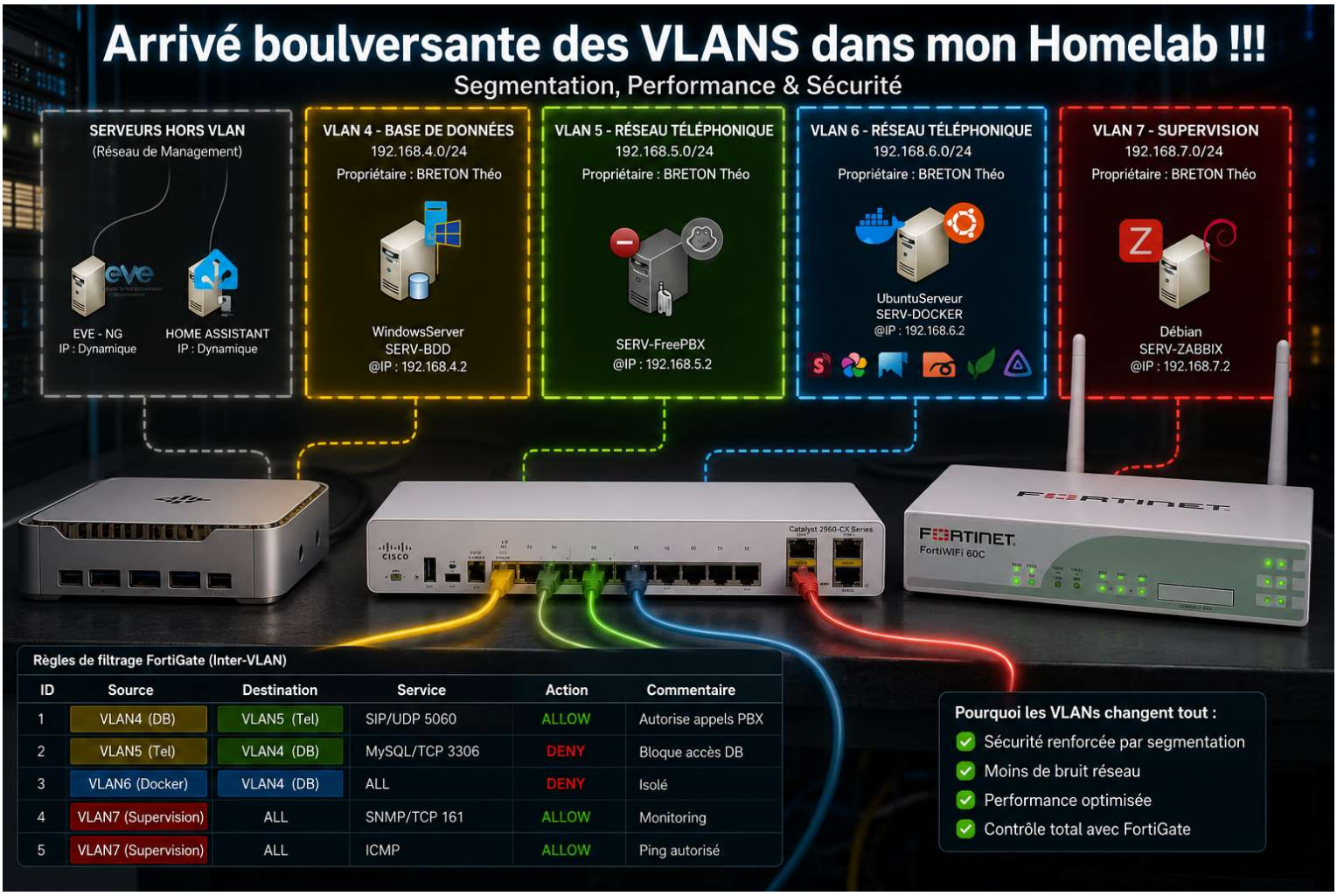
BRETON Théo

PROJET N°7 : CONFIGURATION DES VLANS SUR MON SWITCH 2960-C Serie LL



Etape 1 : Renommer le Switch avec le nom de mon choix

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-HOMELAB_THEO
```

Etape 2 : Création des vlans

```
SW-HOMELAB_THEO#conf t
SW-HOMELAB_THEO(config)#vlan 4
SW-HOMELAB_THEO(config-vlan)# Reseau_Serveur_BDD
SW-HOMELAB_THEO(config)#exit

SW-HOMELAB_THEO(config)#vlan 5
SW-HOMELAB_THEO(config-vlan)# Reseau_Telephonique
SW-HOMELAB_THEO(config)#exit

SW-HOMELAB_THEO(config)#vlan 6
SW-HOMELAB_THEO(config-vlan)# Reseau_Docker
SW-HOMELAB_THEO(config)#exit

SW-HOMELAB_THEO(config)#vlan 7
SW-HOMELAB_THEO(config-vlan)# Reseau_Supervision
SW-HOMELAB_THEO(config)#exit
```

Etape 3 : Configuration du vlan 1

```
SW-HOMELAB_THEO#conf t
SW-HOMELAB_THEO(config)#int vlan 1
SW-HOMELAB_THEO(config-if)#ip address 192.168.3.2 255.255.255.0
SW-HOMELAB_THEO(config-if)#no sh
SW-HOMELAB_THEO(config-if)#exit
```

Etape 4 : Configuration des ports en mode trunk

Le mode trunk permet de laisser passer les VLANs dans mes ports gigabit avec la norme du 802-1q qui va étiquette les paquets qui transite sur le réseau.

```
SW-HOMELAB_THEO#conf t
SW-HOMELAB_THEO(config)#interface range gi0/1-2
SW-HOMELAB_THEO(config-if)#switchport mode trunk
SW-HOMELAB_THEO(config-if)#no sh
SW-HOMELAB_THEO(config-if)#exit
```

Etape 5 : Paramétrage de la gateway pour que switch communique avec le Fortigate présent sur mon Homelab.

```
SW-HOMELAB_THEO#conf t
SW-HOMELAB_THEO(config)#ip default-gateway 192.168.3.1
```

Etape 6 : Configuration des paramètres pour l'accès à l'interface web.

```
Les paramètre par défauts déjà présent :

ip http server
ip http secure-server


Je rajoute cette ligne pour avoir une authentification avec un utilisateur local
inscrit sur le Switch.

SW-HOMELAB_THEO(config)# ip http authentication local
```

Etape 7 : Paramétrage du SSH

Pour pouvoir exécuter des opérations d'administration réseau sur l'équipement à distance il faut utiliser un protocole sécurisé.

```
Switch>enable
Switch#conf t
Switch(config)#line vty 0 4
Switch(config-line)#transport input ssh
Switch(config-line)#login local
Switch(config-line)#password XXXXXX
Switch(config)#ip domain name theo.local
Switch(config)#crypto key generate rsa general-keys modulus 2048
```

Pour ajouter une couche de sécurité j'ai ajouté les options suivantes :

```
Ajout des options :

#Un timeout de 60 secondes pour les sessions ssh en cas d'inactivité
Switch(config)#ip ssh time-out 60

#3 essais pour la connexion au switch
Switch(config)#ip ssh authentication-retries 3
```

Etape 8 : Paramétrage du SNMPv3

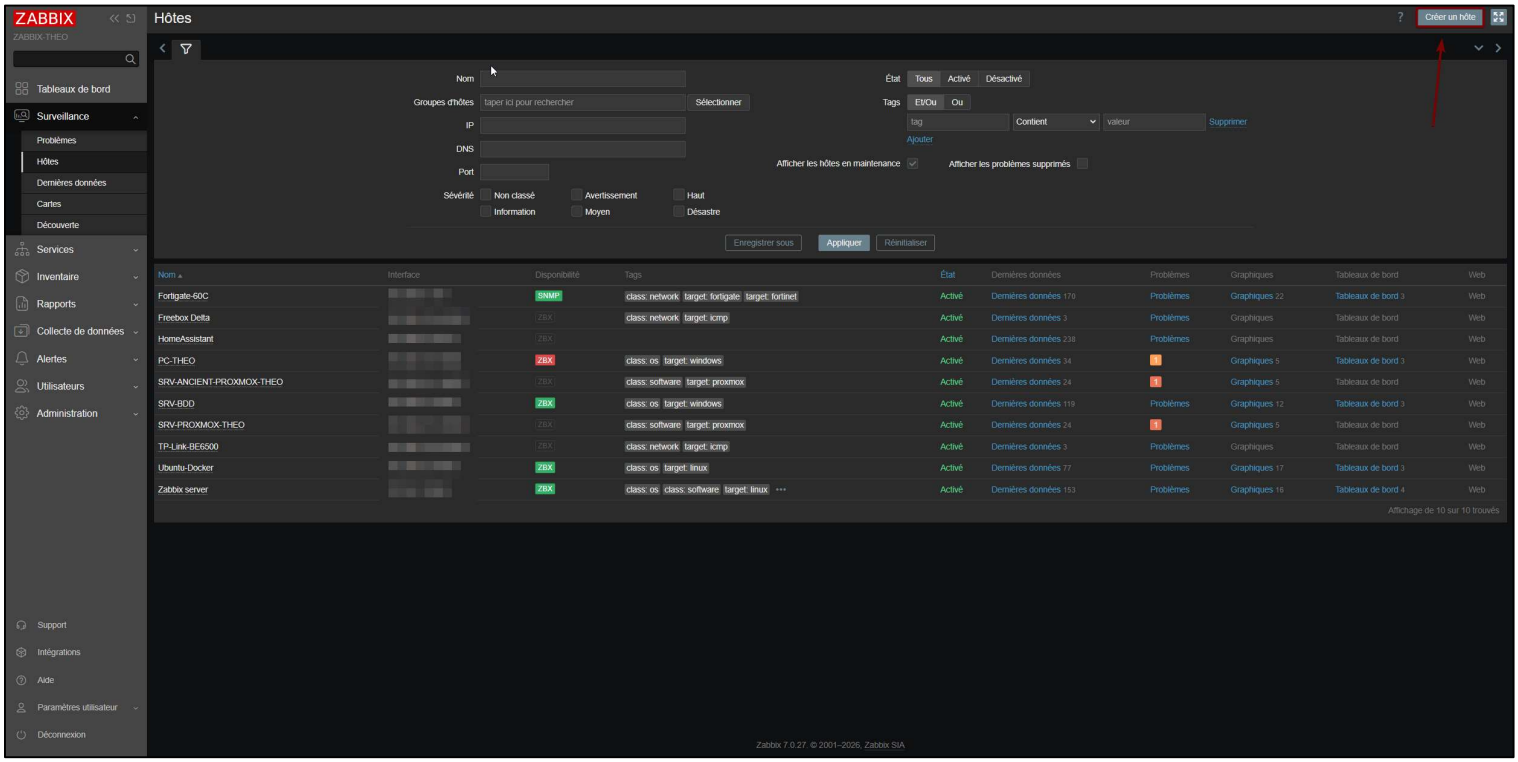
```
Switch(config)#snmp-server group ZABBIX-GROUP v3 priv
Switch(config)# snmp-server user [USER] ZABBIX-GROUP v3 auth sha
[MOT_DE_PASSE_AUTH] priv aes 128 [MOT_DE_PASSE_PRIV]
```

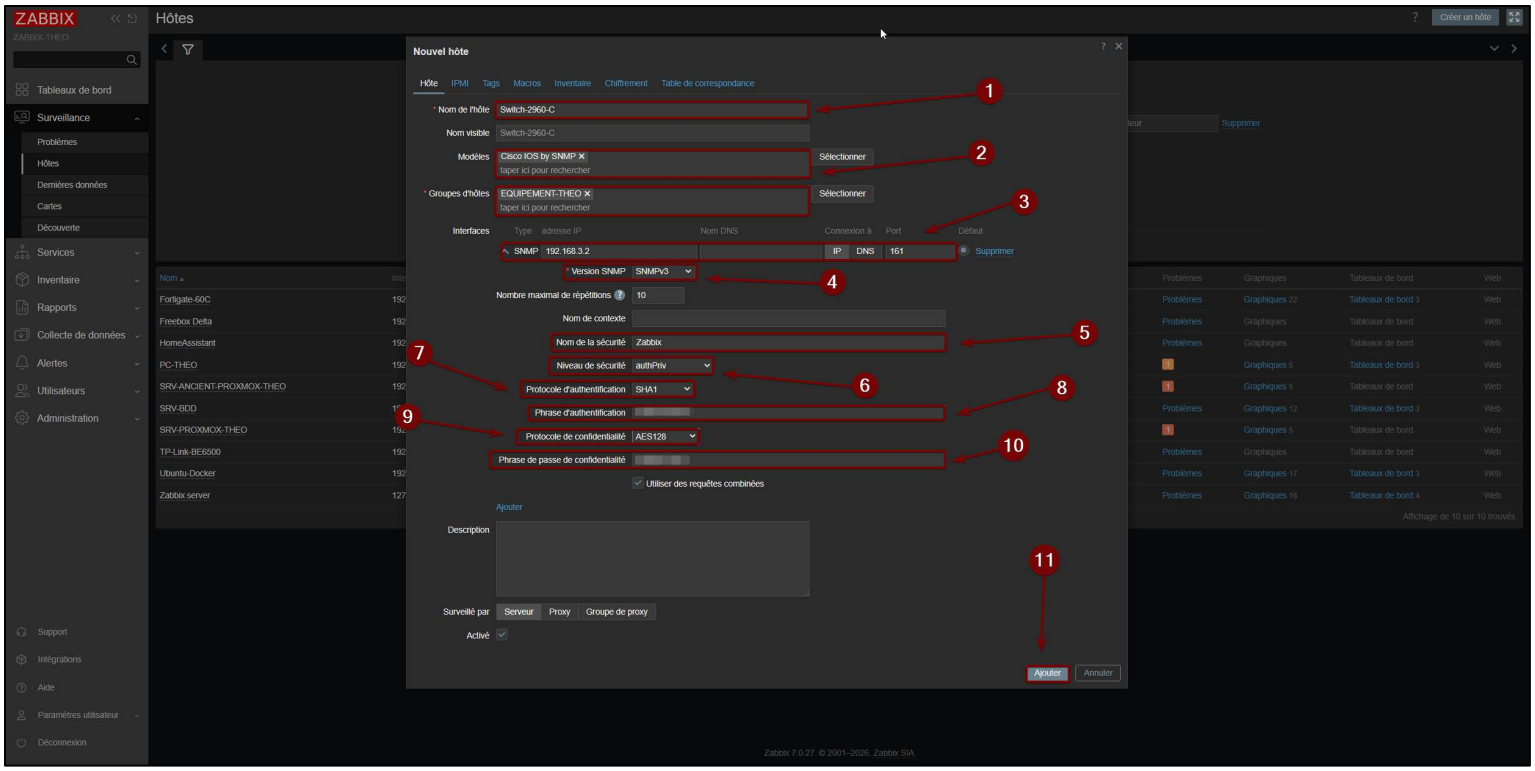
Vérification que notre utilisateur est bien présent :

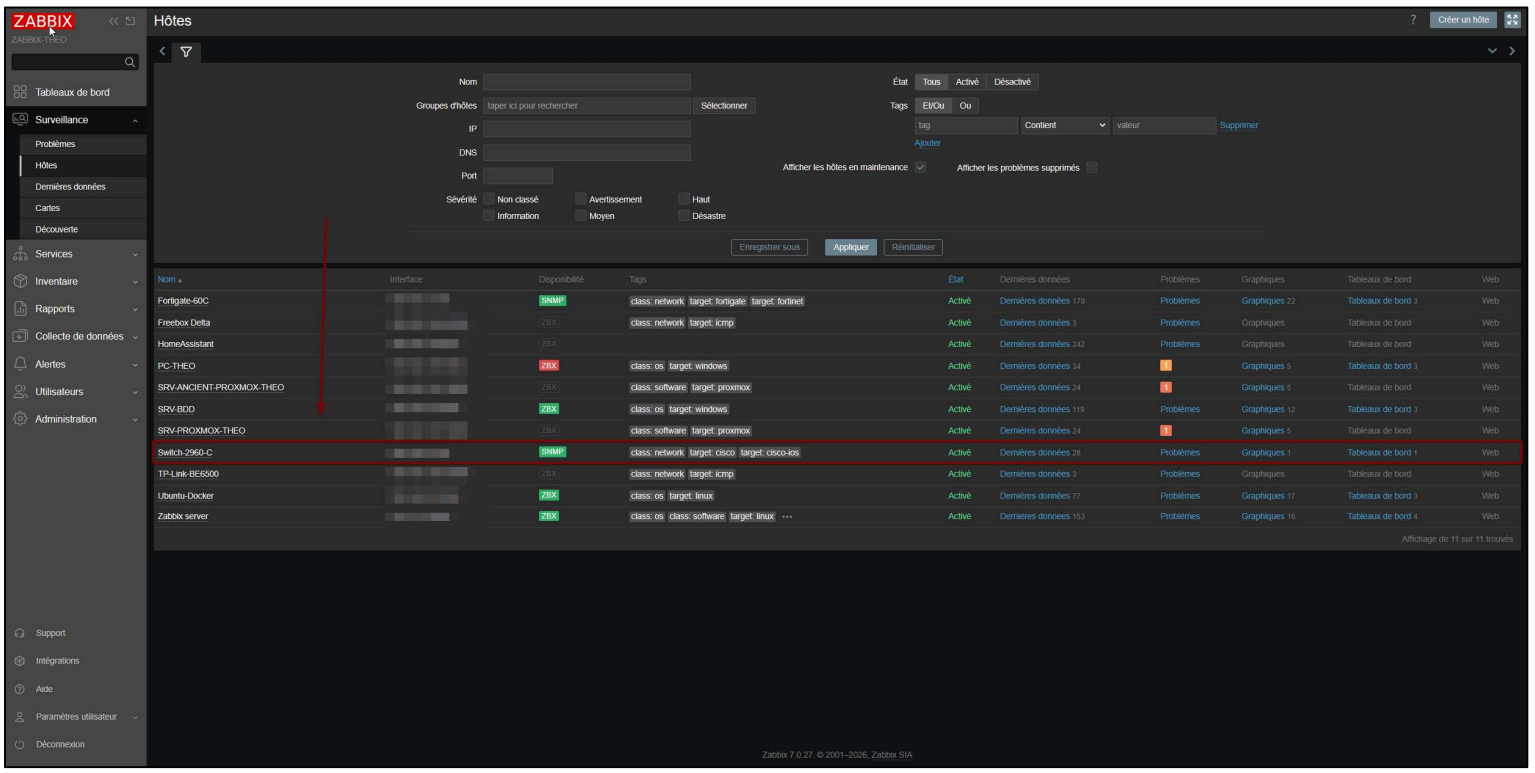
```
SW-HOMELAB_THEO#sh snmp user

User name: Zabbix
Engine ID: 800000090300050F722AC3681
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ZABBIX-GROUP
```

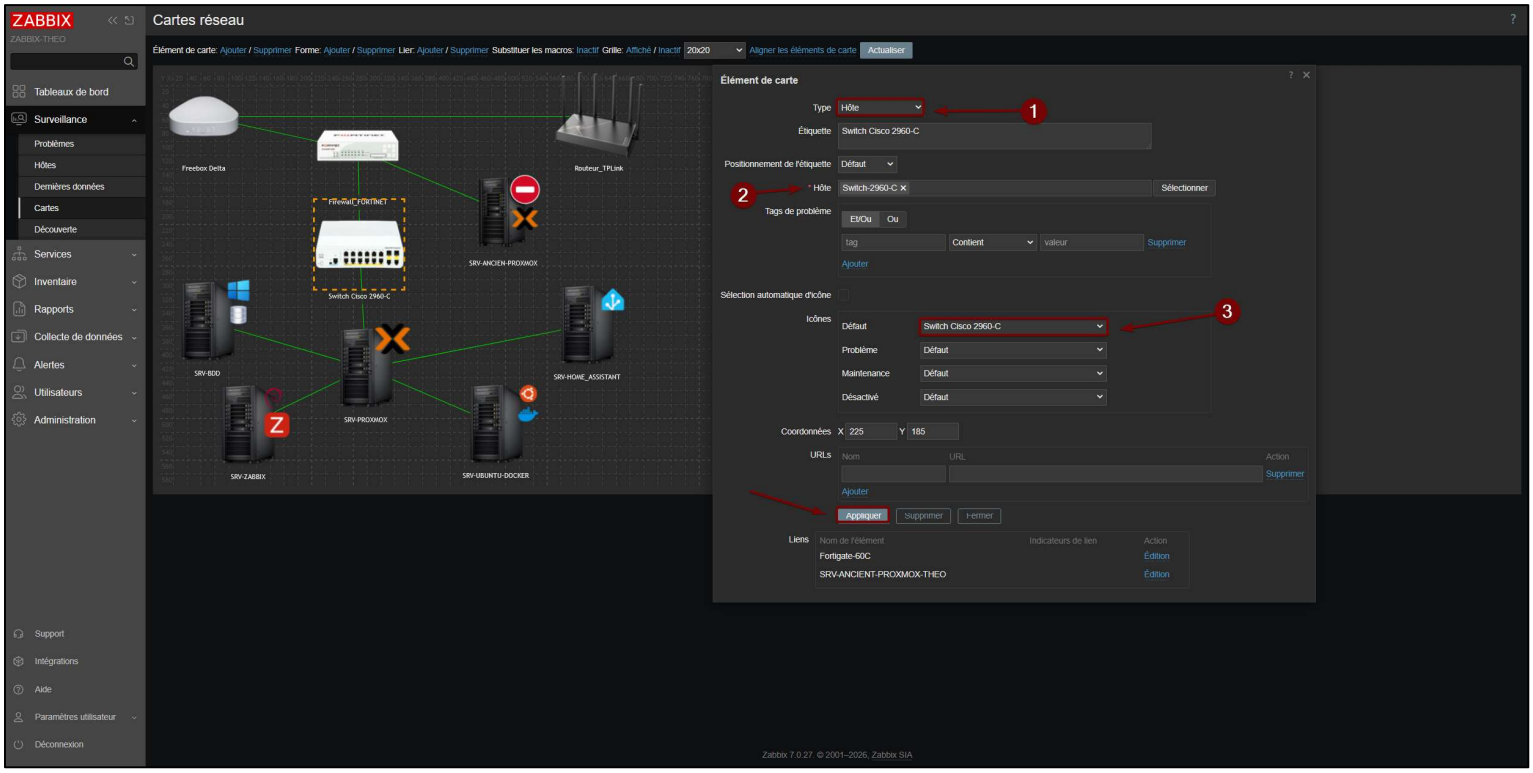
Etape 9 : Ajouter l'équipement à ZABBIX

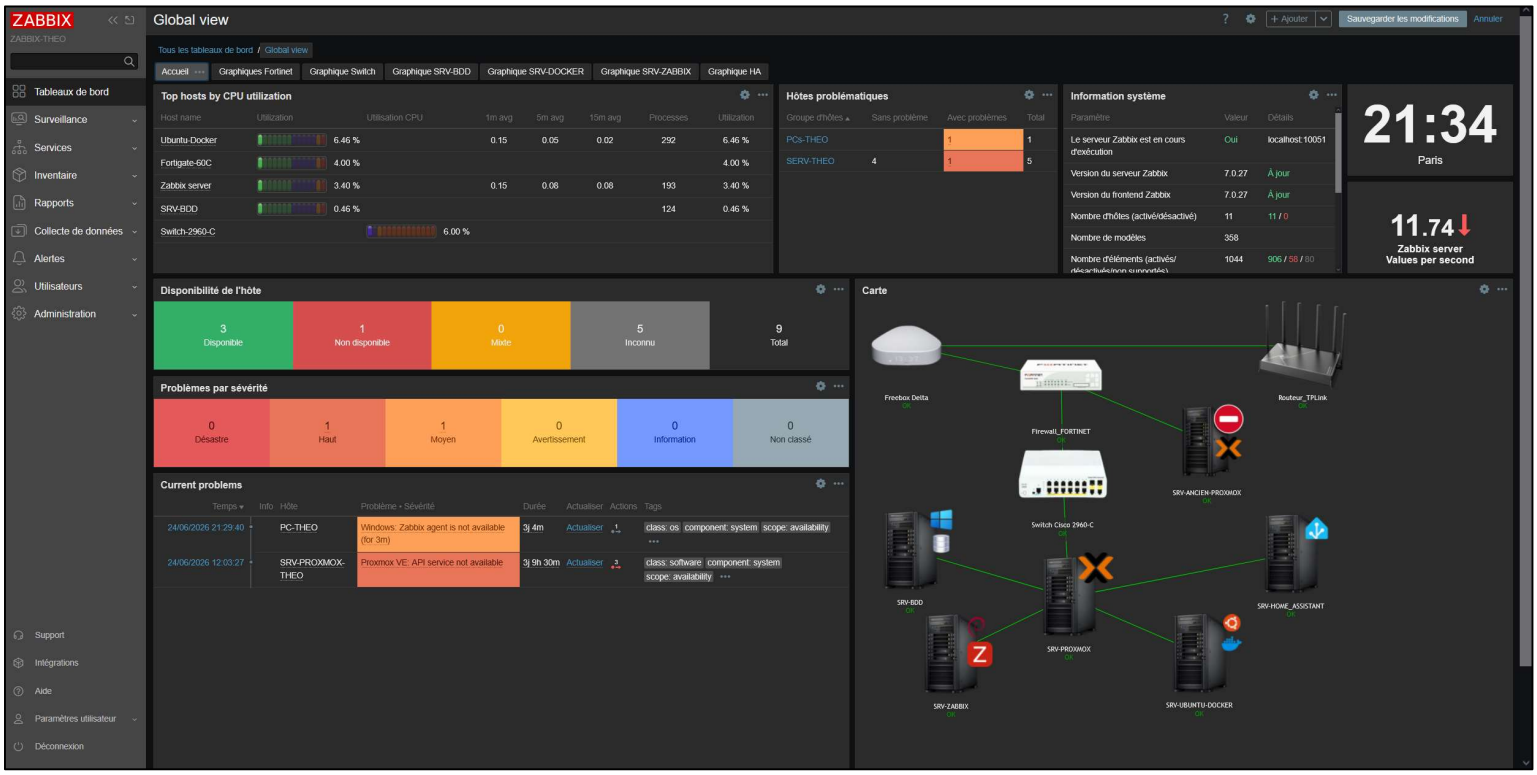



ZABBIX
Hôtes
Nouvel hôte
Hôte
IPMI
Tags
Macros
Inventaire
Chiffrement
Table de correspondance
Nom de l'hôte
Switch-2960-C
Nom visible
Modèles
Cisco IOS by SNMP
Groupes d'hôtes
EQUIPEMENT-THEO
Interfaces
SNMP 192.168.3.2
Version SNMP
SNMPv3
Nombre maximal de répétitions
Nom de contexte
Nom de la sécurité
Zabbix
Niveau de sécurité
authPriv
Protocole d'authentification
SHA1
Phrase d'authentification
Protocole de confidentialité
AES128
Phrase de passe de confidentialité
Utiliser des requêtes combinées
Ajouter
Description
Surveillé par
Serveur
Proxy
Groupe de proxy
Activé
Ajouter
Annuler
1
2
3
4
5
6
7
8
9
10
11


ZABBIX
Hôtes
Créer un hôte
Tableaux de bord
Surveillance
Problèmes
Hôtes
Dernières données
Cartes
Découverte
Services
Inventaire
Rapports
Collecte de données
Alertes
Utilisateurs
Administration
Support
Intégrations
Aide
Paramètres utilisateur
Déconnexion
Nom
Groupes d'hôtes
IP
DNS
Port
Sévérité
État
Tags
Afficher les hôtes en maintenance
Afficher les problèmes supprimés
Enregistrer sous
Appliquer
Réinitialiser
Fortigate-60C
Freebox Delta
HomeAssistant
PC-THEO
SRV-ANCIENT-PROXMOX-THEO
SRV-BDD
SRV-PROXMOX-THEO
Switch-2960-C
TP-Link-BE6500
Ubuntu-Docker
Zabbix server
Affichage de 11 sur 11 trouvés

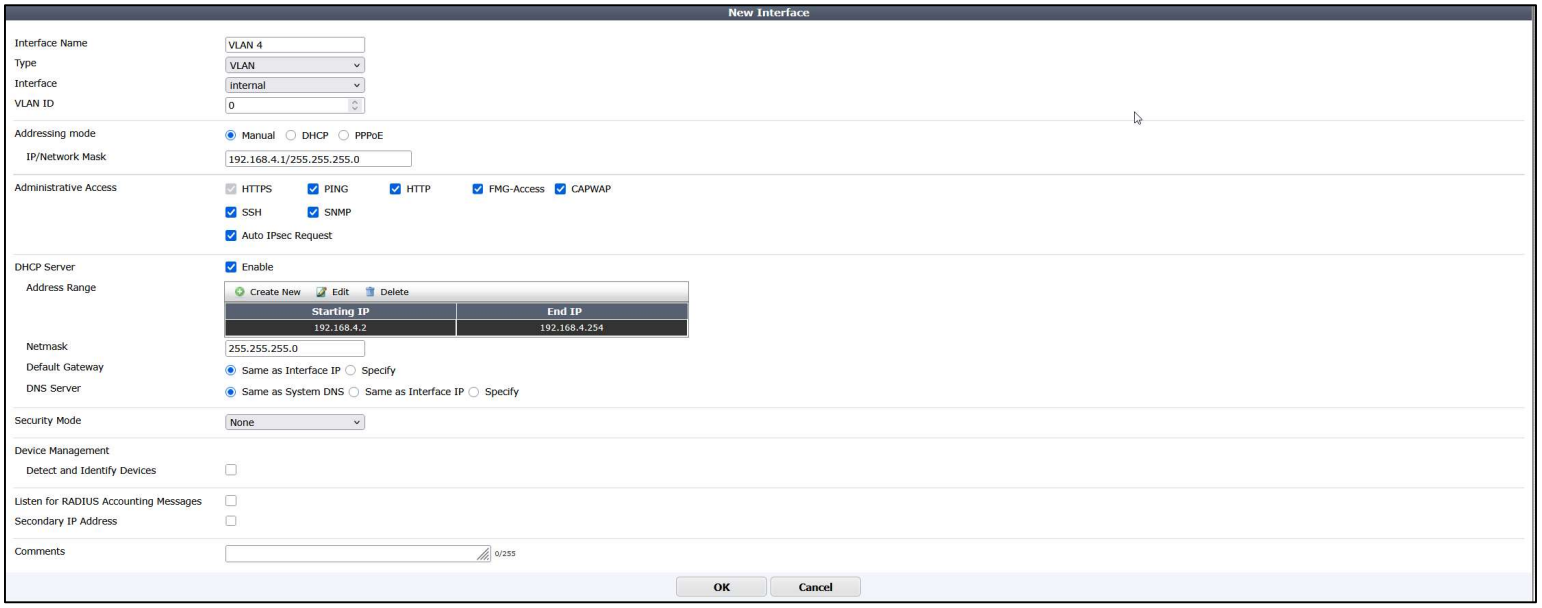
Une fois l'hôte ajouté, on peut le mettre sur la carte :

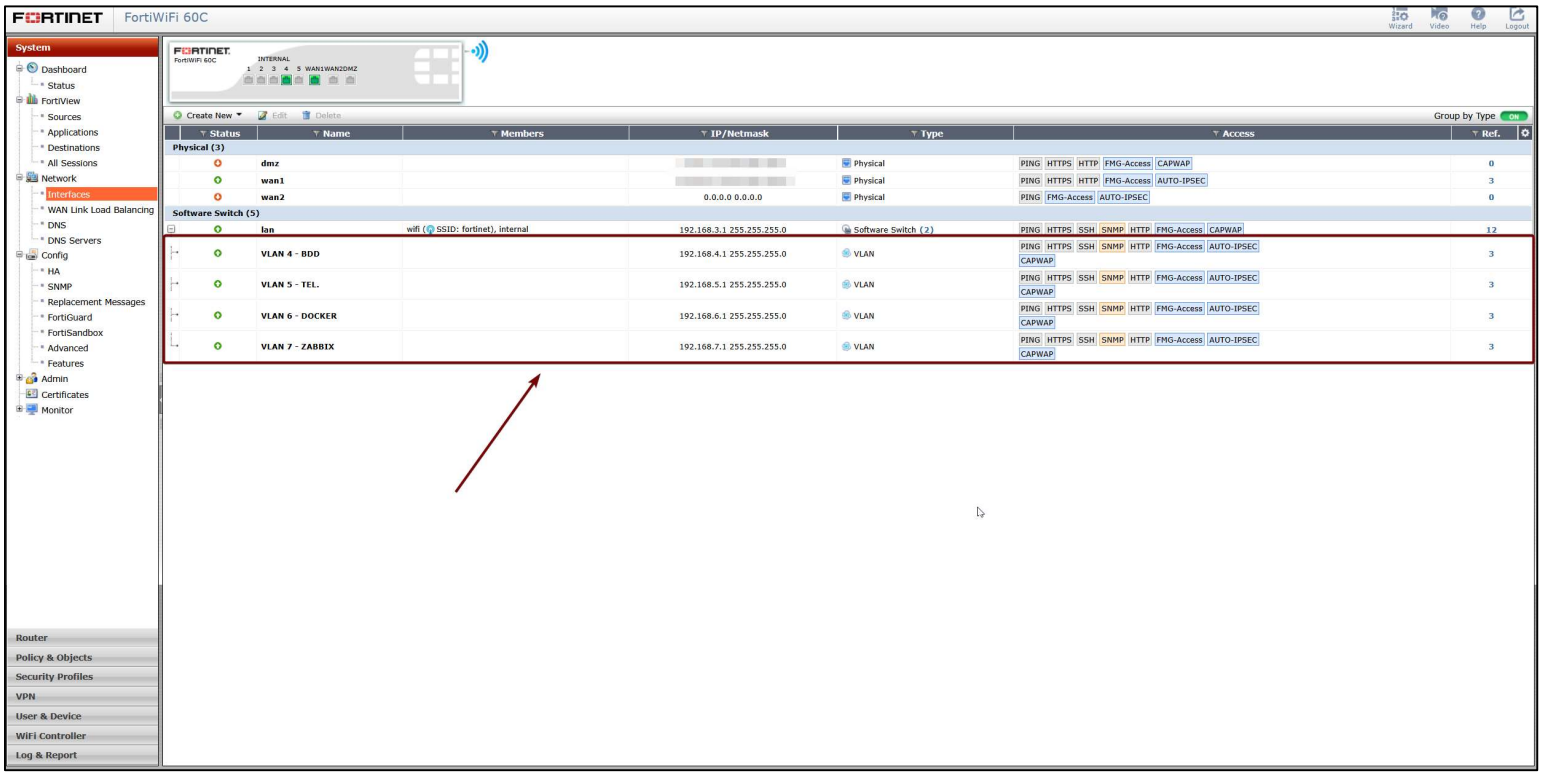




Maintenant que mon switch et liés à ZABBIX, je vais m'occuper des VLANs sur le pare feu :

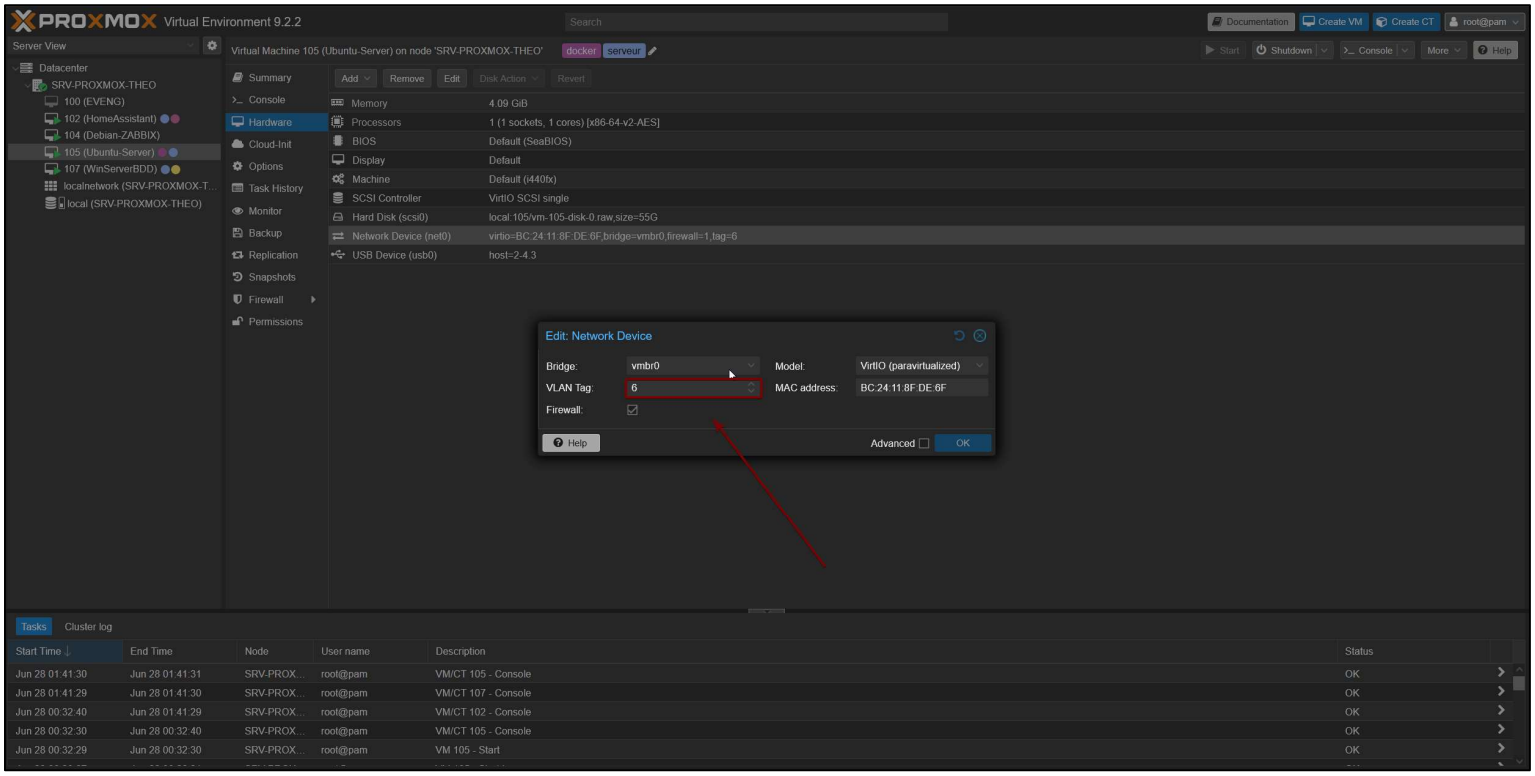
Etape 10 : Créer les VLANs sur le pare-feu

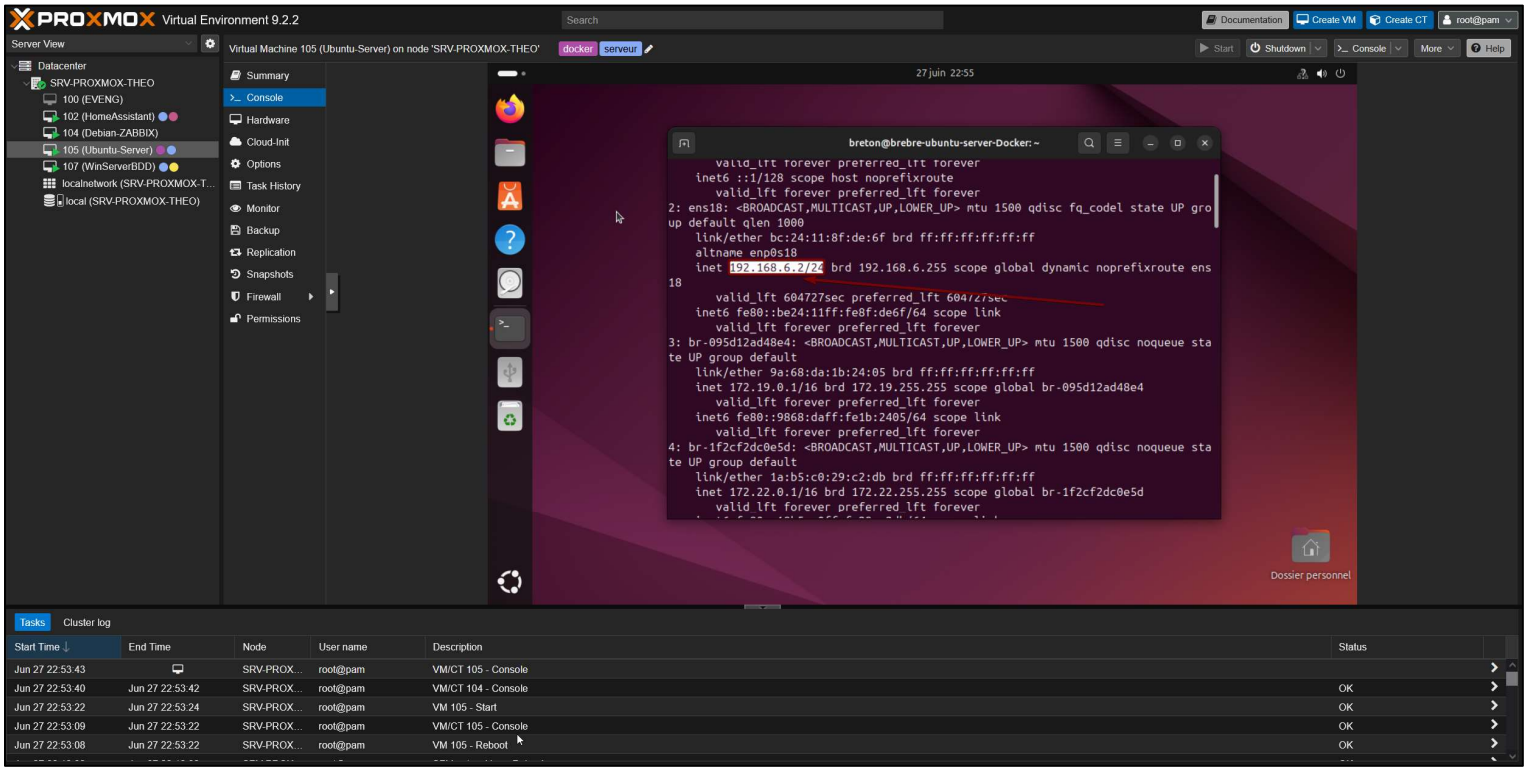




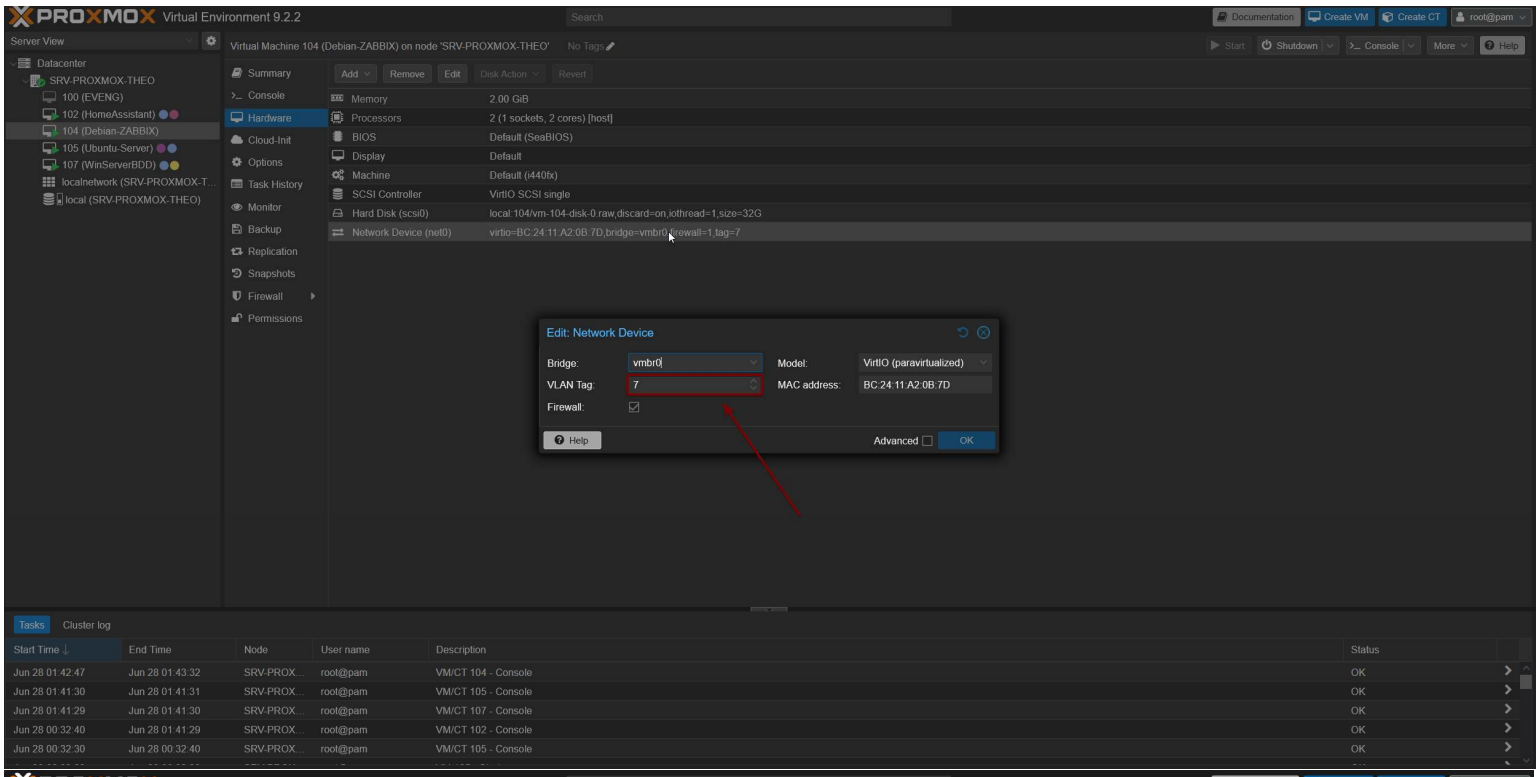
Etape 11 : Basculement des VMs dans les VLANs :

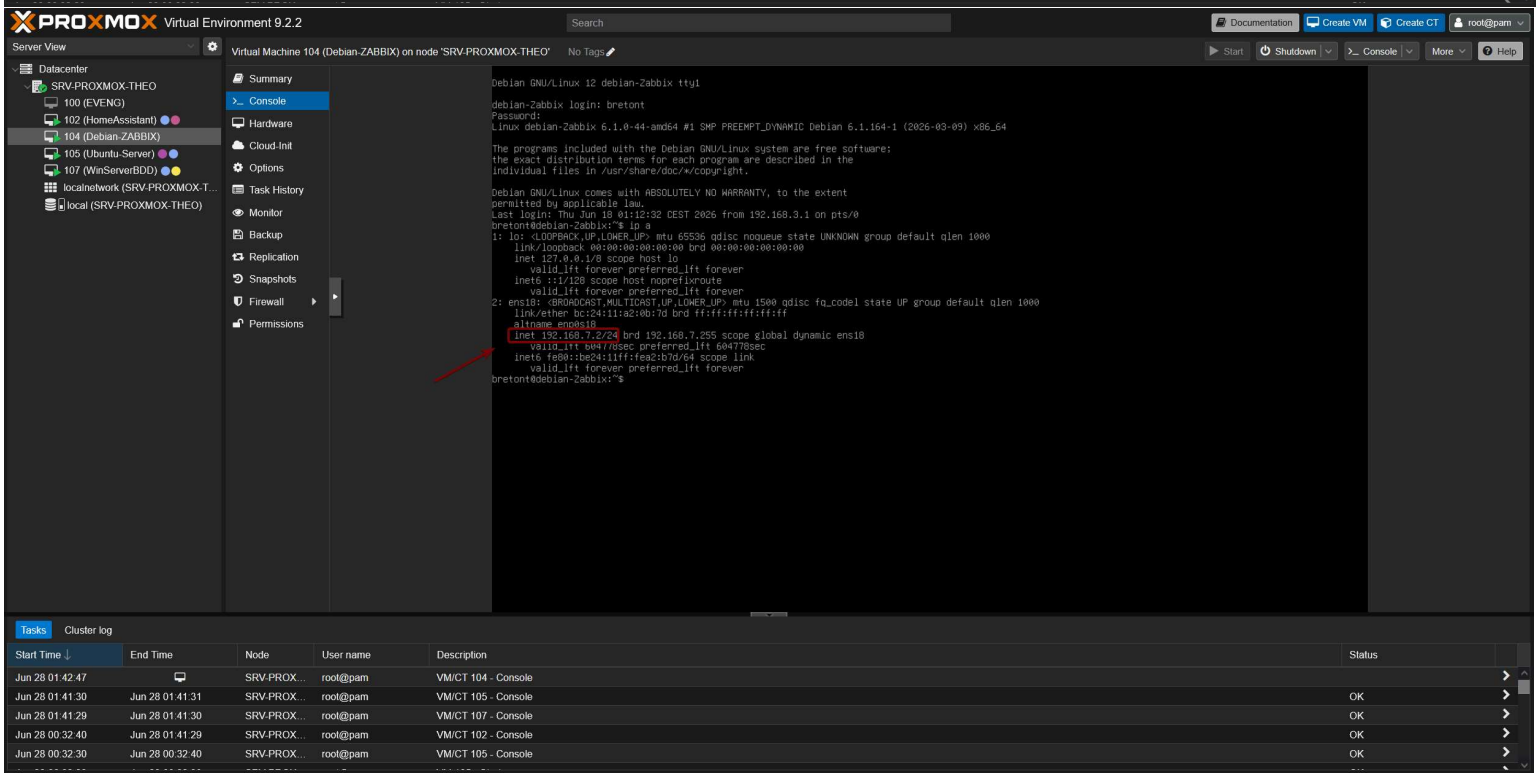
Ubuntu Server – Docker :





Serveur Débian - ZABBIX :

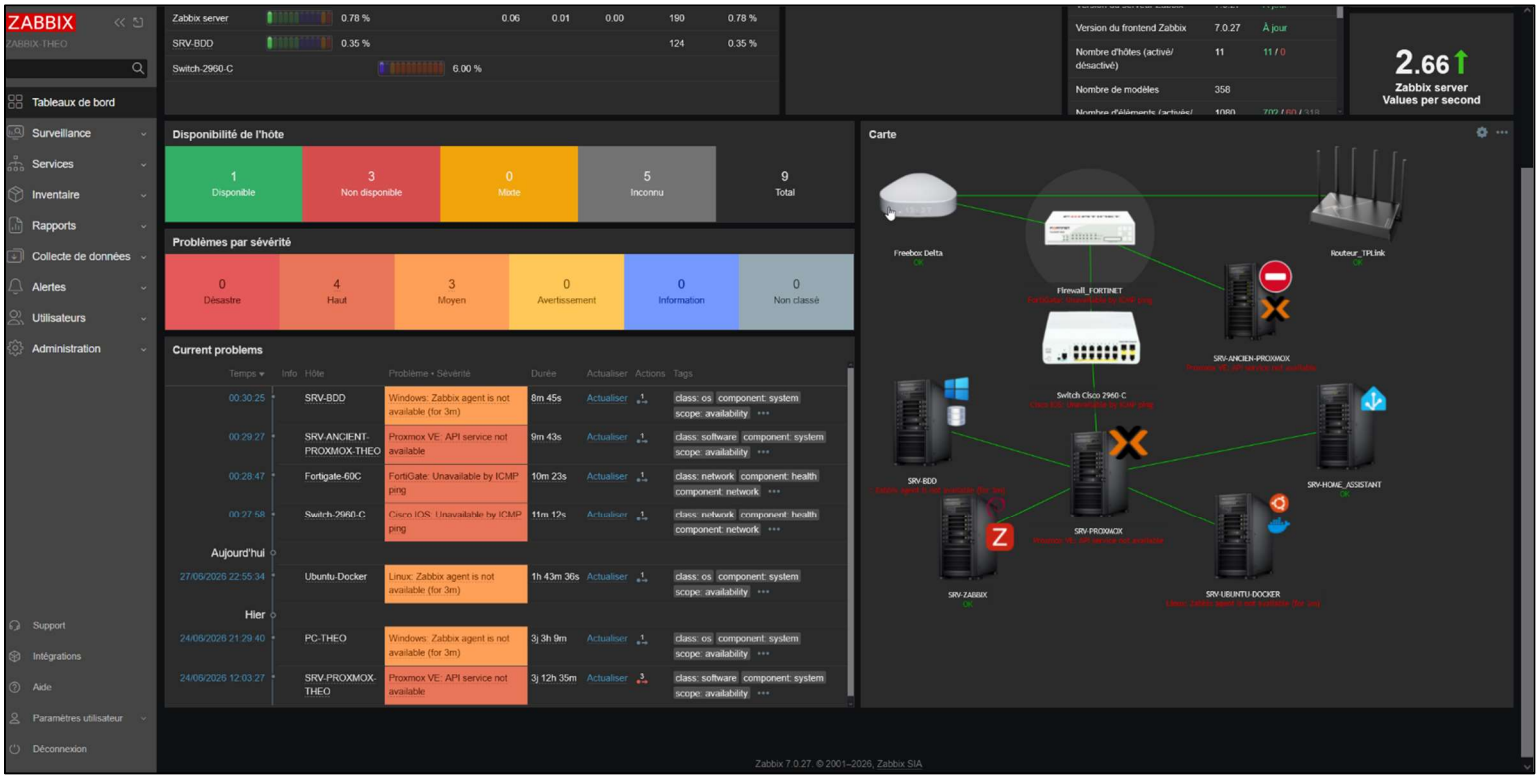




Une fois que l'ensemble des VMs sont passer sur les VLANs le home est totalement casser :

Le serveur de supervision ZABBIX étant totalement isoler dans son VLAN, il ne supervise plus rien du tout.

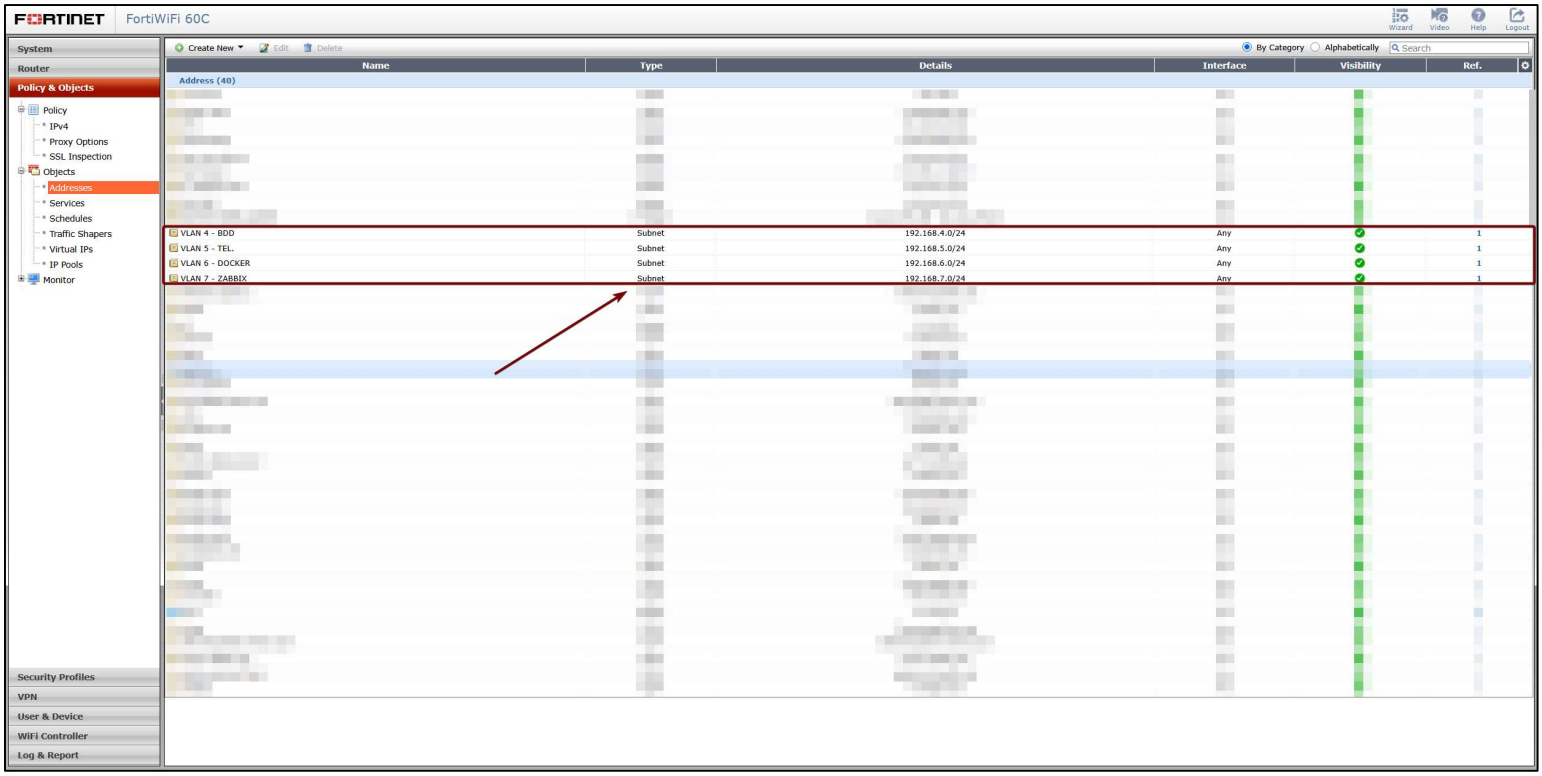
On peut dire que mon Homelab à ce moment la et encore tout cassé !!!!!!



Pour réparer tout sa il faut mettre en place les règle de filtrage.

Etape 12 : Mettre en place les VLANs dans les règles de filtrage

D'abord j'ai créé les objets pour chaque VLAN et leurs @Réseau respective :



1. Le VLAN Zabbix est autorisé à accéder à Internet via le WAN avec NAT activé.
2. Les utilisateurs VPN SSL peuvent accéder au segment LAN principal de l'administration du homelab.
3. Le segment LAN et le VLAN Zabbix peuvent communiquer entre eux.
4. Les utilisateurs FortiClient VPN ont accès à l'ensemble des VLANs du homelab.
5. L'ensemble des VLANs peuvent joindre le segment de supervision Zabbix.
6. Le serveur de supervision peut communiquer avec l'ensemble des VLANs pour collecter les métriques.
7. Des utilisateurs VPN spécifiques ont un accès restreint au serveur de base de données via des protocoles d'administration.
8. Le poste de jeu a accès à la zone démilitarisée.

9. Tout trafic non explicitement autorisé par les règles précédentes est refusé