Cahier des Charges pour l'Indépendance Informatique

1. Introduction

1.1 Objectif du document

Définir le cadre et les spécifications pour le projet d'indépendance informatique du client, incluant la séparation du réseau du lycée, le renouvellement du parc informatique, l'installation d'une nouvelle infrastructure serveur avec firewall, et l'établissement d'une politique de sauvegarde robuste.

1.2 Périmètre du projet

Ce projet comprend le désengagement du système informatique actuel du lycée, la mise en place de nouveaux serveurs et d'un firewall, la mise en œuvre de politiques de sécurité et de sauvegarde, et le renouvellement des équipements informatiques. Tout cela infogéré par un prestataire externe

2. Contexte et Justification

2.1 Contexte actuel

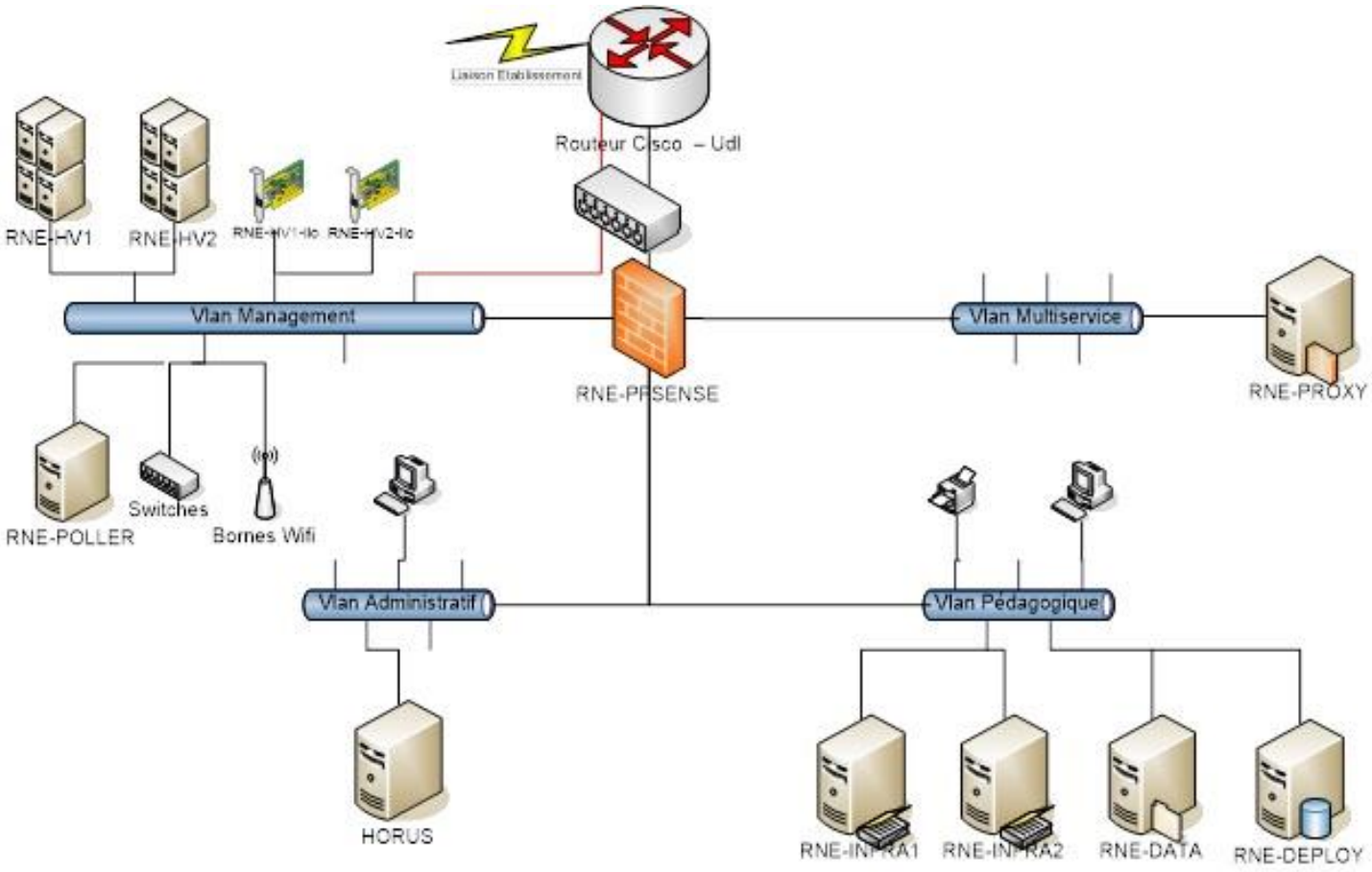
Le CFA est actuellement intégré au système informatique du lycée et dépend de ce dernier pour son fonctionnement informatique, sans connaissance approfondie de l'architecture ou de la gestion de son système informatique.

L'intégralité du parc était gérée par le Grand-Est.

Le CFA possède 350 élèves. 50 postes pédagogiques et 20 pcs administratifs.

Le logiciel SIECLE permet l'export d'un fichier contenant la liste détaillée des élèves et leur classe, ainsi que les professeurs et formateurs.

Voici le schéma du réseau existant :



2.2 Objectifs

Se détacher du réseau du lycée et devenir autonome en termes de gestion informatique, avec une infrastructure renouvelée et sécurisée, avant la rentrée scolaire.

3. Besoins et Exigences

3.1 Infrastructure Serveur

- Remplacement des serveurs : Installation de deux nouveaux serveurs dédiés, l'un à la virtualisation, l'autre à la redondance du premier.
  Ces serveurs doivent pouvoir proposer la virtualisation de plusieurs serveurs virtuels :
    - Un premier serveur pour l'annuaire Active Directory des utilisateurs des services administratifs, le partage des imprimantes et des données.
    - Un second pour l'hébergement de la solution ERP interne
    - Un troisième pour l'annuaire Active Directory des utilisateurs professeurs et élèves, ainsi que le partage des données.

- Redondance : La totalité des machines virtuelles doivent être redondés sur 2 serveurs physiques toutes les heures.
- Sauvegarde : Établissement d'une politique de sauvegarde 3-2-1 pour garantir la sécurité et l'intégrité des données. Cela inclut des sauvegardes sur différents médias et emplacements pour minimiser le risque de perte de données.

3.2 Protection et Firewall

- Sécurité : mise en place d'un système de firewall avancé pour la protection des réseaux contre les menaces externes. Cette solution doit répondre aux attentes de l'ANSSI.
- Filtrage de contenu : Filtrage adaptée du contrôle dédié à l'éducation et aux mineurs. Assurer un hébergement sécurisé des logs pour une période de 365 jours, spécifiquement pour les activités pédagogiques.
  Cette solution doit respecter les lois anti-terrorisme et Hadopi :
  - Conservation des accès Internet et des identités associées
  - Archivage automatique des traces d'accès Internet
  - Loi Anti-terrorisme : Décret N° 2006-358 du 24 Mars 2006
  - Loi Hadopi : Contre le téléchargement illégal
  - Code de Protection Intellectuel (L331)
  - Loi de Protection des Mineurs (Art 227)
  - RGPD N° 2016/679

3.3 Intégration et configuration

Analyse approfondie du système et du réseau existant :

- **Approfondir l'audit réalisé** en s'attardant sur les points suivants :
  - Vulnérabilités du système et du réseau
  - Besoins spécifiques en matière de sécurité et d'intégration
  - Compatibilité avec les nouvelles solutions
  - Performances et capacité du réseau
- **Cartographier l'infrastructure réseau** avec des outils d'analyse automatisés pour identifier les éléments obsolètes ou non sécurisés.
- **Documenter l'architecture du réseau et les configurations existantes** pour faciliter la planification de l'intégration.

Intégration des nouvelles solutions de sécurité :

- **Sélectionner des solutions de sécurité** (firewalls, filtrage de contenu) répondant aux besoins spécifiques d'un établissement de formation et **compatibles avec l'infrastructure existante**.
- **Définir une stratégie de sécurité globale** intégrant les nouvelles solutions et les procédures de sécurité existantes.

Intégration et configuration des nouveaux serveurs :

- **Planifier l'intégration des nouveaux serveurs** en tenant compte de la charge de travail, des besoins en stockage, de la redondance et de la future évolutivité.
- **Migrer les données et les applications** vers les nouveaux serveurs de manière transparente et sans interruption de service.
- **Optimiser la configuration des serveurs** pour maximiser les performances et la sécurité.
- **Mettre en place des solutions de sauvegarde et de restauration** pour garantir la disponibilité des données critiques.

Mise en réseau du matériel sur le cœur de réseau existant :

- **Conserver les différents VLAN présents** pour maintenir la segmentation du réseau et le contrôle d'accès.
- **Configurer les switchs et les routeurs existants** pour garantir une connectivité optimale et sécurisée entre les différents éléments du réseau.
- **Mettre en place des mécanismes de redondance** pour garantir la disponibilité du système en cas de panne.
- **Optimiser les performances du réseau** en fonction des besoins et des usages.

Création de la nouvelle infrastructure et intégration des ordinateurs existants :

- **Définir une architecture réseau flexible et évolutive** capable de répondre aux besoins croissants de l'établissement.
- **Intégrer les ordinateurs existants à la nouvelle infrastructure** en utilisant des technologies de migration appropriées et en préservant les données et les configurations utilisateur.
- **Vérifier la compatibilité des logiciels et des applications** avec la nouvelle infrastructure.
- **Mettre en place des solutions de gestion et de monitoring** pour simplifier l'administration et garantir la sécurité de la nouvelle infrastructure.

4. Planification et Mise en Œuvre

4.1 Calendrier

- **Phase de planification** : Définition précise des besoins et sélection des fournisseurs fin mai 2024
- **Mise en œuvre** : Installation et configuration de l'infrastructure entre le 15 juillet et le 15 août, avec l'assistance de deux techniciens dédiés.

En plus de ces points d'optimisation, il est important de :

- **Communiquer clairement et régulièrement** avec les utilisateurs et les équipes tout au long du processus d'intégration.
- **Former les utilisateurs** aux nouvelles solutions et procédures de sécurité.

4.2 Contrat d'Infogérance <u>(le contrat d'infogérance doit être distinct du contrat d'équipement)</u>

Mise en place d'un contrat d'infogérance pour une maintenance proactive de l'infrastructure, incluant la télémaintenance, les déplacements illimités des techniciens, et une supervision complète du système informatique.

Prise en charge dans le cadre du contrat de maintenance :

- Télémaintenance illimitée

- Déplacements nécessaires illimités

- Main d'œuvre de réparation illimitée

- Prêt de matériel si immobilisation de plus de 72h

- Mise en place d'un extranet pour déclaration des pannes et suivi des interventions avec supervision possible d'un ou plusieurs responsables internes

- Rapport sur simple demande des travaux effectués sur site ou en télémaintenance aux responsables, disponible sur l'extranet

- 1 visite annuelle minimum sur site pour maintenance des postes de manière préventive

- Audit succinct annuel du parc informatique pour évolutions éventuelles

- Gestion, mises à jour et configuration des antivirus (hors fourniture de licences)

- Installation et déploiement des périphériques d'impression (mise en relation avec le prestataire si besoin)

- Gestion des problèmes d'e-mails

- Gestion des problèmes de réseaux (mise en relation avec le FAI si besoin)

- Infogérance des serveurs (gestion des utilisateurs, gestion des sauvegardes, installation des logiciels spécifiques, vérification quotidienne des sauvegardes, supervision quotidienne du serveur)

- Etiquetage des postes