Mise en place d'un serveur NAS Synology en entreprise

Infra Proxmox MFR ST EGREVE

Situation professionnelle

Mise en place d'un pare-feu pfSense dans une infrastructure virtualisée Proxmox

Présentation de la situation professionnelle

Dans le cadre de ma formation en BTS SIO option SISR, j'ai été amené à concevoir et déployer un pare-feu au sein d'une infrastructure entièrement virtualisée sous Proxmox VE.

L'environnement pédagogique dans lequel nous travaillons repose exclusivement sur des machines virtuelles. Aucun parc physique n'est exploité, ce qui impose une architecture réseau entièrement simulée mais réaliste, reproduisant les contraintes d'une infrastructure d'entreprise.

La mise en place de pfSense s'inscrivait dans un projet global de sécurisation et de segmentation réseau. L'objectif était de disposer d'un pare-feu complet, capable d'assurer le filtrage, le NAT, la gestion des VLANs et la mise en place de services réseau avancés, tout en s'intégrant dans une topologie virtualisée.

Il est important de préciser que dans un contexte professionnel avec infrastructure physique, j'aurais naturellement proposé une solution matérielle dédiée telle qu'un WatchGuard ou un pare-feu Zyxel. Toutefois, dans le cadre de cette infrastructure 100 % virtualisée, pfSense constituait la solution la plus cohérente et techniquement pertinente.

Contexte technique

L'infrastructure était hébergée sur Proxmox VE et organisée autour de plusieurs bridges virtuels simulant différents segments réseau : un WAN, un LAN interne, ainsi que d'autres sous-réseaux dédiés aux services (serveurs, DMZ, synchronisation).

Avant la mise en place du pare-feu, la connectivité entre les machines virtuelles était possible, mais aucun filtrage avancé n'était appliqué. Il n'y avait pas de réelle séparation logique entre les zones, ni de politique de sécurité formalisée.

L'objectif était donc d'introduire une couche de sécurité intermédiaire jouant le rôle de passerelle et de point de contrôle centralisé, comme dans une infrastructure d'entreprise classique.

Expression du besoin

Le besoin pédagogique et technique était de :

-segmenter les flux réseau ;

-contrôler les communications entre les différentes zones ;

-mettre en place un accès Internet sécurisé ;

-implémenter des règles de pare-feu adaptées aux différents rôles des machines ;

-préparer l'infrastructure à des évolutions ultérieures (VPN, haute disponibilité, DMZ).

La solution devait également permettre une visualisation claire des flux et offrir des outils de diagnostic facilitant l'analyse des paquets.

Choix de la solution

Dans un environnement physique, l'utilisation d'un pare-feu matériel comme WatchGuard ou Zyxel aurait été privilégiée pour des raisons de performance, de support constructeur et de gestion centralisée.

Cependant, dans notre contexte virtualisé, pfSense présentait plusieurs avantages majeurs :

-compatibilité native avec les environnements virtuels ;

-richesse fonctionnelle équivalente à de nombreuses solutions matérielles ;

-flexibilité de configuration ;

-capacité à simuler des scénarios avancés (VLAN, DMZ, VPN, haute disponibilité).

pfSense est basé sur FreeBSD et offre des fonctionnalités professionnelles telles que le filtrage par états, le NAT avancé, la gestion multi-interfaces et le support de protocoles comme CARP ou OpenVPN.

Le choix s'est donc porté sur pfSense pour sa pertinence technique et pédagogique.

Mise en œuvre dans Proxmox

La première étape a consisté à créer une machine virtuelle dédiée dans Proxmox, à laquelle j'ai attribué plusieurs interfaces réseau virtuelles correspondant aux différents bridges :

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

-une interface LAN connectée au réseau interne ;

-d'autres interfaces selon les besoins (DMZ, synchronisation, etc.).

Après installation de pfSense via l'image ISO officielle, j'ai procédé à l'assignation des interfaces et à la configuration initiale des adresses IP.

Une fois l'accès à l'interface WebGUI opérationnel, j'ai configuré :

-la passerelle par défaut ;

-le serveur DHCP sur le LAN ;

-les premières règles de pare-feu ;

-la politique NAT pour l'accès Internet des machines internes.

La politique de base retenue reposait sur le principe du "deny all" implicite, en autorisant uniquement les flux nécessaires.

Tests et validation

Afin de valider la configuration, j'ai réalisé plusieurs tests :

-vérification de l'obtention d'une adresse IP via DHCP pour les postes clients ;

-test de connectivité vers Internet depuis le LAN ;

-contrôle du blocage des flux non autorisés ;

-analyse des logs de pare-feu pour vérifier le filtrage effectif.

Les outils intégrés à pfSense, notamment les journaux système et les diagnostics réseau, m'ont permis d'analyser précisément le comportement des règles et d'ajuster la configuration si nécessaire.

Impact sur l'infrastructure

L'introduction de pfSense a profondément structuré l'architecture réseau. L'infrastructure est passée d'un simple réseau virtuel fonctionnel à une topologie segmentée et sécurisée, conforme aux bonnes pratiques professionnelles.

La séparation logique entre WAN, LAN et autres segments a permis de simuler un environnement réaliste d'entreprise, facilitant la compréhension des flux réseau et des mécanismes de sécurité.

Ce déploiement a également constitué la base technique pour des projets ultérieurs, notamment la mise en place de la haute disponibilité via CARP et pfsync.

Bilan et retour d'expérience

Cette situation professionnelle m'a permis de mettre en pratique des compétences essentielles en administration réseau et en sécurité des systèmes.

J'ai acquis une meilleure compréhension :

-du rôle central d'un pare-feu dans une architecture ;

-du fonctionnement du filtrage par états ;

-de la logique de segmentation réseau ;

-de la différence entre une solution logicielle virtualisée et un équipement matériel dédié.

Le fait de travailler dans un environnement entièrement virtualisé m'a permis de multiplier les scénarios de test sans risque matériel, tout en reproduisant des architectures proches de celles rencontrées en entreprise.

Cette expérience constitue une base solide pour évoluer vers des environnements professionnels intégrant des solutions matérielles telles que WatchGuard, Zyxel ou Fortinet.