Situation professionnelle
Failover de routeurs sous PfSense

Théo DELETTRE Session 2025 N° candidat : 02345602698

Table des matières

1 Cahier des charges – Expression des besoins

1.1 Descriptif de l'existant

- 8 VLANs (7LAN + 1WAN)
- 1 poste d'administration

1.2 Besoin(s)

- Mise en place de la redondance de pares-feux PfSense.

1.3 Contrainte(s)

- Temps : 4 heures
- Budget : Doit utiliser des solutions gratuites

2 Ressources

2.1 Ressources mises à disposition

- 2 VM pare-feu PfSense autonomes : 1 CPU, 4 Go RAM, 40 Go disque en provisionnement dynamique
- ISO : pfSense-CE-2.7.2-RELEASE-amd64.iso
- Accès administrateur à l'interface web vSphere

2.2 Ressources nécessaires pour la réalisation

- Documentation technique de Netgate sur la redondance de pare-feu

3 Analyse

3.1 Descriptifs des solutions

1. Redondance via CARP (Common Address Redundancy Protocol) :
   - Description : Mise en place d'un cluster de deux pare-feux pfSense configurés avec CARP, permettant la bascule automatique en cas de panne du pare-feu principal.
   - Avantages : Haute disponibilité, bascule automatique transparente pour les utilisateurs, IP virtuelle partagée.
   - Inconvénients : Configuration plus technique, nécessite que les deux pare-feux soient sur le même sous-réseau, synchronisation des paramètres à maintenir.

2. Doubles pares-feux indépendants :
   - Description : Deux pares-feux fonctionnent séparément, et le basculement s'effectue manuellement ou via redondance des routes dans les équipements réseaux.
   -
   - Avantages : Mise en œuvre simple, pas de configuration CARP.
   -
   - Inconvénients : Basculement manuel ou non instantané, risques d'interruption de service plus élevés.

3.2 Comparaison des solutions

Critère	Solution 1 (CARP)	Solution 2 (Indépendants)
Haute disponibilité	Oui	Non (ou manuelle)
Complexité de mise en place	Élevée	Faible
Maintenance	Moyenne	Moyenne à élevée
Coût matériel	Équivalent	Équivalent
Réactivité en cas de panne	Immédiate	Retardée (intervention humaine)

3.3 Choix d'une solution

Solution choisie : Redondance via CARP

Argumentation :

La solution CARP permet une véritable haute disponibilité réseau en assurant une continuité de service même en cas de défaillance d'un des deux pare-feux. Elle offre une configuration robuste avec synchronisation automatique des règles de pare-feu, des alias et des services. Bien qu'un peu plus complexe à mettre en œuvre, elle reste la plus adaptée aux besoins d'un environnement professionnel nécessitant fiabilité, résilience et automatisation du basculement.

3.4 Plan d'adressage – Schéma – Tables de routage

LANs :

LAN	LAN Vswitch	Plage d'adresses (CIDR)	Capacité d'hôtes	Plage DHCP
LAN2 - Critique (inclut Backups)	GRETA-LAN-2080	192.168.2.0/24	254	X
LAN3 - Serveurs	GRETA-LAN-2081	192.168.3.0/24	254	X
LAN4 - Supervision	GRETA-LAN-2082	192.168.4.0/24	254	X
LAN5 - Utilisateurs	GRETA-LAN-2083	192.168.5.0/24	254	192.168.5.10 - 192.168.5.240
LAN6 - Guest (Réseau invité avec vouchers)	GRETA-LAN-2084	192.168.6.0/24	254	192.168.6.10 - 192.168.6.240
LAN99 - HA/PfSync	GRETA-LAN-2085	192.168.99.0/24	254	X
LAN100 - DMZ	GRETA-DMZ-2089	192.168.100.0/24	254	X
WAN (routeur)	WAN_GRETA	192.168.20.0/24	254	X
LAN Distant	X	172.16.10.0/24	254	172.16.10.10 - 172.16.10.240

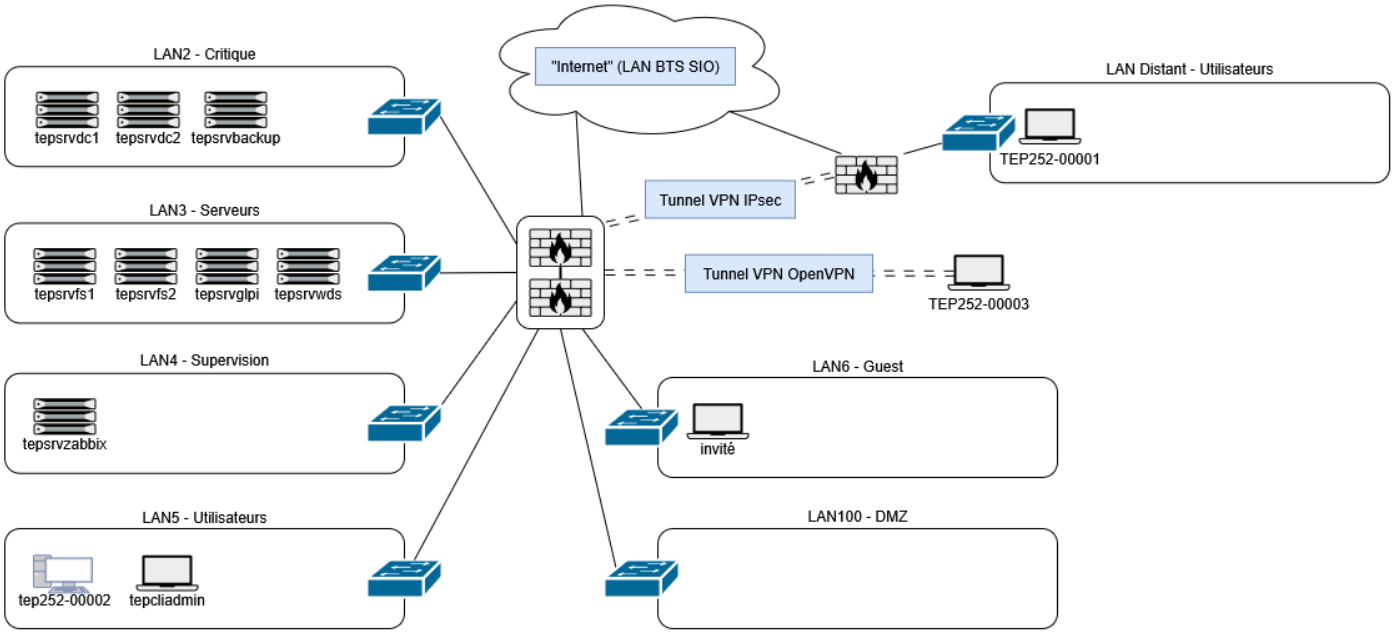
Site principal :

Nom machine	Nom DNS	LAN2	LAN3	LAN4	LAN5	LAN6	LAN99 (PFSYNC)	LAN100 (DMZ)	WAN
UFA208-PfSense-Primary	pfSense-Primary	192.168.2.252	192.168.3.252	192.168.4.252	192.168.5.252	192.168.6.252	192.168.99.1	192.168.100.252	192.168.20.108
UFA208-PfSense-Secondary	pfSense-Secondary	192.168.2.253	192.168.3.253	192.168.4.253	192.168.5.253	192.168.6.253	192.168.99.2	192.168.100.253	192.168.20.109
(IP virt PfSense)	x	192.168.2.254	192.168.3.254	192.168.4.254	192.168.5.254	192.168.6.254	x	192.168.100.254	192.168.20.208
UFA208-tepcliadmin	tepcliadmin.teppe.local	x	x	x	DHCP	x	x	x	x
UFA208-tepsrvdc1	tepsrvdc1.teppe.local	192.168.2.1	x	x	x	x	x	x	x
UFA208-tepsrvdc2	tepsrvdc1.teppe.local	192.168.2.2	x	x	x	x	x	x	x
UFA208-tepsrvbackup	tepsrvbackup.teppe.local	192.168.2.3	x	x	x	x	x	x	x
UFA208-tepsrvfs1	tepsrvdc1.teppe.local	x	192.168.3.1	x	x	x	x	x	x
UFA208-tepsrvfs2	tepsrvdc1.teppe.local	x	192.168.3.2	x	x	x	x	x	x
UFA208-tepsrvwds	tepsrvdc1.teppe.local	x	192.168.3.3	x	x	x	x	x	x
UFA208-tepsrvglpi	glpi.teppe.local	x	192.168.3.4	x	x	x	x	x	x
UFA208-tepsrvzabbix	zabbix.teppe.local	x	x	192.168.4.1	x	x	x	x	x
UFA208-tep252-00002	tep252-00002.teppe.local	x	x	x	DHCP	x	x	x	x
UFA208-invité		x	x	x	x	DHCP	x	x	x

Site distant – postes nomades :

Nom machine	Nom DNS	LAN	WAN (LAN BTS SIO)
PfSense-SiteDistant	PfSense-Site-Distant	172.16.10.254	DHCP
TEP252-00001	TEP252-00001.teppe.local	DHCP	x
TEP252-00003	TEP252-00003.teppe.local	x	DHCP

Topologie :



3.5 Etude de l'impact sur le SI existant

- Sécurité : L'accès à l'interface d'administration reste restreint et sécurisé par des comptes dédiés. La redondance ne diminue pas le niveau de sécurité existant.
- Performance : L'impact sur les performances est négligeable. Le pare-feu secondaire reste en veille active via CARP sans traitement actif du trafic.
- Organisationnel : Amélioration significative de la disponibilité des services réseau. La continuité d'accès est assurée même en cas de défaillance du pare-feu principal.

3.6 Phasage de l'intervention

1. Configuration CARP : Mise en place des adresses IP virtuelles, configuration de la synchronisation XMLRPC (règles, alias, DHCP, etc.).
2. Tests de basculement : Simulations de panne pour valider la reprise automatique.

3.7 Prévision des tests de validation

Test	Attendu	Résultat prévu
Basculement automatique CARP	Le pare-feu secondaire prend le relais en cas de panne	OK
Synchronisation des règles	Les règles créées sur le primaire apparaissent sur le secondaire	OK
Tests de connectivité LAN/WAN	Aucune coupure détectée lors des tests	OK

3.8 Déploiement

Une procédure de configuration de la redondance pfSense sont détaillées dans le document suivant :

https://theodelettre.fr/wp-content/uploads/2025/05/Configuration-du-failover-sous-PfSense.pdf

4 Mise en place

4.1 Réalisation

- Déploiement de deux instances PfSense (maître et esclave) dans le réseau
- Configuration du protocole CARP pour l'IP virtuelle partagée
- Synchronisation automatique de la configuration (firewall rules, NAT, DHCP, etc.)
- Ajout d'une interface de synchronisation dédiée (Sync) entre les deux PfSense
- Test de bascule automatique (failover) en cas de panne du PfSense principal

4.2 Rapport de tests

Test	Procédure	Résultat attendu	Résultat obtenu	Statut
Test de bascule automatique (failover)	Éteindre le PfSense maître	L'IP virtuelle CARP bascule sur l'esclave	Bascule effectuée avec succès	Réussi
Test de synchronisation de configuration	Ajouter une règle NAT sur le PfSense maître	La règle se réplique automatiquement sur le PfSense esclave	Réplication fonctionnelle	Réussi
Test de continuité Internet	Naviguer depuis un poste client durant une bascule	Aucune coupure de connexion observée	Connexion maintenue	Réussi
Test d'accès à l'interface CARP	Accéder à l'interface via l'IP virtuelle	Interface d'administration disponible	Accès réussi	Réussi
Test de redémarrage d'un pare-feu	Redémarrer le PfSense maître, puis l'esclave	Le service reste accessible et l'IP CARP reste active	Fonctionnement correct	Réussi

4.3 Rapport de déploiement

Le déploiement s'est déroulé comme prévu :

- Les deux pare-feux pfSense ont été installés, configurés et interconnectés.
- La redondance CARP a été testée et validée, avec basculement automatique confirmé.
- Les règles de pare-feu, NAT, VPN et DHCP sont désormais synchronisées via XMLRPC.

5 Bilan

5.1 Conclusion

La mise en place de la redondance CARP sur les pare-feux pfSense améliore considérablement la résilience du réseau. En cas de défaillance matérielle ou logicielle du pare-feu principal, le secondaire prend automatiquement le relais sans interruption de service. Cette solution garantit une disponibilité élevée, tout en assurant une gestion centralisée des règles de sécurité et des configurations. Elle constitue un fondement essentiel pour un système d'information fiable.

5.2 Auto-évaluation

Points positifs : bonne documentation.

Points à améliorer : ajouter le support LDAP pour authentification centralisée, mettre en place des sauvegardes automatiques.