TD 8 Réseaux – Network Address Translation (NAT)

Rappel sur les connexions TCP/UDP

Une "connexion" est un ensemble de trames cohérentes (au sens adresse IP, port, séquence, fonctionnalité, …).
Pour TCP, le schéma d'échange de données : **SYN**/SYN+ACK/**ACK**/…/**FIN**/ACK/FIN/**ACK** définit la "connexion" pourvu que les adresses IP, les numéros de ports, et les numéros de séquences soient cohérents. Dans le cas de UDP la "connexion" est définie par les adresses IP et les numéro de ports.

Translation d'adresse (NAT)

Le principe de la translation d'adresse est, pour une "connexion" donnée, de modifier l'adresse IP et/ou le numéro de port d'une des extrémités de la "connexion" à la traversée du translateur.

Le **S**NAT (**Source** NAT) consiste à modifier l'adresse IP **source** et/ou le port **source** d'une « connexion » entre le client C et le serveur S. Coté client la connexion est établie entre C.C.C.C:c et S.S.S.S:s, coté serveur elle semble établie entre N.N.N.N:n et S.S.S.S:s.
Dans le sens C->S le NAT change C.C.C.C:c en N.N.N.N:n
Dans le sens S->C le NAT change N.N.N.N:n en C.C.C.C:c
Applications : Partage de connexion, masquage d'un réseau privé

Le **D**NAT (**Destination** NAT) consiste à modifier l'adresse IP **destination** et/ou le port **destination** d'une connexion entre le client C et le serveur S. Coté client la connexion est établie entre C.C.C.C:c et N.N.N.N:n, coté serveur elle semble établie entre C.C.C.C:c et S.S.S.S:s.
Dans le sens C->S le NAT change N.N.N.N:n en S.S.S.S:s
Dans le sens S->C le NAT change S.S.S.S:s en N.N.N.N:n
Applications : redirection de services, accès aux serveurs d'un réseau privé.

Traduction statique

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

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. Cette configuration définit un pool d'adresses globales internes et des critères pour désigner l'ensemble des adresses locales internes qui doivent être remplacées.

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.
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.

Exercice 1

Soit une DMZ d'adresse IP : 200.100.0.0. Ce réseau est connecté à l'Internet par un routeur d'adresse IP interne 200.100.0.1. Cette DMZ comporte des bastions, entre autre un DNS. Un second routeur 200.100.0.2 permet d'accéder au réseau interne (privé) 192.168.0.0, son IP est 192.168.0.2.

Le réseau interne comporte un DNS/serveur Web (192.168.0.22), un serveur ftp (192.168.0.18), un serveur de mail/serveur pop3 (192.168.0..55). Le réseau interne comporte également des stations de travail.

1) Dessiner l'architecture de ce réseau.
2) Comment sont configurées les tables de routages des différentes machines de ce réseau ?
3) Les machines internes peuvent-elles accéder à l'internet ? Pourquoi ? Solution. Détailler la connexion.
4) Les machines internes peuvent-elles accéder aux services internes ? Par quelles adresses IP et quels ports ?
5) Les machines de l'internet peuvent-elles accéder aux services internes ? Pourquoi ?
6) Le routeur .2 fait du DNAT sur l'adresse IP 200.100.0.2. Que cela signifie-t-il ?
7) Les machines de l'internet peuvent-elles accéder aux services internes ? Par quelles IP et quels ports ?
8) Le DNS de la DMZ est un esclave d'un DNS master situé dans le réseau interne. Que cela implique-t-il au niveau du DNAT ?
9) La machine www.mon.site.com est le serveur web .22. Quelle est l'entrée DNS qui permet sa résolution ?
10) Depuis le réseau interne une machine tente de se connecter à www.mon.site.com, le DNS interne est le master du DNS de la DMZ. Quelle adresse IP va être utilisée ?
11) Donner alors le schéma d'établissement de la connexion tcp entre client et serveur ? Montrer que la connexion ne peut s'établir.
12) Proposer une solution basée sur le DNS.
13) Que faire pour que le service SMTP fonctionne pour les clients internes et pour l'internet ?
14) Que peut-on faire pour le service pop3 ?

Exercice 4

Soit le réseau de la figure ci-dessous à utiliser comme base pour répondre aux questions portant sur NAT.

1) Définissez le terme adresse locale interne dans le contexte NAT (pour la réponse utilisez la figure).
2) Définissez le terme adresse globale interne dans le contexte NAT (pour la réponse utilisez la figure).
3) Créez une configuration NAT étendue (overload) pour la traduction d'une seule adresse IP pour le routeur NAT.
4) Créez une configuration NAT en faisant correspondre l'hôte 10.1.1.1 à l'adresse 200.1.1.11 pour le routeur NAT.

Annexe: Configuration NAT sur routeur Cisco

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.

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.