How to open a reverse tunnel through a Windows PC to access the LAN

What?

If you are trying to access a device on a NATted network, and cannot VPN in, you can use this to open a tunnel through a managed computer on the network, in order to access anything on that computer's LAN

Requirements

1. You need to have powershell (with admin privileges) access to a computer on the LAN (remote background via Syncro / Ninja / etc)
2. You need to have access to a cloud Linux server, a port will be opened on this cloud server that forwards traffic to a device on the computer's LAN network
3. The computer needs to have a network connection that can reach the cloud server

How To Connect

Video guide here: https://www.loom.com/share/883ebba6d93146ac82a0fdd45a16aeb1

> This guide assumes you have a Linux server running in the cloud
> You also need to have a public SSH key added to the authorized_keys file on the server
> We have one in the cloud already set up, use these commands to connect to it and open a

port redirect

1) Open remote background Powershell on a computer connected to the LAN

2) Install the Openssh client on the computer

```
Get-WindowsCapability -Online |  Where-Object Name -like 'OpenSSH*'
```

3) Download the SSH key for the Cloud Linux server, this will let us open a port on that server

```
(New-Object
System.Net.WebClient).DownloadFile("https://ssh.danbuntu.com/files/ceef6b96aa17610858b9eb11520
343e5de8fd0a47858dbef28145f5b96e12f9e", "C:\Windows\Temp\id_rsa_remote")
```

4) Open a reverse port forward to a specific device on the computer's LAN network

Make sure to change these variables to match your scenario

```
# remote IP address of the cloud server
# leave this as is, unless you are using a different server
$CLOUD_IP = "104.238.138.35"

# user name on the cloud server
# leave this as is, unless you changed it
$CLOUD_USER = "remote"

# remote port (on the cloud server) you will connect to
# this can be anything you want, as long as its not being used
$CLOUD_PORT = 65001

# local IP of the device you want to reach (on the LAN)
$LAN_IP = "192.168.1.1"

# local port of the device you want to reach (on the LAN)
$LAN_PORT = 8080



# open the connection
```

```
# if this works well, you should be able to connect to the CLOUD_IP:CLOUD_PORT, and it will redirect the connection to LAN_IP:LAN_PORT
#  [You]  ===>  [CLOUD_IP:CLOUD_PORT]  ==>  [LAN_IP:LAN_PORT]
ssh -o 'StrictHostKeyChecking no' -i C:\Windows\Temp\id_rsa_remote $CLOUD_USER@$CLOUD_IP -R $CLOUD_PORT`:$LAN_IP`:$LAN_PORT
```

How to set up a Linux Cloud Server

To set up a new cloud server to work with reverse port forwarding, do the following

1) SSH in to the server

2) Edit the file `/etc/ssh/sshd_config` and change the `GatewayPorts` to `yes`

```
sudo nano /etc/ssh/sshd_config
```

3) Restart the ssh server

```
sudo systemctl restart sshd
```

4) Create a SSH key and remote user, and save the public key the `authorized_keys` file for the remote user

```
# create ssh key pair
ssh-keygen -f ./sshkey -P ''

# create a user account for SSHing (username remote)
sudo useradd -m remote
sudo mkdir -p /home/remote/.ssh
sudo chown remote.remote -R /home/remote/.ssh
sudo chmod 700 -R /home/remote.ssh

# add the public key to the authorized_keys file for the remote user
sudo cat ./sshkey.pub > /home/remote/.ssh/authorized_keys
```

5) Download the `./sshkey` SSH key, you will need to save this to a publicly accessible location where the computer on the LAN can download it, it will use this key to authenticate with the remote server to open a reverse SSH tunnel

---

Revision #5
Created 1 September 2022 17:34:22
Updated 13 September 2022 17:18:24