Free remote help desk technique

Whitepaper written by Stefano Coletta (Creator) on 5 october 2003
Contact me at creator@mindcreations.com or by visiting http://www.mindcreations.com

In brief

A multiplatform secure, reliable and free solution to fully manage a remote computer from outside a private network (using NAT) or a protected network (using ingress firewall rules only).

Features

- Bypass any ingress firewall rule (needs only egress port 22/tcp open)
- Very hard to hijack/sniff:
    - VNC traffic is securely encrypted through SSH (no cleartext transmissions)
    - Triple authentication: one login for each ssh client and one VNC login to get access to the Managed PC.
    - TightVNC accept only locally originated connections
- Permits remote management even on NAT environments
- Completely realized with open source free software
- Platform independent (TightVNC runs on almost every OS)
- Quite fast (can benefit from ssh compression algorithms and TightVNC compression schemes)
- No need to know the Managed PC IP address
- No need to know the Viewer PC IP address
- Flexible: no matter where you are located, the Managed PC can be reached, no matter where it is connected, you can reach the Managed PC with no configuration changes.

Why do I need this?

Often skilled people are bored to help dummies to solve their daily problems while using PCs. The most common situation is that you have to move from your desk/home to get to their desk/home to show them how things have to be done. You need to see their computer screen and look around to figure out which mysterious and uncommon problem they are experiencing (from their point of view, obviously ☺). Sometimes you can solve their problem by speaking at the phone or by sending them detailed emails… but you know that they are hard to instruct this way… so you have to get to their place and solve the problem wasting your time and patience.
If you are in this situation my idea can become handy to rest at home/desk and get the job done.

What do you need: commonly said “Requirements”

1) The TightVNC client for you and the TightVNC server installed on the PC to be managed
2) A public ssh server reachable from you and your friend/customer/partner.
3) The Putty ssh client (or anything you like) for you and the PC to be managed

The bad news

- Not so easy to set up for beginners
- Does not work when any egress traffic is blocked at perimeter firewall A or B (usually only on heavily secured networks)

How it works

Look at the next figure to follow these steps.

0) The Managed PC starts the TightVNC server.

1) The Managed PC establishes an ssh session (violet) to the Relay System (public IP, port 22/tcp)

2) The SSH Client creates a backward ssh tunnel (red) from the Relay System (127.0.0.1) to the Managed PC (127.0.0.1) for ports 5800 and 5900 using the TCP protocol (from now named “VNC ports”). Now the Relay System can connect itself from localhost to the Managed PC local VNC ports.

3) The Viewer PC establishes an ssh session (blue) to the Relay System (same way of the Managed PC)

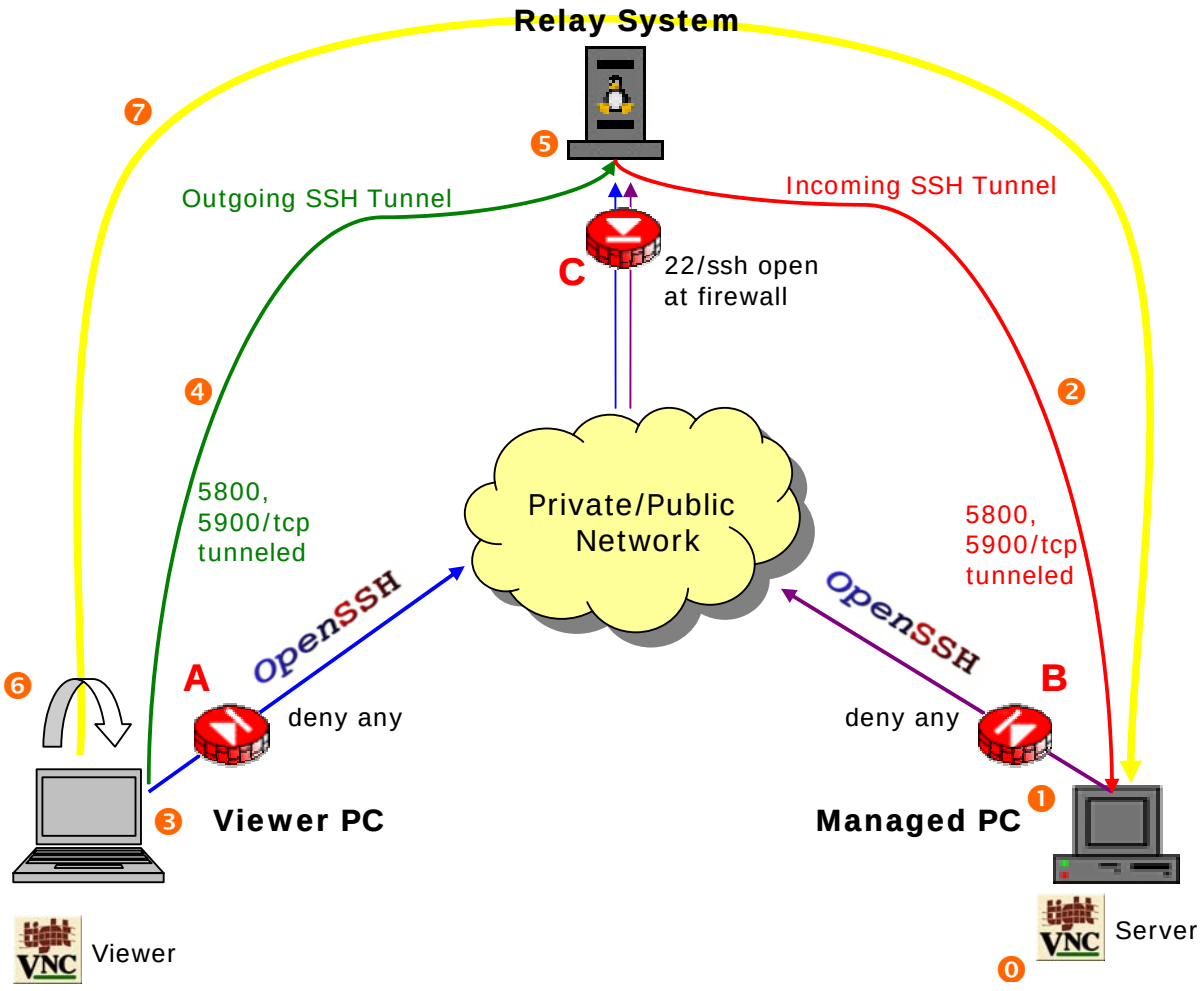
4) The SSH Client creates a forwarding ssh tunnel (green) from the Viewer PC (127.0.0.1) to the Relay System (127.0.0.1) for VNC ports. Now the Viewer PC can connect itself from localhost to the Relay System (127.0.0.1) VNC ports.

5) The two SSH tunnels are automagically merged together at the Relay System permitting the traffic to flow from the Viewer PC to the Managed PC.

6) The Viewer PC starts the TightVNC client pointing it to localhost.

7) The Viewer PC now can control the Managed PC using the TightVNC client over a double tunnel (yellow) over SSH ☺

Flows diagram



How firewalls and NATs are bypassed

If you look at the picture you can see three firewalls (A, B and C) and perhaps two NAT networks (behind A and B firewalls).

Firewalls A and B are configured to deny any ingress packet, while firewall C is permitting ingress traffic only for port 22/tcp. This means that no one can contact the Managed PC or the Viewer PC directly from the outside network. With ssh you can create tunnels: those ones do the trick by only using a single open port (22/tcp) on the Relay System.

When the Managed PC connects to the Relay System and creates the first backward tunnel it effectively opens the port 5800 and 5900 using TCP protocol for the Relay System. They are obviously not really opened on the B firewall but simply backwarded to the Managed PC using the red backward ssh tunnel. The worst thing is done, the first NAT or firewall B is bypassed.

Now the Viewer PC connects to the Relay System creating another tunnel, a forward one, that effectively opens the port 5800 and 5900 using TCP for the Viewer PC. Even these ports are not opened on the C firewall but simply forwarded to the Relay System using the green forward ssh tunnel. At this point even the firewall C is bypassed.

From now, when a connection originates from the Viewer PC towards IP 127.0.0.1 port 5800/tcp (say VNC client for example) it is automatically forwarded to the Relay System on port 5800. In this place we have another tunnel ready that is making the reverse connection and thus forwarding our packet toward IP 127.0.0.1 port 5800/tcp of the Relay System. The second tunnel (the red one) now forwards the packet to the Managed PC port 5800/tcp arriving, finally, to the TightVNC server socket.

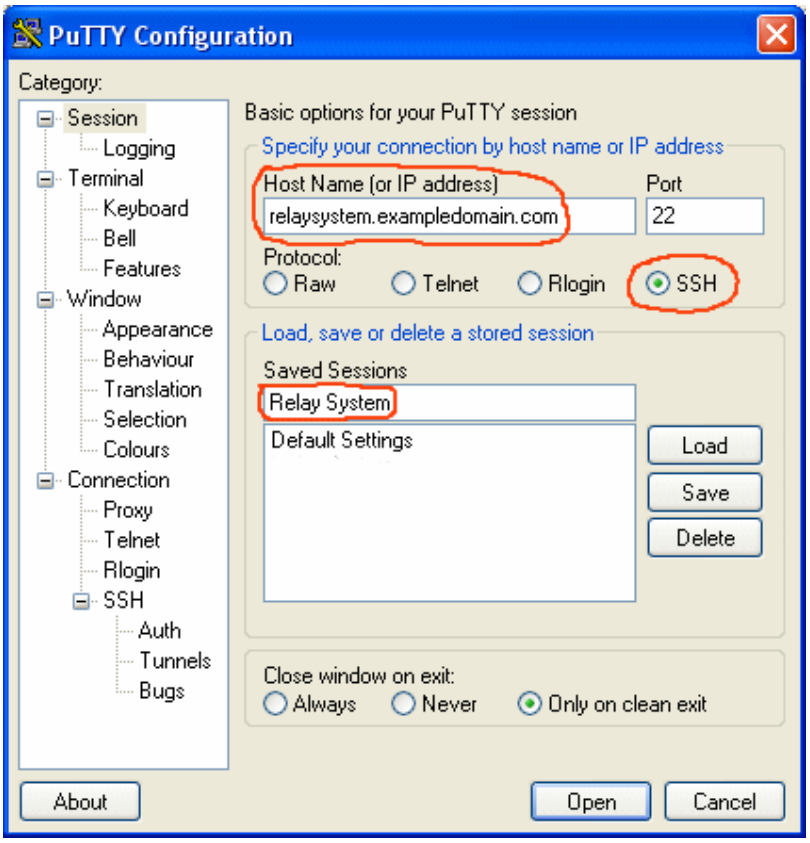
The yellow line now represents the direct connection we have virtually realized using the Relay System as a bridge impersonating a somewhat trusted host for both ends (PCs).

Step by step instructions

Follow these instructions to set up both Managed PC and Viewer PC.

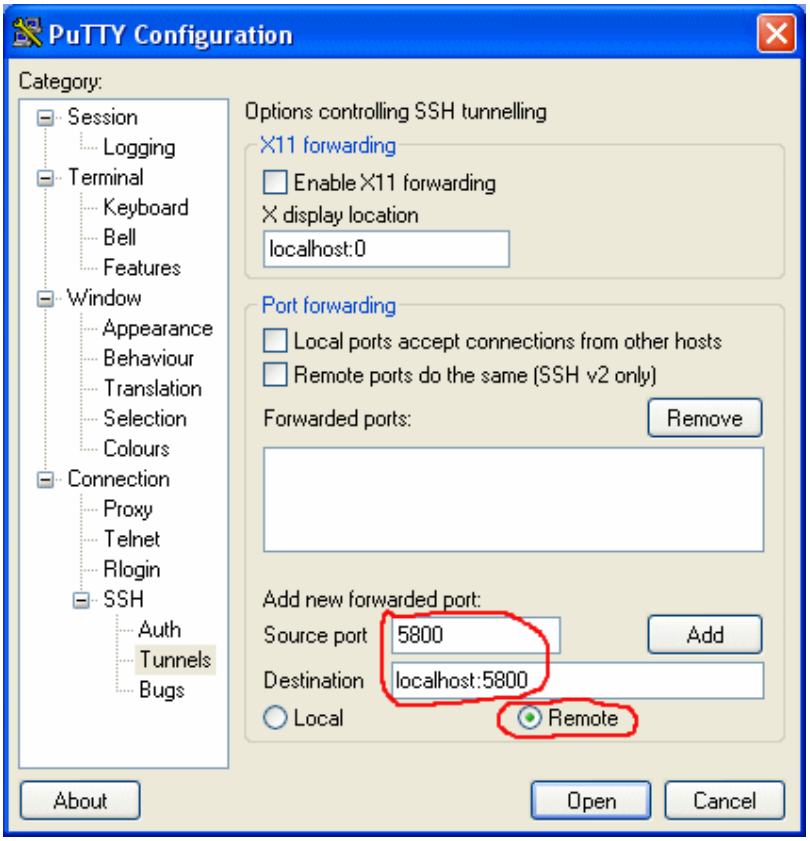
Managed PC side

1) Download TightVNC from http://www.tightvnc.org
2) Launch TightVNC setup and follow onscreen instructions. Let the default choices unchanged.
3) Download Putty from http://www.chiark.greenend.org.uk/~sgtatham/putty/
4) Putty does not require installation, just run it, it is an executable. The following screen appears:



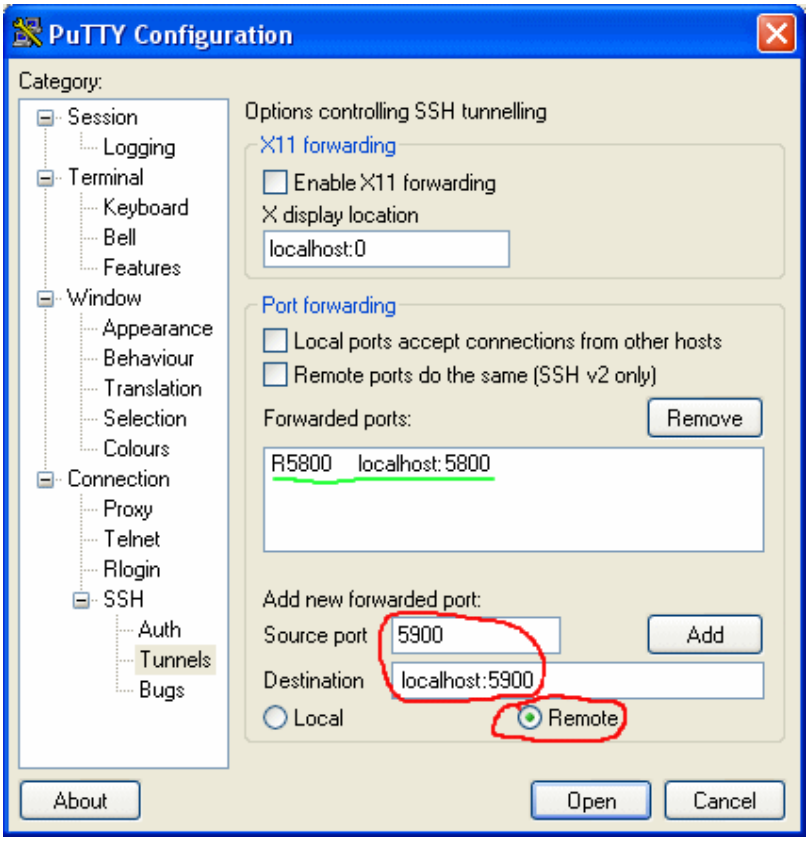
5) Fill the fields as indicated by red circles; substitute relaysystem.exampledomain.com with the real address of your Relay System then click **Save**.

6) Now click on **Tunnels** options under Connection/SSH category, the following screen appears:

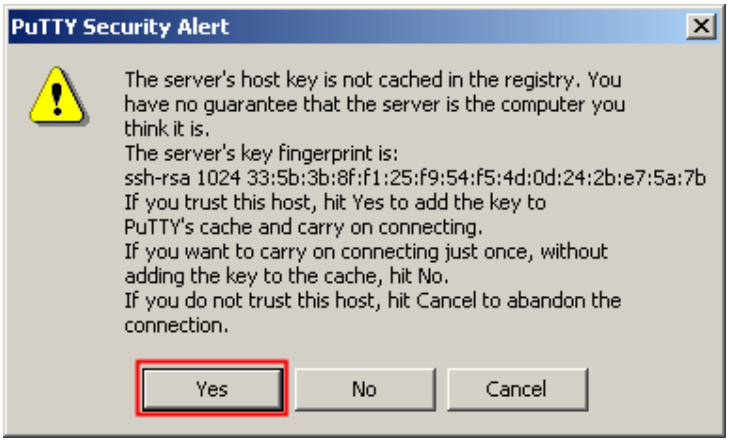


7) Fill the fields as indicated by red circles and then click **Add**.

8) Repeat the same for port 5900 as shown in the next image and click **Add**. Note that the previous port has been added (green underlined).

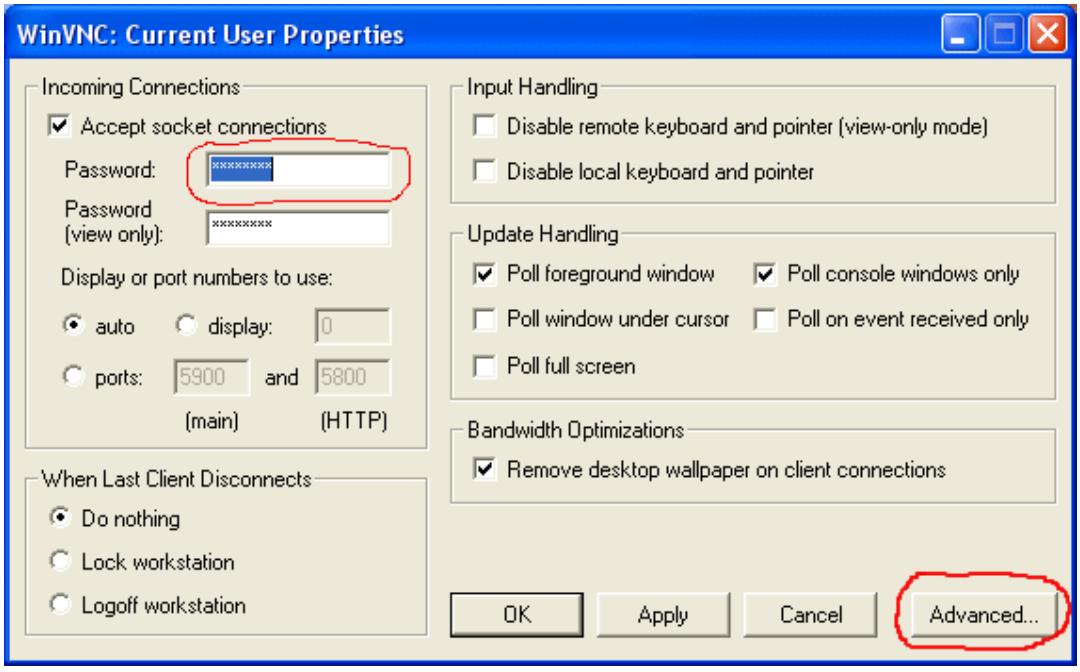


9) **In order to continue you need a valid account on the Relay System.** Now click **Open.** After few seconds a popup window like the following will ask you to accept the key of the remote Relay System.

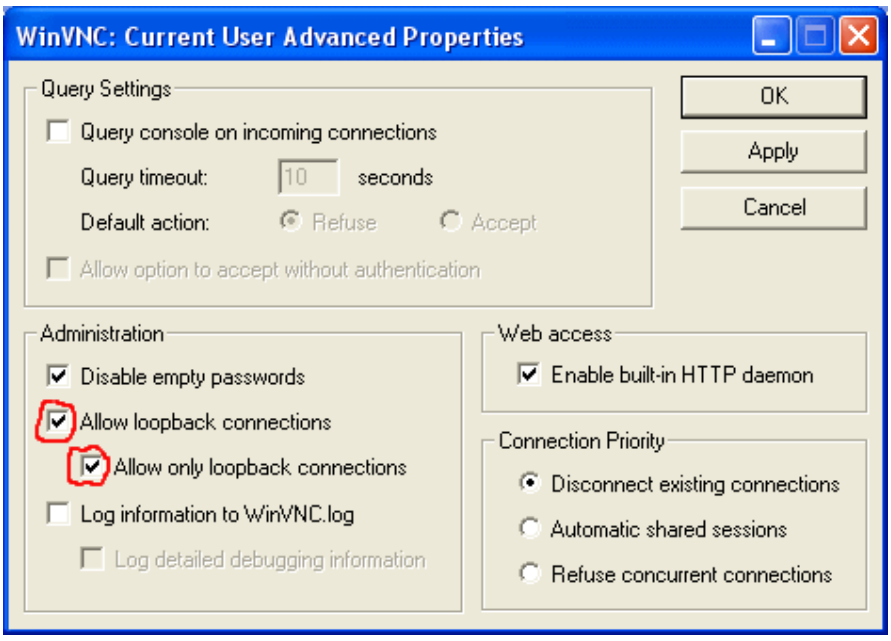


10) Click YES and in the next window type username and password. The ssh part is finally over ☺

11) Launch the TightVNC Server and configure it to suite your needs by right clicking its tray icon and by selecting **Properties**.



12) Specify a password to allow connections to your PC and then click **Advanced**: the next screen will show up.

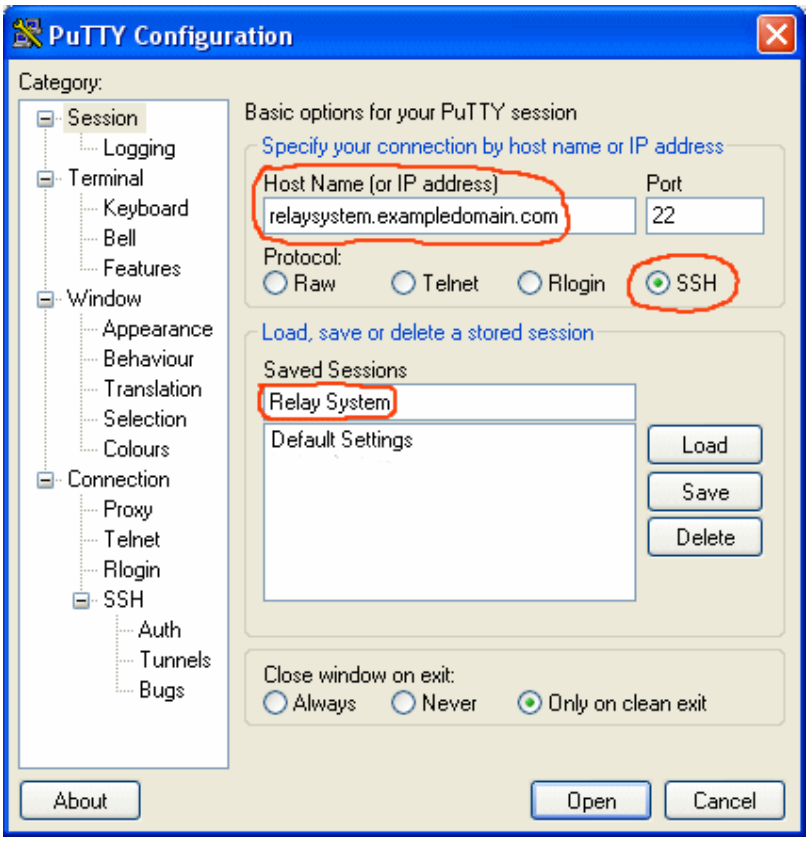


13) Check the “Allow loopback connections” and “Allow only loopback connections” then click **OK** to close this window and **OK** for the previous one.

14) You are done! Just wait for help from the Viewer PC. You’ll see your mouse pointer moving around when the Viewer PC connects to you.

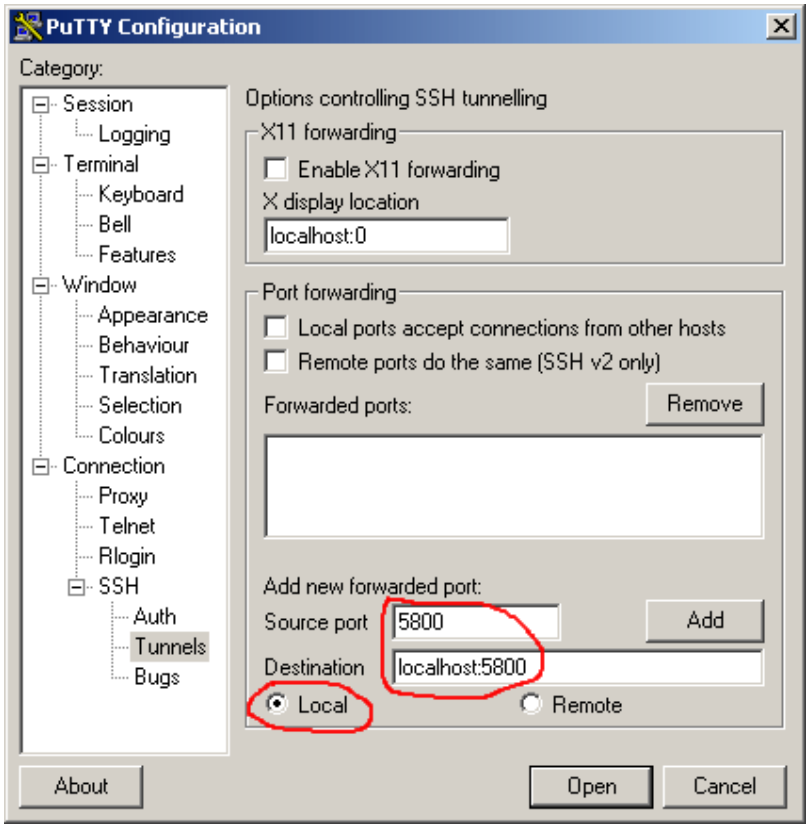
Viewer PC side

1) Download TightVNC from http://www.tightvnc.org
2) Launch TightVNC setup and follow onscreen instructions. Let the default choices unchanged.
3) Download Putty from http://www.chiark.greenend.org.uk/~sgtatham/putty/
4) Putty does not require installation, just run it, it is an executable. The following screen appears:

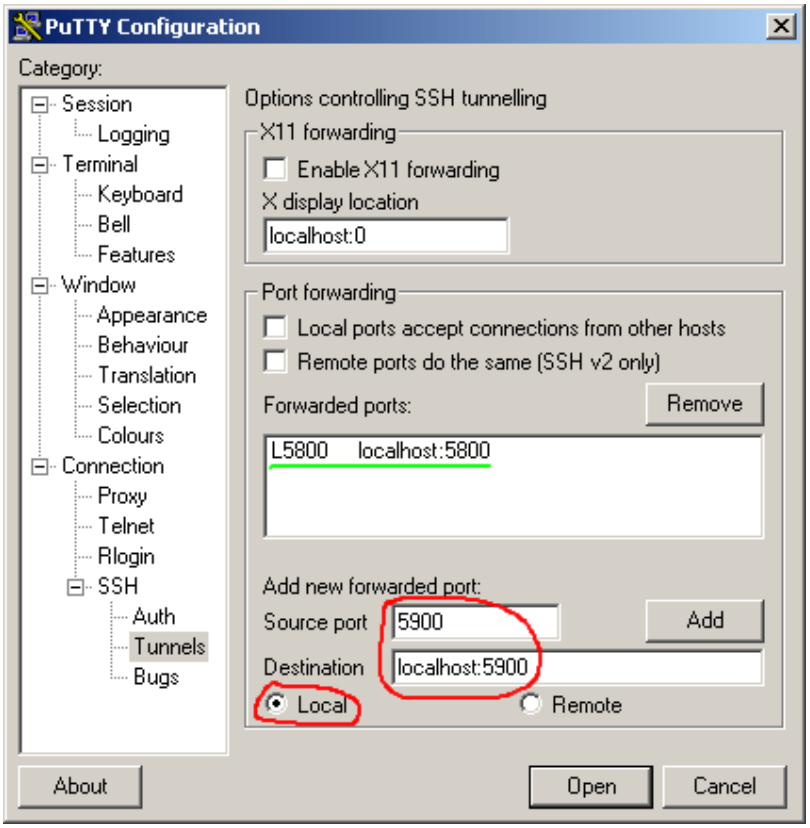


5) Fill the fields as indicated by red circles; substitute relaysystem.exampledomain.com with the real address of your Relay System then click **Save**.

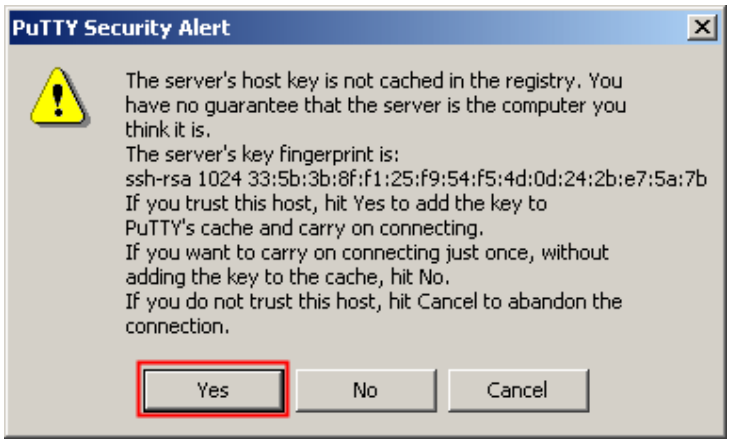
6) Now click on **Tunnels** options under Connection/SSH category, the following screen appears:



7) Fill the fields as indicated by red circles and then click **Add**.
8) Repeat the same for port 5900 as shown in the next image and click **Add**. Note that the previous port has been added (green underlined).

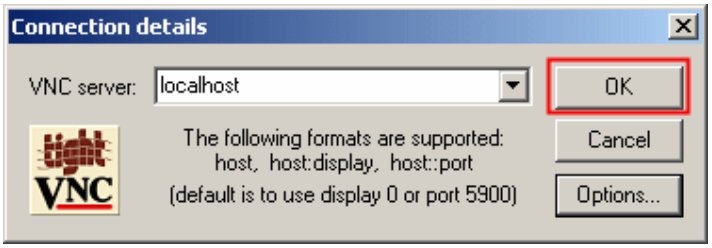


9) **In order to continue you need a valid account on the Relay System.** Now click **Open.** After few seconds a popup window like the following will ask you to accept the key of the remote Relay System.

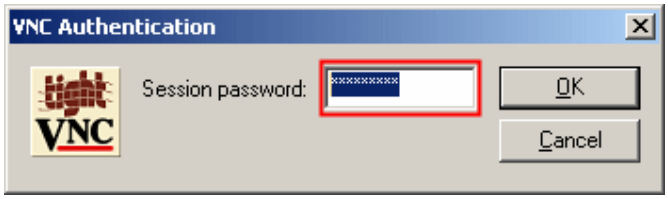


10) Click YES and in the next window type username and password. The ssh part is finally over ☺

11) Launch the TightVNC client (Fast compression or Best compression). The following screen appears:



12) Just click **OK**. If everything works fine now you should see the following screen:



13) Type the Managed PC TightVNC password that you set during the “Managed PC step by step installation instructions” click **OK** and you are on the way! Now you can fully access the Managed PC and help your friend/customer/partner.

Troubleshooting hints

If something goes wrong try to follow these hints to solve your problems.

From a command prompt type:

```
netstat -an
```

on both Viewer PC and Managed PC to see if the following two lines are present in the list that will be displayed after pressing the enter key:

```
  TCP    127.0.0.1:5800         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5900         0.0.0.0:0              LISTENING
```

If not, your tunnels have not being properly created by Putty.
Check your putty configuration to see if the tunnels have been properly configured.
Another possibility is that the port forwarding feature of sshd is disabled by the Relay System administrator. The only way you have to fix this is to contact him asking to re-enable the port forwarding.

NOTE: By default sshd is configured to allow port forwarding.

If you cannot connect to the Relay System try to reach the ssh server by issuing a:

```
telnet relaysystem 22
```

replace the relaysystem string with the address of the real Relay System you are connecting to.

As result you should see a line like this:

SSH-2.0-OpenSSH_3.5p1

This means that you can connect to the Relay Server and thus the firewall configuration is not a problem.

Double check your login/password and eventually ask the Relay System administrator for correct parameters regarding ssh authentication.