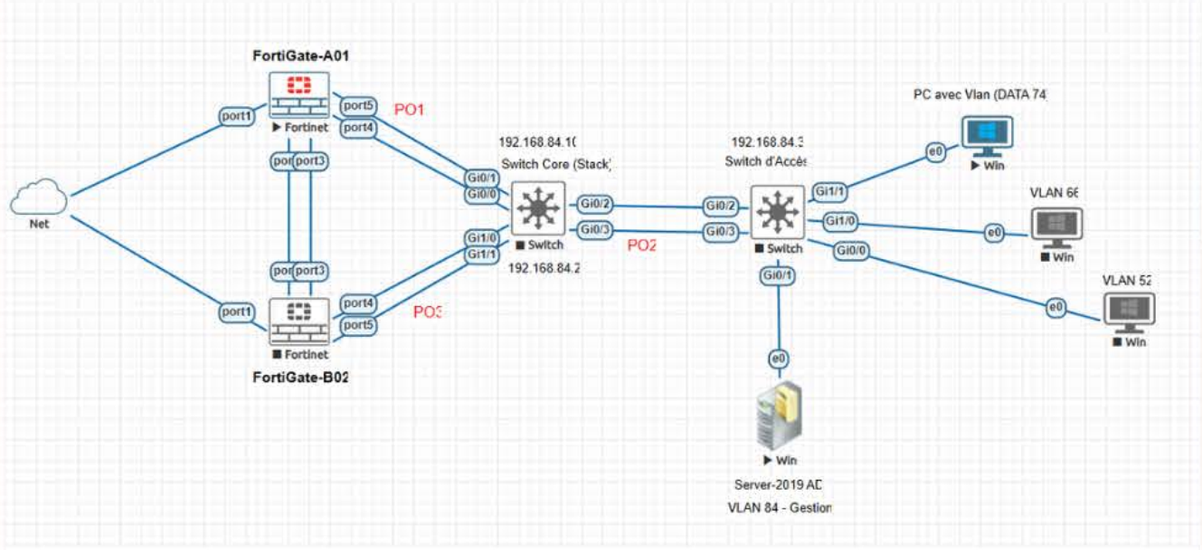
RESEAU EN CLAIR

LAB réseau FORTINET



Prepared By

Réseau En Clair

www.reseauenclair.com

📘 RÉSEAU EN CLAIR : DE L'IDÉE AU LAB ENTREPRISE

Construire, sécuriser et documenter une infrastructure réseau moderne, claire et fiable.

Une initiative des Administrateurs Réseau du Québec

Parce que le savoir ne se garde pas, il se partage.

🧭 Introduction

Bienvenue dans *Réseau en clair*, un guide pensé **par des administrateurs réseau, pour des administrateurs réseau**.

Ce document n'est pas un simple recueil de commandes ou un tutoriel de plus. C'est une **expérience d'apprentissage complète**, ancrée dans la réalité du terrain, conçue pour t'aider à **bâtir, comprendre et sécuriser une architecture d'entreprise** — de la conception du schéma jusqu'à la supervision en production.

Chaque chapitre a été rédigé avec une idée en tête :

te rendre autonome, rigoureux et fier de ton réseau.

Tu y trouveras :

- 🔧 des configurations réelles, expliquées pas à pas,
- 💡 des astuces d'ingénierie éprouvées,
- 🧱 une architecture complète inspirée d'environnements professionnels,
- 🔒 et surtout, une vision claire de la **sécurité et de la documentation** dans un contexte d'entreprise.

🌐 Une initiative québécoise, collaborative et humaine

Réseau en clair est né d'un constat simple :
trop de techniciens apprennent seuls, dans le silence des salles serveurs.
Nous avons voulu créer un espace d'entraide et de clarté, où les professionnels des réseaux du Québec peuvent **partager leurs connaissances, leurs laboratoires, leurs réussites et même leurs erreurs** — avec transparence et bienveillance.
Ce guide est donc **le fruit d'une communauté** : celle des **admins réseau qui n'ont jamais cessé d'apprendre**, de tester, de documenter et de transmettre.

💬 Sur **LinkedIn**, sous la bannière *Réseau en clair*, des administrateurs, formateurs et étudiants échangent chaque semaine leurs labs, leurs configurations et leurs découvertes.
Parce qu'au-delà des VLANs, des câbles et des pare-feux, il y a **une culture du partage** et un **désir collectif de professionnaliser le métier**.

🧠 Pourquoi ce guide ?

Ce guide a un triple objectif :

1. **Former et inspirer** les administrateurs réseau à bâtir des environnements d'entreprise complets, documentés et sécurisés.
2. **Offrir un modèle de documentation claire et uniforme**, applicable à tout projet technique.

3. **Créer un pont entre la pratique et la pédagogie**, pour que chaque configuration devienne un savoir transmissible.

⚙️ À qui s'adresse-t-il ?

Ce guide est pour toi si :

- Tu veux renforcer ta compréhension des VLANs, du routage, du FortiGate et de l'Active Directory.
- Tu souhaites améliorer ta façon de **documenter et présenter** ton travail.
- Tu crois que la technique doit être **aussi claire que fonctionnelle**.
- Tu es un(e) professionnel(le) du réseau, un étudiant en infrastructure TI, ou un formateur passionné.

💡 Ce que tu apprendras

En suivant pas à pas les étapes du guide, tu apprendras à :

✅ Concevoir un **plan d'adressage VLAN clair et logique**

✅ Configurer et **sécuriser un pare-feu FortiGate** selon les bonnes pratiques

✅ Mettre en place un **câblage redondant et une agrégation stable (LACP)**

✅ Déployer un **Active Directory complet** avec DNS et DHCP centralisé

✅ Superviser, documenter et valider la **cohérence d'un réseau professionnel**

🔒 Un mot sur la philosophie du guide

Ici, **pas de copier-coller sans compréhension.** Chaque ligne de commande, chaque concept est

expliqué pour que tu saches **pourquoi tu le fais** — pas seulement comment.
Tu apprendras à lire un réseau comme une carte vivante :
à voir les flux, anticiper les failles, et surtout, à **documenter avec clarté** ce que tu construis.
"Un bon réseau ne se mesure pas qu'à sa disponibilité, mais à la qualité de sa documentation."

🌟 Un avant-goût du parcours

📍 **Étape 1 :** Plan d'adressage et VLAN
📍 **Étape 2 :** Sécurisation du FortiGate
📍 **Étape 3 :** Câblage physique et agrégation
📍 **Étape 4 :** Routage, ACL, DHCP Relay et Active Directory
📍 **Étape 5 :** Tests, supervision et bonnes pratiques de documentation

💬 Un mot de la communauté

"Ce guide, c'est plus qu'un lab : c'est un pont entre les générations d'administrateurs réseau."
— Équipe Réseau en clair, Québec, 2025
Alors prends ton carnet, prépare ton environnement, et embarque avec nous dans cette aventure technique et humaine.

📄 Mentions légales

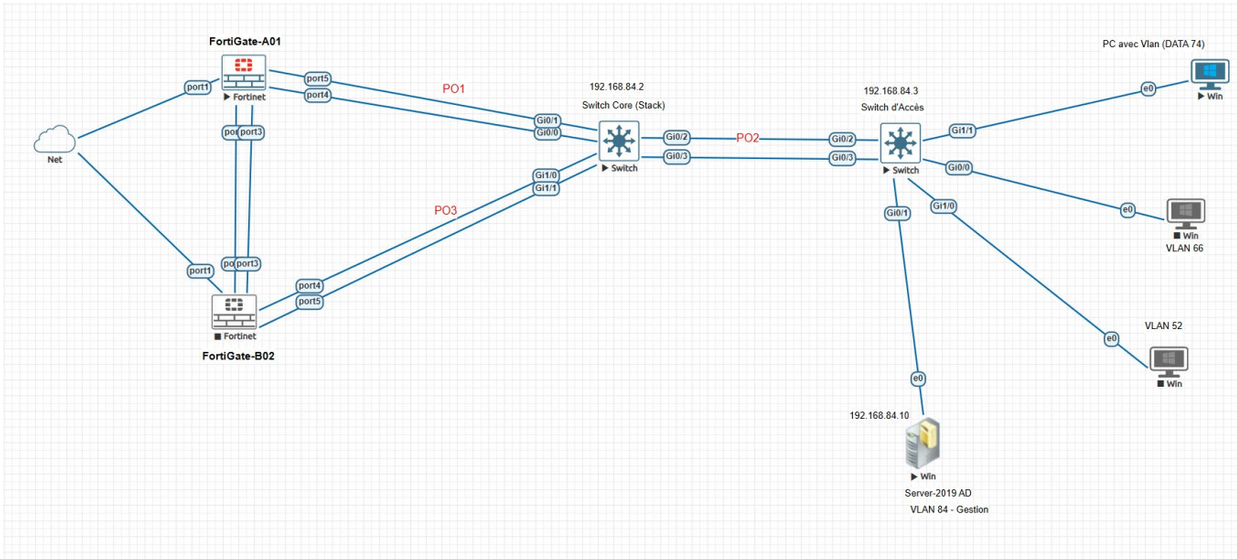
Les exemples, adresses IP, VLANs, et configurations présentés ici sont **fictifs ou adaptés pour des environnements de lab**.
Avant tout déploiement réel, chaque configuration doit être **vérifiée, validée et sécurisée** selon les politiques internes de votre entreprise.

Clause de non-responsabilité :
Les contributeurs ne sauraient être tenus responsables des dommages directs ou indirects résultant de l'utilisation du contenu de ce guide, que ce soit sur des environnements de test ou de production.

Étape 1 — Adressage & Subnetting (par VLAN et par équipement)

1) Objectif

Définir clairement les sous-réseaux, les passerelles et les adresses IP d'équipement pour tout le lab avant la configuration.



✅ 2. Plan d'adressage par VLAN

Tous les VLANs sont en /24 (masque 255.255.255.0).

VLAN	Rôle	Réseau /24	Passerelle (GW)	Broadcast	Hôtes utilisables
520	PROD	192.168.52.0/24	192.168.52.1	192.168.52.255	192.168.52.1 – 192.168.52.254
660	IOT / GUEST	192.168.66.0/24	192.168.66.1	192.168.66.255	192.168.66.1 – 192.168.66.254
745	DATA	192.168.74.0/24	192.168.74.1	192.168.74.255	192.168.74.1 – 192.168.74.254
845	MGMT / Serveurs	192.168.84.0/24	192.168.84.1	192.168.84.255	192.168.84.1 – 192.168.84.254

DNS/AD/DHCP : 10.84.5.10 (dans VLAN 845)

Faire le **hardening d'un FortiGate** (le sécuriser) est une étape **cruciale** avant sa mise en production. Cela consiste à **renforcer la sécurité** du pare-feu pour réduire les risques d'intrusion, d'erreur humaine ou de compromission.

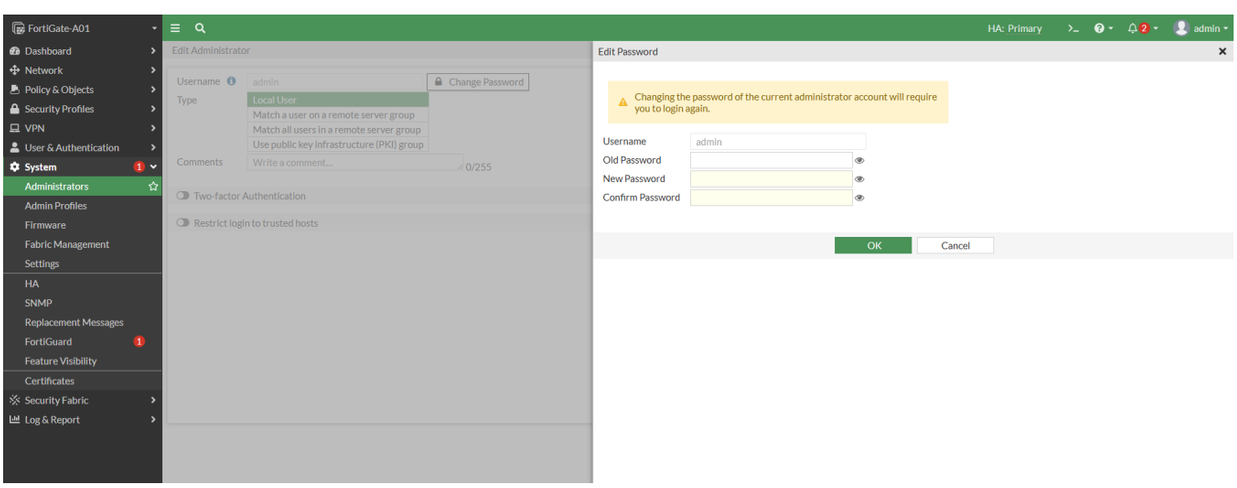
🧱 3. Sécuriser l'accès administratif

🔷 a. Changer le mot de passe par défaut

Par défaut : admin / (vide)

Change-le immédiatement :

```
config system admin
    edit admin
        set password <nouveau_mot_de_passe_complexe>
    next
end
```



Utilise un mot de passe **long (12+ caractères)** avec majuscules, minuscules, chiffres et symboles.

🔷 b. Restreindre l'accès à l'administration

➡️ Par interface :

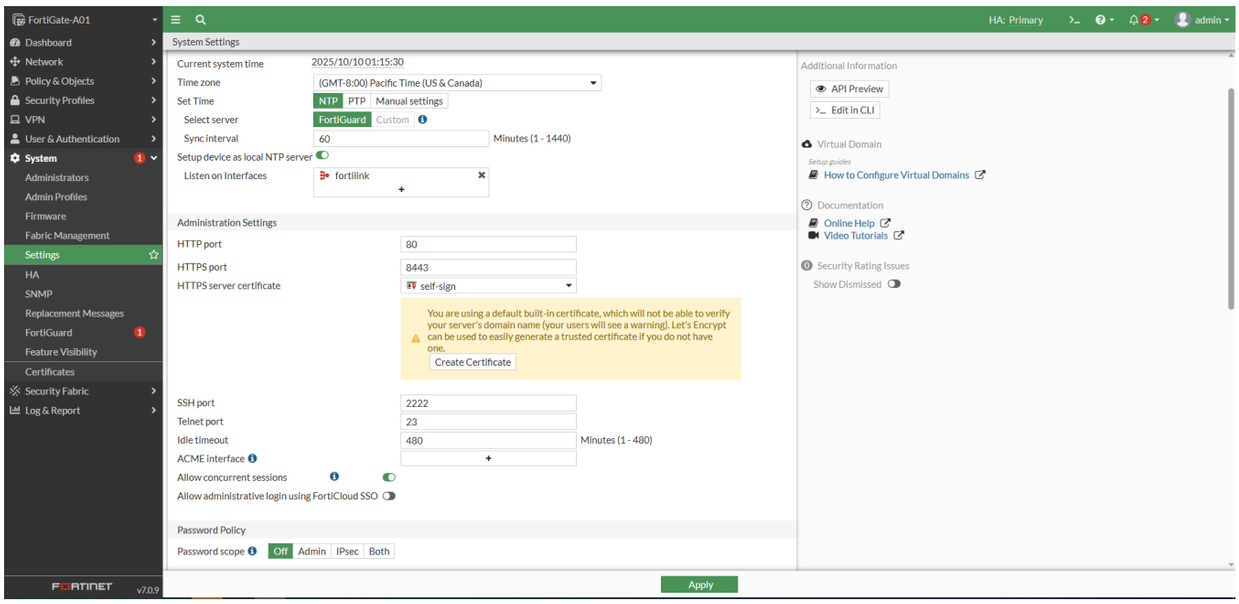
```
config system interface
    edit "wan1"
        set allowaccess ping
    next
    edit "mgmt"
        set allowaccess https ssh
        set trustedhosts 192.168.84.0 255.255.255.0
    next
end
```

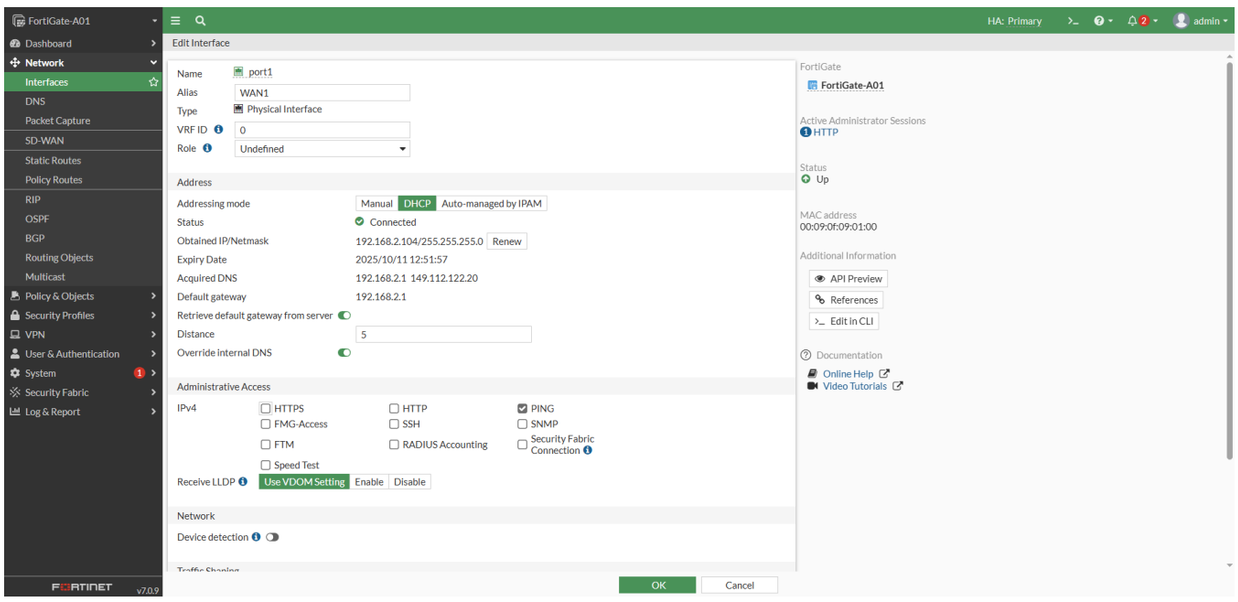
Désactive **l'accès administratif sur les interfaces exposées à Internet (WAN).**

Autorise-le **uniquement depuis ton réseau interne** (par trustedhosts).

🔷 c. Activer HTTPS et SSH seulement

```
config system global
    set admin-sport 8443
    set admin-ssh-port 2222
end
```





d. Activer la déconnexion automatique

```
config system global
    set admin-logout 300
end
```

🧩 4. Désactiver les services inutiles

Moins ton FortiGate écoute de services, mieux c'est.

Vérifie sur chaque interface :

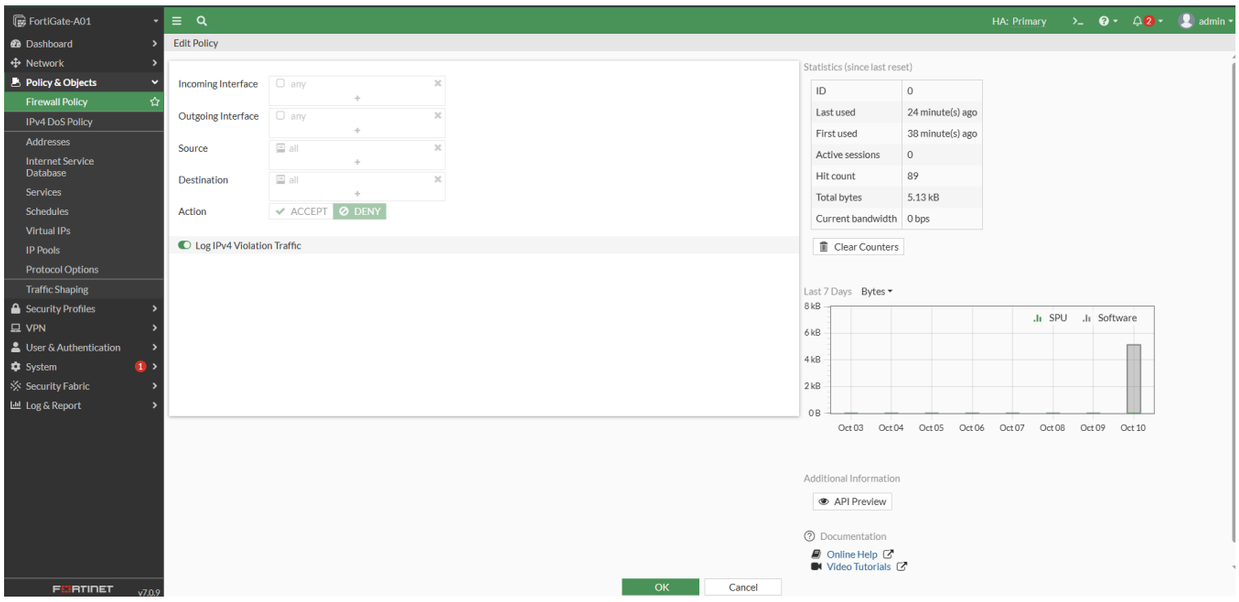
```
config system interface
    edit "wan1"
        set allowaccess ping
        # PAS de http, https, ssh, telnet sur le WAN
    next
end
```

🧰 5. Sécuriser les politiques de pare-feu

🔹 *a. Refuser tout par défaut*

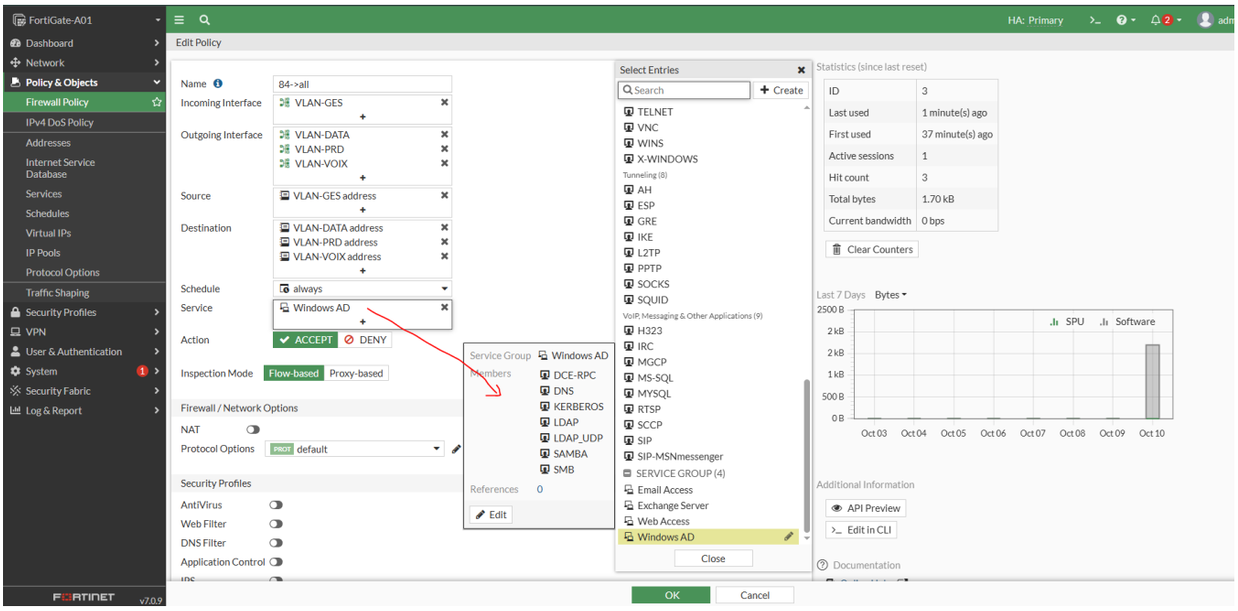
Toujours une **policy implicite de blocage** :

“deny all” à la fin de la liste de règles.



🔹 b. Créer des politiques claires et minimales

- Autorise uniquement ce qui est nécessaire.
- Utilise des **groupes d’adresses** et **services précis**.
- Active **NAT** seulement où c’est utile.



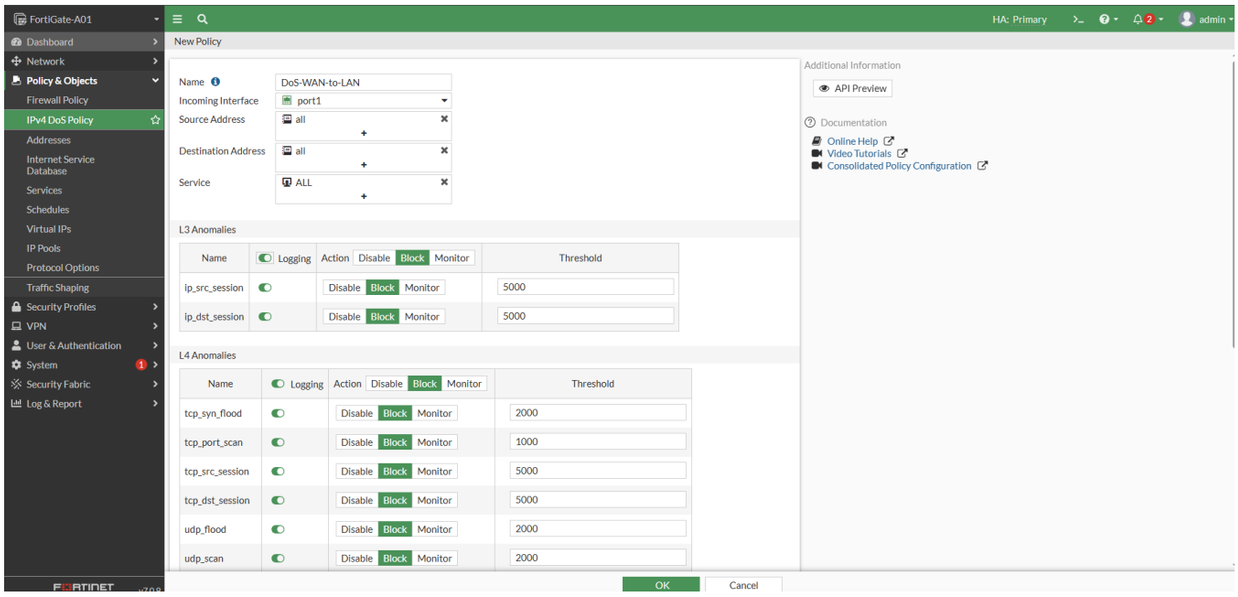
🧠 6. Protéger contre les attaques réseau

🔷 a. Activer DoS policies

Menu : **Policy & Objects → DoS Policy**

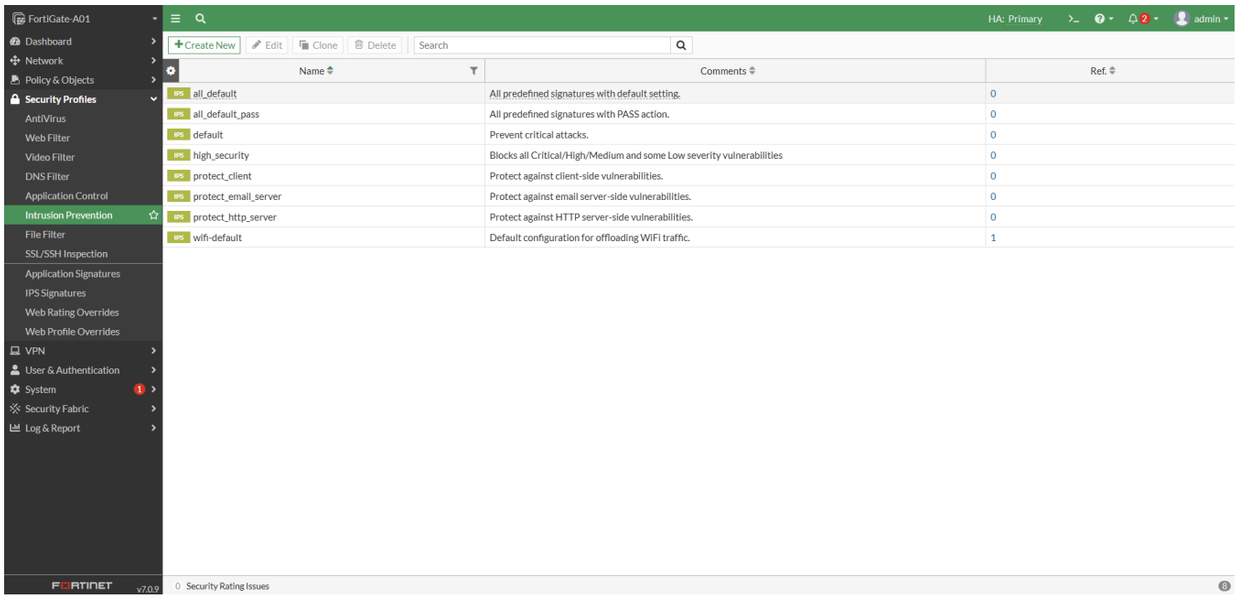
Exemples :

- Protection ICMP flood
- TCP SYN flood
- UDP flood



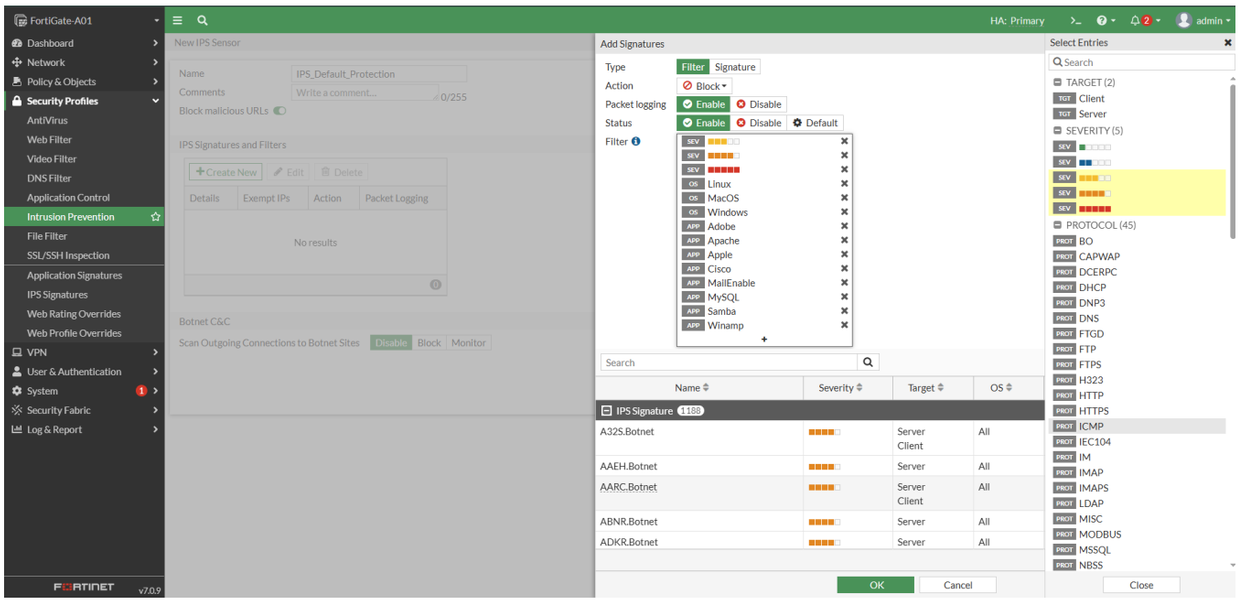
🔷 b. Activer IPS (Intrusion Prevention)

- Menu : **Security Profiles → Intrusion Prevention**
- Applique un profil IPS sur tes politiques Internet.



🔷 c. Activer Antivirus, Web Filtering, Application Control

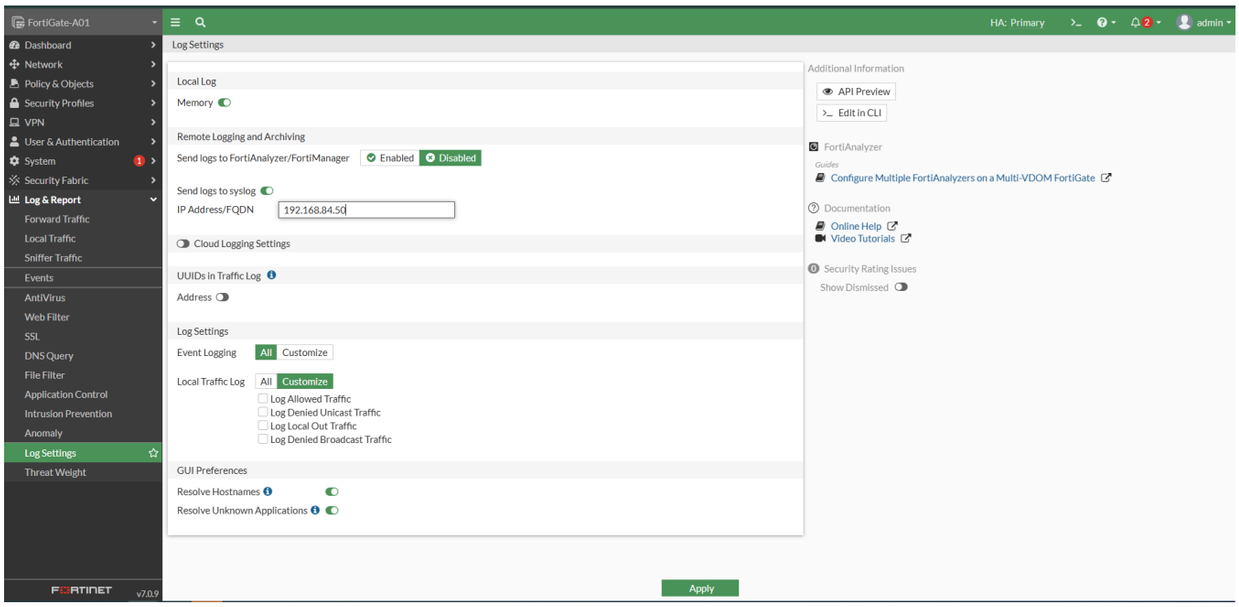
Security Profiles → associer aux politiques sortantes.



📝 7. Journalisation et supervision

🔷 a. Sauvegarder les logs localement ou sur un FortiAnalyzer/Syslog

```
config log syslogd setting
    set status enable
    set server "192.168.84.50"
    set facility local7
end
```



🔷 b. Active le logging sur chaque policy :

Dans chaque règle :

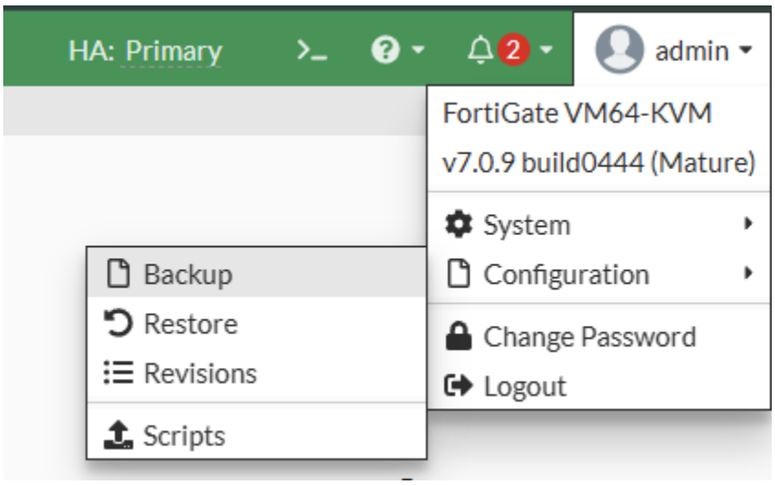
✅ **Log allowed traffic**

✅ **Log denied traffic**

🔑 8. Sauvegarde et versioning

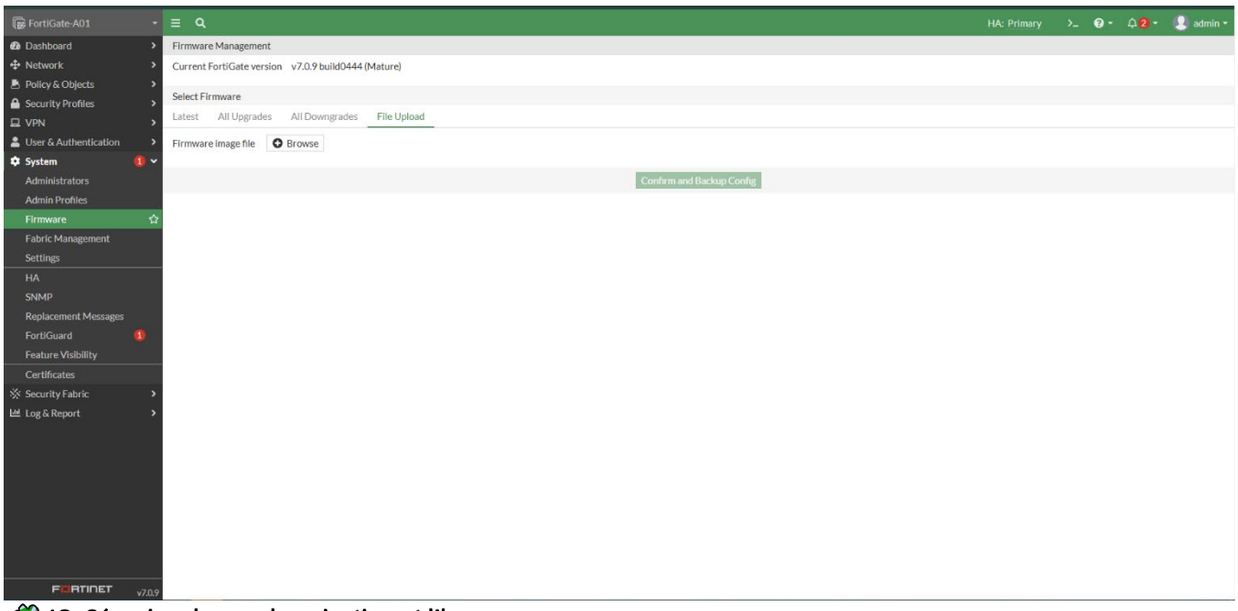
- Exporte une **copie de la configuration** :

```
execute backup config tftp <nom_du_fichier> <ip_du_serveur_tftp>
```



⚙️ 9. Mises à jour et maintenance

- Installe les dernières **firmwares FortiOS** depuis le portail Fortinet.
- Mets à jour les **signatures AV/IPS/Web Filter** régulièrement.
- Planifie des audits réguliers de configuration.



🛠️ 10. Sécuriser la synchronisation et l'heure

Pour éviter les erreurs de logs et de certificats :

```
config system ntp
    set ntpsync enable
    set server "pool.ntp.org"
end
```

📦 11. Restreindre les comptes administrateurs

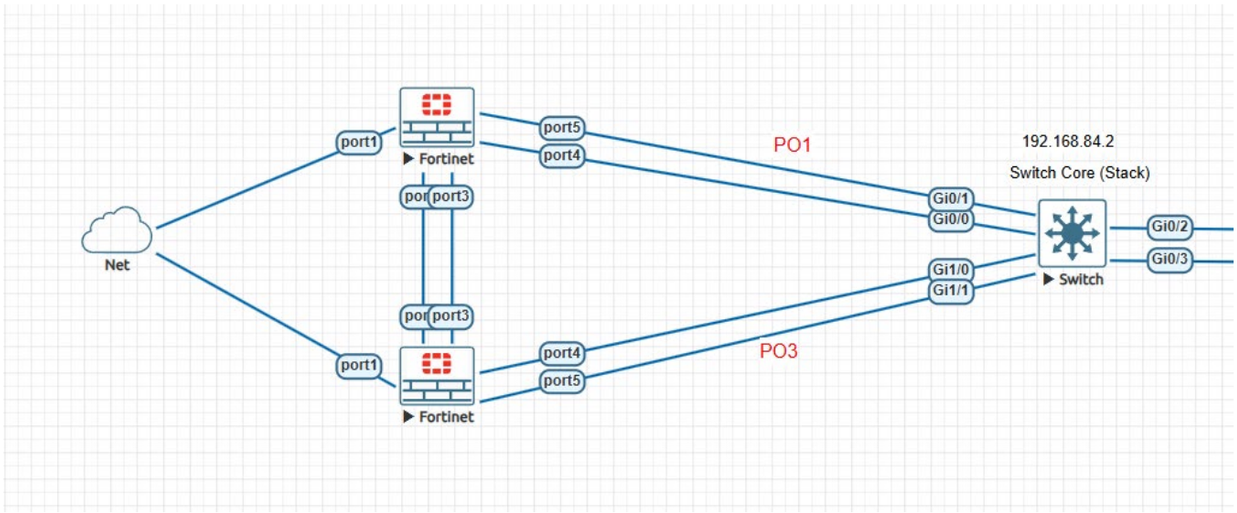
- Crée un compte **admin personnel** par utilisateur.
- Utilise des **profils d'administrateurs** restreints (pas tous "super_admin").

```
config system admin
    edit "support"
        set accprofile "read-only"
        set password <motdepasse>
    next
end
```

✅ 12. Vérifier la configuration de sécurité

Tu peux exécuter :

```
get system status
show system interface
show system admin
```



🧱 1 Objectif du câblage

Le but est de :

- Connecter les **2 FortiGate en HA (FortiGate A et B)**
- Connecter chaque FortiGate au **réseau externe (WAN)** et au **réseau interne (LAN / Core switch)**
- Assurer la **synchronisation** et le **heartbeat** entre les deux FortiGate

🧩 2 Détail des ports du schéma

Élément	Fonction	Détails
port1	WAN (vers Internet)	Connecté au réseau externe (Net)
port3 et port2 FortiGate (A et B)	HA (Heartbeat + Sync)	Lien direct entre les deux FortiGate
port4 et port5	LAN (vers le Switch Core)	Reliés en agrégation de liens (Port-Channel / LACP)
Switch Core (192.168.84.2)	Switch central	Reçoit les liens agrégés PO1 et PO3 depuis chaque FortiGate

🔌 3 Branchement physique étape par étape

🅰 Entre les FortiGate (HA Link)

1. Connecte **port3 et Port4** du FortiGate A vers **port3 et port4** du FortiGate B.
   → Ce lien servira pour la **synchronisation HA (heartbeat, configuration, sessions)**.

💡 Il est recommandé d'utiliser **2 câbles (port3 + port4)** pour redonder la communication HA (tu peux créer un HA link group plus tard).

🅱 Vers le WAN (Internet)

1. Connecte **port1** du FortiGate A vers ton réseau Internet (Net).
2. Connecte **port1** du FortiGate B vers le même réseau Internet (Net).

⚠️ Les deux doivent pointer vers le même réseau WAN (même passerelle). En HA, seul le **FortiGate actif** (Primary) enverra le trafic.

🅾 Vers le réseau interne (LAN / Core Switch)

🔶 FortiGate A :

- Connecte **port4** et **port5** du FortiGate A vers **GiO/O** et **GiO/1** du switch core.
  → Cela formera l'**agrégation PO1 (Port-channel)** sur le switch.

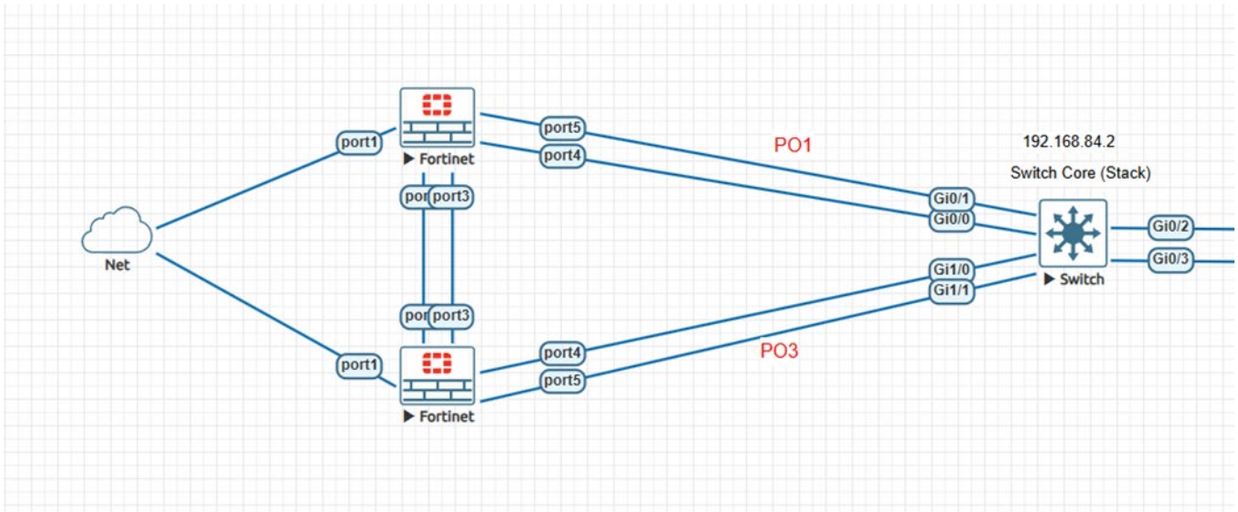
🔶 FortiGate B :

- Connecte **port4** et **port5** du FortiGate B vers **Gi1/0** et **Gi1/1** du switch core.
  → Cela formera l'**agrégation PO3** sur le switch.

💡 L'objectif est d'avoir deux liens logiques redondants :

- **PO1 :** FortiGate A ↔ Switch Core
- **PO3 :** FortiGate B ↔ Switch Core

📦 4 – CONFIGURATION PHYSIQUE & LOGIQUE COMPLÈTE



🔷 Objectif global

Mettre en place une infrastructure redondante et segmentée :

- Deux **FortiGate en HA (Active/Passive)**
- Un **Switch Core** en agrégation (Port-Channel / LACP)
- Un **Switch d'accès** connecté au Core (trunk VLANs)
- Des **VLANs** bien définis pour chaque segment réseau (Prod, Voix, Data, Mgmt)

🧩 PARTIE 1 — CONFIGURATION DES FORTIGATE

⚙️ 1️⃣ Configuration physique du FortiGate

Branchement des ports :

FortiGate	Port	Rôle	Connecté à	Description
A & B	port1	WAN	Réseau Internet	Sortie vers Net
A & B	port2	HA Sync	FG-A ↔ FG-B	Synchronisation / heartbeat
A & B	port3	HA Backup	FG-A ↔ FG-B	Redondance HA
A	port4+5	LAN (LACP)	Switch Core Gi0/0-1	Port-channel PO1
B	port4+5	LAN (LACP)	Switch Core Gi1/0-1	Port-channel PO3

💡 Astuce :

Utilise deux câbles Ethernet identiques pour chaque lien agrégé (même catégorie, même longueur) afin de garantir un équilibrage stable.

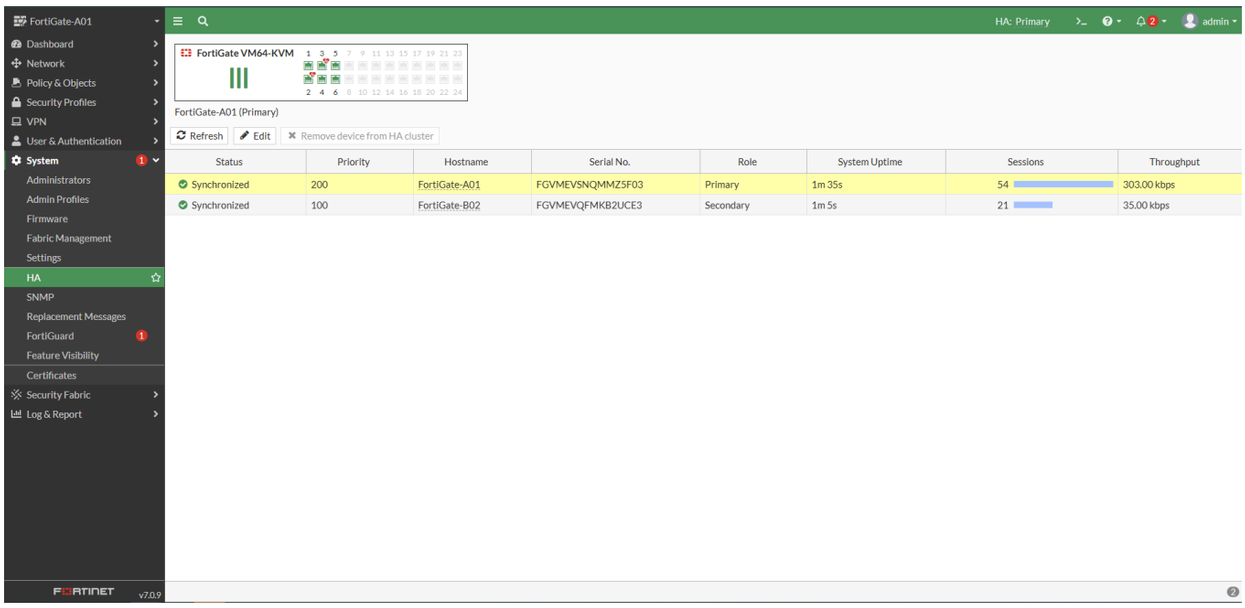
⚙️ 2 Configuration de la Haute Disponibilité (HA)

Sur **FortiGate A** (Master) :

```
config system ha
    set mode a-p
    set group-name "FGT_HA_LAB"
    set group-id 10
    set hbdev "port2" 50 "port3" 50
    set session-pickup enable
    set override enable
    set priority 200
    set monitor "port1" "port4"
end
```

Sur **FortiGate B** (Backup) :

```
config system ha
    set mode a-p
    set group-name "FGT_HA_LAB"
    set group-id 10
    set hbdev "port2" 50 "port3" 50
    set session-pickup enable
    set priority 100
    set monitor "port1" "port4"
end
```



💡 **Explication :**

- a-p = Active / Passive
- hbdev = ports dédiés au heartbeat
- session-pickup = conserve les sessions lors du failover
- override = priorité fixe pour le maître
- priority = 200 (maître) / 100 (esclave)

✅ **Vérification HA :**

```
CLI Console (1)
FortiGate-A01 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 1
Debug: 0
Cluster Uptime: 0 days 0:3:2
Cluster state change time: 2025-10-11 16:50:19
Primary selected using:
    <2025/10/11 16:50:19> FGVMEVSNQMMZ5F03 is selected as the primary because its override priority is larger than peer member FGVMEVQFMKB2UCE3.
    <2025/10/11 16:50:07> FGVMEVSNQMMZ5F03 is selected as the primary because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: enable
Configuration Status:
    FGVMEVSNQMMZ5F03(updated 1 seconds ago): in-sync
    FGVMEVQFMKB2UCE3(updated 5 seconds ago): in-sync
System Usage stats:
    FGVMEVSNQMMZ5F03(updated 1 seconds ago):
        sessions=32, average-cpu-user/nice/system/idle=3%/0%/2%/91%, memory=78%
    FGVMEVQFMKB2UCE3(updated 5 seconds ago):
        sessions=21, average-cpu-user/nice/system/idle=1%/0%/0%/97%, memory=77%
HBDEV stats:
    FGVMEVSNQMMZ5F03(updated 1 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=433246/1480/0/0, tx=1348679/1907/0/0
        port3: physical/10000full, up, rx-bytes/packets/dropped/errors=327236/754/0/0, tx=396418/909/0/0
    FGVMEVQFMKB2UCE3(updated 5 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=1321608/1839/0/0, tx=424584/1455/0/0
        port3: physical/10000full, up, rx-bytes/packets/dropped/errors=370418/849/0/0, tx=319424/736/0/0
Primary     : FortiGate-A01    , FGVMEVSNQMMZ5F03, HA cluster index = 0
Secondary   : FortiGate-B02    , FGVMEVQFMKB2UCE3, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FGVMEVSNQMMZ5F03, HA operating index = 0
Secondary: FGVMEVQFMKB2UCE3, HA operating index = 1
```

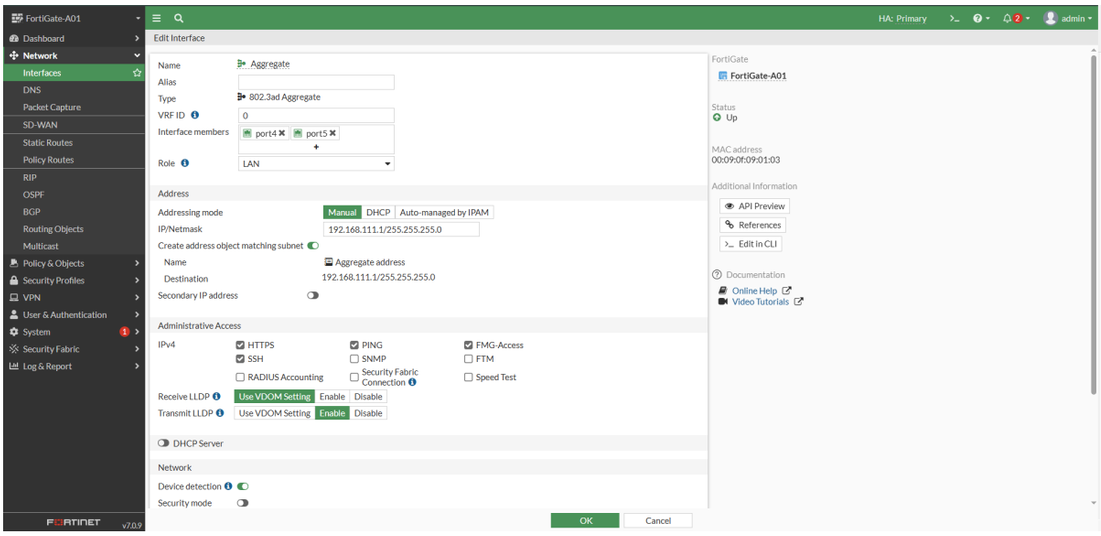
⚙️ 3 Configuration des agrégations (LACP)

Sur **chaque FortiGate** :

```
config system interface
    edit "AGG_LAN"
        set type aggregate
        set member "port4" "port5"
        set lacp-mode active
        set description "LACP vers Core"
    next
end
```

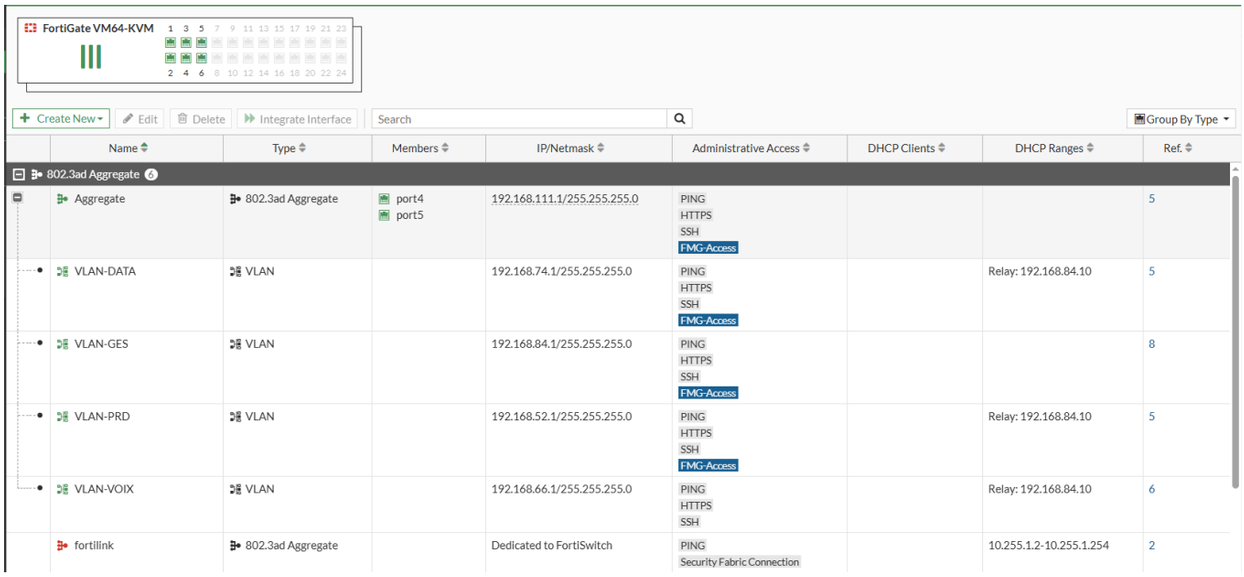
💡 **Astuce :**

Toujours activer lacp-mode active côté FortiGate et channel-group mode active côté Cisco.



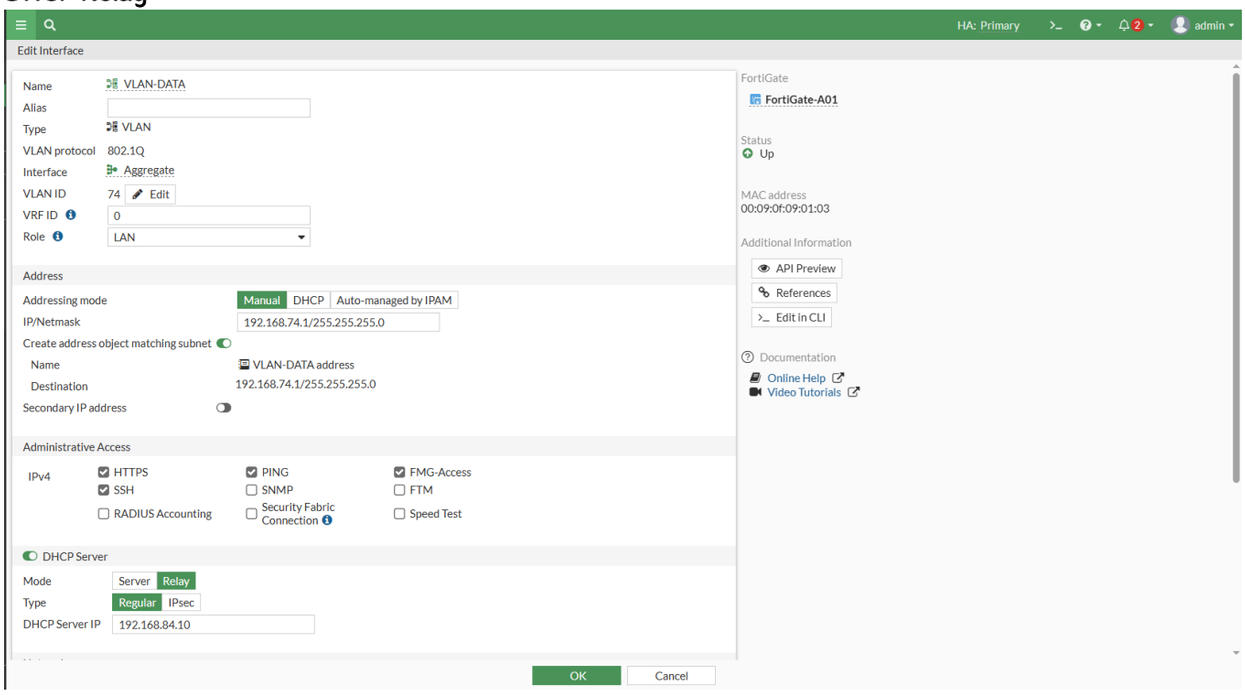
⚙️ 4 Création des VLANs sur le FortiGate

Toujours sur le **FortiGate A (Master)** — le B répliquera via HA :

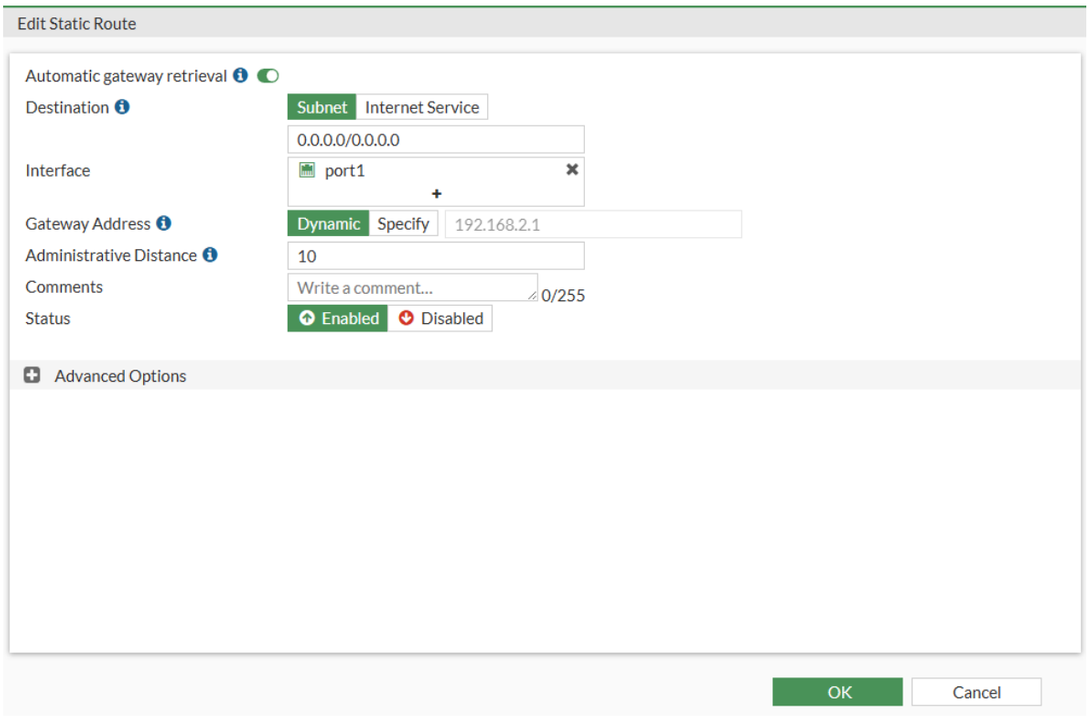


5 DHCP Relay & Routage Inter-VLAN

DHCP Relay



Routes statiques (si besoin WAN)



5 – CONFIGURATION SWITCH CORE ↔ SWITCH D'ACCÈS

⚙️ 1 OBJECTIF TECHNIQUE

- Relier le Switch Core (Stack) au Switch d'Accès par un Port-Channel PO2 (LACP, trunk 802.1Q).
- Permettre la propagation des VLANs 520 (PROD), 660 (IOT), 745 (DATA), 845 (MGMT) sur ce lien.
- Affecter correctement les ports d'accès du Switch d'Accès selon le diagramme.
- Attribuer des adresses de gestion statiques aux deux switches :
  - Core : 192.168.84.2
  - Accès : 192.168.84.3
  - Serveur AD : 192.168.84.10

🧱 2 CONFIGURATION DU SWITCH CORE (192.168.84.2)

Le Core agit comme cœur du réseau. Il centralise tous les VLANs, route vers le FortiGate, et connecte le switch d'accès.

🔌 Configuration du lien agrégé PO2 vers le Switch d'Accès

```
conf t
!
interface range Gi0/2 - 3
 description "Lien vers Switch d'Accès"
 channel-group 2 mode active
!
interface Port-channel2
 description "PO2 - Trunk vers Switch d'Accès"
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 520,660,745,845
 spanning-tree portfast trunk
 no shutdown
!
end
```

💡 **Explication :**

- channel-group 2 mode active → LACP dynamique.
- trunk allowed vlan → seuls les VLANs nécessaires passent sur le lien.
- portfast trunk → évite les délais STP au démarrage.

🌐 **Interface de gestion VLAN 845**

```
interface Vlan845
 description "Interface de gestion Core Switch"
 ip address 10.84.5.2 255.255.255.0
 no shutdown
```

💡 L'interface VLAN845 te permet de **gérer le switch Core** depuis le réseau d'administration (VLAN 845).

🧭 **VLANs à propager (déjà créés, vérification)**

```
vlan 520
 name PROD
vlan 660
 name IOT
vlan 745
 name DATA
vlan 845
 name MGMT
```

🧱 3️⃣ CONFIGURATION DU SWITCH CORE (192.168.84.2)

Le Core agit comme cœur du réseau. Il centralise tous les VLANs, route vers le FortiGate, et connecte le switch d'accès.

```
conf t
!
interface range Gi0/0 - 1
 channel-group 1 mode active
 description "PO1 vers FortiGate-A"
!
interface range Gi1/0 - 1
 channel-group 3 mode active
 description "PO3 vers FortiGate-B"
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan all
 spanning-tree portfast trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan all
 spanning-tree portfast trunk
```

💡 **Astuce :**

Numérote les port-channel selon le FortiGate connecté (PO1 = FGT A, PO3 = FGT B).

⚙️ 4️⃣ Création des VLANs

```
vlan 520
 name PROD
vlan 660
 name IOT
vlan 745
 name DATA
vlan 845
 name MGMT
```

🧩 5️⃣ CONFIGURATION DU SWITCH D'ACCÈS (192.168.84.3)

Le Switch d'Accès distribue les VLANs aux hôtes : PC, serveurs, IoT.
Il reçoit tous les VLANs via le trunk PO2 depuis le Core.

✒️ Configuration du lien agrégé PO2 vers le Core

```
conf t
!
interface range Gi0/2 - 3
 description "Uplink vers Core Switch (PO2)"
 channel-group 2 mode active
!
interface Port-channel2
 description "PO2 - Trunk vers Core Switch"
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 520,660,745,845
 spanning-tree portfast trunk
 no shutdown
!
end
```

💡 Les deux ports GiO/2 et GiO/3 du Switch d'Accès sont **agrégés** en un **lien logique PO2** qui transporte tous les VLANs.

🌐 Interface de gestion VLAN 845 (adresse .3)

```
interface Vlan845
 description "Interface de gestion Switch Accès"
 ip address 10.84.5.3 255.255.255.0
 no shutdown
```

.1O reste le serveur AD/DHCP/DNS.

⚙️ 6️⃣ Lien vers le Switch d'Accès

```
interface Gi0/24
 description "Uplink vers Switch Accès"
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan all
 spanning-tree portfast trunk
```

🧩 7️⃣ CONFIGURATION DU SWITCH D'ACCÈS (192.168.84.3)

Le Switch d'Accès distribue les VLANs aux hôtes : PC, serveurs, IoT.

Il reçoit tous les VLANs via le trunk PO2 depuis le Core.

🌐 Interface de gestion VLAN 845 (adresse .3)

```
interface Vlan845
 description "Interface de gestion Switch Accès"
 ip address 10.84.5.3 255.255.255.0
 no shutdown
```

Cela permet d'administrer le switch via le réseau de gestion (VLAN 845).

🧭 Création des VLANs (doivent correspondre au Core)

```
vlan 520
 name PROD
vlan 660
 name IOT
vlan 745
 name DATA
vlan 845
 name MGMT
```

💡 Tous les VLANs doivent exister localement sur le switch d'accès, même s'ils ne sont pas routés ici.

💻 Configuration des ports d'accès (selon le schéma)

Poste / Serveur	Port	VLAN	Description
PC Data	Gi0/0	74	VLAN DATA
PC IoT	Gi0/1	66	VLAN VOIX
PC Prod	Gi1/0	52	VLAN PROD
Serveur AD/DNS/DHCP	Gi0/1	84	VLAN MGMT

```
interface Gi0/0
 description "PC VLAN DATA (745)"
 switchport mode access
 switchport access vlan 745
 spanning-tree portfast
!
interface Gi0/1
 description "PC VLAN IOT (660)"
 switchport mode access
 switchport access vlan 660
 spanning-tree portfast
!
interface Gi1/0
 description "PC VLAN PROD (520)"
 switchport mode access
 switchport access vlan 520
 spanning-tree portfast
!
interface Gi1/1
 description "Serveur AD - VLAN MGMT"
 switchport mode access
 switchport access vlan 845
 spanning-tree portfast
!
end
```

🧪 Tests à effectuer

1. **Test LACP :**

```
Switch-Core>en
Switch-Core#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi0/0(P)    Gi0/1(P)
2      Po2(SU)         LACP      Gi0/2(P)    Gi0/3(P)
3      Po3(SU)         LACP      Gi1/0(P)    Gi1/1(P)

Switch-Core#
```

→ Le PO2 doit apparaître en mode “P” (active).

2. Test de connectivité gestion :

```
Switch-Core#ping 192.168.84.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.84.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Switch-Core#ping 192.168.84.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.84.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch-Core#ping 192.168.84.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.84.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
Switch-Core#
```

3. **Vérification du trunk :**

```
Switch-Access#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Po2         on               802.1q         trunking      1

Port        Vlans allowed on trunk
Po2         1,52,66,74,84

Port        Vlans allowed and active in management domain
Po2         1,52,66,74,84

Port        Vlans in spanning tree forwarding state and not pruned
Po2         1,52,66,74,84
Switch-Access#
```

🧩 6 – CONFIGURATION DU SERVEUR AD / DNS / DHCP

(Windows Server 2019 - VLAN 845 Gestion)

🎯 Objectif

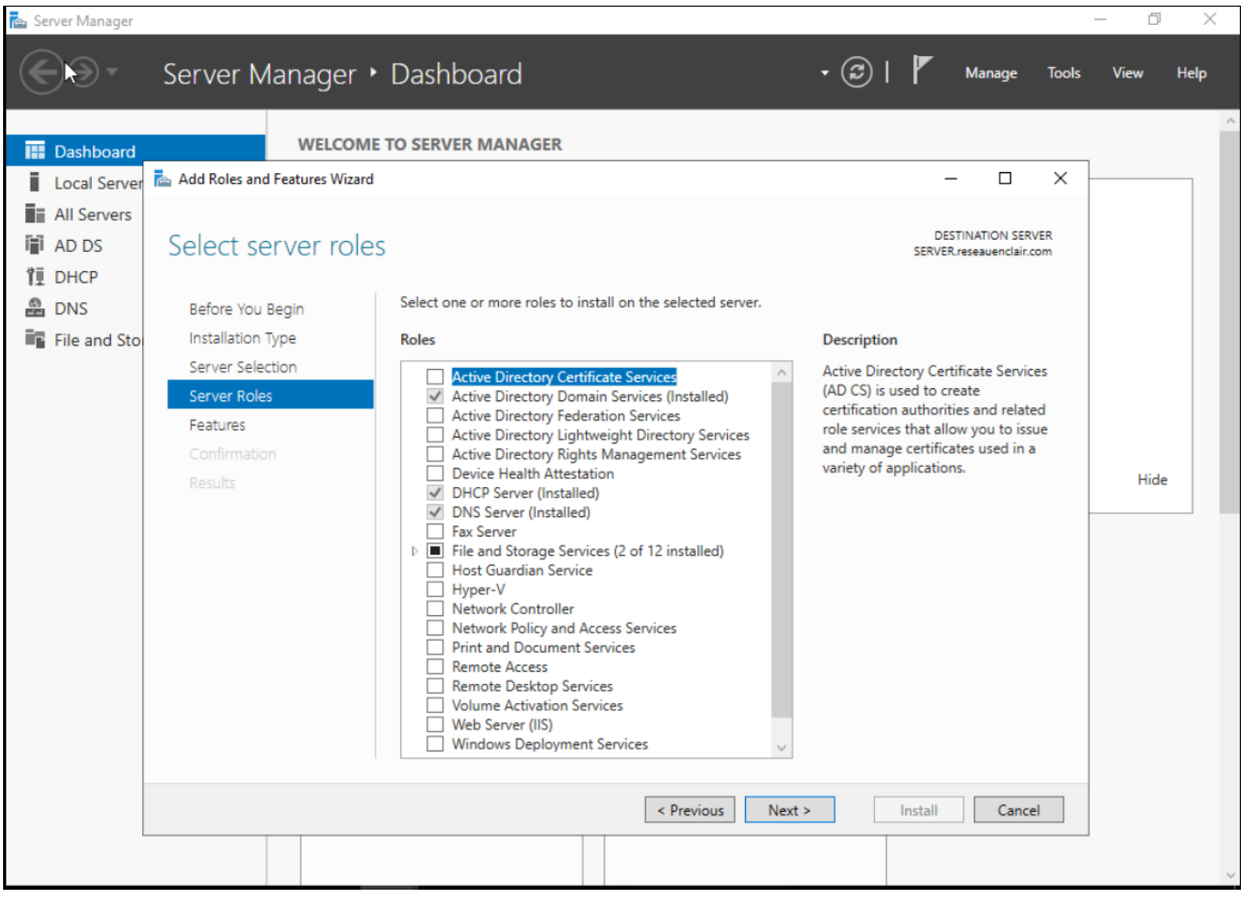
Mettre en place un **contrôleur de domaine Active Directory** sur le VLAN 845, incluant :

- Le **service DHCP** qui distribue les IP pour tous les VLANs (520, 660, 745, 845)
- Le **service DNS**, intégré à l'AD pour la résolution des noms internes
- Le **service AD DS (Active Directory Domain Services)**
- La **synchronisation avec le FortiGate** via le **DHCP Relay**

🖥️ 1️⃣ Paramètres réseau du serveur

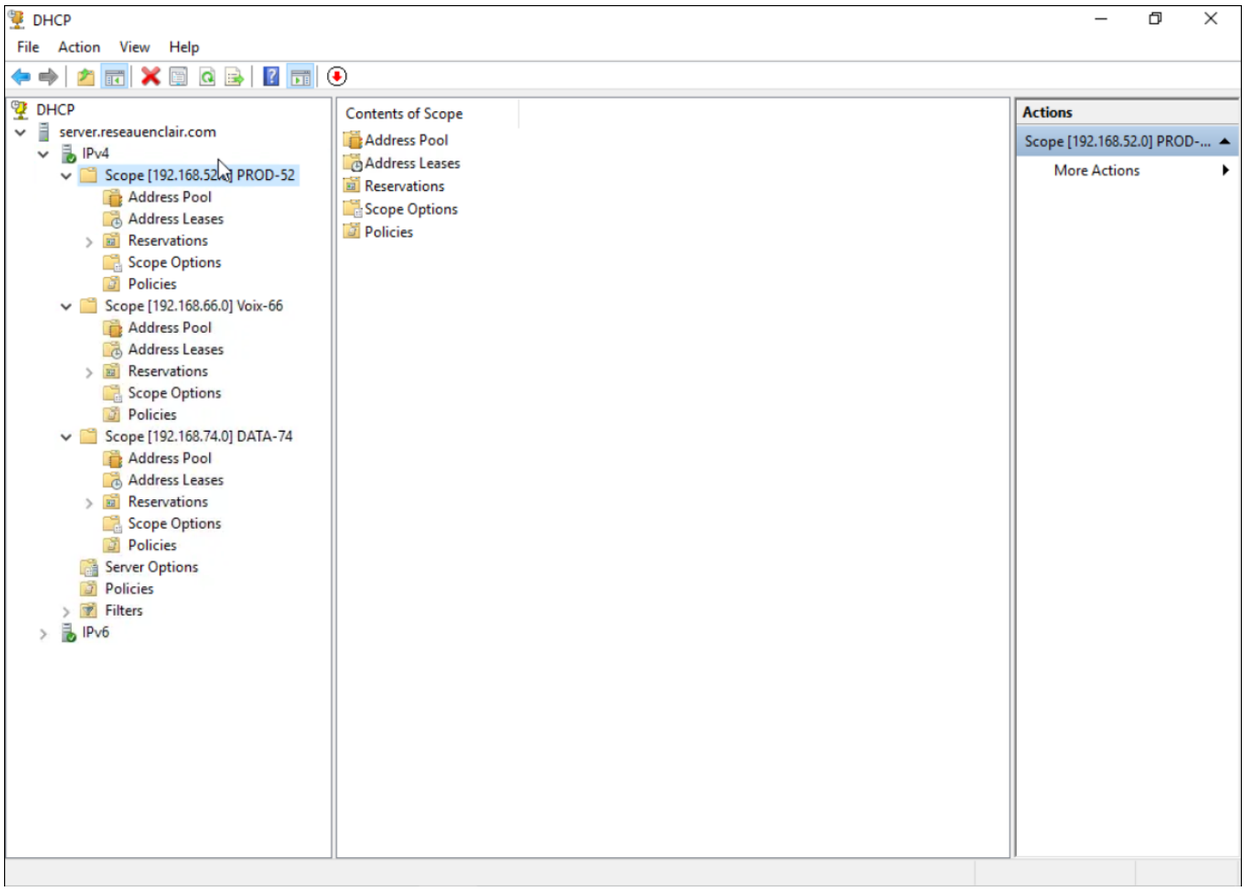
Interface : Ethernet0
VLAN : 84 (MGMT)
Adresse IP : 10.84.5.10 /24
Passerelle : 10.84.5.1 (FortiGate)
DNS local : 127.0.0.1 (auto après configuration DNS)

🧱 2️⃣ Installation des rôles AD DS, DNS et DHCP



📝 3️⃣ Configuration du service DHCP

🔷 Étape 1 – Autoriser le serveur DHCP dans l'AD



◆ Étape 2 – Activer la mise à jour DNS dynamique