

# Configuración de la Categoría de Seguridad VPN de Tunnelización DNS

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Activación de la VPN de túnel DNS](#)

---

## Introducción

Este documento describe cómo configurar la categoría de seguridad VPN de tunnelización DNS en Umbrella.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información de este documento se basa en Umbrella DNS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Overview

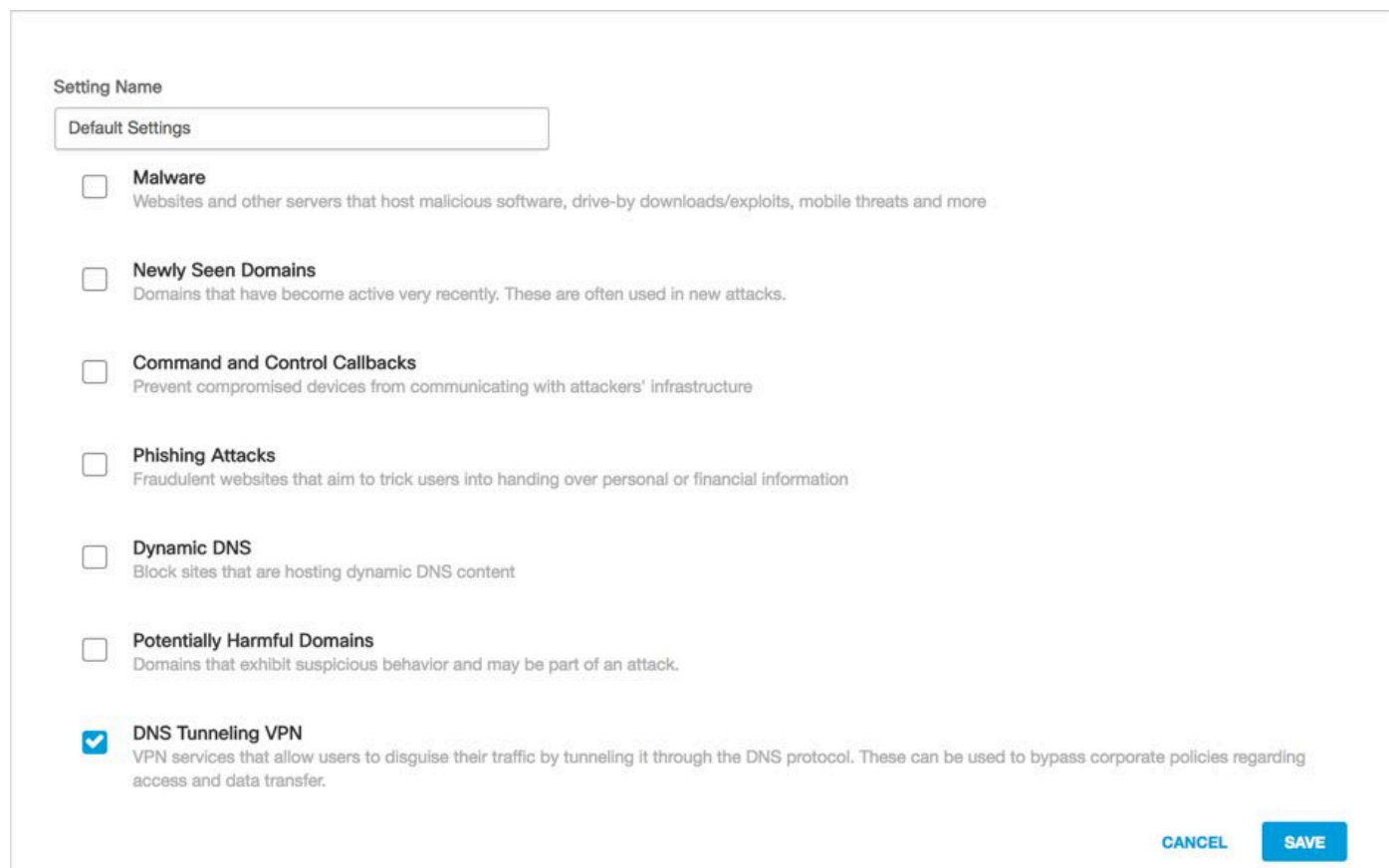
La VPN de tunnelización DNS clasifica los servidores asociados con los servicios VPN de tunnelización DNS en una categoría de seguridad que puede bloquear o permitir y sobre la que puede informar. Estos servicios permiten a los usuarios finales disfrazar el tráfico saliente como consultas DNS, lo que podría infringir el uso aceptable, la prevención de pérdida de datos o las políticas de seguridad. Como resultado, estos servicios suponen una posible amenaza para la seguridad y reducen la visibilidad general de su entorno.

Con esta categoría de seguridad que proporciona una visibilidad inmediata, puede reducir el

riesgo de tunelación DNS y la posible pérdida de datos. Puede bloquear esta categoría directamente o simplemente supervisar los resultados en los informes; esto proporciona la flexibilidad necesaria para determinar cuál es el enfoque adecuado para abordar el problema, en función de su tolerancia al riesgo, uso aceptable o políticas de RR. HH.

## Activación de VPN de túnel DNS

Esta categoría de seguridad se puede activar como cualquier otra en Políticas > Configuración de seguridad, editando a continuación una configuración de seguridad existente. O bien, se puede hacer dentro del asistente de configuración de políticas en sí:



The screenshot shows a configuration window for a security policy. 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 configuration area, there are two buttons: 'CANCEL' and 'SAVE'.

115014823666

La tunelización DNS se puede filtrar a través del informe de búsqueda de actividad:

## Security Categories

Select All

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

APPLY

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).