La Tecnología inalámbrica CWA de la configuración ISE y el hotspot fluye con el WLCs de AireOS y de la última generación

Contenido

Introducción

Este documento describe cómo configurar tres casos del uso del invitado en Identity Services Engine (ISE) con Cisco AireOS y reguladores siguientes del Wireless LAN de Generation(NGWC) (WLCs).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controladores LAN de la tecnología inalámbrica de Cisco (unificados y acceso convergido)
- Identity Services Engine (ISE)

Componentes Utilizados

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

- Versión 2.1 del Cisco Identity Services Engine
- Controlador LAN 5508 8.0.121.0 que se ejecutan de la tecnología inalámbrica de Cisco
- Catalyst inalámbrico del regulador de la última generación (NGWC) 3850(WS-C3850-24P) 03.06.04.E que se ejecuta

Configurar

Diagrama de la red

Los pasos cubiertos en este documento describen la configuración típica en el WLCs unificado y convergido del acceso para soportar cualquier flujo del invitado con el ISE.

La configuración unificó 5508 WLC

Sin importar el caso del uso configurado en el ISE, de la perspectiva del WLC toda comienza con un punto final de red inalámbrica que conecte con un SSID abierto con la filtración MAC habilitada (más la invalidación AAA y el NAC RADIUS) esas puntas al ISE como la autenticación y el servidor de contabilidad. Esto se asegura de que el ISE pueda avanzar dinámicamente los atributos necesarios al WLC para la aplicación acertada de una reorientación al portal del invitado ISE.

Configuración global

1. Agregue el ISE global como una autenticación y servidor de contabilidad.

   - Navegue a la **Seguridad >AAA > autenticación** y haga clic **nuevo**

- Ingrese el ISE IP del servidor y el secreto compartido
- Asegúrese de que el estado del servidor y el **soporte para el RFC 3676** (cambio del soporte de la autorización o CoA) sean ambo conjunto a **habilitado**.
- Bajo AireOS del tiempo de espera del servidor por abandono el WLCs tendrá 2 segundos. Dependiendo de las Características de la red (tiempo de espera, ISE y WLC en las ubicaciones diferentes, etc) puede ser beneficioso aumentar el tiempo de espera del servidor por lo menos a 5 segundos para evitar los eventos de falla innecesarios.
- Haga clic en Apply (Aplicar).
- Si hay los Nodos de los servicios de las políticas múltiples (PSN) a configurar proceden a crear las Entradas de servidor adicionales.

Note: Este ejemplo de la configuración determinada incluye 2 casos ISE

- Navegue a la **Seguridad >AAA > RADIUS > las estadísticas** y haga clic **nuevo**
- Ingrese el ISE IP del servidor y el secreto compartido
- Asegúrese de que fijen al estado del servidor a habilitado
- Aumente el tiempo de espera del servidor en caso necesario (el valor por defecto es 2 segundos).

2. Configuración del retraso.

En el entorno unificado una vez que se acciona el tiempo de espera del servidor el WLC se mueve al servidor configurado siguiente. Después en la línea de la red inalámbrica (WLAN). Si no otro está disponible entonces el WLC selecciona el siguiente en la lista de los servidores globales. Cuando configuran a los servidores múltiples en el SSID (primario, secundario, etc) una vez que ocurre la Conmutación por falla el WLC por abandono continúa enviando el tráfico de la autenticación y (o) de las estadísticas permanentemente al caso secundario incluso si el servidor primario está detrás en línea.

Para atenuar este retraso del permiso del comportamiento. Navegue a la **Seguridad >AAA > RADIUS > retraso.** El comportamiento predeterminado está apagado. La única forma de recuperarse de un evento del servidor-abajo requiere la intervención admin (global despida el estado del administrador del servidor).

Para habilitar el retraso usted tiene dos opciones:

- **Pasivo** - En el modo pasivo, si un servidor no responde al pedido de autenticación del WLC, el WLC mueve el servidor a la cola inactiva y fija un temporizador (intervalo en la opción del Sec). Cuando expira el temporizador, el WLC mueve el servidor a la cola activa con independencia del estado real de los servidores. Si el pedido de autenticación da lugar a un evento de tiempo de espera (que signifique que el servidor todavía está abajo) que la Entrada de servidor se mueve otra vez a la cola inactiva y el temporizador golpea con el pie adentro otra vez. Si responde el servidor con éxito detrás, permanece en la cola activa. Los Valores configurables aquí van a partir 180 a 3600 segundos.

- **Activo -** En el modo activo, cuando un servidor no responde al pedido de autenticación del WLC, el WLC marca el servidor como muerto, después mueve el servidor al pool inactivo del servidor y comienza a enviar los mensajes de la sonda periódicamente hasta que responda ese servidor. Si responde el servidor, después el WLC mueve al servidor muerto al pool activo y para el enviar de los mensajes de la sonda.

En este modo el WLC le requiere ingresar un nombre de usuario y un intervalo de la sonda en los

segundos (180 a 3600).

> **Note**: La sonda del WLC no requiere una autenticación satisfactoria. La manera, un acertado o las autenticaciones fallidas se considera una respuesta del servidor que sea bastante para promover el servidor a la cola activa.

Configure el Service Set Identifier (SSID) del invitado:

- Navegue a la lengueta WLAN y debajo cree el nuevo tecleo de la opción **van**:
- Ingrese el nombre del perfil y el nombre SSID. Haga clic en Apply (Aplicar).
- Conforme a la ficha general seleccione la interfaz o al grupo de interfaces que se utilizarán (VLA N del invitado).
- Bajo la **Seguridad > capa 2 > Seguridad de la capa 2** selecta checkbox de **filtración del mac ninguno** y del permiso.
- Bajo la autenticación determinada y los servidores de contabilidad de la lengueta de los **servidores de AAA habilitó** y seleccionan su primario y servidores secundarios.
- **Actualización interina**: Ésta es una configuración optativa que no agrega ninguna ventajas a este flujo. Si usted prefiere habilitarla, el WLC debo funcionar con 8.x o un código más alto:

Discapacitado: La característica se inhabilita totalmente.

Habilitado con 0 intervalos: El WLC envía las actualizaciones de las estadísticas al ISE cada vez que hay un cambio en la entrada móvil de Block(MSCB) del control de la estación del cliente (IE. Se envían el IPv4 o la asignación de dirección o el cambio del IPv6, el evento de itinerancia del cliente, los etc.) ningunas actualizaciones periódicas adicionales.

Habilitado con un intervalo interino configurado: En este modo el WLC envía las notificaciones al ISE sobre los cambios de la entrada MSCB del cliente y también envía las notificaciones periódicas adicionales de las estadísticas en el intervalo configurado (sin importar cualquier cambios).

- Bajo el permiso de la ficha Avanzadas **permita la invalidación AAA** y bajo **estado del NAC** seleccione el **NAC RADIUS**. Esto se asegura de que el WLC aplique cualquier par de valores de atributos (AVP) que venga del ISE.
- Navegue a la ficha general SSID y fije el estatus SSID a **habilitado**
- **Aplique los** cambios.

Configure la reorientación ACL

Este ACL es referido por el ISE y determina qué tráfico consigue reorientado y qué tráfico será permitido a través.

- Vaya a la **ficha de seguridad** > a las **listas de control de acceso** y haga clic **nuevo**
- Éste es un ejemplo del ACL

Este ACL debe permitir el acceso a y desde los servicios DNS y los Nodos ISE sobre el puerto

TCP 8443. Hay un implícito niega en la parte inferior que significa que el resto del tráfico consigue reorientado al invitado URL porta ISE.

El HTTPS reorienta

Esta característica se soporta en las versiones 8.0.x de AireOS y sube pero se apaga por abandono. Para habilitar el soporte HTTPS vaya a la **Administración del** WLC **>** al **HTTP-HTTPS > al redireccionamiento HTTPS** y fíjelo **habilitó** o aplican el este comando en el CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Las advertencias del certificado después del HTTPS reorientan se habilitan

Después de que https-reoriente se habilite, el usuario pueda experimentar los problemas de la confianza del certificado durante la reorientación. Se ve esto incluso si hay un certificado encadenado válido en el regulador e incluso si este certificado es firmado por un Certificate Authority confiado en las de otras compañías. La razón es que el certificado instalado en el WLC está publicado a su nombre de host o dirección IP de la interfaz virtual. Cuando el cliente intenta el https: //cisco.com, el navegador espera que el certificado sea publicado a cisco.com. Sin embargo, porque el WLC a poder interceptar el GET publicado por el cliente, primero necesita establecer a las sesiones HTTP para quien el WLC presenta su certificado de la interfaz virtual durante la fase del contacto SSL. Esto hace al navegador visualizar una advertencia pues el certificado presentado durante el contacto SSL no se ha publicado al sitio web original que el cliente está intentando acceder (IE. cisco.com se opuso al nombre de host de la interfaz virtual WLC). Usted puede ser que vea diversos mensajes de error del certificado en diversos navegadores pero todos relacionarse con el mismo problema.

Conmutación por falla agresiva

Esta característica se habilita por abandono en el WLCs de AireOS. Cuando se habilita la Conmutación por falla agresiva, el WLC marca al servidor de AAA mientras que insensible y él se mueve al servidor de AAA configurado siguiente después de que un evento de tiempo de espera del radio afecte a un cliente.

Cuando se inhabilita la característica el WLC falla encima al servidor siguiente solamente si el evento de tiempo de espera RADIUS ocurre con por lo menos 3 sesiones de cliente. Esta característica se puede inhabilitar por este comando (no se requiere ninguna reinicialización para este comando):

```
(Cisco Controller) >config radius aggressive-failover disable
```

Para verificar el estado actual de la característica:

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
```

```
Aggressive Failover.............................. Disabled
```

Puente prisionero

Los puntos finales que soportan un mecanismo prisionero del asistente de red (PUEDA) para descubrir un cautivo-porta y el auto-lanzamiento una página del inicio hacen generalmente esto a través de un pseudo-navegador en una ventana controlada mientras que otros puntos finales ponen en marcha a un navegador completamente capaz para accionar esto. Para los puntos finales en donde la PODER pone en marcha a un pseudo-navegador, esto puede romper el flujo cuando está reorientada a un portal prisionero ISE. Esto afecta típicamente a los dispositivos IOS de Apple y tiene especialmente efectos negativos en los flujos que requieren el registro del dispositivo, el DHCP-Rlease del VLA N, el control de la conformidad, el etc.

Dependiendo de la complejidad del flujo funcionando puede ser recomendado para habilitar puente prisionero. En tal escenario, el WLC ignora el mecanismo de detección porta de la PODER y el cliente necesita abrir a un navegador para iniciar el proceso de la reorientación.

Verifique el estatus de la característica:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..................... Disabled
Web Auth Redirect Ports ................... 80,3128
Web Auth Proxy Redirect  .................. Disable
Web Auth Captive-Bypass   ................. Disabled
Web Auth Secure Web  ...................... Enable
Web Auth Secure Redirection  .............. Enable
```

Para habilitar este tipo de la característica este comando:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

El WLC alerta al usuario que para que los cambios tomen a efecto un restauración-sistema (reinicio) son necesarios.

En este momento un **resumen de la red de la demostración** muestra la característica según lo habilitado, pero para que los cambios tomen a efecto el WLC necesitan ser recomenzados.

La configuración convergió 3850 NGWC

Configuración global

1. **Agregue el ISE global como una autenticación y servidor de contabilidad**

   - Navegue al **> Security (Seguridad) de la configuración > al RADIUS > a los servidores** y haga clic **nuevo**
   - Ingrese el **dirección IP del servidor** ISE, el **secreto compartido**, el **tiempo de espera del servidor** y la **cuenta de reintentos** que refleja sus condiciones del medio ambiente.

- Asegúrese de que el **soporte para el RFC 3570** (soporte CoA) esté habilitado.
- Relance el proceso para agregar una entrada del servidor secundario.

2. **Cree al grupo de servidores ISE**

   - Navegue al **> Security (Seguridad) > a los grupos de servidores de la configuración** y haga clic **nuevo**
   - Asigne un nombre al grupo y ingrese un valor de **tiempo muerto** en los minutos. Éste es el tiempo que el regulador mantiene el servidor la cola inactiva antes de que se promueva otra vez a la lista del servidor activo.
   - De la lista disponible de los servidores agreguelos al asignado columna Servers (Servidores).

3. **Global habilite el dot1x**

   - Navegue a la **configuración >AAA > las listas de métodos > general** y habilite el **control del auth del sistema del dot1x**

4. **Configure las listas de métodos**

   - Navegue a la **configuración** >AAA > las **listas de métodos > autenticación** y cree una nueva lista de métodos. En este caso es dot1x y grupo ISE_Group (grupo del tipo creado en el paso anterior). Entonces el golpe **se aplica**

   - Haga lo mismo para considerar (**configuración >AAA > las listas de métodos > las estadísticas**) y la autorización (**configuración >AAA > las listas de métodos > autorización**). Deben parecer esto

5. **Cree el método del MAC-filtro de la autorización**.

Esto se llama de las configuraciones SSID más adelante.

- Navegue a **Configuration> AAA > las listas de métodos > autorización** y haga clic **nuevo**.
- Ingrese el **nombre de la lista de métodos**. Eligió el **tipo = al grupo de la red** y del **Tipo de grupo**.
- Agregue ISE_Group a los grupos de servidores asignados campo.

Configuración SSID

1. **Cree al invitado SSID**

   - Navegue a la **configuración > a la Tecnología inalámbrica > a los WLAN** y haga clic **nuevo**
   - Ingrese el ID DE WLAN, el SSID y el nombre del perfil y el tecleo se aplica.
   - Una vez en las configuraciones SSID bajo la interfaz/grupo de interfaces seleccione la interfaz de la capa 3 del VLA N del invitado.

   - Bajo la **Seguridad > capa 2** selectas **ningunos** y al lado de la **filtración Mac** ingresan el nombre de la lista de métodos del filtro Mac que usted configuró previamente (MacFilterMethod).
   - Bajo lengueta del **servidor de la Seguridad** >AAA seleccione la autenticación adecuada y las listas de los métodos de contabilidad (ISE_Method).

- Bajo el permiso de la **ficha Avanzadas permita la invalidación AAA** y el **estado del NAC.** El resto de las configuraciones se debe ajustar según los requisitos de cada despliegue (tiempo de espera de la sesión, exclusión del cliente, soporte para las extensiones Aironet, etc).

- Navegue a la ficha general fijan el estatus a habilitado. Entonces el golpe **se aplica.**

Reoriente la configuración ACL

Este ACL es referido por el ISE más adelante al access-accept en respuesta a la petición inicial MAB. El NGWC lo utiliza para determinar qué tráfico a reorientar y qué tráfico se debe permitir a través.

- Navegue al **> Security (Seguridad) de la configuración > al ACL > a las listas de control de acceso** y el tecleo **agrega nuevo**.
- Seleccione extendido y ingrese el nombre ACL.
- Esta imagen muestra que un ejemplo de un típico reorienta el ACL:

  Note: La línea 10 es opcional. Esto se agrega generalmente para resolver problemas propone. Este ACL debe permitir el acceso al DHCP, los servicios DNS y también al puerto de servidores ISE TCP 8443(Deny ACE). El tráfico HTTP y HTTPS consigue reorientado (permiso ACE).

Configuración del comando line interface(cli)

Toda la configuración discutida en los pasos anteriores puede también ser aplicada con el CLI.

802.1x global habilitado

```
dot1x system-auth-control
```

Configuración AAA global

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 14.36.157.210 server-key *****
 client 14.36.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 14.36.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 14.36.157.21 auth-port 1812 acct-port 1813
 timeout 5
```

```
 retransmit 2
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

Configuración de Wlan

```
 wlan Guest 1 Guest
 aaa-override
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

Reoriente el Ejemplo de ACL

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 14.36.157.210 eq 8443
    60 deny tcp any host 14.36.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

Soporte HTTP y HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

Note: Si usted aplica un ACL para restringir el acceso al WLC sobre el HTTP, afecta al cambio de dirección.

Configuración ISE

Esta sección describe la configuración requerida en el ISE para soportar todos los casos de las aplicaciones discutida en este documento.

Tareas de configuración comunes ISE

1. Inicie sesión al ISE y navegue a la **administración > a los recursos de red > a los dispositivos de red** y el tecleo **agrega**
2. Ingrese el **nombre** asociado al WLC y al **IP Address del** dispositivo.
3. Marque el cuadro de las **configuraciones de la autenticación de RADIUS** y teclee el **secreto compartido** configurado en el lado del WLC. Entonces haga clic **someten**.

4. Navegue a la **directiva > a la autenticación** y bajo tecleo **MAB edite** y asegure eso bajo **uso: Los puntos finales internos la** opción si **no encuentran al usuario** se fijan **para continuar** (debe estar allí por abandono).

Utilice el caso 1: CWA con la autenticación del invitado en cada conexión del usuario

Descripción del flujo

1. El usuario de red inalámbrica conecta con el invitado SSID.
2. El WLC autentica el punto final basado en su dirección MAC usando el ISE como servidor de AAA.
3. Las devoluciones ISE apoyan y access-accept con dos pares de valores de atributos (AVP): URL-reoriente y URL-reorientar-ACL. Una vez que el WLC aplica este los AVP a la sesión del punto final, las transiciones de la estación a DHCP-requerido y una vez que ase una dirección IP permanece en CENTRAL_WEB_AUTH. En este paso el WLC está listo para comenzar a reorientar el tráfico HTTP/del https del cliente.
4. El usuario final abre al buscador Web y una vez que se genera el tráfico HTTP o HTTPS, el WLC reorienta al usuario al portal del invitado ISE.
5. Una vez que el usuario llega al portal del invitado indica para ingresar las credenciales del invitado (patrocinador-creadas en este caso).
6. Sobre la validación de las credenciales el ISE visualiza la página AUP y una vez que el cliente valida, envían a un tipo dinámico Re-authenticate CoA al WLC.
7. El WLC trata de nuevo la autenticación de filtración MAC sin la publicación de una de-autenticidad a la estación móvil. Esto debe ser inconsútil al punto final.
8. Una vez que sucede el evento de la reautentificación el ISE evalúa de nuevo las directivas de la autorización y este vez el punto final se da un acceso del permiso puesto que había un evento acertado anterior de la autenticación del invitado.

Este proceso se relanza cada vez que el usuario conecta con el SSID.

Configuración

1. Navegue al ISE y navegue a los **centros de trabajo > al acceso de invitado > a la configuración > a los portales del invitado >** seleccionan el **portal patrocinado del invitado** (o cree a un nuevo Patrocinar-invitado porta del tipo).
2. Conforme al **registro del dispositivo del invitado las** configuraciones desmarcan todas las opciones y hacen clic la **salvaguardia**.

3. Navegue a la **directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización**. Haga clic en Add (Agregar).

4. Este perfil se empuja hacia abajo al WLC el Reorientar-**URL** y el Reorientar-URL-**ACL** en respuesta a la petición inicial de puente de la autenticación del mac (MAB).

- Una vez el **auth centralizado** selecto marcado de la **red del cambio de dirección de la red (CWA, MDM, NSP, CPP)**, después teclea el nombre de la reorientación ACL bajo campo **ACL** y bajo **valor** selecciona el **invitado patrocinado Portal(default)** (o cualquier otro portal específico creado en los pasos anteriores).

El perfil debe mirar similar el que está en esta imagen. Entonces haga clic la **salvaguardia**.

Los detalles del atributo en la parte inferior de la página el valor de atributo Pairs(AVPs) como son se avancen al WLC

5. Navegue a la **directiva > a la autorización** e inserte una nueva regla. Esta regla es la que acciona el proceso de la reorientación en respuesta a la petición inicial de la autenticación de MAC del WLC. (En este caso llamado **Wireless_Guest_Redirect**).

6. Bajo **condiciones** elija la **condición existente selecta de la biblioteca**, después bajo **condición compuesta** selecta del **nombre de condición**. Seleccione una condición compuesta predefinida llamada **Wireless_MAB**.

> **Note**: Esta condición consiste en 2 atributos de RADIUS esperados en la forma originada petición del acceso el WLC (IEEE 802.11 de NAS-Port-Type= <present en todo el requests> y tipo de servicio = llamada inalámbricos Check< que refiere a una petición específica un bypass> de la autenticación del mac)

7. Bajo resultados, **estándar** selecto > **CWA_Redirect** (perfil de la autorización creado en el paso anterior). Entonces haga clic **hecho** y **salvaguardia**

8. Navegue al final de la regla de **CWA_Redirect** y haga clic la flecha al lado de **editan**. Entonces seleccione el **duplicado arriba**.

9. Modifique el nombre pues ésta es la directiva esa los emparejamientos del punto final que la sesión se reautentifica una vez sobre el CoA ISE (en este caso Wireless_Guest_Access).

10. Al lado de la condición compuesta de **Wireless_MAB** haga clic **+** símbolo para ampliar las condiciones y para el final del tecleo de la condición de **Wireless_MAB agregue el atributo/el valor**.

11. Bajo “atributo selecto” eligió el **acceso a la red > el flujo del invitado de los iguales de UseCase**

12. Bajo los **permisos** seleccione **PermitAccess**. Entonces haga clic **hecho** y **salvaguardia**

Las dos directivas deben parecer similares a esto:

Utilice el caso 2: CWA con el registro del dispositivo que aplica la autenticación del invitado una vez al día.

Descripción del flujo

1. El usuario de red inalámbrica conecta con el invitado SSID.
2. El WLC autentica el punto final basado en su dirección MAC usando el ISE como servidor de AAA.
3. Las devoluciones ISE apoyan y access-accept con dos pares de valores de atributos (AVP) (URL-reoriente y URL-reorientar-ACL).
4. Una vez que el WLC aplica este los AVP a la sesión del punto final, las transiciones de la estación a DHCP-requerido y una vez que ase una dirección IP permanece en CENTRAL_WEB_AUTH. En este paso el WLC está listo para comenzar a reorientar el tráfico HTTP/del https del cliente.
5. El usuario final abre al buscador Web y una vez que se genera el tráfico HTTP o HTTPS, el WLC reorienta al usuario al portal del invitado ISE.
6. Una vez que el usuario llega al portal del invitado, él consigue indicado para ingresar las credenciales patrocinador-creadas.
7. Sobre la validación de las credenciales el ISE agrega este punto final a un grupo (preconfigurado) específico de la identidad del punto final (registro del dispositivo).
8. Se visualiza la página AUP y una vez que el cliente valida, un tipo dinámico CoA reautentifica. Se envía al WLC.
9. El WLC para tratar de nuevo la autenticación de filtración MAC sin la publicación de una de-autenticidad a la estación móvil. Esto debe ser inconsútil al punto final.
10. Una vez que sucede el re evento de la autenticación el ISE evalúa de nuevo las directivas de la autorización. Esta vez puesto que el punto final es miembro del grupo ISE de la identidad del punto final de la derecha vuelve un acceso valida sin las restricciones.
11. Puesto que el punto final se ha registrado en el paso 6, cada vez que se vuelve ése el usuario, a le se permite en la red hasta que se quite manualmente del ISE, o una directiva de la purgación del punto final ejecuta vaciar los puntos finales que cumplen los criterios.

En este escenario de laboratorio, la autenticación se aplica una vez al día. El activador de la reautentificación es la directiva de la purgación del punto final que quita todos los puntos finales de la identidad usada del punto final agrupa cada día.

> **Note**: Es posible aplicar el evento de la autenticación del invitado basado el tiempo transcurrido desde la aceptación más reciente AUP. Esto puede ser una opción si usted necesita aplicar el inicio del invitado más a menudo que una vez al día (en el ejemplo cada 4 horas).

Configuración

1. En el ISE navegue a los **centros de trabajo > al acceso de invitado > a la configuración > a los portales del invitado** > seleccionan el **portal patrocinado del invitado** (o cree a un nuevo Patrocinar-invitado porta del tipo).
2. Bajo configuraciones del **registro del dispositivo del invitado** verifique que la opción **registre automáticamente al invitado que** se marcan los **dispositivos**. Click **Save**.

3. Navegue a los **tipos del centro de trabajo > del acceso > de la configuración > del invitado del invitado** o apenas haga clic en el atajo especificado bajo configuraciones del registro del

dispositivo del invitado en el portal.

4. Cuando el usuario del patrocinador crea una cuenta de invitado, él le asigna un tipo del invitado. Cada tipo individual del invitado puede tener un punto final registrado que pertenezca a una diversa identidad Group.To del punto final asigne al grupo de la identidad del punto final que el dispositivo debe ser agregado a, seleccione el tipo del invitado las aplicaciones del patrocinador para estos Usuarios invitados (este caso del uso se basa en el semanario (valor por defecto)).

5. Una vez en el tipo del invitado, bajo **opciones del login** seleccione el grupo del punto final del **grupo de la identidad del punto final del** menú desplegable **para el registro del dispositivo del invitado**

6. Navegue a la **directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización**. Haga clic en Add (Agregar).

7. Este perfil se empuja hacia abajo al WLC el Reorientar-**URL** y el Reorientar-URL-**ACL** en respuesta a la petición inicial de puente de la autenticación del mac (MAB).

- Una vez el **auth centralizado** selecto marcado de la **red del cambio de dirección de la red (CWA, MDM, NSP, CPP)**, después teclea el nombre de la reorientación ACL bajo campo **ACL** y bajo **valor** selecciona el portal creado para este flujo (**CWA_DeviceRegistration**).

8. Navegue a la **directiva > a la autorización** e inserte una nueva regla. Esta regla es la que acciona el proceso de la reorientación en respuesta a la petición inicial de la autenticación de MAC del WLC. (En este caso llamado **Wireless_Guest_Redirect**).

9. Bajo **condiciones** eligió la **condición existente selecta de la biblioteca**, después bajo **condición compuesta** selecta del **nombre de condición**. Seleccione una condición compuesta predefinida llamada **Wireless_MAB**.

10. Bajo resultados, **estándar** selecto **> CWA_DeviceRegistration** (perfil de la autorización creado en el paso anterior). Entonces haga clic **hecho** y **salvaguardia**

11. Duplique la directiva arriba, modifique su nombre pues ésta es la directiva que el punto final golpea después de que vuelva del evento de la reautentificación (llamado Wireless_Guest_Access).

12. Bajo **detalles del grupo de la identidad** encajone, **grupo** selecto de la **identidad del punto final** y seleccione al grupo que usted se refirió bajo el invitado Type(GuestEndpoints).

13. Bajo resultados seleccione **PermitAccess**. Haga clic **hecho** y **salve los** cambios.

14. Cree y la directiva de la purgación del punto final que borra el grupo de GuestEndpoint diario.

- Navegue a la **administración** > a la **Administración de la identidad** > a las **configuraciones** > a la **purgación del punto final**
- Bajo reglas de la **purgación** debe haber una por abandono esa cancelacíon de GuestEndpoints de los activadores si el tiempo transcurrido es mayor de 30 días.
- Modifique la política existente para GuestEndpoints o cree un nuevo (en caso de que se ha quitado el valor por defecto). Observe que las directivas de la purgación funcionan con cada día al tiempo definido.

En este caso la condición es miembros de GuestEndpoints con los días transcurridos menos de 1

día

Utilice el caso 3: Portal de HostSpot

Descripción del flujo

1. El usuario de red inalámbrica conecta con el invitado SSID.
2. El WLC autentica el punto final basado en su dirección MAC usando el ISE como servidor de AAA.
3. El ISE vuelve detrás un access-accept con dos pares de valores de atributos (AVP): URL-reoriente y URL-reorientar-ACL.
4. Una vez que el WLC aplica este los AVP a la sesión del punto final, las transiciones de la estación a DHCP-requerido y una vez que ase una dirección IP permanece en CENTRAL_WEB_AUTH. En este paso el WLC está listo para reorientar el tráfico HTTP/del https del cliente.
5. El usuario final abre al buscador Web y una vez que se genera el tráfico HTTP o HTTPS, el WLC reorienta al usuario al portal del hotspot ISE.
6. Una vez en el portal se indica al usuario que valide un Acceptable Use Policy.
7. El ISE agrega la dirección MAC del punto final (ID del punto final) en el grupo de la identidad del punto final configurado.
8. La directiva mantiene el nodo (PSN) ese los procesos que la petición publica una Admin-**restauración** dinámica del tipo CoA al WLC.
9. Una vez que el WLC acaba de procesar el CoA entrante, publica una de-autenticidad al cliente (la conexión es pérdida por el tiempo que toma para que se vuelva el cliente).
10. Una vez que el cliente vuelve a conectar, se crea una nueva sesión tan allí no es ninguna continuidad de la sesión en el lado ISE. Significa que la autenticación está procesada como nuevo subproceso.
11. Puesto que el punto final se agrega al grupo de la identidad del punto final configurado, y hay una directiva de la autorización que marca si el punto final es parte de que agrupa, la nueva autenticación hace juego esta directiva. El resultado es de total acceso a la red del invitado.
12. El usuario no debe tener que validar el AUP otra vez a menos que el objeto de la identidad del punto final se purgue de la base de datos ISE como resultado de una directiva de la purgación del punto final.

Configuración

1. Cree a un nuevo grupo de la identidad del punto final para mover estos dispositivos sobre al registro. Navegue a los **centros > al acceso de invitado > a la identidad de trabajo agrupa > los grupos de la identidad del punto final** y hace clic .

- Ingrese un nombre del grupo (en este caso HotSpot_Endpoints). Agregue una descripción y no hay grupo de padre necesario.

2. Navegue a los **centros de trabajo > al acceso de invitado > a la configuración > a los portales del invitado > portal** selecto del **hotspot (valor por defecto**).

3. Amplíe las configuraciones porta y bajo el grupo selecto de **HostSpot_Endpoints del** grupo de la identidad del punto final bajo el **grupo de la identidad del punto final.** Esto envía los dispositivos registrados al grupo especificado.

4. **Salve los** cambios.

5. Cree el perfil de la autorización que llama el portal del hotspot sobre la autenticación MAB originada por el WLC.

- Navegue a los **elementos de la directiva > de la directiva > a los resultados > a la autorización > a los perfiles de la autorización** y cree uno (HotSpotRedirect).
- **El cambio de dirección de la red (CWA, MDM, NSP, CPP)** es una vez selecto marcado **hot spot**, después teclea el nombre de la reorientación ACL en el campo ACL (Guest_Redirect) y como un portal correcto selecto del valor (**portal del hotspot (valor por defecto)**).

6. Cree la directiva de la autorización que acciona el resultado de HotSpotRedirect por el requerimiento inicial MAB del WLC.

- Navegue a la **directiva > a la autorización** e inserte una nueva regla. Esta regla es la que acciona el proceso de la reorientación en respuesta a la petición inicial de la autenticación de MAC del WLC. (En este caso llamado **Wireless_HotSpot_Redirect**).
- Bajo **condiciones** elija la **condición existente selecta de la biblioteca**, después bajo **condición compuesta** selecta del **nombre de condición**
- Bajo resultados, **estándar** selecto **> HotSpotRedirect** (perfil de la autorización creado en el paso anterior). Entonces haga clic **hecho** y **salvaguardia**

7. Cree la segunda directiva de la autorización.

- Duplique la directiva arriba, modifique su nombre pues ésta es la directiva que el punto final golpea después de que vuelva del evento de la reautentificación (llamado Wireless_HotSpot_Access).
- Bajo **detalles del grupo de la identidad** encajone, **grupo** selecto de la **identidad del punto final** y entonces el grupo que usted creó anterior (**HotSpot_Endpoints**).
- Bajo resultados seleccione **PermitAccess**. Haga clic **hecho** y **salve los** cambios.

8. Configure la directiva de la purgación que borra los puntos finales con mayores de 5 días de un tiempo transcurrido.

- Navegue a la **administración > a la Administración de la identidad > a las configuraciones > a la purgación del punto final** y bajo purgación las reglas crean un nuevo.
- Bajo el cuadro de los **detalles del grupo de la identidad** seleccione el **grupo > HotSpot_Endpoints de la identidad del punto final**
- Bajo tecleo de las **condiciones cree la nueva condición (opción avanzada**).
- Bajo atributo selecto elija *ENDPOINTPURGE: ElapsedDays GREATERTHAN* 5 días

Verificación

Utilice el caso 1

1. El usuario conecta con el invitado SSID.
2. Él abre al navegador y tan pronto como se genere el tráfico HTTP, se visualiza el portal del invitado.
3. Una vez que el Usuario invitado autentica y valida el AUP, se visualiza una página del éxito.

4. Se envía un CoA del reautentificar (transparente al cliente).
5. La sesión del punto final se reautentifica con el acceso total a la red.
6. Cualquier conexión subsiguiente del invitado tiene que pasar la autenticación del invitado antes de acceder a la red.

Flujo de los registros vivos ISE RADIUS:

Utilice el caso 2

1. El usuario conecta con el invitado SSID.
2. Él abre al navegador y tan pronto como se genere el tráfico HTTP, se visualiza el portal del invitado.
3. Una vez que el Usuario invitado autentica y valida el AUP, se registra el dispositivo.
4. Se visualiza una página del éxito y se envía un CoA del reautentificar (transparente al cliente).
5. La sesión del punto final se reautentifica con el acceso total a la red.
6. Cualquier conexión subsiguiente 9s de la ráfaga permitió sin aplicar la autenticación del invitado mientras el punto final todavía esté en el grupo de la identidad del punto final configurado.

Flujo de los registros vivos ISE RADIUS:

Utilice el caso 3

1. El usuario conecta con el invitado SSID.
2. Él abre al navegador y tan pronto como se genere el tráfico HTTP, se visualiza una página AUP.
3. Una vez que el Usuario invitado valida el AUP, se registra el dispositivo.
4. Se visualiza una página del éxito y se envía un CoA de la Admin-restauración (transparente al cliente).
5. El punto final vuelve a conectar con el acceso total a la red.
6. Cualquier conexión subsiguiente de la ráfaga se permite sin aplicar la aceptación AUP (a menos que se configura de otra manera) para mientras siga habiendo el punto final en el grupo de la identidad del punto final configurado.

Local Switching de FlexConnect en AireOS

Cuando se configura el Local Switching de FlexConnect la red Admin necesita asegurar eso:

- Reoriente el ACL se configura como FlexConnect ACL.
- Reoriente el ACL se ha aplicado como directiva cualquier manera con El AP sí mismo bajo lengueta de **FlexConnect > WebAuthentication externo los ACL >** las **directivas >** selecto reorientan el ACL y el tecleo **se aplican**

O agregando la directiva el ACL al grupo de FlexConnect pertenece a (la **Tecnología inalámbrica > los grupos de FlexConnect >** seleccionan el grupo correcto **>** la **asignación > las directivas ACL** seleccionan la reorientación ACL y el tecleo agregan)

La adición de la directiva ACL acciona el WLC para empujar el ACL configurado hacia abajo a los miembros AP del grupo de FlexConnect. El error hacer esto da lugar a una red reorienta el problema.

Escenario del No nativo-ancla

En el auto-ancla (no nativa – Los escenarios del ancla) es importante resaltar los hechos siguientes:

- Reoriente el ACL necesita ser definido en del ancla el WLC no nativo y. Incluso cuando se aplica solamente en el ancla.
- La autenticación de la capa 2 es manejada siempre por el WLC no nativo. Esto es crítico durante las fases de diseño (también para resolver problemas) como toda la autenticación de RADIUS y el tráfico que considera ocurre entre el ISE y el WLC no nativo.

- La reorientación AVP se aplica una vez a la sesión de cliente que el WLC no nativo pone al día a la sesión de cliente en el ancla a través de un mensaje de las manos de la movilidad.
- En este momento el WLC del ancla comienza a aplicar la reorientación usando el Reorientar-ACL se ha preconfigurado que.
- Las estadísticas se deben apagar totalmente en el WLC SSID del ancla para evitar las actualizaciones que consideran que van hacia el ISE (que se refiere al mismo evento de la autenticación) que viene ambos del ancla y no nativo.
- Los ACL basados URL no se soportan en los escenarios del No nativo-ancla.

Troubleshooting

Estados rotos comunes en AireOS y el WLC convergido del acceso

1. **El cliente no puede unirse a al invitado SSID**

Un "**cliente de la demostración detalló xx: xx: xx: xx: xx: xx**" revela que pegan al cliente en el **COMIENZO**. Esto es generalmente un indicador del WLC que no puede aplicar un atributo ese las devoluciones del servidor de AAA.

Verifique que el nombre de la reorientación ACL avanzado por el ISE haga juego exactamente el nombre del ACL predefinido en el WLC.

El mismo principio se aplica a cualquier otro atributo que usted ha configurado el ISE para empujar hacia abajo al WLC (identificaciones de VLAN, nombres de la interfaz, Airespace-ACL, etc). El cliente debe entonces transición al DHCP y entonces a CENTRAL_WEB_AUTH.

2. **Reoriente los AVP se aplican a la sesión de cliente pero reorientan no está trabajando**

Verifique que el estado del administrador de la directiva del cliente sea CENTRAL_WEB_AUTH con un IP Address válido según la interfaz dinámica configurada para el SSID y también que la reorientación ACL y URL-reorienta los atributos está aplicada a la sesión de cliente.

Reoriente el ACL

En el WLCs de AIreOS la reorientación ACL debe permitir explícitamente el tráfico que no debe ser reorientado, como el DNS y el ISE en el puerto TCP 8443 en las ambas direcciones y el deny ip any any implícito acciona el resto del tráfico que se reorientará.

En el acceso convergido la lógica es el contrario. Niegue puentes ACE reorientan mientras que el permiso ACE acciona la reorientación. Esta es la razón por la cual se recomienda para permitir

explícitamente el puerto TCP 80 y 443.

Verifique el acceso al ISE sobre el puerto 8443 del VLA N del invitado. Si todo parece bueno de la perspectiva de la configuración la manera más fácil de moverse adelante es asir una captura detrás del adaptador de red inalámbrica del cliente y verificar donde la reorientación se rompe.

- ¿El resoultion DNS sucede?
- ¿El way handshake TCP 3 se acaba contra la página pedida?
- ¿El WLC vuelve una acción de la reorientación después de que el cliente inicie el GET?
- ¿El way handshake TCP 3 contra el ISE sobre 8443 se completa?

3. **El cliente no puede acceder la red después del ISE avanzó un cambio de VLAN en el final del flujo del invitado**

Una vez que el cliente asió un IP Address al principio del flujo (pre reoriente el estado), si un cambio de VLAN se empuja hacia abajo después de que suceda la autenticación del invitado (CoA del poste reautentifique), la única manera de forzar una versión del DHCP/renueva en el invitado que el flujo (sin el agente de la postura) está a través de los subprogramas java que en los dispositivos móviles no trabaja.

Esto deja el cliente negro-agujereado en el VLA N X con una dirección IP del VLAN Y. Esto debe ser considerada mientras que planea la solución.

4. **El ISE muestra el "error interno HTTP 500, mensaje no encontrado de la sesión del radio" en el invitado que el navegador de cliente durante reorienta**

Esto es generalmente un indicador de la pérdida de la sesión en el ISE (se ha terminado la sesión). La mayoría de las razones comunes para esto están considerando configuraron en el WLC del ancla cuando se ha desplegado el No nativo-ancla. Para reparar estas estadísticas de la neutralización en el ancla y dejar la autenticación y las estadísticas no nativas de la manija.

5. **Las desconexiones del cliente y siguen siendo disconnected o conectan con un diverso SSID después de validar el AUP en el portal del hotspot ISE.**

Esto se puede esperar en el hotspot debido al cambio dinámico de la autorización (CoA) implicado en este flujo (CoA Admin reajustado) ese las causas el WLC para publicar un deauth a la estación inalámbrica. La mayoría de los puntos finales de red inalámbrica no tiene ninguna problemas a volver al SSID después de que suceda la de-autenticidad, pero el cliente conecta en algunos casos con otro SSID preferido en respuesta al de-authenitcate event. Nada se puede hacer del ISE o del WLC para prevenir esto como incumbe hasta el cliente de red inalámbrica a pegarse al SSID original, o para conectar con otro SSID (preferido) disponible.

En este caso el usuario de red inalámbrica debe conectar manualmente de nuevo al hotspot SSID.

WLC de AireOS

(Cisco Controller) >debug client <MAC addr>

El cliente del debug fija PARA HACER EL DEBUG DE un conjunto de los componentes implicados en los cambios de la máquina de estado del cliente.

(Cisco Controller) >debug client <MAC addr>

Componentes del debug AAA

(Cisco Controller) >debug client <MAC addr>

Éste puede ser recursos del impacto dependiendo de la cantidad de usuarios que conecten con MAB o el dot1x SSID. Estos componentes en el nivel de debug registran las transacciones AAA entre el WLC y el ISE e imprimen los paquetes RADIUS en la pantalla.

Esto es crítico si usted que el ISE puede no entregar los atributos previstos, o si el WLC no los procesa correctamente.

El Red-auth reorienta

(Cisco Controller) >debug client <MAC addr>

Esto se puede utilizar para verificar que el WLC está accionando con éxito la reorientación. Éste es un ejemplo de cómo la reorientación debe parecer de los debugs:

(Cisco Controller) >debug client <MAC addr>

NGWC

El cliente del debug fija PARA HACER EL DEBUG DE un conjunto de los componentes implicados en los cambios de la máquina de estado del cliente.

(Cisco Controller) >debug client <MAC addr>

Este componente imprime los paquetes RADIUS (autenticación y las estadísticas) en la pantalla. Esto es práctico cuando usted necesita verificar que el ISE entregue los AVP derechos y también verificar que el CoA se está enviando y se está procesando correctamente.

(Cisco Controller) >debug client <MAC addr>

Esto todas las transiciones AAA (autenticación, autorización y estadísticas) donde están implicados los clientes de red inalámbrica. Esto es crítico de verificar que el WLC analiza correctamente los AVP y los aplica a la sesión de cliente.

(Cisco Controller) >debug client <MAC addr>

Esto puede habilitado cuando usted sospecha un problema de la reorientación en el NGWC.

(Cisco Controller) >debug client <MAC addr>

ISE

Registros vivos RADIUS

Verifique la petición inicial MAB se ha procesado correctamente en el ISE y ese ISE echa los atributos atrás previstos. Navegue a las **operaciones > al RADIUS > los registros vivos** y filtre la salida usando el MAC de cliente bajo **ID del punto final**. Una vez que se encuentra el evento de la autenticación, haga clic en los detalles y después verifique los resultados avanzados como parte del validar.

Tcpdump

Esta característica puede ser utilizada cuando una mirada más profunda en el intercambio del paquete RADIUS entre el ISE y el WLC es necesaria. Esta manera usted puede probar que el ISE envía los atributos correctos en el access-accept sin tener que habilitar los debugs en el lado del WLC. Para comenzar una captura usando TCDDump para navegar a las **operaciones > al Troubleshooting > a las herramientas >General > al tcpdump de las herramientas de diagnóstico.**

Éste es un ejemplo de un flujo correcto capturado con el tcpdump

Aquí están los AVP enviados en respuesta a la petición inicial MAB (segundo paquete en el tiro de pantalla antedicho).

```
(Cisco Controller) >debug client <MAC addr>
```

Debugs del punto final:

Si usted necesita zambullirse más profundo en los procesos ISE que implican las decisiones de políticas, la selección porta, la autenticación del invitado, el CoA que dirige, el etc la manera más fácil de acercarse a esto es habilitar los **debugs de Endpoit** en vez de tener que fijar los componentes completos al nivel de debug.

Para habilitar esto, navegue a las **operaciones > al troubleshooting > a DiagnosticTools > las herramientas > debug generales del punto final.**

Una vez en la página del debug del punto final, ingrese el MAC address del punto final y haga clic el comienzo cuando está listo para reconstruir el problema.

El debug se ha parado una vez hace clic en el link que identifica el ID del punto final para descargar la salida de los debugs.

Información Relacionada

TAC recomendó las estructuras de AireOS

Guía de configuración de controlador de la tecnología inalámbrica de Cisco, versión 8.0.

Guía del administrador del Cisco Identity Services Engine, 2.1 de la versión

Configuración de red inalámbrica universal NGWC con el Identity Services Engine