Cours de sécurité

Pare-feux ('Firewalls')

Gérard Florin
- CNAM -
- Laboratoire CEDRIC -

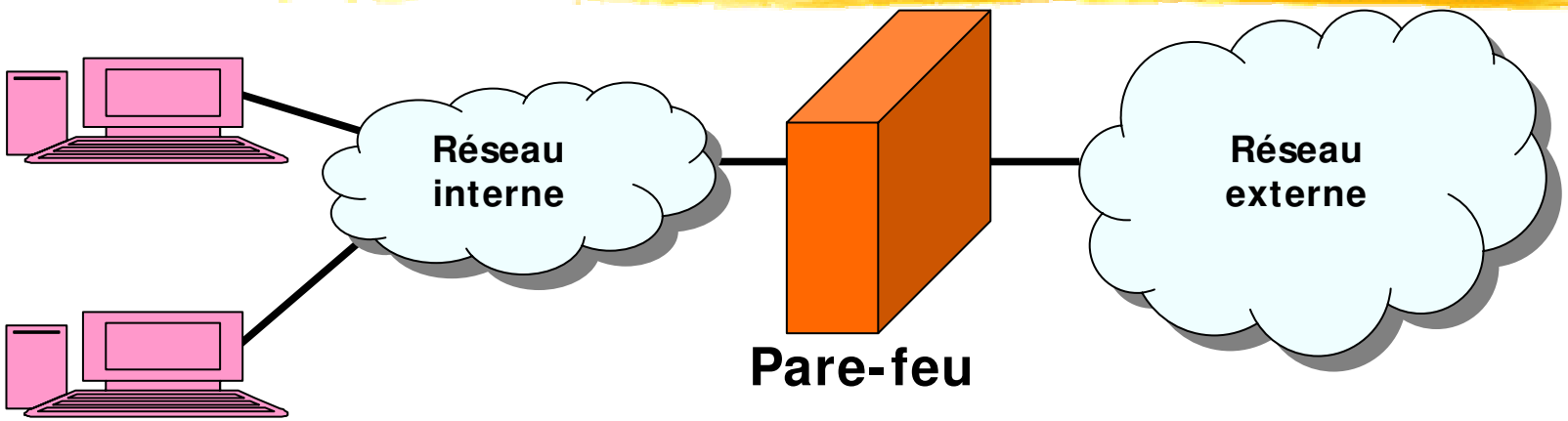
Plan pare-feux

- Introduction
- Filtrage des paquets et des segments
- Conclusion
- Bibliographie

Pare-Feux

Introduction

Pare-feux ('firewalls'): Architecture de base



- **1) Un domaine à protéger : un réseau 'interne'.**
  - Un réseau d'entreprise/personnel que l'on veut protèger
  - Vis à vis d'un réseau 'externe' d'ou des intrus sont suceptibles de conduire des attaques.
- **2) Un pare-feu**
  - Installé en un point de passage obligatoire entre le réseau à protéger (interne) et un réseau non sécuritaire (externe).
  - C'est un ensemble de différents composants matériels et logiciels qui contrôlent le traffic intérieur/extérieur selon une politique de sécurité.
  - Le pare-feu comporte assez souvent un seul logiciel, mais on peut avoir aussi un ensemble complexe comportant plusieurs filtres, plusieurs passerelles, plusieurs sous réseaux ….

Pare-feux ('firewalls'): Définitions de base

- **1) 'Firewall' :** en anglais un mur qui empêche la propagation d'un incendie dans un bâtiment => Français '**mur pare-feu'.**
- **2) Pare-feu :** en informatique une protection d'un réseau contre des attaques.
- **3) Technique employée** : le contrôle d'accès (le filtrage).
  - **a) Notion de guichet** : restriction de passage en un point précis et contrôle des requêtes.
  - **b) Notion d'éloignement** : empêcher un attaquant d'entrer dans un réseau protégé ou même de s'approcher de trop prés de machines sensibles.
  - **c) Notion de confinement** : empêcher les utilisateurs internes de sortir du domaine protègé sauf par un point précis.
  - **d) Généralement** un pare-feu concerne les couches basses Internet (IP/TCP/UDP), mais aussi la couche application (HTTP, FTP, SMTP….).
- **4) Image militaire** la plus voisine de la réalité d'un pare-feu: les défenses d'un chateau-fort (murailles, douves, portes/pont levis, bastion=> confinement, défense en profondeur, filtrage).

Pare-feux : le possible et l'impossible

Ce que peut faire un pare-feux :

- 1) Etre un guichet de sécurité: un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs.
- 2) Appliquer une politique de contrôle d'accès.
- 3) Enregistrer le traffic: construire des journaux de sécurité.
- 4) Appliquer une défense en profondeur (multiples pare-feux)

Ce que ne peut pas faire un pare-feux :

- 1) Protèger contre les utilisateurs internes (selon leurs droits).
- 2) Protèger un réseau d'un traffic qui ne passe pas par le pare-feu (exemple de modems additionnels)
- 3) Protéger contre les virus.
- 4) Protéger contre des menaces imprévues (hors politique).
- 5) Etre gratuit et se configurer tout seul.