Resolver modos de cliente de roaming sin proteger o sin cifrar

Contenido

Introducción

Este documento describe el significado de los estados Unprotected y Unencrypt en Umbrella Roaming Client y cómo resolver problemas.

Estados no protegidos y no cifrados

Cuando el cliente de roaming de Umbrella está en modo no protegido o no cifrado, el icono de la bandeja (Windows) o la barra de menús (OS X) muestran un estado amarillo. El estado se muestra como Sin protección y Sin cifrar.

Requisitos de comunicación

Para proporcionar seguridad y filtrado de contenido, el cliente de roaming de Umbrella debe comunicarse con Umbrella mediante UDP y TCP en los puertos y destinos proporcionados, además de los destinos HTTP enumerados en el artículo Requisitos previos del cliente de roaming:

Puerto	Protocolo	IPv4	IPv6
53	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
53	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35

El cliente de roaming de Umbrella no puede proteger el equipo si se dan estas dos condiciones:

- El equipo está detrás de una conexión que no permite solicitudes DNS de terceros.
- El equipo se encuentra detrás de una conexión que tiene una directiva predeterminada de denegación de firewall de salida.

Cuando se cumplen estas condiciones, el cliente de roaming de Umbrella restaura los servidores DNS delegados por DHCP en las propiedades de conexión de red y continúa con las pruebas hasta que puede ponerse en contacto con los servidores DNS de Umbrella y volver a proporcionar seguridad y filtrado de contenido. Durante los períodos en los que no es posible la comunicación con los servidores DNS de Umbrella, no están disponibles la aplicación de políticas y la generación de informes.

Prueba de Conectividad de Red

Para comprobar si la red permite la comunicación con los servidores DNS de Umbrella, realice manualmente una consulta DNS. Si la red bloquea consultas, el resultado es:

```
$ nslookup opendns.com 208.67.222.222
;; connection timed out; no servers could be reached
```

Si la prueba se realiza correctamente, pero el cliente de roaming de Umbrella sigue indicando "Sin protección/Sin cifrar", abra un vale de soporte y proporcione los resultados de una prueba de diagnóstico. Una consulta correcta aparece como:

```
$ nslookup opendns.com 208.67.222.222
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: opendns.com
```

Sólo estado no cifrado

Si el cliente de roaming de Umbrella muestra Sin cifrar, no puede comunicarse a través del puerto 443/UDP. Por motivos de seguridad, se recomienda permitir que este puerto atraviese el firewall, pero el cliente sigue funcionando sin consultas DNS cifradas. Para obtener más detalles, consulte el artículo Requisitos previos del cliente de roaming.

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).