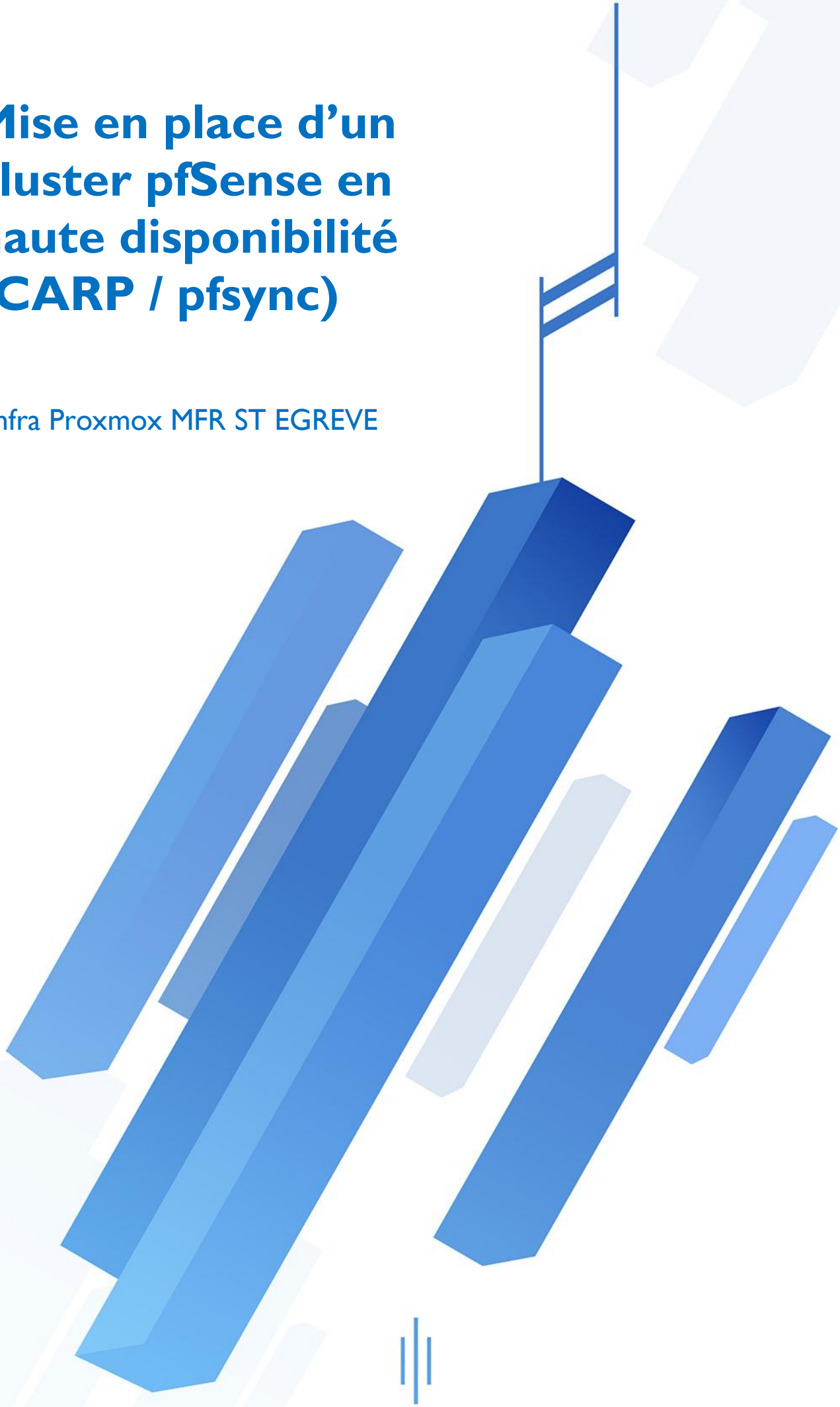
Mise en place d’un cluster pfSense en haute disponibilité (CARP / pfsync)

Infra Proxmox MFR ST EGREVE



Présentation de la situation professionnelle

Dans le cadre de ma formation en BTS SIO option SISR, au sein d'une infrastructure pédagogique entièrement virtualisée sous Proxmox VE, j'ai été amené à mettre en place un système de haute disponibilité réseau basé sur pfSense.

L'environnement de travail de la MFR repose exclusivement sur des machines virtuelles. Aucun équipement physique n'est utilisé, ce qui impose de reproduire, de manière virtualisée, des architectures professionnelles réalistes. Après avoir déployé un premier pare-feu pfSense assurant le routage et le filtrage entre les différents segments réseau, l'objectif a été d'aller plus loin en mettant en œuvre un cluster redondant.

Cette évolution visait à simuler un scénario d'entreprise dans lequel la passerelle réseau ne doit jamais constituer un point de défaillance unique. Dans un contexte réel avec infrastructure physique, une solution matérielle redondée de type WatchGuard ou Zyxel en cluster aurait été proposée. Dans notre environnement virtualisé, la mise en place d'un cluster pfSense via CARP et pfsync représentait l'approche la plus cohérente.

Contexte technique

L'infrastructure était hébergée sous Proxmox VE et structurée autour de plusieurs bridges virtuels simulant différentes zones réseau : un WAN, un LAN interne et un réseau dédié à la synchronisation.

Dans un premier temps, un seul pfSense jouait le rôle de passerelle principale pour l'ensemble des machines virtuelles (serveurs AD, postes clients, services en DMZ). Cette architecture fonctionnait correctement mais présentait une limite évidente : si la machine virtuelle du pare-feu venait à s'arrêter, l'ensemble de l'infrastructure perdait sa connectivité.

L'objectif était donc d'éliminer ce point de défaillance en mettant en place deux pare-feux pfSense fonctionnant en redondance active/passive.

Expression du besoin

Le besoin pédagogique et technique consistait à :

-assurer la continuité de service en cas de panne d'un pare-feu ;

-maintenir les sessions actives lors d'un basculement ;

-synchroniser automatiquement la configuration entre deux nœuds ;

-reproduire un scénario réaliste de haute disponibilité réseau.

La solution devait être entièrement intégrée à l'environnement Proxmox existant, sans matériel supplémentaire

Choix de l’architecture

Le protocole CARP (Common Address Redundancy Protocol) a été retenu pour gérer une adresse IP virtuelle partagée entre les deux pare-feux. Cette adresse devient la passerelle utilisée par les clients du réseau.

Le service pfsync a été configuré afin de synchroniser les états des connexions entre les deux nœuds. Ainsi, lorsqu’un utilisateur établit une session (HTTP, SSH, etc.), celle-ci est répliquée en temps réel vers le pare-feu secondaire.

Enfin, la synchronisation XMLRPC a été mise en place afin de garantir la réplication automatique des règles de pare-feu, des règles NAT et des paramètres système.

Cette combinaison permet de reproduire une architecture de haute disponibilité comparable à celles rencontrées en entreprise.

Mise en œuvre sous Proxmox

Deux machines virtuelles pfSense ont été créées dans Proxmox, chacune disposant de trois interfaces réseau virtuelles :

-une interface WAN connectée au bridge simulant l’accès Internet ;

-une interface LAN connectée au réseau interne ;

-une interface dédiée à la synchronisation (SYNC) entre les deux pare-feux.

Chaque pare-feu a reçu une adresse IP propre sur chaque interface. Ensuite, une adresse IP virtuelle (VIP) a été configurée sur le WAN et sur le LAN via le protocole CARP. Cette VIP représente la passerelle utilisée par les clients.

Le premier pfSense a été défini comme nœud maître, tandis que le second a été configuré en mode secondaire avec une priorité inférieure. En fonctionnement normal, le maître détient l’adresse virtuelle. En cas de panne, le secondaire la récupère automatiquement.

Le réseau de synchronisation, isolé des autres flux, a été utilisé pour pfsync et XMLRPC. Des règles spécifiques ont été ajoutées pour autoriser uniquement le trafic nécessaire à la synchronisation.

Tests de basculement

Afin de valider la configuration, plusieurs scénarios ont été testés.

Dans un premier temps, j'ai vérifié que les clients utilisaient bien l'adresse IP virtuelle comme passerelle. Ensuite, j'ai simulé une panne en arrêtant volontairement la machine virtuelle du pare-feu maître.

Le basculement s'est effectué automatiquement : le second pare-feu a récupéré l'adresse IP virtuelle et la connectivité a été maintenue. Les sessions en cours n'ont pas été interrompues grâce à la synchronisation des états via pfsync.

Après redémarrage du nœud initial, celui-ci a repris son rôle de maître conformément à la priorité configurée.

Les journaux système ont été consultés afin de confirmer la bonne transition d'état et l'absence d'erreurs de synchronisation.

Impact sur l'infrastructure

La mise en place du cluster a profondément amélioré la résilience de l'infrastructure virtualisée. Le pare-feu n'est plus un point de défaillance unique et la continuité de service est assurée même en cas d'arrêt d'une machine virtuelle.

Au-delà de l'aspect technique, cette configuration m'a permis de comprendre concrètement les enjeux de la haute disponibilité : synchronisation des états, gestion des priorités, importance d'un réseau dédié à la réplication.

Cette architecture constitue également une base évolutive vers des scénarios plus avancés, comme la redondance multi-site ou l'intégration de solutions matérielles en environnement réel.

Bilan et retour d’expérience

Cette situation professionnelle m’a permis de travailler sur des notions avancées d’administration réseau et de sécurité, notamment :

-la gestion d’un cluster de pare-feux ;

-la mise en œuvre d’un protocole de redondance (CARP) ;

-la synchronisation des états de connexion (pfsync) ;

-la réplication automatique de configuration (XMLRPC).

Même si l’environnement était pédagogique et virtualisé, l’architecture mise en place reproduit fidèlement des mécanismes utilisés en entreprise.

Cette expérience renforce ma capacité à concevoir des infrastructures tolérantes aux pannes et à anticiper les risques liés aux points de défaillance critiques.