Autenticación Web central con FlexConnect AP en un WLC con el ejemplo de configuración ISE

Contenido

Introducción

Este documento describe cómo configurar la autenticación Web central con el (APS) de los Puntos de acceso de FlexConnect en un regulador del Wireless LAN (WLC) con el Identity Services Engine (ISE) en el modo del Local Switching.

Nota importante: Ahora, la autenticación local en el FlexAPs no se soporta para este escenario.

Otros documentos en esta serie

- Autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine
- Autenticación Web central en el ejemplo de configuración del WLC y ISE

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Identity Services Engine (ISE), versión 1.2.1
- Software del regulador del Wireless LAN, versión - 7.4.100.0

Configurar

Hay métodos múltiples para configurar la autenticación Web central en el regulador del Wireless LAN (WLC). El primer método es la autenticación Web local en la cual el WLC reorienta el tráfico HTTP a un interno o a un servidor externo donde se indica al usuario que autentique. El WLC después trae las credenciales (devueltas vía una petición get HTTP en el caso de un servidor externo) y hace una autenticación de RADIUS. En el caso de un Usuario invitado, un servidor externo (tal como servidor del motor del servicio de la identidad (ISE) o del invitado del NAC (NG)) se requiere mientras que el portal proporciona las características tales como registro y uno mismo-aprovisionamiento del dispositivo. Este proceso incluye estos pasos:

1. Los socios del usuario a la autenticación Web SSID.
2. El usuario abre a su navegador.
3. El WLC reorienta al portal del invitado (tal como ISE o NG) tan pronto como se ingrese un URL.
4. El usuario autentica en el portal.
5. El portal del invitado reorienta de nuevo al WLC con las credenciales ingresadas.
6. El WLC autentica al Usuario invitado vía el RADIUS.
7. El WLC reorienta de nuevo al URL original.

Este proceso incluye mucho cambio de dirección. El nuevo acercamiento es utilizar la autenticación Web central que trabaja con ISE (versiones más adelante de 1.1) y el WLC (versiones más adelante de 7.2). Este proceso incluye estos pasos:

1. Los socios del usuario a la autenticación Web SSID.
2. El usuario abre a su navegador.
3. El WLC reorienta al portal del invitado.
4. El usuario autentica en el portal.
5. El ISE envía un cambio RADIUS de la autorización (CoA - el puerto 1700 UDP) de indicar al regulador que el usuario es válido y avanza eventual los atributos de RADIUS tales como la lista de control de acceso (ACL).
6. Se indica al usuario que revise el URL original.

Esta sección describe los pasos necesarios configurar la autenticación Web central en el WLC y el ISE.

Diagrama de la red

Esta configuración utiliza esta configuración de red:

Configuración del WLC

La configuración del WLC es bastante directa. ¿Un “truco? se utiliza (lo mismo que en el Switches) para obtener la autenticación dinámica URL del ISE. (Puesto que utiliza el CoA, una sesión necesita ser creada como el ID de sesión es parte del URL.) El SSID se configura para utilizar el MAC que filtra, y el ISE se configura para volver un mensaje del access-accept incluso si la dirección MAC no se encuentra de modo que envíe el cambio de dirección URL para todos los usuarios.

Además, el Network Admission Control (NAC) RADIUS y la invalidación AAA deben ser habilitados. El NAC RADIUS permite que el ISE envíe una petición CoA que indique ahora autentican al usuario y puede acceder la red. También se utiliza para la evaluación de la postura en la cual el ISE cambia el perfil del usuario basado en el resultado de la postura.

1. Asegúrese de que el servidor de RADIUS haga el RFC3576 (CoA) habilitar, que es el valor por defecto.

2. Cree una nueva red inalámbrica (WLAN). Este ejemplo crea una nueva red inalámbrica (WLAN) nombrada *CWAFlex* y la asigna a vlan33. (Nota que no tendrá mucho efecto puesto que el Punto de acceso está en el modo del Local Switching.)

3. En la ficha de seguridad, permiso MAC que filtra como Seguridad de la capa 2.

4. En la lengueta de la capa 3, asegúrese que la Seguridad esté inhabilitada. (Si la autenticación Web se habilita en la capa 3, se habilita la autenticación Web local, autenticación Web no central.)

5. En los servidores de AAA tabule, seleccione el servidor ISE como servidor de RADIUS para la red inalámbrica (WLAN). Opcionalmente, usted puede seleccionarla para considerar para tener más información detallada en el ISE.

6. En la ficha Avanzadas, asegure permiten la invalidación AAA se marca y el NAC del radio se selecciona para el estado del NAC.

7. Cree una reorientación ACL.

   ThisACL se refiere al mensaje del access-accept del theISE y define qué tráfico debe ser reorientado (negado por el theACL) así como qué tráfico no debe ser reorientado (permitido por el theACL). Básicamente, el DNS y el tráfico a/desde el theISE necesita ser permitido.

Nota: Un problema con FlexConnect AP es que usted debe crear un FlexConnect ACL a parte de su ACL normal. Este problema se documenta en el bug Cisco CSCue68065 y se repara en la versión 7.5. En el WLC 7.5 y posterior, solamente se requiere un FlexACL, y no hay ACL estándar necesario. El WLC cuenta con que la reorientación ACL vuelta por el ISE sea un ACL normal. Sin embargo, asegurarlo trabaja, usted necesita el mismo ACL aplicado que el FlexConnect ACL.
Este ejemplo muestra cómo crear un FlexConnect ACL nombrado *flexred*:

Cree las reglas para permitir el tráfico DNS así como el tráfico hacia el ISE y para negar el resto.

Si usted quiere la seguridad máxima, usted puede permitir solamente el puerto 8443 hacia el ISE. (Si posturing, usted debe agregar los puertos típicos de la postura, tales como 8905,8906,8909,8910.)

(Solamente en el código antes de la versión 7.5 debido a CSCue68065) elija la **Seguridad > las listas de control de acceso** para crear un ACL idéntico con el mismo nombre.

Prepare el FlexConnect específico AP. Observe que para un despliegue más grande, usted utilizaría típicamente a los grupos de FlexConnect y no realizaría estos elementos sobre una base por-AP por los motivos de escalabilidad.

Haga clic la **Tecnología inalámbrica**, y seleccione el Punto de acceso específico.Haga clic la lengueta de **FlexConnect**, y haga clic **Webauthentication externo ACL**. (Antes de la versión 7.4, esta opción fue nombrada las *directivas de la red*.)

Agregue el ACL (nombrado *flexred* en este ejemplo) al área de directivas de la red. Esto PRE-empujes el ACL al Punto de acceso. No se aplica todavía, pero el contenido ACL se da al AP de modo que pueda aplicarse cuando esté necesitado.

La configuración del WLC es completa ahora.

Configuración ISE

Cree el perfil de la autorización

Complete estos pasos para crear el perfil de la autorización:

1. Haga clic la **directiva**, y después haga clic los **elementos de la directiva**.
2. Haga clic los **resultados**.
3. Amplíe la **autorización**, y después haga clic el **perfil de la autorización**.
4. Haga clic el **botón Add** para crear un nuevo perfil de la autorización para el webauth central.
5. En el **campo de nombre**, ingrese un nombre para el perfil. Este ejemplo utiliza *CentralWebauth*.
6. Elija **ACCESS_ACCEPT de la** lista desplegable del tipo de acceso.
7. Marque la casilla de verificación de la **autenticación Web**, y elija el **auth centralizado de la red de la** lista desplegable.
8. En el campo ACL, ingrese el nombre del ACL en el WLC que define el tráfico que será reorientado. Este los ejemplos utilizan *flexred*.
9. Elija el **valor por defecto de la** lista desplegable de la reorientación.

El atributo de la reorientación define si el ISE ve el portal de Web predeterminada o un portal web de encargo que el ISE admin creó. Por ejemplo, el ACL *flexred* en este ejemplo acciona un cambio de dirección sobre el tráfico HTTP del cliente a dondequiera.

Cree una regla de la autenticación

Complete estos pasos para utilizar el perfil de la autenticación para crear la regla de la autenticación:

1. Bajo menú de la directiva, haga clic la **autenticación**. Esta imagen muestra un ejemplo de cómo configurar la regla de la política de autenticación. En este ejemplo, se configura una regla que accionará cuando se detecta la filtración MAC.

2. Ingrese un nombre para su regla de la autenticación. Este ejemplo utiliza la *Tecnología inalámbrica mab*.
3. Seleccione (**+**) el icono más en si campo de la condición.
4. Elija la **condición compuesta**, y después elija **Wireless_MAB**.
5. Elija el “acceso de red predeterminada” como protocolo permitido.
6. Haga clic la flecha localizada al lado de **y…** para ampliar la regla más lejos.
7. Haga clic **+** icono en el campo de fuente de la identidad, y elija los **puntos finales internos**.
8. Elija **continúan del** si lista desplegable no encontrada del usuario.

Esta opción permite que un dispositivo sea autenticado (a través del webauth) incluso si su dirección MAC no se sabe. Los clientes del dot1x pueden todavía autenticar con sus credenciales y no deben ser tratados a esta configuración.

Cree una regla de la autorización

Ahora hay varias reglas a configurar en la directiva de la autorización. Cuando el PC es asociado, pasará con la filtración del mac; se asume que la dirección MAC no está sabida, así que se vuelven el webauth y el ACL. Esta regla *no sabida MAC* se muestra en la imagen abajo y se configura en esta sección.

Complete estos pasos para crear la regla de la autorización:

1. Cree una nueva regla, y ingrese un nombre. Este ejemplo utiliza el *MAC no sabido*.
2. Haga clic (**+**) el icono más en el campo de la condición, y elija crear una nueva condición.
3. Amplíe la lista desplegable de la **expresión**.
4. Elija el **acceso a la red**, y amplíelo.
5. Haga clic **AuthenticationStatus**, y elija al operador de los **iguales**.
6. Elija **UnknownUser** en el campo derecho.
7. En la página general de la autorización, elija **CentralWebauth** (perfil de la autorización) en el campo a la derecha de la palabra **entonces**.Este paso permite que el ISE continúe aunque no saben al usuario (o el MAC).Ahora presentan los usuarios desconocidos con la página de registro. Sin embargo, una vez que ingresan sus credenciales, se presentan otra vez con un pedido de autenticación en el ISE; por lo tanto, otra regla se debe configurar con una condición se cumpla que si el usuario es Usuario invitado. En este ejemplo, *si* utilizan al *invitado de los iguales de UseridentityGroup*, y él se asume que todos los invitados pertenecen a este grupo.
8. Haga clic las acciones abotonan situado en el final de la regla *no sabida MAC*, y eligen insertar una nueva regla arriba.**Nota:** Es muy importante que esta nueva regla viene antes de la regla *no sabida MAC*.
9. Ingrese el **2do AUTH** en el campo de nombre.
10. Seleccione a un grupo de la identidad como condición. Este ejemplo eligió al **invitado**.
11. En el campo de la condición, haga clic (**+**) el icono más, y elija crear una nueva condición.
12. Elija el **acceso a la red**, y haga clic **UseCase**.
13. Elija los **iguales** como el operador.
14. Elija **GuestFlow** como el operando correcto. Esto significa que usted cogerá a los usuarios que apenas abrieron una sesión en la página web y se vuelven después de que un cambio de la autorización (la parte del flujo del invitado la regla) y solamente si pertenecen al grupo de la identidad del invitado.
15. En la página de la autorización, haga clic (**+**) el icono más (situado al lado de *entonces*) para elegir un resultado para su regla.

    En este ejemplo, se asigna un perfil preconfigurado (vlan34); esta configuración no se muestra en este documento.

    Usted puede elegir una opción del **acceso del permiso** o crear un perfil de encargo para volver el VLA N o los atributos ese usted tiene gusto.

Nota importante: En ISE Version1.3, dependiendo del tipo de autenticación Web, “el caso del uso del flujo del invitado” no se pudo encontrar más. La regla de la autorización

entonces tendría que contener al grupo de usuarios del invitado como la única condición posible.

Habilite la renovación IP (opcional)

Si usted asigna un VLA N, el último paso está para PC del cliente para renovar su dirección IP. Este paso es alcanzado por el portal del invitado para los clientes de Windows. Si usted no fijó un VLA N para la *2da* regla *AUTH* anterior, usted puede saltar este paso.

Observe que en FlexConnect AP, el VLA N necesita preexistir en el AP sí mismo. Por lo tanto, si no lo hace, usted puede crear una asignación en el AP sí mismo VLAN-ACL o en el grupo de la flexión donde usted no aplica ningún ACL para el nuevo VLA N usted quiere crear. Eso crea realmente un VLA N (sin el ACL en él).

Si usted asignó un VLA N, complete estos pasos para habilitar la renovación IP:

1. Haga clic la **administración**, y después haga clic la **Administración del invitado**.
2. Haga clic las **configuraciones**.
3. Amplíe al **invitado**, y después amplíe la **configuración Multi-porta**.
4. Haga clic **DefaultGuestPortal** o el nombre de un portal de encargo que usted pudo haber creado.
5. Haga clic la casilla de verificación de la **versión del DHCP de Vlan**.**Nota:** Esta opción trabaja solamente para los clientes de Windows.

Flujo de tráfico

Puede parecer difícil entender qué tráfico se envía donde en este escenario. Aquí está un estudio rápido:

- El cliente envía la petición de la asociación sobre el aire para el SSID.
- El WLC maneja la autenticación de filtración MAC con el ISE (donde recibe los atributos del cambio de dirección).
- El cliente recibe solamente una respuesta del assoc después de que la filtración MAC sea completa.
- El cliente presenta un pedido de DHCP y eso **LOCALMENTE** es conmutada por el obain del Punto de acceso para una dirección IP del sitio remoto.
- En el estado de Central_webauth, el tráfico marcado para niega en la reorientación ACL (así que HTTP típicamente) **CENTRALMENTE** se conmuta. No es tan el AP que hace el cambio de dirección pero el WLC; por ejemplo, cuando el cliente pide cualquier sitio web, el AP envía esto al WLC encapsulado en CAPWAP y las parodias del WLC que la dirección IP del sitio web y reorienta hacia el ISE.
- Reorientan al cliente al ISE reorienta el URL. Esto **LOCALMENTE** se conmuta otra vez (porque golpea en el permiso en la flexión reorienta el ACL).
- Una vez en el estado de FUNCIONAMIENTO, el tráfico localmente se conmuta.

Verificación

Una vez que asocian al usuario al SSID, la autorización se visualiza en la página ISE.

De la parte inferior para arriba, usted puede ver la autenticación de filtración de la dirección MAC que vuelve los atributos CWA. Está después el login porta con el Nombre de usuario. El ISE entonces envía un CoA al WLC y la autenticación más reciente es una autenticación de filtración del mac de la capa 2 en el lado del WLC, pero el ISE recuerda el cliente y el nombre de usuario y aplica el VLA N necesario que configuramos en este ejemplo.

Cuando cualquier direccionamiento se abre en el cliente, reorientan al navegador al ISE. Asegúrese que el Domain Name System (DNS) esté configurado correctamente.

Se concede el acceso a la red después de que el usuario valide las directivas.

En el regulador, el estado del Administrador de directivas y los cambios de estado del NAC RADIUS de *POSTURE_REQD A EJECUTARSE*.