# How to Bypass Your Corporate Firewall Using SSH Tunneling

~pingywon 2004

**Preface:**

I had gotten a new job and no way to connect back to my house (Terminal service, Radmin, VNC what ever) due to our firewall (ISA). After talking to friends and colleges the following is what was presented to me. I by no means made this up, just consolidated it all here in an easy to read manner with pictures. Everyone loves pictures.

**Key assumptions:**

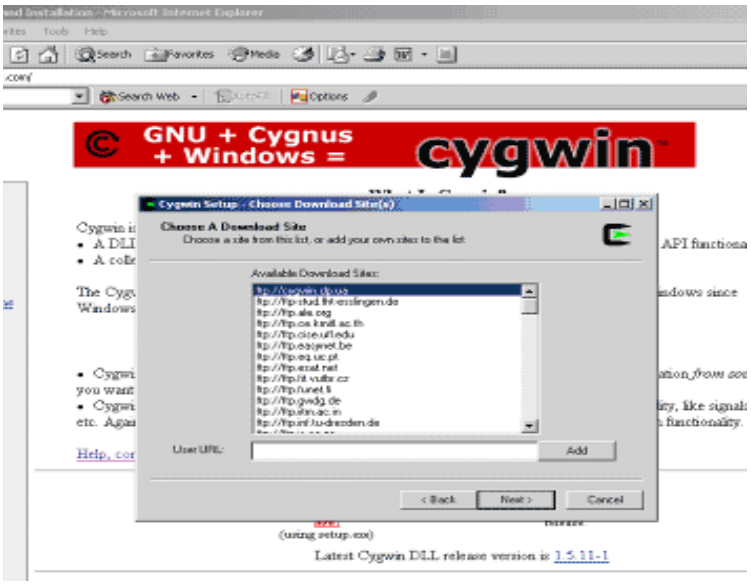
1. You already have some type of remote server listening at home (where ever). Configuring and setting something like this up is easy, but still out of the scope of this doc.
2. You have a clear line of communication with that port that is listening (besides that stupid firewall you are sitting behind at work). You have the port open on your router/fire wall at home.
3. You have already opened port 22 on your home router to allow SSH connections into your home network
4. Whatever firewall you are on at work has port 22 open for SSH traffic (this is normally the case if you have any networking guys on the same segment as you. It is used to control a lot of networking equipment remotely.

**Let's Get To It:**

Download the following

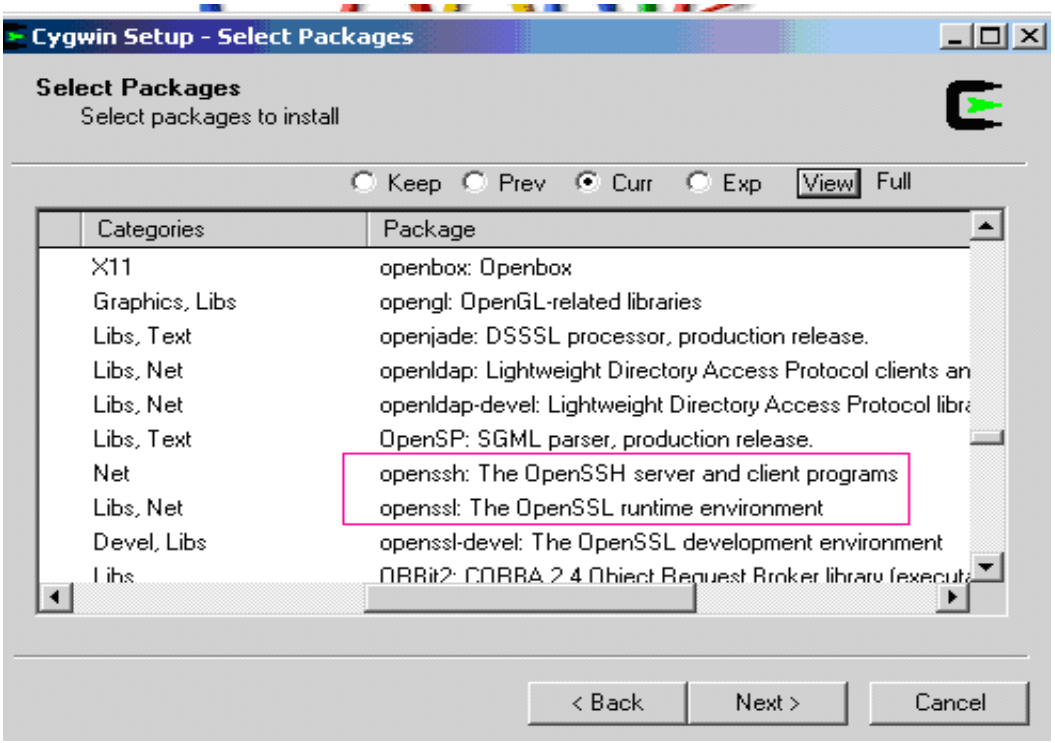
1) **Cygwin** - http://cygwin.com/
2) **PuTTY** - http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Cygwin is a pretty large download (40meg)

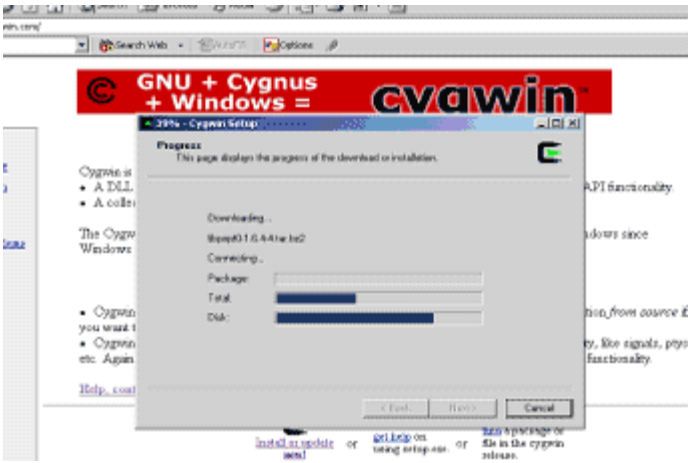



Pick a FTP site to download components from.

**IMPORTANT – On the next screen switch to FULL then scroll to the right an scroll down to the "*open SSH Server and client programs*" and change it from "*skip*" to "*install*"– this will automatically select the runtime environment (which you need)**

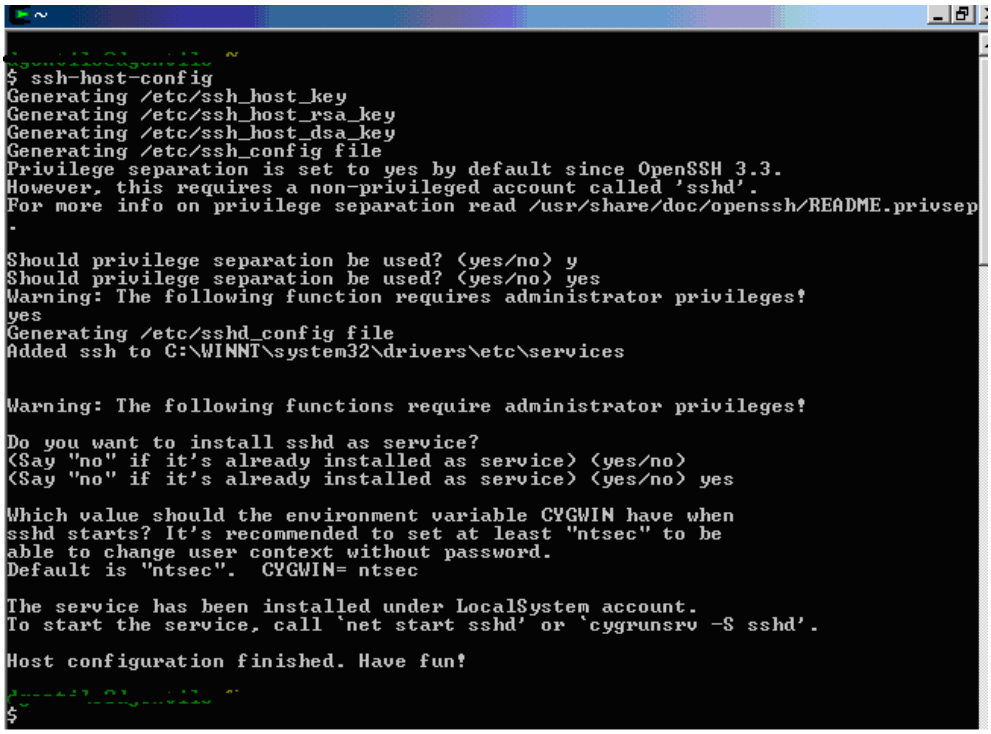



Hit next and let it do its thing. You can add more packages to the install if you like. This will obviously create a longer install time.



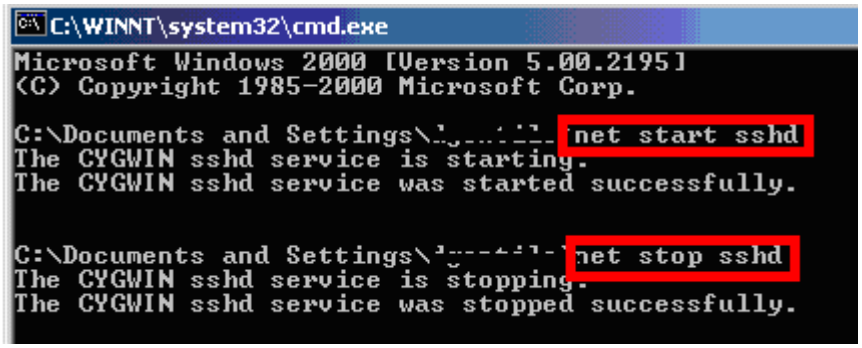

Once the install is done open up your Cygwin icon on your desktop. You will be dropped into your shell.

From the shell we want to type "**ssh-host-config**"
This will install the sshd service.
You will be asked 2 questions answer **YES** to both of them.
Once you have done that it should look *something* like this:




Next step is to execute the SSH daemon (service).
We do this from a command prompt. **START > RUN > CMD <enter>**
The type"**Net Start SSHD**"

It will look something like this:




**Net start sshd** – starts the SSH service
**Net Stop sshd** – Stops the SSH service

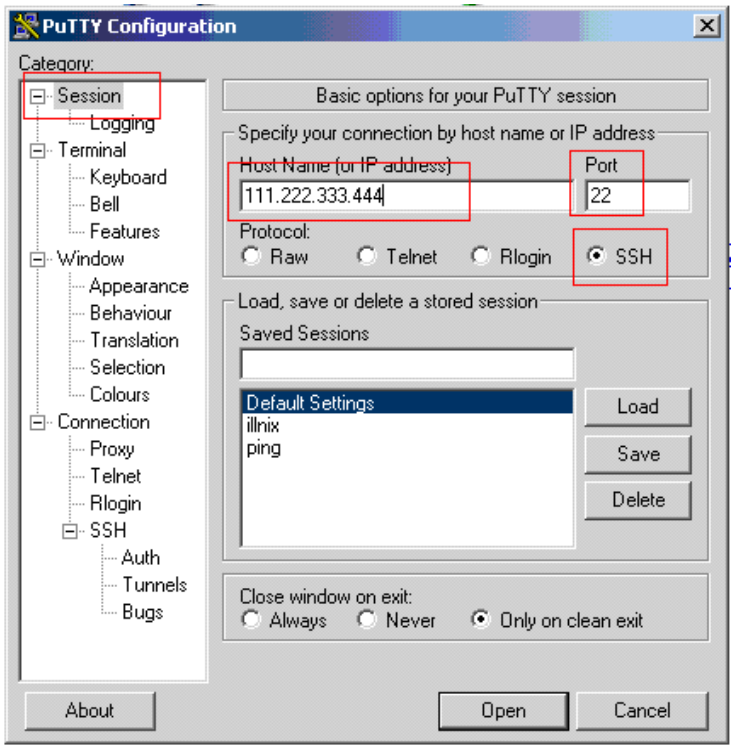
Once the service is running there is no need to restart it even if you restart the PC.

OK – everything up till here has been done at home, and we are still assuming you have some type of remote control already running at home (VNC, Radmin, Terminal services, etc…)

# At Work

Now we will need PuTTY and your remote control client. I use Radmin (**www.radmin.com**) and that is what I will use in this example.

Open up PuTTY – and fill in the parameters to point it to your home.



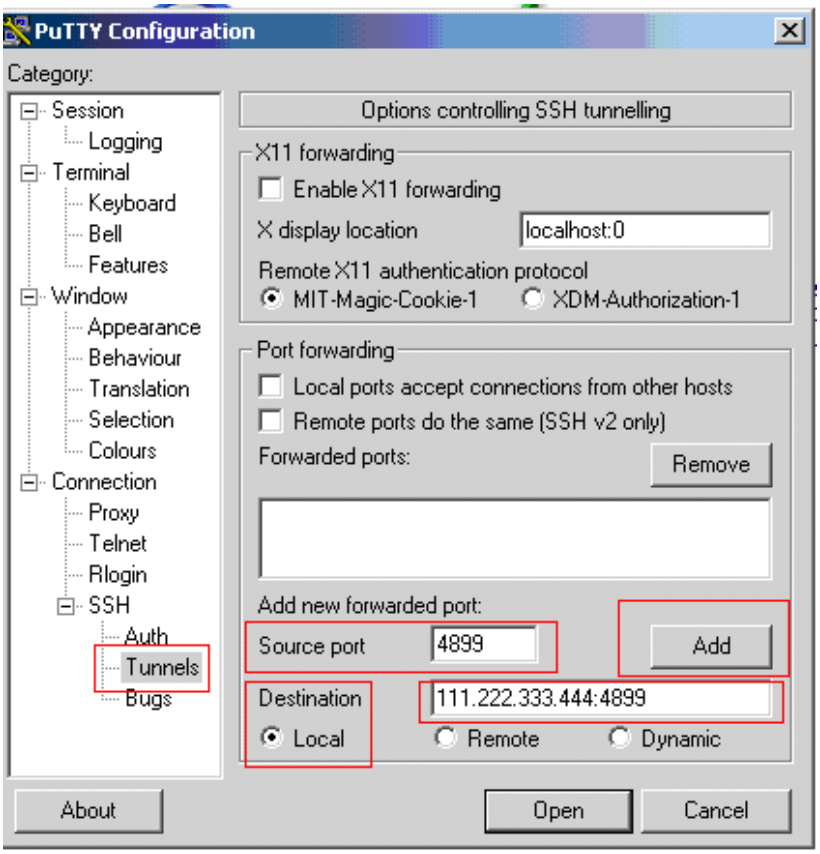

- Enter your external (public) IP address.

- Port is 22
- Select the SSH radio button
- Name your saved session

## Tunnels Category

- Choose the *Tunnels* category
- *Add a new forwarded port*
- *Source port* is the port that your remote control server is listening on at home (Radmin default is 4899)
- *Destination* is your external IP again but after it put a colon and the source port again (E.G. – 111.222.333.444:4899)
- Keep the destination radio button on *local*
- Finally hit *Add* button to add it to your current configuration.
- The port should now be added to the *Forwarded Ports* box (you can add as many as you have a reason to)

## Picture below:

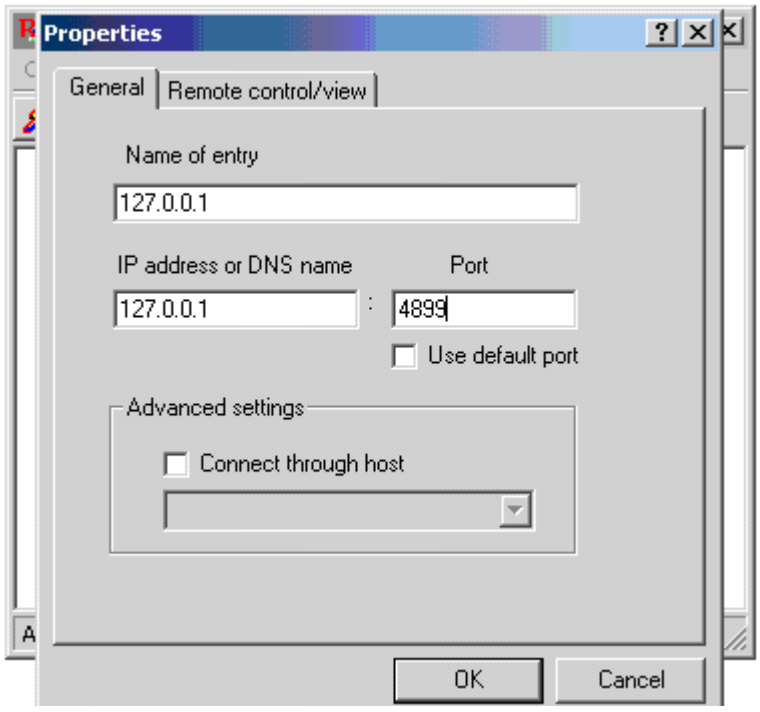


## Important:

Go back to the “Session” Category and name your session and save it. So you don’t have to reconfigure everything every time you open it.

## Remote Control Client:

1. Open your remote control client.
2. Set the port that you are using (Radmin default 4899)
3. IP – set it to your local loop back address ***127.0.0.1***




## Connecting:

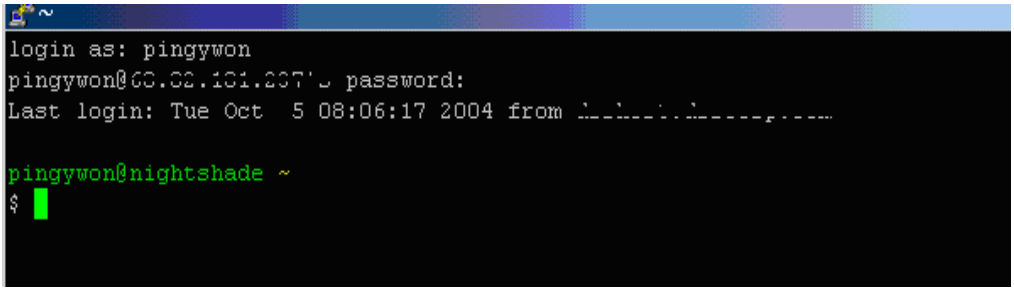
We now have everything set up and are ready to connect. What we are doing is SSHing out port 22 and into port 22 at home. Once that connection is established we are forcing our Radmin connection to go through there as well. So while port 4899 is blocked from going out of my firewall at work port 22 is not. All the firewall sees coming and going is port 22.

In order to sucefully connect we must first connect/establish out SSH connection. For this we will use PuTTY.

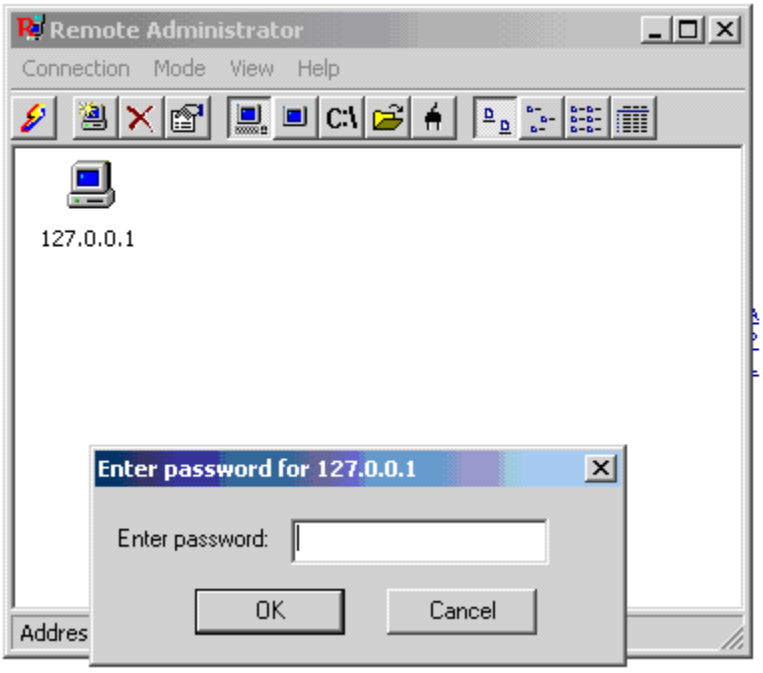
1. Open PuTTY – double click your saved connection which will connect to your house with your Radmin port mapped to it.

2. Login to your SSH connection using your normal windows username and password through PuTTY.
3. Once you're PuTTY connection is established open the remote control client.
4. You should have already save the connection to IP 127..0.0.1
5. Open the connection to 127.0.0.1 – If all went well you should be prompted for a password.
6. Enter your Remote Control password and you're in!

**See pictures below:**




**PuTTY connecting home**




**Radmin connecting home**

# G R E E T Z:

Leadbane – who gave me most of this information
**http://www.illmob.org**
illwill
morning_wood
detro
pygmy

**Old school crew:**
akaran
ratSalad

~pingywon 2004
**pingywon@pingywon.com** – Questions/Comments/Concerns

**http://www.pingywon.com**

Yazat Karatus Arazatus O-bey Productions inc.