Содержание

4 Subscriber athorization in WiFi network by a phone number

Introduction

Due to the tightening of the rules of access through public WiFi hotspots to the network operator, there is a need to identify the subscriber's one way of using the phone number. In this example, we analyze the WiFi access using the athorization by the phone number of subscriber.

Scheme

Sequencing:

1. The subscriber is connected to a WiFi network
2. Showing a welcome page with the information that the user must open a browser and identify yourself [1)]
3. Subscriber opens the browser, it goes to any URL, subscriber is redirected to the athorization page
4. on athorization page user enters a phone number and requests the access code
5. Access code sent to the phone number via SMS
6. Obtained access code the subscriber enters in the form field
7. Session cookies stored on the user device to prevent next redirection for a day [2)], then user's browser is redirected to the requested URL

For the network settings needed:

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 to view 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 schema (inline):

1. > WiFi router, configure to get IP from external DHCP server and welcome page setted [7)]
2. > Network routers
3. > VAS Experts DPI
4. > Border router

all traffik from subscribers pass trought the VAS Experts DPI.

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 VAS Experts DPI whitelist 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 VAS Experts DPI 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 whitelist and activate WiFi default rate plan, sets a cookie in the browser and redirects to the requested URL

source code

VAS Experts DPI Settings

Using class description in protocols.txt

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

Cnverting:

```
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 file with default rate plan default_policing.cfg WiFi internet access with 10 mbit limits:

```
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 file with rate plan captive_portal_hard.cfg to restrict access to internet only several application protocols to use with white 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 white list service:

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

DHCP Configuration

1. configure remote SSH control to DPI server
2. set trigger for new IP issue: 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 such as iphone automatically displays the welcome page opens in a special browser mode, where you can not save the session cookie and the browser you want to open separately
[2]

session cookies are used to re-identify the subscriber in the network that would not be needed again to identify the caller by sending SMS, shelf life can be regulated operator yourself
[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 at 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