

Mission 13 : Sécurisation d'une Infrastructure (Partie2)

0. Pré-requis

Pour réaliser cette mission, il est nécessaire d'avoir :

- Un routeur x64 avec au moins deux interfaces :

WAN : interface de sortie du réseau
VLAN : interface pour les différents VLAN

- Un serveur
- Un switch
- Un ou deux humain(s)

1. Introduction

L'objectif de cette mission est de renforcer la sécurité de notre infrastructure en passant d'une infrastructure à **2 VLAN** vers une infrastructure à **6 VLAN**.

Les avantages pour une entreprise, d'augmenter son nombre de VLANs sont nombreux :

- Amélioration de la sécurité
- Préparation à l'évolution de l'entreprise
- Meilleure séparation des services et des rôles

2. Infrastructure actuelle et visée

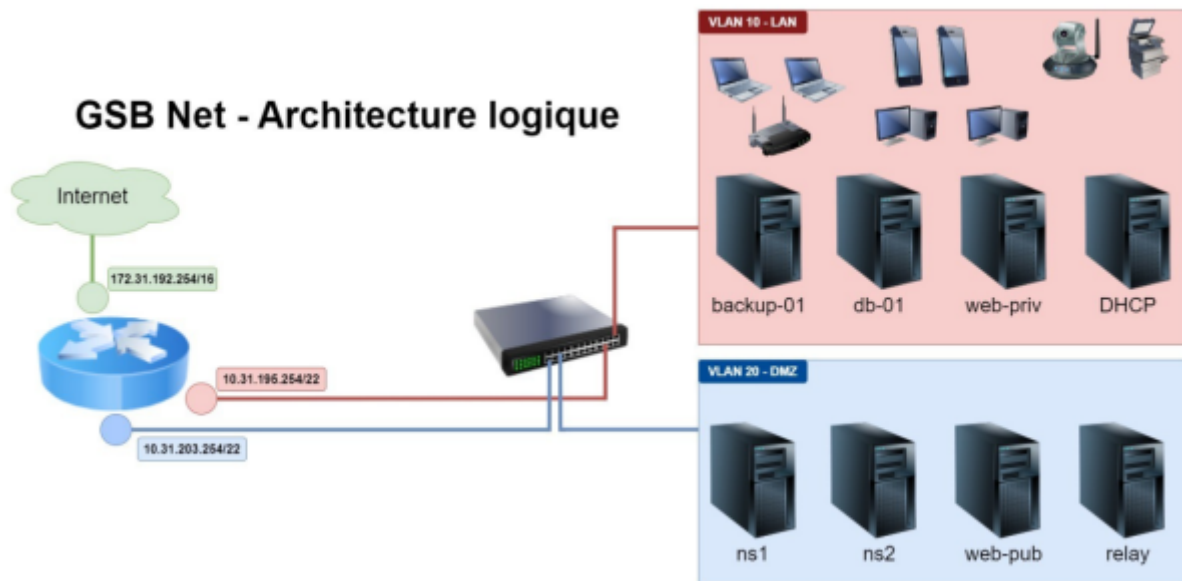
2.1. Infrastructure actuelle

Comme nous nous engageons dans un changement important, il est impératif de réaliser une étude d'impact. Elle nous permettra **d'analyser les conséquences techniques, organisationnelles et fonctionnelles d'un tel changement d'infrastructure.**

Nous n'entrerons pas plus que ça dans les détails car nous avons réalisé un document **"Etuded'impactAdemAmine.pdf"** dans lequel figure une étude d'impact **complète et**

professionnelle de notre mission.

Nous allons commencer par visualiser notre **infrastructure actuelle** :

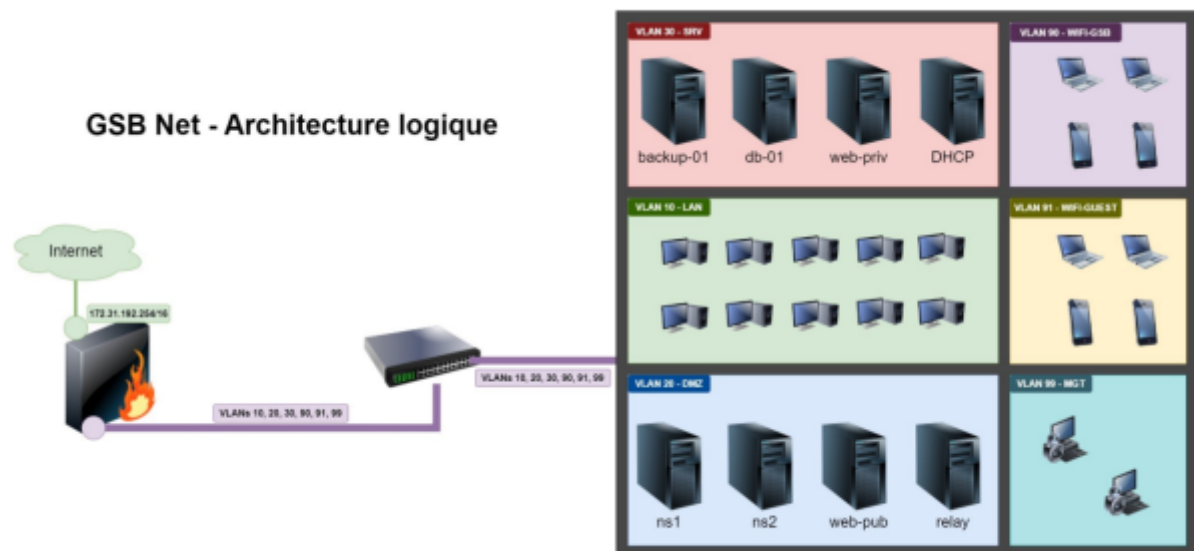


Pour l'instant, nous avons :

- **1 Firewall OPNsense** avec 3 interfaces (WAN, LAN et DMZ)
- 1 switch avec **2 VLAN** (LAN et DMZ)
- 1 Serveur de virtualisation Proxmox avec **2 bridges** (vmbr0 et vmbr1)
- **1 Lien physique par VLAN pour chaque machine** (2 pour le serveur Proxmox et 2 pour le Firewall OPNsense)

2.2. Infrastructure visée

Voici un schéma de l'infrastructure visée :



Nous souhaitons donc passer à :

- **1 Firewall OPNsense**
- 1 switch avec **6 VLAN + 2 liens 802.1q (trunk)**
- 1 serveur de virtualisation Proxmox **avec 6 VLAN**
- 1 Lien physique par machine (**8021q - trunk**)

3. Configuration du switch

3.1 Branchement et accès

Tout d'abord, nous allons configurer **le switch**.

Pour ce faire, on relie **notre switch Cisco** et notre **laptop** (PC de Adem) à l'aide d'un **cable console Cisco (RJ45 -> USB)**.

Ensuite, sur **le laptop** relié au switch, on se rend dans :

Gestionnaire des périphériques ---> Ports (COM et LPT) #Vérification sur quel port est branché le cable console Cisco.

- > Périphériques Universal Serial Bus
- ✓ Ports (COM et LPT)
 - Liens série sur Bluetooth standard (COM3)
 - Liens série sur Bluetooth standard (COM4)
 - USB-SERIAL CH340 (COM6)

On voit bien que notre cable est branché sur **le port USB-SERIAL CH430 (COM6)**

On installe le logiciel PUTTY : <https://www.chiark.greenend.org.uk/~sgtatham/putty/>

Mémo : PuTTY (Switchs utiles)

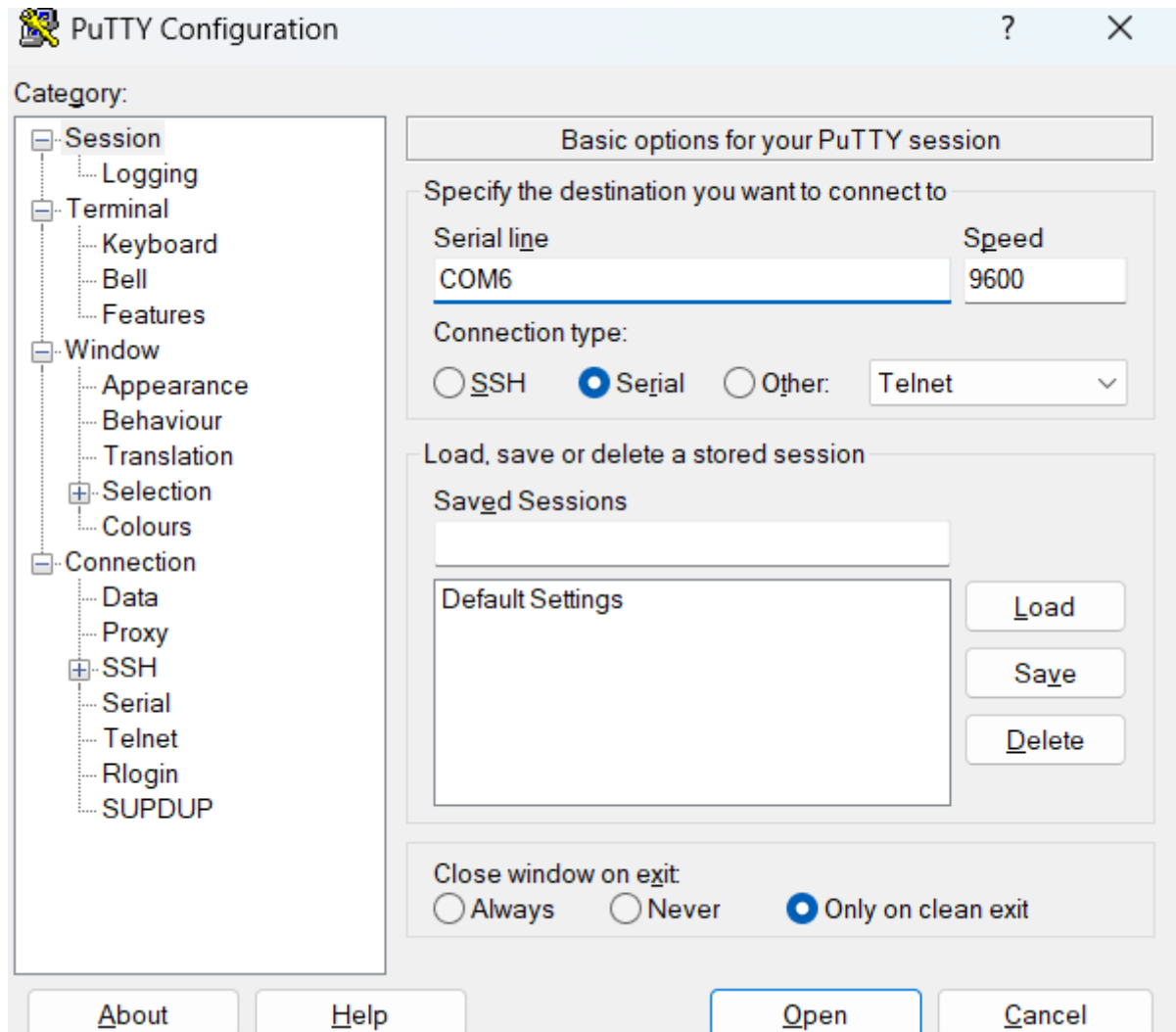
PuTTY peut être lancé en ligne de commande avec différents switchs permettant d'ouvrir rapidement une connexion ou de charger une configuration.

Commandes principales

- **putty -ssh user@hôte** *Ouvre une connexion SSH. *Exemple : **putty -ssh root@192.168.1.10** * **putty -telnet hôte**
 - Ouvre une connexion Telnet.
 - Exemple : **putty -telnet 192.168.1.20**
- **putty -serial COMx** *Ouvre une connexion série. *Exemple : **putty -serial COM3** * **putty -P <port>**
 - Définit le port de connexion.
 - Exemple : **putty -ssh user@hôte -P 2222**
- **putty -i <clé.ppk>** *Utilise une clé privée pour l'authentification. *Exemple : **putty -ssh user@hôte -i ma_cle.ppk** * **putty -load <session>**
 - Charge une session enregistrée.
 - Exemple : **putty -load "ServeurSSH"**

Une fois le logiciel installé, on le lance et se rend dans :

```
Session --> connection type : Serial --> Serial line COM6 --> OPEN
```



3.2 Configuration des VLANS

On passe en mode privilégié et en mode configuration globale :

```
Switch> enable #passage en mode privilégié
Switch# conf t #passer en mode configuration globale
```

> On supprime nos anciens VLAN :

```
Switch(config)# no vlan 10 #supprime le VLAN LAN
Switch(config)# no vlan 20 #supprime le VLAN DMZ
```

On créer nos VLAN un par un :

```
Switch(config)# Vlan 192 #Créer le VLAN 192
Switch(config-vlan)# name LAN #Nommer le VLAN "LAN"
Switch(config-vlan)# exit #Sortir du mode VLAN
```

```
Switch(config)# Vlan 198 #Créer le VLAN 198
Switch(config-vlan)# name LAN #Nommer le VLAN "WIFI-GUEST"
Switch(config-vlan)# exit #Sortir du mode VLAN
```

```
Switch(config)# Vlan 200 #Créer le VLAN 200
Switch(config-vlan)# name LAN #Nommer le VLAN "DMZ"
Switch(config-vlan)# exit #Sortir du mode VLAN
```

```
Switch(config)# Vlan 204 #Créer le VLAN 204
Switch(config-vlan)# name LAN #Nommer le VLAN "SRV"
Switch(config-vlan)# exit #Sortir du mode VLAN
```

```
Switch(config)# Vlan 206 #Créer le VLAN 206
Switch(config-vlan)# name LAN #Nommer le VLAN "MGT"
Switch(config-vlan)# exit #Sortir du mode VLAN
```

3.3 Configuration des port trunk (Proxmox / Switch / OPNsense)

1. CABLE RELIE AU CABLE PROXMOX

On passe en mode privilégié et en mode configuration globale :

```
Switch> enable #mode privilégié
Switch# conf t #mode configuration globale
```

On configure le trunk sur le port relié au serveur Proxmox :

```
Switch(config)# Interface Fa0/1 #Sélectionne le port connecté à proxmox
Switch(config-if)# Switchport trunk encapsulation dot1q #utiliser
l'encapsulation 802.1q pour les VLANs
```

La norme 802.1Q, c'est :

- Un protocole de VLAN (Virtual LAN),
- Qui ajoute un tag dans la trame Ethernet,
- Permettant d'identifier à quel VLAN appartient le trafic,
- Utilisé sur les liens « trunk » entre switches,

```
Switch(config-if)# Switchport mode trunk #définir le port en trunk
Switch(config-if)# Switchport trunk allowed vlan 192,196,198,200,204,206
# Autoriser tous les VLANs
Switch(config-if)# exit #sortir de la configuration de l'interface
```

2. CABLE RELIE AU ROUTEUR OPNSENSE

On passe en mode privilégié et en mode configuration globale :

```
Switch> enable #mode privilégié
Switch# conf t #mode configuration globale
```

On configure le trunk sur le port relié au routeur OPNSENSE :

```
Switch(config)# Interface Fa0/2 #Sélectionne le port connecté à proxmox
Switch(config-if)# Switchport trunk encapsulation dot1q #utiliser
l'encapsulation 802.1q pour les VLANs
Switch(config-if)# Switchport mode trunk #définir le port en trunk
Switch(config-if)# Switchport trunk allowed vlan 192,196,198,200,204,206
# Autoriser tous les VLANs
Switch(config-if)# exit #sortir de la configuration de l'interface
```

4. Configuration du routeur OPNSENSE

4.1 Création des interfaces VLANs

Désormais, pour chaque **VLAN**, nous créeront une **interface VLAN** dans **OPNSENSE**.

On se rend donc dans : **Interfaces -> Devices -> VLAN**

On crée nos VLAN, voici un exemple pour le vlan 192 (LAN) :

The screenshot shows the 'Edit Vlan' configuration window in OPNSENSE. The window has a title bar with 'Edit Vlan' and a close button. Below the title bar, there is a toggle for 'advanced mode' and a 'full help' link. The main content area contains several fields with information icons:

- Device:** A text input field containing 'vlan0.192'. Below it, a note states: 'Leave empty to generate a device name. Custom names are possible, but only if the start of the name matches the required prefix and contains numeric characters or dots, e.g. "vlan0.1.2" or "qinq0.3.4".'
- Parent:** A dropdown menu showing 're1 (64:ee:b7:23:b1:4f)'. Below it, a note states: 'Only VLAN capable interfaces will be shown.'
- VLAN tag:** A text input field containing '192'. Below it, a note states: '802.1Q VLAN tag (between 1 and 4094)'. There is also a small 'i' icon next to the field.
- VLAN priority:** A dropdown menu showing 'Best Effort (0, default)'. Below it, a note states: '802.1Q VLAN PCP (priority code point)'. There is also a small 'i' icon next to the field.
- Description:** A text input field containing 'Interface VLAN 192'. Below it, a note states: 'You may enter a description here for your reference (not parsed)'. There is also a small 'i' icon next to the field.

At the bottom right of the window, there are two buttons: 'Cancel' and 'Save'.

Device —> vlan0.192

Parent —> re1 (64:ee:b7:23:b1:4f) #Interface reliée au switch en trunk

VLAN tag —> 192 #Tag du vlan LAN sur le switch

VLAN priority —> Best Effort (0, default)

Description —> Interface VLAN 192

Maintenant, on se rend dans **Interfaces —> Assignements**

On assigne nos **interfaces** :

+ Assign a new interface

Device	vlan0.192 Interface VLAN 192 (Parent: re1, Tag: 1 ▼)
Description	Interface VLAN 192
Add	

On coche **“enable interface”** pour activer l'interface :

Interfaces: [InterfaceVLAN192]

Basic configuration

i Enable	☐ Enable Interface
i Lock	☐ Prevent interface removal
i Identifier	opt1
i Device	vlan0.192
i Description	InterfaceVLAN192

Save **Cancel**

Puis on configure l'**adresse IPV4 de l'interface vLAN** :

Static IPv4 configuration

i IPv4 address	10.31.195.254	22 ▲
i IPv4 gateway rules	Disabled ▼	

Save **Cancel**

ON FAIS LA MEME CHOSE POUR TOUS LES VLANS

5. Configuration du serveur PROXMOX

5.1 Accès au serveur PROXMOX

Vu le bordel que l'on a foutu en supprimant **nos anciens VLANS, leurs IPS, etc...** , il est évident

que l'on a perdu accès au serveur ProxMox depuis son **interface web**.

Pour récupérer temporairement l'accès à ProxMox sur son interface depuis **notre pc sur le réseau de beaupeyrat**, on va connecté notre pc au switch pour le configurer en ouvrant **le port fa0/12** en **mode access** et en le mettant dans le **vlan 192**.

On fais cela parce qu'en mettant **notre interface sur le mode trunk**, **les paquets circulants dans le vlan LAN sont maintenant tagués** mais notre serveur ProxMox ne s'attend pas à recevoir **des paquets tagués** car on encore rien configuré dessus.

On ouvre donc le port fa0/12 en access :

```
Switch> enable #mode privilégié
Switch# conf t #mode configuration globale
Switch(config)# Interface Fa0/12 #Sélectionne le port fa0/12
Switch(config-if)# Switchport mode access #mettre le port en mode access
Switch(config-if)# Switchport access vlan 192 #attribue le vlan 192 au port fa0/12
Switch(config-if)# exit #sortir de la configuration de l'interface
Switch# write memory #on sauvegarde les modifications
```

5.2 Configuration des VLAN

On a récupéré l'accès au **serveur ProxMox**, on y accède depuis le **pc(réseau beaupeyrat)** toujours branché au **switch** : <https://10.31.192.1:8006>

Pour crée nos **interfaces vlans**, on se rend dans : **Centre de données —> pve-europe —> réseau —> crée —> Linux Vlan**

Éditer: Linux VLAN

Nom:	vlan192	Démarrage automatique:	☒
IPv4/CIDR:	10.31.192.1/22	Périphérique support du VLAN:	vmbr0
Passerelle (IPv4):	10.31.195.254	Étiquette de VLAN:	192
IPv6/CIDR:		Commentaire:	
Passerelle (IPv6):			

Either add the VLAN number to an existing interface name, or choose your own name and set the VLAN raw device (for the latter ifupdown1 supports vlanXY naming only)

MTU: 1500

Avancé ☒ OK

On peut désormais supprimer **notre bridge "vmbr1"** qui nous servait de pont pour **le réseau DMZ**, tous les vlans seront sur le bridge **vmbr0** désormais.

Important

Une machine n'a **qu'une seule passerelle**.

On fait la même chose pour **tous les VLAN**.

5.3 Modification de l'adressage IP des machines virtuelles

Les machines ne sont plus sur les mêmes **VLAN** qu'autrefois, une modification de leur **configuration ip est donc nécessaire**.

Voici un exemple pour le conteneur **priv-db1** qui était anciennement sur **le VLAN LAN (10.31.192.0/22)** et qui se retrouve sur le **VLAN SRV (10.31.204.0/23)** :

Avant :

Éditer: Carte réseau (veth)

Nom: IPv4: ☒ Statique ☐ DHCP

Adresse MAC: IPv4/CIDR:

Pont (bridge): Passerelle (IPv4):

Étiquette de VLAN: IPv6: ☒ Statique ☐ DHCP ☐ SLAAC

Pare-feu: ☒ IPv6/CIDR:

Déconnecter: ☐ Limite de débit (MB/s):

MTU:

☒ Avancé

Ip de la machine → 10.31.192.33/22 #ip sur le réseau LAN

Passerelle → 10.31.195.254 #routeur interface LAN

Pont (bridge) → vmbr0 #pont du réseau LAN

Etiquette de VLAN → aucune #pas encore de VLAN paqueté à gérer

Maintenant :

Éditer: Carte réseau (veth)

Nom:	eth0	IPv4:	☒ Statique ☐ DHCP
Adresse MAC:	BC:24:11:3E:C1:FB	IPv4/CIDR:	10.31.192.33/22
Pont (bridge):	vmbr0	Passerelle (IPv4):	10.31.195.254
Étiquette de VLAN:	aucun VLAN	IPv6:	☒ Statique ☐ DHCP ☐ SLAAC
Pare-feu:	☒	IPv6/CIDR:	Aucun
		Passerelle (IPv6):	
Déconnecter:	☐	Limite de débit (MB/s):	unlimited
MTU:	Identique au pont		

Avancé ☒

Ip de la machine → 10.31.204.33/23 #ip sur le réseau SRV

Passerelle → 10.31.205.254 #routeur interface SRV

Pont (bridge) → vmbr0 #pont des 6 VLAN

Etiquette de VLAN → 204 #étiquette du VLAN SRV

From:

<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-europe:securisationpart2>

Last update: 2025/11/21 07:54

