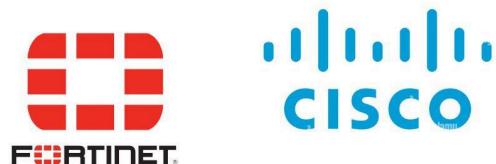


# Rapport de Diagnostic VLAN et Lab FortiGate/Cisco/GNS3



Abdourahamane AbdelWahab

## 1 Contexte du lab

- **Objectif initial** : configurer 3 VLAN (10, 20, 30) sur un switch Cisco relié à un FortiGate fournissant le DHCP pour chaque VLAN.
- **Topologie utilisée :**
  - FortiGate connecté à **SW1 (Cisco L2)**
  - SW1 connecté à 3 switches GNS3 (1 par VLAN)
  - PCs connectés aux switches GNS3
- **Méthode de configuration initiale :**
  - Trunk SW1 ↔ FortiGate pour VLAN 10, 20, 30
  - Ports SW1 ↔ GNS3 configurés en **ACCESS VLAN X**
  - PCs reçoivent automatiquement une IP du VLAN correspondant

## 2 Symptômes observés

- Tout fonctionnait, tous les PCs recevaient une IP.
- Après redémarrage de GNS3 VM :
  - Les PC sur VLAN 10 ne reçoivent plus d'IP
  - Les PC sur VLAN 20 et 30 également tombent après investigation
- **show interfaces trunk** sur SW1 ne montre que Et0/0 (trunk vers FortiGate)  
→ ports vers switches GNS3 n'étaient pas en trunk

## **3 Analyse détaillée du problème**

### **3.1 Ce qui a été fait**

- Chaque switch GNS3 = 1 VLAN
- Port SW1 → GNS3 = ACCESS VLAN X
- Trunk SW1 → FortiGate = VLAN 10, 20, 30

### **3.2 Pourquoi ça a fonctionné avant**

- Les switches GNS3 sont des **bridges logiciels limités**
- Forwardaient parfois les trames VLAN non taguées
- DHCP passait “par chance”
- Lab “tolérant” mais non conforme aux standards L2

### **3.3 Pourquoi ça ne marche plus après redémarrage**

- Comportement des GNS3 Ethernet Switch changé (après reboot)
- Trames VLAN non taguées ne passent plus
- DHCP ne traverse plus le switch GNS3
- Cisco applique strictement 802.1Q → ACCESS ne transporte pas de VLAN vers un autre switch

## 4 Diagnostic technique

Élément	Observation	Statut
Trunk SW1 ↔ FortiGate	VLAN 10, 20, 30 actif	✓ OK
Ports SW1 ↔ GNS3	ACCESS VLAN X	✗ Problématique
VLAN 10 sur SW1	Actif	✓ OK
VLAN 10 sur GNS3	Limité / pas configurable	✗ Non fiable
DHCP VLAN 10	Ne traverse pas	✗ Bloqué

### Cause principale :

Le lien SW1 → switch GNS3 est en **ACCESS** au lieu de **TRUNK**, empêchant le trafic VLAN de passer.

## 5 Bonne pratique (leçon apprise)

### 5.1 Sur les VLAN et L2

- **Un lien entre switches doit toujours être en TRUNK si des VLAN doivent passer**
- Les ports ACCESS ne sont réservés qu'aux hôtes finaux (PC, serveur)
- VLAN sur un switch = segmentation logique, pas physique
- Les VLAN fonctionnant par chance sur un lab GNS3 ne représentent pas une architecture pro

### 5.2 Sur les labs GNS3

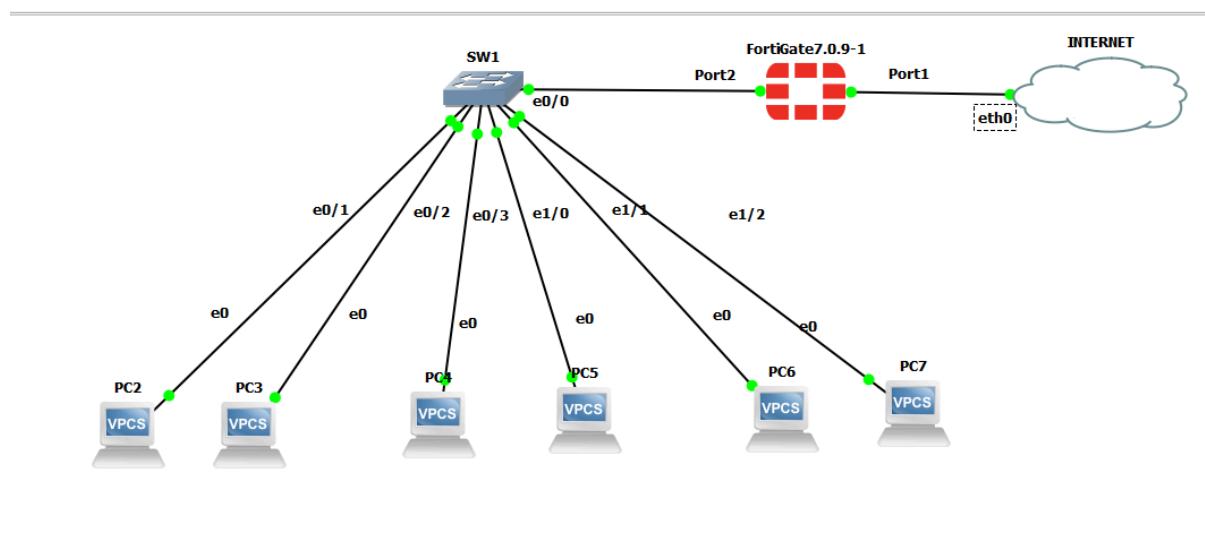
- Switch Ethernet GNS3 **n'est pas un vrai switch L2**
- Impossible de configurer VLAN, STP ou CDP de façon réaliste
- Les comportements observés peuvent tromper

### 5.3 Bonnes pratiques en milieu professionnel

- **1 switch physique** → plusieurs VLAN, ports configurés ACCESS ou TRUNK selon besoin
- Les liens inter-switch → TRUNK avec VLAN autorisés
- DHCP → serveur central ou relay sur switch L3
- Flexibilité : un PC peut changer de VLAN sans déplacer de câble
- Scalabilité : moins de matériel, meilleure gestion

### 5.4 Topologie pro recommandée

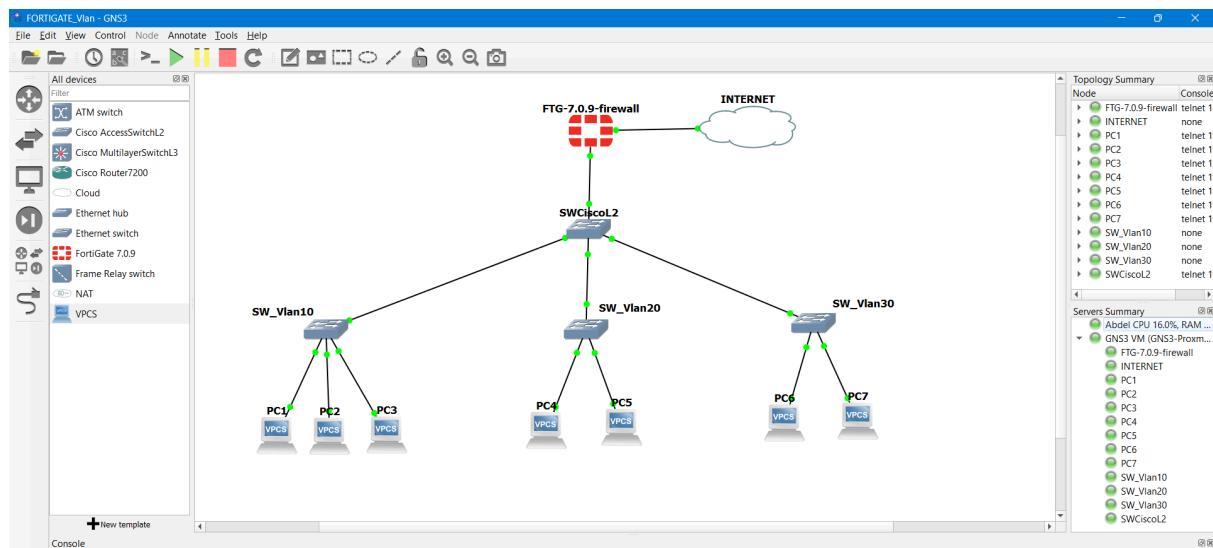
Lier les PCs directement au switch cisco puis configurer en mode access avec le VLAN associé à cette interface vers les PC.



Opter pour une topologie 2/3 ou 3/3, c'est dans ses topologies qu'on va évoluer pour la partie 2...

## 6 Résolution technique pour lab

Pour résoudre le problème avec notre architecture présent



- Mettre les liaison Ports **SWCiscoL2** → Switch GNS3 en mode TRUNK
- Ports sur GNS3 vers PC = ACCESS VLAN correspondant

```
conf t
interface Et0/1
switchport mode trunk
switchport trunk allowed vlan 10
no shutdown
exit

interface Et0/2
switchport mode trunk
switchport trunk allowed vlan 10
no shutdown
exit

interface Et0/3
switchport mode trunk
switchport trunk allowed vlan 10
no shutdown
exit
```

Switch central – **SWCiscoL2**

Abdourahamane AbdelWahab

Port SWCiscoL2	Mode	VLAN autorisés	Connecté à
Et0/0	Trunk	10,20,30	FortiGate port2
Et0/1	Trunk	10	SW_Vlan10
Et0/2	Trunk	20	SW_Vlan20
Et0/3	Trunk	30	SW_Vlan30

### Switch d'accès VLAN 10 – SW\_Vlan10

Port SW_Vlan10	Mode	VLAN	Connecté à
Et0	Trunk	10	SWCiscoL2 Et0/1
Et1	Access	10	PC1
Et2	Access	10	PC2
Et3	Access	10	PC3

### Switch d'accès VLAN 20 – SW\_Vlan20

Port SW_Vlan10	Mode	VLAN	Connecté à
Et0	Trunk	20	SWCiscoL2 Et0/2
Et1	Access	20	PC4
Et2	Access	20	PC5

### Switch d'accès VLAN 30 – SW\_Vlan30

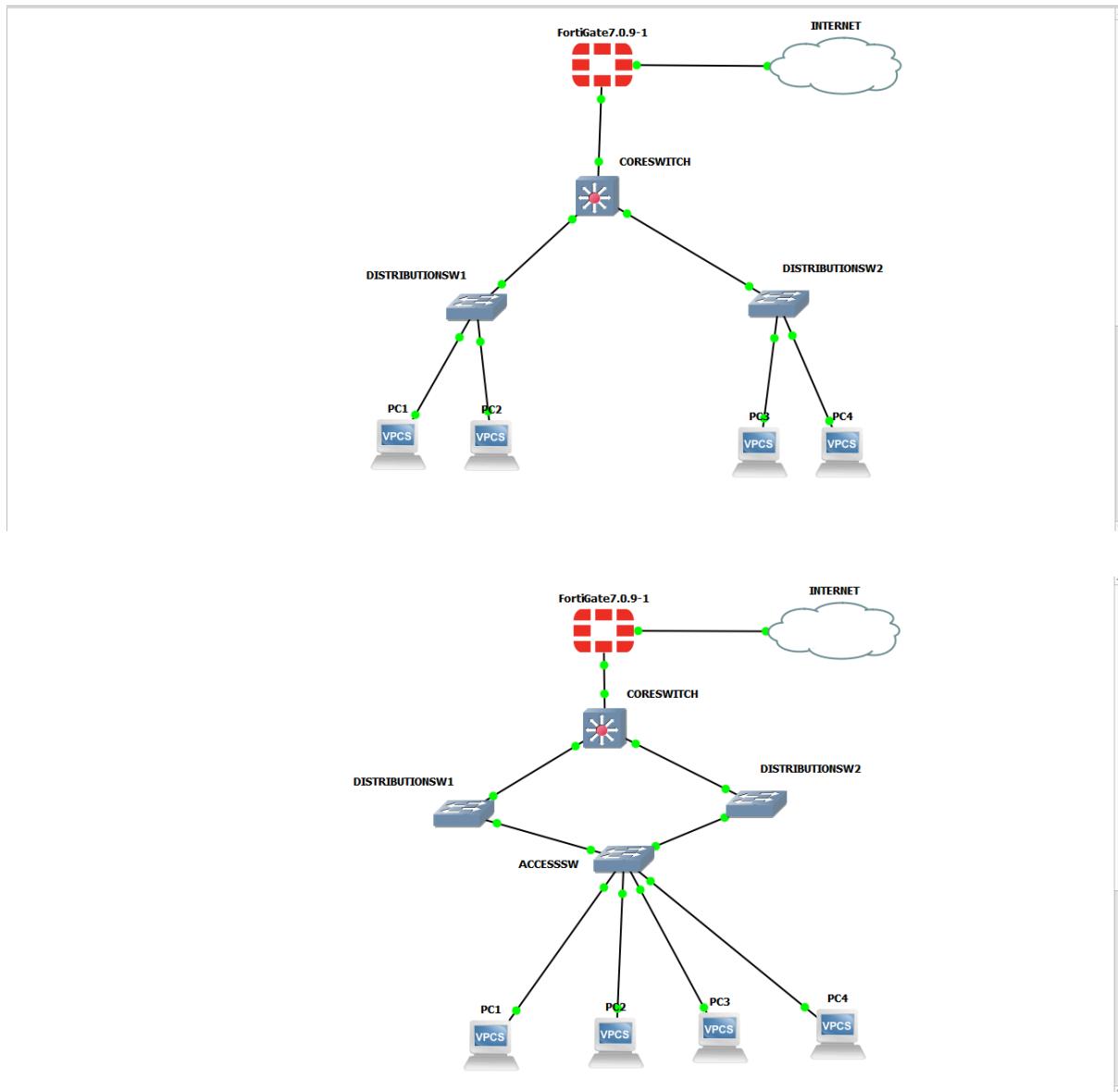
Port SW_Vlan10	Mode	VLAN	Connecté à
Et0	Trunk	30	SWCiscoL2 Et0/3
Et1	Access	30	PC6
Et2	Access	30	PC7

par défaut les switch de GNS3 sont déjà en mode access et on peut pas configurer autrement donc il faut juste mettre en liens trunk la liaison **SWCiscoL2** → Switch GNS3

## **7 Règles à retenir**

- **PC = ACCESS VLAN**
- **Switch ↔ Switch = TRUNK**
- **VLAN = logique, pas physique**
- **GNS3 Ethernet switch = lab pédagogique, pas production**
- **Tester VLAN avec ping et IP statique avant DHCP**

## 8 Amélioration de l'architecture



# Conclusion

1. Le lab a montré la différence entre perception et réalité réseau
2. On a appris à diagnostiquer VLAN / trunk / DHCP
3. Compréhension renforcée des meilleures pratiques pro
4. Préparer le lab avec IOSv-L2 ou un vrai switch émulé pour éviter les fausses illusions



## Phrase clé à retenir :

“Un VLAN qui fonctionne sur un lab GNS3 ne garantit pas qu'il fonctionnera sur un vrai réseau L2. Toujours configurer les trunks et ports ACCESS selon les standards.”