

Procédure paramétrage Firewall

Outils nécessaires :

- 3 PC
- 3 cable Rj45
- fortinet firewall
- box

1ere étape reset le firewall :

Appuyer sur le bouton reset pendant 15 secondes à l'arrière du firewall avec un crayon pour le reset.



2eme étape se connecter à fortigate :

- 1-Connecter un cable Rj45 au firewall qui sera relié à un PC
- 2-sur le navigateur saisir l'IP 192.168.1.99, le site est inaccessible



- 3-Modifier l'adresse IP du PC pour qu'elle soit sur le même réseau que l'adresse du Fortigate qui est 199.168.1.99 :

-A l'aide du cmd regarder l'ip du PC

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [version 10.0.22631.6199]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\herim>ipconfig /all

Configuration IP de Windows

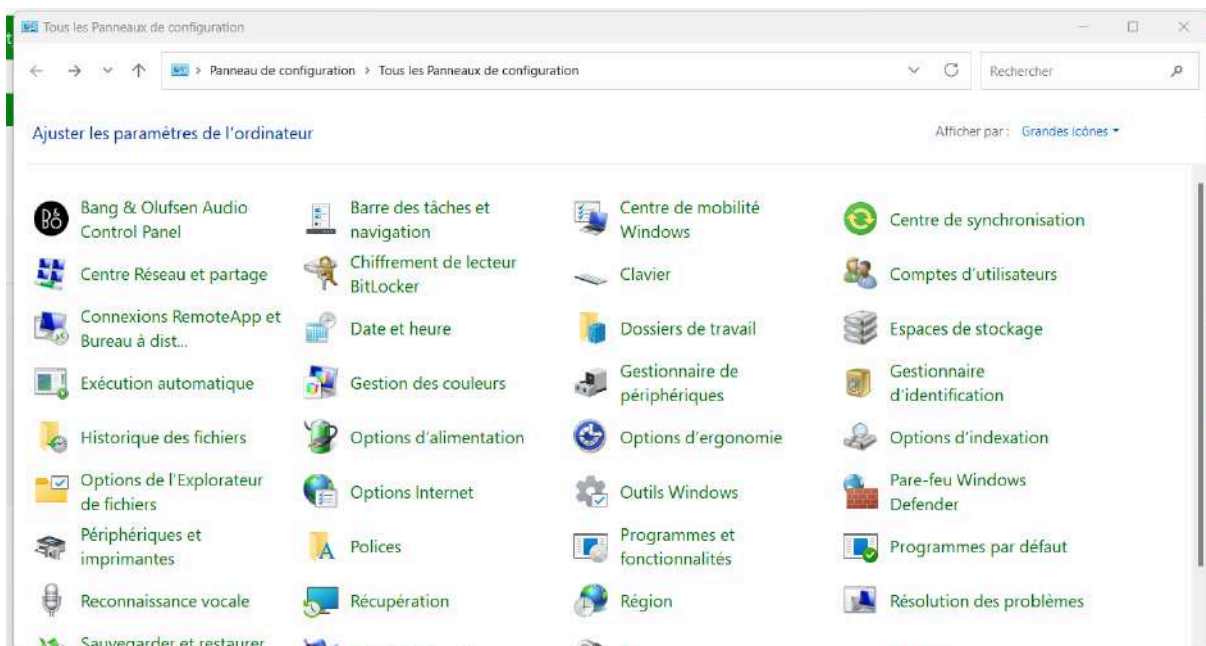
    Nom de l'hôte . . . . . : DESKTOP-CF0AHMC
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: formation.local

Carte Ethernet Ethernet 2 :

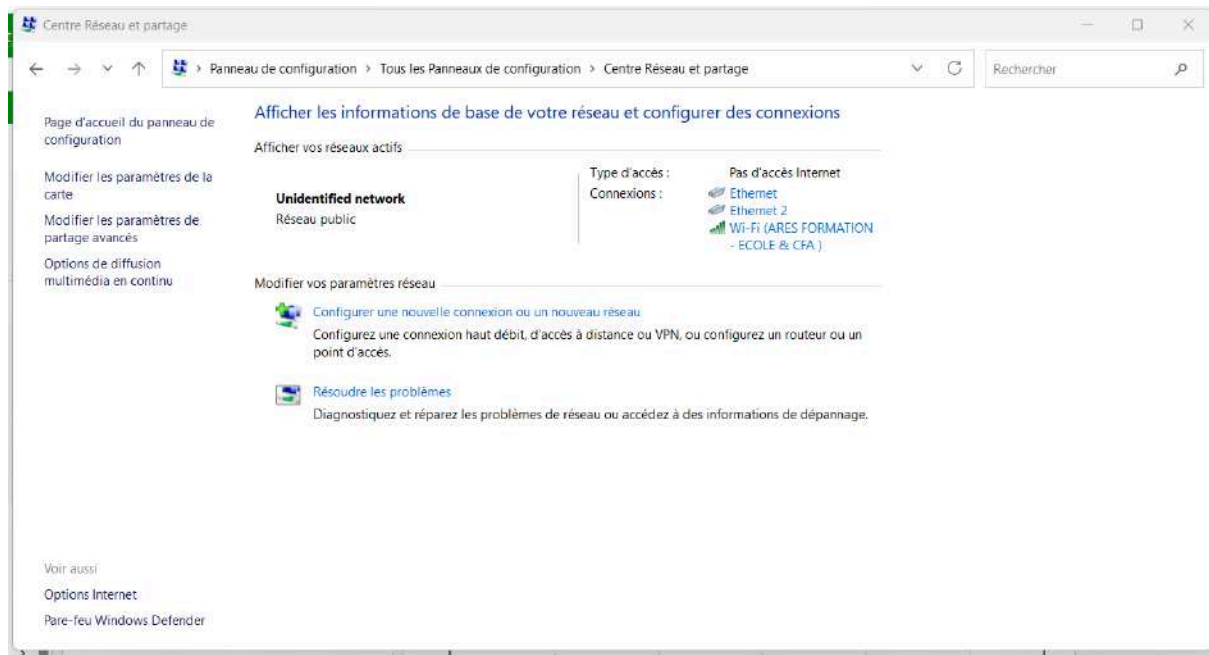
    Suffixe DNS propre à la connexion. . . :
    Description. . . . . : TAP-Windows Adapter V9
    Adresse physique . . . . . : 00-FF-33-6D-8E-BD
    DHCP activé. . . . . : Non
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::22f9:ea73:3f74:cc83%8(préfééré)
    Adresse IPv4. . . . . : 169.254.123.106(préfééré)
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . :
    IAID DHCPv6 . . . . . : 687931187
    DUID de client DHCPv6. . . . . : 00-01-00-01-2C-3B-04-0D-B0-0C-D1-40-37-78
    NetBIOS sur Tcpip. . . . . : Activé

Carte inconnue Wintun :
```

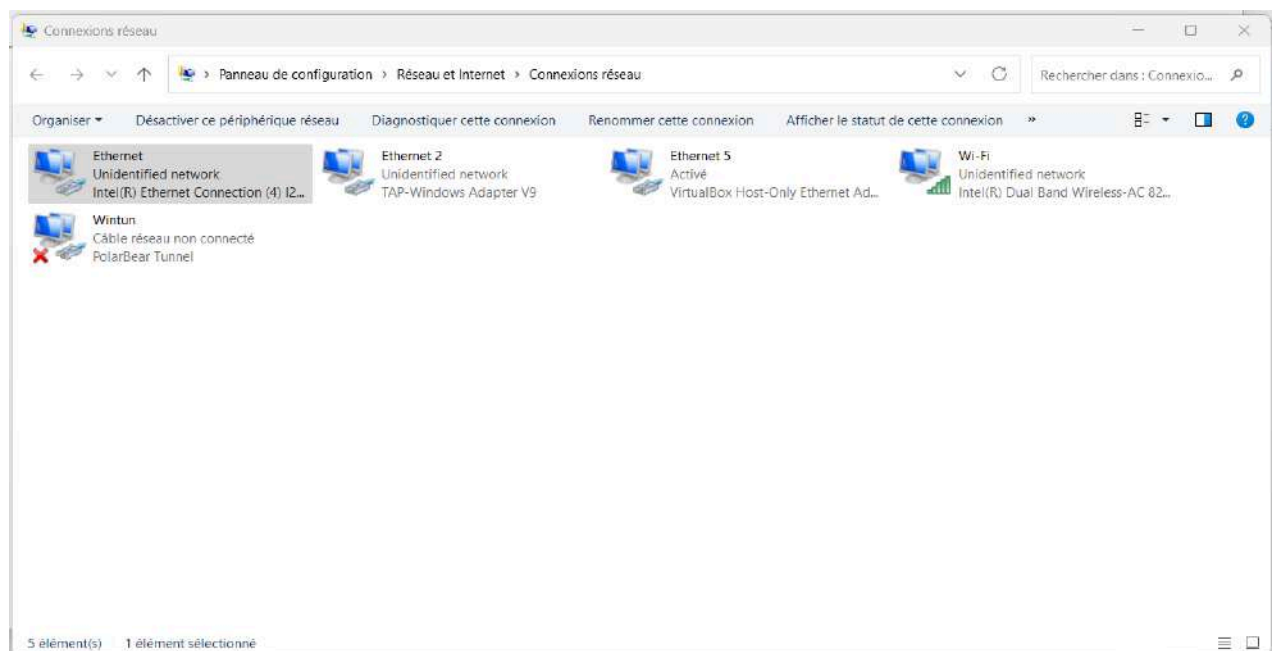
-aller sur le **panneau de configuration**



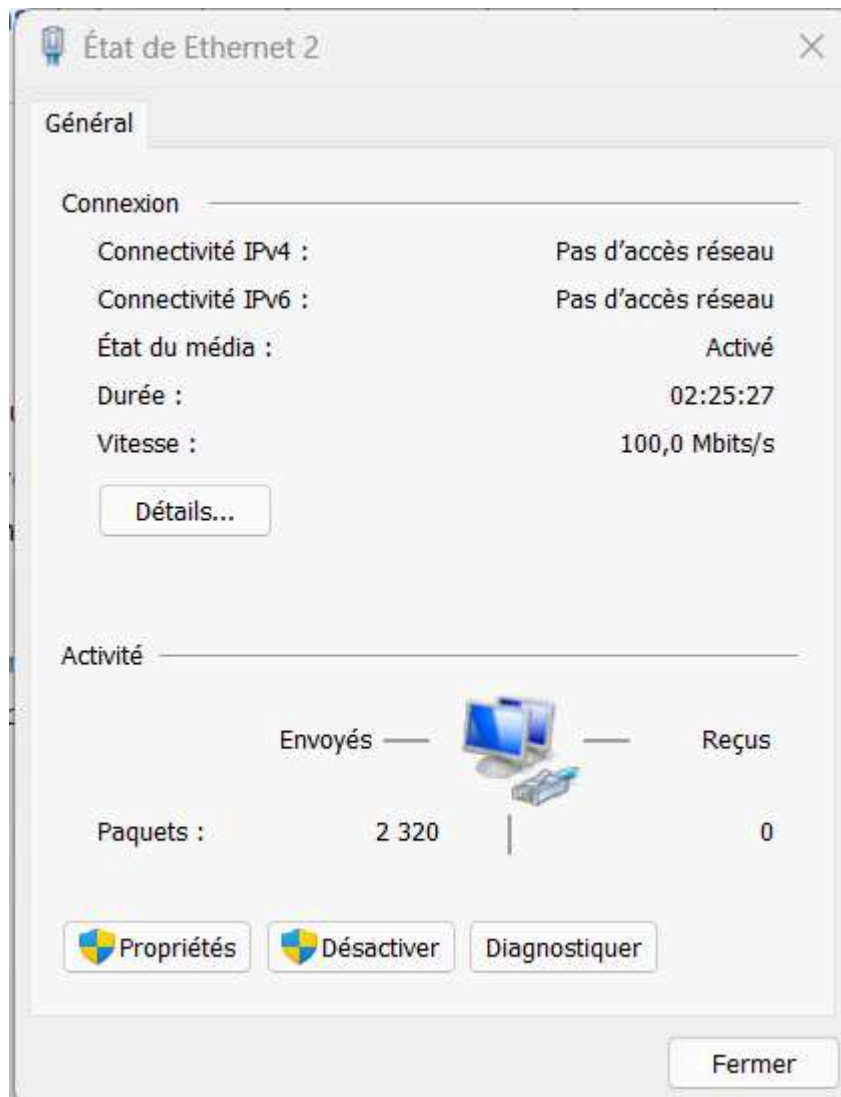
-aller sur le **centre Réseau et partage**



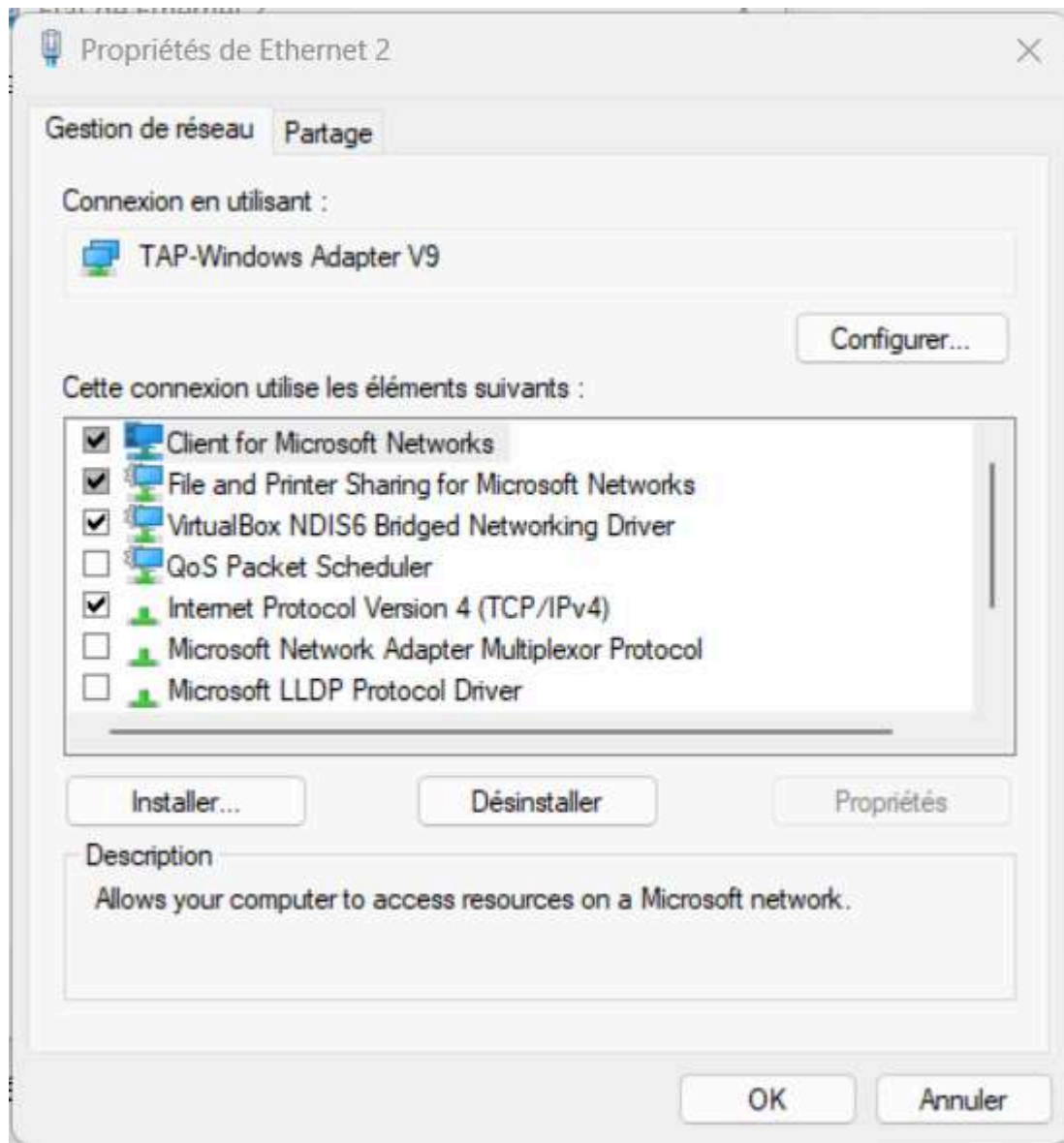
- Sur la partie gauche de l'écran cliquer sur **modifier les paramètres de la carte**, une nouvelle page s'affiche



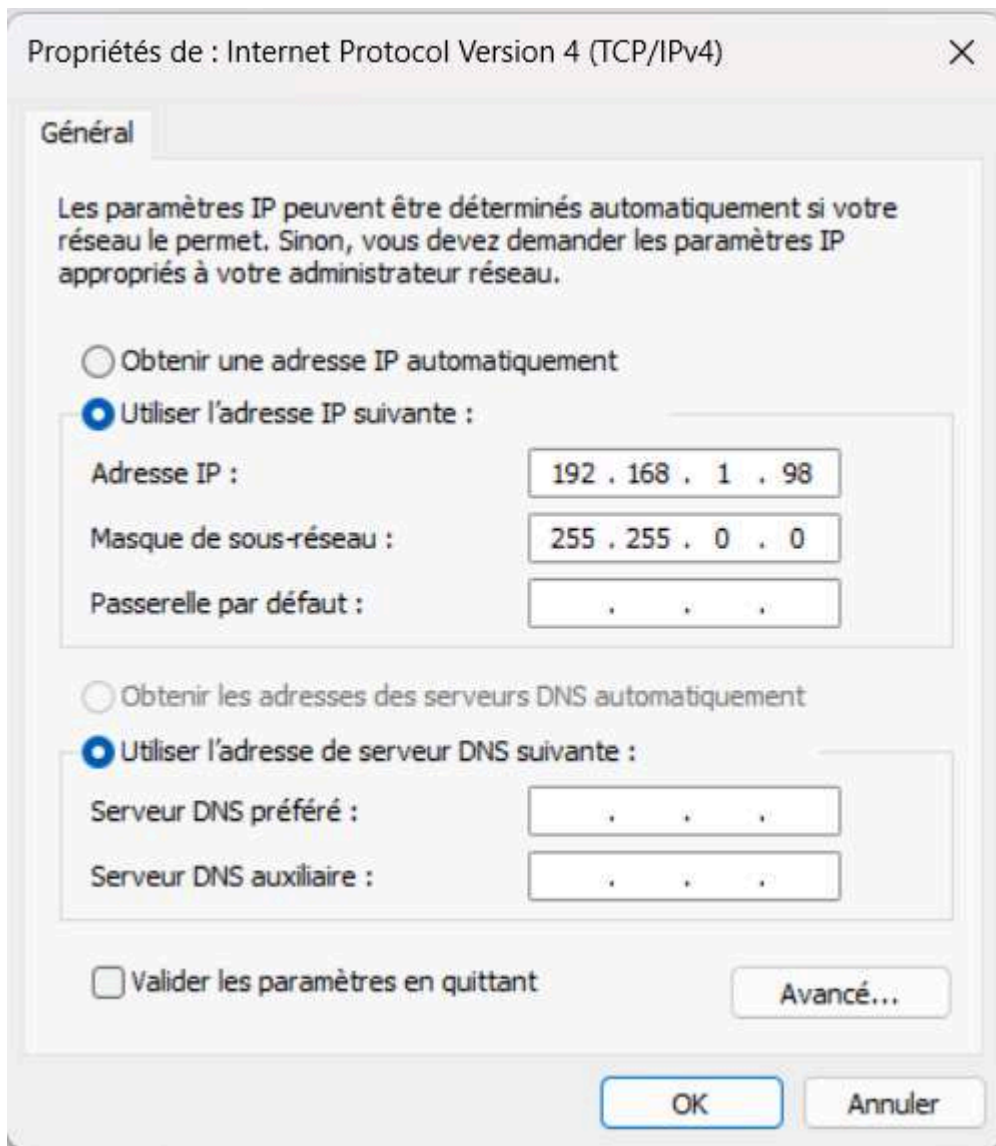
-choisir la carte ethernet correspondante pour changer son IP, une page état de ethernet s'affiche



- cliquer sur les **propriétés**



-cliquer sur **internet protocol version 4(TCP/IPv4)** puis cliquer sur propriétés



-comme sur la capture configurer une adresse ip disponible dans le même réseau que l'adresse du Fortigate qui est 199.168.1.99 et définir le masque de sous réseau en fonction du masque désiré(il se remplit automatiquement mais il faut vérifier qu'il correspond au masque qu'on veut)

-La configuration de l'ip est terminée, fermer toute les fenetres ouverte

3eme étape configuration de fortigate :

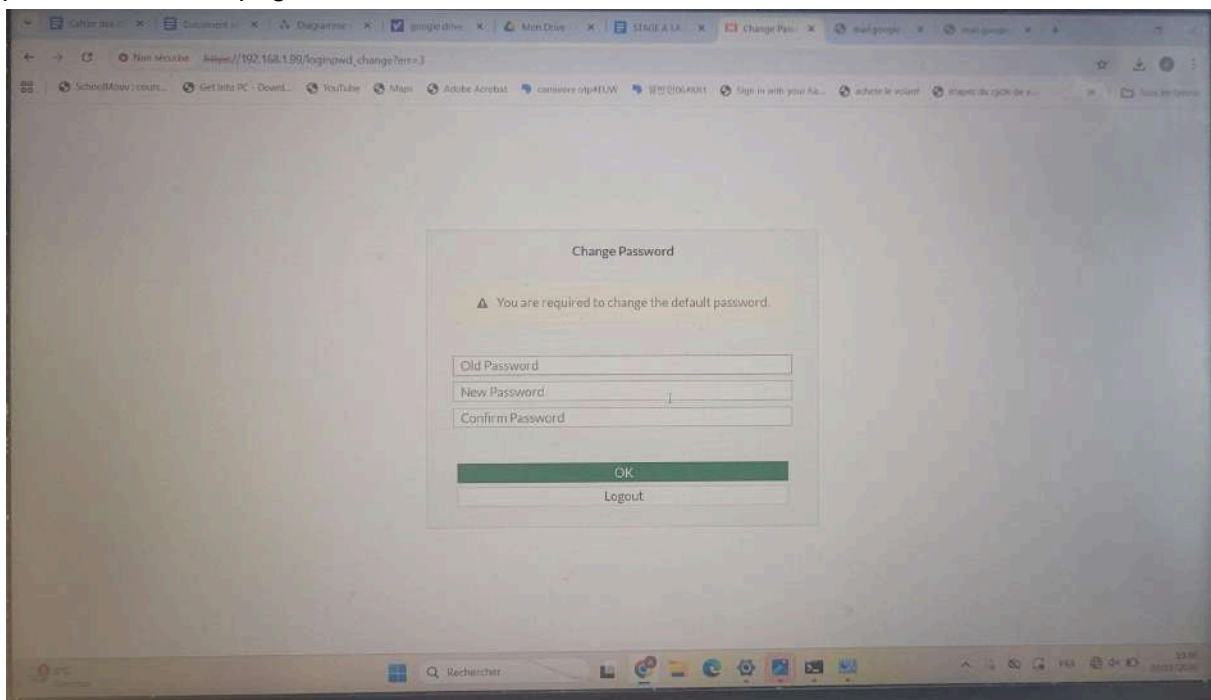
1- Une fois l'adresse Ip changé, se reconnecter sur le navigateur à l'IP 192.168.1.99

2- une page de connexion s'affiche, on saisit un **username** et un **password**

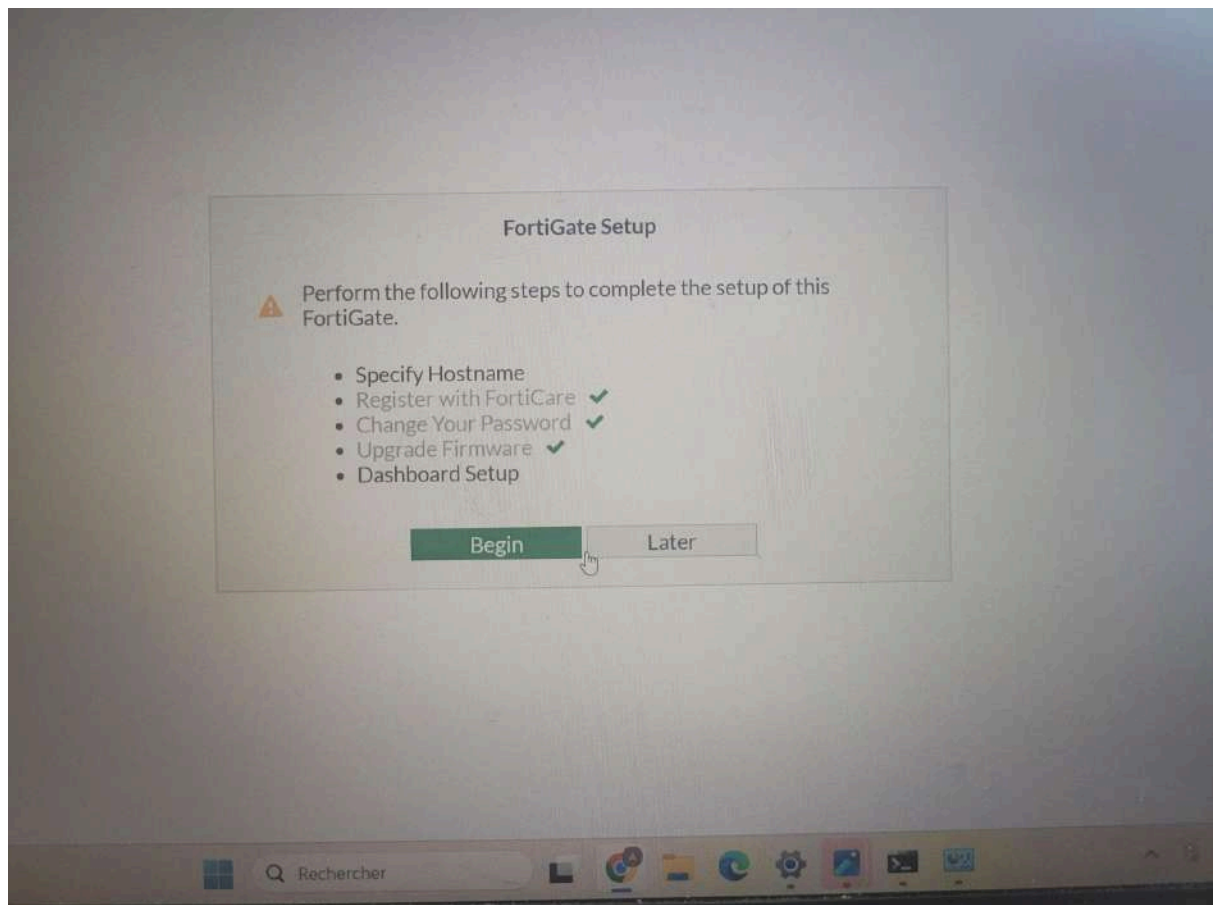




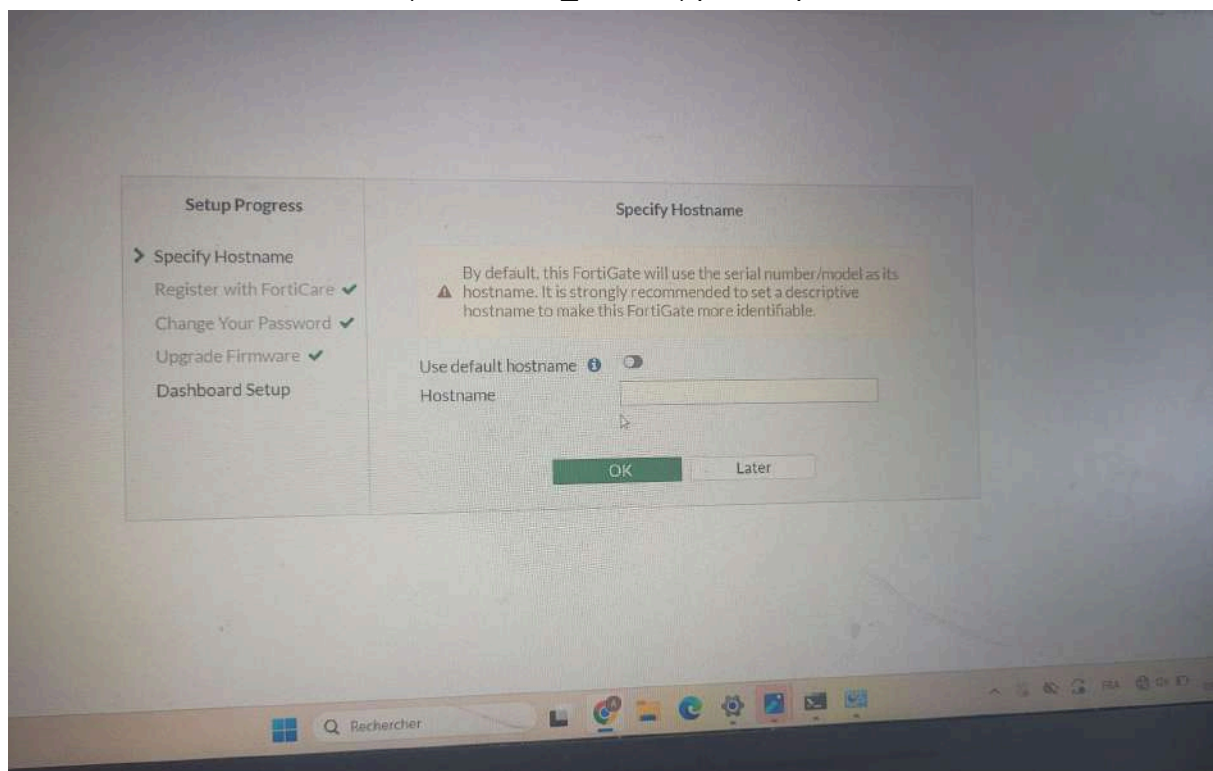
4- sur la nouvelle page,définir un **nouveau mdp** sans remplir la case avec l'**ancien mdp**, puis une nouvelle page s'affiche



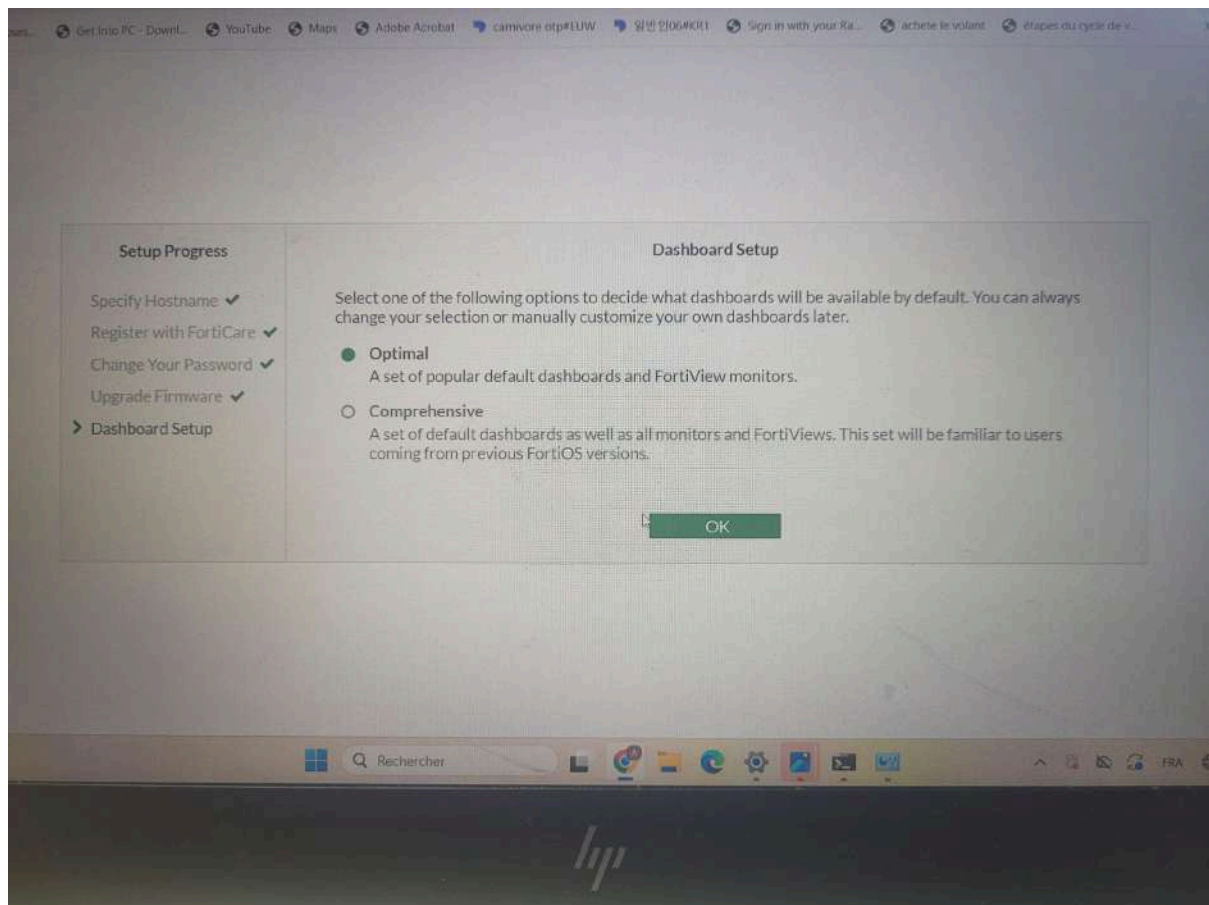
4bis- Une page fortigate setup qui affiche le reste du parametrage à faire, appuyer sur "Begin"



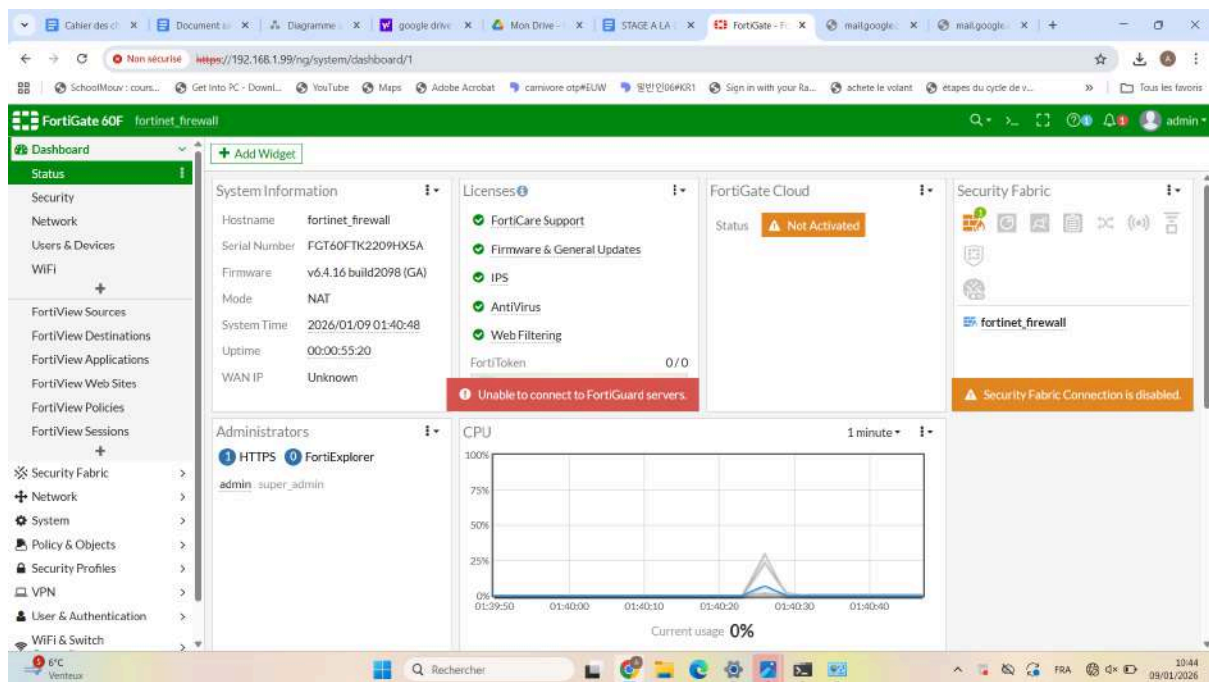
5- il faut choisir un **hostname** (ex: Fortinet_Firewall) puis cliquez sur ok

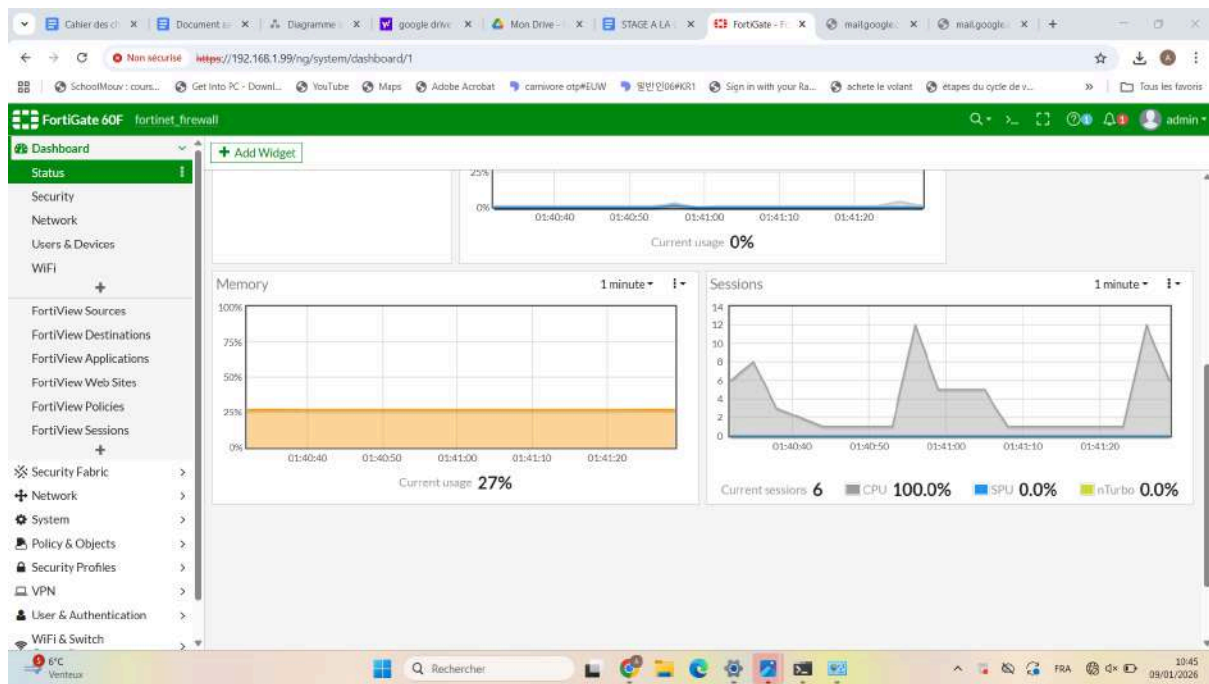


6- Pour le **dashboard setup** laisser l'option **optimal** et cliquer sur ok

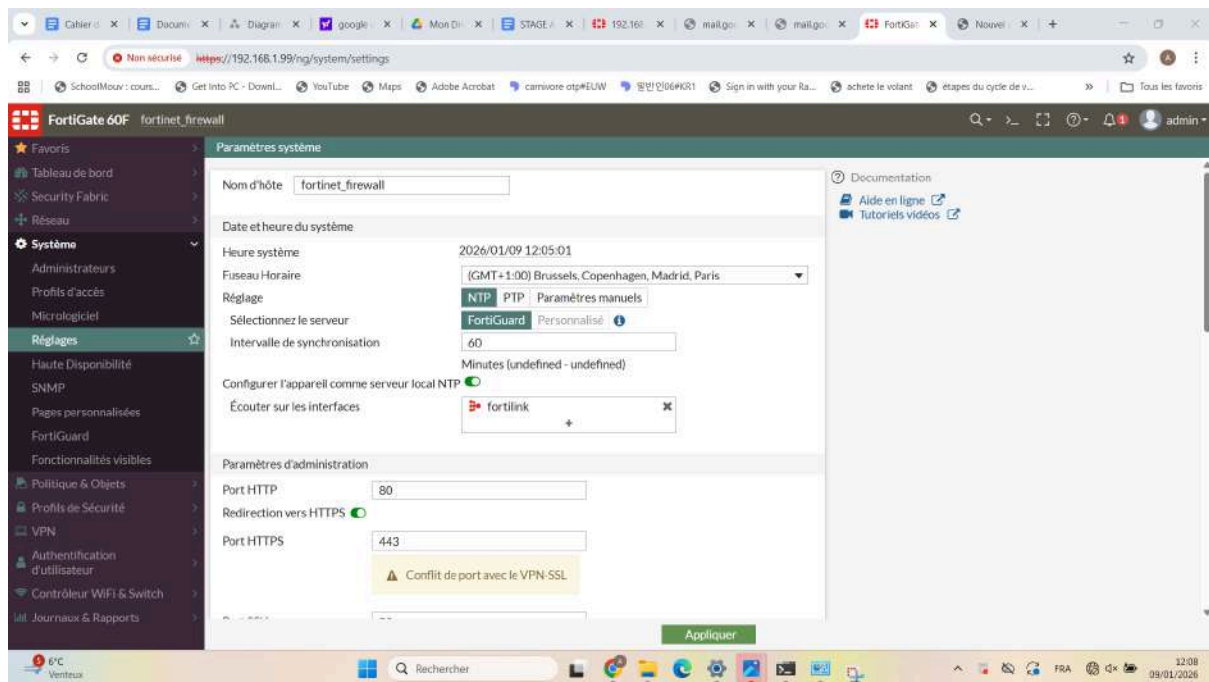


7-Le paramétrage est fini on a maintenant accès aux fonctionnalité du site

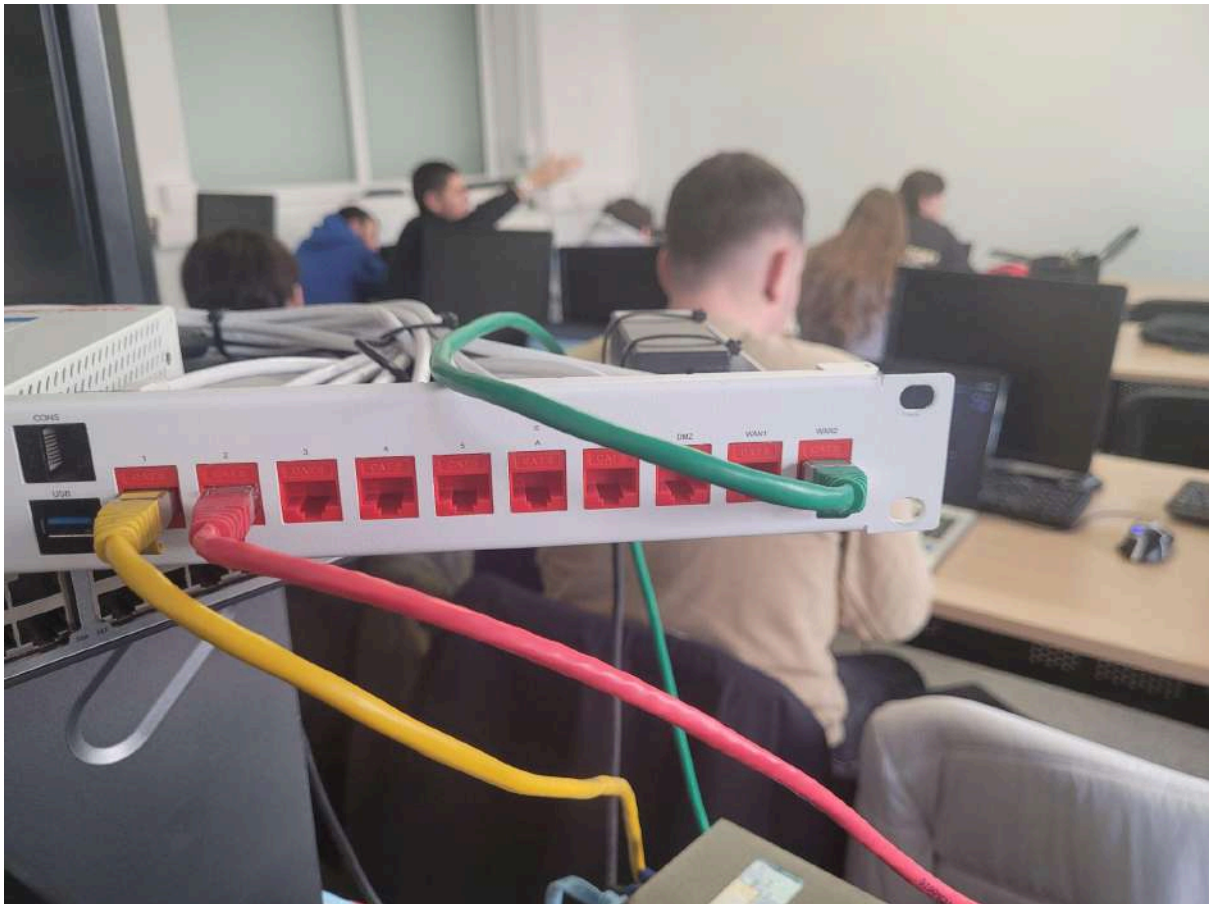




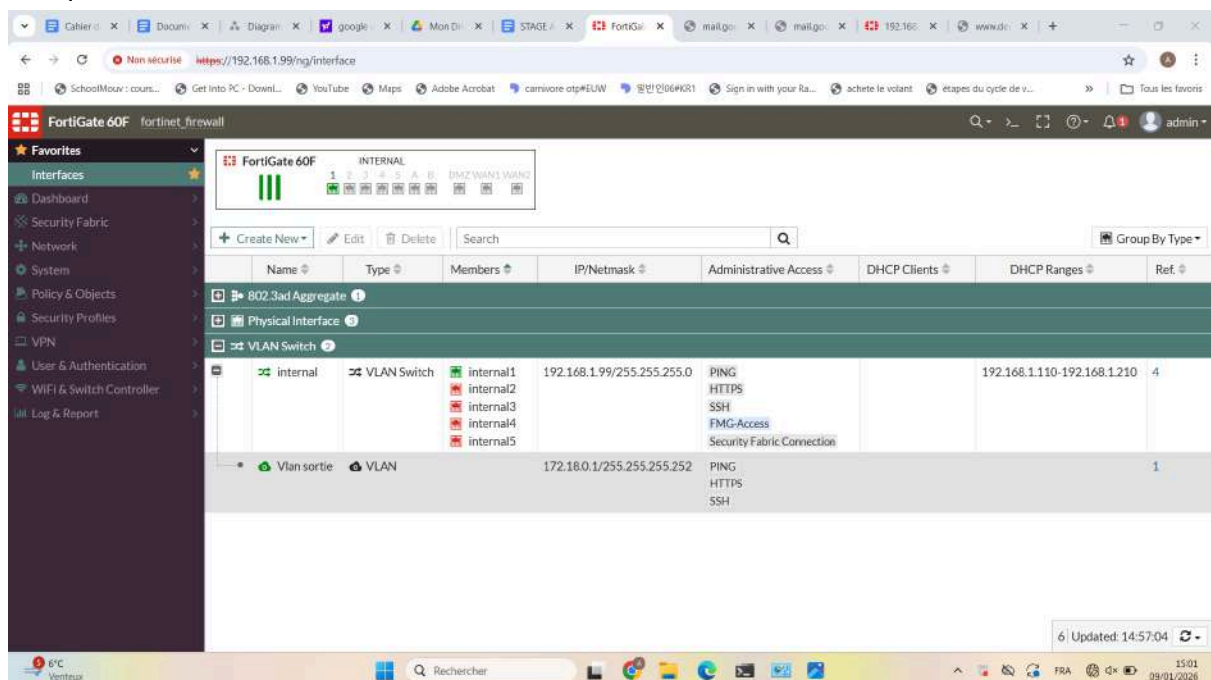
-Dans le dashboard aller dans **système** puis **réglage** et juste modifier le Fuseau horaire sur l'heure de paris et appliquer



Notre répartition des Cable RJ45 sur les ports du fortigate ressemble à ceci :

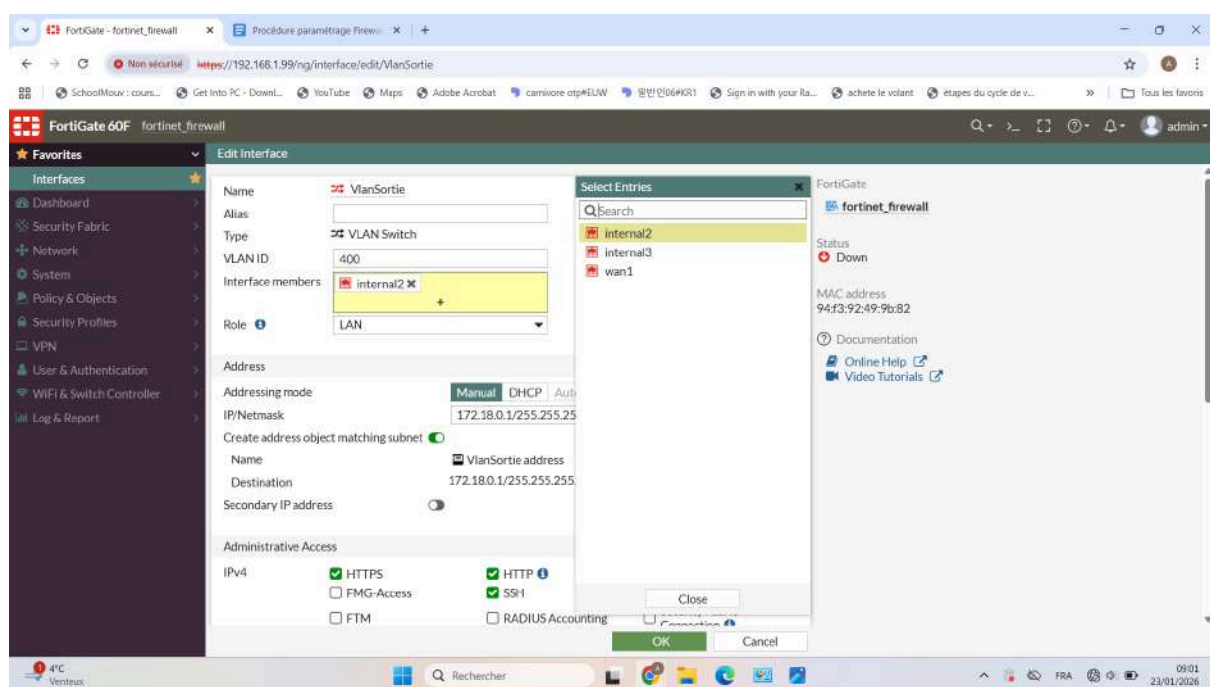
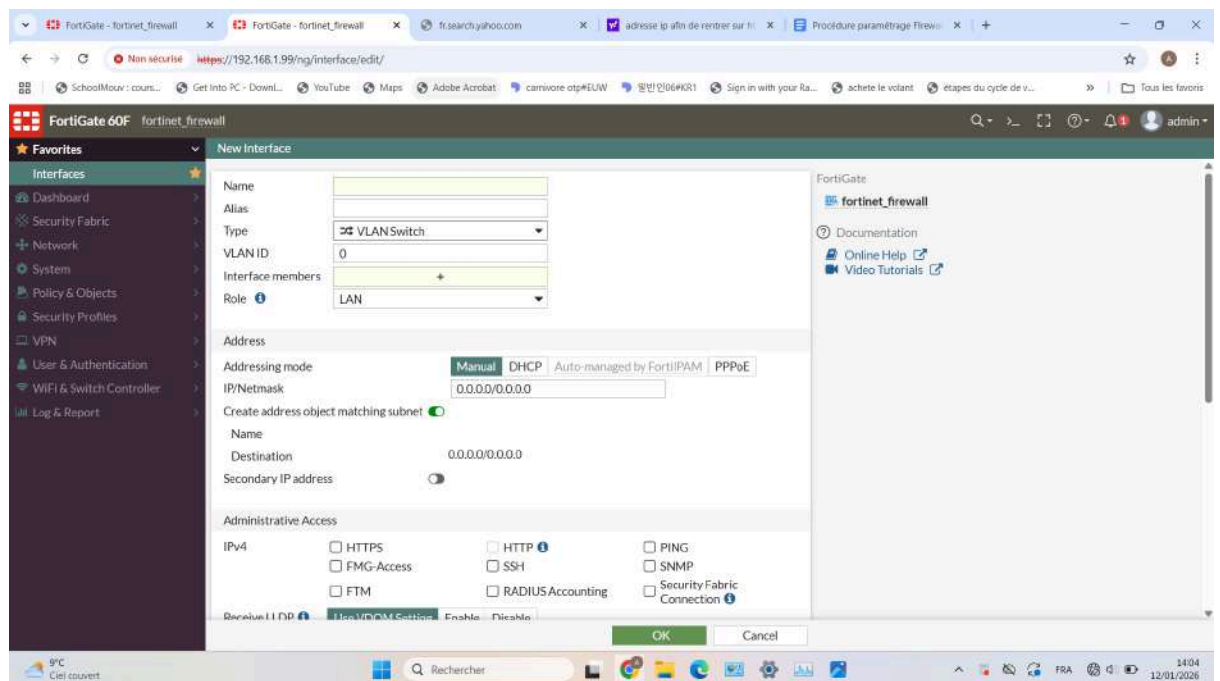


- Revenir sur interfaces puis il faut créer un vlan switch :
- cliquer sur **create new**



- définir le type sur **"Vlan switch"**
- choisir un numéro de vlan pour **"VLAN ID"** ex : 400
- définir le nom dans **"Name"** ex Vlan sortie

- dans interface members cliquer sur le “+” pour ajouter une interface, on choisira l’interface qui connecte le cable Rj 45 au port 2 du fortigate donc interface “internal 2”



-administrative accès : cocher les cases pour lequel on veut autoriser l'administration du fortinet soit **SSH**, **HTTPS** et **PING** il ne sera pas possible d'administrer fortinet pour les cases non cochées.

Name  Vlan sortie address

Destination 172.18.0.1/255.255.255.252

Secondary IP address ☐

Administrative Access

IPv4 ☒ HTTPS ☐ HTTP  ☒ PING

☐ FMG-Access ☒ SSH ☐ SNMP

☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection 

☐ DHCP Server

-Définir la nouvelle adresse IP avec le masque sur la même page

Address

Addressing mode **Manual** DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask 172.18.0.1/255.255.255.252

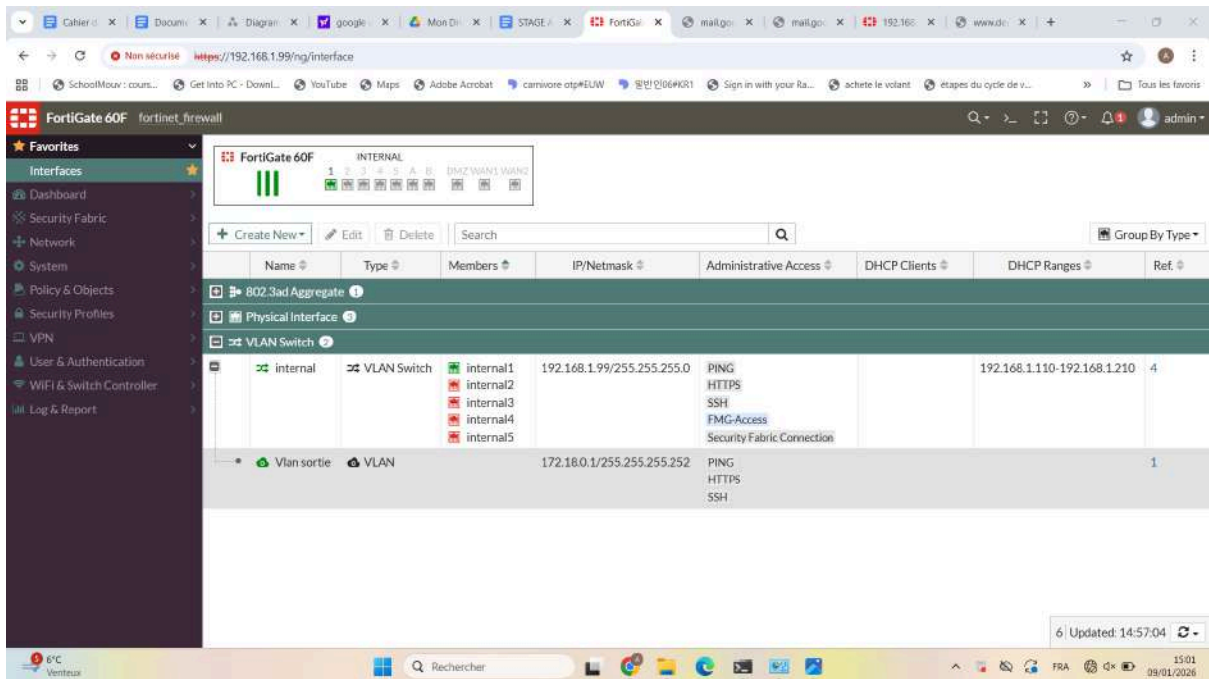
Create address object matching subnet ☒

Name  Vlan sortie address

Destination 172.18.0.1/255.255.255.252

-Si jamais il est nécessaire de supprimer une interface car elle est mal paramétré voici la manipulation à suivre :

Revenir sur la page **interface** puis dans la colonne ref cliquer sur le chiffre correspondant à la colonne à supprimer, une nouvelle page s'affiche

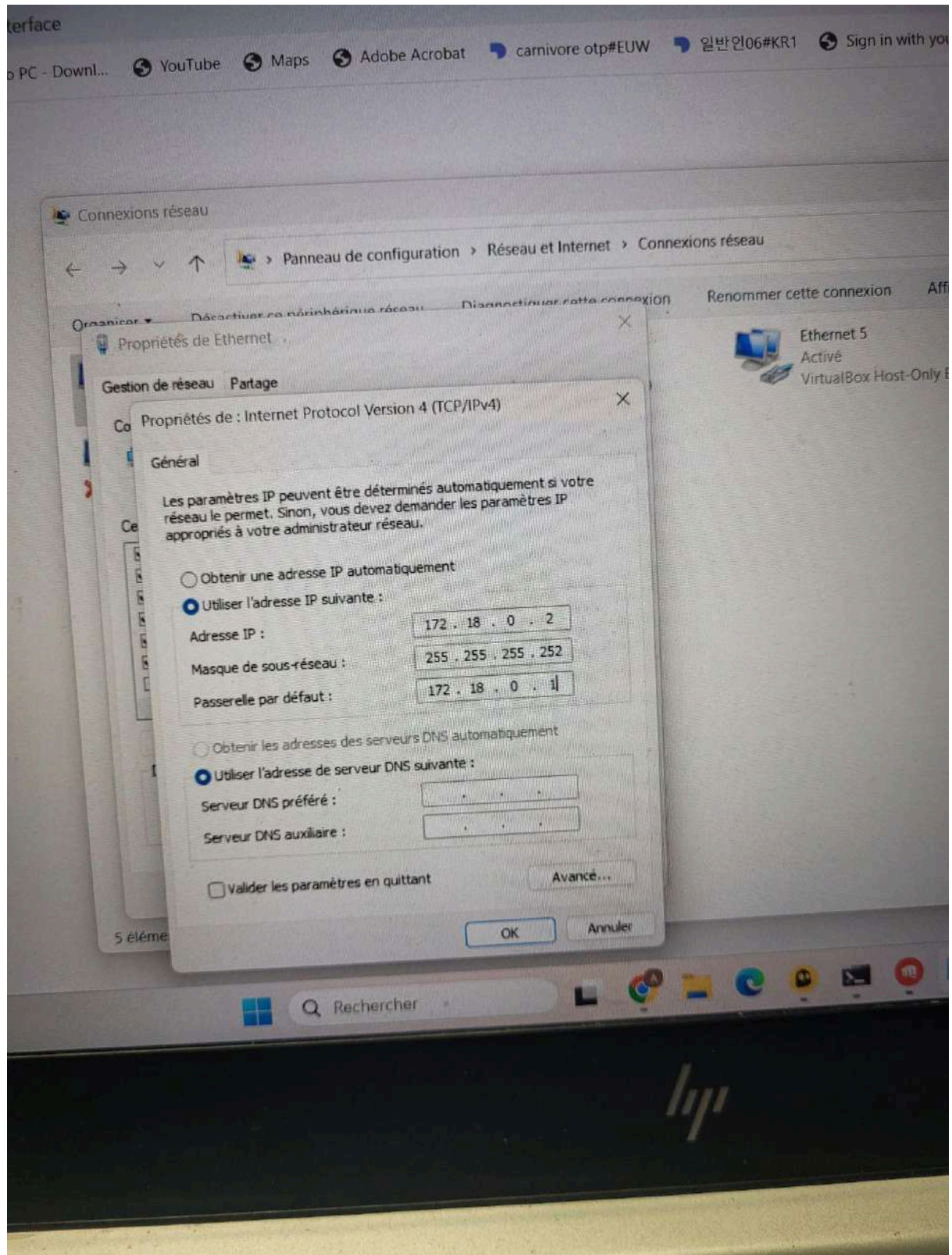


Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate							
Physical Interface							
VLAN Switch							
internal	VLAN Switch	internal1 internal2 internal3 internal4 internal5	192.168.1.99/255.255.255.0	PING HTTPS SSH FMG-Access Security Fabric Connection		192.168.1.110-192.168.1.210	4
Vlan sortie	VLAN		172.18.0.1/255.255.255.252	PING HTTPS SSH			1

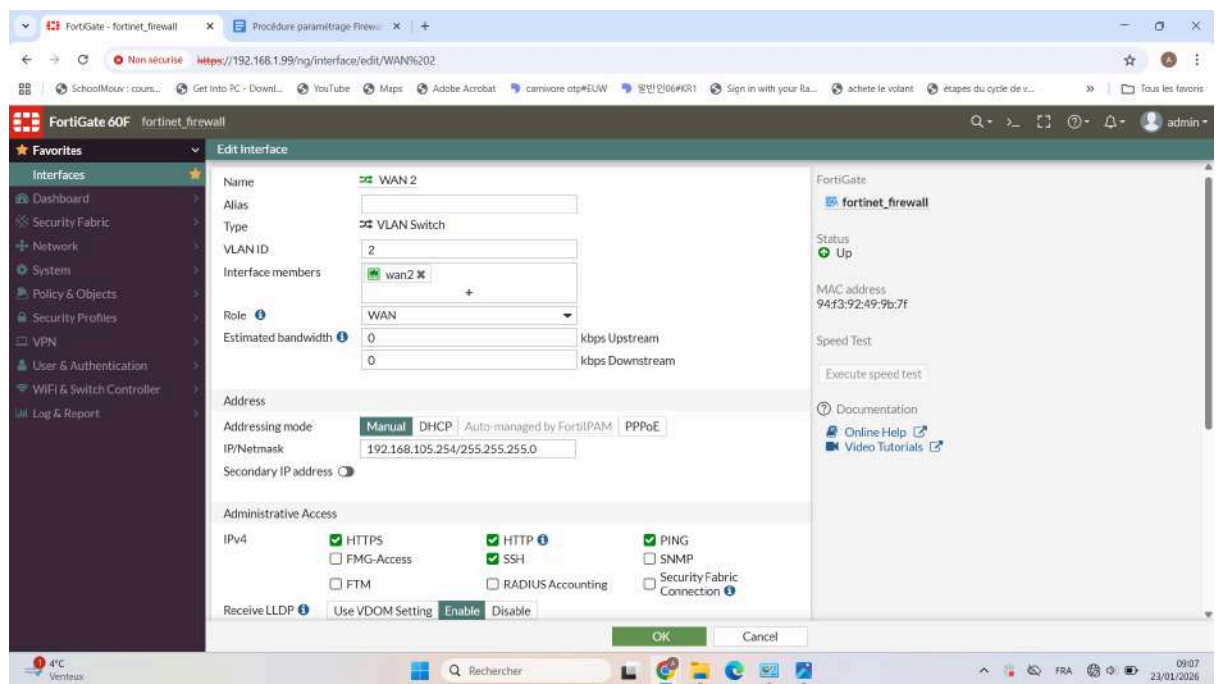
-appuyer sur **delete**, si jamais le bouton n'est pas cliquable, c'est que l'interface n'est pas "disabled et dans ce cas il faudra edit l'interface puis en bas de la page désactiver l'interface

Créer une autre interface WAN :

pour le PC qui se connectera au WAN 2 la paramétrage sera ceci :



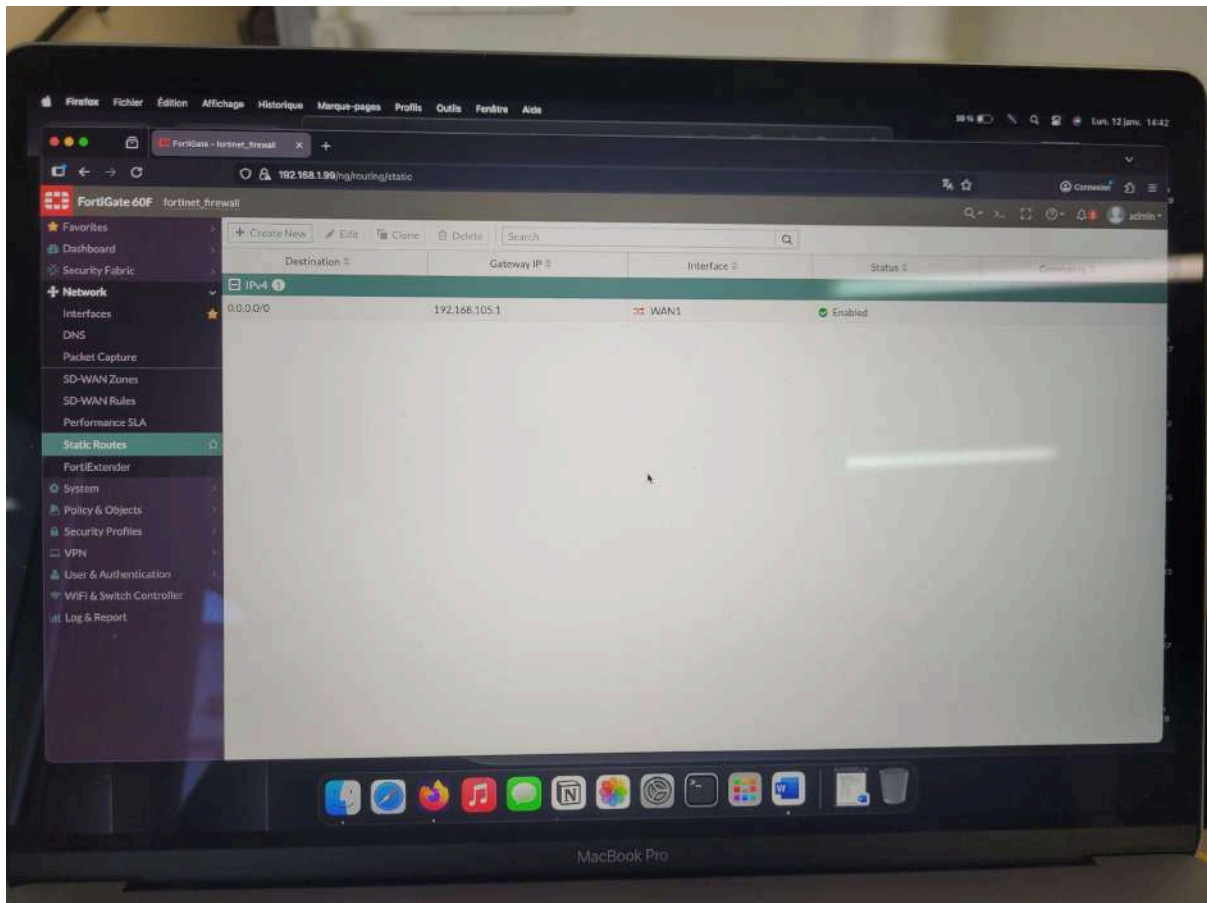
- définir le type sur **"VLAN Switch"**
- choisir un numéro de vlan pour **"VLAN ID"** ex : 2
- définir le nom dans **"Name"** ex WAN 2
- dans interface members cliquer sur le "+" pour ajouter une interface, on choisira l'interface qui connecte le cable Rj 45 au port WAN 2 du fortigate donc interface **"WAN 2"**
- administrative accès : cocher les cases pour lequel on veut autoriser l'administration du fortinet soit **SSH, HTTPS** et **PING** il ne sera pas possible d'administrer fortinet pour les cases non cochées.
- Définir la nouvelle adresse IP 192.168.105.254



Une fois les 2 interfaces créées, tester si fortinet les detecte

-Il faut maintenant paramétrer la passerelle :

- Depuis le **dashboard** aller dans **"Network"** puis **"Static Routes"**
- cliquer sur **"Create new"** (IPv4 Static route)



-Une nouvelle page s'affiche pour paramétrer la passerelle

Remplissez les champs suivants :

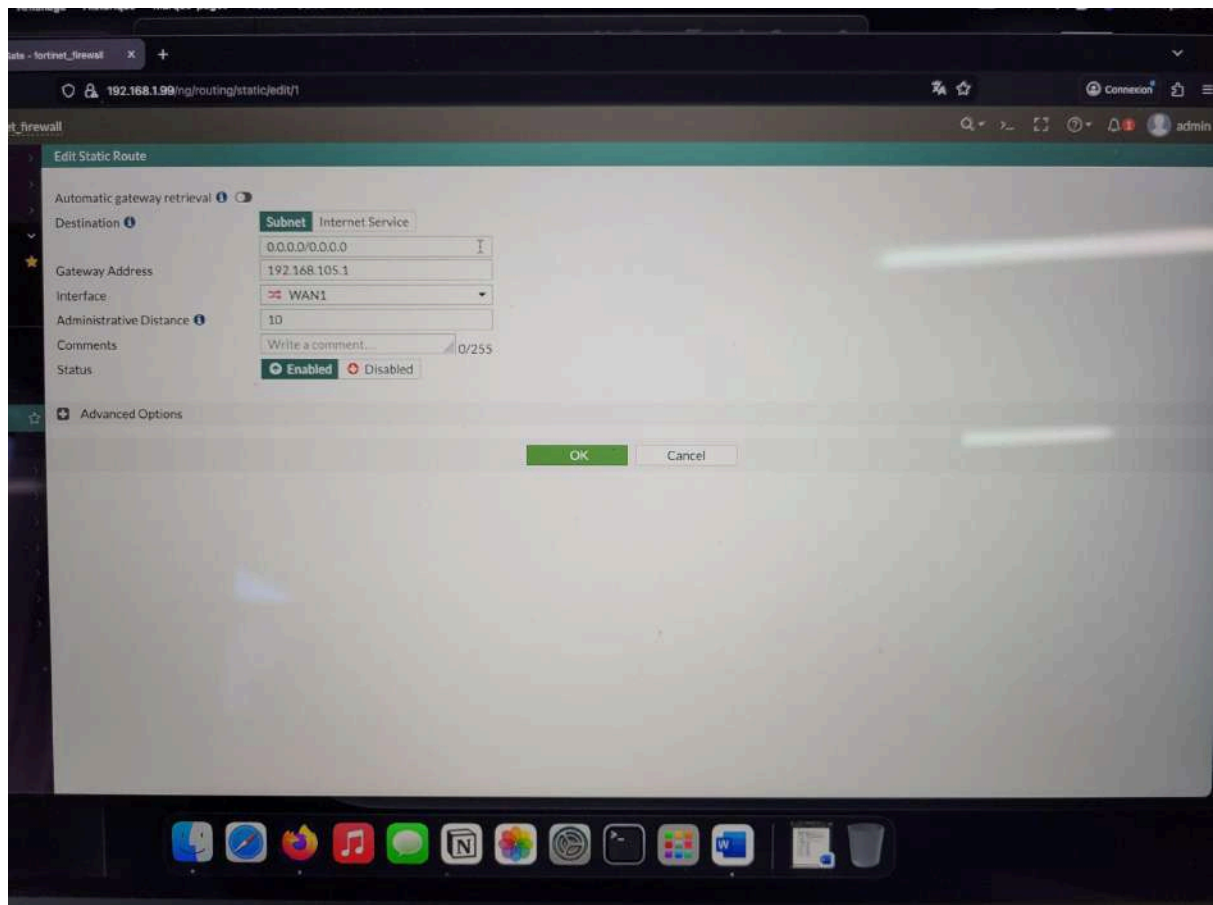
-Destination : Laisser `0.0.0.0/0.0.0.0` (ceci définit la route par défaut pour tout le trafic inconnu).

-Gateway IP : Entrer l'adresse IP du routeur ou de la box internet (ex: `192.168.1.254`).

-Interface : Sélectionner l'interface connectée à ce routeur (souvent `wan1` ou `wan2`).

-Administrative Distance : Laisser par défaut (10) sauf si vous gérez plusieurs liens redondants.

Cliquez sur **OK**.

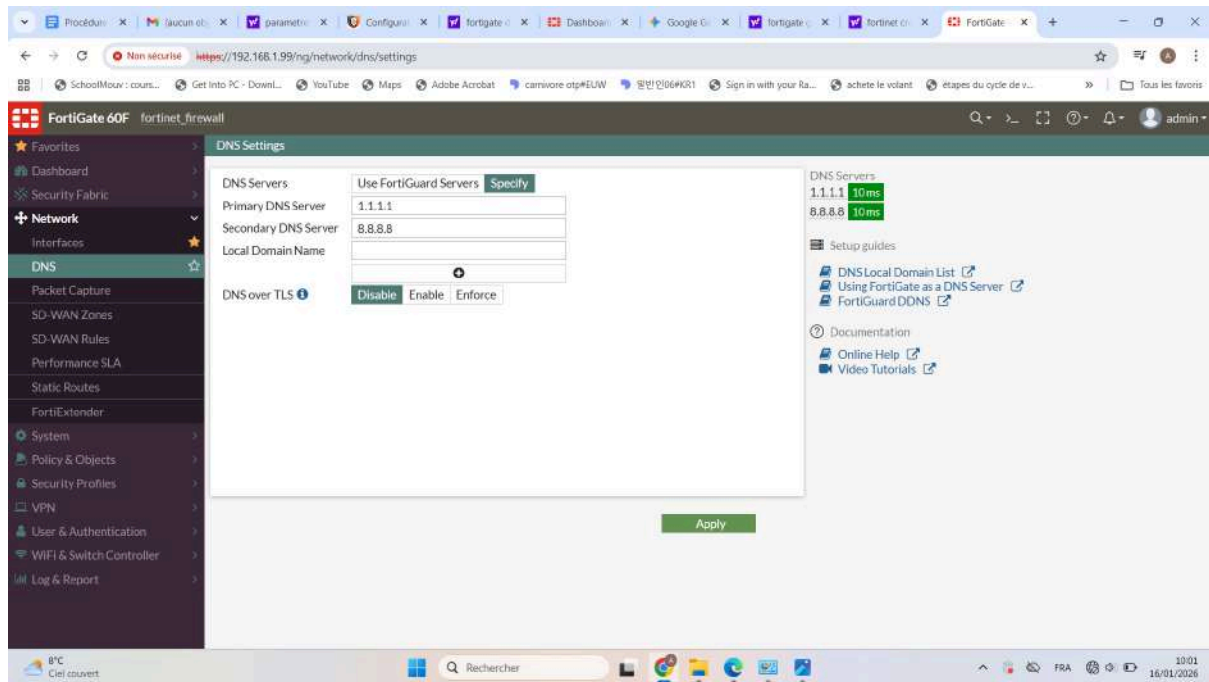


-Paramétrage du DNS :

- depuis le dashboard aller dans “**Network**” puis “**DNS**”
- cliquer sur “**specify**”
- Mettre l’IP du serveur DNS:
 - Primary DNS server** : 1.1.1.1 (IP de CLOUDFLARE)
 - Secondary DNS server** : 8.8.8.8 (IP de GOOGLE)

Pour “**Local domain Name**” ce n’est pas obligatoire de remplir, il faut le faire si on a un domaine interne

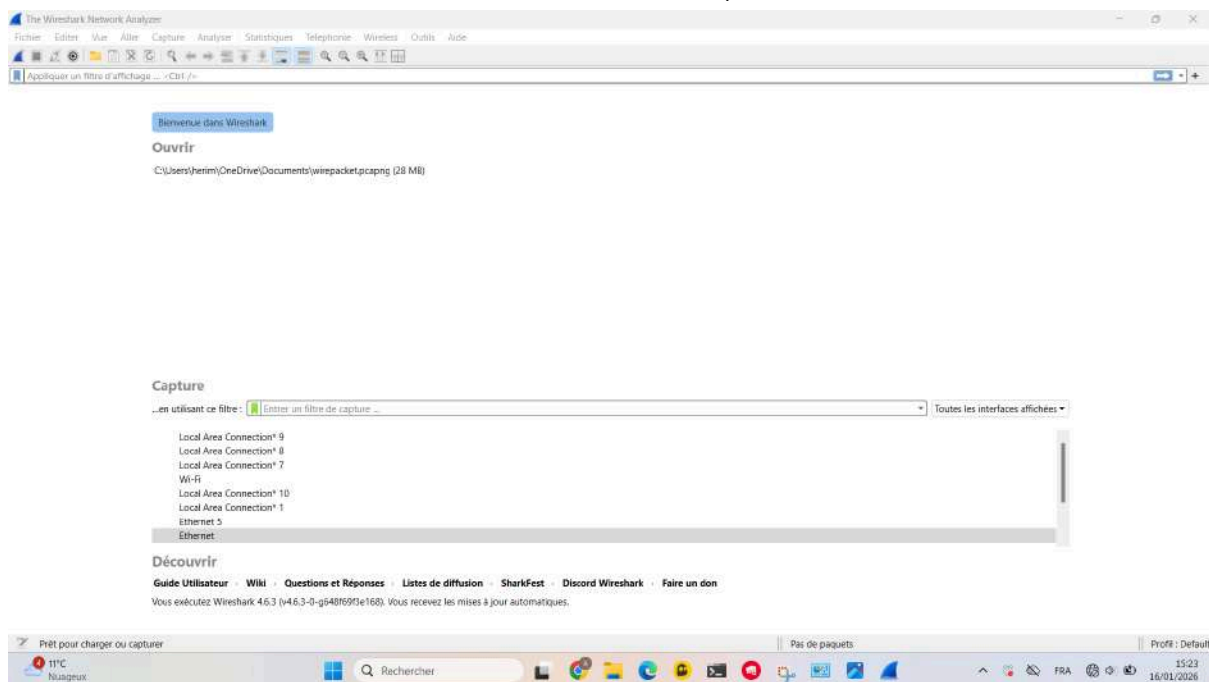
Et enfin cliquer sur “**Apply**”



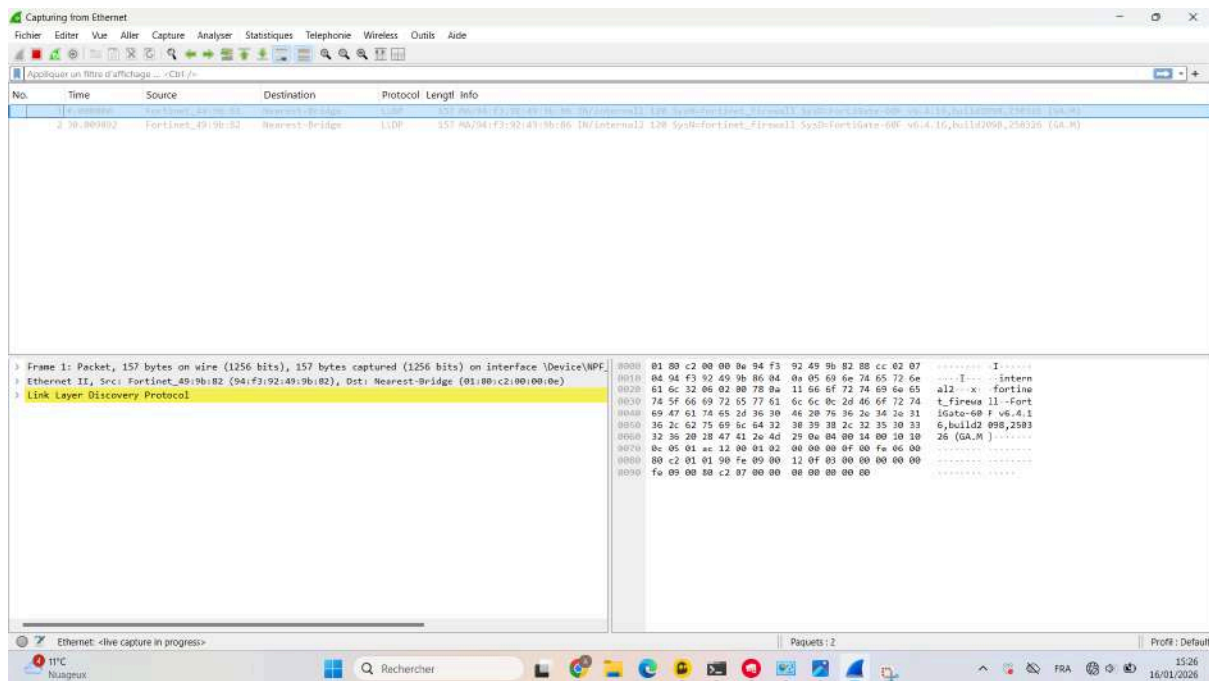
On va maintenant faire des test ping entre les appareils pour voir si tout est est connecté entre :

-Commencer par connecter le PC 2(le PC deux et le relier avec un cable rj45 à la box, le pc2 il faudra modifier la carte réseau du pc2 et définir son ip comme celle de la box
192.168.105.1

-pour analyser les trames qui passent entre les 2 ip des PC on peut utiliser Wireshark : ouvrir wireshark et choisir l'ethernet correspondant l'ip modifié du PC parmi les option(dans notre cas on a modifié ethernet sur la carte réseau)



Une nouvelle page s'affiche avec les trame affichés



pour afficher les trame il faut ouvrir un cmd puis ping l'ip de l'autre PC

```

C:\WINDOWS\system32\CMD x + v
C:\Users\herim>ping 172.18.0.1

Envoi d'une requête 'Ping' 172.18.0.1 avec 32 octets de données :
Réponse de 172.18.0.1 : octets=32 temps<1ms TTL=255
Réponse de 172.18.0.1 : octets=32 temps<1ms TTL=255
Réponse de 172.18.0.1 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 172.18.0.1:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\herim>ping 192.168.105.254

Envoi d'une requête 'Ping' 192.168.105.254 avec 32 octets de données :
Ctrl+C
^C
C:\Users\herim>ping 192.168.105.1

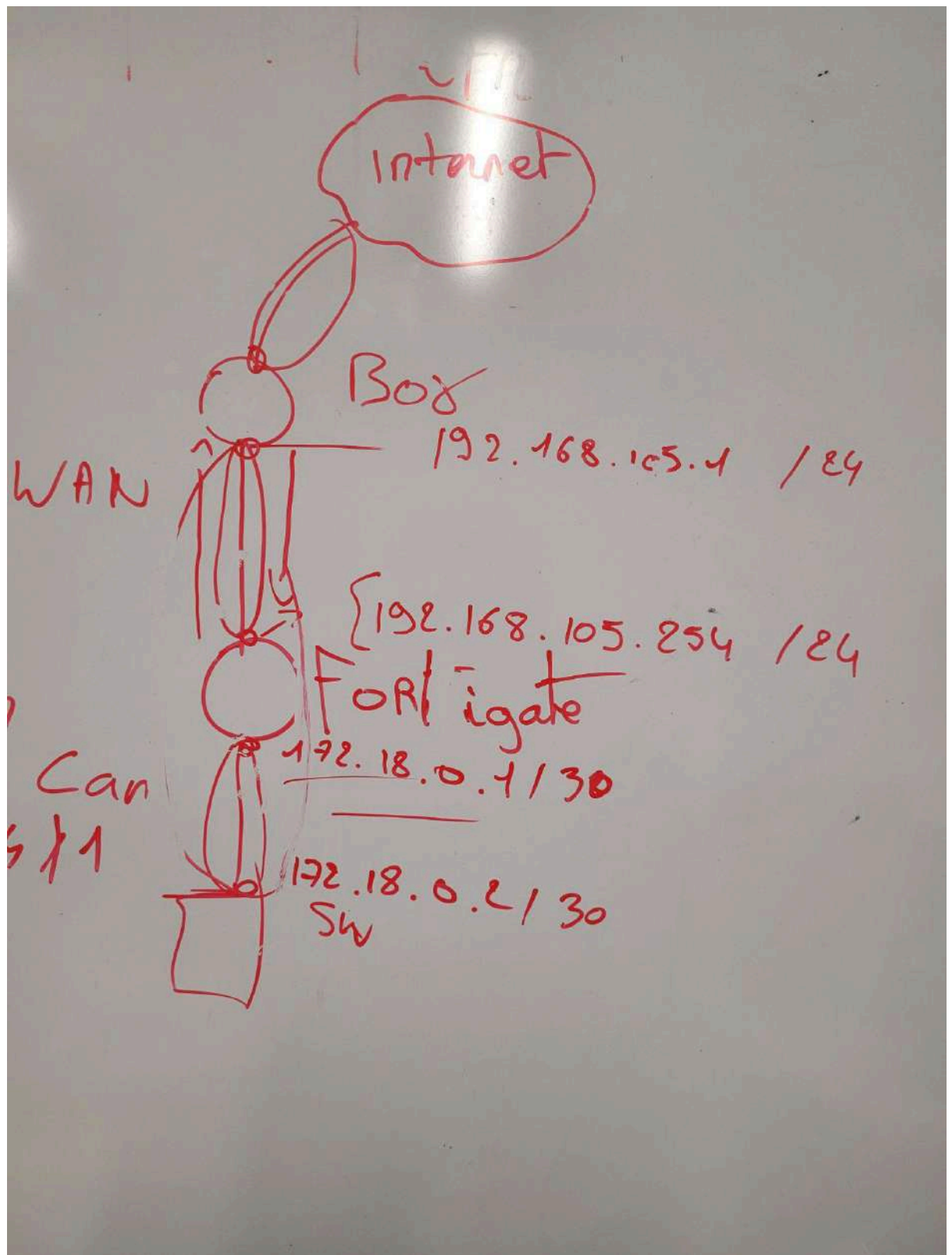
Envoi d'une requête 'Ping' 192.168.105.1 avec 32 octets de données :
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.

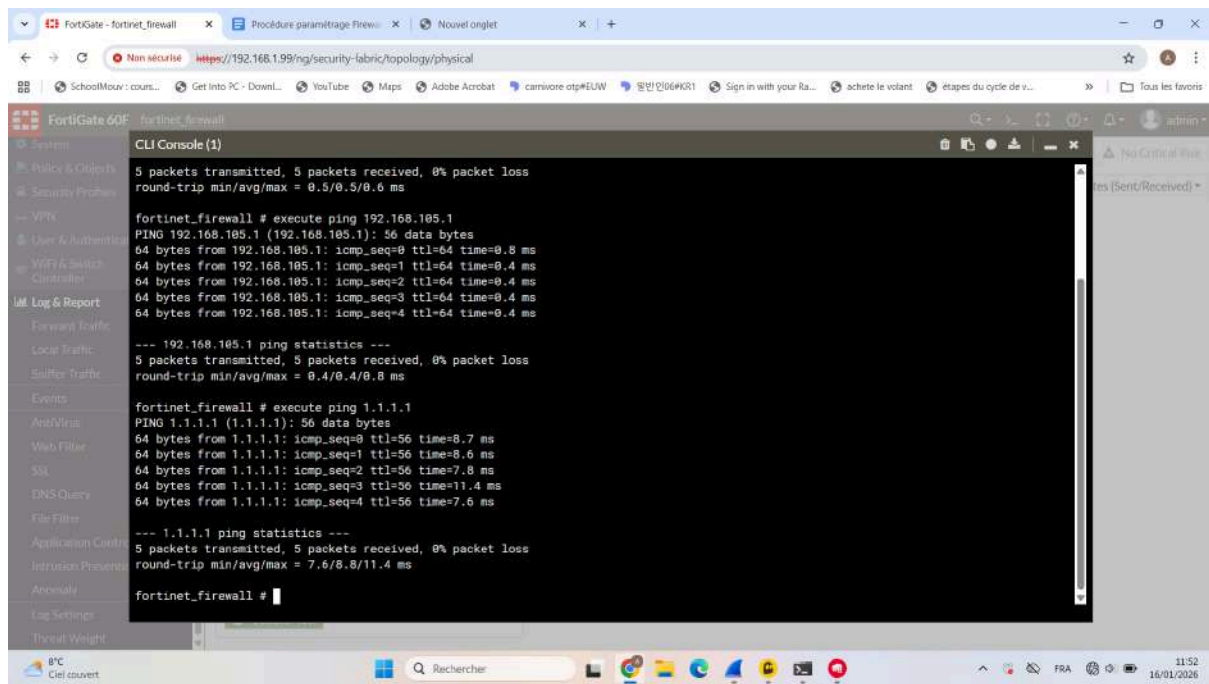
Statistiques Ping pour 192.168.105.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
C:\Users\herim>

```

-On commence par ping depuis notre adresse de fortigate **172.18.0.1** l'adresse de la BOX **192.168.105.1** pour cela depuis le haut de la page du site cliquer sur le signe >_ se situant à côté de la loupe :

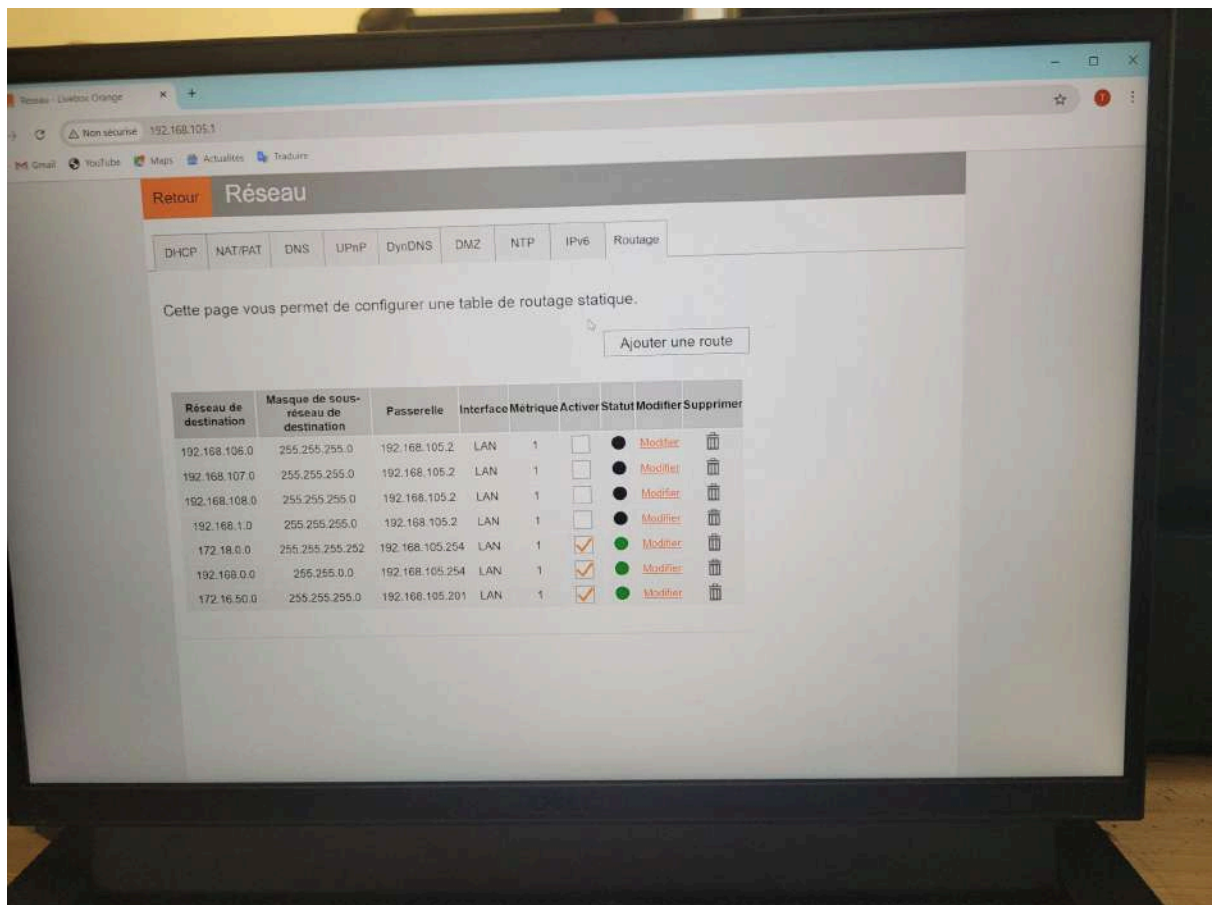
- une console s'ouvre et on ping **192.168.105.1** ça fonctionne
 - on ping maintenant cloudfare **1.1.1.1** ça fonctionne car on a défini la passerelle (la box) **192.168.105.1** pour pouvoir ensuite connaître le chemin jusqu'à internet
- on s'assure que la route de fortigate jusqu'à la box puis internet fonctionne





Pour que cela fonctionne on a modifié les route sur la BOX directement
Pour accéder à la box on se connecte au PC 2 puis on va sur internet et dans la
barre de recherche on met l'ip de la box 192.168.105.1

Il ne reste que les test à faire



On veut maintenant s'assurer que le routage marche dans le sens inverse, du poste **172.18.0.2** jusqu'à fortigate (dont on modifie L'IP pour le pc2) puis jusqu'à la box, et enfin internet comme sur le schéma dans la procédure précédemment

-On modifie l'ip du pc sur **172.18.0.2** puis celle du pc2 sur le fortigate et sur wire shark on teste le passage de trame entre les 2.

-On modifie la carte réseau du pc2 et met l'ip **172.18.0.2** pour effectuer les tests et l'IP du pc sur **192.168.1.98**

Important : Désactiver le parefeu des 3 pc pour effectuer les test PING

Si lors des tests le trafic est bloqué dans 1 seul sens cela vient du fait qu'une session ne peut pas être initiée de l'autre côté.

Si le trafic est bloqué dans un seul sens sur votre FortiGate, cela vient généralement du fait qu'une session ne peut pas être ****initiée**** depuis l'autre côté.

Le FortiGate est un pare-feu à état (stateful) : si une règle autorise A vers B, le retour de B vers A est ****automatiquement**** autorisé pour cette session précise. En revanche, si B essaie de parler à A de lui-même, il sera bloqué s'il n'y a pas de règle spécifique.

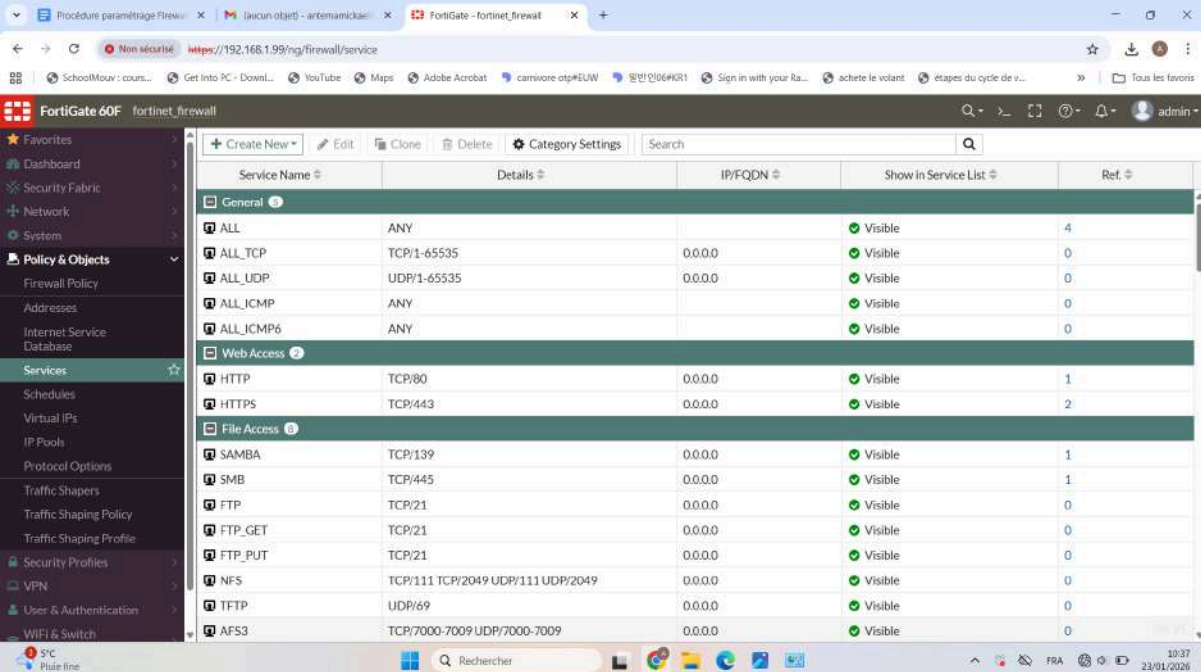
Voici comment débloquent la situation selon votre cas :

1. Créer une règle de retour (Reverse Policy)

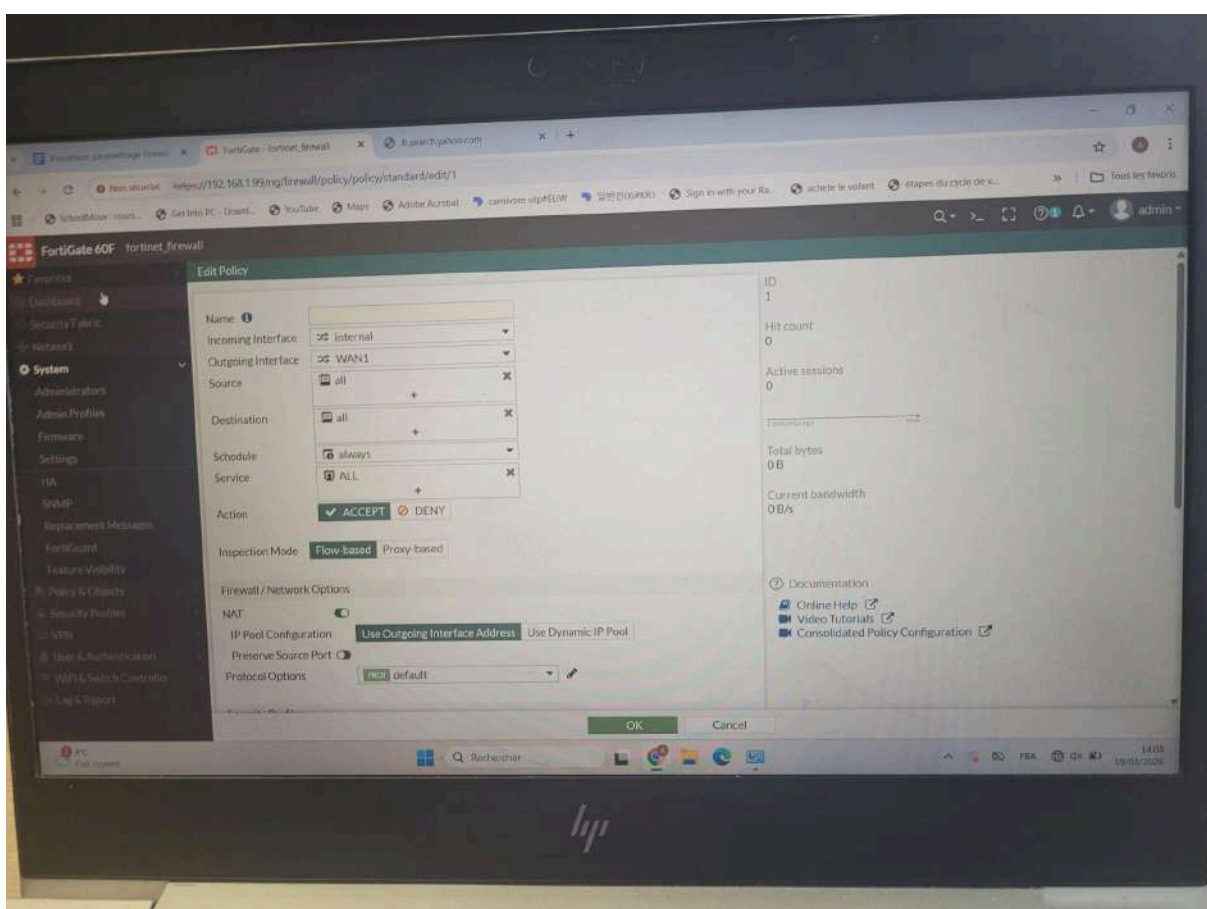
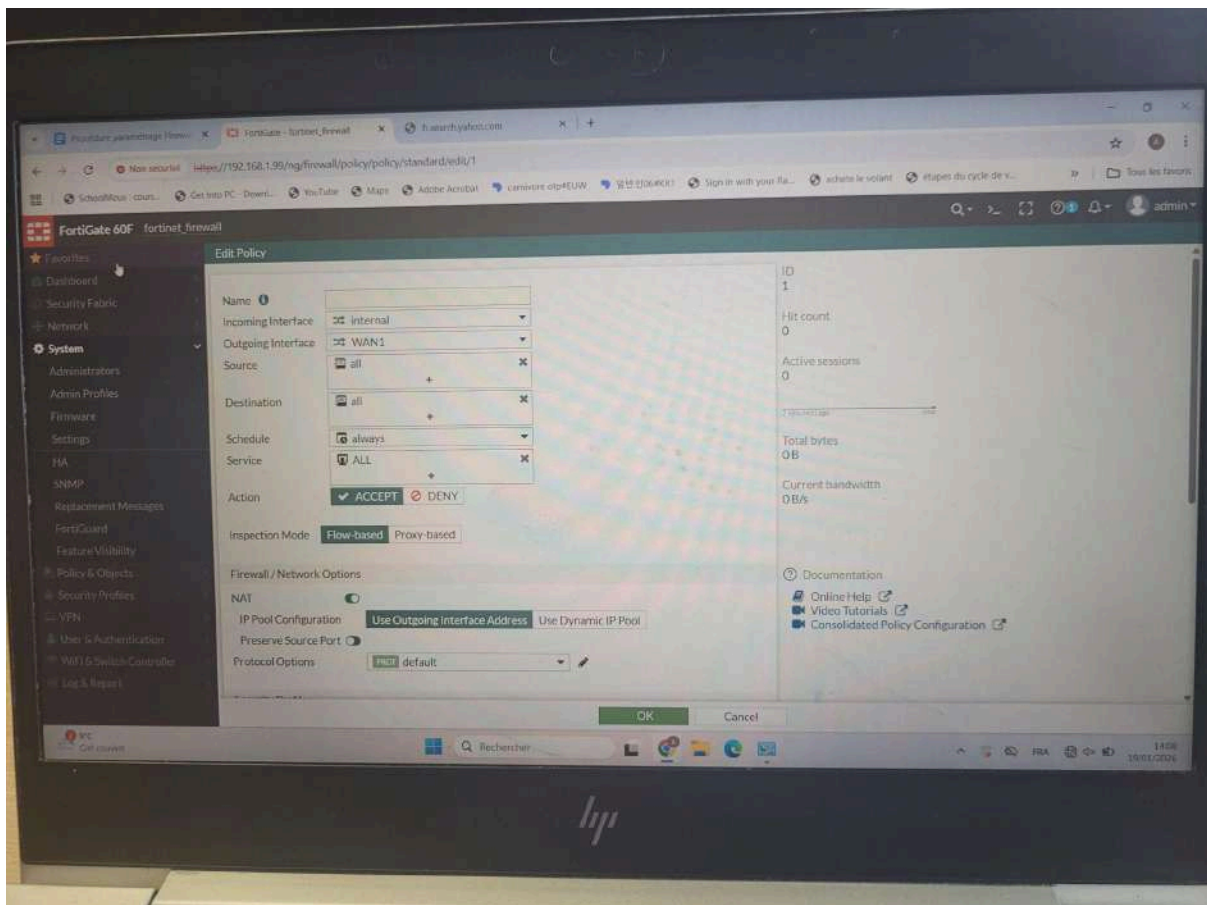
C'est la solution la plus simple si vous voulez que les deux côtés puissent lancer la communication.

****Méthode rapide (Interface Graphique) :****

91. Allez dans ****Policy & Objects**** > ****Firewall Policy****.
2. Faites un clic droit sur la règle existante (celle qui fonctionne dans un sens).
3. Sélectionnez ****Clone Reverse****.
- 3 bis. On peut aussi créer une nouvelle interface à la place
4. La nouvelle règle apparaîtra juste en dessous avec les interfaces, sources et destinations inversées. Elle est créée en mode "Disabled" (désactivée) par défaut.
5. Double-cliquez dessus, donnez-lui un nom et passez son statut à ****Enable****.



Service Name	Details	IP/FQDN	Show in Service List	Ref.
General				
ALL	ANY		Visible	4
ALL_TCP	TCP/1-65535	0.0.0.0	Visible	0
ALL_UDP	UDP/1-65535	0.0.0.0	Visible	0
ALL_ICMP	ANY		Visible	0
ALL_ICMP6	ANY		Visible	0
Web Access				
HTTP	TCP/80	0.0.0.0	Visible	1
HTTPS	TCP/443	0.0.0.0	Visible	2
File Access				
SAMBA	TCP/139	0.0.0.0	Visible	1
SMB	TCP/445	0.0.0.0	Visible	1
FTP	TCP/21	0.0.0.0	Visible	0
FTP_GET	TCP/21	0.0.0.0	Visible	0
FTP_PUT	TCP/21	0.0.0.0	Visible	0
NFS	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	Visible	0
TFTP	UDP/69	0.0.0.0	Visible	0
AFS3	TCP/7000-7009 UDP/7000-7009	0.0.0.0	Visible	0



2. Vérifier l'asymétrie de routage

Si vous avez déjà deux règles (une pour chaque sens) mais que cela ne passe toujours pas, le problème peut être le **"Routage Asymétrique"**. Cela arrive quand le paquet "Aller" passe par le FortiGate, mais que le paquet "Retour" revient par un autre chemin (ou vice versa). Le FortiGate bloque alors le trafic car il ne voit pas la session complète.