Virtualisation des réseaux IP : retour d'expérience

Didier Barthe
Centre de Ressources Informatiques, Université Reims Champage-Ardenne
Campus Moulin de la Housse – 51687 Reims Cedex 2

Résumé

Cet article décrit la méthode de sécurisation de l'infrastructure réseau de notre université par la virtualisation du routage et son utilisation au quotidien 4 ans après sa mise en place.

Notre volonté était de séparer complètement les réseaux utilisés par les personnels, les étudiants (salles libre service, salle de TP, etc …) et les réseaux WIFI. Après une analyse de l'état de l'art, nous avons opté pour la technologie VRF-Lite (VP Routing and Forwarding), disponible sur de nombreux routeurs et commutateurs niveau 3 du constructeur CISCO.

Cette technologie permet de mettre en place au sein d'un même routeur différentes tables de routages étanches les unes par rapport aux autres. Il n'y a plus ensuite qu'à déployer nos différents réseaux au sein de ces tables de routage étanches.

Après une explication approfondie du fonctionnement du système VRF-Lite, nous verrons l'architecture qui a été déployée au sein de notre université. Enfin, nous détaillerons l'utilisation quotidienne de cette technologie ainsi que les évolutions effectuées depuis sa mise en place et celles envisagées dans l'avenir.

Mots clefs

Virtualisation, Sécurité, Routage dynamique, pare-feu, VLAN

1 Introduction

En novembre 2006, nous avons lancé un appel d'offres pour changer le pare-feu d'entrée du réseau de notre université (université composée de 14 campus dans 5 villes de la région Champagne-Ardenne). Outre l'augmentation de la puissance de traitement, nous voulions isoler complètement trois types de réseaux : ceux utilisés par le personnel, par les étudiants et les réseaux WIFI.

Cette opération ne pouvait pas se faire sans modifier radicalement notre architecture réseau. Nous avons décidé de conserver un routeur par campus avec pour tâche le routage des réseaux utilisés localement.

Pour isoler au mieux ces différents réseaux, la solution traditionnelle serait d'avoir sur chaque campus un routeur différent pour chacun des types de réseaux que l'on souhaite isoler. Au jour d'aujourd'hui, la virtualisation de ces routeurs permets d'obtenir le même résultat.

Le constructeur CISCO nous a proposé une solution qui nous permettait d'atteindre ce but sans changer les actifs réseaux déjà en place : les VRF-Lite (VPN routing and forwarding).

2 Fonctionnement des VRF

2.1 Fonctionnement général

Les VRF-Lite permettent d'instancier au sein d'un seul routeur (ou commutateur niveau 3) plusieurs tables de routage étanches. On associe également à ces VRF des « tables de forwarding hardware » qui assurent un routage rapide (exactement comme dans un routeur classique), des interfaces niveau 3 du modèle OSI (IP) et des processus de routage.

L'interconnexion des différents équipements utilisant les VRF se fait au niveau 3 du modèle OSI. Afin d'assurer une étanchéité totale des flux, il est possible d'utiliser une liaison dédiée ou des VLAN. Dans ce dernier cas, les flux de chaque VRF transiteront au travers d'un VLAN spécifique. La connexion entre les équipements se fera alors par un lien 802.1Q.

Pour permettre la communication entre les réseaux des différentes VRF, deux solutions sont proposées.

La première solution est la possibilité de les faire communiquer au sein du même équipement par un processus mBGP et des règles d'import/export de routes. La deuxième est de faire transiter les flux par un routeur ou un pare-feu. Dans ce deuxième cas, chaque VRF est reliée à une entrée du pare-feu. C'est cette solution qui répondait le mieux à nos besoins en terme de sécurité.

2.2 Étude technique

La création de réseaux isolés se fait en deux étapes. La création d'un contexte de routage puis la création des réseaux dans ce contexte de routage.

Voici les commandes minimum pour créer la VRF WIFI :

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

Il existe aussi des commandes pour gérer des route-map, l'import/export dans le cadre de mBGP, une description, etc. qui ne seront pas détaillées ici.

Dans cet exemple, WIFI est le nom de notre VRF, il faudra l'utiliser dans toutes les commandes y faisant référence (attention à la casse).

123:4 est nommé le « route distinguisher » (RD). Dans les documentations constructeur [1], il est indiqué de préciser soit un numéro d'AS et un nombre arbitraire, soit une adresse IP et un nombre arbitraire. Dans la pratique, il suffit que les RD des VRF soient différents.

Une fois la VRF créée, on peut y placer des interfaces de niveau 3. Par exemple :

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

Il est essentiel que la commande « ip vrf forwarding » soit passée avant la commande « ip address ». Au moment où une interface est mise dans une VRF (ou en cas de changement de VRF), elle perd son adresse IP. En effet, on peut avoir la même adresse IP sur des interfaces différentes si elles sont dans des VRF différentes. Lors d'un changement de VRF le système désactive donc l'adresse IP pour éviter un doublon.

L'exemple est fait avec une interface VLAN mais cela fonctionne de la même façon avec des interfaces physiques.

Nous pouvons également ajouter des réseaux distants à l'aide d'un routage statique. Il faudra une fois encore préciser la VRF de travail.

```
ip route vrf WIFI 0.0.0.0 0.0.0.0 192.168.0.254
ip route vrf WIFI 172.16.0.0 255.255.0.0 192.168.0.253
```

2.3 Un cas très particulier

La création d'une VRF revient à ajouter une nouvelle table de routage dans le système, sans pour autant détruire les précédentes. Il y a donc toujours au sein de notre routeur la table de routage normal d'un routeur sans VRF. L'accès à cette table se fait de manière naturelle sans préciser la VRF (création d'interface ou routage statique). Il faut par conséquent être vigilant lors de la modification (ou l'analyse) d'une VRF et ne pas oublier l'élément de commande « vrf *nom_vrf* » sous peine de modifier involontairement la table de routage principale.

3 Mise en place à l'URCA

3.1 État du réseau avant la migration

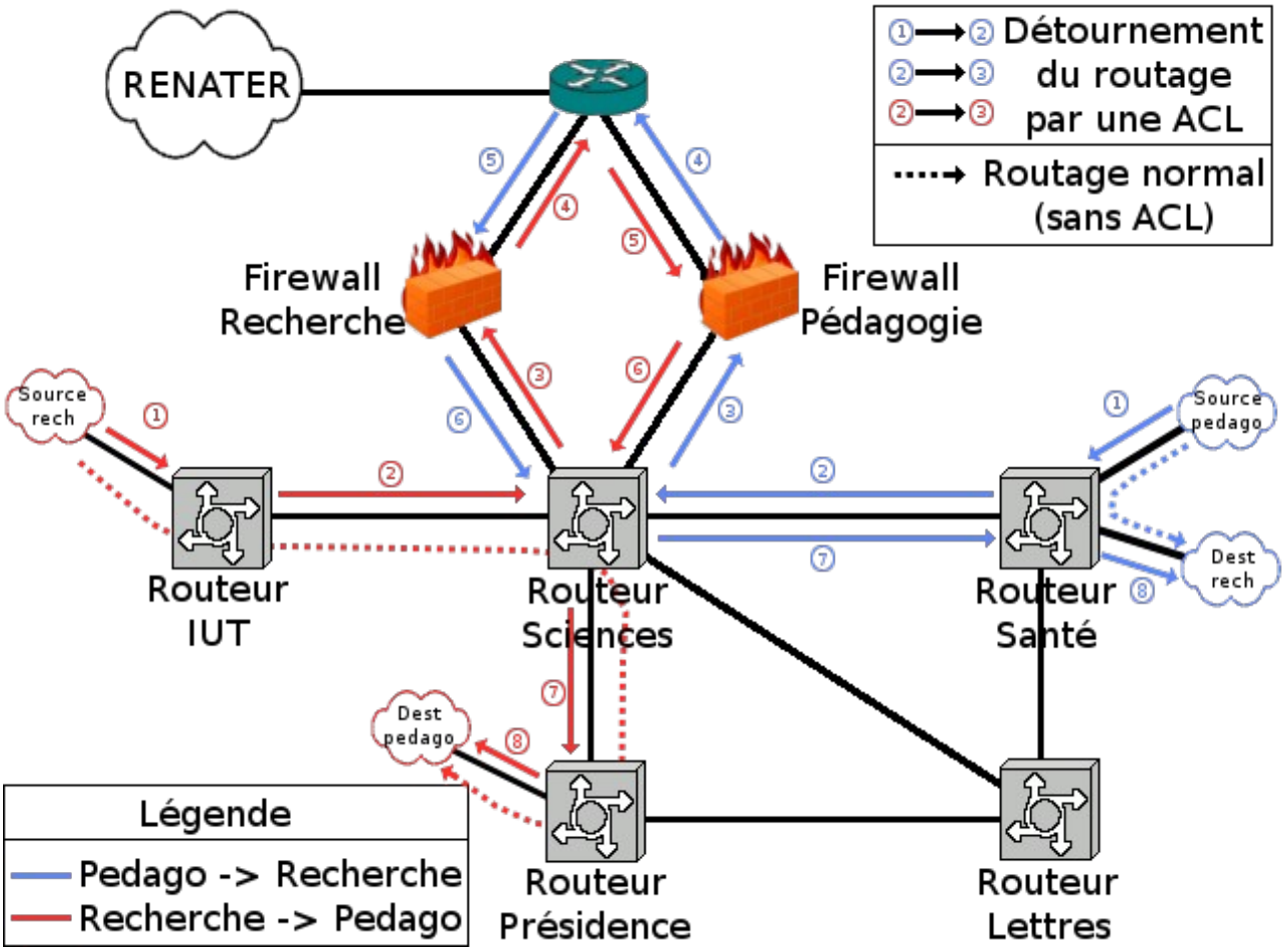

Figure 1: Schéma simplifié des flux dans le réseau avant la migration

Il existait déjà, avant la mise en place des VRF, un partitionnement en deux types de réseaux : recherche et pédagogie. Un pare-feu spécifique sécurisait chacun de ces réseaux. Pour ce faire, nous utilisions ce que l'on appelle le « routage par politique » (PBR : Policy Based Routing). Sur chacun de nos routeurs, nous mettions une liste d'accès (ACL : Access Control List) qui modifiait le routage normal en fonction de l'adresse source du paquet. Ainsi, les paquets en provenance des réseaux pédagogiques étaient « déroutés » vers le pare-feu approprié s'ils allaient en direction de l'internet ou des réseaux recherches. De la même façon, les paquets en provenance des réseaux recherches étaient « déroutés » vers le pare-feu approprié pour atteindre un des réseaux pédagogiques. Le fonctionnement normal routait tous les paquets vers le pare-feu de la recherche.

Cette méthode fonctionnait très bien, mais avait plusieurs inconvénients.

Le premier était la difficulté de gestion due à la complexité des ACL. Pour simplifier cette tâche, les réseaux pédagogiques avaient le plus souvent une forme facilement reconnaissable par les ACL (10.x.2.0/24). Malheureusement, toutes les exceptions (serveur, saturation de classe privée) nécessitaient un travail important et délicat pour modifier l'ensemble des ACL du réseau.

Le second était l'impossibilité de généraliser la méthode. La création de nouveaux types de réseau (WIFI par exemple) nécessitait une augmentation très importante de la complexité et du nombre d'ACL. Il aurait en effet fallu établir pour chaque type de réseau des ACL de façon à accéder à chaque autre type de réseau. Par exemple, pour avoir trois types de réseau au lieu de deux, six ACL auraient été nécessaires par routeur au lieu de quatre (La communication entre deux réseaux nécessite effectivement deux ACL, une par sens de communication).

Le troisième inconvénient concernait la recherche des pannes. La notion de PBR n'apparaît pas dans les tables de routage et la visualisation du trajet des paquets sur les routeurs n'était pas aisée.

3.2 Choix de l'architecture

La principale modification matérielle dans notre réseau a été le remplacement du pare-feu. Les deux pare-feu ont laissé place à une unique machine disposant de huit interfaces réseau (Gigabit Ethernet) et d'une capacité supérieur de traitement. Cette restructuration nous a permis de simplifier les tâches quotidiennes d'administration.

Nous avons également augmenté le nombre de types de réseaux isolés par rapport à nos besoins initiaux. A ce jour, six tables de routage sont instanciées dans nos actifs : serveurs sécurisés (table principale), recherche, pédagogie, WIFI, serveurs et TOIP (récemment ajouté).

Nous avons également décidé de conserver des VLAN multi-campus au sein du backbone pour deux raisons :

- des composantes ont besoin d'avoir le même VLAN dans différents campus (la bibliothèque universitaire par exemple).I l est alors routé sur le campus principal de la composante ;
- des VLAN serveurs sont utilisés par toutes les composantes. Il est routé par le routeur principal en sciences.

La contrepartie de ce choix est la nécessité de conserver le protocole spanning-tree sur l'ensemble du réseau. Cela influence aussi l'interconnexion logique de nos routeurs.

3.3 Interconnexion des routeurs

Pour interconnecter les routeurs, chaque VRF a été branché de manière indépendante avec des VLAN inter-campus. Il y en a un par VRF, soit six en tout. Chacun dispose d'une classe C pour les routeurs. Ainsi, chaque routeur est le voisin de tous les autres. La résolution du maillage passe de ce fait par le protocole spanning-tree déjà mis en place pour les autres VLAN inter-campus. En revanche, le routage dynamique au sein du backbone est simplifié.

Enfin, nous avons connecté les différentes interfaces internes du pare-feu dans chacune des VRF du routeur principal de façon similaire.

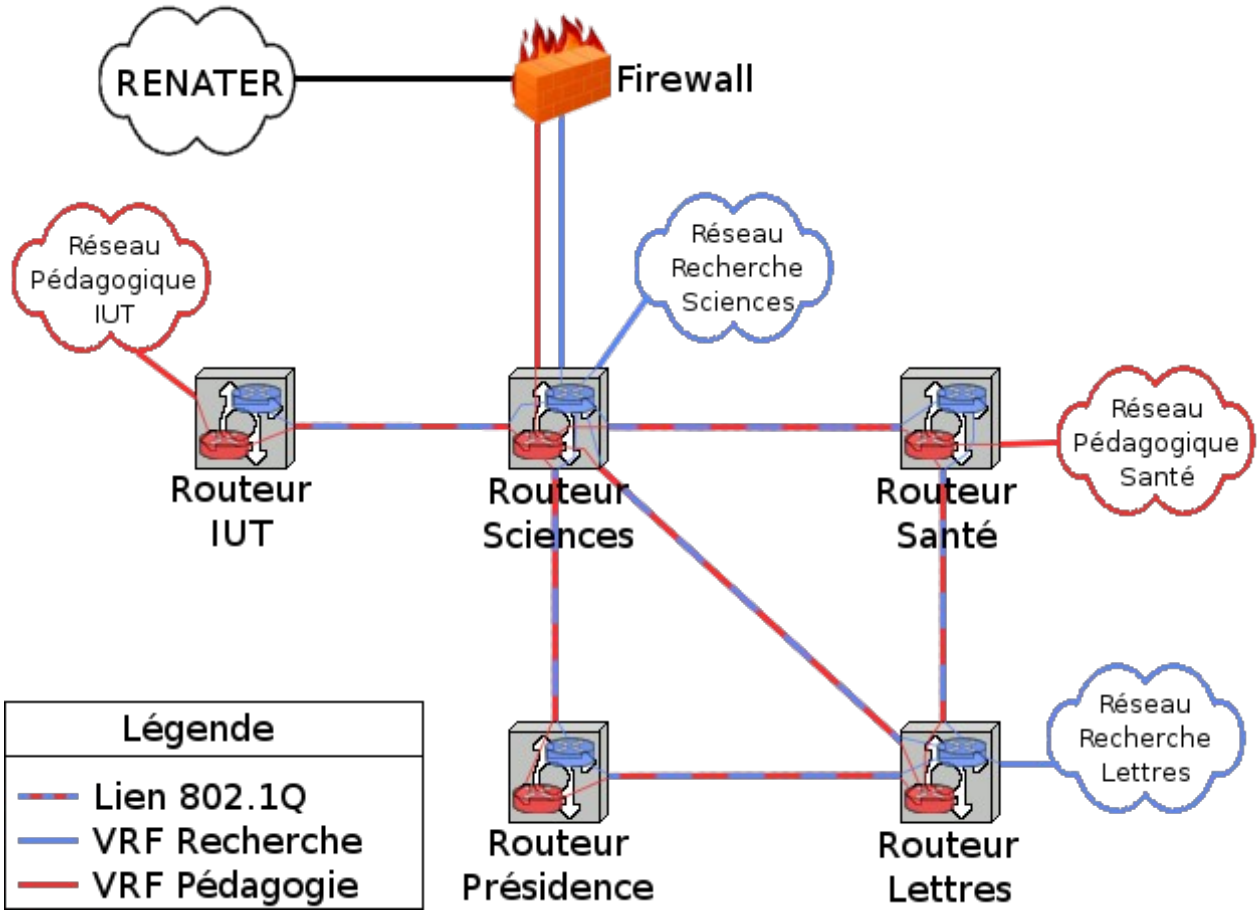

Figure 2: Schéma simplifié des VRF dans notre réseau

3.4 Routage dynamique

La communication des routes entre les différents routeurs et le pare-feu s'établit par routage dynamique avec le protocole OSPF (Open Short-Path First). Il faut faire attention : tous les protocoles de routage dynamiques ne sont pas supportés au sein des VRF. Ce routage dynamique n'a pas pour but de sécuriser notre infrastructure par des redondances de routes, Il s'agit uniquement de connaître dans chaque routeur la topologie du réseau.

Pour les machines, il faut que chacun des processus de routage VRF connaisse les chemins vers les autres réseaux de la même instance. Par exemple, sur le campus santé, la VRF RECHERCHE doit connaître les réseaux RECHERCHE des autres campus, mais pas les réseaux PEDAGOGIQUE ou WIFI. C'est un processus OSPF différent pour chacune des VRF qui est instancié au sein du routeur. Dans notre topologie, cela représente donc six processus OSPF différents par routeur. Le pare-feu n'a, quant à lui, qu'une seule instance OSPF en fonctionnement.

Le protocole OSPF permet de découper notre réseau en plusieurs aires représentées par un numéro. L'aire 0 doit impérativement exister et être connectée aux autres aires du réseau. Au sein d'une aire, les routeurs échangent toutes leurs routes entre-eux. En revanche, il n'y a pas d'échange de routes entre les aires, il n'y a que la connaissance du chemin vers l'aire 0.

C'est le principe mis en place dans notre réseau. Le pare-feu, centre névralgique du routage, est dans l'aire OSPF 0. On a ensuite créé une aire OSPF pour chaque VRF. Ainsi, la table de routage d'une VRF n'est pas « polluée » par les routes des autres VRF. Par ce moyen, on évite de remplir la mémoire du routeur par des informations redondantes.

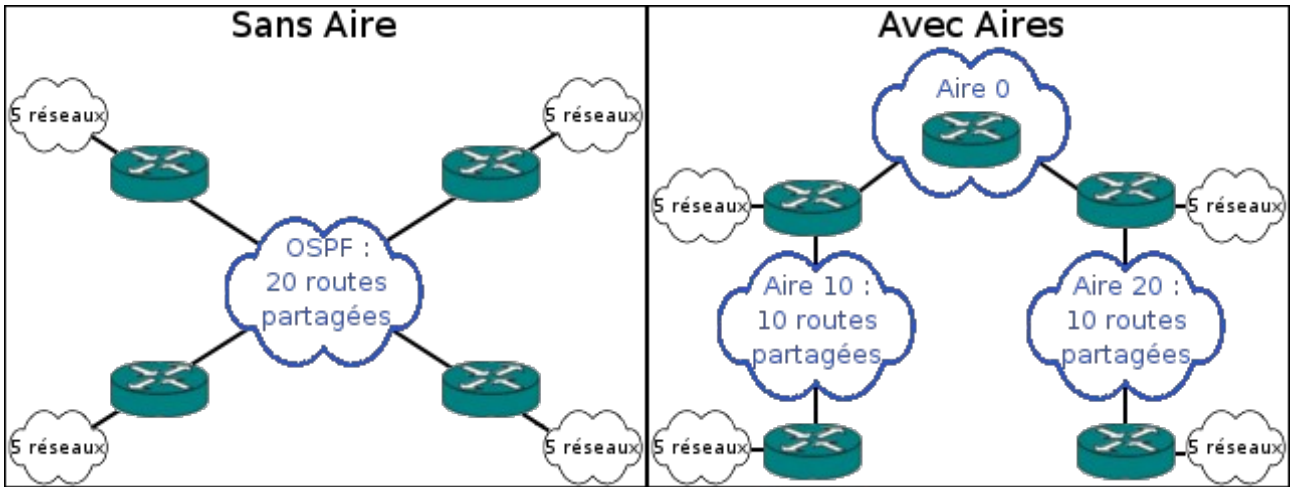

Figure 3: Exemple d'utilisation des aires OSPF

3.5 Plan synthétique global

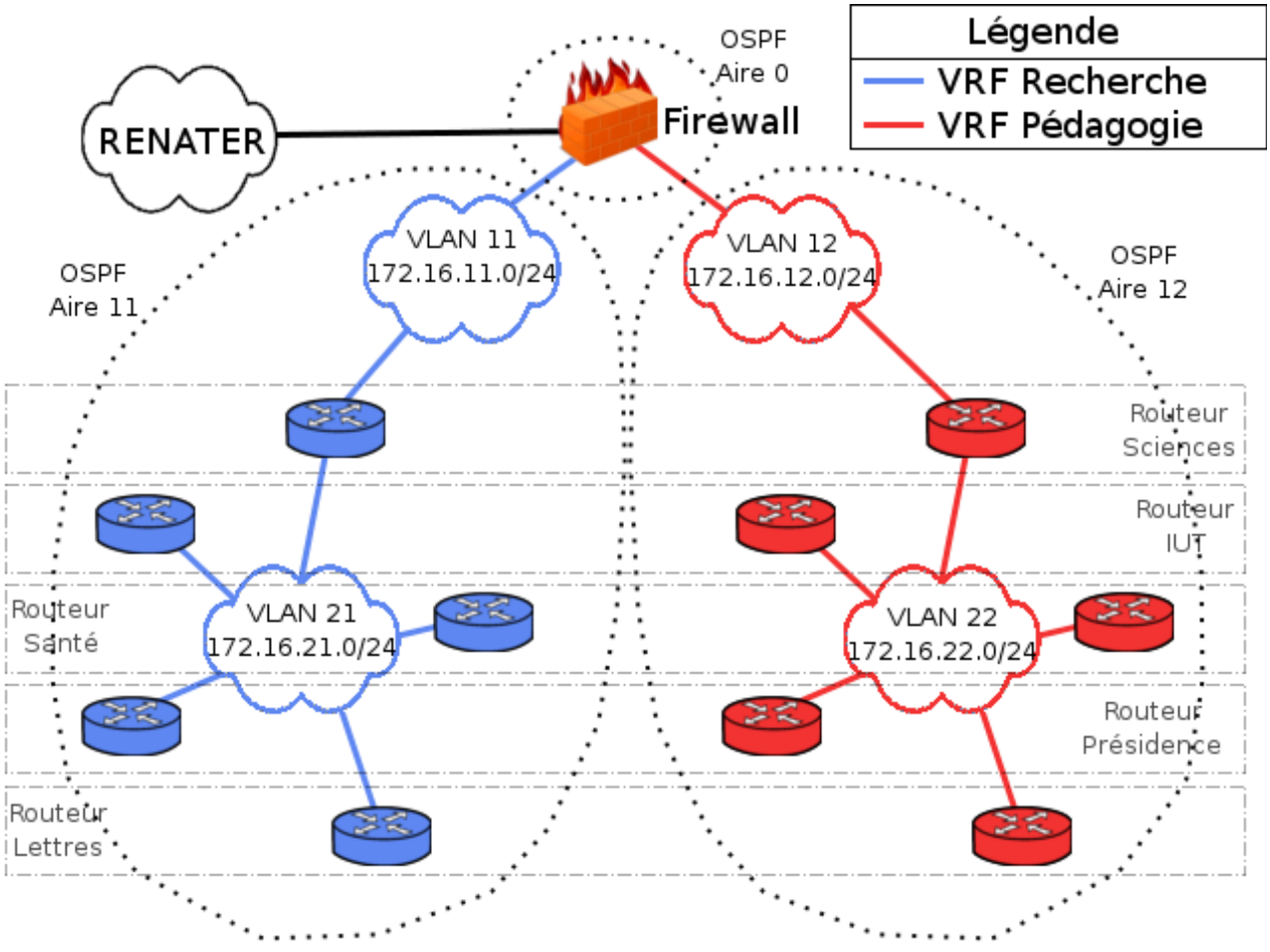

Figure 4: Schéma simplifié de l'interconnexion niveau 3 des routeurs

4 Utilisation quotidienne de la technologie

4.1 Rappel VRF et CPU du routeur

Quand on crée plusieurs instances de routage au sein d'un routeur par la technologie VRF-Lite, il existe toujours une instance par défaut qui n'a pas besoin de déclaration préalable. Si on ne précise pas dans la déclaration d'une interface qu'elle fait partie d'une VRF, alors elle se trouvera dans cette instance par défaut.

La CPU de notre routeur fait toujours parti de cette instance par défaut. Cela inclus tous les processus tournant sur la machine (sauf s'ils sont explicitement dédiés à une VRF comme les processus de routage). La connexion au routeur (via ssh ou telnet) ne peut se faire que par une des interfaces de cette instance.

Pour améliorer la sécurité du routeur, chacun des réseaux des utilisateurs est placé dans une VRF. Ils ne peuvent ainsi pas établir de connexion (via ssh) sur leur passerelle par défaut. Cette sécurité supplémentaire est malgré tout renforcée par des ACL limitant les connexions possibles.

4.2 Gestion des pannes réseau

Les habitudes des utilisateurs et des correspondants informatiques répartis sur l'ensemble des campus restent inchangées. La commande *traceroute* par exemple n'est pas impactée par la modification effectuée (contrairement à l'utilisation de MPLS). Pour les administrateurs des routeurs, il est par contre impératif de préciser dans quelle VRF les commandes sont exécutées.

Par exemple, pour tracer un réseau depuis nos réseaux pédagogiques, a commande à exécuter est :

```
traceroute vrf PEDAGOGIE www.renater.fr
```

De même pour voir l'état de la table de routage des réseaux recherche, la commande est maintenant :

```
show ip route vrf RECHERCHE
```

4.3 Gestion courante du réseau

Le plus gros avantage de ce nouveau système est la facilité avec laquelle nous pouvons ajouter ou modifier des réseaux.

Auparavant, il fallait créer le réseau puis toutes les ACL pour maintenir le blocage au sein de son domaine de travail (Recherche, Pédagogie). Ces opérations étaient très délicates. À de nombreuses occasions, les modifications dans ces listes provoquaient des dysfonctionnements difficilement détectables. Il arrivait aussi que les modifications ne soient pas faites ou seulement partiellement, provoquant au fil des années de nombreuses failles dans la sécurité du réseau.

Désormais, il suffit de placer le réseau dans la bonne VRF pour qu'il soit bloqué dans celle-ci. Les risques d'erreurs se trouvent réduits au minimum.

5 Et Après ...

5.1 Les modifications déjà apportées

Depuis la mise en place du nouveau pare-feu et des VRF, il y a eu un changement majeur dans notre réseau : la mise en place généralisée de la téléphonie sur IP. Cette mise en place a nécessité la création de nombreux réseaux pour les téléphones et les serveurs, avec une forte exigence du point de vue de la sécurité. Cela nécessitait donc une isolation totale des réseaux de TOIP avec tous les autres réseaux de l'université.

Pour ce faire, nous avons rajouté dans l'ensemble de nos routeurs une sixième instance VRF pour y placer la TOIP. Nous avons ensuite créé les règles de filtrage entre les réseaux de la téléphonie et le reste du réseau très simplement.

5.2 Les évolutions envisagées

Cette technologie s'est avérée très efficace dans le réseau métropolitain rémois. Nous envisageons de déployer les VRF sur les réseaux métropolitains des autres villes de notre université. Ce projet est conditionné par l'installation d'un nouveau pare-feu plus performant. Une étude est en cours sur cette opération. Nous envisageons son installation dans le courant de l'année 2012.

6 Conclusion

La virtualisation du routage, mise en place il y a plus de quatre ans, s'avère très robuste. Durant toutes ces années, a ucune panne n'a été déplorée sur cette technologie. Sa flexibilité et sa simplicité d'utilisation nous permettent de répondre rapidement à de nombreuses demandes, dans le respect de la sécurité de notre réseau.

7 Bibliographie

[1] Catalyst 4500 Series Cisco IOS Software Configuration Guide – 12.1(20)EW ; Chapitre 22 Configuring VRF-lite.

[2] Cisco IOS IP and IP Routing Configuration Guide ; Configuring OSPF