LEIDOSCOPE

Étude préalable – Phase 1

Suppression du SPOF de la sortie Internet

BTS SIO option SISR – Bloc 2 – AP2
Groupe 3 : Deniz ELHASOGLU, Nathan OGORECK
Campus Carlo Acutis, Vernon – Novembre 2026

1. Contexte

Objectif : supprimer le SPOF (Single Point Of Failure) de la zone Internet.

Un SPOF est un élément qui, s'il tombe, fait tomber tout le service, faute de solution de secours.

Avant le projet, la sortie Internet reposait sur une seule chaîne : pare-feu → RNET1 → FAI1. La route par défaut du pare-feu pointait directement sur RNET1 (192.168.3.252). RNET1 et FAI1 étaient donc chacun un SPOF : une seule panne coupait Internet pour tout le site.

Après le projet, un second chemin existe (RNET2 → FAI2), et HSRP bascule automatiquement de l'un à l'autre.

La phase 1 comprend trois étapes :

- recensement des pannes possibles ;
- moyens matériels à mettre en place ;
- impact sur l'infrastructure existante.

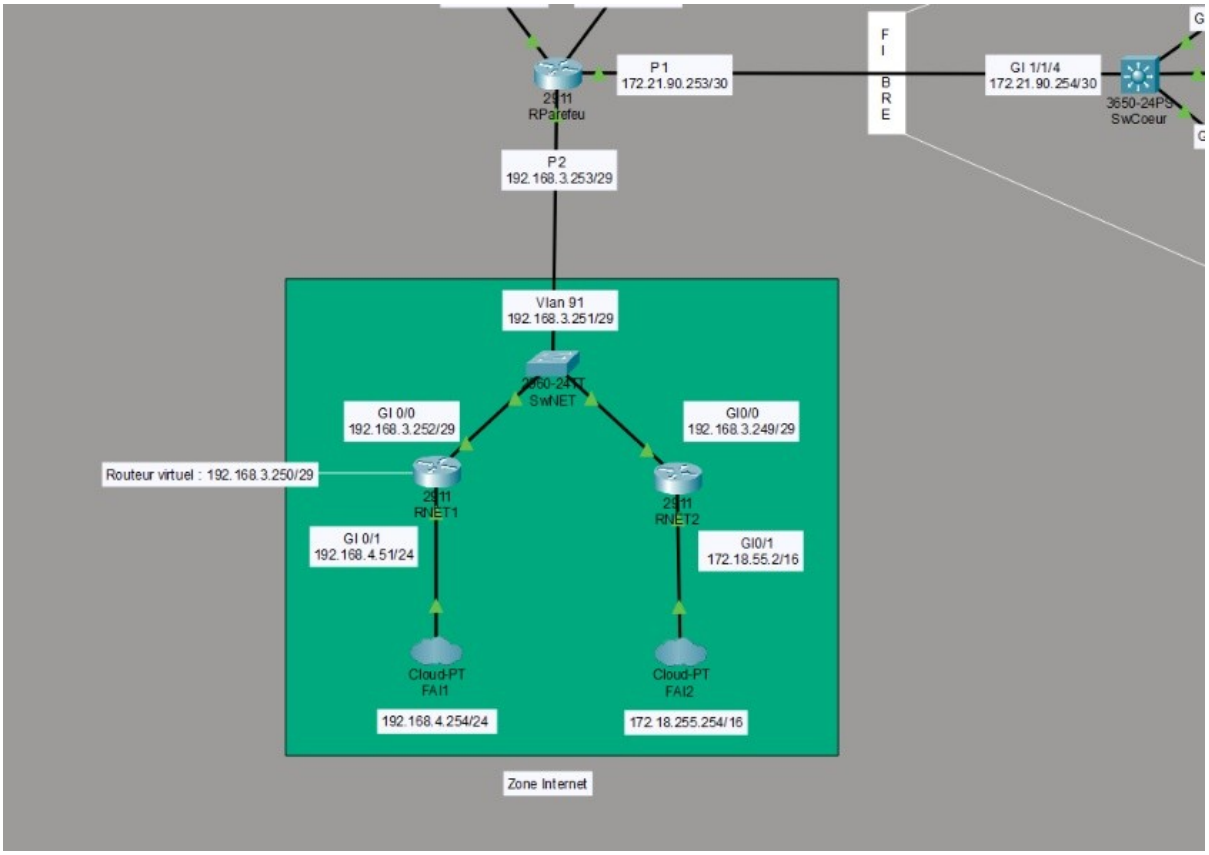

Schéma de la zone Internet après le projet

2. Recensement des pannes possibles

Pour chaque panne : ce qui la détecte, le résultat attendu et le test qui le prouve (voir le rapport de tests).

Panne	Détection	Résultat	Test
RNET1 tombe, ou son câble vers SwNET est coupé	RNET2 ne reçoit plus les hello HSRP	RNET2 devient actif	T04 – validé

Panne	Détection	Résultat	Test
Câble WAN de RNET1 (Gi0/1) débranché	Track 1 (interface) et track 2 (IP SLA)	RNET2 devient actif, sortie par FAI2	T06 – validé
FAI1 en panne, câble toujours branché	Track 2 seul (IP SLA vers 192.168.4.254)	RNET1 passe à 80, RNET2 actif, sortie par FAI2	T07 – validé
Retour à la normale	Les suivis repassent Up	RNET1 reprend la main (preempt)	T05 – validé

Pannes non couvertes

- **SwNET :** s'il tombe, les deux routeurs perdent leur côté LAN. Il reste un SPOF.
- **Pare-feu :** il est seul entre le LAN et les routeurs. C'est aussi un SPOF, hors du périmètre du projet.
- **FAI2 pendant que RNET1 est actif :** RNET2 n'a pas de suivi, donc rien ne signale sa panne. C'est sans conséquence tant que RNET1 fonctionne.

3. Moyens à mettre en place

Matériel

Moyen	Détail	Pourquoi
Second routeur	RNET2, Cisco 2911 comme RNET1, configuré de zéro	Doubler le routeur de sortie
Second accès Internet	FAI2, passerelle 172.18.255.254	Doubler le fournisseur
Switch de raccordement	SwNET, VLAN 91, ports Gi1/0/1 à 1/0/3	Relier pare-feu, RNET1 et RNET2 sur le même réseau
Câblage	RNET2 vers SwNET (Gi1/0/3) et RNET2 vers FAI2	Raccorder le nouveau routeur
Adresses IP	192.168.3.249 pour RNET2, 192.168.3.250 pour l'IP virtuelle, 172.18.55.2 à .7 côté FAI2	Prises dans les plages libres existantes

Logiciel

Uniquement de la configuration, sans matériel à acheter : HSRP, IP SLA et suivi d'objets, NAT/PAT sur RNET2, RIP v2 et SSH.

4. Impact sur l'infrastructure existante

L'impact est faible : trois équipements existants sont modifiés, et les postes clients n'ont rien à changer.

Équipement	Modification	Impact
Pare-feu Zyxel	Route par défaut changée de 192.168.3.252 à 192.168.3.250	Une seule ligne, brève coupure au moment du changement
RNET1	Ajout de HSRP, de l'IP SLA et des suivis sur la configuration AP1	Rien de supprimé : IP, NAT et RIP inchangés
SwNET	Ports Gi1/0/1 à 1/0/3 en access VLAN 91	Un port en plus pour RNET2

Équipement	Modification	Impact
Postes clients	Aucune	Ils passent toujours par le pare-feu

Effets à connaître après une bascule

- Les connexions en cours sont coupées : les traductions NAT sont sur RNET1, RNET2 ne les connaît pas.
- Le serveur 10.51.10.11 change d'adresse publique (192.168.4.59 → 172.18.55.7).
- Les réseaux 10.51 et 10.52 ne sont pas dans l'ACL NAT de RNET2 : à aligner s'ils doivent sortir sur Internet.

Précautions prises

- Intervention sur RNET1 sans toucher à l'existant.
- Sauvegarde de la configuration (write memory, sauvegardes kron vers le serveur TFTP).
- Tests après chaque étape (T01 à T07).