Ejemplo de configuración local de la autenticación Web del portal del invitado del Identity Services Engine

Contenido

Introducción

Este documento describe cómo configurar la autenticación Web local (LWA) con el portal del invitado del Cisco Identity Services Engine (ISE).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Controlador LAN de la tecnología inalámbrica de Cisco (WLC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 1.1 ISE
- Versión 7.4 del WLC

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Este documento describe la configuración de LWA. Sin embargo, Cisco recomienda que usted utiliza la autenticación Web centralizada (CWA) con el ISE siempre que sea posible. Hay algunos escenarios donde se prefiere LWA o la única opción, así que esto es un ejemplo de configuración para esos escenarios.

Configurar

LWA requiere ciertos prerequirements y una configuración importante en el WLC así como algunos cambios necesarios en el ISE.

Antes de que se cubran ésos, aquí está un delinear del proceso LWA con el ISE.

Proceso LWA con el portal del invitado ISE

1. Los intentos del navegador para traer una página web.
2. El WLC intercepta el pedido de HTTP y lo reorienta al ISE.
   Varias informaciones claves se salvan en ese HTTP reorientan la encabezado. Aquí está un ejemplo de la reorientación URL:
   https://mlatosieise.wlaaan.com:8443/guestportal/Login.action?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   Del ejemplo URL, usted puede ver que el usuario intentó alcanzar “yahoo.com.” El URL también contiene la información sobre el nombre del Wireless Local Area Network (red inalámbrica (WLAN)) (mlatosie_LWA), y las direcciones MAC del cliente y del punto de acceso. En el ejemplo URL, 1.1.1.1 **es el** WLC, y mlatosieise.wlaaan.com **es el** servidor ISE.
3. Presentan con la página de registro del invitado ISE y ingresa el usuario el nombre de usuario y contraseña.
4. El ISE realiza la autenticación contra su secuencia configurada de la identidad.

5. El navegador reorienta otra vez. Esta vez, somete las credenciales al WLC. El hojeador proporciona el nombre de usuario y contraseña que el usuario ingresó en el ISE sin ninguna interacción adicional del usuario. Aquí está una petición get del ejemplo al WLC.
   GET
   /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   Una vez más el URL original (**yahoo.com**), el nombre de usuario (**mlatosie@cisco.com**), y la contraseña (**ityh**) son todo incluido.
   Nota: Aunque el URL sea visible aquí, la petición real se somete sobre Secure Sockets Layer (SSL), que es indicada por el HTTPS, y es dura de interceptar.
6. El WLC utiliza el RADIUS para autenticar que nombre de usuario y contraseña contra el ISE y permite el acceso.
7. Reorientan al usuario al portal especificado. Refiera el "**externo ISE de la configuración como a la** sección del **webauth el URL" de** este documento para más información.

Diagrama de la red

Esta figura describe la topología lógica de los dispositivos usados en este ejemplo.

Prerrequisitos de configuración

Para que el proceso LWA trabaje correctamente, un cliente necesita poder obtener:

- Dirección IP y configuración del netmask
- Ruta predeterminado
- Servidor del Domain Name System (DNS)

Todos los éstos se pueden proporcionar el DHCP o la configuración local.

La resolución de DNS necesita trabajar correctamente para que el LWA trabaje.

Configure el WLC

Configure el externo ISE como el Webauth URL

Conforme al **auth de la Seguridad > de la red > a la página de registro de la red**, usted puede acceder esta información.

> Nota: Este ejemplo utiliza un Webauth externo URL y fue tomado de la versión 1.1 ISE. Si usted tiene una diversa versión, consulte la guía de configuración para entender qué debe ser configurada.

Configure el Listas de control de acceso (ACL)

Para que la autenticación Web trabaje, el tráfico permitido debe ser definido.

Determine si FlexConnect ACL o ACL normales debe ser utilizado.

FlexConnect AP utiliza FlexConnect ACL, mientras que los AP que utilizan el uso centralizado ACL normales de la transferencia.

Para entender en qué modo actúa un AP determinado, navegue a la **Tecnología inalámbrica > a los Puntos de acceso** y elija la casilla desplegable del **name> AP modo AP**. Una instalación típica es **local** o **FlexConnect**.

Conforme a la **Seguridad > a las listas de control de acceso,** elija **FlexConnect ACL** o **ACL**.

En este ejemplo, todo el tráfico UDP fue permitido para permitir específicamente el intercambio y el tráfico DNS al ISE (10.48.66.107).

Este ejemplo utiliza FlexConnent, así que se definen FlexConnect y los ACL estándar.

Este comportamiento se documenta en el Id. de bug Cisco CSCue68065 con respecto al WLC 7.4 reguladores.

Configure el Service Set Identifier (SSID) para LWA

Bajo los **WLAN,** elija el **ID DE WLAN** para editar.

Configuración del auth de la red

Aplique los mismos ACL que fueron definidos en el paso anterior y habilite la autenticación Web.

> Nota: Si se utiliza la característica del Local Switching de FlexConnect, la asignación ACL necesita ser agregada en el nivel AP. Esto se puede encontrar conforme a la **Tecnología inalámbrica > a los Puntos de acceso.** Elija el **name>** apropiado **FlexConnect AP > WebAuthentication externo ACL**.
> ;

Configuración del servidor del Authentication, Authorization, and Accounting (AAA)

En este ejemplo, la autenticación y los servidores de contabilidad señalan al servidor anterior-definido ISE.

> Nota: Los valores por defecto bajo **ficha Avanzadas** no necesitan ser añadidos al final del fichero.

Configure el ISE

La configuración ISE consiste en varios pasos.

Primero, defina el dispositivo como dispositivo de red.

Entonces, asegúrese de que existan las reglas de la autenticación y autorización que acomodan este intercambio.

Defina el dispositivo de red

Bajo **administración - > los recursos de red - > los dispositivos de red**, pueblan estos campos:

- Nombre del dispositivo
- Dirección IP del dispositivo
- **Configuraciones > secreto compartido de la autenticación**

Configure la política de autenticación

Bajo la **directiva > autenticación**, agregue una nueva política de autenticación.

Este ejemplo utiliza estos parámetros:

- Nombre: **WLC_LWA_Guests**
- Condición: **Airespace: Airespace-WLAN-identificación.** Esta condición hace juego el ID DE WLAN de 3, que es el ID del **mlatosie_LWA de la** red inalámbrica (WLAN) que fue definido previamente en el WLC.
- {opcional} permite los Protocolos de autenticación que no requieren el certificado **Non_Cert_Auth**, pero los valores por defecto pueden ser utilizados.
- Guest_Portal_Sequence, que define que los usuarios son usuarios local-definidos de los invitados.

Configure la directiva y el resultado de la autorización

Bajo la **directiva > autorización,** defina una nueva directiva. Puede ser mismo una política básica, por ejemplo:

Esta configuración depende de la configuración general del ISE. Este ejemplo se simplifica útil.

Verificación

En el ISE, los administradores pueden monitorear y resolver problemas las sesiones vivas bajo las **operaciones > autenticaciones**.

Dos autenticaciones deben ser consideradas. La primera autenticación es del portal del invitado en el ISE. La segunda autenticación viene como una petición del acceso del WLC al ISE.

Usted puede hacer clic el icono del **informe de la reunión de la autenticación** para verificar que las directivas y las políticas de autenticación de la autorización fueron elegidas.

En el WLC, un administrador puede monitorear a los clientes bajo el **monitor > el cliente**.

Aquí está un ejemplo de un cliente que autenticó correctamente:

Troubleshooting

Cisco recomienda que usted ejecuta los debugs mediante el cliente siempre que sea posible.

Con el CLI, estos debugs proporcionan la información útil:

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

Información Relacionada

- Guía de configuración de Cisco ISE 1.x
- Guía de configuración del WLC 7.x de Cisco
- Soporte Técnico y Documentación - Cisco Systems