ROBUSTSÉCURITÉ

ANALYSE INITIALE ET DÉFINITION DES BESOINS

« Projet de sécurisation de la salle d'exposition de la mairie de Maisons-Alfort »

30/09/2025

Lyes MOUHOUN – Thomas BORAS-DUPUY – Yanis AIT ABBOU V1.1

Table des matières

1- Contexte....2

2-Objectifs du projet....2

L'Objectif de ce document est de définir les besoins, qualifier les problèmes constatés, proposer des solutions, estimer les ressources et présenter une feuille de route (incluant un scénario de test sous Cisco Packet Tracer)....2

3 - Périmètre du projet....2

4 - Analyse des besoins....2

4.1 Besoins fonctionnels....2

4.2 Besoins non fonctionnels....2

5. Problèmes constatés et risques....3

6. Exigences de sécurité (synthèse)....3

7. Solutions à apporter....3

7.1 Architecture & topologie....3

7.2 Segmentation & contrôle du trafic....4

7.3 Protection contre menaces internes....4

7.4 Sécurité physique....4

7.5 Supervision, journaux et réponse à incident....5

7.6 Sauvegardes & continuité....5

8. Ressources disponibles....5

1- Contexte

La Mairie de Maisons-Alfort exploite une salle d'exposition ouverte au public. Un local situé dans cette salle héberge des commutateurs raccordés au réseau interne de la mairie. La collectivité souhaite mettre en place des mesures de sécurité **physiques** et **logiques** afin de garantir la disponibilité des services, la confidentialité des données et l'intégrité du réseau, y compris face aux menaces internes.

2-Objectifs du document

L'objectif de ce document est de définir les besoins, qualifier les problèmes constatés, proposer des solutions, estimer les ressources et présenter une feuille de route (incluant un scénario de test sous Cisco Packet Tracer).

3 - Périmètre du projet

Salle d'exposition (zone publique) et local technique associé.

- Interconnexion avec le réseau communal (cœur / datacenter de la mairie).
- Postes en libre accès, bornes Wi-Fi visiteurs.
- Commutateurs d'accès et d'agrégation.

Hors périmètre (référencés pour dépendances) : SI métiers, serveurs applicatifs centraux, sauvegardes datacenter, postes agents hors salle d'exposition.

4 - Analyse des besoins

4.1 Besoins fonctionnels

L'infrastructure doit avant tout garantir la continuité de service. Cela implique la mise en place de mécanismes de redondance et d'un Plan de Reprise d'Activité (PRA) afin d'assurer la disponibilité des services même en cas de panne ou d'incident technique. La séparation des usages constitue également une exigence essentielle, car le réseau réservé à l'administration doit être strictement isolé du réseau public afin de prévenir toute interférence et de limiter les risques de compromission.

Le contrôle des accès représente un autre besoin majeur puisque chaque connexion doit être authentifiée et tracée, qu'elle émane d'utilisateurs internes ou de visiteurs. Dans le même esprit, la maîtrise du parc informatique doit être totale. Il convient d'empêcher l'ajout

non autorisé de commutateurs, serveurs ou périphériques, qui pourraient fragiliser l'infrastructure.

La supervision et la journalisation jouent un rôle central. Elles doivent permettre une visibilité en temps réel, générer des alertes pertinentes et conserver des historiques horodatés pour faciliter les enquêtes et les interventions en cas d'incident. En parallèle, le respect du RGPD doit être garanti. Le traitement des données doit rester minimal et la conservation des journaux limitée à ce qui est strictement nécessaire.

Enfin, la sécurisation des postes publics constitue un dernier point critique. Ceux-ci doivent être protégés par des antivirus à jour, un contrôle des supports amovibles, la désactivation du démarrage par clé USB, des droits d'accès limités et une restriction des usages Internet afin de réduire les risques liés à leur utilisation.

4.2 Besoins non fonctionnels

La disponibilité du système doit être garantie à hauteur de 99,9 % pendant les heures d'ouverture, ce qui est indispensable pour offrir un service fiable et continu aux usagers. Les performances doivent être conformes aux besoins réels, le débit devant correspondre au lien entrant et s'appuyer sur un câblage adapté, en l'occurrence de catégorie 5, qui répond aux exigences du projet.

La simplicité opérationnelle doit également être assurée. Elle passe par la standardisation des procédures, l'utilisation de modèles de configuration, le recours aux GPO pour une gestion centralisée et la mise en place d'une matrice RACI clarifiant les responsabilités. Cette organisation facilitera l'exploitation quotidienne, réduira les erreurs et garantira une meilleure maîtrise globale de l'infrastructure.

5. Problèmes constatés et risques

- Local technique **dans** la zone publique, **contrôle d'accès insuffisant** (risque d'intrusion/altération).
- Ports commutateurs **accessibles** : possibilité d'ajout d'un switch pirate ou de branchement de PC non enregistré.
- **Manque de segmentation** : risque de latéralisation entre public et réseau communal.
- **Politique de poste insuffisante** sur machines publiques (droits étendus, périphériques USB, cmd, téléchargements).
- **Journalisation lacunaire** : difficulté d'enquête après incident.
- **Redondance limitée** : point de défaillance unique sur certains liens/équipements.

Impact : indisponibilité d'exposition, fuite de données, compromission de comptes, atteinte à l'image de la collectivité.

6. Solutions à apporter

6.1 Architecture

- **Topologie en étoile** : cœur/agrégation central ; chaque station indépendante du reste. Avantage : dépannage facilité et confinement des pannes.
- **Redondance** : au minimum **2 routeurs** et **2 commutateurs** par zone d'usage critique, alimentation secourue (onduleur).
- **Lien Internet** : **débit asymétrique** maintenu (conforme aux besoin) + prioriser trafic administratif (QoS = Quality of Service).
- **Câblage** : tirer/valider des liaisons **Cat5** (ou supérieures) selon débits visés ; brassage ordonné, étiquetage, **verrous RJ-45** sur les ports.

6.2 Segmentation & contrôle du trafic

- **VLAN par usage** :
    - VLAN-EXPO (équipements d'exposition/publiques),
    - VLAN-WIFI (borne publique)
- **ACL / Pare-feu inter-VLAN** : filtrage strict (deny par défaut), tables d'exception minimales
- **Proxy/filtrage Web** : catégorisation URL, blocage téléchargements risqués sur les VLAN publiques
- **IDS/IPS** : détection de signatures et détections comportementales ; bascule blocante (IPS) pour segments à risque.

6.3 Protection contre menaces internes

- **Port Security (couche 2/L2)** :
    - Désactiver tous **ports inutilisés** (bouchons physiques + shutdown sur la console).
    - Lier ports utilisés à l'**adresse MAC autorisée**, si violation → shutdown + alerte.
- **Inventaire centralisé** via **Active Directory** (domaine + DNS) ; **interdire** l'accès réseau aux hôtes non rejoints au domaine (NAC/whitelist).
- **GPO** pour postes publics : droits **moindre privilège**, désactivation **cmd/PowerShell**, exécutions non signées = impossibilité d'installation de programmes, mise à jour auto, **comptes temporaires nominatifs** délivrés à l'accueil sur présentation de carte d'identité.

6.4 Sécurité physique

- Transformer le **local** en **salle technique séparée** accessible via badge uniquement (=horodatage, identification), a minima **armoire** fermée à clé, ancrée, **portes blindées**.
- **Vidéosurveillance** de l'accès armoire/local (conforme RGPD) ; détecteurs d'ouverture.
- **Verrous de câbles** (clips/verrous RJ-45) sur ports en amont/ vers la partie management.

6.5 Supervision, journaux et réponse à incident

- **Syslog/NTP** centralisés (horodatage fiable).
- **Runbooks** : procédures d'isolement VLAN, restauration config, escalade support, notification DPO en cas d'incident.

6.6 Sauvegardes & continuité

- **Sauvegarde de configurations** (routeurs/switchs) quotidienne + avant/après changement.
- **Alimentation** : onduleurs (courant continu), tests trimestriels

7. Ressources disponibles et organisation

- **Temps** : 3 jours
- **Équipe** : 1 chef de projet : M. Borras-Dupuy
  2 employés de l'entreprise : M. Mouhoun et M. Ait Abbou
- **Budget** : l'argent du contribuable de la commune, illimité (virtuellement)
- **Contraintes** : Travail les mardis uniquement, commutateurs Cisco, usage de Packet tracer pour les tests

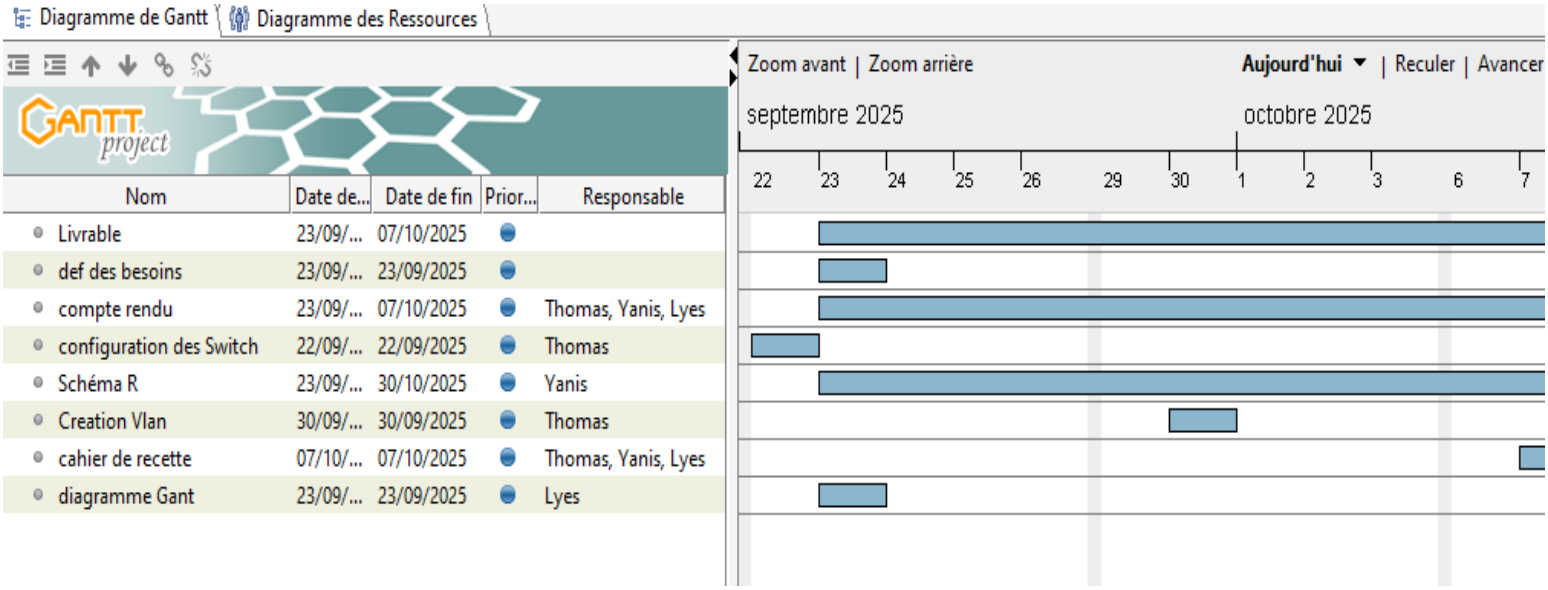
Diagramme de Gantt
Diagramme des Ressources
Zoom avant | Zoom arrière
Aujourd'hui | Reculer | Avancer
septembre 2025
octobre 2025
22 23 24 25 26 29 30 1 2 3 6 7
Nom
Date de...
Date de fin
Prior...
Responsable
Livrable 23/09/... 07/10/2025
def des besoins 23/09/... 23/09/2025
compte rendu 23/09/... 07/10/2025 Thomas, Yanis, Lyes
configuration des Switch 22/09/... 22/09/2025 Thomas
Schéma R 23/09/... 30/10/2025 Yanis
Creation Vlan 30/09/... 30/09/2025 Thomas
cahier de recette 07/10/... 07/10/2025 Thomas, Yanis, Lyes
diagramme Gant 23/09/... 23/09/2025 Lyes