Flujo del invitado de la configuración con ISE 2.0 y el WLC de Aruba

Contenido

Introducción

Los descrbies de este documento caminan para configurar los portales del invitado con el regulador del Wireless LAN de Aruba (WLC). De la versión 2.0 del Identity Services Engine (ISE) el soporte para los dispositivos de acceso a la red (NAD) del otro vendedor se introduce. El ISE soporta actualmente la integración con la Tecnología inalámbrica de Aruba para el invitado, postura y Bring Your Own Device (BYOD) fluye.

> **Note**: Cisco no es responsable de la configuración o del soporte para los dispositivos de los otros vendedores.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

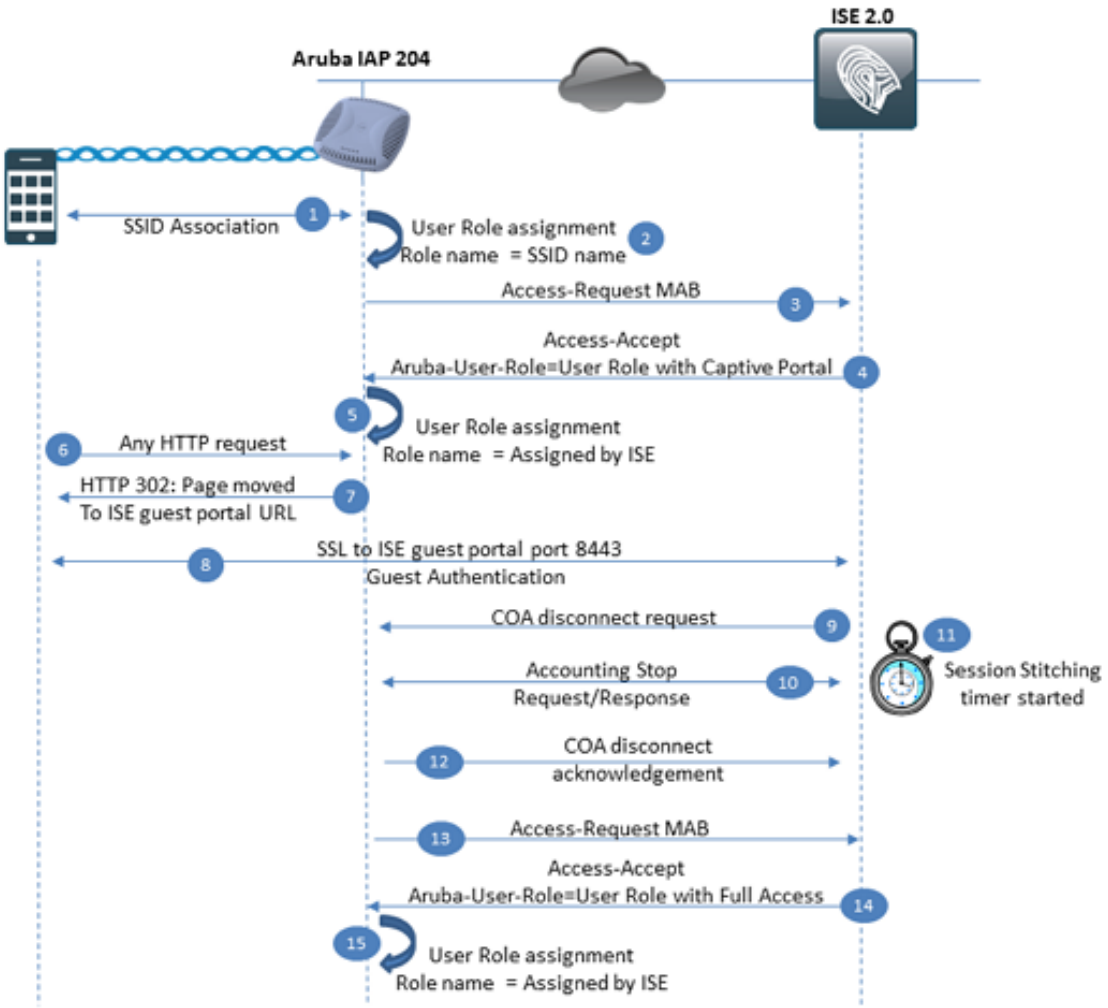
- Configuración de Aruba IAP
- Flujo del invitado en el ISE

Componentes Utilizados

- Software 6.4.2.3 de Aruba IAP 204
- Cisco Identity Services Engine 2.0

Antecedentes

Flujo del invitado



Paso 1. Asocian al usuario al conjunto de servicio Identifer (SSID). El SSID se puede configurar como abierto o con la autenticación de la clave previamente compartida.

Paso 2. Aruba aplica el rol del usuario a esta conexión. El primer rol del usuario es siempre SSID sí mismo. El rol del usuario contiene diversas configuraciones como el VLA N, la restricción del control de acceso, la configuración Cautivo-porta y más. En el rol del usuario del valor por defecto del ejemplo actual asignado al SSID tiene solamente Permiso-toda declaración.

Paso 3. El SSID se configura para proporcionar el MAC que filtra sobre el servidor RADIUS externo. El pedido de acceso MAB del radio (puente de la autenticación de MAC) se envía al ISE.

Paso 4. En el tiempo de la evaluación de la directiva el ISE selecciona el perfil de la autorización para el invitado. Este perfil de la autorización contiene el tipo de acceso igual a ACCESS_ACCEPT y el Aruba-Usuario-papel igual al rol del usuario del nombre configurado localmente en el WLC de Aruba (regulador del Wireless LAN). Este rol del usuario se configura para Cautivo-porta y el tráfico se reorienta hacia el ISE.

Rol del usuario de Aruba

El componente principal que es utilizado por el WLC de Aruba es rol del usuario. El rol del usuario define la restricción de acceso aplicable al usuario a la hora de la conexión. La restricción de acceso puede incluir: Cambio de dirección, lista de control de acceso, VLA N (red de área local virtual), limitación de ancho de banda y otras porta prisioneros. Cada SSID que existe en el WLC de Aruba tiene rol del usuario predeterminado donde está igual el rol del usuario al nombre SSID, todos los usuarios conectados con el SSID específico consigue inicialmente las restricciones del papel predeterminado. El rol del usuario se puede sobregrabar por el servidor de RADIUS, en este caso access-accept debe contener el Aruba-Usuario-papel específico del atributo del vendedor de Aruba. El valor de este atributo es utilizado por el WLC para encontrar el rol del usuario local.

Paso 5. Con los controles del WLC del Aruba-Usuario-papel del atributo localmente para los rol del usuario configurados y aplica requerido.

Paso 6. El usuario inicia el pedido de HTTP en el navegador.

Paso 7. Petición de las interceptaciones del WLC de Aruba debido al rol del usuario configurado para el portal prisionero. Como una respuesta a este WLC de la petición devuelve la página del código 302 HTTP movida con el portal del invitado ISE como nueva ubicación.

Paso 8. El usuario establece la conexión SSL al ISE en el puerto 8443, y proporciona el nombre de usuario/la contraseña en el portal del invitado.

Paso 9. El ISE envía el mensaje del pedido de desconexión COA al WLC de Aruba.

Paso 10. Después de que el WLC del mensaje de la desconexión COA caiga la conexión con el usuario e informe al ISE que la conexión se debe terminar usando el mensaje de la Estadística-petición del radio (parada). El ISE tiene que confirmar que este mensaje se ha recibido con las estadísticas.

Paso 11 El ISE comienza al temporizador de costura de la sesión. Este temporizador se utiliza para vincular la sesión antes y después del COA. Durante este tiempo el ISE recuerda todos los parámetros de sesión como el nombre de usuario, el etc. El segundo intento de autenticación debe ser hecho antes de que este temporizador expire para seleccionar la directiva correcta de la autorización para el cliente. En caso de que si expira el temporizador, el nuevo pedido de acceso sea interpretado como totalmente nueva sesión y directiva de la autorización con el invitado Redirect es aplicada otra vez.

Paso 12. El WLC de Aruba confirma el pedido de desconexión previamente recibido COA con el acuse de recibo de la desconexión COA.

Paso 13. El WLC de Aruba envía el nuevo pedido de acceso del radio MAB.

Paso 14. En el tiempo de la evaluación de la directiva el ISE selecciona el perfil de la autorización para el invitado después de la autenticación. Este perfil de la autorización contiene el tipo de

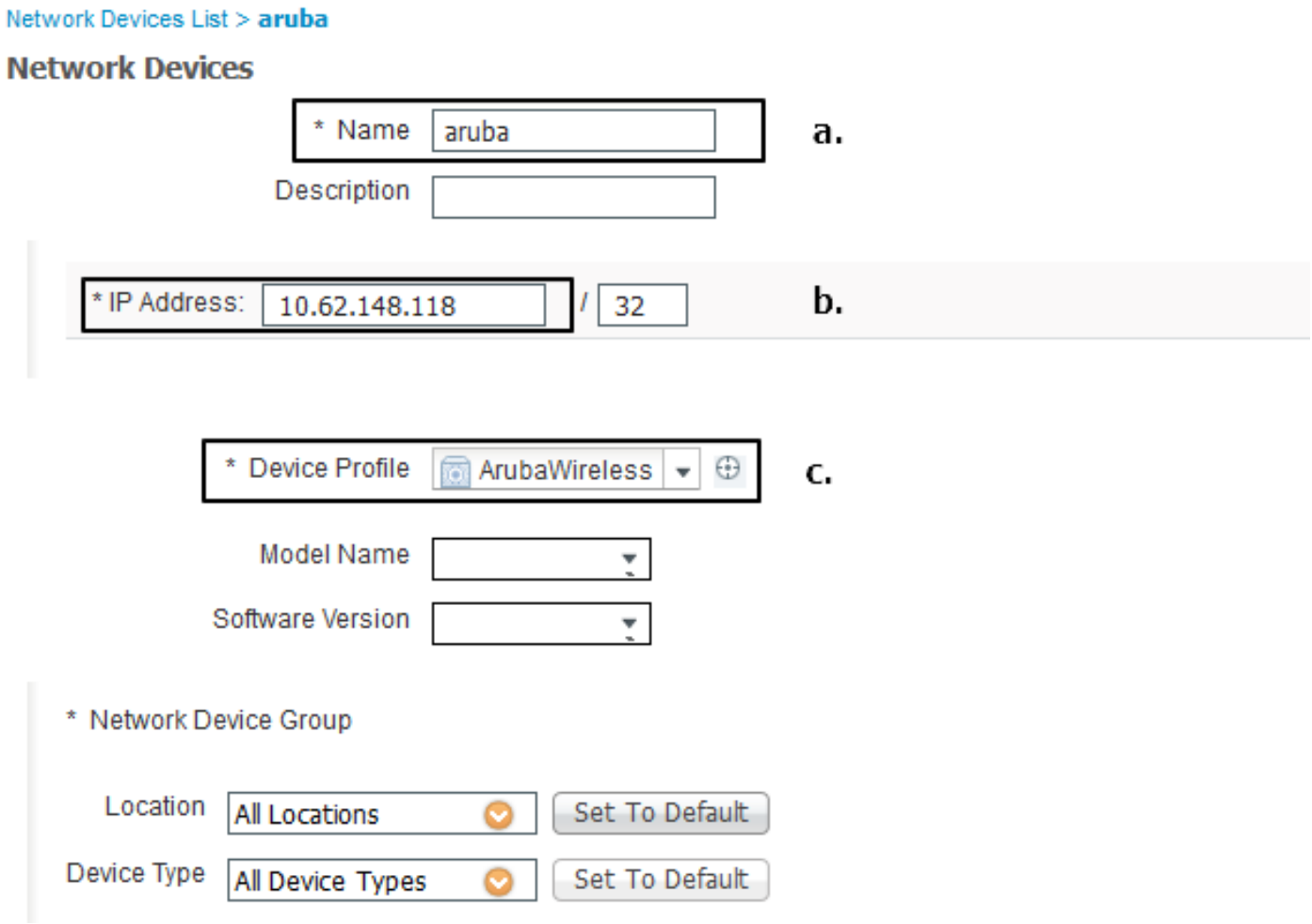
acceso igual a ACCESS_ACCEPT y el Aruba-Usuario-papel igual al rol del usuario del nombre configurado localmente en el WLC de Aruba. Este rol del usuario configurado para permitir todo el tráfico.

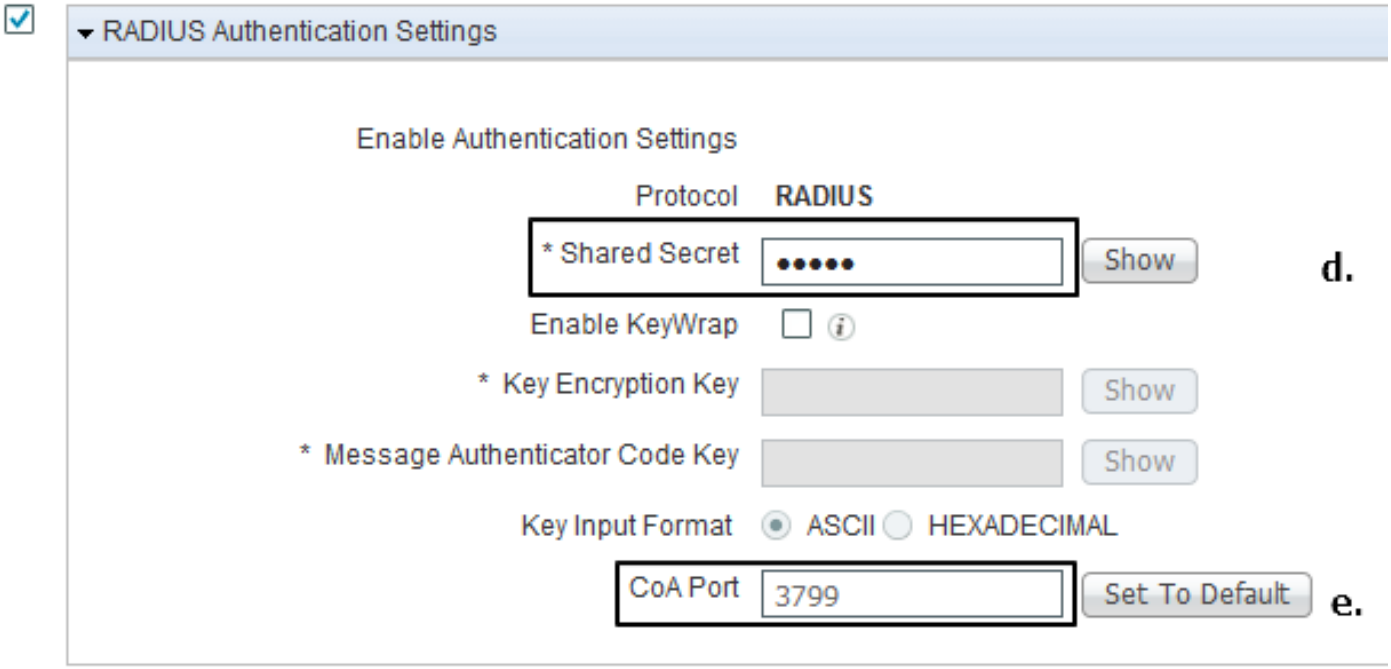
Paso 15. Con el Aruba-Usuario-papel del atributo el WLC marca los rol del usuario localmente configurados y aplica requerido.

Configurar

Paso 1. Agregue el WLC de Aruba como NAD en el ISE.

Navegue a la **administración > a los recursos de red > a los dispositivos de red** y el tecleo **agrega**

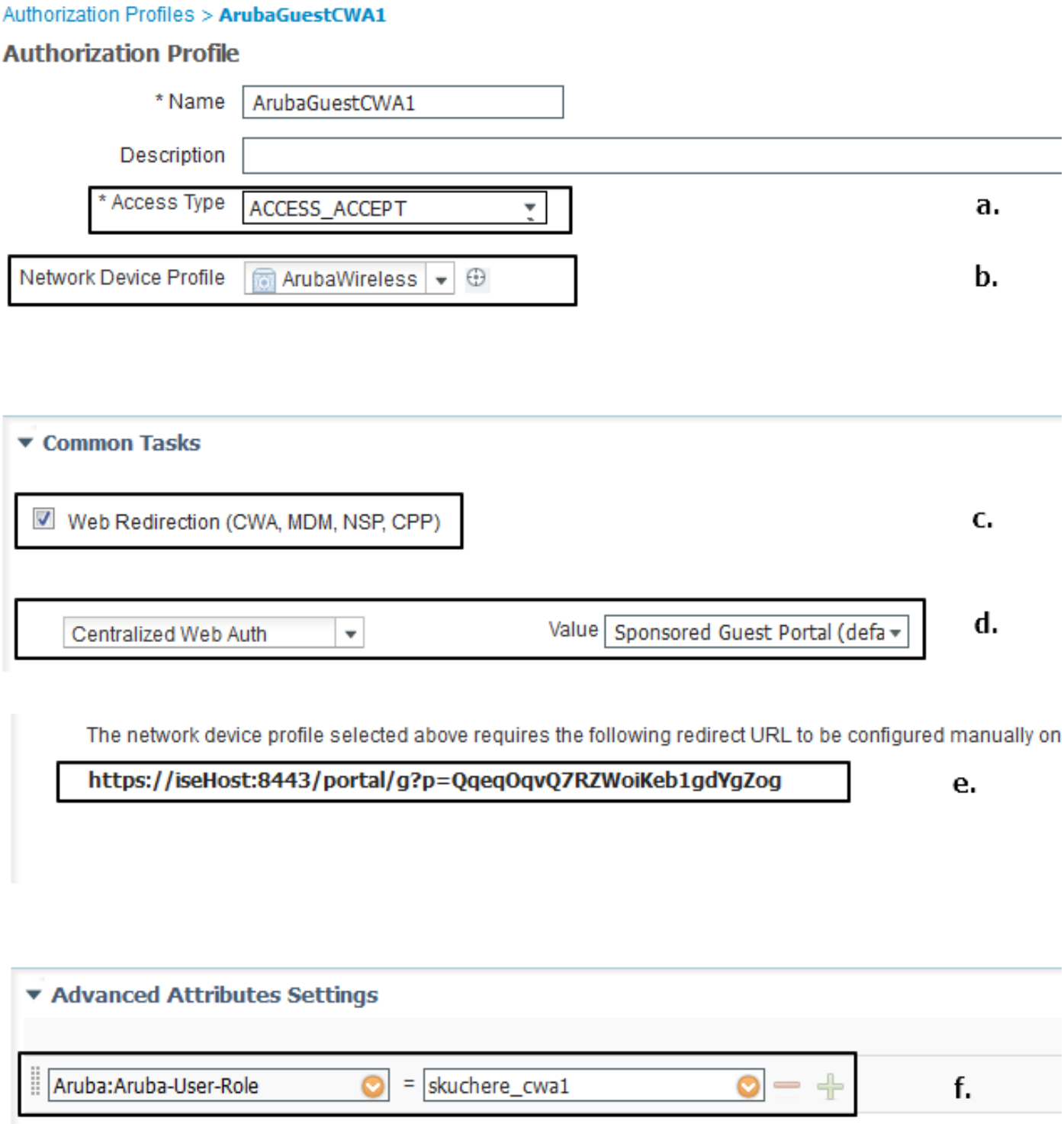




1. Proporcione el nombre de dispositivo de acceso a la red (NAD).
2. Especifique la dirección IP NAD.
3. Elija el perfil del dispositivo de red. Para el WLC de Aruba usted puede utilizar el perfil incorporado ArubaWireless.
4. Proporcione la clave previamente compartida.
5. Defina el puerto COA, el puerto 3799 del uso UDP del ejemplo actual de la forma del dispositivo para el COA.

Paso 2. Perfiles de la autorización de la configuración.

Navegue a la **directiva > a los elementos de la directiva > a los resultados > a la autorización > al perfil** y al haga click en Add de la **autorización** Primero usted tiene que crear el perfil de la autorización para la autenticación Web central (CWA) reorienta, tal y como se muestra en de la imagen.

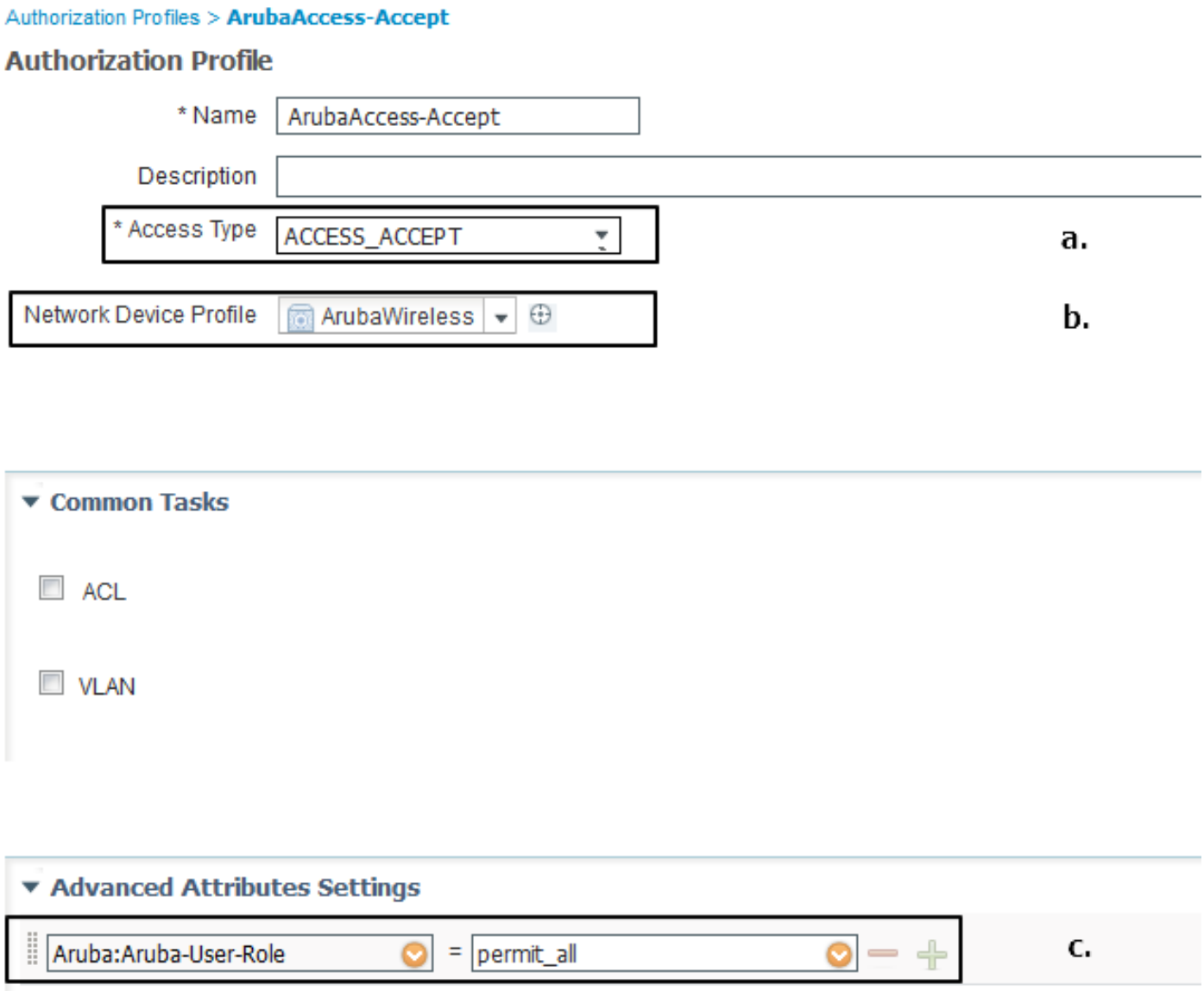


Note: Por abandono todos los perfiles de la autorización tienen el tipo de dispositivo de red igual a Cisco. Si el NAD sí mismo se configura como ArubaWireless y perfil de la autorización se crea para el tipo de otro dispositivo, este perfil nunca se corresponde con para este dispositivo.

1. Defina el **tipo de acceso** como **access-accept**.
2. En el **perfil del** dispositivo de red seleccione **ArubaWireless**.
3. En la sección común de la tarea, habilite la opción del **cambio de dirección de la red**.
4. Pues un **auth centralizado** selecto de la **red del** tipo del cambio de dirección y selecciona el portal del invitado que usted quisiera utilizar para el cambio de dirección.
5. El URL que el ISE presenta se debe definir en el WLC de Aruba como portal prisionero externo URL.

6. En el **atributo avanzado las configuraciones** seccionan, definen del valor de atributo de Aruba el rol del usuario.

El segundo perfil de la autorización se debe crear para proporcionar el acceso para los Usuarios invitados después de la autenticación porta:



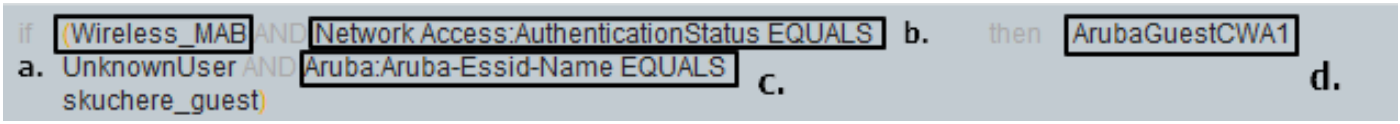
1. Defina el **tipo de acceso** como **access-accept**.
2. En el **perfil del dispositivo de red** seleccione **ArubaWireless**.
3. En la sección **avanzada de las configuraciones del atributo** defina del valor de atributo de Aruba el rol del usuario. Usted configurará después el rol del usuario local en el WLC de Aruba con el mismo nombre.

Paso 3. Directiva de la autorización de la configuración.

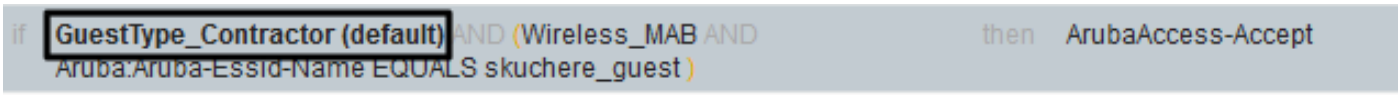
La primera directiva de la autorización es responsable del cambio de dirección del usuario al portal del invitado. En el caso más simple, usted puede utilizar construido en condiciones compuestas

- Wireless_MAB (A.) y
- Igual de AuthenticationStatus del acceso a la red al usuario desconocido (B.) y
- Aruba-Essid-nombre de Aruba igual a su nombre del invitado SSID (C.).

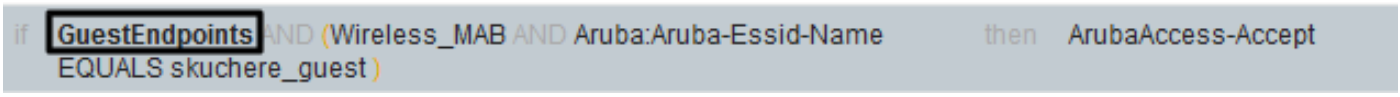
Para esta directiva, el perfil de la autorización de la configuración con reorienta al portal del invitado como consecuencia (la D.)



La segunda directiva de la autorización debe proporcionar el acceso para el Usuario invitado después de la autenticación vía el portal. Esta directiva puede confiar en los datos de la sesión (flujo del invitado del caso del grupo/uso de la Identificación del usuario y así sucesivamente). En este escenario el usuario debe volver a conectar antes de que expire el temporizador de costura de la sesión:



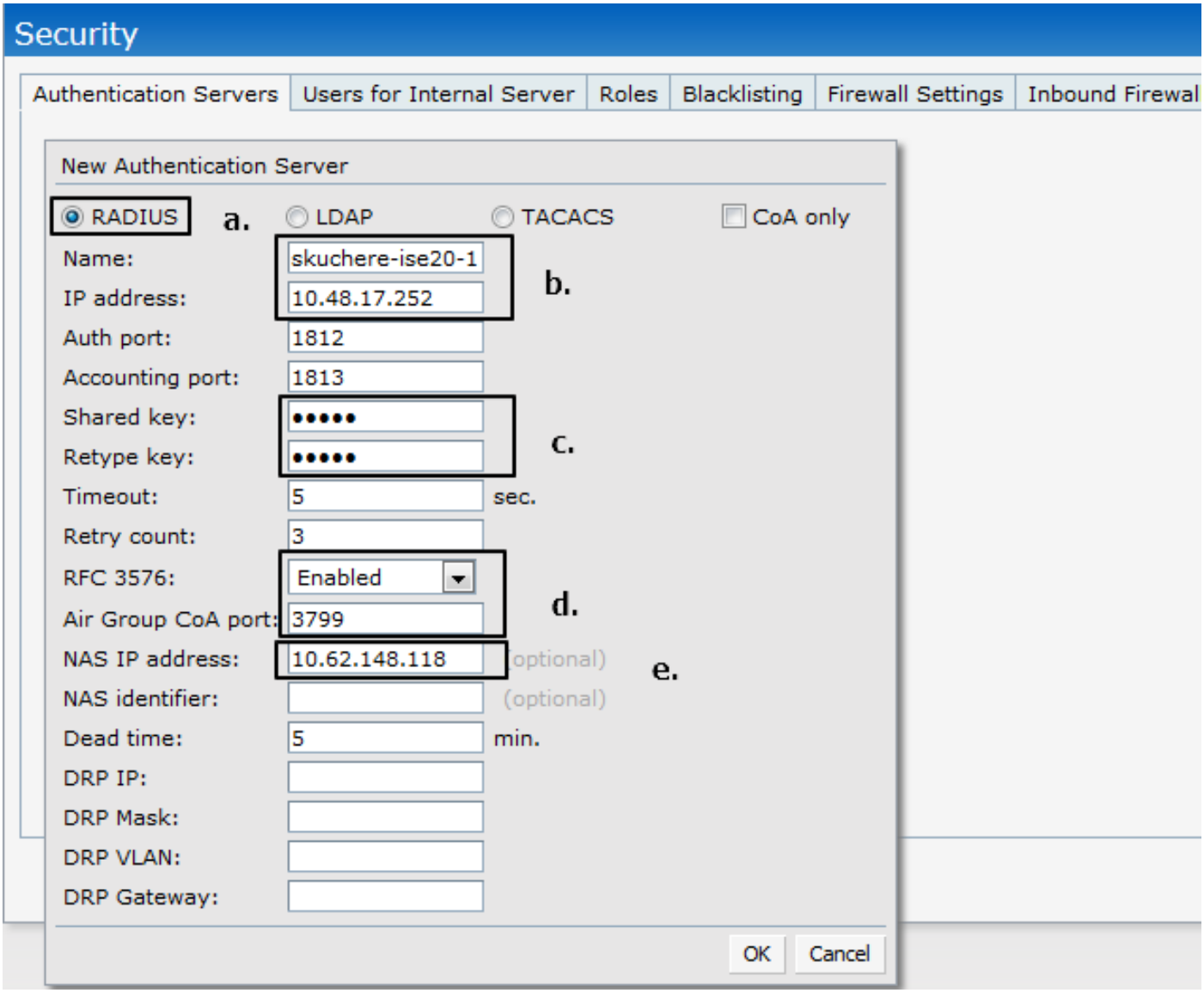
Para protegerse contra la expiración del temporizador de costura de la sesión usted puede confiar en los datos del punto final en vez de los datos de la sesión. Por abandono, el portal patrocinado del invitado en ISE 2.0 se configura para el registro del dispositivo automático del invitado (el dispositivo del invitado se pone automáticamente en el grupo de la identidad del punto final de Guest_Endpoints). Este grupo puede ser utilizado como condición:



Directiva de la autorización en la orden correcta:

Paso 4. Servidor de RADIUS de la configuración en Aruba.

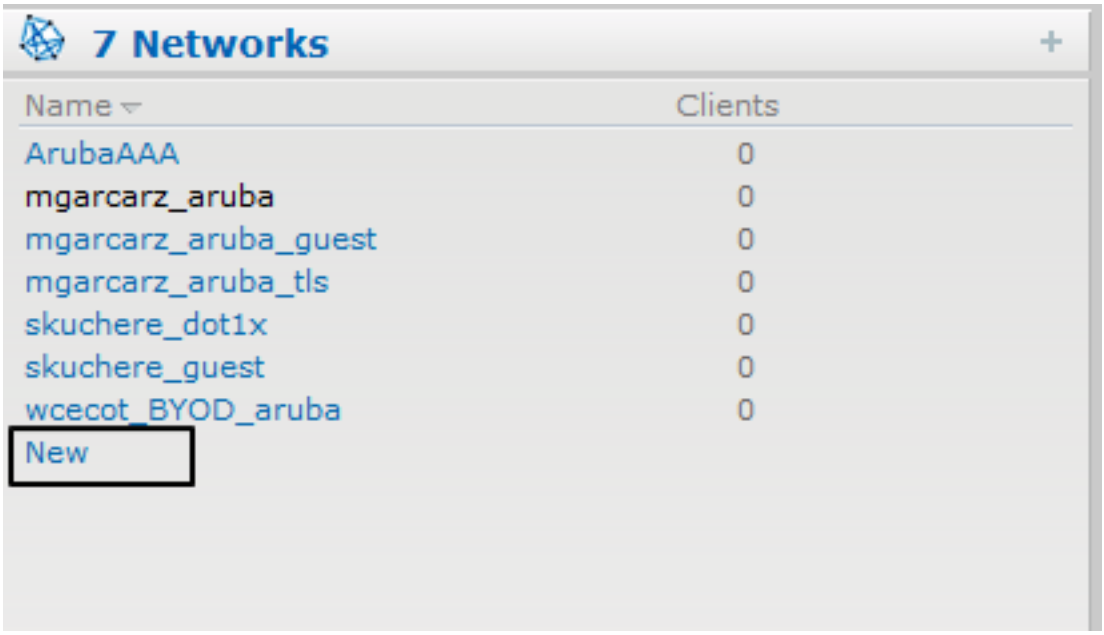
Navegue **Security > Authentication a los servidores** y haga clic **nuevo:**



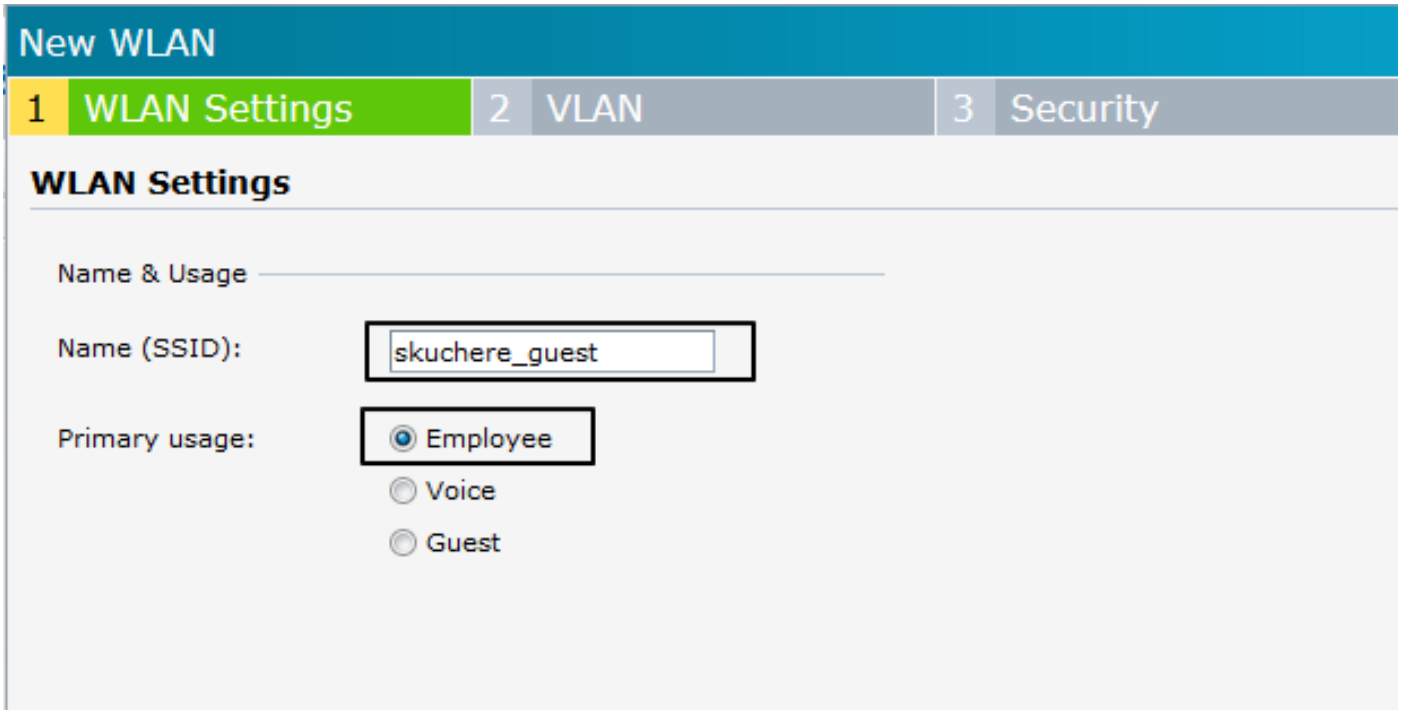
1. Elija el RADIUS como protocolo AAA.
2. Defina el nombre y la dirección IP de servidor de AAA.
3. Especifique la clave previamente compartida.
4. Habilite el soporte del RFC 3576 y defina el puerto COA.
5. Especifique el IP de la interfaz de administración del WLC de Aruba como dirección IP NAS.

Paso 5. Cree al invitado SSID en Aruba.

En la página del panel seleccione **nuevo** en el extremo de la lista de red. El Asistente para la creación SSID debe comenzar. Siga los pasos del Asisitente.

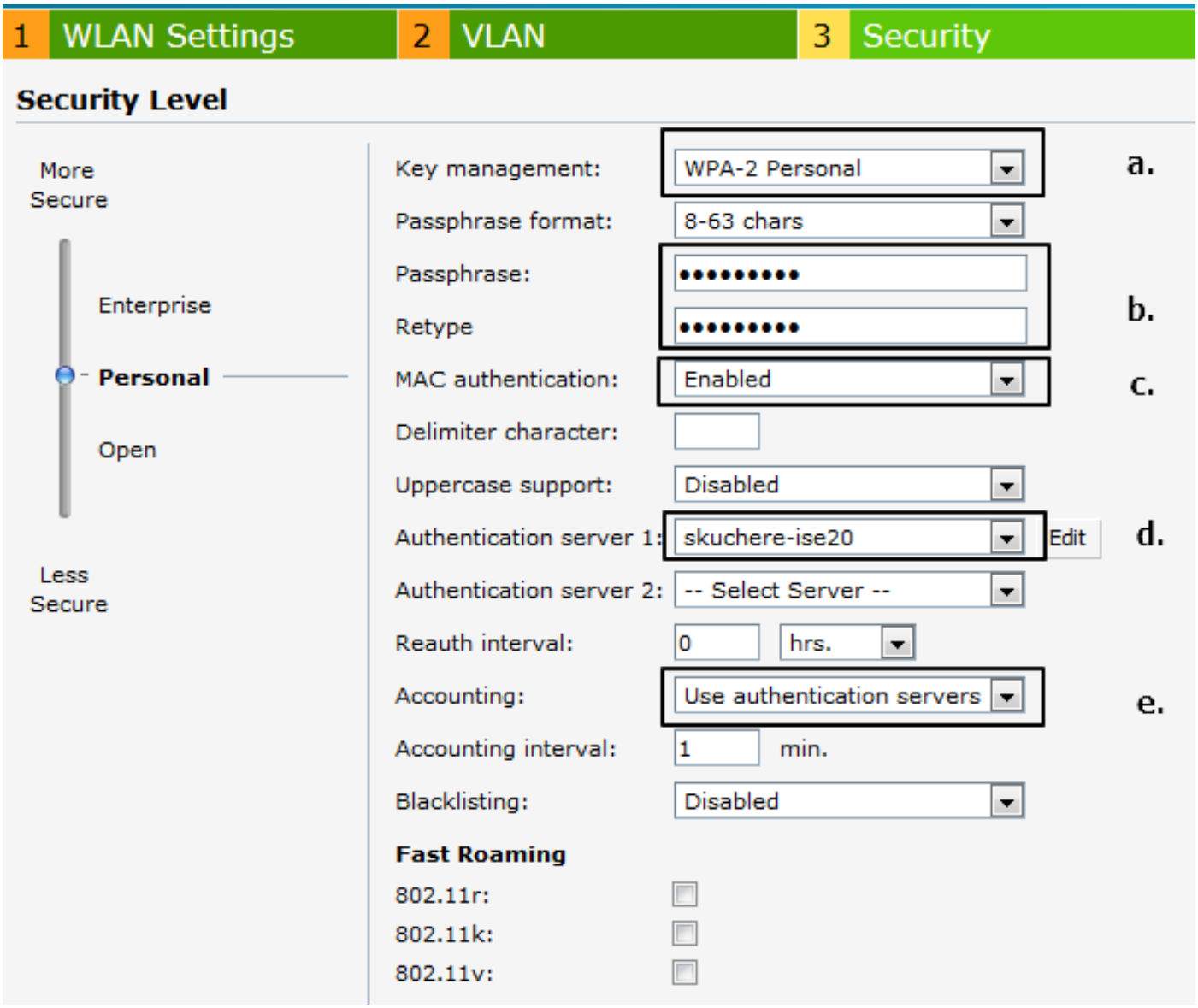


Paso 1. Defina el nombre SSID y el tipo selecto SSID. Aquí, utilizan al empleado del tipo SSID. Este tipo SSID tiene el papel predeterminado con el permiso todo y ninguna aplicación porta prisionera. También, usted puede elegir al invitado del tipo. En tal escenario usted debe definir las configuraciones porta prisioneras durante la configuración SSID.



Paso 2. Asignación del VLA N y de la dirección IP. Aquí, las configuraciones se dejan como valores por defecto, tal y como se muestra en de la imagen.

Paso 3. Ajustes de seguridad. Para el invitado SSID usted puede seleccionar se abre o personal. Personal requiere la clave del PRE-fragmento.



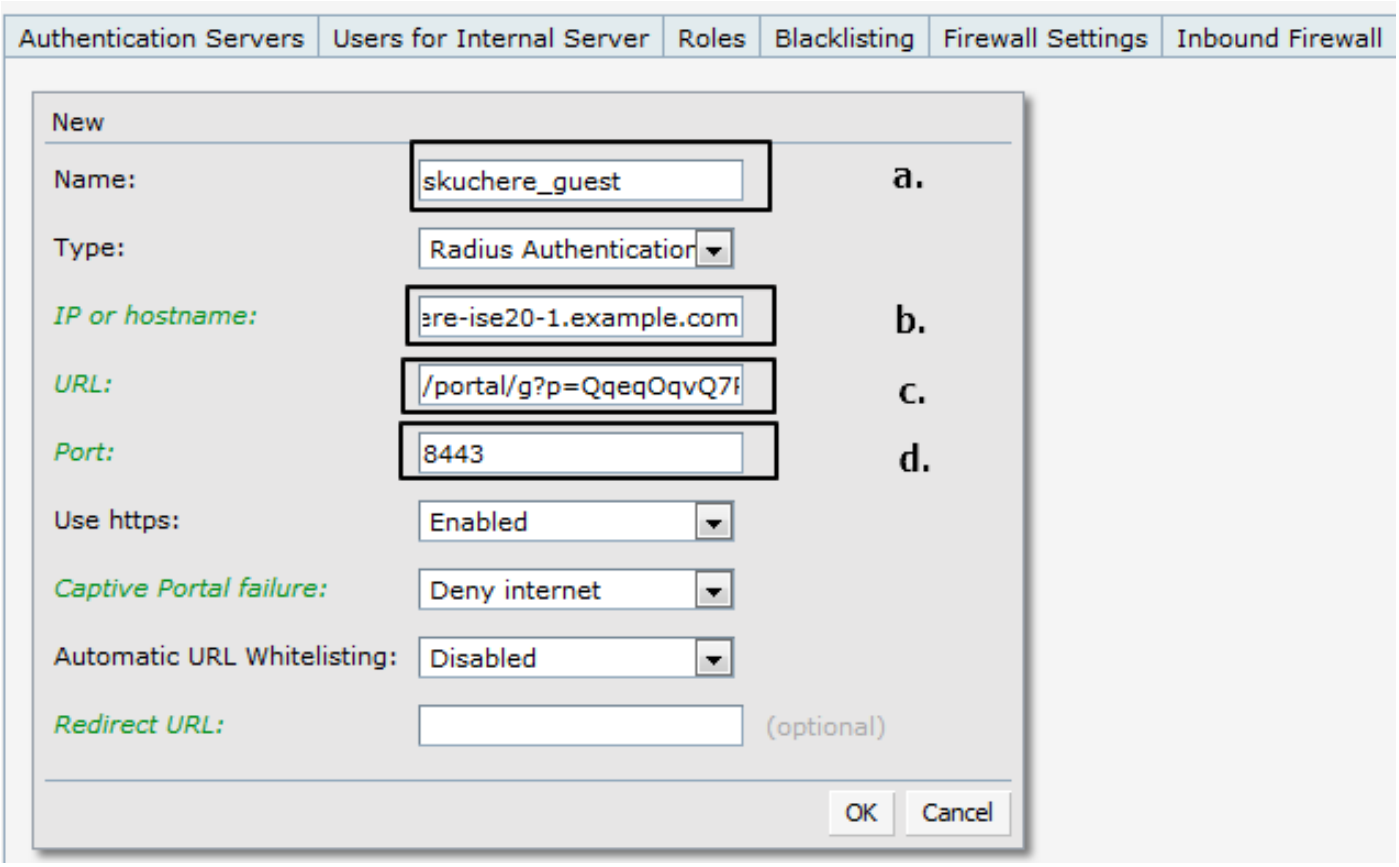
1. Elija el mecanismo de la administración de claves.
2. Defina la clave previamente compartida.
3. Para autenticar al usuario contra el ISE usando la necesidad de filtración MAB MAC de ser habilitado.
4. En la lista de servidores de autenticación elija a su servidor de AAA.

5. Para habilitar las estadísticas hacia el servidor de AAA previamente definido elija al servidor de autenticación del uso en la lista desplegable.

Note: Las estadísticas son cruciales con la tercero-parte NAD. Si el nodo del servicio de la directiva (PSN) no recibe la Estadística-parada para el usuario del NAD, la sesión puede conseguir pegada en el estado comenzado.

Paso 6. Portal prisionero de la configuración.

Navegue a la **Seguridad > los portales prisioneros externos** y cree el nuevo portal, tal y como se muestra en de la imagen:



Paso 1. Especifique el nombre porta prisionero.

Steo 2. define su ISE FQDN o dirección IP. Si usted utiliza la dirección IP, asegúrese de que este IP definido en el campo alternativo sujeto de Name(SAN) del certificado del portal del invitado.

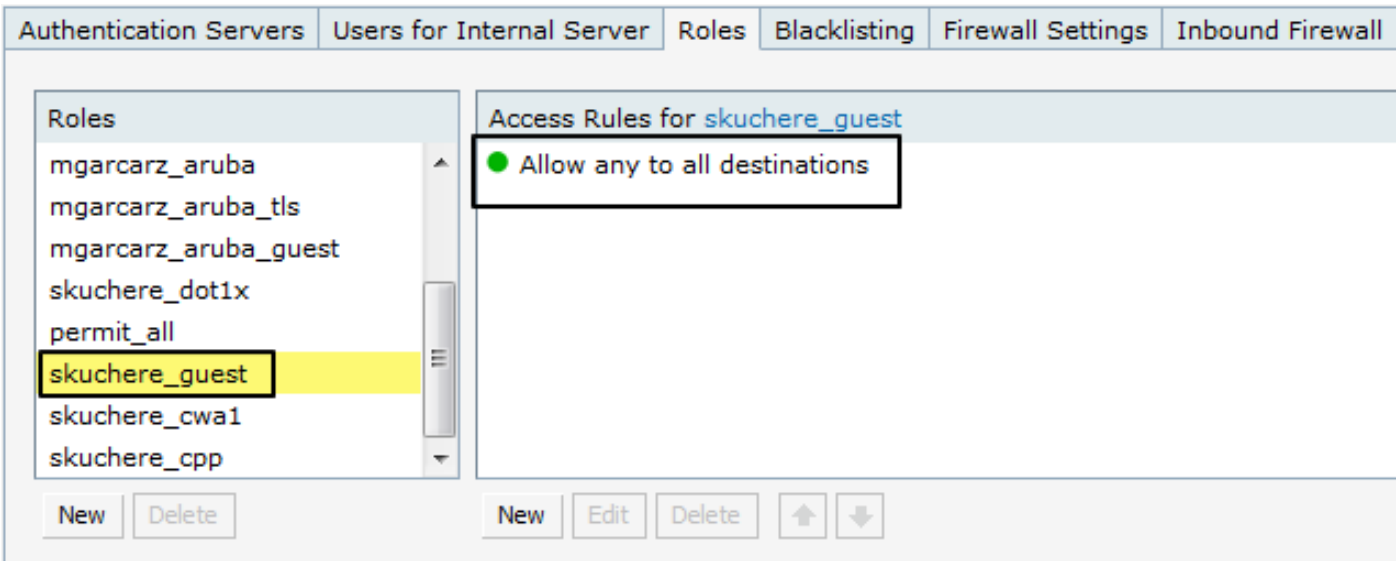
Note: Usted puede utilizar cualquier servidor PSN, pero el usuario debe ser reorientado siempre al servidor donde ocurrió el MAB. Usted tiene que definir generalmente el FQDN del servidor de RADIUS que se ha configurado en el SSID.

Paso 3. Provide reorienta del perfil de la autorización ISE. Usted debe poner aquí la pieza después del número del puerto,

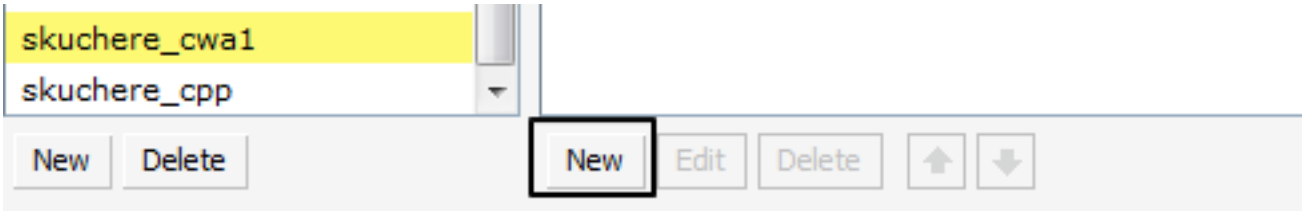
Paso 4. Defina el puerto porta del invitado ISE.

Paso 7. Rol del usuario de la configuración.

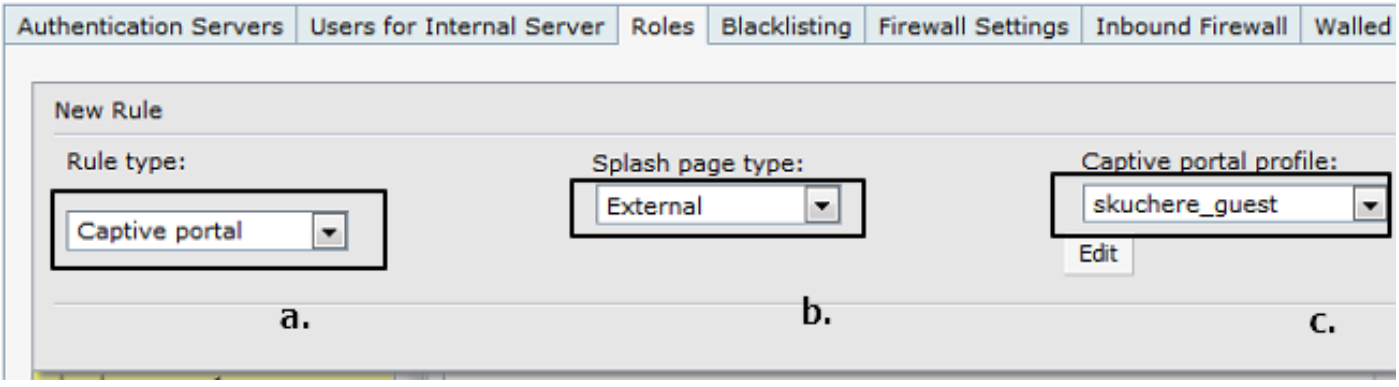
Navegue a la **Seguridad > a los papeles.** Asegúrese de que después de que se cree el SSID, el nuevo papel con el mismo nombre esté presente en la lista con el permiso de la regla de acceso a todos los destinos. Además, cree dos papeles: uno para CWA reorienta y en segundo lugar para el acceso del permiso después de la autenticación en los portales del invitado. Los nombres de estos papeles deben ser idénticos al rol del usuario de Aruba definido en los perfiles de la autorización ISE.



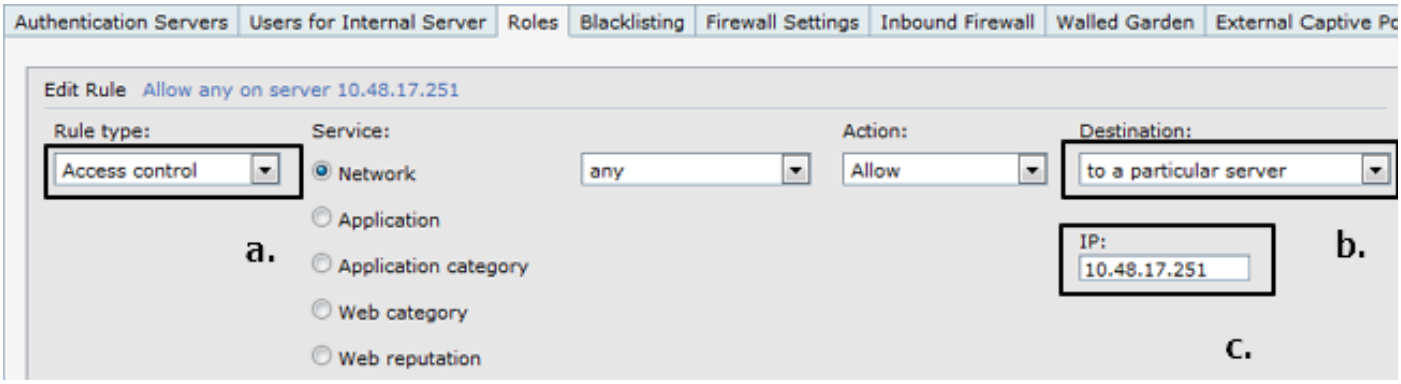
Tal y como se muestra en de la imagen, cree el papel de usuario nuevo de reorientan y agregan la restricción de seguridad.



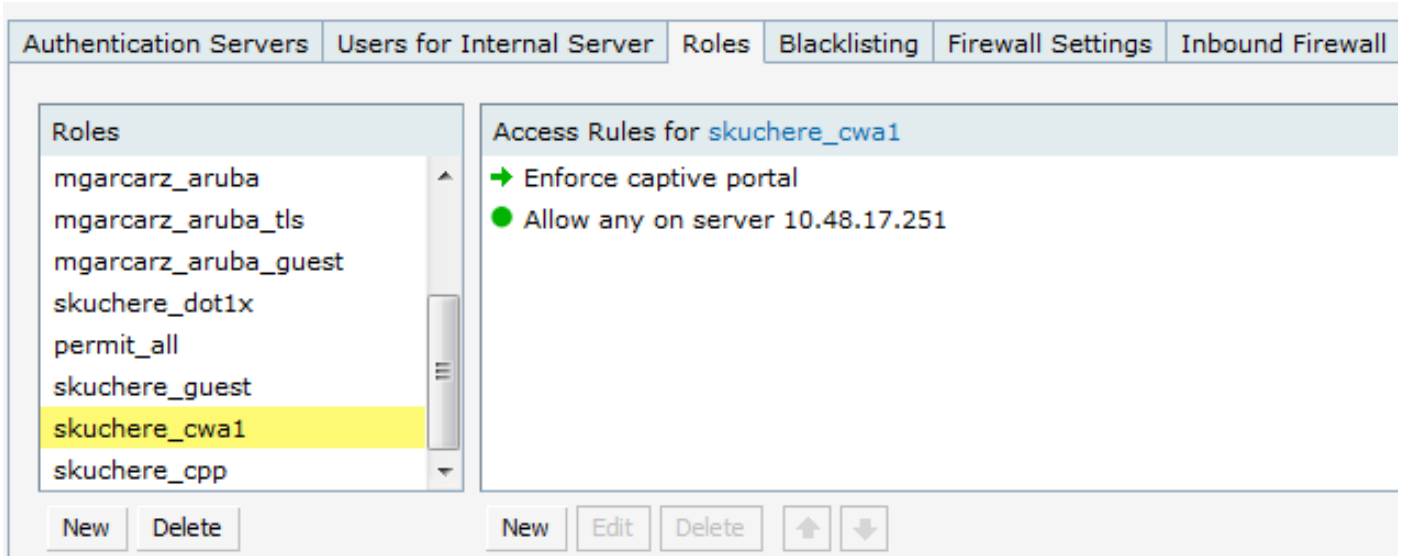
Para la primera restricción usted necesita definir:



Para la segunda restricción usted necesita definir:

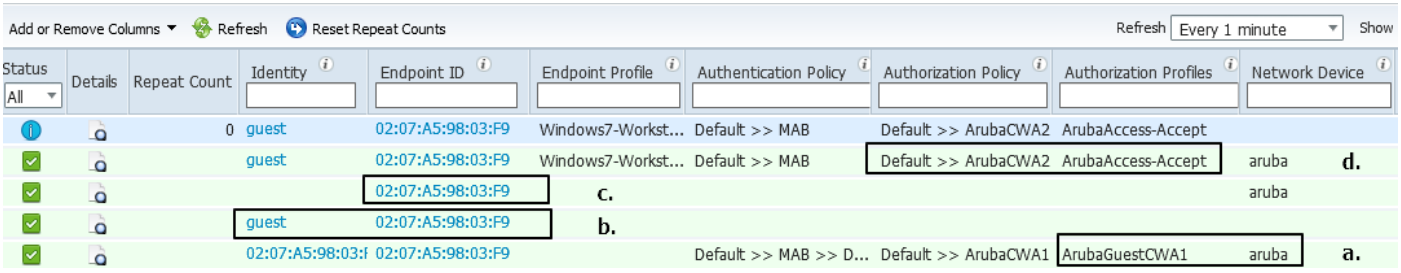


Tal y como se muestra en de la imagen, la regla predeterminada permite ningunos a todos los destinos puede ser borrada. Éste es un resultado sumario de la configuración del papel.



Verificación

Ejemplo del flujo del invitado en las **operaciones > el radio Livelog** ISE.



1. Los primeros MAB y como consecuencia, un perfil de la autorización con CWA reorientan y rol del usuario que tengan portal prisionero configurado en el lado de Aruba.
2. Autenticación del invitado.
3. Cambio acertado de la autorización (CoA).
4. Segundo MAB y como consecuencia un perfil de la autorización con el acceso y el rol del usuario del permiso que tiene permiso toda la regla en el lado de Aruba.

En el lado de Aruba usted puede utilizar a los **clientes de la demostración** ordena para asegurarse de que el usuario esté conectado, dirección IP se asigna y corrige el rol del usuario se asigna como resultado de la autenticación:

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

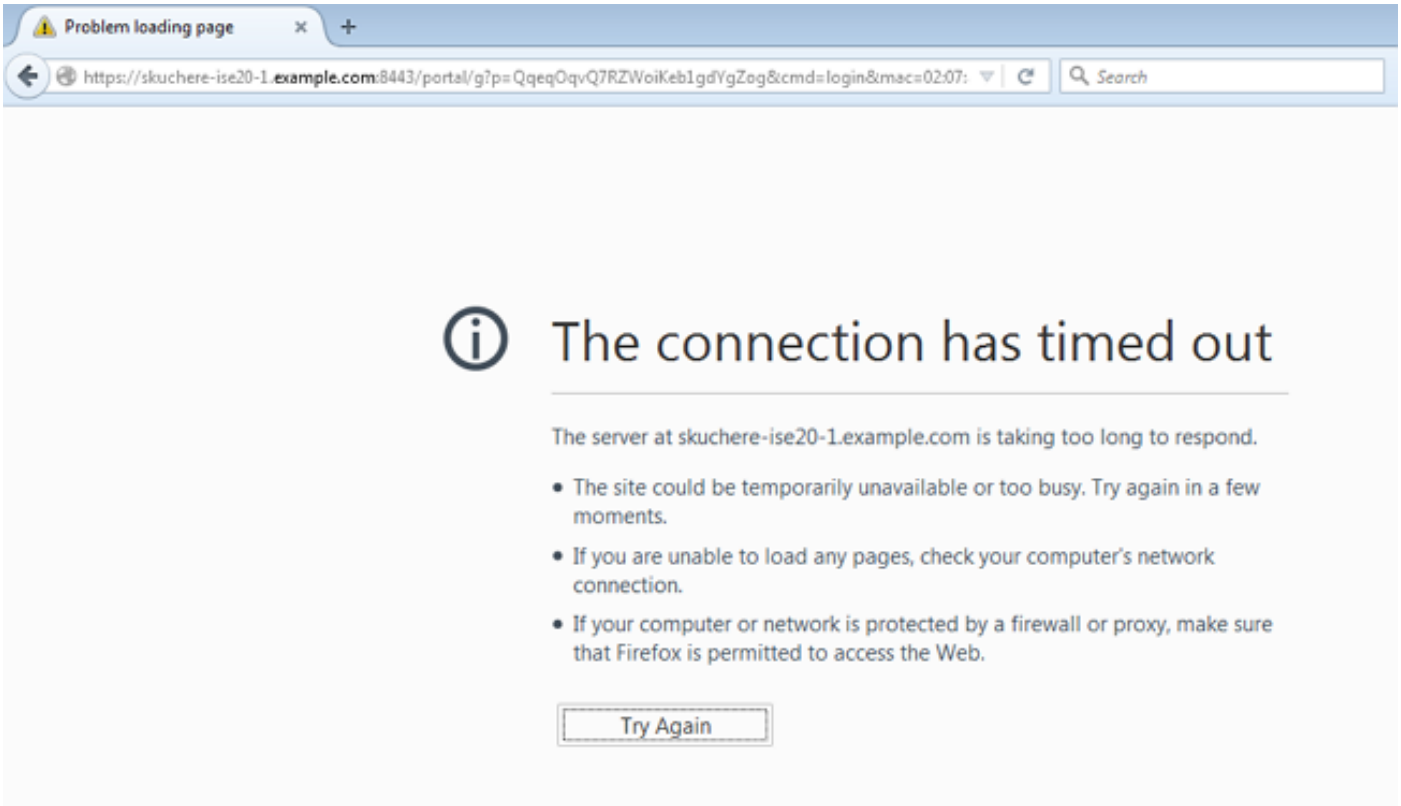
Troubleshooting

COA fallado

En las configuraciones ISE, asegúrese de que Aruba NAD esté configurado con el tipo de dispositivo de red correcto en el lado ISE y puerto COA está definido correctamente en las configuraciones NAD. En el lado de Aruba asegúrese de que el RFC 3576 esté habilitado en las configuraciones del servidor de autenticación y puerto COA está definido correctamente. De la perspectiva de red marque que el puerto 3799 UDP está permitido entre el ISE y el WLC de Aruba.

Reoriente el problema

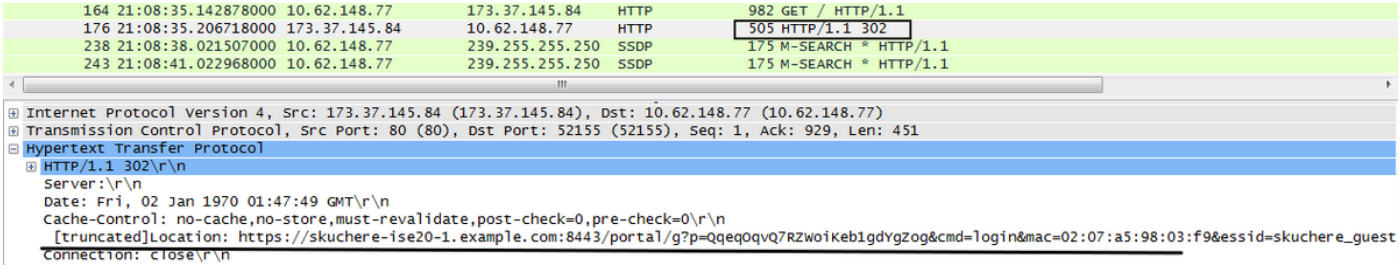
El usuario ve el URL ISE en el navegador pero la página ISE no se visualiza, tal y como se muestra en de la imagen:



En el lado del usuario asegúrese de que el ISE FQDN se pueda resolver con éxito para corregir el IP. En el control lateral de Aruba que el URL ISE está definido correctamente en las configuraciones y el tráfico porta prisioneros hacia el ISE permitido en el rol del usuario de las restricciones de acceso. También marque que el servidor de RADIUS en SSID y ISE PSN en las configuraciones porta prisioneras es el mismo dispositivo. De la perspectiva de red marque que el puerto TCP 8443 está permitido del segmento del usuario al ISE.

Ningún presente del cambio de dirección URL en el navegador del usuario

En el lado del usuario asegúrese de que como el resultado de cada página del código 302 de las devoluciones HTTP del WLC de Aruba del pedido de HTTP se movió con ISE URL.



El temporizador de costura de la sesión expiró

El síntoma típico de este problema es que reorientan al usuario por el por segunda vez al portal del invitado. En este caso en el radio Livelog ISE usted debe ver eso después de que el COA para el segundo perfil de la autorización de la autenticación con CWA se haya seleccionado otra vez. En el lado de Aruba, el papel de usuario real del control con la ayuda de los **clientes de la demostración** ordena.

Como una solución alternativa para este problema usted puede utilizar la directiva basada punto final de la autorización en el ISE para las conexiones después de la autenticación acertada del invitado.