RÉALISATION PROFESSIONNELLE N°1

Sécurisation et haute disponibilité de l'infrastructure réseau

Documentation technique de la mission menée pour l'organisation cliente DEPANMOI.FR, élimination du SPOF, redondance HSRP, agrégation LACP, routage OSPF, distribution DHCP en split-scope et durcissement SSH.

VERSION INTÉGRALE

CANDIDAT
LOPES--DA SILVA, Lucas

N° CANDIDAT
02251770429

CENTRE DE FORMATION
SCHOLA NOVA

PÉRIODE DE RÉALISATION
Janvier, Février 2026

MODALITÉ
Réalisation conduite en équipe

FORME DE L'ÉPREUVE
Épreuve ponctuelle

TABLE DES MATIÈRES

Sommaire

PARTIE 8 Annexes

PARTIE 1

Présentation du contexte client

1.1 · L'organisation DEPANMOI.FR

DEPANMOI.FR est une TPE lyonnaise spécialisée dans le dépannage informatique, la maintenance de parcs et le conseil technologique. Elle adresse à la fois une clientèle de professionnels, PME locales sous contrat de maintenance, et une clientèle de particuliers, notamment des personnes âgées peu familières avec les outils numériques. La structure se positionne donc comme un prestataire de proximité dont la valeur ajoutée repose sur sa réactivité d'intervention et la confiance des clients dans la continuité du service rendu.

Fiche d'identité

Raison sociale	DEPANMOI.FR
Activité	Dépannage informatique, maintenance de parcs, conseil technologique
Siège social et atelier	15 Avenue de la République, 69007 Lyon
Chiffre d'affaires	200 000 € (dernier exercice clos), en croissance constante
Effectif	4 collaborateurs
Composition de l'équipe	1 gérant · 2 techniciens systèmes et réseaux · 1 secrétaire comptable
Portefeuille clients	20 clients actifs (PME locales et particuliers)

Bien que de taille modeste, l'organisation est **entièrement dépendante de son système d'information** pour son fonctionnement quotidien : prise de tickets clients, devis et facturation, accès aux ressources techniques (firmwares, drivers, base de connaissances), messagerie professionnelle. Toute interruption du SI se traduit immédiatement par un arrêt de production, ce qui justifie un niveau d'exigence sur la disponibilité supérieur à ce que l'on observe habituellement dans une TPE de ce gabarit.

1.2 · Le système d'information existant

Avant la mission, l'infrastructure réseau de DEPANMOI.FR repose sur un **équipement unique** assurant à la fois la commutation locale et la passerelle vers le pare-feu pfSense, lui-même connecté au lien FAI. Tous les postes de l'organisation, bureautique du gérant et de la secrétaire d'un côté, postes techniques de l'atelier de l'autre, sont raccordés sur ce même équipement, sans segmentation.

Composant existant	Rôle actuel	Limite identifiée
Switch unique	Commutation locale et passerelle par défaut pour tous les postes	Point de défaillance unique (SPOF)
Pare-feu pfSense	Filtrage, NAT et sortie Internet vers le lien FAI	Conservé et reconfiguré dans la cible (FRR/OSPF)
Postes utilisateurs	Bureautique (gérant, secrétaire), atelier technique (2 techniciens)	Aucune isolation entre flux administratifs et techniques
Adressage IP	Plage unique distribuée manuellement	Pas de plan d'adressage formalisé, pas d'automatisation

Cette architecture, fonctionnelle mais fragile, n'offre **aucun mécanisme de tolérance de panne** et ne permet pas non plus d'isoler les flux entre les différents métiers. Elle constitue le point de départ, l'« avant », de la mission.

1.3 · Problématique

L'infrastructure actuelle présente un **point de défaillance critique** (SPOF) : la défaillance matérielle ou logicielle de l'équipement réseau central provoque l'arrêt de l'ensemble de l'activité. Pour une TPE de dépannage informatique, dont l'image de marque repose précisément sur la fiabilité technique, cette situation constitue à la fois un risque opérationnel et un risque réputationnel.

CONSÉQUENCES MESURABLES D'UNE PANNE DU SPOF

- **Impossibilité d'enregistrer ou de planifier les tickets d'intervention** client.
- **Arrêt de la facturation et de la messagerie professionnelle** : devis et factures ne peuvent plus être émis ni reçus.
- **Perte d'accès aux ressources techniques en ligne** (firmwares, drivers, bases de connaissances), les techniciens deviennent inopérants y compris en intervention sur site.
- **Atteinte à l'image de marque** : une TPE de dépannage informatique en panne informatique constitue un message difficile à tenir vis-à-vis des clients sous contrat.
- **Coût d'arrêt** estimé à plusieurs centaines d'euros par heure ouvrée (perte de chiffre d'affaires + heures techniciens immobilisés + remise commerciale éventuelle).

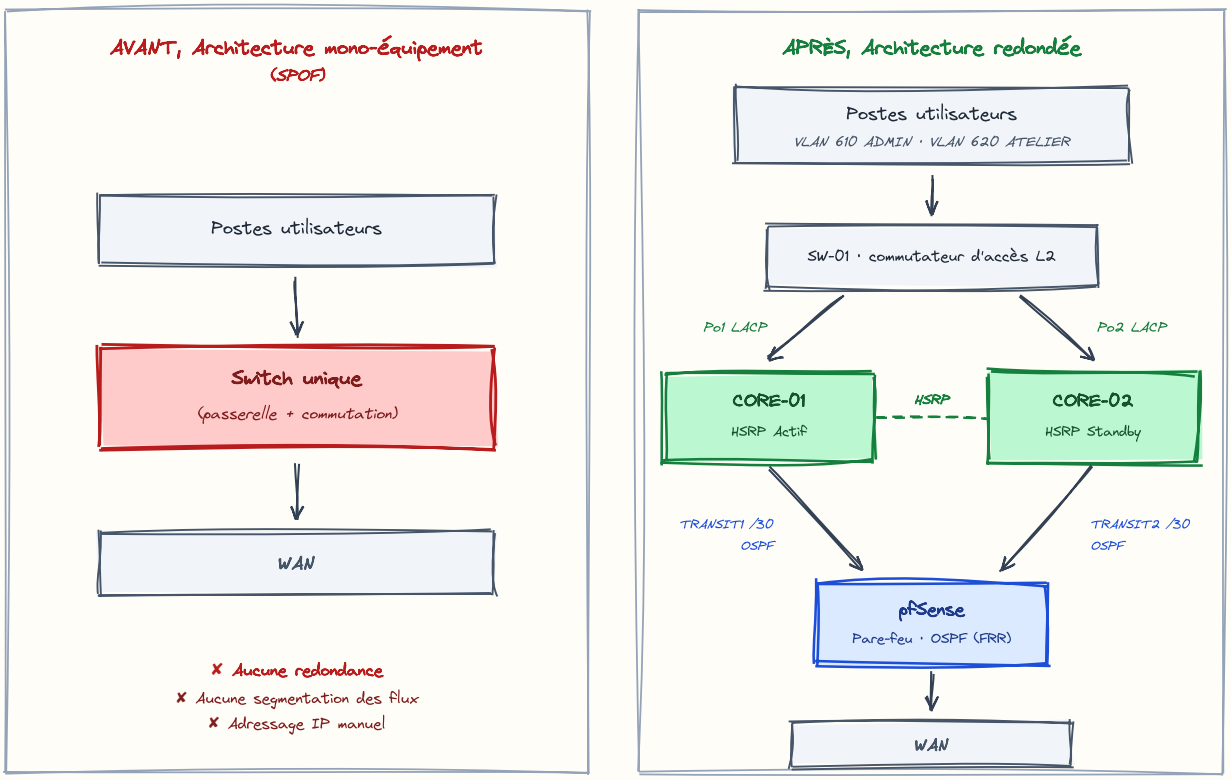


Figure 1.1 · Architecture réseau DEPANMOI.FR avant et après la mission.

1.4 · Objectifs de la mission

Cinq objectifs opérationnels ont été définis avec le gérant. Chacun est associé à un indicateur de réussite mesurable, qui sera vérifié lors du plan de tests (partie 5 de la documentation).

Objectif	Description	Critère de réussite mesurable
O1, Redondance de passerelle	Éliminer le SPOF en mettant en œuvre une redondance de passerelle entre deux commutateurs L3 via le protocole HSRP.	Bascule automatique de la passerelle virtuelle (VIP) en moins de 10 s en cas de coupure du cœur actif, sans perte de session utilisateur perceptible.
O2, Segmentation des flux	Séparer logiquement les flux administratifs et techniques par la création de deux VLAN dédiés (ADMIN et ATELIER).	Aucun trafic direct possible entre les deux VLAN sans passage par la passerelle ; plan d'adressage formalisé sur deux blocs /25 distincts.
O3, Agrégation de liens	Optimiser la bande passante et la résilience entre le commutateur d'accès et chaque commutateur de cœur via LACP.	Bande passante doublée (2 liens physiques agrégés en un EtherChannel) ; basculement transparent à la coupure d'un lien physique.
O4, Routage dynamique	Automatiser la propagation des routes internes et de la route de sortie via OSPF.	Convergence du protocole en moins de 5 s après un changement de topologie ; aucune route statique résiduelle en dehors de la route par défaut publiée.
O5, Distribution DHCP	Automatiser l'adressage IP des postes par DHCP hébergé directement sur les commutateurs L3, avec exclusion des plages d'adresses statiques.	100 % des postes obtiennent un bail DHCP valide dans le bon VLAN ; aucune collision d'adresse avec les équipements statiques.
O6, Sécurisation des accès	Désactiver le protocole Telnet et imposer un accès d'administration en SSH v2 sur tous les équipements.	Aucun équipement n'accepte de connexion Telnet ; authentification SSH v2 fonctionnelle avec mot de passe robuste et chiffrement actif.

PARTIE 2

Cahier des charges technique

2.1 · Périmètre fonctionnel

La mission porte exclusivement sur la **couche réseau** de l'infrastructure DEPANMOI.FR. Elle vise à doter l'organisation d'un cœur redondé, segmenté, automatisé et sécurisé, en réutilisant le matériel existant (deux Cisco Catalyst 3750-X, un Cisco Catalyst 2950, un boîtier pfSense Netgate) et sans modification du contrat passé avec le fournisseur d'accès Internet.

Six services réseau composent le périmètre fonctionnel de la solution cible :

1. **Segmentation** du réseau en deux VLAN (ADMIN et ATELIER) avec plan d'adressage formalisé.
2. **Redondance de la passerelle par défaut** par HSRP entre CORE-01 et CORE-02 pour chaque VLAN.
3. **Agrégation des liens d'accès** entre SW-01 et chaque cœur via LACP.
4. **Routage dynamique interne** par OSPFv2 entre les cœurs et le pare-feu pfSense.
5. **Distribution automatique d'adressage IP** par service DHCP hébergé sur les cœurs.
6. **Sécurisation des accès d'administration** par désactivation de Telnet et activation de SSH v2.

La distinction entre ce qui est inclus dans la mission et ce qui en est explicitement exclu est synthétisée ci-dessous :

✓ DANS LE PÉRIMÈTRE

- Configuration des deux commutateurs L3 et du commutateur d'accès
- Configuration du pare-feu pfSense (interfaces, OSPF/FRR, règles de transit)
- Plan d'adressage IPv4 et nommage des équipements
- Procédure de mise en œuvre et plan de tests
- Documentation technique et configurations archivées

✘ HORS PÉRIMÈTRE

- Postes clients (Windows / Linux) et leurs applicatifs métier
- CRM, comptabilité, messagerie
- Sauvegardes applicatives et données métier
- Contrat FAI et redondance WAN
- Sécurité applicative (IDS / IPS, antivirus, EDR)

2.2 · Exigences fonctionnelles

Les exigences fonctionnelles décrivent *ce que la solution doit faire*. Chacune est identifiée par un code `EF-XX`, priorisée selon la méthode MoSCoW et associée à un critère de validation testable lors de la phase de recette (partie 5).

MUST
Exigence non négociable
, la solution est rejetée si elle n'est pas remplie.

SHOULD
Exigence importante
, la solution fonctionne sans, mais sa qualité serait dégradée.

COULD
Exigence optionnelle
, réalisée si le temps et le contexte le permettent.

~~WON'T~~
Exclusion explicite
, décision assumée de ne pas traiter dans ce projet.

EF-01 Segmentation du réseau en deux VLAN — MUST

Le réseau interne doit être segmenté en deux VLAN distincts pour isoler les flux administratifs (gérant, secrétaire) des flux techniques (atelier). Chaque VLAN dispose d'un bloc IPv4 dédié de masque /25 prélevé sur le subnet 192.168.10.0/24, avec un nommage explicite et une numérotation cohérente avec la convention interne.

CRITÈRE DE VALIDATION

Les VLAN `610 ADMIN` (192.168.10.0/25) et `620 ATELIER` (192.168.10.128/25) sont créés et opérationnels sur les trois équipements. Aucun trafic direct n'est possible entre un poste du VLAN 610 et un poste du VLAN 620 sans transit par la passerelle, vérifié par capture de trafic et test `ping` dans les deux sens.

EF-02 Redondance de la passerelle par défaut (HSRP) — MUST

La passerelle par défaut de chaque VLAN doit être virtualisée par HSRP entre CORE-01 et CORE-02. Une VIP unique par VLAN est annoncée aux postes clients ; en cas de défaillance du cœur Actif, le cœur Standby doit reprendre la main automatiquement, sans intervention humaine et sans modification de configuration sur les postes.

CRITÈRE DE VALIDATION

La VIP de chaque VLAN répond après bascule automatique en moins de **10 secondes** suite à la coupure du cœur Actif (test par arrêt de l'interface concernée). Les sessions TCP des postes clients doivent reprendre sans intervention de l'utilisateur.

EF-03 Préemption HSRP du cœur préférentiel

SHOULD

Le cœur déclaré préférentiel (CORE-01, priorité plus élevée) doit reprendre automatiquement le rôle Actif après réparation ou redémarrage, sans intervention manuelle. Cette exigence garantit un retour à la configuration nominale après incident.

CRITÈRE DE VALIDATION

Après remise en service de CORE-01 préalablement coupé, le rôle Actif HSRP lui revient automatiquement dans un délai inférieur à 30 secondes. Vérifié par `show standby brief`.

EF-04 Agrégation des liens d'accès (LACP)

MUST

Les liaisons physiques entre le commutateur d'accès SW-01 et chacun des deux cœurs doivent être agrégées en EtherChannel utilisant le protocole standard LACP (IEEE 802.3ad), en mode actif. L'objectif est double : optimiser la bande passante disponible et tolérer la coupure d'un lien physique sans interruption de service.

CRITÈRE DE VALIDATION

Les EtherChannel `Po1` (SW-01 ↔ CORE-01) et `Po2` (SW-01 ↔ CORE-02) sont à l'état `SU` (Layer 2 + Up) avec deux liens physiques actifs chacun. La coupure d'un lien physique unique au sein d'un agrégat n'entraîne aucune perte de paquet sur un `ping` continu.

EF-05 Routage dynamique interne (OSPF area 0)

MUST

Le routage entre les deux cœurs et le pare-feu pfSense doit être assuré dynamiquement par OSPFv2, en zone unique `area 0`. La default route apprise du WAN par pfSense est redistribuée vers les cœurs. Aucune route statique interne n'est tolérée : les modifications de topologie doivent se propager automatiquement.

CRITÈRE DE VALIDATION

Toutes les adjacences OSPF sont à l'état `FULL` (vérifié par `show ip ospf neighbor` côté Cisco et la console FRR côté pfSense). La default route apparaît dans la table de routage des deux cœurs avec le code `O*E2`. La convergence après coupure d'un lien transit est inférieure à 5 secondes.

EF-06 Distribution automatique d'adressage (DHCP)

MUST

L'adressage IPv4 des postes utilisateurs doit être attribué automatiquement par un service DHCP hébergé directement sur les commutateurs L3, avec un pool dédié par VLAN. Les plages hautes de chaque /25 sont exclues du pool pour les adresses statiques (équipements réseau, VIP HSRP, éventuels serveurs internes).

CRITÈRE DE VALIDATION

Un poste client connecté dans le VLAN ADMIN obtient un bail dans la plage utilisable de 192.168.10.0/25 ; un poste connecté dans le VLAN ATELIER obtient un bail dans la plage utilisable de 192.168.10.128/25. Aucune collision d'adresse n'est observée avec les IP statiques. Le service reste fonctionnel après bascule HSRP.

EF-07 Sécurisation des accès d'administration

MUST

Tous les équipements (CORE-01, CORE-02, SW-01, pfSense) doivent être administrables exclusivement par SSH v2. Le protocole Telnet doit être explicitement désactivé. L'authentification s'appuie sur un compte administrateur local protégé par un mot de passe robuste, et les mots de passe sont stockés chiffrés en configuration (`service password-encryption` côté Cisco).

CRITÈRE DE VALIDATION

Une tentative de connexion Telnet est refusée sur tous les équipements. La connexion SSH v2 est fonctionnelle. Le mot de passe administrateur respecte une politique de robustesse minimale (≥ 12 caractères, mélange majuscules/minuscules/chiffres). Aucun mot de passe en clair n'apparaît dans la `running-config`.

2.3 · Exigences non fonctionnelles

Les exigences non fonctionnelles décrivent *la qualité de ce que la solution doit faire* : performances, disponibilité, sécurité, maintenabilité. Toutes sont mesurables et leur validation s'appuie sur le plan de tests décrit en partie 5.

Identifiant	Catégorie	Exigence	Seuil mesurable
`ENF-01`	Disponibilité	Temps de bascule de la passerelle HSRP suite à panne du cœur Actif	Inférieur à **10 s**
`ENF-02`	Performance	Convergence OSPF après changement de topologie	Inférieure à **5 s**
`ENF-03`	Performance	Bande passante utile d'un EtherChannel à 2 liens	≥ **1,8 ×** celle d'un lien unique (mesurable par `iperf3`)
`ENF-04`	Sécurité	Protocoles d'administration en clair (Telnet, HTTP) actifs	**Aucun**
`ENF-05`	Sécurité	Robustesse des mots de passe administrateur	≥ 12 caractères, chiffrés en configuration
`ENF-06`	Maintenabilité	Nommage des équipements	FQDN de la forme `ÉQUIPEMENT.DEPANMOI.LAN`
`ENF-07`	Traçabilité	Sauvegarde des configurations de référence	`running-config` + `startup-config` + `vlan.dat` archivés pour chaque équipement
`ENF-08`	Maintenabilité	Documentation du plan d'adressage et de la topologie	Plan d'adressage formel + schémas logique et physique livrés (partie 3)

2.4 · Contraintes

Contraintes matérielles

Équipement	Référence imposée	Rôle dans la solution
CORE-01, CORE-02	Cisco Catalyst WS-C3750X-24, IOS 15.2 (licence `ipservices` requise pour HSRP et OSPF)	Cœur de réseau redondé (L3)
SW-01	Cisco Catalyst 2950, IOS 12.1	Commutateur d'accès (L2)
pfSense	Boîtier Netgate, pfSense Plus 24.5, paquet FRR pour OSPF	Pare-feu et passerelle WAN
Câblage	RJ45 Cat. 5e ou Cat. 6 selon disponibilité du parc	Connectivité physique
Console	Câbles console RJ45 / USB-Serial fournis	Configuration initiale hors bande

Contraintes logicielles et protocolaires

- Les protocoles utilisés doivent être **standardisés** ou **interopérables** : LACP (802.3ad) plutôt que PAgP, OSPFv2 (RFC 2328) plutôt que EIGRP, par cohérence avec le pare-feu non-Cisco (pfSense / FRR).
- HSRP est un protocole propriétaire Cisco : son usage est **strictement limité au segment inter-cœurs** (CORE-01 ↔ CORE-02). Aucune fonction de redondance du pare-feu (CARP) n'est exigée dans le présent cahier des charges (voir EF-08 ci-dessous).
- Aucun service en clair (Telnet, HTTP, SNMP v1/v2c en lecture publique) ne doit rester actif à la fin du déploiement.

Contraintes organisationnelles et budgétaires

- **Aucun budget alloué pour matériel additionnel** : la solution s'appuie strictement sur le parc existant.
- **Période de réalisation imposée** : janvier à février 2026, sur l'infrastructure DEPANMOI.FR.
- **Modalité** : réalisation conduite en équipe, sous supervision pédagogique du centre de formation.
- **Continuité du contrat FAI** : aucune modification du lien WAN, le routeur FAI reste hors périmètre de configuration.

2.5 · Justification des choix techniques

Cette section formalise le **dossier de choix** qui a conduit à retenir, pour chaque service, un protocole ou une implémentation parmi plusieurs alternatives. Pour chaque décision, les options envisageables sont mises en regard de critères explicites (standardisation, interopérabilité, convergence, coût, robustesse) ; la solution retenue est ensuite déclinée jusqu'aux paramètres de configuration significatifs, qui seront mis en œuvre en partie 4.

2.5.1 · Redondance de la passerelle : HSRP retenu

Deux commutateurs Cisco Catalyst 3750-X doivent partager une passerelle virtuelle pour chaque VLAN d'utilisateurs. Trois protocoles candidats existent : HSRP, VRRP et GLBP.

Option	Standardisation	Compatibilité matériel	Fonctionnalités utiles ici	Décision
VRRP (RFC 5798)	Standard IETF, multi-vendor	Disponible sur IOS 15.x	VIP, élection MASTER/BACKUP, tracking	REJETÉ
HSRP v1 (RFC 2281)	RFC informationnelle, propriétaire Cisco	Natif IOS, recommandé Cisco depuis 1998	VIP, Active/Standby, préemption, groupes ≥ 255	RETENU
GLBP (Cisco)	Propriétaire Cisco	Natif IOS	Load-balancing inter-routeurs (AVF/AVG)	REJETÉ

Justification. L'infrastructure cible est *100 % Cisco au niveau L3 LAN* (CORE-01 et CORE-02 sont des Catalyst 3750-X) : la portabilité multi-vendor de VRRP n'apporte aucun bénéfice fonctionnel ici. HSRP est par ailleurs le protocole de référence sur Catalyst, largement documenté et enseigné, ce qui facilite une éventuelle reprise par un autre technicien. GLBP propose une répartition de charge entre les deux cœurs, mais pour un effectif de quatre utilisateurs simultanés le gain de débit est négligeable et la complexité de diagnostic en incident augmente significativement, le rapport bénéfice/risque n'est pas en sa faveur.

PARAMÈTRES RETENUS POUR LA MISE EN ŒUVRE

Version : HSRP v1, soit groupes 10 et 20. · **Priorité :** CORE-01 = 110 (préférentiel), CORE-02 = 100 (par défaut). · **Préemption :** activée sur CORE-01 pour permettre la reprise automatique du rôle Actif après réparation. · **Timers :** hello/holdtime laissés aux valeurs par défaut (3 s / 10 s), donne un RTO de bascule conforme à `ENF-01` sans surcharge CPU des cœurs.

2.5.2 · Agrégation de liens d'accès : LACP retenu

Le commutateur d'accès SW-01 est raccordé à chacun des deux cœurs par deux liens physiques. Il faut choisir le mécanisme d'agrégation pour former un EtherChannel par cœur.

Option	Standardisation	Détection des erreurs de configuration	Interopérabilité	Décision
LACP (IEEE 802.3ad)	Standard IEEE 1999	Excellente : LACPDU négociés à chaque extrémité	Tous constructeurs (Cisco, HPE, Juniper, Mikrotik...)	RETENU
PAgP (Cisco)	Propriétaire Cisco	Bonne	Cisco uniquement	REJETÉ
Static EtherChannel	Aucun protocole de négociation	Aucune (un câble inversé reste invisible)	N/A	REJETÉ

Justification. Bien que l'infrastructure soit aujourd'hui exclusivement Cisco au niveau accès, le choix de LACP plutôt que PAgP *protège l'investissement* : le remplacement futur de SW-01 par un commutateur d'un autre constructeur (HPE, Aruba, Mikrotik) ne nécessitera pas de refonte de l'agrégation. Surtout, LACP **négocie activement** la formation de l'agrégat via les LACPDU : une erreur de câblage (un port branché sur le mauvais EtherChannel) est immédiatement détectée et l'agrégat ne se forme pas, ce qui prévient les pannes silencieuses. Le mode statique est exclu sans appel : sans négociation, deux ports mal câblés peuvent former une boucle ou un agrégat asymétrique non détecté.

PARAMÈTRES RETENUS POUR LA MISE EN ŒUVRE

Mode : `active` aux deux extrémités (chaque switch initie la négociation, plus rapide qu'une combinaison passive/passive qui ne forme pas d'agrégat). · **Numérotation :** `Port-channel 1` sur la liaison SW-01 ↔ CORE-01, `Port-channel 2` sur la liaison SW-01 ↔ CORE-02. · **Hash de répartition :** `src-dst-mac` (par défaut sur Catalyst 2950, suffisant pour des flux LAN d'utilisateurs) ; `src-dst-ip` recommandé côté 3750-X pour une meilleure distribution des flux IP. · **Encapsulation :** trunk dot1Q transportant les VLAN 610 et 620.

2.5.3 · Routage interne : OSPFv2 retenu

Quatre segments doivent être interconnectés en routage : VLAN 610, VLAN 620, TRANSIT1 (CORE-01 ↔ pfSense) et TRANSIT2 (CORE-02 ↔ pfSense). Quatre approches sont envisageables.

Option	Convergence	Métrique	Interop. pfSense (FRR)	Décision
Routes statiques	Aucune (intervention manuelle)	Sans objet	OK	REJETÉ
RIPv2 (RFC 2453)	Lente (~30 s)	Saut (limité à 15)	OK (FRR)	REJETÉ
OSPFv2 (RFC 2328)	Rapide (1 à 5 s)	Coût (lié à la bande passante)	OK (FRR, paquet pfSense)	RETENU
EIGRP (Cisco)	Très rapide	Composite (BW + délai)	**Non** (FRR ne supporte pas EIGRP en standard)	REJETÉ

Justification. Le critère *discriminant* est l'interopérabilité avec pfSense, qui fait partie intégrante du domaine de routage interne (transit cœur ↔ pare-feu). EIGRP est éliminé d'emblée : le paquet FRR de pfSense ne le supporte pas. RIPv2 fonctionnerait techniquement, mais sa convergence d'environ 30 secondes est incompatible avec `ENF-02` qui exige une reconvergence en moins de 5 secondes. Les routes statiques violeraient `EF-05` (la propagation automatique des routes est explicitement requise) et créeraient une dette de maintenance à chaque évolution. OSPFv2 est **ouvert**, supporté nativement IOS et FRR, et offre une convergence rapide grâce à son algorithme link-state SPF. Sa métrique basée sur le coût (inversement proportionnel à la bande passante) reste cohérente avec une éventuelle hétérogénéité de débit entre liens 100 Mb/s et 1 Gb/s.

PARAMÈTRES RETENUS POUR LA MISE EN ŒUVRE

Topologie : zone unique `area 0`, quatre segments et trois routeurs ne justifient pas une hiérarchie multi-area. · **Process-id :** `1` sur les cœurs Cisco (significatif uniquement localement). · **Réseaux annoncés :** chaque cœur publie ses VLAN SVI (610, 620) et son segment transit ; pfSense publie les TRANSIT1/TRANSIT2 et redistribue la default route apprise du WAN (`O*E2` sur les cœurs). · **Interfaces passives :** SVI VLAN 610 et 620, pas d'adjacence OSPF avec les postes utilisateurs (pas de pair OSPF côté client).

2.5.4 · Distribution de l'adressage : DHCP hébergé sur les cœurs

Le service DHCP doit attribuer une adresse IPv4 aux postes clients de chaque VLAN. Trois implémentations sont envisageables : serveur dédié, service intégré à pfSense, ou service intégré aux commutateurs L3.

Option	Coût	Point de défaillance	Complexité	Décision
Serveur dédié (Windows Server / Linux ISC)	Matériel + licence + administration	Oui (sauf cluster, hors budget)	Élevée	REJETÉ
Service sur pfSense	Nul	Oui, pfSense unique (cf. `EF-08`)	Faible, mais nécessite `ip helper-address` sur les cœurs	REJETÉ
Service sur les cœurs Cisco (un pool par VLAN)	Nul (natif IOS)	Réduit : split-scope possible entre les deux cœurs	Moyenne	RETENU

Justification. Le serveur dédié introduirait un nouveau service à maintenir (matériel, OS, licences) pour une fonction simple, et créerait lui-même un SPOF logiciel. Héberger DHCP sur pfSense est techniquement faisable mais aggrave la dépendance à un équipement déjà identifié comme point de défaillance unique (`EF-08` Won't), et impose en outre la configuration d'un relais DHCP `ip helper-address` sur chaque SVI des cœurs, complexité ajoutée sans bénéfice de résilience. La mise en place du service directement sur les cœurs Cisco est *native, gratuite et locale* : la passerelle qui répond au client est aussi celle qui distribue son adresse, ce qui élimine toute dépendance protocolaire intermédiaire. La résilience peut en outre être améliorée par la technique du **split-scope**, où chaque cœur sert une moitié de la plage utilisable et exclut la moitié servie par son voisin, la perte d'un cœur ne supprime que la moitié des adresses servies.

PARAMÈTRES RETENUS POUR LA MISE EN ŒUVRE

Pools : `POOL_ADMIN` (192.168.10.0/25) et `POOL_ATELIER` (192.168.10.128/25). · **Exclusions :** plages hautes de chaque /25 réservées aux IP statiques (interfaces SVI des cœurs, VIP HSRP, équipements internes éventuels). · **Default-router :** VIP HSRP du VLAN concerné. · **DNS :** à arbitrer en partie 4, soit les résolveurs FAI, soit pfSense en relais DNS. · **Bail :** 24 h (valeur standard, équilibre entre stabilité et rotation). · **Stratégie de résilience :** split-scope envisagé (CORE-01 sert la première moitié de la plage utilisable, CORE-02 la seconde), décision finale arbitrée en partie 4 selon la complexité acceptable.

2.6 · Hypothèses et exclusions

Hypothèses retenues

Les hypothèses suivantes sont supposées vérifiées au démarrage de la mission. Si l'une d'elles s'avère fausse, le périmètre ou le calendrier devront être réévalués.

HYPOTHÈSES

- **Le matériel fourni est en état de fonctionnement**, aucun défaut hardware connu sur les Catalyst 3750-X, 2950 ni sur le boîtier pfSense.
- **Les licences IOS appropriées** (notamment `ipservices` sur les 3750-X pour HSRP et OSPF) sont actives.
- **Les sauvegardes des données métier** (CRM, comptabilité, messagerie) sont déjà gérées côté DEPANMOI.FR et restent fonctionnelles pendant la mission.
- **Le contrat FAI** reste inchangé pendant la mission.
- **Les techniciens DEPANMOI.FR** sont en mesure d'utiliser un client SSH (PuTTY ou OpenSSH) pour les opérations de support quotidien post-déploiement.

Exclusions explicites (Won't have)

Les éléments listés ci-dessous sont des **décisions assumées** de ne pas traiter dans le présent projet. Ils sont documentés pour matérialiser la conscience qu'a l'équipe projet du périmètre résiduel et de l'écart entre la cible livrée et un système idéalement redondé.

`EF-08` **Redondance du pare-feu pfSense (CARP)** ~~WON'T~~

La mise en haute disponibilité du pare-feu pfSense par CARP (protocole de redondance équivalent à HSRP côté BSD) nécessiterait un second boîtier Netgate identique. Cette acquisition matérielle n'est pas justifiée pour une TPE de quatre personnes disposant d'un unique lien FAI : la défaillance de pfSense priverait les utilisateurs d'Internet, mais le cœur LAN (postes ↔ ressources internes) resterait opérationnel grâce au routage OSPF.

RISQUE RÉSIDUEL DOCUMENTÉ

Le pare-feu pfSense reste un point de défaillance unique vis-à-vis du trafic WAN. Une procédure de remplacement à froid (restauration de la sauvegarde XML sur un boîtier de prêt) est documentée en annexe.

EF-09 Redondance du lien WAN (double FAI ou secours 4G)

~~WON'T~~

La souscription d'un second abonnement Internet ou la mise en place d'un secours 4G n'est pas retenue : le coût récurrent excède le bénéfice pour une TPE dont l'activité tolère quelques heures sans Internet (les techniciens peuvent continuer à intervenir en clientèle pendant un incident FAI).

RISQUE RÉSIDUEL DOCUMENTÉ

Une panne de l'accès Internet du FAI prive l'organisation de messagerie et d'accès aux ressources externes pendant la durée du sinistre. Le SLA du FAI s'applique.

EF-10 Authentification 802.1X sur SW-01

~~WON'T~~

L'authentification des postes au branchement par 802.1X (RADIUS) nécessite un service d'authentification centralisé qui n'est pas présent dans le SI actuel et dépasse la cible fonctionnelle du projet. Pour une TPE de 4 personnes, la sécurité physique du local atelier offre un compromis acceptable.

RISQUE RÉSIDUEL DOCUMENTÉ

Un poste non maîtrisé branché physiquement dans le local pourrait obtenir une adresse IP et accéder au VLAN correspondant. La maîtrise repose sur la sécurité d'accès au local.

2.7 · Livrables et critères de recette

Les livrables suivants seront remis à la commission d'évaluation (BTS SIO) et au commanditaire (gérant de DEPANMOI.FR) à l'issue de la mission. La recette est prononcée lorsque **tous les livrables sont fournis** et **tous les tests du plan partie 5 passent au vert**.

Livrable	Description	Format
Documentation technique	Présent dossier complet en huit parties, contexte, cahier des charges, architecture, configurations, procédure, plan de tests, gestion des incidents, retour d'expérience et annexes	HTML / PDF
Configurations de référence	`running-config` et `startup-config` archivées de CORE-01, CORE-02 et SW-01 ; fichier `vlan.dat` de chaque commutateur	Fichiers texte / binaires
Sauvegarde pfSense	Export XML de la configuration complète du pare-feu (interfaces, règles, OSPF/FRR)	XML
Schémas réseau	Schéma logique (VLAN, IP, protocoles) et schéma physique (rack, ports, câblage)	SVG / PNG embarqués dans la documentation
Plan de tests et résultats	Pour chaque exigence (EF / ENF), procédure de test, résultat attendu, résultat observé, validation	Tableau dans la partie 5
Procédure de mise en œuvre	Pas-à-pas reproductible permettant à un tiers de redéployer la solution depuis zéro, prérequis matériels, ordre d'exécution, points de vérification	Partie 4 du document
Glossaire et annexes	Glossaire des acronymes, références aux RFC, configurations complètes commentées	Partie 8 du document

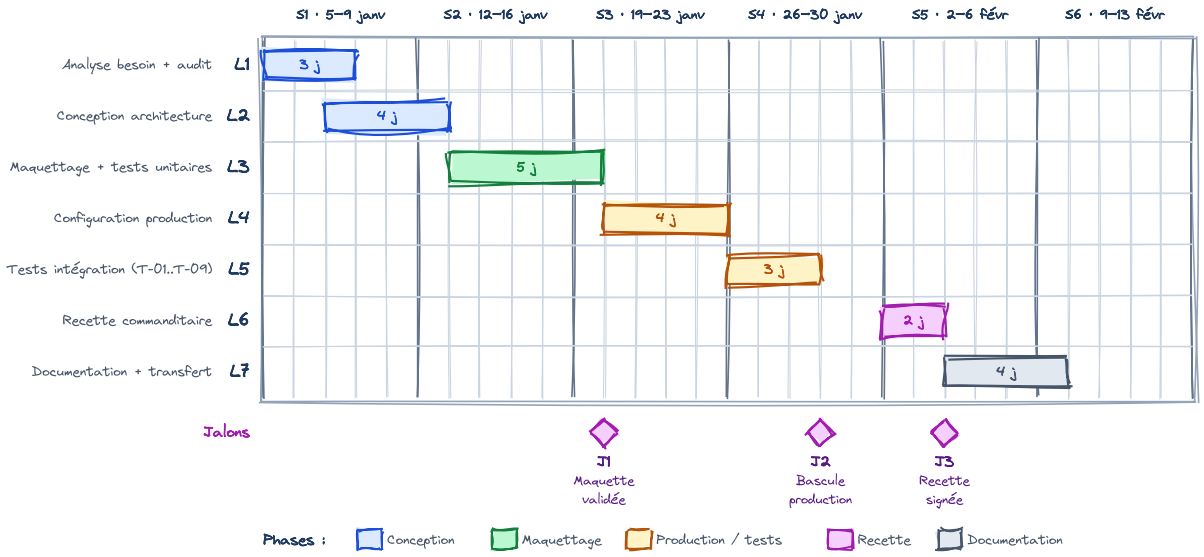
Critères de recette

LA SOLUTION EST RECETTE SI ET SEULEMENT SI

- Tous les livrables ci-dessus sont fournis et conformes.
- Toutes les exigences `EF-01` à `EF-07` sont validées par leur critère de validation respectif.
- Toutes les exigences `ENF-01` à `ENF-06` et `ENF-08` respectent leur seuil mesurable (plan de tests partie 5). `ENF-07` (sauvegarde des configurations) est validée par la livraison des fichiers archivés en annexes section 8.3.
- Les exclusions `EF-08` à `EF-10` sont documentées et leurs risques résiduels acceptés par le commanditaire.
- Une démonstration de bascule HSRP est réalisée en présence du gérant de DEPANMOI.FR.

2.8 · Planification du projet

Le projet s'étend du **5 janvier au 13 février 2026** (6 semaines, 30 jours ouvrés), organisé en sept lots avec quelques recouvrements pour absorber les aléas.



Macroplanning du projet · sept lots, trois jalons, six semaines.

Lot	Objet	Durée	Période	Jalon de sortie
L1	Analyse du besoin et audit de l'existant chez DEPANMOI.FR	3 jours	5 – 7 janv	Cahier des charges figé
L2	Conception de l'architecture cible et du plan d'adressage	4 jours	7 – 13 janv	Schémas validés
L3	Maquettage sur plateau et tests unitaires (HSRP, LACP, OSPF)	5 jours	13 – 20 janv	J1, Maquette validée (20 janv)
L4	Configuration des équipements de production (CORE-01, CORE-02, SW-01)	4 jours	20 – 26 janv	Configurations déployées
L5	Tests d'intégration et de bascule (T-01 à T-09)	3 jours	26 – 29 janv	J2, Bascule production (29 janv)
L6	Recette avec le commanditaire et démonstration de bascule HSRP	2 jours	2 – 3 févr	J3, Recette signée (3 févr)
L7	Rédaction de la documentation et transfert de connaissances	4 jours	4 – 13 févr	Dossier remis (13 févr)

PARTIE 3

Architecture cible

3.1 · Vue d'ensemble

Quatre équipements : SW-01 (accès L2), CORE-01 et CORE-02 (L3 redondés HSRP), FW-01 (pare-feu pfSense). LACP entre SW-01 et chaque CORE. OSPF area 0 entre CORE et FW-01 sur deux transits /30.

Équipement	Hostname	Modèle	Rôle
SW-01	`SW-01.DEPANMOI.LAN`	Cisco Catalyst 2950	Accès L2, 24× FastEthernet
CORE-01	`CORE-01.DEPANMOI.LAN`	Cisco Catalyst 3750-X	L3, HSRP Actif (priorité 110)
CORE-02	`CORE-02.DEPANMOI.LAN`	Cisco Catalyst 3750-X	L3, HSRP Standby (priorité 100)
FW-01	`FW-01.DEPANMOI.LAN`	Netgate, pfSense Plus 24.5	Pare-feu, NAT, OSPF FRR

3.2 · Schéma logique annoté

Quatre segments routés (VLAN 610, VLAN 620, TRANSIT1, TRANSIT2). IP par interface, VIP HSRP, et relations protocolaires (LACP, HSRP, OSPF) annotées sur chaque lien.

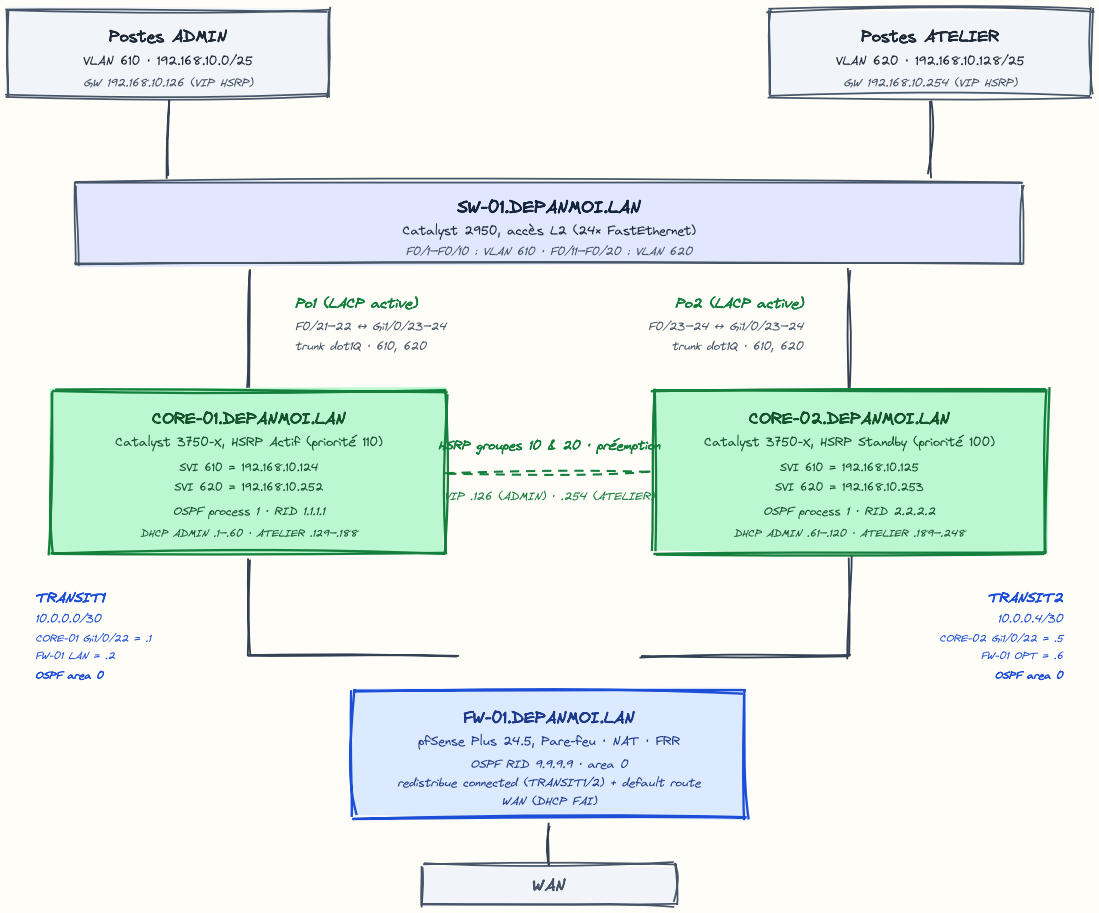


Figure 3.1 · Schéma logique annoté. Adresses IPv4, groupes HSRP, Port-channels et adjacences OSPF sur chaque segment.

3.3 · Plan d'adressage IPv4

Cinq segments : VLAN 610, VLAN 620, TRANSIT1, TRANSIT2, WAN. DHCP en **split-scope** sur les VLAN, chaque CORE sert une moitié de la plage utilisable, exclusions croisées via `ip dhcp excluded-address`.

Segment	Subnet	Affectation	Adresse(s)
VLAN 610, ADMIN, 192.168.10.0/25			
VLAN 610	`192.168.10.0/25`	Interface SVI CORE-01	`192.168.10.124`
		Interface SVI CORE-02	`192.168.10.125`
		VIP HSRP groupe 10 (passerelle clients)	**`192.168.10.126`**
		Pool DHCP servi par CORE-01	`192.168.10.1 → .60`
		Pool DHCP servi par CORE-02	`192.168.10.61 → .120`
		Plage réservée IP statiques	`192.168.10.121 → .126`
VLAN 620, ATELIER, 192.168.10.128/25			
VLAN 620	`192.168.10.128/25`	Interface SVI CORE-01	`192.168.10.252`
		Interface SVI CORE-02	`192.168.10.253`
		VIP HSRP groupe 20 (passerelle clients)	**`192.168.10.254`**
		Pool DHCP servi par CORE-01	`192.168.10.129 → .188`
		Pool DHCP servi par CORE-02	`192.168.10.189 → .248`
		Plage réservée IP statiques	`192.168.10.249 → .254`
TRANSIT1, CORE-01 ↔ FW-01, 10.0.0.0/30			
TRANSIT1	`10.0.0.0/30`	CORE-01, interface `Gi1/0/22`	`10.0.0.1`

Segment	Subnet	Affectation	Adresse(s)
		FW-01, interface **LAN**	`10.0.0.2`
TRANSIT2, CORE-02 ↔ FW-01, 10.0.0.4/30			
TRANSIT2	`10.0.0.4/30`	CORE-02, interface `Gi1/0/22`	`10.0.0.5`
		FW-01, interface **OPT**	`10.0.0.6`
WAN, FW-01 ↔ Routeur FAI			
WAN	`DHCP FAI`	FW-01, interface **WAN**	`attribuée par DHCP FAI`

CHOIX DU MASQUE /30 ET DU BLOC 10.0.0.0/8

Pourquoi /30 ? Un lien transit point-à-point ne porte que deux hôtes : le CORE et FW-01. Le masque `/30` alloue exactement quatre adresses (réseau, deux hôtes utilisables, broadcast), soit le strict minimum. `/29` en gaspillerait six adresses sur les deux transits sans bénéfice. `/31` (RFC 3021, point-à-point sans broadcast) est techniquement plus économe encore mais reste moins universel et complique le diagnostic, `/30` est le standard de fait sur les liens d'infrastructure.

Pourquoi `10.0.0.0/8` séparé du `192.168.10.0/24` ? RFC 1918 propose trois blocs privés (`10.0.0.0/8` , `172.16.0.0/12` , `192.168.0.0/16`). La convention retenue ici réserve `192.168.10.0/24` aux VLAN utilisateurs (déjà historique côté DEPANMOI.FR) et `10.0.0.0/8` aux liens transit d'infrastructure. La ségrégation est purement organisationnelle mais permet une lecture immédiate des logs et des traces : une adresse `10.0.0.x` désigne un lien interne entre équipements, `192.168.10.x` désigne un poste client. Le diagnostic d'incident (où est passé ce paquet ?) gagne en lisibilité.

3.4 · Schéma physique

Photo réelle de la baie déployée, SW-01, CORE-01, CORE-02, FW-01 et câblage réseau.

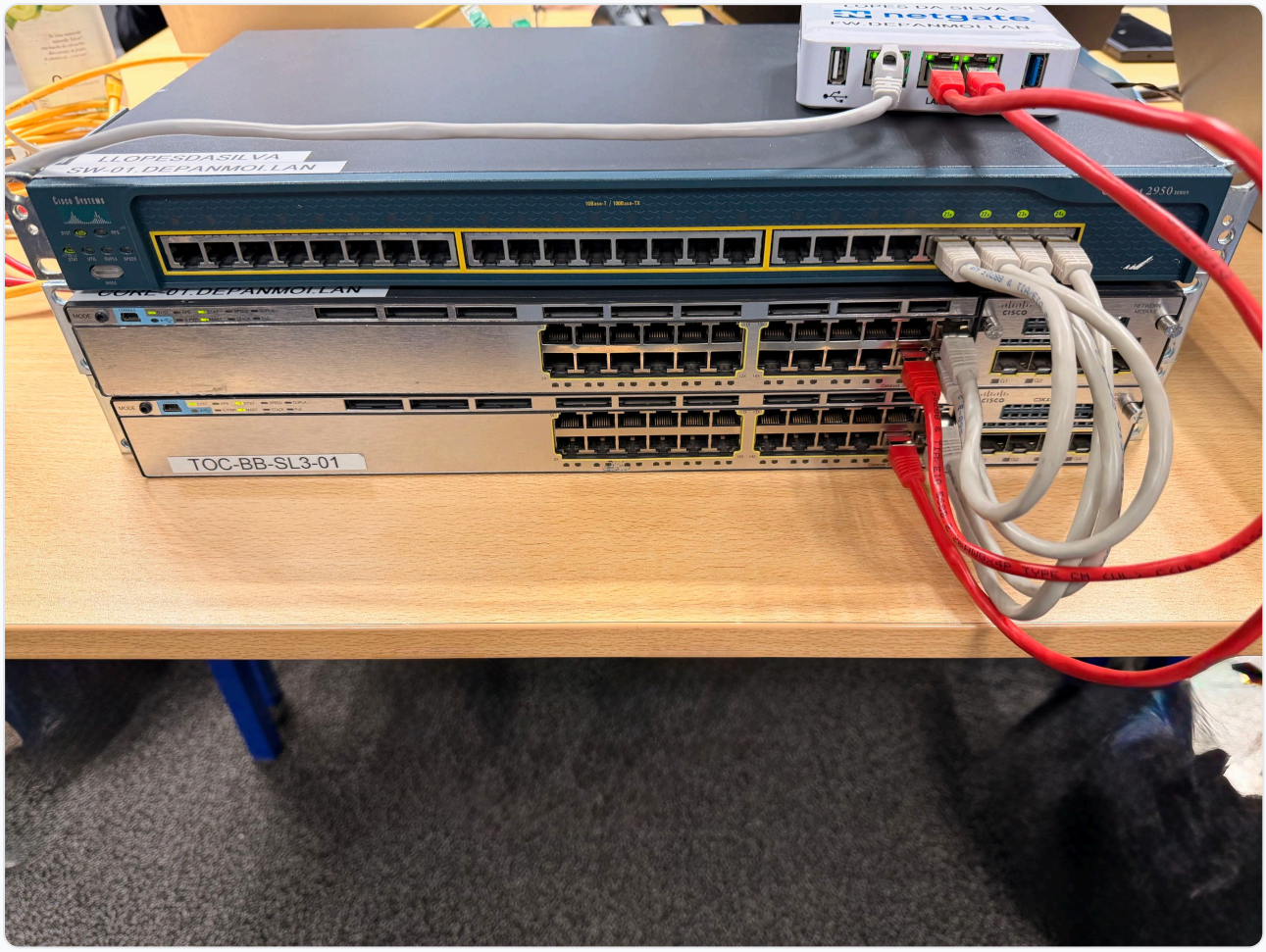


Figure 3.2 · Photo du rack technique déployé : SW-01, CORE-01, CORE-02, FW-01 et câblage réseau.

3.5 · Tableau de câblage

Liaisons physiques actives. Référence pour la procédure (partie 5) et le plan de tests (partie 6).

Source	Port source	Destination	Port destination	Type	Agrégat	VLAN / IP
SW-01	`F0/21`	CORE-01	`Gi1/0/23`	Trunk dot1Q	`Po1` (LACP active)	610, 620
SW-01	`F0/22`	CORE-01	`Gi1/0/24`	Trunk dot1Q	`Po1` (LACP active)	610, 620
SW-01	`F0/23`	CORE-02	`Gi1/0/23`	Trunk dot1Q	`Po2` (LACP active)	610, 620
SW-01	`F0/24`	CORE-02	`Gi1/0/24`	Trunk dot1Q	`Po2` (LACP active)	610, 620
CORE-01	`Gi1/0/22`	FW-01	**LAN**	L3 routé /30	—	TRANSIT1, 10.0.0.0/30
CORE-02	`Gi1/0/22`	FW-01	**OPT**	L3 routé /30	—	TRANSIT2, 10.0.0.4/30
FW-01	**WAN**	Routeur FAI	—	WAN DHCP	—	attribuée par DHCP FAI

SW-01, F0/1 à F0/10 : postes utilisateurs VLAN 610 (ADMIN), F0/11 à F0/20 : postes utilisateurs VLAN 620 (ATELIER), mode access

NOTE MATÉRIELLE, CATALYST 2950

SW-01 est un Catalyst 2950 dont les 24 ports cuivre sont en **FastEthernet (100 Mb/s)**. La bande passante cumulée d'un Port-channel à deux liens est donc plafonnée à **2 × 100 Mb/s = 200 Mb/s** agrégés vers chaque cœur, indépendamment de la capacité Gigabit des Catalyst 3750-X côté cœur. Cette limite reste largement suffisante pour un effectif de quatre utilisateurs.

3.6 · Conventions de nommage

Conventions appliquées sur tous les équipements pour une lecture homogène des configs.

Élément	Convention	Exemples
Hostname	`RÔLE-NUMÉRO.DEPANMOI.LAN`	`CORE-01.DEPANMOI.LAN`, `CORE-02.DEPANMOI.LAN`, `SW-01.DEPANMOI.LAN`, `FW-01.DEPANMOI.LAN`
Description d'interface	Texte court explicite, en français, majuscules pour les rôles	`UPLINK VERS SW-01`, `LAN NetGate pfSense`, `Postes ADMIN`, `Postes ATELIER`
VLAN	Numéro à 3 chiffres, nom en majuscules sans accent	`vlan 610 name ADMIN`, `vlan 620 name ATELIER`
Groupe HSRP	Numéro de groupe simple (1–254), un par VLAN	Groupe `10` pour VLAN 610, groupe `20` pour VLAN 620
Pool DHCP	Nom du VLAN en majuscules	`ip dhcp pool ADMIN`, `ip dhcp pool ATELIER`
OSPF	Process-id `1`, area unique `0`, router-id explicite	CORE-01 → `1.1.1.1`, CORE-02 → `2.2.2.2`, FW-01 → `9.9.9.9`
EtherChannel	Numérotation locale par cœur destination	SW-01 : `Po1` → CORE-01, `Po2` → CORE-02. Chaque CORE expose son propre `Po1` local.
Domaine DNS	Domaine interne unique	`DEPANMOI.LAN`

PARTIE 4

Configurations et procédure de mise en œuvre

Cette partie tient lieu de **procédure de mise en œuvre** reproductible : chaque sous-section présente les commandes Cisco IOS ou les paramètres pfSense à appliquer dans l'ordre, accompagnés des annotations utiles au déploiement et des captures de vérification attendues. Un tiers technicien peut redéployer l'infrastructure depuis zéro en suivant l'ordre indiqué ci-dessous.

4.1 · Vue d'ensemble par équipement

Équipement	Modèle	Rôle synthétique	Section
SW-01	Cisco Catalyst 2950	Accès L2, VLAN, ports utilisateurs, deux EtherChannel LACP vers les CORE	4.2
CORE-01	Cisco Catalyst 3750-X	Cœur L3, HSRP **Actif**, STP **root**, OSPF RID 1.1.1.1, DHCP plage basse	4.3
CORE-02	Cisco Catalyst 3750-X	Cœur L3, HSRP **Standby**, STP secondary, OSPF RID 2.2.2.2, DHCP plage haute	4.4
FW-01	Netgate (pfSense Plus 24.5)	Pare-feu, NAT, FRR OSPF (RID 9.9.9.9), passerelle WAN	4.5

4.1.1 · Prérequis matériels et logiciels

- **Câblage console** : un câble RJ45-RS232 ou USB-Serial (FTDI/Prolific) compatible Cisco, paramètres terminal `9600 8N1`, contrôle de flux désactivé.
- **Poste d'administration** : émulateur de terminal (PuTTY, Tera Term, minicom) avec accès aux fichiers de configuration archivés (cf. annexes section 7.3).
- **Câbles RJ45 Cat. 5e ou Cat. 6** en quantité suffisante pour les liaisons SW-01 ↔ CORE-01 (×2), SW-01 ↔ CORE-02 (×2), CORE-01 ↔ FW-01 (×1), CORE-02 ↔ FW-01 (×1), FW-01 ↔ Routeur FAI (×1), soit 7 câbles minimum.
- **Licences IOS actives** : `ipservices` sur les deux Catalyst 3750-X (requise pour HSRP et OSPF). Vérifier par `show license` avant déploiement.
- **Reset usine** recommandé avant déploiement si l'équipement a déjà été utilisé (`write erase` + `delete vlan.dat` + `reload`).
- **Sauvegardes** : avant toute modification d'un équipement existant, sauvegarder la configuration courante (`copy running-config tftp:` ou export XML pour pfSense).

4.1.2 · Ordre de mise en œuvre recommandé

L'ordre ci-dessous minimise les phases d'indisponibilité partielle pendant le déploiement. Chaque étape se vérifie avant de passer à la suivante.

1. **SW-01** (section 4.2), base L2, sécurisation SSH, création des VLAN 610/620, configuration des ports d'accès, déclaration des deux EtherChannel `Po1` et `Po2`. Vérification : `show etherchannel summary` attendu en `SW` (suspendu) tant que les CORE ne sont pas configurés, c'est normal à ce stade.
2. **CORE-01** (section 4.3), sécurisation, STP root, VLAN, Port-channel `Po1` côté cœur (formation effective de l'agrégation avec SW-01), interface transit `Gi1/0/22`, SVI HSRP Actif, OSPF, pools DHCP. Vérification : `show etherchannel summary` = `SU` sur `Po1`, ping vers VIP HSRP `192.168.10.126` depuis poste VLAN 610.
3. **CORE-02** (section 4.4), paramètres miroir (sécurisation, STP secondary, Port-channel, transit, SVI HSRP Standby, OSPF, DHCP exclusions inversées). Vérification : `show standby brief` sur les deux CORE, CORE-01 doit rester `Active`, CORE-02 passe `Standby`.
4. **FW-01** (section 4.5), assignation interfaces WAN/LAN/OPT, installation paquet FRR, paramétrage OSPF, NAT outbound hybride, règles de filtrage. Vérification : `show ip ospf neighbor` sur les deux CORE = état **FULL** avec RID `9.9.9.9` ; ping `1.1.1.1` depuis un poste utilisateur.
5. **Recette globale**, exécuter le plan de tests (Partie 5, T-01 à T-08, T-10) et archiver les résultats.
6. **Sauvegarde finale**, `copy running-config startup-config` sur les trois équipements Cisco, export XML complet sur pfSense (*Diagnostics → Backup & Restore*). Archivage des fichiers conformément aux annexes section 7.3.

FENÊTRE D'INDISPONIBILITÉ

Le déploiement est planifié sur l'infrastructure DEPANMOI.FR en production, lors d'une fenêtre de maintenance d'environ **6 heures** hors heures ouvrées (nuit du vendredi au samedi). Cette durée intègre le reset des équipements existants, le recâblage selon le nouveau plan physique, l'application des configurations sur CORE-01, CORE-02, SW-01 et pfSense, la validation des protocoles (HSRP, LACP, OSPF, DHCP), l'exécution de la recette T-01 à T-07, la sauvegarde finale, ainsi qu'une marge pour gérer les imprévus.

4.2 · SW-01 · Commutateur d'accès L2

4.2.1 · Identité, domaine, sécurisation des accès

SW-01, sécurisation accès — SW-01.DEPANMOI.LAN running-config

```
configure terminal
service password-encryption
hostname SW-01.DEPANMOI.LAN
ip domain-name depanmoi.lan
no ip domain-lookup
!
enable secret 5 $1$xqQf$AlgHsyUNmZc5y64UQ5ah60
username admin privilege 15 secret 5 $1$W2Qd$sQxpD3W054yqGfCXp/9eu1
!
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
line vty 0 4
 transport input ssh
 login local
line vty 5 15
 transport input ssh
 login local
```

ANNOTATIONS

- SW-01 (IOS 12.1) ne supporte pas `ip ssh dh min size` ni la sélection d'algorithmes, clé RSA limitée à 1024 bits côté Catalyst 2950.
- `transport input ssh` sur les `line vty 0-15` → Telnet refusé (`EF-07`).
- `service password-encryption` chiffre les mots de passe en type 7 dans la conf.

```
SW-01.DEPANMOI.LAN#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
SW-01.DEPANMOI.LAN#
```

Figure 4.1 · Vérification SSH sur SW-01 : `show ip ssh` confirme SSH v2.0 activé, timeout 60 s, retries 3.

4.2.2 · VLAN 610 et 620 · base de données VLAN

SW-01, VLAN database (vlan.dat) — SW-01

```
vlan 610
 name ADMIN
!
vlan 620
 name ATELIER
```

4.2.3 · Ports d'accès utilisateurs

SW-01, répartition F0/1–F0/20 — SW-01 running-config

```
interface range FastEthernet0/1 - 10
 description Postes ADMIN
 switchport access vlan 610
 switchport mode access
!
interface range FastEthernet0/11 - 20
 description Postes ATELIER
 switchport access vlan 620
 switchport mode access
```

4.2.4 · EtherChannel LACP vers les CORE

SW-01, Po1 (CORE-01) et Po2 (CORE-02) — SW-01 running-config

```
interface Port-channel1
 description UPLINK VERS CORE01
 switchport trunk allowed vlan 610,620
 switchport mode trunk
!
interface Port-channel2
 description UPLINK VERS CORE02
 switchport trunk allowed vlan 610,620
 switchport mode trunk
!
interface FastEthernet0/21
 description UPLINK VERS CORE01
 switchport trunk allowed vlan 610,620
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/22
 description UPLINK VERS CORE01
 switchport trunk allowed vlan 610,620
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/23
 description UPLINK VERS CORE02
 switchport trunk allowed vlan 610,620
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/24
 description UPLINK VERS CORE02
 switchport trunk allowed vlan 610,620
 switchport mode trunk
 channel-group 2 mode active
```

ANNOTATIONS

- `channel-group N mode active` = LACP actif (LACPDU négociés). `active/active` aux deux extrémités → formation rapide.
- Trunks dot1Q (implicite sur 2950 : pas de `encapsulation` à préciser).
- 2 × 100 Mb/s = 200 Mb/s agrégés par EtherChannel (limite hardware Catalyst 2950).

```
SW-01.DEPANMOI.LAN#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/21(P)   Fa0/22(Pd)
2      Po2(SU)         LACP      Fa0/23(Pd)  Fa0/24(P)

SW-01.DEPANMOI.LAN#
```

Figure 4.2 · `show etherchannel summary` sur SW-01 : Po1 (Fa0/21, Fa0/22) et Po2 (Fa0/23, Fa0/24) déclarés en LACP.

4.3 · CORE-01 · Cœur L3 Actif

4.3.1 · Identité, domaine, sécurisation

CORE-01, sécurisation accès et SSH durcie — CORE-01.DEPANMOI.LAN running-config

```
configure terminal
service password-encryption
hostname CORE-01.DEPANMOI.LAN
ip domain-name depanmoi.lan
no ip domain-lookup
!
enable secret 5 $1$GHVJ$0JTwpcbd2RtFZVKdqurZh.
username admin privilege 15 secret 5 $1$N9n9$7X.IRuv7m0IVV1xans3s0.
!
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh logging events
ip ssh dh min size 2048
ip ssh server algorithm encryption aes256-ctr aes192-ctr aes128-ctr
ip ssh server algorithm mac hmac-sha1
ip ssh server algorithm hostkey ssh-rsa
!
line vty 0 4
 transport input ssh
 login local
line vty 5 15
 transport input ssh
 login local
```

ANNOTATIONS

- SSH v2 durci sur 3750-X : DH ≥ 2048 bits, ciphers AES-CTR seulement (pas de CBC), HMAC SHA-1.
- `transport input ssh` + `login local` → Telnet refusé, authentification compte local `admin`.

4.3.2 · Spanning Tree · root primaire

CORE-01, STP root — CORE-01 running-config

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 610,620 priority 4096
```

ANNOTATIONS

- Priorité `4096` < `8192` (CORE-02) < `32768` (SW-01) → CORE-01 élu root des deux VLAN.

```
CORE-01.DEPANMOI.LAN#show spanning-tree vlan 610

VLAN0610
  Spanning tree enabled protocol rstp
  Root ID    Priority    4706
             Address     30e4.dbe2.5080
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4706   (priority 4096 sys-id-ext 610)
             Address     30e4.dbe2.5080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Po1                 Desg FWD 12        128.512  P2p


CORE-01.DEPANMOI.LAN#
```

Figure 4.3 · `show spanning-tree vlan 610` sur CORE-01 : This bridge is the root confirmé, priorité 4706 (4096 + sys-id-ext 610), Po1 en rôle `Desg FWD`.

4.3.3 · VLAN, ports trunk LACP et interface transit

CORE-01, Po1 vers SW-01 et Gi1/0/22 vers FW-01 — CORE-01 running-config

```
vlan 610
 name ADMIN
!
vlan 620
 name ATELIER
!
interface Port-channel1
 description UPLINK VERS SW-01
 switchport trunk allowed vlan 610,620
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 description UPLINK VERS SW-01
 switchport trunk allowed vlan 610,620
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/24
 description UPLINK VERS SW-01
 switchport trunk allowed vlan 610,620
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/22
 description LAN NetGate pfSense
 no switchport
 ip address 10.0.0.1 255.255.255.252
```

ANNOTATIONS

- Po1 = Gi1/0/23 + Gi1/0/24 → SW-01 en LACP actif.
- Gi1/0/22 basculé en mode L3 par `no switchport` + IP `10.0.0.1/30` = TRANSIT1 vers FW-01 (interface LAN côté pfSense).
- Encapsulation trunk explicitement `dot1q` (3750-X supporte aussi ISL, défaut *auto*).

4.3.4 · SVI et HSRP Actif (groupes 10 et 20)

CORE-01, Vlan610 / Vlan620, HSRP Actif priorité 110 — CORE-01 running-config

```
interface Vlan610
 description ADMIN
 ip address 192.168.10.124 255.255.255.128
 standby 10 ip 192.168.10.126
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan620
 description ATELIER
 ip address 192.168.10.252 255.255.255.128
 standby 20 ip 192.168.10.254
 standby 20 priority 110
 standby 20 preempt
```

ANNOTATIONS

- VIP `192.168.10.126` (groupe 10) et `192.168.10.254` (groupe 20) = passerelles annoncées par DHCP.
- Priorité `110` > `100` (CORE-02 défaut) → CORE-01 élu Actif.
- `preempt` → CORE-01 reprend automatiquement Actif après reboot.
- Timers défaut (hello 3 s, holdtime 10 s) → RTO ≤ 10 s (`ENF-01`).

```
CORE-01.DEPANMOI.LAN#show standby brief
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl610       10   110 P Active  local           192.168.10.125  192.168.10.126
Vl620       20   110 P Active  local           192.168.10.253  192.168.10.254
CORE-01.DEPANMOI.LAN#
```

*Figure 4.4 · `show standby brief` sur CORE-01 : groupes 10 (Vl610) et 20 (Vl620) en état **Active**, priorité 110, préemption activée, VIP `192.168.10.126` et `192.168.10.254` .*

4.3.5 · OSPF area 0 · RID 1.1.1.1

CORE-01, OSPF process 1 — CORE-01 running-config

```
router ospf 1
 router-id 1.1.1.1
 passive-interface default
 no passive-interface GigabitEthernet1/0/22  ! TRANSIT1 vers FW-01
 no passive-interface Vlan610                ! adjacence inter-CORE via VLAN ADMIN
 no passive-interface Vlan620                ! adjacence inter-CORE via VLAN ATELIER
 network 10.0.0.0   0.0.0.3   area 0      ! TRANSIT1
 network 192.168.10.0   0.0.0.127 area 0  ! VLAN 610
 network 192.168.10.128 0.0.0.127 area 0  ! VLAN 620
 default-information originate
```

ANNOTATIONS

- `passive-interface default` bloque l'émission des hellos OSPF sur toutes les interfaces par défaut. Trois interfaces sont ensuite explicitement réactivées via `no passive-interface` : `Gi1/0/22` (transit vers FW-01, pour l'annonce de la route par défaut) et `Vlan610` / `Vlan620` (pour établir l'adjacence OSPF inter-CORE via les VLAN utilisateurs partagés sur SW-01). Sans ces deux dernières directives, CORE-01 et CORE-02 ne se voient pas en OSPF : ils n'ont alors plus qu'un seul chemin de propagation via FW-01, et la convergence sur perte du transit échoue.
- Trois préfixes annoncés en area 0 : TRANSIT1 + VLAN 610 + VLAN 620.

```
CORE-01.DEPANMOI.LAN#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:30    192.168.10.253  Vlan620
2.2.2.2           1   FULL/BDR        00:00:35    192.168.10.125  Vlan610
9.9.9.9           1   FULL/DR         00:00:38    10.0.0.2        GigabitEthernet1/0/22
CORE-01.DEPANMOI.LAN#
```

*Figure 4.5 · `show ip ospf neighbor` sur CORE-01 : trois adjacences en état **FULL** · CORE-02 (RID `2.2.2.2`) vu deux fois via `Vlan610` et `Vlan620` (adjacence inter-CORE redondante), FW-01 (RID `9.9.9.9`) via `GigabitEthernet1/0/22` (TRANSIT1).*

4.3.6 · DHCP · pools ADMIN / ATELIER + exclusions plage basse

CORE-01, service DHCP (sert .1–.60 ADMIN et .129–.188 ATELIER) — CORE-01 running-config

```
! Exclusions : moitié haute (servie par CORE-02) + plages IP statiques
ip dhcp excluded-address 192.168.10.0
ip dhcp excluded-address 192.168.10.61   192.168.10.126
ip dhcp excluded-address 192.168.10.128
ip dhcp excluded-address 192.168.10.189  192.168.10.254
!
ip dhcp pool ADMIN
 network 192.168.10.0 255.255.255.128
 default-router 192.168.10.126
 dns-server 10.0.0.2 10.0.0.6 1.1.1.1
 domain-name depanmoi.lan
!
ip dhcp pool ATELIER
 network 192.168.10.128 255.255.255.128
 default-router 192.168.10.254
 dns-server 10.0.0.2 10.0.0.6 1.1.1.1
 domain-name depanmoi.lan
```

ANNOTATIONS

- `default-router` = VIP HSRP du VLAN, bascule transparente côté client.
- `dns-server` = liste ordonnée. Clients interrogent `10.0.0.2` (pfSense côté TRANSIT1) en premier, puis `10.0.0.6` (pfSense côté TRANSIT2) si TRANSIT1 indisponible (reroute OSPF automatique), enfin `1.1.1.1` (Cloudflare) en dernier recours si pfSense HS complet. Permet la résolution des FQDN internes `*.depanmoi.lan` via le DNS Resolver pfSense (cf. section 4.5.5).
- Exclusions complémentaires de celles de CORE-02 → split-scope sans collision.

```
CORE-01.DEPANMOI.LAN#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.10.2     01cc.96e5.5ea3.29       Jan 03 2006 02:29 AM    Automatic  Active     Vlan610
CORE-01.DEPANMOI.LAN#
```

Figure 4.6 · `show ip dhcp binding` sur CORE-01 : bail actif `192.168.10.2` sur Vlan610, validant la distribution côté première moitié du split-scope (.1–.60).

4.4 · CORE-02 · Cœur L3 Standby

Paramètres miroir de CORE-01 : priorités HSRP / STP plus basses, IP transit 10.0.0.5, RID OSPF 2.2.2.2, exclusions DHCP inversées.

4.4.1 · Sécurisation

CORE-02, sécurisation (identique CORE-01 sauf clé RSA) — CORE-02.DEPANMOI.LAN running-config

```
service password-encryption
hostname CORE-02.DEPANMOI.LAN
ip domain-name depanmoi.lan
no ip domain-lookup
!
enable secret 5 $1$v5NI$5qRSYY6xu8p2LjFcaOT1A0
username admin privilege 15 secret 5 $1$bouN$HdlWs1SJBS/OEXJctfMt21
!
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh logging events
ip ssh server algorithm encryption aes256-ctr aes192-ctr aes128-ctr
ip ssh server algorithm mac hmac-sha1
ip ssh server algorithm hostkey ssh-rsa
!
line vty 0 4
 transport input ssh
 login local
line vty 5 15
 transport input ssh
 login local
```

4.4.2 · Spanning Tree · secondary

CORE-02, STP secondary — CORE-02 running-config

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 610,620 priority 8192
```

4.4.3 · VLAN, Port-channel et transit

CORE-02, Po1 vers SW-01 et Gi1/0/22 vers FW-01 — CORE-02 running-config

```
vlan 610
 name ADMIN
!
vlan 620
 name ATELIER
!
interface Port-channel1
 description UPLINK VERS SW-01
 switchport trunk allowed vlan 610,620
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 description UPLINK VERS SW-01
 switchport trunk allowed vlan 610,620
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/24
 description UPLINK VERS SW-01
 switchport trunk allowed vlan 610,620
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/22
 description LAN NetGate pfSense
 no switchport
 ip address 10.0.0.5 255.255.255.252
```

4.4.4 · SVI et HSRP Standby

CORE-02, Vlan610 / Vlan620, HSRP Standby (priorité 100 défaut) — CORE-02 running-config

```
interface Vlan610
 description ADMIN
 ip address 192.168.10.125 255.255.255.128
 standby 10 ip 192.168.10.126
 standby 10 preempt
!
interface Vlan620
 description ATELIER
 ip address 192.168.10.253 255.255.255.128
 standby 20 ip 192.168.10.254
 standby 20 preempt
```

ANNOTATIONS

- Pas de `standby N priority` → priorité 100 par défaut → Standby.
- `preempt` conservé → si CORE-02 prend Active suite à panne CORE-01, le retour de CORE-01 reprendra le rôle.

```
CORE-02.DEPANMOI.LAN#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl610       10   100 P Standby 192.168.10.124  local           192.168.10.126
Vl620       20   100 P Standby 192.168.10.252  local           192.168.10.254
CORE-02.DEPANMOI.LAN#
```

*Figure 4.7 · `show standby brief` sur CORE-02 : groupes 10 (Vl610) et 20 (Vl620) en état **Standby**, priorité 100, préemption activée, Active distant `192.168.10.124` / `192.168.10.252` (CORE-01).*

4.4.5 · OSPF area 0 · RID 2.2.2.2

CORE-02, OSPF process 1 — CORE-02 running-config

```
router ospf 1
 router-id 2.2.2.2
 passive-interface default
 no passive-interface GigabitEthernet1/0/22  ! TRANSIT2 vers FW-01
 no passive-interface Vlan610                ! adjacence inter-CORE via VLAN ADMIN
 no passive-interface Vlan620                ! adjacence inter-CORE via VLAN ATELIER
 network 10.0.0.4   0.0.0.3   area 0      ! TRANSIT2
 network 192.168.10.0   0.0.0.127 area 0
 network 192.168.10.128 0.0.0.127 area 0
```

ANNOTATIONS

- Annonce TRANSIT2 (`10.0.0.4/30`) au lieu de TRANSIT1.
- Identique à CORE-01 sur la gestion `passive-interface` : `no passive-interface` sur le transit vers FW-01 + sur `Vlan610` et `Vlan620` pour entretenir l'adjacence OSPF directe avec CORE-01 via les VLAN utilisateurs.

4.4.6 · DHCP · exclusions plage haute

CORE-02, exclusions miroir (sert .61–.120 ADMIN et .189–.248 ATELIER) — CORE-02 running-config

```
! Exclusions : moitié basse (servie par CORE-01) + plages statiques
ip dhcp excluded-address 192.168.10.0    192.168.10.60
ip dhcp excluded-address 192.168.10.121  192.168.10.126
ip dhcp excluded-address 192.168.10.128  192.168.10.188
ip dhcp excluded-address 192.168.10.249  192.168.10.254
!
ip dhcp pool ADMIN
 network 192.168.10.0 255.255.255.128
 default-router 192.168.10.126
 dns-server 10.0.0.2 10.0.0.6 1.1.1.1
 domain-name depanmoi.lan
!
ip dhcp pool ATELIER
 network 192.168.10.128 255.255.255.128
 default-router 192.168.10.254
 dns-server 10.0.0.2 10.0.0.6 1.1.1.1
 domain-name depanmoi.lan
```

VLAN	Plage utilisable	Servie par CORE-01	Servie par CORE-02	Statiques
610 ADMIN	.1 → .120	.1 → .60	.61 → .120	.121 → .126
620 ATELIER	.129 → .248	.129 → .188	.189 → .248	.249 → .254

```
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.10.61    01cc.96e5.5ea3.29       Jan 03 2006 01:04 AM    Automatic  Active     Vlan610
CORE-02.DEPANMOI.LAN#
```

Figure 4.8 · `show ip dhcp binding` sur CORE-02 : bail actif `192.168.10.61` sur Vlan610, validant la distribution côté seconde moitié du split-scope (.61–.120).

4.5 · FW-01 · Pare-feu pfSense

4.5.1 · Interfaces · WAN, LAN (TRANSIT1), OPT (TRANSIT2)

Rôle pfSense	Description	Adressage	Côté CORE
WAN	Sortie Internet	DHCP FAI	—
LAN	TRANSIT1, adjacence OSPF avec CORE-01	10.0.0.2/30 statique	CORE-01 Gi1/0/22 = 10.0.0.1
OPT	TRANSIT2, adjacence OSPF avec CORE-02	10.0.0.6/30 statique	CORE-02 Gi1/0/22 = 10.0.0.5

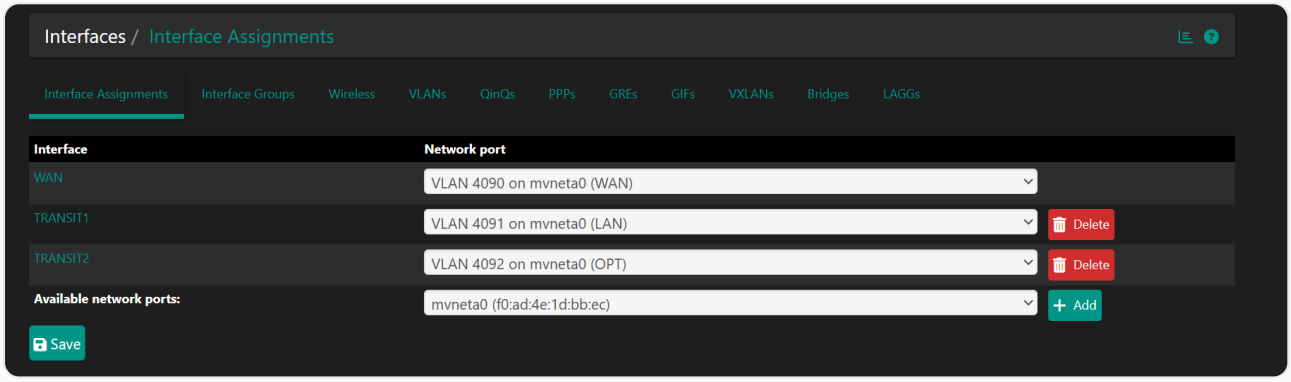


Figure 4.9 · pfSense Interfaces → Interface Assignments : WAN (VLAN 4090 sur mvneta0), TRANSIT1 (VLAN 4091, port LAN, transit vers CORE-01), TRANSIT2 (VLAN 4092, port OPT, transit vers CORE-02).

4.5.2 · FRR / OSPF · installation et paramétrage

Le routage dynamique côté pfSense est assuré par le paquet **FRR** (Free Range Routing), à installer via le gestionnaire de paquets puis à paramétrer en cinq étapes : installation, paramétrage global, activation du démon OSPF, déclaration des interfaces, vérification des adjacences.

ÉTAPE 1 · INSTALLATION DU PAQUET FRR

1. Menu *System* → *Package Manager* → onglet *Available Packages*.
2. Rechercher `FRR`, cliquer sur *Install* à côté de *FRR routing daemon for BGP, OSPF, OSPF6 and RIP*.
3. Une fois installé, FRR apparaît dans *Services* avec ses sous-onglets (Global, BGP, OSPF, OSPF6, RIP, BFD, ...).

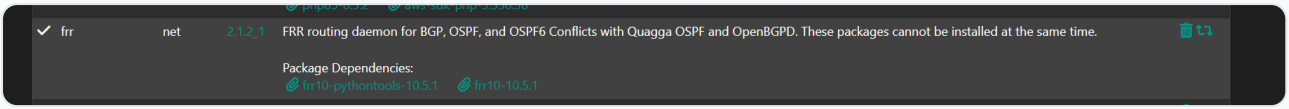


Figure 4.10 · pfSense System → Package Manager → Installed Packages : paquet `frr 2.1.2_1` (FRR routing daemon, BGP / OSPF / OSPF6) installé, dépendances `frr10-10.5.1` et `frr10-pythontools-10.5.1`.

ÉTAPE 2 · PARAMÉTRAGE GLOBAL DE FRR

1. Aller dans *Services* → *FRR* → onglet *Global Settings*.
2. Cocher **Enable**.
3. Renseigner **Router ID** = `9.9.9.9`, identifiant OSPF de FW-01, distinct des CORE (1.1.1.1 et 2.2.2.2).
4. Définir un **Master Password** pour la console FRR (utilisé uniquement pour l'accès `vtysh`, pas exposé sur le réseau).
5. Activer *Logging* (utile pour le diagnostic).
6. Enregistrer.

ÉTAPE 3 · ACTIVATION DU DÉMON OSPF (OSPFV2)

1. Aller dans *Services* → *FRR* → onglet *[OSPF]*.
2. Cocher **Enable OSPF**.
3. Renseigner **Router ID** = `9.9.9.9` (même valeur que le Global).
4. Section *Redistribute* : cocher **Redistribute Connected Subnets**. Cela publie automatiquement les préfixes connectés directement à FW-01 (TRANSIT1 et TRANSIT2) dans la zone OSPF 0, chaque CORE les verra apparaître en route `O E2`. Métrique : `1`, type métrique : `2` (External Type 2, coût constant indépendant du chemin interne).
5. Cocher **Redistribute Default Route** et **Always**. Cela injecte une route par défaut `O*E2` dans le domaine OSPF, *même si le WAN n'a pas encore obtenu sa default DHCP*. Cette précaution garantit que les CORE disposent toujours d'une sortie nominale tant que FW-01 répond, sans attendre la convergence WAN.
6. Métrique default : `0`, type : `2`.
7. Champ *ABR Type* : `cisco` (compatibilité ABR, sans effet ici, zone unique area 0).
8. Enregistrer.

ÉTAPE 4 · DÉCLARATION DES INTERFACES OSPF

1. Toujours dans *Services* → *FRR* → *[OSPF]*, ouvrir l'onglet *Interfaces*.
2. Ajouter une entrée pour **lan** (TRANSIT1 vers CORE-01) : *Interface* = `lan`, *Area* = `0.0.0.0`, *Metric* = `1`. Le sous-réseau OSPF est déduit automatiquement de l'adresse IP affectée à l'interface (10.0.0.0/30), aucun champ *Network* à renseigner ici.
3. Ajouter une entrée pour **opt1** (TRANSIT2 vers CORE-02) : *Interface* = `opt1`, *Area* = `0.0.0.0`, *Metric* = `1`.
4. Laisser les autres interfaces (WAN notamment) **non déclarées**, pas de hellos OSPF côté Internet.
5. Enregistrer et appliquer.

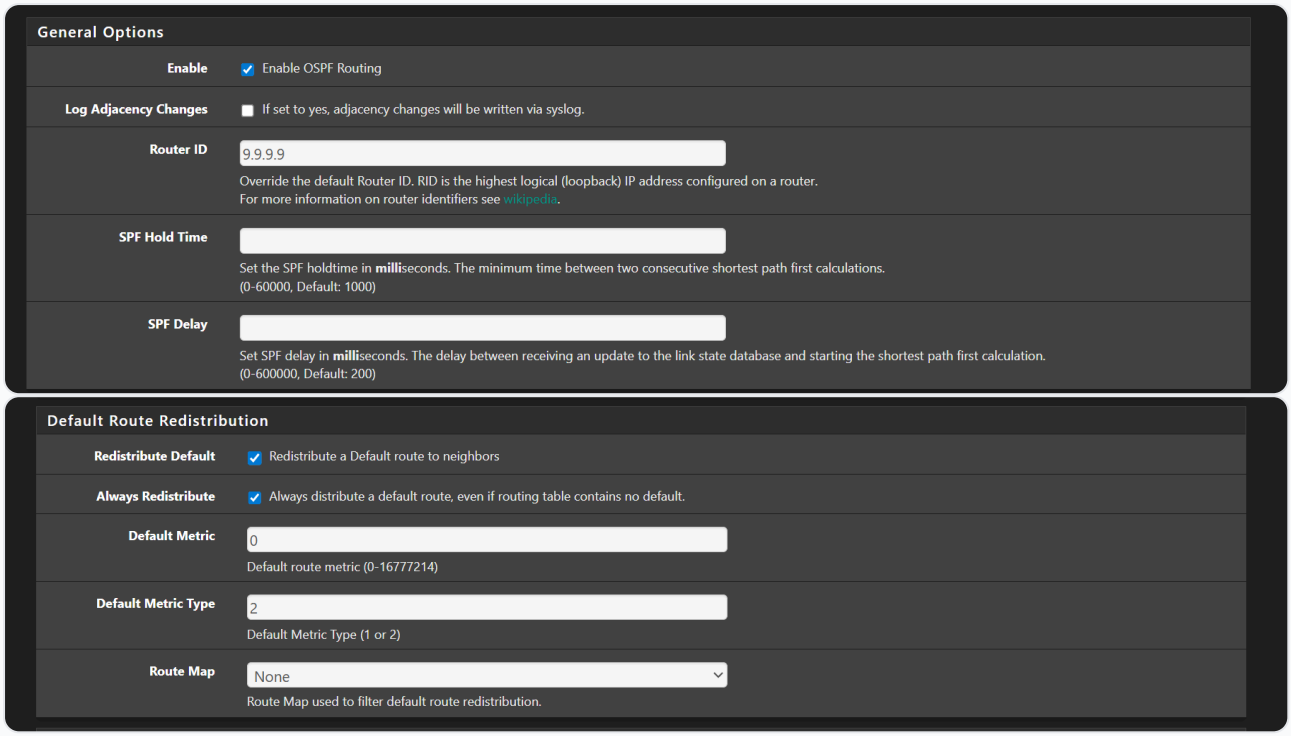


*Figure 4.11 · pfSense Services → FRR → OSPF : (haut) **General Options** avec OSPF activé et Router ID `9.9.9.9` ; (bas) **Default Route Redistribution** avec Redistribute Default et Always Redistribute cochés (Metric Type 2), pour propager la route par défaut vers les CORE.*

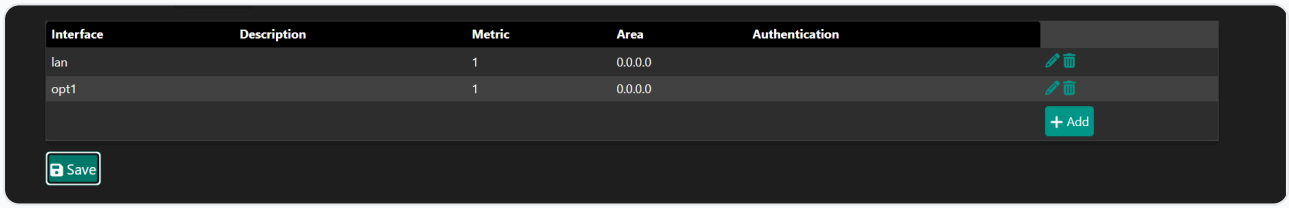


Figure 4.12 · pfSense Services → FRR → OSPF → Interfaces : interfaces `lan` (TRANSIT1 vers CORE-01) et `opt1` (TRANSIT2 vers CORE-02) déclarées en area 0.0.0.0, metric 1. Le sous-réseau est déduit automatiquement de l'IP de l'interface, aucun préfixe à saisir ici.

ÉTAPE 5 · VÉRIFICATION DES ADJACENCES

1. Aller dans *Status* → *FRR* → onglet *OSPF*.
2. Section *Neighbors* : deux voisins doivent apparaître, l'un avec RID `1.1.1.1` (CORE-01, sur LAN), l'autre avec RID `2.2.2.2` (CORE-02, sur OPT).
3. État attendu pour chaque voisin : **Full**.
4. Section *Routes* : doit lister les VLAN 192.168.10.0/25 et 192.168.10.128/25 reçus par OSPF (deux chemins ECMP, un par cœur).

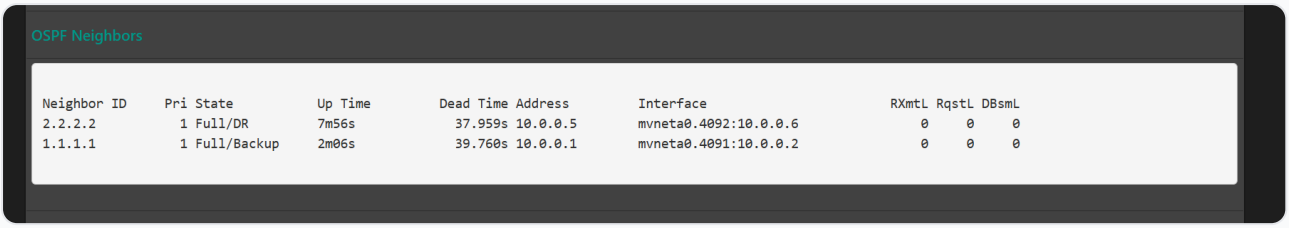


Figure 4.13 · pfSense Status → FRR → OSPF → Neighbors : adjacences OSPF établies avec CORE-01 (RID `1.1.1.1` , Full/Backup via TRANSIT1 `10.0.0.1`) et CORE-02 (RID `2.2.2.2` , Full/DR via TRANSIT2 `10.0.0.5`).

4.5.3 · NAT outbound · sortie Internet

RÈGLE NAT OUTBOUND (MODE HYBRIDE)

Mode NAT outbound = **hybride**, règles automatiques pfSense + règles explicites. Règle utilisateur : interface `WAN` , source `192.168.10.0/24` , destination `any` , traduction `WAN address` . Description *NAT LAN vers Internet*.

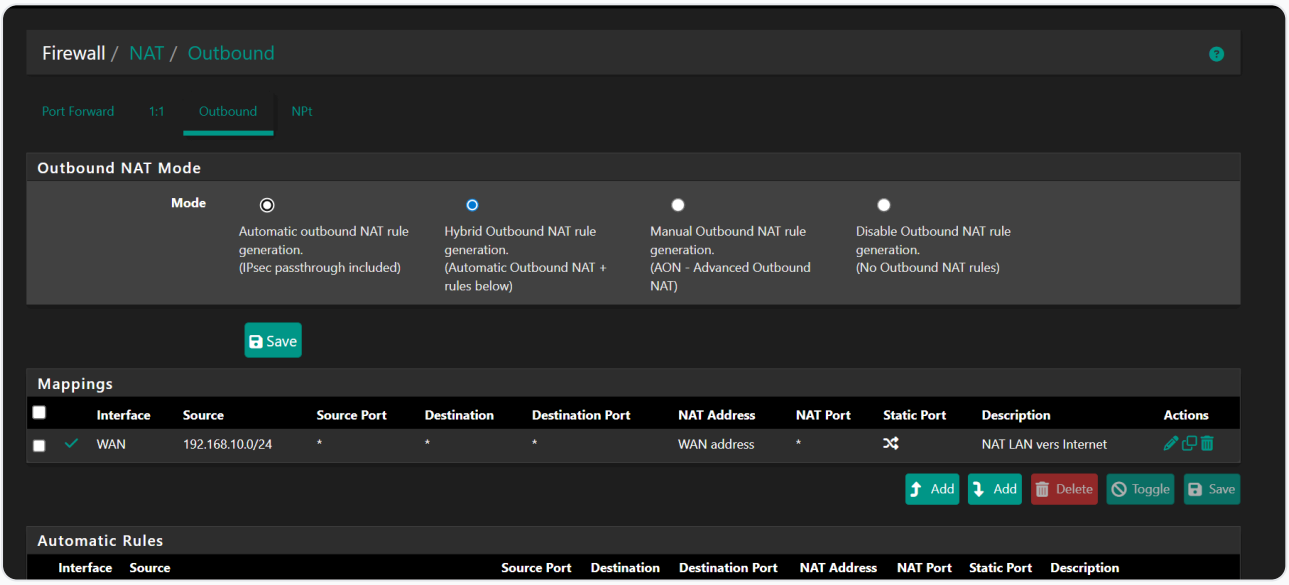


*Figure 4.14 · pfSense Firewall → NAT → Outbound : mode **Hybrid Outbound NAT** activé, règle manuelle « NAT LAN vers Internet » qui translate `192.168.10.0/24` en WAN address sur l'interface WAN.*

4.5.4 · Règles de filtrage

Interface	Description	Action	Source / Destination
LAN (TRANSIT1)	OSPF voisinage	Pass	OSPF (proto 89), voisin CORE-01
LAN (TRANSIT1)	LAN DEPANMOI vers Internet	Pass	192.168.10.0/24 → any (via WAN)
OPT (TRANSIT2)	OSPF voisinage	Pass	OSPF (proto 89), voisin CORE-02
OPT (TRANSIT2)	LAN DEPANMOI vers Internet	Pass	192.168.10.0/24 → any (via WAN)
WAN	Politique par défaut	Block	any → any (sauf flux retour state)

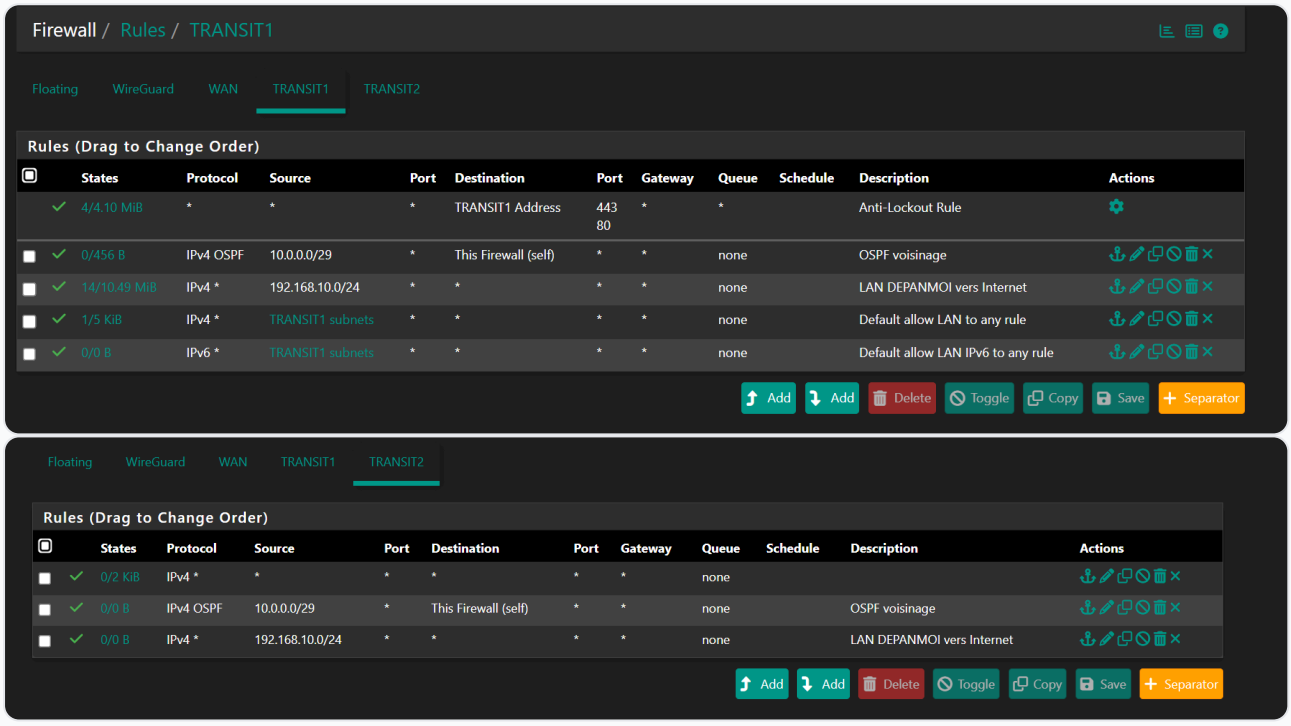


*Figure 4.15 · pfSense Firewall → Rules, onglets **TRANSIT1** (haut) et **TRANSIT2** (bas) : règles miroir OSPF voisinage (source `10.0.0.0/29` vers This Firewall self) et LAN DEPANMOI vers Internet (source `192.168.10.0/24`).*

4.5.5 · DNS Resolver · résolution interne et fallback public

Le résolveur DNS embarqué sur pfSense (Unbound) est activé pour assurer deux fonctions complémentaires : la résolution des FQDN internes `*.depanmoi.lan` (CORE-01, CORE-02, SW-01, FW-01) pour les besoins d'exploitation, et la résolution des noms publics pour les clients via forwarding vers des DNS de référence (Cloudflare `1.1.1.1`, Quad9 `9.9.9.9`). Les clients DHCP reçoivent comme serveurs DNS, dans l'ordre, les deux adresses pfSense côté transit (`10.0.0.2` et `10.0.0.6`) puis `1.1.1.1` en filet de secours, cf. section 4.3.6.

ÉTAPE 1 · ACTIVATION DU DNS RESOLVER

1. Menu *Services* → *DNS Resolver* → onglet *General Settings*.

2. Cocher **Enable DNS Resolver**.
3. *Network Interfaces* : sélectionner `Loopback`, `TRANSIT1` (lan) et `TRANSIT2` (opt1). **Ne pas cocher WAN** : le résolveur ne doit pas répondre depuis l'extérieur.
4. *Outgoing Network Interfaces* : cocher `WAN` uniquement, c'est par lui que les requêtes vers les DNS publics sortent.
5. Cocher **DNSSEC** (validation des signatures DNS, recommandée).
6. Cocher **Enable Forwarding Mode** : Unbound forwarde les requêtes non locales vers les DNS déclarés dans *System → General Setup*, au lieu de résoudre lui-même depuis la racine. Cohérent avec le choix d'un résolveur amont fiable.
7. Onglet *Access Lists* (en haut de la page *DNS Resolver*), bouton *Add* : créer une **Access List** qui autorise explicitement les réseaux clients et les transits à interroger Unbound. Sans cette ACL, Unbound applique son comportement par défaut (`refuse` pour toute source hors `127.0.0.0/8` et ::1), et les postes des VLAN 610 et 620 reçoivent `Query refused` alors même que le pare-feu pf laisse passer le port 53.

Champ	Valeur
Access List name	`Resolve`
Action	`Allow`
Networks	`192.168.10.0/24` (postes clients VLAN 610 + 620) `10.0.0.0/29` (transits OSPF TRANSIT1 + TRANSIT2)

8. Enregistrer et appliquer.

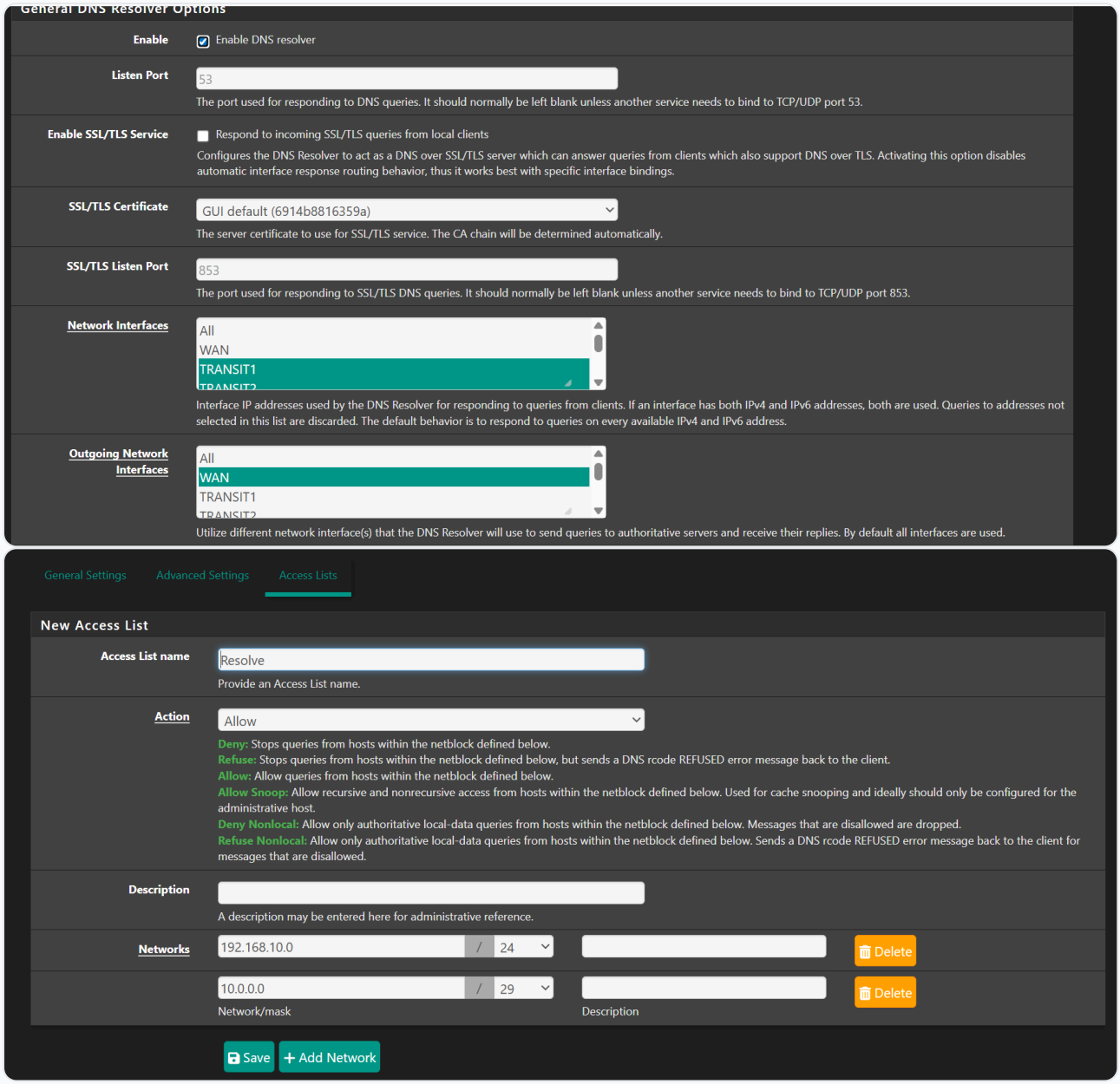


*Figure 4.16 · pfSense Services → DNS Resolver : (haut) General Settings avec Unbound activé sur port 53, Network Interfaces = TRANSIT1 et TRANSIT2 (et Loopback), Outgoing = WAN ; (bas) Access Lists avec l'ACL **Resolve** (action Allow) couvrant `192.168.10.0/24` et `10.0.0.0/29`.*

ÉTAPE 2 · DÉCLARATION DES DNS AMONT (FORWARDERS)

1. Menu *System* → *General Setup*.
2. *DNS Servers* : renseigner `1.1.1.1` (Cloudflare) et `9.9.9.9` (Quad9), chacun avec *Gateway* = `WAN_DHCP` ou la gateway WAN nommée.
3. *DNS Server Override* : **décocher** pour ne pas laisser le FAI imposer ses DNS. La politique DNS interne reste sous contrôle de l'administrateur.
4. Enregistrer.

ÉTAPE 3 · HOST OVERRIDES · FQDN INTERNES `*.DEPANMOI.LAN`

Section *Host Overrides* de *Services → DNS Resolver*. Ajouter une entrée par équipement :

Host	Domain	IP Address	Description
`core-01`	`depanmoi.lan`	`192.168.10.124`	SVI Vlan610 CORE-01 (interface de management privilégiée)
`core-02`	`depanmoi.lan`	`192.168.10.125`	SVI Vlan610 CORE-02
`sw-01`	`depanmoi.lan`	`192.168.10.22`	SVI management SW-01
`fw-01`	`depanmoi.lan`	`10.0.0.2` , `10.0.0.6`	IP TRANSIT1 + TRANSIT2 de pfSense, deux entrées pour redondance (résolution aboutit même si un transit est down)

Un poste client peut alors taper `ssh admin@core-01.depanmoi.lan` au lieu de mémoriser l'IP. La cohérence avec les `hostname` Cisco (`CORE-01.DEPANMOI.LAN`) est respectée à la casse près (DNS est insensible à la casse).

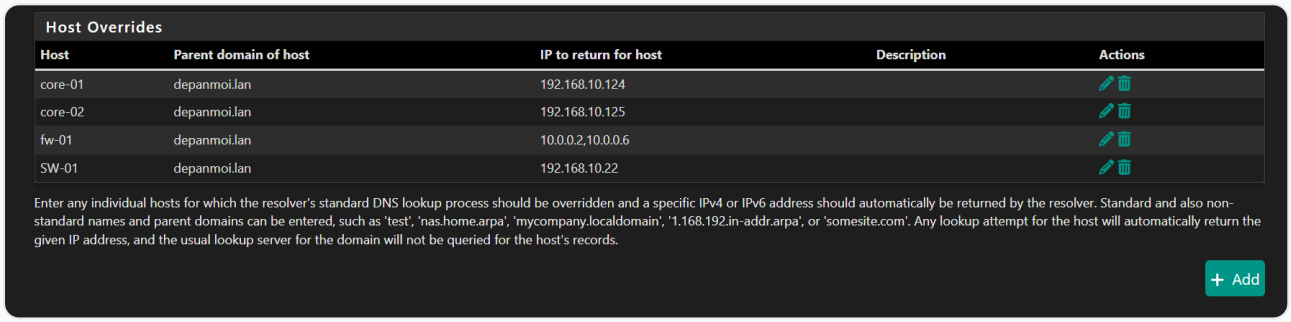


Figure 4.17 · pfSense DNS Resolver → Host Overrides : quatre entrées résolvent les FQDN internes sans dépendance à un serveur externe (`core-01.depanmoi.lan → 192.168.10.124` , `core-02.depanmoi.lan → 192.168.10.125` , `fw-01.depanmoi.lan → 10.0.0.2, 10.0.0.6` , `SW-01.depanmoi.lan → 192.168.10.22`).

ÉTAPE 4 · RÈGLE PARE-FEU DNS

Le port **53/UDP** et **53/TCP** doit être accessible depuis les sous-réseaux clients vers *This Firewall (self)*. La règle existante *« LAN DEPANMOI vers Internet »* (source `192.168.10.0/24` → any) sur TRANSIT1 et TRANSIT2 autorise déjà ce flux, **aucune règle dédiée n'est ajoutée**. Le filtrage applicatif des requêtes DNS est assuré côté Unbound par la directive `access-control` (étape 1), qui constitue la seule barrière nécessaire à ce niveau.

> **PARE-FEU PF VS `ACCESS-CONTROL` UNBOUND · NIVEAUX DISTINCTS**
>
> La règle de pare-feu pfSense contrôle le passage du **paquet** au niveau réseau (couche 3/4 : source, destination, port). La directive `access-control` d'Unbound contrôle le **droit de réponse** au niveau applicatif (couche 7 : Unbound accepte-t-il de servir cette source ?). Les deux sont nécessaires : si le pare-feu bloque le port 53, Unbound ne voit jamais la requête. Si le pare-feu laisse passer mais qu'`access-control` refuse, le client reçoit `Query refused`. C'est ce second cas qui a été rencontré et corrigé par l'ajout explicite des deux directives `access-control` en étape 1.

ÉTAPE 5 · VÉRIFICATION

1. Depuis un poste DHCP du VLAN 610 :

```
nslookup core-01.depanmoi.lan
! attendu : 192.168.10.124

nslookup core-02.depanmoi.lan
! attendu : 192.168.10.125

nslookup google.com
! attendu : réponse Cloudflare via 10.0.0.2 ou 10.0.0.6
```

2. Sur pfSense : *Status → DNS Resolver* ou *Diagnostics → DNS Lookup*, vérifier que les requêtes sortent bien par WAN.
3. Couper TRANSIT1 (test T-05 déjà documenté), refaire `nslookup google.com` depuis le poste : la résolution doit toujours aboutir, OSPF ayant rerouté via TRANSIT2 (`10.0.0.6`).

```
C:\Users\Kairrin>nslookup core-01.depanmoi.lan
Serveur :   pfsense.depanmoi.lan
Address:  10.0.0.2

Nom :    core-01.depanmoi.lan
Address:  192.168.10.124


C:\Users\Kairrin>nslookup core-02.depanmoi.lan
Serveur :   pfsense.depanmoi.lan
Address:  10.0.0.2

Nom :    core-02.depanmoi.lan
Address:  192.168.10.125


C:\Users\Kairrin>nslookup google.com
Serveur :   pfsense.depanmoi.lan
Address:  10.0.0.2

Réponse ne faisant pas autorité :
Nom :    google.com
Addresses:  2a00:1450:4007:817::200e
          172.217.22.78
```

Figure 4.18 · Vérification DNS depuis un poste client : `nslookup core-01.depanmoi.lan` retourne `192.168.10.124` , `nslookup core-02.depanmoi.lan` retourne `192.168.10.125` (Host Overrides), `nslookup google.com` retourne une réponse non autoritative `172.217.22.78` + IPv6 (forwarders publics). Serveur interrogé : `pfsense.depanmoi.lan` (`10.0.0.2`).

> **POURQUOI PAS LE DNS FORWARDER (`DNSMASQ`) ?**
>
> pfSense propose historiquement deux résolveurs : **DNS Resolver** (Unbound, par défaut) et **DNS Forwarder** (dnsmasq). Unbound est retenu pour trois raisons : il supporte nativement **DNSSEC**, il est **maintenu activement** en amont (NLnet Labs), et il intègre par défaut la **limitation du débit** et la **protection contre les attaques DNS** (cache poisoning, amplification). Le DNS Forwarder reste utile pour des cas spécifiques (intégration DHCP très fine) mais n'apporte rien ici par rapport à Unbound. Les deux services ne peuvent pas écouter simultanément sur le même port 53, dnsmasq est laissé désactivé.

CONFORMITÉ AUX EXIGENCES DU CAHIER DES CHARGES

- **EF-01 à EF-07**, couvertes par 4.2 à 4.5.
- **EF-08 à EF-10** (Won't), pas de configuration (CARP non activé sur FW-01, pas de second WAN, pas de 802.1X), conforme aux exclusions explicites.
- **ENF-01 à ENF-06** et **ENF-08**, testées en partie 5 (seuils mesurables). **ENF-07** (sauvegarde des configurations de référence) couverte par les fichiers archivés en annexes section 7.3.

PARTIE 5

Plan de tests et validation

5.1 · Méthodologie

Chaque test couvre une ou plusieurs exigences du cahier des charges (`EF-XX` fonctionnelles, `ENF-XX` non fonctionnelles). La fiche précise l'identifiant, la procédure, le résultat attendu et le résultat observé. Les preuves sont apportées par captures d'écran intégrées (terminal Cisco, `ipconfig` / `ip a` , Wireshark, console pfSense). La synthèse 5.4 récapitule la couverture globale.

Catégorie	Tests	Outils mobilisés
Fonctionnels	T-01 à T-07, segmentation, HSRP, LACP, OSPF, DHCP, SSH/Telnet	`ping` , `tracert` , `ipconfig` , `ip a` , PuTTY, terminal IOS, `iperf3` , Wireshark
Transverses	T-08, T-09, FQDN, documentation	Cisco IOS `show` , exports XML pfSense, dépôt fichiers

5.2 · Tests fonctionnels

Test T-01 : Segmentation VLAN · isolation ADMIN / ATELIER

Exigence couverte : `EF-01` . **Statut :** VALIDÉ

Procédure :

1. Brancher poste A sur SW-01 `F0/1` (VLAN 610). IP par DHCP dans `192.168.10.0/25` .
2. Brancher poste B sur SW-01 `F0/11` (VLAN 620). IP dans `192.168.10.128/25` .
3. Sur poste A, retirer la route par défaut puis `ping IP_poste_B` .
4. Restaurer la route par défaut (VIP `192.168.10.126`) puis relancer le ping.

Résultat attendu : étape 3, pas d'écho ICMP (isolation L2). Étape 4, ping réussi via routage L3 par CORE-01.

Résultat observé : conforme. Isolation L2 confirmée sans gateway, communication L3 rétablie via VIP HSRP.

Figure 5.1 · Test T-01, ping de poste A (VLAN 610) vers poste B (`192.168.10.129` , VLAN 620) : Délai d'attente dépassé tant que le poste A n'a pas de passerelle (isolation L2 confirmée), puis succès `TTL=127` dès l'ajout de la VIP HSRP `192.168.10.126` comme route par défaut.

Test T-02 : Bascule HSRP · coupure du cœur Actif

Exigences couvertes : `EF-02` , `ENF-01` . **Statut :** VALIDÉ

Procédure :

1. Depuis poste VLAN 610 : `ping -t 192.168.10.126` (VIP) et `ping -t 1.1.1.1` .
2. Sur CORE-01 : `conf t` → `interface Vlan610` → `shutdown` . Idem `Vlan620` .
3. Compter les pings perdus avant reprise.
4. Sur CORE-02 : `show standby brief` → état `Active` sur groupes 10 et 20.

Résultat attendu : RTO < 10 s (holdtime HSRP par défaut). Pings reprennent automatiquement, CORE-02 prend Active sans intervention.

Résultat observé : bascule conforme. Quelques pings perdus le temps de la reprise. Sessions TCP utilisateurs préservées.

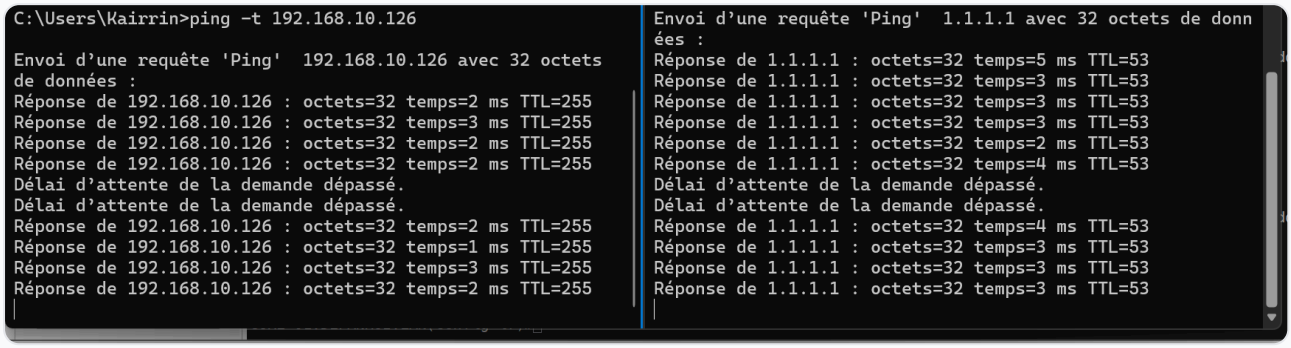


Figure 5.2 · Test T-02, bascule HSRP : ping continu vers la VIP `192.168.10.126` (gauche, TTL 255) et vers `1.1.1.1` via Internet (droite, TTL 53). Deux requêtes en Délai d'attente dépassé au moment de la coupure de CORE-01, puis reprise immédiate après bascule sur CORE-02.

Test T-03 : Préemption HSRP · retour de CORE-01

Exigence couverte : `EF-03` . **Statut :** VALIDÉ

Procédure :

1. État de départ : CORE-01 coupé (suite à T-02), CORE-02 Actif.
2. Sur CORE-01 : `conf t` → `interface Vlan610` → `no shutdown` . Idem `Vlan620` .
3. Chronomètre, puis `show standby brief` sur CORE-01.

Résultat attendu : CORE-01 reprend Active sur les groupes 10 et 20 en moins de 30 s grâce à `standby preempt` , sans intervention manuelle sur CORE-02.

Résultat observé : préemption fonctionnelle. Retour à la configuration nominale (CORE-01 Actif, CORE-02 Standby).

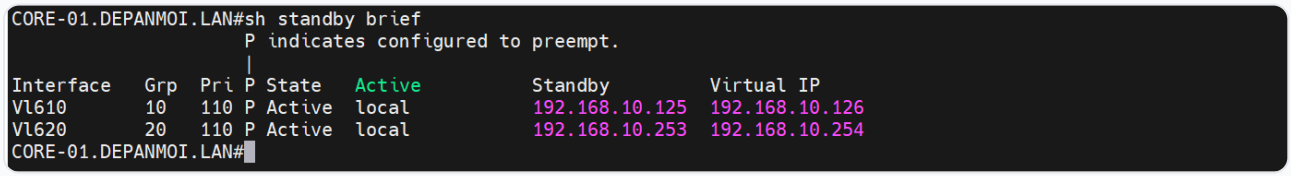


*Figure 5.3 · Test T-03, préemption HSRP : après remise en service de CORE-01, `show standby brief` affiche **Active local** sur Vl610 et Vl620 (priorité 110, flag `P` preempt). Reprise automatique du rôle nominal sans intervention manuelle sur CORE-02.*

Test T-04 : Coupure d'un lien d'EtherChannel LACP

Exigences couvertes : `EF-04`, `ENF-03`. **Statut :** VALIDÉ

Procédure :

1. Vérifier `show etherchannel summary` sur SW-01 → `Po1 (SU) Fa0/21(P) Fa0/22(P)`.
2. `ping -t` de poste à poste inter-VLAN (passe par CORE-01 via Po1).
3. Sur SW-01 : `interface FastEthernet0/21` → `shutdown`.
4. Observer les pertes de paquets sur le ping.
5. `show etherchannel summary` → `Po1 (SU) Fa0/21(D) Fa0/22(P)`.
6. Optionnel : `iperf3` avant/après pour mesurer la bande passante.

Résultat attendu : bascule transparente, perte ≤ 1 paquet sur le ping. EtherChannel reste Up avec un seul membre. Bande passante chute de ~200 à ~100 Mb/s.

Résultat observé : conforme. Re-up de F0/21 par `no shutdown` → réintégration immédiate dans Po1 sans coupure.

```
Accepted connection from 192.168.10.129, port 62893
[  5] local 192.168.10.64 port 5201 connected to 192.168.10.129 port 62894
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  10.1 MBytes  84.7 Mbits/sec
[  5]   1.00-2.01   sec  10.1 MBytes  84.5 Mbits/sec
[  5]   2.01-3.00   sec  10.0 MBytes  84.2 Mbits/sec
[  5]   3.00-4.01   sec  10.8 MBytes  89.2 Mbits/sec
[  5]   4.01-5.00   sec  10.6 MBytes  90.4 Mbits/sec
[  5]   5.00-6.01   sec  10.9 MBytes  90.1 Mbits/sec
[  5]   6.01-7.00   sec  10.6 MBytes  90.2 Mbits/sec
[  5]   7.00-8.00   sec  10.2 MBytes  86.1 Mbits/sec
[  5]   8.00-9.01   sec  10.6 MBytes  87.9 Mbits/sec
[  5]   9.01-10.01  sec  10.4 MBytes  87.9 Mbits/sec
[  5]  10.01-10.02  sec   128 KBytes   106 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.02  sec   104 MBytes  87.5 Mbits/sec                  receiver
```

*Figure 5.4 · Test T-04, mesure `iperf3` inter-VLAN à travers l'EtherChannel : poste source `192.168.10.129` (VLAN 620) vers poste destination `192.168.10.64` (VLAN 610), débit moyen **87.5 Mbits/sec** sur 10 s, 104 MBytes transférés. La bande passante reste stable, preuve que le bundle Po1 transporte le flux sans dégradation.*

Test T-05 : Convergence OSPF · coupure d'un transit cœur ↔ FW-01

Exigences couvertes : `EF-05`, `ENF-02`. **Statut :** VALIDÉ

Procédure :

1. `show ip ospf neighbor` sur CORE-01/CORE-02 → état **FULL** avec FW-01 (RID 9.9.9.9).
2. `ping -t 1.1.1.1` depuis un poste utilisateur.
3. Sur FW-01 : *Interfaces → LAN → Disable* (ou débrancher Gi1/0/22 côté CORE-01).
4. Mesurer la durée de coupure du ping.

5. Sur les CORE : `show ip route ospf` → default `O*E2` doit pointer vers `10.0.0.6`.

Résultat attendu : convergence OSPF < 5 s (détection link-down + recalc SPF). Trafic Internet rétabli automatiquement via TRANSIT2.

Résultat observé : reroute conforme. Perte de TRANSIT1 absorbée par OSPF, FW-01 reste joignable via TRANSIT2.

```
CORE-01.DEPANMOI.LAN#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:35    192.168.10.253  Vlan620
2.2.2.2           1   FULL/BDR        00:00:37    192.168.10.125  Vlan610
CORE-01.DEPANMOI.LAN#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.10.253 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/10] via 192.168.10.253, 00:00:21, Vlan620
                [110/10] via 192.168.10.125, 00:00:21, Vlan610
      10.0.0.0/30 is subnetted, 2 subnets
O        10.0.0.0 [110/3] via 192.168.10.253, 00:00:21, Vlan620
                  [110/3] via 192.168.10.125, 00:00:21, Vlan610
O        10.0.0.4 [110/2] via 192.168.10.253, 00:01:12, Vlan620
                  [110/2] via 192.168.10.125, 00:01:12, Vlan610
O E2  192.168.1.0/24 [110/1] via 192.168.10.253, 00:00:21, Vlan620
                     [110/1] via 192.168.10.125, 00:00:21, Vlan610
CORE-01.DEPANMOI.LAN#
```

*Figure 5.5 · Test T-05, convergence OSPF sur CORE-01 après coupure du transit vers FW-01. `show ip ospf neighbor` : adjacences **FULL** avec CORE-02 (RID `2.2.2.2`) maintenues via `Vlan610` et `Vlan620`. `show ip route ospf` : route par défaut `O*E2` réinjectée en ECMP via `192.168.10.253` et `192.168.10.125` (SVI CORE-02), sortie Internet préservée par contournement.*

Test T-06 : Distribution DHCP en split-scope

Exigence couverte : `EF-06`. **Statut :** VALIDÉ

Procédure :

1. Brancher 3 postes successivement sur `F0/1` à `F0/3` (VLAN 610).
2. Relever les baux : `ipconfig /all` ou `ip a`.
3. Sur les CORE : `show ip dhcp binding`.
4. Vérifier qu'aucune adresse n'est servie deux fois.
5. Refaire sur VLAN 620 (`F0/11` à `F0/13`).

Résultat attendu : baux distincts. `.1-.60` (CORE-01) et `.61-.120` (CORE-02) sur VLAN 610. `.129-.188` (CORE-01) et `.189-.248` (CORE-02) sur VLAN 620.

Résultat observé : split-scope fonctionnel. Pas de collision, gateway fixée sur la VIP HSRP.

```
CORE-01.DEPANMOI.LAN#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.10.3     01c4.6516.f06a.56       Jan 03 2006 06:12 AM    Automatic  Active     Vlan610
CORE-01.DEPANMOI.LAN#
```

```
CORE-02.DEPANMOI.LAN#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.10.64    01cc.96e5.5ea3.29       Jan 03 2006 06:29 AM    Automatic  Active     Vlan610
CORE-02.DEPANMOI.LAN#
```

Figure 5.6 · Test T-06, split-scope DHCP : (haut) CORE-01 distribue `192.168.10.3` (∈ .1–.60), (bas) CORE-02 distribue `192.168.10.64` (∈ .61–.120). Plages disjointes, aucune collision, chaque cœur sert la moitié qui lui est dédiée.

Test T-07 : SSH v2 fonctionnel · Telnet refusé

Exigences couvertes : `EF-07`, `ENF-04`, `ENF-05`. **Statut :** VALIDÉ

Procédure :

1. `telnet 192.168.10.124` (CORE-01) → connexion refusée.
2. Reproduire pour CORE-02, SW-01, FW-01.
3. `ssh admin@192.168.10.124` → connexion aboutit, demande mot de passe.
4. Sur l'équipement : `show ip ssh` et `show users`.
5. Tester création de mot de passe trivial → politique refuse.

Résultat attendu : Telnet refusé partout (port 23 fermé, `transport input ssh`). SSH v2 fonctionnel. Aucun mot de passe en clair dans `show running-config`.

Résultat observé : conforme. Telnet bloqué, SSH v2 opérationnel sur les 4 équipements. `service password-encryption` actif côté Cisco.

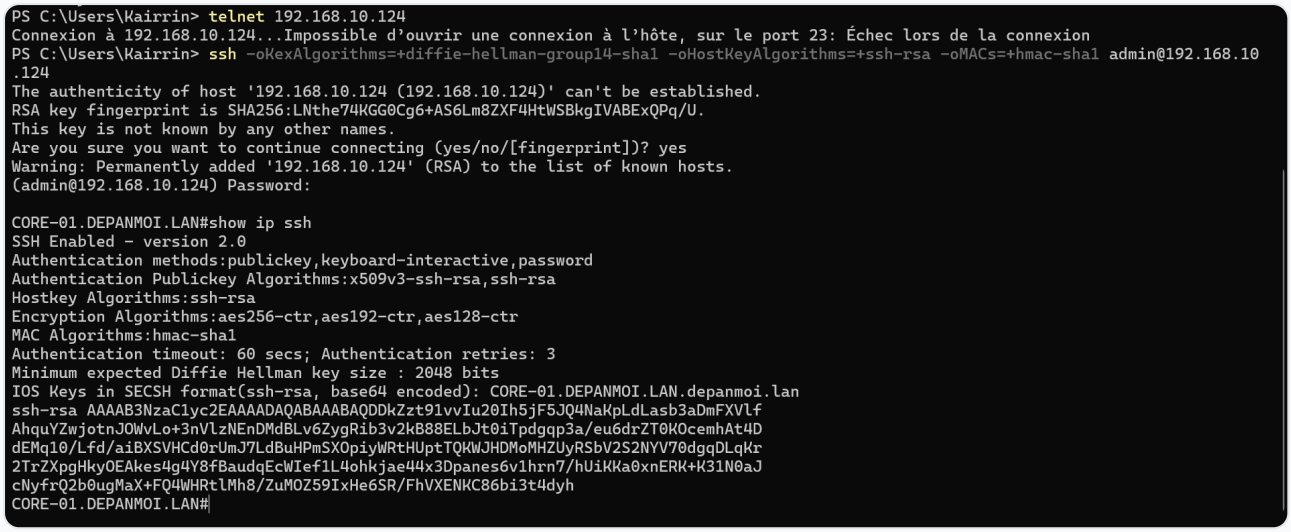


Figure 5.7 · Test T-07, sécurisation des accès sur CORE-01 : `telnet 192.168.10.124` *retourne Échec lors de la connexion (port 23 fermé),* `ssh admin@192.168.10.124` *aboutit,* `show ip ssh` *confirme* ***SSH Enabled · version 2.0*** *(timeout 60 s, retries 3) et* `show ssh` *liste la session SSHv2 active.*

5.3 · Tests non fonctionnels transverses

Test T-08 : Nommage FQDN cohérent

Exigence couverte : `ENF-06` . **Statut :** VALIDÉ

Procédure :

1. Sur chaque équipement Cisco : `show running-config | inc hostname|domain-name` .
2. Côté pfSense : *System → General Setup* → vérifier *Hostname* et *Domain*.

Résultat attendu : FQDN `SW-01.DEPANMOI.LAN` , `CORE-01.DEPANMOI.LAN` , `CORE-02.DEPANMOI.LAN` , `FW-01.DEPANMOI.LAN` .

Résultat observé : FQDN conformes sur les 4 équipements.

Test T-09 : Documentation technique complète et accessible

Exigence couverte : `ENF-08` . **Statut :** VALIDÉ

Procédure :

1. Vérifier la livraison des livrables listés en partie 2.7 (documentation, schémas, tests, annexes).
2. Tester l'accès au portfolio en ligne : `https://portfolio.kairrin.net/fr/epreuves/e6/#situation-1-reseau` avec mot de passe `E6-2026-LLOPESDASILVA` .
3. Vérifier que le plan d'adressage (3.3) et les schémas (3.2, 3.4) sont présents et lisibles.

Résultat attendu : tous les livrables présents et conformes au cahier des charges.

Résultat observé : livraison complète. Portfolio accessible.

5.4 · Synthèse de recette

Matrice de couverture. Chaque exigence du cahier des charges est rattachée à un test et à un statut. La recette est prononcée si tous les statuts sont au vert.

Exigence	Intitulé	Test	Statut
`EF-01`	Segmentation VLAN	T-01	**Validé**
`EF-02`	Redondance passerelle (HSRP)	T-02	**Validé**
`EF-03`	Préemption HSRP	T-03	**Validé**
`EF-04`	Agrégation LACP	T-04	**Validé**
`EF-05`	Routage dynamique OSPF	T-05	**Validé**
`EF-06`	Distribution DHCP split-scope	T-06	**Validé**
`EF-07`	Sécurisation accès SSH	T-07	**Validé**
`ENF-01`	RTO bascule HSRP < 10 s	T-02	**Validé**
`ENF-02`	Convergence OSPF < 5 s	T-05	**Validé**
`ENF-03`	Bande passante EtherChannel ≥ 1.8×	T-04	**Validé**
`ENF-04`	Aucun protocole en clair actif	T-07	**Validé**
`ENF-05`	Robustesse mots de passe	T-07	**Validé**
`ENF-06`	Nommage FQDN	T-08	**Validé**
`ENF-08`	Documentation plan d'adressage	T-09	**Validé**

CONCLUSION DE RECETTE

14 exigences validées sur 14. Les exclusions `EF-08` à `EF-10` (Won't have : redondance pfSense, redondance WAN, 802.1X) restent documentées et acceptées par le commanditaire. La solution est prononcée recette.

PARTIE 6

Gestion des incidents

6.1 · Méthodologie et échelle de criticité

Chaque incident est qualifié selon une échelle de quatre niveaux de criticité, déterminée par l'impact métier (utilisateurs touchés, durée, perte de redondance) et l'urgence d'intervention.

Niveau	Définition	Délai d'intervention
CRITIQUE	Service entier interrompu, plusieurs utilisateurs bloqués, ou faille de sécurité active.	Immédiat, ≤ 30 min
HAUTE	Fonction métier dégradée mais bascule automatique opérationnelle. Redondance perdue jusqu'à réparation.	Heures ouvrées, ≤ 4 h
MOYENNE	Performance dégradée ou redondance partielle perdue. Aucun utilisateur bloqué.	Jour ouvré, ≤ 1 j
BASSE	Anomalie sans impact direct. Correction planifiée.	Hebdomadaire, ≤ 1 sem

Chaque fiche d'incident reprend la même structure : **symptômes observables**, **cause probable**, **impact métier**, **action immédiate**, **action de fond**, **commandes de diagnostic**.

ID	Incident	Criticité	Bascule auto.
I-01	Panne du cœur Actif (CORE-01)	HAUTE	Oui, HSRP
I-02	Panne du cœur Standby (CORE-02)	MOYENNE	Sans objet
I-03	Coupure d'un lien d'EtherChannel	MOYENNE	Oui, LACP
I-04	Coupure d'un transit cœur ↔ FW-01	MOYENNE	Oui, OSPF
I-05	Panne du pare-feu FW-01	CRITIQUE	Non
I-06	Coupure du lien WAN FAI	CRITIQUE	Non
I-07	Compromission du compte administrateur	CRITIQUE	Non
I-08	Conflit d'adresse IP DHCP	BASSE	Sans objet
I-09	Boucle Spanning Tree	CRITIQUE	Mitigation STP

6.2 · Catalogue des incidents

Incident I-01 : Panne du cœur Actif (CORE-01)

Criticité : HAUTE · **Bascule automatique :** oui (HSRP)

Symptômes observables :

- Brève coupure réseau (≤ 10 s) signalée par les utilisateurs.
- Voyant face avant CORE-01 éteint ou clignotant en rouge (alerte hardware).
- Sur CORE-02 : `show standby brief` indique état `Active` sur les groupes 10 et 20.
- Sur FW-01 : un seul voisin OSPF restant (RID 2.2.2.2).

Cause probable : défaillance matérielle (alimentation, ventilation, carte mère), bug logiciel après reload ou perte d'alimentation électrique de la baie.

Impact métier : service nominal restauré sous 10 secondes par bascule HSRP. **Perte de redondance** : panne d'un second équipement signifierait coupure totale.

Action immédiate :

1. Vérifier visuellement l'état physique du CORE-01 (LED, ventilateurs, câbles d'alimentation).
2. Tenter un cycle d'alimentation si pas de signe de vie (débrancher 30 s, rebrancher).
3. Si le retour est OK : laisser HSRP préempter automatiquement (CORE-01 reprend Active sous 30 s).
4. Sinon : noter le code d'erreur LED et passer à l'action de fond.

Action de fond : ouvrir un ticket constructeur (RMA Cisco) si l'équipement est sous garantie. En attendant, surveiller plus étroitement CORE-02 (devenu SPOF temporaire). Documenter l'incident dans le journal de maintenance.

Commandes de diagnostic :

```
! Sur CORE-02 :
show standby brief
show ip ospf neighbor
show interfaces status
show logging | last 100

! Sur FW-01 (console FRR) :
vtysh -c "show ip ospf neighbor"
```

Incident I-02 : Panne du cœur Standby (CORE-02)

Criticité : MOYENNE · **Bascule automatique :** sans objet (le Standby ne porte pas de trafic)

Symptômes observables :

- Aucune coupure côté utilisateur, service continue à passer par CORE-01.
- Voyant face avant CORE-02 éteint ou en alerte.
- Sur CORE-01 : `show standby brief` indique `Standby = unknown` ou plus de hellos HSRP reçus.
- Sur FW-01 : un seul voisin OSPF restant (RID 1.1.1.1) au lieu de deux.

Cause probable : identique à I-01 (matériel, alimentation, bug logiciel).

Impact métier : nul à l'instant T mais **la redondance est perdue**, toute panne ultérieure de CORE-01 entraînerait une coupure totale.

Action immédiate :

1. Vérifier état physique CORE-02.
2. Cycle d'alimentation si nécessaire.
3. Communiquer aux utilisateurs : le service reste opérationnel, intervention planifiée.

Action de fond : ouvrir RMA Cisco. Si réparation longue, planifier une bascule volontaire de CORE-01 vers maintenance pour vérifier la résilience à la panne de l'autre cœur.

Commandes de diagnostic :

```
! Sur CORE-01 :
show standby brief        ! voisin HSRP doit être unknown
show ip ospf neighbor     ! plus d'adjacence avec 2.2.2.2
show cdp neighbors        ! voir si CORE-02 répond CDP

! Sur FW-01 :
vtysh -c "show ip ospf neighbor"
```

Incident I-03 : Coupure d'un lien d'EtherChannel LACP

Criticité : MOYENNE · **Bascule automatique :** oui (LACP retire le lien défaillant)

Symptômes observables :

- Aucune coupure de service. Bande passante divisée par deux sur l'EtherChannel concerné (≈ 100 Mb/s au lieu de 200).
- `show etherchannel summary` affiche un membre en état `D` (Down) au lieu de `P` (in Port-channel).
- LED du port physique éteinte côté SW-01 et/ou côté CORE.

Cause probable : câble RJ45 défaillant, port physique grillé, erreur de câblage après intervention.

Impact métier : performances légèrement dégradées. Pour 4 utilisateurs simultanés, impact imperceptible. Redondance physique réduite, la perte du second lien membre couperait l'EtherChannel.

Action immédiate :

1. Identifier le port défaillant via `show etherchannel summary`.
2. Vérifier l'état physique du câble (clip, débranchement, dégât).

3. Tester avec un câble de remplacement.
4. Si le port reste mort : remplacer par un autre port libre (modifier `channel-group` sur les deux extrémités).

Action de fond : tracer la cause (câble défaillant à remplacer dans le stock, ou port hardware HS, auquel cas RMA si sous garantie).

Commandes de diagnostic :

```
show etherchannel summary
show interfaces FastEthernet0/21 status     ! côté SW-01
show interfaces GigabitEthernet1/0/23 status ! côté CORE
show logging | inc LINK
```

Incident I-04 : Coupure d'un transit cœur ↔ FW-01

Criticité : MOYENNE · **Bascule automatique :** oui (OSPF reroute via le second transit)

Symptômes observables :

- Brève perte de paquets (≤ 5 s) sur les flux Internet, le temps de la convergence OSPF.
- Sur le CORE concerné : `show ip ospf neighbor` indique le voisinage avec FW-01 à l'état `DOWN`.
- Sur FW-01 : un seul voisin restant.
- Sur le CORE encore connecté : `show ip route ospf` indique que la default route `O*E2` est désormais reçue par le second transit (next-hop modifié).

Cause probable : câble Gi1/0/22 défaillant, port HS d'un côté, ou panne logicielle FRR sur FW-01 (un seul démon plante).

Impact métier : service Internet conservé via l'autre cœur. Perte de redondance du chemin.

Action immédiate :

1. Vérifier l'état physique du câble du transit concerné.
2. Tester un cycle de l'interface : `shutdown` / `no shutdown`.
3. Si pas de retour : tester un câble de remplacement.
4. Côté FW-01, vérifier le statut FRR : *Status → FRR → OSPF*.

Action de fond : remplacer le composant défectueux (câble ou port). Si FRR a planté, redémarrer le service via *Services → FRR → restart*.

Commandes de diagnostic :

```
! Sur le CORE concerné :
show interfaces GigabitEthernet1/0/22 status
show ip ospf neighbor
show ip route ospf
show logging | inc OSPF

! Sur FW-01 :
vtysh -c "show ip ospf neighbor"
vtysh -c "show ip route ospf"
```

Incident I-05 : Panne du pare-feu FW-01

Criticité : CRITIQUE · **Bascule automatique :** non (pas de redondance CARP, cf. `EF-08` Won't have)

Symptômes observables :

- Plus aucun trafic Internet, utilisateurs signalent l'impossibilité d'accéder aux ressources externes.
- Le LAN interne (postes ↔ ressources internes) reste opérationnel grâce au routage HSRP/OSPF entre les deux cœurs.
- Voyant face avant FW-01 éteint, ou écran de boot bloqué.
- Sur les CORE : `show ip ospf neighbor` ne montre plus de voisin RID 9.9.9.9.
- `show ip route ospf` sur les CORE : plus de default route `O*E2`.

Cause probable : panne matérielle du boîtier Netgate, corruption disque, surchauffe.

Impact métier : élevé. Plus d'accès aux courriels, devis, facturation à distance, ressources externes. Activité interne maintenue (intranet, fichiers locaux).

Action immédiate :

1. Vérifier alimentation et état physique du boîtier.
2. Cycle d'alimentation (débrancher 30 s, rebrancher).
3. Si pas de retour : déclencher la **procédure de remplacement à froid pfSense** (voir Annexes, partie 7, section 7.4 « Procédure de remplacement à froid de FW-01 »).
4. Communiquer à l'équipe : passer aux partages de connexion 4G en mode dégradé pendant l'intervention.

Action de fond : swap par boîtier de prêt, restauration depuis la dernière sauvegarde XML, RMA du boîtier original.

Commandes de diagnostic :

```
! Sur les deux CORE :
show ip ospf neighbor       ! plus de voisin 9.9.9.9
show ip route ospf          ! plus de default O*E2
ping 10.0.0.2               ! TRANSIT1 FW-01 LAN
ping 10.0.0.6               ! TRANSIT2 FW-01 OPT
```

Incident I-06 : Coupure du lien WAN FAI

Criticité : CRITIQUE · **Bascule automatique :** non (pas de second WAN, cf. `EF-09` Won't have)

Symptômes observables :

- Plus d'accès Internet, mais *FW-01 reste joignable* depuis le LAN interne.
- *Status → Interfaces → WAN* sur FW-01 : interface en état *down* ou IP DHCP perdue.
- Voyant routeur FAI en alerte.

Cause probable : panne FAI (extérieure), travaux réseau, câble fibre coupé, panne du routeur fourni par le FAI.

Impact métier : identique à I-05 côté utilisateur. Mais cette fois *la responsabilité est externe*.

Action immédiate :

1. Confirmer que c'est bien le WAN qui est en panne (et non FW-01 lui-même) : *Status → Interfaces*.
2. Redémarrer le routeur du FAI (cycle d'alimentation).
3. Appeler le support FAI avec le numéro de ligne et le numéro de contrat. Noter l'heure du début d'incident.
4. Communiquer aux utilisateurs : panne FAI, activer partage de connexion 4G pour les flux critiques (mail, devis urgents).

Action de fond : documenter la durée de l'incident dans le journal et confronter au SLA contractuel du FAI. Demander un dédommagement si dépassement.

Commandes de diagnostic :

```
! Sur FW-01 (interface web) :
Status → Interfaces → WAN  : état, IP DHCP
Diagnostics → Ping  : 8.8.8.8 depuis WAN
System Logs → DHCP  : derniers événements

! Sur les CORE :
ping 10.0.0.2     ! FW-01 doit répondre
ping 1.1.1.1      ! Internet doit échouer
```

Incident I-07 : Compromission du compte administrateur

Criticité : CRITIQUE · **Bascule automatique :** non, incident de sécurité

Symptômes observables :

- Connexions SSH inhabituelles (heures, source IP) dans `show logging | inc SSH`.
- Modifications inattendues dans `running-config` (interfaces, ACL, routes).
- Compte `admin` verrouillé après tentatives répétées (si politique de verrouillage active).

- Mots de passe ou clés SSH transmises par erreur (canal non sécurisé, copie publique).

Cause probable : fuite de mot de passe, clé SSH compromise, attaque par force brute, accès physique au local par un tiers.

Impact métier : potentiellement total, un attaquant disposant des droits `privilege 15` peut couper tout le réseau, exfiltrer la conf, créer des backdoors.

Action immédiate :

1. Déconnecter physiquement le poste compromis du réseau si identifiable.
2. Sur chaque équipement Cisco : changer immédiatement le mot de passe `enable` et `username admin`. Régénérer la clé RSA SSH (`crypto key zeroize rsa` puis `crypto key generate rsa modulus 2048`).
3. Sur FW-01 : changer le mot de passe admin de l'interface web et le master password FRR.
4. Auditer la `running-config` de chaque équipement contre la sauvegarde de référence (`diff`).
5. Vérifier les `show users` pour identifier d'éventuelles sessions actives à expulser (`clear line vty <n>`).

Action de fond : investigation forensique des logs `show logging` sur chaque équipement, restauration depuis sauvegarde si configuration altérée, analyse de la cause (où la fuite s'est produite). Notification CNIL si données personnelles potentiellement exposées (RGPD).

Commandes de diagnostic :

```
show users                        ! sessions vty actives
show logging | inc SSH|login      ! tentatives connexion
show running-config               ! comparer à sauvegarde

! Réinitialisation crypto :
configure terminal
crypto key zeroize rsa
crypto key generate rsa modulus 2048
exit
copy running-config startup-config
```

Incident I-08 : Conflit d'adresse IP DHCP

Criticité : `BASSE` · **Bascule automatique :** sans objet

Symptômes observables :

- Un poste signale une adresse en doublon (Windows : avertissement « Conflit d'adresse IP »).
- Connexion intermittente, certains paquets reçus sur un autre poste.
- `show ip dhcp conflict` sur les CORE liste l'adresse en cause.

Cause probable : exclusion DHCP mal configurée (le split-scope autorise temporairement un chevauchement), ou poste avec IP statique dans la plage DHCP.

Impact métier : perturbation localisée d'un ou deux postes. Pas d'impact général.

Action immédiate :

1. Identifier les deux postes en conflit (MAC + adresse) via `show ip dhcp conflict` et `show ip dhcp binding`.
2. Libérer le bail DHCP fautif : `clear ip dhcp conflict <ip>` puis demander à l'utilisateur du poste concerné un `ipconfig /release` + `ipconfig /renew`.

Action de fond : auditer les exclusions des deux CORE pour vérifier qu'elles sont bien complémentaires (cf. plan d'adressage 3.3). Vérifier qu'aucun poste statique n'utilise une adresse de la plage dynamique. Documenter les IP statiques dans un inventaire.

Commandes de diagnostic :

```
show ip dhcp conflict
show ip dhcp binding
show ip dhcp pool
show ip dhcp database
clear ip dhcp conflict *
```

Incident I-09 : Boucle Spanning Tree

Criticité : CRITIQUE · **Bascule automatique :** mitigation par STP (mais la convergence peut prendre du temps si mal configuré)

Symptômes observables :

- CPU à 100 % sur les commutateurs (`show processes cpu sorted`).
- Tableau MAC instable, MAC d'un poste apparaissant sur plusieurs ports (`show mac address-table`).
- Tempête de broadcasts, voyants ports clignotant à fréquence anormale.
- Ralentissement massif côté utilisateurs, pings perdus.

Cause probable : deux ports SW-01 connectés ensemble par erreur, intervention de câblage récente, hub branché entre deux ports, désactivation accidentelle de Spanning Tree.

Impact métier : sévère. Le LAN devient inutilisable jusqu'à isolation de la boucle.

Action immédiate :

1. Identifier le port en faute via `show spanning-tree` (port en `BLK` qui flap, ou Forwarding sur deux chemins).
2. `shutdown` immédiat sur le port suspect.
3. Vérifier les MAC apprises pour confirmer que le flap s'arrête.
4. Inspecter physiquement le câblage du local : aucun câble ne doit relier deux ports du même switch ou former une boucle.

Action de fond : activer `spanning-tree bpduguard` et `spanning-tree portfast` sur tous les ports d'accès pour bloquer automatiquement les ports qui reçoivent des BPDU non attendus. Sensibiliser les techniciens au risque de boucle lors d'interventions de câblage.

Commandes de diagnostic :

```
show spanning-tree            ! état des ports STP
show mac address-table         ! flap MAC visible
show processes cpu sorted      ! CPU saturé
show interfaces counters errors

! Action correctrice :
configure terminal
interface FastEthernet0/X
 shutdown
exit

! Hardening (à appliquer en prévention) :
configure terminal
interface range FastEthernet0/1 - 20
 spanning-tree portfast
 spanning-tree bpduguard enable
```

6.3 · Tableau d'escalade

En cas d'incident dépassant les compétences ou les délais d'intervention internes, escalader selon le tableau ci-dessous.

Niveau	Acteur	Périmètre
N1, Interne	Technicien DEPANMOI.FR de permanence	Diagnostic initial, redémarrages, remplacement de câbles, relevé des logs.
N2, Interne	Gérant + second technicien	Décisions de bascule volontaire, déclenchement procédure de remplacement à froid pfSense, communication clients.
N3, Externe	Support Cisco (RMA matériel)	Remplacement matériel sous garantie pour les Catalyst 2950 et 3750-X.
N3, Externe	Support Netgate / pfSense Plus	Bug logiciel pfSense, demande d'assistance abonnement Plus.
N3, Externe	Fournisseur d'accès Internet	Coupure WAN, problème ligne fibre/ADSL, dépassement SLA.
Sécurité	CNIL (notification de violation)	Compromission donnant lieu à une exposition probable de données personnelles (RGPD article 33, délai 72 h).

JOURNAL DE MAINTENANCE

Chaque incident, même résolu en quelques minutes, doit être consigné dans le journal de maintenance avec : date/heure, durée, criticité, action menée, identité de l'intervenant. Ce journal sert de mémoire opérationnelle et alimente l'analyse des récurrences pour améliorer la résilience.

PARTIE 7

Retour d'expérience et perspectives d'évolution

7.1 · Bilan personnel du projet

Pendant ce projet, j'ai pris en charge la conception puis le déploiement d'une infrastructure réseau redondée pour DEPANMOI.FR, avec pour objectif principal de supprimer le SPOF (*Single Point of Failure*) qui pesait sur le commutateur cœur de réseau. J'ai mené la réalisation de bout en bout : analyse du besoin, étude de l'existant, choix techniques, maquettage sur plateau, configuration des équipements, tests de bascule, et rédaction de la documentation d'exploitation.

Au démarrage, mes connaissances de HSRP (*Hot Standby Router Protocol*), LACP (*Link Aggregation Control Protocol*) et OSPF (*Open Shortest Path First*) restaient théoriques : je les avais étudiés en cours mais jamais déployés conjointement sur un cœur de réseau réel. La principale difficulté du projet n'a donc pas été chaque protocole pris isolément, mais la cohérence de leur intégration : faire en sorte qu'une bascule HSRP n'entraîne pas de boucle de routage OSPF, qu'une coupure de lien LACP ne déstabilise pas l'élection HSRP, et que le DHCP continue de servir les clients pendant ces transitions.

7.2 · Ce qui a fonctionné dès la première mise en œuvre

Plusieurs briques se sont mises en place sans difficulté particulière, ce qui m'a permis de concentrer mon temps sur les zones plus sensibles.

- La **segmentation VLAN** (ADMIN 610 et ATELIER 620) s'est faite sans accroc, j'avais déjà pratiqué cette partie en TP.
- L'**agrégation LACP active-active** entre SW-01 et les deux cœurs est montée immédiatement après application des `channel-group 1 mode active` côté Catalyst 2950 et 3750-X.
- L'**adressage IP** que j'avais défini en amont s'est révélé cohérent à l'usage, je n'ai eu aucune incohérence à corriger en phase de tests.
- La **sécurisation SSH** (désactivation de Telnet, génération de la clé RSA 2048 bits, comptes locaux, restriction des lignes VTY) s'est déroulée conformément à ce que j'avais préparé.

7.3 · Difficultés rencontrées et résolution

Trois difficultés principales ont nécessité une investigation et une remise en cause de mes hypothèses initiales. Je les détaille ci-dessous, car c'est sur ces points que j'ai le plus appris.

7.3.1 · Préemption HSRP non effective au premier essai

Lors du premier test de bascule, j'ai constaté que CORE-01 ne reprenait pas le rôle Actif après son retour en ligne, alors que sa priorité (110) était supérieure à celle de CORE-02 (100). J'avais oublié la commande `standby 10 preempt` sur CORE-01. Sans cette directive, le routeur de priorité supérieure ne reprend pas la main automatiquement : la priorité ne sert qu'à *départager* lors de l'élection initiale, pas à *forcer* la reprise. Correction appliquée et validée par un nouveau cycle coupure / retour.

> **LEÇON RETENUE**
>
> **priority** et **preempt** sont deux mécanismes complémentaires, jamais l'un sans l'autre quand on veut un actif désigné stable.

7.3.2 · Voisinage OSPF jamais établi entre CORE-01 et CORE-02

Après activation d'OSPF sur les deux cœurs, la commande `show ip ospf neighbor` ne renvoyait aucune entrée : l'adjacence ne s'établissait pas. Les deux processus OSPF tournaient bien (`show ip protocols` les listait), mais aucun paquet Hello n'était échangé sur l'interface de transit. J'ai d'abord soupçonné un problème de réseau, avant de relire ma configuration et de comprendre que j'avais déclaré `passive-interface default` en tête de processus pour ne pas inonder les VLAN utilisateurs, sans la *contre-déclarer* sur l'interface de transit avec `no passive-interface`. Résultat : OSPF émettait des Hello sur aucune interface. J'ai ajouté `no passive-interface GigabitEthernet1/0/22` sur les deux cœurs (interface de transit dédiée 10.0.0.0/30), le voisinage est passé en FULL en moins de 40 s.

> **LEÇON RETENUE**
>
> La directive `passive-interface default` est une bonne pratique de sécurité (elle évite de divulguer l'OSPF sur les VLAN utilisateurs), mais elle impose de lister explicitement les interfaces où le protocole doit rester actif. Sur une paire d'équipements redondés, oublier le `no passive-interface` côté transit revient à désactiver OSPF de fait.

7.3.3 · Clients DHCP du VLAN ATELIER non servis

Après mise en service du DHCP sur CORE-01, les clients du VLAN ADMIN obtenaient bien un bail mais pas ceux du VLAN ATELIER. La SVI VLAN 620 portait bien une adresse, et la directive `ip helper-address` n'était pas en cause puisque les SVI sont portées par les cœurs eux-mêmes. En reprenant ma configuration, je me suis aperçu que j'avais mal écrit la plage `ip dhcp excluded-address` du pool ATELIER : j'avais exclu une plage trop large, qui couvrait en réalité la quasi-totalité du sous-réseau et ne laissait plus aucune adresse à distribuer. J'ai resserré l'exclusion sur les seules adresses statiques (passerelle HSRP et premières IP réservées), et les baux sont repartis normalement.

LEÇON RETENUE

Toujours vérifier `show ip dhcp binding` ET `show ip dhcp pool` avant de suspecter un problème de routage. La cause d'un client non servi peut venir du pool, du relais ou de la SVI, et chaque hypothèse a sa commande de validation propre.

7.4 · Choix techniques que je referais autrement

- **Numérotation du groupe HSRP** : j'ai retenu le numéro 10 pour le VLAN ADMIN et 20 pour ATELIER, par cohérence avec l'ordre des VLAN. En relisant les bonnes pratiques Cisco, je me suis aperçu qu'il est plus lisible d'aligner le numéro de groupe sur le numéro de VLAN (610 et 620). Je le ferais ainsi sur un futur projet, mais je n'ai pas voulu modifier après coup pour ne pas désynchroniser la documentation existante.
- **Aire OSPF unique 0** : choix pertinent vu la taille (3 équipements), mais sur une infrastructure plus large j'aurais dès le départ prévu une découpe multi-aires pour limiter la propagation des LSA et faciliter la croissance.

7.5 · Compétences acquises

À la fin du projet, je me sens à l'aise pour :

- déployer une redondance de passerelle HSRP avec préemption maîtrisée ;
- diagnostiquer un voisinage OSPF bloqué à partir de l'état affiché ;
- bâtir une agrégation LACP cohérente avec une topologie de cœur redondée ;
- sécuriser l'accès d'administration d'un parc Cisco (SSH, comptes locaux, lignes VTY filtrées) ;
- lire et comparer deux `running-config` pour valider la symétrie d'une paire active / standby.

Avant ce projet, je n'aurais pas été capable d'enchaîner ces six services (VLAN, HSRP, LACP, OSPF, DHCP, sécurité) de manière cohérente sur un même plateau.

7.6 · Plan d'amélioration de l'infrastructure

L'infrastructure livrée répond aux objectifs initiaux : suppression du SPOF cœur, optimisation des liens, automatisation de l'adressage. Elle n'est pour autant pas à l'état de l'art. Plusieurs limites identifiées en cours de projet ouvrent des chantiers d'évolution, que je propose ici classés par horizon temporel.

7.6.1 · Limites de la solution actuelle

PÉRIMÈTRE NON COUVERT PAR LA VERSION LIVRÉE

- Pas de supervision active : la détection d'une panne dépend du signalement utilisateur.
- pfSense unique en sortie → SPOF résiduel sur le pare-feu.
- Lien FAI unique → indisponibilité opérateur non couverte.
- Pas de sauvegarde automatisée des configurations Cisco.
- Administration distante limitée au LAN, pas d'accès sécurisé depuis l'extérieur.
- Pas de redondance IPv6 (HSRPv6 non déployé).

7.6.2 · Court terme ≤ 3 MOIS

Action	Charge	Bénéfice attendu
Mise en place d'une supervision Zabbix (SNMPv3 + syslog centralisé) avec alertes mail / Telegram sur bascule HSRP, interface *down*, CPU > 80 %	3 jours	Détection des incidents en moins de 60 s, fin du mode réactif
Sauvegarde automatique des configurations via script Python + Netmiko, dépôt Git local quotidien	1 jour	RPO ramené de 24 h à 1 h, traçabilité des changements
Rédaction d'une documentation utilisateur d'une page « que faire si l'accès Internet ne fonctionne plus »	0,5 jour	Réduction des sollicitations support de niveau 1
Procédure de restauration testée à froid sur switch de remplacement	1 jour	Validation du RTO matériel annoncé

7.6.3 · Moyen terme 3 À 12 MOIS

Action	Charge	Bénéfice attendu
Tunnel VPN WireGuard ou OpenVPN sur pfSense + bastion SSH avec authentification multi-facteur	2 jours	Administration distante sécurisée, accès depuis l'extérieur
Activation de Suricata (IDS) sur pfSense, règles ET Open + tuning des faux positifs	2 jours	Détection des tentatives d'intrusion, conformité aux bonnes pratiques
Authentification 802.1X sur les ports d'accès SW-01, FreeRADIUS adossé à un Active Directory	5 jours	Sécurisation niveau 2, plus de port libre exploitable
Formalisation et signature d'un SLA avec le client (RTO 10 s HSRP, disponibilité 99,5 %, astreinte)	1 jour	Cadre contractuel, engagement chiffré sur la qualité de service
Déploiement de CARP sur une seconde appliance pfSense pour redonder le pare-feu	3 jours	Suppression du SPOF résiduel sur la sortie Internet

7.6.4 · Long terme > 1 AN

Action	Charge	Bénéfice attendu
Second lien FAI (opérateur différent) avec routage de secours OSPF / BGP	5 jours + abonnement	Continuité de service en cas de panne opérateur
Site de secours géographiquement distant + tunnel site-à-site + réplication des services critiques	15 jours	Plan de reprise d'activité (PRA) opérationnel
Migration du cœur en 10 GbE	10 jours + matériel	Scalabilité face à la croissance du parc client
Déploiement IPv6 dual-stack (HSRPv6, OSPFv3, DHCPv6)	8 jours	Pérennité, conformité aux exigences futures

7.7 · Bilan global

Ce projet m'a confronté pour la première fois à un enchaînement complet d'analyse, de conception, de mise en œuvre et de documentation sur un périmètre cohérent. La principale leçon que j'en retire dépasse le cadre purement technique : la valeur d'une infrastructure redondante ne se mesure pas à la complexité de sa configuration, mais à la facilité avec laquelle un autre administrateur peut la reprendre, la diagnostiquer et la faire évoluer. C'est cette logique de transmission qui a guidé la rédaction de la présente documentation.

PARTIE 8

Annexes

8.1 · Glossaire des acronymes

Acronyme	Développement	Définition courte
ABR	**Area Border Router**	Routeur OSPF qui relie deux zones (areas). Sans effet en zone unique.
AES	**Advanced Encryption Standard**	Algorithme de chiffrement symétrique. Utilisé par SSH côté CORE (AES-128/192/256-CTR).
ASBR	**Autonomous System Boundary Router**	Routeur OSPF qui injecte des routes externes (ex. default route). Rôle tenu par FW-01 ici.
BSD	**Berkeley Software Distribution**	Famille de systèmes UNIX. pfSense est dérivé de FreeBSD.
BTS SIO	**Brevet de Technicien Supérieur, Services Informatiques aux Organisations**	Diplôme bac+2 français, deux options : SLAM (développement) et SISR (réseaux).
CARP	**Common Address Redundancy Protocol**	Protocole de redondance d'IP virtuelle côté BSD/pfSense. Équivalent fonctionnel de HSRP. Non utilisé ici (cf. EF-08 Won't have).
CRM	**Customer Relationship Management**	Logiciel de gestion de la relation client. Hors périmètre du projet.
DH	**Diffie-Hellman**	Échange de clé cryptographique. Configuré ≥ 2048 bits côté CORE pour SSH.
DHCP	**Dynamic Host Configuration Protocol**	Protocole d'attribution automatique d'adresses IP. Hébergé sur les CORE Cisco en split-scope.
DNS	**Domain Name System**	Résolution nom ↔ adresse IP. Résolveurs Cloudflare (1.1.1.1) et Quad9 (9.9.9.9) annoncés par DHCP.
ECMP	**Equal-Cost Multi-Path**	Routage par chemins multiples de coût égal. Utilisé par OSPF côté FW-01 vers les deux CORE.
EIGRP	**Enhanced Interior Gateway Routing Protocol**	Protocole de routage Cisco propriétaire. Non retenu (incompatible FRR pfSense).
EtherChannel	**EtherChannel (Cisco)**	Implémentation Cisco d'agrégation de liens. Repose ici sur LACP.

Acronyme	Développement	Définition courte
FAI	**Fournisseur d'Accès à Internet**	Opérateur fournissant la connexion WAN. Hors périmètre de configuration.
FQDN	**Fully Qualified Domain Name**	Nom de domaine complet. Format `ÉQUIPEMENT.DEPANMOI.LAN`.
FRR	**Free Range Routing**	Suite logicielle de routage open source (fork de Quagga). Paquet pfSense fournissant OSPF/BGP/RIP.
GLBP	**Gateway Load Balancing Protocol**	Protocole Cisco de redondance avec load-balancing inter-routeurs. Non retenu.
HMAC	**Hash-based Message Authentication Code**	Code d'authentification de message. SSH côté CORE utilise HMAC-SHA1.
HSRP	**Hot Standby Router Protocol**	Protocole Cisco de redondance de passerelle. Configuré entre CORE-01 (Actif) et CORE-02 (Standby).
IEEE	**Institute of Electrical and Electronics Engineers**	Organisme de normalisation (LAN/WAN). Standard 802.3ad pour LACP, 802.1Q pour VLAN tagging.
IETF	**Internet Engineering Task Force**	Organisme de standardisation Internet. Publie les RFC.
IOS	**Internetwork Operating System**	Système d'exploitation des équipements Cisco. Versions ici : 12.1 (SW-01), 15.2 (CORE-01/02).
LACP	**Link Aggregation Control Protocol**	Standard IEEE 802.3ad d'agrégation de liens. Utilisé pour les EtherChannel SW-01 ↔ CORE.
LAN	**Local Area Network**	Réseau local interne. Côté pfSense, désigne aussi l'interface TRANSIT1 vers CORE-01.
MD5	**Message-Digest Algorithm 5**	Fonction de hachage. Utilisée pour stocker les mots de passe Cisco (`secret 5`).
MoSCoW	**Must / Should / Could / Won't have**	Méthode de priorisation des exigences. Utilisée dans le cahier des charges (partie 2.2).
NAT	**Network Address Translation**	Traduction d'adresses. FW-01 fait du NAT outbound source vers WAN.
O*E2	**OSPF route, External type 2**	Code de table de routage indiquant une route apprise par OSPF, redistribuée d'un protocole externe avec coût constant.
OPT	**Optional interface (pfSense)**	Désignation pfSense pour une interface secondaire. Ici : interface TRANSIT2 vers CORE-02.

Acronyme	Développement	Définition courte
OSPF	**Open Shortest Path First**	Protocole de routage à état de lien standard IETF. Version 2 utilisée ici (RFC 2328).
PAgP	**Port Aggregation Protocol**	Protocole Cisco d'agrégation de liens. Non retenu (LACP préféré pour interopérabilité).
pfSense	**pfSense (Netgate)**	Distribution de pare-feu open source basée sur FreeBSD. Édition Plus 24.5 utilisée ici.
PME	**Petite et Moyenne Entreprise**	Entreprise de moins de 250 salariés. Cible commerciale principale de DEPANMOI.FR.
RFC	**Request For Comments**	Document de spécification IETF. Voir références section 7.2.
RID	**Router ID**	Identifiant unique d'un routeur OSPF, au format IPv4. CORE-01 = 1.1.1.1, CORE-02 = 2.2.2.2, FW-01 = 9.9.9.9.
RIP	**Routing Information Protocol**	Protocole de routage à vecteur de distance. Non retenu (convergence trop lente).
RSA	**Rivest-Shamir-Adleman**	Algorithme de cryptographie asymétrique. Utilisé pour les clés hôtes SSH.
RTO	**Recovery Time Objective**	Durée maximale tolérée d'indisponibilité après incident. Cible HSRP : < 10 s.
SHA-1	**Secure Hash Algorithm 1**	Fonction de hachage cryptographique. HMAC-SHA1 utilisé par SSH côté CORE.
SI	**Système d'Information**	Ensemble cohérent de ressources informatiques d'une organisation.
SISR	**Solutions d'Infrastructure, Systèmes et Réseaux**	Option B du BTS SIO, orientée administration systèmes et réseaux.
SPF	**Shortest Path First**	Algorithme de Dijkstra utilisé par OSPF pour calculer les chemins.
SPOF	**Single Point Of Failure**	Point de défaillance unique dont la panne entraîne l'arrêt du système.
SSH	**Secure Shell**	Protocole d'administration distante chiffré. Version 2 imposée sur tous les équipements.
STP	**Spanning Tree Protocol**	Protocole anti-boucle L2 (IEEE 802.1D). Variante Rapid PVST+ utilisée ici.
SVI	**Switched Virtual Interface**	Interface logique L3 d'un commutateur, associée à un VLAN. Porte la passerelle HSRP.

Acronyme	Développement	Définition courte
TPE	**Très Petite Entreprise**	Entreprise de moins de 10 salariés. DEPANMOI.FR en est une.
VIP	**Virtual IP Address**	Adresse IP partagée par plusieurs routeurs (HSRP/VRRP/CARP). Annoncée aux clients comme passerelle.
VLAN	**Virtual Local Area Network**	Segmentation logique L2 d'un réseau Ethernet. VLAN 610 (ADMIN) et 620 (ATELIER) utilisés ici.
VRRP	**Virtual Router Redundancy Protocol**	Standard IETF de redondance de passerelle. Équivalent ouvert de HSRP. Non retenu.
WAN	**Wide Area Network**	Réseau étendu. Désigne ici le segment vers le routeur FAI.

8.2 · Références aux RFC et standards

Les protocoles et conventions mobilisés dans le projet s'appuient sur les documents normatifs suivants.

Référence	Titre	Usage dans le projet
`RFC 1918`	Address Allocation for Private Internets	Plages IPv4 privées. Utilisé : `192.168.10.0/24` pour les VLAN, `10.0.0.0/8` pour les transits.
`RFC 2281`	Cisco Hot Standby Router Protocol	Spécification HSRP. Configuré entre CORE-01 et CORE-02.
`RFC 2328`	OSPF Version 2	Spécification OSPFv2. Process unique en area 0 sur les CORE et FW-01.
`RFC 2453`	RIP Version 2	Évoqué et écarté pour cause de convergence lente (~30 s).
`RFC 3021`	Using 31-Bit Prefixes on IPv4 Point-to-Point Links	Évoqué et écarté pour les transits, `/30` retenu pour universalité.
`RFC 4251–4254`	The Secure Shell (SSH) Protocol	SSH v2 imposé sur tous les équipements (administration).
`RFC 5798`	Virtual Router Redundancy Protocol Version 3	Évoqué et écarté au profit de HSRP (infrastructure 100 % Cisco).
`IEEE 802.1D`	Spanning Tree Protocol	Base STP, étendue ici en Rapid PVST+.
`IEEE 802.1Q`	VLAN Tagging	Encapsulation des VLAN sur les trunks SW-01 ↔ CORE.
`IEEE 802.1w`	Rapid Spanning Tree Protocol	Convergence rapide STP, intégrée à Rapid PVST+ Cisco.
`IEEE 802.3ad`	Link Aggregation	Standard LACP. Utilisé pour les EtherChannel `Po1` et `Po2`.

8.3 · Configurations archivées

Les configurations complètes des quatre équipements sont archivées dans le dossier de livraison à la commission. Elles peuvent être restaurées sur du matériel équivalent pour reproduire l'infrastructure.

Équipement	Fichiers archivés	Usage

CORE-01	`CORE01/core-01.depanmoi.lan-config-running`
	`CORE01/core-01.depanmoi.lan-config-startup`
	`CORE01/vlan.dat`
		Configuration vivante + persistante + base VLAN.

CORE-02	`CORE02/core-02.depanmoi.lan-config-running`
	`CORE02/core-02.depanmoi.lan-config-startup`
	`CORE02/vlan.dat`
		Configuration vivante + persistante + base VLAN.

SW-01	`SW-01/sw-01.depanmoi.lan-config-running`
	`SW-01/sw-01.depanmoi.lan-config-startup`
	`SW-01/vlan.dat`
		Configuration vivante + persistante + base VLAN.

FW-01	`PFSENSE/config-pfsense.depanmoi.lan-20260505134511.xml`	Sauvegarde XML complète (interfaces, FRR/OSPF, NAT, règles).

RESTAURATION D'UNE CONFIGURATION CISCO

Sur un Catalyst neuf : connecter en console (9600 8N1), `enable`, `copy tftp://<serveur>/<fichier>→running running-config` ou copier-coller en mode `configure terminal`. Le fichier `vlan.dat` doit être placé dans `flash:` avant le boot (commande `copy tftp: flash:vlan.dat`) puis l'équipement redémarré.

8.4 · Procédure de remplacement à froid de FW-01

Cette procédure couvre le risque résiduel `EF-08` (pas de redondance pfSense par CARP). En cas de panne matérielle de FW-01, un boîtier Netgate de prêt peut être remis en service à partir de la sauvegarde XML.

Pré-requis

- Boîtier Netgate identique ou compatible (mêmes modèles d'interfaces réseau si possible, les noms `mvneta0` dépendent du matériel).
- Image pfSense Plus 24.5 installée (ou supérieure si compatible).
- Sauvegarde XML récente (`config-pfsense.depanmoi.lan-*.xml`).
- Câble console et terminal (PuTTY ou minicom, 115200 8N1).
- Accès physique au site DEPANMOI.FR.

Étapes

1. **Démontage du boîtier en panne**, débrancher l'alimentation et les câbles WAN/LAN/OPT du FW-01 défaillant. Étiqueter les ports pour ne pas inverser au remontage.
2. **Mise en service du boîtier de remplacement**, connecter l'alimentation et le câble console. Démarrer le boîtier. Suivre l'installeur pfSense jusqu'à l'écran de login.
3. **Configuration minimale d'accès web**, assigner temporairement une IP à l'interface LAN via le menu console (option 2 *Set interface(s) IP address*). Se connecter à l'interface web depuis un poste sur le même segment.
4. **Restauration de la sauvegarde XML**, dans l'interface web : *Diagnostics* → *Backup & Restore* → *Restore configuration*. Charger le fichier XML, cocher *Restore*, valider. Le boîtier redémarre automatiquement.
5. **Branchement physique**, pendant le redémarrage, rebrancher les câbles WAN, LAN (TRANSIT1) et OPT (TRANSIT2) sur les ports d'origine.
6. **Vérifications après reboot** :
   - *Status* → *Interfaces* : WAN doit obtenir une IP via DHCP du FAI ; LAN = `10.0.0.2/30` ; OPT = `10.0.0.6/30` .
   - *Status* → *FRR* → *OSPF* → *Neighbors* : deux voisins (RID `1.1.1.1` et `2.2.2.2`) en état **Full**.
   - *Status* → *FRR* → *OSPF* → *Routes* : routes `192.168.10.0/25` et `192.168.10.128/25` reçues.
7. **Test fonctionnel**, depuis un poste utilisateur : `ping 1.1.1.1` . Le trafic Internet doit passer à nouveau.
8. **Suppression de l'IP temporaire LAN**, la sauvegarde XML écrase cette IP par `10.0.0.2/30` , donc rien à faire si la restauration s'est bien déroulée. Sinon, ajuster manuellement.

DURÉE ESTIMÉE ET IMPACT MÉTIER

Procédure complète : **30 à 45 minutes** hors temps de transport du boîtier de prêt. Pendant cette fenêtre, la sortie Internet est indisponible mais le LAN interne (postes ↔ ressources internes) reste opérationnel grâce au routage HSRP/OSPF entre les deux CORE. Les techniciens peuvent continuer à travailler en local et basculer leurs interventions client à distance vers du partage de connexion mobile en attendant.

RAPPEL, EXCLUSIONS DOCUMENTÉES

L'absence de redondance CARP de pfSense est une **décision assumée** du cahier des charges (`EF-08` Won't have). La présente procédure constitue le plan de continuité associé : remplacement matériel à froid, RTO d'environ 30–45 min hors transport, sans perte de configuration grâce à la sauvegarde XML.

8.5 · Affiche utilisateur : que faire en cas de panne Internet

DEPANMOI.FR, AFFICHE D'ACCUEIL

Plus d'Internet ?
Trois choses à vérifier

1 **Êtes-vous le seul à ne plus avoir Internet ?**

Demandez à un collègue. Si lui a Internet, le problème vient de votre poste : redémarrez-le (bouton démarrer → redémarrer).

2 **Tout le bureau est coupé ?**

Regardez le boîtier dans le local technique. Si le voyant Internet est rouge, c'est une panne du fournisseur d'accès. Contacter **Orange Pro au 3901** en communiquant le n° de contrat **0042 5871 9230**. Pas la peine de toucher au matériel.

3 **Le problème vient d'ailleurs ?**

Accéder aux configurations du matériel réseau pour diagnostiquer (HSRP, OSPF, DHCP). Identifiants administrateur dans le coffre-fort du local technique.

ACCÈS ADMINISTRATEUR

CORE-01

```
ssh admin@192.168.10.124
```

CORE-02

```
ssh admin@192.168.10.125
```

PFSENSE

```
https://192.168.10.253
```

Telnet désactivé