

Instrukcja instalacji OpenVPN na systemie operacyjnym Linux



UWAGA!

Przykładowa instalacja odbywa się na dystrybucji Ubuntu 20.04. Na innych dystrybucjach systemu operacyjnego Linux, instalacja może odbywać się inaczej.

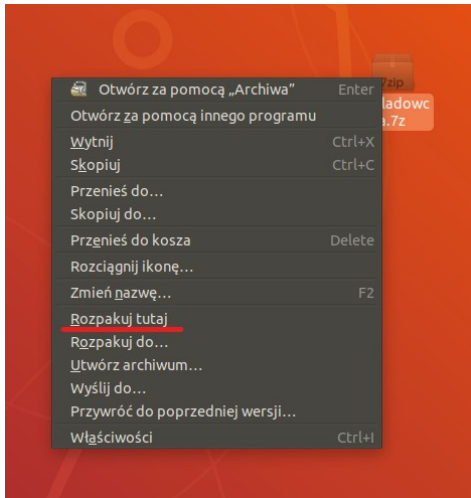
1. Na samym początku należy z wykorzystaniem komend **sudo apt update** oraz **sudo apt install** zainstalować aktualizacje.

```
jacob@jacob-VirtualBox:~$ sudo apt update
[sudo] hasło użytkownika jacob:
Stary:1 http://pl.archive.ubuntu.com/ubuntu bionic InRelease
Stary:2 http://pl.archive.ubuntu.com/ubuntu bionic-updates InRelease
Stary:3 http://pl.archive.ubuntu.com/ubuntu bionic-backports InRelease
Pobieranie:4 http://security.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Pobieranie:5 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11
Metadata [55,1 kB]
Pobieranie:6 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DE
P-11 Metadata [59,5 kB]
Pobieranie:7 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64
DEP-11 Metadata [2 464 B]
Pobrano 206 kB w 1s (164 kB/s)
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Wszystkie pakiety są aktualne.
jacob@jacob-VirtualBox:~$ sudo apt install
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostały zainstalowane automatycznie i nie są już więcej wyma
gane:
 libpkcs11-helper1 linux-headers-5.4.0-77-generic
 linux-hwe-5.4-headers-5.4.0-42 linux-hwe-5.4-headers-5.4.0-77
 linux-image-5.4.0-77-generic linux-modules-5.4.0-77-generic
 linux-modules-extra-5.4.0-77-generic
Aby je usunąć należy użyć "sudo apt autoremove".
0 aktualizowanych, 0 nowo instalowanych, 0 usuwanych i 0 nieaktualizowanych.
```

2. Następnie wykorzystując komendę **sudo apt install openvpn -y** zainstalować klienta OpenVPN.

```
jacob@jacob-VirtualBox:~$ sudo apt install openvpn -y
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostają zainstalowane automatycznie i nie są już więcej wyma
gane:
 linux-headers-5.4.0-77-generic linux-hwe-5.4-headers-5.4.0-42
 linux-hwe-5.4-headers-5.4.0-77 linux-image-5.4.0-77-generic
 linux-modules-5.4.0-77-generic linux-modules-extra-5.4.0-77-generic
Aby je usunąć należy użyć "sudo apt autoremove".
Sugerowane pakiety:
 easy-rsa resolvconf
Zostaną zainstalowane następujące NOWE pakiety:
 openvpn
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 0 nieaktualizowanych.
Konieczne pobranie 470 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 1 136 kB miejsca na dysku.
Pobieranie:1 http://pl.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openv
pn amd64 2.4.4-2ubuntu1.6 [470 kB]
Pobrano 470 kB w 0s (944 kB/s)
Prekonfiguracja pakietów ...
Wybieranie wcześniej niewybranego pakietu openvpn.
(Odczytywanie bazy danych ... 219508 plików i katalogów obecnie zainstalowanych.
)
Przygotowywanie do rozpakowania pakietu ../openvpn_2.4.4-2ubuntu1.6_amd64.deb .
..
Rozpakowywanie pakietu openvpn (2.4.4-2ubuntu1.6) ...
Konfigurowanie pakietu openvpn (2.4.4-2ubuntu1.6) ...
Przetwarzanie wyzwalaczy pakietu man-db (2.8.3-2ubuntu0.1)...
Przetwarzanie wyzwalaczy pakietu ureadahead (0.100.0-21)...
Przetwarzanie wyzwalaczy pakietu systemd (237-3ubuntu10.53)...
```

- Następnie należy wypakować prawym przyciskiem myszy lub komendą archiwum z certyfikatami, wpisując hasło otrzymane przez platformę MS Teams (dostęp 1).

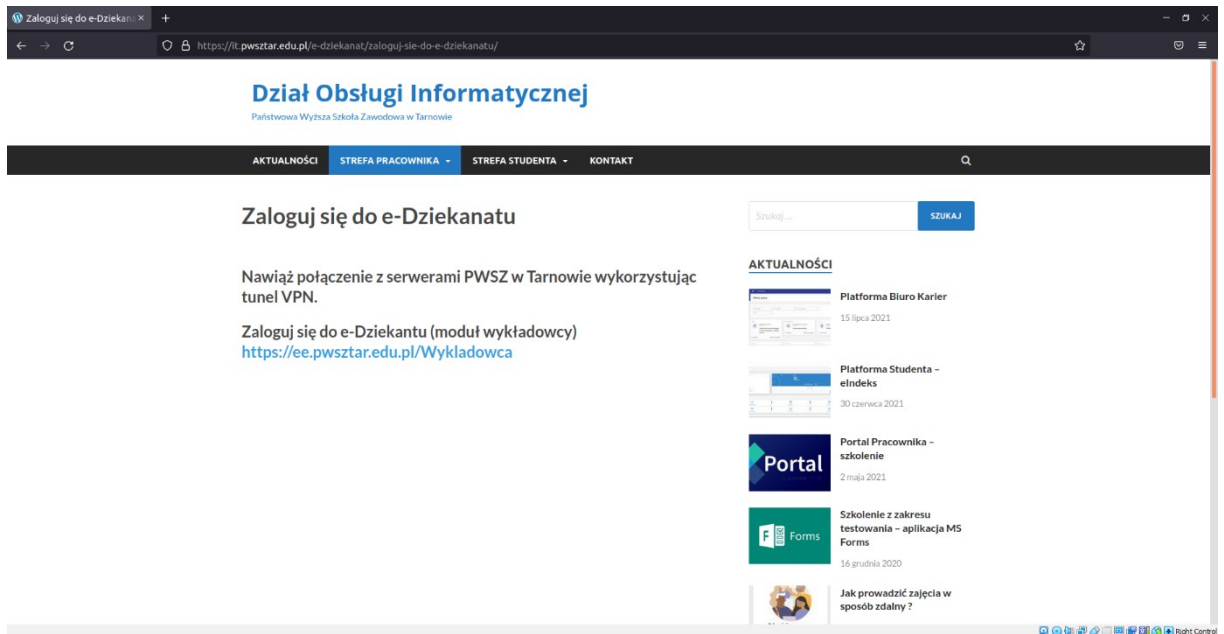


- Następnie wykorzystując polecenie **cd**, należy przejść do lokalizacji gdzie zostało wypakowane archiwum i wykonać polecenie **sudo openvpn --config wykladowca.ovpn**

```

jacob@jacob-VirtualBox:~$ cd /home/jacob/Pulpit/wykladowca/
jacob@jacob-VirtualBox:~/Pulpit/wykladowca$ sudo openvpn --config wykladowca.ovpn
[sudo] hasło użytkownika jacob:
Mon Feb 14 12:58:25 2022 WARNING: file 'wykladowca.key' is group or others accessible
Mon Feb 14 12:58:25 2022 WARNING: file 'ta.key' is group or others accessible
Mon Feb 14 12:58:25 2022 OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PTINFO] [AEAD] built on Jul 19 2021
Mon Feb 14 12:58:25 2022 library versions: OpenSSL 1.1.1 11 Sep 2018, LZO 2.08
Mon Feb 14 12:58:25 2022 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Feb 14 12:58:25 2022 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Feb 14 12:58:25 2022 TCP/UDP: Preserving recently used remote address: [AF_INET]195.150.230.100:7889
Mon Feb 14 12:58:25 2022 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Feb 14 12:58:25 2022 UDP link local: (not bound)
Mon Feb 14 12:58:25 2022 UDP link remote: [AF_INET]195.150.230.100:7889
Mon Feb 14 12:58:25 2022 TLS: Initlal packet from [AF_INET]195.150.230.100:7889, sid=ab2f8148 505b0dd0
Mon Feb 14 12:58:25 2022 VERIFY OK: depth=1, C=PL, ST=Malopolska, L=Tarnow, O=PWSZTarnow, OU=DzialObslugiInformatycznej, CN=pwszstar.edu.pl, name=server, emailAddress=m_niedziela@pwszstar.edu.pl
Mon Feb 14 12:58:25 2022 VERIFY X509 OK
Mon Feb 14 12:58:25 2022 Validating certificate extended key usage
Mon Feb 14 12:58:25 2022 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Mon Feb 14 12:58:25 2022 VERIFY X509 OK
Mon Feb 14 12:58:25 2022 VERIFY OK: depth=0, C=PL, ST=Malopolska, L=Tarnow, O=PWSZTarnow, OU=DzialObslugiInformatycznej, CN=server, name=server, emailAddress=m_niedziela@pwszstar.edu.pl
Mon Feb 14 12:58:25 2022 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Mon Feb 14 12:58:25 2022 [server] Peer Connection Initiated with [AF_INET]195.150.230.100:7889
Mon Feb 14 12:58:26 2022 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Mon Feb 14 12:58:26 2022 PUSH: Received control message: 'PUSH_REPLY,route 172.16.16.0 255.255.248.0,route 172.16.16.20 255.255.255.255,route 172.16.16.21 255.255.255.255,dhcp-option DNS 8.8.8.8,dhcp-option dn DNS 8.8.4.4,route-gateway 172.16.16.1,ping 10,ping-restart 120,ifconfig 172.16.16.132 255.255.248.0,peer-id 32,cipher AES-256-GCM'
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: timers and/or timeouts modified
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: --ifconfig/up options modified
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: route options modified
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: route-related options modified
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: --ip-wtn32 and/or --dhcp-option options modified
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: peer-id set
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: adjusting link_mtu to 1656
Mon Feb 14 12:58:26 2022 OPTIONS IMPORT: data channel crypto options modified
Mon Feb 14 12:58:26 2022 Data Channel: using negotiated cipher 'AES-256-GCM'
Mon Feb 14 12:58:26 2022 Outgoing Data Channel: cipher 'AES-256-GCM' initialized with 256 bit key
Mon Feb 14 12:58:26 2022 Incoming Data Channel: cipher 'AES-256-GCM' initialized with 256 bit key
Mon Feb 14 12:58:26 2022 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=ens3 HWADDR=08:00:27:3c:58:f7
Mon Feb 14 12:58:26 2022 TUN/TAP device tap0 opened
Mon Feb 14 12:58:26 2022 TUN/TAP TX queue length set to 100
Mon Feb 14 12:58:26 2022 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Mon Feb 14 12:58:26 2022 /sbin/ip link set dev tap0 up mtu 1500
Mon Feb 14 12:58:26 2022 /sbin/ip addr add dev tap0 172.16.16.132/21 broadcast 172.16.23.255
Mon Feb 14 12:58:26 2022 /sbin/ip route add 172.16.16.0/21 via 172.16.16.1
RINEILINK answers: file exists
Mon Feb 14 12:58:26 2022 ERROR: Linux route add command failed: external program exited with error status: 2
Mon Feb 14 12:58:26 2022 /sbin/ip route add 172.16.16.20/32 via 172.16.16.1
Mon Feb 14 12:58:26 2022 /sbin/ip route add 172.16.16.21/32 via 172.16.16.1
Mon Feb 14 12:58:26 2022 Initialization Sequence Completed
```

5. Następnie należy przejść na stronę Działu Obsługi Informatycznej i zalogować się do e-Dziekanatu.



6. Powinno ukazać się okno logowania. Należy teraz wpisać login oraz hasło otrzymane za pośrednictwem platformy MS Teams (dostęp 2).

