

Configurer la catégorie de sécurité VPN de tunnellation DNS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Activation du VPN de tunnellation DNS](#)

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

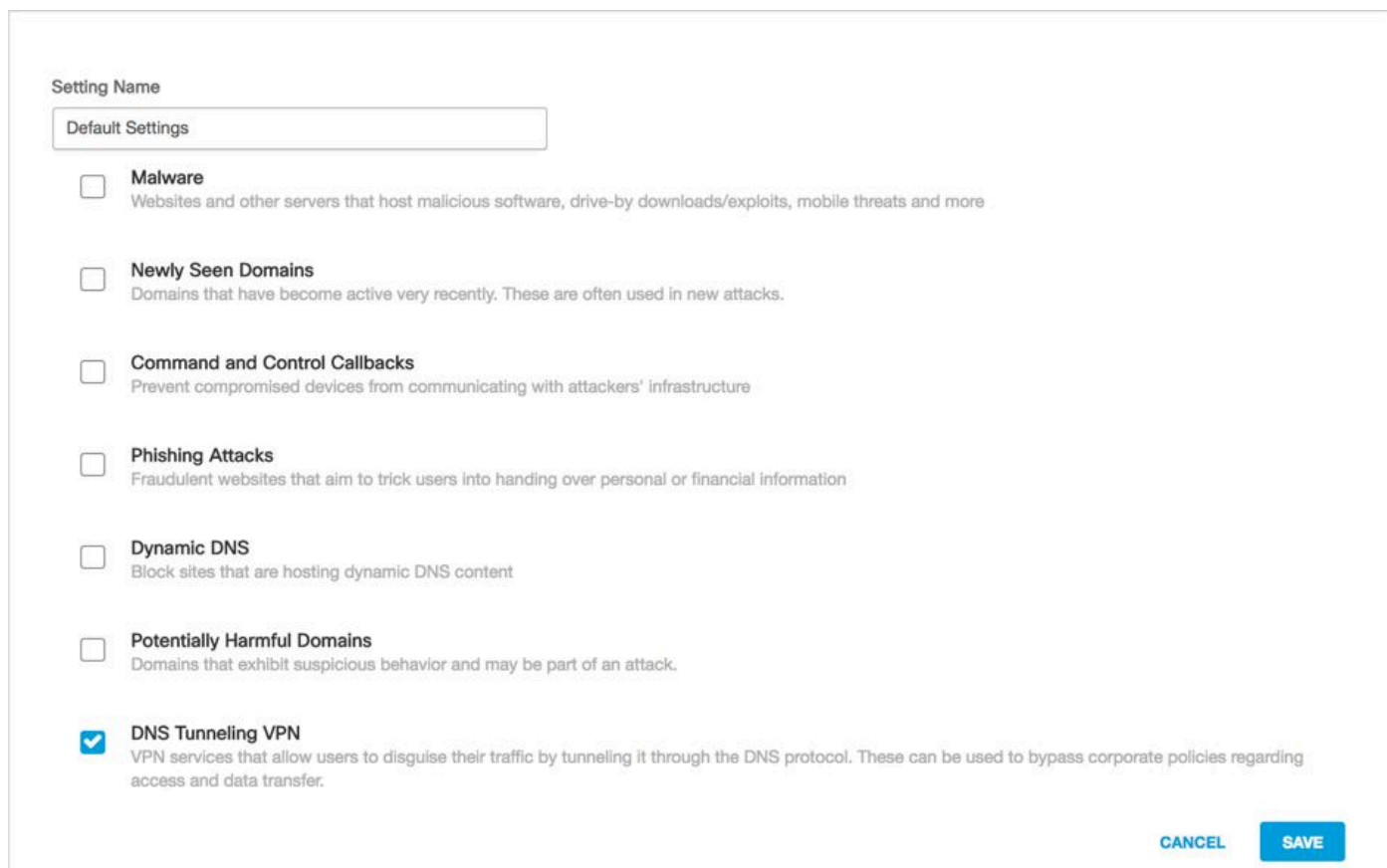
Le VPN de tunnellation DNS classe les serveurs associés aux services VPN de tunnellation DNS dans une catégorie de sécurité que vous pouvez bloquer ou autoriser et sur laquelle vous pouvez générer des rapports. Ces services permettent aux utilisateurs finaux de dissimuler le trafic sortant en tant que 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 tunnellation 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 :



The screenshot shows a configuration window for security settings. At the top, there is a text input field labeled 'Setting Name' containing the text 'Default Settings'. Below this, there is a list of seven security categories, each with a checkbox and a brief description:

- Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more
- Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure
- Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information
- Dynamic DNS**
Block sites that are hosting dynamic DNS content
- Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

At the bottom right of the window, there are two buttons: 'CANCEL' and 'SAVE'.

115014823666

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

Security Categories

Select All

- Command and Control
- Malware
- Phishing
- Unauthorized IP Tunnel Access
- Newly Seen Domains
- Potentially Harmful
- DNS Tunneling VPN**

APPLY

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.