

# Pare-feu Fortigate

## I. Table des matières

II. Fortigate :	1
III. Les Prérequis :	1
La topologie physique et logique de l'infrastructure réseau.....	2
IV. Configuration du pare-feu Fortigate :	2
Installation .....	2
Configuration port 2 et port 10 .....	5
V. Configuration VM Windows 7 et Windows server 2022:.....	8
Installation et configuration réseaux des VM Windows 7 et Windows server 2022 .....	8
Vérification de la connexion Internet .....	10
VI. CONCLUSION :	12

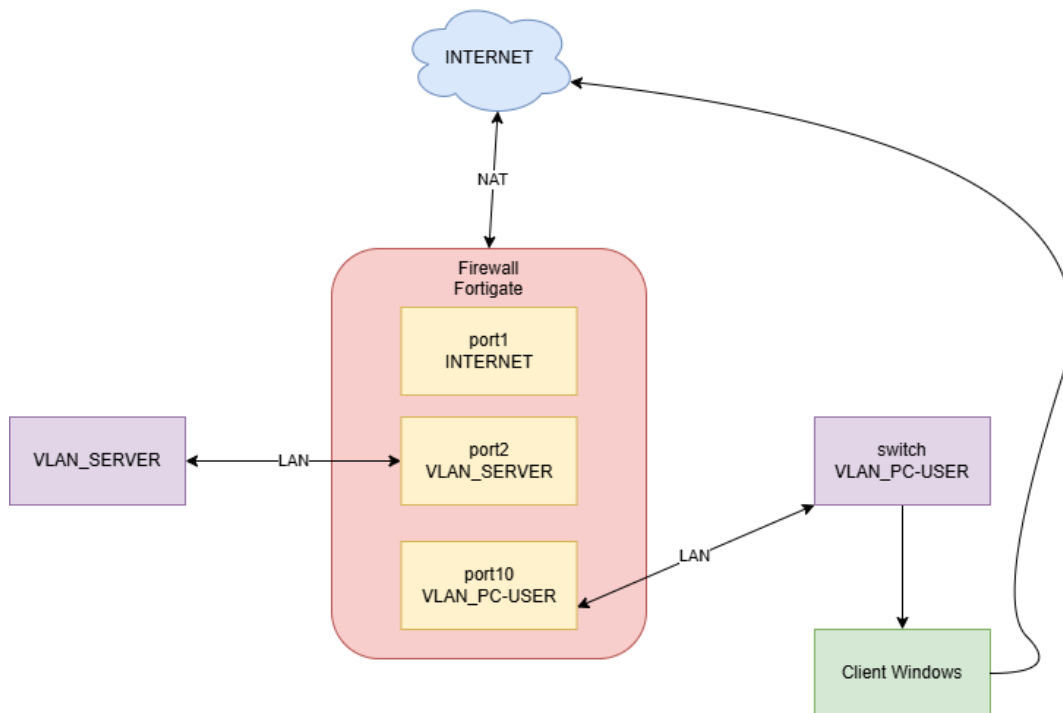
## II. Fortigate :

FortiGate est le [pare-feu réseau](#) le plus déployé, avec plus de 50 % de parts de marché au niveau mondial. Les pare-feu nouvelle génération (NGFW) FortiGate protègent les données, les ressources et les utilisateurs dans les environnements hybrides d'aujourd'hui. Basés sur les [processeurs de sécurité](#) brevetés Fortinet, les pare-feu NGFW FortiGate de Fortinet accélèrent les performances réseaux afin de sécuriser efficacement le volume croissant de trafic riche en données et les applications basées sur le cloud. Les pare-feu nouvelle génération FortiGate, soutenus par les services de [sécurité basée sur l'intelligence artificielle FortiGuard](#) , vous aident à prévenir les cyberattaques et à neutraliser les risques de sécurité grâce à une protection et des réponses persistantes et en temps réel, même contre les menaces les plus récentes et les plus sophistiquées.

## III. Les Prérequis :

Pour la configuration réseaux de base du pare-feu Fortigate je vais avoir besoin d'installer VMware Workstation Pro ensuite j'aurais besoin d'une machine virtuel Fortigate, d'une machine virtuel Windows 7 et pour finir d'une machine virtuel Windows server 2022.

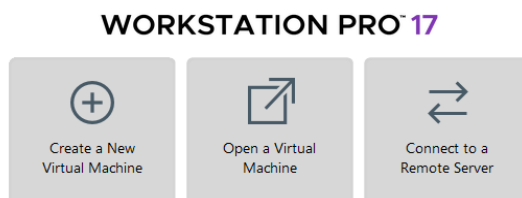
# La topologie physique et logique de l'infrastructure réseau

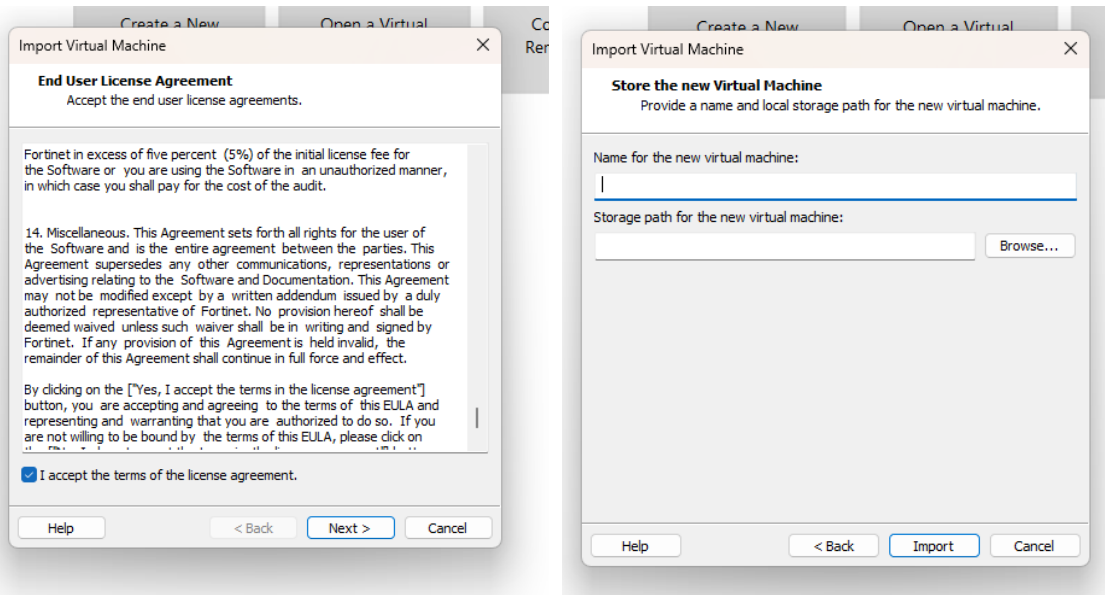


## IV. Configuration du pare-feu Fortigate :

### Installation

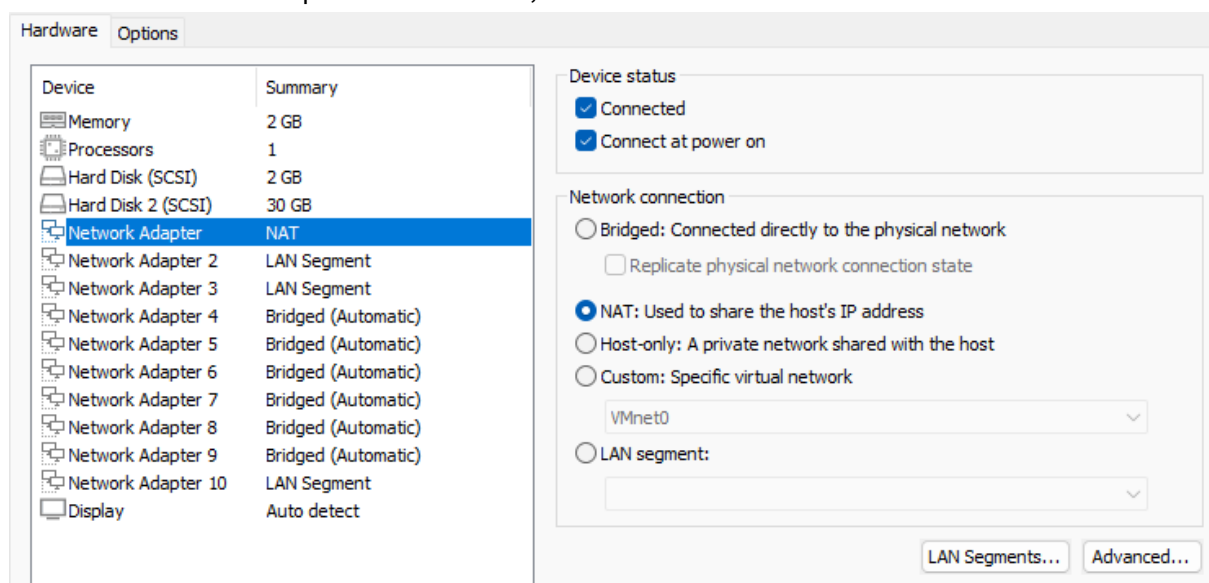
Après avoir complété les prérequis il nous faut aller sur VMware et cliquer sur « Open a Virtual Machine ».





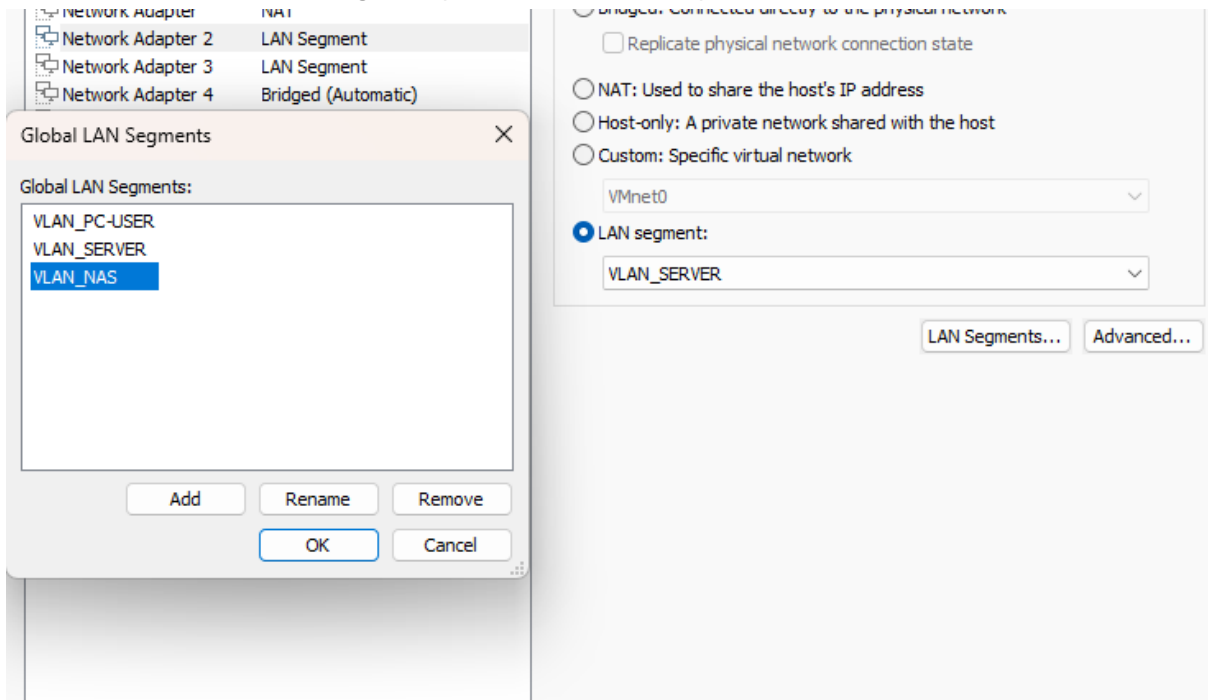
Ensuite je coche la case et je fais « Next »,  
et importe sans forcément donner de nom car sa donnera le même nom que le fichier utilisé,

Après avoir installé la machine virtuelle Fortigate ouvrir la machine virtuelle et avant de l'allumer on doit d'abord aller dans VM puis settings en haut à gauche un fois dans setting on va aller dans Network Adapter et cocher Nat,

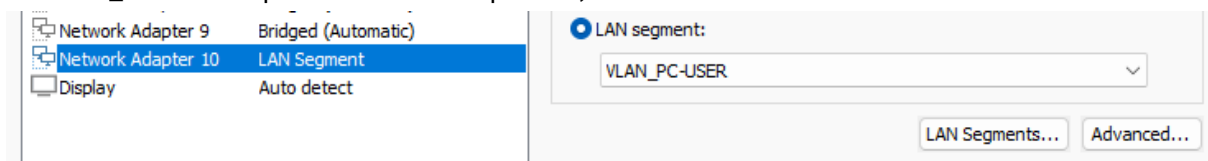


Puis on va cliquer sur Network Adapter 2 puis cocher LAN segment et appuyer sur le bouton LAN segments puis add et on va ajouter VLAN\_PC-USER, VLAN\_SERVER et sélectionner

VLAN\_SERVER dans LAN segment pour le Network Adapter 2,



Et VLAN\_PC-USER pour Network Adapter 10,



En appuyant sur « power on this virtual machine » et lorsque vous arrivez sur login il faut mettre admin et pour le password il ne faut rien mettre car fortigate va vous demander de mettre un nouveau mot de passe mettez admin comme le login pour que ce soit plus simple.

Une fois connecter il faut ensuite executer les commande suivante :

Config system interface

Pour entrer dans l'interface du system.

```

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-UM64 # Timeout

FortiGate-UM64 login:
FortiGate-UM64 login: admin
Password:
Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-UM64 # ^

FortiGate-UM64 #
    
```

```

It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-UM64 # Timeout

FortiGate-UM64 login:
FortiGate-UM64 login: admin
Password:
Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-UM64 # ^

FortiGate-UM64 # config system interface
FortiGate-UM64 (interface) # _
    
```

Puis entrer dans le port 1 avec la commande « edit port1 » puis la commande « set allowaccess ping ssh http https » pour configurer le port 1.

```
FortiGate-UM64 (interface) # edit port1
FortiGate-UM64 (port1) # set allowaccess ping ssh http https_
```

Ensuite il faut utiliser les commande suivante :

- Get system interface physical
- Show system interfaces

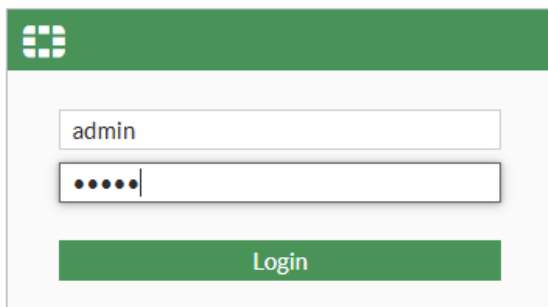
Pour bien vérifier que les configuration sur le port1 on bien été faite.

```
==[port1]
mode: dhcp
ip: 192.168.10.128 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
==[port2]
mode: static
ip: 172.16.3.254 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
==[port3]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
==[port4]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: up
FortiGate-UM64 # get system interface physical
```

```
edit "port1"
set vdom "root"
set mode dhcp
set allowaccess ping https ssh http
set type physical
set alias "INTERNET"
set snmp-index 1
next
edit "port2"
set vdom "root"
set ip 172.16.3.254 255.255.255.0
set allowaccess ping
set type physical
set alias "ULAN_SERVER"
set snmp-index 2
next
edit "port3"
set vdom "root"
set type physical
set snmp-index 3
next
edit "port4"
set vdom "root"
FortiGate-UM64 # show system interface
```

## **Configuration port 2 et port 10**

Une fois la configuration sur la machine virtuelle Fortigate il faut aller sur un navigateur et entrer son adresse ip du port 1, ensuite on arrive sur une page qui demande de rentrer son login et son password se sont les même que ceux entrer dans fortigate.



Ensuite on arrive sur l'écran d'accueil et en haut à droite il y a ce symbole , on clique dessus et on arrive sur l'invite de commande de fortigate puis on vérifie si on a accès à internet

grace au commande suivante :

```
CLI Console (1)
FortiGate-VM64 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=38.3 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=39.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=38.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=37.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=38.8 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 37.6/38.5/39.6 ms

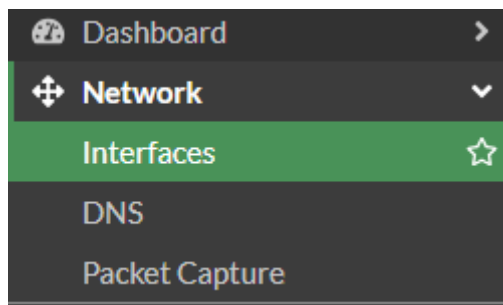
FortiGate-VM64 # execute ping google.fr
PING google.fr (142.250.217.163): 56 data bytes
64 bytes from 142.250.217.163: icmp_seq=0 ttl=128 time=39.5 ms
64 bytes from 142.250.217.163: icmp_seq=1 ttl=128 time=38.0 ms
64 bytes from 142.250.217.163: icmp_seq=2 ttl=128 time=38.3 ms
64 bytes from 142.250.217.163: icmp_seq=3 ttl=128 time=41.1 ms
64 bytes from 142.250.217.163: icmp_seq=4 ttl=128 time=38.0 ms

--- google.fr ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 38.0/38.9/41.1 ms

FortiGate-VM64 #
```

Si ça donne ce résultat cela veut de qu'on a accès a internet.

Ensuite a gauche dans le menus on va dans Network et dans interfaces,



On arrive sur une interface où on peut voir tous les ports et on voit le port1 que l'on a configuré sur la machine virtuel Fortigate, on va dans le port 10 pour le configurer et donner accès a internet au client qui font parti du VLAN\_PC-USER, donc on renome le port 10 VLAN\_PC-USER, on lui donne comme adresse ip 192.168.3.254 et masque de sous-reseaux 255.255.255.0, et enfin on lui donne acces a la commande ping et on appuie sur ok.

Name	<input type="text" value="VLAN_PC-USER (port10)"/>
Alias	<input type="text" value="VLAN_PC-USER"/>
Type	<input type="text" value="Physical Interface"/>
VRF ID <span>?</span>	<input type="text" value="0"/>
Role <span>?</span>	<input type="text" value="Undefined"/>

**Address**

Addressing mode: **Manual** | DHCP | Auto-managed by FortiIPAM

IP/Netmask: 192.168.3.254/255.255.255.0

Secondary IP address:

---

**Administrative Access**

IPv4:  HTTPS  PING  FMG-Access  
 SSH  SNMP  FTM  
 RADIUS Accounting  Security Fabric Connection ⓘ

Receive LLDP ⓘ: **Use VDOM Setting** | Enable | Disable

Transmit LLDP ⓘ: **Use VDOM Setting** | Enable | Disable

Et on fait la même chose pour le port2 mais cette fois on le renomme VLAN\_SERVER.

Name: VLAN\_SERVER (port2)

Alias: VLAN\_SERVER

Type: Physical Interface

VRF ID ⓘ: 0

Role ⓘ: Undefined ▼

---

**Address**

Addressing mode: **Manual** | DHCP | Auto-managed by FortiIPAM

IP/Netmask: 172.16.3.254/255.255.255.0

Secondary IP address:

---

**Administrative Access**

IPv4:  HTTPS  PING  FMG-Access  
 SSH  SNMP  FTM  
 RADIUS Accounting  Security Fabric Connection ⓘ

Receive LLDP ⓘ: **Use VDOM Setting** | Enable | Disable

Transmit LLDP ⓘ: **Use VDOM Setting** | Enable | Disable

Maintenant on va dans policy and objects et firewall policy pour pouvoir donner l'accès à internet au windows 7 et server, on appui sur create new puis on donne un nom a cette règle puis dans Incoming Interface VLAN\_PC-USER et dans Outgoing Interface Port1 qui se nomme INTERNET, ensuite dans Source et Destination on met all et dans service on met ping et Web Access.

Name	VLAN_PC-USER-TO-INTERNET
Incoming Interface	VLAN_PC-USER (port10)
Outgoing Interface	INTERNET (port1)
Source	all
Destination	all
Schedule	always
Service	PING Web Access

Name	VLAN_SERVER-TO-INTERNET
Incoming Interface	VLAN_SERVER (port2)
Outgoing Interface	INTERNET (port1)
Source	all
Destination	all
Schedule	always
Service	PING Web Access
Action	ACCEPT DENY

Et dans SSL Inspection on met certificates-inspection,

SSL Inspection SSL certificate-inspection

## V. Configuration VM Windows 7 et Windows server 2022:

### Installation et configuration réseaux des VM Windows 7 et Windows server 2022

Une fois fait on va devoir installer les machine virtuelle windows 7 et server 2022 de la manière que pour la machine virtuelle fortigate.

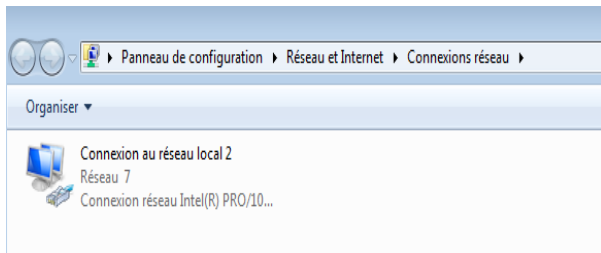
Ensuite on va dans leur settings puis dans Network Adapter et on coche LAN segment et on choisi VLAN\_PC-USER pour Windows 7 et VLAN\_SERVER pour Windows server 2022.

<ul style="list-style-type: none"> <li>Network Adapter</li> <li>USB Controller</li> <li>Display</li> </ul>	<p>LAN Segment</p> <p>Present Auto detect</p>	<p><input type="radio"/> Bridged: Connected directly to the physical network</p> <p><input type="checkbox"/> Replicate physical network connection state</p> <p><input type="radio"/> NAT: Used to share the host's IP address</p> <p><input type="radio"/> Host-only: A private network shared with the host</p> <p><input type="radio"/> Custom: Specific virtual network</p> <p>VMnet0</p> <p><input checked="" type="radio"/> LAN segment:</p> <p>VLAN_PC-USER</p> <p>LAN Segments... Advanced...</p>
<ul style="list-style-type: none"> <li>Network Adapter</li> <li>USB Controller</li> <li>Sound Card</li> <li>Display</li> </ul>	<p>LAN Segment</p> <p>Present Auto detect Auto detect</p>	<p><input type="radio"/> Bridged: Connected directly to the physical network</p> <p><input type="checkbox"/> Replicate physical network connection state</p> <p><input type="radio"/> NAT: Used to share the host's IP address</p> <p><input type="radio"/> Host-only: A private network shared with the host</p> <p><input type="radio"/> Custom: Specific virtual network</p> <p>VMnet0</p> <p><input checked="" type="radio"/> LAN segment:</p> <p>VLAN_SERVER</p> <p>LAN Segments... Advanced...</p>

Ensuite on allume les deux machines et on va dans la barre de recherche de windows et on tape ncpa.cpl pour accéder au connection réseaux.

Programmes (1)

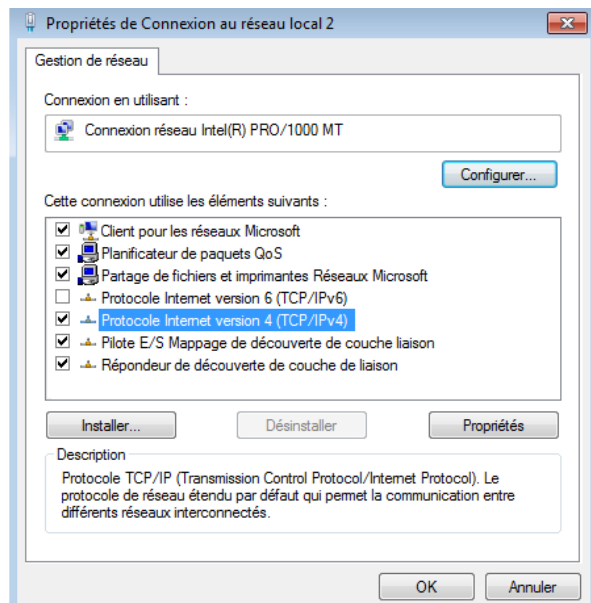
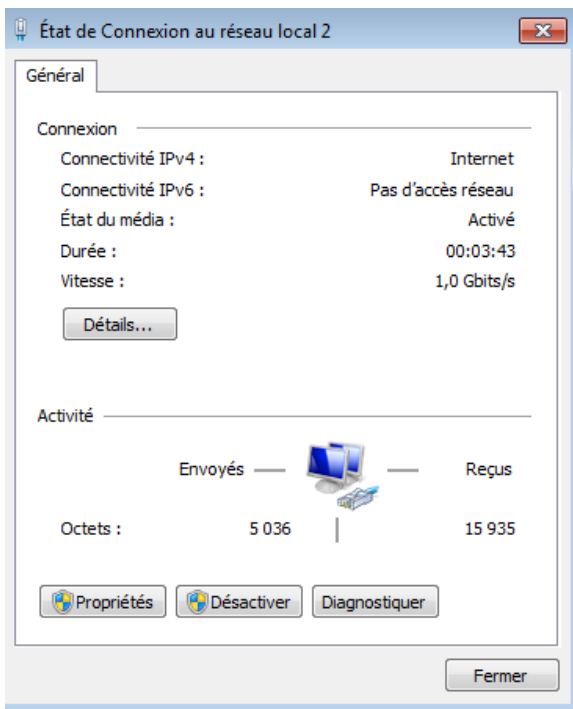
ncpa.cpl



Voir plus de résultats

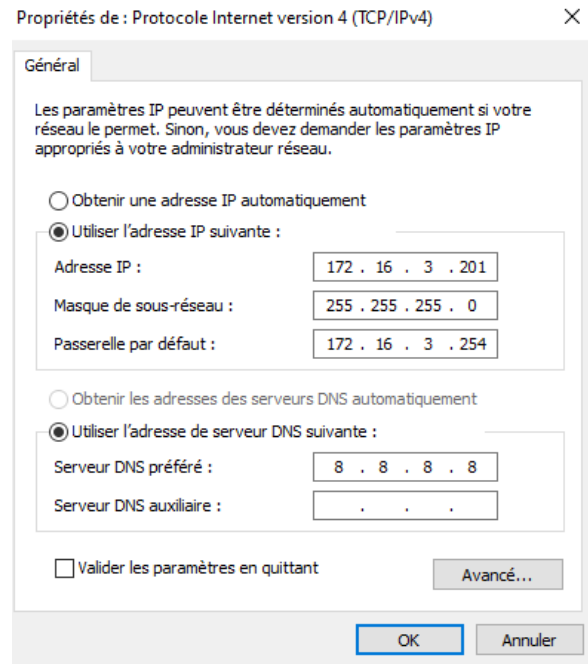
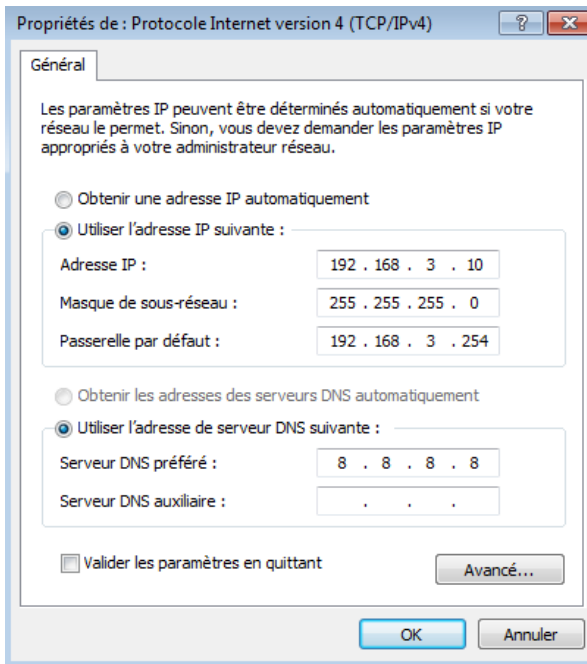
ncpa.cpl Arrêter

Puis on double clique on va dans les propriétés et on double clique encore sur protocole internet version 4,



Puis on rentre les données suivantes :

Pour le Windows 7 et Pour Windows server 2022.



## Vérification de la connexion Internet

Ensuite quand tous cela est fait on va dans la barre de recherche de windows et on tape cmd pour ouvrir l'invite de commande ,

Programmes (1)

cmd

Voir plus de résultats

cmd Arrêter

Et ensuite on entre la commande ipconfig pour voir si notre adresse ip a bien été configurer pour le windows 7 et pour le windows server2022

```
ca\ Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.WIN7A-ENT>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local 2 :
    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 192.168.3.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.3.254

Carte Tunnel isatap.{1B364568-E9BC-47F4-AA38-2C8FBA708592} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

C:\Users\Administrateur.WIN7A-ENT>_
```

```
ca\ Invite de commandes
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Espac>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :
    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::58ac:ccb3:3503:f8f0%11
    Adresse IPv4. . . . . : 172.16.3.201
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 172.16.3.254

C:\Users\Espac>_
```

Puis on ping l'adresse ip de la passerelle par default cest-a-dire le port 2 pour le windows server 2022 et le port 10 pour le windows 7 et si cela donne ce résultat

```
ca\ Administrateur : C:\Windows\system32\cmd.exe

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 192.168.3.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.3.254

Carte Tunnel isatap.{1B364568-E9BC-47F4-AA38-2C8FBA708592} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

C:\Users\Administrateur.WIN7A-ENT>ping 192.168.3.254

Envoi d'une requête 'Ping' 192.168.3.254 avec 32 octets de données :
Réponse de 192.168.3.254 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.3.254 : octets=32 temps<1ms TTL=255
Réponse de 192.168.3.254 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.3.254 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 192.168.3.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\Administrateur.WIN7A-ENT>_
```

```

C:\> Invite de commandes
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Espac>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::58ac:ccb3:3503:f8f0%11
    Adresse IPv4. . . . . : 172.16.3.201
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 172.16.3.254

C:\Users\Espac>ping 172.16.3.254

Envoi d'une requête 'Ping' 172.16.3.254 avec 32 octets de données :
Réponse de 172.16.3.254 : octets=32 temps<1ms TTL=255
Réponse de 172.16.3.254 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.3.254 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.3.254 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 172.16.3.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms

```

pour le windows 7 et pour le windows server 2022,

Alors c'est bon les deux machines peuvent communiquer entre elles, il ne nous reste plus qu'à vérifier si les machine virtuelle on acces a internet et c'est bon donc pour cela il suffit de ping le dns de google c'est-a-dire 8.8.8.8 et de ping un site internet comme par exemple google.fr.

```

C:\Users\Administrateur.WIN70-ENT>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=39 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=44 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=41 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=43 ms TTL=127

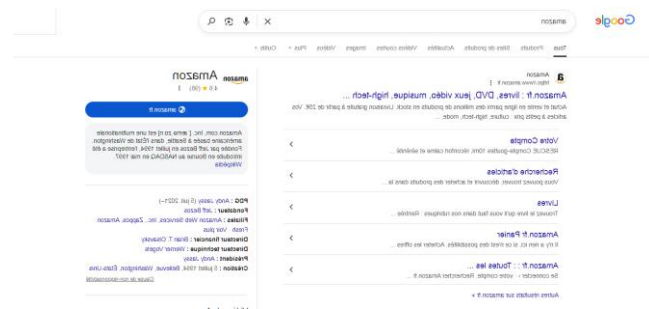
Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
    Minimum = 39ms, Maximum = 44ms, Moyenne = 41ms

C:\Users\Administrateur.WIN70-ENT>ping google.fr

Envoi d'une requête 'ping' sur google.fr [142.250.217.195] avec 32 octets de données :
Réponse de 142.250.217.195 : octets=32 temps=37 ms TTL=127
Réponse de 142.250.217.195 : octets=32 temps=45 ms TTL=127
Réponse de 142.250.217.195 : octets=32 temps=41 ms TTL=127
Réponse de 142.250.217.195 : octets=32 temps=41 ms TTL=127

Statistiques Ping pour 142.250.217.195:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
    Minimum = 37ms, Maximum = 45ms, Moyenne = 41ms

```



Si ça donne ça alors c'est bon les deux machine on accès a internet,on peut aller vérifier sur google.

## VI. CONCLUSION :

Grace à cette procédure Vous pourrez mettre en place une configuration réseaux de base du pare-feu Fortigate.