NAT Devices

## Service Overview

*You can use a* ***NAT device*** *to enable instances in a private subnet to connect to the internet (for example, for software updates) or other AWS services, but prevent the internet from initiating connections with the instances. A NAT device forwards traffic from the instances in the private subnet to the internet or other AWS services, and then sends the response back to the instances. When traffic goes to the internet, the source IPv4 address is replaced with the NAT device’s address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances’ private IPv4 addresses.*

*NAT devices are not supported for IPv6 traffic—use an egress-only internet gateway instead.*

## Use cases / Considerations

***NAT gateways.*** *You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances*

* *Redundant inside the Availability Zone*
* *Preferred by the enterprise*
* *Starts at 5Gbps and scales currently to 45Gbps*
* *No need to patch*
* *Not associated with security groups*
* *Automatically assigned a public ip address*
* *Remember to update your route tables.*
* *No need to disable Source/Destination Check*

***NAT instances.*** *You can create your own network address translation AMI and run it on an EC2 instance as NAT instance in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the internet.*

* *When creating a NAT instance, Disable Source/Destination Check on the Instance.*
* *NAT instances must be in a public subnet.*
* *There must be a route out of the private subnet to the NAT instance, in order for this to work.*
* *The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size.*
* *You can create high availability using Autoscaling Groups, multiple subnets in different AZs, and a script to automate failover.*
* *Behind a Security Group*

# [*Comparing NAT gateways and NAT instances*](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html)

## Governance

# [*Monitoring NAT gateways using Amazon CloudWatch*](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway-cloudwatch.html)

## Cautions

*If you have resources in multiple Availability Zones and they share one NAT gateway, in the event that the NAT gateway’s Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.*

## Pricing considerations

*You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply.*

*https://aws.amazon.com/vpc/pricing/*

## More details

[NAT devices for your VPC - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat.html)