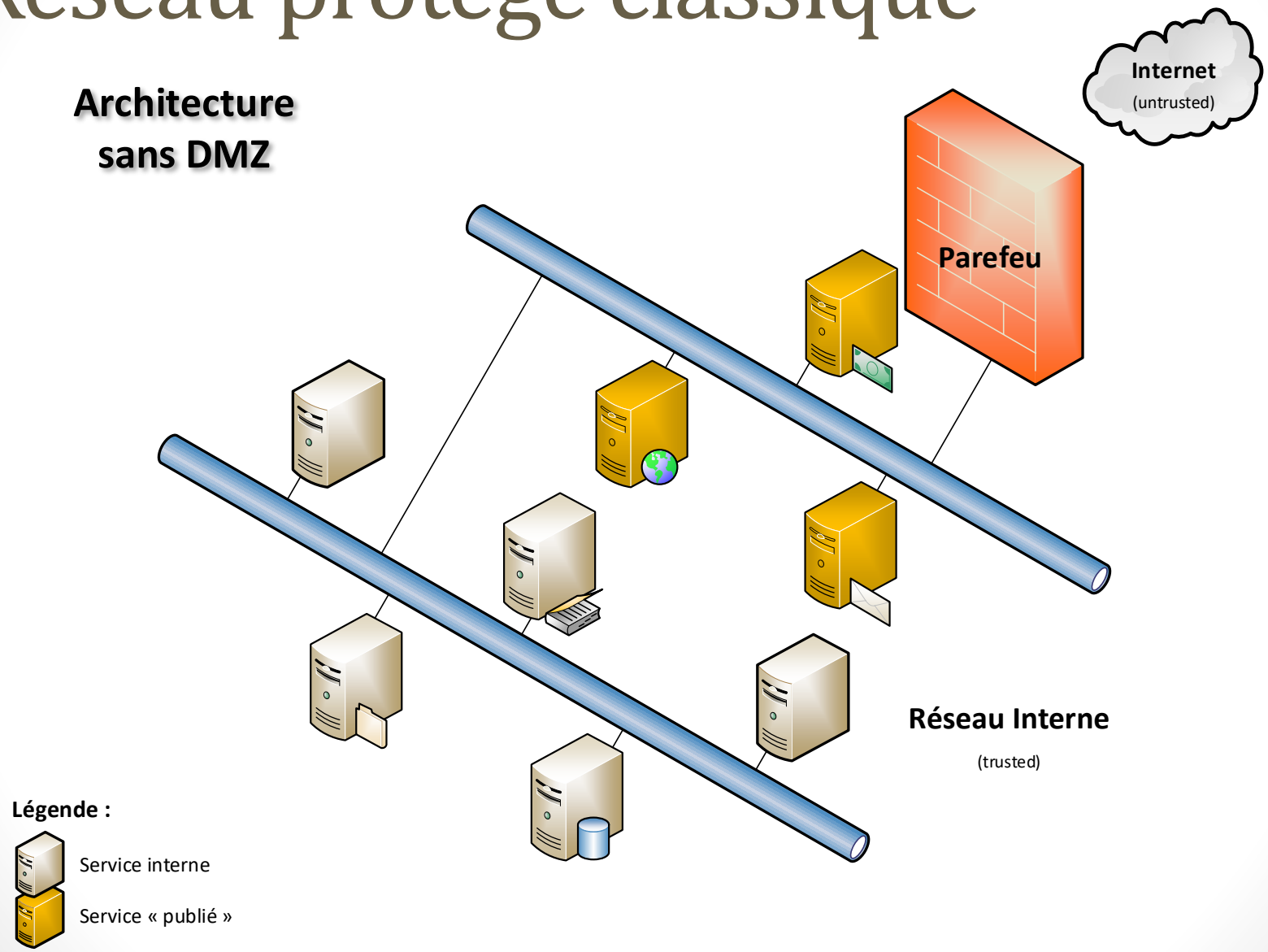
Sécurisation des réseaux

Principe de la DMZ

Introduction

- Terme emprunté géopolitique / militaire
  - Corée du nord / Corée du sud
  - 27/07/1953 - 250 km de long et 4 km de large

Réseau protégé classique



Réseau protégé classique

- 1 Parefeu
- Services publiés (disponibles depuis internet)
- La compromission d'un des services publiés peut compromettre l'ensemble de l'unique réseau interne.
- La compromission du parefeu met en danger tout le réseau local

Application du principe DMZ

- Réseaux
  - Zone tampon entre le réseau interne et Internet
  - *"screened subnet" / "sous-réseau filtré"*
  - *"perimeter network«*
- *Des réseaux définis selon le degré de confiance qu'on leur accorde*
  - Réseaux de confiance (trusted)
  - Réseaux non fiables (untrusted)
  - Réseaux partiellement fiables (semi-trusted)

Principe général

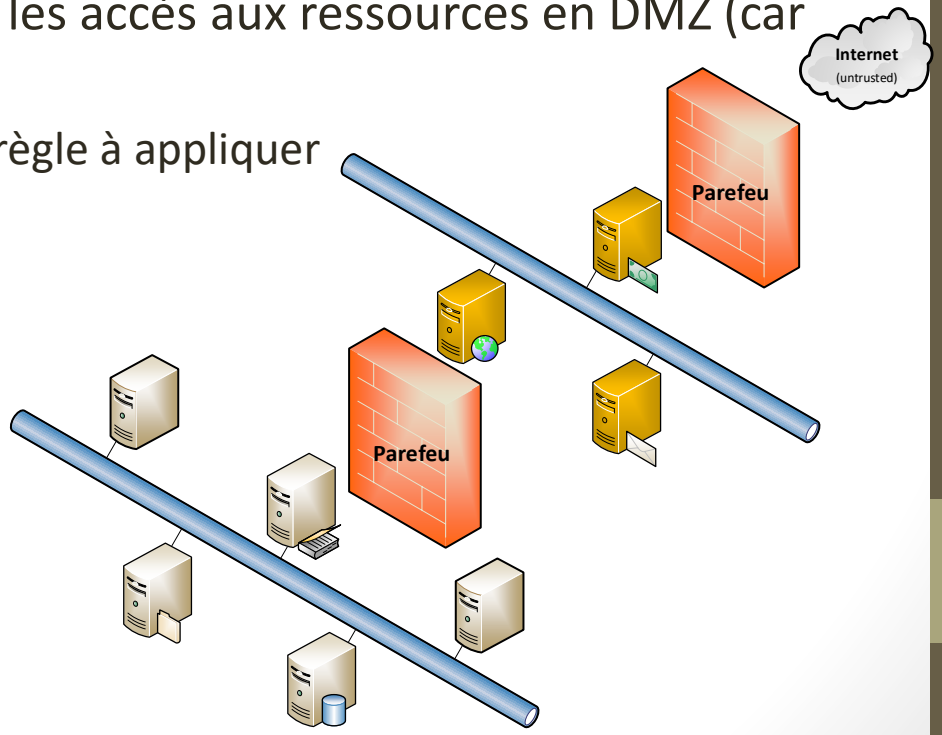
- Qui trouve-t-on dans la DMZ
  - Serveurs qui publient des services vers des réseaux non fiables
    - Messagerie
    - Web
    - E-Commerce
    - …
  - Protection partielle grâce au pare-feu
  - Compromission possible liée à la proximité immédiate d'Internet
- Réseau différents (domaine de diffusion)
- Utilisation de pare-feu en séparation des flux/accès réseau

Plusieurs configurations

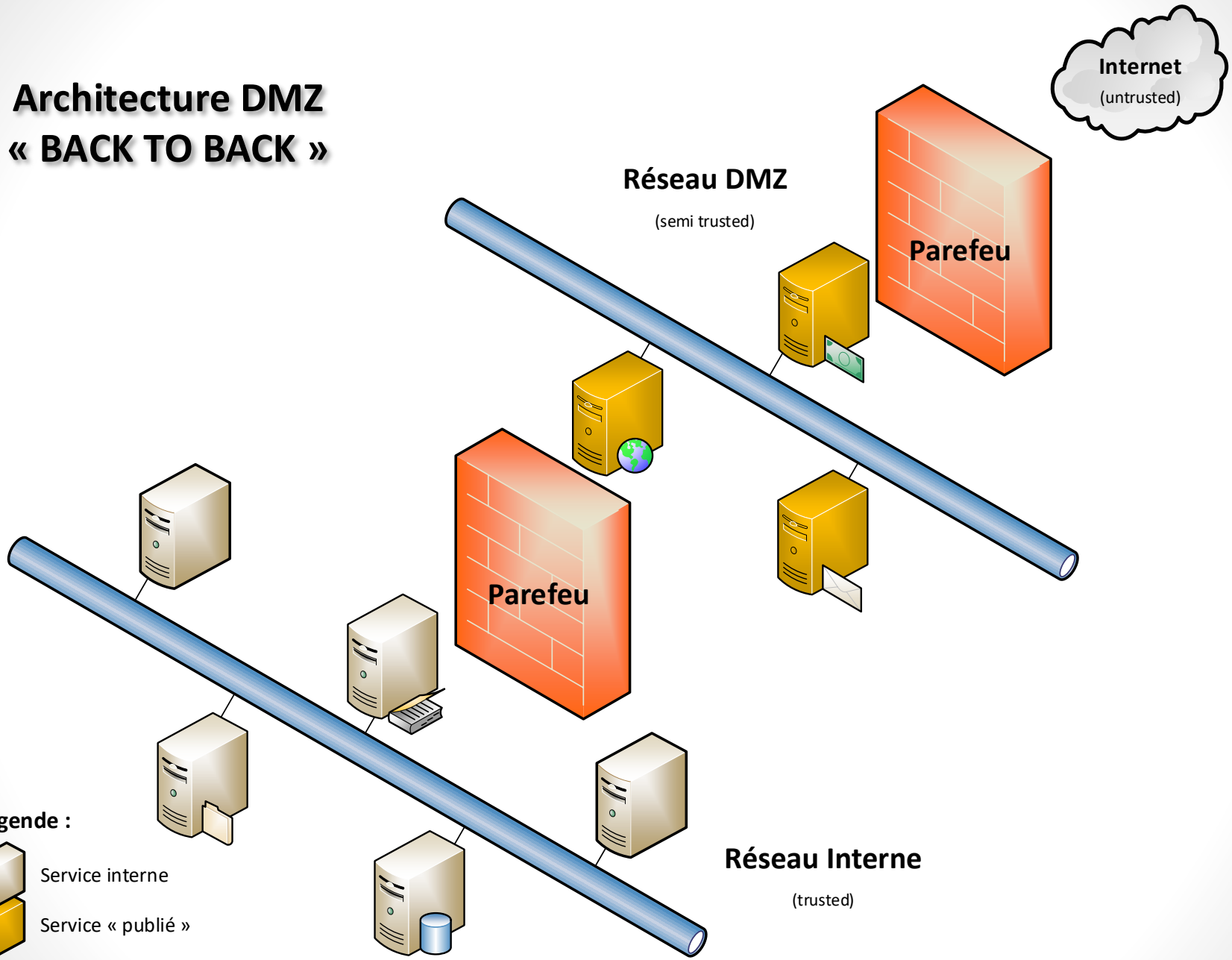
- Back to back DMZ
- Trihomed DMZ

« Back to Back »

- 2 pare-feu indépendants
  - Configuration des pare-feu simplifiée
    - Attention aux règles qui se contrarient ! (autorisé sur l'un, interdit sur l'autre…)
  - Performances accrues pour les accès aux ressources en DMZ (car règles simples)
    - Identification rapide de la règle à appliquer

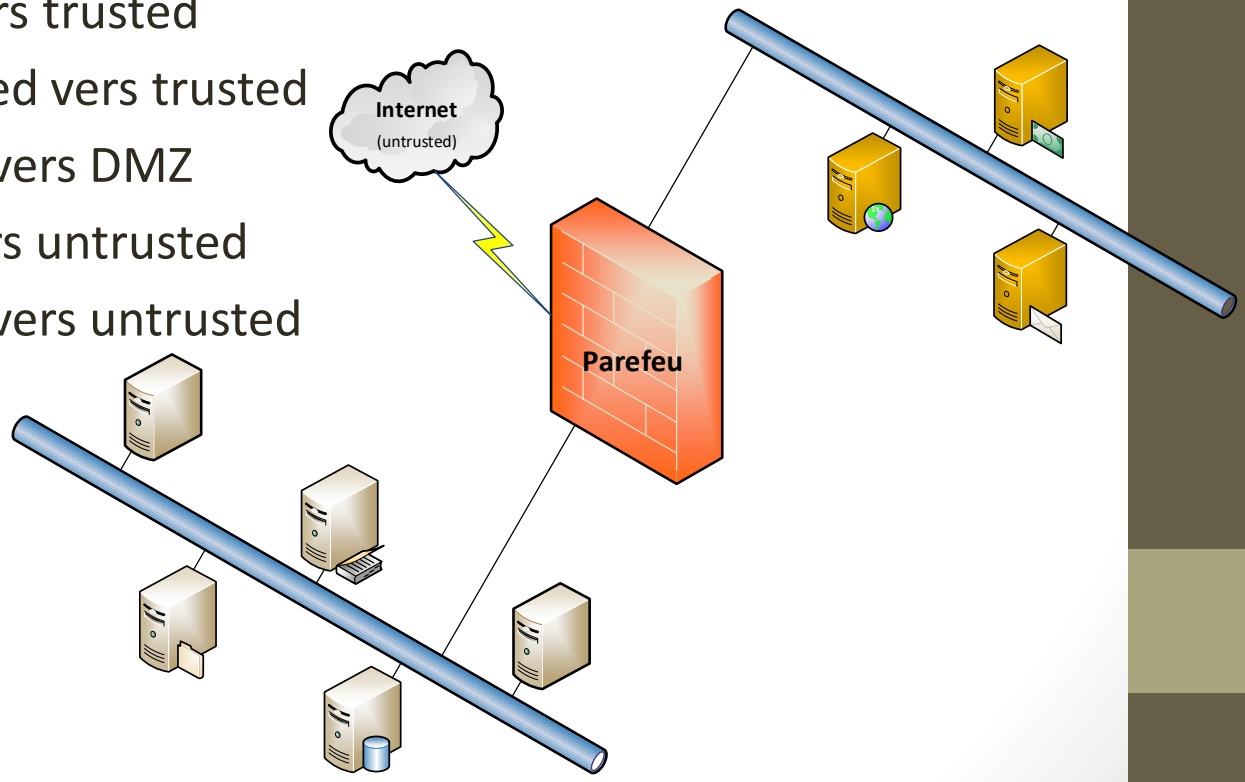


Architecture DMZ « BACK TO BACK »

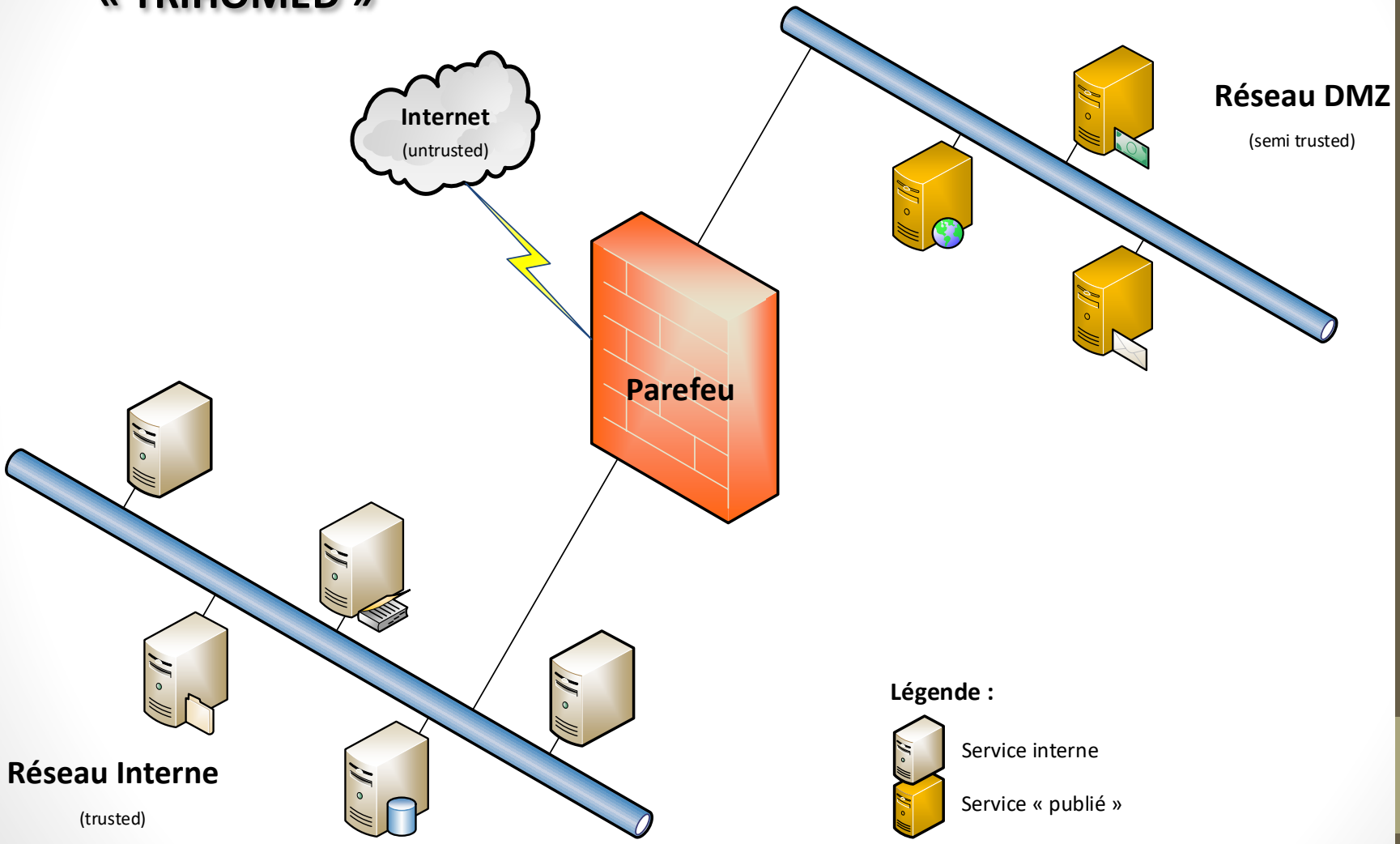


« Trihomed »

- 3 'pattes' trusted / DMZ / untrusted
- 6 règles :
  - incoming : untrusted vers DMZ
  - incoming : DMZ vers trusted
  - incoming : untrusted vers trusted
  - outgoing : trusted vers DMZ
  - outgoing : DMZ vers untrusted
  - outgoing : trusted vers untrusted



Architecture DMZ « TRIHOMED »



« Trihomed »

- La DMZ simplifie les règles de filtrage.
- Evite de définir des règles pour chaque serveur selon qu'il serait accessible depuis l'extérieur ou non…
  - Serait nécessaire si pas de DMZ.

Le pot de miel

- DMZ "Honeynet"
  - Piège à hackers
    - Utilisation de honeypots = **1** serveur avec des VMs et une bonne grosse alarme d'intrusion
    - Objectif = attirer les hackers et les identifier
      - Méthodes d'attaques
      - IP
      - etc.
    - Appliquer les éventuels correctifs sur le réseau réel.

Règles de sécurité

- En DMZ :
  - Stop des services inutiles
  - Services activés avec les privilèges minimums
  - Mots de passe forts
  - Suppression des comptes utilisateurs inutiles
  - Comptes par défaut renommés / déguisés (description, etc.)
  - Mises à jour de sécurité faites
  - Journalisation de sécurité ET lire les journaux fréquemment !

Tendances

- Réseaux complexes
- Plusieurs DMZ
- Encapsulation des zones de confiance à plusieurs niveaux (donc plusieurs pare-feu ?)