Virtualisation des réseaux IP retour d'expérience

JRES de Toulouse

Vendredi 25 novembre 2011

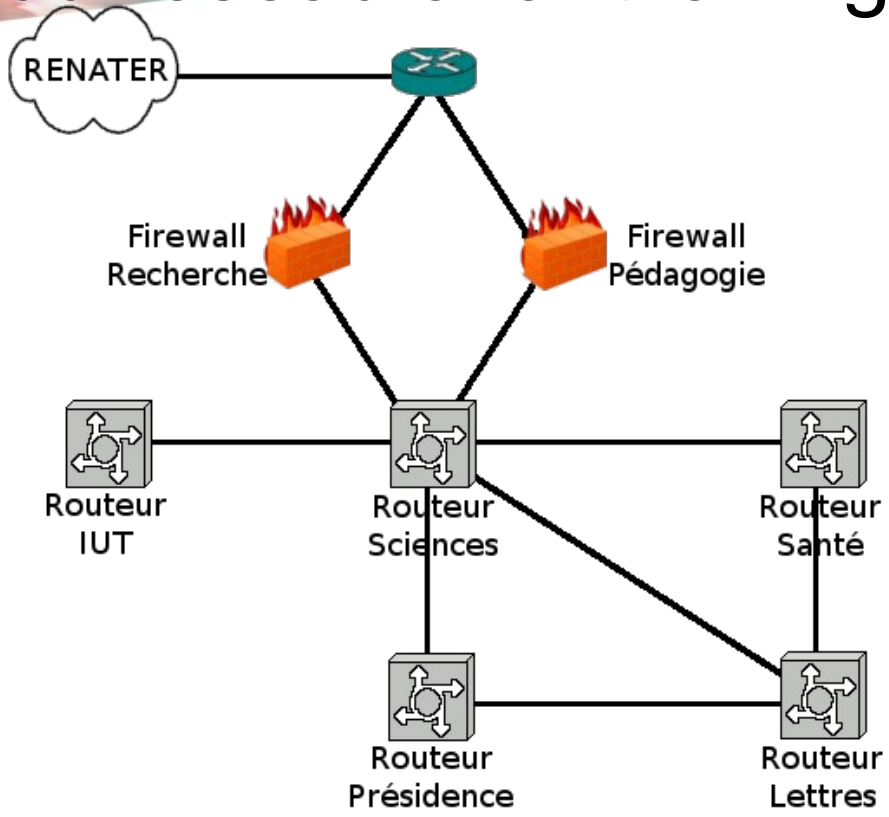
Université de Reims Champagne-Ardenne

Contexte du projet

- De nombreux équipements obsolètes
- Le système de pare-feu particulièrement bloquant
- Congestion dans le réseau

- En novembre 2006, nous avons lancé un appel d'offre pour renouveler ces appareils

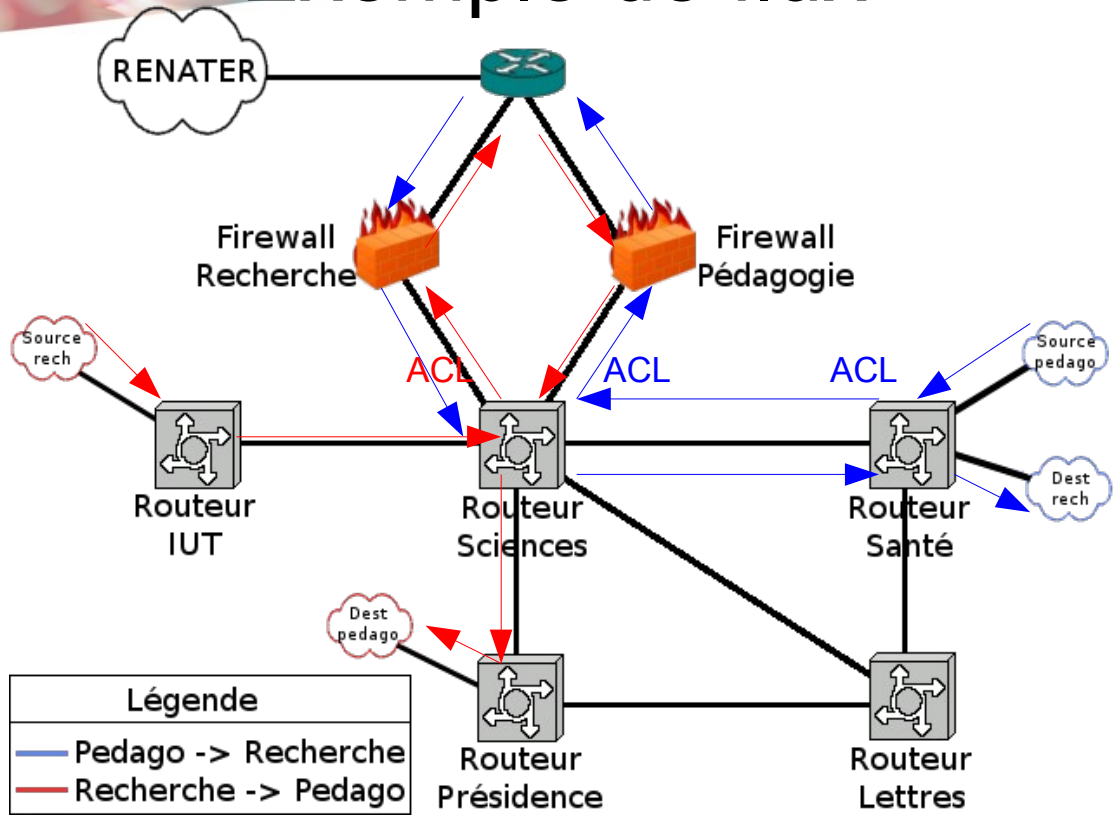
État du réseau avant la migration



Pourquoi deux pare-feu ?

- Isoler les réseaux de recherche des réseaux pédagogiques
- Un pare-feu par type de réseau
- Routage conditionnel (PBR) sur les adresses sources et les adresses destinations dans chacun des routeurs

Exemple de flux



Inconvénients

- Les ACL : une source d'erreur
- Impossibilité de généraliser la méthode pour isoler d'autres réseaux (WIFI par exemple)
- Recherche de panne complexe

La solution retenue : VRF-Lite

- Technologie permettant d'instancier plusieurs tables de routage étanches au sein d'un seul appareil
- Fonctionne sur des routeurs ou des commutateurs niveau 3
- Fonctionne avec tous les routeurs déjà mis en place dans notre réseau

Mise en place technique 1/3

- Les VRF doivent être déclarées :

```
ip vrf WIFI
  rd 123:4
exit
```

  - Le choix du nom de la VRF (WIFI) est important
  - Les rd (route distinguisher) doivent être différents pour chaque VRF

Mise en place technique 2/3

- Nous pouvons maintenant mettre les interfaces niveau 3 dans la VRF

```
interface Vlan2
  ip vrf forwarding WIFI
  ip address 192.168.1.1 255.255.255.0
exit
```

  - Il faut déclarer la VRF de travail (ip vrf forwarding) avant de mettre l'adresse IP

Mise en place technique 3/3

- Routage statique

```
ip route vrf WIFI 0.0.0.0 0.0.0.0 192.168.0.254
```

- Routage dynamique

```
router ospf 6509 vrf WIFI
  redistribute connected subnets
  redistribute static subnets
exit
```

Un cas particulier

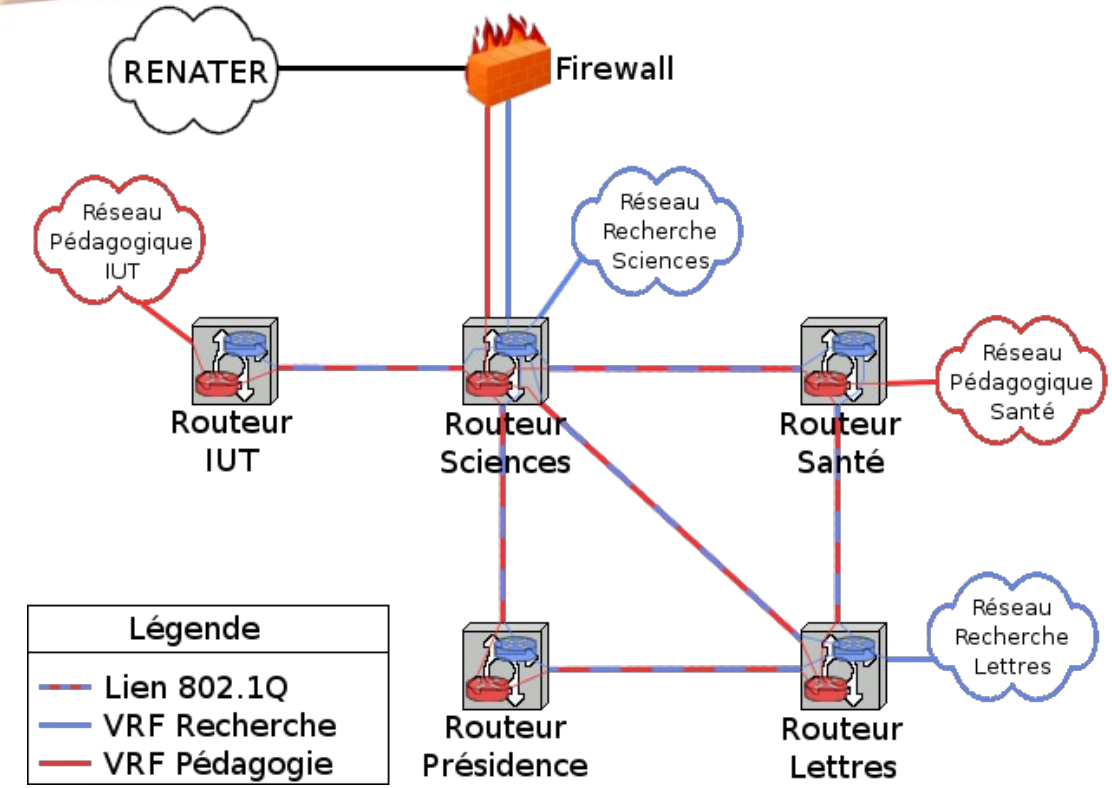
- La table de routage « normale » existe toujours
- On y accède de manière traditionnelle

```
interface Vlan 3
  ip address 192.168.3.254 255.255.255.0
exit
ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

Mise en place à l'URCA

- 1 seul pare-feu disposant de huit interfaces gigabit ethernet
- 6 instances VRF reliées à ce pare-feu (5 à l'origine du projet)
- Conservation des VLAN multi-campus

Schéma simplifié du réseau avec VRF



L'interconnexion des routeurs

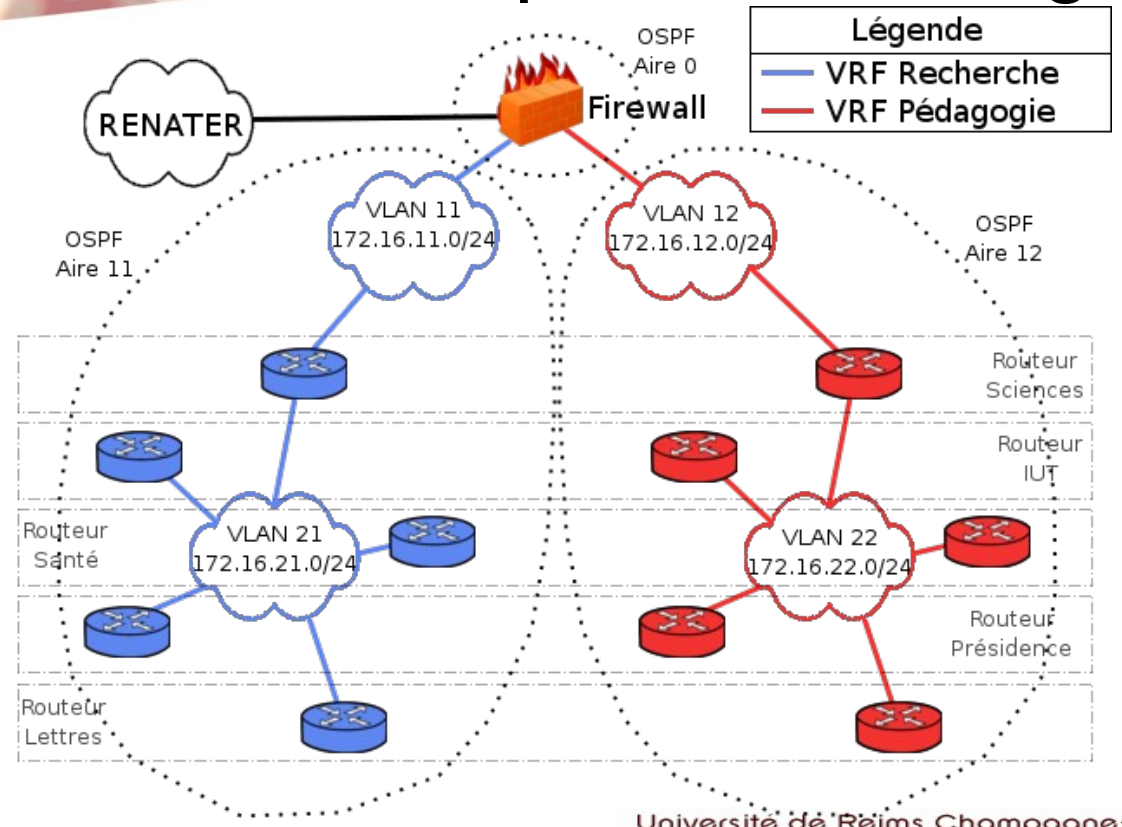
- Les VRF de tous les routeurs sont reliées ensemble par un réseau de classe C dans un VLAN multi-campus

- Ces 6 VLAN transitent entre les machines par un lien 8021.Q

Routage dynamique

- Le routage dynamique se fait par OSPF
- Il y a une instance OSPF distincte par VRF
- Chaque VRF est dans une aire OSPF différente
- Le pare-feu est dans l'aire OSPF 0

Schéma simplifié du routage



Utilisation quotidienne

- VRF transparentes pour les usagers (sortie identique pour traceroute)
- Une petite contrainte pour les administrateurs : ne pas oublier de préciser la VRF de travail

```
traceroute vrf PEDAGOGIE www.renater.fr
show ip route vrf RECHERCHE
```

- L'isolation des réseaux simplifiée : il suffit de mettre le réseau dans la bonne VRF

Sécurité

- Il y a bien une isolation totale entre les VRF
- Dans les routeurs, la CPU travaille dans la VRF par défaut
  - connexion à la machine uniquement sur une interface de celle-ci
  - un utilisateur dans une autre VRF ne peut pas s'y connecter

Évolutions

- Ajout d'une sixième VRF depuis l'installation de base pour sécuriser la TOIP

- Mise en place envisagée pour tous les réseaux métropolitains de la région Champagne-Ardenne

Conclusion

- Technologie fiable : aucune panne déplorée en plus de 4 ans d'exploitation
- Une mise en place un peu délicate, mais une exploitation quotidienne simple
- La flexibilité du système permet de répondre à de nombreuses demandes
- Clarification des règles de sécurité de notre réseau

Merci de votre attention