

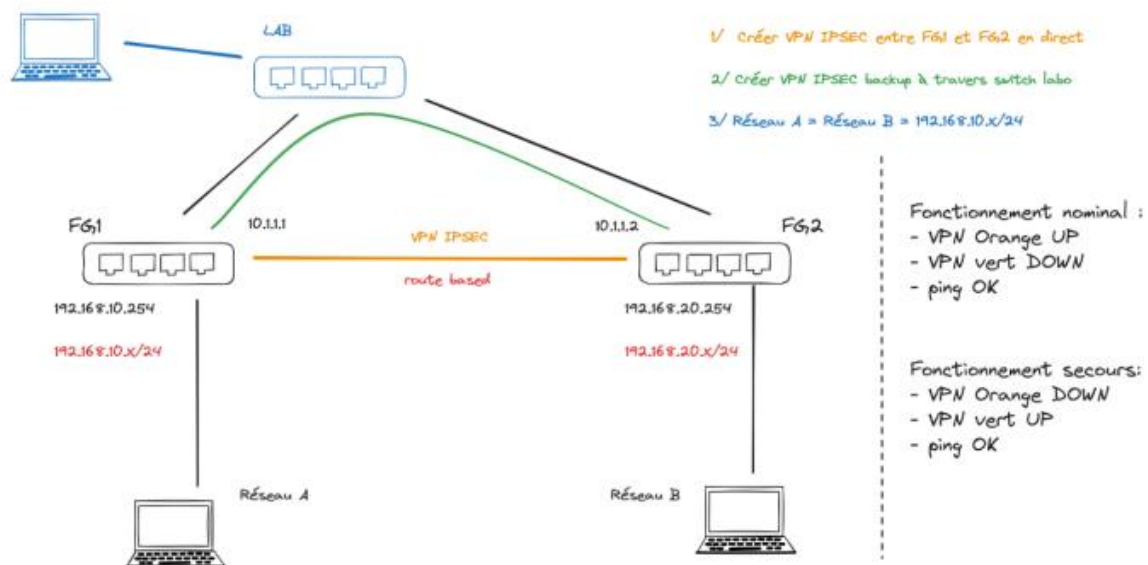
# Solution de Sécurisation Réseau avec FortiGate

Date : Février 2025

## Introduction

Dans le cadre de mon stage chez **CYKLAD**, j'ai eu l'opportunité de travailler sur la sécurisation des infrastructures réseau via la configuration d'un **firewall FortiGate**. L'objectif était de garantir une protection optimale des échanges de données en mettant en place des solutions adaptées aux besoins des entreprises, notamment en matière de contrôle du trafic et de connectivité sécurisée à distance.

## Objectif du Projet



Ce projet visait à **déployer et configurer un firewall FortiGate** afin de :

- **Sécuriser l'infrastructure réseau** en définissant des politiques de sécurité strictes.
- **Gérer la segmentation du réseau** grâce à la configuration des interfaces et des routes.
- **Mettre en place des connexions VPN sécurisées** (IPsec et SSL) pour garantir l'accès à distance aux ressources.

## Solution Développée

### 1. Configuration de Base du Firewall

#### Installation et Paramétrage Initial

- Déploiement et configuration d'un firewall **FortiGate** pour sécuriser l'infrastructure.
- **Segmentation réseau** : configuration des interfaces et attribution d'adresses IP statiques.
- **Mise en place des routes** pour assurer la communication entre les différents sous-réseaux.

#### 💡 Exemple de configuration :

- **Interconnexion (LAN1)** → 10.1.1.1
- **Réseau "labs" (LAN2)** → 10.10.15.41
- **Réseau sécurisé (LAN3)** → 192.168.10.254

### 2. Mise en Place d'un VPN IPsec

#### Présentation du VPN IPsec

Un VPN (Virtual Private Network) **IPsec** permet d'établir un tunnel chiffré entre deux réseaux distants, garantissant la confidentialité et l'intégrité des données échangées.

#### Avantages du VPN IPsec :

- ✓ **Chiffrement des données** : protection contre les interceptions.
- ✓ **Authentification renforcée** : vérification des appareils autorisés.
- ✓ **Protection contre les attaques** : utilisation de numéros de séquence pour éviter les attaques de replay.

#### 💡 Cas d'utilisation chez CYKLAD :

- Connexion **inter-sites** pour permettre la communication entre différents bureaux.
- Interconnexion **de firewalls** pour assurer la redondance et la continuité des services.

### 3. Déploiement du VPN SSL

#### Pourquoi un VPN SSL ?

Le VPN **SSL** est essentiel pour permettre un **accès sécurisé au réseau de l'entreprise** aux employés travaillant à distance.

## Fonctionnalités mises en place :

- ✅ Portails d'accès sécurisé.
- ✅ Authentification des utilisateurs pour restreindre les accès.
- ✅ Définition de **règles de sécurité** strictes pour éviter toute intrusion.

## 💡 Cas d'utilisation chez CYKLAD :

- **Télétravail sécurisé** : connexion aux ressources internes de l'entreprise.
- **Administration à distance** des firewalls FortiGate des clients.

---

## Compétences, Défis et Impact

### Compétences et Défis

La mise en place de ces solutions m'a permis de renforcer mes compétences en :

- **Sécurisation des infrastructures réseau** (Firewall, VPN).
- **Configuration avancée de FortiGate** et des politiques de sécurité.
- **Gestion des accès et authentification des utilisateurs.**

Les principaux défis rencontrés :

- ⚠️ **Configuration des interfaces et des VLANs** pour la segmentation réseau.
- ⚠️ **Gestion des règles de pare-feu** pour filtrer le trafic sans bloquer les services essentiels.
- ⚠️ **Intégration des VPNs** et gestion des certificats de sécurité.

### Impact et Conclusion

L'implémentation du firewall FortiGate et des VPNs a **renforcé la sécurité des réseaux d'entreprise**, en garantissant :

- ✅ Un **contrôle strict du trafic** grâce aux règles de pare-feu.
- ✅ Une **connexion sécurisée pour les employés à distance** via VPN.
- ✅ Une **meilleure gestion des ressources réseau** et des accès utilisateurs.

### Perspectives d'Évolution

Les prochaines améliorations envisagées incluent :

- 🚀 **Automatisation des règles de sécurité** via des scripts et des API Fortinet.
- 🚀 **Mise en place d'un monitoring avancé** avec des outils SIEM.
- 🚀 **Intégration de solutions Zero Trust** pour encore plus de sécurité.