



**Kauno technologijos universitetas**

Informatikos fakultetas

## **VPN tinklo sudarymas ir saugumo tyrimas**

Kompiuterių tinklų sauga (T120M121)

Atliko:

IFM-1/3 gr. studentas

Eligijus Kiudys

2021 m. lapkričio 27 d.

Priėmė:

Asist. Šatkauskas Nerijus

**Kaunas 2021**

## 1. Darbo eiga.

### 1. Pasirengimas laboratoriniam darbui

#### 1.1. Pašalinamas virtualus interfeisas

```
openvpn --rmtun --dev tap0
```

#### 1.2. Išinstaliuoti OpenVPN

```
apt-get --purge remove openvpn
```

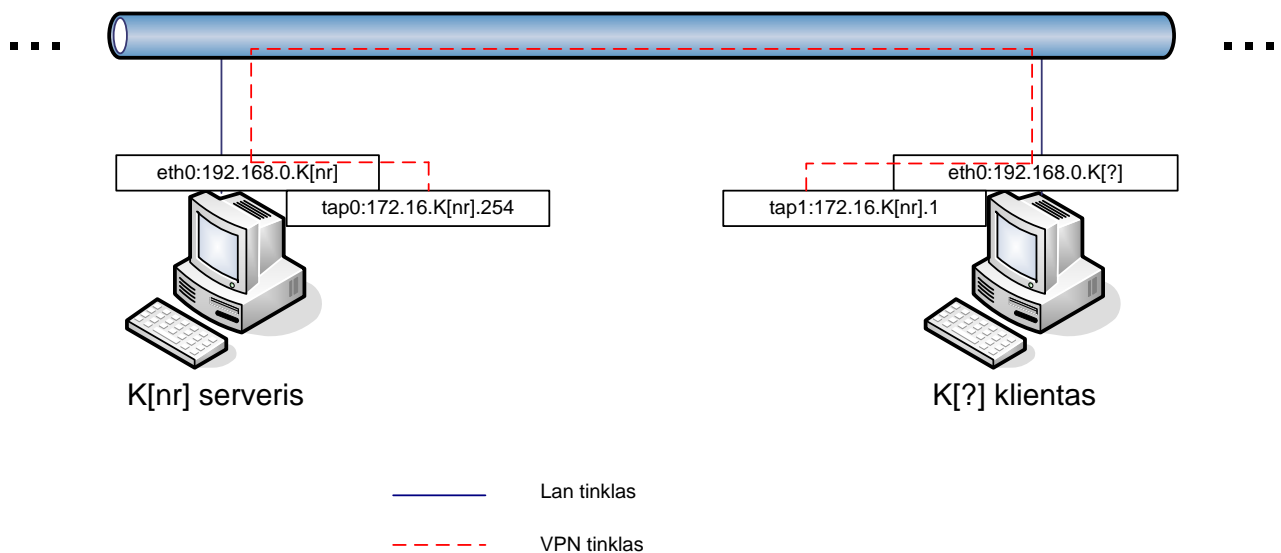
#### 1.3. Ištrinami OpenVPN konfigūracijos katalogai

```
rm -r /root/secret  
rm -r /root/openvpn
```

## 2. OpenVPN įdiegimas ir kliento konfigūravimas

**Pastaba!** *Generuojant raktus/sertifikatus bei konfigūruojant IP adresus 'S[nr]' simboliu žymimas serverio numeris, o 'K?' simboliu kliento(jūsų) kompiuterio numeris.*

**Laboratorinio darbo schema:**



```
root@K9:~# echo 'deb http://old-releases.ubuntu.com/ubuntu/ karmic main restricted universe multiverse
```

```
deb http://old-releases.ubuntu.com/ubuntu/ karmic-updates main restricted universe multiverse
```

```
deb http://old-releases.ubuntu.com/ubuntu/ karmic-security main restricted universe multiverse  
' > /etc/apt/sources.list
```

```
root@K9:~# apt-get update # Atsisiuncia paketu sarasus
```

### 2.1. Į sistemą įdiegiamas openvpn paketas:

```
apt-get install openvpn
```

### 2.2. Sukuriamas katalogas raktams, visi pakeitimai laboratorinio darbo metu bus atliekami šiame kataloge

```
mkdir /root/secret
```

### 2.3. Nukopijuojami raktų kūrimo įrankiai į sukurta katalogą ir pakeičiamas darbinis katalogas

```
cp -R /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /root/secret/  
cd /root/secret/
```

### 2.4. Prieš pradėdant raktų ir sertifikatų generavimą, reikia nustatyti pradinis sertifikatų parametrus. Šie parametrai saugomi *vars* faile. Failo redagavimui naudosime *nano* programą

```
nano vars
```

Numatytąjį rakto dydį 1024 pakeiskite į 2048, ilgesnis raktas suteikia didesnę saugumą, tačiau nuo rakto ilgio priklauso Diffie-Hellman parametrų generavimo laikas, bei TLS sujungimo laikas. KEY\_SIZE turi būti suderintas abiejuose ryšio užmezgime dalyvaujančiuose kompiuteriuose.

```
export KEY_SIZE=2048  
export KEY_COUNTRY="LT"  
export KEY_PROVINCE=""  
export KEY_CITY="Kaunas"  
export KEY_ORG="KTU"  
export KEY_EMAIL=K6_klientas@K6.lt
```

### 2.5. Nuskaitomi raktų ir sertifikatų parametrai

```
source ./vars
```

### 2.6. Išvalomas katalogas

```
./clean-all
```

### 2.7. Generuojami Diffie-Hellman parametrai, kadangi rakto dydis buvo padidintas iki 2048 bitų, todėl šių parametrų generavimas gali užtrukti keletą minučių, turėkite kantrybės ir palaukite kol bus baigtas parametrų generavimas.

```
./build-dh
```

### 2.8. Sukuriame katalogą konfigūracijai ir raktams

```
mkdir /root/openvpn
```

### 2.9. Generuojamas sertifikato prašymas.

```
./build-req K6_client
```

```
Generating a 2048 bit RSA private key
```

```
..+++
```

```
.....+++
```

```
writing new private key to 'K6_client.key'
```

```
-----
```

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [LT]:
```

**Spauskite Enter**

```
State or Province Name (full name) []:
```

**Spauskite Enter**

```
Locality Name (eg, city) [Kaunas]:
```

**Spauskite Enter**

Organization Name (eg, company) [KTU]: **Spauskite Enter**

Organizational Unit Name (eg, section) []: **Spauskite Enter**

Common Name (eg, your name or your server's hostname) [K?\_client]: **Spauskite Enter**  
Name []: **Spauskite Enter**

Email Address [K6\_klientas@K6.lt]: **Spauskite Enter**

Please enter the following 'extra' attributes  
to be sent with your certificate request

A challenge password []: **Spauskite Enter**

An optional company name []: **Spauskite Enter**

Nukopijuokite K6\_client.key į /root/openvpn katalogą

```
cp keys/K?_client.key /root/openvpn
```

## 2.10. Sugeneruotas sertifikato prašymas turi būti nusiųstas dėstytojui

Siunčiamas failas '/root/secret/keys/K6\_client.csr'

Sertifikato prašymo persiuntimui į serverį galite naudotis komandą:

```
scp /root/secret/keys/K6_client.csr root@ 158.129.6.169:/root/secret/keys
```

## 2.11. Į /tmp/ katalogą parsisiųskite failus K6\_client.crt, ca.crt ir ta.key iš dėstytojo:

```
scp root@ 158.129.6.169:/root/secret/keys/K6_client.crt /tmp/
```

taip pat iš ir kitus 2 failus: **ca.crt** ir **ta.key**

**# DĖMESIO iš dėstytojo gautą ca.crt pervadinkite į ca\_s[nr].crt, kad neužrašytumėte jo ant savo ca.crt. ta.key pervadinkite į ta\_s[nr].key Jei parsisiųsti failai išsaugoti /tmp/ kataloge, tuomet naudokite žemiau esančias komandas failų perkėlimui į /root/openvpn katalogą, jei ne – perkėlimo komandą atitinkamai pakoreguokite.**

```
mv /tmp/K6_client.crt /root/openvpn  
mv /tmp/ca.crt /root/openvpn/ca_S203.crt  
mv /tmp/ta.key /root/openvpn/ta_S203.key
```

## 2.12. Sukonfigūruokite OpenVPN klientą

Pakeiskite darbinį katalogą

```
cd /root/openvpn
```

Nusikopijuokite šabloninį kliento konfigūracijos failą

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf client.conf
```

Failo redagavimui naudojama nano programa.

```
nano client.conf
```

Konfigūraciniame faile aktyvūs parametrai eilutės pradžioje neturi kabliataškio (;). Nereikalingi parametrai išjungiami eilutės pradžioje parašius kabliataškį.

Konfigūraciniame faile atliekami tokie pakeitimai:

dev tap	# Bus naudojamas L2 VPN
;dev tun	# Išjungiamas L3 VPN parametras
remote 158.129.6.169 1194	# Nurodomas serverio IP adresas ir prievadas
ca /root/openvpn/ca_S203.crt	# Nurodomi reikiami atitinkami keliai iki
cert /root/openvpn/K6_client.crt	# reikiamų sertifikatų ir raktų
key /root/openvpn/K6_client.key	

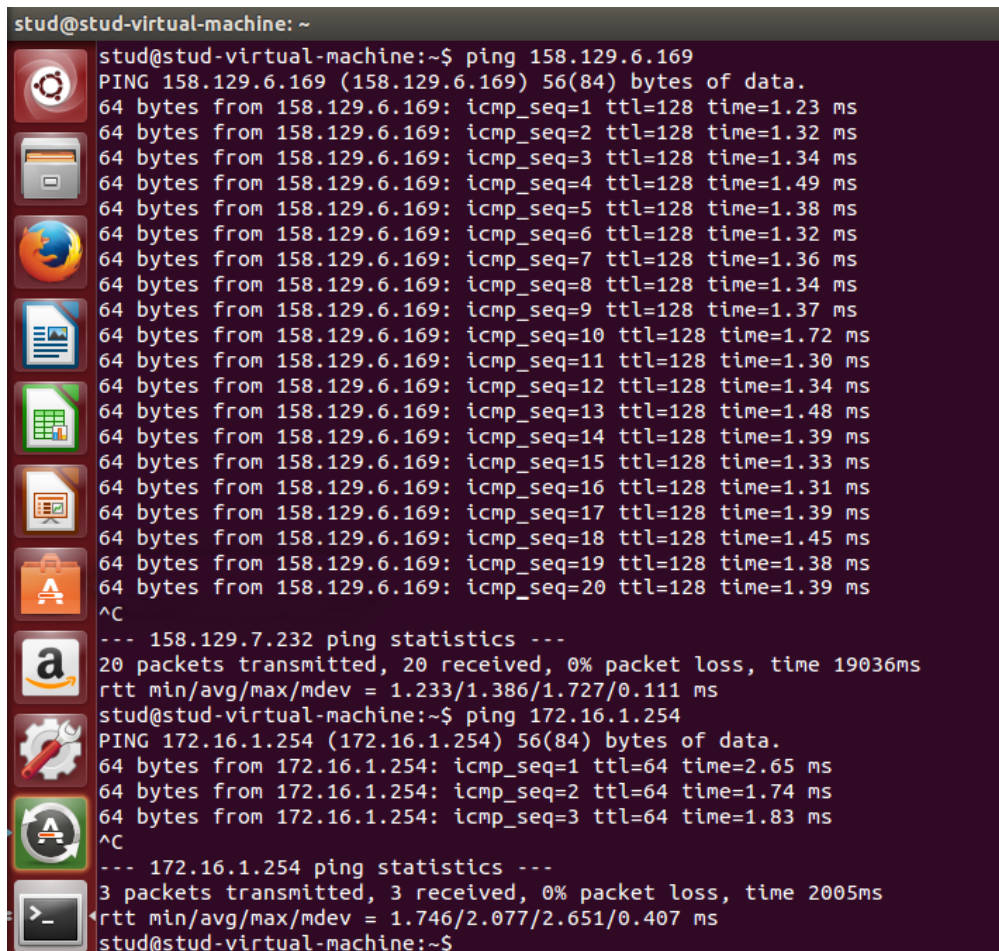
```
tls-auth /root/openvpn/ta_G203.key 1
```

### 2.13. Paleidžiamas OpenVPN klientas

```
openvpn --config /root/openvpn/client.conf
```

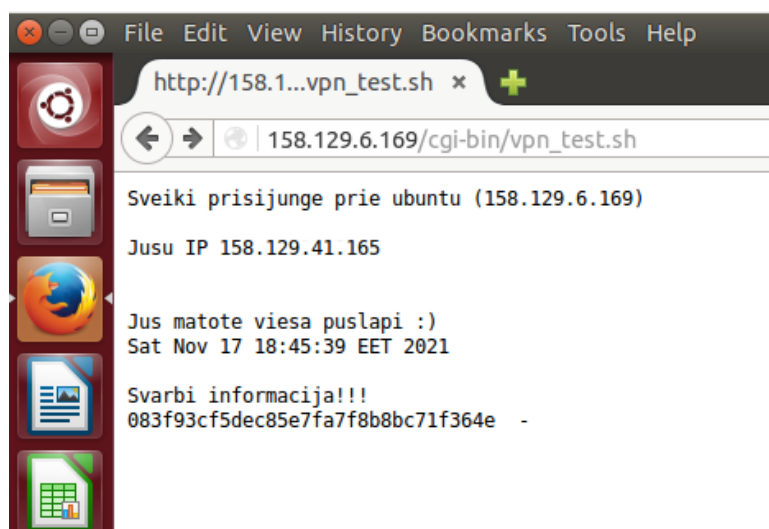
## 3. Darbo išvados

Gavus rezultatus galime matyti, kad VPN yra sukonfigūruotas gerai. Konfigūruojant VPN buvo problemų, kad nėjo gerai sukonfigūruoti, bet gale susitvarkiau iškilusias problemas ir viską pavyko užbaigti.

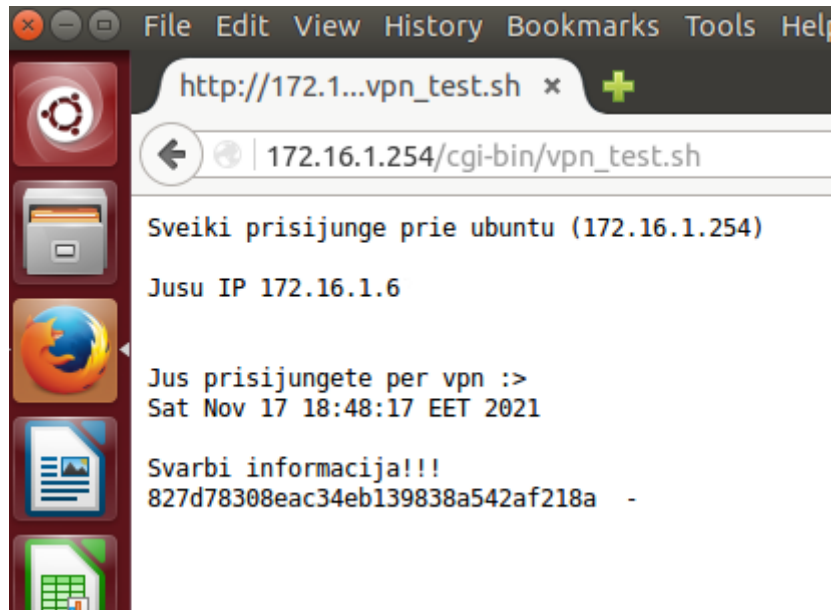


```
stud@stud-virtual-machine: ~  
stud@stud-virtual-machine:~$ ping 158.129.6.169  
PING 158.129.6.169 (158.129.6.169) 56(84) bytes of data.  
64 bytes from 158.129.6.169: icmp_seq=1 ttl=128 time=1.23 ms  
64 bytes from 158.129.6.169: icmp_seq=2 ttl=128 time=1.32 ms  
64 bytes from 158.129.6.169: icmp_seq=3 ttl=128 time=1.34 ms  
64 bytes from 158.129.6.169: icmp_seq=4 ttl=128 time=1.49 ms  
64 bytes from 158.129.6.169: icmp_seq=5 ttl=128 time=1.38 ms  
64 bytes from 158.129.6.169: icmp_seq=6 ttl=128 time=1.32 ms  
64 bytes from 158.129.6.169: icmp_seq=7 ttl=128 time=1.36 ms  
64 bytes from 158.129.6.169: icmp_seq=8 ttl=128 time=1.34 ms  
64 bytes from 158.129.6.169: icmp_seq=9 ttl=128 time=1.37 ms  
64 bytes from 158.129.6.169: icmp_seq=10 ttl=128 time=1.72 ms  
64 bytes from 158.129.6.169: icmp_seq=11 ttl=128 time=1.30 ms  
64 bytes from 158.129.6.169: icmp_seq=12 ttl=128 time=1.34 ms  
64 bytes from 158.129.6.169: icmp_seq=13 ttl=128 time=1.48 ms  
64 bytes from 158.129.6.169: icmp_seq=14 ttl=128 time=1.39 ms  
64 bytes from 158.129.6.169: icmp_seq=15 ttl=128 time=1.33 ms  
64 bytes from 158.129.6.169: icmp_seq=16 ttl=128 time=1.31 ms  
64 bytes from 158.129.6.169: icmp_seq=17 ttl=128 time=1.39 ms  
64 bytes from 158.129.6.169: icmp_seq=18 ttl=128 time=1.45 ms  
64 bytes from 158.129.6.169: icmp_seq=19 ttl=128 time=1.38 ms  
64 bytes from 158.129.6.169: icmp_seq=20 ttl=128 time=1.39 ms  
^C  
--- 158.129.7.232 ping statistics ---  
20 packets transmitted, 20 received, 0% packet loss, time 19036ms  
rtt min/avg/max/mdev = 1.233/1.386/1.727/0.111 ms  
stud@stud-virtual-machine:~$ ping 172.16.1.254  
PING 172.16.1.254 (172.16.1.254) 56(84) bytes of data.  
64 bytes from 172.16.1.254: icmp_seq=1 ttl=64 time=2.65 ms  
64 bytes from 172.16.1.254: icmp_seq=2 ttl=64 time=1.74 ms  
64 bytes from 172.16.1.254: icmp_seq=3 ttl=64 time=1.83 ms  
^C  
--- 172.16.1.254 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2005ms  
rtt min/avg/max/mdev = 1.746/2.077/2.651/0.407 ms  
stud@stud-virtual-machine:~$
```

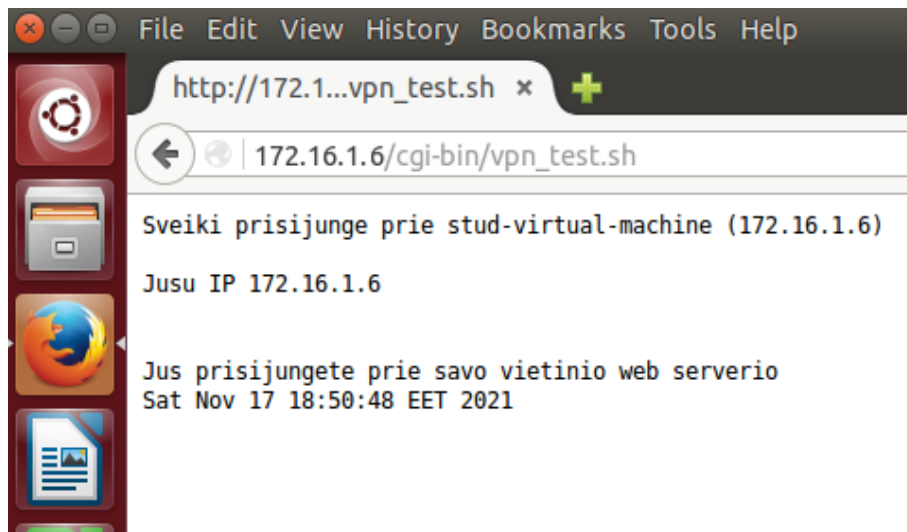
pav. 1 Ping komandos panaudojimas



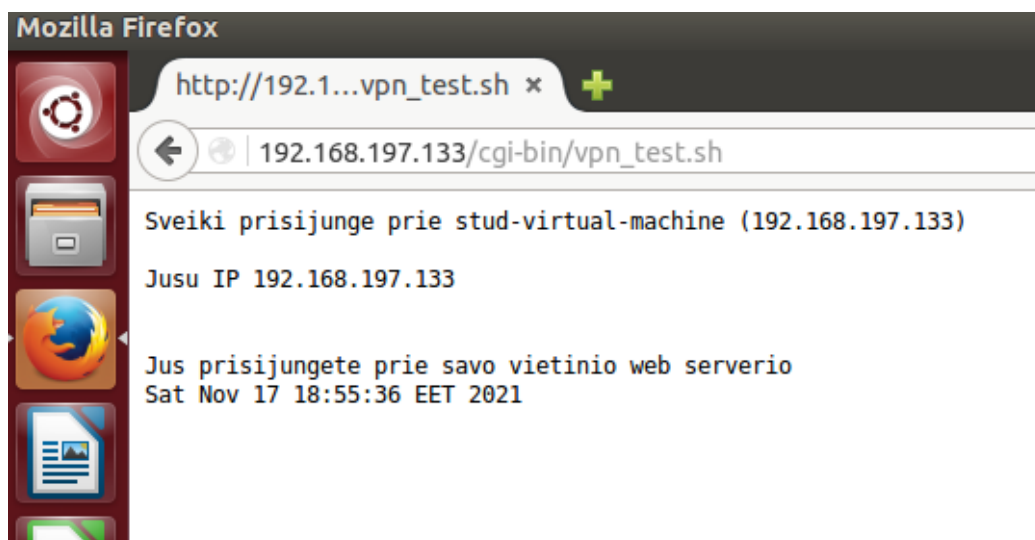
pav. 2 158.129.6.169/cgi-bin/vpn\_test.sh turinys



pav. 3 Puslapio 172.16.1.254/cgi-bin/vpn\_test.sh turinys



pav. 4 Puslapio 172.16.1.6/cgi-bin/vpn\_test.sh turinys



pav. 5 Puslapio 192.168.197.133/cgi-bin/vpn\_test.sh turinys