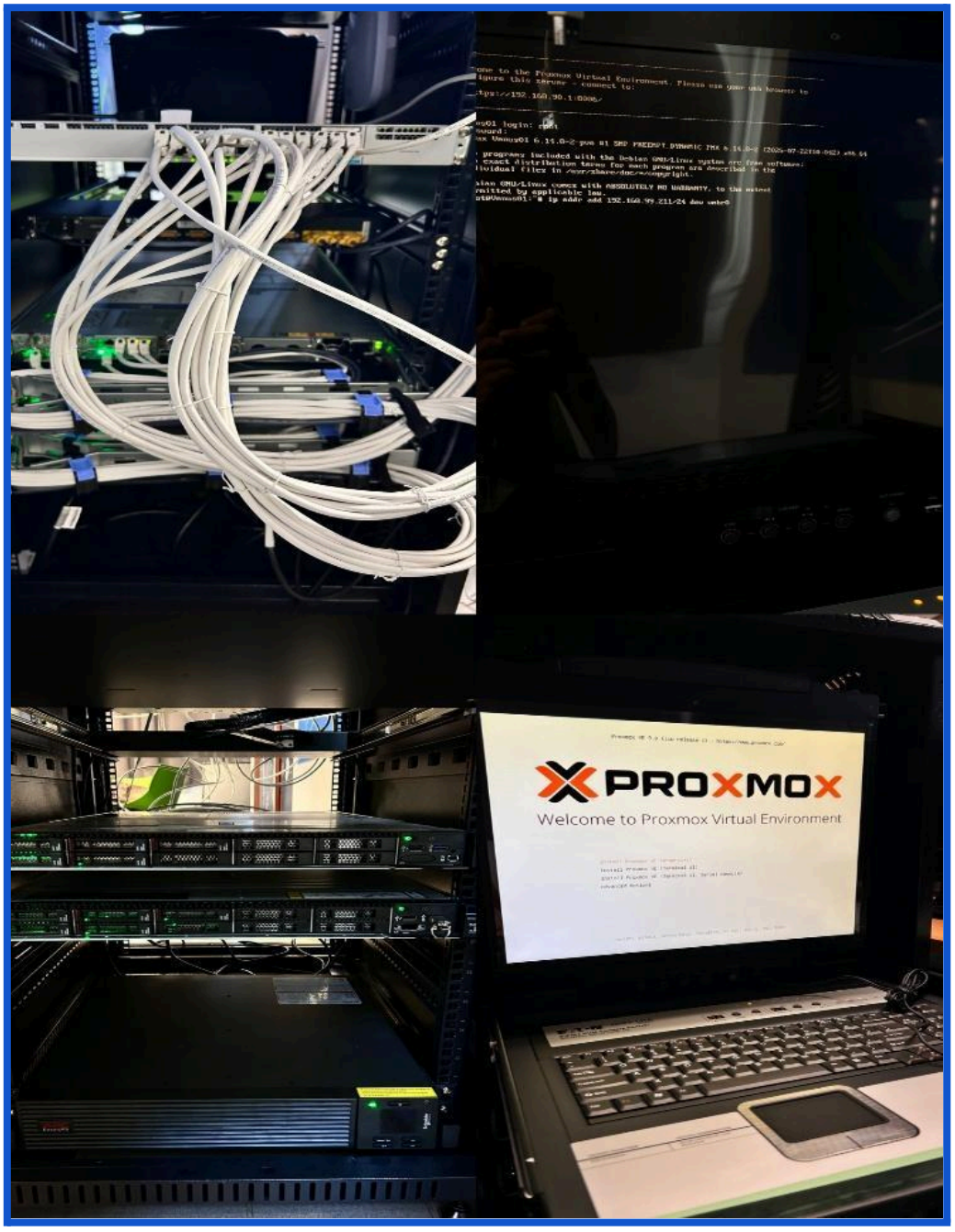
BTS SIO – SERVICES INFORMATIQUES AUX ORGANISATIONS

OPTION SISR – SOLUTIONS D'INFRASTRUCTURE, SYSTÈMES ET RÉSEAUX

Session : 2024-2026

DOSSIER TECHNIQUE E6 - Projet 1

Conception et déploiement de l'infrastructure Vénus



GOVINDIN Devendra

TABLE DES MATIÈRES

PROJET 1 – CONCEPTION ET DÉPLOIEMENT DE L'INFRASTRUCTURE VÉNUS

PROJET 1 - INFRASTRUCTURE VENUS

I]-PRÉSENTATION DU CONTEXTE

A.D.N Services est une PME en pleine expansion, spécialisée dans l'accompagnement à la transition digitale aux professionnels. Dans le cadre de son développement stratégique, l'entreprise ouvre sa toute première implantation physique sur l'île de La Réunion.

** A.D.N = Accompagnement au Développement Numérique*

Cette création d'agence requiert la conception d'une architecture système et réseau complète, partant de zéro. L'infrastructure déployée, identifiée par le nom de projet Vénus et associée au domaine interne `venus.local`, doit supporter les activités de l'entité locale et lui fournir une totale autonomie technique.

En tant que prestataire informatique, ma mission s'est concentrée sur la conception et le déploiement du socle de cette infrastructure. L'enjeu est d'assurer la haute disponibilité de la virtualisation et la ségrégation stricte des flux, afin de livrer une base saine et opérationnelle pour l'hébergement des futurs services d'infrastructure et les outils de gestion, de supervision, de sauvegarde et de cybersécurité de l'agence.

Localisation : île de la Réunion
Type de structure : PME
Utilisateurs cibles : les différents services de l'infrastructure *(administration, accueil, ressources humaines, direction, marketing etc…)*
Besoin : Isolation strictes des services et continuité de services.

II] ANALYSE DES BESOINS ET CONTRAINTES

A. Besoins fonctionnels

Pour répondre au cahier des charges de A.D.N Services, l'infrastructure doit couvrir les domaines suivants :

1. Sécurité réseau et périmétrique :
    - ***Protection matérielle*** *:* Déploiement d'un pare-feu physique (NGFW) pour assurer la frontière, le routage et le filtrage avec l'extérieur.
    - ***Accès à distance*** *:* Mise en place d'un tunnel VPN IPsec pour permettre l'administration sécurisée de l'infrastructure à distance ou le télétravail pour certains employés.
    - ***Évolutivité*** *:* L'architecture doit prévoir la possibilité d'isoler de futurs services exposés (DMZ).

2. Préparation à l’intégration des services systèmes :
    - ***Routage des services d'identité*** *:* le réseau doit être configuré *(agents de relais DHCP, objets et règles de flux)* pour permettre l'intégration fluide d'un futur contrôleur de domaine Active Directory centralisant les authentifications locales.
3. Préparation à l'exploitation et la maintenance :
    - ***Supervision et Helpdesk*** *:* L'architecture réseau doit être conçue pour héberger et laisser communiquer les futures solutions de gestion de parc et de supervision proactive.

B. Contraintes techniques

- **Continuité de services et évolutivité** : L'architecture doit tolérer les pannes matérielles et permettre l'ajout de nouvelles machines virtuelles sans refonte globale.
- **Standardisation** : Les équipements doivent provenir de constructeurs leaders *(Cisco, Fortinet)* pour garantir la robustesse et faciliter la maintenance par tout prestataire qualifié.
- **Performance** : L'interconnexion entre le stockage, la virtualisation et le cœur de réseau s'appuiera sur des liaisons à 10 Gbit/s pour éviter les goulots d'étranglement.

C. Contraintes économiques et organisationnelles

- **Optimisation budgétaire** : Le recours à un hyperviseur Open Source permettra de supprimer les coûts de licences logicielles, allouant ainsi le budget vers du matériel physique performant.
- **Délais** : L'infrastructure doit être opérationnelle avant mai 2026 pour permettre les déploiements applicatifs de l'équipe système.

III]-ARCHITECTURE MATÉRIELLE

A. Serveur – ThinkSystem SR630 V3

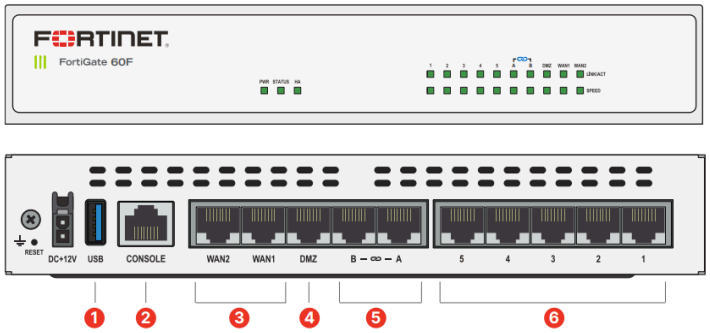
Composant	Spécification	Rôle et Justification du Choix
Châssis	Lenovo ThinkSystem SR630 V3	Format compact (1U) pour optimiser l'espace dans la baie.
Processeurs	Intel Xeon Gold 5416S par serveur	Puissance de calcul garantissant l'exécution simultanée des VMs
Mémoire Vive	256 Go TruDDR5 (8x32Go)	Capacité étendue pour répondre aux exigences d'allocation RAM des multiples VMs
Contrôleur RAID	ThinkSystem RAID 9350-16i (4 Go Cache Flash) par serveur	Tolérance de panne matérielle. Le cache dédié accélère les écritures et décharge le CPU des calculs de parités
Stockage	5x SSD SATA 960 Go	Technologie SSD assurant une faible latence et une réactivité maximale
Réseau Rapide	Adaptateur BroadCOM 57416	2 ports 10 Gbit/s dédiés aux opérations de management Proxmox.
Réseau Annexe	Adaptateur BroadCOM 5719	4 ports 1 Gbit/s pour segmenter physiquement le trafic applicatif.
Gestion	Port IMM dédié (1 Gbit/s) + Lenovo XClarity Pro	Interface hors-bande (XClarity Pro) pour la gestion matérielle à distance.
Alimentation	2x Blocs 1100W Titanium	Redondance électrique avec remplacement à chaud assurant la continuité de service et une haute efficacité énergétique
Fond de panier	SATA 10 x 2,5"	Permet une grande évolutivité pour l'ajout futur de stockage sans modification matérielle.

B. Switch – Cisco catalyst 9200 (POE+)

Équipement central de l'infrastructure de distribution (Niveau 2/3).

- Rôle : Il centralise la connectivité filaire de l'agence et assure la segmentation logique des flux. Ses ports PoE+ sont provisionnés pour alimenter de futurs équipements périphériques (téléphonie IP, bornes Wi-Fi).
- Interfaces : 16 ports RJ45 Gigabit et 8 ports 10 Gigabit.

C. Pare-feu : Fortinet Fortigate 60F



Appliance de sécurité de nouvelle génération (NGFW) placée en bordure de réseau.

- Rôle : Il protège le réseau contre les menaces externes, gère l'accès à Internet via le fournisseur, opère le routage au sein de l'infrastructure local de manière sécurisée et centralise les accès VPN distants.
- Interfaces : 5 ports LAN Gigabit, 1 port DMZ et 2 ports WAN Gigabit.

IV]-ETUDE COMPARATIVE ET CHOIX TECHNIQUE

A. Comparatif des solutions de stockage *(5 disques par serveur)*

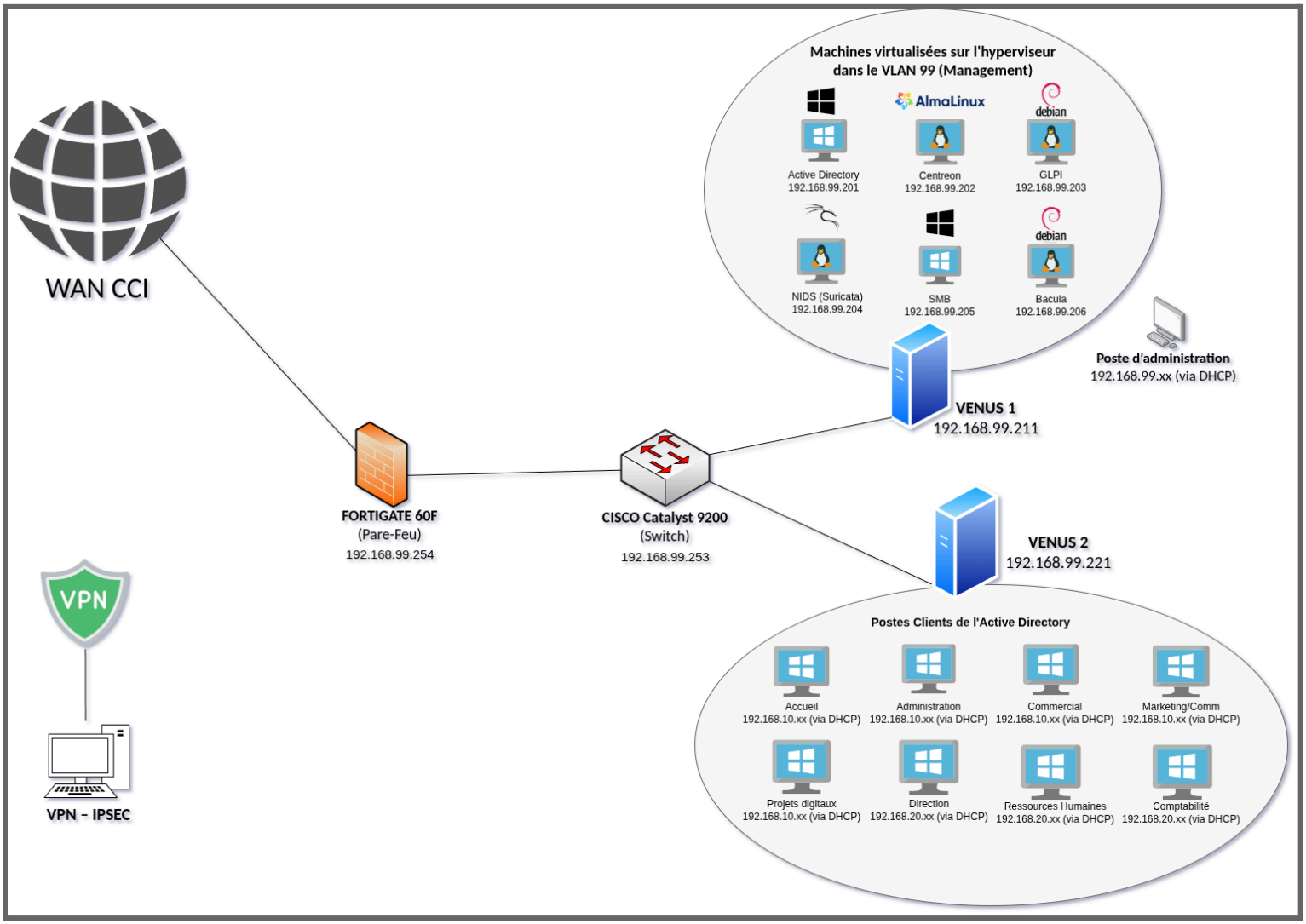
Solutions	Configuration	Tolérance de pannes	Performance	Avis
RAID 6	RAID 6 *(1 OS + 4 disques VM)*	Excellente: Tolère la perte simultanée de 2 disques	Correcte	**Retenue**. Sécurité maximale des données. En cas de panne du disque OS, l'autre nœud Proxmox permet le redémarrage via les sauvegardes.
RAID 5	2 disques en RAID 1 (OS) + 3 disques en RAID 5 (VMs).	Faible : Tolère la perte d'un seul disque par grappe.	Bonne	**Écarté**. Risque de perte de données trop élevé les machines virtuelles de production.
RAID 10	1 disque OS + 4 disques en RAID 10 (2 miroirs).	Moyenne (1 disque par miroir)	Excellente	**Écarté**. Capacité utile trop réduite (50%) face aux besoins d'évolution de l'agence.

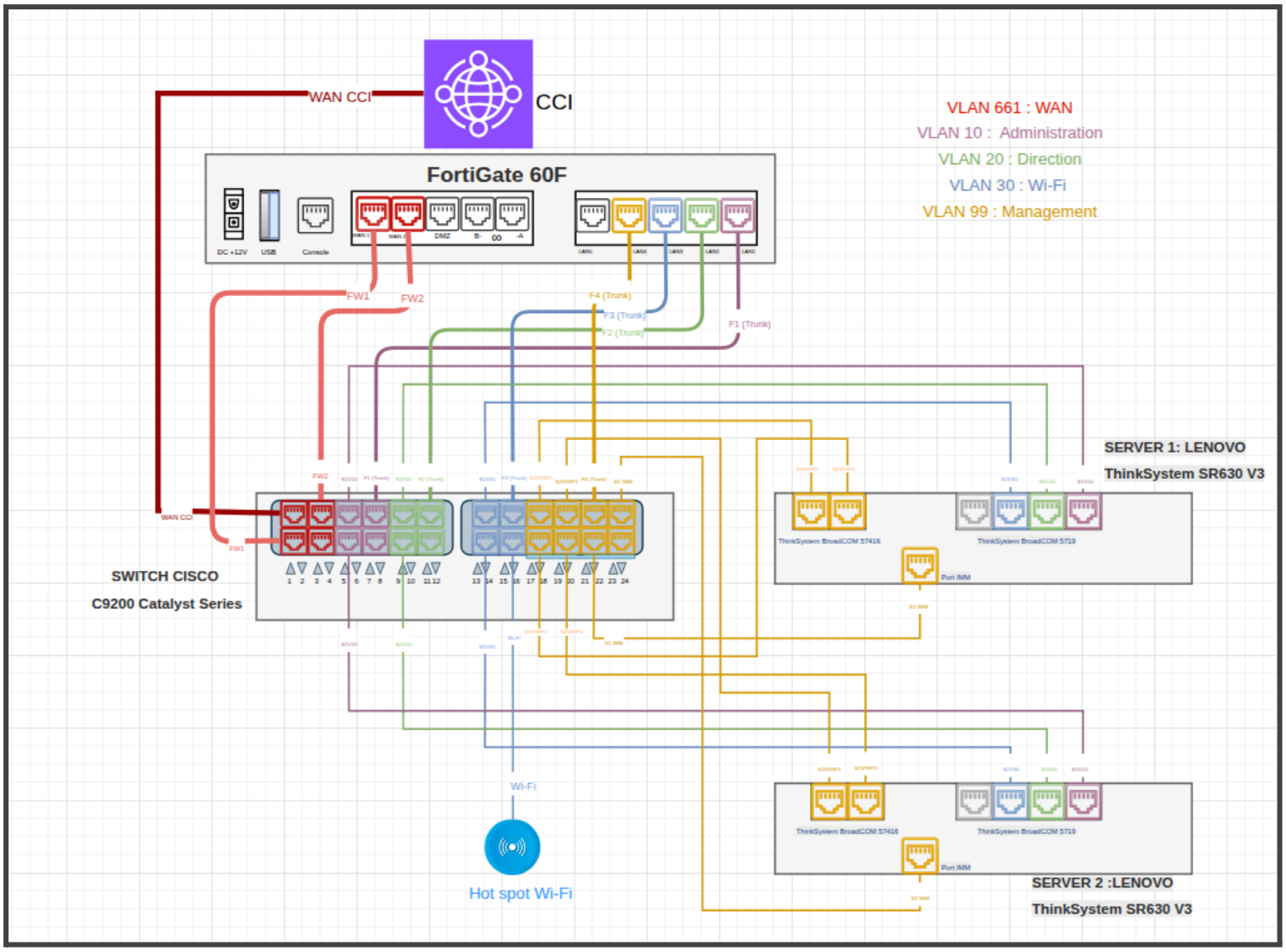
Note sur la continuité de service : la résilience repose sur le cluster de management Proxmox. Si le disque OS d'un serveur tombe, il suffit de réinstaller l'hyperviseur sur un disque neuf, tandis que le second serveur assure la production grâce à la restauration des sauvegardes gérées par l'équipe logicielle.

B. Comparatif des solutions de virtualisation

Solutions	Licence	Avantages	Inconvénients	Avis
VMware vSphere (ESXi)	Licence payante	Standard industriel extrêmement stable et riche en fonctionnalités	Coût de licence par cœur inadapté au budget.	**Écarté.** Surcoût de licence important
Microsoft Hyper-V	Licence Payante	Intégration parfaite avec l'écosystème Windows et Active Directory.	Nécessite des licences Windows Server Datacenter coûteuses pour exploiter un cluster.	**Écarté**. Surcoût de licence important
Proxmox VE	Open Source	Intègre nativement et sans surcoût la gestion de cluster (Haute Disponibilité) et le backup.	Interface parfois moins intuitive que. Support technique constructeur en option.	**Retenue.** Répond au budget tout en offrant des fonctions nécessaires à l'infrastructure

V] -INFRASTRUCTURE PROPOSÉE POUR UNE MISE EN ŒUVRE





L'infrastructure retenue pour A.D.N Services s'articule autour de 4 zones clés :

1. **Liaison WAN** : L'agence dispose d'un accès réseau externe fourni par la CCI (Compagnie de Connectivité Interentreprises), l'opérateur chargé de l'interconnexion sécurisée du site.
2. **Sécurité et Routage** : Le FortiGate 60F gère le point d'entrée WAN, contrôle les politiques de filtrage inter-VLAN et maintient les tunnels VPN IPsec.
3. **Distribution Réseau** : Le Cisco Catalyst 9200 centralise le câblage et segmente logiquement le trafic en différents sous-réseaux.
4. **Haute Disponibilité** : Les deux serveurs Lenovo virtualisés sous Proxmox forment une grappe (cluster) pour garantir la résilience et l'administration centralisée des services.

VI]-RÉALISATION TECHNIQUE – BAIE VENUS

A. Déploiement de l'infrastructure réseau

La segmentation isole les différents environnements. Le commutateur SW-Venus assure la séparation de niveau 2, et le FortiGate porte les passerelles de niveau 3.

1. Segmentation réseau et plan d'adressage

Segmentation des VLANs

VLAN ID	Nom	Adresse IP	Passerelle
661	WAN CCI	172.16.60.80/22 *(IP Interface FAI)*	172.16.63.254
10	Administration	192.168.10.0/24 *(réseau)*	192.168.10.254
20	Direction	192.168.20.0/24 *(réseau)*	192.168.20.254
30	Wi-Fi	192.168.30.0/24 *(réseau)*	192.168.30.254
99	Management	192.168.99.0/24 *(réseau)*	192.168.99.254

Note de sécurité et contexte pédagogique :
Dans un environnement de production réel, la divulgation des plans d'adressage complets, et plus particulièrement des adresses IP publiques, est proscrite dans les documentations non classifiées afin d'éviter toute fuite d'information réseau. De plus, bien que l'adresse 172.16.60.80/22 de l'interface WAN simule ici l'adresse IP publique de la baie Vénus fournie par notre opérateur, il s'agit techniquement d'une adresse privée au réseau interne fourni par le centre de formation.

Attribution des ports (Switch - FortiGate)

VLAN ID	Switch	FortiGate
661	ACCESS : port 1, 2, 3 et 4	WAN 1
10	ACCESS : port 5, 6 et 8 TRUNK : port 7	Internal 1
20	ACCESS : port 9, 10 et 12 TRUNK : port 11	Internal 2
30	ACCESS : port 13, 14 et 16 TRUNK : port 15	Internal 3
99	ACCESS : port 17, 18, 19, 20, 22, 23 et 24 TRUNK : port 21	Internal 4

Remarque : L'accès à l'administration du switch est sécurisé via le protocole SSH accessible depuis le VLAN 99-Management à l'adresse : 192.168.99.253/24.

2. Configuration du switch

Création des VLANs et sécurisation SSH

La première étape consiste à la création des VLANs et à configurer l'accès distant sécurisé pour l'administration. *(Illustration avec le VLAN 99)*

Création du VLAN de management

```
SW-Venus(config)# vlan 99
SW-Venus(config-vlan)# name Management
```

Configuration de l'IP de gestion

```
SW-Venus(config)# interface vlan 99
SW-Venus(config-if)# IP address 192.168.99.253 255.255.255.0
SW-Venus(config-if)# no shutdown
```

Activation du SSH (Accès distant sécurisé)

```
SW-Venus(config)# IP domain-name venus.local
SW-Venus(config)# crypto key generate rsa
```

Affectation des ports en access

```
SW-Venus(config)# interface range Gi1/0/5-6, Gi1/0/8
SW-Venus(config-if-range)# switchport mode access
SW-Venus(config-if-range)# switchport access vlan 10
SW-Venus(config-if-range)# no shutdown
```

Affectation des ports en trunk

```
SW-Venus(config)# interface Te1/0/21
SW-Venus(config-if)# switchport mode trunk
SW-Venus(config-if)# switchport trunk allowed vlan 99
```

La passerelle par défaut :

```
SW-Venus(config)# ip default-gateway 192.168.99.254
```

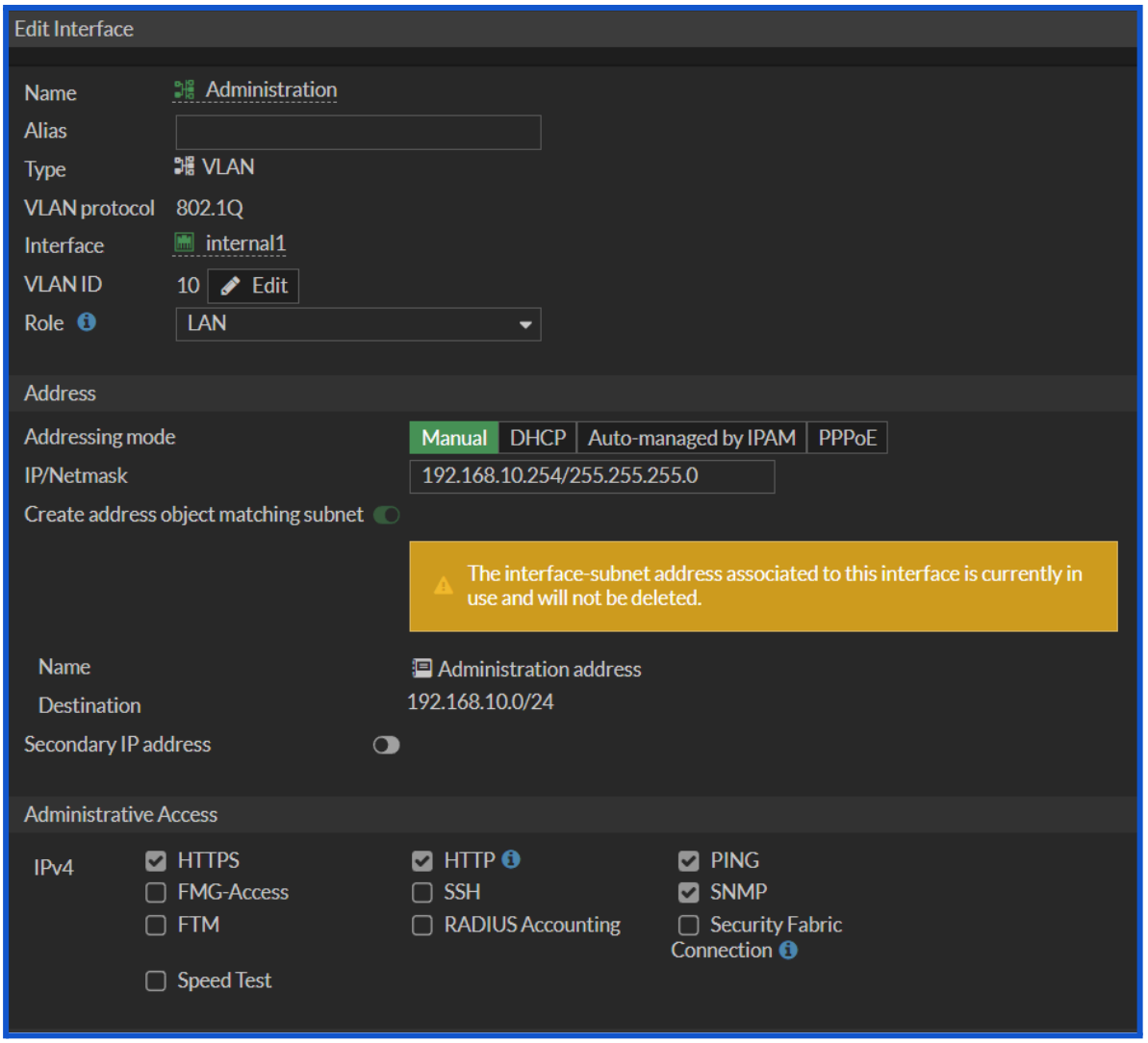
```
C:\Windows\System32>ssh admin@192.168.99.253
(admin@192.168.99.253) Password:



SW-Venus#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Administration                   active    Gi1/0/5, Gi1/0/6, Gi1/0/8
20   Direction                        active    Gi1/0/9, Gi1/0/10, Gi1/0/12
30   Wi-Fi                            active    Gi1/0/13, Gi1/0/14, Gi1/0/16
99   Management                       active    Te1/0/17, Te1/0/18, Te1/0/19, Te1/0/20, Te1/0/22, Te1/0/23, Te1/0/24
661  WAN-CCI                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW-Venus#
```

Récapitulatif des VLAN créés avec la commande : `SW-VENUS#show vlan brief`

3. Configuration du pare-feu Fortigate 60F

Interfaces logiques : Chaque VLAN dispose d'une sous-interface virtuelle sur le Fortigate (ex: Internal 1 = 192.168.10.254). Côté WAN, l'interface wan1 est configurée en 172.16.60.80/22 pour s'interconnecter au réseau de l'opérateur CCI.

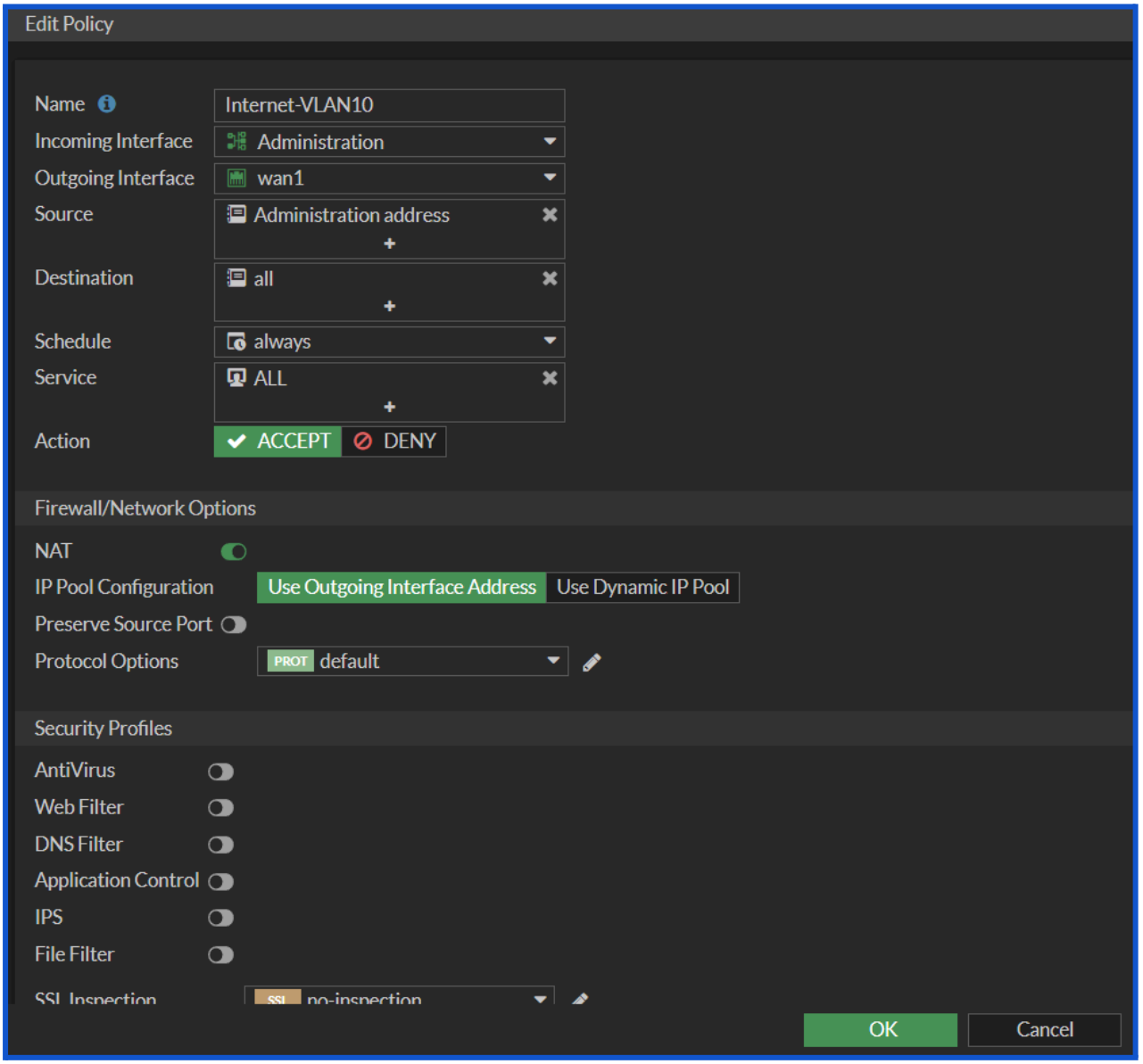
- `Interface internal 1 (VLAN 10) : 192.168.10.254/24`
- `Interface internal 2 (VLAN 20) : 192.168.20.254/24`
- `Interface internal 3 (VLAN 30) : 192.168.30.254/24`
- `Interface internal 4 (VLAN 99) : 192.168.99.254/24`



Exemple de création d'interface (VLAN 10)

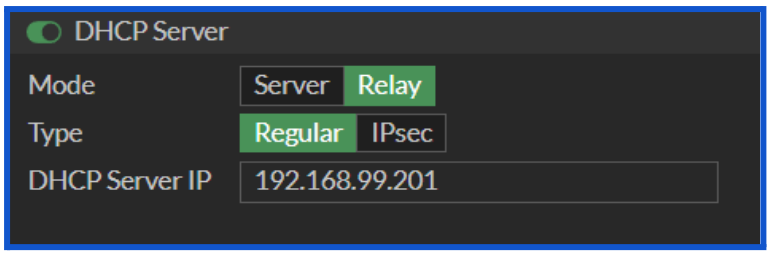
Stratégies de sécurité : Basées sur le principe du moindre privilège, des règles strictes de pare-feu et de NAT dynamique ont été créées pour n'autoriser que les flux de sortie légitimes vers Internet.

Source	Destination	Service	Action	NAT
Administration	WAN 1	All	Autorisé	Oui
Direction	WAN 1	All	Autorisé	Oui
Wi-Fi	WAN 1	All	Autorisé	Oui
Management	WAN 1	All	Autorisé	Oui



Exemple de création de règle autorisant la sortie vers Internet

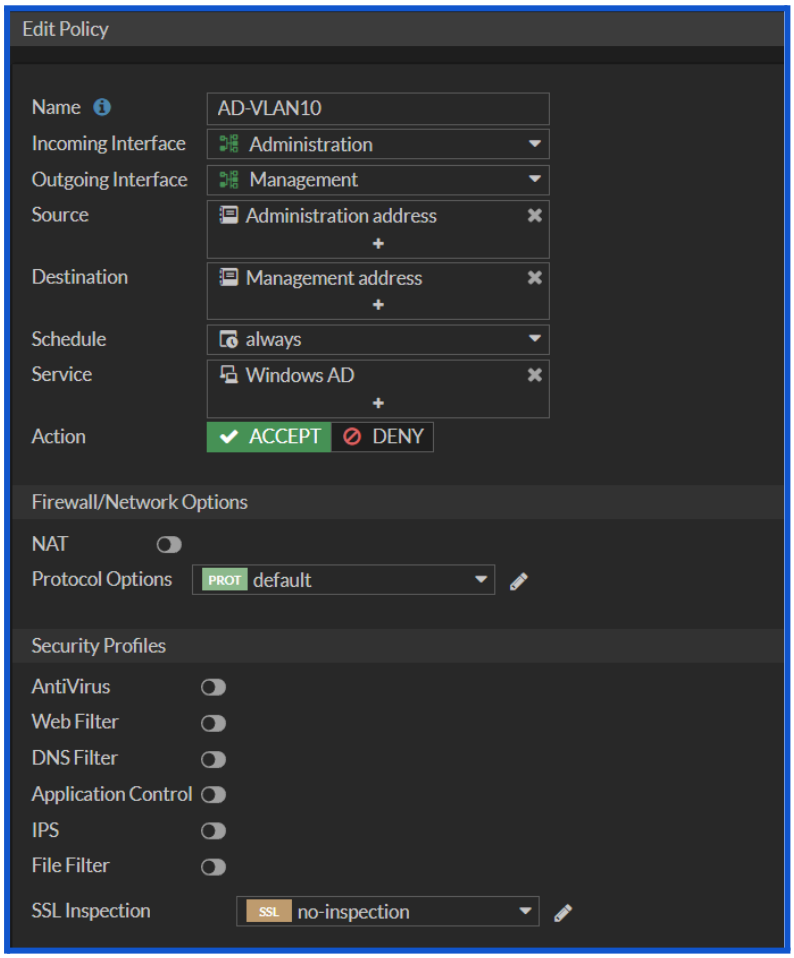
Configuration du relais DHCP (DHCP Relay) : Pour permettre aux terminaux d'obtenir une IP dynamique depuis le futur serveur Windows (192.168.99.201) situé dans le VLAN Management, des agents de relais DHCP ont été activés sur les sous-interfaces du FortiGate.



Activation du DHCP Relay et attribution de l'IP du serveur DHCP

Source	Destination	Service	Action	NAT
Administration	Management	Windows AD	Autorisé	Non
Direction	Management	Windows AD	Autorisé	Non
Wi-Fi	Management	Windows AD	Autorisé	Non
Management	Management	Windows AD	Autorisé	Non

Règles autorisant les flux provenant de l'Active Directory



Exemple de création de règle autorisant les service du contrôleur de domaine (AD)

4. Accès distant sécurisé

Pour administrer la baie Vénus à distance ou permettre le télétravail pour certains employés, des solutions VPN IPsec a été configuré *(ici illustré par le VLAN 10)*

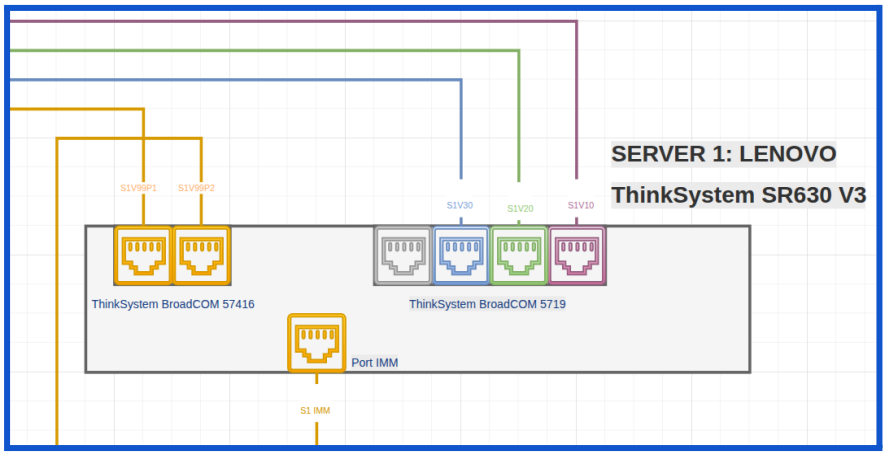
- Authentification : Sécurisation par clé pré-partagée (PSK) et restriction à un groupe d'utilisateurs dédié défini dans le pare-feu.
- Réseau IPsec : Les clients FortiClient reçoivent une IP dans la plage `192.168.110.1 - 192.168.110.10` et utilisent le futur serveur DNS interne `(192.168.99.201)`.
- Sécurité cryptographique : Pour éviter les conflits d'interfaces, un *Peer ID* personnalisé (`vpn-VLAN10`) a été défini. Le protocole d'échange de clés s'appuie sur un groupe Diffie-Hellman élevé (DH 20) pour les deux phases de négociation, garantissant une forte robustesse.

Note: Lorsque l'infrastructure sera opérationnelle et mise en production, les employés pourront se connecter via l'application Forti-Client VPN en configurant une nouvelle connexion correspondante à la configuration établie sur le FortiGate.

B. Mise en oeuvre de l'hyperviseur

1. Configuration réseau de l'hyperviseur

Pour exploiter les six cartes réseaux disponibles par serveur, le routage virtuel de Proxmox s'appuie sur des ponts Linux (Linux Bridges). Chaque pont attache virtuellement une interface réseau physique à un VLAN du commutateur Cisco.



Légende :
S1V10 - Serveur 1 VLAN 10
S1V20 - Serveur 1 VLAN 20
S1V30 - Serveur 1 VLAN 30
S1V99P1 - Serveur 1 VLAN 99 Patte 1
S1V99P2 - Serveur 1 VLAN 99 Patte 1 *(pour cluster)*
S1 IMM - Serveur 1 IMM *(port Management du serveur Lenovo)*
Note: Branchement et configuration identique sur le 2ème serveur

Interface Physique	Bridge Linux	VLAN	Adresse IP/CIDR
ens6f0np0	vmbr0	VLAN 99	192.168.99.211/24
ens6f1np1	vmbr1	VLAN 99 (lien cluster)	192.168.99.212/24
ens2f0	vmbr2	VLAN 10	192.168.10.211/24
ens2f1	vmbr3	VLAN 20	192.168.20.211/24
ens2f2	vmbr4	VLAN 30	192.168.30.211/24

2. Création et intégration du cluster Proxmox

Afin de centraliser l'administration et de répondre aux exigences de continuité de service, les deux serveurs physiques ont été regroupés au sein d'un cluster (grappe de serveurs) nommé "Venus".

L'initialisation a été réalisée sur le premier serveur (Venus01). Lors de la création de la grappe, l'interface réseau 192.168.99.211 a été explicitement assignée. Ce paramétrage est essentiel : il permet de dédier un lien physique unique à la communication entre les serveurs, évitant ainsi de saturer le réseau de production des machines virtuelles.

Une fois le cluster actif sur le premier nœud, l'interface Proxmox a généré une clé de jonction sécurisée. Sur le second serveur (Venus02), il suffit d'utiliser l'option "Rejoindre la grappe de serveurs", d'y coller cette clé et de s'authentifier avec le compte administrateur du nœud principal. Après une brève synchronisation des nœuds, le serveur a intégré la grappe avec succès.

Résultat : Les deux serveurs sont désormais parfaitement synchronisés et administrables depuis une interface web unique. En cas de panne matérielle sur l'un des serveurs, cette configuration unifiée permet de restaurer et de redémarrer très rapidement les machines virtuelles sur le serveur restant, garantissant ainsi la continuité de service.

*Note : L'infrastructure Vénus disposant de deux serveurs physiques Lenovo (et non du minimum de 3 nœuds requis pour un basculement automatique), ce cluster a été mis en place comme un **cluster de management**. Son objectif principal est de centraliser l'administration sur une seule interface web et de permettre le rétablissement des machines virtuelles en cas de panne matérielle.*

VII] ARTICULATION AVEC L'ÉQUIPE SYSTÈME ET MISE À DISPOSITION DE L'INFRASTRUCTURE

La mise en œuvre de la Baie Vénus a permis de livrer un environnement matériel, réseau et virtualisé pleinement opérationnel. Mon intervention, dans le cadre de ce premier projet, s'est concentrée sur la fondation de l'infrastructure : le câblage, la segmentation réseau, la sécurisation périmétrique, le déploiement de Proxmox et la création du cluster de management.

Je fais également partie de l'équipe système dans le cadre de travaux complémentaires menés sur cette même infrastructure. Toutefois, pour respecter le périmètre strict de ce dossier de conception, seuls les éléments relevant de la réalisation matérielle et réseau sont détaillés ici.

Les opérations logicielles qui en ont découlé — telles que le déploiement des machines virtuelles Windows Server (Active Directory, DNS, DHCP,SMB), l'installation de la supervision (Centreon),de la solution de gestion de parc et ticketing (GLPI) et solutions de sauvegardes (Bacula) — pourront être réalisées avec succès par l'équipe système, en s'appuyant directement sur la base technique que j'ai préparée (relais DHCP configurés, VLANs routés, règles de flux pré-établies).

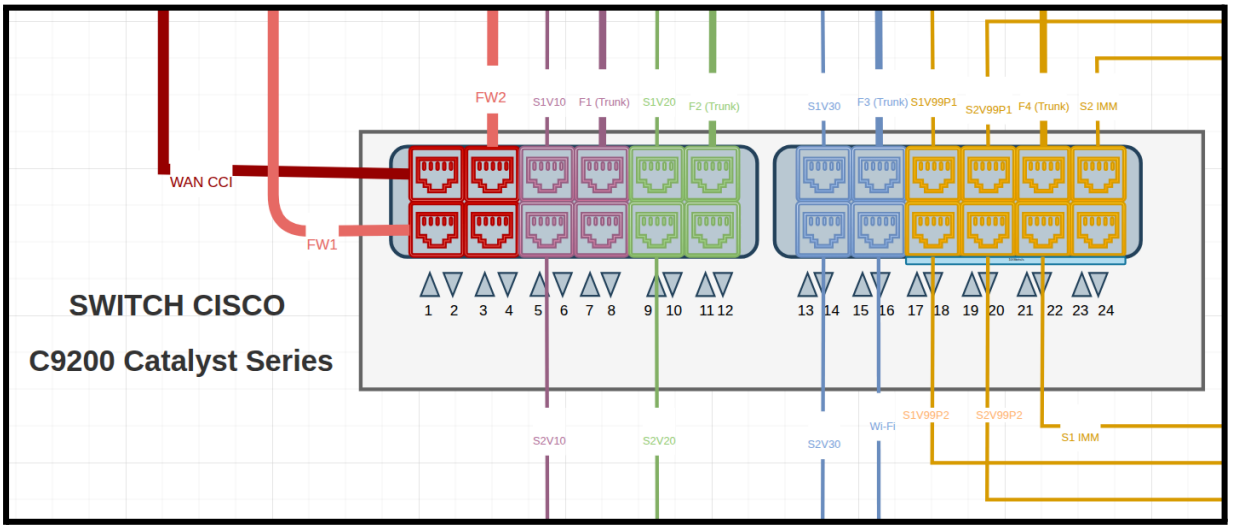
Enfin, cette architecture cloisonnée, surveillée et administrable à distance a été spécifiquement pensée pour accueillir mon second projet professionnel : le déploiement futur d'un Système de Détection d'Intrusion Réseau (NIDS) destiné à analyser les flux malveillants au sein de l'agence.

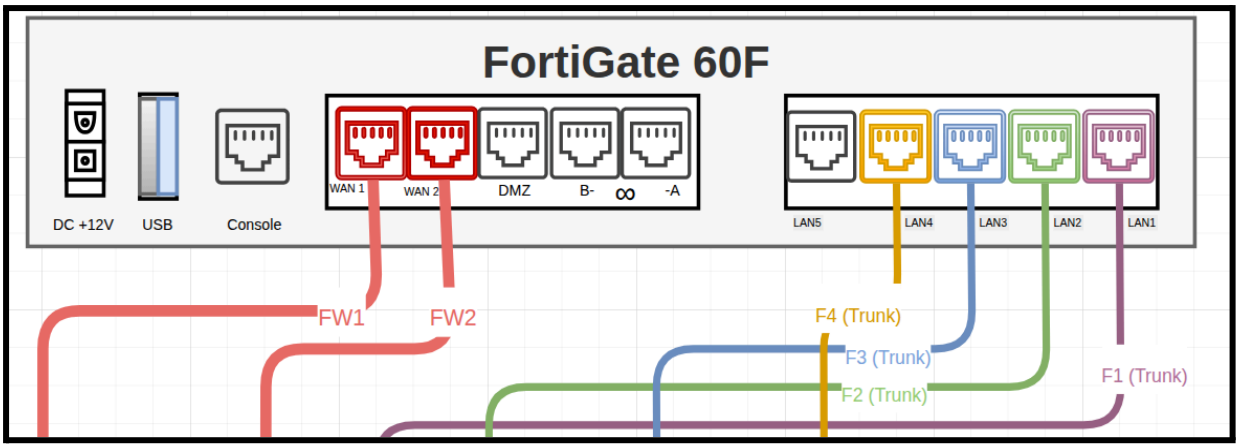
VIII] CONCLUSION

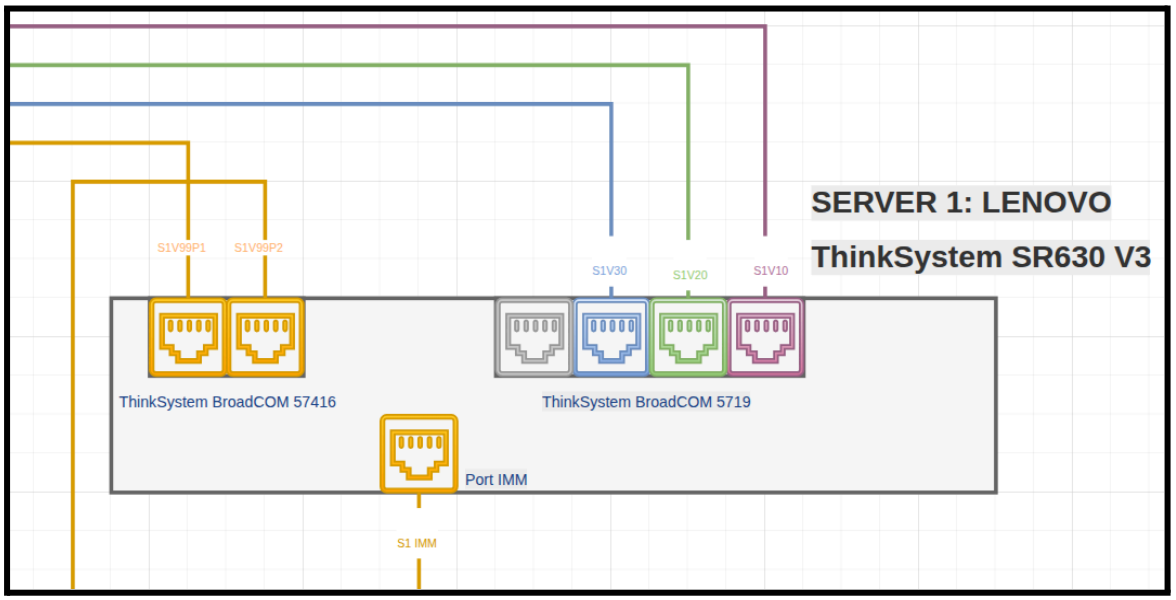
Ce projet a permis de concevoir et de déployer avec succès une infrastructure virtualisée et sécurisée, bâtie de zéro pour répondre aux exigences de la première agence physique de A.D.N Services.
La solution repose sur une architecture segmentée robuste, où le commutateur Cisco centralise la distribution et où le pare-feu FortiGate assure un contrôle intransigeant du routage, du filtrage et des accès distants. Le choix d'un environnement Proxmox permet de concilier une administration centralisée performante et une préparation optimale à la continuité de service, tout en maîtrisant les coûts logiciels.
La mise en production de la baie Vénus démontre qu'il est possible de fournir à une agence une autonomie technique complète, sécurisée et évolutive. Ce socle offre aujourd'hui à A.D.N Services une base stable, prête à supporter le développement de ses activités, le déploiement futur des services d'infrastructure ainsi que différents outils de gestion, de supervision, de sauvegarde et de cybersécurité.

IX] ANNEXES

- Annexe A : Schéma physique détaillé du câblage

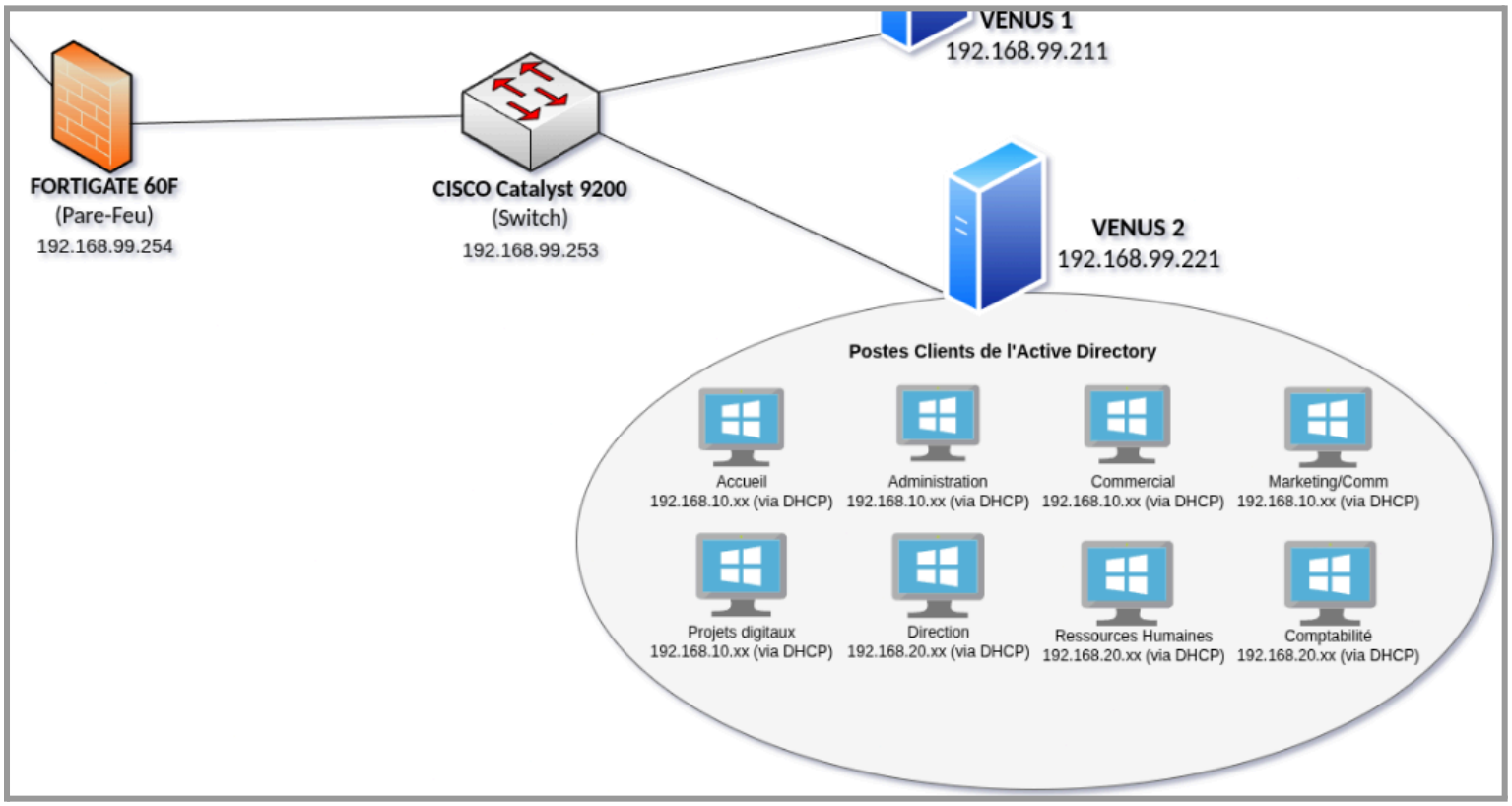


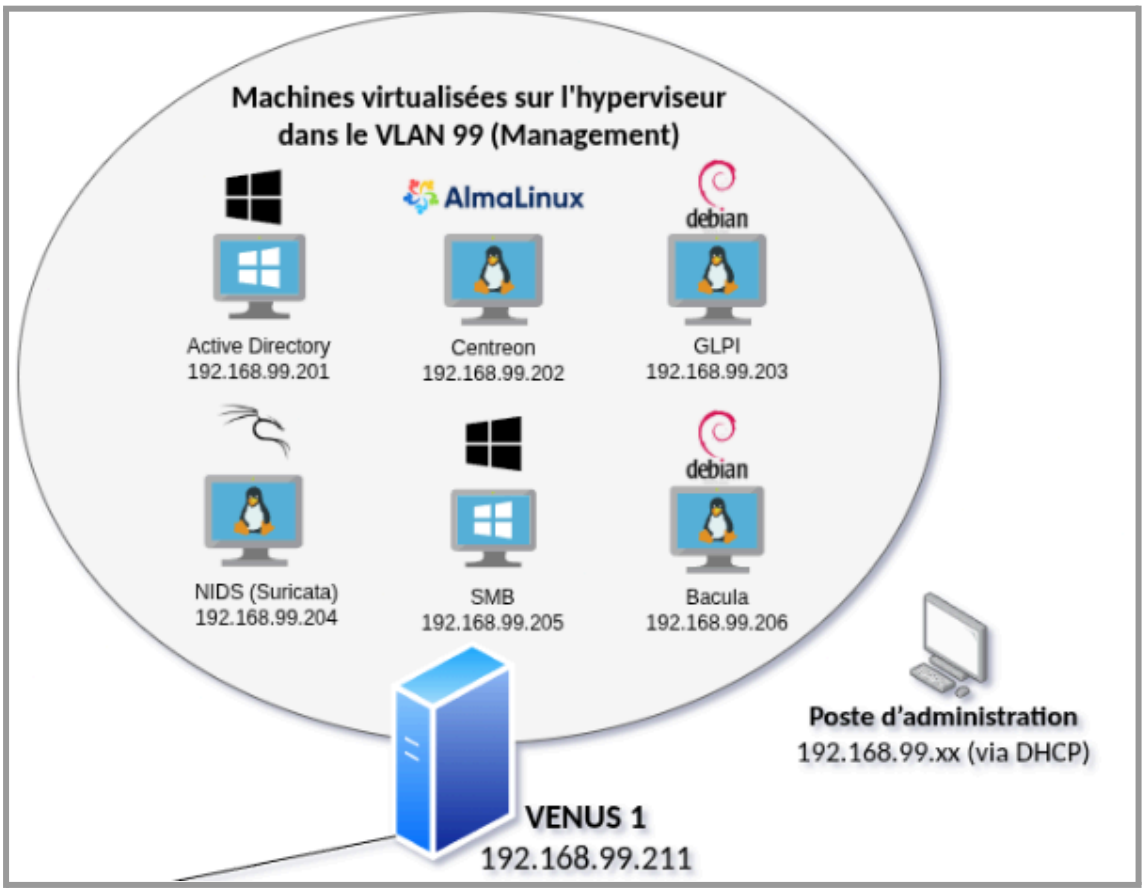




Configuration identique sur les deux serveurs

- Annexe B : Schéma logique détaillé





- Annexe C : Captures de la configuration des règles, du NAT et du VPN IPsec sur le FortiGate

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
				HTTPS Security Fabric Connection			
internal1	Physical Interface		0.0.0.0/0.0.0.0				1
Administration	VLAN		192.168.10.254/255.255.255.0	PING HTTPS SNMP HTTP		Relay: 192.168.99.201	4
internal2	Physical Interface		0.0.0.0/0.0.0.0				1
DIRECTION	VLAN		192.168.20.254/255.255.255.0	PING HTTPS SNMP HTTP		Relay: 192.168.99.201	3
internal3	Physical Interface		0.0.0.0/0.0.0.0				1
Wi-Fi	VLAN		192.168.30.254/255.255.255.0	PING HTTPS SNMP HTTP		Relay: 192.168.99.201	3
internal4	Physical Interface		0.0.0.0/0.0.0.0				1
Management	VLAN		192.168.99.254/255.255.255.0	PING HTTPS SSH SNMP HTTP		Relay: 192.168.99.201	6

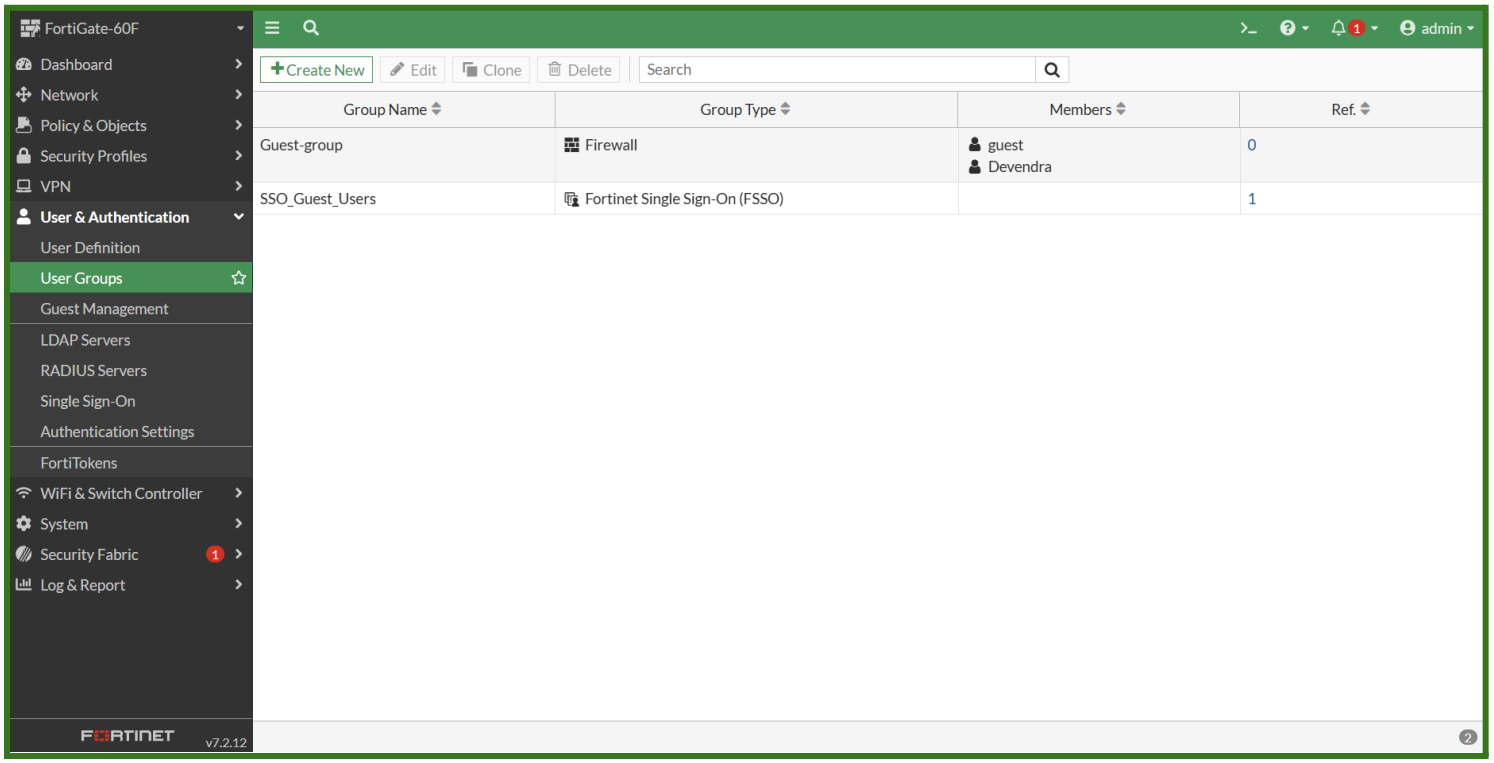
Vue d'ensemble des interfaces configurées sur le FortiGate.

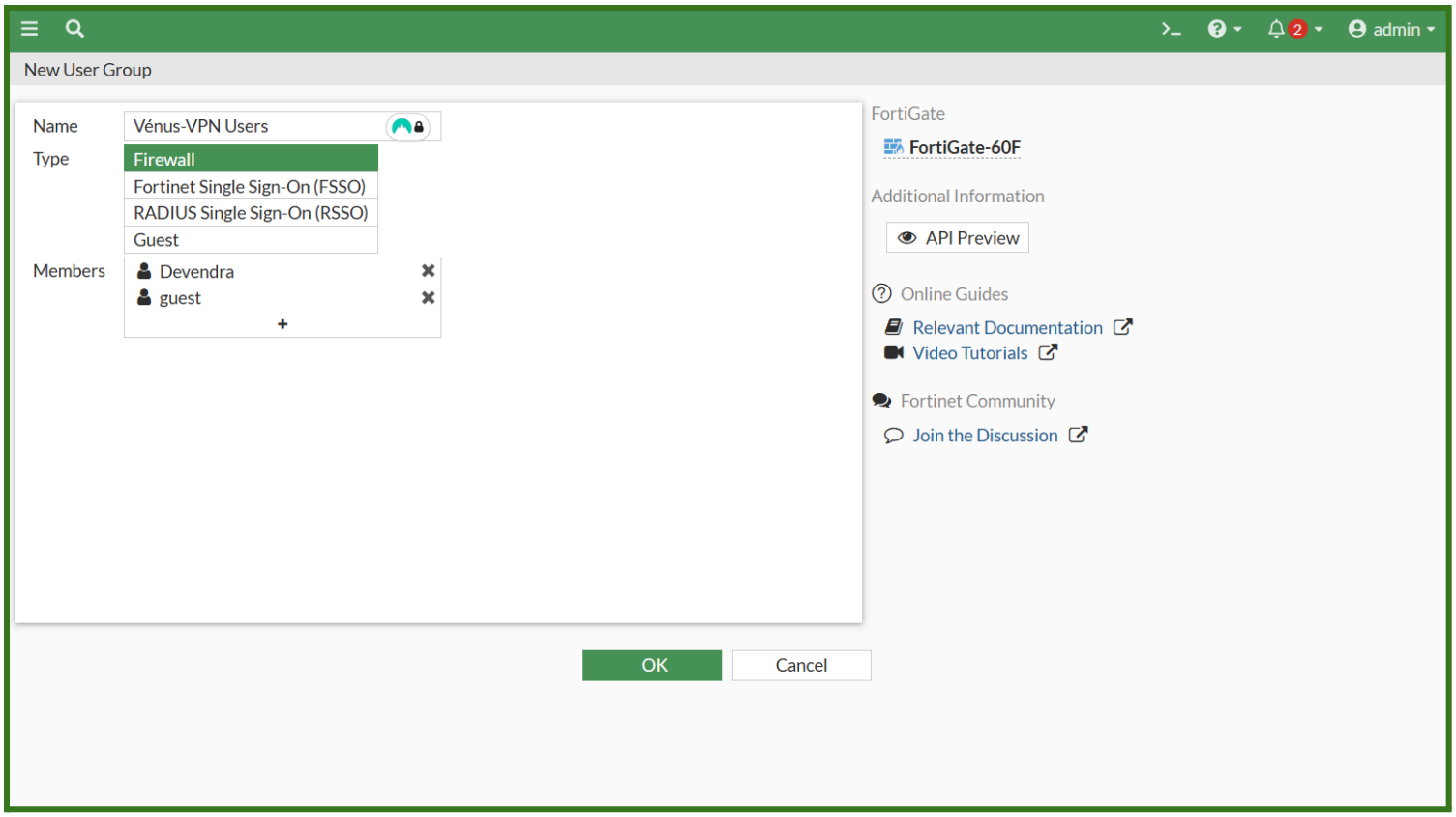
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
Administration → Management 1										
AD-VLAN10	Administration address	Management address	always	Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	399.29 kB	Standard
Administration → wan1 1										
Internet-VLAN10	Administration address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
DIRECTION → Management 1										
AD-VLAN20	DIRECTION address	Management address	always	Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	0 B	Standard
DIRECTION → wan1 1										
Internet-VLAN20	DIRECTION address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Management → wan1 1										
Internet-VLAN99	Management address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	36.42 MB	Standard
Venus-VPN → Management 1										
vpn_Venus-VPN_remote_0	Venus-VPN_range	Management address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	194.06 MB	Standard
VPN-VLAN10 → Administration 1										
vpn_VPN-VLAN10_remote_0	VPN-VLAN10_range	Administration address	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Wi-Fi → Management 1										
AD-VLAN30	Wi-Fi address	Management address	always	Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	0 B	Standard
Wi-Fi → wan1 1										
Internet-VLAN30	Wi-Fi address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Implicit 1										

Vue de la table de filtrage complète synthétisant l'ensemble des flux autorisés sur l'infrastructure Vénus.

Accès distant sécurisé (VPN IPsec)

1. Création du groupe d'utilisateurs



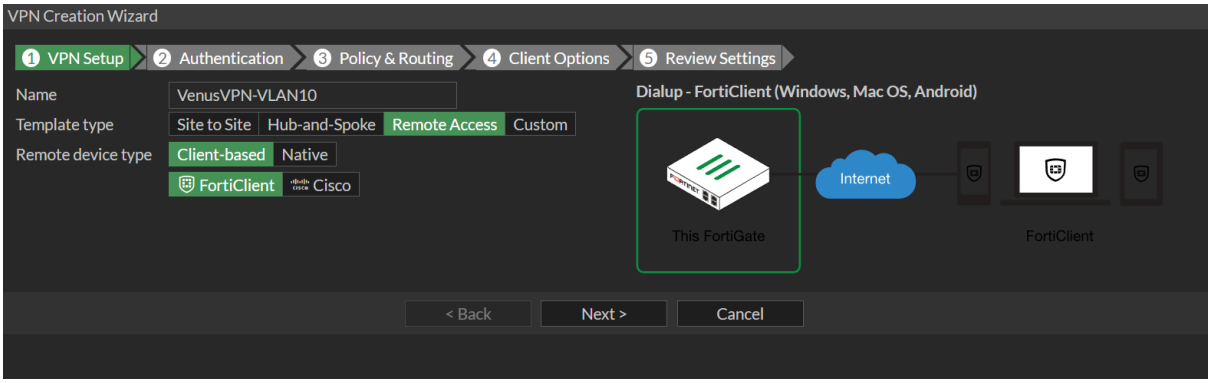


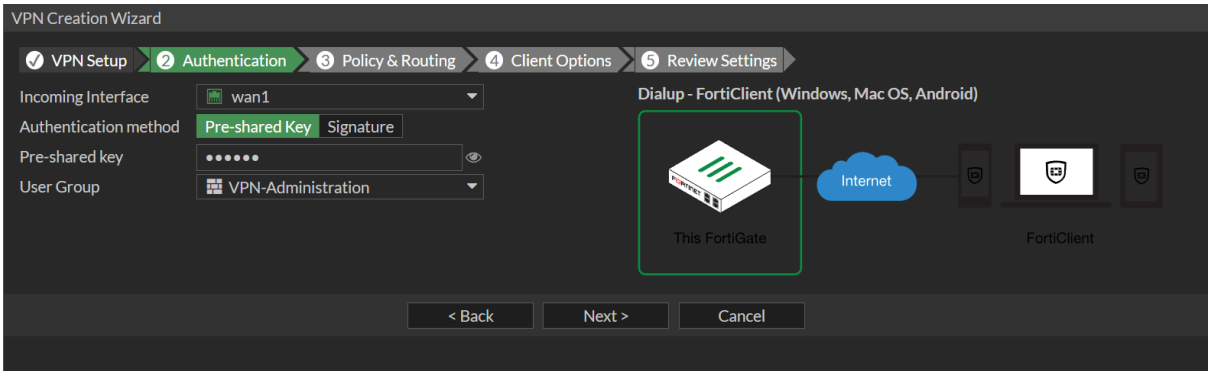
admin

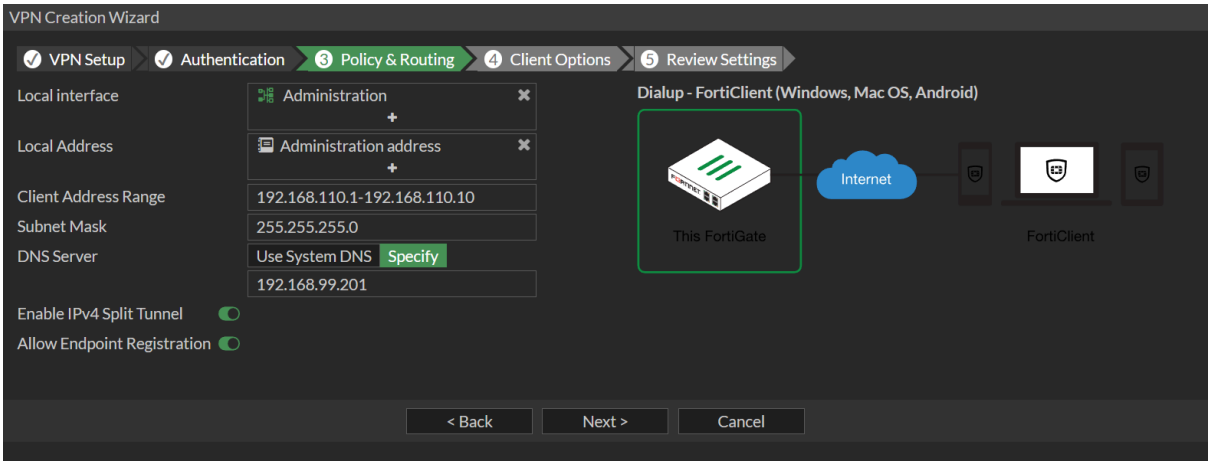
Create New | Edit | Clone | Delete | Search

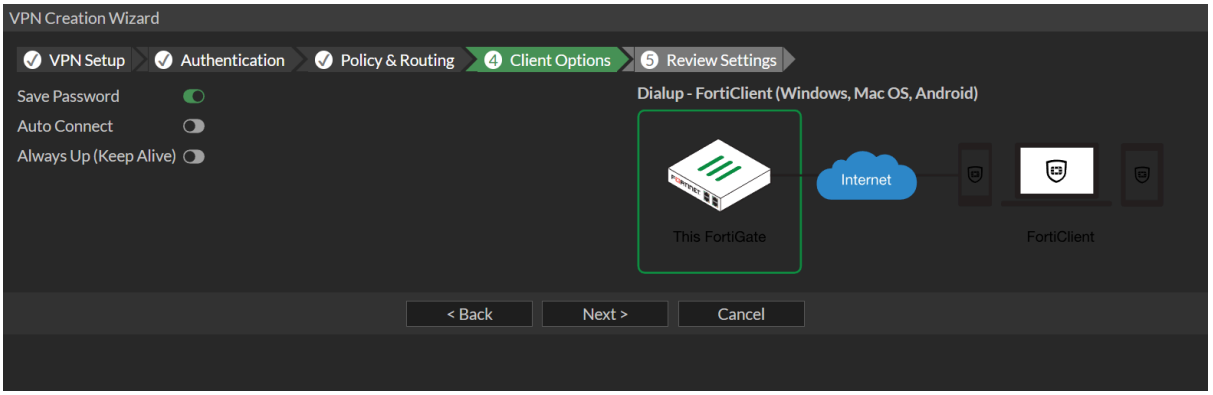
Group Name	Group Type	Members	Ref.
Guest-group	Firewall	guest Devendra	0
Vénus-VPN Users	Firewall	Devendra guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

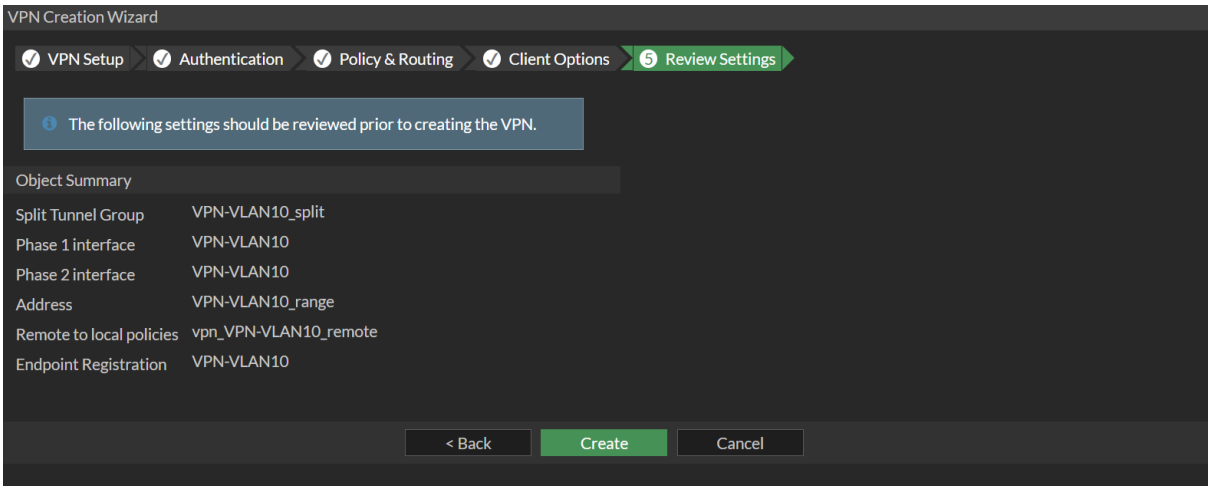
2. Configuration du tunnel IPsec



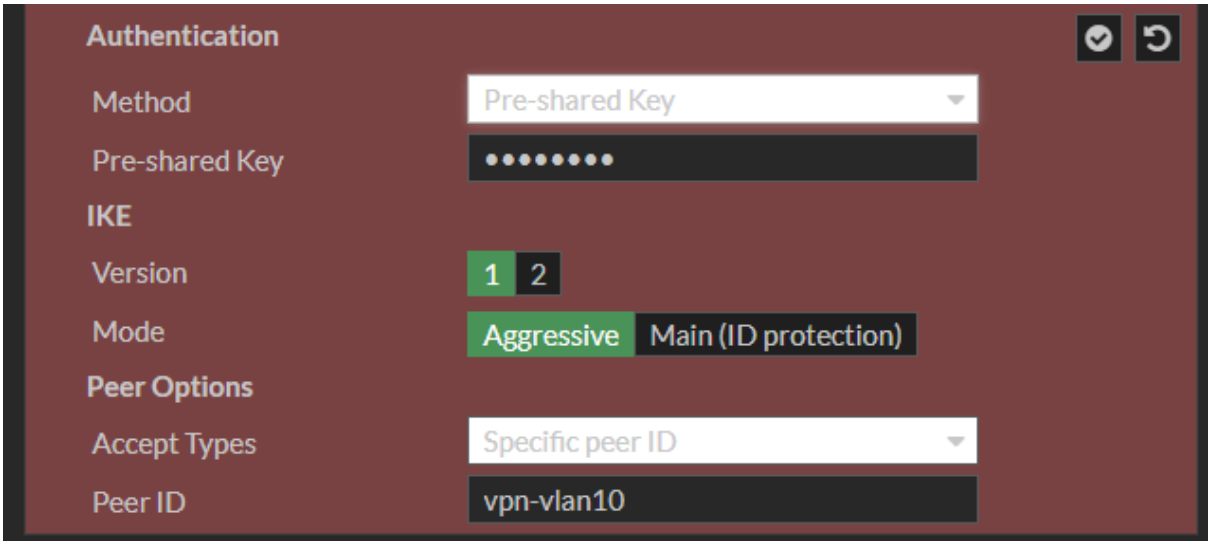




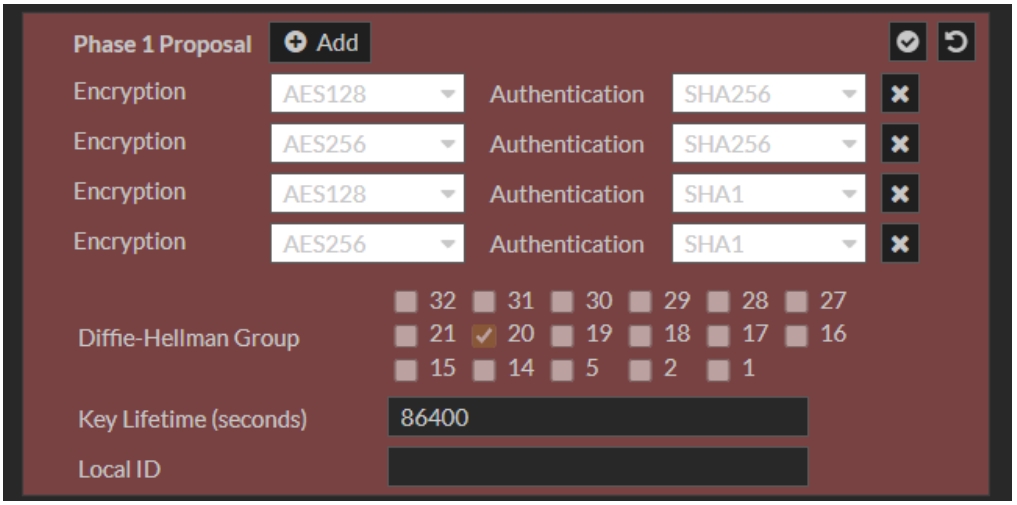


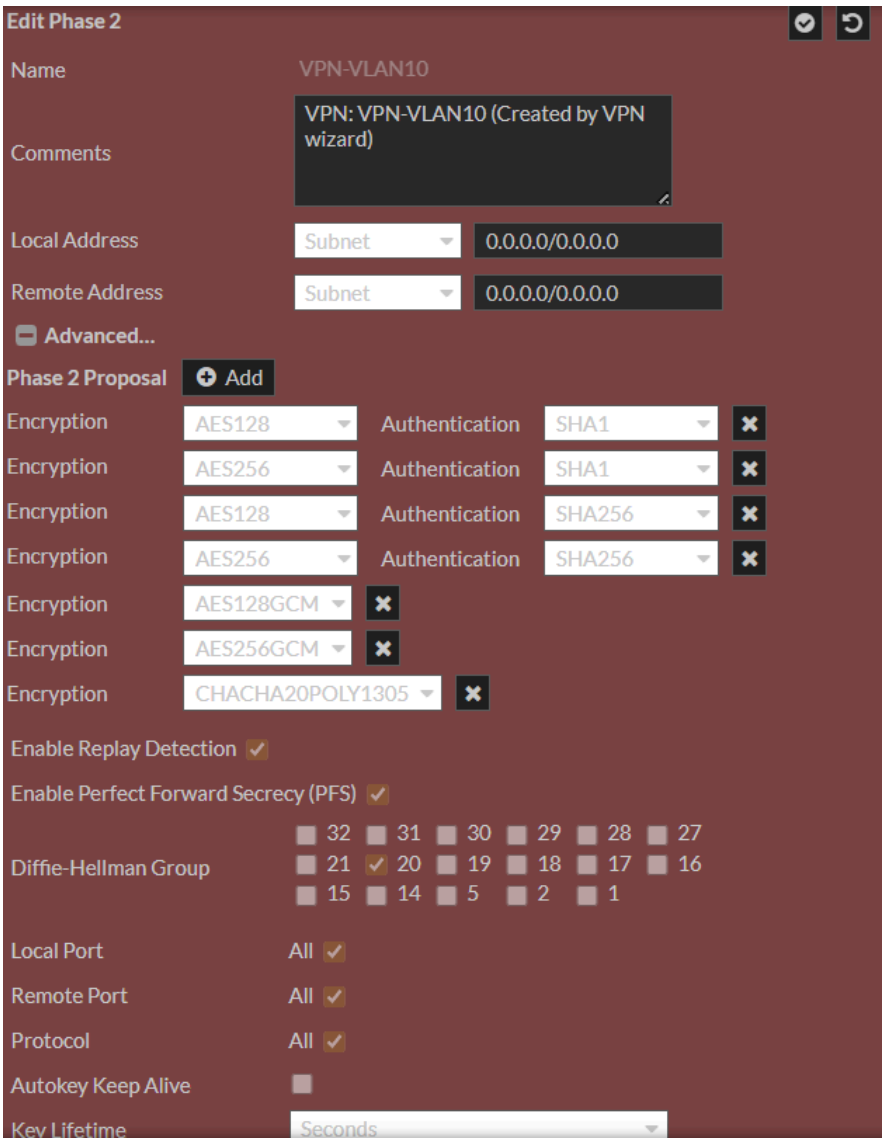


Passage en mode Custom



Ajout du Peer ID (ID du VPN)

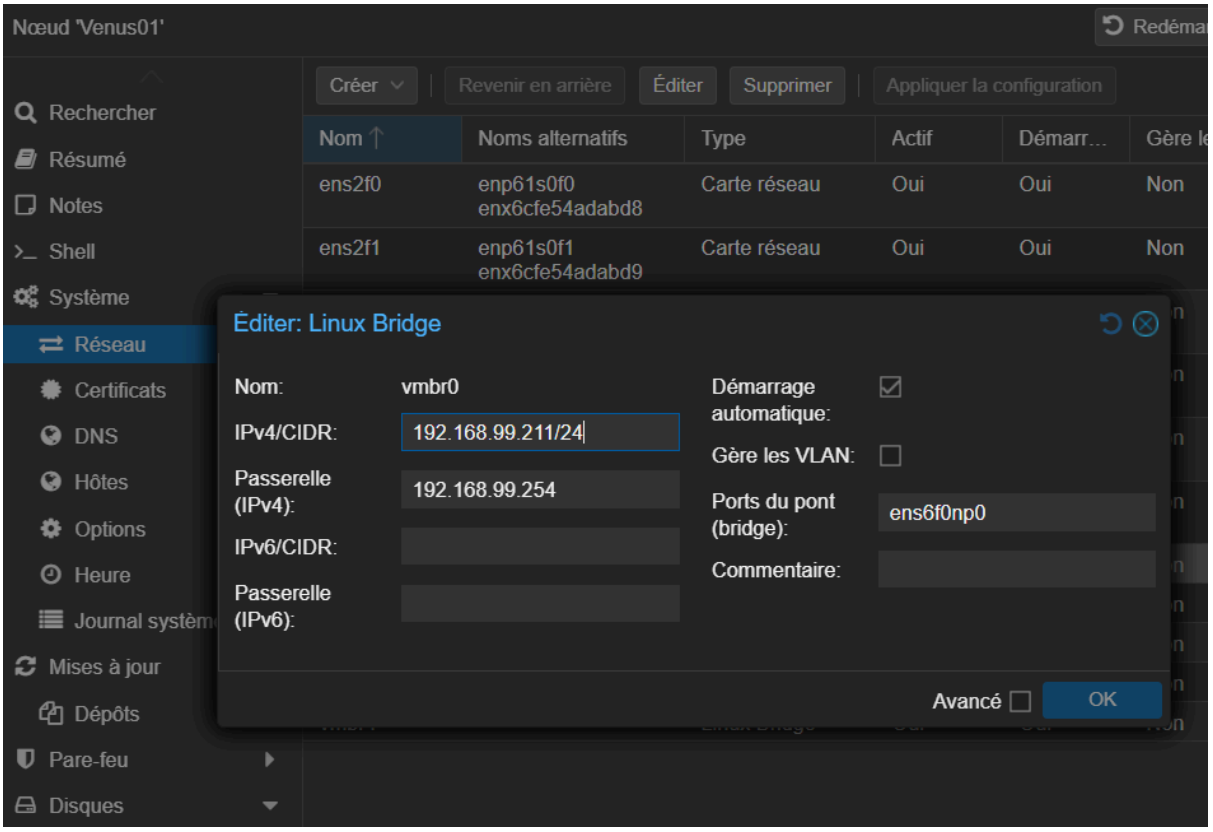


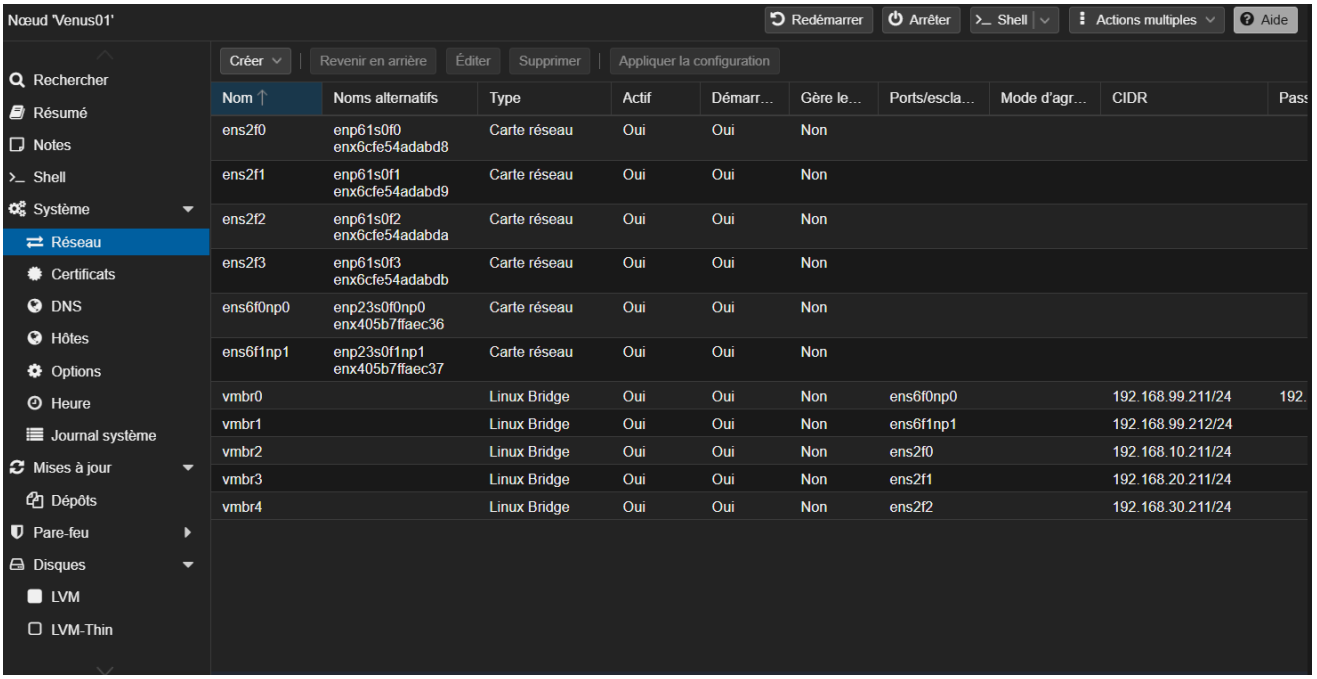


Configuration du DH Group des phase 1 et 2

- Annexe D : Captures de la configuration des Linux Bridges et des interfaces réseaux sur Proxmox

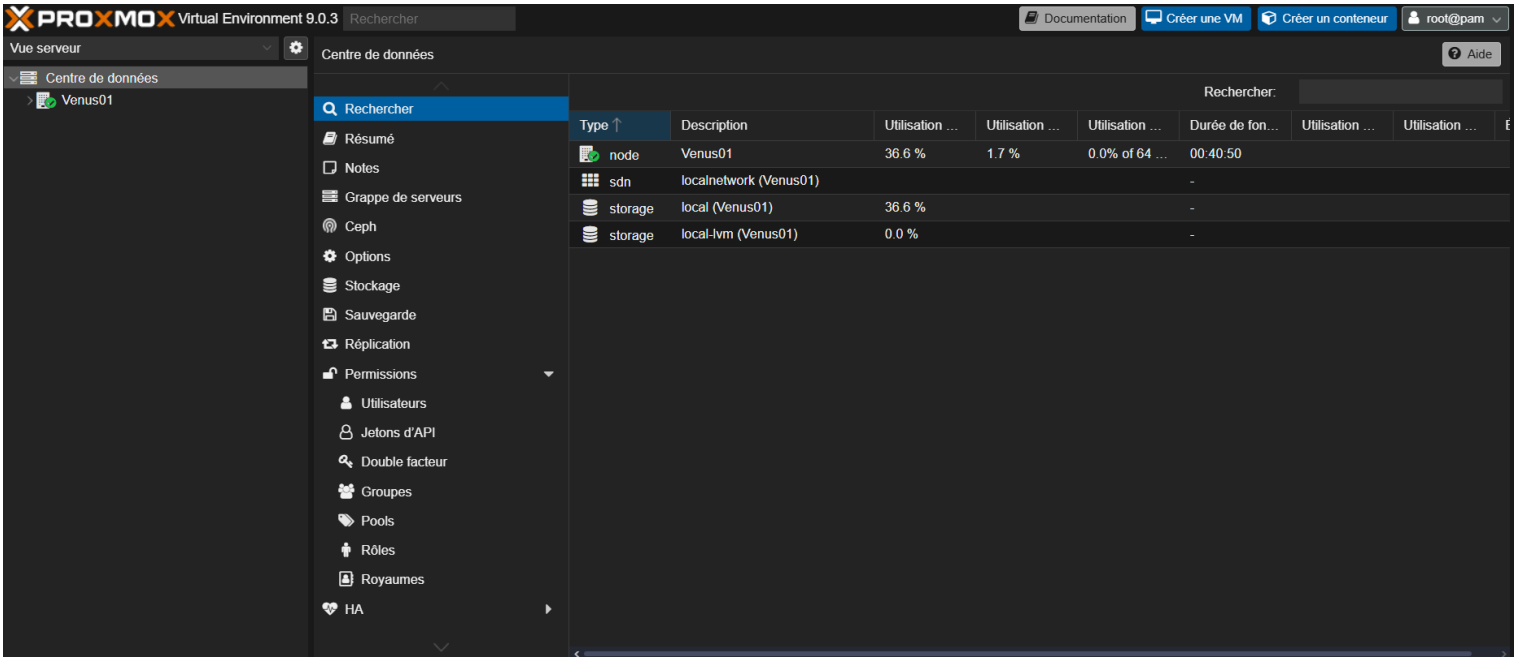
Création des Linux Bridge

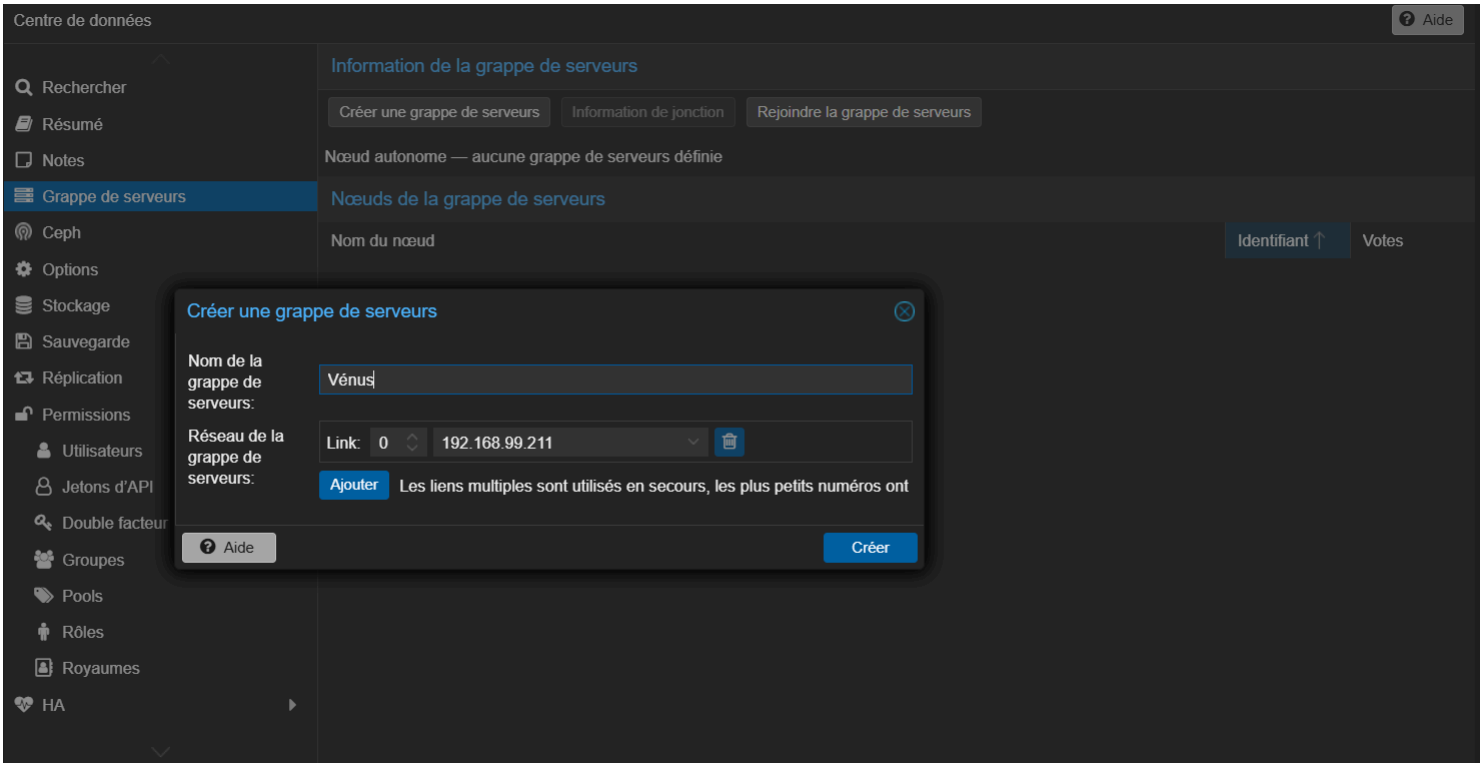


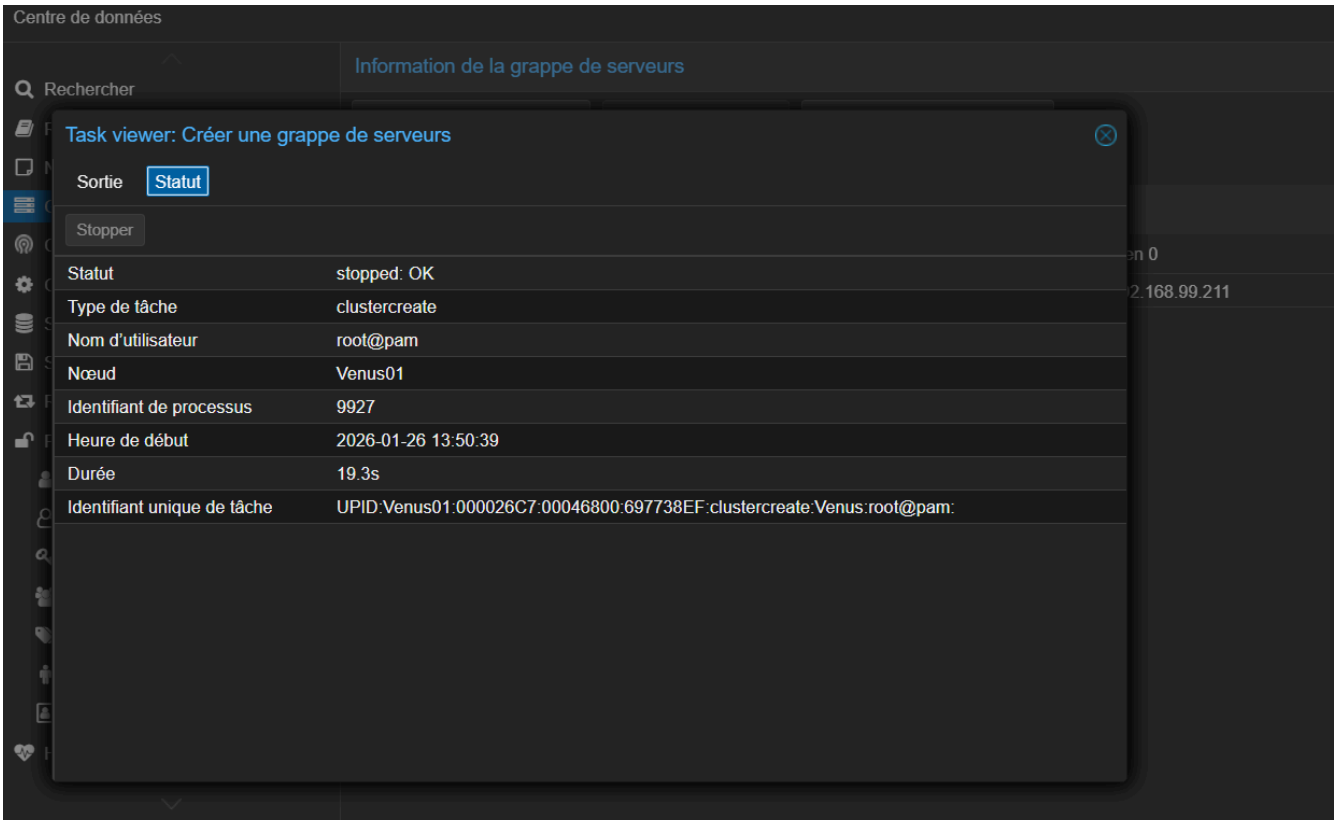


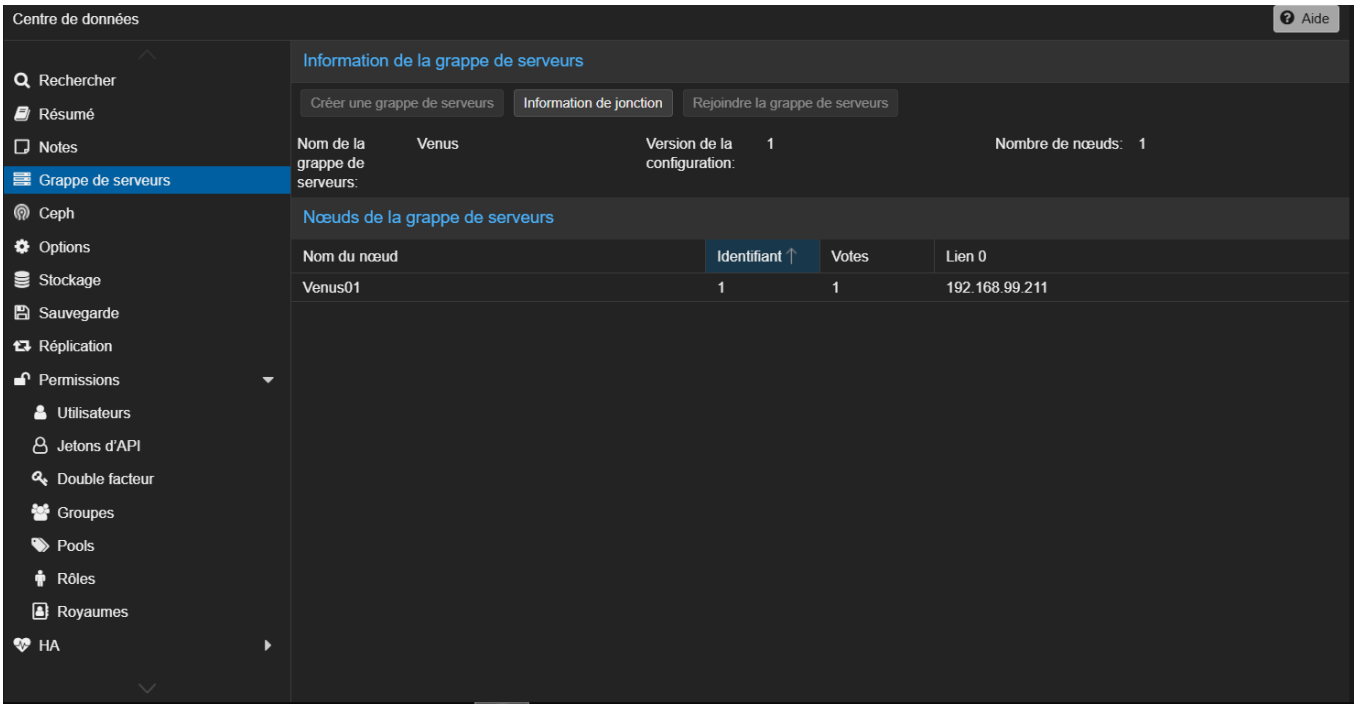
Création du cluster de Management

1ère partie sur Vénus01 :

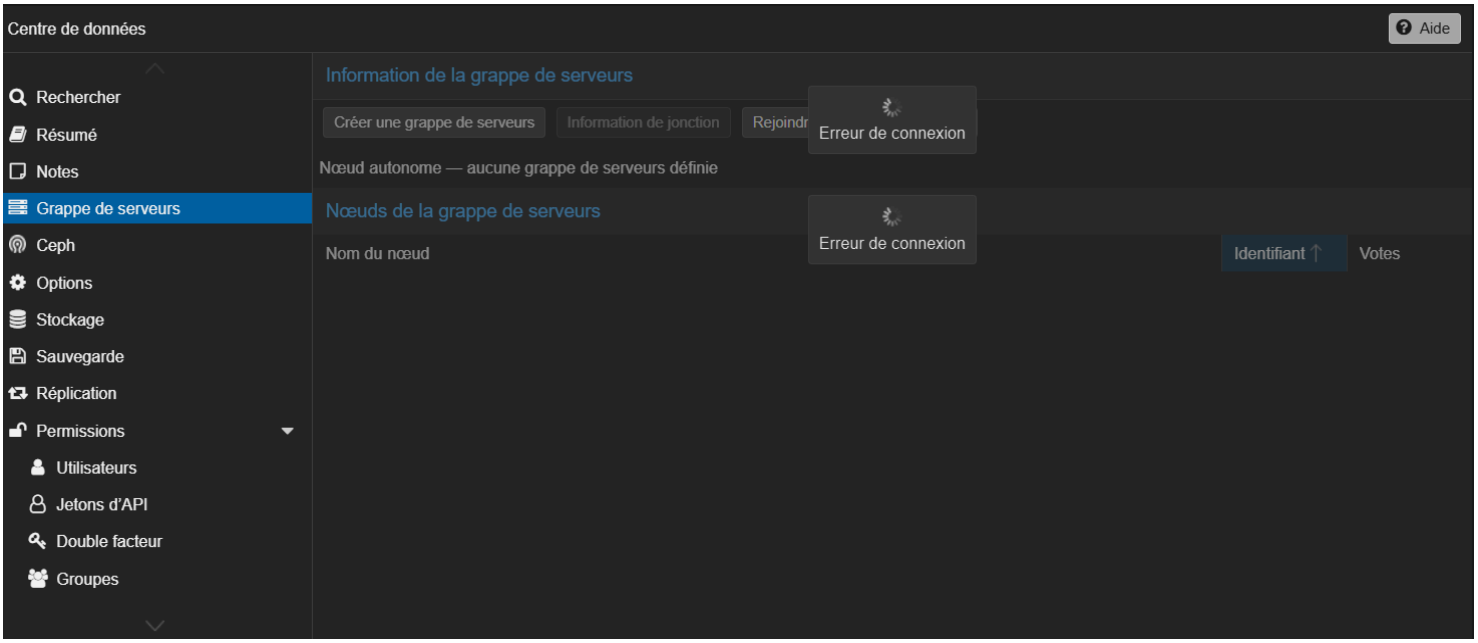


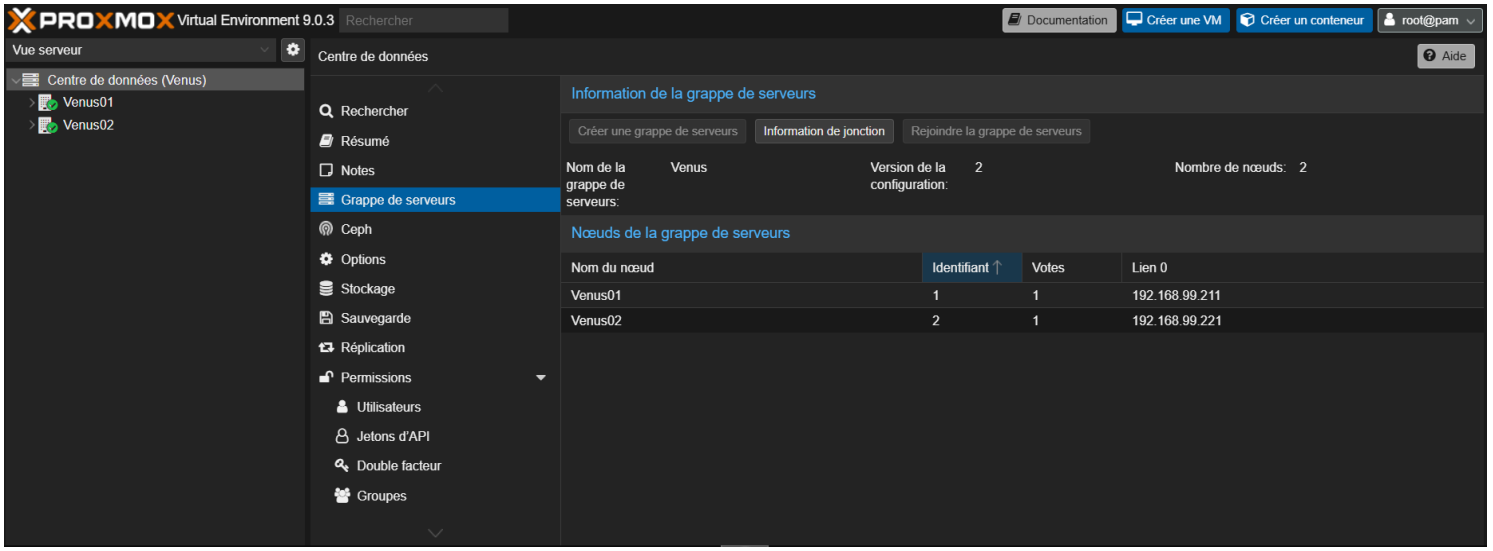



Centre de données
Information de la grappe de serveurs
Rechercher
Task viewer: Créer une grappe de serveurs
Sortie
Statut
Stopper
Statut stopped: OK
Type de tâche clustercreate
Nom d'utilisateur root@pam
Nœud Venus01
Identifiant de processus 9927
Heure de début 2026-01-26 13:50:39
Durée 19.3s
Identifiant unique de tâche UPID:Venus01:000026C7:00046800:697738EF:clustercreate:Venus:root@pam:


Centre de données
Aide
Rechercher
Résumé
Notes
Grappe de serveurs
Ceph
Options
Stockage
Sauvegarde
Réplication
Permissions
Utilisateurs
Jetons d'API
Double facteur
Groupes
Pools
Rôles
Royaumes
HA
Information de la grappe de serveurs
Créer une grappe de serveurs
Information de jonction
Rejoindre la grappe de serveurs
Nom de la grappe de serveurs: Venus
Version de la configuration: 1
Nombre de nœuds: 1
Nœuds de la grappe de serveurs
Nom du nœud
Identifiant
Votes
Lien 0
Venus01
1
1
192.168.99.211

2nde partie sur Vénus02:





Note: Les captures contenant les clés d'appairage du cluster Proxmox (et les mots de passe)ont été volontairement exclues de la documentation. Dans une démarche de cybersécurité (Moindre privilège), les informations cryptographiques ou d'authentification ne doivent jamais figurer en clair dans la documentation technique d'une entreprise pour éviter toute fuite de données (Data Leak)."