CLOUD
COMPUTING
APPLICATIONS

VPC: Gateways

Prof. Reza Farivar

Internet Gateways

- Internet Gateway is a logical construct, not a specific instance or resource

- AWS does quite a bit of behind the scene work to allow highly available internet to all the required Availability Zones in the VPC

- Is attached to a VPC

- Highly available, redundant, and horizontally scaled

- → in the route tables, it is referred to by its name (e.g. igw-05ae7f551a8154d1a), not an IP address

NAT Gateways

- Network Address Translation
  - Just like your home wireless router
- Virtual router or a gateway in a public subnet that enables instances in a private subnet to interact with the internet
  - IPV4 only
- Modifies the network address information in the IP header
  - It receives traffic from an EC2 instance residing in a private subnet
  - before forwarding the traffic to the internet, replaces the reply-to IPv4 address with its own public or Elastic IP address
  - When a reply is received from internet, it changes the reply-to address from its IP address to the EC2 instance private IP address
- Two types of NAT
  - NAT Instance → Runs as as EC2 instance
  - NAT Gateway → fully managed by AWS, requires elastic IP
    - Better availability and higher bandwidth

Data Flow
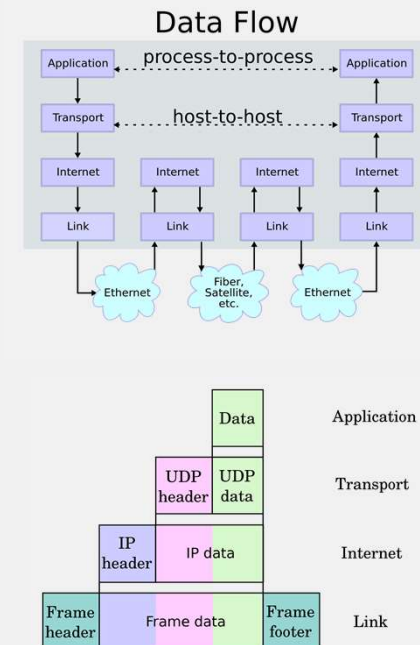
Bastion Host

- Use a bastion host to access private machines hosted in a private network in a VPC

- Bastion host: "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"

Further reading: https://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/