| **Attribute** | **NAT gateway** | **NAT instance** |
| --- | --- | --- |
| 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. | Use a script to manage failover between instances. |
| Bandwidth | Scale up to 100 Gbps. | Depends on the bandwidth of the instance type. |
| Maintenance | Managed by AWS. You do not need to perform any maintenance. | Managed by you, for example, by installing software updates or operating system patches on the instance. |
| Performance | Software is optimized for handling NAT traffic. | A generic AMI that's configured to perform NAT. |
| Cost | Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways. | Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size. |
| Type and size | Uniform offering; you don’t need to decide on the type or size. | Choose a suitable instance type and size, according to your predicted workload. |
| Public IP addresses | Choose the Elastic IP address to associate with a public NAT gateway at creation. | 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. |
| Private IP addresses | Automatically selected from the subnet's IP address range when you create the gateway. | Assign a specific private IP address from the subnet's IP address range when you launch the instance. |
| Security groups | 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. | Associate with your NAT instance and the resources behind your NAT instance 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. | Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides. |
| Flow logs | Use flow logs to capture the traffic. | Use flow logs to capture the traffic. |
| Port forwarding | Not supported. | Manually customize the configuration to support port forwarding. |
| Bastion servers | Not supported. | Use as a bastion server. |
| Traffic metrics | View [CloudWatch metrics for the NAT gateway](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway-cloudwatch.html). | View CloudWatch metrics for the instance. |
| Timeout behavior | When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet). | When a connection times out, a NAT instance sends a FIN packet to resources behind the NAT instance to close the connection. |
| IP fragmentation | Supports forwarding of IP fragmented packets for the UDP protocol.  Does not support fragmentation for the TCP and ICMP protocols. Fragmented packets for these protocols will get dropped. | Supports reassembly of IP fragmented packets for the UDP, TCP, and ICMP protocols. |