Table of Contents

Subscriber athorization in WiFi network by a phone number

We recommend that you explore the Wi-Fi HotSpot module feature, the control is carried out via DPIUI2 graphical interface.
There is an option for self-implementation of this module below.

Introduction

Due to the tightening of the rules for access through public WiFi hotspots to the operator's network, it became necessary to identify the subscriber in one of the ways by the phone number, by passport data or through the portal of state services. In this example, we will analyze the organization of access using subscriber identification by phone number.

Workflow

Sequencing:

1. the subscriber connects to the WiFi network
2. a welcome page appears with information, that the subscriber must open a browser and identify themselves [1)]
3. the subscriber opens the browser, when going to any URL, the subscriber is redirected to the identification page
4. the subscriber enters a phone number, requests an access code
5. the access code is sent to the phone number via SMS
6. the subscriber enters the received access code
7. session cookies are written to the subscriber device with storage for 24 hours [2)] and the transition to the requested one occurs. user URL.

For the network settings you will need:

1. DHCP server for the centralized issuance of subscribers addresses with a possibility when issuing a new IP address to call a shell script [3)]
2. The virtual machine with installed Apache WEB-server (httpd), module for viewing statistics and reports (nfsen)
3. Access to the service for sending SMS messages [4)]
4. (Optional) the NAT to reduce usage of IPv4 addresses, and the NAT log record translations IP ↔ IP, PORT [5)]
5. (Optional) the Radius authentication to get network subscriber identifier [6)]

Network diagram (inline):

1. WiFi router, configured to recieve IP from external DHCP server, and a welcome page setted [7)]

2. Network routers
3. Stingray Service Gateway
4. Border router

Thus, all subscriber traffic passes through the SSG.

The sequence of operation:

1. Subscriber unit is connected to a WiFi router
2. WiFi router requests a new IP from the DHCP server
3. DHCP server runs a shell script when new IP issued and sends the data to WiFi router
4. Shell script sets on the SSG Allow list service for subscriber and rate plan with access restrictions
5. Welcome page is shown to subsriber, the subscriber activates the browser and enters any URL
6. The SSG redirects the subcriber to athoruzation page, WEB-server shows the athorizathion page [8)], the user enters a phone number and press "get the access code"
7. WEB-server receives a request for an access code generates a random number and sends it to the subscriber's phone, the user enters the code into the form and click to confirm
8. WEB-server receives a request for confirmation of access code if the code is correct, is a shell script to remove the service Allow list and activate WiFi default rate plan, sets a cookie in the browser and redirects to the requested URL.

Source code

Stingray Service Gateway Settings

Using class description in protocols.txt

```
http    cs0
https   cs0
dns     cs0
default cs1
```

Converting:

```
cat protocols.txt|lst2dscp /etc/dpi/protocols.dscp
```

From the source code copy the directory to DPI server:

```
htdocs/wifi/.script в /home/fastdpi/
```

Create a tariff file default_policing.cfg for Internet access via WiFi - 10 mbit:

```
htb_inbound_root=rate 10mbit
htb_inbound_class0=rate 1mbit ceil 10mbit
htb_inbound_class1=rate 1mbit ceil 10mbit
htb_inbound_class2=rate 8bit ceil 10mbit
htb_inbound_class3=rate 8bit ceil 10mbit
htb_inbound_class4=rate 8bit ceil 10mbit
```

```
htb_inbound_class5=rate 8bit ceil 10mbit
htb_inbound_class6=rate 8bit ceil 10mbit
htb_inbound_class7=rate 8bit ceil 10mbit
htb_root=rate 10mbit
htb_class0=rate 1mbit ceil 10mbit
htb_class1=rate 1mbit ceil 10mbit
htb_class2=rate 8bit ceil 10mbit
htb_class3=rate 8bit ceil 10mbit
htb_class4=rate 8bit ceil 10mbit
htb_class5=rate 8bit ceil 10mbit
htb_class6=rate 8bit ceil 10mbit
htb_class7=rate 8bit ceil 10mbit
```

Create a tariff file captive_portal_hard.cfg to block access to the Internet together with an Allow list:

```
htb_inbound_root=rate 256kbit
htb_inbound_class0=rate 8bit ceil 256kbit
htb_inbound_class1=rate 8bit ceil 8bit
htb_inbound_class2=rate 8bit ceil 8bit
htb_inbound_class3=rate 8bit ceil 8bit
htb_inbound_class4=rate 8bit ceil 8bit
htb_inbound_class5=rate 8bit ceil 8bit
htb_inbound_class6=rate 8bit ceil 8bit
htb_inbound_class7=rate 8bit ceil 8bit
htb_root=rate 256kbit
htb_class0=rate 8bit ceil 256kbit
htb_class1=rate 8bit ceil 8bit
htb_class2=rate 8bit ceil 8bit
htb_class3=rate 8bit ceil 8bit
htb_class4=rate 8bit ceil 8bit
htb_class5=rate 8bit ceil 8bit
htb_class6=rate 8bit ceil 8bit
htb_class7=rate 8bit ceil 8bit
```

Configure an Allow list service:

```
cp_server=yoursite.ru/welcome.php
```

DHCP Configuration

1. configure remote command execution via SSH to DPI server
2. set to trigger to issue a new IP: ssh dpi_user@dpi_host "/home/fastdpi/_add_captive_portal.sh <IP>"

Web Server Configuration

1. configure remote SSH control to DPI server
2. configure Apache, example in directory conf/ of source code:

в conf.d/php.ini move/add settings from sample conf/php.ini
include file main.conf
configure DocumentRooot on /var/www/html/htdocs/wifi/

3. copy htdocs/ in /var/www/html
4. edit /var/www/html/htdocs/wifi/.script/remove_captive_portal.sh
5. edit /var/www/html/htdocs/wifi/request.php set USER и PASSWORD for SMS service access

1)
for mobile devices, for example iphone, the automatically displayed welcome page opens in a special browser mode, in which session cookies cannot be saved and you need to open the browser separately.
2)
session cookies are used to re-identify the subscriber in the network so that it is not required to re-identify the subscriber by sending SMS, the storage period can be regulated by the operator independently.
3)
feel plugged in to DPI
4)
in this example www.smsdirect.ru service
5) , 6)
will not be considered further, to simplify the scheme
7)
welcome page is on the WEB server
8)
as verified by the presence of a cookie, if the cookie is there, then there is an automatic check-in according to the subscriber's network stored in a cookie