

Практикалық сабақ №14: VPN технологияларын пайдалану схемалары. IPsec туралы ақпарат.

VPN (Virtual Private Network) - виртуалды жеке желі, бір-бірінен белгілі бір қашықтықта орналасқан бірнеше компьютерді бір логикалық желіге біріктірудің тәсілі.

Сіз VPN – ді әртүрлі мақсаттарда пайдалана аласыз-желіні ұйымдастырудан бастап, жұмыс/ойын үшін интернетке кіруге дейін. Бұл жағдайда сіз өзіңіздің әрекеттеріңіз үшін заңды жауапкершілікті түсінуіңіз керек.

Ubuntu Linux жүйесінде серверлік баптаулар

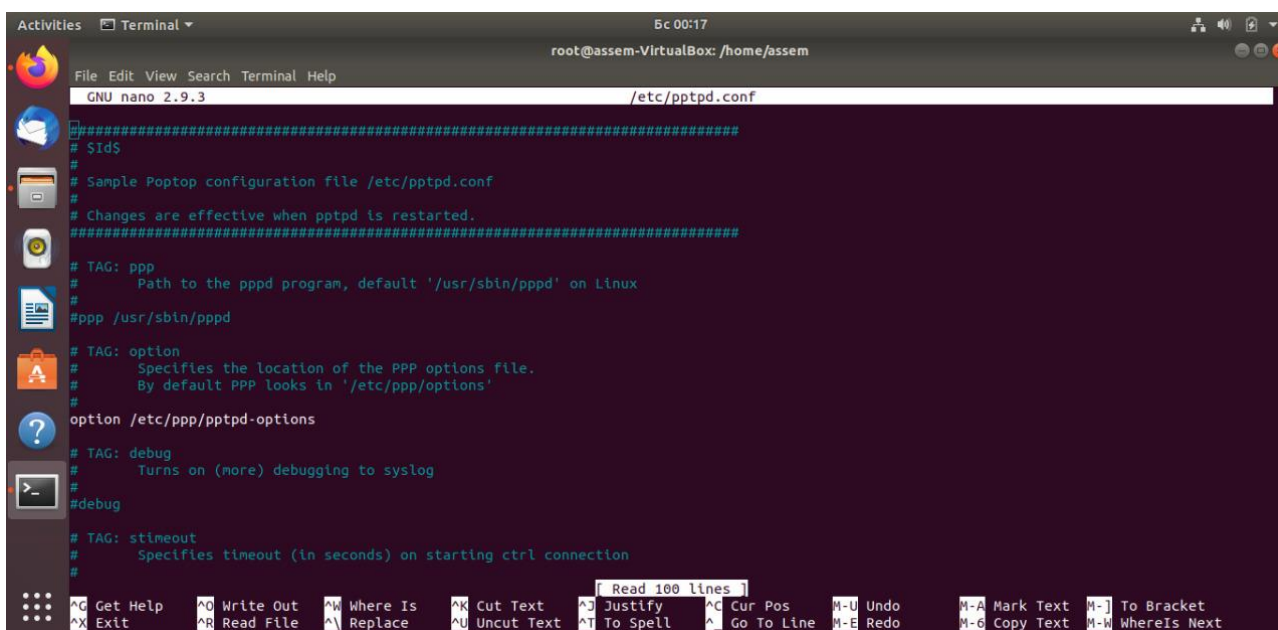
Сервер үшін Linux-ті қолданған дұрыс, онымен жұмыс істеу оңайырақ. Ең оңай нұсқа – PPTP, ол клиенттердің компьютерлеріне сертификаттарды орнатуды қажет етпейді, аутентификация пайдаланушы аты мен пароль арқылы жүзеге асырылады.

Алдымен қажетті пакеттерді орнатыңыз:

```
root@assem-VirtualBox:/home/assem# sudo apt install pptpd
Reading package lists... Done
Building dependency tree
```

Әрі қарай, мекен-жай ауқымын және басқа да негізгі параметрлерді орнату керек. Өңдеу үшін /etc/pptpd файлын ашыңыз.conf:

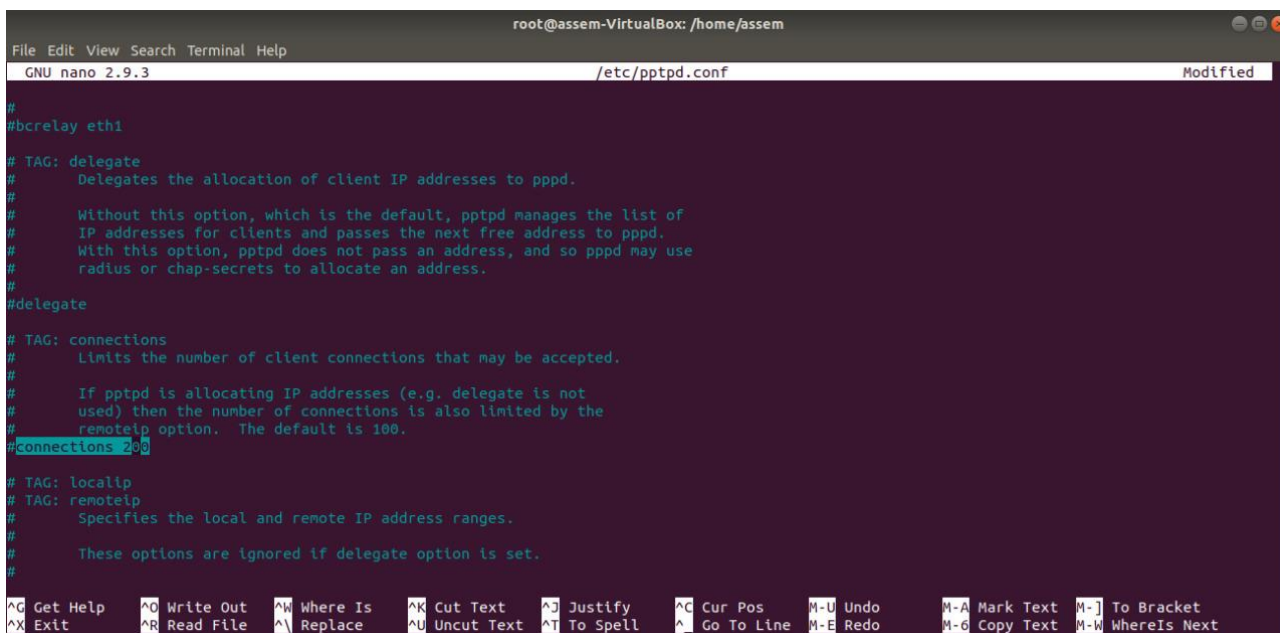
sudo nano /etc/pptpd.conf



```
root@assem-VirtualBox: /home/assem
GNU nano 2.9.3 /etc/pptpd.conf
#####
# $Id$
#
# Sample Poptop configuration file /etc/pptpd.conf
#
# Changes are effective when pptpd is restarted.
#####
# TAG: ppp
# Path to the pppd program, default '/usr/sbin/pppd' on Linux
#pppd /usr/sbin/pppd
#
# TAG: option
# Specifies the location of the PPP options file.
# By default PPP looks in '/etc/ppp/options'
#
option /etc/ppp/pptpd-options
#
# TAG: debug
# Turns on (more) debugging to syslog
#
#debug
#
# TAG: stimeout
# Specifies timeout (in seconds) on starting ctrl connection
#
#####
Read 100 lines
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^U Undo ^A Mark Text ^] To Bracket
^X Exit ^R Read File ^L Replace ^U Uncut Text ^T To Spell ^_ Go To Line ^E Redo ^G Copy Text ^_ Whereis Next
```

Егер бізге бір уақытта 100-ден астам байланыс қажет болса, "қосылымдар" параметрін ізденізі, оны ажыратыңыз және қажетті мәнді көрсетіңіз, мысалы:

connections 200



```
root@assem-VirtualBox: /home/assem
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/pptpd.conf Modified

#
#bcrelay eth1

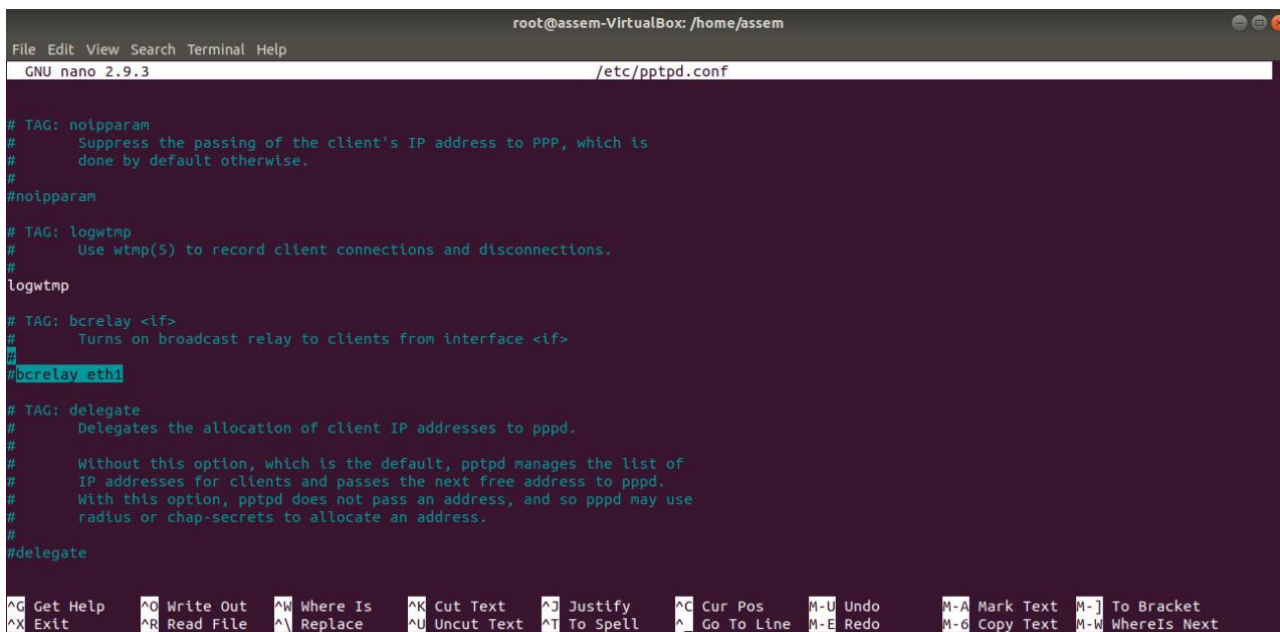
# TAG: delegate
#   Delegates the allocation of client IP addresses to pppd.
#
#   Without this option, which is the default, pptpd manages the list of
#   IP addresses for clients and passes the next free address to pppd.
#   With this option, pptpd does not pass an address, and so pppd may use
#   radius or chap-secrets to allocate an address.
#
#delegate

# TAG: connections
#   Limits the number of client connections that may be accepted.
#
#   If pptpd is allocating IP addresses (e.g. delegate is not
#   used) then the number of connections is also limited by the
#   remotelip option. The default is 100.
#connections 200

# TAG: localip
# TAG: remotelip
#   Specifies the local and remote IP address ranges.
#
#   These options are ignored if delegate option is set.
#

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text   M-J To Bracket
^X Exit          ^R Read File    ^L Replace      ^U Uncut Text  ^T To Spell    ^_ Go To Line   M-E Redo       M-G Copy Text  M-W WhereIs Next
```

Егер виртуалды желі арқылы тарату пакеттерін жіберу қажет болса, bcrelay параметрінің де түсініктеме берілгеніне көз жеткізу керек:



```
root@assem-VirtualBox: /home/assem
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/pptpd.conf

# TAG: noipparam
#   Suppress the passing of the client's IP address to PPP, which is
#   done by default otherwise.
#
#noipparam

# TAG: logwtmp
#   Use wtmp(5) to record client connections and disconnections.
#
logwtmp

# TAG: bcrelay <if>
#   Turns on broadcast relay to clients from interface <if>
#
#bcrelay eth1

# TAG: delegate
#   Delegates the allocation of client IP addresses to pppd.
#
#   Without this option, which is the default, pptpd manages the list of
#   IP addresses for clients and passes the next free address to pppd.
#   With this option, pptpd does not pass an address, and so pppd may use
#   radius or chap-secrets to allocate an address.
#
#delegate

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text   M-J To Bracket
^X Exit          ^R Read File    ^L Replace      ^U Uncut Text  ^T To Spell    ^_ Go To Line   M-E Redo       M-G Copy Text  M-W WhereIs Next
```

Осыдан кейін файлдың соңына өтіп, мекен-жай параметрлерін қосыңыз:



```
#remotelip 10.10.10.2-254
#listen 11.22.33.44
localip 10.10.10.1
remotelip 10.10.10.2-254
listen 11.22.33.44

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text   M-J To Bracket
^X Exit          ^R Read File    ^L Replace      ^U Uncut Text  ^T To Spell    ^_ Go To Line   M-E Redo       M-G Copy Text  M-W WhereIs Next
```

```
GNU nano 2.9.3 /etc/ppd/ptpd.conf Modified
#
# 2. If you give more IP addresses than the value of connections,
# it will start at the beginning of the list and go until it
# gets connections IPs. Others will be ignored.
#
# 3. No shortcuts in ranges! ie. 234-8 does not mean 234 to 238,
# you must type 234-238 if you mean this.
#
# 4. If you give a single localIP, that's ok - all local IPs will
# be set to the given one. You MUST still give at least one remote
# IP for each simultaneous client.
#
# (Recommended)
#localip 192.168.0.1
#remotepip 192.168.0.234-238,192.168.0.245
# or
#localip 192.168.0.234-238,192.168.0.245
#remotepip 192.168.1.234-238,192.168.1.245
#localip 10.10.10.1
#remotepip 10.10.10.2-254
#listen 11.22.33.44
```

Бірінші параметр жергілікті желідегі сервердің IP мекенжайын көрсетеді, екіншісі-клиенттерге берілген IP мекенжайларының ауқымы, үшіншісі кіріс қосылымдарын қабылдау үшін интерфейстерді қандай сыртқы мекен-жай бойынша тыңдау керектігін көрсетеді. Яғни, бірнеше сыртқы мекен-жайлар болған кезде сіз тек біреуін тыңдай аласыз. Егер үшінші параметр көрсетілмесе, барлық қол жетімді сыртқы мекенжайлар тыңдалады.

Сақтап, файлды жабамыз. Қосымша параметрлер /etc/ppp/pptpd-опциялар файлында көрсеміз: `sudo nano /etc/ppp/pptpd-options`

```
File /etc/ppp/pptpd-options is being edited (by root with nano 2.9.3, PID 2590); continue?
Y Yes
N No [AC] Cancel
```

Біріншіден, біз аутентификацияның ескі және қауіпті әдістерін қолдануға тыйым салатын жолдар бар екеніне көз жеткіземіз:

```
name pppd
# Optional: domain name to use for authentication
# domain mydomain.net
# Strip the domain prefix from the username before authentication.
# (applies if you use pppd with chapms-strip-domain patch)
#chapms-strip-domain
# Encryption
# (There have been multiple versions of PPP with encryption support,
# choose with of the following sections you will use.)
# BSD licensed ppp-2.4.2 upstream with MPPE only, kernel module ppp_mppe.o
# {{{
refuse-pap
refuse-chap
refuse-mschap
# Require the peer to authenticate itself using MS-CHAPv2 [Microsoft
# Challenge Handshake Authentication Protocol, Version 2] authentication.
require-mschap-v2
# Require MPPE 128-bit encryption
```


Сондай-ақ, біз proхуарр опциясы қосылғанын тексереміз (тиісті жолда түсініктеме берілген(комментарий)) және қосымша бір пайдаланушының бірнеше қосылыстарына рұқсат беру немесе тыйым салу үшін біз lock опциясына түсініктеме береміз (рұқсат) немесе түсініктеме береміз (тыйым салу).

```
proхуарр

# Normally pptpd passes the IP address to pppd, but if pptpd has been
# given the delegate option in pptpd.conf or the --delegate command line
# option, then pppd will use chap-secrets or radius to allocate the
# client IP address. The default local IP address used at the server
# end is often the same as the address of the server. To override this,
# specify the local IP address here.
# (you must not use this unless you have used the delegate option)
#10.8.0.100

# Debian: do not replace the default route
nodefaultroute

# Logging

# Enable connection debugging facilities.
# (see your syslog configuration for where pppd sends to)
#debug
```

```
# Miscellaneous

# Create a UUCP-style lock file for the pseudo-tty to ensure exclusive
# access.
lock

# Disable BSD-Compress compression
nobsdcomp

# Disable Van Jacobson compression
# (needed on some networks with Windows 9x/ME/XP clients, see posting to
# poptop-server on 14th April 2005 by Pawel Pokrywka and followups,
# http://marc.theaimsgroup.com/?t=111343175400006&r=1&w=2 )
novj
novjccomp

# turn off logging to stderr, since this may be redirected to pptpd,
# which may trigger a loopback
nologfd

# put plugins here
# (putting them higher up may cause them to sent messages to the pty)
```

```
# client. See KB311218 in Microsoft's knowledge base for more information.
ms-dns 10.0.0.1
ms-dns 10.0.0.2
```

Сондай-ақ, файлды сақтаңыз және жабыңыз. Енді тек пайдаланушыларды құру қалды:

```
sudo nano /etc/ppp/chap-secrets
```

Әр VPN пайдаланушысына бір жол беріледі, онда оның аты, қашықтағы мекенжайы, паролі және жергілікті мекен-жайы дәйекті түрде көрсетіледі.

Егер пайдаланушының сыртқы статикалық IP болса және тек ол пайдаланылатын болса, қашықтағы мекенжайды көрсетуге болады, әйтпесе қосылымды дәл қабылдау үшін жұлдызшаны көрсеткен дұрыс. Егер сіз пайдаланушының виртуалды желіде бірдей IP мекенжайын бөлектегіңіз келсе, Жергілікті адресі көрсетуі керек. Мысалы:

```
# Secrets for authentication using CHAP
# client      server  secret          IP addresses
user1 * password1 *
user2 11.22.33.44 password2 *
user3 * password3 10.10.10.10
```

User1 пайдаланушысы үшін Қосылымдар кез-келген сыртқы мекен-жайдан алынады, бірінші қол жетімді жергілікті болады. User2 үшін бірінші қол жетімді жергілікті мекен-жай таңдалады, бірақ қосылымдар тек 11.22.33.44 мекен-жайынан қабылданады. User3 үшін Қосылымдар кез-келген жерден қабылданады, бірақ жергілікті мекен-жай әрқашан біз ол үшін сақтаған 10.10.10.10-ға бөлінеді.

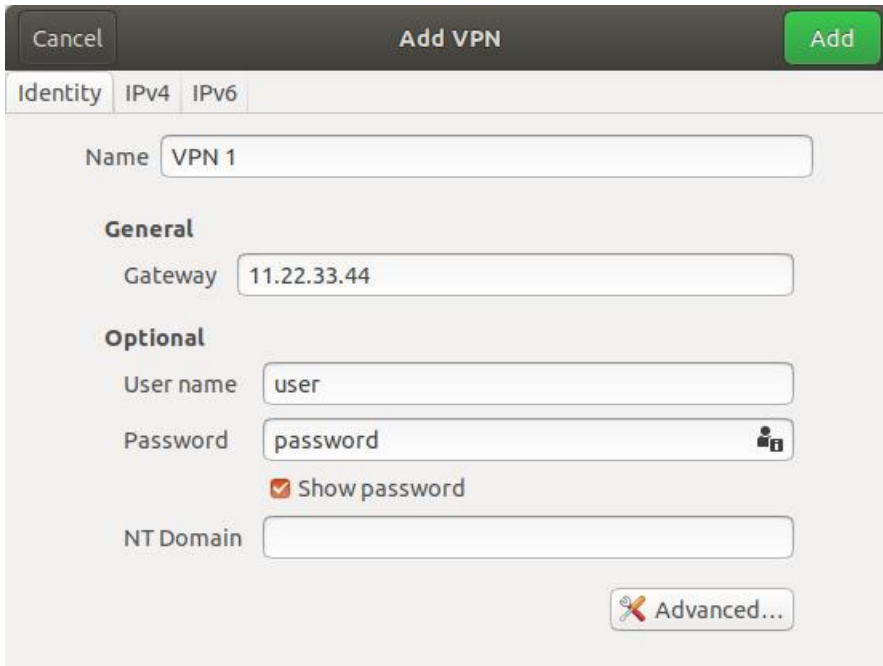
Осымен VPN серверін орнату аяқталды, оны қайта іске қосыңыз(перезапуск) (Linux астында компьютерді қайта іске қосудың қажеті жоқ):

VPN клиенттерді баптау.

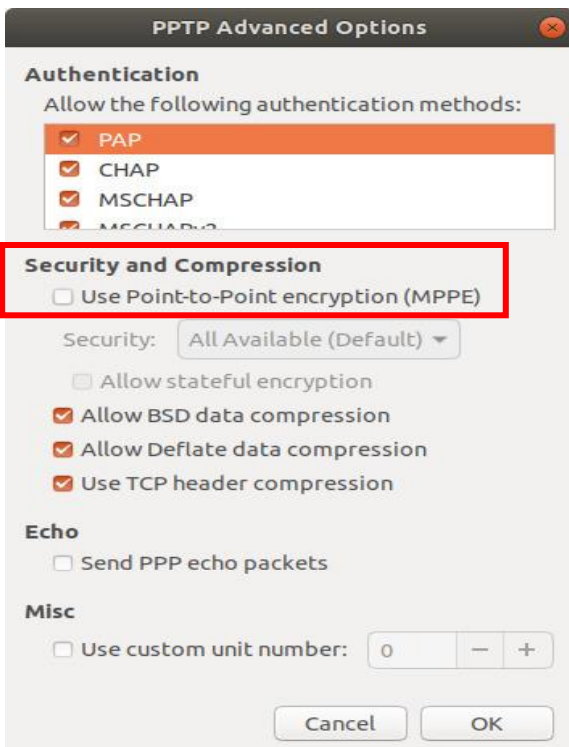
Клиент бөлігін кез-келген амалдық жүйеде орнатуға болады, мен Ubuntu Linux 18.04-ті мысал ретінде қолданамын.

Клиенттік компьютерде желілік қосылыстарды ашыңыз. "Қосу" түймесін басып, PPTP қосылымын таңдаңыз:

VPN қосылымының атауын стандартты етіп қалдыруға болады немесе сіз үшін ыңғайлы және түсінікті көрсете аласыз – бұл талғамға байланысты. Біз қосылатын сервердің сыртқы IP мекенжайын" шлюз " өрісіне енгіземіз ("тыңдау" опциясында конфигурацияланған кезде көрсетілген), төменде аты мен пароль. Оң жақта "Пароль" өрісінде алдымен "осы пайдаланушы үшін құпия сөзді Сақтау" опциясын таңдау керек»):

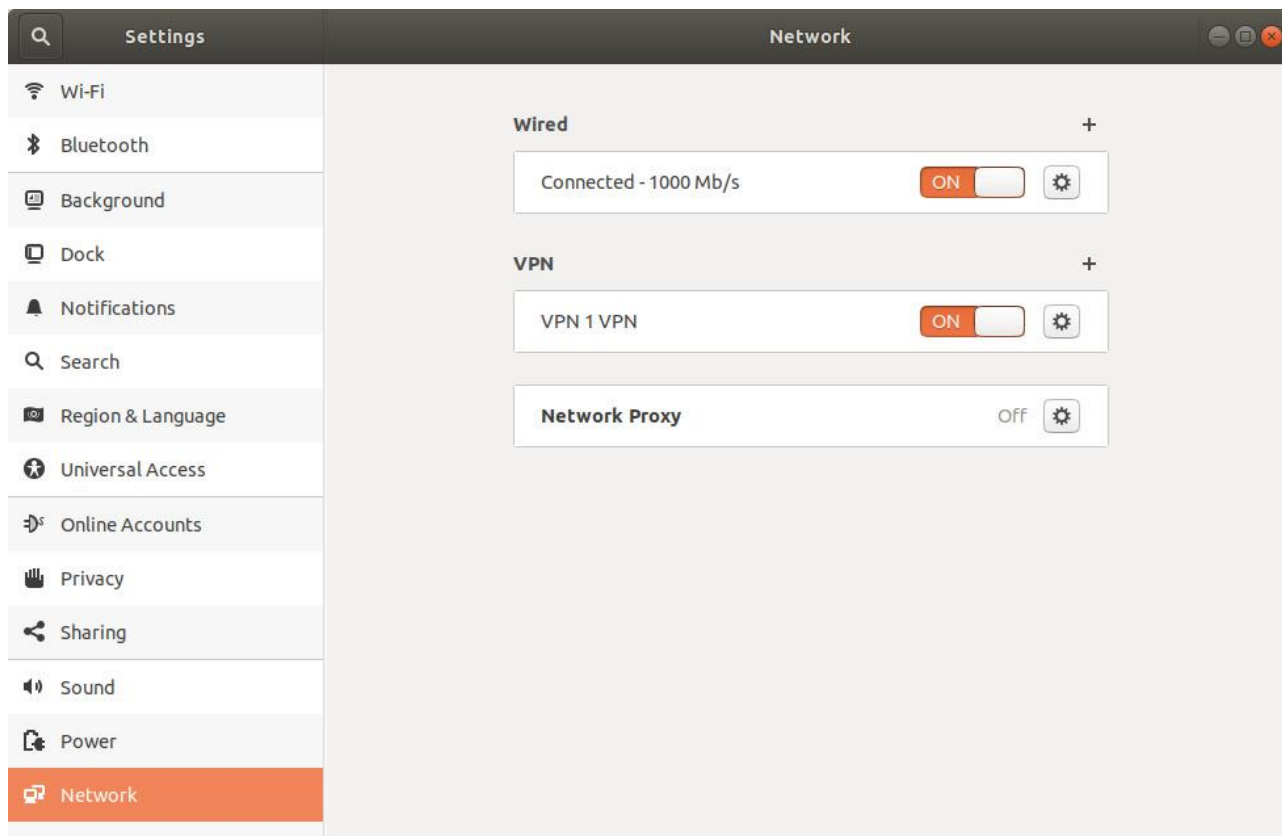


Әрі қарай, "қосымша" түймесін басып, "MPPE шифрлауын пайдалану" опциясын белгілеңіз, әйтпесе сервер сіздің қосылымыңызды қабылдамайды:



Осыдан кейін біз терезелерді жауып, серверге қосыламыз. Егер сервер сіздің жергілікті желіңізден тыс болса, интернетке кіру қажет.

Осымен виртуалды желіні ұйымдастыруды аяқтаймыз, бірақ ол тек компьютерлерді жергілікті желіге қосады. Интернетке желі сервері арқылы кіру үшін тағы бір параметр жасау керек.



VPN арқылы Интернетке кіруді баптау

VPN серверінде келесі командаларды енгізіңіз: iptables -t nat -A POSTROUTING -o eth0 -s 10.10.10.1/24 -j MASQUERADE

```
iptables -A FORWARD -s 10.10.10.1/24 -j ACCEPT
```

```
iptables -A FORWARD -d 10.10.10.1/24 -j ACCEPT
```

```
assem@assem-VirtualBox:~$ sudo su
root@assem-VirtualBox:/home/assem# sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@assem-VirtualBox:/home/assem# iptables -t nat -A POSTROUTING -o eth0 -s 10.10.10.1/24 -j MASQUERADE
root@assem-VirtualBox:/home/assem# iptables -A FORWARD -s 10.10.10.1/24 -j ACCEPT
root@assem-VirtualBox:/home/assem# iptables -A FORWARD -d 10.10.10.1/24 -j ACCEPT
root@assem-VirtualBox:/home/assem#
```

мұнда 10.10.10.1/24 – сервердің жергілікті мекен-жайы және желі маскасы.

Осыдан кейін біз өзгерістерді серверді қайта жүктегеннен кейін де жұмыс істейтін етіп сақтаймыз:

```
root@assem-VirtualBox:/home/assem# iptables-save
# Generated by iptables-save v1.6.1 on Wed Dec  9 17:07:06 2020
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
COMMIT
# Completed on Wed Dec  9 17:07:06 2020
# Generated by iptables-save v1.6.1 on Wed Dec  9 17:07:06 2020
*filter
```

Барлық өзгерістерді қолданамыз:

```
-A ufw-user-limit-accept -j ACCEPT
COMMIT
# Completed on Wed Dec  9 17:07:06 2020
root@assem-VirtualBox:/home/assem# iptables-apply
```

Осыдан кейін сіз интернетке кіре аласыз. Егер сіз өзіңіздің IP-мекенжайыңызды көрсететін сайтқа кірсеңіз, сіз өзіңіздің емес, сыртқы сервер мекенжайын көресіз (егер олар сәйкес келмесе).

L2TP сервері ыңғайлы, себебі ол қосылу үшін кірістірілген Windows құралдарын пайдалануға мүмкіндік береді. Бұл нұсқаулықта біз оны Ubuntu 16.04 және 18.04-те орнату және конфигурациялау процесін қарастырамыз. Нәтижесінде **біз мынандай нәтиже аламыз:**

**L2TP туннель протоколын қолданатын VPN сервері.*

**Ортақ кілт + пайдаланушының аутентификациясы арқылы қосылымды қорғауды .*

**Жергілікті желіге кіру.*

Біз келесі параметрлерді орындаймыз:

IPSEC

L2TP

PPP

Интернетке және жергілікті желіге кіру

Ақаулық диагностикасы

IPSEC орнату

IPSec басқару үшін strongswan пакеті қолданылады-оны мына пәрменмен орнатып аламыз: `sudo apt-get install strongswan`

```
assem@assem-VirtualBox:~$ sudo su
[sudo] password for assem:
root@assem-VirtualBox:/home/assem# apt-get install strongswan
Reading package lists... Done
Building dependency tree
Reading state information... Done
strongswan is already the newest version (5.6.2-1ubuntu2.5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@assem-VirtualBox:/home/assem#
```

Ipsec орнату үшін конфигурация файлын ашамыз:

Configsetup үшін қосамыз:

```
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    # strictcrlpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#    leftsubnet=10.1.0.0/16
#    leftcert=selfCert.der
#    leftsendcert=never
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightcert=peerCert.der
#    auto=start

#conn sample-with-ca-cert
#    leftsubnet=10.1.0.0/16
#    leftcert=myCert.pem
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightid="C=CH, O=Linux strongSwan CN=peer name"
#    auto=start

config setup
charondebug="all"
uniqueids=yes
"/etc/ipsec.conf" 50L, 985C
```

```

config                                     setup
virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12
    protostack=netkey
virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12
protostack=netkey
"/etc/ipsec.conf" 53L, 1100C written

```

* `virtual_private` біз үшін ең маңызды параметр болып табылады және жеке желілерді анықтайды. Бұл мысалда жергілікті желілер үшін сақталған желілер жай тізімделген-біз басқаларды көрсете аламыз.

... сондай-ақ төменде қоямыз:

```

conn l2tpvpn
    type=transport
    authby=secret
    pfs=no
    rekey=no
    keyingtries=2
    left=%any
    leftprotoport=udp/l2tp
    leftid=@l2tpvpnsrver
    right=%any
    rightprotoport=udp/%any
    auto=add

```

```

conn                                     l2tpvpn
                                         type=transport
                                         authby=secret
                                         pfs=no
                                         rekey=no
                                         keyingtries=2
                                         left=%any
    leftprotoport=udp/l2tp
    leftid=@l2tpvpnsrver
                                         right=%any
                                         rightprotoport=udp/%any
    auto=add

```

* `type` — қосылым түрі.

* `authby` — екі түйінді аутентификациялау әдістері.

* PFS-Perfect Forward Secrecy дегенді білдіреді. Қосылым кілттері арнасында тамаша құпиялылықты іске қосуға мүмкіндік береді.

- * Rekey — бұл байланыс аяқталған кезде қайта тексереді.
- * keyingtries-қосылу немесе оны ауыстыру туралы "келісу" әрекеттерінің саны.
- *left- сол жақ қатысушының (сервердің) IP мекенжайы.
- * leftport әдісі-сол жақ (сервер) жұмыс істейтін хаттама мен портты анықтайды.
- * leftid — қосылыстың сол жақ қатысушысының идентификациясы.
- * right — оң жақ қатысушының (клиенттің) IP мекенжайы.
- * rightport жолы-оң жақ (клиент) жұмыс істейтін хаттама мен портты анықтайды. Бұл жерде UDP және кез-келген порт көрсетілген.
- *auto функциясы-IPsec іске қосылған кезде автоматты түрде іске қосылатын операция.

Құпия кілт жасаймыз->ол үшін vi /etc/ipsec.secrets файлды өңдеу үшін ашыңыз:

```
%any %any : PSK "my_key_password"
```

қосыңыз

-бұл мысалда біз кез-келген IP-ге қосылу үшін **my_key_password** ортақ паролін орнатамыз.

Strongswan іске қосуға (автозапуск) және қызметті қайта бастауға (перезапуск) рұқсат етіңіз:

```
systemctl enable strongswan
```

```
systemctl restart strongswan
```

```
root@assem-VirtualBox:/home/assem# systemctl enable strongswan
root@assem-VirtualBox:/home/assem# systemctl restart strongswan
root@assem-VirtualBox:/home/assem#
```

L2TP

L2TP серверін орнатыңыз:

```
apt-get install xl2tpd
```

Сервер параметрлері файлын ашыңыз:

```
vi /etc/xl2tpd/xl2tpd.conf
```

ЖӘНЕ ҚОСАМЫЗ

```
root@assem-VirtualBox:/home/assem# apt-get install xl2tpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
 xl2tpd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 70,6 kB of archives.
After this operation, 224 kB of additional disk space will be used.
Get:1 http://kz.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 xl2tpd amd64 1.3.10-1ubuntu1 [70,6 kB]
Fetched 70,6 kB in 7s (10,1 kB/s)
Selecting previously unselected package xl2tpd.
(Reading database ... 168546 files and directories currently installed.)
Preparing to unpack .../xl2tpd_1.3.10-1ubuntu1_amd64.deb ...
Unpacking xl2tpd (1.3.10-1ubuntu1) ...
Setting up xl2tpd (1.3.10-1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.43) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
root@assem-VirtualBox:/home/assem#
```

```
;
; [lac cisco] ; Another quick LAC
; lns = cisco.marko.net ; * Required, but can take from default

[global]
port = 1701
access control = no
ipsecsaref = yes
force userspace = yes
auth file = /etc/ppp/chap-secrets

[lns default]
ip range = 176.16.10.10-176.16.10.200
local ip = 176.16.10.1
name = l2tpserver
pppoptfile = /etc/ppp/options.xl2tpd
flow bit = yes
exclusive = no
hidden bit = no
length bit = yes
require authentication = yes
require chap = yes
refuse pap = yes
] require authentication = yes
```

```
[global]
port = 1701
access control = no
ipsecsaref = yes
force userspace = yes
auth file = /etc/ppp/chap-secrets

[lns default]
ip range = 176.16.10.10-176.16.10.200
local ip = 176.16.10.1
name = l2tpserver
pppoptfile = /etc/ppp/options.xl2tpd
flow bit = yes
exclusive = no
hidden bit = no
```


length	bit	=		yes
require	authentication		=	yes
require	chap	=		yes
refuse pap	= yes			

Бұл жерде:

*port — VPN жұмыс істейтін UDP порты. 1701 ж.

*accesscontrol — клиенттердің параметрлерінде көрсетілген белгілі бір IP бар клиенттерден ғана сұрауларды қабылдау немесе қабылдамау.

*ipsecsaref-бірдей IP мекенжайлары бар бірнеше клиенттерді бақылауға мүмкіндік беретін ipsecSecurityAssociation пайдалану немесе керегі жоқ екенін көрсетеді.

* forceuserspace-L2TP пакеттерін декапсуляциялау арқылы өнімділікті арттырады.

* authfile — аутентификация файлының жолы.

*iprange — қосылған Клиенттерге тағайындалған мекенжайлар ауқымы.

*localip — VPN желісіндегі сервердің IP мекенжайы.

*name — келісу процесі үшін Сервер атауы.

*pprportfile — rppd параметрі бар файл жолы.

*flowbit — пакеттерге реттік нөмірлер қосуға мүмкіндік береді.

*exclusive-егер сіз yes-ке қойсаңыз, сервер клиентпен бір ғана байланыс орнатуға мүмкіндік береді.

* hiddenbit-AVP жасыру немесе жоқ.

*lengthbit-жүктемені көрсететін ұзындық битін пайдалану.

*requireauthentication — аутентификацияны талап ету.

*requirechap-CHAP протоколы бойынша PPP аутентификациясын талап ету.

*refusepap -PAP протоколы бойынша PPP аутентификациясын талап ету.

vpn-серверге іске қосуға (автозапуск)және қызметті қайта бастауға(перезапуск) рұқсат етіңіз және қайта қосамыз:

```
systemctl enable xl2tpd
```

```
systemctl restart xl2tpd
```

```
root@a  
File Edit View Search Terminal Help  
root@assem-VirtualBox:/home/assem# systemctl restart xl2tpd
```

PPP

Конфигурациялық файлды өңдеу үшін ашыңыз:

```
vi /etc/ppp/options.xl2tpd
```

және қосамыз:

```
noccp  
auth  
crtstcs  
mtu 1410  
mru 1410  
nodefaultroute  
lock  
noproxyarp  
silent  
modem  
asynsmar 0  
hide-password  
require-mschap-v2  
ms-dns 77.88.8.8  
ms-dns 8.8.8.8
```

```
noccp  
auth  
crtstcs  
mtu 1410  
mru 1410  
nodefaultroute  
lock  
noproxyarp  
silent  
modem  
asynsmar 0  
hide-password  
require-mschap-v2  
ms-dns 77.88.8.8  
ms-dns 8.8.8.8
```

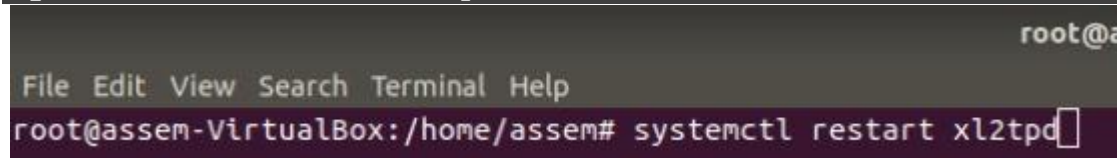
Пайдаланушыны жасаймыз. Ол үшін файлды ашыңыз: `vi /etc/ppp/chap-secrets`

Және қосамыз

```
"user1"      l2tpserver      "password1"      "172.16.10.10"  
"user2" l2tpserver "password2" *
```

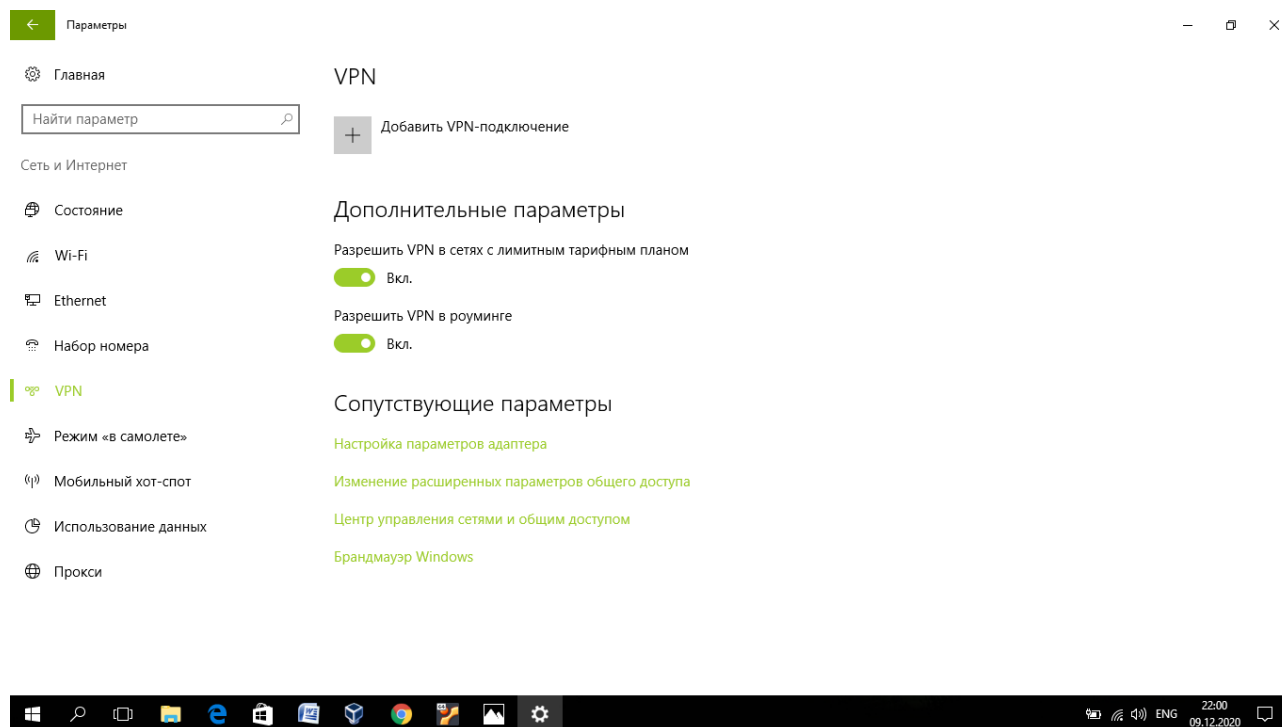
Xl2tpd қайта іске қосыңыз:

```
systemctl restart xl2tpd
```



Клиентті баптау

Vpn бөліміндегі желі және Интернет параметрлерінде біз жаңа байланыс жасаймыз:



*Қосылым атауы — ерікті атау.

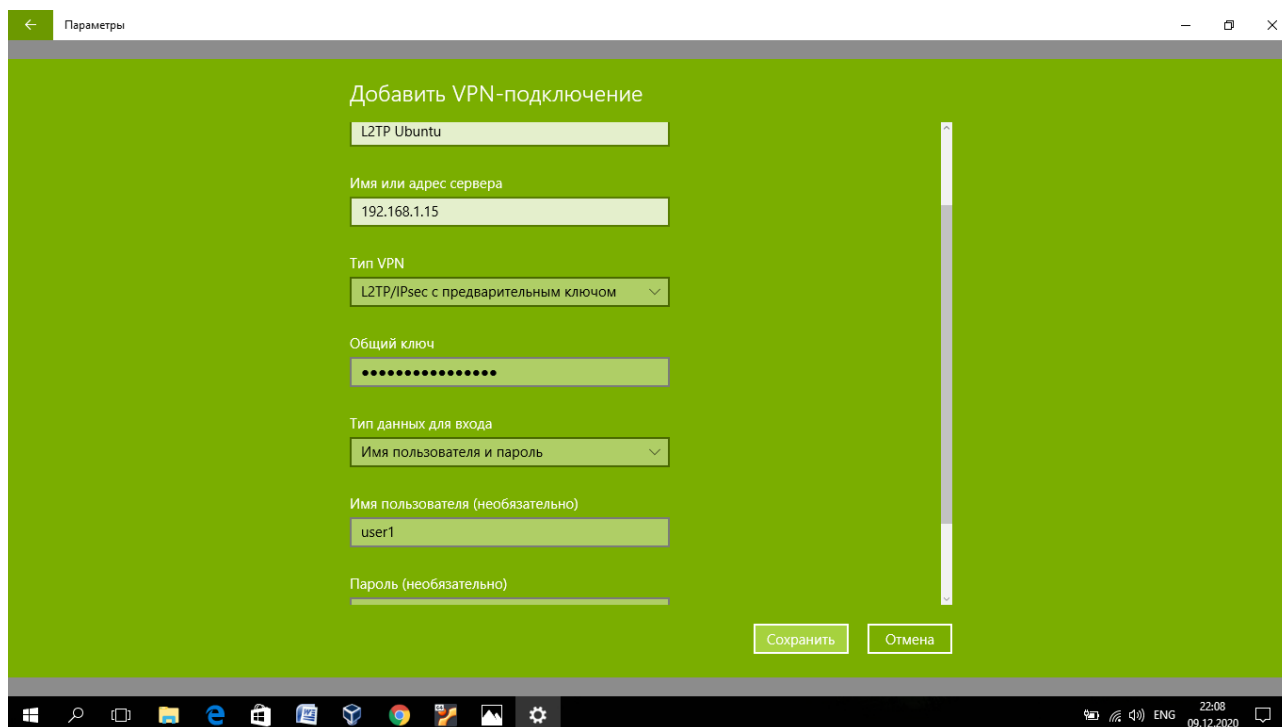
*Сервер атауы немесе мекен — жайы-біз қосылатын VPN серверінің мекен-жайы.

*Vpn түрі-біздің жағдайымыз үшін алдын-ала кілтпен L2TP/IPsec таңдаңыз.

*Жалпы кілт-біз /etc/ipsec.secrets файлында орнатқан кілт.

*Кіру деректерінің түрі-пайдаланушы мен парольді таңдаңыз.

*Пайдаланушы аты мен пароль-біз /etc/ppp/char-secrets файлында орнатқан логин мен пароль.



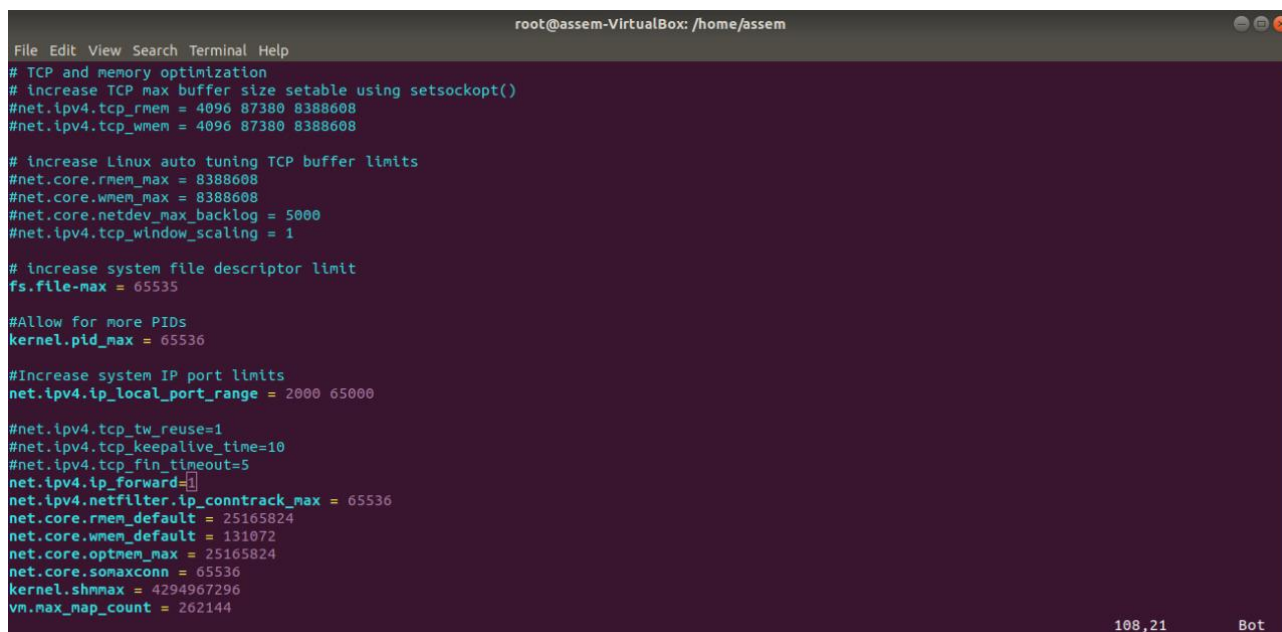
Интернетке және жергілікті желіге кіру

VPN желісіне қосылғаннан кейін біз интернетке кіре алмаймыз немесе жергілікті желі түйіндеріне қосыла алмаймыз. Мұны түзету үшін файлды өңдеу үшін ашыңыз:

```
vi /etc/sysctl.d/99-sysctl.conf
```

```
net.ipv4.ip_forward=1
```

осы қатарды қосамыз



* Біз желілік сұраулардың алға жылжуына рұқсат бердік және серверді шлюз ретінде орнаттық.

Орнатуды қолданғаннан кейін:

```
sysctl -p /etc/sysctl.d/99-sysctl.conf

root@assem-VirtualBox: /home/assem

File Edit View Search Terminal Help

root@assem-VirtualBox:/home/assem# sysctl -p /etc/sysctl.d/99-sysctl.conf
net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_synack_retries = 2
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv6.conf.default.router_solicitations = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.default.dad_transmits = 0
net.ipv6.conf.default.max_addresses = 1
sysctl: cannot stat /proc/sys/kernel/exec-shield: No such file or directory
kernel.randomize_va_space = 1
fs.file-max = 65535
kernel.pid_max = 65536
```

Iptables-ке ереже қосыңыз:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

* бұл ереже eth0 интерфейсінде маскарадингті қамтиды. Желілік адаптердің мәнін командаға ауыстыру керек.

Бірыңғай желілік интерфейс жағдайында басқа ештеңе жасаудың қажеті жоқ- Ubuntu Интернет шлюзі ретінде жұмыс істей бастайды.

Бірнеше желілік адаптерлер жағдайында желілік экранды баптаймыз:

```
iptables -A FORWARD -i eth1 -o eth0 -m state --
stateRELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

root@assem-VirtualBox:/home/assem# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
root@assem-VirtualBox:/home/assem#
```

* eth1 ішкі желі үшін, ал eth0 сыртқы желі үшін қолданылады деп болжанады.

Мәселелерді (проблемаларды) диагностикалау

Жоғарыда сипатталған параметр логтың болуын білдірмейді. Ол үшін PPP үшін конфигурация файлы ашыңыз:

```
vi /etc/ppp/options.xl2tpd
```

```
noccp
auth
crtstcts
mtu 1410
mru 1410
nodefaultroute
lock
noproxyarp
silent
modem
asynsmar 0
hide-password
require-mschap-v2
ms-dns 77.88.8.8
ms-dns 8.8.8.8
logfile /var/log/xl2tpd/xl2tpd.log
debug
```

```
logfile /var/log/xl2tpd/xl2tpd.log
debug
```

Журнал үшін каталог жасаңыз:

```
mkdir /var/log/xl2tpd
```

```
root@assem-VirtualBox:/home/assem# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
root@assem-VirtualBox:/home/assem# vi /etc/ppp/options.xl2tpd
root@assem-VirtualBox:/home/assem# mkdir /var/log/xl2tpd
root@assem-VirtualBox:/home/assem#
```

Xl2tpd қызметін қайта іске қосыңыз:

```
root@a
File Edit View Search Terminal Help
root@assem-VirtualBox:/home/assem# systemctl restart xl2tpd
```

Біз серверге қосылуға тырысамыз-проблемалар туындаған жағдайда журналды қадағалаймыз:

```
root@assem-VirtualBox:/home/asse
File Edit View Search Terminal Help
root@assem-VirtualBox:/home/assem# tail -f /var/log/xl2tpd/xl2tpd.log
```

Алдымен NetworkManager көмегімен VPN орнатыңыз. Сіз орнатқан VPN желілерінің көпшілігі PPTP протоколын пайдаланады. PPTP 1723 TCP порты арқылы жұмыс істейді. Егер сіз жергілікті машинаның шығысындағы немесе жергілікті желінің брандмауэріндегі порттарды бұғаттасаңыз, сізге осы портты ашу қажет болады. Егер сіз бәрін жауып тастаған қауіпсіздіктің жанкүйері болмасаңыз, көп жағдайда 1723 порты ашық болады. Енді хабарландыру аймағында NetworkManager белгішесін табыңыз (сізде ол басқаша көрінуі мүмкін). Оның көмегімен біз желі параметрлерін реттеп, VPN қосылымдарын іске қосамыз.

VPN қосылымдарын құруды бастау үшін PPTP модулін орнатайық. Және білесіз бе? Ол үшін командалық жолдың (CLI) Интер-фейсін пайдаланудың қажеті жоқ. PPTP "қосымшаларды орнату/жою" арқылы қол жетімді. Бұл CLI-ді ұнатпайтындар үшін орнатуды жеңілдетеді. Қосу→Орнату/Жою ... түймесін басып, іздеу жолағына "VPN" енгізіңіз. Егер сіз кему ретімен танымалдылық бойынша сұрыптасаңыз, біздің модуль ең жоғарғы жағында болады. Белгі қоямыз, түрлі өзгерістер енгіземіз пароль және "Жабу" түймесін басамыз. Барлығы өте қарапайым. CLI әуесқойлары үшін: қажетті пакеттерді орнату үшін келесі пәрменді енгізіңіз:

```
sudo aptitude install network-manager-pptp
```

Енді NETWORKMANAGER үшін PPTP модулі орнатылып, байланыс орнатайық. Хабарлама аймағындағы NetworkManager белгішесін тінтуірдің оң жақ түймесімен нұқыңыз, контекстік мәзір пайда болады. Мәтінмәндік мәзірде "соединенияны өзгерту..." түймесін басыңыз, белгішені сол жақ батырмамен нұқып, vpn қосылымдарын таңдаңыз→vpn теңшеу(баптау)...

"Желілік қосылымдар" терезесінде "VPN" қойындысын басу керек.

Содан кейін "Қосу" (қосу), содан кейін "жасау..." (Жасау) түймесін басыңыз.

Қосылым атауын өңдеңіз. Сіз кез-келген атауды орната аласыз, бірақ егер сіз бірнеше қосылымды құруды жоспарласаңыз немесе алты айдан кейін орнатқаныңызды есте сақтағаныңызға сенімді болмасаңыз, онда қосылымды сіз қосылған жердің атымен атаған дұрыс.

"Шлюз" (Gateway) өрісіне шлюздің IP мекенжайын немесе FQDN (толық домен атауы) енгізіңіз. Жеке өзім IP мекенжайын енгіземін. Содан кейін "пайдаланушы аты" өрісін толтырыңыз. Әдетте мен парольді енгізбеймін-менің ойымша, бұл жақсы әдет. Егер сіз парольді енгізгіңіз келсе, онда бұл өз қолыңызда. Шифрлауды орнату және қосылу үшін "mpre шифрлауын

пайдалану" (UsePoint-to — PointEncryption (MPPE)) құсбелгісін қою үшін "қосымша..." бөліміне кіру қажет болуы мүмкін. Көптеген VPN желілері шифрланған қосылымды қажет етеді. "ОК"түймесін басыңыз.

"IPv4 параметрлері" (IPv4 settings) қойындысы — өнімді пайдаланушылар үшін.
* Мұнда VPN желісі үшін DNS серверлерін өзгертуге, ішкі желіге негізделген әртүрлі желілік маршруттарды орнатуға және статикалық IP мекенжайын тағайындауға болады.