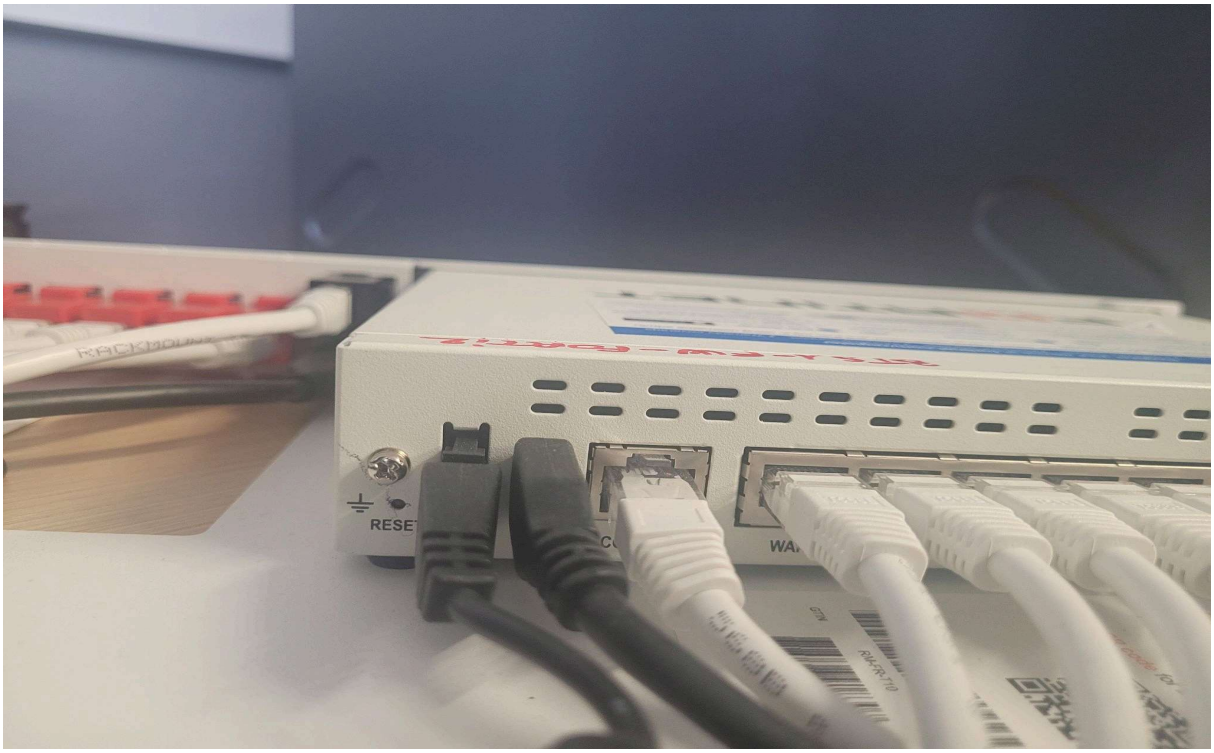
Procédure paramétrage FIrewall

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.

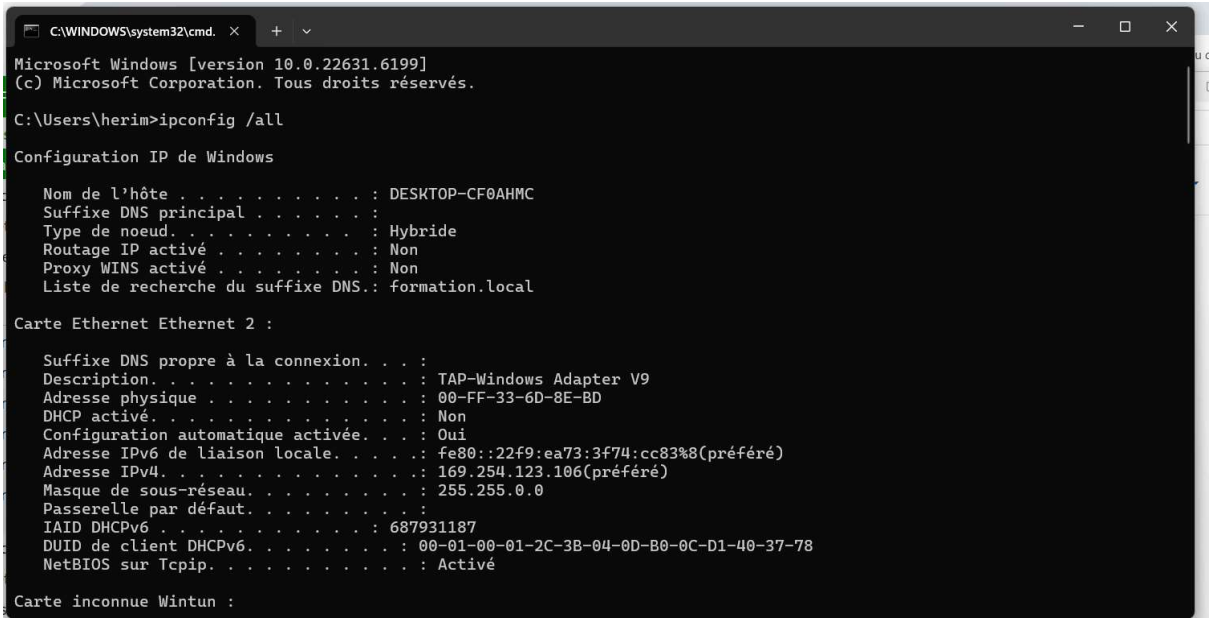


2eme étape se connecter à fortigate :

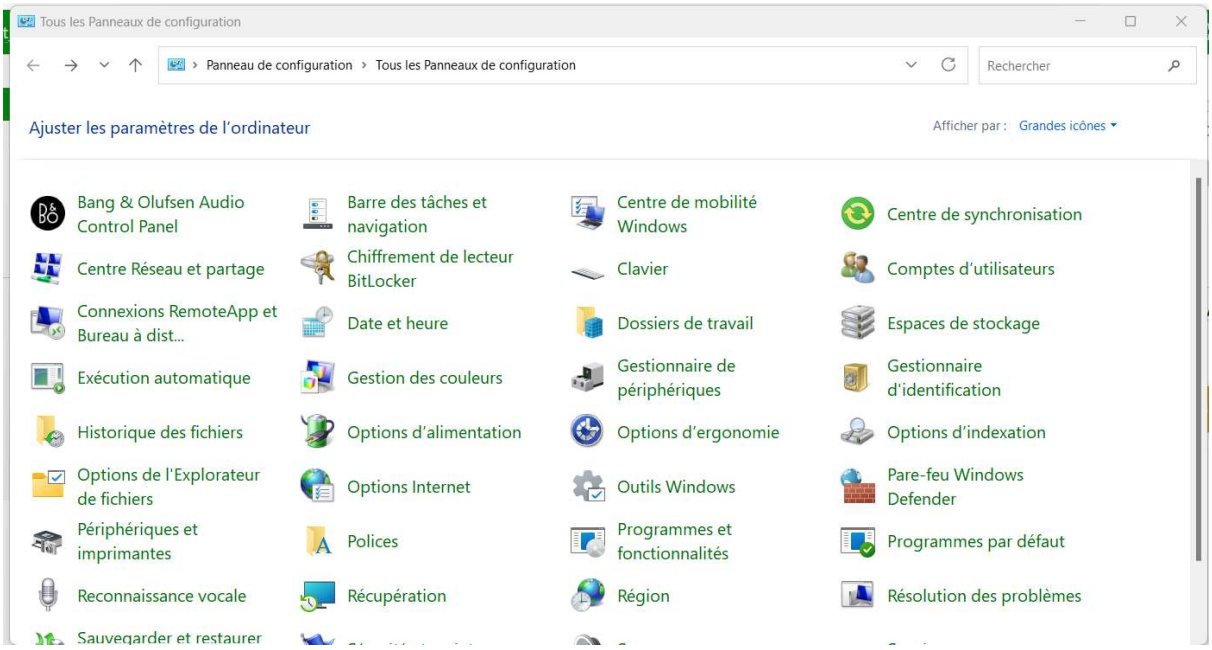
1-Connecter un cable Rj45 au firewall qui sera relié à un PC
2-sur le navigateur saisir l'IP 192.168.1.99, le site est inaccessible

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 :

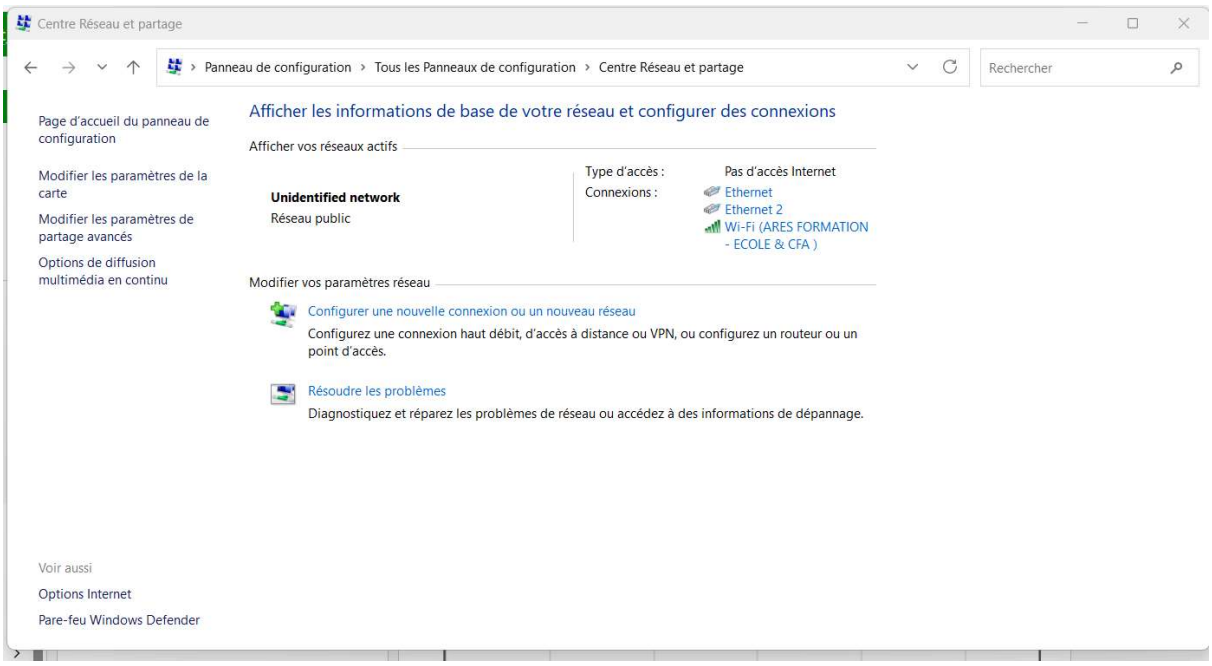
-A l'aide du cmd regarder l'ip du PC



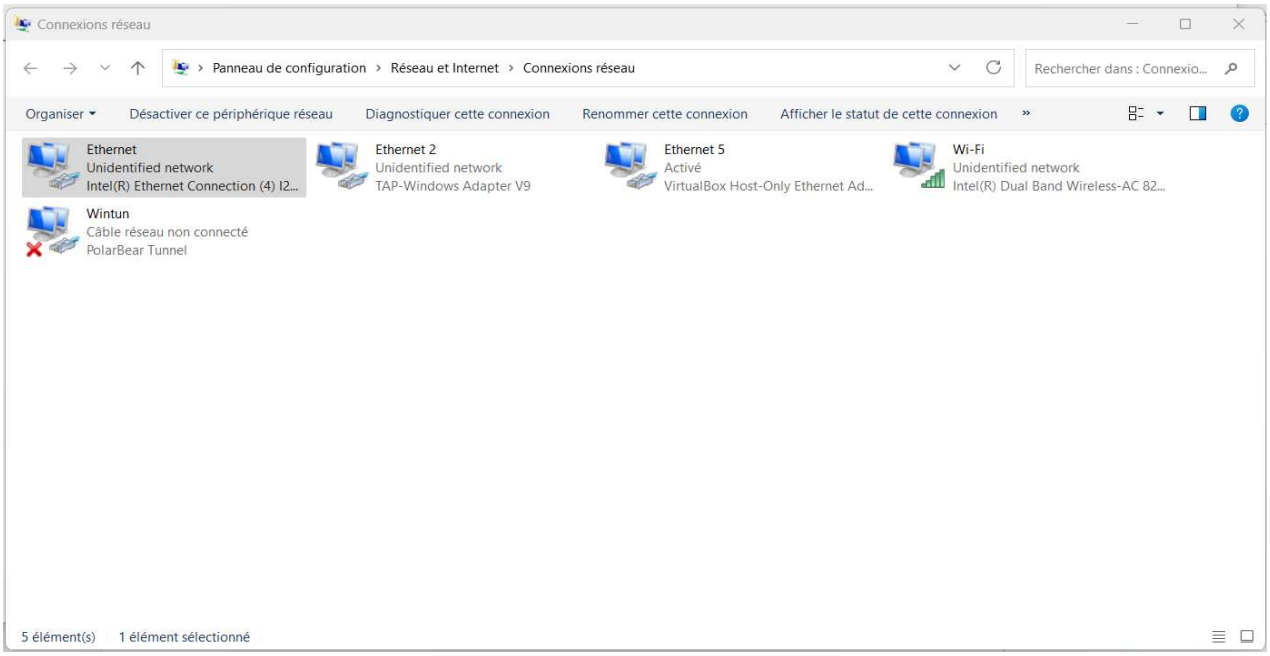
-aller sur le **panneau de configuration**



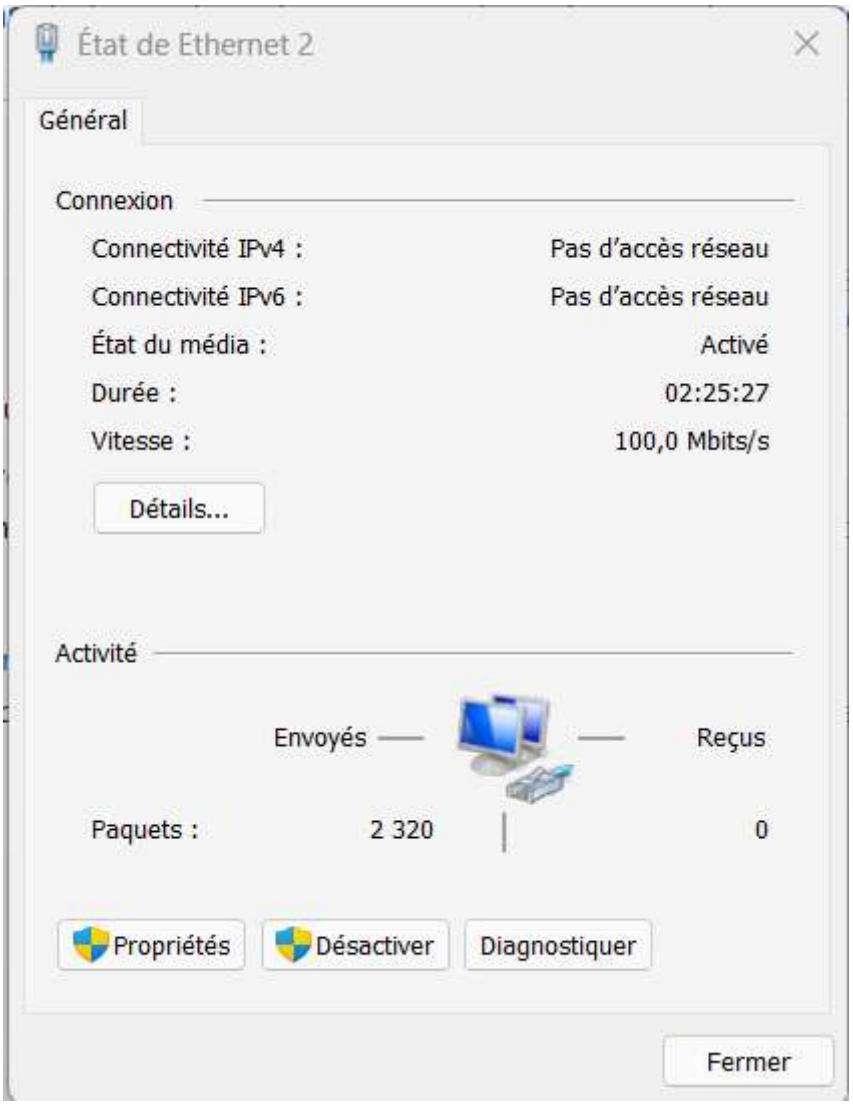
-aller sur le **centre Réseau et partage**



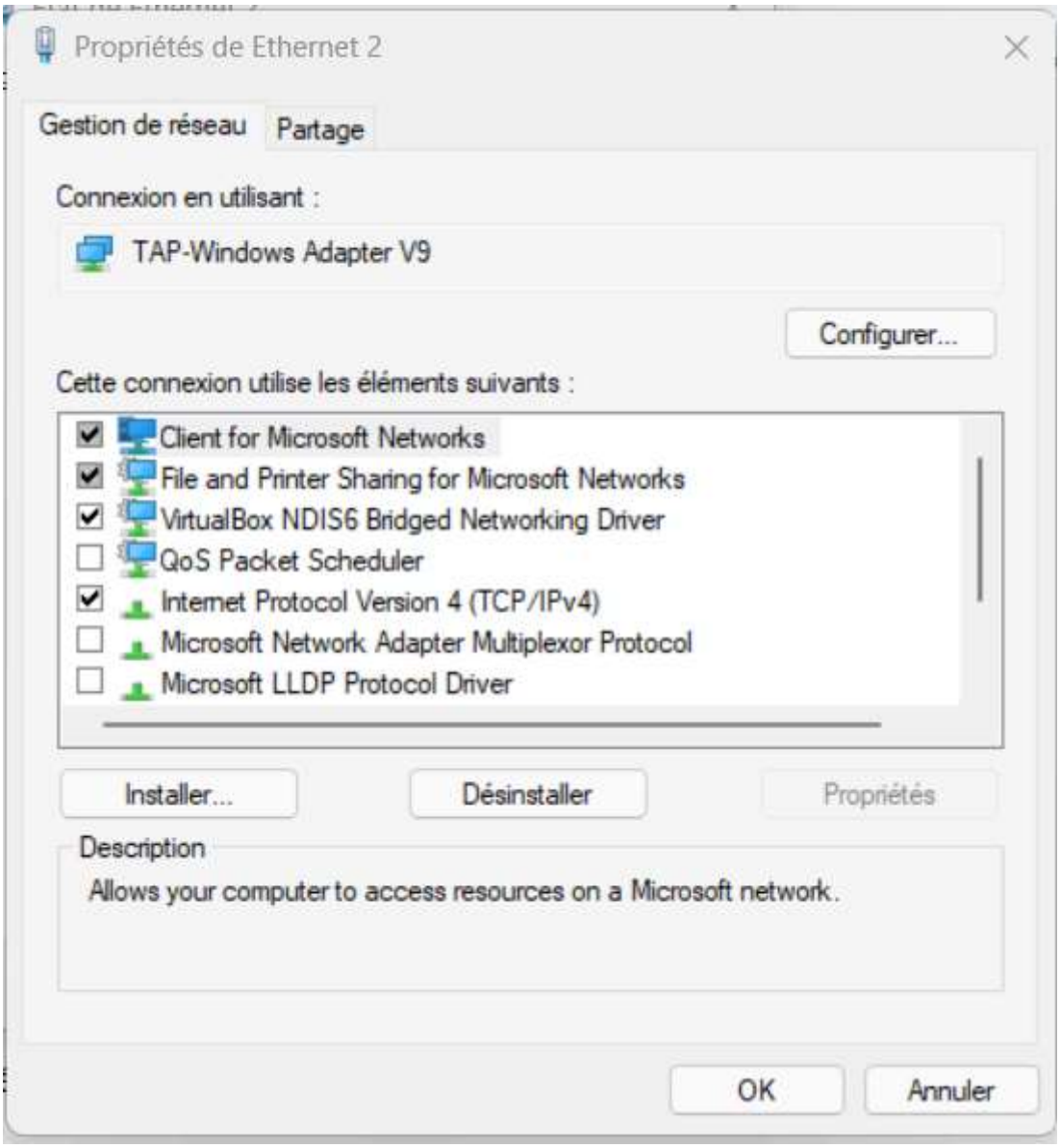
- Sur la partie gauche de l'écran cliquer sur **modifier les paramètres de la carte**, une nouvelle pas s'affiche



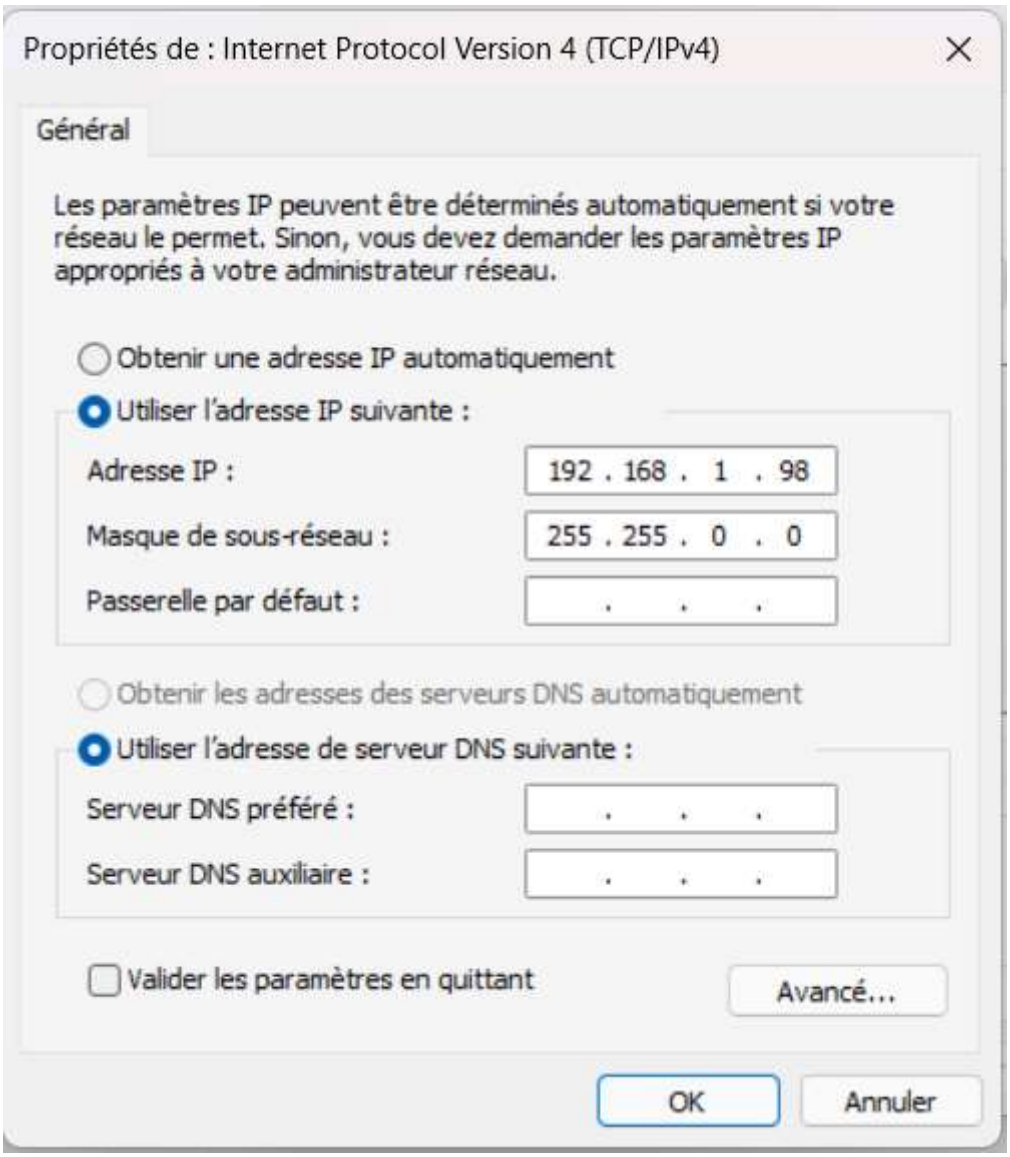
-choisir la carte ethernet correspondante pour changer son IP, une page état de ethernet s'affiche



- cliquer sur les **propriétés**



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



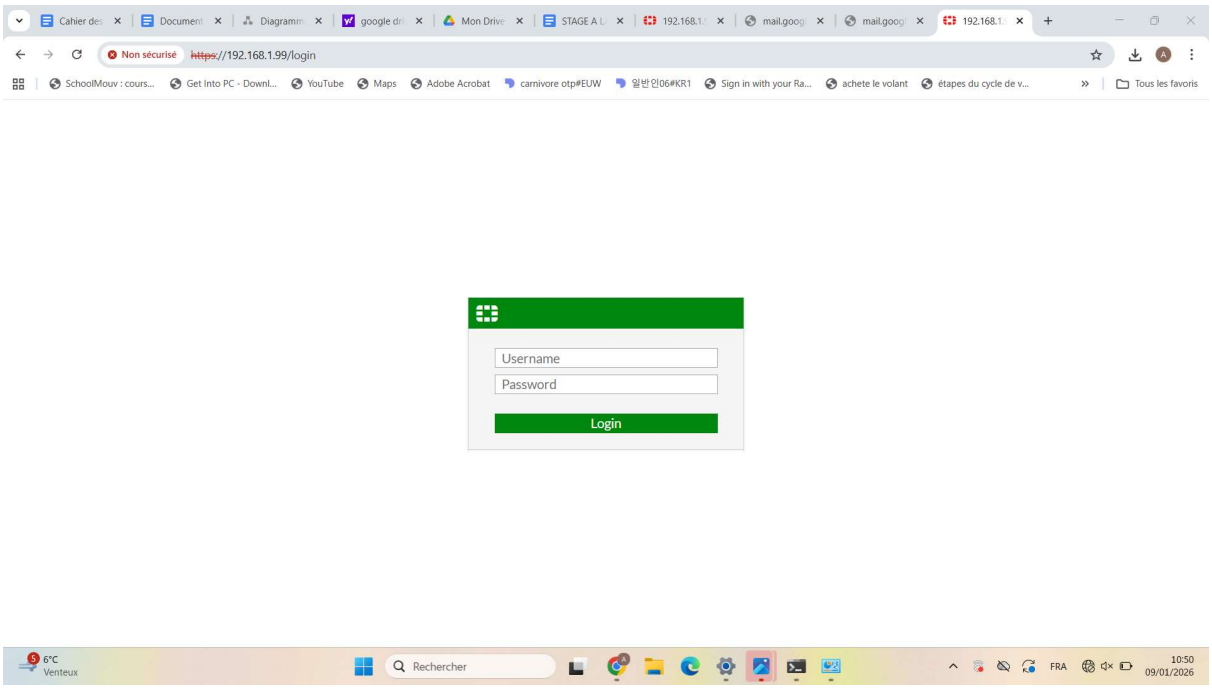
-comme sur la capture configurer une adresse ip disponible dans le même réseau que l'adresse du Fortigate qui est 199.168.1.99 et definir le masque de sous réseau en fonction du masque désiré(il se remplit automatiquement mais il faut vérifier qu'il correspond au masque qu'on veut)

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

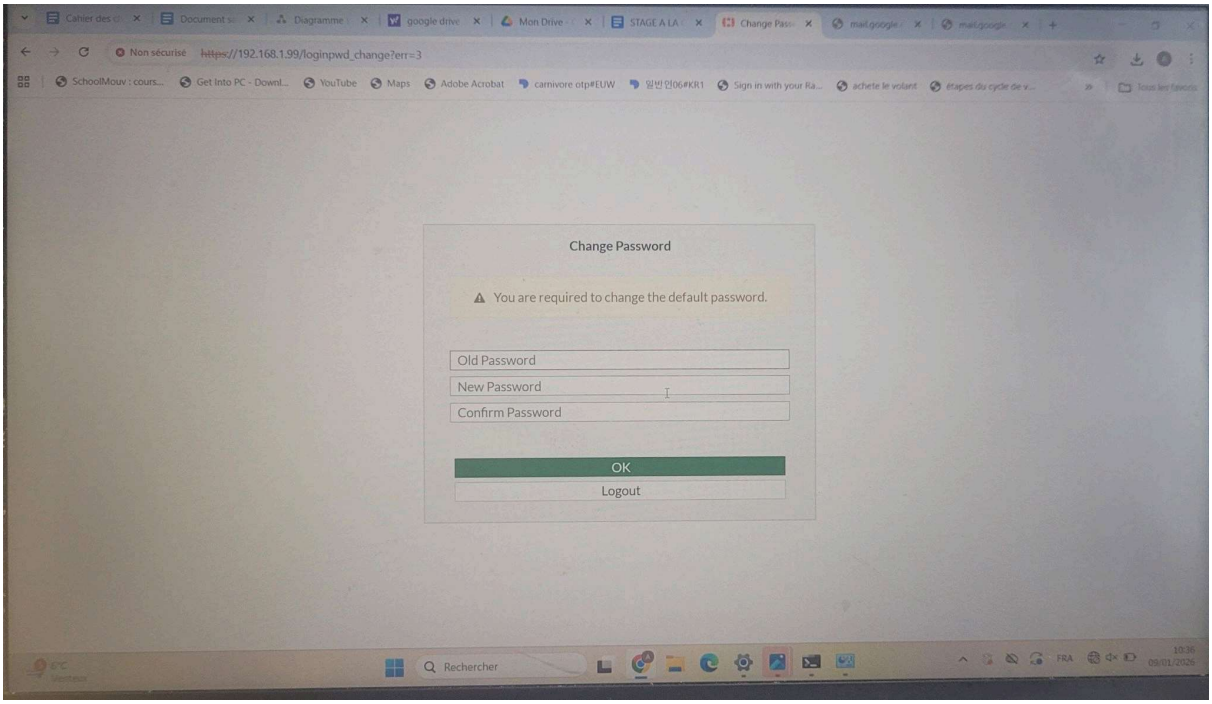
3eme étape configuration de fortigate :

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

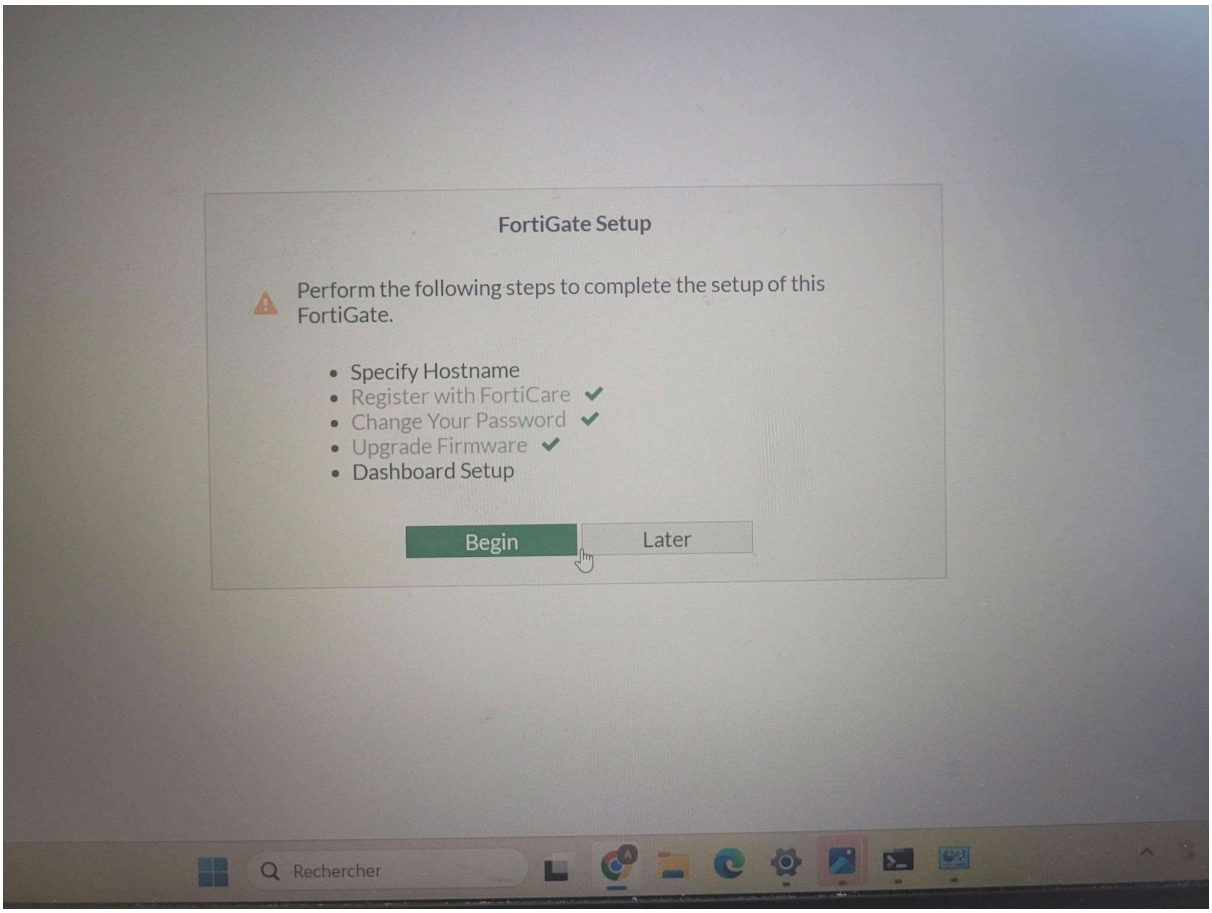
2- une page de connexion s'affiche, on saisit un **username** et un **password**



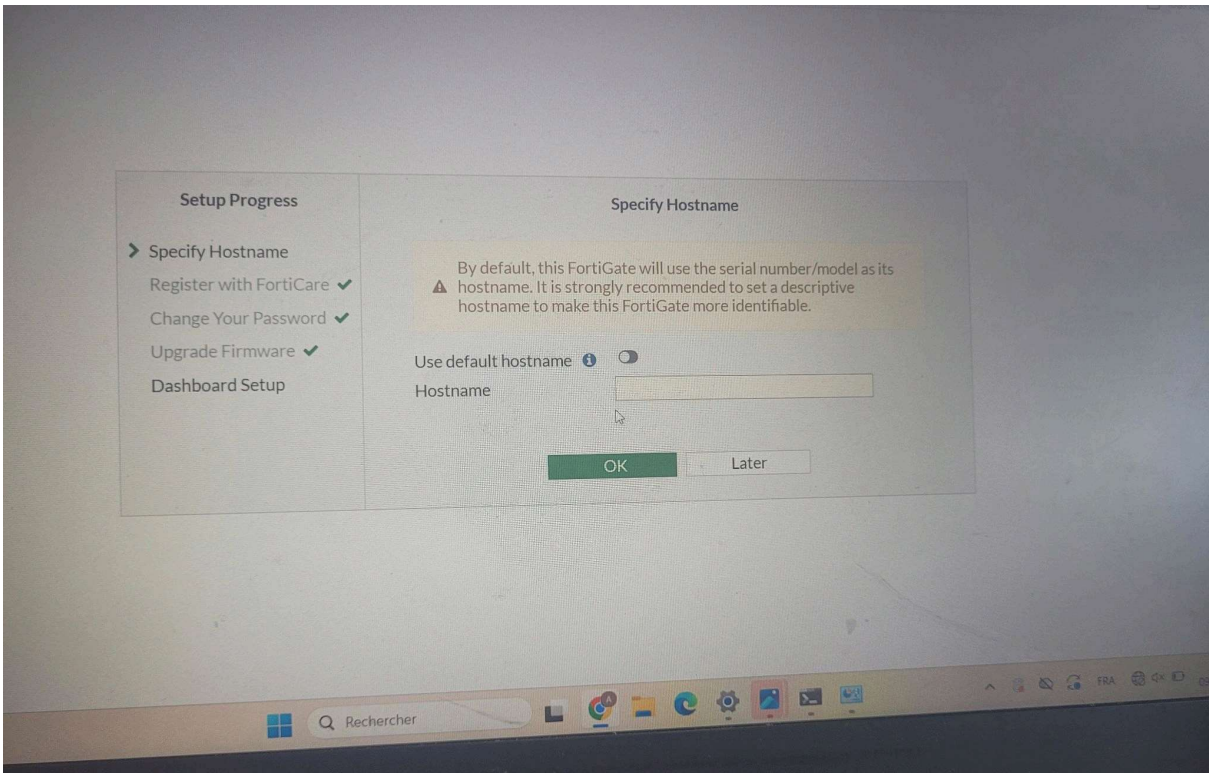
4- sur la nouvelle page,définir un **nouveau mdp** sans remplir la case avec **l'ancien mdp**, puis une nouvelle page s'affiche



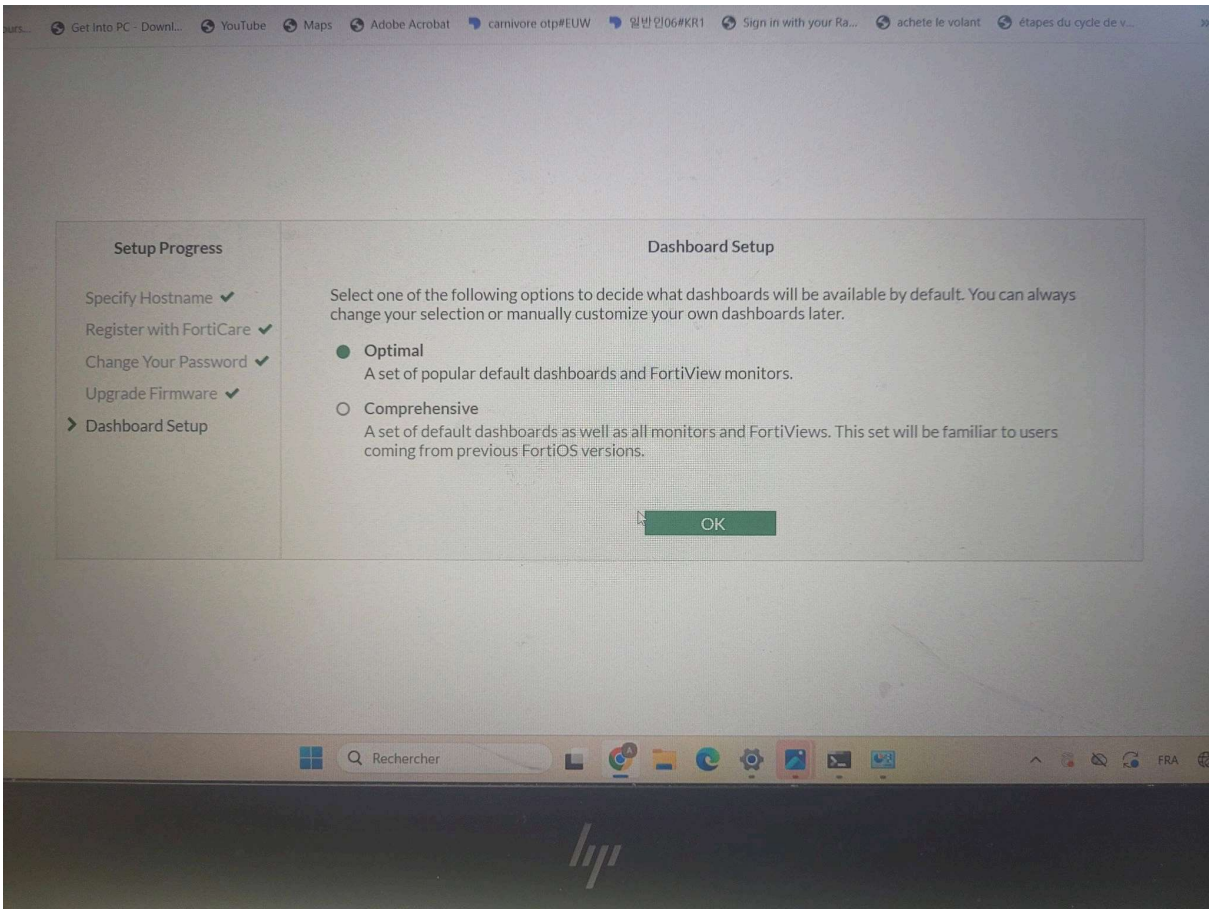
4bis- Une page fortigate setup qui affiche le reste du paramétrage à faire, appuyer sur "Begin"



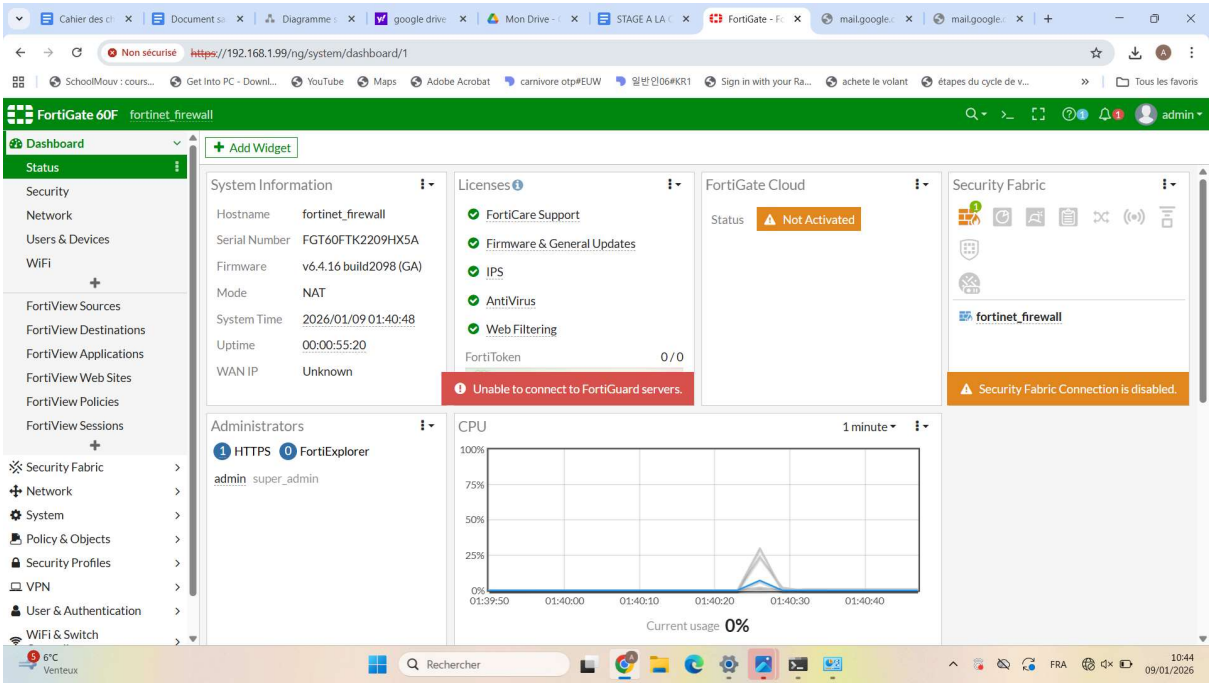
5- il faut choisir un **hostname** (ex: Fortinet_Firewall) puis cliquez sur ok

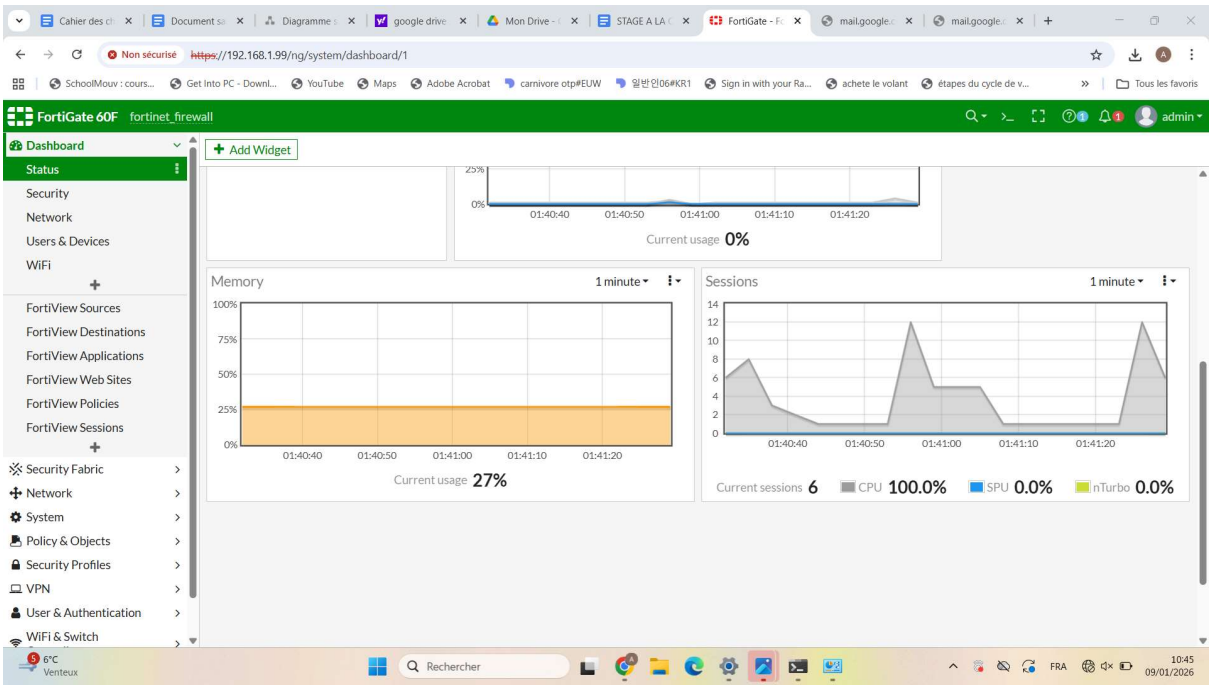


6- Pour le **dashboard setup** laisser **l'option optimal** et cliquer sur ok

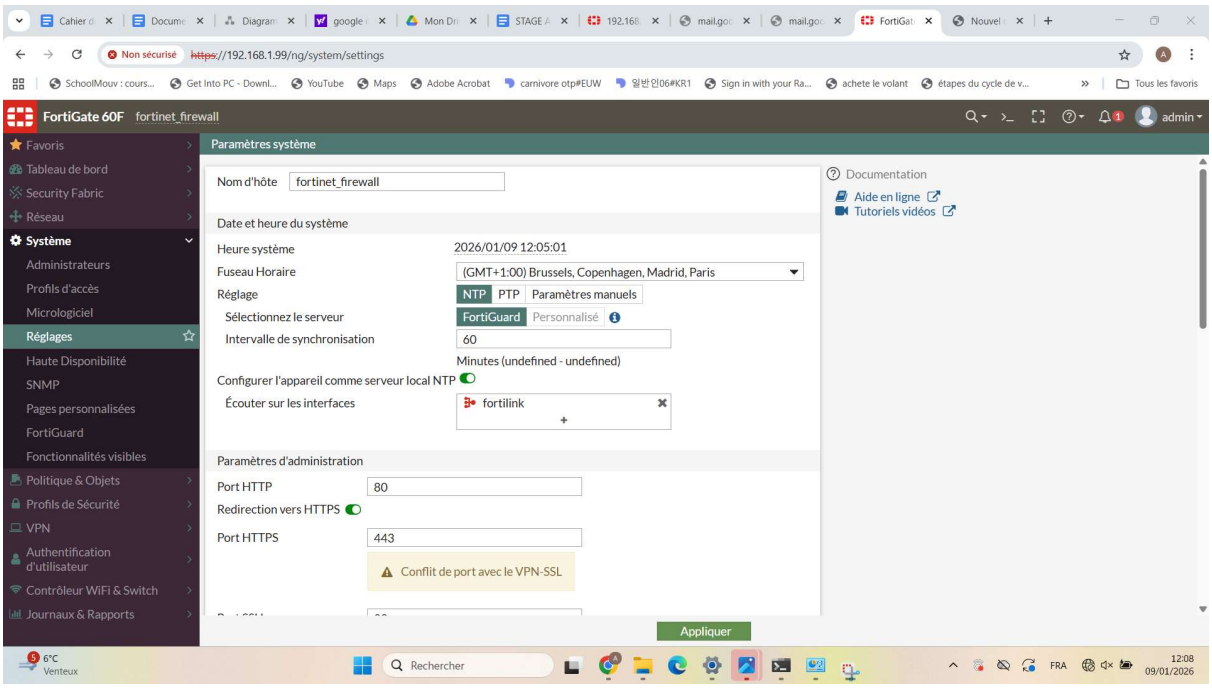


7-Le paramétrage est fini on a maintenant accès aux fonctionnalité du site

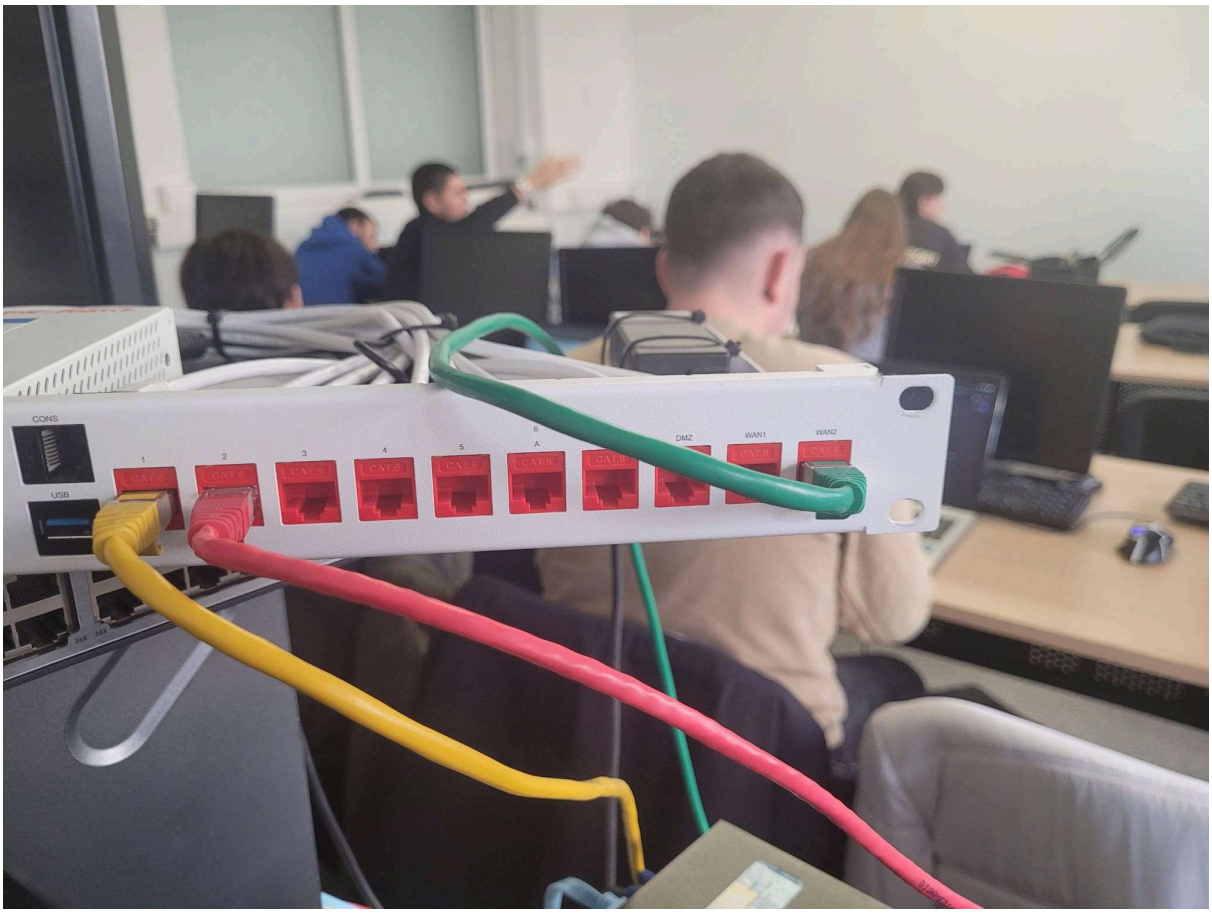




-Dans le dashboard aller dans **système** pui **réglage** et juste modifier le Fuseau horaire sur l'heure de paris et appliquer

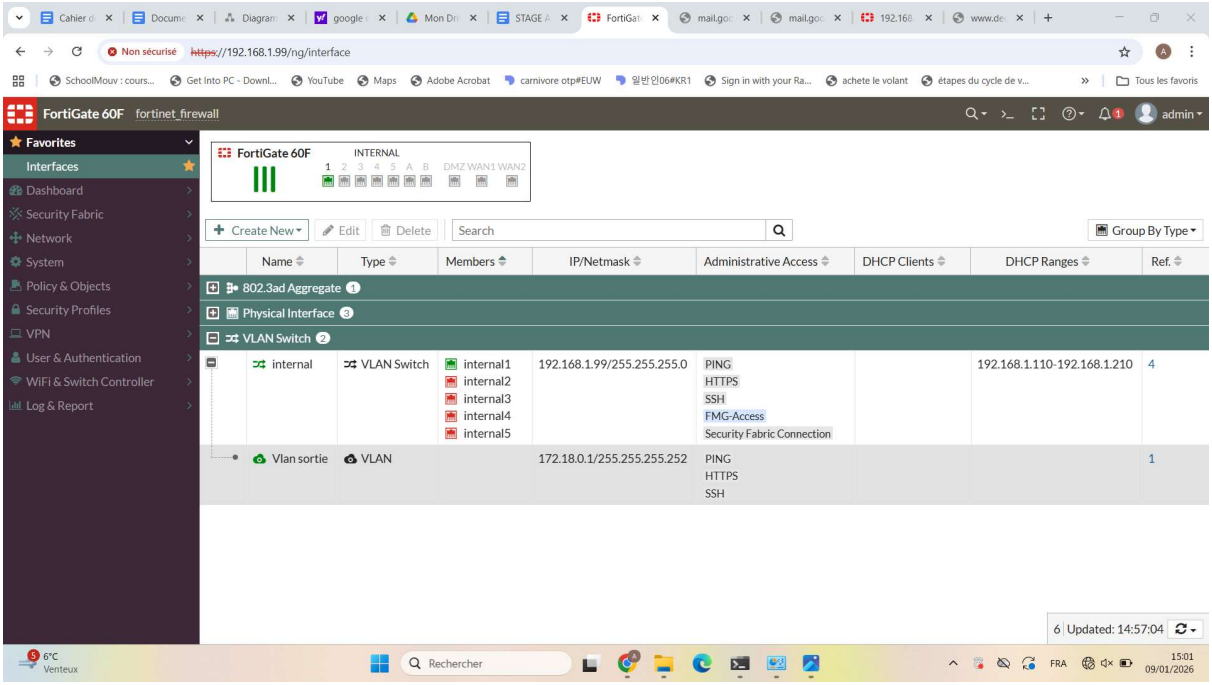


Notre répartition des Cable RJ45 sur les ports du fortigate ressemble à ceci :



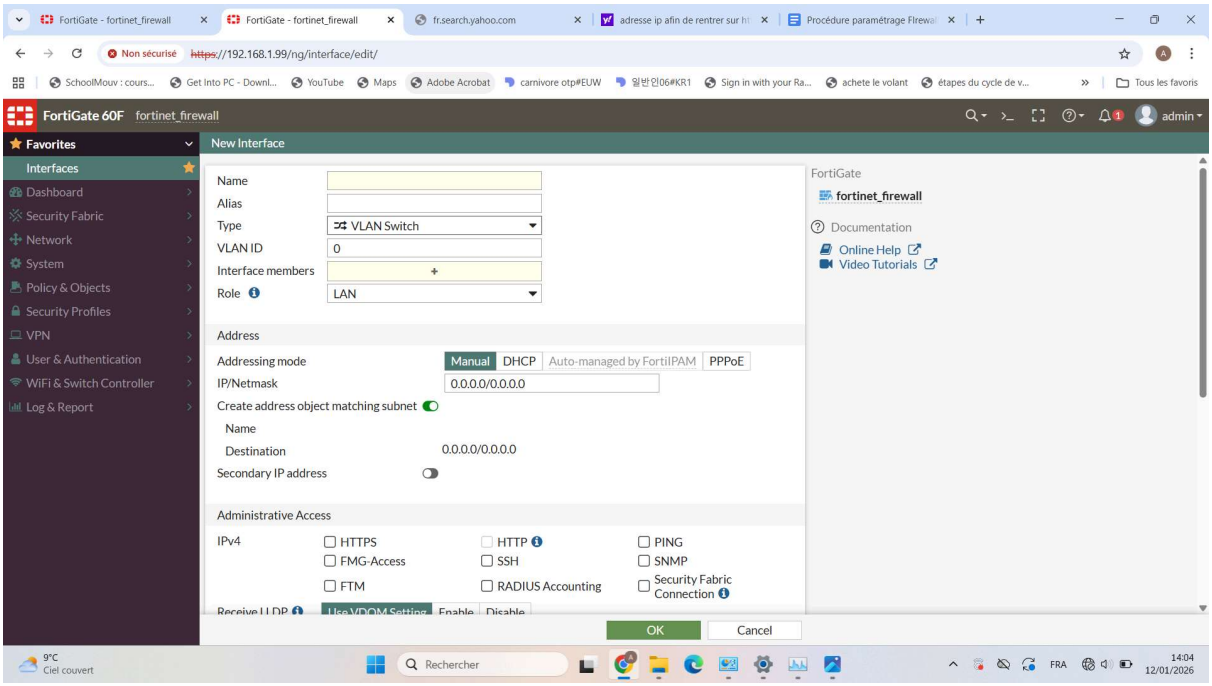
-Revenir sur interfaces puis il faut créer un vlan switch :

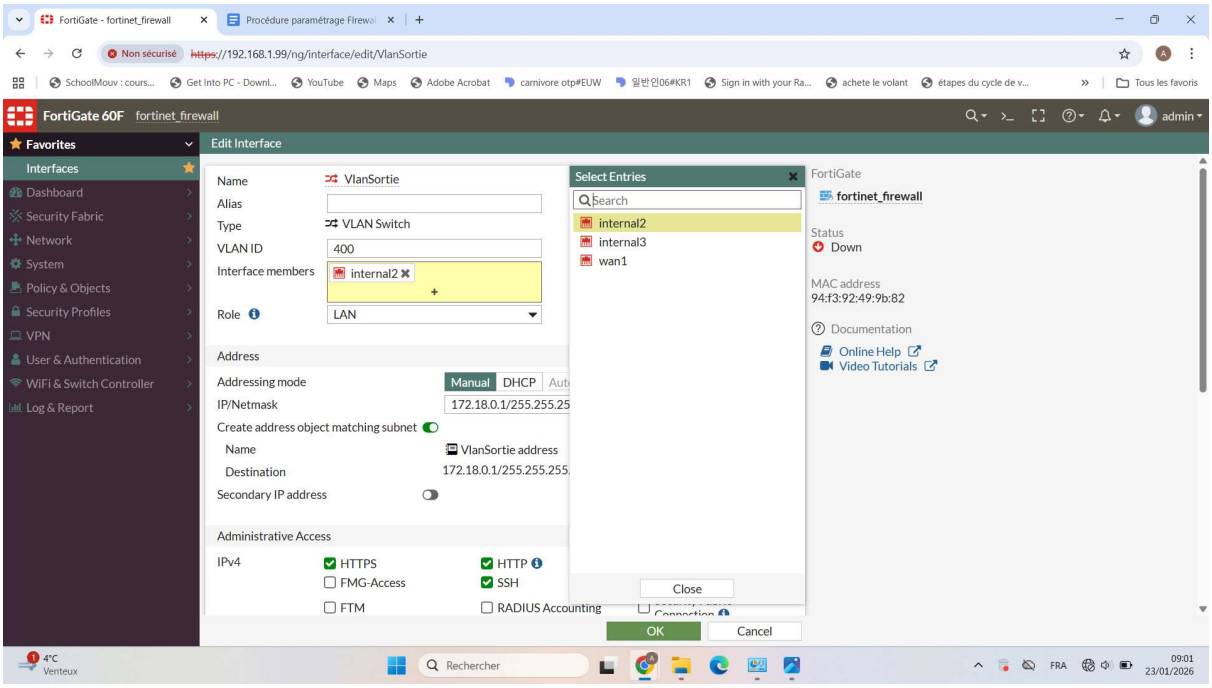
-cliquer sur **create new**



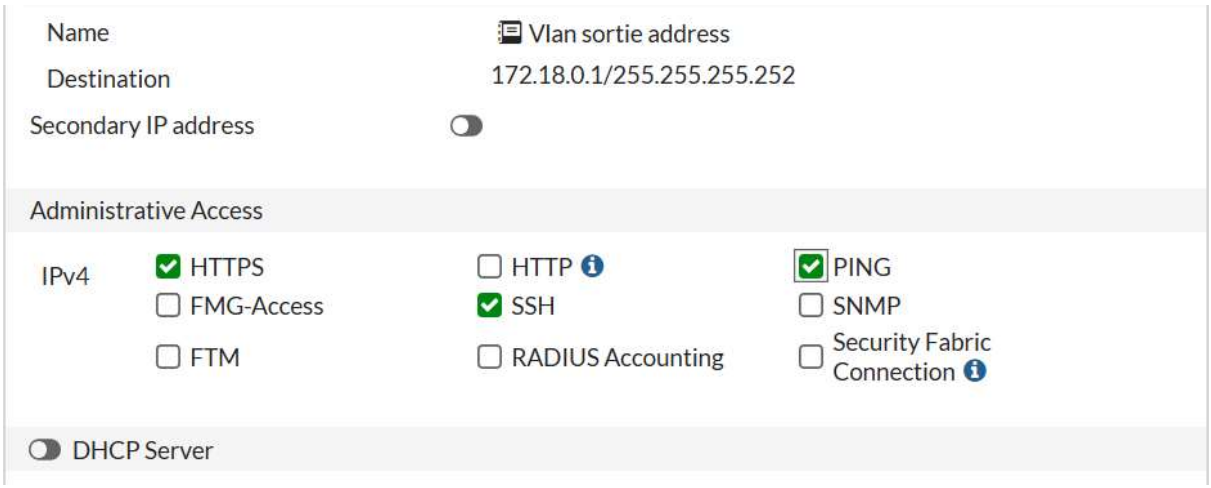
- définir le type sur “**Vlan switch**”
- choisir un numéro de vlan pour “**VLAN ID**” ex : 400
- définir le nom dans “**Name**” ex Vlan sortie

- 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”





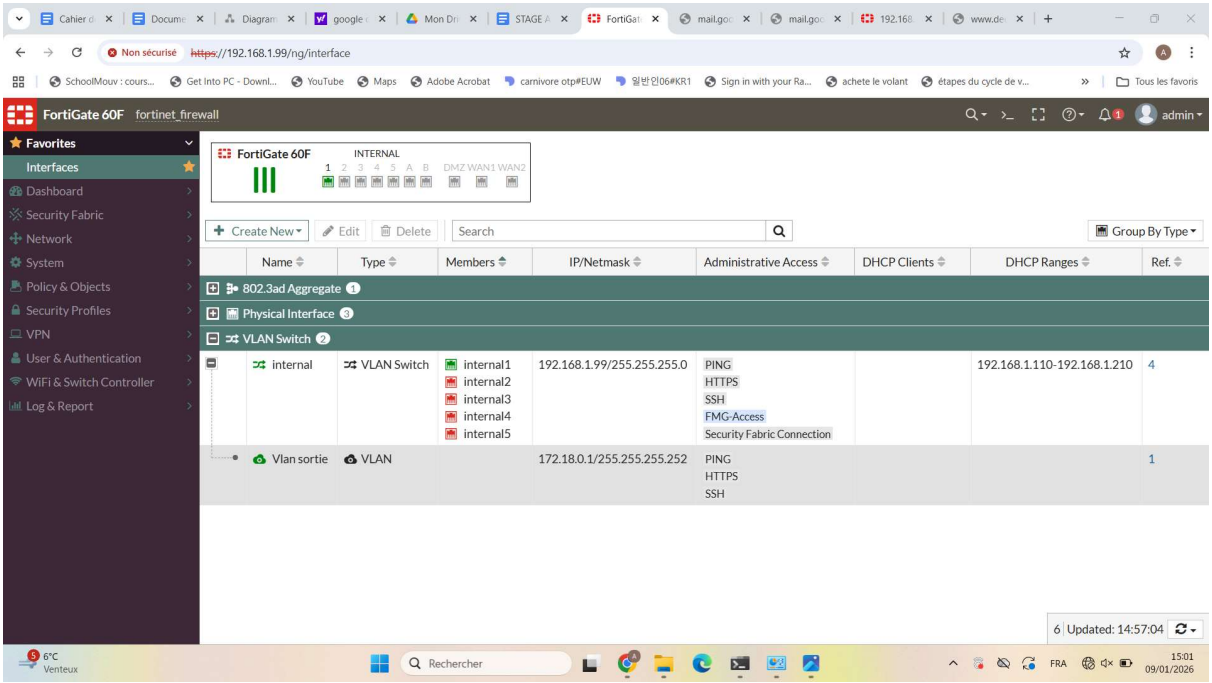
-administrative accès : cocher les cases pour lequel on veut autoriser l'administration du fortinet soit **SSH**, **HTTPS** et **PING** il ne sera pas possible d’administrer fortinet pour les cases non cochées.



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

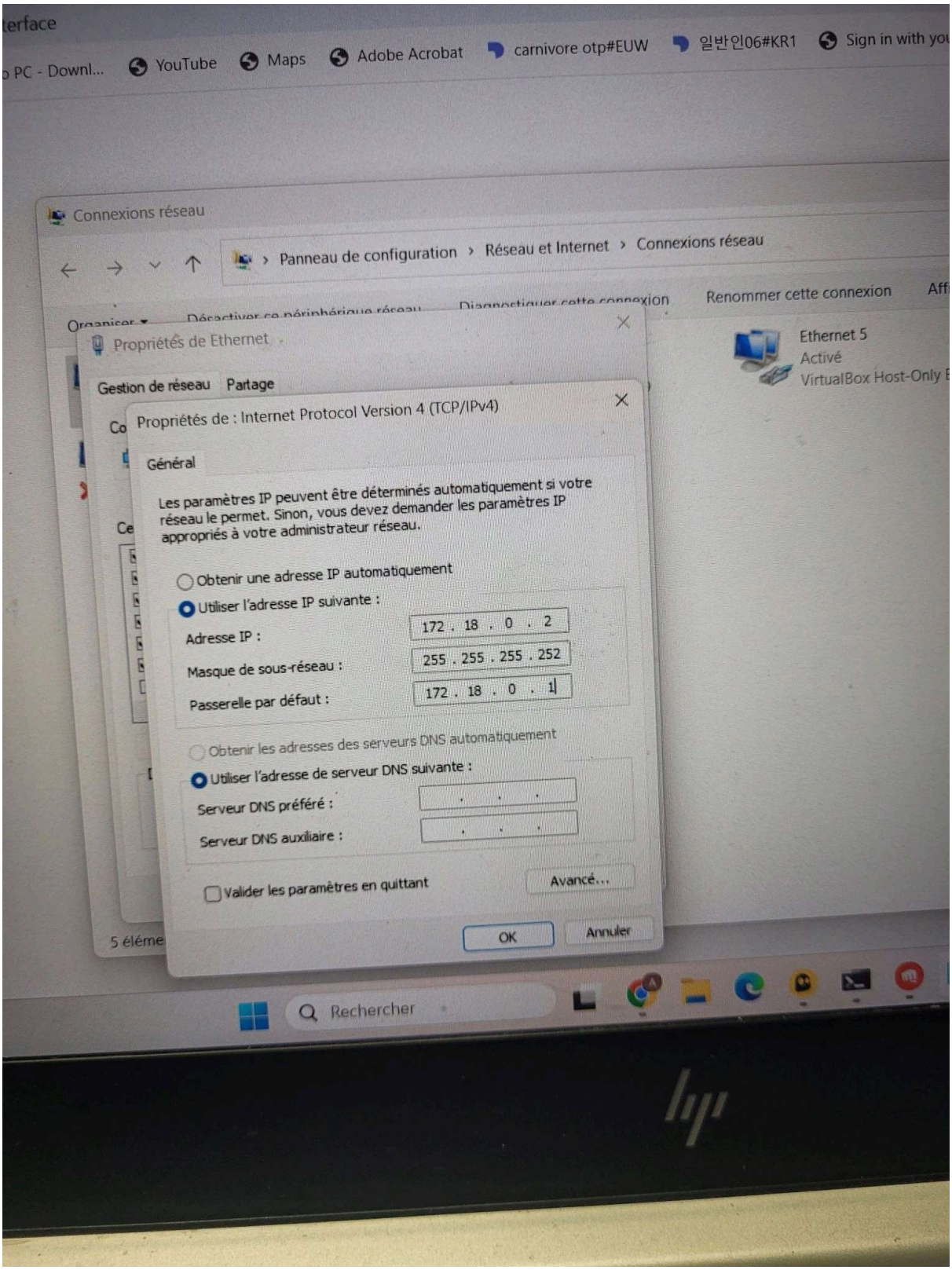
-Si jamais il est nécessaire de supprimer une interface car elle est mal paramétré voici la manipulation à suivre :

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

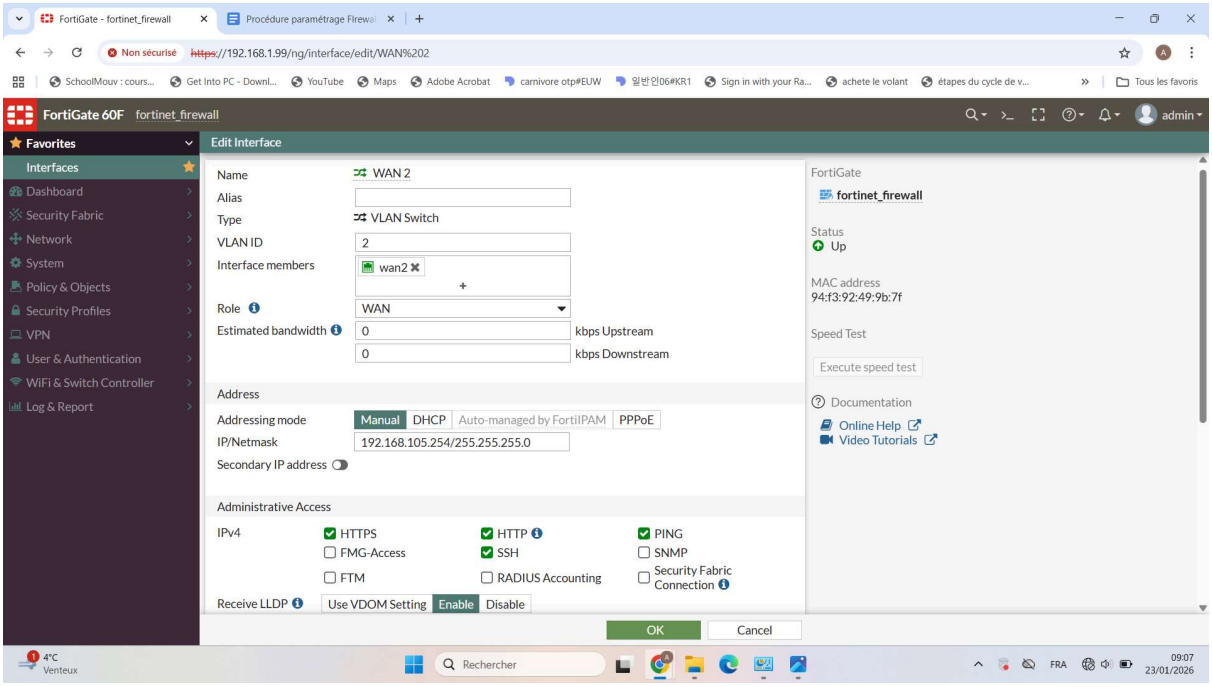


-appuyer sur **delete**, si jamais le bouton n’est pas cliquable, c’est que l’interface n’est pas “disabled et dans ce cas il faudra edit l’interface puis en bas de la page désactiver l’interface

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.
- Definir la nouvelle adresse IP 192.168.105.254

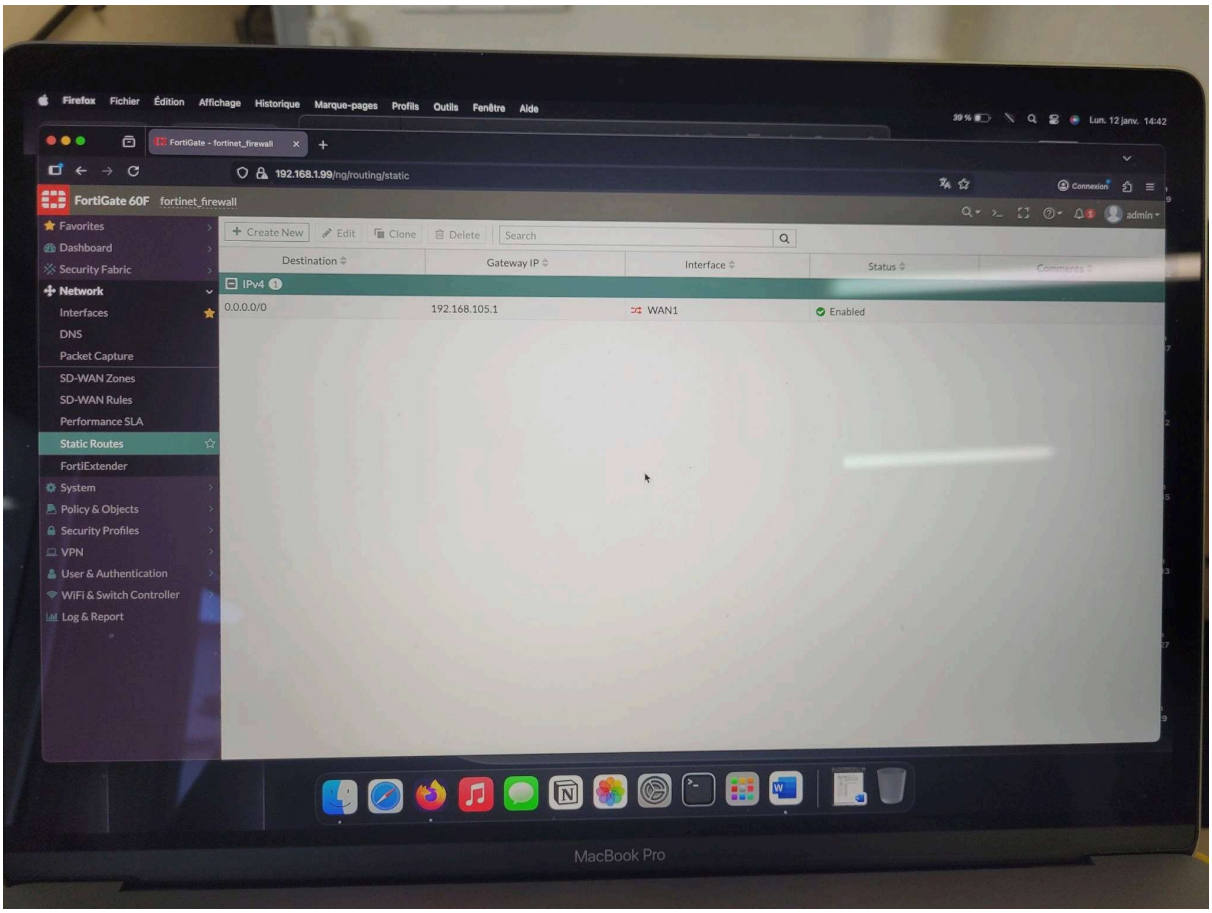


Une fois les 2 interfaces créées, tester si fortinet les detecte

-Il faut maintenant paramétrer la passerelle :

-Depuis le **dashboard** aller dans “**Network**” puis “**Static Routes**”

-cliquer sur “**Create new**” (IPv4 Static route)

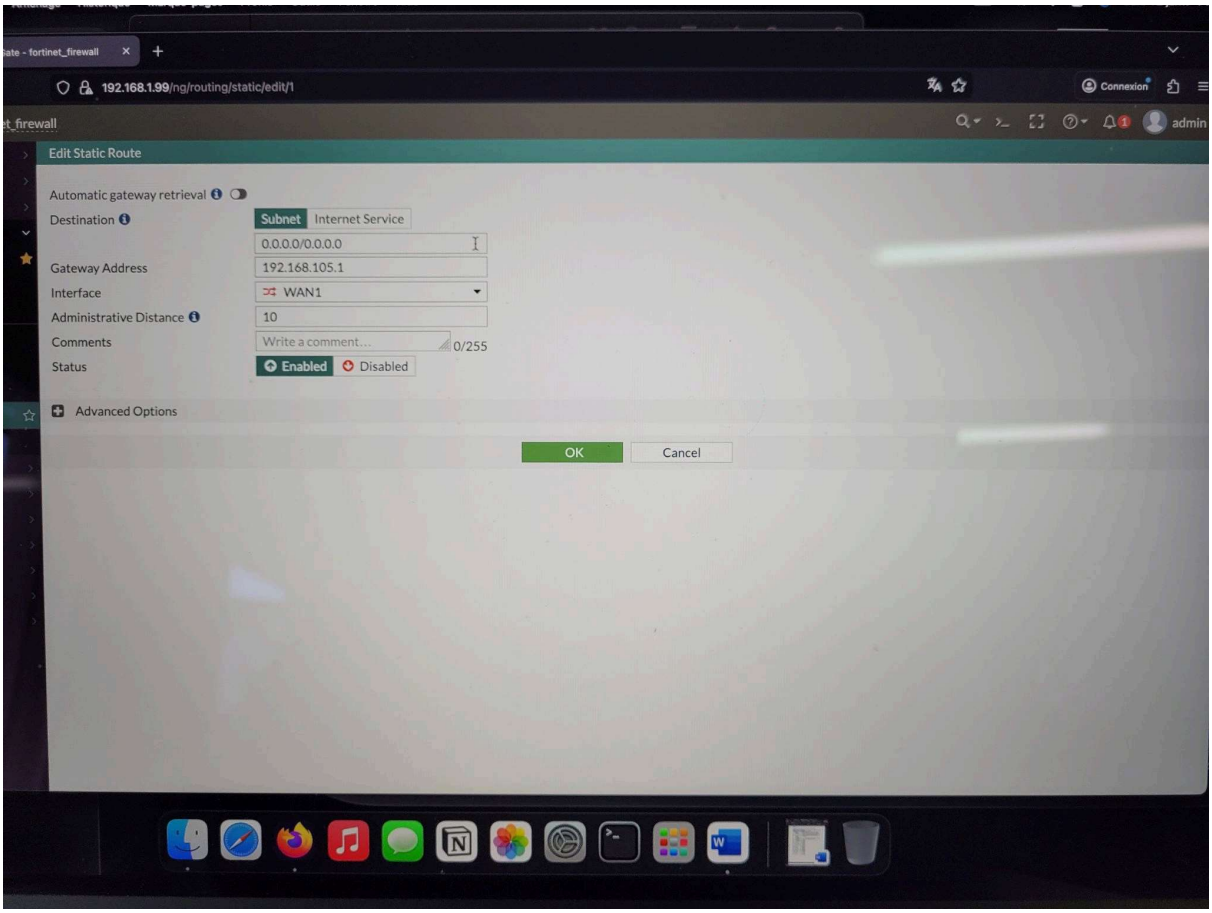


-Une nouvelle page s’affiche pour paramétrer la passerelle

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**.

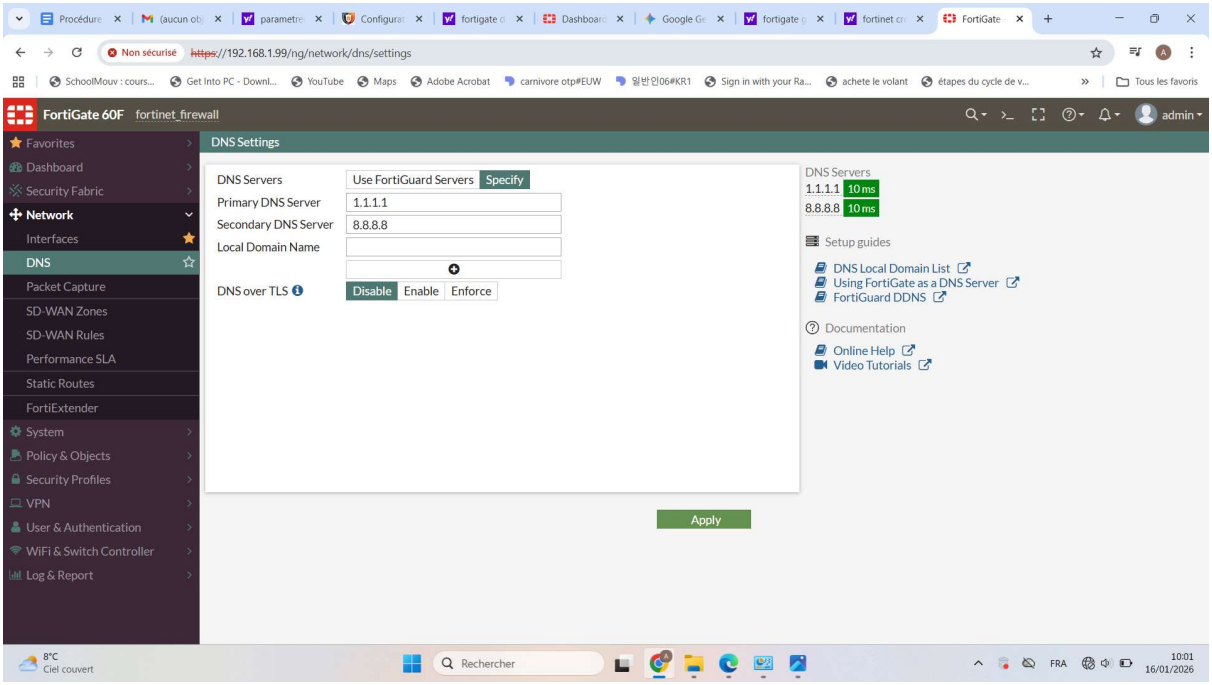


-Paramétrage du DNS :

-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)

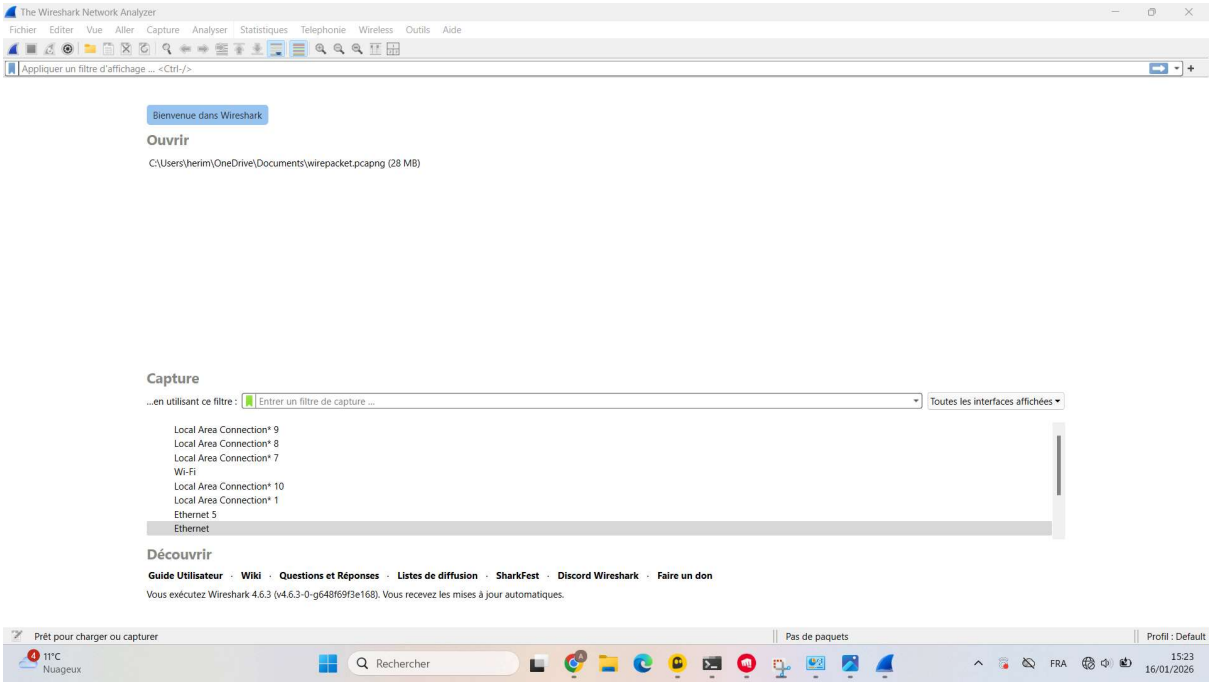
Pour “**Local domain Name”** ce n’est pas obligatoire de remplir, il faut le faire si on a un domaine interne

Et enfin cliquer sur “**Apply”**

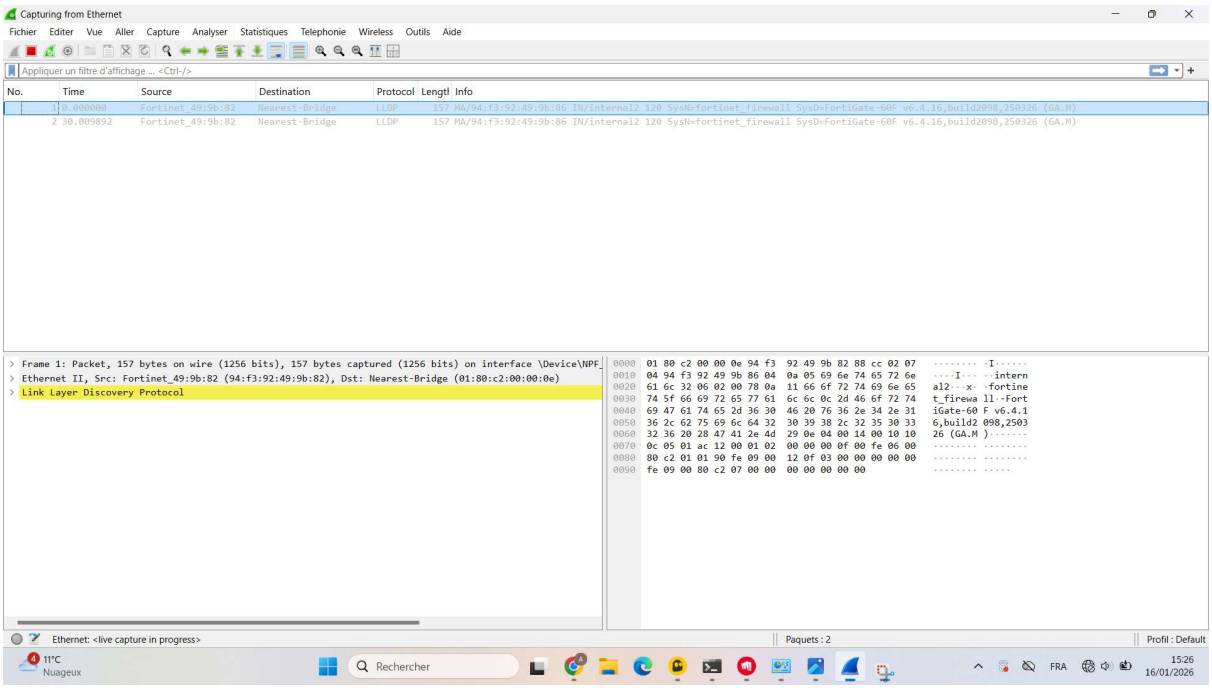


On va maintenant faire des test ping entre les appareils pour voir si tout est est connecté entre :
-Commencer par connecter le PC 2(le PC deux et le relier avec un cable rj45 à la box, le pc2 il faudra modifier la carte réseau du pc2 et définir son ip comme celle de la box 192.168.105.1

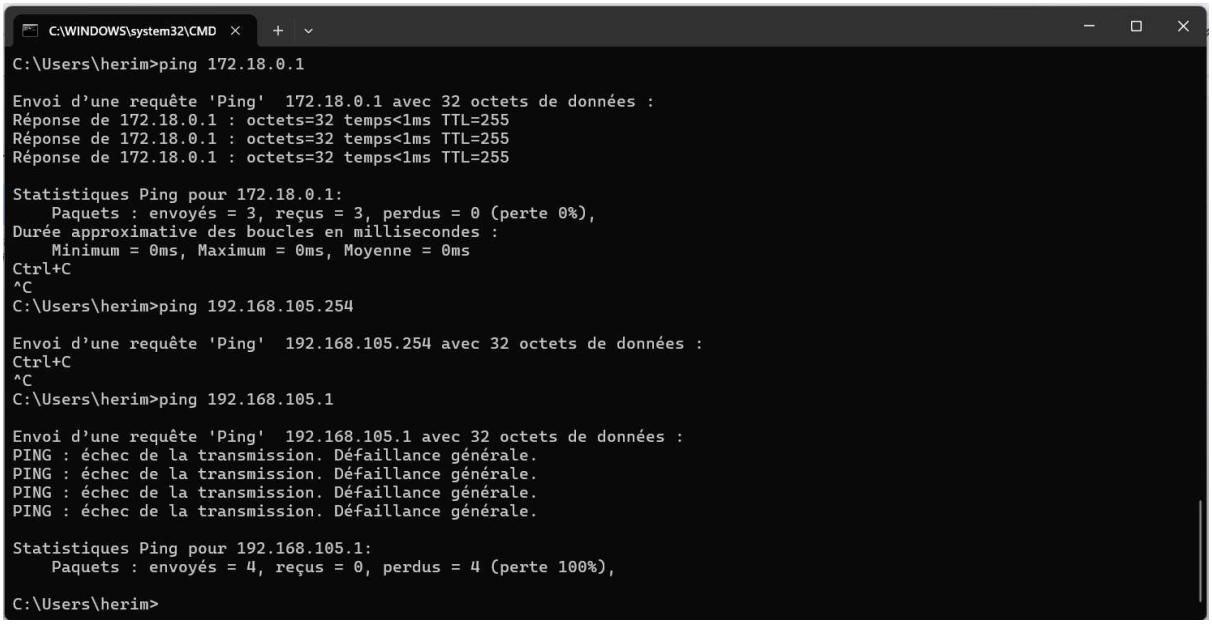
-pour analiser les trames qui passent entre les 2 ip des PC on peut utiliser Wireshark : ouvrir wireshark et choisir l'etehernet correspondant l'ip modifié du PC parmis les option(dans notre cas on a modifé ethernet sur la carte réseau)



Une nouvelle page s'affiche avec les trame affichés



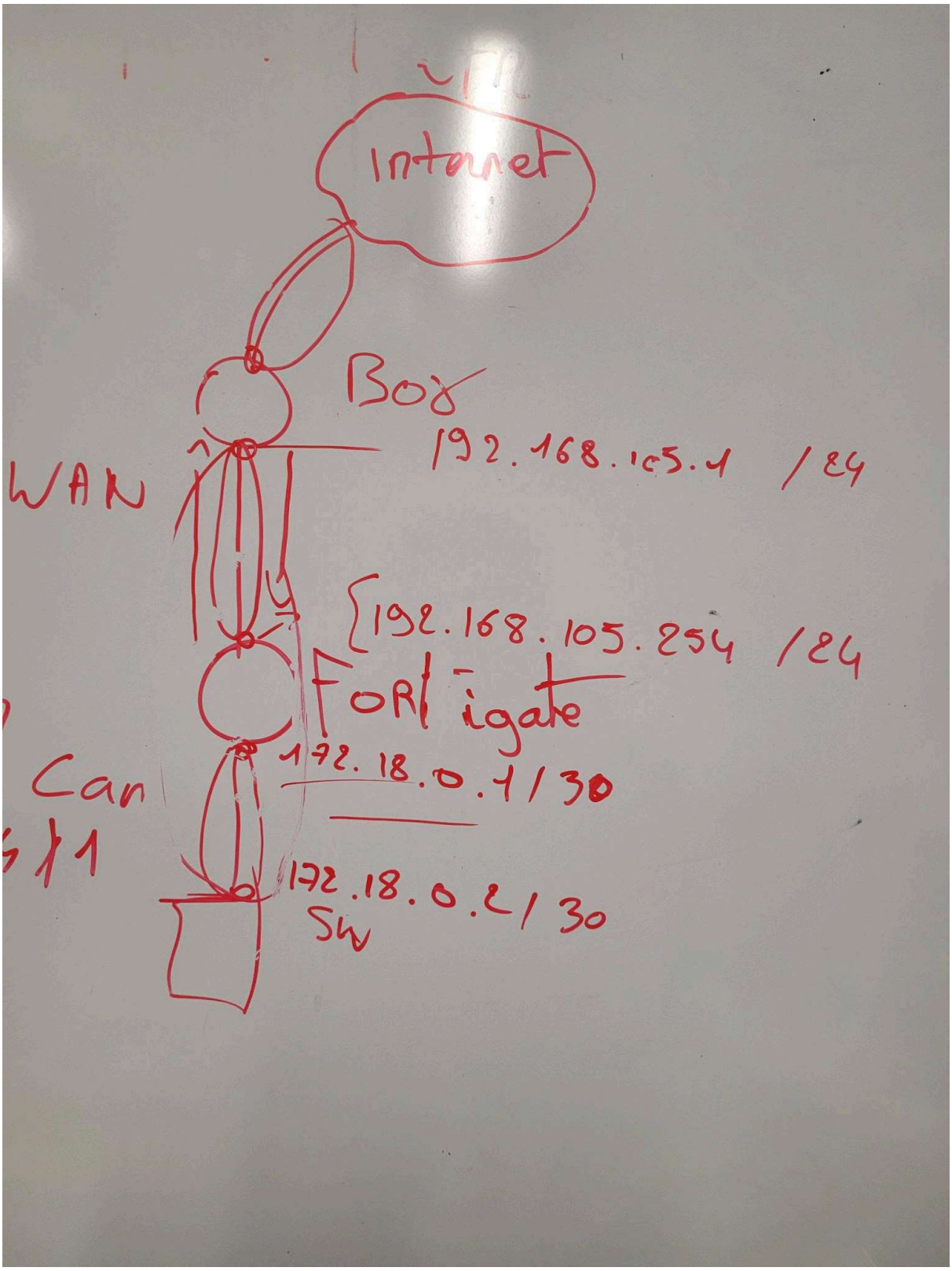
pour afficher les trame il faut ouvrir un cmd puis ping l'ip de l'autre PC

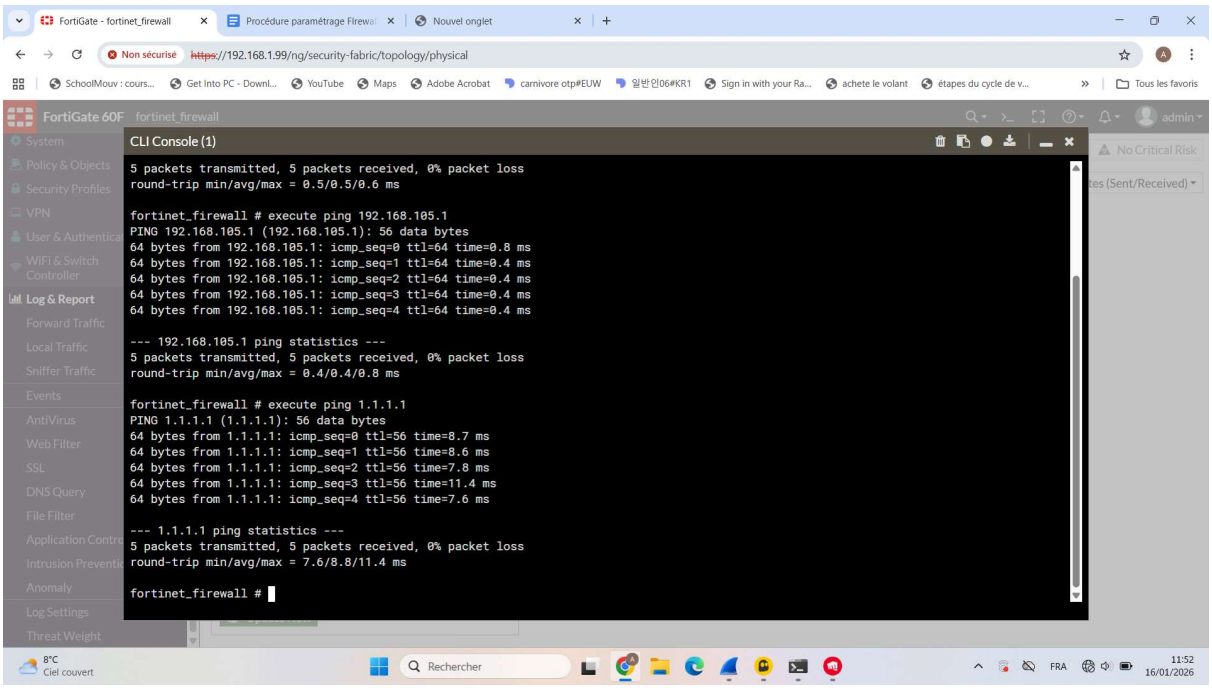


-On commence par ping depuis notre adresse de fortigate 172.18.0.1 l'adresse de la BOX 192.168.105.1 pour cela depuis le haut de la page du site cliquer sur le signe >_ se situant à côté de la loupe :

- une console s'ouvre et on ping 192.168.105.1 ça fonctionne
- on ping maintenant cloudflare 1.1.1.1 ça fonctionne car on a défini la paserelle (la box) 192.168.105.1 pour pouvoir ensuite connaitre le chemin jusqu'à internet

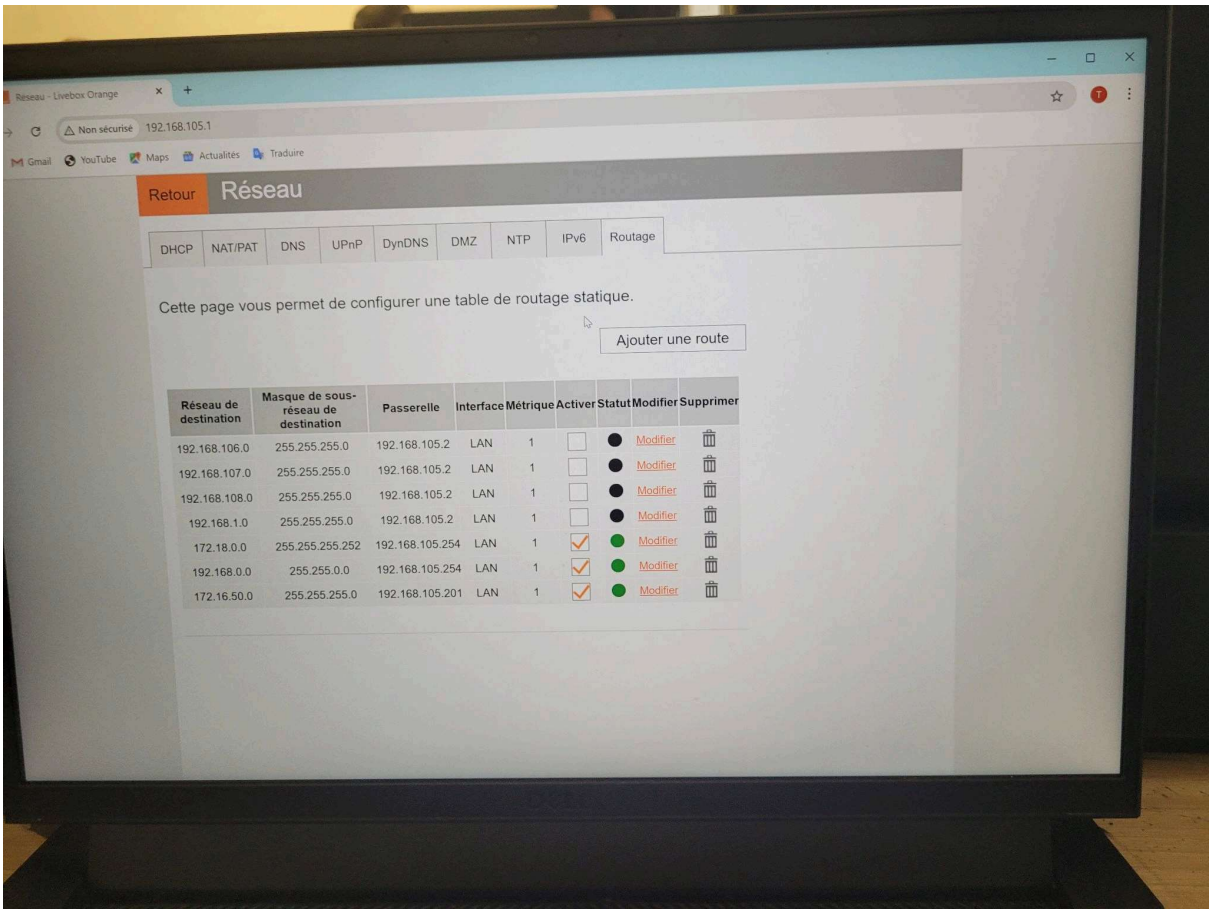
on s'assure que la route de fortigate jusqu'à la box puis internet fonctionne


Internet
Box
192.168.105.1 /24
WAN
192.168.105.254 /24
FORTIgate
172.18.0.1/30
172.18.0.2/30
SW



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'a fortigate (dont on modifie L'IP pour le pc2) puis jusqu'a 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.

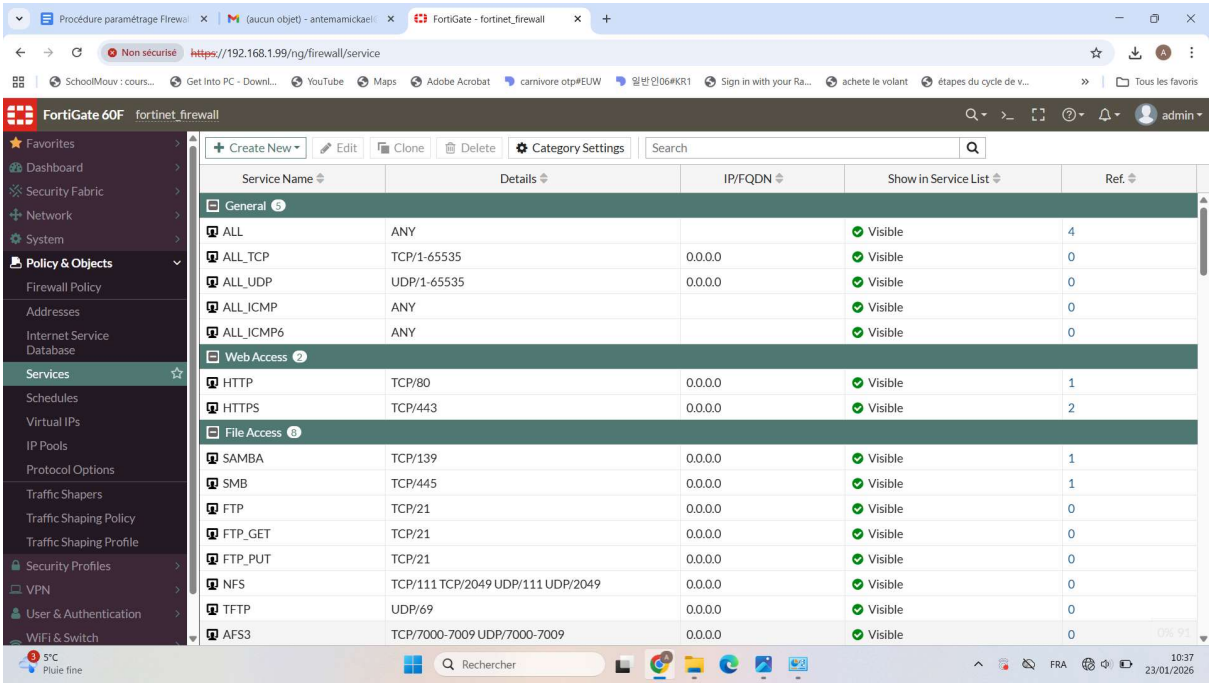
Le FortiGate est un pare-feu à état (stateful) : si une règle autorise A vers B, le retour de B vers A est automatiquement autorisé pour cette session précise. En revanche, si B essaie de parler à A de lui-même, il sera bloqué s'il n'y a pas de règle spécifique.

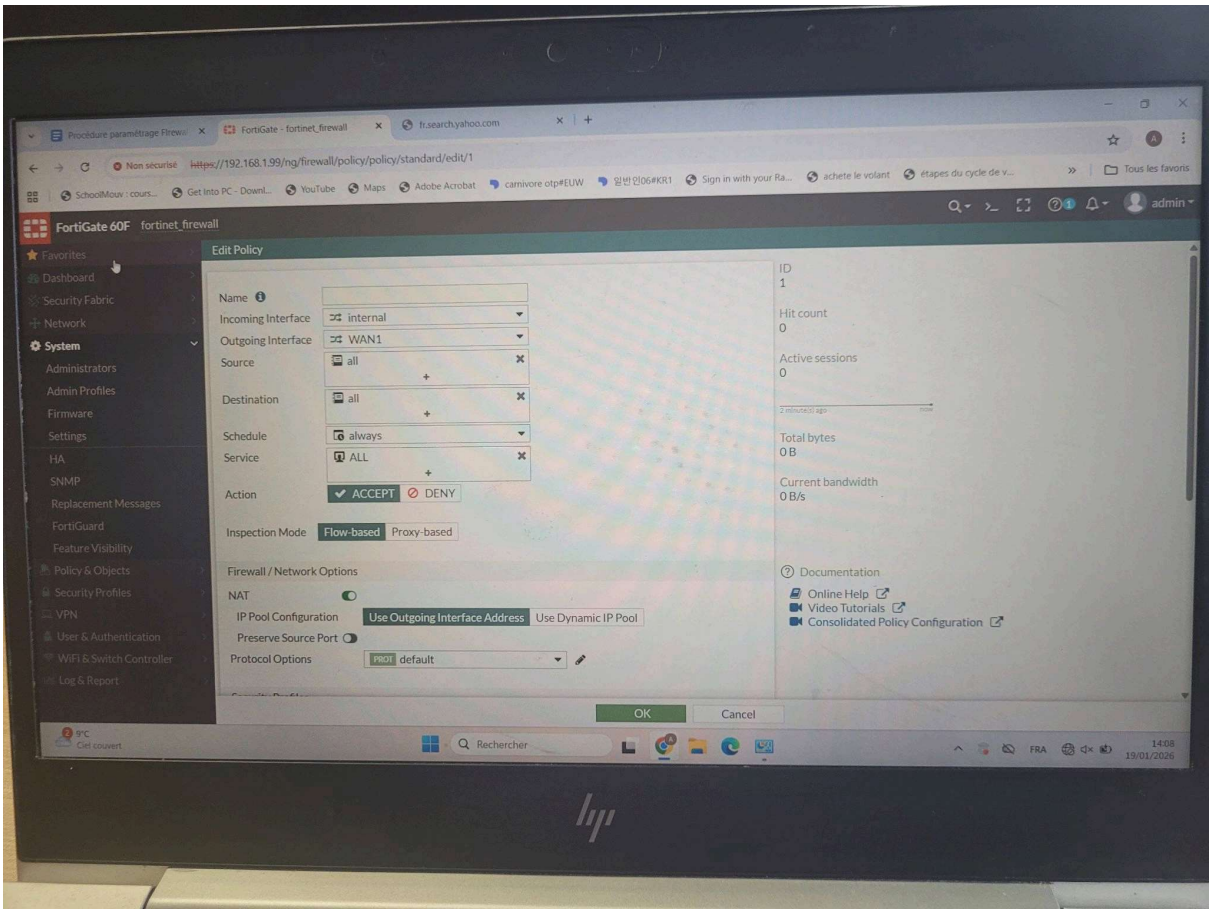
Voici comment débloquer la situation selon votre cas :

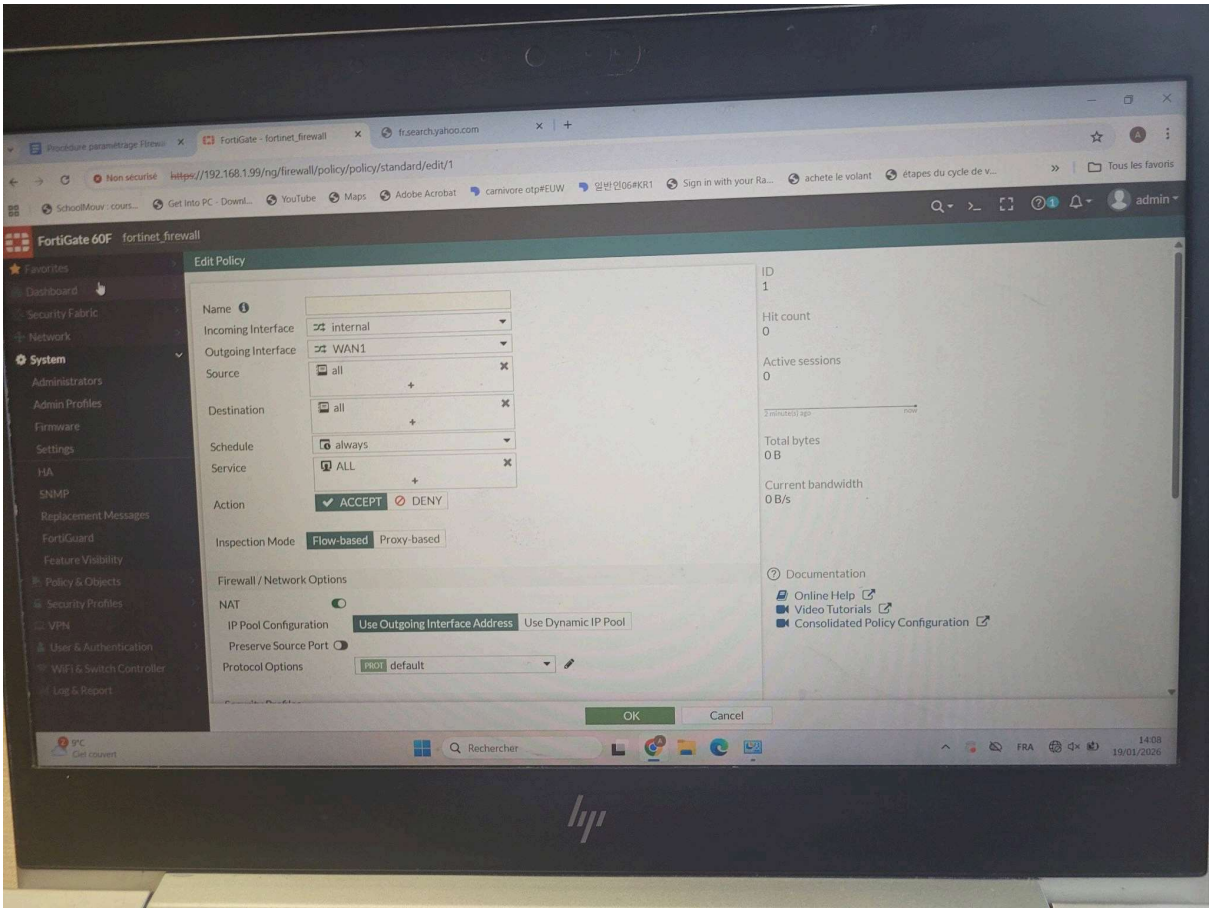
1. Créer une règle de retour (Reverse Policy)

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.




FortiGate 60F fortinet_firewall
Edit Policy
Name
Incoming Interface internal
Outgoing Interface WAN1
Source all
Destination all
Schedule always
Service ALL
Action ACCEPT DENY
Inspection Mode Flow-based Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool
Preserve Source Port
Protocol Options PROT default
ID 1
Hit count 0
Active sessions 0
Total bytes 0 B
Current bandwidth 0 B/s
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration
OK
Cancel


FortiGate 60F fortinet_firewall
Edit Policy
Name
Incoming Interface internal
Outgoing Interface WAN1
Source all
Destination all
Schedule always
Service ALL
Action ACCEPT DENY
Inspection Mode Flow-based Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool
Preserve Source Port
Protocol Options PROT default
ID 1
Hit count 0
Active sessions 0
Total bytes 0 B
Current bandwidth 0 B/s
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration
OK
Cancel

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.