

AWS free socks proxy over ssh

Requirements

1. Credit/Debit card with a balance of at least 1\$
2. Valid phone number that you can verify by either sms or voice.
3. [Putty](#)
4. [Firefox](#)

Disclaimer: This tutorial is intended for privacy and security purposes only. Do not use this guide to circumvent terms of service for online services or illegal activity. AWS services can incur fees if you go beyond the usage limits. Be sure to enable billing alerts and be aware of the usage limits.

Aws Setup.

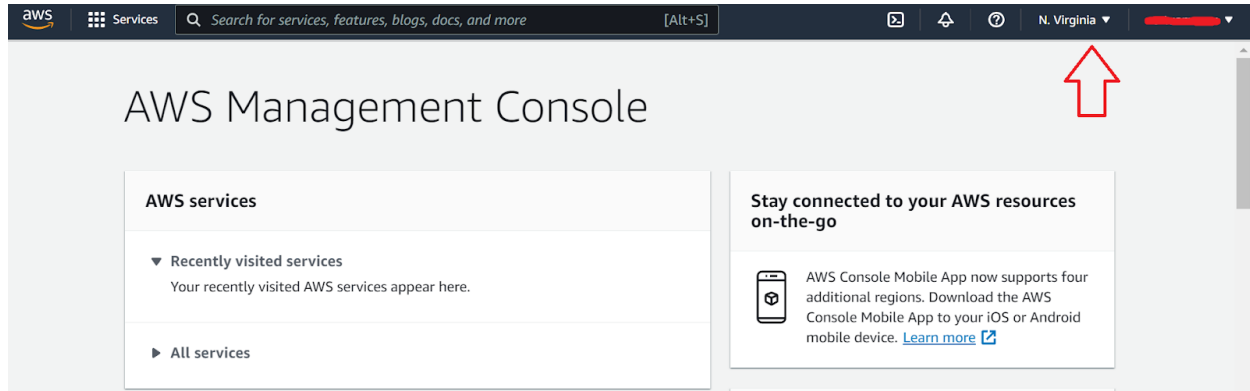
Create an account.

Go to [Cloud Services - Amazon Web Services \(AWS\)](#) and create a new account. Once you have done so, you can go to console.aws.amazon.com to log in. Select root user on the login screen and enter your email and password when prompted.

Selecting a region.

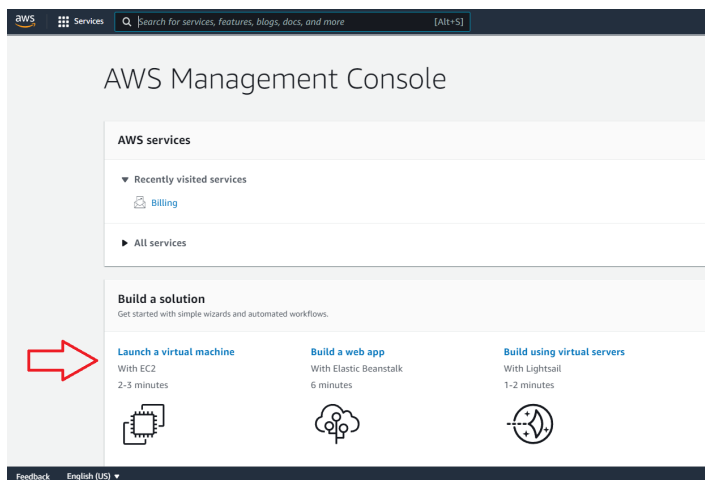
From the aws console screen, you may select a region for your account to be in. If the purpose of making this proxy is interfacing with a specific service, it is recommended you choose the amazon region closest to that server. This is a complicated topic as many online services are load balanced based of where the request is made from. But many server locations can be found by doing the google search “Company name server location”. If you are lucky you can get into the same datacenter as the server because many services use amazon for hosting.

To select the region, click next to the username and pick one. If prompted to confirm, hit continue.

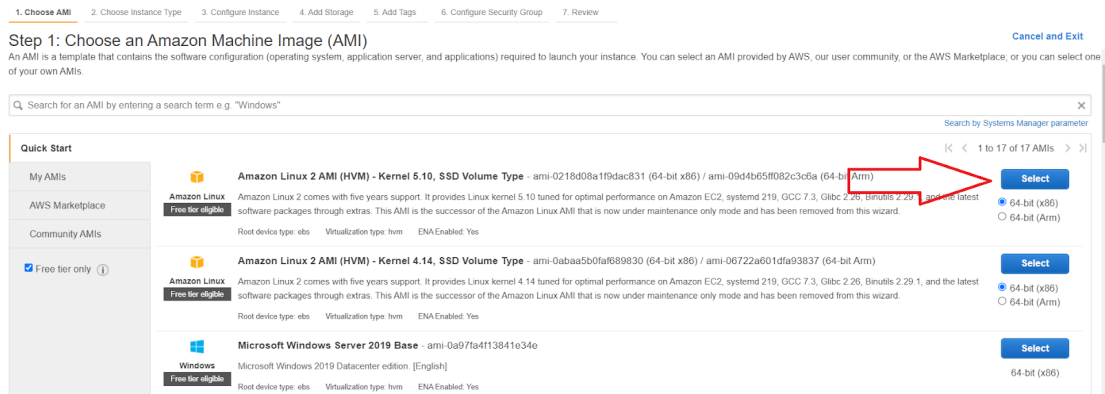


Create Server

- Confirm the aws console is set to the region you desire to host the server in.
- Click launch a virtual machine

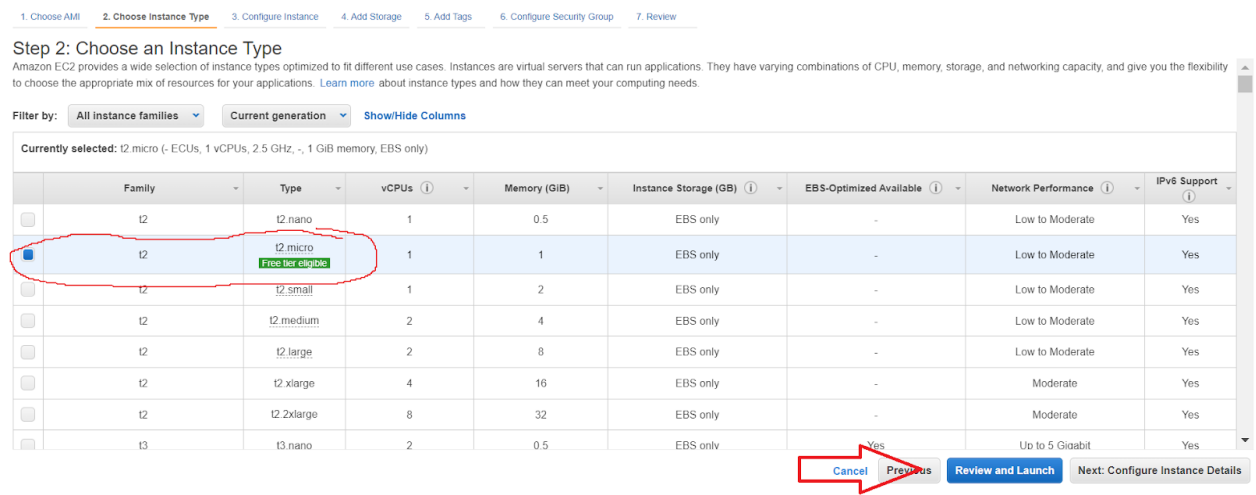


- c. Pick a free tier eligible linux server. It is easiest to pick the first option. The windows servers are not compatible with this tutorial.



- d. Select Instance Type.

The instance type t2.micro should be selected by default. Confirm it is selected and says free tier eligible and click review and launch at the bottom of the page.



- e. Launch instance

Click launch in the bottom right. If you would like to restrict connections to only your ip for added security, click edit security groups and change source to your ip. This can be done before or after the server is launched.

- f. Create encryption key pair for connections to the server.

After clicking launch in the previous step you will be prompted to create a key pair. It is recommended you keep this file on a thumb drive or use other measures to keep it safe.

1. Select create new keypair in the popup.
2. Select RSA
3. Set a name
4. Click download file.

Select an existing key pair or create a new key pair X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair ▼

Key pair type
☒ RSA ☐ ED25519

Key pair name
serverkeys

Download Key Pair

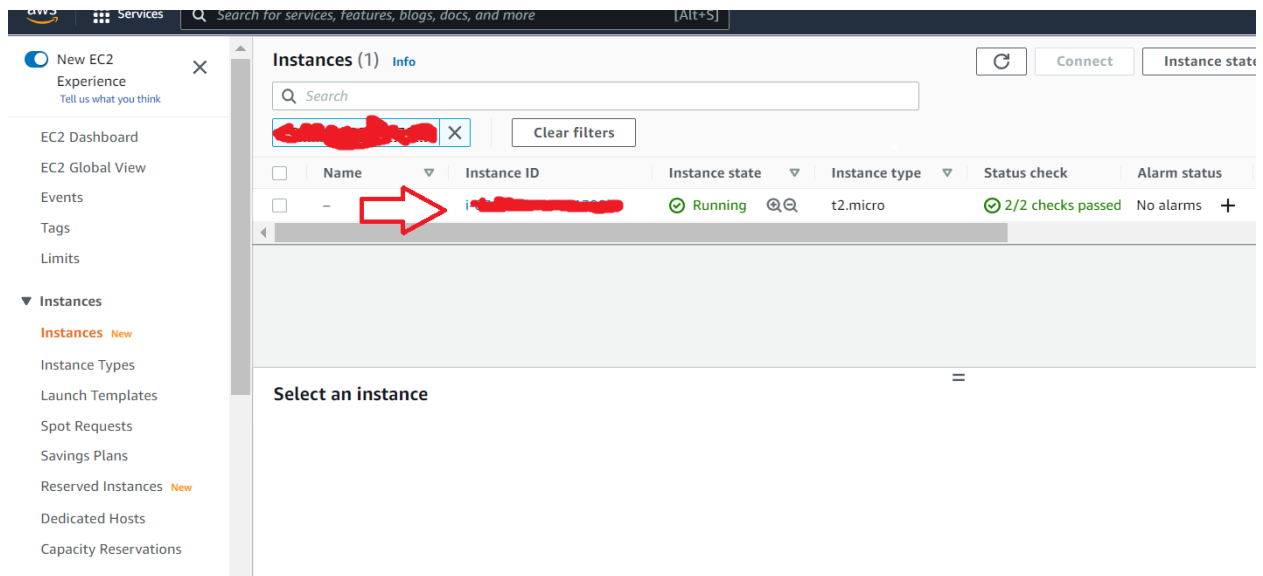
... You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

5. Click Launch instances to complete the setup.

g. Get server IP.

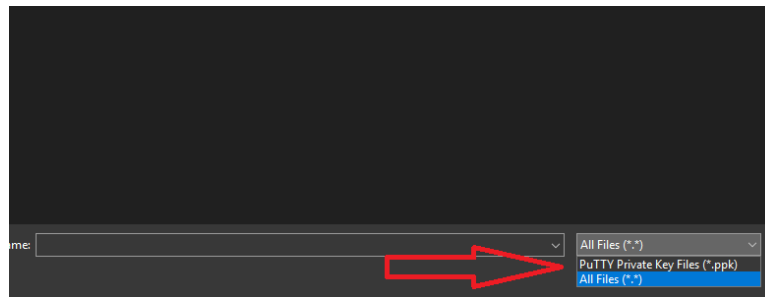
The server might take some time to get deployed by amazon. Usually from 1-30 minutes. To find the server in the management console go to console.aws.amazon.com and select EC2 from the list of recently used services. There you should see your instance listed. Click the instance ID.



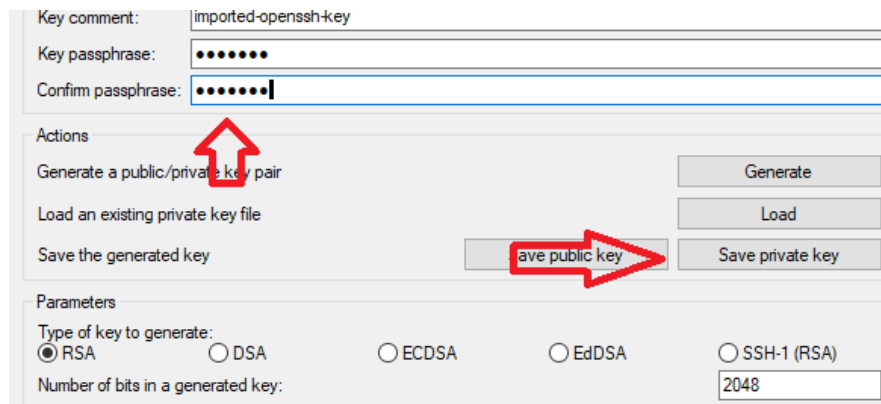
From the server instance screen you can verify it is running and copy the Public IPv4 address. You will need this for the configuration of putty on your machine.

Putty setup

- a. Set up private key for putty.
 1. Open the app PuTTYgen that was installed with putty and click load.
 2. Select all files in the file open dialog

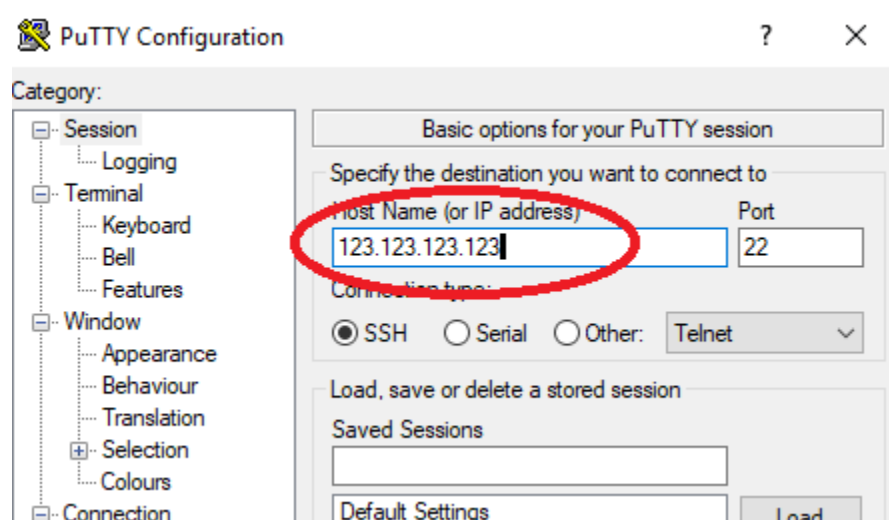


3. Locate the .pem file you created in section F of the server setup and open it.
4. Enter a password you will use to protect your key with and then save the private key.

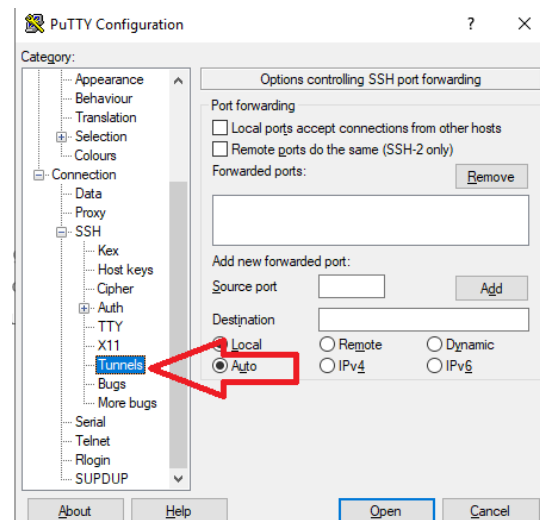


- b. Configure Putty
 1. Open PuTTY
 2. If you already use putty for other things then load the default configuration.

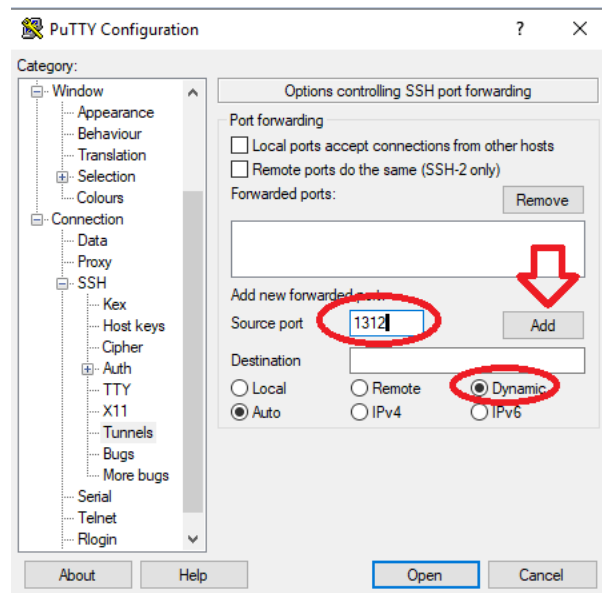
3. In the Host Name field, enter the IPv4 address collected in AWS Server Setup section G.



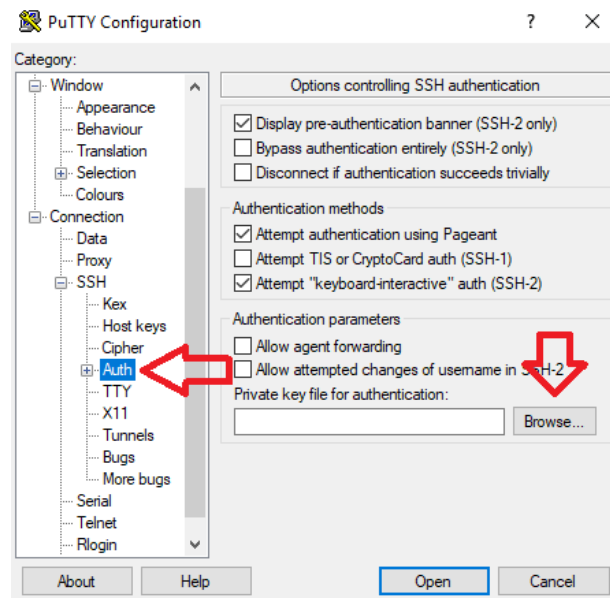
4. In the menu to the left, expand Connection>SSH and select tunnels.



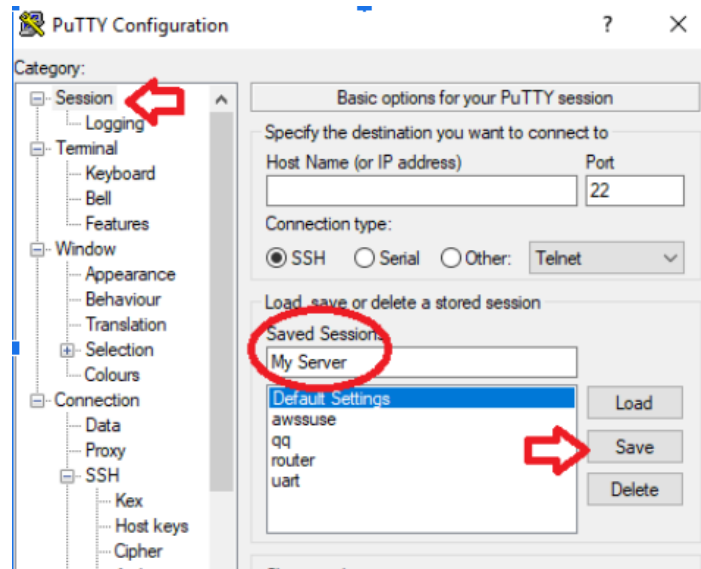
5. In the tunnels settings Enter a source port and select Dynamic. Then hit the Add button.



6. In the menu on the left select Auth under Connections>SSH. Then browse for the ppk file you created in section A of putty configuration.

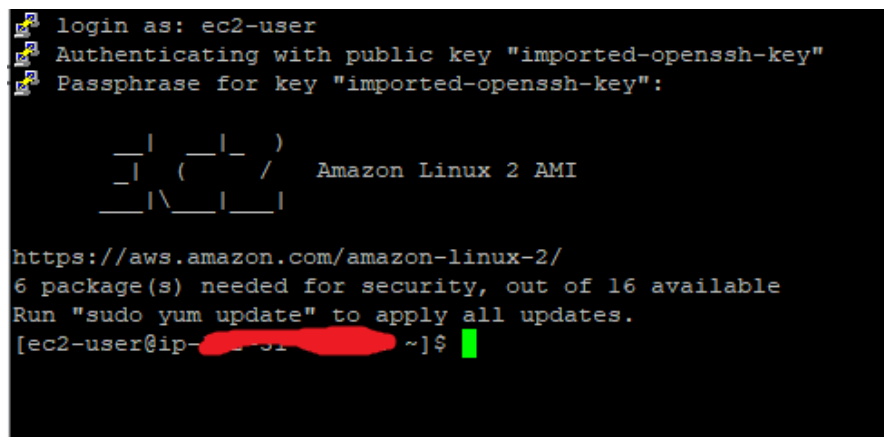


7. In the menu on the left scroll up and select Session. Enter a name for your server connection and click save.



c. Establishing SSH connection to AWS server

1. Open putty, select the server you saved in the previous step and click load.
2. Click open to begin the connection.
3. On first connection you will be prompted with a security alert. Click accept.
4. At the login prompt type the username **ec2-user** and hit enter. Then enter the password you created in Putty Configuration section A step 4 . Once you see the screen below, you are connected and the proxy is running.



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":

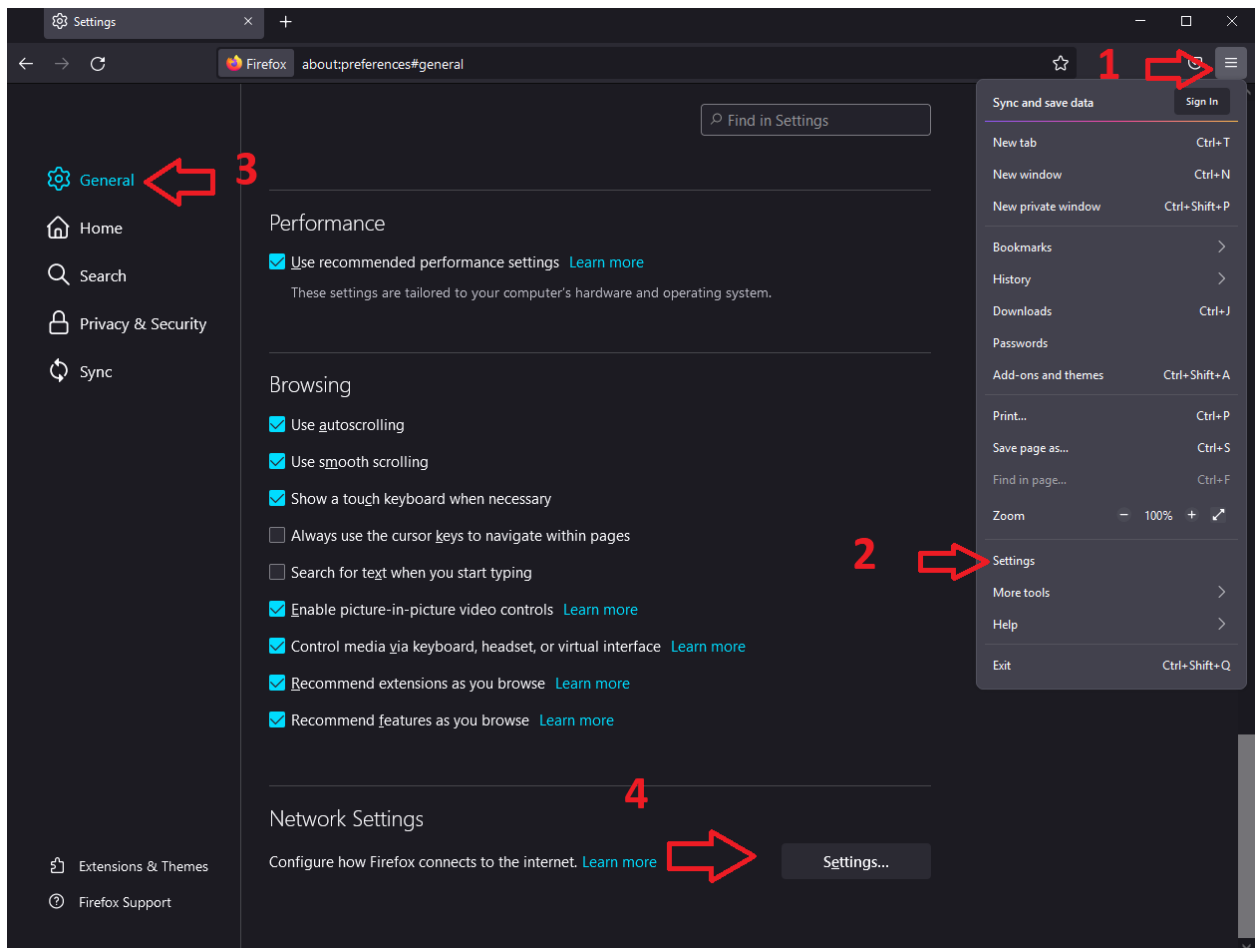
  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
6 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-... ~]$
```

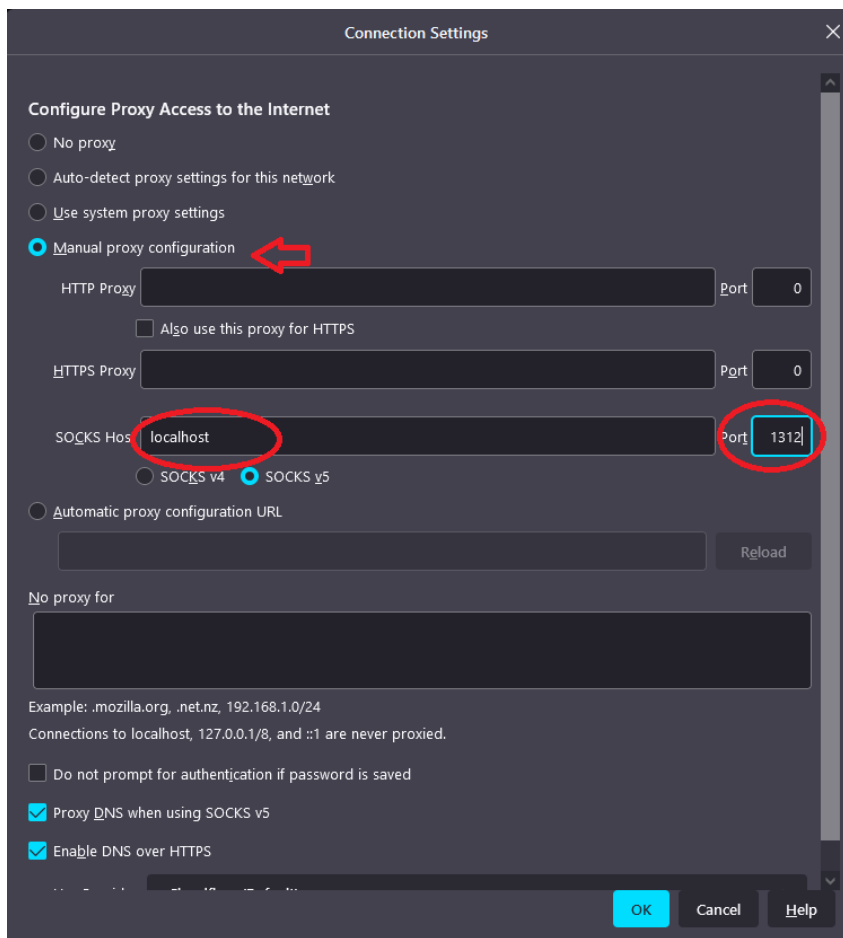
Note: If you see a message about packages needing updates for security it is advisable to type “sudo yum update” and follow the prompts to keep the server secure.

Firefox Configuration

A. Open Firefox and navigate to the network settings.



- B. In the network settings select manual proxy configuration then enter localhost under SOCKS host and the port you configured in putty for the port. Hit ok to save.



The browser will now route all traffic for firefox through putty to the amazon server. To disable, go to the network settings for firefox and set proxy to No proxy.

Note: Putty must be connected to the server or you will be unable to visit any websites using firefox unless you disable the proxy.