
LAB PRATIQUE : SECURISATION D'UN RESEAU AVEC FORTIGATE

AUTEUR : TRESOR OSSOHOU

Table des matières

Avant-propos	3
I- INSTALLATION DE FORTIGATE ET CONFIGURATIONS DE BASE	4
1- Connection à EVE-NG	4
2- Import d'image dans EVE-NG	5
3- Installation de fortigate	6
4- Configuration de base.....	8
II- Configurer un serveur DHCP sur un pare-feu FortiGate	10
1- Mise en place d'un Serveur DHCP.....	10
2- Création d'une route par Défaut.....	15
3- Création d'une règle de Pare-Feu	15
III- Gestion Sécurisée des comptes	17
IV- Configuration du LDAP Active Directory Sur Pare-feu FortiGate	21
1- Configuration et préparation des groupes et comptes utilisateurs.....	21
2- Créer un compte de Service Administrateur dédiée à l'authentification de l'annuaire AD sur FortiGate	21

Avant-propos

Ce document présente un laboratoire pratique de sécurité réseau réalisé dans un environnement virtualisé.

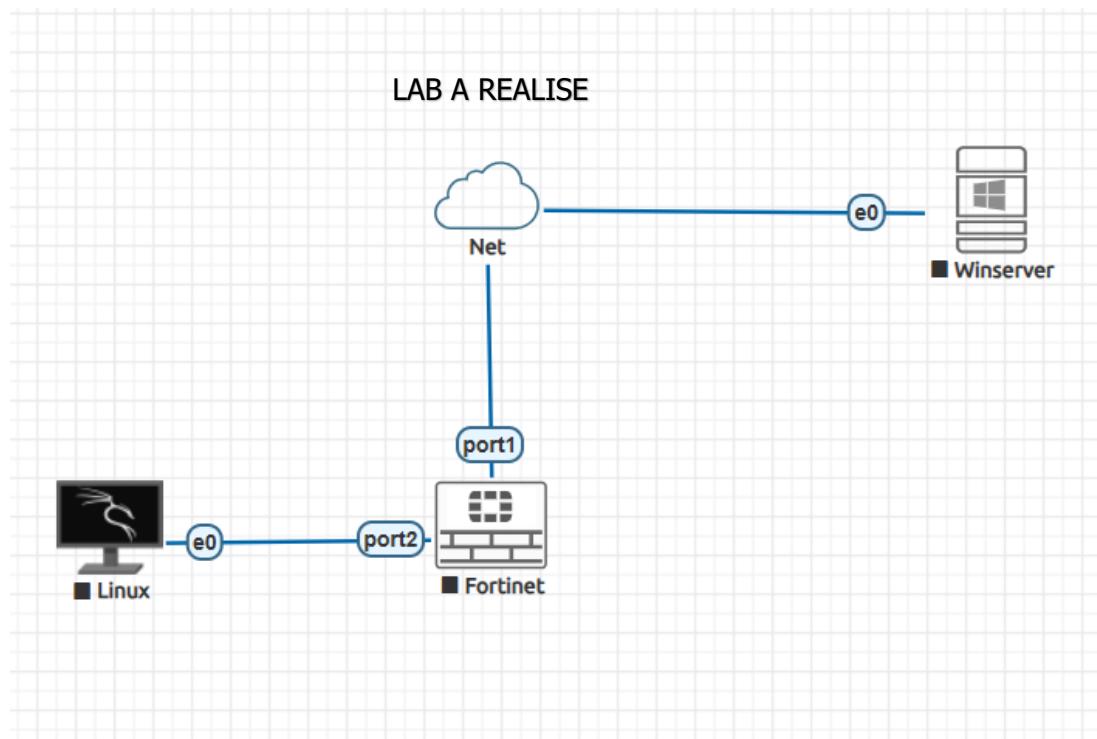
L'objectif de ce lab est de mettre en œuvre un pare-feu **FortiGate** et d'explorer ses principales fonctionnalités dans un contexte proche d'un environnement d'entreprise.

La configuration s'articule autour de plusieurs éléments clés du FortiGate, notamment la gestion des interfaces réseau, le routage, les règles de pare-feu et la mise en place d'un **serveur DHCP**. Dans ce lab, le service DHCP est configuré directement sur le **port2 du FortiGate**, permettant à tout équipement connecté à cette interface de recevoir automatiquement une adresse IP ainsi que les paramètres réseau nécessaires à la communication.

En parallèle, un **Windows Server** est déployé et configuré avec un service **LDAP**, assurant une authentification centralisée des utilisateurs. Cette intégration permet à l'ensemble des comptes présents dans l'annuaire d'accéder aux services contrôlés par le FortiGate, illustrant un mécanisme de contrôle d'accès basé sur l'identité, largement utilisé en entreprise.

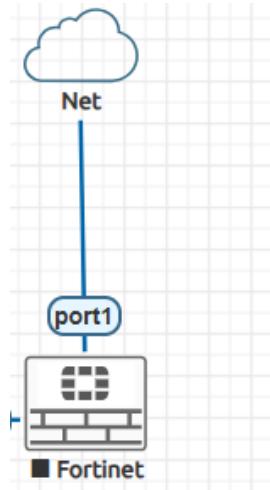
Un poste **Linux** est également intégré au réseau afin de tester la connectivité, la distribution des adresses IP via DHCP et la validité des règles de sécurité appliquées par le pare-feu.

Ce laboratoire s'inscrit dans une démarche progressive d'apprentissage des fondamentaux de la **sécurité réseau**, de la **gestion des identités**, et de l'**administration des pare-feu**, avec une orientation pratique vers les environnements SOC et les infrastructures modernes.



I- INSTALLATION DE FORTIGATE ET CONFIGURATIONS DE BASE

OBJECTIF :



1- Connection à EVE-NG

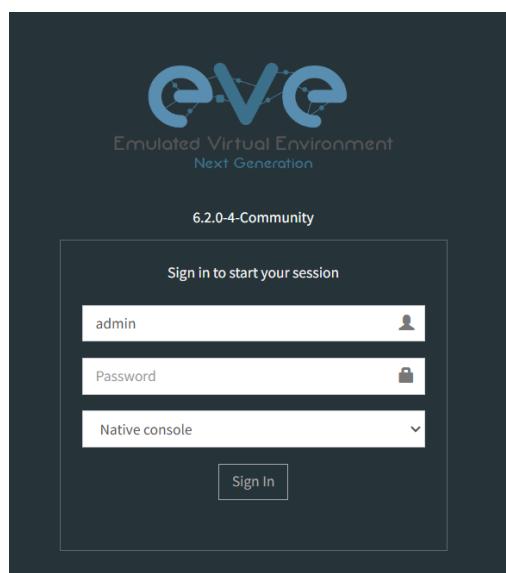
[Telechargez Eve-Ng ici](#)

Après avoir installé EVE-NG sur VMWARE, nous allons nous connecter et créer commencer notre premier LAB. Rappelons que les accès par défaut d'EVE sont :

Eve-ng login : root

Password : eve

Nous allons ensuite saisir l'adresse IP (192.168.217.143 dans mon cas) dans notre navigateur, on aura donc :



Saisir :

UserName : admin

Password : eve

2- Import d'image dans EVE-NG

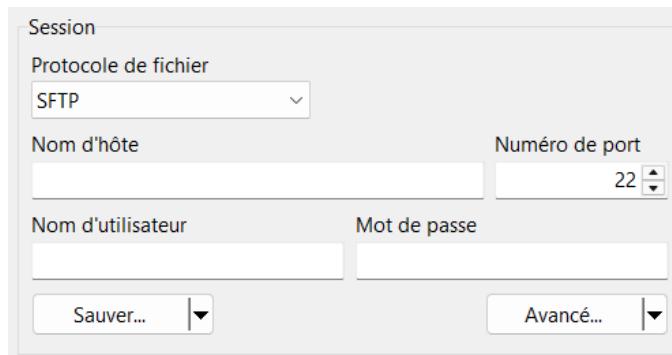
Vous avez la possibilité de télécharger les différentes images à travers ces différents liens :

[Fortigate 7.2.0](#)

[Télécharger toutes les images que vous avez besoin ici](#) ou encore [ici](#)

NB : Durant l'installation d'EVE, certains logiciels sont nécessaires tels que WinScp et UltraVNC

Après avoir fini de télécharger les images dont vous avez besoin, ouvrir WinScp



Dans la partie de Nom d'hôte, entrez votre adresse IP, puis votre nom d'utilisateur et votre mot de passe.

L'emplacement de l'image Qemu est /opt/unetlab/addons/qemu/ coller y les images Qemu téléchargées

Nom	Taille	Date de modification	Droits	Propriét...
..				
winserver-S2019-VL-x...		18/12/2025 00:04:17	rwxr-xr-x	root
win-10-x64-VL19		18/12/2025 00:01:48	rwxr-xr-x	root
viosl2-adventuresek9...		17/12/2025 23:57:14	rwxr-xr-x	root
linux-ubuntu-srv-16.04...		17/12/2025 23:57:13	rwxr-xr-x	root
linux-ubuntu-desktop...		17/12/2025 23:56:35	rwxr-xr-x	root
linux-kali-2025.4-amd...		21/12/2025 00:07:46	rwxr-xr-x	root
linux-kali-2018.1-amd...		17/12/2025 23:54:16	rwxr-xr-x	root
fortinet-FGT-v7.6.5		18/12/2025 12:01:58	rwsr-sr-x	root
fortinet-FGT-v7.20		23/12/2025 23:37:25	rwsr-sr-x	root
firepower6-NGIPS-6.3...		17/12/2025 23:51:19	rwxr-xr-x	root
csr1000v-universalk9.0...		17/12/2025 23:50:13	rwxr-xr-x	root
csr1000v-universalk9.0...		17/12/2025 23:48:56	rwxr-xr-x	root
csr1000vng-universalk...		17/12/2025 23:48:56	rwxr-xr-x	root

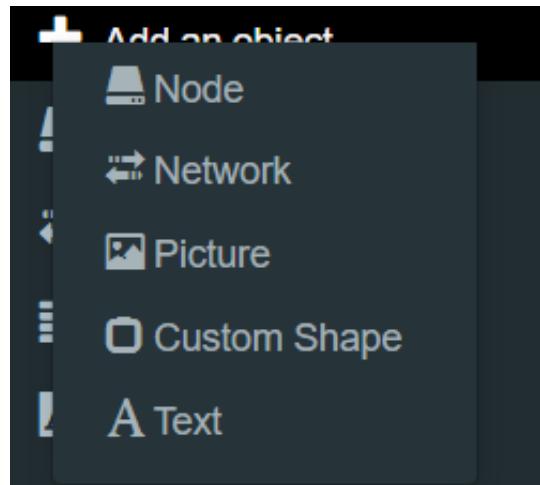
Pour la suite du document, l'idéal serait de télécharger les images qui sont présentes sur l'image ci-dessus.

Assurez-vous que le nom de votre dossier image commence comme indiqué sur [Le site de Eve-NG](#) sinon l'image ne sera pas reconnue

Rendez vous sur [Le Site de EVE-Ng pour plus d'informations](#)

3- Installation de fortigate

Nous allons prémièrement ajouter un nuage pour le réseaux

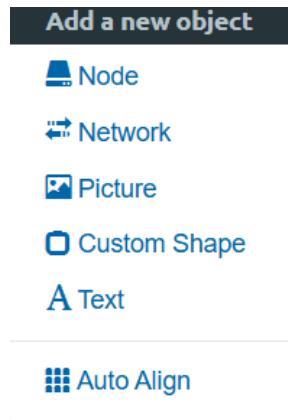


Cliquez sur Network et ensuite prendre un nuage de type Management(Cloud0)

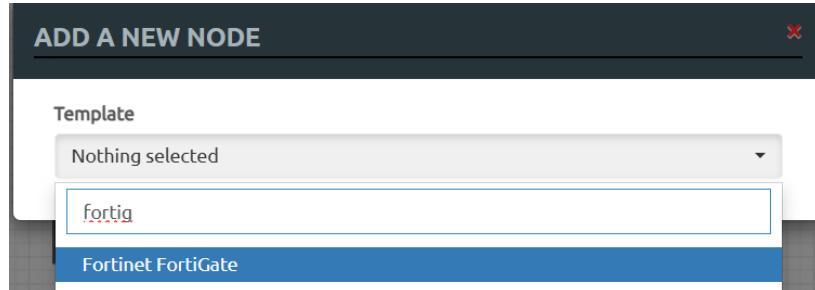
ADD A NEW NETWORK

Number of networks to add	1
Name/Prefix	Net
Type	Management(Cloud0)
Icon	01-Cloud-Default.svg
Left	0
Top	0
<button>Save</button> <button>Cancel</button>	

Nous allons maintenant ajouter notre pare-feu Fortigate



Cliquez sur Node et recherchez Fortigate



Dans notre cas nous utiliserons la version 7.2.0

4- Configuration de base

Nous allons maintenant double-cliquez sur Fortigate

Lors de la première connexion, le login est admin et le mot de passe par défaut est nul.
Ainsi, nous devrons cliquer sur la touche 'entrez' et demander la configuration d'un nouveau mot de passe.

```
System is starting...
Formatting shared data partition ... done!
Starting system maintenance...
Serial number is FGVMEVD7FPCVDB4C

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

Dans un premier temps, nous allons activer le mode DHCP pour le port 1 afin d'obtenir une adresse IP, puis procéder à l'activation de certains accès comme le ping, http, https, ssh, fgtm en utilisant ces commandes :

config system interface

edit port1

set mode dhcp

set allowaccess ping http https ssh fgtm

next

end

Explication rapide

- **set mode dhcp** → FortiGate reçoit son IP automatiquement (depuis ta box / ISP)
- **set allowaccess** → autorise l'accès admin C les tests

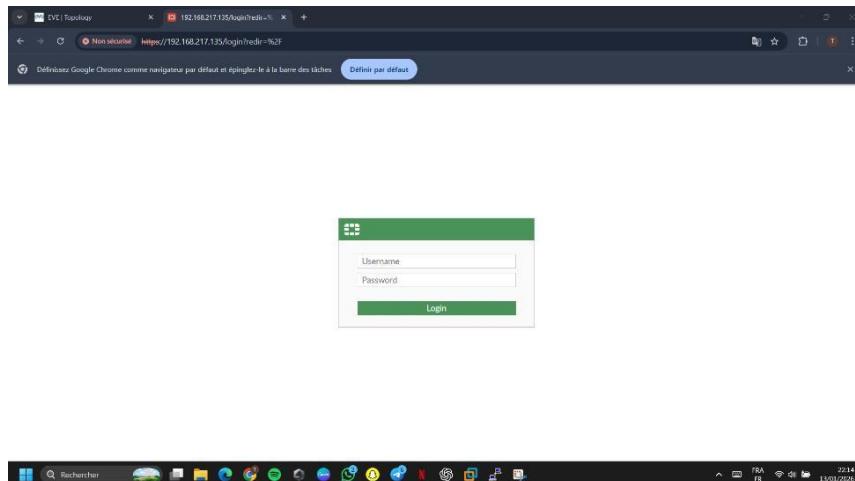
Nous allons maintenant vérifier si Fortigate a reçu une adresse IP et si les permissions ont été activées :

```
FGVMEVCYND5QEK63 # get system interface
== [ port1 ]
name: port1 mode: dhcp ip: 192.168.217.135 255.255.255.0 status: up ne
tbios-forward: disable type: physical ring-rx: 0 ring-tx: 0 netflow-sam
pler: disable sflow-sampler: disable src-check: enable explicit-web-pro
xy: disable explicit-ftp-proxy: disable proxy-captive-portal: disable m
tu-override: disable wccp: disable drop-overlapped-fragment: disable dr
op-fragment: disable
== [ port2 ]
```

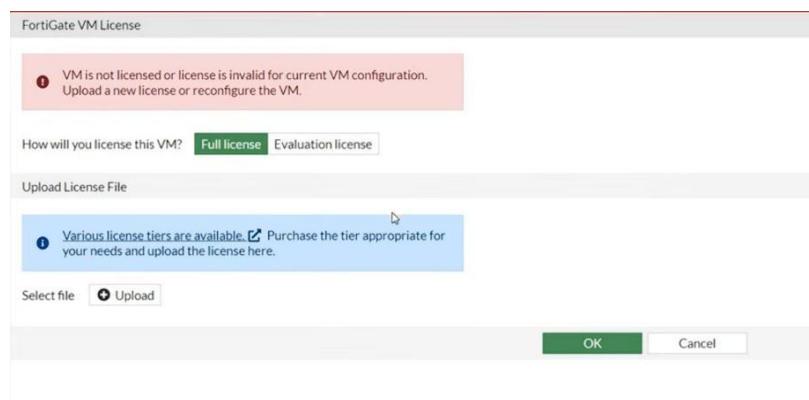
```
FGVMEVCYND5QEK63 # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh snmp http telnet fgfm ftm
        set type physical
        set snmp-index 1
    next
```

Il est évident que tout a été activé.

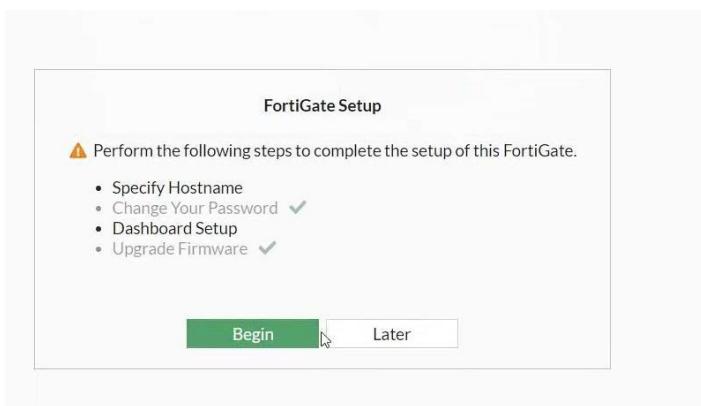
Nous allons ouvrir un nouvel onglet et entrer l'adresse IP de Fortigate (192.168.217.135 dans mon cas) :

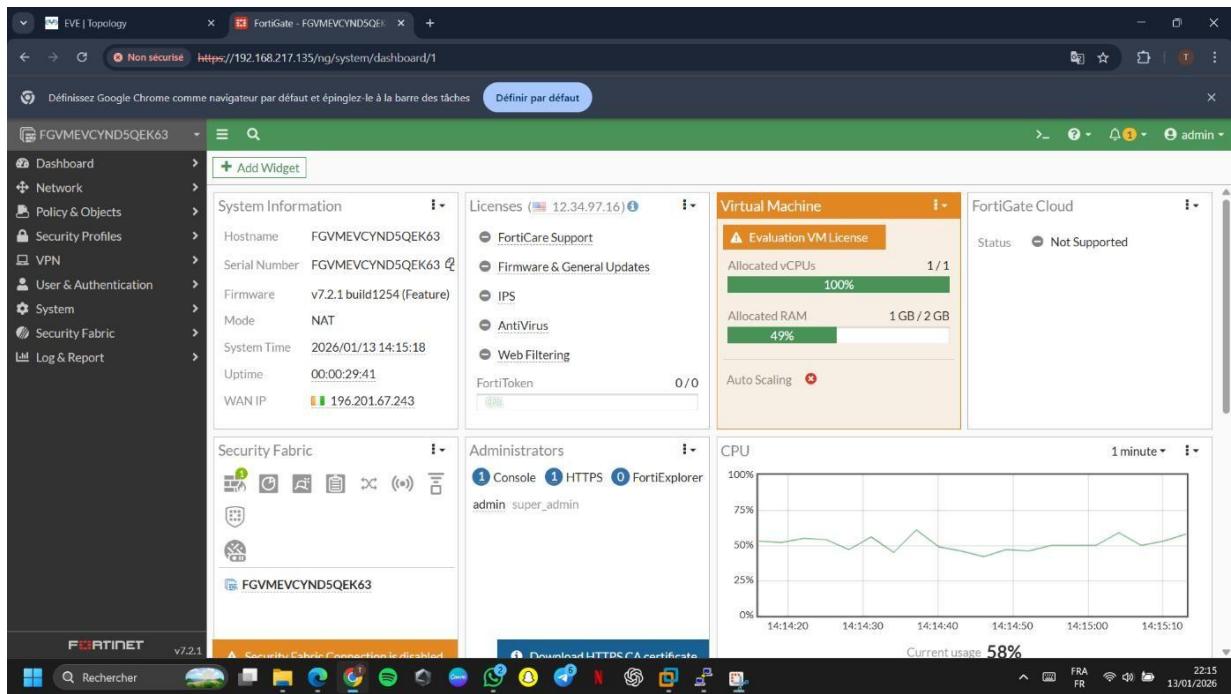


Entrez les identifiants de votre Pare-Feu



Selectionnez **Evaluation License** puis connectez-vous à un compte qui doit être préalablement créé sur [le site de Fortigate](#)





II- Configurer un serveur DHCP sur un pare-feu FortiGate

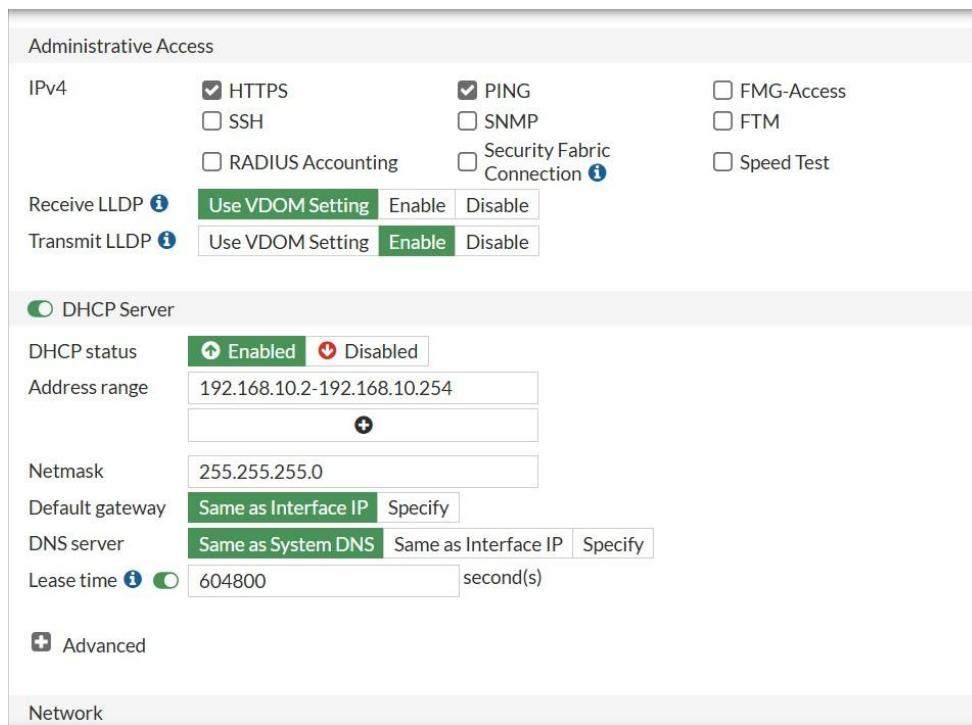
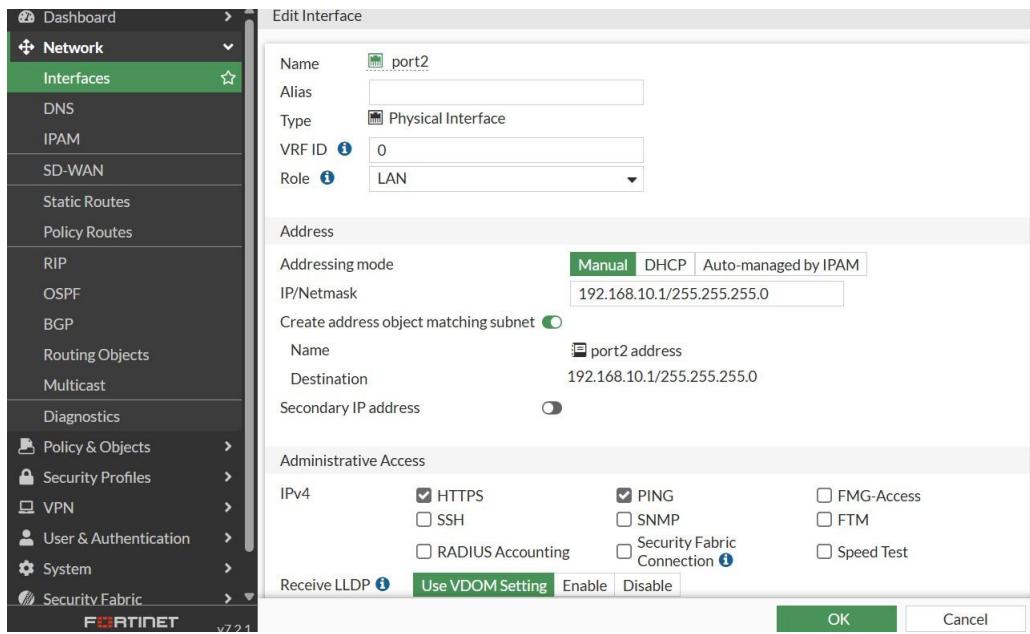
1- Mise en place d'un Serveur DHCP

Après avoir accédé à notre Fortigate, nous allons procéder à la configuration du serveur DHCP pour le port 2 afin d'attribuer une adresse IP à tout appareil connecté sur ce port.

Dans le menu déroulant nous allons cliquer sur Network > Interfaces

Name	Type	Members	IP/Netmask
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch
port1	Physical Interface		192.168.217.135/255.255.255.0
port2	Physical Interface		192.168.10.1/255.255.255.0
port3	Physical Interface		0.0.0.0/0.0.0.0

Ensuite, cliquez deux fois sur le port 2 pour y accéder.
 Faire ensuite les réglages comme les images ci-dessous :



NB : Il ne faut JAMAIS utiliser le même réseau que le WAN (dans notre cas le port 1/Internet), sinon le FortiGate ne saura pas : « Est-ce que cette machine est sur Internet ou dans mon réseau local ? »

Je rappelle aussi que :

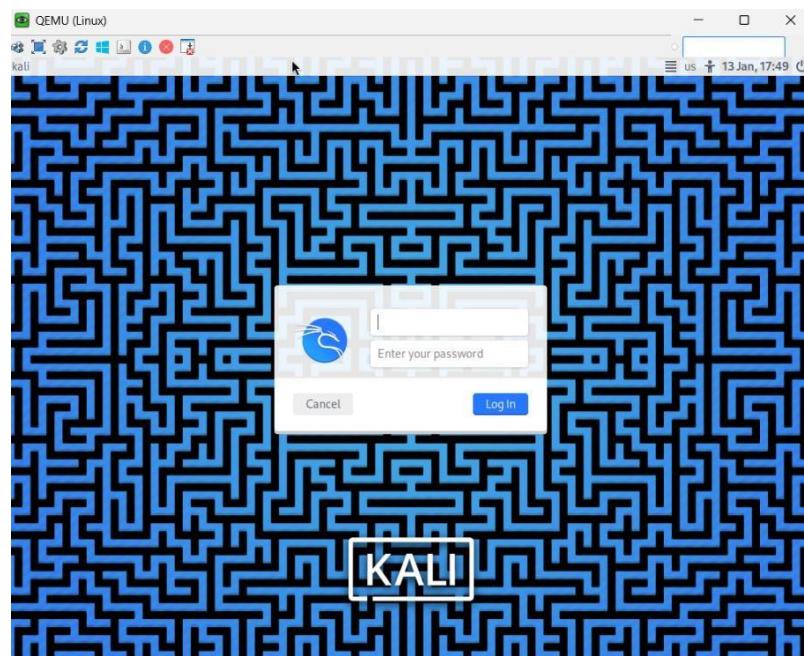
Je n'ai pas choisi 192.168.10.1 parce que c'est joli

Je l'ai choisi parce que :

- Il est dans un réseau privé
- Il est différent du WAN
- Il est logique pour une passerelle LAN
- Il permet au NAT et au routage de fonctionner

Vérification :

Avant de tester le DHCP du port2 du FortiGate, je vais d'abord connecter mon PC Kali directement à Internet afin d'effectuer toutes les mises à jour nécessaires.



Pour la version de kali 2025.4 les identifiants par défauts sont :

User : kali

Password : kali

- **sudo apt update** sert à mettre à jour la liste des logiciels disponibles sur ton système Linux (Debian, Ubuntu, Kali, etc.).

```
$ sudo su
[sudo] password for kali:
[root@kali]~[/home/kali]
# sudo apt update
get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.5
B]
6% [3 Contents-amd64 8,418 kB/52.5 MB 16%]
```

- **sudo apt install isc-dhcp-client** sert à installer le client DHCP ISC sur ton système Linux.

```
[root@kali]~[/home/kali]
# sudo apt install isc-dhcp-client
Installing:
  isc-dhcp-client

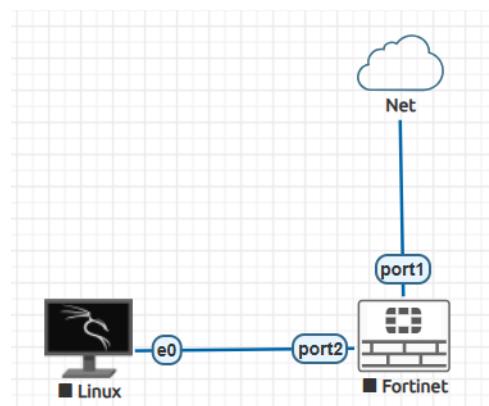
Installing dependencies:
  isc-dhcp-common

Suggested packages:
  resolvconf  avahi-autoipd  isc-dhcp-client-ddns

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 939
  Download size: 1,217 kB
  Space needed: 3,079 kB / 63.1 GB available

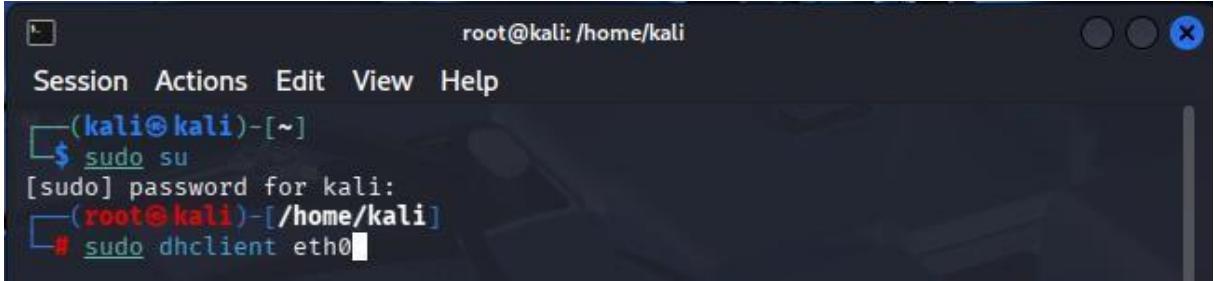
Continue? [Y/n] ■
```

Une fois les mises à jour terminées, je connecterai le PC Kali au **port2** du **FortiGate**, qui est configuré comme interface LAN avec un **serveur DHCP activé**.



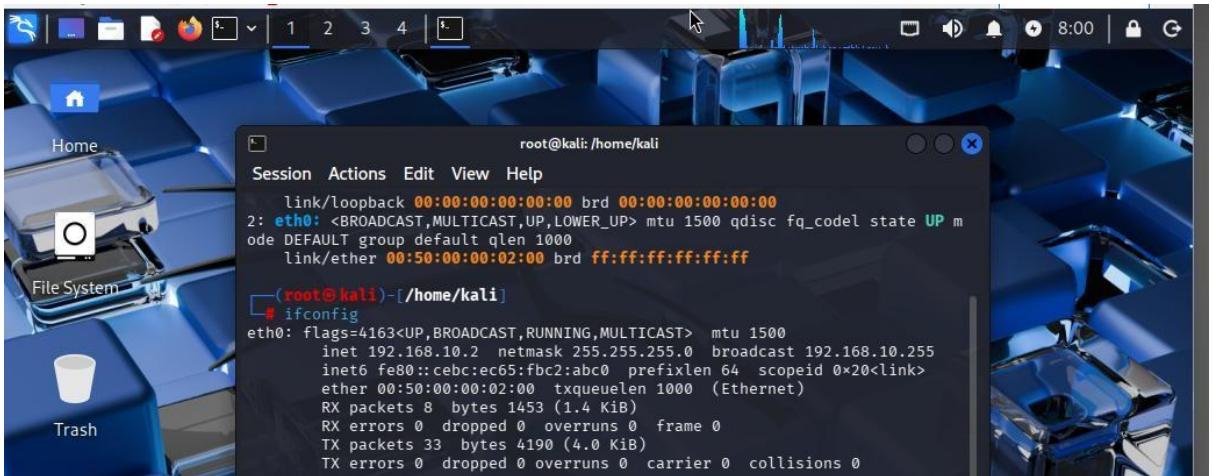
Ensuite, je mettrai la carte réseau de Kali en **mode DHCP (automatique)** afin qu'il obtienne automatiquement :

- Une adresse IP,
- Un masque,
- Une passerelle,
- Et un serveur DNS fournis par le FortiGate.



```
root@kali: /home/kali
Session Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo su
[sudo] password for kali:
[(root㉿kali)-[/home/kali]]# sudo dhclient eth0
```

- **sudo dhclient eth0**, c'est le client DHCP de Linux. Son rôle est de demander automatiquement une adresse IP à un serveur DHCP sur le réseau.



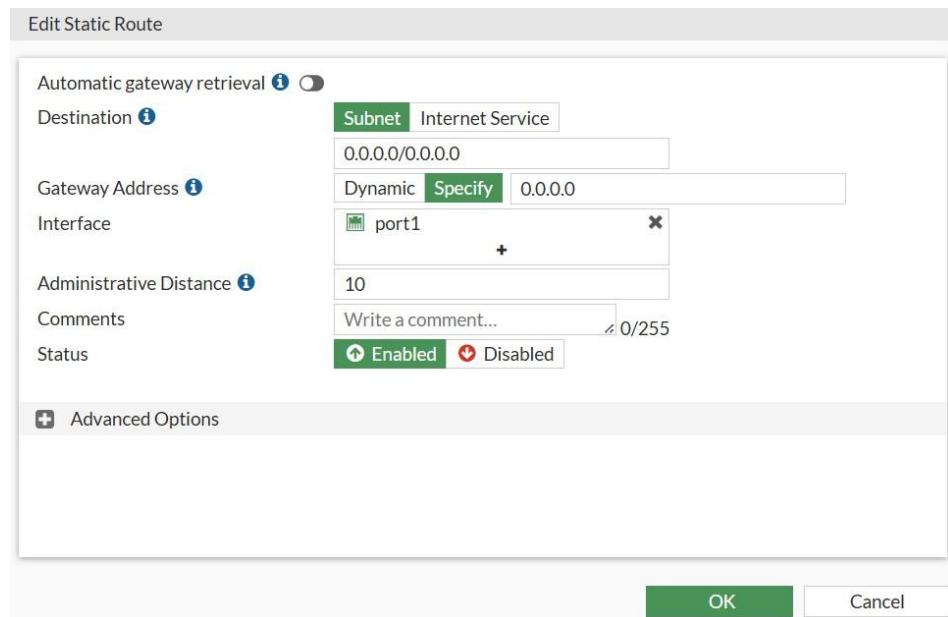
```
root@kali: /home/kali
Session Actions Edit View Help
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:00:00:02:00 brd ff:ff:ff:ff:ff:ff
[(root㉿kali)-[/home/kali]]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.2 netmask 255.255.255.0 broadcast 192.168.10.255
        ether 00:50:00:00:02:00 txqueuelen 1000 (Ethernet)
        RX packets 8 bytes 1453 (1.4 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 33 bytes 4190 (4.0 Kib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Le FortiGate (port2) a bien distribué une adresse IP disponible dans son **pool DHCP** (ici 192.168.10.2).
- Le protocole DHCP a réussi : Kali a demandé une IP → FortiGate a attribué 192.168.10.2 → Kali a accepté.

2- Création d'une route par Défaut

Maintenant que le DHCP du port2 est opérationnel et que mon PC Kali est intégré au réseau LAN du FortiGate, nous allons configurer une route statique sur le FortiGate vers le WAN afin de permettre l'accès à Internet.

Dans le menu déroulant nous allons cliquer sur Network > Static Routes > Create New



Faire les Réglages comme ci-dessus puis ok.

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	0.0.0.0	port1	Enabled	admin

3- Création d'une règle de Pare-Feu

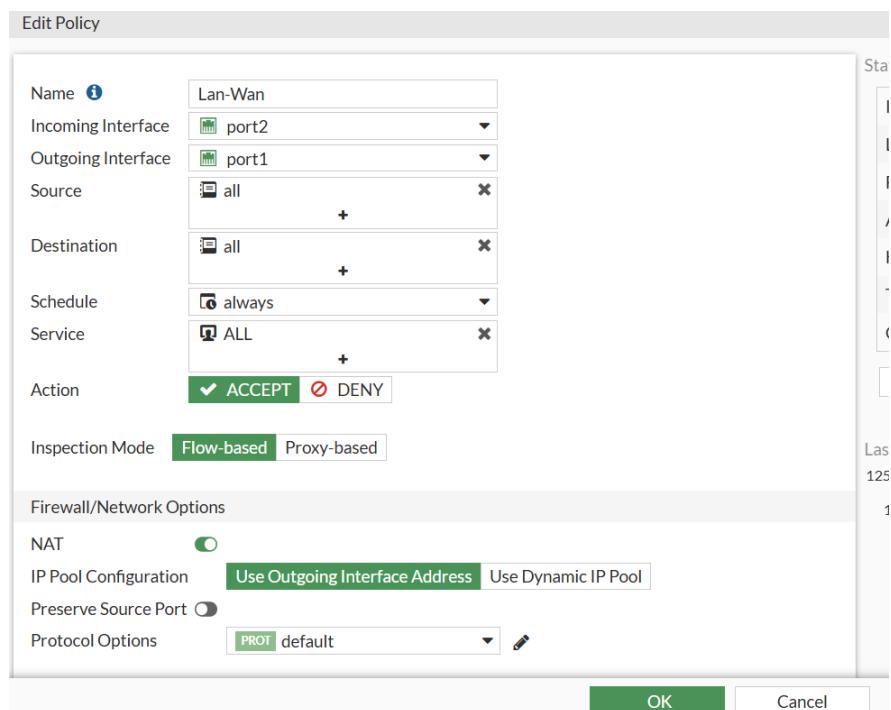
Ensuite, je vais créer une règle de pare-feu (policy) entre le LAN (port2) et le WAN (port1) avec NAT activé, pour que mon PC puisse sortir sur Internet tout en restant protégé par le FortiGate.

Dans le menu déroulant nous allons cliquer sur Policy Objects > Firewall Policy > Create New.

Dans FortiGate, pour créer une **règle de pare-feu via Policy Objects > Firewall Policy > Create New**, il faut configurer plusieurs paramètres principaux qui contrôlent le trafic :

- **Source** : définit qui initie la connexion, c'est-à-dire l'interface et les adresses IP ou réseaux autorisés à envoyer du trafic.
- **Destination** : définit où le trafic peut aller, en précisant l'interface et les adresses IP ou réseaux ciblés.
- **Schedule** : permet de définir quand la règle est active, par exemple toujours, selon un calendrier récurrent ou à un moment précis.
- **Service** : définit le type de trafic autorisé, c'est-à-dire les protocoles et ports (HTTP, HTTPS, ou un service personnalisé).

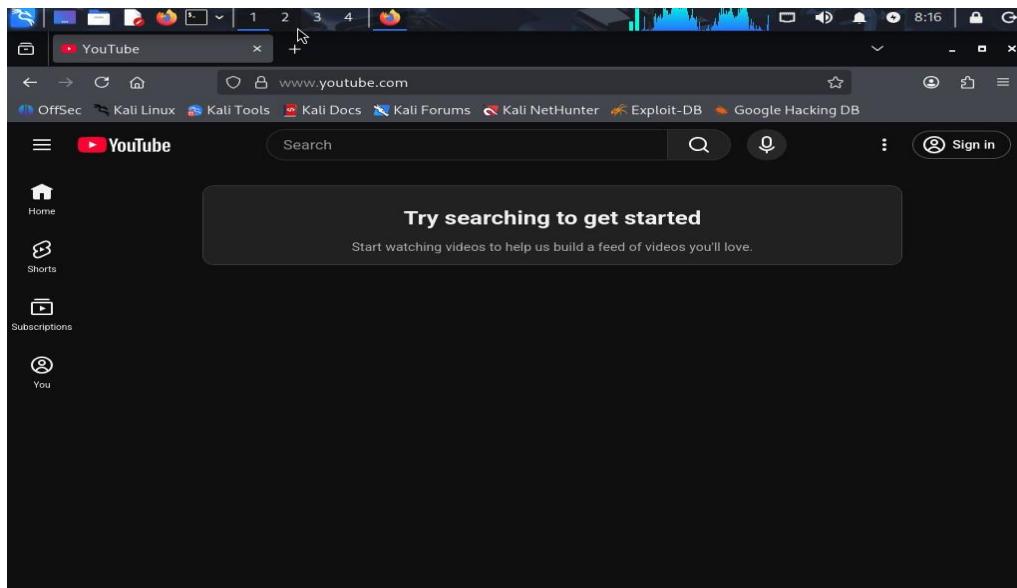
Dans notre cas, pour débuter et tester le trafic facilement, on utilise par défaut All pour la source, la destination, le service et Always pour le schedule, afin que rien ne soit bloqué avant d'affiner la règle comme l'image ci-dessous.



Interface Pair View											
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes		
port2 → port1	Lan-Wan	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	8.66 kB	
Implicit											

Vérification :

Pour tester, nous allons essayer d'accéder à Youtube.com



III- Gestion Sécurisée des comptes

Dans le menu déroulant **System > Settings**, nous pouvons voir les réglages de base de Fortigate. Nous avons également la possibilité de mettre des politiques de mot de passe pour les comptes admin.

A screenshot of the FortiGate configuration interface showing the "Password Policy" section. It includes fields for "Password scope" (set to "Admin"), "Minimum length" (set to 8), "Minimum number of new characters" (set to 0), and toggle switches for "Character requirements", "Allow password reuse", and "Password expiration".

Setting	Value
Password scope	Admin
Minimum length	8
Minimum number of new characters	0
Character requirements	Off
Allow password reuse	On
Password expiration	Off

La **Password Policy** dans FortiGate définit les règles de sécurité pour les mots de passe des utilisateurs afin de protéger l'accès au système.

- **Password Scope** : détermine à quels utilisateurs ou groupes la politique s'applique (ex. admins vs utilisateurs standards).
- **Minimum length (8)** : le mot de passe doit contenir au moins 8 caractères.
- **Minimum number of new characters (0)** : aucun nombre minimum de caractères différents n'est exigé lors du changement de mot de passe.

- **Character requirements** : permet d'exiger des majuscules, minuscules, chiffres ou caractères spéciaux pour renforcer la complexité du mot de passe.
- **Allow password reuse** : contrôle si un utilisateur peut réutiliser un ancien mot de passe ; si désactivé, l'utilisateur doit choisir un mot de passe totalement nouveau.
- **Password expiration** : définit la durée maximale avant que le mot de passe doive être changé pour limiter le risque de compromission.

Pour créer un compte administrateur dans le menu déroulant **System > Administrators**

The screenshot shows the FortiGate management interface. The left sidebar is collapsed. The main area displays a table titled 'Administrators' with one row visible: 'System Administrator' (Profile: super_admin, Type: Local, Status: Disabled). A 'Create New' button is highlighted in green at the top left of the table area.

Par défaut, nous avons un compte admin qui a pour profil super_admin. Il est généralement recommandé de ne pas l'utiliser et de créer un autre compte.

Cliquons sur Create New pour créer un compte Admin

Voici les différents champs à remplir lors de la création d'un nouvel administrateur sur FortiGate et leur rôle dans la gestion des accès et des permissions.

The dialog box is titled 'New Administrator'. It contains the following fields:

- Username:** FortiAdmin
- Type:** Local User (selected)
- Password:** [REDACTED]
- Confirm Password:** [REDACTED]
- Comments:** Write a comment... (0/255)
- Administrator profile:** [REDACTED]
- Optional checkboxes:**
 - Two-factor Authentication
 - Restrict login to trusted hosts
 - Restrict admin to guest account provisioning only

At the bottom right are 'OK' and 'Cancel' buttons.

Username : le nom d'utilisateur de l'administrateur.

- Exemple : FortiAdmin.
- C'est le nom que l'administrateur utilisera pour se connecter à l'interface FortiGate.

Type : le type de compte administrateur.

- Options possibles : **Local Admin**, **Read-Only**, **Super Admin**, ou comptes liés à **LDAP/RADIUS**.
- Détermine les **droits et le niveau d'accès** de cet administrateur sur le FortiGate.

Password : mot de passe pour le compte administrateur.

- Il doit respecter la **Password Policy** définie sur le FortiGate (longueur minimale, complexité, etc.).

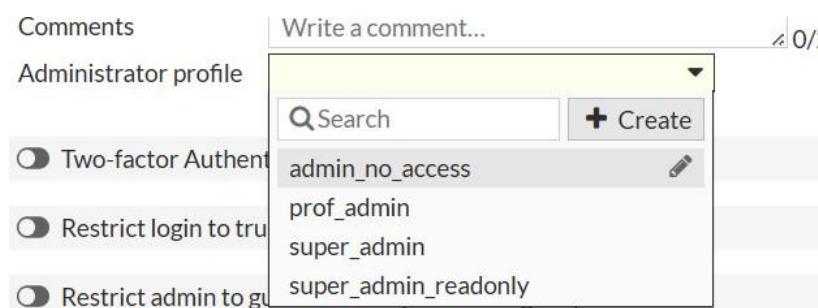
Comments : champ optionnel pour ajouter des notes sur l'administrateur.

- Par exemple : "Administrateur principal du firewall" ou "Compte temporaire pour test".
- Limité à 255 caractères.

Administrator profile : ce champ permet de sélectionner le profil d'accès ou rôle de l'administrateur. Il définit les permissions de l'administrateur, c'est-à-dire ce qu'il peut voir et faire sur le FortiGate.

- Super Admin → accès complet à toutes les fonctions et configurations du firewall.
- Read-Only → accès limité à la lecture seule, sans possibilité de modifier la configuration.
- Profils personnalisés → permettent de créer un profil sur mesure, en attribuant uniquement les droits nécessaires selon les besoins spécifiques de l'administrateur.

En résumé, ce champ gère les permissions et offre la possibilité de créer de nouveaux profils via "**Create New**", afin d'adapter les droits aux responsabilités et sécuriser l'accès de chaque compte administrateur.



New Admin Profile

Name	<input type="text" value="Lecteur"/>
Comments	<input type="text" value=""/>

Access Permissions

Access Control	Permissions	Set All ▾
Security Fabric	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
FortiView	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
Firewall	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	

Nous allons pour le test créer un profil lecteur que nous allons attribuer à notre compte FortiAdmin.

New Administrator

Username	<input type="text" value="FortiAdmin"/>
Type	<input checked="" type="radio"/> Local User Match a user on a remote server group Match all users in a remote server group Use public key infrastructure (PKI) group
Password	<input type="password" value="*****"/> <input type="button" value=""/>
Confirm Password	<input type="password" value="*****"/> <input type="button" value=""/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Administrator profile	<input type="text" value="Lecteur"/>
<input type="checkbox"/> Two-factor Authentication <input type="checkbox"/> Restrict login to trusted hosts <input type="checkbox"/> Restrict admin to guest account provisioning only	

IV- Configuration du LDAP Active Directory Sur Pare-feu FortiGate

LAB Environment

LDAP Server:

- OS : Windows Server 2019 Standard
- Rôle : AD DC
- P : 192.168.217.3
- Domain Name : LAB.LOCAL
- Security Group : Forti-Admins
- Users : john.doe C michel.brown

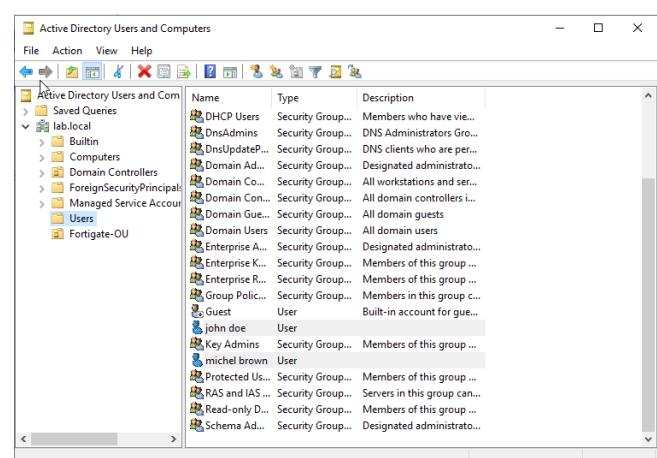
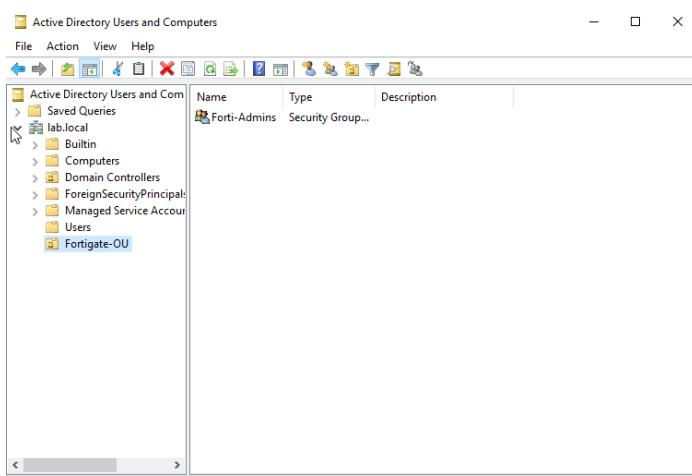
FortiGate Firewall:

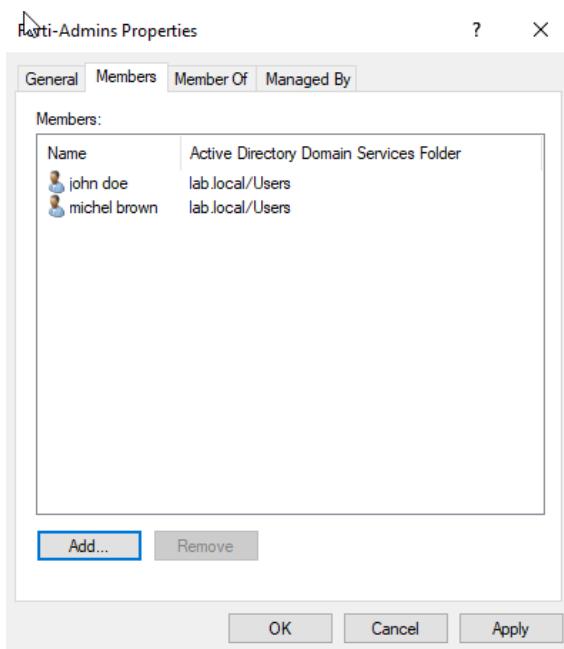
- OS : FortiGate-VM64-KVM
- Firmware : v7.2.0
- IP : 192.168.217.135

1- Configuration et préparation des groupes et comptes utilisateurs

Pour les différentes étapes de ce point, vous pouvez visiter mon profil GitHub où j'ai fait une LAB sur AD via [Mise en place d'un environnement de gestion des utilisateurs et des ressources sous Windows Server 2016](#).

2- Créer un compte de Service Administrateur dédiée à l'authentification de l'annuaire AD sur FortiGate





3- Configuration de l'authentification administrative via Active Directory (LDAP) sur FortiGate

- **Ajout du Serveur LDAP :** Dans le menu déroulant Utilisateur C Authentification → Serveurs LDAP → Nouveau (ID= SAMAccountName)

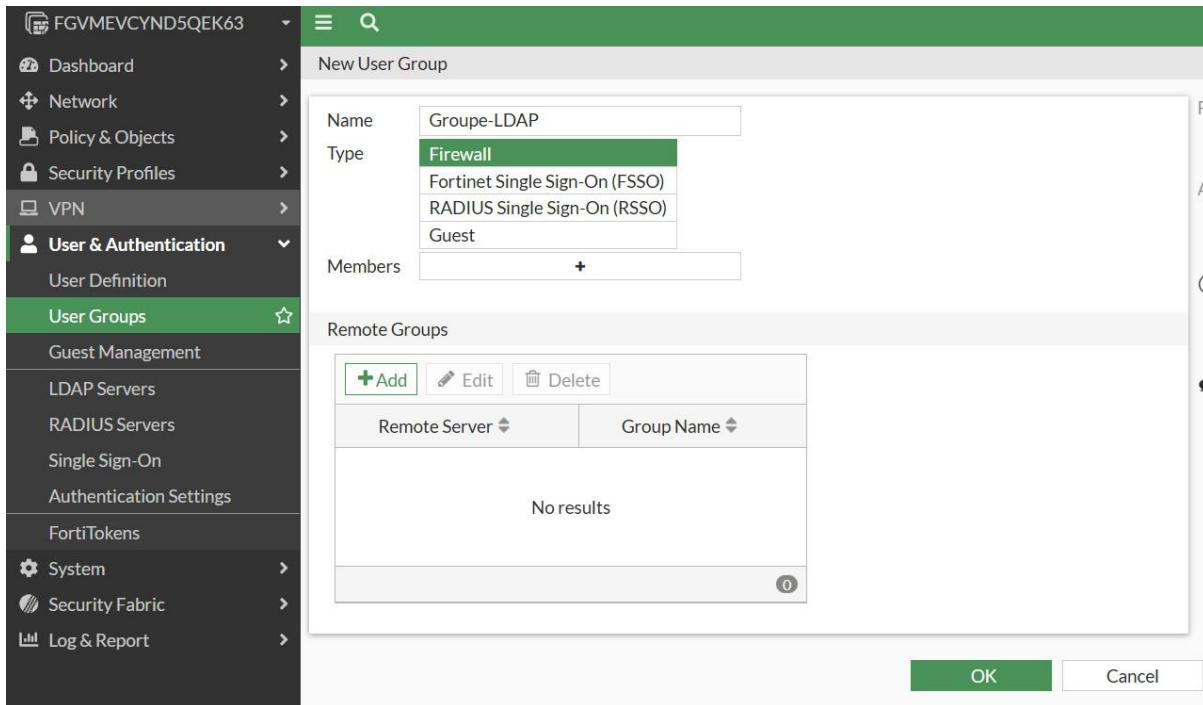
SAMAccountName (Security Account Manager Account Name) est le **nom de connexion historique** d'un utilisateur ou d'un ordinateur dans un domaine Windows.

Dans le Champ Server IP/Name, on y insère l'adresse IP de notre Serveur AD, dans Bind Type/Regular nous allons associer un compte administrateur. Par défaut, nous allons prendre le compte standard (mais il est généralement recommandé d'en créer un autre).

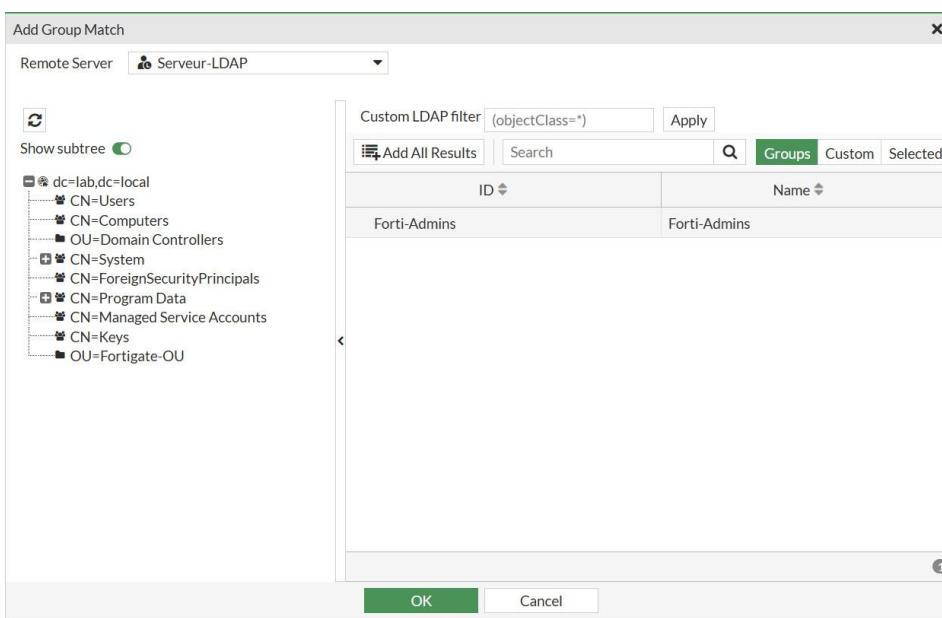
On va cliquer ensuite sur Test Connectivity pour tester la connexion, puis faire des recherches pour Distinguished Name et enfin sélectionner la racine, puis ok

NB : Il est essentiel de se connecter à un compte avant de faire une recherche dans Distinguished Name

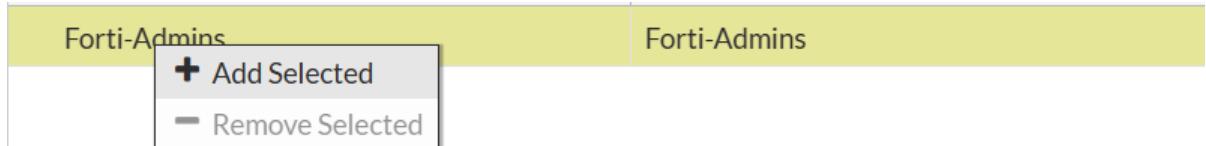
- Ajout Groupe d'utilisateurs : Dans le menu déroulant Utilisateur C
Authentification → Groupe d'utilisateurs → Nouveau



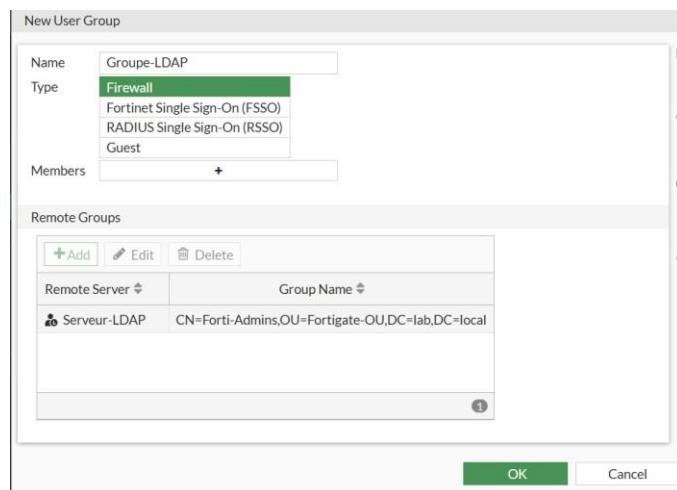
Concernant l'ajout des membres nous allons choisir Remote Groups (**Groupes à distance**) puis cliquer sur ADD



Pour Remote Server (Serveur Distant), nous allons rechercher le serveur que nous venons de créer (Serveur-LDAP), dérouler la racine puis cliquer 2 fois sur l'OU que nous avons créé préalablement (Fortigate) ensuite faire un clic droit sur Forti-Admins



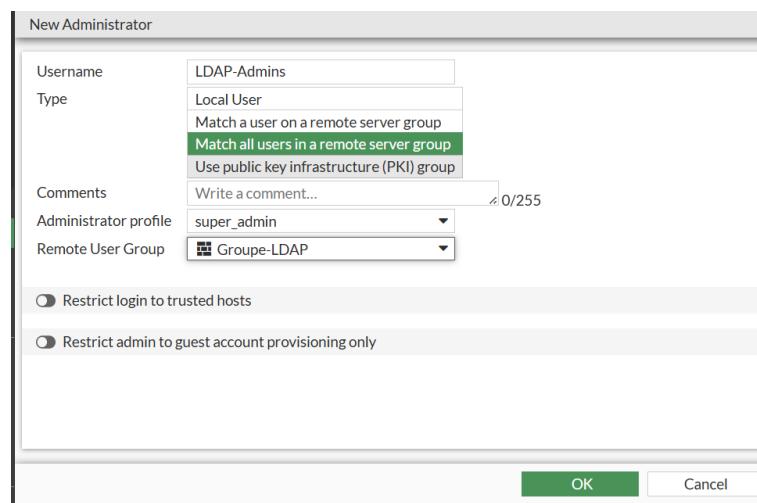
Puis sélectionner Add Selected



Puis ok

User Groups			
Group Name	Group Type	Members	Ref.
Groupe-LDAP	Firewall	Serveur-LDAP	0
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

- **Ajout Compte Administrateurs : Système → Administrateurs → Nouvel Admin**
(Associez tous les utilisateurs d'un groupe de serveurs distants)

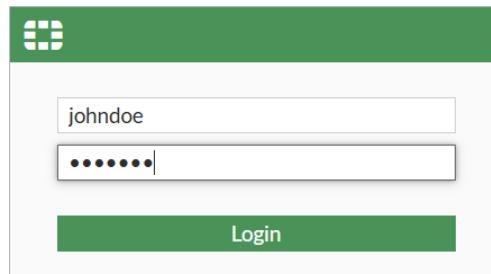


Puis OK

System Administrator (3)				
User	Role	Type	Access	Status
FortiAdmin	Lecteur	Local	Disabled	✗
LDAP-Admins	super_admin	Remote+Wildcard	Disabled	✗
admin	super_admin	Local	Disabled	✗

Vérification :

Essayons de nous connecter avec le compte de M.John Doe créé ci-dessus



The image shows a login interface with a green header and footer. The main area has two input fields: one for 'username' containing 'johndoe' and another for 'password' containing a series of dots. A large green 'Login' button is at the bottom.

