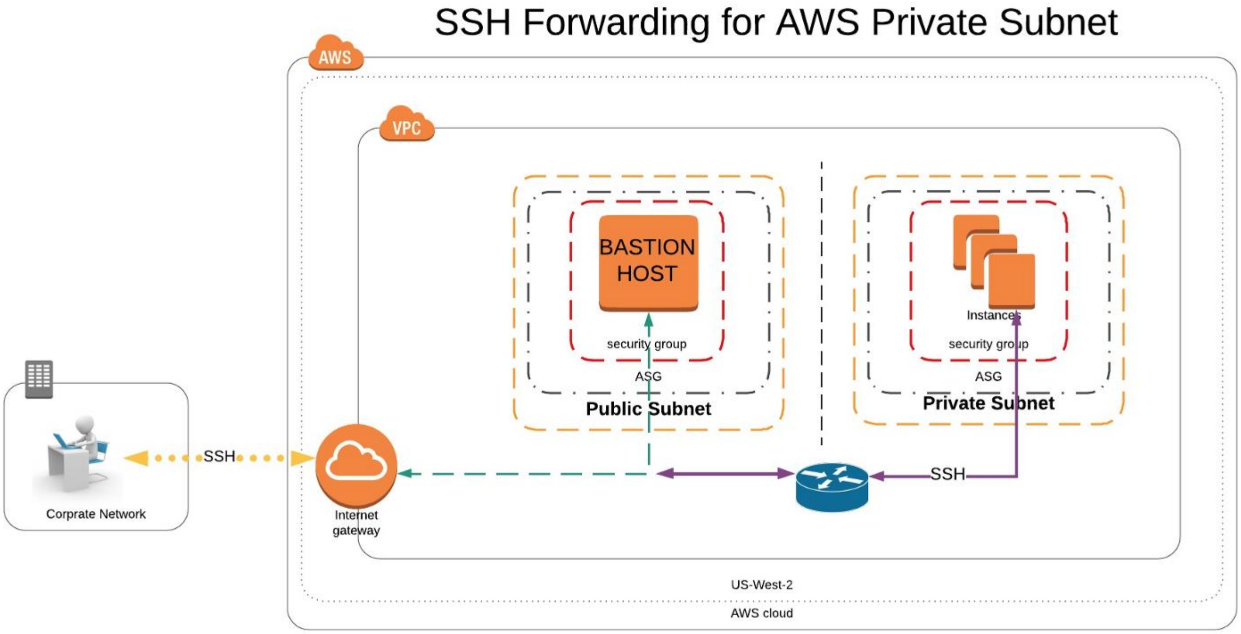
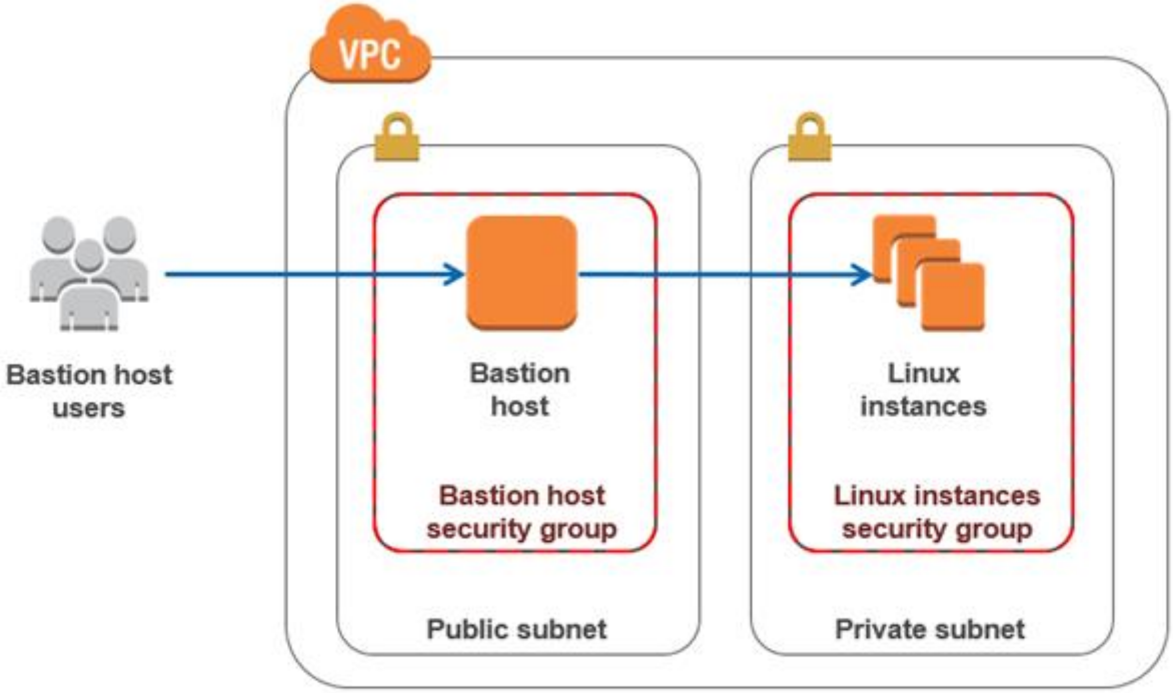
AWS Bastion-Host



A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration. For example, you can use a bastion host to mitigate the risk of allowing SSH connections from an external network to the Linux instances launched in a private subnet of your Amazon Virtual Private Cloud (VPC).

In this blog post, I will show you how to leverage a bastion host to record all SSH sessions established with Linux instances. Recording SSH sessions enables auditing and can help in your efforts to comply with regulatory requirements.

Amazon VPC enables you to launch AWS resources on a virtual private network that you have defined. The bastion host runs on an Amazon EC2 instance that is typically in a public subnet of your Amazon VPC. Linux instances are in a subnet that is not publicly accessible, and they are set up with a security group that allows SSH access from the security group attached to the underlying EC2 instance running the bastion host. Bastion host users connect to the bastion host to connect to the Linux instances, as illustrated in the following diagram.



You can adapt this architecture to meet your own requirements. For example, you could have the bastion host in a separate Amazon VPC and a VPC peering connection between the two Amazon VPCs. What matters is that the bastion host remains the only source of SSH traffic to your Linux instances.