Bastion Host

A security best practice is to keep only the internet accessible endpoints in the public subnet and keep all other resources in the private subnet of your VPC.

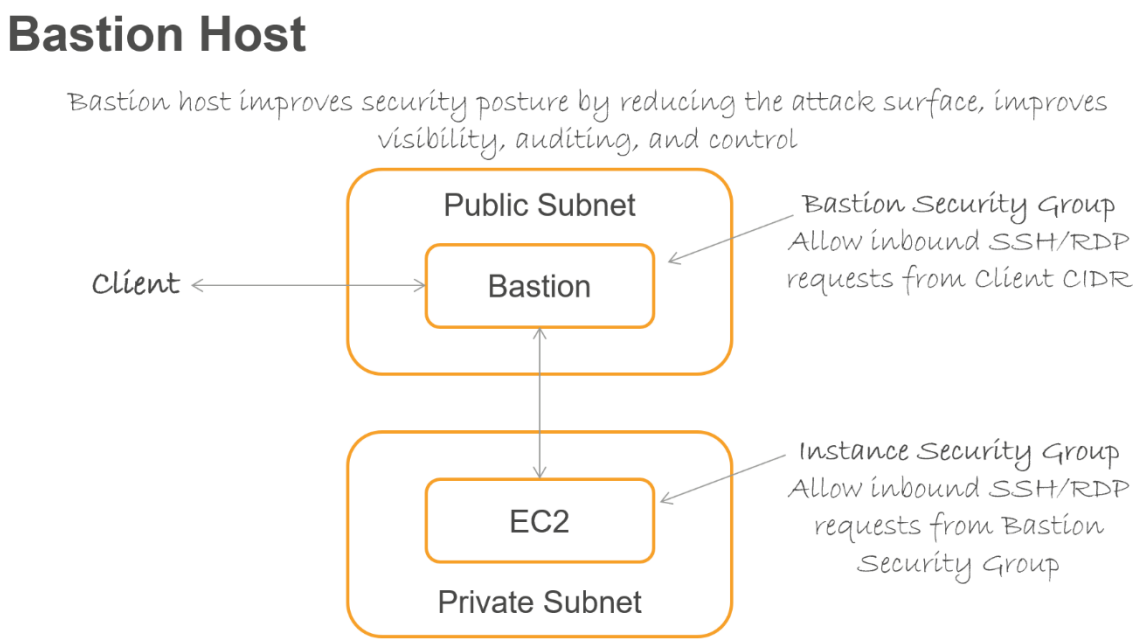
This reduces the attack surface and improves the security posture of your infrastructure.

However, you need the ability to access your EC2 instances in the private subnet.

There are a couple of ways to access private instances

- Bastion Host for Linux or Windows Remote Gateway for Windows systems
- AWS Systems Manager – Session Manager (covered in the Systems Manager topic)

In this article, I will give an overview of how to configure your Bastion Host and Putty SSH client for credential forwarding.



Bastion Host

Launch an EC2 instance and name it as Bastion Host

Configure Bastion Host Security Group to allow inbound SSH access from the client CIDR

With this configuration, the client can log in to the bastion host using SSH.

Private Instance Configuration

The private EC2 instance needs to allow SSH connection from the bastion host

Configure Instance Security Group to allow inbound SSH access from Bastion Host Security Group

With this configuration, the Client can log in to the bastion host and then hop into the private instance.

Credential Forwarding

We now need to manage credentials to log in to the bastion host and the private instance. These instances can allow login access using the same key pair, or they could use different key pairs.

The client needs private keys to connect to the bastion host and then to the private instance.

The important point is private keys stay with the client and never stored in the bastion host.

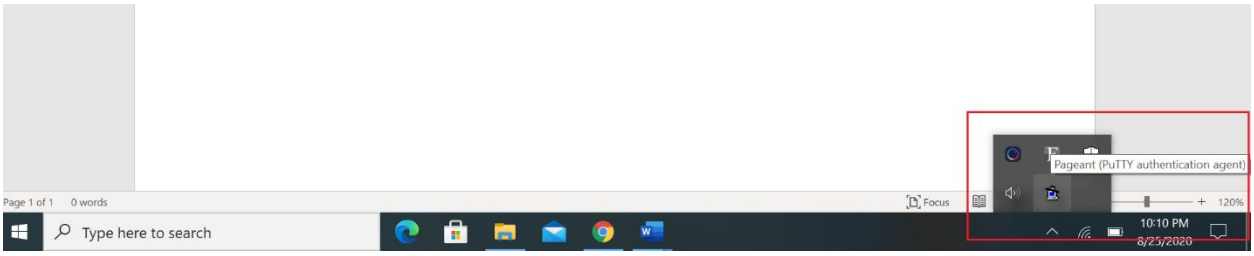
With Putty, you can configure credential forwarding that will automatically forward your credentials to the instance.

Putty

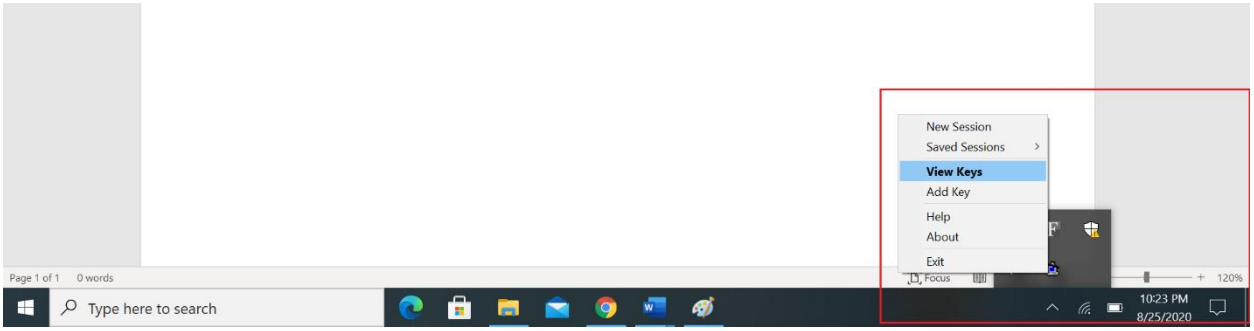
The putty installer comes with the Pageant utility. The pageant is putty authentication agent that holds your private key in memory which you can use to connect to the server

From your Windows machine, start the **Pageant** tool

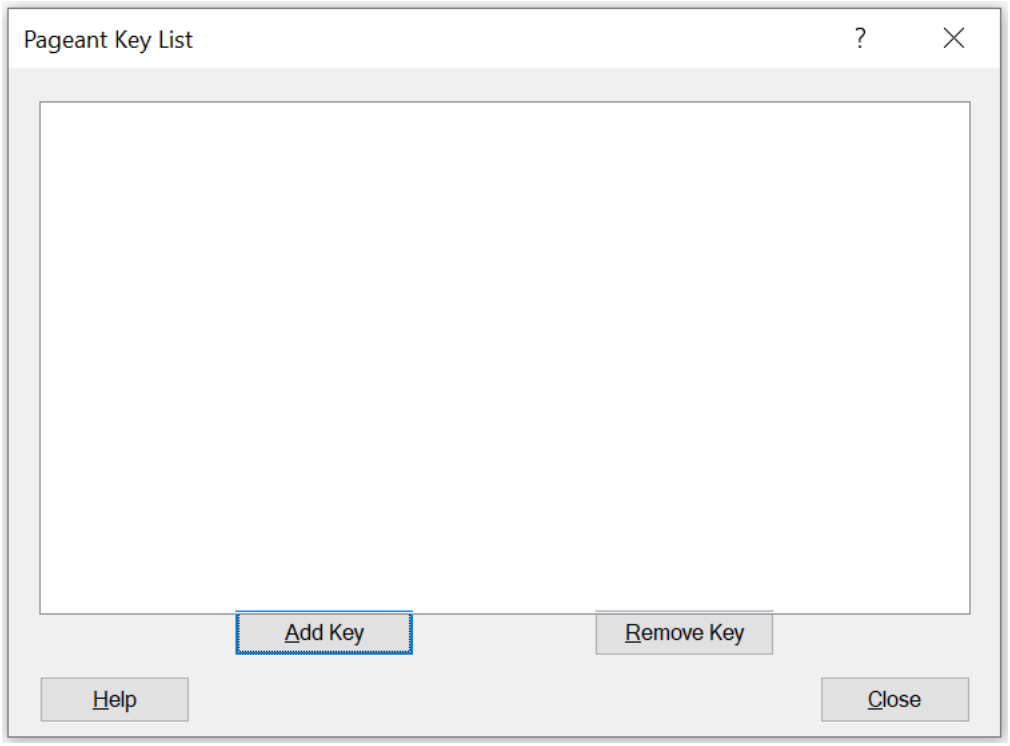
Pageant tool starts up in the tray



Right-click on Pageant Tool icon and Select **View Keys**

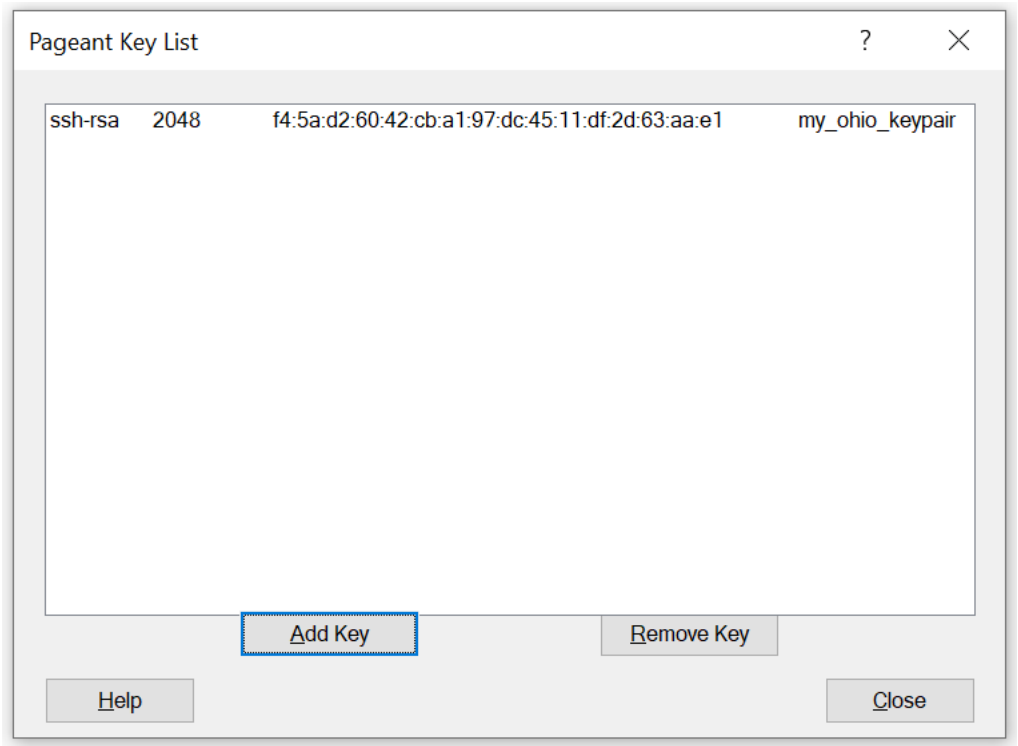


Add key in the Pageant Key List window



Choose your private key file

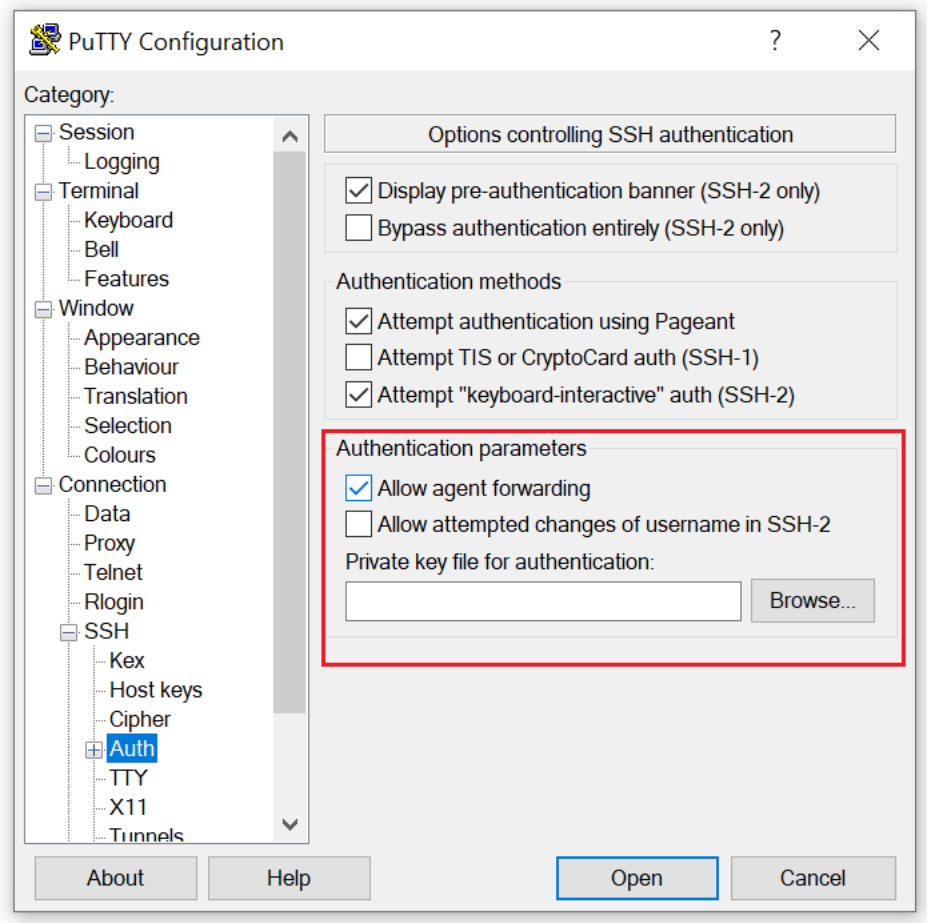
You can also add multiple private keys – for example, if you are using different keypair for bastion and the private instance. You can now use the keys to log in to the instances



Configure Putty

Now launch your Putty tool and expand Connection -> SSH -> Auth

And **Enable Allow agent forwarding**



You can now connect to the bastion host from Putty using keys in the Pageant tool.

From the bastion host terminal, you can connect to the private instance

Run the command

```
ssh ec2-user@<private IP>
```

You are now logged into the private instance. Note: ec2-user is the default user name in Amazon Linux AMI.

Bastion host improves security posture by reducing the attack surface, improves visibility, auditing, and control

References

https://aws.amazon.com/blogs/security/securely-connect-to-linux-instances-running-in-a-private-amazon-vpc/

https://aws.amazon.com/blogs/security/controllingng-network-access-to-ec2-instances-using-a-bastion-server/