NAC: Integración LDAP con el ejemplo de configuración ACS 5.x y posterior

Contenido

Introducción

Este documento proporciona una configuración de muestra para configurar el faro y el Cisco Secure Access Control System (ACS) 5.x y posterior para habilitar los dispositivos de Cisco configurados para puente de la autenticación de MAC (MAB) de manera eficaz y eficiente para autenticar los dispositivos con capacidad non-802.1X en la red autenticada.

Cisco ha implementado una característica llamada MAB en su Switches, así como el soporte indispensable en el ACS, para acomodar los puntos finales en las redes 802.1X-enabled que no pueden autenticar con el 802.1x. Estas funciones se aseguran de que los puntos finales que intentan conectar con la red 802.1X-enabled que no se equipan de las funciones del 802.1x, por ejemplo, no tienen un supplicant funcional del 802.1x, se pueden autenticar antes de la admisión, así como tienen política de uso de la red básica aplicada en su conexión.

El MAB habilita la red que se configurará para admitir los dispositivos identificados con el uso de su dirección MAC como los credenciales primarios cuando el dispositivo no puede participar en el protocolo del 802.1x. Para que el MAB sea desplegado y utilizado con eficacia, el entorno debe tener medios de identificar los dispositivos en el entorno que no son capaces de la autenticación del 802.1x, y de mantener una base de datos actualizada de estos dispositivos en un cierto plazo como se mueve, agrega y los cambios ocurren. Esta lista necesita ser poblada y ser mantenida en el servidor de autenticación (ACS) manualmente, o a través de algunos medios alternativos

para asegurarse de que los dispositivos que autentican en el MAC son completados y válidos en cualquier momento.

El Profiler del punto final del faro puede automatizar el proceso de la identificación de NON-autenticar los puntos finales, ésos sin los suplicantes del 802.1x, y el mantenimiento de la validez de estos puntos finales en las redes de la escala diversa en la funcionalidad de monitoreo del perfilado y del comportamiento del punto final. A través de una interfaz LDAP estándar, el sistema del faro puede servir como una base de datos externa o directorio de los puntos finales que se autenticarán con el MAB. Cuando una petición MAB se recibe de la infraestructura del borde, el ACS puede preguntar el sistema del faro para determinar independientemente de si un punto final dado se debe admitir a la red basada en la mayoría de la información actual sobre el punto final conocido por el faro. Esto previene la necesidad de la configuración manual.

Para una configuración similar usando las versiones anterior que ACS 5.x, refiera al NAC: Integración LDAP con el ejemplo de la configuración de ACS.

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 3750 Switch que funciona con el Software Release 12.2(25)SEE2 de Cisco IOS®
- Cisco Secure ACS 5.x y posterior

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El MAB es funciones esenciales para el soporte dinámico de los dispositivos tales como impresoras, Teléfonos IP, máquinas de fax y otros dispositivos con capacidad non-802.1X en el despliegue del entorno post-802.1X. Sin una capacidad MAB, los puertos de acceso a la red que proporcionan Conectividad a los puntos finales capaces non-802.1X deben ser aprovisionado estáticamente para no intentar la autenticación del 802.1x o con el uso de las otras funciones que proporcionan las opciones muy limitadas de la directiva. Por las razones obvias, esto no es intrínsecamente scalable en los entornos para empresas grandes. Con el MAB habilitado conjuntamente con el 802.1x en todos los puertos de acceso, los puntos finales capaces

conocidos non-802.1X se pueden mover dondequiera en el entorno y todavía conecte confiablemente (y con seguridad) con la red. Porque los dispositivos admitidos a la red se están autenticando, diversas directivas se pueden aplicar a diversos dispositivos.

Además, los puntos finales capaces non-802.1X que no se conocen en el entorno, tal como laptopes que pertenezcan a los visitantes o a los contratistas, pueden ser acceso restringido proporcionado a la red con el MAB si están deseados.

Mientras que el nombre sugiere, puente de la autenticación de MAC utiliza la dirección MAC del punto final como los credenciales primarios. Con el MAB habilitado en un puerto de acceso, si un punto final conecta y no puede responder al desafío de autenticación del 802.1x, el puerto invierte al modo MAB. El Switch que intenta el MAB de un punto final hace un pedido de RADIUS estándar al ACS con el MAC de la estación. Intenta conectar con la red y pide la autenticación del punto final del ACS antes de la admisión del punto final a la red.

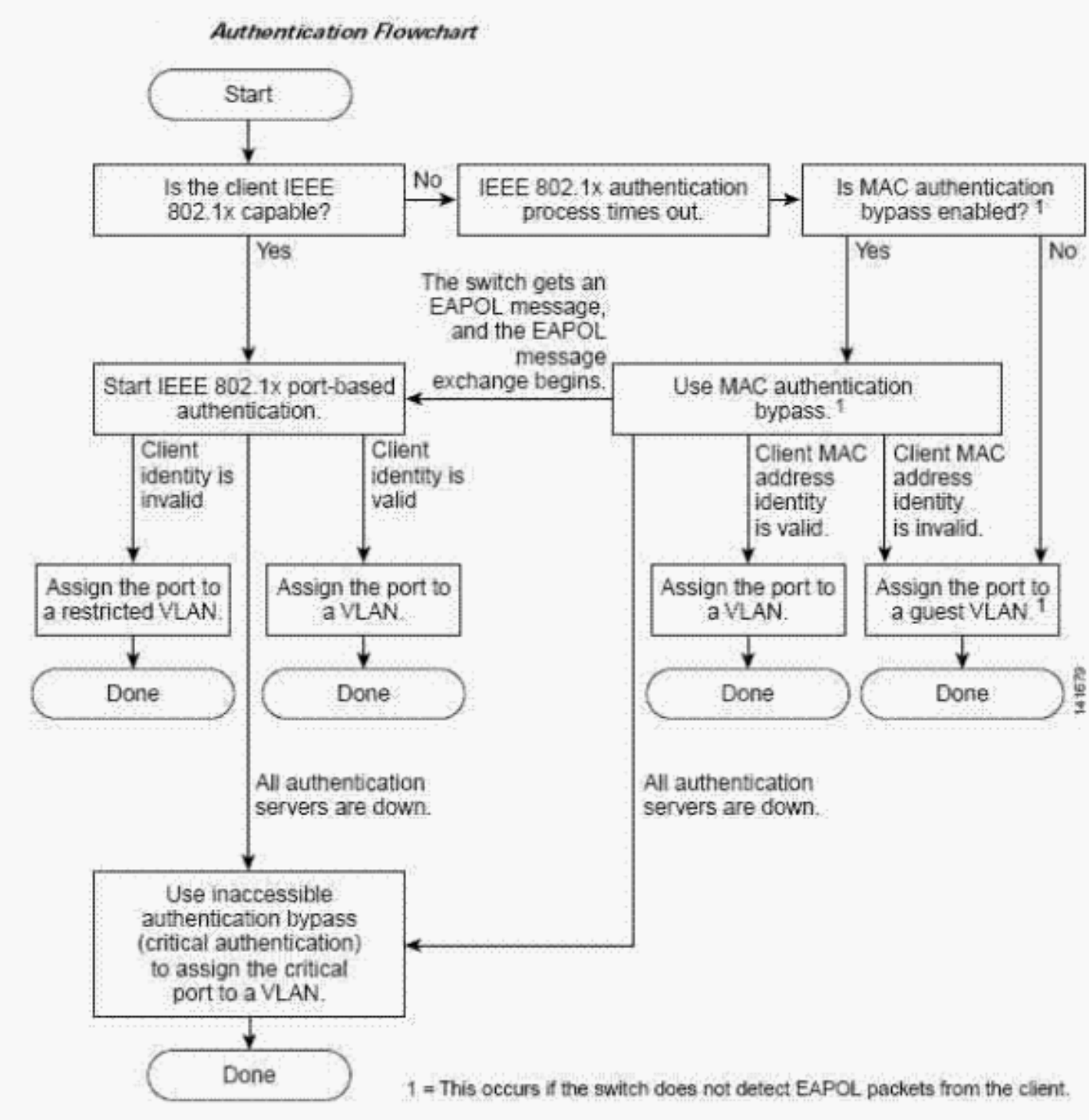
Configuración

Diagrama del organigrama

Este organigrama ilustra cómo el MAB se utiliza conjuntamente con la autenticación del 802.1x en la infraestructura del borde de Cisco mientras que los nuevos puntos finales intentan conectar con la red.

Este documento utiliza este flujo de trabajo del organigrama:

Figura 1: Flujo de la autenticación



El ACS se puede configurar para utilizar su propia base de datos interna o a un servidor LDAP externo para autenticar las peticiones del usuario de la dirección MAC. El sistema del Profiler del punto final del faro LDAP-se habilita completamente por abandono y se puede utilizar por el ACS para autenticar las peticiones del usuario de la dirección MAC con las funciones estándar LDAP. Porque el faro automatiza la detección así como el perfilado de todos los puntos finales en la red, el ACS puede preguntar el faro con el LDAP para determinar si el MAC se admite a la red, y que agrupen el punto final deben ser asociados. Esto automatiza y aumenta perceptiblemente la característica MAB, determinado en los entornos para empresas grandes.

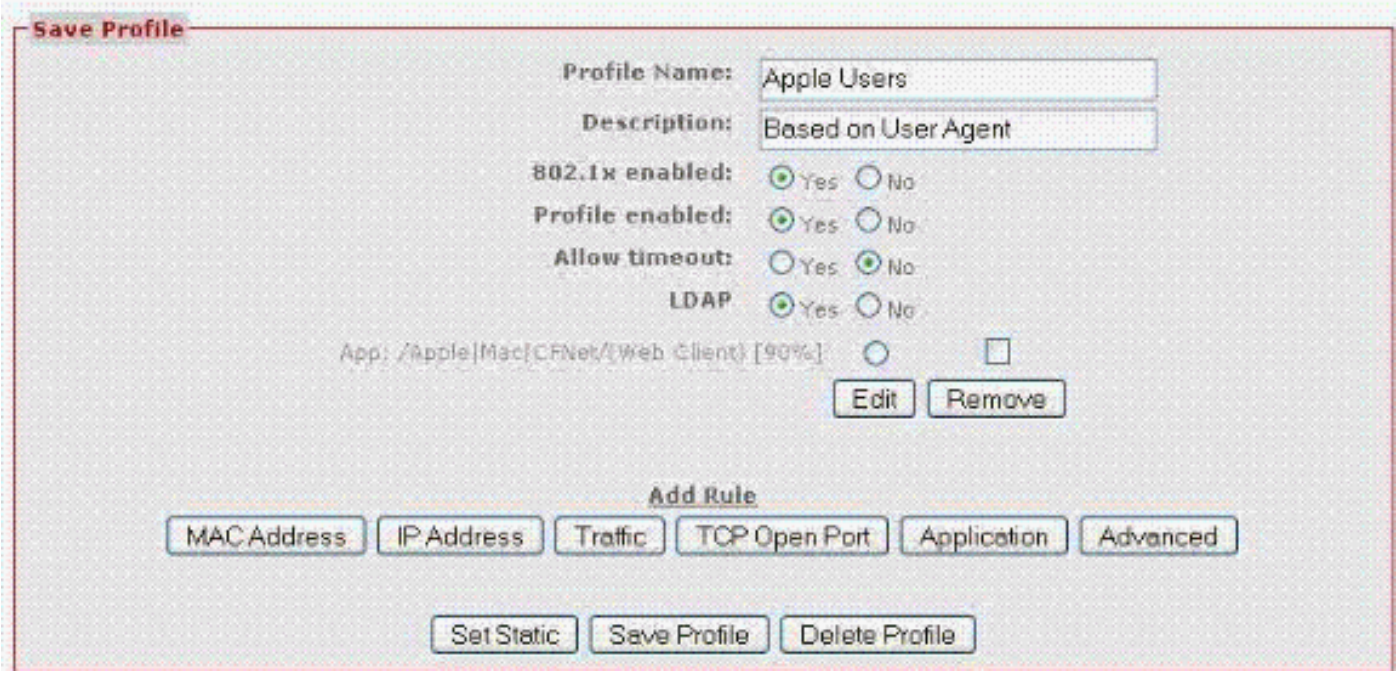
Con la funcionalidad de monitoreo del comportamiento proporcionada por el faro, los dispositivos que se observan para comportarse contrario con los perfiles habilitados para el MAB son transitioned fuera de 4 perfiles LDAP-habilitados y fallar posteriormente la tentativa regular siguiente de la reautentificación.

Configuración del sistema del Profiler del punto final del faro para el MAB

La configuración del sistema del faro para la integración con el ACS con el propósito del soporte MAB es directa pues las funciones LDAP se habilitan por abandono. La tarea de configuración primaria es identificar los perfiles que contienen los puntos finales que se desean para ser autenticados con el MAB en el entorno, y entonces habilitar esos perfiles para el LDAP. Típicamente, los perfiles del faro, que contienen los dispositivos poseyeron por la organización, deben ser acceso a la red proporcionado cuando estaban considerados en un puerto con todo se saben para no poder autenticar con el 802.1x. Típicamente, éstos son los perfiles que contienen las impresoras, los Teléfonos IP o UPSs manejable como ejemplos comunes.

Si las impresoras perfiladas por el faro fueron colocadas en un perfil nombrado *Printers*, y los Teléfonos IP en un perfil nombraron los *Teléfonos IP*, por ejemplo, después la necesidad de estos perfiles de ser habilitado para el LDAP tales que los puntos finales puestos en esos perfiles dan lugar a la autenticación satisfactoria como el teléfono del IP e impresoras sabidos en el entorno con el MAB. Si usted habilita un perfil para el LDAP, éste requiere elegir el botón de radio LDAP en la configuración del perfil del punto final, tal y como se muestra en de este ejemplo:

Figura 2: Habilite un perfil para el LDAP



Cuando la autenticación de MAC de los proxys ACS a balizar con el LDAP, la interrogación consiste en dos interrogaciones sub. Ambos deben volver un resultado válido, no nulo. La primera interrogación a balizar es independientemente de si el MAC está sabido para balizar, por ejemplo, si se ha descubierto y se ha agregado a la base de datos del faro. Si el punto final tiene todavía ser descubierto por el faro, el punto final se considera ser desconocido.

La segunda interrogación no es necesaria en el caso de los puntos finales que el faro no ha descubierto y no está en su base de datos. Si el punto final se ha descubierto y está en la base de datos del faro, la interrogación siguiente es determinar el perfil actual del punto final. Si un punto final tiene todavía ser perfilado o está actualmente en un perfil no 5 habilitados para el LDAP, el resultado desconocido se vuelve al ACS, y la autenticación del punto final por el faro falla. Depende de cómo se configura que éste puede dar lugar al dispositivo con la negación del acceso a la red en conjunto, o se dé el ACS una directiva que sea apropiada para los dispositivos el desconocido o del invitado.

Solamente en el caso donde está un punto final el MAC que el faro ha descubierto y colocado en un perfil LDAP-habilitado, la respuesta es que el punto final está conocido y perfilado por el faro esté vuelto al ACS. Lo que es más importante, porque faro de estos puntos finales proporciona el nombre del perfil actual. Esto permite al ACS para asociar los puntos finales conocidos a los grupos de Cisco SecureAccess. Esto habilita una determinación granular de la directiva hecha, tan granular como una política diferenciados para cada perfil LDAP-habilitado faro, si está deseada.

Configuración de ACS para el MAB y utilización del faro como Base de datos de usuarios externa

La configuración del ACS para el MAB y de la utilización del faro como Base de datos de usuarios externa requiere tres pasos claros. La orden ilustrada en este documento sigue un flujo de trabajo que sea eficiente cuando realiza la configuración MAB en su totalidad, y pueda variar para los sistemas que han sido en funcionamiento con otros modos de autenticación configurados ya.

Cuando usted intenta el MAB para un punto final específico que intente conectar con la red, el ACS pregunta el faro en el LDAP para determinar si el faro ha descubierto el MAC, y qué faro del perfil ha puesto actualmente el MAC address adentro según lo descrito anterior en el documento.

En este documento, se crean dos perfiles separados:

- BeaconKnownDevices — para los puntos finales descubiertos y perfilados por el faro
- BeaconUnknownDevices — para los dispositivos que no son sabidos actualmente por el faro

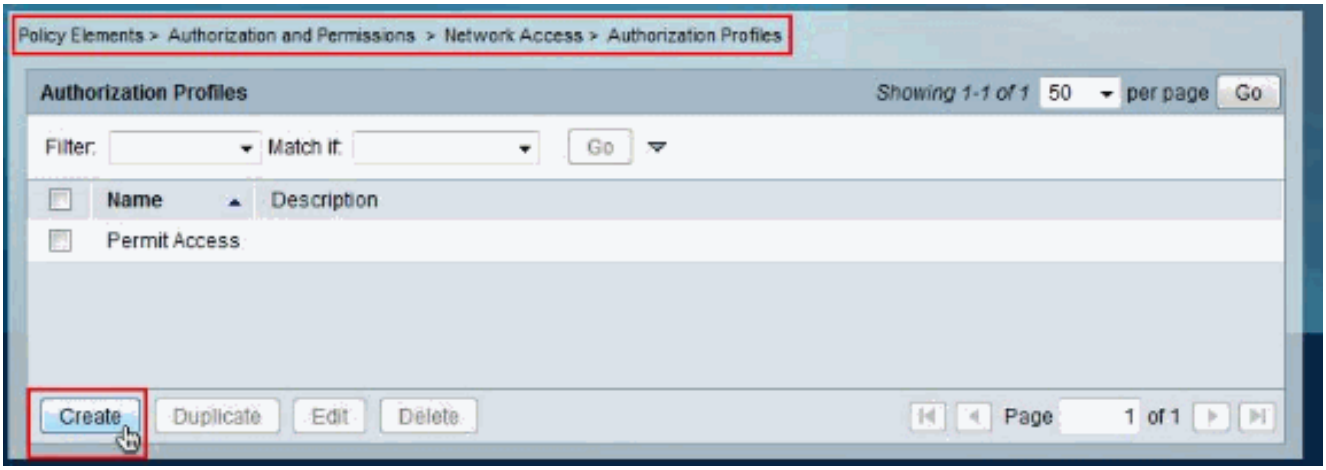
Cualquier faro no ha descubierto el MAC, ni lo ha perfilado actualmente a un perfil LDAP-habilitado. El perfil de BeaconKnownDevices pondrá los puntos finales en el VLAN10 y el perfil de BeaconUnkownDevices pondrá los puntos finales en el VLA N 7.

Más adelante en este documento, una conexión LDAP al Profiler del punto final del faro del ACS se crea y eligen del Profiler del punto final del faro basado en qué puntos finales serán considerados como dispositivos de BeaconKnown, y serán asignados los grupos el perfil de BeaconKnownDevices (que los pondrá en el VLA N 10). Todos los dispositivos desconocidos que cualquier faro no ha descubierto el MAC, ni lo ha perfilado actualmente en un perfil LDAP-habilitado serán asignados el perfil de BeaconUnkownDevices (que los pondrá en el VLA N 7).

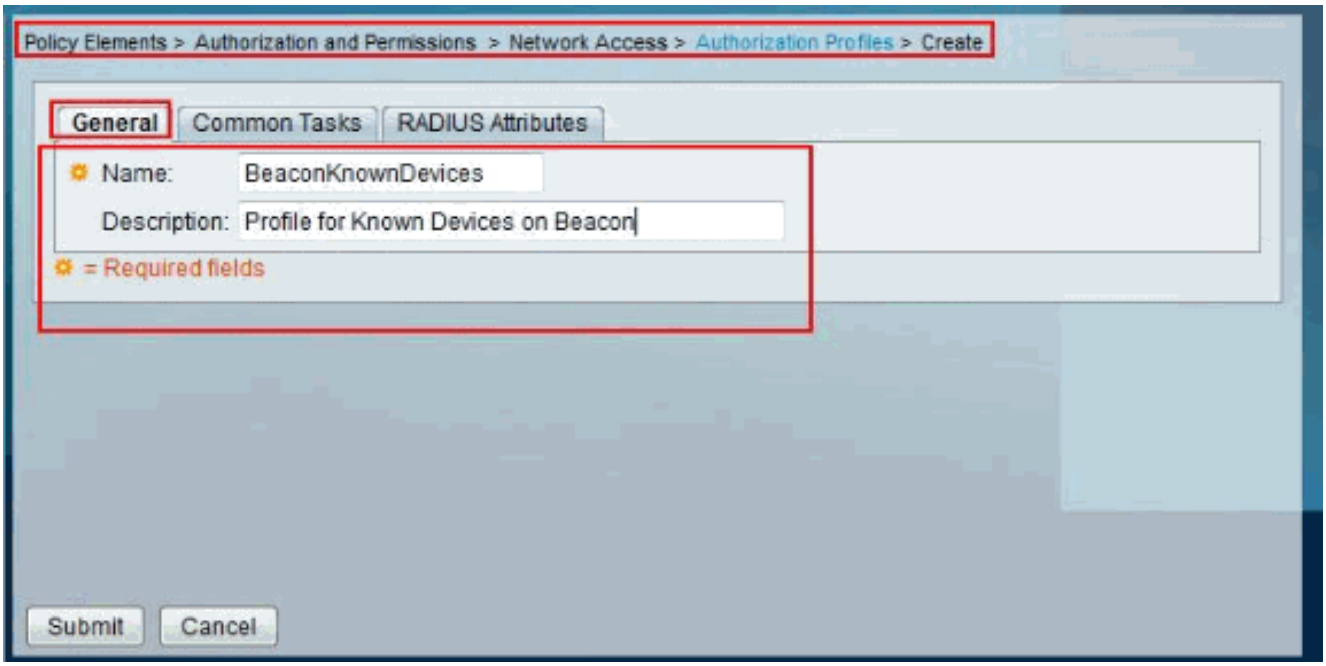
Cree un perfil de la autorización

Complete estos pasos para crear un perfil de la autorización:

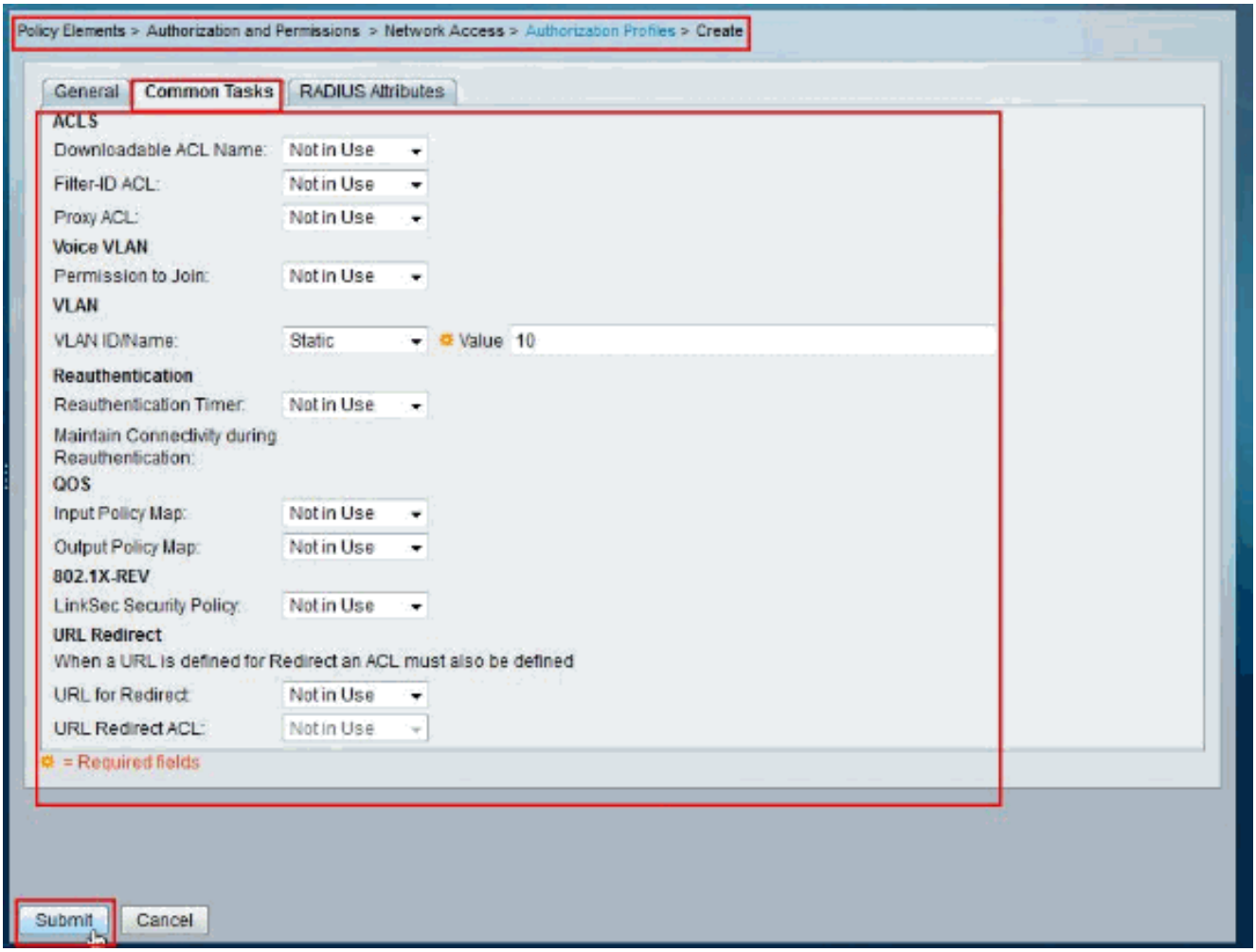
1. Elija los **elementos > la autorización de la directiva y los permisos > el acceso a la red > los perfiles** y el tecleo de la **autorización crean** para crear un nuevo perfil de la autorización.



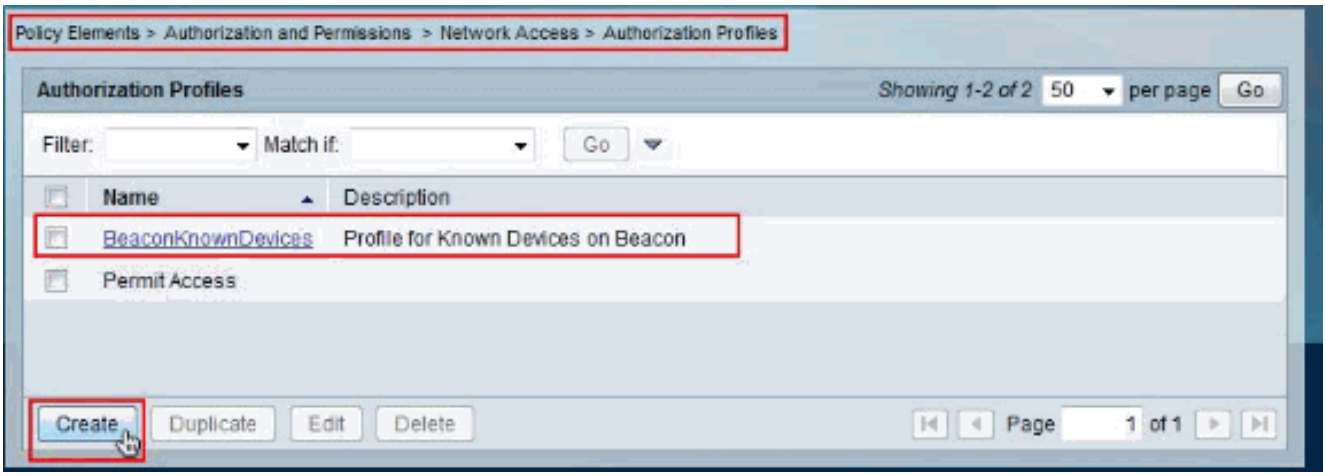
2. Proporcione el **nombre del** nuevo perfil de la autorización.



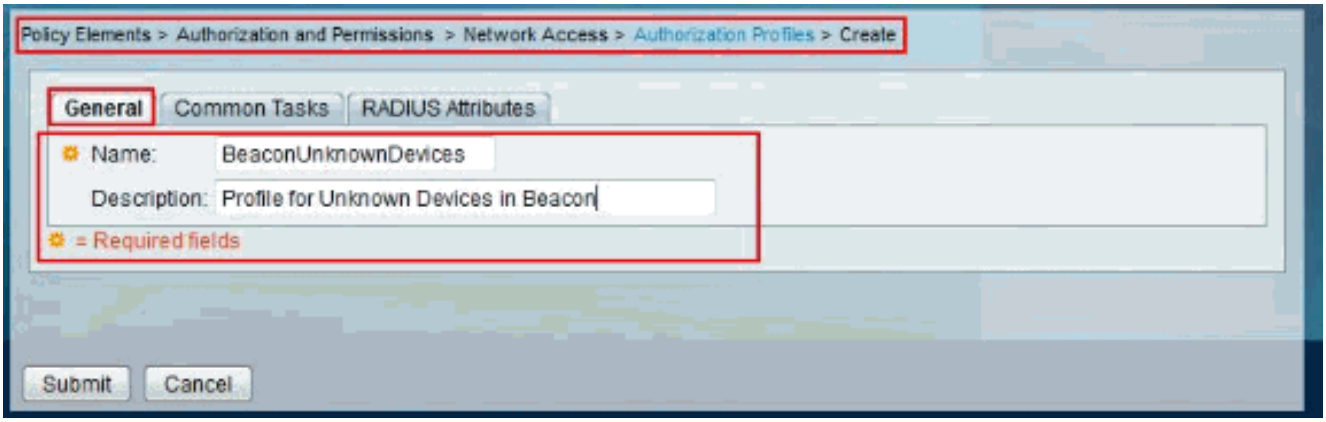
3. En las **tareas comunes la** lengueta fijó el **VLA N a los parásitos atmosféricos** con el **valor** como **10.** Entonces, el tecleo **somete**.



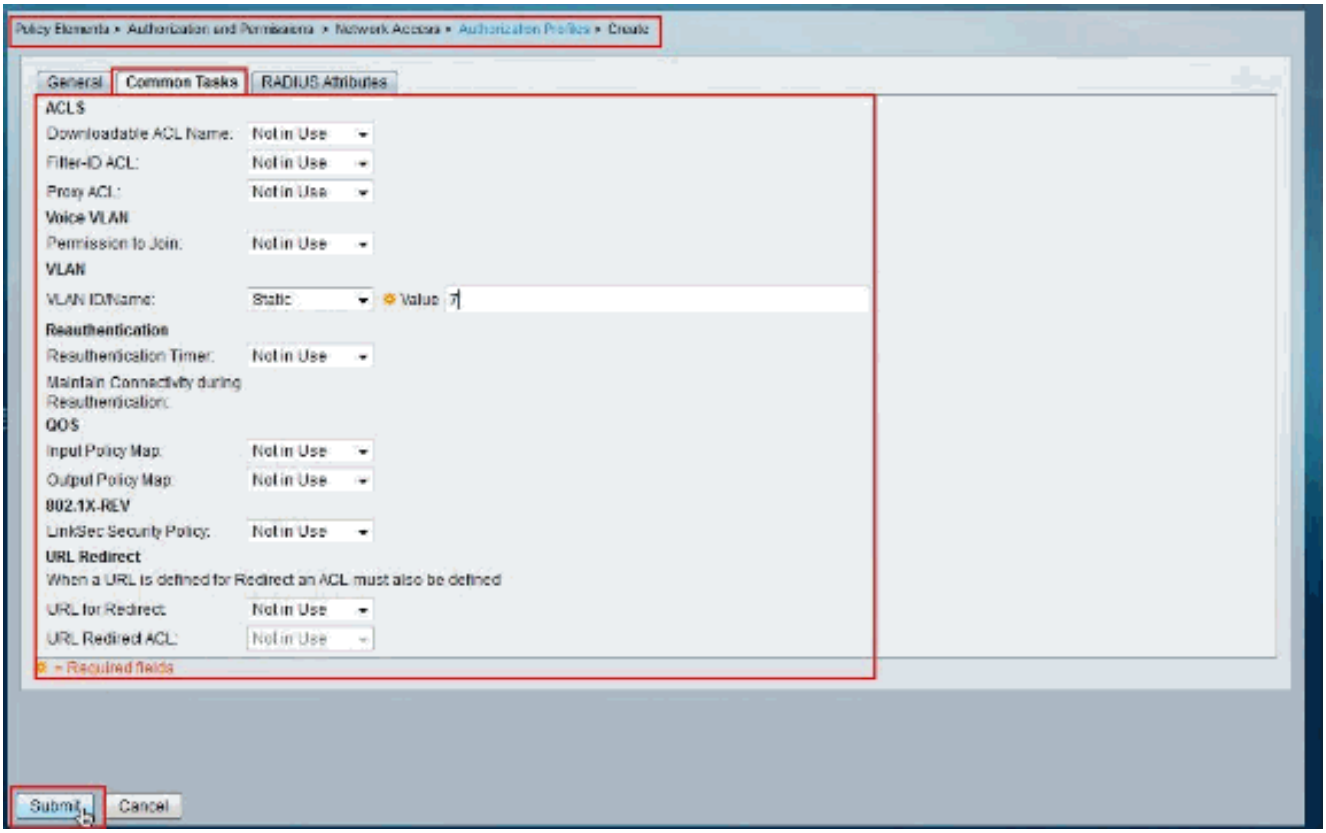
4. Elija los **elementos > la autorización de la directiva y los permisos > el acceso a la red > los perfiles** y el tecleo de la **autorización crean** para crear un nuevo perfil de la autorización.



5. Proporcione el **nombre del** nuevo perfil de la autorización.



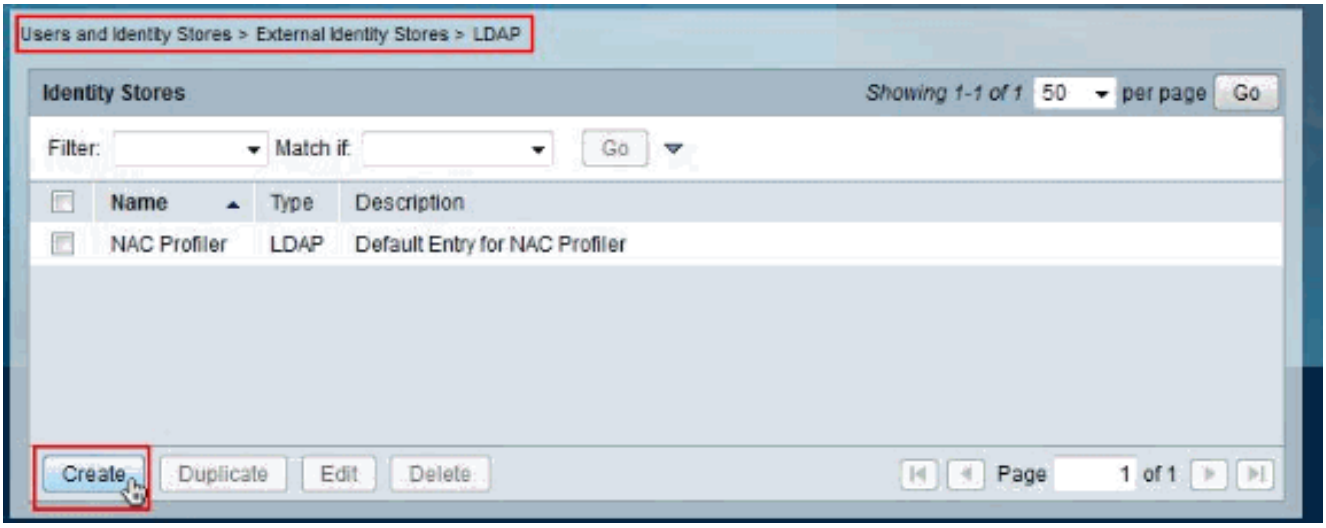
6. En las **tareas comunes la** lengueta fijó el **VLA N a los parásitos atmosféricos** con el **valor** como **7.** Entonces, el tecleo **somete**.



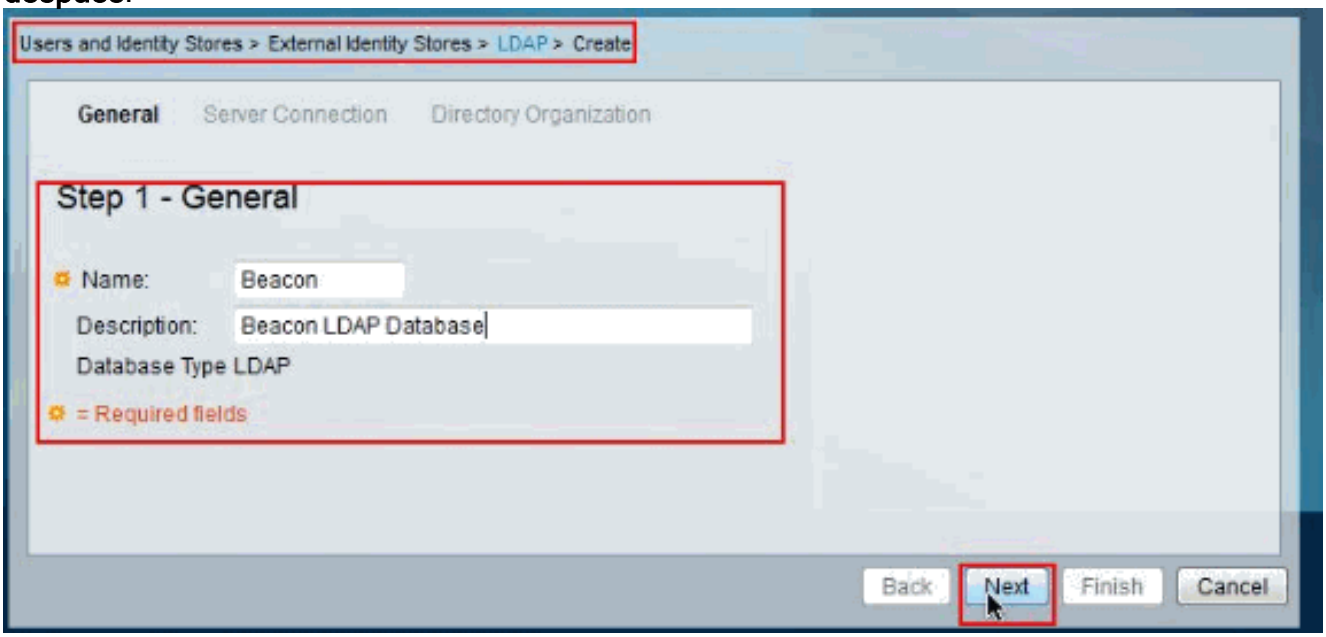
Cree una conexión de base de datos de LDAP

Complete los pasos para crear una conexión de base de datos de LDAP:

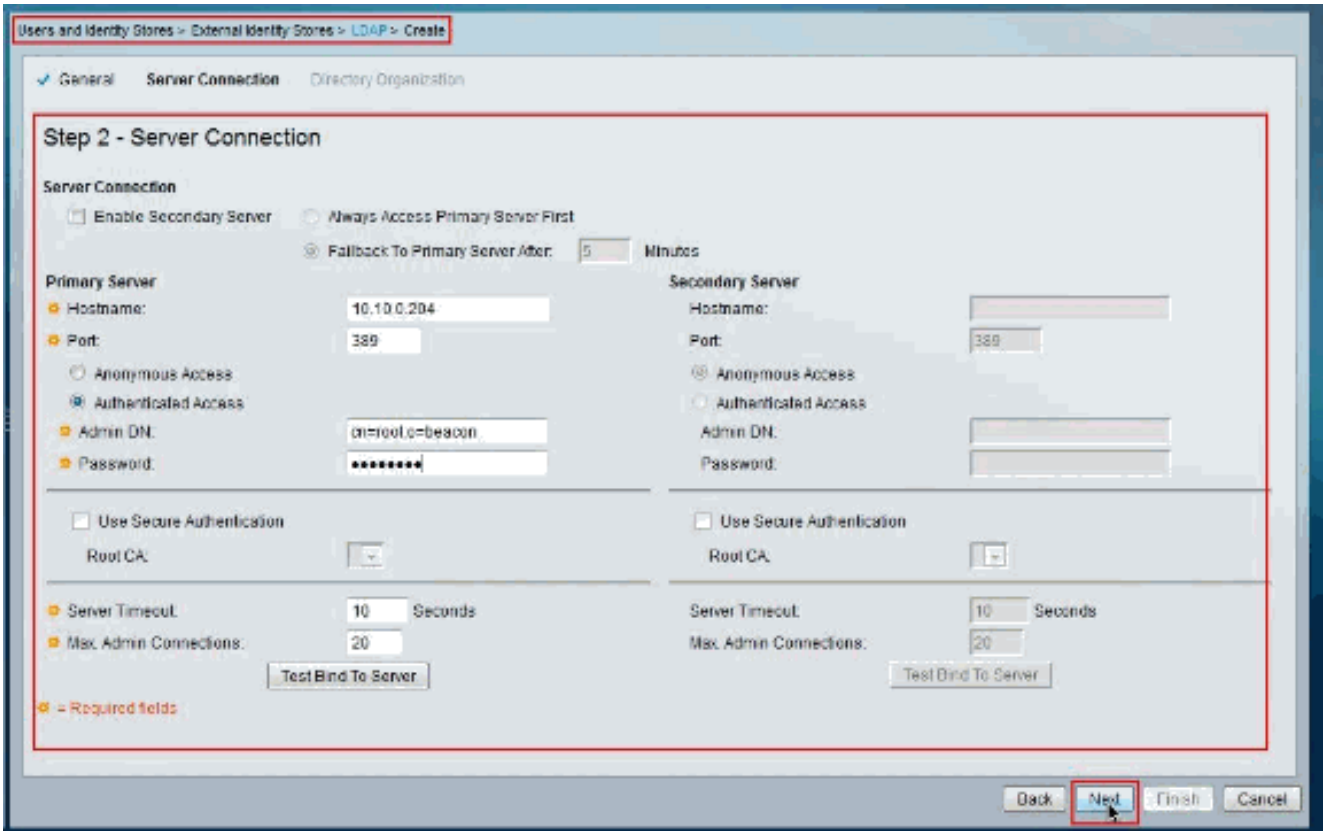
1. Elija a los **usuarios y la identidad salva > identidad externa salva > LDAP** y tecleo **crea** para crear una nueva conexión de base de datos de LDAP.



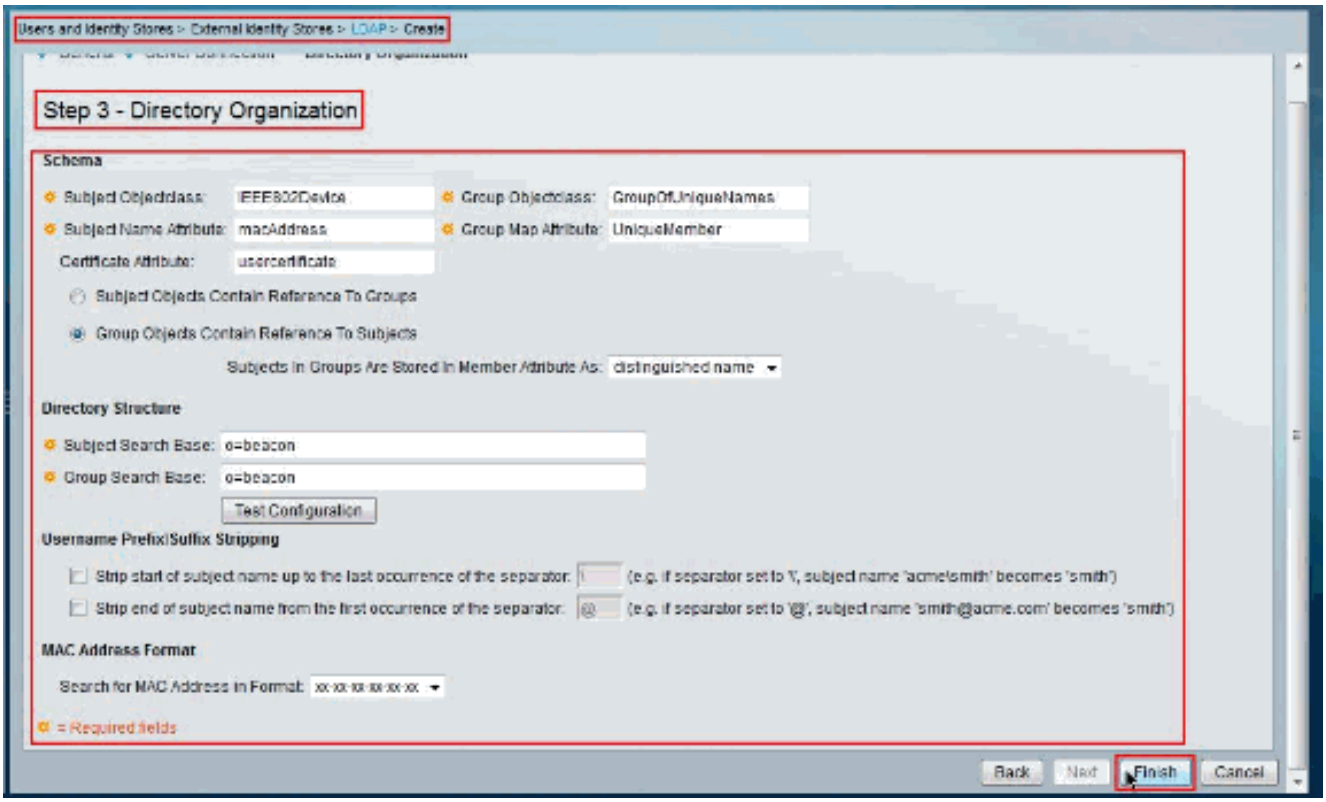
2. Proporcione un **nombre** para la nueva **conexión de base de datos de LDAP** y haga clic **después**.



3. En la lengueta de la **conexión del servidor** ingrese el **nombre de host/el IP Address del LDAP del FARO separan, viran hacia el lado de babor, Admin DN, la contraseña** (GBSbeacon en este ejemplo). Entonces, haga clic
después.

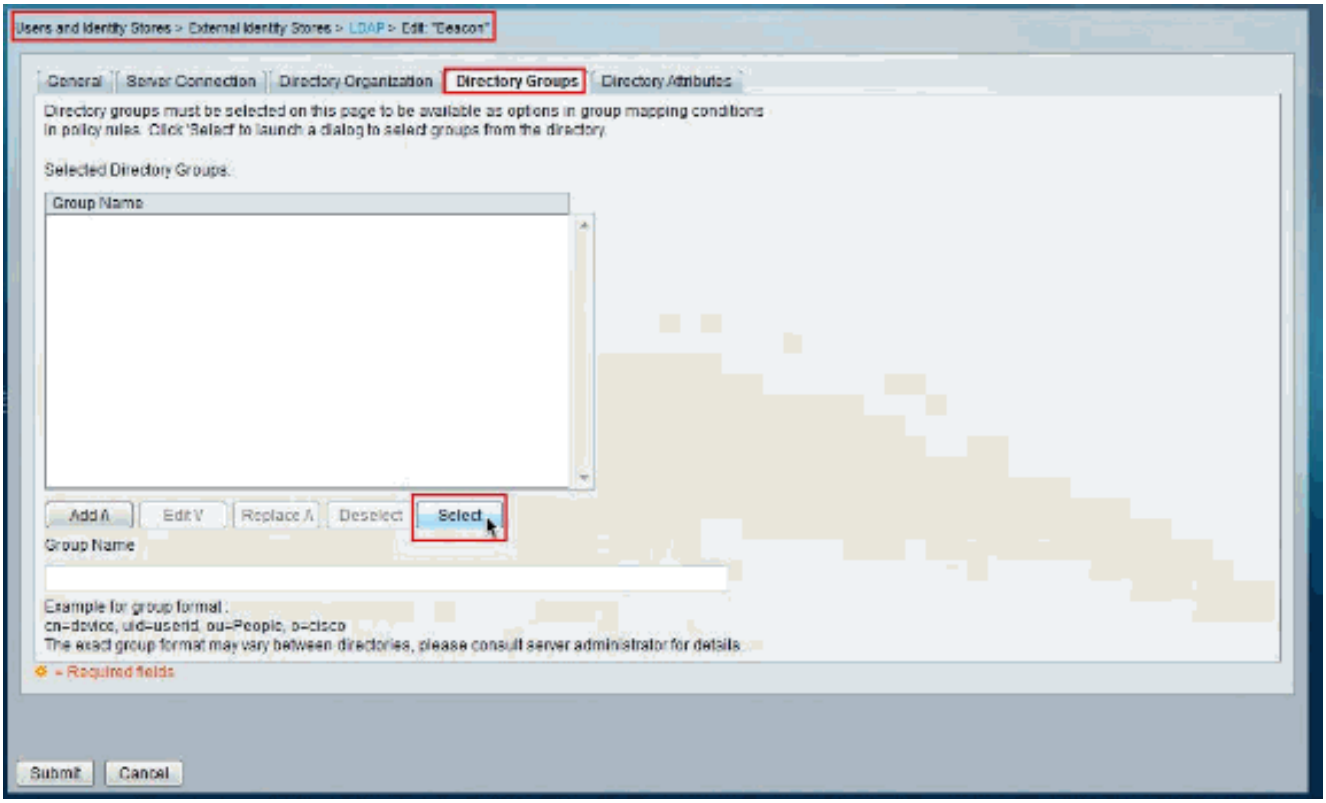


4. En la lengueta de la **organización del directorio** ingrese la Información requerida. Entonces, clic en
Finalizar.

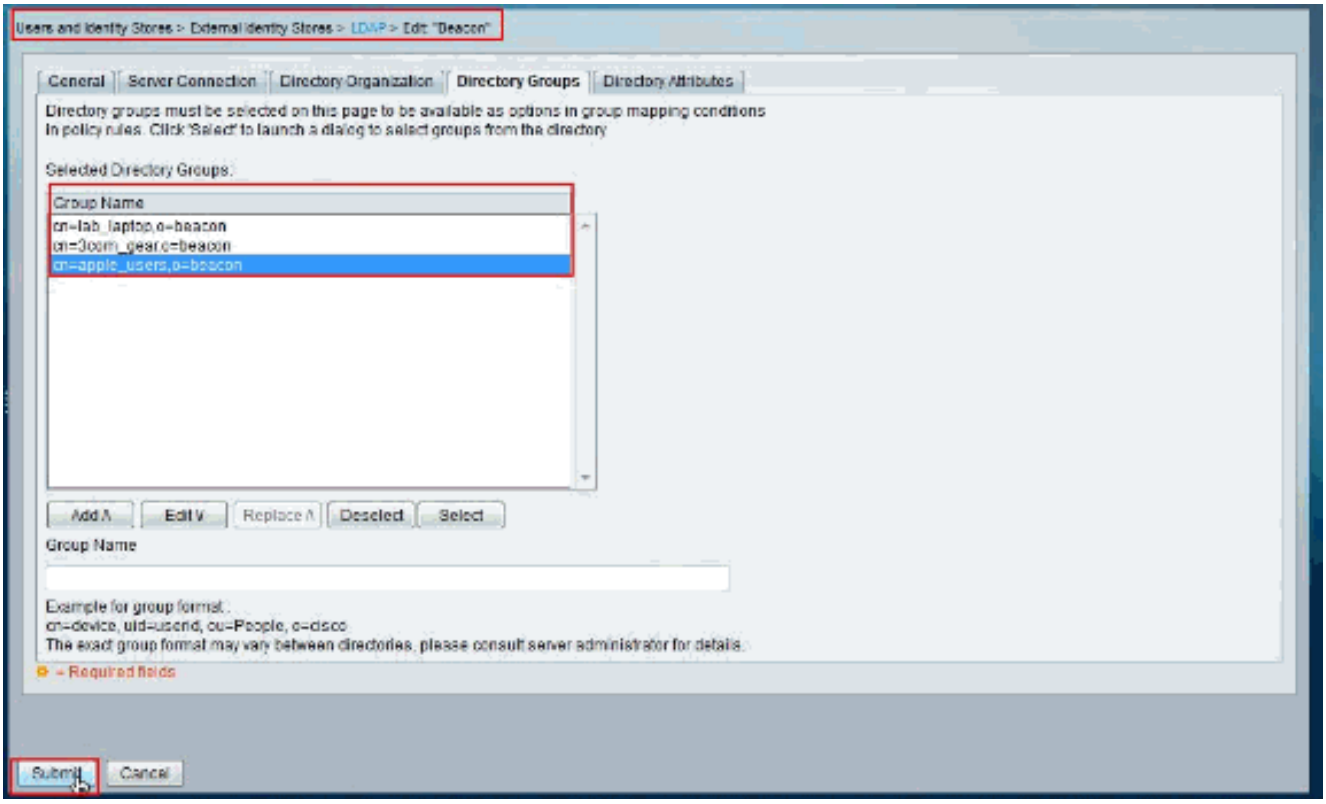


5. Haga clic la **conexión LDAP** creada recientemente (faro en este ejemplo).

6. Elija la lengueta de los **grupos del directorio** y haga clic **selecto**.
conexión.



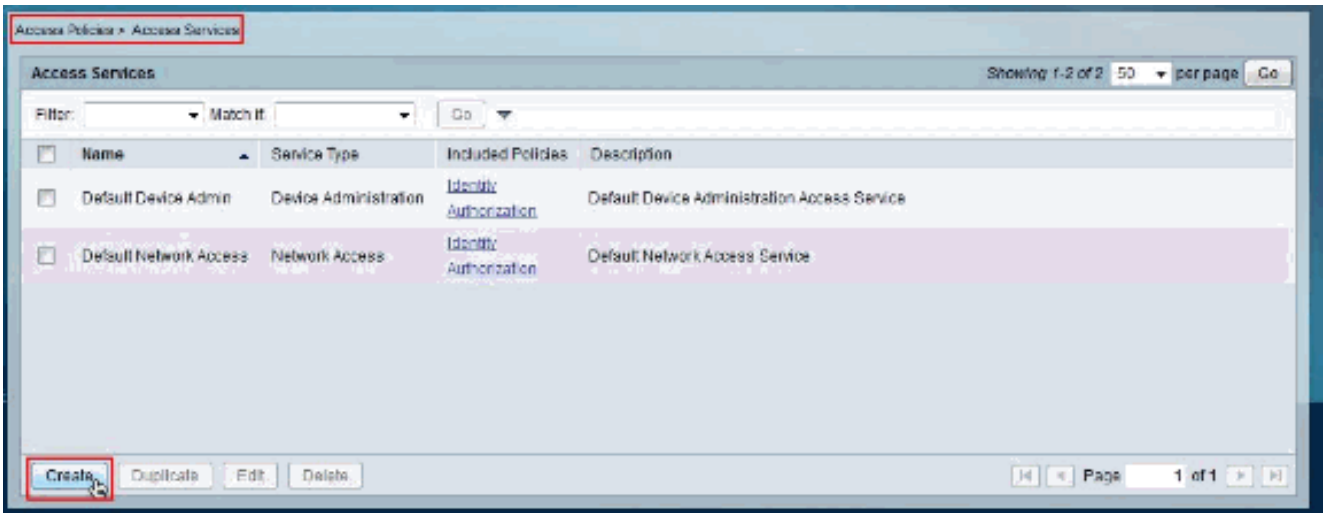
7. Seleccione a todos los grupos en la siguiente pantalla que usted quiere asociar a **BeaconKnownDevices**.
8. En este ejemplo eligen a estos grupos, a saber lab_laptop, 3com_gear y los apple_users. Entonces, el tecleo
somete.



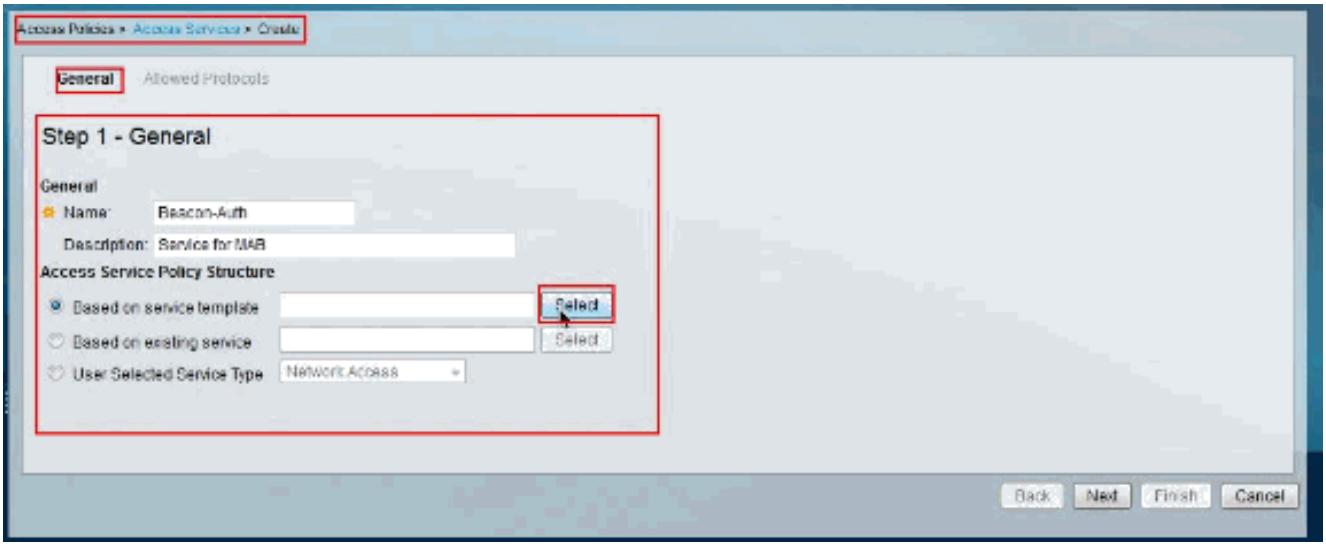
Servicios del acceso de la configuración

Complete estos pasos para configurar los servicios del acceso:

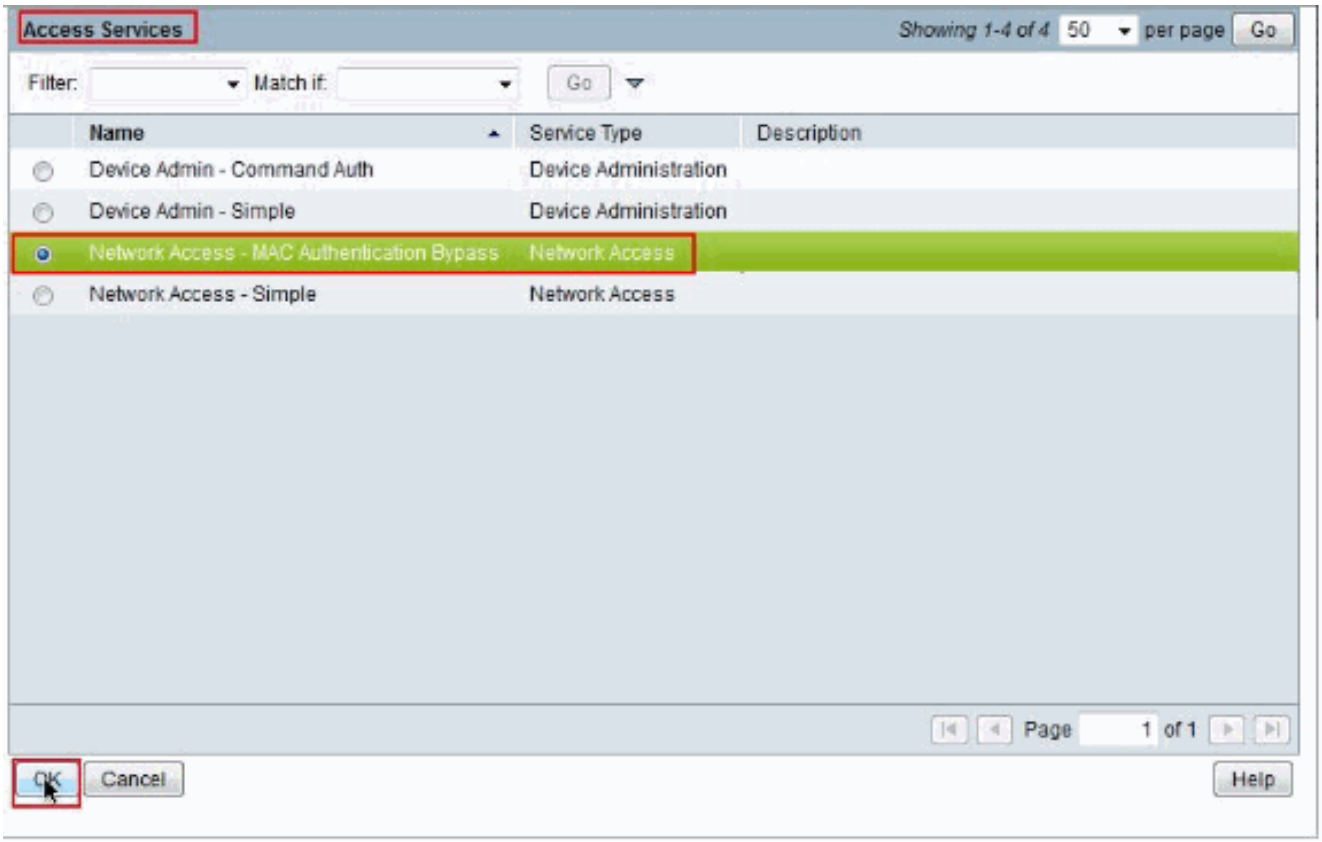
1. Elija las **políticas de acceso > los servicios del acceso** y el tecleo **crea** para crear un nuevo servicio del
acceso.



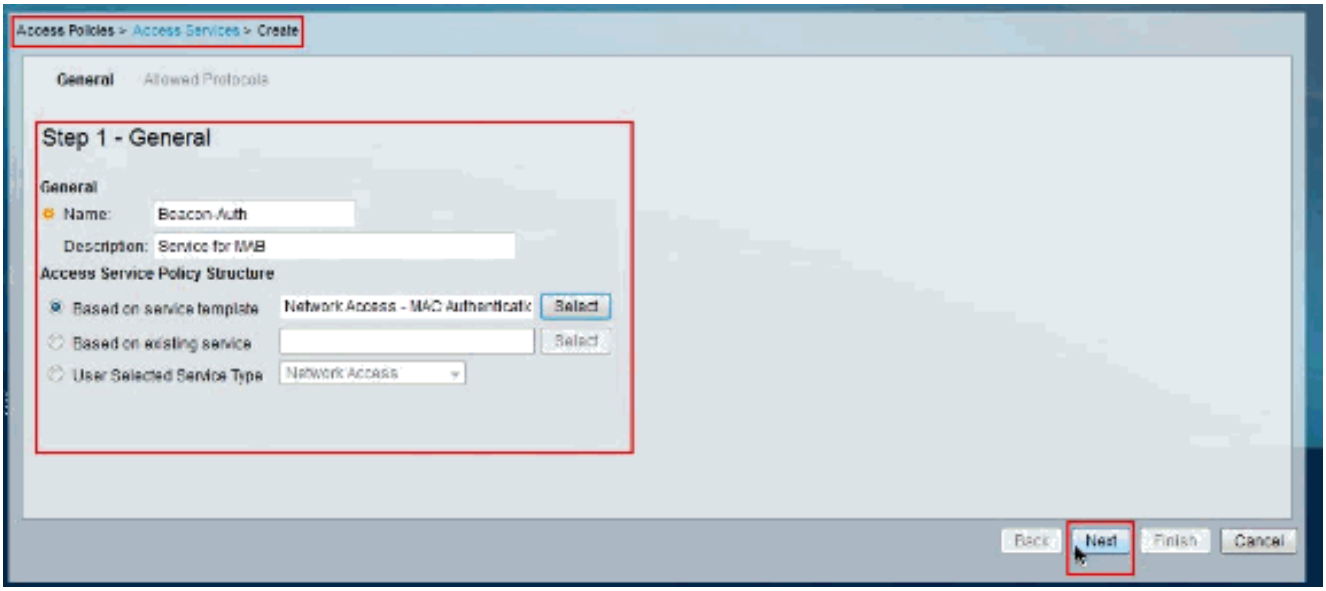
2. En la **ficha general** proporcione el **nombre del** nuevo servicio, después haga clic **selecto** al lado de **basado en la plantilla del**
servicio.



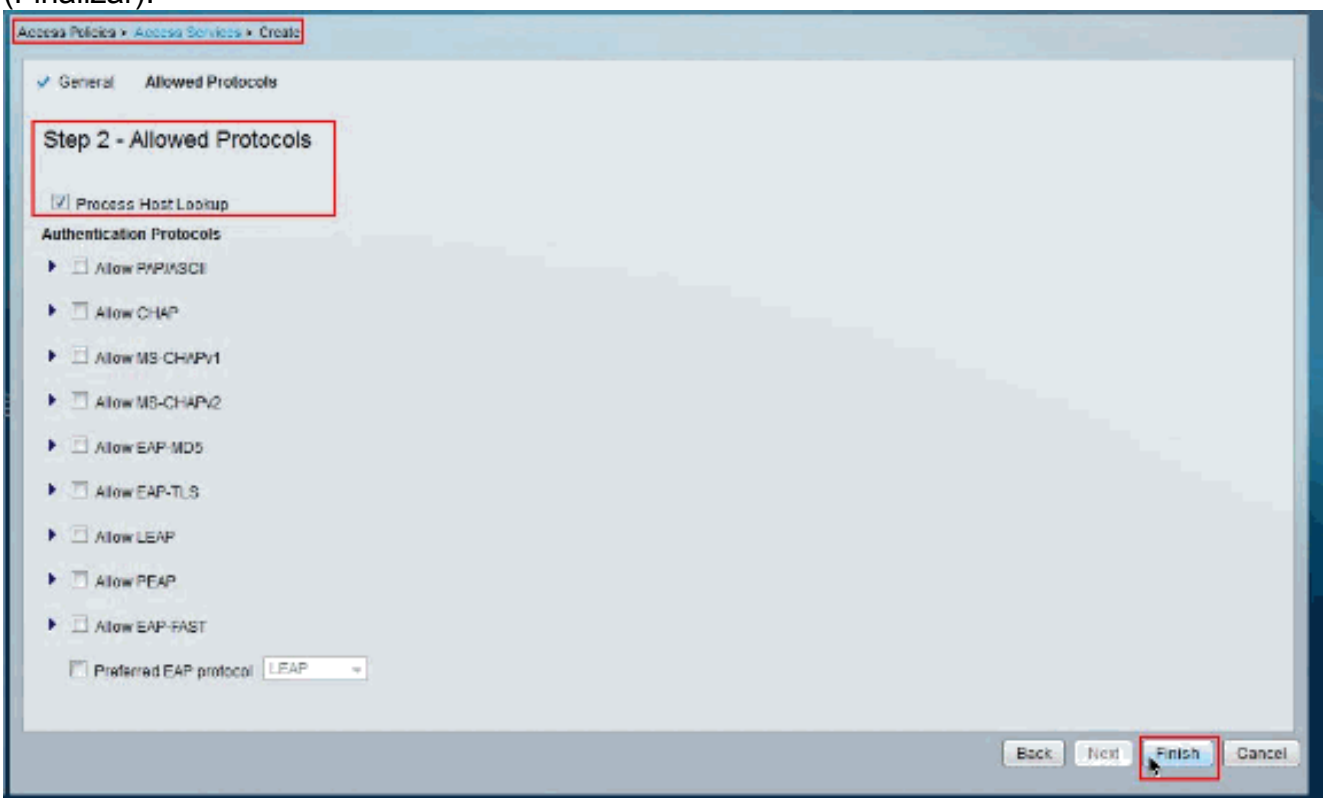
3. Elija el **acceso a la red - Puente de la autenticación de MAC** y **AUTORIZACIÓN** del tecleo.



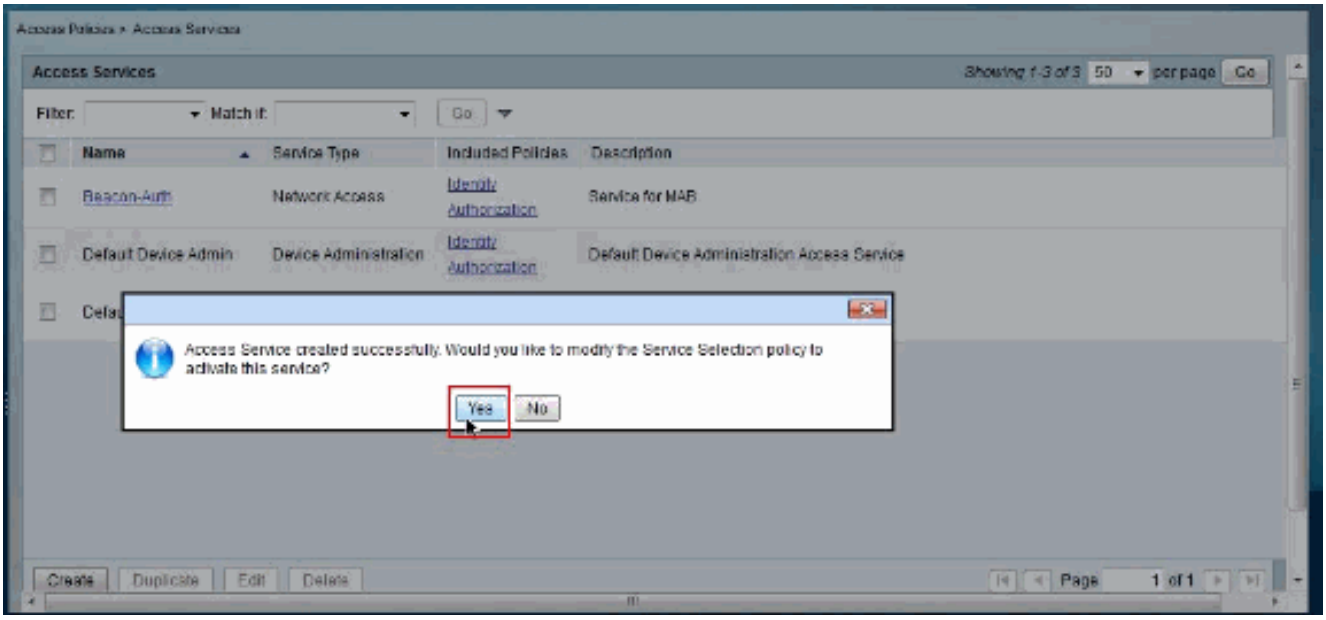
4. Haga clic en Next (Siguiente).



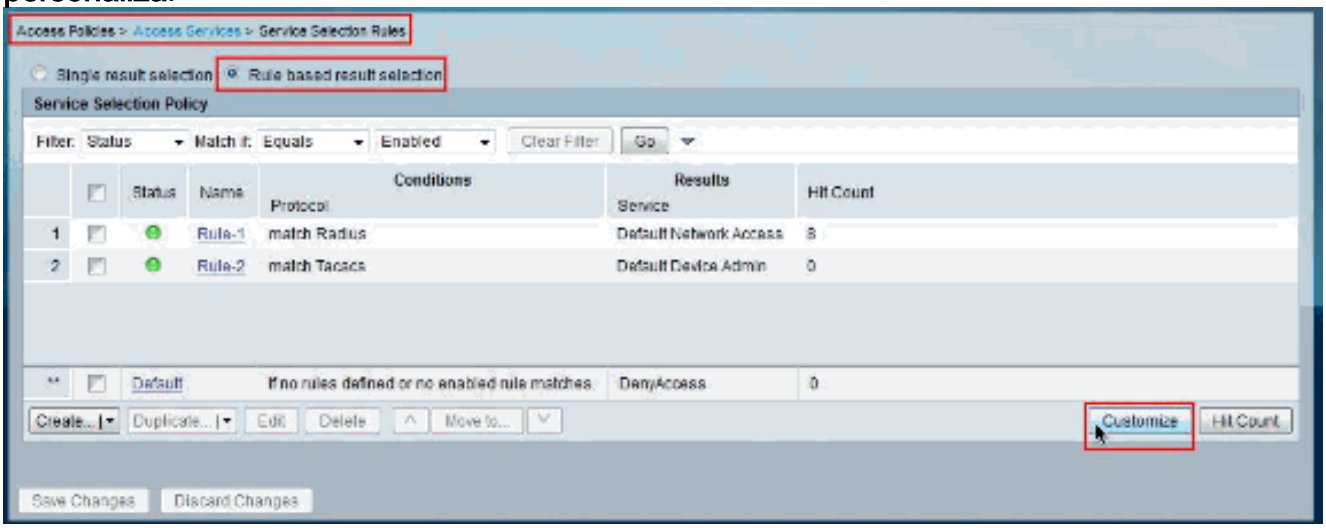
5. Haga clic en Finish (Finalizar).



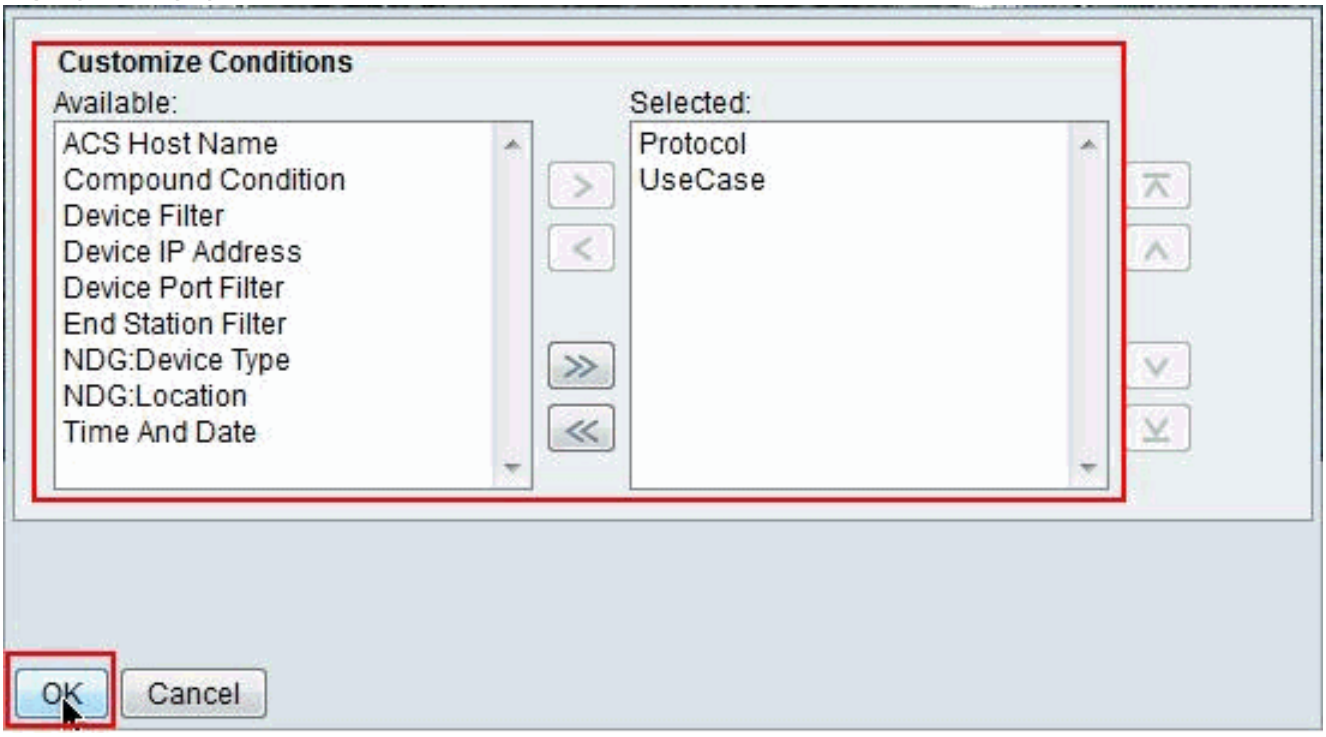
6. Haga clic en Sí



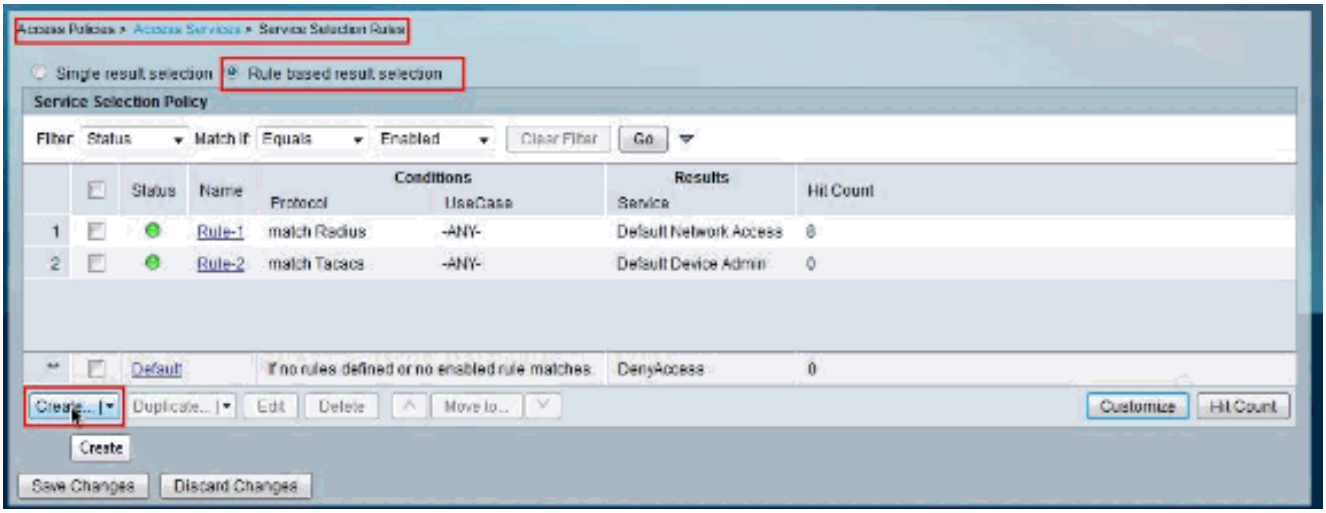
7. El tecleo **personaliza**.



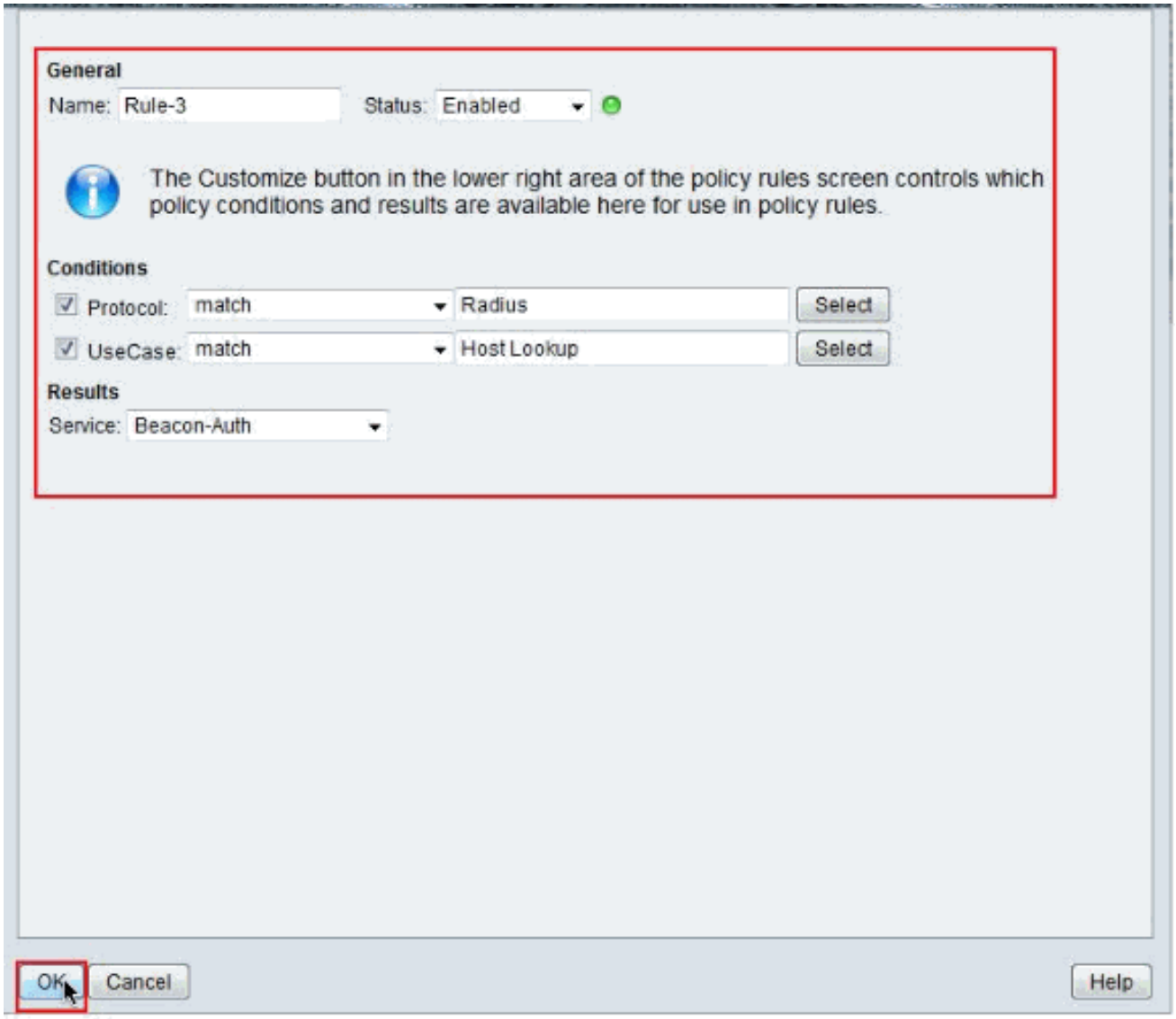
8. Mueva **UseCase** desde **haber seleccionado disponible** y haga clic la **AUTORIZACIÓN**.



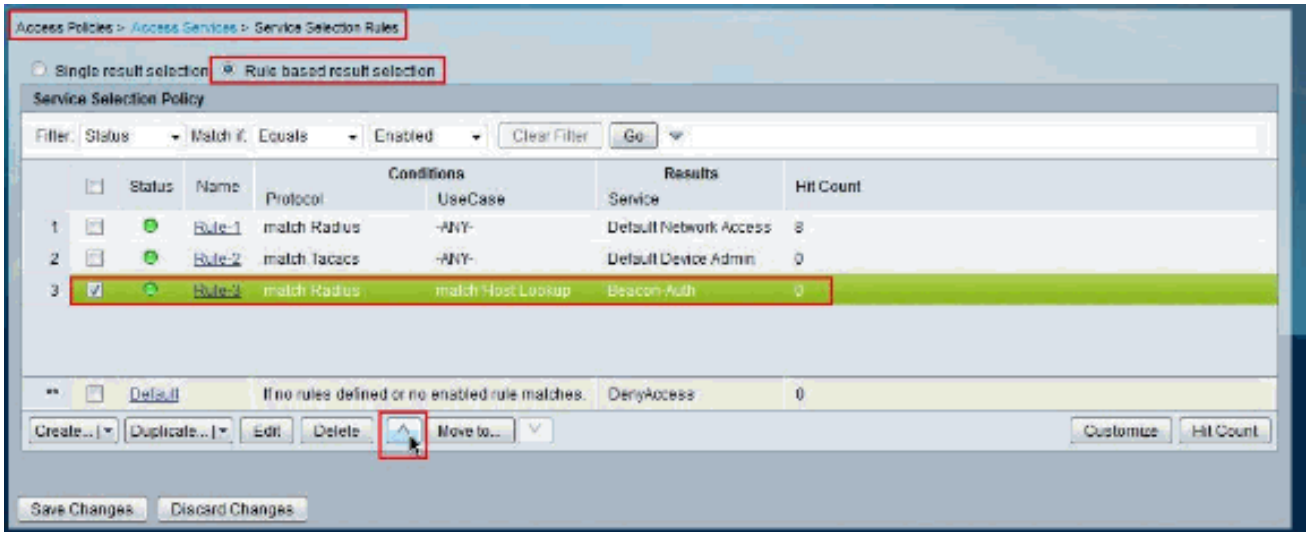
9. El tecleo **crea** para crear una nueva **regla de selección del servicio**.



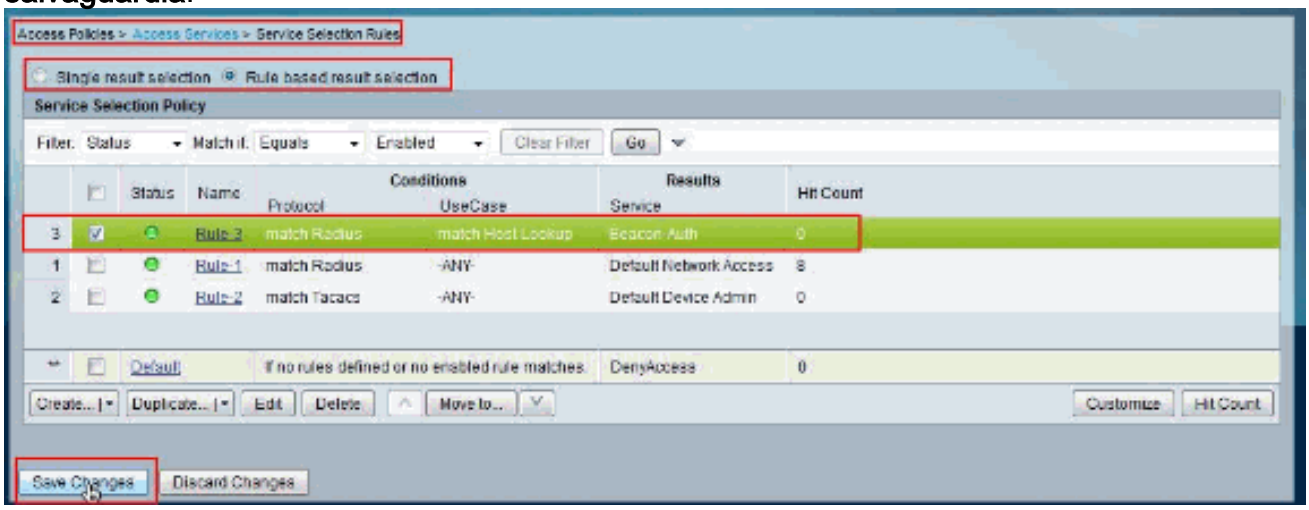
10. Seleccione el **protocolo** y utilice el **radio** como el valor. Semejantemente, **UseCase** selecto y el uso **reciben las operaciones de búsqueda** como valor. Elija el Faro-**auth** como el servicio y haga clic la **AUTORIZACIÓN**.



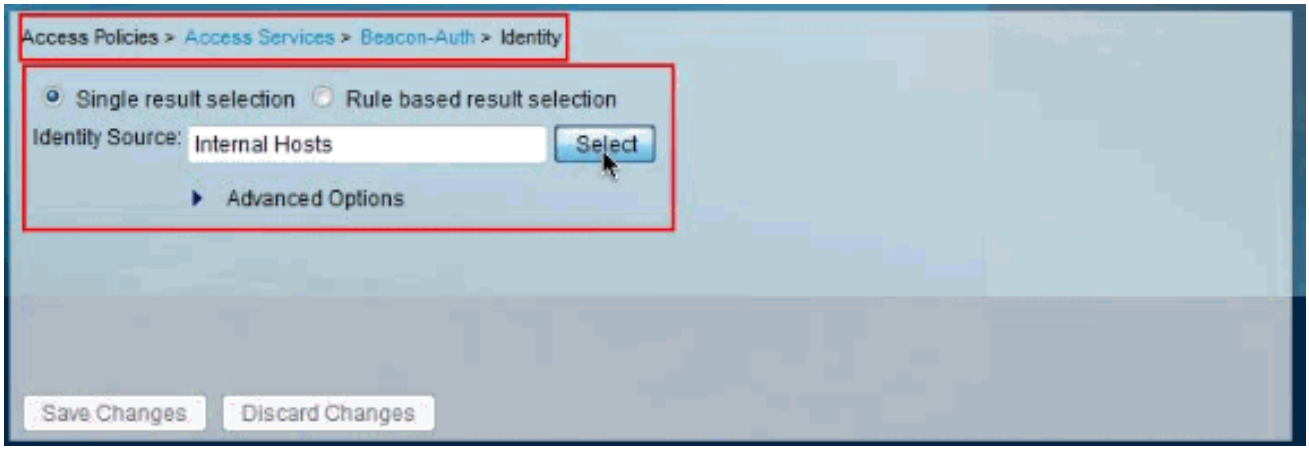
11. Mueva la regla creada recientemente al top.



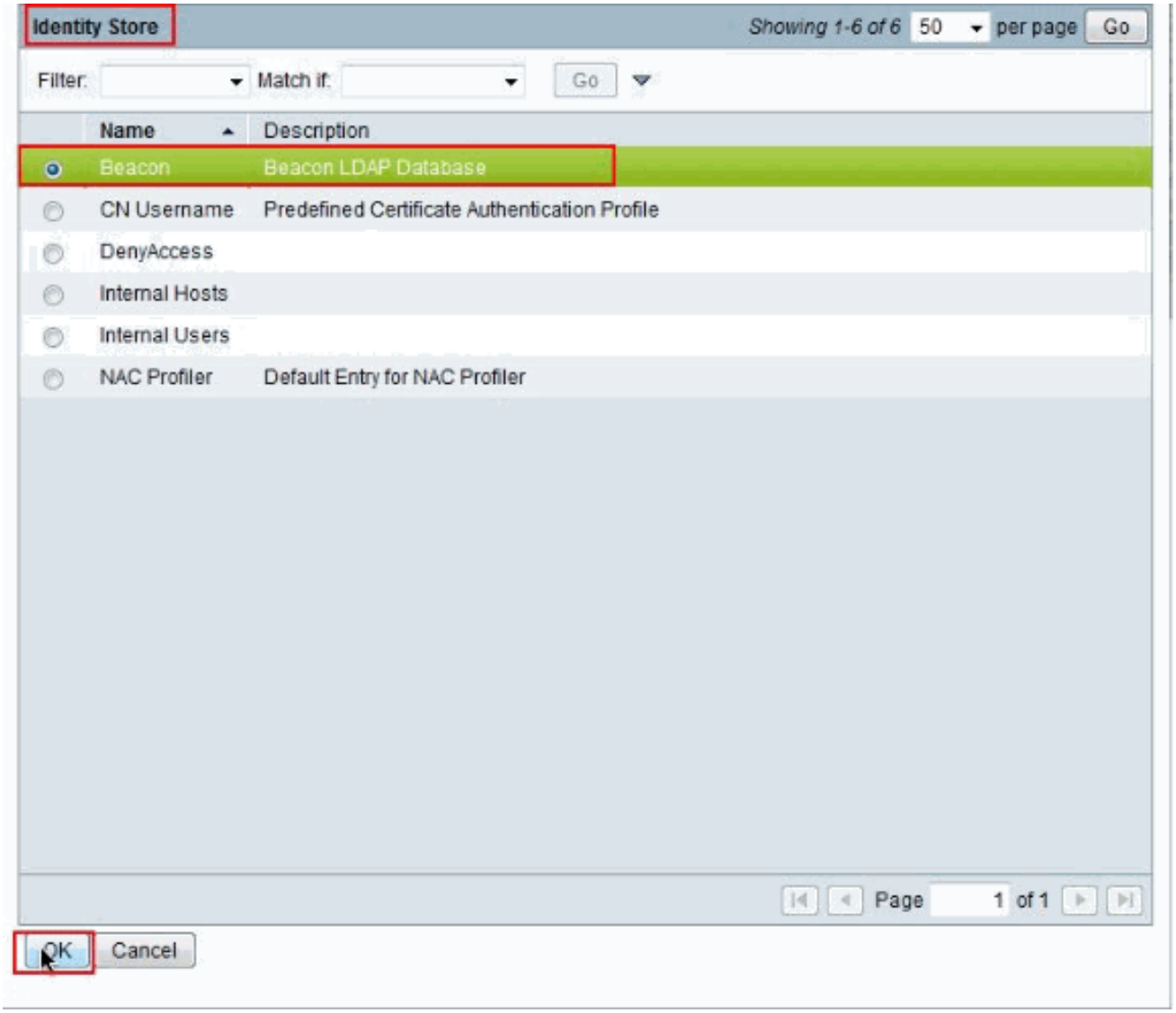
12. Haga clic los **cambios de la salvaguardia**.



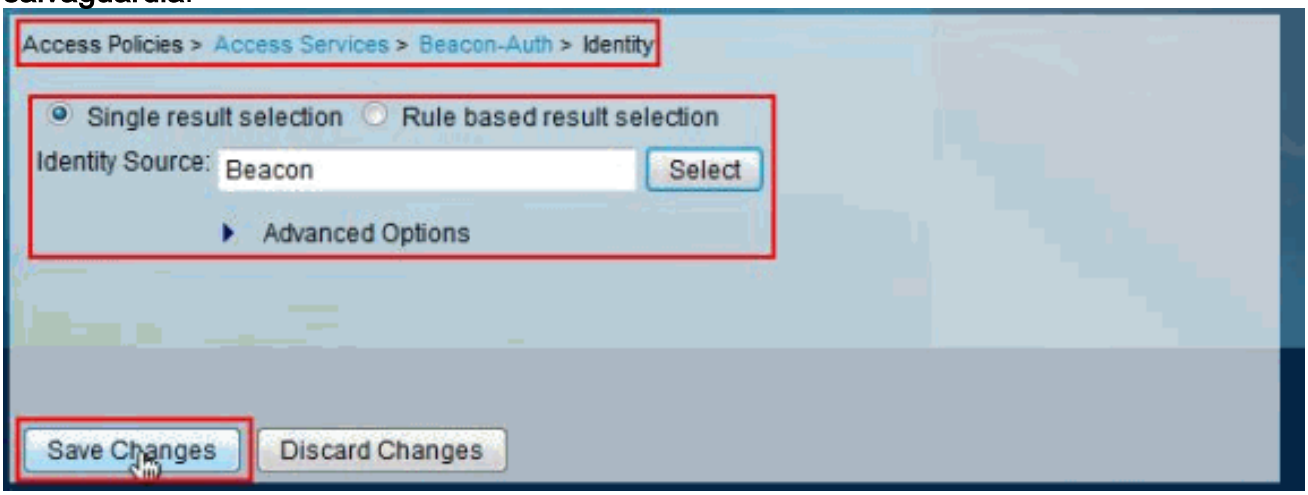
13. Elija las **políticas de acceso > el acceso mantiene > Faro-auth > identidad** y hace clic **selecto** al lado de la **fuente de la identidad**.



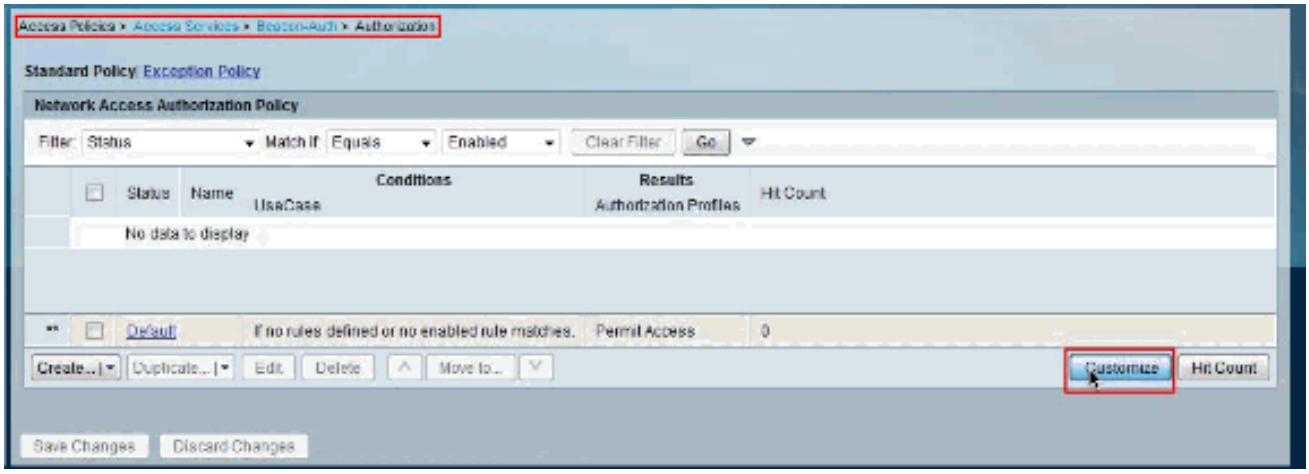
14. Elija el **faro** y haga clic la **AUTORIZACIÓN**.



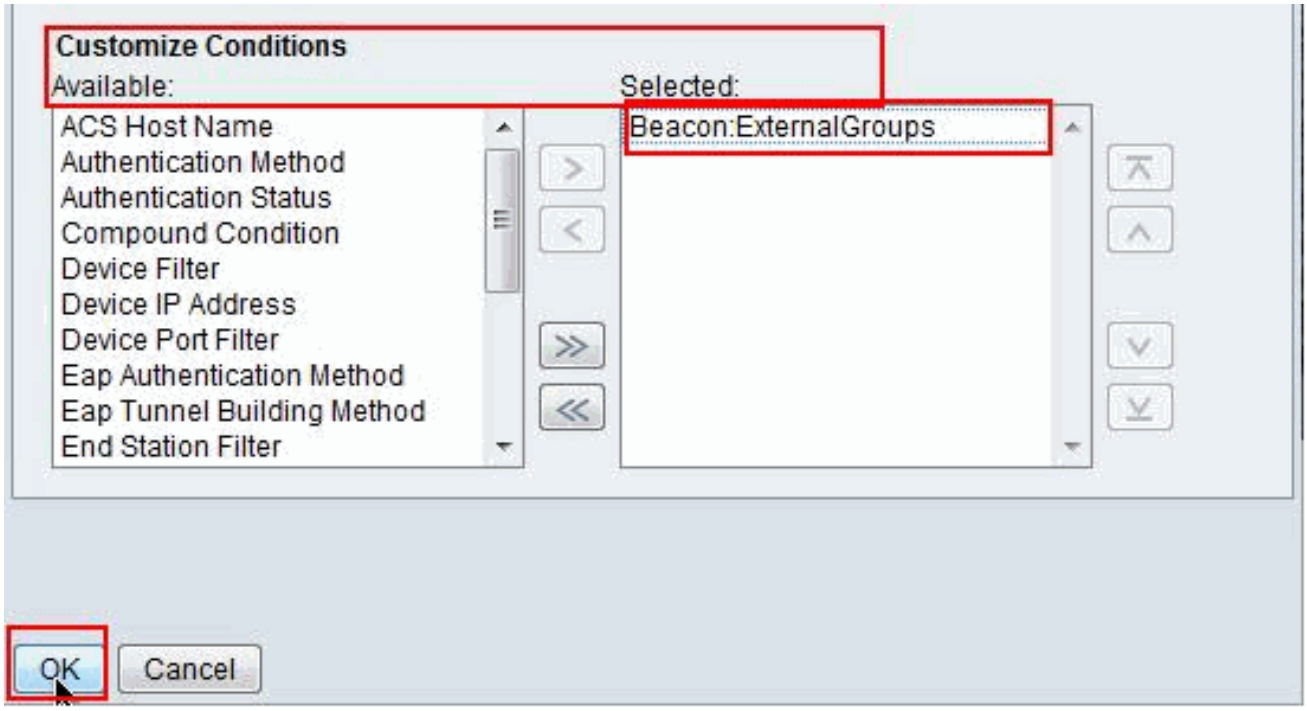
15. Haga clic los **cambios de la salvaguardia**.



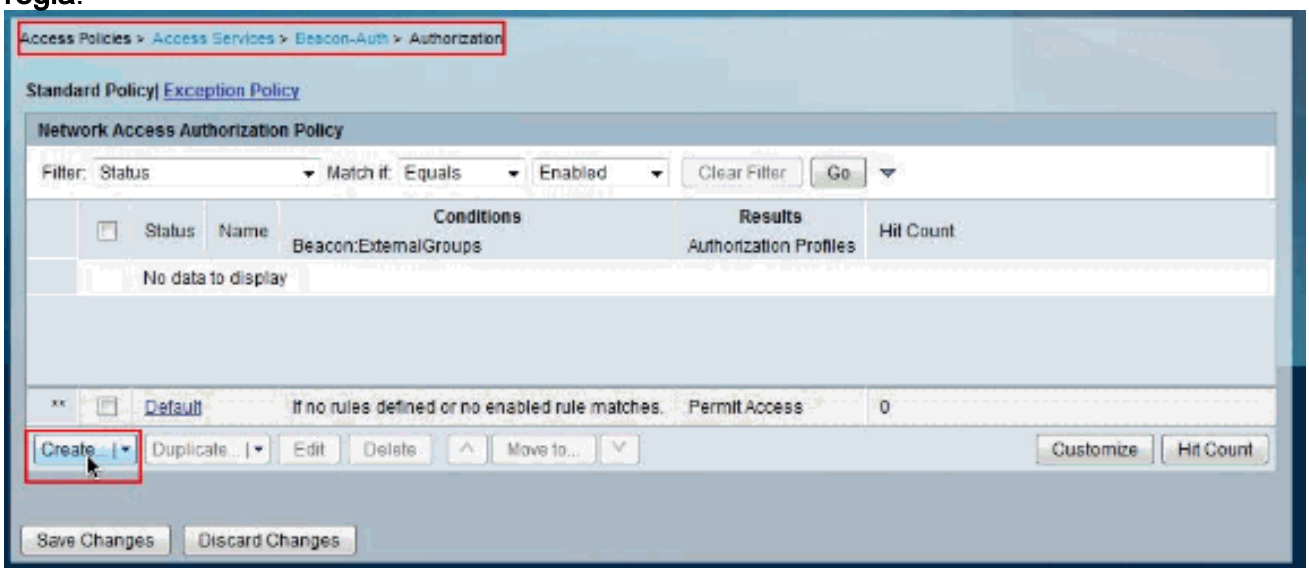
16. Elija las **políticas de acceso > el acceso mantiene > Faro-auth > autorización** y el tecleo **personaliza**.



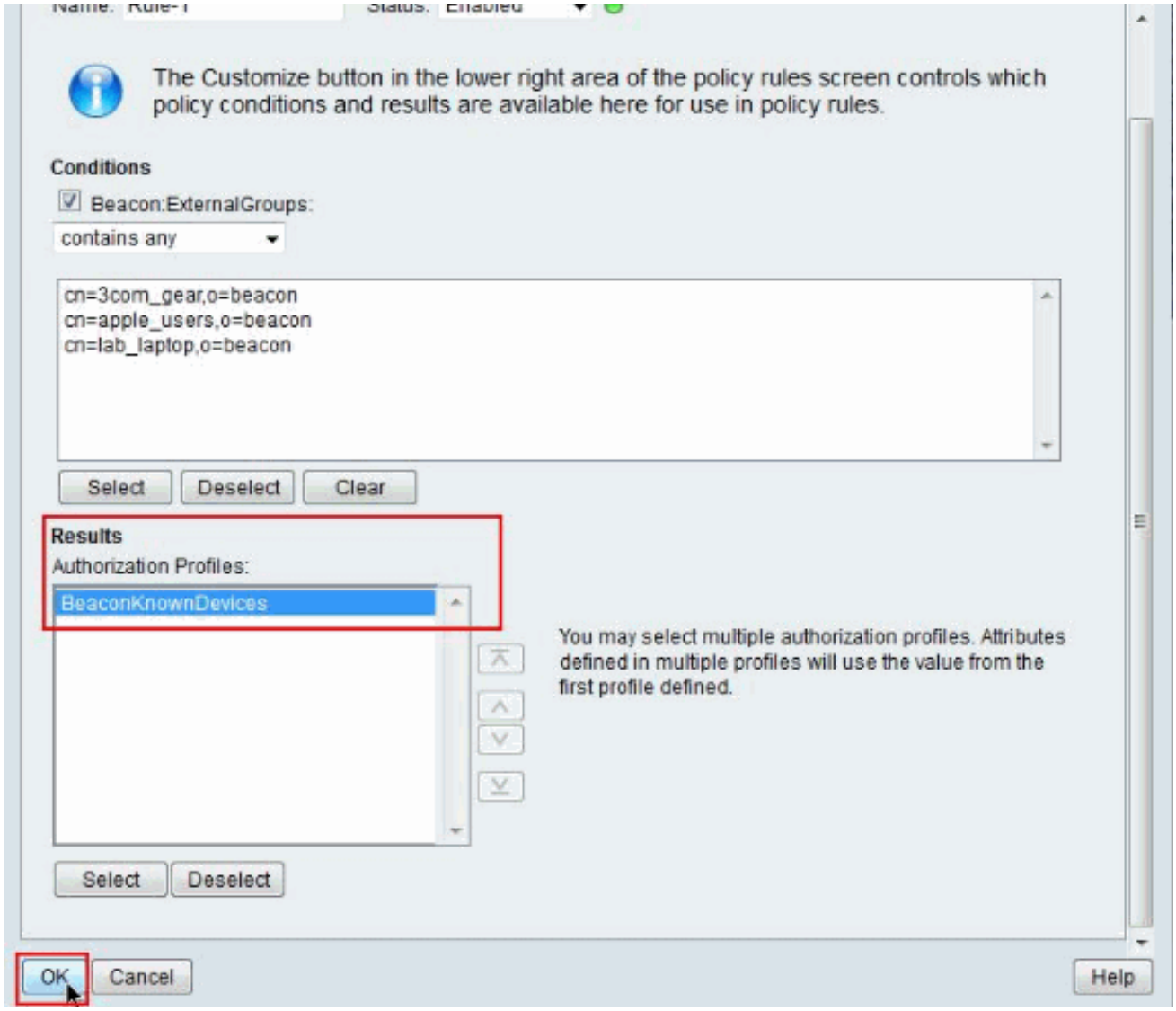
17. **Faro del** movimiento**: ExternalGroups de disponible seleccionó** y de la **AUTORIZACIÓN del** tecleo.



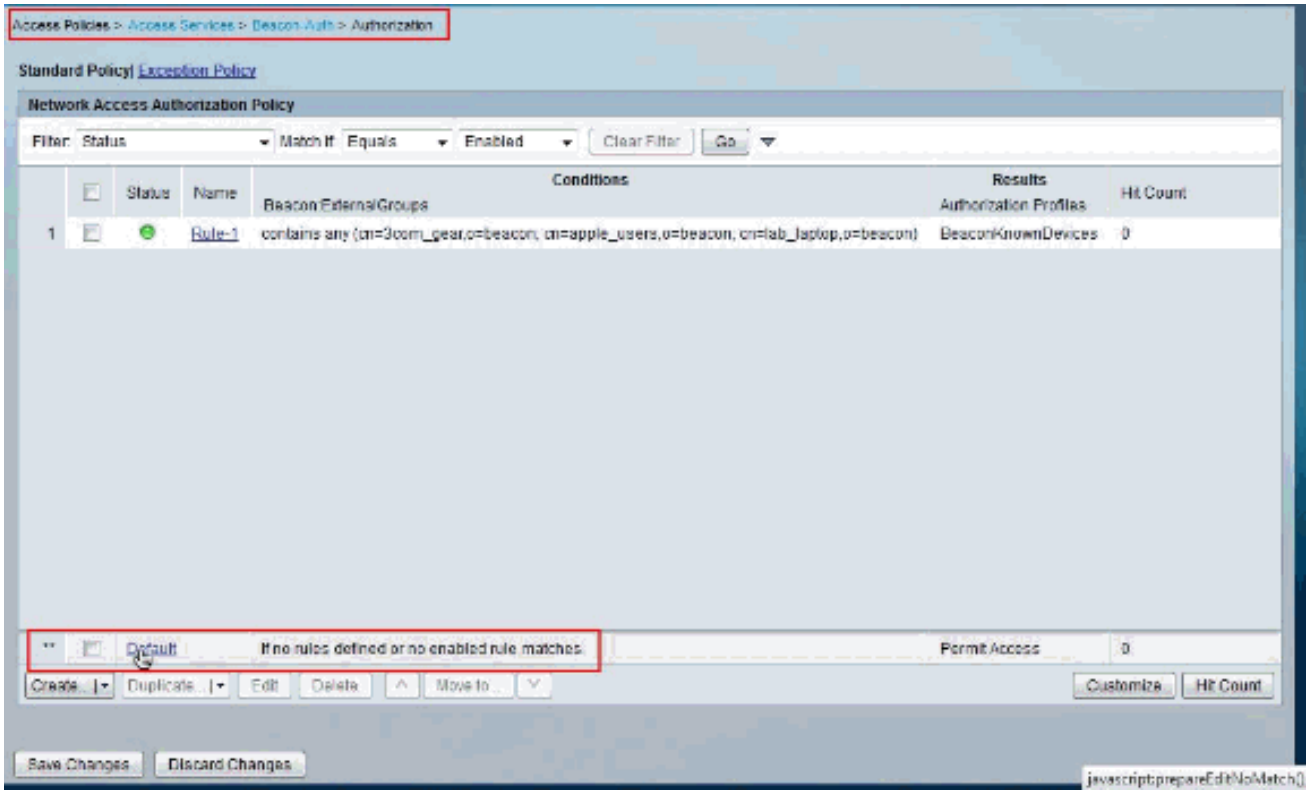
18. El tecleo **crea** para crear una nueva **regla**.



19. Elija 3com_users, los apple_users y el lab_laptop como las condiciones y la autorización perfilan **BeaconKnownDevices** como **resultado**. Entonces, **AUTORIZACIÓN del** tecleo.

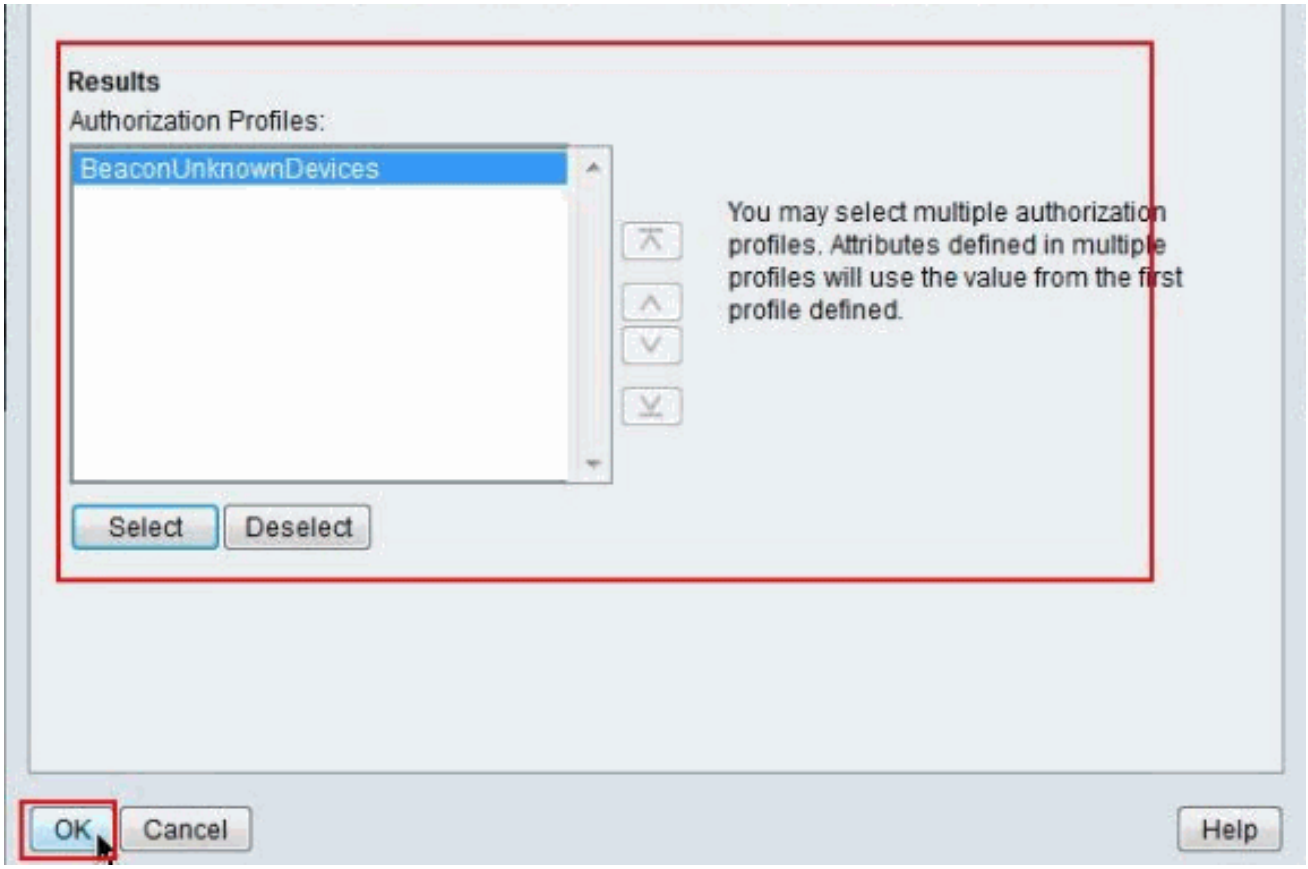


20. **Valor por defecto del** tecleo.

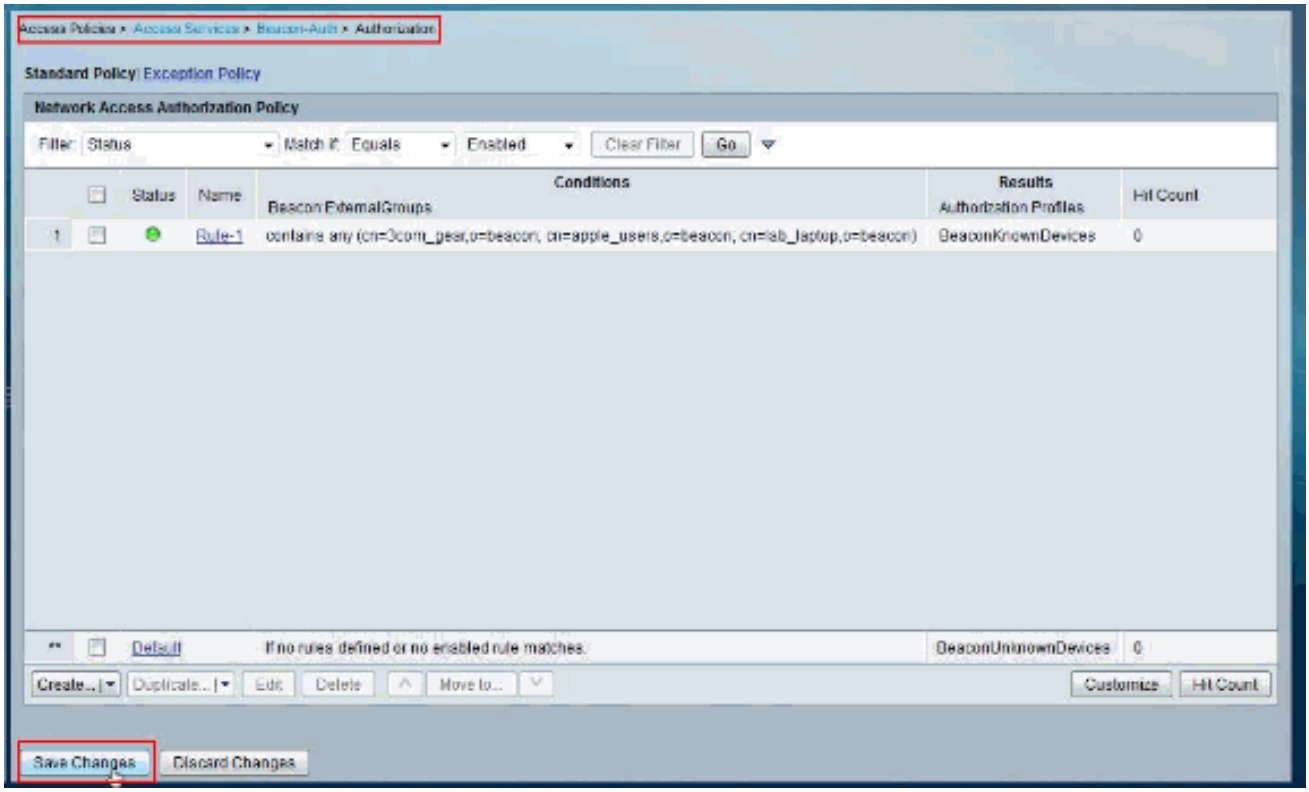


21. Elija 3com_users, los apple_users y el lab_laptop como las condiciones y la autorización

perfilan **BeaconUnKnownDevices** como resultado. Entonces, **AUTORIZACIÓN del** tecleo.



22. **Cambios de la salvaguardia del** tecleo.



Esto completa el procedimiento.

Configuración del switch para puente de la autenticación de MAC

Esta configuración del switch proporciona un ejemplo de configuración para la autenticación del

802.1x con el MAB habilitado, y la reasignación del VLAN dinámico requerida para aplicar los atributos de RADIUS vueltos del ACS.

Switch

```
switch#show running-config ! version 12.2 no service pad
service timestamps debug uptime service timestamps log
datetime service password-encryption service sequence-
numbers ! ! aaa new-model aaa authentication login
default line aaa authentication enable default enable
aaa authentication dot1x default group radius aaa
authorization network default group radius aaa
accounting dot1x default start-stop group radius ! aaa
session-id common switch 1 provision ws-c3750g-24ts ip
subnet-zero ip routing no ip domain-lookup ! ! ! ! ! !
dot1x system-auth-control no file verify auto spanning-
tree mode pvst spanning-tree extend system-id ! vlan
internal allocation policy ascending ! ! interface Port-
channel1 switchport trunk encapsulation dot1q switchport
trunk allowed vlan 5,7,9,10 ! interface Port-channel2
description LAG/trunk to einstein switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk ! interface Port-channel3
description "LAG to Edison" switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk ! interface
GigabitEthernet1/0/1 switchport trunk encapsulation
dot1q switchport trunk allowed vlan 5,7,9,10 channel-
group 1 mode passive ! interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,7,9,10 channel-group 1 mode passive !
interface GigabitEthernet1/0/3 switchport trunk
encapsulation dot1q switchport trunk allowed vlan
5,7,9,10 channel-group 1 mode passive ! interface
GigabitEthernet1/0/4 switchport access vlan 7 switchport
mode access ! interface GigabitEthernet1/0/5 switchport
access vlan 5 switchport mode access spanning-tree
portfast ! interface GigabitEthernet1/0/6 switchport
trunk encapsulation dot1q switchport trunk allowed vlan
5,7,9 switchport mode trunk switchport nonegotiate !
interface GigabitEthernet1/0/7 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/8 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/9 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/10 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/11 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/12 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/13 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/14 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/15 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/16 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/17 switchport access vlan 5
```

```
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/18 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/19 switchport mode access dot1x mac-
auth-bypass dot1x pae authenticator dot1x port-control
auto dot1x timeout quiet-period 10 dot1x timeout reauth-
period 60 dot1x timeout tx-period 10 dot1x timeout supp-
timeout 10 dot1x max-req 1 dot1x reauthentication dot1x
auth-fail max-attempts 1 spanning-tree portfast !
interface GigabitEthernet1/0/20 switchport mode access
dot1x mac-auth-bypass dot1x pae authenticator dot1x
port-control auto dot1x timeout quiet-period 10 dot1x
timeout reauth-period 60 dot1x timeout tx-period 10
dot1x timeout supp-timeout 10 dot1x max-req 1 dot1x
reauthentication dot1x auth-fail max-attempts 1
spanning-tree portfast ! interface GigabitEthernet1/0/21
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/22
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/23
switchport access vlan 10 spanning-tree portfast !
interface GigabitEthernet1/0/24 switchport access vlan
10 spanning-tree portfast ! interface
GigabitEthernet1/0/25 ! interface GigabitEthernet1/0/26
! interface GigabitEthernet1/0/27 ! interface
GigabitEthernet1/0/28 ! interface Vlan1 no ip address
shutdown ! interface Vlan5 ip address 10.1.1.10
255.255.255.0 ! interface Vlan9 ip address 10.9.0.1
255.255.0.0 ! interface Vlan10 ip address 10.10.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! interface Vlan11 ip address 10.11.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! ip default-gateway 10.1.1.1 ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route 10.30.0.0
255.255.0.0 10.10.0.2 ip route 10.40.0.0 255.255.0.0
10.10.0.2 ip http server ip http secure-server ! ! snmp-
server community public RW snmp-server host 10.1.1.191
public radius-server host 10.10.0.100 auth-port 1645
acct-port 1646 key 7 05090A1A245F5E1B0C0612 radius-
server source-ports 1645-1646 ! control-plane ! ! line
con 0 password 7 02020D550C240E351F1B line vty 0 4
password 7 00001A0803790A125C74 line vty 5 15 password 7
00001A0803790A125C74 ! end
```

Verificación

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

Información Relacionada

- Cisco NAC Appliance (Clean Access)
- Cisco Secure Access Control System
- Soporte Técnico y Documentación - Cisco Systems