filtrage personnalisées.

Fonctionnement de FamilyShield

FamilyShield utilise des adresses de résolution DNS spécifiques. Lorsqu'un utilisateur tente d'accéder à un domaine, les requêtes DNS sont résolues via les résolveurs FamilyShield. Si le domaine est classé comme étant restreint par FamilyShield, la réponse DNS est bloquée ou redirigée en fonction du comportement du service.

Remarque : Étant donné qu'il s'agit d'un protocole DNS, il contrôle principalement l'accès par résolution de noms de domaine.

Adresses de serveur DNS

Configurez ces adresses de serveur DNS sur le point d'extrémité ou sur les paramètres DNS du routeur/DHCP :

- 208.67.222.123
- 208.67.220.123

Vérification de l'utilisation de FamilyShield

- Vérifiez que le périphérique ou le réseau est configuré pour utiliser les adresses de serveur DNS de FamilyShield.
- Testez la résolution de noms pour un domaine autorisé connu et confirmez la résolution normale.
- Si le filtrage du contenu ne semble pas fonctionner, vérifiez qu'aucune autre méthode DNS ne remplace la configuration (par exemple, VPN DNS, navigateur DNS-over-HTTPS ou paramètres DNS configurés manuellement).

Limites

- Le filtrage basé sur DNS peut être contourné si un utilisateur modifie les paramètres DNS, utilise un VPN ou utilise DNS-over-HTTPS (DoH) dans le navigateur.
- Le comportement de filtrage est basé sur les catégories et n'est pas identique à une solution d'inspection de contenu de pare-feu ou de proxy complet.

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.