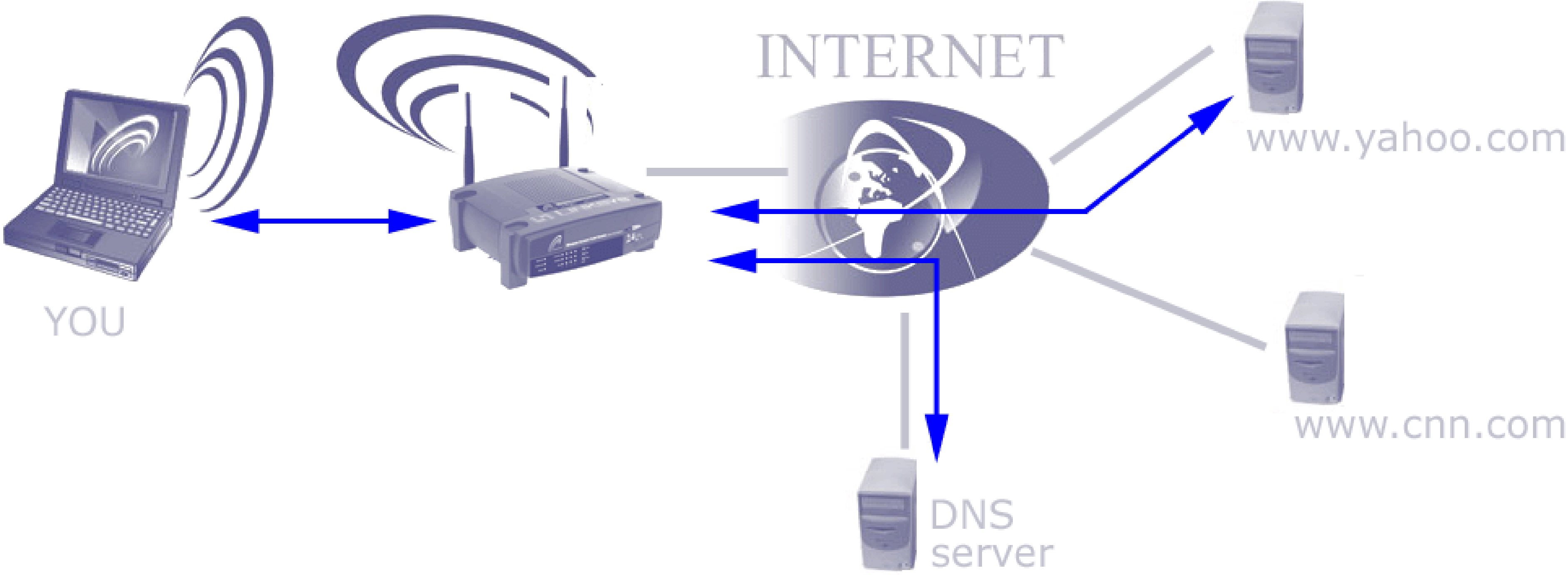
Defending Yourself Against The Wily Wireless Hacker

Brian S. Walden
NYCWireless Presentation
October 27, 2004

http://wifidefense.cuzuco.com/

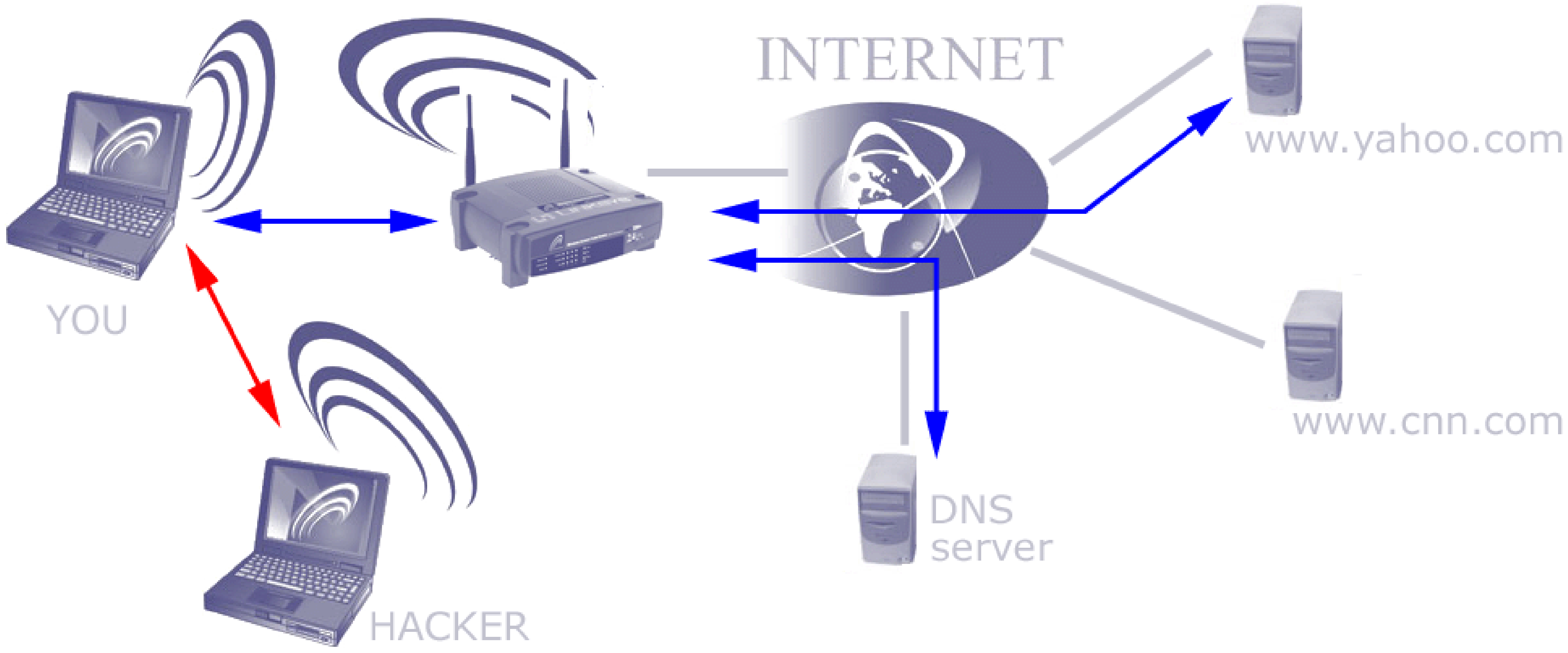
What You Expect



Common Hacker Techniques

- Direct Break-In
- Man-In-The-Middle
  - DNS Spoofing
  - Rogue Access Points
  - Connection Hijacking

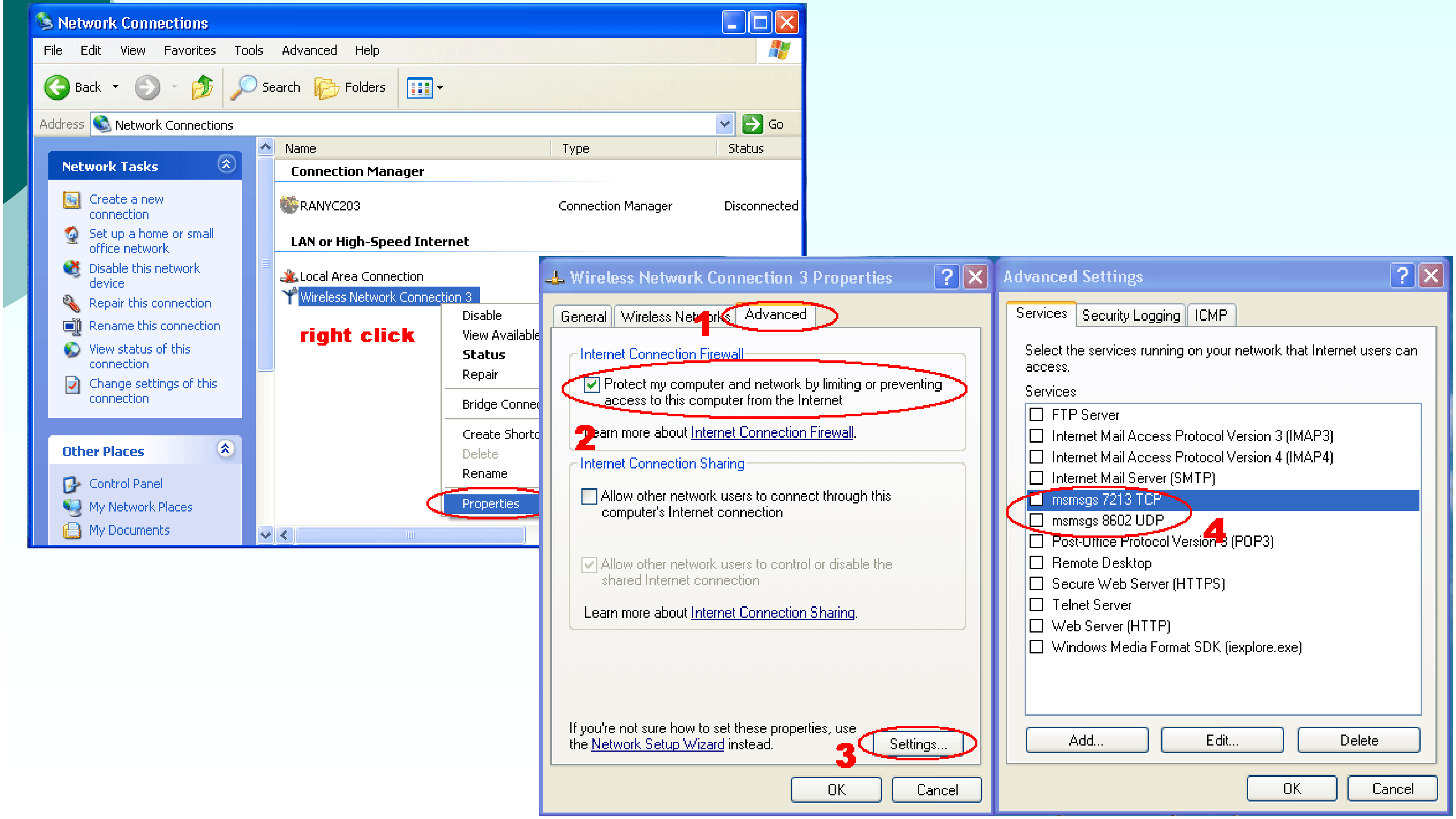
Direct Break-In



Direct Break-In Defense

- Windows
  - Built In Firewall in XP
  - Third Party Software Firewall
    - Kerio Personal Firewall
    - ZoneAlarm
    - Sygate Personal Firewall
- Linux/UNIX
  - Turn off unused services
  - TCP wrappers
  - IPfilter (Solaris, BSDs)
  - IPtables (Linux)

XP Firewall (pre SP2)



Internet Connection Firewall

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

☐ Allow other network users to connect through this computer's Internet connection

☑ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

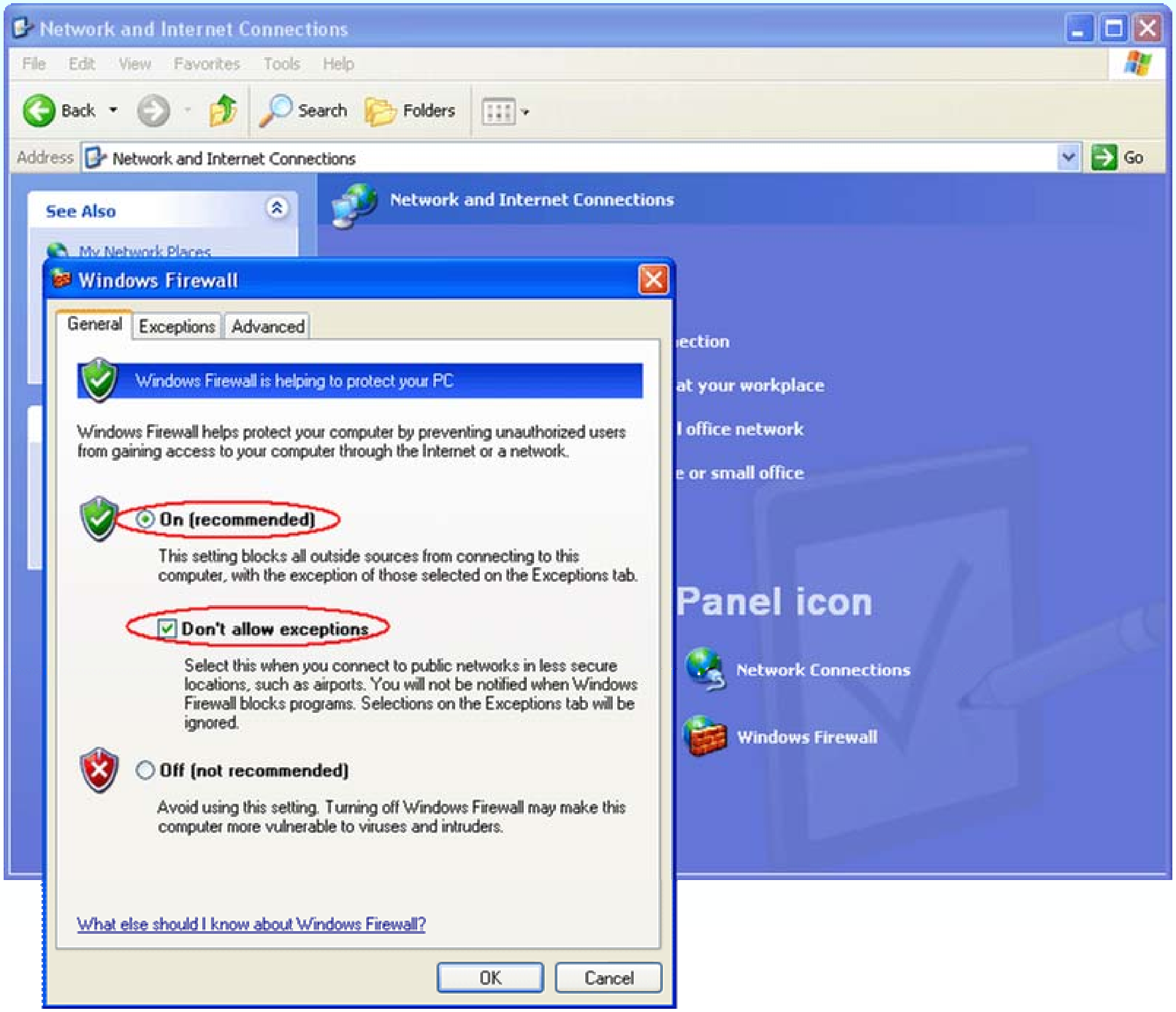
If you're not sure how to set these properties, use the Network Setup Wizard instead.

Select the services running on your network that Internet users can access.

Services

- ☐ FTP Server
- ☐ Internet Mail Access Protocol Version 3 (IMAP3)
- ☐ Internet Mail Access Protocol Version 4 (IMAP4)
- ☐ Internet Mail Server (SMTP)
- ☐ msmsgs 7213 TCP
- ☐ msmsgs 8602 UDP
- ☐ Post-Office Protocol Version 3 (POP3)
- ☐ Remote Desktop
- ☐ Secure Web Server (HTTPS)
- ☐ Telnet Server
- ☐ Web Server (HTTP)
- ☐ Windows Media Format SDK (iexplore.exe)

XP SP2 Firewall



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

☑ Don't allow exceptions

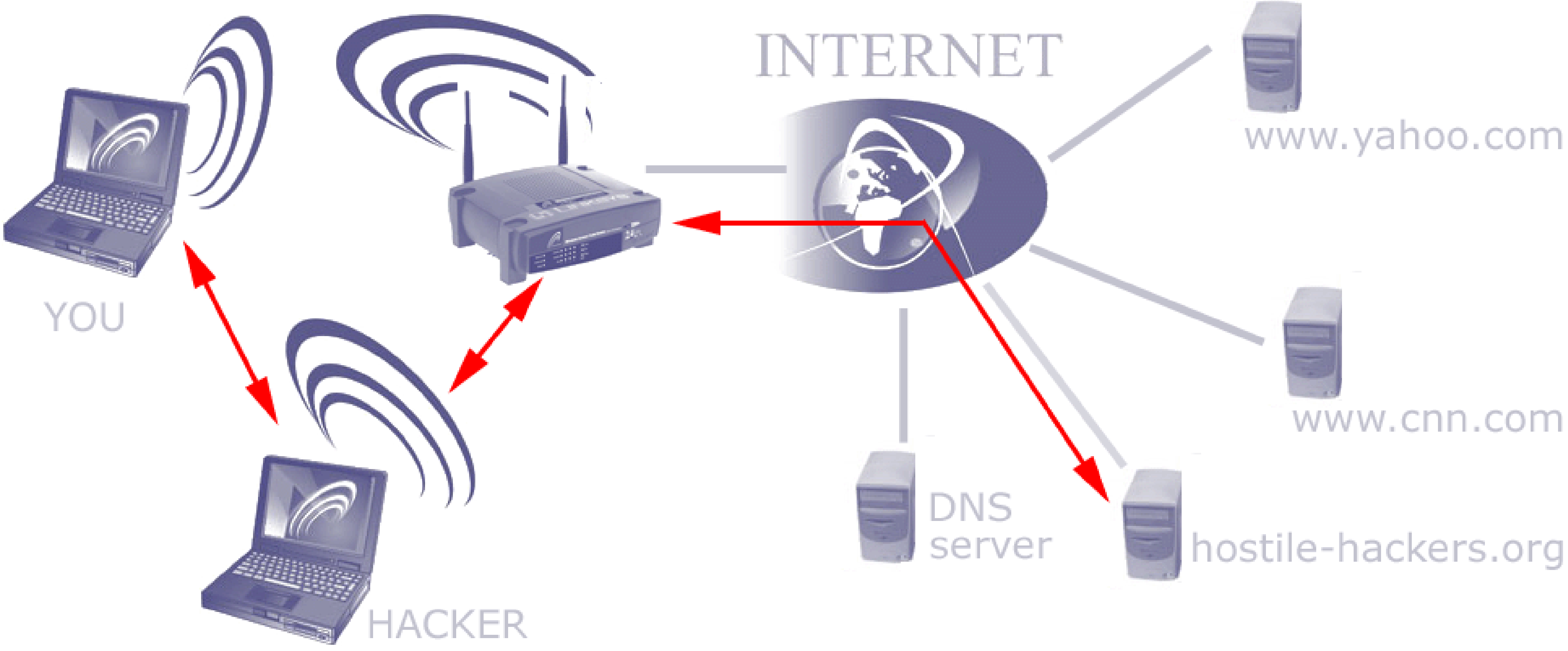
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

Man-In-The-Middle



Man-In-The-Middle Defense

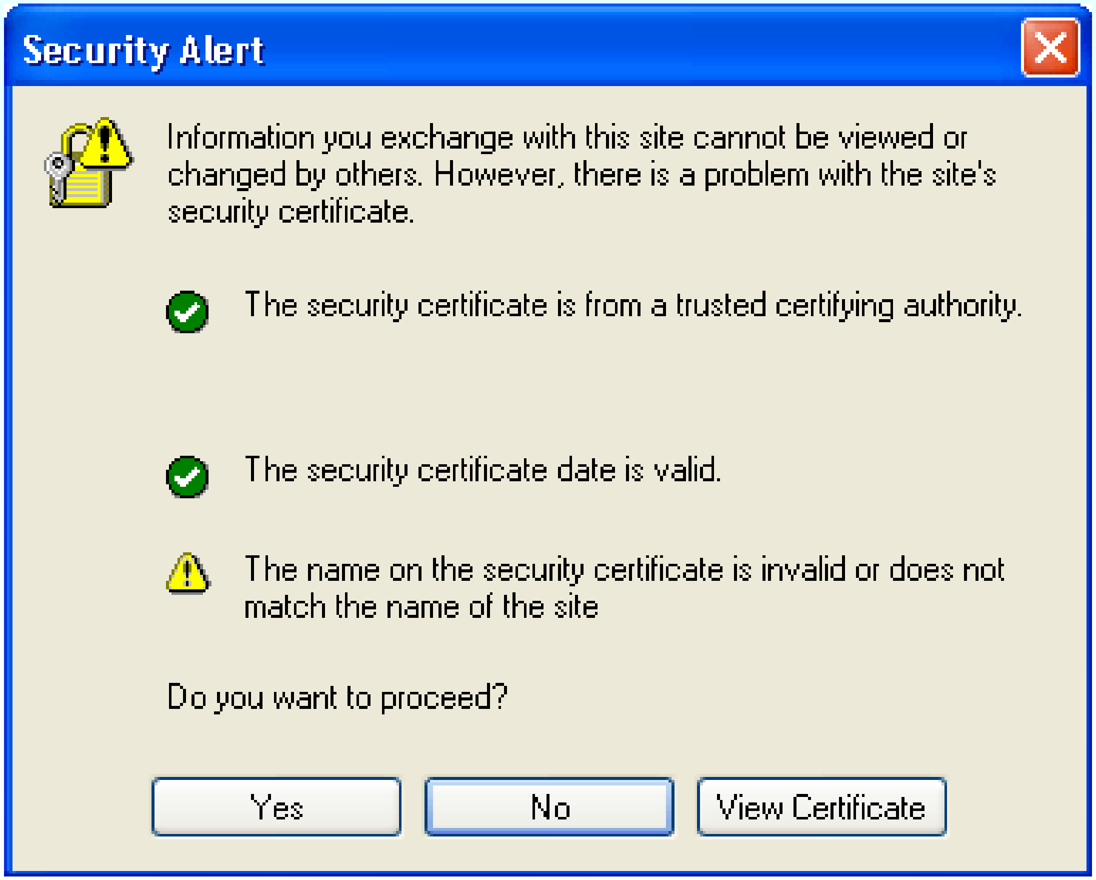
Everything in SSL (check that certificate)

- www.megaproxy.com

Use some sort of Virtual Private Networking (VPN)

- Creates an encrypted tunnel between you and and some other server
  - ○ Encryption hides what sites you are accessing
  - ○ Encryption is tamper resistant
- Most often used for remote access

SSL: the Certificate Check Should Alert You to Tampering



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

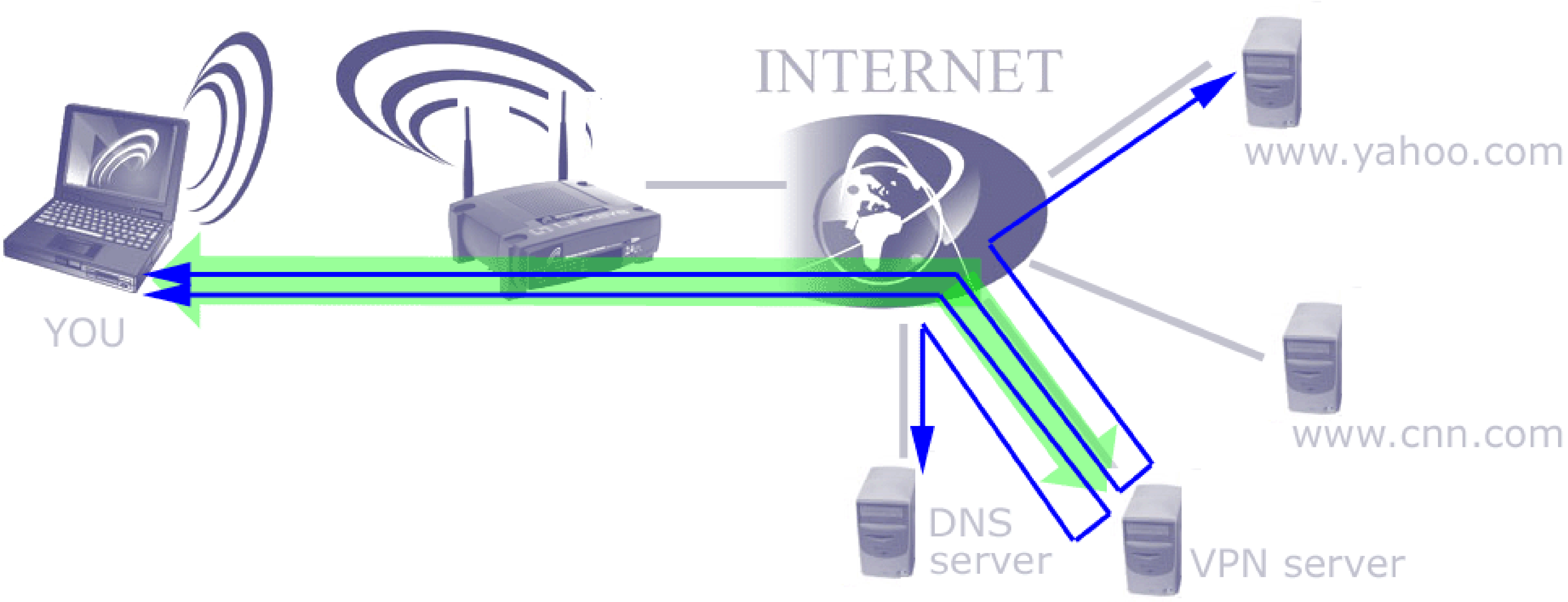
✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

How VPN changes access



How do I get a VPN?

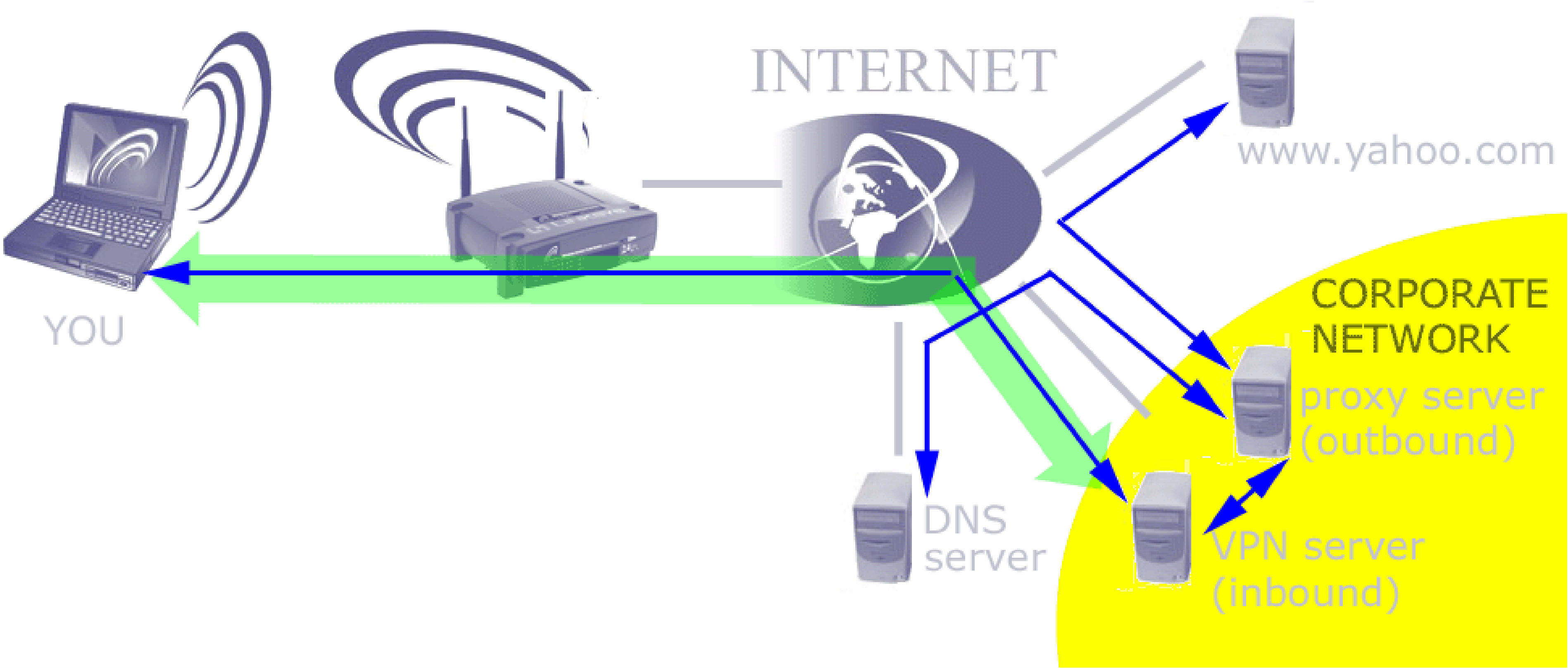
- Have an employer that supplies a remote access solution
- Roll Your Own – Do It Yourself

  It’s not difficult

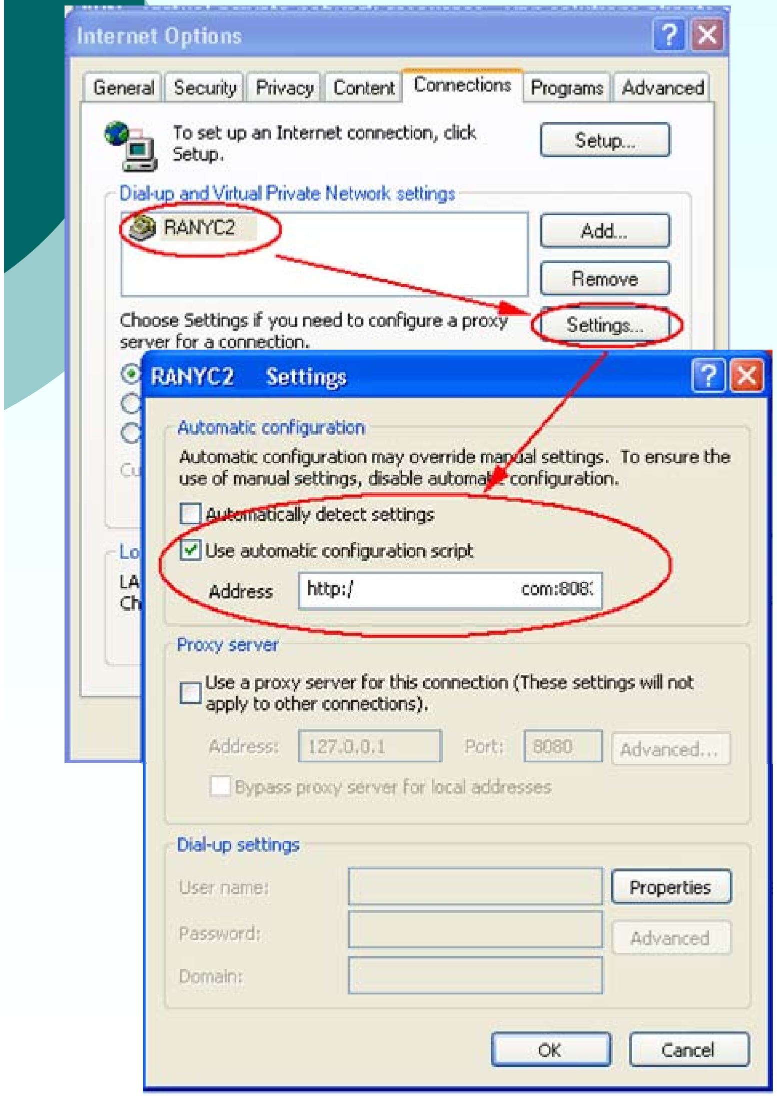
An Employer Supplied VPN

- Pros
  - They did most of the work and/or paid for the solution
  - You might get support
  - May protect you from questionable websites
- Cons
  - May only be available for Windows hosts
  - You’re not really on the internet anymore
  - May restricted you from any number of websites
  - Privacy: employer might record all sites you access
  - Policy: employer might disallow this type of use

Corporate VPN & PROXY



Need to use employers proxies



Internet Options

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

RANYC2

Choose Settings if you need to configure a proxy server for a connection.

RANYC2 Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☑ Use automatic configuration script

Address: http:/ com:808(

Proxy server

☐ Use a proxy server for this connection (These settings will not apply to other connections).

Address: 127.0.0.1 Port: 8080

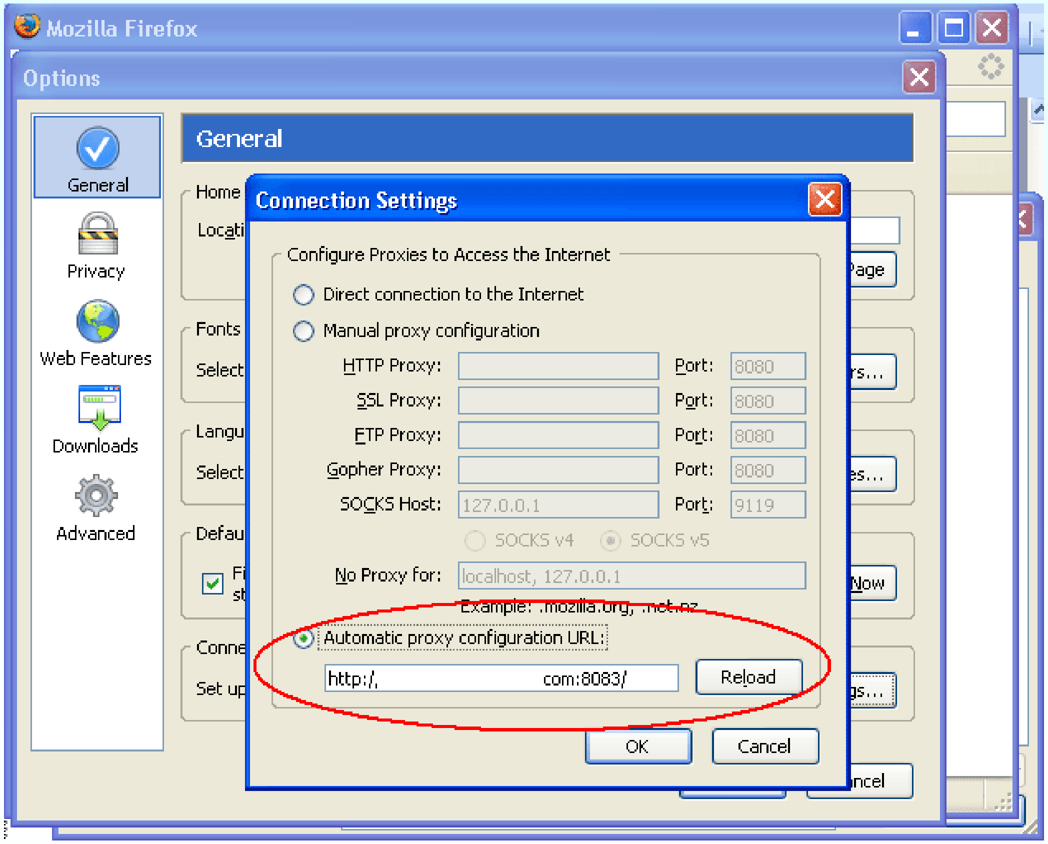
☐ Bypass proxy server for local addresses

Dial-up settings

User name:

Password:

Domain:



Mozilla Firefox

Options

Connection Settings

Configure Proxies to Access the Internet

○ Direct connection to the Internet

○ Manual proxy configuration

HTTP Proxy: Port: 8080

SSL Proxy: Port: 8080

FTP Proxy: Port: 8080

Gopher Proxy: Port: 8080

SOCKS Host: 127.0.0.1 Port: 9119

○ SOCKS v4 ● SOCKS v5

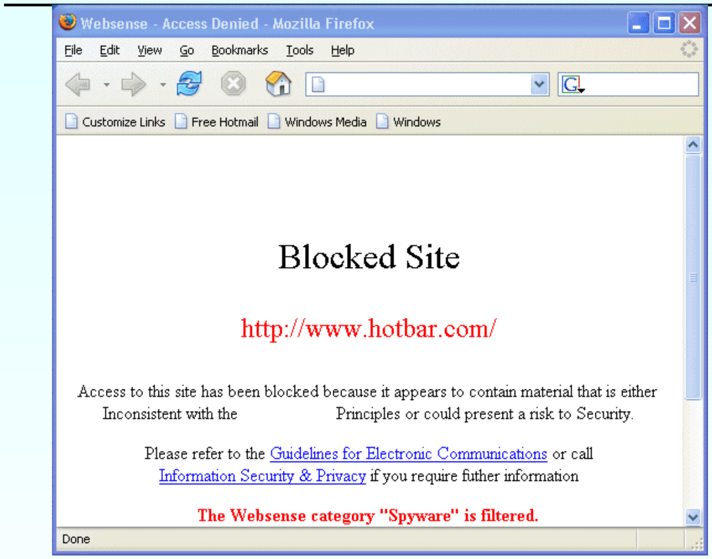
No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz

● Automatic proxy configuration URL:

http:/, com:8083/

Employer Filtering


Websense - Access Denied - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Customize Links Free Hotmail Windows Media Windows
Done

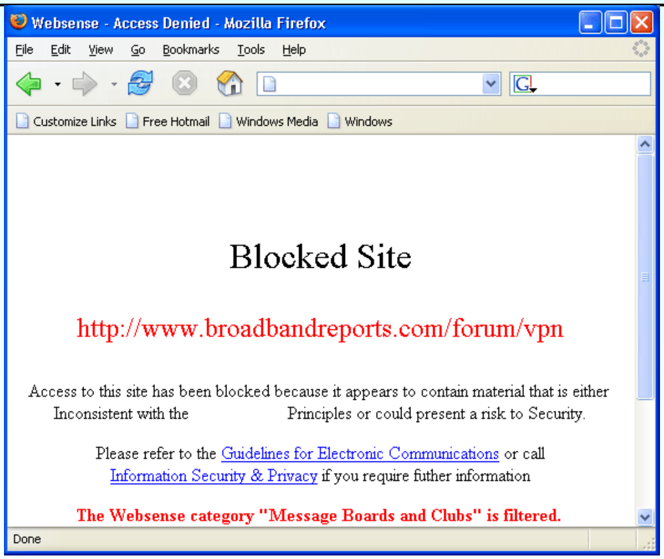
Blocked Site

http://www.hotbar.com/

Access to this site has been blocked because it appears to contain material that is either Inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require futher information

The Websense category "Spyware" is filtered.


Websense - Access Denied - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Customize Links Free Hotmail Windows Media Windows
Done

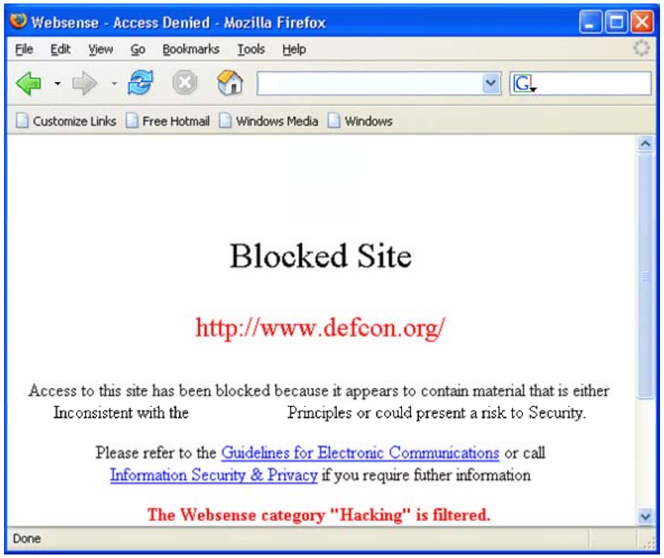
Blocked Site

http://www.broadbandreports.com/forum/vpn

Access to this site has been blocked because it appears to contain material that is either Inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require futher information

The Websense category "Message Boards and Clubs" is filtered.


Websense - Access Denied - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Customize Links Free Hotmail Windows Media Windows
Done

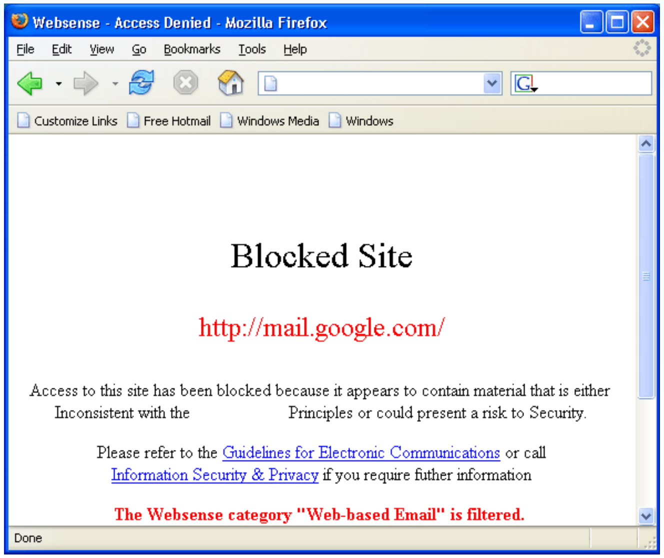
Blocked Site

http://www.defcon.org/

Access to this site has been blocked because it appears to contain material that is either Inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require futher information

The Websense category "Hacking" is filtered.


Websense - Access Denied - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Customize Links Free Hotmail Windows Media Windows
Done

Blocked Site

http://mail.google.com/

Access to this site has been blocked because it appears to contain material that is either Inconsistent with the Principles or could present a risk to Security.

Please refer to the Guidelines for Electronic Communications or call Information Security & Privacy if you require futher information

The Websense category "Web-based Email" is filtered.

Roll Your Own – Do It Yourself

Easier Than You Think

- Microsoft VPN
- Use SSH tunnels
  - Works under Windows
  - Works under UNIX/Linux
  - Works under Macs
- Requires another computer you trust somewhere else on the Internet
  - At your home
  - Collocated at a hosting facility or ISP
  - Purchase a shell account

Microsoft VPN

- Windows has a built in VPN, Microsoft's PPTP
- It seems to have some security flaws
  - http://www.schneier.com/pptp-faq.html
  - http://www.schneier.com/paper-pptpv2.html
- UNIX/Linux client: PPTP Client
- UNIX/Linux server: Poptop
- Cisco routers and firewalls can talk it too
- Uses a modified GRE/IP (not TCP/IP)
- If you only want to secure web browsing there's an easier way that's more secure

VPN with SSH

- SSH is Secure SHell
  - Available on just about every platform
  - Commonly considered “encrypted telnet”
  - But has much more
    - Has port tunneling capability built in
    - Has a SOCKS server built in
  - There’s two versions: 1 and 2
    - Use version 2
    - Use a newer server, there were some flaws in older implementations
  - Easy to use
  - Only uses a single TCP/IP port (default is 22)
  - No problems with Network Address Translation (NAT)

SSH Software

- Client
  - SSH
    - Comes standard on UNIX/Linux/Mac OSX
    - Free Windows clients: PuTTY
      - Easy download, no install (no admin rights needed)
- Server
  - SSHD on a remote host
    - Comes standard on UNIX/Linux
    - Free Widows server: opensshd
      - Easy download and install

Remote is UNIX/Linux

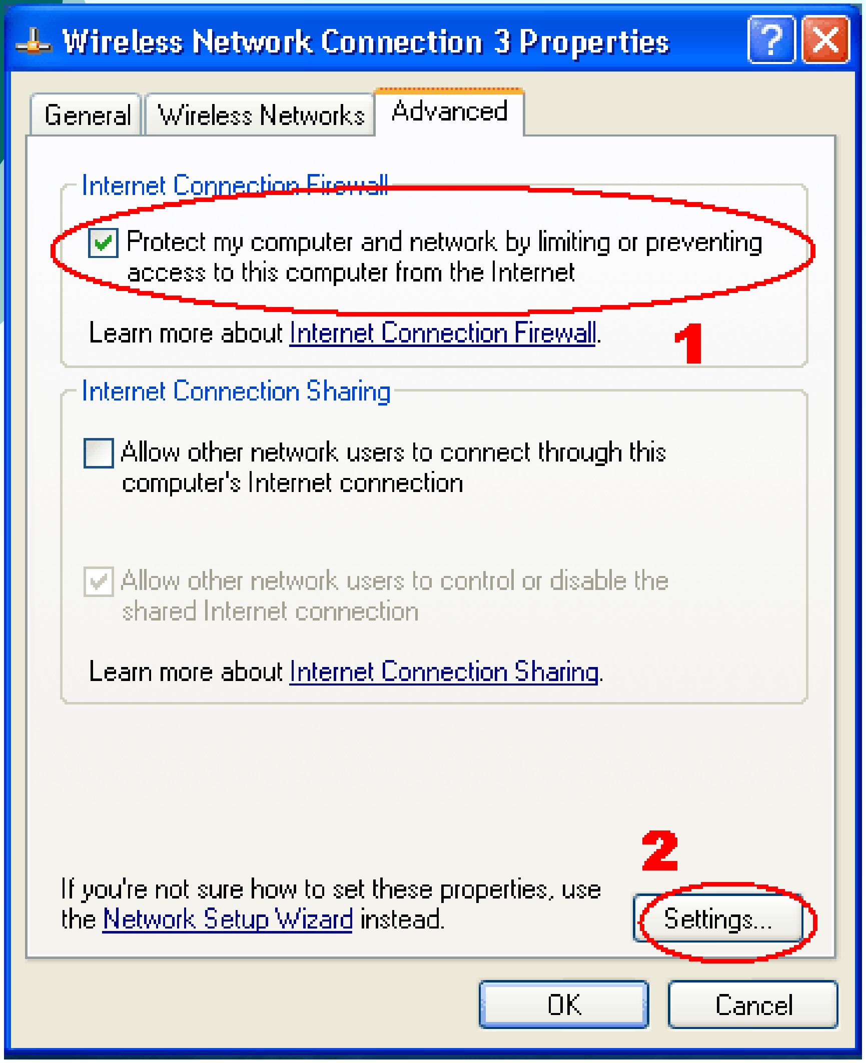
- SSHD is all ready there, just use it
- Use an any account you can log into (root account not recommended)
- Buy a shell account that allows you to ssh into (e.g. panix offers one at $10/month or $100/year)

Remote is Windows

- Download the OpenSSH for
  http://sshwindows.sourceforge.net/
- Install and start it
  - net start openssd
- Or if you currently use cygwin (ignore if you don't know what this is)
  - Download these packages -
    - **openssh**
    - **cygrunsrv**
    - **perl (not need for ssh, but we'll use it later)**
  - Configure it with ssh-host-config in a cygwin shell
    - **Answer privilege separation "no"**
    - **Answer CYGWIN= "ntsec tty"**
  - Start service with cygrunsrv –S sshd
- Windows user account MUST have a password

Remote is Windows XP (pre SP2)

Accept connections on port 22 (part 1)



Wireless Network Connection 3 Properties

General | Wireless Networks | Advanced

Internet Connection Firewall

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

1

Internet Connection Sharing

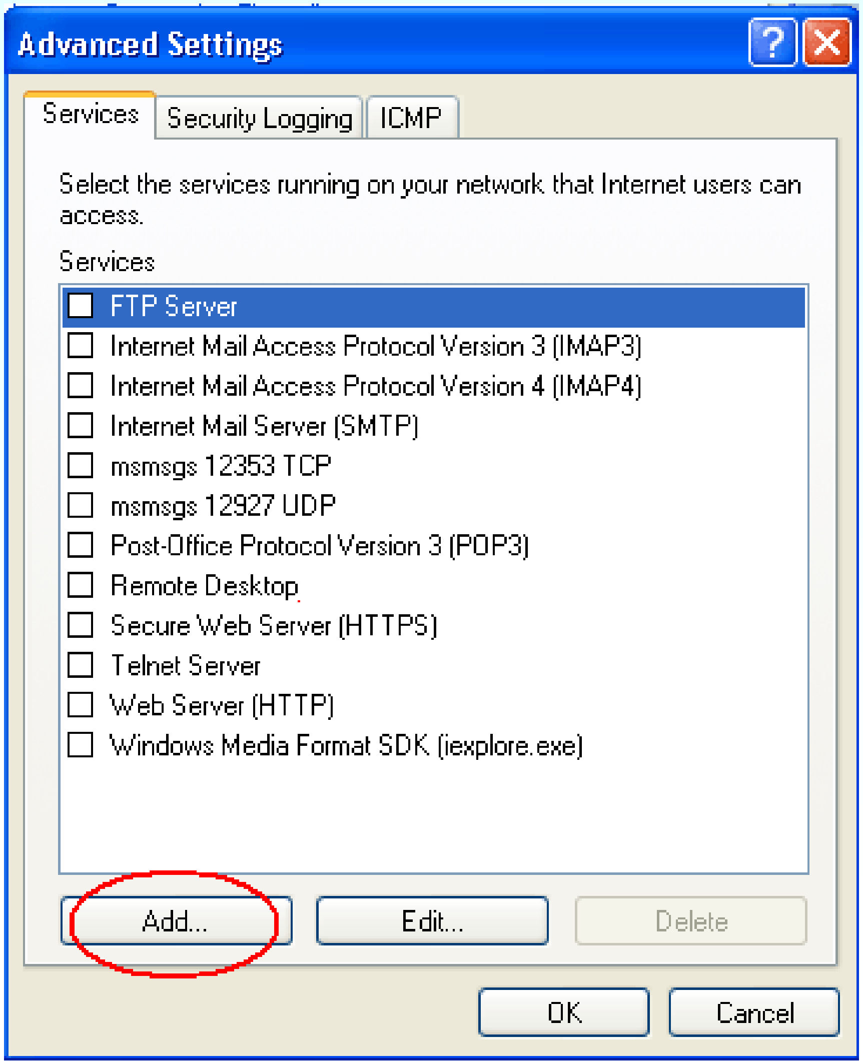
□ Allow other network users to connect through this computer's Internet connection

☑ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

2

If you're not sure how to set these properties, use the Network Setup Wizard instead.



Advanced Settings

Services | Security Logging | ICMP

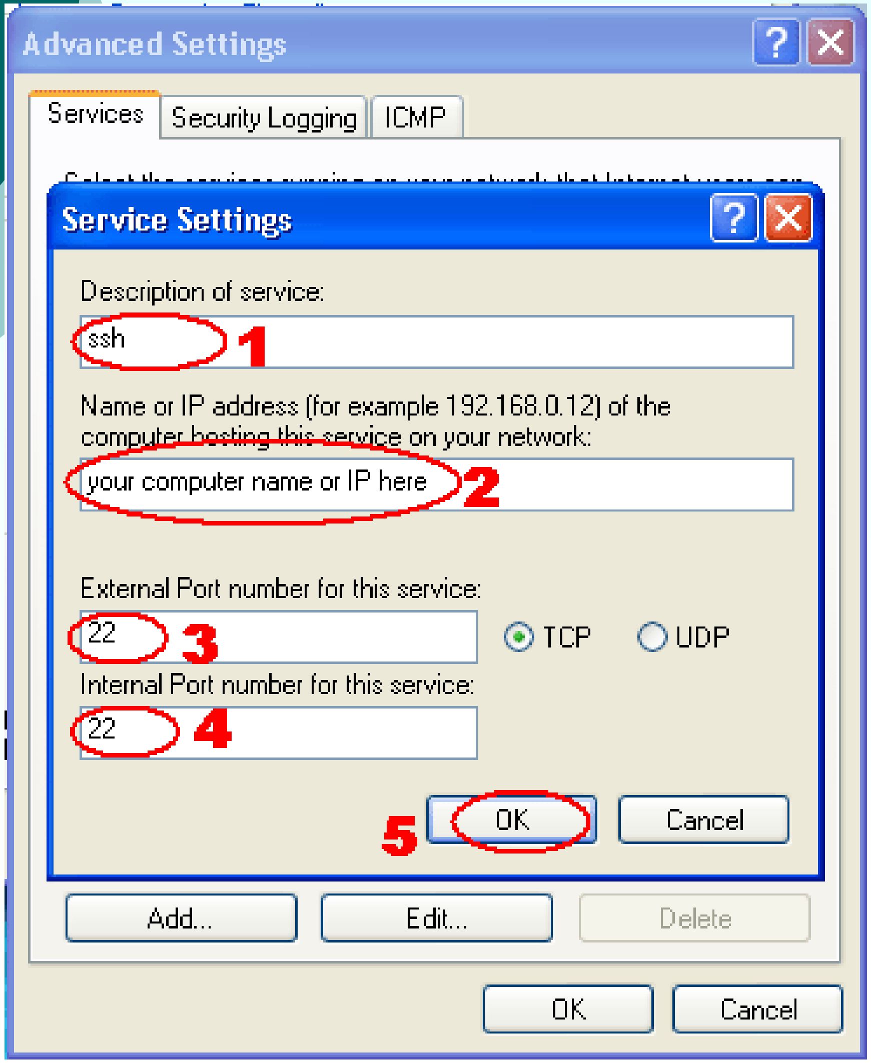
Select the services running on your network that Internet users can access.

Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ msmsgs 12353 TCP
- □ msmsgs 12927 UDP
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)
- □ Windows Media Format SDK (iexplore.exe)

Remote is Windows XP (pre SP2)

Accept connections on port 22 (part 2)



Description of service:

ssh 1

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:

your computer name or IP here 2

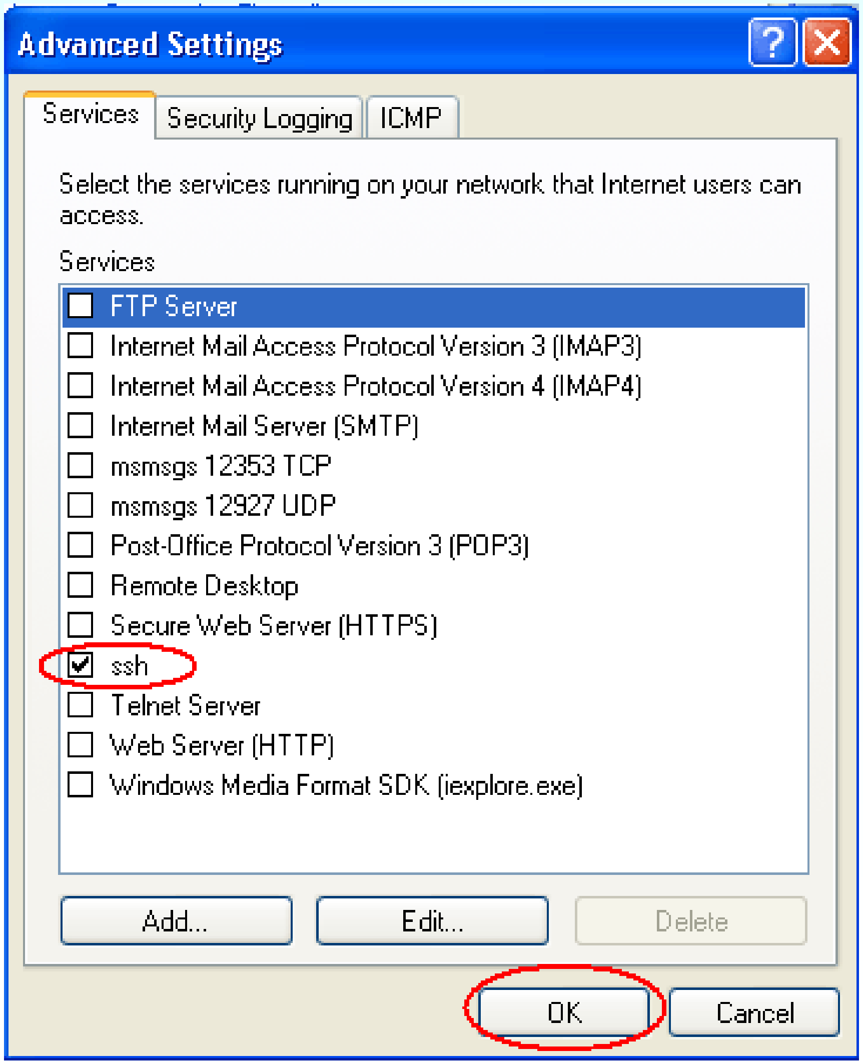
External Port number for this service:

22 3 ● TCP ○ UDP

Internal Port number for this service:

22 4

5 OK



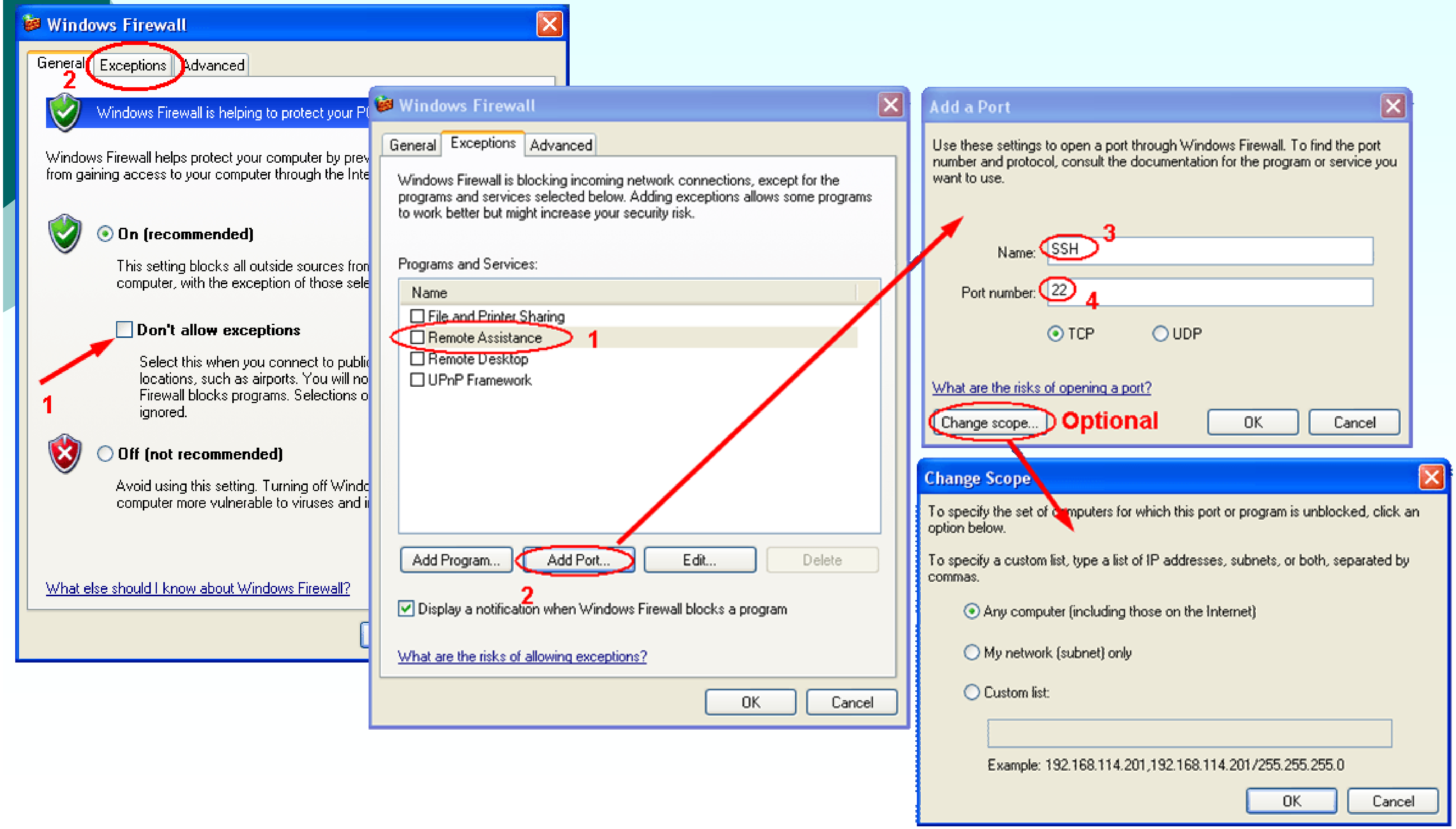
Select the services running on your network that Internet users can access.

Services

- ☐ FTP Server
- ☐ Internet Mail Access Protocol Version 3 (IMAP3)
- ☐ Internet Mail Access Protocol Version 4 (IMAP4)
- ☐ Internet Mail Server (SMTP)
- ☐ msmsgs 12353 TCP
- ☐ msmsgs 12927 UDP
- ☐ Post-Office Protocol Version 3 (POP3)
- ☐ Remote Desktop
- ☐ Secure Web Server (HTTPS)
- ☑ ssh
- ☐ Telnet Server
- ☐ Web Server (HTTP)
- ☐ Windows Media Format SDK (iexplore.exe)

Remote is Windows XP SP2

Accept connections on port 22



Windows Firewall is helping to protect your P

Windows Firewall helps protect your computer by prev from gaining access to your computer through the Inte

● On (recommended)

This setting blocks all outside sources fron computer, with the exception of those sele

□ Don't allow exceptions

Select this when you connect to publi locations, such as airports. You will no Firewall blocks programs. Selections o ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windo computer more vulnerable to viruses and i

What else should I know about Windows Firewall?

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name
□ File and Printer Sharing
□ Remote Assistance
□ Remote Desktop
□ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: SSH

Port number: 22

● TCP ○ UDP

What are the risks of opening a port?

To specify the set of computers for which this port or program is unblocked, click an option below.

To specify a custom list, type a list of IP addresses, subnets, or both, separated by commas.

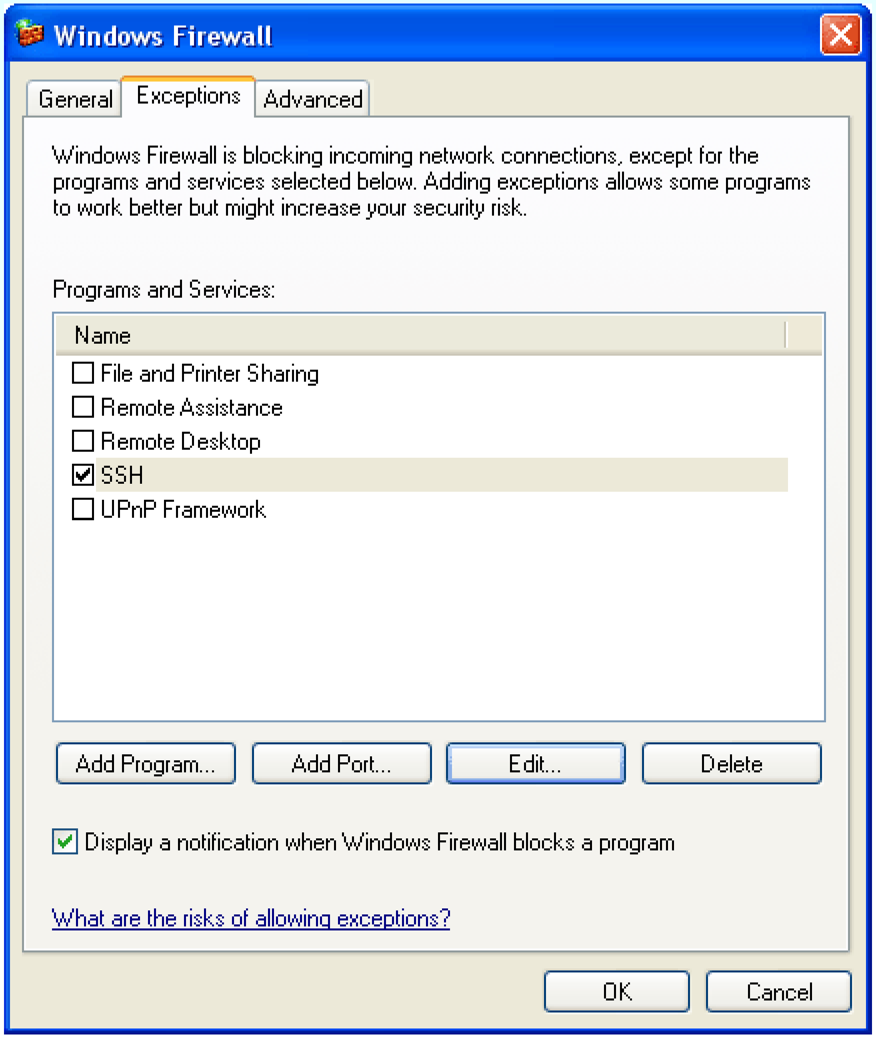
● Any computer (including those on the Internet)

○ My network (subnet) only

○ Custom list:

Example: 192.168.114.201,192.168.114.201/255.255.255.0

Remote is Windows XP SP2
Accept connections on port 22



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

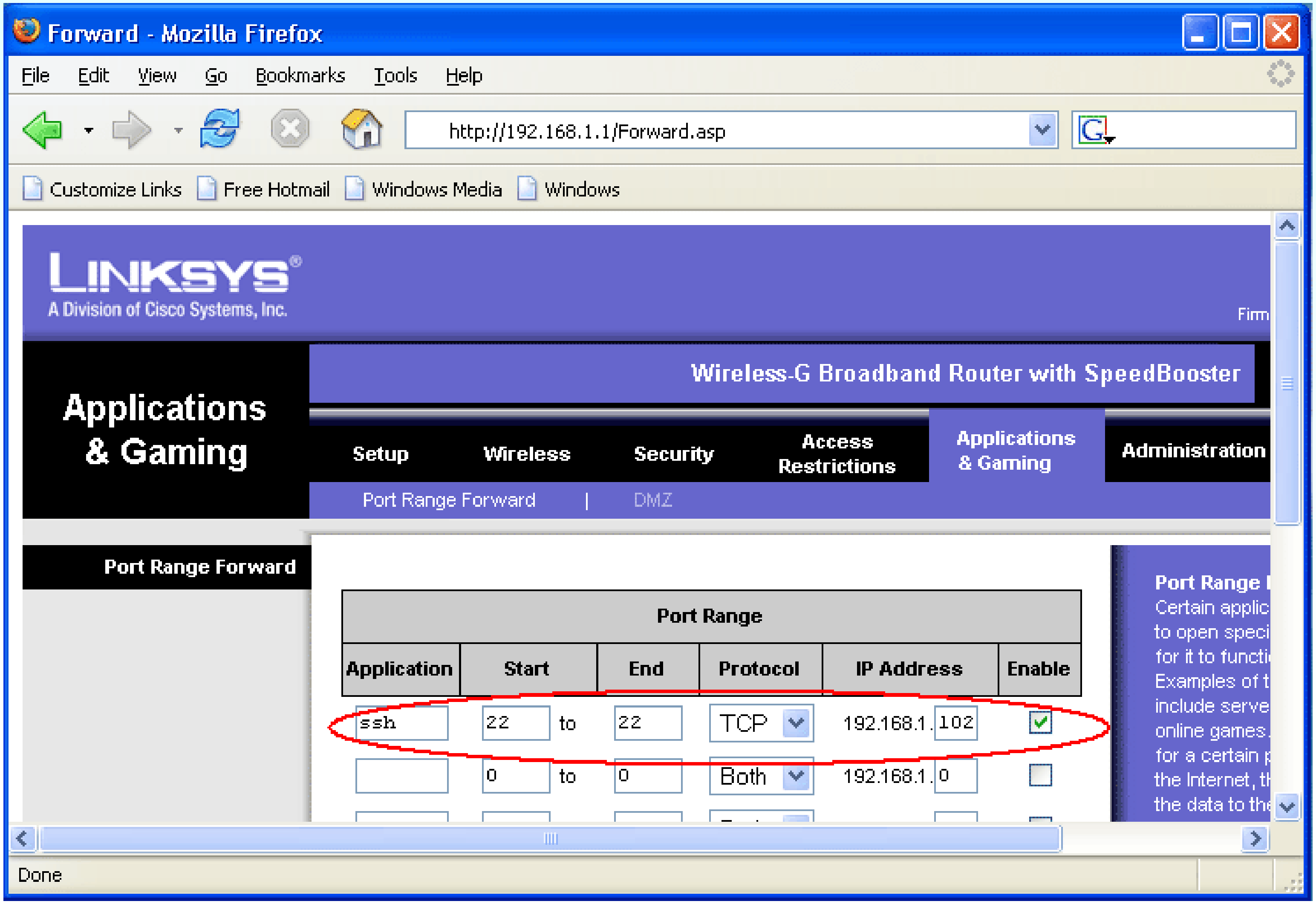
Name
□ File and Printer Sharing
□ Remote Assistance
□ Remote Desktop
☑ SSH
□ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Open Inbound Port 22 on External Firewalls

Home users: remember to open up and map port 22 on your router/firewall to your internal server



http://192.168.1.1/Forward.asp

Port Range						
Application	Start		End	Protocol	IP Address	Enable
ssh	22	to	22	TCP	192.168.1.102	☑
	0	to	0	Both	192.168.1.0	□

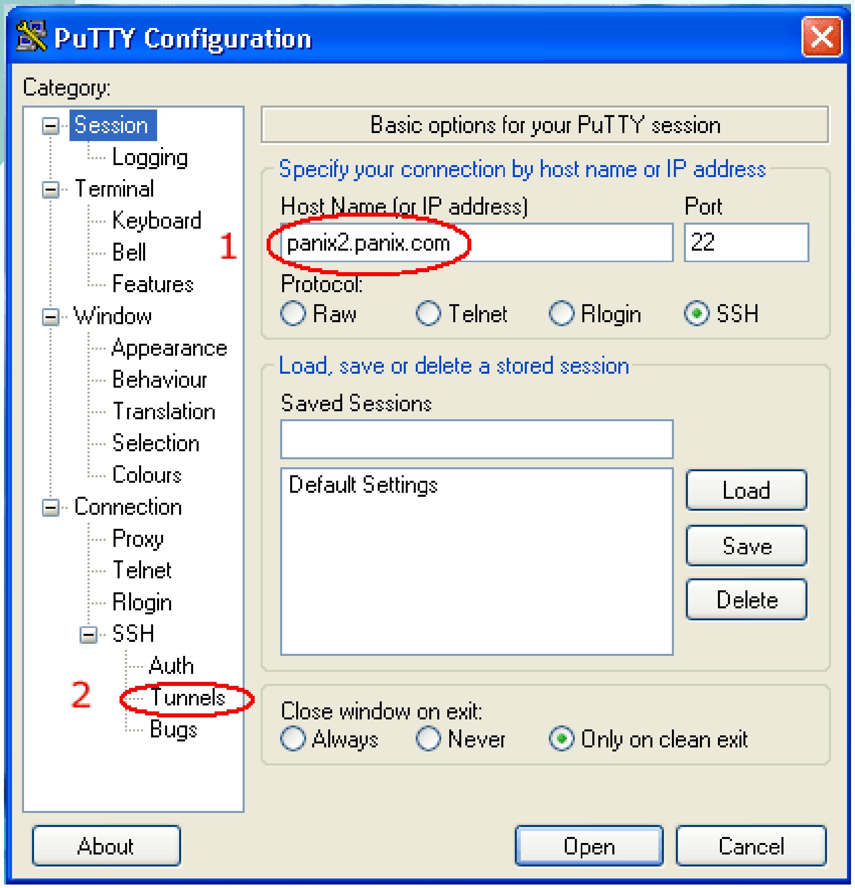
Port Range I
Certain applic
to open speci
for it to functi
Examples of t
include serve
online games.
for a certain p
the Internet, th
the data to the

Client: Start SSH with SOCKS

- UNIX/Linux:

```
$ ssh –D9119 user@remote-host.com
```

- Windows: PuTTY



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): panix2.panix.com

Port: 22

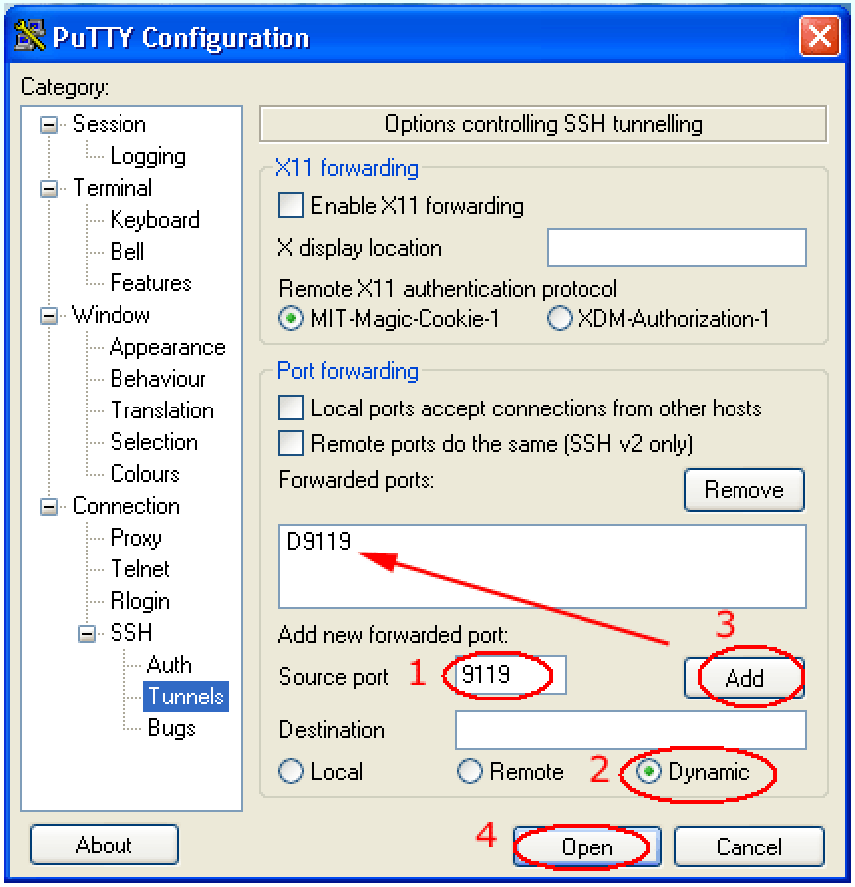
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



PuTTY Configuration

Category:

Options controlling SSH tunnelling

X11 forwarding

□ Enable X11 forwarding

X display location

Remote X11 authentication protocol: ● MIT-Magic-Cookie-1 ○ XDM-Authorization-1

Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH v2 only)

Forwarded ports: D9119

Add new forwarded port:

Source port: 9119

Destination

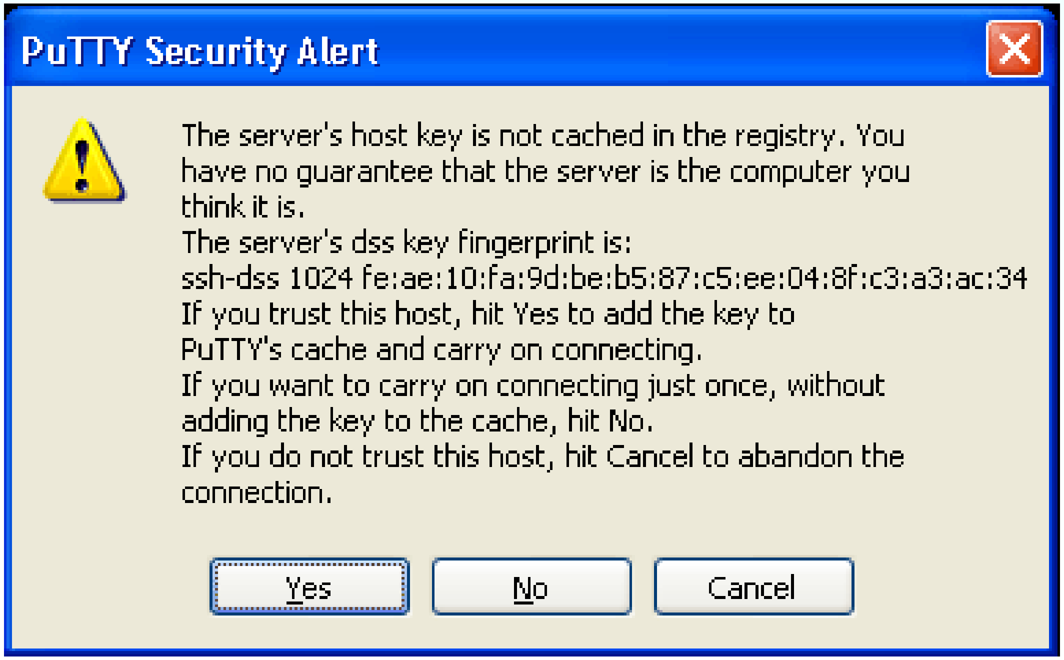
○ Local ○ Remote ● Dynamic

Have the SSH key before hand

- First time use will prime key on client side
- UNIX/Linux/Cygwin –

```
$ ssh cuzuco.com
The authenticity of host 'cuzuco.com (196.12.190.248)' can't be established.
DSA key fingerprint is 71:87:41:2c:f7:c8:82:96:95:12:74:c7:79:ab:a1:7d.
Are you sure you want to continue connecting (yes/no)?
```

- Windows (PuTTY) –



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's dss key fingerprint is:
ssh-dss 1024 fe:ae:10:fa:9d:be:b5:87:c5:ee:04:8f:c3:a3:ac:34
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

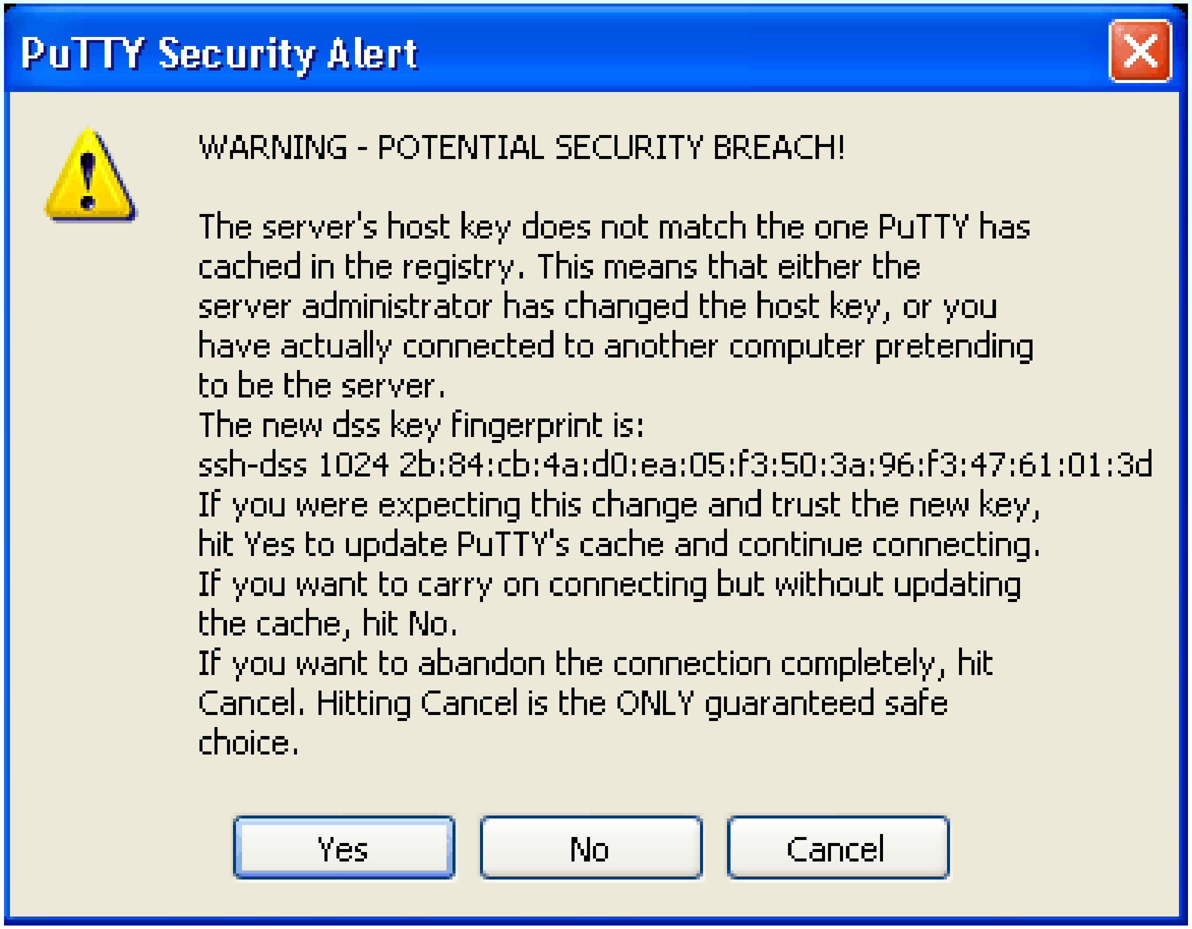
Server key is different (probable attack)

- UNIX/Linux/Cygwin –

```
$ ssh cuzuco.com
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-
   middle attack)!
It is also possible that the DSA host key has just been
   changed.
The fingerprint for the DSA key sent by the remote host is
2b:84:cb:4a:d0:ea:05:f3:50:3a:96:f3:47:61:01:3d.
Please contact your system administrator.
Add correct host key in /net/u/16/b/bsw/.ssh/known_hosts to
   get rid of this message.
Offending key in /net/u/16/b/bsw/.ssh/known_hosts:90
DSA host key for cuzuco.com has changed and you have requested
   strict checking.
Host key verification failed.
```

Server key is different (probable attack)

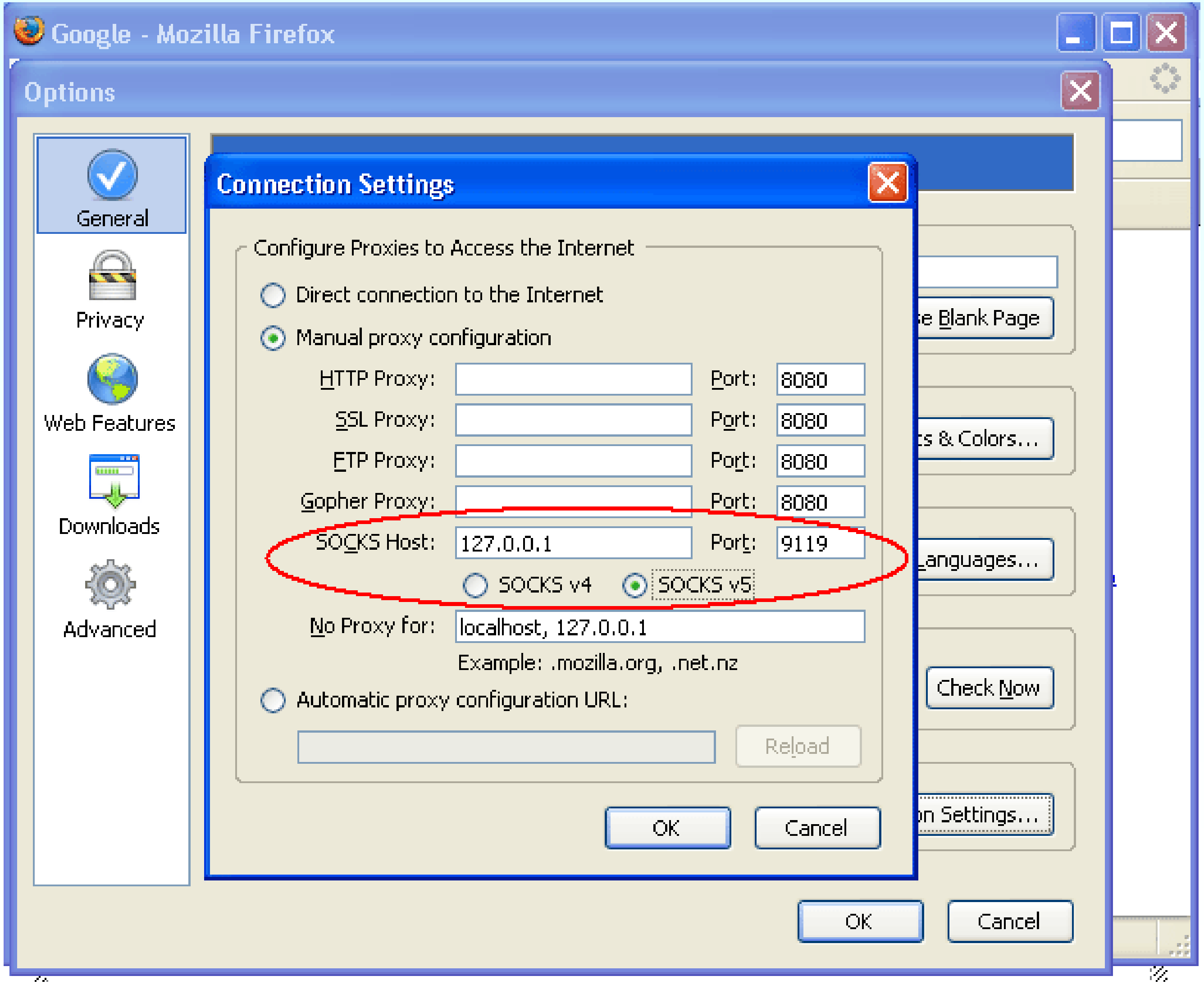
- Windows (PuTTY) –



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.
The new dss key fingerprint is:
ssh-dss 1024 2b:84:cb:4a:d0:ea:05:f3:50:3a:96:f3:47:61:01:3d
If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating the cache, hit No.
If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Firefox to use SOCKS



Connection Settings

Configure Proxies to Access the Internet

○ Direct connection to the Internet

● Manual proxy configuration

HTTP Proxy: Port: 8080

SSL Proxy: Port: 8080

FTP Proxy: Port: 8080

Gopher Proxy: Port: 8080

SOCKS Host: 127.0.0.1 Port: 9119

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

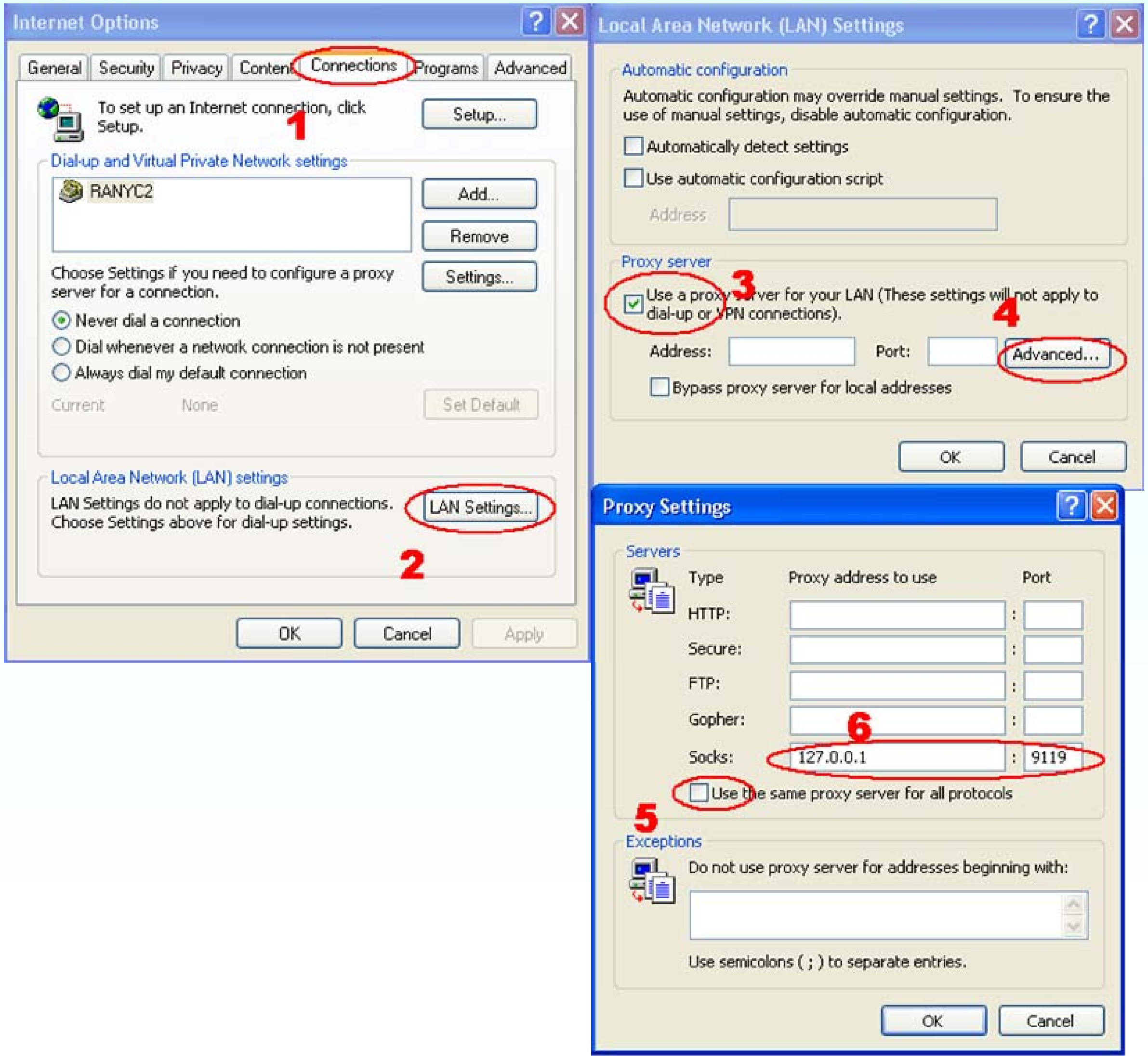
Example: .mozilla.org, .net.nz

○ Automatic proxy configuration URL:

Reload

OK Cancel

IE to use SOCKS



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

To set up an Internet connection, click Setup.

Setup...

Dial-up and Virtual Private Network settings

RANYC2

Add... Remove

Choose Settings if you need to configure a proxy server for a connection.

Settings...

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None Set Default

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

LAN Settings...

OK Cancel Apply

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced...

□ Bypass proxy server for local addresses

OK Cancel

Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:		
Secure:		
FTP:		
Gopher:		
Socks:	127.0.0.1	9119

□ Use the same proxy server for all protocols

Exceptions

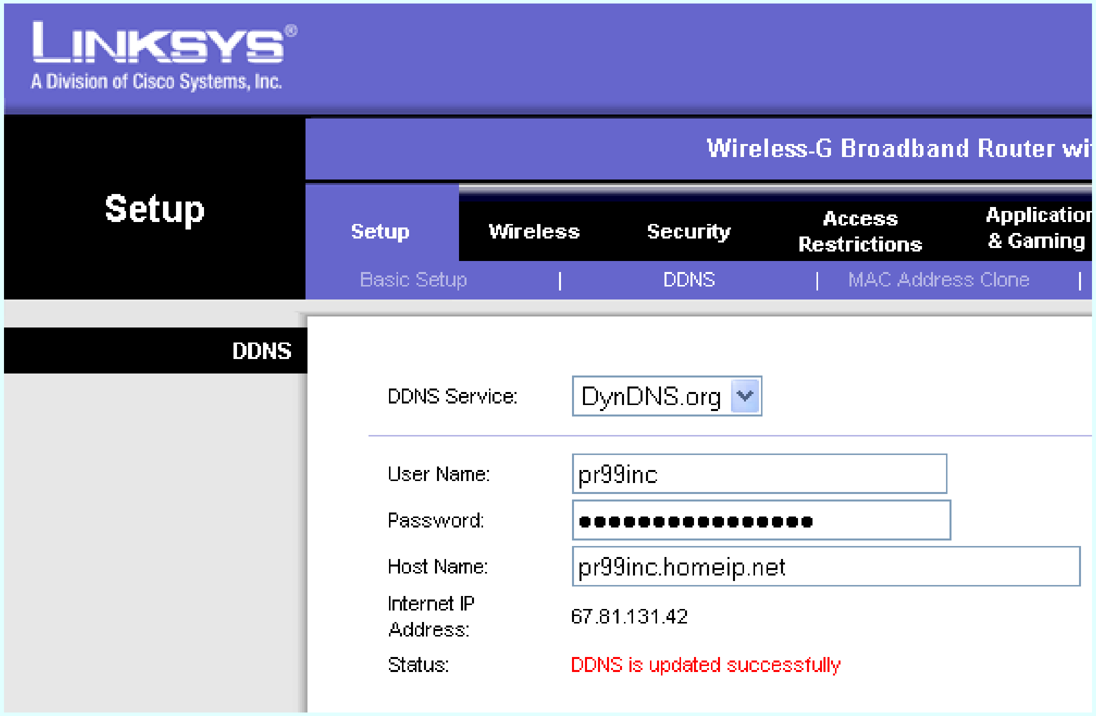
Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

OK Cancel

My home IP address changes all the time

- Use a free dynamic DNS service such as
  - **dyndns.org**
  - **zoneedit.com**
- Use an agent on your machine to automatically update the IP to a static name or it maybe built into your router.


LINKSYS®
A Division of Cisco Systems, Inc.
Wireless-G Broadband Router wi
Setup
Setup
Wireless
Security
Access Restrictions
Application & Gaming
Basic Setup | DDNS | MAC Address Clone |
DDNS

DDNS Service: DynDNS.org

User Name: pr99inc

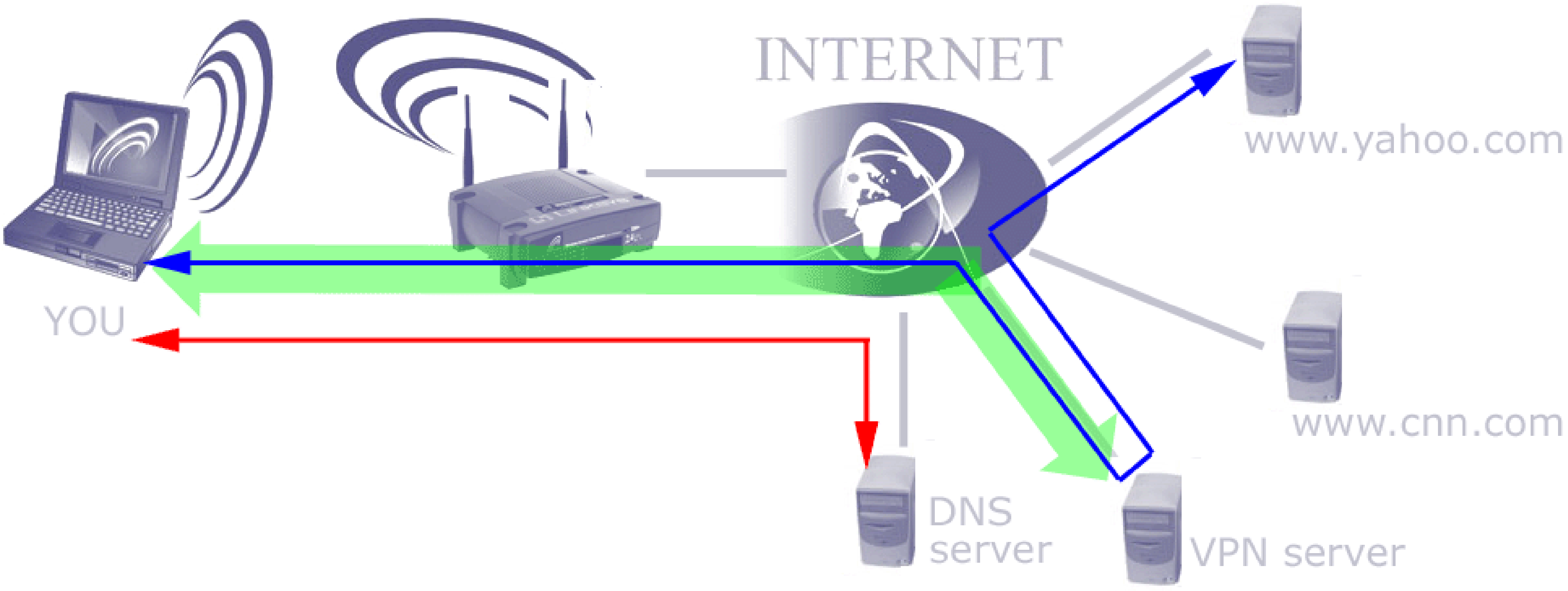
Password: ●●●●●●●●●●●●●●●●●

Host Name: pr99inc.homeip.net

Internet IP Address: 67.81.131.42

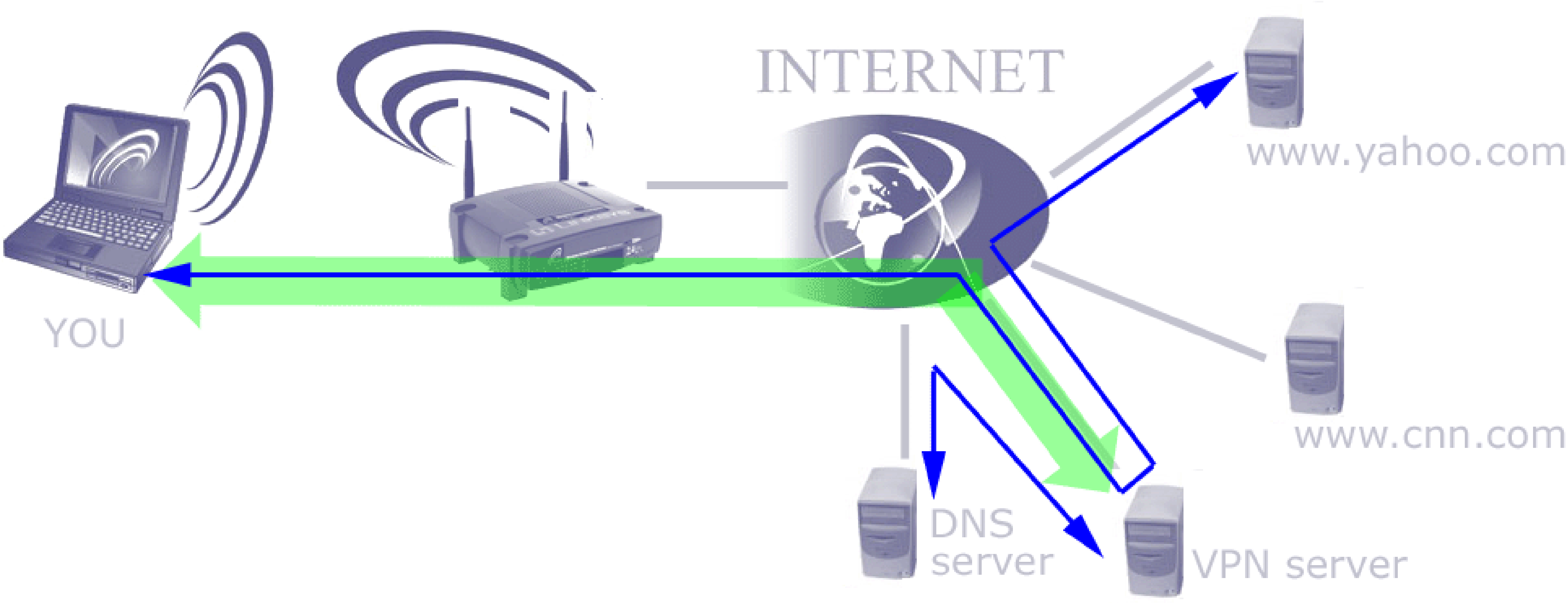
Status: DDNS is updated successfully

The Problem with SOCKS



Client does a DNS lookup and then sends that IP to the SOCKS server. DNS spoof attack may still succeed.

Use A Proxy Server as well



PROXY Software

- Client
  - Nothing need: It's built into the browser
- Server
  - UNIX/Linux
    - Simple perl program

      -or-
    - Squid
  - Windows
    - Simple perl program (requires Cygwin or ActiveState perl installed)

      -or-
    - FreeProxy
  - There's no shortage of proxy server software written in C, perl, or java

Get the perl proxy

Can be found at

http://www.cis.upenn.edu/sdt/proxy.pl

-or-

http://www.cs.princeton.edu/~dabo/proxy/proxy.pl

Make a small edit

change

```
require "sys/socket.ph";
```

to

```
use Socket;
```

Perl for windows

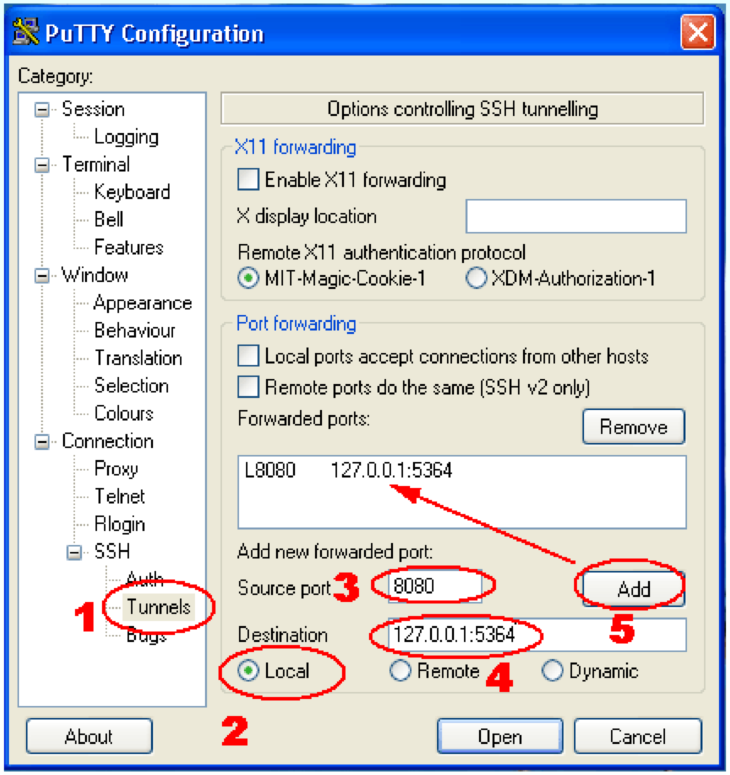
- If you are running Cygwin you probably all ready have perl
- Otherwise you can download a free copy from ActiveState
  - http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl
- Alternatively if you have to download something, you can just get FreeProxy instead of perl binaries and the perl proxy program

Client: Start SSH with tunnel

- UNIX/Linux/Cygwin:

```
$ ssh –L8080:127.0.0.1:5364 user@remote-host.com
```

- Windows: PuTTY



PuTTY Configuration

Options controlling SSH tunnelling

X11 forwarding

□ Enable X11 forwarding

X display location

Remote X11 authentication protocol

● MIT-Magic-Cookie-1 ○ XDM-Authorization-1

Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH v2 only)

Forwarded ports:

L8080 127.0.0.1:5364

Add new forwarded port:

Source port 8080

Destination 127.0.0.1:5364

● Local ○ Remote ○ Dynamic

- If using FreeProxy change the number 5364 to 8080

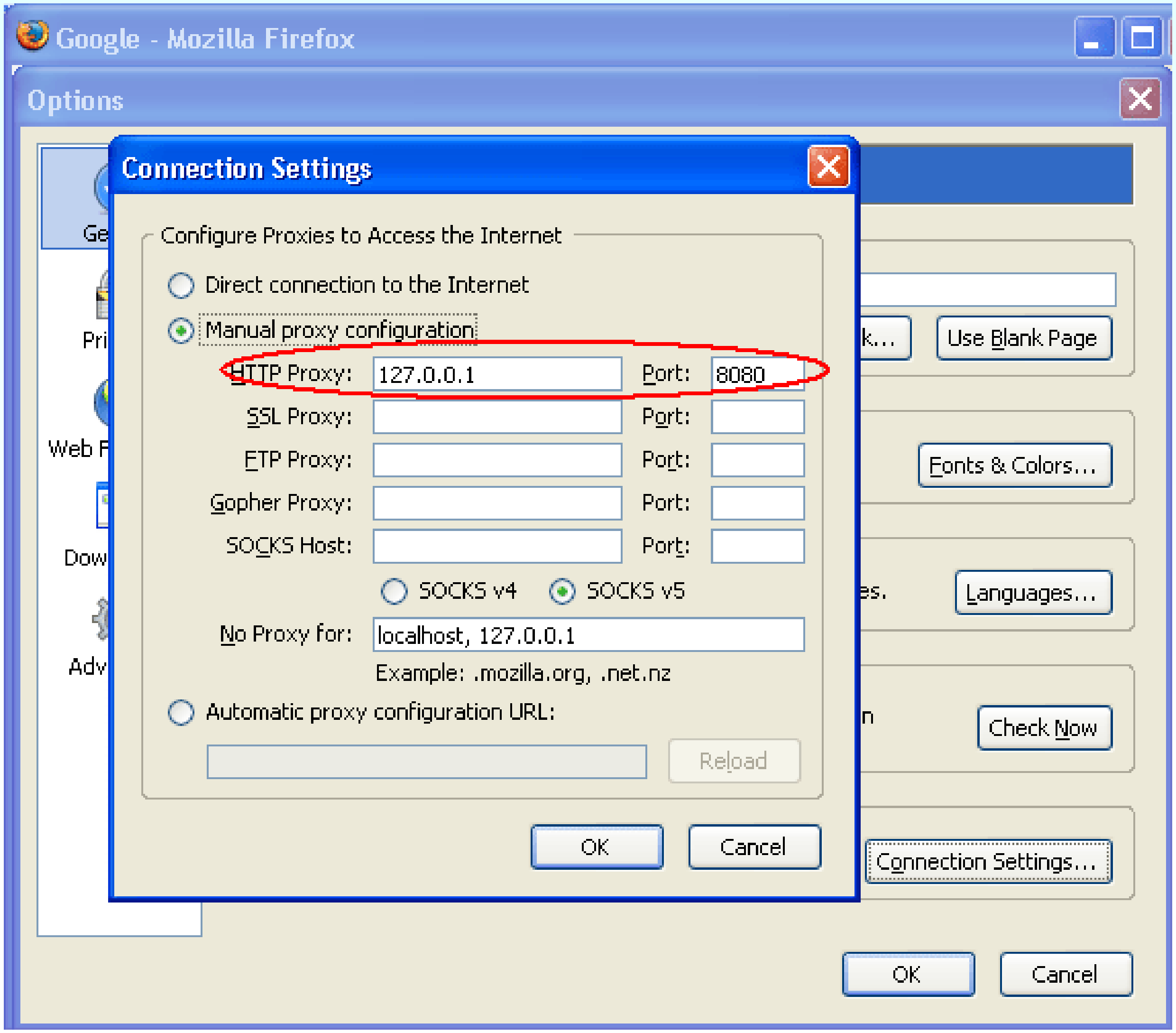
Running The Proxy

- SSH into the remote machine
- Windows run -
  - If using FreeProxy, must start it before
  - If using perl

    ```
    \perl\bin\perl proxy.pl
    ```
- UNIX/Linux/Cygwin run -

  ```
  $ perl proxy.pl
  ```

Firefox to use perl proxy



Configure Proxies to Access the Internet

○ Direct connection to the Internet

● Manual proxy configuration

HTTP Proxy: 127.0.0.1 Port: 8080

SSL Proxy: Port:

FTP Proxy: Port:

Gopher Proxy: Port:

SOCKS Host: Port:

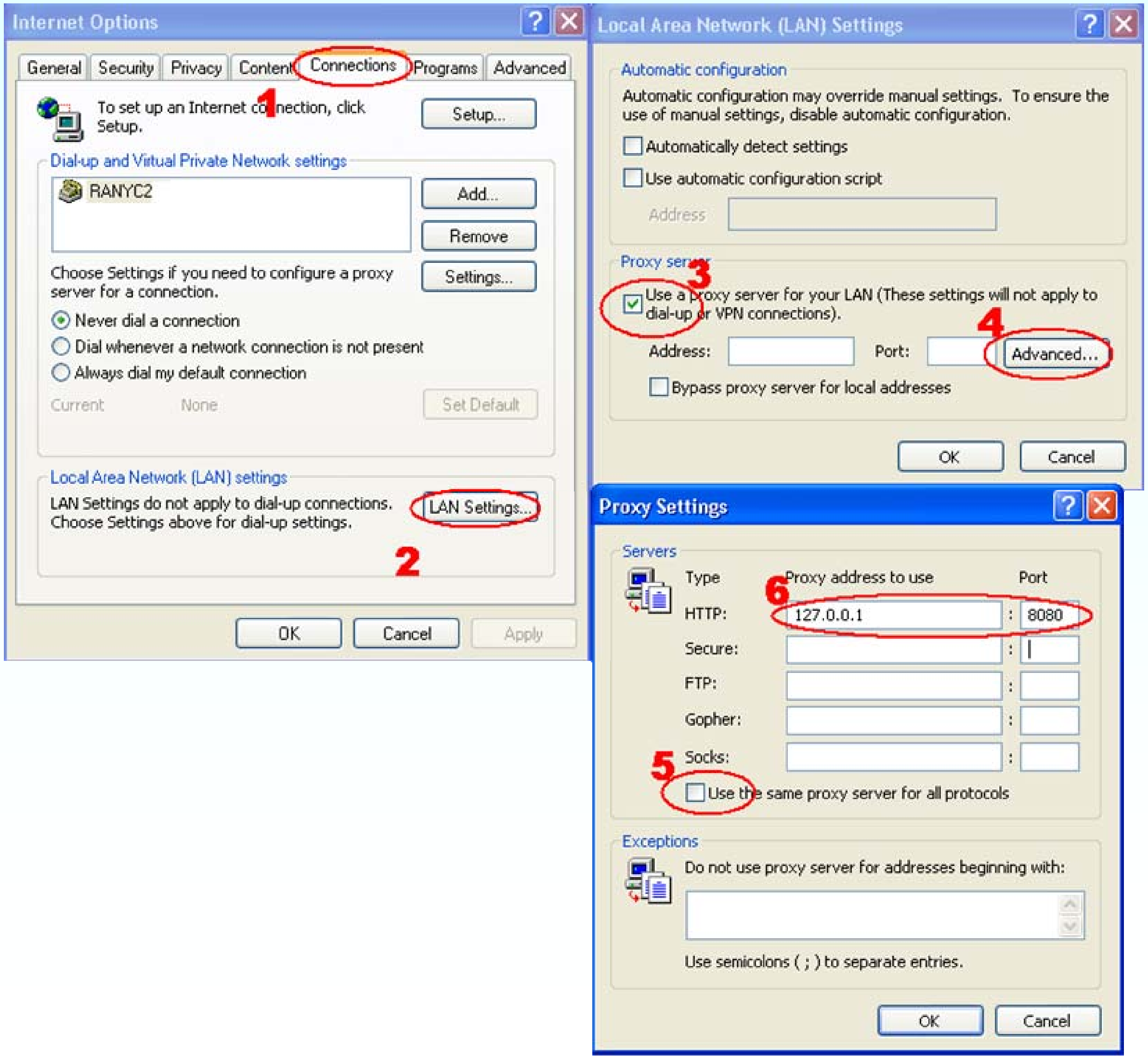
○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz

○ Automatic proxy configuration URL:

IE to use perl proxy



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

RANYC2

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

□ Bypass proxy server for local addresses

Servers

Type	Proxy address to use		Port
HTTP:	127.0.0.1	:	8080
Secure:		:	
FTP:		:	
Gopher:		:	
Socks:		:	

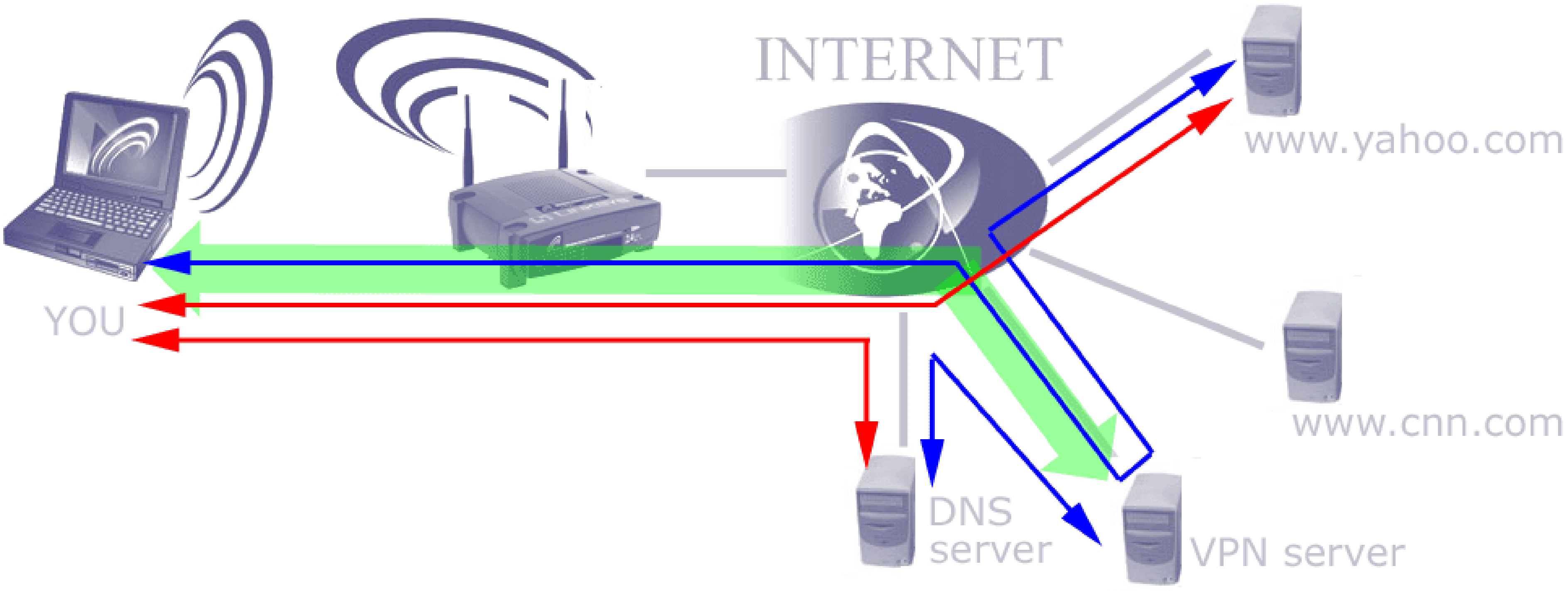
□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

Perl Proxy does not support SSL Pass-though



Standard access (non-SSL) goes through proxy

SSL access goes direct

No SSL support is not that bad

- Since SSL is one of the ways you can secure yourself, only DNS spoofing can happen
- Just watch for sites that have certificate problems (as noted previously)
- Or use a proxy server that supports SSL pass through (FreeProxy, squid)

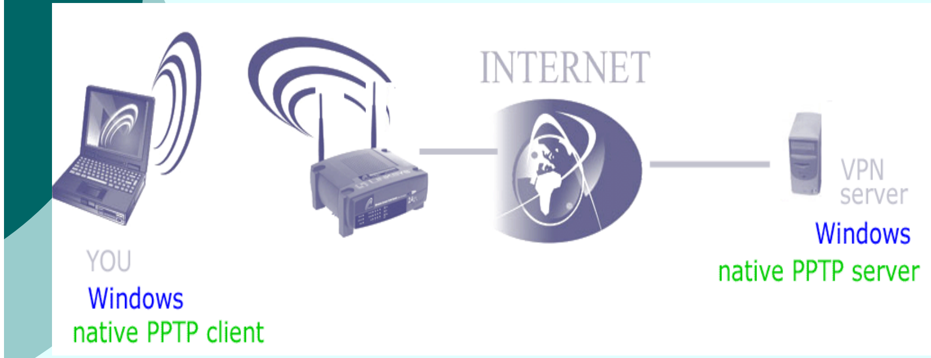
Performance Considerations

- CPU
  - Encryption uses CPU cycles on both the client and server
  - Usually only an issue if you have many clients on a single slow server
- Bandwidth
  - The server must relay all traffic (doubles the data)
  - The server’s upload speed becomes the maximum download speed (think home DSL line with slow upload)

Other Considerations

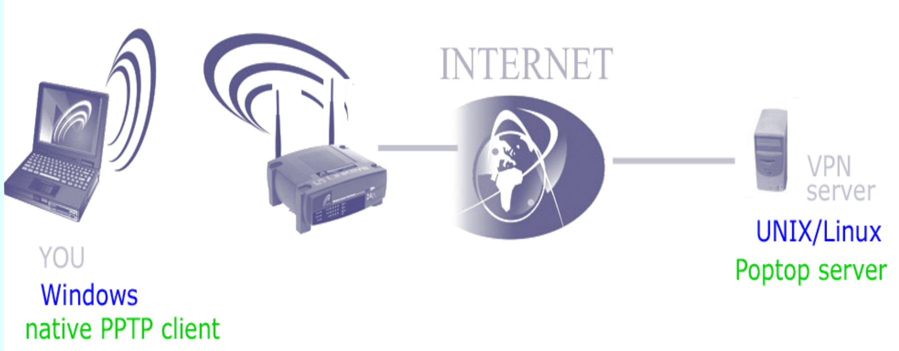
- VPN tunnels require continuous communication
  - If you roam from one AP to another, your session will disconnect and you have to reconnect it
  - If you loose association to the AP for any reason (weak signal, noisy radio environment, AP reboots) your session will disconnect and you have to reconnect it
- If you need more than just web browsing you may need a full VPN
  - PPTP
  - IPSec

Full VPN Combinations



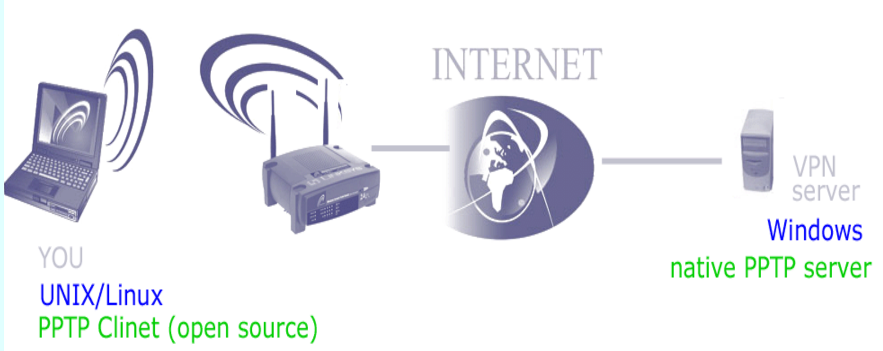
Windows
native PPTP server

Windows
native PPTP client



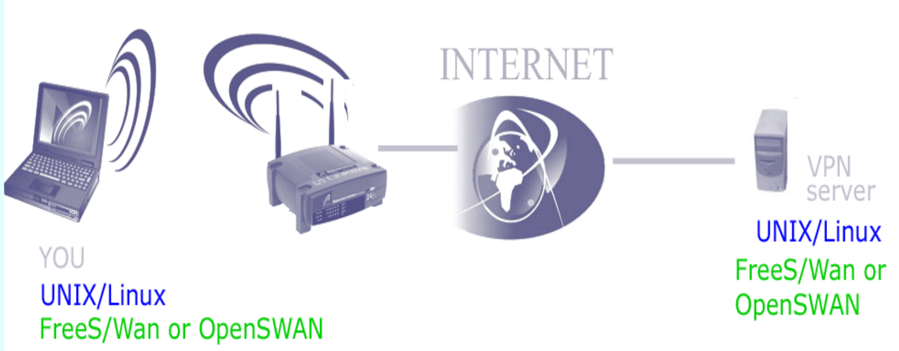
UNIX/Linux
Poptop server

Windows
native PPTP client



Windows
native PPTP server

UNIX/Linux
PPTP Clinet (open source)



UNIX/Linux
FreeS/Wan or
OpenSWAN

UNIX/Linux
FreeS/Wan or OpenSWAN

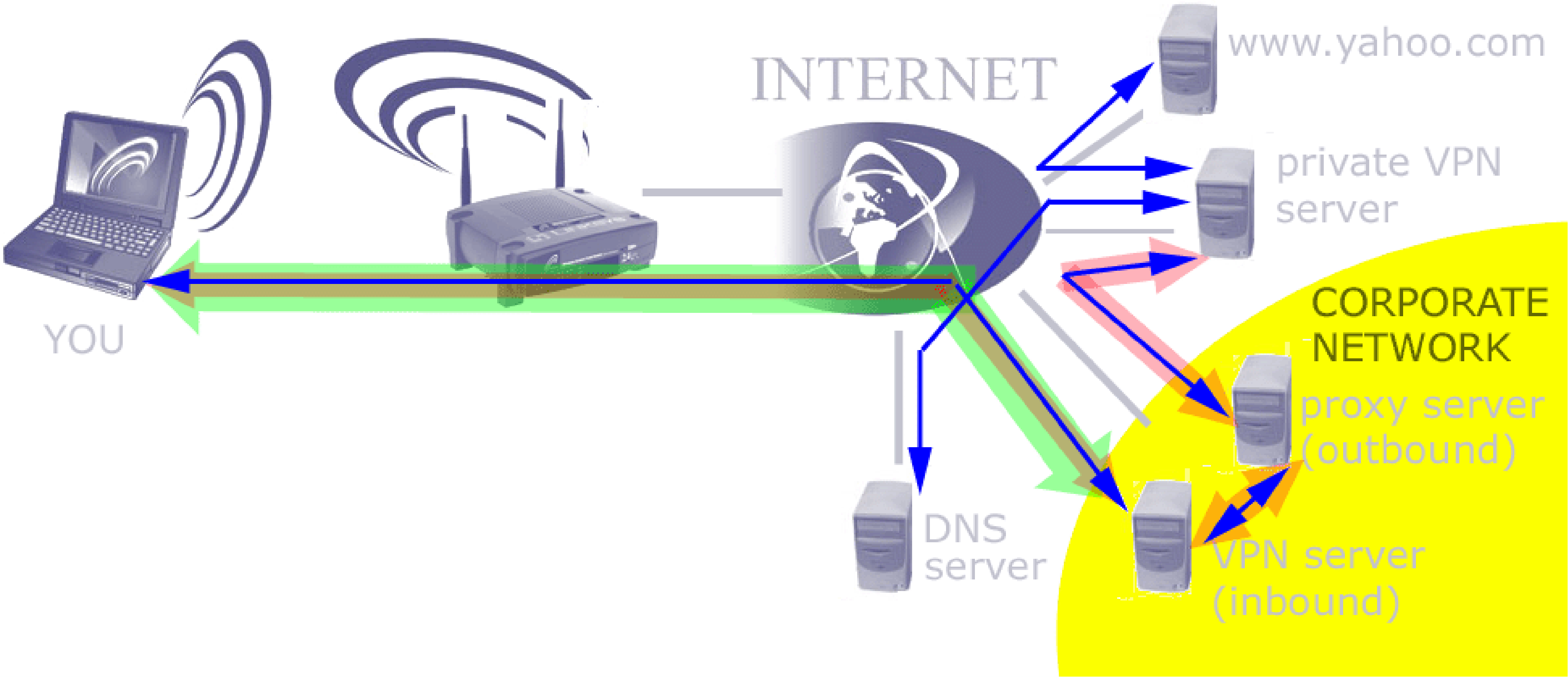
Other Good Ideas

- Use Anti-Virus software
  - AntiVir
  - AVG Anti-Virus
- Use Anti-Spyware
  - Spybot Search & Destroy
  - Ad-Aware
- Use Anti-Browser Spoofing and Hijacking
  - Spoofstick
  - Ad-Aware
- Don’t Use IE
  - Firefox
  - Maxthon (was MyIE2)
- Don’t Use Outlook
  - Thunderbird

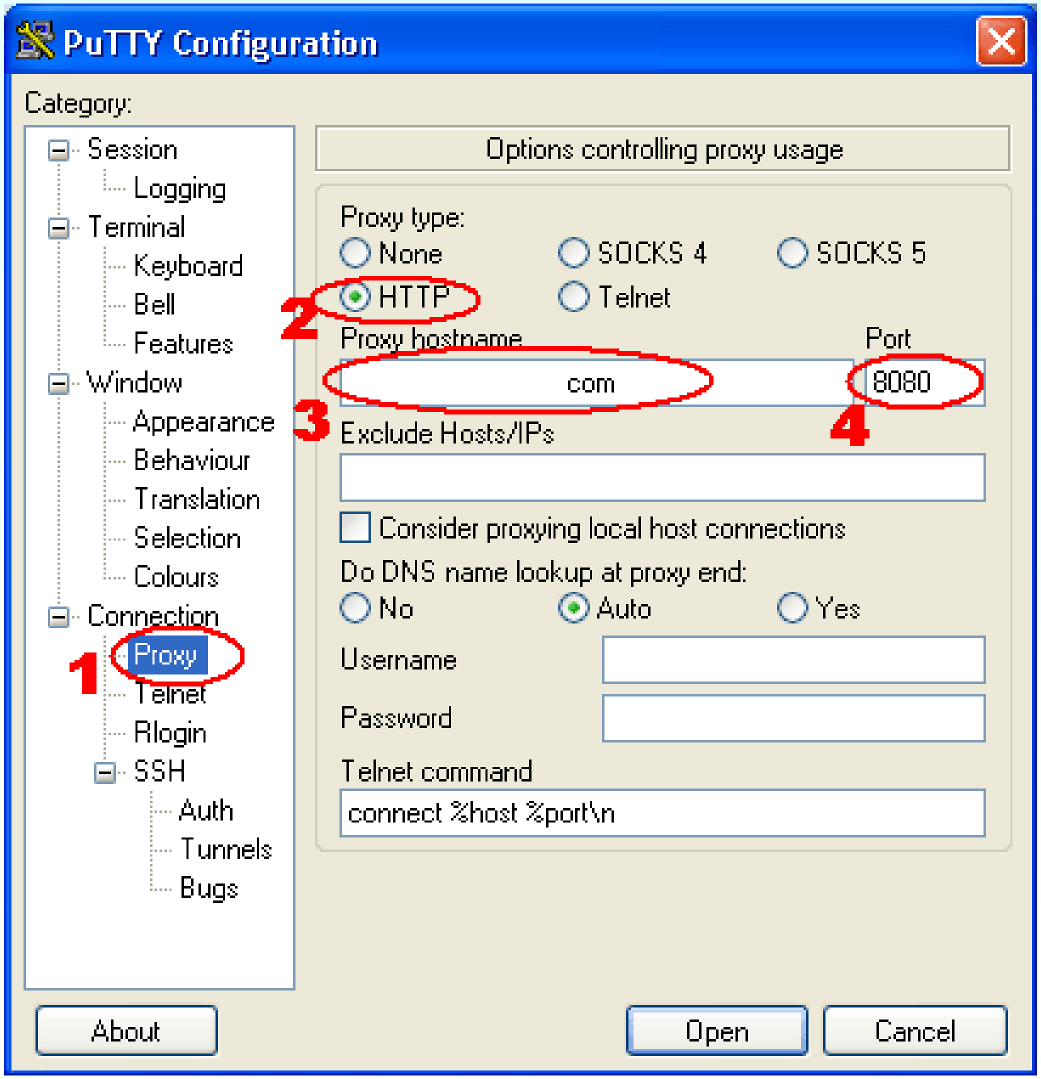
Not limited to just Wi-Fi

- These techniques can be used on any network not trusted, wired or not.
- Can also be used to tunnel out from restricted networks.
- You don’t have to use port 22 for sshd, you can use any unused port. You can put it on 443 if you are not running an SSL web server. This port is always allowed out through proxies. You can run it on a random high port to “hide” it.

Stuck on the Corporate LAN/VPN? SSH tunnel out



PuTTY can Tunnel Through Proxy



PuTTY Configuration

Options controlling proxy usage

Proxy type:

○ None ○ SOCKS 4 ○ SOCKS 5

● HTTP ○ Telnet

Proxy hostname: com

Port: 8080

Exclude Hosts/IPs:

□ Consider proxying local host connections

Do DNS name lookup at proxy end:

○ No ● Auto ○ Yes

Username:

Password:

Telnet command: connect %host %port\n

We’re Done

- All software noted in this document is available at no cost
- The links for all of the software, references and services can be found at http://wifidefense.cuzuco.com/
- The home router/firewall/access point screens are from a Linksys WRT54GS