# Содержание



# Введение

Этот документ описывает новые характеристики в платформе Identity Services Engine (ISE), которая позволяет перенаправлению иметь место со сторонними устройствами доступа к сети (NADs).

# Предварительные условия

## Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Гостевой поток на ISE
- DNS и протоколы DHCP

## Используемые компоненты

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

- Cisco Catalys коммутатор серии 2960
- Cisco ISE, выпуск 2.1

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.

# Общие сведения

Дополнительные характеристики как Гость, Положение и BYOD в современных сетях, требуют прямого соединения между устройством клиента и AAA-сервером. В предыдущих версиях ISE это было выполнено путем передачи динамического URL перенаправления и Списка контроля доступа (ACL) к NAD.

Существует два Обязательных атрибута, которые передаются в профиле авторизации за перенаправлением в значении атрибута Париж (AV):

- Пара значение-атрибут Cisco? URL перенаправления: значение URL является динамичным, и оно создано для каждого сеанса. Важные части URL перенаправления являются Узлом Сервиса Политики Классифицированное имя домена Fuly (PSN FQDN) и Идентификатор сеанса.
- Пара значение-атрибут Cisco? ACL перенаправления: Эта пара значение-атрибут содержит название ACL, которое должно существовать на NAD. С помощью этого ACL решает NAD, должны ли пакеты быть перенаправлены или позволены через NAD.

Традиционный подход перенаправления может только быть внедрен с Cisco устройства NAD. Для третьей стороны поддержка NAD статическое перенаправление URL было добавлено в ISE 2.0. В то время как этот подход более независим от платформы, он все еще требует поддержки перенаправления HTTP на NAD.

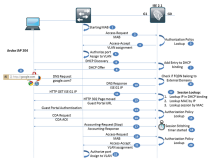
Начиная с ISE 2.1 был добавлен новый стиль перенаправления. Этот подход не требует поддержки перенаправления HTTP на NAD. Основная идея позади этого метода должна использовать ISE в качестве обрушения грунта DNS.

DNS и функциональная возможность сервера ' DHCP были добавлены к выпуску ISE 2.1 для использования его в качестве обрушения грунта DNS. Теперь сервер ISE может назначить IP-адреса на пользователей, которые должны быть перенаправлены и определить себя как сервер DNS. Это позволяет ISE перенаправлять подключения пользователя к себе без любой функциональности Web-сервера на NAD. Однако NAD должен все еще поддержать изменение авторизации (CoA) и динамическое назначение сетей VLAN.

В ISE этот подход может использоваться для этих потоков перенаправления:

- Гостевой поток: ISE отвечает на любой запрос DNS, инициируемый пользователем с собственным IP-адресом. Этот ответ заставляет клиента устанавливать соединение HTTP с ISE. В этом соединении возвращается ISE, URL перенаправления с помощью стандартного HTTP кодируют перемещенные 302 страницы.
- BYOD/Posture (Только Anyconnect)? в обоих сценариях, приложении Собственного соискателя, настраивающего (NSP) или модуле Положения Anyconnect инициирует соединение с enroll.cisco.com, который перенаправлен к ISE с помощью тех же шагов в качестве гостевого потока.

## Движение пакетов



1. NAD запускает процесс MAB для присоединенного устройства. Процесс MAB на коммутаторах Cisco запускается согласно приоритету метода аутентификации и не, прежде чем первый кадр будет принят от конечного устройства.
2. Access-request MAB передается ISE.
3. ISE оценивает политику проверки подлинности и авторизация для входящего запроса доступа. Во время оценки политики авторизации Тип Сетевого устройства (значение уровня NAD) по сравнению с типом Сетевого устройства, определенным в профиле авторизации. Только профили авторизации для Типа устройства соответствующей сети могут быть выбраны.

   **Примечание:** Для перенаправления Гостевого VLAN ISE должен выбрать профиль авторизации, которые содержат веб-Перенаправление (CWA, MDM, NSP, CPP) и назначение VLAN. Клиентская потребность, которая будет назначена на сегмент сети, который имеет ISE как единственный сервер DHCP.

1. ISE возвращает Access-Accept со сведениями о виртуальной локальной сети (VLAN).
2. Коммутатор авторизует порт и применяет Параметры VLAN.
3. Клиент инициирует DHCP, обнаруживают. Если ПК расположен в том же сегменте как ISE, пакет достигает ISE непосредственно. В случае подключения L3 между клиентом и ISE, IP ISE должен быть настроен как вспомогательный IP - адрес на NAD для ретранслятора DHCP.
4. ISE добавляет сведения о клиенте к своей таблице привязки DHCP. IP-адрес клиента и MAC используются ISE для поиска сеанса.
5. Предложение DHCP передается клиенту. В этом предложении IP-адрес ISE задан как сервер DNS.
6. Пользователь открывает web-браузер и перешел к google.com, который инициирует запрос DNS к ISE.
7. ISE проверяет, принадлежит ли целевой FQDN Внешним доменам. Если это делает, то ISE отправляет этот запрос к серверу DNS, определенному в параметрах настройки пула DHCP. Если не ISE возвращает собственный IP-адрес в ответ.
8. Web-браузер инициирует TCP - подключение к ISE и запросы о google.com.
9. На этом этапе ISE ищет аутентифицируемый сеанс для входящего HTTP-запроса GET. Это важно для построения корректного URL Перенаправления.

   **Примечание:** ISE использует эти правила для поиска сеанса:
   1. IP поиска в привязке DHCP
   2. MAC поиска IP
   3. Сеанс поиска MAC

1. ISE отвечает HTTP 302 страницы, перемещенные в URL перенаправления.
2. Пользователь таким образом перенаправлен к гостевому порталу, и весь гостевой поток, настроенный на ISE, имеет место здесь.
3. После успешной гостевой аутентификации ISE пробегает Политику авторизации еще раз, чтобы проверить, были ли какие-либо новые атрибуты добавлены к сеансу и если оконечная точка во время гостевого потока требует изменения авторизации (CoA). Как только следующая политика авторизации определена, ISE готовит запрос CoA.
4. Обмен CoA request/CoA ACK имеет место между ISE и NAD. Порт Возвращается или Сброс Admin, CoA - необходимость, поскольку это инициирует получение нового IP-адреса в заключительной VLAN. NAD должен поддержать Радиус или SNMP CoA для

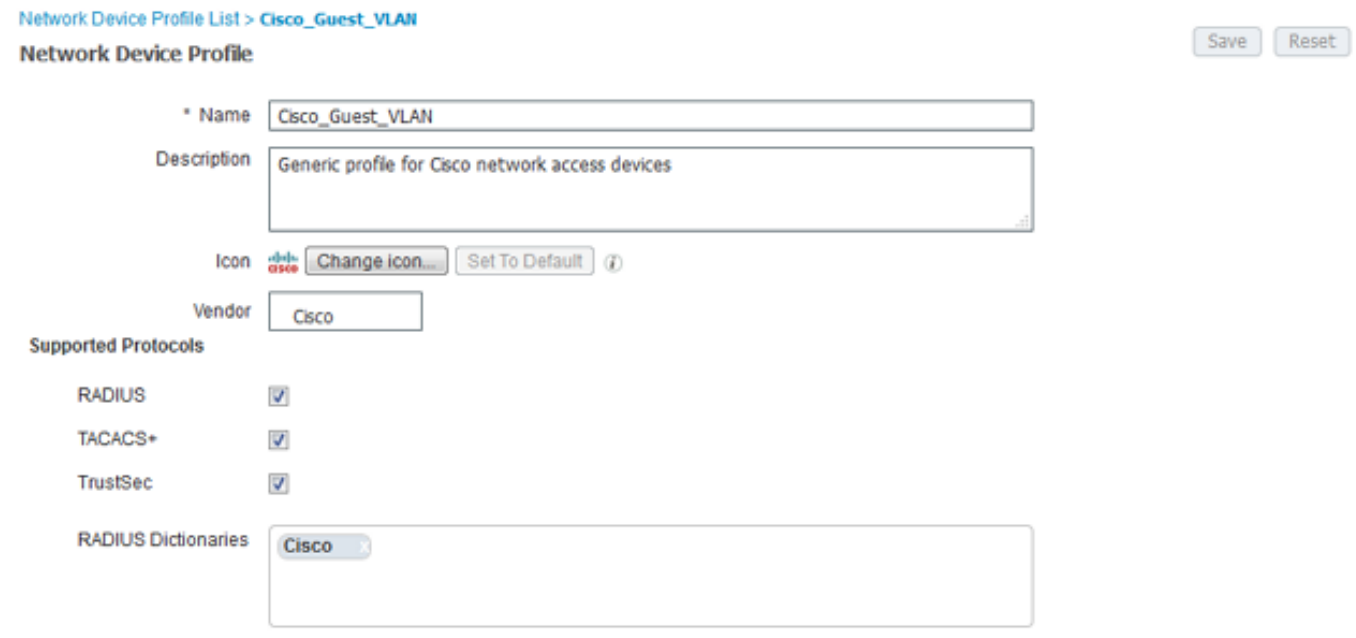
этого шага для работы.
5. Бухгалтерский запрос Останавливается для разъединенного сеанса, передается ISE. ISE подтверждает этот запрос путем передачи Бухгалтерского Ответа.
6. ISE запускает таймер сшивания сеанса (20 секунд по умолчанию). В это время все атрибуты сеанса (исключая: GUEST_TYPE, Использование case=Guest Поток), сохранены ISE. В случае, если новый запрос доступа о том же ID вызывающих станции получен в это время, все атрибуты сеанса связаны с новым сеансом.
7. Новый access-request MAB передается за конечным устройством после сильного удара порта CoA.
8. ISE определяет Аутентификацию/Политику авторизации для нового запроса. На этом этапе ISE использует атрибуты сеанса и/или атрибуты оконечной точки для корректного выбора политики.
9. Access-Accept передается с заключительными сведениями о виртуальной локальной сети (VLAN). Загружаемый список контроля доступа (DACL) может быть передан вместо этого, для ограничения трафика на виртуальной локальной сети (VLAN) по умолчанию также.
10. Коммутатор авторизует порт в новой VLAN и применяет DACL, если включено.

# Настройка

## Настройте ISE

### 1. Создайте профиль сетевого устройства

Для этого конкретного примера, коммутатор Cisco, используемый в качестве NAD. Поэтому существующий Профиль Сетевого устройства Cisco, дублированный и модифицируемый как требуется. Перейдите к администрированию> Сетевые ресурсы> Профили Сетевого устройства и добавьте новый профиль.




Перейдите к Администрированию> Сетевые ресурсы> Сетевые устройства и добавьте нового устройства.

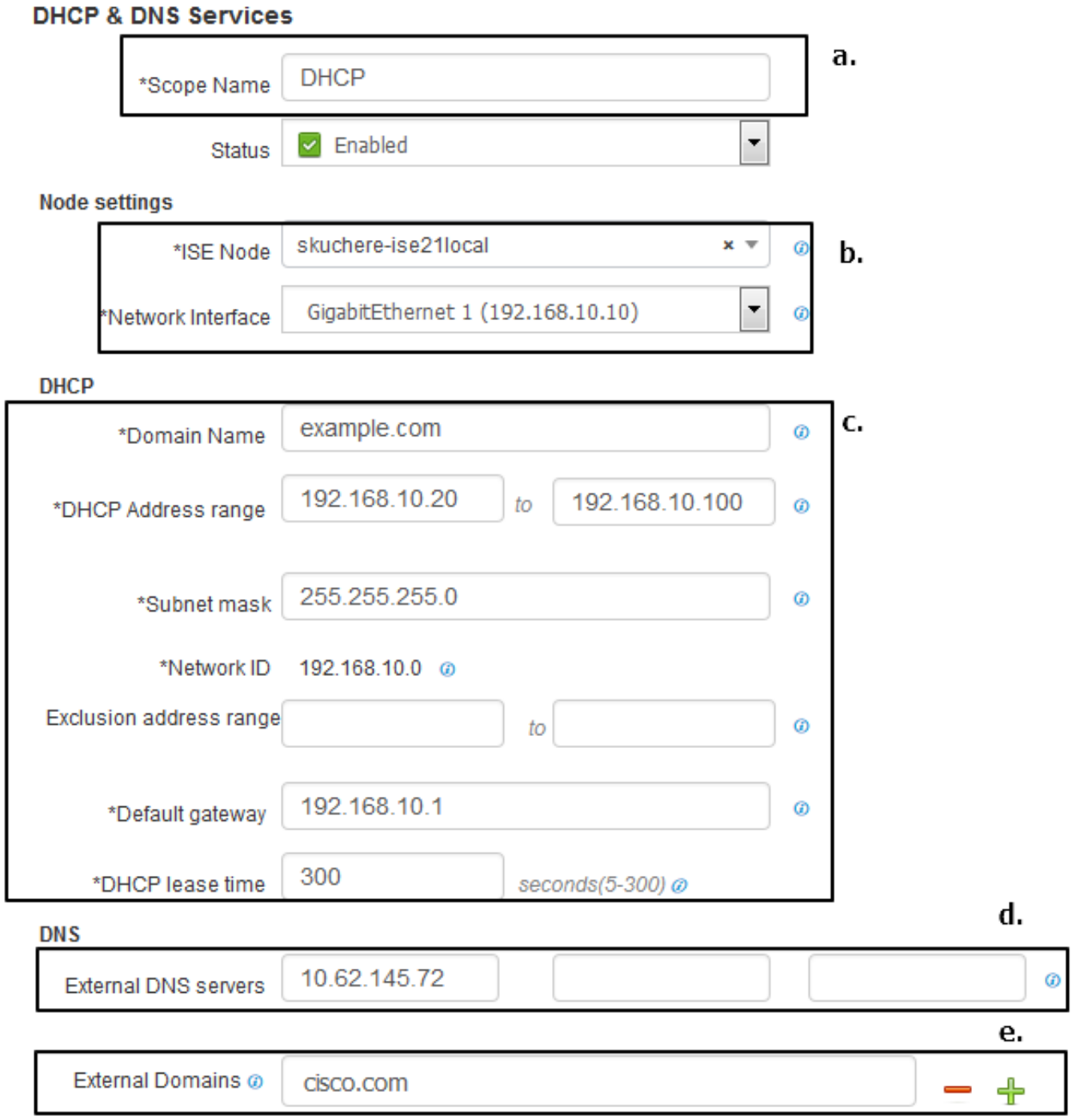
### 2. Создайте сетевое устройство

o. Обратите внимание на установку Профилем Сетевого устройства.

b. Все другие параметры настройки являются стандартными.

### 3. Настройте сервер DHCP

Пул сервера DHCP связан с определенным узлом ISE и его интерфейсом. Перейдите к администрированию> Система> Параметры настройки>, DHCP & DNS Services> Добавляет




o. Название области DHCP должно быть настроено.

**b.** Выберите узел, на который DNS и сервисы DHCP, которые должны работать и интерфейс на том узле, который должен использоваться.

**c .** Определите Диапазон IP-адресов DHCP, шлюз по умолчанию, адреса, исключенные из области и время аренды DHCP.

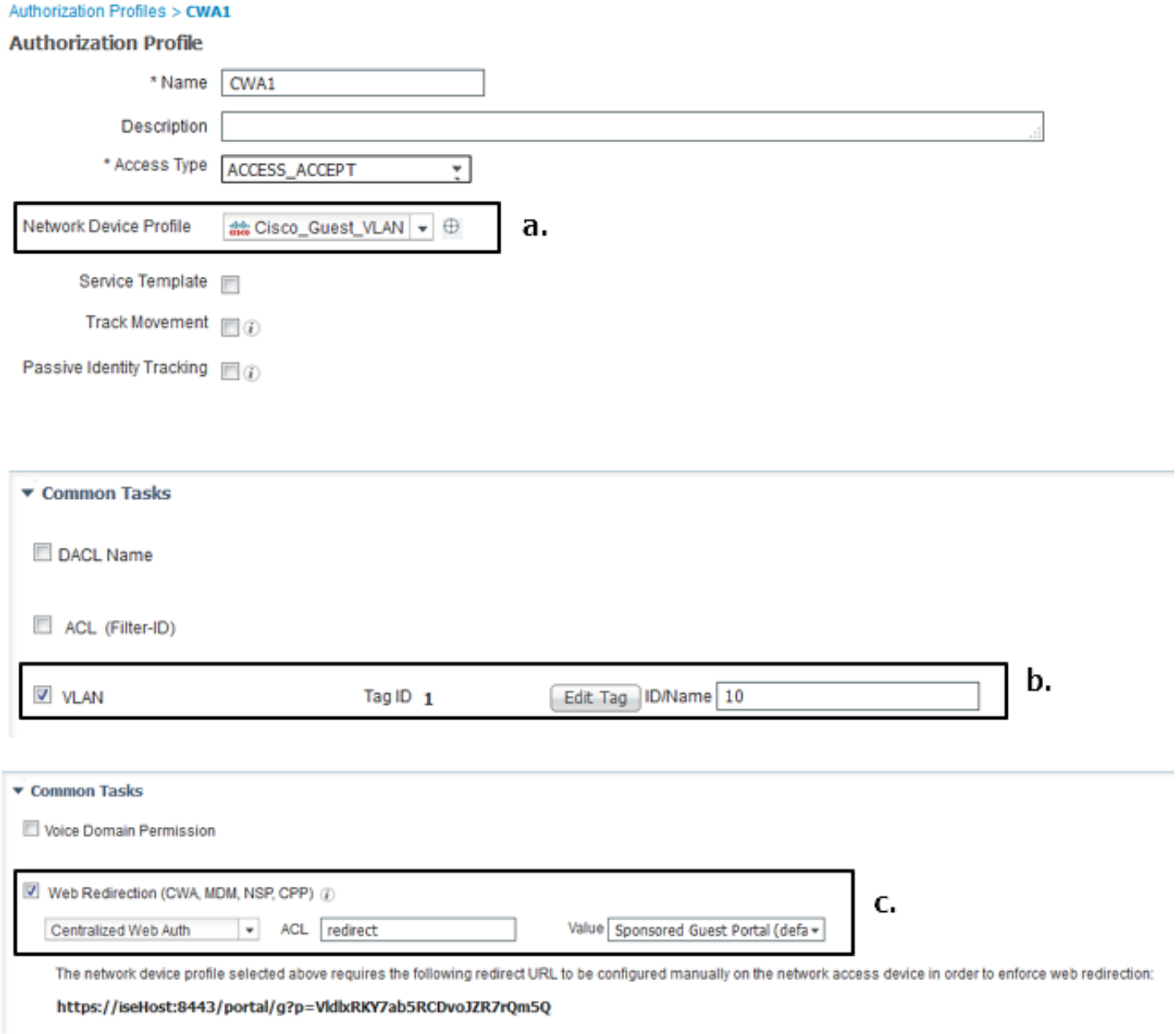
**d.** Дополнительно, определите внешние IP-адреса сервера DNS. Они нужно делать запрос для Внешних доменов.

**e.** Дополнительно, определите названия внешних доменов. ISE делает запрос внешних серверов DNS и возвращает фактический IP-адрес вместо его собственного.

### 4. Настройте профиль авторизации

Перейдите к Политике> Элементы Политики> Результаты> Авторизация> Профили Авторизации. Два профиля авторизации необходимы для завершенного гостевого потока:

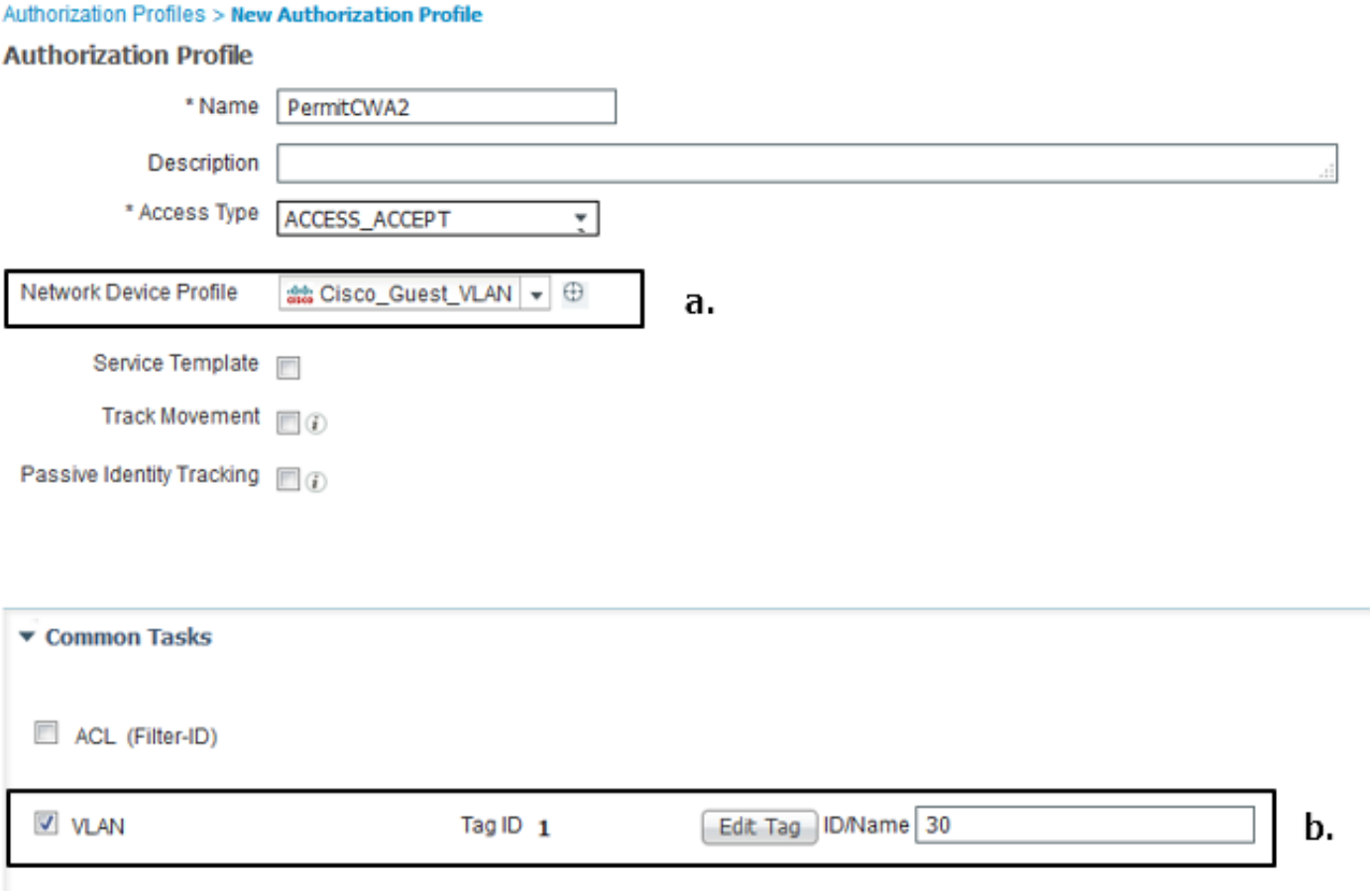
- Профиль авторизации перенаправления (CWA1)
- Разрешите профиль Авторизации доступа (PermitCWA2)



**o.** Профиль Сетевого устройства: Только запросы аутентификации, прибывающие из NADs, назначенного на этот профиль, могут привести к этому профилю авторизации,

**b.** Параметры VLAN: VLAN, определенные здесь, должны существовать на NAD. Интерфейс ISE, настроенный для DHCP, должен или принадлежать этой VLAN или если быть настроенным как IP - помощник на шлюзе, обслуживающем эту VLAN.

**c .** Параметры настройки перенаправления: Для текущего примера Центральная веб-аутентификация была определена как тип перенаправления и спонсируемый гостевой портал, определенный как гостевой портал. Форма все еще просит название ACL Перенаправления. Так как профиль сетевого устройства был реконфигурирован для статического перенаправления URL, это название ACL никогда не будет передаваться NAD.

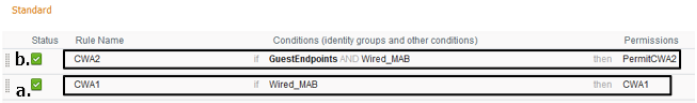



**o.** Профиль Сетевого устройства: Только запросы аутентификации, прибывающие из NADs, назначенного на этот профиль, могут привести к этому профилю авторизации,

**b.** Параметры VLAN: После присвоения порта клиента к этой VLAN пользователь должен получить IP-адрес от обычного сервера DHCP.

5. Настройте политику авторизации для гостевого доступа

Перейдите к Политике> Авторизация. Настройте две политики: один для действия перенаправления и другого для пользовательского доступа после аутентификации на Гостевом Портале.



**o.** Первые соответствия политики авторизации Проводной MAB как метод аутентификации и профиль авторизации перенаправления назначены в результате.

**b.** Вторая политика авторизации может базироваться любой на атрибутах сеанса (Вариант использования = Гостевой Тип Потока/Гостя / Внешняя AD группа, если гости аутентифицировали AD использования), или на атрибутах оконечной точки (Идентификационная группа оконечной точки). Регистрация устройства должна быть позволена на гостевом портале использовать Endpoint Identity Group.

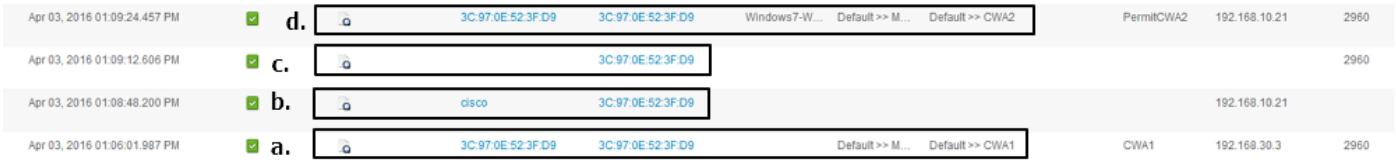
### Настройте NAD

Коммутатор Cisco был настроен для MAB на интерфейсе и имеет поддержку COA.

> **Примечание:** Центр технической поддержки Cisco (TAC) не предлагает поддержки конфигурации Независимого поставщика NADs.

## Проверка

Успешный гостевой поток похож на это в Операциях ISE> Радиус Livelog:




**o.** Это - первая аутентификация MAB. Профиль авторизации с перенаправлением выбран в результате.

**b.** Это - гостевая аутентификация. После того, как этот ISE действия делает переоценку политики, чтобы решить, необходим ли CoA.

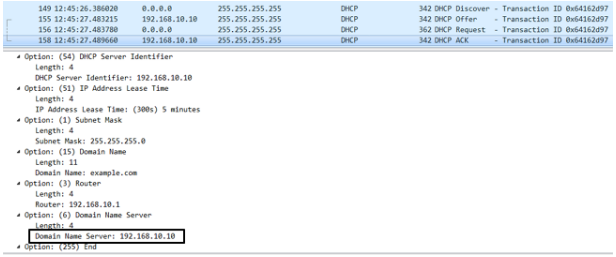
**c .** CoA был успешно завершен.

**d.** Это - вторая аутентификация MAB. Профиль авторизации для гостевого доступа выбран в результате.

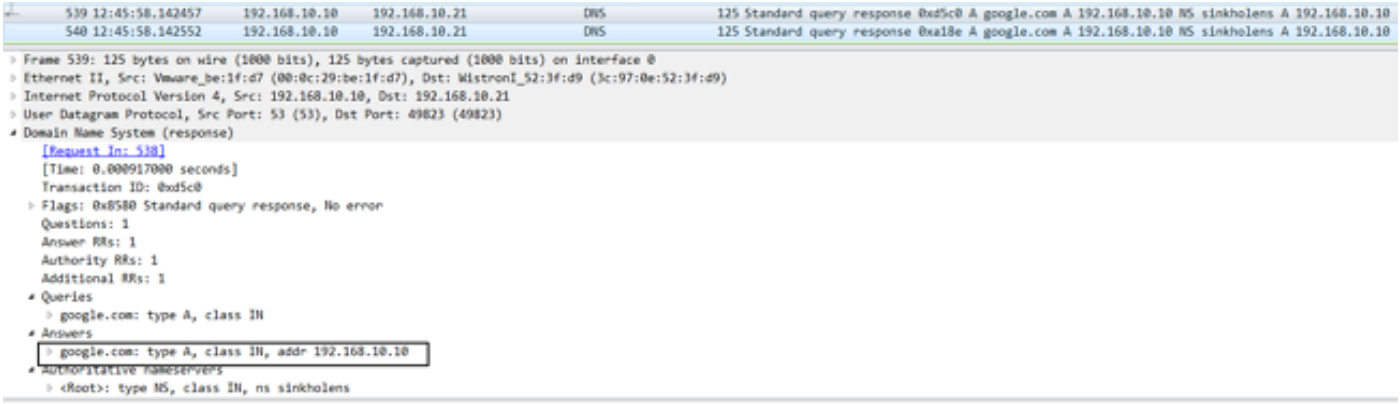
## Устранение неполадок

Проверьте, назначен ли IP-адрес на клиента правильно. Это может быть сделано путем сбора захвата пакета на клиенте или ISE.

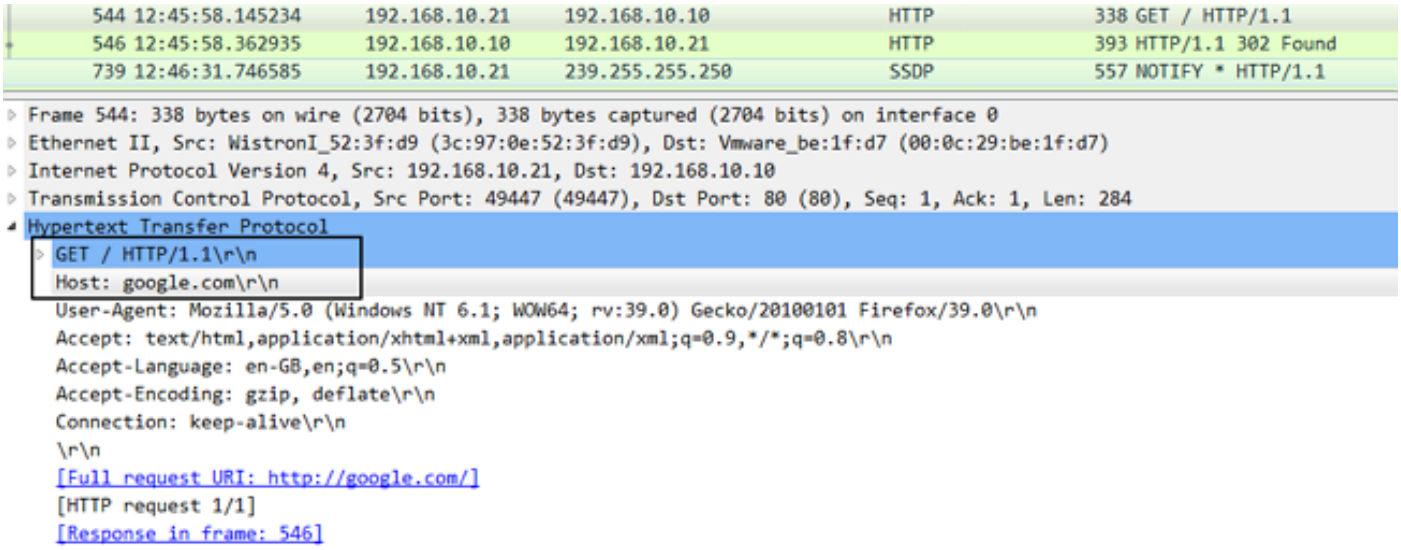
Этот перехват от клиента показывает успешное квитирование DHCP с IP DNS то же как ISE.



Проверьте, действует ли ISE должным образом как обрушение грунта DNS. Захват пакета может помочь подтверждать, переходит ли запрос к ISE и если ISE отвечает на него с собственным IP-адресом:




Проверьте, работает ли перенаправление HTTP должным образом. После того, как это получит IP-адрес ресурса и установит TCP - подключение к ISE, клиент передает HTTP-запрос GET к ISE. Это может быть подтверждено в захвате пакета клиентской стороны:




В то же время ISE определяет, существует ли какой-либо сеанс для этого клиента. Этот процесс поиска сеанса на ISE может быть проверен в журнале prrt-управления:

После поиска сеанса ISE возвращает URL перенаправления к клиенту в ответе HTTP 302: