

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 if IGW (Internet gateway) keeps the track of which private IPV4 is requesting information.

IPv6 = All IPv6 Address are publicly routable

Stateful / Stateless firewalls.



Learn more on the internet

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

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

stateless also requires two rules

- ① Request rule. | USES ephemeral port which ranges from
- ② Respond rule. | 1024 - 65535

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

NACL

Network Access Control List

① two sets 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 denies access.

If nothing else matches then deny by default
As NACL requires two separate

connection request & respond this may increase traffic as this gets complex pretty quickly due to higher no. of connections 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 OSF layer
which means they have more features

 VPC Security Groups (SG)

https://learn.cantrill.io adriancantrill

- **STATEFUL** - detect response traffic automatically
- Allowed (IN or OUT) request = allowed response
- **NO EXPLICIT DENY** ... only ALLOW or Implicit DENY
- .. can't block specific bad actors
- Supports IP/CIDR ... and logical resources
- .. including other security groups AND ITSELF
- Attached to ENI's not instances (or if the UI shows it this way)
to specific elastic network interfaces known as ENI's.

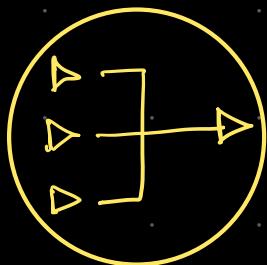
They are not attached to subnets like NACL

but they are attached to ENI's - elastic network interface

security groups cannot explicitly block traffic.

NAT

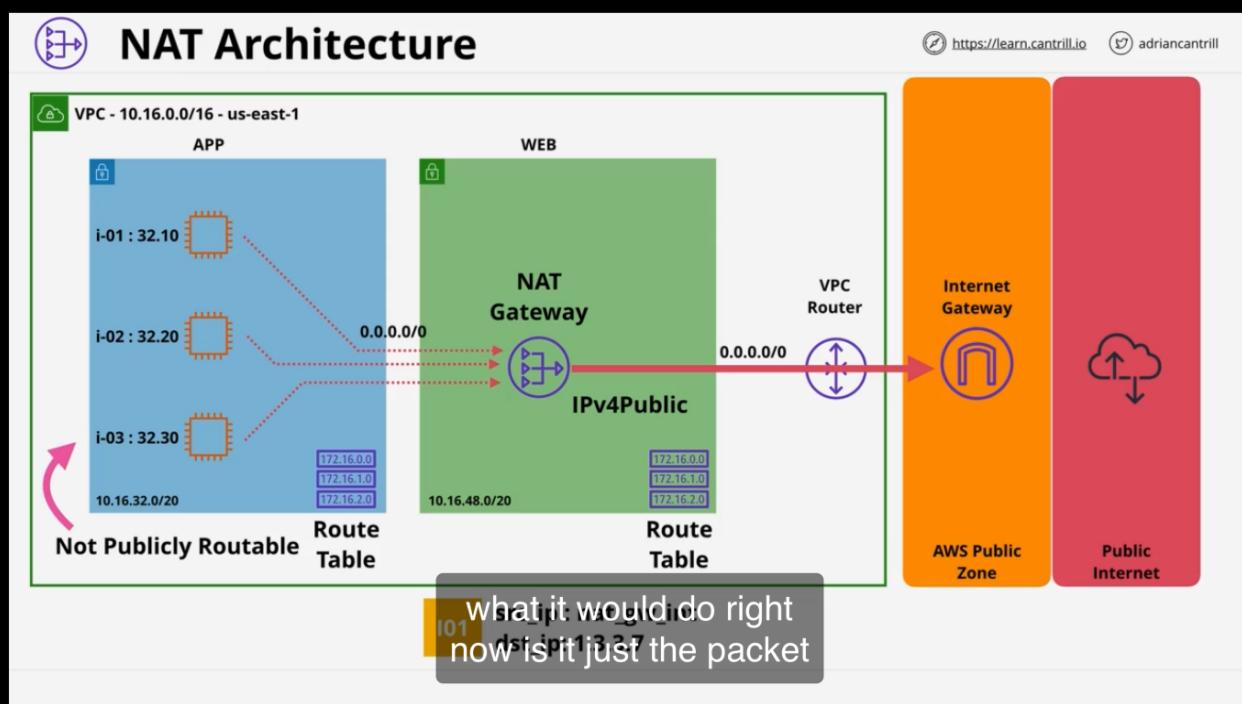
- Network Address Translation



NAT is many private IP to one single private IP

IP MASQUERAADING -

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

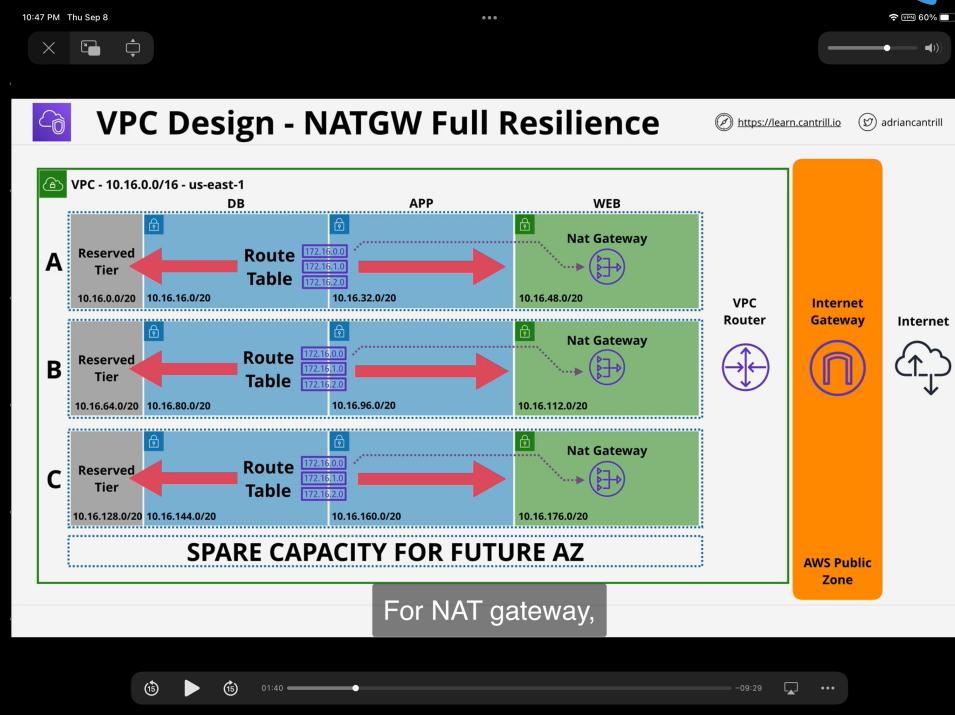


NAT Gateway allows multiple private IP's to masquerade behind one single public ip. That's why the masquerade term

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 4 cent/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 preferred 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 knobs.

Nat Instance vs NAT Gateway	
Attribute	NAT gateway
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.
Bandwidth Maintenance	Can scale up to 45 Gbps. Managed by AWS. You do not need to perform any maintenance.
Performance Cost	Software is optimized for handling NAT traffic. Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.
Type and size	Uniform offering: you don't need to decide on the type or size.
Security groups	Cannot be associated with a NAT gateway. You can associate security groups with your resources behind the NAT gateway to control inbound and outbound traffic.
Network ACLs	Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides.
Flow logs	Use flow logs to capture the traffic.
Port forwarding	Not supported.
Bastion servers	Not supported.
EC2 Instance	
NAT instance	Use a script to manage failover between instances.
	Depends on the bandwidth of the instance type. Managed by you, for example, by installing software updates or operating system patches on the instance.
	A generic Amazon Linux AMI that's configured to perform NAT. Charged depending on the number of EC2 instances that you use, duration of usage, and instance type and size. Choose a suitable instance type and size, according to your predicted workload.
Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.	
Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides.	
Use flow logs to capture the traffic.	
Manually customize the configuration to support port forwarding.	
Use as a bastion server.	
Disable Source/Destination Checks	
or something that's incredibly low volume,	

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

What about IPv6?

- NAT isn't required for IPv6
- All IPv6 addresses in AWS are publicly routable
- The Internet Gateway works with ALL IPv6 IPs directly
- NAT Gateways **don't work with IPv6**
- ::/0 Route + IGW for bi-directional connectivity
- ::/0 Route + Egress-Only Internet Gateway - Outbound Only

is a different type of gateway known as