AWS NAT Gateway

A Network Address Translation (NAT) gateway in Amazon Web Services (AWS) is a highly available, managed network component that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances.

NAT gateways are used to provide outbound-only internet connectivity for instances in private subnets, which do not have public IP addresses or Elastic IP addresses.

There are two types of NAT gateways:

- **A NAT gateway using a public IP address**: This type of NAT gateway allows instances in your private subnets to connect to the internet or other AWS services, but does not allow incoming traffic from the internet to reach your instances. The NAT gateway uses a public IP address to connect to the internet, and the traffic from your private instances is translated to the NAT gateway's public IP address before being sent out to the internet.
- **A NAT gateway using an Elastic IP address**: This type of NAT gateway works in the same way as a NAT gateway using a public IP address, but the NAT gateway uses an Elastic IP address instead of a public IP address.

  An Elastic IP address is a static, public IP address that you can assign to your NAT gateway and that you can use to connect to the internet.

If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To improve resiliency, 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.

The following characteristics and rules apply to NAT gateways:

- A NAT gateway supports the following protocols: TCP, UDP, and ICMP.
- NAT gateways are supported for IPv4 or IPv6 traffic. For IPv6 traffic, NAT gateway performs NAT64. By using this in conjunction with DNS64 (available on Route 53 resolver), your IPv6 workloads in a subnet in Amazon VPC can communicate with IPv4 resources.
- These IPv4 services may be present in the same VPC (in a separate subnet) or a different VPC, on your on-premises environment or on the internet.

- A NAT gateway supports 5 Gbps of bandwidth and automatically scales up to 100 Gbps. If you require more bandwidth, you can split your resources into multiple subnets and create a NAT gateway in each subnet.
- A NAT gateway can process one million packets per second and automatically scales up to ten million packets per second. Beyond this limit, a NAT gateway will drop packets. To prevent packet loss, split your resources into multiple subnets and create a separate NAT gateway for each subnet.
- Each IPv4 address can support up to 55,000 simultaneous connections to each unique destination. A unique destination is identified by a unique combination of destination IP address, the destination port, and protocol (TCP/UDP/ICMP). You can increase this limit by associating up to 8 IPv4 addresses to your NAT Gateways (1 primary IPv4 address and 7 secondary IPv4 addresses). You are limited to associating 2 Elastic IP addresses to your public NAT gateway by default. You can increase this limit by requesting a quota adjustment.
- You can pick the private IPv4 address to assign to the NAT gateway or have it automatically assigned from the IPv4 address range of the subnet. The assigned private IPv4 address persists until you delete the private NAT gateway. You cannot detach the private IPv4 address and you cannot attach additional private IPv4 addresses.
- You cannot associate a security group with a NAT gateway. You can associate security groups with your instances to control inbound and outbound traffic.
- You can use a network ACL to control the traffic to and from the subnet for your NAT gateway. NAT gateways use ports 1024–65535.
- A NAT gateway receives a network interface. You can pick the private IPv4 address to assign to the interface or have it automatically assigned from the IPv4 address range of the subnet. You can view the network interface for the NAT gateway using the Amazon EC2 console. You cannot modify the attributes of this network interface.
- A NAT gateway cannot be accessed through a ClassicLink connection that is associated with your VPC.
- You can't route traffic to a NAT gateway through a VPC peering connection, a Site-to-Site VPN connection, or AWS Direct Connect. A NAT gateway cannot be used by resources on the other side of these connections.