FICHE D'ACTIVITÉ : Mise en place d'un pare-feu OPNsense et configuration d'un tunnel IPsec site-to-site

Contexte de la mission

L'entreprise **DUALYA** souhaite interconnecter ses deux sites distants, **Paris** et **Arcachon**, via un tunnel **IPsec**. Cette interconnexion doit permettre un **échange sécurisé** des données entre les réseaux internes tout en garantissant un **haut niveau de sécurité** et une **continuité de service**.

Le choix s'est porté sur **OPNsense** comme pare-feu, car il offre une **interface web intuitive**, des **fonctionnalités avancées de sécurité** et une **grande flexibilité** en matière de gestion des règles de filtrage et de VPN.

Table des matières

Veille effectuée avant-projet / Étude et choix de la solution

Avant de choisir **OPNsense** pour cette interconnexion, une étude a été menée sur plusieurs solutions de pare-feu et de VPN :

- **PFsense** : Très proche d'OPNsense, mais avec une communauté moins active.
- **MikroTik** : Performant, mais plus complexe à configurer.
- **Fortinet / Cisco ASA** : Solutions robustes, mais plus coûteuses et nécessitant des licences supplémentaires.

Le choix d'OPNsense a été fait pour les raisons suivantes :

- **Gratuit et open-source**, avec une communauté active.
- **Interface web conviviale**, facilitant l'administration.
- **Support natif d'IPsec**, sans nécessiter de modules additionnels.
- **Mises à jour régulières**, garantissant la sécurité et la compatibilité.

Étapes du projet / Planning / Ordonnancement / Collaboration

Étapes principales :

1. **Installation et configuration d'OPNsense** sur les deux sites.
2. **Configuration des interfaces réseau** sur chaque site.
3. **Mise en place du tunnel IPsec** en respectant les bonnes pratiques de sécurité.
4. **Application des règles de pare-feu** pour filtrer le trafic VPN.
5. **Tests et validation de la connectivité**.
6. **Documentation et formation** sur la maintenance de la solution.

Liste du matériel / Inventaire

Matériel utilisé :

- **Deux machines dédiées** pour OPNsense (une par site).
- **Connexions Internet** (une par site, avec IP publique).
- **Switchs et routeurs** pour la gestion du réseau local.

Adressage IP :

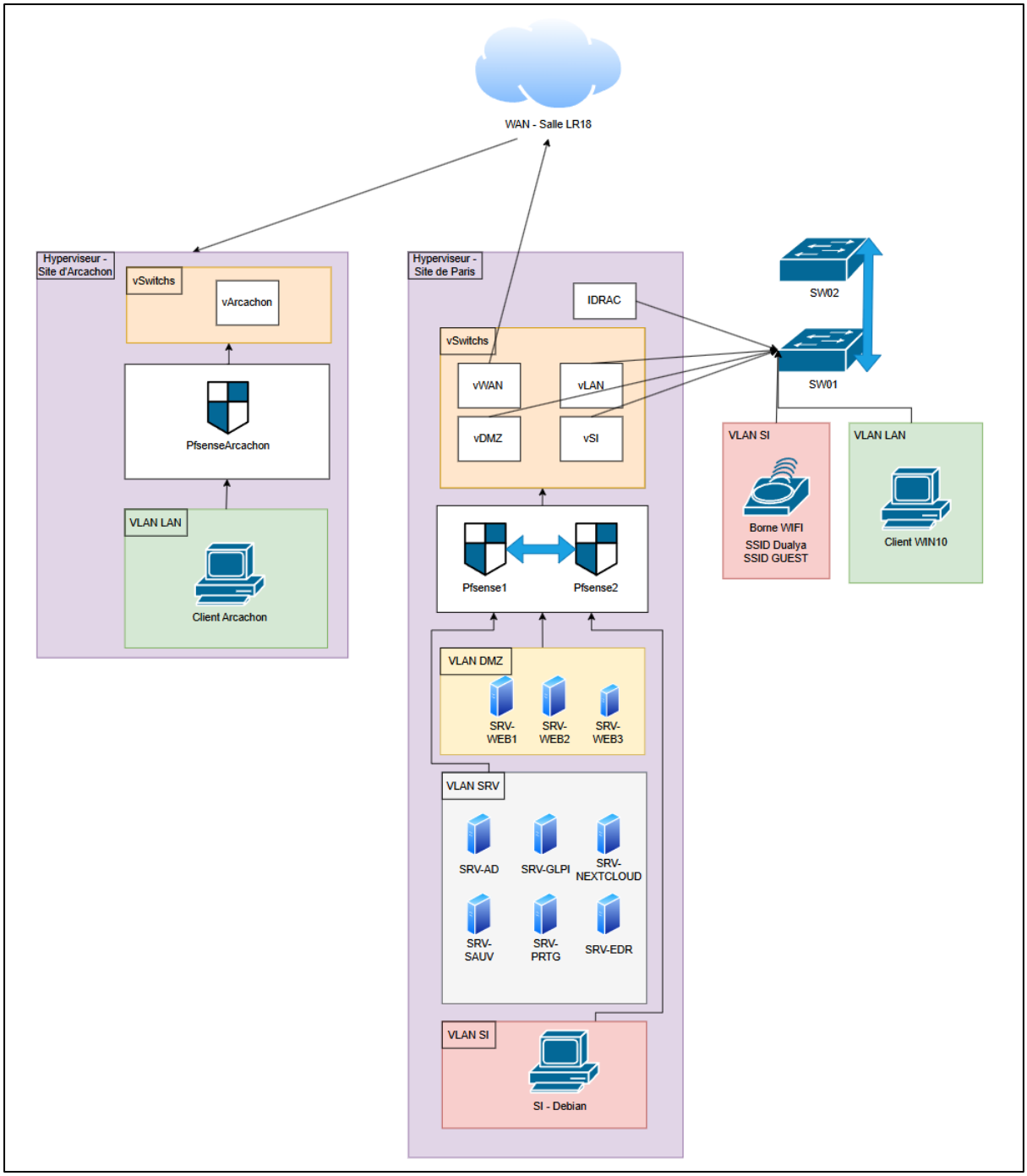
Site Paris

- WAN : **10.0.85.210/24**
- LAN : **10.85.210.60/26**

Site Arcachon

- WAN : **10.0.45.210/24**
- LAN : **10.45.210.60/26**

Topologie logique de l'infrastructure



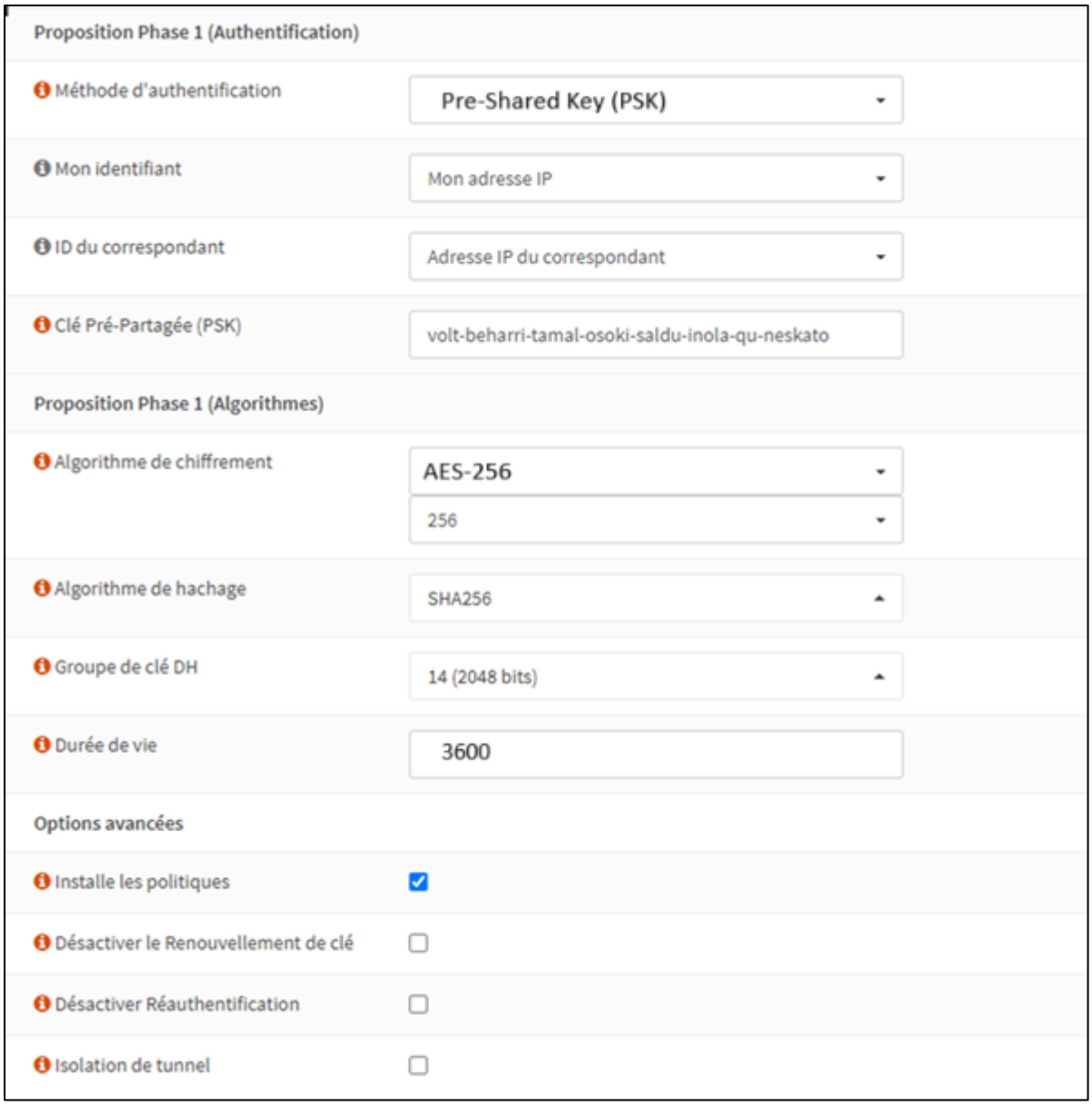
Déroulement de la mission en lien avec les compétences

A. Installation et configuration initiale d'OPNsense

1. **Installation d'OPNsense** sur chaque machine dédiée.
2. **Configuration des interfaces réseau (WAN/LAN)**.
3. **Mise à jour des paquets** et activation des modules de sécurité.

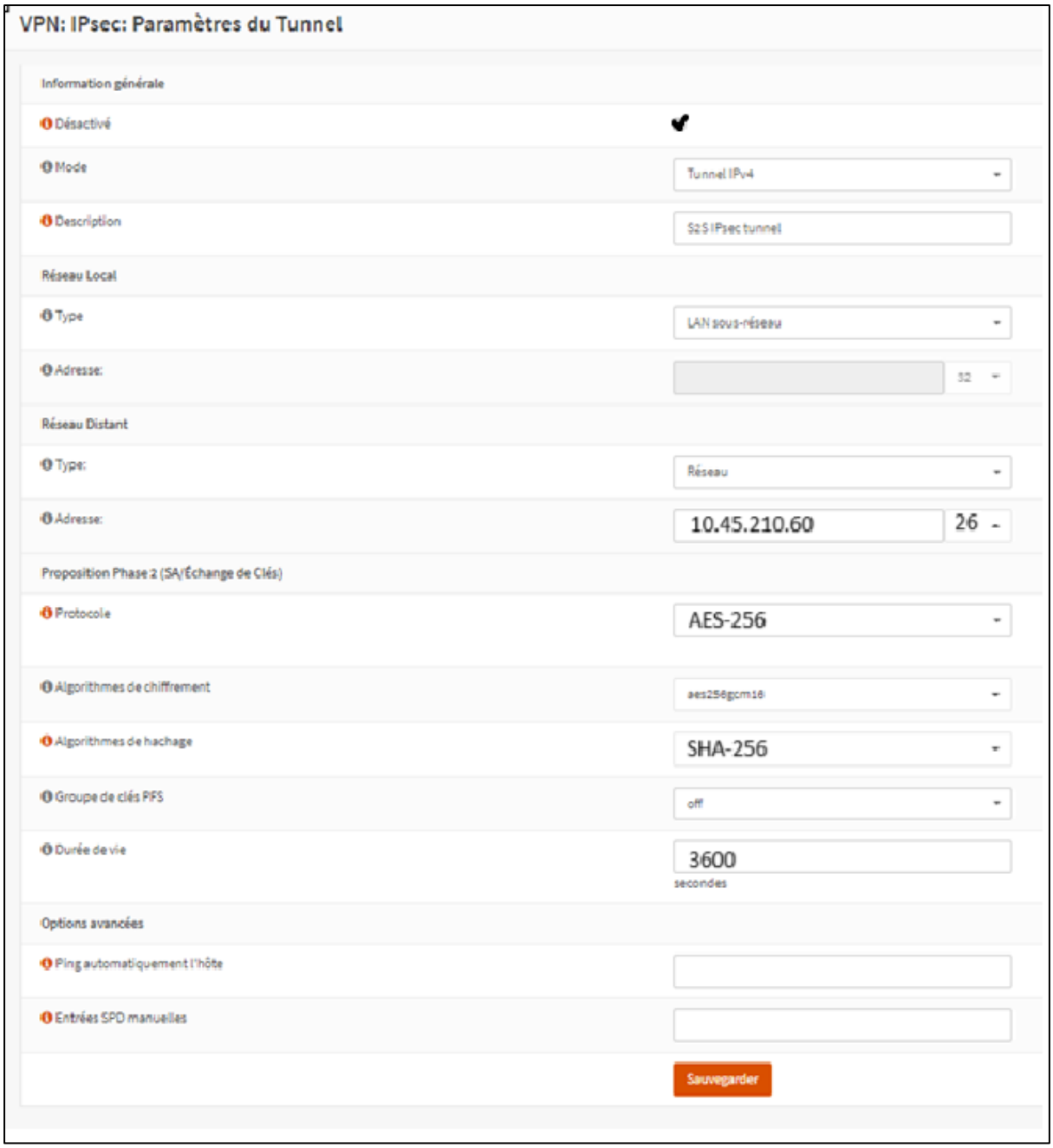
B. Configuration du tunnel IPsec

1. **Accès à l'interface Web** d'OPNsense : *VPN > IPsec > Phase 1*.



2. **Configuration de la Phase 1 (Authentification)** :
    - Mode : **Main**.
    - Authentification : **Pre-Shared Key (PSK)**.
    - Algorithmes de chiffrement : **AES-256, SHA-256, DH Group 14**.
    - Durée de vie : **3600 secondes**.

3. **Configuration de la Phase 2 (Chiffrement du trafic)** :
    - Réseau local Paris : **10.85.210.60/26**.
    - Réseau local Arcachon : **10.45.210.60/26**.
    - Algorithmes : **ESP, AES-256, SHA-256**.
    - Mode : **Tunnel**.



4. **Ajout des règles de pare-feu** :
    - Autorisation du trafic **IPsec** sur l'interface WAN.
    - Autorisation du trafic entre les réseaux internes sur IPsec.
5. **Vérification et activation** :
    - **Lancement du tunnel**.
    - **Vérification des logs** pour identifier d'éventuelles erreurs.

Conclusion

Cette activité m'a permis d'approfondir mes compétences en **sécurisation des réseaux** et en **administration de pare-feu**. La mise en place d'un tunnel IPsec requiert une **bonne maîtrise des protocoles de chiffrement** et des **règles de pare-feu**. Les tests et analyses des logs ont été essentiels pour garantir une connectivité stable et sécurisée.

J'ai rencontré des défis techniques, notamment des problèmes de routage et de compatibilité des algorithmes, mais ces obstacles ont renforcé mes capacités de **résolution de problèmes** et d'**optimisation réseau**. Cette expérience me sera précieuse pour la gestion future d'infrastructures sécurisées.