

# L3 informatique TP n°3 : Ressources partagées et pare-feux

Sovanna Tan

Septembre 2009, rev. octobre 2014

# Plan

1 Ressources partagées

2 Le pare-feu

1 Ressources partagées

2 Le pare-feu

# Les protocoles Microsoft

OSI	SMB
7 Application	Application
6 Présentation	SMB/CIFS
5 Session	
4 Transport	NBT
3 Réseau	

## NBT

NBT signifie NetBIOS (Network Basic Input Out-put System) over TCP/IP. NetBIOS est à l'origine une API IBM. Il a été standardisé dans les RFC 1001 et 1002. Il s'occupe de la résolution de nom.

## SMB/CIFS

SMB signifie Server Message Block, CIFS, Common Internet File System. Ce protocole est utilisé dans le voisinage réseau.

# NBT

## Services offerts par NBT

- Service de noms
- Service de session : mode connecté full-duplex, analogue à circuit virtuel TCP
- Service de datagramme analogue à UDP

# SMB/CIFS

## Fonctionnement de SMB/CIFS

### Protocole en mode connecté

- Echanges dans un circuit virtuel (VC)
- Scénario : requête du client/réponse du serveur

## Fonctionnalités

### Nombreuses opérations

- Ouverture/fermeture de fichier
- Création/suppression de fichier ou de répertoire
- Lecture/écriture dans un fichier
- Recherche de fichiers
- Gestion de file d'attente pour les imprimantes

# Balayage du voisinage réseau

Le voisinage réseau contient des Domaines et des Workgroups.

## Master Browser (MB)

Machine élue qui maintient une liste partielle de machines sur un réseau local et la diffuse aux autres.

## Workgroup

La liste des machines est maintenue par un Master Browser élu. Le MB ne peut pas traverser un routeur.

## Domaine

La liste des machines est maintenue par le contrôleur de domaine principal (PDC) qui est Domain Master Browser (DMB). Si le réseau est routé, il y a un MB élu sur chaque brin de réseau qui se synchronise avec le DMB pour le maintien de la liste.

# Implémentations

- Microsoft
- Samba



# Autres protocoles

## Network File System (NFS)

Protocole de partage de fichiers très utilisé sous Unix.

## Apple Filing Protocol (AFP)

Protocole de partage de fichiers natif sous Mac OS 9.

## Web-based Distributed Authoring and Versioning (WebDAV)

Protocole qui permet de partager des fichiers sur le web.

1 Ressources partagées

2 Le pare-feu

# Sources

- *Network Security Hacks*, 2<sup>nd</sup> edition, Andrew Lockhart, O'Reilly, 2006.
- <http://www.netfilter.org/>
- Présentation du Pare-feu Windows :  
[http://www.microsoft.com/france/windows/xp/sp2/sp2\\_wfintro.msp](http://www.microsoft.com/france/windows/xp/sp2/sp2_wfintro.msp)

# Définitions

## Pare-feu

Système qui filtre les paquets réseau pour protéger l'accès aux données accessibles à travers le réseau ainsi qu'aux services offerts par les serveurs.

## Pare-feu réseau

Equipement réseau qui sépare le réseau Intranet du réseau Internet.

## Pare-feu personnel

Protège le poste de travail.

# Netfilter le pare-feu Linux

## Netfilter - Iptables

Le pare-feu `netfilter` est intégré au noyau Linux depuis la version 2.4. On le paramètre avec la commande `iptables` en définissant trois listes de règles.

- INPUT : filtre les paquets entrants
  - OUTPUT : filtre les paquets sortants
  - FORWARD : filtre les paquets routés
- 
- Pour consulter la liste des règles actives : `iptables -L`
  - Sert de pare-feu personnel sur les postes de travail et les serveurs.
  - S'emploie aussi en tant que pare-feu réseau sur une machine dotée de plusieurs interfaces.
  - Gère la translation d'adresses (NAT).

# Le pare-feu windows

## Microsoft Internet Connexion Firewall (ICF)

Pare-feu personnel inclus dans Windows depuis XP Service Pack 2.

- Sous XP, il ne filtre que les connexions entrantes. Depuis Vista, Il filtre les connexions entrantes et sortantes. Il manque encore un système de notifications qui alerte lors des blocages des connexions sortantes.
  - Il utilise un jeu de règles. Par défaut, les connexions entrantes sont bloquées et les connexions sortantes autorisées.
  - Il permet l'enregistrement (log) des paquets filtrés.
- 
- D'autres pare-feux personnels peuvent se substituer au pare-feu Microsoft comme ZoneAlarm ou Comodo.