

# Erhvervsakademi Midtjylland

---

Lillelundvej 29 ▪ DK-7400 Herning

Telefon +45 97 12 52 00

**Titel:** Netværk  
**Tema:** VPN-Server  
**Projektperiode:** uge 40 - 43 2003

## IT projekt-

## ITE 3. Semester

## -Virtual Private Network

**Vejleder:** Benny Dyhr Thomsen

**Side antal:** 25 sider

**Afsluttet:** 23 Oktober 2003

**Udarbejdet af:** Kenneth Dalbjerg & Ole Brix Rosengreen

## Forord

Som udgangspunkt i vores projekt, går vi ud fra at brugeren har en Debian-box og de dertil krævede ressourcer. Derudover bør man have en basal viden omkring navigering og brug af Linux, fordi det følgende materiale ellers kan virke lidt komplekst.

Ellers er den følgende dokumentation udformet som en guide, hvor at de aspekter vi mener kræver en forklaring, har fået det.

---

Kenneth Dalbjerg

---

Ole B. Rosengreen

## Formål

Formålet med dette projekt er først og fremmest at skabe et bedre kendskab til teorien omkring VPN, samtidig med at det udføres i praksis.

Hvis det er muligt at skabe en sikker forbindelse som skolen/systemadministratoren godkender, vil det muligvis blive anvendt på skolens server.

Derved kan vi elever få adgang til skolens netværk hjemmefra uden sikkerhedskravene bliver brudt. På den måde kan man oprette et fælles lagringsmedie, hvor det er muligt at dele opgaver, notater osv.

## Indholdsfortegnelse

<b>FORORD</b> .....	<b>2</b>
<b>FORMÅL</b> .....	<b>2</b>
<b>PROJEKTBEKRIVELSE</b> .....	<b>4</b>
<b>INDLEDNING</b> .....	<b>5</b>
<b>1. OPSÆTNING AF VPN-SERVER</b> .....	<b>6</b>
1.1 OPSÆTNING AF NETVÆRK INTERFACES:.....	6
1.2 INSTALLATION AF NØDVENDIGE PAKKER.....	7
1.3 DOWNLOADING AF KERNEN OG PATCHES .....	8
1.4 KOMPILERING/PATCHING AF KERNEN.....	8
1.5 KOMPILERING/PATCHING AF PPP .....	10
1.6 OPSÆTNING AF PPP .....	11
1.7 KOMPILERING AF POPTOP.....	13
1.8 OPSÆTNING AF POPTOP .....	13
<b>2. OPSÆTNING AF MASQUERADING-SCRIPT</b> .....	<b>15</b>
<b>3. OPSÆTNING AF WINDOWS XP PRO KLIENT</b> .....	<b>16</b>
<b>KONKLUSION</b> .....	<b>24</b>
<b>KILDER</b> .....	<b>25</b>
INSTALLERING AF POPTOP.....	25
KONFIGURATION AF POPTOP.....	25
BLANDEDE LINKS.....	25

## Projektbeskrivelse

### **Opsætning af VPN Server/klient:**

Vi vil i de følgende uger arbejde med opsætning af en VPN server i Linux. Til løsning af opgaven vil vi bruge programmet Poptop [www.poptop.org/](http://www.poptop.org/), som er et gratis open-source projekt.

Derudover skal der opstilles 1 klient: *1 stk. Windows XP.*

### Krav til VPN'en:

Få adgang til et lukket netværk.

Se mapper og printere som er delt på netværket.

## Indledning

Kort sagt er VPN en sikker forbindelse mellem to, ellers ”usikre” netværk. VPN, der står for Virtual Private Network, findes efterhånden i mange afskygninger og kan anvendes af de fleste platforme. Vi har valgt at bruge Debian platformen, der er en af Linux’s mange distributioner. Et af kodeordene ved opsætning af VPN er kryptering, da det jo gerne skal være en sikker linie man opretter.

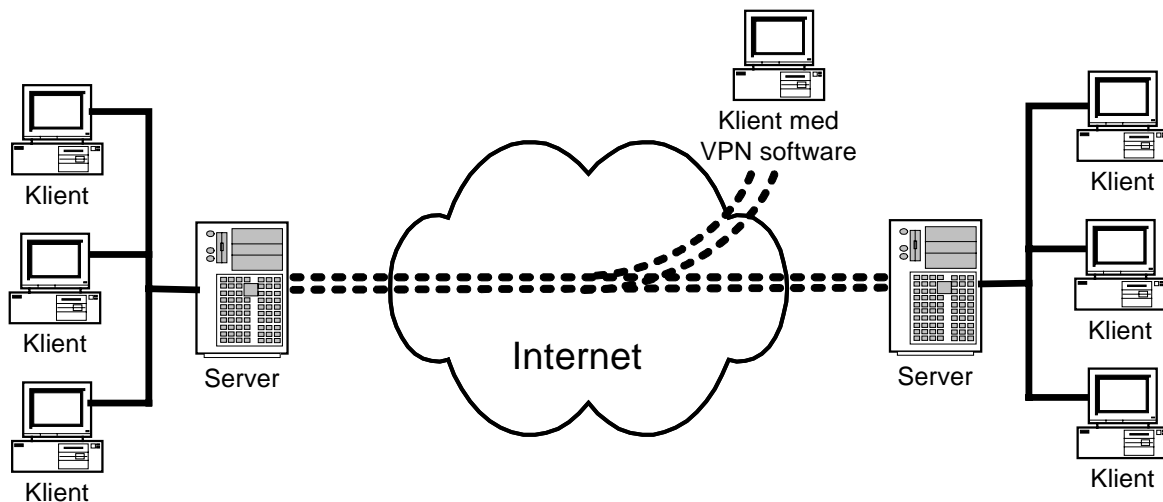
Der findes flere forskellige typer af kryptering bl.a. IPsec, PGP og MPPE.

Den sidst nævnte krypteringsprotokol, MPPE, anvendes af Poptop og findes i tre forskellige udgaver, nemlig 40 bit, 56 bit og 128 bits kryptering. Hvilken af krypterings mulighederne man anvender, kommer an på hvor sikker man vil have sin VPN-tunnel. Vi har selvfølgelig brugt 128 bits kryptering.

MPPE (Microsoft Point-To-Point Encryption Protocol) bruger RSA RC4 algoritmen til at kryptere med og er i Debian et samlet modul der skal kompileres sammen med kernen, men det vender vi tilbage til senere. MPPE er dog inkluderet i alle Windows-udgaverne.

For at transportere pakker gennem netværket bruges PPP-protokollen. PPP (rfc1661) er en Internet standard for at overfører IP pakker over en seriel linie, PPP står for Point to Point Protocol. Og da vi laver en Point-to-Point-Tunneling Protocol, altså punkt til punkt tunnel forbindelse, fra Klient til Serveren gør vi brug af PPP.

For at brugeren skal kunne logge ind på VPN-serveren kræver det en login-protokol. Som f.eks. PAP eller MS CHAP. Poptop understøtter kun MS CHAP , men den findes i to versioner, nemlig version 1 og version 2. Vi anvender selvfølgelig MS CHAP V2 [[RFC2759](#)], da den indeholder lidt flere features, som f.eks. mulighed for at brugeren selv kan skifte password når serveren meddeler at det er udløbet. Denne feature understøttes mærkeligt nok ikke af Poptop, men der er nok andre ting der understøttes i stedet, det har vi bare ikke haft tid til at undersøge.



Herover, et eksempel på opsætning af VPN over Internettet, hvor man kan se den sikre forbindelse mellem to ellers adskilte net. Men det er også muligt for den enkelte bruger/klient at skabe sig adgang til det afskærmede net via VPN tunnelen.

## Opsætning af VPN-server

Vi har som sagt valgt at bruge den frie software Poptop til Linux, men der findes også andre udgaver så som FreeS/WAN, Ipsse osv. Som klient har vi valgt en Windows XP som udgangspunkt, men Poptop understøtter også Windows 95/98/Me/NT/2000 og naturligvis Linux.

Vi har i vores server monteret to netværkskort bl.a. for at øge sikkerheden, men også for at gøre det hele lidt mere overskueligt. Det ene kort bruges til den eksterne IP og det andet kort bruges til IP'en på det interne net.

Det er dog også muligt at have 2 IP'er på samme kort, men nu havde vi lige muligheden for at isætte et ekstra, plus at vi gerne vil have sikkerheden så høj som muligt.

### **Opsætning af Netværk interfaces:**

Vi har som før nævnt 2 netkort i vores maskine. Den eksterne side er det "ikke sikre" netværk, og den interne er det "sikre" netværk.

På den eksterne side har vi **192.168.1.0/24** net og på den interne side har vi **192.168.2.0/24** net, og det er henholdsvis **eth0** på den eksterne og **eth1** på den interne.

I Debian sætter man netværket op i **/etc/network/interfaces**, vi bruger en editor som hedder **nano** til at redigere med. Så derfor skriver vi

```
host:~# nano /etc/network/interfaces
```

Så kommer vi ind i opsætning af netværk enheder, toppen af filen se således ud

```
# /etc/network/interfaces -- configuration file for ifup(8), ifdown(8)

# The loopback interface
auto lo
iface lo inet loopback

# The first network card - this entry was created during the Debian installation
```

Vi har så slettet alt efter "# The first network card - this entry was created during the Debian installation" og sat dette ind:

```
auto eth0
iface eth0 inet static
    address 192.168.1.38
    broadcast 192.168.1.255
    netmask 255.255.255.0
    network 192.168.1.0
    gateway 192.168.1.1

auto eth1
iface eth1 inet static
```

```
address 192.168.2.2
broadcast 192.168.2.255
netmask 255.255.255.0
network 192.168.2.0
```

Dette bevirker at enheden **eth0**, få ip'en **192.168.1.38** og **eth1** få ip'en **192.168.2.2**. Gatewayen får ip'en **192.168.1.1**, og det er den serveren bruger for at kunne for kontakt til Internettet med her på skolen.

Nå man har redigeret i **/etc/network/interface** skal netværket genstartes, og det gøres på denne måde:

```
host:~# /etc/init.d/networking restart
```

## ***Installation af nødvendige pakker***

Med en jomfru-Debian, altså en box der ikke er installeret noget på, kræver det at man henter nogle forskellige pakker for at kunne komme videre i installationen af Poptop.

<b>ssh</b> -	Til fjernstyring af Debian-boxen, f.eks. via Putty
<b>mc</b> -	(Midnight Commander) For fil redigering, giver et overskuelig overblik over mapper og filer på maskinen lokalt.
<b>wget</b> -	Bruges til at hente filer på Internettet.
<b>patch</b> -	For at kunne patche kernen og andre kildekoder.

For at kunne kompilere kernen, "The Debian Way" skal man bruge følgende:

<b>make</b> -	Bruges til at lave "menu config"
<b>gcc</b> -	GCC er GNU C compileren.
<b>libncurses5-dev</b>	Er nogle "free" udviklings biblioteker til "ncurses". Ncurses indeholder nogle forskellige opsætninger af tekst, grafik, farver osv.
<b>kernel-package</b>	Er en samling af scripts som gør det lettere at kompilere kernen i Linux.

For at hente pakkerne bruger man **apt-get**, som er en integreret del af Debians pakkesystem.

```
host:~# apt-get install ssh mc wget patch make gcc libncurses5-dev kernelpackage
```

Det skulle skabe grundlaget for at kunne komme fejlfrt gennem installationen, men vi skal ikke kunne udelukke at der vil blive brug for øvrige pakker.

## Downloading af kernen og patches

Man skal bruge et par kildekoder og patches for at kunne installere Poptop, med kryptering. Disse filer kan hentes direkte ned til serveren med **wget**, den bruges på denne måde

```
host:~# wget url
```

Følgende filer skal man have hentet og lagt ind i /usr/local/src.

```
host:~# cd /usr/local/src
host:/usr/local/src# wget http://samba.org/ftp/ppp/ppp-2.4.1.tar.gz
host:/usr/local/src# wget http://planetmirror.com/pub/mppe/ppp-2.4.1-openssl-0.9.6-mppe-patch.gz
host:/usr/local/src# wget http://planetmirror.com/pub/mppe/ppp-2.4.1-MSCHAPv2-fix.patch.gz
host:/usr/local/src# wget http://belnet.dl.sourceforge.net/sourceforge/poptop/pptpd-1.1.4-b4.tar.gz
```

Følgende filer skal man have hentet og lagt ind i /usr/src/.

```
host:~# cd /usr/src
host:~# wget http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.22.tar.bz2
host:~# wget http://planetmirror.com/pub/mppe/linux-2.4.16-openssl-0.9.6b-mppe.patch.gz
```

## Kompilering/patching af kernen

Vi starter med at pakke kernen ud, hvorefter vi laver et ”symlink” (en såkaldt genvej) til mappen ”linux” og det gøres på følgende måde:

```
host:~# tar jxvf linux-2.4.22.tar.gz
```

Så skal der laves et symlink som hedder /usr/src/linux der peger på /usr/src/linux-2.4.22/

```
host:~# ln -s /usr/src/linux-2.4.22 /usr/src/linux
```

Pak derefter **linux-2.4.16-openssl-0.9.6b-mppe.patch.gz** ud, dette gøres med:

```
host:~# gzip -d /usr/src/linux-2.4.16-openssl-0.9.6b-mppe.patch.gz
```

Herefter flyttes **linux-2.4.16-openssl-0.9.6b-mppe.patch** ind i /usr/src/linux og dette gøres med:

```
host:~# mv /usr/src/linux-2.4.16-openssl-0.9.6b-mppe.patch /usr/src/linux
```

Så! Nu skulle kernel-materialet være pakket ud og klar til anvendelse. Vi går ind i mappen /usr/src/linux.

```
host:~# cd /usr/src/linux
```



Herefter skal vi patche kernen, dette gøres med

```
host:~# patch -p1 < linux-2.4.16-openssl-0.9.6b-mppe.patch
```

Den spørger om den skal overskrive ”**drivers/net/Makefile.orig**” og det siger du 'y' til.

Nu skulle kernen være klar til at blive kompileret og det gøres med følgende kommando:

```
host:~# cd /usr/src/linux/  
host:~# make menuconfig
```

Herefter skal du vælge de moduler du skal bruge på dit system.

Du skal huske at tage ALT ppp ting med som MODULER (M), som er under Network device support.

Du skal også huske at tage iptables med hvis man skal bruge VPN tunnelen som gateway.

Når du har valgt de moduler du skal bruge og har afsluttet og gemt, skriver du:

```
host:~# make-kpkg --revision=mitimage.1.0 kernel_image
```

Dette kan godt tage et stykke tid, så hvis man skal på tonden er det et godt tidspunkt nu.

Efter den er færdig med at kompilere skal du installere kernen.

```
host:~# cd ..  
host:~# dpkg -i kernel-image-2.4.22_mitimage.1.0_i386.deb
```

Herefter genstarter du maskinen.

## **Kompilering/patching af PPP**

De før downloadede filer, som ligger i /usr/local/src skal nu bruges. Vi starter med at pakke selve PPP-kildekoden ud.

```
host:~# cd usr/local/src  
host:~# tar xzfv ppp-2.4.1.tar.gz
```

Herefter skal de to patches så pakkes ud.

```
host:~# gzip -d ppp-2.4.1-openssl-0.9.6-mppe-patch.gz  
host:~# gzip -d ppp-2.4.1-MSCHAPv2-fix.patch.gz
```

Og flyttes over i mappen ppp-2.4.1

```
host:~# mv ppp-2.4.1-openssl-0.9.6-mppe-patch ppp-2.4.1/  
host:~# mv ppp-2.4.1-MSCHAPv2-fix.patch ppp-2.4.1/
```

Skift til mappen ppp-2.4.1

```
host:~# cd ppp-2.4.1
```

Nu skulle kildekoden til PPP være klar til at blive patchet og det gøres sådan:

```
host:~# patch -p1 < ppp-2.4.1-openssl-0.9.6-mppe-patch  
host:~# patch -p1 < ppp-2.4.1-MSCHAPv2-fix.patch
```

Herefter skal PPP bare konfigureres.

```
host:~# ./configure  
host:~# make  
host:~# make install
```

## Opsætning af PPP

Det første man skal have redigeret i, er **/etc/ppp/options**

Der står en masse i denne fil, men dette sletter man. Dette letteste er at slette filen og så oprette den igen.

```
host:~# rm /etc/ppp/options
host:~# touch /etc/ppp/options
```

Herefter skal man så have åbnet filen i en editor, vi bruger igen **nano**.

```
host:~# nano /etc/ppp/options
```

Følgende har vi sat ind i filen.

```
debug
auth
+chapms-v2
require-chapms-v2
mppe-128
mppe-stateless
name server_name
proxyarp
```

debug, gør sådan at hver gang der sker noget med ppp logger den det til **/var/log/syslog**, dette kan godt bliver svært at holde styr på, da der i forvejen bliver logget en del i **/var/log/syslog**, derfor kan man ændre dette så det f.eks. bliver logget til **/var/log/pptpd.log** filen (Dog bliver det stadig logget i syslog).

For at gøre dette skal filen **/var/log/pptpd.log** oprettes

```
host:~# touch /var/log/pptpd.log
```

Herefter skal man have redigeret i **/etc/syslog.conf**, hvor man i bunden af denne skal have sat følgende ind:

```
daemon.debug /var/log/pptpd.log
```

Så skal vi have genstartet **syslogd**.

```
host:~# /etc/init.d/syslogd restart
```

Og så skulle den logge til ppp. (Dog skal du huske og genstarte PPP, men det gør vi længere nede i dette kapitel)

**auth**, betyder at der er godkendelse på forbindelsen, herefter skal man addere (+) eller subtrahere (-) de forskellige godkendelses protokoller. Vi har valgt at tage **chapms-v2** med, da det er den nyeste måde at logge ind på. Så der skal være et "+" ud for **chapms-v2**.

**require-chapms-v2**, gør det at serveren kræver at der bliver brugt **chapms-v2**, og man kan altså ikke koble sig på med noget andet.

Der er også nogen andre former for require & refuse og dette er **refuse-chap**, **refuse-mschap**, **require-mschap-v2**, **require-mppe**. Og disse henholdsvis kræver eller nægter de efterfølgende login metoder eller protokoller.

**mppe-128**, med denne krypteres dataene med 128 bit, mod **mppe-40**, hvor de så kun krypteres med 40 bit. Desto mere dataene krypteres jo svære er det at dekryptere dataene.

**mppe-stateless** er den måde pakkerne bliver sendt af sted, der findes 2 måder **stateless** & **stateful**, ppp 2.4.1 understøtter ikke **stateful**. Med **stateless** bliver begge sider synkroniseret ved log ind. Alle pakkerne får et unikt nummer, hvis så modtageren ser et hul, vil den spørge efter pakken. Dette kræver en del, da den hele tiden at skal synkronisere på overførelsen. Med **stateful**, laver den en synkronisering i starten, og hver pakke får også her et unikt nummer, men i **stateful** synkroniserer den ikke konstant, modtageren tjekker bare om der kommer et hul. Gør der det vil den smide alle de pakker den modtager herefter væk, og bede om at få den pakke engang mere. Derfor er det en fordel at bruge **stateless** til et transmissionsmedie, som kunne finde på at smide pakker væk tit, og **stateful** til et transmissionsmedie som ikke smider så mange pakker væk. **Stateless** bruges f.eks. også til trådløst LAN.

**proxyarp** gør således at man kan snakke med andre maskiner som står på det net, som serveren man kobler sig op til står på. Men man skal dog stadig have et masquading-script (eller firewall-script) kørende.

Efter man har sat sin ppp op kan man genstarte ppp med:

```
host:~# /etc/init.d/ppp restart
```

Hvis den brokker sig over at den ikke er startet, skriver man bare:

```
host:~# /etc/init.d/ppp start
```

Ønsker man så at stoppe ppp kan man skrive.

```
host:~# /etc/init.d/ppp stop
```

## Kompilering af Poptop

Kompileringen og udpakningen foregår næsten ligesom med PPP, men for en sikkerhedsskyld gennemgår vi den her alligevel.

Vi skifter til mappen /usr/local/src og pakker ud.

```
host:~# cd /usr/local/src
host:~# tar xzfv pptpd-1.1.4-b4.tar.gz
```

Herefter køres konfigurationen næsten ligesom med PPP.  
Vi skifter først til mappen poptop-1.1.4/

```
host:~# cd /usr/local/src/poptop-1.1.4/
host:~# ./configure --prefix=/usr/local/poptop
host:~# make
host:~# make install
```

Kommando nr. 2 “--prefix=/usr/local/poptop” gør at Poptop kommer til at ligge i mappen /usr/local/poptop.

Nu mangler vi bare den sidste opsætning af krypteringsmetoder og adgangskontrol.

## Opsætning af Poptop

Opsætningen af poptop er lige til at gå til, den eneste fil man skal ændre i er: /etc/pptpd.conf, men den skal lige oprettes først:

```
host:~# touch /etc/pptpd.conf
```

vores fil ser således ud:

```
debug
localip 192.168.2.1
remoteip 192.168.2.240-254
```

**debug** betyder at den logger mere end normalt, så man kan tjekke hvad det er som går galt, dette er godt i test fasen, men i produktion burde man nok slå dette fra, da ens log filer ellers hurtigt kunne blive fyldt op.

**localip** er den lokale IP på maskinen, denne må gerne være en enkel IP-adresse, men er der angivet flere skal der være en for hver klient som logger på.

**remoteip:** Dette er de IP-adresser som klienterne får når de kobler på, her skal der være en for hver bruger som kobler sig på.

For at starte poptop skal du skrive **/usr/local/poptop/sbin/pptpd -d** dette vil starte Poptop op som en "daemon" (service). Ønsker man at Poptop skal starte op når man starter sin Debian op, skal man lave et init.d job. Dette gøres således:

```
host:~# nano /etc/init.d/pptpd
```

Og ligge dette ind som tekst

```
#!/bin/sh

case "$1" in
start)
  echo -n "Running pptpd "
  /usr/local/poptop/sbin/pptpd -d
  echo "."
  ;;
*)
  echo "Usage: /etc/init.d/pptpd {start}"
  exit 1
esac

exit 0
```

Herefter skal man køre følgende kommando:

```
host:~# chmod 777 /etc/init.d/pptpd
host:~# update-rc.d pptpd defaults
```

Herefter vil Debian automatisk starte Poptop op, når den bliver startet op.

## Opsætning af Masquerading-script

For at man kan snakke sammen med maskiner bag VPN serveren, skal man aktivere et masquerade, dette gør man ved at lave en fil, som f.eks. kunne hedde **masqing.sh**, som vi ligger i **/usr/local/bin**. Denne fil skal vi have lavet eksekverbar med **chmod** til 777 så vi kan starte den.

```
host:~# chmod 777 /usr/local/bin/masqing.sh
```

Indholdet af denne fil skal være følgende:

```
#!/bin/sh  
  
# tillad forwarding af pakker  
echo "1" > /proc/sys/net/ipv4/ip_forward
```

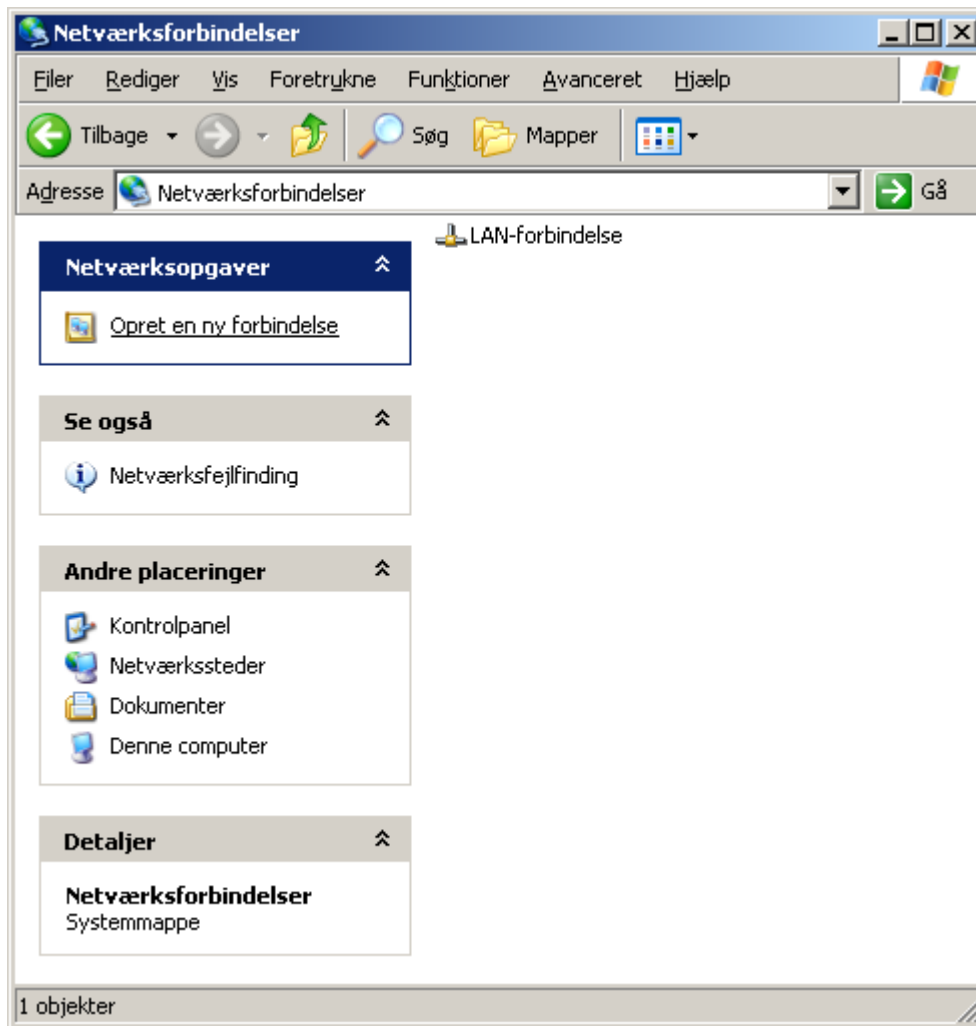
Her tillader vi forwarding af pakker, og det er faktisk nok til at det bliver muligt at se maskiner bag VPN serveren.

Det er altid en god ide at lave en firewall, når man har en maskine som står direkte på Internettet, men i vores forsøg sad vi på et lukket net, og havde derfor ikke behov for det. I Linux kan man bruge iptables eller ipchains til at lukke og åbne for pakker og derved sætte en firewall op.

## Opsætning af Windows XP Pro klient

Opsætningen af VPN klienten i WinXP Pro kræver ikke nogen speciel software eller patches som vi brugte under installationen af Debian.

Det første man gør, er at gå ind i kontrolpanelet, hvorefter man åbner ”**Netværksforbindelser.**” Derefter skulle der gerne komme et vindue frem som minder lidt om billedet herunder.



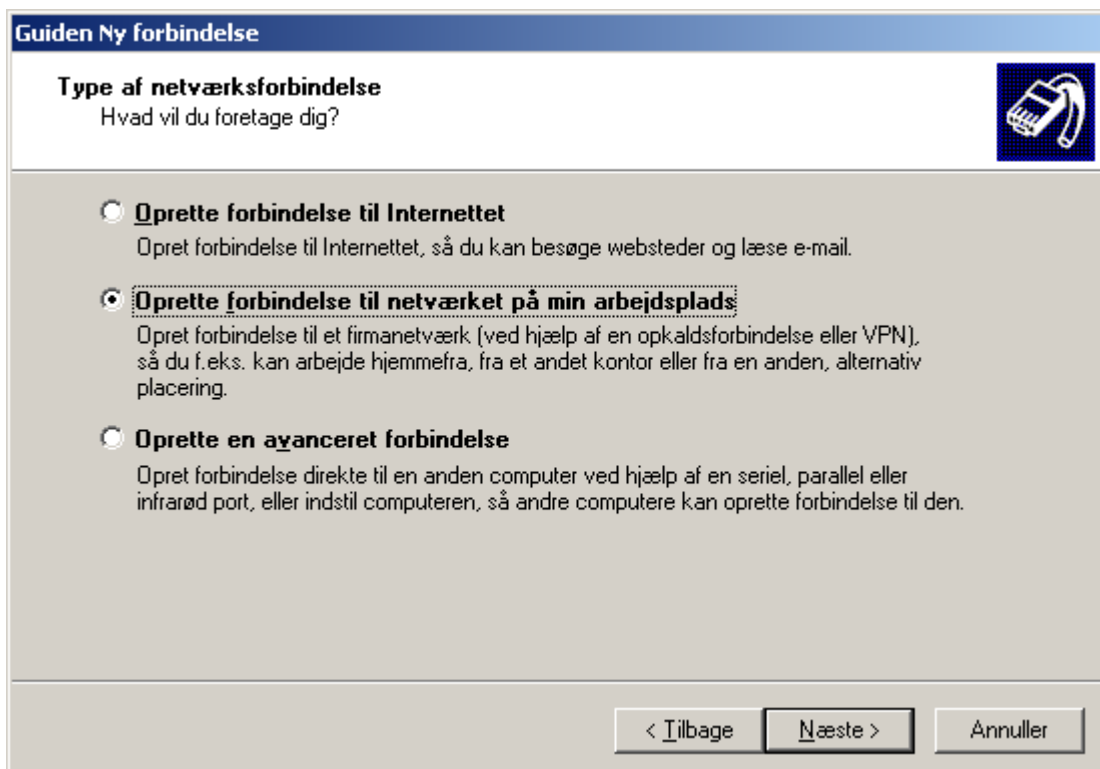
Herefter trykker man på ”**Opret en ny forbindelse**” ude til venstre i vinduet.



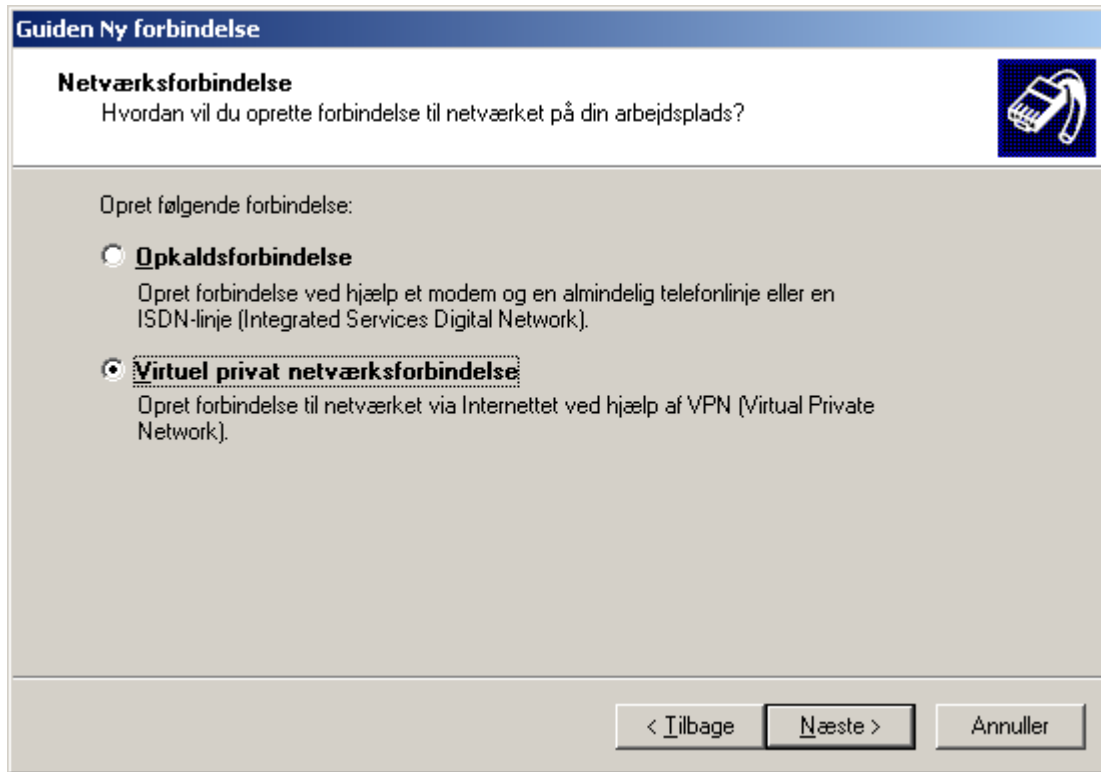
Nu skulle denne guide gerne komme frem og der trykkes på ”Næste”.



Man vælger at ”Oprette forbindelse til netværket på min arbejdsplads” og trykker ”Næste”.



Her vælger man selvfølgelig ”**Virtuel privat netværksforbindelse**” og trykker ”**Næste**”.



**Guiden Ny forbindelse**

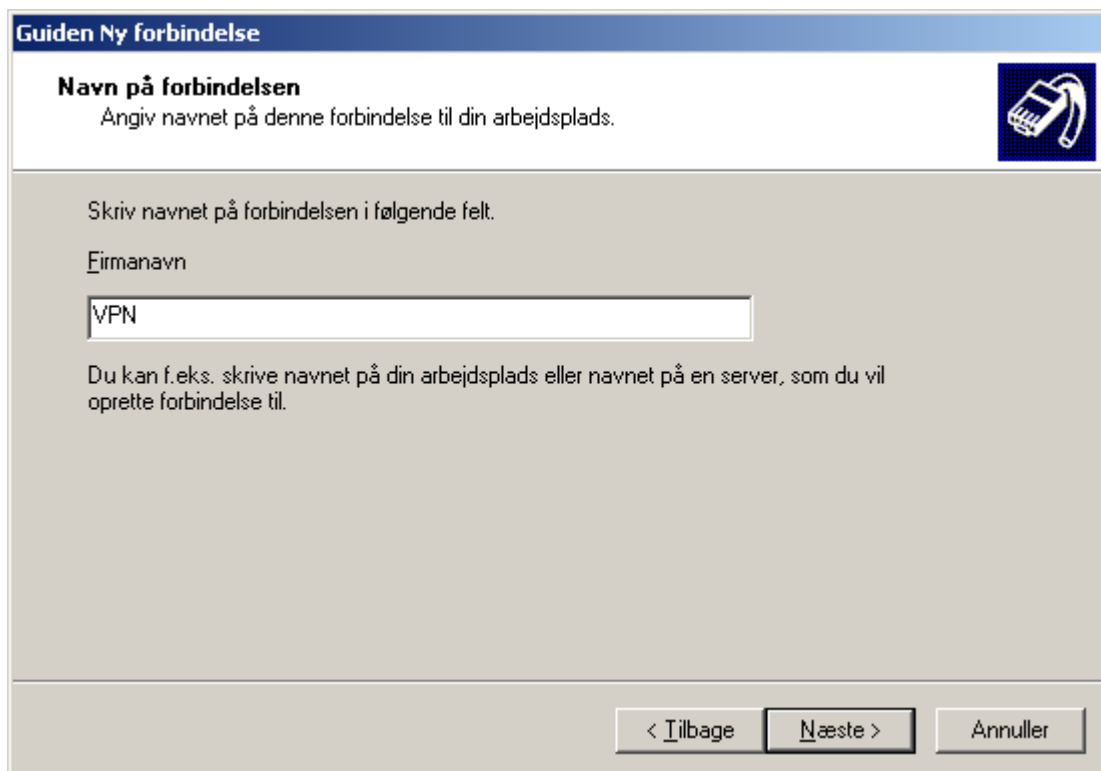
**Netværksforbindelse**  
Hvordan vil du oprette forbindelse til netværket på din arbejdsplads?

Opret følgende forbindelse:

- Opkaldsforbindelse**  
Opret forbindelse ved hjælp et modem og en almindelig telefonlinje eller en ISDN-linje (Integrated Services Digital Network).
- Virtuel privat netværksforbindelse**  
Opret forbindelse til netværket via Internettet ved hjælp af VPN (Virtual Private Network).

< Tilbage    Næste >    Annuller

Som navn kan man skrive hvad man nu lyster, vi har skrevet VPN. Tryk ”**Næste**”.



**Guiden Ny forbindelse**

**Navn på forbindelsen**  
Angiv navnet på denne forbindelse til din arbejdsplads.

Skriv navnet på forbindelsen i følgende felt.

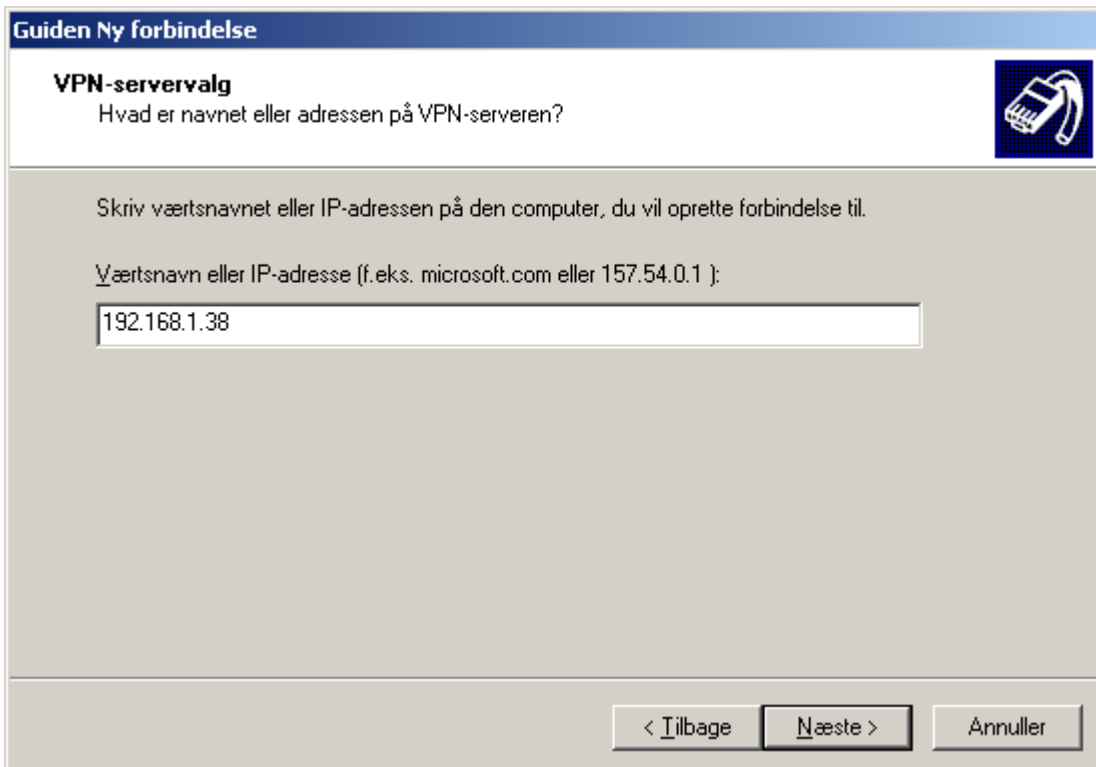
Firmanavn

VPN

Du kan f.eks. skrive navnet på din arbejdsplads eller navnet på en server, som du vil oprette forbindelse til.

< Tilbage    Næste >    Annuller

Dernæst skal man angive IP'en på den Debian-box man satte op tidligere. Det var i vores tilfælde 192.168.1.38. Tryk "Næste".



**Guiden Ny forbindelse**

**VPN-servervalg**  
Hvad er navnet eller adressen på VPN-serveren?

Skriv værtsnavnet eller IP-adressen på den computer, du vil oprette forbindelse til.

Værtsnavn eller IP-adresse (f.eks. microsoft.com eller 157.54.0.1):

< Tilbage **Næste** > Annuller

Af sikkerhedsmæssige grunde vælger vi at forbindelsen kun skal være tilgængelig for vores bruger. Vælg "Kun til eget brug" og tryk "Næste".



**Guiden Ny forbindelse**

**Forbindelsestilgængelighed**  
Du kan gøre den nye forbindelse tilgængelig for enhver bruger eller kun for dig selv.

En forbindelse, der alene oprettes til eget brug, gemmes i din brugerkonto og vil ikke være tilgængelig, medmindre du er logget på.

Opret denne forbindelse:

Til alle brugere

**Kun til eget brug**

< Tilbage **Næste** > Annuller

Hvis man har lyst til endnu en genvej på skrivebordet er man velkommen til at markere boksen i dette vindue, men det gider vi ikke og trykker ”Udfør”.

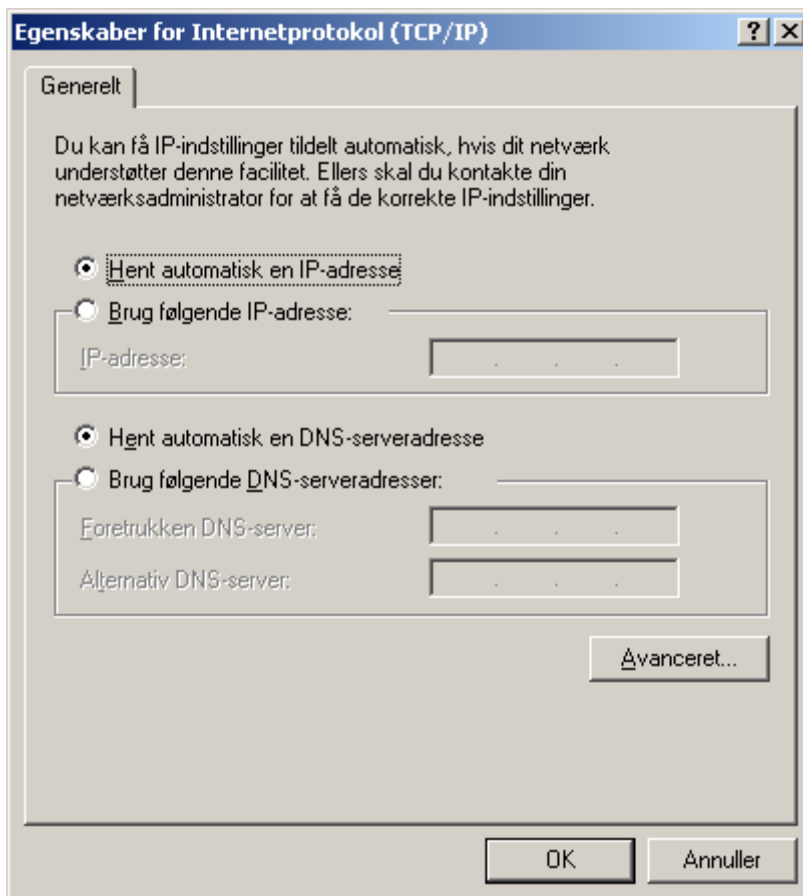
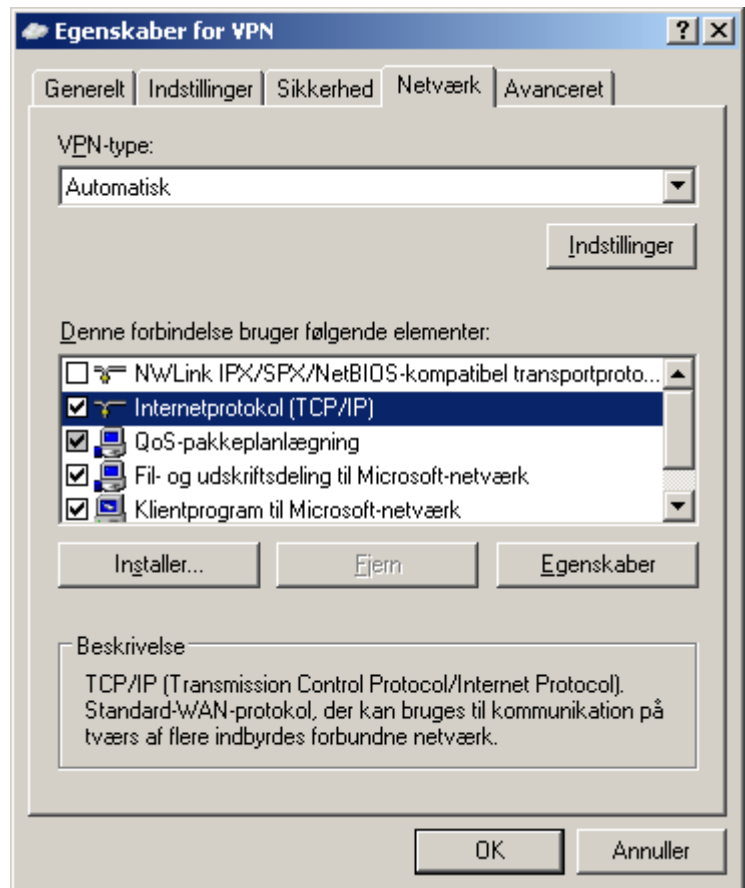


Nu er de grundlæggende indstillinger sat op og vi går videre til opsætning af selve opkaldsforbindelsen. Brugernavn, **vpn**, og adgangskode, **test**, tages ind. Derefter trykker man på ”Egenskaber”.

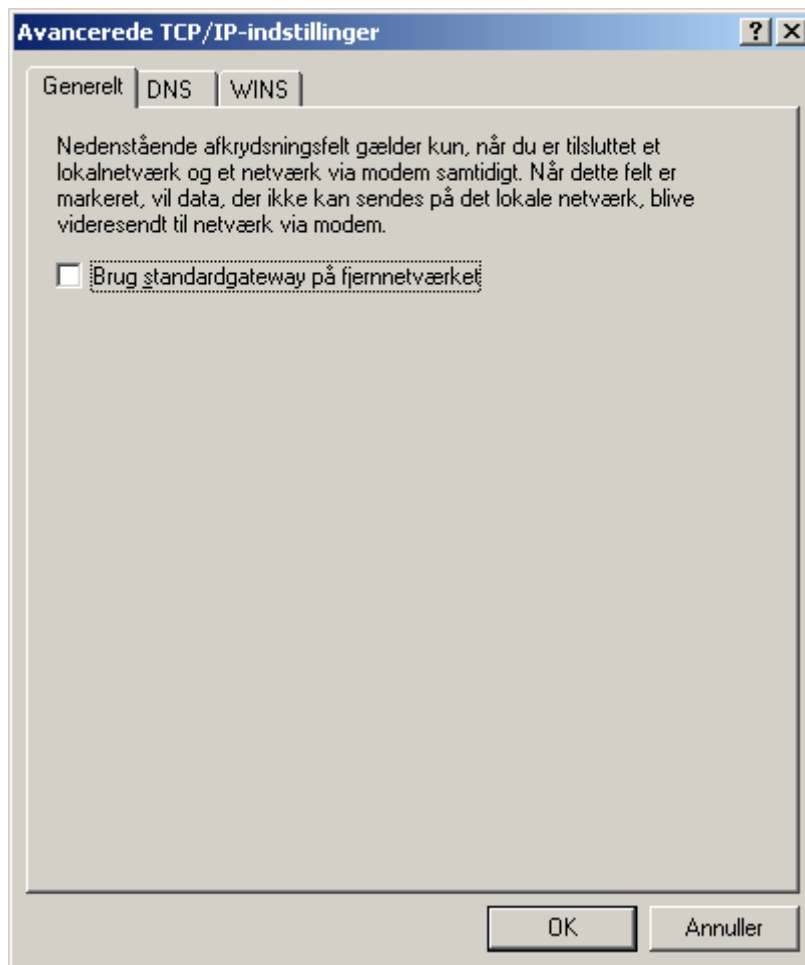


Under egenskaber vælger man fanbladet ”**Netværk**” og markerer ”Internetprotokol(TCP/IP)” som vist herunder og trykker **egenskaber**.

NB: Hvis man har IPX/SPX/NetBIOS protokollen installeret som vi har, skal man lige fjerne fluebenet fordi den ikke bliver nødvendig.



Når dette vindue kommer frem vælger man ”**Avanceret**”.



For ikke at bruge VPN-gate wayen som internet-gateway, fjerner man fluebenet her til venstre ved at trykke på.

**”Brug standardgateway på fjernnetværket”** og trykker **”Ok”**.

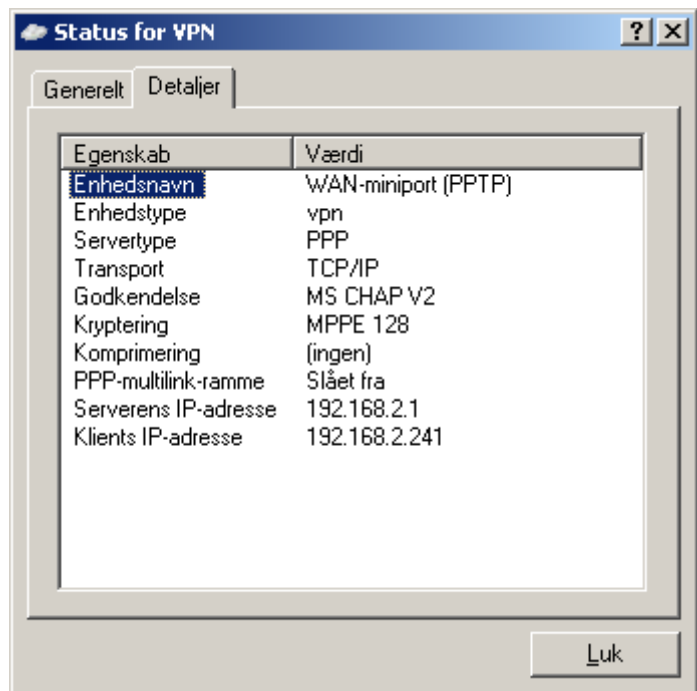
Man vil så kun få adgang til nettet bag gatewayen og ikke anvende gatewayen til surfing osv.

Derefter trykker man ”Ok” igen og så en sidste ”Ok” og man skulle være tilbage til billedet herunder, hvor man trykker **”Tilslut”**

Nu skulle man gerne have adgang til serveren med IP 192.168.1.38. (Som den hedder i vores tilfælde.)



Efter at man har fået etableret forbindelse, kan man vælge at se status for sin VPN forbindelse. Den skulle gerne komme til at se ud som den her til højre, hvor man kan se at vi anvender MS CHAP V2 som godkendelses protokol og MPPE 128 til kryptering.



## Konklusion

Når man sætter sig for at prøve noget software på en Linux-box, skal man ikke forvente at man får alt serveret på et sølvfad. Dokumentationen er til tider meget dårlig og man kan hurtigt miste modet når de fejl der opstår kun består af Hexadecimale tal, men der er håb forude!

Søgemaskinen Google er faktisk et genialt stykke værktøj når det gælder fejlsøgning.

Der er efterhånden mange som har oprettet nogle tråde der med tiden også har fået et svar og ved at søge på fejlkoden kommer der ofte en tråd med et svar, eller et forslag til hvad muligvis kan være galt.

Vi fandt hurtigt ud af at Poptop kildekoden ikke bare skulle kompileres og så var man "up and going", det kræver en del patches i kernen, men også patches til nogle af de moduler man er nødt til at hente ude fra. Ikke nok med det, man kan med stor fordel gøre sig umage med at anskaffe patches der er skrevet af den samme programmør, fordi at open-software ikke altid er kompatibelt med hinanden. Det konkluderede vi i hvert fald efter lang tids søgen på Google. De patches og kilde koder vi henvender til, i denne dokumentation, er kompatible med hinanden.



## Kilder

### ***Installerings af Poptop.***

<http://poptop.sourceforge.net/dox/source-howto.html>

### ***Konfiguration af Poptop.***

<http://poptop.sourceforge.net/dox/modules.conf.txt>

<http://poptop.sourceforge.net/dox/pptpd.conf.txt>

<http://poptop.sourceforge.net/dox/options.pptpd.txt>

<http://poptop.sourceforge.net/dox/chap-secrets.txt>

### ***Blandede links.***

<http://poptop.sourceforge.net/dox/>

<http://www.poptop.org>

<http://people.freebsd.org/~nsayer/802-11.html> “stateless option”

<http://iptables-tutorial.frozentux.net/iptables-tutorial.html> Opsætning af Masquerading.