# Configuración de Umbrella Roaming Client en una red de la empresa

## Contenido



## Introducción

Este documento describe la configuración del cliente de roaming de Umbrella en la red de su empresa.

## Overview

El cliente de roaming de Umbrella es una gran herramienta para proteger a los usuarios remotos, pero también puede proteger a los usuarios de su red corporativa, lo que agrega otra capa de seguridad. En función de las necesidades de la empresa, algunos administradores desean la protección continuada del cliente de roaming de Umbrella en la red corporativa, mientras que otros administradores prefieren que el cliente de roaming de Umbrella se retire en favor de otras políticas de Umbrella.

Umbrella ofrece flexibilidad sobre cómo funciona el cliente de roaming de Umbrella cuando entra en su red. En este artículo se esbozan estos enfoques diferentes.

## Objetivos

P). ¿Por qué debería desactivar el cliente de roaming de Umbrella en la red de mi empresa?

Normalmente no es necesario deshabilitar el cliente de roaming de Umbrella para que funcione con DNS interno y externo. El cliente de roaming de Umbrella utiliza la función Domain Management para dirigir el tráfico DNS interno a los servidores DNS normales. Esto le permite conservar la protección y la conectividad mientras el cliente de roaming de Umbrella se ejecuta en los terminales de la red.

Sin embargo, a veces hay razones para considerar la inhabilitación de la protección del cliente de roaming...

- Proporcionar una política diferente "*dentro de la red*" y "*fuera de la red*" a los usuarios de roaming que abandonan la red.
- El uso de un servidor DNS interno en la red de una empresa ofrece algunas ventajas en términos de almacenamiento en caché y reducción del tráfico DNS saliente.
- El cliente de roaming de Umbrella envía periódicamente mensajes de sondeo para verificar la conexión con Umbrella. Este tráfico adicional puede no ser deseado cuando tiene un gran número de clientes.

P) ¿Por qué querría que el cliente de roaming de Umbrella permaneciera activado en la red de mi empresa?

Por otro lado, hay algunas buenas razones para mantener el cliente de roaming habilitado en todo momento:

- Asegúrese de que el equipo cliente de roaming de Umbrella utiliza la misma directiva en todo momento.
- Tener siempre el nombre de host del cliente de roaming de Umbrella identificable en los informes (en lugar de la identidad de la red), para informes granulares.
- El cliente de roaming utiliza tráfico 'DNS cifrado' para mejorar la privacidad
- Para los usuarios del gateway web seguro (mediante AnyConnect), el cliente debe permanecer activado para proporcionar el filtrado web SWG.

## Modos de funcionamiento

Siempre activo

El cliente de roaming de Umbrella puede permanecer activado incluso cuando se utiliza en la red de la empresa. En este modo, las políticas se configuran mediante la identidad de cliente de itinerancia de Umbrella y esta identidad aparece en los informes.

| | |
|---|---|
| Política | La identidad de cliente de roaming de Umbrella se utiliza siempre. |
| Informes | La identidad del cliente de roaming de Umbrella siempre aparece en los informes que ofrecen granularidad por equipo |
| Tráfico DNS | • El cliente de roaming de Umbrella continúa enviando consultas de DNS directamente a Umbrella, incluso cuando se encuentra en la red de una |

| | |
|---|---|
| | empresa.<br>• Las consultas enviadas a Umbrella están cifradas, lo que proporciona seguridad adicional.<br>• Las consultas de 'Dominios internos' se enrutan a sus servidores DNS normales y no se envían a Umbrella. |
| Mensajes de sondeo | El cliente de roaming de Umbrella continúa enviando mensajes de sondeo para determinar la disponibilidad de Umbrella. |

Cómo configurar el modo 'Siempre activo':

1. Vaya a Identidades > Equipos en roaming.
2. Haga clic en el icono (Configuración del cliente de roaming).
3. Desactive Disable DNS redirection while on an Umbrella Protected Network y haga clic en Save.
4. Cree una política independiente para sus clientes de roaming de Umbrella y asegúrese de que sea la prioridad más alta (la más alta de la lista). La política de cliente de roaming de Umbrella debe tener una prioridad mayor que cualquier política basada en identidades de red.

Usar política de red normal
El cliente de roaming de Umbrella está habilitado y continúa hablando directamente con Umbrella; sin embargo, la identidad de red se utiliza tanto para políticas como para informes. Este modo se activa simplemente colocando la política de red en una prioridad más alta que la política de cliente de roaming de Umbrella.

| | |
|---|---|
| Política | La política de red se utiliza cuando está en la red protegida. Esto permite diferentes políticas de conexión/desconexión de la red. |
| Informes | • Los informes se asocian a la identidad de red como la identidad principal.<br>• Los informes todavía le permiten buscar a través del nombre de host del cliente de roaming de Umbrella para filtrar los resultados solo para ese cliente. |

| | |
|---|---|
| |  |
| Tráfico DNS | • El cliente de roaming de Umbrella continúa enviando consultas de DNS directamente a Umbrella, incluso cuando se encuentra en la red de una empresa.<br>• Las consultas enviadas a Umbrella están cifradas, lo que proporciona seguridad adicional.<br>• Las consultas de 'Dominios internos' se enrutan a sus servidores DNS normales y no se envían a Umbrella. |
| Mensajes de sondeo | El cliente de roaming de Umbrella continúa enviando mensajes de sondeo para determinar la disponibilidad de Umbrella. |

Cómo 'Utilizar la Política de Red Regular':

1. Vaya a Identidades > Equipos en roaming.
2. Haga clic en el icono (Configuración del cliente de roaming).
3. Desactive Disable DNS redirection while on an Umbrella Protected Network y haga clic en Save.
4. Cree una política independiente para su red o redes. Asegúrese de que la política de su red tenga mayor prioridad que cualquier política basada en el cliente de roaming.

Desactivar tras redes protegidas (ideal para redes más pequeñas)
El cliente de roaming de Umbrella puede 'retroceder' cuando detecta que está en una red protegida. Esto significa que la identidad de la red se utiliza tanto para políticas como para informes.

Este modo es similar en comportamiento al modo 'Usar política de red regular' excepto que el cliente de roaming de Umbrella se inhabilita a sí mismo y no interfiere con el tráfico DNS.

| | |
|---|---|
| Política | La política de red se utiliza cuando está en la red protegida. Esto permite diferentes políticas de conexión/desconexión de la red. |

| | |
|---|---|
| Informes | En la red protegida, no hay granularidad por equipo para los informes. Los informes solo se asocian a la identidad de red. |
| Tráfico DNS | Cuando está en la red protegida, el cliente de roaming de Umbrella no interfiere con las consultas DNS y éstas van al servidor DNS interno normal. |
| Mensajes de sondeo | El cliente de roaming de Umbrella continúa enviando mensajes de sondeo para determinar que se encuentra en una red protegida. |

Cómo configurar Disable behind protected networks:

1. Vaya a Identidades > Equipos en roaming.
2. Haga clic en el icono (Configuración del cliente de roaming).
3. Seleccione Disable DNS redirection while on an Umbrella Protected Network y haga clic en Save.
4. Navegue hasta Políticas > Lista de Políticas.
5. Cree una política independiente para su red o redes. Asegúrese de que la política de su red tenga mayor prioridad que cualquier política basada en el cliente de roaming de Umbrella.
6. Los servidores DNS locales deben reenviarse a los resolvers de Umbrella y deben estar registrados correctamente en el panel de Umbrella.
7. Para que esta función funcione, la IP de salida utilizada por la estación de trabajo cliente debe estar registrada con la misma identidad de red que la IP de salida utilizada por los servidores DNS internos. Para obtener más información, consulte este artículo.

Deshabilitar detrás de dominio de red de confianza (ideal para redes más grandes)

Ahora es posible elegir un 'dominio de red de confianza' configurado por el cliente. El cliente intenta resolver este dominio DNS (registro A) y deshabilitar la protección cuando el dominio se resuelve correctamente.  Se ha diseñado para ser un registro DNS solo interno que solo se resuelve cuando el cliente está en la red de la empresa.

| | |
|---|---|
| Política | El cliente se retira cada vez que se detecta el dominio de confianza y no recibe necesariamente la política o el filtrado de Umbrella.  Recomendamos añadir otras funciones de Umbrella (p. ej. Protección de la red) para garantizar que la política se sigue aplicando en la red de la empresa. |

| | |
|---|---|
| Informes | El cliente se retira cada vez que se detecta el dominio de confianza y no recibe necesariamente la política o el filtrado de Umbrella. Si la red está protegida por otras funciones de Umbrella (p. ej. Protección de red), el tráfico aparece en los informes bajo la identidad de la red. |
| Tráfico DNS | Cuando está en la red de confianza, el cliente de roaming de Umbrella no interfiere con las consultas DNS y éstas van al servidor DNS interno normal. |
| Mensajes de sondeo | El cliente de roaming de Umbrella inhabilita la mayoría de sus pruebas de 'sondeo' DNS en este estado, lo que reduce en gran medida la cantidad de tráfico generado por los clientes de roaming. |

Cómo configurar Trusted Network Domain:

1. Cree un registro A de DNS en sus servidores DNS internos (p. ej. magic.mydomain.tld).
    1. El registro debe ser un "subdominio" (3 etiquetas DNS como mínimo)
    2. El registro debe resolver una dirección RFC-1918 interna
    3. Tenga cuidado de asegurarse de que el registro no existe públicamente
2. Vaya a Identidades > Equipos en roaming.
3. Haga clic en el icono (Configuración del cliente de roaming).
4. Seleccione la opción Trusted Network Domain e ingrese el nombre de dominio (por ejemplo, magic.mydomain.tld). Click Save.

## Uso del cliente de roaming de Umbrella con un dispositivo virtual de Umbrella

Como parte del producto Umbrella 'Insights' (en los paquetes Platform y Insights), proporcionamos un Virtual Appliance (VA) que actúa como reenviador DNS dentro de su red. Este AV es la clave para obtener visibilidad sobre el origen de las solicitudes DNS en su red y también es necesario para nuestra integración con Active Directory.

De forma predeterminada, el cliente de roaming de Umbrella se deshabilita a sí mismo si detecta que se está utilizando un VA para el reenvío de DNS. Si el VA se ha asignado como el servidor DNS (ya sea mediante DHCP o parámetros estáticos), el cliente de roaming de Umbrella detecta esto y se deshabilita a sí mismo.

Retroceso de VA

| | |
|---|---|
| Política | Con el retroceso de VA activado, la identidad de VA se utiliza para decidir la política elegida. Se pueden crear políticas basadas en las siguientes identidades:<br>• Usuario de AD (solo si está habilitada la integración de AD)<br>• Equipo AD (solo si está habilitada la integración AD)<br>• Red interna<br>• Nombre del sitio de paraguas.<br>Haga clic aquí para obtener más información sobre la precedencia de las políticas. |
| Informes | Con la función de retroceso de VA activada, el cliente de roaming de Umbrella se desactiva cuando está detrás de un VA y no se muestra en los informes. Los informes se registran como:<br>• Usuario de AD (solo si está habilitada la integración de AD)<br>• Equipo AD (solo si está habilitada la integración AD)<br>• Red interna<br>• Nombre del sitio de paraguas.<br>Además, la dirección IP interna del cliente se registra para cada solicitud.<br>  |
| Tráfico DNS | • El cliente de itinerancia de Umbrella no interfiere con las consultas DNS y se dirigen al dispositivo virtual.<br>• El VA reenvía las consultas de DNS externo a Umbrella (cifrado).<br>• El dispositivo virtual enruta las consultas DNS internas según corresponda y las reenvía a los servidores DNS internos configurados. |
| Mensajes de sondeo | El cliente de roaming de Umbrella sigue enviando mensajes de sondeo a Umbrella, pero lo hace a una velocidad reducida. |

Cómo configurar VA Backoff:

1. Esta función está activada de forma predeterminada, pero puede comprobar su estado (y opcionalmente desactivarla)
2. Vaya a Identidades > Equipos en roaming.
3. Haga clic en el icono (Configuración del cliente de roaming).
4. Seleccione la opción VA Backoff.

# Módulo de seguridad de roaming Cisco Umbrella AnyConnect

El módulo Umbrella para Cisco AnyConnect admite todos los modos operativos descritos anteriormente. También hay disponibles dos modos adicionales específicos de AnyConnect. Ambos modos se pueden habilitar en el panel de Umbrella en la página Identidades > Equipos en roaming; sin embargo, se requiere una configuración adicional en el perfil VPN de AnyConnect.

- Respete la detección de redes de confianza de AnyConnect.
  Esta función hace que el módulo Umbrella Security se desactive cuando Cisco AnyConnect determina que se encuentra en una red de confianza. Esto se basa en la función Trusted Network Detection de AnyConnect para identificar la red. Los dominios de confianza, los servidores DNS y las URL se pueden utilizar para identificar la red de su empresa. Para obtener más información, consulte la documentación de AnyConnect.
- Inhabilite el cliente de roaming mientras las sesiones VPN de túnel completo estén activas
  Con esta función activada, el módulo Umbrella se desactiva cuando AnyConnect está conectado a una VPN de túnel completo (o túnel todo DNS).

Cuando está desactivado, el cliente de roaming no filtra el tráfico DNS, por lo que es importante asegurarse de que su red está cubierta por otro sistema de seguridad, como nuestra función de protección de red.

# Más información

Si desea desactivar el cliente de roaming en la red de su empresa pero necesita más control, o si desea hablar de otras opciones, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

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).