

Arrivé bouleversante des VLANS dans mon Homelab !!!

Segmentation, Performance & Sécurité



Règles de filtrage FortiGate (Inter-VLAN)

ID	Source	Destination	Service	Action	Commentaire
1	VLAN4 (DB)	VLAN5 (Tel)	SIP/UDP 5060	ALLOW	Autorise appels PBX
2	VLAN5 (Tel)	VLAN4 (DB)	MySQL/TCP 3306	DENY	Bloque accès DB
3	VLAN6 (Docker)	VLAN4 (DB)	ALL	DENY	Isolé
4	VLAN7 (Supervision)	ALL	SNMP/TCP 161	ALLOW	Monitoring
5	VLAN7 (Supervision)	ALL	ICMP	ALLOW	Ping autorisé

Pourquoi les VLANs changent tout :

- ✓ Sécurité renforcée par segmentation
- ✓ Moins de bruit réseau
- ✓ Performance optimisée
- ✓ Contrôle total avec FortiGate

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

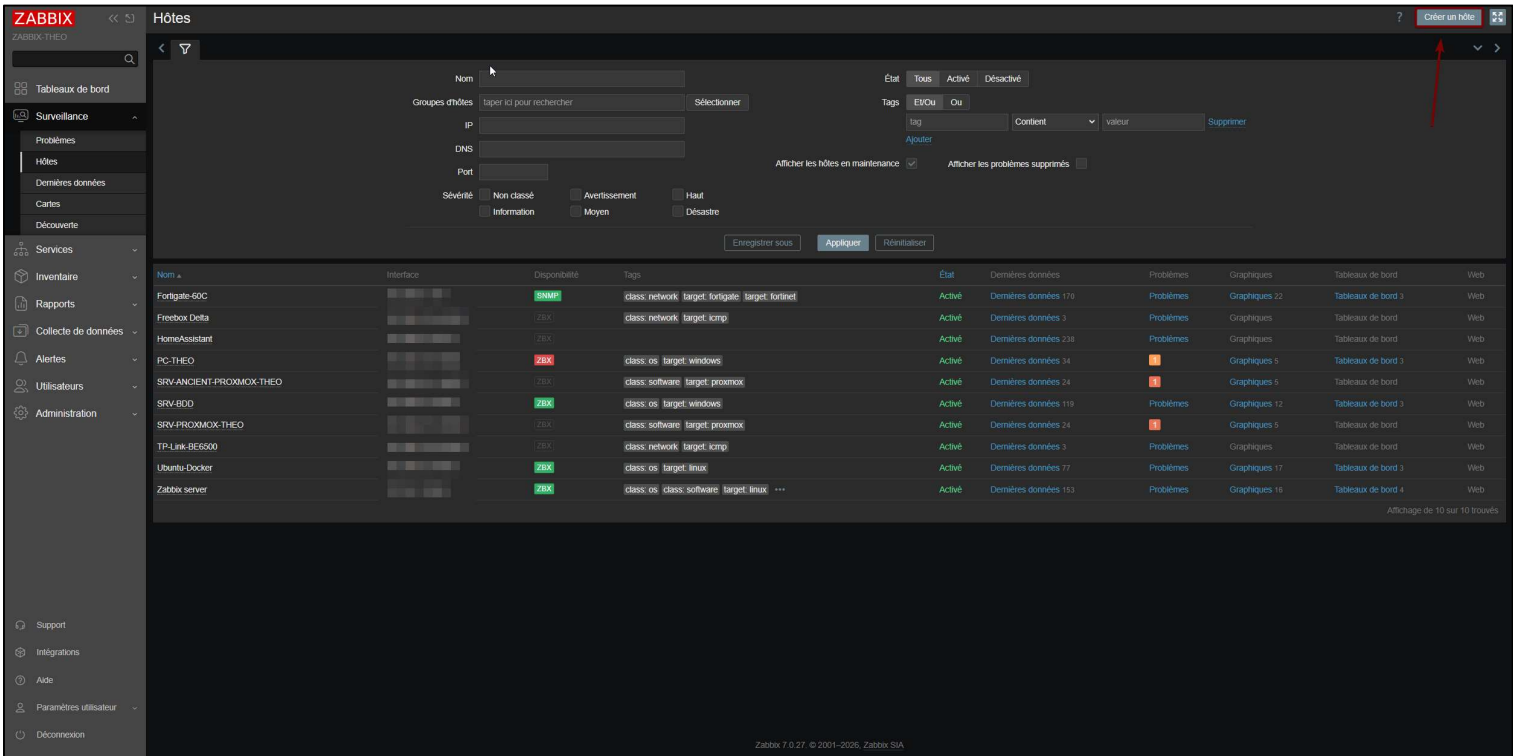
```
Switch(config)#snmp-server group ZABBIX-GROUP v3 priv
Switch(config)#snmp-server user [USER] ZABBIX-GROUP v3 auth sha
[MOT_DE_PASSE_AUTH] priv aes 128 [MOT_DE_PASSE_PRIV]
```

Vérification que notre utilisateur est bien présent :

```
SW-HOMELAB_THEO#sh snmp user

User name: Zabbix
Engine ID: 80000009030050F722AC3681
storage-type: nonvolatile          active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ZABBIX-GROUP
```

Etape 9 : Ajouter l'équipement à ZABBIX



ZABBIX

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

Hôtes

Nouvel hôte

Hôte

IPMI

Tags

Macros

Inventaire

Chiffrement

Table de correspondance

* Nom de l'hôte

Switch-2960-C

Nom visible

Switch-2960-C

Modules

Cisco IOS by SNMP: X

Sélectionner

* Groupes d'hôtes

EQUIPEMENT-THEO X

Sélectionner

Interfaces

SNMP

192.168.3.2

Version SNMP

SNMPv3

Nombre maximal de répétitions

10

Nom de contexte

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

Description

Surveillé par

Serveur

Proxy

Groupe de proxy

Activé

Appliquer

Annuler

Problèmes

Graphiques

Tableaux de bord

Web

Problèmes

Graphiques 22

Tableaux de bord 3

Web

Problèmes

Graphiques

Tableaux de bord

Web

Problèmes

Graphiques 5

Tableaux de bord 3

Web

Problèmes

Graphiques 12

Tableaux de bord 3

Web

Problèmes

Graphiques 5

Tableaux de bord

Web

Problèmes

Graphiques

Tableaux de bord

Web

Problèmes

Graphiques 17

Tableaux de bord 3

Web

Problèmes

Graphiques 16

Tableaux de bord 4

Web

ZABBIX

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

Hôtes

Nom

Groupes d'hôtes

IP

DNS

Port

Sevérité

Non classé

Information

Avertissement

Moyen

Haut

Désastre

État

Tous

Activé

Désactivé

Tags

Et/Ou

Ou

Contient

valeur

Supprimer

Attacher les hôtes en maintenance

Attacher les problèmes supprimés

Enregistrer sous

Appliquer

Réinitialiser

Nom	Interface	Disponibilité	Tags	Etat	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
Fortigate-50C		SNMP	class: network target: fortigate target: fortinet	Activé	Dernières données 170	Problèmes	Graphiques 22	Tableaux de bord 3	Web
Freebox Delta		TEL	class: network target: icmp	Activé	Dernières données 3	Problèmes	Graphiques	Tableaux de bord	Web
HomeAssistant		TEL	class: os target: windows	Activé	Dernières données 242	Problèmes	Graphiques	Tableaux de bord	Web
PC-THEO		TEL	class: os target: windows	Activé	Dernières données 34		Graphiques 5	Tableaux de bord 3	Web
SRV-ANCIENT-PROXMOX-THEO		TEL	class: software target: proxmox	Activé	Dernières données 24		Graphiques 5	Tableaux de bord	Web
SRV-BDD		TEL	class: os target: windows	Activé	Dernières données 119	Problèmes	Graphiques 12	Tableaux de bord 3	Web
SRV-PROXMOX-THEO		TEL	class: software target: proxmox	Activé	Dernières données 24		Graphiques 5	Tableaux de bord	Web
Switch-2960-C		SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 26	Problèmes	Graphiques 1	Tableaux de bord 1	Web
TP-Link-BE6500		TEL	class: network target: icmp	Activé	Dernières données 3	Problèmes	Graphiques	Tableaux de bord	Web
Ubuntu-Docker		TEL	class: os target: linux	Activé	Dernières données 77	Problèmes	Graphiques 17	Tableaux de bord 3	Web
Zabbix server		TEL	class: os class: software target: linux ...	Activé	Dernières données 153	Problèmes	Graphiques 16	Tableaux de bord 4	Web



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

ZABBIX

Global view

Tous les tableaux de bord / Global view

Accueil

Graphiques Fortinet

Graphique Switch

Graphique SRV-BDD

Graphique SRV-DOCKER

Graphique SRV-ZABBIX

Graphique HA

Tableaux de bord

Surveillance

Services

Inventaire

Rapports

Collecte de données

Alertes

Utilisateurs

Administration

Top hosts by CPU utilization

Host name	Utilization	Utilisation CPU	1m avg	5m avg	15m avg	Processes	Utilization
Ubuntu-Docker		6.46 %	0.15	0.05	0.02	292	6.46 %
Fortigate-60C		4.00 %					4.00 %
Zabbix server		3.40 %	0.15	0.08	0.08	193	3.40 %
SRV-BDD		0.46 %				124	0.46 %
Switch-2960-C		6.00 %					

Hôtes problématiques

Groupe d'hôtes	Sans problème	Avec problèmes	Total
PCS-THEO		1	1
SERV-THEO	4	1	5

Information système

Paramètre	Valeur	Détails
Le serveur Zabbix est en cours d'exécution	Oui	localhost:10051
Version du serveur Zabbix	7.0.27	A jour
Version du frontend Zabbix	7.0.27	A jour
Nombre d'hôtes (activé/désactivé)	11	11 / 0
Nombre de modèles	358	
Nombre d'éléments (actifs/désactivés/inconnus ou non envoyés)	1044	906 / 58 / 80

Disponibilité de l'hôte

3 Disponible	1 Non disponible	0 Inhibé	5 Inconnu	9 Total
--------------	------------------	----------	-----------	---------

Problèmes par sévérité

0 Désastre	1 Haut	1 Moyen	0 Avertissement	0 Information	0 Non classé
------------	--------	---------	-----------------	---------------	--------------

Current problems

Temps	Info	Hôte	Problème - Sévérité	Durée	Actualiser	Actions	Tags
24/06/2026 21:29:40		PC-THEO	Windows: Zabbix agent is not available (for 3m)	3 4m	Actualiser	1	class: os component: system scope: availability
24/06/2026 12:03:27		SRV-PROMOX-THEO	Promox VE API service not available	3 9h 30m	Actualiser	2	class: software component: system scope: availability

Carte

Support

Intégrations

Aide

Paramètres utilisateur

Déconnexion

21:34

Paris

11.74 ↓

Zabbix server
Values per second

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

Etape 10 : Créer les VLANs sur le pare-feu

New Interface

Interface Name

VLAN 4

Type

VLAN

Interface

internal

VLAN ID

0

Addressing mode

☒ Manual ☐ DHCP ☐ PPPoE

IP/Network Mask

192.168.4.1/255.255.255.0

Administrative Access

☒ HTTPS ☒ SSH ☒ Auto IPsec Request

☒ PING ☒ SNMP

☒ HTTP ☒ FMG-Access ☒ CAPWAP

DHCP Server

☒ Enable

Address Range

Create New Edit Delete

Starting IP	End IP
192.168.4.2	192.168.4.254

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP ☐ Specify

DNS Server

☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

Security Mode

None

Device Management

Detect and Identify Devices

☐

Listen for RADIUS Accounting Messages

☐

Secondary IP Address

☐

Comments

OK

Cancel

FortiWiFi 60C

System

Dashboard

Status

FortiView

Sources

Applications

Destinations

All Sessions

Network

Interfaces

WAN Link Load Balancing

DNS

DNS Servers

Config

HA

SNMP

Replacement Messages

FortiGuard

FortiSandbox

Advanced

Features

Admin

Certificates

Monitor

Router

Policy & Objects

Security Profiles

VPN

User & Device

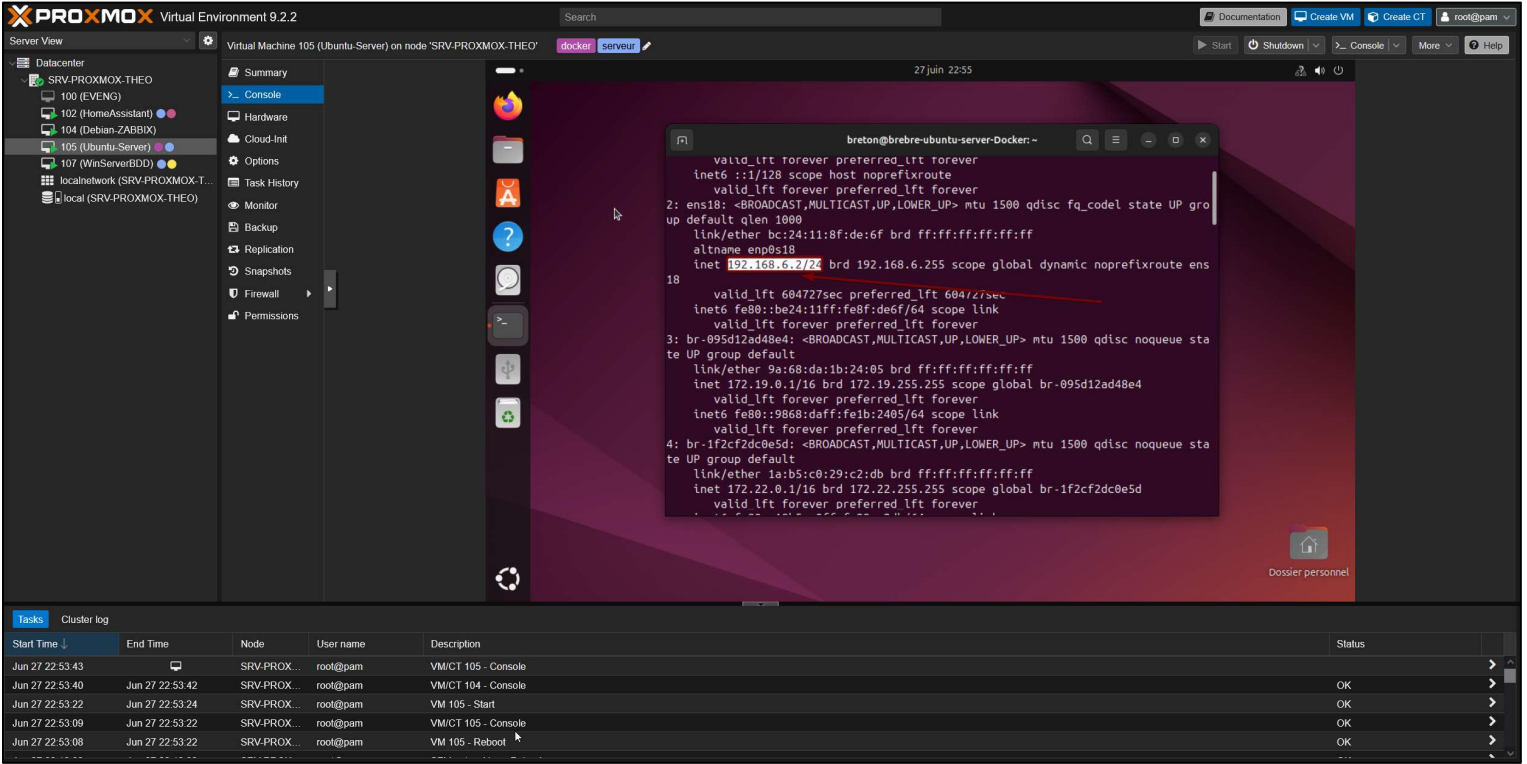
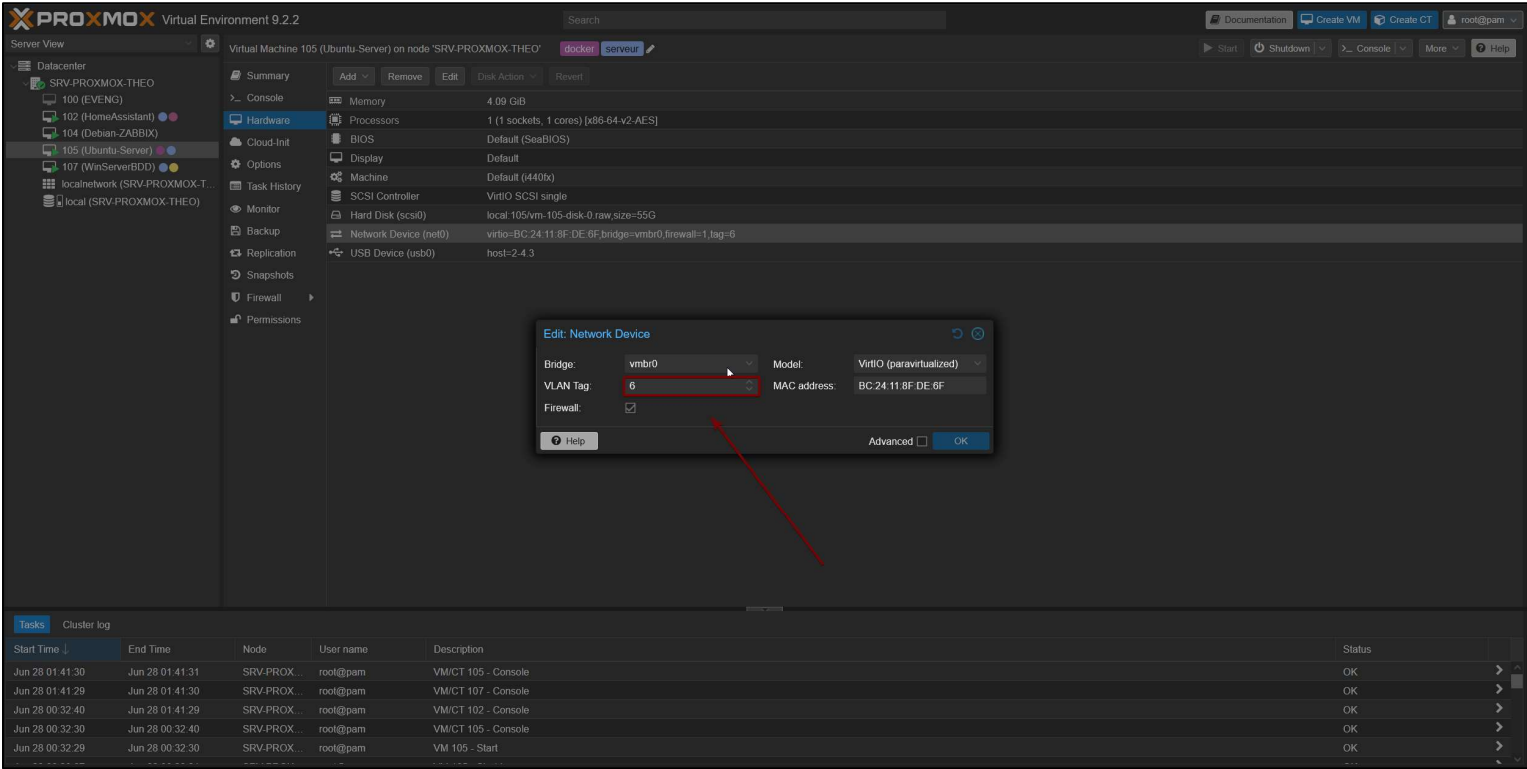
WiFi Controller

Log & Report

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (3)						
	dmz			Physical	PING HTTPS HTTP FMG-Access CAPWAP	0
	wan1			Physical	PING HTTPS HTTP FMG-Access AUTO-IPSEC	3
	wan2		0.0.0.0 0.0.0.0	Physical	PING FMG-Access AUTO-IPSEC	0
Software Switch (5)						
	lan	wifi (SSID: fortinet), internal	192.168.3.1 255.255.255.0	Software Switch (2)	PING HTTPS SSH SNMP HTTP FMG-Access CAPWAP	12
	VLAN 4 - BDD		192.168.4.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP HTTP FMG-Access CAPWAP AUTO-IPSEC	3
	VLAN 5 - TEL.		192.168.5.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP HTTP FMG-Access CAPWAP AUTO-IPSEC	3
	VLAN 6 - DOCKER		192.168.6.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP HTTP FMG-Access CAPWAP AUTO-IPSEC	3
	VLAN 7 - ZABBIX		192.168.7.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP HTTP FMG-Access CAPWAP AUTO-IPSEC	3

Etape 11 : Basculement des VMs dans les VLANs :

Ubuntu Server – Docker :



The screenshot shows the Proxmox VE interface with the 'Edit: Network Device' dialog open. The dialog has the following fields:

- Bridge:** vmbrit (dropdown menu)
- Model:** VirtIO (paravirtualized) (dropdown menu)
- VLAN Tag:** 7 (text input field, highlighted with a red box and a red arrow pointing to it)
- MAC address:** BC:24:11:A2:0B:7D (text input field)
- Firewall:** ☒ (checkbox)
- Buttons:** Help, Advanced ☐, OK

The background shows the 'Hardware' tab of the VM configuration for '104 (Debian-ZABBIX)' on node 'SRV-PROXMOX-THEO'. The network device is listed as 'virtio-BC:24:11:A2:0B:7D,bridge=vmbrit,tag=7'.

PROXMOX Virtual Environment 9.2.2

Search

Documentation Create VM Create CT root@pam

Server View

Datacenter

SRV-PROXMOX-THEO

100 (EVENG)

102 (HomeAssistant)

104 (Debian-ZABBIX)

105 (Ubuntu-Server)

107 (WinServerBDD)

localnetwork (SRV-PROXMOX-THEO)

local (SRV-PROXMOX-THEO)

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

Virtual Machine 104 (Debian-ZABBIX) on node 'SRV-PROXMOX-THEO'

No Tags

Start Shutdown Console More Help

Debian GNU/Linux 12 debian-zabbix tty1

debian-zabbix login: brenton
 Password:
 Linux debian-zabbix 6.1.0-44-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.164-1 (2026-03-09) x86_64

 The programs included with the Debian GNU/Linux system are free software;
 the exact distribution terms for each program are described in the
 individual files in /usr/share/doc/*/copyright.

 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
 permitted by applicable law.
 Last login: Thu Jun 18 01:12:32 CEST 2026 from 192.168.3.1 on pts/0
 brenton@debian-zabbix:~\$ ip a
 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid_lft forever preferred_lft forever
 inet6 ::1/128 scope host noprefixroute
 valid_lft forever preferred_lft forever
 2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether bc:24:11:a2:00:7d brd ff:ff:ff:ff:ff:ff
 allname_ens18
 inet 192.168.7.224/24 brd 192.168.7.255 scope global dynamic ens18
 valid_lft 604770sec preferred_lft 604770sec
 inet6 fe80::be24:11ff:fe24:b7d/64 scope link
 valid_lft forever preferred_lft forever
 brenton@debian-zabbix:~\$

Tasks Cluster log

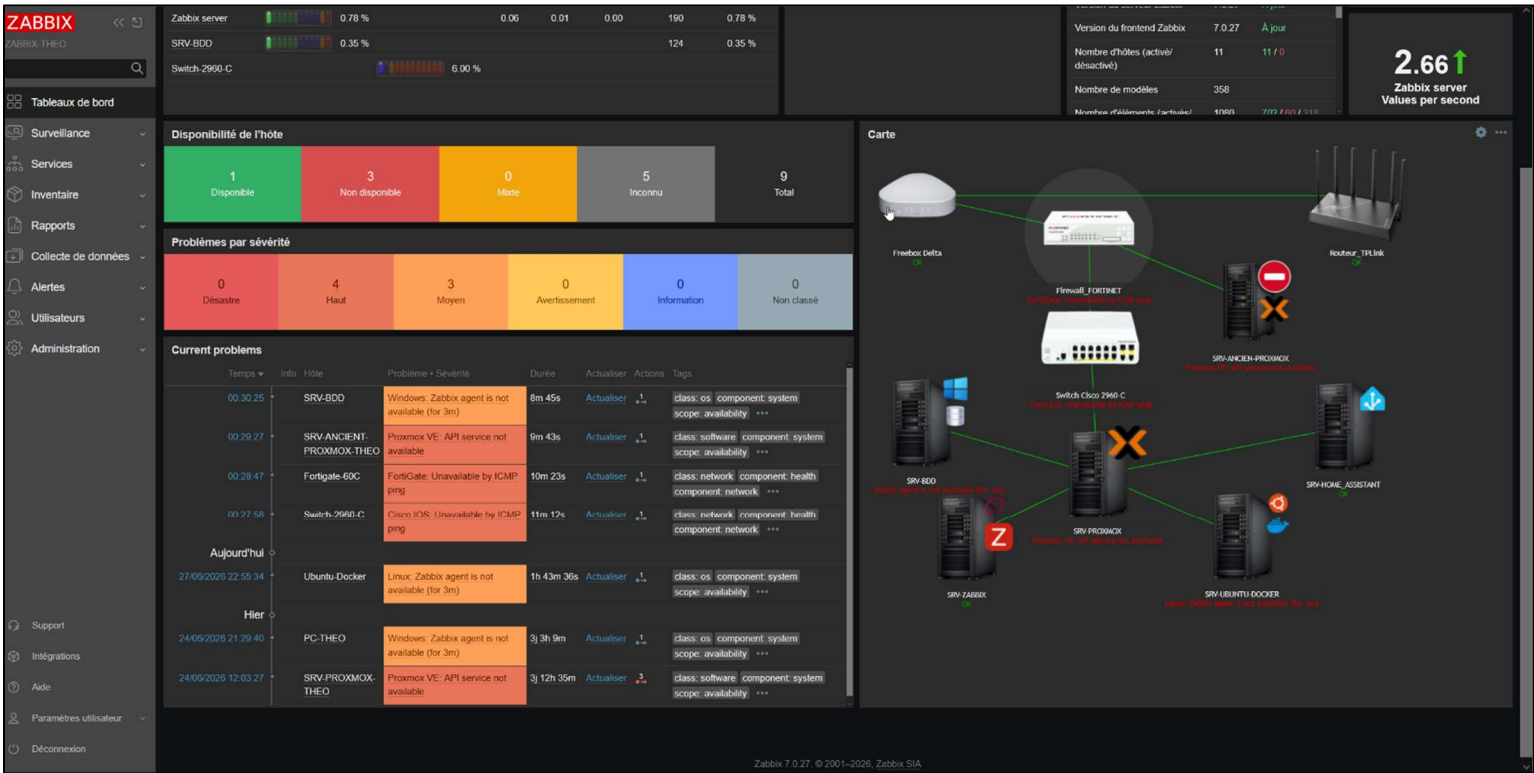
Start Time ↓	End Time	Node	User name	Description	Status
Jun 28 01:42:47		SRV-PROX...	root@pam	VM/CT 104 - Console	
Jun 28 01:41:30	Jun 28 01:41:31	SRV-PROX...	root@pam	VM/CT 105 - Console	OK
Jun 28 01:41:29	Jun 28 01:41:30	SRV-PROX...	root@pam	VM/CT 107 - Console	OK
Jun 28 00:32:40	Jun 28 01:41:29	SRV-PROX...	root@pam	VM/CT 102 - Console	OK
Jun 28 00:32:30	Jun 28 00:32:40	SRV-PROX...	root@pam	VM/CT 105 - Console	OK

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.



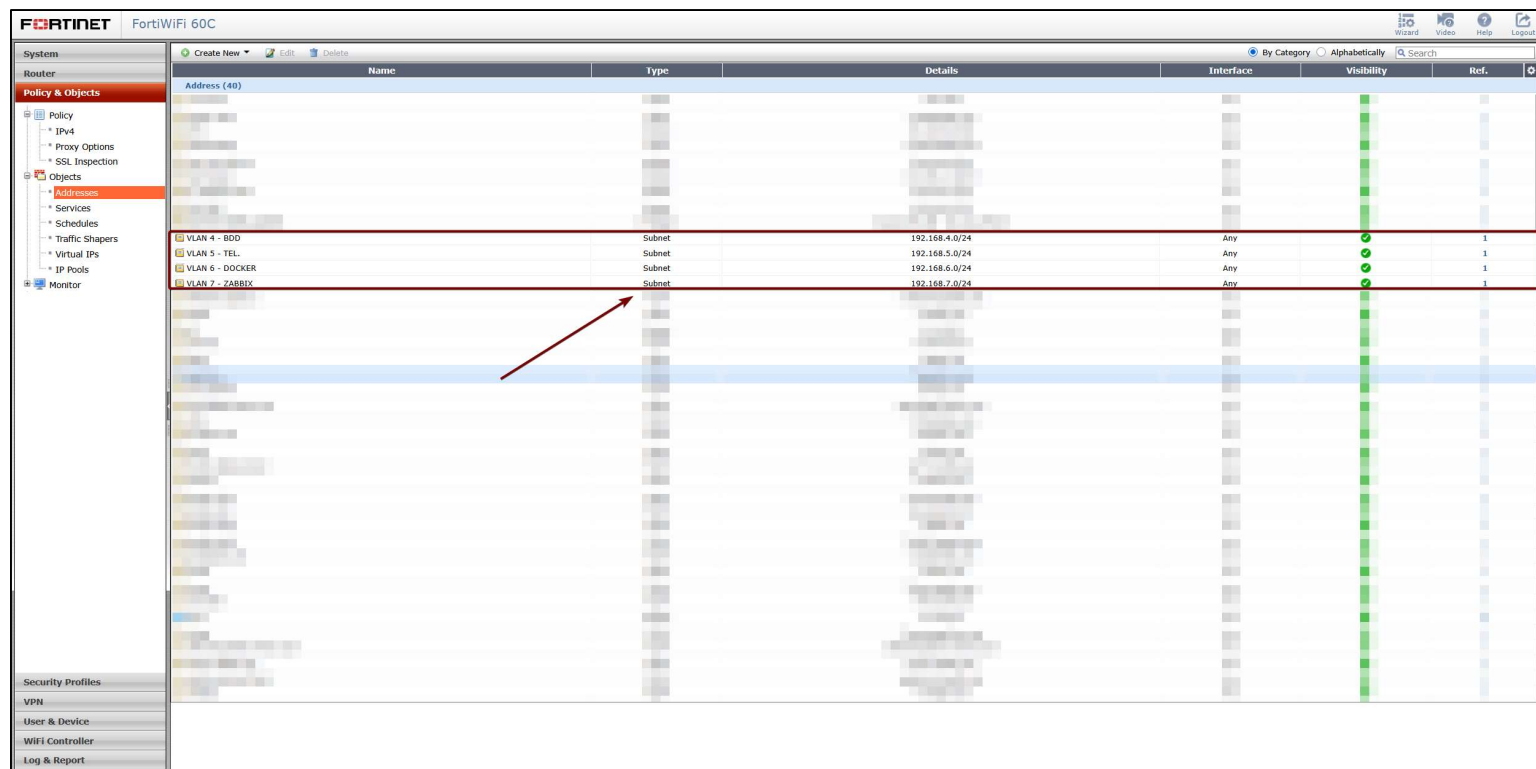
On peut dire que mon Homelab à ce moment la et encore tout cassé !!!!!



Pour réparer tout ça il faut mettre en place les règles 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 :



Name	Type	Details	Interface	Visibility	Ref.
VLAN 4 - BDD	Subnet	192.168.4.0/24	Any	✓	1
VLAN 5 - TEL	Subnet	192.168.5.0/24	Any	✓	1
VLAN 6 - DOCKER	Subnet	192.168.6.0/24	Any	✓	1
VLAN 7 - ZABBIX	Subnet	192.168.7.0/24	Any	✓	1

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