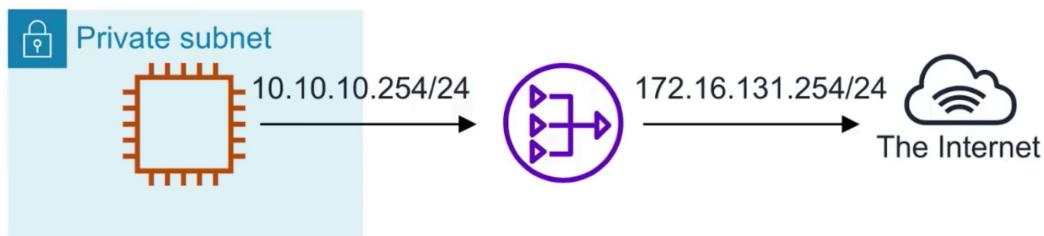




Network Address Translation (NAT)

Network Address Translation (NAT) is the method of **re-mapping** one IP address space into another.



If you have a private network and you need to help gain outbound access to the internet you would need to use a NAT gateway to remap the Private IPs

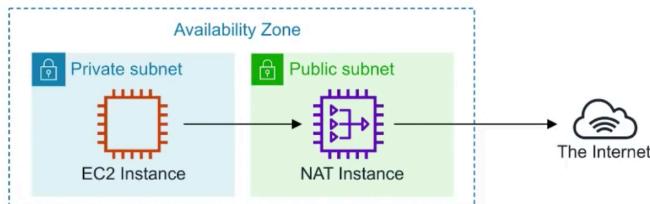
If you have two networks which have conflicting network addresses you can use a NAT to make the addresses more agreeable



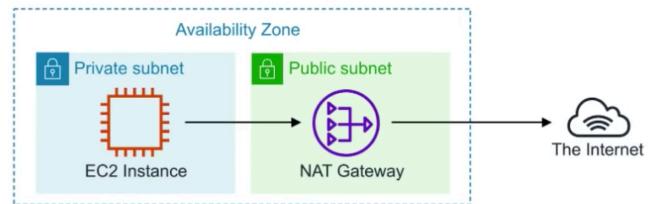
NAT Instances vs NAT Gateways

NATs have to run within a **Public Subnet**

NAT Instances (legacy) are individual EC2 instances. Community AMIs exist to launch NAT Instances.



NAT Gateways is a managed service which launches redundant instances within the selected AZ.



A screenshot of the AWS Lambda console search results. The search bar at the top contains 'amzn-ami-vpc-nat'. The results list shows one item: 'amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-ebs - ami-00a9d4a05375b2763'. Below the item, it says 'Amazon Linux AMI 2018.03.0.20181116 x86_64 VPC HVM ebs'. At the bottom, it shows 'Root device type: ebs' and 'Virtualization type: hvm'.



NAT Instance and NAT Gateway *CheatSheet*

- When creating a NAT instance you **must disable source and destination checks** on the instance
 - NAT instances **must exist in a public subnet**
 - You must have a **route out** of the private subnet to the NAT instance
 - The size of a NAT instance determines **how much traffic can be handled**
 - **High availability** can be achieved using **Autoscaling Groups**, multiple **subnets in different AZs**, and **automate failover between them using a script**.
-
- NAT Gateways are **redundant inside an Availability Zone** (can survive failure of EC2 instance)
 - You can only have **1 NAT Gateway inside 1 Availability Zone** (cannot span AZs)
 - Starts at 5 Gbps and scales all the way up to 45 Gbps
 - NAT Gateways are the **preferred setup for enterprise systems**.
 - There is no **requirement to patch NAT Gateways**, and there is no **need to disable Source/Destination checks** for the NAT Gateway (unlike NAT Instances)
 - NAT Gateways are **automatically assigned a public IP address**
 - **Route Tables** for the NAT Gateway MUST be updated
 - Resources in multiple AZs sharing a Gateway will **lose internet access if the Gateway goes down**, unless you create a **Gateway in each AZ** and configure **route tables** accordingly