Administration d'un Intranet

- Déterminer un plan d'adressage
- Configuration des tables de routages
- Utilisation d'un NAT (Network Adressing Translation)
- Mise en place d'un pare-feux (Firewall)

Rappel: Le routage dans Internet

- **La décision dans IP du routage:**
  - Table de routage:
    - Adresse destination (partie réseau), netmask, adresse routeur voisin
  - Consultation de la table de routage à l'arrivée d'un paquet:
    - Pour chaque ligne de la table de routage (***Adr, netmask, AdrRouteur***) faire
      - ★Si (***adresse destination du paquet*** AND ***netmask***) = ***Adr*** alors
        - envoyer le paquet au routeur voisin d'adresse ***AdrRouteur***
          - Pour cela faire appel à ARP pour connaître son adresse Ethernet
      - ★Sinon passer à la ligne suivante
    - Si l'adresse n'est pas dans la table alors renvoyer un paquet ICMP: "*destination inaccessible*" à la machine source

Environnement et contraintes

- Intranet d'une entreprise
- 3 types d'utilisateurs
  - 25 cadres
  - 25 administratifs
  - 10 ateliers
  - 2 machines spécialisées (SF1 et SF2) pour être des serveurs de fichiers
- Application NFS (Network File System) permettant d'accéder de façon transparente sur une machine locale, les fichiers sur le disque dur distant du serveur de fichier

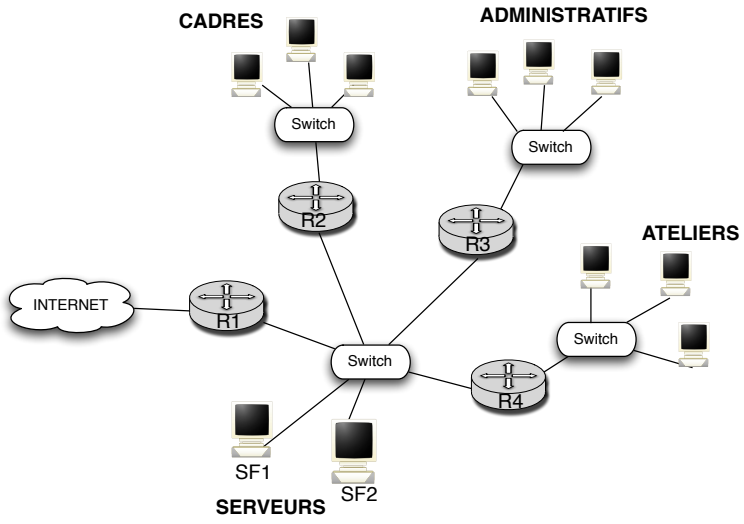
Contraintes

- Cadres : accès à toutes les machines de l'Intranet, SF1, SF2 et à l'Internet
- Administratifs : Accès à toutes les machines « administratifs » et SF1 (Pas d'accès Internet)
- Ateliers : Accès à toutes les machines « Ateliers » et SF2 (Pas d'accès Internet)
- Réseaux Ethernet
- Routeurs à 2 ports Ethernet

Choix de l'infrastructure réseau

- Découpage en plusieurs réseaux pour "isoler" les communications
- Diminue la charge des switchs
- Commutateurs (switch) Ethernet
  - Possibilité de les cascader si le nombre de ports est insuffisant
- Choix de la place des serveurs de fichier à discuter
- Un seul routeur en sortie:
  - sécurité, possibilités de filtrage…
  - Un port particulier vers Internet : ligne spécialisée avec un autre protocole: ADSL(PPP), ATM...
- Possibilités d'un seul routeur à 6 pattes (problème prix/ performances)

Topologie

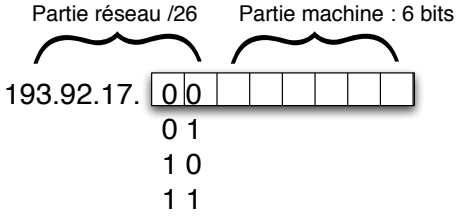


Choix des adresses

- **Adresse publique :** donnée par un organisme international de gestion des adresses (A chercher sur le web *Inter NIC* (Internet Network Information Center)
- Supposons que l'on obtienne le **préfixe** suivant**:** 193.92.17 / 24
- **Pour machines ne communiquant pas avec l'extérieur possibilité d'adresses privées:**
  - Trois plages d'adresses privées:
    - **10.0.0.0/8**: 10.0.0.1 à 10.255.255.254
    - **172.16.0.0/12**: 172.16.0.1 à 172.31.255.254
    - **192.168.0.0/16**: 192.168.0.1 à 192.168.255.254
  - Economie d'adresse mais si on veut changer de contraintes, il faut tout reconfigurer
  - Possibilités de faire de la translation d'adresses (NAT)

Découpage en "sous-réseaux" (Subnetting)

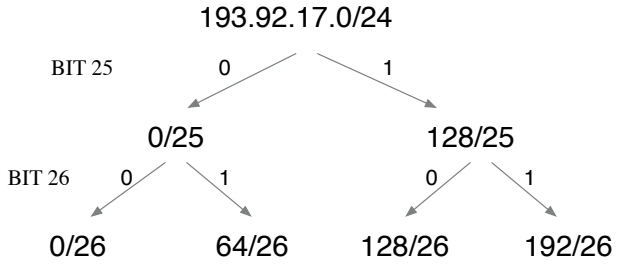
- On choisit d'affecter des adresses publiques à l'ensemble de l'Intranet
- 4 réseaux, 1 seule plage d'adresses publiques
- Changement des netmasks
  - 2 bits de poids fort de la partie machine sont attribués à la partie réseau de l'adresse
  - On transforme un /24 en quatre /26



Sous-réseaux

- La partie réseau est appelé **Prefixe**
- **Netmask : 255.255.255.192**
- **4 réseaux:**
  - 193.92.17.**0 /26**
  - 193.92.17.**64 /26**
  - 193.92.17.**128 /26**
  - 193.92.17.**192 /26**
- **Nombre de machines par réseau : 64 -2 = 62**
  - Adresse partie machine
    - à 0 interdit (désigne un réseau)
    - à 11..111 interdit (broadcast)

Arbre de découpage



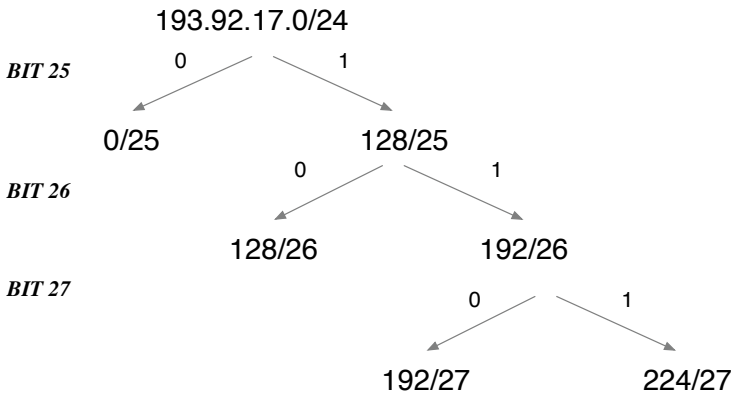
Sous-réseaux

- **Exemple pour le réseau** 193.92.17.**128 /26**
  - 1ère adresse machine: dernier octet: **10** 000001=129
  - dernière adresse: **10** 111110=190
- **Plages d'adresses /26:**
  - 193.92.17.**1** à 193.92.17.**62**
  - 193.92.17.**65** à 193.92.17.**126**
  - 193.92.17.**129** à 193.92.17.**190**
  - 193.92.17.**193** à 193.92.17.**254**

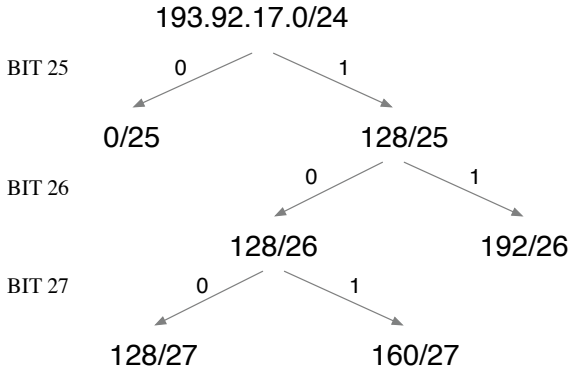
Sous réseaux de tailles variables

- Supposons que le nombre de machine cadre est de 100
- Au lieu de quatre /26: un /25, un /26 et deux /27
  - **0** : 0 /25
  - **111**: 224 /27
  - **110** : 192 /27
  - **10** : 128 / 26
- Quel est le nombre de machines sur chaque sous réseau ?
- Donnez les plages d'adresses de ces 4 sous réseaux ?

Arbre de découpage en sous réseaux



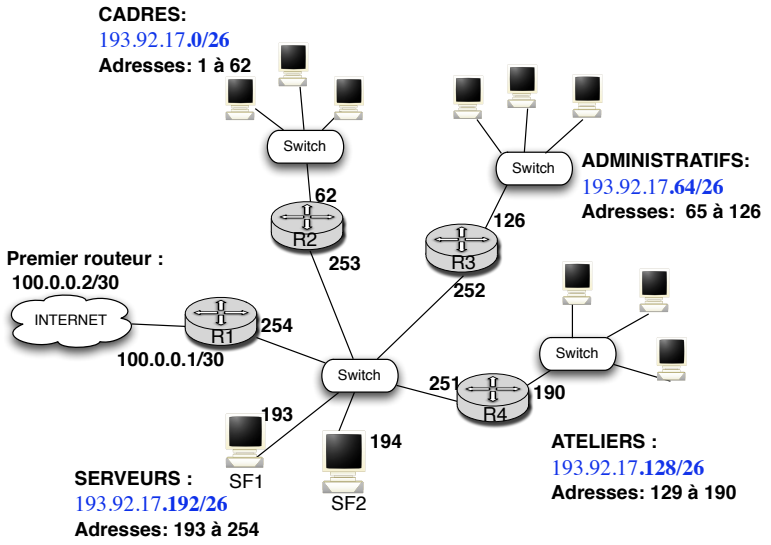
Arbre de découpage : exemple d'une autre solution



Plan d'adressage

- Après le découpage en sous réseau, on fait un plan du réseau en notant pour chaque interface des machines et des routeurs les adresses attribuées
- Les routeurs ont une adresse dans chaque réseau auquel ils sont connectés
- Pour de vrai, on note aussi sur ce plan les noms des interfaces
- Par convention les administrateurs réseaux affectent souvent les premières (ou dernières) adresses aux interfaces des routeurs
- Avec le découpage en 4 réseaux voila ce que cela donne

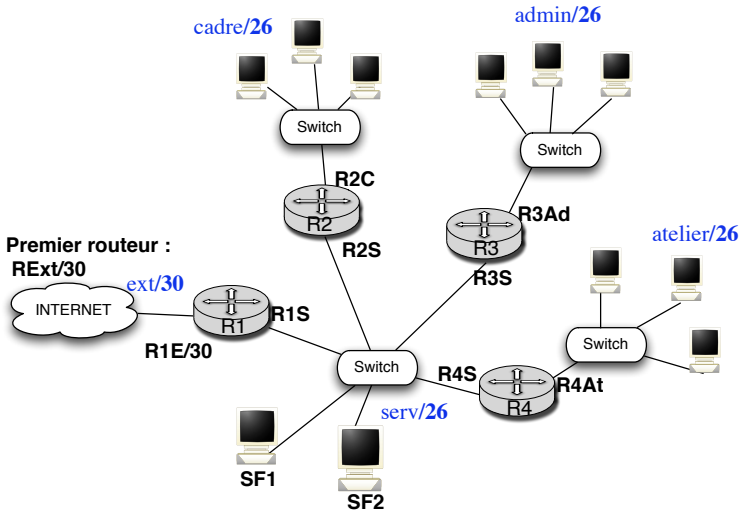
Plan d'adressage



Configuration routage

- On utilise des noms à la place des adresses
  - Il pourrait être notés dans les fichiers */etc/hosts* et */etc/networks*
  - Adresses des réseaux:
    - cadre 193.92.17.0/26
    - admin 193.92.17.64/26
    - atelier 193.92.17.128/26
    - serv 193.92.17.192/26
    - ext 100.0.0.0/30
  - La convention pour les routeur est *R_NumeroRouteur_InitialeReseau*
  - Par exemple *R3S* désigne l'adresse du routeur 3 dans le réseau Serveur

Plan d'adressage avec des noms



Tables de routage

- Format d'une table de routage :

  Adresse réseau destination / Netmask / Adresse du routeur voisin

  - Le Netmask est donné en décimal ou en notation ***/nombre de bits de la partie réseau*** (taille du préfixe)
- Exemple d'une table de routage pour une machine du réseau *cadre*
  - **A l'origine:** *cadre/26 direct*
    - **Connexion directe sur le réseau cadre après la configuration de l'interface**
  - **Une ligne par défaut:**
    - *Default R2C*
    - Quelle que soit l'adresse destination envoyer à R2C
    - **Default : adresse 0.0.0.0 Netmask 0.0.0.0**

Tables de routage

- Donnez les tables de routage des machines des trois autres réseaux, de SF1 et SF2, et des routeurs R1, R3 et R4 en respectant les contraintes:
  - Cadres : accès à toutes les machines de l'Intranet, SF1, SF2 et à l'Internet
  - Administratifs : Accès à toutes les machines « administratifs » et SF1
  - Ateliers : Accès à toutes les machines « Ateliers » et SF2

- **Routeur 2 :**
  - *cadre/26 direct*
  - *serv/26 direct*
  - *admin/26 R3S*
  - *atelier/26 R4S*
  - *default R1S*
    - Default pour l'accès à Internet

- **Machine cadre**
  - *cadres/26 direct*
  - *default R2C*

Tables de routage

- **Machines atelier :**
  - *atelier direct*
  - *Default R4At*
- **Machines atelier :**
  - Elles envoient des paquets quelle que soit l'adresse destination
  - Les paquets à destination de l'Internet sont aussi envoyés sur le réseau (charge inutile)
- Il vaut donc mieux préciser les réseaux auxquels l'atelier peut accéder
  - **Machine Atelier**
    - *atelier/26 direct*
    - *serv/26 R4At*
  - **Machine admin**
    - *admin/26 direct*
    - *serv/26 R3Ad*

Tables de routage

- **Routeur 1 :**
  - *Ext/26 direct*
  - *serv/26 direct*
  - *cadres/26 R2S*
  - *default Rext*

  On ne met pas les réseaux admin et atelier qui ne communiquent pas avec l'extérieur
- **Routeur 3:**
  - *serv/26 direct*
  - *admin/26 direct*
- **Routeur 4:**
  - *serv/26 direct*
  - *atelier/26 direct*

  Les machines atelier et admin ne communiquent qu'avec les serveurs

Tables de routage

- Avec la table de routage donnée pour les machines atelier est ce qu'elles peuvent accéder aux deux serveurs SF1 et SF2 (et à toutes les machines qui seraient sur le reseau serv)?
- Si oui comment faire pour qu'elle ne puisse accéder qu'à SF2 ?
  - **Machine Atelier**
    - *atelier/26 direct*
    - *SF2/32 R4At*
  - **Machine Admin**
    - *admin/26 direct*
    - *SF1/26 R3At*
  - Netmask /32 pour comparer tous les bits

Routage

- Expliquez ce qu'il se passe si un cadre ping une machine Atelier
- Une contrainte Atelier n'accède pas au cadre mais Cadre accède au atelier peut elle être résolue par le routage ?

Tables de routage

- Les paquets vont des cadres aux ateliers mais ne peuvent revenir.
- Contrainte unidirectionnelle impossible au niveau routage:
  - Si *cadre* accède à l'atelier alors l'atelier doit accéder au cadre
- On peut définir des interdictions grâce aux pare feux (voir plus loin)
- **Table machine atelier**
  - *atelier/26 direct*
  - *SF2/32 R4At (netmask 255.255.255.255)*
  - *cadre/26 R4At*
- **Table de routage de Routeur 4:** il faut rajouter cadre aussi
  - *serv/26 direct*
  - *atelier/26 direct*
  - *cadre/26 R2S*

Tables de routage

- **Routeur 3 :**
  - *admin/26 direct*
  - *serv/26 direct*
  - *cadre/26 R2S*
- **Machines admin**
  - *admin/26 direct*
  - *SF1/32 R3Ad (netmask 255.255.255.255)*
  - *cadre/26 R3Ad*
- **SF1:**
  - *serv/26 direct*
  - *cadre/26 R2S*
  - *admin/26 R3S*
- **SF2:**
  - *serv/26 direct*
  - *cadre/26 R2S*
  - *atelier/26 R4S*

Problème de boucle

- Que se passe t-il si un paquet arrivant sur R1 depuis l'extérieur est à destination d'une adresse de Admin ?
- Le paquet est renvoyé à l'extérieur car Admin n'est pas dans la table du routeur 1
- Du coup ce paquet inonde le réseau Est, c'est la cata !
- Peux se résoudre par des listes d'accès (voir les pare-feux plus loin)

Routage automatique

- On utilise le protocole RIP dans l'Intranet
- Quelle sont les tables de routage auxquelles ont aboutit pour les 4 routeurs et les machines des 4 réseaux ?
- Remarque: on peut ne faire tourner RIP que sur l'interface interne du routeur 1

Routage automatique RIP
Tables de routage

- **Routeur 1 :**
  - *Ext/26 direct 1*
  - *serv/26 direct 1*
  - *cadres/26 R2S 2*
  - *admin/26 R3S 2*
  - *atelier/26 R4S 2*
- **Routeur 3:**
  - *serv/26 direct 1*
  - *admin/26 direct 1*
  - *cadres/26 R2S 2*
  - *atelier/26 R4S 2*
- **Routeur 4:**
  - *serv/26 direct 1*
  - *atelier/26 direct 1*
  - *admin/26 R3S 2*
  - *cadres/26 R2S 2*

- Les métriques de RIP sont aussi données

- **Machine cadre**
  - *cadre/26 direct 1*
  - *admin/26 R2C 3*
  - *serv/26 R2C 2*
  - *atelier/26 R2C 3*

- **Machine atelier**
  - *atelier/26 direct 1*
  - *admin/26 R4At 3*
  - *serv/26 R4At 2*
  - *cadre/26 R4At 3*

Accès à l'extérieur

- Les machines *cadres* peuvent elles accéder à Internet ?
- Comment faire pour y remédier ?
- On rajoute à la main (ou via DHCP) une ligne par défaut dans la table des cadres et dans la table de R1
- **Remarque**: ces destinations statiques ne sont pas pris en compte par RIP (et ne sont pas propagées)

- **Routeur 1 :**
  - *Ext/26 direct 1*
  - *serv/26 direct 1*
  - *cadres/26 R2S 2*
  - *admin/26 R3S 2*
  - *atelier/26 R4S 2*
  - *Default Rext*
- **Machine cadre**
  - *cadre/26 direct 1*
  - *admin/26 R2C 3*
  - *serv/26 R2C 2*
  - *atelier/26 R2C 3*
  - *Default R2C*

Paquet RIP

- Quel est contenu des paquets RIP envoyés par le routeur R2 sur les 2 réseaux auxquels il est connecté ?
- Remarque en RIPV1 pas de netmask, supposons RIPV2 utilisé

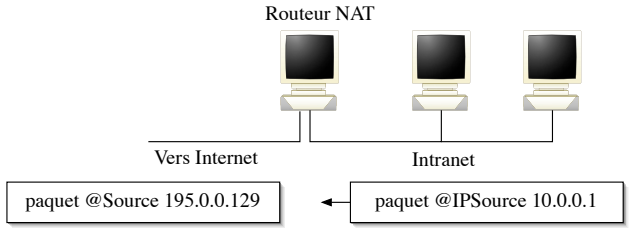
- **Sur le reseau Serv**
  - *cadre/26 1*
  - *admin/26 16 (car horizon coupé)*
  - *serv/26 1*
  - *atelier/26 16 (car horizon coupé)*
- **Sur le reseau Cadre**
  - *cadre/26 1*
  - *admin/26 2*
  - *serv/26 1*
  - *atelier/26 2*

La translation d'adresse réseau (NAT)

- Le NAT est fortement utilisé pour économiser des adresses IPV4
- N'existe plus en IPV6
- Les routeurs inclut dans les box classiques des fournisseurs d'accès utilise systématiquement la translation d'adresse
- Vous avez chez vous toujours une adresse privée, souvent 192.168.0.x

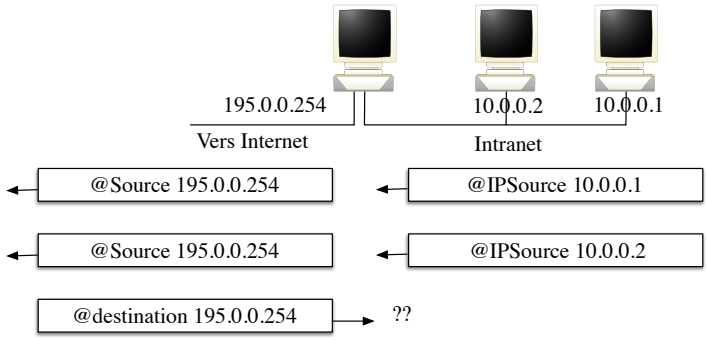
Principe de la translation d'adresse

- On utilise des adresses privées à l'intérieur de l'Intranet (192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8)
- Une seule adresse publique est nécessaire celle de l'interface externe du routeur de sortie
- Le routeur de sortie va modifier l'entête IP de tout paquet provenant d'une machine interne en remplaçant l'adresse source IP privée par une adresse publique
- Vue de l'extérieur, le routeur se fait passer pour la machine source



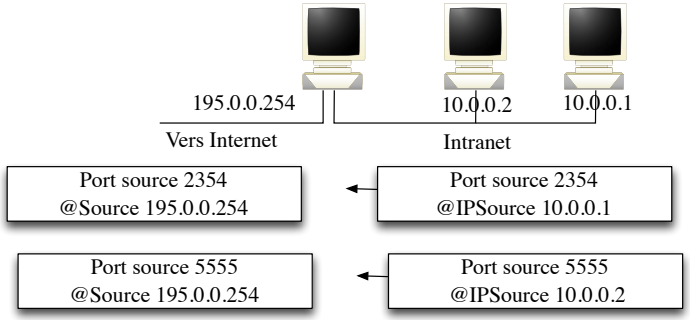
Principe de la translation d'adresse

- Permet d'attribuer dynamiquement lors des connexions des adresses IP publiques aux adresses privées
- L'adresse source des paquets devient l'adresse externe du routeur
- **Problème** : En cas de plusieurs connexions en même temps comment le routeur peut il rediriger les paquets qui reviennent du réseau vers la bonne machine ?



L'association connexion/@privée

- Se fait au moment du premier paquet qui sort en se rappelant le numéro de port source (mémorisation dans une table)

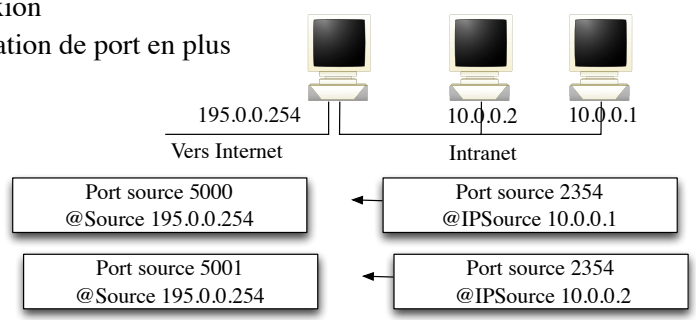


Mémorisation dans la table NAT:

2354 10.0.0.1
5555 10.0.0.2

L'association connexion/@privée

- Problème : si plusieurs connexions avec le même port source en même temps ?
- Attribution d'un port source virtuel unique à chaque connexion
- Translation de port en plus



Mémorisation dans la table NAT:

2354 10.0.0.1 5000
2354 10.0.0.2 5001

Contraintes du NAT

- Une seule adresse publique suffit pour un nombre quelconque de machines dans l'Intranet
- On ne peut pas initier une connexion depuis l'extérieur
- Comment avoir un serveur WEB par exemple dans l'Intranet ?

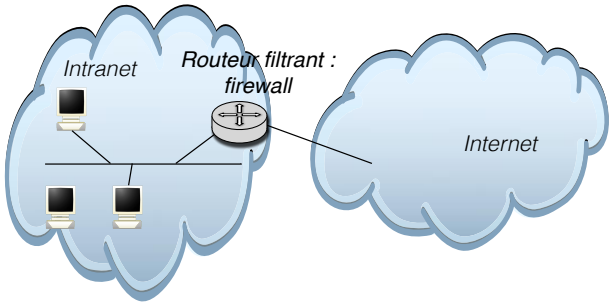
Le *port forwarding*

- **Utiliser dans la NAT pour rendre une machine accessible depuis l'extérieur**
- **On mets en dur dans la table NAT du routeur**
  - port fixe: port privée/ adresse privée
  - Par exemple **21: 21/10.0.0.1** (port d'un serveur FTP)
  - Les paquets arrivant de l'extérieur vers (**195.0.0.254, 21**) seront redirigés vers (**10.0.0.1, 21**)
  - Problème si deux serveurs FTP sur 2 machines différentes ?
- **Le "*port mapping*" consiste à changer de port sur la machine interne**
  - Par exemple : **80: 8080/10.0.0.1**
  - Un serveur http est lancé sur 10.0.0.1 sur le port 8080

Sécurité d'un Intranet Filtrage de paquet

- Accès limités aux ressources de l'Intranet ("sécurité d'accès")
  - Utilisateur ?
  - Machines
  - Serveurs
  - Applications
- Possibilité de filtrage de paquets à l'entrée (et/ou sortie) de l'Intranet
  - Potentiellement dangereux (connus et non connus)
- Mise en place d'un ***garde barrière*** ou ***pare-feux*** (***Firewall***)
- Possibilité de mettre aussi un pare-feu sur une machine utilisateur pour filtrer les paquets rentrant

Principe Pare-feux



Principe du filtrage

- **Filtrage**:
  - Machine : adresse IP source / destination (entête IP)
  - Application : port source / destination (entête TCP/UDP)
    - No port destination : serveur standard
  - Utilisateur: autre technologie (VPN Virtual Private Network avec authentification)
- **Analyse des entêtes IP/TCP-UDP par le routeur pare-feux pour chaque paquet reçu**
  - Augmente considérablement le travail du routeur (performance ?)
  - Pas d'analyse des données
- **Définition par l'administrateur réseau d'une liste de filtres (*"acces list"*)**

Les listes d'accès

- **Deux politiques de gestion**
  - On interdit ce que l'on ne veut pas (connu), le reste est autorisé
    - Facile à mettre en place mais moins sécuritaire, ce qui est inconnu n'est pas filtré
  - On autorise ce que l'on veut, le reste est interdit
    - Plus délicat, il ne faut rien oublier dans les autorisations
    - Maintenance plus importante (nouvelles autorisations à la demande des utilisateurs)

Fonctionnement des liste d'accès

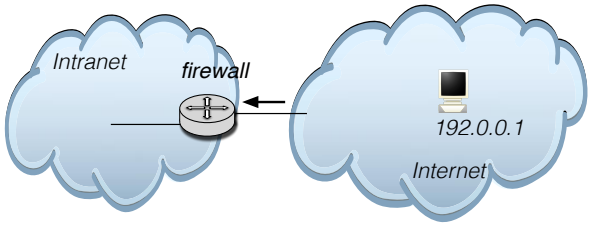
- Une liste d'accès: liste de règle d'interdiction ou d'autorisation sur différents critères:
  - **Adresse source / Adresse Destination / Port source / Port destination / Protocole / règle**
- Les règles sont passées en revue séquentiellement (ordre important) jusqu'à que l'une d'elle soit vérifiée
- La règle précise le rejet ou l'autorisation de passage du paquet
- On peut préciser sur quelle interface du routeur sont appliqués les filtres
- On peut préciser si les filtres sont appliqués pour les paquets venant du réseau ou sortant vers le réseau

Filtrage sur adresse

- On note * pour signifier "toutes les possibilités"
- **Exemple sur l'interface d'entrée d'un routeur d'accès à un Intranet**

Adr source	**Adr destination**	**Port source**	**Port destination**	**Protoc.**	**Règle**	**sens**
192.0.0.0.1	*	*	*	*	*autorisé*	*entrant*
*	*	*	*	*	*interdit*	*entrant*

- Seuls les paquets issus de la machine 192.0.0.1 peuvent rentrer dans l'Intranet



Filtrage sur adresse

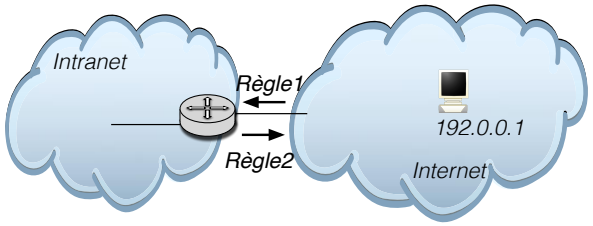
- Par contre, n'importe quel paquet peut sortir de l'Intranet
- On peut rajouter la règle symétrique pour interdire la sortie des paquets qui ne sont pas destinés à 192.0.0.1:

Adr source / Adr destination / Port source/ Port destination / Protoc. / Règle / sens

*192.0.0.0.1 / * / * / * / * / autorisé / entrant*

** / 192.0.0.0.1 / * / * / * / autorisé / sortant*

** / * / * / * / * / interdit / **



Exemple Acces List

- **Autoriser seulement les cadres à sortir vers Internet**
- **Sur Interface de sortie de R1:**
  - **Adr source / Adr destination / Port source/ Port destination / Règle / sens**
  - cadre/26 / * / * / * / autorisé / sortant
  - * / cadre/26 / * / * / autorisé /entrant
  - * / * / * / * / interdit / *
- **Pas de filtrage sur l'application**

Filtrage sur numéro de port

- **Filtrage sur application**
- **On veut interdire tout sauf la navigation sur le WEB depuis l'Intranet (port serveur web 80)**

Adr source / Adr destination / Port source/ Port destination / Protoc. / Règle / sens

** / * / * / 80 / TCP / autorisé / sortant*

** / * / * / * / * / interdit / sortant*

- Cela n'empêche pas des paquets provenant d'Internet de rentrer dans l'Intranet
  - On peut rajouter la règle symétrique

** / * / 80 / * / TCP / autorisé / entrant*

** / * / * / * / * / interdit / entrant*

Filtrage multiple

- **Autoriser l'accès depuis l'extérieur sur un serveur WEB de l'Intranet (sur une machine d'adresse 193.92.17.62)**
- **Autoriser toute sortie vers un serveur web à l'extérieur**

Adr source / Adr destination / Port S / Port D / Protoc. / ACK / Règle / sens

*193.92.17.62 / * / 80 / * / TCP / * / autorisé / sortant*

** / 193.92.17.62 / * / 80 / TCP / * / autorisé / entrant*

*cadre/26 / * / * / 80 / TCP / * / autorisé / sortant*

** / cadre/26 / 80 / * / TCP / **1** / autorisé / entrant*

** / * / * / * / * / * / interdit / ******

- Dans la pratique les listes d'accès possèdent des centaines de lignes
- Attention, à l'ordre des règles est primordiale et peut aboutir à des contradictions