A CraSSH Course In SSH

Annette Mechelke
Women Who Code /connect, May 2022

Goal & Agenda

- Goals:
  - Gain familiarity with SSH
  - Use a SSH Config file
- Agenda
  - Overview of the SSH protocol
  - A little bit of cryptography
  - Some practical examples

- Who am I?
  - Software engineer who deploys code
  - Startup background
  - Not an infrastructure or networking expert

SSH Protocol

The **Secure Shell Protocol** (SSH) is a

cryptographic network protocol

for

operating network services securely over an unsecured network.

a definition of a secure way to communicate

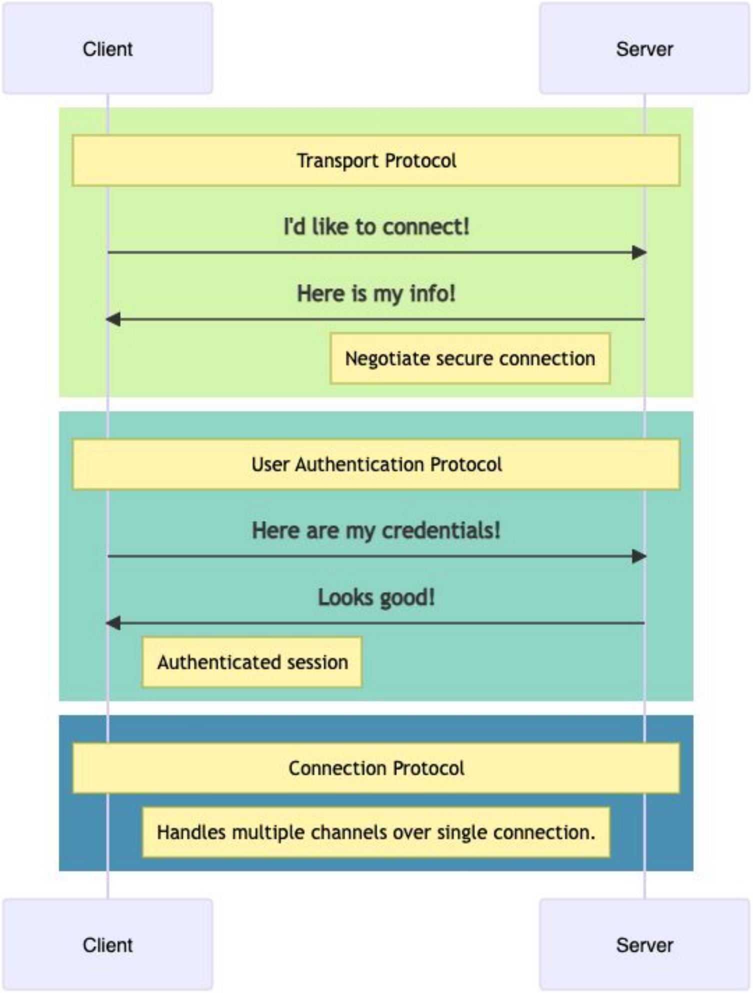
that allows you to execute programs securely over the internet

How did SSH become ubiquitous?

- Created in 1995, the beginning of the internet era
- Widely distributed open source implementation, OpenSSH
- Flexible architecture that is highly extensible.
- Supports many use cases

Protocol

- Client-server architecture
- Three sub-protocols:
  - Transport
  - User Authentication
  - Connection



Client

Server

Transport Protocol

I'd like to connect!

Here is my info!

Negotiate secure connection

User Authentication Protocol

Here are my credentials!

Looks good!

Authenticated session

Connection Protocol

Handles multiple channels over single connection.

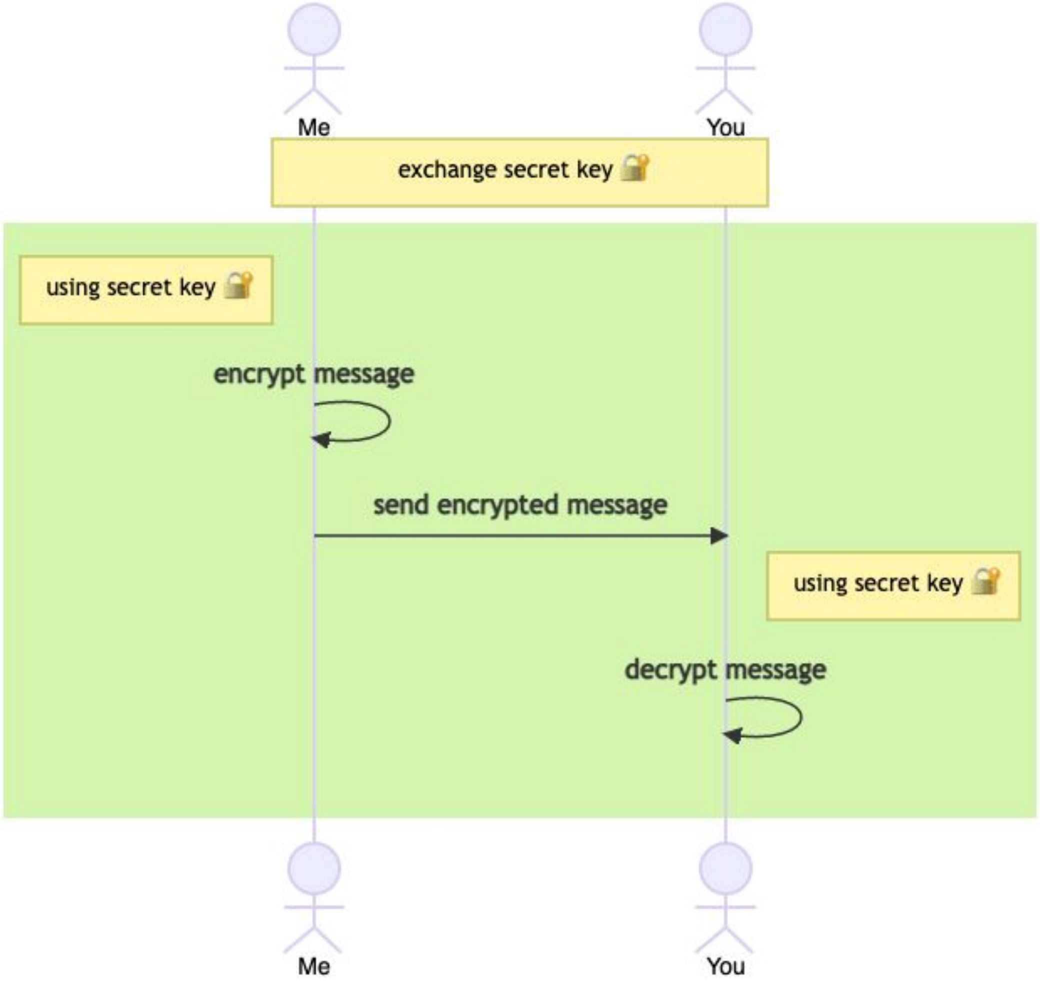
Client

Server

Cryptography Detour

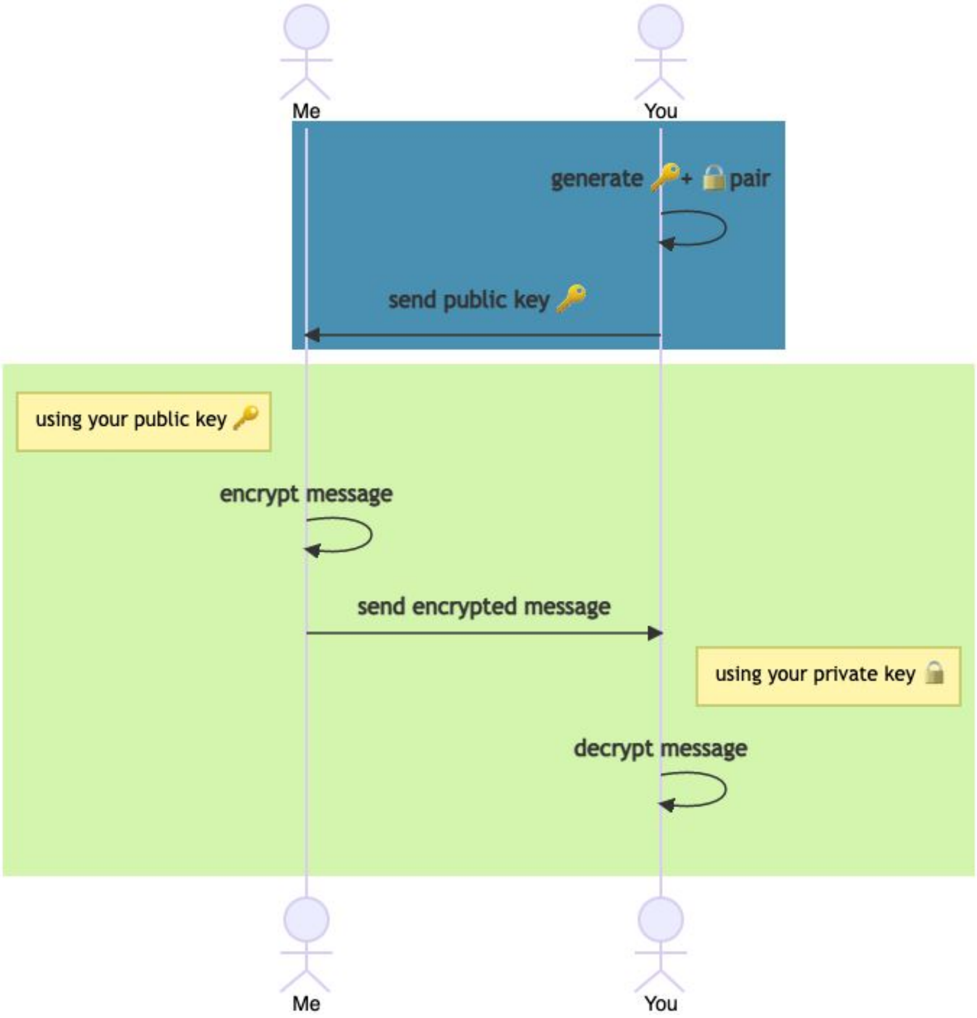
Symmetric Cryptography

- Parties exchanging messages needed to have access to the same shared key 🔐.
- **Symmetric** because the same key works in both directions.



Asymmetric Cryptography

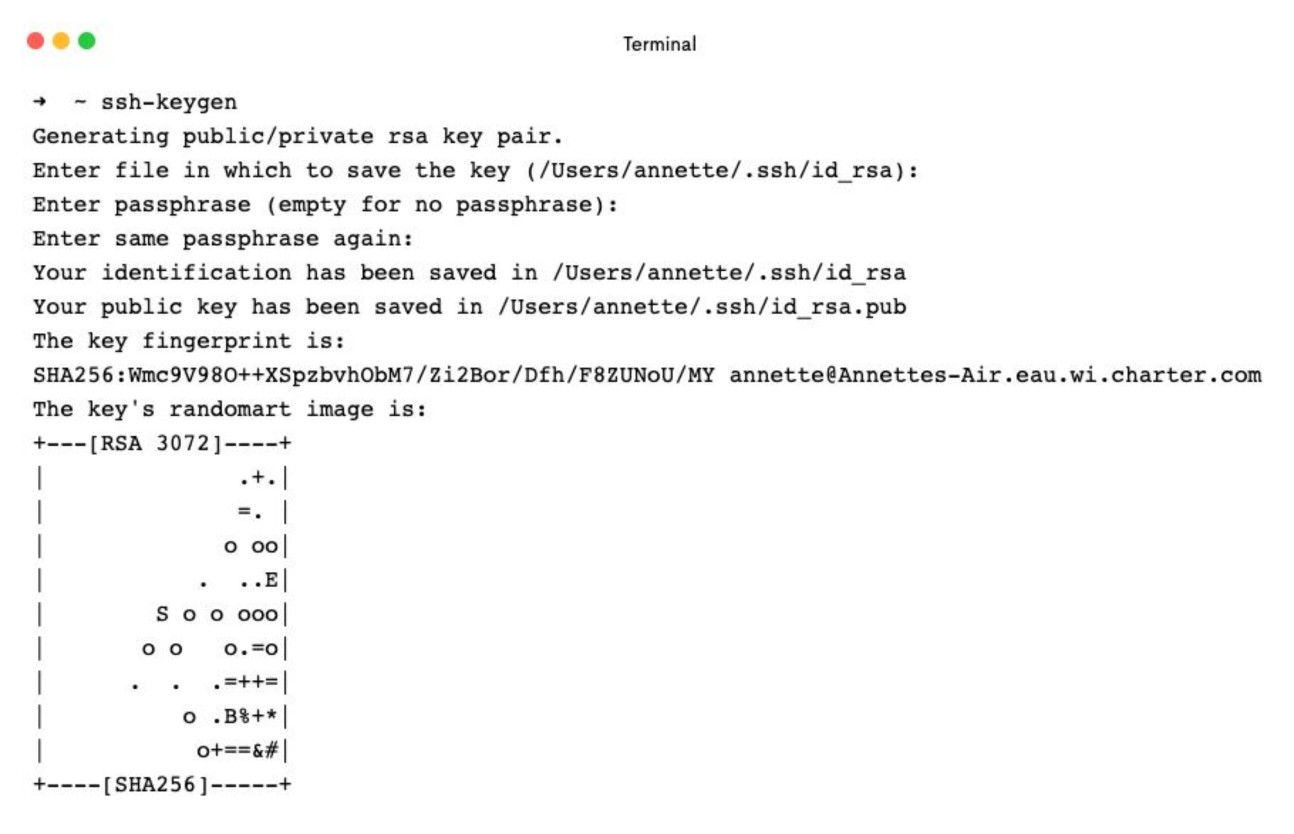
- **Asymmetric** algorithms rely on **key pairs** (🔑 + 🔒)
- A message encrypted with one key, 🔑, can only be decrypted by it's partner, 🔒
- Algorithms are based on "one way" mathematical function.



The Practical Bit

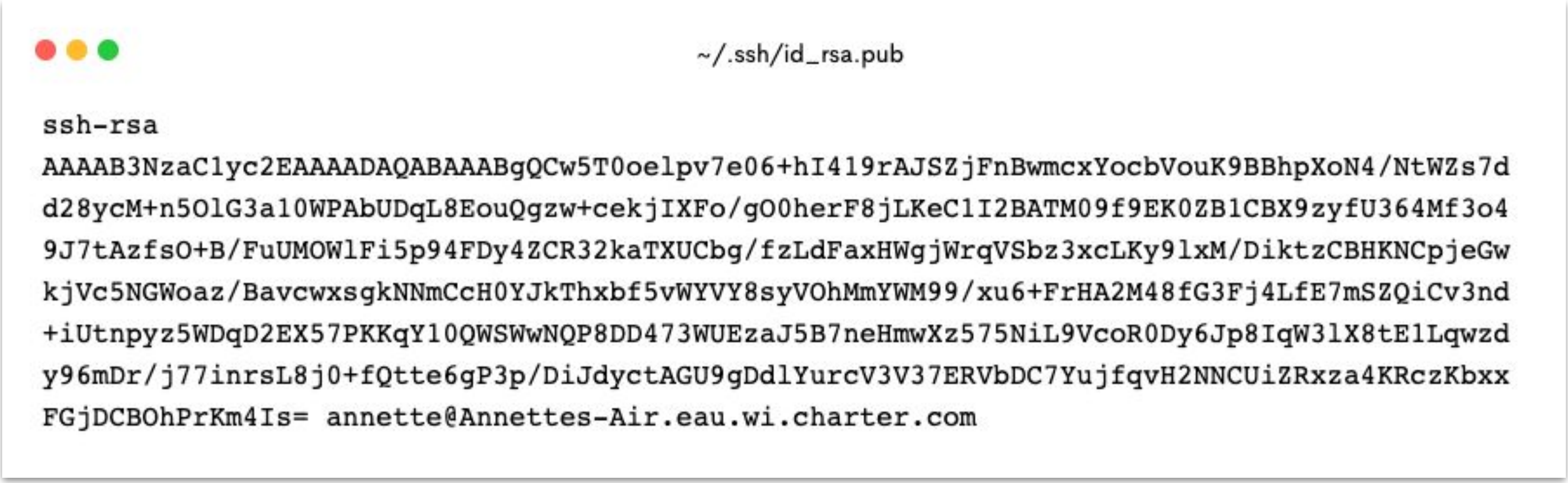
Use Case: Generate An SSH Key For Git

ssh-keygen



```
➜  ~ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/annette/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/annette/.ssh/id_rsa
Your public key has been saved in /Users/annette/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Wmc9V98O++XSpzbvhObM7/Zi2Bor/Dfh/F8ZUNoU/MY annette@Annettes-Air.eau.wi.charter.com
The key's randomart image is:
+---[RSA 3072]----+
|              .+.|
|              =. |
|             o oo|
|           .  ..E|
|        S o o ooo|
|       o o   o.=o|
|      .  .  .=++=|
|          o .B%+*|
|           o+==&#|
+----[SHA256]-----+
```

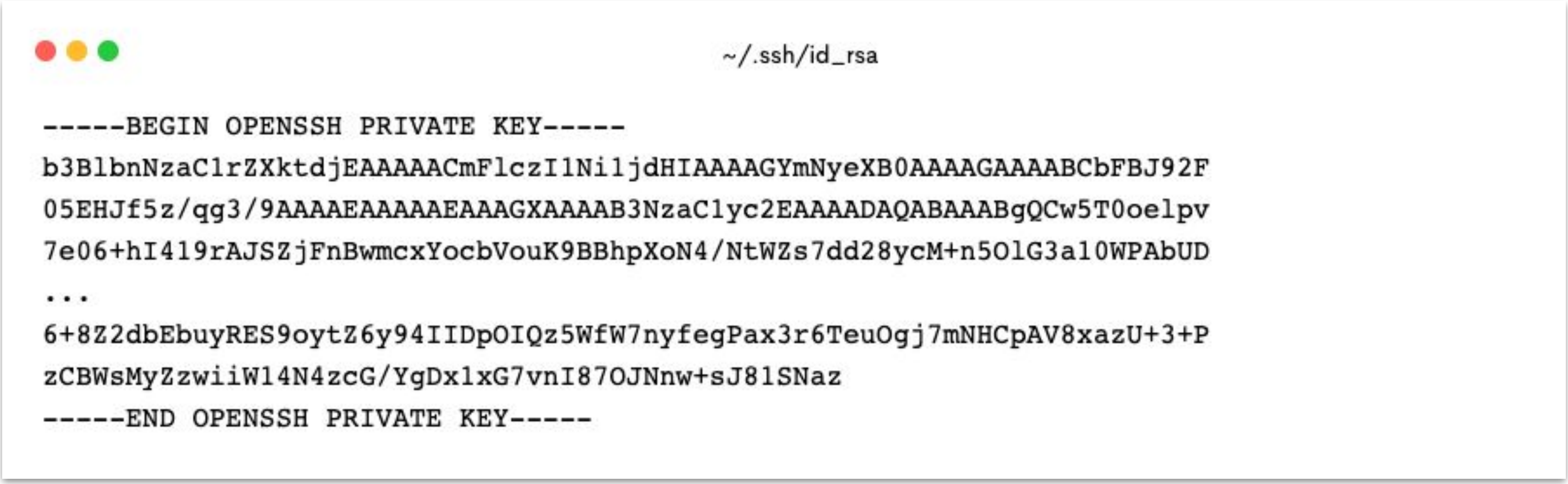
Key Files



~/.ssh/id_rsa.pub

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCw5T0oelpv7e06+hI419rAJSZjFnBwmcxYocbVouK9BBhpXoN4/NtWZs7d
d28ycM+n5OlG3al0WPAbUDqL8EouQgzw+cekjIXFo/gO0herF8jLKeC1I2BATM09f9EK0ZB1CBX9zyfU364Mf3o4
9J7tAzfsO+B/FuUMOWlFi5p94FDy4ZCR32kaTXUCbg/fzLdFaxHWgjWrqVSbz3xcLKy9lxM/DiktzCBHKNCpjeGw
kjVc5NGWoaz/BavcwxsgkNNmCcH0YJkThxbf5vWYVY8syVOhMmYWM99/xu6+FrHA2M48fG3Fj4LfE7mSZQiCv3nd
+iUtnpyz5WDqD2EX57PKKqY10QWSWwNQP8DD473WUEzaJ5B7neHmwXz575NiL9VcoR0Dy6Jp8IqW3lX8tE1Lqwzd
y96mDr/j77inrsL8j0+fQtte6gP3p/DiJdyctAGU9gDdlYurcV3V37ERVbDC7YujfqvH2NNCUiZRxza4KRczKbxx
FGjDCBOhPrKm4Is= annette@Annettes-Air.eau.wi.charter.com
```

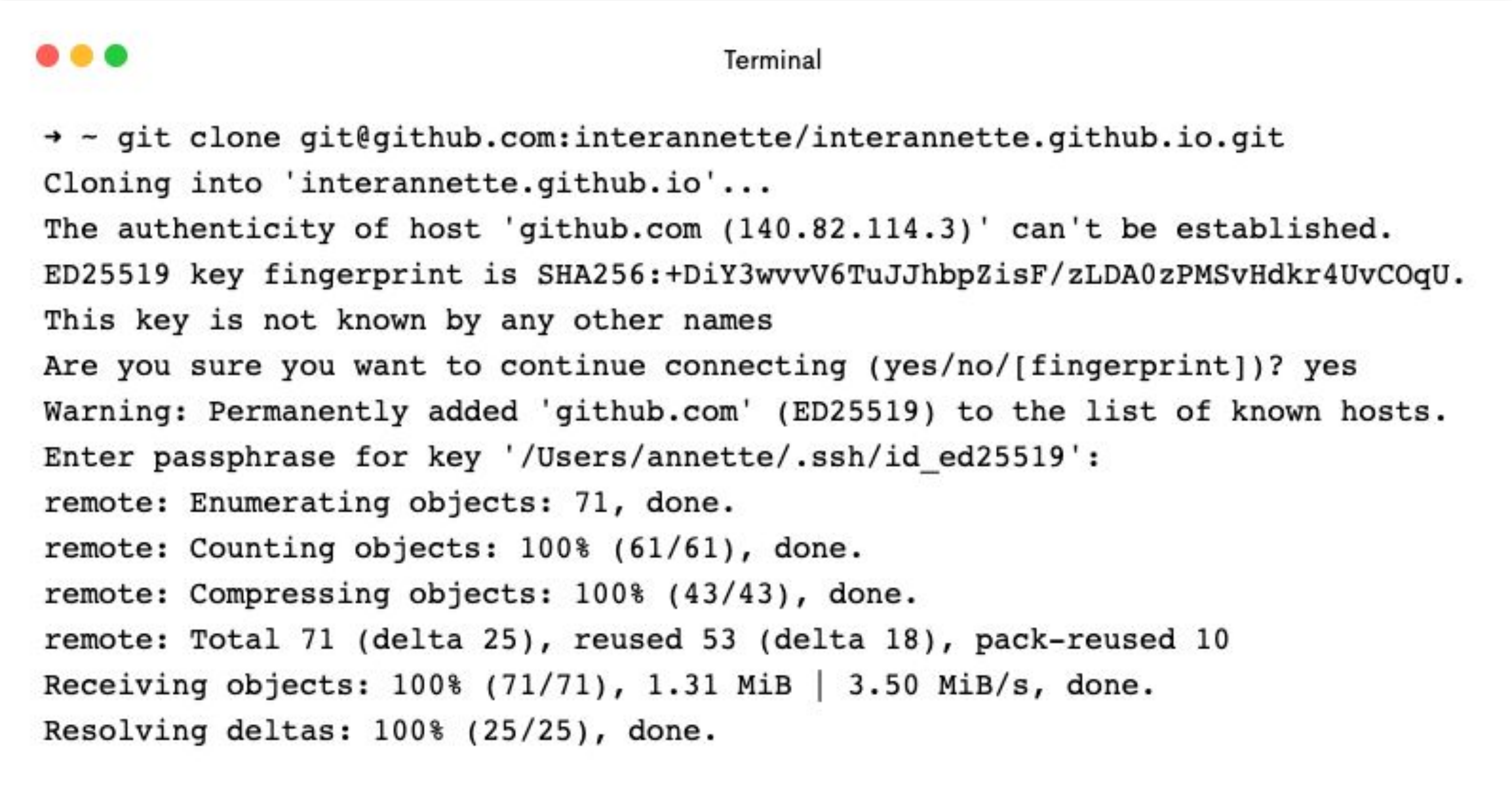
Key Files



~/.ssh/id_rsa

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCbFBJ92F
05EHJf5z/qg3/9AAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCw5T0oelpv
7e06+hI419rAJSZjFnBwmcxYocbVouK9BBhpXoN4/NtWZs7dd28ycM+n5OlG3a10WPAbUD
...
6+8Z2dbEbuyRES9oytZ6y94IIDpOIQz5WfW7nyfegPax3r6TeuOgj7mNHCpAV8xazU+3+P
zCBWsMyZzwiiW14N4zcG/YgDx1xG7vnI87OJNnw+sJ81SNaz
-----END OPENSSH PRIVATE KEY-----
```

Git



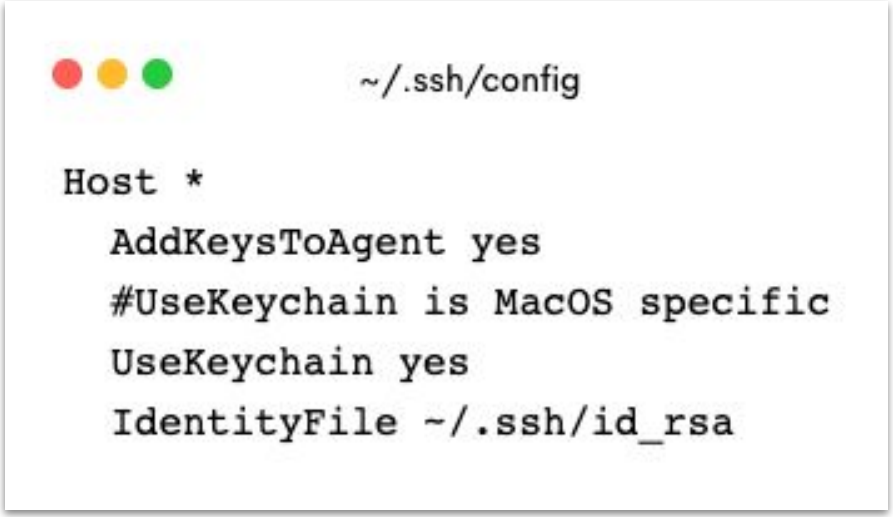
```
➜ ~ git clone git@github.com:interannette/interannette.github.io.git
Cloning into 'interannette.github.io'...
The authenticity of host 'github.com (140.82.114.3)' can't be established.
ED25519 key fingerprint is SHA256:+DiY3wvvV6TuJJhbpZisF/zLDA0zPMSvHdkr4UvCOqU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'github.com' (ED25519) to the list of known hosts.
Enter passphrase for key '/Users/annette/.ssh/id_ed25519':
remote: Enumerating objects: 71, done.
remote: Counting objects: 100% (61/61), done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 71 (delta 25), reused 53 (delta 18), pack-reused 10
Receiving objects: 100% (71/71), 1.31 MiB | 3.50 MiB/s, done.
Resolving deltas: 100% (25/25), done.
```

It works!

But it’s not easy...

We can make it easy by adding a config file.

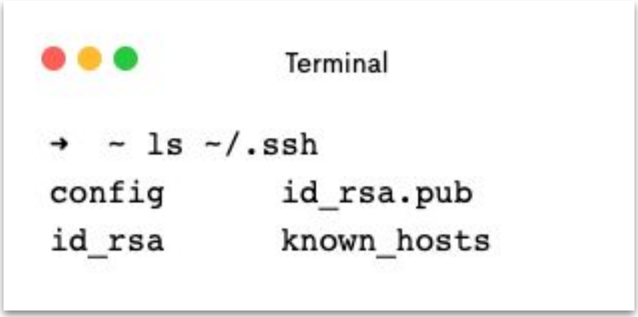
Config File



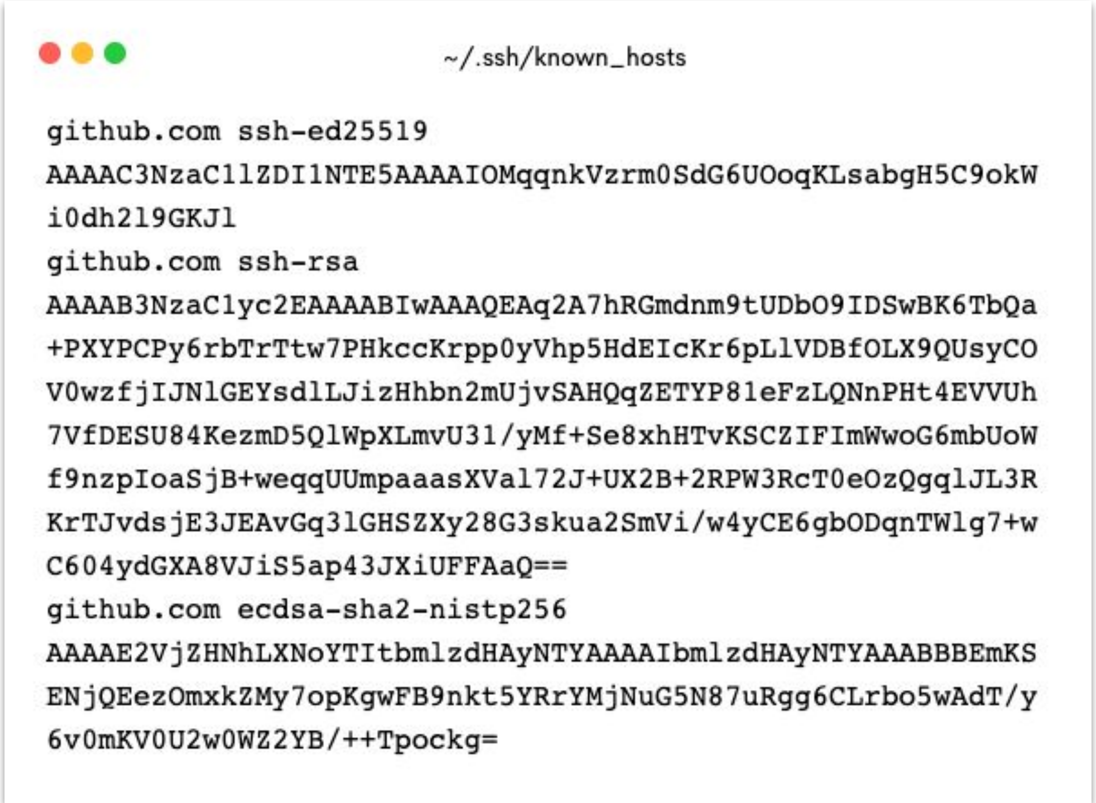
~/.ssh/config

```
Host *
  AddKeysToAgent yes
  #UseKeychain is MacOS specific
  UseKeychain yes
  IdentityFile ~/.ssh/id_rsa
```

Client ~/.ssh



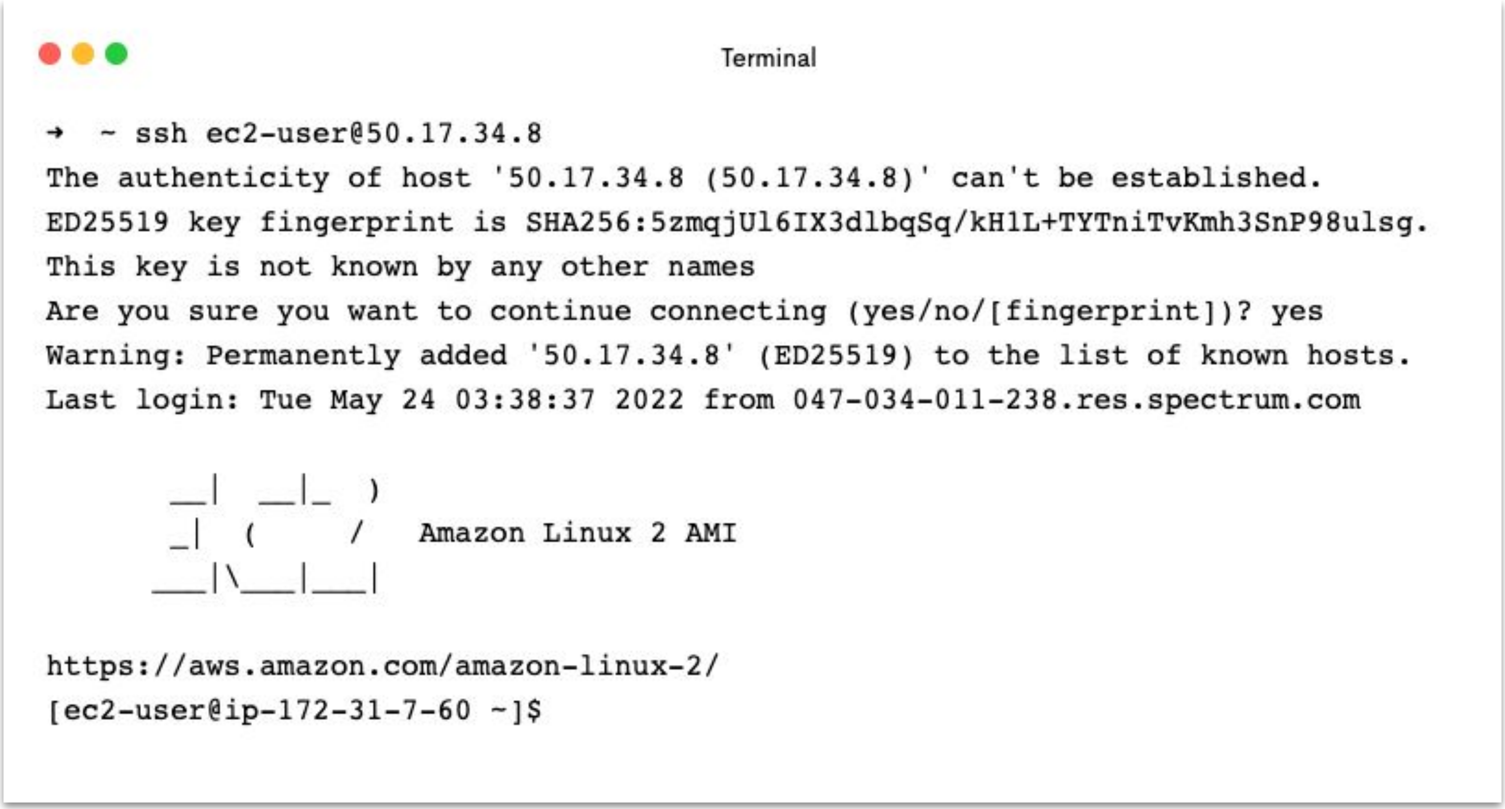
```
➜  ~ ls ~/.ssh
config      id_rsa.pub
id_rsa      known_hosts
```



```
github.com ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIOMqqnkVzrm0SdG6UOoqKLsabgH5C9okW
i0dh2l9GKJl
github.com ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAq2A7hRGmdnm9tUDbO9IDSwBK6TbQa
+PXYPCPy6rbTrTtw7PHkccKrpp0yVhp5HdEIcKr6pLlVDBfOLX9QUsyCO
V0wzfjIJNlGEYsdlLJizHhbn2mUjvSAHQqZETYP81eFzLQNnPHt4EVVUh
7VfDESU84KezmD5QlWpXLmvU31/yMf+Se8xhHTvKSCZIFImWwoG6mbUoW
f9nzpIoaSjB+weqqUUmpaaasXVal72J+UX2B+2RPW3RcT0eOzQgqlJL3R
KrTJvdsjE3JEAvGq3lGHSZXy28G3skua2SmVi/w4yCE6gbODqnTWlg7+w
C604ydGXA8VJiS5ap43JXiUFFAaQ==
github.com ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEmKS
ENjQEezOmxkZMy7opKgwFB9nkt5YRrYMjNuG5N87uRgg6CLrbo5wAdT/y
6v0mKV0U2w0WZ2YB/++Tpockg=
```

Use Case: Run An Application In The Cloud

ssh <user>@<host>



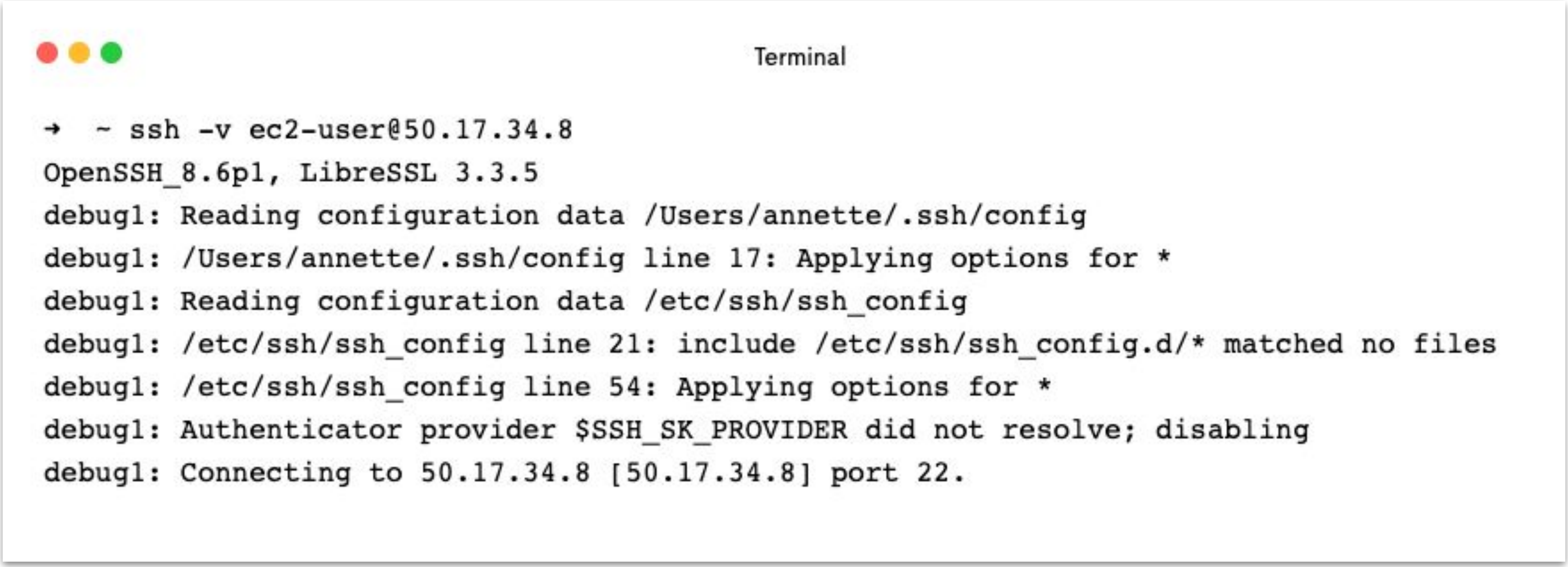
```
➜  ~ ssh ec2-user@50.17.34.8
The authenticity of host '50.17.34.8 (50.17.34.8)' can't be established.
ED25519 key fingerprint is SHA256:5zmqjUl6IX3dlbqSq/kH1L+TYTniTvKmh3SnP98ulsg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '50.17.34.8' (ED25519) to the list of known hosts.
Last login: Tue May 24 03:38:37 2022 from 047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-7-60 ~]$
```

It didn’t work!

What went wrong?

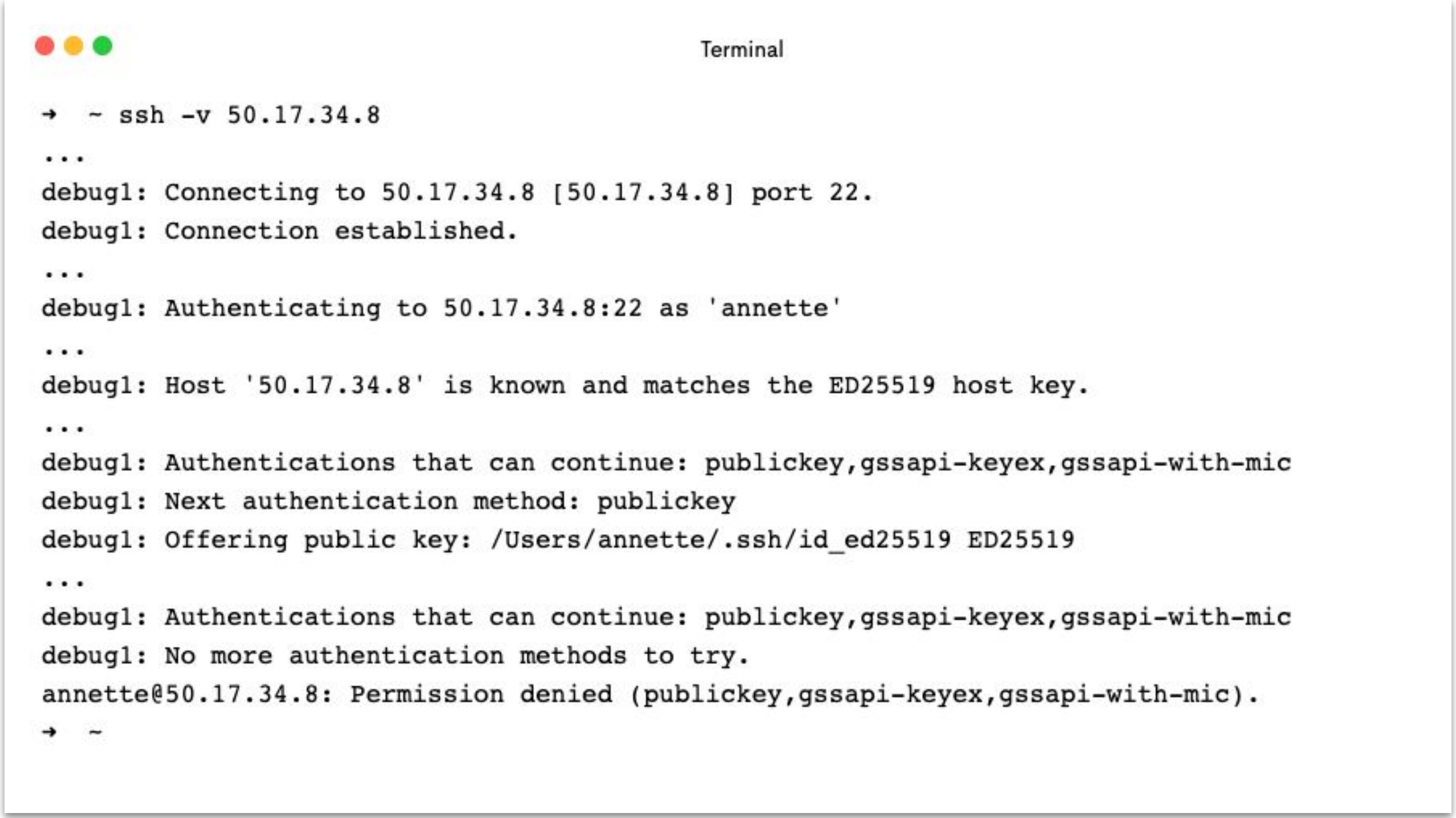
`-v` to the rescue!

Transport Layer Issues



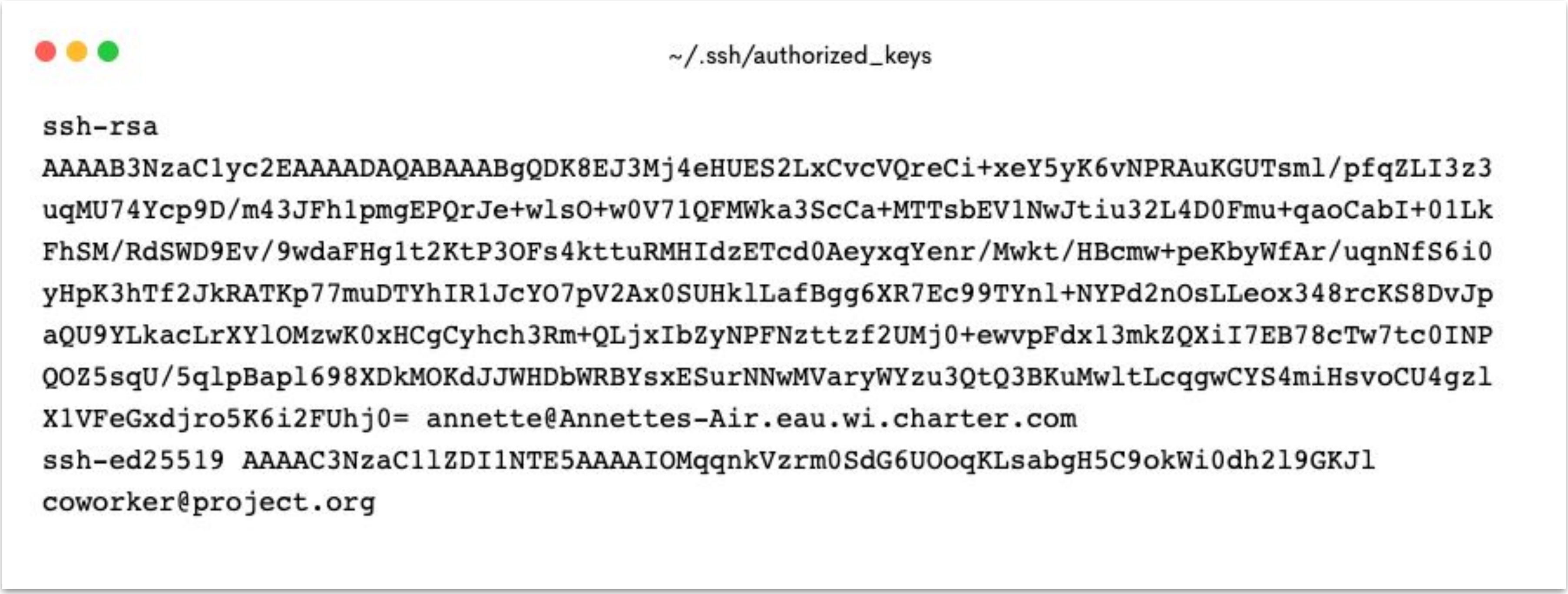
```
➜  ~ ssh -v ec2-user@50.17.34.8
OpenSSH_8.6p1, LibreSSL 3.3.5
debug1: Reading configuration data /Users/annette/.ssh/config
debug1: /Users/annette/.ssh/config line 17: Applying options for *
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 21: include /etc/ssh/ssh_config.d/* matched no files
debug1: /etc/ssh/ssh_config line 54: Applying options for *
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to 50.17.34.8 [50.17.34.8] port 22.
```

User Authentication Layer Issues



```
➜  ~ ssh -v 50.17.34.8
...
debug1: Connecting to 50.17.34.8 [50.17.34.8] port 22.
debug1: Connection established.
...
debug1: Authenticating to 50.17.34.8:22 as 'annette'
...
debug1: Host '50.17.34.8' is known and matches the ED25519 host key.
...
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic
debug1: Next authentication method: publickey
debug1: Offering public key: /Users/annette/.ssh/id_ed25519 ED25519
...
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic
debug1: No more authentication methods to try.
annette@50.17.34.8: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
➜  ~
```

authorized_keys

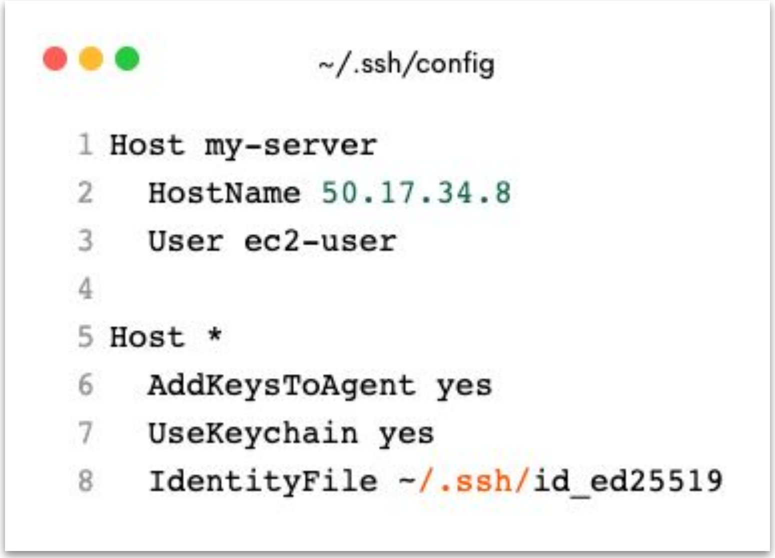


```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDK8EJ3Mj4eHUES2LxCvcVQreCi+xeY5yK6vNPRAuKGUTsml/pfqZLI3z3
uqMU74Ycp9D/m43JFh1pmgEPQrJe+wlsO+w0V71QFMWka3ScCa+MTTsbEV1NwJtiu32L4D0Fmu+qaoCabI+01Lk
FhSM/RdSWD9Ev/9wdaFHg1t2KtP3OFs4kttuRMHIdzETcd0AeyxqYenr/Mwkt/HBcmw+peKbyWfAr/uqnNfS6i0
yHpK3hTf2JkRATKp77muDTYhIR1JcYO7pV2Ax0SUHklLafBgg6XR7Ec99TYnl+NYPd2nOsLLeox348rcKS8DvJp
aQU9YLkacLrXYlOMzwK0xHCgCyhch3Rm+QLjxIbZyNPFNzttzf2UMj0+ewvpFdx13mkZQXiI7EB78cTw7tc0INP
QOZ5sqU/5qlpBapl698XDkMOKdJJWHDbWRBYsxESurNNwMVaryWYzu3QtQ3BKuMwltLcqgwCYS4miHsvoCU4gzl
X1VFeGxdjro5K6i2FUhj0= annette@Annettes-Air.eau.wi.charter.com
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOMqqnkVzrm0SdG6UOoqKLsabgH5C9okWi0dh2l9GKJl
coworker@project.org
```

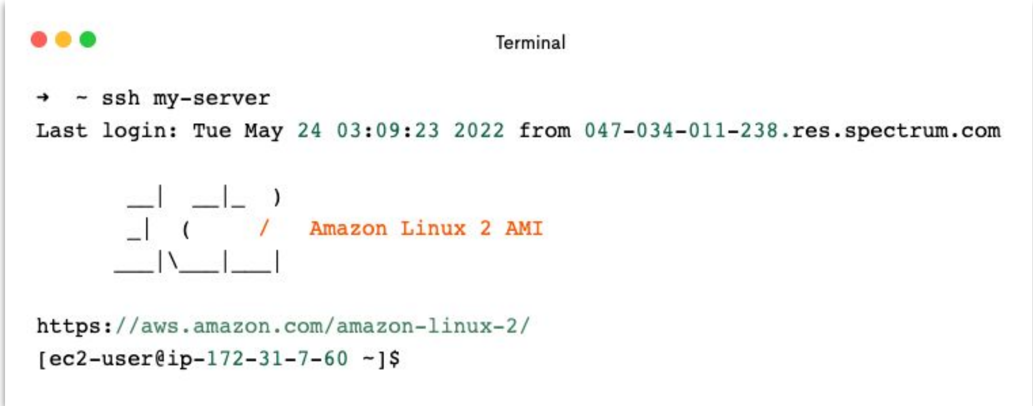
It works!

Let’s make it easy…

Add Host To Config

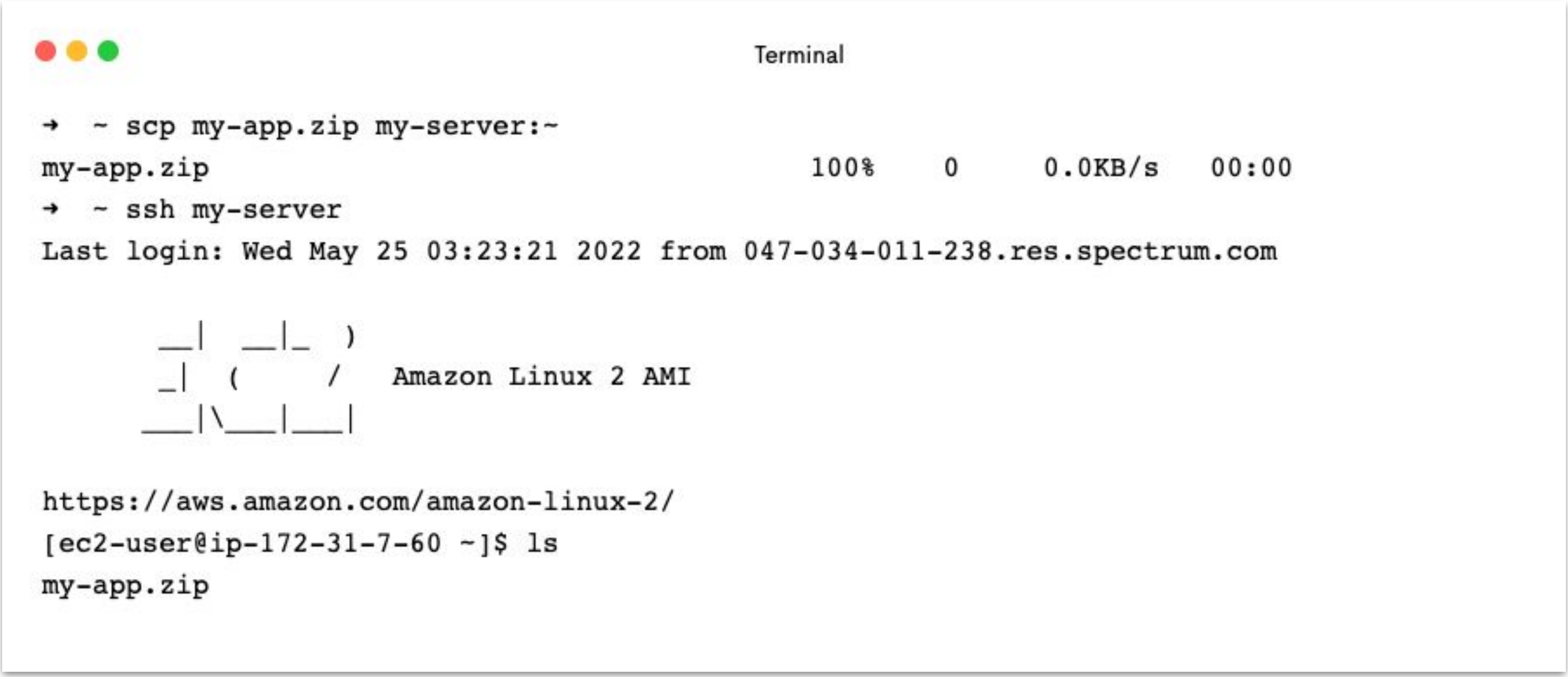


```
Host my-server
  HostName 50.17.34.8
  User ec2-user

Host *
  AddKeysToAgent yes
  UseKeychain yes
  IdentityFile ~/.ssh/id_ed25519
```



```
➜  ~ ssh my-server
Last login: Tue May 24 03:09:23 2022 from 047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-7-60 ~]$
```

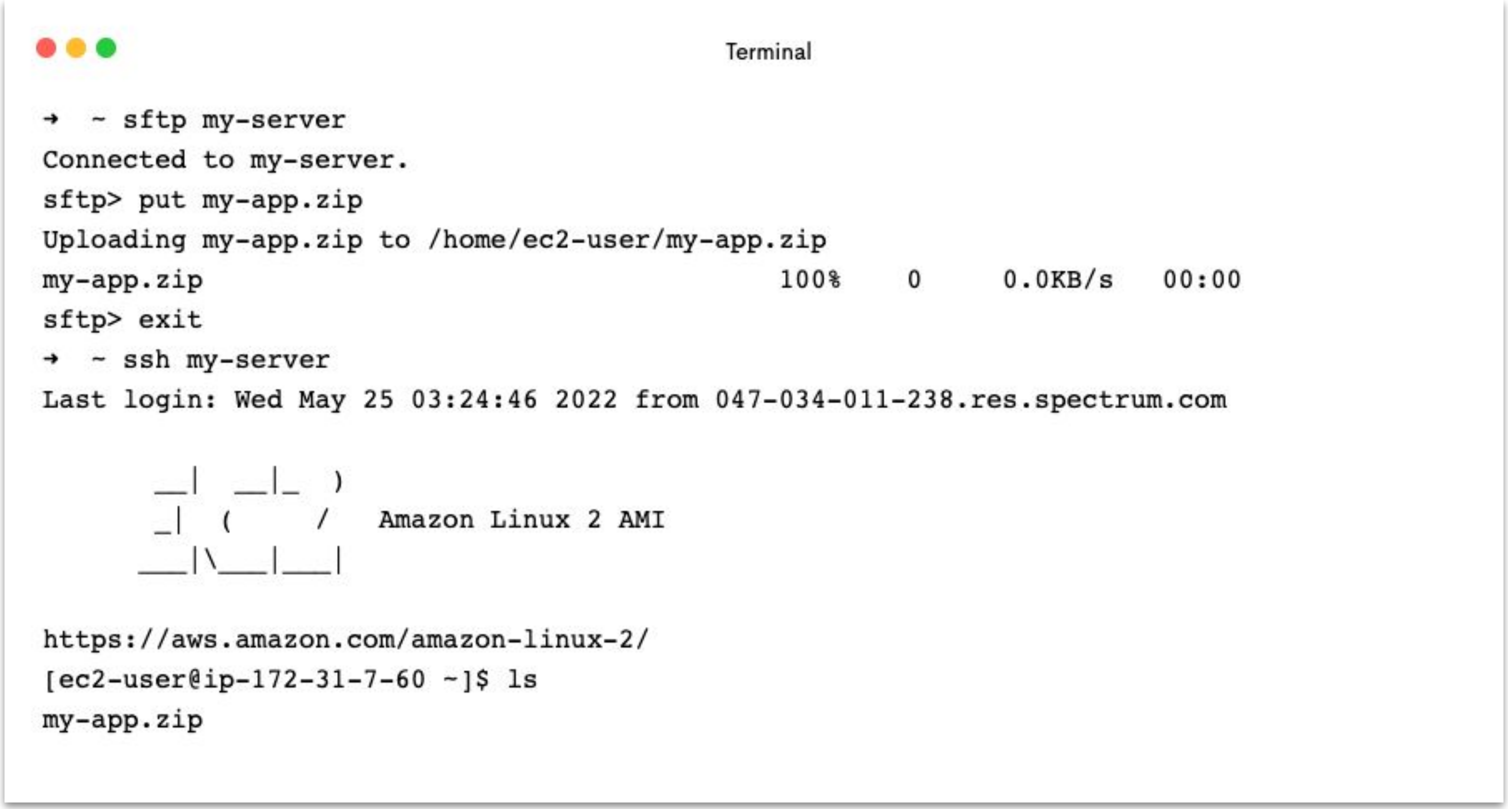
Bonus Config Feature: `scp` & `sftp`



Terminal

```
➜  ~ scp my-app.zip my-server:~
my-app.zip                                    100%    0     0.0KB/s   00:00
➜  ~ ssh my-server
Last login: Wed May 25 03:23:21 2022 from 047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-7-60 ~]$ ls
my-app.zip
```

Bonus Config Feature: `scp` & `sftp`

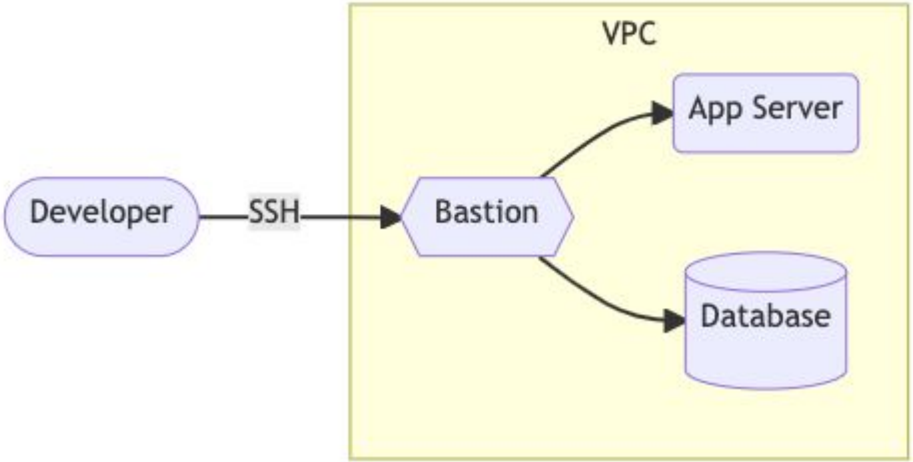


```
➜  ~ sftp my-server
Connected to my-server.
sftp> put my-app.zip
Uploading my-app.zip to /home/ec2-user/my-app.zip
my-app.zip                                        100%    0     0.0KB/s   00:00
sftp> exit
➜  ~ ssh my-server
Last login: Wed May 25 03:24:46 2022 from 047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-7-60 ~]$ ls
my-app.zip
```

Use Case: VPC & Bastion Server

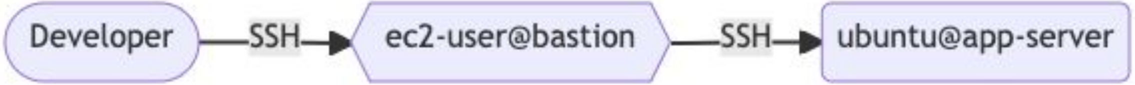
Context: Bastion Hosts

- Even though SSH is secure, like anything else it can be compromised.
- If you have a large infrastructure, rather than leave all the servers open to the world, lock down all but one host and funnel all traffic there.
- This is what is called a **bastion host**, or a **jump server.**
- Most often this is the only host that has SSH enabled to public IPs



Use Case: Access A Host Through Bastion Host

You need see why something is failing on my application server? You need an SSH tunnel!

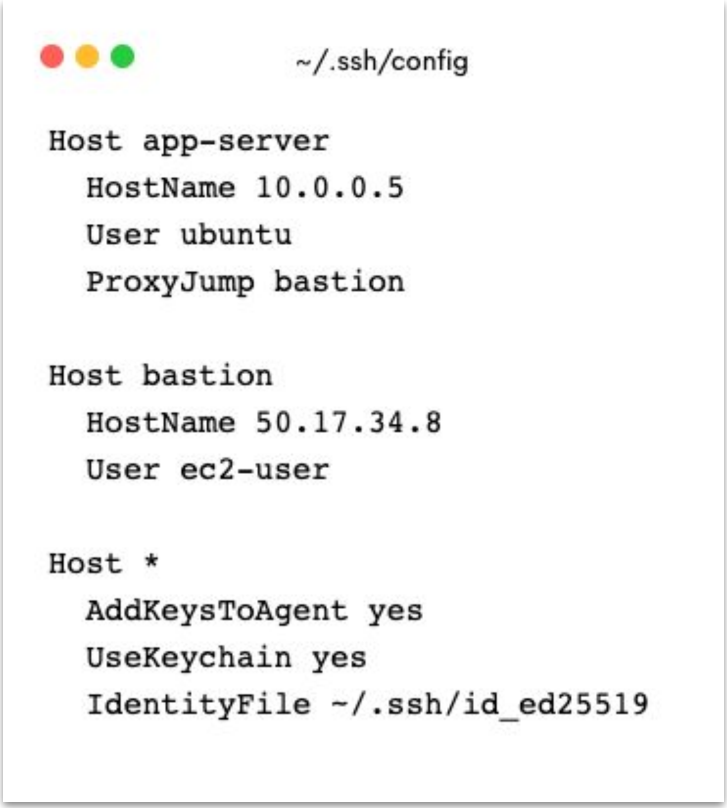


```
ssh -J <bastion user>@<bastion host> <user>@<host>
ssh -J ec2-user@bastion ubuntu@app-server
ssh -J ec2-user@50.17.34.8 ubuntu@10.0.0.5
```

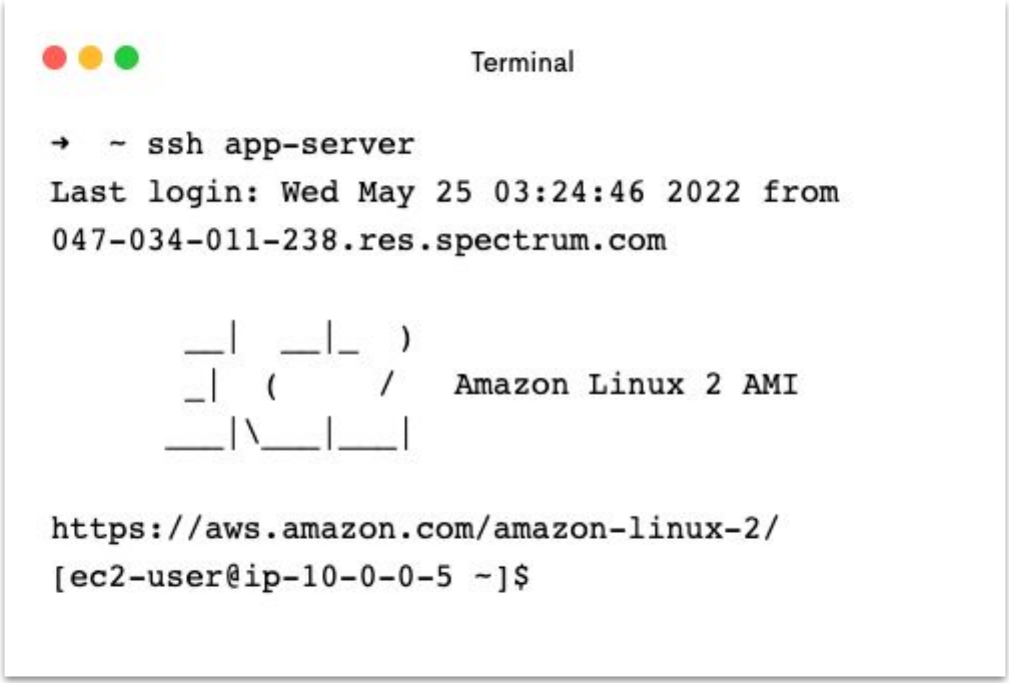
It works!

Let’s make it easy…

ProxyJump Config

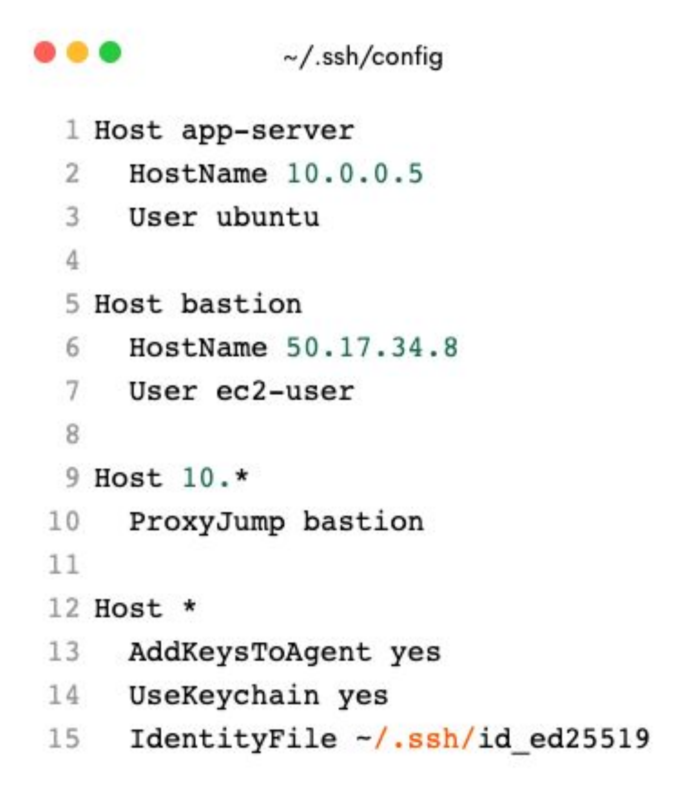


```
Host app-server
  HostName 10.0.0.5
  User ubuntu
  ProxyJump bastion

Host bastion
  HostName 50.17.34.8
  User ec2-user

Host *
  AddKeysToAgent yes
  UseKeychain yes
  IdentityFile ~/.ssh/id_ed25519
```



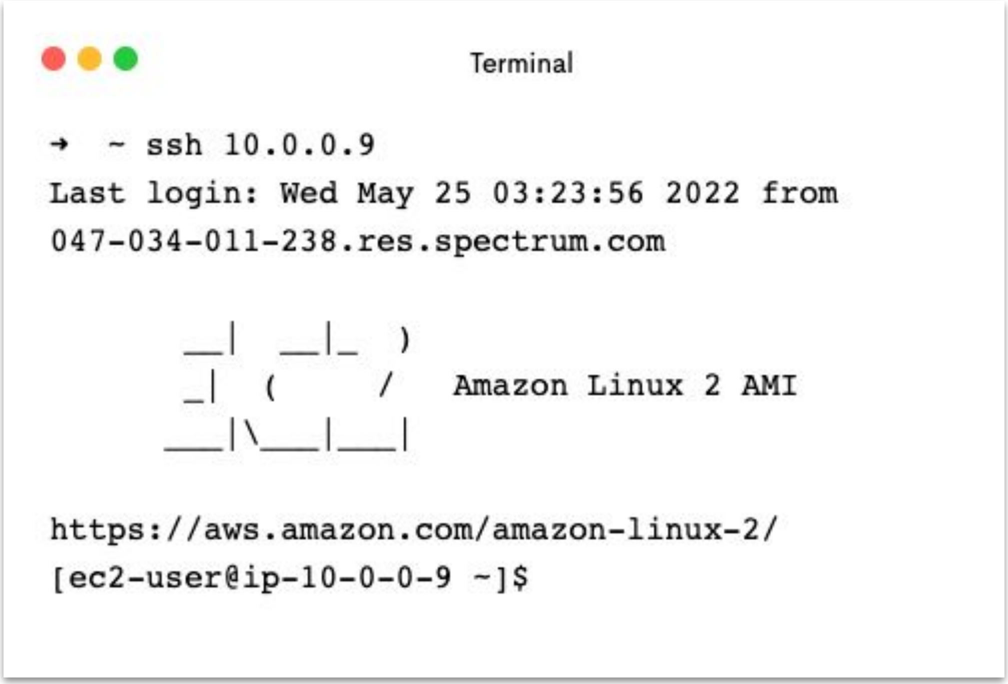
```
➜  ~ ssh app-server
Last login: Wed May 25 03:24:46 2022 from
047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-5 ~]$
```

ProxyJump Config



~/.ssh/config

```
Host app-server
  HostName 10.0.0.5
  User ubuntu

Host bastion
  HostName 50.17.34.8
  User ec2-user

Host 10.*
  ProxyJump bastion

Host *
  AddKeysToAgent yes
  UseKeychain yes
  IdentityFile ~/.ssh/id_ed25519
```

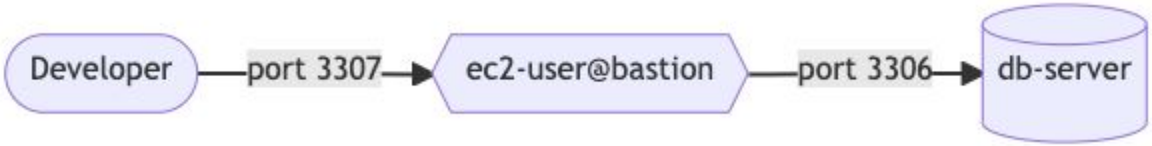


Terminal

```
➜  ~ ssh 10.0.0.9
Last login: Wed May 25 03:23:56 2022 from
047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-9 ~]$
```

Use Case: Access A Resource Through Bastion Host

You want to run locally against a test database,
but it's inside a VPC. You need port forwarding!

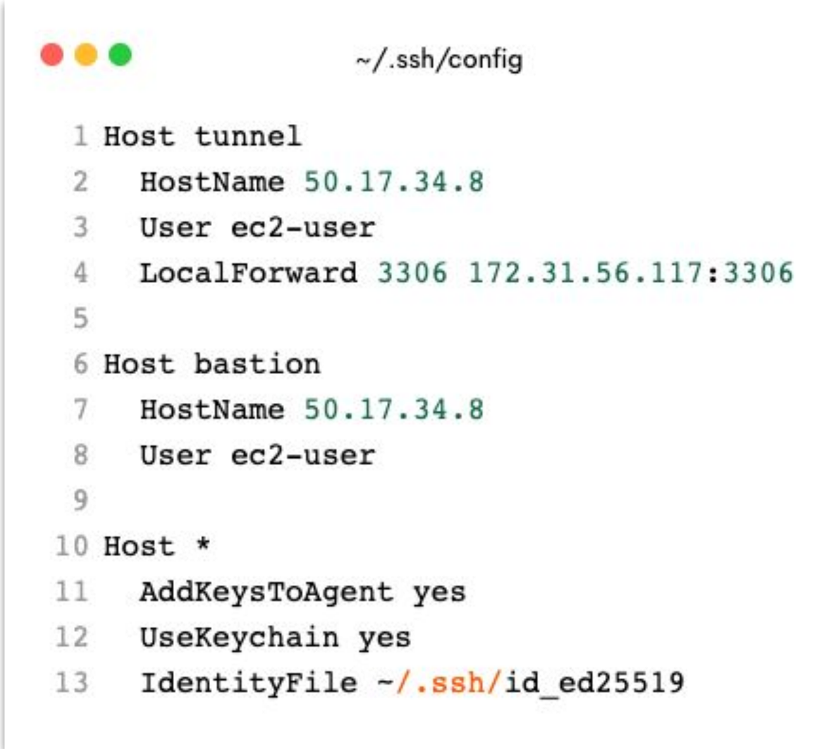


```
ssh -L <local port>:<database host>:<database port> <bastion user>@<bastion
host>
ssh -L 3307:db-server:3306 ec2-user@bastion
ssh -L 3307:10.0.0.12:3306 ec2-user@50.17.34.8
```

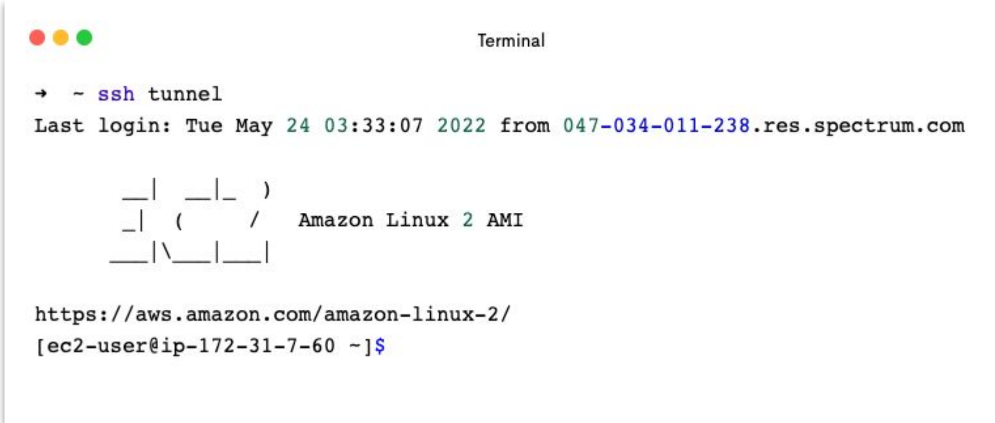
It works!

Let’s make it easy…

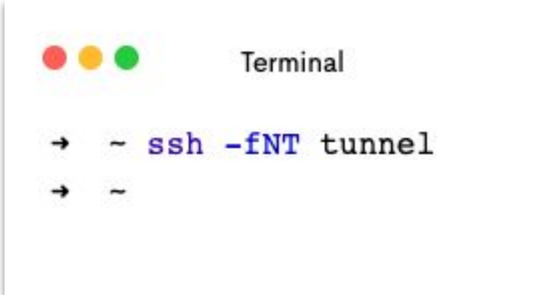
Use Case: Access A Resource Through Bastion Host



```
Host tunnel
  HostName 50.17.34.8
  User ec2-user
  LocalForward 3306 172.31.56.117:3306

Host bastion
  HostName 50.17.34.8
  User ec2-user

Host *
  AddKeysToAgent yes
  UseKeychain yes
  IdentityFile ~/.ssh/id_ed25519
```



```
➜  ~ ssh tunnel
Last login: Tue May 24 03:33:07 2022 from 047-034-011-238.res.spectrum.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-7-60 ~]$
```



```
➜  ~ ssh -fNT tunnel
➜  ~
```

SSH can do many things.

A config file can make it easy!

Thanks!

To Women Who Code, and you!

annette.mechelke.us