NAT Instance Source Destination Check

Chandra Lingam,

AWS networking infrastructure checks the source and destination of each network packet.

This check detects source IP address spoofing (for example, a malware running on an EC2 instance sending a packet with a different IP address as source)

It also prevents an EC2 instance from receiving a message that is meant for another EC2 instance.

If the source or destination address is invalid, it will drop the packet

Both these are done to protect the multi-tenant infrastructure and to protect your EC2 instances

NAT instance is a special EC2 instance. It acts as a middle-man to allow outbound internet calls for instances in a private subnet.

For this to work, you need to configure your private subnet route table to send all non-local traffic (for example: 0.0.0.0/0) to the NAT instance. NAT instance, in turn, sends and receives the requests on behalf of your private instance (It is very similar to a wireless router in your home network)

In order to specify a NAT instance as a **target** in the route table, you must disable Source and Destination Check on a NAT instance

- Select the **instance,** from **Actions,** Choose **Networking**
- Choose **Change Source/Dest. Check**
- Verify Source Destination Check is **disabled**

If source/destination check is not disable, you cannot specify a NAT instance as a target in the route table

Note: This comes up frequently in various certification exams