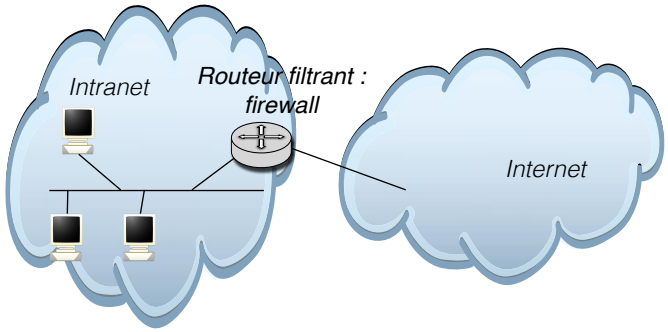
Introduction à la sécurité des réseaux

- **Deux grandes classes de problèmes de sécurité**
  - **Chiffrement permettant de garantir**
    - »La confidentialité des messages
    - »L'authentification des interlocuteurs
    - »L'intégrité et la non répudiation des messages
  - **Contrôle d'accès aux ressources (sécurité des communications)**
    - »Interdiction de l'accès à certaines ressources : applications, machines, réseaux
    - »Solution les pare-feux et les proxys applicatifs

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)
  - Possibilité de filtrage d'autres protocoles (ICMP en particulier)
- **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 (ACL: Acces Control List)**

Les listes de contrôle 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 contrôle d'accès

- Une liste de contrôle d'accès: liste de filtres (ou règles) d'interdiction ou d'autorisation sur différents critères:

  Adresse source / Adresse Destination / Port source / Port destination / Protocole / règle

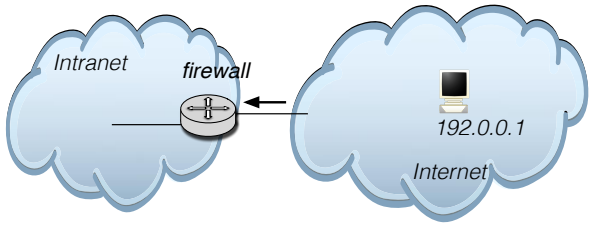
- Les règles sont passées en revue séquentiellement (ordre important) jusqu'à que l'une d'elle soit vérifiée
- La règle précise le rejet ou l'autorisation de passage du paquet
- On peut préciser sur quelle interface du routeur sont appliqués les filtres
- On peut préciser si les filtres sont appliqués pour les paquets venant du réseau ou sortant vers le réseau (voir exemple Cisco plus loin)

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*

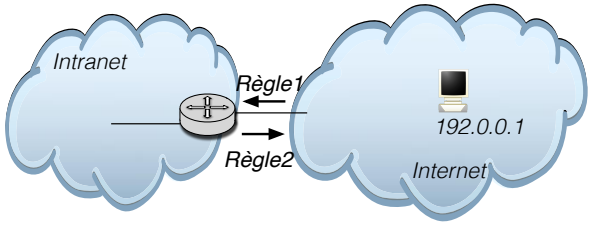
  - Seuls les paquets issus de la machine 192.0.0.1 peuvent rentrer dans l'Intranet



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*	*



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	*

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

*	*	*	80	TCP	autorisé	sortant
*	*	80	*	TCP	autorisé	entrant
*	*	*	*	*	interdit	*

Filtrage sur adresse et port

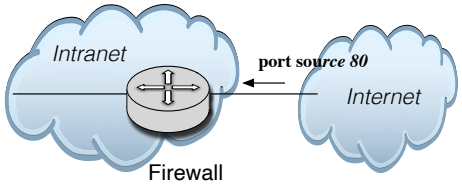
- **Amélioration pour interdire tout accès depuis l'extérieur**
- **Supposons que les adresses de l'Intranet sont 192.0.0.0/25**

Adr source	Adr destination	Port source	Port destination	Protoc.	Règle	sens
192.0.0.0/25	*	*	80	TCP	autorisé	sortant
*	192.0.0.0/25	80	*	TCP	autorisé	entrant
*	*	*	*	*	interdit	*

- On peut rajouter ainsi une paire de règle pour chaque application permise
- Si une translation d'adresse (NAT) est effectué sur le routeur on peut décider d'effectuer le filtrage avant la translation sur l'interface côté Intranet ou après la translation (interface côté extérieur)

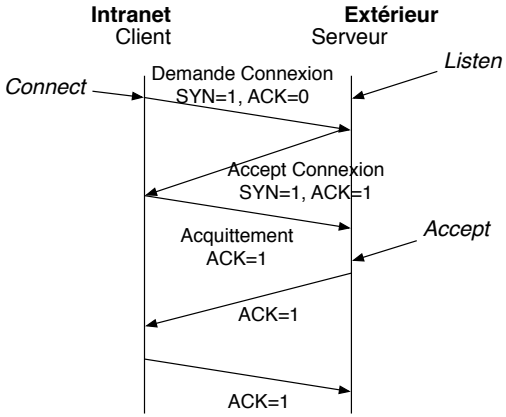
Problème des paquets entrants non voulus

- Avec les filtres précédents une machine extérieure peut:
  1. utiliser une adresse de l'Intranet. Des paquets peuvent alors rentrer dans l'Intranet à destination d'un serveur WEB mais les réponses ne pourront pas re-sortir à cause du routage
  2. lancer un client avec un port source égal au port 80 et peut alors se connecter sur un serveur dans l'Intranet
- Pour éviter cela on peut définir une règle de filtrage supplémentaire sur le flag ACK de l'entête TCP



Rappel sur TCP

Seul le 1er paquet d'ouverture de connexion TCP comporte le flag ACK à 0



On ne laisse passer de l'extérieur vers l'Intranet que les paquets avec ACK=1

Filtrage sur ouverture de connexion TCP

- **Filtre sur la valeur du flag ACK**

Adr source	Adr destination	Port S	Port D	Protoc.	ACK	Règle	sens
192.0.0.0/24	*	*	*80*	*TCP*	*	*autorisé*	*sortant*
*	*192.0.0.0/24*	*80*	*	*TCP*	***1***	*autorisé*	*entrant*
*	*	*	*	*	*	*interdit*	*

- Seuls les paquets portant le flag ACK à 1 peuvent rentrer dans l'Intranet, donc les demandes de connexions TCP ne peuvent pas rentrer
- Filtrage impossible pour UDP et d'autres protocoles
- On peut préciser le protocole dans la règle de filtrage

Filtrage multiple

- **Autoriser l'accès depuis l'extérieur sur serveur WEB de l'Intranet (sur 192.0.0.1)**
- **Autoriser toute sortie vers un serveur web à l'extérieur**

Adr source	Adr destination	Port S	Port D	Protoc.	ACK	Règle	sens
192.0.0.1	*	*80*	*	*TCP*	*	*autorisé*	*sortant*
*	*192.0.0.1*	*	*80*	*TCP*	*	*autorisé*	*entrant*
192.0.0.0/25	*	*	*80*	*TCP*	*	*autorisé*	*sortant*
*	*192.0.0.0/25*	*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

Exemple pratique sur un routeur CISCO

- **Reprenons l'exemple 2, on veut interdire tout sauf la navigation sur le WEB depuis l'Intranet (port serveur web 80)**

```
access-list 101 permit tcp 192.0.0.0 0.0.0.255
0.0.0.0 255.255.255.255 eq 80
```

- Permet le passage des paquets d'adresse source 192.0.0.0/24 vers n'importe quelle adresse destination et vers le port destination 80
- On peut aussi écrire:

```
access-list 101 permit tcp 192.0.0.0 0.0.0.255 any
host eq http
```

- **Puis interdiction de tout le reste :**

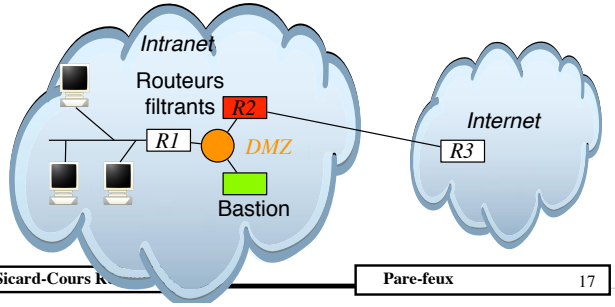
```
acces-list 101 deny ip any any
```


Exemple pratique sur un routeur CISCO

- Il faut ensuite associer cette ACL à une interface
- On peut le faire en entrée ou en sortie (ou les deux)
  - En entrée: les règles sont appliquées au paquet provenant du réseau (avant le routage)
  - En sortie: les règles sont appliquées au paquet sortant vers le réseau (après le routage)
- Sous le menu de configuration de l'interface côté extérieur:
  - **`ip access-group 101 out`**
  - Applique à l'interface choisie (ici interface côté extérieur) l'ACL 101 en sortie (paquets partant sur le réseau)
- **Remarque**: avec cette seule ACL on ne filtre pas les paquets provenant de l'extérieur. On peut pour cela, appliquer la règle symétrique soit sur la même interface mais en entrée, soit sur l'interface intérieure en sortie

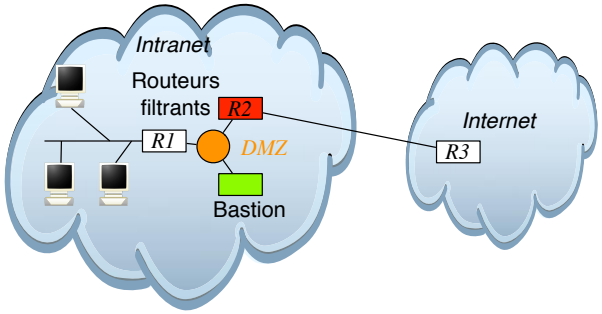
Passerelle d'application (proxy)

- Permet de rajouter des filtres sur les données propres aux applications
  - Par exemple : Nom d'utilisateur, adresse web ....
  - On parle aussi de proxy applicatifs
- Un proxy par application à filtrer
- Les proxys s'exécutent sur une machine dédiée (appelé ***bastion***)située en générale dans une zone particulière à l'entrée de l'Internet appelée zone démilitarisée (***DMZ***)
  - Permet de coupler le filtrage sur ***acces list*** et le filtrage ***applicatif***



Bastion

- Règles de filtrage plus simple:
  - Sur Routeur R1: filtre autorisation seulement Intranet <-> Bastion
  - Sur Routeur R2: filtre autorisation seulement Bastion <-> Internet
- Le bastion peut héberger aussi des serveurs accessibles de l'extérieur



Les proxys

- Filtrage applicatif
- Le proxy sert de relai entre le client et le serveur
- Il analyse le contenu des données de l'application
- Dédié à une application
  - proxy http
  - proxy ftp
  - ...
- Il faut spécifier au niveau de l'application client l'existence du proxy (effectué par l'utilisateur)
- Mais il existe aussi des proxy-transparents (redirection au niveau routage et donc invisible à l'utilisateur)

Passerelle d'application

- Exemple :
  - Navigateur WEB: spécification de l'adresse IP et du numéro de port du serveur passerelle
  - La passerelle reçoit toutes les requêtes http (contenant l'URL à interroger) et peut observer, filtrer à volonté
  - Elle met son adresse IP en source et son numéro de port
  - Elle reçoit donc les réponses et elle peut donc aussi observer, filtrer les réponses ...
- Possibilité d'observation, de filtrage sur
  - mots-clés, URL, compte utilisateur ...
- détection virus,
- statistique,
- cache,
- facturation...
- Attention travail important pour chaque paquet, l'efficacité (débit, latence) peut baisser de façon importante en cas de charge significative

Passerelle d'application

- Exemple de Proxys
  - Squid (open source) : web
  - Privoxy : suppression des publicités, filtrage suivant le contenu des pages ... (en plus de Squid)
  - SSH Proxy (open source): dédié exclusivement à ssh
- Il existe des proxys publiques
  - Proxy.free.fr (client du réseau Free)
  - JanusVM: navigation anonyme et sécurisé
  - JAP (Java Anon Proxy) (Open source)
  - Intérêt: anonymat de la connexion, chiffrement, cache ....

Proxy transparent

- La redirection vers le proxy peut être complètement inconnu de l'utilisateur
  - Pas de configuration de l'application cliente (navigateur WEB par exemple)
  - On parle alors de proxy transparent
- Peut se faire simplement à l'aide d'une redirection sur le routeur de sortie (R1 dans notre exemple ou R2 si il n'y pas de DMZ)
- Tout les paquets à destination du port 80 arrivant de l'Intranet doivent être redirigés vers la machine sur laquelle tourne le proxy (web par exemple)
- Il faut configurer la machine sur laquelle tourne le proxy pour qu'elle accepte des paquets dont le port est 80 et l'adresse IP n'est pas la sienne (possible dans la plupart des systèmes)
- Ce type de proxy peut être très bien mise en place par votre fournisseur d'accès à votre insu !

Exemple d'attaques

- Malgré les filtrages certaines attaquent sont encore possibles
  - Saturation d'un réseau
  - Saturation d'un serveur (Web par exemple)
  - Défacement ou barbouillage de site Web
  - Usurpation d'adresse
  - ....

Le «Deny of service» DoS

- Existe depuis le début d'Internet (année 80)
- Différents DoS:
  - Faiblesse des implémentations des protocoles
    - Paquet ICMP trop gros, plante IP
    - Entête TCP tronquée avec checksum correct
    - Fragmentation IP erronée (champ offset faux)
  - Inondation de demande de connexion TCP (Syn Flood)
    - Envois de demande de connexion sans envoyer le 3eme paquet de l'ouverture, ressources allouée explosent
  - Flux UDP (UDP flooding) qui sature le réseau, plus aucune connexion TCP possible

Distributed DoS

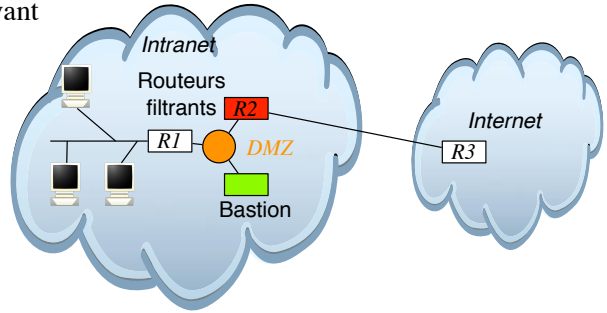
- les DOS peuvent être lancé depuis une seule machine (facile à contrer)
- Mais on peut les lancer depuis une multitude de machine (à l'aide de virus par exemple)
- On parle alors de DoS distribué (DDoS)

• Exemple célèbre de DDoS: attaque en 2000 de nombreux serveurs (eBay, Amazon, Yahoo, CNN...) arrêtés pendant plusieurs jours

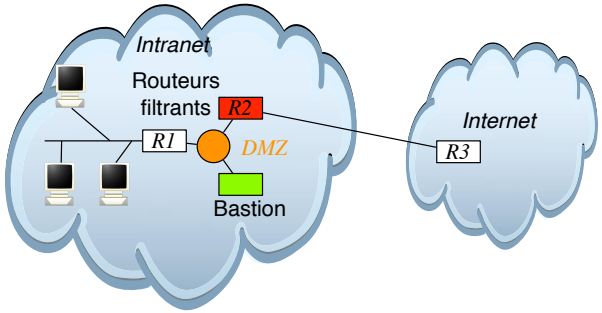
- DDoS toujours d'actualité et très difficile à éviter

Exercices

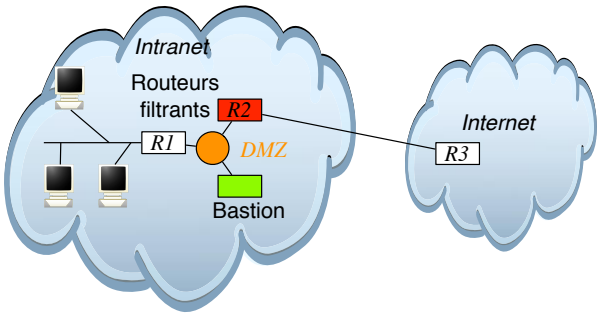
- Soit le réseau suivant



- On possède la plage d'adresse 192.0.0.224/28, elle va permettre d'adresser la DMZ et le réseau entre R2 et R3
- On dispose d'un bastion sur laquelle tourne des proxys et est installé un serveur WEB
- Donnez un plan d'adressage utilisant
  - du NAT dynamique (sur R1) pour les machines utilisateurs
  - Des adresses publiques pour la DMZ



- Donnez les tables de routage des routeurs et des machines utilisateurs
- Est ce que le 1er routeur dans Internet (R3) a connaissance des sous-reséaux (DMZ et R2-R3) de l'Intranet ?
- Si non comment un ping de R3 vers R1 peut-il fonctionner ?
- Comment configure t-on le NAT sur R1 ?
- Expliquez les transformations effectuées sur les paquets dans les routeurs 1 et 2.



- Donnez les listes d'accès sur R2 et R1 pour que
  - la passerelle applicative soit accessible depuis l'extérieur pour n'importe quelle application
  - les machines utilisateurs ne puissent accéder qu'à la passerelle applicative ?
- Est ce que l'on peut accéder via *ssh* depuis l'extérieur à une machine utilisateur ? Et de l'intérieur vers l'extérieur ?