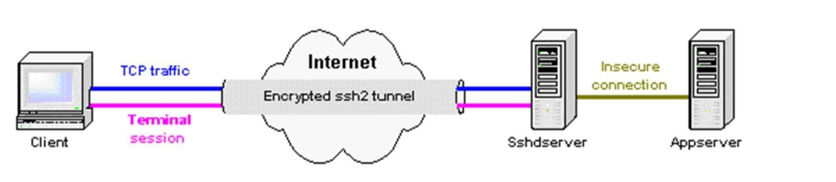
**Dept Computing TUD Private Cloud Connection from Windows Client Guide**



https://support.ssh.com/manuals/client-user/32/Tunneling\_Explained.html

**Introduction**

‘Local port forwarding’ forwards traffic coming into a local port to a specified remote port. For example, all traffic coming to port 1234 on the client could be forwarded to port 23 on the server (host).

Note: The value of localhost is resolved after the Secure Shell connection has been established - so when defining local forwarding (outgoing tunnels), localhost refers to the server (remote host computer) you have connected to.

Remote port forwarding does the opposite: it forwards traffic coming to a remote port to a specified local port. For example, all traffic coming to port 1234 on the server (host) could be forwarded to port 23 on the client (localhost).

**Note this doc uses example IP 192.168.1.1 as ‘final’ destination Windows 2022 server. You should change this to your assigned IP address.**

**Implementation**

**Part1 Establish CLGate Secure Tunnel**

TUD Tallaght Computing Gateway server is 193.1.127.10 for everyone (always!) cf. with TUD topology diagram. SSH Port is non-standard 2201 (note: ssh usually uses standard 22).

On Win desktop/laptop, open a command prompt; Brings you to your home directory which brings you to c:\users\whatever-you-login-as) and then under that there is a ‘**.ssh**’ folder starting with a dot.

**If it isn't there, it should be created.**



Navigate into it



Copy your private key into it. In this example, I am using user x12345678 and key id\_ed25519.x12345678.

Via windows file explorer, under ‘view’ tab, make sure you have both ‘file name extensions’ and ‘hidden items’ are ticked.

A screenshot of a computer

Description automatically generated

Navigate to the folder .ssh and create a config text file (right click new document file). this will create config.txt.

Rename it config. i.e. no txt extension.

Via Notepad, add the following content to it, replacing x12345678 with your own student number. Don’t forget to save it.

Host clgate

        Hostname 193.1.127.10

        User x12345678

        Port 2201

        IdentityFile    id\_ed25519.x12345678

Now test the ssh connection: Text

Description automatically generated

Type **yes <enter>** to continue connecting. If successful will see the welcome below.

A screenshot of a computer

Description automatically generated with medium confidence

Remember everything you type into the command prompt here will be executed on our dedicated SSH server cl-gate e.g.

Text

Description automatically generated

Break the connection, type **exit** **<enter>**.

Text

Description automatically generated

**Part 2. Create Tunnel end-point link**

**Windows Server**

This cl-gate server will be our gateway to tunnel to our endpoint server (check allocation spreadsheet or ask lecturer). In this case, I wish to RDP to endpoint Windows machine 172.16.0.2. So, I will add the following entry to the config file (of course, use your allocated end-point IP address) and save.

LocalForward 127.0.0.1:5902 172.16.0.2:3389

My config file now contains this:

Host clgate

Hostname 193.1.127.10

User x12345678

Port 2201

IdentityFile C:\Users\david\.ssh\id\_ed25519.x12345678

LocalForward 127.0.0.1:5902 172.16.0.2:3389

Now press CTRL+R and type mstsc <enter> to launch RDP. Enter Computer & port details 127.0.0.1:5902, which will now connect to 172.16.0.2 on remote port 3389. Click edit to add user credentials for remote server.

Graphical user interface, text, application

Description automatically generated

To login as Local Administrator use "\administrator" (or hostname\administrator, eg. win2019-01 \administrator) as user name, with "Computing1" as password.

Graphical user interface, application

Description automatically generated

Click ok and connect.

RDP Window will open with remote GUI presented.

When finished, close the RDP session AND log-off the gateway ssh session (using exit command).

