Solucionar problemas de aplicaciones que no son de navegador en general

Contenido

Introducción

Este documento describe cómo resolver problemas de aplicaciones que no son de navegador en Cisco Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

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

En este artículo se explican las prácticas recomendadas y los pasos de solución de problemas para configurar aplicaciones que no son de explorador para que funcionen con Umbrella Secure

Web Gateway. En la mayoría de los casos, no se requieren cambios de configuración. Sin embargo, algunas aplicaciones no funcionan bien con las funciones de seguridad/inspección (como el descifrado SSL) y se deben agregar excepciones para que la aplicación funcione con un proxy web. Esto se aplica a Umbrella SWG, así como a otras soluciones de proxy web.

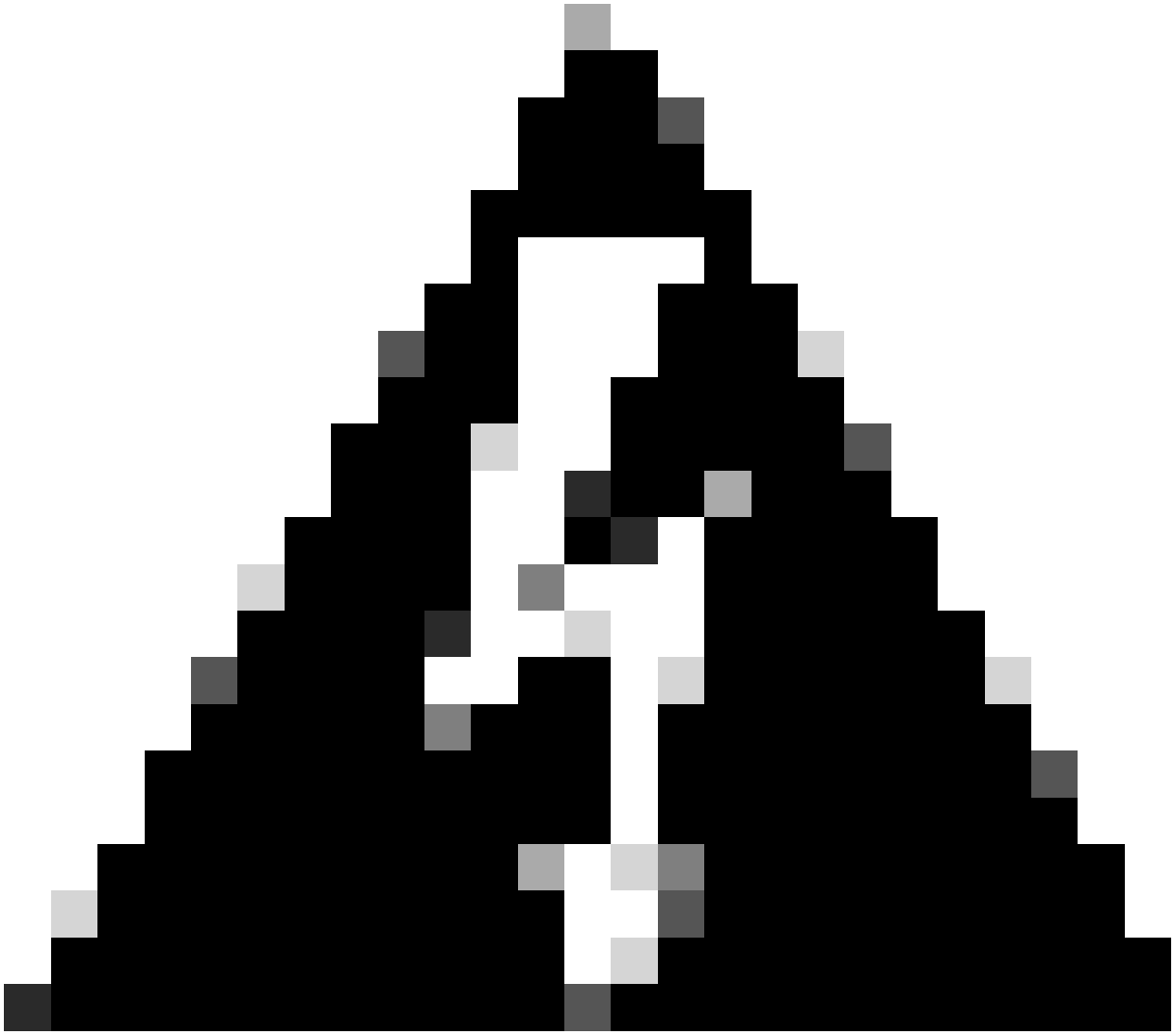
Esto es útil en circunstancias en las que la versión de sitio web/navegador de una aplicación funciona, pero la versión de escritorio/móvil de la aplicación no.

Problemas de compatibilidad

Las aplicaciones pueden ser incompatibles por los siguientes motivos:

Instalación de Umbrella Root CA	La CA raíz de Cisco Umbrella siempre debe ser confiable para conexiones TLS incorrectas. • Solución: Para las aplicaciones que no son web, asegúrese de que la CA raíz de Cisco Umbrella sea de confianza en el almacén de certificados del sistema/equipo local.
Fijación de certificados	La fijación de certificados (PKP) se produce cuando la aplicación espera recibir una hoja precisa (o certificado de CA) para validar el intercambio de señales de TLS. La aplicación no puede aceptar un certificado generado por un proxy web y no es compatible con las funciones de descifrado SSL. • Solución: Omitir la aplicación o el dominio del descifrado SSL mediante una lista de descifrado selectivo (consulte Advertencia después de la tabla) Puede encontrar más detalles sobre las aplicaciones que se sabe que se ven afectadas por la fijación de certificados aquí: Fijación de clave pública/Fijación de certificados
Compatibilidad con versión TLS	La aplicación puede utilizar una versión/cifrado de TLS anterior que SWG no admite por motivos de seguridad. • Solución: Evite que el tráfico se envíe a Umbrella mediante la función Dominios externos (PAC/AnyConnect) o exclusiones de VPN (túnel) (consulte Advertencia después de la tabla).
Protocolo no web	Algunas aplicaciones utilizan protocolos que no son http(s), pero siguen enviando estos datos a través de los puertos web comunes interceptados por SWG. SWG no puede entender este tráfico. • Solución: Consulte con el proveedor de la aplicación para determinar las direcciones de destino o los intervalos de IP que utiliza el software. Este software debe excluirse de SWG mediante dominios externos

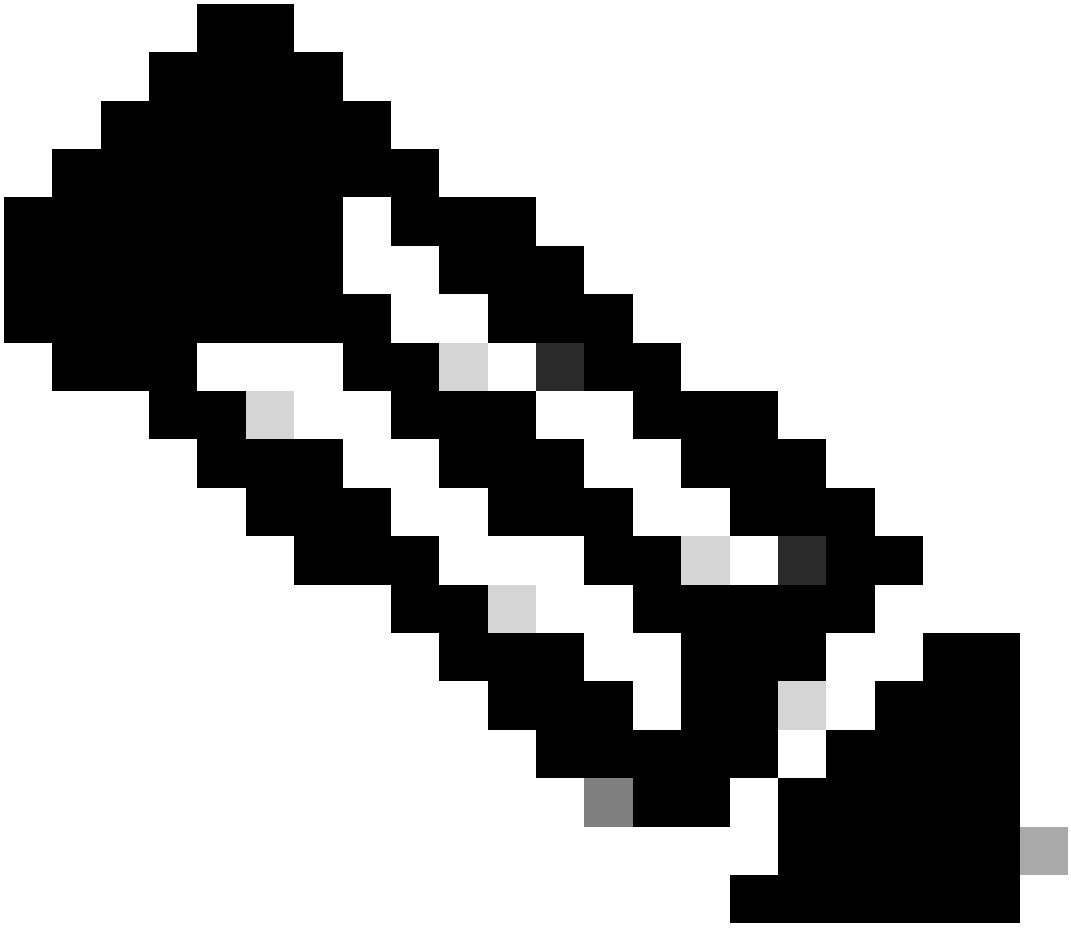
	(PAC/AnyConnect) o exclusiones de VPN (túnel) (consulte Advertencia después de la tabla).
Autenticación SAML	La mayoría de las aplicaciones que no son navegadores no pueden realizar la autenticación SAML. Umbrella no desafía las aplicaciones que no son navegadores para SAML y, por lo tanto, las políticas de filtrado basadas en usuario/grupo no pueden coincidir. • Solución: Habilite la función Sustitutos IP para que la información del usuario se pueda almacenar en caché para su uso con aplicaciones que no sean del explorador. • Alternativa: Permitir la aplicación/dominio en una regla web basada en identidades de red o túnel (no usuarios/grupos).
Solicitudes de rango HTTP	Algunas aplicaciones utilizan solicitudes HTTP "Byte-Range" al descargar datos; lo que significa que sólo se descarga una pequeña parte del archivo a la vez. Estas solicitudes están desactivadas por motivos de seguridad en SWG, ya que esta técnica también se puede utilizar para omitir la detección antivirus. • Solución (HTTPS): Omitir la aplicación o el dominio del descifrado SSL* en Umbrella mediante listas de descifrado selectivo. • Solución (HTTP): Omita la aplicación o el dominio del análisis antivirus* mediante una regla web con la opción Override Security. • Alternativa: Póngase en contacto con el servicio de asistencia de Umbrella si desea activar las solicitudes Range de forma predeterminada* para su organización.
Compatibilidad explícita de proxy	Algunas aplicaciones no respetan la configuración de proxy del sistema (p. ej. PAC) y, por lo general, no son compatibles con proxies web explícitos. Estas aplicaciones no se enrutan a través de Umbrella SWG en una implementación de archivo PAC. • Solución: La aplicación debe estar permitida a través del firewall de la red local. Consulte al proveedor de la aplicación para obtener más información sobre los destinos/puertos que se permitirán.



Advertencia: La creación de estas excepciones puede desactivar las funciones de inspección de seguridad, incluidos el análisis antivirus, el análisis de DLP, los controles de arrendatarios, el control de tipo de archivo y la inspección de URL. Solo debe hacerlo si está satisfecho de confiar en el origen de estos archivos. La necesidad empresarial de la aplicación debe sopesarse frente al impacto en la seguridad que supone la desactivación de estas funciones.

Aplicaciones de Microsoft 365

La función de compatibilidad de Microsoft 365 excluye automáticamente varios dominios de Microsoft de las funciones de descifrado SSL y aplicación de políticas. Esta función se puede habilitar para resolver problemas con la versión de escritorio de las aplicaciones de Microsoft. Para obtener más información, consulte Administración de la configuración global.

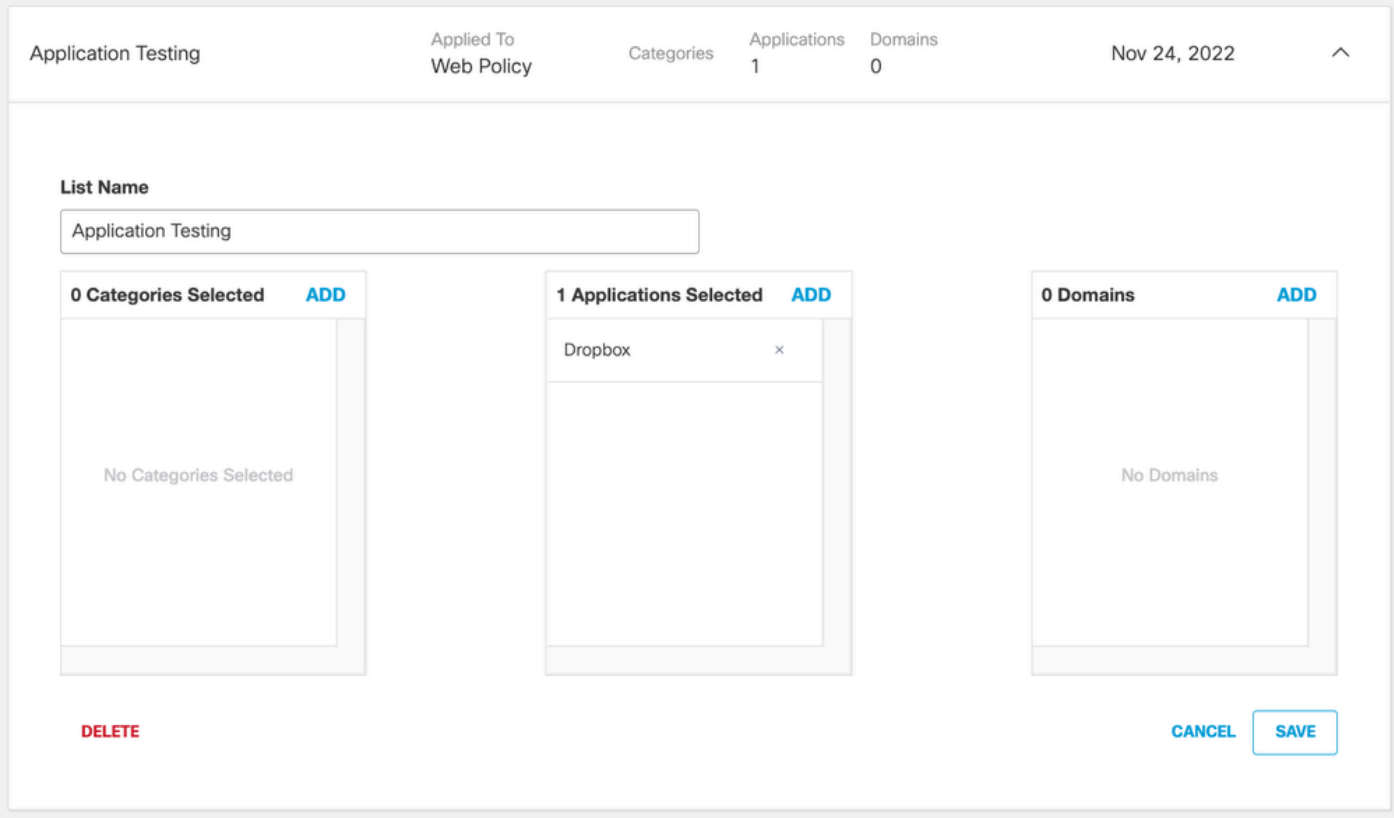


Nota: La función de compatibilidad de Microsoft 365 no excluye todos los dominios de Microsoft. Umbrella utiliza las recomendaciones de Microsoft para la lista de dominios que deben excluirse del filtrado. Para obtener más información, vea Nuevas categorías de terminales de Office365.

Omisión de fijación de certificado

La fijación de certificados (PKP) es una causa común de problemas de compatibilidad de aplicaciones. Cisco proporciona una lista completa de las aplicaciones denominadas que se pueden configurar para omitir el descifrado SSL y obtener una solución alternativa. El descifrado selectivo se puede configurar en Políticas > Listas de descifrado selectivo.

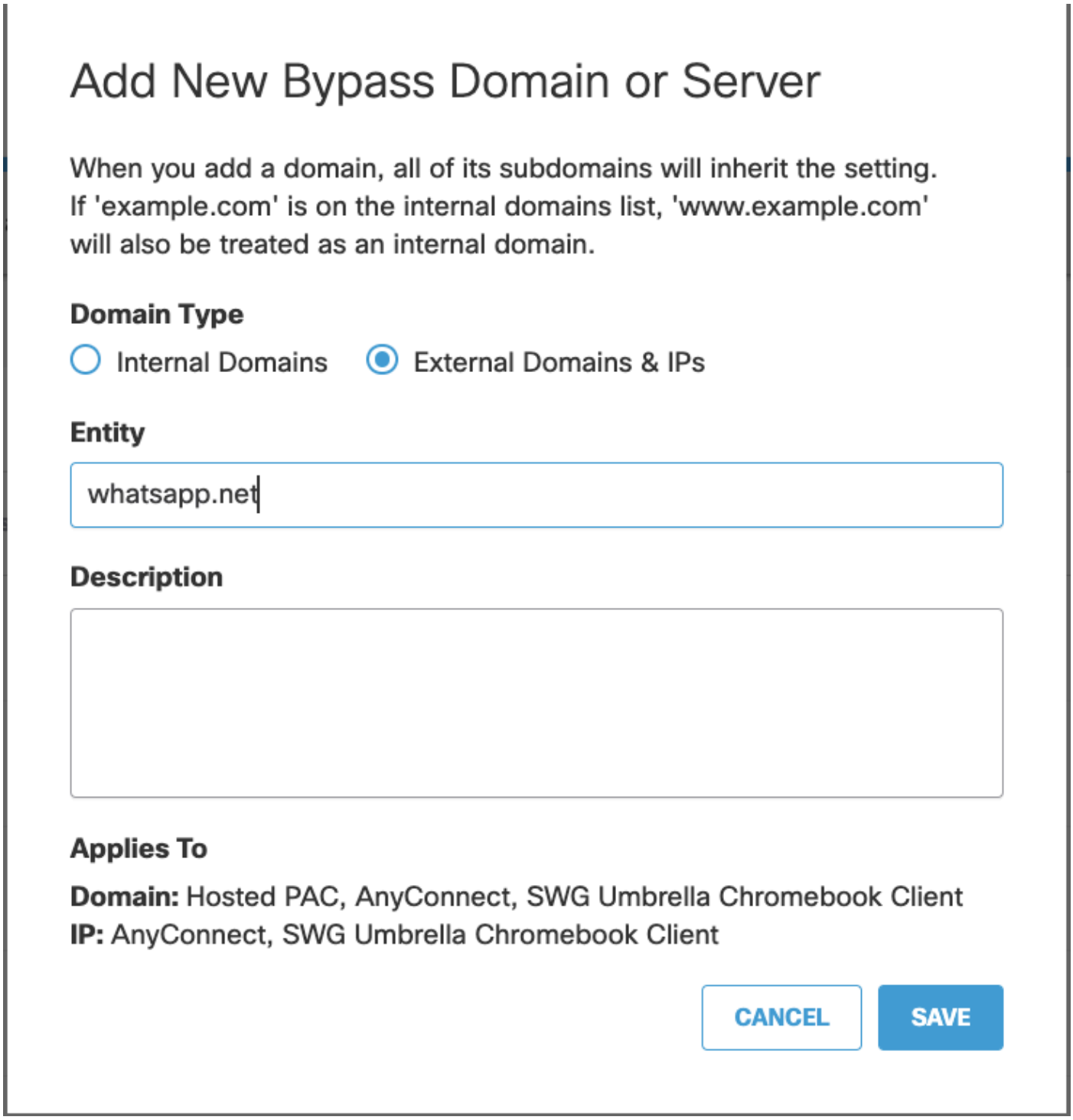
En la mayoría de los casos, el administrador puede resolver los problemas de fijación de certificados simplemente excluyendo la aplicación por su nombre. Esto significa que estos problemas se pueden resolver sin tener que aprender o mantener listas de dominios.



Alternativamente, las aplicaciones se pueden omitir en función del dominio de destino/dirección IP. Póngase en contacto con el proveedor de la aplicación para determinar la lista aplicable de dominios/direcciones IP o consulte Identificación de exclusiones para la fijación de certificados.

Desvío de compatibilidad TLS

Las versiones de TLS antiguas o personalizadas son una causa común de problemas de compatibilidad de aplicaciones. Estos problemas se pueden resolver excluyendo el tráfico de Umbrella en Implementaciones > Administración de dominios > Dominios externos e IP. En un despliegue de túnel, el tráfico sólo se puede excluir agregando excepciones en la configuración VPN.



Póngase en contacto con el proveedor de la aplicación para determinar la lista aplicable de dominios/direcciones IP que se deben excluir o consulte "Identificación de exclusiones para versiones de TLS incompatibles" (más adelante en este artículo).

Resolución de problemas (avanzada)

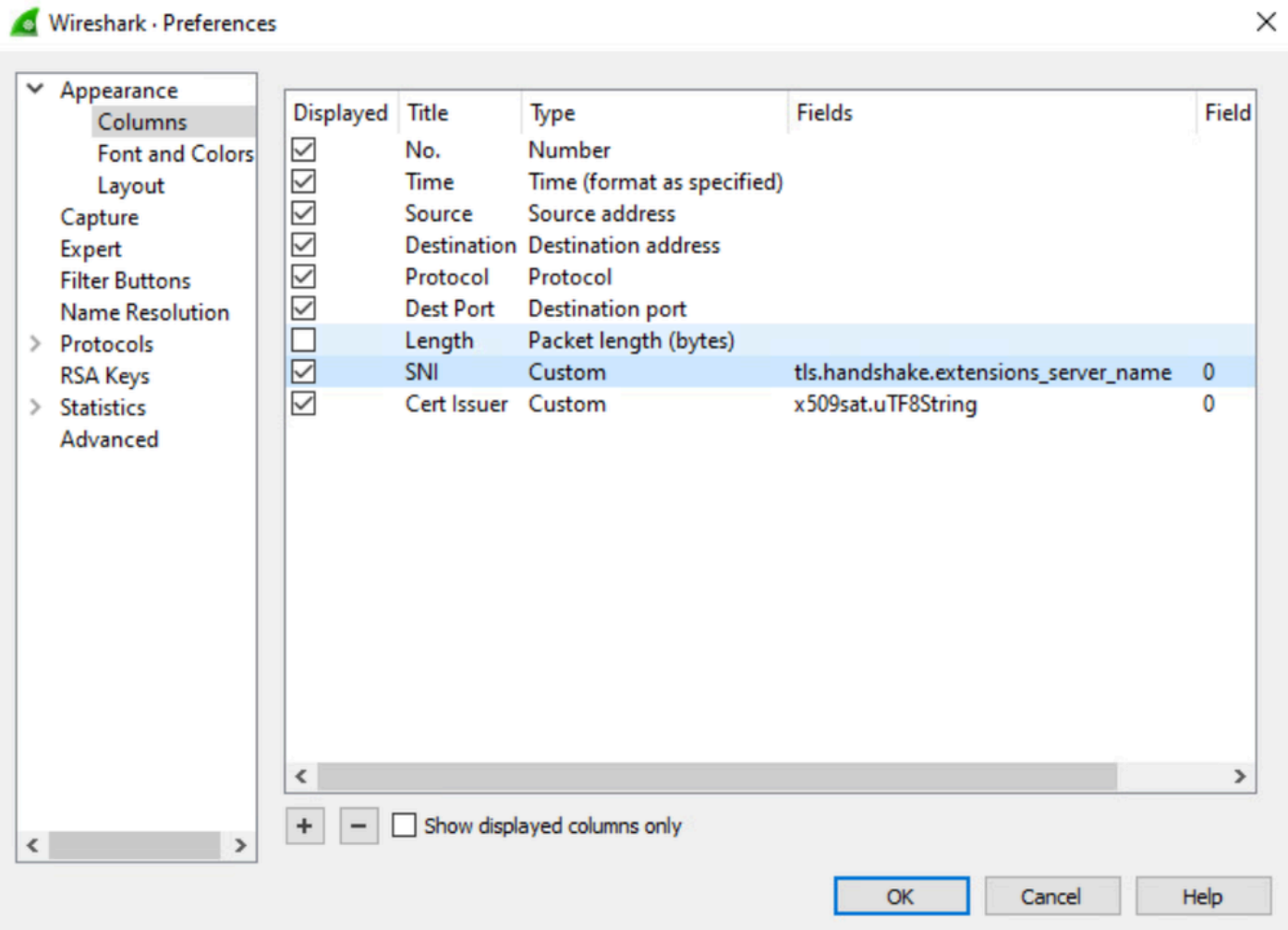
Las instrucciones restantes de este artículo utilizan capturas de paquetes Wireshark (www.wireshark.org) con fines de resolución de problemas. Wireshark puede ayudar a identificar qué dominios utilizan las aplicaciones para ayudar a implementar exclusiones personalizadas. Antes de empezar, agregue estas columnas personalizadas en Wireshark:

1. Descargue Wireshark de [www.wireshark.org.](http://www.wireshark.org)

2. Vaya a Edición > Preferencias > Columnas.

3. Cree columnas de tipo Personalizado con estos campos:

```
http.host
tls.handshake.extensions_server_name
x509sat.uTF8String
```



Para realizar una captura de paquetes, siga estas instrucciones o consulte Captura de tráfico de red con Wireshark.

1. Ejecute Wireshark como administrador.

2. Seleccione las interfaces de red relevantes en Captura > Opciones.

- Para implementaciones PAC/de túnel, realice la captura en la interfaz de red LAN normal.
- Para las implementaciones de AnyConnect, realice capturas en la interfaz de red LAN y en la interfaz de bucle invertido.

3. Cierre todas las demás aplicaciones excepto la aplicación problemática.

4. Vaciar la caché DNS: `ipconfig /flushdns`

5. Inicie la captura de Wireshark.

6. Replique rápidamente el problema y detenga la captura de Wireshark.

Identificar exclusiones para el anclaje de certificados

La fijación de certificados se aplica en el cliente, lo que significa que el comportamiento exacto y los pasos de resolución difieren para cada aplicación. En el resultado de la captura, busque señales indicadoras de que falla una conexión TLS:

- Se está cerrando o restableciendo rápidamente una conexión TLS (RST o FIN).
- Se está reintentando repetidamente una conexión TLS.
- Cisco Umbrella está emitiendo el certificado para la conexión TLS, por lo que se está descifrando.

Estos filtros de Wireshark de ejemplo pueden ayudar a ver los detalles importantes de las conexiones TLS.

Túnel / AnyConnect

```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.rese
```

Encadenamiento de PAC/proxy

```
tcp.port eq 443 && (http.request.method eq CONNECT || tcp.flags.reset eq 1)
```

En este ejemplo, la aplicación de escritorio DropBox se ve afectada por la fijación de certificados al intentar conectarse a client.dropbox.com.

(tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.reset eq 1 || tcp.flags.fin eq 1)

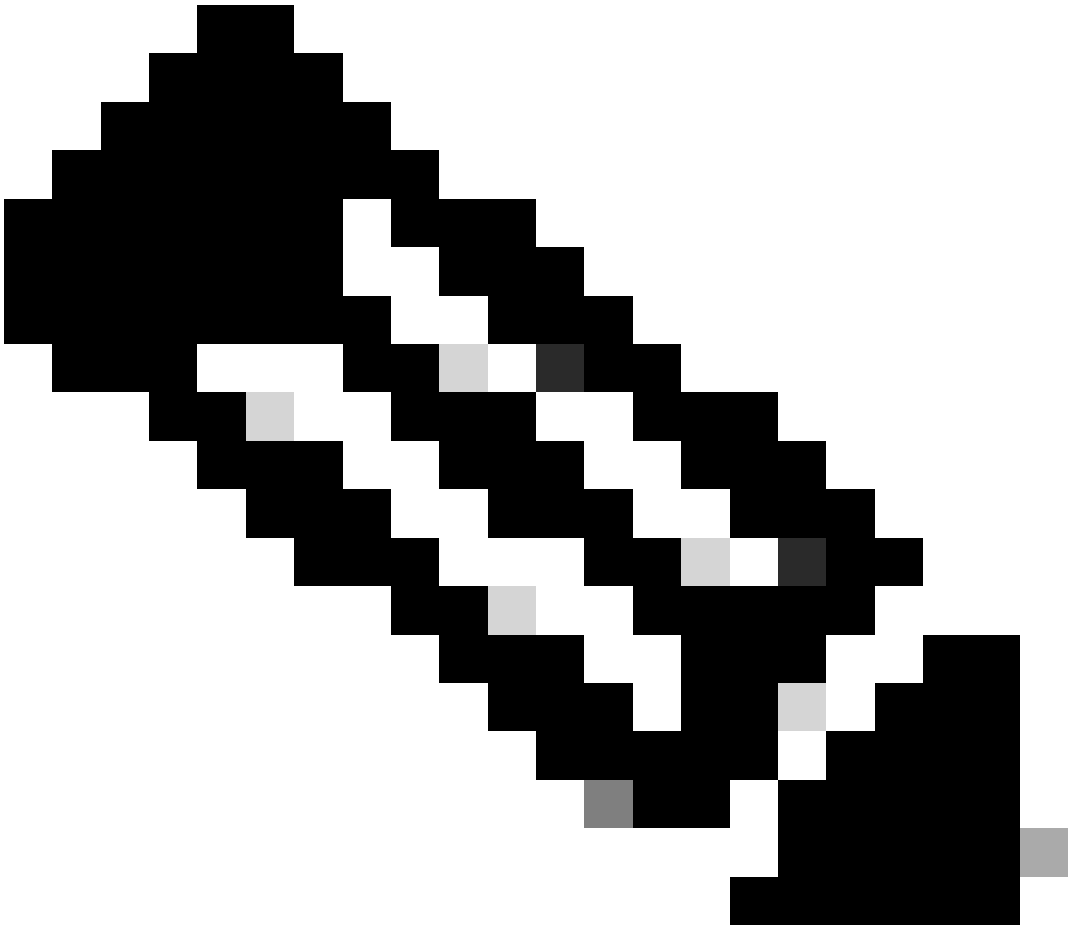
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148		443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
292	43.141656	162.125.6.13	10.10.199.101	TLSv1.2	65149		Certificate, Server Key Exchange, Server Hello Done
296	43.175867	10.10.199.101	162.125.6.13	TCP	443		65149 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
297	43.211415	162.125.6.13	10.10.199.101	TCP	65149		443 → 65149 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
306	46.361407	13.107.21.200	10.10.199.101	TCP	65123		443 → 65123 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
309	46.458616	13.107.21.200	10.10.199.101	TCP	65125		443 → 65125 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
315	48.228572	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
320	48.272897	162.125.6.13	10.10.199.101	TLSv1.2	65151		Certificate, Server Key Exchange, Server Hello Done
324	48.315138	10.10.199.101	162.125.6.13	TCP	443		65151 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
326	48.346412	162.125.6.13	10.10.199.101	TCP	65151		443 → 65151 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
330	48.357435	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
335	48.408976	162.125.6.13	10.10.199.101	TLSv1.2	65152		Certificate, Server Key Exchange, Server Hello Done
339	48.449204	10.10.199.101	162.125.6.13	TCP	443		65152 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
341	48.483947	162.125.6.13	10.10.199.101	TCP	65152		443 → 65152 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
345	48.514224	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
350	48.555627	162.125.6.13	10.10.199.101	TLSv1.2	65153		Certificate, Server Key Exchange, Server Hello Done
354	48.595411	10.10.199.101	162.125.6.13	TCP	443		65153 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261888 Len=0
356	48.631537	162.125.6.13	10.10.199.101	TCP	65153		443 → 65153 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
360	48.641737	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
365	48.685384	162.125.6.13	10.10.199.101	TLSv1.2	65154		Certificate, Server Key Exchange, Server Hello Done
369	48.742518	10.10.199.101	162.125.6.13	TCP	443		65154 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
370	48.779104	162.125.6.13	10.10.199.101	TCP	65154		443 → 65154 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
375	50.854534	10.10.199.101	172.217.15.110	TCP	443		64903 → 443 [FIN, ACK] Seq=2 Ack=74 Win=1020 Len=0
376	50.888092	172.217.15.110	10.10.199.101	TCP	64903		443 → 64903 [FIN, ACK] Seq=74 Ack=3 Win=83 Len=0
381	53.801686	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
387	53.845602	162.125.6.13	10.10.199.101	TLSv1.2	65156		Certificate, Server Key Exchange, Server Hello Done
390	53.888995	10.10.199.101	162.125.6.13	TCP	443		65156 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261120 Len=0
392	53.919018	162.125.6.13	10.10.199.101	TCP	65156		443 → 65156 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
396	53.929107	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
402	53.972689	162.125.6.13	10.10.199.101	TLSv1.2	65157		Certificate, Server Key Exchange, Server Hello Done
405	54.011019	10.10.199.101	162.125.6.13	TCP	443		65157 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261120 Len=0
406	54.047260	162.125.6.13	10.10.199.101	TCP	65157		443 → 65157 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0

Destination IP

Server Name

Retries

FIN Flag



Nota: Después de agregar las exclusiones necesarias, puede repetir estos pasos varias

veces para identificar todos los destinos utilizados por la aplicación.

Identificar exclusiones para versiones de TLS incompatibles

Busque conexiones SSL/TLS que no utilicen los protocolos TLS1.2+ obligatorios admitidos por Umbrella SWG. Esto puede incluir protocolos heredados (TLS1.0 o anterior) o protocolos personalizados implementados por una aplicación.

Este filtro de ejemplo muestra los paquetes de intercambio de señales TLS iniciales junto con las consultas DNS.

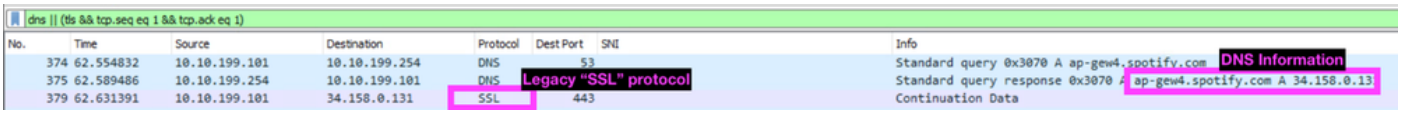
Túnel / AnyConnect

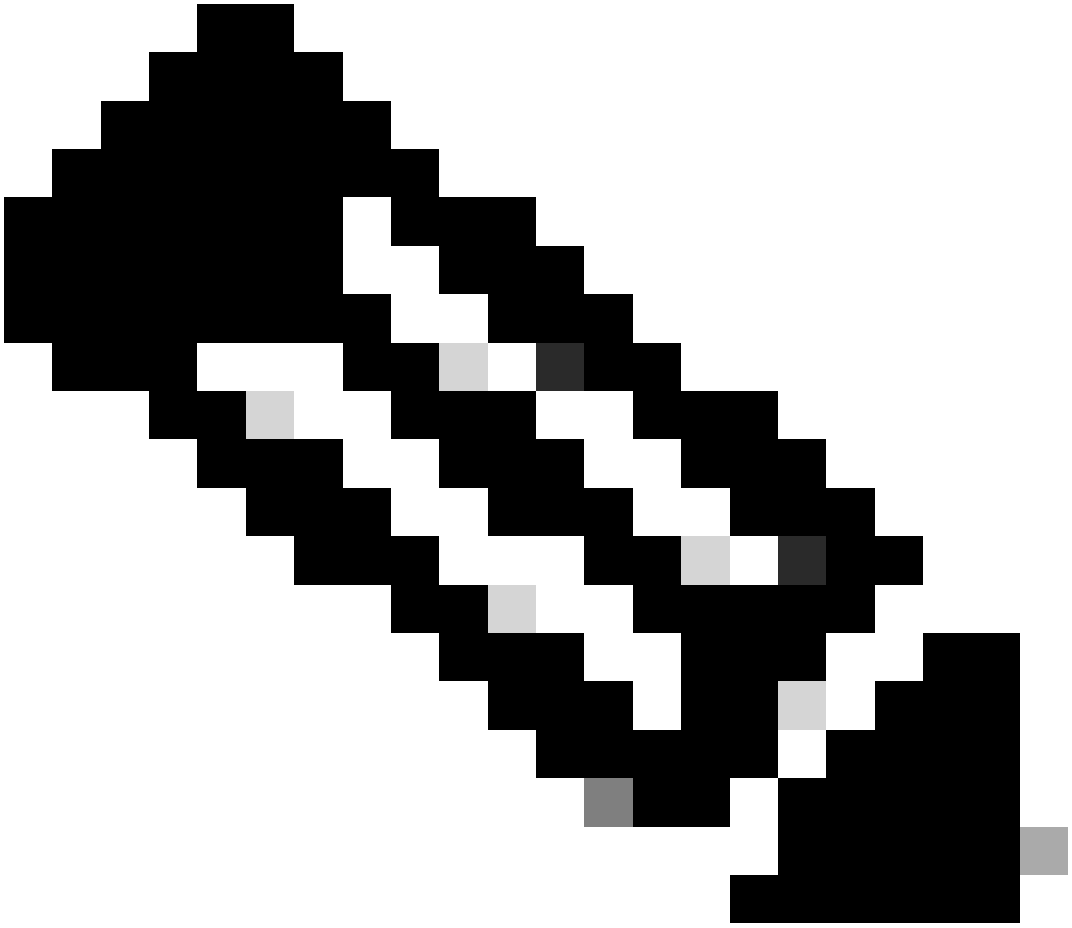
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

Encadenamiento de PAC/proxy

```
dns || http.request.method eq CONNECT
```

En este ejemplo, la aplicación de escritorio de Spotify está intentando conectarse a ap-gew4.spotify.com mediante un protocolo "SSL" no estándar o heredado que no se puede enviar a través de SWG.





Nota: Después de agregar las exclusiones necesarias, puede repetir estos pasos varias veces para identificar todos los destinos utilizados por la aplicación.

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).