Внутренняя веб-аутентификация для гостевого доступа на автономном примере конфигурации AP

Содержание

Введение

Этот документ описывает, как настроить для гостевого доступа на автономных точках доступа (AP) с использованием страницы внутренней сети, которая встроена в сам AP.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с темами в данном документе перед началом конфигурации:

- Как настроить автономные AP для главной операции
- Как настроить локальный сервер RADIUS на автономных AP
- Как работает web-аутентификация как мера по безопасности уровня 3

Используемые компоненты

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

- AIR-CAP3502I-E-K9, который выполняет Cisco IOS®, отображает 15.2 (4) JA1
- Intel Centrino Усовершенствованные-N 6200 беспроводных адаптеров AGN (Версия драйвера 13.4.0.9)
- Microsoft Windows 7 утилит соискателя

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

Web-аутентификацией является Уровень 3 (L3) характеристика безопасности, которая позволяет автономным AP заблокировать IP - трафик (кроме DHCP и Сервера доменных имен (DNS) связанные пакеты), пока гость не предоставляет допустимое имя пользователя и пароль в веб-портале, к которому перенаправлен клиент, когда открыт браузер.

С web-аутентификацией отдельное имя пользователя и пароль должно быть определено для каждого гостя. Гость аутентифицируется с именем пользователя и паролем или локальным сервером RADIUS или внешним сервером RADIUS.

Эта функция была представлена в Cisco IOS Release 15.2 (4) JA1.

Конфигурация точки доступа

> **Примечание:** Этот документ предполагает, что Виртуальный интерфейс моста (BVI) 1 на AP имеет IP-адрес 192.168.10.2 / 24, и что пул DHCP определен внутренне на AP для IP-адресов 192.168.10.10 до 192.168.10.254 (IP-адреса 192.168.10.1 до 192.168.10.10 исключены).

Выполните эти шаги для настройки AP для гостевого доступа:

1. Добавьте новые идентификаторы наборов сервисов (SSID), назовите их **Гостем** и настройте их для web-аутентификации:

```
ap(config)#dot11 ssid Guest

ap(config-ssid)#authentication open

ap(config-ssid)#web-auth

ap(config-ssid)#guest-mode

ap(config-ssid)#exit
```

2. Создайте опознавательное правило, где необходимо задать протокол проверки подлинности прокси-сервера, и называть его **web_auth**:

```
ap(config)#ip admission name web_auth proxy http
```

3. Примените SSID (Гость) и опознавательное правило (web_auth) к радиоинтерфейсу. Данный пример использует 802.11b/g радио:

```
ap(config)#interface dot11radio 0

ap(config-if)#ssid Guest

ap(config-if)#ip admission web_auth

ap(confi-if)#no shut

ap(config-if)#exit
```

4. Определите список методов, который задает, где аутентифицируются учетные данные пользователя. Свяжите название списка методов с web_auth опознавательным правилом и назовите его web_list:

```
ap(config)#ip admission name web_auth method-list authentication web_list
```

5. Выполните эти шаги, чтобы настроить Аутентификацию, авторизацию и учет (AAA) на AP и локальном сервере RADIUS, и связать список методов с локальным сервером RADIUS на AP:

   Включите AAA:

```
ap(config)#aaa new-model
```

   Настройте локальный сервер RADIUS:

```
ap(config)#radius-server local

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Создайте гостевые учетные записи и задайте их срок действия (в минутах). Создайте одну учетную запись пользователя с именем пользователя и паролем user1 и установите пожизненное значение в 60 минут:

```
ap(config)#dot11 guest

ap(config-guest-mode)#username user1 lifetime 60 password user1

ap(config-guest-mode)#exit

ap(config)#
```

   Можно создать других пользователей с тем же процессом.

   Примечание: Необходимо включить radius-server local для создания гостевых учетных записей.

   Определите AP как сервер RADIUS:

```
ap(config)#radius-server host 192.168.10.2 auth-port 1812
 acct-port 1813 key cisco
```

   Свяжите список web-аутентификации с локальным сервером:

```
ap(config)#aaa authentication login web_list group radius
```

Примечание: Можно использовать внешний сервер RADIUS для хостинга учетных записей гостя. Чтобы сделать это, настройте **команду radius-server host** для обращения к внешнему серверу вместо IP-адреса AP.

Настройте беспроводного клиента

Выполните эти шаги для настройки беспроводного клиента:

1. Для настройки беспроводной сети на утилите соискателя окон с SSID под названием **Гость** перейдите к **Сети, и Интернет> Управляют Беспроводными сетями** и **нажмите Add**.

2. Выберите **подключение Manually к беспроводной сети** и введите необходимую информацию, как показано в этом образе:

3. **Нажмите кнопку Next.**

Проверка

После того, как конфигурация завершена, клиент может обычно соединяться с SSID, и вы видите это на консоли AP:

```
%DOT11-6-ASSOC: Interface Dot11Radio0, Station ap 0027.10e1.9880
 Associated KEY_MGMT[NONE]

ap#show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address   IP address  IPV6 address Device    Name Parent State

0027.10e1.9880  0.0.0.0     ::           ccx-client ap  self   Assoc
```

У клиента есть динамический IP - адрес 192.168.10.11. Однако, когда вы пытаетесь пропинговать IP-адрес клиента, он отказывает, потому что не полностью аутентифицируется клиент:

```
ap#PING 192.168.10.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
```

```
.....

Success rate is 0 percent (0/5)
```

Если клиент открывает браузер и пытается достигнуть **http://1.2.3.4**, например, клиент перенаправлен к внутренней странице входа:

> **Примечание:** Этот тест завершен со случайным IP-адресом, введенным непосредственно (здесь, введенный URL **1.2.3.4**) без потребности в трансляции URL через DNS, потому что DNS не использовался в тесте. В обычных сценариях пользователь вводит URL домашней страницы, и трафик DNS позволен, пока клиент не передает сообщение GET HTTP к решенному адресу, который перехвачен AP. AP имитирует адрес веб-сайта и перенаправляет клиента к странице входа, сохраненной внутренне.

Как только клиент перенаправлен к странице входа, учетные данные пользователя введены и проверены против локального сервера RADIUS согласно конфигурации точки доступа. После успешной аутентификации полностью позволен трафик, который прибывает из и переходит к клиенту.

Вот сообщение, которое передается пользователю после успешной аутентификации:

После успешной аутентификации можно просмотреть информацию о IP-адресе клиента:

```
ap#show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address   IP address   IPV6 address Device  Name Parent State

0027.10e1.9880 192.168.10.11 ::      ccx-client ap   self  Assoc
```

Эхо-запросы клиенту после успешной аутентификации завершены, должен работать должным образом:

```
ap#ping 192.168.10.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

> **Примечание:** Роуминг между AP во время web-аутентификации не предоставляет плавный опыт, потому что клиенты должны войти к каждому новому AP, с которым они соединяются.

Кастомизация

Подобный IOS на маршрутизаторах или коммутаторах, можно настроить страницу с пользовательским файлом; однако, не возможно перенаправить к странице внешней web - страницы.

Используйте эти команды для настройки портала файлов:

- файл страницы входа ip admission proxy http
- ip admission proxy http истек файл подкачки
- файл подкачки успеха ip admission proxy http
- файл подкачки сбоя ip admission proxy http