

PROJET D'AUDIT TECHNIQUE

AUDIT STRATÉGIQUE M2L

Accompagnement Cyber &
Infrastructure

COLLECTIF ALTERZEN

Agenda

- 01 Présentation du Collectif AlterZen
- 02 Diagnostic SI & Architecture Proxmox
- 03 Analyse de la Segmentation Réseau
- 04 Problématique 1 : Redondance & Sécurité
- 05 Problématique 2 : WiFi Enterprise 802.1X
- 06 Roadmap & Jalons de Production

L'ÉQUIPE PROJET ALTERZEN

LÉO B.

DIRECTEUR GÉNÉRAL & MARKETING

MOHAMED-AMINE B.

GOUVERNANCE & FINANCES

ABEL T.

RESPONSABLE INGÉNIERIE & IT

ABDESSAMAD E.

LEAD DEV & DATA ENGINEERING

XIMENG C.

CYBERSÉCURITÉ & INFRASTRUCTURE

CRISTAL B.

EXPÉRIENCE UTILISATEUR & DESIGN

NOÉ L.

DÉVELOPPEMENT MARCHÉ & ALLIANCES

CONTEXTE : LA MAISON DE LORRAINE

La M2L est une structure mutualisant les moyens techniques et humains pour 24 ligues sportives régionales.



Hébergement de structures sportives.



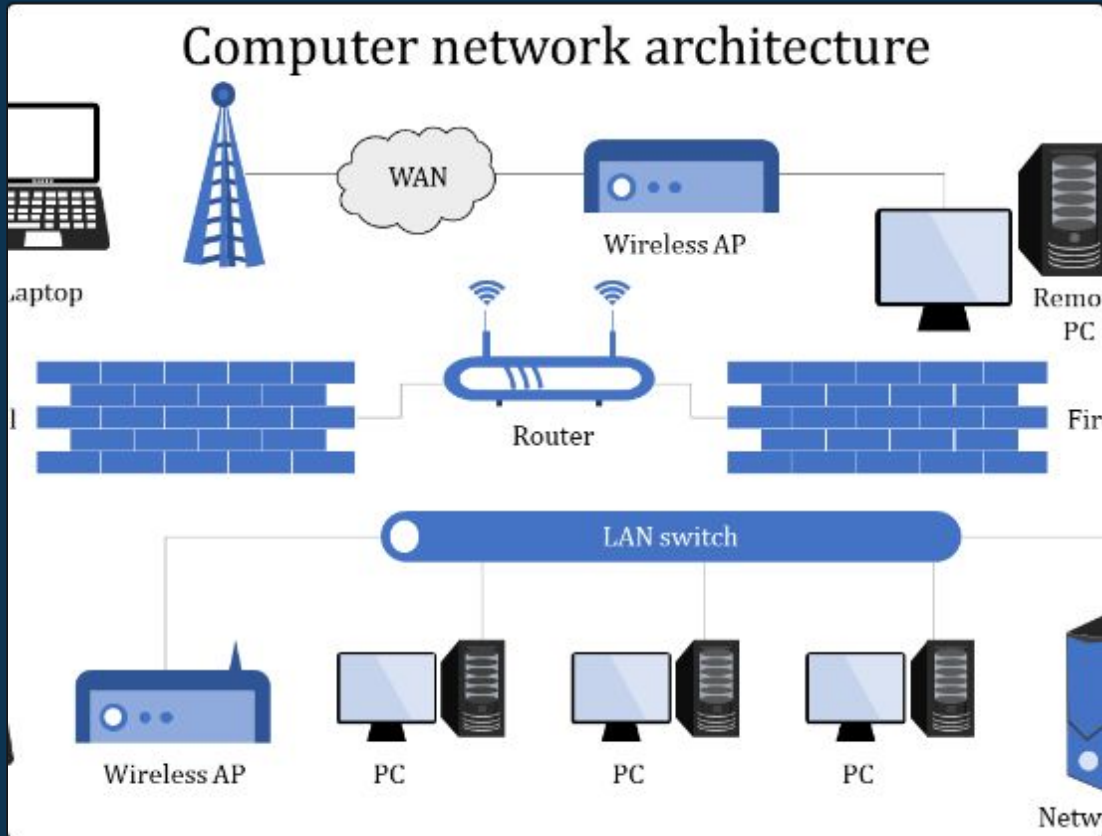
Mise à disposition de services SI partagés.



Besoin critique d'isolement inter-ligues.



AUDIT INFRASTRUCTURE CIBLE



Architecture Virtualisée

-  **Hyperviseur** : Proxmox (10.20.50.87).
-  **Firewall** : pfSense (10.20.50.88).
-  **Segmentation** : Schéma IP 172.16.0.0/16.
-  **Passerelle** : Freebox -> WAN pfSense.

SEGMENTATION IP & VLANS

VLAN	Usage / Fonction	Réseau (CIDR)
99	Hyperviseur + Backup	172.16.99.0/24
2 / 3	Impression / NAS	172.16.2.0/24 - 172.16.3.0/24
4 / 5	GLPI / DMZ	172.16.4.0/24 - 172.16.5.0/24
6	Base de Données (BDD)	172.16.6.0/24
7 / 8	Admin / Postes Employés	172.16.7.0/24 - 172.16.8.0/24
9 / 10	AD+DHCP / Zabbix	172.16.9.0/24 - 172.16.10.0/24

// Note : La segmentation en /24 permet d'isoler chaque domaine de broadcast.

| SUPERVISION & GESTION (ZABBIX/GLPI)



Zabbix (VLAN 10)

Monitoring temps réel des hyperviseurs et des services critiques (Active Directory, pfSense).



GLPI (VLAN 4)

Ticketing pour les 24 ligues sportives hébergées.



BDD (VLAN 6)

Base de données centralisée et étanche, accessible uniquement par les serveurs applicatifs via firewalling.

ANALYSE DES VULNÉRABILITÉS

Diagnostic Critique

- ! Réseau "Flat" par défaut (avant segmentation).
- ! Absence de redondance de la passerelle WAN.
- ! WiFi visiteurs non isolé du réseau de gestion.



PHASE
OPÉRATIONNELLE

Problématiques Stratégiques

Définition des enjeux AP2

PROBLÉMATIQUE N°1

Infrastructure : Amélioration & Sécurité

Comment optimiser les performances et garantir la haute disponibilité de l'architecture M2L ?

-  Mise en place de la haute disponibilité (HSRP/VRRP).
-  Finalisation du routage inter-VLAN sur pfSense.
-  Filtrage granulaire via règles de Firewalling (ACLs).

TECHNOLOGIE : REDONDANCE HSRP



Continuité de Service

Élimination des "Single Points of Failure" (SPOF) via le basculement automatique.

Passerelle Virtuelle (VIP) -> Redondance pfSense.

- ⚡ Failover automatique < 3 secondes.
- ↻ Synchronisation des états de session Firewall.

| PROBLÉMATIQUE N°2

Réseau Sans-Fil : Sécurisation

Comment sécuriser l'accès WiFi et isoler les flux externes des secrets industriels de la M2L ?

-  Authentification 802.1X via RADIUS/NPS.
-  Séparation physique des SSIDs (Pro vs Visiteurs).
-  Affectation dynamique de VLAN selon l'identité AD.

TECHNOLOGIE : WIFI 802.1X

Authentification Enterprise

Abandon des clés partagées (PSK) au profit d'identifiants individuels centralisés.

-  **Serveur RADIUS** : Interfacé avec l'AD du VLAN 9.
-  **EAP-PEAP** : Tunnel TLS pour protéger les mots de passe.
-  **VLAN Guest** : Portail captif et accès WAN seul.



FOCUS : ARCHITECTURE PROXMOX

Virtualisation de l'écosystème

Toutes les machines (GLPI, Zabbix, AD, pfSense) sont opérées en machines virtuelles (VM) sur l'hôte Proxmox.



Allocation dynamique des ressources (RAM/vCPU).



Snapshots quotidiens et plan de reprise d'activité (VLAN 99).



Gestion des ponts virtuels (vSwitch) vers le LAN physique.

RÔLE DU FIREWALL PFSENSE



Cœur de Sécurité

Routage : Routage Inter-VLAN pour le réseau 172.16.x.x.

Filtrage : Interdiction de communication entre VLAN Admin et VLAN Employés par défaut.

Services : Serveur DNS Resolver et DHCP pour tous les réseaux de ligues.

SOUVERAINETÉ & SÉCURITÉ

RGPD 2024

Isolation stricte des données personnelles des employés et membres des ligues.

Data Control

Données hébergées localement (NAS/BDD) sous contrôle direct du CROSL.

Audits

Journalisation centralisée (Syslog) pour une traçabilité totale des accès WiFi/LAN.

L'AVANTAGE ALTERZEN

-  **Matching Tech** : Infrastructure alignée sur les besoins réels.
 -  **Protection** : Sécurité native dès le design (Segmentation).
 -  **Support** : Suivi technique et transfert de compétences.
-

QUESTIONS ?

Propulsons l'infrastructure M2L vers
demain

www.alterzen.com contact@alterzen.com

BTS SIO - PROJET AP1/AP2
