BTS SERVICES INFORMATIQUES AUX ORGANISATIONS (SIO)

Option SISR – Épreuve E6 : Parcours de professionnalisation

Ressource :	Documentation Technique – Réalisation Professionnelle n°2 (RP2)
Sujet :	Mise en place d'une infrastructure réseau sécurisée en Haute Disponibilité (Cluster CARP / pfsync) sous pfSense pour le Port de Cherbourg
Candidat :	Vandesquille Axel
Établissement :	Lycée Saint-Exupéry – Saint-Raphaël

1. Contexte et Architecture Réseau Virtualisée

1.1 Justification du besoin et de la solution

Dans le cadre de la modernisation et de la sécurisation des infrastructures du Port de Cherbourg, la continuité de service des flux réseaux et des accès internes/externes est une priorité absolue. Afin de pallier tout dysfonctionnement matériel ou logiciel sur la passerelle principale sans interrompre l'activité des utilisateurs, l'implémentation d'un cluster de pare-feux redondants s'est avérée indispensable.

La solution retient l'usage de deux instances virtuelles de l'IUT de sécurité **pfSense** configurées en mode Haute Disponibilité (HA). Ce choix permet d'assurer un basculement transparent des flux grâce à l'association de trois protocoles majeurs :

- **CARP (Common Address Redundancy Protocol) :** Permet le partage d'adresses IP virtuelles (VIP) redondées entre les deux pare-feux.
- **pfsync :** Assure la réplication en temps réel des tables d'états de connexions (State Table).
- **XMLRPC :** Automatise la synchronisation complète des configurations (règles de filtrage, NAT, alias) du Master vers le Slave.

Pour des raisons de flexibilité et de validation d'architecture ("Proof of Concept"), l'intégralité de la maquette est réalisée au sein d'un environnement 100 % virtualisé sous l'hyperviseur Oracle VM VirtualBox.

1.2 Plan d'adressage Réseau du Cluster

Le déploiement s'appuie sur quatre réseaux distincts isolés par des commutateurs virtuels ("Réseau interne" dans l'hyperviseur) :

Équipement / Interface	Réseau IP (CIDR)	IP Physique Master	IP Physique Slave	IP Virtuelle CARP (VIP)
WAN (Accès Extérieur)	192.168.1.0/24 (DHCP)	192.168.1.41	192.168.1.5	**172.17.102.250** (VHID 100)
LAN (Utilisateurs internes)	192.168.3.0/24	192.168.3.254	192.168.3.253	**192.168.3.252** (VHID 101)
OPT1 (Zone DMZ)	192.168.2.0/24	192.168.2.254	192.168.2.253	**192.168.2.251** (VHID 102)
OPT2 (Lien Synchro pfsync)	192.168.4.0/24	192.168.4.1	192.168.4.2	*Aucune (Lien direct)*
VM Cliente de test (LAN)	192.168.3.0/24	192.168.3.55	N/A	Passerelle : 192.168.3.252

2. Procédure de Configuration pas à pas

2.1 Configuration de l'environnement virtuel (Hyperviseur)

Chaque VM pfSense est provisionnée avec 4 cartes réseau configurées de la manière suivante :

- **Carte 1 (WAN) :** Mode Accès par pont (Bridge) ou NAT (interfacé sur la box physique pour simuler Internet).
- **Carte 2 (LAN) :** Mode Réseau interne, Nom : `LAN-Réseau`.
- **Carte 3 (OPT1) :** Mode Réseau interne, Nom : `DMZ-Réseau`.
- **Carte 4 (OPT2) :** Mode Réseau interne, Nom : `PFSYNC-Lien`.

> ***Note de sécurité cruciale :*** *Dans les paramètres avancés de chaque carte en réseau interne, le* ***Mode de promiscuité*** *est positionné sur* ***« Autoriser tout » (Allow All)*** *afin de permettre aux trames CARP de transiter correctement d'une interface virtuelle à l'autre.*

2.2 Initialisation des adresses physiques et accès LAN

1. Attribution des adresses IPv4 physiques statiques depuis le menu console (Options `2) Set interface(s) IP address`) sur les deux nœuds conformément au plan d'adressage.
2. Connexion à l'interface d'administration Web (WebGUI) depuis la VM cliente située dans le LAN via l'adresse `https://192.168.3.254` (Master) puis `https://192.168.3.253` (Slave).

2.3 Configuration de la synchronisation XMLRPC et pfsync (Sur le Master)

Afin d'unifier la politique de sécurité, la réplication automatique est activée :

1. Navigation vers **System > High Avail. Sync**.

2. Activation du protocole sur l'interface de synchronisation dédiée :
   - Enclenchement de la case *Synchronize States*.
   - *Synchronize Interface :* `OPT2 (pfsync)`.
   - *pfsync Synchronize Peer IP :* `192.168.4.2` (IP du Slave).
3. Renseignement des paramètres de réplication des configurations (XMLRPC Sync) :
   - *Synchronize Config to IP :* `192.168.3.253`.
   - *Remote System Username/Password :* Identifiants d'administration du Slave.
   - Sélection des options à synchroniser (*Firewall Rules*, *Nat Configuration*, *Virtual IPs*).

2.4 Création des adresses IP Virtuelles CARP

Les VIP partagées qui feront office de passerelles résilientes sont configurées depuis l'interface du Master (et répliquées sur le Slave) via le menu **Firewall > Virtual IPs > Add** :

- **Type :** CARP
- **Interface LAN :** IP `192.168.3.252` / Masque `/24` / Password du cluster / VHID : `101`.
- **Interface DMZ (OPT1) :** IP `192.168.2.251` / Masque `/24` / Password du cluster / VHID : `102`.
- **Interface WAN :** IP `172.17.102.250` / Masque `/24` / Password du cluster / VHID : `100`.

2.5 Sécurisation par le NAT Sortant Hybride (Outbound NAT)

Pour garantir le maintien des accès Internet lors d'une bascule, le masquage d'adresses doit impérativement s'effectuer derrière la VIP du WAN et non l'IP propre du Master :

1. Direction **Firewall > NAT > Outbound**.
2. Sélection du mode **Création hybride de règles NAT sortantes (Hybrid Outbound NAT)**.
3. Modification ou validation des règles automatiques de mappage pour que le champ *Translation / Target Address* pointe exclusivement sur la **VIP WAN (`172.17.102.250`)**.

3. Procédures de Vérification et de Validation (Démonstration Jury)

3.1 Validation des rôles d'état CARP

La page de diagnostic **Status > CARP** permet de s'assurer de la bonne distribution de la charge au sein du cluster :

- **Sur l'hôte Master :** L'écran indique explicitement l'état **« MASTER »** sur l'ensemble des VIP (WAN, LAN, DMZ). Le pare-feu intercepte et traite activement les flux.
- **Sur l'hôte Slave :** L'écran indique l'état **« BACKUP »**. Les interfaces virtuelles sommeillent en écoutant les paquets de "Heartbeat" émis par le Master.

3.2 Validation de la synchronisation des règles

Toute modification apportée sur le pare-feu de tête (ex: ajout d'une règle d'autorisation sur l'interface LAN) se répercute instantanément sur le second nœud. Sur le pfSense Slave, les règles apparaissent automatiquement sous l'onglet **Firewall > Rules > LAN**.

3.3 Validation du suivi des connexions (pfsync)

Le diagnostic de la table des états (**Diagnostics > États**) permet de prouver la réplication temps réel : lorsqu'une VM cliente initie un flux persistant (ex: flux ICMP ou téléchargement), la session réseau associée à l'adresse IP source du client (`192.168.3.55`) est visible simultanément en mémoire sur le Master et sur le Slave.

3.4 Simulation de panne et comportement normal ("Crash Test")

Lors de la coupure physique ou logicielle du nœud Master (simulation par déconnexion du câble virtuel de l'interface LAN dans VirtualBox ou activation du "Mode de maintenance CARP") :

1. Le pfSense Slave détecte l'absence de trames Heartbeat en moins de 3 secondes.
2. Le Slave fait basculer instantanément le statut de ses VIP de `BACKUP` à `MASTER`.
3. La VM cliente, configurée avec la passerelle virtuelle `192.168.3.252`, ne subit aucune interruption de service visible (perte maximale d'un seul paquet réseau lors de la convergence).