Mise en place d'un pare-feu avec redondance - PfSense

Sommaire

Cahier des charges – Expression des besoins

Descriptif de l'existant

L'infrastructure est inexistante, j'ai seulement accès à une sortie Internet via le LAN du GRETA.

Besoin(s)

Dans le cadre d'un TP pédagogique, je dois mettre en place deux serveurs pfSense et les synchroniser à l'aide de pfSync. Je dois aussi leur configurer une Virtual IP (VIP) à l'aide de CARP, cela permettra aux clients d'avoir une seule IP comme passerelle par défaut.

Contrainte(s)

J'ai 16 heures pour mettre en place cette solution et tester si le failover et la VIP fonctionnent correctement.

Ressources

Ressources mises à disposition

J'ai à ma disposition une machine hôte qui possède Hyper-V comme logiciel de virtualisation, de plus j'ai accès au réseau LAN du GRETA ce qui me permet d'avoir un accès à Internet.

Ressources nécessaires à la mise en place

J'ai besoin d'une machine hôte qui a un logiciel de virtualisation, j'ai aussi besoin d'un accès à Internet, ainsi que les ISO de pfSense et de Windows 11.

Gestion des ressources

J'ai déjà à ma disposition l'ISO de Windows 11 25H2. Je dois aller chercher l'ISO de pfSense sur Internet.

Analyse

Descriptifs des solutions

PfSense est un pare-feu open-source basé sur FreeBSD. Il propose un ensemble de fonctionnalités avancées telles que le filtrage stateful, le NAT, la gestion de VPN (OpenVPN, IPsec, WireGuard), le DNS Resolver, la haute disponibilité (pfSync), ainsi qu'un large écosystème de packages comme Snort ou Suricata. L'interface d'administration est intuitive

et permet une prise en main efficace. Le produit s'installe aussi bien sur du matériel dédié que dans des environnements virtualisés comme Hyper-V, Proxmox ou VMWare.

Fortinet FortiGate est un pare-feu très complet utilisé dans les entreprises. Il ne sert pas seulement à bloquer ou autoriser des ports, mais il inclut aussi plusieurs protections essentielles comme l'analyse du trafic chiffré, le blocage des sites dangereux, la détection des attaques, l'antivirus, la gestion des VPN et l'analyse des fichiers suspects dans un environnement isolé. L'appareil fonctionne avec FortiOS, un système conçu pour offrir de bonnes performances et un haut niveau de sécurité. Il utilise également FortiGuard, un service qui fournit des mises à jour régulières pour rester protégé contre les nouvelles menaces. Ce type de solution est surtout utilisé dans des environnements professionnels où la sécurité est une priorité absolue.

Comparaison des solutions (tableau)

Fonctionnalités	**PfSense**	**Fortinet FortiGate**
Coûts	Gratuit, support optionnel.	Payant, matériel + licences nécessaires.
OS d'installation	FreeBSD.	OS propriétaire *(FortiOS)*.
Firewall stateful / NAT	Oui.	Oui, optimisé matériellement.
VPN	OpenVPN, IPsec, WireGuard.	IPsec optimisé, SSL-VPN FortiClient.
Haute disponibilité	CARP, pfsync, XMLRPC Sync.	HA Active/Passive ou Active/Active.
IDS/IPS	Oui via plugins *(Snort, Suricata)*.	Natif *(FortiGuard IPS)*.
Filtrage web / antivirus	Limité, dépend de plugins.	Très complet *(WebFilter, AV, filtrage SSL)*.
Support constructeur	Communauté + support Netgate.	Support obligatoire pour signatures et updates.
Intégration UTM	Partielle via plugins.	Complète, orientée NGFW.
Complexité d'installation	Simple et rapide.	Moyenne, dépend du modèle.
Complexité d'utilisation	Moyenne.	Moyen à élever.
Déploiement virtualisé	Excellent.	Possible mais moins flexible.
Open source / Communauté	Oui.	Non.

Choix d'une solution - Argumentation

J'ai choisi PfSense car il s'agit d'une solution open-source et entièrement gratuite, tout en offrant des fonctionnalités de niveau professionnel. Il permet également de déployer une véritable architecture de haute disponibilité grâce à CARP, pfSync et XMLRPC Sync. Ces fonctionnalités rendent possible la mise en place d'un cluster de pare-feu cohérent et efficace, en s'appuyant sur des outils intégrés nativement et sans coût supplémentaire.

Plan d'adressage - Schéma - Tables de routage

- Tableau d'adressage :

Nom du réseau	Adresse réseau	Masque de sous réseau	Première adresse	Dernière adresse	Adresse de broadcast
WAN	172.26.0.0	255.255.248.0 *(/21)*	172.26.0.1	172.26.7.254	172.26.7.255
LAN	192.168.10.0	255.255.255.0 *(/24)*	192.168.10.1	192.168.10.254	192.168.10.255
SYNC	10.0.0.0	255.255.255.252 *(/30)*	10.0.0.1	10.0.0.2	10.0.0.3

- Tableau des IP :

Machines	Interfaces	Adresses IP	Masque	Passerelle	DNS
pfSense-FW1	WAN	192.168.1.2	255.255.255.0	192.168.1.1	1.1.1.1 & 8.8.8.8
	LAN	192.168.10.2	255.255.255.0	⌀	⌀
	SYNC	10.0.0.1	255.255.255.252	⌀	⌀
pfSense-FW2	WAN	192.168.1.3	255.255.255.0	192.168.1.1	1.1.1.1 & 8.8.8.8
	LAN	192.168.10.3	255.255.255.0	⌀	⌀
	SYNC	10.0.0.2	255.255.255.252	⌀	⌀
PC-Client	LAN	192.168.10.10	255.255.255.0	192.168.10.1	1.1.1.1 & 8.8.8.8

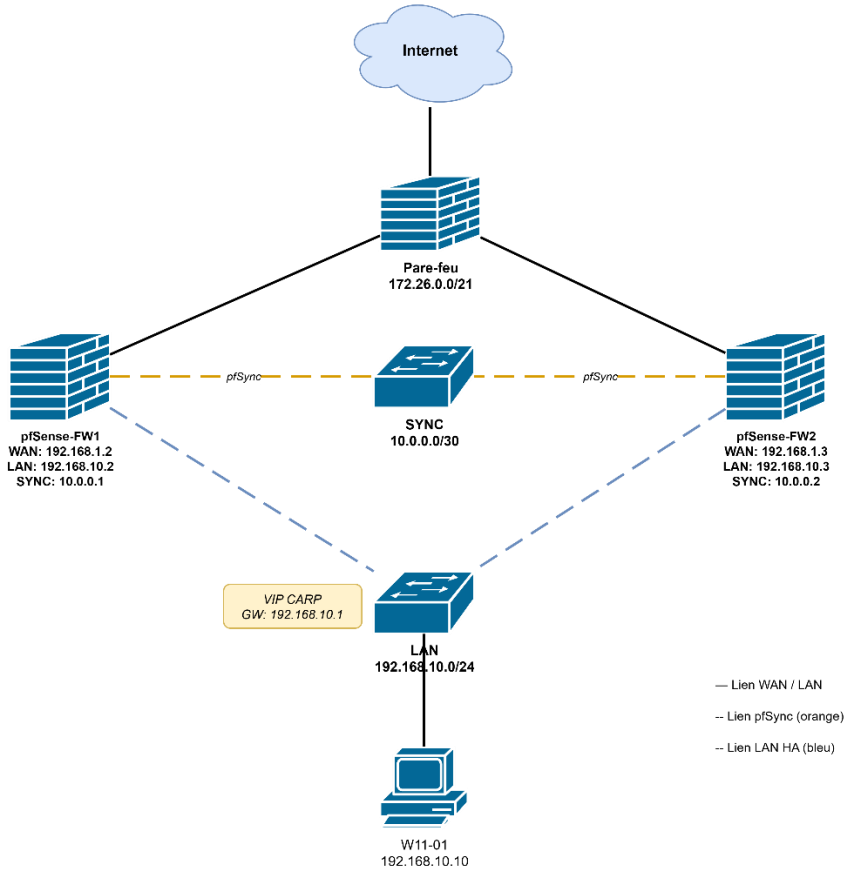
- Table de routage de pfSense-FW1 :

Adresse réseau	Masque réseau	Adresse passerelle	Métrique
192.168.1.0	255.255.255.0	⌀	LINK
192.168.10.0	255.255.255.0	⌀	LINK
10.0.0.0	255.255.255.252	⌀	LINK
0.0.0.0	0.0.0.0	192.168.1.1	1

- Table de routage de pfSense-FW2 :

Adresse réseau	Masque réseau	Adresse passerelle	Métrique
192.168.1.0	255.255.255.0	⌀	LINK
192.168.10.0	255.255.255.0	⌀	LINK
10.0.0.0	255.255.255.252	⌀	LINK
0.0.0.0	0.0.0.0	192.168.1.1	1

Schéma du réseau



Étude de l'impact sur le SI existant

L'intégration de CARP et pfSync dans une infrastructure réseau représente une amélioration majeure de la sécurité et de la disponibilité des pare-feux. Elle apporte de la haute disponibilité, renforce la continuité de service et impacte autant la technique que l'organisation et les responsabilités du service informatique.

- **Impact technique :**

La mise en place de CARP et pfSync nécessite deux pare-feux configurés en cluster sous pfSense, chacun avec des interfaces dédiées (LAN, WAN, SYNC). Une IP virtuelle doit être partagée, et un lien SYNC fiable doit permettre la réplication des sessions et des règles. Ce fonctionnement impose une configuration précise du routage, des VLAN, des certificats et des services réseau. Le cluster devient sensible à la cohérence des versions, aux mises à jour simultanées et à la stabilité du lien SYNC. Une mauvaise configuration peut entraîner une instabilité ou une perte de continuité de service.

- **Impact organisationnel :**

L'arrivée d'un cluster impose de revoir les procédures internes. Toute action (mise à jour, ajout de règle, maintenance) doit être pensée pour fonctionner sur deux nœuds synchronisés. Les changements doivent être coordonnés, documentés et mieux préparés.

- **Impact stratégique :**

CARP et pfSync renforcent fortement la résilience du SI. Les services critiques (VPN, Internet, DMZ, filtrage…) ne dépendent plus d'un seul pare-feu, ce qui réduit les risques d'interruption. Cela améliore la continuité d'activité, un point essentiel pour toute organisation ayant des obligations de disponibilité.

- **Impact humain :**

Les équipes doivent monter en compétence : fonctionnement d'un cluster, bascules, split-brain, bonnes pratiques de maintenance.
Les techniciens doivent être plus rigoureux dans la gestion des configurations et capables de diagnostiquer les incidents liés à la synchronisation ou au basculement entre nœuds. Cette évolution renforce la culture de fiabilité, mais nécessite une période d'adaptation et de formation.

- **Impact juridique**

Même si CARP et pfSync ne manipulent pas directement des données personnelles, ils contribuent à maintenir la disponibilité des services qui protègent ces données, ce qui aide à respecter les obligations (RGPD, normes internes).
La traçabilité devient essentielle : logs des synchronisations, des changements, des bascules. Ces journaux doivent être conservés correctement pour répondre aux audits et permettre une analyse fiable après incident.

Phasage de l'intervention

Je commencerai par installer les deux pfSense et configurer leurs interfaces réseau. J'effectuerai ensuite la configuration de base sur chaque pare-feu, puis je mettrai en place la synchronisation pfSync entre les deux nœuds. Pour finir, je créerai l'adresse IP virtuelle CARP sur le LAN afin d'assurer la haute disponibilité du cluster.

Prévision des tests de validation

Après l'installation et la configuration des deux pfSense, je commencerai par vérifier que chaque pare-feu est accessible via son interface web et que les interfaces WAN, LAN et SYNC utilisent bien les adresses configurées. Je testerai également que les deux équipements répondent correctement aux pings.
Une fois la synchronisation pfSync mise en place et la VIP CARP créée, je testerai la synchronisation pfSync en contrôlant que la VIP CARP créée sur le premier pfSense est bien répliquée automatiquement sur le second.
Enfin, après la création de l'adresse virtuelle CARP, je testerai son bon fonctionnement en accédant au réseau via l'IP virtuelle puis en simulant l'arrêt du pare-feu principal afin de vérifier que la bascule vers le second s'effectue sans interruption du service. Je m'assurerai également que le retour du pfSense principal se fait correctement lorsque celui-ci redevient disponible.

Mise en place

La partie Mise en place a été rédigée sur Notion, vous la trouverez via le lien suivant : https://mathys-demon.notion.site/Configuration-de-CARP-et-pfSync-2b38102ecdc980119b42ebc1bbadb851.

Bilan

Conclusion

L'installation des 2 pfSense avec pfSync et CARP fonctionne en respectant le délai imparti de 16 heures. Les tests de bascule se sont déroulés correctement et automatiquement sans impact pour l'utilisateur.

Auto-évaluation

J'ai réussi à correctement installer et configurer mes 2 serveurs pfSense. J'ai eu un peu de mal à comprendre pourquoi CARP ne fonctionnait pas à cause d'Hyper-V qui bloquait les adresses MAC dans les paramètres des cartes réseaux et la recherche de solutions m'a pris un peu de temps. J'essaierai à l'avenir de prendre moins de temps à trouver mes réponses aux problèmes.