Resolución de Problemas de HSTS y Errores de Pinning Certificate

Contenido

Introducción

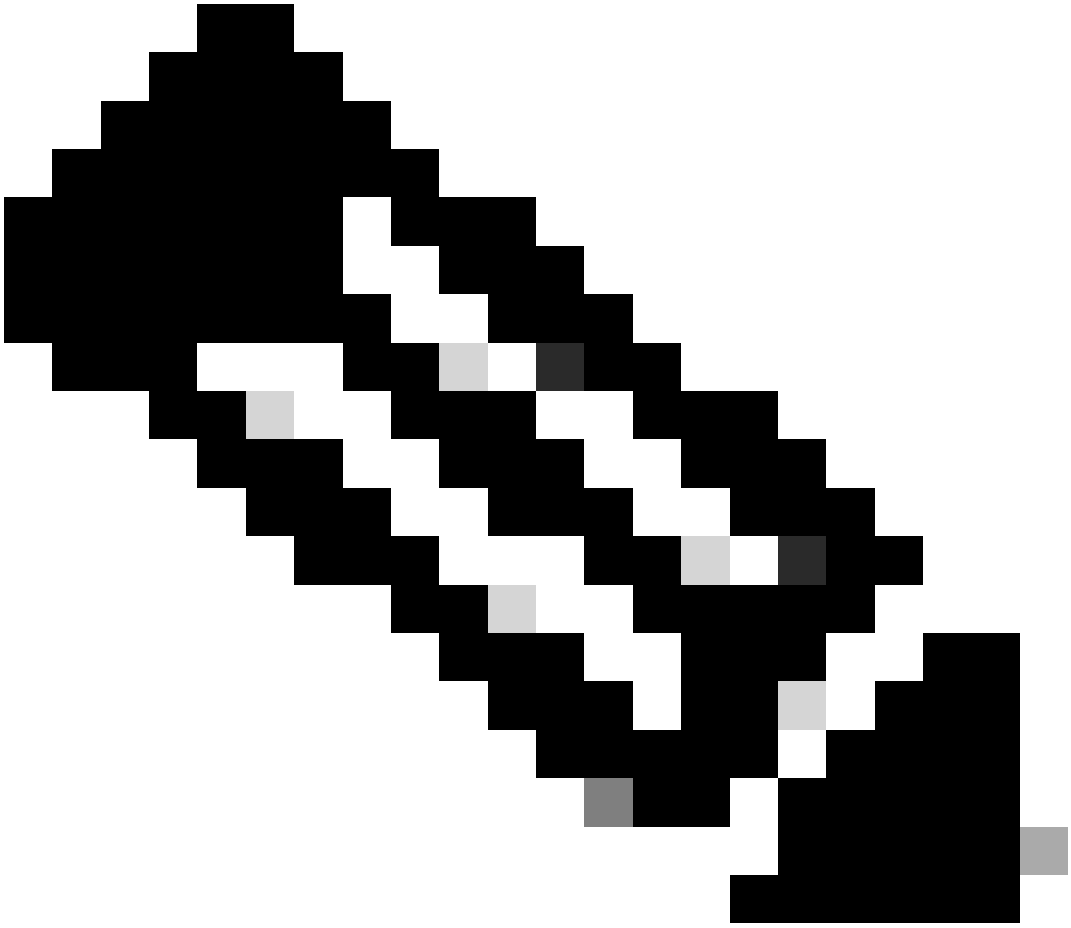
Este documento describe cómo borrar un error de certificado "Su conexión no es de confianza/no es privada" que no se puede eludir.

Error de certificado

Cuando aparezca un error de certificado para `*.opendns.com` o `*.cisco.com` pero no se pueda omitir agregando una excepción de certificado como se describe en la documentación de Cisco Umbrella Administrar el certificado raíz de Cisco Umbrella, siga estos pasos para permitir que se borre el error de certificado.

Cuando no puede omitir el error de certificado agregando una excepción, esto se debe a la implementación de HTTP Strict Transport Security (HSTS) o a la fijación de certificados precargada en exploradores modernos. La comunicación entre ciertos navegadores y ciertos sitios web se realiza de una manera que incluye el requisito de utilizar HTTPS y no es posible realizar ninguna excepción o derivación. Esta seguridad adicional para las páginas HTTPS evita que la página de bloqueo de Umbrella y el mecanismo de la página de bloqueo de bypass funcionen cuando HSTS está activo para un sitio web.

Como resultado, no se puede acceder a la página en cuestión a través de Block Page Bypass (BPB) (de hecho, es posible que la pantalla Bypass ni siquiera aparezca). Estos métodos pueden permitir el acceso al inicio de sesión de BPB, pero después del inicio de sesión, el error de certificado vuelve a aparecer y deniega el acceso. Revise el resto de este artículo si está viendo un error de certificado en Google Chrome, Mozilla Firefox, Safari que no se puede omitir y está tratando de acceder al inicio de sesión de bypass.



Nota: Ya está disponible una solución para este problema que es más fácil de administrar y persistente para todos los sitios.

Como resultado, esta información sigue siendo aplicable, pero ahora se puede solucionar con una solución permanente. Intente instalar la CA raíz de Cisco mediante la documentación de Cisco Umbrella: Administrar el certificado raíz de Cisco Umbrella

---

IMPORTANTE: Si el dominio se encuentra en la lista anclada de HSTS, no puede agregarse una excepción, ya que la lista es en realidad no omisible si se está ejecutando Chrome, Safari o Firefox (Internet Explorer (IE) no se ve afectado). El desvío de página de bloqueo no funciona para sitios como este. Para obtener una lista completa de los servicios que utilizan HSTS por estos tres navegadores, revise la búsqueda de código de Google Chromium. Entre los servicios destacados de esta lista se incluyen:

- Google (y los recursos de Google, como Gmail, Youtube o Google Docs)
- Dropbox
- Twitter

- Facebook

Si esto le está causando un problema a usted o a sus usuarios y le gustaría ver cambios en el desvío de página de bloqueo para ayudar a aliviar este problema, envíe un correo electrónico a umbrella-support@cisco.com o a su gerente de cuentas para enviar una solicitud de características. Nuestros equipos de ingeniería y gestión de productos son conscientes de las dificultades que presentan los certificados y la omisión de páginas bloqueadas, y están probando rediseños alternativos de esta función.

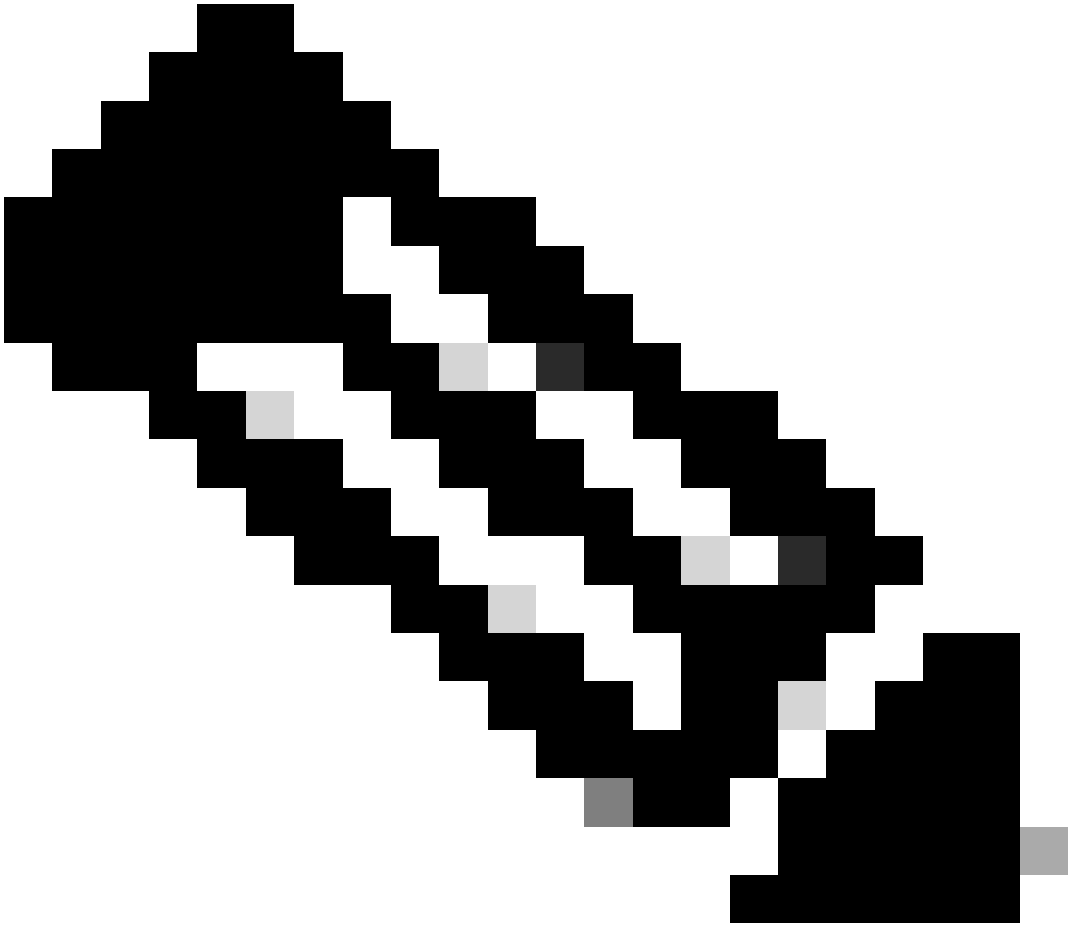
Posibles soluciones

Hay algunas maneras de resolver estos problemas. En primer lugar, estas secciones muestran cómo utilizar políticas más granulares para solucionar este problema. En segundo lugar, puede utilizar configuraciones de explorador, pero éstas se aíslan en un subconjunto de los exploradores afectados por este problema.

Gestión de políticas y el cliente de roaming

Puede haber problemas con la configuración de la red o con la política de uso aceptable (RR. HH.) que impidan esta solución. La gestión de políticas no es una solución eficaz si se permite a los usuarios visitar estos dominios solo a determinadas horas (por ejemplo, durante la hora de la comida). Umbrella no puede proporcionar una aplicación de políticas basada en tiempo con nuestro servicio, por lo que simplemente permitir a un usuario acceder al sitio todo el tiempo podría ser problemático. En un equipo compartido, como un terminal público, el cliente de roaming de Umbrella no puede diferenciar entre usuarios y no puede permitir fácilmente los dominios adecuados para las personas adecuadas.

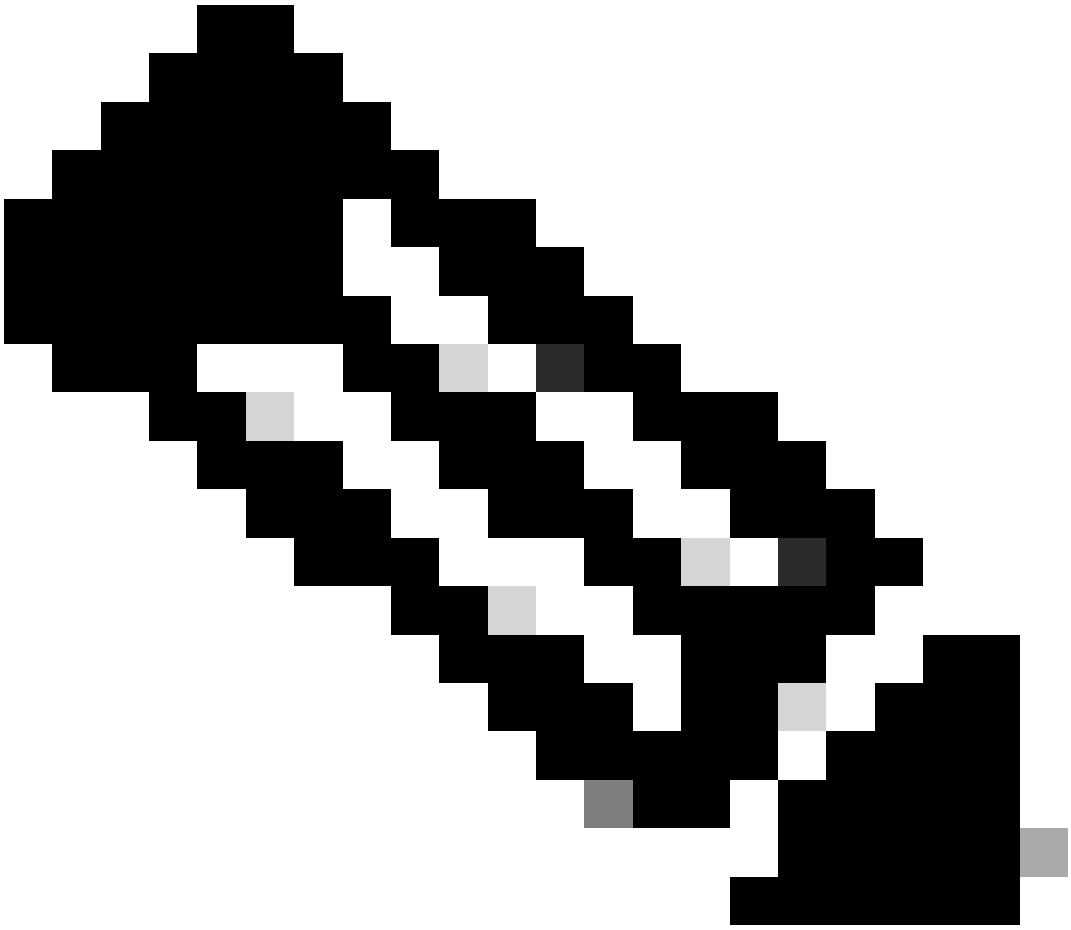
La administración de políticas no es tan eficaz cuando se tienen en cuenta identidades no granulares, como Sitios o Redes, a menos que el administrador se sienta cómodo al conceder a todos los usuarios de esa red el mismo acceso. La administración de directivas funciona mejor cuando se aplica a un subconjunto de usuarios a los que se permite el acceso a sitios mientras que el resto de la red no puede hacerlo, y singularizando a esos usuarios instalando el cliente de itinerancia en sus equipos y aplicando la jerarquía de directivas adecuada.



Nota: Cisco anunció el fin del ciclo de vida de Umbrella Roaming Client el 2 de abril de 2024. La fecha final de soporte técnico para Umbrella Roaming Client es el 2 de abril de 2025. Toda la funcionalidad de Umbrella Roaming Client está disponible actualmente en Cisco Secure Client. Cisco sólo proporciona innovaciones futuras en Cisco Secure Client. Recomendamos a los clientes que comiencen a planificar y programar su migración ahora. Consulte este artículo de KB para obtener orientación sobre cómo migrar de Umbrella Roaming Client a Cisco Secure Client.

Una administración de políticas adecuada es la mejor solución a este problema porque el navegador no recibe una respuesta de validación fallida en primer lugar. Si a algunos de sus usuarios se les permite acceder a sitios a los que normalmente necesitarían utilizar el desvío de página de bloqueo para acceder, puede configurar una política independiente para estos usuarios y agregar los dominios que se les puede permitir utilizar a la lista de permitidos. Dado que las solicitudes de los usuarios nunca se bloquean, el explorador nunca recibe una solicitud de un dominio con un certificado no coincidente. Puede utilizar Umbrella Roaming Client para proporcionar estas políticas específicas. Esto significa que está poniendo ciertos dominios en una lista de permitidos para ciertos usuarios en todo

momento del día para evitar estos errores.



Nota: El cliente de roaming de Umbrella es una forma eficaz de distribuir directivas concretas a varios usuarios, pero si ha habilitado la integración de Active Directory (AD), también puede aplicar estas directivas permitidas a usuarios de AD concretos.

Omitir errores de excepción de certificado (Chrome sólo para Windows)

Solo Chrome para Windows se puede configurar para ignorar los errores de excepción de certificado, lo que mitiga este error. Se le indica al navegador que ignore el error y en su lugar se ve la página normal de bloqueo de Umbrella.

IMPORTANTE: Este método es más arriesgado que ajustar la administración de directivas porque el explorador está configurado para omitir los errores de certificados. Es posible que, como resultado, el navegador pueda estar sujeto a ataques de intrusos (MiTM). Como resultado, no

podemos recomendar esto como un enfoque seguro para tratar este error, pero es una solución alternativa.

Estos cambios de configuración deben realizarse por ordenador, lo que dificulta el trabajo en entornos de gran escala, pero funciona.

Firefox, Safari y Chrome para Mac OS X

Firefox, Safari y Chrome para Mac OS X no pueden configurarse para ignorar los errores de excepciones de certificado para dominios anclados y siempre respeta la lista HSTS. No existe una solución alternativa conocida para estos errores.

Internet Explorer

Internet Explorer (IE) no implementa restricciones HSTS. Como resultado, no es necesario configurar IE y no muestra este error. Esto está sujeto a cambios en futuras versiones de IE si Microsoft decide implementar HSTS en el navegador.

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).