Table of Contents

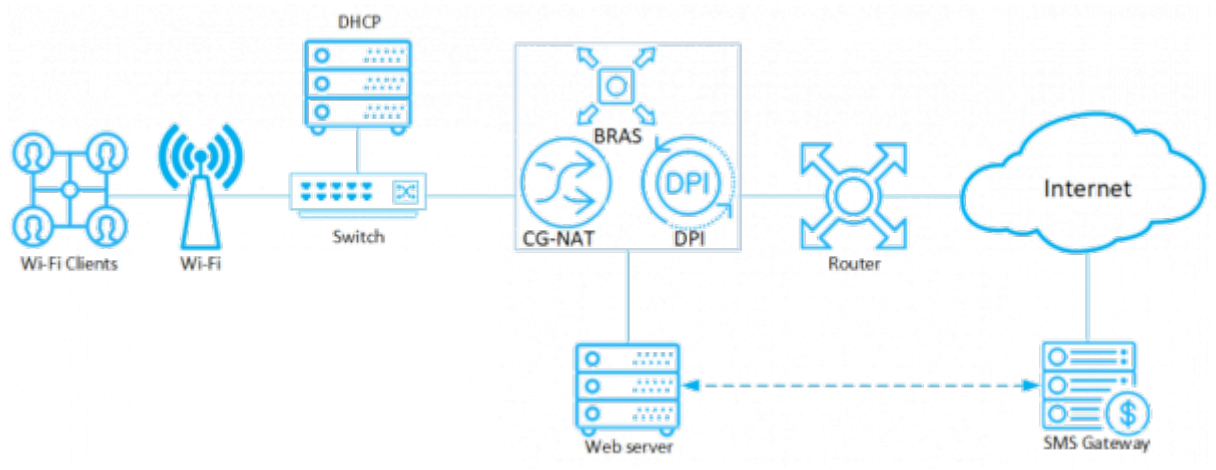
Wi-Fi HotSpot (Captive Portal для Wi-Fi авторизации) 3
Введение 3
Архитектура 3
Сценарий применения 3
Инсталляция и обновление 4
Рекомендации к оборудованию 4
Перед установкой 4
Инсталляция 5
Обновление 6
Конфигурация 6
Информация о версиях 7
Взаимодействие с абонентом 8

Wi-Fi HotSpot (Captive Portal для Wi-Fi авторизации)

Введение

Модуль предоставляет возможность реализовать сценарий: Идентификация абонента в сети WiFi с помощью мобильного телефона.

Архитектура

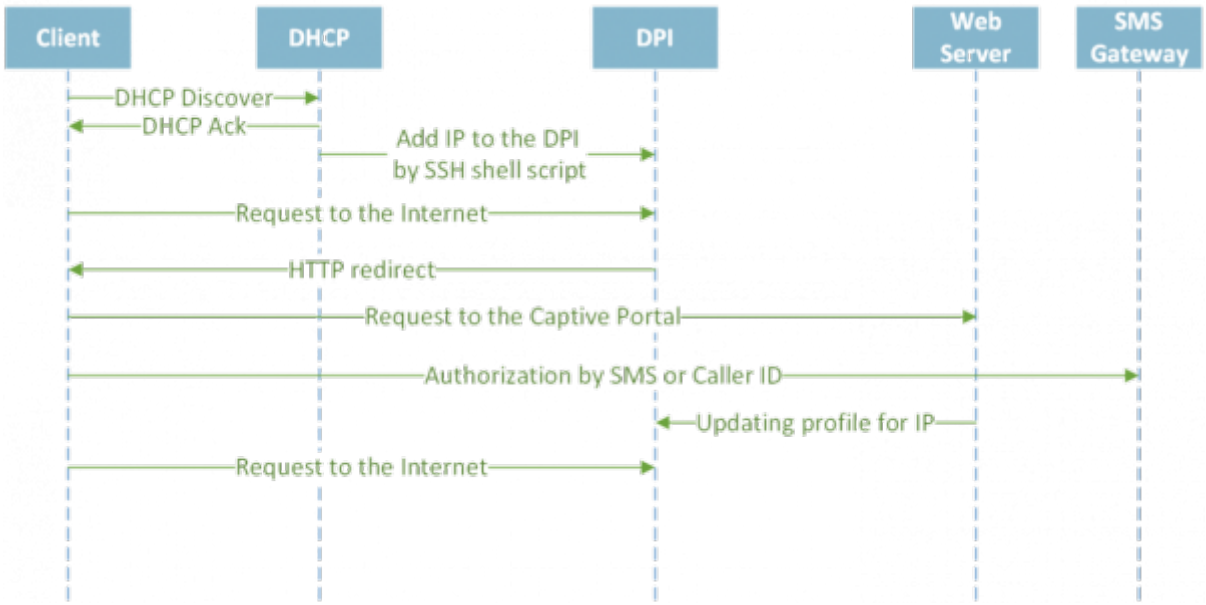


Сценарий применения

Подробная инструкция развертывания Wi-Fi Hot Spot.

В момент, когда абонент подключается к Wi-Fi, роутер обращается к DCHP-серверу для получения нового IP-адреса. Сервер возвращает данные адреса на роутер и вызывает shell-script, активирующий тариф с ограниченным доступом и «Белый список». В белые списки здесь имеет смысл включить, например, сайт провайдера или организации, предоставляющий публичный Wi-Fi.

Далее абонент перенаправляется в браузер на стартовую страницу, где ему необходимо пройти авторизацию по номеру телефона. Web-сервер получает ответ об успешной авторизации от SMS шлюза и с помощью shell-script удаляет ограничения на DPI и перенаправляет на нужную страницу.



Инсталляция и обновление

Рекомендации к оборудованию

Для подсистемы можно использовать оборудование или виртуальные машины со следующими характеристиками:

1. Процессор (CPU) - 2.5 ГГц, 1 шт
2. Оперативная память (RAM) - 512 Мб - 1 Гб
3. Жесткий диск (HDD) - 20 Гб - 50 Гб
4. Операционная система - CentOS 8.x, VEOS, CentOS Stream 8.x, Oracle Linux Server 8.x, AlmaLinux 8.x
5. Сетевая плата (NIC) - от 10 Мб/сек

Не устанавливайте подсистему на то же оборудование, где установлены DPI и GUI! Используйте для этого отдельную виртуальную машину.

Перед установкой

Новая ВМ

1. Убедитесь, что установлен openssh-clients - необходим для подключения к DPI
2. Все остальное необходимое окружение будет установлено автоматически

Старая ВМ

1. Убедитесь, что установлен openssh-clients - необходим для подключения к DPI
2. Если установлен PHP версии < 7.1, удалите старую версию:

```
yum -y remove php*
```

Новая версия будет установлена автоматически при установке dpiui2.

3. Если установлен MySql, удалите:

```
yum remove mysql mysql-server mysql-community-common
```

Также удалите директорию MySql:

```
mv /var/lib/mysql /var/lib/mysql_old_backup
```

При установке wifi_hotspot будет установлен MariaDB 10.4

Инсталляция

Перед установкой или обновлением проверьте наличие интернета. Запуски скриптов выполняйте из под root или sudo.

Внимание: Требуется отключить selinux. Для этого установите SELINUX=disabled в файле /etc/selinux/config и перегрузите сервер.

Для установки или обновления запустите скрипт: wifi_hotspot-rpm_install.sh.

```
source <(curl https://vasexperts.ru/install/wifi_hotspot-rpm_install.sh)
```

Будет произведена установка rpm-пакета wifi_hotspot. Будет произведена автоматическая настройка согласно конфигурации.

В процессе установки будет произведена установка / обновление окружения:

1. PHP >= 7.1
2. MariaDB >= 10.4
3. Apache
4. Composer
5. PHP SSH2 lib
6. Laravel/Lumen

В процессе установки будут открыты необходимые порты, а также запущен cron для выполнения фоновых задач по расписанию.

Установка подсистемы будет произведена в папку:

```
/var/www/html/wifi_hotspot/
```

После инсталляции, введите в браузере:

```
http://<IP адрес VM>/
```

Обновление

Для обновления ранее установленной версии, выполните команду

```
yum install -y wifi_hotspot
```

Конфигурация

Системные настройки модуля находятся в файле .env

```
/var/www/html/wifi_hotspot/backend/.env
```

Содержимое файла следующее:

```
#Системные настройки, лучше не трогать
APP_ENV=local
APP_DEBUG=true
APP_KEY=
APP_TIMEZONE=UTC

#Системные настройки подключения к БД MySql, лучше не трогать
DB_CONNECTION=mysql
DB_HOST=localhost
DB_PORT=3306
DB_DATABASE=wifi_hotspot
DB_USERNAME=root
DB_PASSWORD=vasexperts

#Настройки подключения к SMTP-серверу. Нужны для отправки данных по авторизации в
режиме отладки.
CFG_SMTP_UNAME=smtptestvasexperts@gmail.com
CFG_SMTP_PW=pH3xkXTp1
CFG_SMTP_HOST=smtp.gmail.com
CFG_SMTP_PORT=587
CFG_SMTP_SECURE=tls
CFG_SMTP_SENDER=smtptestvasexperts@gmail.com

#Системные настройки, трогать нельзя
CACHE_DRIVER=file
QUEUE_DRIVER=database
SESSION_DRIVER=cookie

#
#Настройка экспорта AAA-сессий (файлы с сессиями храняться в папке
/var/www/html/wifi_hotspot/backend/storage/aaa_events)
#
```

```
#Включение/отключение экспорта AAA-сессий
AAA_EXPORT_ENABLED=0
#IP-адрес NAS сервера, IPv4/IPv6, если неизвестно - 0.0.0.0
AAA_HOTSPOT_IP=0.0.0.0
#порт NAS сервера, число, если неизвестно - 0
AAA_HOTSPOT_PORT=0
#ИД точки подключения к сети передачи данных, целое число в диапазоне от 0 до 1000,
необходимо заполнять для абонентов публичных Wifi-точек,
# соответствует идентификатору точки подключения в поле 1 из выгрузки точек
подключения
AAA_HOTSPOT_ID=0
# Удаление файлов AAA-сессий, 0 - не удалять
OLD_AAA_FILE_LIFETIME_DAYS=0

#Длина кода авторизации абонентов
AUTH_CODE_LENGTH=6

#Замена ведущего знака "+" в номере телефона (0/1)
CFG_PHONE_REPLACE_LEADING_PLUS=0

#Замена ведущей "8" на "7" в номере телефона (0/1)
CFG_PHONE_REPLACE_LEADING_8_BY_7=0
```

Если были внесены изменения в .env, необходимо выполнить команду

```
php /var/www/html/wifi_hotspot/backend/artisan queue:restart
```

```
/var/www/html/wifi_hotspot/frontend/env.js
```

Содержимое файла следующее:

```
var AppEnv = {};

// Плейхолдер в поле для ввода кода авторизации абонента
AppEnv.AuthCodePlaceHolder = "000000";
```

Информация о версиях

Версия v.1.3.3 (16.10.2023)

- Добавлена возможность автоподстановки кода из СМС в поле ввода кода (на мобильных устройствах);
- Добавлена опция в файле конфигурации (backend/.env) OLD_AAA_FILE_LIFETIME_DAYS для удаления файлов AAA-сессий спустя указанное количество дней (по-умолчанию 0 - не удалять)

Версия v.1.2.19 (11.04.2022)

Исправление ошибок, возникавших при использовании сервисов, которые не поддерживали номера телефонов с ведущим знаком "+" и/или "8":

- Добавлена возможность удалению ведущего знака "+" в номере телефона
- Добавлена возможность замены ведущей "8" на "7" в номере телефона

Версия v.1.2.17 (01.03.2022)

- Исправлены ошибки в скрипте авторизации/деавторизации абонентов;
- Расширены логи авторизации/деавторизации абонентов
- Добавлена возможность экспорта AAA-сессий
- Добавлена возможность конфигурировать длину кода авторизации абонентов

Версия v.1.2.4 (02.10.2020)

- исправление багов

Версия v.1.1.0 (06.11.2019)

- Переработан процесс замены логотипа и иконки через интерфейс dpiui2
- Изменен ограничение размера файла логотипа или иконки с 64кб до 750кб

Версия v.1.0.10 (25.10.2019)

- Исправление отображения портала на мобильных устройствах
- Исправление алгоритма повторной авторизации

Версия v.1.0.7 (15.09.2019)

- Создан новый модуль Wi-Fi HotSpot

Взаимодействие с абонентом

Взаимодействие HotSpot с абонентом на СКАТ и команды, выполняющиеся при этом:

1. Скрипт, который вызывается DHCP-триггером (отгружается на СКАТ `/var/dpiui2/add_captive_portal_auth.sh`). К IP абонента применяется профиль услуги 5 и профиль полисинга для авторизации

```
fdpi_ctrl load --service 5 --profile.name='hotspot_white_list_profile'
--ip $1
fdpi_ctrl load --policing --profile.name='wifi_hotspot_auth_policing' -
```

```
-ip $1
```

2. Команды, выполняющиеся на СКАТ при успешной авторизации пользователя:
    1. Если абонент с таким логином уже существует:

    ```
    fdpi_ctrl list --bind --login='[phone]'
    ```

    2. Убрать с абонента профиль полисинга для авторизации:

    ```
    fdpi_ctrl del --policing --ip=[ip]
    ```

    3. Убрать с абонента 5 услугу:

    ```
    fdpi_ctrl del --service 5 --ip=[ip]
    ```

    4. Убрать с абонента 11 услугу (NAT):

    ```
    fdpi_ctrl del --service 11 --ip=[ip]
    ```

    5. Создать bind-абонента:

    ```
    fdpi_ctrl load --bind --user='[phone]:[ip]'
    ```

    6. Применить к абоненту профиль полисинга для доступа в интернет:

    ```
    fdpi_ctrl load --policing --profile.name='wifi_hotspot_policing' -
    -login='[phone]'
    ```

    7. В случае, если в форме в GUI установленны услуги, которые необходимо применить к абоненту:

    ```
    fdpi_ctrl load --service [service] --login='[phone]'
    ```

    8. В случае, если в форме в GUI установленны профили услуг, которые необходимо применить к абоненту:

    ```
    fdpi_ctrl load --service [service] --profile.name='[profile_name]'
    --login='[phone]'
    ```

3. Команды, выполняющиеся на СКАТ, когда сессия авторизованного пользователя истекла.
    1. Убрать с абонента профиль полисинга для доступа в интернет:

    ```
    fdpi_ctrl del --policing --login='[phone]'
    ```

    2. Получить список услуг, примененных к абоненту и убрать их:

    ```
    fdpi_ctrl list --service --login='[phone]'
        fdpi_ctrl del --service [service] --login='[phone]'
    ```

    3. Удалить bind-абонента:

    ```
    fdpi_ctrl del --bind --login='[phone]'
    ```

    4. Выполнить на СКАТ скрипт добавления профиля услуги 5 и профиля полисинга для

авторизации (см. п.1)

```
sh /var/dpiui2/add_captive_portal_auth.sh [ip]
```