

Stage Fontreyne 2021

Livre blanc

Projet réalisé par Théo PERDIGON



Sommaire

Cahier des charges	2
Infrastructure du réseau	3
1 - Plan d'adressage	3
2 - Schéma logique du réseau	5
3 - Schéma physique du réseau	6
Serveur d'authentification et de contrôle d'accès	7

Cahier des charges

Le réseau n'a aucun système de contrôle d'accès internet, il faut donc trouver une solution afin de répertorier chaque utilisateurs et d'avoir des logs en cas d'incident.

Il faut donc :

- Mettre en place un serveur d'authentification type portail captif pour tous les utilisateurs
- Créer un compte pour les utilisateurs avec des limites de temps de connexion pour certains utilisateurs
- Mettre en place une blacklist pour interdire les sites illicites
- Générer des tickets pour les utilisateurs afin de leur transmettre leurs identifiants
- Configurer des exceptions d'authentification pour les serveurs

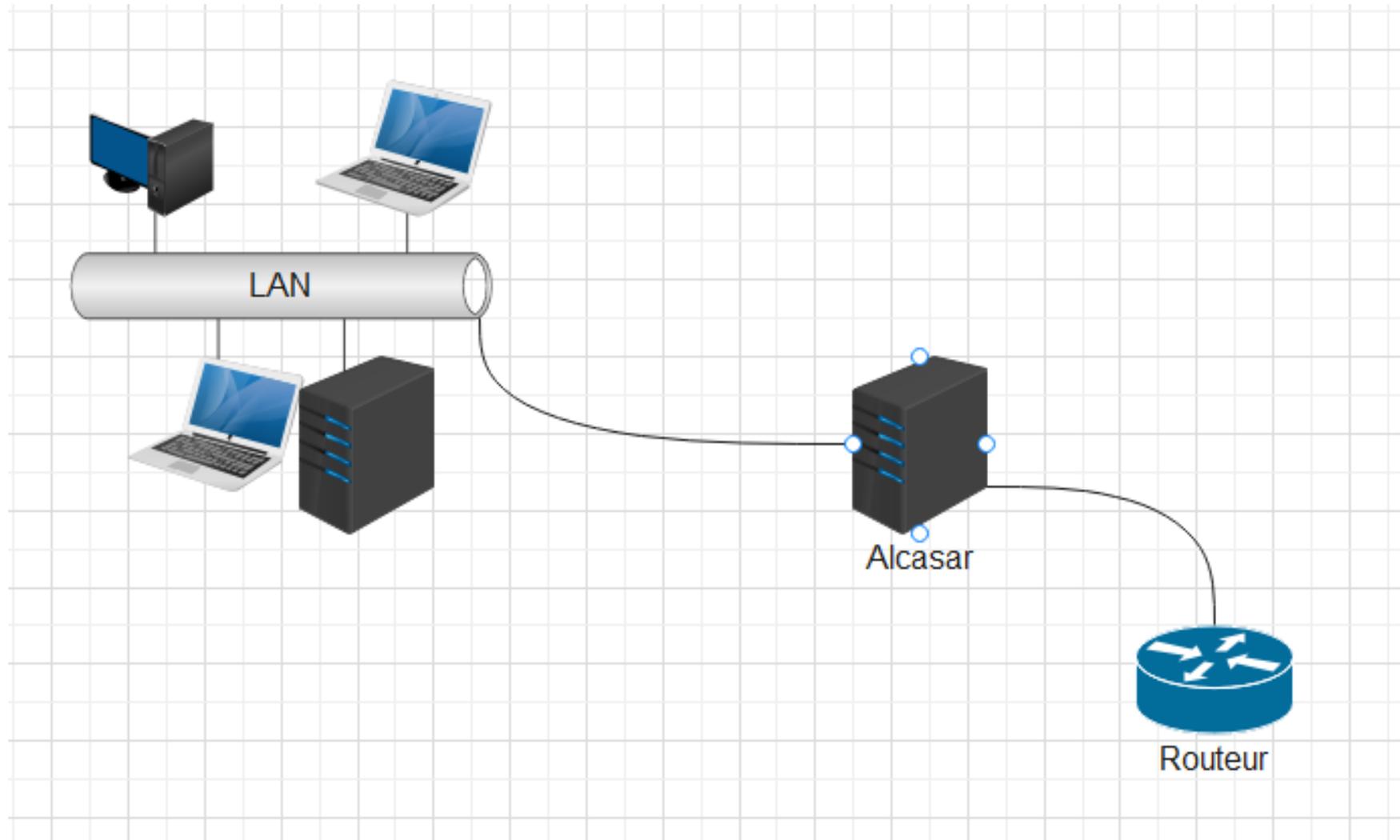
Infrastructure du réseau

1 - Plan d'adressage

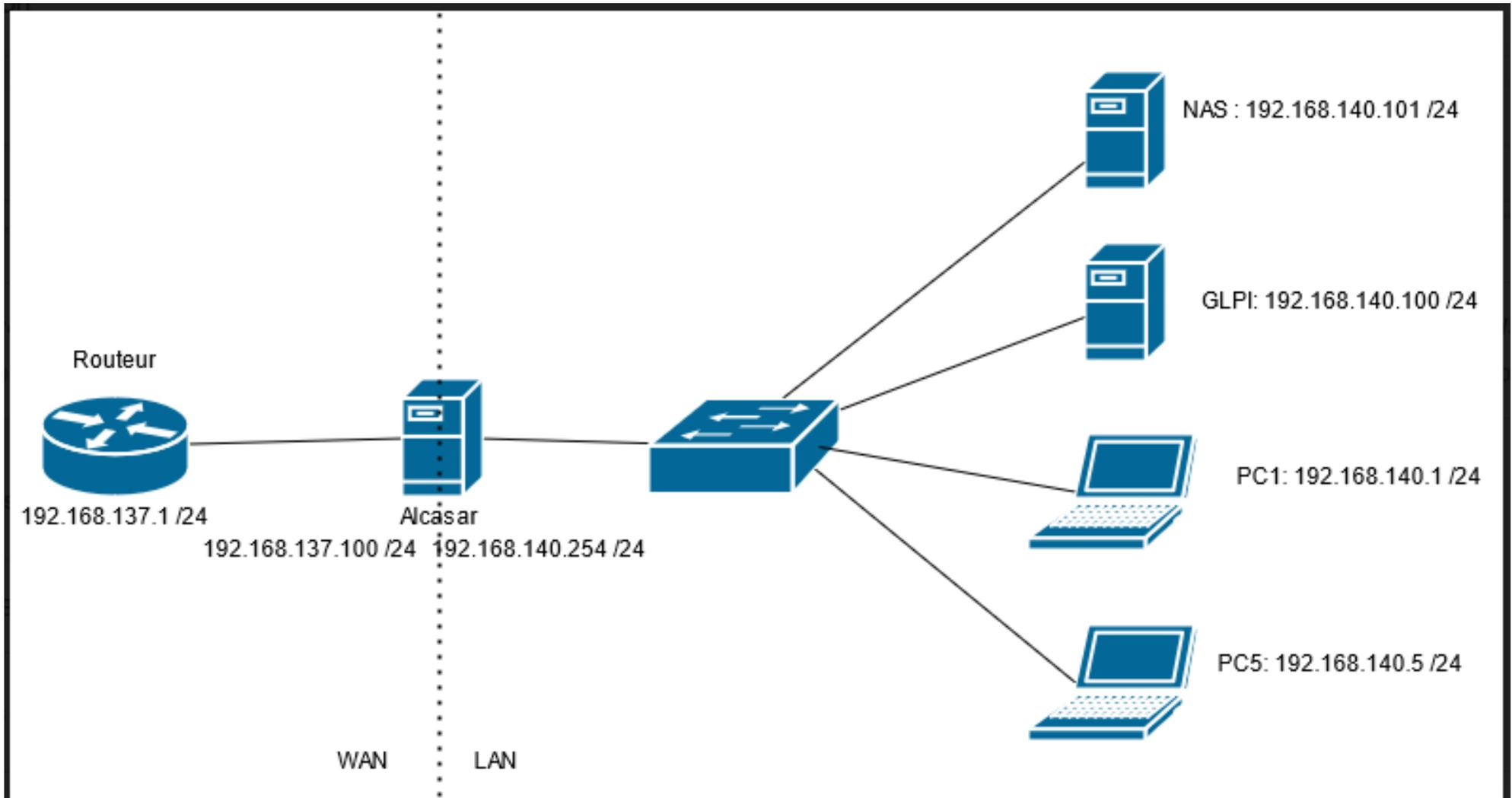
Le réseau est divisé en deux parties, WAN et LAN

Nom	LAN	WAN
Routeur principal	-	192.168.137.1 /24
Alcasar	192.168.140.254 /24	192.168.137.100 /24
GLPI	192.168.140.100 /24	-
NAS	192.168.140.101 /24	-

2 - Schéma logique du réseau



3 - Schéma physique du réseau



Serveur d'authentification et de contrôle d'accès

Afin de répondre au cahier des charges à 100%, une solution a été retenue, **Alcasar**.
Installation faite sur une distribution **Linux Mageia 7.1**.

La blacklist utilisée est celle fournie par Alcasar par défaut.

Les invités, externes à l'établissement on une limite de temps concernant la connexion internet

Durée maximale d'une session (en secondes)	<input type="text"/>	s ▼
Durée de connexion maximale (en secondes)	120	s ▼
Durée de connexion maximale mensuelle (en secondes)	120	s ▼
Durée de connexion maximale journalière (en secondes)	120	s ▼
Période hebdomadaire	<input type="text"/>	▼