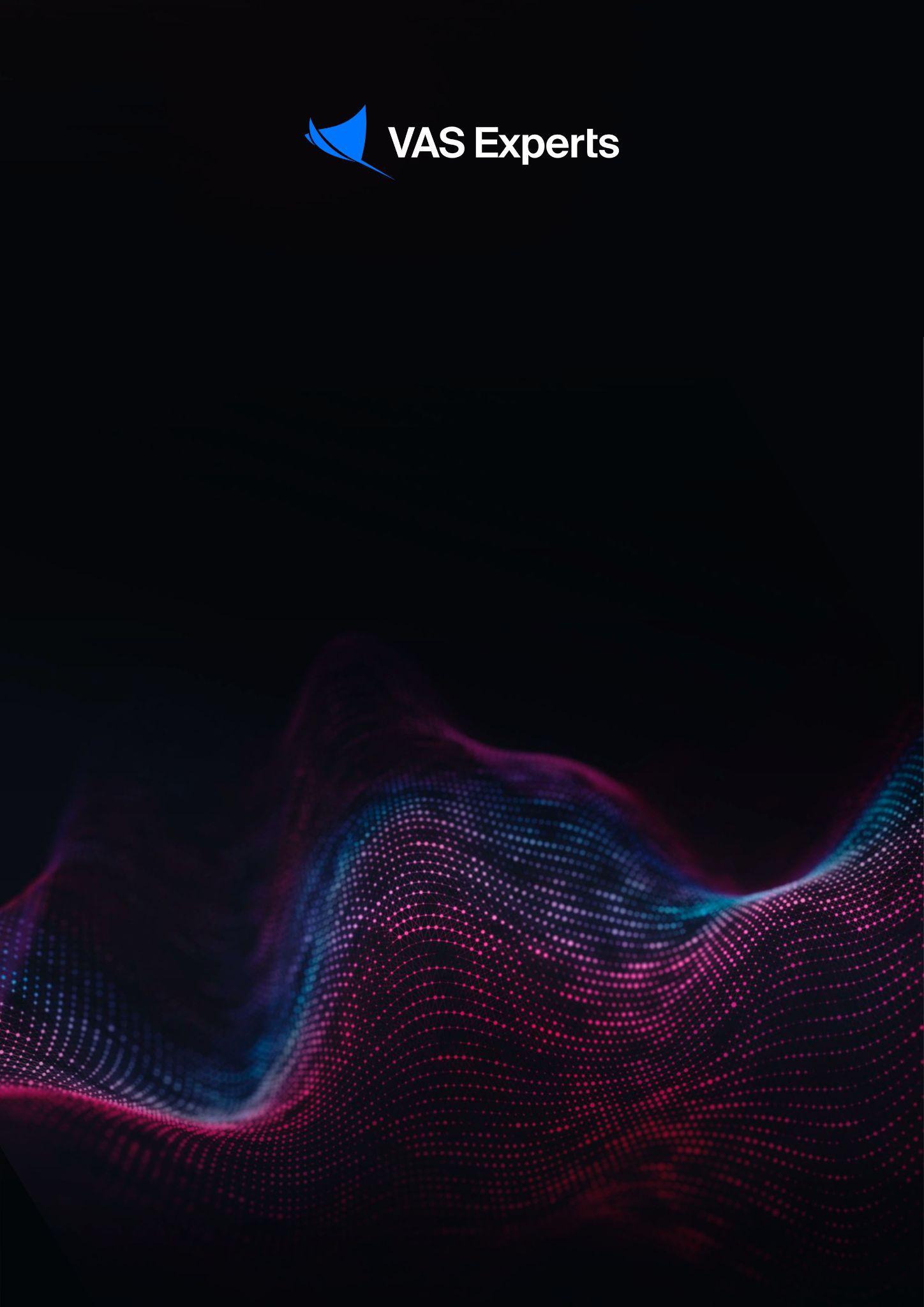
****

**Инструкция по установке  
 и настройке**

**WiFi HotSpot и СКАТ DPI**

**Содержание документа**

[Топология сети](#_i5p1tbi1fz2c) **1**

[Последовательность действий при авторизации](#_olzmlf2mzn8j) **2**

[Установка виртуальных машин (ВМ)](#_r5zsmuw37uhe) **3**

[Установка и настройка dpiui\_vm](#_lru8fa77x3yt) **3**

[Установка и настройка cp\_wifi\_vm](#_5zf7eo8ckwrm) **4**

[Установка и настройка dhcp-isc на cp\_wifi\_vm](#_7akg1dgugzno) **5**

[Настройка СКАТ](#_c990buqxww2v) **9**

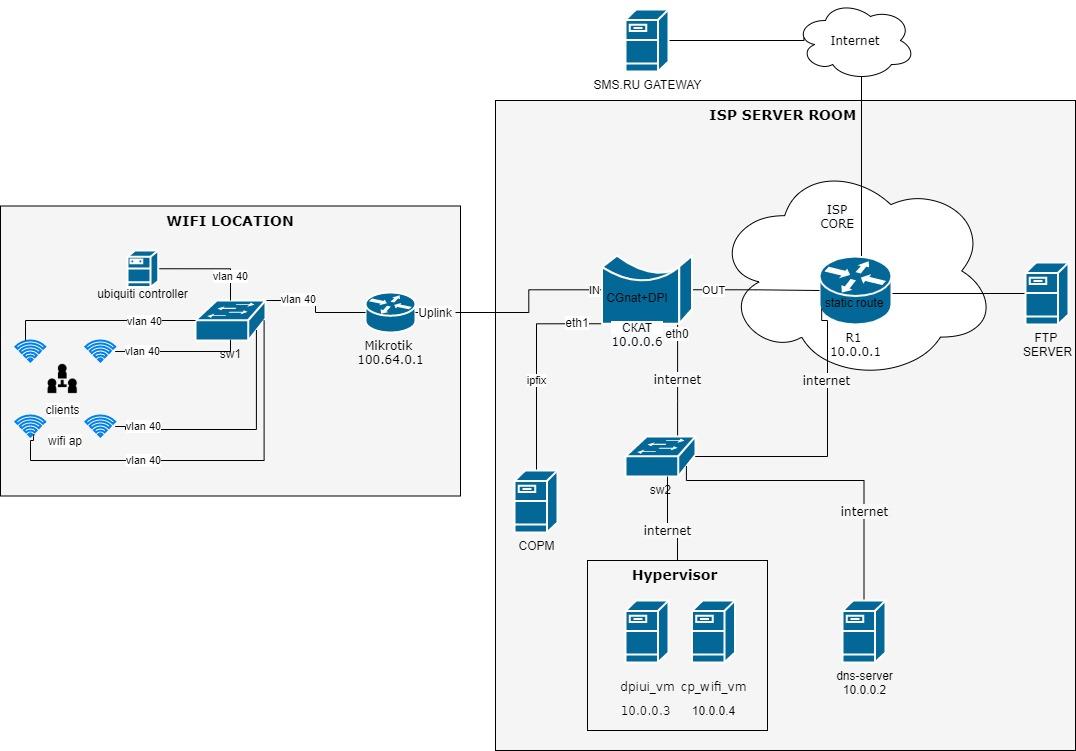
[Настройка DPI и Hotspot через DPIUI](#_sswcz96b0w5i) **12**

[Настройка Микротика 100.64.0.1](#_w0c3sa7ys4h0) **15**

[Настройка unifi network](#_i8wddhrtsog2) **15**

# **Топология сети**

1. Подключить оборудование согласно топологии сети.



# **Последовательность действий при авторизации**

1. Абонент подключается к сети WiFi
2. Появляется welcome page с информацией, что абонент должен открыть браузер и идентифицировать себя
3. Абонент отрывает браузер, при переходе на любой URL, происходит переадресация абонента на страницу идентификации
4. Абонент вводит телефонный номер, запрашивает код доступа
5. Код доступа отправляется на телефонный номер через SMS
6. Абонент вводит полученный код доступа
7. Происходит запись сессионной куки на абонентское устройство с сохранением в заданного периода и происходит переход на запрошенный пользователем URL

# **Установка виртуальных машин (ВМ)**

1. Создаём 2 виртуальные машины со следующими минимальными характеристиками:

* dpiui\_vm – 1 cpu, 2Gb Ram, 50G hard disk, Guest OS Centos 7, nic 1
* cp\_wifi\_vm – 1 cpu, 1Gb Ram, 30G hard disk, Guest OS Centos 7, nic

1. Устанавливаем последнюю версию CentOS-7 (build-2009 на момент написания) на обе виртуальные машины. По ходу установки выбираем (minimal install) минимальную установку.

После установки ОС, входим в консоль и устанавливаем пакеты на обе ВМ:  
yum install epel-release

и после: yum install nano tcpdump openssh-server openssh-clients

1. Выключить selinux на обоих ВМ:

* Отредактировать файл /etc/sysconfig/selinux
* SELINUX=disabled и перезагрузить ВМ

# **Установка и настройка dpiui\_vm**

1. Установить dpiui на dpiui\_vm по следующей инструкции:

<https://wiki.vasexperts.ru/doku.php?id=dpi:dpi_components:dpiui:install_and_update:install>

1. Настроить сеть на обоих ВМ и СКАТ:

BOOTPROTO=static

ONBOOT=yes

IPADDR=10.0.0.x

NETMASK=255.255.255.0

GATEWAY=10.0.0.1

DNS1=10.0.0.2

IPADDR — указать для каждого хоста согласно схеме (или использовать свою адресацию).

1. Войти в GUI и добавить обе ВМ и СКАТ в разделе «ОБОРУДОВАНИЕ», следуя инструкции по ссылке:

<https://wiki.vasexperts.ru/doku.php?id=dpi:dpi_components:dpiui:user_guide:admin_section:equipment_management:start>

# **Установка и настройка cp\_wifi\_vm**

1. Установить пакет wifi\_hotspot на cp\_wifi\_vm по следующей инструкции:

https://wiki.vasexperts.ru/doku.php?id=dpi:dpi\_components:%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C\_wi-fi\_hotspot:start

1. Отредактируем конфиг файл для hotspot:  
   nano /var/www/html/wifi\_hotspot/backend/.env

Изменяем/добавляем только эти строчки:

* **AAA\_HOTSPOT\_IP – 10.0.0.4**   
  Адрес NAS сервера, IPv4/IPv6, если неизвестно – 0.0.0.0
* **AAA\_HOTSPOT\_PORT – 0**   
  Порт NAS сервера, число, если неизвестно - 0
* **AAA\_HOTSPOT\_ID – 2**   
  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\_EXPORT\_ENABLED=1**   
  Включить экспорт ААА
* **AUTH\_CODE\_LENGTH=4**   
  Поменять кол-во символов в коде для SMS авторизации

Если прописали параметр AUTH\_CODE\_LENGTH, то надо в файле **/var/www/html/wifi\_hotspot/frontend/env.js** установить значение:

AppEnv.AuthCodePlaceHolder = "0000";

В конце выполнить команду:

php /var/www/html/wifi\_hotspot/backend/artisan queue:restart

# **Установка и настройка dhcp-isc на cp\_wifi\_vm**

1. Установить пакет dhcp-isc — **yum install dhcp expect**
2. Далее настраиваем скрипты статического arp и конфиг файл dhcpd.conf**:**

* Сначала конфиг файл dhcpd — **nano /etc/dhcp/dhcpd.conf**

Поставить свои значения **option domain-name** и option **ntp-servers**!

| * ddns-update-style none; * authoritative; * db-time-format local; * log-facility local7; * subnet 100.64.0.0 netmask 255.255.252.0 { * range 100.64.0.3 100.64.3.254; * default-lease-time 600; * max-lease-time 600; * option subnet-mask 255.255.252.0; * option broadcast-address 100.64.3.255; * option routers 100.64.0.1; * option ntp-servers <ntp-server>; * option domain-name-servers 10.0.0.2; * option domain-name "name.local"; * on commit { * set ClientIP = binary-to-ascii(10, 8, ".", leased-address); * set ClientMac = concat ( * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,1,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,2,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,3,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,4,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,5,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,6,1))),2)); * log(concat("Request: IP: ", ClientIP, " Mac: ", ClientMac)); * execute("/usr/local/etc/dhcpd/clients\_add\_drop.sh", "add", ClientIP, ClientMac);} * on release { * set ClientIP = binary-to-ascii(10, 8, ".", leased-address); * set ClientMac = concat ( * suffix (concat ("0", binary-to-ascii (16, 8, "", * substring(hardware,1,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,2,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,3,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,4,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,5,1))),2), ":", * suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,6,1))),2)); * log(concat("Release: IP: ", ClientIP, " Mac: ", ClientMac)); * execute("/usr/local/etc/dhcpd/clients\_add\_drop.sh", "drop\_rls", ClientIP, ClientMac);} * on expiry { * set ClientIP = binary-to-ascii(10, 8, ".", leased-address); * log(concat("Timeout: IP: ", ClientIP)); * execute("/usr/local/etc/dhcpd/clients\_add\_drop.sh", "drop\_exp", ClientIP);} * } * subnet 10.0.0.0 netmask 255.255.255.0 { * } |
| --- |

Создаём директории и изменяем её права:

| * mkdir /usr/local/etc/dhcpd/ && chown dhcpd:dhcpd /usr/local/etc/dhcpd/ * touch /usr/local/etc/dhcpd/clients\_add\_drop\_mysql.sh && touch /usr/local/etc/dhcpd/clients\_add\_drop.sh  && chown dpiacc:dpiacc /usr/local/etc/dhcpd/\* * chmod 755 /usr/local/etc/dhcpd/ * chmod 755 /usr/local/etc/dhcpd/\* |
| --- |

Теперь скопируем следующий скрипт в **/usr/local/etc/dhcpd/clients\_add\_drop.sh**:

| * #!/usr/bin/expect -f * set METHOD [lindex $argv 0] * set IP\_ADDR [lindex $argv 1] * set MAC\_ADDR [lindex $argv 2] * set MAC\_ADDR [string toupper $MAC\_ADDR] * # клиентский интерфейс на микротике: * set INT\_ClIENT "vWifi" * set status 0 * #Записываем dhcp-lease (start and end) в базе hotspot * spawn /usr/local/etc/dhcpd/./clients\_add\_drop\_mysql.sh "$METHOD" "$IP\_ADDR" "$MAC\_ADDR" * expect "end\_mysql"; * #Подключаемся к роутеру * spawn ssh -i /usr/local/etc/dhcpd/.ssh/id\_rsa admin+t@100.64.0.1 -oStrictHostKeyChecking=no -oUserKnownHostsFile=/dev/null * expect { * "password:" {send "\n";} * "timeout" {set status 1;} * ">" {} * } * if { $METHOD == "add" && $status == 0} { * send "ip arp add address=$IP\_ADDR mac-address=$MAC\_ADDR interface=$INT\_ClIENT\r"; * expect ">"; * send "ip firewall address-list remove \[find address=$IP\_ADDR list=DROP\_CLIENTS\]\r"; * expect ">"; * send "log info \"ADD: $IP\_ADDR -- $MAC\_ADDR\"\r"; * expect ">" * send "quit\r"; * expect eof * } elseif { $METHOD == "drop\_rls" && $status == 0} { * send "ip arp remove \[find mac-address=$MAC\_ADDR\]\r"; * expect ">"; * send "ip firewall address-list add address=$IP\_ADDR list=DROP\_CLIENTS\r"; * expect ">"; * send "log info \"DROP\_RLS: $IP\_ADDR -- $MAC\_ADDR\"\r"; * expect ">" * send "quit\r"; * expect eof * } elseif { $METHOD == "drop\_exp" && $status == 0} { * send "ip arp remove \[find address=$IP\_ADDR\]\r"; * expect ">"; * send "ip firewall address-list add address=$IP\_ADDR list=DROP\_CLIENTS\r"; expect ">"; send "log info \"DROP\_EXP: $IP\_ADDR\"\r"; expect ">" send "quit\r"; expect eof } elseif {$status == 0} { send "quit\r"; * expect eof * exit 1; * } * set status 0 * #Подключаемся к скату и прописываем статическую запись абона. * spawn ssh -i /usr/local/etc/dhcpd/.ssh/id\_rsa dpisu@10.0.0.6 -oStrictHostKeyChecking=no -oUserKnownHostsFile=/dev/null * expect { * "password" {send "\r"} * "timeout" {set status 1; exit 4} * "\$" {} * } * if {$status == 0} { * send "/var/dpiui2/add\_captive\_portal\_auth\_ivstar.sh $IP\_ADDR\r" * expect "\$" * send "exit\r"; * expect eof * } |
| --- |

И скопируем в **/usr/local/etc/dhcpd/clients\_add\_drop\_mysql.sh** скрипт для добавления в базу hotspot данных о dhcp-lease:

| * #!/bin/bash * METHOD=$1 * IP\_ADDR=$2 * MAC\_ADDR=$3 * MYSQL\_CONNECT\_LEASEDB="mysql -u root -pvasexperts -Dwifi\_hotspot -h 127.0.0.1" * if [ "$METHOD" = "add" ]; then * echo "insert into hotspot\_aaa(TYPE,MAC,IP) values("1",\""$MAC\_ADDR"\",\""$IP\_ADDR"\");" | $MYSQL\_CONNECT\_LEASEDB * elif * [ "$METHOD" = "drop\_rls" ]; then * echo "insert into hotspot\_aaa(TYPE,MAC,IP) values("2",\""$MAC\_ADDR"\",\""$IP\_ADDR"\");" | $MYSQL\_CONNECT\_LEASEDB * elif * [ "$METHOD" = "drop\_exp" ]; then * echo "insert into hotspot\_aaa(TYPE,MAC,IP) values("2",\"""\",\""$IP\_ADDR"\");" | $MYSQL\_CONNECT\_LEASEDB * fi  echo "end mysql" |
| --- |

Включаем сервер dhcpd и добавим правило в firewall:

systemctl enable dhcpd

systemctl start dhcpd  
firewall-cmd --permanent —add-service=dhcp

firewall-cmd --reload

1. Создадим скрипт для переноса файла сессий на ftp:

mkdir /srv/aaa/

mkdir /srv/aaa/processed/

mkdir /srv/aaa/script/

touch /srv/aaa/script/script.sh

Скопируем содержимое в **/srv/aaa/script/script.sh**:

| * #!/bin/bash * FTP\_ADDR="<ip ftp>" * FTP\_USER="<user ftp>" * FTP\_PASS="<password ftp>" * #директория с ааа hotspot * DIR="/var/www/html/wifi\_hotspot/backend/storage/aaa\_events" * ls $DIR | while read f; do * curl --user $FTP\_USER:$FTP\_PASS --upload-file $DIR/$f ftp://$FTP\_ADDR/ISP/aaa/ > /dev/null 2>&1 * mv $DIR/$f /srv/aaa/processed |
| --- |

и добавим на выполнение в cron:

| * crontab -e \*/5 \* \* \* \* /srv/aaa/script/script.sh |
| --- |

1. Создадим открытый и закрытый ключ:

| * mkdir usr/local/etc/dhcpd/.ssh && cd usr/local/etc/dhcpd/.ssh * ssh-keygen -t rsa |
| --- |

Секретную фразу оставляем пустой   
***Внимание! Переносим id.pub на скат (10.0.0.6) и микротик (100.64.0.1)!***

* скат (10.0.0.6): перенести файл по ssh на скат и добавить в **authorized\_keys**

cat id.pub >> ~/.ssh/authorized\_keys

* микротик (100.64.0.1): перенести файл по ssh или через web интерфейс и сделать import

user ssh-keys import public-key-file=id.pub user=admin

# 

# **Настройка СКАТ**

1. Настроим на скате db для юзеров:

| * nano /etc/dpi/fastdpi.conf  udr=1 |
| --- |

1. Настроим фильтрацию по федеральному списку:

| * black\_list\_sm=0 federal\_black\_list=1 * #редирект на страничку * black\_list\_redirect=<http://block.lan/> |
| --- |

1. Сделаем класс по умолчанию: class\_order=0
2. Включим выгрузку ipfix:

* Настроить интерфейс eth1: nano /etc/sysconfig/network-scripts/ifcfg-eth1

| * BOOTPROTO=none * ONBOOT=yes * IPADDR=<ip address> * PREFIX=24 |
| --- |

| * netflow=8 * netflow\_dev=eth1 * netflow\_timeout=20 * netflow\_full\_collector\_type=2 * netflow\_full\_collector=127.0.0.1:1500 * netflow\_passive\_timeout=10 * netflow\_active\_timeout=20 * netflow\_rate\_limit=30 * ipfix\_dev=eth1 * ipfix\_tcp\_collectors=<ip:port ipfix collectors> * ipfix\_meta\_tcp\_collectors=<ip:port ipfix collectors> * ipfix\_observation=127 * ipfix\_dns\_tcp\_collectors=<ip:port ipfix collectors> * ipfix\_nat\_udp\_collectors=<ip:port ipfix collectors> |
| --- |

1. Сделаем трафик в class 7 минимальным:

| * tbf\_class7=rate 1kbit * tbf\_inbound\_class7=rate 1kbit |
| --- |

1. Включим редирект на captive portal: cp\_server=10.0.0.4 (ip cp)
2. Выключим nat для приватных адресов: nat\_exclude\_private=1
3. Остальные настройки СКАТ:

| * ctrl\_port=29000 * ctrl\_dev=lo * scale\_factor=1 * num\_threads=2 * class\_order=0 * mem\_tracking\_flow=1500000 * mem\_tracking\_ip=3000000 * http\_parse\_reply=1 * rlimit\_fsize=32000000000 |
| --- |

1. Заменить содержимое скрипта /var/dpiui2/add\_captive\_portal\_auth\_ivstar.sh  
   на следующие:

| * #!/bin/sh * fdpi\_ctrl load --service 5 --profile.name='hotspot\_white\_list\_profile' --ip $1 * fdpi\_ctrl load --service 11 --profile.name='NAT\_PUBLIC\_WIFI' --ip $1 * fdpi\_ctrl load --policing --profile.name='wifi\_hotspot\_auth\_policing' --ip $1 |
| --- |

1. Добавить открытый ключ для доступа с hotspot на скат в файл /home/dpisu/.ssh/authorized\_keys:

| * #!/bin/sh * fdpi\_ctrl load --service 5 --profile.name='hotspot\_white\_list\_profile' --ip $1 * fdpi\_ctrl load --service 11 --profile.name='NAT\_PUBLIC\_WIFI' --ip $1 * fdpi\_ctrl load --policing --profile.name='wifi\_hotspot\_auth\_policing' --ip $1 |
| --- |

Сохраняем все изменения в файле /etc/dpi/fastdpi.conf и делаем reboot.

1. Настроим интерфейс eth0 для доступа к hotspot и dpiui

| * nano /etc/sysconfig/network-scripts/ifcfg-eth0 |
| --- |

| * BOOTPROTO=none ONBOOT=yes IPADDR=10.0.0.6 PREFIX=24 DNS1=10.0.0.2 |
| --- |

# **Настройка DPI и Hotspot через DPIUI**

* Настройка приоритизации по протоколам

1. Переходим во вкладку Управление DPI → ПРИОРИТИЗАЦИЯ ПО ПРОТОКОЛАМ (DSCP) → Редактор

*cs0 – что пропускаем*

*cs1 – что зажимаем тарифом*

*cs7 – что зажимаем глобально*

| * Bittorrent cs7 * default cs1 * dns cs0 * http cs0 * https cs0 |
| --- |

1. CG-NAT в СКАТе:

Переходим во вкладку Управление услугами → Услуги → CGNAT

Создаем профиль:

Описание: NAT\_WIFI

Тип: CGNAT

Nat IP пул: <public ip>

Число tcp сессий: 1000 (на абонента)

Число udp сессий: 1000 (на абонента)

* **Настройка Hotspot:**

1. Переходим во вкладку Управление услугами → Hotspot

Web сервер: WiFi-Hotspot (ВМ (cp\_wifi\_vm) заведенная ранее в dpiui)

Captive portal URL: [https://10.0.0.4](https://10.0.0.4/) (url cp)

Время жизни сессии: 36000

URL для редиректа: [https://google.ru](https://google.ru/) (страничка редиректа после успешной авторизации)

1. Включаем WiFi и SMS авторизацию

SMS авторизацию через сервис sms.ru:

Метод: Post

Url: <https://sms.ru/sms/send>

1. Тело (From):

| * api\_id = <id из личного кабинета sms.ru> * to = [PHONE] * msg = Ваш код для WIFI: [CODE] |
| --- |

* **Настройка тарифов Hotspot (в редакторе):**

1. Тариф для авторизации:

| * htb\_inbound\_root=rate 5mbit ceil 5mbit burst 2500kbit cburst 2500kbit * htb\_inbound\_class0=rate 8bit ceil 5mbit burst 8bit cburst 2500kbit * htb\_inbound\_class1=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_inbound\_class2=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_inbound\_class3=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_inbound\_class4=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_inbound\_class5=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_inbound\_class6=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_inbound\_class7=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_root=rate 100kbit ceil 100kbit burst 50kbit cburst 50kbit * htb\_class0=rate 8bit ceil 100kbit burst 8bit cburst 50kbit * htb\_class1=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_class2=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_class3=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_class4=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_class5=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_class6=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_class7=rate 8bit ceil 8bit burst 8bit cburst 8bit |
| --- |

1. Тариф для бесплатного WiFi:

| * htb\_inbound\_root=rate 10mbit ceil 10mbit burst 5mbit cburst 5mbit * htb\_inbound\_class0=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class1=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class2=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class3=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class4=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class5=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class6=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_inbound\_class7=rate 8bit ceil 8bit burst 8bit cburst 8bit * htb\_root=rate 10mbit ceil 10mbit burst 5mbit cburst 5mbit * htb\_class0=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class1=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class2=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class3=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class4=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class5=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class6=rate 8bit ceil 10mbit burst 8bit cburst 5mbit * htb\_class7=rate 8bit ceil 8bit burst 8bit cburst 8bit |
| --- |

1. Услуги:

Переходим к управлению услугами и включаем **CGNAT** и выбираем профиль **NAT\_WIFI**

1. Белый список:

Переходим во вкладку Управление услугами → услуги → черные и белые списки.

Выбираем нужный профиль и создаем список:

ip 10.0.0.4 (ip cp)

Если для cp есть запись в dns, то добавляем так:

cn example.com

Сохраняем настройки через интерфейс.

# **Настройка Микротика 100.64.0.1**

1. Настройка клиентского интерфейса микротика

Обновить до Router OS 6.48.x

| * /interface vlan * add arp=reply-only arp-timeout=10m interface=sfp1 name=vWifi vlan-id=40 * /ip settings * set icmp-rate-limit=5 rp-filter=strict * /ip address * add address=100.64.0.1/22 interface=vWifi network=100.64.0.0 * /ip dhcp-relay * add dhcp-server=10.0.0.4 disabled=no interface=vWifi local-address=100.64.0.1 name=relay1 * /ip dns * set servers=10.0.0.2 * /ip route * add distance=1 dst-address=10.0.0.4/32 gateway=<указать шлюз> pref-src=100.64.0.1 * /system clock * set time-zone-name=Europe/Moscow * /system ntp client * set enabled=yes primary-ntp=<указать ntp сервер> * /tool bandwidth-server * set authenticate=no enabled=no |
| --- |

1. Настроить ip связь между dhcp/hotspot и микротиком

# 

# **Настройка unifi network**

1. Настроить точки ubiquiti:

* Установить unifi network на сервер
* Настроить dhcp для выдачи настроек точкам
* Если точки и контроллер в разных подсетях, то в dhcp указываем option 43 и присваиваем ей значение ip контроллера (в формате hex). Используя инструкцию: <https://help.ui.com/hc/en-us/articles/204909754-UniFi-Device-Adoption-Methods-for-Remote-UniFi-Controllers>

**Внимание!** Нужно переключиться на старый интерфейс, для этого надо отжать рычажок в System Settings → New USER Interface

1. Настроить Сеть и прочее:

* Перейти в настройки и далее в Network

Создать новою сеть и указать vlan 40 и название WiFi-Client, шлюз указать как 100.64.0.1/22, остальное не имеет значение

* Перейти в настройки и далее в Guest Control

В Pre-Authorization Access указать ip hotspot (10.0.0.4)

* Перейти в настройки и далее в Wireless Networks
* Создаём wifi сеть
* Сразу открываем ADVANCED OPTIONS
* Вписываем любое имя/SSID
* Ставим галочку напротив Enabled
* Ставим галочку напротив Open
* Ставим галочку напротив Guest Policy
* В Network выбираем WiFi-Client
* Ставим галочку напротив Block LAN to WLAN Multicast and Broadcast Data
* Ставим галочку напротив Allow BSS Transition with WNM
* Ставим галочку напротив Block Tunneled Link Direct Setup (TDLS) connections
* Ставим галочку напротив Isolates stations on layer 2 (ethernet) level
* Нажимаем Save

