LICENCE PROFESSIONNELLE GESTION DES RESEAUX ET SYSTEMES DE TELECOMMUNICATIONS

ANNEE 2006/2007

POINTS A PRENDRE EN COMPTE POUR LA MISE EN PLACE D'UNE POLITIQUE DE SECURITE EN ENTREPRISE

Jean-Christophe FORTON

SOMMAIRE

I) Concepts de base

$$\text{Risque} = \frac{\text{menace} \times \text{vulnérabilité}}{\text{Contre-mesure}}$$

- Menace = action de nuire
- Vulnérabilité = taux d'exposition à une menace
- Contre-mesure = vient prévenir la menace

I) Concepts de base

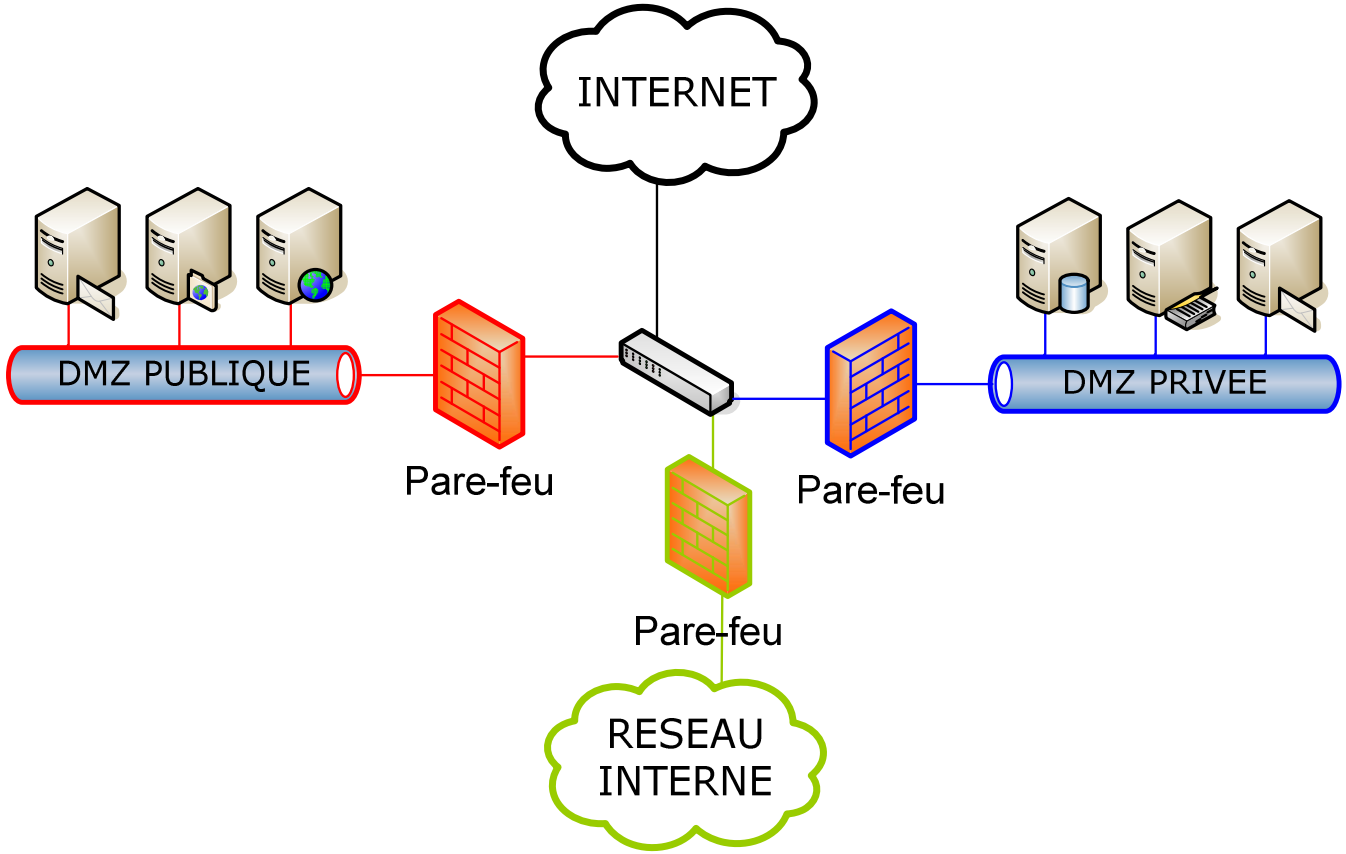
En sécurité, on essayera de remplir les objectifs suivant :

- **Intégrité** : prévenir la modification des données,
- **Confidentialité** : prévenir la visualisation des données,
- **Authentification** : prévenir les accès non autorisés,
- **Disponibilité** : garantir l'accès aux données,
- **Non répudiation** : garantir qu'une transaction a eu lieu,

sans pour autant compliquer le fonctionnement du système.

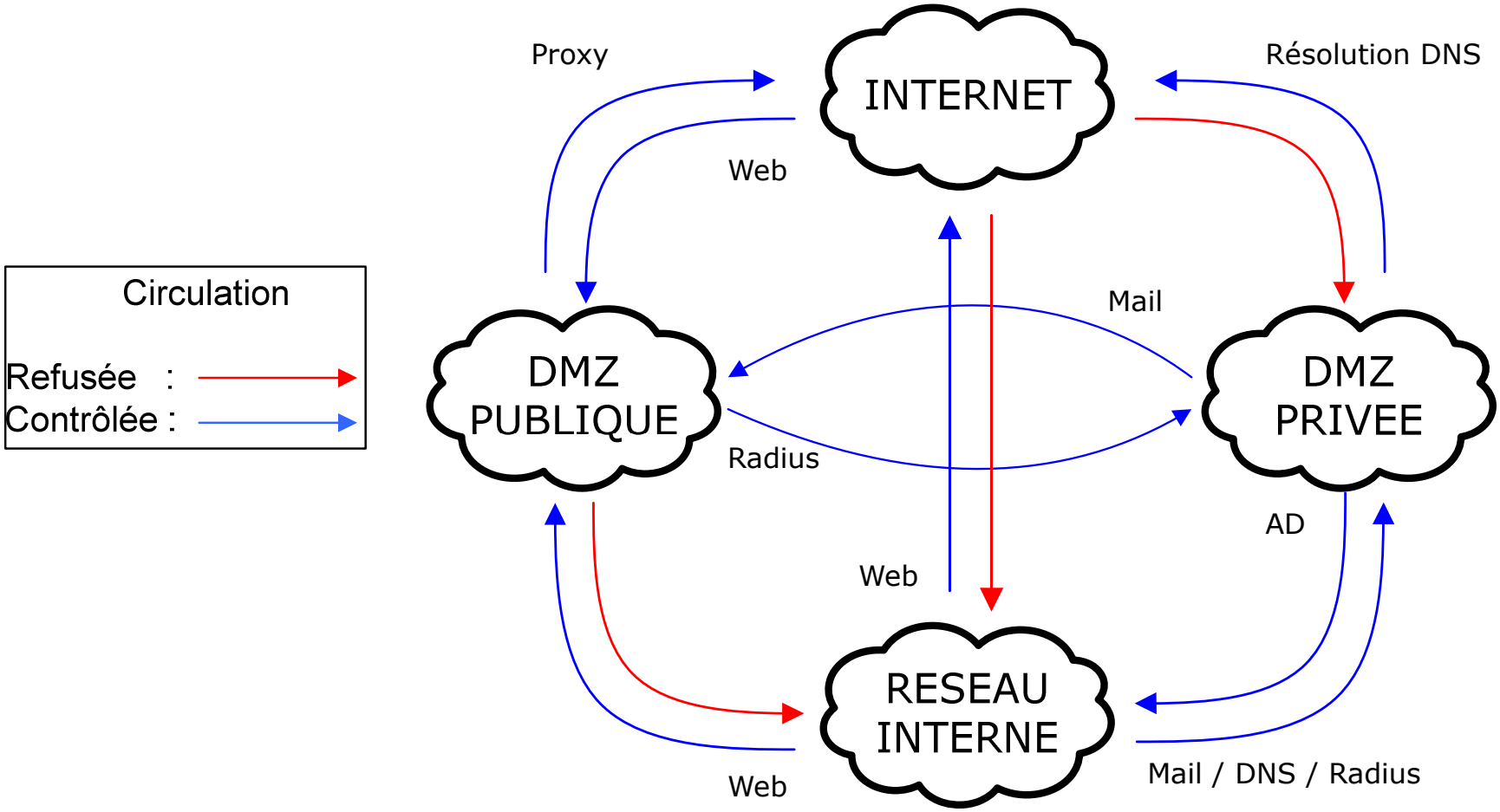
II) Architecture réseau sécurisée

Concept des DMZ



II) Architecture réseau sécurisée

Symbolisation des échanges



Jean-Christophe FORTON

III) Configuration du matériel utilisé en sécurité

Sécurité logique

- **Pare-feu** : prévient des intrusions mais empêche les comportements anormaux (spam, backdoor, etc…).
- **Sonde** : assure la non répudiation, prend des décisions.

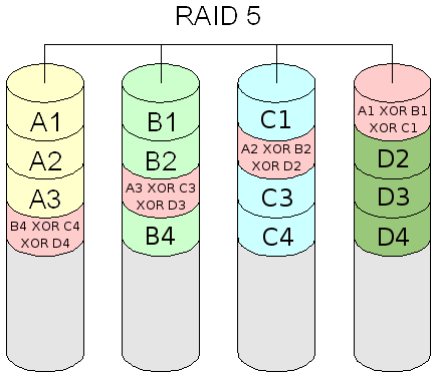
- **Routeur** : sécuriser les échanges.
- **Passerelle** : installation d'une sonde (évite les paquets reset).

III)Configuration du matériel utilisé en sécurité

Sécurité physique

- **SAN** : assure une haute disponibilité, dissuade l'écoute.
- **RAID (1, 5**): permet la sécurisation des données grâce à la redondance.

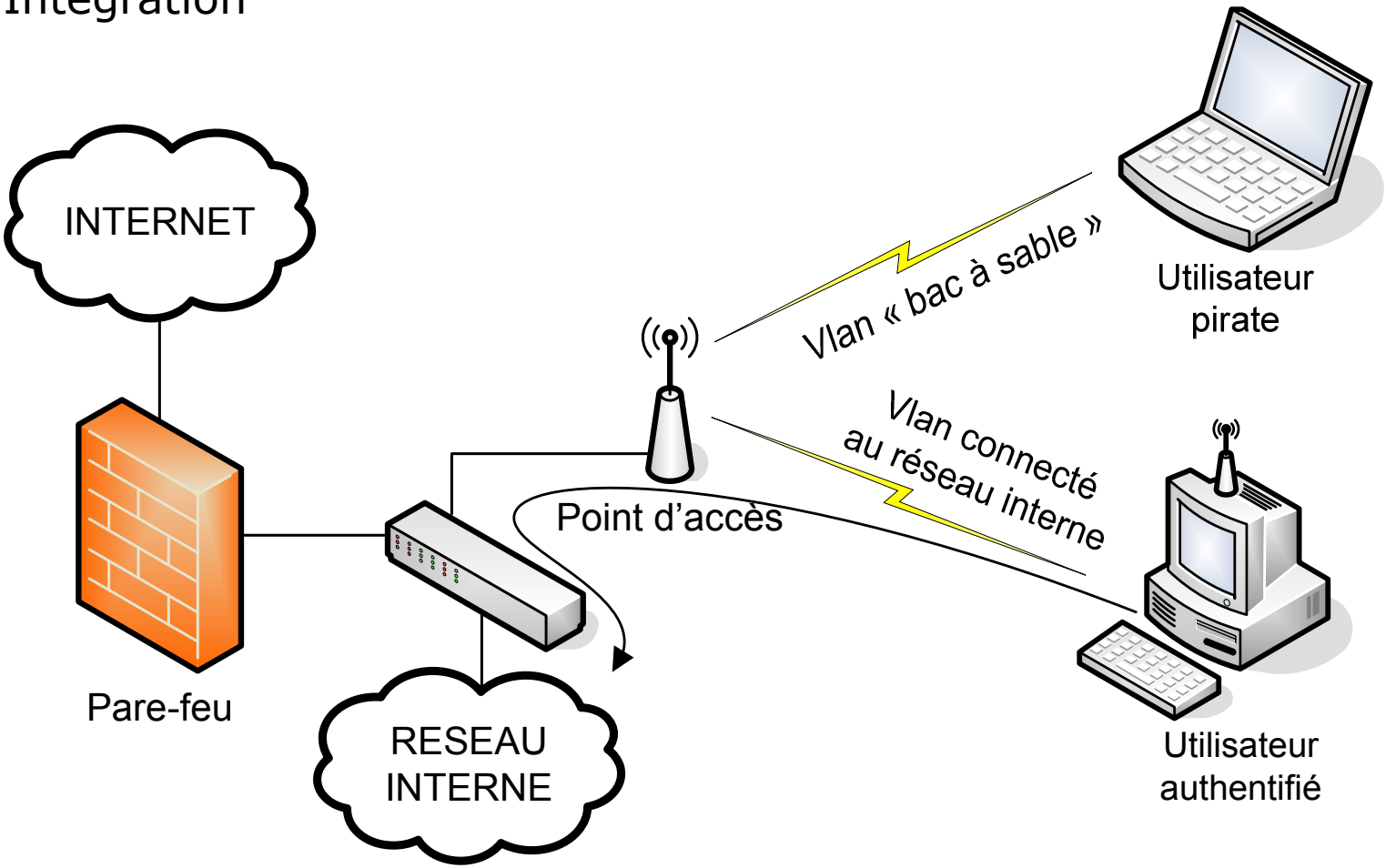
A1 XOR A1 = 1



- **Onduleur** : assure le fonctionnement de l'installation pendant une courte panne de courant (redondance secteur).
- **Groupe électrogène**

IV) Intégration et sécurisation des réseaux sans fil

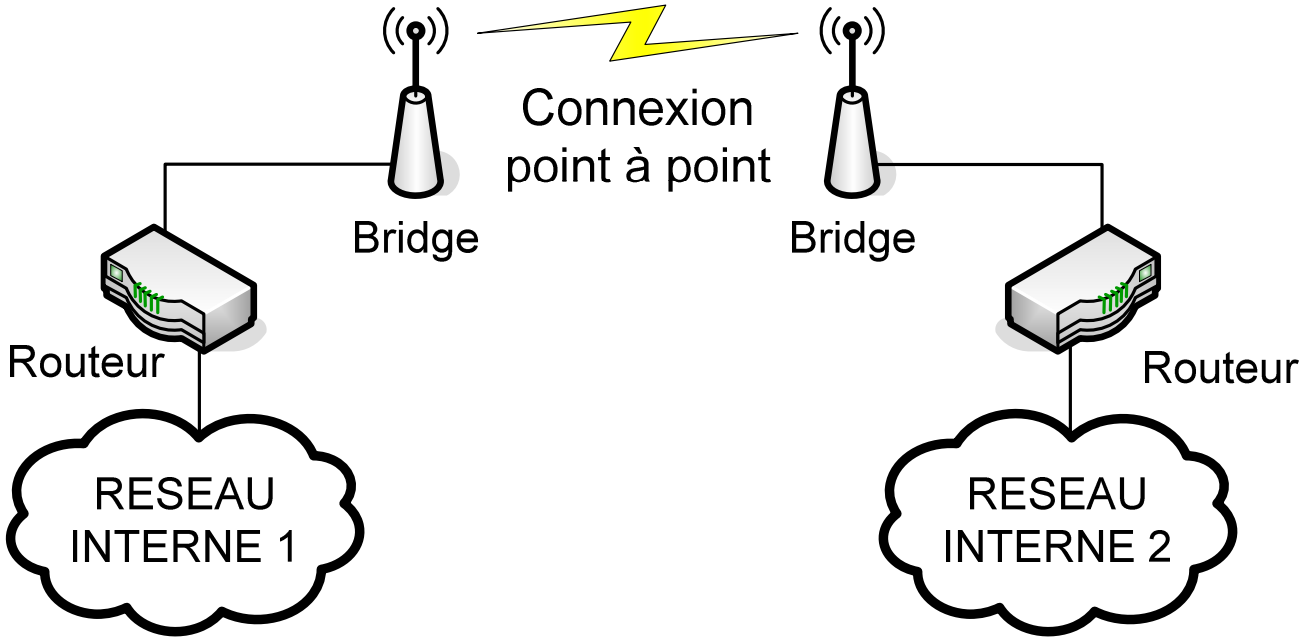
Intégration



Point d'accès connecté

IV) Intégration et sécurisation des réseaux sans fil

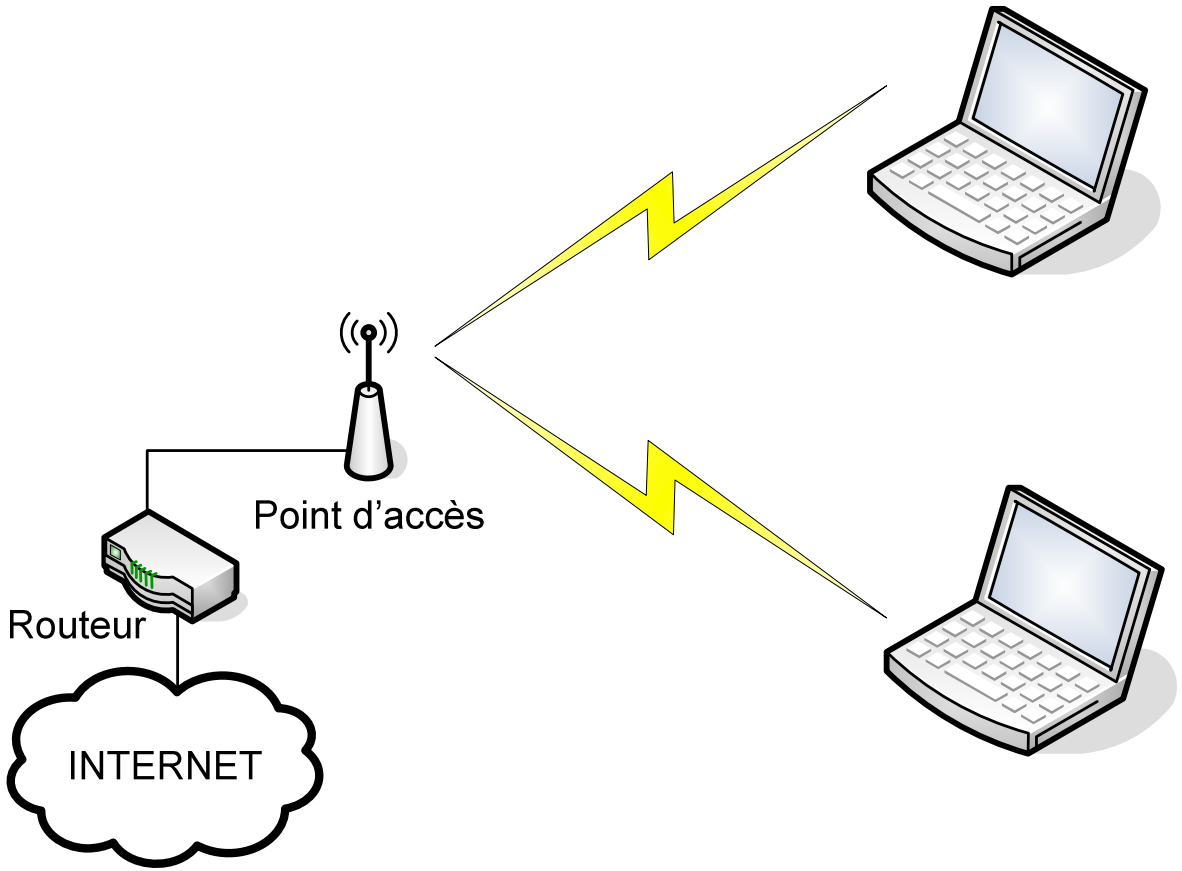
Intégration



Utilisation de bridge

IV) Intégration et sécurisation des réseaux sans fil

Intégration



Point d'accès non connecté

IV) Intégration et sécurisation des réseaux sans fil

Sécurisation

- **Authentification des utilisateurs** : Radius

  EAP-TLS ou EAP-PEAP

- **Authentification des matériels** : Radius / TACAS+

- **Cryptage de la liaison radio** :

  WPA (grâce au radius) ou WPA-PSK (si peu d'utilisateurs)

V) Sensibilisation, contrôle et sécurisation des postes clients

Sensibilisation

- **Informer les utilisateurs sur les risques.**
- **Charte informatique.**
- **Sensibilisation à la sécurité.**

V) Sensibilisation, contrôle et sécurisation des postes clients

Contrôle

Le contrôle doit se faire au niveau logiciel.

- On ne peut pas **interdire l'installation de logiciels**,
- On ne peut pas permettre aux clients d'apporter des **virus**.

Pour cela on peut utiliser des softs comme **OCS Inventory NG.**

V) Sensibilisation, contrôle et sécurisation des postes clients

Sécurisation

Les clients doivent être munis :

- de firewalls,
- d'antivirus,
- d'anti spam (si possible)

Pour les gros parc informatique on privilégiera les solutions « entreprise ».

MERCI

UNIVERSITE JOSEPH FOURIER
GRENOBLE 1
SCIENCES.TECHNOLOGIE.SANTÉ

Jean-Christophe FORTON

WiSNORT Server 2003 NETASQ Secure Internet Connectivity SNORT MySQL