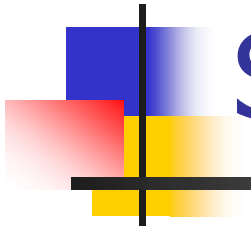
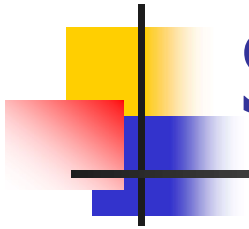


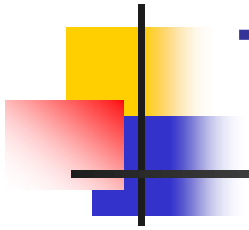
Cours d'architecture logicielle
Tactiques de conception
Sécurité

Lydie du Bousquet
Philippe Lalanda
Université Grenoble-Alpes



Sécurité

- Un système est sécurisé lorsqu'il est capable de résister à des utilisations non autorisées tout en fonctionnant nominalement
- La sécurité est une mesure de la capacité d'un système à repousser des attaques
- La sécurité est caractérisée selon différentes dimensions
  - La confidentialité
  - L’authentification
  - L'intégrité
  - La disponibilité
  - La traçabilité & la non-répudiation



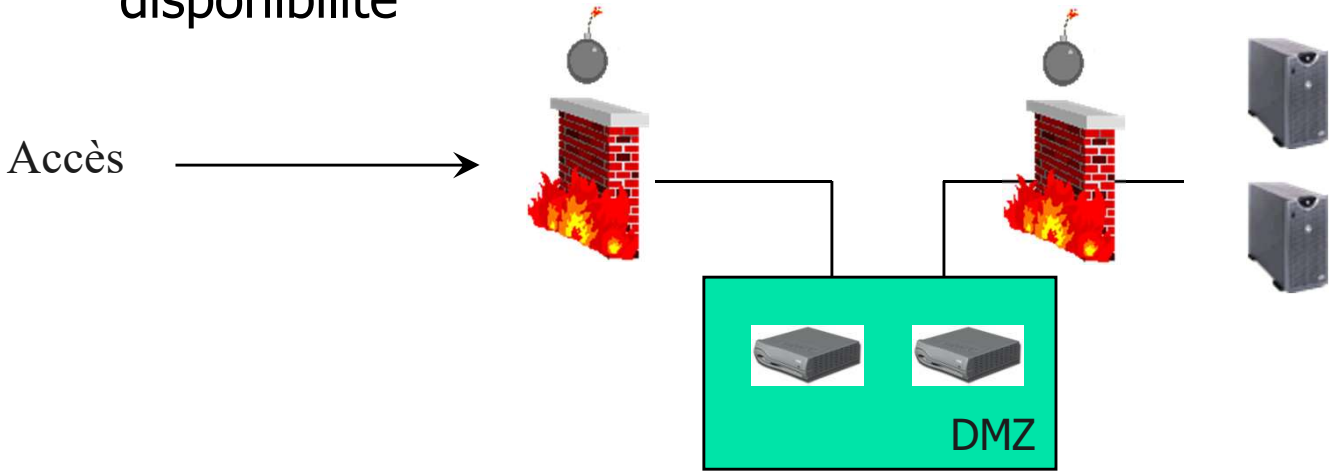
Tactiques pour la sécurité

- Pour garantir un fonctionnement nominal tout en résistant aux attaques
- Utilisation de tactiques pour
  - résister aux attaques
  - détecter les attaques
  - traiter les attaques

4. Sécurité

Tactique de résistance aux attaques – 1 « limiter l'exposition »

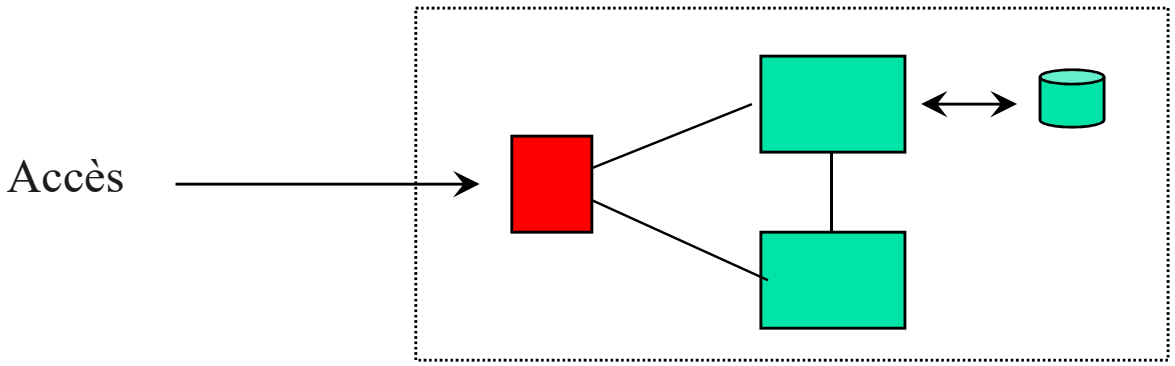
- Principe
  - répartition des services sur différents composants et différents "hosts"
  - utilisation d'un composant de type firewall
  - utilisation d'une DMZ (entre l'Internet et le firewall)
- Remarque
  - en opposition avec les tactiques de performance, voire de disponibilité



4. sécurité

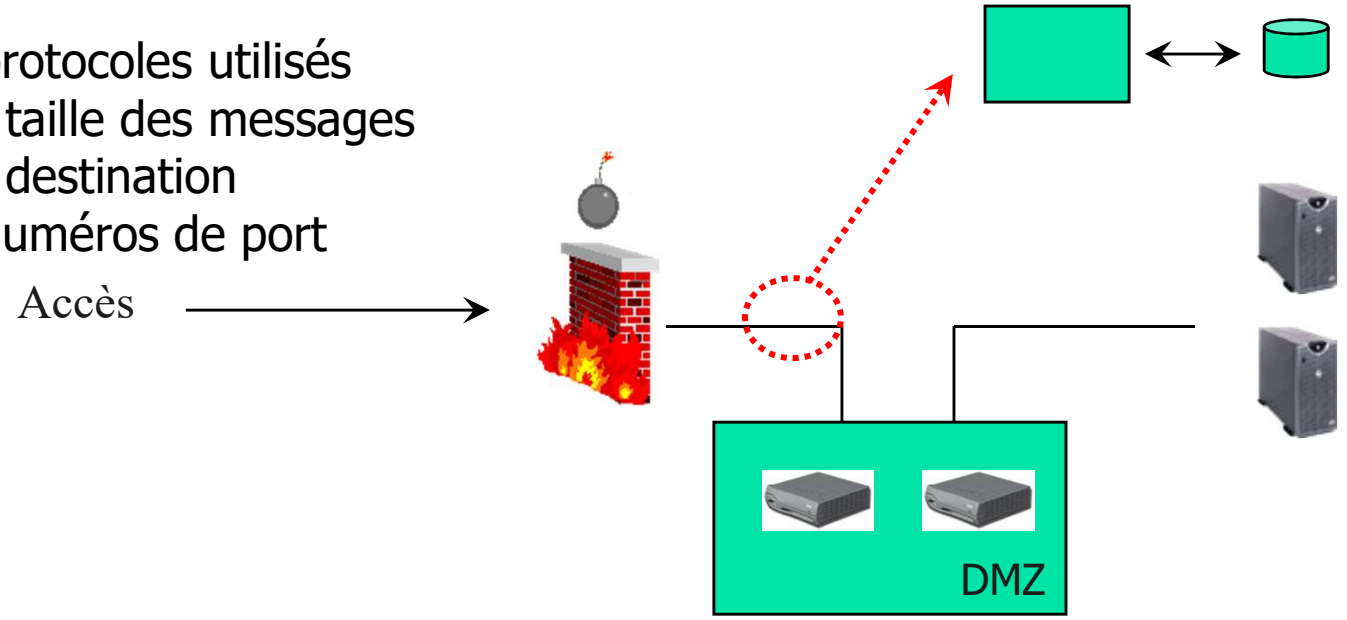
Tactique de résistance aux attaques – 2 « protéger les communications »

- Principes
  - Utiliser des techniques de chiffrement (avec des clés symétriques ou asymétriques)
  - création d'un composant global assurant la sécurisation des communications
    - Chiffrement
    - Établissement de profils d'utilisateurs, de mots de passe, …
    - Logging

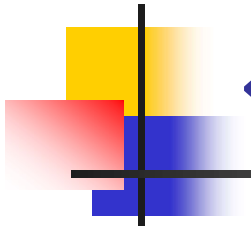


Tactique de détection des attaques « composant de détection »

- Principe : introduire un composant de détection d'intrusion
  - comparaison des patterns de communication avec ceux d'une base de données
  - en cas de soupçon, comparaison avec des patterns d'attaques connues
  - pour faire ces comparaisons, certains messages sont filtrés sur la base
    - des protocoles utilisés
    - de la taille des messages
    - de la destination
    - des numéros de port



Tactique de traitement des attaques « composant de Log »



- Principe : introduire un composant de Log pour
  - stocker des informations de communication
  - stocker de l'état courant avec une attention particulière aux informations administratives (mots de passe, liste d'utilisateurs, noms de domaine, etc.)
- Remarque
  - le composant de log est souvent l'objet d'attaques et doit être protégé (conception détaillée)
  - tactique proche des tactiques de redondance pour la disponibilité

Résumé des tactiques