Using IPsec on the NANOG Network

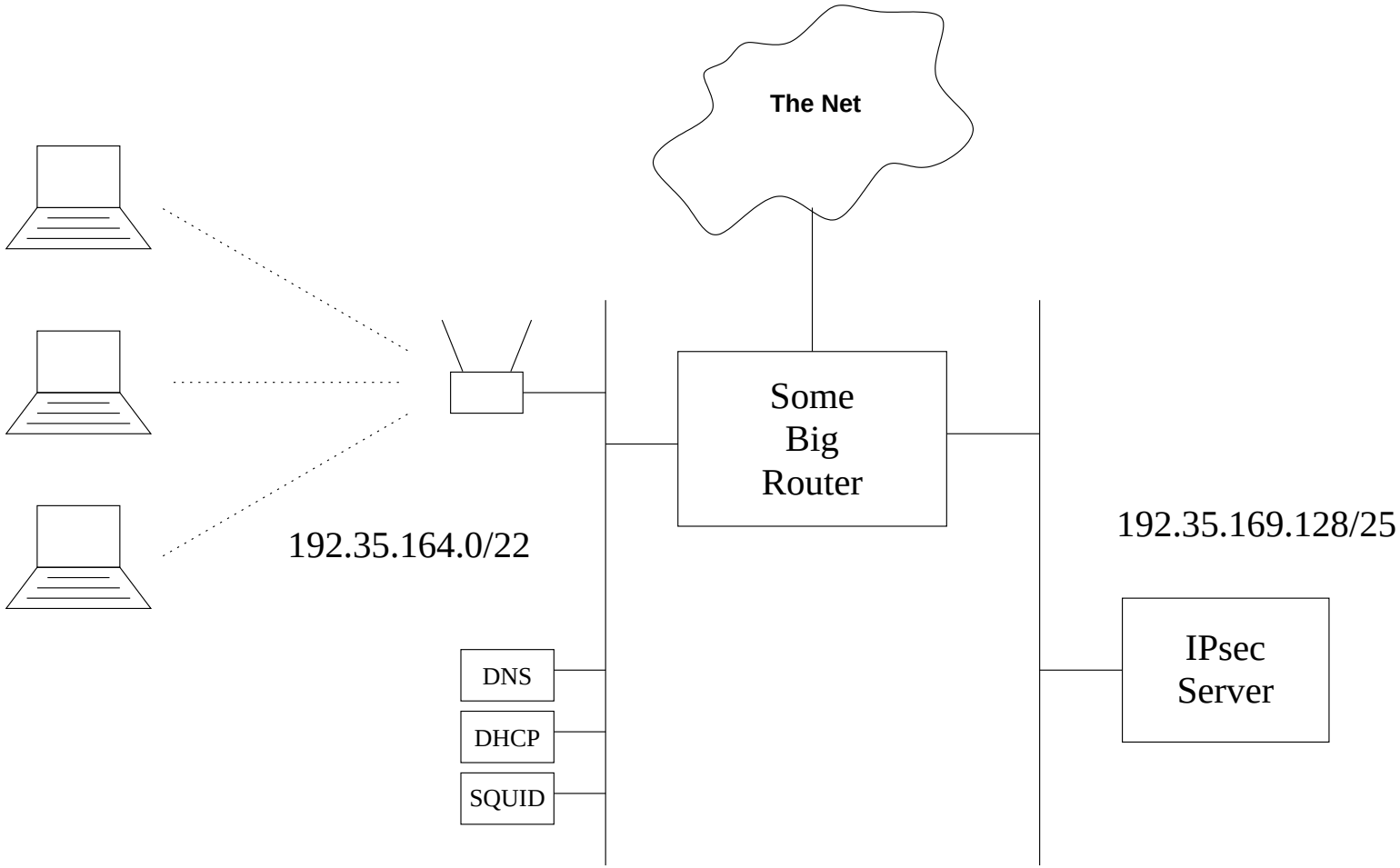
Duane Wessels
The Measurement Factory, Inc.
wessels@measurement-factory.com

NANOG 31
May 2004

Motivation

- The wireless network makes it easy for anyone to eavesdrop.
- We can encrypt (wireless) traffic locally and decrypt it once it gets to the wires.

Network Diagram



Caveats

- Does not prevent eavesdropping out on the Internet.
- Traffic to/from the local subnet may not be encrypted.
- Does not secure your laptop from attacks (i.e., this is not a firewall).
- We are mainly interested in encryption, no so much in authentication.

Big Picture

- Your IPsec client creates a security association with the IPsec server. We're using pre-shared keys.
- Your laptop gets a secondary IP address, assigned automatically or manually, depending on your operating system.
- Outgoing packets are encrypted if they match an IPsec Security Policy Database (SPD) entry. These contain src/dest addresses and masks, port numbers, etc.
- For Windows XP using L2TP, the security association uses your primary IP address and L2TP port numbers.

Big Picture

- For Linux/BSD/Mac, the security association uses your secondary IP address. Then we use NAT/routing tricks to make outgoing packets have the secondary IP address.
- The IPsec server has proxy ARP entries for these secondary addresses.
- Packets coming in from the outside hit the IPsec server, where they are encrypted and then tunneled back to your laptop.

IP Addresses

192.35.XXX.YYY XXX: 165–167 YYY: 1–254	your primary address, assigned by DHCP
192.35.169.ZZZ ZZZ: 130-179 ZZZ: 180-229	Secondary address automatically assigned for L2TP manually assigned for Linux/BSD/Mac
192.35.169.254	IPsec server — racoon
192.35.169.252	IPsec server — isakmpd
192.35.169.253	Remote tunnel endpoint for L2TP users

The Windows XP Way

- Use the built-in L2TP+IPSEC client.
- Create new VPN connection.
- Establish security association between XP and IPsec server.
- Establish L2TP tunnel between XP and IPsec server. All L2TP traffic will be encrypted.
- The tunnel address becomes new default route.
- Secondary address assigned automatically by L2TP daemon on IPsec server.

The Mac OS/X Way

- Download VaporSec.
- Or use built-in *racoon*.
- Add an IP alias on the ethernet interface.
- Add default route through alias address.
- Secondary/alias address assigned manually.

The FreeBSD Way

- Need IPSEC support in the kernel.
- Need to install *racoon* or *isakmpd*.
- Add an IP alias on the ethernet interface.
- Establish security association with the IPsec server.
- Add default route through alias address.
- Secondary/alias address assigned manually.

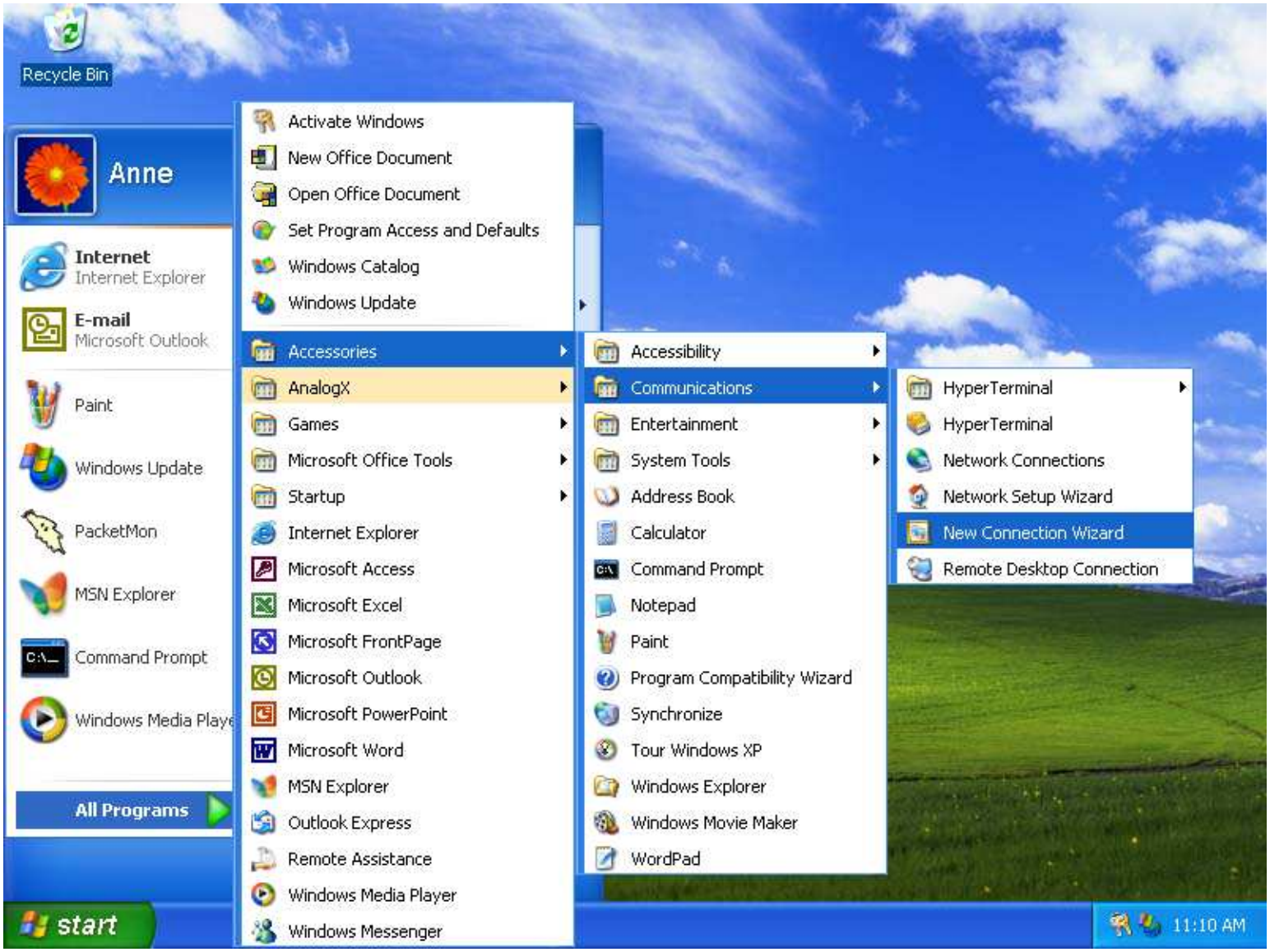
The Linux Way

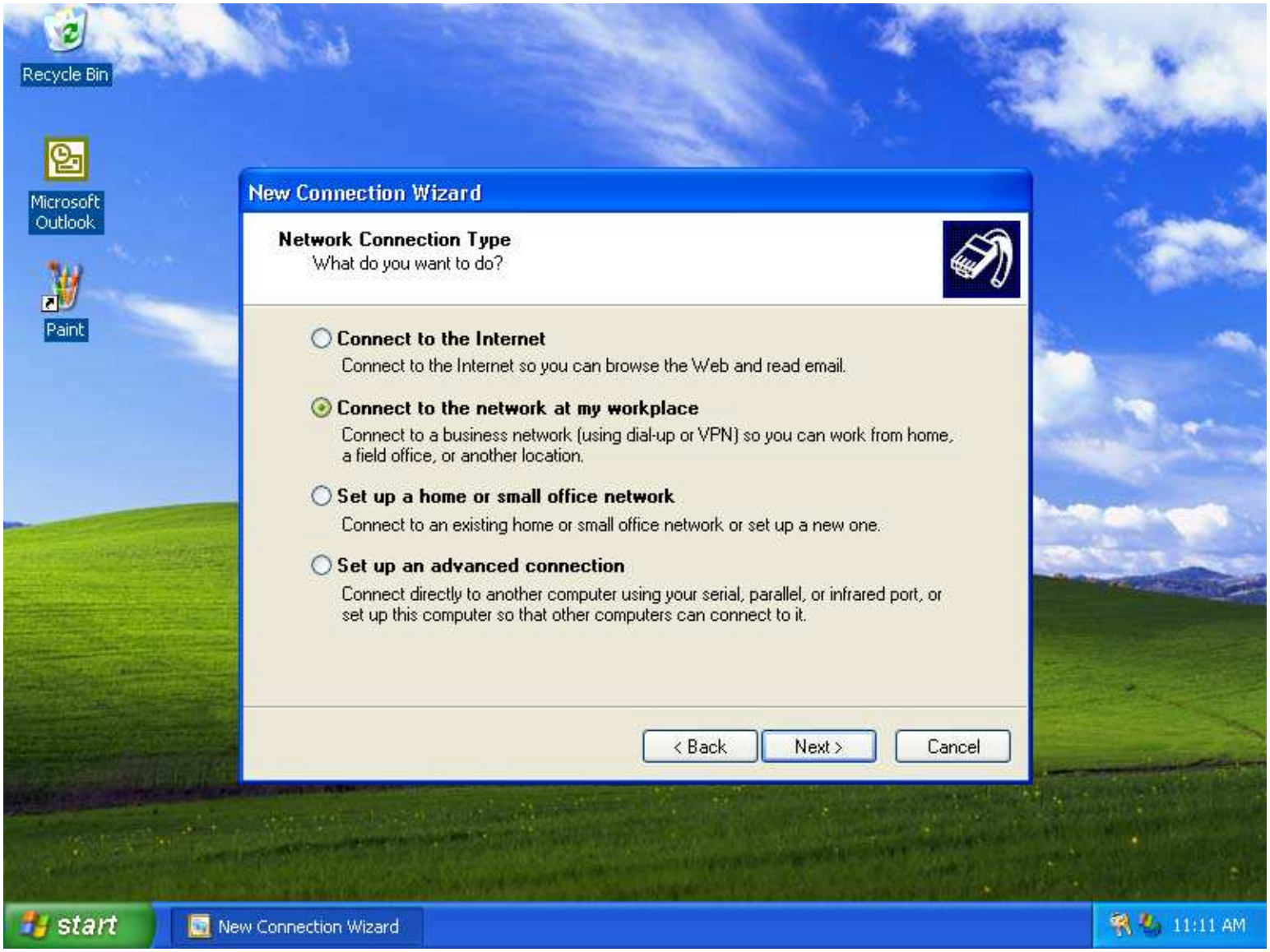
- Need to install FreeS/WAN (now Openswan).
- Add an IP alias on the ethernet interface.
- Establish security association with the IPsec server.
- Add some iptables rules to NAT outgoing packets to the alias address.
- Secondary/alias address assigned manually.

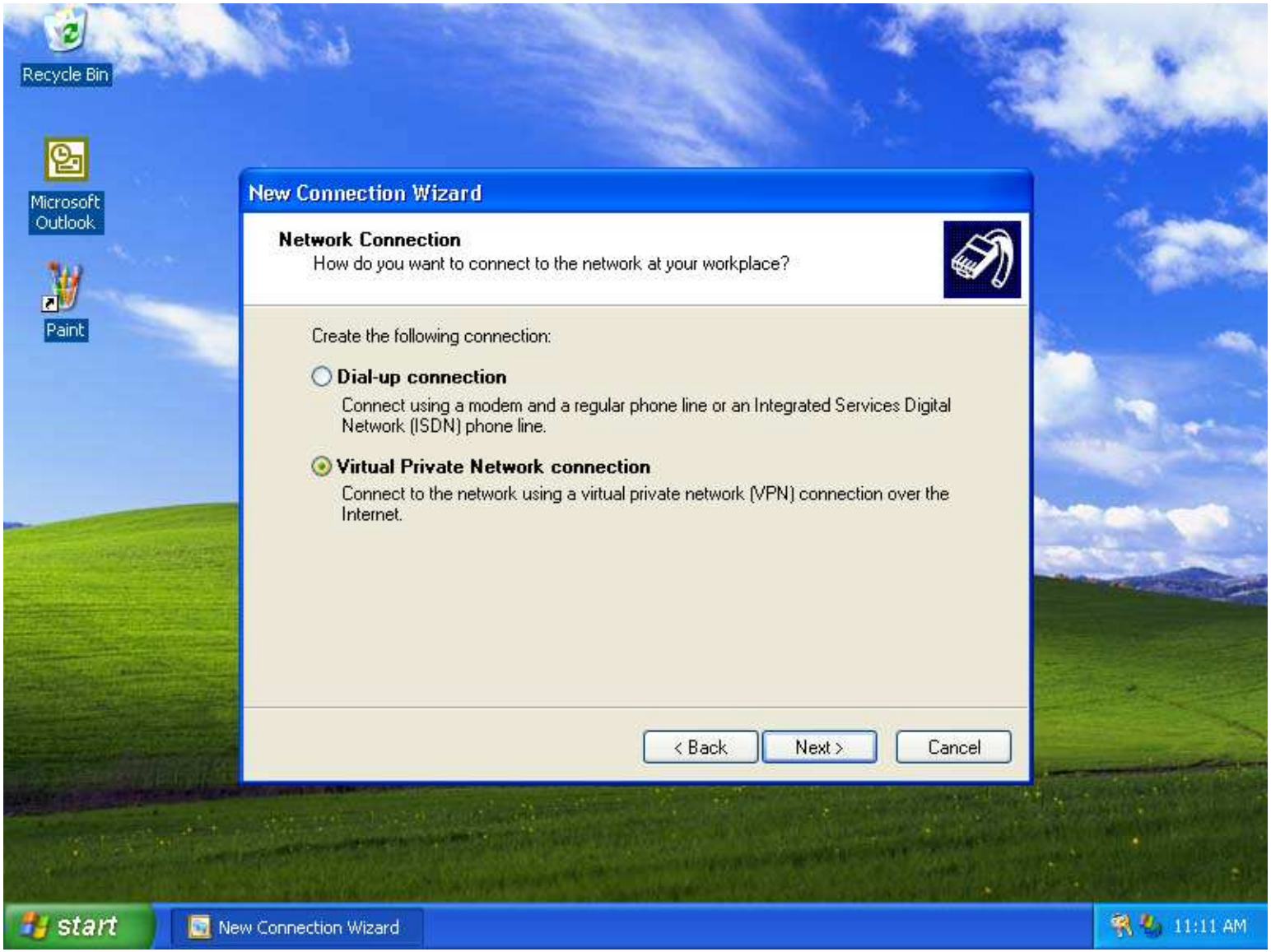
The Windows XP Way

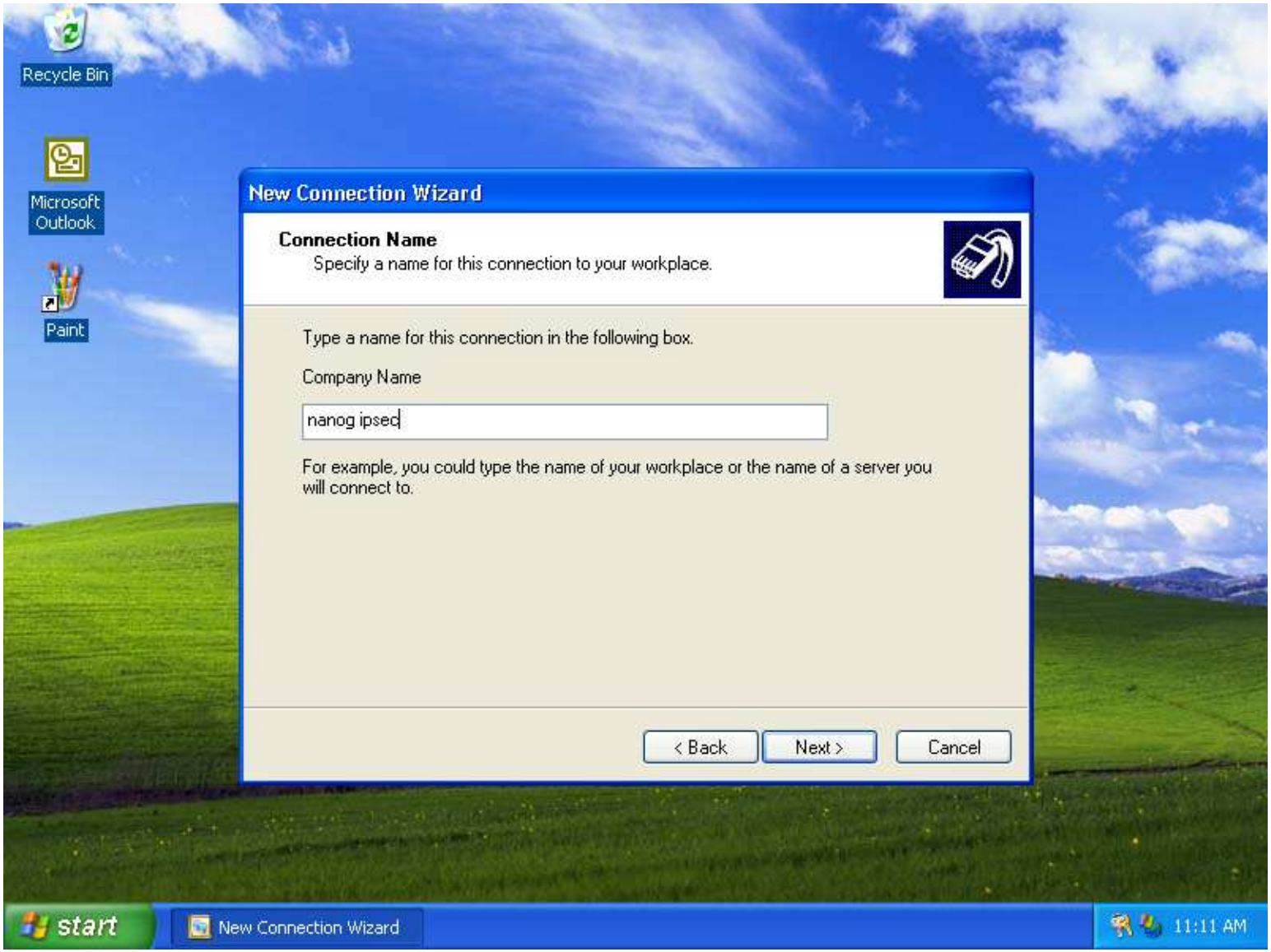
Enable IPsec Service

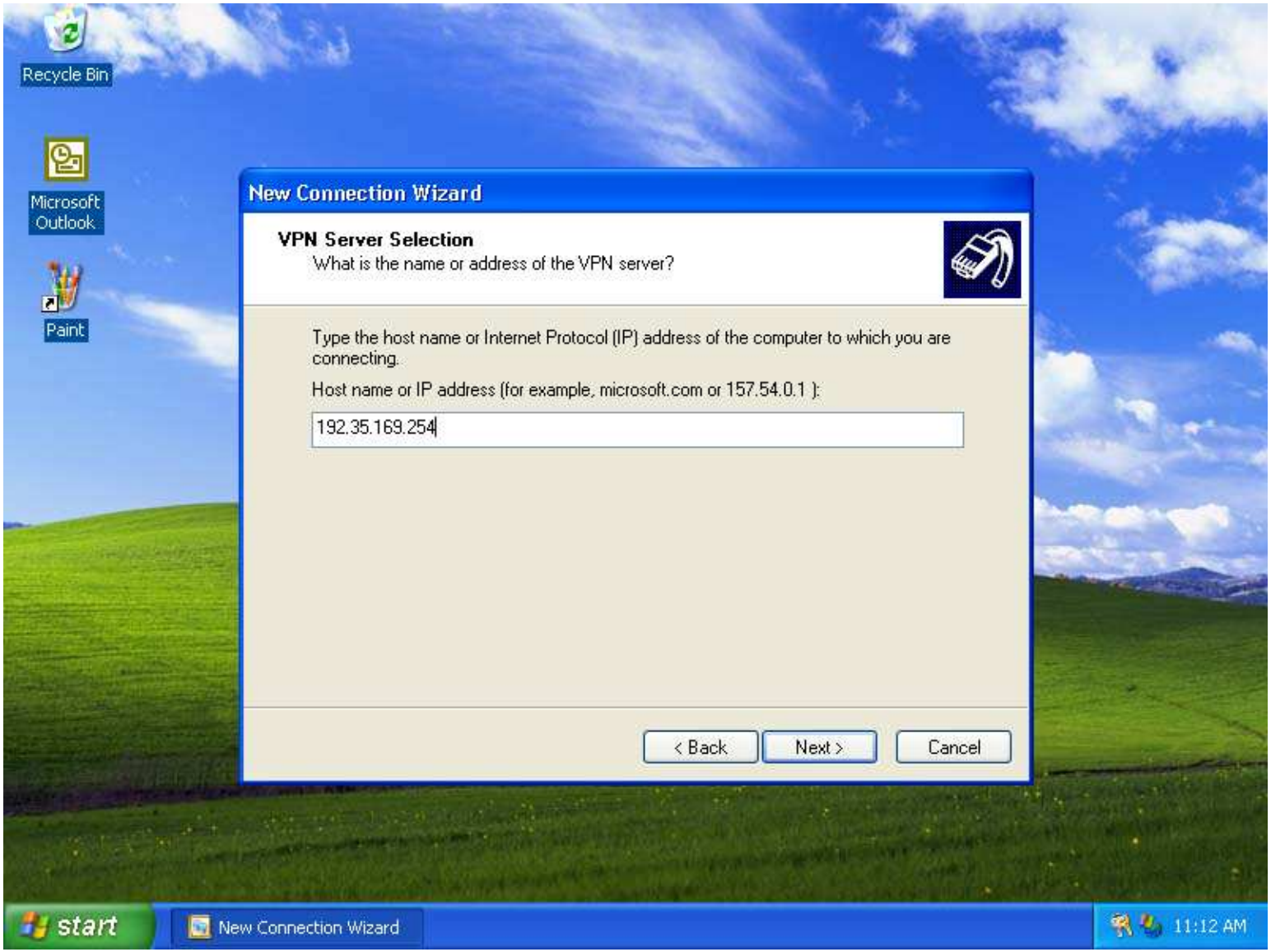
- Sorry, no screendump yet
- Control Panel
- Something something
- Services
- IPsec service
- Start it
-

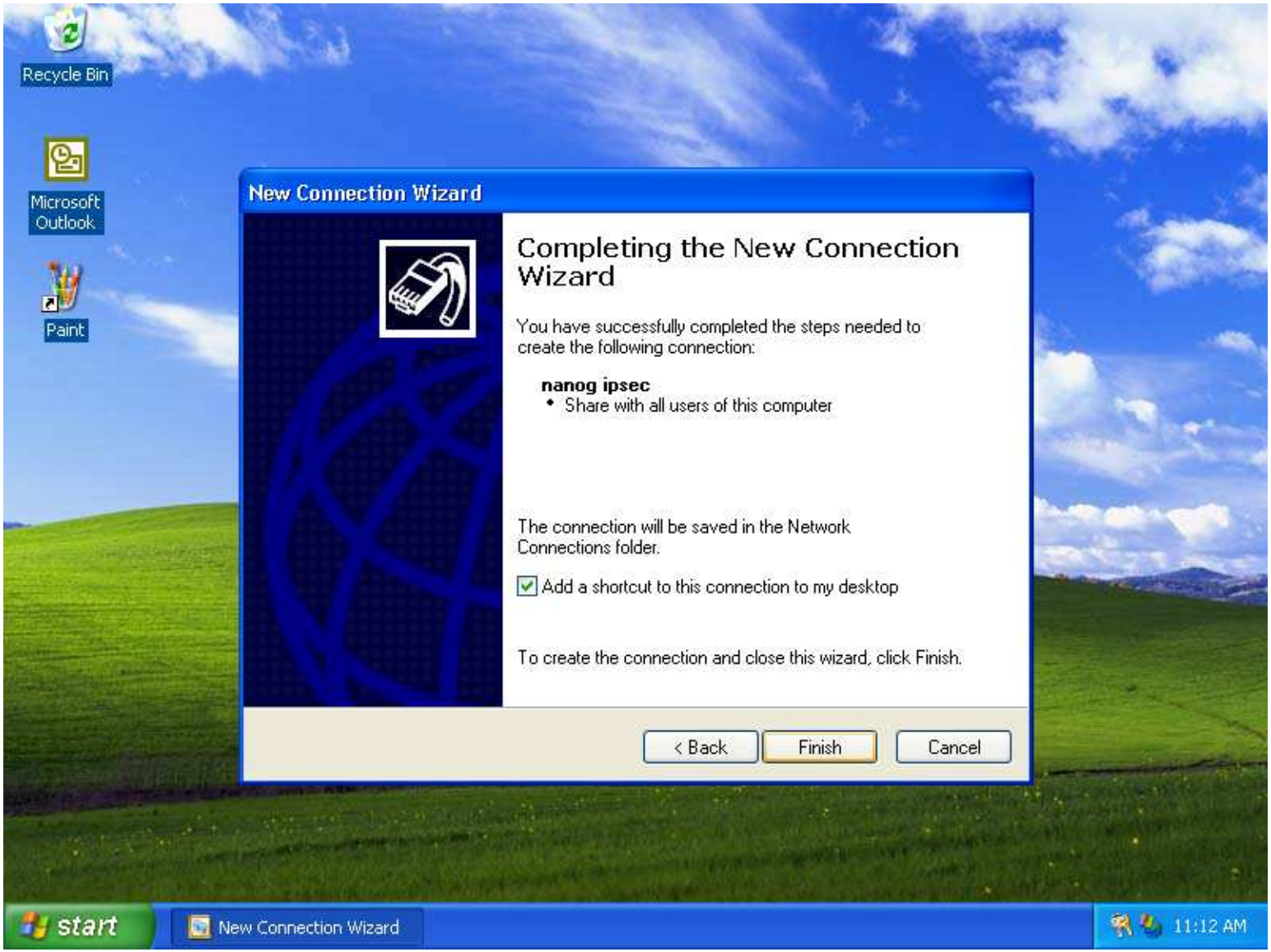

Recycle Bin
Anne
Internet
Internet Explorer
E-mail
Microsoft Outlook
Paint
Windows Update
PacketMon
MSN Explorer
Command Prompt
Windows Media Playe
All Programs
start
Activate Windows
New Office Document
Open Office Document
Set Program Access and Defaults
Windows Catalog
Windows Update
Accessories
AnalogX
Games
Microsoft Office Tools
Startup
Internet Explorer
Microsoft Access
Microsoft Excel
Microsoft FrontPage
Microsoft Outlook
Microsoft PowerPoint
Microsoft Word
MSN Explorer
Outlook Express
Remote Assistance
Windows Media Player
Windows Messenger
Accessibility
Communications
Entertainment
System Tools
Address Book
Calculator
Command Prompt
Notepad
Paint
Program Compatibility Wizard
Synchronize
Tour Windows XP
Windows Explorer
Windows Movie Maker
WordPad
HyperTerminal
HyperTerminal
Network Connections
Network Setup Wizard
New Connection Wizard
Remote Desktop Connection
11:10 AM

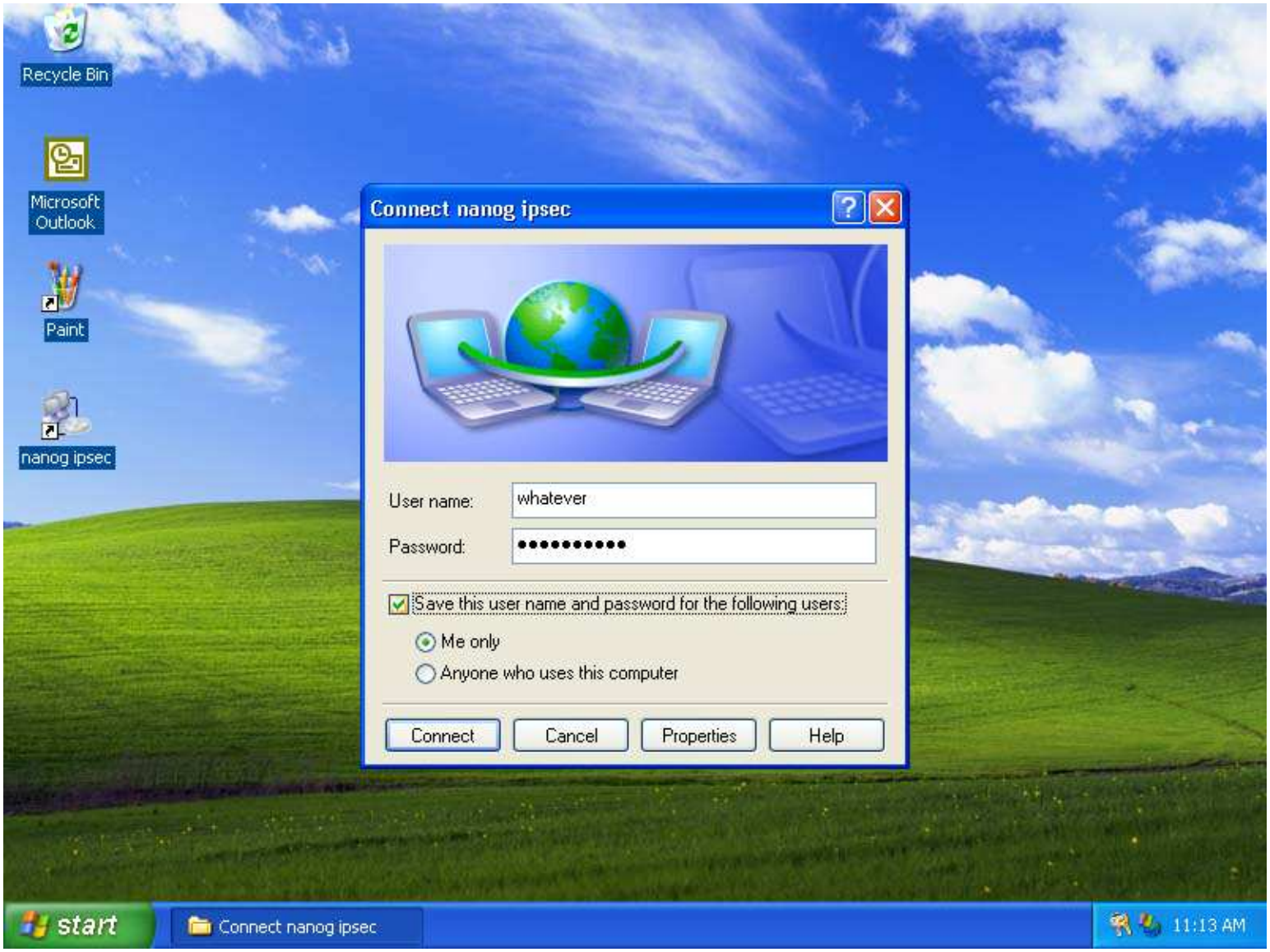

Recycle Bin
Microsoft Outlook
Paint
New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel
start
New Connection Wizard
11:11 AM


Recycle Bin
Microsoft Outlook
Paint
New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel
start
New Connection Wizard
11:11 AM


Recycle Bin
Microsoft Outlook
Paint
New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
nanog ipsec
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel
start
New Connection Wizard
11:11 AM

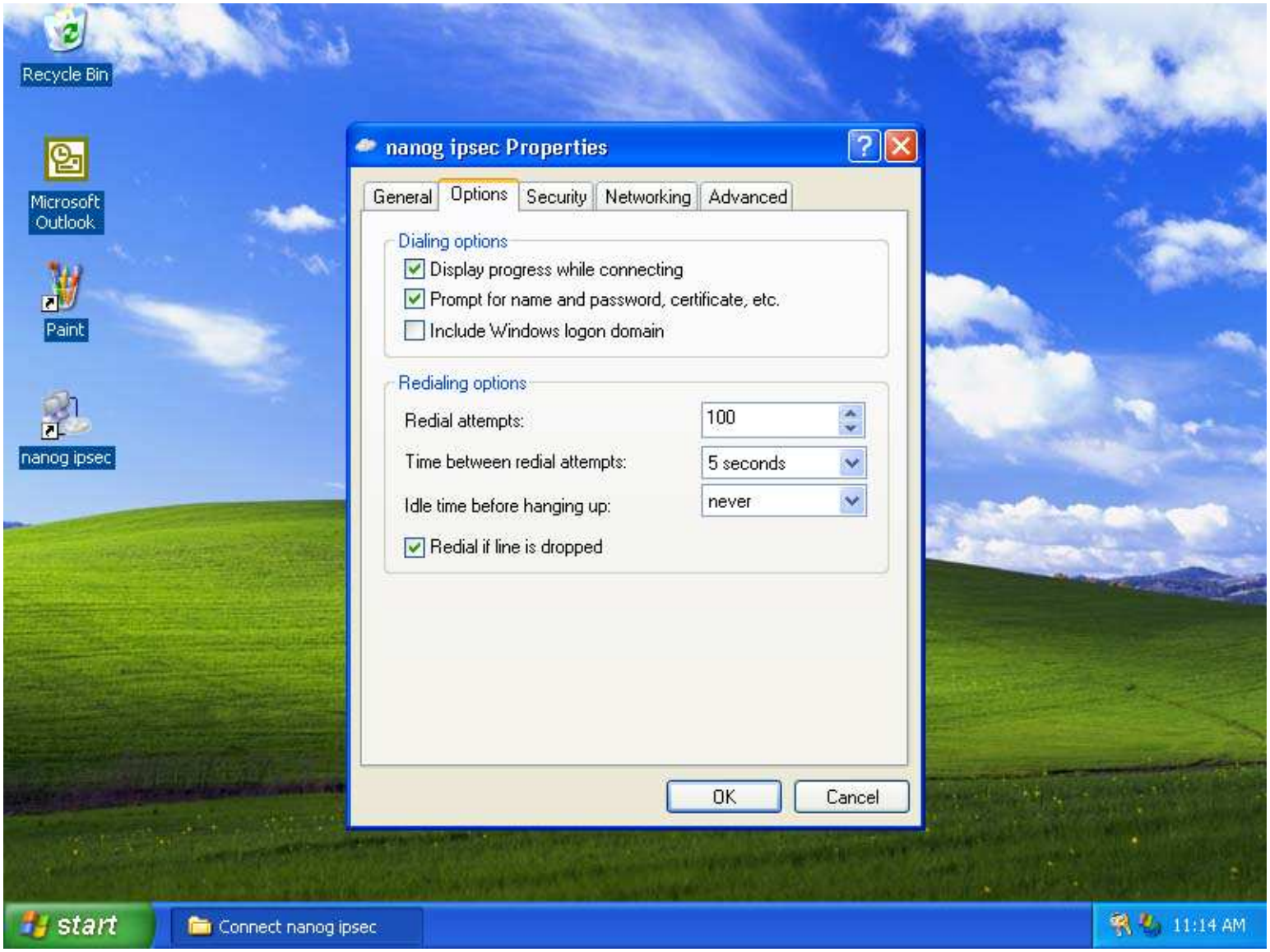

Recycle Bin
Microsoft Outlook
Paint
New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
192.35.169.254
< Back
Next >
Cancel
start
New Connection Wizard
11:12 AM


Recycle Bin
Microsoft Outlook
Paint
New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
nanog ipsec
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel
start
New Connection Wizard
11:12 AM

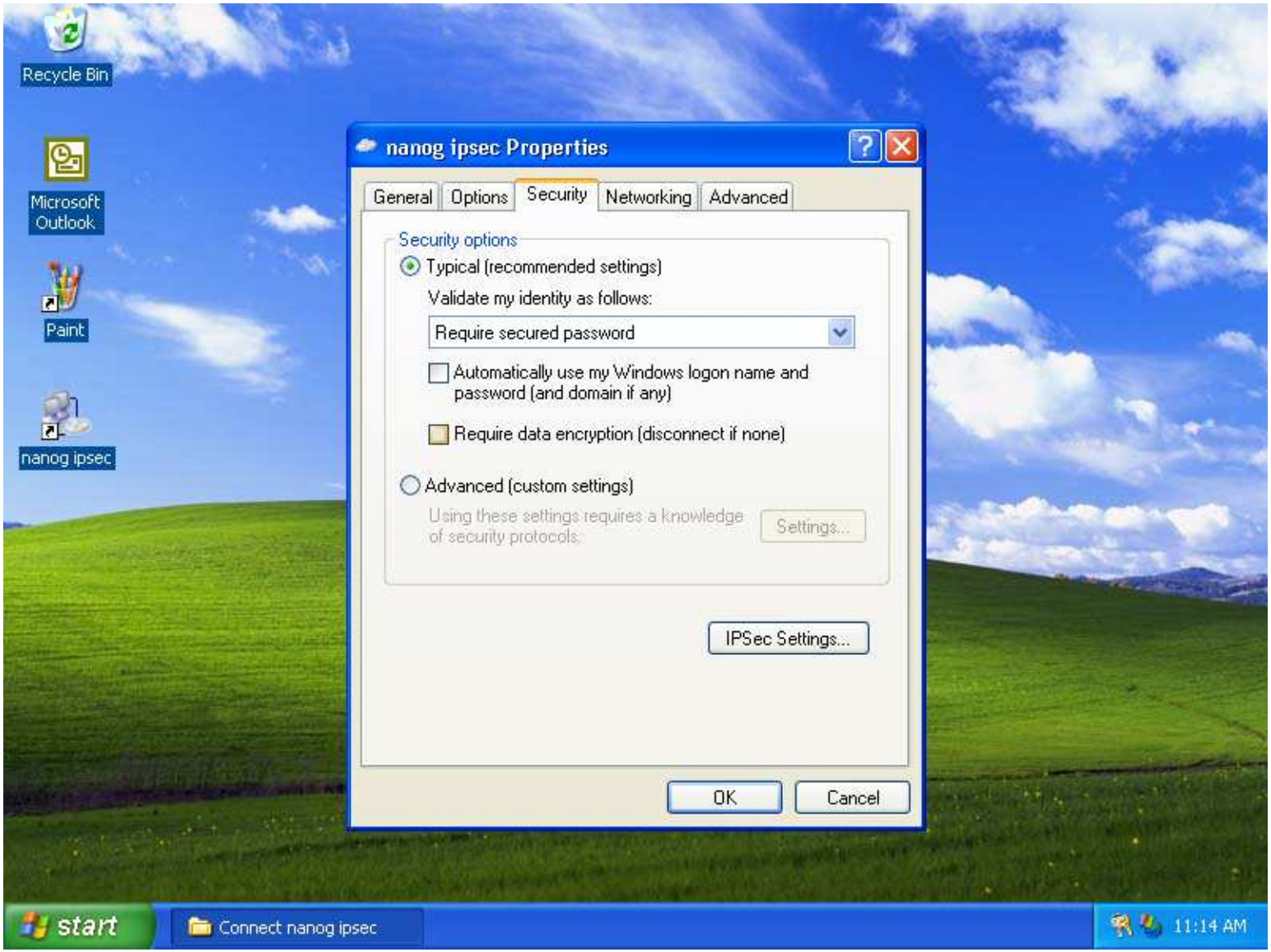


Username: can be anything

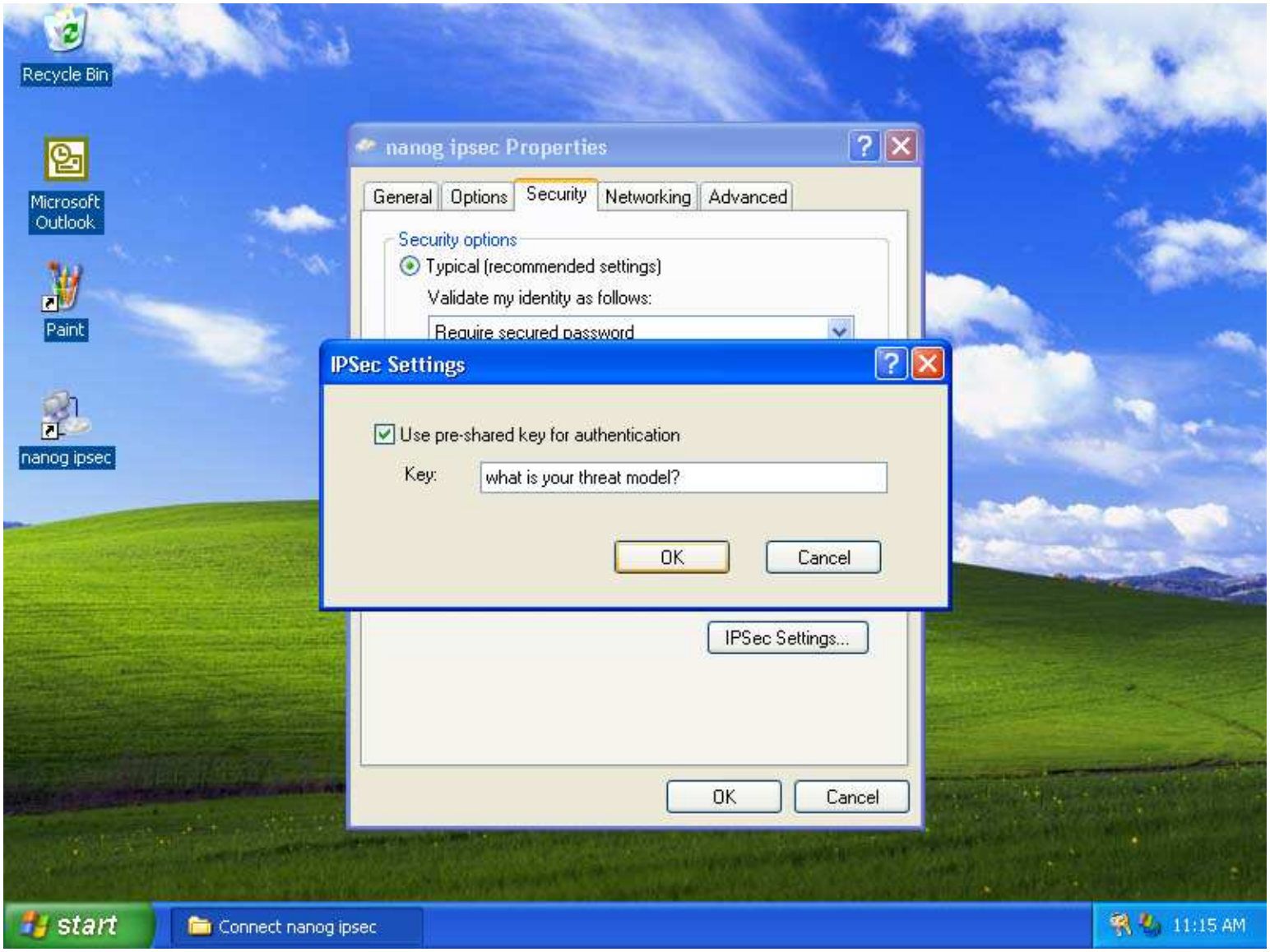
Password: passphrase



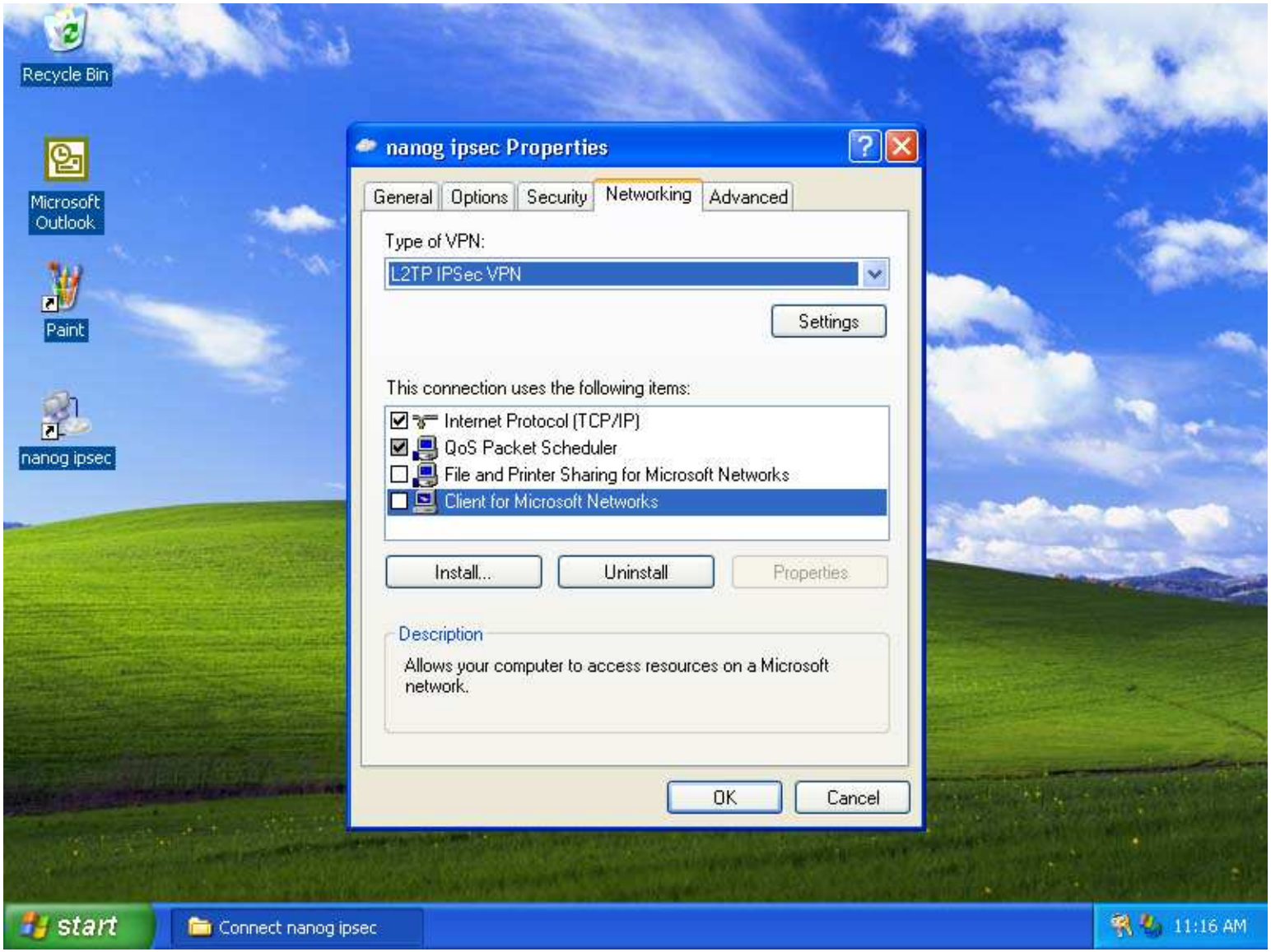
Probably want to increase redial attempts and decrease time between. Select "Redial if line is dropped."



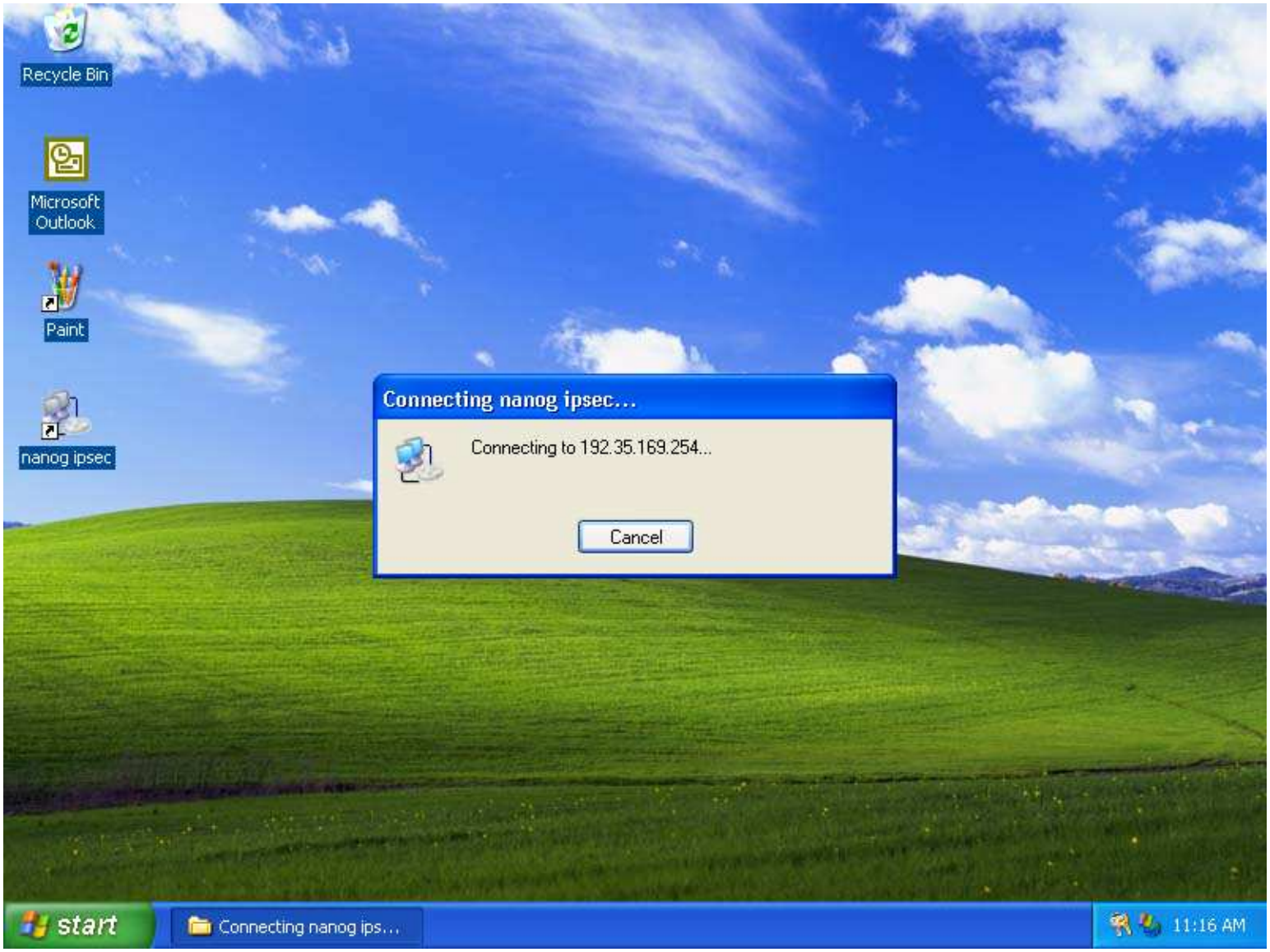
Uncheck "Require data encryption." That refers to L2TP/PPP encryption, NOT IPsec!

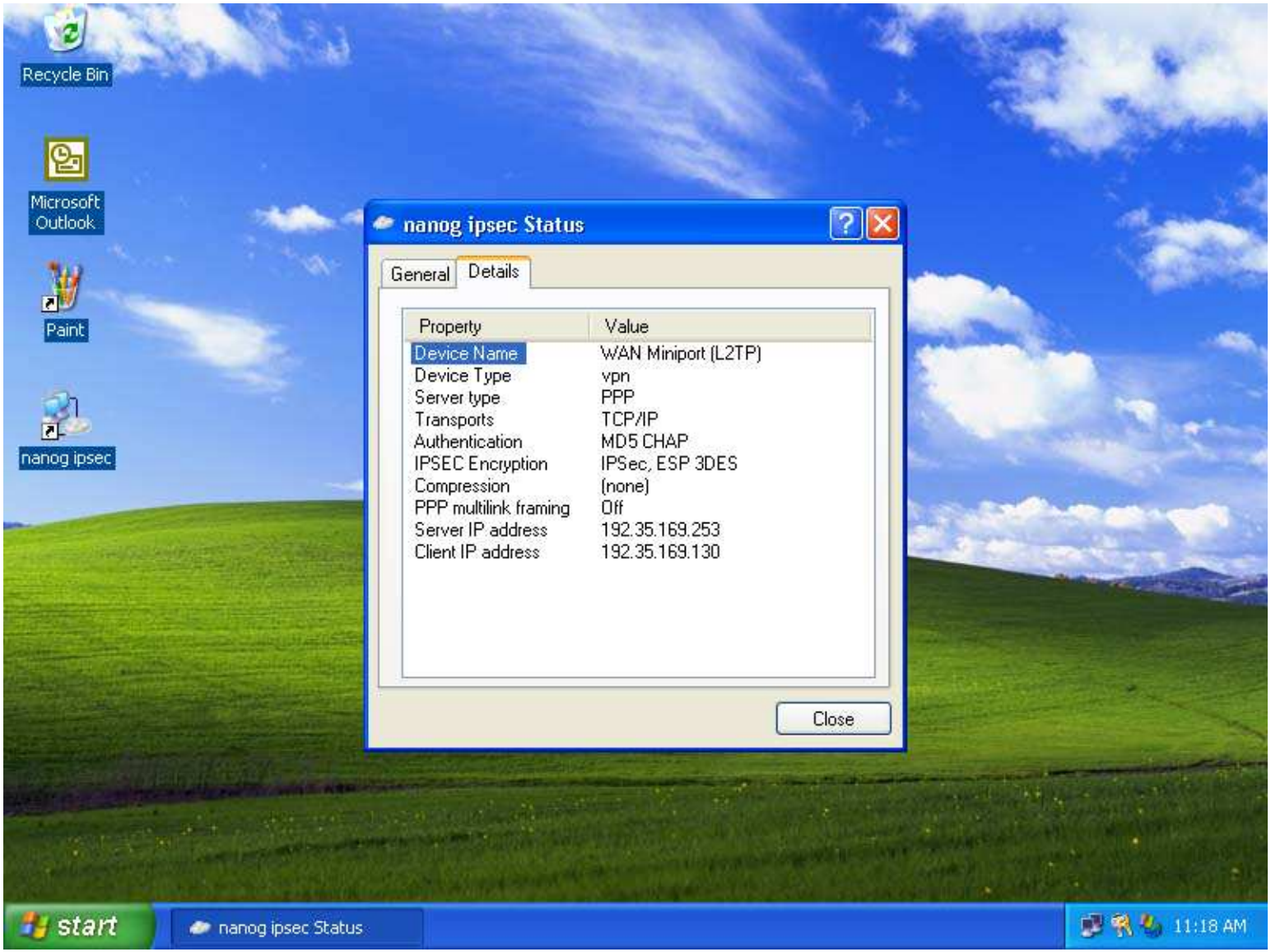


what is your threat model?



Select "L2TP IPsec VPN"


Recycle Bin
Microsoft Outlook
Paint
nanog ipsec
Connecting nanog ipsec...
Connecting to 192.35.169.254...
Cancel
start
Connecting nanog ips...
11:16 AM


Recycle Bin
Microsoft Outlook
Paint
nanog ipsec
nanog ipsec Status
General
Details
Property
Value
Device Name
WAN Miniport (L2TP)
Device Type
vpn
Server type
PPP
Transports
TCP/IP
Authentication
MD5 CHAP
IPSEC Encryption
IPSec, ESP 3DES
Compression
(none)
PPP multilink framing
Off
Server IP address
192.35.169.253
Client IP address
192.35.169.130
Close
start
nanog ipsec Status
11:18 AM

The Mac OS/X Way

VaporSec

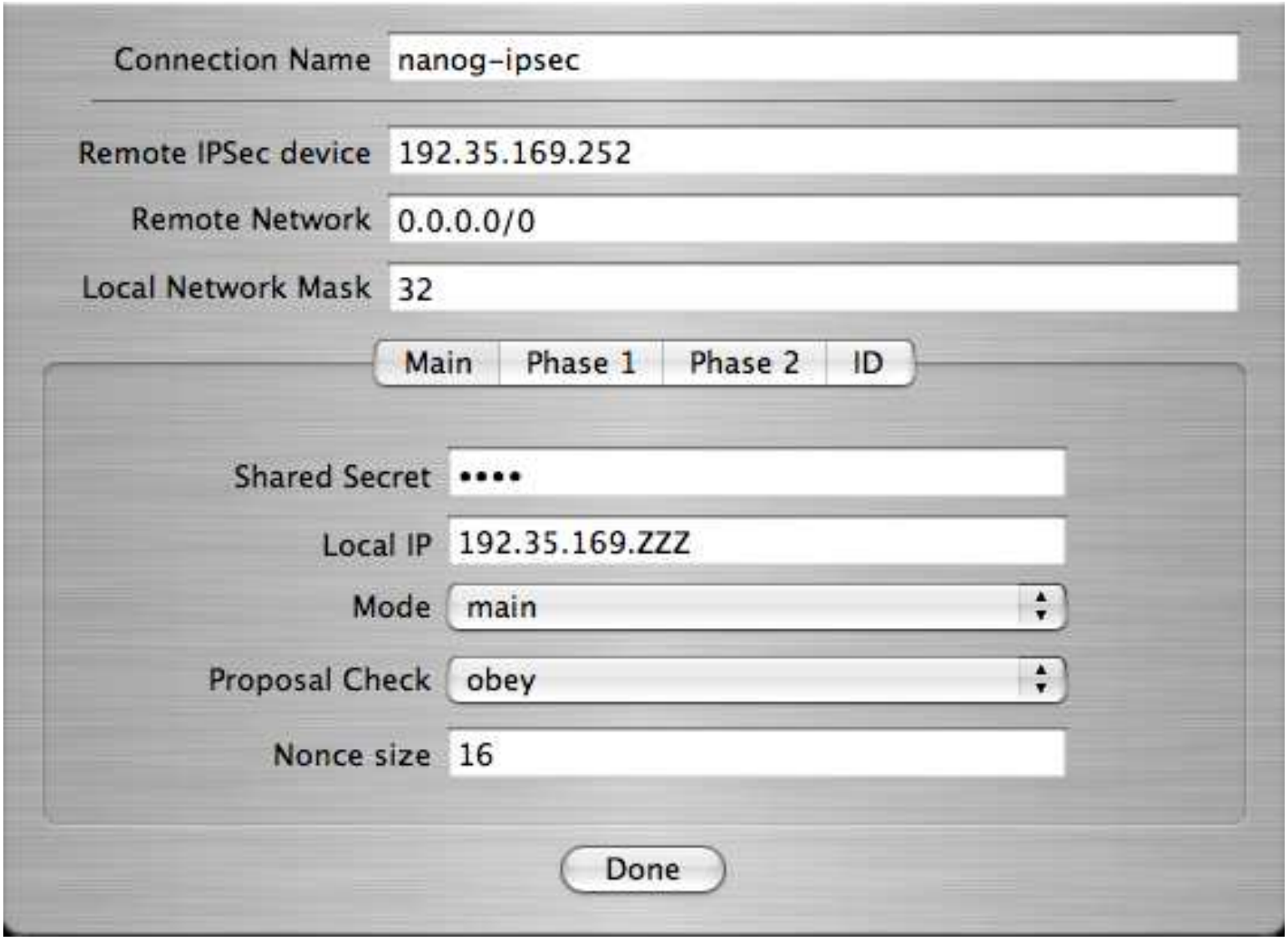
- VaporSec is a GUI front-end for *racoon*.
- You can get it from http://www.afp548.com/Software/VaporSec/
- We'll use the same aliasing and routing tricks as FreeBSD.

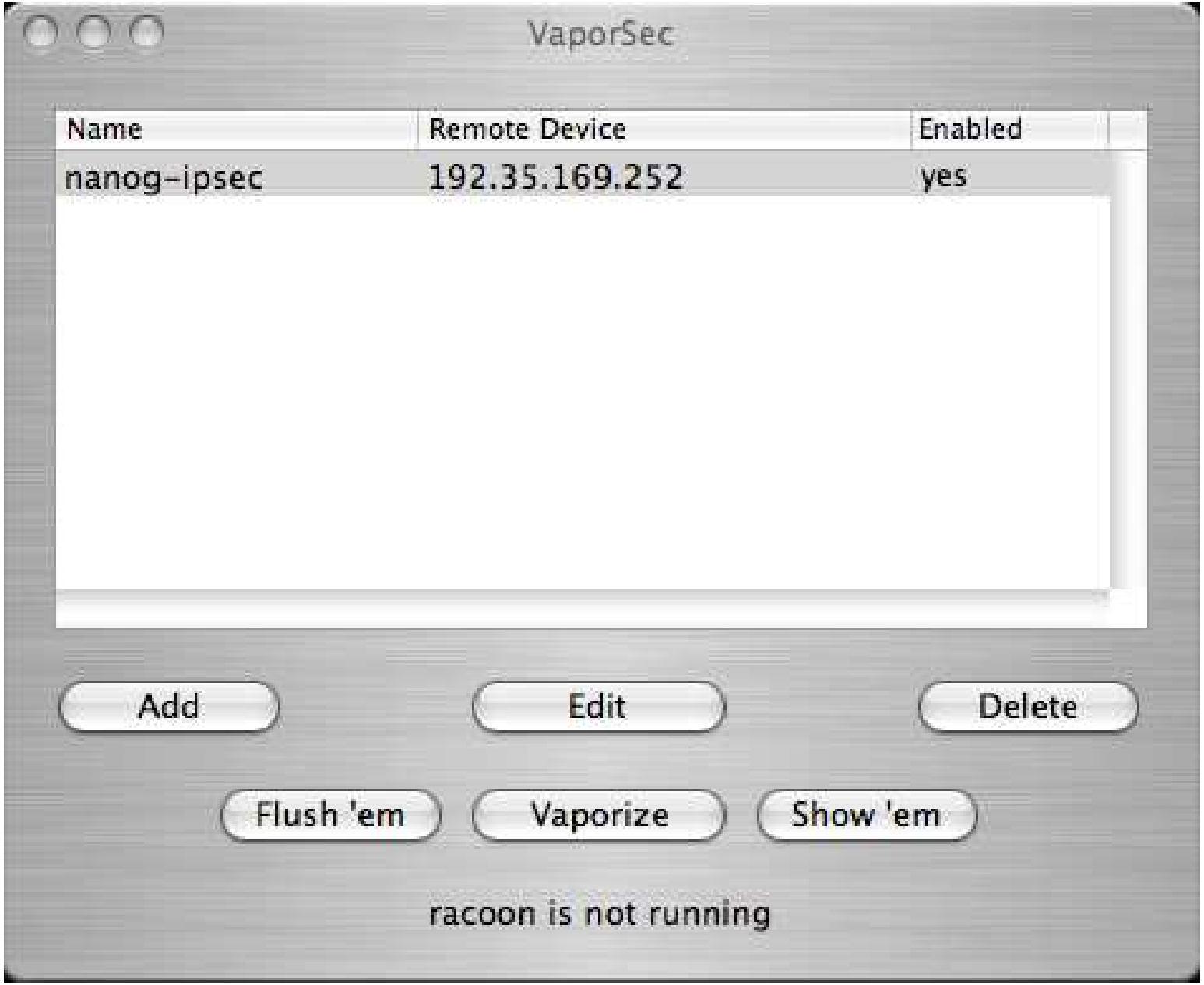
Add IP Alias and Routes

- Execute these commands as root:

```
# ifconfig en1 alias 192.35.169.ZZZ netmask 255.255.255.255
# route add 192.35.169.252 192.35.164.1
# route delete -net 0
# route add -net 0 192.35.169.ZZZ
```

- Use whatever interface name corresponds to your primary IP address.


Connection Name
nanog-ipsec
Remote IPSec device
192.35.169.252
Remote Network
0.0.0.0/0
Local Network Mask
32
Main
Phase 1
Phase 2
ID
Shared Secret
••••
Local IP
192.35.169.ZZZ
Mode
main
Proposal Check
obey
Nonce size
16
Done



Select Vaporize to activate IPsec.

The FreeBSD Way (isakmpd)

Configure your kernel

- If your kernel doesn't already support IPsec, add these two lines to the kernel configuration file:

```
options         IPSEC
options         IPSEC_ESP
```

- Then configure, compile, install the kernel, and reboot.

Install isakmpd

- You can install *isakmpd* from FreeBSD ports:

```
# cd /usr/ports/security/isakmpd
# make
# make install
```

- Or get a binary from:
  `ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-4-stable/security/isakmpd-20030903.tgz`

Download a copy of isakmpd.conf

- Download

  `http://192.35.164.31/ipsec/freebsd-isakmpd/isakmpd.conf.txt`

- Save it as /usr/local/etc/isakmpd/isakmpd.conf
- Make sure it has mode "600" permissions.
- Change 192.35.XXX.YYY to your primary IP address.
- Change 192.35.169.ZZZ to your secondary IP address.
- Your primary address shouldn't change during the meeting, but if it does you'll need to edit the config file and restart.

A Startup Script

```
killall isakmpd
setkey -D ; setkey -DP

ifconfig fxp0 alias 192.35.169.ZZZ netmask 255.255.255.255

route add 192.35.169.252 192.35.164.1
route delete -net 0
route add -net 0 192.35.169.ZZZ

/usr/local/sbin/isakmpd -4
```

Try It Out

- Check syslog for errors.
- In one window, run *tcpdump*:

```
# tcpdump -n
```

- In another window, ping something:

```
# ping 216.66.24.58
```

- You should see:

```
12:34:22.974789 192.35.169.252 > 192.35.XXX.YYY:
    ESP(spi=0x53955a6d,seq=0x2)
12:34:22.975117 192.35.XXX.YYY > 192.35.169.252:
    ESP(spi=0x8e5fbc5d,seq=0x2)
```

The FreeBSD Way (racoon)

Install racoon

- To install *racoon* from ports:

```
# cd /usr/ports/security/racoon
# make
# make install
```

- Note that *racoon* will now start automatically when you reboot.

Download a copy of racoon.conf

- Download
  http://192.35.164.31/ipsec/freebsd-racoon/racoon.conf.txt
- Change 192.35.XXX.YYY to your primary IP address.

Set the pre-shared key

- Put this line in /usr/local/etc/racoon/psk.txt:

```
192.35.169.252  what is your threat model?
```

- chmod 400 /usr/local/etc/racoon/psk.txt

Create the IPsec policy

- Add these lines to /etc/ipsec.conf

```
spdadd 0.0.0.0/0 192.35.169.ZZZ/32 any -P in ipsec
 esp/tunnel/192.35.169.252-192.35.XXX.YYY/require;
spdadd 192.35.169.ZZZ/32 0.0.0.0/0 any -P out ipsec
 esp/tunnel/192.35.XXX.YYY-192.35.169.252/require;
```

A Startup Script

```
killall racoon
setkey -DP ; setkey -D

ifconfig fxp0 alias 192.35.169.ZZZ netmask 255.255.255.255

route add 192.35.169.252 192.35.164.1
route delete -net 0
route add -net 0 192.35.169.ZZZ

setkey -f /etc/ipsec.conf
/usr/local/sbin/racoon
```

Notes on racoon

- Raccon does not establish the security association until there is traffic to send.
- In my experience, *isakmpd* worked better than *racoon* as an IKE client, but YMMV.

The Linux Way

Kernel Configuration

- Under Networking options:

```
<*> IP Security Protocol (FreeS/WAN IPSEC)
--- IPSec options (FreeS/WAN)
[*]    IPSEC: IP-in-IP encapsulation (tunnel mode)
[*]    IPSEC: Authentication Header
[*]       HMAC-MD5 authentication algorithm
[*]       HMAC-SHA1 authentication algorithm
[*]    IPSEC: Encapsulating Security Payload
[*]       3DES encryption algorithm
[*]    IPSEC Modular Extensions
```

Install FreeS/WAN

- Use your Linux distribution's favorite technique for installing packages: rpm, apt-get, emerge, etc.
- Or http://www.freeswan.org/download.html
- Or http://www.openswan.org/code/
- Includes kernel patches so you probably need to recompile your kernel.

Download an ipsec.conf Template

- `http://192.35.164.31/ipsec/linux-freeswan/ipsec.conf.txt`
- Save it as /etc/ipsec/ipsec.conf
- Change 192.35.XXX.YYY to your primary address
- Change 192.35.169.ZZZ to your secondary address

Set the pre-shared key

- Put this line in /etc/ipsec/ipsec.secrets:

```
192.35.XXX.YYY 192.35.169.252: PSK "what is your threat model?"
```

Startup Script

```
encrypt_local=no        # or yes
ifconfig eth0:0 192.35.169.ZZZ netmask 255.255.255.255

iptables -t nat --flush
iptables -t nat -A POSTROUTING --destination 192.35.169.252 -j ACCEPT
if test $encrypt_local = "no" ; then
  iptables -t nat -A POSTROUTING --destination 192.35.164.0/22 -j ACCEPT
fi
iptables -t nat -A POSTROUTING -p ! 50 -j SNAT --to-source 192.35.169.ZZZ

route add 192.35.169.252 gw 192.35.164.1
/usr/sbin/ipsec setup --start

if test $encrypt_local = "yes" ; then
  sleep 5 ; route delete -net 192.35.164.0/22 eth0
fi
```

Try It Out

- Execute the script from the previous slide or reboot your computer.
- Check syslog for errors.
- Run *tcpdump* and *ping* to see if it works.
- Check for security associations by running:

```
# ipsec look
```

Final Thoughts

MTU Issues

- Packets encapsulated inside IPsec are going to get bigger and may exceed the Ethernet MTU.
- To check for fragmentation, run *tcpdump* during a large data transfer.
- You may want or need to manually lower the MTU on your Ethernet interface to something like 1460 bytes.

Suspending your Laptop

- Sometimes suspending and waking a laptop causes a "DHCP refresh."
- This might delete your secondary/alias address and change your default route.

Key Lifetimes

- Key lifetimes are configurable, but we are generally using default values.
- Sometimes observe short periods of time when IPsec traffic is suspended as keys are renegotiated.
- Longer key lifetimes mean fewer renegotiations, at the expense of weaker security.

The End