TD N° 3

Rémy Grünblatt – remy@grunblatt.org

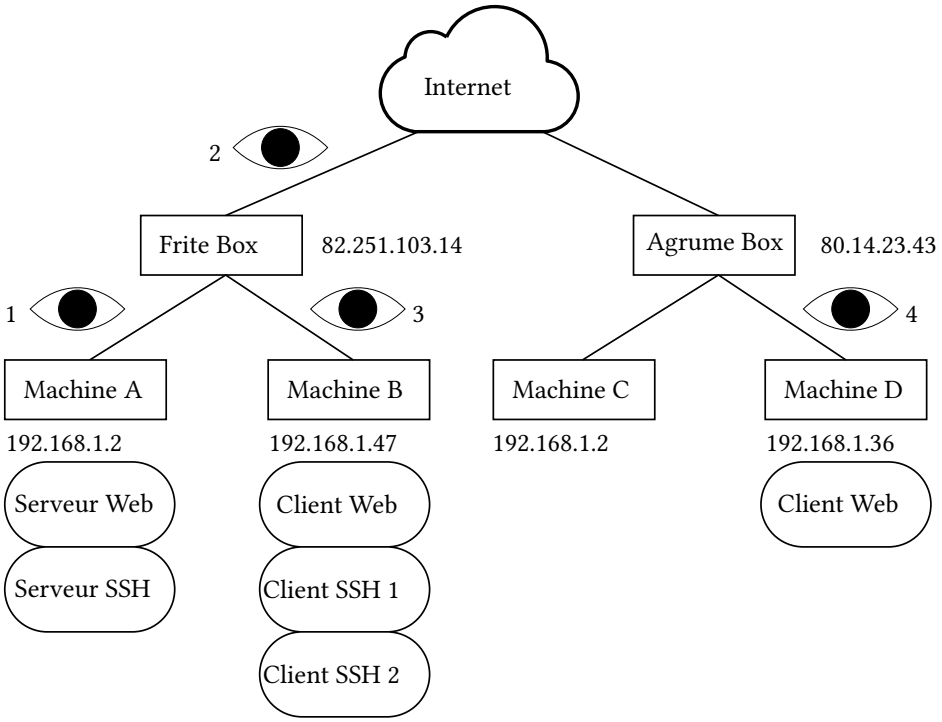
20 février 2020

Réseaux IPs : Network Address Translation (NAT)

En IPv4, il n'y a pas suffisamment d'adresses IP pour adresser l'ensemble des périphériques informatiques actuellement utilisés. On utilise donc un mécanisme, appelé NAT, qui permet d'attribuer une adresse à tout terminal (et donc lui permet de communiquer sur Internet).

1. Quelle est la différence entre une adresse IP dite « publique » et une adresse IP dite « privée » ?
2. Rappelez les différentes plages d'adresses privées réservées (par la RFC 1918), et leurs caractéristiques (nombre d'adresses, première et dernière adresse, notation CIDR, masque de sous-réseau).
3. Rappeler la structure d'un header UDP et d'un header TCP (en particulier les quatres premiers champs).
4. Qu'est ce qu'un NAT ? Quel est le rôle de la passerelle lorsque qu'une communication d'une machine avec une adresse privée se fait avec une machine possédant une adresse IP publique ?
5. Quels sont les avantages du NAT ? Quels sont les inconvénients du NAT ?
6. Proposer une structure de données (en C) permettant de décrire une table de correspondance NAT.

On étudie la situation suivante :



On considère deux réseaux locaux classiques, derrières des *box* d'opérateurs, connecteés à Internet. La machine A héberge un serveur web, un serveur SSH, et les machine B et D des clients Web, voir SSH.

1. Donnez des exemples de serveurs Web, de clients Web. Sur quel(s) port(s) opèrent ils, classiquement ? Même question pour SSH.
2. Quels sont les services traditionnellement présents sur les « box » ?
3. On suppose qu'il y a deux NATs dynamiques (i.e. sans règles pré-définies) au niveau des Box. Qui peut communiquer avec Machine A ?

4. On suppose maintenant qu'il y a une règle de NAT statique sur la Frite Box qui permet de rediriger le traffic reçu sur son port 80 vers le port 80 de la machine A (« redirection de port »). Le client Web de Machine D fait une requête http vers le serveur web. Au niveau des points d'observations 1, 2, et 4, décrire la forme du header IP, et du header du protocole encapsulé dans IP.
5. Proposer une solution pour permettre à deux applications sur deux machines derrière des NATs dynamiques de communiquer entre elles directement, sans passer par une application tierce (il sera possible d'utiliser temporairement une autre machine qui n'est pas derrière un NAT).
6. Sur vos téléphones portables munis de forfait « data » (wifi désactivé) si vous en avez, vérifiez quelle type de connectivité (ipv4, ipv6) vous avez en allant sur le site `http://monip.org/` . Que pouvez vous en déduire sur votre connexion ?
7. Le Code des postes et des communications électroniques, en particulier l'Article L34−1, demande aux opérateurs de communications électroniques d'enregistrer, pour chaque connexion de l'abonné, entre autres, l'identifiant de la connexion, l'identifiant du terminal utilisé pour la connexion si possible, l'heure de début et de fin de la connexion. Un site web ayant été piraté, l'administrateur regarde les logs et y trouve des informations sur l'attaquant. Il souhaite porter plainte : quelles informations doit-il transmettre à la police (et donc quelles informations l'opérateur doit stocker) afin de l'aider dans sa recherche du pirate informatique ?

Réseaux IPs : DHCP et DNS

1. À quoi servent les protocoles DHCP et DNS ?
2. Quel protocole est utilisé par le protocole DNS ? Quel protocole est utilisé par le protocole DHCP ? À quelles couches appartiennent ces protocoles ?
3. Préciser à quoi sert les messages DHCPDISCOVER, DHCOFFER, DHCPREQUEST, DHCPACK, DHCPNAK, DHCPRELEASE, DHCPINFORM ?
4. Que se passe-t-il si deux serveurs DHCP sont lancés sur le même réseau local ?
5. À quoi sert un enregistrement DNS de type A, AAAA, MX ?