Using PuTTY to Connect to vFXTs on Google Cloud

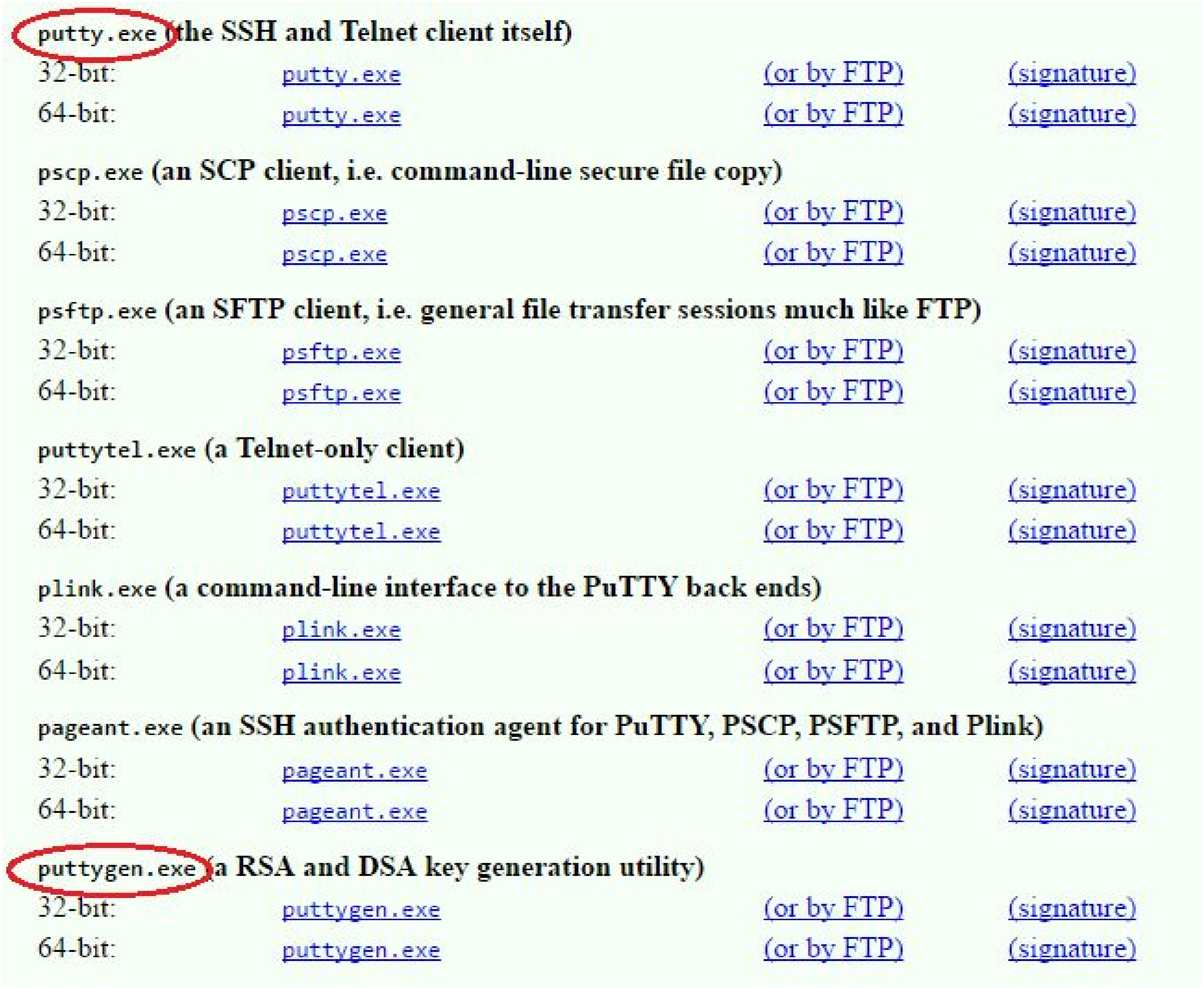
Process Overview

1. Download and Install PuTTY
2. Create SSH keys using puttygen
3. Copy key to virtual machine
4. Setup SSH session using PuTTY
5. Connect to Avere vFXT

This process assumes that an instance with a public IP address (like a NAT) is in the project.

Part 1: Download and Install PuTTY and Puttygen

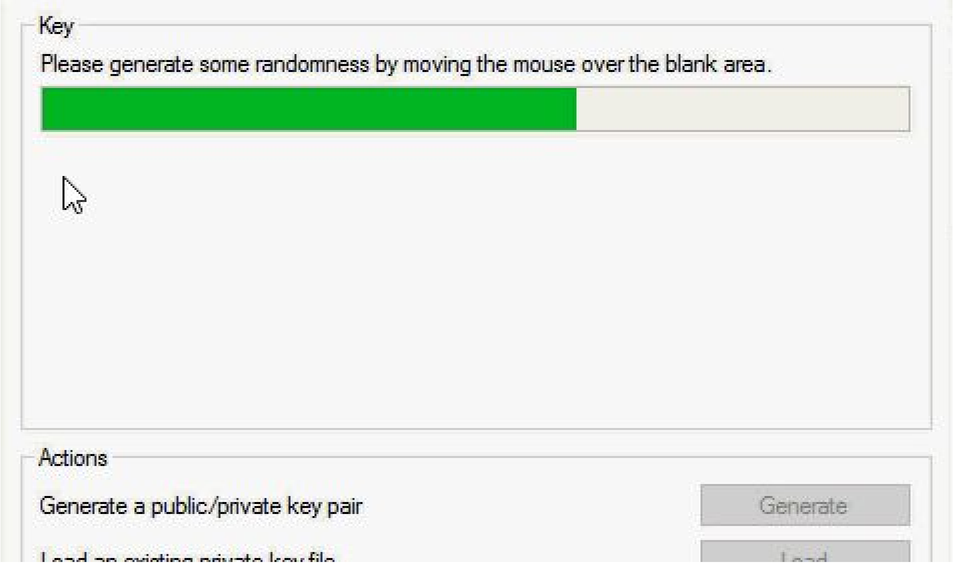
Download and install PuTTY and puttygen from the download page. This requires admin permissions on the local machine.



putty.exe (the SSH and Telnet client itself)			
32-bit:	putty.exe	(or by FTP)	(signature)
64-bit:	putty.exe	(or by FTP)	(signature)
pscp.exe (an SCP client, i.e. command-line secure file copy)			
32-bit:	pscp.exe	(or by FTP)	(signature)
64-bit:	pscp.exe	(or by FTP)	(signature)
psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)			
32-bit:	psftp.exe	(or by FTP)	(signature)
64-bit:	psftp.exe	(or by FTP)	(signature)
puttytel.exe (a Telnet-only client)			
32-bit:	puttytel.exe	(or by FTP)	(signature)
64-bit:	puttytel.exe	(or by FTP)	(signature)
plink.exe (a command-line interface to the PuTTY back ends)			
32-bit:	plink.exe	(or by FTP)	(signature)
64-bit:	plink.exe	(or by FTP)	(signature)
pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)			
32-bit:	pageant.exe	(or by FTP)	(signature)
64-bit:	pageant.exe	(or by FTP)	(signature)
puttygen.exe (a RSA and DSA key generation utility)			
32-bit:	puttygen.exe	(or by FTP)	(signature)
64-bit:	puttygen.exe	(or by FTP)	(signature)

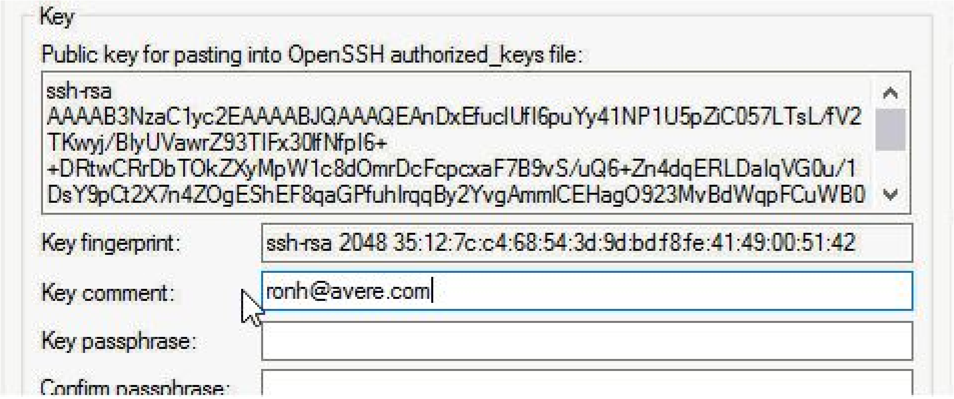
Part 2: Create SSH keys using puttygen

If not already installed, download and install putty from Intel software market.
Run puttygen.
Click **Generate**.
Move the mouse over the window to generate randomness.



Please generate some randomness by moving the mouse over the blank area.

Change the key comment to username@company.com. This does not have to be your real email address or company login. Example: ronh@avere.com. Note this username which is the part before the @ symbol. You will need it later.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAnDxEfuclUfI6puYy41NP1U5pZiC057LTsL/fV2
TKwyj/BlyUVawrZ93TIFx30lfNfpI6+
+DRtwCRrDbTOkZXyMpW1c8dOmrDcFcpcxaF7B9vS/uQ6+Zn4dqERLDalqVG0u/1
DsY9pCt2X7n4ZOgEShEF8qaGPfuhIrqqBy2YvgAmmlCEHagO923MvBdWqpFCuWB0
```

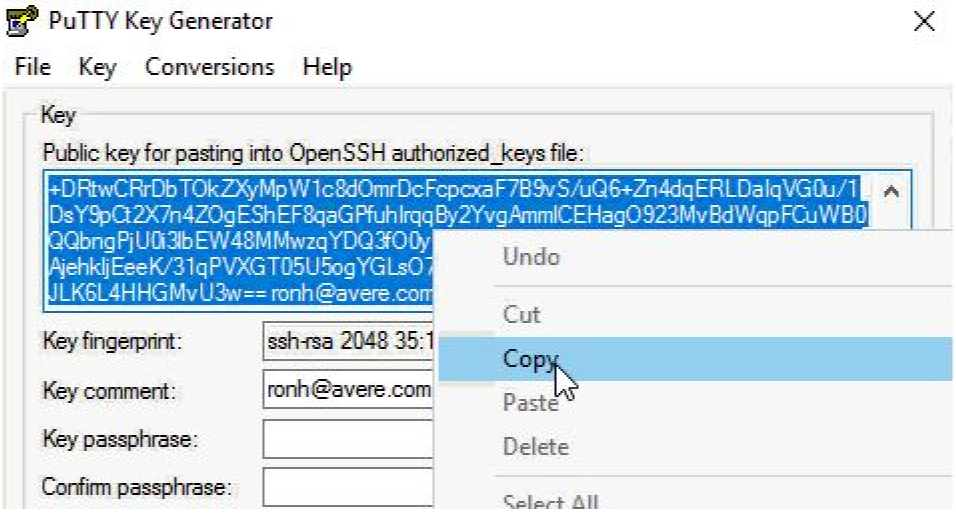
Key fingerprint: ssh-rsa 2048 35:12:7c:c4:68:54:3d:9d:bd:f8:fe:41:49:00:51:42

Key comment: ronh@avere.com

Click **Save private key** and **Yes**.
Navigate to a location that you will remember. Create a new folder if preferred.
Provide a name for the key like the username provided earlier and click **Save**.
Keep the puttygen window open for the next step.

Part 3: Copy key to virtual machine

Copy the key at the top of the window. Be sure to select everything.



Public key for pasting into OpenSSH authorized_keys file:

```
+DRtwCRrDbTOkZXyMpW1c8dOmrDcFcpcxaF7B9vS/uQ6+Zn4dqERLDalqVG0u/1
DsY9pCt2X7n4ZOgEShEF8qaGPfuhlrqqBy2YvgAmmlCEHagO923MvBdWqpFCuWB0
QQbngPjU0i3lbEW48MMwzqYDQ3fO0y
AjehkljEeeK/31qPVXGT05U5ogYGLsO7
JLK6L4HHGMvU3w== ronh@avere.com
```

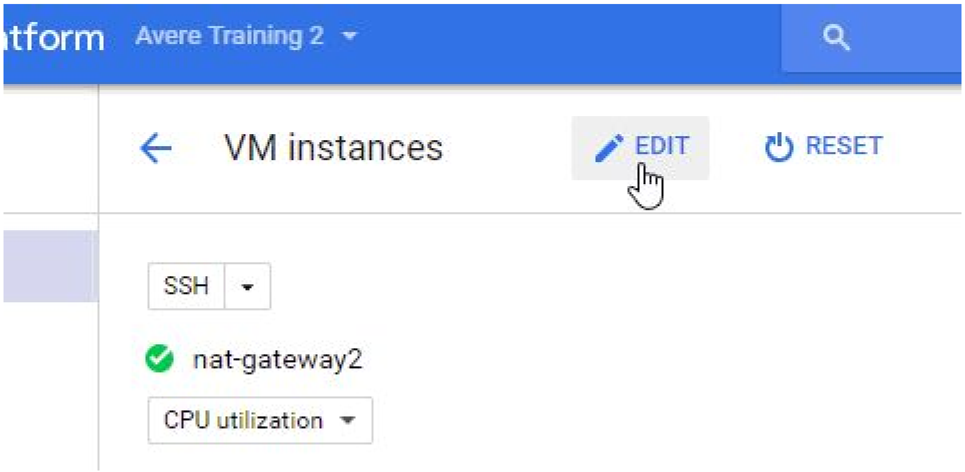
Key fingerprint: ssh-rsa 2048 35:1

Key comment: ronh@avere.com

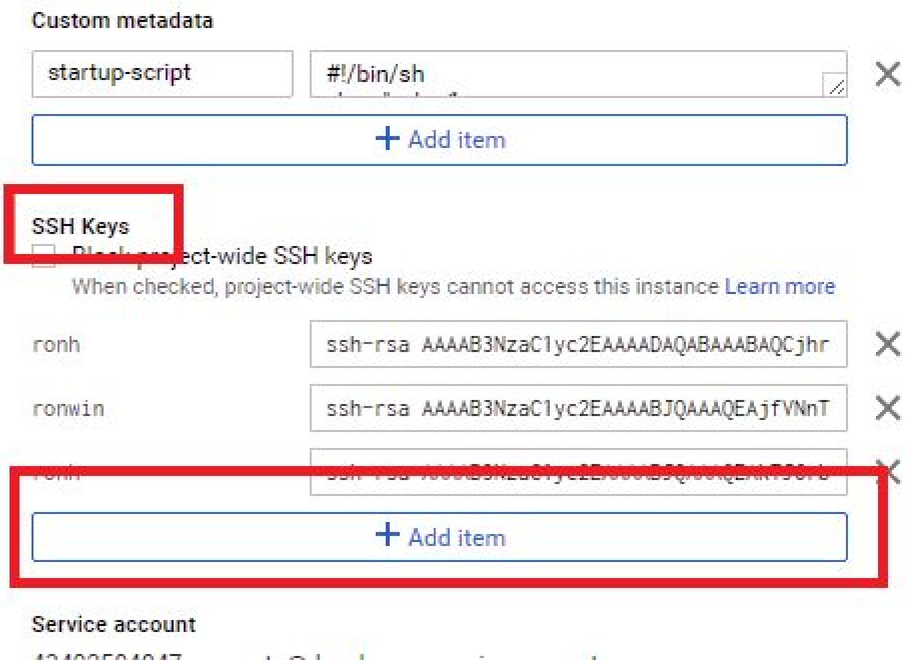
Key passphrase:

Confirm passphrase:

Navigate back to the Google Cloud Platform (GCP) console in your browser.
Click on the instance with the public IP address.
Click the **Edit** button at the top.



Scroll down to the SSH Keys section.
Click **Add item**.



Custom metadata

startup-script	#!/bin/sh

SSH Keys

□ Block project-wide SSH keys

When checked, project-wide SSH keys cannot access this instance Learn more

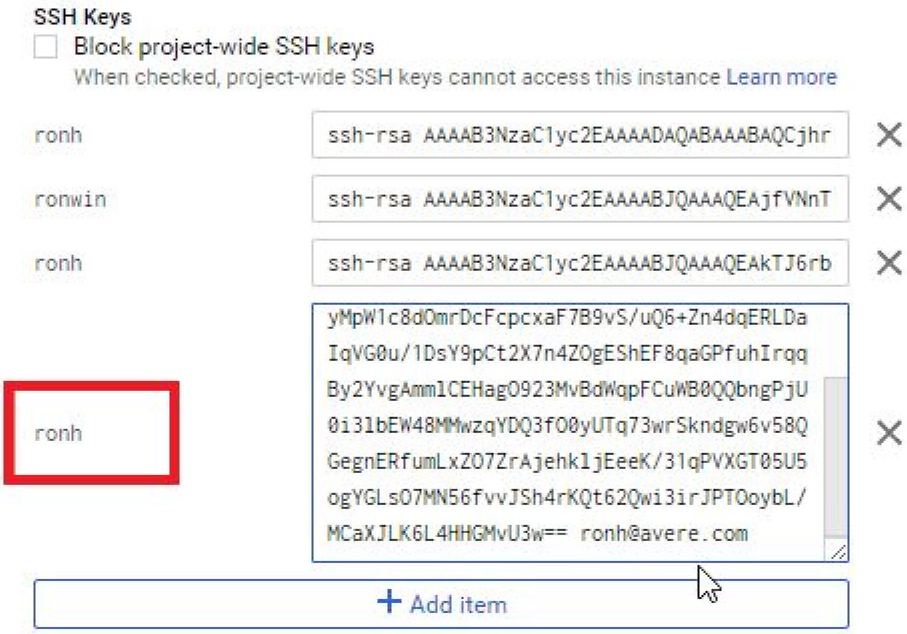
ronh	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjhr

ronwin	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAjfVNnT

ronh	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAkTJ6rb

Service account

Paste your key.
Verify it shows your username (like ronh).



SSH Keys

□ Block project-wide SSH keys

When checked, project-wide SSH keys cannot access this instance Learn more

ronh	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjhr

ronwin	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAjfVNnT

ronh	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAkTJ6rb

ronh

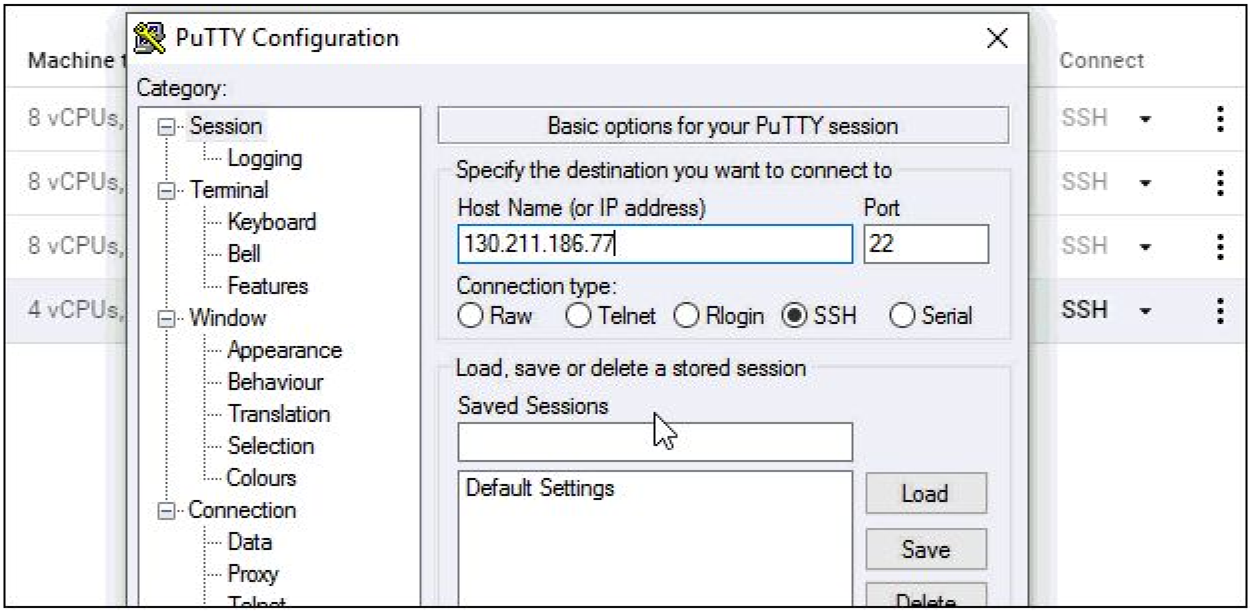
```
yMpW1c8dOmrDcFcpcxaF7B9vS/uQ6+Zn4dqERLDa
IqVG0u/1DsY9pCt2X7n4ZOgEShEF8qaGPfuhIrqq
By2YvgAmm1CEHagO923MvBdWqpFCuWB0QQbngPjU
0i31bEW48MMwzqYDQ3fO0yUTq73wrSkndgw6v58Q
GegnERfumLxZO7ZrAjehk1jEeeK/31qPVXGT05U5
ogYGLsO7MN56fvvJSh4rKQt62Qwi3irJPTOoybL/
MCaXJLK6L4HHGMvU3w== ronh@avere.com
```

Scroll to the bottom and click **Save**.

Part 4: Setup SSH session using PuTTY

This part requires the public IP address, a local port for tunneling, and the vFXT management IP address. If internet access requires a proxy server, you will need that information.

In the GCP console, copy the External IP address of the instance.
In putty, paste the External IP address in the “Host Name (or IP address)” field.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 130.211.186.77

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

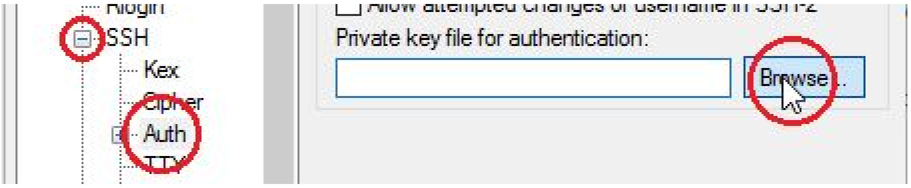
Saved Sessions

Default Settings

Enter a name for this stored session. Example: Avere vFXT
Click **Save**.

To add any proxy settings for your company’s proxy server, click **Proxy** on the left.

In the left navigation, click the **+** next to SSH.
Click **Auth**.
Click **Browse**.



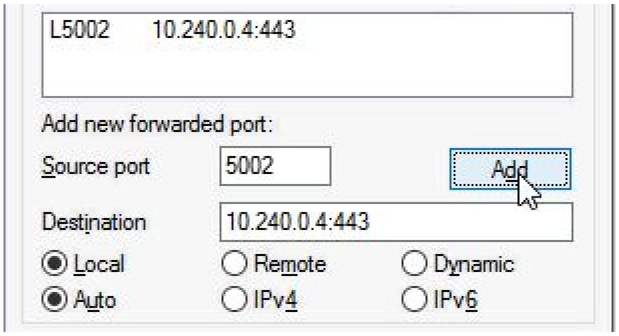
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

Navigate to the .ppk file from Part 2.
Double click the .ppk file.

Click **Tunnels** on the left.

Enter a port, like 8443, that you can use for tunneling in the Source port field. If this port is not available, please choose another port like 5002. To see what ports are available, run `netstat -p TCP -an |find "127.0.0.1"` to see local ports being used.
For the Destination, copy and paste the vFXT management IP address (example: 10.240.0.4).
Add **:443** to the end of the Destination.
Click **Add**.



L5002 10.240.0.4:443

Add new forwarded port:

Source port 5002

Destination 10.240.0.4:443

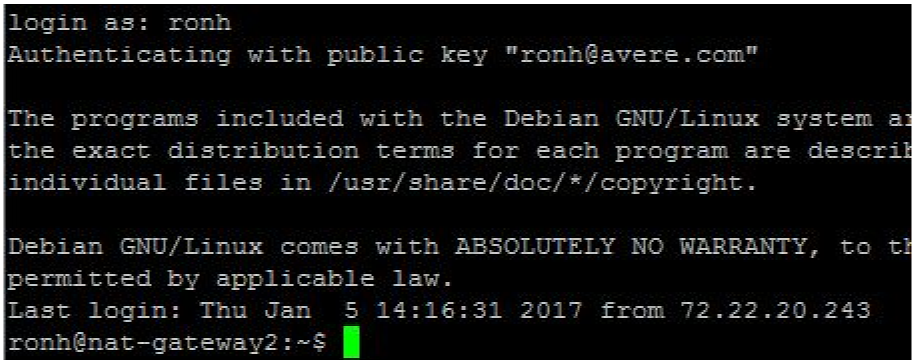
● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

Scroll to the top left and click **Session**.
Click the **Save** button on the right. This second Save session is required to keep your changes.

Part 5: Connect to Avere vFXT

From putty, click **Open** in the lower right.
Enter your username from Part 2. Do not include the @ symbol or anything after it. Example: ronh.
Press Enter and you should see a command prompt.



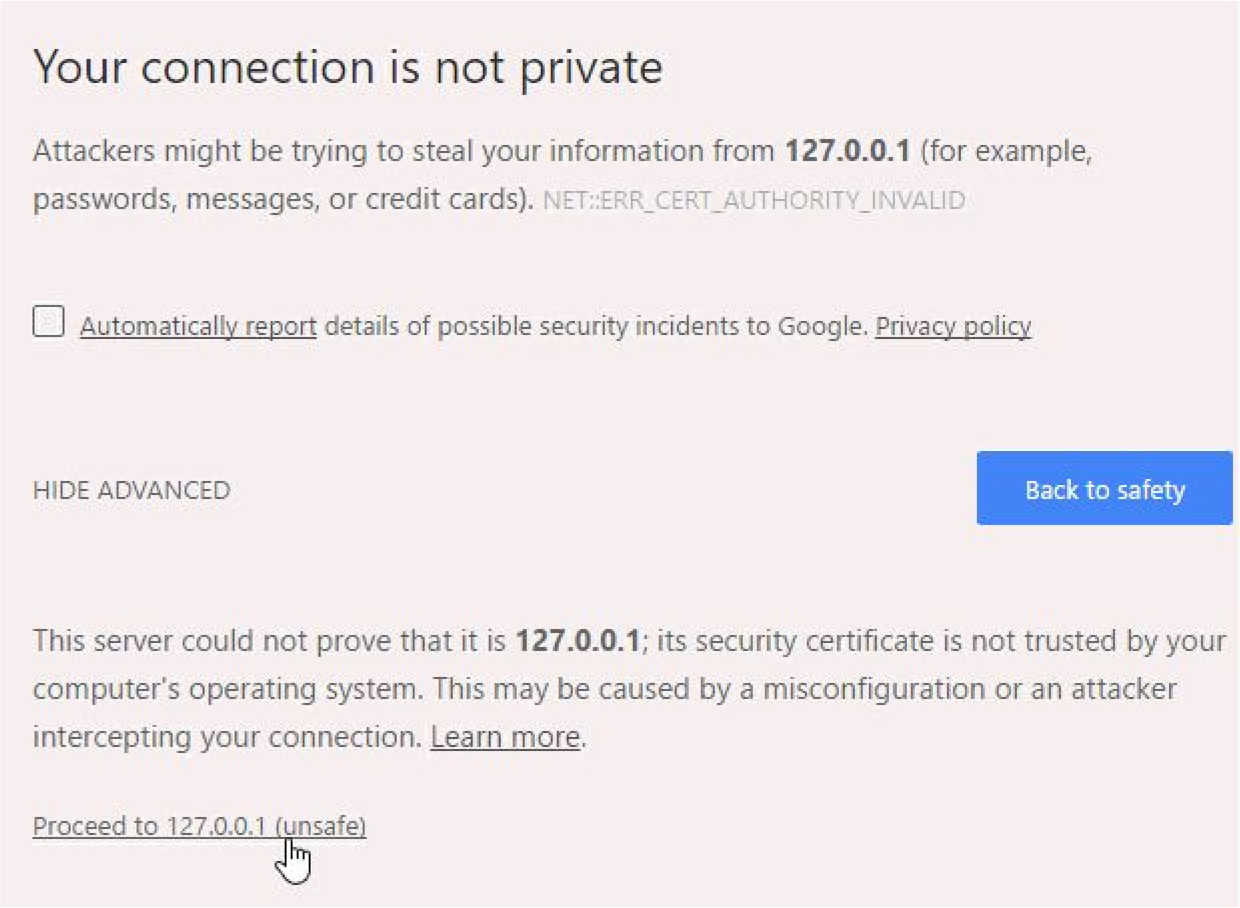
```
login as: ronh
Authenticating with public key "ronh@avere.com"

The programs included with the Debian GNU/Linux system a
the exact distribution terms for each program are descri
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to t
permitted by applicable law.
Last login: Thu Jan  5 14:16:31 2017 from 72.22.20.243
ronh@nat-gateway2:~$
```

In your browser, navigate to https://127.0.0.1:8443. Change the port if you used a different port. The browser will show that the session is not private. Indicate that you understand and navigate to it. In Chrome, for example, click **Advanced** in the lower left and then **Proceed to 127.0.0.1**.

At the Avere Control Panel, enter **admin** for the username and provide the password.



Your connection is not private

Attackers might be trying to steal your information from **127.0.0.1** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **127.0.0.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to 127.0.0.1 (unsafe)

Reconnecting

Virtual machines receive new IP addresses after each restart. When reconnecting to your cluster, you will need to provide the new public IP address in putty.

Open putty.
Select the Avere vFXT session that was previously saved.
Click **Load**.
Paste the new, public IP address in the “Host Name (or IP address)” field of putty.
Click **Save**.