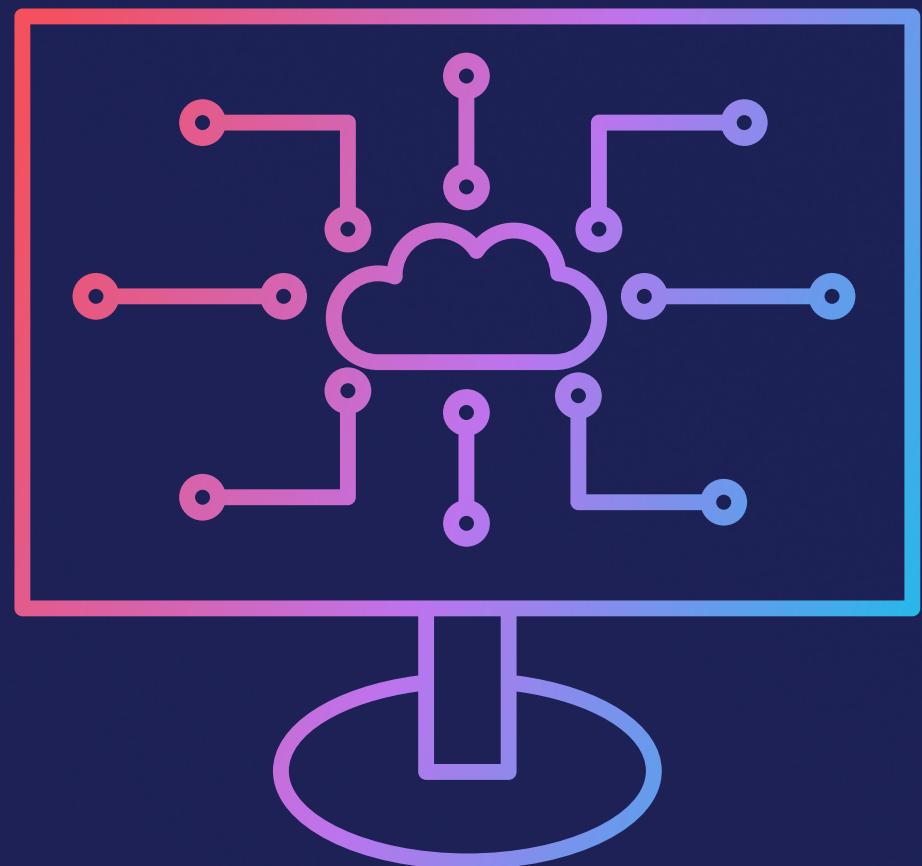




# LA SÉCURISATION D'UN RÉSEAU INFORMATIQUE AU SEIN D'UNE ENTREPRISE



# PRÉSENTATION DE LA TEAM :



**Matthieu Delaroche**



**Yassine Abbas**



**Nathan Buonomo**



**Damian Baerts**



**Tiago Fazenda teles**

# SOMMAIRE

01

INTRODUCTION

02

LES MÉTHODES ORGANISATIONNELLES

03

LA SÉCURISATION D'UN POSTE EN  
ENTREPRISE

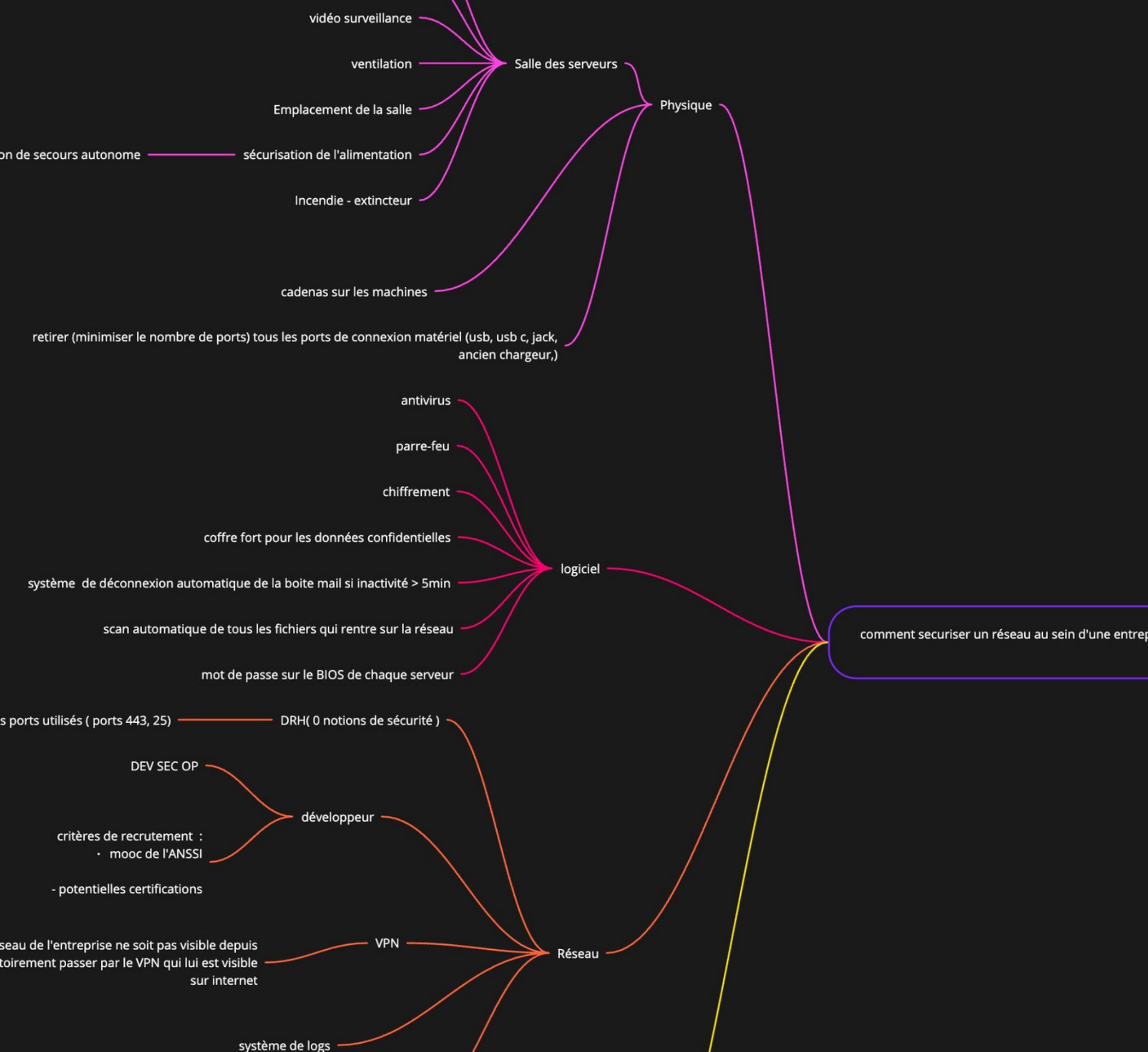
04

LA SÉCURISATION DU RÉSEAU

05

MATRICE DES FLUX

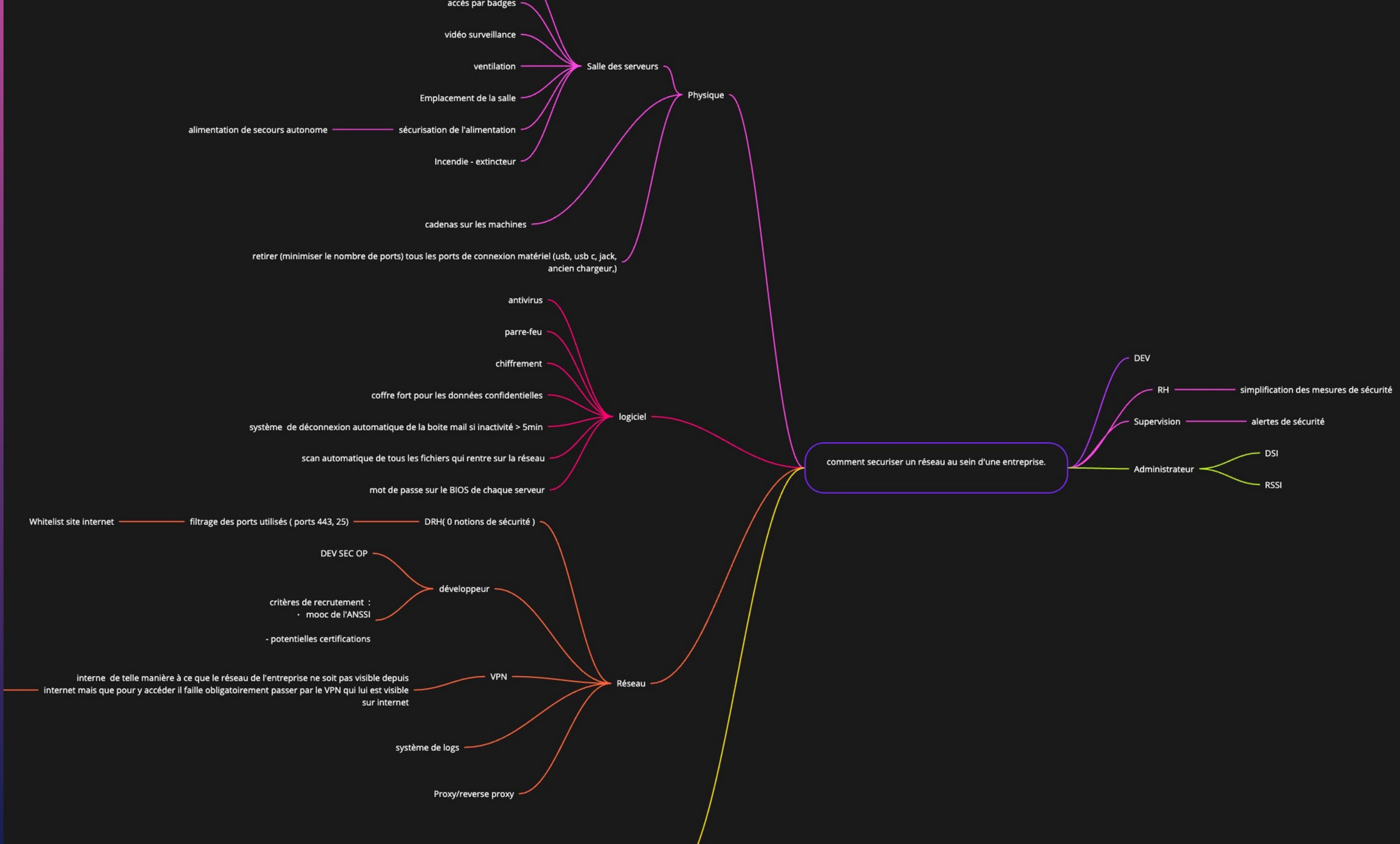
# INTRODUCTION



LE NOMBRE DE CYBER ATTAQUES AUGMENTENT ÉNORMÉMENT AU SEIN DES ENTREPRISES. TOUTES LES ENTREPRISES DOIVENT OBLIGATOIREMENT SÉCURISER LEURS RÉSEAUX. POUR CELA, IL EXISTE DE NOS JOURS ÉNORMÉMENT DE MANIÈRES DE SÉCURISER SON RÉSEAU PLUS OU MOINS EFFICACEMENT.

# MIND

# MAPP



# MÉTHODES ORGANISATIONNELLES

- CAMPAGNE DE SENSIBILISATION À TOUT LE PERSONNEL  
(SENSIBILISATION ACTIVE ET PASSIVE)
- OBLIGATION DE PASSER LE MOOC DE L'ANSSI POUR LES  
DÉVELOPPEURS .
- INTERDICTION D'APPORT D'HARDWARE EXTERNE À  
L'ENTREPRISE
- ÉVALUATIONS DE CONFORMITÉ
- TESTS DE VULNÉRABILITÉ



# LA SÉCURISATION DU POST

## Sécurité via Logiciel

- L'ANTIVIRUS -> BITDEFENDER
- LE COFFRE FORT
- PROTOCOLE DE FERMETURE AUTOMATIQUE DE LA SESSION
- MOT DE PASSE SUR LES BIOS
- GESTIONNAIRE DE MOT DE PASSE
- MISE EN PLACE D'UN LOGICIEL WHITE LIST



# LA SÉCURISATION DU POST

## Sécurité Physique

---

- PROTÉGER LES ORDINATEURS PHYSIQUEMENT
- PORT USB/USB-C



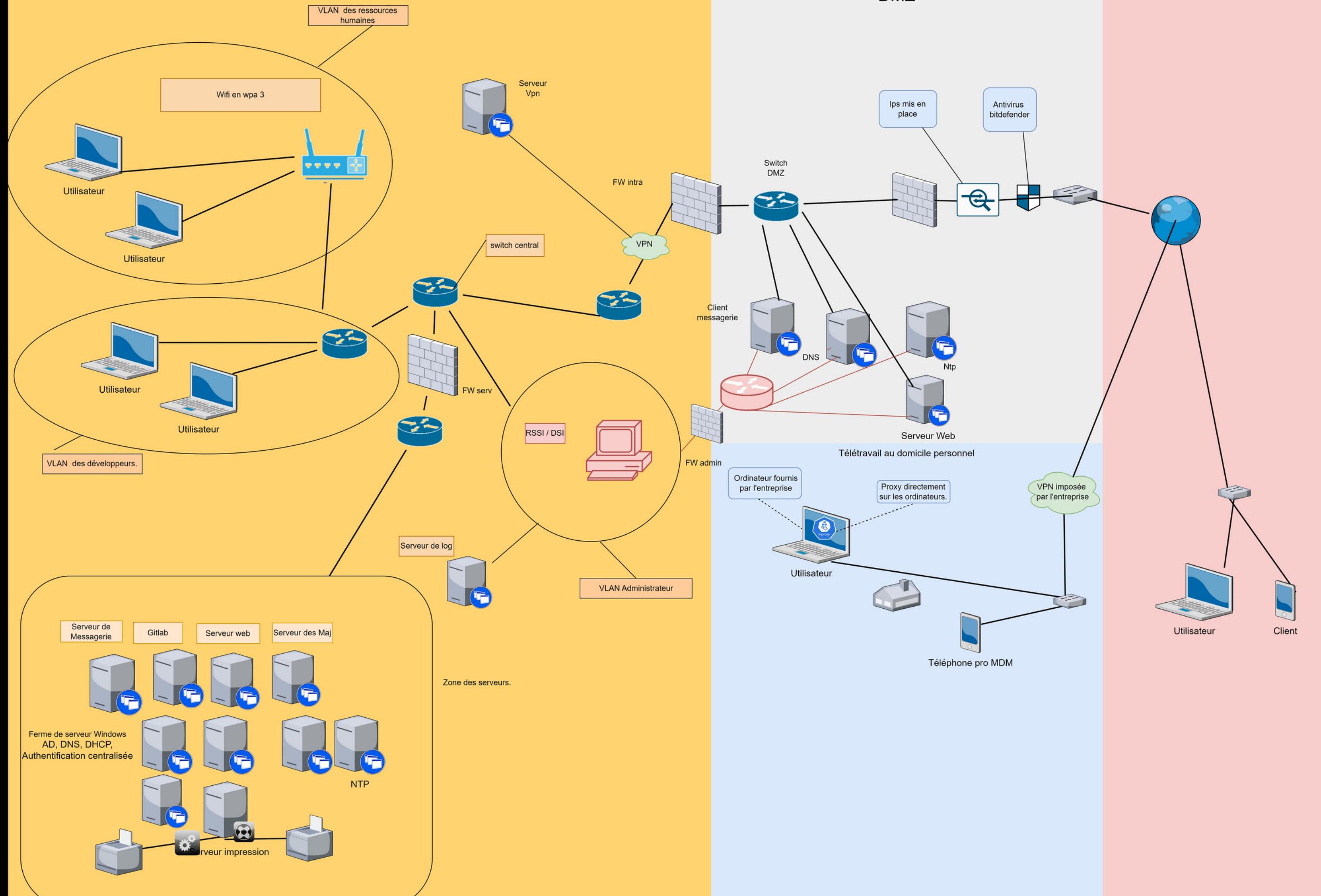
# LA SÉCURISATION DU POST

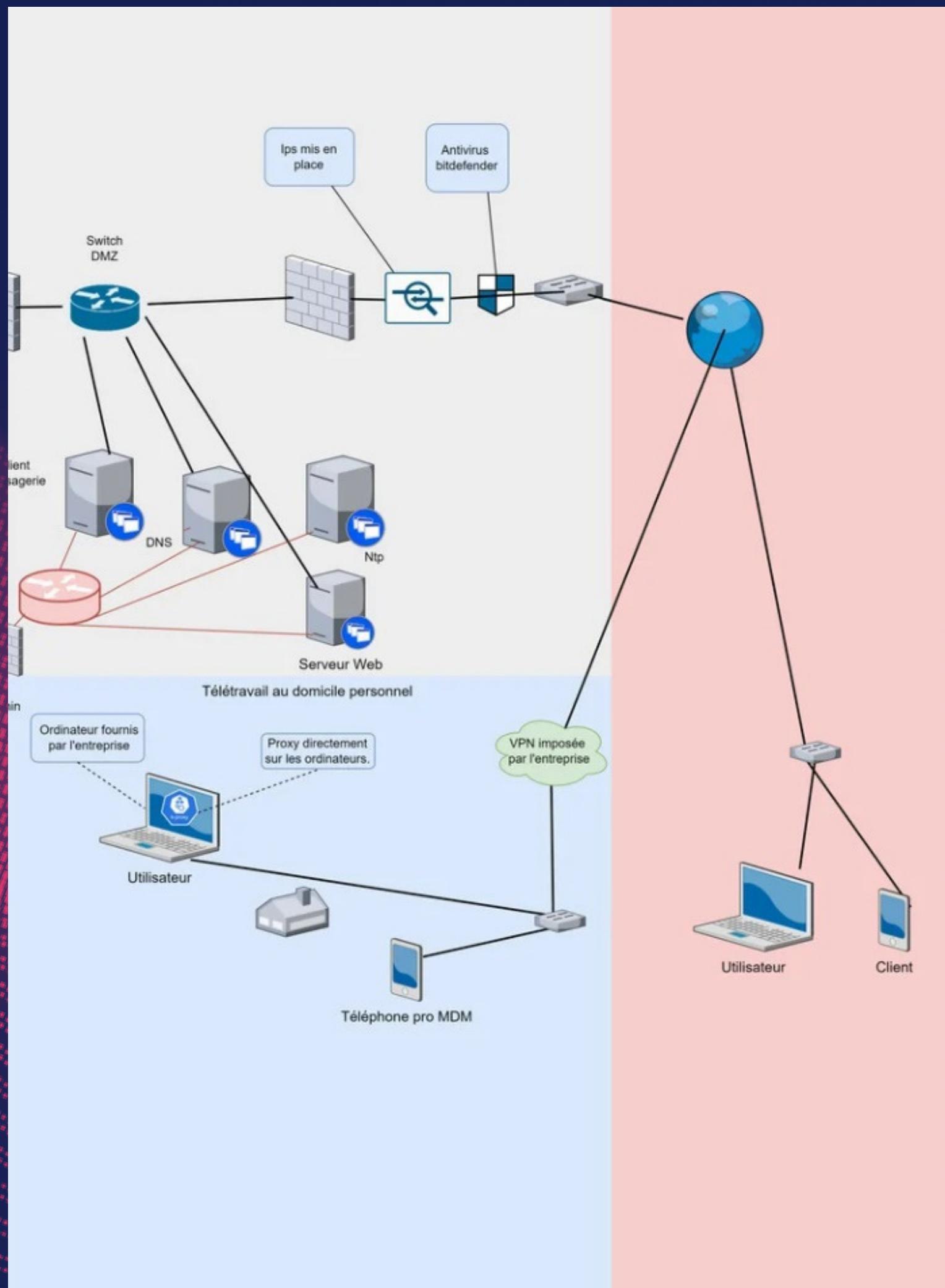
## Sécurité Réseaux

---

- MISE EN PLACE DE VPN
- MISE EN PLACE DE PROXY
- SÉCURISATION WIFI EN WPA 3







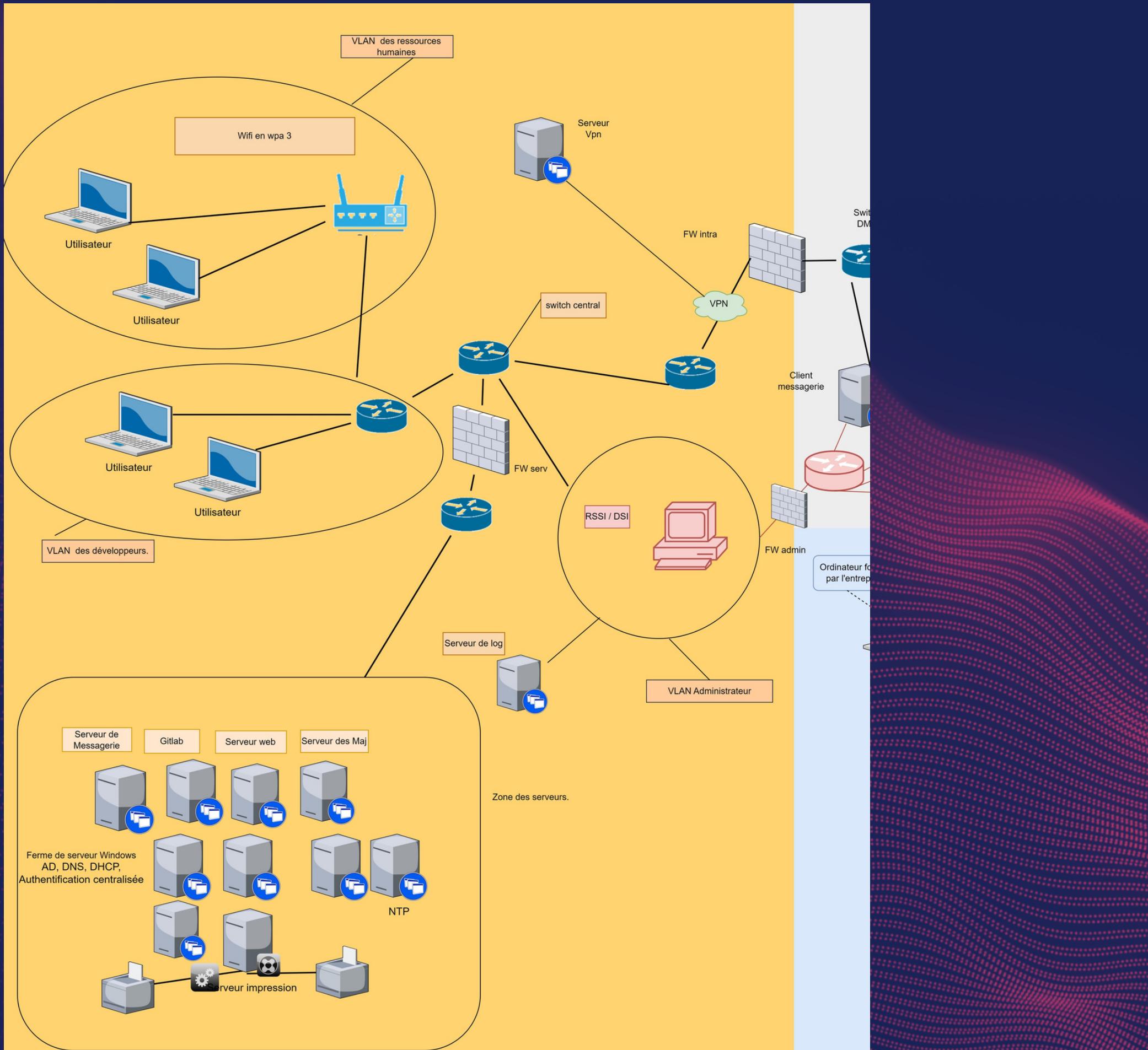
## KEY POINTS :

### DMZ :

- MISE EN PLACE D'UN ANTIVIRUS
- MISE EN PLACE D'UN IPS (SURVEILLANCE TRAFFIC)
- MISE EN PLACE D'UN SWITCH AU SEIN DE LA DMZ

### ZONE TÉLÉTRAVAIL :

- MISE EN PLACE OBLIGATOIRE DU VPN DE L'ENTREPRISE.
- TÉLÉPHONE PRO GÉRÉE PAR UN LOGICEL MDM.
- OBLIGATION D'UTILISER UN ORDINATEUR FOURNI PAR L'ENTREPRISE CONFIGURÉ AVEC UN PROXY.



## KEY POINTS :

### ZONE INTRANET

- MISE EN PLACE DU VPN A L'ENTRÉE DU RÉSEAU
- MISE EN PLACE DE 3 VLAN POUR CHAQUE GROUPE D'INDIVIDUS
- MISE EN PLACE D'UN FIRE WALL POUR LES RÈGLES DE COMMUNICATIONS DES SERVEURS
- REGROUPEMENT DES SERVEURS DANS UNE ZONE DÉDIÉE
- MISE EN PLACE D'UN SECOND FIREWALL ENTRE LA DMZ ET LE VLAN ADMIN

## MATRICE DES FLUX SERVEUR

ID	Type de flux	Machine Source	Machine Destination	Port	Protocole	Allow/Deny	Libellé
1	Envole Mails	Vlan RH/dev	Serveur de Messagerie	25	SMTP	Allow	Permet aux employés sur le réseau d'envoyer des mails via le service de messagerie de l'entreprise
2	Reception mails	Serveur de Messagerie	Vlan RH/dev	995	POP	Allow	Permet aux employés sur le réseau de recevoir des mails via le service de messagerie de l'entreprise
3	Envole mails	Vlan Admin	Serveur de Messagerie	25	SMTP	Allow	Permet aux admins sur le réseau d'envoyer des mails via le service de messagerie de l'entreprise
4	Reception mails	Serveur de Messagerie	Vlan Admin	995	POP	Allow	Permet aux employés sur le réseau de recevoir des mails via le service de messagerie de l'entreprise
5	Gestion de projet	ALL	Gitlab	80/443	HTTP/ HTTPS	Allow	Permet aux employés d'accéder à la plateforme Gitlab pour faire de la gestion de projets. ( Ce service est relié à tous les autres pour permettre aux employés de pourvoir intégrer avec des services externes tels que intégrer des mails, imprimer des documents,etc...)
6	espace de stockage	Vlan RH/Dev	Serveur Web	21	FTP	Allow	Permet aux machines du Vlan RH/Dev de déposer des fichiers sur le serveur Web
7	espace de stockage	Serveur Web	Vlan RH/Dev	20	FTP	Allow	Permet aux machines du Vlan RH/Dev de récupérer des fichiers sur le serveur Web
8	espace de stockage	Vlan Admin	Serveur Web	21	FTP	Allow	Permet aux machines du Vlan Admin de déposer des fichiers sur le serveur Web
9	espace de stockage	Serveur Web	Vlan Admin	20	FTP	Allow	Permet aux machines du Vlan Admin de récupérer des fichiers sur le serveur Web
10	mise à jour	Serveur de Maj	ALL	20	FTP	Allow	Permet au serveur de Maj d'envoyer les Maj aux différents services sur l'intranet ( services et machines )
11	mise à jour	Serveur de Maj	switch central	21	FTP	Allow	Permet au serveur des Maj de se connecter au switch central. Cette règle à pour finalité de relier le serveur de Maj à internet.
12	authentification	authentification centralisée	Vlan RH/Dev	445	TCP	allow	permet aux employés de s'authentifier sur le réseau de l'entreprise
13	authentification	authentification centralisée	Vlan Admin	445	TCP	allow	permet aux admins de s'authentifier sur le réseau de l'entreprise
14	Horloge	ALL	NTP	123	NTP	Allow	Cette règle permet à toutes les machines du réseau de se synchroniser sur une heure commune
15	imprimante	VLAN RH/Dev	serveur impression	21	ftp	allow	permet aux employés d'imprimer les fichier
16	imprimante	VLAN admin	serveur impression	21	ftp	allow	permet aux admins d'imprimer les fichier
17	Nom de domaine	DNS	switch central	53	DNS	Allow	Permet au DNS de se connecter au switch central. Cette règle à pour finalité de relier le serveur DNS de l'intranet à internet.
18	Horloge internet	NTP	switch central	123	NTP	Allow	Permet au NTP de se connecter au switch central. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
19	Interdiction globale	Routeur	ALL	-	-	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites

## MATRICE DES FLUX ADMIN / DMZ

ID	Type de flux	Machine Source	Machine Destination	Port	Protocole	Allow/Deny	Libellé
1	mails	Vlan admin	client de messagerie	25	SMTP	ALLOW	Permet aux admin d'accéder au client de messagerie depuis une machine du Vlan Admin. Cette règle est mise en place pour permettre aux admin de surveiller le serveur de messagerie externe
2	nom de domaines	Vlan admin	DNS	53	DNS	ALLOW	Permet aux admin d'accéder au service DNS ( domaine name system) depuis une machine du Vlan Admin. Cette règle est mise en place pour permettre aux admin de surveiller le serveur de messagerie externe
3	horloge	Vlan admin	NTP	123	NTP	ALLOW	Permet aux admin d'accéder au client NTP ( Network Time Protocol ) depuis une machine du Vlan Admin. Cette règle est mise en place pour permettre aux admin de surveiller le serveur de messagerie externe
4	accès au site web	Vlan admin	Serveur Web	80/443	HTTP/HTTPS	ALLOW	Permet aux admin d'accéder au serveur web depuis une machine du Vlan Admin. Cette règle est mise en place pour permettre aux admin de surveiller et d'intervenir sur le serveur de messagerie externe
5	Horloge internet	switch DMZ	routeur	123	NTP	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
6	Serveur de Maj	switch DMZ	Routeur	21	FTP	Allow	Permet au serveur de Maj de récupérer les Maj de tous les services et machines
7	Interdiction globale	Routeur	ALL	*	*	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites
8							

## MATRICE DES FLUX INTERNET

ID	Type de flux	Machine Source	Machine Destination	Port	Protocole	Allow/Deny	Libellé
1	mails	routeur	client de messagerie	25	SMTP	ALLOW	permet aux utilisateurs d'accéder au client de messagerie depuis l'extérieur. Ils n'auront pas accès à toutes les fonctionnalités, notamment...
2	nom de domaine DMZ	DNS	client de messagerie, NTP, Serveur web	53	DNS	ALLOW	Permettre au client DNS d'associer des noms de domaines à tous les autres services de la zone internet ( client messagerie, NTP et Serveur Web )
3	horloge DMZ	NTP	client de messagerie, DNS, Serveur web	123	NTP	ALLOW	Permet au service NTP de synchroniser tous les services de la zone internet ( Client messagerie, DNS et Serveur Web )
4	accès au site web	routeur	Serveur Web	80/443	HTTP/HTTPS	ALLOW	Permet à tout utilisateur d'accéder au serveur web depuis internet
5	Serveur de Maj	serveur de maj	routeur	21	FTP	Allow	Permet au serveur de Maj de récupérer les Maj de tous les services et machines
6	nom de domaine intranet	switch DMZ	routeur	53	DNS	Allow	Permet au switch DMZ de se connecter à internet pour interroger les sites internets pour obtenir leur nom de domaine
7	Horloge internet	switch DMZ	routeur	123	NTP	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
8	connexion internet Vlan RH/Dev	switch DMZ	routeur	80/443	HTTP/HTTPS	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le Vlan RH/Dev à internet.
9	connexion internet Admin	switch DMZ	routeur	80/443	HTTP/HTTPS	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le Vlan Admin à internet.
10	Serveur de Maj	switch DMZ	routeur	21	FTP	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le serveur de Maj à internet.
11	Interdiction globale	Routeur	ALL	*	*	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites

## MATRICE DES FLUX INTRANET

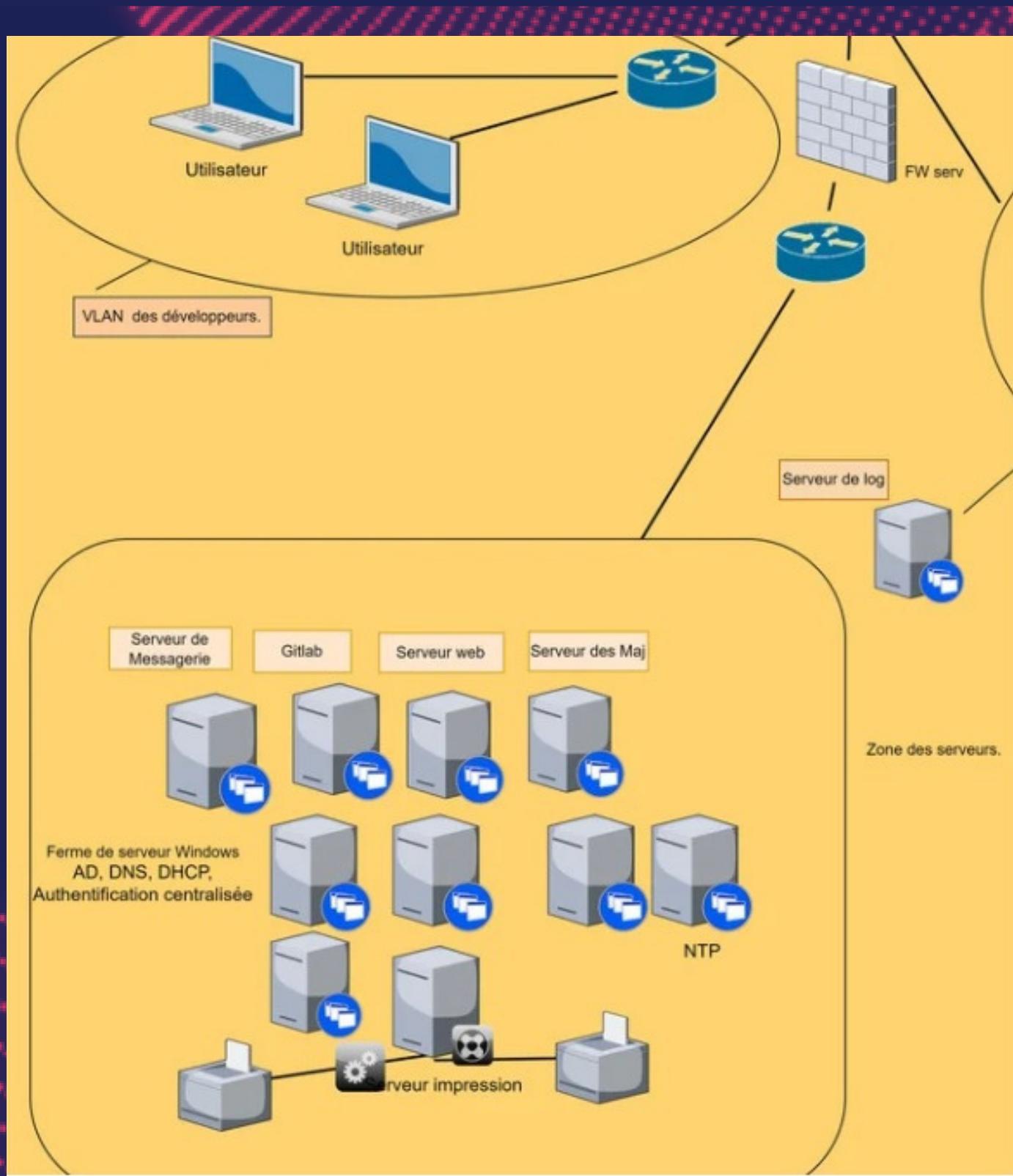
ID	Type de flux	Machine Source	Machine Destination	Port	Protocole	Allow/Deny	Libellé
1	Serveur de Maj	switch central	switch DMZ	21	FTP	Allow	Permet au switch central de se connecter au switch DMZ. Cette règle à pour finalité de relier le serveur de Maj à internet.
2	Horloge internet	switch central	switch DMZ	123	NTP	Allow	Permet au switch central de se connecter au switch DMZ. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
3	connexion internet Vlan RH/Dev	Vlan RH/Dev	switch DMZ	80/443	HTTP/HTTPS	Allow	Permet au Vlan RH/dev de se connecter au switch DMZ . Cette règle à pour finalité de relier le Vlan RH/Dev à internet.
4	connexion internet Admin	Vlan Admin	switch DMZ	80/443	HTTP/HTTPS	Allow	Permet au Vlan Admin de se connecter au switch DMZ . Cette règle à pour finalité de relier le Vlan RH/Dev à internet.
5	Nom de domaine	switch central	switch DMZ	53	DNS	Allow	Permet au switch central de se connecter au switch central 2. Cette règle à pour finalité de relier le serveur DNS de l'intranet à internet.
6	VPN	VPN	ALL	*	*	ALLOW	Applique un système de " remplaçage d'ip " sur toutes les requêtes venant des machines du réseau interne
7	Interdiction globale	Routeur	ALL	*	*	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites

# MATRICE DE FLUX : SERVEUR

5	Gestion de projet	ALL	Gitlab	80/443	HTTP/ HTTPS	Allow	Permet aux employés d'accéder à la plateforme Gitlab pour faire de la gestion de projets. ( Ce service est relié à tous les autres pour permettre aux employés de pourvoir intégrer avec des services externes tels que intégrer des mails, imprimer des documents,etc...)
---	-------------------	-----	--------	--------	----------------	-------	--

18	Horloge internet	NTP	switch central	123	NTP	Allow	Permet au NTP de se connecter au switch central. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
----	------------------	-----	----------------	-----	-----	-------	---

19	Interdiction globale	Routeur	ALL	*	*	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites
----	----------------------	---------	-----	---	---	------	--

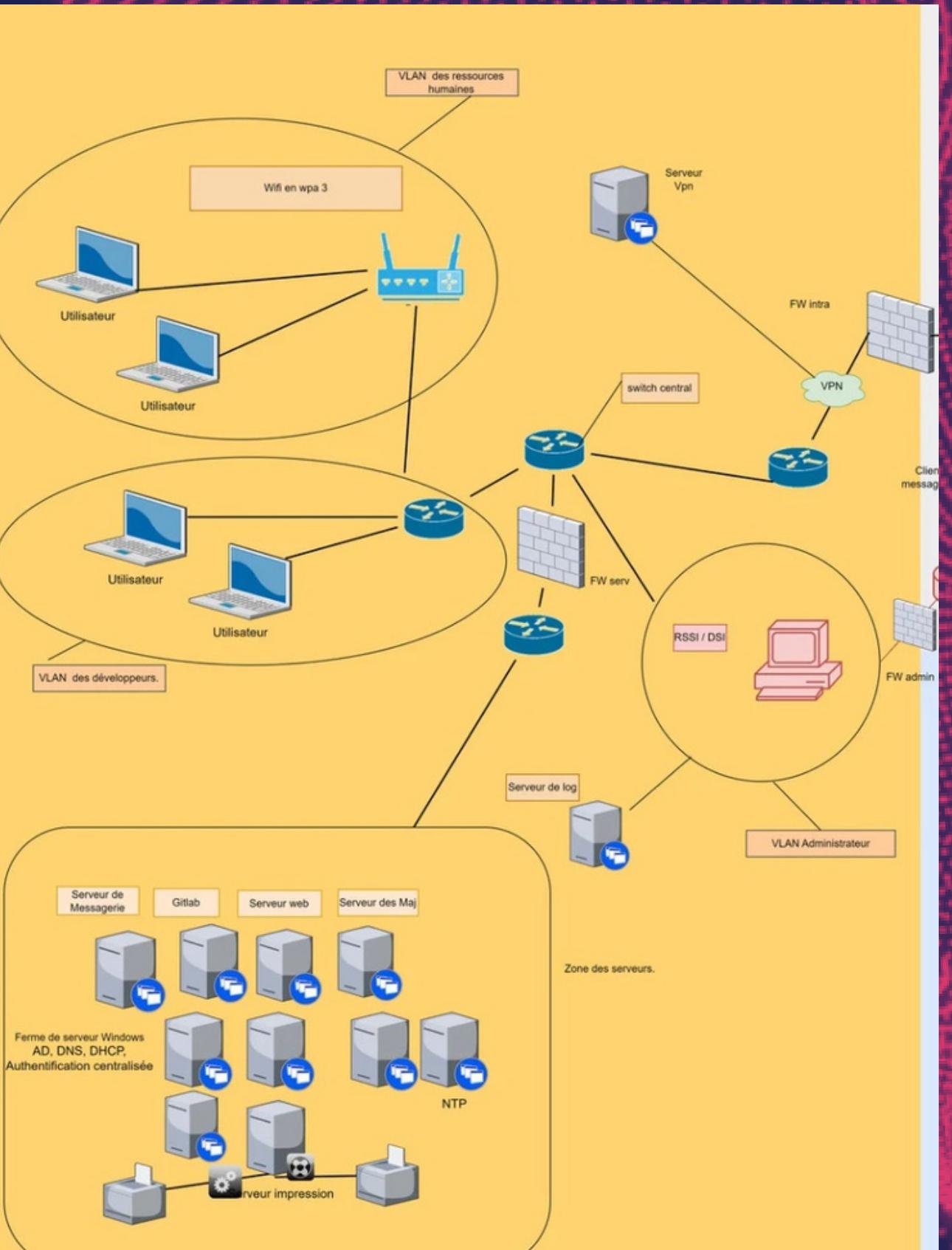


# MATRICE DE FLUX :

## INTRANET

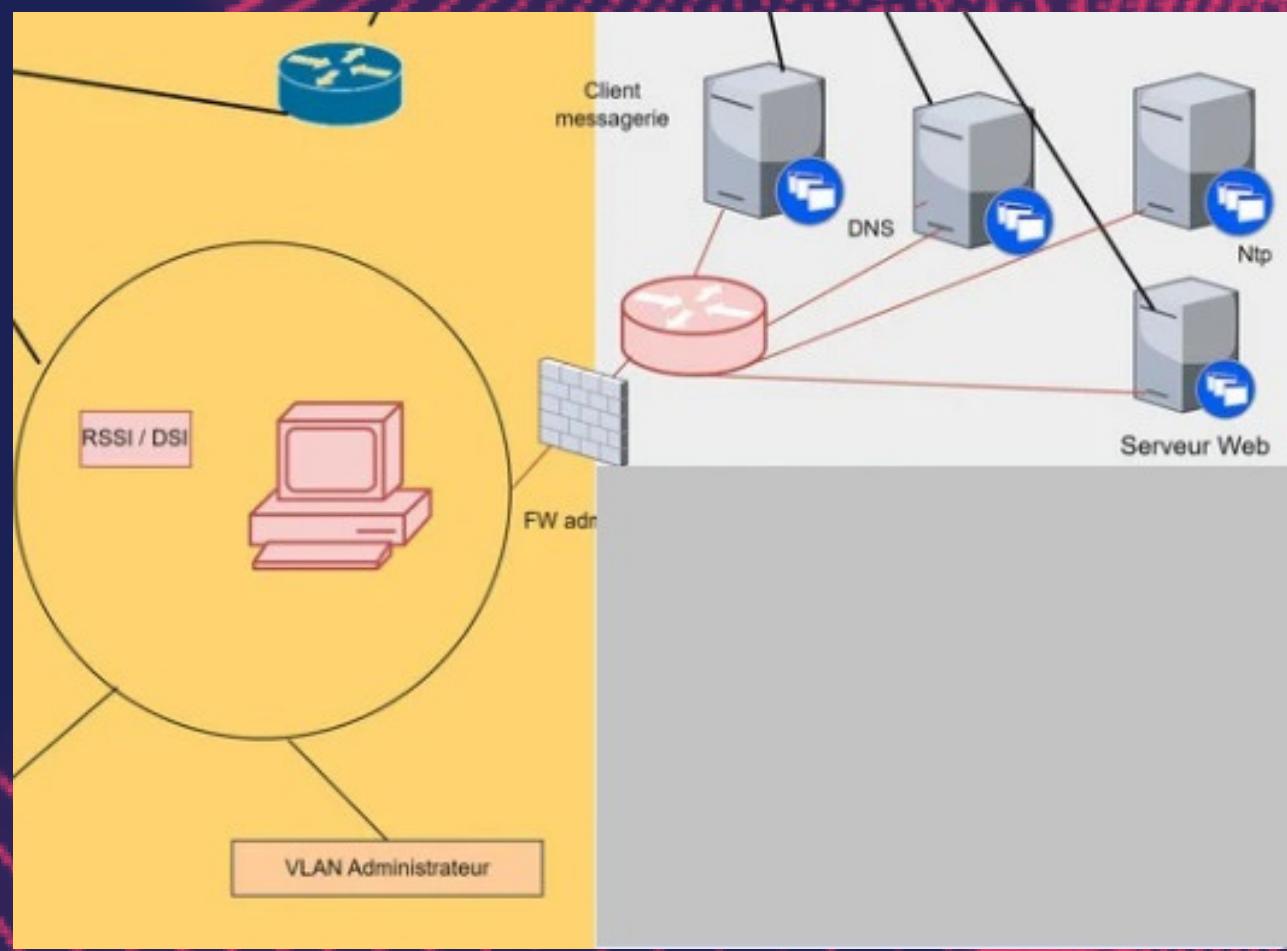
2	Horloge internet	switch central	switch DMZ	123	NTP	Allow	Permet au switch central de se connecter au switch DMZ. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
---	------------------	----------------	------------	-----	-----	-------	--

6	VPN	VPN	ALL	*	*	ALLOW	Applique un système de " remplacement d'ip " sur toutes les requêtes venant des machines du réseau interne
---	-----	-----	-----	---	---	-------	--



## MATRICE DE FLUX : ADMIN / DMZ

4	accès au site web	Vlan admin	Serveur Web	80/443	HTTP/HTTPS	ALLOW	Permet aux admin d'accéder au serveur web depuis une machine du Vlan Admin. Cette règle est mise en place pour permettre aux admin de surveiller et d'intervenir sur le serveur de messagerie externe
5	Horloge internet	switch DMZ	routeur	123	NTP	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
7	Interdiction globale	Routeur	ALL	*	*	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites

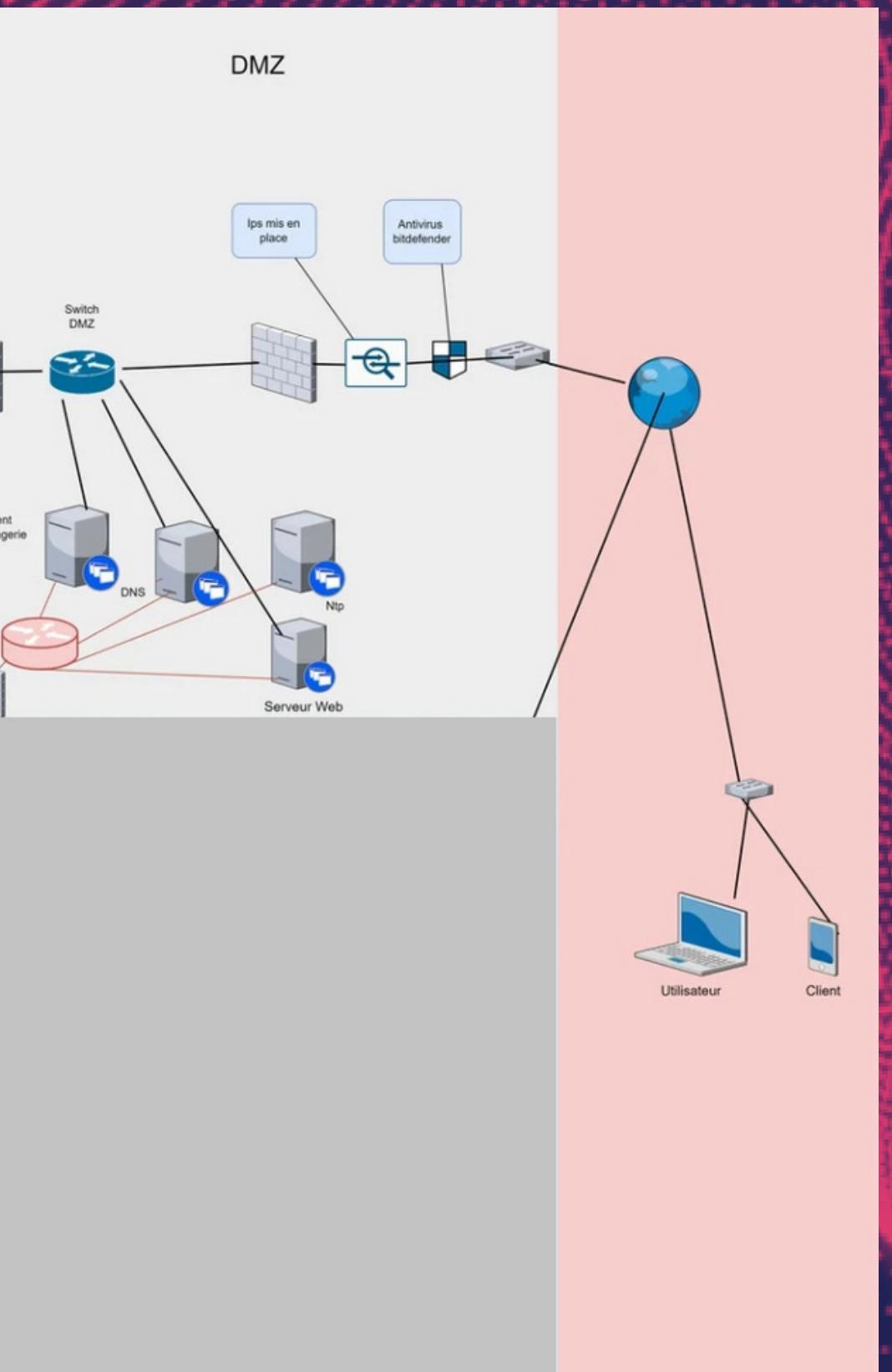


# MATRICE DE FLUX : INTERNET

3	horloge DMZ	NTP	client de messagerie, DNS, Serveur web	123	NTP	ALLOW	Permet au service NTP de synchroniser tous les services de la zone internet ( Client messagerie, DNS et Serveur Web)
---	----------------	-----	---	-----	-----	-------	--

7	Horloge internet	switch DMZ	routeur	123	NTP	Allow	Permet au switch DMZ de se connecter au routeur. Cette règle à pour finalité de relier le serveur NTP de l'intranet à internet.
---	---------------------	------------	---------	-----	-----	-------	--

11	Interdiction globale	Routeur	ALL	*	*	DENY	Toutes les accès/règles qui ne sont pas explicitement autorisées sont interdites
----	----------------------	---------	-----	---	---	------	--





## CONCLUSION

385 000 ATTAQUES EN 2022

AU PREMIER TRIMESTRE 2022, 9 ATTAQUES  
RANSOMWARES

PROTECTION DES POSTES (SOFTWARE ET HARDWARE)

UN ÊTRE IMPARFAIT NE PEUT CRÉER LA PERFECTION

MERCI DE NOUS AVOIR ÉCOUTÉS !

