# VPN-

- , , .

, :

- ( ), ;
- ;
- , - Mikrotik , OpenWrt.

, :

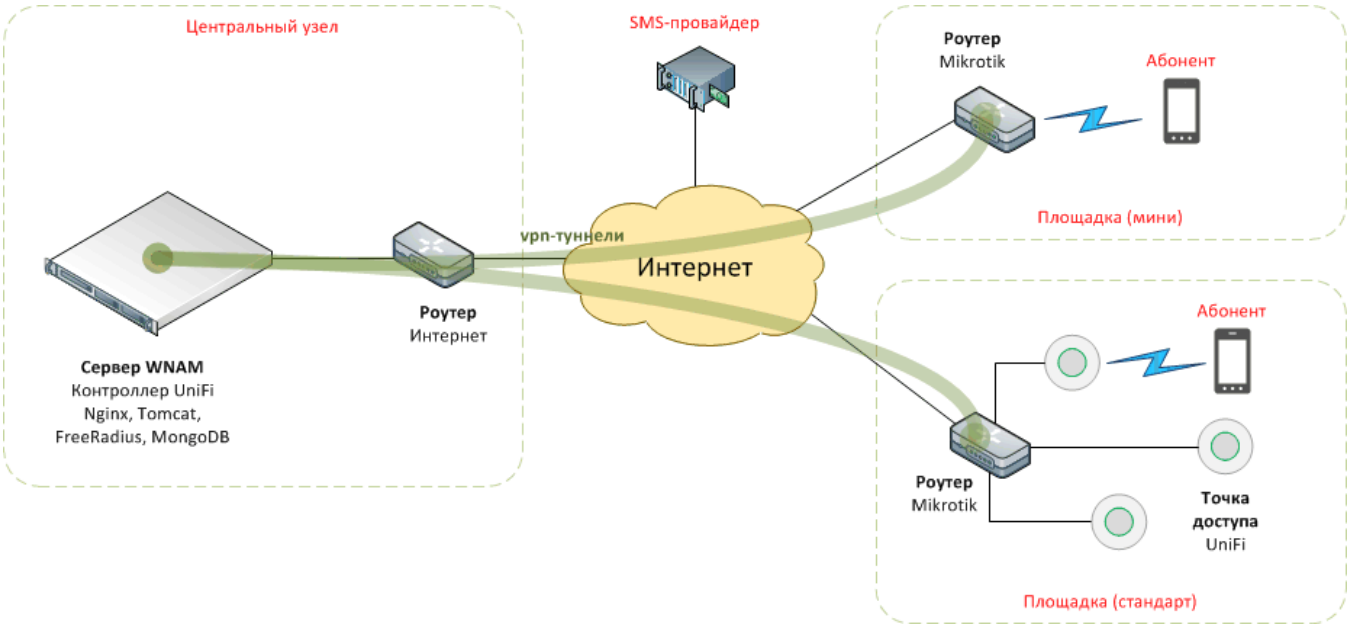
- Wi-Fi , ( );
- (Layer-2) , ( Mikrotik, Cisco ASR, Alcatel ..);
- ( ).

:

1. - . (WAN) , (LAN) , .
2. -. Wi-Fi LAN- Wi-Fi, "access point".
3. - (, SSID ..) Uniquity UniFi. , UniFi WNAM. " ".
4. VPN-. RADIUS- .
5. ( , ), RADIUS NetFlow WNAM , ( ) - .
6. VPN- OpenVPN .

IP- . . :

- () - 1.2.3.4;
- wnam.provider.ru, () 1.2.3.4 ( Let's Encrypt);
- vpn.provider.ru, () 1.2.3.4 ( VPN );
- - 10.1.0.255/24, 10.1.0.254;
- - 10.1.0.1 - 10.1.0.253/24;
- LAN- - 10.1.1.1/24 - 10.1.253.1/24, . , 253 10.1.N.1/24, 10.1.N.2-10.1.N.254 10.1.0.N.




:

- eth0: 1.2.3.4
- tun0: 10.1.0.255

**OpenVPN**

**openvpn**:

```
apt-get install openvpn easy-rsa
```

:
easy-rsa  etc

```
cp -r /usr/share/easy-rsa /etc
```

:

```
cd /etc/easy-rsa
```

(CA):

```
./easyrsa init-pki
touch pki/.rnd
./easyrsa build-ca
```

`Enter New CA Key Passphrase:` , .
`Common Name (eg: your user, host, or server name) [Easy-RSA CA]:` , WNAM.
- **dh.pem**

```
./easyrsa gen-dh
```

:

```
./easyrsa gen-req ovpn-server nopass
./easyrsa sign-req server ovpn-server
```

**pki/issued**.

openvpn:

```
mkdir /etc/openvpn/keys
cp pki/ca.crt pki/dh.pem /etc/openvpn/keys
cp pki/private/ovpn-server.key pki/issued/ovpn-server.crt /etc/openvpn/keys
```

**/etc/openvpn/server.conf**:

```
mode server

dev tun

proto tcp-server
 tls-server
 port 1194
 topology subnet

ca keys/ca.crt
 cert keys/ovpn-server.crt
 key keys/ovpn-server.key
 dh keys/dh.pem

cipher AES-128-CBC
 auth md5

keepalive 10 120
 status /var/log/openvpn-status.log
 log /var/log/openvpn.log
 user nobody
 group nogroup
```

```
persist-key
 persist-tun

ifconfig 10.1.0.255 10.1.0.254
 ifconfig-pool 10.1.0.1 10.1.0.253
 route 10.1.0.0 255.255.0.0
 push "route 10.1.0.255"
 ifconfig-pool-persist ipp.txt 0

auth-user-pass-verify /etc/openvpn/verify.sh via-file
 script-security 2
 verify-client-cert none
 username-as-common-name

verb 2
```

, **/etc/openvpn/verify.sh:**

```
#!/bin/sh
 USERS=`cat /etc/openvpn/user.pass`
 vpn_verify() {
 if [ ! $1 ] || [ ! $2 ]; then
 #echo "No username or password: $*"
 exit 1
 fi
 ## it can also be done with grep or sed
 for i in $USERS; do
 if [ "$i" = "$1:$2" ]; then
 ## you can add here logging of users
 ## if you have enough space for log file
 #echo `date` $1:$2 >> your_log_file
 exit 0
 fi
 done
 }
 if [ ! $1 ] || [ ! -e $1 ]; then
 #echo "No file"
 exit 1
 fi
 ## $1 is file name which contains
 ## passed username and password
 vpn_verify `cat $1`
 #echo "No user with this password found"
 exit 1
```

:

```
chmod +x /etc/openvpn/verify.sh
```

IP- **/etc/openvpn/user.pass:**

```
vpn1,10.1.0.1
vpn2,10.1.0.2
vpn3,10.1.0.3
```

VPN **/etc/openvpn/ipp.txt:**

```
vpn1:ate45cf7y345c5y2x3
vpn2:r2d346c34t4356yucf
vpn3:23cxterthure5y2yw3
```

openvpn **/var/log/openvpn.log.**

```
systemctl daemon-reload
systemctl restart openvpn
```

Mikrotik n cz , vpn- "**vpn1**".

WAN **ether1-gateway** :

```
/ip address
add address=272.16.130.9/24 interface=ether1-gateway network=272.16.130.0

/ip route
add distance=1 gateway=272.16.130.1
```

LAN/WLAN **bridge** :

```
/ip address
add address=10.1.1.1/24 interface=bridge-guest network=10.1.1.0
```

OpenVpn WNAM:

```
/interface ovpn-client
add auth=md5 cipher=aes128 connect-to=vpn.provider.ru name=wnam
password=ate45cf7y345c5y2x3 user=vpn1
```

DHCP DNS :

```
/ip dhcp-server
add address-pool=dhcp-1 disabled=no interface=bridge lease-time=1h name=server

/ip dhcp-server network
add address=10.1.1.0/24 dns-server=8.8.4.4 gateway=10.1.1.1

/ip pool
add name=dhcp-102 ranges=10.1.1.2-10.1.1.254

/ip dns
set allow-remote-requests=yes servers=8.8.4.4

/ip dns static
add address=10.1.0.255 name=wnam.provider.ru
```

DNS ( ) , VPN-.

(NAT):

```
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" out-
interface=ether1-gateway
add action=masquerade chain=srcnat out-interface=wnam src-address=10.1.1.0/24
```

:

```
/ping wnam.provider.ru src-address=10.1.1.1
```

```
/system telnet wnam.provider.ru port=80
```

RADIUS NetFlow :

```
/radius
 add address=wnam.provider.ru domain=wnam secret=wnam_radius service=hotspot

/ip traffic-flow
set interfaces=ether1-gateway
/ip traffic-flow target
add dst-address=wnam.provider.ru port=20002 version=5
```

:

```
/ip hotspot
 add disabled=no idle-timeout=none interface=bridge name=mk-wnam profile=mk-
profile-wnam

/ip hotspot profile
add dns-name=mk.provider.ru hotspot-address=10.1.1.1 html-directory=hotspot
login-by=http-pap name=mk-profile-wnam radius-default-domain=wnam radius-interim-
update=5m use-radius=yes

/ip hotspot user profile
set [ find default=yes ] add-mac-cookie=no name=default1 shared-users=unlimited
status-autorefresh=1h

/ip hotspot walled-garden
add dst-host=*.gosuslugi.ru dst-port=443
add dst-host=ocsp.int-x3.letsencrypt.org dst-port=80
add dst-host=cert.int-x3.letsencrypt.org dst-port=80
add dst-host=*.provider.ru dst-port=443
add dst-host=provider.ru dst-port=443
add dst-host=*.provider.ru dst-port=80
add dst-host=provider.ru dst-port=80
add dst-host=10.1.0.255 dst-port=80
```

**hotspot/rlogin.html** :

```
<html><head><title>...</title>
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="expires" content="-1">
</head>
<body>
<form name="wnamlogin" action="http://wnam.provider.ru/cp/mikrotik" method="post">
 <input type="hidden" name="dst" value="$(link-orig)" />
 <input type="hidden" name="username" value = "user"/>
 <input type="hidden" name="password" value = "password" />
 <input type="hidden" name="mac" value = "$(mac)" />
 <input type="hidden" name="ip" value = "$(ip)" />
 <input type="hidden" name="server-name" value = "$(server-name)" />
 <input type="hidden" name="server-address" value = "$(server-address)" />
 <input type="hidden" name="client-id" value="$(client-id)"/>
 <input type="hidden" name="site-id" value="$(site-id)"/>
</form>
<script type="text/javascript">
<!--
 document.wnamlogin.submit();
//-->
</script>
</body>
</html>
```

**WNAM**

:

- - Mikrotik;
- ( ) - 10.1.0.1;
- : " ", " ", " NetFlow.

. IP- 10.1.1.0/24 ( IP- ).