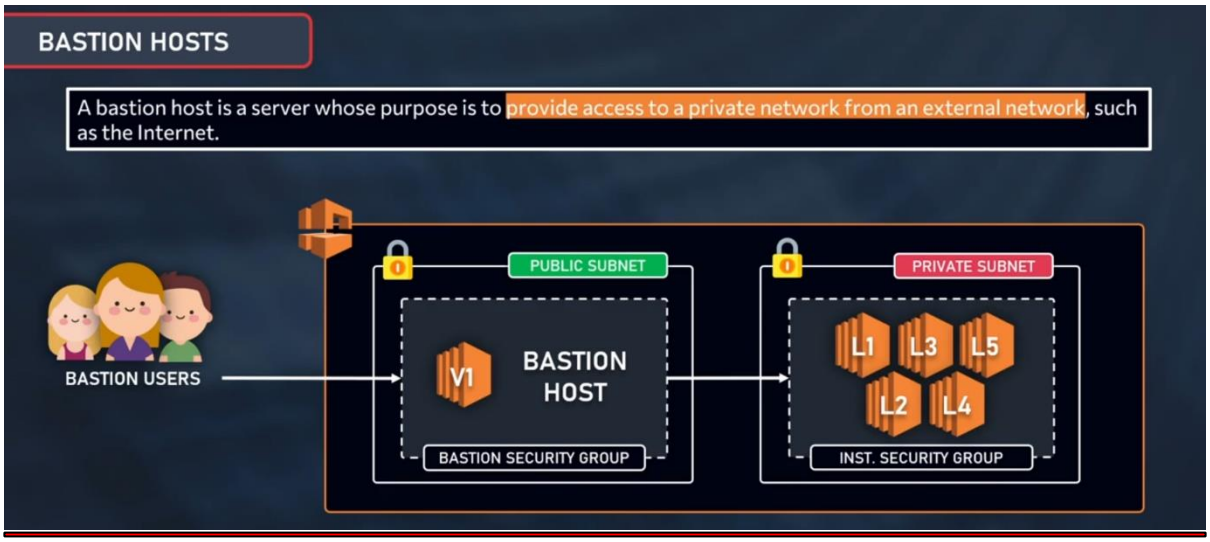
BASTION HOST



What is Bastion Host ?

- Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP.
- Once remote connectivity has been established with the bastion host, it then acts as a 'jump' server, allowing you to use SSH or RDP to login to other instances (within private subnets) deeper within your network.
- When properly configured through the use of security groups and Network ACLs, the bastion essentially acts as a bridge to your private instances via the Internet.

Do I need one of those in my environment?

- If you require remote connectivity with your private instances over the public Internet, then **yes**!

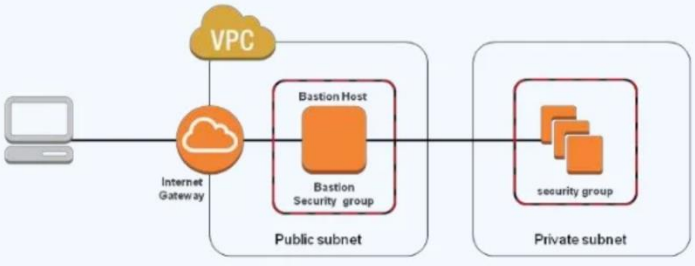


diagram shows connectivity flowing from an end user to resources on a private subnet through an bastion host

CREATED BY:- VIVEK GANDHI

N.O.T.E

- When designing the bastion host for your AWS infrastructure, you shouldn't use it for any other purpose, as that could open unnecessary security holes. You need to keep it locked down as much as possible.

creating a bastion host for your AWS infrastructure

- Launch an EC2 instance as you normally would for any other instance.
- Apply your OS hardening as required.
- Set up the appropriate security groups (SG).
- Implement either SSH-Agent Forwarding (Linux connectivity) or Remote Desktop Gateway (Windows connectivity).
- Deploy an AWS bastion host in each of the Availability Zones you're using.

Configuring security groups

- First, create a SG that will be used to allow bastion connectivity for your existing private instances.
- This SG should only accept SSH or RDP inbound requests from your bastion hosts across your Availability Zones.
- Apply this group to all your private instances that require connectivity.

create a security group to be applied to your bastion host

- Inbound and outbound traffic must be restricted at the protocol level as much as possible.
- The inbound rule base should accept SSH or RDP connections only from the specific IP addresses (usually those of your administrators' work computers).
- You definitely want to avoid allowing universal access (0.0.0.0/0).
- Your outbound connection should again be restricted to SSH or RDP access to the private instances of your AWS infrastructure. An easy way to do this is to populate the 'Destination' field with the ID of the security group you're using for your private instances.

Handling keys

- SSH and RDP connections require private and public key access to authenticate.
- This does not pose a problem when you are trying to connect to your bastion host from a local machine, as you can easily store the private key locally.
- You implement either Remote Desktop Gateway (for connecting to Windows instances) or SSH-agent forwarding (for Linux instances). Both of these solutions eliminate the need for storing private keys on the bastion host.