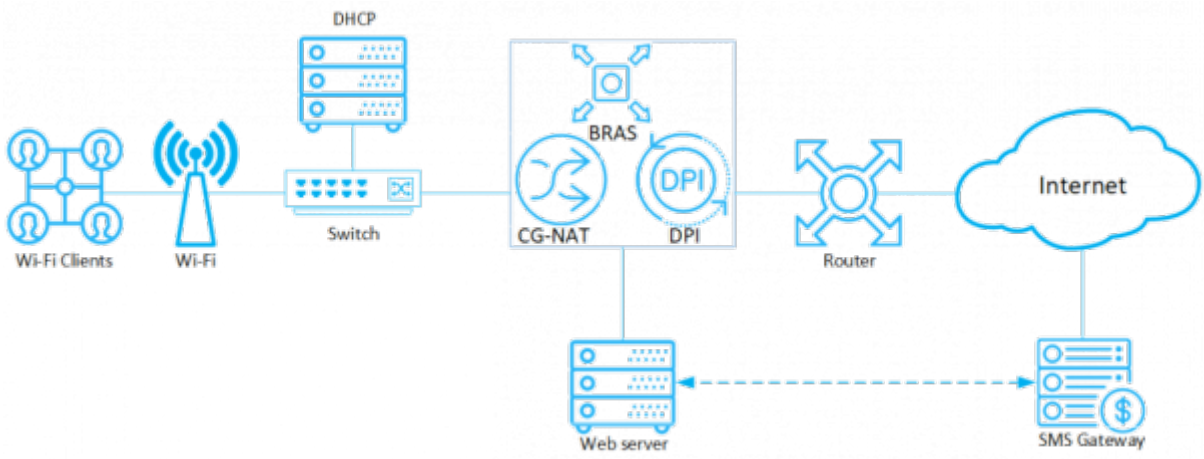
Содержание

Wi-Fi HotSpot (Captive Portal for Wi-Fi authorization)

Introduction

The module provides the feature to authorize users by phone number in public Wi-Fi networks.

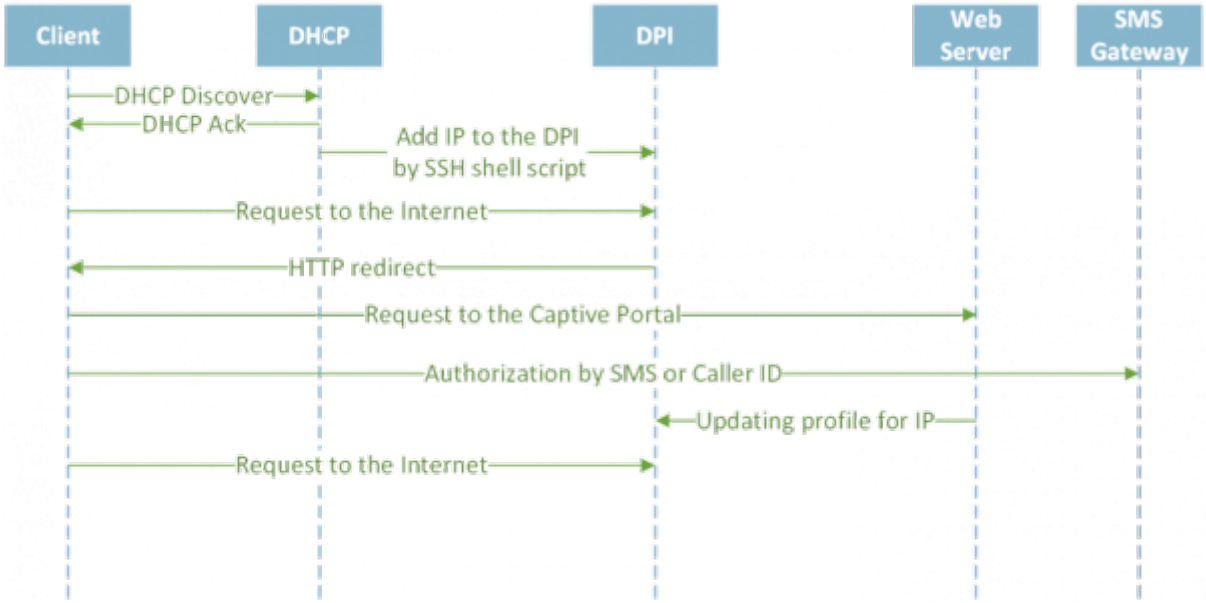
Architecture



Scenarios of use

When a subscriber connects to Wi-Fi, the router requests the DCHP server to obtain a new IP address. The server returns the addresses to the router and runs the shell-script, which activates the tariff with limited access and the “White List”. It makes sense to include in the white lists, for example, the site of the provider or organization providing public Wi-Fi.

Then the subscriber is redirected to the browser start page, where he needs to go through the authorization by phone number. The web server receives a successful authorization response from the SMS gateway and, using a shell-script, disables restrictions specified on the DPI and redirects the subscriber to the desired page.



Installation and Upgrade

Hardware Recommendations

In order to run the module you can use the following hardware or virtual machines matching the following characteristics:

1. CPU 2.5 GHz, 1 pcs
2. RAM 512 MB - 1 GB
3. HDD 20 GB - 50 GB
4. Operating system CentOS 7.x, CentOS 8.x, VEOS, CentOS Stream 8.x, Oracle Linux Server 8.x, AlmaLinux 8.x
5. NIC ranging from 10 Mbps

Do not install the module on the same hardware running the DPI or the SSG DPI 2 management interface! Use a dedicated virtual machine instead.

Before installation

New Virtual Machine

1. Make sure the openssh-clients is installed, it is required to connect to the DPI
2. The rest of environment will be installed automatically

Old Virtual Machine

1. Make sure the openssh-clients is installed, it is required to connect to the DPI
2. If PHP version <7.1 is installed, uninstall the old one:

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

The new version will be installed automatically during dpiui2 installation.

3. If MySql is installed, uninstall it:

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

Also delete the MySql directory:

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

During wifi_hotspot installation MariaDB 10.4+ will be installed

CentOS 6

Recommended operating system is Cent Cent OS 7+ If you need to install the module on Cent OS 6, make sure that supervisor 3+ is installed. If you do not have the needed package, plese install it using the following commands:

```
sudo wget https://vasexperts.ru/install/supervisor-3.0-1.gf.el6.noarch.rpm
yum install supervisor-3.0-1.gf.el6.noarch.rpm
```

Installation

Before installing or upgrading, check your internet connection. Run scripts with root privilege or using sudo.

Attention: You should to disable selinux. To do this, set SELINUX = disabled in the /etc/selinux/config file and restart server.

Attention: If you've configured the virtual machine using HotSpot Management section before you install this module, all the needed tools and settings will be installed automatically.

To install, run the script:

```
#!/usr/bin/env bash

info () {
    echo -e " info:    $@ ";
}
```

```
ok () {
    echo -e " done:    $@ ";
}

error () {
    echo -e  " ERROR:  $@";
}

CENTOSRELEASE=`cat /etc/redhat-release`
SUBSTR=`echo $CENTOSRELEASE|cut -c1-22`
SUBSTR2=`echo $CENTOSRELEASE|cut -c1-26`

#Check OS version
CentOsVersion=0
if [ "$SUBSTR" = "CentOS Linux release 7" ]
    then
        CentOsVersion=70
elif [ "$SUBSTR2" == "CentOS release 6.5 (Final)" ]
    then
        CentOsVersion=65
elif [ "$SUBSTR2" == "CentOS release 6.4 (Final)" ]
    then
        CentOsVersion=64
else
    CentOsVersion=60
fi

#Configure repos
info "Configuring repos..."

rpm --import http://vasexperts.ru/centos/RPM-GPG-KEY-vasexperts.ru
rpm -Uvh http://vasexperts.ru/centos/6/x86_64/vasexperts-repo-1-0.noarch.rpm


MARIADB_REPO=/etc/yum.repos.d/mariadb.repo
if [ "$CentOsVersion" == 70 ]
then
        rpm -Uvh
https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
        rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
        echo "[mariadb]
name=MariaDB
baseurl=http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1" > $MARIADB_REPO

else

        rpm -Uvh
https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm
        rpm -Uvh https://mirror.webtatic.com/yum/el6/latest.rpm
```

```
        MACHINE_TYPE=`uname -m`
        if [ ${MACHINE_TYPE} == 'x86_64' ]
        then

echo "[mariadb]
name=MariaDB
baseurl=http://yum.mariadb.org/10.4/centos6-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1" > $MARIADB_REPO

else
echo "[mariadb]
name=MariaDB
baseurl=http://yum.mariadb.org/10.4/centos6-x86
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1" > $MARIADB_REPO
fi


fi
ok "Finished Configuring repos."

#wifi_hotspot install
info "Wifi hotspot package installing..."

yum install -y wifi_hotspot --exclude=php-common*;

info "Finished wifi_hotspot package installing."
```

The rpm wifi_hotspot package will be installed. It will be configured automatically according to the default configuration.

Installation/upgrading of the following environment will be performed during the installation:

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

The necessary ports will be opened, and cron will be launched to perform scheduled background tasks during the installation process.

The module will be installed to the

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

directory.

After the installation, enter in the browser:

```
http://<IP address of VM>/
```

Upgrade

To update a previously installed version, run the following command:

```
yum install -y wifi_hotspot
```

Configuration

System settings of the module are in the .env file:

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

The contents of the file are as follows:

```
#System settings, it’s worth to avoid modifying it
APP_ENV=local
APP_DEBUG=true
APP_KEY=
APP_TIMEZONE=UTC

#System settings for connecting to the MySql database, it’s worth to avoid
modifying it
DB_CONNECTION=mysql
DB_HOST=localhost
DB_PORT=3306
DB_DATABASE=wifi_hotspot
DB_USERNAME=root
DB_PASSWORD=vasexperts

#Settings for connecting to the SMTP server. They serve to send
authorization data in debug mode.
CFG_SMTP_UNAME=smtptestvasexperts@gmail.com
CFG_SMTP_PW=
CFG_SMTP_HOST=smtp.gmail.com
CFG_SMTP_PORT=587
CFG_SMTP_SECURE=tls
CFG_SMTP_SENDER=smtptestvasexperts@gmail.com

#System settings, modifying is fobidden
CACHE_DRIVER=file
QUEUE_DRIVER=database
SESSION_DRIVER=cookie

#Debugging mode for interaction between Hotspot and DPI. When enabled, a
request to the SMS/call authorization service is not sent. Authorization
code 0000.
```

```
#Default 0
DEBUG_MODE=0
```

If .env file has been modified, you should run the following command:

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

Version Information

Version v.1.3.5 (18.06.2024)

- Added the ability to set a priority authorization method (available for version dpiui2 >= 2.34.5)
- Added the ability to enable debug mode for the Hotspot interaction script with SKAT (option DEBUG_MODE in /var/www/html/wifi_hotspot/backend/.env)
- Bugfix

Version v.1.3.3 (16.10.2023)

- Added possibility of auto substitution of code from SMS into the code input field (on mobile devices);
- Added option in the configuration file (backend/.env) OLD_AAA_FILE_LIFETIME_DAYS to delete AAA-session files after a specified number of days (default is 0 - do not delete)

Version v.1.2.19 (11.04.2022)

Corrects errors that occurred when using services that did not support phone numbers with a leading "+" and/or "8" sign:

- Added possibility to delete leading "+" sign in phone number
- Added option to replace the leading "8" with "7" in the phone number

Version v.1.2.17 (01.03.2022)

- Fixed errors in subscriber authorization/deauthorization script;
- Extended subscriber authorization/deauthorization logs
- Added ability to export AAA sessions
- Added the ability to configure the length of subscribers authorization code

Version v.1.2.4 (02.10.2020)

- Bugs fixed

Version v.1.1.0 (06.11.2019)

- The process of replacing the logo and icons through the dpiui2 interface reworked
- The size limitation of logo or icon file from 64kb to 750kb changed

Version v.1.0.10 (10/25/2019)

- Correction of the display of the portal on mobile devices
- Correction of the re-authorization algorithm

Version v.1.0.7 (15.09.2019)

- Created a new Wi-Fi HotSpot module

Subscriber Interaction

Interaction between HotSpot and the subscriber on the SSG and the commands executed during this process:

1. Script triggered by DHCP (unloaded on SSG at `/var/dpiui2/add_captive_portal_auth.sh`). Service profile 5 and policing profile for authorization are applied to the subscriber's IP

```
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. Commands executed on the SSG upon successful user authorization:
    1. If a subscriber with this login already exists:

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

    2. Remove the policing profile for authorization from the subscriber:

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

    3. Remove service 5 from the subscriber:

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

    4. Remove service 11 (NAT) from the subscriber:

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

    5. Create a bind subscriber:

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

6. Apply the policing profile for internet access to the subscriber:

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

7. If services are set in the GUI form that need to be applied to the subscriber:

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

8. If service profiles are set in the GUI form that need to be applied to the subscriber:

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

3. Commands executed on the SSG when the authorized user's session has expired:
    1. Remove the policing profile for internet access from the subscriber:

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

    2. Retrieve the list of services applied to the subscriber and remove them:

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

    3. Delete the bind subscriber:

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

    4. Execute the script on the SSG to add service profile 5 and policing profile for authorization (see item 1)

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