VPC Traffic Flow - Sequence of Steps

Request and Response

Let's look at the sequence of steps a request must go through before it reaches an AWS hosted endpoint.

Let's assume our endpoint is an EC2 instance.

External Request
  -> Internet Gateway
    -> Router / Route Table
      -> Network ACL (attached to subnet)
        -> Security Group (attached to instance)
          -> Public Instance

When Public Instance makes an outbound request, it flows in direction opposite to what is shown here.

Instances behind a NAT are private and cannot receive unsolicited in-bound request. However, they can make outbound request and receive a response.

Private Instance (in private subnet)
  -> Security Group
    -> Network ACL (for private subnet)
      -> Router / Route Table
        -> Network ACL (for public subnet where NAT is hosted)
          -> NAT (in public subnet)
            -> Router / Route Table
              -> Internet Gateway
                -> External Destination

Amazon Reference: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html