Configurer la catégorie de sécurité VPN de tunnellisation DNS

Table des matières

Introduction

Ce document décrit comment configurer la catégorie de sécurité VPN de tunneling DNS dans Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Umbrella DNS.

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

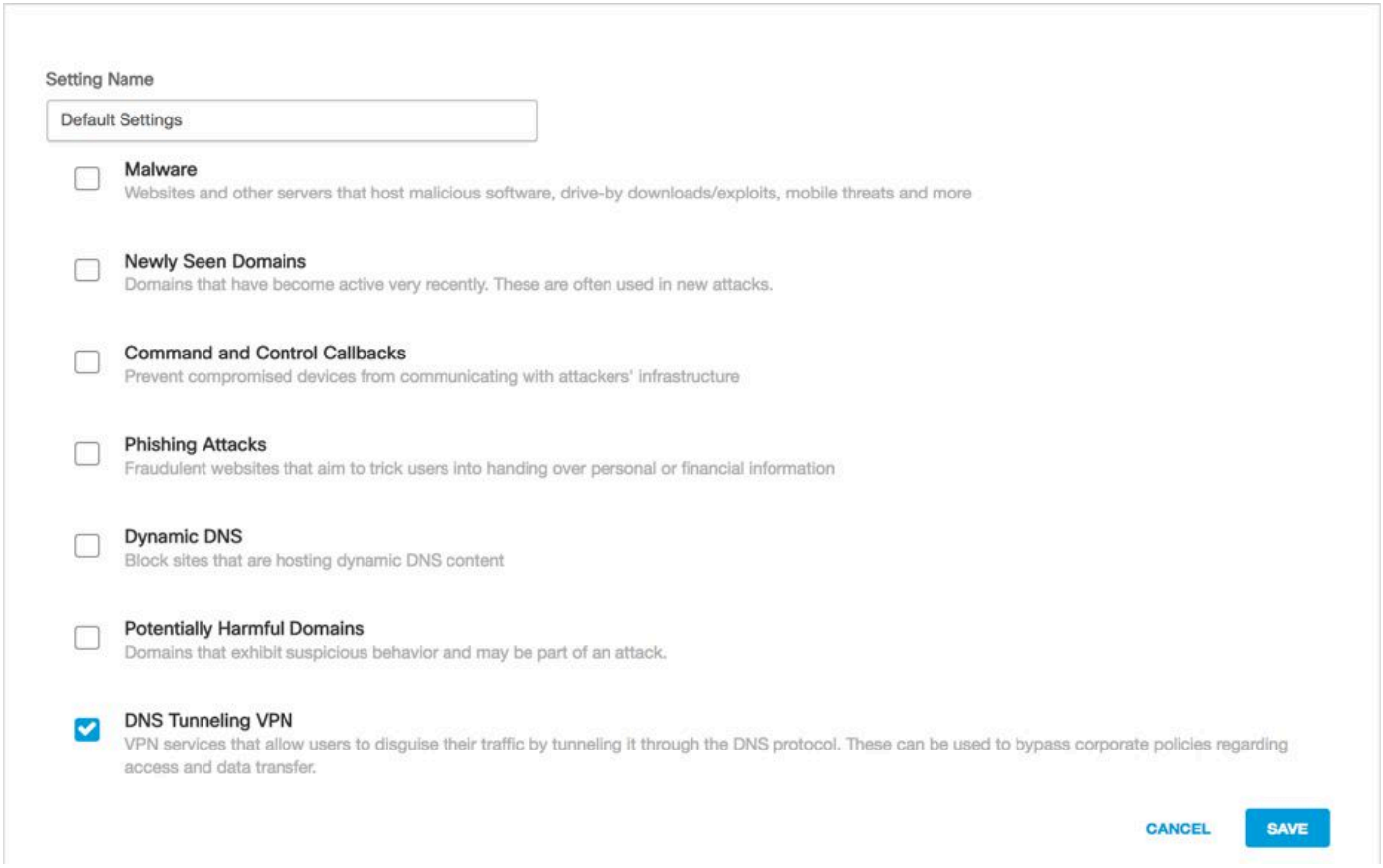
Le VPN de tunnellisation DNS classe les serveurs associés aux services VPN de tunnellisation DNS dans une catégorie de sécurité que vous pouvez bloquer ou autoriser et sur laquelle vous pouvez générer des rapports. Ces services permettent aux utilisateurs finaux de dissimuler le trafic sortant en tant que requêtes DNS, ce qui peut constituer une violation des politiques d'utilisation acceptable, de prévention des pertes de données ou de sécurité. Par conséquent, ces services représentent une menace potentielle pour la sécurité et réduisent la visibilité globale de votre environnement.

Grâce à cette catégorie de sécurité offrant une visibilité immédiate, vous pouvez réduire le risque

de transmission tunnel DNS et de perte de données potentielle. Vous pouvez bloquer directement cette catégorie, ou simplement surveiller les résultats dans les rapports ; vous avez ainsi la possibilité de déterminer quelle est la bonne approche pour aborder le problème, en fonction de votre tolérance au risque, de votre utilisation acceptable ou de vos politiques en matière de RH.

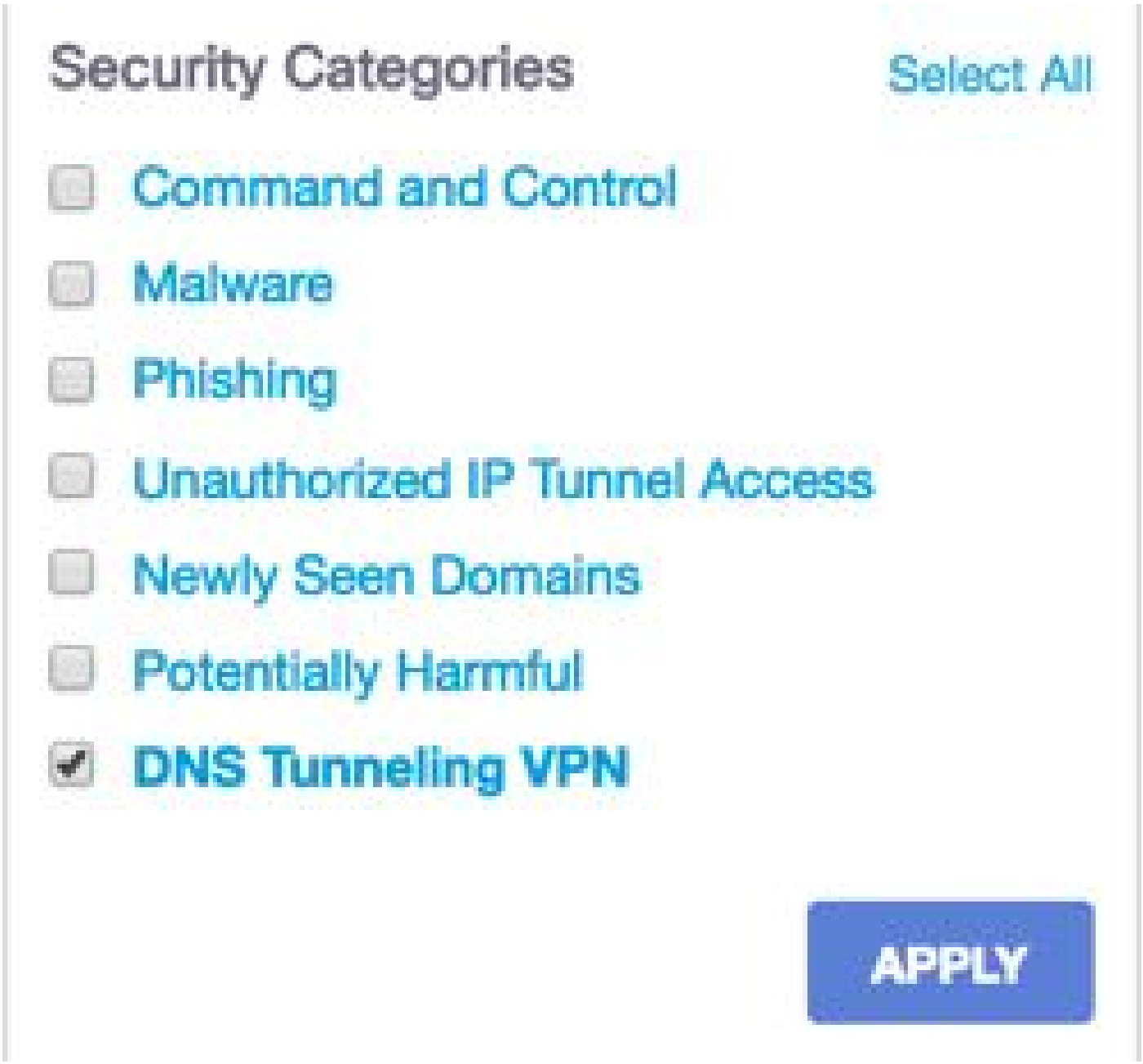
Activation du VPN de tunnellisation DNS

Cette catégorie de sécurité peut être activée comme n'importe quelle autre sous Stratégies > Paramètres de sécurité, puis en modifiant un paramètre de sécurité existant. Vous pouvez également le faire dans l'assistant de configuration de stratégie :



115014823666

La tunnellisation DNS peut être filtrée par rapport à via le rapport de recherche d'activité :



115015008983

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.