PAT – changes IP addresses and ports (modifies layer 3 and layer 4 header)

Dynamic – translation device chooses POST attributes

Dynamic PAT – the administrator defines the set of pre and post translation attributes, and the device determines the actual post-translation IP address and port.

A screen shot of a computer

AI-generated content may be incorrect.

Here we are saying that the IP address space of 10.6.6.0/24 (all IP addresses in the inside network) will share this one public IP address. We can notice that the ports haven’t been displayed here even though it’s a PAT, we will cover that soon. But as of right now, all hosts in the inside network will share that one public IP address. The router will keep track of the translations it’s made in a translation table.

When host A sends a packet, it will come from the SRC IP address and port of 10.6.6.61:2222. When this packet hits the router, the router will see that it matches the dynamic PAT configuration and modify the IP:Port to the shared IP address (32.8.2.66) and to the port 7777.

A screenshot of a computer

AI-generated content may be incorrect.

As we can see the packet (after crossed the router) now has the SRC IP address:Port of 32.8.2.66:7777.

NEXT PAGE

Now when host B sends a packet, its SRC IP address is 10.6.6.62 and it will use a SRC Port of 3333. It will match our dynamic PAT mapping, then our routing will translate the source IP:Port to the shared IP addresses and a new port of 8888:

A screenshot of a computer

AI-generated content may be incorrect.

As we can see, after the packet crosses the router, the SRC IP address is now using the shared one and it has the new port of 8888.

Lets focus on the ports though, host A’s packet has a DST Port of 443 which we can tell that it is a HTTPS request. Host A’s packet has a DST Port of 80 which we can tell that it is a HTTP request.

When you’re making a well-known port request (HTTP, HTTPS, FTP, SMTP, SSH etc) the application is determining the DST Port, that is where the 443 and 80 come from. The SRC Ports.

As for the SRC Ports, they are randomly selected by the hosts, host A randomly selected Port 2222 and host B randomly selected Port 3333. There are around 65,000 available ports, sometimes, although rare, 2 hosts can both randomly choose the same SRC Port.

A computer screen shot of a diagram

AI-generated content may be incorrect.

As we can see host C randomly choose the same SRC Port as host B, but in the translation table, they get translated to different ports on the same public IP address.

Now lets explore the response traffic.

A computer screen shot of a diagram

AI-generated content may be incorrect.

So, the first server will send a response packet to host A with the SRC IP address:Port of 82.6.4.2:443 and the DST IP address:Port of 32.8.2.66:7777. This will cross the router, and the router will un-translate the DST IP address and notice that the incoming packet is destined to the first entry, so it knows to send it to host A. Now the second server will send a response packet to host B with the SRC IP address:Port of 28.2.4.6:80 and a DST IP address:Port of 32.8.2.66:8888, when it crosses the router, it will untranslated the DST IP address:Port and see that it is destined to host B, and it will then be forwarded to host B. The same happens for the last response packet.

Lets go back to the other image where the hosts were sending data to the servers:

A computer screen shot of a diagram

AI-generated content may be incorrect.

Take a look at the routers translation table, firstly the ports are chosen randomly by the hosts, then they are re-randomised again when they get translated into the public IP address, literally we can see they change. We will explore the reason for this:

NEXT PAGE:

A diagram of a computer

AI-generated content may be incorrect.

The image above is if the case was that the ports are not re-randomised after translation. So, if the ports do not get re-randomised, then host A chooses 2222 and keeps 2222, host B chooses 3333 and keeps 3333, then host C chooses 3333 also and keeps 3333.

Now when the servers respond, this is where it becomes problematic.

A screenshot of a computer

AI-generated content may be incorrect.

When the first server sends a response packet to host A, it works well because there is one entry for the port 2222, however for the second server sending a packet each to host C, both entries have the same public IP address with the same port of 3333, so both packets don’t know where to go, whereas when the ports are re-randomised after IP address translation, they have new ports so they know where to go.

A screenshot of a computer

AI-generated content may be incorrect.

These packets are literally identical, as well as the public IP:Port mapping, it wouldn’t know how to forward the packet.

An important thing is that dynamic PAT is unidirectional, traffic must be initiated from the inside first for outside traffic to ever come inside. If inside traffic was never initiated, whatever outside traffic comes in will be dropped, this is because no translation entry exists.

A screenshot of a computer

AI-generated content may be incorrect.

Host D wants to send data to the public IP address with the port of 443, we know that anything sent to the shared public IP address will definitely arrive to the router. When it arrives, it will check for an entry that matches the 443 port, because there isn’t one, the packet will be dropped. The router has no idea whether the packet is destined to host A or host B or any host within the 10.6.6.0/24 network IP space. The only reason the first 2 packets were able to be sent to host A and host B is because the traffic was initially initiated by them, host A and B sent data to the servers before the servers sent data back. Meaning that when host A and B sent data, that’s when the entry came, this allowed the server to send a response packed. Host Z cant send anything to any host in the inside network because nothing from the inside network ever sent anything to host Z in the first place meaning there is no entry for it, so the router will drop the packet. For traffic to flow, traffic must be initiated from the inside.

However, if you want that host Z data to go through you could combine a static PAT with our dynamic PAT, we could tell the router which host should get that packet by configuring a static PAT that says hey this IP address and port (32.8.2.66:443) will always map to this IP address and port (host C). If this static PAT is configured, then the router would know how to forward the packet.

A quick summary note is that dynamic PATs allow many hosts with private IP’s to share one public IP which is sometimes referred to as many to one or one to many. Dynamic PATs are the greatest potential for IP address conservation. Unique source ports must be re-assigned after IP translation as mentioned earlier. However, there is a limitation in this, this means that each shared public IP address allows for around 65,000 concurrent connections. To solve this just add more public IP addresses to allow for more than 65,000 connections. And also dynamic PATs are unidirectional meaning that internal hosts must initiate for outside traffic to ever be sent back to the hosts which initiated, if not then any packets from outside coming inside will be dropped... unless a static PAT is configured to allow that one packet configuration through.