**What is NAT Gateway:**

* A NAT gateway is a fully managed service provided by AWS that allows resources in private subnets to access the internet
* A NAT gateway is created in a public subnet and has an Elastic IP address assigned to it
* The private subnet’s traffic is routed through the NAT gateway, which translates the private IP address to the public IP address assigned to the NAT gateway.
* NAT gateways are highly available and can handle large amounts of traffic.

**What is NAT instance:**

* A NAT instance is a EC2 instance that is deployed in a public subnet and acts as a NAT device for resources in private subnets
* The NAT instance is responsible for translating the private IP address of resources in the private subnet to a Public IP address.
* NAT instances can be customized to suit specific needs, but they require more management and maintenance than NAT gateways.

**Difference between NAT Gateway & NAT Instance**

|  |  |  |
| --- | --- | --- |
| **Attribute** | **NAT Instance** | **NAT Gateway** |
| **Type and Size** | Choose a suitable  instance size and type, according to your  predicted workload | Uniform offering: You  don’t need to decide on the type or size |
| **Public IP addresses** | Use an Elastic IP address or a Public IP address with a NAT instance. You can  change the public IP address at any time by associating a new Elastic IP address with the instance. | Choose the Elastic IP address to associate with a public NAT  gateway at creation |
| **Private IP Addresses** | Assign a Specific  private IP address from the subnet’s IP address range when you launch the instance | Automatically selected from the subnet’s IP address range when you create the gateway |
| **Security Groups** | Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic | You cannot associate security groups with  NAT gateways. You can associate them with the 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  instance resides | 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 | Use flow logs to |

|  |  |  |
| --- | --- | --- |
|  | capture the traffic | capture the traffic |
| **Port Forwarding** | Manually customize the configuration to support port forwarding | Not supported |
| **Bastion Servers** | Use a Bastion server | Not supported |
| **Traffic Metrics** | When a connection timeout, a NAT instance sends a FIN packet to resources behind the NAT instance to close  the connection | When a connection timeout, a NAT gateway returns an RST packet to any resource behind the NAT gateway that  attempt to continue the connection (it does not send a FIN packet) |

**Creation of NAT Gateway:**

**Prerequisites:**

* Create the VPC, Public & Private Subnets, route table, IGW
* Create the EC2 instance in public and private subnets
* Create the NAT Gateway
* Update the NAT gateway in the private route table
* Test the connection