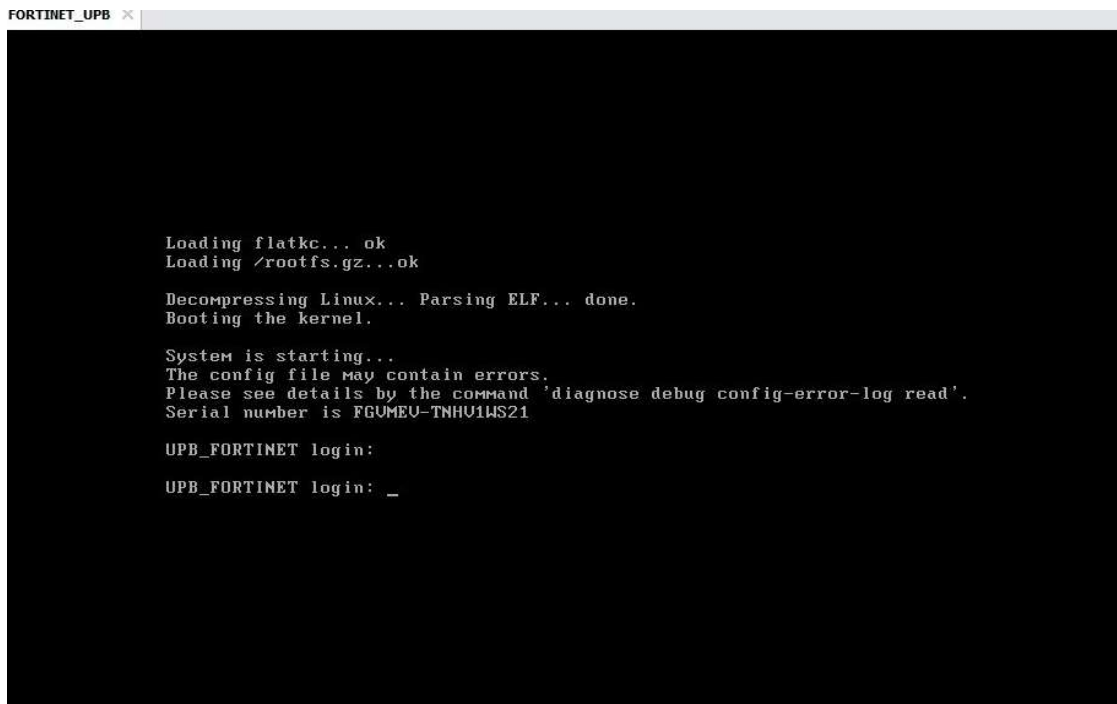


MISE EN PLACE D'UN PORTAIL CAPTIF SUR PARE-FEU FORTIGET

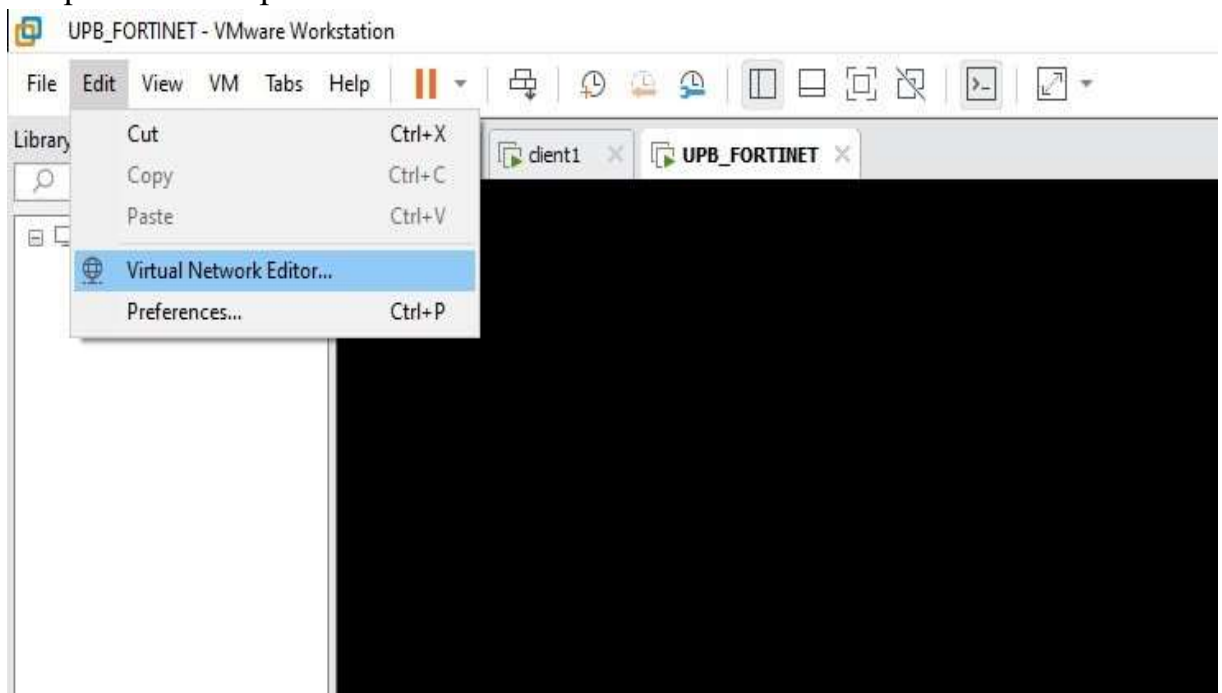
Etape 1:

- Créer une machine virtuelle avec l'os de Fortinet version 7.2.0

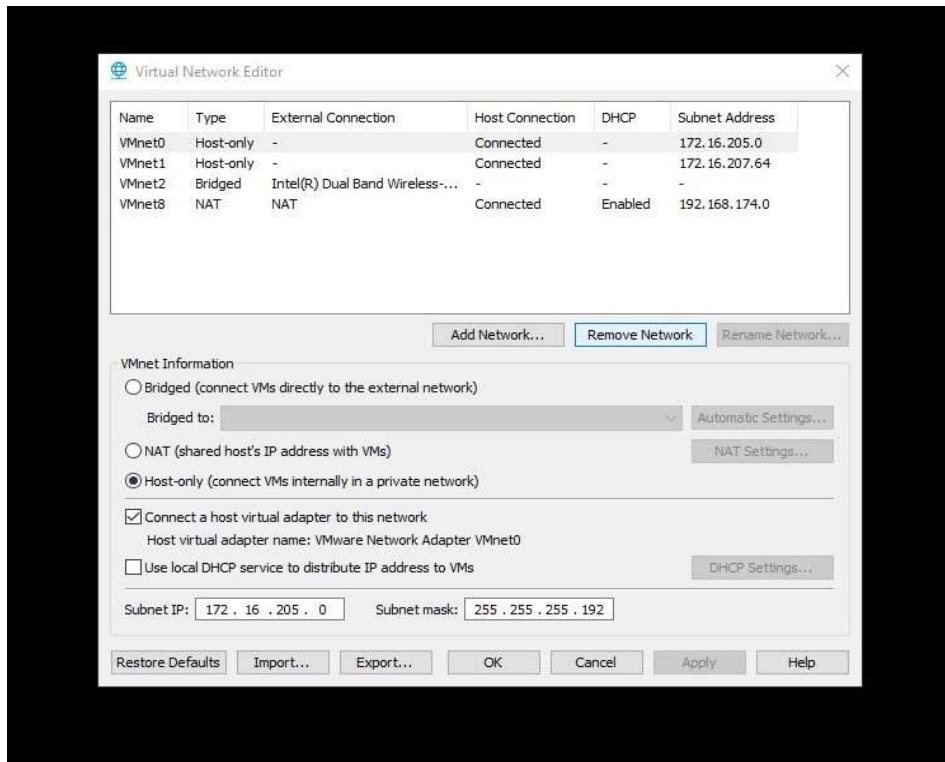


- Créer une machine cliente Windows
- Supprimer les vmnet par défaut et créer de nouvelles interfaces vmnet adapté à notre exercice :

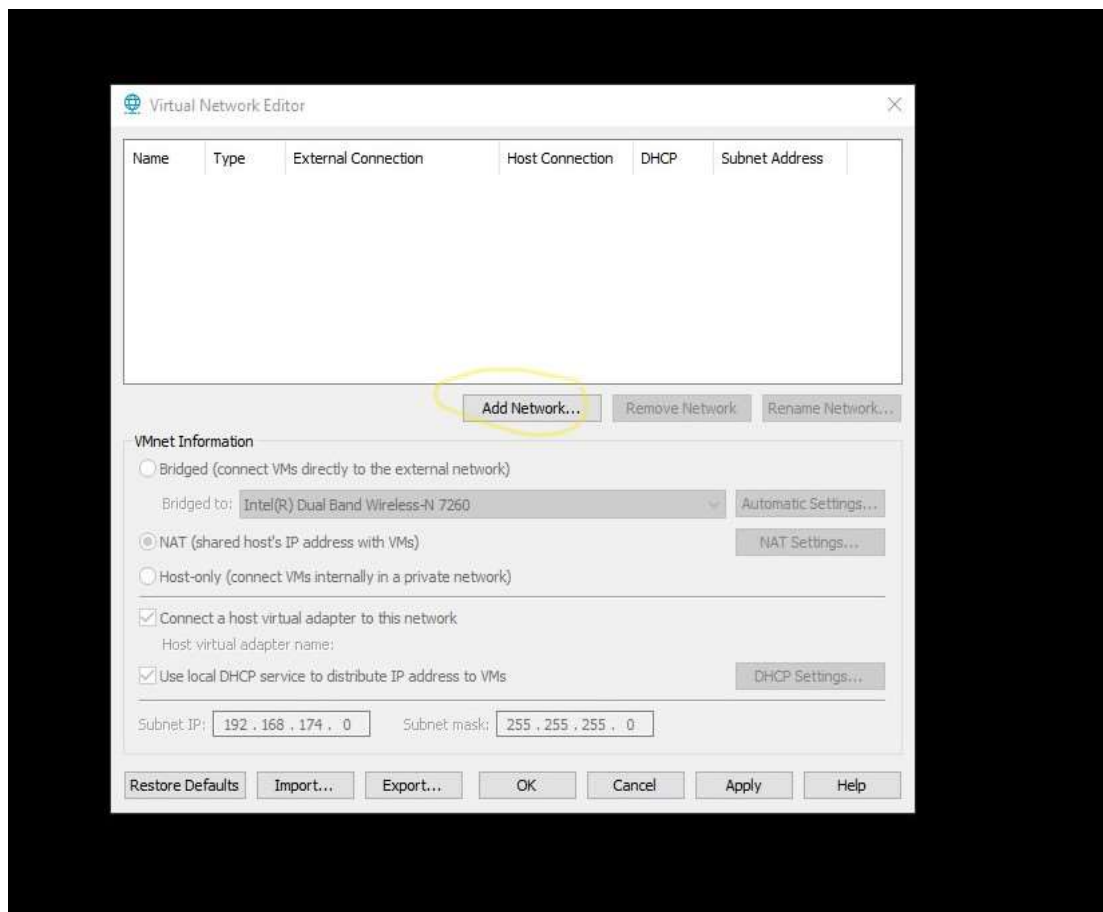
Cliquez sur **Edit** puis **Virtual Network Editor**



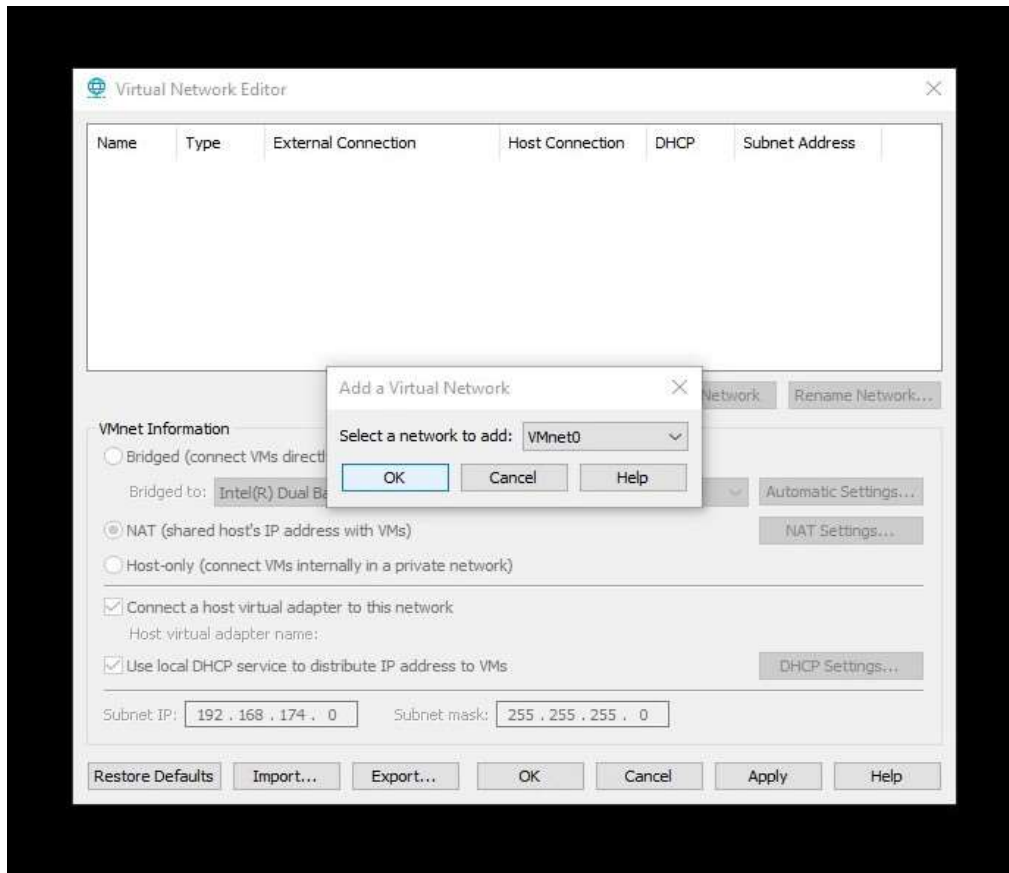
Ensuite on supprime les « Vmnet » qui sont installés par défaut en faisant « Remove Network » :



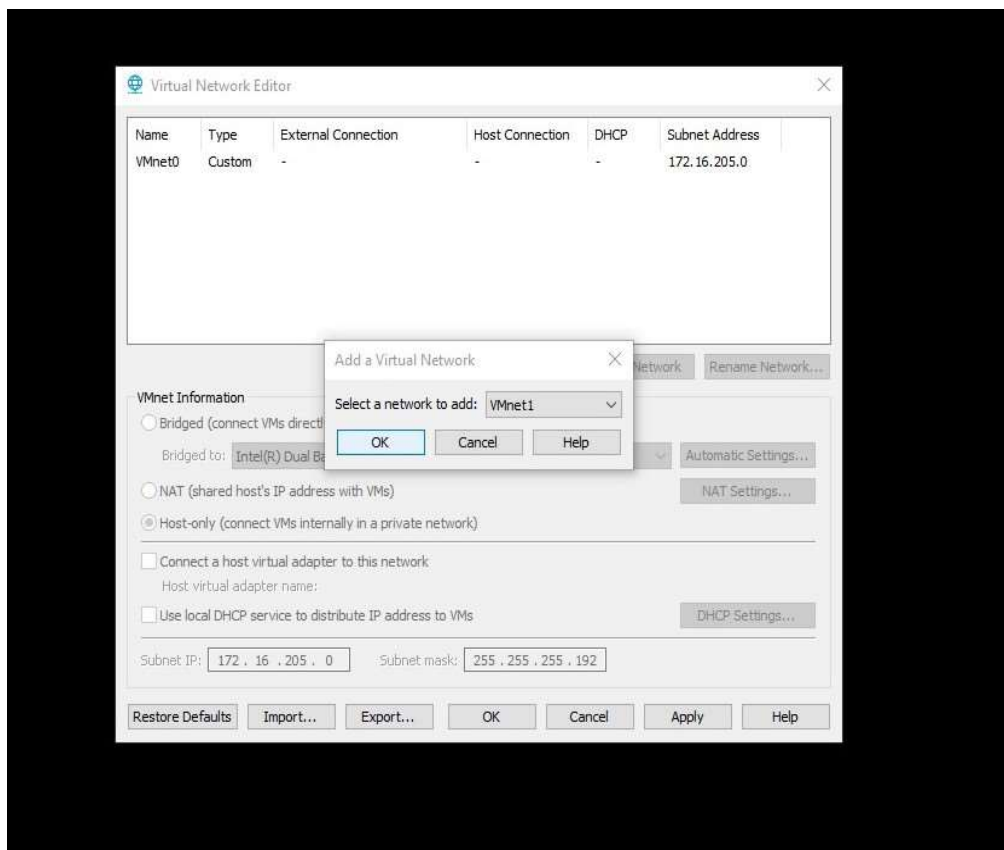
On crée ensuite de nouvelles interfaces « Vmnet » en faisant « Add Network » :



On sélectionne Vmnet0 :

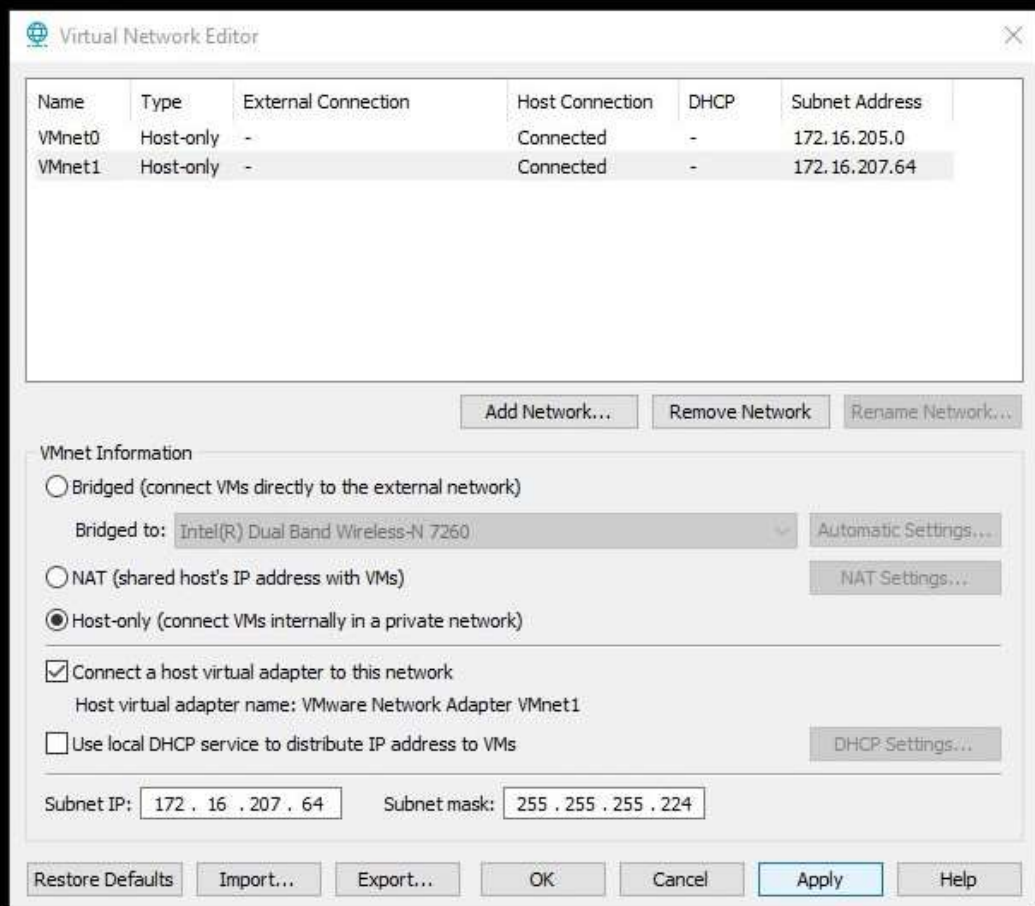


On crée une seconde interface Vmnet :



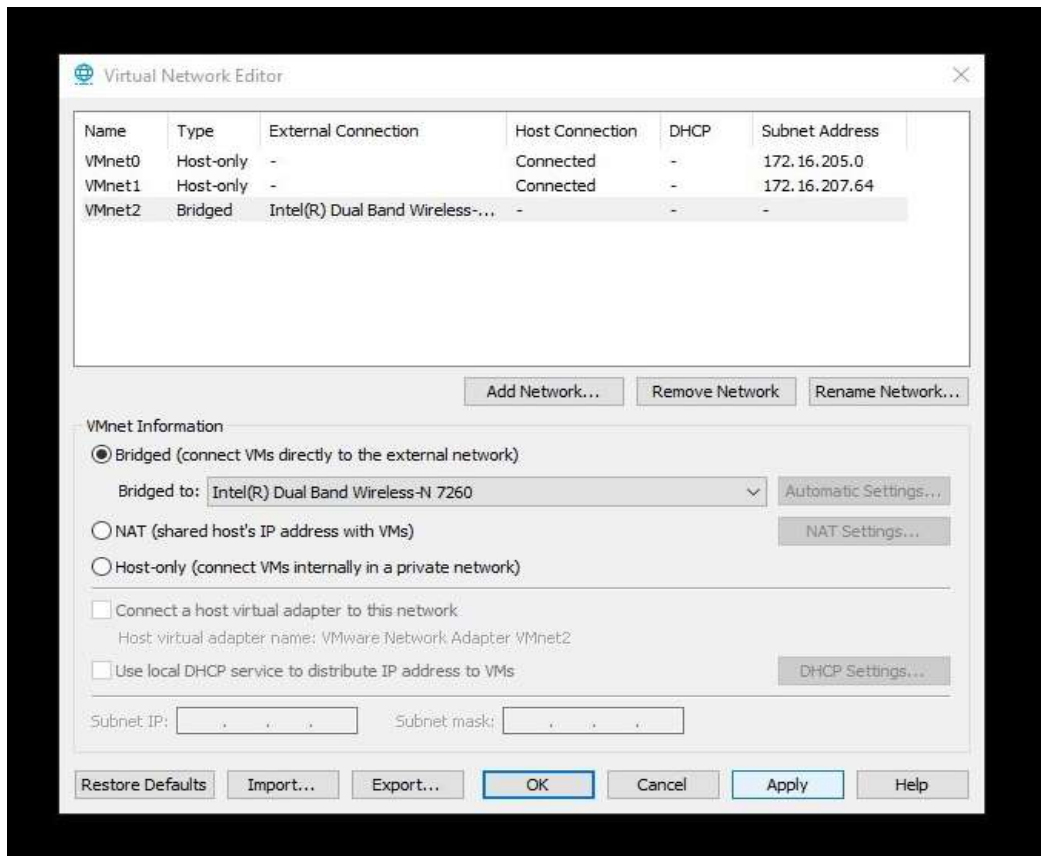
On coche Host-Only puis on entre l'adresse réseau 172.16.207.64/27 ainsi que son masque car cette interface sera celle qui connectera notre réseau LAN.

NB : Faites la même chose pour le Vmnet0 tout en configurant l'adresse réseau 172.16.205.0/26 car cette interface sera celle qui connectera notre hôte physique à notre machine virtuelle



Nous allons maintenant configurer notre interface vmnet qui nous permettra d'aller sur internet :

- On fait Add Network puis on crée l'interface Vmnet2
- On coche Bridged et on déroule la liste qui contient les cartes réseaux
- On sélectionne « Wireless dual band » sur Windows et « Wlan0 » sur linux.

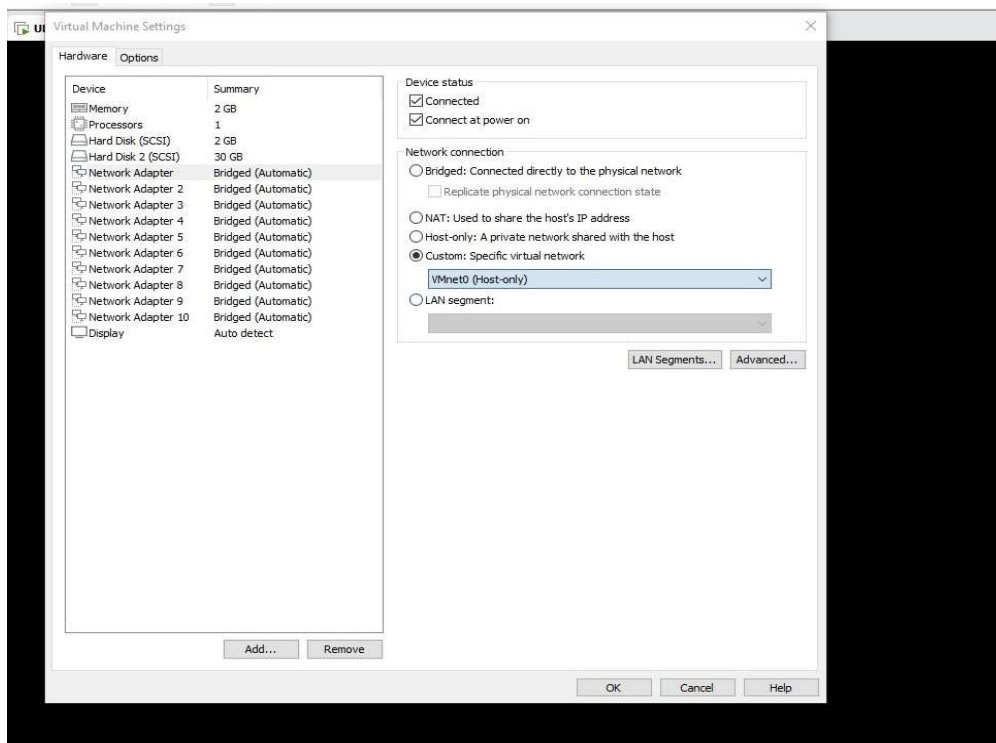


Une fois que c'est terminer on clique sur « Apply » puis sur « OK ».

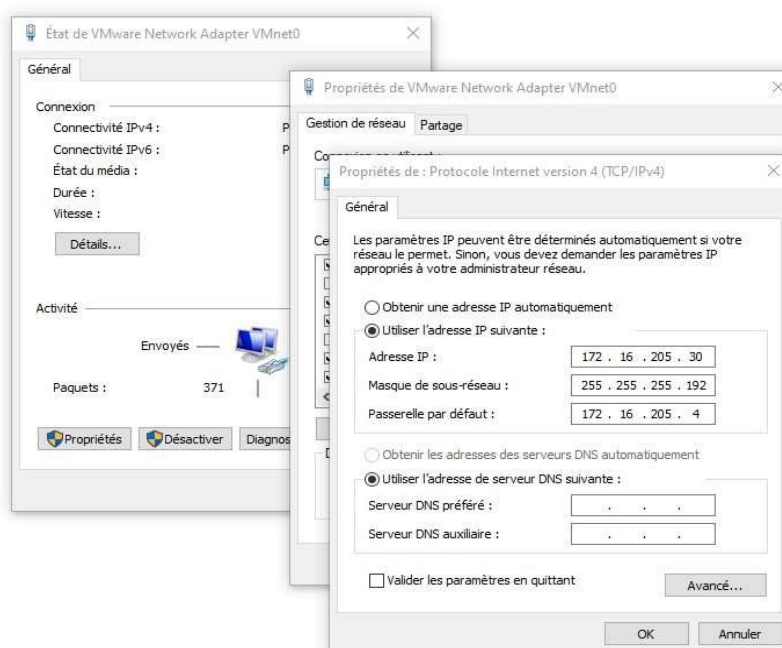
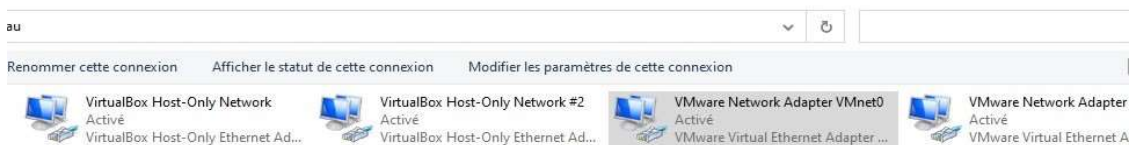
.....

*Configuration de notre port1 sur notre pare-feu

- On sélectionne la première carte réseau qui représente notre port1 puis on le met en « custom » ensuite « vmnet0 »



Après cela nous allons sur notre machine physique et nous allons éditer la carte virtuelle Vmnet0 en lui donnant une adresse IP qui est dans le même réseau que l'adresse IP du port1 de notre fortigate.



Si l'étape précédente est validée on effectue un Ping vers l'adresse IP du port1 de notre Fortiget. On ouvre notre navigateur et on insère l'adresse du port 1 de notre fortiget dans l'url :

Dans notre cas c'est <http://172.16.205.4>



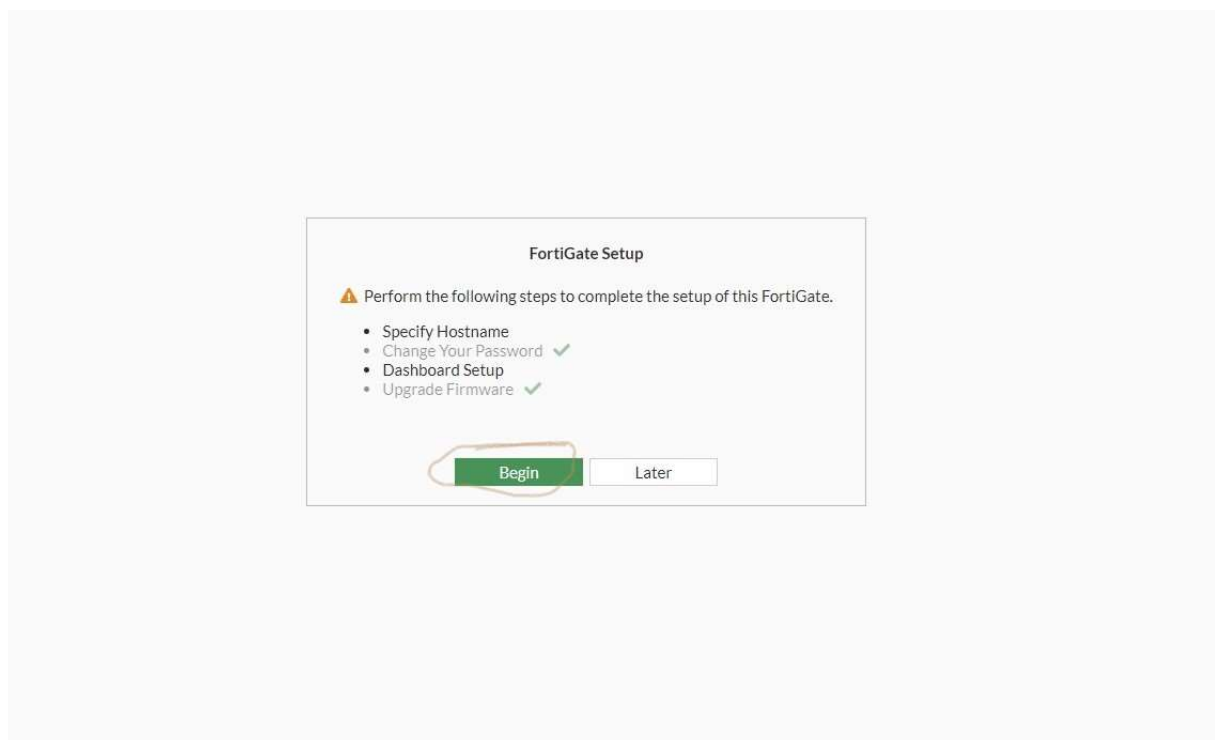
Username

Password

Login



-On insère notre nom d'utilisateur et notre mot de passe configuré dans l'étape 1.



Setup Progress	Specify Hostname
<ul style="list-style-type: none"> > Specify Hostname Change Your Password ✓ Dashboard Setup Upgrade Firmware ✓ 	<p>By default, this FortiGate will use the serial number/model as its hostname. It is strongly recommended to set a descriptive hostname to make this FortiGate more identifiable.</p> <p>Use default hostname ? <input type="checkbox"/></p> <p>Hostname <input type="text" value="FORTINET_UPB"/></p> <p> <input type="button" value="OK"/> <input type="button" value="Later"/> </p>

Setup Progress	Dashboard Setup
<ul style="list-style-type: none"> Specify Hostname ✓ Change Your Password ✓ > Dashboard Setup Upgrade Firmware ✓ 	<p>Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later.</p> <p> <input checked="" type="radio"/> Optimal A set of popular default dashboards and FortiView monitors. </p> <p> <input type="radio"/> Comprehensive A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions </p> <p> <input type="button" value="OK"/> <input type="button" value="Later"/> </p>

Nous allons dans le menu > Network>Interfaces>port 2.

Nous allons donc configurer le port 2 de notre Fortiget qui sera le port de notre réseau Interne.

Avant cela nous allons créer un groupe d'utilisateur et des utilisateurs qui pourront s'authentifier via le portail captif que nous allons créer sur notre port2.

FortiGate - FORTINET_UPB

Non sécurisé | 172.16.205.4/ng/user/local

FORTINET_UPB

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
 - User Definition
 - User Groups
 - Guest Management
 - LDAP Servers
 - RADIUS Servers
 - Single Sign-On
 - Authentication Settings
 - FortiTokens
- System
- Security Fabric
- Log & Report

Create New Edit Clone Delete Search

Name	Type	Two-factor Authentication	Groups	Status	Ref.
guest	LOCAL		Guest-group	Enabled	1

0 Security Rating Issues

Taper ici pour rechercher

29°C Edlairies 21:08 30/03/2023

FortiGate - FORTINET_UPB

Non sécurisé | 172.16.205.4/ng/user/wizard

FORTINET_UPB

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
 - User Definition
 - User Groups
 - Guest Management
 - LDAP Servers
 - RADIUS Servers
 - Single Sign-On
 - Authentication Settings
 - FortiTokens
- System
- Security Fabric
- Log & Report

Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

FortiNAC User

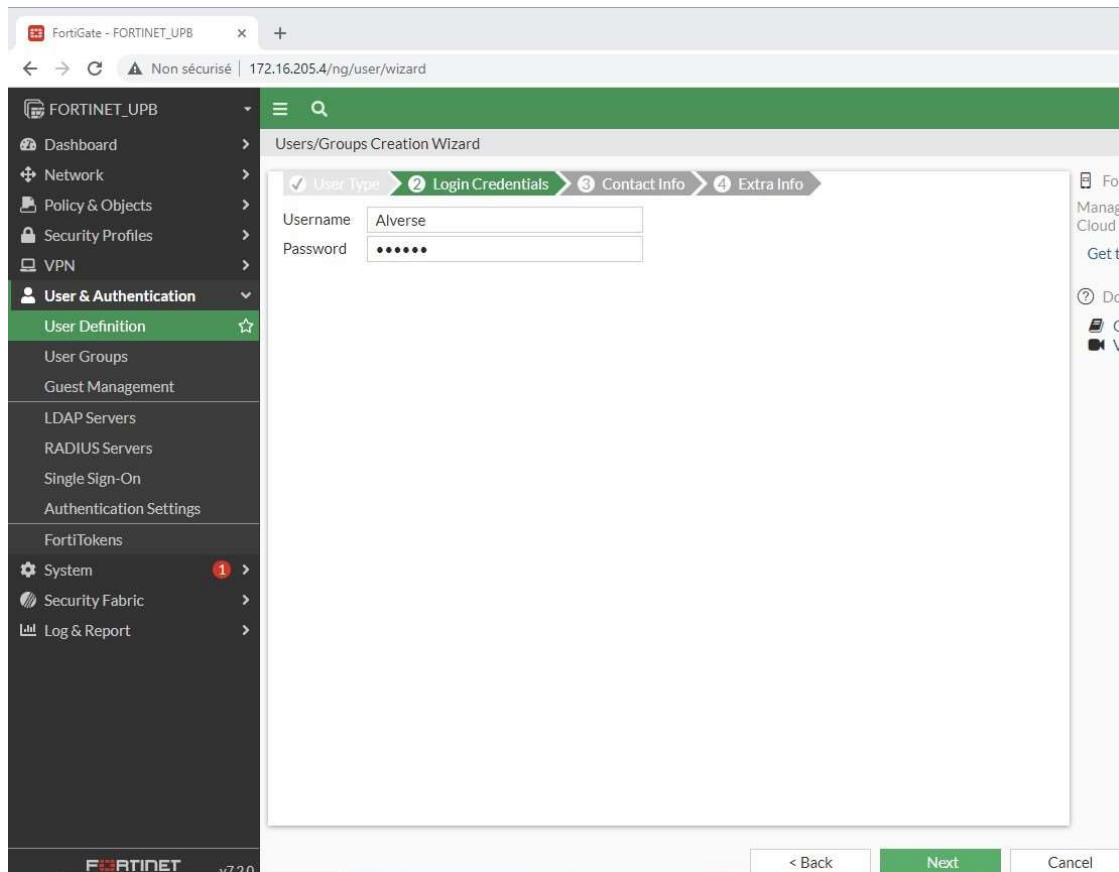
FortiEx Manage yo Cloud subs Get the a

Docum

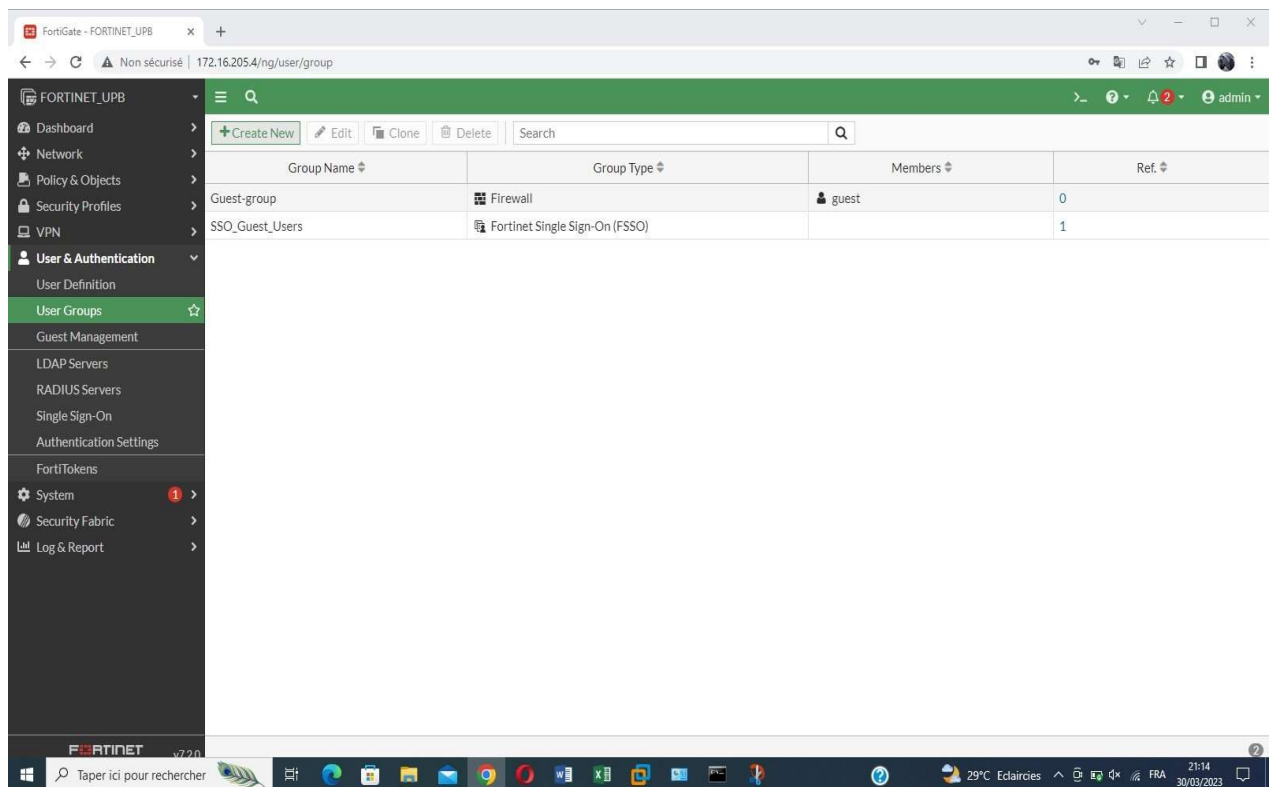
Onlin

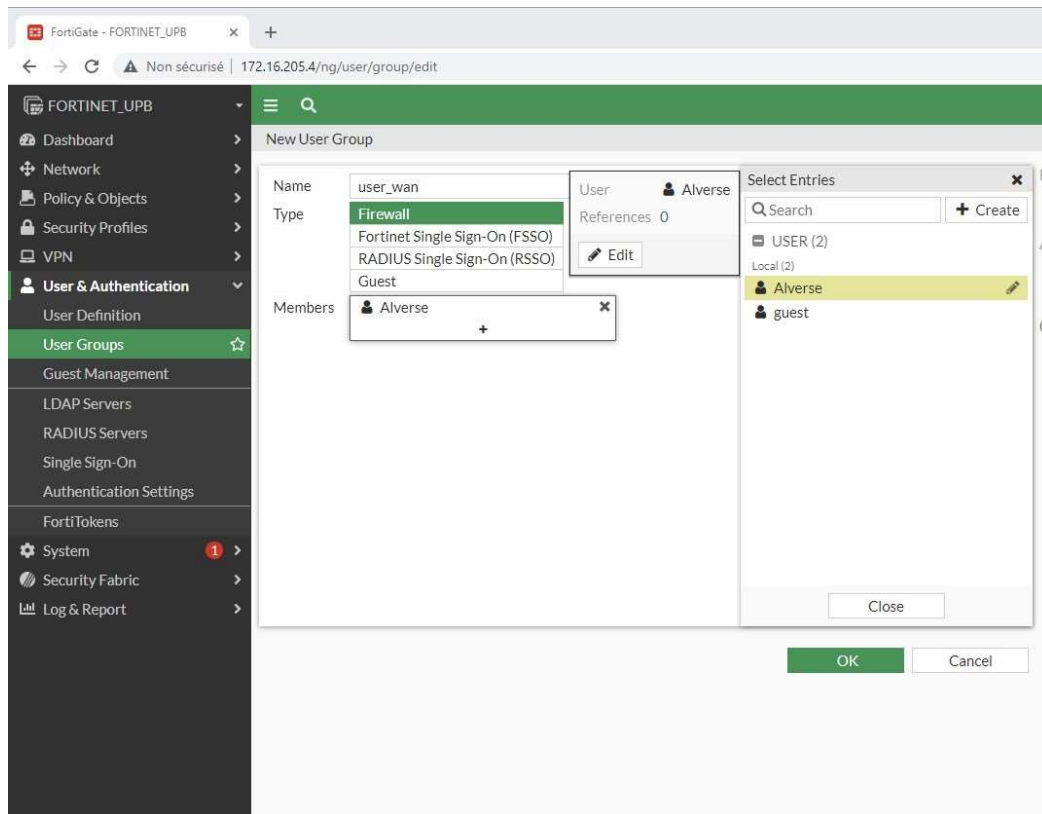
Videc

< Back Next Cancel

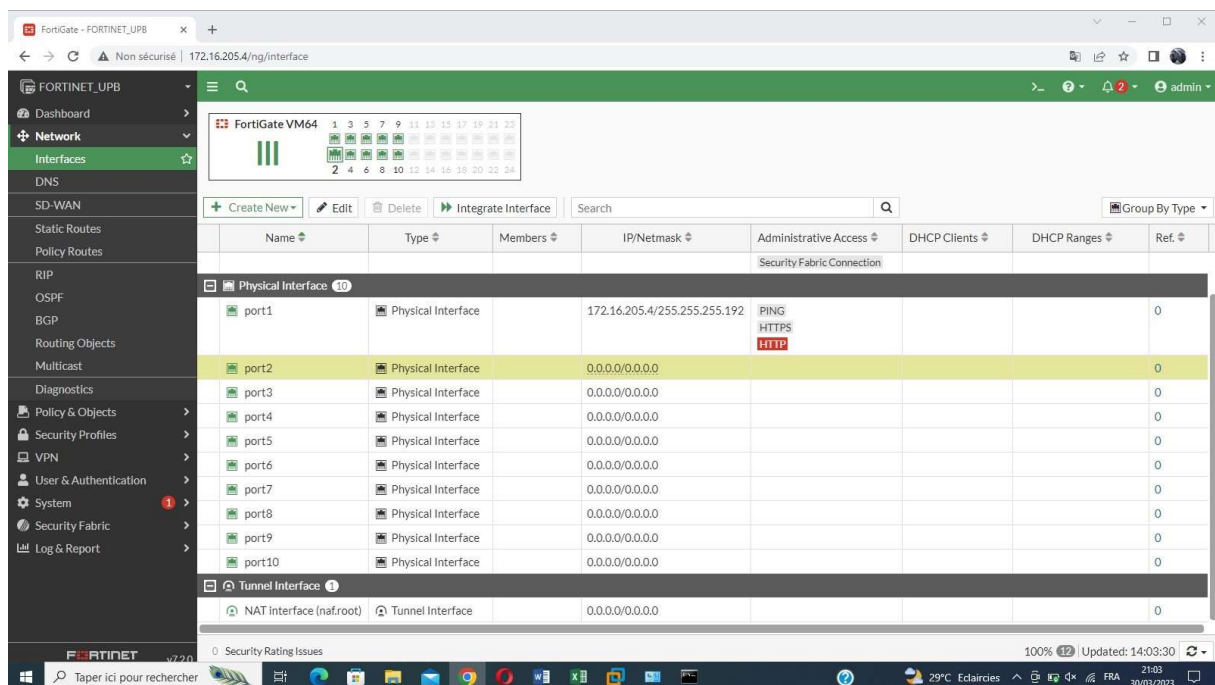


Ensuite nous allons créer le groupe auquel va appartenir l'utilisateur :

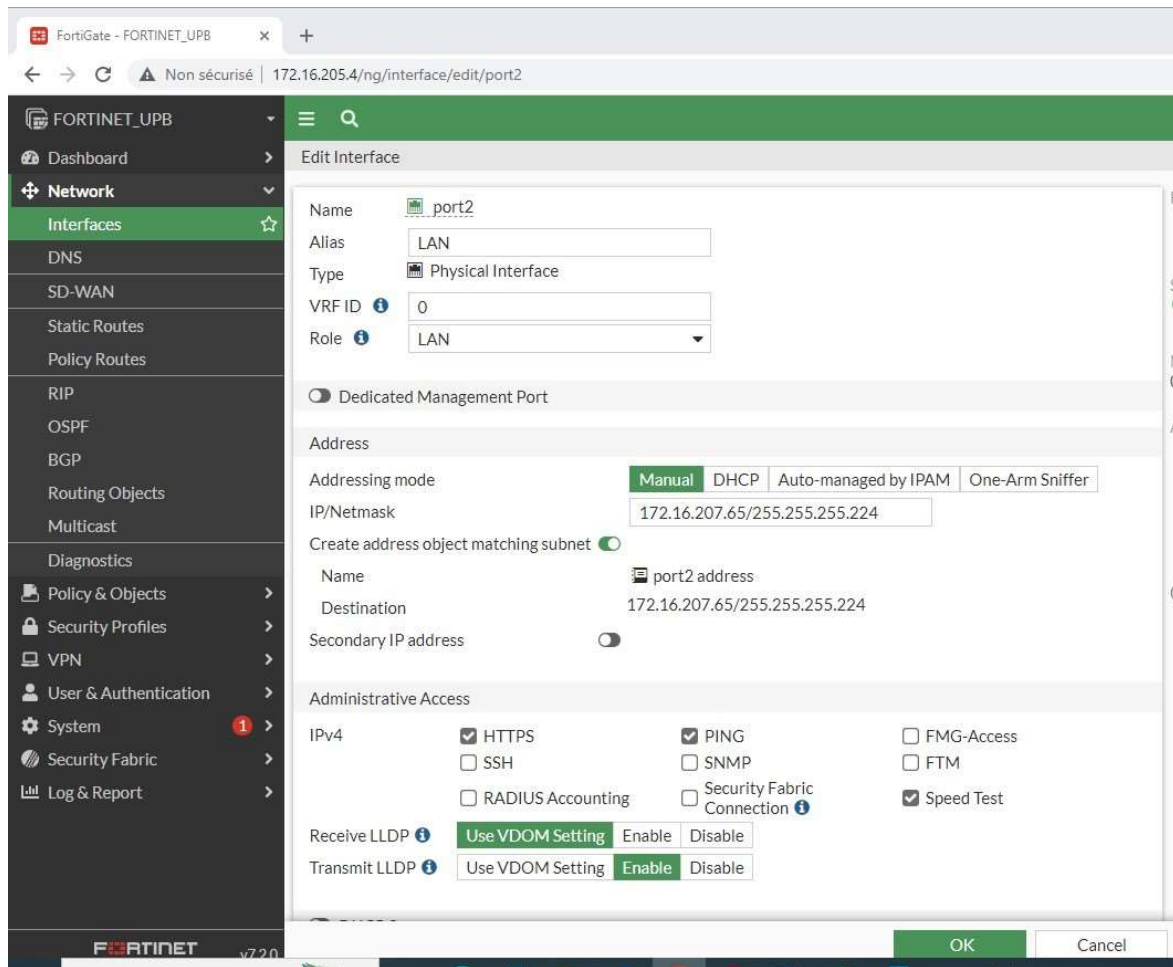




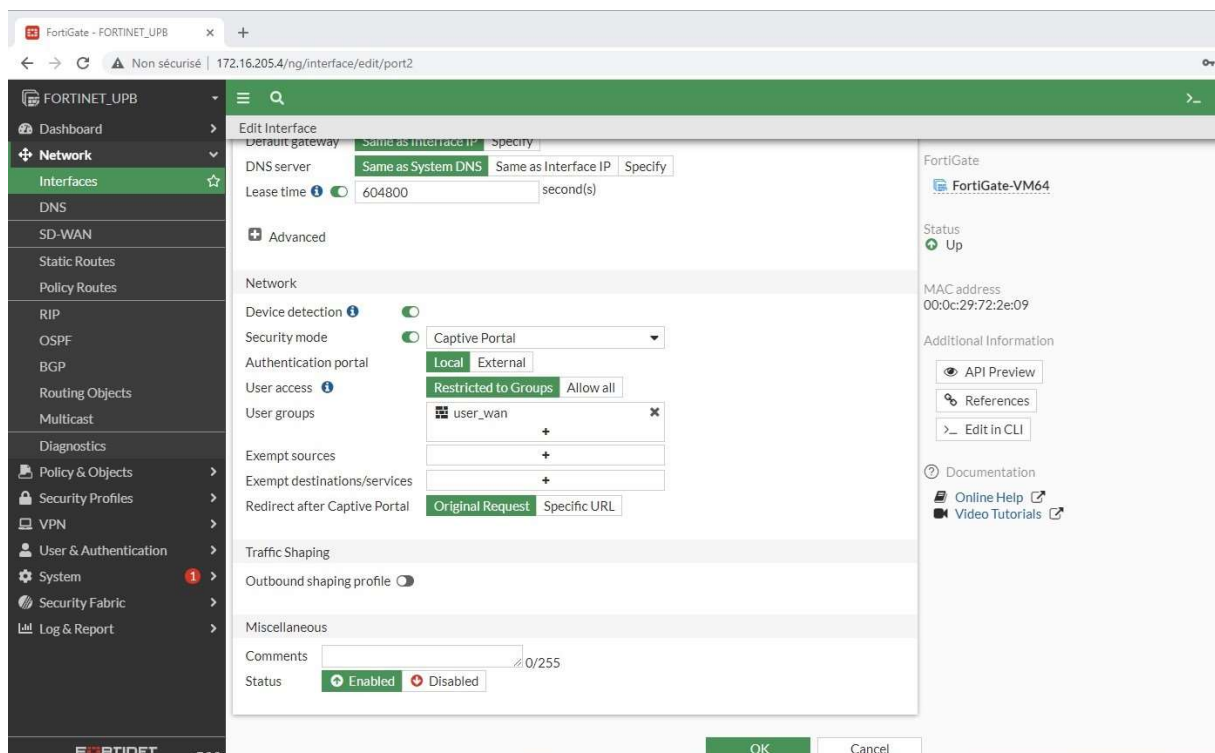
Après avoir créé l'utilisateur et le groupe d'utilisateur on vient ensuite éditer le port2 de notre pare-feu



On édite le port2 qu'on va appeler LAN



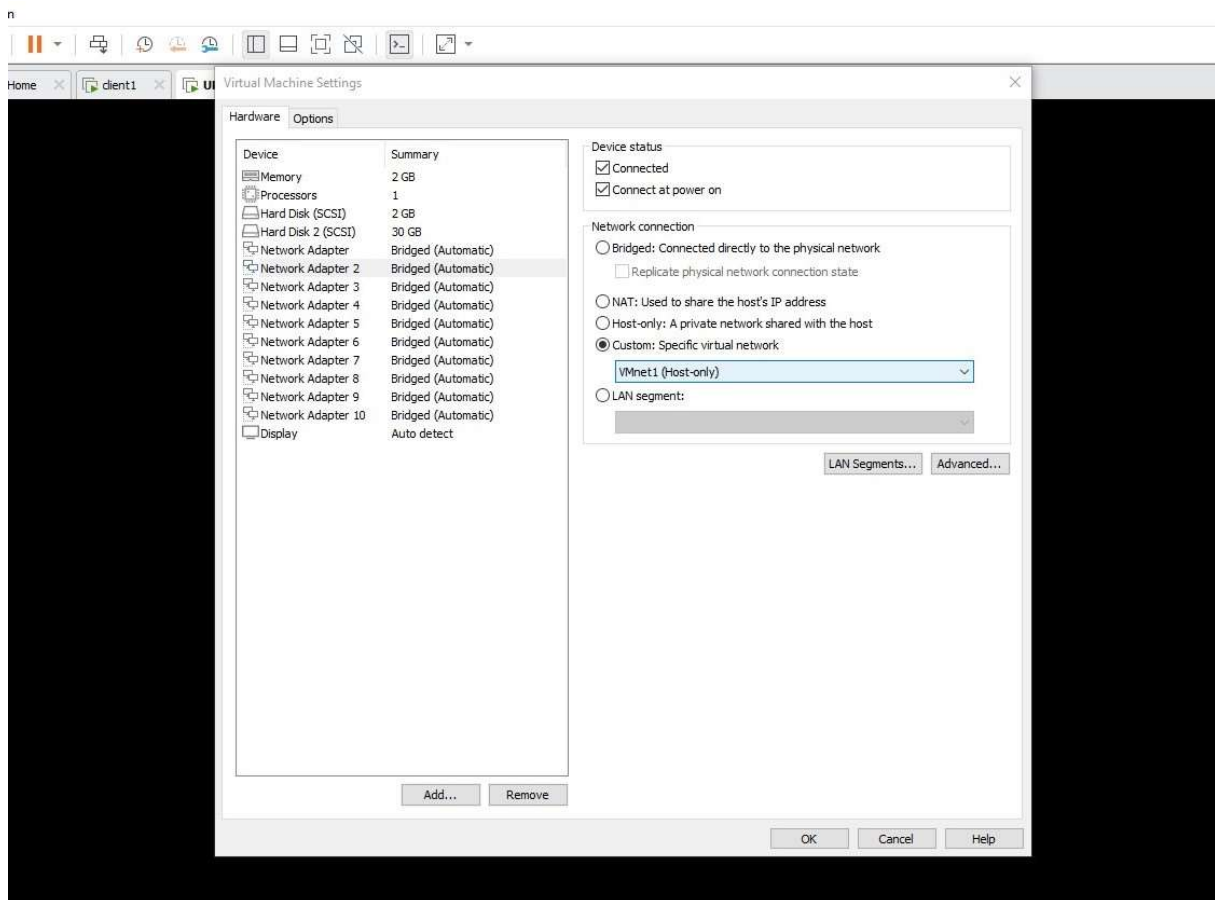
On active **Security mode** pour le portail captif, on clique sur **restricted Groups** puis on ajoute le groupe d'utilisateur créé précédemment



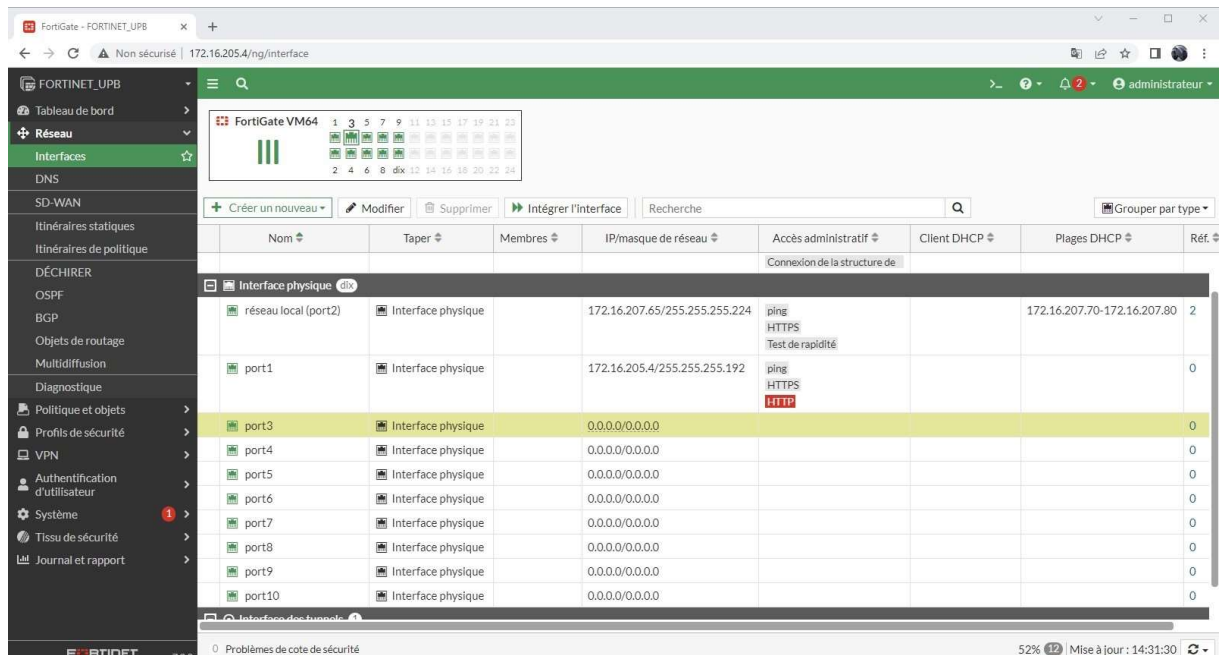
On active l'option DHCP server si nous voulons donner automatiquement des adresses aux hôtes du réseau LAN puis on fais « OK ».



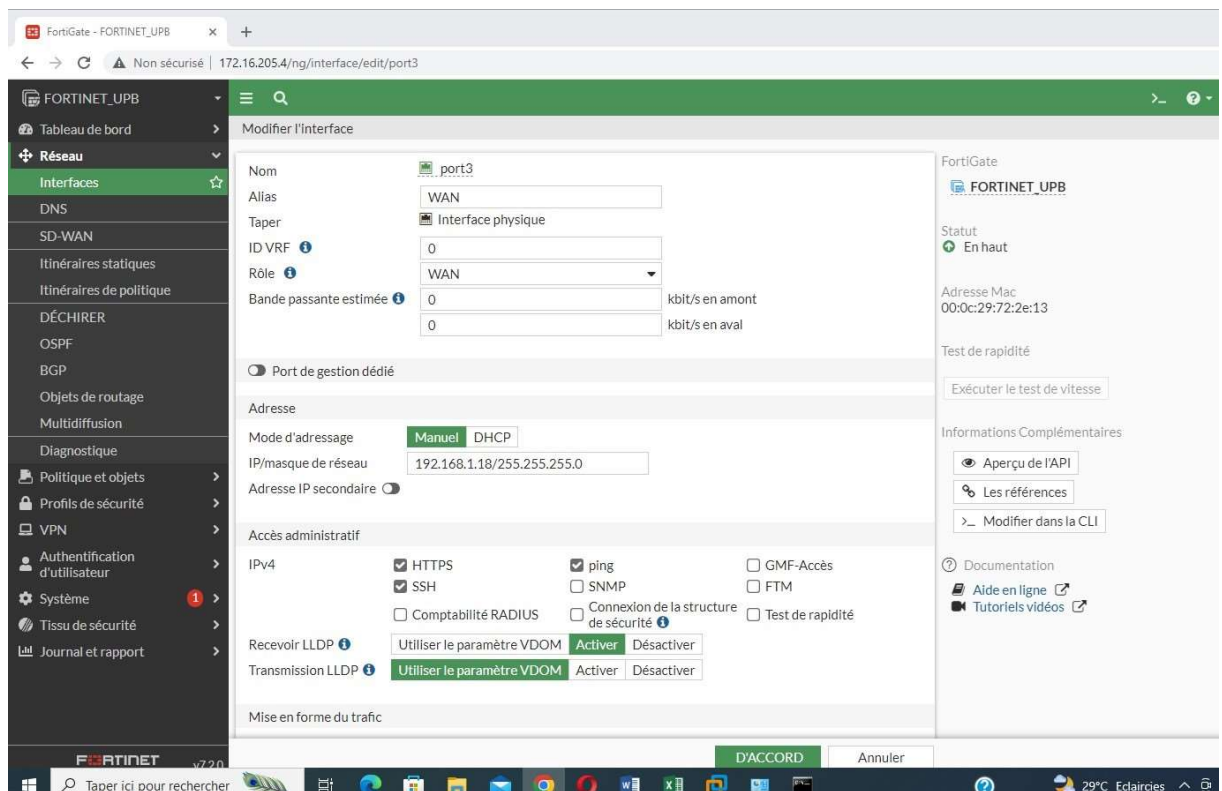
On se rend sur notre machine virtuelle fortigate puis on met l'interface 2 qui représente notre port2 en « Custom » et dans le « Vmnet1 » qu'on a dédié a notre réseau LAN



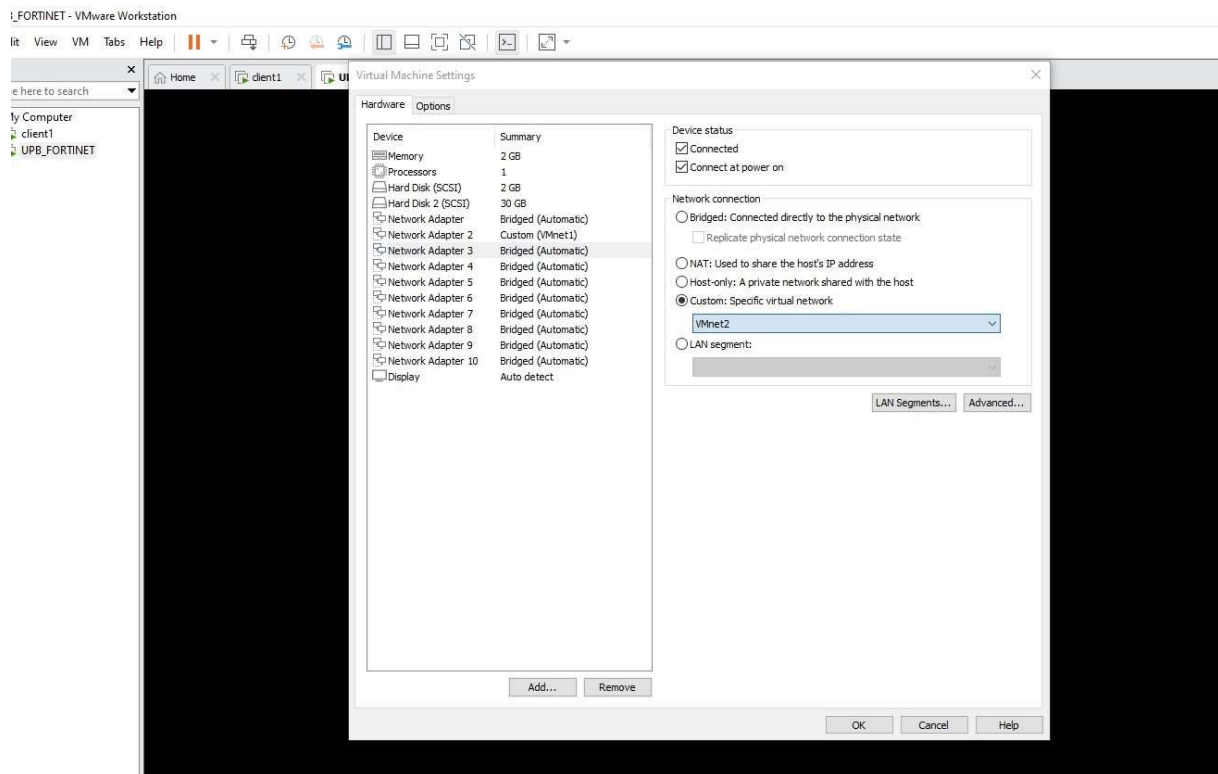
On passe à la configuration de notre port3 qui nous permettra de sortir sur internet.



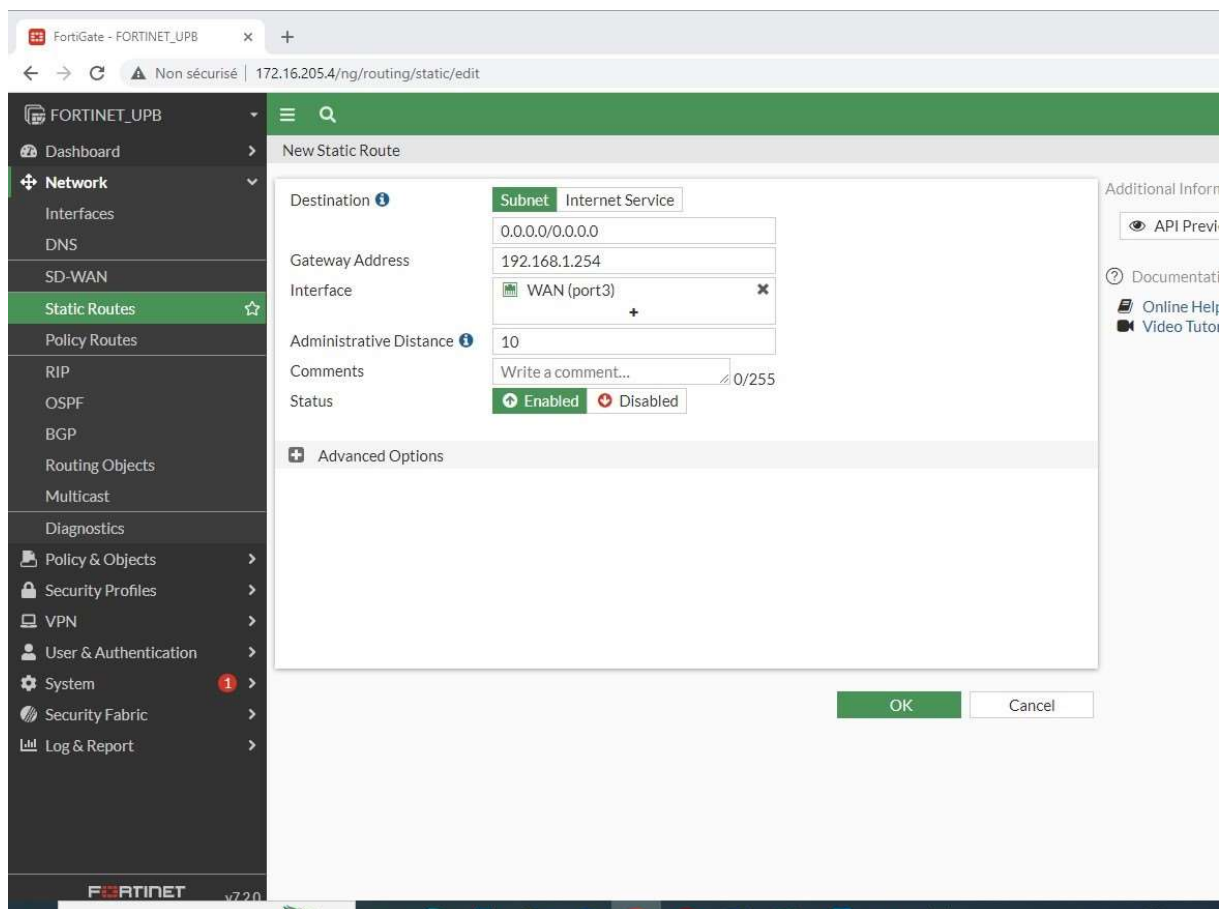
On met l'adresse distribuée par M. Goualo lors du TP puis on clique sur « D'ACCORD ».



On se rend ensuite sur notre machine virtuelle Fortigate puis on configure notre adaptateur 3 qui représente notre port3 en « custom » et « Vmnet2 »

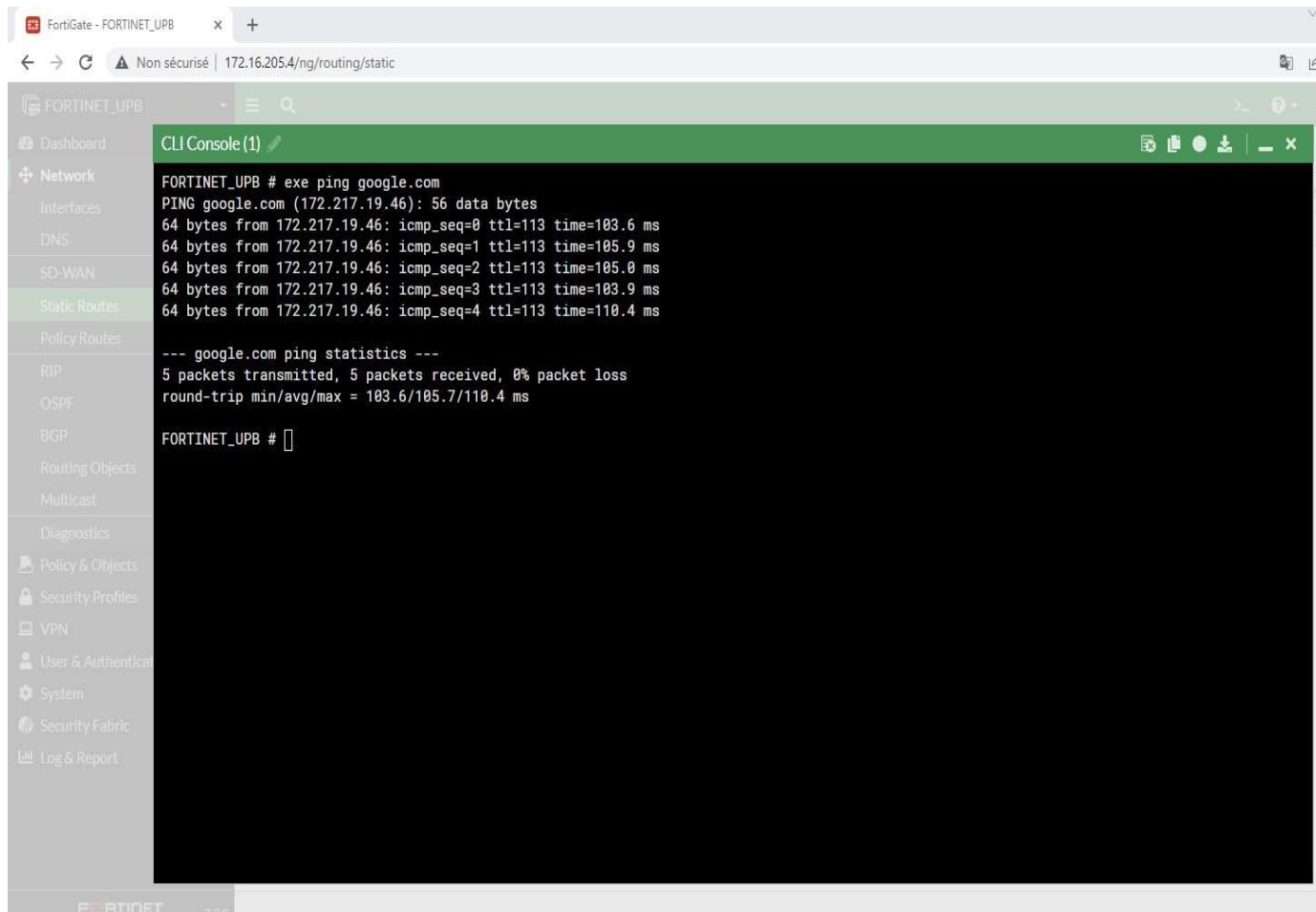


On crée ensuite une route par défaut :



On fait Ping vers google.com avec la commande: **exe ping google.com** pour vérifier l'état de connexion entre notre fortiget et internet :

NB : Assurez-vous que votre carte wifi est connectée à un point d'accès wifi



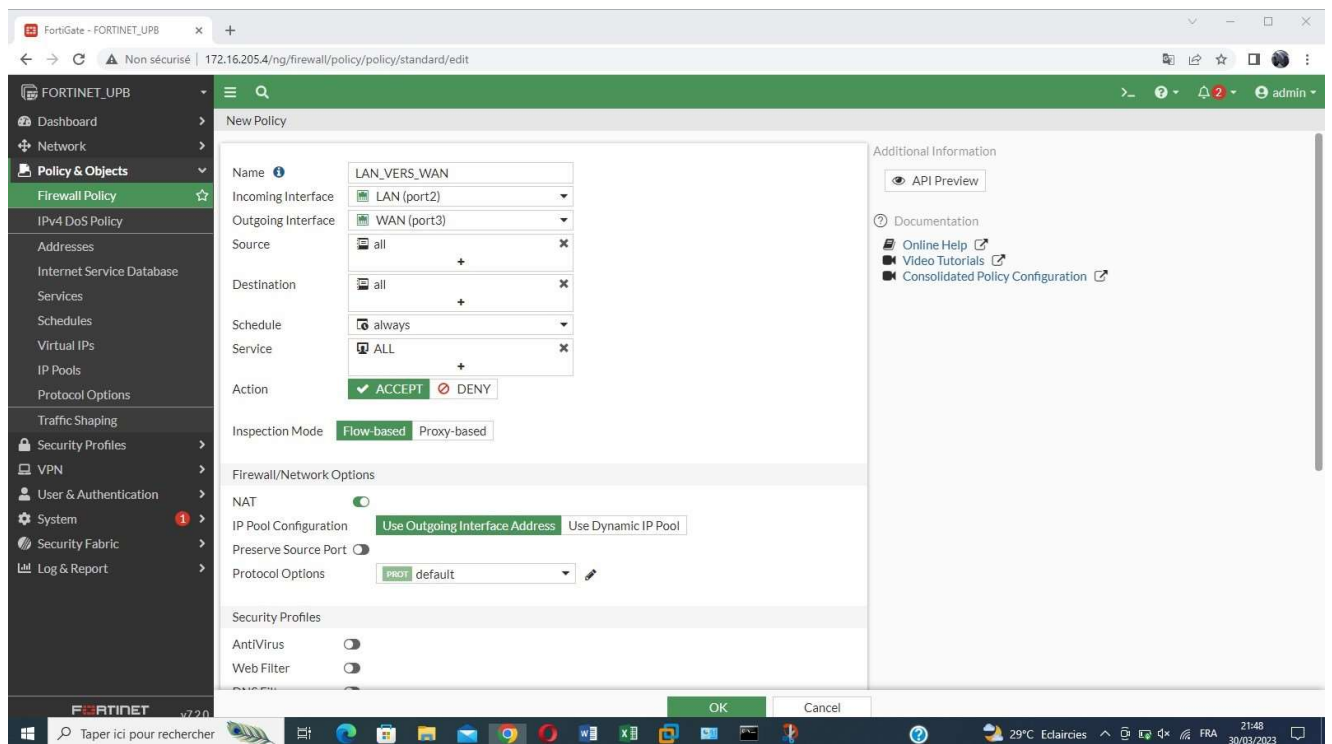
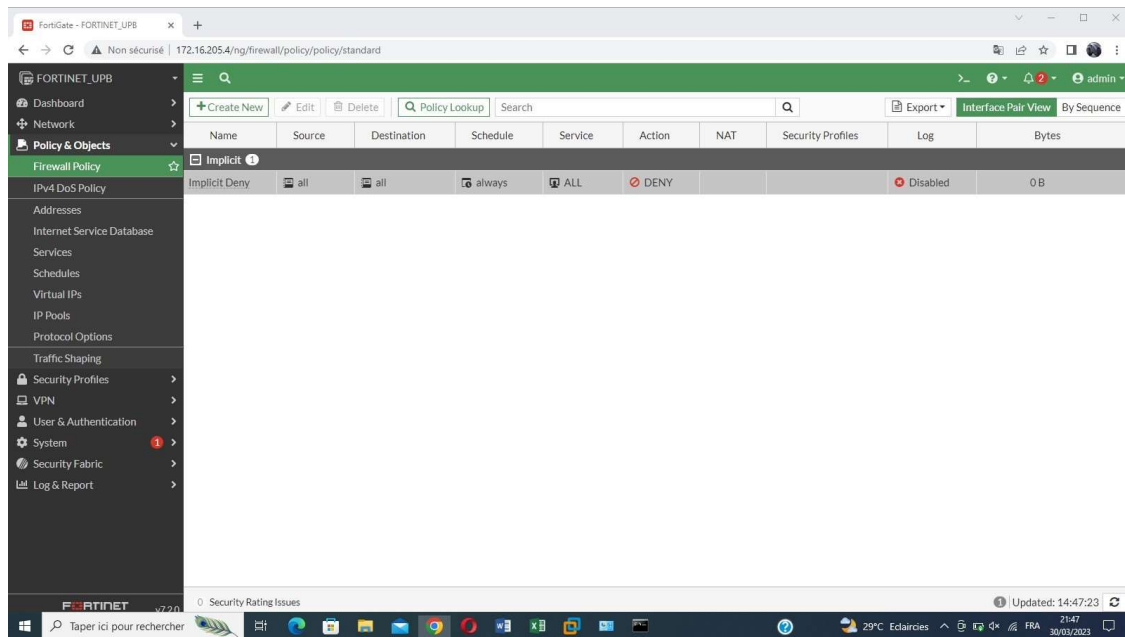
The screenshot shows the FortiGate web interface with the CLI console open. The console displays the command 'exe ping google.com' and its output, which includes five successful ping attempts with varying round-trip times and a summary statistics block.

```
FORTINET_UPB # exe ping google.com
PING google.com (172.217.19.46): 56 data bytes
64 bytes from 172.217.19.46: icmp_seq=0 ttl=113 time=103.6 ms
64 bytes from 172.217.19.46: icmp_seq=1 ttl=113 time=105.9 ms
64 bytes from 172.217.19.46: icmp_seq=2 ttl=113 time=105.0 ms
64 bytes from 172.217.19.46: icmp_seq=3 ttl=113 time=103.9 ms
64 bytes from 172.217.19.46: icmp_seq=4 ttl=113 time=110.4 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 103.6/105.7/110.4 ms

FORTINET_UPB #
```

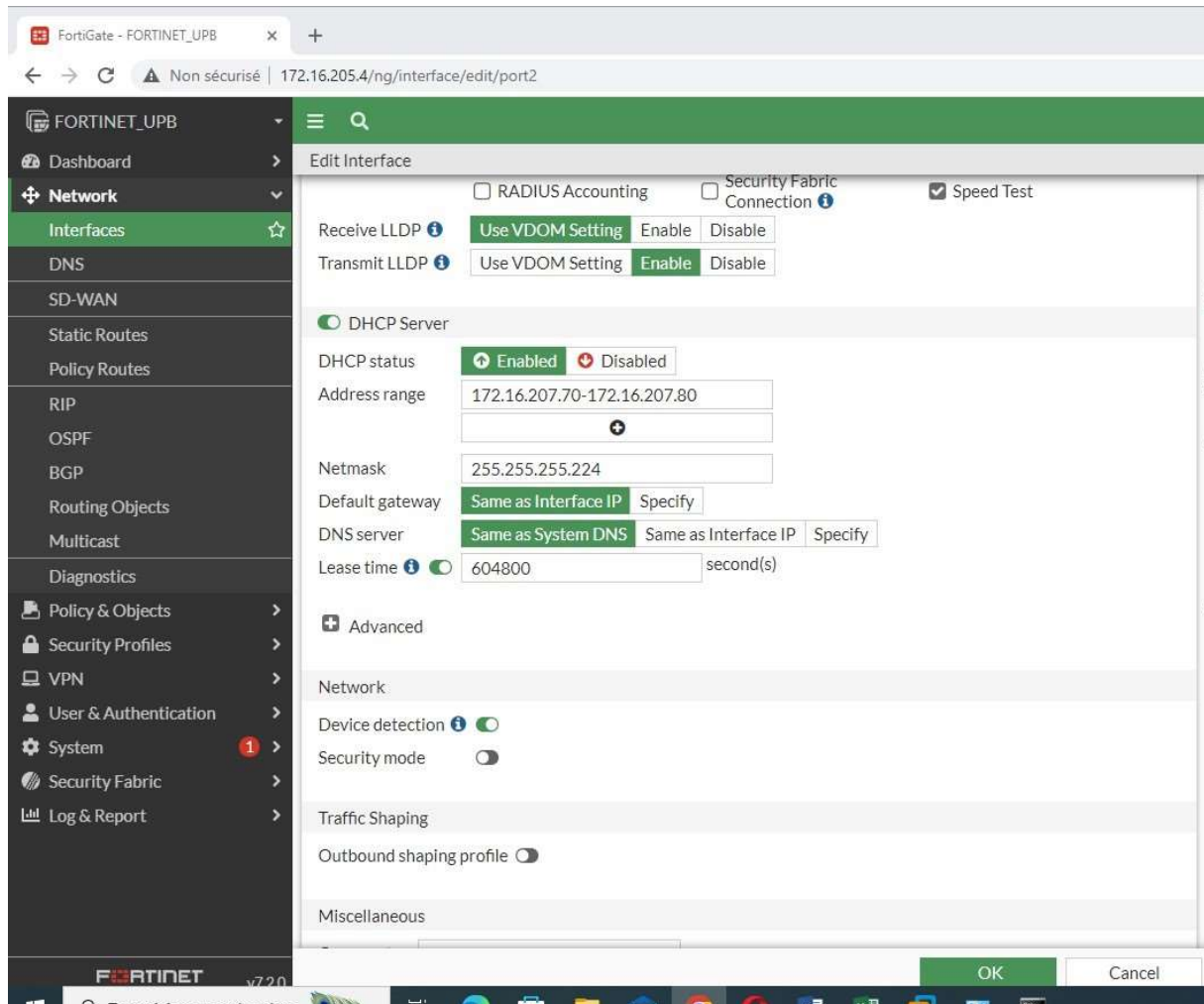
Il faut créer une règle qui permet d'autoriser le trafic entre notre Port2(LAN) et notre port3(WAN).

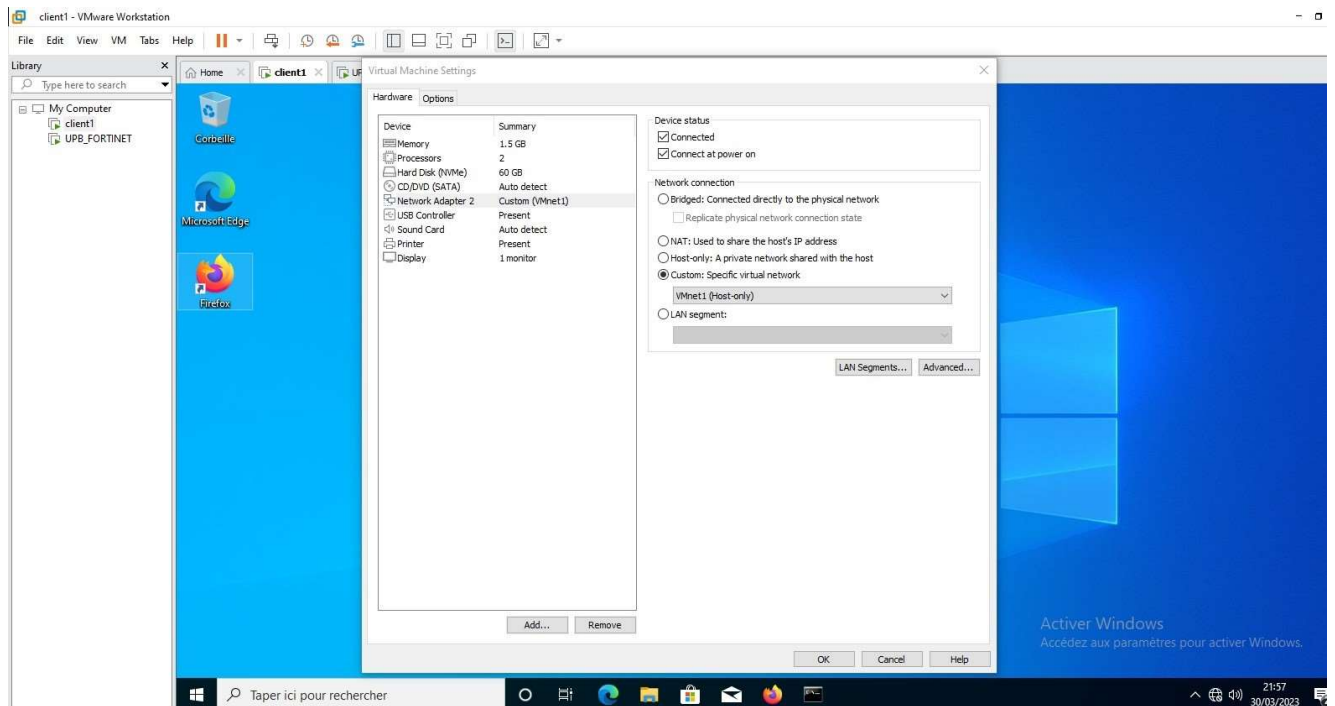


Rendons nous sur la machine virtuelle notre client1

-On met la carte réseau dans le même vmnet que celui du port LAN de notre fortiget qui est le vmnet1.

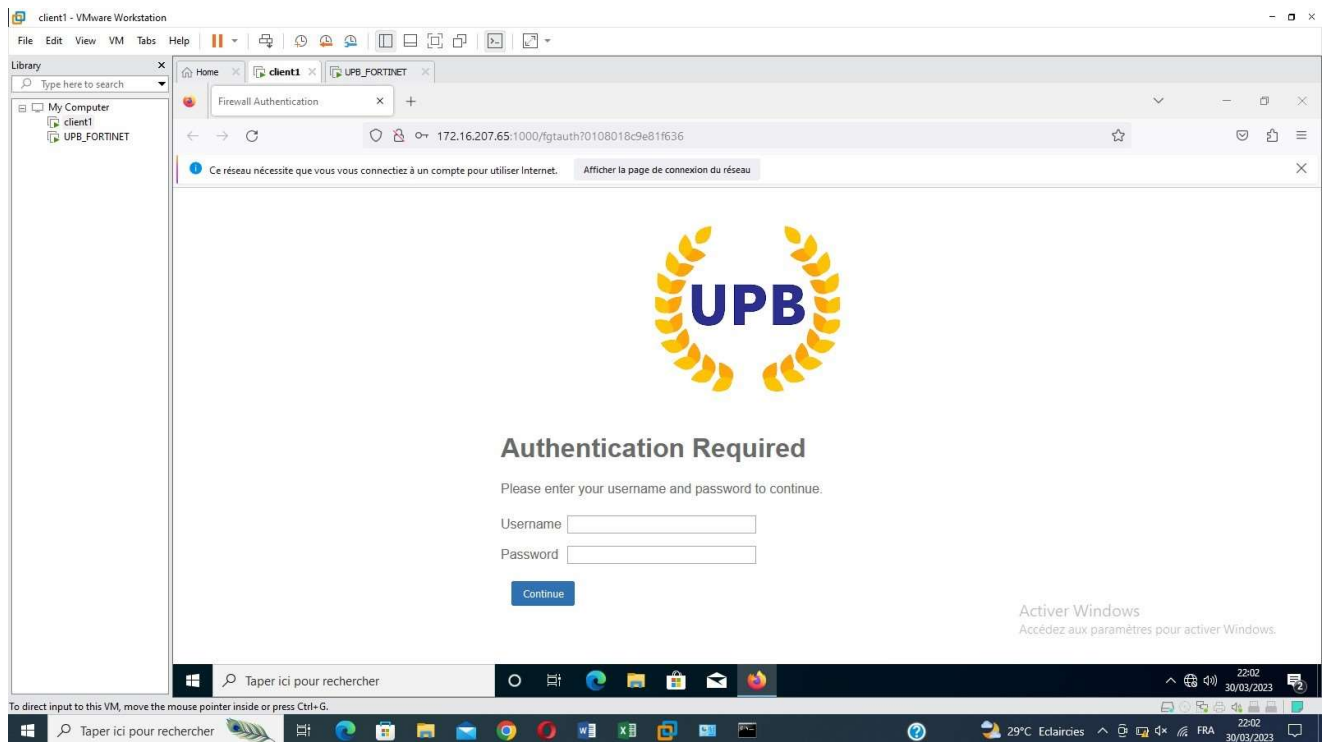
-Le client 1 reçoit automatiquement une adresse IP parce qu'on a activé le DHCP SERVER sur le port2 .





Le portail captif se lance automatiquement :

On insère le nom d'utilisateur et le mot de passe créé précédemment



Après l'authentification nous avons directement accès à internet.

