VPC Routing & Internet Gateway

Higher the subnet, Higher the priority

Internet Gateway

IPV4 - public Addresses are not directly assigned to EC2.

Traffic goes from gateway & IGW (Internet gateway) keeps the track of which private IPV4 is requesting information.

IPV6 = All IPV6 Address are publicaly reroutable

Stateful / Stateless firewalls.

↓

Learn more on the internet

Stateless - This firewall is generally uses ephemoral ports when sending data from clients due to which every port is monitored.

also they dosn't know if traffic is inbound or outbound.

statless also requires two rules

① Request rule.
② Respond rule.

uses ephemoral port which ranges from 1024 - 65535

- statefull firewalls - uses fixed ports that means automatic approval of connection.

NACL

Network Access control List

① two set's of rules
- Inbound
- outbound

NACL - They are stateless

They see Request & respond as two different things.

In NACL if deny comes first then it doesn't check for other and denys Access.
If nothing else matches then deny by default
As NACL requires two seperate connection request & respond this may increase traffic as this get's complex pretty quickly due to higher no. of connection is required.
for VPC this may slow-up other traffic

By default VPC has catch all allow

Custom NACL has deny by default

Network Access Control Lists (NACL)

https://learn.cantrill.io adriancantrill

- **STATELESS** - **REQUEST** and **RESPONSE** seen as different
- Only impacts **data crossing subnet boundary**
- NACLs can **EXPLICITLY ALLOW** and **DENY**
- IPs/CIDR, Ports & protocols - no logical resources
- NACLs cannot be assigned to AWS resources - **only subnets**
- Use together with Security Groups to add explicit DENY (Bad IPs/Nets)
- Each subnet can have **one NACL** (Default or Custom)
- A NACL can be associated with **MANY Subnets**

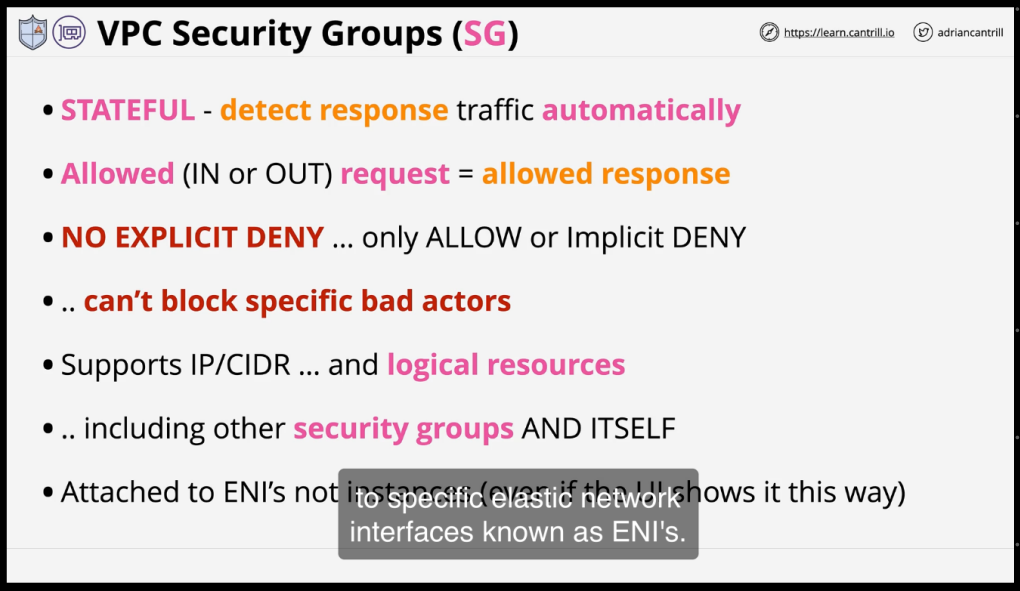
about network ACLs for this lesson.

Security Groups

— stateful

x - Explicitly deny is not there

operate above NACL on OSI Layer which means they have more features

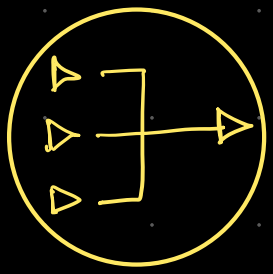


they are not attached to subnets like NACL but they are attached to ENI's - elastic network interface.

security groups cannot explicitly block traffic.

NAT

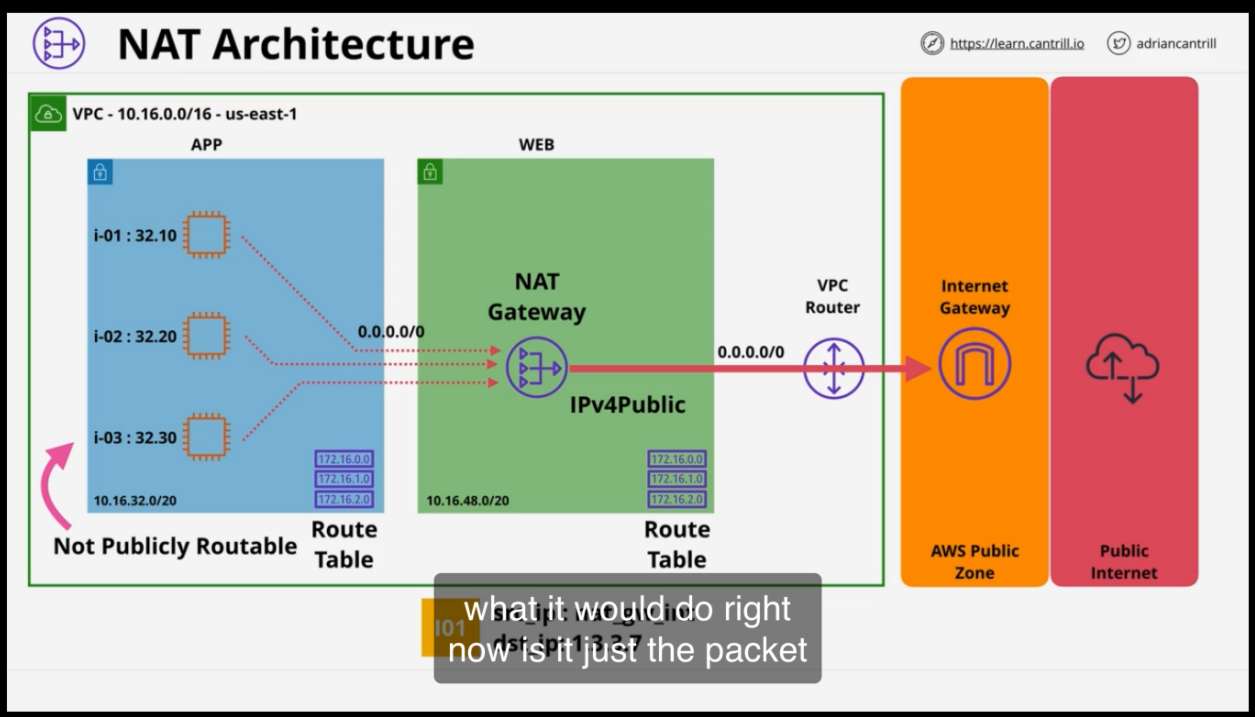
- Network Address Translation



NAT is many private IP to one sigle private IP

IP MASQUERADING -

NAT Gateway is used to send
data from private ip subnets to internet

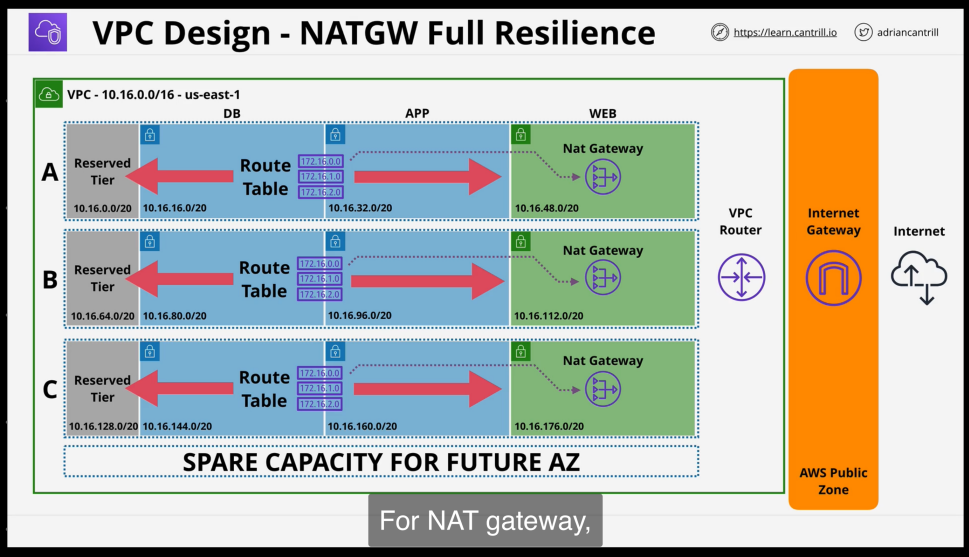


NAT Gateway allows multiple private IP's to masquerade behind one single public ip. That's why the masquerade term

for Every AZ we need one NAT Gateway & one routing Table
for ex. if we need to manage bandwidth we can just create new NAT Gateway to manage the bandwidth
4 cent/hr - for NAT Gateway & data processing charge 4cent/hr

NAT Gateways has two different charges for payment

NAT Gateway has to be deployed on every AZ



NAT Instance is run on Ec2 instance!

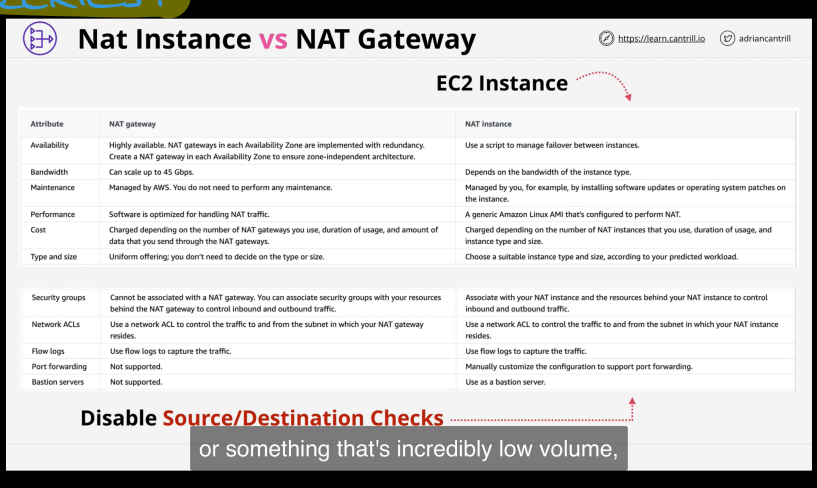
It's not prefered to use NAT instances better to use NAT Gateway. Limited by features.

NAT instances are cheaper than NAT Gateway for High volume data.

A NAT Gateway cannot be used as bastion host.

NAT Gateway doesn't support security groups

It uses knackles.



NAT is not required for IPv6.
Doesn't work with IPv6