

La sécurisation des réseaux

Le parefeu

Principe

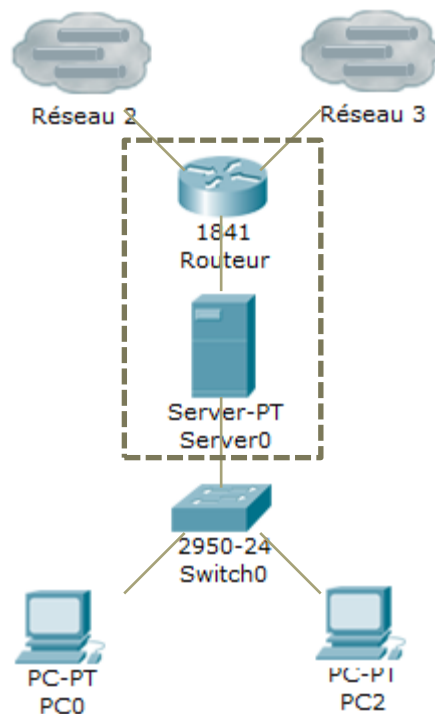
- Assure les fonctions d'un routeur évolué
 - Positionné à la limite de plusieurs réseaux
- Filtre les paquets
 - *Autorise ou refuse...*
 - Selon leur provenance et leur destination
 - Selon leur nature (protocole, port...)
- Journalise les événements
- Neutralise (blacklist)

Fonction routeur

- Routeur ou couplé à un routeur
- Filtre les trames :
 - Doit être un point de passage obligatoire
 - Configuration du réseau
 - Ou passerelle imposée (moins fiable)

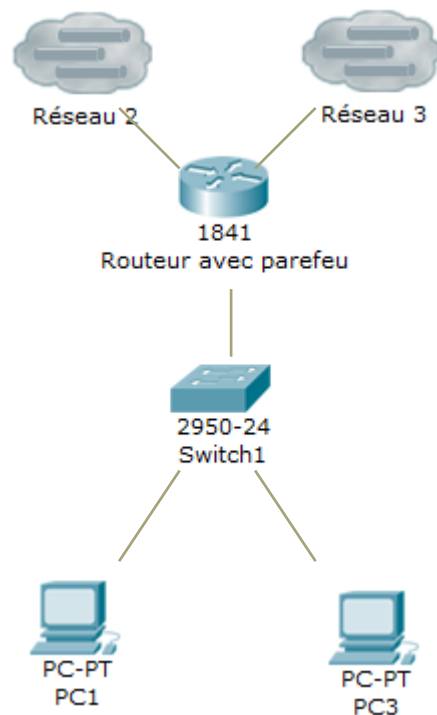
Configurations possibles

- Parefeu derrière un routeur



Server0 peut assurer les fonctions de parefeu et confier le routage à un routeur. Mais il n'est pas maître des interfaces du routeur et ne peut déterminer la provenance réelle des paquets. Il ne peut filtrer qu'en fonction du contenu

Configurations possibles



Le routeur assure les fonctions de parefeu en plus du routage. Il est maître de la provenance des paquets.

S'il s'agit d'un routeur matériel, il est possible qu'il ne dispose pas de fonctions avancées.

S'il s'agit d'un serveur (PC par exemple) avec un nombre d'interfaces suffisant, le choix du logiciel est possible.


Filtrage source/destination

- Application de ***règles (rules)*** cumulatives
 - Chaque logiciel à sa propre mécanique d'application des règles.
Se documenter
- Exemple.
 - Interdit tout ce qui va du réseau 1 vers le réseau 2
 - Autoriser les paquets qui proviennent de l'ordinateur A du réseau 1 vers le réseau 2
- Permet d'autoriser uniquement l'ordinateur A à communiquer avec le réseau 2

Filtrage sur contenu

- Filtrer sur un port prédéfini
 - N'autoriser que certains services spécifiques à être exposés à d'autres équipements/réseaux
 - Exemple : Interdire HTTP (80), RDP quand la demande provient d'un réseau non fiable
- Filtrer en fonction du contenu ou des caractéristiques du paquet
- Un filtrage trop strict peut provoquer des dysfonctionnements du système
- Un filtrage équilibré peut limiter la transmission d'informations 'parasites' et contribuer à sécuriser le réseau

Quelques parefeux

- Microsoft
 - Forefront TMG 
 - ISA server
- netFilter
- Distributions parefeu :
 - IPCop
 - PFsense
 - IPFire
 - ...