TP N°6 : Configuration de la translation d'adresse (NAT)

Dans ce TP on s'intéressera à la configuration d'un translateur d'adresses sur un routeur Cisco. Ce mode permet de se servir de passerelles (de routeur dans notre cas) de manière transparente à un réseau local. Les adresses privées du réseau local ne sont pas visibles de l'extérieur, seule l'adresse de la passerelle l'est.

1. Introduction

La fonction de translation d'adresses NAT permet d'utiliser des adresses IP privées sur un LAN et de translater ces adresses pour les rendre accessible depuis un réseau public comme Internet.

Pour cela, la traduction NAT se sert d'une adresse publique qu'elle substitue à l'adresse privée de chaque paquet sortant. Le réseau privé est définit sur l'interface intérieure et l'adresse publique sur l'interface extérieure du routeur, comme illustré à la figure 1.

Le système Cisco IOS supporte plusieurs variantes de NAT :

1.1. Traduction statique

Dans sa forme la plus simple, NAT statique, une adresse privée unique est redirigée, vers une adresse publique unique.

Par exemple, toute adresse source d'un paquet émanant de 10.10.10.1 sera remplacée par l'adresse 171.16.68.1. Cette dernière est employé par le routeur pour le compte de l'adresse privée. La traduction statique représente une configuration qui crée une relation simple, de cardinalité (1,1), où à une adresse utilisée publiquement correspond une seule adresse utilisée en privée.

1.2. Traduction dynamique

La traduction dynamique ressemble à la traduction statique, c'est-à-dire qu'à une adresse globale correspond une seule adresse locale. La différence réside dans le fait que la substitution se fait dynamiquement.

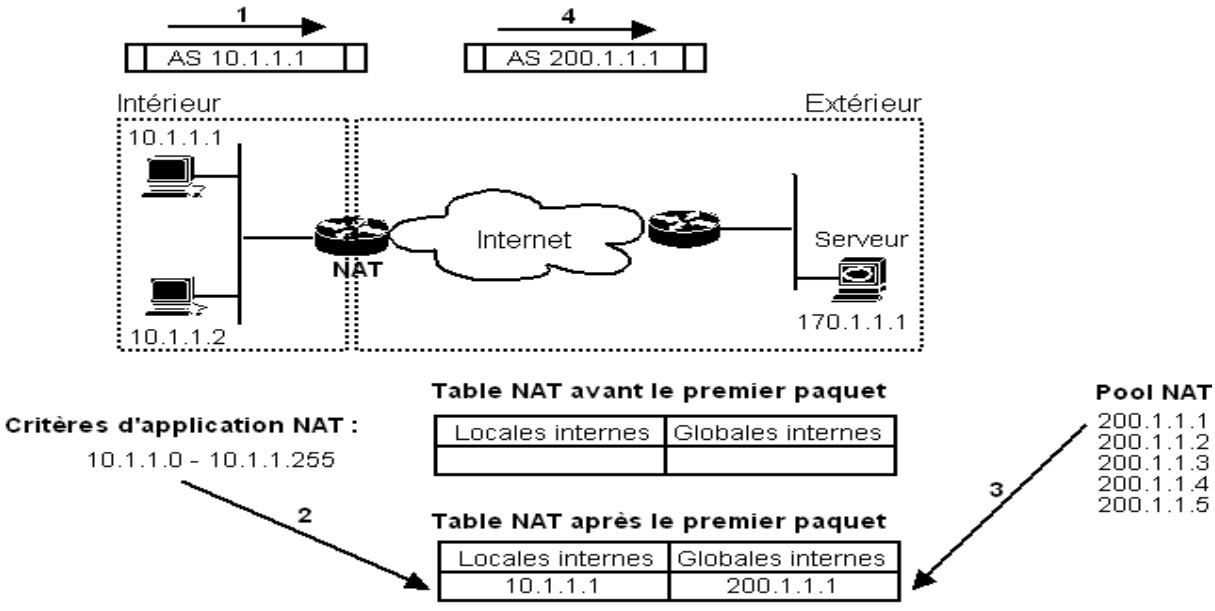


Figure1 : *Traduction NAT dynamique.*

Cette configuration définit un pool d'adresses globales internes et des critères pour désigner l'ensemble des adresses locales internes qui doivent être remplacées. La figure 1 spécifie un pool de cinq adresses globales internes, de 200.1.1.1 à 200.1.1.5. Nat a été configuré pour traduire les adresses qui commencent par 10.1.1 dans les paquets sortants. Les chiffres 1, 2, 3 et 4 dans la figure illustrent la succession des événements.

A Noter que le routeur alloue les adresses définies dans le pool jusqu'à épuisement de celles-ci.

1.3. Traduction étendue avec PAT ou overloading

NAT ne peut gérer simultanément que le nombre d'hôtes défini par le nombre d'adresses du pool. Un problème se pose donc lorsque le nombre d'adresses disponibles est inférieur à celui des adresses à servir. C'est le cas d'une entreprise où un très grand pourcentage d'hôtes internes accèdent à Internet, ce qui entraîne la nécessité d'avoir une grande quantité d'adresses publiques.

L'overloading, ou traduction PAT (*Port Address Translation*), permet à NAT de mieux s'adapter à l'augmentation des clients Internet d'une entreprise, au moyen de quelques adresses publiques seulement.

PAT tire partie de la façon dont TCP/IP se sert des ports. Pour servir une grande quantité d'adresses locales internes avec peu d'adresses globales internes publiques, PAT utilise un numéro de port en plus de l'adresse. Pour chaque combinaison unique d'adresse locale et une entrée de port correspond une combinaison unique d'adresse globale et de port. La figure 2 illustre le principe de traduction étendue avec PAT.

1.4. Traduction lors de chevauchement d'adresses (overlapping)

La traduction dynamique peut également être utilisée dans le cas où un réseau interne ne recourt pas aux adresses privées mais à des adresses publiques déjà enregistrées par une société.

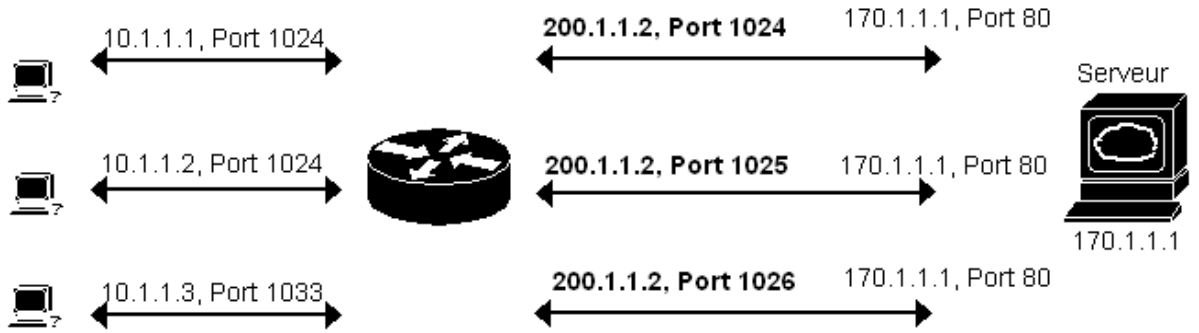


Figure 2 : Traduction étendue avec PAT.

Considérant le cas de la figure 3. Du fait que l'espace d'adressage se chevauche, un client de la société A ne peut envoyer un paquet IP à l'hôte légitime, 170.1.1.1. Dans la figure, l'hôte 170.1.1.10 verrait cette adresse comme étant l'adresse d'un hôte d'un même LAN et n'enverrait même pas le paquet au routeur.

NAT peut résoudre ce problème en substituant l'adresse de destination 170.1.1.1 (dite *adresse globale externe*) par l'adresse de destination 192.168.1.1. Celle-ci est appelée adresse locale externe car elle est utilisée sur le réseau local pour désigner un hôte externe situé sur Internet.

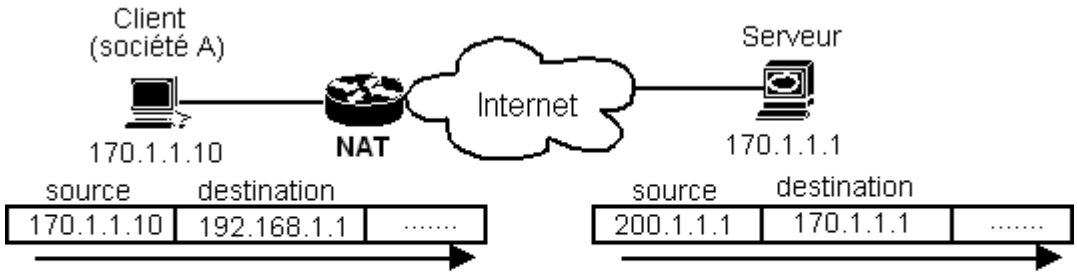


Table NAT après le premier paquet

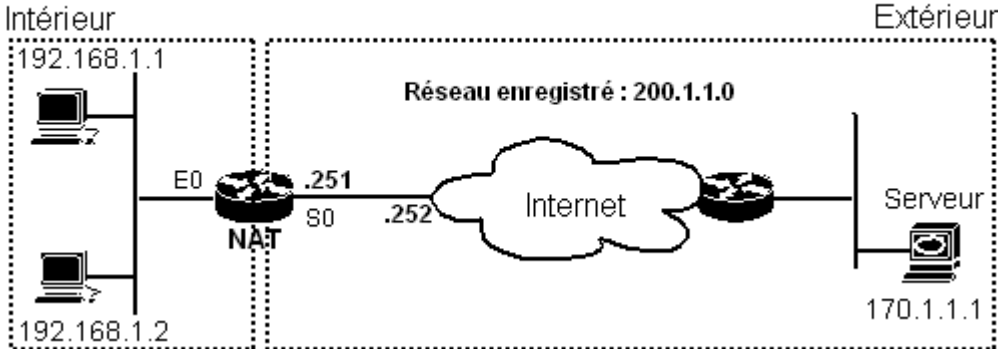
Locales iinternes	Globales internes	Locales externes	Globales externes
170.1.1.10	200.1.1.1	192.168.1.1	170.1.1.1

Figure 3 : Traduction lors de chevauchement d'adresses.

2. Travail à réaliser

Considérant la topologie de réseau d'entreprise ci-dessous. Le routeur principal est connecté au LAN par l'interface Ethernet 0 (192.168.1.3/24), donc E0 sera l'interface intérieure et S0 l'interface connectée à Internet (200.1.1.251/24).

Nous voulons que le routeur principal convertisse les adresses privées du LAN sur l'adresse IP autorisée du réseau 200.1.1.0. Pour cela, on définit les scénarios 1, 2, 3 et 4 à mettre en œuvre. Pour chaque scénario, il est demander de configurer la traduction NAT appropriée et d'afficher les informations pertinentes concernant NAT.



Scénario 1 - Configuration NAT statique

Les hôtes A et B doivent pouvoir accéder au serveur via la commande Telnet et/ou ping.

Scénario 2 - Configuration NAT dynamique

Les adresses globales sont réunies sous forme d'un pool d'adresses **net-200** qui seront assignées dynamiquement. Le pool contient les adresses de 200.1.1.1 à 200.1.1.5. Les hôtes A et B doivent pouvoir accéder au serveur.

Scénario 3 - Configuration NAT avec PAT

Dans ce scénario, le FAI a donné à l'entreprise un sous-ensemble du réseau 200.1.1.0, le sous-réseau CIDR 200.1.1.248/30. Autrement dit, l'entreprise possède deux adresses utilisables : 200.1.1.249 et 200.1.1.250. La fonction NAT sur le routeur de l'entreprise doit traduire les adresses locales en l'adresse 200.1.1.249.

Annexe:

A. Terminologie NAT

Dans la terminologie employé avec NAT, nous avons d'un coté des adresses privées et, de l'autre, des adresses publiques. Cisco emploie le terme *inside local address*, soit adresses locales internes pour les premières, et le terme *inside global address*, soit adresses globales internes pour les secondes.

Dans certaines configurations, il est cependant possible de recourir au changement d'une adresse désignant un hôte externe. Dans ce cas, les adresses seront qualifiées de *globales externes* et *locales externes*, c'est-à-dire qu'elles seront utilisées sur le réseau public ou privé, mais l'hôte se trouvera à l'extérieur.

Type d'adresse	Description
Locale interne	Adresse qui désigne un hôte situé sur un réseau interne d'entreprise et ne peut pas être présentée à l'extérieur, sur le réseau public. Elle est donc utilisée en privé uniquement.
Globale interne	Adresse qui désigne un hôte situé sur un réseau interne d'entreprise mais qui est utilisée sur le réseau public. C'est l'adresse que le routeur NAT substitue à l'adresse source d'un paquet sortant.
Globale externe	Adresse qui désigne un hôte situé sur un réseau public extérieur au site NAT, soit Internet, et qui est utilisée sur ce réseau.
Locale externe	Adresse qui désigne un hôte situé sur un réseau public extérieur à l'entreprise, soit Internet, mais qui est utilisée sur le réseau interne de l'entreprise. Elle est souvent identique à l'adresse globale externe sauf dans une certaine configuration où le routeur NAT la substitue à l'adresse globale externe.

B. Commandes de configuration de NAT

B.1 – Configuration NAT statique

étape	Commande	objectif
1	**ip nat inside source static** local-ip global-ip	Establish static translation between an inside local @ and an inside global @.
2	**Interface** type number	Specify the inside interface.
3	**ip nat inside**	Mark the interface as connected to the inside.
4	**Interface** type number	Specify the outside interface.
5	**ip nat outside**	Mark the interface as connected to the outside.

B.2 – Configuration NAT dynamique

étape	Commande	objectif
1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}	Define a pool of global addresses to be allocated as needed.
2	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Define a standard access list permitting those addresses
3	**ip nat inside source list** *access-list-number* **pool** *name*	Establish dynamic source translation, specifying the access list defined in the prior step.

4	**Interface** type number	Specify the inside interface.
5	**ip nat inside**	Mark the interface as connected to the inside.
6	**Interface** type number	Specify the outside interface.
7	**ip nat outside**	Mark the interface as connected to the outside.

Note: The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access-list.) An access list that is too permissive can lead to unpredictable results.

B.3 – Configuration NAT avec PAT (overloading)

étape	Commande	objectif
1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}	Define a pool of global addresses to be allocated as needed.
2	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Define a standard access list.
3	**ip nat inside source list** *access-list-number* {**interface** *type-num*| **pool** *name*} **overload**	Establish dynamic source translation, identifying the access list defined in the prior step.
4	**Interface** type number	Specify the inside interface.
5	**ip nat inside**	Mark the interface as connected to the inside.
6	**Interface** type number	Specify the outside interface.
7	**ip nat outside**	Mark the interface as connected to the outside.

Remarque: Pour configurer la traduction statique des adresses externes (outside source address) il suffit de remplacer le mot clé **inside** par **outside** dans l'étape 1. Idem pour la traduction dynamique, remplacer **inside** par **outside** dans l'étape 3.

C. Commandes de vérification de NAT

Il vous est possible d'utiliser la commande "**debug ip nat**" pendant que vous pingez les hôtes des deux cotés du tunnel pour vérifier le bon fonctionnement du NAT. D'autres commandes utiles sont :

Commande	objectif
show ip nat statistics	Affiche les compteurs pour les paquets et les entrées de la table NAT ainsi que des informations de configuration basiques.
show ip nat translations [verbose]	Affiche la table NAT.
clear ip nat translation *	Supprime la totalité des entrées dynamiques de la table NAT.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Supprime une entrée dynamique selon les paramètres utilisés.