

Préparé par l'équipe technique du Prologic  
Au profit de l'institut supérieur des études technologiques de Mahdia



## Table des matières

I. Introduction .....	5
1. Cadre du projet .....	5
2. Objectif du projet.....	5
3. Liste des tâches .....	5
4. Equipements acquis.....	6
4.1 Description du switch access S5720-28X-PWR-LI-AC.....	6
4.2 Description du switch core S5730-36C-PWH-HI .....	7
4.3 Description du access controller Huawei AC6508.....	8
4.4 Description du access point Huawei AP4050DN.....	9
4.5 Description du Firewall Fortigate 301E.....	9
II. High Level Design .....	10
III. Low Level Design du Switch Core.....	11
1. Spécifications du switch Huawei S5730-36C-PWH-HI.....	11
2. Architecture Core .....	13
3. Configuration initiale .....	13
4. Configuration des interfaces .....	14
5. Configuration du GVRP.....	17
6. Configuration du service DHCP .....	18
7. Configuration de route statique .....	18
8. Configuration du protocole RSTP .....	18
IV. Low Level Design des Switches Access .....	19
1. Spécifications du switch Huawei S5720-28X-PWR-LI-AC .....	19
2. Architecture LAN.....	21
3. Switch Access SW-ADM .....	21
3.1 Configuration initiale.....	21
3.2 Configuration des interfaces.....	22
4. Switch Access SW-DEPI.....	23
4.1 Configuration initiale.....	23
4.2 Configuration des interfaces.....	23
5. Switch Access SW-GES .....	24
5.1 Configuration initiale.....	24
5.2 Configuration des interfaces.....	25
6. Switch Access DEP-M .....	26

6.1 Configuration initiale.....	26
6.2 Configuration des interfaces.....	26
7. Switch Access DEP-BIB.....	27
7.1 Configuration initiale.....	27
7.2 Configuration des interfaces.....	27
V. Low Level Design de l'Access Point.....	28
1. Spécifications du point d'accès Huawei AP4050DN .....	28
2. Liste des APs .....	29
VI. Low Level Design du contrôleur d'accès AC .....	31
1. Spécifications du contrôleur d'accès Huawei AC6508 .....	31
2. Architecture Wi-Fi .....	32
3. Configuration initiale .....	33
4. Configuration des VLANs Wi-Fi .....	33
5. Configuration des interfaces de l'AC.....	35
6. Ajout des APs au contrôleur.....	36
7. Configuration des SSIDs des APs .....	36
8. Configuration des VAP profiles .....	37
9. AP groups .....	37
10. Configuration du DHCP .....	38
11. Configuration complète de l'AC .....	38
VII. Low Level Design du Firewall Fortigate 301E .....	39
1. Spécifications du Fortigate 301E .....	39
2. Architecture WAN .....	40
3. Configuration initiale .....	41
4. Configuration des interfaces .....	41
5. Configuration des routes .....	42
6. Routes statiques .....	43
7. Configuration des règles de sécurité.....	43
VIII. Conclusion .....	44

## Liste des tableaux

Tableau 1: Description des ports/modules du switch core .....	11
Tableau 2: Spécifications du switch Huawei S5730-36C-PWH-HI.....	12
Tableau 3: Configuration initiale du SW-FD .....	13
Tableau 4: Liste des VLANs du SW-FD.....	14
Tableau 5: Liste des interfaces du SW-FD .....	15
Tableau 6: Liste des interfaces Vlanif du SW-FD .....	16
Tableau 7: Configuration du DHCP .....	18
Tableau 8: Liste des switches access.....	19
Tableau 9: Description des ports/modules du switch access.....	20
Tableau 10: Spécifications du switch Huawei S5720-28X-PWR-LI-AC .....	20
Tableau 11: Configuration initiale du SW-ADM.....	21
Tableau 12: Les interfaces de switch SW-ADM.....	22
Tableau 13: Configuration initiale du SW-DEPI .....	23
Tableau 14: Les interfaces de switch SW-DEPI .....	23
Tableau 15: Configuration initiale du SW-GES .....	24
Tableau 16: Les interfaces de switch SW-GES .....	25
Tableau 17: Configuration initiale du DEP-M .....	26
Tableau 18: Les interfaces de switch DEP-M .....	26
Tableau 19: Configuration initiale du DEP-BIB .....	27
Tableau 20: Les interfaces de switch DEP-BIB .....	27
Tableau 27: Spécifications des APs .....	28
Tableau 28: Liste des APs .....	30
Tableau 29: Spécification de Huawei AC6508.....	32
Tableau 30: Configuration de base de l'AC .....	33
Tableau 31: Tableau comparatif des modes de transfert.....	35
Tableau 32: Liste des VLANs .....	35
Tableau 33: Interfaces de l'AC.....	35
Tableau 34: Interfaces Vlanif de l'AC .....	36
Tableau 35: SSIDs configurés .....	36
Tableau 36: VAP profiles .....	37
Tableau 37: Ports du Fortigate 301E .....	39
Tableau 38: Configuration initiale du firewall Fortigate .....	41
Tableau 39: Table de routage.....	42
Tableau 40: Les règles de sécurité.....	43

## Liste des figures

Figure 1: Switch S5720-28X-PWR-LI-AC .....	7
Figure 2: Switch S5730-36C-PWH-HI .....	8
Figure 3: Access Controller Huawei AC6508 .....	8
Figure 4: Access Point Huawei AP4050DN .....	9
Figure 5: Firewall Fortigate 301E .....	9
Figure 6: Architecture globale .....	10
Figure 7: Vue d'ensemble du switch Huawei S5730-36C-PWH-HI .....	11
Figure 8: Architecture core .....	13
Figure 9: Configuration des interfaces XG0/1/1-8 du SW-FD .....	17
Figure 10: Routes statique .....	18
Figure 11: Vue d'ensemble du switch Huawei S5720-28X-PWR-LI-AC .....	19
Figure 12: Architecture LAN .....	21
Figure 13: Déploiement des Fat APs .....	29
Figure 14: Déploiement des Fit APs + AC .....	30
Figure 15: Architecture Wi-Fi .....	32
Figure 16: Architecture WAN .....	40
Figure 17: Configuration des interfaces du firewall .....	41
Figure 18: routes statiques .....	43
Figure 19: Les règles de sécurité .....	43

## I. Introduction

### 1. Cadre du projet

Prologic est un intégrateur du réseau et de sécurité informatique professionnel disposant des compétences, de l'expérience et du personnel qualifié pour exécuter de manière irréprochable les tâches relatives à l'approvisionnement, au pilotage et à la supervision réseau. Il pourra vous fournir des prestations liées à l'intégration, à la virtualisation, à la sauvegarde des données, aux conseils et au support.

Ce présent rapport est rédigé dans le cadre du projet de "la mise en place d'une infrastructure réseau à ISET Mahdia", pour décrire notre solution proposée par l'équipe technique du Prologic afin de répondre aux besoins d'installation du réseau et de sécurité exigée par l'organisme d'ISET pour assurer le bon fonctionnement dans leur environnement.

### 2. Objectif du projet

L'objectif du projet consiste en la mise en place d'une nouvelle infrastructure réseau au profit de l'institut supérieur des études technologiques de Mahdia dans le cadre de la refonte de son infrastructure. Le but de ce projet est d'avoir un réseau interne/externe consolidé, performant et le plus essentiel sécurisé afin de garantir la confidentialité des données circulant le réseau.

### 3. Liste des tâches

Le périmètre du projet s'articule autour des prestations demandées au niveau du cahier des charges à savoir :

- La Livraison, l'installation, la configuration et la mise en place de la nouvelle infrastructure réseau qui fait l'objectif de la refonte.
- La mise en rack, l'installation des modules d'alimentation et le câblage des équipements.
- L'implémentation de nouvelles configurations sur les équipements concernés, à savoir la configuration du switch core, des différents switches access, du firewall et du contrôleur d'accès Wi-Fi.
- Effectuer les opérations de tests préventifs des équipements avant et après les interventions en conformité avec les préconisations du constructeur.

- Assurer les mises à jour Software nécessaires afin de garantir toutes évolutions logicielles et matérielles recommandées par les constructeurs.
- Assurer un transfert de compétences lié à l'ensemble de la configuration faite au cours du projet.
- Rédiger un livrable exigé au niveau du cahier de charges à savoir la rédaction d'un rapport résumant toutes les étapes de mise en place et de configurations.

#### 4. Equipements acquis

Comme première étape dans le projet de “la mise en place d’une infrastructure à ISET Mahdia”, Prologic s’est déplacé au local d’ISET Mahdia pour mettre en place et installer les nouveaux équipements suivants :

- 5 switches access Huawei S5720-LI
- 1 switch core Huawei S5730-SI
- 1 access controller Huawei AC6508
- 24 access points Huawei AP4050DN
- 1 firewall Firewall Fortigate 301E

##### 4.1 Description du switch access S5720-28X-PWR-LI-AC

Le S5720-LI est un commutateur Gigabit Ethernet à économie d'énergie de nouvelle génération qui fournit des ports d'accès GE flexibles et 10 ports de liaison montante GE. S'appuyant sur un matériel hautement performant de nouvelle génération et la plate-forme de routage polyvalente (VRP) de Huawei, le S5720-LI prend en charge la pile intelligente (iStack), la mise en réseau Ethernet flexible et un contrôle de sécurité diversifié. Il offre aux clients un gigabit écologique, facile à gérer, facile à développer et économique pour la solution de bureau. De plus, Huawei personnalise des modèles spécialisés pour répondre aux exigences des clients en fonction de scénarios particuliers.

Ce switch dispose des caractéristiques suivantes :

- 24 ports Ethernet 10/100/1000 Base-T, 4 ports 10 Gigabit SFP+
- Bloc d'alimentation AC, prenant en charge l'alimentation redondante (RPS)
- PoE+



- Performances de transfert: 108 Mpps
- Capacité de commutation: 336 Gbit/s



Figure 1: Switch S5720-28X-PWR-LI-AC

#### 4.2 Description du switch core S5730-36C-PWH-HI

Le S5730-36C-PWH-HI est un switch Huawei de la série S5730-HI, fournissant 24 ports 10/100/1000 BASE-T, 4 ports 10GE SFP +, 1 emplacement d'extension, PoE ++, sans module d'alimentation. Les switches Gigabit Ethernet Huawei S5730-HI sont agiles de nouvelle génération développés par Huawei qui fournissent un accès gigabit complet fixe et des interfaces de liaison montante 10GE ainsi qu'un ou deux emplacements pour l'extension d'interface de liaison montante. Ces switches sont développés sur la base de la plate-forme de routage polyvalente (VRP) de Huawei pour implémenter la définition de logiciel et le changement de service à la demande. Avec les services et la convergence du réseau au cœur, les switches fournissent la fonction de mobilité gratuite pour garantir une expérience utilisateur cohérente. La fonction Super Virtual Fabric (SVF) virtualise l'ensemble du réseau en un seul appareil. En outre, ces switches prennent en charge un réseau Ethernet flexible, des solutions de tunnel VPN complètes, diverses méthodes de contrôle de sécurité, un déploiement intelligent et des opérations et une maintenance simples. Les switches de la série S5730-HI sont les meilleurs choix pour les couches d'accès ou d'agrégation des réseaux de campus de moyenne et grande taille et la couche centrale des réseaux de petits campus.

Ce switch dispose des caractéristiques suivantes :

- Ports 24 ports Ethernet 10/100/1000 Base-T, 10 ports Gigabit 4 ports SFP+
- Alimentation de secours 1+1, avec alimentation AC, DC ou AC + DC
- PoE++



- Capacité de commutation: 758 Gbit/s



Figure 2: Switch S5730-36C-PWH-HI

#### 4.3 Description du access controller Huawei AC6508

L'AC 6508 est un contrôleur d'accès sans fil fixe (AC) de petite capacité pour les petites et moyennes entreprises. Il peut gérer jusqu'à 256 points d'accès (AP) et fournit une fonction de commutation GE, permettant un accès intégré pour les utilisateurs filaires et sans fil. L'AC présente une évolutivité élevée et offre aux utilisateurs une flexibilité considérable dans la configuration du nombre de points d'accès gérés. Lorsqu'il est utilisé avec les points d'accès 802.11ax, 802.11ac et 802.11n de la série complète de Huawei, l'AC6508 peut être utilisé pour construire des réseaux de campus de petite et moyenne taille, des réseaux de bureau d'entreprise, des réseaux métropolitains sans fil (MAN) et des réseaux de couverture hotspot.



Figure 3: Access Controller Huawei AC6508

#### 4.4 Description du access point Huawei AP4050DN

Huawei AP4050DN est un point d'accès (AP) de nouvelle génération qui prend en charge 802.11ac Wave 2, 2 x 2 MIMO et deux flux spatiaux. Le point d'accès est conforme aux protocoles 802.11n et 802.11ac et peut fournir un accès gigabit aux utilisateurs sans fil, améliorant considérablement l'expérience utilisateur. L'AP4050DN est applicable aux petites et moyennes entreprises, aéroports, gares, stades, cafés et centres de divertissement.



Figure 4: Access Point Huawei AP4050DN

#### 4.5 Description du Firewall Fortigate 301E

La série FortiGate 300E offre des capacités de firewall de nouvelle génération pour les moyennes et grandes entreprises, avec la flexibilité d'être déployée sur le campus ou dans la succursale de l'entreprise. Il fait une protection contre les cybers menaces grâce aux performances élevées, à l'efficacité de la sécurité et à la visibilité approfondie alimentés par un processeur de sécurité.

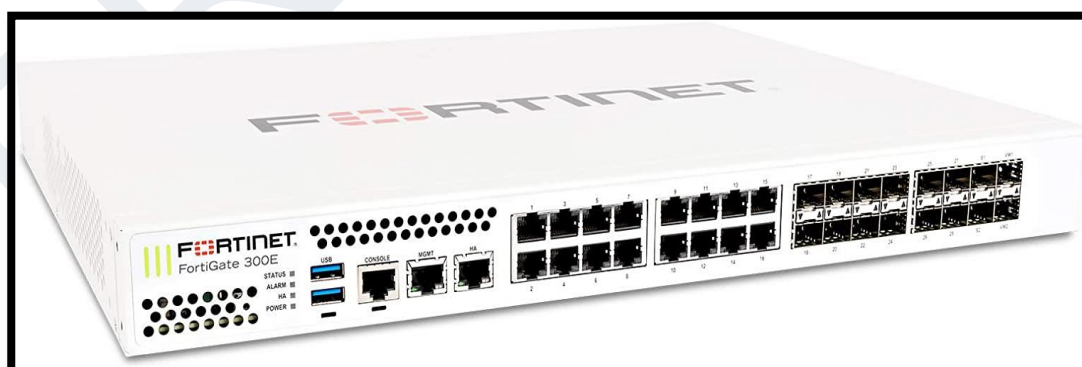


Figure 5: Firewall Fortigate 301E

## II. High Level Design

High Level Design, dont l'abréviation est HLD, est la conception globale de l'architecture du réseau. Cette norme décrit la relation entre les différents nœuds et le flux de trafic entre eux.

La figure suivante présente la nouvelle architecture mise en place à ISET Mahdia.

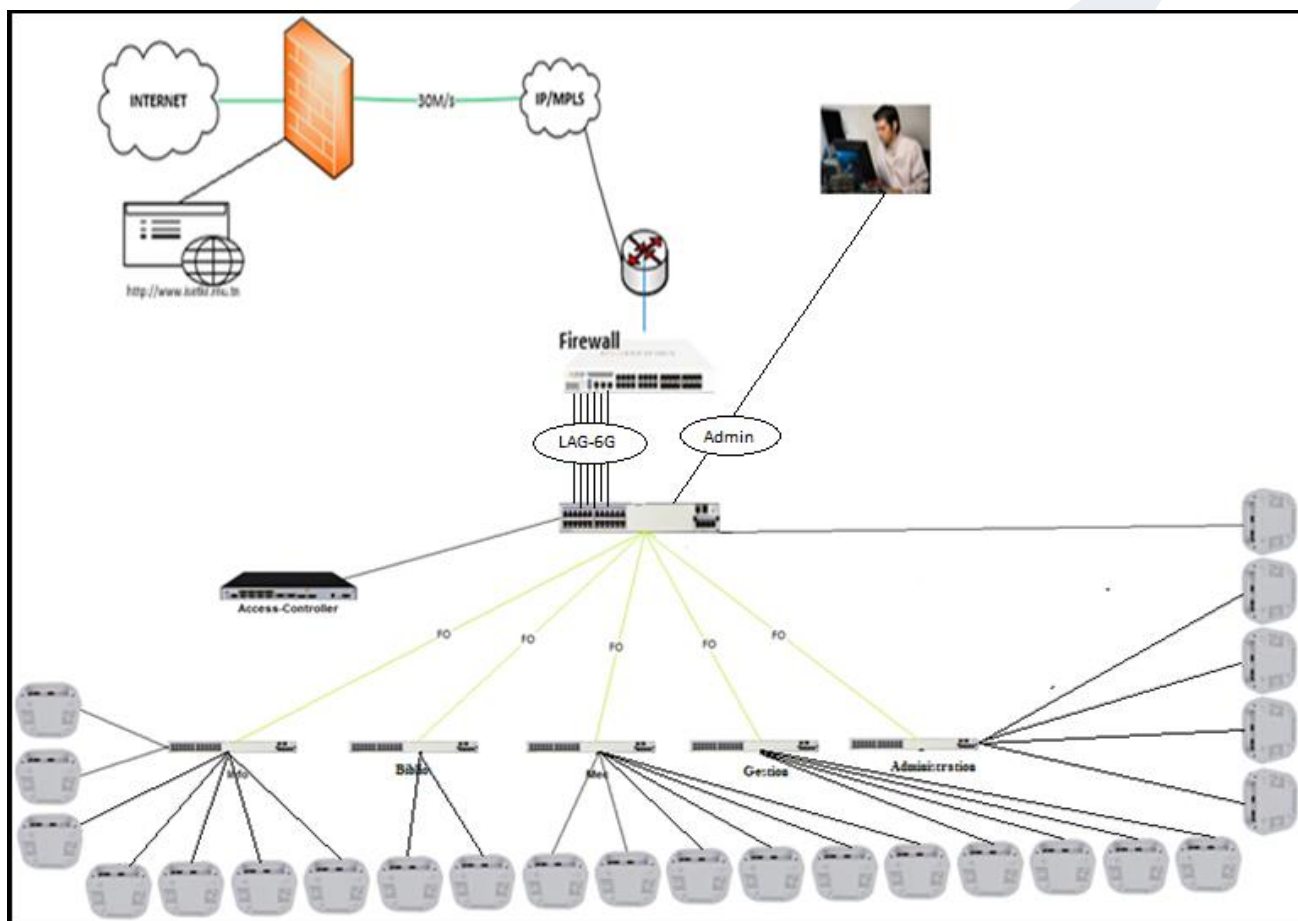


Figure 6: Architecture globale

L'ancien réseau d'ISET était un réseau plat et vulnérable. Il n'était pas segmenté où nous avons trouvé que les serveurs et le réseau LAN étaient dans la même plage réseau. Les équipements réseaux et informatiques étaient obsolètes. Nous avons trouvé un manque au niveau de composants de sécurité et de la documentation qui était insuffisante pour ne pas dire inexistante.

Avec la refonte du réseau, nous avons ajouté une couche de sécurité grâce au Firewall. Nous avons mis en place de nouveaux équipements, que vous trouvez leurs descriptions détaillées ci-dessous, dans le but de segmenter le réseau. Aussi, nous avons fait des liaisons

optiques entre le switch core et les switches access afin d'augmenter la capacité et la performance du réseau. Et nous avons installé un réseau Wi-Fi pour étendre la couverture et faciliter la mobilité entre les différents départements d'ISET.

### III. Low Level Design du Switch Core

#### 1. Spécifications du switch Huawei S5730-36C-PWH-HI

Dans l'infrastructure d'ISET, nous avons utilisé un seul switch Huawei S5730-36C-PWH-HI qui joue le rôle du switch core ou fédérateur et qui va assurer l'agrégation de tout flux venant des couches inférieures.

Vous trouvez, ci-dessous, la structure (front/back panels) du switch Huawei S5730-36C-PWH-HI avec un tableau décrivant les différents ports et modules du switch.

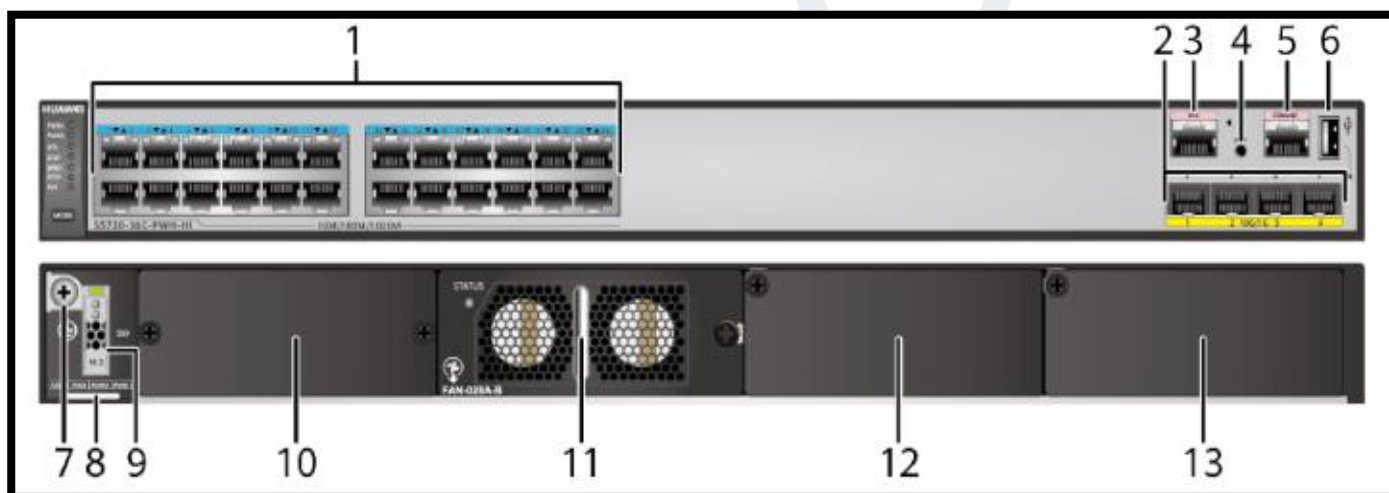


Figure 7: Vue d'ensemble du switch Huawei S5730-36C-PWH-HI

Tableau 1: Description des ports/modules du switch core

Numéro de port / module	Description
1	24 ports PoE++ 10/100 /1000 BASE-T
2	4 ports 10GE SFP+ Les modules et câbles applicables sont: - Module optique GE - Module optique GE-CWDM - Module optique GE-DWDM - Module cuivre GE - Module optique 10GE SFP+ - Module optique 10GE-CWDM - Module optique 10GE-DWDM

	<ul style="list-style-type: none"> <li>- Câbles en cuivre haute vitesse SFP+ 1m, 3m, 5m et 10m</li> <li>- Câbles AOC 3m et 10m</li> <li>- Câbles en cuivre d'empilage dédiés SFP+ de 0,5m et 1,5m (utilisés pour l'empilage sans configuration)</li> </ul>
3	Port de management ETH
4	Bouton PNP <b>NB:</b> Pour restaurer les paramètres d'usine et réinitialiser le switch, maintenez le bouton enfoncé pendant au moins 6 secondes. La réinitialisation entraînera une interruption de service. Soyez prudent lorsque vous appuyez sur le bouton PNP.
5	Port de console
6	Port USB
7	Vis de terre <b>NB:</b> Il est utilisé avec un câble de masse.
8	Étiquette ESN <b>NB:</b> Vous pouvez le dessiner pour afficher l'adresse ESN et MAC du switch.
9	Emplacement pour carte SSD <b>NB:</b> Carte SSD enfichable prise en charge: - SSD-240Go
10	Fente pour carte arrière <b>NB:</b> Cartes prises en charge: <ul style="list-style-type: none"> <li>- ES5D21Q02Q00</li> <li>- ES5D21X08T00</li> <li>- ES5D21X08S00</li> </ul>
11	Emplacement du ventilateur <b>NB:</b> Module de ventilateur applicable: <ul style="list-style-type: none"> <li>- FAN-028A-B</li> </ul>
12	Emplacement 1 du module d'alimentation <b>NB:</b> Modules d'alimentation applicables: <ul style="list-style-type: none"> <li>- Module d'alimentation PoE 500 W CA</li> <li>- Module d'alimentation PoE DC 650 W</li> <li>- Module d'alimentation PoE CA de 1150 W</li> <li>- Module d'alimentation PoE 1000 W CA (applicable dans V200R013C00 et versions ultérieures)</li> </ul>
13	Emplacement 2 du module d'alimentation <b>NB:</b> Les mêmes modules d'alimentation applicables dans l'emplacement 1.

Dans le tableau ci-dessous, vous trouvez les différentes caractéristiques techniques principales du switch core :

Tableau 2: Spécifications du switch Huawei S5730-36C-PWH-HI

Spécification	Valeur
<b>Interfaces</b>	24 x Ethernet 10/100/1000 ports, 8 x 10GE SFP+
<b>Performance du transfert</b>	240 Mpps
<b>Capacité du tableau d'adresses MAC</b>	32000 adresses MAC

<b>Capacité de commutation</b>	758 Gbit/s
<b>Flash</b>	128 MB
<b>RAM</b>	512 MB

## 2. Architecture Core

L'architecture core forme la partie centrale du réseau qui est constituée du switch fédérateur, le contrôleur d'accès WIFI, le Firewall et les différentes parties du réseau local d'ISET. Nous avons fait une agrégation de liens afin de permettre le regroupement de plusieurs interfaces physiques en une seule interface logique. Ce regroupement est configuré entre le switch fédérateur Huawei et le firewall Fortigate afin d'augmenter le débit et la bande passante et de faire une redondance des liens pour assurer une haute disponibilité.

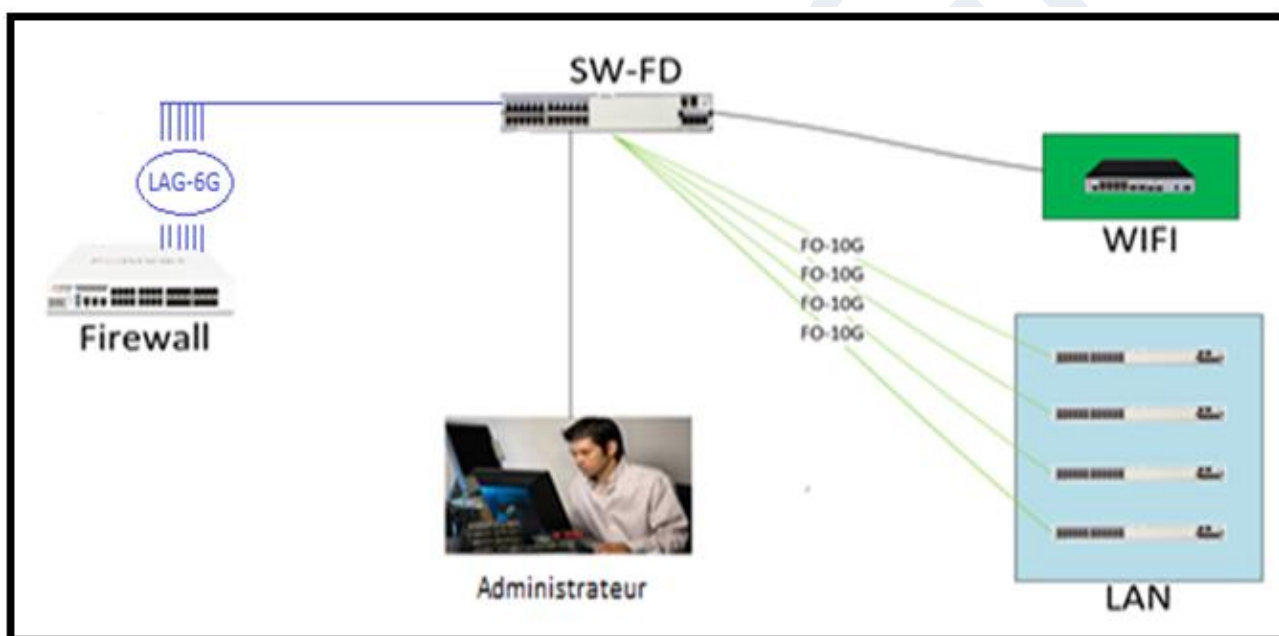


Figure 8: Architecture core

## 3. Configuration initiale

Le tableau suivant présente la configuration de base du switch fédérateur à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 3: Configuration initiale du SW-FD

Attributs du switch à configurer	Valeur
<b>Nom</b>	SW-FD
<b>Login / Password</b>	admin / Admin@123\$
<b>Vlan de management</b>	vlan 99 (name Devices-MGMT)
<b>Adresse IP de management</b>	172.16.99.2/24
<b>Méthodes de management</b>	Telnet, http, ssh, terminal



Le tableau suivant regroupe la liste des VLANs configurés sur le switch fédérateur.

Tableau 4: Liste des VLANs du SW-FD

VLAN Name	VLAN ID	Adresse réseau / masque	Description
<b>ADMINISTRATION</b>	10	172.16.10.0/24	vlan pour les personnes
<b>DPT-TI</b>	20	172.16.20.0/24	vlan wired pour DPT-TI
<b>DPT-GESTION</b>	30	172.16.30.0/24	vlan wired pour DPT-GESTION
<b>DPT-GM</b>	40	172.16.40.0/24	vlan wired pour DPT-GM
<b>WAN</b>	41	-	vlan WAN de bibliotheque
<b>BIB</b>	50	172.16.50.0/24	vlan wired pour le bibliotheque
<b>-</b>	60	-	vlan wired pour Birouni
<b>Finance</b>	70	-	
<b>NVR</b>	80	172.16.80.0/24	vlan wired pour NVR les cameras
<b>APs</b>	90	-	vlan wifi pour les APs
<b>Devices-MGMT</b>	99	172.16.99.0/24	vlan pour MGMT des equipements
<b>WLAN-ENSG</b>	120	172.16.120.0/24	vlan WIFI pour les enseignants
<b>Wifi-etudiant_TI</b>	130	172.16.130.0/24	vlan wifi pour les etudiants
<b>Wifi-etudiant_GES</b>	131	172.16.131.0/24	
<b>Wifi-etudiant_MEC</b>	132	172.16.132.0/24	
<b>Wifi-etudiant_BIB</b>	133	172.16.133.0/24	
<b>WLAN-Personnel</b>	140	172.16.140.0/24	vlan wifi pour les personnels
<b>GUEST</b>	150	172.16.150.0/24	
<b>SERV</b>	160	-	vlan pour les serveurs
<b>inetrconnect</b>	1300	20.20.20.2/30	vlan interconnect

## 4. Configuration des interfaces

Les interfaces de switch peuvent être configurées en deux modes selon le trafic qui les traversent:

- Mode access : sert à transporter le trafic d'un seul vlan. Par défaut, ce mode transportera le trafic du vlan natif (VLAN 1). Si les ports du switch sont affectés comme ports access, il peut être considéré comme les ports du switch appartenant à un seul domaine de diffusion. Tout trafic arrivant sur ces ports est considéré comme appartenant au VLAN attribué au port. Une liaison access se fait entre le switch et un périphérique terminal.

- Mode Trunk : sert à acheminer le trafic de plus d'un VLAN. Il fait un grand avantage car pour transporter le trafic de groupe de VLAN, un seul port de switch peut être suffisant et donne une grande utilité si l'utilisateur souhaite échanger du trafic entre plusieurs switches ayant plus d'un vlan configuré. Une liaison trunk s'établit entre le switch et un autre équipement du réseau.



Le tableau suivant regroupe toutes les interfaces configurées du switch core.

Tableau 5: Liste des interfaces du SW-FD

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
<b>GigabitEthernet 0/0/1</b>	Trunk	-	-	Vers le port 1 du firewall (Agrégation des liens)
<b>GigabitEthernet 0/0/2</b>	Trunk	-	-	Vers le port 2 du firewall (Agrégation des liens)
<b>GigabitEthernet 0/0/3</b>	Trunk	-	-	Vers le port 3 du firewall (Agrégation des liens)
<b>GigabitEthernet 0/0/4</b>	Trunk	-	-	Vers le port 4 du firewall (Agrégation des liens)
<b>GigabitEthernet 0/0/5</b>	Trunk	-	-	Vers le port 5 du firewall (Agrégation des liens)
<b>GigabitEthernet 0/0/6</b>	Trunk	-	-	Vers le port 6 du firewall (Agrégation des liens)
<b>GigabitEthernet 0/0/7</b>	Access	41	-	Vers port 7 du Firewall (wan)
<b>GigabitEthernet 0/0/8</b>	-	-	-	Vide
<b>GigabitEthernet 0/0/9</b>	-	-	-	Vide
<b>GigabitEthernet 0/0/10</b>	Access	99	-	Port management
<b>GigabitEthernet 0/0/11</b>	Access	20	-	Vlan 20 (port test)
<b>GigabitEthernet 0/0/12</b>	-	-	-	vide
<b>GigabitEthernet 0/0/13</b>	-	-	-	vide
<b>GigabitEthernet 0/0/14</b>	-	-	-	vide
<b>GigabitEthernet 0/0/15</b>	-	-	-	vide
<b>GigabitEthernet 0/0/16</b>	-	-	-	vide
<b>GigabitEthernet 0/0/17</b>	-	-	-	vide
<b>GigabitEthernet 0/0/18</b>	-	-	-	vide
<b>GigabitEthernet 0/0/19</b>	-	-	-	Vide
<b>GigabitEthernet 0/0/20</b>	-	-	-	vide
<b>GigabitEthernet 0/0/21</b>	-	-	-	vide

<b>GigabitEthernet 0/0/22</b>	Access	30	-	Vlan 30 (port test)
<b>GigabitEthernet 0/0/23</b>	Trunk	90 99 120 130 133 140 150	90	AP salle serveur (Ap-serv)
<b>GigabitEthernet 0/0/24</b>	Trunk	90 99 150	-	Vers le port 1 de l'AC
<b>XGigabitEthernet 0/0/1</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/2</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/3</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/4</b>	-	-	-	vide
<b>XGigabitEthernet 0/1/1</b>	Trunk	ALL	-	Vers le switch access de l'administration
<b>XGigabitEthernet 0/1/2</b>	Trunk	ALL	-	Vers le switch access du département Informatique
<b>XGigabitEthernet 0/1/3</b>	Trunk	ALL	-	Vers le switch access du département Gestion
<b>XGigabitEthernet 0/1/4</b>	Trunk	ALL	-	Vers le switch access du département Mécanique
<b>XGigabitEthernet 0/1/5</b>	Trunk	ALL	-	Vers le switch access de la Bibliothèque
<b>XGigabitEthernet 0/1/6</b>	-	-	-	vide
<b>XGigabitEthernet 0/1/7</b>	-	-	-	vide
<b>XGigabitEthernet 0/1/8</b>	-	-	-	vide

Le tableau suivant regroupe toutes les interfaces Vlanif configurées du switch core.

Tableau 6: Liste des interfaces Vlanif du SW-FD

Vlanif	Adresse IP/Masque	DHCP	Description
<b>80</b>	172.16.80.1/24	non	NVR
<b>99</b>	172.16.99.2/24	non	Devices-MGMT
<b>1300</b>	20.20.20.2/30	non	interconnect

## 5. Configuration du GVRP

Pour faciliter et rendre dynamique la configuration des VLANs dans le reste des switches, nous avons utilisé le protocole GVRP.

Le protocole d'enregistrement GARP VLAN (GVRP) est une application du GARP (Generic Attribute Registration Protocol) qui fournit un service d'enregistrement VLAN au moyen de la configuration dynamique (enregistrement) et de la distribution des informations d'appartenance au VLAN. GVRP réduit les risques d'erreurs dans la configuration du VLAN en fournissant automatiquement la cohérence des ID VLAN sur le réseau. GVRP sert à propager automatiquement les VLANs vers d'autres appareils compatibles GVRP, sans avoir besoin de configurer manuellement les VLANs sur chaque équipement. De plus, si la configuration VLAN sur un périphérique se change, GVRP change automatiquement les configurations VLAN des périphériques affectés.

Le GVRP est activé globalement sur le switch core et il est configuré le protocole GVRP sur les interfaces liées au switches d'accès (de l'interface XGigabitEthernet0/1/1 jusqu'à l'interface XGigabitEthernet0/1/8).

La figure suivante montre le résultat de la configuration des interfaces XG0/1/1-5.

```
#
interface XGigabitEthernet0/1/1
  port link-type trunk
  port trunk allow-pass vlan 2 to 4094
  gvrp
#
interface XGigabitEthernet0/1/2
  port link-type trunk
  port trunk allow-pass vlan 2 to 4094
  gvrp
#
interface XGigabitEthernet0/1/3
  port link-type trunk
  port trunk allow-pass vlan 2 to 4094
  gvrp
#
interface XGigabitEthernet0/1/4
  port link-type trunk
  port trunk allow-pass vlan 2 to 4094
  gvrp
#
interface XGigabitEthernet0/1/5
  port link-type trunk
  port trunk allow-pass vlan 2 to 4094
  gvrp
#
```

Figure 9: Configuration des interfaces XG0/1/1-8 du SW-FD

## 6. Configuration du service DHCP

Le serveur DHCP sert à attribuer d'une façon dynamique les adresses IP et d'autres informations de configuration réseau (passerelle, DNS) aux utilisateurs finaux. L'utilisateur n'a plus besoin de saisir ces informations manuellement, le serveur s'en charge. Au niveau du switch fédérateur, nous avons activé le DHCP sur tous les VLANs (wired + wireless) sauf les VLANs de management et des APs qui est configuré au niveau de l'AC.

Tableau 7: Configuration du DHCP

VLAN	Adresse réseau	Gateway / Masque	DHCP	DNS
10	172.16.10.0/24	172.16.10.1/24	oui	8.8.8.8
20	172.16.20.0/24	172.16.20.1/24	oui	8.8.8.8
30	172.16.30.0/24	172.16.30.1/24	oui	8.8.8.8
40	172.16.40.0/24	172.16.40.1/24	oui	8.8.8.8
50	172.16.50.0/24	172.16.50.1/24	oui	8.8.8.8
120	172.16.120.0/24	172.16.120.1/24	oui	8.8.8.8
130	172.16.130.0/24	172.16.130.1/24	oui	8.8.8.8
131	172.16.131.0/24	172.16.131.1/24	oui	8.8.8.8
132	172.16.132.0/24	172.16.132.1/24	oui	8.8.8.8
133	172.16.133.0/24	172.16.133.1/24	oui	8.8.8.8
140	172.16.140.0/24	172.16.140.1/24	oui	8.8.8.8
150	172.16.150.0/24	172.16.150.1/24	oui	8.8.8.8

## 7. Configuration de route statique

Nous avons configuré deux routes statique la première va diriger tout le trafic entrant au switch core vers le firewall Fortigate et la deuxième du FortiClient vers le firewall.

```
ip route-static 0.0.0.0 0.0.0.0 20.20.20.1
ip route-static 10.212.134.0 255.255.255.0 20.20.20.1
```

Figure 10: Routes statique

## 8. Configuration du protocole RSTP

Le protocole RSTP (Rapid Spanning Tree Protocol) est un protocole réseau qui garantit une topologie sans boucle pour les réseaux Ethernet. De nos jours, c'est une solution populaire pour implémenter des réseaux redondants. Ce protocole est intégré à l'IEEE 802.1Q-2014. RSTP fournit une convergence plus rapide que 802.1D STP lorsque des changements de topologie se produisent. RSTP définit trois états de port: suppression, apprentissage et transfert et cinq rôles de port: racine, désigné, alternatif, de sauvegarde et désactivé.

Nous avons configuré le protocole STP en mode RSTP comme suit :

```
#
stp mode rstp
#
```

#### IV. Low Level Design des Switches Access

##### 1. Spécifications du switch Huawei S5720-28X-PWR-LI-AC

Dans l'infrastructure d'ISET, nous avons mis en place 5 switches Huawei S5720-28X-PWR-LI-AC qui forment la couche d'accès du réseau. Ils sont distribués sur les différents départements comme suit :

Tableau 8: Liste des switches access

Département	Switch	Nom Switch
Administration	Huawei S5720-LI	SW-ADM
Informatique	Huawei S5720-LI	SW-DEPI
Gestion	Huawei S5720-LI	SW-GES
Mécanique	Huawei S5720-LI	DEP-M
Bibliothèque	Huawei S5720-LI	DEP-BIB

Vous trouvez, ci-dessous, la structure (front/back panels) du switch Huawei S5720-28X-PWR-LI-AC avec un tableau décrivant les différents ports et modules du switch.

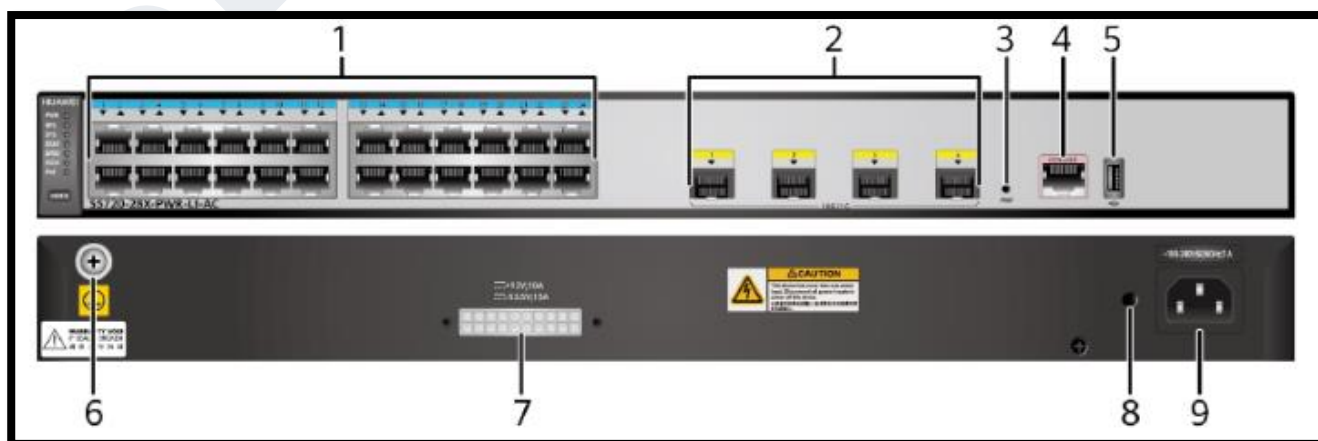


Figure 11: Vue d'ensemble du switch Huawei S5720-28X-PWR-LI-AC

Tableau 9: Description des ports/modules du switch access

Numéro de port / module	Description
1	24 ports PoE+ 10/100 /1000 BASE-T
2	4 ports 10GE SFP+ Les modules et câbles applicables sont: - Module optique GE - Module optique GE-CWDM - Module optique GE-DWDM - Module cuivre GE - Module optique 10GE SFP+ - Module optique 10GE-CWDM - Module optique 10GE-DWDM - Câbles en cuivre haute vitesse SFP+ 1m, 3m, 5m et 10m - Câbles AOC 3m et 10m - Câbles en cuivre d'empilage dédiés SFP+ de 0,5m et 1,5m (utilisés pour l'empilage sans configuration)
3	Bouton PNP <b>NB:</b> Pour restaurer les paramètres d'usine et réinitialiser le switch, maintenez le bouton enfoncé pendant au moins 6 secondes. La réinitialisation entraînera une interruption de service. Soyez prudent lorsque vous appuyez sur le bouton PNP.
4	Port de console
5	Port USB
6	Vis de terre <b>NB:</b> Il est utilisé avec un câble de masse.
7	Prise RPS <b>NB:</b> Il est utilisé avec un câble RPS, qui n'est pas remplaçable à chaud.
8	Prise pour sangle de verrouillage du câble d'alimentation CA <b>NB:</b> La sangle de verrouillage du câble d'alimentation CA n'est pas fournie avec le commutateur.
9	Prise secteur <b>NB:</b> Il est utilisé avec un câble d'alimentation CA.

Dans le tableau ci-dessous, vous trouvez les différentes caractéristiques techniques principales des switches access:

Tableau 10: Spécifications du switch Huawei S5720-28X-PWR-LI-AC

Spécification	Valeur
Interfaces	24 x Ethernet 10/100/1000 ports, 4 x 10GE SFP+
Performance du transfert	96 Mpps
Capacité du tableau d'adresses MAC	16000 adresses MAC
Capacité de commutation	336 Gbit/s
Flash	128 MB
RAM	256 MB

## 2. Architecture LAN

Les switches facilitent le partage des ressources en connectant ensemble tous les périphériques, y compris les ordinateurs, les imprimantes et les serveurs, dans un réseau de petite entreprise. Grâce au switch, ces appareils connectés peuvent partager des informations et se parler, peu importe où ils se trouvent dans un bâtiment ou sur un campus.

Dans ce cadre, notre équipe a mis en place 5 switches access. Les 5 switches access sont reliés au switch fédérateur ou core par les liaisons fibres de 10GE. La figure suivante décrit l'architecture du réseau local LAN.

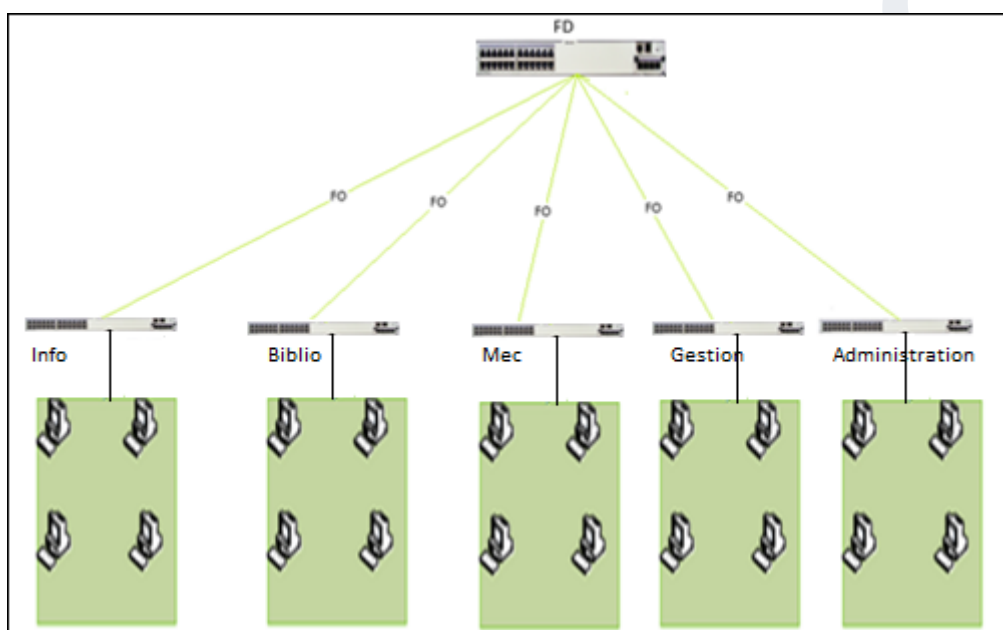


Figure 12: Architecture LAN

## 3. Switch Access SW-ADM

### 3.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch SW-ADM à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 11: Configuration initiale du SW-ADM

Attributs du switch à configurer	Valeur
<b>Nom</b>	SW-ADM
<b>Login / Password</b>	admin / Admin@123\$
<b>Vlan de management</b>	vlan 99 (name Devices-MGMT)
<b>Adresse IP de management</b>	172.16.99.4/24
<b>Méthodes de management</b>	Telnet, ssh, http, terminal



### 3.2 Configuration des interfaces

Tableau 12: Les interfaces de switch SW-ADM

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
<b>Vlanif</b>	-	99	-	Management (172.16.99.4/24)
<b>GigabitEthernet 0/0/1</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/2</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/3</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/4</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/5</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/6</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/7</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/8</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/9</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/10</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/11</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/12</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/13</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/14</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/15</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/16</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/17</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/18</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/19</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/20</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/21</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/22</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/23</b>	Access	10	-	Vide
<b>GigabitEthernet 0/0/24</b>	Access	10	-	Vide
<b>XGigabitEthernet 0/0/1</b>	Trunk	ALL	-	Vers le SW-FD
<b>XGigabitEthernet 0/0/2</b>	-	-	-	Vide
<b>XGigabitEthernet 0/0/3</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/4</b>	-	-	-	-

## 4. Switch Access SW-DEPI

### 4.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch SW-DEPI à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 13: Configuration initiale du SW-DEPI

Attributs du switch à configurer	Valeur
<b>Nom</b>	SW-DEPI
<b>Login / Password</b>	admin / Admin@123\$
<b>Vlan de management</b>	vlan 99 (name Devices-MGMT)
<b>Adresse IP de management</b>	172.16.99.5/24
<b>Méthodes de management</b>	Telnet, ssh, http, terminal

### 4.2 Configuration des interfaces

Tableau 14: Les interfaces de switch SW-DEPI

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
<b>Vlanif</b>	-	99	-	Management (172.16.99.5/24)
<b>GigabitEthernet 0/0/1</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/2</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/3</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/4</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/5</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/6</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/7</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/8</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP

<b>GigabitEthernet 0/0/9</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/10</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/11</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/12</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/13</b>	Trunk	90 99 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/14</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/15</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/16</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/17</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/18</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/19</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/20</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/21</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/22</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/23</b>	Access	20	-	vide
<b>GigabitEthernet 0/0/24</b>	Access	20	-	vide
<b>XGigabitEthernet 0/0/1</b>	Trunk	ALL	-	Vers le SW-FD
<b>XGigabitEthernet 0/0/2</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/3</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/4</b>	-	-	-	vide

## 5. Switch Access SW-GES

### 5.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch SW-GES à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 15: Configuration initiale du SW-GES

Attributs du switch à configurer	Valeur
<b>Nom</b>	SW-GES
<b>Login / Password</b>	admin / Admin@123\$
<b>Vlan de management</b>	vlan 99 (name Devices-MGMT)
<b>Adresse IP de management</b>	172.16.99.6/24
<b>Méthodes de management</b>	Telnet, http, ssh

## 5.2 Configuration des interfaces

Tableau 16: Les interfaces de switch SW-GES

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
<b>Vlanif</b>	-	99	-	Management (172.16.99.6/24)
<b>GigabitEthernet 0/0/1</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/2</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/3</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/4</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/5</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/6</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/7</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/8</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/9</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/10</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/11</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/12</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/13</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/14</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/15</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/16</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/17</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/18</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/19</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/20</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/21</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/22</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/23</b>	Access	30	-	vide
<b>GigabitEthernet 0/0/24</b>	Access	30	-	vide
<b>XGigabitEthernet 0/0/1</b>	Trunk	ALL	-	Vers le SW-FD
<b>XGigabitEthernet 0/0/2</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/3</b>	-	-	-	vide
<b>XGigabitEthernet 0/0/4</b>	-	-	-	vide

## 6. Switch Access DEP-M

### 6.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch DEP-M à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 17: Configuration initiale du DEP-M

Attributs du switch à configurer	Valeur
<b>Nom</b>	DEP-M
<b>Login / Password</b>	admin / Admin@123\$
<b>Vlan de management</b>	vlan 99 (name Devices-MGMT)
<b>Adresse IP de management</b>	172.16.99.7/24
<b>Méthodes de management</b>	Telnet, http, terminal, ssh

### 6.2 Configuration des interfaces

Tableau 18: Les interfaces de switch DEP-M

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
<b>Vlanif</b>	-	99	-	Management (172.16.99.7/24)
<b>GigabitEthernet 0/0/1</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/2</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/3</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/4</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/5</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/6</b>	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
<b>GigabitEthernet 0/0/7</b>	Access	40	-	vide
<b>GigabitEthernet 0/0/8</b>	Access	40	-	vide
<b>GigabitEthernet 0/0/9</b>	Access	40	-	vide
<b>GigabitEthernet 0/0/10</b>	Access	40	-	vide
<b>GigabitEthernet 0/0/11</b>	Access	40	-	vide
<b>GigabitEthernet 0/0/12</b>	Access	40	-	vide

GigabitEthernet 0/0/13	Access	40	-	vide
GigabitEthernet 0/0/14	Access	40	-	vide
GigabitEthernet 0/0/15	Access	40	-	vide
GigabitEthernet 0/0/16	Access	40	-	vide
GigabitEthernet 0/0/17	Access	40	-	vide
GigabitEthernet 0/0/18	Access	40	-	vide
GigabitEthernet 0/0/19	Access	40	-	vide
GigabitEthernet 0/0/20	Access	40	-	vide
GigabitEthernet 0/0/21	Access	40	-	vide
GigabitEthernet 0/0/22	Access	40	-	vide
GigabitEthernet 0/0/23	Access	40	-	vide
GigabitEthernet 0/0/24	Access	40	-	vide
XGigabitEthernet 0/0/1	Trunk	ALL	-	Vers le SW-FD
XGigabitEthernet 0/0/2	-	-	-	vide
XGigabitEthernet 0/0/3	-	-	-	vide
XGigabitEthernet 0/0/4	-	-	-	vide

## 7. Switch Access DEP-BIB

### 7.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch DEP-BIB à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 19: Configuration initiale du DEP-BIB

Attributs du switch à configurer	Valeur
Nom	DEP-BIB
Login / Password	admin / Admin@123\$
Vlan de management	vlan 99 (name Devices-MGMT)
Adresse IP de management	172.16.99.8/24
Méthodes de management	Telnet, http, terminal, ssh

### 7.2 Configuration des interfaces

Tableau 20: Les interfaces de switch DEP-BIB

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	99	-	Management (172.16.99.8/24)
GigabitEthernet 0/0/1	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
GigabitEthernet 0/0/2	Trunk	90 120 130 131 132 133 140 150	90	Vers AP
GigabitEthernet 0/0/3	Access	50	-	Vide

GigabitEthernet 0/0/4	Access	50	-	Vide
GigabitEthernet 0/0/5	Access	50	-	Vide
GigabitEthernet 0/0/6	Access	50	-	Vide
GigabitEthernet 0/0/7	Access	50	-	Vide
GigabitEthernet 0/0/8	Access	50	-	Vide
GigabitEthernet 0/0/9	Access	50	-	Vide
GigabitEthernet 0/0/10	Access	50	-	Vide
GigabitEthernet 0/0/11	Access	50	-	Vide
GigabitEthernet 0/0/12	Access	50	-	Vide
GigabitEthernet 0/0/13	Access	50	-	Vide
GigabitEthernet 0/0/14	Access	50	-	Vide
GigabitEthernet 0/0/15	Access	50	-	Vide
GigabitEthernet 0/0/16	Access	50	-	Vide
GigabitEthernet 0/0/17	Access	50	-	Vide
GigabitEthernet 0/0/18	Access	50	-	Vide
GigabitEthernet 0/0/19	Access	50	-	Vide
GigabitEthernet 0/0/20	Access	50	-	Vide
GigabitEthernet 0/0/21	Access	50	-	Vide
GigabitEthernet 0/0/22	Access	50	-	Vide
GigabitEthernet 0/0/23	Access	50	-	Vide
GigabitEthernet 0/0/24	Access	41	-	Vide
XGigabitEthernet 0/0/1	Trunk	ALL	-	Vers le SW-FD
XGigabitEthernet 0/0/2	-	-	-	Vide
XGigabitEthernet 0/0/3	-	-	-	Vide
XGigabitEthernet 0/0/4	-	-	-	Vide

## v. Low Level Design de l'Access Point

### 1. Spécifications du point d'accès Huawei AP4050DN

Avec un point d'accès sans fil (AP), nous pouvons facilement connecter plusieurs appareils pour des connexions sans fil avec une meilleure commodité et une plus grande flexibilité. En tant que l'un des éléments clés de la construction de réseaux sans fil, le choix des points d'accès est crucial en fonction des différents besoins des utilisateurs. Au sein de l'infrastructure d'ISSET, nous avons mis en place 24 APs de la marque Huawei du modèle AP4050DN et dont les spécifications comme suit :

Tableau 21: Spécifications des APs

Spécification	Valeur
<b>Dimensions (H x L x P)</b>	35 mm x 170 mm x 170 mm
<b>Entrée d'alimentation</b>	12 V $\pm$ 10% Alimentation PoE: conforme à la norme IEEE 802.3af/at
<b>Consommation électrique maximale</b>	12,1 W <b>NB:</b> la consommation électrique maximale réelle dépend des lois et réglementations locales
<b>Température de fonctionnement</b>	-10°C à +50°C



Type d'antenne	Antennes bi-bande omnidirectionnelles intégrées
Nombre maximum d'utilisateurs simultanés	≤ 512
Puissance d'émission maximale	2,4 GHz: 23 dBm (puissance combinée) 5 GHz: 23 dBm (puissance combinée) <b>NB:</b> la puissance d'émission réelle dépend des lois et réglementations locales
MIMO	flux spatiaux 2 x 2: 2
Protocoles radio	802.11a/b/g/n/ac/ac Wave 2
Débit maximum	1,267 Gbit/s

## 2. Liste des APs

Les point d'accès peuvent fonctionner en mode Fat, Fit ou Cloud. Par défaut, un AP fonctionne en mode Fit.

La différence la plus visible entre un AP Fat et un AP Fit réside dans le port WAN. Fat AP possède le port WAN qui est facile à dire. En outre, Fat AP qui possède à la fois des ports WAN et LAN peut prendre en charge des fonctions de sécurité telles que le serveur DHCP, le DNS, le clonage d'adresses MAC, l'accès VPN et le pare-feu. En tant que périphérique réseau pouvant fonctionner indépendamment, le Fat AP peut implémenter la numérotation, le routage et certaines autres fonctions. En règle générale, les gros points d'accès sont utilisés comme points d'accès autonomes qui peuvent fonctionner en l'absence de tout contrôleur.

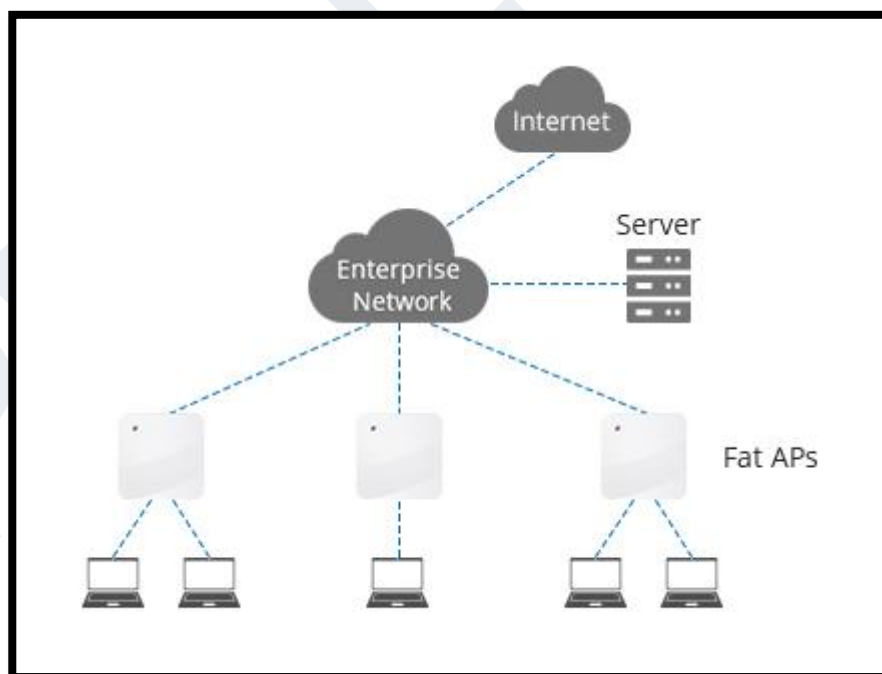


Figure 13: Déploiement des Fat APs

Par contre, Fit AP vise à réduire la complexité du matériel des points d'accès d'origine. Fit AP, sans système d'exploitation complet propre, supprime le routage, le DNS, le serveur DHCP et de nombreuses autres fonctions de chargement et ne conserve que la partie d'accès sans fil. En tant que composant du LAN sans fil, le Fit AP ne peut pas fonctionner indépendamment et nécessite une coopération avec la gestion d'AC. En fait, les points d'accès Fit sont assez courants dans l'utilisation quotidienne, ce qui équivaut à un commutateur ou un concentrateur sans fil, ne fournissant qu'une seule conversion de signal filaire / sans fil et une fonction de réception / transmission de signal sans fil.

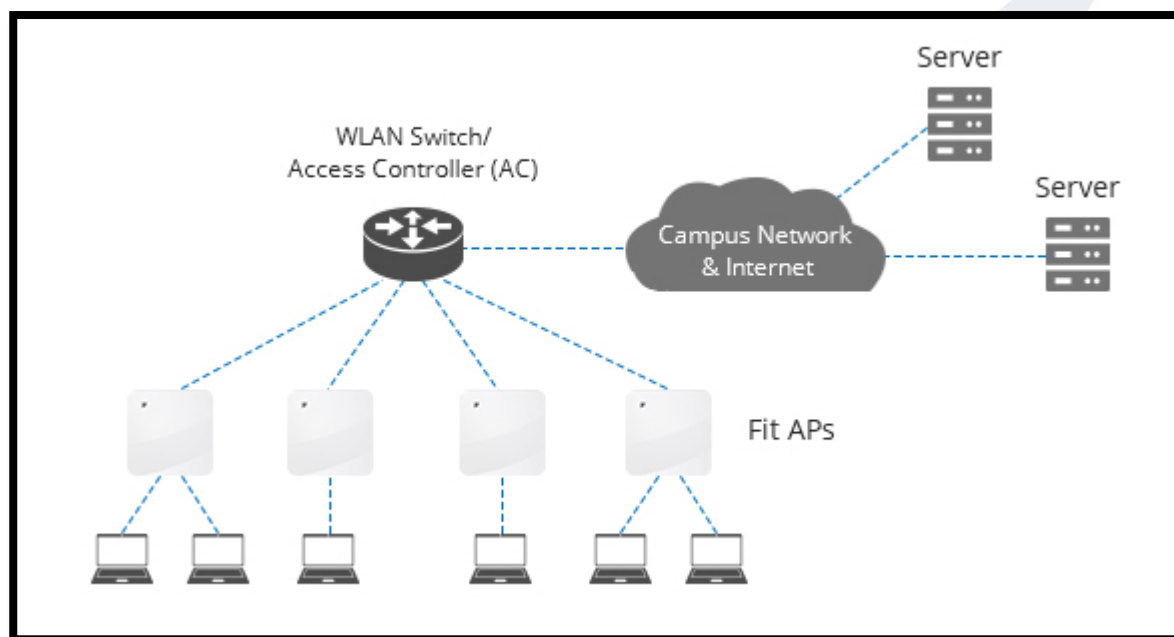


Figure 14: Déploiement des Fit APs + AC

Le déploiement du réseau Wi-Fi comportant un AC et des Fit APs est largement utilisé dans les campus de taille moyenne et grande comme l'ISET.

Le tableau suivant regroupe tous les APs répartis sur les différents départements d'ISET.

Tableau 22: Liste des APs

Point d'accès	Nom	Adresse MAC	S/N
AP 1	ap-serv	d0c6-5b76-a500	21500831023GKA019890
AP 2	ap-ges1	d0c6-5b76-a3e0	21500831023GKA019881
AP 3	ap-ges2	d0c6-5b76-a400	21500831023GKA019882
AP 4	ap-ges3	d0c6-5b76-a460	21500831023GKA019885
AP 5	ap-ges4	d0c6-5b76-9f20	21500831023GKA019843
AP 6	ap-adm1	18cf-2434-e540	21500831023GKA015005
AP 7	ap-adm2	d0c6-5b76-a3c0	21500831023GKA019880

<b>AP 8</b>	ap-adm3	d0c6-5b76-a180	21500831023GKA019862
<b>AP 9</b>	ap-adm4	d0c6-5b76-9e20	21500831023GKA019835
<b>AP 10</b>	ap-inf1	d0c6-5b77-21a0	21500831023GKA021571
<b>AP 11</b>	ap-inf2	d0c6-5b76-a960	21500831023GKA019925
<b>AP 12</b>	ap-inf3	d0c6-5b76-ac20	21500831023GKA019947
<b>AP 13</b>	ap-inf4	d0c6-5b76-acc0	21500831023GKA019952
<b>AP 14</b>	ap-inf5	d0c6-5b76-bae0	21500831023GKA020065
<b>AP 15</b>	ap-inf6	d0c6-5b76-a1e0	21500831023GKA019865
<b>AP 16</b>	ap-bib1	d0c6-5b76-9ee0	21500831023GKA019841
<b>AP 17</b>	ap-bib2	d0c6-5b76-a020	21500831023GKA019851
<b>AP 18</b>	ap-HalMec	d0c6-5b76-a040	21500831023GKA019852
<b>AP 19</b>	ap-ci	d0c6-5b76-a2c0	21500831023GKA019872
<b>AP 20</b>	ap-mec1	d0c6-5b76-a920	21500831023GKA019923
<b>AP 21</b>	ap-mec2	d0c6-5b76-ac80	21500831023GKA019950
<b>AP 22</b>	ap-mec3	d0c6-5b77-0840	21500831023GKA021368
<b>AP 23</b>	ap-mec4	d0c6-5b76-a520	21500831023GKA019891
<b>AP 24</b>	ap-buv	d0c6-5b76-ad60	21500831023GKA019957

## vi. Low Level Design du contrôleur d'accès AC

### 1. Spécifications du contrôleur d'accès Huawei AC6508

L'AC6508 est un contrôleur d'accès fixe sans fil (AC). Il peut gérer jusqu'à 256 points d'accès (le nombre des points d'accès à gérer dépend de la licence) et fournit une fonction de commutateur GE, permettant un accès intégré pour les utilisateurs filaires et sans fil. L'AC offre une grande évolutivité et offre aux utilisateurs une grande flexibilité dans la configuration du nombreux APs gérés.

L'AC6508 fournit 2 interfaces optiques 10GE et 10 interfaces électriques GE, prenant en charge des performances de transfert jusqu'à 6 Gbit/s. Le tableau suivant présente les spécifications de l'AC.

Tableau 23: Spécification de Huawei AC6508

Spécification	Valeur
<b>Les ports</b>	10 x 1GE et 2 x 10GE SFP+
<b>Source de courant</b>	Adaptateur AC/DC
<b>Capacité de transfert</b>	6 Gbit/s
<b>Nombre maximum de points d'accès gérés</b>	256
<b>Nombre maximum d'utilisateurs d'accès</b>	4K
<b>Réseau AP-AC</b>	Réseau de couches 2 ou 3
<b>Modes de transfert</b>	Transfert direct ou transfert de tunnel (Direct forwarding or tunnel forwarding)
<b>Mode AC actif / veille</b>	1 + 1 HSB ou N + 1 backup
<b>Protocoles radio</b>	802.11 a/b/g/n/ac/acWave 2/ax
<b>Dimensions (H x L x P)</b>	43,6mm x 210mm x 250mm

## 2. Architecture Wi-Fi

Parmi les exclusivités du projet est la partie Wi-Fi. Nous avons mis en place 24 points d'accès contrôlés par un seul nœud qui est l'AC et distribués sur l'ensemble des switches access comme suit :

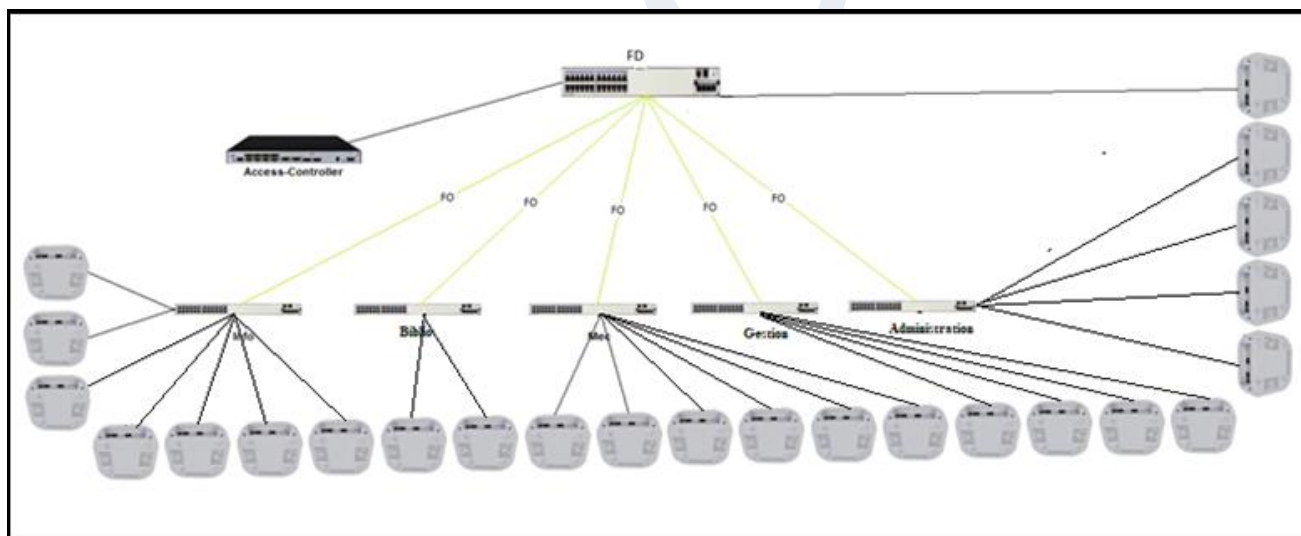


Figure 15: Architecture Wi-Fi

### 3. Configuration initiale

Le tableau suivant détaille les paramètres de base configurés dans le contrôleur.

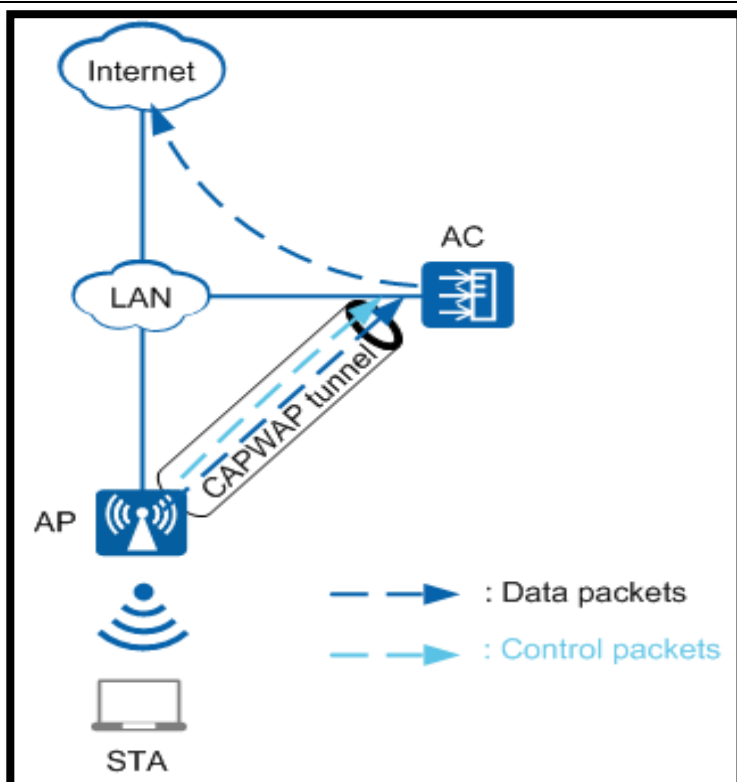
Tableau 24: Configuration de base de l'AC

Paramètres	Valeur
Nom	AC-Mahdia
Adresse de gestion	172.16.99.254
Masque de réseau	255.255.255.0
VLAN de management	99
Login/mot de passe	admin / Admin@123\$

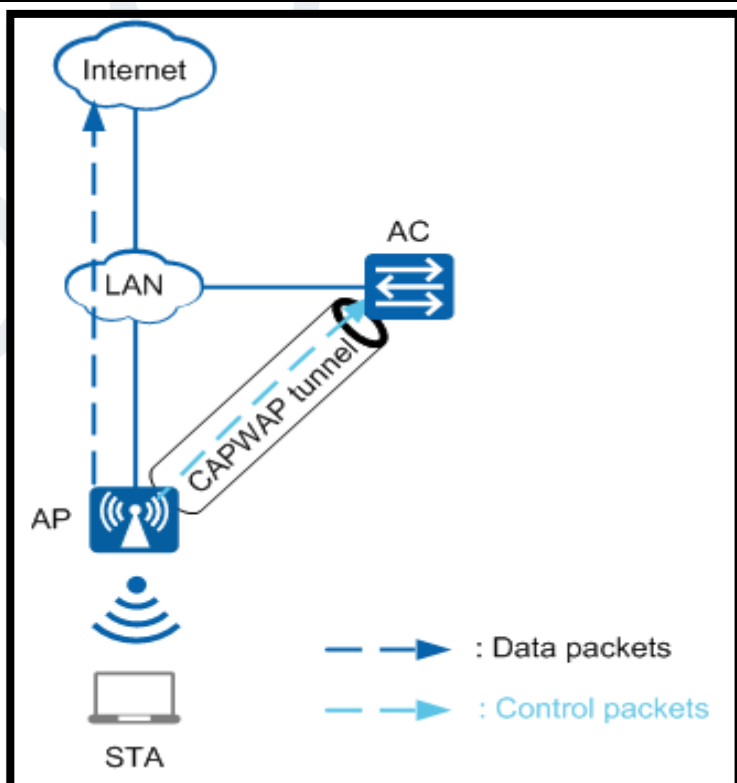
### 4. Configuration des VLANs Wi-Fi

Les paquets transmis sur un WLAN comprennent des paquets de gestion (paquets de contrôle) et des paquets de données (paquets de service). Les paquets de gestion sont transmis via les tunnels de contrôle de contrôle et de fourniture de points d'accès sans fil (CAPWAP). Les paquets de données peuvent être transférés en mode tunnel, direct ou soft Generic Routing Encapsulation (GRE), selon qu'ils sont transmis via des tunnels de données CAPWAP. Le mode tunnel est également appelé mode centralisé et le mode direct est également appelé mode local.

En mode de transfert de tunnel, les points d'accès encapsulent les paquets de données utilisateur sur un tunnel de données CAPWAP et les envoient à un AC. L'AC transmet ensuite ces paquets à un réseau de couche supérieure.



En mode de transfert direct, les points d'accès transmettent les paquets de données utilisateur à un réseau de couche supérieure sans les encapsuler sur un tunnel de données CAPWAP.



Le tableau suivant compare entre les 2 modes de transfert.

Tableau 25: Tableau comparatif des modes de transfert

Mode de transfert de données	Avantage	Désavantage
Transfert de tunnel	Un AC transmet de manière centralisée les paquets de données, ce qui est sécurisé et facilite la gestion et le contrôle centralisés. Les nouveaux appareils peuvent être facilement déployés et configurés, avec de petits changements sur le réseau.	Les données de service doivent être transmises par un AC, ce qui est inefficace et augmente la charge sur le AC.
Transfert direct	Les données de service n'ont pas besoin d'être transmises par un AC, ce qui est efficace et réduit la charge sur l'AC.	Les données de service ne peuvent pas être gérées ou contrôlées de manière centralisée. Le déploiement de nouveaux appareils entraîne de grands changements sur le réseau.

Le tableau ci-dessous illustre la liste des VLANs Wi-Fi configurés dans le contrôleur d'accès.

Tableau 26: Liste des VLANs

SSID	VLAN de service	AP Groupe	Mode de transfert	Authentification
ENS	120	ap-isetm	Forwarding	Enseignant@2020
ADM	140	ap-administration	Forwarding	Personnel@2020
ETUD	130, 131, 132, 133	ap-isetm	Forwarding	Etudiants@2020
Guest	150	ap-isetm	Tunnel	Guest@2020

## 5. Configuration des interfaces de l'AC

Le tableau ci-contre présente la configuration des interfaces de contrôleur d'accès connecté au switch core.

Tableau 27: Interfaces de l'AC

Interface	Description	Type	Vlan
GigabitEthernet0/0/1	Liaison avec le switch core	Trunk	90 99 120 130 131 132 133 140 150
GigabitEthernet0/0/3	Management	Access	99



Configuration:

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan 90 99 120 130 to 133 140 150

interface GigabitEthernet0/0/3

port link-type access

port default vlan 99

Nous avons configuré les interfaces VLANif comme il est montré dans le tableau suivant.

Tableau 28: Interfaces Vlanif de l'AC

Vlanif	IP address
90	172.16.90.1/24
99	172.16.99.254/24
150	172.16.150.100/24

## 6. Ajout des APs au contrôleur

Au niveau contrôleur d'accès, nous avons ajouté tous les points d'accès manuellement en utilisant l'adresse MAC de chaque point d'accès. Les lignes de commande sont comme suit :

wlan

ap auth-mode mac-auth

ap-mac d0c6-5b76-a500 ap-id 1

## 7. Configuration des SSIDs des APs

Le tableau suivant détaille les paramètres des SSID configurés.

Tableau 29: SSIDs configurés

SSID	VLAN de service	AP Groupe	Authentification
ENS	120	ap-isetm	Enseignant@2020
ADM	140	ap-administration	Personnel@2020

ETUD	130,131,132,133	ap-isetm	Etudiants@2020
GUEST	150	ap-isetm	Guest@2020

## 8. Configuration des VAP profiles

Le tableau suivant détaille les paramètres des VAP profiles configurés.

Tableau 30: VAP profiles

VAP profil	VLAN de service	SSID profil	Smart Roaming
Enseignants	120	ENS	Activé
Etudiants	130	ETUD	Activé
Personnel	140	ADM	Activé
Guest	150	Guest	Activé
etudiant_BIB	133	ETUD	Activé
etudiant_MEC	132	ETUD	Activé
etudiant_GES	131	ETUD	Activé

## 9. AP groups

Dans l'ISSET, le contrôleur gère 24 FIT AP. Pour simplifier et faciliter les opérations, nous avons distribué les APs sur deux groupes d'AP et nous avons effectué des configurations uniformément dans chaque groupe AP. Donc, tous les AP du même groupe reçoivent les mêmes configurations.

Le tableau suivant présente les différents paramètres d'AP groups configurés.

Nom	VAP Profile	Nombres AP	Radio 0 profile	Radio 1 profile	Radio 2 profile	Domain
ap-isetm	Enseignants Etudiants Personnel Guest etudiant_GES etudiant_BIB etudiant_MEC	20	2.4G	5G	5G	domain1

ap-administrati on	Personnel	4	2.4G	5G	5G	domain1
-----------------------	-----------	---	------	----	----	---------

## 10. Configuration du DHCP

Pour assurer la communication entre les points d'accès et le contrôleur d'accès, un serveur DHCP doit être configuré au niveau du contrôleur pour fournir les adresse IP dans la plage d'adresse du vlan 90, au point d'accès connecté. L'AC fonctionne comme serveur DHCP pour allouer des adresses IP aux APs. Les APs obtiennent l'adresse IP de l'AC en utilisant la fonction DNS, l'option DHCP dans les paquets DHCP ou les protocoles de découverte de couche 2, puis configurent les tunnels de données avec l'AC.

La configuration du DHCP est comme suit :

ip pool AP

gateway-list 172.16.90.1

network 172.16.90.0 mask 255.255.255.0

dns-list 8.8.8.8

## 11. Configuration complète de l'AC

Création de VLAN, description et nom du VLAN	vlan 90 description " vlan pour les APs" name AP
Configuration du pool DHCP	ip pool AP gateway-list 172.16.90.1 network 172.16.90.0 mask 255.255.255.0 dns-list 8.8.8.8
Configuration d'interface vlanif, (adresse IP, DHCP)	interface Vlanif90 ip address 172.16.90.1 255.255.255.0 dhcp select global
Configuration interface trunk vlan 90, 99, 120, 130, 131, 132, 133, 140, 150	interface GigabitEthernet0/0/1 port link-type trunk port trunk allow-pass vlan 90 99 120 130 to 133 140 150
Configuration de l'interface source du contrôleur	capwap source interface vlanif90
Configuration du security-profile	security-profile name Guest security wpa2 psk pass-phrase ***** tkip
Configuration d'un SSID	ssid-profile name Etudiants

	ssid ETUD
Configuration du VAP profile, (service vlan, SSID, security profile)	va vap-profile name Etudiants service-vlan vlan-id 130 ssid-profile Etudiants security-profile Etudiants
Configuration du domaine	regulatory-domain-profile name domain1
Création de groupe des points d'accès, affectation du vap profile à un groupe ap avec radio all	ap-group name ap-isetm regulatory-domain-profile domain1 vap-profile Enseignants wlan 1 radio all vap-profile Etudiants wlan 2 radio all
Ajout d'AP avec MAC adresse, name AP, ID-AP, groupe ap	ap-mac d0c6-5b76-a500 ap-id 1 ap-name ap-serv ap-group ap-isetm

## vii. Low Level Design du Firewall Fortigate 301E

### 1. Spécifications du Fortigate 301E

La série FortiGate 300E offre des capacités de pare-feu de nouvelle génération pour les moyennes et grandes entreprises, avec la flexibilité d'être déployé sur le campus ou la branche d'entreprise. Il protège contre les Cyber-menaces avec processeur de sécurité haute performance, efficacité de la sécurité et une grande visibilité.

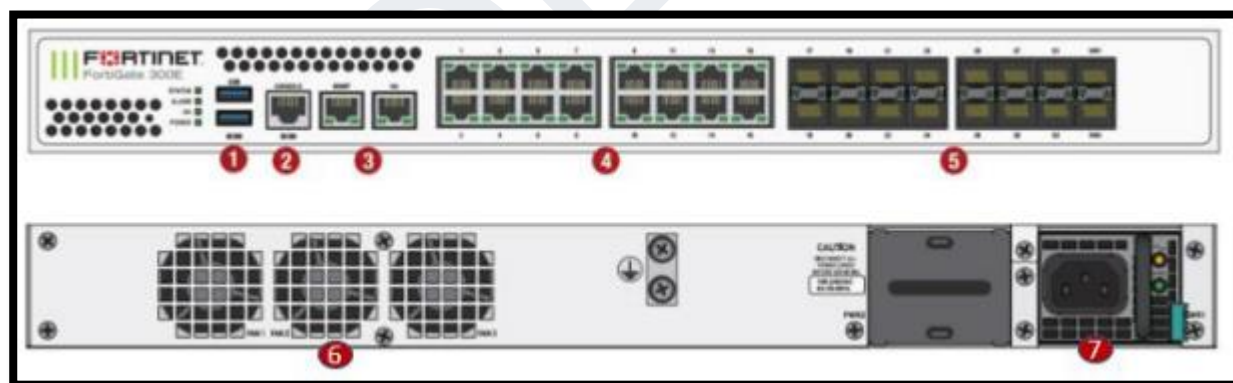


Tableau 31: Ports du Fortigate 301E

1	PORT USB
2	Port console
3	2xGE RJ45 MGMT/HA Ports
4	16xGE RJ45 Ports
5	16xGE SFP Slots
6	Fan
7	PSU

Dans ce projet, nous avons mis en place un seul firewall de la marque Fortinet et du modèle 301E dont les spécifications comme suit :

Spécification	Valeur
<b>Nombre de Ports</b>	16x GE RJ45 Port, 1x GE RJ45 MGMT, 1x GE HA Port, 16x GE SFP Slots, Console Port, USB Port
<b>Firewall Policies</b>	10,000
<b>Concurrent Sessions (TCP)</b>	4 Millions
<b>Local Storage</b>	240 SSD
<b>SSL-VPN Throughput</b>	2.5Gbps
<b>Numéro de série</b>	FG3H1E5819903229

## 2. Architecture WAN

Pour assurer la sécurité, il est recommandé de séparer l'accès internet du trafic local d'ISET. Pour cela nous avons installé un firewall Fortigate 301E entre le réseau internet et le réseau LAN pour le filtrage du trafic entrant et sortant. Aussi, le firewall Fortigate va assurer la sécurité d'accès vers le serveur WEB et l'accès à distance par les VPNs clients.

L'architecture WAN est présentée par la figure suivante :

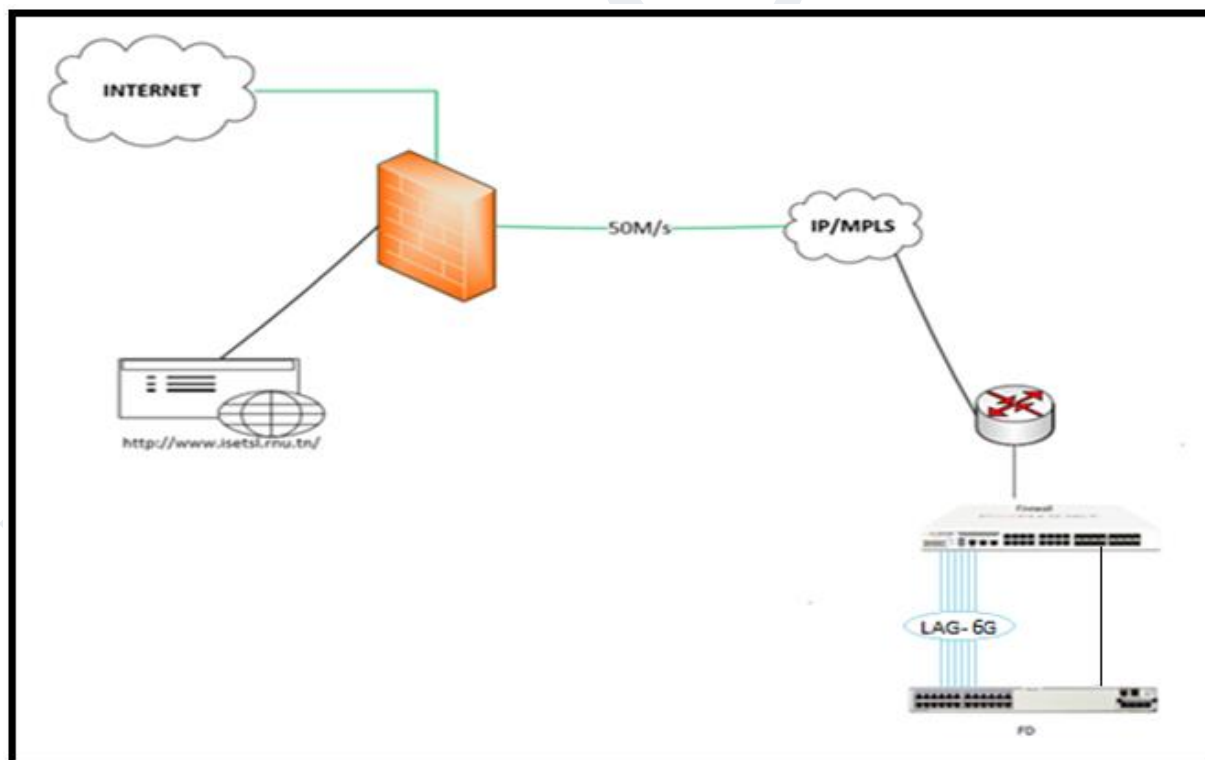


Figure 16: Architecture WAN

### 3. Configuration initiale

Le tableau suivant présente la configuration de base du firewall Fortigate à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Tableau 32: Configuration initiale du firewall Fortigate

Attributs du switch à configurer	Valeur
<b>Nom</b>	ISET-Mahdia
<b>Login / Password</b>	admin / Admin@123\$
<b>Vlan de management</b>	vlan 99 (name Devices-MGMT)
<b>Adresse IP de management</b>	17.16.99.1/24
<b>Méthodes de management</b>	Telnet, http, terminal

### 4. Configuration des interfaces

Nous avons configuré l'interface d'agrégation de lien en combinant 6 ports (port 1, port 2, port3 et port 4 et port 5 et port 6) comme le montre la figure ci-dessous et le port 7 comme interface WAN avec l'adresse IP 41.229.130.130/25.

NOM DE L'INTERFACE	PORT	IP/NETMASK
LAG	Port1	20.20.20.1/30
	Port2	
	Port3	
	Port4	
	Port5	
	Port6	
WAN	Port7	41.229.125.2/24

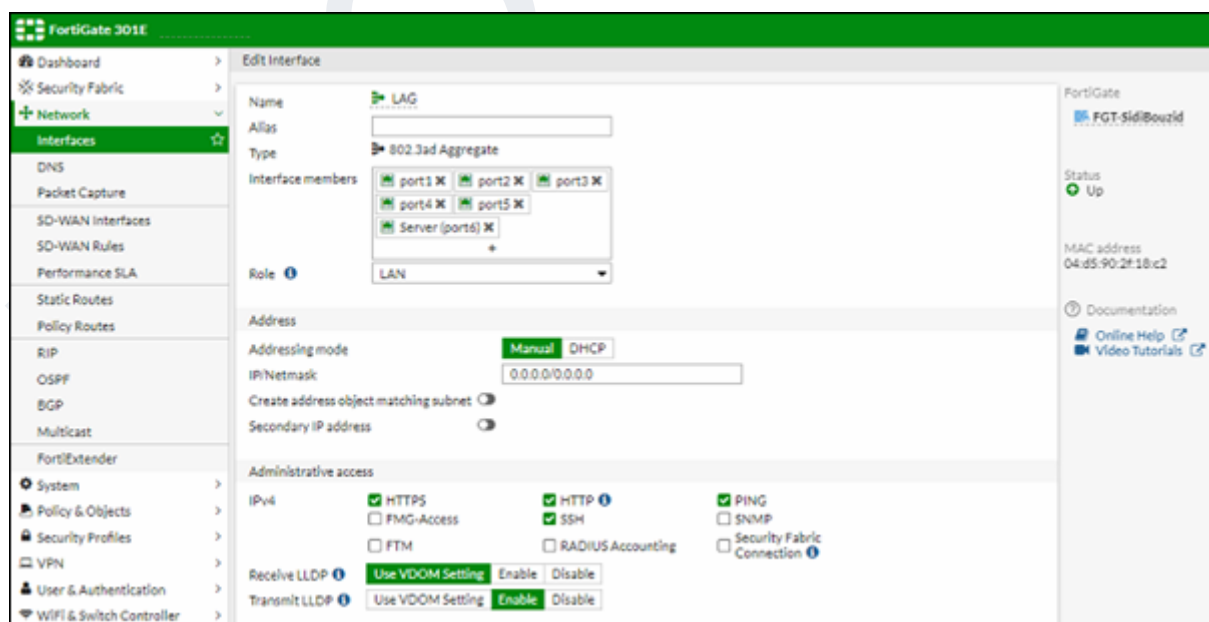


Figure 17: Configuration des interfaces du firewall

## 5. Configuration des routes

Dans le firewall, nous avons configuré les routes suivantes :

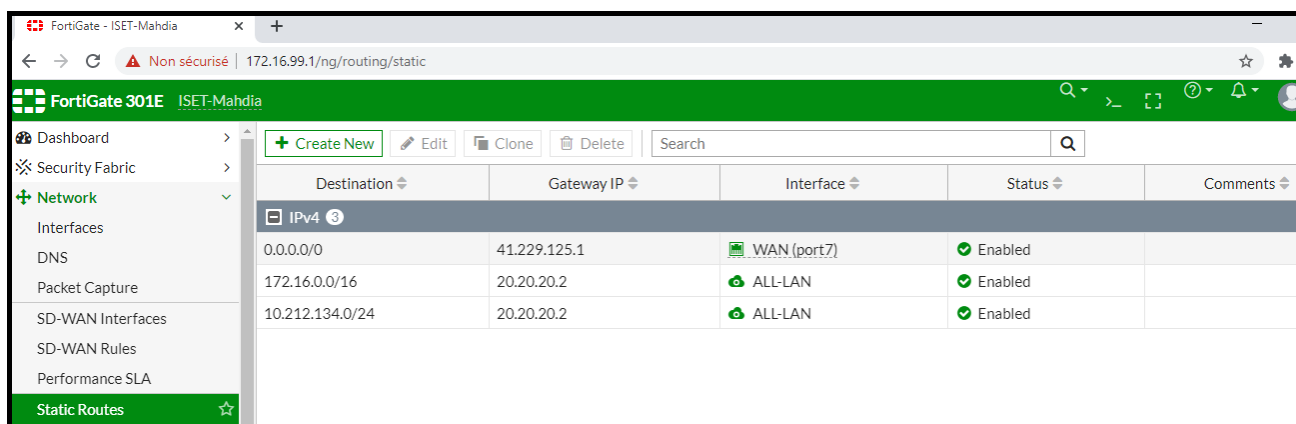
Tableau 33: Table de routage

SOURCE DANS LE FW	GATEWAY	DESTINATION	DESCRIPTION
Port 7 : 41.229.125.2	@ du routeur : 41.229.125.1	0.0.0.0/0	Internet
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.10.0/24	Administration
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.20.0/24	DPT-TI
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.30.0/24	DPT-GESTION
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.40.0/24	DPT-GM
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.50.0/24	BIB
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.80.0/24	NVR
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.120.0/24	WLAN-ENSG
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.130.0/24	Wifi-etudiant_TI
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.131.0/24	Wifi-etudiant_GES
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.132.0/24	Wifi-etudiant_MEC
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.133.0/24	Wifi-etudiant_BIB
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.140.0/24	WLAN-Personnel
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	172.16.150.0/24	GUEST
LAG : 20.20.20.1	LAG dans SW FD : 20.20.20.2	10.212.134.0/24	VPN



## 6. Routes statiques

Nous avons défini trois routes statiques comme montre la figure ci-dessous.



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	41.229.125.1	WAN (port7)	Enabled	
172.16.0.0/16	20.20.20.2	ALL-LAN	Enabled	
10.212.134.0/24	20.20.20.2	ALL-LAN	Enabled	

Figure 18: routes statiques

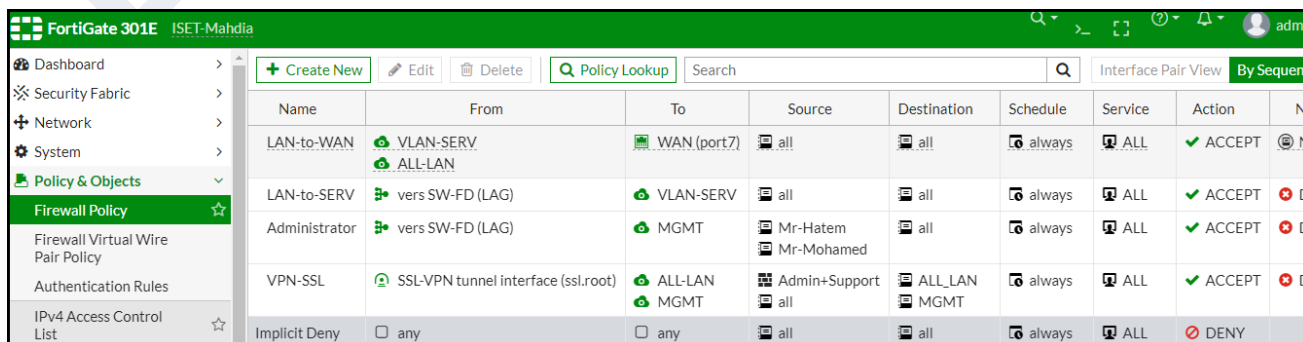
## 7. Configuration des règles de sécurité

Afin d'améliorer la sécurité, on a créé des règles qui gèrent le trafic intra/intra, intra/extra et extra/intra. Le tableau suivant détaille les règles configurées sur le Firewall.

Tableau 34: Les règles de sécurité

Nom	Source Zone	Src @IP	Dst Zone	Dst @IP	Service	NAT
LAN-to-WAN	VLAN-SERV ALL-LAN	all	WAN	all	all	NAT-NET
LAN-to-SERV	LAG	all	VLAN-SERV	all	all	Disable
Administrator	LAG	M.Hatem M.Mohamed	MGMT	all	all	Disable
VPN-SSL	SSL-VPN tunnel interface	Admin Support	ALL-LAN MGMT	ALL-LAN MGMT	all	Disable

La figure ci-dessous indique la liste des règles déclarées au niveau du Firewall.



Name	From	To	Source	Destination	Schedule	Service	Action	NAT
LAN-to-WAN	VLAN-SERV ALL-LAN	WAN (port7)	all	all	always	ALL	ACCEPT	NAT-NET
LAN-to-SERV	vers SW-FD (LAG)	VLAN-SERV	all	all	always	ALL	ACCEPT	Disable
Administrator	vers SW-FD (LAG)	MGMT	Mr-Hatem Mr-Mohamed	all	always	ALL	ACCEPT	Disable
VPN-SSL	SSL-VPN tunnel interface (ssl.root)	ALL-LAN MGMT	Admin+Support all	ALL_LAN MGMT	always	ALL	ACCEPT	Disable
Implicit Deny	any	any	all	all	always	ALL	DENY	

Figure 19: Les règles de sécurité

## **viii. Conclusion**

Pendant ce projet, nous avons fait une étude détaillée du réseau informatique d'ISET Mahdia afin de relever les différentes insuffisances présentées par le dit réseau. L'architecture, que nous avons mis à la place de l'ancienne architecture, fait face à ces insuffisances permettant de rendre le réseau beaucoup plus sécurisé et performant.

Tout au long de nos interventions, nous avons pris en compte au besoins du notre client, ISET Mahdia, pour avoir enfin un réseau bien segmenté et sécurisé assurant le bon fonctionnement des équipements et des logiciels et favorisant une transmission rapide et sécurisée des données qui répond aux besoins et aux priorités de la société et ses employés.