Гостевой портал платформы Identity Services Engine локальный пример конфигурации web-аутентификации

Содержание

Введение

Этот документ описывает, как настроить Локальную web-аутентификацию (LWA) с платформой Cisco Identity Services Engine (ISE) гостевой портал.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ISE
- Контроллер беспроводной локальной сети Cisco (WLC)

Используемые компоненты

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

- Версия 1.1 ISE
- Версия 7.4 WLC

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

Этот документ описывает конфигурацию LWA. Однако Cisco рекомендует использовать Централизованную web-аутентификацию (CWA) с ISE, когда это возможно. Существует несколько сценариев, где LWA предпочтен или единственная опция, таким образом, это - пример конфигурации для тех сценариев.

Настройка

LWA требует определенных предварительных требований и основной конфигурации на WLC, а также нескольких изменениях, необходимых на ISE.

Прежде чем те покрыты, вот структура процесса LWA с ISE.

Процесс LWA с гостевым порталом ISE

1. Браузер пытается выбрать веб-страницу.
2. WLC перехватывает запрос HTTP и перенаправляет его к ISE.
   Несколько важных частей информации сохранены в том заголовке перенаправления HTTP. Вот пример URL перенаправления:
   https://mlatosieise.wlaaan.com:8443/guestportal/Login. действие?
   switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirec t=yahoo.com/
   От URL в качестве примера вы видите, что пользователь пытался достигнуть "yahoo.com". URL также содержит информацию о названии Wireless Local Area Network (WLAN) (mlatosie_LWA), и MAC-адреса точки доступа (AP) и клиент. В URL в качестве примера, **1.1.1.1** WLC, и **mlatosieise.wlaaan.com** является сервером ISE.
3. Пользователю предоставляют гостевую страницу входа ISE и вводит имя пользователя и пароль.
4. ISE выполняет аутентификацию против своей настроенной идентификационной

последовательности.

5. Браузер перенаправляет снова. На этот раз это отправляет учетные данные WLC. Браузер предоставляет имя пользователя и пароль, которое пользователь ввел в ISE без любого дополнительного взаимодействия от пользователя. Вот запрос GET в качестве примера к WLC.
   GET/login.html?
   redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   Снова, исходный URL **(yahoo.com)**, имя пользователя **(mlatosie@cisco.com)**, и пароль **(ityh)** все включен.
   Примечание: Несмотря на то, что URL видим здесь, фактический запрос отправлен по Уровню защищенных сокетов (SSL), который обозначен HTTPS и труден перехватить.
6. WLC использует RADIUS, чтобы аутентифицировать то имя пользователя и пароль против ISE и предоставляет доступ.
7. Пользователь перенаправлен к указанному порталу. См. **"Настраивают внешний ISE как webauth URL"** раздел этого документа для получения дополнительной информации.

Схема сети

Этот рисунок описывает логическую топологию устройств, используемых в данном примере.

Предварительные условия для конфигурации

Для процесса LWA для работы должным образом клиент должен быть в состоянии получить:

- IP-адрес и конфигурация маски подсети
- Маршрут по умолчанию
- Сервер Системы доменных имен (DNS)

Всем им можно предоставить DHCP или локальную конфигурацию.

Разрешение DNS должно работать должным образом для LWA для работы.

Настройте WLC

Настройте внешний ISE как URL Webauth

Под **Безопасностью> веб-Аутентификация> Веб-страница для входа**, можно обратиться к этой информации.

> **Примечание:** Данный пример использует Внешний URL Webauth и был взят от Версии 1.1 ISE. Если у вас есть другая версия, консультируйтесь с руководством по конфигурации для понимания то, что должно быть настроено.

Настройте списки контроля доступа (ACL)

Для web-аутентификации для работы должен быть определен позволенный трафик.

Определите, должны ли использоваться ACL FlexConnect или обычные ACL.

AP FlexConnect используют ACL FlexConnect, в то время как AP, которые используют централизованную коммутацию, используют обычные ACL.

Для понимания, в каком режиме определенный AP работает, перейдите к **беспроводным сетям> точки доступа** и выберите раскрывающееся окно **Режима AP name> AP**. Типичное развертывание или **локально** или **FlexConnect**.

Под **Безопасностью> Списки контроля доступа,** выберите **FlexConnect ACLs** или **ACL**.

В данном примере весь трафик UDP был разрешен для специфического разрешения обмена DNS и трафика к ISE (10.48.66.107).

Данный пример использует FlexConnent, таким образом, определены **и** FlexConnect и стандартные ACL.

Это поведение задокументировано в идентификатор ошибки Cisco CSCue68065 относительно контроллеров WLC 7.4.

Настройте идентификаторы наборов сервисов (SSID) для LWA

Под **WLAN** выберите **WLAN ID** для редактирования.

Веб-подлинная конфигурация

Примените те же ACL, которые были определены в предыдущем шаге и включают web-аутентификацию.

> **Примечание:** Если функция локального коммутатора FlexConnect использована, сопоставление ACL должно быть добавлено на уровне AP. Это может быть найдено под **беспроводными сетями> точки доступа.** Выберите соответствующий **Name> AP FlexConnect> Внешние ACL WebAuthentication**.
> ;

Конфигурация аутентификации, авторизации и учета (AAA)

В данном примере и аутентификация и учетные серверы указывают к ранее определенному серверу ISE.

> **Примечание:** Настройки по умолчанию под **Вкладкой Дополнительно** не должны быть добавлены.

Настройте ISE

Конфигурация ISE состоит из нескольких шагов.

Во-первых, определите устройство как сетевое устройство.

Затем гарантируйте, что существуют правила проверки подлинности и авторизация, которые принимают этот обмен.

Определите сетевое устройство

При **администрировании-> Сетевые ресурсы-> Сетевые устройства**, заполните эти поля:

- Device Name
- IP-адрес устройства
- **Параметры аутентификации> Общий секретный ключ**

Настройте политику аутентификации

Под **Политикой> Аутентификация**, добавьте новую политику аутентификации.

Данный пример использует эти параметры:

- Name: **WLC_LWA_Guests**
- **Condition:Airespace:Airespace-Wlan-Id.** Это условие совпадает с ИДЕНТИФИКАТОРОМ WLAN 3, который является ID WLAN **mlatosie_LWA**, который был ранее определен на WLC.
- {дополнительный} Это позволяет протоколы аутентификации, которые не требуют сертификата**, Non_Cert_Auth**, но настройки по умолчанию может использоваться.
- Guest_Portal_Sequence, который определяет это пользователи, является локально определенными гостевыми пользователями.

Настройте политику авторизации и результат

Под **Политикой> Авторизация,** определите новую политику. Это может быть очень простая политика, такая как:

Эта конфигурация зависит от общей конфигурации ISE. Данный пример целеустремленно упрощен.

Проверка

На ISE администраторы могут контролировать и устранить неполадки оперативных сеансов при **Операциях> Аутентификации**.

Должны быть замечены две аутентификации. Первая аутентификация от гостевого портала на ISE. Вторая аутентификация стала запросом доступа от WLC до ISE.

Можно нажать **Опознавательный** значок **Сведений отчета** для проверки, какая политика авторизации и политика аутентификации были выбраны.

На WLC администратор может контролировать клиентов под **Монитором> Клиент**.

Вот пример клиента, который аутентифицировался должным образом:

Устранение неполадок

Cisco рекомендует выполнить отладки посредством клиента, когда это возможно.

Через CLI эти отладки предоставляют полезные сведения:

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

Дополнительные сведения

- Cisco ISE 1.x руководство по конфигурации
- WLC Cisco 7.x руководство по конфигурации
- Cisco Systems – техническая поддержка и документация