OSI 3 – 4 : filtrage, NAT, PAT

Le filtrage va nous permettre de créer des zones de confiance dans notre réseau avec les règles que nous aurons définies. Cette séquence explique également les techniques NAT et PAT qui sont complémentaires au filtrage, et surtout, comment elles se combinent entre elles.

Contenu

1. Introduction

Le sujet d'étude de cas 2004 de Nouvelle-Calédonie de feu le BTS IG proposait un exercice sur la sécurité très intéressant, mais pas si facile.

Extrait de l'étude de cas :

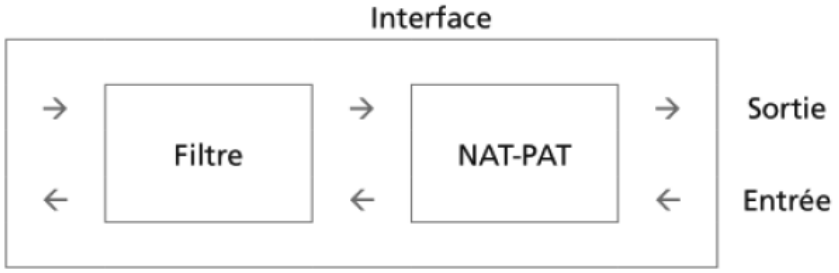
Pour maintenir la sécurité interne de l'entreprise VISTE, la société de service propose de ne pas mettre les serveurs HTTP et Mail sur le réseau interne. Sur le routeur général, les règles suivantes ont été écrites :
Règles NAT (Network Address Translation) et PAT (Port Address Translation) appliquées sur l'interface 172.16.0.129 (une interface du routeur NAT/PAT) :

IP	Port	<---->	IP	Port
172.16.0.66	2020		192.168.0.5	5600

Règle de filtrage appliquée sur l'interface 172.16.0.129 :

N° règle	Interface	IP Source	Port Source	IP Destination	Port Destination	Action
1	172.16.0.129	*	*	*	*	Refusé

Principes d'association des règles de filtrage et de NAT-PAT sur une interface :



• Sur un paquet en sortie d'une interface, on applique d'abord les règles de filtrage puis les règles NAT-PAT.
• Sur un paquet en entrée d'une interface, on applique d'abord les règles NAT-PAT puis les règles de filtrage.

Le serveur HTTP utilise le port 1060 pour communiquer et le serveur de bases de données le port 2020.

***Question :** donner les adresses IP et les ports source et destination d'un paquet envoyé par le serveur HTTP au serveur de bases de données (voir schéma page suivante).*

Réponse : nous allons rappeler ce qu'est le filtrage, puis revenir sur les notions de translation d'adresse et de translation de port, enfin nous verrons que la combinaison de tout ça n'est qu'après tout, juste une question de rigueur intellectuelle.

2. Rappel sur le filtrage

L'en-tête d'un paquet contient principalement :

- les adresses MAC et IP de la source et du destinataire ;
- les ports source et destination des services.

On peut donc filtrer sur ces différents critères, voyons un peu comment peut se représenter une table de filtrage (théorique, chaque logiciel adopte parfois une présentation différente) :

N° règle	Interface	IP Source	Port Source	IP Destination	Port Destination	Action
1	172.16.0.129	*	*	*	*	Refusé

Quelques points à connaître impérativement :

- Les règles portent un numéro d'ordre (1, 2, 3 etc.), en effet la table de filtrage sera lue ligne par ligne, la première règle correspondant sera appliquée.
- L'interface désigne la carte réseau sur laquelle s'applique la règle.
- Les @ source, port source, @ destination et port destination permettent de fixer les conditions de filtrage.
- Enfin, si la condition est remplie, on applique l'action (accepter : on laisse passer le message, refuser : on ne laisse pas passer).

Il existe différents niveaux de pare-feux :

- stateless : le pare-feu analyse chaque paquet indépendamment. Pour autoriser un service, il faut donc toujours deux règles (une pour les paquets sortants et l'autre pour les paquets entrants). Ce type de pare-feu peut être considéré comme obsolète;
- statefull : il est capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés ;
- applicatif : ils vérifient la complète conformité du paquet à un protocole attendu. Permet de vérifier par exemple que seul du HTTP passe bien par le port TCP 80.

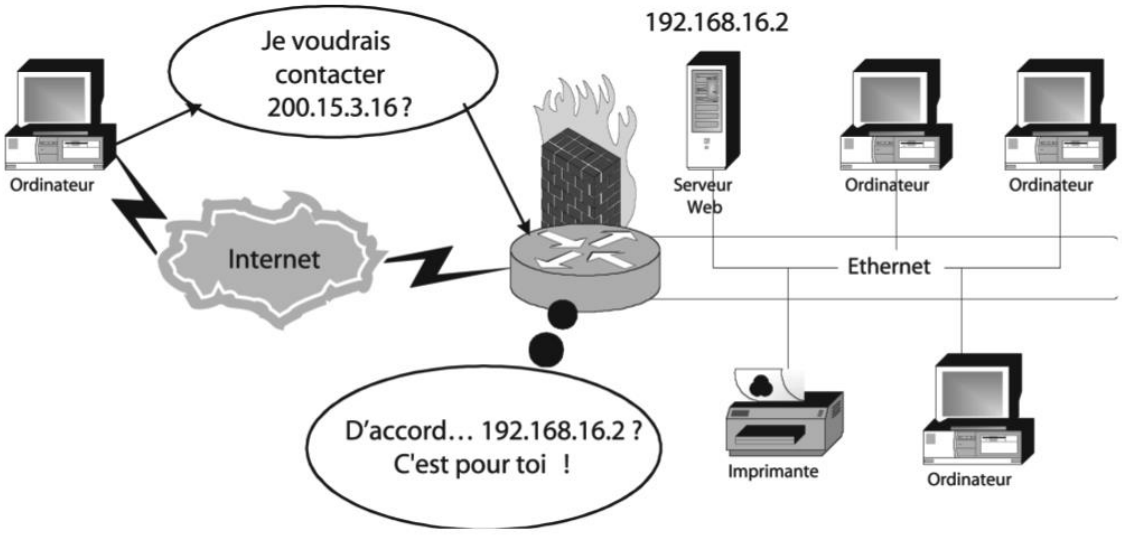
3. La translation d'adresse : NAT

NAT signifie Network Address Translation, en français : translation d'adresse réseau.

Avant de voir comment, voyons pourquoi… Dans le message accepté par le routeur quelle était l'adresse du destinataire ? La « vraie » adresse IP du destinataire, donc la source connaissait cette adresse ! Est-ce toujours souhaitable ?

Par mesure de précautions, on peut effectivement cacher la vraie adresse d'un serveur par du NAT. Mais il faut aussi savoir que le NAT (et l'adressage IP privé) a été inventé pour pallier le faible nombre d'adresses IPv4. En effet, est-il vraiment utile que tous les ordinateurs de la terre possèdent une IP publique ?

Le principe est le suivant :

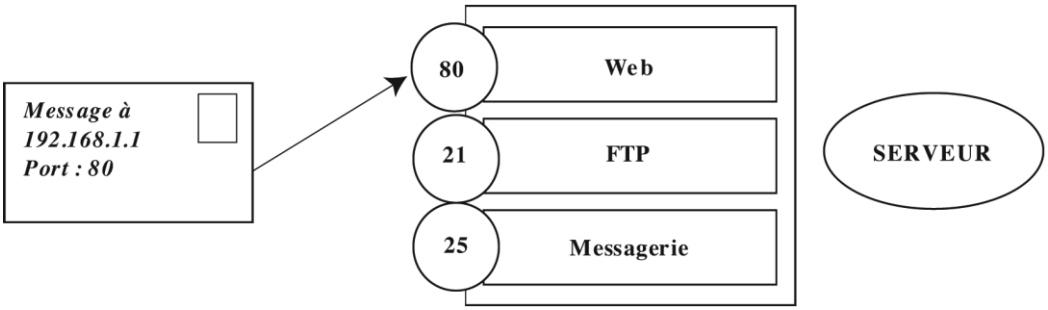


Alors comment ça marche ? Oh en théorie c'est très simple : le routeur désencapsule le message jusqu'au datagramme IP = il « enlève » toutes les informationss des couches 1&2… là il remplace l'@IP du destinataire (200.15.3.16) par la « vraie » qu'il a dans sa table (192.168.16.2), CQFD.

Et au retour lorsque le serveur répond ? Eh bien le routeur fait la même chose… dans l'autre sens. Il remplace la « vraie IP » par une factice : le client n'y voit que du feu !

4. La translation de port : PAT

Chaque application utilise un port de communication différent qui est identifié par un numéro de port. On peut imaginer qu'une machine physique appelée « serveur » exécute simultanément 3 services : web, ftp et smtp. Il faut bien pouvoir désigner un service particulier sur la machine d'IP 192.168.1.1 :



Dans l'analyse d'une trame on retrouve bien sûr le port de communication du service... Et si on cachait aussi le « vrai » numéro de port ?

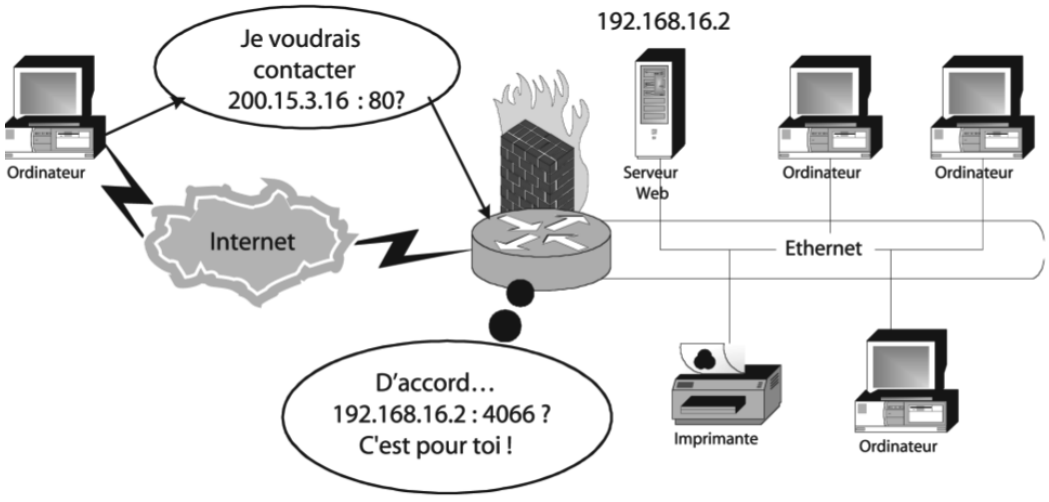
Qui c'est qui va embêter mon serveur web si je le mets sur le port 4066 ? (évitez xx80 d'accord ?) Avant de le trouver sur 4066 il faudra que le « client » soit au courant ou... passe en revue mes ports ouverts : on parle alors de scan de ports (un des logiciels les plus connus est nmap).

Eh bien même principe que le NAT : c'est le routeur qui va échanger dans la transmission le numéro de port... vu de l'extérieur ce sera peut-être le 80 (port natif d'un service web), mais le vrai sera 4066 et hop !

Le PAT nous permet aussi de joindre une machine depuis Internet lorsque celle-ci ne dispose que d'une IP privée.

5. Combinaison NAT/PAT par l'exemple

Prenons le schéma suivant qui est le même que le précédent, la notion de port en plus :



Vous connaissez la notation : 200.15.3.16:80 ? Cela veut tout simplement dire : je communique avec l'hôte d'@IP xxxx sur le port yy, donc on tape xxxx:yy

Donc sur le schéma exemple vous avez remarqué : le client demande 200.15.3.16:80 et finalement le « vrai » destinataire c'est 192.168.16.2:4066 !!! C'est le routeur qui fait tout ça.

6. Résolution de l'exercice étude de cas 2004

Reprenons le sujet :

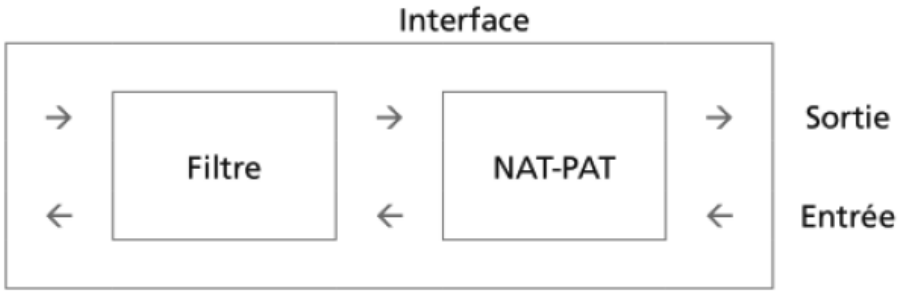
Pour maintenir la sécurité interne de l'entreprise VISTE, la société de service propose de ne pas mettre les serveurs HTTP et Mail sur le réseau interne. Sur le routeur général, les règles suivantes ont été écrites :
Règles NAT (Network Address Translation) et PAT (Port Address Translation) appliquées sur l'interface 172.16.0.129 :

IP	Port	<---->	IP	Port
172.16.0.66	2020		192.168.0.5	5600

Règle de filtrage appliquée sur l'interface 172.16.0.129 :

N° règle	Interface	IP Source	Port Source	IP Destination	Port Destination	Action
1	172.16.0.129	*	*	*	*	Refusé

Principes d'association des règles de filtrage et de NAT-PAT sur une interface :

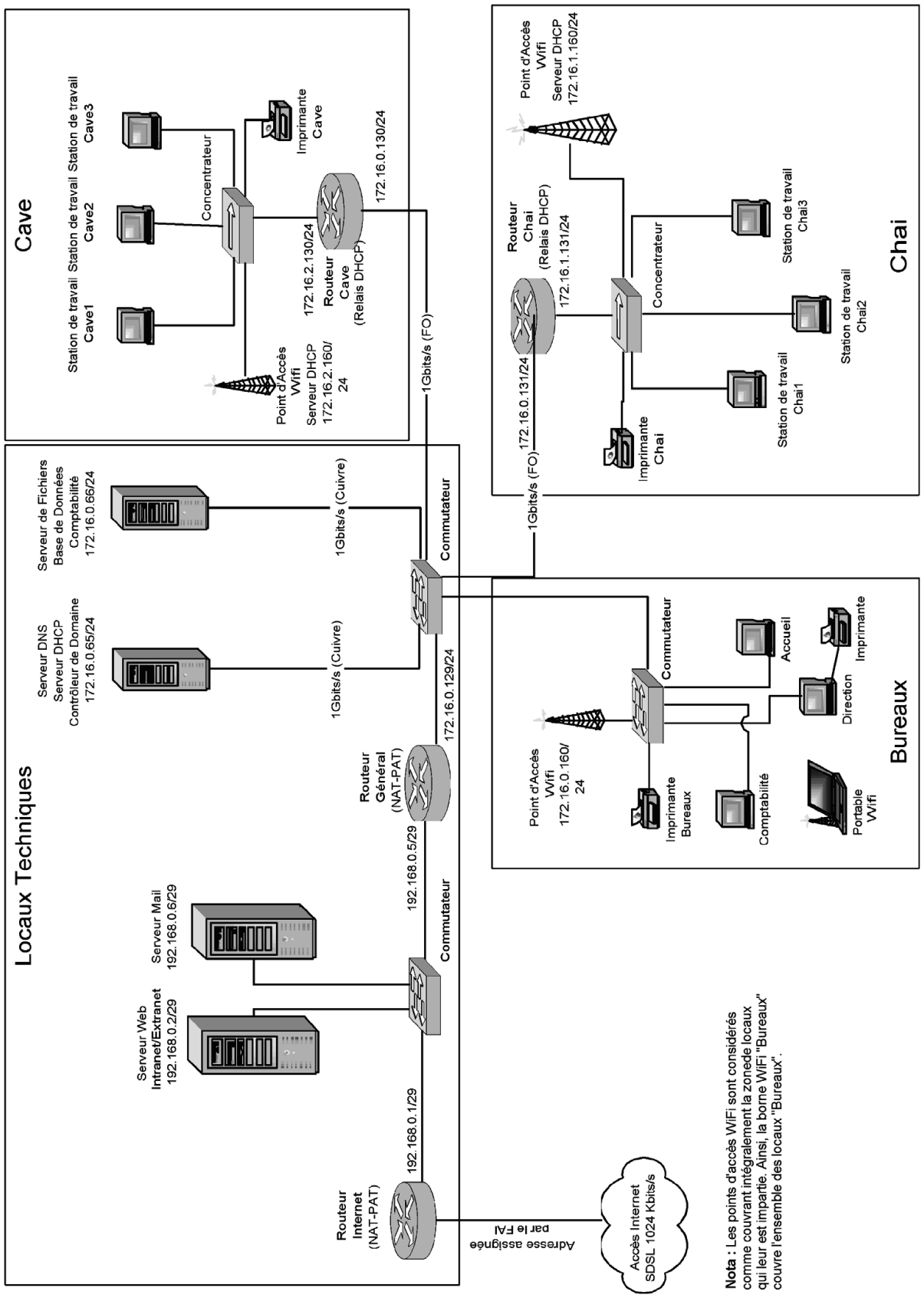


- *Sur un paquet en sortie d'une interface, on applique d'abord les règles de filtrage puis les règles NAT-PAT.*
- *Sur un paquet en entrée d'une interface, on applique d'abord les règles NAT-PAT puis les règles de filtrage.*

Le serveur HTTP utilise le port 1060 pour communiquer et le serveur de bases de données le port 2020.

***Question :** donner les adresses IP et les ports source et destination d'un paquet envoyé par le serveur HTTP au serveur de bases de données (voir schéma page suivante).*

Schéma :


Cave
Station de travail Cave1
Station de travail Cave2
Station de travail Cave3
Concentrateur
Imprimante Cave
172.16.2.130/24
Routeur Cave (Relais DHCP)
172.16.0.130/24
Point d'Accès Wifi Serveur DHCP 172.16.2.160/24
1Gbits/s (FO)
Chai
Point d'Accès Wifi Serveur DHCP 172.16.1.160/24
Routeur Chai (Relais DHCP)
172.16.1.131/24
Concentrateur
Station de travail Chai3
Station de travail Chai2
Station de travail Chai1
Imprimante Chai
172.16.0.131/24
1Gbits/s (FO)
Locaux Techniques
Serveur de Fichiers Base de Données Comptabilité 172.16.0.66/24
Serveur DNS Serveur DHCP Contrôleur de Domaine 172.16.0.65/24
1Gbits/s (Cuivre)
1Gbits/s (Cuivre)
Commutateur
172.16.0.129/24
Routeur Général (NAT-PAT)
192.168.0.5/29
Commutateur
Serveur Mail 192.168.0.6/29
Serveur Web Intranet/Extranet 192.168.0.2/29
192.168.0.1/29
Routeur Internet (NAT-PAT)
Adresse assignée par le FAI
Accès Internet SDSL 1024 Kbits/s
Bureaux
Point d'Accès Wifi 172.16.0.160/24
Commutateur
Accueil
Imprimante
Direction
Imprimante Bureaux
Comptabilité
Portable Wifi
Nota : Les points d'accès WiFi sont considérés comme couvrant intégralement la zonede locaux qui leur est impartie. Ainsi, la borne WiFi "Bureaux" couvre l'ensemble des locaux "Bureaux".

Solution :
Le paquet est envoyé du serveur HTTP (192.168.0.2) sur le port 1060 comme l'indique le texte, et à destination du serveur de bases de données (172.16.0.66) pour le port 2020.

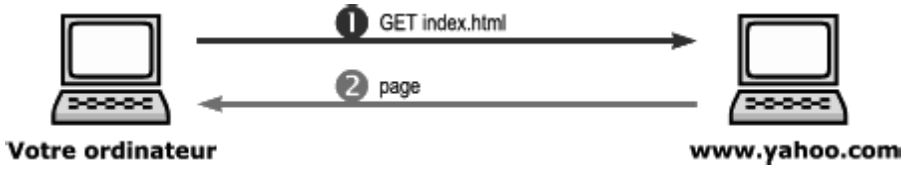
Mais le paquet est pris en charge par le routeur NAT qui va assurer la translation de certaines valeurs. En effet l'adresse 172.16.0.66 et le port 2020 vont être convertis en l'adresse 192.168.0.5 et le port 5600.

Les valeurs définitives seront donc :

- Adresse IP source : 192.168.0.2
- Port source : 1060
- Adresse IP Destination : 192.168.0.5
- Port Destination : 5600

7. Proxy

En l'absence de proxy, la requête est directement envoyée du client au serveur :



Lorsqu'un proxy est utilisé, il fait l'intermédiaire entre le client et le serveur. Du point de vue du serveur, c'est donc le proxy qui est client :

Un serveur mandataire ou proxy est ainsi un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs mandataires sont notamment utilisés pour assurer les fonctions suivantes :

- accélération de la navigation : mémoire cache, compression des données, filtrage des publicités ou des contenus lourds (java, flash) ;
- la journalisation des requêtes (logging) ;
- la sécurité du réseau local ;
- le filtrage et l'anonymat.