Ejemplo de configuración registrado uno mismo del portal del invitado de la versión 1.3 ISE

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Topología y flujo
Configurar
WLC
ISE
Verificación
Troubleshooting
Configuración optativa
Configuraciones del Uno mismo-registro
Configuraciones del invitado del login
Configuraciones del registro del dispositivo
Configuraciones de la conformidad del dispositivo del invitado
Configuraciones BYOD
Cuentas Patrocinador-aprobadas
Entregue las credenciales vía SMS
Registro del dispositivo
Postura
BYOD
Cambio de VLAN
Información Relacionada

Introducción

La versión 1.3 del Cisco Identity Services Engine (ISE) tiene un tipo nuevo de portal del invitado llamado el portal registrado uno mismo del invitado, que permite el uno mismo-registro de los Usuarios invitados cuando él accede a los recursos de red. Este portal permite que usted configure y que personalice las características múltiples. Este documento describe cómo configurar y resolver problemas estas funciones.

Prerequisites

Requisitos

Cisco recomienda que usted tiene experiencia con la configuración ISE y el conocimiento básico de estos temas:

- Implementaciones ISE y flujos del invitado
- Configuración de los reguladores del Wireless LAN (WLC)

Componentes Utilizados

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

- Microsoft Windows 7
- Versión 7.6 y posterior del WLC de Cisco
- Software ISE, versión 3.1 y posterior

Topología y flujo

Este escenario presenta las opciones múltiples disponibles para los Usuarios invitados cuando realizan el uno mismo-registro.

Aquí está el flujo general:

Paso 1. Socios del Usuario invitado al Service Set Identifier (SSID): Invitado. Esto es una red abierta con el MAC que filtra con el ISE para la autenticación. Esta autenticación hace juego la segunda regla de la autorización en el ISE y el perfil de la autorización reorienta al portal registrado uno mismo del invitado. El ISE vuelve un access-accept RADIUS con dos cisco av-pair:

- URL-reorientar-ACL (que el tráfico debe ser reorientado, y el nombre de la lista de control de acceso (ACL) definido localmente en el WLC)
- URL-reoriente (donde reorientar ese tráfico al ISE)

Paso 2. Reorientan al Usuario invitado al ISE. Bastante que las credenciales para iniciar sesión, el usuario que los tecleos “no tienen una cuenta”. Reorientan al usuario a una página donde esa cuenta puede ser creada. Un código secreto opcional del registro se pudo habilitar para limitar el privilegio del uno mismo-registro a la gente que conoce ese valor secreto. Después de que se cree la cuenta, el usuario es credenciales proporcionadas (nombre de usuario y contraseña) y abre una sesión con esas credenciales.

Paso 3. El ISE envía un cambio RADIUS de la autorización (CoA) Reauthenticate al WLC. El WLC reautentifica al usuario cuando envía el pedido de acceso del RADIO con el atributo del autorizar-Solamente. El ISE responde con el access-accept y el Airespace ACL definidos localmente en el WLC, que proporciona el acceso a Internet solamente (el acceso final para el Usuario invitado depende de la directiva de la autorización).

Observe que para las sesiones del Protocolo de Autenticación Extensible (EAP), el ISE debe enviar un CoA termina para accionar la reautentificación porque la sesión EAP está entre el supplicant y el ISE. Pero para MAB (MAC que filtra), el CoA Reauthenticate es bastante; no hay necesidad de-associate/de-authenticate el cliente de red inalámbrica.

Paso 4. El Usuario invitado ha deseado el acceso a la red.

Las características adicionales múltiples como la postura y Bring Your Own Device (BYOD) pueden ser habilitadas (discutido más adelante).

Configurar

WLC

1. Agregue al nuevo servidor de RADIUS para la autenticación y las estadísticas. Navegue a la **Seguridad >AAA > radio > autenticación** para habilitar CoA RADIUS (RFC 3576).

   Hay una configuración similar para considerar. También se aconseja configurar el WLC para enviar el SSID en estación que recibe la llamada el atributo ID, que permite que el ISE configure las reglas flexibles basadas en el SSID:

2. Bajo los WLAN tabule, cree al invitado del Wireless LAN (red inalámbrica (WLAN)) y configure la interfaz correcta. Fije la Seguridad Layer2 a **ningunos** con la filtración MAC. En los servidores de la Seguridad/del Authentication, Authorization, and Accounting (AAA), seleccione la dirección IP ISE para la autenticación y las estadísticas. En la ficha Avanzadas, habilite la **invalidación AAA** y fije el estado del Network Admission Control (NAC) al NAC RADIUS (soporte CoA).

3. Navegue a la **Seguridad > a las listas de control de acceso > a las listas de control de acceso** y cree dos Listas de acceso:

   GuestRedirect, que permite el tráfico que no debe ser reorientado y reorienta el resto del tráficoInternet, que se niega para las redes corporativas y se permite para todos los demás

   Aquí está un ejemplo para GuestRedirect ACL (necesidad de excluir el tráfico a/desde el ISE del cambio de dirección):

ISE

1. Navegue al **acceso de invitado > a la configuración > a los portales del invitado**, y cree un nuevo tipo porta, portal registrado uno mismo del invitado:

2. Elija el nombre porta que será referido al perfil de la autorización. Fije todas las otras configuraciones para omitir. Bajo arreglo para requisitos particulares porta de la página, todas las páginas presentadas pueden ser personalizadas.

3. Perfiles de la autorización de la configuración:

   Invitado (con el cambio de dirección al nombre porta y a ACL GuestRedirect del invitado)

   PermitInternet (con Internet del igual del Airespace ACL)

4. Para verificar las reglas de la autorización, navegue a la **directiva > a la autorización**. En la versión 1.3 ISE por abandono para la autenticación fallada del acceso de puente de la autenticación de MAC (MAB) (dirección MAC no encontrada) se continúa (no rechazado). Esto es muy útil para los portales del invitado porque no hay necesidad de cambiar cualquier cosa en las reglas de la autenticación predeterminada.

   Los usuarios nuevos que se asocian al invitado SSID no son todavía parte de cualquier grupo de la identidad. Esta es la razón por la cual hacen juego la segunda regla, que utiliza el perfil de la autorización del invitado para reorientarlos al portal correcto del invitado.

   Después de que un usuario cree una cuenta y abra una sesión con éxito, el ISE envía un CoA RADIUS y el WLC realiza la reautentificación. Esta vez, la primera regla se corresponde con junto con el perfil PermitInternet de la autorización y vuelve el nombre ACL que se aplica en el WLC.

5. Agregue el WLC como dispositivo de acceso a la red de la **administración > de los recursos de red > de los dispositivos de red**.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Después de que usted se asocie al invitado SSID y teclee un URL, después le reorientan a la página de registro:

2. ¿Puesto que usted no tiene ningunas credenciales todavía, usted debe elegir **no tiene una cuenta?** opción. Una nueva página que permite las visualizaciones de la creación de una cuenta. Si la opción del código del registro fue habilitada bajo configuración porta del invitado, se requiere ese valor secreto (éste se asegura de que solamente no prohiban la gente con los permisos correctos el uno mismo-registro).

3. Si hay algunos problemas con la contraseña o la política de usuario, navegue al **acceso de invitado > a las configuraciones > a la política de contraseña del invitado o el acceso de invitado > las configuraciones > la directiva del nombre de usuario del invitado** para cambiar las configuraciones. Aquí tiene un ejemplo:

4. Después de la creación de una cuenta acertada, le presentan con las credenciales (contraseña generada según las políticas de contraseña del invitado):

5. Haga clic la **muestra encendido** y proporcione las credenciales (la contraseña adicional del acceso pudo ser requerida si estuvo configurada bajo el portal del invitado; éste es otro mecanismo de seguridad que permite solamente a los que conozcan la contraseña para iniciar sesión).

6. Cuando es acertado, un Acceptable Use Policy opcional (AUP) pudo ser presentado (si está configurado bajo el portal del invitado). La página del acceso del poste (también portal inferior configurable del invitado) pudo también visualizar.

   La página más reciente confirma que se ha concedido el acceso:

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

En esta etapa, el ISE presenta estos registros:

Aquí está el flujo:

- El Usuario invitado encuentra la segunda regla de la autorización (Guest_Authenticate) y se reorienta al invitado (“Auhentication tuvo éxito”).
- Reorientan al invitado para el uno mismo-registro. Después de que con éxito el login (con la cuenta creada recientemente), ISE envíe el CoA Reauthenticate, que es confirmado por el WLC (“autorización dinámica tenida éxito”).
- El WLC realiza la reautentificación con el atributo del autorizar-Solamente y se vuelve el nombre ACL (“Autorizar-Solamente tuvo éxito”). Proporcionan el invitado el acceso a la red

correcto.

Los informes (las **operaciones > señalan que > el ISE señala > los informes del acceso de invitado > informe del invitado del master**) también confirman eso:

Un usuario del patrocinador (con los privilegios correctos) puede verificar el estado actual de un Usuario invitado.

Este ejemplo confirma que la cuenta está creada, pero el usuario nunca ha abierto una sesión ("aguardando la conexión con el sistema inicial"):

Configuración optativa

Para cada etapa de este flujo, diversas opciones pueden ser configuradas. Todo el esto se configura por el portal del invitado en el **acceso de invitado > la configuración > los portales > PortalName del invitado > edita > las configuraciones porta del comportamiento y del flujo**. Configuraciones más importantes incluyen:

Configuraciones del Uno mismo-registro

- Tipo del invitado - Describe cuánto tiempo la cuenta es activo, las opciones del vencimiento de la contraseña, las horas de inicio de sesión y las opciones (ésta es la mezcla de perfil y de rol de invitado del tiempo de la versión 1.2 ISE)
- Código del registro - Si están habilitados, solamente no prohiben los usuarios que conocen el código secreto el uno mismo-registro (debe proporcionar la contraseña cuando se crea la cuenta)
- AUP - Valide la directiva del uso durante el uno mismo-registro
- El requisito para que el patrocinador apruebe/activa la cuenta de invitado

Configuraciones del invitado del login

- Código de acceso - Si están habilitados, solamente se permite a los Usuarios invitados que conocen el código secreto iniciar sesión
- AUP - Valide la directiva del uso durante el uno mismo-registro
- Opción del cambio de la contraseña

Configuraciones del registro del dispositivo

- Por abandono, el dispositivo se registra automáticamente

Configuraciones de la conformidad del dispositivo del invitado

- Tiene en cuenta una postura dentro del flujo

Configuraciones BYOD

- Permite a los usuarios corporativos que utilizan el portal como invitados para registrar sus

dispositivos personales

Cuentas Patrocinador-aprobadas

Si seleccionan a los **invitados uno mismo-registradoes Require a ser** opción **aprobada**, después la cuenta creada por el invitado se debe aprobar por un patrocinador. Esta característica pudo utilizar el correo electrónico para entregar la notificación al patrocinador (para la aprobación de la cuenta de invitado):

Si el servidor o el valor por defecto del Simple Mail Transfer Protocol (SMTP) de la notificación del correo electrónico no se configura, después la cuenta no será creada:

El registro de guest.log confirma que el global del direccionamiento usado para la notificación falta:

```
2014-08-01 22:35:24,271 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null.  A global default From address can be
configured in global settings for SMTP server.
```

Cuando usted tiene la configuración apropiada del correo electrónico, se crea la cuenta:

Después de que usted permita a los **invitados uno mismo-registradoes Require para ser** opción **aprobada**, los campos del nombre de usuario y contraseña se quitan automáticamente del **incluir esta información sobre la** sección de la **página del éxito del Uno mismo-registro**. Esta es la razón por la cual, cuando la aprobación del patrocinador es necesaria, las credenciales para los Usuarios invitados no se visualizan por abandono en la página web que presenta la información para mostrar que se ha creado la cuenta. En lugar deben ser entregadas por los servicios de mensajería cortos (SMS) o el correo electrónico. Esta opción se debe habilitar en la **notificación credencial del envío sobre la aprobación usando la** sección (marca email/SMS).

Un correo electrónico de notificación se entrega al patrocinador:

Los registros del patrocinador en el patrocinador porta y aprueban la cuenta:

Desde aquí, se permite al Usuario invitado iniciar sesión (con las credenciales recibidas por el correo electrónico o SMS).

En resumen, hay tres direcciones de correo electrónico usadas en este flujo:

- Notificación “” del direccionamiento. Esto se define estáticamente o se toma de la cuenta del patrocinador y se utiliza como del direccionamiento para ambos: notificación a patrocinar (para la aprobación) y detalles credenciales al invitado. Esto se configura bajo el **acceso de invitado > la configuración > las configuraciones > configuraciones del correo electrónico del invitado**.

- Notificación “” a dirigir. Esto se utiliza para notificar al patrocinador que ha recibido una aprobación del explicar. Esto se configura en el portal del invitado bajo el **acceso de invitado > la configuración > los portales del invitado > los invitados uno mismo-registradoes Require porta del name> que se aprobarán > petición de aprobación del correo electrónico a**.

- Invitado “” a dirigir. Esto es proporcionada por el Usuario invitado durante el registro. Si **envíe la notificación credencial sobre la aprobación usando el correo electrónico** se selecciona, el correo electrónico con los detalles credenciales (nombre de usuario y contraseña) se entrega al invitado.

Entregue las credenciales vía SMS

Las credenciales del invitado se pueden también entregar por SMS. Estas opciones deben ser configuradas:

1. Elija el proveedor de servicio de SMS:

2. Marque la **notificación credencial del envío sobre la aprobación usando:** Casilla de verificación de **SMS**.

3. Entonces, piden el Usuario invitado elegir el proveedor disponible cuando él crea una cuenta:

4. SMS se entrega con el proveedor y el número de teléfono elegidos:

5. Usted puede configurar los proveedores de SMS bajo la **administración > el sistema > las configuraciones > el gateway de SMS**.

Registro del dispositivo

Si seleccionan a los **invitados de la permit para registrar la opción de dispositivos** después de que un Usuario invitado abra una sesión y valide el AUP, usted puede registrar los dispositivos:

Note que el dispositivo se ha agregado ya automáticamente (está en la lista de dispositivos Manage). Esto es porque los **dispositivos del invitado del registro** fueron seleccionados **automáticamente**.

Postura

Si se selecciona la opción de la **conformidad del dispositivo del invitado del requerir**, después los Usuarios invitados son aprovisionado con un agente que realice la postura (agente NAC/Web) después de que inicien sesión y validen el AUP (y realice opcionalmente el registro del dispositivo). El ISE procesa las reglas del aprovisionamiento del cliente para decidir a qué agente debe ser aprovisionado. Después el agente que se ejecuta en la estación realiza la postura (según las reglas de la postura) y envía los resultados al ISE, que envía el CoA reauthenticate

para cambiar el estatus de autorización si es necesario.

Las reglas posibles de la autorización pudieron parecer similares a esto:

Los primeros usuarios nuevos que encuentran la regla de Guest_Authenticate para reorientar al portal del invitado del registro del uno mismo. Después de que los uno mismo-registros del usuario y abran una sesión, el CoA cambia el estatus de autorización y proporcionan el usuario el acceso limitado para realizar la postura y la corrección. Solamente después que es el agente del NAC el aprovisionado y la estación es obedientes hace el estatus de autorización del cambio CoA de nuevo para proporcionar el acceso a Internet.

Los problemas comunes con la postura incluyen la falta de reglas correctas del aprovisionamiento del cliente:

Esto puede también ser confirmada si usted examina el archivo de guest.log (nuevo en la versión 1.3 ISE):

```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

Si seleccionan a los **empleados de la permit para utilizar los dispositivos personales en la opción de red**, después los usuarios corporativos que utilizan este portal pueden pasar con BYOD fluyen y registran los dispositivos personales. Para los Usuarios invitados, esa configuración no cambia cualquier cosa.

¿Qué los “empleados que usan el portal como invitado” significan?

Por abandono, los portales del invitado se configuran con el almacén de la identidad de **Guest_Portal_Sequence**:

Ésta es la secuencia interna del almacén que intenta a los usuarios internos primero (antes de los Usuarios invitados):

Cuando en esta etapa en el portal del invitado, el usuario proporciona las credenciales que se definen en los usuarios internos salvan y el cambio de dirección BYOD ocurre:

Los usuarios corporativos de esta manera pueden realizar BYOD para los dispositivos personales.

Cuando en vez de las credenciales de los usuarios internos, se proporcionan se continúan las credenciales de los Usuarios invitados, flujo normal (ningún BYOD).

Cambio de VLAN

Esto es una opción similar al cambio de VLAN configurado para el portal del invitado en la versión 1.2 ISE. Permite que usted ejecute activeX o los subprogramas java, que acciona el DHCP para liberar y para renovar. Esto es necesario cuando el CoA acciona el cambio del VLA N para el

punto final. Cuando se utiliza el MAB, el punto final no es consciente de un cambio del VLA N. Una Solución posible es cambiar el VLA N (la versión del DHCP/renueva) con el agente del NAC. Otra opción es pedir una nueva dirección IP vía el applet vuelto en la página web. Un retardo entre la versión/CoA/renueva puede ser configurado. Esta opción no se soporta para los dispositivos móviles.

Información Relacionada

- Servicios de la postura en la guía de configuración de Cisco ISE
- Tecnología inalámbrica BYOD con el Identity Services Engine
- Soporte ISE SCEP para el ejemplo de configuración BYOD
- Guía de administradores de Cisco ISE 1.3
- Autenticación Web central en el ejemplo de configuración del WLC y ISE
- Autenticación Web central con FlexConnect AP en un WLC con el ejemplo de configuración ISE
- Soporte Técnico y Documentación - Cisco Systems