**Firewall :**

Le firewall que l’on va utiliser est PFSense car il est facile d’utilisation mais aussi car nous l’avons déjà utilisé lors d’un projet en premier année en tant que routeur.

En termes de configuration, il faudra installer PFSense sur une vm linux en ajouter 3 carte réseau, 1 pour le réseau WAN (le physique ou NAT), 1 pour le réseau LAN (le virtuel) et 1 pour la synchronisation des pares-feux (pour le actif/passif).

**VPN :**

Pour la connexion VPN site à site, nous allons utiliser IPSec car même si OpenVPN est plus sécuriser, il est plus pour du client à site et il est plus compliqué à réaliser. Alors que IPSec est assez facile utilisation mais aussi complet avec un choix de cryptage assez important.

C’est à faire sur tous les firewalls.

En termes de configuration, il faut :

* Ajouter la Gateway du réseau distant
* Mettre IP du WAN
* Choisir IPv4
* Choisir la méthode d’authentification entre clé partagé (PSK) et le certificat (RSA) nous nous choisissons PSK pour plus de sécurité.
* Saisir l’ip public (par défaut)
* Saisir l’ip adresse de l’autre paire (par défaut)
* Saisir un mot de passe
* Choisir l’algorithme de chiffrement, nous allons prendre AES 128bits SHA256, car ça convient de tous.
* Le temps de vie de la connexion, on part du principe qu’on travaille maximum 8h donc 28 800 secondes.

Ensuite il faut sauvegarder et appliquer.

Pour l’IPSec il faut :

* Voir la phase 2
* Ajouter la p2
* Mettre le tunnel de transport en Tunnel IPv4 car c’est le protocole internet utilisé (Ip VIP voir partie Actif/Passif)
* Mettre le réseau local d’accès, nous laissons par défaut
* Le NAT pour le tunnel IPSec, a configurer seulement si les 2 réseaux sont identiques
* Remote Network qui est le réseau du site distant

Même procédé que pour la phase 1 pour le protocole de chiffrement :

* AES 128 SHA256
* Puis l’host à ping automatiquement afin de garder le tunnel ouvert (IP du serveur)

C’est à faire sur tous les firewalls.

Ensuite il faut ajouter les règles de tous les côtés des pares-feux dans Firewall/Rules/LAN :

* Lan : autoriser la carte lan vers le réseau distant
* Source : LAN
* Destination : Réseau Distant

Puis dans Firewall/Rules/IPSec :

* Choisir l’interface IPSec
* Source : IPSec (Réseau distant)
* Destination : Lan net

Et faire les vérifications en essayant par exemple d’accéder à la page web du serveur distant grâce à son IP.

**Pour la partie Actif/Passif :**

Il faut que sur les firewalls, on a au minimum 1 WAN, 1 LAN.

* Il faut donc :
* Créer une ip virtuel (Virtuel Interface Protocol)
* Type CARP (qui est le plus utilisé pour la haute disponibilité [qui est la communication entre les firewalls)
* Interface : l'interface sur laquelle la VIP doit être configurée. Nous configurons la première sur l'interface WAN, puis la seconde sur l'interface LAN.
* Adresse : l'adresse VIP et le masque du subnet de l'interface
* Virtual IP Password : mot de passe permettant de sécuriser les échanges au sein du groupe d'hôtes se partageant la VIP. Ce mot de passe devra être re-saisi sur le PFSense esclave.
* Virtual Host Identifier groupe : Un serveur peut faire partie de plusieurs groupes de VIP. Afin d'identifier chaque groupe, un ID unique lui est assigné. Nous laissons la valeur par défaut.
* Advertising Frequency : la valeur du champ "Skew" à 0 désigne le master (PFSense maitre). Une valeur plus élevée désignera l'esclave (PFSense esclave). La valeur de base correspond au timeout en seconde au bout duquel l'hôte sera considéré comme inaccessible. Par défaut 1.
* Nous faisons la même chose pour le Lan et sur le firewall passif.

Il nous reste à configurer la haute-disponibilité. Pour cela, se rendre dans "System" > "High Avail. Sync" :

* Synchronize States : activer pfsync qui est le synchronisateur
* Synchronize Interface : nous choisissons LAN par défaut
* pfsync Synchronize Peer IP : saisir l'adresse IP LAN du serveur PFSense esclave.
* Synchronize Config to IP : sur le serveur PFSense Maitre, saisir l'adresse IP du serveur PFSense esclave (comme précédemment, il faut saisir l'adresse IP de l'interface choisie). Ce champ doit être laissé vider sur le serveur PFSense esclave.
* Remote System Username : sur le serveur PFSense maitre, saisir le nom d'utilisateur utilisé pour se connecter sur l’interface du PFSense esclave ("admin" par défaut). Ce champ doit être laissé vide sur le serveur PFSense esclave.
* Remote System Password : sur le serveur PFSense maitre, saisir le mot de passe du compte utilisateur saisi ci-dessus. Ce champ doit être laissé vide sur le serveur PFSense esclave.

Puis, nous choisissons les services que nous souhaitons synchroniser en cochant les cases appropriées. Par défaut, nous recommandons de tout cocher.

Autoriser les flux de réplication au niveau des règles du firewall :

Il nous reste à autoriser les flux de réplications sur les firewalls. La configuration se passe dans "Firewall" > "Rules".  
Si la réplication se fait via l'interface LAN.

Il y a deux flux réseau à autoriser :

* le flux pour la synchronisation XML-RPC qui s'effectue via le port 443 (d'un appel de procédure à distance afin de récolter les informations des pares-feux utilisant HTTPS)
* le flux pour la synchronisation du protocole pfsync

Sur le firewall maitre, nous créons donc une première règle de firewall (en cliquant sur le bouton "Add") avec les paramètres suivants :

* Action : nous choisissons "Pass"
* Interface : nous choisissons l'interface dédiée à la réplication (LAN)
* Address Family : IPv4 par défaut
* Protocol : TCP pour la communication/transmission
* Source : nous indiquons un alias qui contiendra les adresses IP des interfaces de synchronisation de chaque pfSense sinon on peut choisir l'ensemble du réseau rattaché à l'interface de synchronisation (LAN net)
* Destination : nous choisissons "This firewall (self)" pour dire qu’on veut choisir ce firewall
* Destination port range : nous choisissons HTTPS 443 (port par défaut de XML-RPC)

Sur le firewall primaire toujours, nous créons une seconde règle de firewall avec les paramètres suivants :

* Action : nous choisissons "Pass"
* Interface : nous choisissons l'interface dédiée à la réplication (LAN)
* Address Family : IPv4 par défaut
* Protocol : PFSYNC pour la synchronisation
* Source : nous indiquons un alias qui contiendra les adresses IP des interfaces de synchronisation de chaque PFSense sinon on peut choisir l'ensemble du réseau rattaché à l'interface de synchronisation (LAN net)
* Destination : nous choisissons "This firewall (self)" pour dire qu’on veut choisir ce firewall

Ces deux règles de firewall ont été répliquées automatiquement sur le PFSense esclave.

**DMZ :**

Il faut se connecter au firewall.

Il faut ensuite attribuer les interfaces à leurs place respectives :

* WAN = em0
* LAN = em1
* Optional 1 = em2

Ajouter une IP et une Gateway a Opt1

Ensuite on sur le site PFSense :

* on va modifier le nom de l’interface Opt1
* puis créer une règle dans Firewall/Rules DMZ et tout mettre par défaut
* pour que le WAN atteigne la DMZ il faut créer une règle dans Firewall/Nat en redirigeant WAN vers le DMZ

**Serveur SQL :**

Nous allons utiliser MySQL serveur car il permet la répliquée et la synchronisation et il est facile d’utilisation.

Pour la réplication il faut :

* créer un utilisateur commun à tous les serveurs.

Dans le serveur maitre il faut :

* Modifier le fichier etc/mysql/my.cnf en ajoutant les autres serveurs puis redémarrer le serveur
* Faire un SHOW MASTER STATUS afin de voir les caractéristiques utilisé par le serveur maitre

Ensuite dans les serveur esclaves il faut :

* Editer comme le même fichier que pour le serveur maitre

Il faut ensuite :

* Prendre le fichier binaire de la bdd maitre et la copier dans le serveur esclave
* Puis il faut expliquer au serveur esclave auprès de quel serveur maitre il doit se répliquer avec CHANGE MASTER TO
* Puis on teste la réplication

Puis faire la même chose avec les serveurs esclaves afin que tous le monde ai les même données