Corregir errores de visualización de página EUN en SWA para solicitudes HTTPS explícitas

Contenido

Introducción

Este documento describe el problema de las páginas EUN que se muestran incorrectamente en el SWA de Cisco para solicitudes HTTPS explícitas.

Prerequisites

Requirements

La información de este documento supone que:

- El dispositivo web seguro (SWA) se implementa en modo explícito.
- El SWA se ejecuta en las versiones 7.7.0 y anteriores.
- Las solicitudes HTTPS están bloqueadas, con advertencias o requieren confirmación por parte del usuario.
- El descifrado HTTPS está activado.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Problema

Las páginas Advertencia, Reconocimiento o Notificación de usuario final (EUN) no se muestran correctamente para las solicitudes HTTPS explícitas. El explorador muestra una página de notificación incompleta o no muestra la página en absoluto y, en su lugar, muestra una página de error.

Hay varios problemas que rodean estas páginas cuando se utilizan solicitudes HTTPS explícitas. Cuando configura el navegador para utilizar un proxy, el tráfico HTTPS se dirige al SWA a través de HTTP. Esta solicitud tiene formato HTTPS sobre HTTP.

Existen dos problemas conocidos con los navegadores que no manejan correctamente las respuestas HTTP que el SWA devuelve para las solicitudes HTTPS explícitas:

1. Cuando una solicitud HTTPS explícita se bloquea, se avisa o requiere la confirmación del usuario, el SWA devuelve un código de estado HTTP/403.
2. En esta respuesta, el SWA incluye el contenido de la notificación que debe representarse normalmente en la pantalla para que pueda verse. Sin embargo, en algunos casos, el navegador no puede entender la respuesta dentro del contenido devuelto.

Este es el comportamiento del navegador que se observa:

- Cuando se utilizan Internet Explorer versión 6 (IE6) y algunas versiones de IE7, estas solicitudes no pueden representar todo el contenido de la respuesta HTML. El navegador solo respeta los primeros bytes (el contenido dentro del primer paquete) e ignora el resto. En estos casos, verá una página incompleta que sólo muestra unos pocos caracteres.

  Nota: Si este es el caso, Cisco recomienda que reduzca la página de notificación predeterminada de la respuesta SWA. Para obtener más información sobre cómo editar la página EUN, consulte la sección Edición de archivos HTML de la página de notificación directamente de la guía del usuario SWA.

- Cuando se utilizan IE8 y las versiones más recientes de Mozilla Firefox versión 3, el navegador ignora completamente la respuesta que el SWA devuelve y la enmascara con su propia página de error. Este comportamiento del navegador contradice el propósito de la notificación 403 y provoca la interrupción de la función.

Solución

Esta sección describe el proceso que ocurre cuando el descifrado HTTPS está habilitado en el SWA. Este problema se ha resuelto en SWA versión 7.7.0-500 y posteriores (Cisco bug ID CSCzv25138) Como solución alternativa al problema descrito anteriormente, utilice la información proporcionada para asegurarse de que su sistema esté configurado en consecuencia.

Este es un ejemplo del flujo de tráfico cuando se envía una solicitud HTTPS explícita:

- Cuando se habilita el descifrado HTTPS, el SWA primero valida la solicitud con las políticas de descifrado.

- Si la solicitud está marcada para PASSTHROUGH, se permite el tráfico (sin advertencia ni EUN).

- Si la solicitud está marcada como DESCIFRADA, se valida con las directivas de Access. En este caso, si la política de acceso está configurada para ADVERTIR o BLOQUEAR, la página EUN se muestra correctamente. Desafortunadamente, para la confirmación, el usuario debe navegar a la página HTTP y la confirmación, que requiere la navegación a través del proxy y, a continuación, al sitio HTTPS.

- El SWA recuerda la dirección IP del cliente y no requiere otro reconocimiento hasta que caduca el temporizador.

Información Relacionada

- Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance - GD (implementación general) - Cisco

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).