Every type of NAT we have done has one thing in common, we made a translation decision based upon matching just the source.

Let’s look at our static NAT example:

A diagram of a green circle with arrows and a tree

AI-generated content may be incorrect.

The router says to translate this IP address into that one. When the packet hits the router, it looks at the SRC IP address to see if it matches the configuration. Same for the static PAT:

A diagram of a green circular object with white dots and yellow wires

AI-generated content may be incorrect.

When that packet hits the router, it checks to see how the SRC IP address should be translated.

The same is for dynamic PAT and dynamic NAT too. They are all based upon matching the SRC of packets to the translation configuration of the router.

A policy NAT is making a translation decision based upon matching both the SRC and DST. This lets you translate packets differently based on where they are going not just where they are coming from. Once the packet is matched, the translation is done by the same type of translations that we have discussed. Policy NATs are just based on matching both the SRC and DST.

Let’s show an example of policy NAT:

A screenshot of a chat

AI-generated content may be incorrect.

NEXT PAGE

Notice the second condition is the regular condition for a dynamic PAT that if the SRC IP address is within the 10.6.6.0/24 network then translate it to the public IP address of 32.8.2.66. but the first condition is the policy NAT, which is that if the SRC IP address is within them 10.6.6.0/24 network and the DST IP address is 45.5.4.9 then translate the SRC IP address into the public IP address of 32.8.2.77.

Lets see this in action, we will also keep track of the routers translation table.

A screenshot of a computer

AI-generated content may be incorrect.

As we can see host A has the DST IP address which is within the IP space of 10.6.6.0/24 and the DST IP address is 45.5.4.9 so it will follow the policy NAT, and it will be translated into the public IP address of 32.8.2.7 which we can see is confirmed in the routers translation table.

As for host B, we can see that the SRC IP address is within the IP space of 10.6.6.0/24 and the DST IP address is not destined to 45.5.4.9 meaning it doesn’t pass the condition of the policy NAT, therefore it looks at the other condition and translates it to the default public IP address which we can see is confirmed in the routers translation table.

Also since this is a dynamic PAT, the IP address as well as the ports are changing.