Firewall et architectures de sécurité

Centre Réseau Communication

Université Louis Pasteur - Strasbourg

Plan

- Qu'est-ce qu'un firewall ?
- Comment mettre en place un firewall ?
- Technologies de filtrage
- Architectures de sécurité
- Recommandations
- Firewall CRC

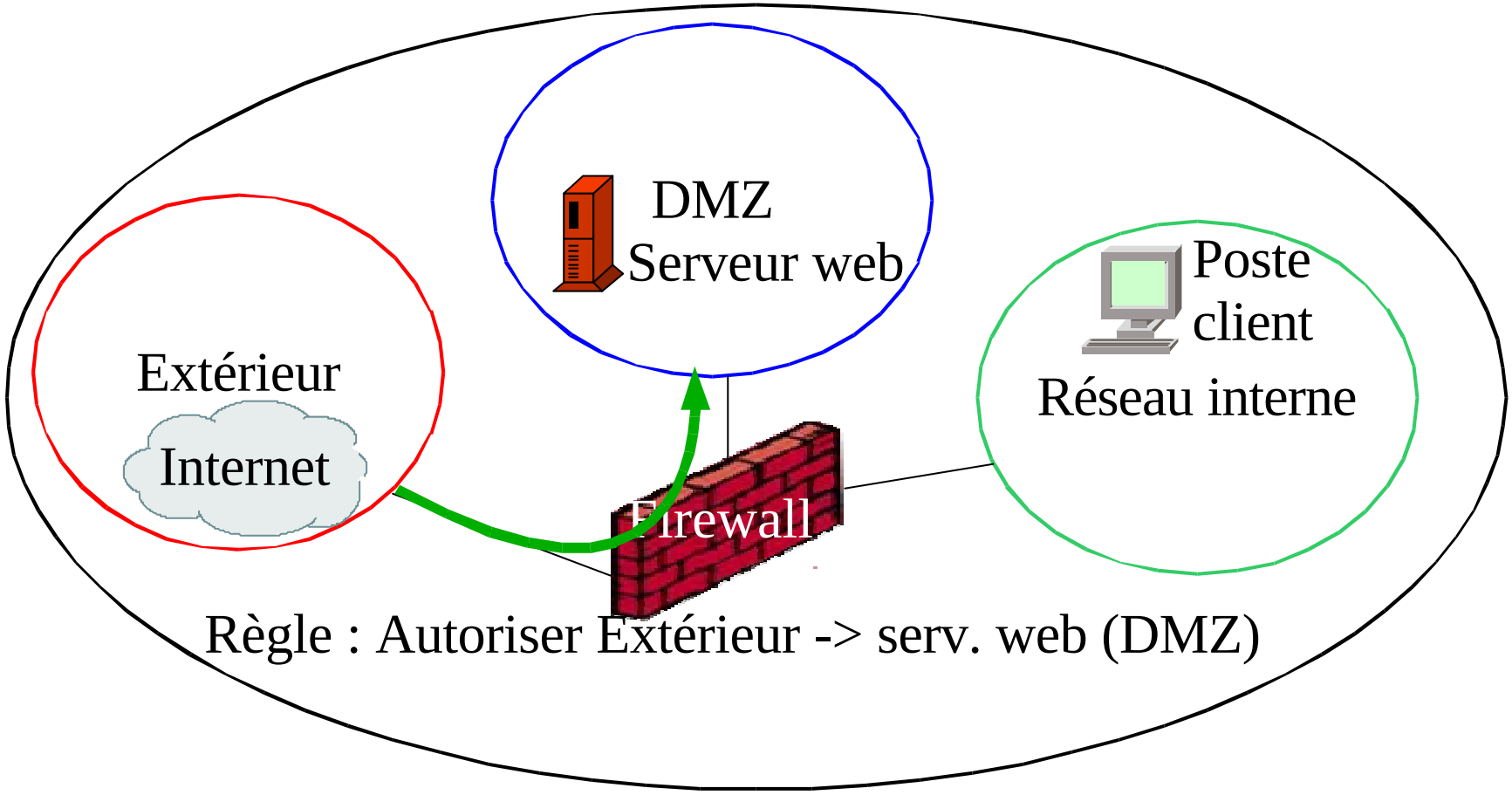
Qu'est-ce qu'un Firewall ? (1/3)

- En français : pare-feu, garde-barrière
- Matériel : ordinateur avec des cartes réseau
- Un dispositif de filtrage des paquets réseau
  - Fonctionne au niveau 3 et 4 (réseau/transport)
  - Plus rarement au niveau 7 (application)
  - => “Intelligence” limitée
- Au centre d'une architecture de réseau sécurisé
- Ce n'est qu'**un** élément de la politique de sécurité

Qu'est-ce qu'un firewall ? (2/3)
Architecture réseau sécurisé

- Firewall au centre du réseau
- Partitionnement du réseau en plusieurs zones
  - Interne, Extérieur, Zone Démilitarisée (DMZ)
- Sécurité d'une zone définie par rapport aux autres
- Règles de filtrage

Qu'est-ce qu'un firewall ? (3/3)
Architecture réseau sécurisée



Ce qu'un Firewall N'EST PAS

- Ça ne se limite pas à l'installation d'une boîte : la sécurité est une **démarche globale**
- Le firewall **n'est pas** la solution définitive à tous les problèmes : la sécurité est un processus constant

Comment mettre en place un firewall ? (1/3)

- Implication de la direction dans le projet
- Communication à destination des utilisateurs
- Analyse de l'existant :
  - Architecture réseau et système
  - Applications : protocoles, ports utilisés,
  - Populations concernées
  - Evaluer les risques
- Cerner les contraintes
  - Evolutions envisagées du réseau, des applications...
  - Moyens matériels et humain
  - Temps

Comment mettre en place un firewall ? (2/3)

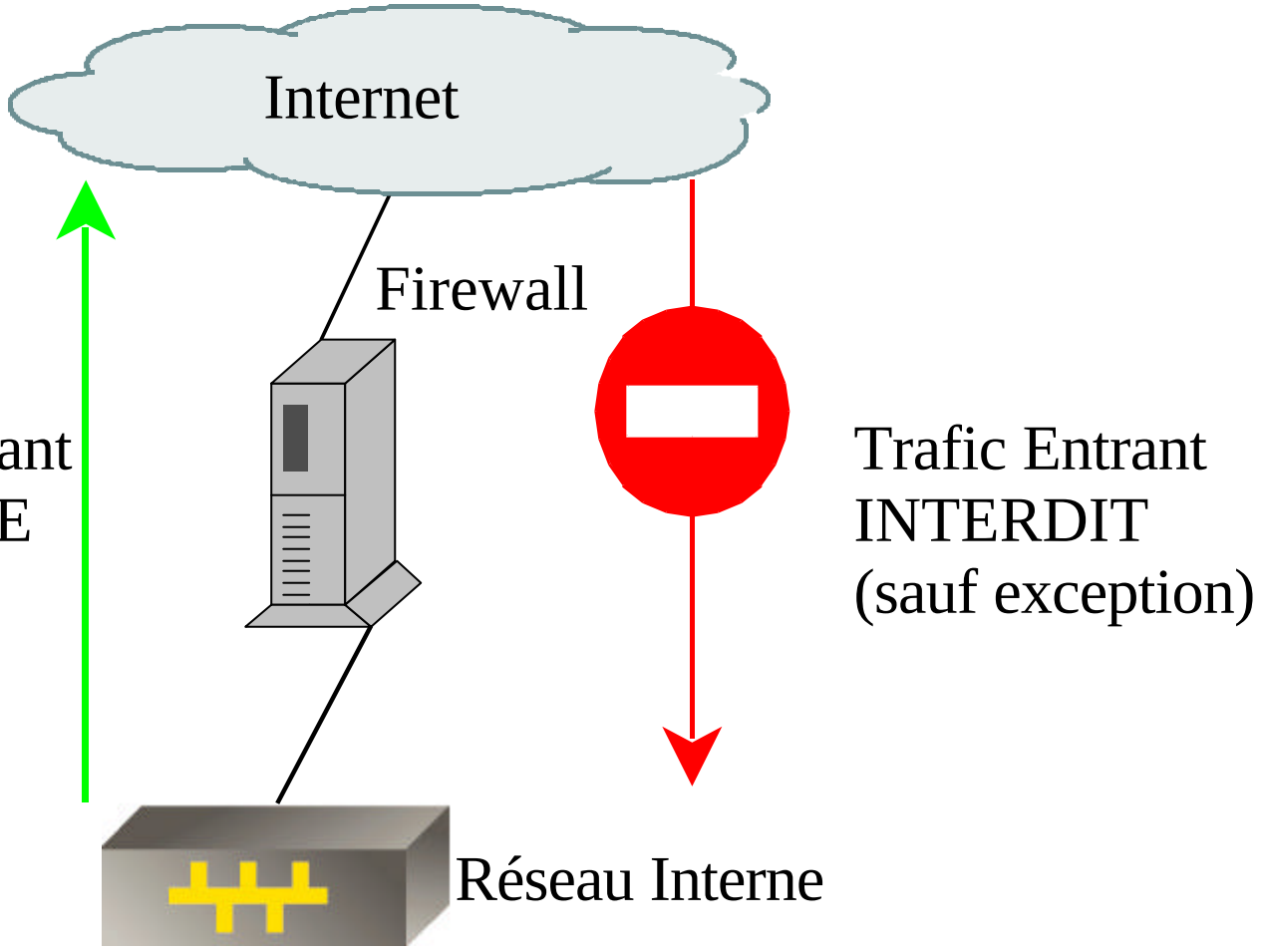
- Définir les zones
  - Regrouper les ordinateurs :
    - par population,
    - par application
  - Définir le niveau de sécurité requis pour chaque zone
  - Définir les relations de confiances entre chaque zone
- Matrice de flux
- Rédaction des règles
- Faire des choix :
  - Remettre en question certaines habitudes
  - Modification de certaines applications

Comment mettre en place un firewall ? (3/3)

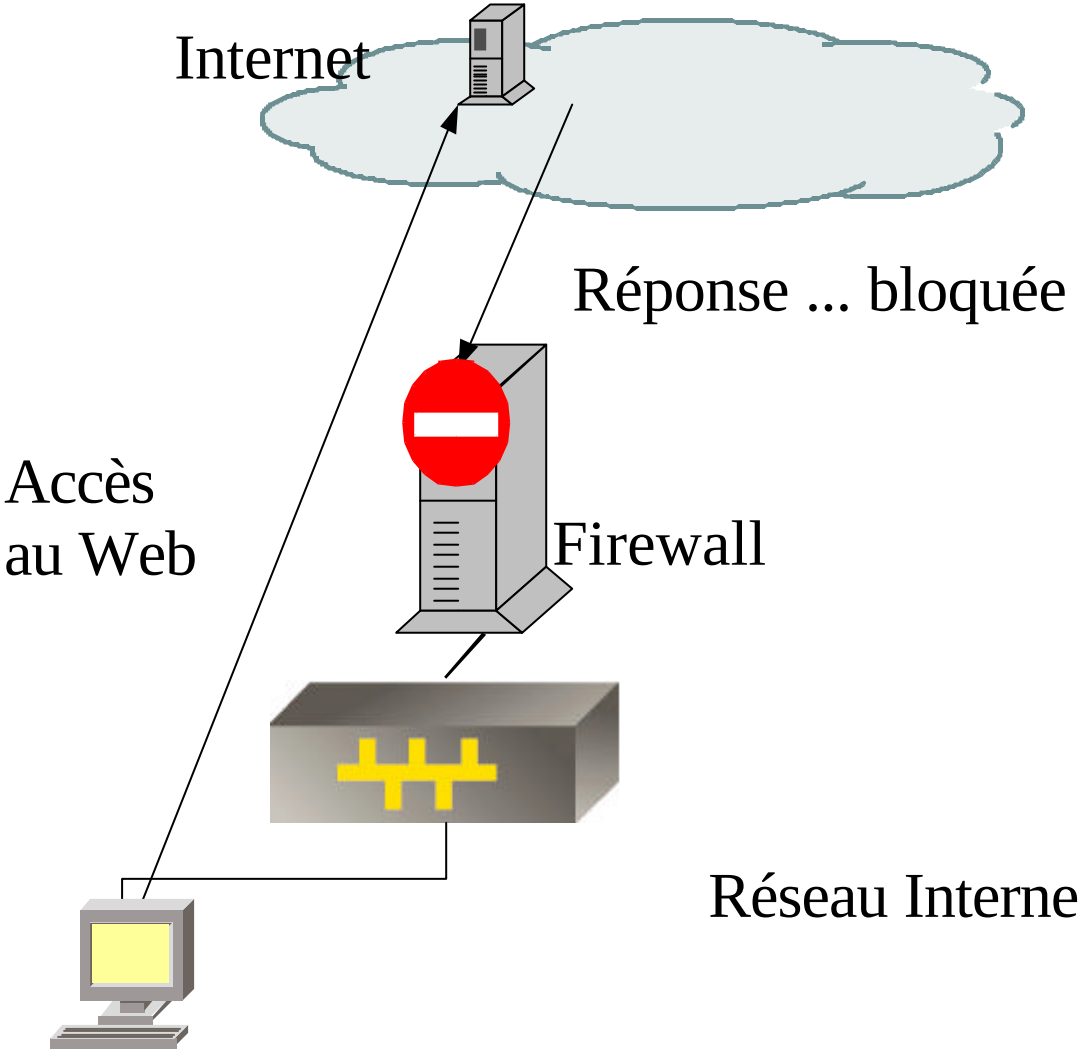
- Définir les rôles techniques et politiques
  - Responsable de l'exploitation quotidienne
    - Maintenance matérielle et logicielle ?
    - Gestion des logs éventuelle
  - Qui est responsible de la MAJ des règles ?
- Formation des administrateurs
- Communication
- Mise en place
- Validations
  - Fonctionnement des applications
  - Conformité à la politique

Rappel : filtrage à état/sans état

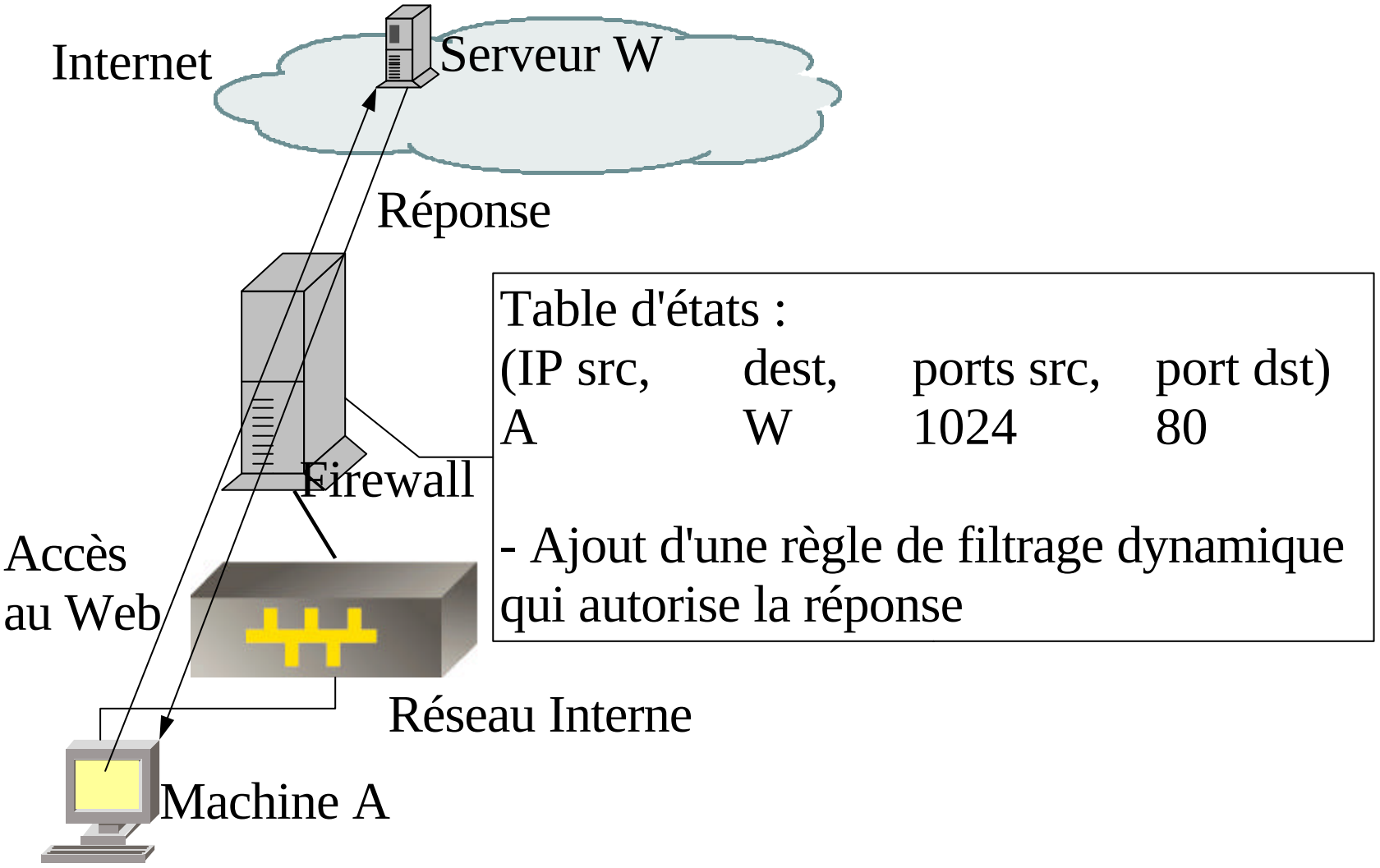
Une politique de sécurité par défaut :



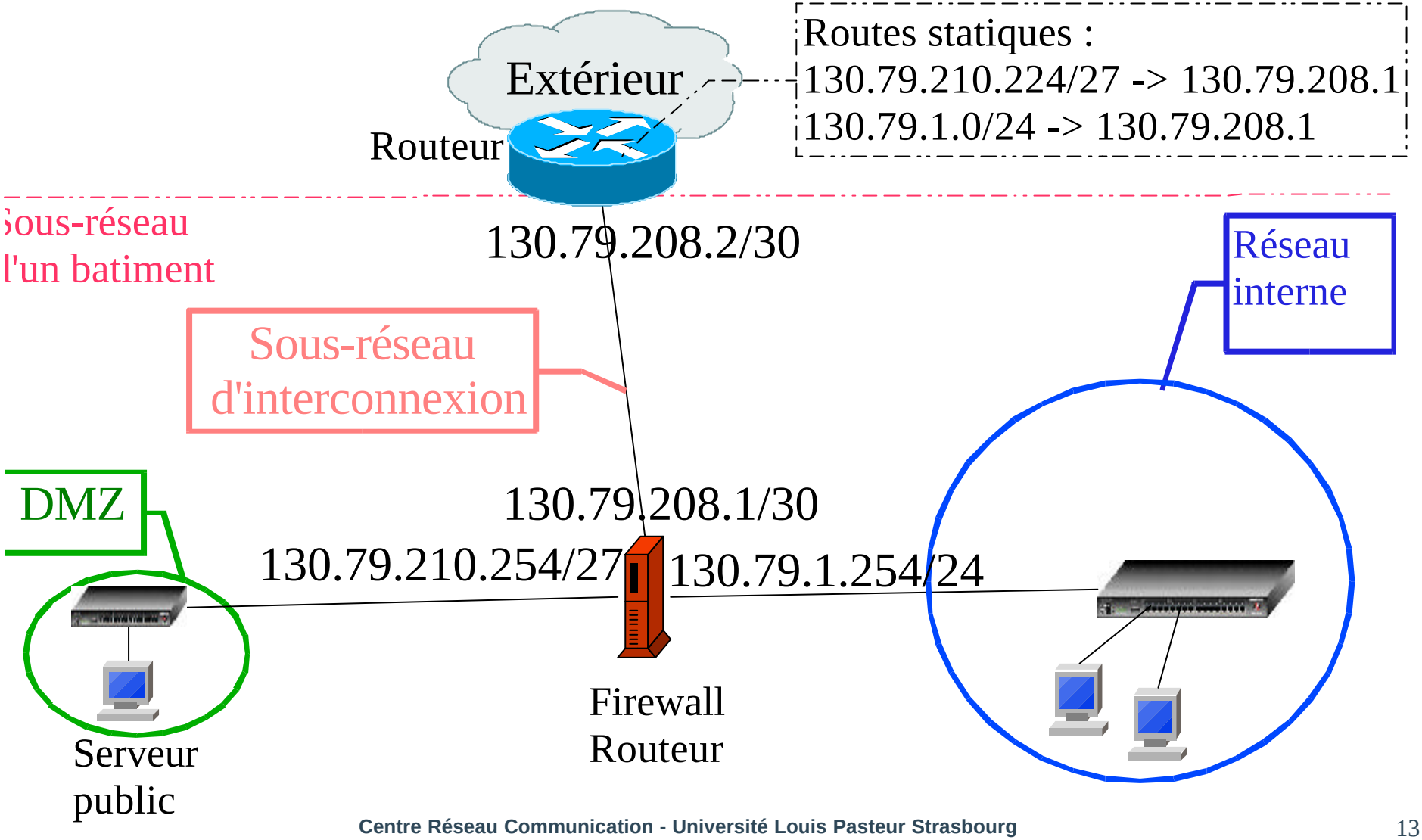
Problème du filtrage sans état



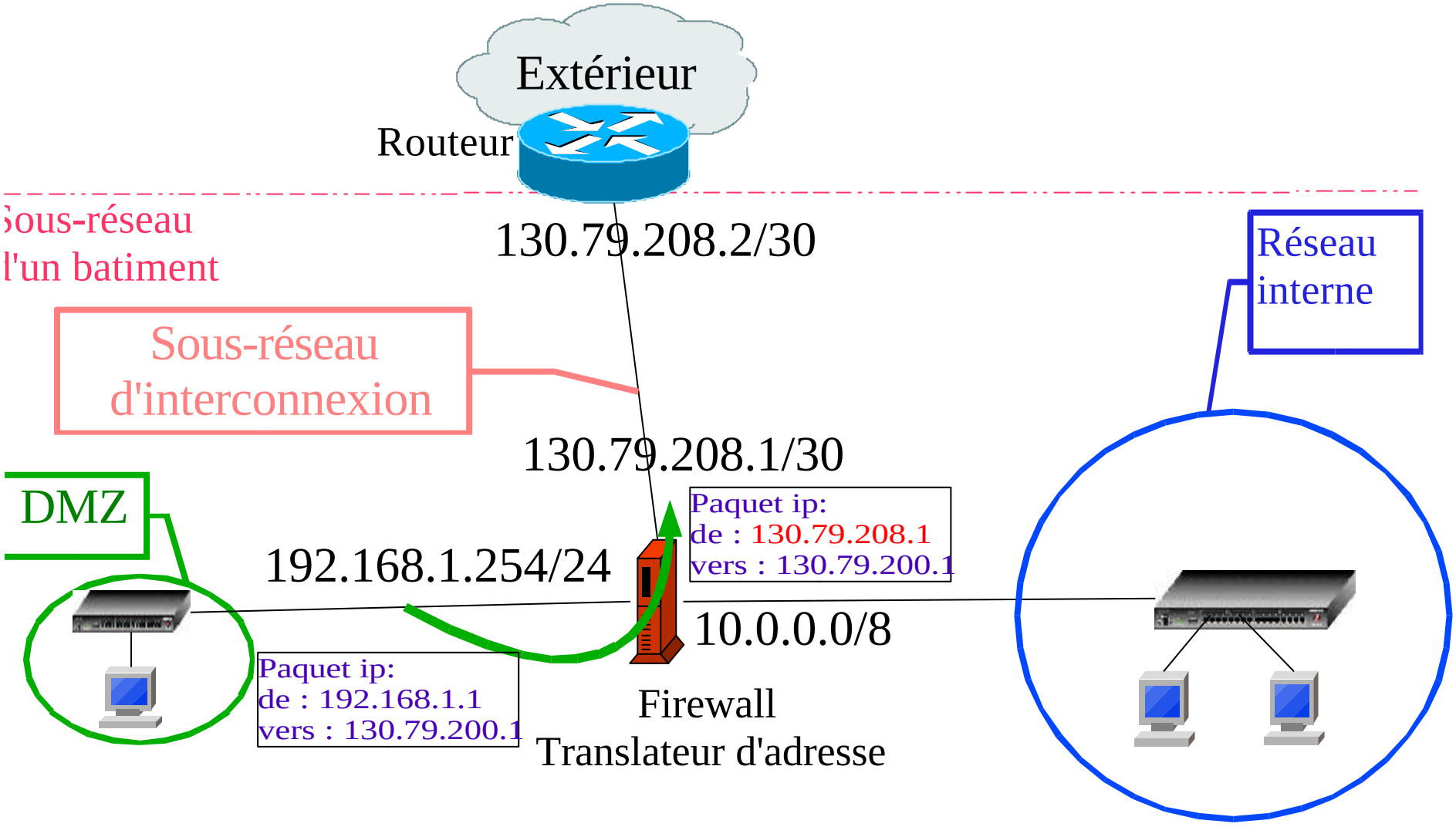
Filtrage avec état



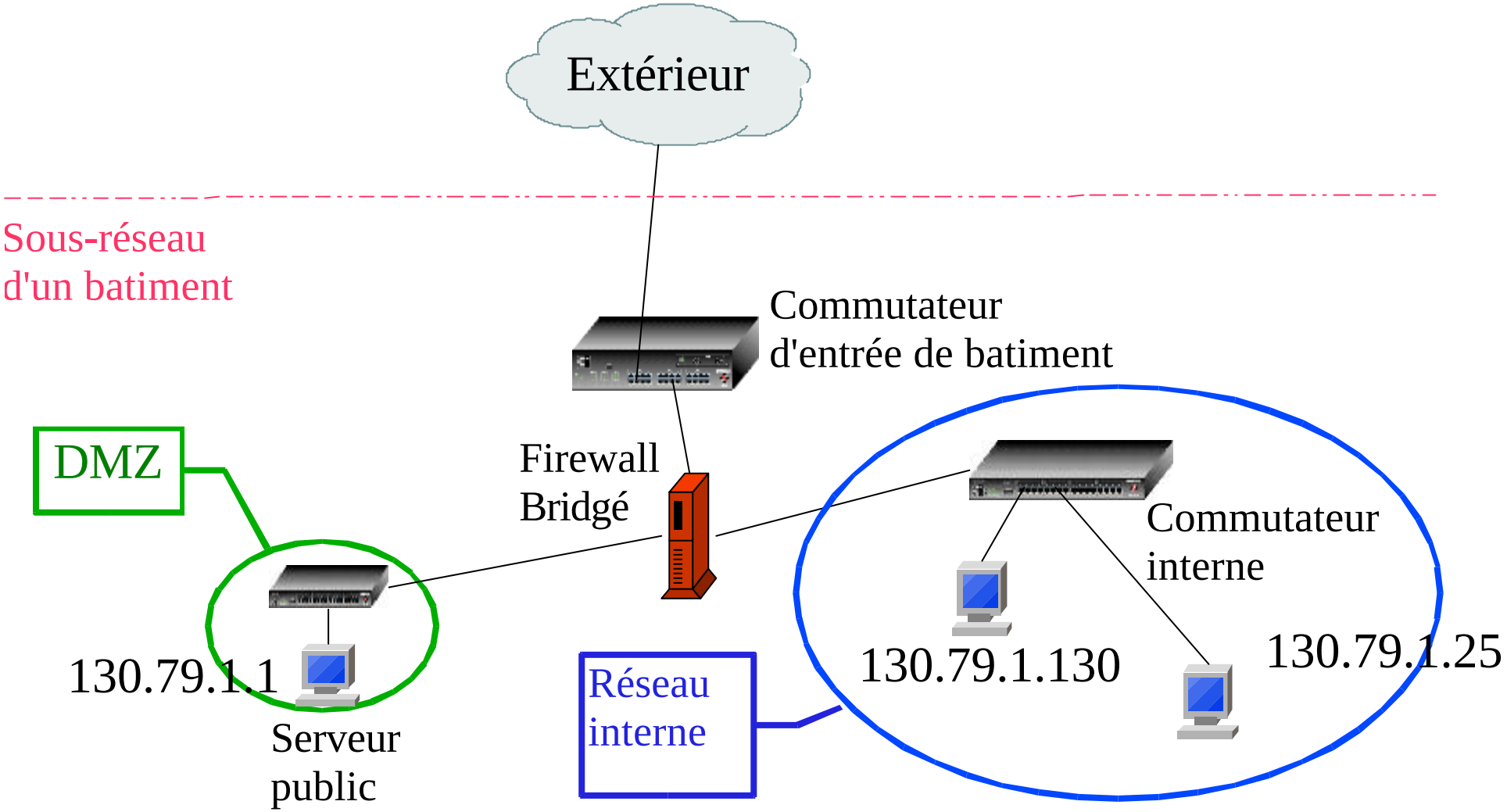
Architectures : Firewall routé (1/3)



Architectures : NAT (2/3)



Architectures : Pont filtrant (3/3)



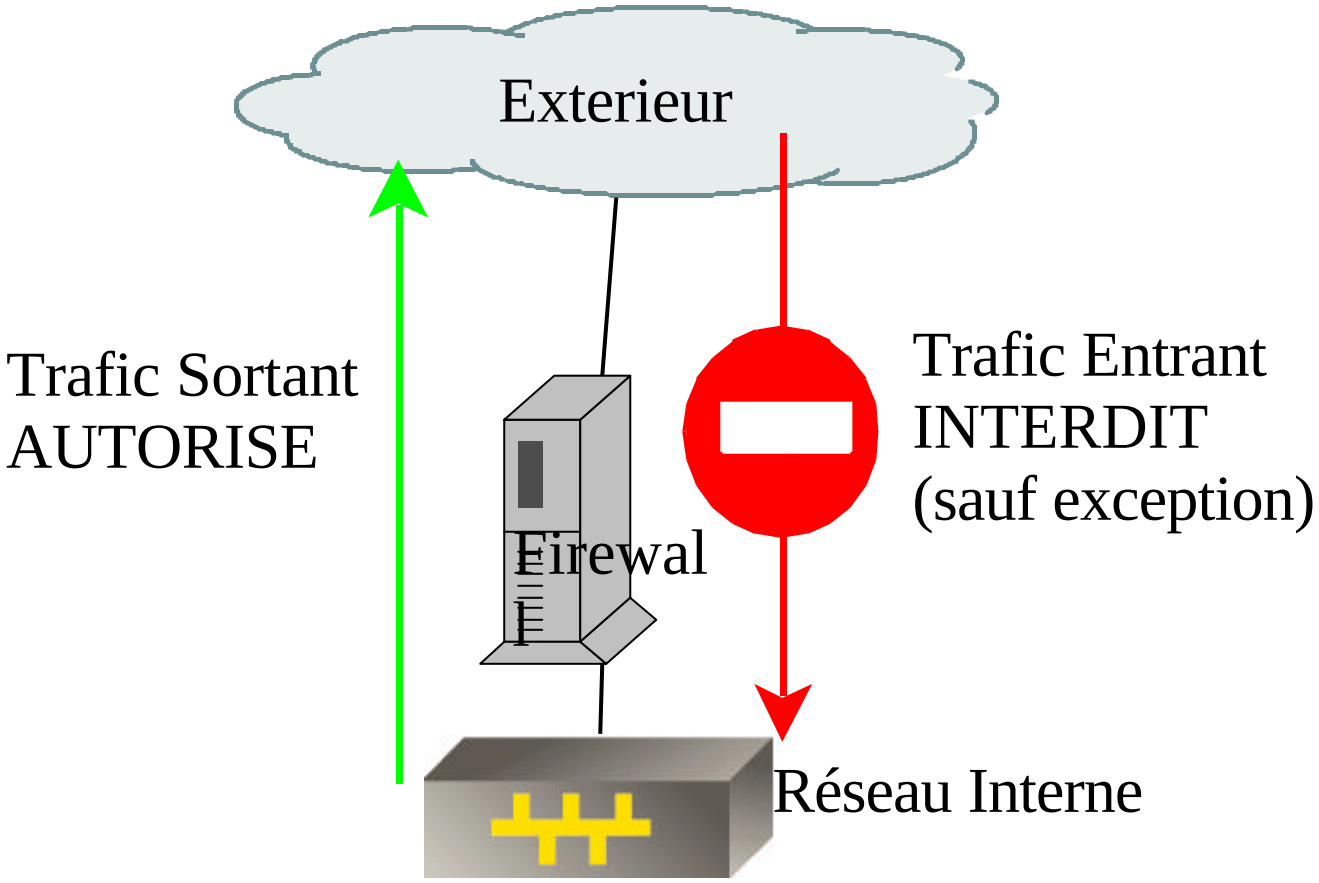
Recommandations

- Politique par défaut :
  - interdire tout accès de l'extérieur vers le réseau interne
- Firewall bridgé : solution transparente
- Créer une DMZ
- Accès depuis l'extérieur :
  - Limités au strict nécessaire : serveurs public
  - VPN pour les utilisateurs nomades

Firewall CRC (1/4)

- Technologie :
  - Firewall Bridge
  - CD bootable
  - Linux Debian Woody, noyau 2.4 + Netfilter Bridge patch
  - Interface texte (Dialog)
- Téléchargeable sur :
  - http://www-crc.u-strasbg.fr/securite/fwcrc/

Firewall CRC : Politique de sécurité par défaut (2/4)



Firewall CRC : interface (3/4)

Firewall CRC : évolutions (4/4)

- Interface WEB
- Filtrage avancé couplé à une base de donnée d'objets
- Gestion des logs (syslog)
- Support de plus de deux interfaces