



INSTITUT AFRICAÏN D'INFORMATIQUE  
REPRESENTATION DU CAMEROUN  
CENTRE D'EXCELLENCE TECHNOLOGIQUE  
PAUL BIYA  
BP : 1379 Yaoundé(Cameroun)  
Tel : (237) 242 72 99 57 / 242 72 99 58  
Site web : [www.iaicameroun.com](http://www.iaicameroun.com)  
E-mail : [contact@iaicameroun.com](mailto:contact@iaicameroun.com)



**HIGH-TECH  
TRAINING INSTITUTE**  
KNOWLEDGE IS POWER

HIGH-TECH TRAINING INSTITUTE  
YAOUNDE-MFOUNDI MALL  
Tel : (237) 695 873 542 / 676 422 704  
E-mail : [infos@hti.net](mailto:infos@hti.net)

# CONFIGURATION DES VLANs SUR LE FIREWALLS FORTIGATE EN UTILISANT PNetLab

**REDIGE PAR :**

**MENGUENE ETEME STEVE NAZAIRE**

**Etudiant à l'IAI-Cameroun niveau 1**

**FILIERE : SYSTEME ET RESEAU**

**ANNEE ACADEMIQUE 2024-2025**

## TABLE DES MATIERES

### INTRODUCTION

- I. Objectif du Projet
- II. Technologie / équipement utilisés
- III. Topologie réseau
- IV. Etapas principales
- V. Résultat obtenus
- VI. Difficultés rencontrées / solutions
- VII. Captures d'écran
- VIII. Résumé

## INTRODUCTION

La segmentation du réseau est une pratique essentielle pour garantir la sécurité, la performance et la gestion efficace des flux de données dans une infrastructure informatique.

Les Vlan (Virtual Local Area Networks) permettent de diviser un réseau physique en plusieurs réseaux logiques indépendants. Dans ce projet, nous avons configuré plusieurs VLANs sur un firewall **FortiGate** virtuel dans l'environnement **PNetLab**, afin de simuler un réseau d'entreprise sécurisé et bien organisé.

## I. OBJECTIFS DU PROJET

Les principaux objectifs de ce projet sont :

- Mettre en place une segmentation réseau à l'aide des VLANs.
- Comprendre le rôle du **firewall FortiGate** dans la gestion des VLANs.
- Configurer les interfaces VLAN, les politiques de sécurité et les routes nécessaires.
- Vérifier la connectivité et la communication inter-VLAN contrôlée.
- Démontrer la capacité d'intégration du **FortiGate** dans un environnement virtuel PnetLab.

## II. TECHNOLOGIES ET EQUIPEMENTS UTILISES

### Logiciels de simulation :

- Simulateur : PNETLAB

### Equipements Virtuels :

- 1 \* FortiGate
- 1 \* Switch Cisco vIOS
- 3 \* PC (Virtual PC- Windows)

Technologie réseau : VLAN, Trunk, Access port, Routage inter-VLAN, politiques de sécurité, IP addressing.

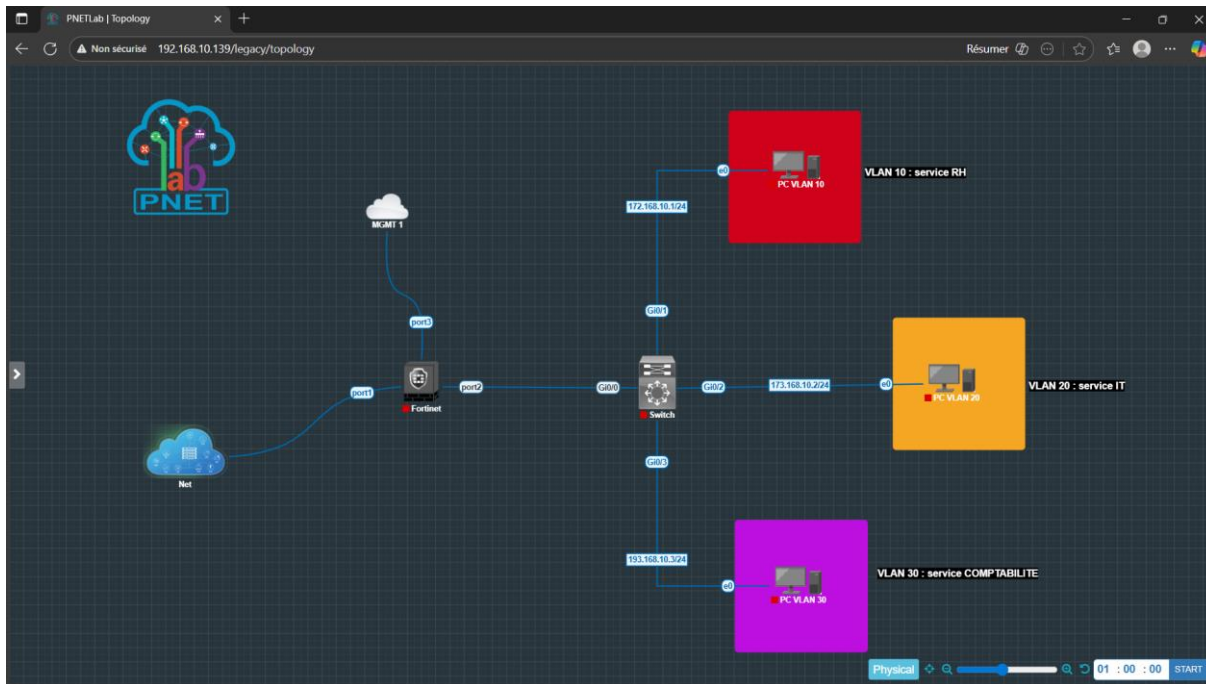
Système d'exploitation : Cisco IOS, FortiOS

## III. TOPOLOGIE RESEAU

### DESCRIPTION DE LA TOPOLOGIE

- Le FortiGate est connecté à un switch Cisco via une interface trunk.
- Trois VLANs sont configurés :
  - VLAN 10 : service RH

- VLAN 20 : service IT
- VLAN 30 : service Comptabilité.
- Chaque VLAN possède un sous-réseau IP distinct, et un PC est assigné à chaque VLAN.



## IV. ETAPES DE MISE EN ŒUVRE

### 1) Création des VLANs sur le switch Cisco

Switch

```

sw1ch(config)#
*Oct  9 11:41:54.736: %PLATFORM-5-SIGNATURE_VERIFIED: Image 'flash0:/vios_l2-adv
enterprisek9-m' passed code signing verification
sw1ch(config)#hostname SW1
SW1(config)#!
SW1(config)#vlan 10
SW1(config-vlan)#name Service-RH
SW1(config-vlan)#!
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name Service-IT
SW1(config-vlan)#!
SW1(config-vlan)#vlan 30
SW1(config-vlan)#name Service-Comptabilite
SW1(config-vlan)#!
SW1(config-vlan)#
  
```

### 2) Configuration des ports d'Access et du trunk

```
Switch(config)#hostname SW1
SW1(config)#!
SW1(config)#vlan 10
SW1(config-vlan)#name Service-RH
SW1(config-vlan)#!
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name Service-IT
SW1(config-vlan)#!
SW1(config-vlan)#vlan 30
SW1(config-vlan)#name Service-Comptabilite
SW1(config-vlan)#!
SW1(config-vlan)#int g0/0
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#!
SW1(config-if)#int g0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#!
SW1(config-if)#int g0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#!
SW1(config-if)#int g0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30
```

### 3) Configuration des interfaces VLANs sur le FortiGate

Configuration du Fortigate Via invite de commande (CLI), ici nous avons configurer le nom de notre fortigate, configurer l'interface **port 3** qui est notre cloud management et par la suite nous avons attribuer une adresse IP de manière dynamique (DHCP) et autoriser certains Access tel que « **http, https, ssh, ping** » à ce port dont le port 3.

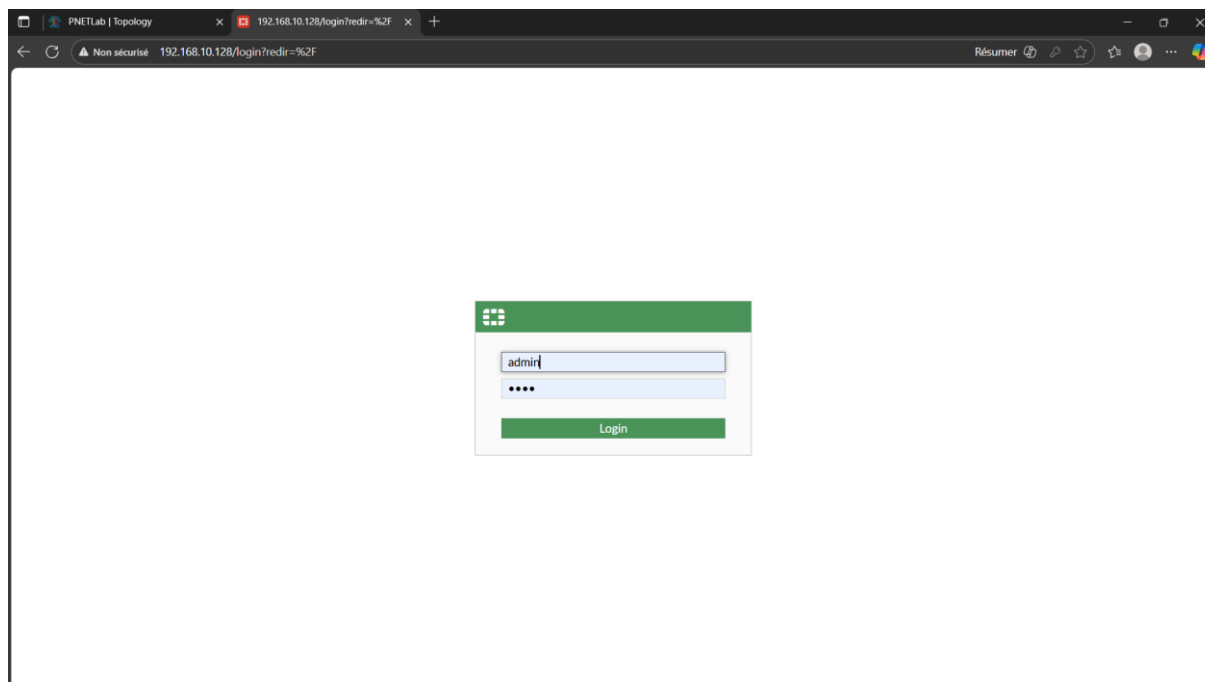
```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

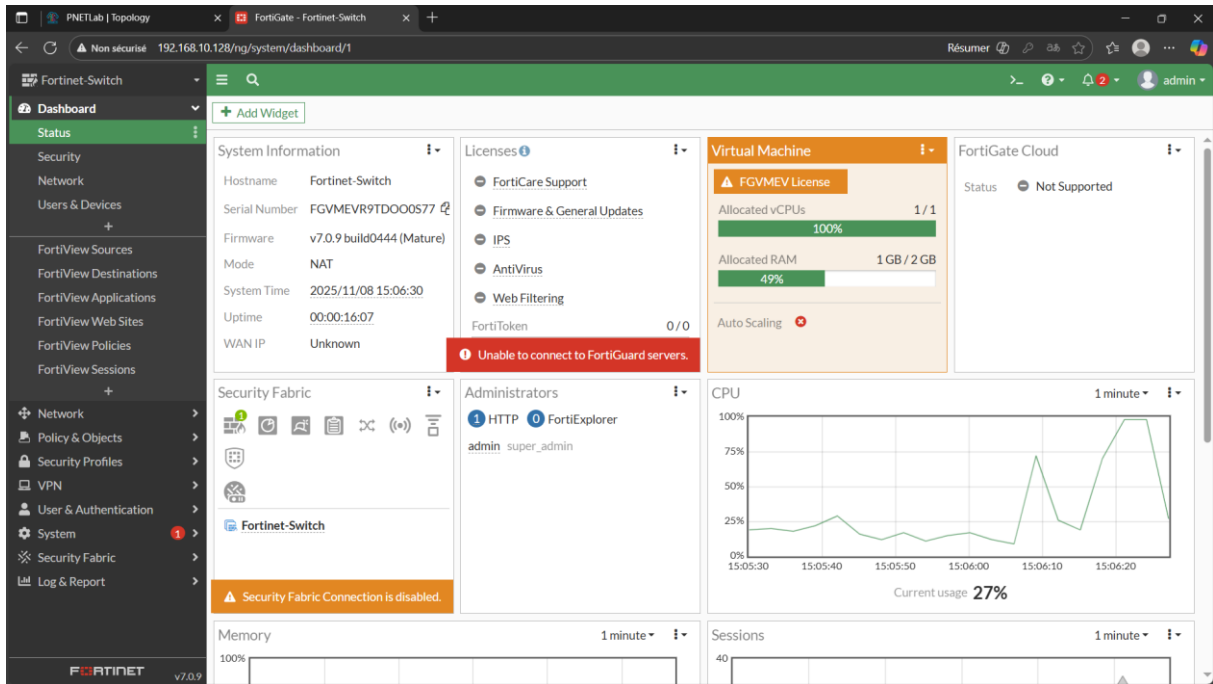
FortiGate-VM64-KVM # conf sy int
FortiGate-VM64-KVM (interface) # edi "port3"
FortiGate-VM64-KVM (port3) # set mode dhcp
FortiGate-VM64-KVM (port3) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port3) # end
FortiGate-VM64-KVM # conf sy global
FortiGate-VM64-KVM (global) # set hostname Fortinet-Switch
FortiGate-VM64-KVM (global) # end

Fortinet-Switch # show sy int
name      Name.
fortilink static  0.0.0.0 0.0.0.0 10.255.1.1 255.255.255.0 up  disable a
ggregate
l2t.root  static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable tunnel
naf.root  static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable tunnel
port1     dhcp    0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable physical
port2     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable physical
port3     dhcp    0.0.0.0 0.0.0.0 192.168.10.128 255.255.255.0 up  disable phy
sical
port4     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable physical
ssl.root  static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable tunnel

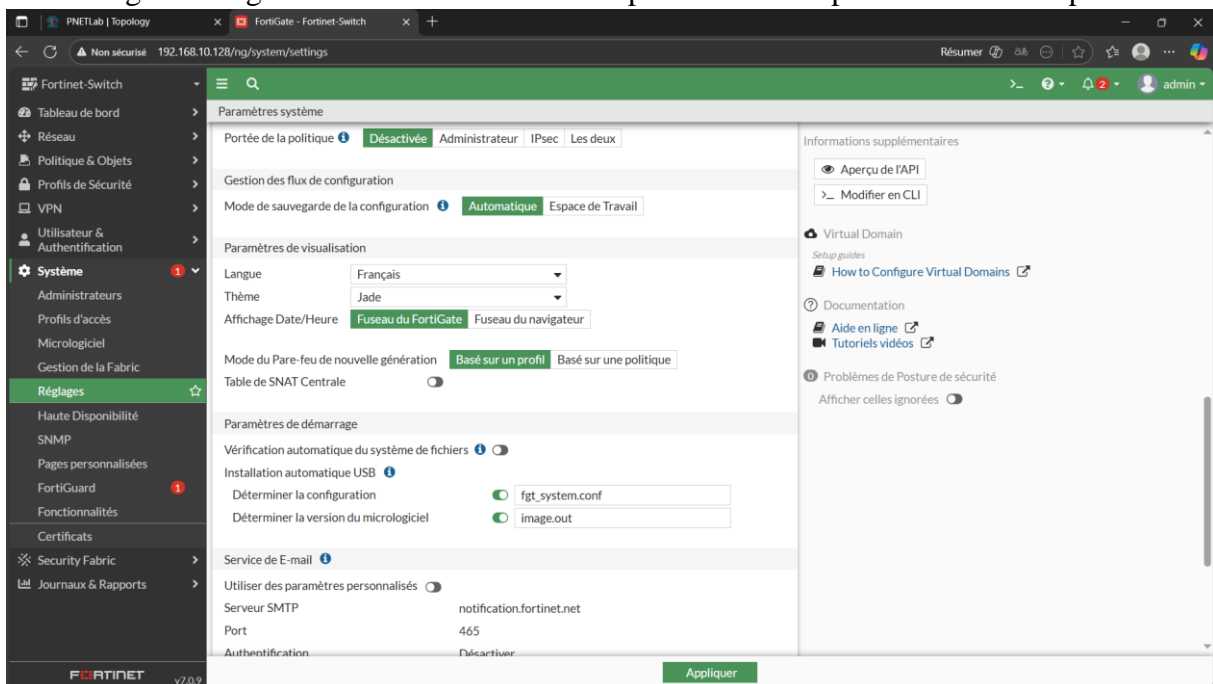
Fortinet-Switch # show sy int █
```

## Configuration du fortinet (firewall) sur interface graphique





Ont changé de langue et la durée de la session pour un travail plus stable et compréhensible



Configuration des différents interfaces et attribution des adresse IP.

**PORT 1** : pour qui nous permet d'aller sur internet encore appeler **port WAN** et activation de certains Access tel quel le http, https, ssh, ping.



**Nouvelle interface**

- Nom: Service-RH
- Alias: Service-RH
- Type: VLAN
- Protocole de VLAN: 802.1q 802.1qd
- Interface: port2
- ID VLAN: 10
- ID de VRF: 0
- Rôle: LAN

**Adresse**

- Mode d'adressage: Manuel DHCP Auto-géré par FortiIPAM
- IP/Masque: 172.168.10.1/24
- Créer un objet pour l'adresse de l'interface:
- Nom: Service-RH address
- Destination: 172.168.10.1/24
- Adresses IP Secondaires:

**Accès administratif**

- IPv4:
  - HTTPS
  - SSH
  - Comptabilisation RADIUS
  - PING
  - SNMP
  - Security Fabric
  - Accès FMG
  - FTM
  - Test de débit

État DHCP:  Activé  Désactivé

Nom	Type	Membres	IP/Masque	Accès administratif	Clients DHCP	Page
<b>Agrégat 802.3ad</b>						
fortilink	Agrégat 802.3ad		Dédié à FortiSwitch	PING Security Fabric		10.255.1
<b>Interface de tunnel</b>						
NAT interface (naf.root)	Interface de tunnel		0.0.0.0/0.0.0.0			
<b>Interface physique</b>						
port2	Interface physique		0.0.0.0/0.0.0.0			
Service-Compta (Service-Compta)	VLAN		193.168.10.3/255.255.255.0	PING HTTPS SSH		193.168.
Service-IT (Service-IT)	VLAN		173.168.10.2/255.255.255.0	PING HTTPS SSH	2	173.168.
Service-RH (Service-RH)	VLAN		172.168.10.1/255.255.255.0	PING HTTPS SSH		172.168.
port3	Interface physique		192.168.10.128/255.255.255.0	PING HTTPS		

**Port 3 :** Désactivation du port 3 (cloud management) pour que la connexion passe par le nôtre port qui est le port2

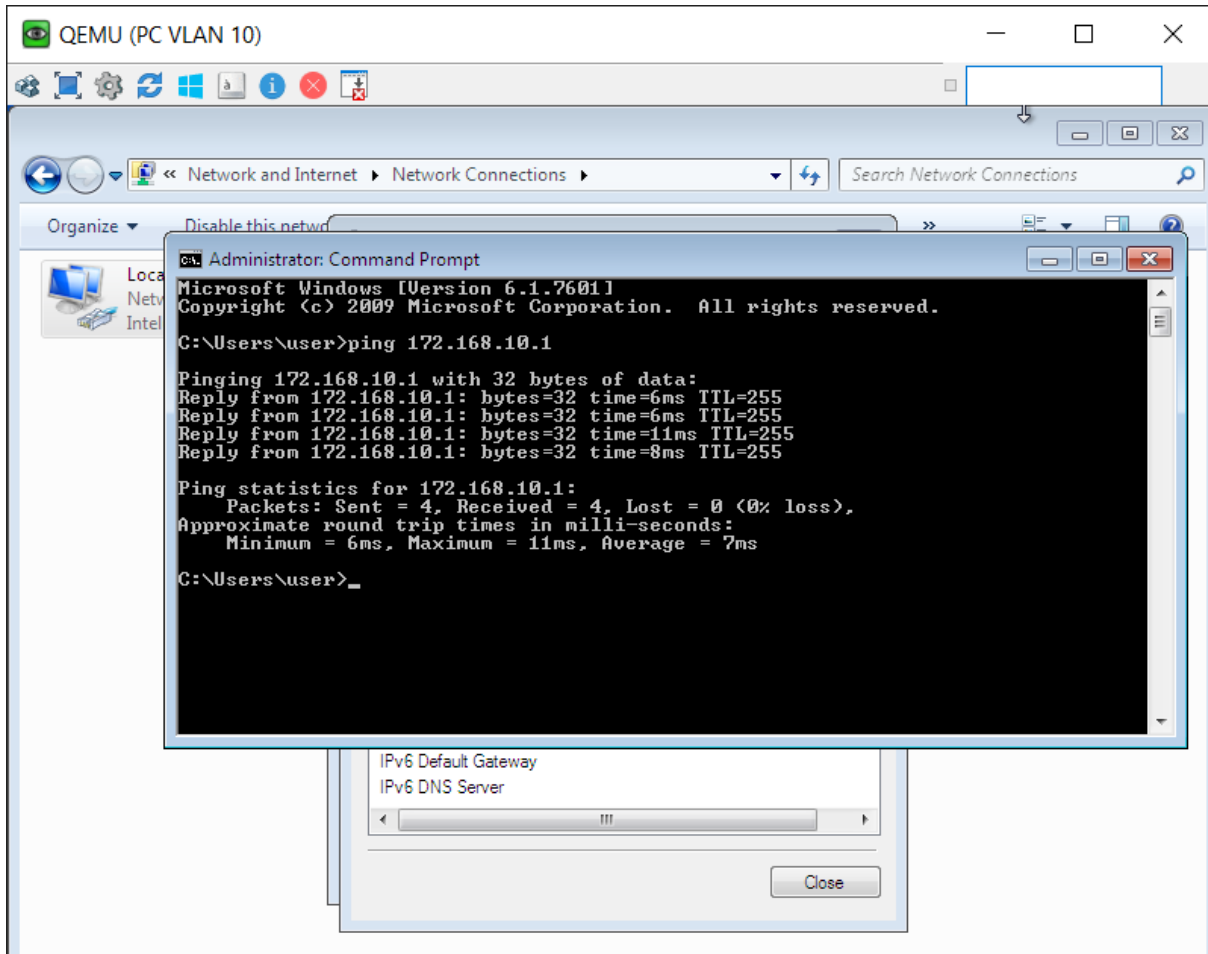
The screenshot shows the FortiGate web interface for configuring the 'Mangemnt (port3)' interface. The configuration is set to DHCP mode. The IP address is 192.168.10.128 with a subnet mask of 255.255.255.0. The DNS server is 192.168.10.2. The interface is active. The 'Accès administratif' section shows that HTTPS, HTTP, and PING are enabled. The 'Reception LLDP' section is set to 'Utiliser le paramètre du VDOM'.

Property	Value
Nom	Mangemnt (port3)
Alias	Mangemnt
Type	Interface physique
ID de VRF	0
Rôle	Indéfini
Port de Gestion Dédié	<input type="radio"/>
Adresse	
Mode d'adressage	Manuel DHCP Auto-géré par FortiIPAM Capture One-Arm
État	Connecté
Adresse IP et masque obtenus	192.168.10.128/255.255.255.0
Expiration	2025/11/11 18:25:14
Serveur DNS obtenu	192.168.10.2
Obtenir dynamiquement la route par défaut	<input type="checkbox"/>
Remplacer le serveur DNS pré-configuré	<input type="checkbox"/>
Accès administratif	
IPV4	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING
	<input type="checkbox"/> Accès FMG <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM <input type="checkbox"/> Comptabilisation RADIUS <input type="checkbox"/> Security Fabric
	<input type="checkbox"/> Test de débit
Reception LLDP	Utiliser le paramètre du VDOM Activer Désactiver

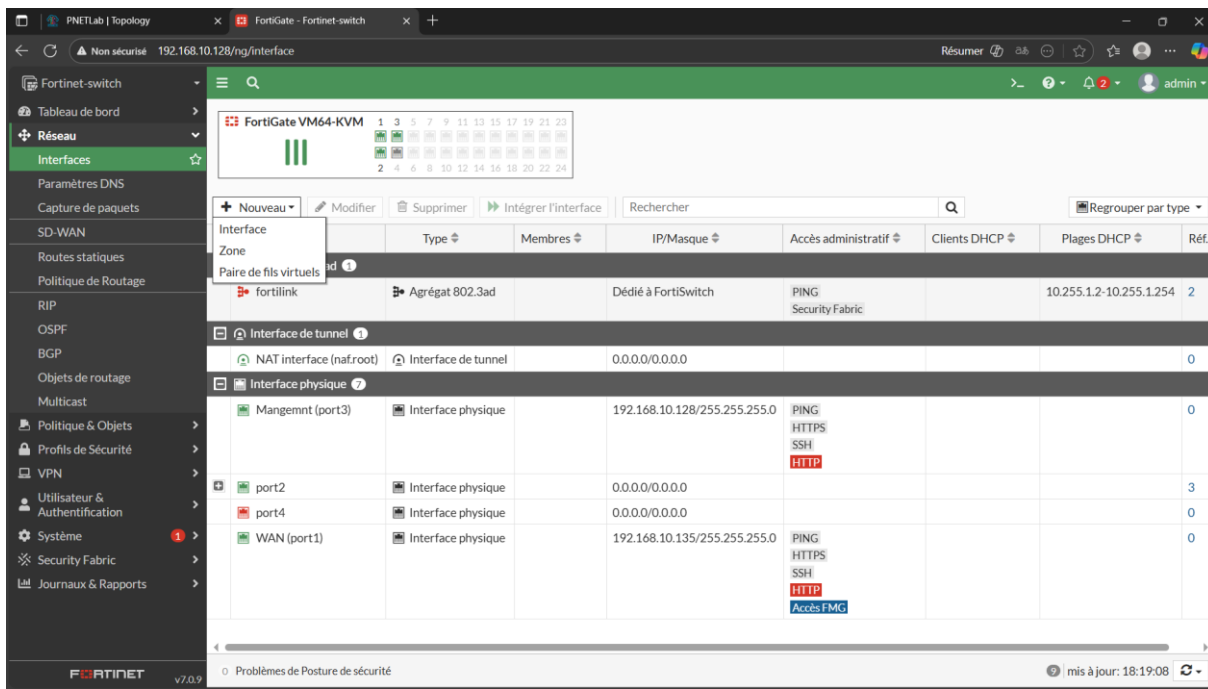
**NB : Vérifier que nos machines ont eu des adresses IP**

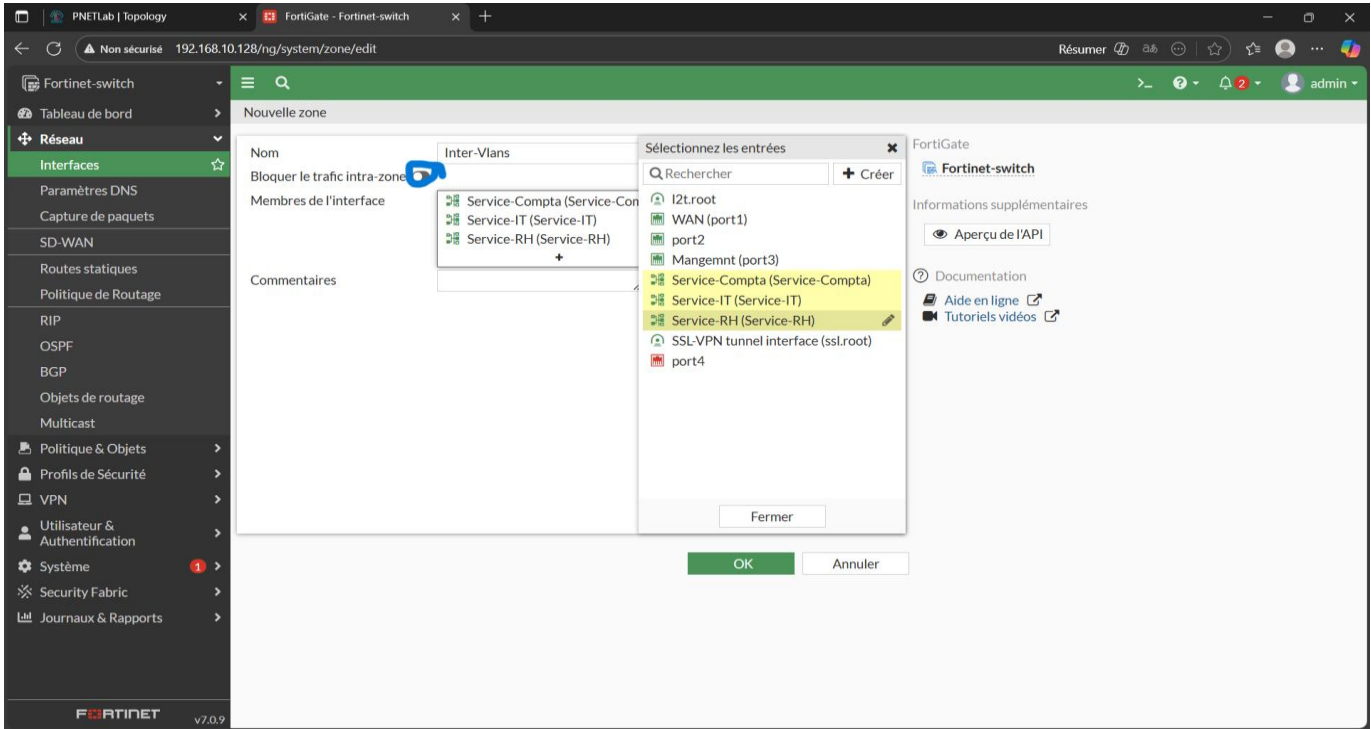
The screenshot shows the Windows Network Connections window. The 'Local Area Connection Status' window is open for 'Network 3'. The 'Network Connection Details' window is also open, showing the following information:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Network Connecti...
Physical Address	50-5C-B2-00-CE-00
DHCP Enabled	Yes
IPv4 Address	172.168.10.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, November 12, 2025 2:10:28
Lease Expires	Wednesday, November 19, 2025 2:10:27
IPv4 Default Gateway	172.168.10.1
IPv4 DHCP Server	172.168.10.1
IPv4 DNS Server	192.168.10.2
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::a99f:903d:f7dd:b7b7%11
IPv6 Default Gateway	
IPv6 DNS Server	

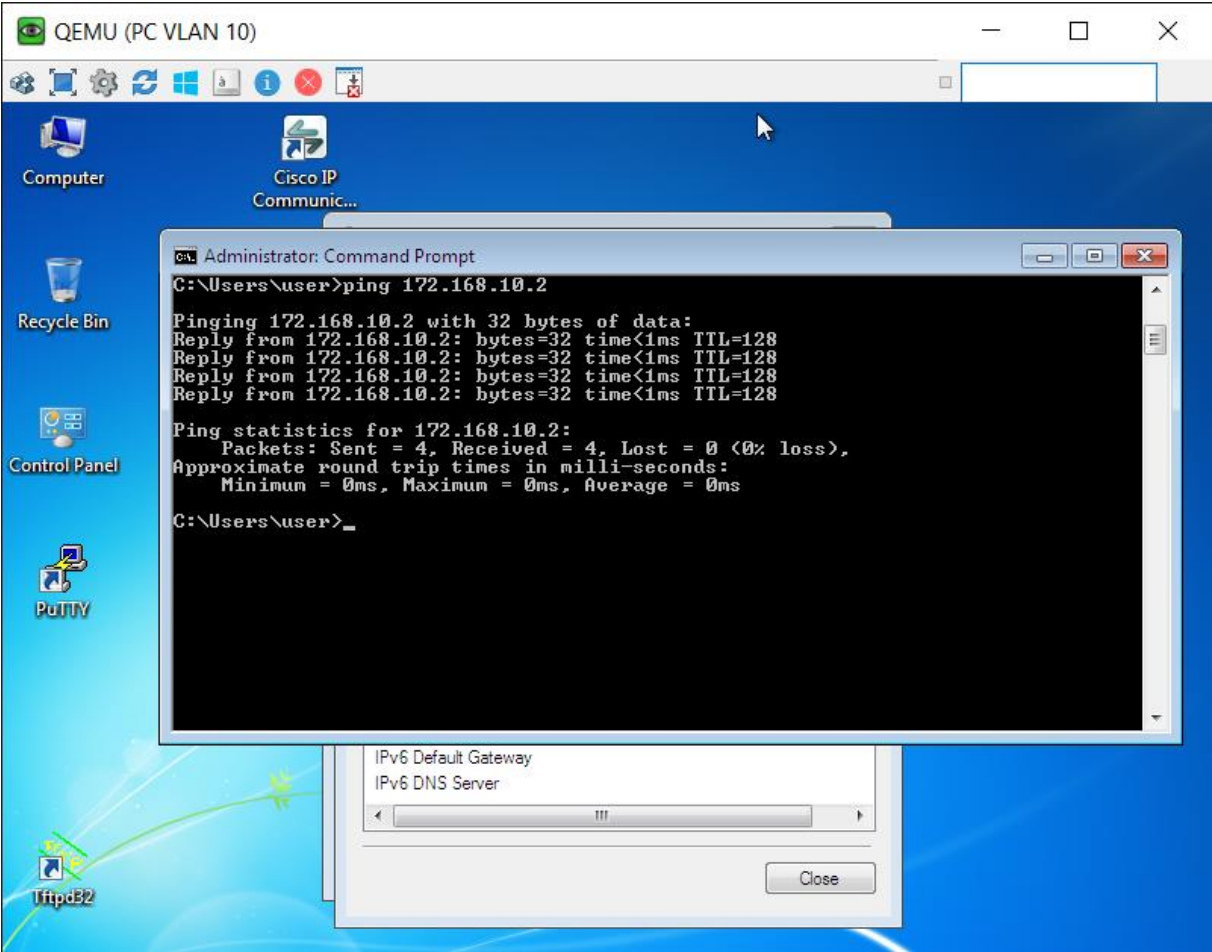


## Création d'une ZONE pour permettre à ce que tous nos VLANs communique



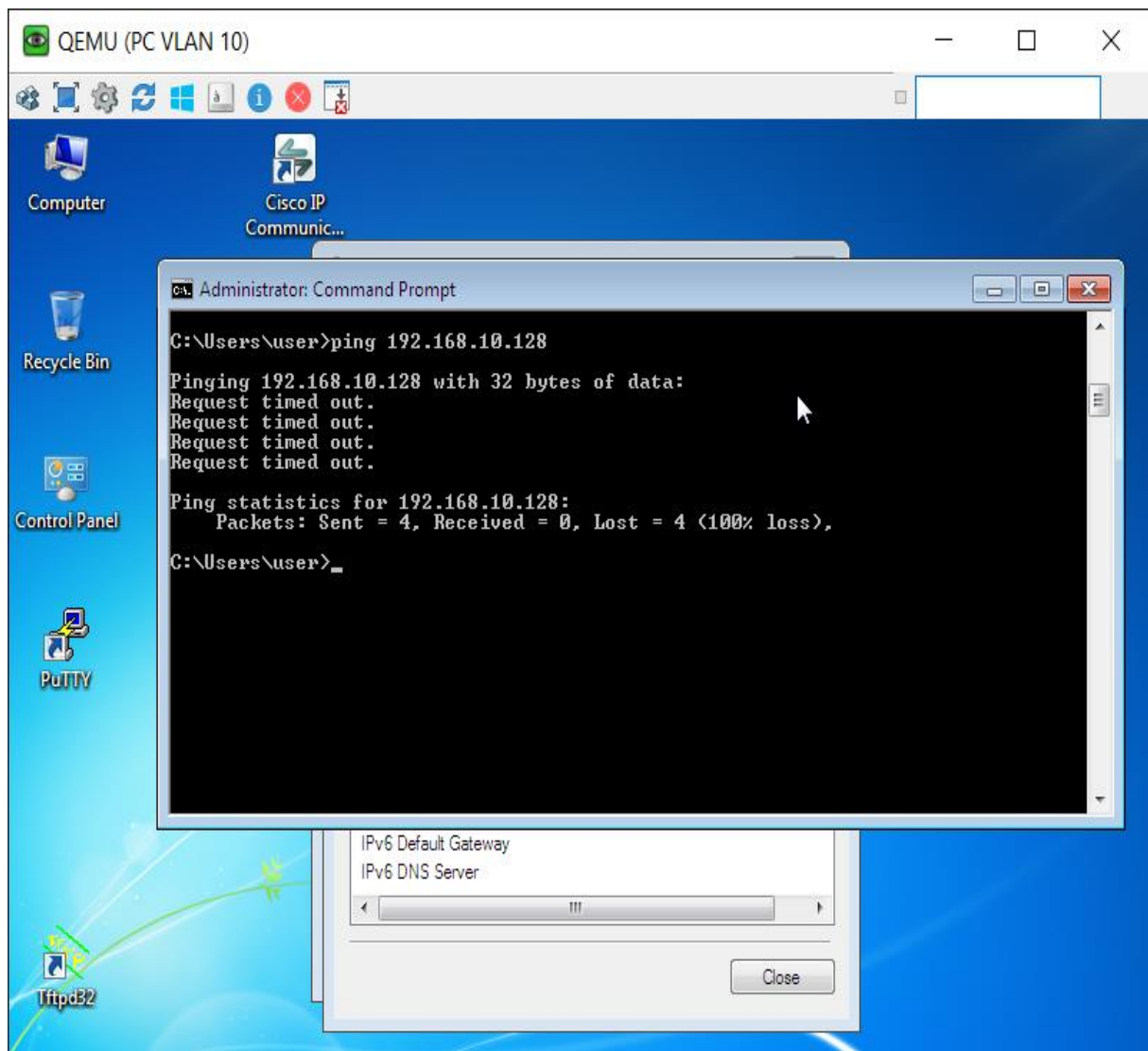


**NB :** Vérification si nos machines communiquent via un ping : 173.168.10.2/24



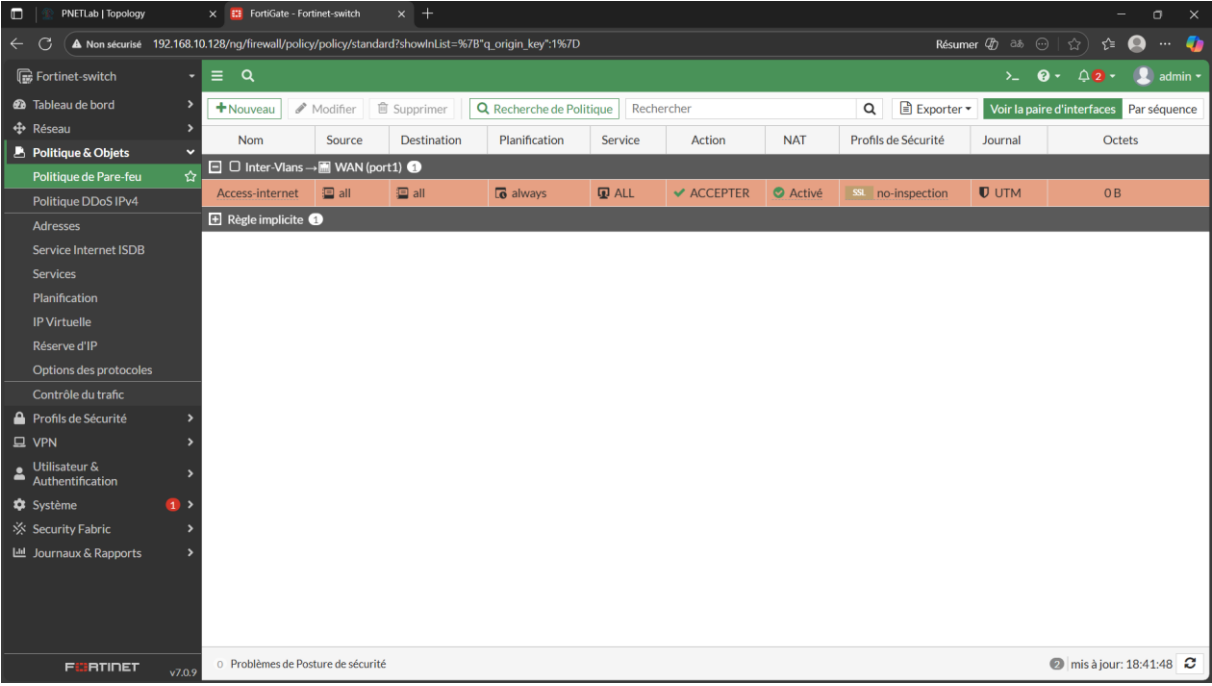
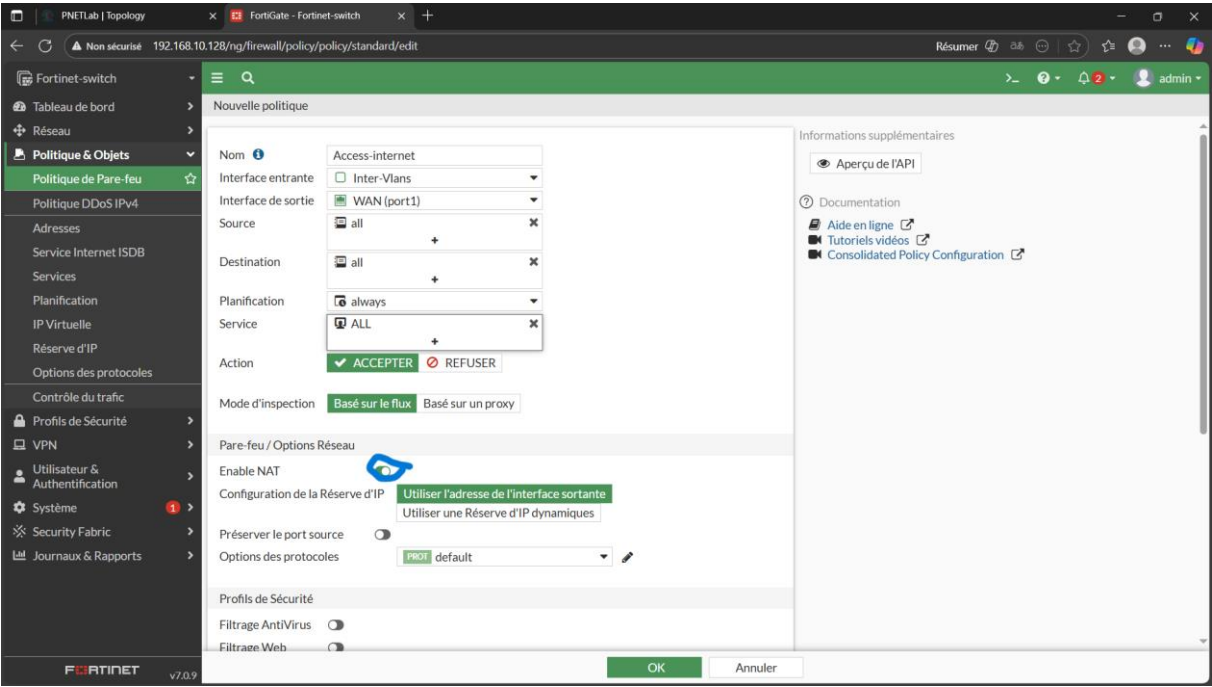
## Permettre à ce que nos machines puissent avoir Access a l'internet (Configuration des règles de sécurité)

- Essayons de faire un ping sur internet via IP 192.168.10.128

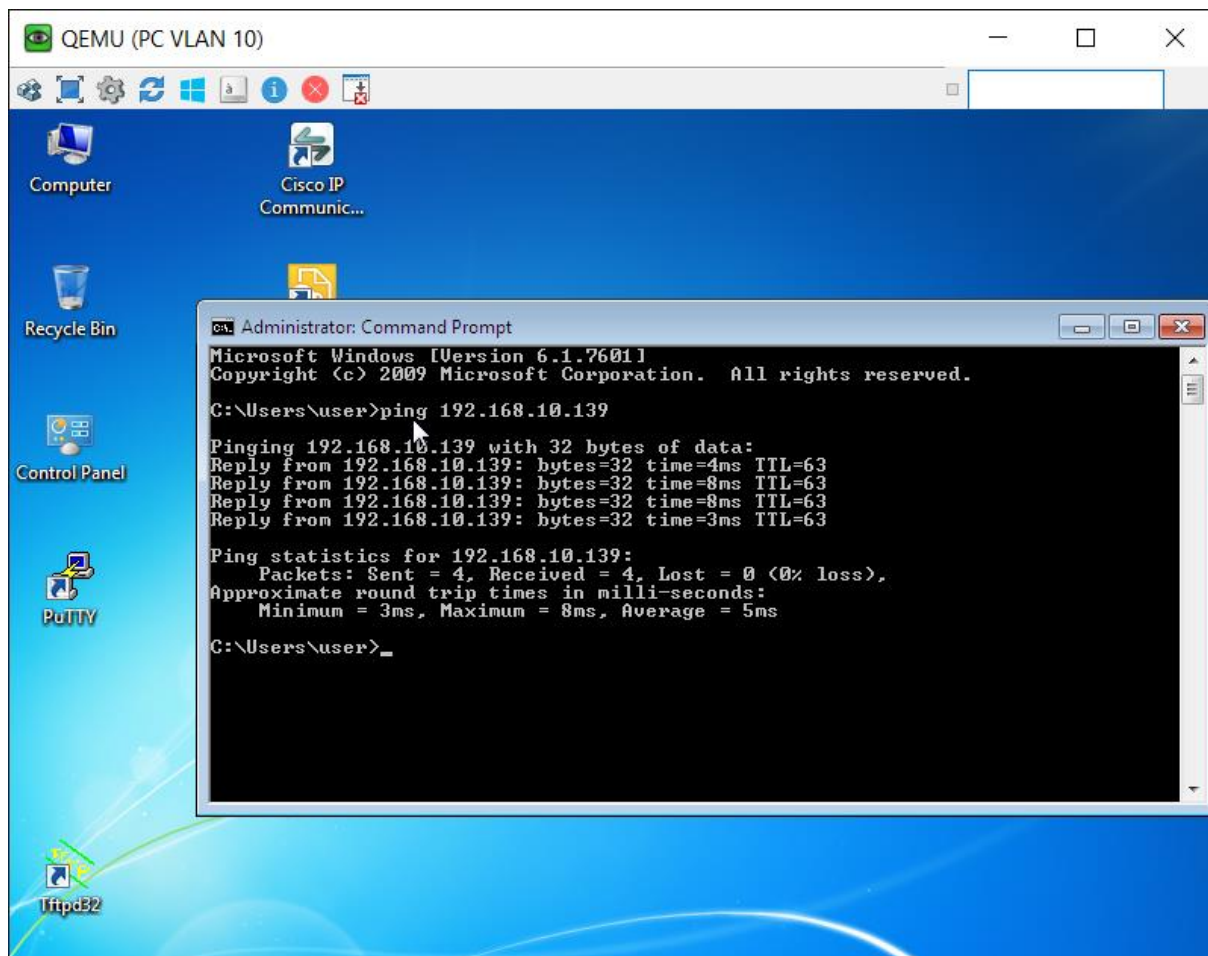


Internet ne passe pas car nous n'avons aucune connexion entre nos VLANs et internet parce que aucune politique de sécurité n'a été créé au niveau de notre firewall forinet

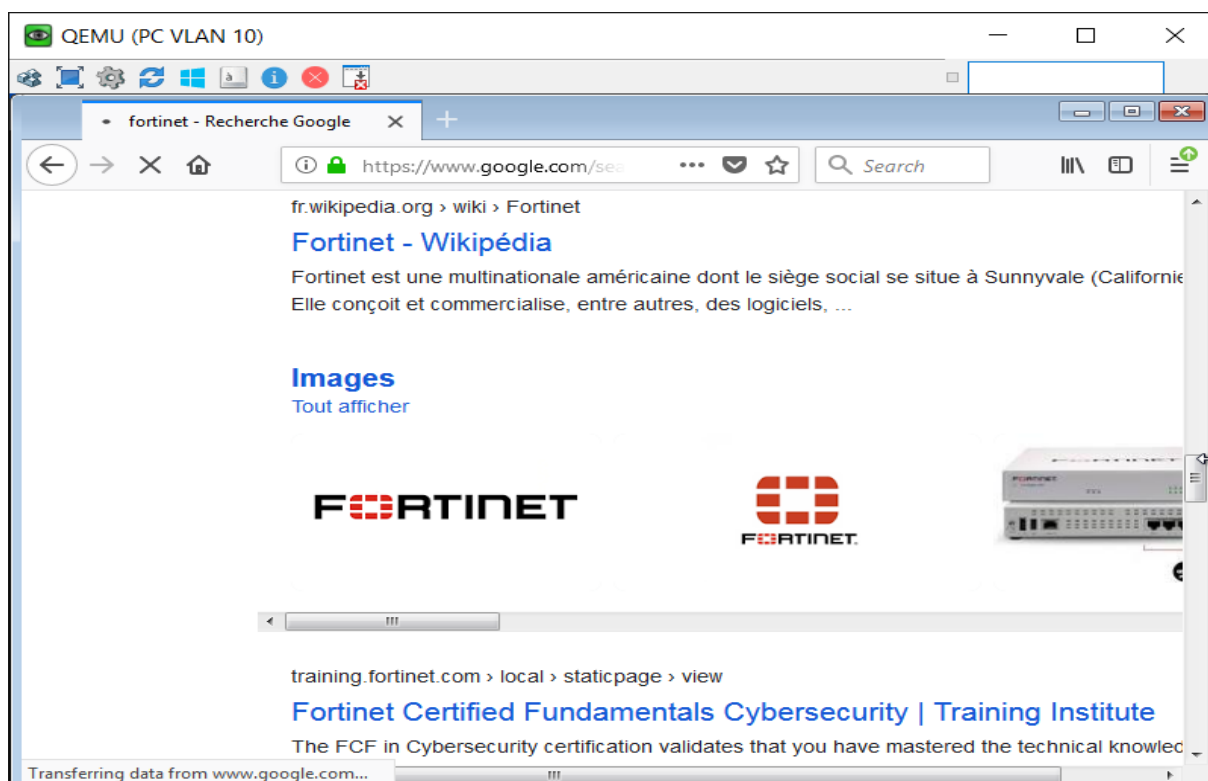
- Création des politiques de sécurité (toujours se rassurer que le NAT est actif)

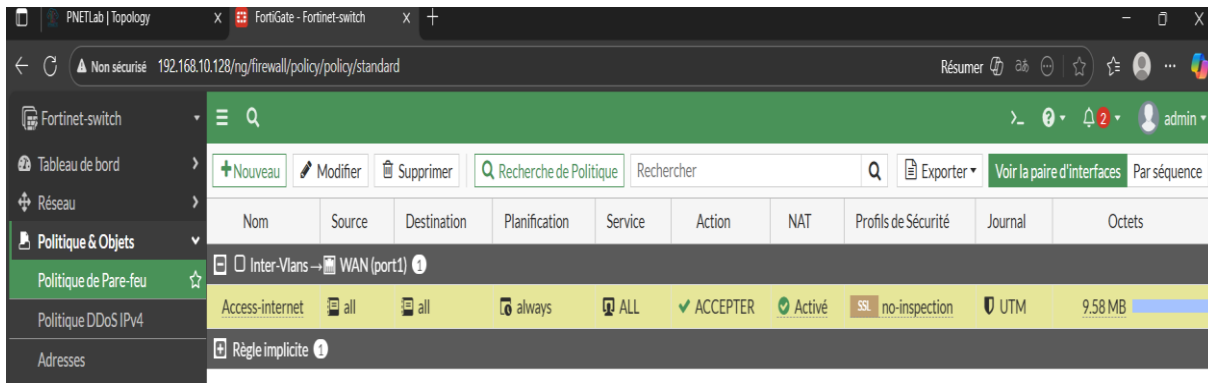


- Vérifions maintenant que internet passe toujours un ping IP 192.168.128.10/24



- Allons sur internet avec un de nos PC pour faire une recherche





Ce pare-feu **FortiGate** permet aux utilisateurs internes (**réseau Inter-Vlans**) d'accéder à **Internet via l'interface WAN**, grâce à la politique "**Access-internet**".

Il accepte tout le trafic sortant, sans restriction de protocole ni de destination, et **effectue une traduction d'adresse (NAT)** pour rendre la navigation Internet possible.

Selon les statistiques affichées, la règle a déjà permis le transfert d'environ **9,58 Mo de données**, ce qui montre que le trafic circule effectivement à travers cette politique et que les utilisateurs du réseau interne accèdent bien à Internet.

## RESULTATS OBTENUS

- ❖ Chaque PC a pu communiquer avec le FortiGate via son VLAN.
- ❖ Le FortiGate a assuré le routage inter-VLAN.
- ❖ Les politiques de sécurité ont permis de contrôler les échanges entre les services (ex : RH ne peut pas accéder à IT sans autorisation).
- ❖ Le test de connectivite (Ping) a validé la configuration réussie.

## V. DIFFICULTES RENCONTREES ET SOLUTIONS APORTEES

DIFFICULTE	CAUSE	SOLUTION
Aucune commutation entre VLANs	Trunk mal configure	Revoir la configuration su switch et du port Trunk
Ping bloque	Politique de sécurité absente	Création d'un firewall Policy appropriée
Interface VLAN inactive	Mauvaise affectation du port	Vérifier le mapping des interfaces dans Pnetlab

## VI. ANALYSE DU TRAFIC ET SECURITE IPSEC

Même si le focus du projet est sur les VLANs, une analyse du trafic montre que le FortiGate inspecte les paquets entre VLANs et applique les politiques définies.

Une extension possible serait **la mise en place d'un tunnel IPsec** entre deux FortiGate pour relier des VLANs distants de manière sécurisée.

## VII. CE QUE J'AI APPRIS

- Compréhension du rôle des VLANs dans la segmentation réseau.
- Configuration du FortiGate pour gérer plusieurs sous-réseaux virtuels.
- Création et application de politiques de sécurité inter-VLAN.
- Maîtrise de la simulation d'infrastructure dans **PnetLab**.
- Importance du diagnostic réseau (Ping, tracer, show commands).

## VIII. CONCLUSION

Ce projet m'a permis de consolider mes compétences en **administration réseau et sécurité**. La mise en place des VLANs sur FortiGate via PnetLab m'a aidé à comprendre la gestion des flux internes dans une architecture d'entreprise et la mise en œuvre de politiques de sécurité adaptées.

Cette expérience est une étape importante vers la maîtrise des réseaux professionnels et la préparation à des certifications comme le **Fortinet NSE** ou le **CCNA Security**.