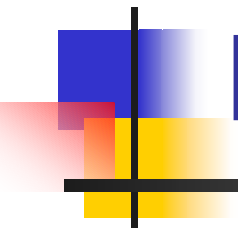


Pare-Feu à l'IPCMS

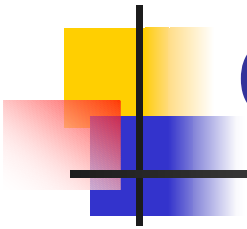
Fabien Muller

présentation au séminaire informatique du 3 juin

Pourquoi ?

Le choix du « tout ouvert » n'est plus pertinent

- Systèmes trop nombreux, ouverts par défaut, avec des bogues
- Administrateurs trop peu nombreux
- Impossibilité de sécuriser chaque poste

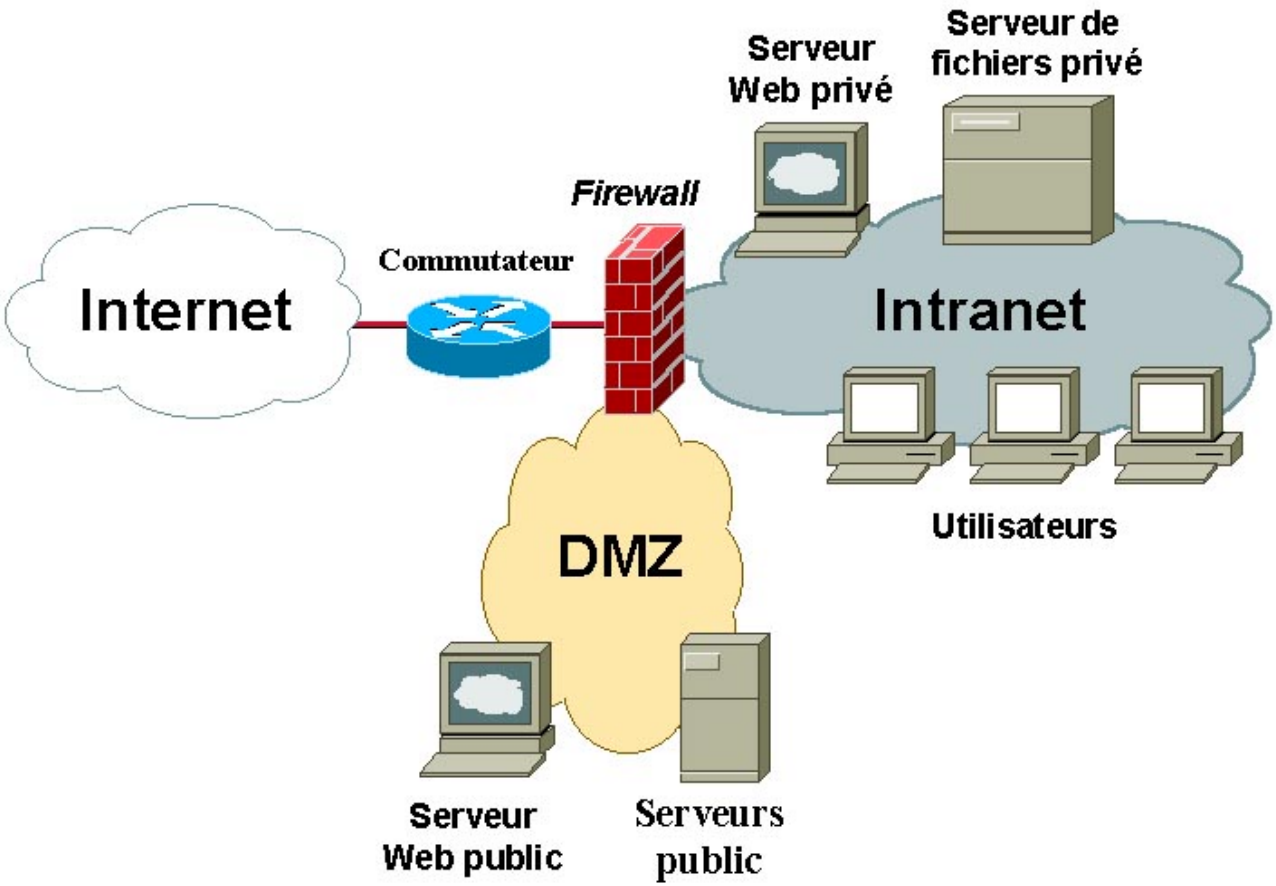


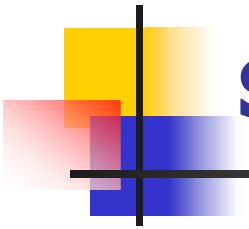
Comment ?

Par filtrage des flux de données

- Limiter les communications entre l'extérieur et l'intérieur
- Restreindre le nombre de machines à configurer, mettre à jour et surveiller
- Mise en place d'une zone démilitarisée

Architecture retenue





solution retenue

le Pare-Feu inclus dans linux

- Solution du domaine public
- Système ouvert
- Evolution aisée
- Coût faible

principe du pare-feu Linux

- Netfilter

  module de filtrage intégré directement dans le noyau permettant d'effectuer du : *filtrage de paquets, des opérations de translation d'adresses, des opérations de marquage de paquets*

- Iptables

  Commande permettant de configurer les règles

Fonctionnalités de filtrage

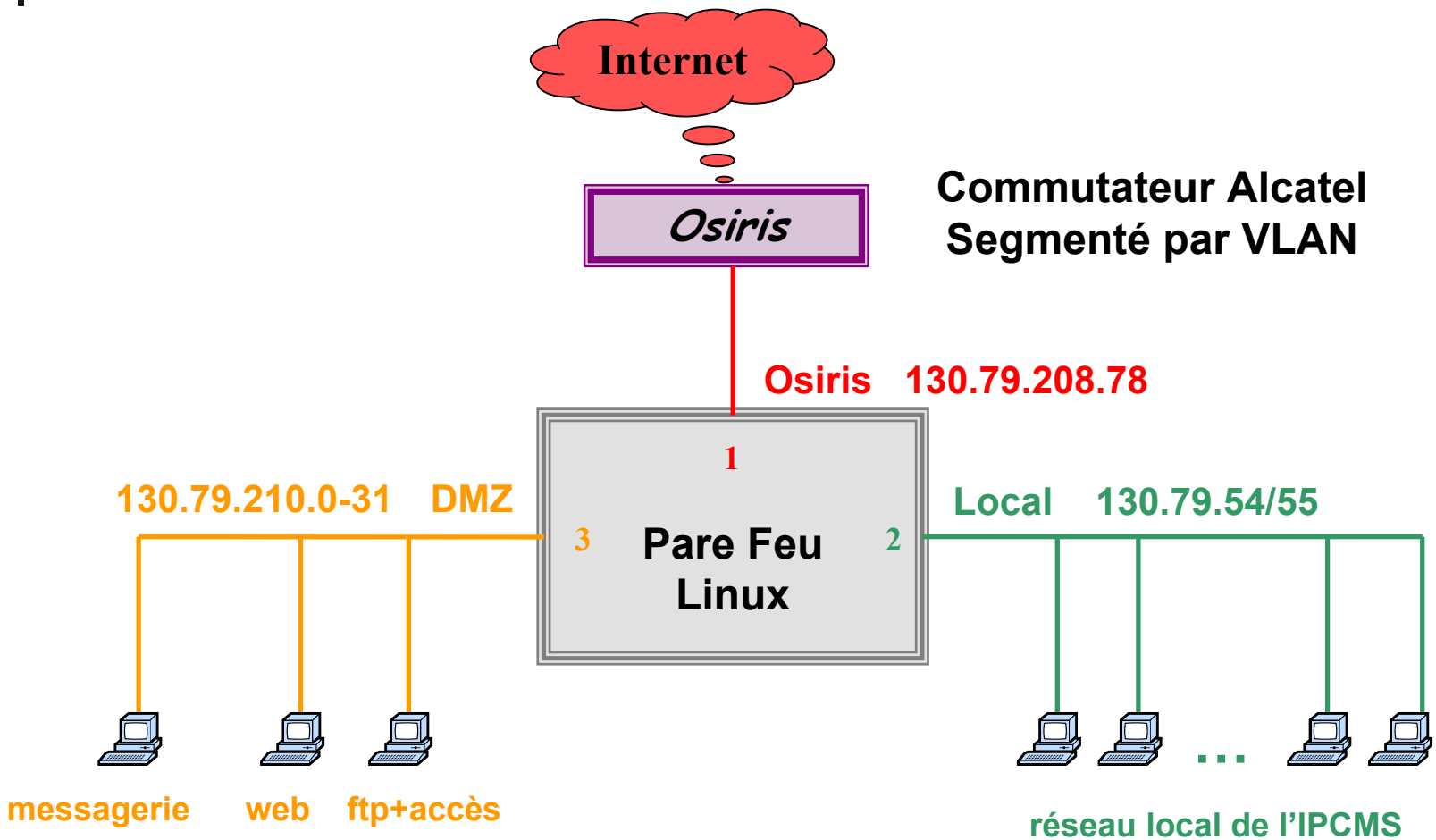
- Filtrage

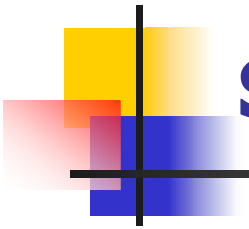
  de paquets mal formés ou standard, par port, interface, protocole, adresses MAC, VLAN

  des drapeaux TCP : SYN, ACK, FIN, URG, RST, PSH

  des anomalies de connexions
- Suivi de connexion (stateful inspection)
- Traçage étendu des logs
- Limitation des tentatives de deny de service

schéma structurel





spécifications matérielles

- 2 serveurs IU de transtec (un spare)
- processeur : Intel pentium III à 1 GHZ
- mémoire : 512 Mo
- disque dur : 2 x 18 Go mirroré
- 3 interfaces 100Mbits/sec
- Garantie avec intervention sous 4 H

matrice des flux de l'IPCMS

ens du filtrage	Réseau local	Internet	DMZ
Réseau local		Pas de filtrage	Web (http) connexion cryptée (ssh) Messagerie : (pop, imap, smtp,https) Sauvegarde (tina) ftp anonyme
Internet	accès interdit		Web (http) connexion cryptée (ssh) messagerie (smtp, https) ftp anonyme
DMZ	connexion cryptée	web connexion cryptée Messagerie (smtp Osiris)	

Gestion des logs

- **detescan** : outil d'analyse

  Routeurs/commutateurs (Cisco, Foundry Networks, Allied Telesyn, etc.)

  Firewalls logiciels (Linux ipchains et iptables)
- **Script perl** : développé par le LORIA
- **Disponible sur le serveur de l'UREC** :

  http://www.urec.cnrs.fr/securite/outils/destescan.html

Gestion des logs

- **Actions** :

  Comptabilisation des paquets refusés par port et machine

  Production d'un rapport de synthèse avec en tête le résumé de toutes les intrusions détectées et à la suite, le détail des scans

- **Utilisation** :

  Exécution quotidienne par la crontab

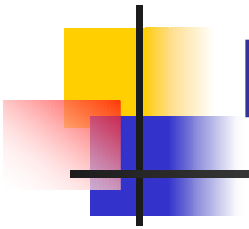
  Transmission des rapports à :

  certscan@renater.fr et Jean.Benoit@crc.u-strasbg.fr

Bilan

- Solution en service depuis 18 mois
- bon niveau de sécurité
- performances réseau maintenues
- insertion facile à l'existant
- règles de sécurité acceptées par les utilisateurs
- Rejet de centaines de tentatives journalièrement
- Gestion efficace des logs
- remise en état dans l'heure en cas de panne

… pour un coût financier de 4000 €



Bilan

- **Cependant** :

  Améliorer le suivi des incidents

  La syntaxe de iptables est complexe mais la configuration peut être facilitée en utilisant l'outil graphique fwbuilder

  Ne dispense pas de protéger les machines :

  - mise à jour des systèmes
  - installation des patchs de sécurités
  - filtrage locale (tcp-wrapper)