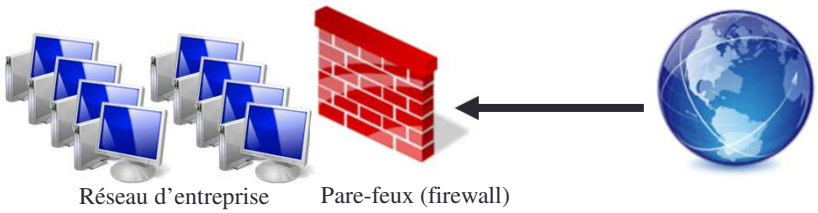
IP

Firewall / Parefeu

Définition

- Un pare-feux est un équipement/logiciel effectuant un filtrage des paquets
- Il sert à sécuriser un réseau des attaques extérieures
- Il sert à limiter la sortie d'informations sensibles



Réseau d'entreprise Pare-feux (firewall)

Types de pare-feux

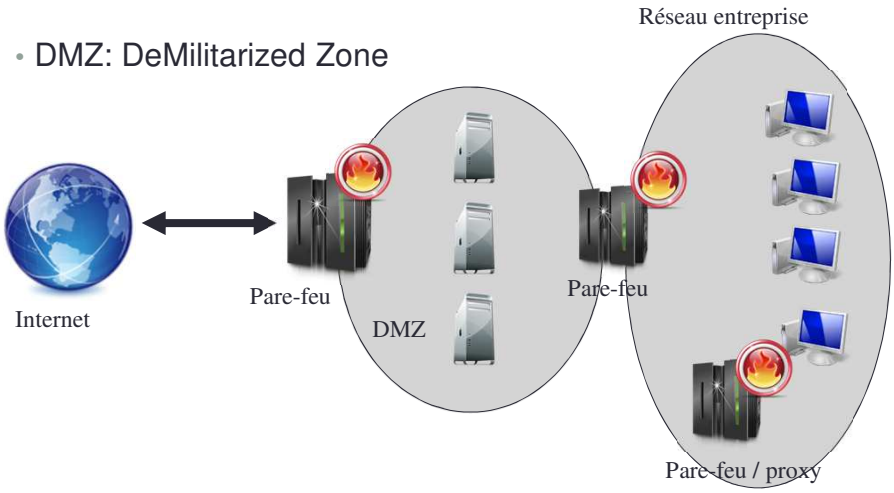
- Pare-feux local au SE
  - Windows / Linux

- Pare-feux sur les routeurs (ACL)
  - Règles de filtrage des paquets
- Pare-feux dédié (*appliance*)

- Pare-feux applicatifs (proxy par exemple)

Topologie classique

- DMZ: DeMilitarized Zone



Type de filtrage: sans état

- Sans état
  - Filtrage indépendant d'un paquet à l'autre
  - S'appuie sur des règles d'admissions/rejets
  - Les règles s'appliquent sur les champs IP et TCP/UDP
- Exemples
  1. reject ip.src=10.0.1.1
  2. accept tcp.port.dst=23 | tcp.port.src=23
  3. accept ip.dest in 10.0.0.0/24 && ip.src in 192.168.0.0/16
  4. accept ip.src in 10.0.0.0/24 && ToS=7

Types de filtrage: avec état

- *Stateful packet Inspection (SPI)*
- Le pare-feu conserve des informations sur les communications en cours:
  - Connexion TCP
    - Quadruplet identifiant la connexion
    - Numéro de séquence
  - UDP
    - Quadruplet identifiant la connexion
    - Requête en attente d'une réponse
- Intérêt:
  - Pas possible d'émettre des paquets d'une connexion qui n'existe pas
    - Exemple: des segments TCP dans une connexion en cours (N° de séq invalide)
    - Exemple: des réponses de services UDP (sans requêtes)
  - La configuration du firewall peut se faire que dans un sens (un contexte est mis en place pour les réponses)

Politique de sécurité

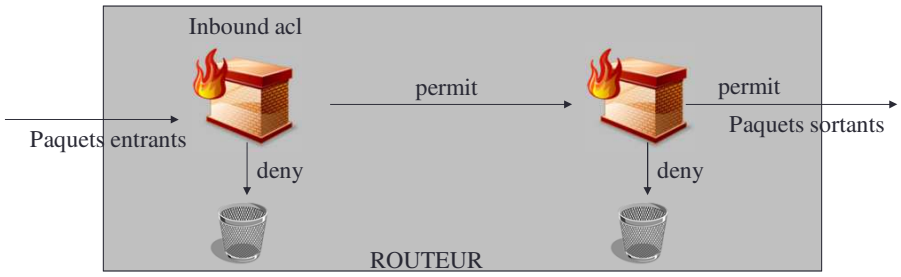
- Permissif
  - Accepter tout sauf ce qui est interdit
  - Peut s'appliquer au trafic sortant
- Restrictif
  - Refuser tout sauf ce qui est accepté
  - S'applique au trafic entrant

Firewall applicatifs

- Firewall / Proxy
  - Connexion des clients sur le proxy
  - Filtrage en fonction des:
    - URL
    - Données applicatives
  - Pare-feu configurer pour ne laisser passer que le trafic du proxy
- Pare-feu applicatif
  - Interprétation des données applicatives à la volée

Mise en œuvre: routeur cisco

- Routeur Cisco: ACL (access list)
  - Standard (de 0 à 99) uniquement sur les adresses IP sources (*stateless*)
  - Etendue (de 100 à 199 et de 2000 à 2699) sur les champs des en-têtes IP et TCP-UDP-ICMP



Mise en œuvre: routeur cisco (2)

- Une ACL est une liste de règles
- Les règles sont vérifiés les unes après les autres
- Algorithme
  - Si le paquet vérifie les critères de la règle, on l'applique (*permit/deny*)
  - Sinon on passe à la règle suivante
  - Si le paquet ne vérifie aucune règle, le *deny* s'applique
- Remarque: utilisation de masques inversés (wildcard) pour spécifier des plages d'adresses:
  - 0 = prendre en compte
  - 1 = ne pas prendre en compte

Mise en œuvre routeur cisco: configuration

Attention: adresses sources uniquement!

number prenant des valeurs dans [1-99]: *standard ACL*
access-list number **remark** name
access-list number **permit|deny** source source_wildcard
ip access-group number **in|out** //en mode interface
show access-list
show ip access-list
show access-list number

```
monRouteur(conf)#access-list 1 remark Une ACL de tests pour ce cours
monRouteur(conf)#access-list 1 permit 10.0.0.0 0.0.0.255
monRouteur(conf)#interface fastEthernet 0/1
monRouteur(conf-if)#ip access-group  1 out
monRouteur(conf-if)#end
monRouteur(conf)#
```

Mise en œuvre routeur cisco: configuration

```
monRouteur(conf)#access-list 1 remark Une autre ACL de tests pour ce cours
monRouteur(conf)#access-list 1 deny 10.0.0.1 0.0.0.0
monRouteur(conf)#access-list 1 permit 0.0.0.0 255.255.255.255
monRouteur(conf)#interface fastEthernet 0/1
monRouteur(conf-if)#ip access-group  1 out
monRouteur(conf-if)#end
monRouteur(conf)#
```

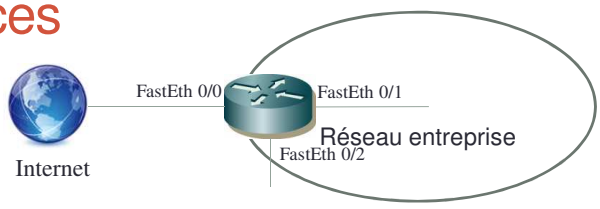
```
monRouteur(conf)#access-list 1 remark Une autre ACL de tests pour ce cours
monRouteur(conf)#access-list 1 deny host 10.0.0.1
monRouteur(conf)#access-list 1 permit any
monRouteur(conf)#interface fastEthernet 0/1
monRouteur(conf-if)#ip access-group  1 out
monRouteur(conf-if)#end
monRouteur(conf)#
```

Mise en œuvre routeur cisco: configuration

number prenant des valeurs dans [100-199 | 2000-2699]: *Extended ACL*
access-list number **remark** name
access-list number **permit|deny** proto src src_wildcard dest dest_wildcard [**tos** tos]
access-list number **permit|deny** icmp src src_wildcard dest dest_wildcard
[icmp-type [icmp-code] |icmp-message] [**tos** tos]
access-list number **permit|deny tcp** src src-wildcard **[operator** [port]] dest dest-wildcard
[operator [port]] **[established | syn] [tos** tos]
access-list number **permit|deny udp** src src-wildcard **[operator** [port]] dest dest-wildcard
[operator [port]] **[tos** tos]

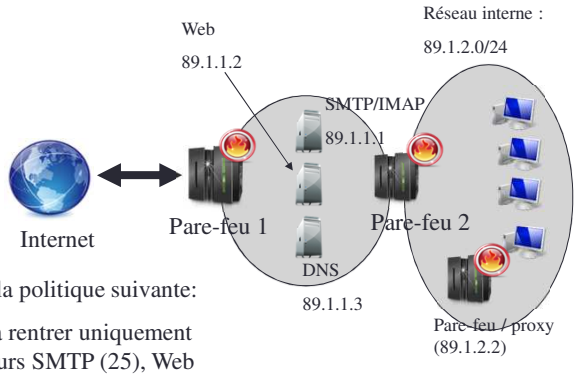
operator = eq ; lt ; gt ; neq ; range

Exercices



- Donnez les commandes pour la politique de filtrage suivant:
  - Exercice 1: Seul le trafic IP provenant de 30.0.0.0/16 est autorisé à rentrer sur le site.
  - Exercice 2: politique permissive. Tout est accepté sauf:
    - Le trafic provenant des adresses IP src 30.0.0.0/24 (de l'extérieure)
    - Le trafic tcp avec comme numéro de port 23; 24 ; 25 (de l'intérieur ou de l'extérieur)
    - Les pings (de l'intérieur ou de l'extérieur)
  - Exercice 3: Il faut que les salariés de l'entreprise puisse accéder à Internet. Tout le reste est bloqué.
  - Exercice 4: politique restrictive. Rien n'est accepté sauf:
    - Le service offert par un serveur interne 10.3.0.1 sur le port 85 (tcp)
    - Le trafic tcp provenant des PCs externes 10.4.0.0./24 sur les ports destinations 80 et 23.
    - Tous les messages ICMP

Exercice 5:



On souhaite mettre en œuvre la politique suivante:

Le trafic externe est autorisé à rentrer uniquement dans la DMZ pour les 3 serveurs SMTP (25), Web (80) et DNS (53).

Aucune connexion provenant de l'extérieure doit être accepté dans le réseau interne (celui avec les PCs).

Les PCs du réseau interne doivent pouvoir se connecter au serveur DNS et au serveur IMAP (143) / SMTP de la DMZ. On a mis en place un proxy dans la zone interne. Les machines du réseau interne ne peuvent accéder au web que par ce proxy.

Décrivez les règles qui doivent être mise en œuvre sur les différents firewall.