AYYADI Aymane

BTS SIO SISR

Livrable 1

Cahier des charges

PROJET
SÉCURITÉ CIVILE

Table de matière :

I. Rappel des besoins et objectifs

Le projet consiste à concevoir et déployer une infrastructure réseau sécurisée, redondée et supervisée.

L'architecture repose sur la mise en place de deux pare-feux pfSense configurés en haute disponibilité, permettant d'assurer la continuité de service en cas de panne.

Une zone DMZ est mise en place afin d'isoler les services exposés, notamment un serveur de messagerie.

Un accès distant sécurisé est assuré grâce à un VPN OpenVPN de type Road Warrior.

L'infrastructure comprend également :
- Deux contrôleurs de domaine Active Directory sous Windows Server 2022 (redondance)
- Un serveur de téléphonie IP (Asterisk)
- Un serveur de supervision (PRTG)
- Un serveur de messagerie (Modoboa)

Trois postes clients sont déployés :
- Un client LAN pour les tests utilisateurs
- Un client en DMZ pour les tests d'accès
- Un client distant via VPN OpenVPN

Objectifs :
- Assurer la haute disponibilité des services
- Garantir la sécurité du réseau
- Permettre un accès distant sécurisé
- Superviser l'ensemble de l'infrastructure

II. Solutions

A. Étude des solutions (100% fidèle à ton projet)

Plusieurs solutions techniques ont été étudiées afin de répondre aux besoins du projet.

Pare-feu :

- Solution retenue : pfSense
Permet la gestion du réseau, la mise en place d'une DMZ, du NAT et du VPN.

VPN :
- Solution retenue : OpenVPN (Road Warrior)
Permet un accès distant sécurisé pour les utilisateurs.

Active Directory :
- Solution retenue : Windows Server 2022
Deux serveurs sont déployés pour assurer la redondance (principal + secondaire).

Messagerie :
- Solution retenue : Modoboa (Debian)
Solution open-source permettant la gestion des emails (SMTP, IMAP, Webmail).

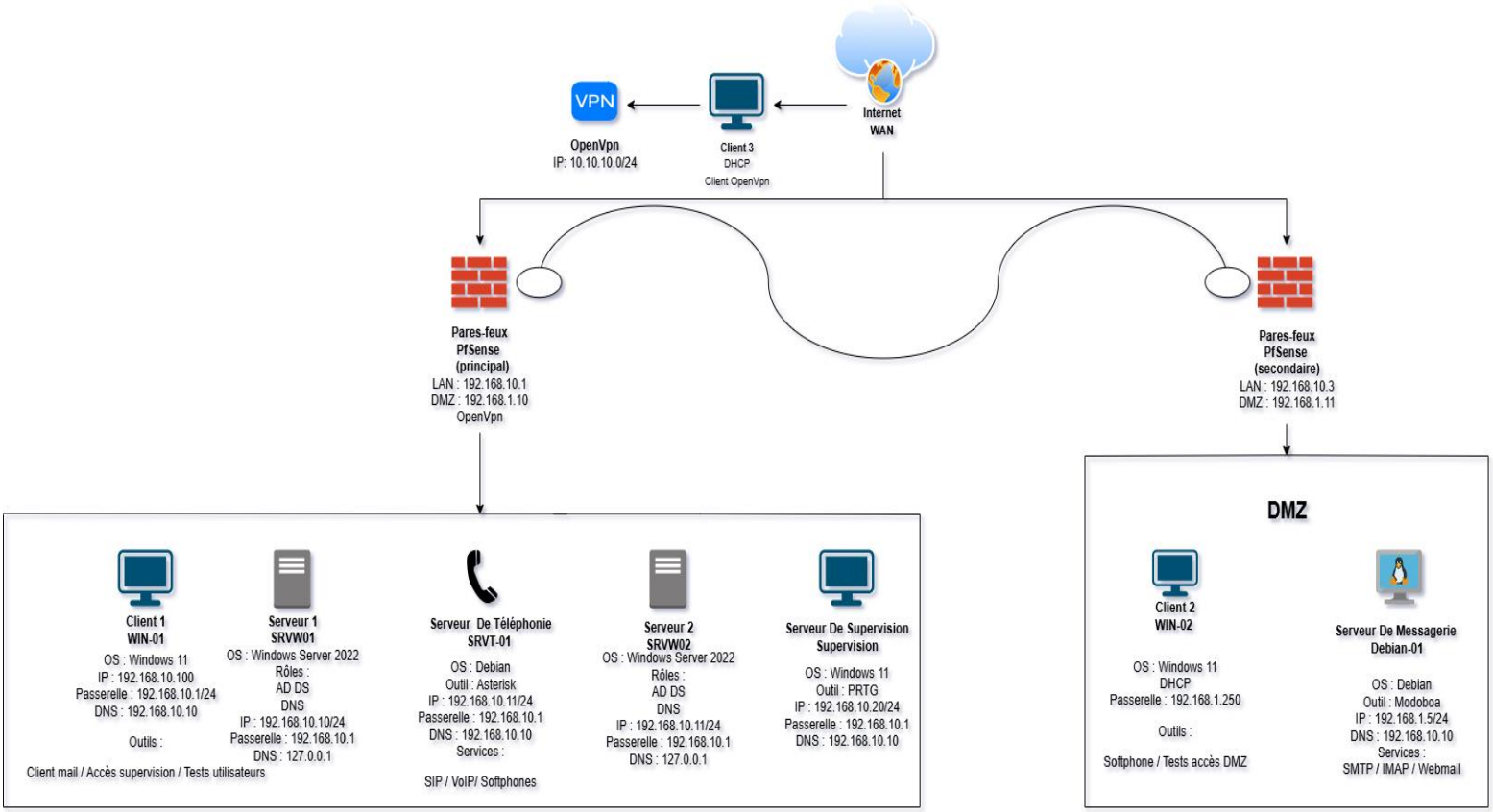
Téléphonie :
- Solution retenue : Asterisk (Debian)
Permet la mise en place d'un système VoIP avec softphones.

Supervision :
- Solution retenue : PRTG (Windows)
Permet de surveiller les équipements et services réseau en temps réel.

B. Tableau comparatif

Composant	Solution choisie	Justification
Pare-feu	2 pfSense	Open-source, fiable, haute disponibilité
VPN	OpenVPN	Accès distant sécurisé
Active Directory	2 serveurs Windows 2022	Redondance des services
Messagerie	Modoboa	Open-source, solution complète
Téléphonie	Asterisk	Flexible, VoIP
Supervision	PRTG	Interface simple, supervision temps réel

III. Schéma réseau



Le réseau est segmenté en deux zones :

- Réseau LAN :
Contient les serveurs internes :
- Deux contrôleurs de domaine Active Directory
- Un serveur de téléphonie (Asterisk)
- Un serveur de supervision (PRTG)
- Un client de test (Windows 11)

- DMZ :
Contient :
- Un serveur de messagerie (Modoboa sous Debian)
- Un client de test DMZ

Un accès distant est mis en place via un VPN OpenVPN permettant à un client externe d'accéder au réseau de manière sécurisée.

Cette architecture garantit :
- La séparation des services

- La sécurité du réseau
- La haute disponibilité

IV. Budget

Catégorie	Montant (€)	Explication
Matériel	5 000	Serveurs (virtualisés ou physiques)
Réseau	1 000	Équipements réseau (pfSense)
Logiciels	500	Licence PRTG
Open-source	0	pfSense, Asterisk, Modoboa
Main-d'œuvre	1 500	Installation et configuration
TOTAL	8 000	Budget global du projet

V. Sommaire

◈ DMZ (Demilitarized Zone) :
Zone réseau isolée entre le réseau interne et Internet, permettant d'héberger des services accessibles depuis l'extérieur tout en protégeant le réseau interne.

◈ Supervision :
Ensemble des outils et techniques permettant de surveiller l'état des équipements, des serveurs et des services d'un réseau en temps réel (alertes, performances, disponibilité).

◈ OpenVPN :
Solution de VPN open-source permettant de créer un tunnel sécurisé entre un utilisateur distant et un réseau local via Internet.

◈ AD DS (Active Directory Domain Services) :
Service d'annuaire de Microsoft permettant de gérer les utilisateurs, ordinateurs et ressources du réseau de manière centralisée.

◈ DNS (Domain Name System) :
Service permettant de traduire les noms de domaine en adresses IP pour faciliter la communication entre les machines.

◈ Asterisk :
Solution open-source de téléphonie IP permettant de gérer les appels VoIP, les extensions et les communications internes.

◈ PRTG :
Outil de supervision réseau permettant de surveiller les performances, les services et les équipements informatiques en temps réel.

◈ Pare-feu (pfSense) :
Système de sécurité réseau permettant de filtrer le trafic entrant et sortant afin de protéger l'infrastructure contre les accès non autorisés.

◈ VPN (Virtual Private Network) :
Réseau privé virtuel permettant de connecter des utilisateurs ou des sites distants de manière