Administration des Systèmes et Réseaux

LES SERVEURS NAT ET PAT

Translation d'adresses et de ports et redirection de ports

Auteur: Bernard GIACOMONI - Autoentreprise GIACOMONI Bernard

Version	Date	Objet
1.0	21/10/2019	Version initiale

Table des matières

I. INTRODUCTION:.....3
II. MÉCANISMES DE TRANSLATION :.....4
II.1. TRANSLATION D'ADRESSE STATIQUE (STATIC NAT):.....4
II.1.1. PRINCIPE:.....4
II.1.2. LIMITES DE LA TRANSLATION D'ADRESSE STATIQUE:.....5
II.2. TRANSLATION D'ADRESSES "DYNAMIQUE" (DYNAMIC NAT) :.....5
II.2.1. TRANSLATION DE PORT-INTERROGATION D'UN SERVEUR WAN PAR UN CLIENT LAN :.....5
II.2.2. LIMITES DE LA NAT DYNAMIQUE:.....7
II.3. LA TRANSLATION DE PORT (PORT FORWARDING):.....7
II.3.1. LA REDIRECTION DE PORT (PORT FORWARDING):.....7
II.3.2. CAS PARTICULIER DES SERVEURS:.....8

I.INTRODUCTION:

L'existence des adresses IP V4 privées permet de limiter l'attribution des adresses IP publiques (routables) aux seuls équipement connectés directement au web (les machines connectées au web par des lignes dédiées ou les "routeurs web"). Elle permet donc de pallier dans une certaine mesure la pénurie d'adresses IP V4. Elle permet également de sécuriser les réseaux locaux contre les attaques en provenance de l'extérieur en masquant les adresses IP des machines locales.

Cependant, les hôtes d'un réseau local dotés d'adresses IP privées non routables, ne peuvent communiquer directement avec les machines situées en dehors du LAN. Or, il est souvent nécessaire qu'un hôte d'un LAN puisse interroger un serveur sur le web pour se connecter à des sites HTTP, télécharger des fichiers, émettre des mails, interroger des boîtes mail, etc. De même, il doit être possible d'installer dans un LAN des serveurs accessibles depuis le web.

Ces possibilités sont offertes par les technique de TRANSLATION D'ADRESSES et de TRANSLATION DE PORTS offertes par les serveurs NAT/PAT (Network Address Translation et Port Address Translation).

II.MÉCANISMES DE TRANSLATION :

II.1.TRANSLATION D'ADRESSE STATIQUE (STATIC NAT):

II.1.1.PRINCIPE:

La Translation d'Adresses Réseau ou Network Address Translation (NAT) consiste à établir une correspondance entre des adresses IP privées d'un LAN et des adresses IP publiques (routables), puis à remplacer dans les messages une adresse par sa correspondante selon que l'on émet depuis le LAN vers le WAN ou inversement. Le schéma ci-dessous illustre ce mécanisme :

EXEMPLE DE TABLE NAT STATIQUE :

La table ci-dessous met en correspondance des adresses locales et des adresses publiques routables:

Adresse IP locale (attribuée localement)	Adresse IP routable (attribuée par l'IANA)
192.168.1.1	203.22.71.16
192.168.1.3	196.67.24.251
192.168.1.7	17.22.56.187

COMMENTAIRES:

Au niveau de la passerelle LAN/WAN (routeur web, box, etc.), le logiciel NAT effectue les opérations suivantes:

- Dans les requêtes adressées par les hôtes locaux au LAN vers des hôtes extérieurs, l'adresse d'émission (adresse IP locale de l'émetteur) est remplacée pas l'adresse IP routable qui lui correspond dans la table. Par exemple, dans une requête émise par la machine d'adresse IP 192.168.1.3, cette adresse serait remplacée par 196.67.24.251 si le NAT utilisait le tableau ci-dessus;
- Dans les requêtes adressées par une machine extérieure au LAN à une machine locale, l'adresse de destination (qui est l'adresse IP routable associée à l'hôte) est remplacée par l'adresse locale correspondante. Par exemple, dans la réponse émise par la machine qui a reçu la précédente requête, l'adresse de destination 196.67.24.251 serait remplacée par l'adresse interne 192.168.1.3 si le NAT utilisait le tableau ci-dessus.

Pour l'extérieur du LAN, les adresses locales sont MASQUÉES par les adresses publiques qui leur correspondent.

REMARQUES:

- La translation d'adresse, telle qu'elle est décrite ci-dessus, concerne uniquement la couche réseau (couche IP de TCP/IP, couche 3 de l'OSI). Elle peut donc être implantée directement en-dessus de la couche IP du routeur, ce qui la rend transparente pour les applications;
- Pour que le système de translation d'adresses fonctionne, il est nécessaire que les hôtes locaux concernés par la translation soient en mode "IP fixe";
- La translation d'adresse, telle qu'elle est décrite ci-dessus est souvent appelée "NAT STATIQUE" car les correspondances entre IP publiques et privées sont des données statiques.

II.1.2.LIMITES DE LA TRANSLATION D'ADRESSE STATIQUE:

Le mécanisme de translation d'adresses décrit ci-dessus a l'avantage d'être très simple. Il permet effectivement aux machines locales de dialoguer avec les machines externes tout en masquant les adresses IP internes pour l'extérieur du LAN. Cependant, comme il implique de disposer d'une adresse publique pour chaque adresse interne, il ne permet pas d'économiser des adresses publiques.

II.2.TRANSLATION D'ADRESSES "DYNAMIQUE" (DYNAMIC NAT) :

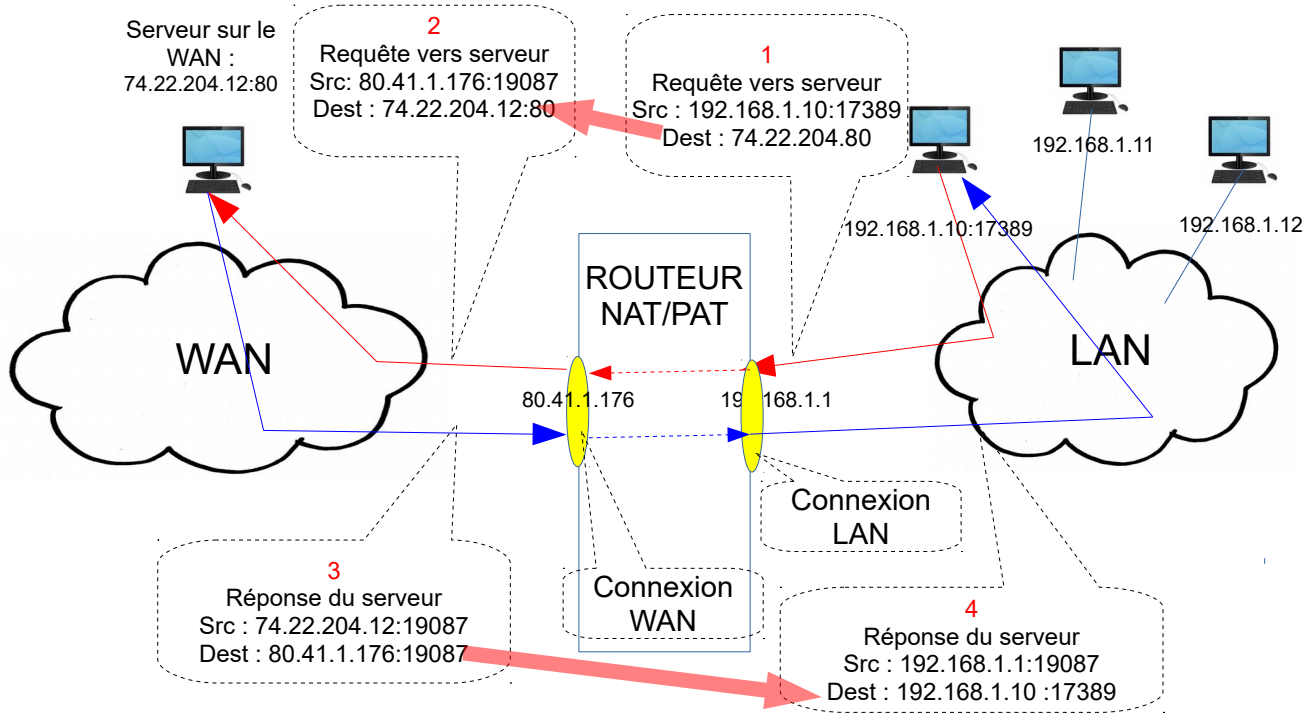
II.2.1.TRANSLATION DE PORT-INTERROGATION D'UN SERVEUR WAN PAR UN CLIENT LAN :

Pour faire effectivement une économie d'adresses publiques, il faut réussir à MASQUER PLUSIEURS adresses locales par UNE SEULE adresse publique. Ceci peut être réalisé par la Translation de Port (ou Port Address Translation – PAT), dont le mécanisme est décrit ci-après:

- ***Émission vers un serveur du WAN***: lorsqu'un client appartenant au LAN émet une requête vers un serveur du WAN, le routeur effectue dans les paquets correspondants les transformations suivantes:
  - Il remplace l'adresse de l'émetteur par une des adresse publiques dont il dispose (c'est la translation d'adresse ou NAT). La couche IP est donc modifiée;
  - Il remplace également la valeur du port source par une autre valeur qu'il choisit dynamiquement et automatiquement dans une plage d'adresses permises (c'est la translation de port ou PAT). La couche TCP est donc également modifiée;
  - Il tient à jour pour chaque IP publique qu'il utilise une table de correspondance entre les numéros des ports qu'il a attribués et les adresses et ports internes du client (c'est la "table NAT dynamique");
- ***En réception de la réponse du serveur***, le routeur utilise la table de correspondance pour effectuer dans les paquets reçus les translations suivantes:

- En fonction de la valeur du port destinataire, il substitue à l'adresse IP publique de destination l'adresse IP interne du client;
- Il substituer à la valeur du port destinataire la valeur du port source interne (port interne du client) qu'il a conservé dans la table NAT.

Le schéma commenté de la page suivante illustre ce mécanisme dans le cas où un hôte du LAN (client) interroge un serveur situé à l'extérieur de ce LAN :



COMMENTAIRES:

- L'hôte 192.168.1.10 du LAN émet depuis le port 17389 une requête vers le serveur 74.22.204.12 (port 80), par l'intermédiaire de la passerelle par défaut (le routeur);
- Le routeur relaie cette requête vers le serveur après avoir substitué son adresse externe publique 80.41.1.176 à d'adresse IP locale source (couche IP) et le numéro de port 19087 au numéro de port source 17389 (couche TCP). En même temps, il mémorise les valeurs substituées. Le routeur substitue DYNAMIQUEMENT à la valeur du port source d'origine une valeur qu'il choisit dans certaines plages qui lui sont allouées;
- Pour le serveur, la requête qu'il reçoit alors a été émise par le socket 80.41.1.176:19087. Il renvoie donc la réponse à ce socket;
- A la réception de la réponse sur sa connexion WAN, le routeur la redirige vers sa connexion LAN en faisant les substitutions inverses: l'IP destination 192.168.1.10 est substituée à l'IP 80.41.1.176 et le port destination 17389 est substitué au port

19087.

L'hôte client émetteur de la requête reçoit donc bien la réponse à sa requête comme si le serveur était connecté directement au LAN.

II.2.2.LIMITES DE LA NAT DYNAMIQUE:

Le mécanisme de NAT/PAT dynamique ne fonctionne que dans le cas où le premier message est émis par un hôte du LAN (en effet, c'est ce premier message qui lui permet de faire l'association de l'adresse privée à une valeur de port externe). Dans le cas où c'est un hôte externe au LAN qui initie l'échange, aucune association entre le port externe de destination et un couple @IP interne/ports interne n'est disponible. Le routeur est donc incapable de déterminer à quel hôte du LAN le message s'adresse.

Le mécanisme de NAT/PAT dynamique ne fonctionne donc que dans le cas où le premier message est émis par un hôte du LAN, car c'est ce premier message qui lui permet de créer l'association de l'adresse privée à une valeur de port source externe.

De ce fait, si le NAT/PAT dynamique permet à un CLIENT du LAN d'interroger un SERVEUR externe au LAN, il ne permet pas d'héberger sur le LAN un SERVEUR utilisable par des clients externes au LAN.

II.3.LA TRANSLATION DE PORT (PORT FORWARDING):

II.3.1.LA REDIRECTION DE PORT (PORT FORWARDING):

Elle consiste tout simplement à établir une correspondance STATIQUE (sous forme d'un tableau de redirection de ports) entre les couples (adresse publique, valeur de ports destination) des paquets entrant dans le routeur et les couples (adresse privée, port interne):

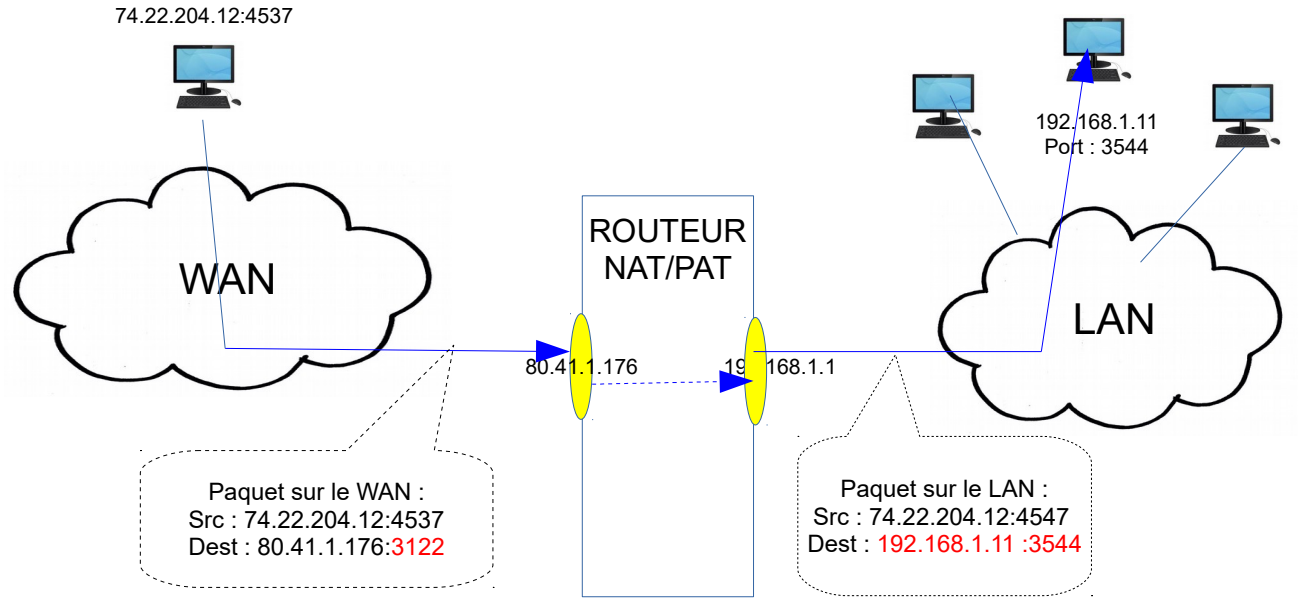
- Lorsqu'un paquet en provenance du WAN atteint le routeur, celui-ci vérifie que la valeur de son port de destination figure dans le tableau;
- Si cette valeur est absente du tableau, le paquet est traité normalement par le NAT/PAT dynamique: il est accepté s'il correspond à la réponse d'un serveur, sinon il est rejeté;
- Si cette valeur est dans le tableau, le routeur remplace l'adresse IP de destination et la valeur du port de destination par les valeurs contenues dans le tableau et émet le paquet sur le LAN.

Le schéma suivant illustre ce fonctionnement :

EXEMPLE: Supposons que la table de redirection de ports d'un routeur contienne les données suivantes:

@IP publique	Port externe	@IP privée	Port interne
80.41.1.176	3122	192.168.1.11	3544

A la réception sur l'interface public 80.41.1.176 du routeur d'un paquet dont le port de destination est 3122, le logiciel de redirection de port va remplacer l'adresse de destination 80.41.1.176 par 192.168.1.11 et la valeur du port de destination par 3544, puis il va émettre ce paquet sur le LAN. Le paquet sera donc redirigé vers le processus qui a ouvert le port 3544 dans l'hôte 192.168.1.11 :



La redirection de port permet donc à des clients extérieurs d'adresser des messages à des logiciels hébergés par des hôtes du LAN sans que ces messages constituent des réponses à des requêtes de ces hôtes. Elle permet donc, en particulier de rendre accessible de l'extérieur un SERVEUR interne au LAN.

II.3.2.CAS PARTICULIER DES SERVEURS:

Certains numéros de ports sont assignés par l'IANA (Internet Assigned Numbers Authority) dans la plage 0-1023. En particulier, des valeurs par défaut sont assignées aux ports d'écoute des principaux types de serveurs: 80 pour HTTP (serveur web), 21 pour FTP, 22 pour SSH, 23 pour Telnet, 25 pour SMTP et 110 pour POP3, etc.

Lorsqu'un client interroge un serveur, il le fait par l'intermédiaire d'une URL. Cette URL permet d'indiquer le numéro de port d'écoute (par exemple, l'URL

http://www.monsiteweb.fr:3456 permet d'envoyer une requête de protocole http sur le port 3456 du site web dont l'URL est www.monsiteweb.fr), mais dans la pratique, seuls des utilisateurs avertis sont capables d'utiliser cette possibilité. De ce fait, c'est la valeur par défaut qui est prise en compte dans l'immense majorité des cas. Pour une requête HTTP, la valeur par défaut est 80: la requête sera donc adressée à ce port.

En résumé, même si techniquement on peut toujours assigner à un serveur un autre port d'écoute que le port par défaut, et si l'on peut prendre en compte cette valeur dans les URL, cette option n'est pas idéale du point de vue de l'utilisateur.

De ce fait, POUR UNE MÊME ADRESSE IP EXTERNE, il ne peut y avoir sur un LAN qu'UN SEUL SERVEUR D'UN TYPE DONNÉ ACCESSIBLE DE L'EXTÉRIEUR (un seul serveur HTTP, un seul serveur FTP, etc.): pour avoir plusieurs serveurs de même type, il faut pouvoir assigner chacun d'eux à une adresse IP externe différente:

EXEMPLE :

Soit le tableau de redirection de ports suivant :

@IP publique	Port externe	@IP privée	Port interne
80.41.1.176	80	192.168.1.11	80 (HTTP)
80.41.1.176	21	192.168.1.11	21 (FTP)
80.41.1.178	80	192.168.1.12	80 (HTTP)
80.41.1.178	25	192.168.1.12	25 (TELNET)

COMMENTAIRES :

- Dans ce tableau de redirection de ports, nous pouvons voir que le LAN héberge deux serveurs HTTP (port 80). C'est possible car ces deux serveurs sont masqués par des adresses publiques différentes : 80.41.1.176 et 80.41.1.178 ;
- Le poste d'adresse privée 192.168.1.11 héberge deux serveurs : un serveur HTTP et un serveur FTP, tous deux masqués par la même adresse publique (80.41.1.176).