Projet « [VPN Redondant] »

Etude finale

Version 1.3

10 janvier 2006

Historique des révisions

Date	Version	Description	Auteur
11 octobre 2005	1.0	Création du document	Guillaume Coqueblin
26 octobre 2005	1.1	Révision	Guillaume Coqueblin
21 décembre 2005	1.2	Etude finale	Christophe CHARNAY
10 janvier 2006	1.3	Etude finale	Christophe CHARNAY

Sommaire

1 Introduction

1.1 Contexte, objectifs et contraintes

L'objectif du projet est de faire l'étude et la réalisation d'un prototype montrant une interconnexion de deux réseaux privés (ou plus) via un VPN chiffré utilisant IPsec.
Les passerelles d'interconnexions (à In'tech INFO) seront en binôme et redondantes.

Les principaux intervenants du projet, sont :

Commanditaire : In'Tech Info
Contacts et références : Eric Lalitte
Aurélien Bordes
Membres du projet : Alexis Carle
Christophe Charnay (Chef De Projet)
Guillaume Coqueblin
Utilisateurs : Elèves In'Tech Info

Objectifs de la solution proposée

- Réalisation de la plate-forme
- Installation d'OpenBSD sur les passerelles
- Une solution VPN doit permettre aux utilisateurs distants de se connecter aux ressources du réseau local.
- Configuration réseau (routage, filtrage avec pf)
-
- Configuration IPsec
- La solution doit assurer la confidentialité et l'intégrité des données à travers Internet.
- Mise en place de la redondance (CARP, pfsync, sasync)
- Pour l'utilisateur aucune différence ne doit apparaître dans son utilisation des ressources du système d'information.
- Mise en place de l'authentification par certificats
- La solution doit générer et mettre à jour les clefs pour le chiffrement des données pour le client et le serveur.
- Analyse du trafic et des logs.

Bénéfices attendus

- Connaissance d'OpenBSD, configuration du système
- Conception et réalisation de démonstration
- Connaissance de pf
- Utilisation de CARP et pfsync
- Connaissance d'IPsec
- Étude de sasyncd
- Acquérir des automatismes pour le débogage des systèmes et des réseaux.

Contraintes :

Utilisation d'OpenBSD 3.8 car IPsec est implanté nativement dans OpenBSD, entre autres, avec le service isakmpd basé sur le protocole IKE. Il intègre aussi nativement les services nécessaires a la redondances : carp, sasync et pfsync.

Le projet est en développement sur un réseau, « a priori » de confiance, et sur lequel nous n'avons ni contrôle, ni supervision.

Le basculement d'une machine à l'autre doit s'effectuer de manière totalement transparente et sécurisée pour les clients.

1.2 Glossaire

Openbsd : distribution de base Unix

VPN : Virtual Private Network (Réseau Privé Virtuel) liaison entre 2 réseaux distants

Redondant : La redondance, d'une façon générale, se rapporte à la qualité ou à l'état d'être en surnombre, par rapport à la normale ou à la logique. Ce qui peut avoir la connotation négative de superflu, mais aussi un sens positif quand cette redondance est voulue afin de prévenir un dysfonctionnement.

IPsec : IPsec est un protocole permettant le transport de données chiffrées sur un réseau IP pour établir un réseau privé virtuel.

Sasync : Service de synchronisation des règles de chiffrement d'IPsec lors d'un crash d'une passerelle.

Carp: Common Address Redundancy Protocol (Protocole de redondance d'adresse commune), ARP permet a plusieurs hôtes dans un même réseau local de partager un plage d'adresse IP. Son but premier est de s'assurer que les adresses sont toujours disponibles, mais dans certaines configurations, carp, permet aussi de fournir de la balance de charge.

Pf: Packet Filter, fichier de configuration des règles du firewall.

Routage: Dans le cas présent, le routage est le transfert de paquets d'un réseau à un autre

Filtrage: Règles établies par le firewall qui autorisent ou refusent le routage des paquets

NAT: Network Adress Translation, permet de rendre des adresses du réseau local routable sur internet.

Haute Disponibilité: Le cluster de haute disponibilité est un ensemble de serveurs physiques, au nombre minimum de deux, afin d'obtenir une activité de services par tous temps, en toutes conditions

1.3 Documents de référence

- http://www.openbsd.org,
- pages man d'Openbsd,
- Plan d'Assurance Qualité,
- planning.doc

2 L'existant

Nous avons déjà à notre disposition 2 machines sous Openbsd et le réseau Itinet.

3 Recueil des besoins

3.1 Utilisateurs

Les élèves d'In'tech INFO, et par la suite, suivant le niveau de qualité de réalisation de ce projet et du projet « firewall redondant », la commercialisation d'une solution firewall-vpn redondants auprès des sociétés et SSII.

3.2 Besoins fonctionnels

Le système à réaliser se doit de faire la liaison entre 2 réseaux distants de manière redondante et sécurisée, mais il doit passer la NAT.Tout ceci doit se faire de manière transparente pour l'utilisateur, même en cas de perte de connexion sur l'une des machines VPN.

3.3 Besoins non fonctionnels

Nos besoins non fonctionnels sont de l'ordre du matériel. Le chiffrement des données circulant à travers les machines faisant office de serveur VPN pouvant être assez conséquent, la machine devra disposer d'un processeur d'au moins 1GHz, de 256Mo de mémoire vive, ainsi que la connectique liée à la redondance (au total 6 cartes réseau, 5 câbles torsadés, dont 1 croisé).

4 Orientations techniques

4.1 Architecture générale de la solution

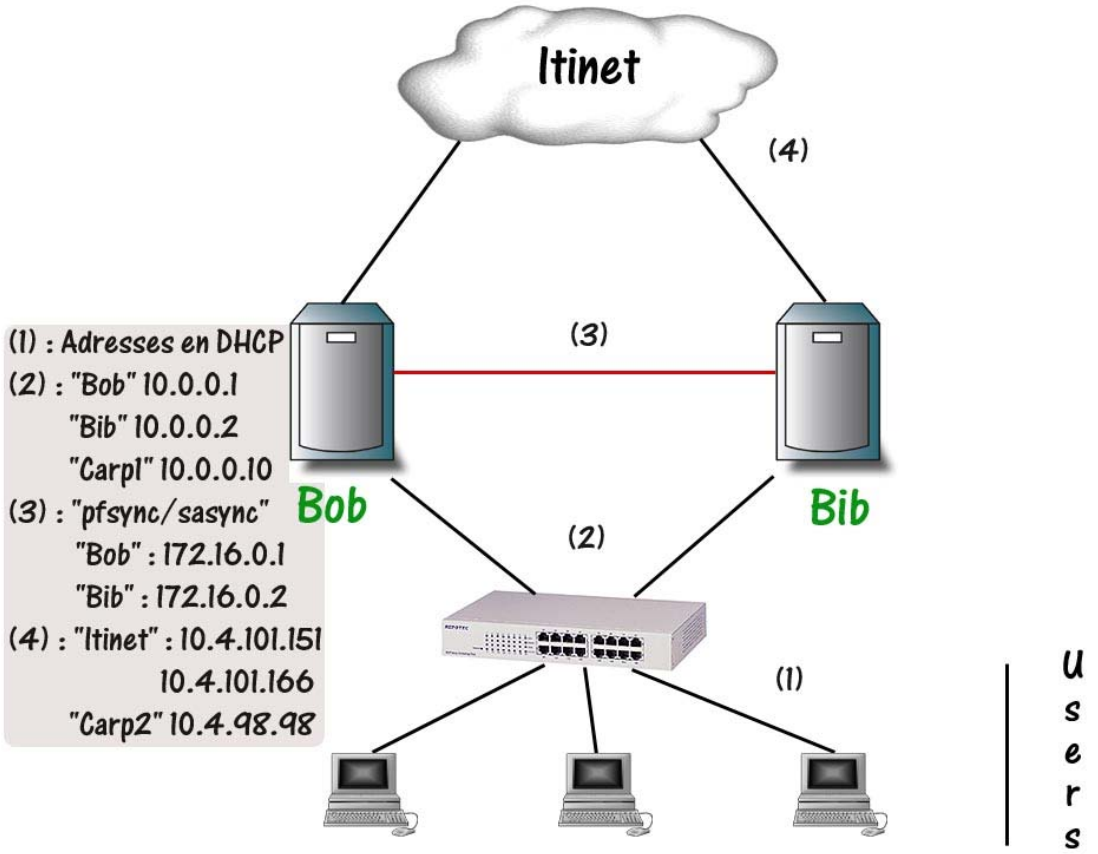
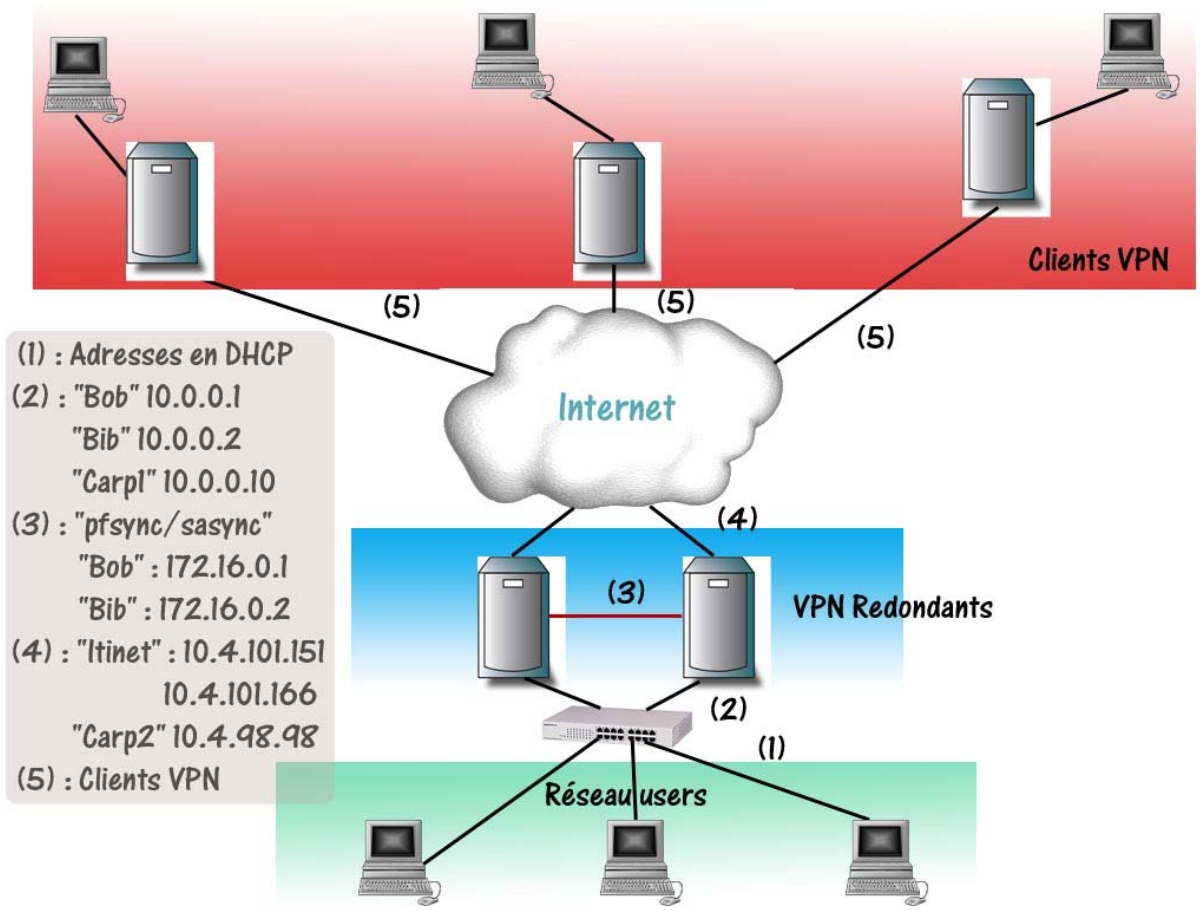


Schéma général de la solution VPN redondant



4.2 Technologies et outils

Le système d'exploitation qui est utilisé est Openbsd 3.8, ainsi que des outils n'existant que dans la version 3.8, comme par exemple :

- **Carp :**

CARP veut dire "Common Address Redundancy Protocol". L'objectif premier de ce protocole est de permettre à un groupe d'hôtes sur un même segment réseau de partager une même adresse IP. On appelle un groupe d'hôtes utilisant CARP un "groupe de redondance". Le groupe de redondance se voit attribuer une adresse IP partagée entre les membres du groupe. Au sein de ce groupe, un hôte est désigné comme "maître". Les autres membres sont appellés "esclaves". L'hôte maître est celui qui "prend" l'adresse IP partagée. Il répond à tout trafic ou requête ARP à l'attention de cette adresse. Chaque hôte peut appartenir à plusieurs groupes de redondance.

Nous utilisons CARP pour créer un groupe de VPN redondants. L'adresse IP virtuelle attribuée au groupe de redondance est désignée comme l'adresse du routeur par défaut sur les machines clientes. Dans le cas où le VPN maître rencontre une panne ou est déconnecté du réseau, l'adresse IP virtuelle sera prise par un des VPN esclaves et le service continuera à être rendu sans interruption.

CARP supporte IPv4 et IPv6.

L'hôte maître du groupe envoi des annonces régulières sur le réseau local afin que les hôtes esclaves puissent savoir qu'il est toujours disponible. Si les hôtes esclaves ne reçoivent plus d'annonce de la part du maître durant une période de temps configurable, alors l'un d'eux devient le nouveau maître. Ce dernier est celui dont les valeurs configurées pour advbase et advskew sont les plus faibles.

Afin d'empêcher un utilisateur malicieux sur le segment réseau d'usurper les annonces CARP, chaque groupe peut être doté d'un mot de passe. Ainsi chaque paquet CARP envoyé au groupe est protégé par SHA1 MAC.

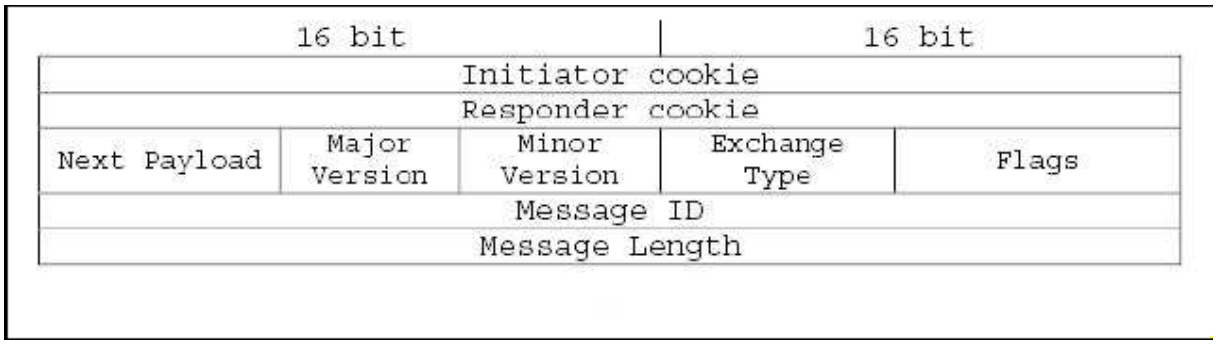
- **Isakmpd :**

Le rôle d'ISAKMP est d'établir, de négocier, de modifier ou de supprimer des Associations de Sécurité et leurs attributs.

Ce protocole constitue un cadre générique indépendant des mécanismes en faveur desquels la négociation a lieu et de ceux par lesquels la sécurisation est réalisée ; c'est pour cette dernière raison qu'un document appelé DOI (Domain Of Interpretation - Document définissant les paramètres négociés et les conventions relatives a l'utilisation de ISAKMP dans un cadre précis-) est nécessaire.

ISAKMP se déroule en deux phases :

- Tout d'abord, création de la SA ISAKMP, qui servira à la sécurisation de l'ensemble des échanges futurs : on a donc négociation d'attributs relatifs à la sécurité, authentification des identités des tiers, génération des clefs...
- Ensuite, négociation de paramètres de sécurité relatifs à une SA à établir pour un mécanisme donne (par exemple AH ou ESP), via la SA ISAKMP établie dans la phase précédente.



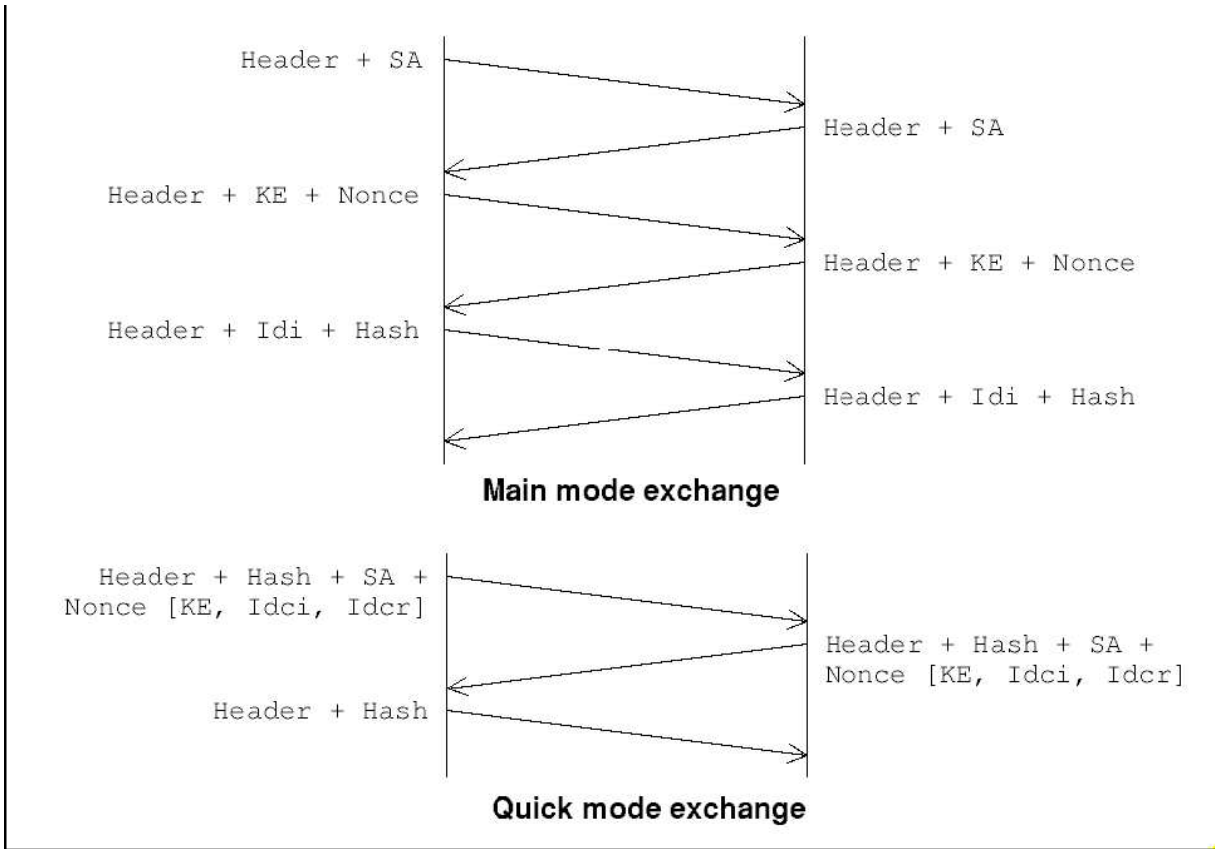
Entête d'ISAKMP

```
(18:51:02)[root@Bob] ~ $ isakmpd -dv4
185110.462353 Default isakmpd: phase 1 done: initiator id cabinet-crearte.com, responder id itinet.fr, src: 10.4.98.98 dst: 81.57.45.105
185110.843036 Default isakmpd: quick mode done: src: 10.4.98.98 dst: 81.57.45.105
```

Connexion d'un client à Isakmpd

- **IKE :**

IKE est le protocole de gestion des clefs implémente par IPSec. Il comprend 4 modes, qui gèrent les échanges de paramètres entre les entités souhaitant communiquer ; le but est de créer la SA dans les deux pairs a l'aide des deux phases d'ISAKMP. La première phase est utilisée pour créer une SA IKE - via les échanges identity protect exchange et aggressive exchange d'ISAKMP-, la deuxième pour négocier les paramètres nécessaires a la création de la SA IPSec.



Echange IKE classique

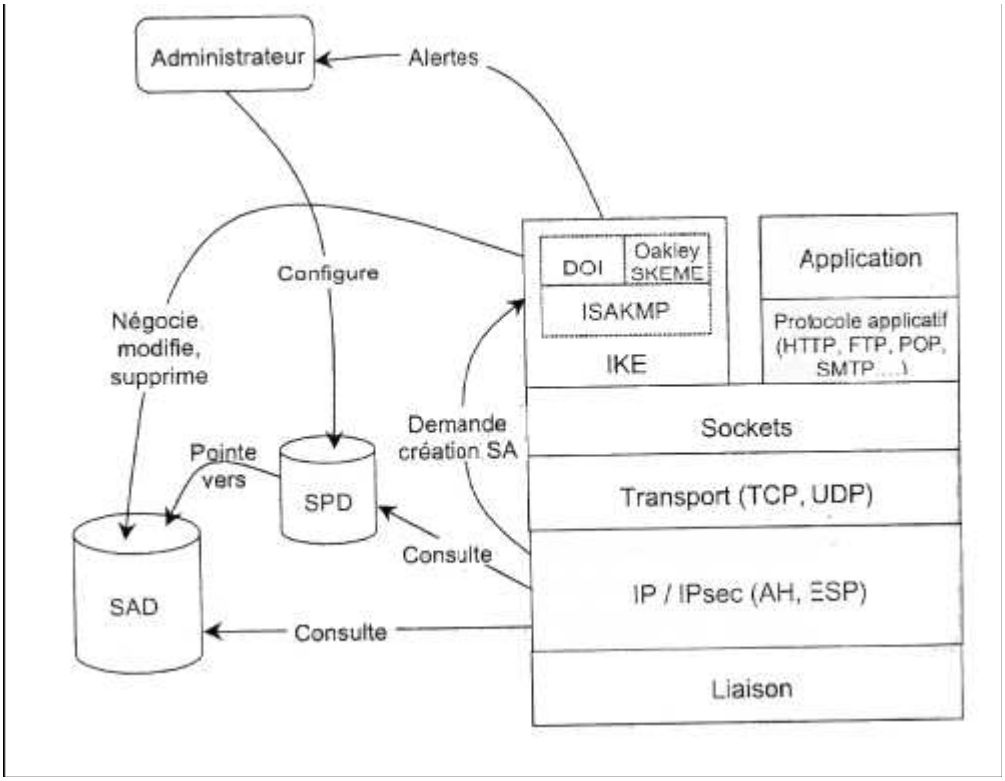
- **Ipsec :**

A l'heure actuelle, plusieurs solutions VPN existent et sont utilisées sur Internet : IPsec est celle que l'on retrouve le plus souvent, et de nombreux facteurs indiquent que cette situation tend à se généraliser (supporte nativement par de nombreux systèmes d'exploitation, protocole ouvert, etc.).

Notre étude suivante se limitera donc à IPsec et aux mécanismes qu'il engendre; avant d'entrer dans les détails techniques, revenons aux principes de base d'IPsec.

IPsec se présente sous la forme d'un ensemble de mécanismes permettant d'initier, au niveau réseau, des connexions entre systèmes distants.

Le schéma suivant rappelle les principes de son fonctionnement :



On note à la vue de ce schéma qu'IPsec repose sur le protocole IKE, qui permet une connexion sécurisée entre les entités désirant communiquer, et les protocoles AH et ESP, qui traitent les données utiles de la couche IP afin de les protéger selon la politique choisie ; c'est donc ces protocoles que nous allons étudier en détail.

Avant que les paquets puissent être sécurisés par IPsec, une SA (Associations de Sécurité) doit exister. Elle peut être créée manuellement ou dynamiquement.

Le protocole IKE est utilisé pour la création dynamique de cette SA; il s'agit d'un protocole hybride basé sur les protocoles ISAKMP, Oakley et SKEME : il utilise les bases d'ISAKMP, les modes d'Oakley et les techniques de partage des clefs de SKEME.

- **Pf (Packet Filter) :**

Packet Filter est le système utilisé par OpenBSD pour filtrer le trafic TCP/IP et effectuer des opérations de Traduction d'Adresses IP ("NAT"). PF est aussi capable de normaliser, de conditionner le trafic TCP/IP, et de fournir des services de contrôle de bande passante et gestion des priorités des paquets. PF fait partie du noyau GENERIC d'OpenBSD depuis la version 3.0. Les précédentes versions d'OpenBSD utilisaient un ensemble logiciel pare- feu/NAT différent qui n'est plus supporté.

- **Pfsync :**

Pfsync prend en charge la réplication des tables de sessions entre les firewalls. En d'autres mots chaque firewall possédant une interface pfsync activée émet des informations sur les sessions qu'il prend en charge sur le réseau.

(Pfsync utilise des interfaces virtuelles *pfsync0*)

Par exemple il envoie un paquet multicast sur le réseau pour indiquer qu'une session tcp a été ouverte ou fermée, avec toutes les informations sur la session. Ce qui permet aux équipements configurés pour se synchroniser sur pfsync de se mettre à jour par rapport aux changements des tables des autres firewalls.

Cette dernière fonctionnalité couplée à CARP, permet de créer des backup du firewall maître. Avec la synchronisation activée (pfsync), lorsqu'un équipement de backup prend la main, il possède toutes les informations sur les tables de sessions et peu continuer à filtrer le trafic réseau sans interruption. Dans nos tests il y a un temps de latence très court lors du basculement d'un serveur à l'autre.

Au niveau des services et des utilisateurs passant par ce firewall il n'y a pas de coupure de sessions lorsque la ou les adresses ip des firewalls basculent d'un serveur à l'autre.

Note : Les adresses Ip prisent en charge par Carp, sont appellées VIP (Virtual Ip).

Il est aussi important de noter que lorsque le firewall maître ressuscite, il ne reprend la main que lorsque pfsync à effectué sont travail de synchronisation par rapport au serveur maître en cours, ceci grâce a la combinaison de carp et pfsync.

Résultat : pas de coupure de session même lorsque le premier serveur réapparaît sur le réseau.

- **Sasyncd :**

Le démon sasyncd synchronise les informations des SA et SPD IPsec entre plusieurs passerelles IPsec. La méthode la plus utilisé est de faire fonctionner sasyncd sur un serveur isakmpd et de partager une même IP grâce à l'outil carp.

Le démon fonctionne soit en mode maître soit en esclave, dans lequel le maître récupère tous les paquets de changement d'SA IPsec et envoie les informations à tous les clients afin qu'ils disposent des mêmes données.

Lorsqu'un esclave se connecte ou se reconnecte, Le maître transmet instantanément toutes les informations des SA et SPD IPsec en cours.

```
{19:18:21}[root@Bob] ~ $ sasyncd -dv
carp_init: locking runstate to MASTER
net_connect: peer "10.4.101.166" not ready yet
net_disconnect_peer: peer "10.4.101.166" removed
net_connect: peer "10.0.0.2" not ready yet
net_disconnect_peer: peer "10.0.0.2" removed
```

```
{21:07:59}[root@Bib] ~ $ sasyncd -dv
carp_init: locking runstate to SLAVE
net_connect: peer "10.4.101.151" not ready yet
net_disconnect_peer: peer "10.4.101.151" removed
net_connect: peer "10.0.0.1" connected, fd 5
net_ctl: peer "10.0.0.1" state change to MASTER
net_disconnect_peer: peer "10.0.0.1" removed
```

- **Certificat X509**

  Les certificats X509 permettent l'authentification entre le serveur et le client vpn. Pour cela nous devons générer la clef RSA, le certificat pour le CA et le CSR (Certificate Signing Request) en utilisant openssl.

5 Analyse des risques

Le risque majeur est que le fait de mettre en place une solution sur la base d'un système d'exploitation encore en version « testing » ne soit pas tout à fait au point, et les outils fiables et sécurisés.

6 Plan de travail

Suivant ce qui a été établi lors d'une réunion avec Aurélien Bordes et Eric Lalitte les étapes sont les suivantes :

- Etude et mise en place de la redondance, en utilisant *carp*
- Sécurisation de la connexion sortante grâce à *IPsec* et *isakmpd*
- Configuration du firewall par les règles *pf*
- Synchronisation des règles de sécurité avec *SAsyncd*

- Synchronisation des règles de filtrage entre les deux serveurs grâce à *pfsync*
- Tests finaux et écoute du trafic
- Rédaction d'une documentation
- Démonstration en temps réel.

7 Livrable

Nous restituons à l'école les 2 machines, installées et configurées, accompagnées d'une documentation décrivant notre étude.
La maintenance sera à la charge du client.