Wyższa Szkoła Informatyki i Zarządzania

w Bielsku-Białej

Przedmiot: Kryptologia

Temat: Sprawozdanie z projektu

Autor: Dominik Skrzyp 4012

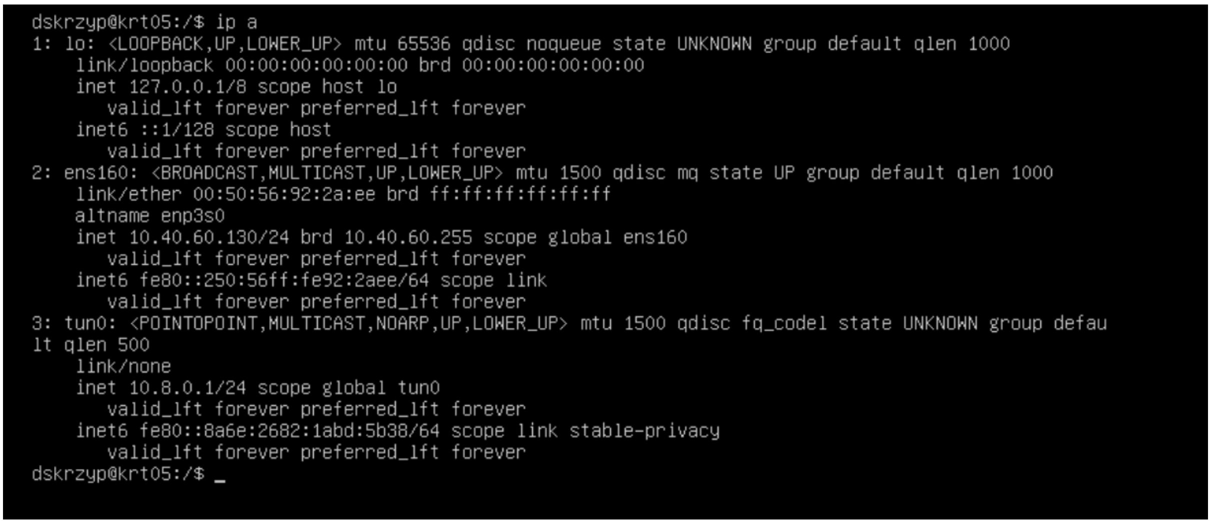
Prowadzący: Prof. Łukasz Florek

Rok Akademicki: 2023/24

1. Czym jest OpenVPN

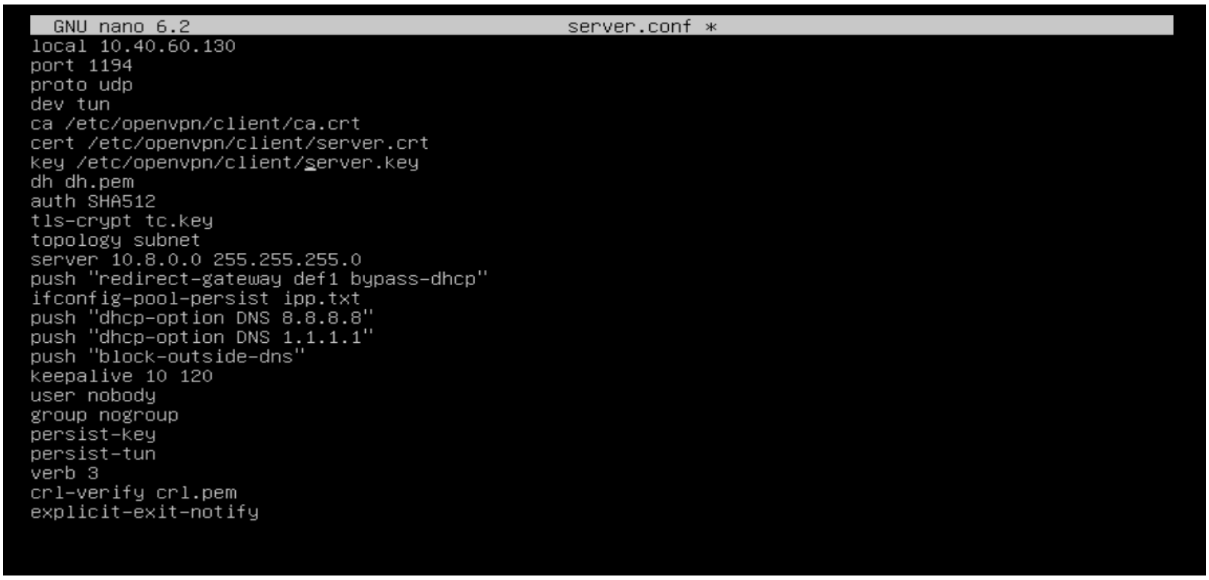
OpenVPN to otwarte oprogramowanie służące do tworzenia wirtualnych prywatnych sieci (VPN). Jest to protokół, który umożliwia bezpieczne połączenia między zdalnymi komputerami poprzez publiczną sieć, taką jak internet. OpenVPN wykorzystuje różne techniki kryptograficzne, takie jak protokoły SSL/TLS, do zapewnienia poufności, integralności i autentyczności danych przesyłanych między klientami i serwerami VPN.

2. Konfiguracja wirtualnej maszyny



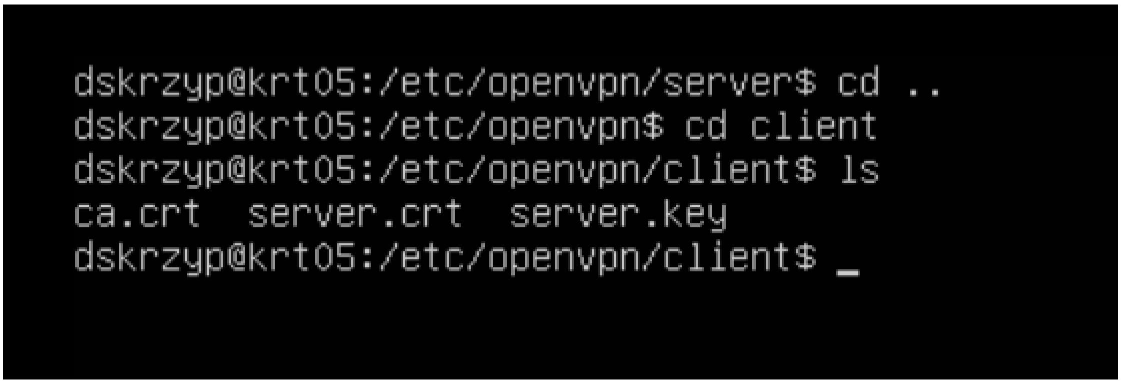
```
dskrzyp@krt05:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:92:2a:ee brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 10.40.60.130/24 brd 10.40.60.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe92:2aee/64 scope link
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group defau
lt qlen 500
    link/none
    inet 10.8.0.1/24 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::8a6e:2682:1abd:5b38/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
dskrzyp@krt05:/$ _
```

3. Konfiguracja plików



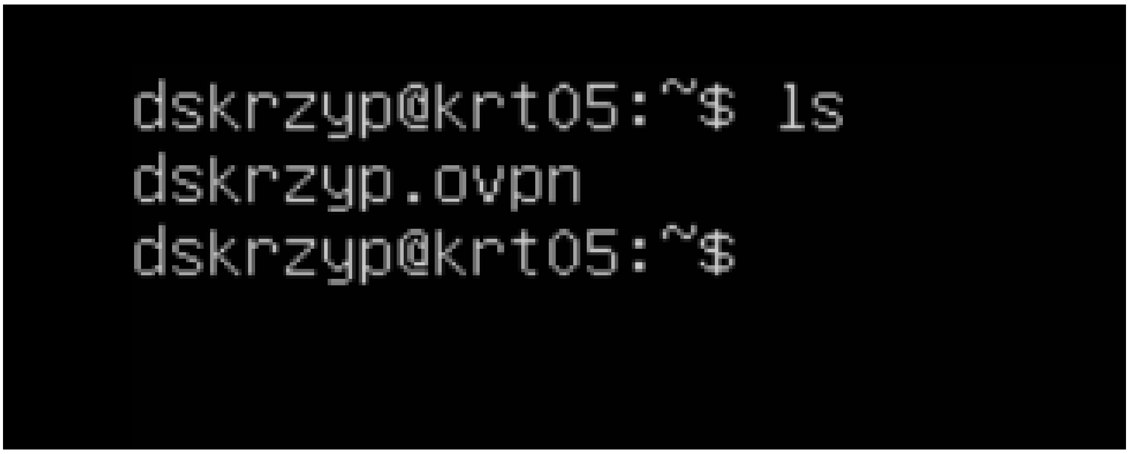
```
  GNU nano 6.2                                 server.conf *
local 10.40.60.130
port 1194
proto udp
dev tun
ca /etc/openvpn/client/ca.crt
cert /etc/openvpn/client/server.crt
key /etc/openvpn/client/server.key
dh dh.pem
auth SHA512
tls-crypt tc.key
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 1.1.1.1"
push "block-outside-dns"
keepalive 10 120
user nobody
group nogroup
persist-key
persist-tun
verb 3
crl-verify crl.pem
explicit-exit-notify
```

4. Certyfikaty OpenVPN



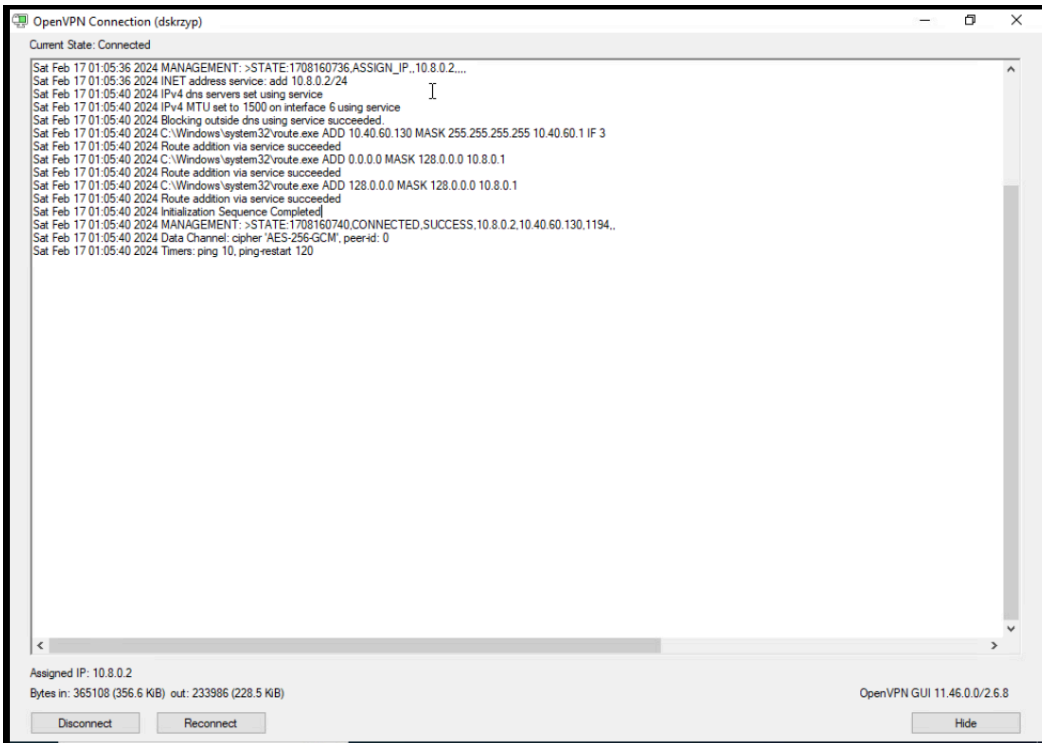
```
dskrzyp@krt05:/etc/openvpn/server$ cd ..
dskrzyp@krt05:/etc/openvpn$ cd client
dskrzyp@krt05:/etc/openvpn/client$ ls
ca.crt  server.crt  server.key
dskrzyp@krt05:/etc/openvpn/client$ _
```

5. Stworzony plik .ovpn



```
dskrzyp@krt05:~$ ls
dskrzyp.ovpn
dskrzyp@krt05:~$
```

6. Połączenie po stronie klienta



Current State: Connected

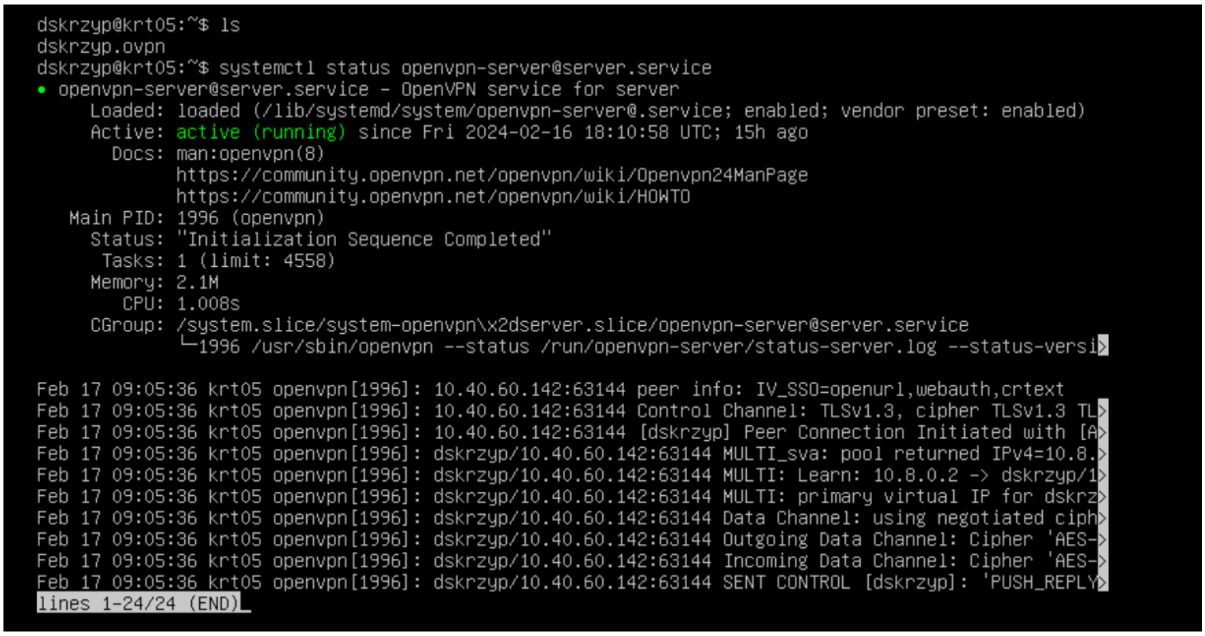
```
Sat Feb 17 01:05:36 2024 MANAGEMENT: >STATE:1708160736,ASSIGN_IP,,10.8.0.2,,,,
Sat Feb 17 01:05:36 2024 INET address service: add 10.8.0.2/24
Sat Feb 17 01:05:40 2024 IPv4 dns servers set using service
Sat Feb 17 01:05:40 2024 IPv4 MTU set to 1500 on interface 6 using service
Sat Feb 17 01:05:40 2024 Blocking outside dns using service succeeded.
Sat Feb 17 01:05:40 2024 C:\Windows\system32\route.exe ADD 10.40.60.130 MASK 255.255.255.255 10.40.60.1 IF 3
Sat Feb 17 01:05:40 2024 Route addition via service succeeded
Sat Feb 17 01:05:40 2024 C:\Windows\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.8.0.1
Sat Feb 17 01:05:40 2024 Route addition via service succeeded
Sat Feb 17 01:05:40 2024 C:\Windows\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.8.0.1
Sat Feb 17 01:05:40 2024 Route addition via service succeeded
Sat Feb 17 01:05:40 2024 Initialization Sequence Completed
Sat Feb 17 01:05:40 2024 MANAGEMENT: >STATE:1708160740,CONNECTED,SUCCESS,10.8.0.2,10.40.60.130,1194,,
Sat Feb 17 01:05:40 2024 Data Channel: cipher 'AES-256-GCM', peer-id: 0
Sat Feb 17 01:05:40 2024 Timers: ping 10, ping-restart 120
```

Assigned IP: 10.8.0.2

Bytes in: 365108 (356.6 KiB) out: 233986 (228.5 KiB)

OpenVPN GUI 11.46.0.0/2.6.8

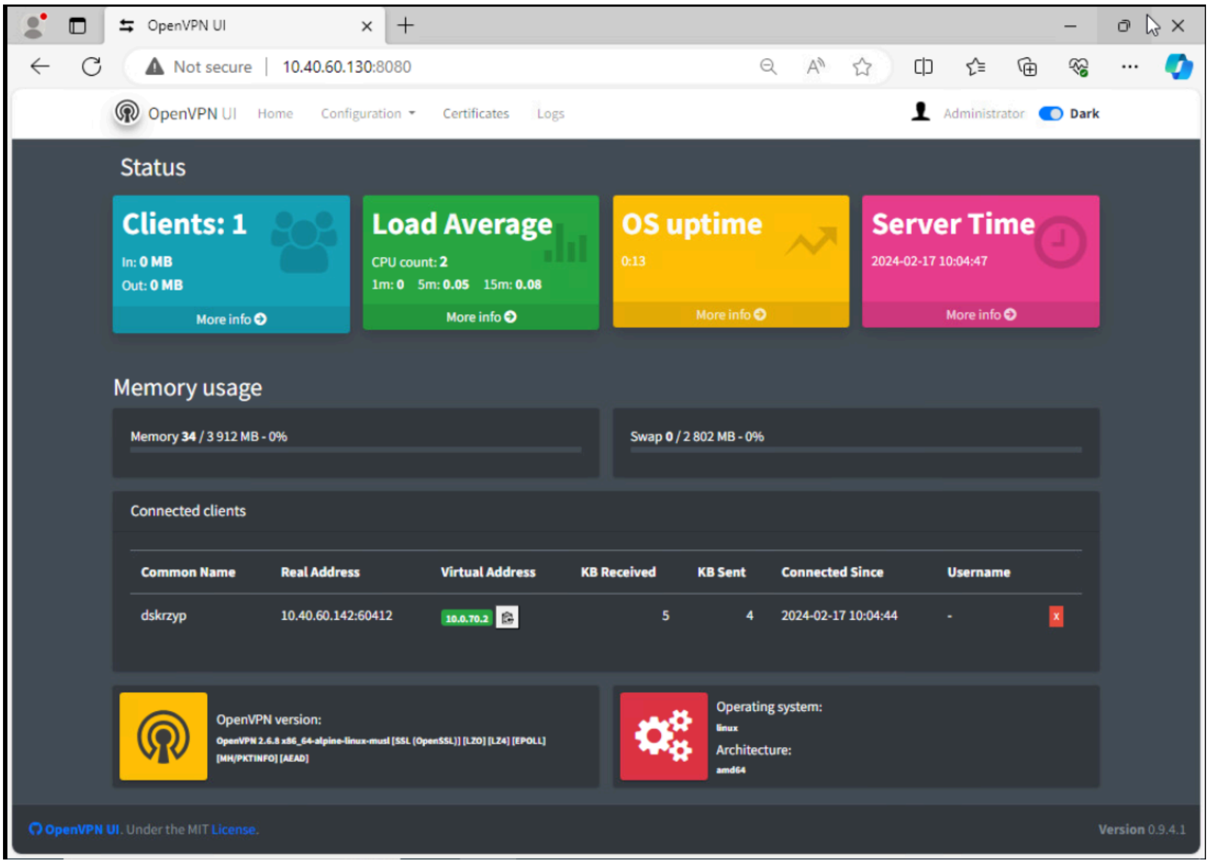
7. Logi z serwera Ubuntu



```
dskrzyp@krt05:~$ ls
dskrzyp.ovpn
dskrzyp@krt05:~$ systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-02-16 18:10:58 UTC; 15h ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 1996 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 4558)
     Memory: 2.1M
        CPU: 1.008s
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
             └─1996 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-versi>

Feb 17 09:05:36 krt05 openvpn[1996]: 10.40.60.142:63144 peer info: IV_SSO=openurl,webauth,crtext
Feb 17 09:05:36 krt05 openvpn[1996]: 10.40.60.142:63144 Control Channel: TLSv1.3, cipher TLSv1.3 TL>
Feb 17 09:05:36 krt05 openvpn[1996]: 10.40.60.142:63144 [dskrzyp] Peer Connection Initiated with [A>
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 MULTI_sva: pool returned IPv4=10.8.>
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 MULTI: Learn: 10.8.0.2 -> dskrzyp/1>
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 MULTI: primary virtual IP for dskrz>
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 Data Channel: using negotiated ciph>
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 Outgoing Data Channel: Cipher 'AES->
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 Incoming Data Channel: Cipher 'AES->
Feb 17 09:05:36 krt05 openvpn[1996]: dskrzyp/10.40.60.142:63144 SENT CONTROL [dskrzyp]: 'PUSH_REPLY>
lines 1-24/24 (END)
```

8. Interfejs graficzny OpenVPN UI



Status

Clients: 1

In: **0 MB**

Out: **0 MB**

More info

Load Average

CPU count: **2**

1m: **0** 5m: **0.05** 15m: **0.08**

More info

OS uptime

0:13

More info

Server Time

2024-02-17 10:04:47

More info

Memory usage

Memory **34** / 3 912 MB - 0%

Swap **0** / 2 802 MB - 0%

Connected clients

Common Name	Real Address	Virtual Address	KB Received	KB Sent	Connected Since	Username	
dskrzyp	10.40.60.142:60412	10.0.70.2	5	4	2024-02-17 10:04:44	-	x

OpenVPN version:

OpenVPN 2.6.8 x86_64-alpine-linux-musl [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [MH/PKTINFO] [AEAD]

Operating system:

linux

Architecture:

amd64

OpenVPN UI. Under the MIT License.

Version 0.9.4.1