I. Plan d'adressage IP :

Le plan d'adressage IP **192.168.10.0 /27** est attribué au siège social et aux agences. Nous avons choisi un réseau de classe C car il nous permet d'avoir un nombre important de réseaux (environ 2097152 réseaux) et un nombre faible d'hôtes (environ 254 hôtes) ce qui est en matière d'utilisateurs. Avec un CIDR de 27, il y aura seulement 30 machines disponibles par sous-réseau.

A- Siège Social :

Le plan d'adressage IP **192.168.10.0 /27** est attribué au siège social.

Ci-dessous, le plan d'adressage IP du siège social :

VLAN SIEGE SOCIAL	**VLAN 1 DSI**	**VLAN 2 SRH**	**VLAN 3 SFC**	**VLAN 4 SAB**	**VLAN 5 SAP**
Masque	255.255.255.224	255.255.255.224	255.255.255.224	255.255.255.224	255.255.255.224
Adresse du réseau	**192.168.10.0/27**	**192.168.20.0/27**	**192.168.30.0/27**	**192.168.40.0/27**	**192.168.50.0/27**
Adresse de diffusion	**192.168.10.31**	**192.168.20.31**	**192.168.30.31**	**192.168.40.31**	**192.168.50.31**
Plage adresse DHCP 1	192.168.10.2 192.168.10.30	192.168.20.2 192.168.20.30	192.168.30.2 192.168.30.30	192.168.40.2 192.168.40.30	192.168.50.2 192.168.50.30
Serveurs DHCP	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)
Passerelle	**192.168.10.30**	**192.168.20.30**	**192.168.30.30**	**192.168.40.30**	**192.168.50.30**

VLAN SIEGE SOCIAL	**VLAN 6 SFP**	**VLAN 100 SERVEUR DHCP**	**VLAN DMZ**
Masque	255.255.255.224	255.255.255. 248	255.255.255.248
Adresse du réseau	**192.168.60.0/27**	**192.168.1.0/29**	**192.168.2.0/29**
Adresse de diffusion	**192.168.60.31**	**192.168.1.7**	**192.168.2.7**
Plage adresse DHCP 1	192.168.60.3 192.168.60.30	192.168.1.2 192.168.1.6	
Serveurs DHCP	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	
Passerelle	**192.168.60.30**	**192.168.1.6**	**192.168.2.6**

Ensuite, voici le plan de brassage :

SW1-Siège	Ports
VLAN10 (DSI)	**Port 2 à 10**
VLAN20 (SRH)	**Port 11 à 20**
VLAN 60 (SFP)	**Port 21 à 22**
VLAN 100 (SRV)	**Port 23**
Imprimante (DSI)	**Port 10**
Trunk	**Port 1**
SW2-Siège	**Ports**
VLAN30 (SFC)	**Port 1 à 10**
VLAN40 (SAP)	**Port 11 à 16**
VLAN 50 (SAB)	**Port 17 à 20**
Imprimante (SFC-C)	**Port 23**
Trunk	**Port 24**

B- Agences :

Le plan d'adressage IP **192.168.50.0 /26** est attribué au siège social.

Nous avons choisi ce CIDR (/26) car il va nous permettre d'avoir un total de 62 machines par sous-réseau.

VLAN Agences	VLAN 51 Agence 1	VLAN 52 Agence 2	VLAN 53 Agence 3	VLAN 54 Agence 4	VLAN 55 Agence 5
Masque	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192
Adresse du réseau	**192.168.51.0/26**	**192.168.52.0/26**	**192.168.53.0/26**	**192.168.54.0/26**	**192.168.55.0/26**
Adresse de diffusion	**192.168.51.63**	**192.168.52.63**	**192.168.53.63**	**192.168.54.63**	**192.168.55.63**
Serveurs DHCP	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)
Plage adresse DHCP 1	192.168.51.2 192.168.51.62	192.168.52.2 192.168.52.62	192.168.53.2 192.168.53.62	192.168.54.2 192.168.54.62	192.168.55.2 192.168.55.62
Passerelle	**192.168.51.62**	**192.168.52.62**	**192.168.53.62**	**192.168.54.62**	**192.168.55.62**

VLAN Agences	VLAN 56 Agence 6	VLAN 57 Agence 7	VLAN 58 Agence 8	VLAN 59 Agence 9	VLAN 60 Agence 10
Masque	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192

Adresse du réseau	**192.168.56.0/26**	**192.168.57.0/26**	**192.168.58.0/26**	**192.168.59.0/26**	**192.168.60.0/26**
Adresse de diffusion	**192.168.56.63**	**192.168.57.63**	**192.168.58.63**	**192.168.59.63**	**192.168.60.63**
Serveurs DHCP	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)
Plage adresse DHCP 1	192.168.56.2 192.168.56.62	192.168.57.2 192.168.57.62	192.168.58.2 192.168.58.62	192.168.59.2 192.168.59.62	192.168.60.2 192.168.60.62
Passerelle	**192.168.56.62**	**192.168.57.62**	**192.168.58.62**	**192.168.59.62**	**192.168.60.62**

VLAN Agences	**VLAN 61 Agence 11**	**VLAN 62 Agence 12**	**VLAN 63 Agence 13**	**VLAN 64 Agence 14**	**VLAN 65 Agence 15**
Masque	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192
Adresse du réseau	**192.168.61.0/26**	**192.168.62.0/26**	**192.168.63.0/26**	**192.168.64.0/26**	**192.168.65.0/26**
Adresse de diffusion	**192.168.61.63**	**192.168.62.63**	**192.168.63.63**	**192.168.64.63**	**192.168.65.63**
Serveurs DHCP	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)	192.168.1.2 (DHCP 1)
Plage adresse DHCP 1	192.168.61.2 192.168.61.62	192.168.62.2 192.168.62.62	192.168.63.2 192.168.63.62	192.168.64.2 192.168.64.62	192.168.65.2 192.168.65.62
Passerelle	**192.168.61.62**	**192.168.62.62**	**192.168.63.62**	**192.168.64.62**	**192.168.65.62**

DHCP	**DHCP Agence**
Masque	255.255.255. 248
Adresse du réseau	**192.168.2.0/29**
Adresse de diffusion	**192.168.2.7**
Plage adresse DHCP 1	**192.168.2.2 192.168.2.6**

Brassage switch des agences (en rapport avec la maquette) :

Switch :

SW1-Agence-1	**Ports**

VLAN 51 (Agence 1)	Ports 3 à 19
VLAN 100 (SRV)	Port 24
Imprimante	Port 3
Trunk	Port 23 et 22

SW2-Agence-2	Ports
VLAN 52 (Agence 2)	Ports 3 à 15
VLAN 100 (SRV)	Ports 21 à 22
Imprimante	Port 4
Trunk	Port 23 et 24

Brassage Agence 1 :

ROU1-Agence-1	Ports	Encapsulation
VLAN 51 (Agence 1)	Port 2 à 10	0/0.51
VLAN 100 (SRV)	Port 21 à 22	0/0.100

Brassage agence 2 :

ROU2-Agence-2	Ports	Encapsulation
VLAN 52 (Agence 2)	Port 2 à 10	0/0.52
VLAN 100 (SRV)	Port 21 à 22	0/0.100

VPNSEC :

Agence 1 :

VPNsec	Ports	IP route
SW1-Agence-1	Port g0/0	192.168.51.252/30
ROU-Vpsec1	Port Se0/0/0	10.1.1.1/30

Agence 2 :

VPNsec	Ports	IP route
SW2-Agence-2	Port g0/1	192.168.52.252/30
ROU-Vpsec2	Port Se0/0/1	15.1.1.1/30

VPN :

ROU_VPN	Ports	IP Route
DMZ	Port g0/0	192.168.1.1/29
ROU-Vpsec1	Port S0/0/0	15.1.1.2/30

ROU-Vpsec2	Port S0/0/1	10.1.1.2/30

De plus, le Vlan Serveur qui regroupe le DHCP, l'AD, les serveurs de gestion, de backup et de maintenance sont placés dans le réseau **192.168.2.0/29**.

II. Protection de l'infrastructure :

L'augmentation de l'activité en télétravail engendre des risques de cyber-attaques. L'accès à internet doit se faire de manière sécurisée. Pour cela nous utiliserons plusieurs protocoles comme :

- Le **protocole SSH** afin de pouvoir effectuer une administration à distance en mode sécurisé.
- Le **protocole Access List** cette fonctionnalité permet à l'administrateur de réseau de filtrer les paquets entrants ou sortant dans le routeur. On retrouve deux types d'ACL :
- **Access List Standard** : seul l'adresse IP est utilisée pour le filtrage.
- **Extended Access List** : la source et la destination de l'adresse IP et du port sont utilisées pour le filtrage.

a) Pare-feu :

Pour cela nous avons choisi d'installer deux pares-feux sur l'ensemble de l'infrastructure avec une zone démilitarisée (DMZ).

On rappelle que la zone démilitarisée est un sous-réseau contenant des machines qui sont susceptibles d'être accédé via internet. Ce sous-réseau est séparé du réseau local et isolé via un pare-feu. Dès lors, le réseau est séparé en deux :

L'Inside Zone **:** qui représente la zone interne à l'entreprise (donc le réseau avec vlan et les machines).

L'Outside Zone **:** qui représente la zone extérieure à l'entreprise comme Internet par exemple ou dans ce contexte, l'IT CLOUD.

Le périmètre de sécurité est représenté par les fonctions suivantes :

- Un pare-feu ;
- Une DMZ ;
- Un VPN entre le réseau interne du siège social et des agences vers le réseau externe d'IT CLOUD

Nous avons choisi cette infrastructure avec une zone démilitarisée car l'entreprise possède ses serveurs sur l'hébergeur IT CLOUD. Dès lors, une protection est nécessaire contre les intrusions provenant de réseau externe.

Pour cette infrastructure nous avons préconisé le pare-feu CISCO ASA.

Cette solution propose un éventail de services comme :

- Une robuste sécurité Web, sur site ou en nuage ;
- Un système complet de prévention des intrusions (IPS) pour protéger les réseaux contre les menaces connues ;
- Protection complète contre les menaces et les programmes malveillants évolués ;

b) VPN

Un VPN est un réseau privé virtuel qui permet de configurer un canal sécurisé pour la navigation en ligne. On peut alors établir une connexion cryptée et sécurisée entre un serveur et des machines. Nous avons choisi d'utiliser le service **PureVPN**.

PureVPN fournit un cryptage de niveau militaire qui permet de sécuriser toutes les informations de l'entreprise contre les cybercriminels. D'autres fonctionnalités sont incluses comme un pare-feu NAT pour bloquer le trafic non demandé, un tunnel partagé, une sécurité contre les fuites DNS et une authentification à 2 facteurs.

Nous allons utiliser le protocole d'**IPsec** qui est un ensemble de protocoles mis au point pour crypter et rendre les communications sécurisées et privées sur les réseaux IP.

Il sera installé sur le réseau des agences afin que celles-ci puissent rejoindre les serveurs de l'entreprise sans risque.