

Service NAT

(NAT, PAT et Port Forwarding)

Comment un ordinateur (adresse privée) peut-il communiquer avec un serveur (adresse publique) sur Internet ?

1 – Pourquoi utilise-t-on le NAT

Les adresses IPv4 publiques sont limitées. Les réseaux locaux utilisent donc des plages privées, non routées sur l'Internet public.

Plage privée IPv4	Préfixe CIDR	Plage adresse IP
10.0.0.0	/8	10.0.0.0 à 10.255.255.255
172.16.0.0	/12	172.16.0.0 à 172.31.255.255
192.168.0.0	/16	192.168.0.0 à 192.168.255.255

À retenir

Une adresse privée peut être réutilisée dans des milliers de réseaux différents. Elle n'est pas unique à l'échelle mondiale et ne doit pas être annoncée sur Internet.

Solution : il faut "filtrer et modifier" les adresses IP privées

=> On remplace l'adresse privée par une adresse publique

Cette opération se nomme "Translation NAT". Elle est effectuée par le service NAT au niveau du routeur

2 – Types de services NAT

- Service NAT Statique (1 pour 1)

Le service NAT assure la translation d'adresse privée → publique. On dispose du même nombre d'adresses privées que d'adresses publiques. == > Très peu utilisé

Adresse interne	Adresse publique
10.0.1.6	194.34.56.2

- Service NAT Dynamique

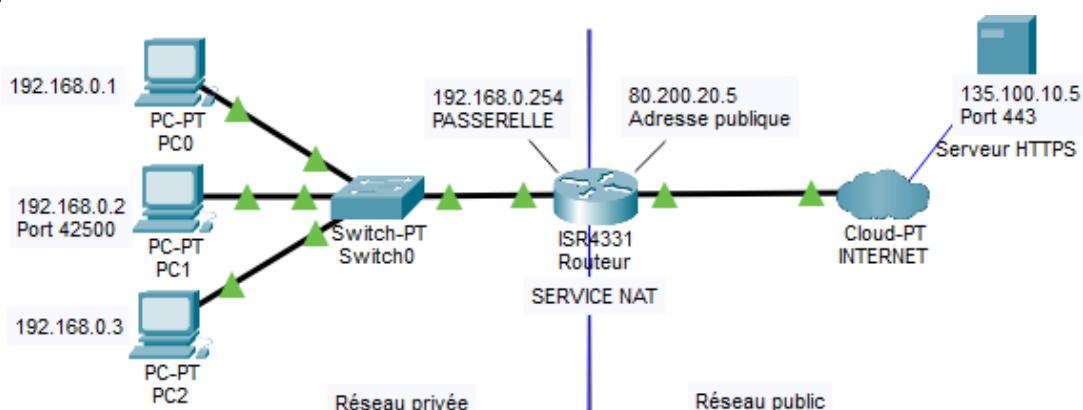
Les machines internes reçoivent temporairement une adresse parmi un pool d'adresses publiques disponibles. Le nombre de connexions simultanées est limité par la taille du pool.

Le NAT dynamique pur traduit les adresses mais ne repose pas obligatoirement sur la modification des ports. Il ne doit pas être confondu avec le PAT.

3 – Principe du service PAT

Exemple

PC1 (192.168.0.2) ouvre une connexion HTTPS vers 135.100.10.5:443. Le routeur possède l'adresse publique 80.200.20.5.



Cette communication s'effectuera en deux étapes : communication entre PC1 et le routeur (Service) NAT puis entre le routeur et le serveur.

Etape 1 : Communication entre PC1 et le routeur

@MAC Dest	@MAC Source	@IP source	@IP destination	Port Source	Port Destination
Passerelle	MAC PC1	192.168.0.2	135.100.10.5	42500	443

Etape 2 : Communication entre le routeur et le serveur

@MAC Dest	@MAC Source	@IP source	@IP destination	Port Source	Port Destination
MAC du prochain routeur	MAC routeur coté public	80.200.20.5	135.100.10.5	42500	443

Le serveur répond vers 80.200.20.5 et le port public 42500.

Le routeur consulte sa table de translation, remplace l'adresse et le port de destination par 192.168.0.2:42500, puis transmet le paquet à PC1.

Détail de la communication retour du serveur vers PC1.

Etape 1 : Communication entre le serveur et le routeur

@MAC Dest	@MAC Source	@IP source	@IP destination	Port Source	Port Destination
MAC du prochain routeur	MAC serveur	135.100.10.5	80.200.20.5	443	42500

Remarque

Le serveur ne sait pas qu'il communique avec PC1. Pour lui, son interlocuteur, c'est le routeur.

Etape 2 : Communication entre le routeur et PC1

@MAC Dest	@MAC Source	@IP source	@IP destination	Port Source	Port Destination
MAC PC1	MAC Passerelle	135.100.10.5	192.168.0.2	443	42500

Le routeur (Service NAT) met à jour sa table de translation NAT pour ne pas commettre d'erreurs de communication entre la source et le destinataire.

Table translation (PAT)	
Infos réseau local	Info réseau public
@IP Source / @IP Dest Port Source / Port Dest	@IP Source / @IP Dest Port Source / Port Dest
192.168.0.2 / 135.100.10.5 42500 / 80	80.200.20.5 / 135.100.10.5 42500 / 80

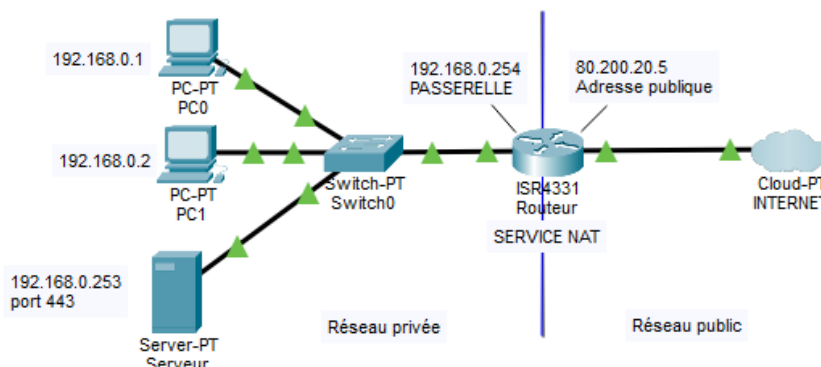
4 – Le port Forwarding

Cas où l'on souhaite consulter depuis Internet un serveur situé dans un réseau privé.

La demande venant de l'extérieur du réseau privé, la table de translation du routeur ne trouve pas de correspondance. Logiquement la demande est rejetée.

Solution : autoriser les demandes externes à accéder seulement au serveur interne.

⇒ **Mise en place d'une redirection : port FORWARDING.**



Le principe

Toute requête envoyée depuis Internet vers l'interface 80.200.20.5 avec le port 443 sera redirigée vers l'interface 192.168.0.253 sur le port 443.

Exemple de table FORWARDING

@ IP externe routeur (@IP publique)	Port externe (Routeur)	@IP interne (@IP serveur)	Port interne (Serveur)
80.200.20.5	443	192.168.0.253	443

5 – TD

En tant qu'administrateur, vous administrez le réseau 10.0.0.0/23 et disposez du bloc public 194.34.56.0/29. Proposez une solution de service NAT.

4 serveurs Web (port TCP 80)	@IP 10.0.1.6 → 10.0.1.9
2 serveurs DNS (port UDP 53)	@IP 10.0.1.11 → 10.0.1.12
Il y a 200 salariés environ	@IP 10.0.0.20 → 10.0.0.250

Travail demandé

- Identifier l'adresse réseau, l'adresse de broadcast et le nombre d'adresses hôtes utilisables du /23.
- Identifier les adresses théoriquement utilisables dans le /29 public et préciser qu'une adresse peut être réservée à la passerelle opérateur selon le contrat.
- Proposer une stratégie de PAT pour les postes utilisateurs.
- Proposer une redirection des quatre serveurs Web. Peut-on rediriger les quatre sur la même IP publique et le même port TCP 80 ? Justifier.
- Proposer une redirection correcte des deux DNS en TCP 53 et UDP 53.
- Produire une table finale : IP publique, protocole, port externe, IP interne, port interne, justification.

Solution

Le réseau 10.0.0.0/23

- Masque de sous réseau : 255.255.254.0
- Plage : 10.0.0.1 à 10.0.1.254.
- Adresse IP diffusion : 10.0.1.255

Adresses Utilisables dans le réseau en /29

- Nom réseau : 194.23.56.0
- Masque de sous réseau : 255.255.255.248
- Plage : 194.23.56.1 à 194.23.56.6
- Adresse de diffusion : 194.23.56.7

Stratégie PAT pour les postes salariés

Utilisation de la première adresse publique : 194.23.56.1. On fait du PAT.

Redirection des quatre serveurs Web

On peut utiliser une adresse publique par serveur WEB pour les deux ports : TCP 80/443

Rediriger les quatre serveurs web sur la même IP publique.

On peut utiliser une seule IP publique en TCP 80/443. Le service NAT distribue ensuite les requêtes vers les quatre serveurs selon le nom DNS ou le chemin demandé dans l'URL.

Redirection correcte des deux DNS

Il faut penser à rediriger le protocole TCP 53 mais aussi UDP 53 vers le serveur DNS.

Table finale : IP publique, protocole, port externe, IP interne, port interne

Fonction	Protocole	IP publique	Port externe	IP interne	Port interne
Sortie Internet Salariés	HTTP / HTTPS / DNS 80 / 443 / 53	194.34.56.1	80/443/53	10.0.0.20 → 10.0.0.250	Variable, dépend du PC
Serveur web 1	TCP	194.34.56.2	80/443	10.0.1.6	80/443
Serveur DNS 1	TCP / UDP		53	10.0.1.12	53
Serveur web 1	TCP	194.34.56.3	80/443	10.0.1.7	80/443
Serveur web 1	TCP	194.34.56.4	80/443	10.0.1.8	80/443
Serveur web 1	TCP	194.34.56.5	80/443	10.0.1.9	80/443
Serveur DNS 1	TCP / UDP	194.34.56.6	53	10.0.1.11	53

Il y a plusieurs solutions.