Настройте гостевой поток с WLC Арубы и ISE 2.0

Содержание

Введение

Этот документ descrbies шагает для настройки гостевых порталов с Контроллером беспроводной локальной сети (WLC) Арубы. От поддержки версии 2.0 платформы Identity Services Engine (ISE) третьей стороны представлены Устройства доступа к сети (NAD). ISE в настоящее время поддерживает интеграцию с беспроводными сетями Арубы для Гостя, Положения и потоков BYOD.

> **Примечание:** Cisco не ответственна за конфигурацию или поддержку устройств от других поставщиков.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

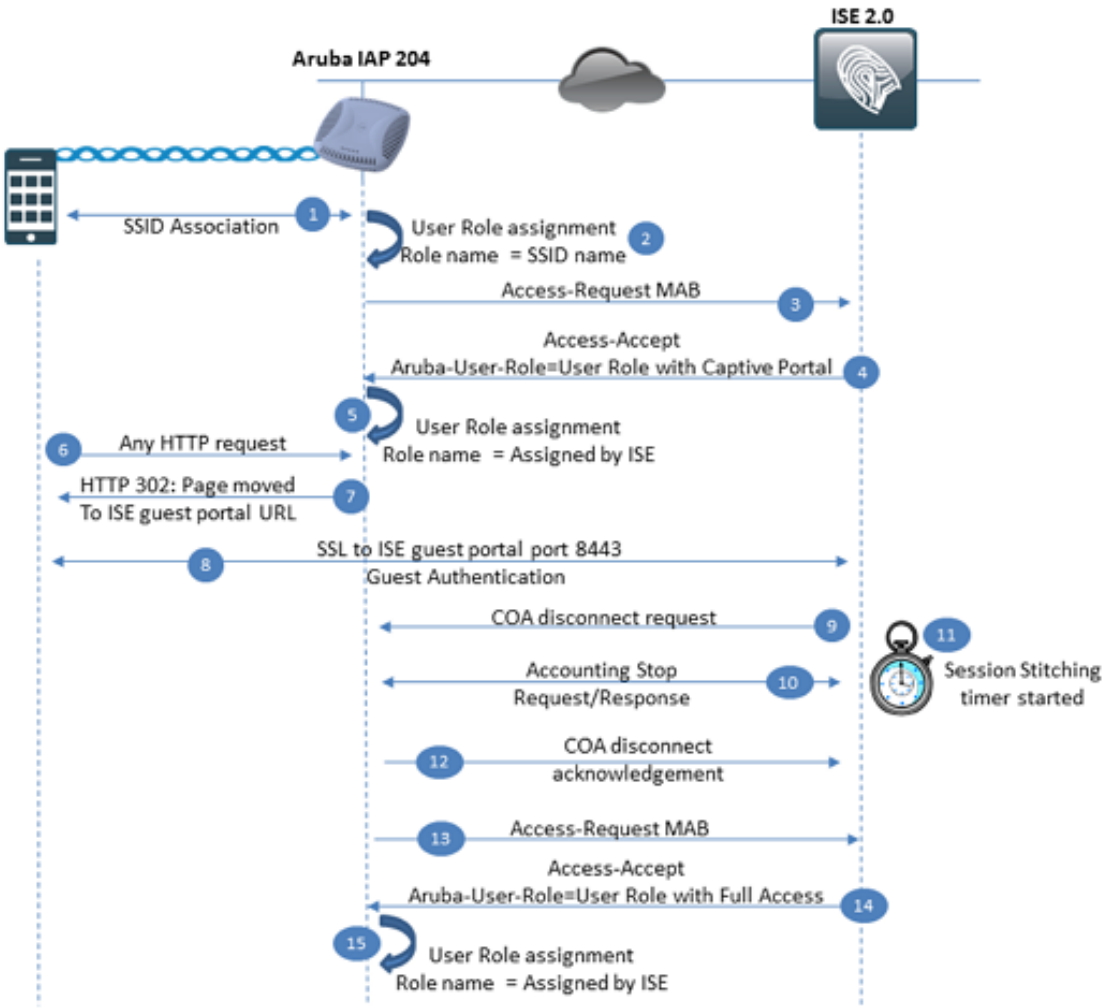
- Аруба конфигурация IAP
- Гостевой поток на ISE

Используемые компоненты

- Программное обеспечение Aruba IAP 204 6.4.2.3
- Платформа Cisco Identity Services Engine 2.0

Общие сведения

Гостевой поток



Шаг 1. Пользователь привязан к Набору сервисов Identifer (SSID). SSID может быть настроен как открытый или с аутентификацией предварительного общего ключа.

Шаг 2. Аруба применяет Роль пользователя к этому соединению. Первая роль пользователя всегда является самим SSID. Роль пользователя содержит другие параметры настройки как VLAN, ограничение Контроля доступа, Присоединенная Настройка портала и больше. В роли пользователя текущего примера по умолчанию, назначенной на SSID, имеет только оператор Permit - All.

Шаг 3. SSID настроен для обеспечения фильтрации по MAC-адресам по внешнему серверу RADIUS. MAB радиуса (Обход Проверки подлинности MAC) access-request передается ISE.

Шаг 4. . При оценке политики ISE времени выбирает профиль авторизации для Гостя. Этот профиль авторизации содержит Тип доступа, равный ACCESS_ACCEPT и Роли пользователя Арубы, равной названию Роли пользователя, настроенному локально на WLC Арубы (Контроллер беспроводной локальной сети). Эта роль пользователя настроена для Присоединенного Портала, и трафик перенаправлен к ISE.

Роли пользователя Арубы

Основным компонентом, который используется WLC Арубы, является Роль пользователя. Роль пользователя определяет ограничение доступа, применимое к пользователю во время соединения. Ограничение доступа может включать: Присоединенное Портала перенаправление, Список контроля доступа, VLAN (Виртуальная локальная сеть), Ограничение пропускной способности и другие. Каждый SSID, который существует на WLC Арубы, имеет Роль пользователя по умолчанию, где Роль пользователя равна названию SSID, все пользователи соединились с определенным SSID, первоначально получают ограничения от роли по умолчанию. Роль пользователя может быть перезаписана сервером RADIUS в этом случае, Access-Accept должен содержать Арубу Определяемая поставщиком Роль пользователя Арубы атрибута. Значение от этого атрибута используется WLC для обнаружения локальной роли пользователя.

Шаг 5. . С атрибутом WLC Роли пользователя Арубы проверяет локально для ролей настроенного пользователя и применяется, потребовал того.

Шаг 6. Пользователь инициирует запрос HTTP в браузере.

Шаг 7. WLC Арубы перехватывает запрос из-за роли пользователя, настроенной для Присоединенного портала. Поскольку ответ на этот WLC запроса возвращает Код HTTP 302 страницы, перемещенные с гостевым порталом ISE как новое местоположение.

Шаг 8. Пользователь устанавливает подключение SSL к ISE на порту 8443 и вводит имя пользователя в гостевом портале.

Шаг 9. ISE передает сообщение запроса отключения COA к WLC Арубы.

Шаг 10. После того, как WLC сообщения разъединения COA отбрасывает соединение с пользователем и сообщает ISE, что соединение должно быть завершено с помощью Бухгалтерского Запроса Радиуса (Останавливают) сообщение. ISE должен подтвердить, что это сообщение было получено с Учетом.

Шаг 11. ISE запускает таймер Сшивания Сеанса. Этот таймер используется для привязки сеанса прежде и после COA вместе. В это время ISE помнит все параметры сеанса как имя пользователя и т.д. Вторая попытка аутентификации должна быть сделана перед этим таймером истекают для выбора корректной Политики авторизации для клиента. В случае, если, если таймер истекает, новый Access-Request будет интерпретироваться как абсолютно новый сеанс, и политика авторизации с Гостевым Перенаправлением будет применена снова.

Шаг 12. WLC Арубы подтверждает ранее полученный запрос отключения COA с подтверждением разъединения COA.

Шаг 13. WLC Арубы передает новый Access-Request Радиуса MAB.

Шаг 14. При оценке политики ISE времени выбирает профиль авторизации для Гостя после

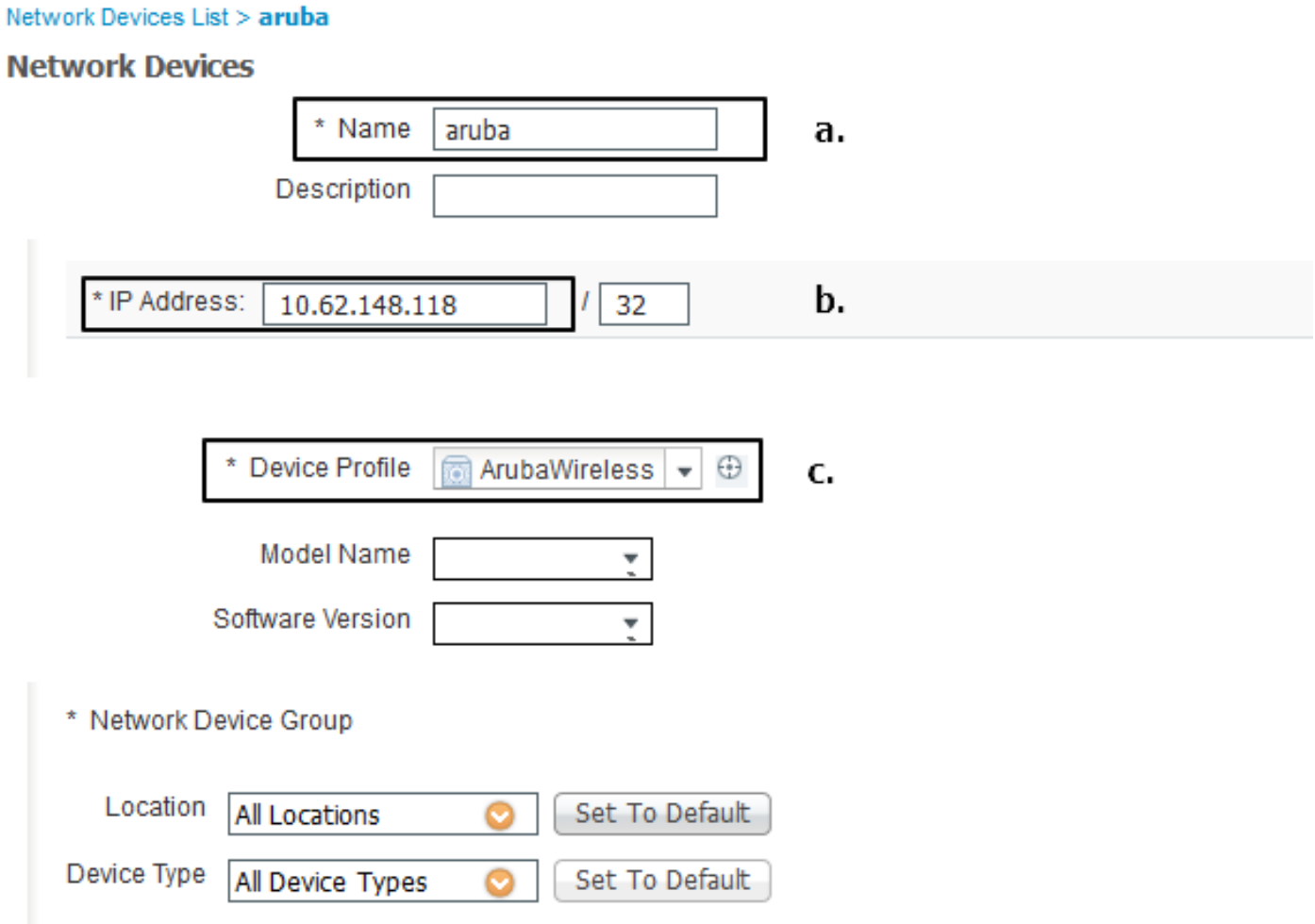
аутентификации. Этот профиль авторизации содержит Тип доступа, равный ACCESS_ACCEPT и Роли пользователя Арубы, равной названию Роли пользователя, настроенному локально на WLC Арубы. Эта роль пользователя, настроенная для разрешения всего трафика.

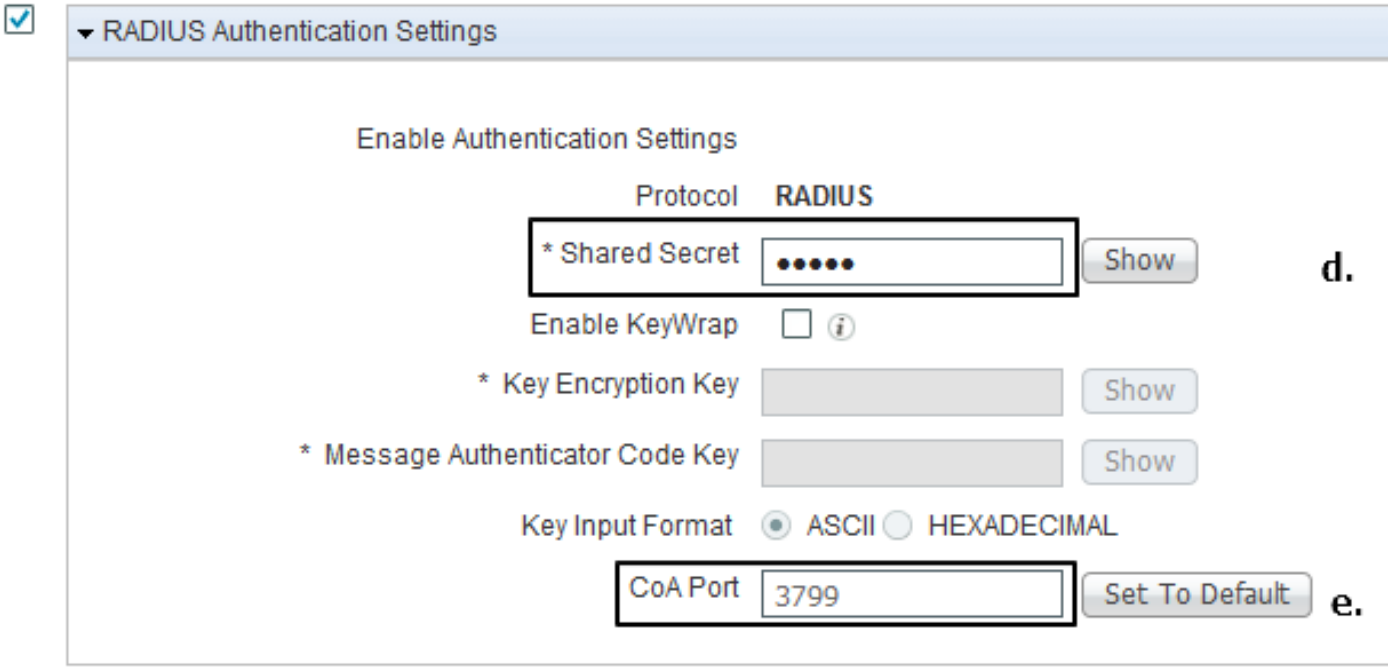
Шаг 15. С атрибутом WLC Роли пользователя Арубы проверяет локально роли настроенного пользователя и применяется, потребовал того.

Настройка

Шаг 1. Добавьте WLC Арубы как NAD в ISE.

Перейдите к **администрированию> Сетевые ресурсы> Сетевые устройства** и **нажмите Add**

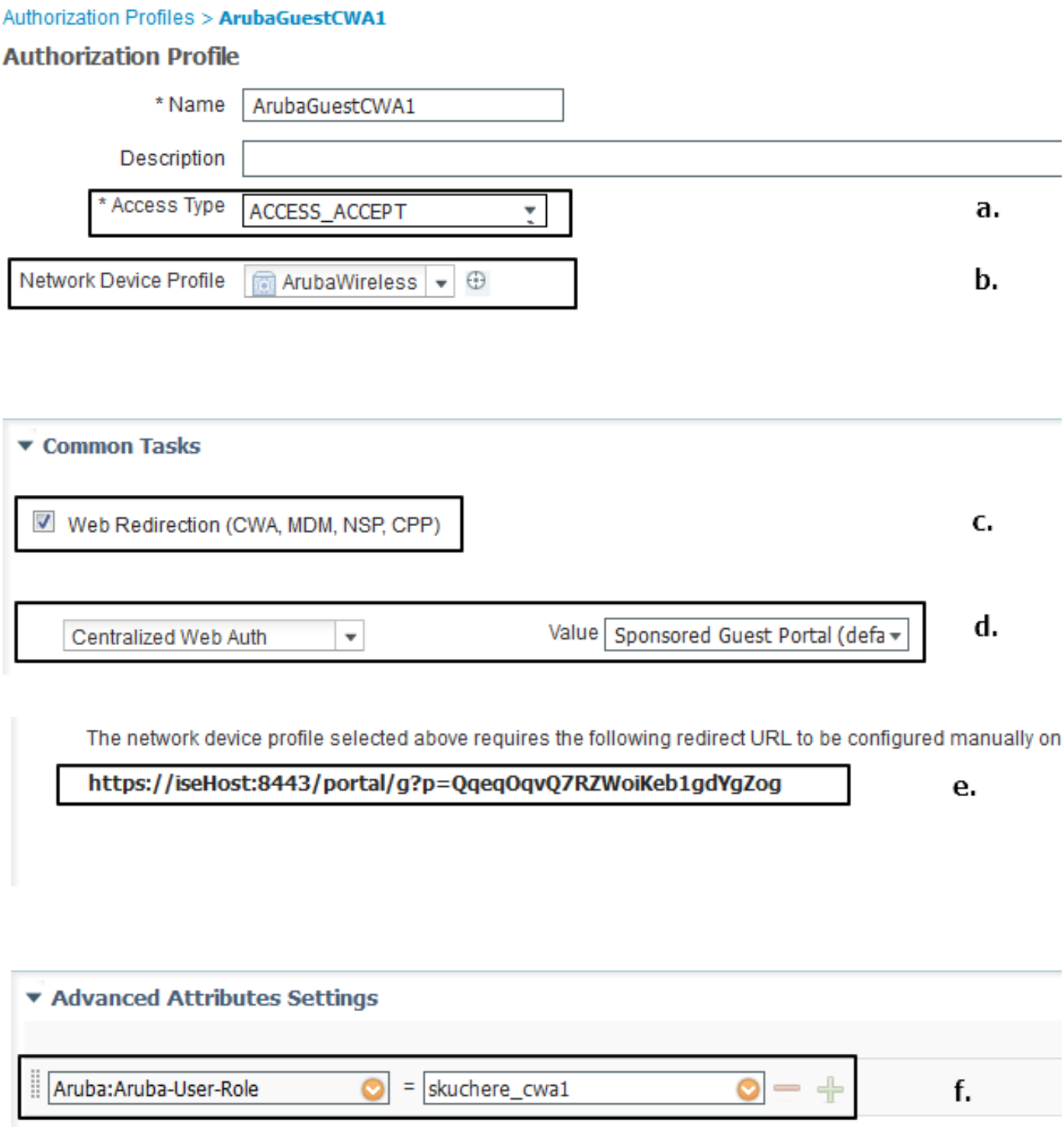




1. Предоставьте название Устройства доступа к сети (NAD).
2. Задайте IP-адрес NAD.
3. Выберите Network Device Profile. Для WLC Арубы можно использовать встроенный профиль ArubaWireless.
4. Предоставьте предварительный общий ключ.
5. Определите порт COA, порт 3799 UDP использования текущего примера формы устройства для COA.

Шаг 2. Настройте профили авторизации.

Перейдите к **Политике> Элементы Политики> Результаты> Авторизация> Профиль Авторизации** и **нажмите Add.** Сначала необходимо создать профиль авторизации для перенаправления Центральной веб-аутентификации (CWA), как показано в образе.

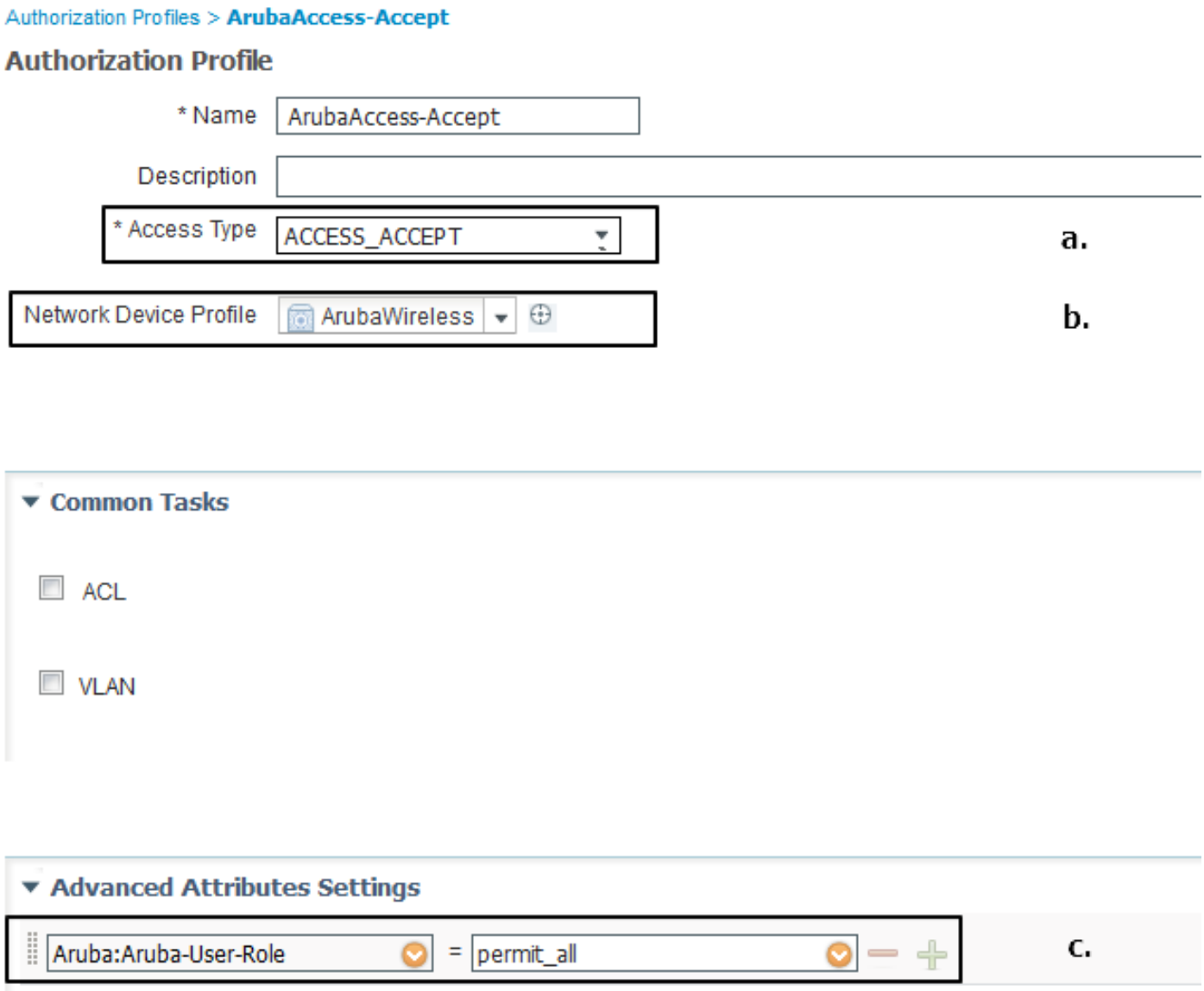


Примечание: По умолчанию все Профили Авторизации имеют тип сетевого устройства, равный Cisco. Если сам NAD настроен как ArubaWireless, и профиль авторизации создан для другого типа устройства, с этим профилем никогда не совпадают для этого устройства.

1. Определите **тип доступа** как **Access-Accept**.
2. В **Сетевом устройстве Профиль** выбирают **ArubaWireless**.
3. В разделе общей задачи включите **веб-**опцию **Redirection**.
4. Как тип перенаправления выбирают **Centralized Web Auth** и выбирают гостевой портал, который требуется использовать для перенаправления.
5. URL, что подарки ISE должны быть определены на WLC Арубы как внешний Присоединенный портала URL.

6. В **Усовершенствованном** разделе **Параметров настройки Атрибута** определите значение атрибута Роли пользователя Арубы.

Второй профиль авторизации должен быть создан для обеспечения доступа для гостей после портала аутентификации:



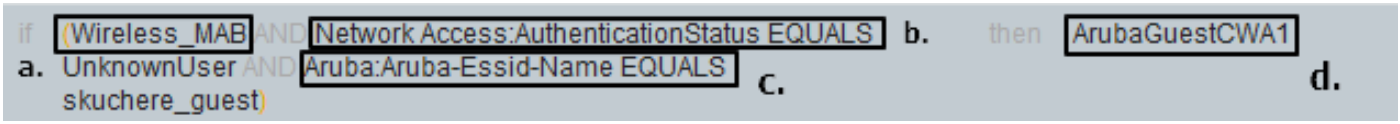
1. Определите **тип доступа** как **Access-Accept**.
2. В **Сетевом устройстве Профиль** выбирают **ArubaWireless**.
3. В **Усовершенствованном Атрибуте** раздел **Параметров настройки** определяют значение атрибута Роли пользователя Арубы. Позже вы настроите локальную Роль пользователя на WLC Арубы с тем же названием.

Шаг 3. Настройте политику авторизации.

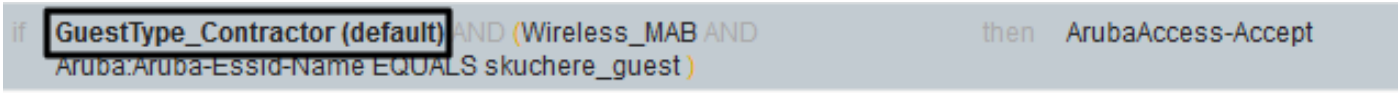
Первая политика авторизации ответственна за пользовательское перенаправление к гостевому порталу. В самом простом случае можно использовать созданный в составном условии

- Wireless_MAB (a. и
- Доступ к сети AuthenticationStatus равняется Неизвестному пользователю (b. и
- Аруба Aruba-Essid-Name равняется вашему гостевому названию (c) SSID..

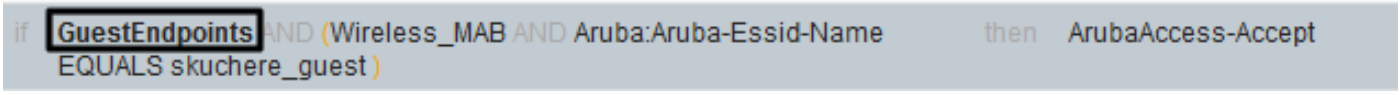
Для этой политики настройте профиль авторизации с перенаправлением к гостевому порталу в результате (d).



Вторая политика авторизации должна предоставить доступ для гостя после аутентификации через портал. Эта политика может полагаться на данные сеанса (Гостевой поток User Identity Group/Use case и так далее). В этом сценарии должен воссоединиться пользователь перед таймером Сшивания Сеанса истеките:



Для защиты себя от истечения срока действия таймера Сшивания Сеанса, можно полагаться на данные оконечной точки вместо данных сеанса. По умолчанию Спонсируемый Гостевой портал на ISE 2.0 настроен для автоматической гостевой регистрации устройства (Гостевое устройство автоматически размещено в идентификационную группу оконечной точки Guest_Endpoints). Эта группа может использоваться в качестве условия:

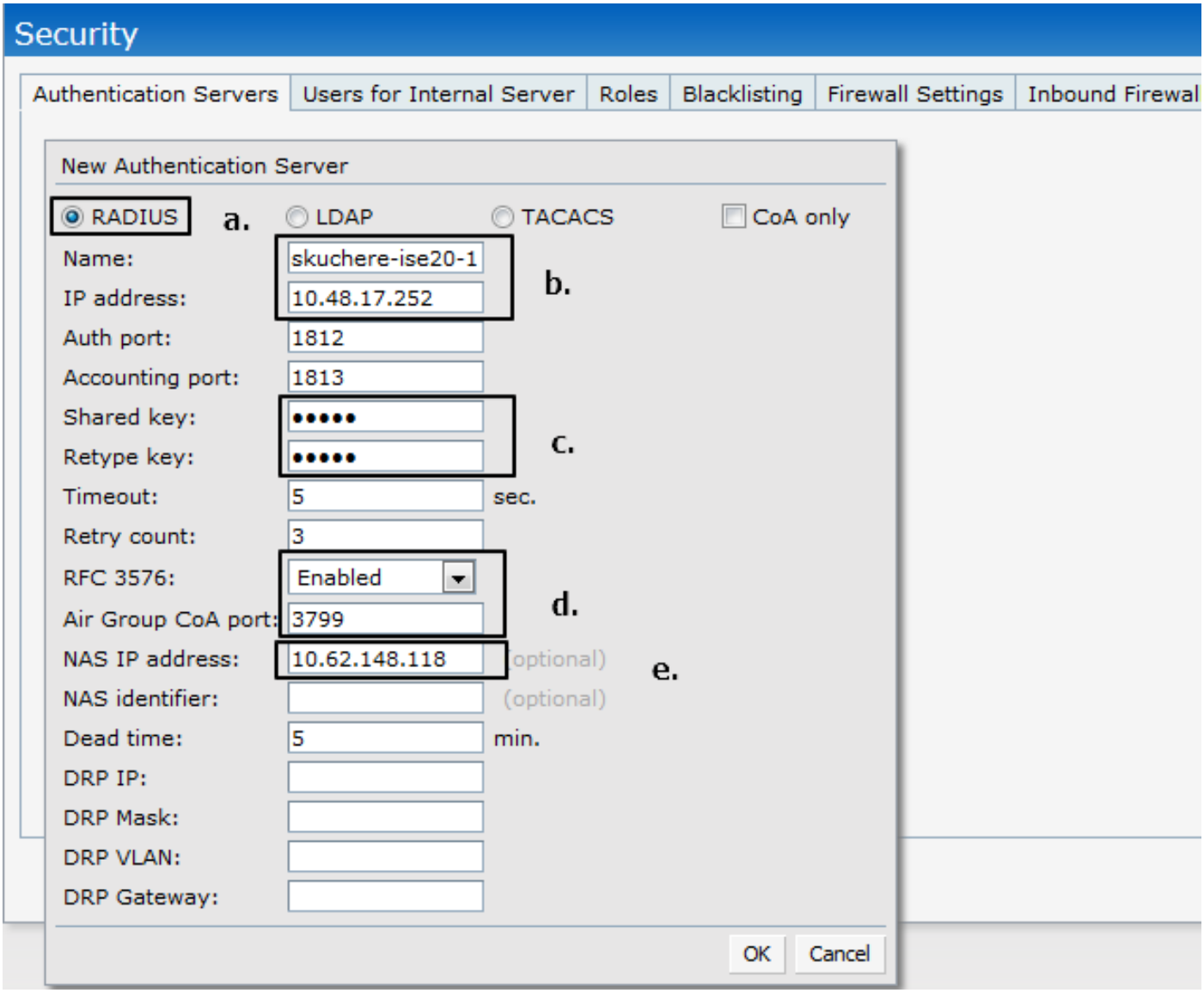


Политика авторизации в правильном порядке:

if	**GuestEndpoints** AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept
if	(Wireless_MAB AND Network Access:AuthenticationStatus EQUALS UnknownUser AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaGuestCWA1

Шаг 4. . Настройте сервер RADIUS на Арубе.

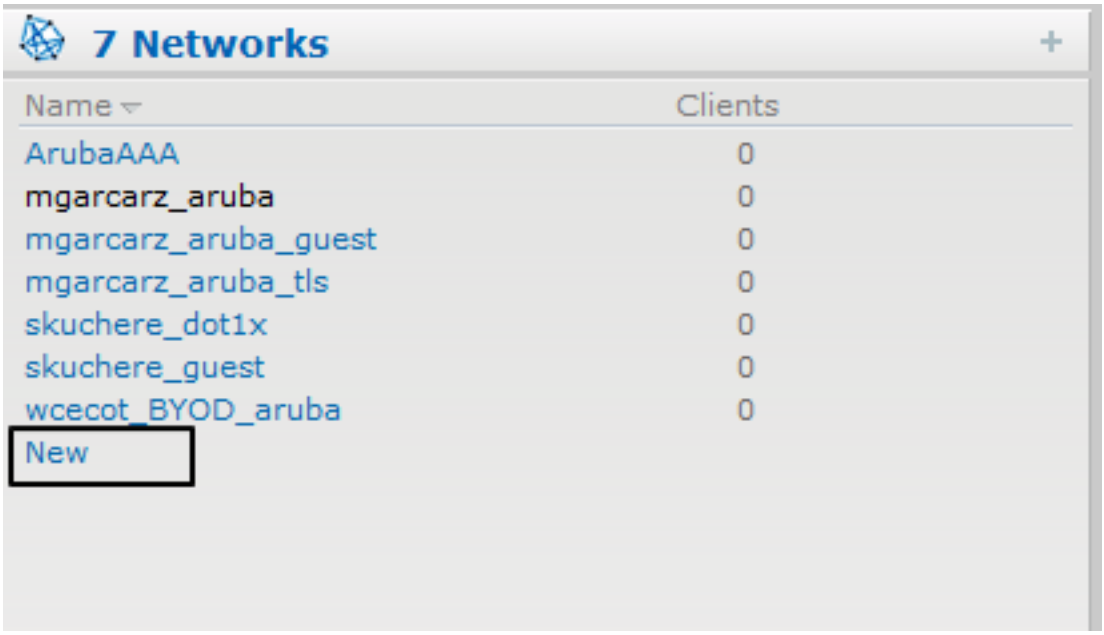
Перейдите к **Серверам Security> Authentication** и нажмите **New:**



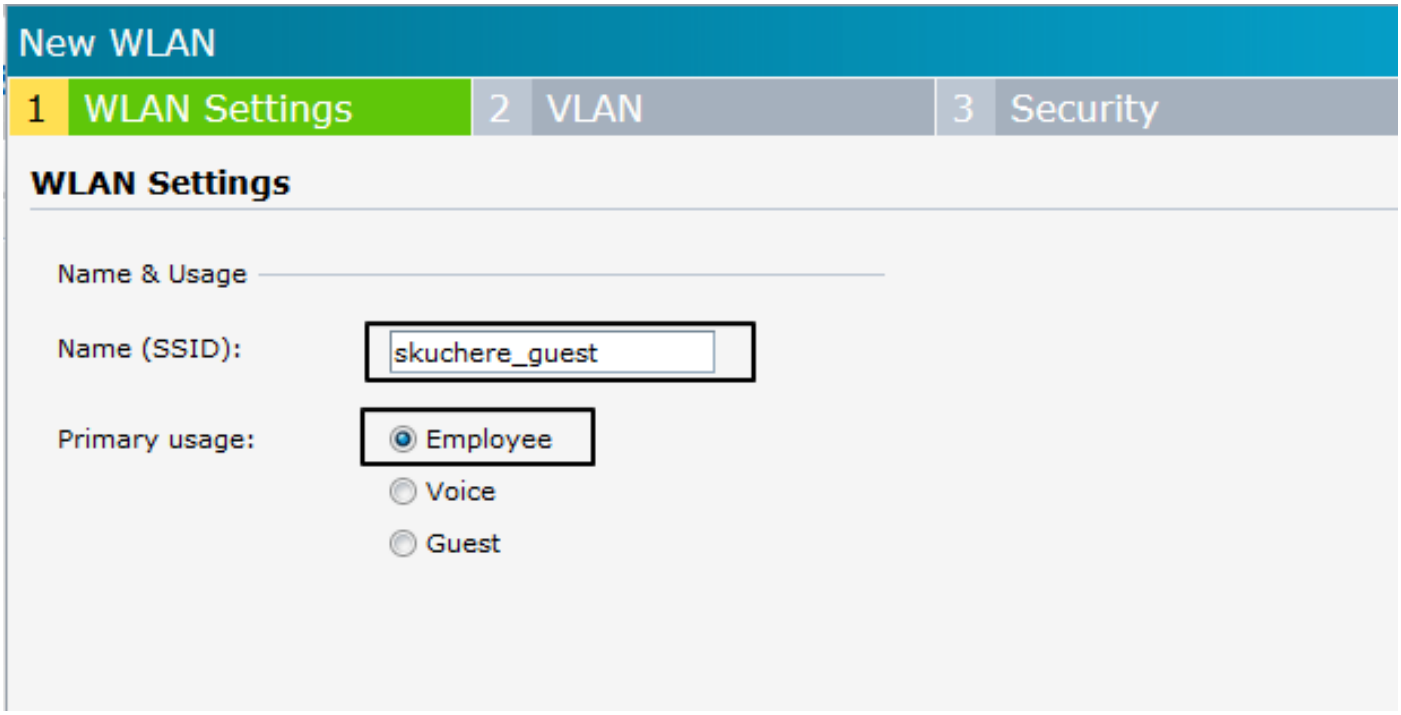
1. Выберите RADIUS в качестве протокола AAA (проверка подлинности, авторизация и учет).
2. Определите название AAA-сервера и IP-адрес.
3. Задайте предварительный общий ключ.
4. RFC Enable 3576 поддержки и определяет порт COA.
5. Задайте IP интерфейса управления WLC Арубы как IP-адрес NAS.

Шаг 5. . Создайте гостевой SSID на Арубе.

В информационной панели страница выбирают **New** в конце списка сети. Мастер создания SSID должен запустить. Выполните действия мастера.

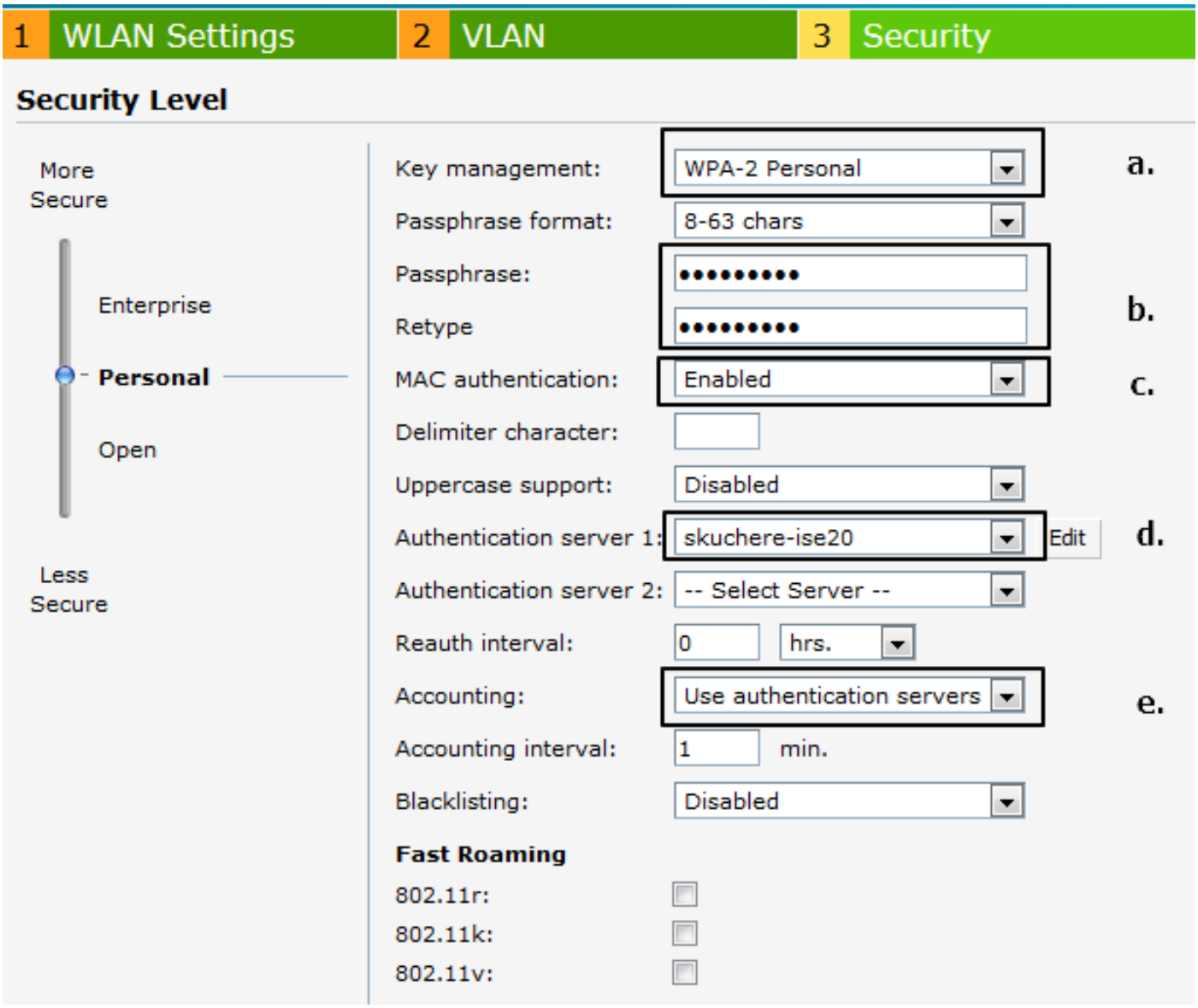


Шаг 1. Определите название SSID и выберите тип SSID. Здесь, Сотрудник типа SSID используется. Этот тип SSID имеет роль по умолчанию с разрешением все и никакое Присоединенное Портала Осуществление. Кроме того, можно выбрать Гостя типа. В таком сценарии необходимо определить присоединенные настройки портала во время конфигурации SSID.



Шаг 2. Назначение VLAN и присвоение IP-адреса. Здесь, параметры настройки оставляют как настройки по умолчанию, как показано в образе.

Шаг 3. Настройки безопасности. Для гостевого SSID можно выбрать Open или Personal. Персональный требует ключа перед клочком.



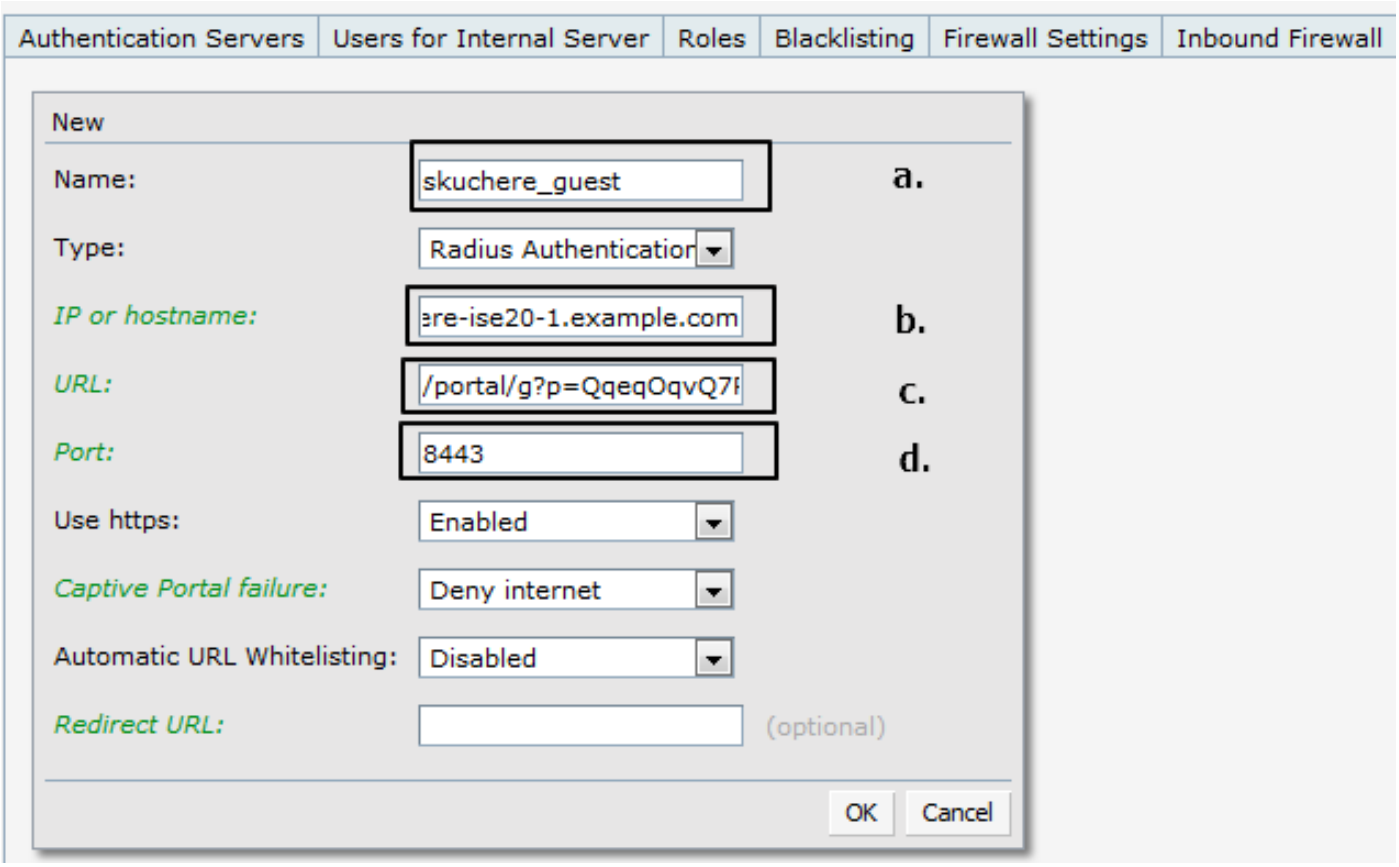
1. Выберите механизм Key Management.
2. Определите предварительный общий ключ.
3. Аутентифицировать пользователя против ISE с помощью фильтрации по MAC-адресам MAB должно быть включено.
4. В списке серверов аутентификации выбирают ваш AAA-сервер.

5. Чтобы позволить считать к ранее определенному AAA-серверу выбирают Use Authentication server в выпадающем списке.

Примечание: Учет крайне важен с третьей частью NADs. Если Узел сервиса политики (PSN) не получает Учет - Останавливаются для пользователя от NAD, сеанс может застрять в Запущенном состоянии.

Шаг 6. Настройте присоединенный портал.

Перейдите к **Безопасности> Внешние Присоединенные Порталы** и создайте новый портал, как показано в образе:



Шаг 1. Задайте присоединенное портала название.

Steo 2. Определите свой ISE FQDN или IP-адрес. При использовании IP-адрес, гарантируете, что этот IP определил в поле альтернативного имени субъекта (SAN) Гостевого Сертификата Портала.

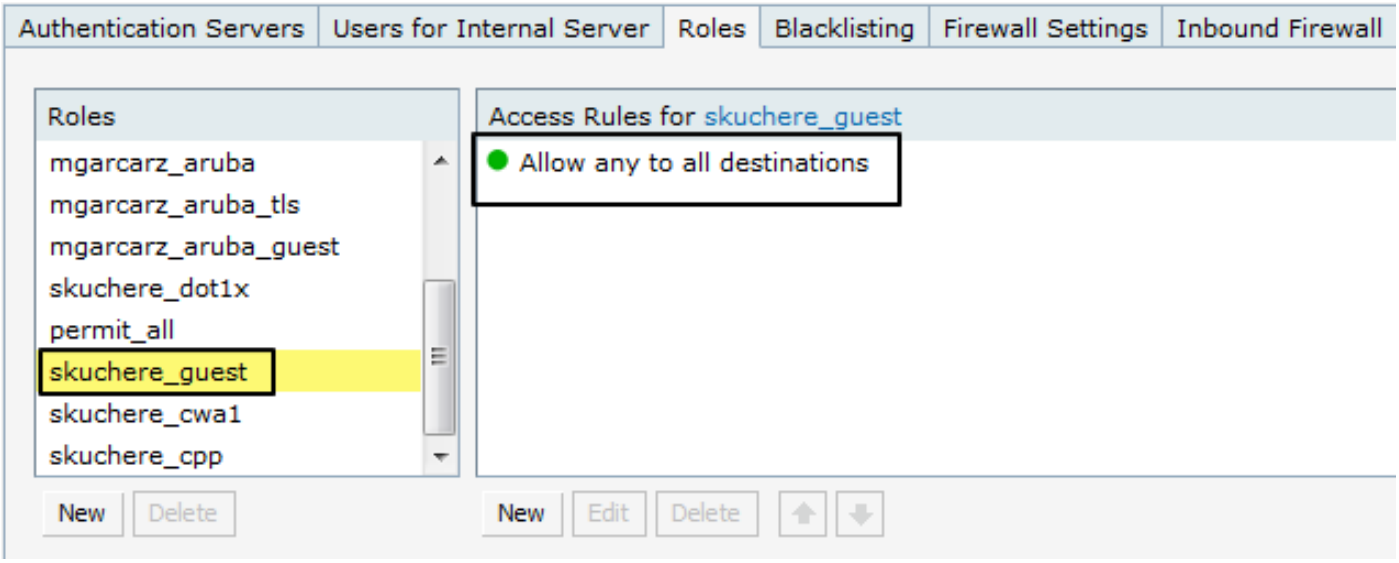
Примечание: Можно использовать любой сервер PSN, но пользователь должен всегда перенаправляться к серверу, где MAB имел место. Обычно необходимо определить FQDN сервера RADIUS, который был настроен на SSID.

Шаг 3. Предоставьте перенаправление от Профиля авторизации ISE. Необходимо поместить здесь часть после номера порта,

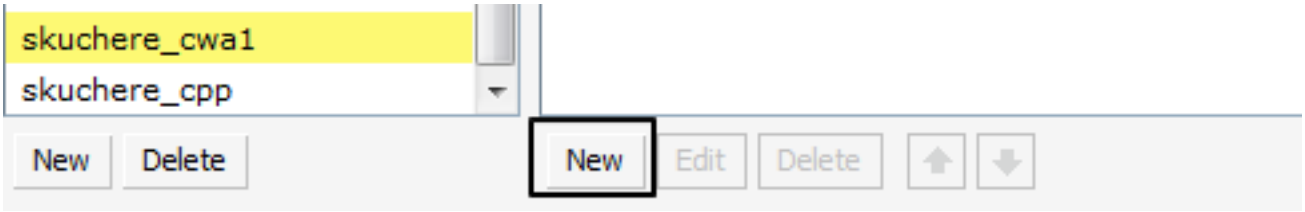
Шаг 4. . Определите гостевой порт портала ISE.

Шаг 7. Настройте роли пользователя.

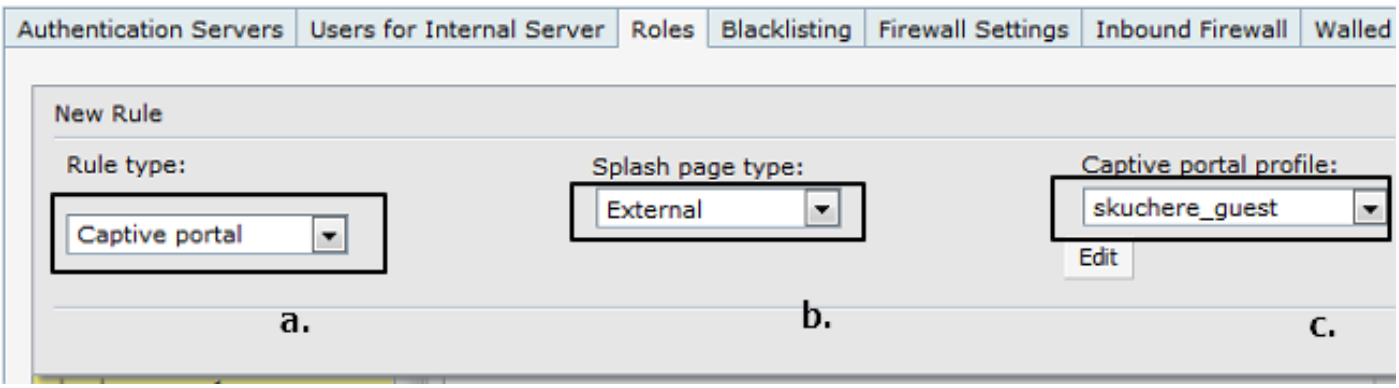
Перейдите к **Безопасности> Роли.** Гарантируйте, что после того, как SSID создан, новая роль с тем же названием присутствует в списке с разрешением на правило доступа любой всем назначениям. Кроме того, создайте две роли: один для перенаправления CWA и второй для доступа разрешения после аутентификации на гостевых порталах. Названия этих ролей должны быть идентичны Роли пользователя Арубы, определенной в Профилях авторизации ISE.



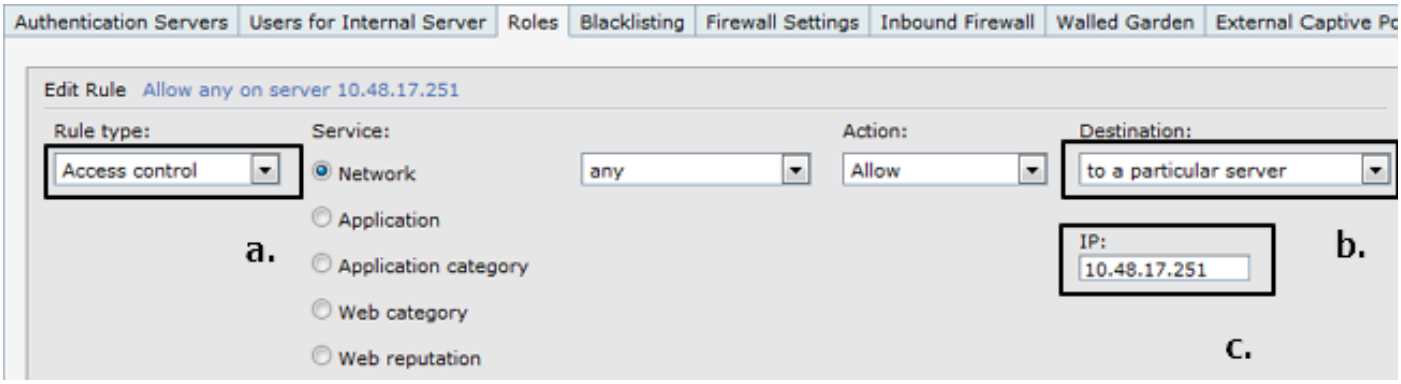
Как показано в образе, создайте роль нового пользователя для перенаправления и добавьте ограничение безопасности.



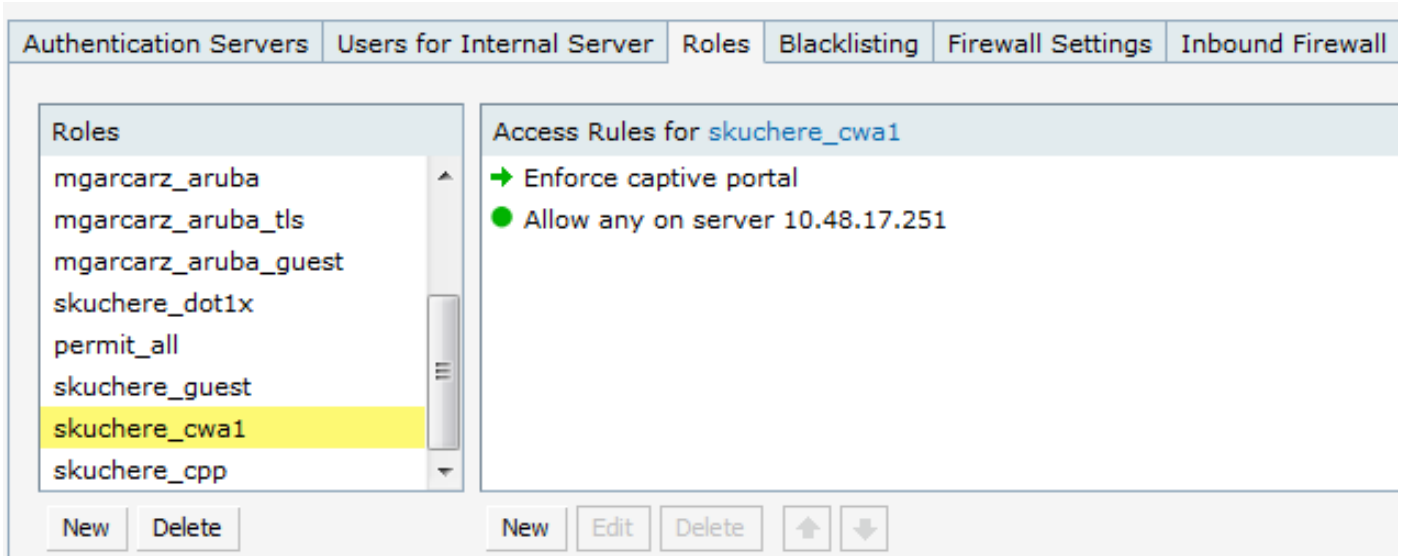
Для первого ограничения необходимо определить:



Для второго ограничения необходимо определить:

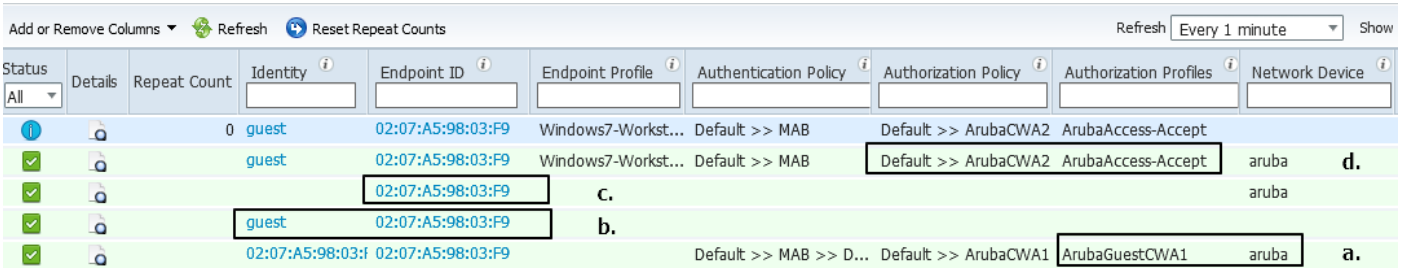


Как показано в образе, стандартное правило Позволяет, что любой всем назначениям может быть удален. Это - итоговый результат конфигурации роли.



Проверка

Пример гостя течет в **Операциях** ISE**> Радиус Livelog**.



1. Первый MAB и в результате авторизация представляет с перенаправлением CWA и Ролью пользователя, которым настроили Присоединенный портал на стороне Арубы.
2. Гостевая аутентификация.
3. Успешное изменение авторизации (CoA).
4. Второй MAB и в результате авторизация представляет с доступом разрешения и Ролью пользователя, которая имеет разрешение все правило о стороне Арубы.

На стороне Арубы можно использовать**, показывают** команду **клиентов**, чтобы гарантировать, что пользователь связан, IP-адрес назначен, и корректная роль пользователя назначена в результате аутентификации:

```
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
```

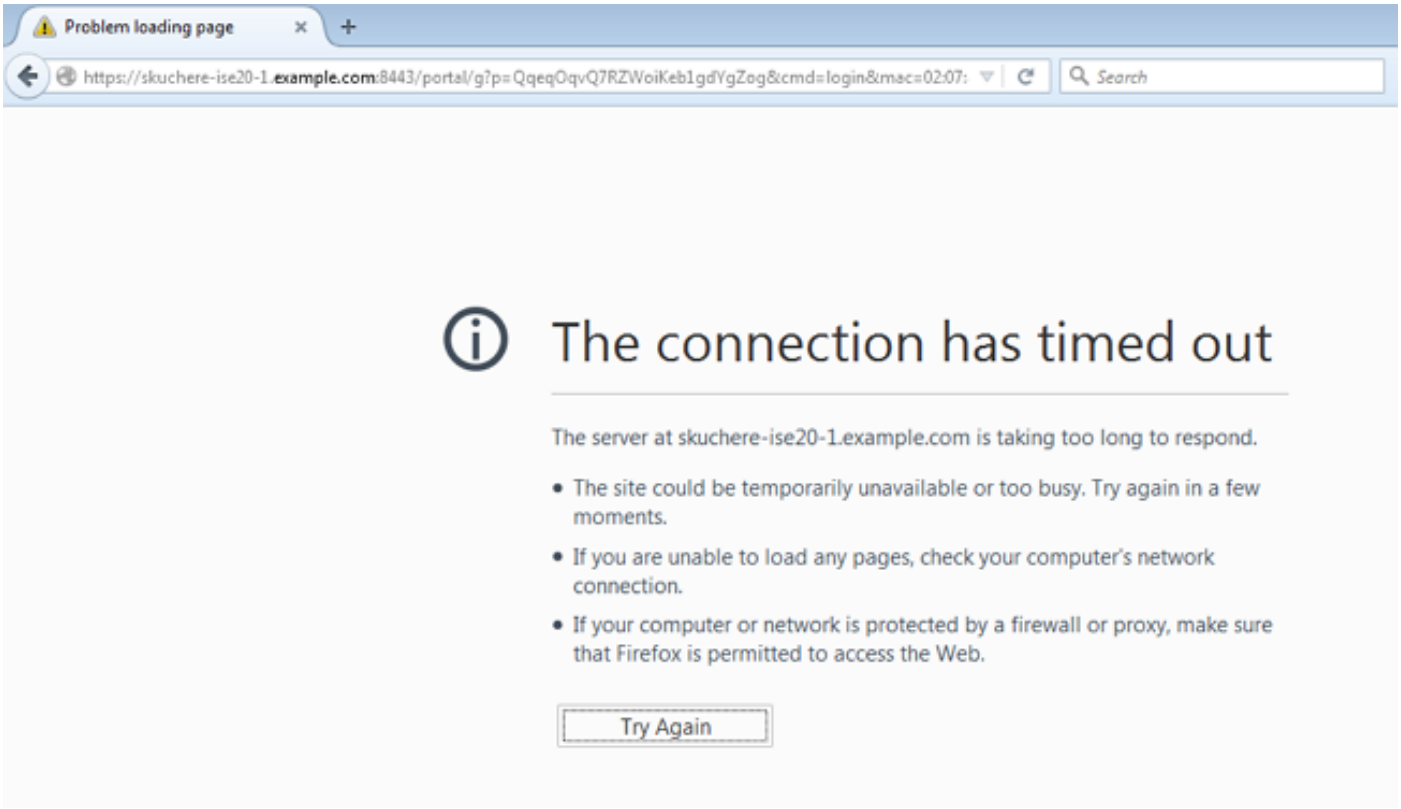
Устранение неполадок

Подведенный COA

В параметрах настройки ISE гарантируйте, что Аруба, NAD настроен с типом устройства нужной сети на стороне ISE и порту COA, правильно определена в параметрах настройки NAD. На Арубе сторона гарантирует, что RFC 3576 включен в параметрах настройки Сервера проверки подлинности, и порт COA определен правильно. От проверки точки зрения сети, что порт 3799 UDP позволен между WLC Арубы и ISE.

Проблема перенаправления

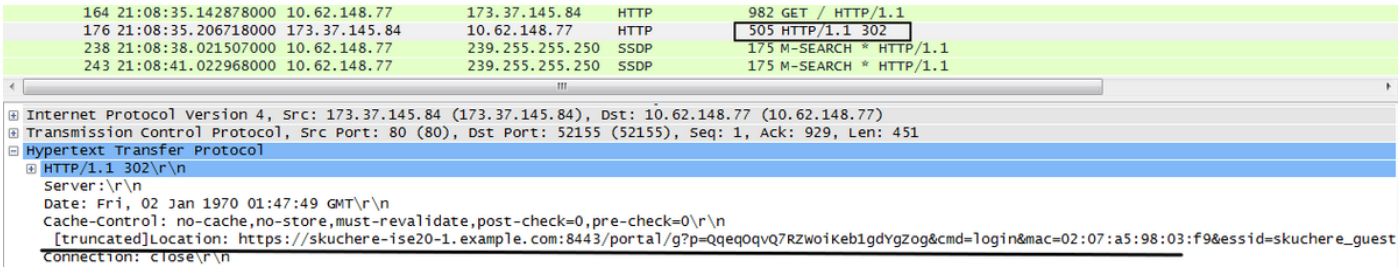
Пользователь видит URL ISE в браузере, но страница ISE не отображена, как показано в образе:



На стороне пользователя гарантируют, что ISE FQDN может быть успешно решен для исправления IP. На Арубе сторона проверяет, что URL ISE определен правильно в присоединенных настройках портала и трафике к ISE, позволенному в ограничениях доступа Роли пользователя. Aslo проверяют, что сервер RADIUS на SSID и PSN ISE в присоединенных настройках портала является тем же устройством. От проверки точки зрения сети, что порт TCP 8443 позволен от пользовательского сегмента до ISE.

Никакой подарок URL перенаправления в пользовательском браузере

На стороне пользователя гарантируют, что как результат каждого запроса HTTP WLC Арубы возвращается, HTTP кодируют 302 страницы, перемещенные с URL ISE.



Таймер сшивания сеанса истек

Типичный симптом этой проблемы - то, что пользователь перенаправлен во второй раз к гостевому порталу. В этом случае в Радиусе ISE Livelog необходимо видеть, что после COA для второго опознавательного профиля Авторизации с CWA был выбран снова. На стороне Арубы проверьте роль реального пользователя с помощью команды **клиентов показа**.

Как обходной путь для этой проблемы можно использовать основанную политику авторизации оконечной точки на ISE для соединений после успешной гостевой аутентификации.