BRETON Théo
BERLINGEN Gary
CAMPUS CARLO ACUTIS



Document de validation de compétences

AP2 – Infrasite

1. Présentation du contexte d'entreprise

L'entreprise de services du numérique SATO est le leader international de la transformation digitale avec environ 20 000 collaborateurs dans 15 pays et un chiffre d'affaires annuel de l'ordre de 2 milliards d'euros.

Grâce à ses technologies de pointe et son expertise digitale et sectorielle, SATO accompagne la transformation digitale de ses clients dans les secteurs de la défense, finance, santé, industrie, médias, énergie & utilités industrielles, secteur public, distribution, télécoms et transports. SATO vient de vous recruter pour prendre en charge ces nombreux projets.

L'entreprise cliente Maintenance Aero Services (MAS) est une société cliente de SATO, elle a été créée dans les années 1960. Son métier est de proposer toutes les opérations de maintenance aéronautique sur des avions commerciaux court et moyen-courrier. Ses clients sont principalement des compagnies aériennes trop petites pour disposer de leur propre service de maintenance. Les prestations de MAS couvrent une large palette : visites de maintenance régulières des appareils, évolutions techniques demandées par les constructeurs, reconditionnement d'appareils (par exemple en cas de changement de propriétaire), travaux de peinture de la carlingue et réparations de toutes sortes.

Après une reprise par des investisseurs à la suite d'une liquidation judiciaire en 2020, l'entreprise est à nouveau en pleine croissance et compte profiter de l'accroissement continu du trafic aérien pour augmenter son activité. Des embauches sont prévues tout au long de l'année.

MAS est organisée en différents services :

- service production qui prend en charge l'ensemble des opérations à mener sur les avions ;
- service commercial qui soumet des propositions commerciales aux clients ;
- service études qui soumet des propositions techniques aux clients
- service direction et RH qui regroupe la direction et les ressources humaines ;
- service formation qui se charge de tous les parcours de formation des salariés, notamment en fonction des exigences des certifications et des préconisations des constructeurs ;
- service informatique (IT) qui prend en charge la fourniture et le pilotage des services informatiques au sein de l'entreprise.
- Service comptabilitéwx

2. **Contraintes**

- Le protocole de routage utilisé est le protocole RIP V2
- Les différents services et serveurs côté LAN ainsi que la zone DMZ devront pouvoir accéder à
- Internet sachant qu'il est impossible d'accéder à la configuration du routeur principal de connexion Internet (routeur du LABO : 192.168.4.254)
- Le serveur web hébergé dans la DMZ devra être accessible depuis le LAN et l'extérieur
- Il vous faudra respecter le plan d'adressage et de nommage de l'entreprise.
- Assurer une sauvegarde automatique sur les jours ouvrés (du lundi au vendredi) de l'ensemble des configurations.
- Chaque membre du groupe devra disposer de ses propres serveurs virtualisés sur la maquette finale.
- Les différents services devront pouvoir accéder au serveur AD.
- Les services ne devront pas communiquer entre eux.
- Le pare-feu doit permettre l'entrée des connexions vers le serveur Web situé dans la DMZ depuis le LAN et Internet.
- Le pare-feu doit permettre aux utilisateurs situés dans la zone LAN d'accéder à Internet de façon sécurisée.
- Limiter au strict nécessaire l'accès aux éléments se trouvant dans la DMZ.
- Le service IT devra lui seul pouvoir depuis le LAN et l'extérieur administrer de manière sécurisée l'ensemble des éléments d'interconnexion qui devront bénéficier d'un contrôle d'accès et de messages d'avertissement.
- Seul le service IT aura accès au TFTP
- Des règles complémentaires peuvent être envisagées après accord.

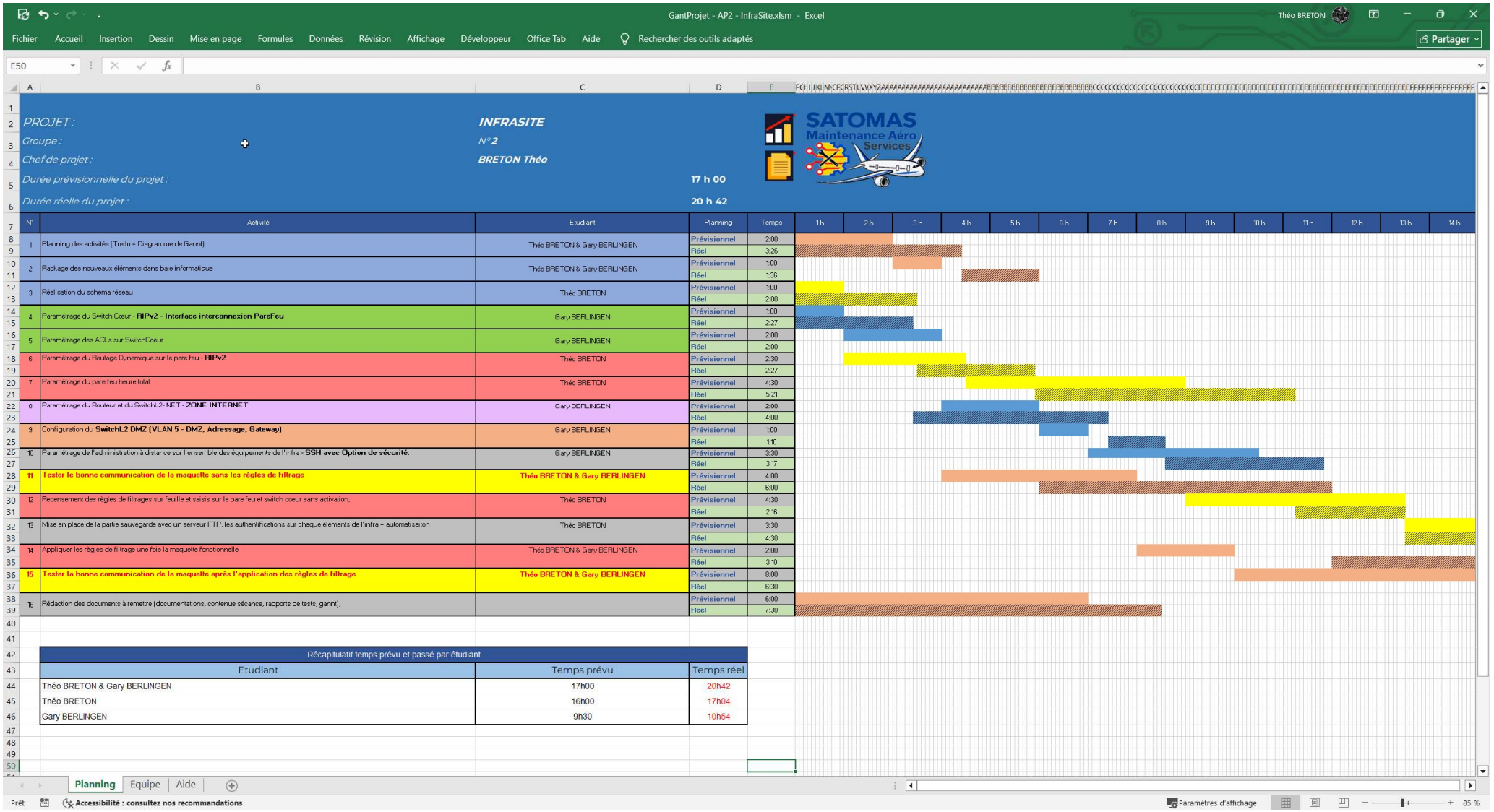
3. Réalisation du Travail

A.1 Planification du travail

Mission 1 : Répartition des tâches

Membre du binôme	Activités
☛ BRETON Théo (Chef de Projet) ☛ BERLINGEN Gary (Binôme)	A.1 Planification du projet
☛ BRETON Théo (Chef de Projet)	A.2 Réalisation du schéma réseau
☛ BRETON Théo (Chef de Projet) ☛ BERLINGEN Gary (Binôme)	A3. Rackage des équipements dans la baie informatique
☛ BERLINGEN Gary (Binôme)	A.4 Paramétrage du SwitchCoeur
☛ BRETON Théo (Chef de Projet)	A.5 Paramétrage du Pare-feu
☛ BERLINGEN Gary (Binôme)	A.6 Administration distante
☛ BRETON Théo (Chef de Projet)	A.7 Sauvegarde
☛ BERLINGEN Gary (Binôme)	A.8 - Switch L2 – DMZ
☛ BERLINGEN Gary (Binôme)	A.9 - Routeur ZONE INTERNET
☛ BRETON Théo (Chef de Projet)	A.10 Rédaction de la documentation
☛ BRETON Théo (Chef de Projet)	A.11 Diaporama chef de projet

Mission 2 : Réalisation du Gantt



GantProjet - AP2 - InfraSite.xlsm - Excel

Fichier Accueil Insertion Dessin Mise en page Formules Données Révision Affichage Développeur Office Tab Aide Rechercher des outils adaptés

PROJET :	INFRASITE
Groupe :	N° 2
Chef de projet :	BRETON Théo
Durée prévisionnelle du projet :	17 h 00
Durée réelle du projet :	20 h 42

SATOMAS Maintenance Aéro Services

N°	Activité	Etudiant	Planning	Temps
1	Planning des activités (Trello + Diagramme de Gannt)	Théo BRETON & Gary BERLINGEN	Prévisionnel	2:00
			Réel	3:26
2	Rackage des nouveaux éléments dans baie informatique	Théo BRETON & Gary BERLINGEN	Prévisionnel	1:00
			Réel	1:36
3	Réalisation du schéma réseau	Théo BRETON	Prévisionnel	1:00
			Réel	2:00
4	Paramétrage du Switch Cœur - **RIPv2 - Interface interconnexion PareFeu**	Gary BERLINGEN	Prévisionnel	1:00
			Réel	2:27
5	Paramétrage des ACLs sur SwitchCoeur	Gary BERLINGEN	Prévisionnel	2:00
			Réel	2:00
6	Paramétrage du Routage Dynamique sur le pare feu - **RIPv2**	Théo BRETON	Prévisionnel	2:30
			Réel	2:27
7	Paramétrage du pare feu heure total	Théo BRETON	Prévisionnel	4:30
			Réel	5:21
0	Paramétrage du Routeur et du SwitchL2- NET - **ZONE INTERNET**	Gary DERLINGEN	Prévisionnel	2:00
			Réel	4:00
9	Configuration du **SwitchL2 DMZ (VLAN 5 - DMZ, Adressage, Gateway)**	Gary BERLINGEN	Prévisionnel	1:00
			Réel	1:10
10	Paramétrage de l'administration à distance sur l'ensemble des équipements de l'infra - **SSH avec Option de sécurité.**	Gary BERLINGEN	Prévisionnel	3:30
			Réel	3:17
11	**Tester la bonne communication de la maquette sans les règles de filtrage**	**Théo BRETON & Gary BERLINGEN**	Prévisionnel	4:00
			Réel	6:00
12	Recensement des règles de filtrages sur feuille et saisis sur le pare feu et switch coeur sans activation.	Théo BRETON	Prévisionnel	4:30
			Réel	2:16
13	Mise en place de la partie sauvegarde avec un serveur FTP, les authentifications sur chaque éléments de l'infra + automatisaiton	Théo BRETON	Prévisionnel	3:30
			Réel	4:30
14	Appliquer les règles de filtrage une fois la maquette fonctionnelle	Théo BRETON & Gary BERLINGEN	Prévisionnel	2:00
			Réel	3:10
15	**Tester la bonne communication de la maquette après l'application des règles de filtrage**	**Théo BRETON & Gary BERLINGEN**	Prévisionnel	8:00
			Réel	6:30
16	Rédaction des documents à remettre (documentations, contenue sécance, rapports de tests, gannt),		Prévisionnel	6:00
			Réel	7:30

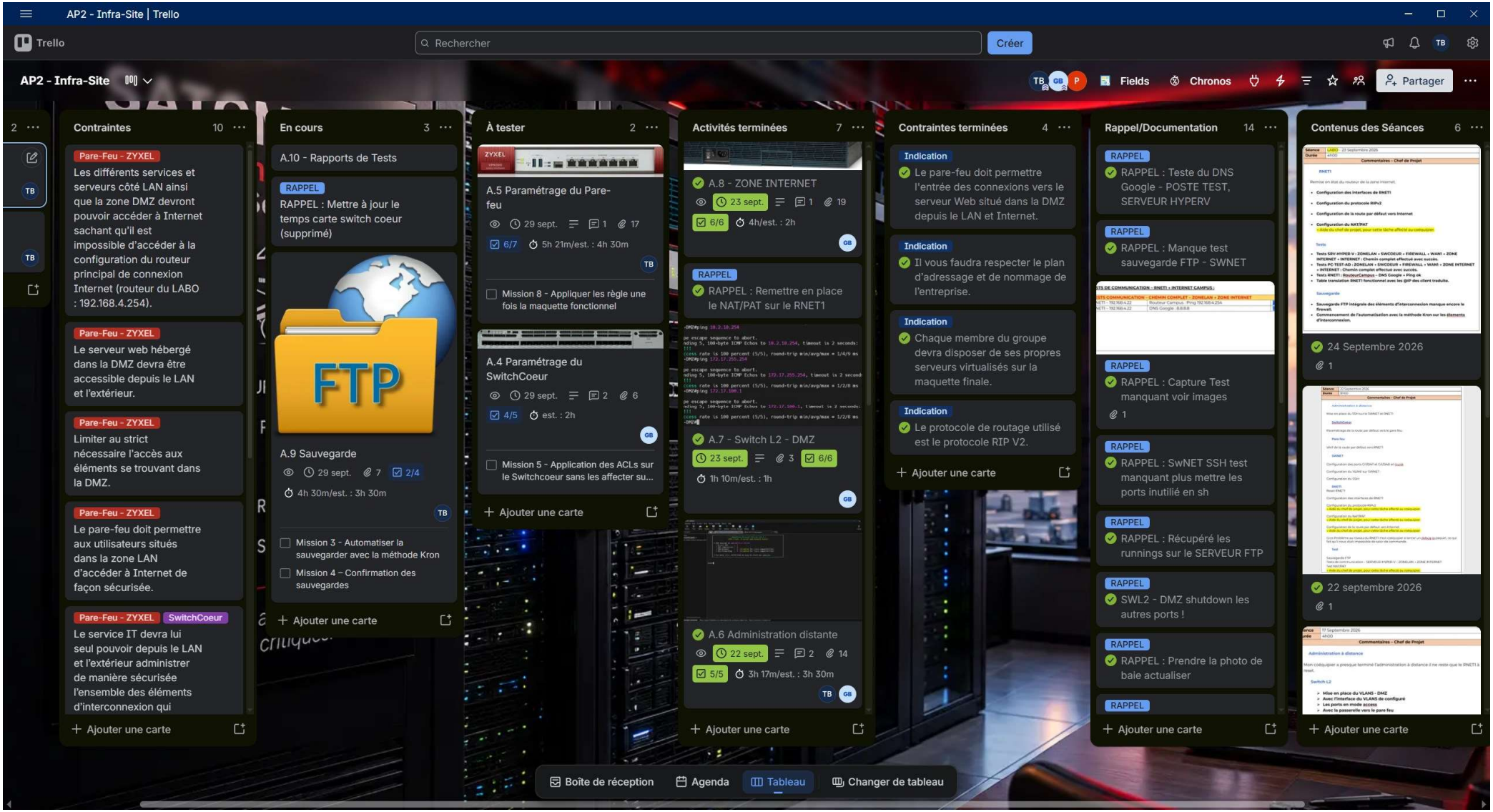
Récapitulatif temps prévu et passé par étudiant

Etudiant	Temps prévu	Temps réel
Théo BRETON & Gary BERLINGEN	17h00	20h42
Théo BRETON	16h00	17h04
Gary BERLINGEN	9h30	10h54

Planning Equipe Aide

Prêt Accessibilité : consultez nos recommandations Paramètres d'affichage 85 %

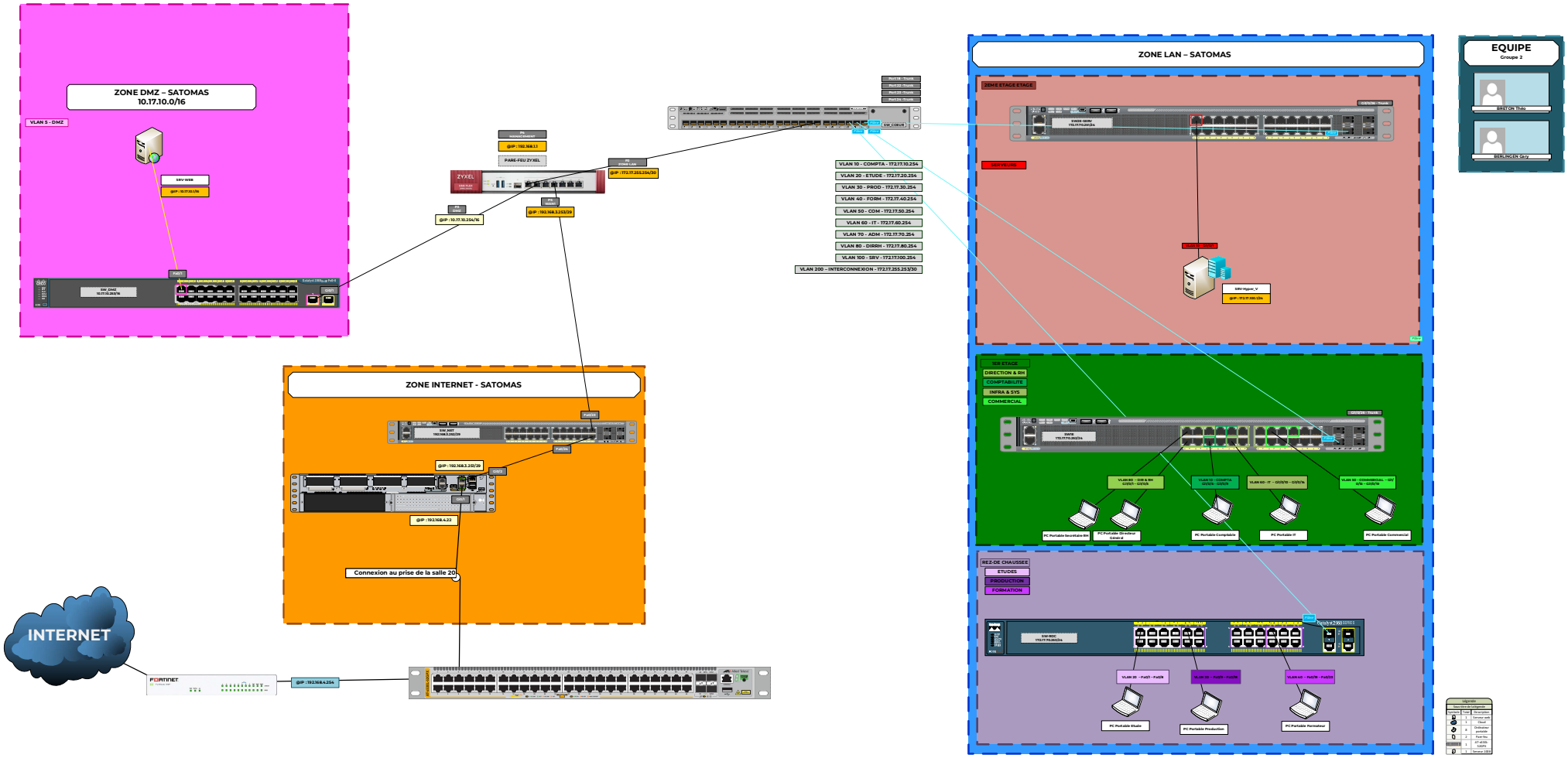
Mission 2 : Mis en œuvre du Trello

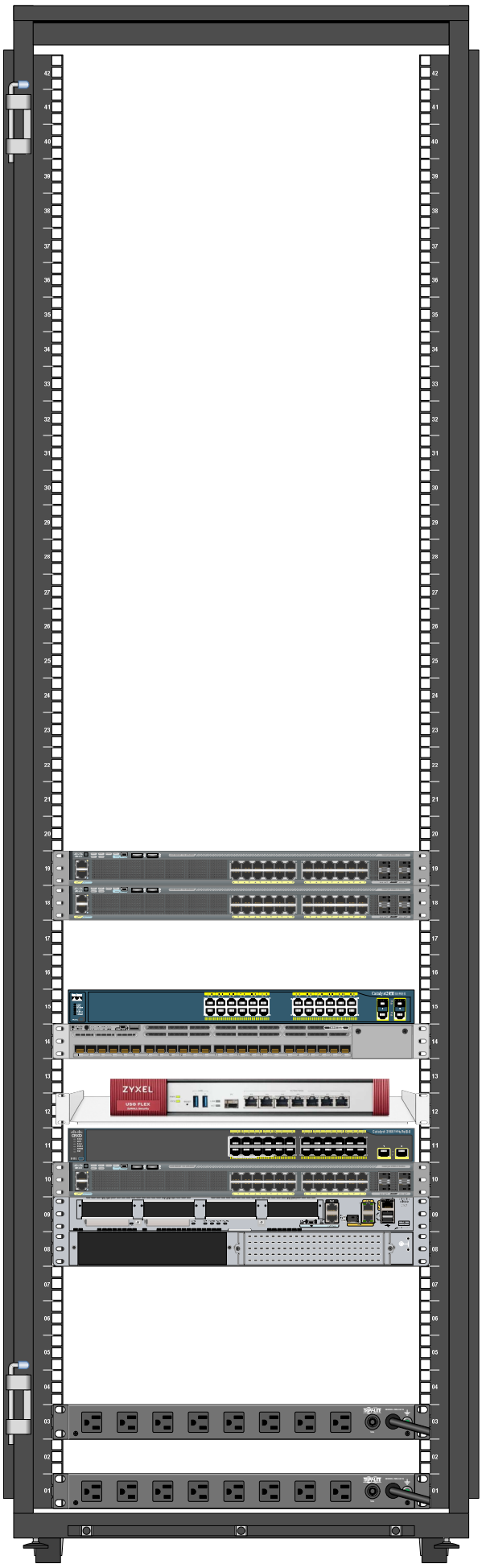


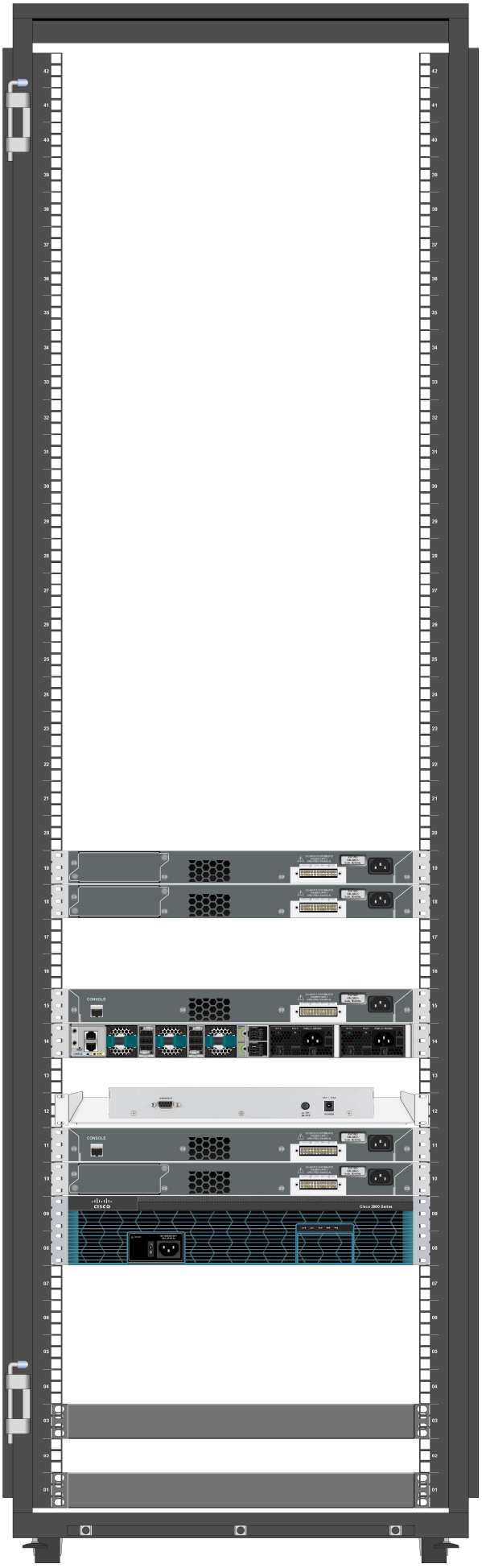
A.2 Réalisation du schéma réseau

Concevoir le schéma réseau logique initial de la maquette. L'outil de conception n'est pas imposé. Faire apparaitre sur le schéma l'ensemble des éléments physiques et logiques pour le groupe. Imprimer et conserver le document.

MAQUETTE SATOMAS

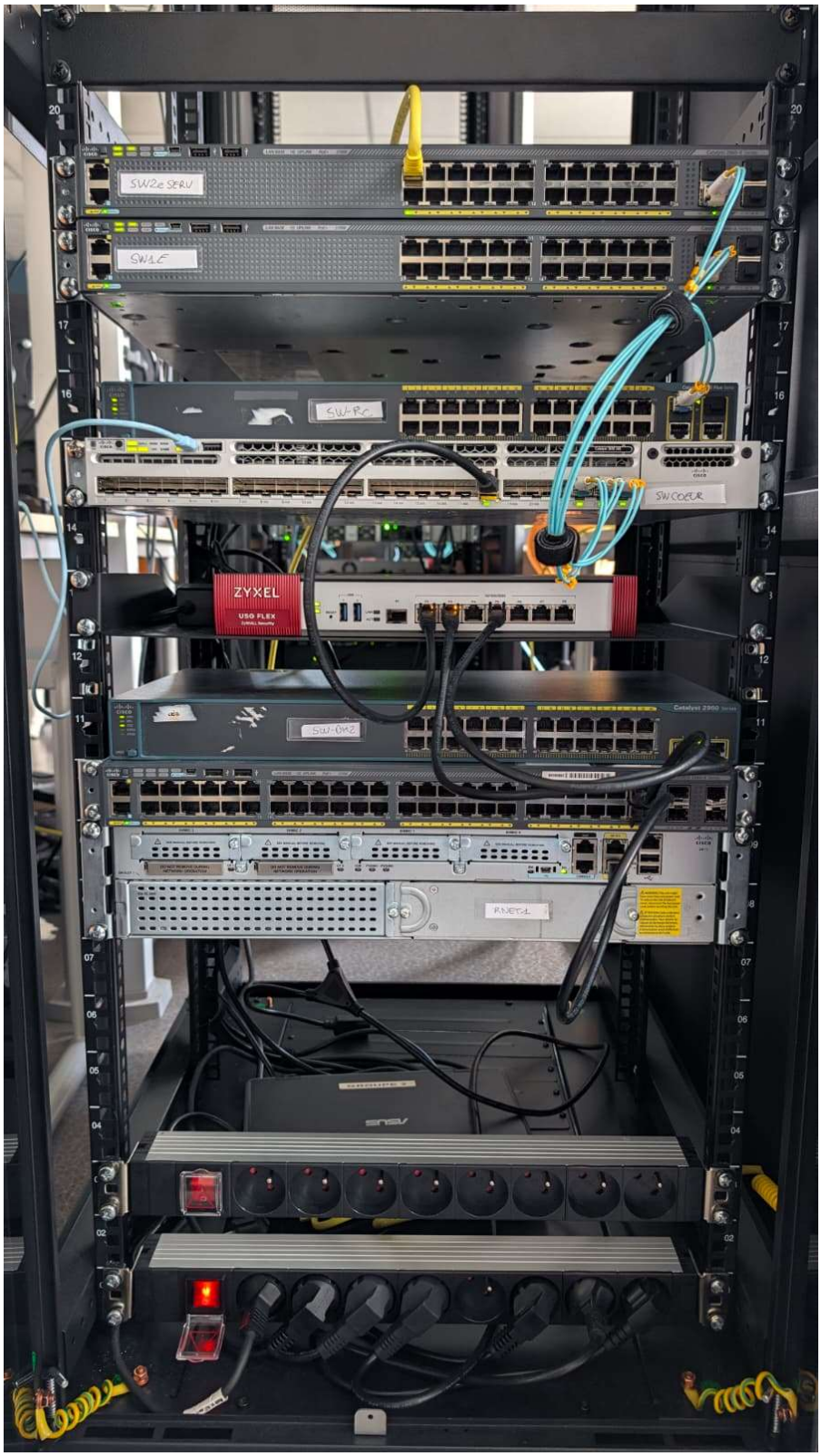



ZYXEL



A3. Rackage des équipements dans la baie informatique

- **RNET1**
- **Switch ZONE INTERNET**
- **Switch DMZ**
- **Pare feu Zyxel**



A.4 Paramétrage du SwitchCoeur

Mission 1 : Création du VLAN200

```
SwCoeur(config)# vlan 200

SwCoeur (config-vlan)# name INTERCONNEXION

SwCoeur (config-vlan)# exit

SwCoeur (config)# interface vlan 10

SwCoeur (config-if)#ip address 172.17.255.253 255.255.255.252
```

Mission 2 : Mettre le port connecté au Zyxel en mode acces vlan 200

```
SwCoeur(config)#int gi2/0/18
SwCoeur(config-if)#switchport access vlan 200
```

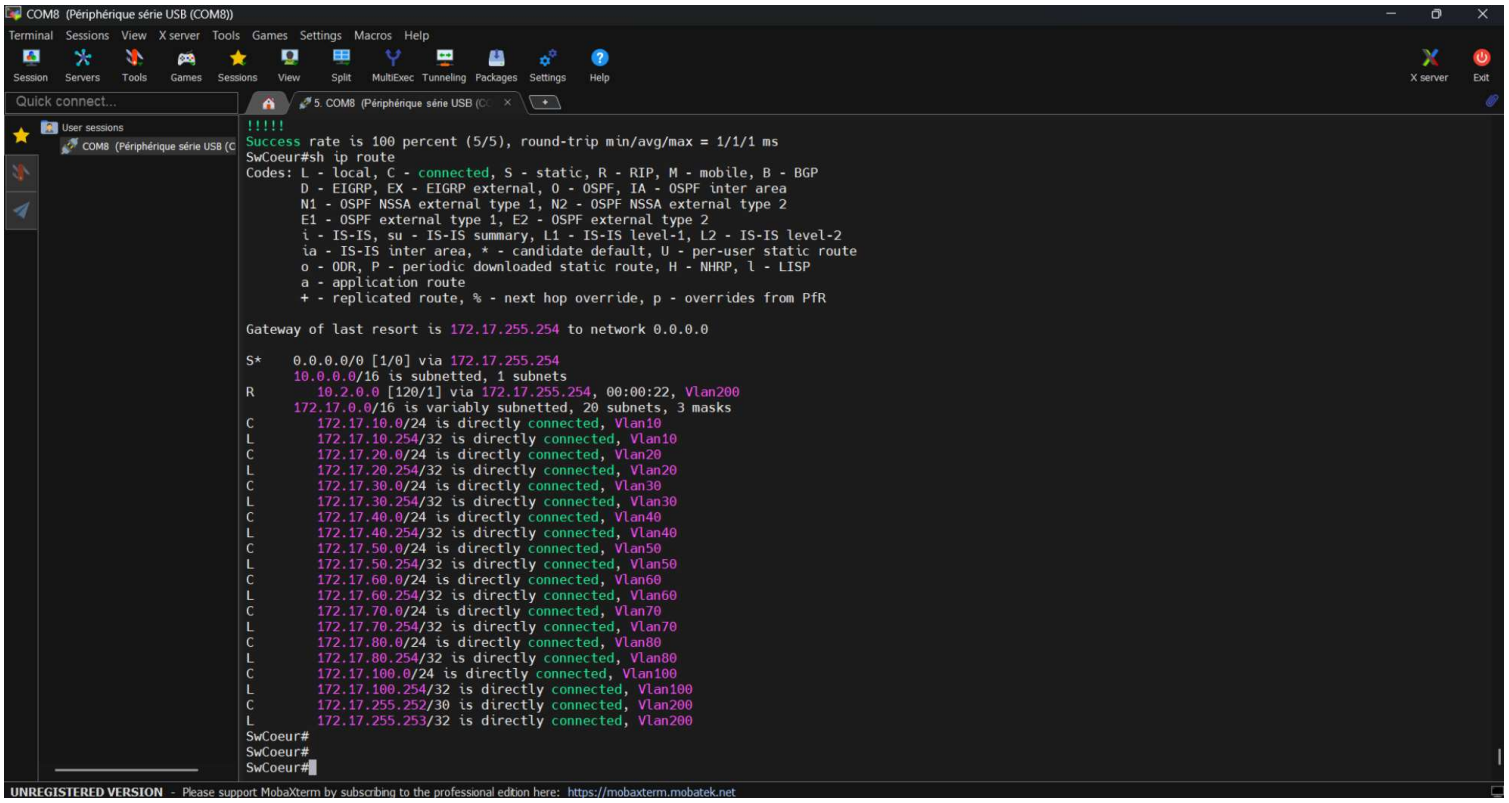
```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi2/0/1, Gi2/0/2, Gi2/0/3
                                                Gi2/0/4, Gi2/0/5, Gi2/0/6
                                                Gi2/0/7, Gi2/0/8, Gi2/0/9
                                                Gi2/0/10, Gi2/0/11, Gi2/0/12
                                                Gi2/0/13, Gi2/0/14, Gi2/0/15
                                                Gi2/0/16, Gi2/0/17, Gi2/0/19
                                                Gi2/0/20, Gi2/0/21
10   Compta                           active
20   Etude                            active
30   Prod                             active
40   Form                             active
50   COM                              active
60   IT                               active
70   ADM                              active
80   DIRRH                            active
100  SRV                              active
200  INTERCONNEXION                   active    Gi2/0/18
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
 --More--
```

Mission 3 : Paramétrage Routage Dynamique

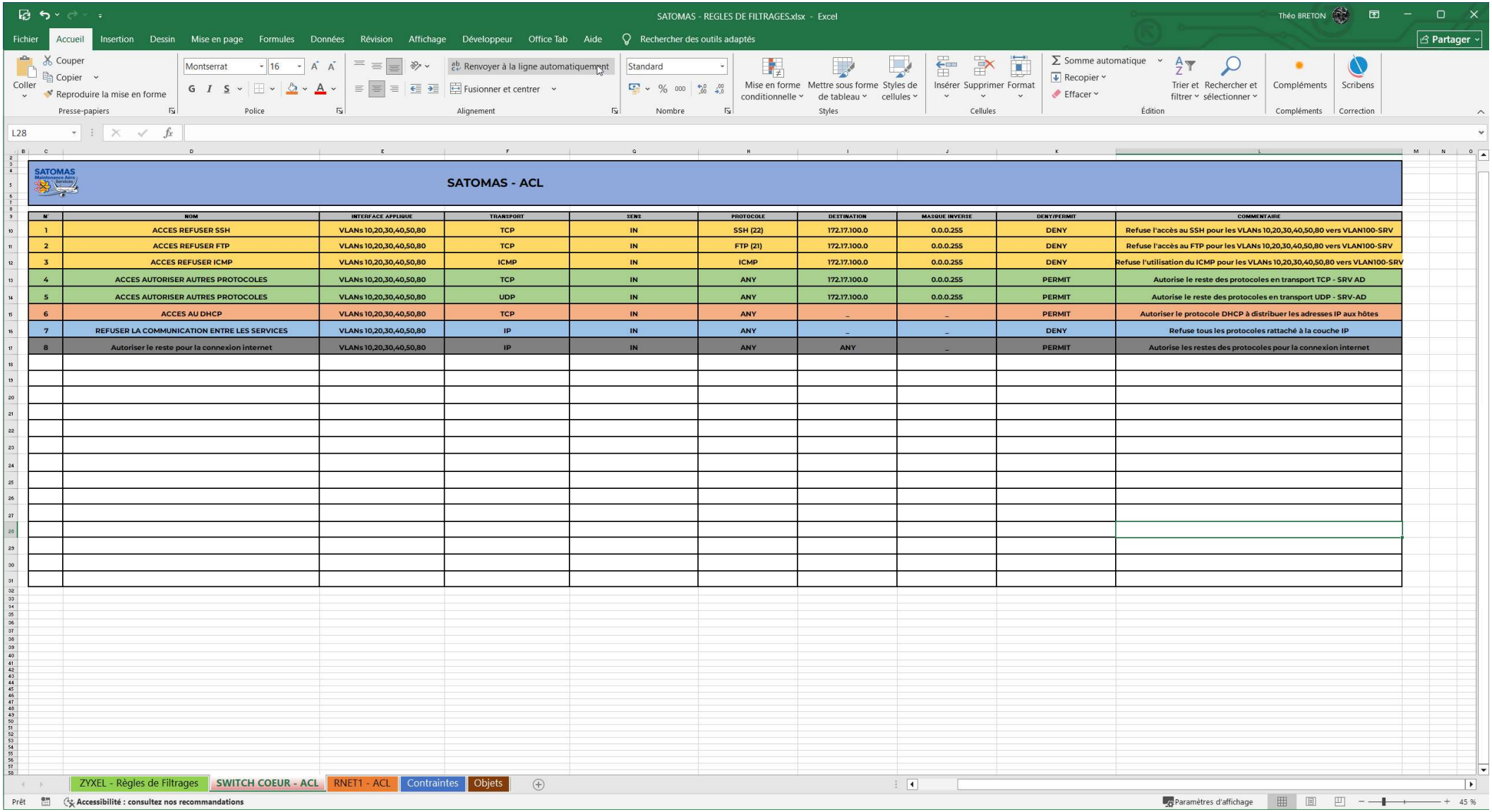
La version 2 du RIP se base sur la classless, elle ne prends pas en compte la classe de l'adresse.

```
SwCoeur(config)# router rip
SwCoeur(config-router)# version 2
SwCoeur(config-router)# network 172.17.0.0
```

Une fois le RIPv2 configuré sur le pare feu et le Switch Cœur on obtient bien les réseaux manquant :


COM8 (Périphérique série USB (COM8))
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
User sessions
COM8 (Périphérique série USB (C
5. COM8 (Périphérique série USB (C
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SwCoeur#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 172.17.255.254 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 172.17.255.254
10.0.0.0/16 is subnetted, 1 subnets
R 10.2.0.0 [120/1] via 172.17.255.254, 00:00:22, Vlan200
172.17.0.0/16 is variably subnetted, 20 subnets, 3 masks
C 172.17.10.0/24 is directly connected, Vlan10
L 172.17.10.254/32 is directly connected, Vlan10
C 172.17.20.0/24 is directly connected, Vlan20
L 172.17.20.254/32 is directly connected, Vlan20
C 172.17.30.0/24 is directly connected, Vlan30
L 172.17.30.254/32 is directly connected, Vlan30
C 172.17.40.0/24 is directly connected, Vlan40
L 172.17.40.254/32 is directly connected, Vlan40
C 172.17.50.0/24 is directly connected, Vlan50
L 172.17.50.254/32 is directly connected, Vlan50
C 172.17.60.0/24 is directly connected, Vlan60
L 172.17.60.254/32 is directly connected, Vlan60
C 172.17.70.0/24 is directly connected, Vlan70
L 172.17.70.254/32 is directly connected, Vlan70
C 172.17.80.0/24 is directly connected, Vlan80
L 172.17.80.254/32 is directly connected, Vlan80
C 172.17.100.0/24 is directly connected, Vlan100
L 172.17.100.254/32 is directly connected, Vlan100
C 172.17.255.252/30 is directly connected, Vlan200
L 172.17.255.253/32 is directly connected, Vlan200
SwCoeur#
SwCoeur#
SwCoeur#
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Mission 4 : Recenser les ACLs à appliquer sur le Switch Coeur



SATOMAS - REGLES DE FILTRAGES.xlsx - Excel

SATOMAS - ACL

N°	NOM	INTERFACE APPLIQUE	TRANSPORT	SENS	PROTOCOLE	DESTINATION	MASQUE INVERSE	DENY/PERMIT	COMMENTAIRE
1	ACCES REFUSER SSH	VLANs 10,20,30,40,50,80	TCP	IN	SSH (22)	172.17.100.0	0.0.0.255	DENY	Refuse l'accès au SSH pour les VLANs 10,20,30,40,50,80 vers VLAN100-SRV
2	ACCES REFUSER FTP	VLANs 10,20,30,40,50,80	TCP	IN	FTP (21)	172.17.100.0	0.0.0.255	DENY	Refuse l'accès au FTP pour les VLANs 10,20,30,40,50,80 vers VLAN100-SRV
3	ACCES REFUSER ICMP	VLANs 10,20,30,40,50,80	ICMP	IN	ICMP	172.17.100.0	0.0.0.255	DENY	Refuse l'utilisation du ICMP pour les VLANs 10,20,30,40,50,80 vers VLAN100-SRV
4	ACCES AUTORISER AUTRES PROTOCOLES	VLANs 10,20,30,40,50,80	TCP	IN	ANY	172.17.100.0	0.0.0.255	PERMIT	Autorise le reste des protocoles en transport TCP - SRV AD
5	ACCES AUTORISER AUTRES PROTOCOLES	VLANs 10,20,30,40,50,80	UDP	IN	ANY	172.17.100.0	0.0.0.255	PERMIT	Autorise le reste des protocoles en transport UDP - SRV-AD
6	ACCES AU DHCP	VLANs 10,20,30,40,50,80	TCP	IN	ANY	_	_	PERMIT	Autoriser le protocole DHCP à distribuer les adresses IP aux hôtes
7	REFUSER LA COMMUNICATION ENTRE LES SERVICES	VLANs 10,20,30,40,50,80	IP	IN	ANY	_	_	DENY	Refuse tous les protocoles rattaché à la couche IP
8	Autoriser le reste pour la connexion internet	VLANs 10,20,30,40,50,80	IP	IN	ANY	ANY	_	PERMIT	Autorise les restes des protocoles pour la connexion internet

Mission 6 : Application des ACLs une fois la maquette fonctionnel

```
ip access-list extended ACCES
```

Refuser aux services le SSH, le FTP et le ping vers le VLAN 100 - SRV réservés au VLAN 60 - IT

```
deny tcp any 172.17.100.0 0.0.0.255 eq 22 [SSH]
deny tcp any 172.17.100.0 0.0.0.255 eq 21 [FTP]
deny icmp any 172.17.100.0 0.0.0.255      [ICMP]
```

Autoriser les autres protocoles vers le VLAN 100 - SRV (accès au serveur AD)

```
permit tcp any 172.17.100.0 0.0.0.255
permit udp any 172.17.100.0 0.0.0.255
```

Laisser passer le DHCP

```
permit udp any eq bootpc any eq bootps
```

Refuser la communication entre les services

```
deny ip any 172.17.0.0 0.0.255.255
```

Autoriser le reste (Internet, DMZ), filtré ensuite par le pare-feu

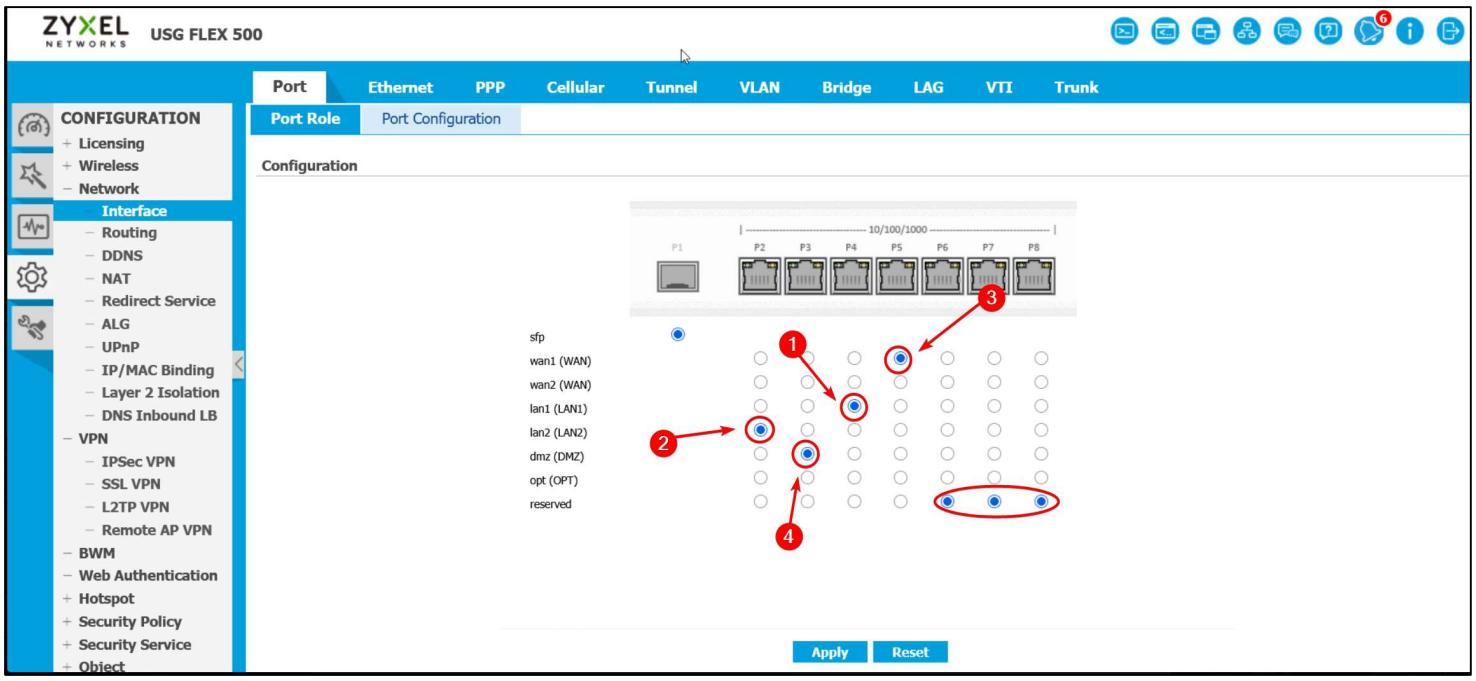
```
permit ip any any
```

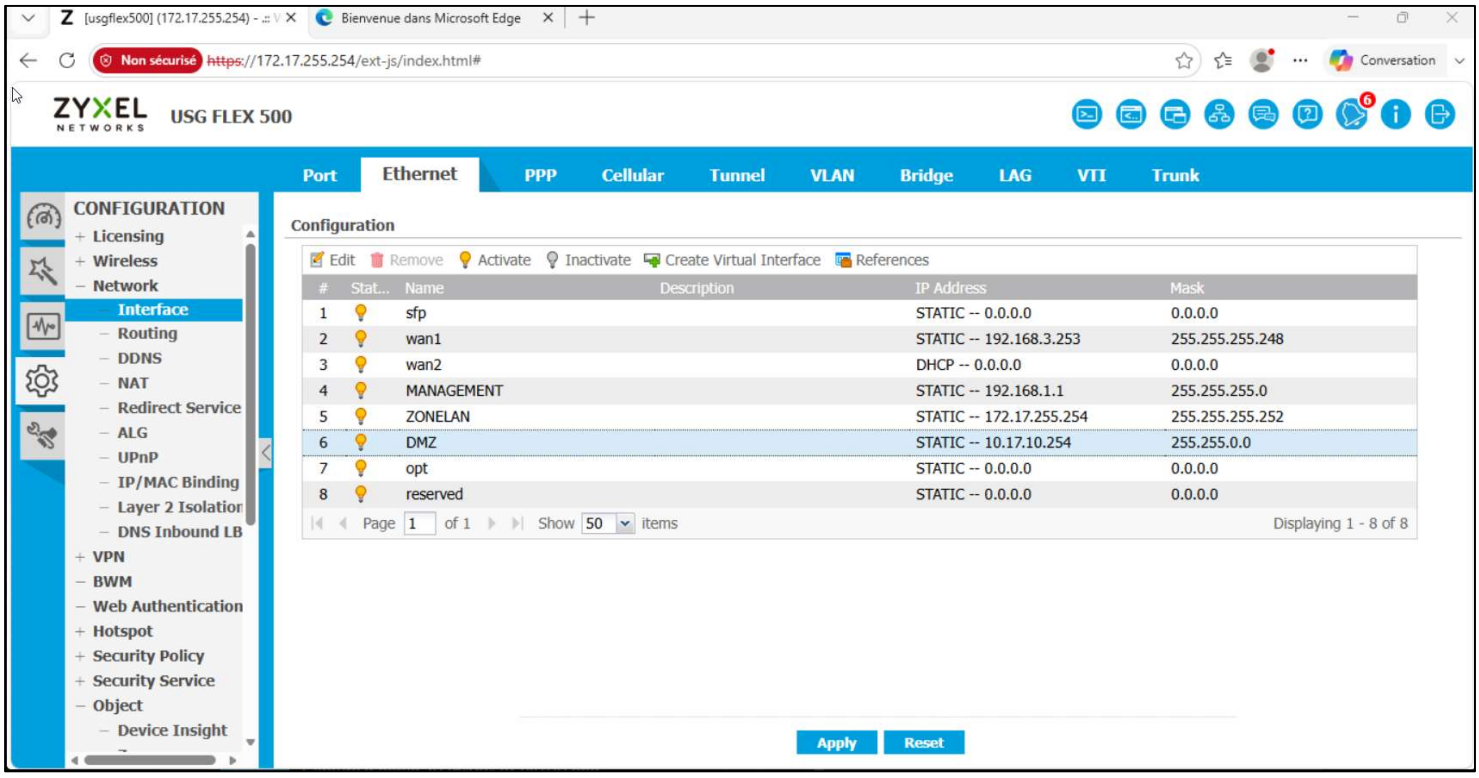
Affecter cette ACL sur les VLANS sauf les VLANS ci-dessous :

- VLAN 60 - IT
- VLAN 70 - ADM
- VLAN 100 - SERVEUR
- VLAN 200 - INTERCONNEXION

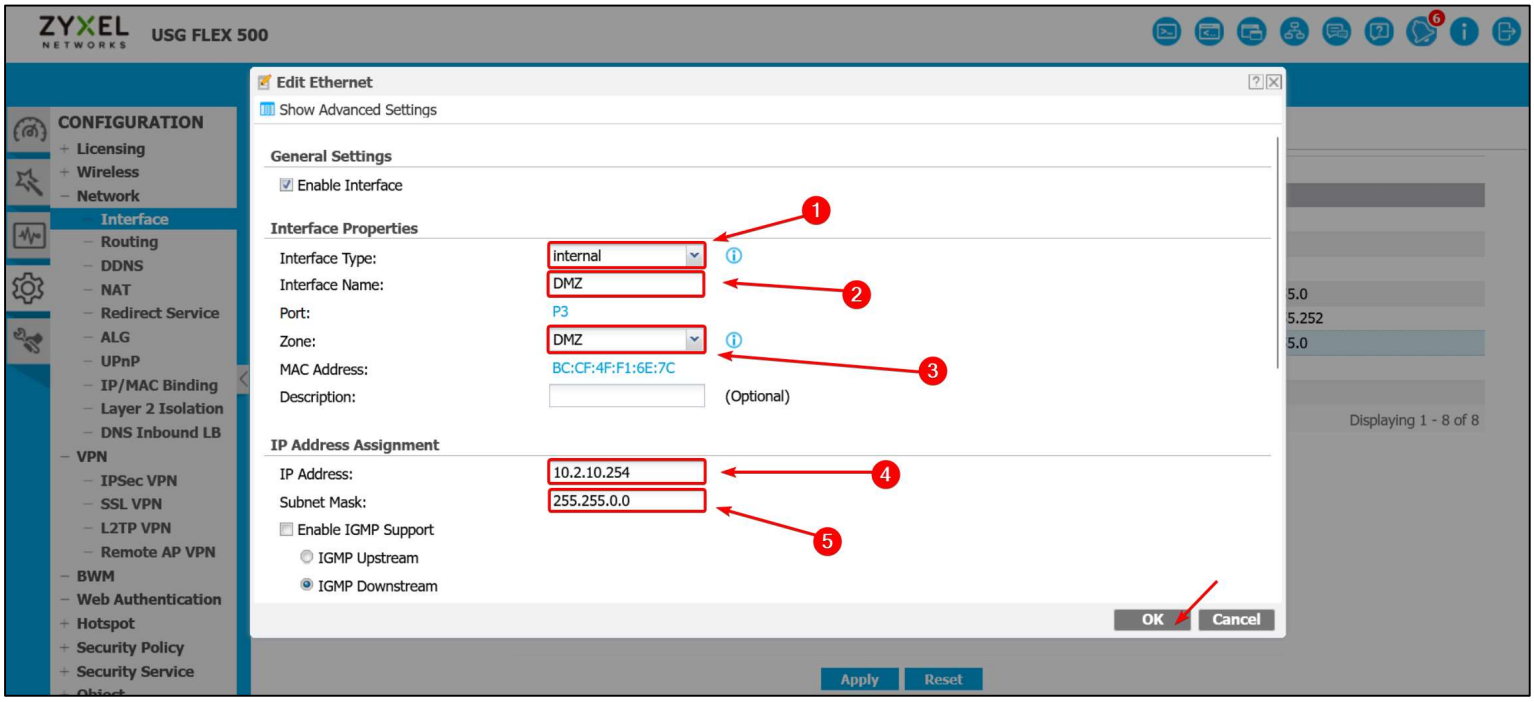
A.5 Paramétrage du Pare-feu

Mission 1 : Configuration des interfaces du pare-feu :

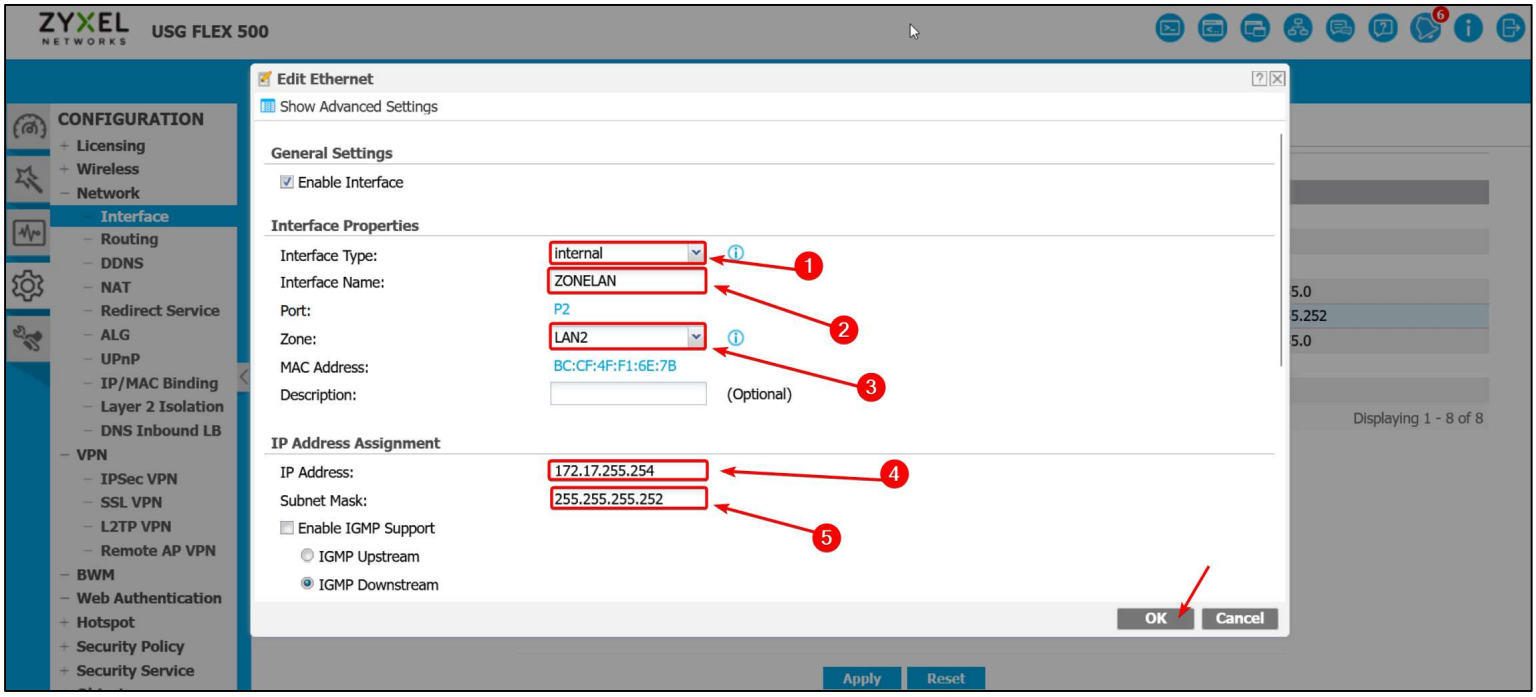




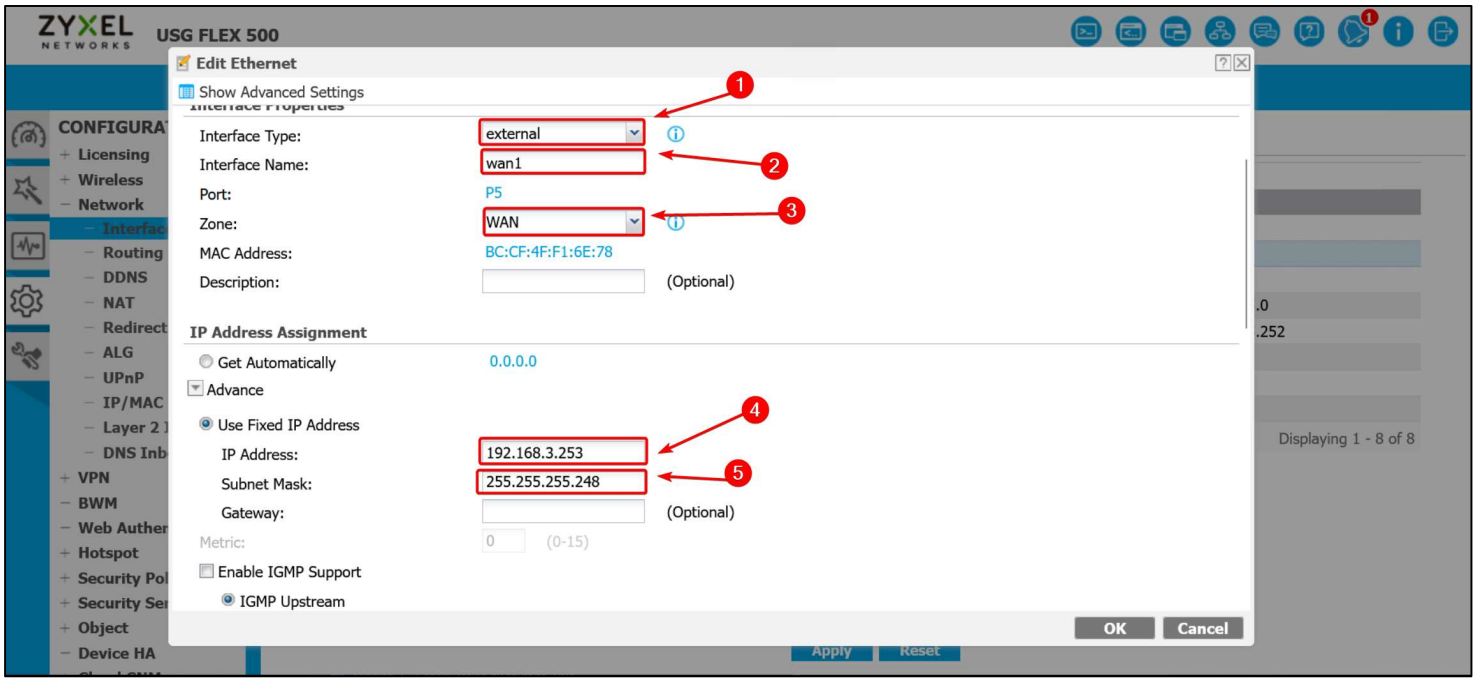
→ Interface DMZ



→ Interface ZONELAN



→ Interface WAN

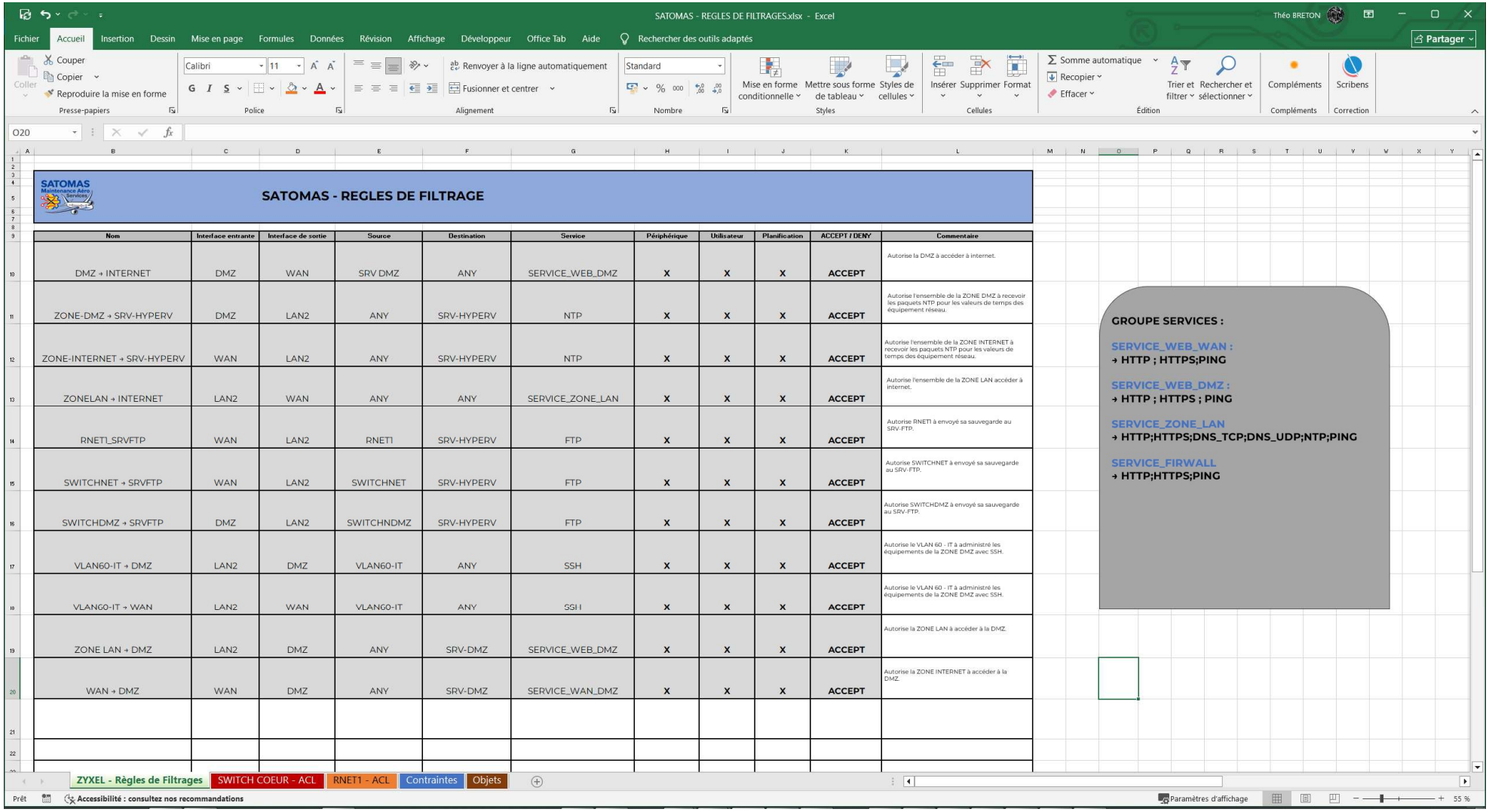


Mission 2 : Configuration du RIPv2 sur le pare feu

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network DMZ
Router(config-router)# network ZONELAN
Router(config-router)# network wan1
Router(config-router)# exit
```

Mission 3 : Recensement des règles de filtrage à mettre en place sur le Pare Feu

Création d'un fichier excel pour l'infra SATOMAS sur les règles de filtrage qui seront mise en place.



SATOMAS - REGLES DE FILTRAGES.xlsx - Excel

SATOMAS - REGLES DE FILTRAGE

Nom	Interface entrante	Interface de sortie	Source	Destination	Service	Périphérique	Utilisateur	Planification	ACCEPT / DENY	Commentaire
DMZ → INTERNET	DMZ	WAN	SRV DMZ	ANY	SERVICE_WEB_DMZ	X	X	X	ACCEPT	Autorise la DMZ à accéder à internet.
ZONE-DMZ → SRV-HYPERV	DMZ	LAN2	ANY	SRV-HYPERV	NTP	X	X	X	ACCEPT	Autorise l'ensemble de la ZONE DMZ à recevoir les paquets NTP pour les valeurs de temps des équipement réseau.
ZONE-INTERNET → SRV-HYPERV	WAN	LAN2	ANY	SRV-HYPERV	NTP	X	X	X	ACCEPT	Autorise l'ensemble de la ZONE INTERNET à recevoir les paquets NTP pour les valeurs de temps des équipement réseau.
ZONELAN → INTERNET	LAN2	WAN	ANY	ANY	SERVICE_ZONE_LAN	X	X	X	ACCEPT	Autorise l'ensemble de la ZONE LAN accéder à internet.
RNET1_SRVFTP	WAN	LAN2	RNET1	SRV-HYPERV	FTP	X	X	X	ACCEPT	Autorise RNET1 à envoyé sa sauvegarde au SRV-FTP.
SWITCHNET → SRVFTP	WAN	LAN2	SWITCHNET	SRV-HYPERV	FTP	X	X	X	ACCEPT	Autorise SWITCHNET à envoyé sa sauvegarde au SRV-FTP.
SWITCHDMZ → SRVFTP	DMZ	LAN2	SWITCHNDMZ	SRV-HYPERV	FTP	X	X	X	ACCEPT	Autorise SWITCHDMZ à envoyé sa sauvegarde au SRV-FTP.
VLAN60-IT → DMZ	LAN2	DMZ	VLAN60-IT	ANY	SSH	X	X	X	ACCEPT	Autorise le VLAN 60 - IT à administré les équipements de la ZONE DMZ avec SSH.
VLAN60-IT → WAN	LAN2	WAN	VLAN60-IT	ANY	SSH	X	X	X	ACCEPT	Autorise le VLAN 60 - IT à administré les équipements de la ZONE DMZ avec SSH.
ZONE LAN → DMZ	LAN2	DMZ	ANY	SRV-DMZ	SERVICE_WEB_DMZ	X	X	X	ACCEPT	Autorise la ZONE LAN à accéder à la DMZ.
WAN → DMZ	WAN	DMZ	ANY	SRV-DMZ	SERVICE_WAN_DMZ	X	X	X	ACCEPT	Autorise la ZONE INTERNET à accéder à la DMZ.

GROUPE SERVICES :

SERVICE_WEB_WAN :
→ HTTP ; HTTPS;PING

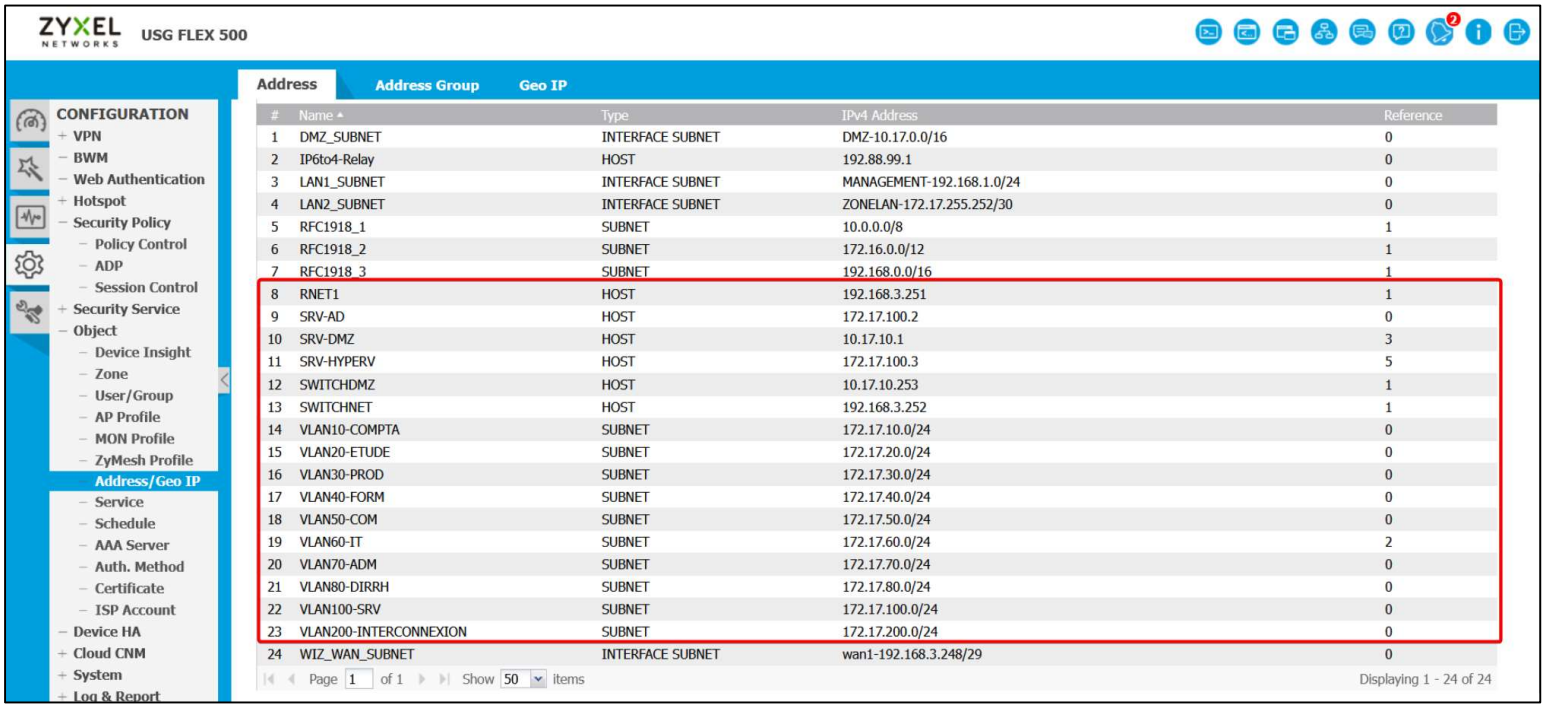
SERVICE_WEB_DMZ :
→ HTTP ; HTTPS ; PING

SERVICE_ZONE_LAN
→ HTTP;HTTPS;DNS_TCP;DNS_UDP;NTP;PING

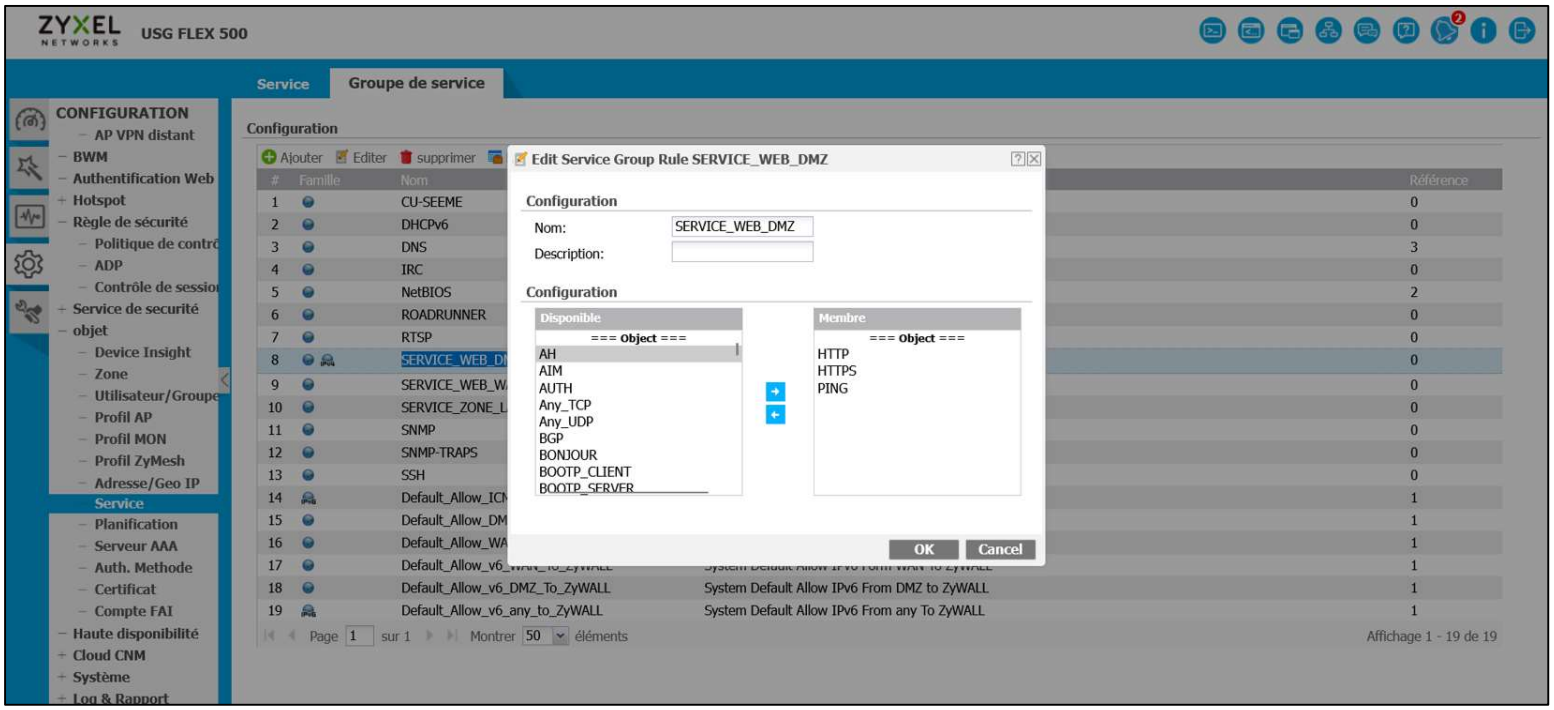
SERVICE_FIRWALL
→ HTTP;HTTPS;PING

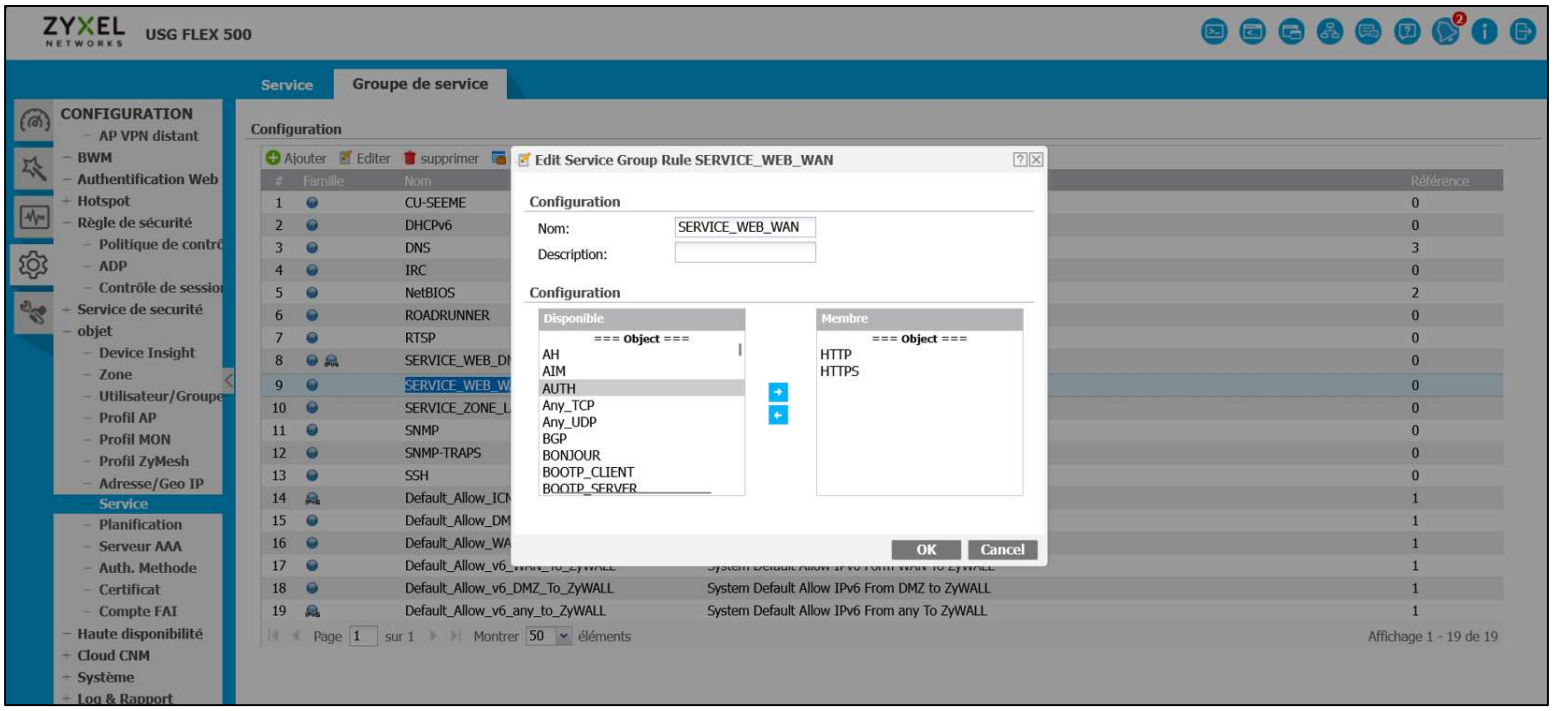
ZYXEL - Règles de Filtrages | SWITCH COEUR - ACL | RNET1 - ACL | Contraintes | Objets

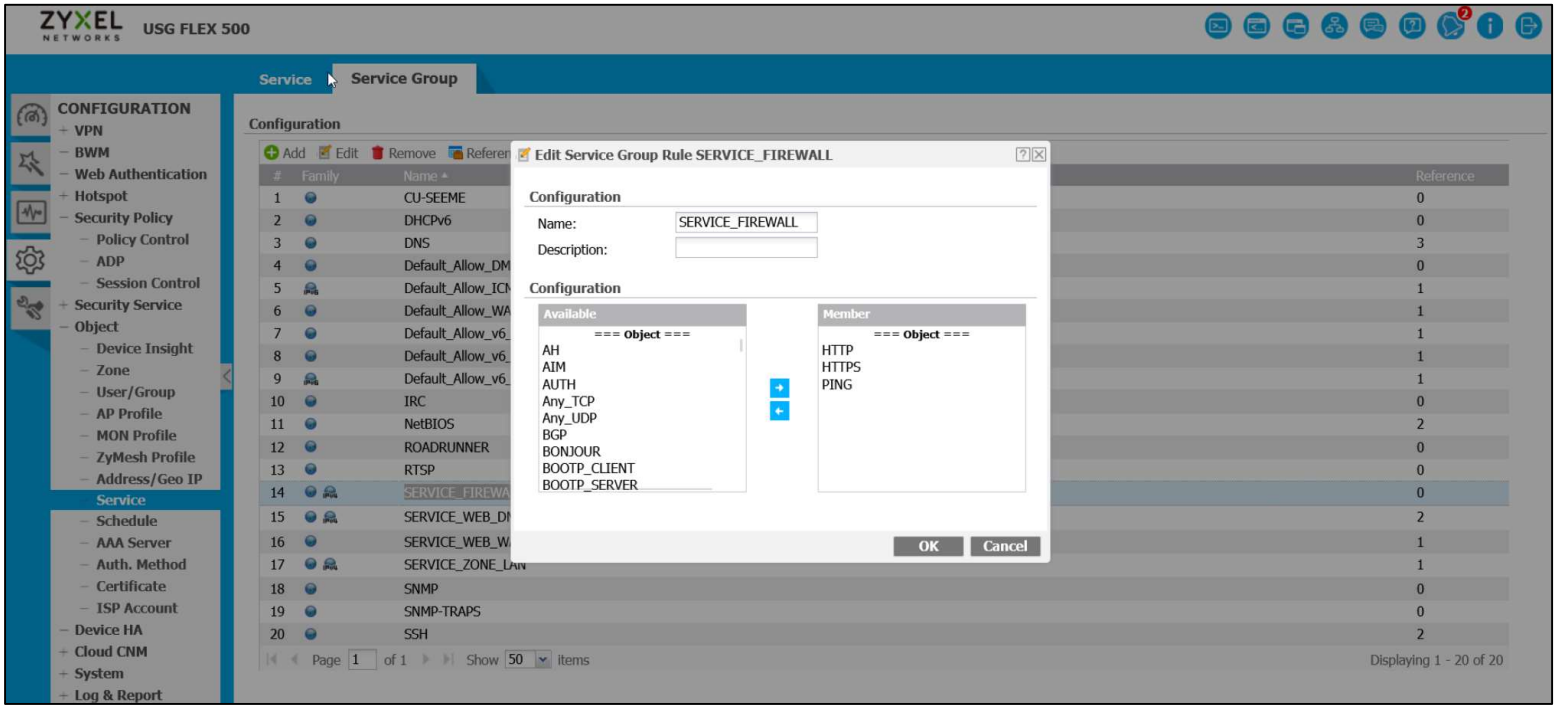
Mission 4 : Configuration des objets

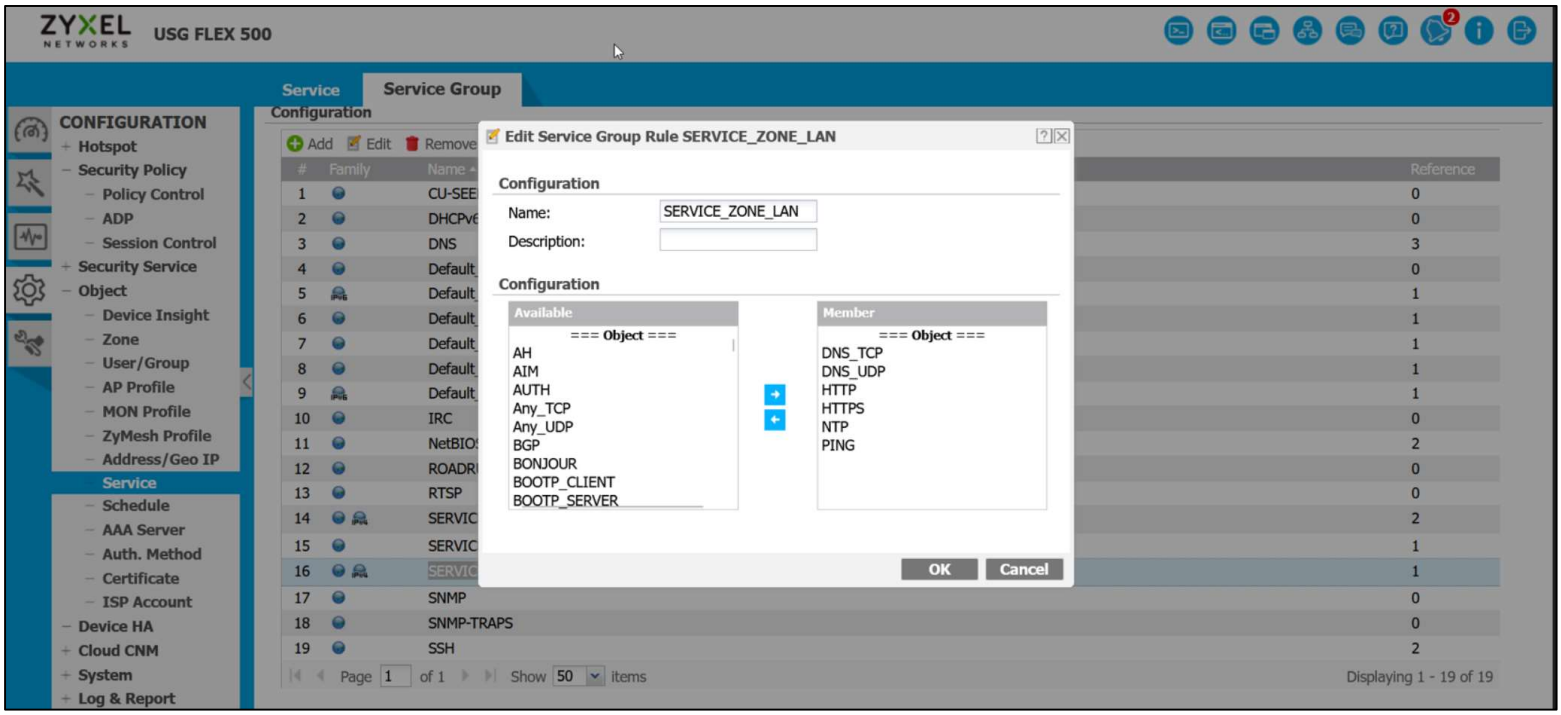


→ Groupe de services

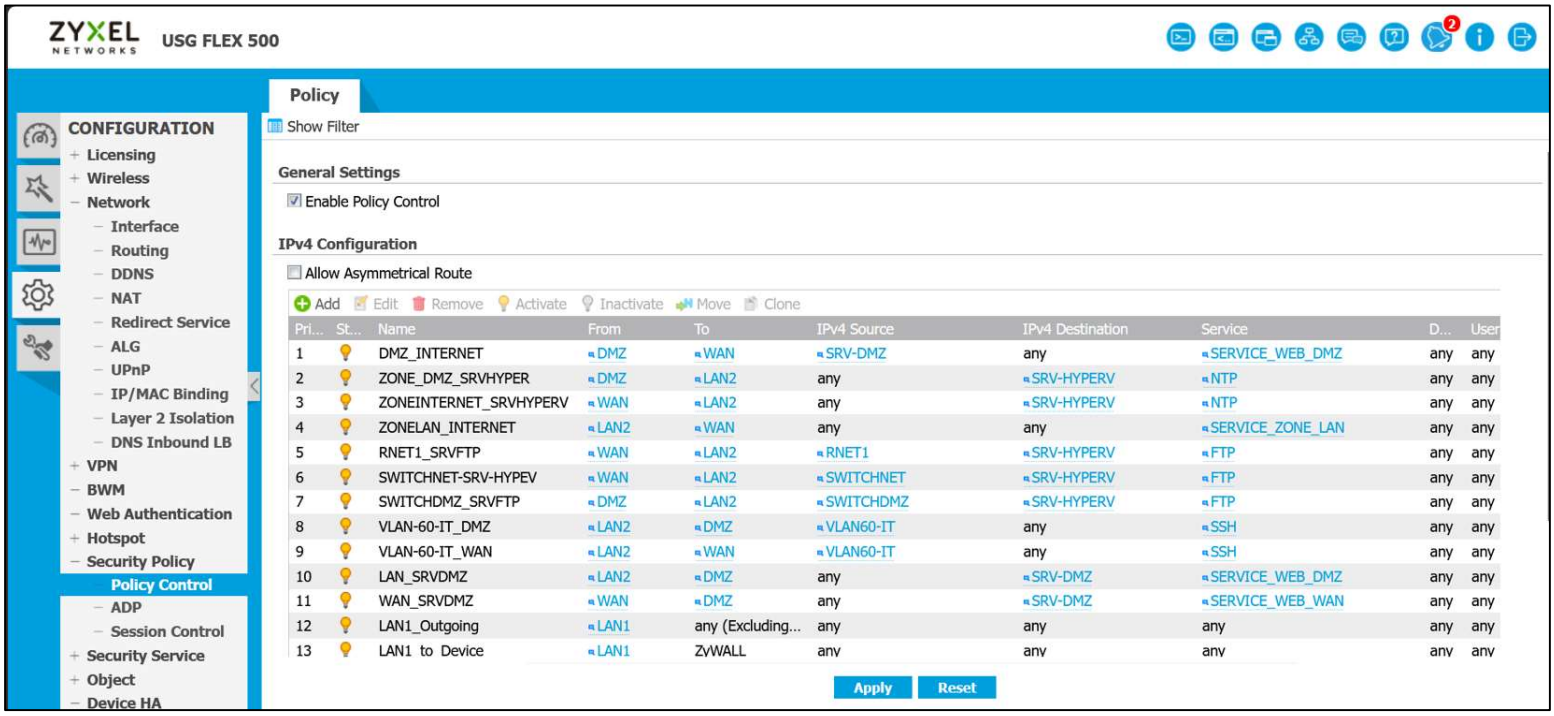



ZYXEL NETWORKS
USG FLEX 500
Service
Groupe de service
CONFIGURATION
AP VPN distant
BWM
Authentification Web
Hotspot
Règle de sécurité
Politique de contrô
ADP
Contrôle de sessio
Service de securité
objet
Device Insight
Zone
Utilisateur/Groupe
Profil AP
Profil MON
Profil ZyMesh
Adresse/Geo IP
Service
Planification
Serveur AAA
Auth. Methode
Certificat
Compte FAI
Haute disponibilité
Cloud CNM
Système
Log & Rapport
Configuration
Ajouter
Editer
supprimer
Edit Service Group Rule SERVICE_WEB_WAN
Configuration
Nom:
SERVICE_WEB_WAN
Description:
Configuration
Disponible
=== Object ===
AH
AIM
AUTH
Any_TCP
Any_UDP
BGP
BONJOUR
BOOTP_CLIENT
BOOTP_SERVER
Membre
=== Object ===
HTTP
HTTPS
OK
Cancel
Référence
Default_Allow_v6_DMZ_To_ZyWALL
System Default Allow IPv6 From DMZ to ZyWALL
Default_Allow_v6_any_to_ZyWALL
System Default Allow IPv6 From any To ZyWALL
Page 1 sur 1
Montrer 50 éléments
Affichage 1 - 19 de 19


ZYXEL NETWORKS
USG FLEX 500
Service
Service Group
CONFIGURATION
VPN
BWM
Web Authentication
Hotspot
Security Policy
Policy Control
ADP
Session Control
Security Service
Object
Device Insight
Zone
User/Group
AP Profile
MON Profile
ZyMesh Profile
Address/Geo IP
Service
Schedule
AAA Server
Auth. Method
Certificate
ISP Account
Device HA
Cloud CNM
System
Log & Report
Configuration
Add
Edit
Remove
Edit Service Group Rule SERVICE_FIREWALL
Configuration
Name:
SERVICE_FIREWALL
Description:
Configuration
Available
=== Object ===
AH
AIM
AUTH
Any_TCP
Any_UDP
BGP
BONJOUR
BOOTP_CLIENT
BOOTP_SERVER
Member
=== Object ===
HTTP
HTTPS
PING
OK
Cancel
Reference
Page 1 of 1
Show 50 items
Displaying 1 - 20 of 20

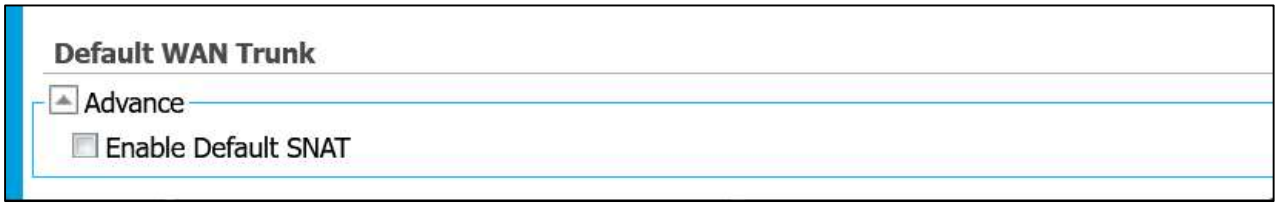


Mission 5 : Configuration des règles de filtrage



Mission 6 : Application des règles de filtrage

Désactivation NAT Par défaut.



A.6 Administration distante

Mission 1 : Paramétrage du SSH pour l'administration à distance

Mission 2 : Mise en place de l'expiration de la session

Mission 3 : Mise en place du nombre de tentative

Mission 4 : Mettre les mots de passe du mode enable

→ SwitchCoeur

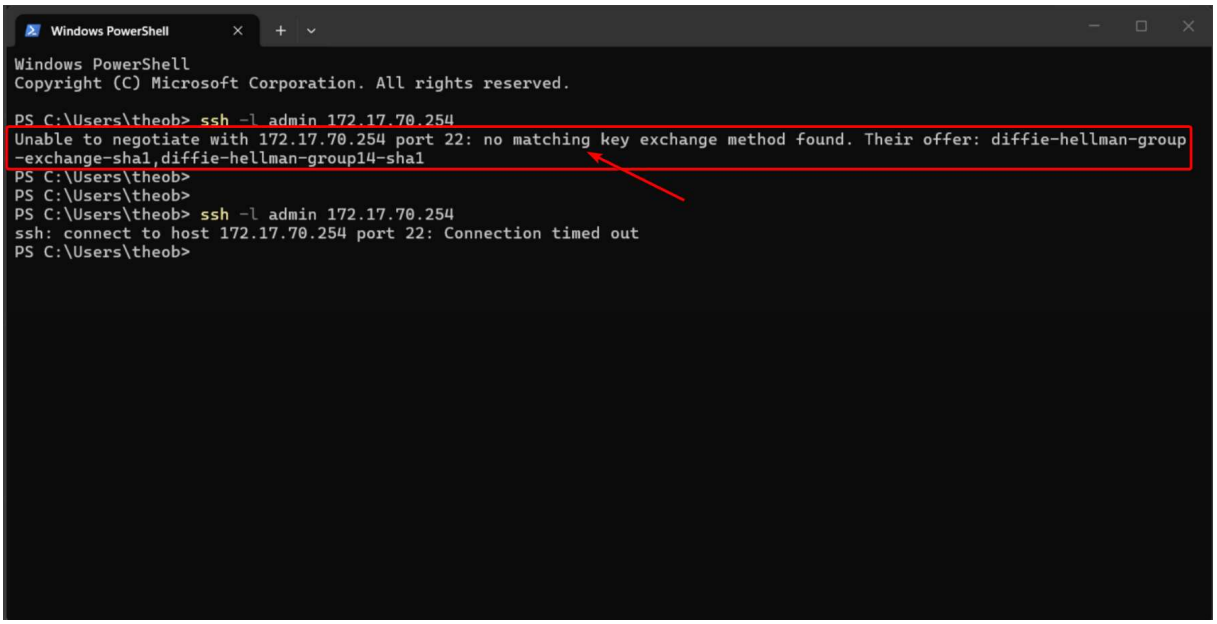
```
SwCoeur#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwCoeur(config)#line vty 0 1
SwCoeur(config-line)#transport input ssh
SwCoeur(config-line)#login local
SwCoeur(config-line)#password cisco
SwCoeur(config-line)#ip ssh version 2
SwCoeur(config)#
SwCoeur(config)#crypto key generate rsa general-keys modulus 2048
% You already have RSA keys defined named SwCoeur.ssh.key.
% They will be replaced.

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
*Sep 16 14:33:27.032: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SwCoeur.
[OK] (elapsed time was 5 seconds)

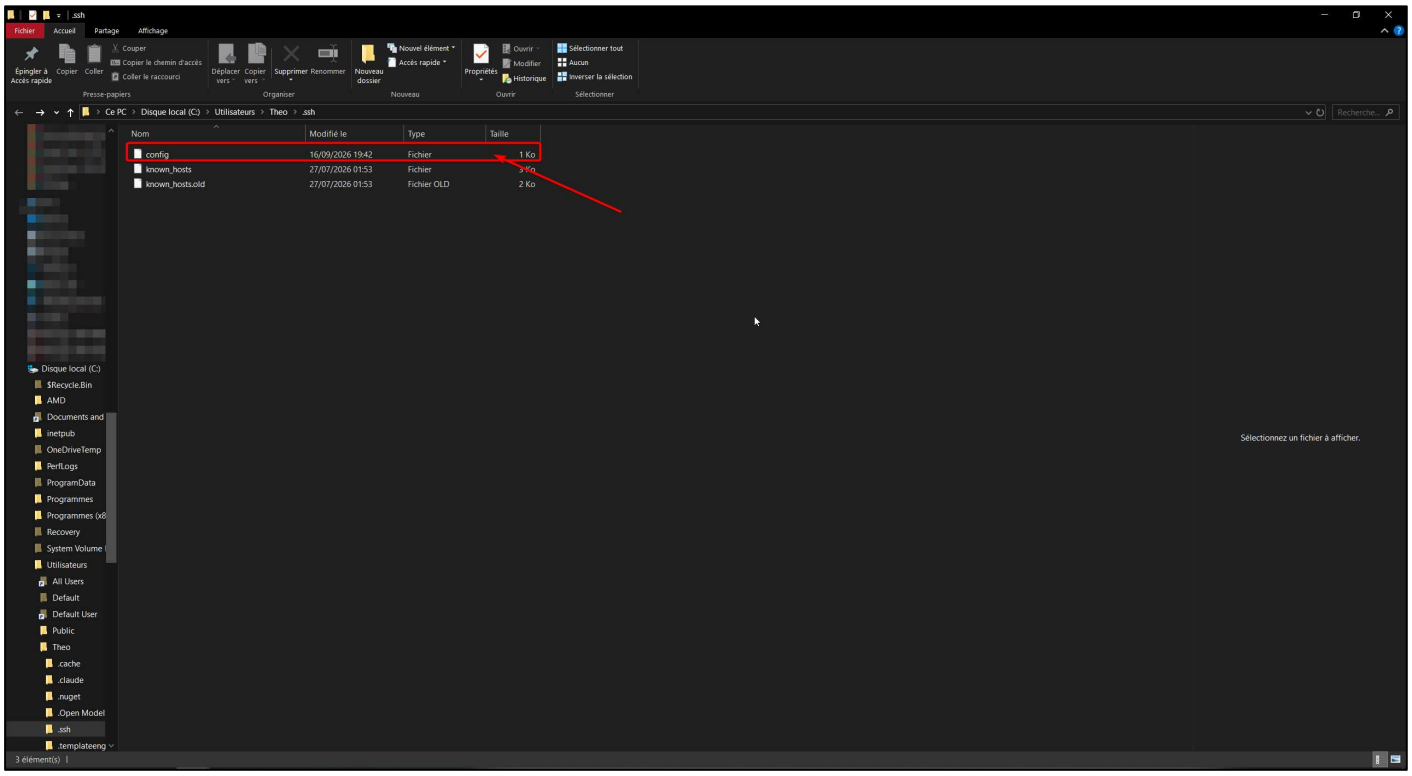
SwCoeur(config)#username admin password cisco
SwCoeur(config)#ip ssh time-out 60
SwCoeur(config)#ip ssh authentication-retries 3
```

***Même opération répété sur l'ensemble des éléments qui compose l'infrastructure de SATOMAS. Voir le Rapport de test pour la validation du SSH sur les équipements.**

Certain équipement Cisco utilise d'algorithme de chiffrement qui empêche la connexion SSH sur un poste Client. Le problème est que le switch utilise de vieux algorithme tandis que le pc client utilise des algorithme récent, par conséquent la connexion échoue.



Pour régler ce problème j'ai créé un fichier dans le chemin **`C:\Users\NOMUTILISATEUR\.ssh`**



Ce que contient le fichier « **config** »

```
Host 172.17.70.* 10.2.10.* 192.168.3.*
    User admin
    KexAlgorithms +diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
    HostKeyAlgorithms +ssh-rsa
    PubkeyAcceptedAlgorithms +ssh-rsa
    Ciphers +aes128-cbc,aes256-cbc
```

Mission 4 : Mettre les mots de passe du mode enable

```
SWNET

SwNet>
SwNet>
SwNet>en
SwNet#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwNet(config)#enable secret cisco

SWDMZ

Sw-DMZ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sw-DMZ(config)#enable secret cisco
Sw-DMZ(config)#exit

SWRC

SwRC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwRC(config)#enable secret cisco
SwRC(config)#

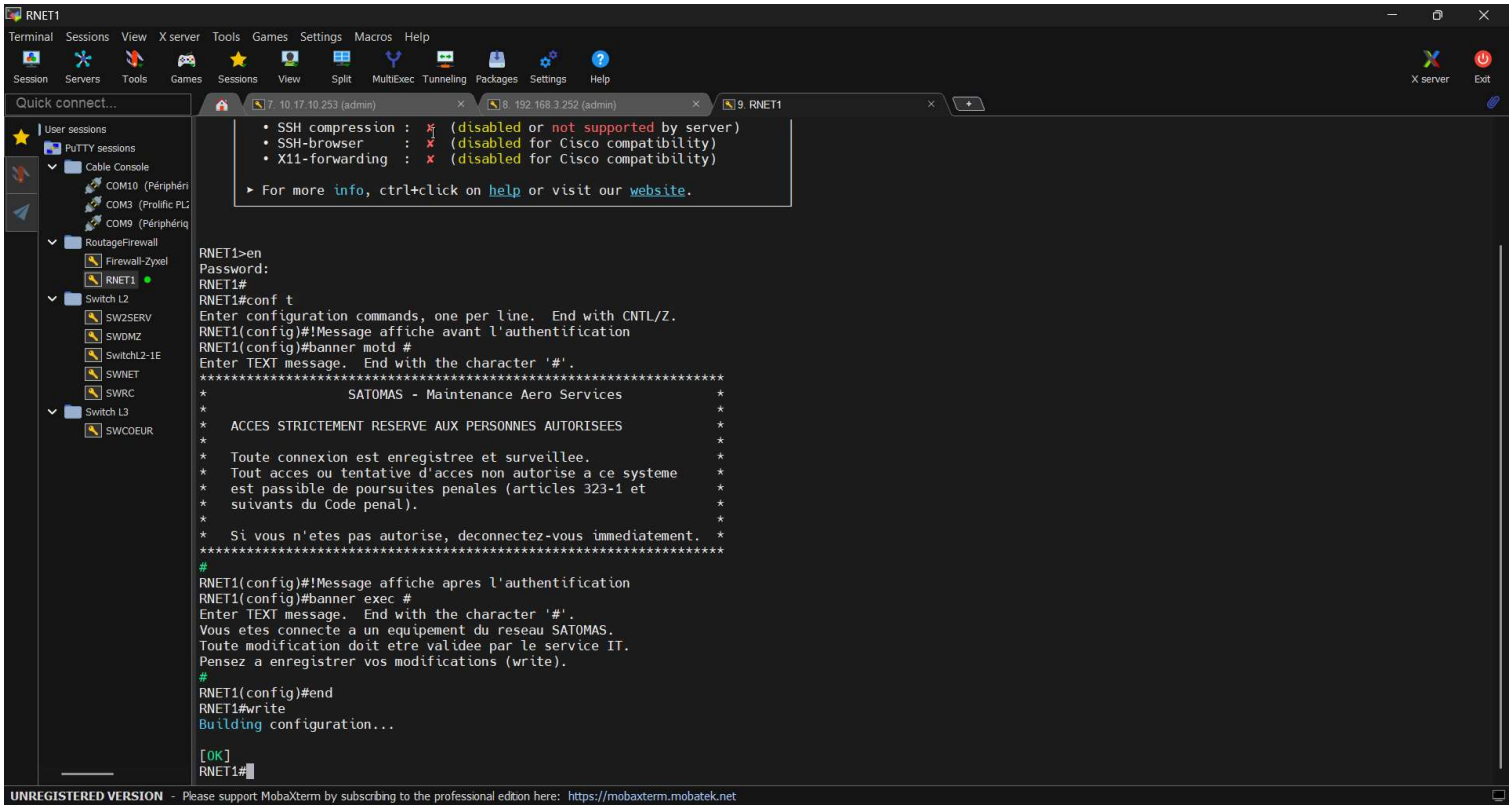
SW1E

Sw1E#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sw1E(config)#enable secret cisco
Sw1E(config)#end
Sw1E#
Sep 22 11:12:32.993: %SYS-5-CONFIG_I: Configured from console by console

SW2ESERV

Sw2eServ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sw2eServ(config)#enable secret cisco
Sw2eServ(config)#end
Sw2eServ#
Sep 22 09:14:27.645: %SYS-5-CONFIG_I: Configured from console by console
```

Mission 5 : Mettre les mots de passe du mode enable



A.7 - Switch L2 – DMZ

Mission 1 : Mise en place du VLAN 5 – DMZ

```
Sw-DMZ# conf t
Sw-DMZ(config)# vlan 5
Sw-DMZ(config-vlan)# name DMZ
Sw-DMZ(config-vlan)# exit
Sw-DMZ(config)#
```

Mission 2 : Configuré l'interface du vlan 5

```
Sw-DMZ# conf t
Sw-DMZ(config)# interface vlan 5
Sw-DMZ(config-if)# ip address 10.17.10.253 255.255.0.0
Sw-DMZ(config-if)# no shutdown
Sw-DMZ(config-if)# exit
Sw-DMZ(config)#
```

Mission 3 : Mise en place des ports en mode access sur la liaison Switch – Parefeu et Switch – SRV-WEB affecté au VLAN5

```
Sw-DMZ# conf t
Sw-DMZ(config)# interface fa0/1
Sw-DMZ(config-if)# switchport mode access
Sw-DMZ(config-if)# switchport access vlan 5
Sw-DMZ(config-if)# exit
Sw-DMZ(config)# interface gi0/1
Sw-DMZ(config-if)# switchport mode access
Sw-DMZ(config-if)# switchport access vlan 5
Sw-DMZ(config-if)# exit
Sw-DMZ(config)#
```

Mission 4 : Mise en place de la gateway sur le switch

```
Sw-DMZ# conf t
Sw-DMZ(config)# ip default-gateway 10.17.10.254
Sw-DMZ(config)#
```

Mission 5 : Configurer les authentifications FTP

```
Sw-DMZ# conf t
Sw-DMZ(config)# ip ftp username svc-backup-cisco
Sw-DMZ(config)# ip ftp password Admin123
Sw-DMZ(config)#
```

Mission 6 : Configurer le SSH

***Même opération répété sur l'ensemble des éléments qui compose l'infrastructure de SATOMAS. Voir le Rapport de test pour la validation du SSH sur les équipements.**

A.8 - ZONE INTERNET

→ SwitchNET

Mission 1 : Configuration des ports Gi1/0/47 et Gi1/0/48 en trunk :

```
interface GigabitEthernet1/0/47
description port-parefeu
switchport mode trunk
!
interface GigabitEthernet1/0/48
description port-routeur
switchport mode trunk
```

Mission 2 : Paramétrage du VLAN1

```
interface Vlan1
ip address 192.168.3.252 255.255.255.248
```

Mission 3 : Configuration de la Gateway

```
ip default-gateway 192.168.3.253
```

Mission 4 : Paramétrage des authentifications FTP

```
ip ftp username svc-backup-cisco
ip ftp password Admin123
```

Mission 4 : Paramétrage du SSH

***Même opération répété sur l'ensemble des éléments qui compose l'infrastructure de SATOMAS. Voir le Rapport de test pour la validation du SSH sur les équipements.**

→ RNET1

Mission 5 : Configuration des interfaces de RNET1 :

```
interface GigabitEthernet0/1
ip address 192.168.4.22 255.255.255.0
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.3.251 255.255.255.248
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
```

Mission 6 : Configuration du RIPv2

Configuration de l'interface Gi0/1 en mode passif pour éviter toute diffusion des VLANs au moyen du RIP sur le réseau LABO

```
router rip version 2

network 192.168.3.0

network 192.168.4.0

no auto-summary

passive-interface GigabitEthernet0/1
```

Mission 7 : Configuration de la route par défaut vers Internet

```
ip route 0.0.0.0 0.0.0.0 192.168.4.254
```

Mission 8 : Configuration de la route par défaut vers Internet

```
ip nat inside source list 1 interface GigabitEthernet0/1 overload

ip nat inside source static 10.2.10.1 192.168.4.23

ip nat inside source static 172.17.100.3 192.168.4.24

access-list 1 permit 172.17.0.0 0.0.0.255

access-list 1 permit 10.2.0.0 0.0.255.255

interface GigabitEthernet0/2 → Interne

ip nat inside

interface GigabitEthernet0/1 → Vers Internet

ip nat outside
```

Mission 9 : Mise en place d'une ACL pour bloquer l'accès SSH depuis Internet.

```
conf t

access-list 10 deny 192.168.4.0 0.0.0.255

access-list 10 permit any

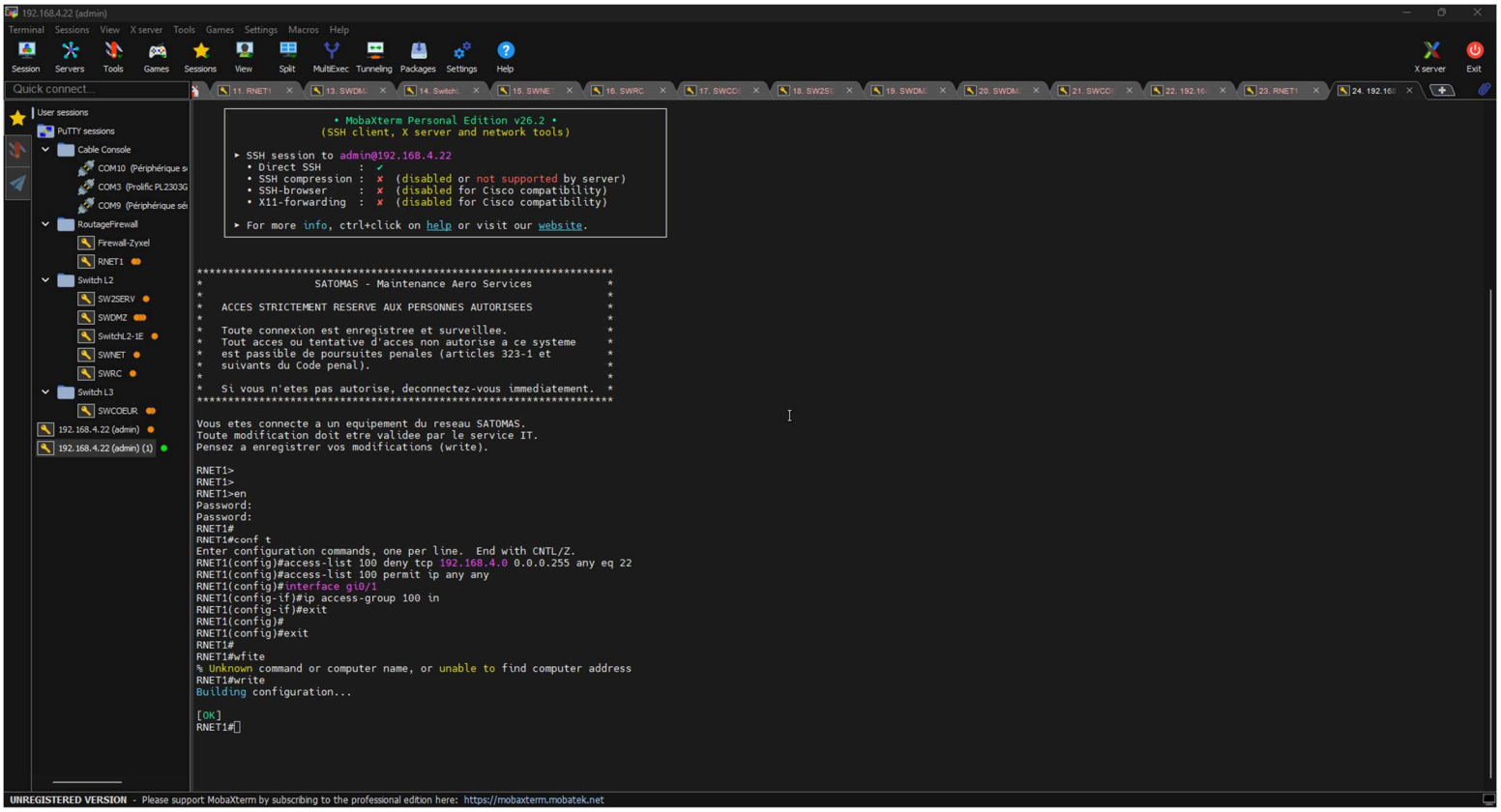
line vty 0 15

access-class 10 in
```

```
exit

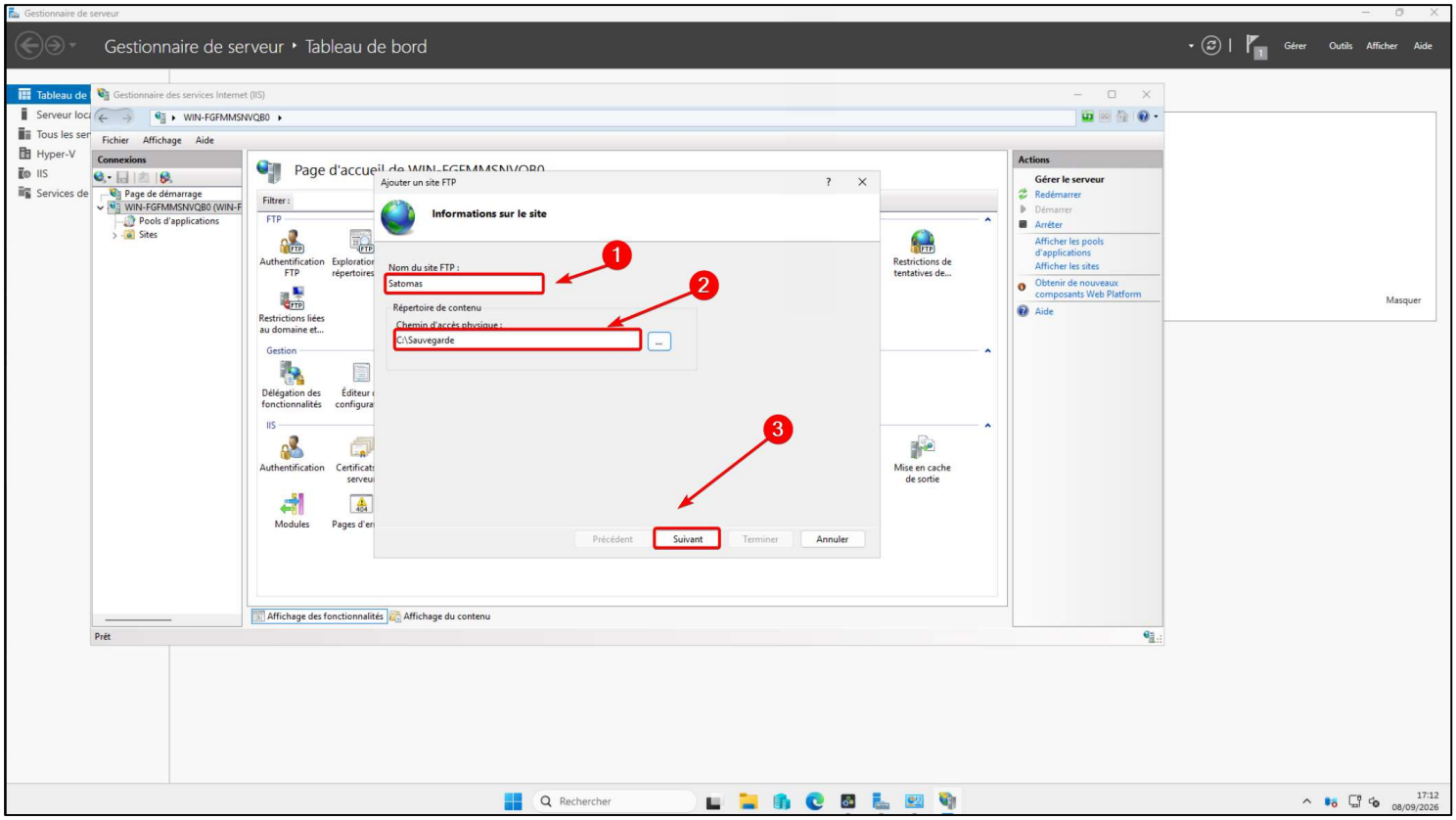
end

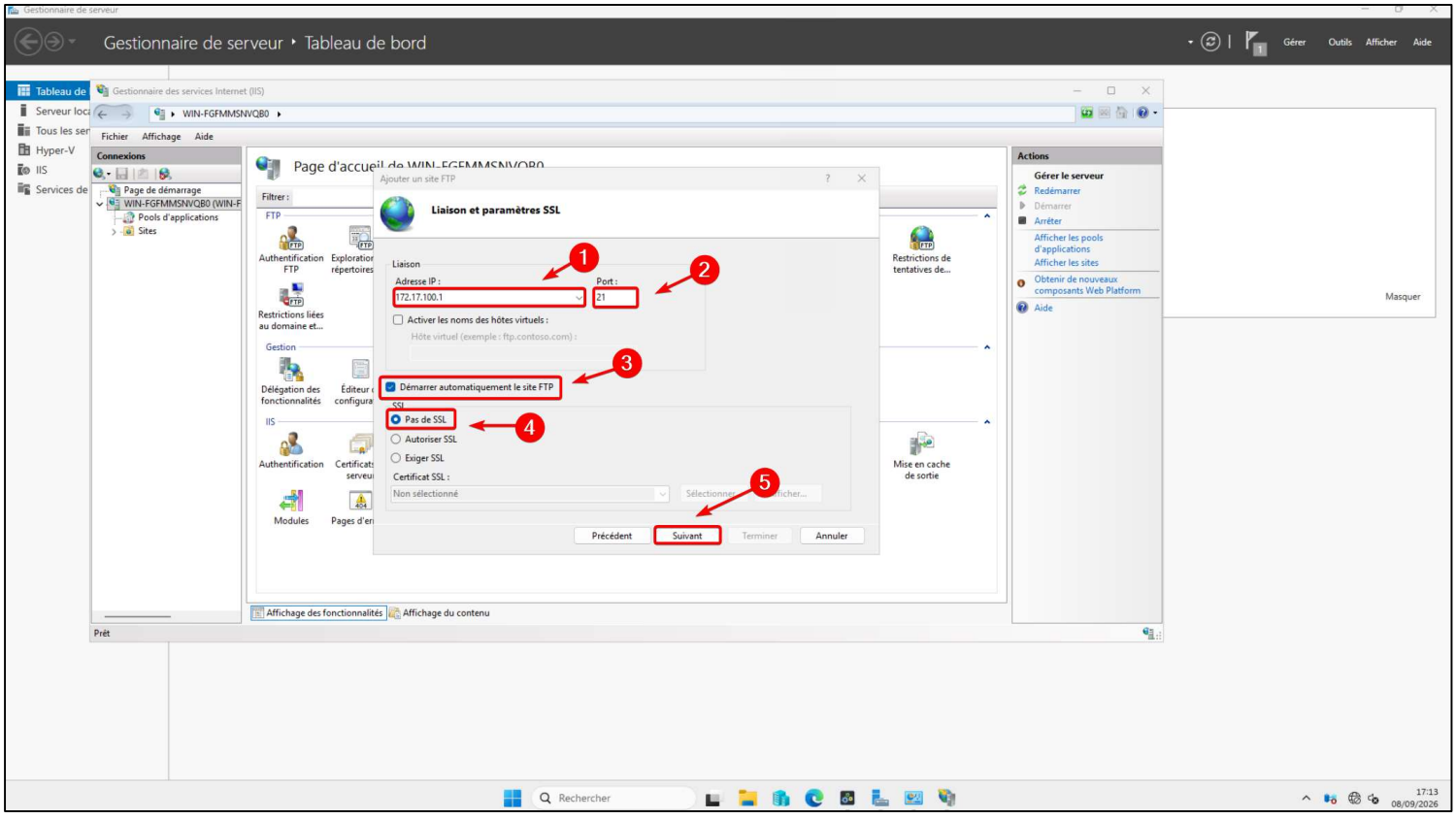
write
```

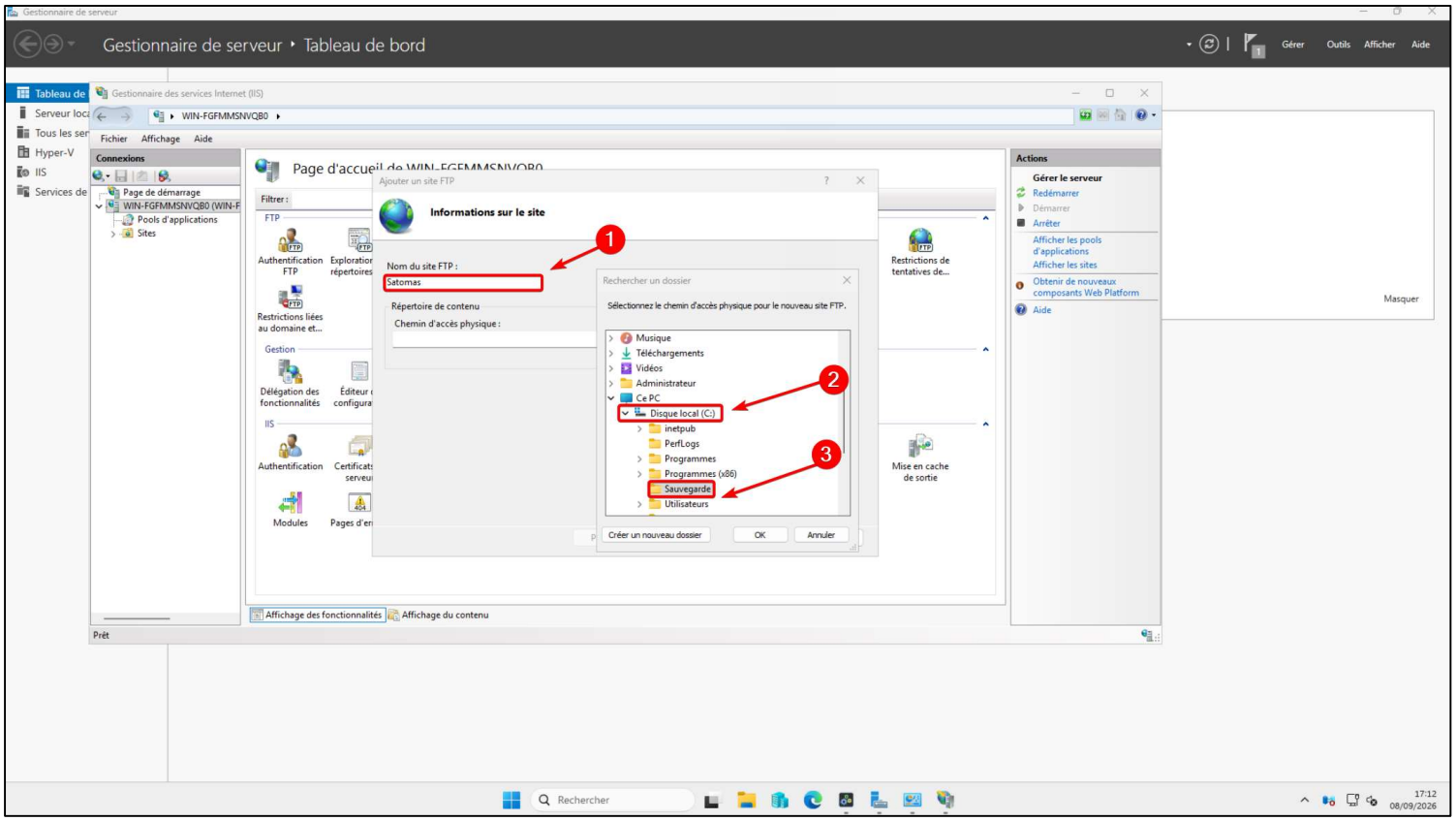


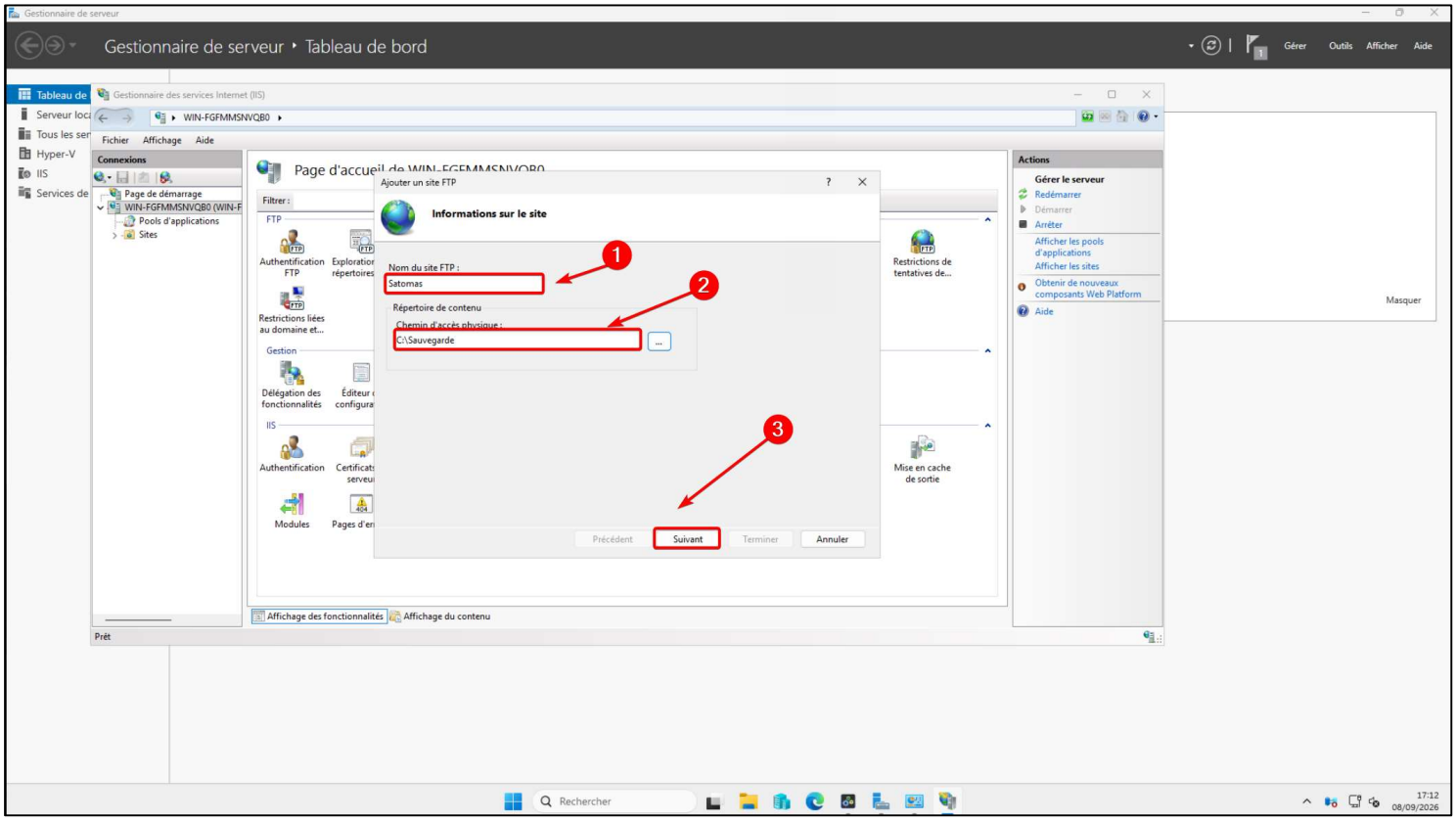
A.9 Sauvegarde

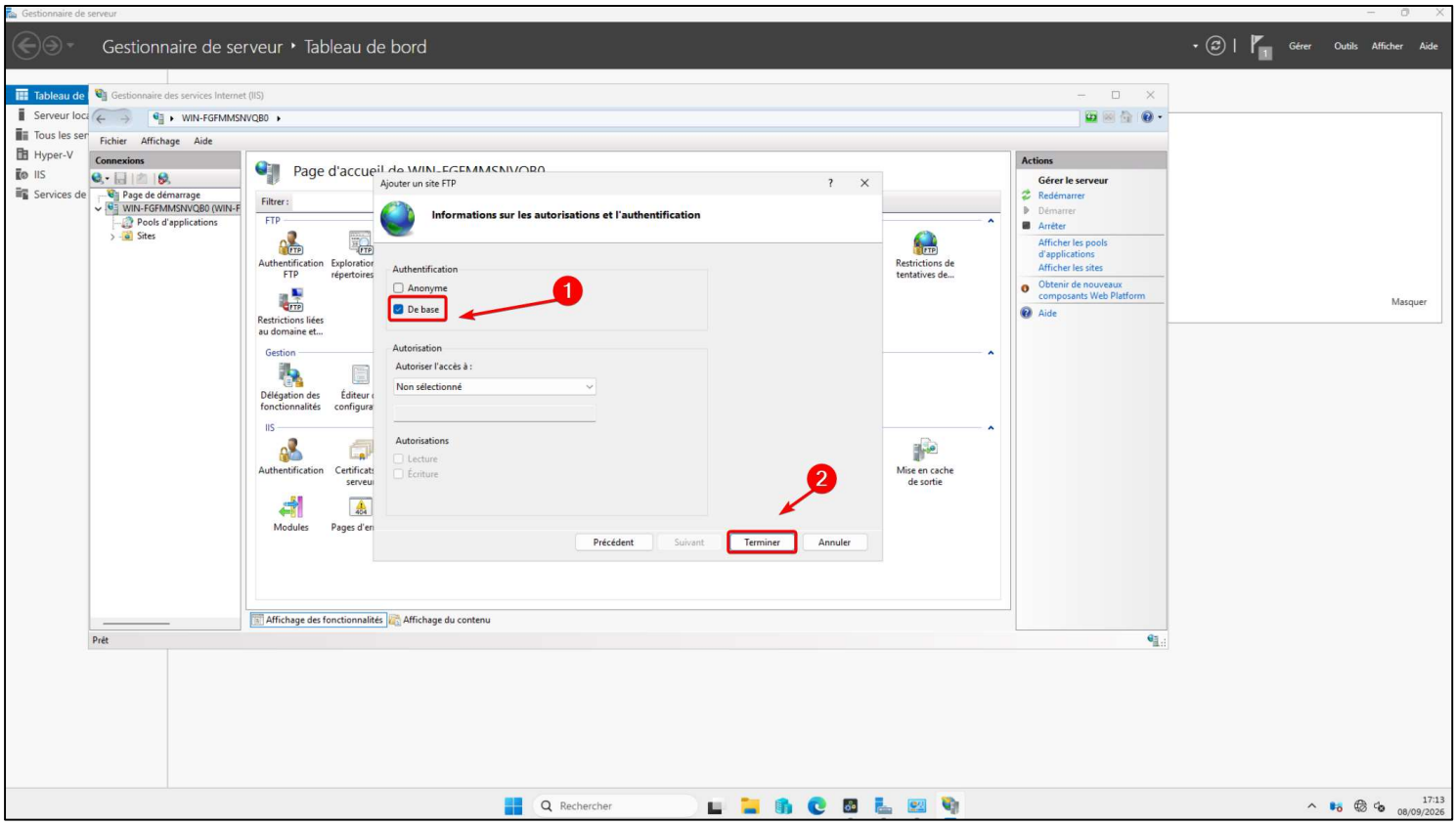
Mission 1 : Mise en place du serveur FTP sur l'infra :

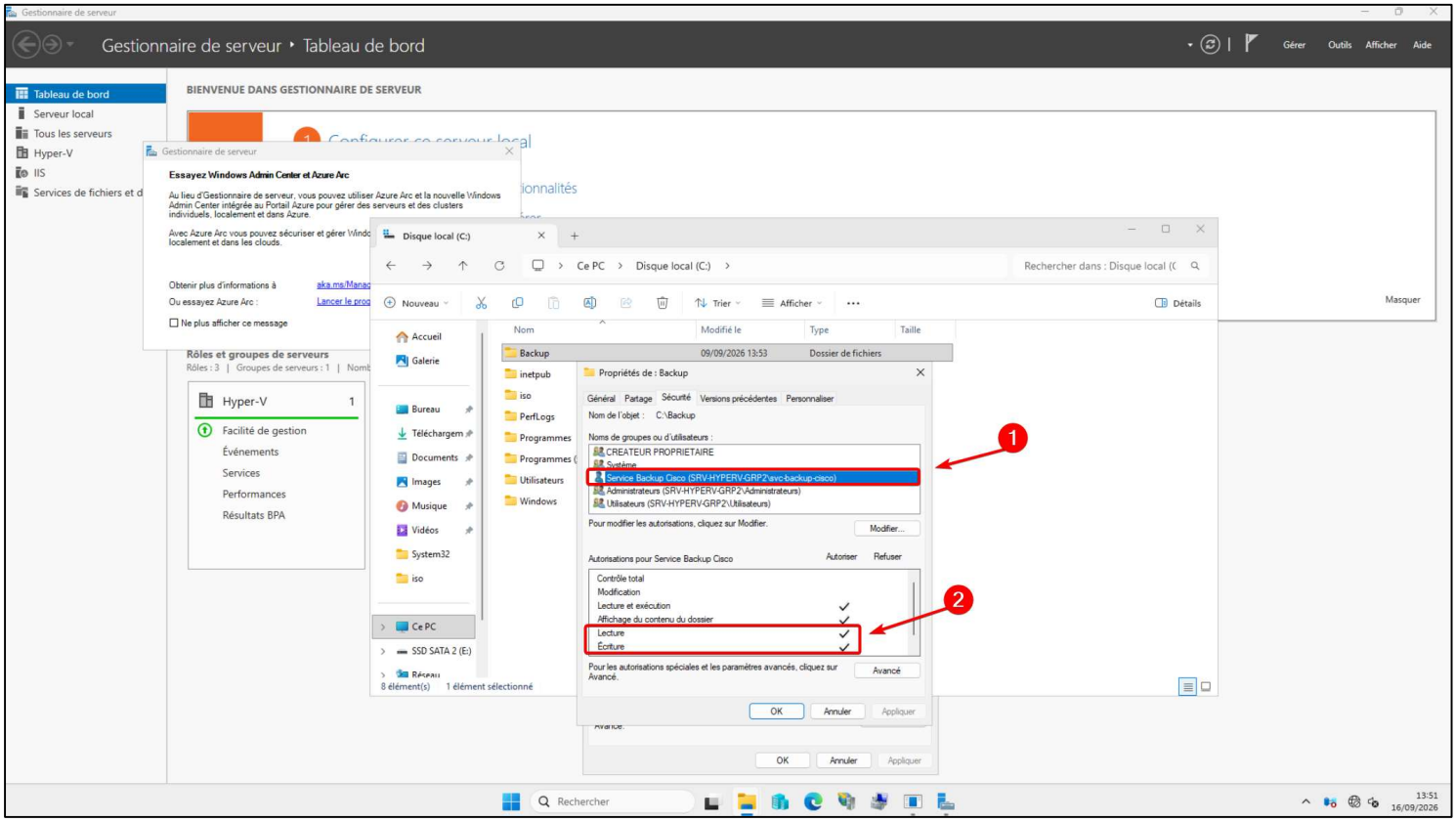





Gestionnaire de serveur • Tableau de bord
Ajouter un site FTP
Informations sur le site
Nom du site FTP :
Satomas
Répertoire de contenu
Chemin d'accès physique :
Rechercher un dossier
Sélectionnez le chemin d'accès physique pour le nouveau site FTP.
Musique
Téléchargements
Vidéos
Administrateur
Ce PC
Disque local (C:)
inetpub
PerfLogs
Programmes
Programmes (x86)
Sauvegarde
Utilisateurs
Créer un nouveau dossier
OK
Annuler
1
2
3


Gestionnaire de serveur • Tableau de bord
Ajouter un site FTP
Informations sur le site
Nom du site FTP :
Satomas
Répertoire de contenu
Chemin d'accès physique :
C:\Sauvegarde
Précédent
Suivant
Terminer
Annuler
1
2
3





Mission 2 : Mise en place des authentification FTP sur les équipements physique :

→ SwitchCoeur

```
ip ftp username svc-backup-cisco
ip ftp password Admin123
```

→ SwitchRDC

```
ip ftp username svc-backup-cisco
ip ftp password Admin123
```

→ Switch1E

```
ip ftp username svc-backup-cisco
ip ftp password Admin123
```

→ Switch2E-SERV

```
ip ftp username svc-backup-cisco
ip ftp password Admin123
```

→ SwitchDMZ

```
ip ftp username svc-backup-cisco
ip ftp password Admin123
```

Mission 3 - Automatiser la sauvegarder avec la méthode Kron

```
conf t

#Fuseau horaire et heure d'été
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00

#Renseignement du serveur NTP
ntp server 172.17.100.3
service password-encryption
file prompt quiet

#Les authentification FTP
ip ftp username svc-backup-cisco
ip ftp password Admin123

#Commandes de sauvegarde
kron policy-list SaveConfig
cli write
cli copy running-config ftp://172.17.100.3/
exit

#Sauvegarde le mardi à 17h
kron occurrence SaveConfigTuesday at 17:00 Tue recurring
policy-list SaveConfig
exit

#Sauvegarde le mercredi à 16h
kron occurrence SaveConfigWednesday at 16:00 Wed recurring
policy-list SaveConfig
exit
end
```

```
write
```

Mission 4 – Mise en place du NTP sur le serveur

Étape 1 : définir les sources NTP externes

```
w32tm /config /manualpeerlist:"0.fr.pool.ntp.org,0x8 1.fr.pool.ntp.org,0x8 2.fr.pool.ntp.org,0x8"
/syncfromflags:manual /reliable:YES /update
```

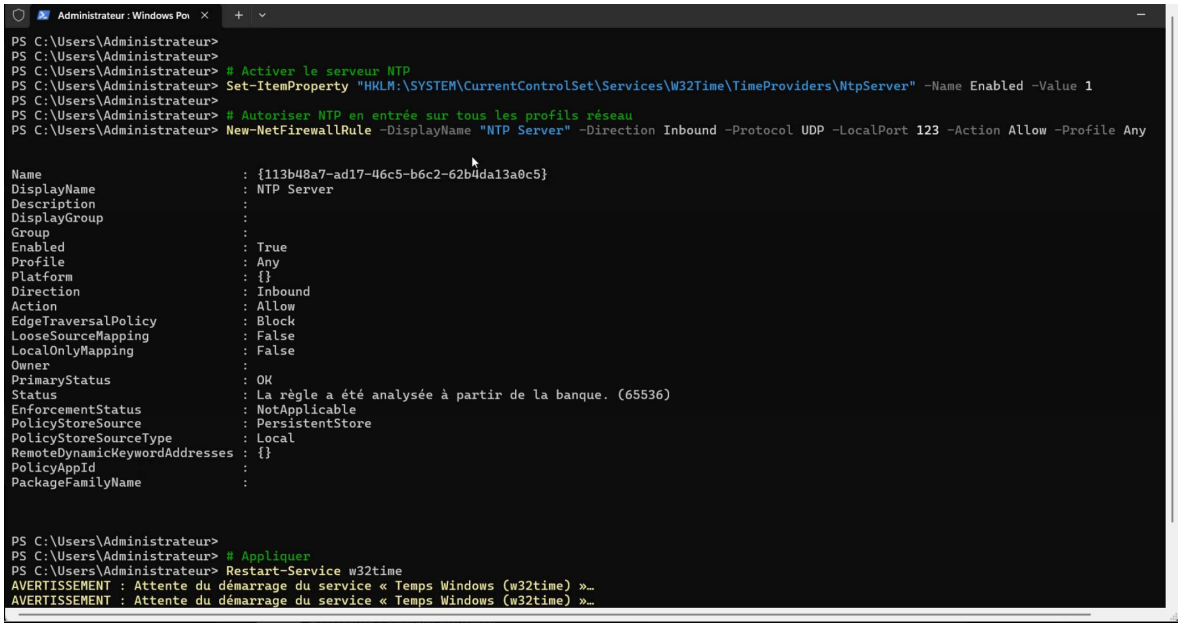
- manualpeerlist : les serveurs du pool NTP français utilisés comme sources.
- 0x8 : mode client standard. C'est celui qui fonctionne avec le pool, contrairement à 0x1 que tu avais essayé au début et qui laissait les sources « En attente ».
- syncfromflags:manual : le serveur utilise cette liste et non la hiérarchie du domaine.
- reliable:YES : le serveur s'annonce comme source de temps fiable pour les autres équipements.

Étape 2 : activer le rôle de serveur NTP

```
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer" -Name
Enabled -Value 1
```

Étape 3 : ouvrir le port NTP dans le pare-feu Windows

```
New-NetFirewallRule -DisplayName "NTP Server" -Direction Inbound -Protocol UDP -LocalPort 123 -
Action Allow -Profile Any
```



Étape 4 : démarrage automatique et redémarrage du service

```
Set-Service w32time -StartupType Automatic
Restart-Service w32time
w32tm /resync /rediscover
```

Étape 5 : vérifications

```
w32tm /query /status
w32tm /query /peers
netstat -ano -p udp | findstr ":123"
```

```
PS C:\Users\Administrateur> Restart-Service w32time
PS C:\Users\Administrateur> New-NetFirewallRule -Name "NTP-Server-In" -DisplayName "Serveur NTP (UDP 123)" -Direction Inbound -Protocol UDP -LocalPort
Action Allow -Profile Any


Name                            : NTP-Server-In
DisplayName                     : Serveur NTP (UDP 123)
Description                     :
DisplayGroup                    :
Group                           :
Enabled                         : True
Profile                         : Any
Platform                        : {}
Direction                       : Inbound
Action                          : Allow
EdgeTraversalPolicy             : Block
LooseSourceMapping              : False
LocalOnlyMapping                : False
Owner                           :
PrimaryStatus                   : OK
Status                          : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus               : NotApplicable
PolicyStoreSource               : PersistentStore
PolicyStoreSourceType           : Local
RemoteDynamicKeywordAddresses   : {}
PolicyAppId                     :
PackageFamilyName               :



PS C:\Users\Administrateur> w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 1 (Référence principale, synchronisée par l'horloge du réveil)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0000000s
Dispersion de racine : 10.0000000s
```

```
Administrateur : Windows Po

PS C:\Users\Administrateur> w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 1 (Référence principale, synchronisée par l'horloge du réveil)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0000000s
Dispersion de racine : 10.0000000s
ID de référence : 0x4C4F434C (Nom de la source :  "LOCL")
Heure de la dernière synchronisation réussie : 29/09/2026 15:41:37
Source : Local CMOS Clock
Intervalle d'interrogation : 6 (64s)

PS C:\Users\Administrateur> w32tm /query /peers
Nb d'homologues : 3

Homologue : 0.fr.pool.ntp.org,0x1
État : En attente
Temps restant : 798.0611677s
Mode : 0 (Réservé)
Couche : 0 (Non spécifié)
HomologueIntervalle d'interrogation : 0 (Non spécifié)
HôteIntervalle d'interrogation : 0 (Non spécifié)

Homologue : 1.fr.pool.ntp.org,0x1
État : En attente
Temps restant : 798.0611589s
Mode : 0 (Réservé)
Couche : 0 (Non spécifié)
HomologueIntervalle d'interrogation : 0 (Non spécifié)
HôteIntervalle d'interrogation : 0 (Non spécifié)

Homologue : 2.fr.pool.ntp.org,0x1
État : En attente
Temps restant : 798.0611455s
Mode : 0 (Réservé)
Couche : 0 (Non spécifié)
```

Mission 5 – Réception des sauvegardes :

