

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

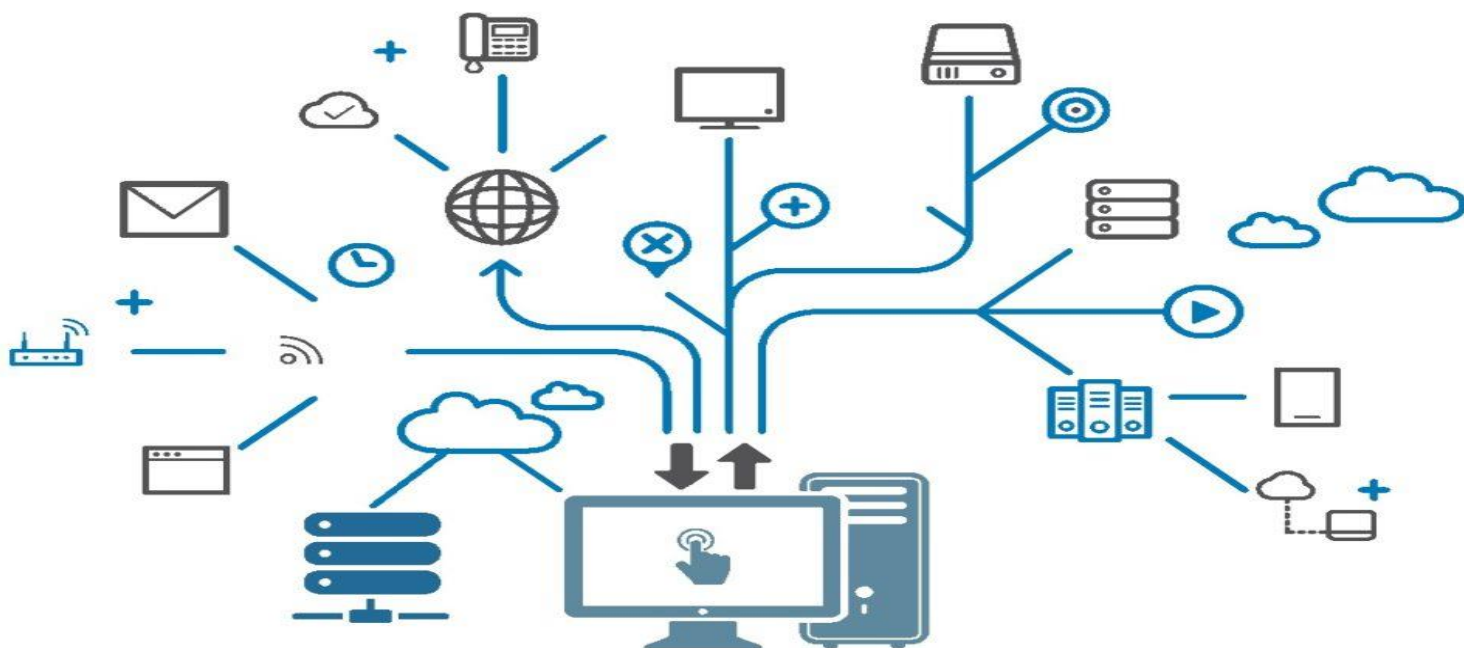


Table des matières

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	14
4. Configuration des interfaces	15
5. Configuration du GVRP.....	18
6. Configuration du service DHCP	19
7. Configuration de route statique	19
8. Configuration du protocole RSTP	20
IV. Low Level Design des Switches Access	20
1. Spécifications du switch Huawei S5720-28X-PWR-LI-AC	20
2. Architecture LAN.....	22
3. Switch Access SW-textile.....	23
3.1 Configuration initiale.....	23
3.2 Configuration des interfaces.....	24
4. Switch Access SW-Administration	25
4.1 Configuration initiale	25
4.2 Configuration des interfaces.....	25
5. Switch Access SW-mecanique	26
5.1 Configuration initiale.....	26
5.2 Configuration des interfaces.....	27
6. Switch Access SW-Chimie.....	28

6.1 Configuration initiale.....	28
6.2 Configuration des interfaces.....	28
7. Switch Access SW-Gestion.....	29
7.1 Configuration initiale.....	29
7.2 Configuration des interfaces.....	30
8. Switch Access SW-Biblio	31
8.1 Configuration initiale.....	31
8.2 Configuration des interfaces.....	31
V. Low Level Design de l'Access Point.....	32
1. Spécifications du point d'accès Huawei AP4050DN	32
2. Liste des APs	33
VI. Low Level Design du contrôleur d'accès AC	35
1. Spécifications du contrôleur d'accès Huawei AC6508	35
2. Architecture Wi-Fi	36
3. Configuration initiale	37
4. Configuration des VLANs Wi-Fi	37
5. Configuration des interfaces de l'AC	39
6. Ajout des APs au contrôleur.....	40
7. Configuration des SSIDs des APs	40
8. Configuration des VAP profiles	41
9. AP groups	41
10. Configuration du DHCP.....	42
11. Configuration du WDS:.....	43
12. Configuration complète de l'AC.....	46
VII. Low Level Design du Firewall Fortigate 301E	48
1. Spécifications du Fortigate 301E	48
2. Architecture WAN	49
3. Configuration initiale	50
4. Configuration des interfaces	51
5. Configuration des routes.....	52
6. Routes statiques	53
7. Configuration des règles de sécurité.....	53
III. Conclusion	54

Liste des tableaux

Tableau 1: Description des ports/modules du switch core	12
Tableau 2: Spécifications du switch Huawei S5730-36C-PWH-HI.....	13
Tableau 3: Configuration initiale du FD-Ksar-halel	14
Tableau 4: Liste des VLANs du FD-Ksar-halel	15
Tableau 5: Liste des interfaces du FD-Ksar-halel	16
Tableau 6: Liste des interfaces Vlanif du FD-Ksar-halel	17
Tableau 7: Configuration du DHCP	19
Tableau 8: Liste des switches access.....	20
Tableau 9: Description des ports/modules du switch access.....	21
Tableau 10: Spécifications du switch Huawei S5720-28X-PWR-LI-AC	22
Tableau 11: Configuration initiale du SW-textile	23
Tableau 12: Les interfaces de switch SW-textile	24
Tableau 13: Configuration initiale du SW-Administration	25
Tableau 14: Les interfaces de switch SW-Administration	25
Tableau 15: Configuration initiale du SW-mecanique	27
Tableau 16: Les interfaces de switch SW-mecanique	27
Tableau 17: Configuration initiale du SW-Chimie	28
Tableau 18: Les interfaces de switch SW-Chimie.....	28
Tableau 19: Configuration initiale du SW-Gestion	29
Tableau 20: Les interfaces de switch SW-Gestion	30
Tableau 21: Configuration initiale du SW-Biblio.....	31
Tableau 22: Les interfaces de switch SW-Biblio	31
Tableau 27: Spécifications des APs.....	32
Tableau 28: Liste des APs	34
Tableau 29: Spécification de Huawei AC6508.....	36
Tableau 30: Configuration de base de l'AC	37
Tableau 31: Tableau comparatif des modes de transfert.....	39
Tableau 32: Liste des VLANs	39
Tableau 33: Interfaces de l'AC.....	39
Tableau 34: Interfaces Vlanif de l'AC	40
Tableau 35: SSIDs configurés	40
Tableau 36: VAP profiles	41
Tableau 37: Ports du Fortigate 301E	49
Tableau 38: Configuration initiale du firewall Fortigate	50
Tableau 39: Table de routage.....	52
Tableau 40: Les règles de sécurité.....	53

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'ensmble du switch Huawei S5730-36C-PWH-HI.....	11
Figure 8: Architecture core.....	14
Figure 9: Configuration des interfaces XG0/1/1-6 du FD-Ksar-halel	18
Figure 10: Routes statiques	20
Figure 11: Vue d'ensmble du switch Huawei S5720-28X-PWR-LI-AC.....	21
Figure 12: Architecture LAN.....	23
Figure 13: Déploiement des Fat APs	33
Figure 14: Déploiement des Fit APs + AC	34
Figure 15: Architecture Wi-Fi	36
Figure 16: Architecture WDS	43
Figure 17: Architecture WAN	50
Figure 18: Interface Dashboard du FortiGate	51
Figure 19: Configuration des interfaces du firewall	52
Figure 20: routes statiques	53
Figure 21: Les règles de sécurité.....	54

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 Ksar Hellal", 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 Ksar Hellal 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 Ksar Hellal”, Prologic s’est déplacé au local d’ISET Ksar Hellal pour mettre en place et installer les nouveaux équipements suivants :

- 6 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.

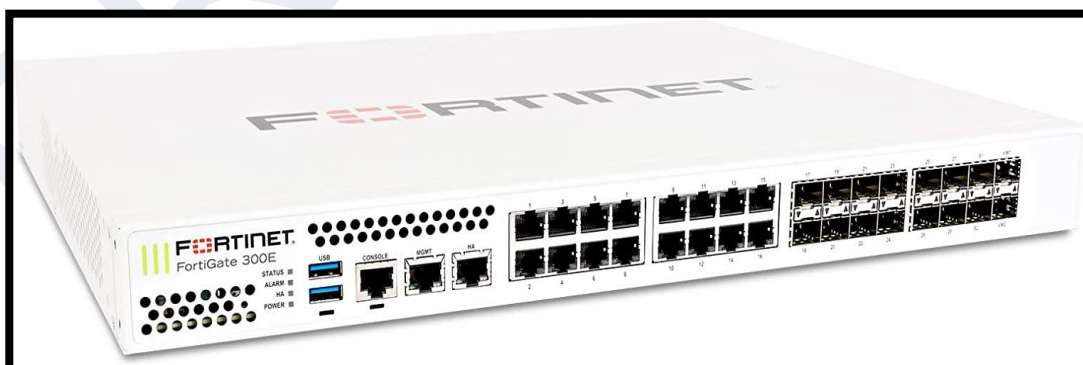


Figure 5: Firewall Fortigate 301E

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 Ksar Hellal.

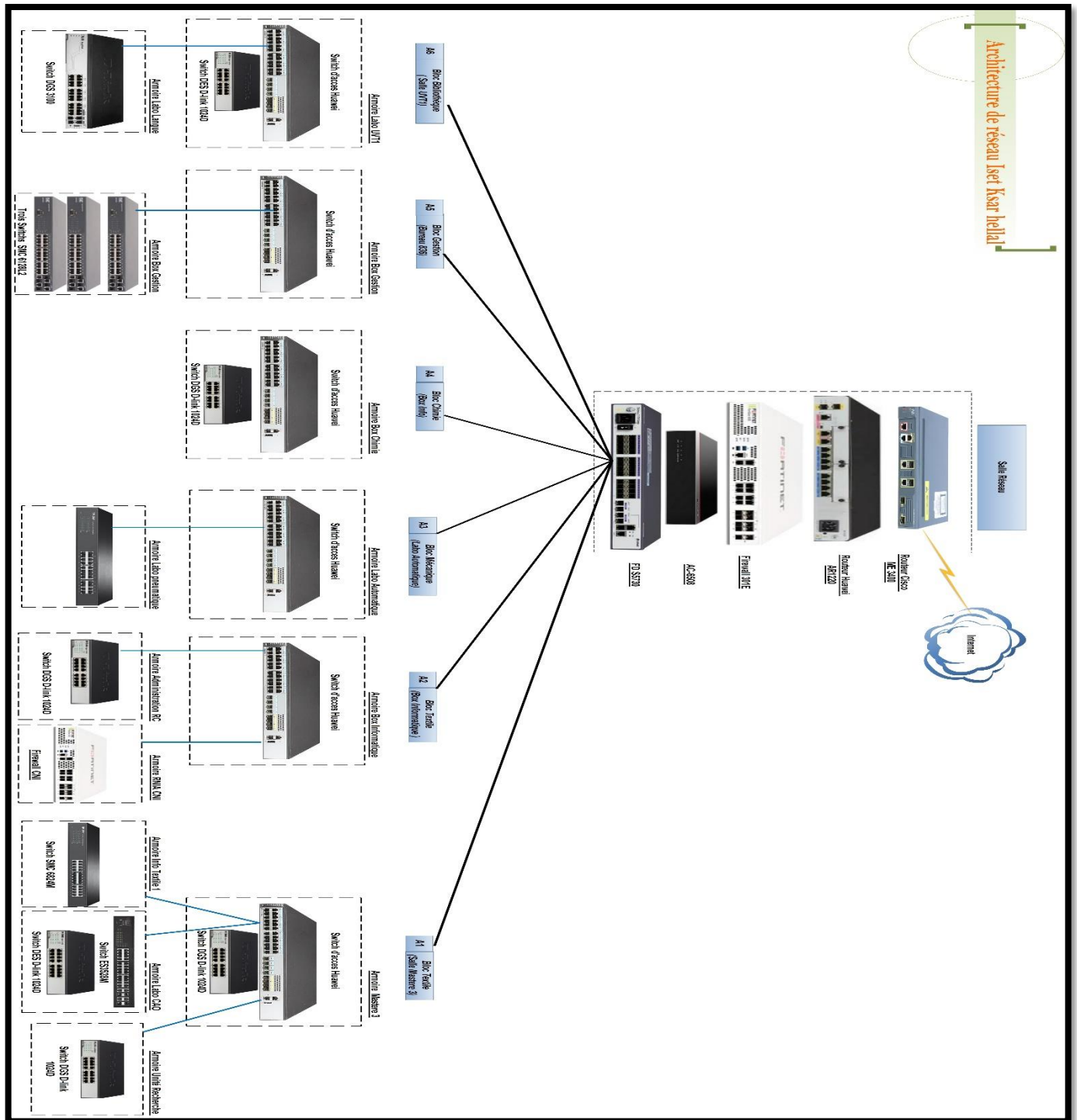


Figure 6: Architecture globale

L'ancien réseau d'ISSET 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.

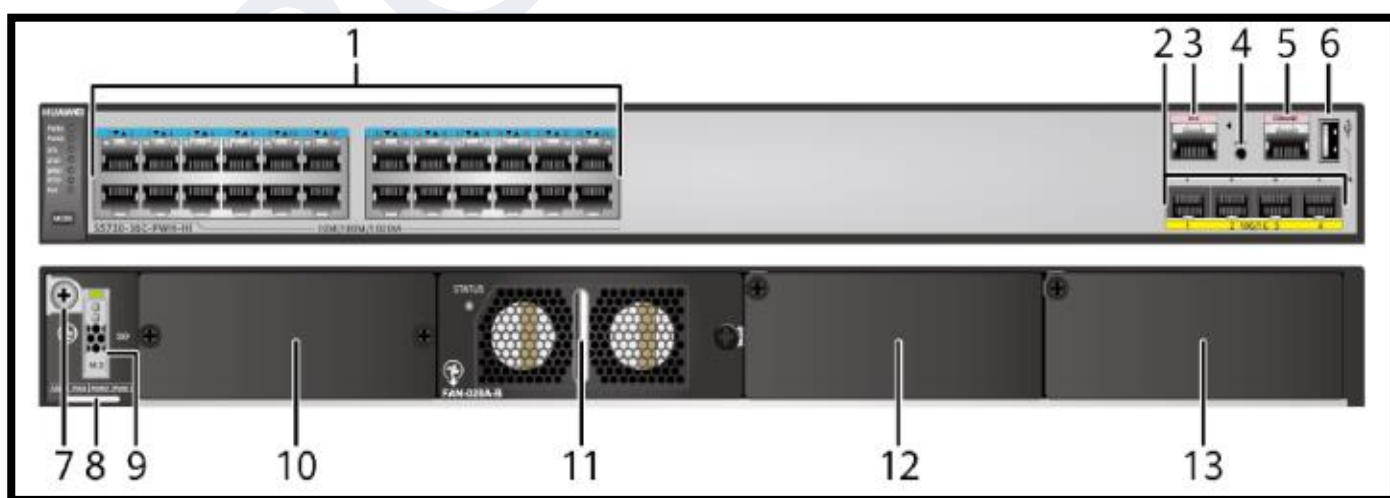


Figure 7: Vue d'ensemble du switch Huawei S5730-36C-PWH-HI

Tableau 1: Description des ports/modules du switch core

Numéro de port / module	Description
1	24 ports PoE++ 10/100 /1000 BASE-T
2	<p>4 ports 10GE SFP+</p> <p>Les modules et câbles applicables sont:</p> <ul style="list-style-type: none"> - 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	Port de management ETH
4	<p>Bouton PNP</p> <p>NB: 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.</p>
5	Port de console
6	Port USB
7	<p>Vis de terre</p> <p>NB: Il est utilisé avec un câble de masse.</p>
8	<p>Étiquette ESN</p> <p>NB: Vous pouvez le dessiner pour afficher l'adresse ESN et MAC du switch.</p>
9	<p>Emplacement pour carte SSD</p> <p>NB: Carte SSD enfichable prise en charge: - SSD-240Go</p>
10	<p>Fente pour carte arrière</p> <p>NB: Cartes prises en charge:</p> <ul style="list-style-type: none"> - ES5D21Q02Q00 - ES5D21X08T00 - ES5D21X08S00
11	<p>Emplacement du ventilateur</p> <p>NB: Module de ventilateur applicable:</p> <ul style="list-style-type: none"> - FAN-028A-B
12	<p>Emplacement 1 du module d'alimentation</p> <p>NB: Modules d'alimentation applicables:</p> <ul style="list-style-type: none"> - Module d'alimentation PoE 500 W CA - Module d'alimentation PoE DC 650 W - Module d'alimentation PoE CA de 1150 W - Module d'alimentation PoE 1000 W CA (applicable dans V200R013C00 et versions ultérieures)
	Emplacement 2 du module d'alimentation

13

NB: 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
Interfaces	24 x Ethernet 10/100/1000 ports, 8 x 10GE SFP+
Performance du transfert	240 Mpps
Capacité du tableau d'adresses MAC	32000 adresses MAC
Capacité de commutation	758 Gbit/s
Flash	128 MB
RAM	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'ISSET. 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.

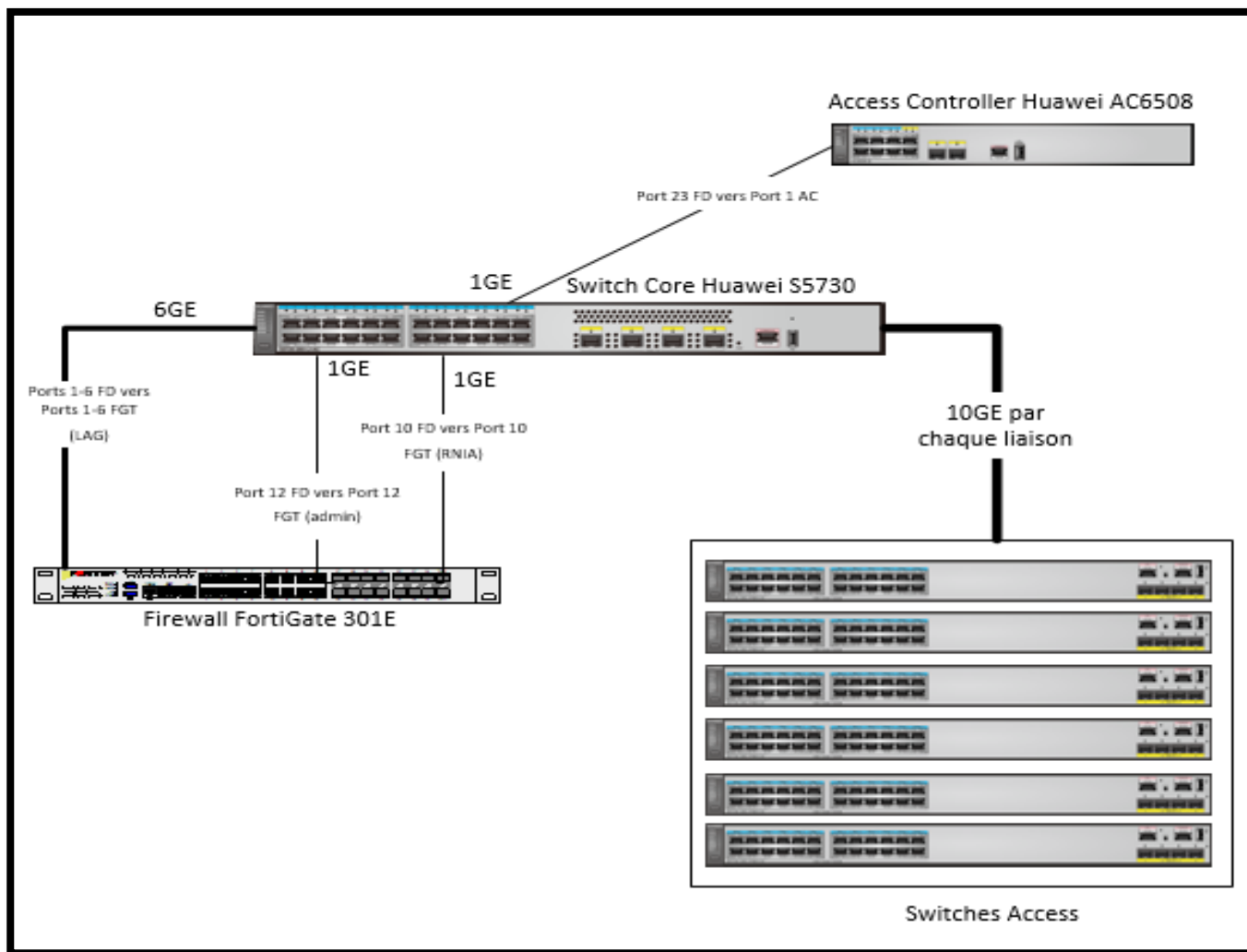


Figure 8: Architecture core

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 FD-Ksar-halel

Attributs du switch à configurer	Valeur
Nom	FD-Ksar-halel
Login / Password	admin / \$FD_Ksar2020
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.1/24
Méthodes de management	SSH, Telnet, http, terminal

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

Tableau 4: Liste des VLANs du FD-Ksar-halel

VLAN Name	VLAN ID	Adresse réseau / masque	Description
MGMT	32	172.31.32.0/24	VLAN de management des équipements
SERVER	33	172.31.33.0/24	VLAN des serveurs
ENS	36	172.31.36.0/24	VLAN wired pour les enseignants
ADM	37	172.31.37.0/24	VLAN wired pour les personnels de l'administration
Camera	40	172.31.40.0/24	VLAN wired pour les caméras
VOICE	41	172.31.41.0/24	VLAN wired pour les téléphones VoIP
Controle-access	42	172.31.42.0/24	VLAN wired pour le contrôle d'accès aux salles
Visiteur	43	172.31.43.0/24	VLAN wired pour les visiteurs
ETUD	44	172.31.44.0/24	VLAN wired pour les étudiants
ETUD-45	45	172.31.45.0/24	VLAN wired pour les étudiants
ETUD-46	46	172.31.46.0/24	VLAN wired pour les étudiants
APs	90	172.31.90.0/24	VLAN pour les APS
RNIA	99	-	VLAN wired pour RNIA
WIFI-Enseignants	120	172.16.120.0/24	VLAN WiFi pour les enseignants
WIFI-Administration	130	172.16.130.0/24	VLAN WiFi pour les personnels de l'administration
WIFI-Etudiants	140	172.16.140.0/24	VLAN WiFi pour les étudiants
WIFI-Etudiants-141	141	172.16.141.0/24	VLAN WiFi pour les étudiants
WIFI-Etudiants-142	142	172.16.142.0/24	VLAN WiFi pour les étudiants
Visiteurs	160	172.16.160.0/24	VLAN WiFi pour les visiteurs
administrateur	190	172.31.190.0/30	VLAN de l'administrateur
inter-co	1300	20.20.20.0/30	VLAN d'interconnexion en FD-FW

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 FD-Ksar-halel

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
GigabitEthernet 0/0/1	Trunk	-	-	Vers le port 1 du firewall (Agrégation des liens)
GigabitEthernet 0/0/2	Trunk	-	-	Vers le port 2 du firewall (Agrégation des liens)
GigabitEthernet 0/0/3	Trunk	-	-	Vers le port 3 du firewall (Agrégation des liens)
GigabitEthernet 0/0/4	Trunk	-	-	Vers le port 4 du firewall (Agrégation des liens)
GigabitEthernet 0/0/5	Trunk	-	-	Vers le port 5 du firewall (Agrégation des liens)
GigabitEthernet 0/0/6	Trunk	-	-	Vers le port 6 du firewall (Agrégation des liens)
GigabitEthernet 0/0/7	-	-	-	Vide
GigabitEthernet 0/0/8	-	-	-	Vide
GigabitEthernet 0/0/9	Access	32	-	Port management
GigabitEthernet 0/0/10	Access	99	-	Vers le port 10 du Firewall (RNIA)
GigabitEthernet 0/0/11	Access	37	-	Port pour l'administration
GigabitEthernet 0/0/12	Access	190	-	Vers le port 12 du Firewall (administrateur)
GigabitEthernet 0/0/13	-	-	-	Vide
GigabitEthernet 0/0/14	-	-	-	Vide
GigabitEthernet 0/0/15	Access	33	-	Vers serveur
GigabitEthernet 0/0/16	Access	33	-	Vers serveur
GigabitEthernet 0/0/17	Access	33	-	Vers serveur
GigabitEthernet 0/0/18	Access	33	-	Vers serveur
GigabitEthernet 0/0/19	Access	32	-	Port management

GigabitEthernet 0/0/20	Access	44	-	Port étudiant
GigabitEthernet 0/0/21	-	-	-	Vide
GigabitEthernet 0/0/22	-	-	-	Vide
GigabitEthernet 0/0/23	Trunk	32 90 160	-	Vers port 1 de l'AC
GigabitEthernet 0/0/24	Access	36	-	Port enseignant
XGigabitEthernet 0/0/1	-	-	-	Vide
XGigabitEthernet 0/0/2	-	-	-	Vide
XGigabitEthernet 0/0/3	-	-	-	Vide
XGigabitEthernet 0/0/4	-	-	-	Vide
XGigabitEthernet 0/1/1	Trunk	ALL	-	Vers le switch de département textile
XGigabitEthernet 0/1/2	Trunk	ALL	-	Vers le switch de l'administration
XGigabitEthernet 0/1/3	Trunk	ALL	-	Vers le switch de département mécanique
XGigabitEthernet 0/1/4	Trunk	ALL	-	Vers le switch de département chimie
XGigabitEthernet 0/1/5	Trunk	ALL	-	Vers le switch de département gestion
XGigabitEthernet 0/1/6	Trunk	ALL	-	Vers le switch de la bibliothèque
XGigabitEthernet 0/1/7	-	-	-	Vide
XGigabitEthernet 0/1/8	-	-	-	Vide

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

Tableau 6: Liste des interfaces Vlanif du FD-Ksar-halel

Vlanif	Adresse IP/Masque	DHCP	Description
32	172.31.32.1/24	non	Management
90	172.31.90.1/24	non (DHCP configuré au niveau de l'AC)	APs
160	172.16.160.1/24	non	WiFi visiteurs
1300	20.20.20.2/30	non	Interconnexion FD-FW

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 XGigabitEthernet0/1/6).

La figure suivante montre le résultat de la configuration des interfaces XG0/1/1-6.

```
#
interface XGigabitEthernet0/1/1
description "vers le switch Textile"
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface XGigabitEthernet0/1/2
description "vers le switch Administration"
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface XGigabitEthernet0/1/3
description "vers le switch AMecanique"
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface XGigabitEthernet0/1/4
description "vers le switch Chimie"
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface XGigabitEthernet0/1/5
description "vers le switch Gestion"
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface XGigabitEthernet0/1/6
description "vers le switch Bibliotheque"
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
```

Figure 9: Configuration des interfaces XG0/1/1-6 du FD-Ksar-halel

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 les VLANs WiFi de service (sauf le VLAN WiFi Guest qui est configuré au niveau de l'AC) et sur tous les VLANs wired. Le DHCP de VLAN management des APs est configuré au niveau de l'AC.

Tableau 7: Configuration du DHCP

VLAN	Adresse réseau	Gateway / Masque	DHCP	DNS
36	172.31.36.0/24	172.31.36.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
44	172.31.44.0/24	172.31.44.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
45	172.31.45.0/24	172.31.45.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
46	172.31.46.0/24	172.31.46.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
120	172.16.120.0/24	172.16.120.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
130	172.16.130.0/24	172.16.130.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
140	172.16.140.0/24	172.16.140.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
141	172.16.141.0/24	172.16.141.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2
142	172.16.142.0/24	172.16.142.1/24	oui	8.8.8.8 172.31.33.1 172.31.33.2

7. Configuration de route statique

Nous avons configuré 2 routes statiques qui vont diriger tout le trafic entrant au switch core vers le firewall Fortigate.

```
#
ip route-static 0.0.0.0 0.0.0.0 20.20.20.1
ip route-static 172.16.0.0 255.255.0.0 20.20.20.1
#
```

Figure 10: Routes statiques

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 6 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
Bibliothèque	Huawei S5720-LI	SW-Biblio
Chimie	Huawei S5720-LI	SW-Chimie
Gestion	Huawei S5720-LI	SW-Gestion
Mécanique	Huawei S5720-LI	SW-mecanique
Textile	Huawei S5720-LI	SW-textile
Administration	Huawei S5720-LI	SW-Administration

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.

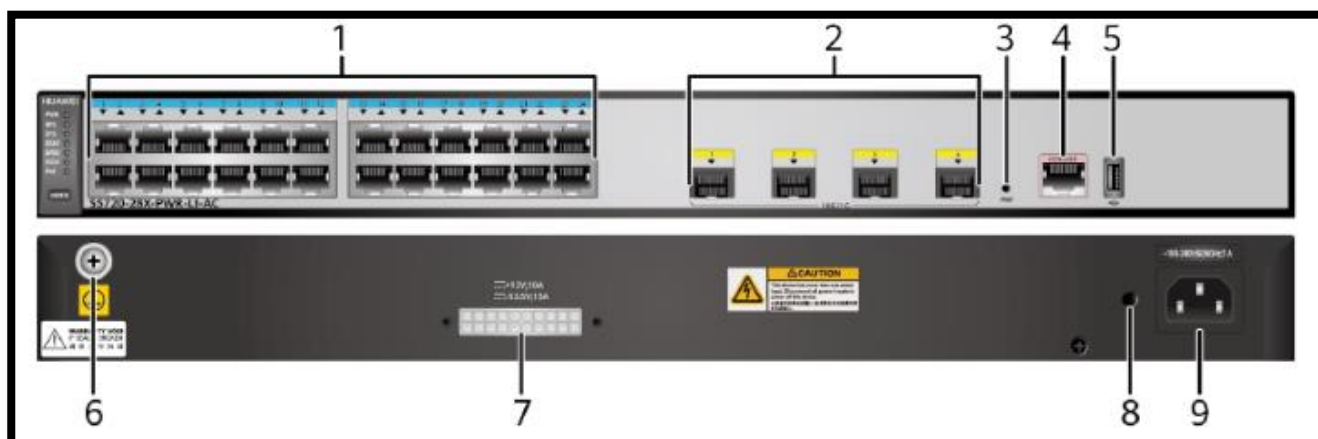


Figure 11: Vue d'ensemble du switch Huawei S5720-28X-PWR-LI-AC

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 NB: 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 NB: Il est utilisé avec un câble de masse.
7	Prise RPS NB: Il est utilisé avec un câble RPS, qui n'est pas remplaçable à chaud.
	Prise pour sangle de verrouillage du câble d'alimentation CA

8	NB: La sangle de verrouillage du câble d'alimentation CA n'est pas fournie avec le commutateur.
9	Prise secteur NB: 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 6 switches access. Les 6 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.

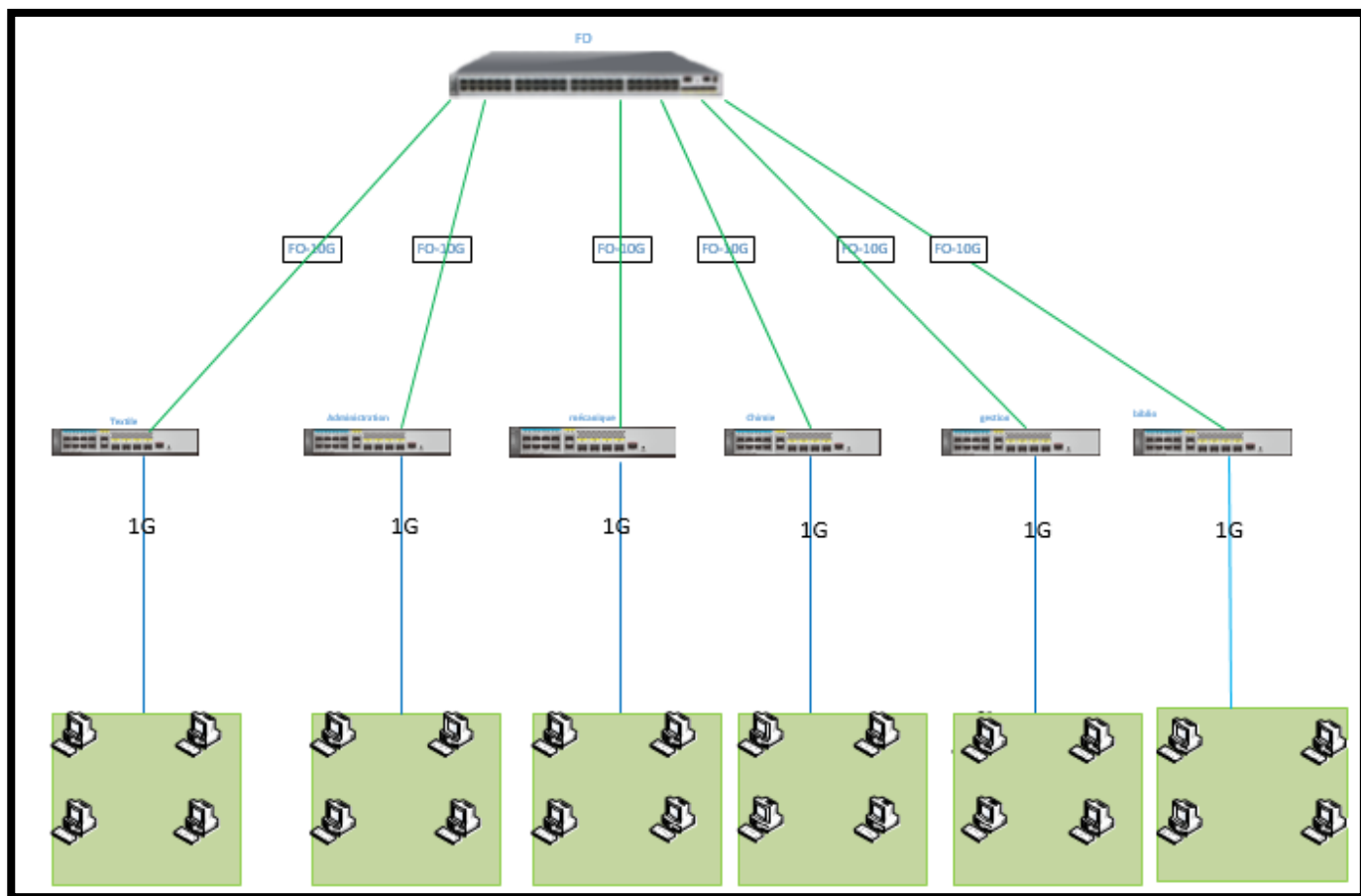


Figure 12: Architecture LAN

3. Switch Access SW-textile

3.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch SW-textile 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-textile

Attributs du switch à configurer	Valeur
Nom	SW-textile
Login / Password	admin / \$SW_Ksar2020
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.2/24
Méthodes de management	SSH, Telnet, http, terminal

3.2 Configuration des interfaces

Tableau 12: Les interfaces de switch SW-textile

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	32	-	Management (172.31.32.2/24)
GigabitEthernet 0/0/1	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/2	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/3	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/4	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/5	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/6	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/7	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/8	Access	46	-	Vers prise pour étudiant
GigabitEthernet 0/0/9	Access	46	-	Vers prise pour étudiant
GigabitEthernet 0/0/10	Access	46	-	Vers prise pour étudiant
GigabitEthernet 0/0/11	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/12	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/13	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/14	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/15	Access	44	-	Vers prise pour étudiant
GigabitEthernet 0/0/16	-	-	-	Vide
GigabitEthernet 0/0/17	-	-	-	Vide
GigabitEthernet 0/0/18	-	-	-	Vide
GigabitEthernet 0/0/19	-	-	-	Vide
GigabitEthernet 0/0/20	-	-	-	Vide
GigabitEthernet 0/0/21	-	-	-	Vide
GigabitEthernet 0/0/22	-	-	-	Vide
GigabitEthernet 0/0/23	-	-	-	Vide
GigabitEthernet 0/0/24	Access	30	-	Port management
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

4. Switch Access SW-Administration

4.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch SW-Administration 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-Administration

Attributs du switch à configurer	Valeur
Nom	SW-Administration
Login / Password	admin / \$SW_Ksar2020
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.3/24
Méthodes de management	SSH, Telnet, http, terminal

4.2 Configuration des interfaces

Tableau 14: Les interfaces de switch SW-Administration

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	32	-	Management (172.31.32.3/24)
GigabitEthernet 0/0/1	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/2	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/3	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/4	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/5	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/6	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/7	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/8	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/9	Access	37	-	Vers prise de l'administration

GigabitEthernet 0/0/10	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/11	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/12	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/13	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/14	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/15	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/16	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/17	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/18	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/19	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/20	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/21	Access	40	-	Vers caméra
GigabitEthernet 0/0/22	Access	40	-	Vers caméra
GigabitEthernet 0/0/23	Access	99	-	Vers RNIA
GigabitEthernet 0/0/24	Access	32	-	Port management
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

5. Switch Access SW-mecanique

5.1 Configuration initiale

Le tableau suivant présente la configuration de base du switch SW-mecanique 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-mecanique

Attributs du switch à configurer	Valeur
Nom	SW-mecanique
Login / Password	admin / \$SW_Ksar2020
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.4/24
Méthodes de management	SSH, Telnet, http, terminal

5.2 Configuration des interfaces

Tableau 16: Les interfaces de switch SW-mecanique

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	32	-	Management (172.31.32.4/24)
GigabitEthernet 0/0/1	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/2	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/3	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/4	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/5	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/6	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/7	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/8	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/9	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/10	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/11	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/12	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/13	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/14	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/15	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/16	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/17	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/18	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/19	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/20	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/21	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/22	Trunk	90 120 130 140 141 142 160	90	Vers AP

GigabitEthernet 0/0/23	-	-	-	Vide
GigabitEthernet 0/0/24	Access	32	-	Port management
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

6. Switch Access SW-Chimie

6.1 Configuration initiale

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

Tableau 17: Configuration initiale du SW-Chimie

Attributs du switch à configurer	Valeur
Nom	SW-Chimie
Login / Password	admin / \$SW_Ksar2020
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.5/24
Méthodes de management	SSH, Telnet, http, terminal

6.2 Configuration des interfaces

Tableau 18: Les interfaces de switch SW-Chimie

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	32	-	Management (172.31.32.5/24)
GigabitEthernet 0/0/1	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/2	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/3	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/4	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/5	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/6	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/7	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/8	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/9	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/10	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/11	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/12	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/13	Access	45	-	Vers prise pour étudiant
GigabitEthernet 0/0/14	Access	45	-	Vers prise pour étudiant

GigabitEthernet 0/0/15	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/16	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/17	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/18	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/19	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/20	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/21	-	-	-	Vide
GigabitEthernet 0/0/22	-	-	-	Vide
GigabitEthernet 0/0/23	-	-	-	Vide
GigabitEthernet 0/0/24	Access	32	-	Port management
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 SW-Gestion

7.1 Configuration initiale

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

Tableau 19: Configuration initiale du SW-Gestion

Attributs du switch à configurer	Valeur
Nom	SW-Gestion
Login / Password	admin / \$SW_Ksar2020
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.6/24
Méthodes de management	SSH, Telnet, http, terminal

7.2 Configuration des interfaces

Tableau 20: Les interfaces de switch SW-Gestion

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	32	-	Management (172.31.32.6/24)
GigabitEthernet 0/0/1	Access	190	-	Vers PC de l'administrateur
GigabitEthernet 0/0/2	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/3	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/4	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/5	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/6	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/7	Access	44	-	Vers prise pour étudiant
GigabitEthernet 0/0/8	Access	44	-	Vers prise pour étudiant
GigabitEthernet 0/0/9	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/10	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/11	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/12	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/13	Access	40	-	Vers caméra
GigabitEthernet 0/0/14	-	-	-	Vide
GigabitEthernet 0/0/15	-	-	-	Vide
GigabitEthernet 0/0/16	-	-	-	Vide
GigabitEthernet 0/0/17	-	-	-	Vide
GigabitEthernet 0/0/18	-	-	-	Vide
GigabitEthernet 0/0/19	-	-	-	Vide
GigabitEthernet 0/0/20	-	-	-	Vide
GigabitEthernet 0/0/21	-	-	-	Vide
GigabitEthernet 0/0/22	-	-	-	Vide
GigabitEthernet 0/0/23	-	-	-	Vide
GigabitEthernet 0/0/24	Access	32	-	Port management
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

8. Switch Access SW-Biblio

8.1 Configuration initiale

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

Tableau 21: Configuration initiale du SW-Biblio

Attributs du switch à configurer	Valeur
Nom	SW-Biblio
Login / Password	admin / admin951
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.7/24
Méthodes de management	SSH, Telnet, http, terminal

8.2 Configuration des interfaces

Tableau 22: Les interfaces de switch SW-Biblio

Port physique	Mode	VLANs	PVID (pour les VLANs WiFi)	Description
Vlanif	-	32	-	Management (172.31.32.7/24)
GigabitEthernet 0/0/1	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/2	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/3	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/4	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/5	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/6	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/7	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/8	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/9	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/10	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/11	Access	37	-	Vers prise de l'administration
GigabitEthernet 0/0/12	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/13	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/14	Access	36	-	Vers prise d'enseignant

GigabitEthernet 0/0/15	Access	36	-	Vers prise d'enseignant
GigabitEthernet 0/0/16	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/17	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/18	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/19	Trunk	90 120 130 140 141 142 160	90	Vers AP
GigabitEthernet 0/0/20	-	-	-	Vide
GigabitEthernet 0/0/21	-	-	-	Vide
GigabitEthernet 0/0/22	-	-	-	Vide
GigabitEthernet 0/0/23	Access	44	-	Vers prise pour étudiant
GigabitEthernet 0/0/24	Access	32	-	Port management
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 23: Spécifications des APs

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

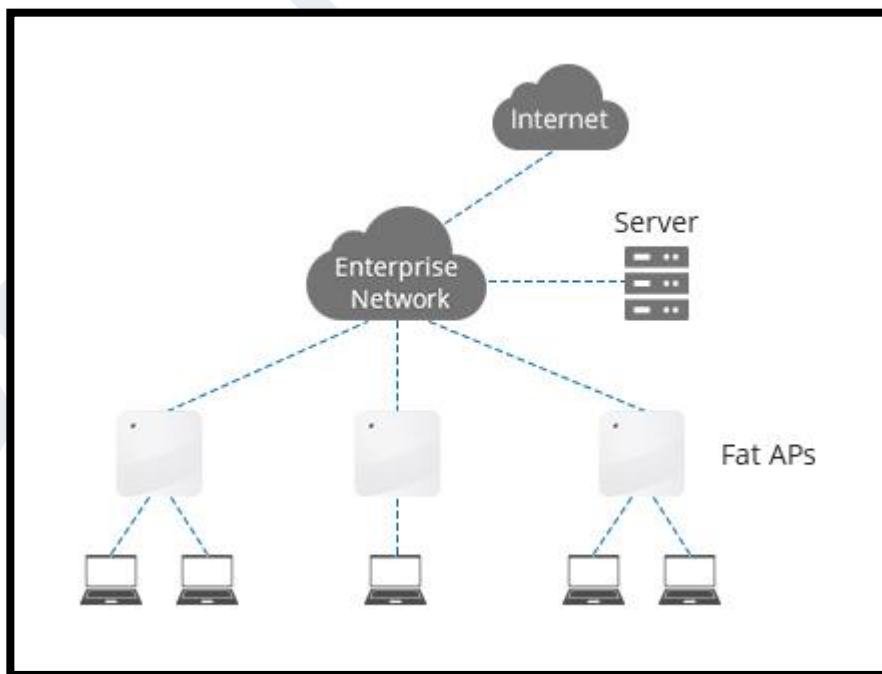


Figure 13: Déploiement des Fat APs

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.

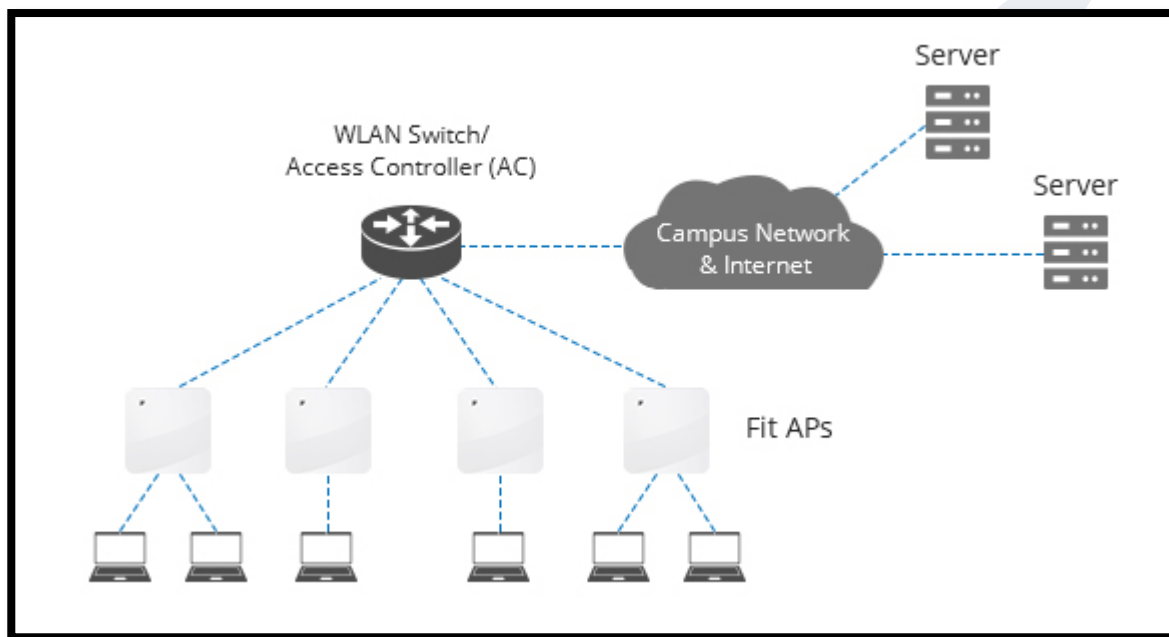


Figure 14: Déploiement des Fit APs + AC

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 24: Liste des APs

Point d'accès	Nom	Adresse MAC	S/N
AP 1	ap-cote-Mastere	d0c6-5b76-a4c0	21500831023GKA019888
AP 2	ap-cote-Association-Textile	18cf-2473-af40	21500831023GKA016674
AP 3	ap-Metrologie	18cf-2473-ae40	21500831023GKA016666
AP 4	ap-Unite-recherche	18cf-2473-ada0	21500831023GKA016661
AP 5	ap-salle-reunion	d0c6-5b76-9e80	21500831023GKA019838

AP 6	ap-RC-cote-cour	d0c6-5b76-9d80	21500831023GKA019830
AP 7	ap-RC-Administration	18cf-2473-ae20	21500831023GKA016665
AP 8	ap-Confection	18cf-2473-b4a0	21500831023GKA016717
AP 9	ap-escalier-1-etage	18cf-2473-ae00	21500831023GKA016664
AP 10	ap-Labo-Mecanique	18cf-2473-ade0	21500831023GKA016663
AP 11	ap-Buvette	d0c6-5b76-9b80	21500831023GKA019814
AP 12	ap-Chimie-Armoire	4467-476e-2280	21500831023GKB031966
AP 13	ap-bureaux-enseignants	4467-476e-2320	21500831023GKB031971
AP 14	ap-Labo-LGTEX	d0c6-5b76-dec0	21500831023GKA020352
AP 15	ap-entre-bloc-chimie	d0c6-5b76-9c00	21500831023GKA019818
AP 16	ap-Hall-chimie	18cf-2473-b560	21500831023GKA016723
AP 17	ap-Labo-info	18cf-2473-b6e0	21500831023GKA016735
AP 18	ap-Gestion-1-etage	18cf-2473-ad80	21500831023GKA016660
AP 19	ap-salle-prof-RC	18cf-2473-ae60	21500831023GKA016667
AP 20	ap-Gestion-Externe	18cf-2473-bb00	21500831023GKA016768
AP 21	ap-Salle-Lecteur	18cf-2473-aea0	21500831023GKA016669
AP 22	ap-Entre-Biblio	18cf-2473-ad60	21500831023GKA016659
AP 23	ap-Amphi-1	18cf-2473-aec0	21500831023GKA016670
AP 24	ap-Amphi-2	18cf-2473-adc0	21500831023GKA016662

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 25: Spécification de Huawei AC6508

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

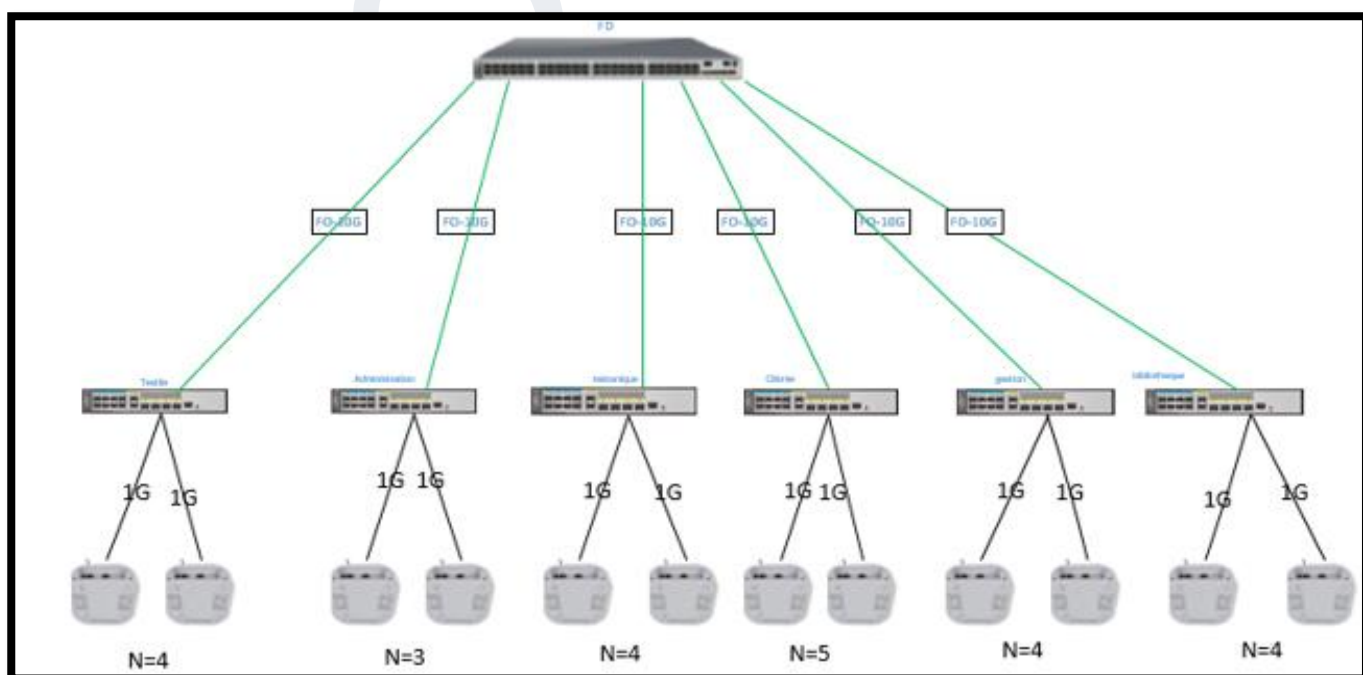


Figure 15: Architecture Wi-Fi

3. Configuration initiale

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

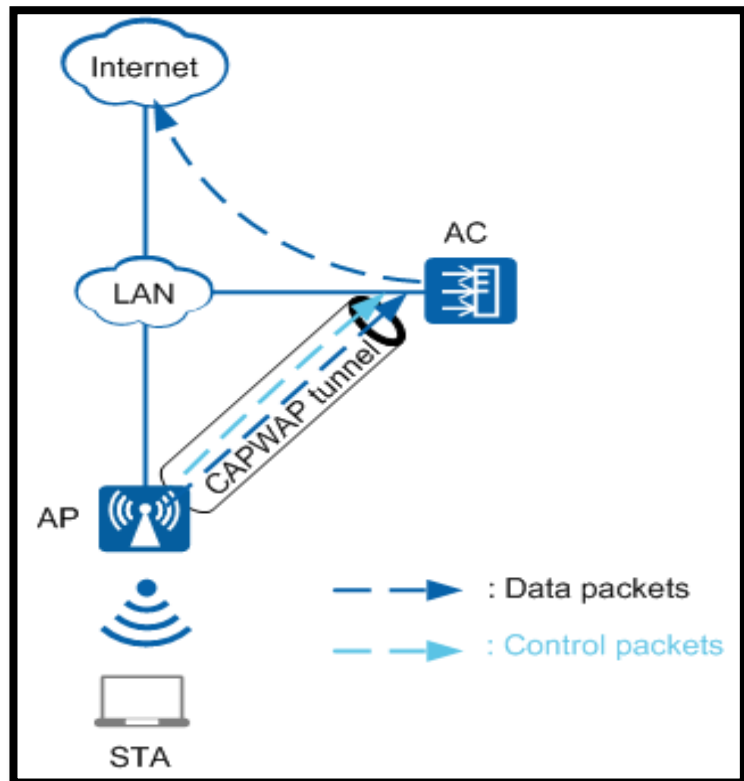
Tableau 26: Configuration de base de l'AC

Paramètres	Valeur
Nom	AC-ISET-Ksar
Adresse de gestion	172.31.32.10
Masque de réseau	255.255.255.0
VLAN de management	32
Login/mot de passe	admin / \$AC_Ksar2020

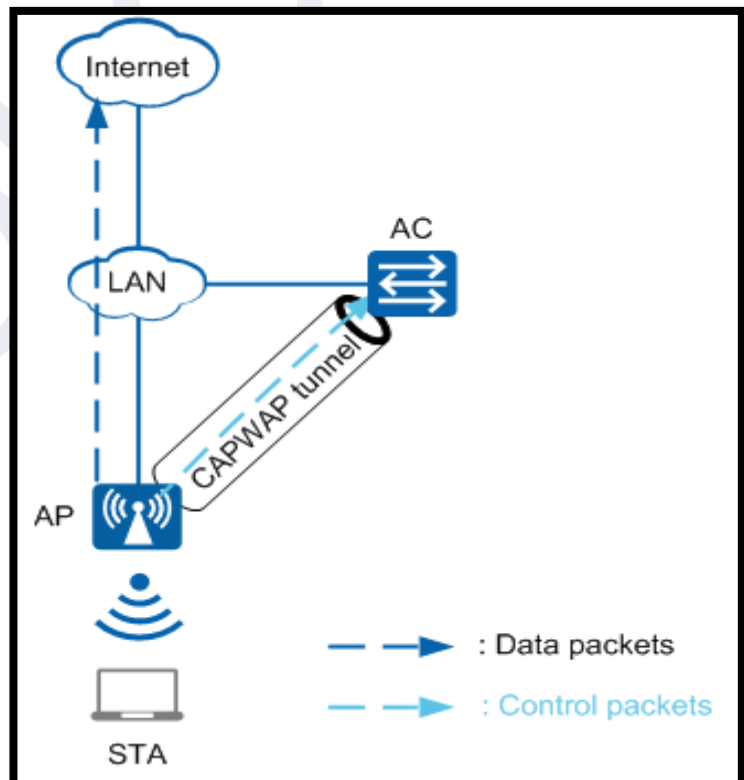
4. Configuration des VLANs Wi-Fi

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 27: 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 28: Liste des VLANs

VLAN ID	NOM
32	MGMT
90	APs
120	ensi
130	administration
140	etudiant
141	etudiant-141
142	etudiant-142
160	guest

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 29: Interfaces de l'AC

Interface	Description	Type	VLANs
GigabitEthernet0/0/1	Liaison avec le switch core	Trunk	ALL
GigabitEthernet0/0/10	Management	Access	32

Configuration:

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/10
 port link-type access
 port default vlan 32
#
```

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

Tableau 30: Interfaces Vlanif de l'AC

Vlanif	IP address	DHCP
32	172.31.32.10/24	Non
90	172.16.90.2/24	Oui
160	172.16.160.100/24	Oui

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-id 1 type-id 75 ap-mac d0c6-5b76-a4c0 ap-sn 21500831023GKA019888

ap-name ap-cote-Mastere

ap-group ap-etu+ens

7. Configuration des SSIDs des APs

Le tableau suivant détaille les paramètres des SSID configurés.

Tableau 31: SSIDs configurés

SSID	VLAN de service	AP Groupe	Mode de transfert	Authentification
ETUD	140, 141, 142	ap-all ap-etu+ens ap-group1 ap-groupe2	Forwarding	Iset_Kh@etud
ENS	120	ap-all	Forwarding	Wi-Fi@Isetkh

		ap-ens ap-etu+ens ap-ens+adm+guest ap-group1 ap-groupe2		
ADM	130	ap-all ap-etu+ens ap-ens+adm+guest ap-group1 ap-groupe2	Forwarding	Adm#Iset@kh
Guest	160	ap-all ap-etu+ens ap-ens+adm+guest ap-group1 ap-groupe2	Tunnel	Guest@Iset*Kh

8. Configuration des VAP profiles

Le tableau suivant détaille les paramètres des quatre VAP profiles configurés.

Tableau 32: VAP profiles

VAP profil	VLAN de service	SSID profil	Smart Roaming
Guest	160	Guest	Activé
Etudiants	140	ETUD	Activé
Etudiants-141	141	ETUD	Activé
Etudiants-142	142	ETUD	Activé
Enseignants	120	ENS	Activé
Administration	130	ADM	Activé

9. AP groups

Dans l'iset, le contrôleur gère 24 FIT AP. Pour simplifier et faciliter les opérations, nous avons distribué les APs sur trois 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-all	Enseignants Etudiants Administration Guest Etudiants-141 Etudiants-142	7	2.4G	5G	5G	domain1
ap-ens	Enseignants	1	2.4G	5G	5G	domain1
ap-etu+ens	Enseignants Etudiants Etudiants-141 Etudiants-142	8	2.4G	5G	5G	domain1
ap-ens+adm+guest	Enseignants Administration Guest	4	2.4G	5G	5G	domain1
ap-group1	Enseignants Etudiants Administration Guest Etudiants-141 Etudiants-142	2	2.4G	5G	5G	domain1
ap-groupe2	Enseignants Etudiants Administration Guest Etudiants-141 Etudiants-142	2	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. Nous avons configuré aussi le DHCP du VLAN service WiFi des visiteurs au niveau de l'AC car son mode de transfert est mode tunnel.

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
 option 43 sub-option 3 ascii 172.16.90.2
#
ip pool guest
 gateway-list 172.16.160.1
 network 172.16.160.0 mask 255.255.255.0
 dns-list 8.8.8.8 172.31.33.1 172.31.33.2
#
```

11. Configuration du WDS:

Dans ISET Ksar Hellal, nous avons mis en place un réseau WDS composé des 4 APs. Nous avons 2 APs distants (AP amphi 1 et AP amphi 2) qui ne sont pas connectés à l'AC. Ils disposent seulement d'une alimentation électrique. Dans ce cas, grâce au WDS, ils reçoivent le fichier de configuration de l'AC par l'intermédiaire des 2 autres APs connectés directement à l'AC comme décrit la figure suivante :

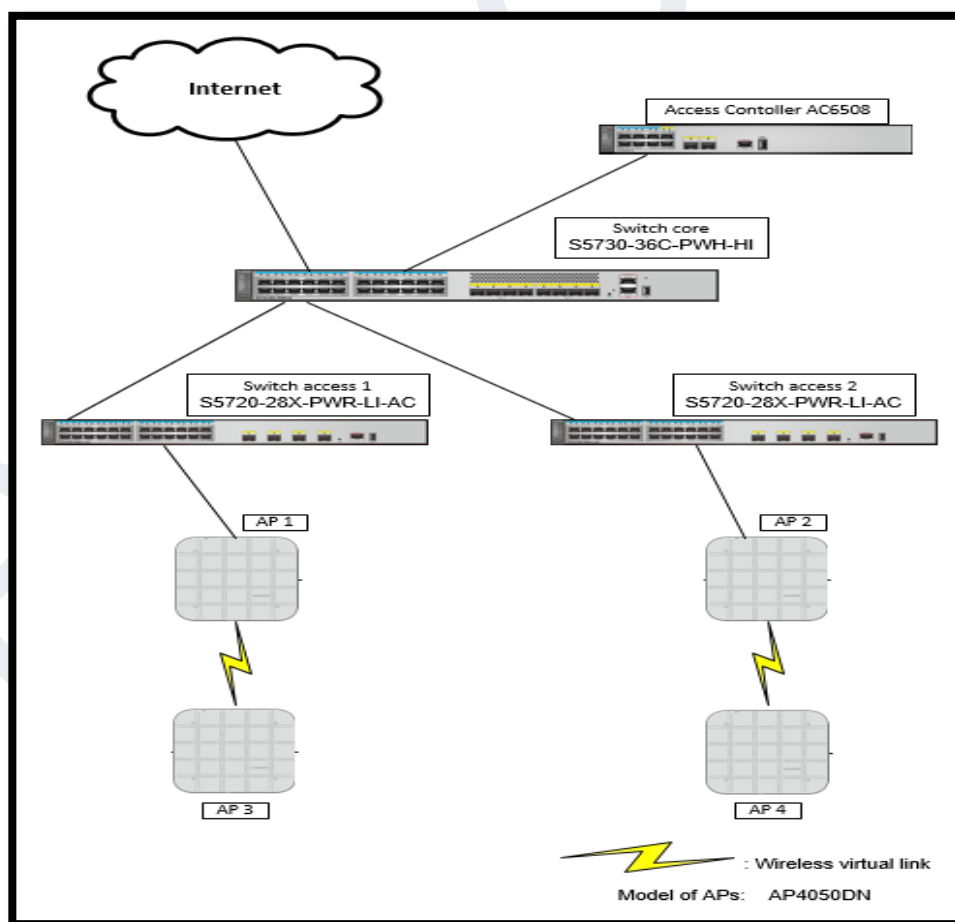


Figure 16: Architecture WDS

Un système de distribution sans fil (WDS) connecte au moins deux réseaux locaux câblés ou sans fil à l'aide de liaisons sans fil pour établir un grand réseau.

Sur un réseau WLAN traditionnel, les points d'accès se connectent à un secteur via des liaisons montantes filaires. Cependant, les connexions filaires sont difficiles ou coûteuses à mettre en œuvre dans les zones où les câbles réseau sont difficiles à déployer, comme les tunnels et les quais. La technologie WDS connecte les points d'accès à un point d'accès à l'aide de liaisons sans fil pour faciliter le déploiement WLAN dans des environnements géographiques complexes, réduire les coûts de déploiement du réseau, permettre une mise en réseau flexible et faciliter l'extension du réseau.

Les points d'accès sur un réseau WDS fonctionnent dans l'un des modes suivants:

- Racine ou root: un point d'accès racine se connecte à un courant alternatif à l'aide d'une liaison filaire et se connecte à un point d'accès intermédiaire ou feuille à l'aide d'une liaison montante sans fil.
- Milieu ou middle: un point d'accès intermédiaire est un nœud intermédiaire utilisant des liaisons sans fil pour connecter un point d'accès racine en amont et un point d'accès feuille en aval.
- Feuille ou leaf: un point d'accès feuille se connecte à un point d'accès racine ou intermédiaire à l'aide d'une liaison sans fil montante.

Les technologies WDS et maillées peuvent implémenter un pontage sans fil entre les points d'accès. Un réseau WDS prend en charge un maximum de trois sauts (par exemple, une liaison WDS peut être établie le long d'un nœud racine, d'un nœud intermédiaire et d'un nœud feuille), possède une topologie arborescente et ne prend pas en charge la redondance de liaison entre les nœuds. D'un autre côté, un réseau maillé prend en charge un maximum de huit sauts, possède une topologie maillée et prend en charge la redondance des liens entre les nœuds. Ces facteurs rendent un réseau maillé plus fiable qu'un réseau WDS. Vous pouvez choisir la technologie WDS ou maillée pour déployer le pontage sans fil entre les points d'accès en fonction de vos besoins de mise en réseau.

Dans notre cas, le scénario de configuration de WDS est comme suit :

Déclaration des profils root et leaf	<pre>wds-whitelist-profile name wds-list1 peer-ap mac 18cf-2473-adc0 peer-ap mac 18cf-2473-aec0 wds-profile name wds-leaf security-profile wds-security vlan tagged 90 120 130 140 to 142 160 wds-name wlan-wds wds-profile name wds-root security-profile wds-security vlan tagged 90 120 130 140 to 142 160 wds-name wlan-wds wds-mode root</pre>
Profil de sécurité du WDS	<pre>security-profile name wds-security security wpa2 psk pass-phrase **** aes</pre>

Création du groupe APs root	ap-group name ap-group1 radio 0 vap-profile Enseignants wlan 1 vap-profile Etudiants wlan 2 vap-profile Administration wlan 3 vap-profile Guest wlan 4 vap-profile Etudiants-141 wlan 5 vap-profile Etudiants-142 wlan 6 radio 1 wds-profile wds-root wds-whitelist-profile wds-list1
Création du groupe APs leaf	ap-group name ap-groupe2 radio 0 vap-profile Enseignants wlan 1 vap-profile Etudiants wlan 2 vap-profile Administration wlan 3 vap-profile Guest wlan 4 vap-profile Etudiants-141 wlan 5 vap-profile Etudiants-142 wlan 6 radio 1 wds-profile wds-leaf
Déclaration de l'AP « ap-Gestion-1-etage » comme AP root	ap-id 18 type-id 75 ap-mac 18cf-2473-ad80 ap-sn 21500831023GKA016660 ap-name ap-Gestion-1-etage ap-group ap-group1 radio 0 eirp 127 calibrate auto-channel-select disable calibrate auto-tpower-select disable radio 1 coverage distance 4 calibrate auto-channel-select disable calibrate auto-tpower-select disable
Déclaration de l'AP « ap-Buvette » comme AP root	ap-id 11 type-id 75 ap-mac d0c6-5b76-9b80 ap-sn 21500831023GKA019814 ap-name ap-Buvette ap-group ap-group1 radio 0 eirp 127 calibrate auto-channel-select disable calibrate auto-tpower-select disable radio 1 coverage distance 4 calibrate auto-channel-select disable calibrate auto-tpower-select disable
Déclaration de l'AP « ap-Amphi-2 » comme AP leaf	ap-id 24 type-id 75 ap-mac 18cf-2473-adc0 ap-sn 21500831023GKA016662 ap-name ap-Amphi-2 ap-group ap-groupe2

	radio 0 vap-profile Enseignants wlan 1 vap-profile Etudiants wlan 2 vap-profile Administration wlan 3 vap-profile Guest wlan 4 frequency 5g eirp 127 calibrate auto-channel-select disable calibrate auto-tpower-select disable radio 1 coverage distance 4 calibrate auto-channel-select disable calibrate auto-tpower-select disable
Déclaration de l'AP «ap-Amphi-1» comme AP leaf	ap-id 23 type-id 75 ap-mac 18cf-2473-aec0 ap-sn 21500831023GKA016670 ap-name ap-Amphi-1 ap-group ap-groupe2 radio 0 vap-profile Enseignants wlan 1 vap-profile Etudiants wlan 2 vap-profile Administration wlan 3 vap-profile Guest wlan 4 eirp 127 calibrate auto-channel-select disable calibrate auto-tpower-select disable radio 1 coverage distance 4 calibrate auto-channel-select disable calibrate auto-tpower-select disable

12. Configuration complète de l'AC

Création de VLAN, description et nom du VLAN	vlan 90 description " vlan pour les APs" name APs
Configuration des pools DHCP	ip pool ap gateway-list 172.16.90.1 network 172.16.90.0 mask 255.255.255.0 option 43 sub-option 3 ascii 172.16.90.2 ip pool guest gateway-list 172.16.160.1 network 172.16.160.0 mask 255.255.255.0 dns-list 8.8.8.8 172.31.33.1 172.31.33.2
Configuration d'interface vlanif, (adresse IP, DHCP)	interface Vlanif32 ip address 172.31.32.10 255.255.255.0

	<pre> interface Vlanif90 ip address 172.16.90.2 255.255.255.0 dhcp select global interface Vlanif160 ip address 172.16.160.100 255.255.255.0 dhcp select global </pre>
Configuration interface trunk vlan ALL	<pre> interface GigabitEthernet0/0/1 port link-type trunk port trunk allow-pass vlan 2 to 4094 </pre>
Configuration de l'interface source du contrôleur	<pre> capwap source interface vlanif90 </pre>
Configuration du security- profile	<pre> security-profile name ensig security wpa2 psk pass-phrase ***** tkip security-profile name guest security wpa2 psk pass-phrase ***** tkip security-profile name etudiant security wpa2 psk pass-phrase ***** tkip security-profile name administration security wpa2 psk pass-phrase ***** tkip security-profile name administration security wpa2 psk pass-phrase ***** tkip security-profile name wds-security security wpa2 psk pass-phrase ***** tkip </pre>
Configuration d'un SSID	<pre> ssid-profile name adm ssid ADM ssid-profile name ens ssid ENS ssid-profile name etu ssid ETU ssid-profile name Guest ssid Guest </pre>
Configuration du VAP profile, (service vlan, SSID, security profile)	<pre> vap-profile name Guest forward-mode tunnel service-vlan vlan-id 160 ssid-profile Guest security-profile guest </pre>

	vap-profile name default vap-profile name Etudiants service-vlan vlan-id 140 ssid-profile etu security-profile etudiant vap-profile name Enseignants service-vlan vlan-id 120 ssid-profile ens security-profile ensig vap-profile name Etudiants-141 service-vlan vlan-id 141 ssid-profile etu security-profile etudiant vap-profile name Etudiants-142 service-vlan vlan-id 142 ssid-profile etu security-profile etudiant vap-profile name Administration service-vlan vlan-id 130 ssid-profile adm security-profile administration
Configuration du domaine	regulatory-domain-profile name domain1 country-code TN
Création de groupe des points d'accès, affectation du vap profile à un groupe ap avec radio all (exemple ap-ens)	ap-group name ap-ens regulatory-domain-profile domain1 radio 0 vap-profile Enseignants wlan 1 radio 1 vap-profile Enseignants wlan 1 radio 2 vap-profile Enseignants wlan 1
Ajout d'AP avec MAC adresse, name AP, ID-AP, groupe ap	ap-id 2 type-id 75 ap-mac 18cf-2473-af40 ap-sn 21500831023GKA016674 ap-name ap-cote-Association-Textile ap-group ap-ens+adm+guest

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.

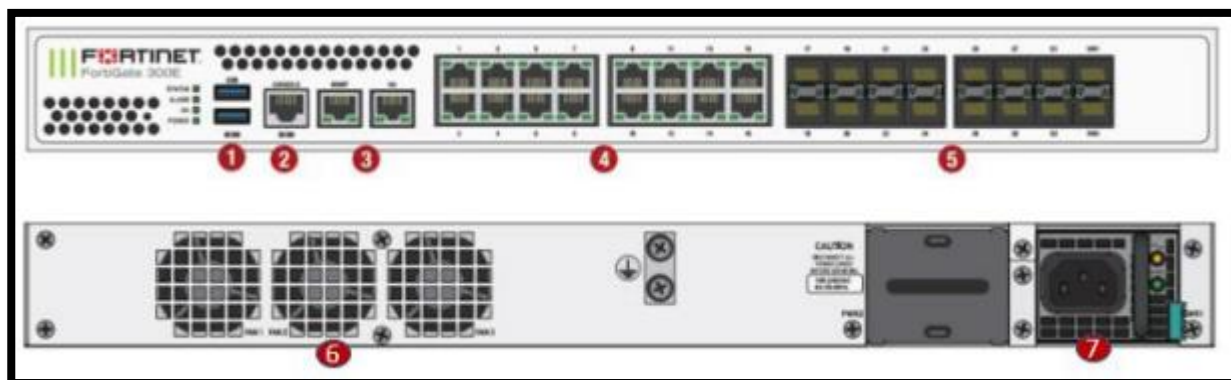


Tableau 33: Ports du Fortigate 301E

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

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 :

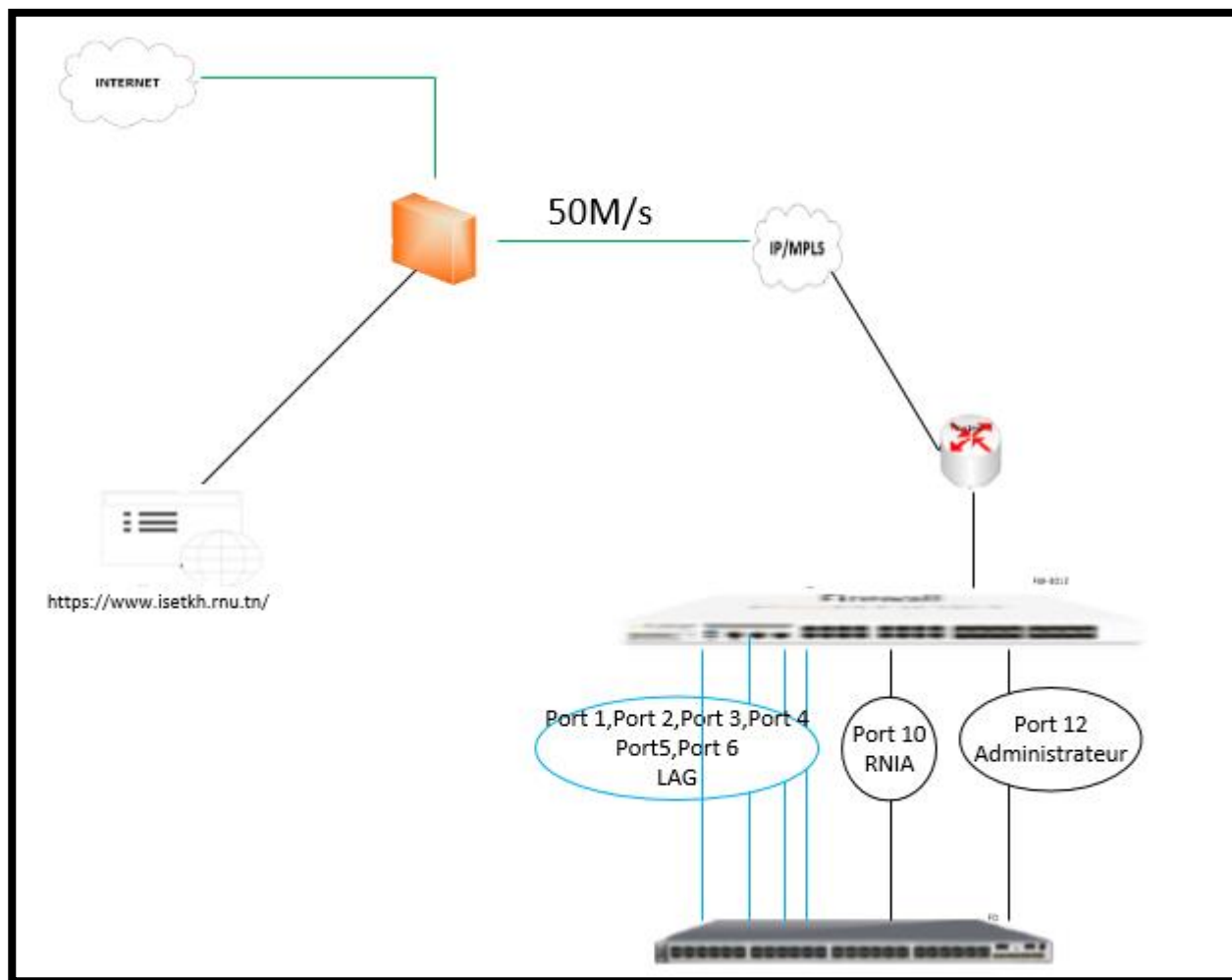


Figure 17: Architecture WAN

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 34: Configuration initiale du firewall Fortigate

Attributs du switch à configurer	Valeur
Nom	ISET-KsarHlel
Login / Password	admin / \$FGT_SL@isetkh
Vlan de management	vlan 32 (name MGMT)
Adresse IP de management	172.31.32.254/24
Méthodes de management	SSH, Telnet, http, terminal
S/N	FG3H1E5819902989

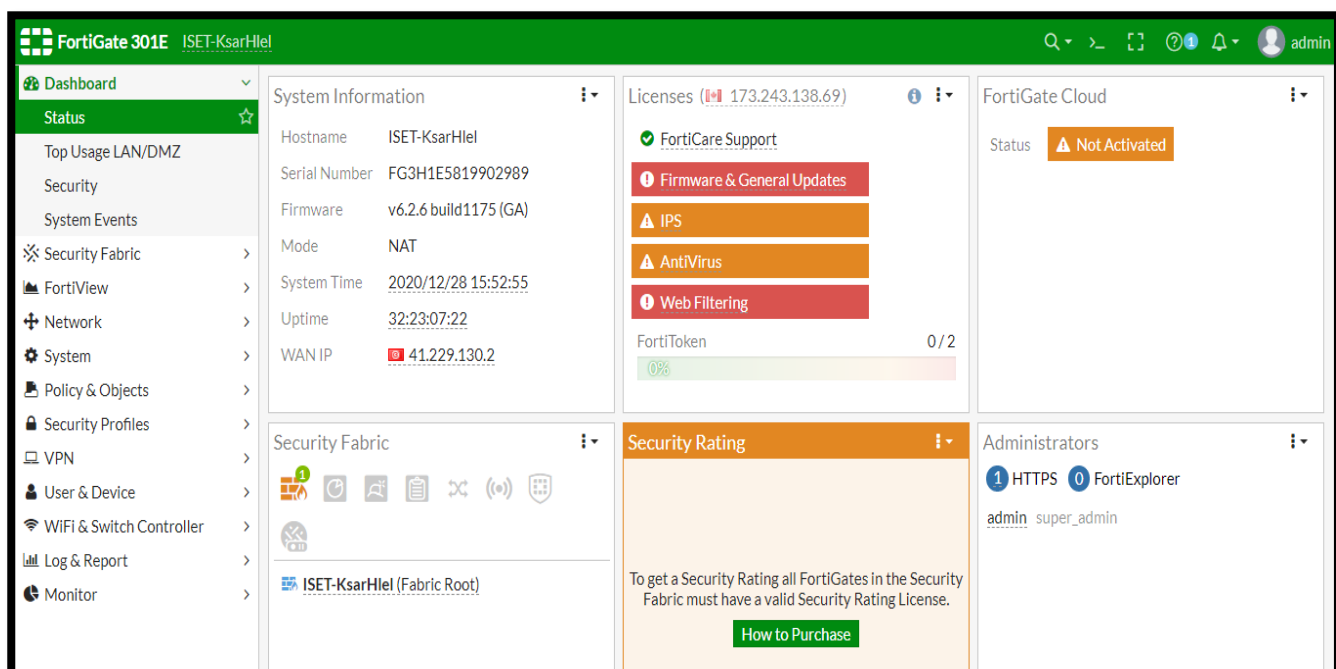


Figure 18: Interface Dashboard du FortiGate

4. Configuration des interfaces

Nous avons configuré l'interface d'agrégation de lien en combinant six ports (port 1, port 2, port3 et port 4 et port 5 et port 6) comme le montre la figure ci-dessus et le port 7 comme interface WAN avec l'adresse IP 41.229.130.2/24.

NOM DE L'INTERFACE	PORT	IP/NETMASK
LAG	Port1	20.20.20.1/30
	Port2	
	Port3	
	Port4	
	Port5 (MGMT)	
	Port6 (SERV)	
WAN	Port7	41.229.130.2/24
RNIA	Port10	192.168.99.250/24
Administrateur (VLAN 190)	Port 12	172.31.190.1/30

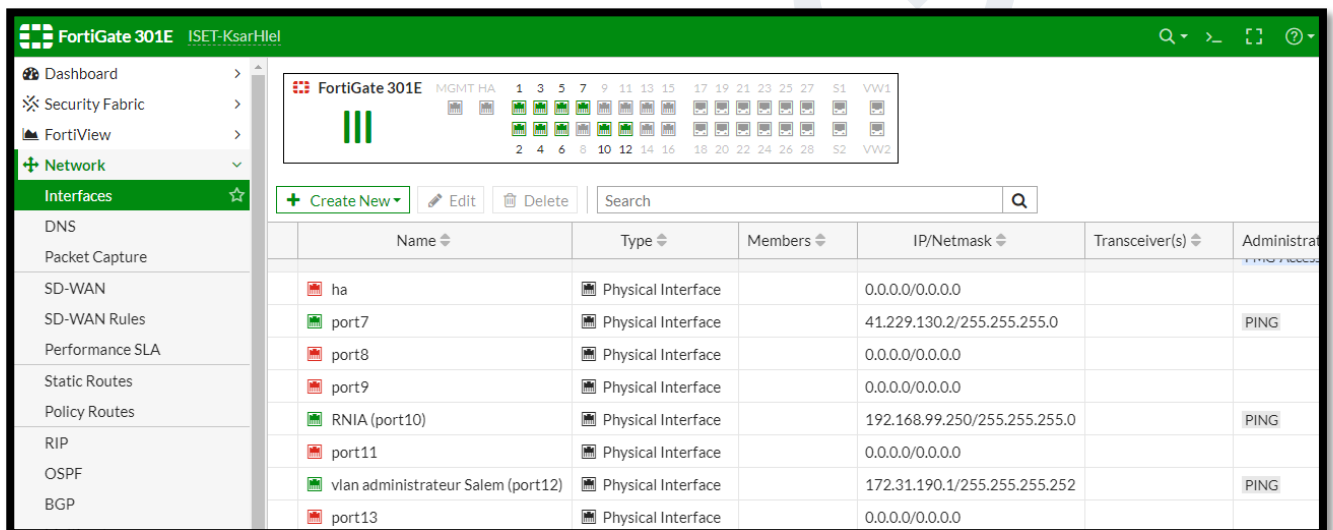
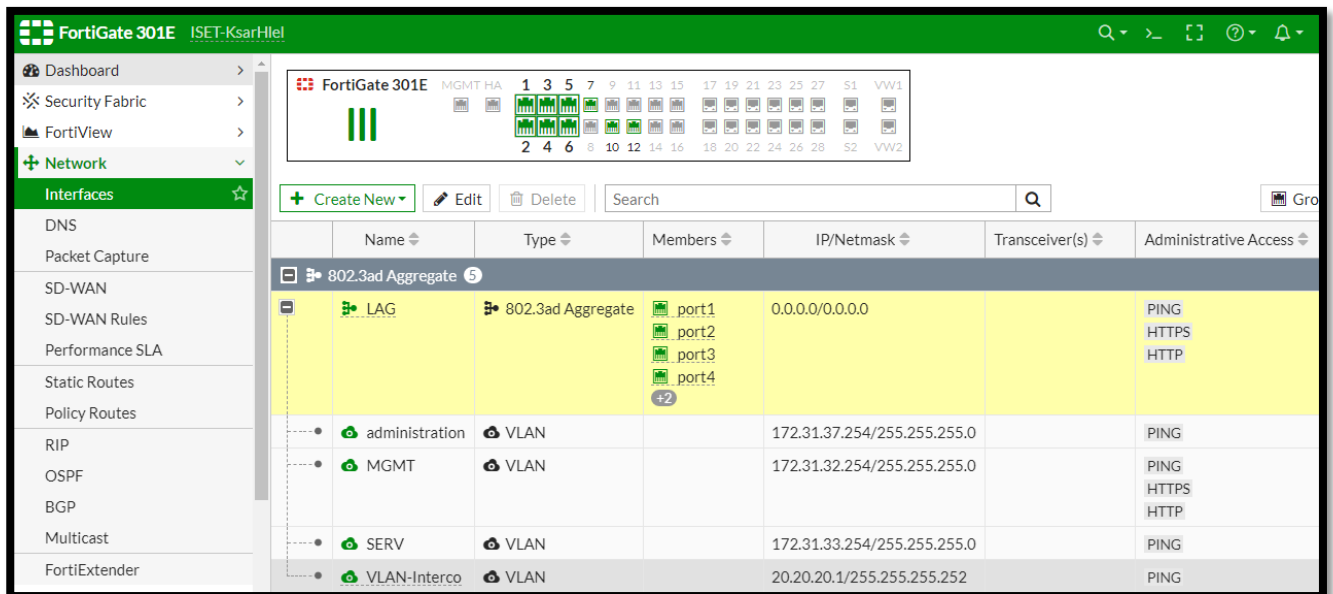


Figure 19: Configuration des interfaces du firewall

5. Configuration des routes

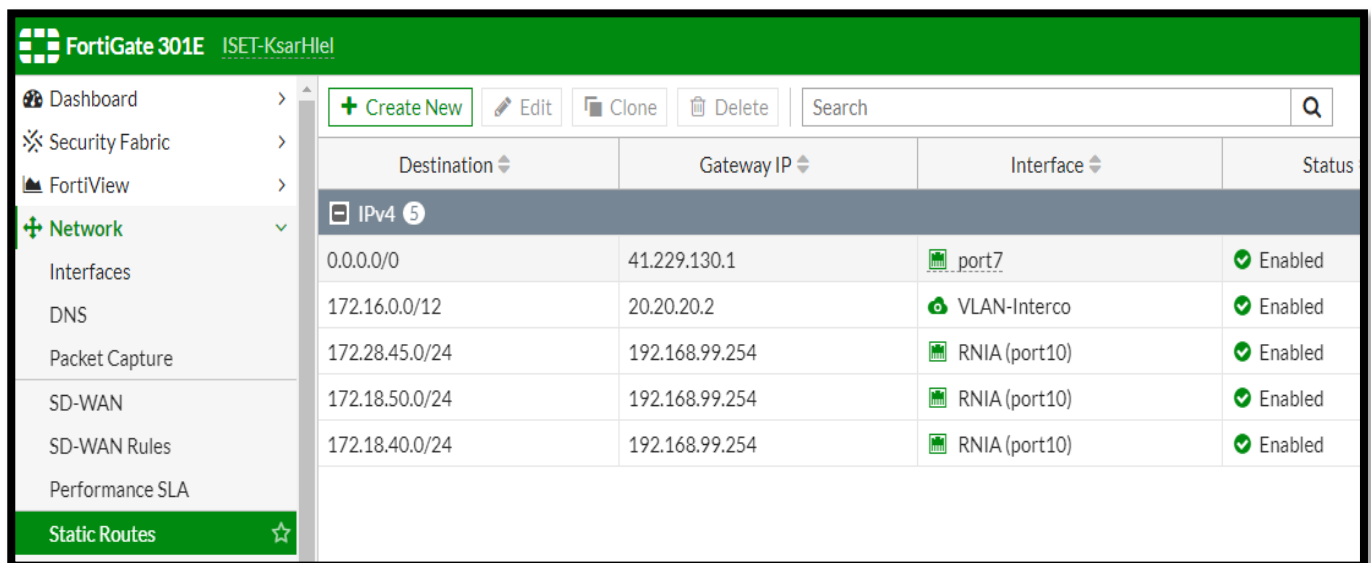
Dans le firewall, nous avons configuré les routes suivantes :

Tableau 35: Table de routage

SOURCE DANS LE FW	GATEWAY	DESTINATION	DESCRIPTION
Port 7 : 41.229.130.2	@ du routeur : 41.229.130.1	0.0.0.0/0	Internet
VLAN-Interco	LAG dans SW FD : 20.20.20.2	172.16.0.0/12	Trafic FD-FW

6. Routes statiques

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



Destination	Gateway IP	Interface	Status
IPv4 5			
0.0.0.0/0	41.229.130.1	port7	Enabled
172.16.0.0/12	20.20.20.2	VLAN-Interco	Enabled
172.28.45.0/24	192.168.99.254	RNIA (port10)	Enabled
172.18.50.0/24	192.168.99.254	RNIA (port10)	Enabled
172.18.40.0/24	192.168.99.254	RNIA (port10)	Enabled

Figure 20: 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 36: Les règles de sécurité

Nom	Source Zone	Src @IP	Dst Zone	Dst @IP	Service	NAT
Wired-to-net	SERV VLAN-Interco	all	WAN	all	all	Enabled
SERV-VLAN	Administration VLAN-Interco	all	SERV	all	all	Disabled
SERV-to-Internet	SERV	all	WAN	all	all	Enabled
SSL-VPN	SSL-VPN	all	Administration MGMT SERV VLAN-Interco	all	all	Enabled
Salem-vers-all	Port 12	all	Administration MGMT SERV VLAN-Interco	all	all	Enabled
Administration-to-NET	administration	all	WAN	all	all	Enabled

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

FortiGate 301E ISET-KsarHlel							
<div> <div>Dashboard</div> <div>Security Fabric</div> <div>FortiView</div> <div>Network</div> <div>System</div> <div>Policy & Objects</div> <div>IPv4 Policy</div> <div>IPv4 Virtual Wire Pair Policy</div> <div>Authentication Rules</div> <div>Multicast Policy</div> <div>IPv4 Access Control List</div> <div>IPv4 DoS Policy</div> <div>Addresses</div> <div>Internet Service</div> </div> <div> <div>Create New</div> <div>Edit</div> <div>Delete</div> <div>Policy Lookup</div> <div>Search</div> <div>Interface Pair View</div> <div>By Sequence</div> </div>							
ID	Name	From	To	Source	Destination	Schedule	Service
4	Wi-Fi_to_Net	port8	port7	all	all	always	ALL
7	Wired-to-net	administration Enseignants Etudiants visiteur	port7	all	all	always	ALL
5	SERV-VLAN	administration Enseignants Etudiants port8	SERV (port6)	all	all	always	ALL
6	to cni	administration	RNA (port10)	Groupe- Adab	adeb1 adeb2 mankoulet	always	HTTP HTTPS tcp-1541 tcp-1551 tcp-1561 tcp-1571

IPv4 Virtual Wire Pair Policy	9	dns-cni	administration	RNA (port10)	Groupe- Adab	dns-cni	always	DNS
Authentication Rules	8	SERV-to-Internet	SERV (port6)	port7	all	all	always	ALL
Multicast Policy	10	SSL-VPN	SSL-VPN tunnel interface (ssl.root)	Management (port5) administration Enseignants Etudiants LAG	all Admin+Support	MGMT all lan	always	ALL
IPv4 Access Control List	11	Salem-vers-all	vlan administrateur Salem (port12)	LAG Management (port5) port7 port8 administration Enseignants	all	all	always	ALL
IPv4 DoS Policy								
Addresses								
Internet Service Database								
Services								
Schedules								

Figure 21: Les règles de sécurité

III. Conclusion

Pendant ce projet, nous avons fait une étude détaillée du réseau informatique d'ISET Ksar Hellal 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 les besoins de notre client, ISET Ksar Hellal, 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.