# Livrable 2 – Documentation technique

# 🌐 LOT 1 - Déploiement du Cœur Réseau : pfSense Haute Disponibilité (HA) et Dual WAN

[⬅️ Retour au Menu Livrable 2] | [🏠 Retour à l'accueil]

**Samy ALBISSER AP4 – Groupe 3**

***La Résilience du COD : Tolérance aux pannes et Continuité de Service***

> **Objectif Stratégique :** Le Centre Opérationnel Départemental (COD) ne peut souffrir d'aucune coupure réseau en période de crise. Ce premier lot vise à mettre en place le cœur de l'infrastructure réseau en respectant une architecture de **Haute Disponibilité (High Availability)**. En nous basant sur les recommandations de notre étude préalable, nous avons déployé un cluster de deux pare-feux **pfSense** virtuels sous Proxmox. Ce cluster exploite les protocoles **CARP** (pour la redondance de passerelle), **pfsync** (pour la synchronisation des états) et intègre un mécanisme de **Failover** pour redonder l'accès Internet (Dual WAN).

---

## 0. Plan d'Adressage du Cœur Réseau (Cluster pfSense)

*Note : Conformément à l'environnement de maquettage, l'adressage LAN a été fixé sur la plage `192.168.1.0/24`.*

| Hôte / Interface | Rôle | Réseau / VLAN | Adresse IP |
|---|---|---|---|
| **VIP-LAN (CARP)** | Passerelle Virtuelle Client | LAN | **192.168.1.254/24** |
| **SA-PF01 (Master)** | Routeur Principal | LAN (vtnet1) | 192.168.1.1/24 |
| | | SYNC (vtnet3) | 192.168.99.1/30 *(Dédié HA)* |
| **SA-PF02 (Backup)** | Routeur Secondaire | LAN (vtnet1) | 192.168.1.2/24 |
| | | SYNC (vtnet3) | 192.168.99.2/30 *(Dédié HA)* |

---

## 1. Préparation de l'Hyperviseur (Proxmox VE)

### 1.1. Configuration Matérielle des VMs (Hyperviseur Proxmox)

Afin de garantir l'isolation des flux et de respecter l'architecture cible, chaque machine virtuelle (VM 25700 pour `SA-PF01` et VM 25702 pour `SA-PF02`) a été provisionnée avec **1 vCPU, 1 Go de RAM** et **4 cartes réseaux (VirtIO)**.

Pour que le cluster Haute Disponibilité (CARP/pfsync) fonctionne correctement, les deux pare-feux doivent impérativement être connectés aux mêmes réseaux virtuels de niveau 2. Voici le plan de câblage virtuel appliqué à l'identique sur les deux nœuds :

| Carte réseau Proxmox | Commutateur Virtuel (Bridge) | Rôle / Affectation pfSense |
|---|---|---|
| **net0** | `AP4_WAN01` | **WAN** (Accès Internet |

| Carte réseau Proxmox | Commutateur Virtuel (Bridge) | Rôle / Affectation pfSense |
|---|---|---|
| | | Primaire) |
| **net1** | `SAMALB` | **LAN** (Réseau interne du COD) |
| **net2** | `AP4_WAN02` | **WAN2** (Accès Internet Secondaire / Secours) |
| **net3** | `SASYNCLAN` | **SYNC** (Lien direct et isolé pour la synchronisation du Cluster) |

*(Note : Un commutateur virtuel nommé `SASYNCWLAN` a également été provisionné sur l'hyperviseur, mais n'est pas exploité dans l'architecture actuelle).*

### 1.2. Assignation des interfaces sous pfSense

Une fois les systèmes démarrés, l'assignation des interfaces a été réalisée via la console, puis validée sur l'interface Web (`Interfaces > Interface Assignments`) sur les deux nœuds :

- **WAN** -> `vtnet0`
- **LAN** -> `vtnet1`
- **WAN2** -> `vtnet2`
- **SYNC** -> `vtnet3`

---

## 2. Déploiement du Cluster Haute Disponibilité (HA)

### 2.1. Configuration de l'interface de Synchronisation (SYNC)

L'interface SYNC est critique : elle fait transiter les états des connexions en temps réel et les modifications de configuration. Elle **doit être isolée** du trafic utilisateur.

1. **Activation :** Sur SA-PF01 et SA-PF02, activer l'interface `SYNC`.
2. **Adressage :**
   - SA-PF01 : IP Statique `192.168.99.1/30`
   - SA-PF02 : IP Statique `192.168.99.2/30`
3. **Pare-feu :** Dans `Firewall > Rules > SYNC`, création d'une règle "Allow All" en IPv4 pour autoriser les protocoles de synchronisation (TCP 443 pour XMLRPC et le protocole natif pfsync).

### 2.2. Création de l'Adresse IP Virtuelle (CARP)

Pour que les postes de travail du COD ne perdent jamais leur passerelle, nous utilisons le protocole CARP (Common Address Redundancy Protocol).

**Sur SA-PF01 (Nœud Principal) :**

1. Aller dans `Firewall > Virtual IPs > Add`.
2. **Type** : CARP
3. **Interface** : LAN
4. **Address** : `192.168.1.254 / 24` (C'est la passerelle distribuée aux clients).
5. **Virtual IP Password** : `P@sswordHA`
6. **VHID Group** : 1
7. **Advertising Frequency (Base / Skew)** : `1 / 0` (Le Skew à 0 indique que c'est le Master prioritaire).

**Sur SA-PF02 (Nœud Secondaire) :**

La configuration est automatiquement poussée si XMLRPC est configuré (voir étape suivante), mais le **Skew** sera défini sur `100` pour signifier qu'il est le Backup.

### 2.3. Activation de pfsync et XMLRPC

**Sur SA-PF01 :**

1. Aller dans `System > High Avail. Sync`.
2. Cocher **Synchronize States** et sélectionner l'interface `SYNC`.
3. **pfsync Synchronize Peer IP** : `192.168.99.2`.
4. **XMLRPC Sync** : Entrer l'IP du nœud secondaire (`192.168.99.2`), les identifiants administrateur de SA-PF02, et cocher tous les modules à synchroniser (Rules, NAT, Virtual IPs, DHCP, etc.).

**Sur SA-PF02 :**

1. Aller dans `System > High Avail. Sync`.
2. Cocher uniquement **Synchronize States** vers `192.168.99.1`. Ne pas configurer XMLRPC ici pour éviter une boucle de synchronisation.

---

## 3. Configuration du Service DHCP

Le service DHCP est indispensable pour distribuer automatiquement la passerelle virtuelle aux agents du COD.

**Sur SA-PF01 :**

1. Aller dans `Services > DHCP Server > LAN`.
2. **Backend** : `Kea DHCP` (Nouveau moteur DHCP moderne de pfSense).
3. **Range** : `192.168.1.100` à `192.168.1.200` (Plage définie pour les tests de maquette).
4. **Gateway** : `192.168.1.254` (L'IP de la VIP CARP, et **surtout pas** l'IP physique du routeur).

5. *Note : La configuration est automatiquement répliquée sur SA-PF02 grâce à XMLRPC.*

---

## 4. Tolérance aux pannes WAN (Failover Multi-WAN)

Afin de pallier la perte d'une ligne Internet au COD, nous mettons en place un groupe de passerelles (Gateway Group).

1. **Vérification des passerelles :** Dans `System > Routing > Gateways`, s'assurer que les passerelles `WANGW` et `WAN2GW` sont bien créées et supervisées (Ping IP).
2. **Création du Groupe :** Dans `System > Routing > Gateway Groups` :
   - Nom : `MULTIPLEXAGE_WAN`
   - Priority : `WAN` en Tier 1 (Principal), `WAN2` en Tier 2 (Secours).
   - Trigger Level : `Member Down` (Bascule uniquement si le lien primaire est physiquement hors ligne ou ne répond plus aux pings).
3. **Mise en service dans le Pare-feu :** Dans `Firewall > Rules > LAN`, modification de la règle de sortie "Default allow LAN to any" :
   - Cliquer sur *Advanced Options*.
   - Ligne **Gateway** : Sélectionner `MULTIPLEXAGE_WAN`.

---

**Conclusion et Validation :**

L'architecture de cœur de réseau est désormais robuste. Les tests de débranchement à chaud (virtuel) de l'interface LAN du PF01 ou de son extinction brutale démontrent un basculement (Failover) sur le PF02 en moins de 3 secondes, avec maintien du trafic continu (ping `8.8.8.8`).

# 🆔 LOT 2 - Déploiement de l'Annuaire Centralisé (Active Directory)

[ 🔙 Retour au Menu Livrable 2] | [ 🏠 Retour à l'accueil]

***Le Cœur de la Sécurité : Identité et Authentification Centralisée***

> **Objectif Stratégique :** Le Centre Opérationnel Départemental (COD) nécessite une gestion stricte et centralisée des identités (agents, administrateurs) pour garantir la traçabilité et la sécurité des accès. Ce lot consiste à déployer une forêt Active Directory unique (`sidsic.lan`). Pour assurer la continuité de service (haute disponibilité), l'annuaire repose sur **deux contrôleurs de domaine** : un serveur principal avec interface graphique (GUI) pour faciliter l'administration quotidienne, et un serveur secondaire en version "Core" (sans interface) pour réduire la surface d'attaque et l'empreinte mémoire.

## 0. Plan d'Adressage des Serveurs (LOT 2)

| Hôte | Rôle | OS | Réseau (VLAN LAN) | Passerelle |
|---|---|---|---|---|
| **SRV-AD01** | DC Principal, DNS | Windows Server 2022 (GUI) | **192.168.1.10/24** | 192.168.1.254 (VIP CARP) |
| **SRV-AD02** | DC Secondaire, DNS | Windows Server 2022 (Core) | **192.168.1.11/24** | 192.168.1.254 (VIP CARP) |

## 1. Prérequis et Configuration Réseau Initiale

Avant la promotion des serveurs, il est impératif de configurer des adresses IP statiques et de pointer les requêtes DNS correctement.

### 1.1. Configuration Matérielle des VMs (Hyperviseur Proxmox)

Afin que les contrôleurs de domaine puissent communiquer avec l'ensemble des équipements de la zone de confiance (LAN), ils doivent être raccordés au bon commutateur virtuel sous Proxmox.

Pour les deux machines virtuelles (`SRV-AD01` et `SRV-AD02`), une seule carte réseau (VirtIO) est nécessaire. Elle doit être pontée sur le réseau LAN du COD :

| Carte réseau Proxmox | Commutateur Virtuel (Bridge) | Rôle / Affectation de la VM |
|---|---|---|
| **net0** | `SAMALB` | **LAN** (Réseau interne du COD) |

### 1.2. Configuration de SRV-AD01 (GUI)

1. Depuis le Panneau de configuration (`ncpa.cpl`), ouvrir les propriétés de la carte réseau LAN.
2. **Désactivation de l'IPv6 :** Décocher la case **Protocole Internet version 6 (TCP/IPv6)**. Cela permet d'éviter les "bruits" réseaux et l'enregistrement d'adresses APIPA dans le futur serveur DNS.
3. Sélectionner **Protocole Internet version 4 (TCP/IPv4)** et configurer :
    - **Adresse IP** : `192.168.1.10`
    - **Masque** : `255.255.255.0`
    - **Passerelle** : `192.168.1.254` (L'IP virtuelle du cluster pfSense).
    - **Serveur DNS préféré** : `192.168.1.10` (Lui-même, en prévision du rôle DNS).
    - **Serveur DNS auxiliaire** : `192.168.1.11` (Le futur DC secondaire).
4. Renommer le serveur en `SRV-AD01` et redémarrer.

### 1.3. Configuration de SRV-AD02 (Core)

1. Au démarrage de la session, l'utilitaire `sconfig` s'ouvre automatiquement.
2. Choisir l'option **8) Paramètres réseau**.
3. Configurer l'adresse IP statique : `192.168.1.11` / Masque `255.255.255.0` / Passerelle `192.168.1.254`.
4. Configurer les serveurs DNS : Principal `192.168.1.11` (lui-même) et Secondaire `192.168.1.10` (le DC principal).
5. Quitter `sconfig` (option 15) pour revenir à l'invite PowerShell.
6. **Désactivation de l'IPv6 :** Taper la commande suivante pour couper l'IPv6 sur toutes les cartes :

   ```
   Disable-NetAdapterBinding -Name "*" -ComponentID ms_tcpip6
   ```

7. Relancer `sconfig`, choisir l'option **2) Nom de l'ordinateur**, renommer en `SRV-AD02` et redémarrer.

---

## 2. Création de la Forêt Active Directory (SRV-AD01)

### 2.1. Installation du rôle AD DS

1. Ouvrir le **Gestionnaire de serveur**.
2. Cliquer sur **Ajouter des rôles et fonctionnalités**.
3. Sélectionner **Services AD DS** (Active Directory Domain Services) et inclure les outils de gestion.
4. Lancer l'installation. Le rôle **Serveur DNS** sera automatiquement coché et installé lors de la promotion.

### 2.2. Promotion en Contrôleur de Domaine

1. Cliquer sur le drapeau de notification en haut à droite > **Promouvoir ce serveur en contrôleur de domaine**.
2. Opération de déploiement : **Ajouter une nouvelle forêt**.
3. Nom de domaine racine : **`sidsic.lan`**.
4. Saisir le mot de passe de restauration des services d'annuaire (DSRM) : `P@ssword10`.
5. Conserver les chemins par défaut pour la base de données (NTDS), les journaux et le dossier SYSVOL.
6. Cliquer sur **Installer**. Le serveur redémarre automatiquement. Le domaine `sidsic.lan` est désormais opérationnel.

---

# 3. Ajout du Contrôleur Secondaire (SRV-AD02 - Core)

Pour garantir la haute disponibilité de l'authentification et respecter les bonnes pratiques Microsoft, le serveur Core sera administré de manière centralisée. Le rôle sera installé et promu à distance, directement depuis l'interface graphique du contrôleur principal (`SRV-AD01`).

## 3.1. Jonction au domaine (sur SRV-AD02)

Afin que le serveur principal puisse administrer le serveur Core de façon sécurisée, ce dernier doit d'abord être membre du domaine.

1. Sur `SRV-AD02`, lancer l'utilitaire `sconfig`.
2. Choisir l'option **1) Domaine/Groupe de travail** et sélectionner **Domaine** (D).
3. Taper le nom du domaine : `sidsic.lan`.
4. Renseigner un compte autorisé à joindre le domaine (ex: `sidsic\Administrateur`) et son mot de passe.
5. Modifier le nom de l'ordinateur si nécessaire, puis **Redémarrer** le serveur pour appliquer les changements.

## 3.2. Installation du rôle à distance (sur SRV-AD01)

1. Se connecter sur `SRV-AD01` avec le compte Administrateur du domaine.
2. Ouvrir le **Gestionnaire de serveur**, cliquer sur **Gérer** > **Ajouter des serveurs**.
3. Dans l'onglet *Active Directory*, cliquer sur *Rechercher*, sélectionner `SRV-AD02`, l'ajouter à la colonne de droite et valider (**OK**).
4. Cliquer ensuite sur **Gérer** > **Ajouter des rôles et fonctionnalités**.
5. À l'étape *Sélection du serveur de destination*, choisir impérativement **SRV-AD02.sidsic.lan**.
6. Cocher le rôle **Services AD DS** (Active Directory Domain Services), accepter l'ajout des outils de gestion et finaliser l'installation.

## 3.3. Promotion en Contrôleur de domaine (sur SRV-AD01)

1. Une fois l'installation terminée, cliquer sur le drapeau de notification (attention au bandeau jaune) dans le Gestionnaire de serveur de `SRV-AD01`.
2. Cliquer sur le lien **Promouvoir ce serveur en contrôleur de domaine** (qui cible toujours le SRV-AD02).
3. Choisir l'opération : **Ajouter un contrôleur de domaine à un domaine existant** (`sidsic.lan`).
4. Saisir le mot de passe de restauration DSRM (`P@ssword10`).
5. Conserver les options par défaut (Catalogue global, Serveur DNS) et lancer l'installation.
6. Le serveur `SRV-AD02` va redémarrer automatiquement et deviendra opérationnel en tant que DC de secours.

---

# 4. Structuration de l'Annuaire (Unités d'Organisation, Utilisateurs et Groupes)

Afin de préparer l'application des futures Stratégies de Groupe (GPO) et d'organiser logiquement les ressources du COD, nous devons structurer l'annuaire. L'utilisation de la console graphique depuis `SRV-AD01` est privilégiée.

## 4.1. Création de l'arborescence (OUs)

1. Sur `SRV-AD01`, ouvrir le **Gestionnaire de serveur** > **Outils** > **Utilisateurs et ordinateurs Active Directory** (`dsa.msc`).
2. Faire un clic droit sur la racine du domaine `sidsic.lan` > **Nouveau** > **Unité d'organisation**.
3. Nommer cette UO racine : `COD_SIDSIC` (laisser la case *Protéger le conteneur contre une suppression accidentelle* cochée).
4. Faire un clic droit sur la nouvelle UO `COD_SIDSIC` > **Nouveau** > **Unité d'organisation** pour créer les sous-dossiers suivants :
    - `Agents_Terrain` (Destiné aux futurs utilisateurs du VPN et d'eBrigade).
    - `Administration` (Destiné aux comptes techniques et à l'équipe IT du SIDSIC).
    - `Serveurs` (Destiné à accueillir les futurs serveurs applicatifs comme la VoIP ou la Messagerie).

## 4.2. Création des Groupes de Sécurité

Les groupes permettront de gérer les droits d'accès (aux dossiers partagés, au VPN, etc.) de manière globale, sans avoir à gérer les permissions utilisateur par utilisateur.

1. Faire un clic droit dans l'UO `Agents_Terrain` > **Nouveau** > **Groupe**.
2. Nom du groupe : `GRP_Agents` (Étendue : *Globale*, Type : *Sécurité*).
3. Répéter l'opération dans l'UO `Administration` pour créer le groupe `GRP_Admins`.

## 4.3. Création des Comptes Utilisateurs (Tests)

1. Faire un clic droit dans l'UO `Agents_Terrain` > **Nouveau** > **Utilisateur**.
2. Remplir les informations (ex: Prénom : *Agent*, Nom : *01*, Nom d'ouverture de session : `agent01@sidsic.lan`).
3. Définir un mot de passe complexe (ex: `P@ssword123!`). Pour les tests, décocher *L'utilisateur doit changer le mot de passe à la prochaine session* et cocher *Le mot de passe n'expire jamais*.
4. Une fois l'utilisateur créé, faire un clic droit dessus > **Ajouter à un groupe...** > taper `GRP_Agents` et valider.

5. Créer de la même manière un compte `admin01` dans l'UO `Administration` et l'ajouter au groupe `GRP_Admins` (ainsi qu'au groupe natif `Admins du domaine` pour lui donner les pleins pouvoirs).

### 4.4. Configuration des Translateurs DNS (Accès Internet)

Afin que les postes clients n'interrogent que nos contrôleurs de domaine tout en conservant l'accès à Internet, nous devons configurer des "Translateurs" (Forwarders) sur nos serveurs DNS. **Cette configuration doit être appliquée sur les deux contrôleurs pour garantir la haute disponibilité de la résolution externe.**

1. Sur `SRV-AD01`, ouvrir le **Gestionnaire de serveur** > **Outils** > **DNS**.
2. Faire un clic droit sur le nom du serveur (`SRV-AD01`) et choisir **Propriétés**.
3. Aller dans l'onglet **Redirecteurs**.
4. Cliquer sur **Modifier** et ajouter **uniquement** l'adresse IP du DNS de l'école ou de la passerelle WAN : `10.10.10.1`. *(Note : Les DNS publics comme 8.8.8.8 ont été volontairement exclus car ils sont bloqués par le pare-feu du réseau physique hôte)*.
5. Valider par **OK**.
6. Répéter impérativement la même opération (étapes 1 à 5) en se connectant à la console DNS du second serveur (`SRV-AD02`), soit en l'ajoutant dans la console DNS de `SRV-AD01`, soit via PowerShell. Le domaine se chargera désormais de résoudre les requêtes externes de manière redondante.

---

## 5. Adaptation du DHCP (pfSense) et Validation DNS

Pour que les postes de travail (et les futurs agents connectés) puissent joindre le domaine `sidsic.lan`, ils doivent obligatoirement interroger nos contrôleurs de domaine pour la résolution DNS. Il faut donc modifier le service DHCP pour qu'il distribue les bonnes adresses DNS.

### 5.1. Modification des serveurs DNS distribués

1. Se connecter à l'interface d'administration web du pare-feu principal (`SA-PF01`).
2. Naviguer dans le menu **Services** > **DHCP Server** et sélectionner l'onglet **LAN**.
3. Descendre jusqu'à la section **Servers**.
4. Dans les champs **DNS Servers**, renseigner les adresses statiques de nos contrôleurs de domaine :
    - Serveur DNS 1 : `192.168.1.10` (`SRV-AD01`)
    - Serveur DNS 2 : `192.168.1.11` (`SRV-AD02`)
5. *Point de vigilance :* Ne laisser aucun DNS public externe (comme 8.8.8.8) dans cette liste. Si un client Windows reçoit un DNS public en secours, il risque d'y envoyer ses requêtes d'authentification AD, ce qui fera échouer la connexion au domaine.

6. Cliquer sur **Save** tout en bas, puis sur le bouton **Apply Changes** en haut de la page. *(Rappel : grâce à XMLRPC, cette configuration est automatiquement synchronisée vers SA-PF02)*.

### 5.2. Validation sur un poste client (Test de recette)

Pour s'assurer que la modification DHCP est bien active :

1. Allumer un poste client Windows 10/11 connecté au réseau LAN.
2. Ouvrir une invite de commande (`cmd.exe`).
3. Forcer le renouvellement du bail DHCP avec les commandes :
   - `ipconfig /release`
   - `ipconfig /renew`
4. Taper `ipconfig /all` et vérifier la ligne **Serveurs DNS** : elle doit afficher `192.168.1.10` et `192.168.1.11`.
5. Taper `ping sidsic.lan` : le domaine doit résoudre l'une des deux adresses IP de nos contrôleurs, confirmant que le réseau est prêt à accueillir des machines dans l'Active Directory.

---

# LOT 3 - Accès Distant Sécurisé (VPN Road Warrior)

[ Retour au Menu Livrable 2] | [ Retour à l'accueil]

***La Mobilité Sécurisée : Connecter les agents de terrain au COD***

> **Objectif Stratégique :** En situation de crise, les agents déployés sur le terrain (Poste de Commandement Opérationnel) doivent accéder aux ressources internes du Centre Opérationnel Départemental (eBrigade, Téléphonie, Messagerie) de manière sécurisée. Nous déployons un tunnel **OpenVPN en mode Road Warrior**. Afin de garantir les meilleures performances possibles, notamment pour les flux voix en temps réel (VoIP) qui sont très sensibles à la latence, le tunnel utilise le protocole standard **UDP (port 1194)**. L'authentification est directement interfacée avec notre **Active Directory** (Lot 2), appliquant ainsi le principe de centralisation des identités (SSO).

---

## 0. Paramètres de l'Architecture VPN

Afin de ne pas créer de conflits de routage, un sous-réseau spécifique est dédié aux clients nomades connectés via le tunnel VPN.

| Paramètre | Valeur Technique | Justification |
|---|---|---|
| **Protocole / Port** | OpenVPN (UDP / 1194) | Protocole standard, |

| Paramètre | Valeur Technique | Justification |
|---|---|---|
| | | performant et optimisé pour le trafic temps réel (VoIP). |
| **Réseau Tunnel (Virtuel)** | `10.8.0.0 / 24` | Plage d'adressage isolée, distribuée aux clients VPN. |
| **Réseau Local (Cible)** | `192.168.1.0 / 24` | Accès au réseau LAN du COD. |
| **Chiffrement (ANSSI)** | AES-256-GCM / SHA256 | Respect des normes cryptographiques imposées. |

## 1. Intégration de l'Active Directory (LDAP) dans pfSense

Pour que les agents utilisent leurs identifiants de session Windows pour se connecter au VPN, pfSense doit pouvoir interroger nos contrôleurs de domaine. Une attention particulière est portée aux chemins de recherche (Base DN) pour inclure l'ensemble des Unités d'Organisation de notre annuaire.

1. Se connecter à `SA-PF01` et aller dans `System > User Manager > Authentication Servers`.
2. Cliquer sur **Add** pour déclarer le serveur AD et configurer les paramètres suivants :
    - **Descriptive name** : `AD_SIDSIC`
    - **Type** : `LDAP`
    - **Hostname or IP address** : `192.168.1.10` (`SRV-AD01`)
    - **Port value** : `389` (TCP)
    - **Search scope** : `Entire Subtree` *(Indispensable pour autoriser pfSense à fouiller dans les sous-dossiers de l'AD).*
    - **Base DN** : `DC=sidsic,DC=lan`
    - **Authentication containers** : Cliquer sur le bouton bleu *Select a container* et cocher au minimum :
        - `OU=COD_SIDSIC,DC=sidsic,DC=lan` (Pour cibler les agents et l'équipe IT).
        - `CN=Users,DC=sidsic,DC=lan` (Pour cibler le compte Administrateur natif).
    - **Bind anonymous** : Décocher la case.
    - **Bind credentials** : Renseigner les identifiants d'un compte autorisé au format UPN (ex: `Administrateur@sidsic.lan`) et son mot de passe.
    - **User naming attribute** : `sAMAccountName` *(Standard requis pour Microsoft Active Directory).*
3. Cliquer sur **Save**.

4. *Test de validation :* Aller dans `Diagnostics > Authentication`, sélectionner `AD_SIDSIC` et tester avec le compte `agent01` (créé au Lot 2). L'authentification doit réussir avec un message en vert.

---

## 2. Création de l'Infrastructure à Clé Publique (PKI)

OpenVPN nécessite des certificats pour chiffrer les échanges. Nous allons créer une Autorité de Certification (CA) locale et un certificat pour le serveur.

1. **Création de la CA :**
   - Aller dans `System > Certificates > Authorities` > **Add**.
   - Method : `Create an internal Certificate Authority`.
   - Descriptive name : `SIDSIC-CA`.
   - Key type : `RSA` / `2048` bits.
   - Remplir les champs d'identification :
     - Country Code : `FR` (France)
     - State or Province : `Bas-Rhin`
     - City or Locality : `Strasbourg`
     - Organization : `SIDSIC` (Service Interministériel Départemental des Systèmes d'Information et de Communication)
     - Organizational Unit : `COD` (Centre Opérationnel Départemental)
     - Email Address : `admin@sidsic.lan`
     - Common Name : `SIDSIC-CA`
   - Sauvegarder.
2. **Création du Certificat Serveur :**
   - Aller dans `System > Certificates > Certificates` > **Add/Sign**.
   - Method : `Create an internal Certificate`.
   - Descriptive name : `pfSense-VPN-Server`.
   - Certificate authority : `SIDSIC-CA`.
   - Certificate Type : `Server Certificate`.
   - Common name : `pfSense-VPN-Server`
   - Sauvegarder.

---

## 3. Configuration du Serveur OpenVPN

La création du tunnel s'effectue sur le nœud principal (`SA-PF01`). *(Rappel : grâce au Lot 1, cette configuration sera automatiquement répliquée sur SA-PF02).*

1. Aller dans `VPN > OpenVPN > Servers` et cliquer sur **Add**.
2. **General Information :**

- Server Mode : `Remote Access (User Auth)` (Pour utiliser l'AD).
- Backend for authentication : `AD_SIDSIC`.
- Protocol : `UDP on IPv4 only`.
- Interface : `WAN`.
- Local Port : `1194`.

3. **Cryptographic Settings :**
   - TLS Key : Cocher `Automatically generate a TLS Key`.
   - Peer Certificate Authority : `SIDSIC-CA`.
   - Server Certificate : `pfSense-VPN-Server`.
   - Data Encryption Algorithms : `AES-256-GCM` et `AES-256-CBC`.
   - Auth digest algorithm : `SHA256`.
4. **Tunnel Settings :**
   - IPv4 Tunnel Network : `10.8.0.0/24`.
   - IPv4 Local network(s) : `192.168.1.0/24`.
   - Concurrent connections : `10` (Limite fixée par le cahier des charges).
5. **Advanced Client Settings :**
   - DNS Default Domain : `sidsic.lan`.
   - DNS Server 1 : `192.168.1.10`.
   - DNS Server 2 : `192.168.1.11`.
6. Cliquer sur **Save**.

---

## 4. Ouverture des Flux (Règles de Pare-feu)

Pour autoriser l'établissement du tunnel depuis l'extérieur, puis autoriser les nomades à accéder au LAN, deux règles doivent être créées :

1. **Autoriser la connexion WAN vers OpenVPN :**
   - Aller dans `Firewall > Rules > WAN`.
   - Action : `Pass` / Interface : `WAN` / Protocol : `UDP`.
   - Destination : `WAN net` / Destination Port : `OpenVPN (1194)`.
   - Description : `Allow OpenVPN Inbound (UDP 1194)`.
2. **Autoriser le trafic à l'intérieur du Tunnel vers le LAN :**
   - Aller dans `Firewall > Rules > OpenVPN`.
   - Action : `Pass` / Interface : `OpenVPN` / Protocol : `Any`.
   - Source : `OpenVPN net` / Destination : `LAN net`.
   - Description : `Allow VPN clients to access COD LAN`.

---

## 5. Déploiement et Test Client (Recette)

Pour faciliter le déploiement sur les postes des agents, nous utilisons le package officiel d'exportation.

1. **Installation de l'outil :**
   - Aller dans `System > Package Manager > Available Packages`.
   - Chercher et installer **`openvpn-client-export`**.
2. **Génération du fichier client :**
   - Aller dans `VPN > OpenVPN > Client Export`.
   - Sélectionner le serveur `Remote Access Server`.
   - Host Name Resolution : S'assurer que l'IP publique ou virtuelle du WAN est bien renseignée.
   - Tout en bas de la page, télécharger le fichier de configuration standard (`Inline Configuration / Most Clients`).
3. **Test de connexion depuis l'extérieur (Poste Agent01) :**
   - Sur un poste Windows 11 connecté à un réseau externe (ex: partage de connexion 4G mobile), installer le client *OpenVPN Connect*.
   - Importer le fichier `.ovpn` généré précédemment.
   - Lancer la connexion : la fenêtre demande un nom d'utilisateur et un mot de passe.
   - Saisir : `agent01` et son mot de passe Active Directory.
   - **Validation :** Le tunnel monte (l'icône passe au vert). Le poste reçoit une IP en `10.8.0.x`. Le `ping 192.168.1.10` (Contrôleur de domaine) répond correctement. L'agent est connecté de manière sécurisée.

---

# 📞 LOT 4 - Déploiement de la Téléphonie Sécurisée (VoIP)

[ ⬅️ Retour au Menu Livrable 2] | [ 🏠 Retour à l'accueil]

***Communications de Crise : Confidentialité et Haute Disponibilité***

> **Objectif Stratégique :** En période de gestion de crise, les communications vocales du Centre Opérationnel Départemental (COD) sont hautement confidentielles. Ce lot vise à déployer un autocommutateur téléphonique privé (IPBX) basé sur **FreePBX / Asterisk**. Pour garantir une sécurité absolue (Anti-Écoute / Sniffing), les flux de signalisation sont chiffrés via **SIP-TLS** et l'audio via **SRTP**. Conformément au cahier des charges, ce serveur n'est accessible que depuis la zone de confiance (LAN) et le tunnel nomade (VPN OpenVPN du Lot 3). **Aucune exposition vers l'Internet (WAN) n'est autorisée.** L'annuaire Active Directory est interrogé pour centraliser la gestion des utilisateurs.

## 0. Plan d'Adressage du Serveur VoIP (LOT 4)

| Hôte | Rôle | OS | Réseau (VLAN LAN) | Passerelle |
|---|---|---|---|---|
| **SRV-VOIP01** | Serveur IPBX (FreePBX) | **Debian 12.5 (Standard)** | **192.168.1.40/24** | 192.168.1.254 (VIP CARP) |

## 1. Installation du Serveur et Configuration Réseau (Lignes de commande)

L'installation repose sur une machine virtuelle Debian 12 vierge. Ce choix d'architecture garantit une maîtrise totale du système d'exploitation et unYe cohérence avec le reste de notre infrastructure Linux.

### 1.1. Configuration de l'Adressage Statique

Une fois Debian installé, il faut fixer l'adresse IP pour que les téléphones puissent toujours trouver le serveur.

1. Se connecter en `root` sur la console de la VM.
2. Éditer le fichier de configuration réseau : `nano /etc/network/interfaces`
3. Remplacer la configuration DHCP par la configuration statique suivante :

```
auto eth0
iface eth0 inet static
    address 192.168.1.40
    netmask 255.255.255.0
    gateway 192.168.1.254
```

4. Éditer le fichier de résolution DNS : `nano /etc/resolv.conf`

```
nameserver 192.168.1.10
nameserver 192.168.1.11
domain sidsic.lan
```

5. Appliquer la configuration en redémarrant le service réseau : `systemctl restart networking`.

### 1.2. Déploiement de FreePBX 17 via le script officiel

L'éditeur Sangoma propose un script d'installation automatisé pour Debian 12, qui installe toutes les dépendances (Apache, MariaDB, PHP 8) et compile Asterisk.

1. Mettre à jour le système :

```
apt update && apt upgrade -y
```

2. Installer l'utilitaire de téléchargement `wget` si absent :

```
apt install wget -y
```

3. Lancer le script d'installation officiel FreePBX pour Debian :

```
wget https://github.com/FreePBX/sng_freepbx_debian_install/raw/master/sng_freepbx_debian_install.sh -O /tmp/sng_freepbx_debian_install.sh

bash /tmp/sng_freepbx_debian_install.sh
```

4. *Le script va tourner pendant environ 10 à 15 minutes*. Une fois terminé, redémarrer la machine : `reboot`.

5. Depuis un poste Windows sur le réseau (ex: le PC admin), ouvrir un navigateur web et aller sur `http://192.168.1.40`. L'assistant de premier démarrage demande de créer le compte administrateur (ex: `admin` / `P@sswordVoIP!`).

---

## 2. Configuration Cryptographique (SIP-TLS et SRTP)

Par défaut, la voix sur IP passe en clair sur le réseau. Pour empêcher l'interception des appels (man-in-the-middle), nous devons générer des certificats et forcer l'IPBX à utiliser le canal sécurisé PJSIP.

### 2.1. Création du Certificat Interne

1. Dans l'interface web FreePBX, aller dans le menu **Admin** > **Certificate Management**.
2. Cliquer sur le bouton **New Certificate** puis sur **Generate Self-Signed Certificate**.
3. Remplir le formulaire :
   - **Hostname** : `srv-voip01.sidsic.lan`
   - **Description** : `Certificat_VoIP_SIDSIC`
4. Cliquer sur **Generate Certificate**.
5. Une fois créé, cliquer sur le bouton de validation (coche) dans la colonne "Default" pour définir ce certificat par défaut.

### 2.2. Activation du transport sécurisé (TLS)

1. Aller dans le menu **Settings** > **Asterisk SIP Settings**.
2. Dans l'onglet **General SIP Settings**, repérer la section *Local Networks* et s'assurer que notre réseau y est bien déclaré : `192.168.1.0 / 24`.
3. Cliquer tout en haut sur le sous-onglet **SIP Settings (chan_pjsip)**.
4. Descendre jusqu'à la section **TLS/IPv4** et configurer :

- **Certificate Manager** : Sélectionner `Certificat_VoIP_SIDSIC` (celui qu'on vient de créer).
- **SSL Method** : `tlsv1_2`
- **tls - 0.0.0.0 - All :** Yes
- **Port to Listen On (tls)** : `5061` (C'est le port standard pour le SIP sécurisé).

5. Cliquer tout en bas sur **Submit**, puis sur le gros bouton rouge **Apply Config** (en haut à droite) pour appliquer les paramètres au cœur d'Asterisk.

---

## 3. Intégration à l'Active Directory (LDAP)

Plutôt que de recréer manuellement tous les agents, FreePBX va s'interfacer avec le contrôleur de domaine (SRV-AD01) pour importer les utilisateurs.

1. Aller dans le menu **Admin** > **User Management**.
2. Dans l'onglet **Directories**, cliquer sur **Add** puis choisir **Microsoft Active Directory**.
3. Remplir rigoureusement les paramètres de la section *Directory Settings* :
   - **Host(s)** : `192.168.1.10`
   - **Port** : `389`
   - **Username** : `CN=Administrateur,CN=Users,DC=sidsic,DC=lan` *(C'est ce format strict qui valide la connexion)*.
   - **Password** : Le mot de passe de l'administrateur.
   - **Domain** : `sidsic.lan`
   - **Base DN** : `DC=sidsic,DC=lan` *(Pour chercher dans toute l'arborescence)*.
4. Dans la section *Operational Settings*, s'assurer que **Create Missing Extensions** est réglé sur `Don't Create` (les numéros seront affectés manuellement).
5. Cliquer sur **Submit**.
6. Forcer une synchronisation immédiate en cliquant sur l'icône de rafraîchissement (à droite de la barre de recherche). Les comptes de l'AD (ex: agent01, admin01) remontent désormais automatiquement dans l'onglet Users.

---

## 4. Création des Extensions Téléphoniques (Postes)

Maintenant que l'infrastructure sécurisée est en place, nous devons attribuer un numéro de téléphone interne (extension) à nos utilisateurs.

1. Aller dans le menu **Connectivity** > **Extensions**.
2. Cliquer sur **Add Extension** > **Add New PJSIP Extension**.
3. **Dans l'onglet "General" :**
   - **User Extension** : `101` (Le numéro de téléphone).
   - **Display Name** : `Agent 01`

- **Secret** : Remplacer le mot de passe généré par un mot de passe connu et complexe (ex: `P@ssVoIP101!`).
- **Select User Directory :** `AD_SIDSIC`
- **Link to a Default User** : Ouvrir la liste déroulante et sélectionner `agent01` (issu de l'AD).

4. **Dans l'onglet "Advanced" (C'est ici qu'on force la sécurité) :**
   - **Transport** : Sélectionner `0.0.0.0-tls` (Pour forcer le téléphone à communiquer sur le port 5061 sécurisé).
   - **Media Encryption** : Sélectionner `SRTP via in-SDP (sdes)` (C'est cette option précise qui chiffre la voix/l'audio).
   - **Enable AVPF** : Mettre sur `Yes`
   - **Force AVP** : Mettre sur `Yes`
5. Répéter l'opération complète pour créer l'extension `102` (pour `admin01`).
6. Cliquer sur **Submit** puis sur le bouton rouge **Apply Config**.

---

## 5. Déploiement du Client (Softphone Linphone) et Recette

Afin de valider que la téléphonie fonctionne uniquement de manière sécurisée et interne (via le réseau LAN ou le tunnel VPN du Lot 3), nous utilisons le client logiciel libre **Linphone** sur les postes clients.

### 5.1. Configuration du softphone Linphone et gestion du certificat

**Étape A : Paramétrage initial dans l'interface**

1. Sur le poste client Windows, lancer Linphone.
2. Cliquer sur l'assistant **Utiliser un compte SIP**.
3. Remplir les informations de connexion :
   - **Nom d'utilisateur** : `101`
   - **Mot de passe** : `P@ssVoIP101!`
   - **Domaine SIP** : `192.168.1.40`
   - **Transport** : Choisir impérativement **TLS**.
4. Valider l'enregistrement. À ce stade, la connexion échoue (erreur de paramètres) car le certificat du serveur IPBX est auto-signé et Linphone le bloque par sécurité.
5. Quitter complètement Linphone (clic droit sur l'icône dans la zone de notification en bas à droite de la barre des tâches > **Quitter**).

**Étape B : Acceptation du certificat auto-signé (Fichier de configuration)**

Afin d'autoriser Linphone à faire confiance à notre certificat interne, une modification du fichier de configuration maître est nécessaire :

1. Sur le clavier, appuyer sur `Windows + R` pour ouvrir la fenêtre *Exécuter*.

2. Taper `%localappdata%\linphone` et valider par *Entrée* pour ouvrir le répertoire de l'application.
3. Repérer le fichier `linphonerc` (sans extension) et l'ouvrir avec le Bloc-notes.
4. Rechercher la balise `[sip]`.
5. Ajouter (ou modifier) la ligne suivante juste en dessous pour désactiver la vérification stricte de l'autorité de certification :

   ```
   verify_server_certs=0
   ```

6. Sauvegarder le fichier (`Ctrl + S`) et fermer le Bloc-notes.

**Étape C : Validation cryptographique**

1. Relancer Linphone. Grâce à la modification précédente, le client se connecte instantanément au serveur en TLS (voyant vert).
2. Aller dans les **Paramètres** de votre compte, Activez AVPF sur les deux linphone.

### 5.2. Scénarios de Validation (Checklist de Recette)

Pour s'assurer du respect strict du cahier des charges, les tests suivants ont été exécutés :

- ✅ **Test 1 : Appel LAN à LAN (Chiffré)**
  - *Action :* Le poste `101` (Agent01) appelle le poste `102` (Admin01) en interne.
  - *Résultat :* L'appel aboutit. Un "cadenas fermé" s'affiche sur l'interface de Linphone, confirmant que le flux audio SRTP (chiffrement de bout en bout) est bien actif.
- ✅ **Test 2 : Appel depuis l'extérieur via VPN (Road Warrior)**
  - *Action :* Le poste `101` est connecté sur un point d'accès externe (ex: partage 4G), monte son tunnel OpenVPN UDP (Lot 3), puis lance un appel vers le `102`.
  - *Résultat :* L'appel aboutit sans erreur. La qualité vocale est préservée grâce au protocole UDP du VPN, et la signalisation transite de manière invisible par le tunnel chiffré.

---

# 📧 LOT 5 - Déploiement de la Messagerie Interne Sécurisée (iRedMail)

[ 🔙 Retour au Menu Livrable 2] | [ 🏠 Retour à l'accueil]

***Communications Officielles : Serveur de Messagerie et Travail Collaboratif***

**Objectif Stratégique :** Les agents du Centre Opérationnel Départemental (COD) doivent pouvoir échanger des informations critiques, des rapports d'interventions (générés par eBrigade) et recevoir des alertes de supervision, même en cas de coupure totale d'Internet. Pour répondre à ce besoin d'autonomie et de sécurité, un serveur de messagerie local basé sur la solution open-source **iRedMail** a été déployé sous Linux (Debian 12). Cette solution "tout-en-un" intègre des mécanismes de sécurité avancés (antispam, antivirus, Fail2ban) et propose le Webmail professionnel Roundcube. Conformément au cahier des charges, l'authentification des boîtes mails est couplée à l'Active Directory (SSO).

---

## 0. Plan d'Adressage du Serveur de Messagerie (LOT 5)

| Hôte | Rôle | OS | Réseau (VLAN LAN) | Passerelle |
|---|---|---|---|---|
| **SRV-MAIL01** | Serveur SMTP/IMAP (iRedMail) | Debian 12.5 | **192.168.1.50/24** | 192.168.1.254 (VIP CARP) |

---

## 1. Préparation du Serveur et Enregistrements DNS

La messagerie est le service réseau le plus strict concernant la résolution de noms. Avant même d'installer iRedMail, le serveur doit posséder un nom de domaine pleinement qualifié (FQDN) et être reconnu par l'Active Directory.

### 1.1. Adressage statique et Nom d'hôte (Sur Debian)

1. Créer une machine virtuelle Debian 12 vierge et la connecter au réseau LAN.
2. Fixer l'adresse IP statique dans `nano /etc/network/interfaces` :

```
auto eth0
iface eth0 inet static
    address 192.168.1.50
    netmask 255.255.255.0
    gateway 192.168.1.254
```

3. Configurer le FQDN du serveur. C'est **obligatoire** pour iRedMail.
    - Éditer `nano /etc/hostname` et inscrire : `srv-mail01`
    - Éditer `nano /etc/hosts` et ajouter la ligne suivante en premier :

      ```
      192.168.1.50   srv-mail01.sidsic.lan   srv-mail01
      ```

4. Redémarrer le serveur (`reboot`) et vérifier avec la commande `hostname -f` (qui doit retourner `srv-mail01.sidsic.lan`).

### 1.2. Enregistrements DNS (Sur SRV-AD01)

Pour que les autres serveurs (comme PRTG ou eBrigade) sachent où envoyer les e-mails, il faut créer les enregistrements DNS sur le contrôleur de domaine.

1. Ouvrir le Gestionnaire de serveur > Outils > **DNS** sur `SRV-AD01`.
2. Développer la zone de recherche directe `sidsic.lan`.
3. **Créer un Hôte (A) :** Clic droit > *Nouvel hôte (A ou AAAA)*. Nom : `srv-mail01`, Adresse IP : `192.168.1.50`.
4. **Créer le pointeur Mail (MX) :** Clic droit > *Nouveau système d'échange de courrier (MX)*.
    - Hôte ou domaine : (laisser vide).
    - Nom de domaine complet du serveur de messagerie : `srv-mail01.sidsic.lan`.
    - Priorité : `10`.

---

## 2. Déploiement Automatisé d'iRedMail

iRedMail utilise un script de déploiement interactif qui compile et configure automatiquement Postfix (Envoi), Dovecot (Réception), MariaDB (Base de données), Nginx (Serveur Web) et Roundcube (Webmail).

1. Mettre à jour le système et installer l'utilitaire d'archivage :

```
apt update && apt upgrade -y
apt install tar gzip wget -y
```

2. Télécharger et extraire la dernière version stable d'iRedMail :Bash

```
cd /root
wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.6.8.tar.g
z
tar -zxf 1.6.8.tar.gz
cd iRedMail-1.6.8/
```

3. Lancer l'assistant d'installation :Bash

```
bash iRedMail.sh
```

4. **Réponses à l'assistant d'installation (Écrans bleus) :**
    - *Welcome :* Yes
    - *Default mail storage :* `/var/vmail`
    - *Web Server :* `Nginx`
    - *Backend :* Choisir `MariaDB` (Plus léger et parfaitement adapté pour notre architecture).

- *Domain name :* `sidsic.lan` (Attention : ne pas mettre srv-mail01 ici, juste le domaine).
- *Password for postmaster :* Renseigner un mot de passe fort (ex: `P@sswordMail123!`).
- *Optional components :* Cocher `Roundcubemail`, `SOGo`, `Fail2ban`.

5. Valider par `Y` et laisser le script travailler. À la fin, redémarrer le serveur (`reboot`).

---

## 3. Intégration à l'Active Directory (LDAP)

Conformément au cahier des charges, les agents ne doivent pas avoir un mot de passe supplémentaire à retenir. Nous allons configurer l'interface Webmail (Roundcube) pour qu'elle s'appuie sur l'annuaire du COD (`SRV-AD01`) pour vérifier les identifiants et récupérer le carnet d'adresses global.

1. Éditer le fichier de configuration principal de Roundcube :

   ```
   nano /opt/www/roundcubemail/config/config.inc.php
   ```

2. Ajouter et adapter le bloc de configuration LDAP suivant pour faire le pont avec Windows Server :PHP

   ```php
   $config['ldap_public']['sidsic_ad'] = array(
     'name'          => 'Annuaire Global COD',
     'hosts'         => array('192.168.1.10'),
     'port'          => 389,
     'use_tls'       => false,
     'ldap_version'  => 3,
     'user_specific' => false,
     'base_dn'       => 'DC=sidsic,DC=lan',
     'bind_dn'       => 'CN=Administrateur,CN=Users,DC=sidsic,DC=lan',
     'bind_pass'     => 'P@ssw0rd', // Mot de passe du compte de service A
   D
     'filter'        => '(&(objectClass=user)(objectCategory=person)(mail=
   *))',
     'search_fields' => array('mail', 'cn', 'sAMAccountName'),
     'name_field'    => 'cn',
     'email_field'   => 'mail',
     'surname_field' => 'sn',
     'firstname_field' => 'givenName',
     'scope'         => 'sub',
     'referrals'     => false,
   );
   ```

3. Créer manuellement la boîte mail locale correspondante à l'agent (ex: `agent01@sidsic.lan`) via le panneau d'administration web d'iRedMail

(`https://192.168.1.50/iredadmin`) afin de générer son espace de stockage `/var/vmail`.

---

## 4. Automatisation du Provisionnement (Script DevOps)

Pour pallier la séparation entre le backend MariaDB et l'Active Directory (architecture "Split Brain"), un script de synchronisation automatisé a été développé en Bash. Il interroge l'AD à intervalles réguliers et crée les nouvelles boîtes mail dans la base de données de manière transparente.

- **Création du script de synchronisation** (`/root/sync_ad_mail.sh`) :

```
#!/bin/bash
# 1. Récupération des emails des utilisateurs AD possédant une adresse
USERS_AD=$(ldapsearch -x -H ldap://192.168.1.10 -D "CN=Administrateur,C
N=Users,DC=sidsic,DC=lan" -w "P@ssw0rd" -b "DC=sidsic,DC=lan" "(&(objec
tClass=user)(objectCategory=person)(mail=*))" mail | grep "^mail:" | cu
t -d" " -f2)

for EMAIL in $USERS_AD; do
    USER_PART=$(echo $EMAIL | cut -d"@" -f1)

    # 2. Vérification de l'existence dans iRedMail (MariaDB)
    CHECK=$(mysql vmail -e "SELECT username FROM mailbox WHERE username
='$EMAIL';" -sN)

    if [ -z "$CHECK" ]; then
        # 3. Provisionnement automatique de la boîte mail
        mysql vmail -e "INSERT INTO mailbox (username, password, name,
domain, maildir, quota, active, created) VALUES ('$EMAIL', '{PLAIN}stor
ed_in_ad', '$USER_PART', 'sidsic.lan', 'sidsic.lan/$USER_PART/', 1024,
1, NOW());"

        # 4. Création de l'espace de stockage physique
        mkdir -p /var/vmail/vmail1/sidsic.lan/$USER_PART/Maildir
        chown -R vmail:vmail /var/vmail/vmail1/sidsic.lan/$USER_PART/
    fi
done
```

- **Planification (Crontab) :** Le script est exécuté automatiquement par le système via une tâche cron (`crontab -e`), assurant un provisionnement quasi-immédiat des nouveaux agents : `* * * * /root/sync_ad_mail.sh > /dev/null 2>&1`

## 5. Finalisation et Sécurisation (HTTPS)

Par défaut, iRedMail génère un certificat auto-signé. Comme pour les serveurs précédents, l'accès au Webmail est forcé en HTTPS pour garantir la confidentialité des échanges, particulièrement si des agents se connectent via le VPN.

- L'interface d'administration du serveur est accessible sur : **`https://192.168.1.50/iredadmin`**
- Le Webmail (Interface Utilisateur) est accessible sur : **`https://192.168.1.50/mail`**

---

## 6. Scénarios de Validation (Checklist de Recette)

Afin de garantir que le système de messagerie est pleinement opérationnel et prêt à relayer les futures alertes du système de supervision (Lot 6), les tests suivants ont été réalisés avec succès :

- ✅ **Test 1 : Accès Webmail et Carnet d'adresses AD**
  - *Action :* Connexion à l'interface Webmail (`/mail`) avec le compte `agent01@sidsic.lan`. Clic sur le bouton "Contacts".
  - *Résultat :* L'annuaire Active Directory du SIDSIC s'affiche. L'agent peut rechercher d'autres agents du COD sans avoir à connaître leurs adresses exactes.
- ✅ **Test 2 : Flux de messagerie interne (Envoi / Réception)**
  - *Action :* Depuis le compte `agent01`, rédaction d'un rapport de situation ("Main Courante eBrigade") envoyé à `admin01@sidsic.lan`.
  - *Résultat :* L'e-mail est distribué instantanément dans la boîte de réception de l'administrateur sans transiter par Internet (Routage 100% interne et sécurisé).
- ✅ **Test 3 : Relais SMTP (Préparation Supervision PRTG)**
  - *Action :* Un test de connexion SMTP sur le port 587 (STARTTLS) est simulé depuis le réseau LAN.
  - *Résultat :* Le serveur iRedMail accepte l'authentification et autorise le relayage. Le système est prêt à être utilisé par PRTG (Lot 6) pour l'envoi d'alertes automatisées aux administrateurs.

# 💻 LOT 6 - Déploiement du Portail Métier Collaboratif (eBrigade)

[ 🔙 Retour au Menu Livrable 2] | [ 🏠 Retour à l'accueil]

***Application Métier (eBrigade) : Hébergement Web Isolé en DMZ***

**Objectif Stratégique :** Le Centre Opérationnel Départemental s'appuie sur l'application métier eBrigade pour gérer le personnel, les interventions et générer des mains courantes informatisées en temps réel. Pour garantir la sécurité globale de l'infrastructure, cette application est hébergée sur une machine virtuelle Linux (Pile LAMP) placée dans une Zone Démilitarisée (DMZ). L'accès se fait exclusivement en HTTPS. Une politique de sécurité stricte (Pare-feu pfSense, pare-feu local UFW, et Fail2ban) est appliquée pour contrer les attaques web. Enfin, un "Mode Dégradé" est configuré pour permettre l'accès à l'application depuis Internet en cas d'évacuation physique du COD.

---

## 0. Plan d'Adressage de la Zone DMZ (LOT 6)

*Attention : Ce réseau est physiquement et logiquement isolé du LAN (`192.168.1.0/24`).*

| Hôte / Interface | Rôle | Réseau | Adresse IP |
|---|---|---|---|
| **VIP-DMZ (CARP)** | Passerelle Virtuelle DMZ | DMZ | **172.16.10.254/24** |
| **SA-PF01 (Master)** | Interface DMZ Physique | DMZ (vtnet4) | 172.16.10.252/24 |
| **SA-PF02 (Backup)** | Interface DMZ Physique | DMZ (vtnet4) | 172.16.10.253/24 |
| **SRV-WEB01** | Serveur Web eBrigade (LAMP) | DMZ | **172.16.10.10/24** |

---

## 1. Préparation de l'Infrastructure Réseau (Cluster pfSense)

Pour garantir l'isolation complète du serveur, une 5ème interface réseau a été provisionnée sur le cluster pfSense sous Proxmox.

### 1.1. Adressage et Haute Disponibilité (CARP)

1. Ajout de l'interface `vtnet4` sur les deux pare-feux, nommée **DMZ**.
2. Création d'une adresse virtuelle commune (VIP CARP) sur l'interface DMZ : `172.16.10.254/24` (avec un VHID différent de celui du LAN).

### 1.2. Règles de filtrage DMZ (Principe du Moindre Privilège)

Dans **Firewall > Rules > DMZ**, les flux sortants de la DMZ ont été strictement limités :

- **Pass :** `DMZ net` vers `192.168.1.10` sur le port **53 (DNS)**. *(Permet la résolution de noms via l'AD).*
- **Pass :** `DMZ net` vers `192.168.1.10` sur le port **389 (LDAP)**. *(Permet la future authentification sur l'annuaire).*

- **Pass :** `DMZ net` vers `Any` sur les ports **80/443 (HTTP/HTTPS)**. *(Permet les mises à jour du serveur)*.
- **Block :** `DMZ net` vers `LAN net` sur **Any**. *(Protège le réseau interne en cas de compromission du serveur web)*.

### 1.3. Règle de Routage Interne (Bypass Multi-WAN)

Puisque le réseau LAN est configuré pour envoyer tout son trafic vers Internet (Failover Multi-WAN du Lot 1), il a fallu créer une exception de routage.

Dans **Firewall > Rules > LAN**, ajout d'une règle placée **tout en haut** de la liste :

- **Pass :** `LAN subnets` vers `DMZ net` sur **Any** (Gateway par défaut). *(Force le trafic à destination de la DMZ à rester en interne)*.

---

## 2. Déploiement du Serveur Web (Pile LAMP)

1. Création d'une machine virtuelle Debian vierge connectée au commutateur virtuel de la DMZ sur l'hyperviseur Proxmox.

2. Configuration de l'IP statique dans `/etc/network/interfaces` et du DNS dans `/etc/resolv.conf`.

3. Installation du socle technique (Apache2, MariaDB, PHP 8.2) :Bash

```
apt update && apt upgrade -y  apt install apache2 mariadb-server php libapache2-mod-php php-mysql php-xml php-mbstring php-curl php-zip php-gd php-intl unzip wget -y
```

---

## 3. Sécurisation et Base de Données

### 3.1. Durcissement SQL et Cloisonnement

1. Sécurisation globale du moteur de base de données via `mysql_secure_installation` (désactivation du login root à distance, suppression des utilisateurs anonymes).

2. Création d'une base de données dédiée et d'un utilisateur à droits restreints pour eBrigade :SQL

```
CREATE DATABASE ebrigade_db CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;  CREATE USER 'user_ebrigade'@'localhost' IDENTIFIED BY 'P@sswordWeb123!';  GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'user_ebrigade'@'localhost';  FLUSH PRIVILEGES;
```

### 3.2. Sécurité Locale (ANSSI : UFW & Fail2ban)

Mise en place d'une "Défense en profondeur" autonome sur la machine Linux :

1. Installation : `apt install ufw fail2ban -y`
2. Configuration du pare-feu applicatif (fermeture de tous les ports non essentiels) :Bash

   ```
   ufw default deny incoming  ufw default allow outgoing  ufw allow ssh
   ufw allow http  ufw allow https  ufw enable
   ```

3. Activation du service de bannissement IP `fail2ban` pour contrer les attaques par force brute.

---

## 4. Installation de l'Application eBrigade (HTTPS)

1. Téléchargement et extraction de la dernière version stable officielle :Bash

   ```
   cd /tmp  wget
   https://github.com/GIPdA/libreBrigade/releases/download/v5.3.2/ebrigade
   -5.3.2.zip -O ebrigade.zip  unzip ebrigade.zip  mv ebrigade-5.3.2
   /var/www/html/ebrigade
   ```

2. Attribution des droits d'écriture au service Web :Bash

   ```
   chown -R www-data:www-data /var/www/html/ebrigade  chmod -R 755
   /var/www/html/ebrigade
   ```

3. Activation du chiffrement SSL et configuration des VirtualHosts (`000-default.conf` et `default-ssl.conf`) pour faire pointer la racine Web sur le dossier `/ebrigade`. Redémarrage d'Apache.

---

## 5. Mise en Production : Modes Nominal et Dégradé

### 5.1. Mode Nominal (Accès Interne)

Les utilisateurs connectés au réseau LAN du COD accèdent à l'application via l'URL sécurisée : **`https://172.16.10.10`**. L'assistant d'installation initial a permis de lier l'application à la base de données MariaDB et de générer le compte Super Administrateur local.

### 5.2. Mode Dégradé (Accès Externe via NAT)

Afin de permettre la continuité de commandement depuis Internet (évacuation du COD), une règle de redirection de ports (Port Forwarding) a été déployée sur pfSense.

- **Firewall > NAT > Port Forward :**
  - Interface : `WAN`
  - Protocole : `TCP`
  - Port destination : `443` (`HTTPS`)
  - Redirection vers (Target IP) : `172.16.10.10` sur le port `443`
- L'application est ainsi accessible depuis l'extérieur en utilisant l'adresse IP publique (WAN) du pare-feu pfSense.

---

# 📈 LOT 7 - Supervision : Métrologie Réseau et Alertes Proactives (PRTG)

[ ⬅️ Retour au Menu Livrable 2] | [ 🏠 Retour à l'accueil]

***Supervision : Métrologie Réseau et Alertes Proactives***

> **Objectif Stratégique :** Afin de garantir la continuité des opérations du Centre Opérationnel Départemental (COD), ce lot déploie une solution de supervision centralisée basée sur **PRTG Network Monitor**. Conformément au cahier des charges, l'outil évalue l'incidence de la VoIP sur le réseau via une métrologie stricte (gigue, latence, pertes de paquets). Le système surveille la disponibilité des équipements critiques (routeurs, serveurs) et intègre un dispositif d'alerte proactive par e-mail, routé localement via le serveur de messagerie interne (iRedMaildu Lot 5), assurant ainsi une diffusion des alertes sans aucune dépendance à Internet.

---

## 0. Plan d'Adressage du Serveur de Supervision (LOT 7)

| Hôte | Rôle | OS | Réseau (VLAN LAN) | Passerelle |
|---|---|---|---|---|
| **SRV-PRTG01** | Serveur de Supervision (PRTG) | **Windows Server 2022** | **192.168.1.60/24** | 192.168.1.254 (VIP CARP) |

---

## 1. Préparation du Serveur et Installation de PRTG

L'installation de PRTG s'effectue sur un environnement Windows Server. L'outil intègre nativement son propre serveur web et sa propre base de données propriétaire, ce qui réduit considérablement les efforts de maintenance et garantit une stabilité optimale en temps de crise.

### 1.1. Configuration de l'Adressage Statique et DNS

Afin que le serveur PRTG puisse interroger l'ensemble des équipements et résoudre leurs noms, il doit d'abord être correctement inséré dans le domaine.

1. Se connecter en `Administrateur` sur la console de la VM Windows Server 2022.
2. Ouvrir les propriétés de la carte réseau (`ncpa.cpl`).
3. Désactiver l'IPv6 (pour éviter le bruit réseau) et configurer l'IPv4 :
   - **Adresse IP** : `192.168.1.60`
   - **Masque de sous-réseau** : `255.255.255.0`
   - **Passerelle par défaut** : `192.168.1.254`
   - **Serveur DNS préféré** : `192.168.1.10` (SRV-AD01)
4. Joindre le serveur au domaine `sidsic.lan` et redémarrer la machine.

### 1.2. Déploiement de PRTG Network Monitor

1. Télécharger l'installateur officiel de **PRTG Network Monitor** (Licence Freeware, limitée à 100 capteurs, suffisante pour le périmètre du COD).
2. Lancer l'exécutable et suivre l'assistant d'installation (les paramètres par défaut pour le serveur web et la base de données intégrée sont recommandés).
3. À l'issue de l'installation, un navigateur s'ouvre automatiquement sur l'URL locale `https://127.0.0.1`.
4. Se connecter avec les identifiants par défaut (`prtgadmin` / `prtgadmin`) et modifier immédiatement le mot de passe dans les paramètres de compte pour des raisons de sécurité.

---

## 2. Découverte et Monitoring de Base (SNMP / WMI)

Pour offrir une vue d'ensemble (Dashboard) claire et pertinente en salle de crise, PRTG interroge les équipements cibles à l'aide de protocoles standards. L'ajout des capteurs a été réalisé manuellement (sans auto-découverte globale) afin de maîtriser la consommation des ressources et de ne cibler que les métriques critiques (respect de la limite de 100 capteurs de la licence Freeware).

### 2.1. Supervision du Pare-feu (pfSense) via SNMP

1. Sur le pare-feu `SA-PF01`, activer le service SNMPv2c dans **Services** > **SNMP**.
2. Renseigner le champ **Read Community String** avec une communauté dédiée en lecture seule (ex: `Public_COD`) et cibler uniquement l'interface `LAN` pour la sécurité.
3. Dans l'interface PRTG, aller dans **Équipements** > **Ajouter un équipement**.
4. Dans l'arborescence, sélectionner le groupe cible **Infrastructure du réseau** et cliquer sur OK.
5. Saisir le nom de l'équipement (ex: `pfSense - Pare-feu`) et son adresse IP (`192.168.1.254`).

6. Dans la section *Identification pour les systèmes SNMP*, décocher l'héritage, forcer la version **SNMP v2c**, et renseigner la chaîne de communauté correspondante (`Public_COD`).
7. **Important :** Dans la section *Détection du réseau*, sélectionner **Aucune détection automatique** pour éviter l'importation massive de capteurs non pertinents. Valider.
8. Sur la page de l'équipement, cliquer sur **Ajouter un capteur** et ajouter un par un les sondes critiques :
    - **Ping**
    - **Trafic SNMP** (en sélectionnant les interfaces `vtnet0` pour le WAN et `vtnet1` pour le LAN).
    - **Charge CPU SNMP**.

## 2.2. Supervision de l'Active Directory via WMI

1. Dans l'interface PRTG, aller dans **Équipements** > **Ajouter un équipement**.
2. Dans l'arborescence, sélectionner le dossier **Windows** puis **Serveurs** et cliquer sur OK.
3. Saisir le nom de l'équipement (ex: `SRV-AD01 - Contrôleur de Domaine`) et son adresse IP (`192.168.1.10`).
4. Descendre jusqu'à la section *Informations d'identification pour les systèmes Windows*.
5. Décocher la case d'héritage et remplir les champs avec un compte à privilèges :
    - **Domaine :** `sidsic.lan`
    - **Utilisateur :** `Administrateur`
    - **Mot de passe :** [Mot de passe de l'administrateur AD]
6. Dans la section *Détection du réseau*, sélectionner **Aucune détection automatique** et valider.
7. Une fois l'équipement créé, cliquer sur **Ajouter un capteur** et rechercher les capteurs WMI spécifiques pour valider la santé du contrôleur de domaine :
    - **Espace libre de multiples disques (WMI)**
    - **Mémoire**
    - **Service Windows :** Sélectionner le service **Serveur DNS** pour s'assurer de la résolution des noms.
    - **Service Windows :** Sélectionner le service **Services de domaine Active Directory** (NTDS) pour s'assurer de la disponibilité de l'annuaire.

---

## 3. Métrologie VoIP (QoS, Jitter, Latence)

C'est le cœur de ce lot : garantir que le réseau LAN est capable de supporter les communications téléphoniques du COD sans dégradation (voix hachée, écho). La VoIP utilisant le protocole UDP, elle est extrêmement sensible aux variations de délai.

### 3.1. Déclaration du Serveur et Ajout des Capteurs de Métrologie

1. Dans l'interface PRTG, aller dans **Équipements** > **Ajouter un équipement**.
2. Dans l'arborescence, sélectionner le dossier **`Linux / macOS / Unix`** (puisque FreePBX tourne sous Debian 12) et cliquer sur OK.
3. Saisir le nom de l'équipement (ex: `SRV-VOIP01 - Téléphonie IPBX`) et son adresse IPv4 : `192.168.1.40`.
4. Dans la section *Détection du réseau*, sélectionner **Aucune détection automatique** et valider pour créer l'équipement.
5. Sur la page de ce nouvel équipement, cliquer sur **Ajouter un capteur** et ajouter les deux sondes suivantes :
    - **Ping** : Ce capteur standard permet de mesurer en temps réel le **Temps de réponse (Latence)** et le pourcentage de **Perte de paquets** (qui doit rester à 0%).
    - **Gigue du Ping (Ping Jitter)** : Ce capteur spécialisé envoie une rafale de paquets UDP/ICMP pour mesurer l'instabilité du réseau.
6. **Validation :** Le tableau de bord affiche une Gigue (Jitter) mesurée à **~0,73 ms**, ce qui est très largement inférieur au seuil critique des 30 ms. Cela prouve que l'infrastructure réseau garantit une communication vocale claire et sans coupure en situation de crise.

---

## 4. Dispositif d'Alerte par E-mail (Lien avec le Lot 5)

En cas de défaillance matérielle ou réseau, les administrateurs doivent être avertis de manière proactive, avant même que les utilisateurs ne signalent la panne. Ce système s'appuie sur le relais SMTP interne mis en place au Lot 5.

### 4.1. Paramétrage de la passerelle SMTP dans PRTG

1. Aller dans **Configuration** > **Administration du système** > **Diffusion des messages**.
2. Dans la section *Distribution SMTP*, sélectionner : **Utiliser un serveur SMTP relais**.
3. Remplir les informations de connexion vers notre serveur iRedMail:
    - **Nom de l'expéditeur** : `Supervision PRTG`
    - **Adresse e-mail de l'expéditeur** : `supervision@sidsic.lan`
    - **Serveur SMTP** : `192.168.1.50` (SRV-MAIL01)
    - **Port SMTP** : `587`
    - **Sécurité** : `STARTTLS`
    - **Authentification** : Utiliser un compte fonctionnel valide de iRedMail (ex: `testlocal@sidsic.lan` et son mot de passe (P@ssw0rd iRedMail)).
4. Cliquer sur **Sauvegarder et tester**. PRTG enverra un mail de validation confirmant que l'interconnexion avec le Lot 5 est opérationnelle.

### 4.2. Création des Déclencheurs (Triggers)

1. Aller dans le menu principal Configuration > Paramètres du compte > Modèles de notification et créer un nouveau modèle nommé Alerte Panne Critique COD.
2. Définir l'action sur **Envoyer un e-mail** vers l'adresse de l'administrateur système.
3. Se rendre sur un équipement critique (ex: Le capteur *Ping* du serveur eBrigade en DMZ).
4. Cliquer sur l'onglet **Déclencheurs de notification**.
5. Ajouter un déclencheur d'état : *Lorsque le capteur est à l'état [En Panne] pendant au moins [60] secondes, exécuter [Alerte Panne Critique COD]*.

---

## 5. Scénarios de Validation (Checklist de Recette)

Pour s'assurer du respect strict du cahier des charges, les tests de métrologie et d'alerting suivants ont été exécutés :

- ✅ **Test 1 : Métrologie de la VoIP en temps réel**
  - *Action :* Vérification du capteur QoS/Jitter sur l'équipement SRV-VOIP01 dans l'interface de PRTG.
  - *Résultat :* Le graphique génère des données stables. La gigue (Jitter) est mesurée sous le seuil critique des 30ms, confirmant que la configuration des commutateurs (VLAN) et du routage n'impacte pas le trafic audio en clair ou chiffré.
- ✅ **Test 2 : Simulation de panne et Alerting SMTP (Proactivité)**
  - *Action :* Sur le serveur eBrigade (SRV-WEB01), le service Apache2 est arrêté volontairement via la commande `systemctl stop apache2` pour simuler un crash applicatif.
  - *Résultat :* Au bout d'une minute (cycle de scan), PRTG détecte que le port HTTP/HTTPS ne répond plus. Le capteur passe au rouge (Down). Le déclencheur s'active et un e-mail contenant le diagnostic détaillé est instantanément reçu dans la boîte de réception Webmail iRedMail de l'administrateur.