Contenido

Introducción

Este documento describe las nuevas funciones en Identity Services Engine (ISE) que permita que el cambio de dirección ocurra con los dispositivos de acceso a la red de tercera persona (NAD).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Flujo del invitado en el ISE
- DNS y protocolos DHCP

Componentes Utilizados

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

- 2960 Series Switch de Cisco Catalys
- Cisco ISE, 2.1 de la versión

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Las funciones avanzadas como el invitado, la postura y Bring Your Own Device (BYOD) en las redes modernas, requieren la comunicación directa entre el dispositivo del cliente y el servidor de AAA. En las versiones anteriores ISE que esto fue lograda enviando un dinámico reoriente el URL y la lista de control de acceso (ACL) al NAD.

Hay dos atributos obligatorios que se envían en un perfil de la autorización para el cambio de dirección en el valor de atributo París (AV):

- ¿Pares del Cisco AV? Reoriente el URL: El valor URL es dinámico y se crea para cada sesión. Las partes importantes de reorientan el URL son el nombre del dominio aprobado de Fuly del nodo del servicio de la directiva (PSN FQDN) y ID de sesión.
- ¿Pares del Cisco AV? Reoriente el ACL: Este par AV contiene un nombre ACL que deba existir en el NAD. Con la ayuda de este ACL, el NAD decide a si los paquetes se reorientan o se permiten con el NAD.

El acercamiento tradicional del cambio de dirección se puede implementar solamente con los dispositivos de Cisco NAD. Para el soporte del otro vendedor NAD, el cambio de dirección URL estático había sido agregado en ISE 2.0. Mientras que este acercamiento es más independiente de la plataforma, todavía requiere el soporte de la redirección de HTTP en el NAD.

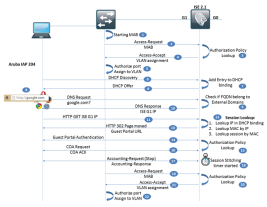
El comenzar con el 2.1 ISE un nuevo estilo de reorienta se ha agregado. Este acercamiento no requiere el soporte de la redirección de HTTP en el NAD. La idea principal detrás de este método es utilizar el ISE como dolina DNS.

El DNS y la funcionalidad del servidor DHCP se han agregado a la versión del 2.1 ISE para utilizarla como dolina DNS. Ahora el servidor ISE puede asignar los IP Addresses a los usuarios que necesitan ser reorientados y se define como servidor DNS. Esto permite que el ISE reoriente las conexiones del usuario a sí mismo sin ningunas funciones del servidor Web en el NAD. Sin embargo, el NAD debe todavía soportar el cambio de la asignación de la autorización (COA) y del VLAN dinámico.

En el ISE, este acercamiento se puede utilizar para estos flujos del cambio de dirección:

- Flujo del invitado: Las respuestas ISE a cualquier petición DNS iniciada por el usuario con su propia dirección IP. Esta respuesta hace al cliente establecer una conexión HTTP con el ISE. A este respecto, el ISE vuelve la reorientación URL usando la página estándar del código 302 HTTP movida.
- ¿BYOD/Posture (Anyconnect solamente)? en ambos escenarios, el supplicant nativo Provisioning la aplicación (NSP) o el módulo de la postura de Anyconnect inicia una conexión a enroll.cisco.com, que consigue reorientada al ISE usando los mismos pasos que el flujo del invitado.

Flujo de paquetes



1. El NAD comienza el proceso MAB para el dispositivo conectado. El proceso MAB en el comienzo de los switches Cisco según la prioridad del método de autentificación y no antes de la primera trama se recibe del dispositivo extremo.
2. El pedido de acceso MAB se envía al ISE.
3. El ISE evalúa la directiva de la autenticación y autorización para la petición entrante del acceso. Durante la evaluación de la directiva de la autorización, comparan al tipo de dispositivo de red (configuración del nivel NAD) con el tipo de dispositivo de red definido en el perfil de la autorización. Solamente los perfiles de la autorización para el tipo de dispositivo de red que corresponde con pueden ser seleccionados.

   Nota: Para el VLA N del invitado reoriente, el ISE necesita seleccionar un perfil de la autorización que contienen el cambio de dirección de la red (CWA, MDM, NSP, CPP) y la asignación VLAN. La necesidad del cliente de ser asignado a un segmento de red que tiene ISE como el único servidor DHCP.

1. El ISE vuelve un access-accept con la información de VLAN.
2. Conmute autoriza el puerto y aplica las configuraciones de VLAN.
3. El DHCP de los iniciados del cliente descubre. Si el PC está situado en el mismo segmento que el ISE, el paquete alcanza el ISE directamente. En caso de la Conectividad L3 entre el cliente y el ISE, el IP ISE se debe configurar como IP Helper Address en el NAD para el relé DHCP.
4. El ISE agrega la información del cliente a su tabla de vinculación del DHCP. IP del cliente y MAC son utilizados por el ISE para las operaciones de búsqueda de la sesión.
5. La oferta de DHCP se envía al cliente. En esta oferta, la dirección IP ISE se especifica como el servidor DNS.
6. El usuario abre a un buscador Web y navega a google.com que accione una petición DNS al ISE.
7. El ISE marca si la blanco FQDN pertenece a los dominios externos. Si lo hace, después el ISE envía esta solicitud a un servidor DNS definida en las configuraciones del agrupamiento DHCP. Si no el ISE vuelve su propia dirección IP en la respuesta.
8. El buscador Web inicia una conexión TCP al ISE y las peticiones para google.com.
9. El ISE mira en esta etapa para arriba la sesión autenticada para la petición get entrante HTTP. Esto es importante para construir el correcto reorienta el URL.

   Nota: El ISE utiliza estas reglas para las operaciones de búsqueda de la sesión:
   1. IP de las operaciones de búsqueda en atar del DHCP
   2. Operaciones de búsqueda MAC por el IP
   3. Sesión de las operaciones de búsqueda por el MAC

1. El ISE responde con la página HTTP 302 movida a la reorientación URL.
2. Reorientan al usuario así al invitado porta y el flujo entero del invitado configurado en el ISE ocurre aquí.
3. Después de una autenticación acertada del invitado, el ISE se ejecuta con las directivas de la autorización una vez más para marcar si algunos nuevos atributos fueron agregados a la sesión y si el punto final durante el flujo del invitado requiere el cambio de la autorización (CoA). Una vez que se identifica la directiva siguiente de la autorización, el ISE prepara la petición CoA.
4. El intercambio de la petición/CoA ACK CoA ocurre entre el ISE y el NAD. Un CoA de la restauración de la despedida o Admin del puerto es una necesidad pues éste acciona la

obtención de una nueva dirección IP en el VLA N final. El NAD necesita soportar el radio o el CoA SNMP para que este paso trabaje.

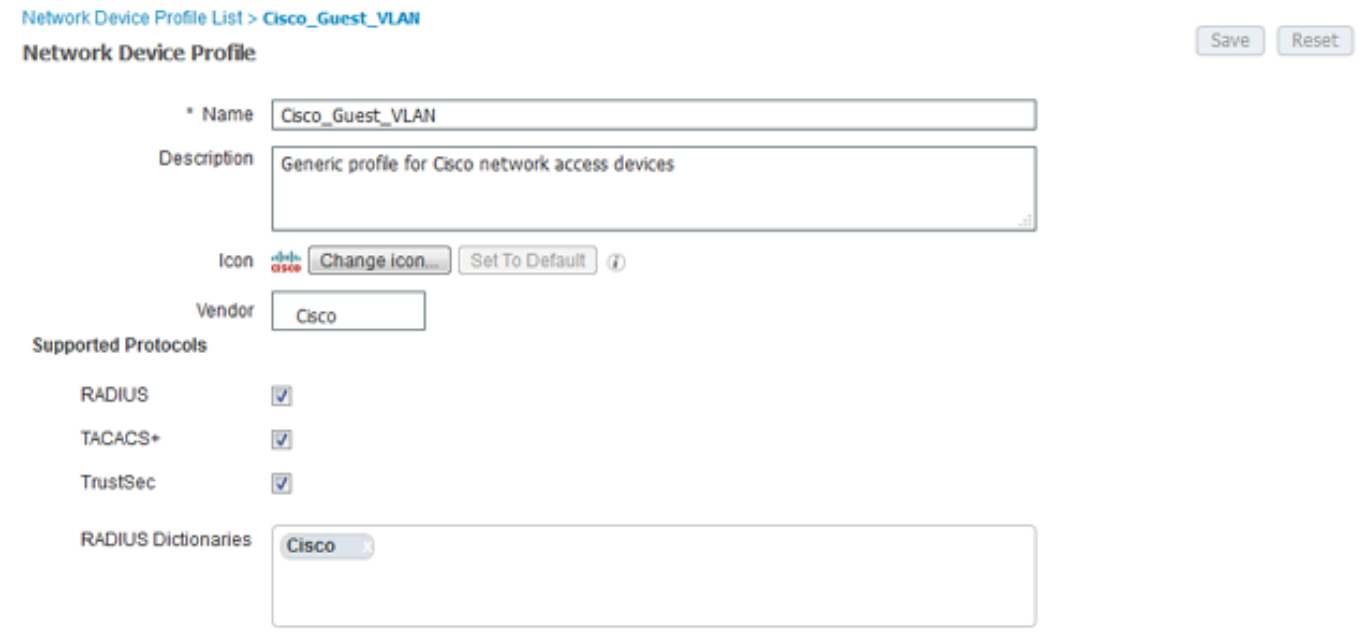
5. La parada de la Estadística-petición para la sesión disconnected se envía al ISE. El ISE reconoce esta petición enviando una Estadística-respuesta.
6. El ISE comienza a un temporizador de costura de la sesión (20 segundos por abandono). Durante este tiempo todos los atributos de sesión (ex: GUEST_TYPE, el flujo más case=Guest del uso) son guardados por el ISE. En caso de que un nuevo pedido del acceso la misma estación de llamada ID se reciba durante este tiempo, todos los atributos de sesión están limitados a la nueva sesión.
7. Un nuevo pedido de acceso MAB se envía para el dispositivo extremo después de que despedida del puerto CoA.
8. El ISE identifica la directiva de la autenticación/de la autorización para la nueva petición. El ISE utiliza en esta etapa los atributos de sesión y/o los atributos del punto final para la selección correcta de la directiva.
9. Un access-accept se envía con la información de VLAN final. Una lista de control de acceso transferible (DACL) se puede enviar en lugar de otro, para restringir el tráfico en el VLAN predeterminado también.
10. Conmute autoriza el puerto en el nuevo VLA N y aplica un DACL si está incluido.

Configurar

Configuración ISE

1. Cree el perfil del dispositivo de red

Para este ejemplo en particular, un switch Cisco utilizado como NAD. Por lo tanto, el perfil existente del dispositivo de red de Cisco duplicado y modificado como sea necesario. Navegue a la administración > a los recursos de red > a los perfiles del dispositivo de red y agregue el nuevo perfil.



2. Cree el dispositivo de red

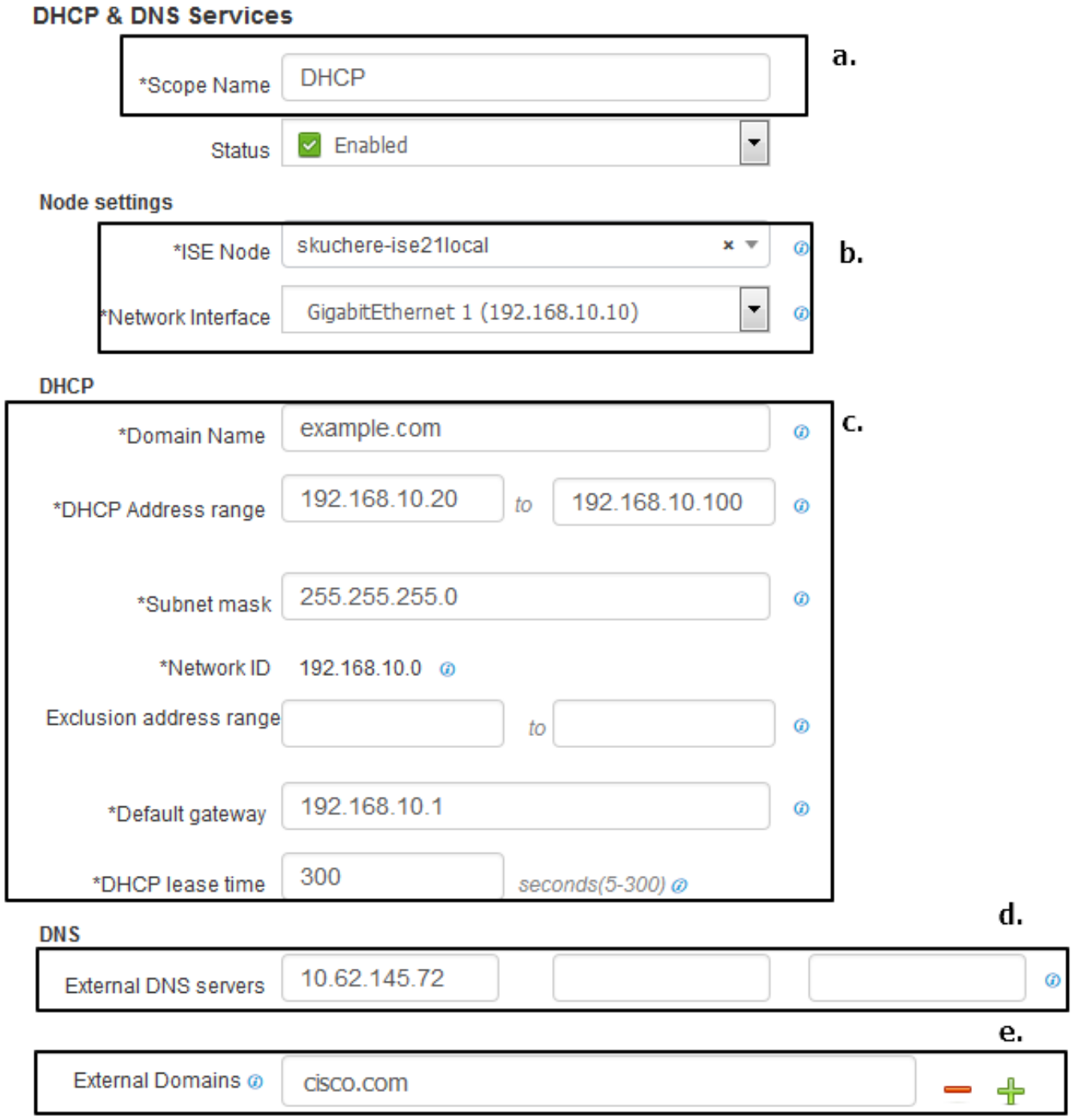
Navegue a la administración > a los recursos de red > a los dispositivos de red y agregue el nuevo dispositivo.

a. Observe la configuración para el perfil del dispositivo de red.

b. El resto de las configuraciones son estándar.

3. Servidor DHCP de la configuración

El pool del servidor DHCP está limitado a un nodo determinado ISE y a su interfaz. Navegue a la administración > al sistema > a las configuraciones > a los servicios del DHCP y DNS > Add



a. El nombre del alcance de DHCP necesita ser configurado.

b. Seleccione el nodo en el cual los servicios DNS y del DHCP que deben ejecutarse y la interfaz en ese nodo que debe ser utilizado.

c. Defina el alcance del IP Address del DHCP, el default gateway, los direccionamientos excluidos del alcance y el Tiempo de validez del DHCP.

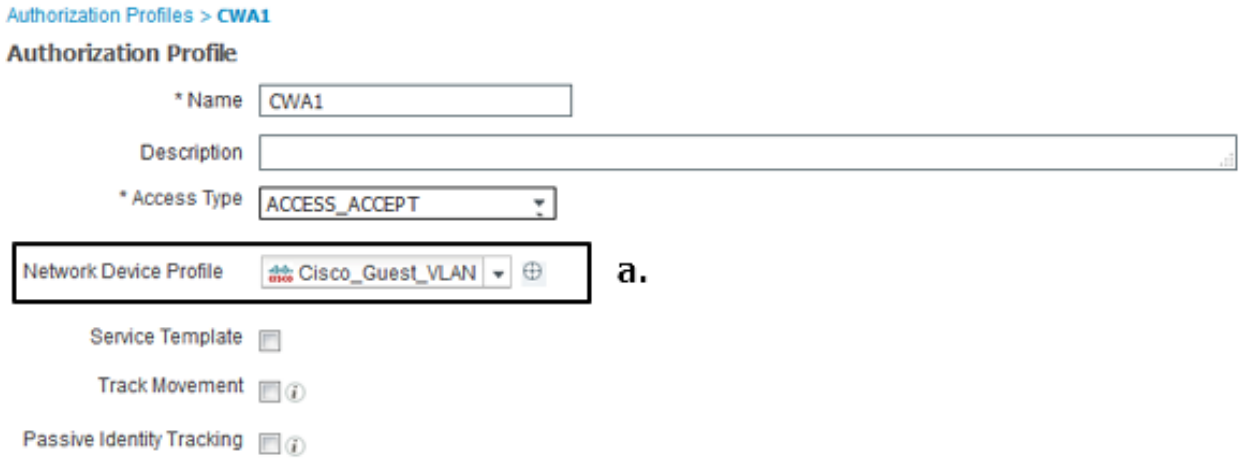
d. Opcionalmente, defina los IP Addresses externos del servidor DNS. Éstos se deben preguntar para los dominios externos.

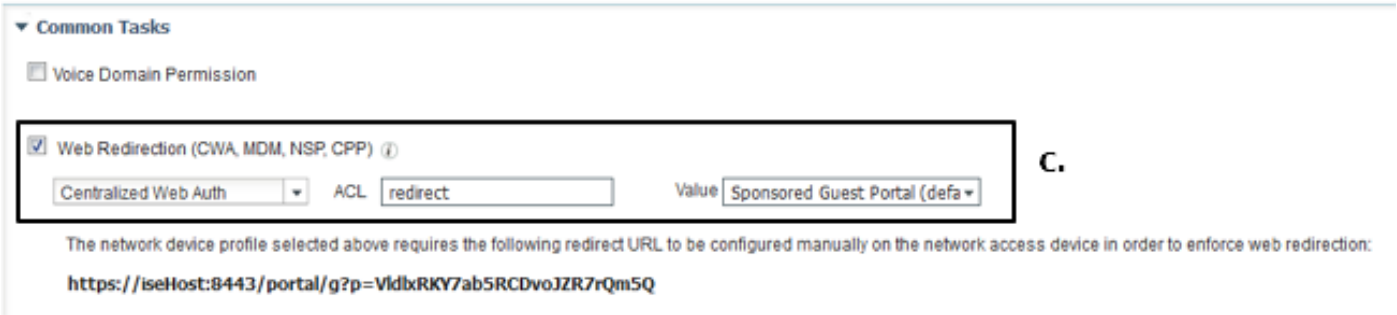
e. Opcionalmente, defina los nombres de los dominios externos. El ISE pregunta a los servidores DNS externos y vuelve la dirección IP real en vez sus la propio.

4. Perfil de la autorización de la configuración

Navegue a la directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización. Dos perfiles de la autorización son necesarios para el flujo completo del invitado:

- Reoriente el perfil de la autorización (CWA1)
- Permita el perfil de la autorización de acceso (PermitCWA2)

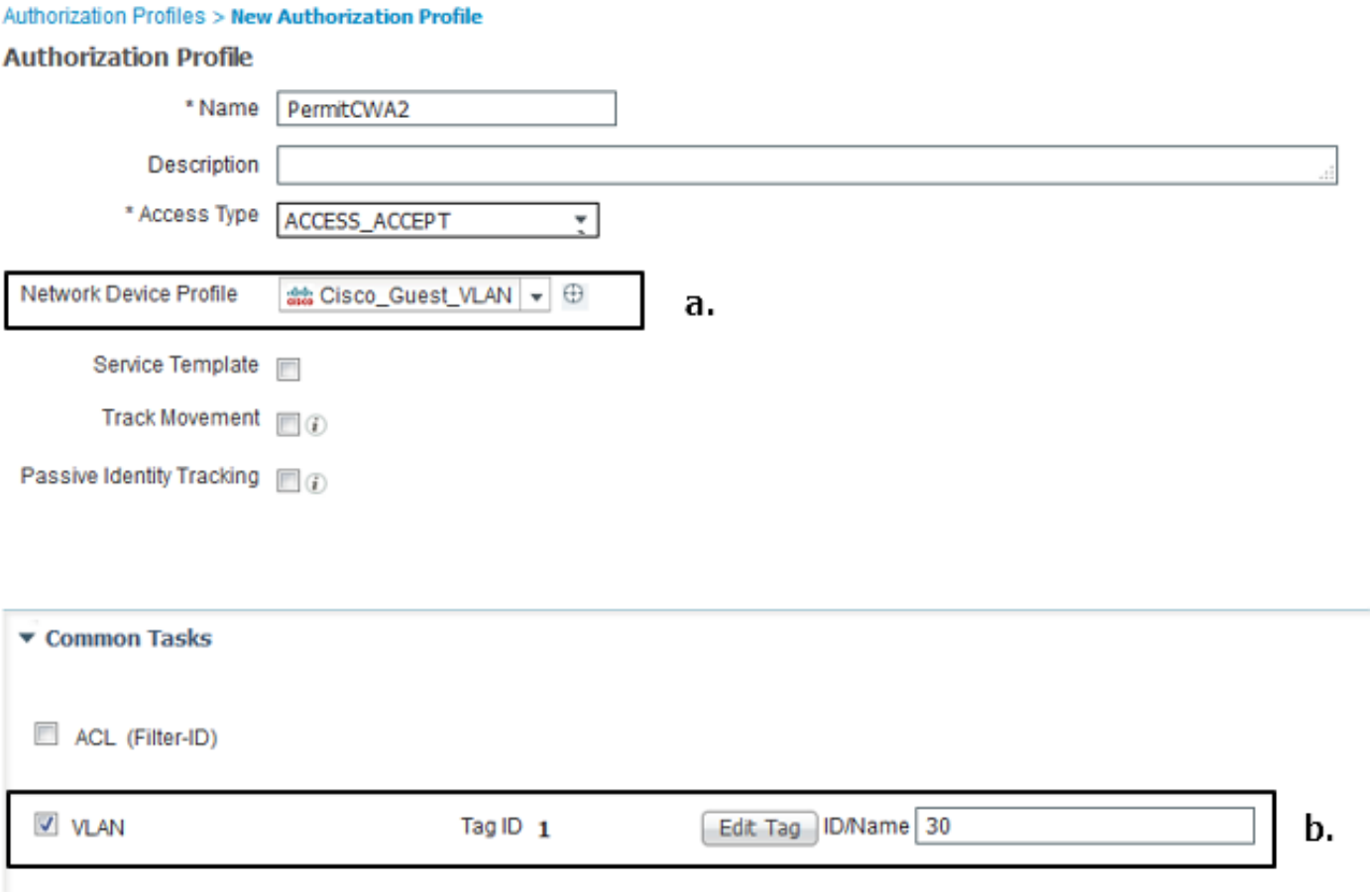




a. Perfil del dispositivo de red: Solamente los pedidos de autenticación que vienen de los NAD asignados a este perfil pueden dar lugar a este perfil de la autorización,

b. Configuraciones de VLAN: Los VLA N definidos aquí deben existir en el NAD. La interfaz ISE configurada para el DHCP debe o pertenecer a este VLA N o se debe configurar como ayuda IP en el gateway que mantiene este VLA N.

c. Reoriente las configuraciones: Para el ejemplo actual la autenticación Web central fue definida como reorienta tipo, y portal patrocinado del invitado definido como portal del invitado. La forma todavía pide el nombre de la reorientación ACL. Puesto que el perfil del dispositivo de red se ha configurado de nuevo para el URL estático reoriente, este nombre ACL nunca será enviado al NAD.

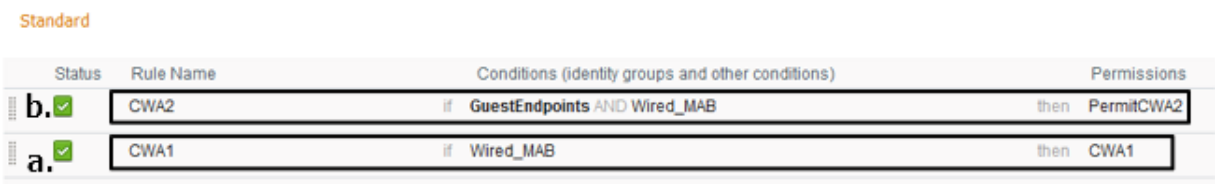


a. Perfil del dispositivo de red: Solamente los pedidos de autenticación que vienen de los NAD asignados a este perfil pueden dar lugar a este perfil de la autorización,

b. Configuraciones de VLAN: Después de asignar un puerto de cliente a este VLA N, el usuario debe conseguir una dirección IP de un servidor DHCP regular.

5. Configure las directivas de la autorización para el acceso de invitado

Navegue a la directiva > a la autorización. Configure dos directivas: uno para reorienta la acción y la otra para el acceso del usuario después de la autenticación en el portal del invitado.



a. La primera directiva de la autorización hace juego el MAB atado con alambre mientras que un método de autentificación y el perfil de la autorización de la reorientación se asigna como consecuencia.

b. La segunda directiva de la autorización se puede basar en los atributos de sesión (flujo del caso = del invitado del uso/tipo grupo externo del invitado AD si los Usuarios invitados autenticados usando el AD) o en los atributos del punto final (grupo de la identidad del punto final). El registro del dispositivo necesita ser habilitado en el portal del invitado para utilizar al grupo de la identidad del punto final.

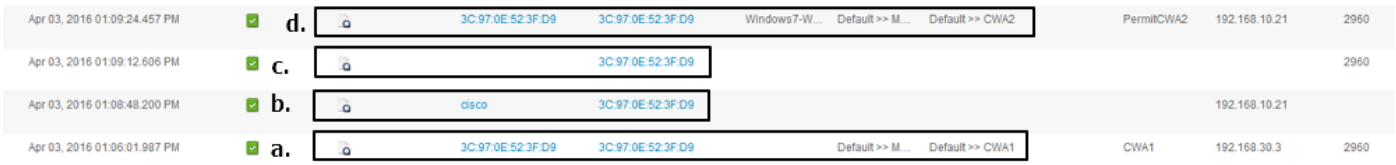
Configuración NAD

El switch Cisco se ha configurado para el MAB en la interfaz y tiene soporte COA.

> Nota: El Centro de Asistencia Técnica de Cisco (TAC) no ofrece ningún soporte para la configuración de los NAD de tercera persona.

Verificación

Un flujo acertado del invitado parece esto en las operaciones > el radio Livelog ISE:



a. Ésta es la primera autenticación MAB. El perfil de la autorización con reorienta se selecciona como consecuencia.

b. Ésta es la autenticación del invitado. Después de que esta acción ISE haga una nueva evaluación de la directiva para decidir a si el CoA es necesario.

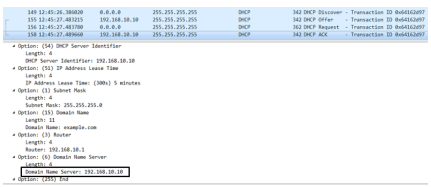
c. Un CoA fue completado con éxito.

d. Ésta es la segunda autenticación MAB. El perfil de la autorización para el acceso de invitado se selecciona como consecuencia.

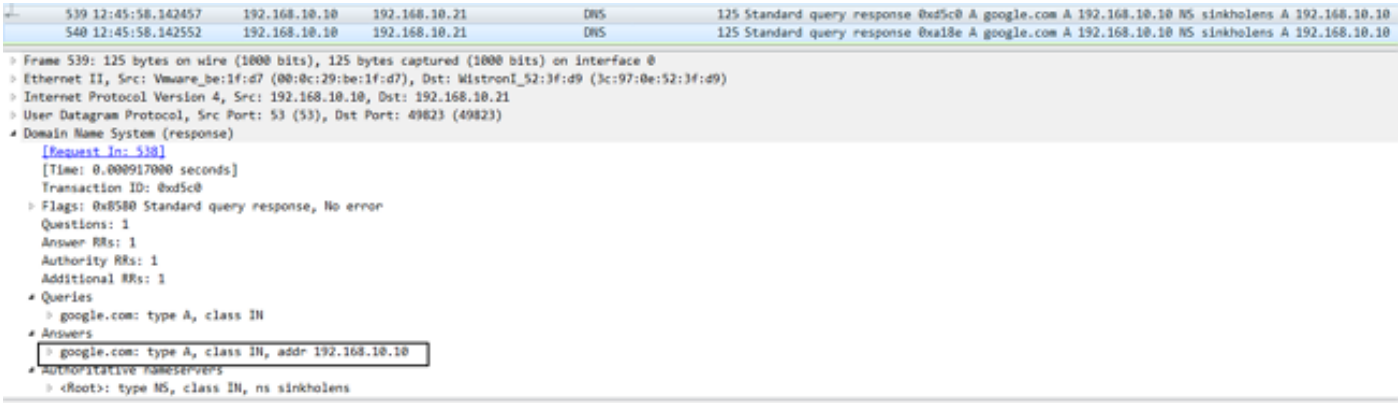
Troubleshooting

Marque si la dirección IP se asigna al cliente correctamente. Esto puede ser hecha recogiendo a una captura de paquetes en el cliente o el ISE.

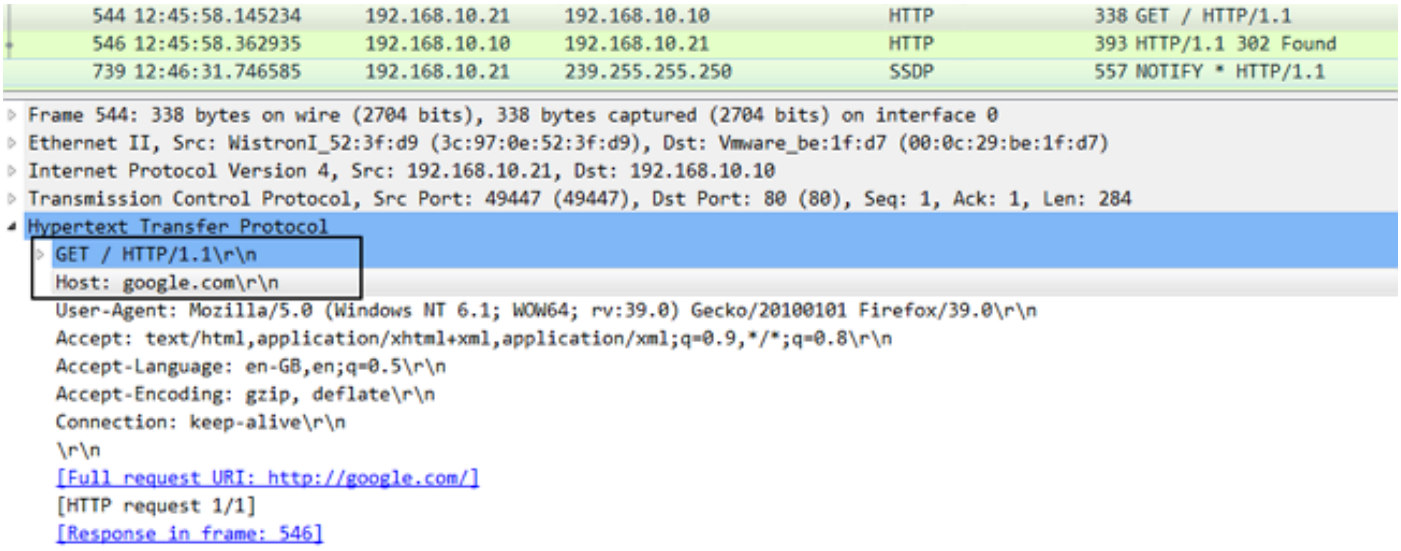
Esta captura del cliente muestra a apretón de manos acertado del DHCP con el IP DNS lo mismo que el ISE.



Marque si el ISE está actuando correctamente como dolina DNS. Una captura de paquetes puede ayudar a confirmar si la petición va al ISE y si el ISE responde a él con su propia dirección IP:



Marque si el HTTP reorienta los trabajos correctamente. Después de que consiga la dirección IP del recurso y establezca una conexión TCP al ISE, el cliente envía una petición get HTTP al ISE. Esto se puede confirmar en una captura de paquetes del lado del cliente:



Al mismo tiempo, el ISE determina si cualquier sesión existe para este cliente. Este proceso de las operaciones de búsqueda de la sesión en el ISE puede ser llegado registro de la prrt-Administración:

Después de las operaciones de búsqueda de la sesión, el ISE vuelve la reorientación URL al cliente en una respuesta HTTP 302: