Autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine

Contenido

Introducción

Este documento describe cómo configurar la autenticación Web central con los clientes atados con alambre conectados con el Switches con la ayuda del Identity Services Engine (ISE).

El concepto de autenticación Web central se opone a la autenticación Web local, que es la autenticación Web usual en el Switch sí mismo. En ese sistema, sobre el error dot1x/mab, el Switch Conmutación por falla al perfil del webauth y reorientará el tráfico del cliente a una página web en el Switch.

La autenticación Web central ofrece la posibilidad para tener un dispositivo central que actúe como portal web (en el th es el ejemplo, el ISE). La diferencia principal comparada a la autenticación Web local usual es que está desplazada para acodar 2 junto con la autenticación mac/dot1x. El concepto también diferencia en que el servidor de RADIUS (ISE en este ejemplo) vuelve los atributos especiales que indican al Switch que un cambio de dirección de la red debe ocurrir. Esta solución tiene la ventaja para eliminar cualquier retardo que fuera necesario para que la autenticación Web golpee con el pie. Global, si la dirección MAC de la estación del cliente no es sabida por el servidor de RADIUS (pero otros criterios puede también ser utilizado), los

atributos del cambio de dirección de las devoluciones del servidor, y el Switch autoriza la estación (vía el [MAB] de puente de la autenticación de MAC) pero pone una lista de acceso para reorientar el tráfico de la Web al portal. Una vez que el usuario abre una sesión en el portal del invitado, es posible vía CoA (cambio de la autorización) despedir el puerto del switch de modo que ocurra una nueva autenticación MAB de la capa 2. El ISE puede entonces recordar que era usuario del webauth y aplicar los atributos de la capa 2 (como VAN dinámico assignment) al usuario. Un componente de ActiveX puede también forzar PC del cliente para restaurar su dirección IP.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE)
- Configuración del switch del ® del Cisco IOS

Componentes Utilizados

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

- Cisco Identity Services Engine (ISE), versión 1.1.1
- Cisco Catalyst 3560 Series Switch que funciona con la versión de software 12.2.55SE3

  Note: El procedimiento es similar o idéntico para otros modelos del switch Catalyst. Usted puede utilizar estos pasos en todas las versiones de Cisco IOS Software para el Catalyst a menos que se indique lo contrario.

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.

Configurar

Información general

La configuración ISE se compone de estos cinco pasos:

1. Cree el Access Control List transferible (ACL).
2. Cree el perfil de la autorización.
3. Cree una regla de la autenticación.
4. Cree una regla de la autorización.
5. Habilite la renovación IP (opcional).

Cree ACL descargable

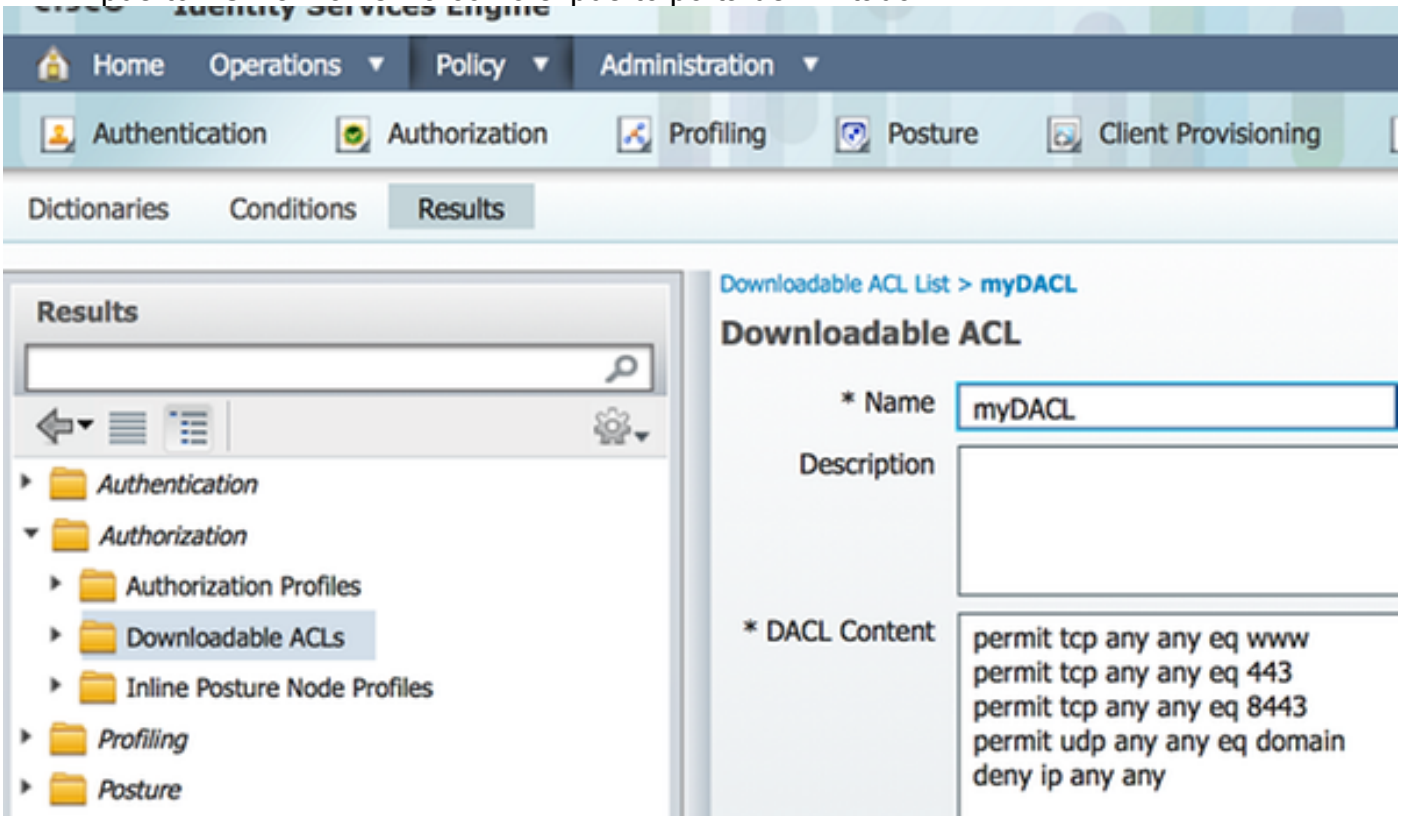
Esto no es un paso obligatorio. La reorientación ACL devuelta con el perfil central del webauth determina que el tráfico (HTTP o HTTPS) se reorienta al ISE. ACL descargable permite que usted defina se permite qué tráfico. Usted debe tener en cuenta típicamente el DNS, el HTTP, y 8443 y negar el resto. Si no, el Switch reorienta el tráfico HTTP pero permite otros protocolos.

Complete estos pasos para crear ACL descargable:

1. Haga clic la **directiva**, y haga clic los **elementos de la directiva**.
2. Haga clic los **resultados**.
3. Amplíe la **autorización**, y haga clic los **ACL transferibles**.
4. Haga clic el **botón Add** para crear un nuevo ACL descargable.
5. En el **campo de nombre**, ingrese un nombre para el DACL. Este ejemplo utiliza el *myDACL*.

Esta imagen muestra el contenido típico DACL, que permite:

- DNS - resuelva el nombre de host del portal ISE
- HTTP y HTTPS - permita el cambio de dirección
- El puerto TCP 8443 - sirva como el puerto porta del invitado



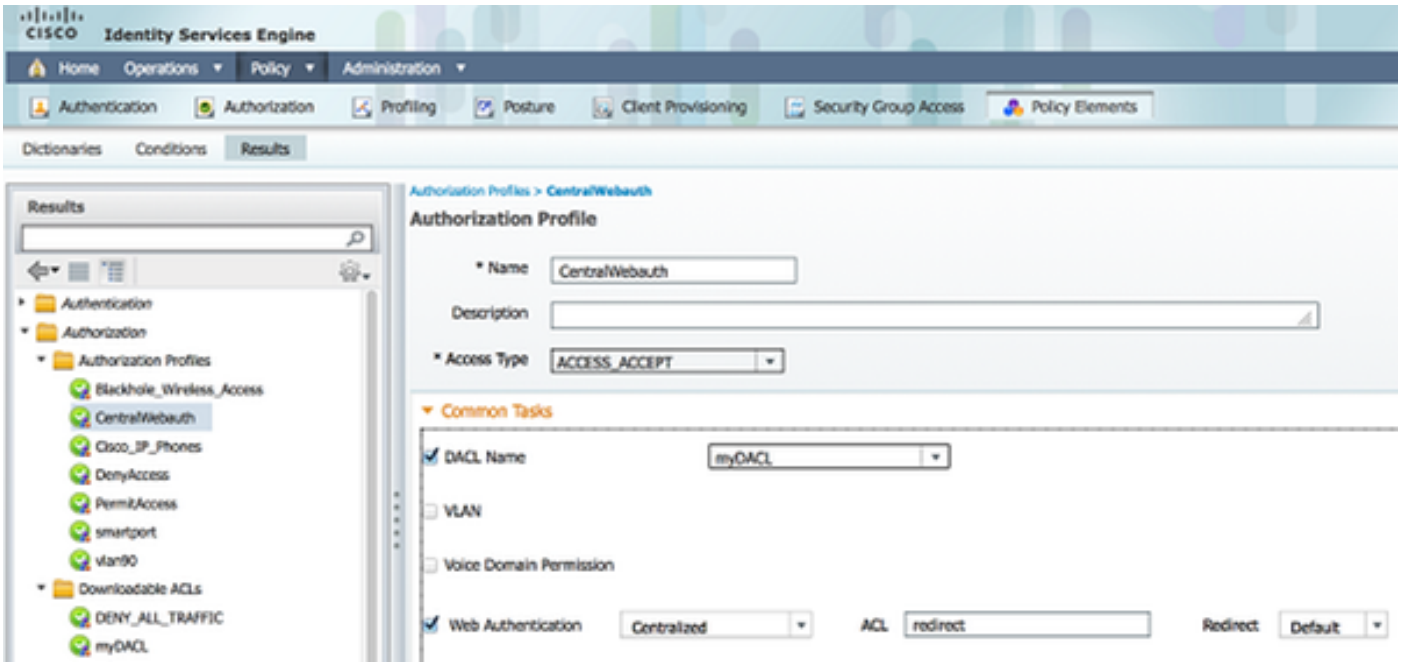
Cree el perfil de la autorización

Complete estos pasos para crear el perfil de la autorización:

1. Haga clic la **directiva**, y haga clic los **elementos de la directiva**.
2. Haga clic los **resultados**.
3. Amplíe la **autorización**, y 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 **centralizado de la** lista desplegable.
8. En el campo ACL, ingrese el nombre del ACL en el Switch que define el tráfico que se reorientará. Este los ejemplos utilizan *reorientan*.
9. Elija el **valor por defecto de la** lista desplegable de la reorientación.
10. Marque el checkbox del **nombre DACL**, y elija el **myDACL del** lsit del descenso-abajo si usted decide utilizar un DACL en vez de un puerto estático ACL en el Switch.

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, la *reorientación* ACL en este ejemplo acciona un cambio de dirección sobre el tráfico HTTP o HTTPS del cliente a dondequiera. El ACL se define en el Switch más adelante en este ejemplo de configuración.

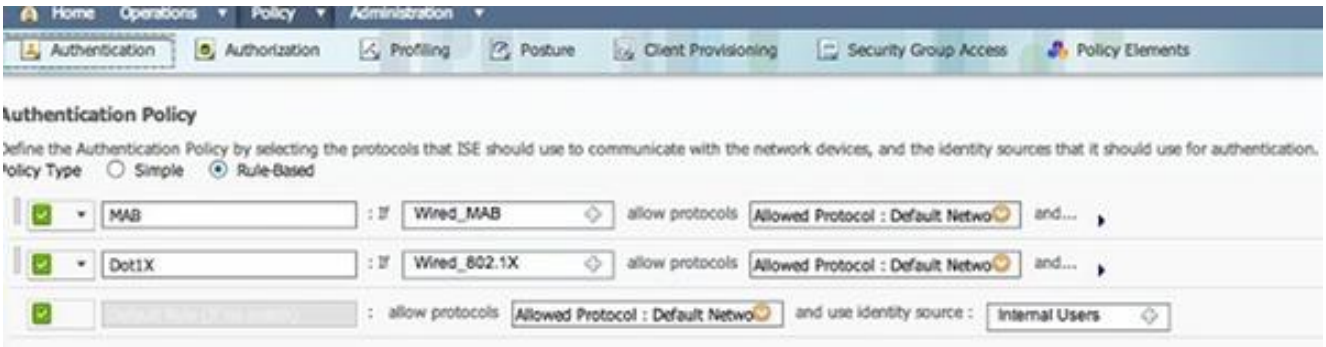


Cree una regla de la autenticación

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**.

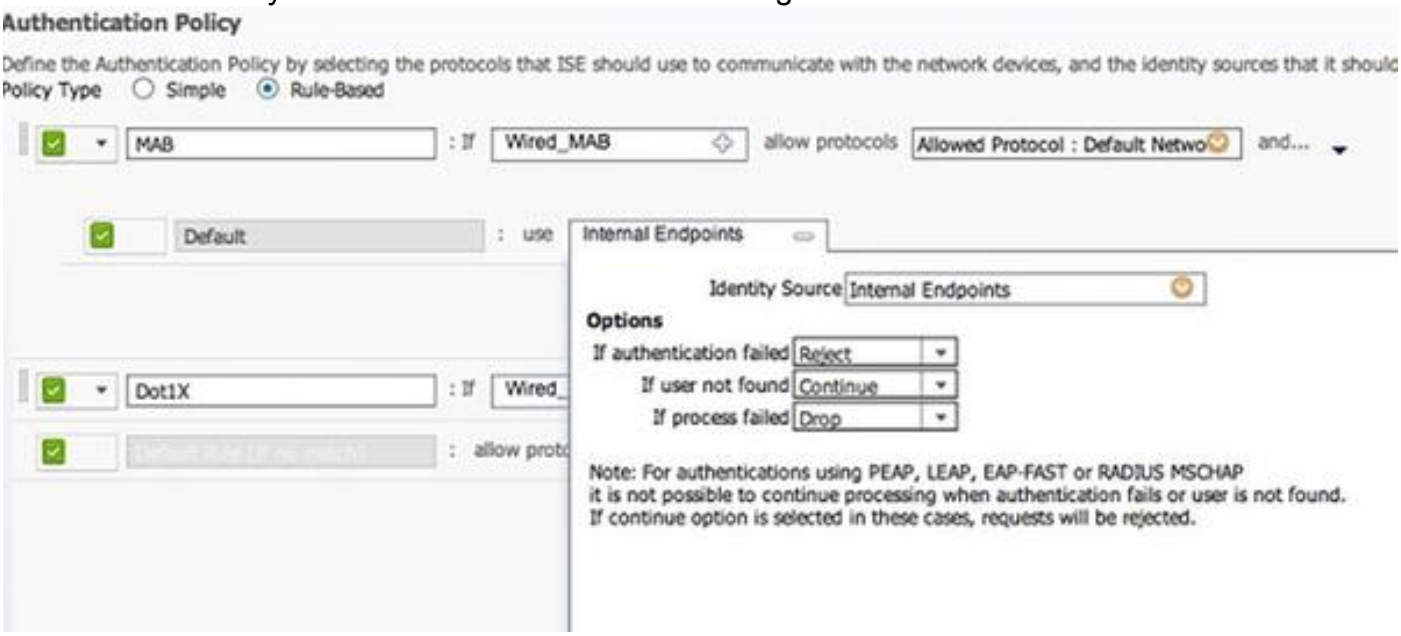
   Esta imagen muestra un ejemplo de cómo configurar la regla de la política de autenticación. En este ejemplo, se configura una regla que acciona cuando se detecta el MAB.



2. Ingrese un nombre para su regla de la autenticación. Este ejemplo utiliza el *MAB*.
3. Seleccione (**+**) el icono más en si campo de la condición.

4. Elija la **condición compuesta**, y elija **Wired_MAB**.
5. Haga clic la flecha localizada al lado de **y…** para ampliar la regla más lejos.
6. Haga clic **+** icono en el campo de fuente de la identidad, y elija los **puntos finales internos**.
7. 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 se enchufa el PC, pasa con el MAB; 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 esta imagen 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.

   Note: Es muy importante que esta nueva regla viene antes de la regla *no sabida MAC*.
9. Ingrese un nombre para la nueva regla. Este ejemplo utiliza al Ser-uno-*INVITADO*.
10. Elija una condición que haga juego a sus Usuarios invitados.

    Este ejemplo utiliza *InternalUser: IdentityGroup iguala al invitado* porque todos los Usuarios invitados están limitados al grupo del *invitado* (o a otro grupo que usted configuró en sus configuraciones del patrocinador).
11. Elija **PermitAccess** en el cuadro del resultado (situado a la derecha de la palabra *entonces*).

    Cuando autorizan al usuario en la página de registro, el ISE recomienza una autenticación de la capa 2 en el puerto del switch, y un nuevo MAB ocurre. En este escenario, la diferencia es que un indicador invisible está fijado para que el ISE recuerde que era usuario invitado-autenticado. Esta regla es *2do AUTH*, y la condición es *acceso a la red: UseCase iguala GuestFlow*. Se cumple esta condición cuando el usuario autentica vía el webauth, y el puerto del switch se fija otra vez para un nuevo MAB. Usted puede asignar cualquier atributo que usted tenga gusto. Este ejemplo asigna un perfil *vlan90* para asignar el usuario el VLA N 90 en su segunda autenticación MAB.
12. Haga clic las **acciones** (situadas en el final de la regla del Ser-uno-INVITADO), y elija la **nueva regla del separador de millares arriba**.
13. Ingrese el **2do AUTH** en el campo de nombre.
14. En el campo de la condición, haga clic (**+**) el icono más, y elija crear una nueva condición.
15. Elija el **acceso a la red**, y haga clic **UseCase**.
16. Elija los **iguales** como el operador.
17. Elija **GuestFlow** como el operando correcto.
18. 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 (vlan90); esta configuración no se muestra en este documento.

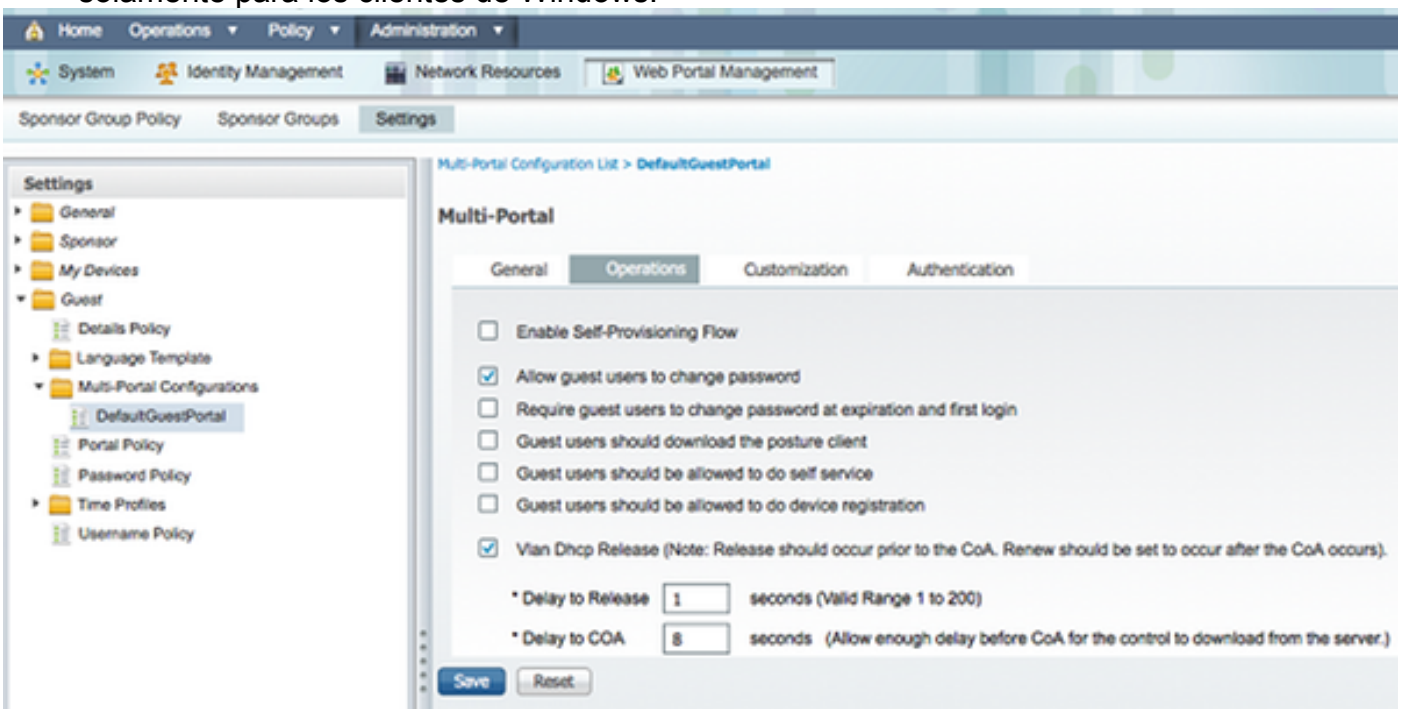
    Usted puede elegir una opción del **acceso del permiso** o crear un perfil de encargo para volver el VLA N o los atributos ese usted tiene gusto.

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.

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

1. Haga clic la **administración**, y haga clic la **Administración del invitado**.
2. Haga clic las **configuraciones**.
3. Amplíe al **invitado**, y 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 el cuadro de **Releasecheck del DHCP de Vlan**. **Note**: Esta opción trabaja solamente para los clientes de Windows.



Configuración del switch (extracto)

Esta sección proporciona un extracto de la configuración del switch. Vea la configuración del switch (llena) para la configuración total.

Esta muestra muestra una configuración simple MAB.

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

El VLAN 100 es el VLA N que proporciona la conectividad de red completa. Un puerto predeterminado ACL (*webauth* Nombrado) es aplicado y definido como se muestra aquí:

```
ip access-list extended webauth
permit ip any any
```

Esta configuración de muestra da el acceso a la red completo incluso si no autentican al usuario; por lo tanto, usted puede ser que quiera restringir el acceso a los usuarios de unauthenticated.

En esta configuración, el HTTP y el HTTPS que hojean no trabaja sin la autenticación (por el otro ACL) puesto que el ISE se configura para utilizar una reorientación ACL (nombrada *reoriente*). Aquí está la definición en el Switch:

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

Esta lista de acceso se debe definir en el Switch para definir en qué tráfico realizará el Switch el cambio de dirección. (Hace juego en el *permiso*.) En este ejemplo, cualquier tráfico HTTP o HTTPS que el cliente envíe los activadores un cambio de dirección de la red. Este ejemplo también niega la dirección IP ISE así que el tráfico al ISE va al ISE y no reorienta en un loop. (En este escenario, niegue no bloquea el tráfico; apenas no reorienta el tráfico.) Si usted utiliza los puertos HTTP inusuales o un proxy, usted puede agregar otros puertos.

Otra posibilidad es permitir el acceso HTTP a algunos sitios web y reorientar otros sitios web. Por ejemplo, si usted define en el ACL un permiso para los servidores Web internos solamente, los clientes podrían hojear la red sin la autenticidad pero encontrarían la reorientación si intentan acceder a un servidor Web interno.

El paso más reciente es permitir el CoA en el Switch. Si no, el ISE no puede forzar el Switch a reauthenticate al cliente.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

Este comando se requiere para que el Switch reoriente basado en el tráfico HTTP:

```
ip http server
```

Este comando se requiere para reorientar basado en el tráfico HTTPS:

```
ip http secure-server
```

Estos comandos son también importantes:

```
radius-server vsa send authentication
radius-server vsa send accounting
```

Si no autentican al usuario todavía, el **num> del <interface de la sesión internacional de la autenticación de la demostración** vuelve esta salida:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
```

```
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Note: A pesar de una autenticación acertada MAB, se pone la reorientación ACL puesto que la dirección MAC no era sabida por el ISE.

Configuración del switch (llena)

Esta sección enumera la configuración del switch completa. Se han omitido algunas interfaces y líneas de comando innecesarias; por lo tanto, esta configuración de muestra se debe utilizar para la referencia solamente y no debe ser copiada.

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Configuración de proxy de HTTP

Si usted utiliza un proxy de HTTP para sus clientes, significa que sus clientes:

- Utilice un puerto poco convencional para el protocolo HTTP
- Envíe todo su tráfico a ese proxy

Para hacer que el Switch escuche en el puerto poco convencional (por ejemplo, 8080), utilice estos comandos:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Usted también necesita configurar a todos los clientes para guardar el usar de su proxy pero para no utilizar el proxy para la dirección IP ISE. Todos los hojeadores incluyen una característica que permita que usted ingrese los nombres del host o los IP Addresses que no deben utilizar el proxy. Si usted no agrega la excepción para el ISE, usted encuentra una página de la autenticación del loop.

Usted también necesita modificar su cambio de dirección ACL para permitir en el puerto del proxy (8080 en este ejemplo).

NOTA IMPORTANTE sobre el Switch SVI

Ahora, el Switch necesita una interfaz virtual del Switch (SVI) para contestar al cliente y enviar el cambio de dirección del portal web al cliente. Este SVI no tiene que necesariamente estar en el cliente subnet/VLAN. Sin embargo, si el Switch no tiene ningún SVI en el cliente subnet/VLAN, tiene que utilizar un de los otros SVI y enviar el tráfico según lo definido en la tabla de ruteo del cliente. Esto significa típicamente que el tráfico está enviado a otro gateway en la base de la red; este tráfico vuelve al switch de acceso dentro de la subred cliente.

De los Firewall el tráfico del bloque típicamente y al mismo Switch, como en este escenario, así que el cambio de dirección no pudieron trabajar correctamente. Las soluciones alternativas son permitir este comportamiento en el Firewall o crear un SVI en el switch de acceso en la subred cliente.

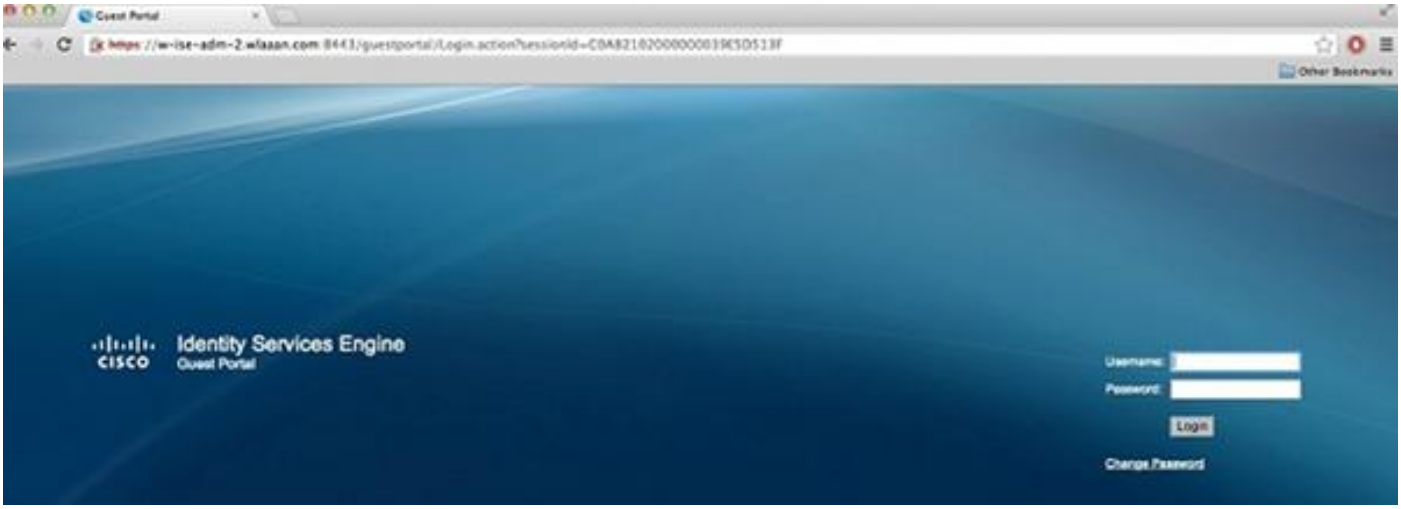
NOTA IMPORTANTE sobre el redireccionamiento HTTPS

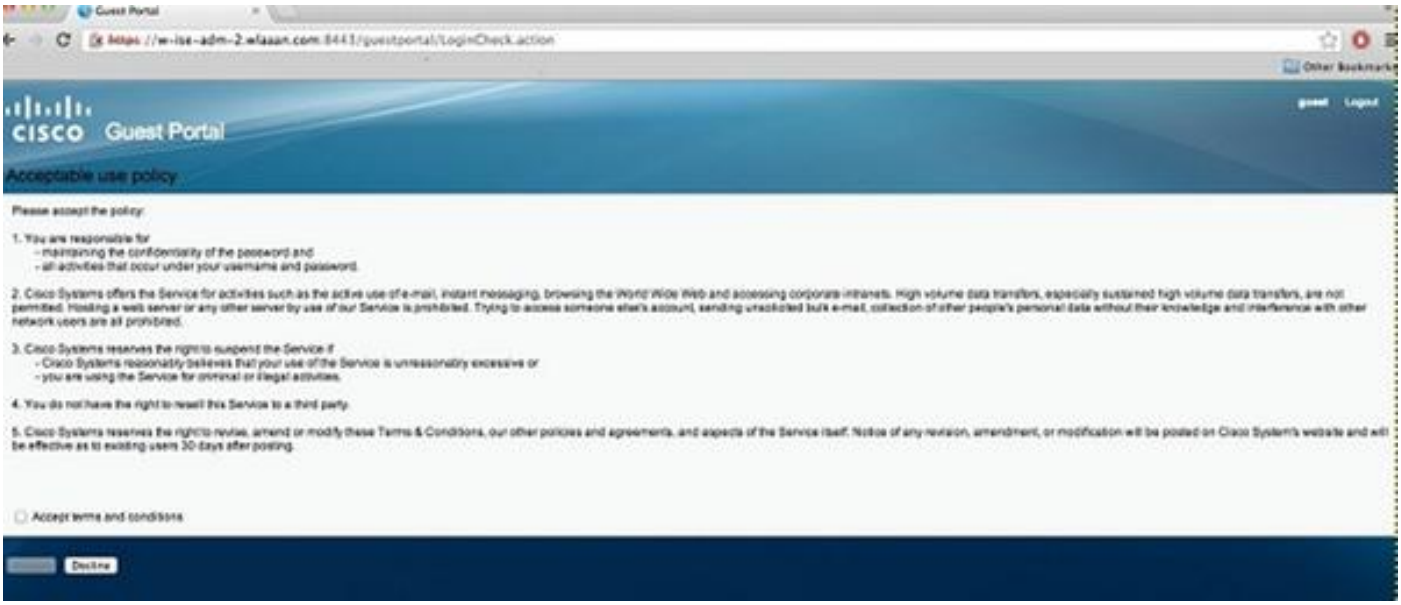
El Switches puede reorientar el tráfico HTTPS. Así, si el cliente del invitado tiene un homepage en el HTTPS, el cambio de dirección ocurre correctamente.

El concepto entero de cambio de dirección se basa sobre el hecho de que las parodias de un dispositivo (en este caso, el Switch) la dirección IP del sitio web. Sin embargo, un aspecto importante se presenta cuando el Switch intercepta y reorienta el tráfico HTTPS porque el Switch puede presentar solamente su propio certificado en el apretón de manos de Transport Layer Security (TLS). Puesto que éste no es el mismo certificado que el sitio web pidió originalmente, la mayoría del comandante del problema de los navegadores alerta. Los navegadores manejan correctamente el cambio de dirección y la presentación de otro certificado como problemas de seguridad. No hay solución alternativa para esto, y no hay manera para el Switch al spoof su certificado original del sitio web.

Resultado final

PC del cliente enchufa y realiza el MAB. La dirección MAC no se sabe, así que el ISE avanza los atributos del cambio de dirección de nuevo al Switch. El usuario intenta ir a un sitio web y se reorienta.





Cuando la autenticación de la página de registro es acertada, el ISE despide el switchport a través del cambio de la autorización, que comienza otra vez una autenticación MAB de la capa 2.

Sin embargo, el ISE sabe que es un cliente anterior del webauth y autoriza al cliente basado en las credenciales del webauth (aunque esto es una autenticación de la capa 2).

En los registros de la autenticación ISE, la autenticación MAB aparece en la parte inferior del registro. Aunque sea desconocida, la dirección MAC fue autenticada y perfilada, y los atributos del webauth fueron vueltos. Después, la autenticación ocurre con el nombre de usuario del usuario (es decir, los tipos de usuario sus credenciales en la página de registro). Inmediatamente después de la autenticación, una nueva autenticación de la capa 2 ocurre con el nombre de usuario como credenciales; este paso de la autenticación es donde usted puede volver atribuye tal VLAN dinámico.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco Identity Services Engine
- Guía de referencia de comandos del Cisco Identity Services Engine
- Integración de ISE (Identity Services Engine) con el WLC de Cisco (regulador del Wireless LAN)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems