Comprendre les paramètres de désinstallation DNS et SWG pour CSC

Table des matières

Introduction

Ce document décrit les paramètres d'interruption DNS et Secure Web Gateway (SWG) pour Cisco Secure Client (CSC).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Secure Client.

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

Jusqu'au 25 avril 2024 environ, le comportement de réémission temporisée du module SWG du client sécurisé Cisco ne pouvait pas être contrôlé quel que soit l'état du module DNS et dépendait des paramètres de réémission temporisée DNS pour activer/désactiver la protection SWG. Pour résoudre ce problème, Umbrella a découplé le comportement du module DNS et du module SWG, permettant ainsi une gestion indépendante en fonction des besoins. Cette fonctionnalité est disponible pour les clients sécurisés Cisco sur les versions 5.1.3.62 et ultérieures où Umbrella a découplé les paramètres de réémission temporisée DNS et SWG pour permettre un contrôle

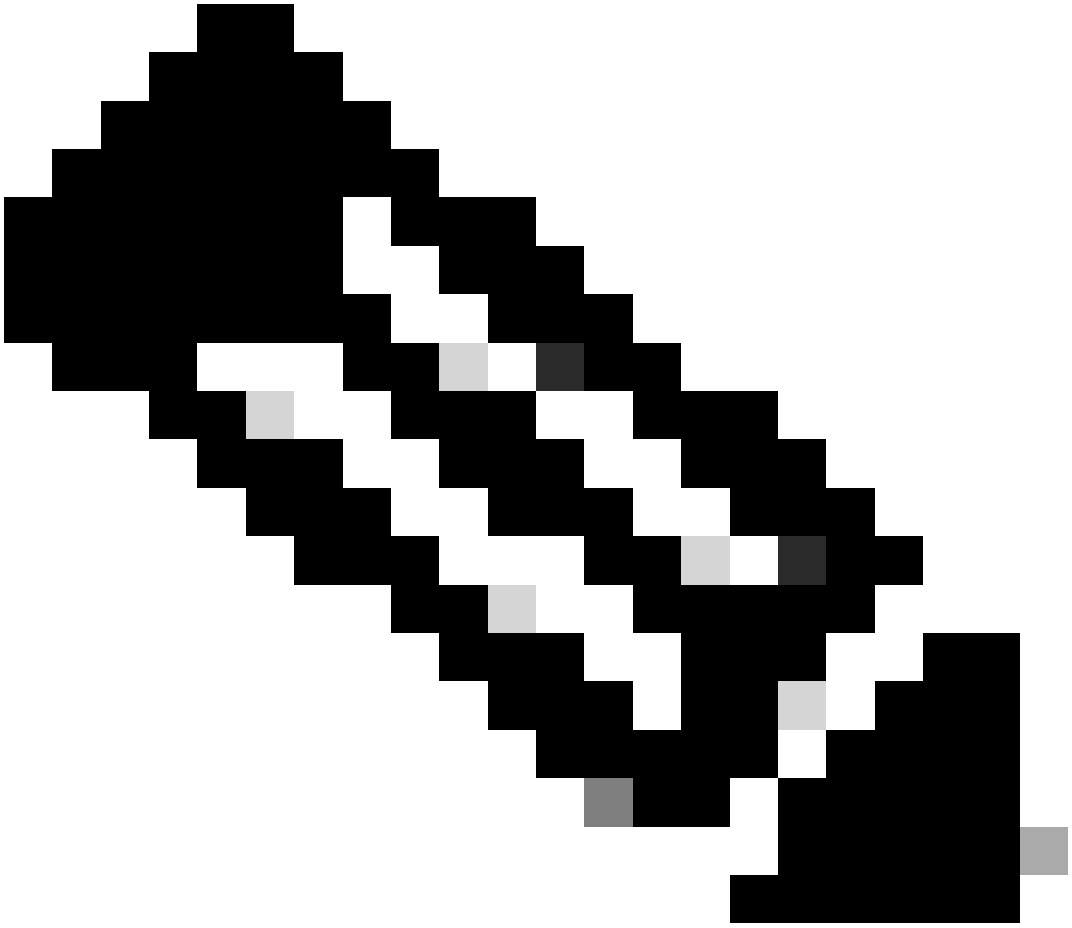
granulaire amélioré. Les clients sur les versions antérieures ne suivaient pas la réémission arrière du module SWG séparé.

Lorsque la fonctionnalité de réémission temporisée de la passerelle Web sécurisée est activée, le module SWG du CSC suit le comportement du module DNS. Cependant, cela ne se produit pas avec tous les paramètres de réémission temporisée DNS. Dans la section suivante, les paramètres de réémission temporisée DNS que le module SWG respecte ou ne respecte pas sont détaillés.

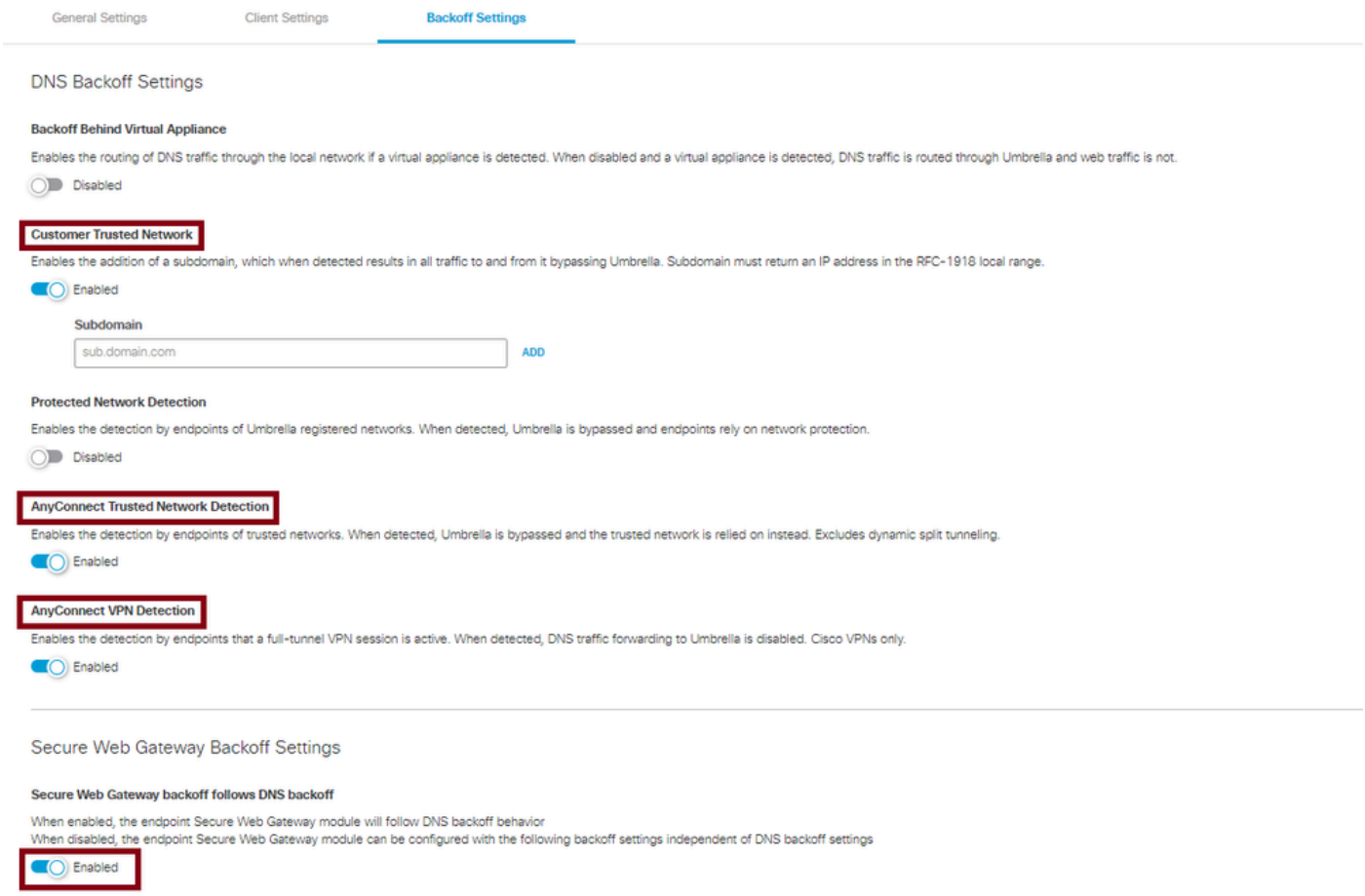
Quels paramètres de désactivation DNS provoquent la désactivation de SWG ?

Ces paramètres d'interruption DNS provoquent l'interruption de SWG :

- Réseau de confiance du client : La configuration d'un domaine Customer Trusted Network dans les paramètres de réémission temporisée DNS est l'une des méthodes les plus simples. En hébergeant un domaine interne qui se résout en une adresse RFC1918, DNS et SWG peuvent tous deux effectuer une réémission temporisée simultanée. Le client Umbrella est codé pour interroger ce domaine. S'il parvient à résoudre le domaine en une adresse IP privée, il identifie le périphérique comme se trouvant sur un réseau privé et protégé, provoquant l'arrêt du module DNS. Ce mécanisme de réémission temporisée est également respecté par le module Web, qui peut également se réémission temporisée lorsque le module DNS parvient à résoudre le domaine.
- Détection de réseau fiable AnyConnect
- Détection VPN AnyConnect



Remarque : Les paramètres de réémission temporisée DNS restent fonctionnels sur les clients sécurisés Cisco exécutant des versions antérieures à 5.1.3.62, car ils ont été mis en oeuvre avant le découplage des paramètres de réémission temporisée DNS et SWG.

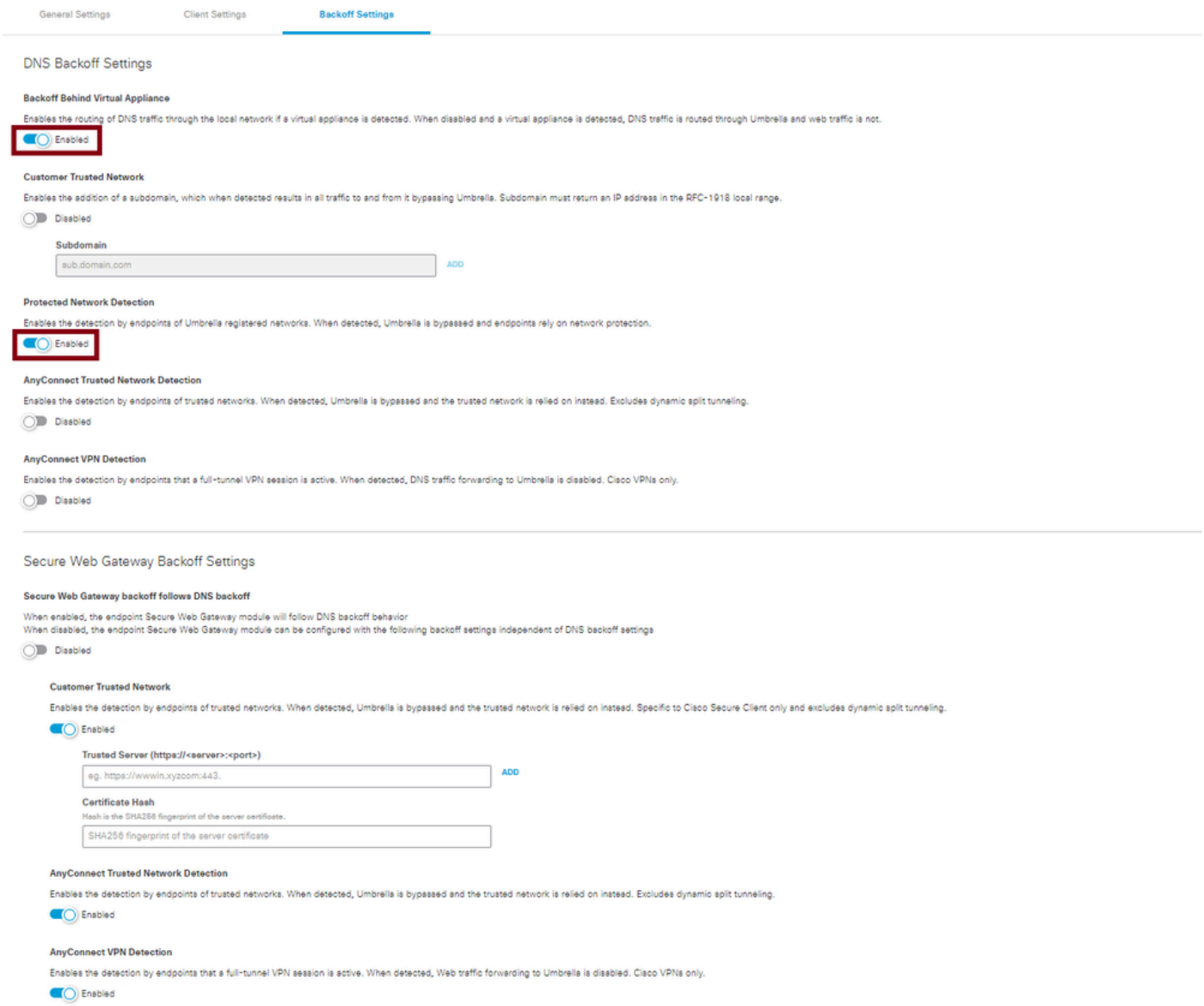


27885424859028

Quels paramètres de désactivation DNS n'entraînent pas la désactivation de SWG ?

La configuration de ces deux fonctions de réémission temporisée DNS n'entraîne pas la désactivation de SWG. Par conséquent, vous devez configurer les paramètres de réémission temporisée SWG de manière sélective, indépendamment de l'état de configuration DNS. Cette question est traitée plus en détail dans la section suivante.

- Retour arrière derrière l'appliance virtuelle : À partir d'AnyConnect 4.10.07061 (MR7) et Secure Client 5.0.02075 (MR2), le module SWG peut rester activé sur les réseaux où une appliance virtuelle Umbrella est présente. Si vous comptiez précédemment sur la présence d'une appliance virtuelle pour désactiver le module SWG et la redirection Web sur un réseau donné, vous pouvez utiliser le domaine de réseau sécurisé ou la détection de réseau sécurisé AnyConnect.
- Détection de réseau protégé



27885587178772

Paramètres de désactivation SWG indépendants

Si ces fonctions de réémission temporisée DNS ne sont pas activées dans votre environnement, vous pouvez utiliser exclusivement l'un des paramètres de réémission temporisée SWG décrits ici pour vous assurer que SWG reste désactivé :

- Réseau de confiance du client
- Détection de réseau fiable AnyConnect
- Détection VPN AnyConnect

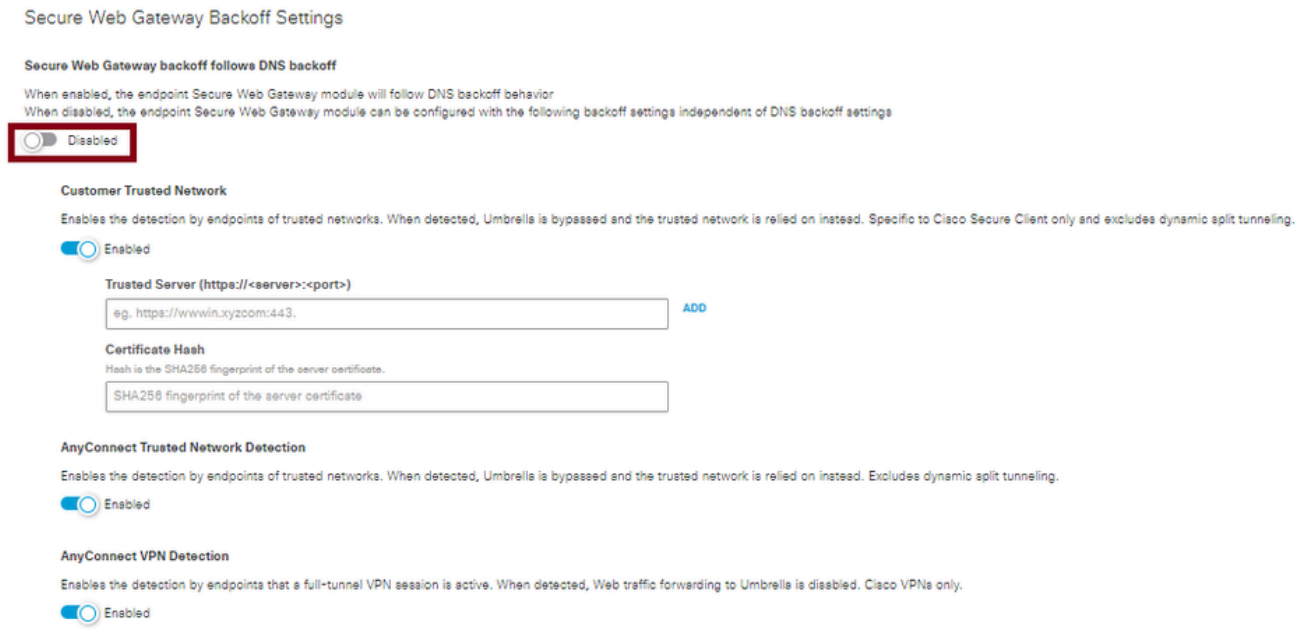
Cette nouvelle fonctionnalité permet au module SWG de fonctionner indépendamment du module DNS. Cette fonctionnalité est disponible pour les clients sécurisés Cisco utilisant la version 5.1.3.62 et les versions ultérieures. Configurez l'une des bascules explicites de désactivation SWG dans le tableau de bord :

- Réseau de confiance du client : L'une des options consiste à utiliser l'option Customer

Trusted Network sous les paramètres de réémission temporisée SWG où vous pouvez configurer un serveur interne que le client peut atteindre pour confirmer qu'il se trouve sur le réseau protégé. Vous devez vous assurer que le serveur Web est accessible par le client, obtenir un certificat sur ce serveur et copier le hachage du certificat dans le tableau de bord Umbrella.

Les deux autres options s'appliquent exclusivement aux connexions VPN :

- Détection de réseau fiable AnyConnect
- Détection VPN AnyConnect



27886005743764

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.