Sécurité réseau
Les Défenses

Sommaire

- **Problématique**
- **Les défenses**
- **Références**

La sécurité : problématique

- **Audit de sécurité**
  - Quels sont les machines utilisées,
  - Quels type de réseaux,
  - Quels sont les systèmes,
  - Quels type d'applications
- **Se protéger des intrusions**
  - Quelles sont-elles ?
  - Les types d'intrusion
  - Les journaux (logs)
- **Se protéger à l'intérieur**
  - Connaître les personnes de l'entreprise
  - Autorisation – exclusion : Cf politique interne
  - Qui fait quoi ?
- **Avec quoi se protéger ?**
  - Connaître les outils de sécurisation
  - Connaître les outils d'audit
  - Connaître les fonctionnalités de filtrage des éléments actifs du réseau

En résumé : la méthode

- Analyser les besoins et les risques
  - audit de l'architecture
- Déterminer les outils et les techniques à utiliser : adopter une politique de sécurité
  - Stratégie des mots de passe
  - Gestion des accès
  - Gestion des certificats et des signatures
  - Gestion des clés
- Mettre en place la tracabilité
  - mise en place de journaux (logs), outils de surveillances

Les défenses

- Plusieurs modèles ou niveaux de sécurité existent :
  - La sécurité par l'hôte : chaque machine est sécurisée à un certain niveau (protections locales et sur les l'accès aux ressources)
  - La sécurité par le réseau : l'accès à l'ensemble des ressources du réseau est protégé par un firewall
- La sécurité sur Internet passe le plus souvent par l'utilisation de firewall ou pare-feu.

Les systèmes pare-feu (1)

- Un firewall intervient à trois niveaux :
  - Restreindre l'accès à un point précis
  - Empêcher l'accès aux ressources à des utilisateurs non-reconnus
  - Restreindre la sortie à un point précis
- Physiquement , un système pare-feu est une combinaison d'éléments matériels (ordinateur, routeur, …) et logiciels.

Les systèmes pare-feu (2)

- Acteur d'une politique de sécurité pour la restriction de l'accès au réseau en un point précis; il ne peut à lui seul résoudre tous les problèmes de sécurité.
- Un pare-feu joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle OSI.
- Trois types principaux de pare-feu :
  - Filtrage de paquets
  - Filtrage de paquets avec état
  - Filtrage applicatif (ou proxy)

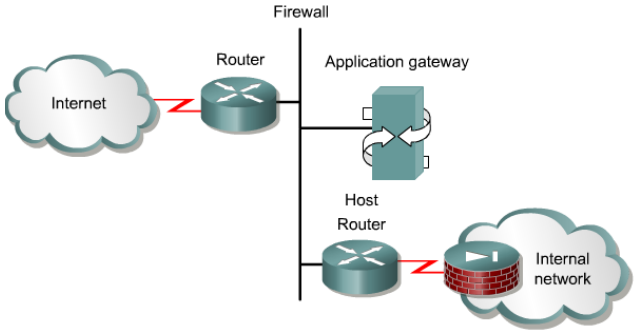
Politique de sécurité

- Politique permissive (*open config*) : politique qui repose sur le principe que par défaut on laisse tout passer puis on va restreindre pas à pas les accès et les services explicitement interdits.
- Politique stricte (*close config*) : politique qui repose sur le principe inverse : on commence par tout interdire, puis on décide de laisser seulement passer les services ou adresses explicitement autorisées.
- **Il est mieux d'interdire tout ce qui n'est pas explicitement permis que de permettre ce qui n'est pas explicitement interdit.**
  - On ne connaît jamais à l'avance toutes le menaces qu'on va subir
  - Si on fait un oubli, il vaut mieux interdire quelque-chose d'utile que d'autoriser une attaque!

Politique de sécurité

- Une politique : série de règles
  - **SI** *condition* **ALORS** *action*
  - *condition* : ensemble de sélecteurs (entêtes IP, TCP, UDP)
  - *action* : Accept, reject …

Les Firewalls (1)



A firewall is an architectural structure that exists between the user and the outside world to protect the internal network from intruders.

Source: Cisco system

Les Firewalls (2)

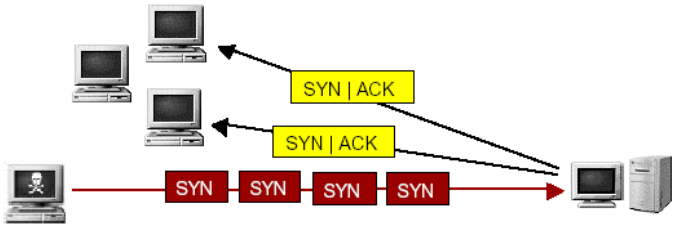
- Logiciel/Matériel :
  - Station de travail standard avec logiciel firewall (IP-tables)
  - Boîte noire spécialisée qui contient aussi un logiciel (Cisco PIX, Cisco IOS…)
- Sans mémoire (stateless)
  - Ne se rappelle pas des paquets qu'il à déjà vu.
- Avec mémoire (stateful)
  - Garde une trace des paquets et des connexions qui passent dans des tables d'état interne
  - Reconstruit l'état de chaque connexion, voire de certains protocoles.

Les Firewalls à mémoire

- Les FW à mémoire connaissent les connexions établies et peuvent automatiquement autoriser le trafic de retour.
- TCP:
  - Pour chaque connexion il sait à quoi doit ressembler le prochain paquet (Flags, numéros de séquence);
  - Il peut éliminer les paquets qui ne correspondent pas;
  - Il peut empêcher le syn-flooding.

SYN-flooding

- **Principe** : Envoyer massivement des demandes de connexion (**flag SYN à 1**) vers la machine cible avec des adresses sources aléatoires.
- La machine cible renvoie les SYN-ACK en réponse à chaque SYN reçu

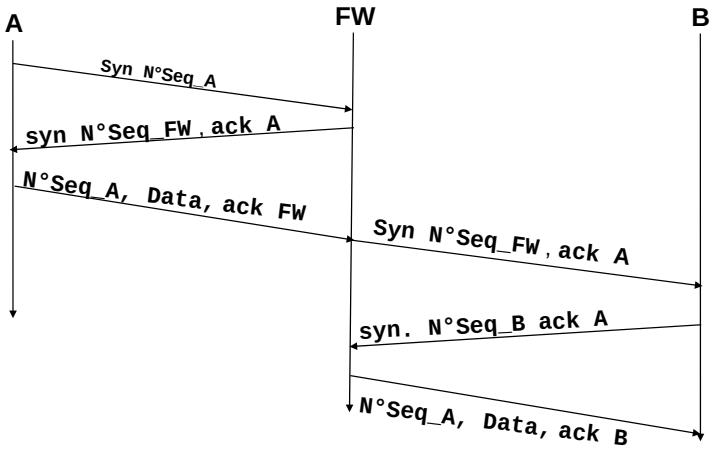


- Aucun ACK n'est renvoyé pour établir la connexion : connexions semi-ouvertes consomment des ressources mémoire ;
- Au bout d'un moment, la machine cible est saturée et ne peut plus accepter de connexions ;

Protection SYN-flooding (1)

- **Simple**:
  - Le FW surveille les tentatives d'ouverture de connexion qu'il voit passer;
  - S'il constate qu'une connexion reste à demi-ouverte trop longtemps, il envoie un RST
- **Avancée**:
  - Le FW temporise les paquets syn et génère lui-même un syn-ack
  - C'est seulement s'il reçoit un ack qu'il envoie le syn original

Protection SYN-flooding (2)



- Le FW doit générer un N°Seq à la place de B ;
- Il passera le reste de la connexion à ajuster les numéros de séquences ;

Types de Firewalls

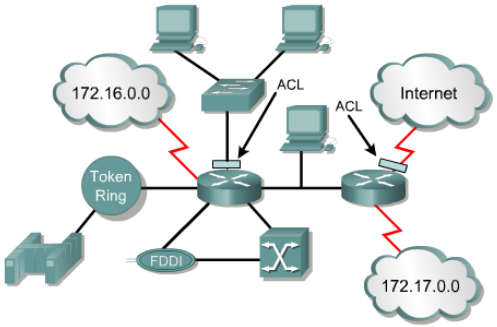
Plusieurs types de firewalls existent :

- Filtrage de niveau 2 : adresses MAC ➔ identification d'une carte réseau.
- Filtrage de niveau 3 : adresses IP ➔ identification de la machine + prise en compte basique des en-têtes TCP/UDP.
- Filtrage de niveau 4 : suivi d'état ➔ prise en compte de la globalité de la communication pour effectuer le filtrage.
- Filtrage de niveau 7 : filtrage applicatif ➔ Permet d'éliminer les paquets avec un contenu non désiré (Virus).
- Firewalls authentifiants ➔ Le FW peut exiger une authentification avant de laisser passer une connexion.

Filtrage de paquets (1)

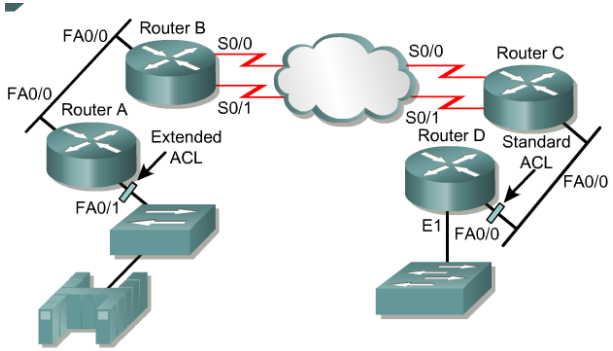
- Généralement des routeurs (**Screening Router**) qui permettent d'accorder ou de refuser l'accès en fonctions des éléments suivants :
  - l'adresse source ;
  - l'adresse destination ;
  - le protocole TCP ou UDP ;
  - le numéro de port.
- Opère au niveau des couches OSI suivantes :
  - Réseau et Transport
- Exemple : les ACL (*Access List Control*)

ACLs



- **Les ACLs sont des listes de conditions permettant d'autoriser ou d'interdire des paquets arrivant ou sortant sur une interface d'un routeur.**

Emplacement des ACLs



- Les ACLs Standard doivent etre placées le plus pret possible de la destinantion.
- Les ACLs étendues doivent etre placées le plus pret possible de la source du trafic refusé.

Source: Cisco system

Filtrage de paquets (2)

- Exemple de filtrage sélectif :
  - Blocage de toutes les connexions entrantes sauf pour la messagerie SMTP (filtrage par service sur N° port 25) ;
  - Blocage des connexions entrantes Telnet pour la machine serveur FTP (filtrage par adresse et par service).
- Le filtrage des flags (cf. protection contre le Syn-Flooding)

Filtrage de paquets (3)

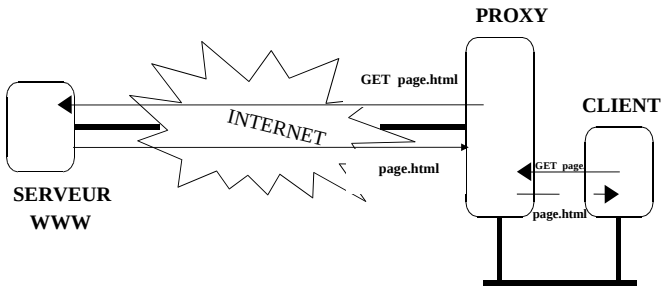
Limites de la technique

- **Manque de souplesse** : Offre une défense simple et efficace, mais manque de souplesse pour sa mise en place en protection d'un réseau.
- **Difficulté pour gérer certains protocoles** : Certains protocoles sont particulièrement délicats à gérer à l'aide de cette technique comme FTP (le suivi des échanges FTP est une opération complexe).

Proxy Firewall (1)

- Firewall de type applicatif qui filtre les communications application par application (couche 7 du modèle OSI).
- Permet un filtrage fin au niveau du contenu des paquets échangés :
  - traiter les requêtes et réponses à la place du système à protéger ;
  - les transmettre, après vérifications, ou les bloquer.
- Les serveurs proxy configurés pour HTTP permettent aussi le stockage de pages web dans un cache (Proxy cache) :
  - accélérer le transfert des informations fréquemment consultées vers les clients connectés.

Proxy Firewall (2)



Proxy Firewall (3)

Limites de la technique

- **Adaptabilité**: tout protocole transitant par le *firewall* doit être connu de celui-ci, pour pouvoir bénéficier de ses capacités de *proxy.*
- **Difficulté**: il est extrêmement délicat d'obtenir un système éliminant réellement toutes les attaques envisageables; la gamme de protocoles à examiner étant particulièrement vaste.
- **Performance :** le gain de sécurité obtenu à l'aide du *proxy* applicatif se paie en termes de performances

Firewalls authentifiants

- Le FW peut exiger une authentification avant de laisser passer une connexion.
- **En sortie**: permet de limiter l'accès Internet aux utilisateurs privilégiés
- **En entrée**: permet d'autoriser l'accès à des ressources internes pour des collaborateurs en déplacement.
- **L'authentification** peut se faire par rapport à une base locale ou en interrogeant une base centrale (protocoles RADIUS et TACACS)

Translation d'adresse (1)

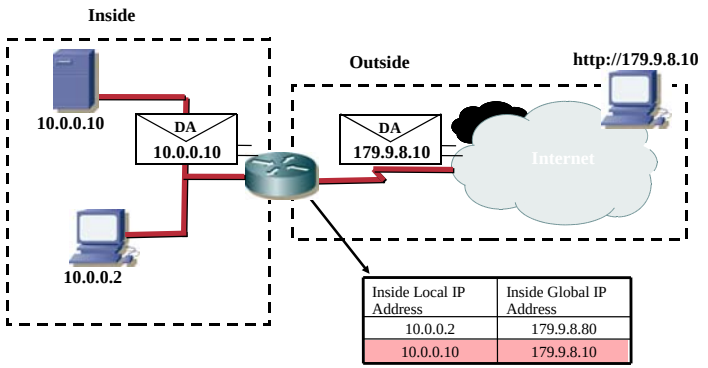
- La translation d'adresse est basée sur l'utilisation des adresses privées, non routables sur Internet : (10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.31.255.255, 192.168.0.0 à 192.168.255.255)
- Elle permet d'isoler le trafic local du trafic public de l'Internet et nécessite l'utilisation d'un translateur d'adresse NAT.
- Le NAT qui peut être localisé sur le routeur ou sur le proxy Server peut travailler suivant 3 types de translations **:**
  - n @ privées vers 1 @ publique (NAT dynamique ou PAT)
  - n @ privées vers m @ publiques (NAT dynamique ou PAT);
  - 1 @ privées vers 1 @ publiques (NAT statique).

NAT – Les termes

- Inside Local Addresses – An IP address assigned to a host inside a network. This address is likely to be a RFC 1918 private address.
- Inside Global Address – A legitimate IP address assigned by the service provider that represents one or more inside local IP address to the outside world.
- Outside Local Address - The IP address of an outside host as it known to the hosts in the inside network.
- Outside Global Address - The IP address assigned to a host on the outside network. The owner of the host assigns this address.

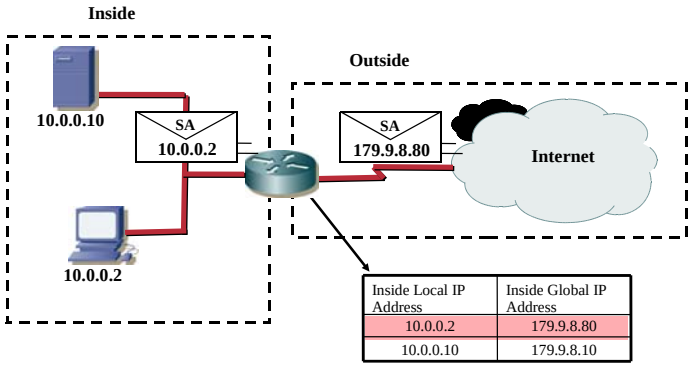
NAT Statique

- Static NAT is designed to allow one-to-one mapping of local and global addresses.



NAT Dynamique

- Dynamic NAT is designed to map a private IP address to a public address.

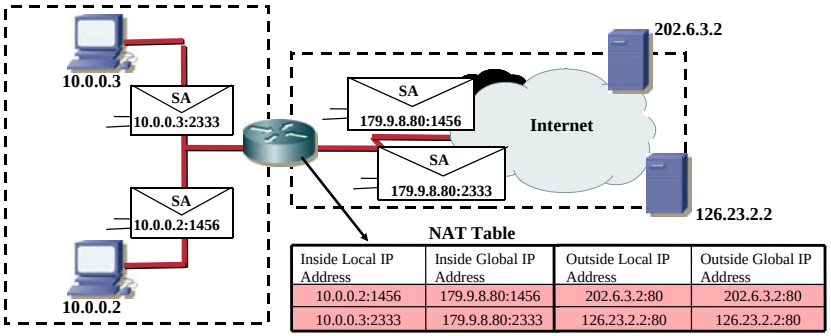


Inside Local IP Address	Inside Global IP Address
10.0.0.2	179.9.8.80
10.0.0.10	179.9.8.10

Translation de ports (1)

- La translation de ports utilise des numéros de ports TCP non standards, généralement supérieurs à 1023.
- Un problème se pose donc lorsque le nombre d'adresses disponibles est inférieur à celui des adresses à servir (adresses privés).
- PAT tire partie de la façon dont TCP/IP se sert des ports: pour chaque combinaison unique d'adresse locale et une entrée de port correspond une combinaison unique d'adresse globale et de port.

Translation de ports (2)



NAT Table

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
10.0.0.2:1456	179.9.8.80:1456	202.6.3.2:80	202.6.3.2:80
10.0.0.3:2333	179.9.8.80:2333	126.23.2.2:80	126.23.2.2:80

Autres possibilités des pare-feu

- **Filtrage de contenu** (URL, *spam* mails, applets Java, …)
- **Réseaux virtuels privés (VPN)** : les VPN permettent de canaliser un trafic sécurisé d'un point à un autre sur des réseaux de type Internet.
- **Tolérance de pannes** : certains pare-feu, comme CISCO/PIX supportent ces fonctionnalités (généralement exécution des pare-feu par paire pour permettre un une disponibilité élevée)
- **Détection des intrusions (IDS)**

Filtrage URL

(Source cisco.com)

- Controler les accès WEB
- Solutions:
  - **Black/White Lists**
  - **Third-Party Filter Server**
    - **…**

Black/White Lists

Listes statiques:

- Deux options:
  - Créer une liste locale d'URL sur le routeur
    Utiliser (en conjonction) un serveur tiers (third-party)
- Si le serveur tiers est utilisé, les URLs sont d'abord comparées à la liste locale, puis envoyées au serveur tiers
- Protocol supported: HTTP

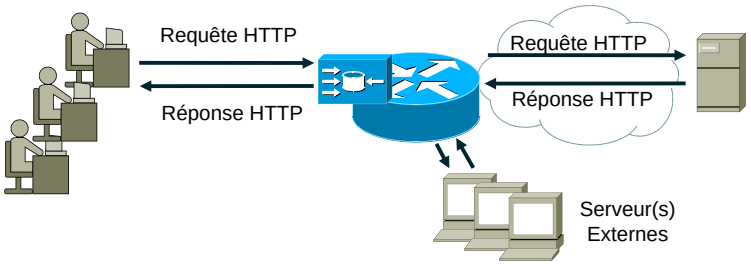
```
rtr(config)# ip inspect name insp http urlfilter
rtr(config)# ip urlfilter exclusive-domain deny www.notallowed.com
rtr(config)# ip urlfilter exclusive-domain permit www.cisco.com
```

(Source cisco.com)

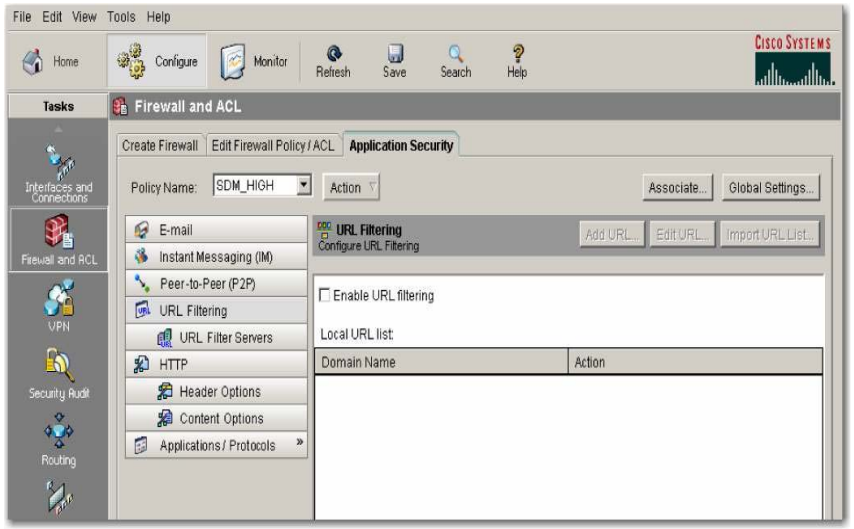
Serveur Filtre Tiers

Requêtes URL envoyées à un serveur tiers; les réponses utilisées pour décider si la requête est autorisée ou pas

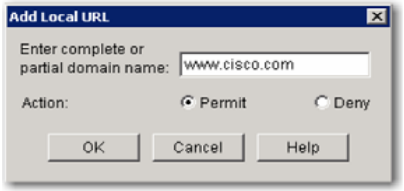
- Plusieurs serveurs peuvent etre utilisés
- Un serveur est actif à la fois

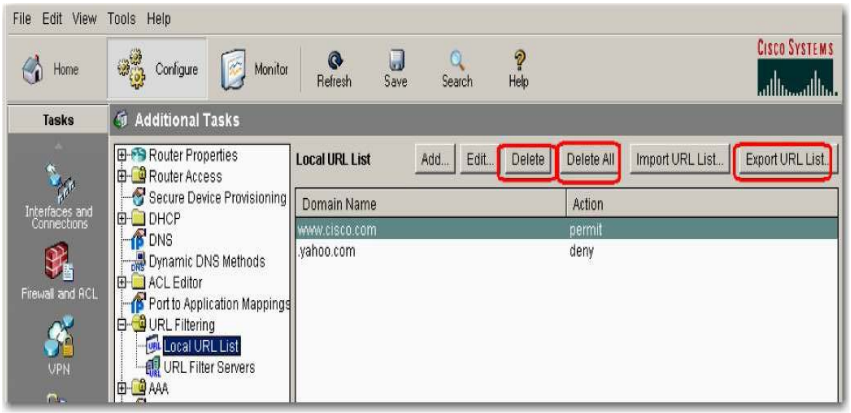


Configuration d'une liste d'url locale

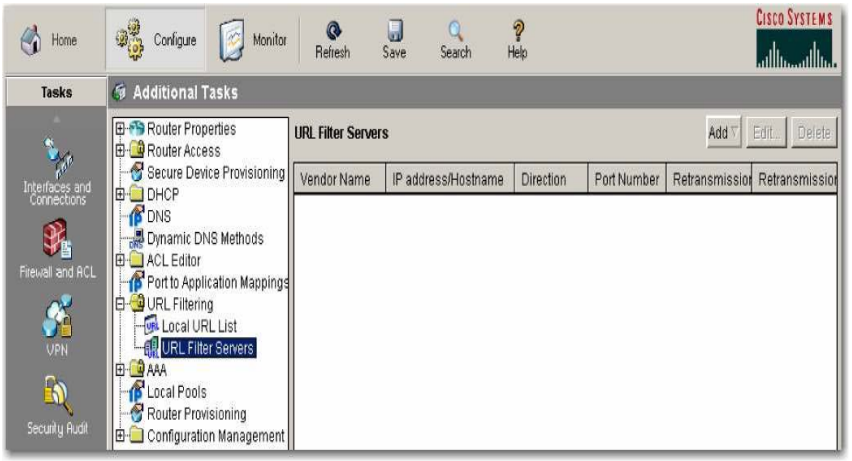


URL Filtering (cont.)

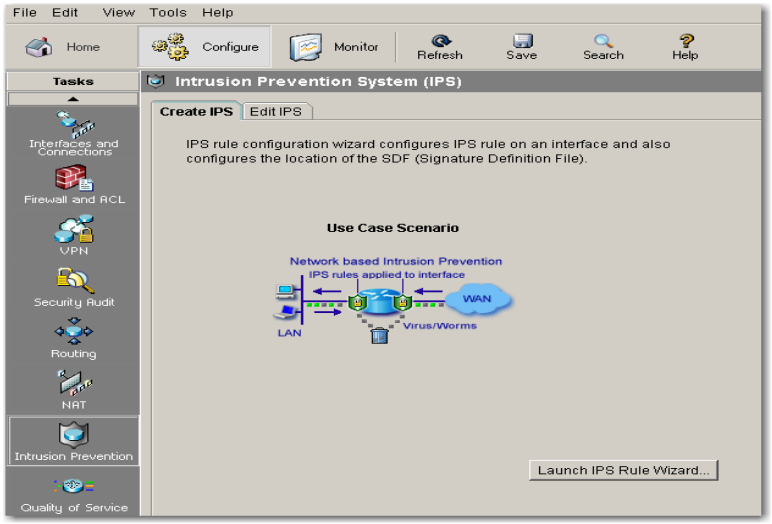




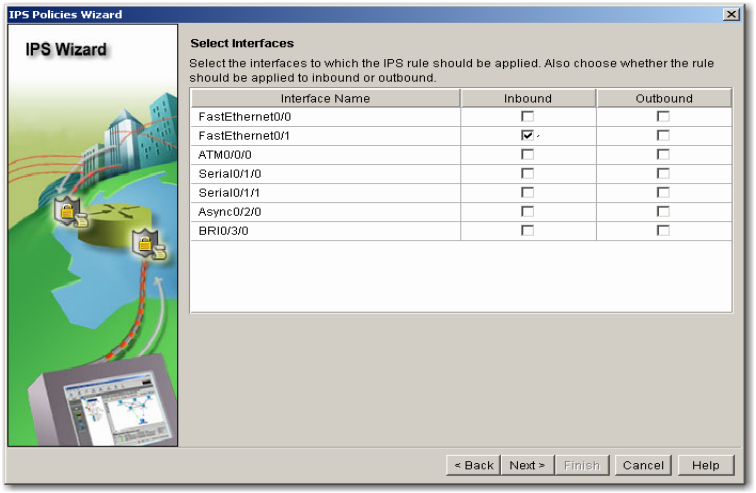
Configuration d'un serveur pour filtrage d'url



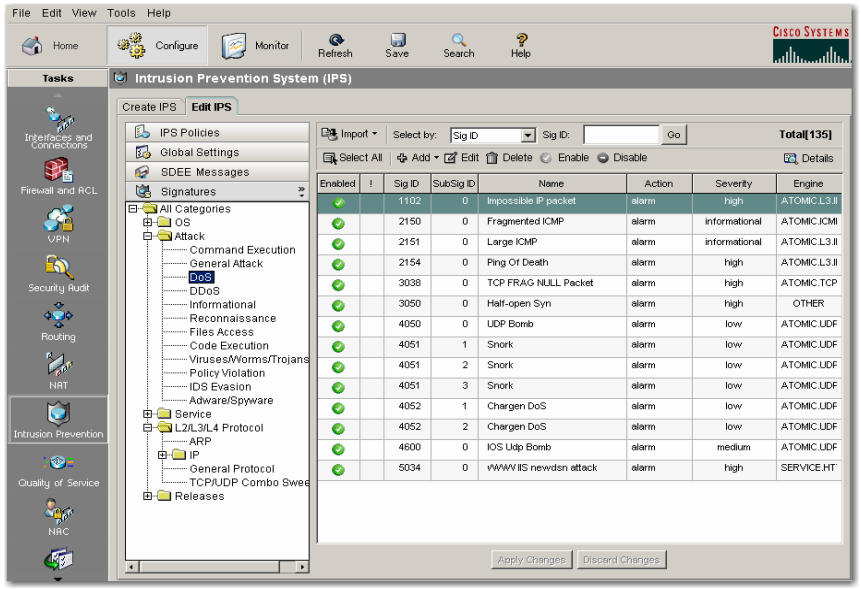
Intrusion Prevention System (IPS)



IPS (cont.)



IPS (cont.)



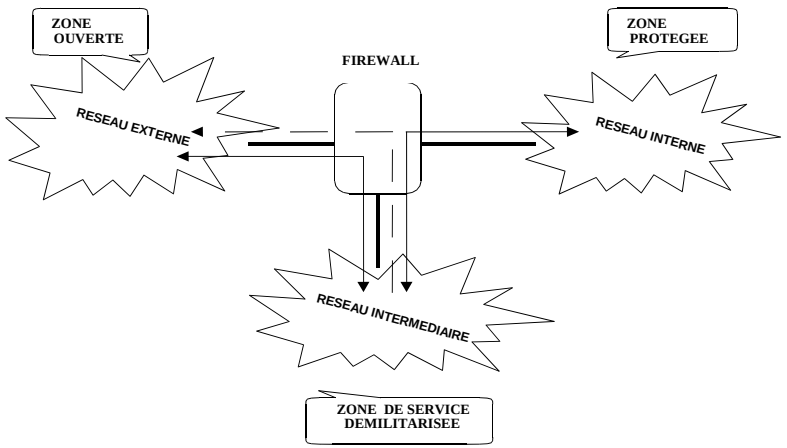
En résumé

- **Avantages :**
  - Fonctionne comme un équipement réseau ➔ facile à installer.
  - Bloque un très grand nombre d'attaques.
  - Possibilité de gestion et de configuration à distance et centralisées.
  - Solution bon marché au vu de son efficacité.
- **Inconvénients :**
  - Nécessite de répertorier de manière exhaustive tous les flux à autoriser.
  - De nombreuses solutions sur le marché.
  - Combiner au-moins le filtrage de niveau 3 et 4 pour être efficace.
  - Pour effectuer le filtrage, ne se base que sur les en-têtes des trames, non sur les données (sauf niveau 7).

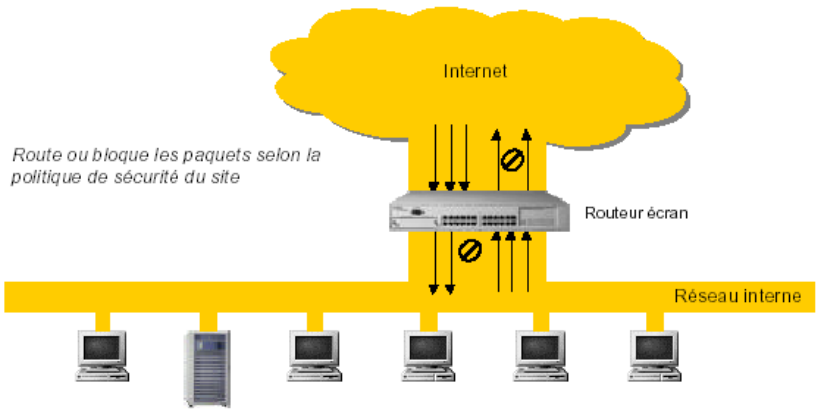
Typologie des firewalls (1)

- Plusieurs **zones de sécurité** commune aux réseaux. Elles déterminent un niveau de sécurité en fonction des accès réseaux et définissent les bases de l'architecture.
- **Réseaux externes** : réseau généralement le plus ouvert. Pas ou très peu de contrôle sur les informations, les systèmes et les équipements qui se trouvent dans ce domaine.
- **Réseaux internes** : réseau dont les éléments doivent être sérieusement protégés. Zone où l'on trouve les mesures de sécurité les plus restrictives.
- **Réseaux intermédiaires** : compromis entre les deux précédentes.
  - Zone isolée hébergeant des services mises à disposition des réseaux internes et externes (serveurs de messagerie, Web, FTP et DNS) .
  - Appelée aussi **réseau de service** ou de **zone démilitarisée** (**DMZ**), est considérée comme la zone la moins protégée de tout le réseau.

Typologie des firewalls (2)



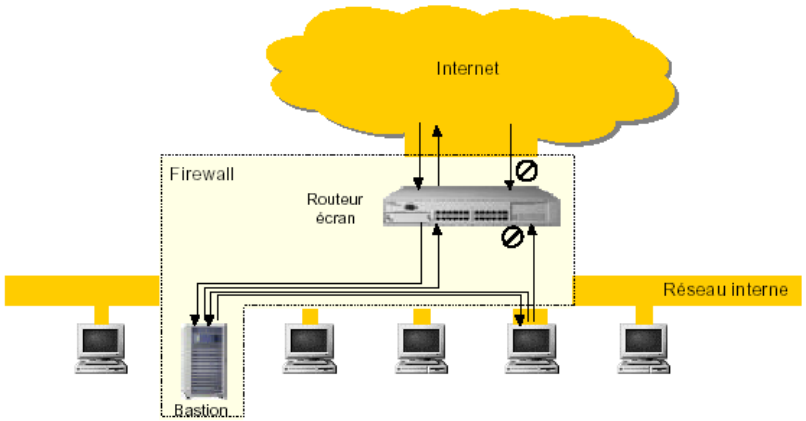
Firewall à routeur écran



Architecture la moins chère qui permet de faire un filtrage IP simple mais efficace.

Laisse passer les services entrant vers les serveurs du LAN et laisse sortir les demandes de service vers l'Internet.

Firewall avec bastion



Toutes les connexions en provenance de l'Internet passent forcément par le bastion qui se trouve sur le réseau interne. Il s'agit d'une machine directement exposée aux attaques.

Les clients du réseau interne peuvent accéder directement à l'Internet pour les services non mandatés par le bastion, sinon ils passent obligatoirement par les proxies du bastion.

Les serveurs publiques Web, DNS ou de Mail sont vus aussi comme des Bastions.

Firewall avec bastion

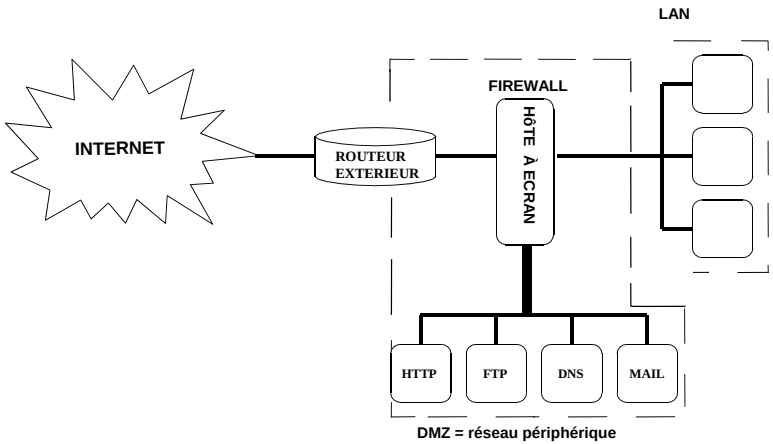
NAT + Filtrage

- **Configuration**:
  - NAT Dynamique pour les machines internes
  - NAT statique pour les serveurs accessibles
  - Filtrage sortant (trafic utile)
  - Filtrage entrant (blocage des l'accès au niveau du firewall)
- **Limitations:**
  - Connexions directes sur les serveurs internes (exploits, DoS)
- **Application :**
  - Sécurité basse.

Firewall à zone démilitarisée (1)

- Utilisation d'un sous-réseau à part pour isoler les bastions : c'est **la zone démilitarisée (DMZ)**.
  - Il s'agit d'un contrôle au niveau des protocoles de la couche application (FTP, HTTP, SMTP,...)
  - Cette séparation est effectuée et contrôlée par un pare-feu.
- La DMZ joue le rôle d'espace intermédiaire entre le réseau interne, dit de confiance, et un réseau non maîtrisé, donc potentiellement dangereux.
  - Permet d'isoler les machines publiques (Web, DNS, FTP, Mail, ...) du réseau interne.
  - Permet de contenir les attaques: Si le bastion est percé, le pirate est isolé dans la DMZ et ne peut pas accéder au réseau interne facilement.

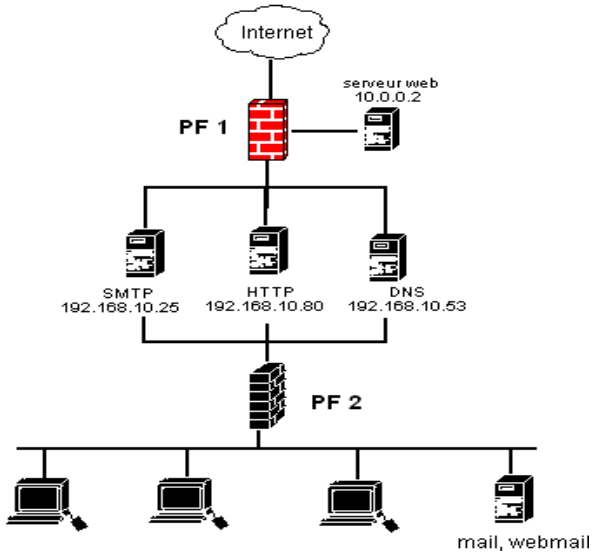
Firewall à zone démilitarisée (2)



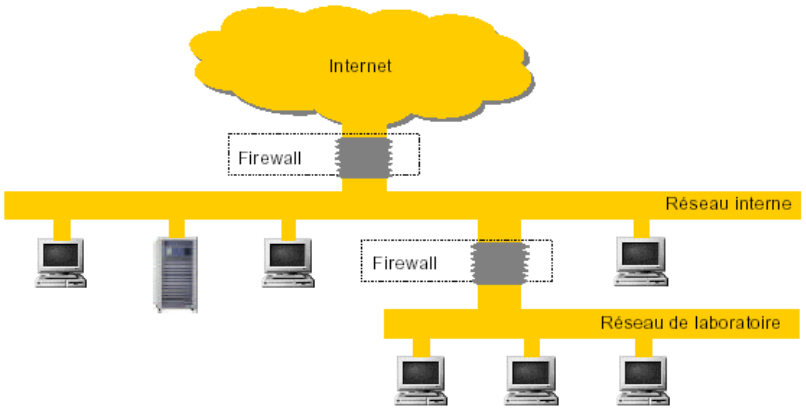
Firewall à zone démilitarisée (3)

- **Configuration**:
  - Machines internes ne peuvent se connecter qu'au proxy
  - NAT dynamique sortant
  - Filtrage sortant (trafic utile)
  - Filtrage entrant (blocage des l'accès au niveau firewall)
- **Application** :
  - Sécurité moyenne.

DMZ en sandwich.



Firewalls hiérarchiques



Souvent utilisé pour isoler un réseau de test interne à une entreprise.

Références

- http://www.hsc.fr/
- Transparents DESS DCISS 2002/2003 (*bulfone@icp.inpg.fr)*
- Transparents Cisco (URL Filtering)
- Les systèmes pare-feu, polycopie LT La Salle Avignon