Версия 1.3 ISE сам зарегистрированный гостевой пример конфигурации портала

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Топология и поток
Настройка
WLC
ISE
Проверка
Устранение неполадок
Необязательная конфигурация
Саморегистрационные параметры настройки
Гостевые параметры настройки входа в систему
Параметры настройки регистрации устройства
Гостевые параметры настройки соответствия устройства
Параметры настройки BYOD
Утвержденные спонсорами учетные записи
Отправьте Учетные данные через CM
Регистрация устройства
Положение
BYOD
Изменение VLAN
Дополнительные сведения

Введение

Платформа Cisco Identity Services Engine (ISE), Версия 1.3 имеет новый тип Гостевого Портала, вызванного Сам Зарегистрированный Гостевой Портал, который позволяет гостям саморегистрироваться, когда они получают доступ к сетевым ресурсам. Этот Портал позволяет вам настраивать и настраивать множественные функции. Этот документ описывает, как настроить и устранить неполадки этой функциональности.

Предварительные условия

Требования

Cisco рекомендует иметь опыт с конфигурацией ISE и базовыми знаниями об этих темах:

- Развертывания ISE и Гостевые потоки
- Конфигурация контроллеров беспроводной локальной сети (WLC)

Используемые компоненты

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

- Microsoft Windows 7
- Версия 7.6 WLC Cisco и позже
- Программное обеспечение ISE, версия 3.1 и позже

Топология и поток

Этот сценарий представляет составные опции, доступные гостям, когда они выполняют саморегистрацию.

Вот общий поток:

Шаг 1. Гость связывается к идентификаторам наборов сервисов (SSID): Гость. Это - открытая сеть с фильтрацией по MAC-адресам с ISE для аутентификации. Эта аутентификация совпадает со вторым правилом авторизации на ISE и перенаправлениях профиля авторизации Гостю Сам Зарегистрированный Портал. ISE возвращает Access-Accept RADIUS с двумя Cisco-av-pair:

- acl перенаправления URL (какой трафик должен быть перенаправлен, и название Списка контроля доступа (ACL), определенного локально на WLC),
- перенаправление URL (где перенаправить тот трафик - к ISE),

Шаг 2. Гость перенаправлен к ISE. Вместо того, чтобы предоставлять учетные данные для регистрации, пользователь нажимает "Do not have a account". Пользователь перенаправлен к странице, где может быть создана та учетная запись. Дополнительный секретный регистрационный код мог бы быть включен для ограничения саморегистрационной привилегии людьми, которые знают то секретное значение. После того, как учетная запись создана, пользователь является предоставленными учетными данными (имя пользователя и пароль) и входит с теми учетными данными.

Шаг 3. ISE передает изменение авторизации RADIUS (CoA), Повторно аутентифицируются на WLC. WLC проходит повторную проверку подлинности пользователя, когда он передает Access-Request RADIUS с атрибутом Только авторизования. ISE отвечает Access-Accept и ACL Airespace, определенным локально на WLC, который предоставляет доступ к Интернету только (заключительный доступ для гостя зависит от политики авторизации).

Обратите внимание на то, что для сеансов Протокола EAP, ISE должен передать CoA, Оконечный для инициирования повторной проверки подлинности, потому что сеанс EAP между соискателем и ISE. Но для MAB (фильтрация по MAC-адресам), Повторно аутентифицируются CoA, достаточно; нет никакой потребности к de-associate/de-authenticate

беспроводного клиента.

Шаг 4. . Гость желал доступа к сети.

Множественные дополнительные опции как положение и BYOD могут быть активированы (обсудил позже).

Настройка

WLC

1. Добавьте новый сервер RADIUS для Аутентификации и Учета. Перейдите к **Безопасности> AAA> Радиус> Аутентификация** для включения RADIUS CoA (RFC 3576).

   Существует подобная конфигурация для Учета. Также рекомендуется настроить WLC для передачи SSID в атрибуте ID Вызываемой станции, который позволяет ISE настраивать гибкие правила на основе SSID:

2. Под вкладкой WLAN создайте Беспроводную локальную сеть (WLAN) Гость и настройте Корректный Интерфейс. Набор безопасность Layer2 ни к **Одному** с фильтрацией по MAC-адресам. В Серверах Безопасности/¦утентификации, авторизации и учета (AAA) выберите IP-адрес ISE и для Аутентификации и для Учета. На Вкладке Дополнительно включите **Замену AAA** и установите Состояние Network Admission Control (NAC) в NAC RADIUS (поддержка CoA).

3. Перейдите к **Безопасности> Списки контроля доступа> Списки контроля доступа** и создайте два списка доступа:

   GuestRedirect, который разрешает трафик, который не должен быть перенаправлен и перенаправляет весь другой трафикИнтернет, который запрещен для корпоративных сетей и разрешен для всех других

   Вот пример для GuestRedirect ACL (должен исключить ISE к/ота трафика из перенаправления):

ISE

1. Перейдите к **Гостевому доступу>, Настраивают> Гостевые Порталы** и создают новый портала тип, Сам Зарегистрированный Гостевой Портал:

2. Выберите портала название, на которое сошлются в профиле авторизации. Заставьте все другие параметры настройки принимать значение по умолчанию. При Кастомизации Страницы портала могут быть настроены все представленные страницы.

3. Настройте профили Авторизации:

   Гость (с перенаправлением к Гостевому названию портала и ACL GuestRedirect)

   PermitInternet (с ACL Airespace равняются Интернету),

4. Для проверки правил авторизации перейдите к **Политике> Авторизация**. В Версии 1.3 ISE по умолчанию для отказавшего доступа Обхода проверки подлинности MAC (MAB) (MAC-адрес, не найденный), аутентификация продолжена (не отклоненный). Это очень полезно для Гостевых Порталов, потому что нет никакой потребности изменить что-либо в правилах проверки подлинности по умолчанию.

   Новые пользователи, которые связываются к Гостевому SSID, еще не являются частью никакой идентификационной группы. Это - то, почему они совпадают со вторым правилом, которое использует Гостевой профиль авторизации для перенаправления их к корректному Гостевому Порталу.

   После того, как пользователь создает учетную запись и входит успешно, ISE передает RADIUS CoA, и WLC выполняет повторную проверку подлинности. На этот раз с первым правилом совпадают наряду с профилем авторизации PermitInternet и возвращает название ACL, которое применено на WLC.

5. Добавьте WLC как Устройство Доступа к сети от **администрирования> Сетевые ресурсы> Сетевые устройства**.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

1. После того, как вы свяжетесь с Гостевым SSID и введете URL, тогда вы перенаправлены к странице входа:

2. Так как у вас еще нет учетных данных, необходимо ли выбрать **Do not have an account?** параметр. Новая страница, которая позволяет показы создания учетной записи. Если опция Registration Code была включена под Гостевой конфигурацией Портала, то секретное значение требуется (это гарантирует, что только людям с соответствующими разрешениями разрешают самозарегистрироваться).

3. Если существуют какие-либо проблемы с паролем или пользовательской политикой, перешли к **Гостевому доступу> Параметры настройки> Политика Пароля гостевого пользователя или Гостевой доступ> Параметры настройки> Гостевая Политика Имени пользователя** для изменения настроек. Например:

4. После успешного создания учетной записи вам предоставляют учетные данные (пароль, генерируемый согласно политике пароля гостевого пользователя):

5. Нажмите **Sign On** и предоставьте учетные данные (дополнительный Код доступа Доступа мог бы требоваться, если настроено под Гостевым Порталом; это - другой механизм обеспечения безопасности, который позволяет только тем, кто знает, что пароль входит).

6. Когда успешный, дополнительная политика допустимого использования (AUP) могла бы быть представлена (если настроено под Гостевым Порталом). Страница Access The Post (также конфигурируемый под Гостевым Порталом) могла бы также отобразиться.

   Последняя страница подтверждает, что был предоставлен доступ:

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

На данном этапе ISE представляет эти журналы:

Вот поток:

- Гость встречается со вторым правилом авторизации (Guest_Authenticate) и перенаправлен Гостю ("Auhentication, за которым следуют").

- Гость перенаправлен для саморегистрации. После успешно вход в систему (с недавно созданной учетной записью), ISE передает CoA, Повторно аутентифицируются, который подтвержден WLC ("Динамическая Авторизация, за которой следуют").

- WLC выполняет повторную проверку подлинности с атрибутом Только авторизования, и название ACL возвращено ("Только авторизование, за которым следуют"). Гость предоставлен доступ нужной сети.

Отчёты (**Операции> Отчёты> Отчёты о ISE> Отчёты о Гостевом доступе> Основной Гостевой Отчёт**) также подтверждают что:

Пользователь спонсора (с соответствующими полномочиями) в состоянии проверить текущий статус гостя.

Данный пример подтверждает, что учетная запись создана, но пользователь никогда не входил ("Ожидание Первоначального входа в систему"):

Необязательная конфигурация

Для каждого этапа этого потока могут быть настроены различные варианты. Все это настроено на Гостевой Портал в **Гостевом доступе>, Настраивают> Гостевые Порталы>, PortalName> Редактируют> Портала Поведение и параметры настройки потока**. Более важные параметры настройки включают:

Саморегистрационные параметры настройки

- Гостевой Тип - Описывает, сколько времени учетная запись активна, опции истечения пароля, часы регистрации и опции (это - смесь Профиля Времени и Роли guest от Версии 1.2 ISE),
- Регистрационный код - Если включено, только пользователям, которые знают секретный код, разрешают самозарегистрироваться (должен предоставить пароль, когда учетная запись создана),
- AUP - Принимает Политику Использования во время саморегистрации
- Требование для спонсора для утверждения гостевой учетной записи

Гостевые параметры настройки входа в систему

- Коду доступа - Если включено, только гости, которые знают секретный код, позволяют войти
- AUP - Принимает Политику Использования во время саморегистрации
- Опция изменения пароля

Параметры настройки регистрации устройства

- По умолчанию устройство зарегистрировано автоматически

Гостевые параметры настройки соответствия устройства

- Обеспечивает положение в потоке

Параметры настройки BYOD

- Позволяет корпоративным пользователям, которые используют портал в качестве гостей для регистрации их персональных устройств

Утвержденные спонсорами учетные записи

Если **Требовать, чтобы самозарегистрированные гости были утвержденной** опцией, выбрано, то учетная запись, созданная гостем, должна быть утверждена спонсором. Эта функция могла бы использовать электронную почту, чтобы отправить уведомление спонсору (для гостевого утверждения учетной записи):

Если сервер Протокола SMTP или по умолчанию из уведомления от электронной почты не будут настроены, то учетная запись не будет создана:

Журнал от guest.log подтверждает, что отсутствует глобальный от адреса, используемого для уведомления:

```
2014-08-01 22:35:24,271 ERROR [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null. A global default From address can be
configured in global settings for SMTP server.
```

Когда у вас есть надлежащая почтовая конфигурация, учетная запись создана:

После включения **Требовать, чтобы самозарегистрированные гости были утвержденной** опцией, поля имени пользователя и пароля автоматически удалены из **Того, чтобы включать эту информацию о** разделе **страницы Self-Registration Success**. Это - то, почему, когда утверждение спонсора необходимо, учетные данные для гостей не отображены по умолчанию на веб-странице, которая представляет информацию, чтобы показать, что была создана учетная запись. Вместо этого они должны быть отправлены Службами коротких сообщений (SMS) или электронной почтой. Эта опция должна быть включена в **учетном уведомлении Передачи после утверждения с помощью** раздела (отметьте ЭЛЕКТРОННУЮ ПОЧТУ/СМ).

Уведомление электронной почты отправлено спонсору:

Спонсор входит в портал Спонсора и утверждает учетную запись:

С этого момента гостю разрешают войти (с учетными данными, полученными по электронной почте или СМ).

Таким образом, существует три адреса электронной почты, используемые в этом потоке:

- Уведомление "От" адреса. Это определяется статически или берется от учетной записи спонсора и используется в качестве От адреса для обоих: уведомление спонсору (для утверждения) и учетные данные назначает в гостя. Это настроено под **Гостевым**

доступом>, Настраивают> Параметры настройки> Гостевые Параметры настройки Электронной почты.

- Уведомление адресу. Это используется, чтобы уведомить спонсора, что это получило учетную запись на утверждение. Это настроено в Гостевом Портале под **Гостевым доступом>, Настраивают> Гостевые Порталы>, Портала Name> Требует, чтобы самозарегистрированные гости были утверждены > Почтовый запрос на подтверждение к**.

- Гость "Для" адресации. Это предоставлено гостем во время регистрации. Если **Передают учетное уведомление после утверждения с помощью Электронной почты**, выбран, электронная почта с учетным подробным (именем пользователя и паролем) отправлена гостю.

Отправьте Учетные данные через СМ

Гостевые учетные данные могут быть также отправлены СМ. Эти опции должны быть настроены:

1. Выберите поставщика услуг СМ:

2. Проверьте **учетное уведомление Передачи после использования утверждения:** флажок **SMS**.

3. Затем гостя просят выбрать доступного поставщика, когда он создает учетную запись:

4. СМ отправлен с выбранным поставщиком и номером телефона:

5. Можно настроить Поставщиков СМ при **администрировании> Система> Параметры настройки> СМ шлюз**.

Регистрация устройства

Если **Позволять гости для регистрации параметра Выберите устройства** выбраны после того, как гость входит и принимает AUP, можно зарегистрировать устройства:

Заметьте, что устройство было уже добавлено автоматически (оно идет, Управляют Списком устройств). Это вызвано тем, что **Автоматически зарегистрируйтесь, гостевые устройства** был выбран.

Положение

Если **Потребовать гостевая** опция **соответствия устройства** выбрана, то гости настроены с Агентом, который выполняет положение (Агент NAC/Сети) после того, как они входят и принимают AUP (и дополнительно выполните регистрацию устройства). ISE обрабатывает Клиента, Настраивающего правила решить, какой Агент должен быть настроен. Затем Агент, который работает на станции, выполняет положение (согласно правилам Положения) и передает результаты к ISE, который передает CoA, повторно аутентифицируются для изменения статуса авторизации в случае необходимости.

Возможные правила авторизации могли бы выглядеть подобными этому:

Первые новые пользователи, которые встречаются с перенаправлением правила Guest_Authenticate к Сам Гостевой портал Регистра. После того, как пользователь саморегистрируется и входит, статусу авторизации изменений CoA и пользователю предоставляют ограниченный доступ для выполнения положения и исправления. Только после того, как Агент NAC настроен, и станция совместима, делает статус авторизации изменения CoA еще раз для обеспечения доступа к Интернету.

Типичные проблемы с положением включают отсутствие корректного Клиента, Настраивающего правила:

Это может также быть подтверждено при исследовании guest.log файла (новый в Версии 1.3 ISE):

```
2014-08-01 21:35:08,435 ERROR [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

Если **Позволять сотрудники для использования персональных устройств на параметре Network** выбраны, то корпоративные пользователи, которые используют этот портал, могут пройти BYOD, текут и регистрируют персональные устройства. Для гостей та установка ничего не изменяет.

Что делает "сотрудников, использующих портал в качестве гостя" среднее значение?

По умолчанию гостевые порталы настроены с идентификационным хранилищем **Guest_Portal_Sequence**:

Это - внутренняя последовательность хранилища, которая судит Внутренних пользователей сначала (перед Гостями):

Когда на данном этапе на гостевом портале, пользователь предоставляет учетные данные, которые определены в хранилище Внутренних пользователей, и перенаправление BYOD происходит:

Таким образом, корпоративные пользователи могут выполнить BYOD для персональных устройств.

Когда вместо учетных данных Внутренних пользователей, учетные данные Гостей

предоставлены, обычный поток продолжен (никакой BYOD).

Изменение VLAN

Это - подобная опция к изменению VLAN, настроенному для Гостевого Портала в Версии 1.2 ISE. Это позволяет вам выполнять activeX или приложение Java, которое инициирует DHCP, чтобы освободить и возобновить. Когда CoA инициирует изменение VLAN для оконечной точки, это необходимо. Когда MAB используется, оконечная точка не знает об изменении VLAN. Возможное решение должно изменить VLAN (DHCP освобождают/возобновляют) с Агентом NAC. Другая опция должна запросить, чтобы новый IP-адрес через апплет возвратился на веб-странице. Задержка между release/CoA/renew может быть настроена. Эта опция не поддерживается для мобильных устройств.

Дополнительные сведения

- Сервисы положения на Руководстве по конфигурации Cisco ISE
- Беспроводной BYOD с платформой Identity Services Engine
- SCEP ISE поддерживает для Примера конфигурации BYOD
- Cisco ISE 1.3 руководства администратора
- Центральная веб-аутентификация на WLC и примере конфигурации ISE
- Центральная веб-аутентификация с AP FlexConnect на WLC с примером конфигурации ISE
- Cisco Systems – техническая поддержка и документация