Configuración de la autenticación de inicio de sesión único Kerberos en SWA

Contenido

Introducción

Este documento describe los pasos para configurar a los usuarios de proxy para que tengan autenticación de inicio de sesión único (SSO) a través de Kerberos en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.
- Administración básica de Active Directory.

Cisco recomienda tener instaladas estas herramientas:

- SWA físico o virtual.

- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA.
- Acceso administrativo a Active Directory.

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.

Antes de comenzar

Si el cliente proxy intenta acceder a un sitio web y se le pide que introduzca las credenciales manualmente, siga estos pasos para solucionar el problema.

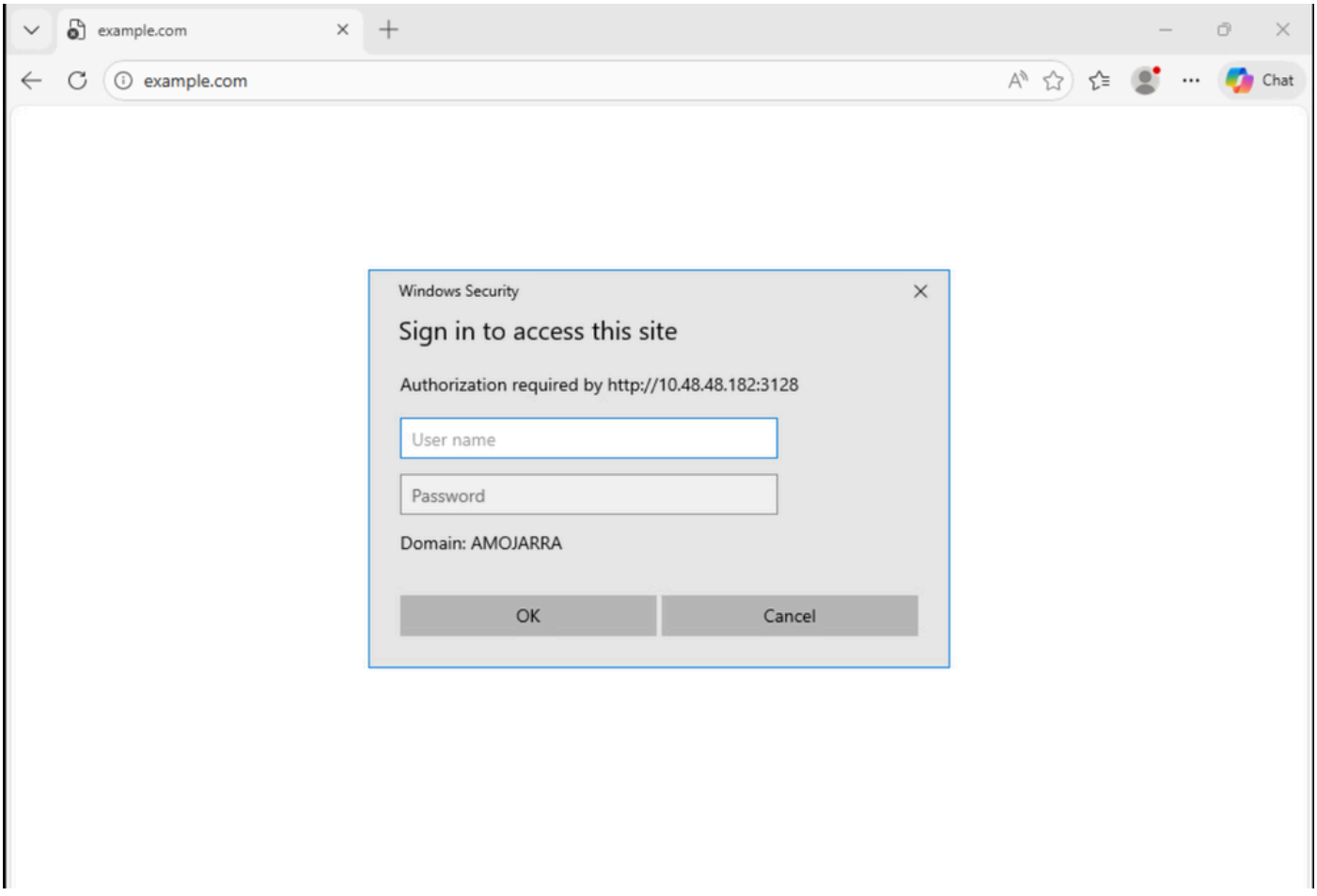


Imagen - Solicitud de autenticación de usuario

Paso 1. Verifique los Logs de Acceso relacionados con el cliente.

Paso 1.1. Inicie sesión en la CLI.

Paso 1.2. Ejecute grep.

Paso 1.3. Seleccione el número asociado a. registros de acceso.

Paso 1.4. En el campo Enter the regular expression to grep escriba la dirección IP del cliente.

Paso 1.5. Pulse Intro hasta que vea ¿Desea seguir los registros?, escriba "Y" y pulse Intro hasta que vea los registros de Accesos.

Paso 1.6. Reproduzca el problema intentando acceder a cualquier sitio web desde el PC cliente.

Paso 1.7. Confirme el perfil de identificación que recibe el tráfico.

En este ejemplo, el perfil de identificación es Auth_ID:

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

Paso 2. Compruebe el perfil de identificación.

Paso 2.1. Inicie sesión en la GUI del SWA.

Paso 2.2. Desde Web Security Manager, seleccione Perfiles de identificación.

Paso 2.3. Haga clic en el nombre del perfil de identificación al que estaba llegando el tráfico.

Paso 2.4. Confirme que el Esquema de Autenticación no esté configurado en Básico.

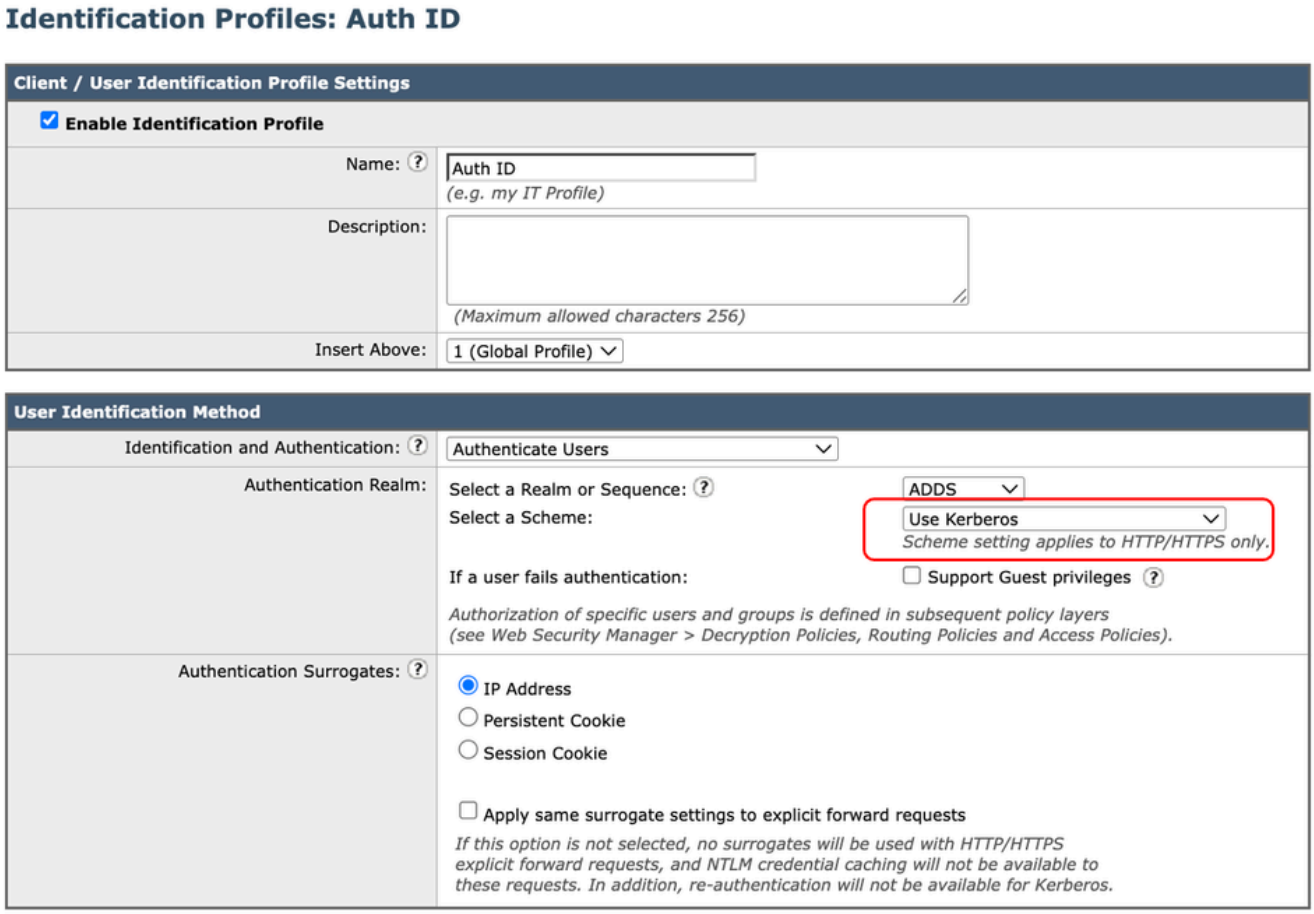


Imagen - Esquema de autenticación

Paso 3. Pruebe SWA y la conectividad de Active Directory.

Paso 3.1. Desde la GUI de SWA, navegue hasta Red y seleccione Autenticación.

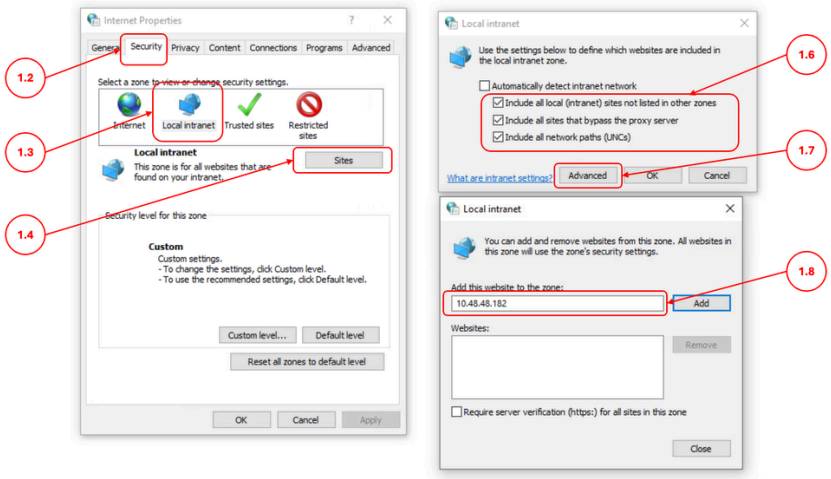
Paso 3.2. Haga clic en el Nombre de rango de autenticación.

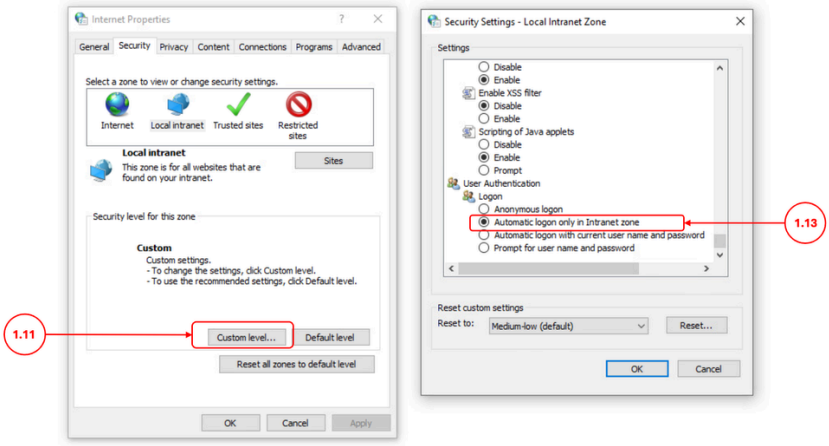
Paso 3.3. Haga clic en Start Test para revisar el SWA y el estado de conectividad del directorio activo.

Si no se encuentra ningún error, verifique la configuración del equipo cliente como se describe en este artículo.

Configuración del PC cliente

Siga estos pasos para verificar la configuración del PC cliente:

Pasos	Detalles
Paso 1. Sitios de Intranet local	Paso 1.1. En el menú de inicio, escriba Internet Option (Opción de Internet) y pulse Intro. Paso 1.2. En la ventana Propiedades de Internet, haga clic en la ficha Seguridad. Paso 1.3. Seleccione Intranet local. Paso 1.4. Haga clic en Sitios. Paso 1.5. Asegúrese de que la casilla de verificación Detectar automáticamente la red de intranet no esté seleccionada. Paso 1.6. Seleccione estas tres opciones: • Incluir todos los sitios locales (intranet) no enumerados en otras zonas • Incluir todos los sitios que omiten el servidor proxy • Incluir todas las rutas de acceso de red (UNC) Paso 1.7. Haga clic en Avanzado. Paso 1.8. Introduzca el FQDN o la dirección IP del SWA y agregue a la lista. Paso 1.9. (Opcional) Dependiendo de sus políticas de seguridad internas, puede inhabilitar Requiere verificación del servidor.  Imagen - Configuración de los sitios de Internet locales Paso 1.10. Haga clic en Cerrar y Aceptar.

	Paso 1.11. En la ficha Seguridad, haga clic en Nivel personalizado. Paso 1.12. Desplácese hasta Autenticación de usuario. Paso 1.13. Asegúrese de que la opción Inicio de sesión automático sólo en la zona Intranet está seleccionada.  Imagen: inicio de sesión automático para usuarios de la intranet
Paso 2. Recopile los registros	Si el Paso 1 no corrigió la autenticación SSO a través de Kerberos: Paso 2.1. Cambie los registros de autenticación SWA a Seguimiento y revise los registros. Paso 2.2. Agregue [Auth-Method = %m] como un campo personalizado a los registros de acceso. para obtener más información, visite: Configure el parámetro de rendimiento en los registros de acceso. Paso 2.3. Ejecute un filtro de captura de paquetes para la dirección IP del cliente y la dirección IP de Active Directory y confirme que la PC del cliente está enviando el vale de servicio Kerberos al SWA.

Nota: Asegúrese de que ha configurado el FQDN del SWA en la configuración de proxy del navegador.

Información Relacionada

- Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance

- Configuración del firewall para el dispositivo web seguro
- Configuración de la captura de paquetes en el dispositivo de seguridad de contenido
- Configurar el parámetro de rendimiento en registros de acceso
- Acceder a registros de appliances web seguros
- Uso de las prácticas recomendadas de los dispositivos web seguros: Cisco
- Omitir autenticación en dispositivo web seguro - 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).