Настройте беспроводные сети ISE CWA и потоки хот-спота с WLC AireOS и следующего поколения

Содержание

Введение

Этот документ описывает, как настроить три гостевых варианта использования в Механизме Identity Services (ISE) с Cisco AireOS и Следующим поколением (NGWC) Контроллеры беспроводной локальной сети (WLC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Контроллеры беспроводной локальной сети Cisco (Объединенный и сходившийся доступ)
- Платформа Identity Services Engine (ISE)

Используемые компоненты

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

- Версия 2.1 Платформы Cisco Identity Services Engine
- Контроллер WLAN Cisco 5508 выполнений 8.0.121.0
- Контроллер беспроводной локальной сети следующего поколения (NGWC) catalyst 3850 (WS-C3850-24P) выполнение 06.03.04. E

Настройка

Схема сети

Шаги, покрытые этим документом, описывают типичную конфигурацию и на Унифицированных и на Сходившихся WLC Доступа для поддержки любого Гостевого потока с ISE.

Настройте объединенный 5508 WLC

Независимо от варианта использования, настроенного в ISE, с точки зрения WLC, все это запускается с беспроводной оконечной точки, которая соединяется с Открытым SSID с включенной фильтрацией по MAC-адресам (Плюс замена AAA и NAC RADIUS), который указывает к ISE как аутентификация и учетный сервер. Это гарантирует, что ISE может динамично выдвинуть необходимые атрибуты к WLC для успешного осуществления перенаправления к Гостевому Порталу ISE.

Глобальная конфигурация

1. Добавьте ISE глобально как Аутентификацию и Учетный сервер.

- Перейдите к **Безопасности> AAA> Аутентификация** и нажмите **New**

- Введите IP - сервер ISE и общий секретный ключ
- Гарантируйте, что Состояние сервера и **Поддержка RFC 3676** (Изменение поддержки Авторизации или CoA) оба установлены во **Включенный**.
- Под server timeout по умолчанию WLC AireOS будут иметь 2 секунды. В зависимости от сетевых характеристик (задержка, ISE и WLC в других местоположениях, и т.д.) это может быть выгодно для увеличения server timeout по крайней мере до 5 секунд для предотвращения ненужных событий аварийного переключения.
- **Щелкните "Применить".**
- Если существуют Узлы Сервисов несколька правил (PSN) для настройки, продолжают создавать дополнительные серверные записи.

Примечание: Этот пример определенной конфигурации включает 2 экземпляра ISE

- Перейдите к **Безопасности> AAA> RADIUS> Учет** и нажмите **New**
- Введите IP - сервер ISE и Общий секретный ключ
- Гарантируйте, что Состояние сервера установлено во Включенный
- Увеличьте server timeout, если необходимый (по умолчанию составляет 2 секунды).

2. Конфигурация нейтрализации.

В унифицированной среде, как только server timeout инициирован шаги WLC к следующему настроенному серверу. Затем в линии от WLAN. Если никто другой не доступен тогда, WLC выбирает следующий в списке глобальных серверов. Когда несколька адресов серверов настроены на SSID (Основной, Вторичный, и т.д.), как только аварийное переключение происходит, WLC по умолчанию продолжает передавать аутентификацию и (или) бухгалтерский трафик постоянно к Вторичному экземпляру, даже если основной сервер вернулся онлайн.

Для смягчения этого поведения , включают нейтрализацию. Перейдите к **Безопасности> AAA> RADIUS> Нейтрализация.** Поведение по умолчанию выключено. Единственный способ восстановиться с события server-down требует вмешательства admin (глобально возвращаются административный статус сервера).

Для включения нейтрализации, у вас есть две опции:

- **Пассивный-** В пассивном режиме, если сервер не отвечает на запрос аутентификации WLC, WLC перемещает сервер к неактивной очереди и устанавливает таймер (Интервал в опции Sec). Когда таймер истекает, WLC перемещает сервер к активной очереди независимо от реального состояния серверов. Если запрос аутентификации приводит к событию истечения времени ожидания (что означает, что сервер все еще не работает), серверная запись перемещена снова к Неактивной очереди, и таймер умирает снова. Если сервер успешно отвечает назад, это остается в Активной очереди. Настраиваемые значения здесь идут с 180 до 3600 секунд.

- **Активный -** В активном режиме, когда сервер не отвечает на запрос аутентификации WLC, WLC отмечает сервер как мертвый, затем перемещается, сервер к неактивному серверу объединяют, и начинает передавать тестовые сообщения периодически, пока не отвечает тот сервер. Если сервер отвечает, то WLC перемещает неработающий сервер в активный пул и прекращает передавать тестовые сообщения.

В этом режиме WLC требует, чтобы вы ввели имя пользователя и тестовый интервал в секундах (180 - 3600).

> **Примечание:** Зонд WLC не требует успешной аутентификации. Так или иначе успешное или ошибки проверки подлинности считают ответом сервера, которого является достаточно для продвижения сервера Активную очередь.

Настройте идентификаторы наборов сервисов (SSID) гостя:

- Перейдите к вкладке WLAN, и под Create New опция нажимает **Go**:
- Введите название SSID и Имя профиля. **Щелкните "Применить".**
- Под Вкладкой Общие выбирают Interface или Interface Group, который будет использоваться (Гостевой VLAN).
- Под **Безопасностью> Уровень 2> безопасность уровня 2** выбирает **None** и включает флажок **Mac Filtering**.
- Под **AAA Servers** вкладка установила Аутентификацию и Учетные серверы к **включенному** и выбирает вашего основного и дополнительные серверы.
- **Промежуточное Обновление**: Это - произвольная конфигурация, которая не добавляет преимуществ к этому потоку. Если вы предпочитаете включать его, WLC, я должен работать 8.x или более высокий код:

Отключенный: опция полностью отключена.

Включенный с 0 Интервалами: WLC передает бухгалтерские обновления ISE каждый раз, когда существует изменение в записи Контрольного блока мобильной станции (MSCB) клиента (ie. IPv4 или присвоение адреса IPv6 или изменение, событие роуминга клиента, и т.д.), Никакие дополнительные периодические обновления не отосланы.

Включенный с настроенным Промежуточным Интервалом: В этом режиме WLC передает уведомления ISE на изменения записи MSCB клиента, и это также передает дополнительные периодические бухгалтерские уведомления в заданном интервале (независимо от любых изменений).

- Под Вкладкой Дополнительно Включают**, Позволяют, что Замена AAA** и Под **состоянием NAC** выбирает **RADIUS NAC**. Это гарантирует, что WLC применяет любые пары значений атрибутов (AVP), которые прибывают из ISE.
- Перейдите к вкладке Общие SSID и установите статус SSID во **Включенный**
- **Примените** изменения.

Настройте ACL перенаправления

На этот ACL ссылается ISE, и это определяет, какой трафик перенаправлен и какой трафик будет позволен через.

- Перейдите **к Вкладке Безопасность> Списки контроля доступа** и нажмите **New**

- Это - пример ACL

Этот ACL должен предоставить доступ к и от сервисов DNS и узлов ISE по порту TCP 8443. Существует неявное, запрещают в нижней части, которая означает, что остаток трафика перенаправлен к Гостевому URL Портала ISE.

Перенаправление HTTPS

Эта функция поддерживается в версиях AireOS 8.0.x и но она выключена по умолчанию. Для включения поддержки HTTPS переходят **к менеджменту** WLC> **HTTPS HTTP> Перенаправление HTTPS** и устанавливают его во **Включенный** или применяют эту команду в CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Предупреждения сертификата после перенаправления HTTPS включены

После того, как перенаправление https включено, пользователь может испытать проблемы доверия сертификата во время перенаправления. Это замечено, даже если существует допустимый цепочечный сертификат на контроллере и даже если этот сертификат подписан доверенным центром сертификации третьей стороны. Причина состоит в том, что сертификат , установленный на WLC, выполнен к его имени хоста Виртуального интерфейса или IP-адресу. Когда клиент попробует https://cisco.com, браузер ожидает, что сертификат будет выполнен к cisco.com. Однако для WLC, чтобы быть в состоянии перехватить GET, выполненный клиентом, это сначала должно установить сеанс HTTPS , для которого WLC представляет свой Сертификат Виртуального интерфейса во время фазы подтверждения связи SSL. Это заставляет браузер отображать предупреждение, поскольку сертификат, представленный во время подтверждения связи SSL, не был выполнен к исходному веб-сайту, клиент пытается обратиться (ie. cisco . com, настроенный против имени хоста Виртуального интерфейса WLC). Вы могли бы видеть другие сообщения об ошибках сертификата в других браузерах, но все касаются той же проблемы.

Агрессивное аварийное переключение

Эта опция активирована по умолчанию в WLC AireOS. Когда агрессивное аварийное переключение включено, WLC отмечает AAA-сервер как безразличный, и это перемещается в следующий настроенный AAA-сервер после того, как событие истечения времени ожидания РАДИУСА влияет на одного клиента.

Когда опция отключена переключения при отказе WLC к следующему серверу, только если событие истечения времени ожидания RADIUS происходит по крайней мере с 3 сеансами клиента. Эта опция может быть отключена этой командой (Никакая перезагрузка не требуется для этой команды):

```
(Cisco Controller) >config radius aggressive-failover disable
```

Проверить текущий статус функции:

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
```

```
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Присоединенный обход

Оконечные точки, которые поддерживают механизм Присоединенного помощника по работе в сети (CNA), чтобы обнаружить присоединенный портал и автозапустить страницу регистрации обычно, делают это через псевдобраузер в управляемом окне, в то время как другие оконечные точки запускают полностью способный браузер для инициирования этого. Для оконечных точек, где CNA запускает псевдобраузер, это может сломать поток , когда перенаправлено к присоединенному порталу ISE. Это, как правило, влияет на устройства IOS Apple, и это имеет особенно негативные эффекты в потоках, которые требуют регистрации устройства, DHCP-Rlease VLAN, проверки соответствия, и т.д.

В зависимости от сложности потока в использовании можно рекомендовать включить Присоединенный Обход. В таком сценарии WLC игнорирует механизм обнаружения портала CNA, и клиент должен открыть браузер для инициирования процесса перенаправления.

Проверьте статус функции:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect  ..... Disable
Web Auth Captive-Bypass   ..... Disabled
Web Auth Secure Web  ..... Enable
Web Auth Secure Redirection  ..... Enable
```

Для включения этой опции вводят эту команду:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

WLC предупреждает пользователя, что для изменений для вступления в силу необходима система сброса (перезапуск).

На этом этапе **show network summary** показывает функцию, как включено, но для изменений для вступления в силу должен быть перезапущен WLC.

Настройте сходившийся 3850 NGWC

Глобальная конфигурация

1. **Добавьте ISE глобально как Аутентификацию и Учетный сервер**

- Перейдите к**> Security Конфигурации> RADIUS> Серверы** и нажмите **New**
- Введите **IP-адрес сервера** ISE, **общий секретный ключ**, **server timeout** и **Число повторов**, которое отражает ваши условия среды.
- Гарантируйте, что включена **Поддержка RFC 3570** (поддержка CoA).

- Повторите процесс для добавления записи Дополнительного сервера.

2. **Создайте группу серверов ISE**

   - Перейдите к**> Security Конфигурации> Группы серверов** И нажмите **New**
   - Назначьте название к группе и введите значение **Deadtime** в минутах. Это - время, когда контроллер поддерживает сервер в Неактивной очереди, прежде чем это будет продвинуто снова на список активного сервера.
   - От Доступных Серверов список добавляют их к Назначенному Столбцу серверов.

3. **Глобально включите Dot1x**

   - Перейдите к **Конфигурации> AAA> Списки методов> Общий** и включите **системный Контроль за Аутентификацией Dot1x**

4. **Настройте списки методов**

   - Перейдите к **Конфигурации> AAA> Списки методов> Аутентификация** и создайте новый Список методов. В этом случае это - Тип Dot1x и Группа ISE_Group (группа, созданная в предыдущем шаге). Затем соответствие **Применяется**

   - Сделайте то же для учета (**Конфигурация> AAA> Списки методов> считающий**) и Авторизация (**Конфигурация> AAA> Списки методов> Авторизация**). Они должны быть похожими на это

5. **Создайте метод фильтра MAC авторизации**.

Это вызывают от параметров настройки SSID позже.

- Перейдите к **Конфигурации> AAA> Списки методов> Авторизация** и нажмите **New**.
- Введите **имя списка методов**. Выбрал **тип = Network and Group Type Group**.
- Добавьте ISE_Group к полю Assigned Server Groups.

Конфигурация SSID

1. **Создайте гостевой SSID**

   - Перейдите к **Конфигурации> беспроводные сети> WLAN** и нажмите **New**
   - Введите ИДЕНТИФИКАТОР WLAN, SSID и Имя профиля и нажмите Apply.
   - Однажды в параметрах настройки SSID под Интерфейсом / Интерфейсная группа выбирают Guest VLAN Layer 3 interface.

   - Под **Безопасностью> Уровень 2** выбирает **None**, и следующий за **фильтрацией Mac** вводят Имя Списка методов Фильтра Mac, которое вы ранее настроили (Макфилтерметод).
   - Под **Безопасностью>** Вкладка **AAA-сервера** выбирают правильную проверку подлинности и списки Методов учета (ISE_Method).

   - Под **Вкладкой Дополнительно** включают**, Позволяют Замену AAA** и **состояние NAC.** Остаток параметров настройки должен быть отрегулирован согласно каждым

развертываниям требования (превышение времени ожидания сеанса, Клиентское Исключение, Поддержка Расширений Aironet, и т.д.).

- Перейдите к Вкладке Общие, устанавливает Статус во Включенный. Затем соответствие **Применяется.**

Конфигурация списков управления доступом (ACL) перенаправления

На этот ACL ссылается ISE позже в access-accept в ответ на начальный запрос MAB. NGWC использует его для определения, какой трафик перенаправить и какой трафик должен быть позволен через.

- Перейдите к**> Security конфигурации> ACL> Списки контроля доступа** и **нажмите Add New**.
- Выберите Extended и введите Имя ACL.
- Это изображение показывает пример типичного ACL Перенаправления:

  Примечание: Линия 10 является дополнительной. Это обычно добавляется для устранения проблем, делает предложение. Этот ACL должен предоставить доступ к DHCP, сервисы DNS и также к порту TCP 8443 серверов ISE (Запретите ACE). Трафик HTTP и Трафик HTTPS перенаправлены (ACE Разрешения).

Конфигурация интерфейса командной строки (CLI)

Вся конфигурация, обсужденная в предыдущих шагах, может также быть применена через CLI.

802.1x Глобально включен

```
dot1x system-auth-control
```

Глобальная конфигурация AAA

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 14.36.157.210 server-key *****
 client 14.36.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 14.36.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 14.36.157.21 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
```

```
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

WLAN Configuration

```
 wlan Guest 1 Guest
 aaa-override
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

Пример ACL перенаправления

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 14.36.157.210 eq 8443
    60 deny tcp any host 14.36.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

HTTP и поддержка HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

Примечание: При применении ACL для ограничения доступа к WLC по HTTP, это влияет на перенаправление.

Настройте ISE

В этом разделе описываются конфигурацию, требуемую на ISE поддерживать все случаи использования, обсужденные в этом документе.

Общие задачи конфигурации ISE

1. Вход в систему к ISE и перешел к **администрированию> Сетевые ресурсы> Сетевые устройства** и **нажмите Add**

2. Введите **Имя**, привязанное к WLC и **IP-адресу** устройства.
3. Установите флажок **параметров настройки Проверки подлинности RADIUS** и введите **Общий секретный ключ**, настроенный на стороне WLC. **Затем щелкните Submit (Отправить).**

4. Перейдите к **Политике>, Аутентификация** и под **MAB** нажимает **Edit** и гарантирует что при **Использовании: Внутренние Оконечные точки**, которые опция**, Если пользователь не найден**, собирается **Продолжить** (Это должно быть там по умолчанию).

Вариант использования 1: CWA С Гостевой Аутентификацией в каждом подключении пользователя

Обзор потока

1. Пользователь беспроводной связи соединяется с Гостевым SSID.
2. WLC аутентифицирует оконечную точку на основе своего MAC-адреса с помощью ISE в качестве AAA-сервера.
3. ISE возвращается назад и access-accept с двумя Парами значений атрибутов (AVP): перенаправление URL и acl перенаправления URL. Как только WLC применяет это AVP к сеансу оконечной точки, переходы станции к Требуемому от DHCP и как только это захватывает IP-адрес, это остается в CENTRAL_WEB_AUTH. При этом шаге WLC готов начать перенаправлять http клиента / трафик HTTPS.
4. Конечный пользователь открывает web-браузер и однажды трафик HTTP, или Трафик HTTPS генерируется, WLC перенаправляет пользователя к гостевому порталу ISE.
5. Как только пользователь добирается до Гостевого Портала, он побуждает вводить гостевые учетные данные (созданный спонсорами в этом случае).
6. На учетные данные ISE проверки отображает страницу AUP и как только клиент принимает, Динамический тип CoA Проходят повторную проверку подлинности , отослан в WLC.
7. WLC повторно обрабатывает аутентификацию фильтрации по MAC-адресам, не выполняя de-authenticate к мобильной станции. Это должно быть бесшовным к оконечной точке.
8. Как только случай повторной проверки подлинности происходит, ISE переоценивает Политику авторизации, и на этот раз оконечной точке предоставляют доступ Разрешения, так как было предыдущее успешное гостевое событие аутентификации.

Этот процесс повторяет себя каждый раз пользовательские подключения к SSID.

!--- конфигурацию

1. Перейдите к ISE и перейдите для **Работы Центров>, Гостевой доступ> Настраивает>, Гостевые Порталы>** Выбирают **Sponsored Guest Portal** (или создайте нового портала Спонсируемого Гостя типа).
2. При **Госте** параметры настройки **Регистрации устройства** сняли флажок со всеми опциями и нажимают **Save**.

3. Перейдите к **Политике> Элементы Политики> Результаты> Авторизация> Профили Авторизации**. **Нажмите Add.**

4. Этот профиль оттолкнут к WLC **URL Перенаправления** и **ACL URL ПЕРЕНАПРАВЛЕНИЯ** в ответ на начальный запрос Обхода аутентификации Mac (MAB).

- Однажды **веб-перенаправление (CWA, MDM, NSP, CPP)** проверенный выбирают **Centralized Web Auth**, затем Вводят имя ACL Перенаправления под полем **ACL**, и под **Значением** выбирают **Спонсируемый Гостевой Портал (по умолчанию)** (или любой другой определенный портал, созданный в предыдущих шагах).

Профиль должен выглядеть подобным тот в этом изображении. Затем нажмите **Save**.

Подробные данные атрибута внизу страницы Пары значений атрибутов (AVP), как они быть выдвинутыми к WLC

5. Перейдите к **Политике> Авторизация** и вставьте новое правило. Это правило является тем, которое инициирует процесс перенаправления в ответ на начальный запрос проверки подлинности MAC от WLC. (В этом случае названный **Wireless_Guest_Redirect**).

6. При **Условиях** выбирают **Select Existing Condition from Library**, затем при **условии, название** выбирает **условие Compound**. Выберите предустановленное составное условие по имени **Wireless_MAB**.

> **Примечание:** Это условие состоит из 2 атрибутов RADIUS, ожидаемых в инициируемом Запросе Доступа, формируют WLC (Port-type NAS = IEEE 802.11 <подарок во всех беспроводных запросах> и Service-Type = Проверка Вызова <который обращается к конкретному запросу для обхода аутентификации Mac>),

7. Под результатами выберите **Standard> CWA_Redirect** (Профиль Authorization, созданный в предыдущем шаге). Затем нажмите **Done** и **Save**

8. Перейдите до конца **CWA_Redirect**, управляют и нажимают стрелку рядом с **Редактированием**. Затем выберите **копию выше**.

9. Модифицируйте название, поскольку это - политика, с которой совпадает оконечная точка, как только сеанс пройден повторную проверку подлинности на CoA ISE (В этом случае Wireless_Guest_Access).

10. Рядом с щелчком условия составного объекта **Wireless_MAB +** символ для расширения условий и к концу условия **Wireless_MAB нажмите Add Атрибут/Значение**.

11. Под “Выбирают Атрибут”, выбрал **Network Access> поток UseCase Equals Guest**

12. В соответствии с **Разрешениями** выбирают **PermitAccess**. Затем нажмите **Done** и **Save**

Эти две политики должна выглядеть подобной этому:

Вариант использования 2: CWA с Регистрацией устройства, принуждающей гостевую аутентификацию один раз в день.

Обзор потока

1. Пользователь беспроводной связи соединяется с Гостевым SSID.
2. WLC аутентифицирует оконечную точку на основе своего MAC-адреса с помощью ISE в качестве AAA-сервера.
3. ISE возвращается назад и access-accept с двумя Парами значений атрибутов (AVP) (перенаправление URL и acl перенаправления URL).
4. Как только WLC применяет это AVP к сеансу оконечной точки, переходы станции к Требуемому от DHCP и как только это захватывает IP-адрес, это остается в CENTRAL_WEB_AUTH. При этом шаге WLC готов начать перенаправлять http клиента / трафик HTTPS.
5. Конечный пользователь открывает web-браузер и однажды трафик HTTP, или Трафик HTTPS генерируется, WLC перенаправляет пользователя к гостевому порталу ISE.
6. Как только пользователь добирается до Гостевого Портала, ему предлагают ввести созданные спонсорами учетные данные.
7. На учетные данные ISE проверки добавляет эту оконечную точку к определенной (предварительно сконфигурированной) Endpoint Identity Group (Регистрация устройства).
8. Страница AUP отображена и как только клиент принимает, Динамический тип CoA Проходят повторную проверку подлинности. Отослан в WLC.
9. WLC, чтобы повторно обработать аутентификацию фильтрации по MAC-адресам, не выполняя de-authenticate к мобильной станции. Это должно быть бесшовным к оконечной точке.
10. Как только случай аутентификации ре происходит, ISE переоценивает Политику авторизации. На этот раз, так как оконечная точка является участником правильного ISE Endpoint Identity Group, возвращается, доступ принимают без ограничений.
11. Так как оконечная точка была зарегистрирована в шаге 6, каждый раз, когда пользователь возвращается, ему разрешают в сети, пока это не удалено вручную из ISE, или Политика Чистки Оконечной точки выполняет сбрасывание оконечных точек, соответствующих критериям.

В этом лабораторном сценарии аутентификация принуждена один раз в день. Триггер повторной проверки подлинности является Политикой Чистки Оконечной точки, которая удаляет все оконечные точки используемой Endpoint Identity Group каждый день.

> **Примечание:** Возможно принудить гостевое событие аутентификации на основе Времени работы (астрономического) начиная с последнего принятия AUP. Если необходимо принудить Гостевой Вход в систему чаще что один раз в день (в примере каждые 4 часа), это может быть опцией.

!--- конфигурацию

1. На ISE перешли для **Работы Центров>, Гостевой доступ> Настраивает>, Гостевые Порталы>** Выбирают **Sponsored Guest Portal** (или создайте нового портала Спонсируемого Гостя типа).
2. При **Госте** параметры настройки **Регистрации устройства** проверяют, что **опция Automatically регистрируется, гостевые устройства** проверен. **Нажмите Save.**

3. Перейдите для **Работы центра>, Гостевой доступ> Настраивает> Гостевые Типы** или просто щелкает по ярлыку, заданному при Гостевых Параметрах настройки Регистрации устройства в портале.

4. Когда Пользователь Спонсора создает гостевую учетную запись, он назначает гостевой тип на нее. Каждый отдельный Гостевой Тип может иметь зарегистрированную оконечную точку, которая принадлежит другой Endpoint Identity Group. Для присвоения Endpoint Identity Group, устройство должно быть добавлено к, выбрать Guest Type использование спонсора для этих гостей (Этот вариант использования основывается Еженедельный (по умолчанию)).

5. Однажды в гостевом типе, под **Опциями Входа в систему** выбирают Endpoint Group от **Идентификационной группы Оконечной точки** выпадающего меню **для гостевой регистрации устройства**

6. Перейдите к **Политике> Элементы Политики> Результаты> Авторизация> Профили Авторизации**. **Нажмите Add.**

7. Этот профиль оттолкнут к WLC **URL Перенаправления** и **ACL URL ПЕРЕНАПРАВЛЕНИЯ** в ответ на начальный запрос Обхода аутентификации Mac (MAB).

- Однажды **веб-перенаправление (CWA, MDM, NSP, CPP)** проверенный выбирают **Centralized Web Auth**, затем Вводят имя ACL Перенаправления под полем **ACL**, и под **Значением** выбирают портал, созданный для этого потока **(CWA_DeviceRegistration)**.

8. Перейдите к **Политике> Авторизация** и вставьте новое правило. Это правило является тем, которое инициирует процесс перенаправления в ответ на начальный запрос проверки подлинности MAC от WLC. (В этом случае названный **Wireless_Guest_Redirect**).

9. При **Условиях** выбрал **Select Existing Condition from Library**, затем при **условии, название** выбирает **условие Compound**. Выберите предустановленное составное условие по имени **Wireless_MAB**.

10. Под результатами выберите **Standard> CWA_DeviceRegistration** (Профиль Authorization, созданный в предыдущем шаге). Затем нажмите **Done** и **Save**

11. Копируйте политику выше, модифицируйте ее название, поскольку это - политика соответствия оконечной точки после того, как это возвращается из события повторной проверки подлинности (названный Wireless_Guest_Access).

12. Под **Подробной** коробкой **Identity Group** выберите **Endpoint Identity Group** и выберите группу, на которую вы сослались под Гостевым Типом (GuestEndpoints).

13. Под Результатами выбирают **PermitAccess**. Нажмите **Done** и **сохраните** изменения.

14. Создайте и политика чистки оконечной точки, которая ежедневно очищает GuestEndpoint Group.

- Перейдите к **администрированию> Управление идентификацией> Параметры настройки> Чистка Оконечной точки**
- По правилам **Чистки** должно быть то по умолчанию, которое инициирует удаление GuestEndpoints, если Время работы (астрономическое) больше, чем 30 дней.
- Модифицируйте существующую политику для GuestEndpoints или создайте новый (в случае, если по умолчанию был удален). Обратите внимание на то, что политика чистки, выполняемая каждый день заданное время.

В этом случае условие является Участниками GuestEndpoints с Прошедшими Днями меньше

чем 1 день

Вариант использования 3: портал HostSpot

Обзор потока

1. Пользователь беспроводной связи соединяется с Гостевым SSID.
2. WLC аутентифицирует оконечную точку на основе своего MAC-адреса с помощью ISE в качестве AAA-сервера.
3. ISE возвращает назад access-accept с двумя Парами значений атрибутов (AVP): перенаправление URL и acl перенаправления URL.
4. Как только WLC применяет это AVP к сеансу оконечной точки, переходы станции к Требуемому от DHCP и как только это захватывает IP-адрес, это остается в CENTRAL_WEB_AUTH. При этом шаге WLC готов перенаправить http клиента / трафик HTTPS.
5. Конечный пользователь открывает web-браузер и однажды трафик HTTP , или Трафик HTTPS генерируется, WLC перенаправляет пользователя к Порталу ISE HotSpot.
6. Однажды в портале пользователю предлагают принять политику допустимого использования.
7. ISE добавляет MAC-адрес оконечной точки (Идентификатор оконечной точки) в Идентификационную группу настраиваемой оконечной точки.
8. Узел Policy Services (PSN), который обрабатывает запрос, выполняет Динамический тип CoA**, Перезагруженный Admin** к WLC.
9. Как только WLC заканчивает обрабатывать входящий CoA, он выполняет de-authenticate клиенту (соединение является потерей в течение времени, которое требуется для клиента для возвращения).
10. Как только клиент воссоединяется, новый сеанс создан, таким образом, нет никакой непрерывности сеанса на стороне ISE. Это означает, что аутентификация обработана как новый поток.
11. Так как оконечная точка добавлена к настраиваемой оконечной точке Identity Group, и существует Политика авторизации, которая проверяет, является ли оконечная точка частью той группы, новая аутентификация совпадает с этой политикой. Результатом является полный доступ к Гостевой сети.
12. Пользователю не придется принять AUP снова, пока Объект Identity Оконечной точки не очищен от базы данных ISE в результате политики чистки оконечной точки.

!--- конфигурацию

1. Создайте New Endpoint Identity Group для перемещения этих устройств в после регистрации. Перейдите для **Работы Центров> Гостевой доступ> Identity Groups> Endpoint Identity Groups** и щелчок .

- Введите имя группы (В этом случае HotSpot_Endpoints). Добавьте описание, и никакая Parent Group не необходима.

2. Перейдите для **Работы Центров>, Гостевой доступ> Настраивает>, Гостевые Порталы>** выбирают **Hotspot Portal (по умолчанию)**.

3. Разверните Настройки портала, и под Endpoint Identity Group выбирают группу **HostSpot_Endpoints** под **Endpoint Identity Group.** Это передает зарегистрированные

устройства указанной группе.

4. Сохраните изменения.

5. Создайте профиль Авторизации, который называет Портал HotSpot на аутентификацию MAB инициируемым WLC.

- Перейдите к **Политике> элементы Политики> Результаты> авторизация> Профили Авторизации** и создайте один (HotSpotRedirect).
- Как только **веб-перенаправление (CWA, MDM, NSP, CPP)** проверено, выбирают **Hot Spot**, затем вводят имя ACL Перенаправления в поле ACL (Guest_Redirect) и как Значение выбирает корректный портал (**Портал Хот-спота (по умолчанию)**).

6. Создайте Политику авторизации, которая инициирует результат HotSpotRedirect после начального запроса MAB от WLC.

- Перейдите к **Политике> Авторизация** и вставьте новое правило. Это правило является тем, которое инициирует процесс перенаправления в ответ на начальный запрос проверки подлинности MAC от WLC. (В этом случае названный **Wireless_HotSpot_Redirect**).
- При **Условиях** выбирают **Select Existing Condition from Library**, затем при **условии, название** выбирает **условие Compound**
- Под результатами выберите **Standard> HotSpotRedirect** (Профиль Authorization, созданный в предыдущем шаге). Затем нажмите **Done** и **Save**

7. Создайте вторую Политику авторизации.

- Копируйте политику выше, модифицируйте ее название, поскольку это - политика соответствия оконечной точки после того, как это возвращается из события повторной проверки подлинности (названный Wireless_HotSpot_Access).
- Под **Подробной** коробкой **Identity Group** выберите **Endpoint Identity Group** и затем группу, которую вы создали более ранний **(HotSpot_Endpoints)**.
- Под Результатами выбирают **PermitAccess**. Нажмите **Done** и **сохраните** изменения.

8. Настройте политику чистки, которая очищает оконечные точки со Временем работы (астрономическим), больше, чем 5 дней.

- Перейдите к **администрированию> Управление идентификацией> Параметры настройки>, Чистка Оконечной точки** и по правилам Чистки создает новое.
- Под **Identity Group Подробная** коробка выбирают **Endpoint Identity Group> HotSpot_Endpoints**
- При **условиях** нажимают **Create New Condition (Advanced Option)**.
- Под Выбирают Attribute, выбирают *ENDPOINTPURGE: дни ElapsedDays GREATERTHAN 5*

Проверка

Вариант использования 1

1. Пользователь соединяется с Гостевым SSID.
2. Он открывает браузер и как только трафик HTTP генерируется, гостевой портал отображен.
3. Как только гость аутентифицирует и принимает AUP, страница успеха отображена.
4. Проходить повторную проверку подлинности CoA отослан (очевидный для клиента).
5. Сеанс оконечной точки пройден повторную проверку подлинности с полным доступом к сети.
6. Любое последующее гостевое соединение должно передать гостевую аутентификацию прежде, чем получить доступ к сети.

Вытекайте из RADIUS ISE Оперативные журналы:

Вариант использования 2

1. Пользователь соединяется с Гостевым SSID.
2. Он открывает браузер и как только трафик HTTP генерируется, гостевой портал отображен.
3. Как только гость аутентифицирует и принимает AUP, устройство зарегистрировано.
4. Страница успеха отображена, и Проходить повторную проверку подлинности CoA отослан (очевидный для клиента).
5. Сеанс оконечной точки пройден повторную проверку подлинности с полным доступом к сети.
6. Любое последующее соединение порыва 9 с, позволенных, не принуждая гостевую аутентификацию пока оконечная точка, находится все еще в Идентификационной группе настраиваемой оконечной точки.

Вытекайте из RADIUS ISE Оперативные журналы:

Вариант использования 3

1. Пользователь соединяется с Гостевым SSID.
2. Он открывает браузер и как только трафик HTTP генерируется, страница AUP отображена.
3. Как только гость принимает AUP, устройство зарегистрировано.
4. Страница успеха отображена, и Перезагруженный Admin CoA отослан (очевидный для клиента).
5. Оконечная точка повторно соединяется с полным доступом с сетью.
6. Любое последующее соединение порыва позволено, не принуждая принятие AUP (пока иначе не настроен) столько, сколько оконечная точка остается в Идентификационной группе настраиваемой оконечной точки.

Локальный коммутатор FlexConnect в AireOS

Когда локальный коммутатор FlexConnect настроен потребности Сети Admin гарантировать что:

- ACL перенаправления настроен как FlexConnect ACL.
- ACL перенаправления был применен как политика так или иначе через сам AP под Вкладкой **FlexConnect> Внешние ACL WebAuthentication>, Политика>** Выбирает Redirect

ACL и нажимает **Apply**

Или путем добавления ACL Политики к FlexConnect Group принадлежит (**беспроводные сети>, FlexConnect Groups>** Выбирает корректную группу**> Сопоставление ACL>, Политика** Выбирает Redirect ACL и нажмите Add),

Добавление ACL политики инициирует WLC для оттолкнутого настроенного ACL участникам AP FlexConnect Group. Сбой, чтобы сделать это приводит к веб-проблеме перенаправления.

Сценарий внешний привязки

В сценариях (Внешних Привязки) автопривязки важно выделить следующие факты:

- ACL перенаправления должен быть определен и на Внешнем и на WLC Привязки. Даже когда это только принуждено на Привязке.
- Аутентификация уровня 2 всегда обрабатывается Внешним WLC. Это важно во время стадий проектирования (также для устранения проблем) как вся Проверка подлинности RADIUS, и бухгалтерский трафик происходит между ISE и внешним WLC.

- Как только AVP Перенаправления применены к сеансу клиента, Внешний WLC обновляет сеанс клиента в Привязке через мобильность handoff сообщение.
- На этом этапе WLC Привязки начинает принуждать Перенаправление с помощью ACL Перенаправления, который был предварительно сконфигурирован.
- Учет должен быть полностью выключен на SSID WLC Привязки, чтобы избежать считать обновления, идущие к ISE (ссылающийся на то же опознавательное событие) прибывающий и от Привязки и Внешний.
- URL базировался, ACL не поддерживаются в сценариях Внешних Привязки.

Устранение неполадок

Общие нарушенные состояния и на AireOS и на Сходившемся WLC Доступа

1. **Клиент неспособен присоединиться к Гостевому SSID**

“**Показывают, что клиент детализировал xx:xx:xx:xx:xx:xx**”, показывает, что клиент застревает в **ЗАПУСКЕ**. Обычно это - индикатор неспособности WLC для применения атрибута, который возвращает AAA-сервер.

Проверьте, что название ACL Перенаправления, выдвинутое ISE, совпадает точно с названием предустановленного ACL на WLC.

Тот же принцип применяется к любому другому атрибуту, который вы настроили ISE для оттолкнутого к WLC (ИДЕНТИФИКАТОРЫ VLAN, Имена интерфейсов, ACL Airespace, и т.д.). Клиент должен тогда перейти к DHCP и затем CENTRAL_WEB_AUTH.

2. **AVP перенаправления применены к сеансу клиента, но не работает перенаправление**

Проверьте, что менеджер политики клиента, состояние является CENTRAL_WEB_AUTH с действительным IP - адресом согласно настроенному динамическому интерфейсу для SSID и также что ACL Перенаправления и атрибуты Перенаправления URL применены к сеансу клиента.

ACL перенаправления

В WLC AIreOS ACL перенаправления должен явно позволить трафик, который не должен быть перенаправлен, как DNS и ISE на Порте TCP 8443 в обоих направлениях, и неявные запрещают, что перенаправлен ip любой любой триггерный остаток трафика.

На Установившемся доступе логика является противоположным. Запретите перенаправление обходов ACE, в то время как ACE разрешения инициируют перенаправление. Это - то, почему рекомендуется явно разрешить порт TCP 80 и 443.

Проверьте доступ к ISE по порту 8443 от гостевого VLAN. Если все выглядит хорошим с точки зрения конфигурации, самый легкий способ продвинуться состоит в том, чтобы захватить перехват позади беспроводного адаптера клиента и проверить, где ломается перенаправление.

- Разрешение DNS происходит?
- Этапное установление связи TCP 3 закончено против запрошенной страницы?
- WLC возвращает действие перенаправления после того, как клиент будет инициировать GET?
- Этапное установление связи TCP 3 против ISE - более чем 8443 завершенные?

3. **Клиент неспособен обратиться к сети после того, как ISE выдвинул изменение VLAN в конце гостевого потока**

Как только клиент захватил IP-адрес в начале потока (Пред состояние Перенаправления), если изменение VLAN оттолкнуто после того, как Гостевая аутентификация происходит (перенесите CoA, проходят повторную проверку подлинности), единственный способ вызвать выпуск DHCP / возобновляют в Гостевом потоке (без агента положения), через Java-апплет, которые в мобильных устройствах не работают.

Это оставляет клиента помещенным в черный список в VLAN X с IP-адресом VLAN Y. Это нужно рассмотреть при планировании решения.

4. **ISE показывает “внутреннюю ошибку HTTP 500, сеанс Радиуса, не найденный” сообщение в Гостевом браузере клиента во время перенаправления**

Это обычно - индикатор потери сеанса на ISE (сеанс был завершен). Когда Внешняя Привязка была развернута, наиболее распространенная причина этого считает настроенным на WLC Привязки. Для решения проблемы это отключает учет на Привязке и оставляет Внешнюю Аутентификацию маркера и Учет.

5. **Клиент разъединяет и остается разъединенным или соединяется с другим SSID после принятия AUP в портале HotSpot ISE**.

Это может ожидаться в HotSpot из-за Динамического изменения Авторизации (CoA), вовлеченный в этот поток (Сброс CoA Admin), который заставляет WLC выполнять deauth к терминалу беспроводной связи. У большинства беспроводных оконечных точек нет проблем для возвращения к SSID после того, как de-authenticate произойдет, но в некоторых случаях клиентские подключения к другому предпочтительному SSID в ответ на de-authenitcate событие. Ничто не может быть сделано от ISE или WLC для предотвращения этого, как это до беспроводного клиента, чтобы придерживаться исходного SSID или соединиться с другим доступным (предпочтительным) SSID.

В этом случае пользователь беспроводной связи должен вручную соединиться назад с

HotSpot SSID.

AireOS WLC

(Cisco Controller) >debug client <MAC addr>
Отладьте клиентские наборы к DEBUG ряд компонентов, вовлеченных в изменения Машины Состояния клиента.

(Cisco Controller) >debug client <MAC addr>
Компоненты Debug AAA

(Cisco Controller) >debug client <MAC addr>
Это может быть ресурсами влияния в зависимости от количества пользователей, которые соединяются через SSID Dot1X или MAB. Эти компоненты в Уровне отладки делают запись транзакций AAA между WLC и ISE и распечатывают Пакеты RADIUS на экране.

Это важно, если вы, что ISE может не отправить ожидаемые атрибуты, или если WLC не обрабатывает их правильно.

Веб-подлинное перенаправление

(Cisco Controller) >debug client <MAC addr>
Это может использоваться, чтобы проверить, что WLC успешно инициирует перенаправление. Это - пример того, как перенаправление должно быть похожим от отладок:

(Cisco Controller) >debug client <MAC addr>

NGWC

Отладьте клиентские наборы к DEBUG ряд компонентов, вовлеченных в изменения Машины Состояния клиента.

(Cisco Controller) >debug client <MAC addr>
Этот компонент распечатывает Пакеты RADIUS (Аутентификация и Считающий) на экране. Это удобно, когда необходимо проверить, что ISE отправляет правильные AVP и также проверить, что CoA передается и обрабатывается правильно.

(Cisco Controller) >debug client <MAC addr>
Это будет все переходы AAA (аутентификация, авторизация и учет), где вовлечены беспроводные клиенты. Это важно, чтобы проверить, что WLC анализирует правильно AVP и применяет их к сеансу клиента.

(Cisco Controller) >debug client <MAC addr>
Это может, включил , когда вы подозреваете проблему перенаправления на NGWC.

(Cisco Controller) >debug client <MAC addr>

ISE

RADIUS Оперативные журналы

Проверьте, что начальный запрос MAB был обработан правильно в ISE, и тот ISE пододвигает ожидаемые атрибуты обратно. Перейдите к **Операциям> RADIUS>**

Оперативные журналы и фильтруйте выходные данные с помощью MAC - адреса клиента под **Идентификатором оконечной точки**. Как только опознавательное мероприятие учреждено, щелкните по подробным данным и затем проверьте Результаты, выдвинутые как часть принятия.

TCPDUMP

Эта функция может быть использована, когда более глубокое изучает обмен Пакета RADIUS между ISE, и WLC необходим. Таким образом, можно доказать, что ISE передает корректные атрибуты в access-accept , не имея необходимость включать отладки на стороне WLC. Для начала перехвата с помощью TCDDump перешли к **Операциям> Устранение неполадок> Инструменты диагностики> Общие средства> TCPDump.**

Это - пример корректного потока, перехваченного через TCPDump

Вот AVP, передаваемые в ответ на начальный запрос MAB (второй пакет в снимке экрана выше).

```
(Cisco Controller) >debug client <MAC addr>
```

Отладки оконечной точки:

Если необходимо погрузиться глубже в процессы ISE, которые включают решения о применении политики, портала выбор, гостевую аутентификацию, обработку CoA, и т.д. самый легкий способ приблизиться, это должно включить **Отладки Endpoit** вместо того, чтобы иметь необходимость установить завершенные компоненты в уровень отладки.

Для включения этого перейдите к **Операциям> Устраняющий неполадки> DiagnosticTools> Общие средства > Отладка EndPoint.**

Однажды на странице отладки Оконечной точки, введите MAC-адрес оконечной точки , и щелчок начинают, когда готовый воссоздавать проблему.

Как только отладка была остановлена, нажимают на ссылку, которая определяет идентификатор оконечной точки для загрузки выходных данных отладки.

Дополнительные сведения

TAC рекомендуемые сборки AireOS

Руководство конфигурации контроллера беспроводной связи Cisco, выпуск 8.0.

Руководство администратора платформы Cisco Identity Services Engine, выпуск 2.1

Универсальная Конфигурация беспроводной сети NGWC с Идентификационным Механизмом сервисов