Contexte M2L

1. Présentation Générale de l'infrastructure à réaliser

L'infrastructure a été volontairement séparée en 2 pôles distincts pour des raisons de gestion du trafic, de sécurité et d'administration des différents services (voir schéma 1).

Le réseau intègre une partie spécifique à la M2L. Ce réseau regroupe un ensemble de ressources partageables entre M2L et les différentes ligues (Annuaire, Serveurs divers DHCP, DNS, et une DMZ, ...) ainsi que les équipements du parc de la M2L.

L'autre partie constitue l'infrastructure propre louée aux différentes ligues adhérentes de la M2L, chaque Ligue aura son propre sous-réseau.

Chaque ligue est responsable de l'installation des équipements, de leur exploitation et leur maintenance. Elle délègue ces diverses tâches au département réseau de M2L qui agit en tant que prestataire par le biais d'un contrat de service.

L'infrastructure générale repose sur un ensemble de 4 bâtiments avec les impondérables et impératifs techniques que cela peut engendrer. Ce site constitue l'infrastructure réseau dans laquelle sont intégrés les postes et serveurs informatiques, une infrastructure mobile WIFI, un service d'accès à Internet sécurisé et des liaisons télécoms permettant à la M2L de proposer des connexions dédiées avec ses partenaires.

Le domaine M2L.local a été choisi pour héberger l'infrastructure générale. La gestion et l'administration du réseau sont assurées par un contrôleur de domaine LDAP.

2. Le réseau

Comme le montre clairement le schéma 1, la maquette réseau M2L intègre les sous réseaux de l'association M2L, les sous réseaux des ligues, l'infrastructure de sécurité DMZ et enfin le service d'accès à Internet. Le service Informatique du département réseau de la M2L héberge toute la structure de contrôle et de supervision du parc informatique du site.

3. Plan d'adressage IP (Annexe 2)

Le réseau général est construit autour de l'adresse 172.16.0.0 avec un masque de 16 bits. Toutefois il faut penser l'infrastructure avec un ensemble de 32 ligues préconisé comme capacité d'hébergement maximale de M2L. Dans cette infrastructure 60 adresses IP seront affectées à chaque ligue dans un environnement double DHCP, soit un masque de 24 bits par sous réseau. Chaque ligue ayant son VLAN.

Le plan d'adressage IP 192.168.0.0/29 est attribué à la DMZ publique et 192.168.1.0/29 à la DMZ privée. Le plan 172.16.99.0/29 est destiné au sous réseau de gestion.

Un tableau en annexe 2 décrit le plan d'adressage IP de l'ensemble du réseau et propose une gestion des adresses par adressage dynamique et adressage fixe.

Un ensemble d'adresses IP fixes est réservé pour les équipements réseau, serveurs et postes terminaux ceci pour chaque sous réseaux.

Des choix d'administration préconisent des règles d'ingénierie imposant de placer les plages d'adresses fixes sur les adresses les plus hautes (réservées pour chaque sous réseau) avec les équipements de réseau placés aux adresses les plus hautes.

Une plage d'adresse pour les postes à adressage dynamique est établie et tient compte de l'installation de 2 serveurs DHCP pour l'implantation d'une tolérance de panne sur le service réseau DHCP. Voir Tableau Annexe 2.

4. Infrastructure M2L

Ce réseau regroupe les fonctions suivantes :

- Une structure de VLAN de niveau 1, comprenant 7 sous réseaux VLAN, organisée selon la structure hiérarchique de M2L (structure par département). La maquette comprend :
  - Le VLAN du service Informatique du département Réseau (VLAN INFORMATIQUE) placé dans le réseau 172.16.2.224 /27.
  - Le VLAN de gestion qui permet d'accéder à distance aux équipements réseau via le poste Administrateur du service Informatique du département réseau. Le VLAN de gestion de M2L est dans le sous réseau 172.16.99.0/29.
  - Les VLAN ligues Karaté, Athlé et Yoga destinés aux postes des ligues sportives.
  - Les VLAN Wifi public et permanent.
  - Un VLAN VOIP, qui permet d'isoler les communications VOIP des autres communications.

- Deux routeurs RTM2L permettent d'interconnecter ces sous réseaux au réseau général via des sous interfaces VLAN et l'encapsulation 802.1Q. Le service HSRP permettra d'assurer la redondance du routeur principal en cas de défaillance de ce dernier.

- Un réseau assure le lien entre les zones LIGUES et M2L. Les équipements de réseau sont administrés par les postes administrateurs.

- L'administration à distance en mode sécurisé via le protocole SSH permet une prise de contrôle à distance des équipements routeurs et commutateurs du réseau global.

- Les services et applications nécessaires au fonctionnement général du site. Tous ces services et applications sont administrés par :
  - Des serveurs DHCP, DNS, Active Directory redondés ;
  - Des services applicatifs : gestion de parc GLPI, FTP ;
  - Une plateforme de supervision assurée par Zabbix ;
  - Une plateforme collaborative (Nextcloud) sur un serveur Linux : un dossier partagé pour chaque ligue et un dossier commun accessible par toutes les ligues en lecture seule.
  - Un serveur Asterisk assure les communications VOIP des téléphones IP.
  - Deux serveurs de base de données qui hébergeront les bases de données des serveurs.
  - Des serveurs Web pour les sites web des ligues et le site vitrine de la M2L.
  - Un serveur de backup qui réalisera des sauvegardes régulières des fichiers des sites web des serveurs web de la M2L et des bases de données.

4. Infrastructure des ligues

Chaque ligue est intégrée à un sous réseau dans un VLAN. Le plan d'adressage des ligues est donné dans le tableau Annexe 2.

La maquette comprend la ligue Karaté, Athlétisme et Yoga. Les postes sont équipés d'OS Windows ou Linux, intégrant chacun un agent GLPI pour la supervision de parc.

Les ligues sont réparties sur les commutateurs SWLIGUES1, SWLIGUES2 et SWLIGUES3.
Le commutateur de distribution SWLIGUES1 assure le lien entre les commutateurs SWLIGUES2, SWLIGUES3 et les routeurs RTLIGUES.

Les sous réseaux des ligues sont connectés au réseau général par les routeurs RTLIGUES, supportant des sous interfaces VLAN et l'encapsulation 802.1Q.

Cette structure de réseau de commutateurs dite à chemin redondant, doit assurer la continuité du service sur la transmission des données. Elle est installée en utilisant 3 commutateurs connectés en boucle. Le spanning-tree est activé par défaut, pour privilégier les chemins principaux qui relient les commutateurs d'accès au commutateur de distribution et assurer une continuité de service.
Le protocole HSRP assure la redondance des routeurs RTLIGUE.

5. Accès Internet et DMZ

Le pare-feu Pfsense principal assure le périmètre de sécurité avec l'Internet au travers d'une interconnexion entre le réseau interne, la DMZ publique et Internet.

La zone DMZ publique intègre le service FTP, ainsi qu'un serveur HaProxy pour l'accès aux serveurs WEB. Ces services doivent être accessibles depuis l'extérieur.

L'ensemble des services des DMZ seront accessibles depuis le réseau interne sous certaines conditions (droits, mots de passe).

4. Règles de contrôle d'accès

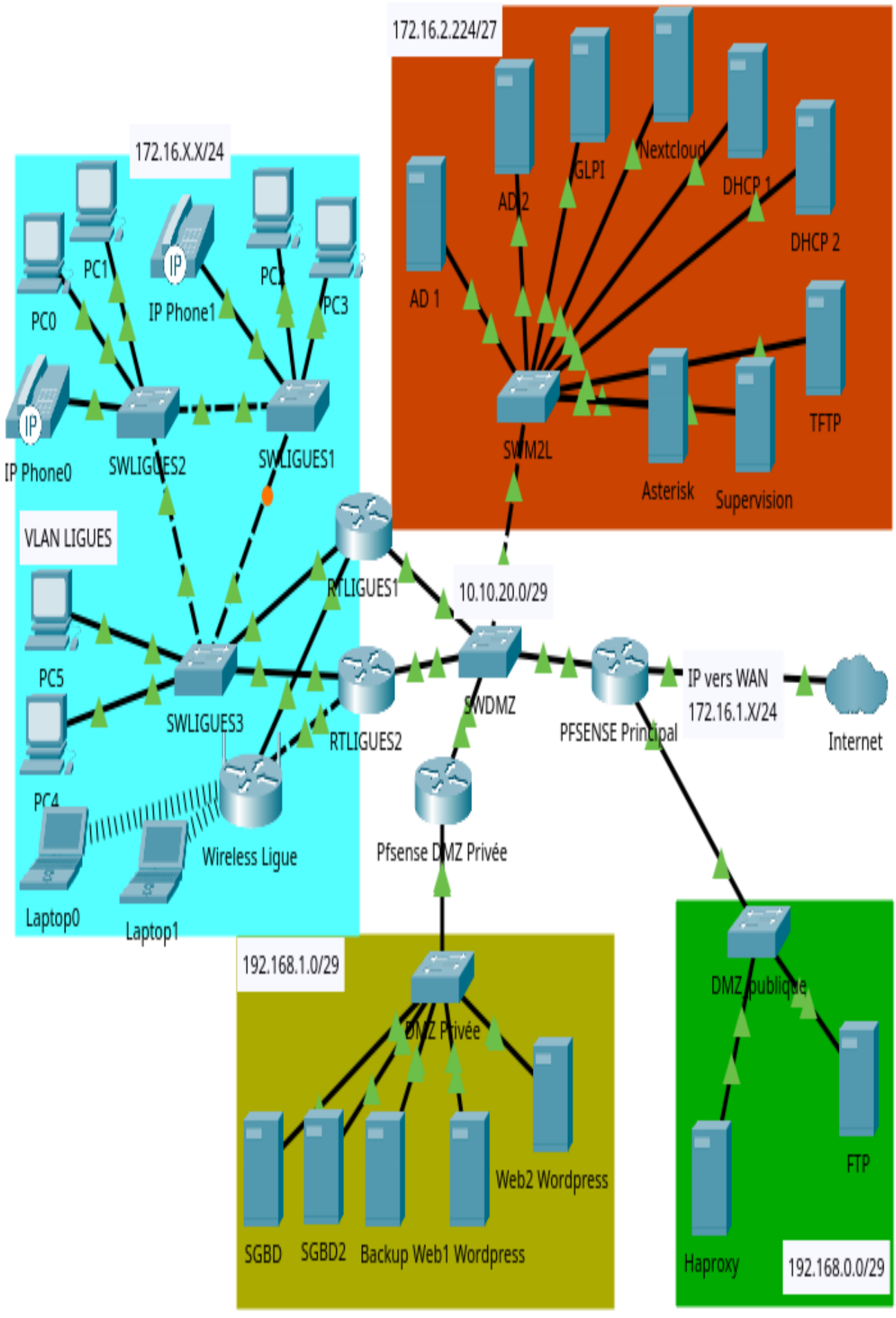
1/ Les sous réseaux des ligues et de M2L peuvent accéder à Internet.
2/ Les Internautes peuvent accéder aux ressources de la DMZ mais pas aux réseaux privés Ligues et M2L. Les utilisateurs externes ont accès uniquement au site web vitrine de la M2L.
3 / Les sous réseaux M2L peuvent accéder aux ressources de la DMZ tout comme les ligues.
4 / Une ligue peut communiquer avec une autre ligue, mais pas avec les autres :
Le VLAN 10 ↔ VLAN 11 ↔ VLAN 12 (le VLAN10 ne peut pas communiquer avec le VLAN 12 et inversement).
5 / Tout trafic ICMP en provenance d'Internet est interdit.

5. Maintenance

La détection de pannes, l'analyse du réseau et le monitoring s'effectueront via les serveurs GLPI, Zabbix, les protocoles SNMP ou encore l'analyseur de trames Wireshark. Les utilisateurs du réseau peuvent envoyer un ticket d'incident via l'interface GLPI.

La prise de contrôle à distance via le protocole SSH permet de surveiller, modifier ou visualiser les états des équipements de réseau.
Enfin, l'IDS Snort, installé sur Pfsense, détectera et analysera les possibles attaques sur la M2L.

Annexe 1 : Schéma du Réseau :



Annexe 2 : Adressage IP

Adressage zone M2L

VLAN M2L	VLAN2 INFORMATIQUE
Adresse Réseau	172.16.2.224
Masque	255.255.255.224
Adresse diffusion	172.16.2.255
Passerelle	172.16.2.254
Service DHCP	NON

Adressage zone LIGUES

VLAN LIGUES	VLAN10 KARATE	VLAN11 ATHLE	VLAN12 YOGA	VLAN32....
Adresse Réseau	172.16.10.0	172.16.11.0	172.16.12.0	
Masque	255.255.255.0	255.255.255.0	255.255.255.0	
Adresse diffusion	172.16.10.255	172.16.11.255	172.16.12.255	
Plage DHCP	172.16.10.1 → 172.16.10.60	172.16.11.1 → 172.16.11.60 →	172.16.12.1 → 172.16.12.60 →	
Plage Fixe	172.16.10.240 → 172.16.10.254	172.16.11.240 → 172.16.11.254	172.16.12.240 → 172.16.12.254	
Passerelle	172.16.10.254	172.16.11.254	172.16.12.254	

Adressage zone Gestion

VLAN de GESTION	VLAN 99 GESTION LIGUES
Adresse Réseau	172.16.99.16
Masque	255.255.255.240
Adresse diffusion	172.16.99.31
Plage DHCP	172.16.99.17 → 172.16.2.24
Plage Fixe	172.16.99.25 → 172.16.2.29
Passerelle	172.16.99.30

Adressage zone VOIP

VLAN de VOIP	VLAN 5 VOIP
Adresse Réseau	172.16.5.0
Masque	255.255.255.0
Adresse diffusion	172.16.5.255
Plage DHCP	172.16.5.1 → 172.16.5.60
Plage Fixe	172.16.5.240 → 172.16.2.254
Passerelle	172.16.5.254

Adressage zone DMZ Publique

	DMZ
Adresse Réseau	192.168.0.0
Masque	255.255.255.248
Adresse diffusion	192.168.0.7
Plage Fixe	192.168.0.1 → 192.168.0.5
Passerelle	192.168.0.6
Service DHCP	NON

Adressage zone DMZ Privée

	DMZ
Adresse Réseau	192.168.1.0
Masque	255.255.255.248
Adresse diffusion	192.168.1.7
Plage Fixe	192.168.1.1 → 192.168.1.5
Passerelle	192.168.0.6
Service DHCP	NON

Adressage réseaux d'interconnexion

Plan	LIGUES ← → Pfsense Principal	LIGUES ← → WIFI
Réseau	10.10.20.0	10.10.30.0
Masque	255.255.255.248	255.255.255.248
Diffusion	10.10.20.7	10.10.30.7
Passerelle	10.10.20.1 / 10.10.20.2	10.10.30.1 / 10.10.30.2

Adressage serveurs

Serveur	**Nom DNS**	**Adresse IP**
Hyperviseur	M2L-Hyperviseur	172.16.2.241
AD - DNS1	M2L-AD1	172.16.2.242
AD - DNS2	M2L-AD2	172.16.2.243
Asterisk	M2L-ASTERISK	172.16.2.244
DHCP 1	M2L-DHCP1	172.16.2.245
DHCP 2	M2L-DHCP2	172.16.2.246
GLPI	M2L-GLPI	172.16.2.247
ZABBIX	M2L-ZABBIX	172.16.2.248
NEXTCLOUD	M2L-NEXTCLOUD	172.16.2.249
TFTP	M2L-TFTP	172.16.2.250

Serveur HAPROXY	M2L-HAPROXY	192.168.0.1
Serveur FTP DMZ	M2L-FTP	192.168.0.2
Serveur WEB1	M2L-WEB1	192.168.1.1
Serveur WEB2	M2L-WEB2	192.168.1.2
SGBD	M2L-SGBD	192.168.1.3
SGBD2	M2L-SGB1	192.168.1.4
Backup	M2L-Backup	192.168.1.5

Réseaux WIFI

Adresse Réseau	172.16.13.0	172.16.14.0
Masque	255.255.255.0	255.255.255.0
SSID	INVITE	PERMANENT
Password	wifi2023i	wifi2023p
Clé	WPA2	WPA2
VLAN	13	14
Plage DHCP	172.16.13.1→ 172.16.13.60	172.16.14.1→ 172.16.14.60
Plage Fixe	172.16.13.61→ 172.16.13.254	172.16.14.61→ 172.16.14.254
Passerelle	172.16.13.254	172.16.14.254