NAC: интеграция LDAP с ACS 5.x и более поздний пример конфигурации

Содержание

Введение

Этот документ предоставляет пример конфигурации для настройки Маяка и системы управления доступом Cisco Secure Access Control System (ACS) 5.x и позже позволить устройствам Cisco, настроенным для Обхода проверки подлинности MAC (MAB) эффективно и продуктивно аутентифицировать устройства с поддержкой не802.1X в аутентифицируемой сети.

Cisco реализовала опцию под названием MAB на их коммутаторах, а также необходимую поддержку в ACS, для размещения оконечных точек в поддерживающих 802.1X сетях, которые не могут аутентифицироваться через 802.1X. Эта функциональность гарантирует, что оконечные точки, пытающиеся соединиться с поддерживающей 802.1X сетью, которые не оборудованы функциональностью 802.1X, например, не имеют функционального соискателя 802.1X, могут аутентифицироваться перед разрешением, а также принуждать политику использования базовой основы сети всюду по их соединению.

Когда устройство не в состоянии участвовать в протоколе 802.1X, MAB позволяет сети быть настроенной для принятия определенных устройств с использованием их MAC-адреса как основные учетные данные. Для MAB, который будет развернут и использован эффективно, среда должна иметь средство определить устройства в среде, которые не способны к

аутентификации 802.1X и поддерживают актуальную базу данных этих устройств в течение долгого времени как шаги, добавляет, и изменения происходят. Этот список должен заполняться и вестись в Сервере проверки подлинности (ACS) вручную, или через некоторые альтернативные средства, чтобы гарантировать, что устройства, которые аутентифицируются на MAC, завершены и допустимы в любой момент времени.

Профилировщик Оконечной точки Маяка может автоматизировать процесс идентификации неаутентифицирующихся оконечных точек, тех без соискателей 802.1X и обслуживания законности этих оконечных точек в сетях переменного масштаба на Мониторинге функциональных возможностей Профилирования и Поведения Оконечной точки. Через стандартный Интерфейс LDAP система Маяка может служить Внешней базой данных или Каталогом оконечных точек, которые будут аутентифицироваться через MAB. Когда запрос MAB получен от граничной инфраструктуры, ACS может сделать запрос системы Маяка, чтобы определить, нужно ли данную оконечную точку допустить в сетевое на актуальнейшей информации об оконечной точке, известной Маяком. Это предотвращает потребность в настройке вручную.

Для подобной конфигурации с помощью версий ранее, чем ACS 5.x, обратитесь к NAC: Пример конфигурации интеграции LDAP с AcS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутатор Cisco 3750, который выполняет релиз 12.2 программного обеспечения Cisco IOS (25) SEE2
- Cisco Secure ACS 5.x и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

MAB является существенной функциональностью для динамической поддержки устройств, таких как принтеры, IP-телефоны, факсы и другие устройства с поддержкой не802.1X в развертываниях пост802.1X среды. Без возможности MAB порты доступа к сети, которые

предоставляют подключение не802.1X способные оконечные точки, должны быть настроены статически для не попытки аутентификации 802.1X или с помощью других функций, которые предоставляют очень ограниченные опции policy. По очевидным причинам это является по сути не масштабируемым в средах крупных предприятий. С MAB, включенным в сочетании с 802.1X на всех портах доступа, известный не802.1X, способные оконечные точки могут быть перемещены куда угодно в среде и все еще надежно (и надежно) соединяются с сетью. Поскольку устройства, которые допускают в сеть, аутентифицируются, другая политика может быть применена к другим устройствам.

Кроме того, не802.1X способные оконечные точки, которые не известны в среде, такой как портативные ПК, которые принадлежат посетителям или подрядчикам, может быть предоставленным ограниченным доступом к сети через MAB при желании.

Как название предполагает, Обход Проверки подлинности MAC использует MAC-адрес оконечной точки как основные учетные данные. С MAB, включенным на порте доступа, если оконечная точка соединяется и не в состоянии отвечать на аутентификационное препятствие 802.1X, порт возвращается к режиму MAB. Коммутатор, который делает попытку MAB оконечной точки, делает стандартный Запрос RADIUS к ACS с MAC станции. Это пытается соединиться с сетью и запрашивает аутентификацию оконечной точки от ACS перед разрешением оконечной точки к сети.

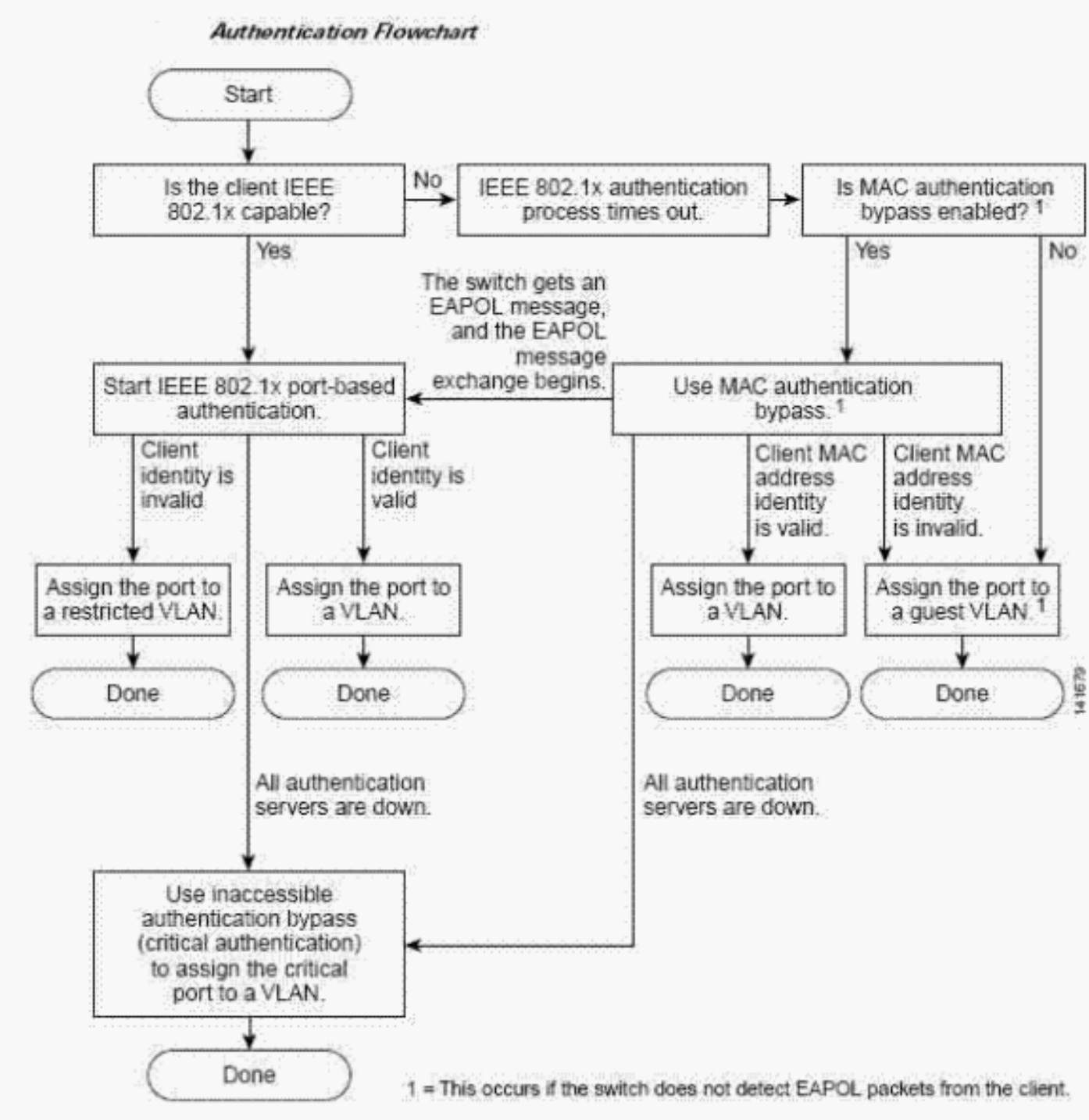
!--- конфигурацию

Схема блок-схемы

Эта блок-схема иллюстрирует, как MAB используется в сочетании с аутентификацией 802.1X на граничной инфраструктуре Cisco, поскольку новые оконечные точки пытаются соединиться с сетью.

Этот документ использует этот поток операций Блок-схемы:

Рисунок 1: Опознавательный поток



ACS может быть настроен для использования или его собственной внутренней базы данных или внешнего Сервера LDAP для аутентификации запросов пользователя MAC-адреса. Система Профилировщика Оконечной точки Маяка является полностью поддерживающей LDAP по умолчанию и может быть использована ACS для аутентификации запросов пользователя MAC-адреса через стандартную функциональность LDAP. Поскольку Маяк автоматизирует обоих обнаружение, а также Профилирование всех оконечных точек в сети, ACS может сделать запрос Маяка через LDAP, чтобы определить, нужно ли MAC допустить в сеть, и которые группируются, оконечная точка должна быть сопоставлена. Это значительно автоматизирует и улучшает функцию MAB, особенно в средах крупных предприятий.

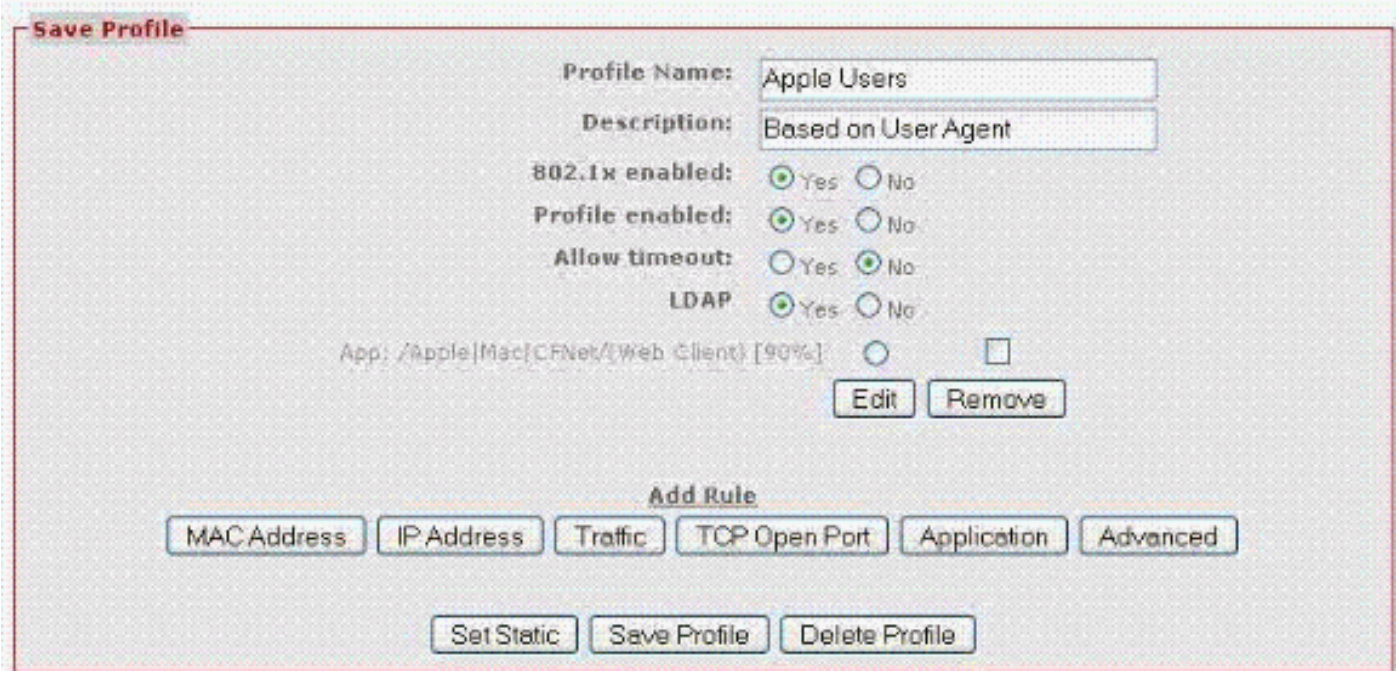
Через Поведенческий Мониторинг функциональных возможностей, предоставленный Маяком, устройства, которые, как наблюдают, ведут себя противоречиво с Профилями, включенными для MAB, переходятся из 4 поддерживающих LDAP профилей и впоследствии отказывают следующую обычную попытку повторной проверки подлинности.

Конфигурация системы профилировщика оконечной точки маяка для MAB

Конфигурация системы Маяка для интеграции с ACS в целях поддержки MAB является прямой, поскольку функциональность LDAP добавлена по умолчанию. Основная задача конфигурации должна определить Профили, которые содержат оконечные точки, которые желаемы, чтобы аутентифицироваться через MAB в среде, и затем включить те Профили для LDAP. Как правило, Профили Маяка, которые содержат устройства, принадлежавшие организации, должны быть предоставленным доступом к сети, когда замечено на порту, все же, как известно, неспособны аутентифицироваться через 802.1X. Как правило, это Профили, которые содержат принтеры, IP-телефоны или управляемый UPSs как общие примеры.

Если бы принтеры, представленные Маяком, были размещены в профиль под названием *Принтеры* и IP-телефоны в профиле под названием *IP-телефоны*, например, то эти профили должны быть включены для LDAP, таким образом, что оконечные точки разместили в те Профили результат в успешной аутентификации как известный IP-телефон и принтеры в среде через MAB. При включении профиля для LDAP это требует выбора кнопки с зависимой фиксацией LDAP в Настройке профиля Оконечной точки, как показано в данном примере:

Рис. 2: Включите профиль для LDAP



Когда проверка подлинности MAC ACS - прокси к Маяку через LDAP, запрос состоит из двух запросов sub. Оба из них должны возвратить допустимый, непустой результат. Первый запрос к Маяку - известен ли MAC Маяку, например, если это было обнаружено и добавлено к базе данных Маяка. Если оконечная точка должна все же быть обнаружена Маяком, оконечная точка, как полагают, неизвестна.

Второй запрос не необходим в случае оконечных точек, которые Маяк не обнаружил и не находится в его базе данных. Если оконечная точка была обнаружена и находится в базе данных Маяка, следующий запрос должен определить текущий Профиль оконечной точки. Если оконечная точка должна все же быть представлена или в настоящее время находится в профиле не 5, включил для LDAP, неизвестный результат возвращен к ACS и аутентификации оконечной точки сбоями Маяка. Это зависит от того, как ACS настроен, что это может привести к устройству с отказом доступа к сети в целом или быть дано Политику,

которая является соответствующей гостевым устройствам или неизвестному.

Только в случае, где MAC является оконечной точкой, которую Маяк обнаружил и разместил в поддерживающий LDAP Профиль, ответ состоит в том, что оконечная точка известна и Представлена Маяком, который будет возвращен к ACS. Самое главное для этих оконечных точек Маяк предоставляет текущее Имя профиля. Это позволяет ACS сопоставить известные оконечные точки с Cisco SecureAccess Groups. Это включает гранулированное сделанное определение Политики, столь же гранулированное как отдельная политика для каждого Маяка поддерживающий LDAP Профиль, при желании.

Конфигурация AcS для MAB и использования маяка как внешняя база данных пользователей

Конфигурация ACS для MAB и использования Маяка как Внешняя база данных пользователей требует трех следующих действий. Заказ, проиллюстрированный в этом документе, придерживается потока операций, который эффективен, когда это выполняет конфигурацию MAB полностью и может варьироваться для систем, которые были в действии с другими режимами аутентификации, уже настроенными.

Когда вы делаете попытку MAB для конкретной оконечной точки, которая пытается соединиться с сетью, ACS делает запрос Маяка на LDAP, чтобы определить, обнаружил ли Маяк MAC, и во что Маяк Профиля в настоящее время размещал MAC-адрес, как описано ранее в документе.

В этом документе созданы два отдельных профиля:

- BeaconKnownDevices — для оконечных точек, обнаруженных и Представленных Маяком
- BeaconUnknownDevices — для устройств, которые не в настоящее время известны Маяком

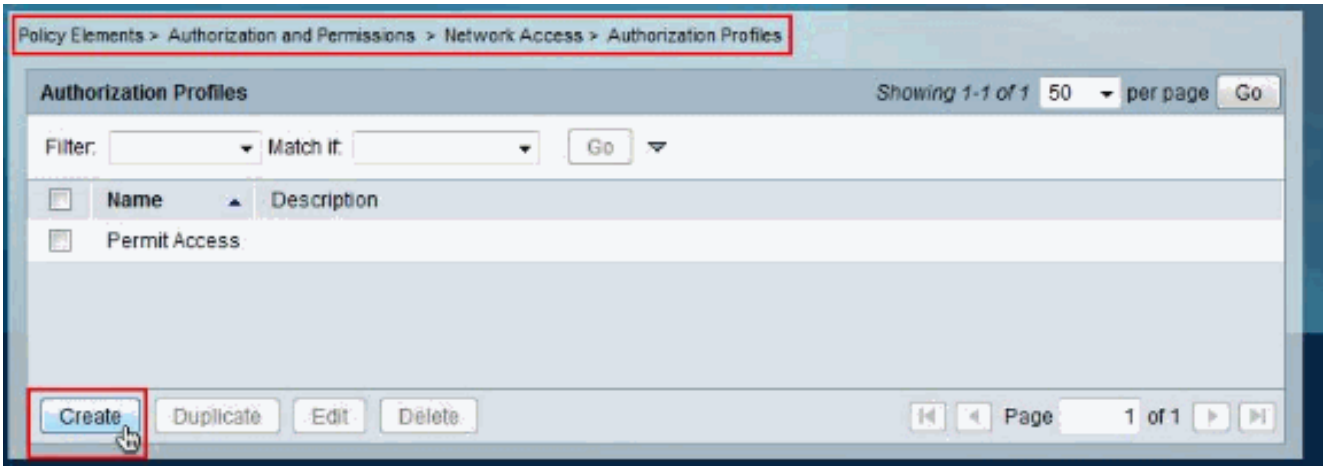
Или Маяк не обнаружил MAC или в настоящее время не представлял его к поддерживающему LDAP профилю. Профиль BeaconKnownDevices поместит оконечные точки в VLAN 10, и профиль BeaconUnkownDevices поместит оконечные точки в VLAN 7.

Позже в этом документе, Соединение LDAP Профилировщику Оконечной точки Маяка от ACS создано, и группы выбраны от Профилировщика Оконечной точки Маяка, на основе которого оконечные точки рассмотрят как устройства BeaconKnown и назначат профиль BeaconKnownDevices (который поместит их в VLAN 10). Всем неизвестным устройствам, что или Маяк не обнаружил MAC или в настоящее время не представлял его в поддерживающий LDAP профиль, назначат профиль BeaconUnkownDevices (который поместит их в VLAN 7).

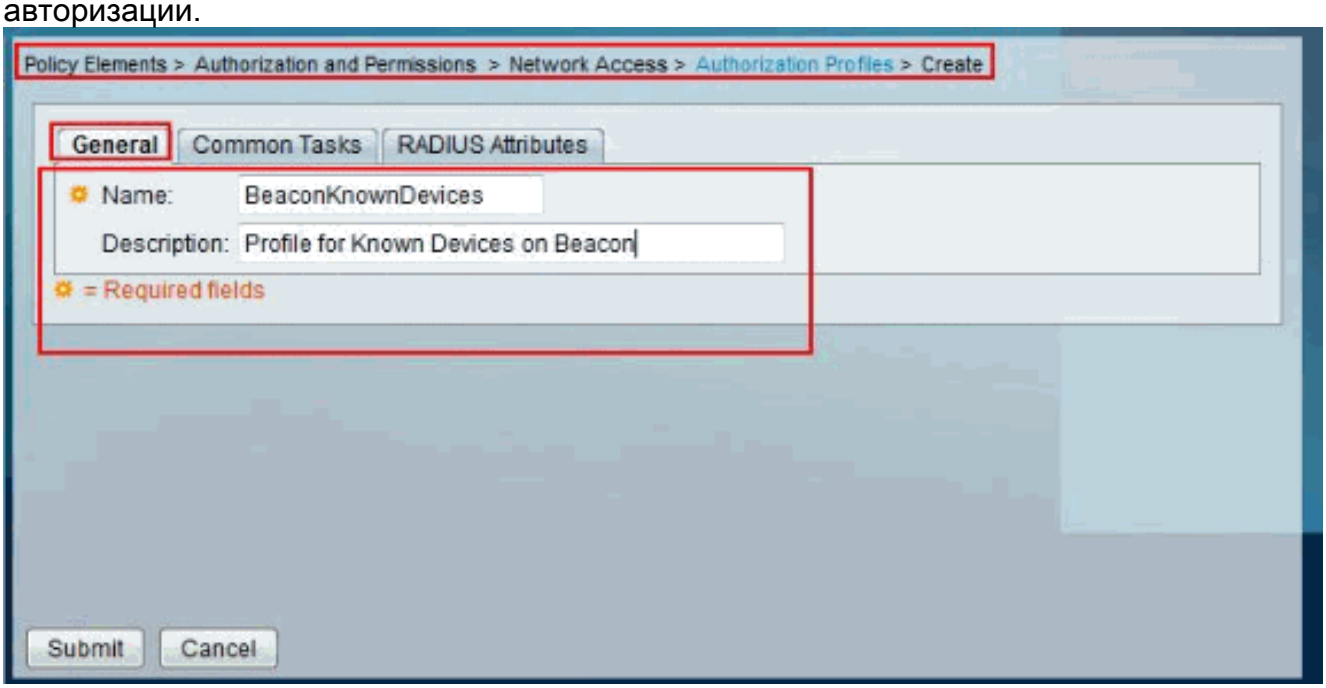
Создайте профиль авторизации

Выполните эти шаги для создания Профиля Авторизации:

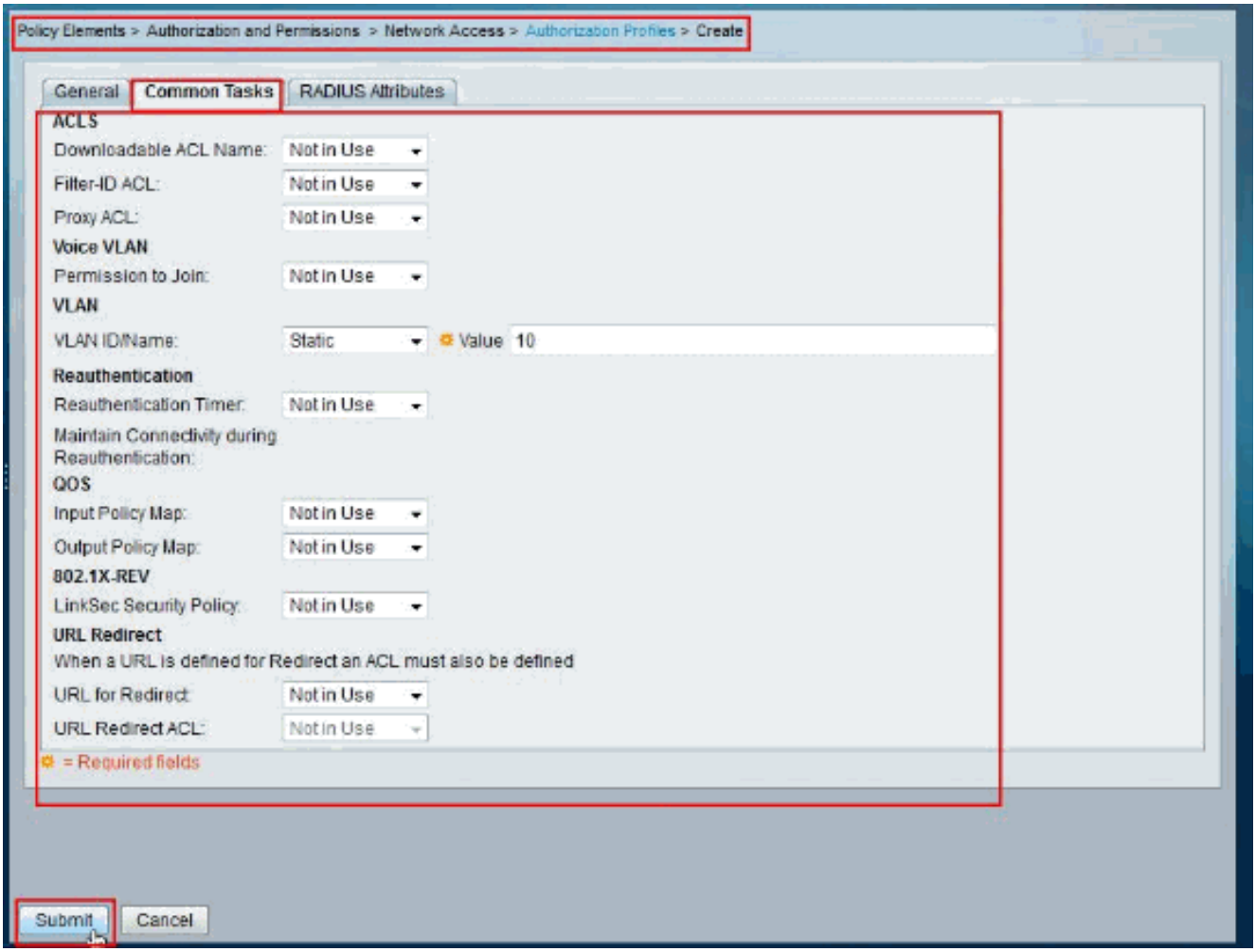
1. Выберите **Policy Elements> Authorization и Permissions> Network Access> Authorization Profiles** и нажмите **Create** для создания нового профиля авторизации.



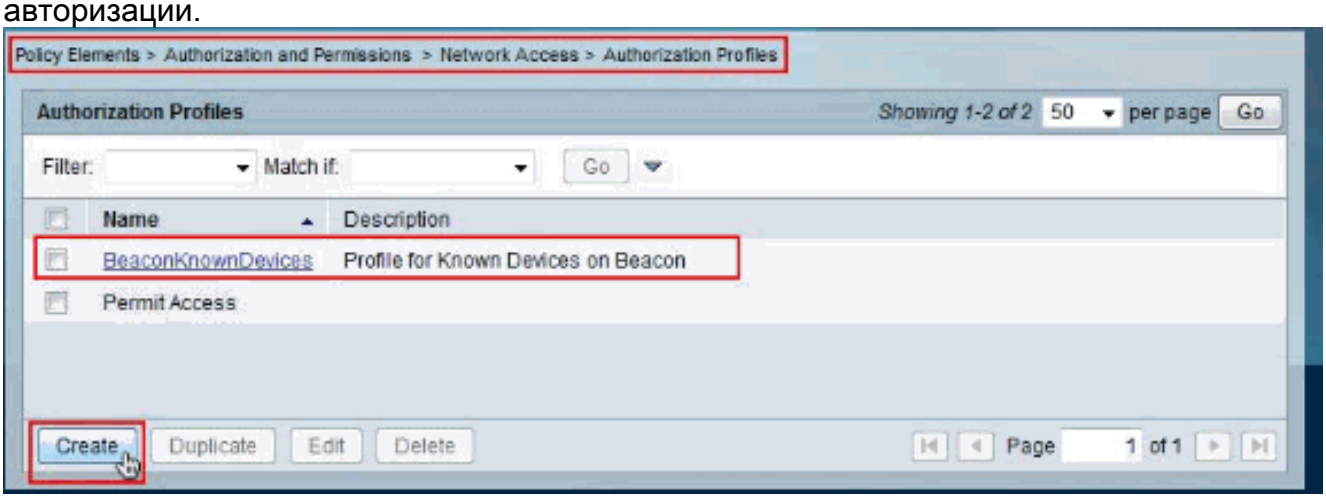
2. Предоставьте **Название** нового профиля авторизации.



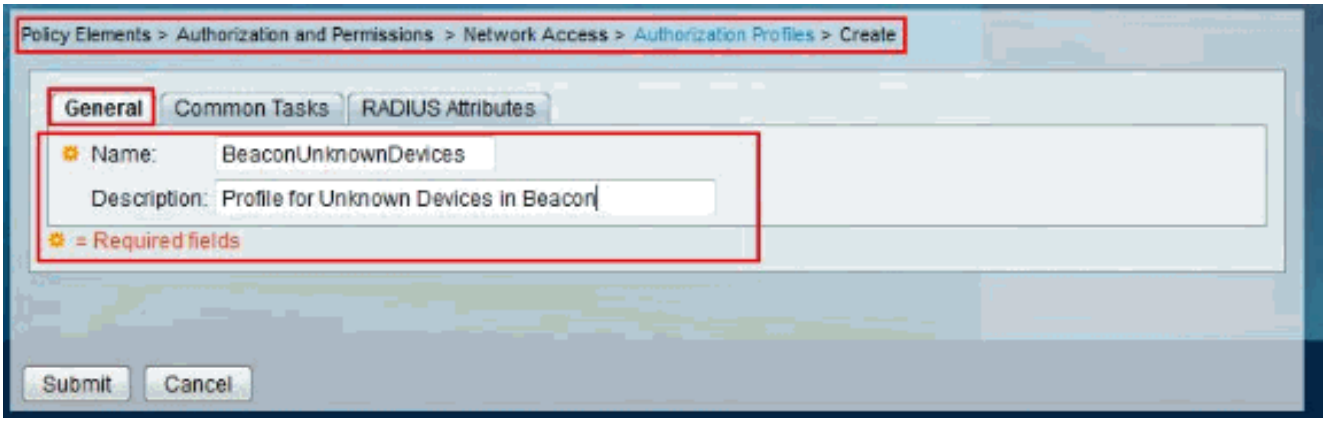
3. В **Common Tasks** вкладка установила **VLAN в Статический** со **Значением** как **10**. **Затем щелкните Submit (Отправить).**



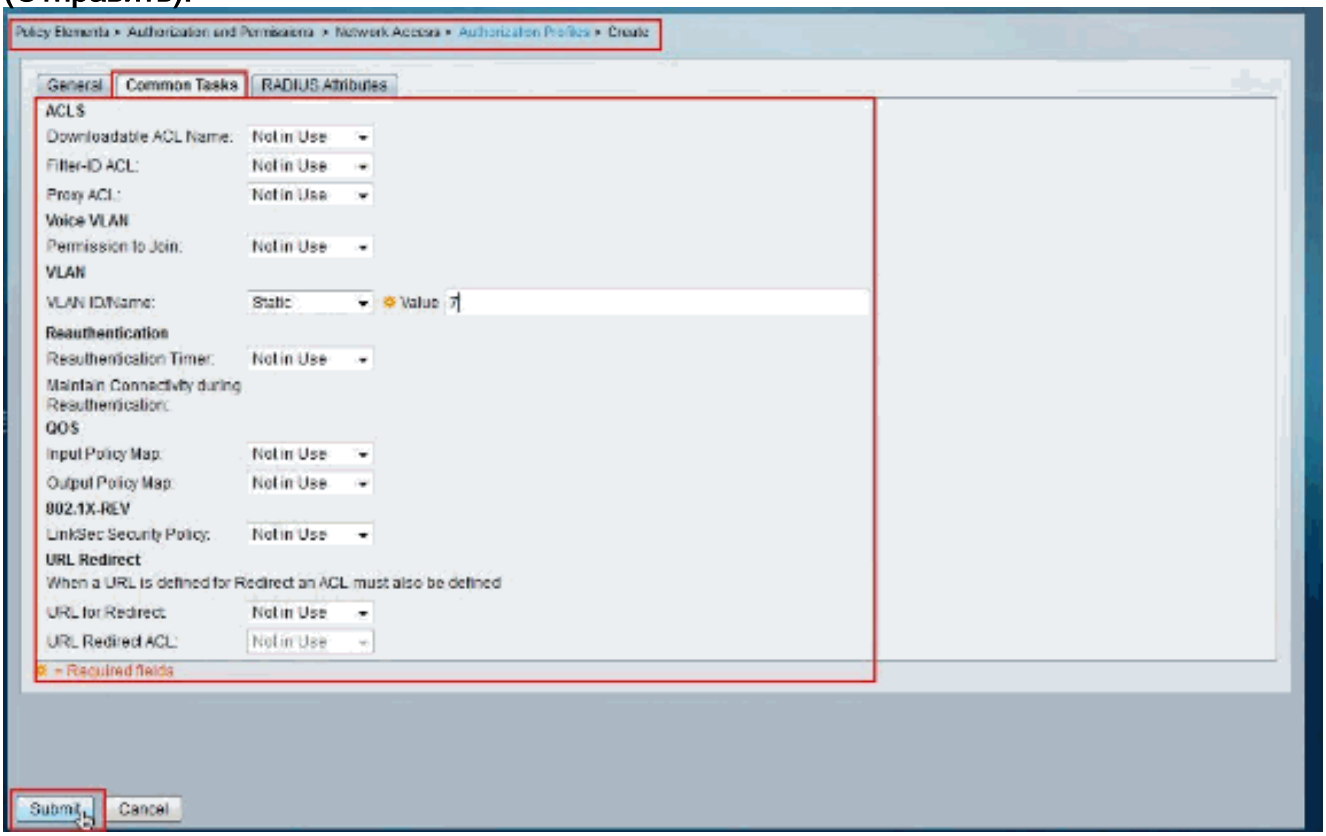
4. Выберите **Policy Elements> Authorization и Permissions> Network Access> Authorization Profiles** и нажмите **Create** для создания нового профиля авторизации.



5. Предоставьте **Название** нового профиля авторизации.



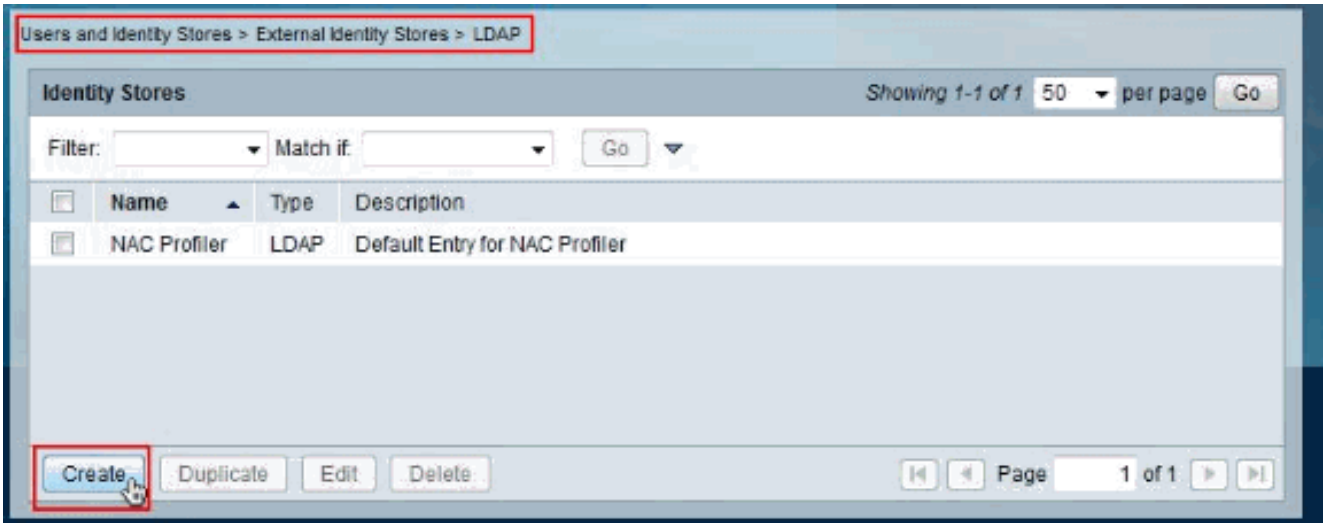
6. В **Common Tasks** вкладка установила **VLAN** в **Статический** со **Значением** как **7**. **Затем щелкните Submit**
(Отправить).



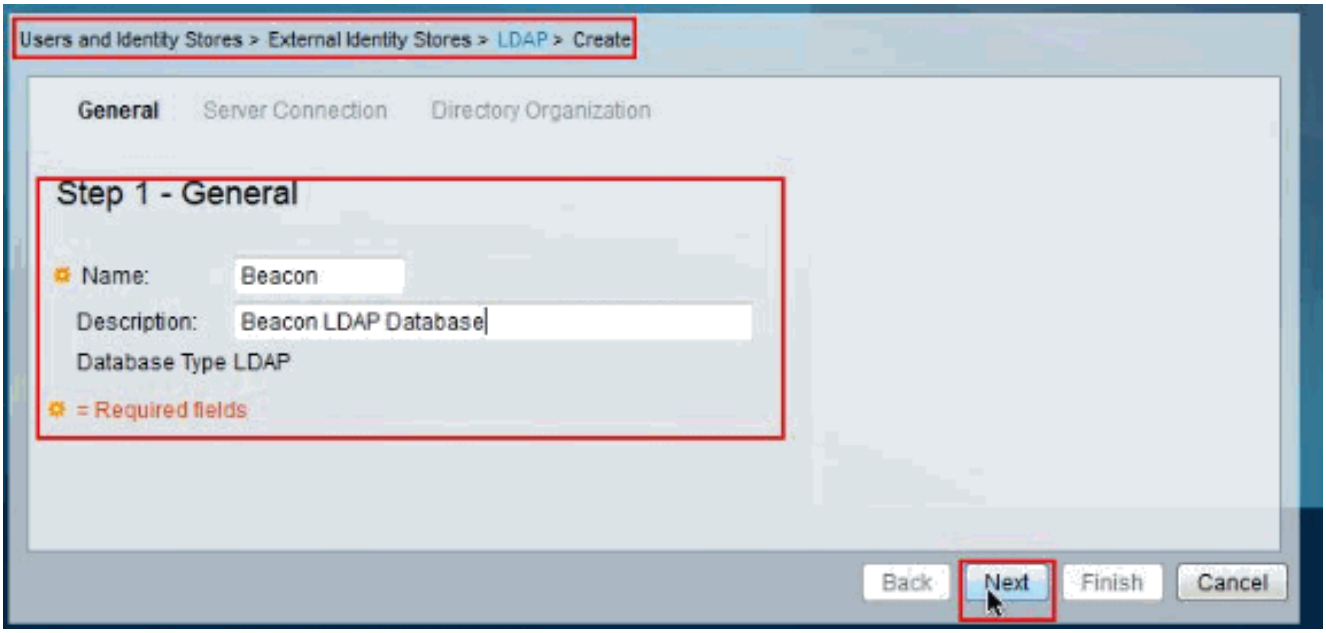
Создайте соединение базы данных LDAP

Выполните шаги для создания соединения базы данных LDAP:

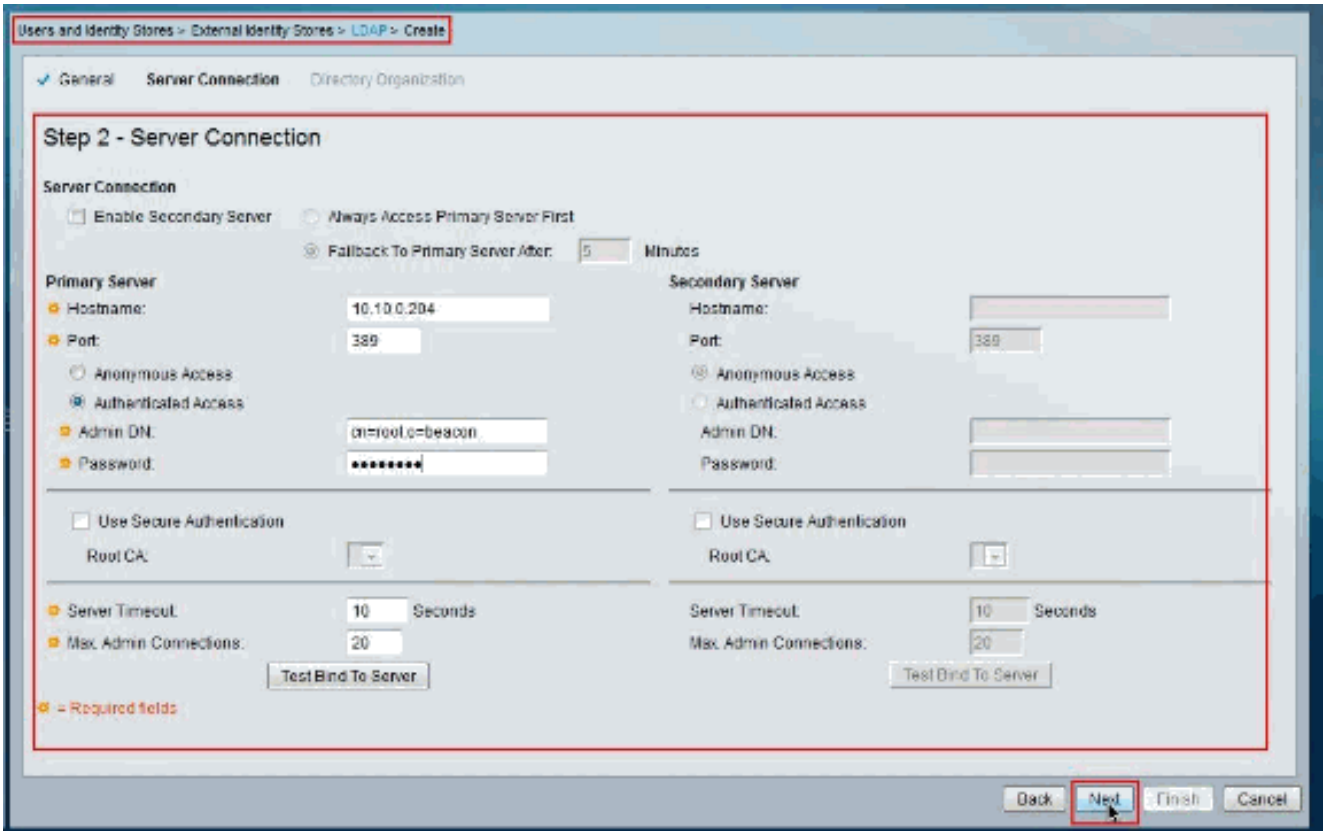
1. Выберите **Users и Identity Stores> External Identity Stores> LDAP** и нажмите **Create** для создания нового соединения базы данных
LDAP.



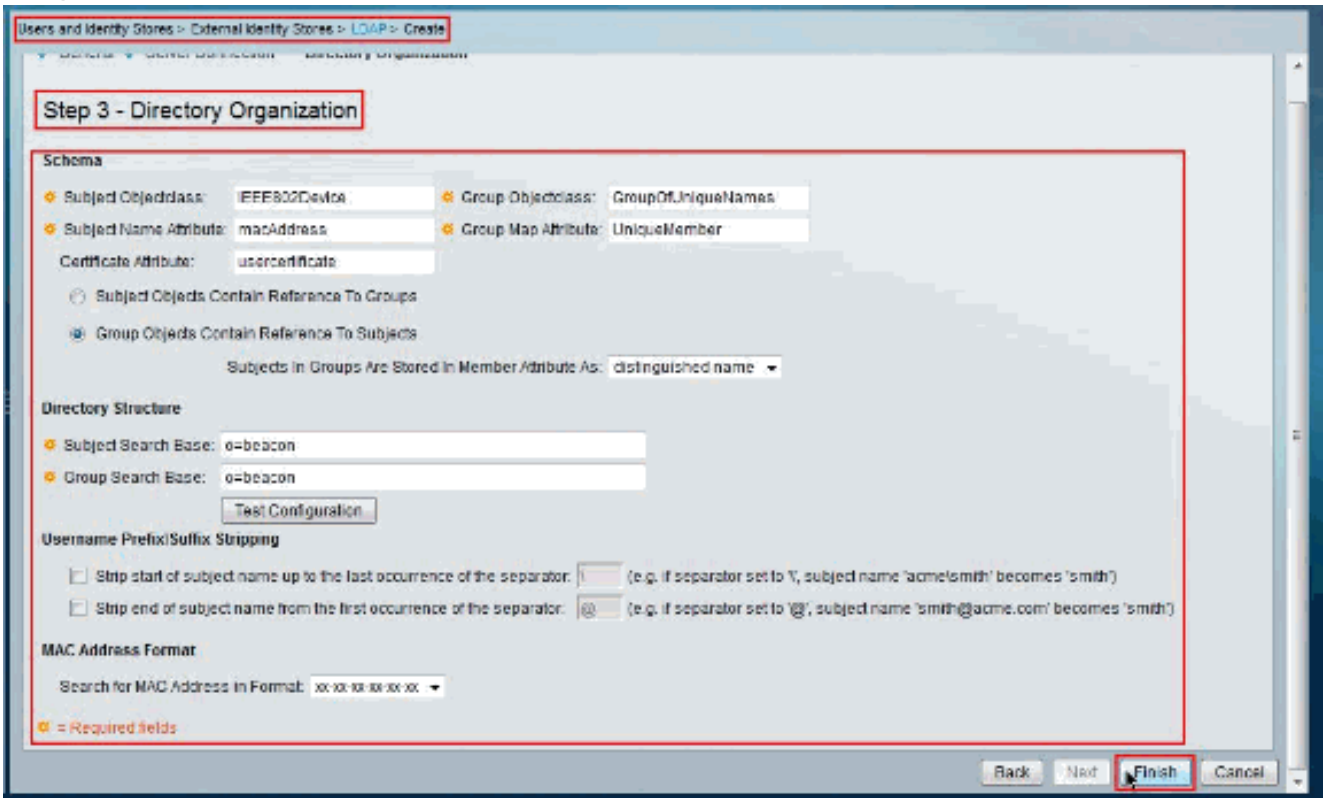
2. Предоставьте **Название** для нового **соединения базы данных LDAP** и нажмите **Next**.



3. В **Server Connection** входит вкладка**, ИМЯ ХОСТА/IP-АДРЕС LDAP МАЯКА Разъединяют, портируют, DN Admin, Пароль** (GBSbeacon в данном примере). **Нажмите кнопку Next.**

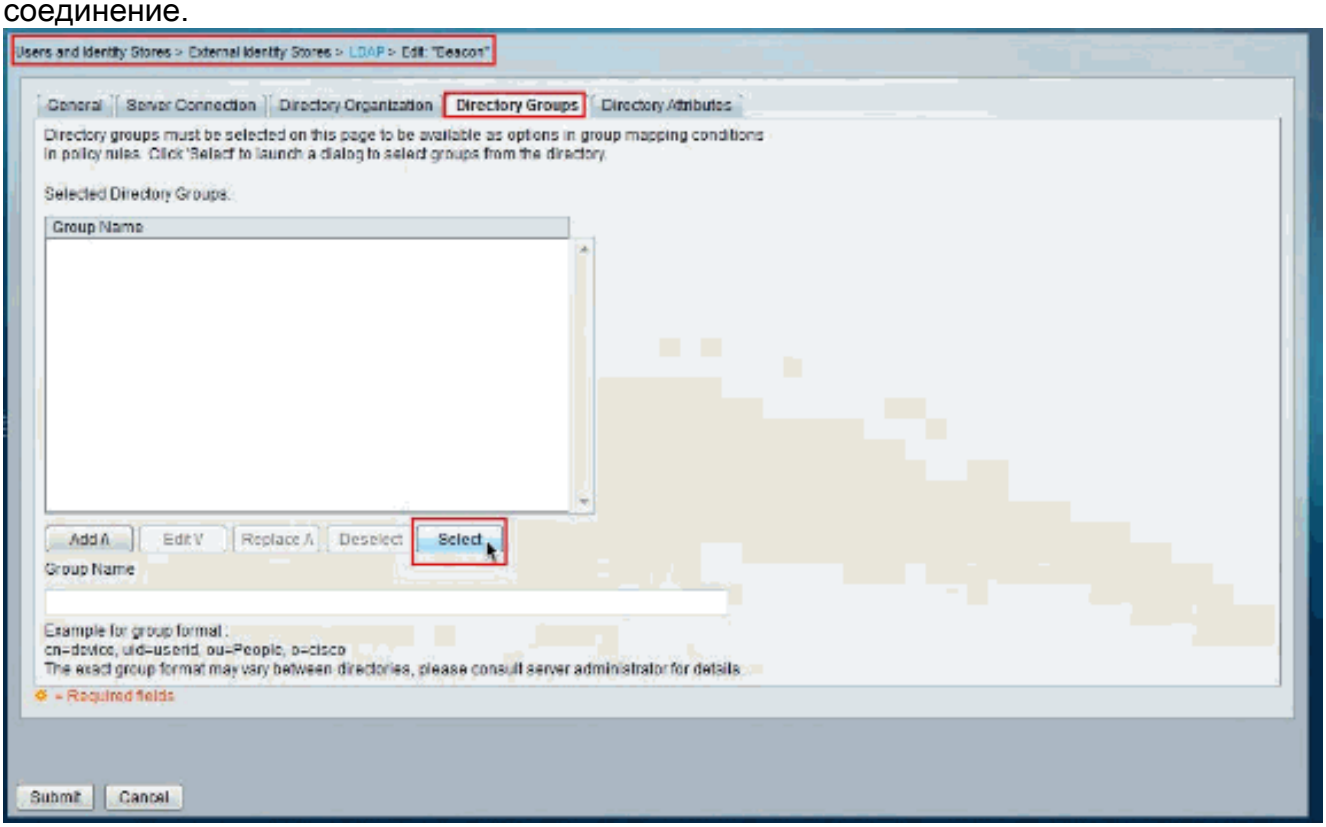


4. В **Directory Organization** вкладка вводят необходимую информацию. **После этого нажмите кнопку**
Finish.

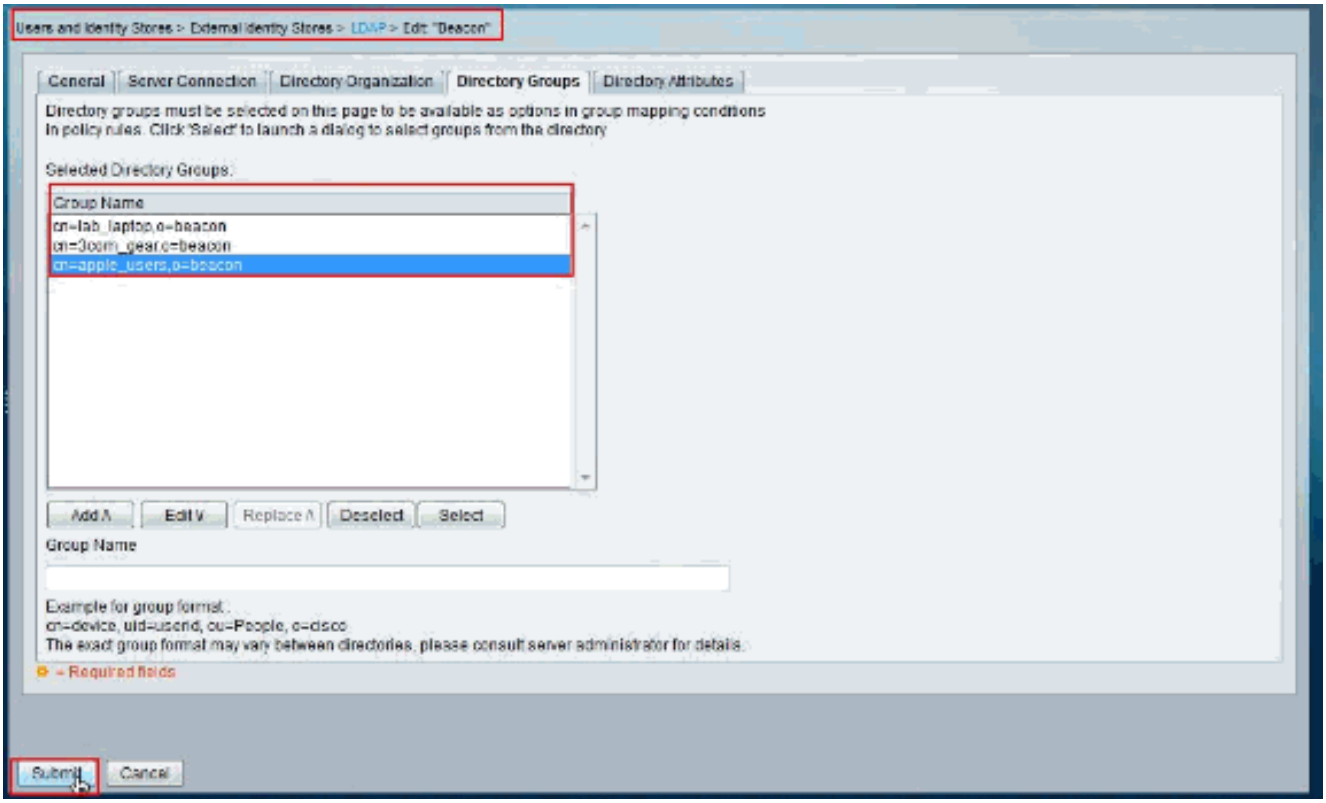


5. Нажмите недавно созданное **Соединение LDAP** (Маяк в данном примере).

6. Выберите вкладку **Directory Groups** и нажмите **Select**.
соединение.



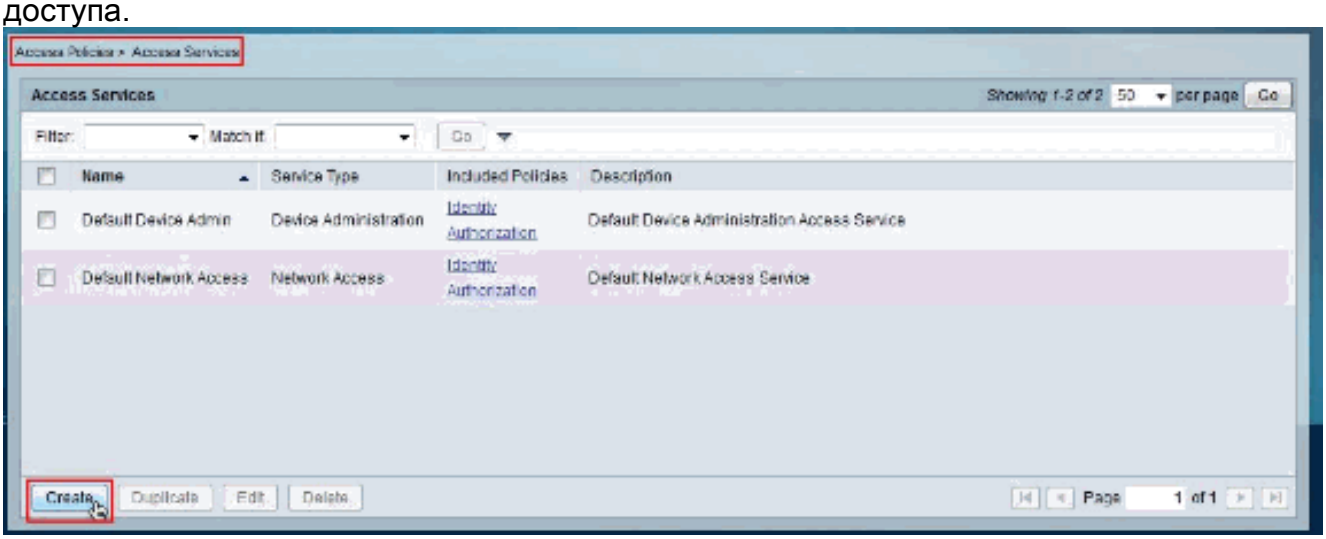
7. Выберите все группы в следующем экране, который вы хотите сопоставить с **BeaconKnownDevices**.
8. В данном примере выбраны эти группы, а именно, lab_laptop, 3com_gear и apple_users. **Затем щелкните Submit**
(Отправить).



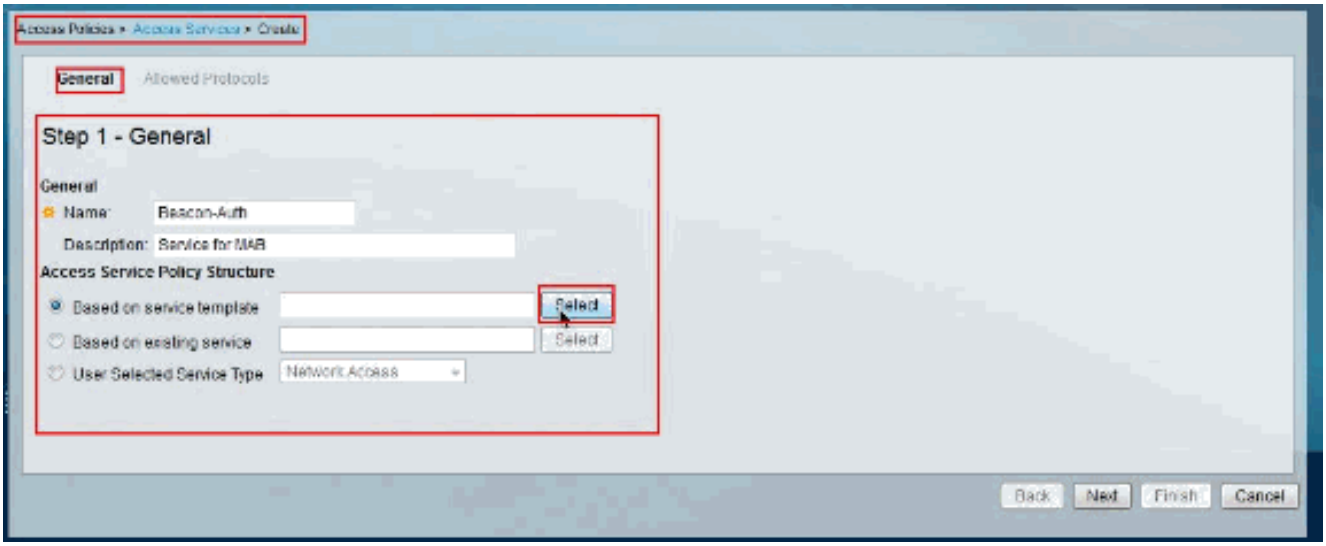
Настройте службы доступа

Выполните эти шаги для настройки Служб доступа:

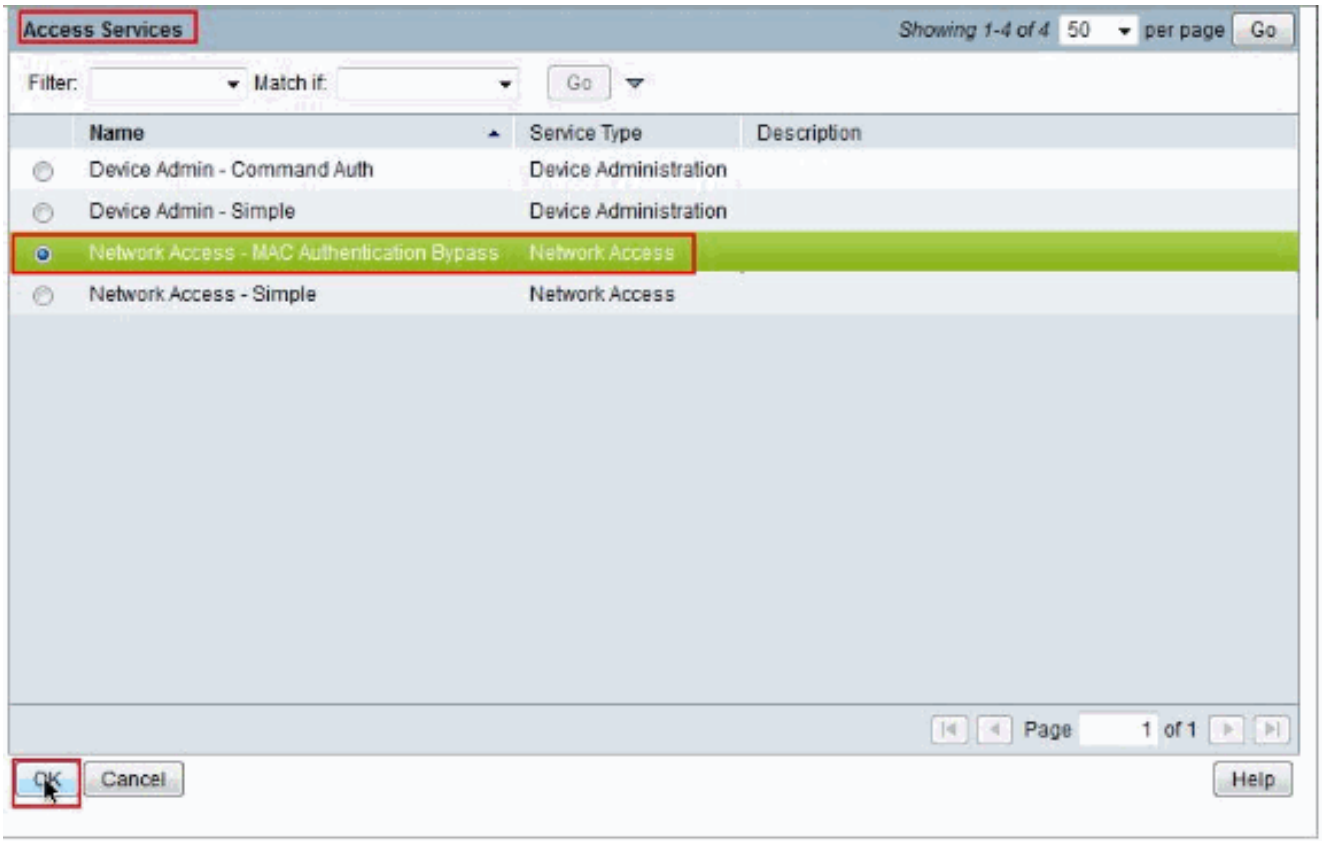
1. Выберите **Access Policies> Access Services** и нажмите **Create** для создания новой Службы
доступа.



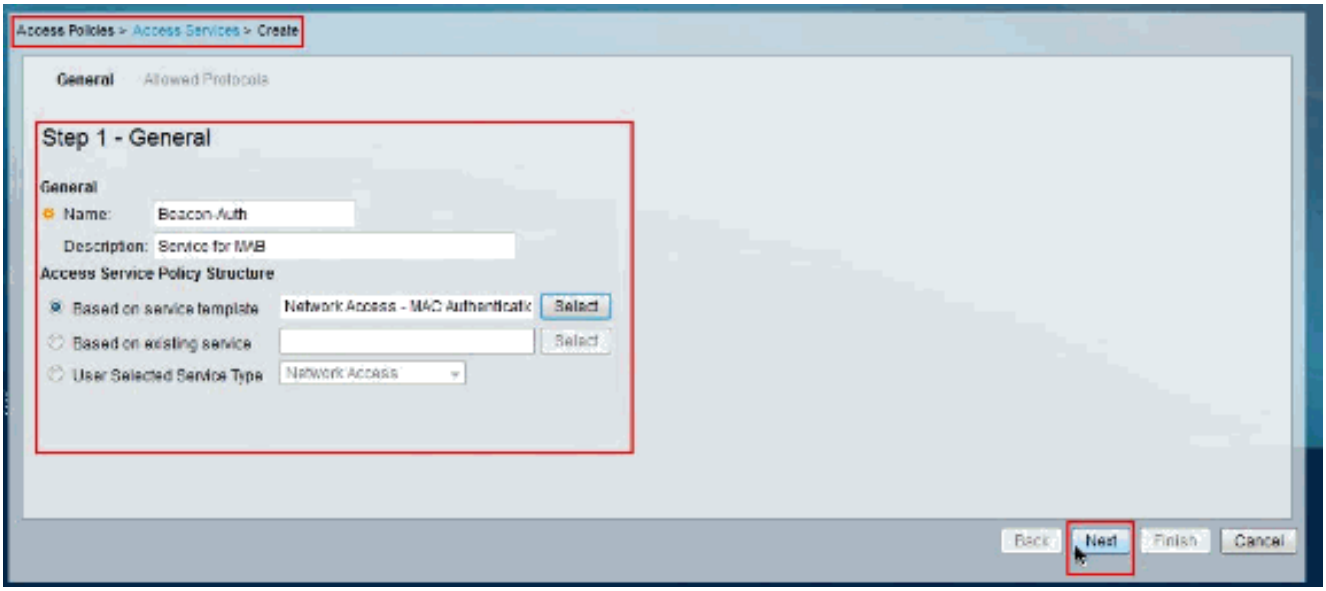
2. Во **Вкладке Общие** предоставляют **Название** нового сервиса, затем нажимают **шаблон Select next to Based on**
Service.



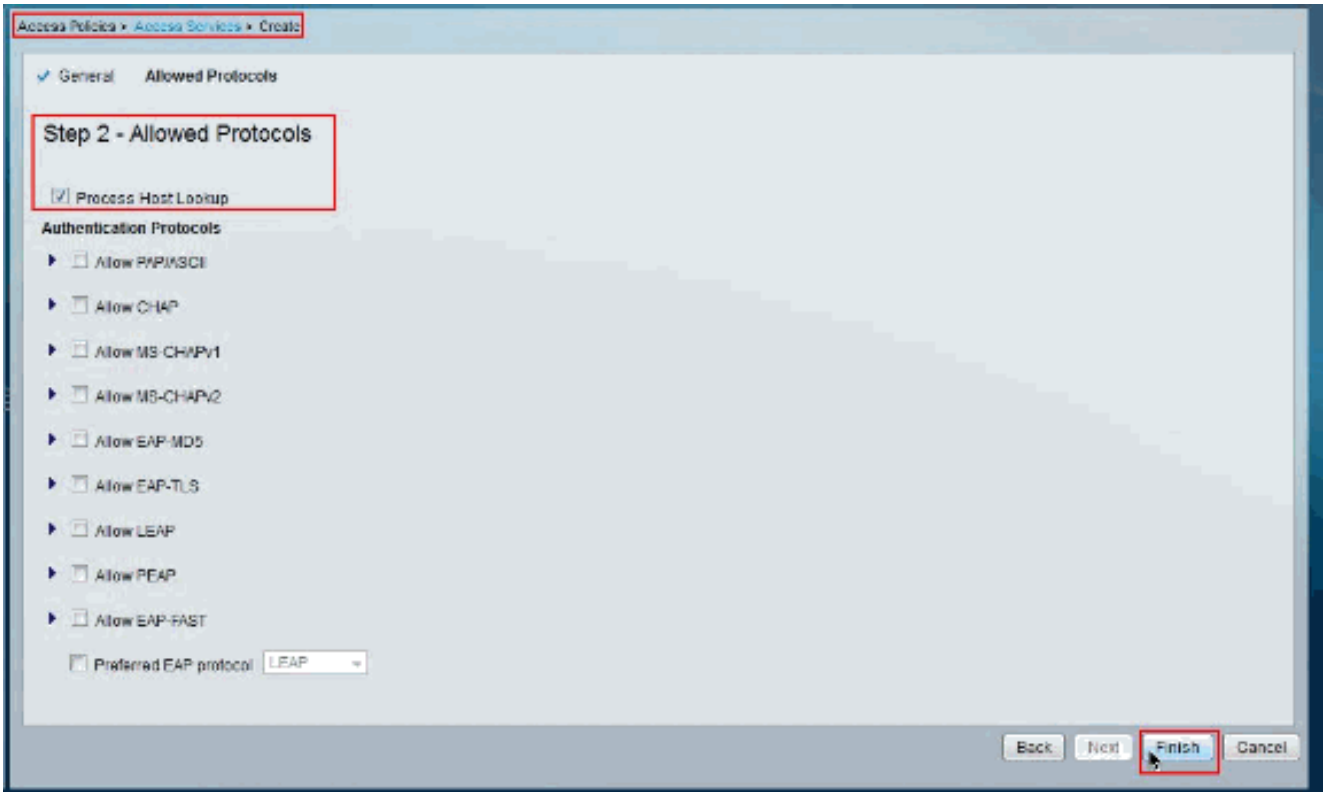
3. Выберите **Network Access - Обход Проверки подлинности MAC** и нажмите **OK**.



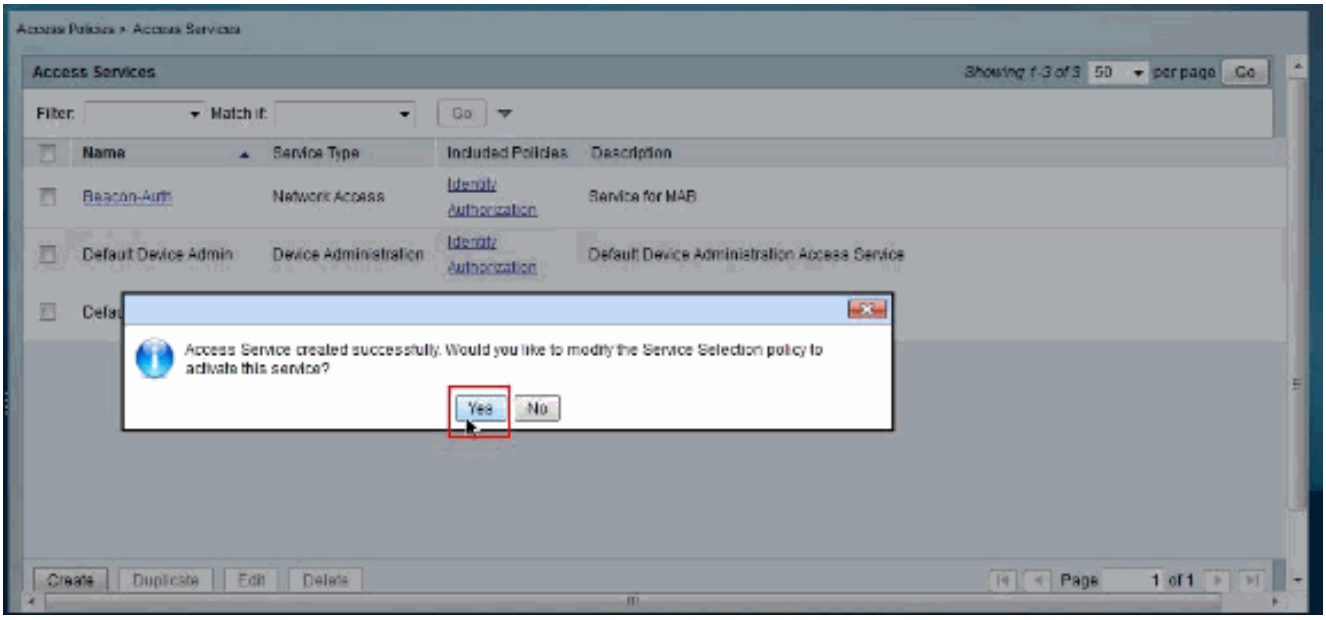
4. **Нажмите кнопку Next.**



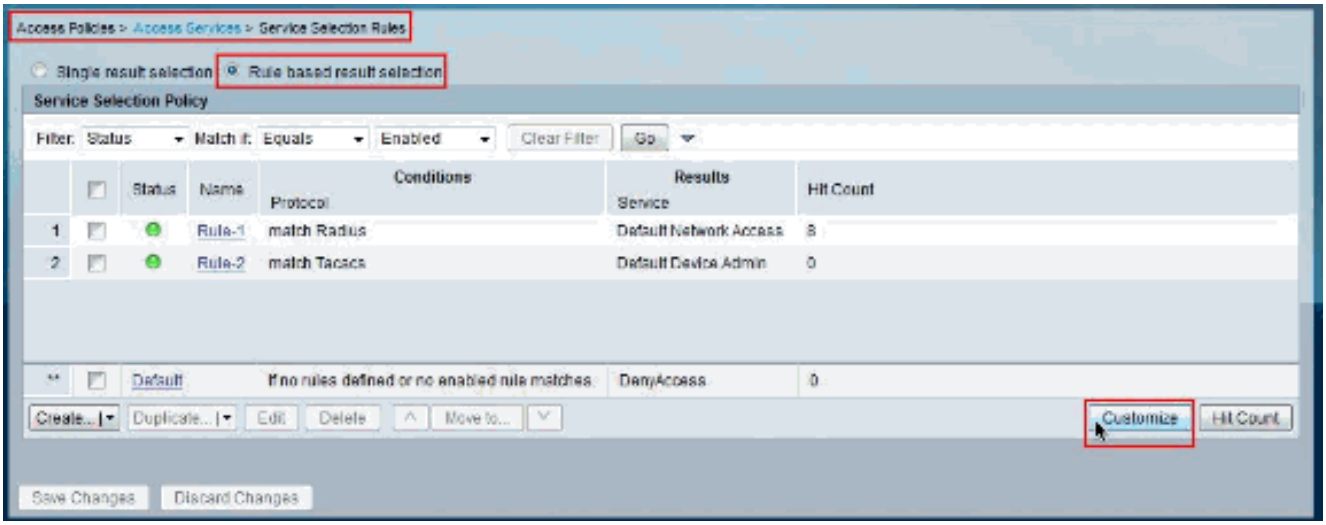
5. Нажмите кнопку Finish.



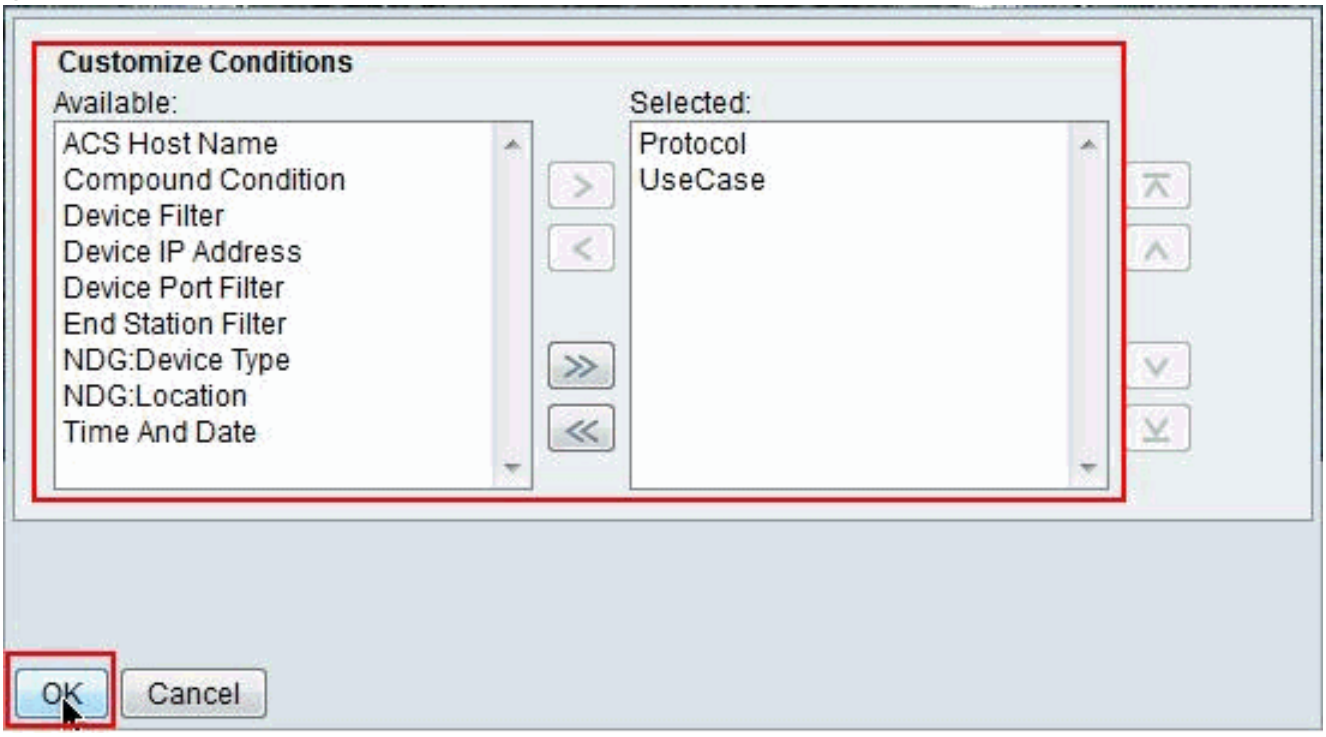
6. Нажмите кнопку YES.



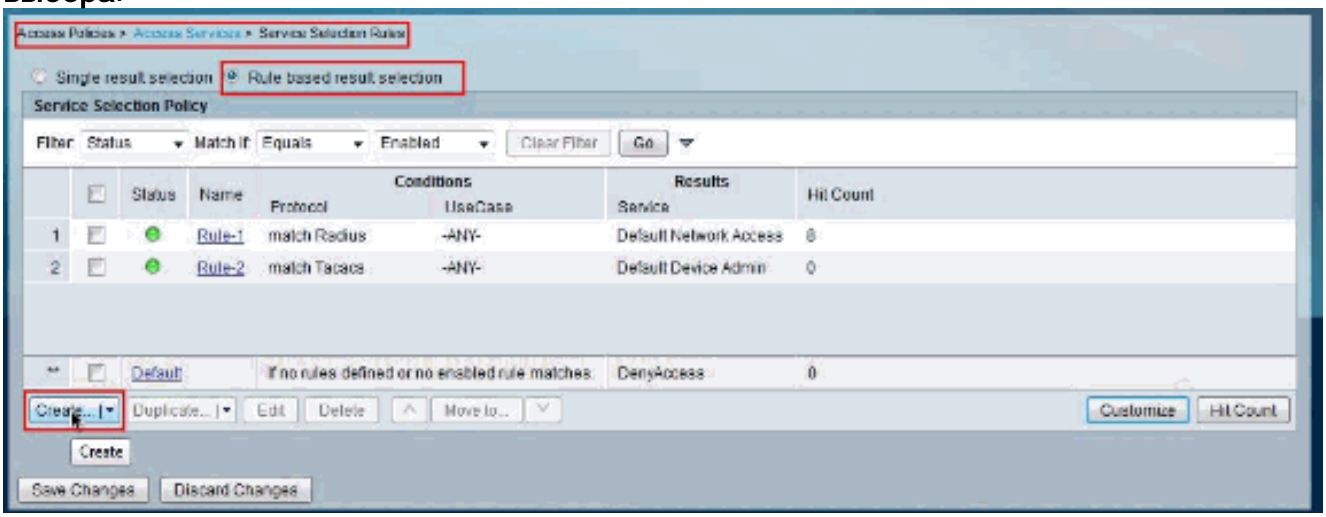
7. Нажмите **Customize**.



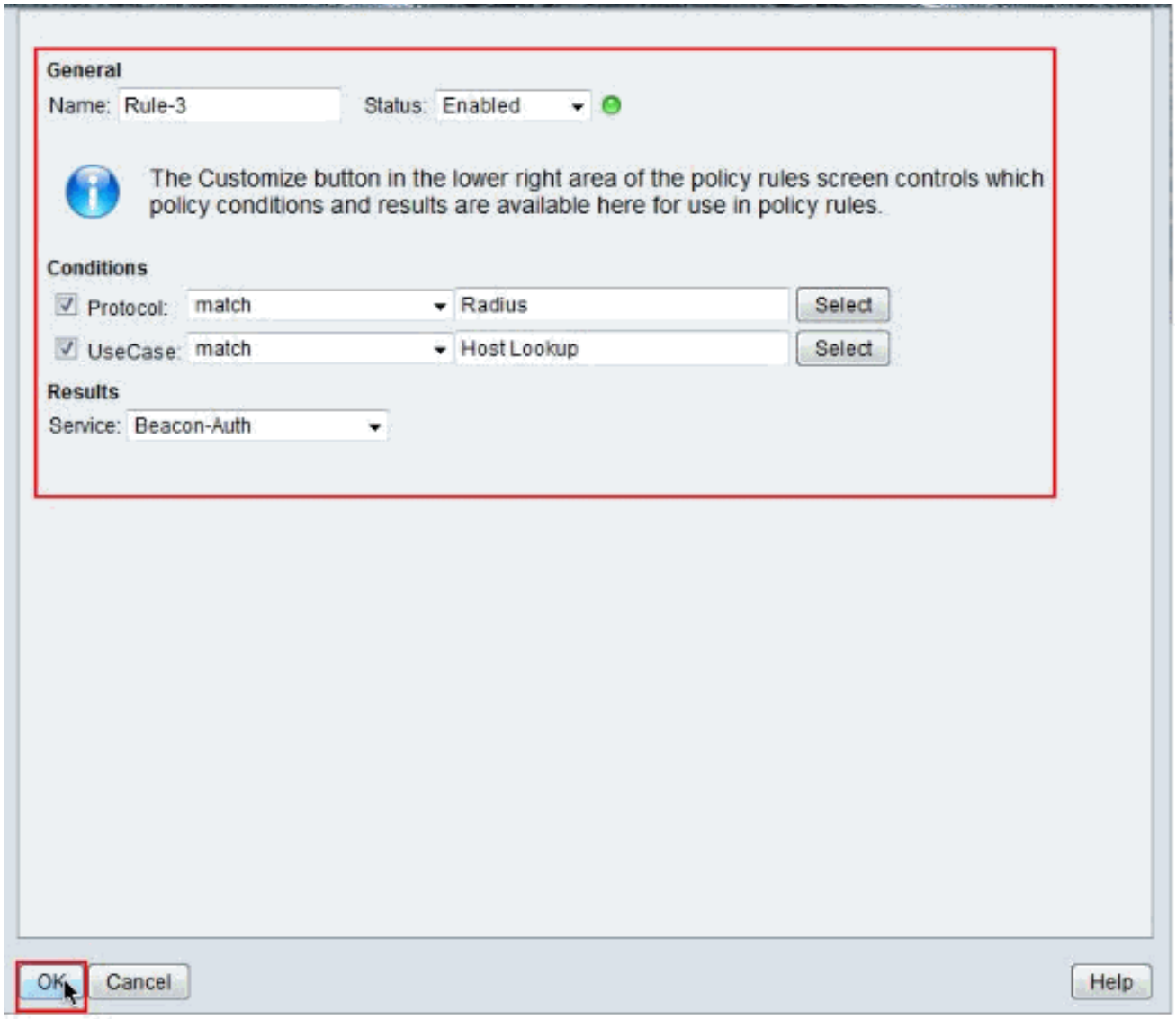
8. Переместите **UseCase** от **Доступного** до **Выбранного** и нажмите **OK**.



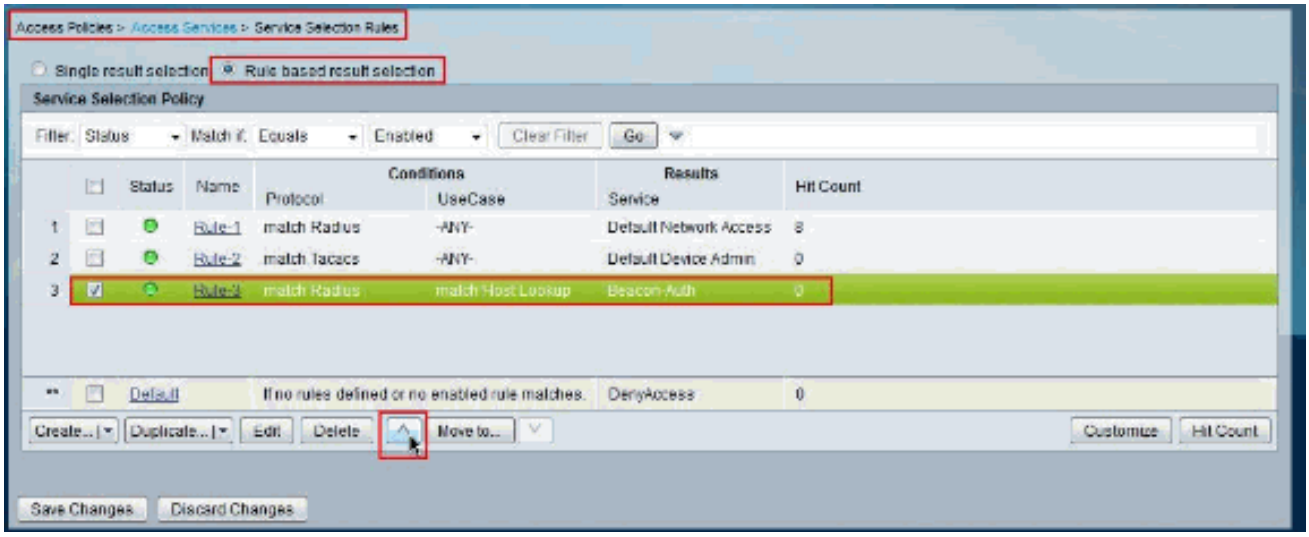
9. Нажмите **Create** для создания нового **Сервисного Правила выбора**.



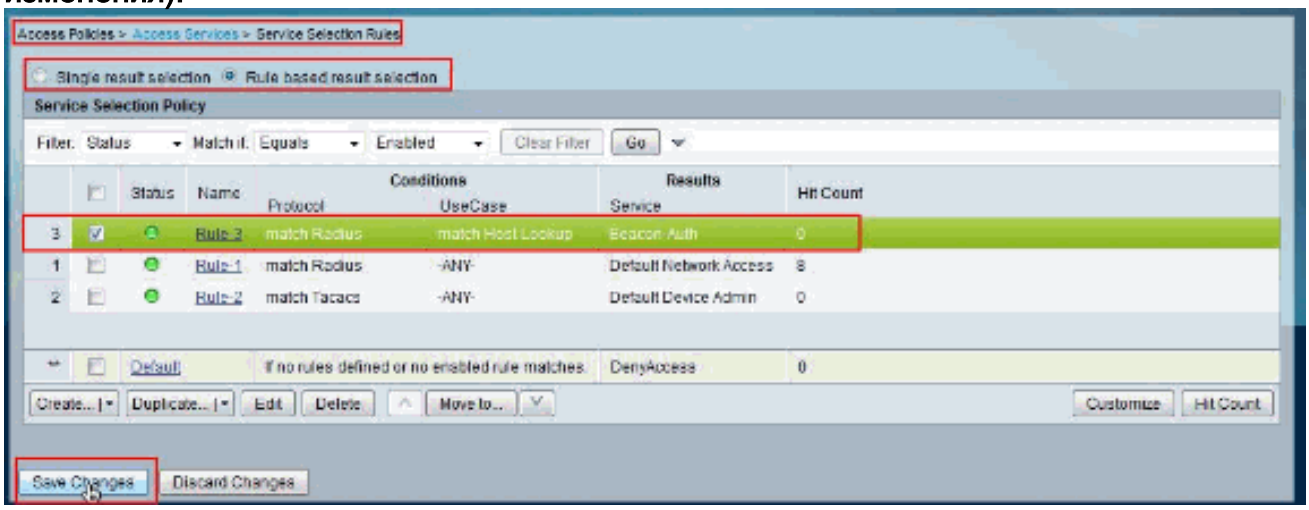
10. Выберите **Protocol** и используйте **Радиус** в качестве значения. Точно так же выберите **UseCase** и используйте **Поиск Хоста** в качестве значения. Выберите **Beacon-Auth** в качестве сервиса и нажмите **OK**.



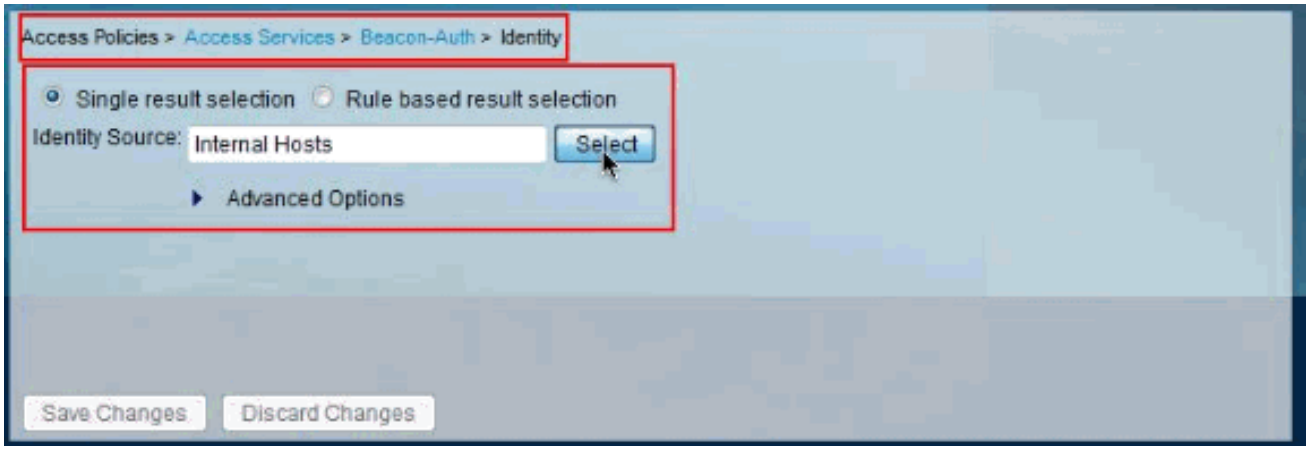
11. Переместите недавно созданное правило в вершину.



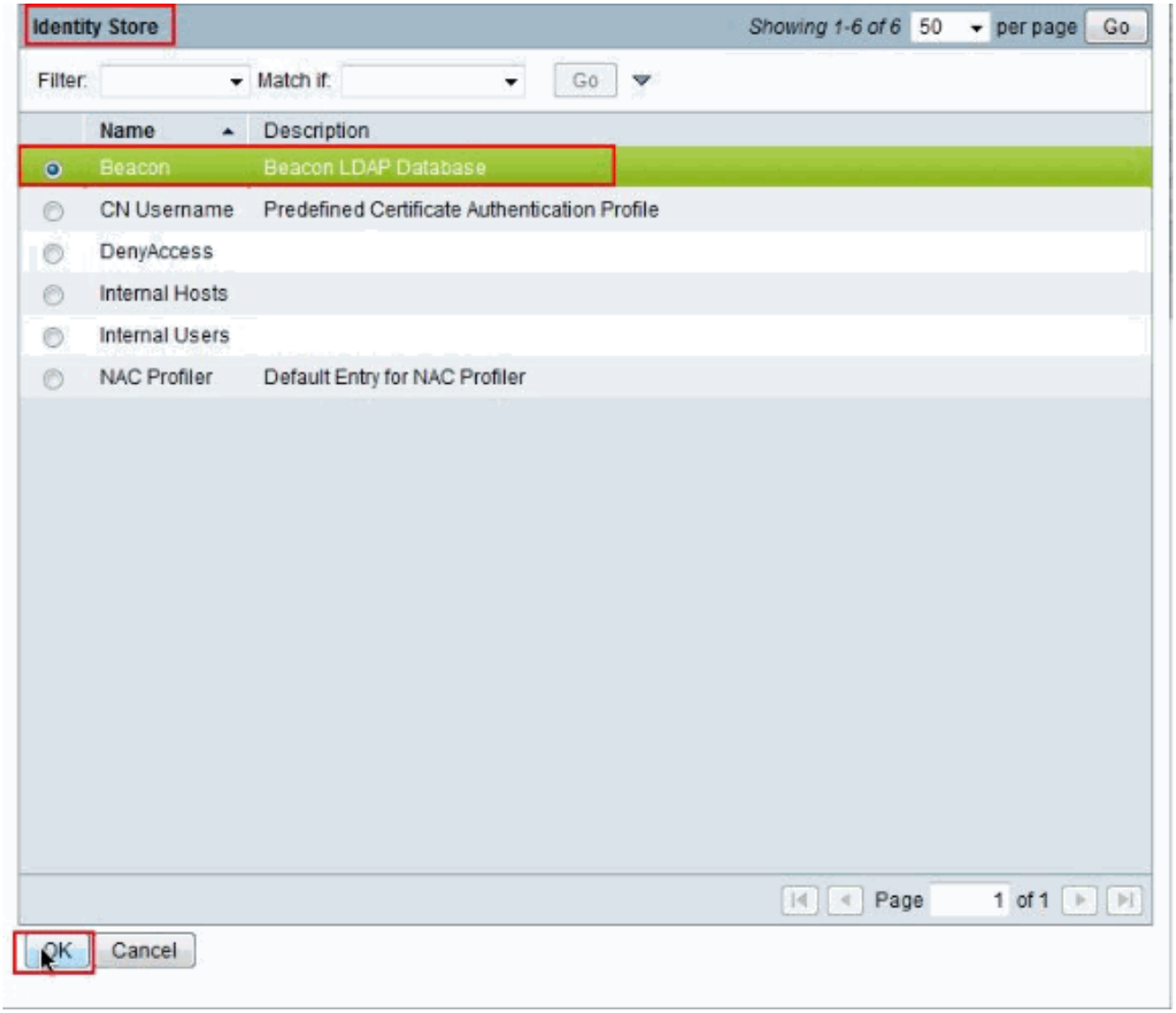
12. **Нажмите кнопку Save Changes (Сохранить изменения).**



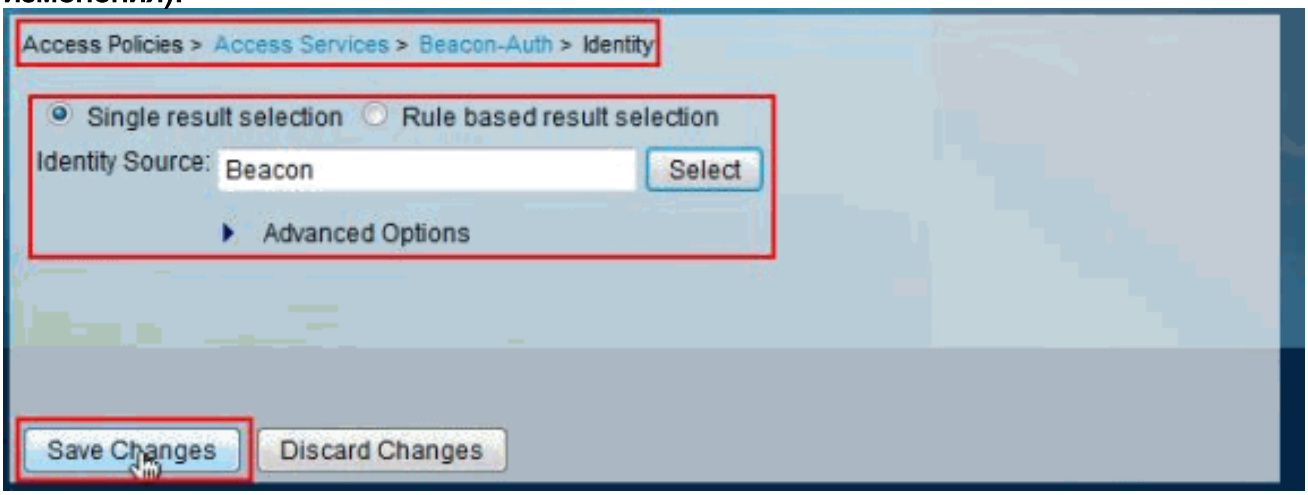
13. Выберите **Access Policies> Access Services> Beacon-Auth> Identity** и нажмите **Select**, следующий за **Идентификационным Источником**.



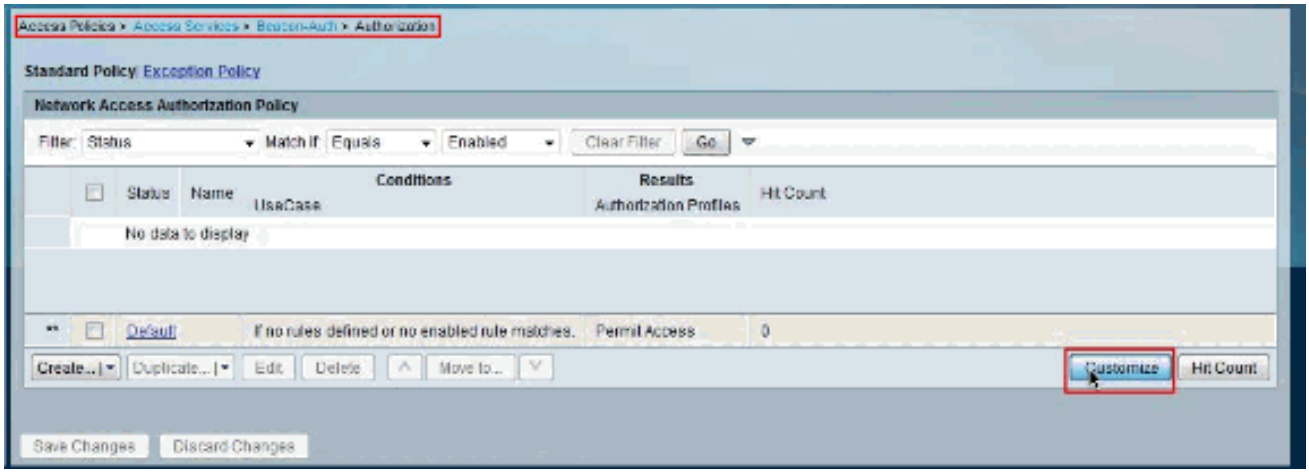
14. Выберите **Beacon** и нажмите **OK**.



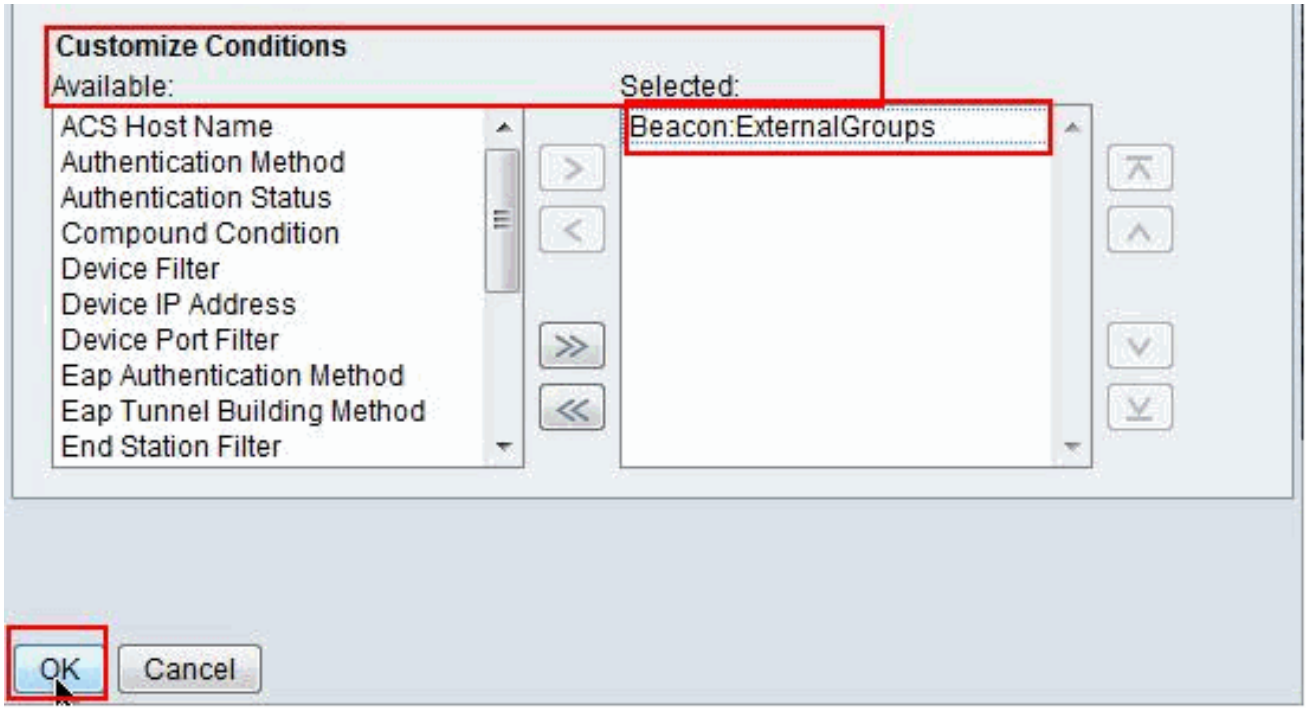
15. **Нажмите кнопку Save Changes (Сохранить изменения).**



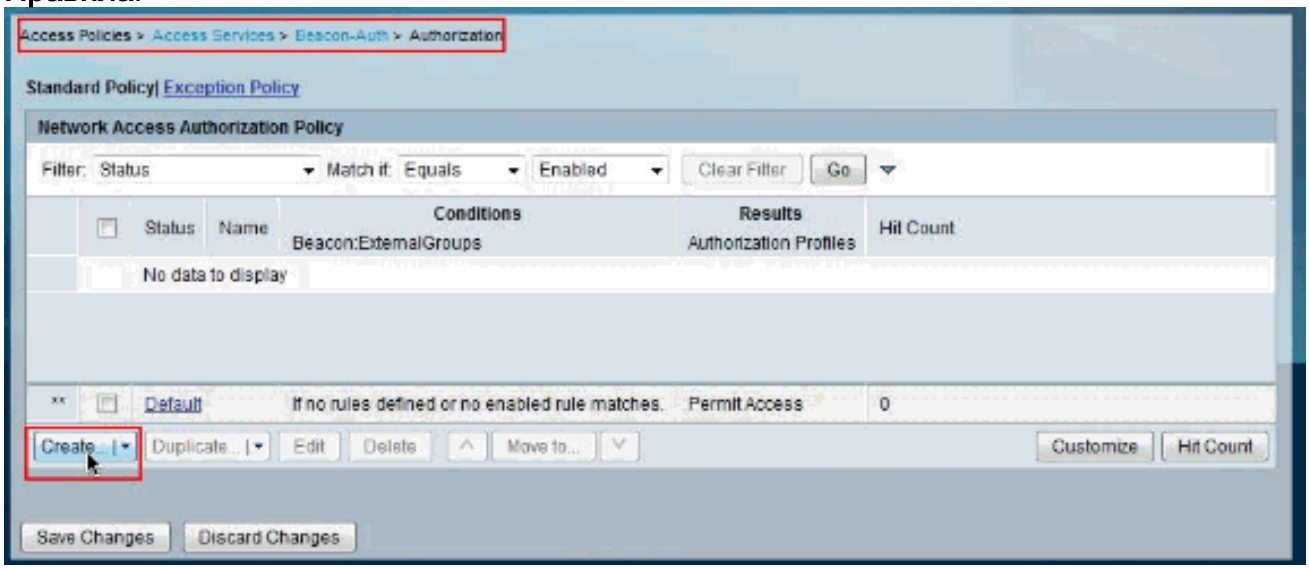
16. Выберите **Access Policies> Access Services> Beacon-Auth> Authorization** и нажмите **Customize**.



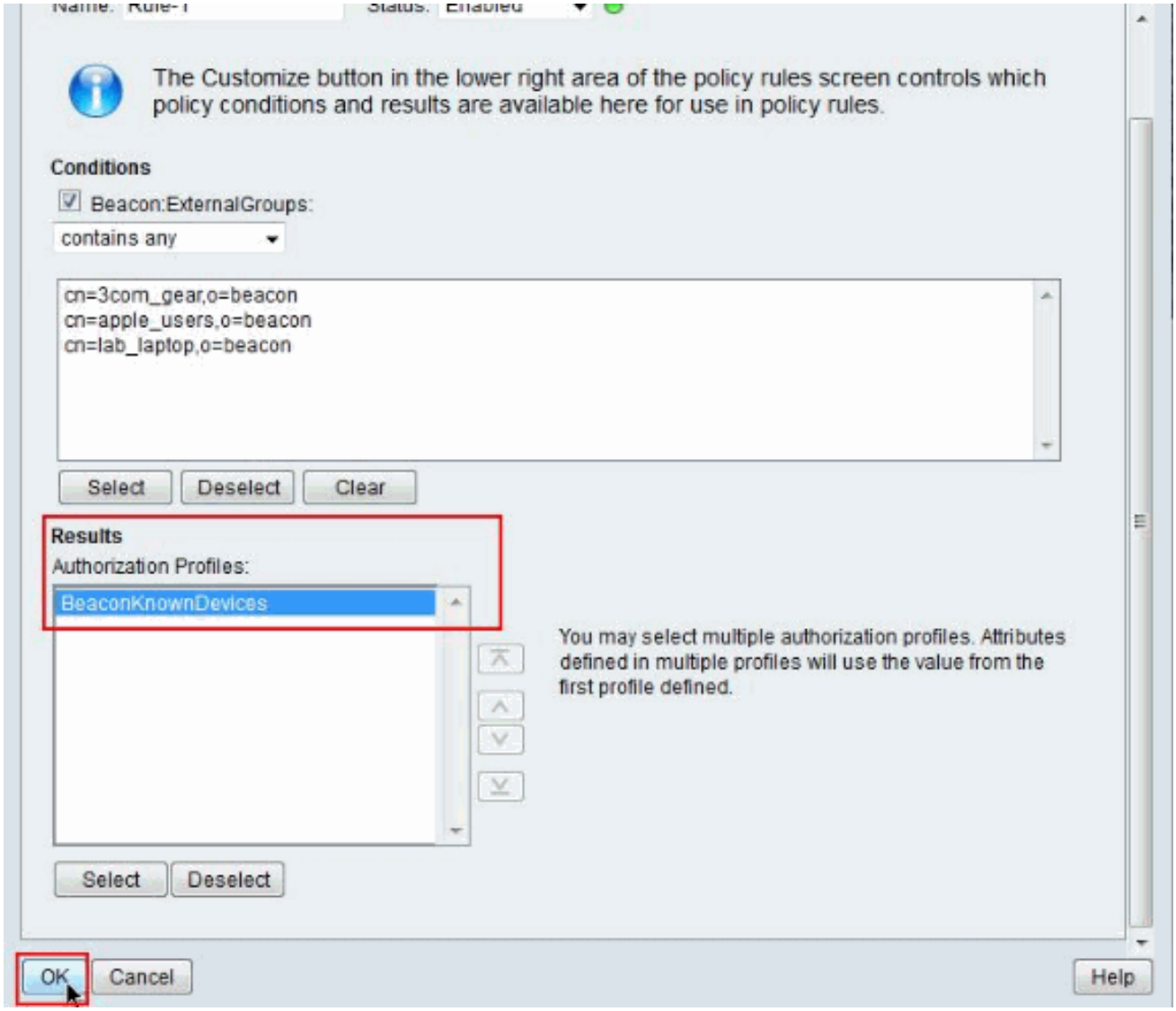
17. Переместите **Beacon:ExternalGroups** от **Доступного** до **Выбранного** и нажмите **OK**.



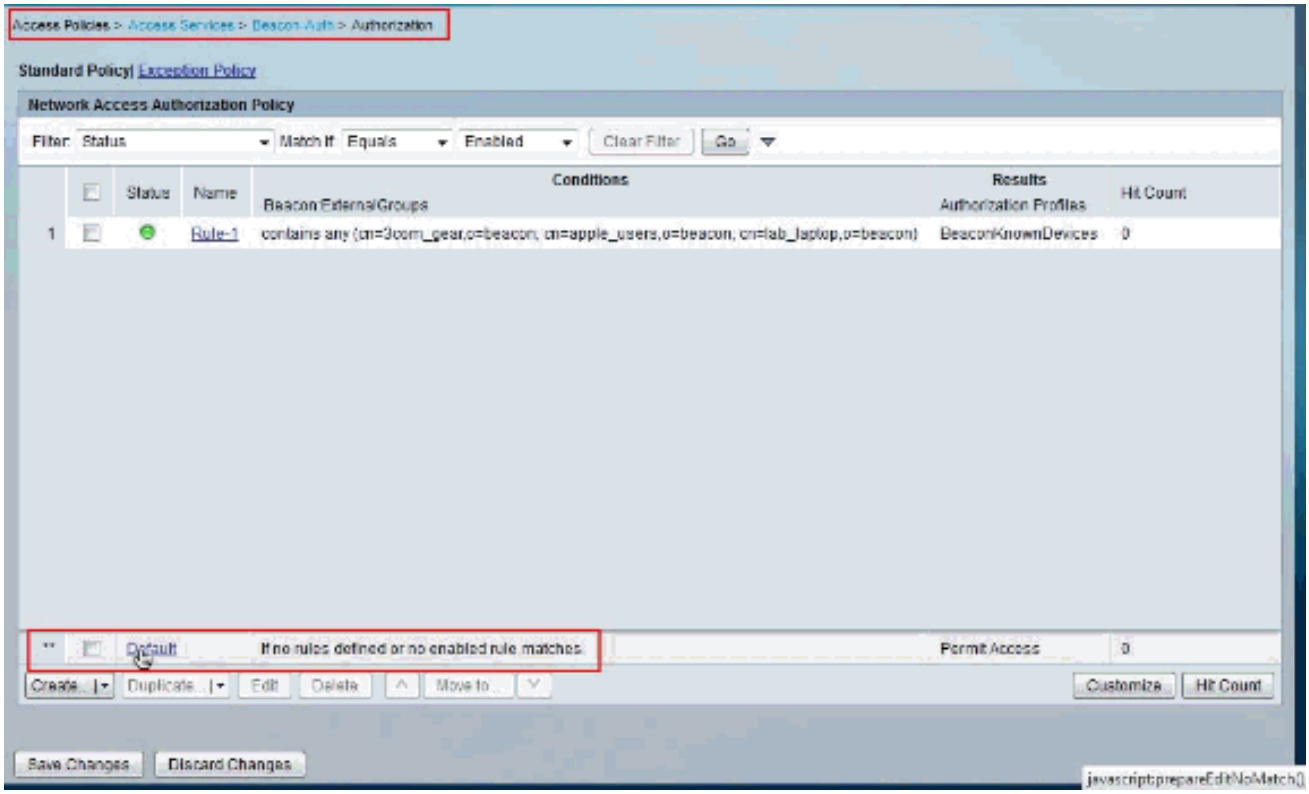
18. Нажмите **Create** для создания нового **Правила**.



19. Выберите 3com_users, apple_users и lab_laptop как условия и Профиль Авторизации **BeaconKnownDevices** как **Результат**. **Затем нажмите кнопку OK.**

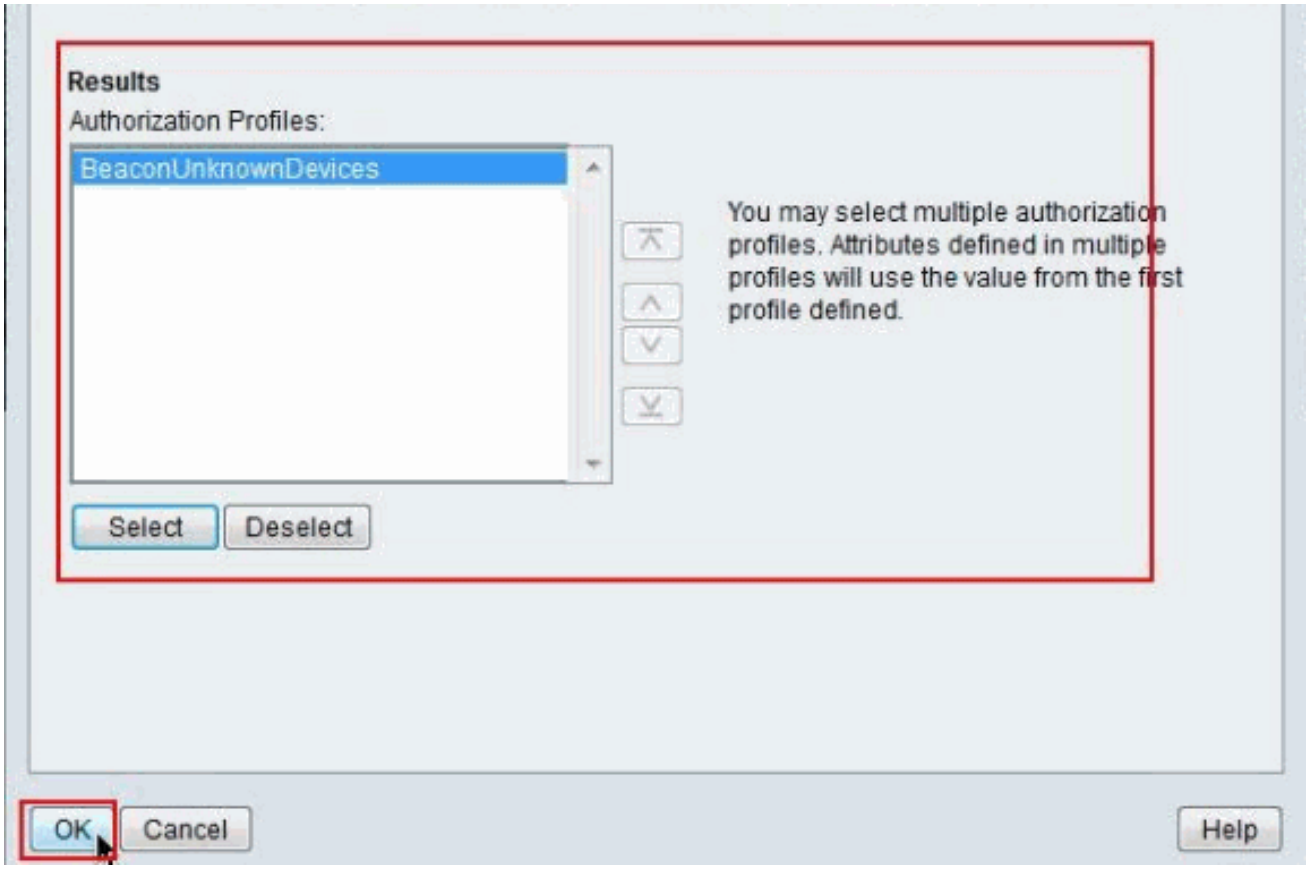


20. Нажмите **Default**.

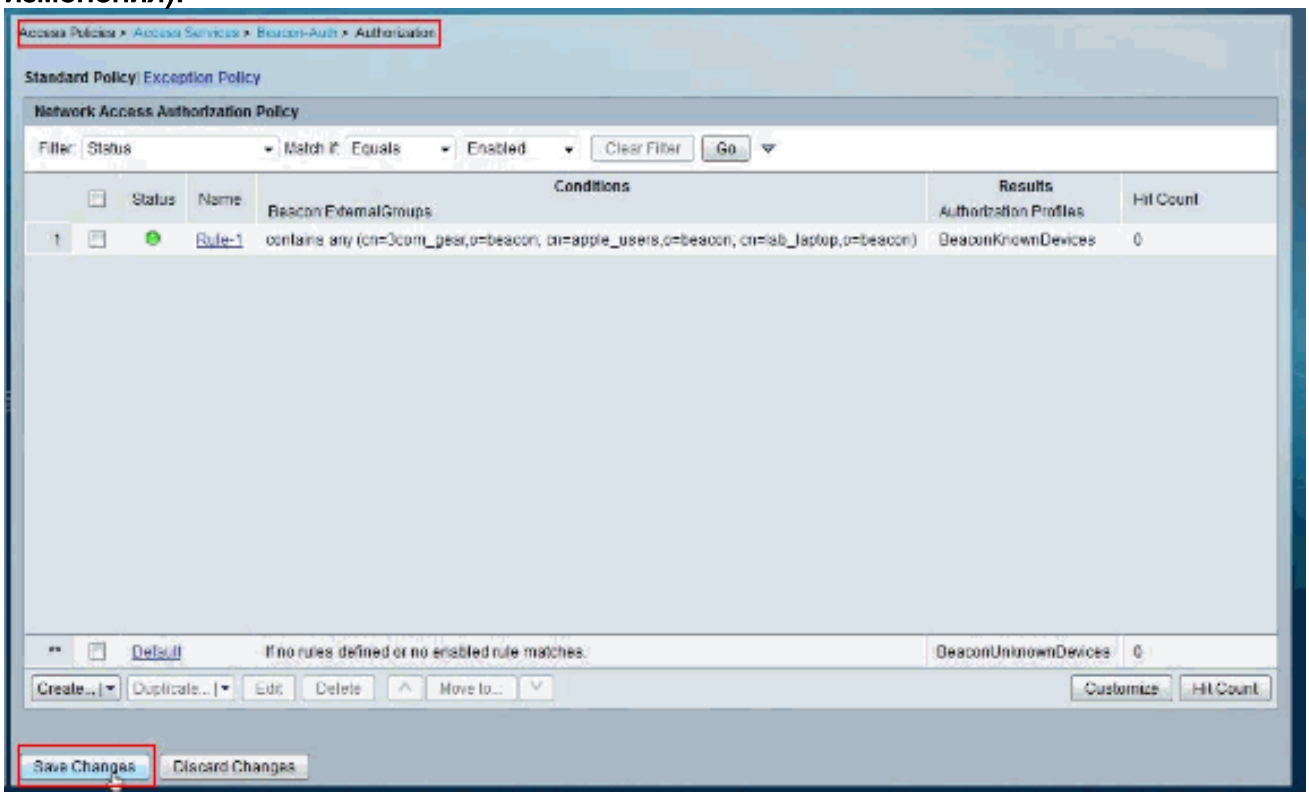


21. Выберите 3com_users, apple_users и lab_laptop как условия и Профиль Авторизации

BeaconUnKnownDevices как Результат. **Затем нажмите кнопку OK.**



22. **Нажмите кнопку Save Changes (Сохранить изменения).**



Это завершает процедуру.

Конфигурация коммутатора для обхода проверки подлинности MAC

Эта конфигурация коммутатора предоставляет пример конфигурации для аутентификации

802.1X с MAB, включенным, и перевод по службе динамической LAN потребовал для применения, атрибуты RADIUS возвратились из ACS.

Коммутатор

```
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
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Дополнительные сведения

- Cisco NAC Appliance (Clean Access)
- Система управления доступом Cisco Secure Access Control System
- Cisco Systems – техническая поддержка и документация