DOSSIER TECHNIQUE E6 - PROJET 1

Conception
de l'infrastructure Vénus

Présenté par : **Allan Brennus**
BTS SIO (Option SISR)
Session 2026

TABLE DES MATIÈRES

1. Présentation du Contexte et Enjeux

1.1 Le projet de l'entreprise

Dans le cadre de ma formation en Brevet de Technicien Supérieur aux Services Informatiques aux Organisations (BTS SIO) avec l'option Solutions d'Infrastructure, Systèmes et Réseaux (SISR), j'ai eu l'opportunité de prendre en charge un projet d'envergure. J'ai été missionné pour concevoir, déployer de A à Z, et documenter l'infrastructure informatique complète de la SARL Fantôme.

Cette entreprise nécessitait une refonte et la mise en place d'une infrastructure réseau locale connectée sur le WAN CCIR. Cette création d'agence impliquait la conception d'une architecture robuste, capable de soutenir les activités quotidiennes et d'assurer un cloisonnement strict.

1.2 Les enjeux de l'infrastructure Vénus

Le projet, identifié sous le nom de code "Vénus" et lié au domaine interne "venus.local", portait des enjeux majeurs. Il s'agit de confectionner une baie de brassage hautement fonctionnelle, sécurisée contre les menaces externes, et surtout évolutive pour l'avenir.

2. Analyse approfondie des Besoins et Contraintes

2.1 Besoins Fonctionnels Exprimés

- Haute disponibilité (High Availability) : Les services critiques, tels que l'Active Directory, la messagerie et les futures applications métiers, doivent être disponibles en permanence. L'infrastructure doit donc intégrer une tolérance aux pannes matérielles (redondance).
- Segmentation réseau stricte : Pour des raisons évidentes de sécurité informatique et d'optimisation des performances de la bande passante, les différents profils d'utilisateurs (Administration, Direction, Invités Wi-Fi, Service IT) doivent être isolés logiquement.
- Administration distante : Les équipes de support informatique ne seront pas toujours sur place. Il est donc indispensable de pouvoir intervenir à distance sur les équipements réseau et les serveurs, de manière totalement chiffrée via un réseau privé virtuel (VPN).
- Préparation à l'observabilité : L'architecture réseau devait être pensée dès sa conception pour pouvoir accueillir très rapidement des solutions de gestion de parc informatique (GLPI) et de supervision proactive (Centreon).

2.2 Contraintes du projet

- Optimisation budgétaire : Privilégier systématiquement les solutions logicielles open-source de qualité entreprise (Proxmox, Centreon, GLPI, Linux) afin de réduire les coûts liés aux licences logicielles, permettant ainsi d'investir le budget dans du matériel de très haute qualité.
- Délai de mise en œuvre : L'infrastructure devait être totalement opérationnelle en moins de 6 semaines pour permettre l'ouverture de l'agence dans les temps.

3. Étude des Caractéristiques Techniques du Matériel

Afin de répondre à ces exigences, j'ai sélectionné et installé du matériel professionnel de niveau entreprise. Voici le détail de chaque équipement déployé dans la baie de brassage Vénus.

3.1 Les Serveurs : Lenovo ThinkSystem SR630 V3

J'ai choisi de déployer deux serveurs rack Lenovo ThinkSystem SR630 V3. Ces serveurs de format 1U offrent un excellent compromis entre puissance de calcul, densité dans la baie et fiabilité matérielle.

Caractéristiques matérielles poussées :

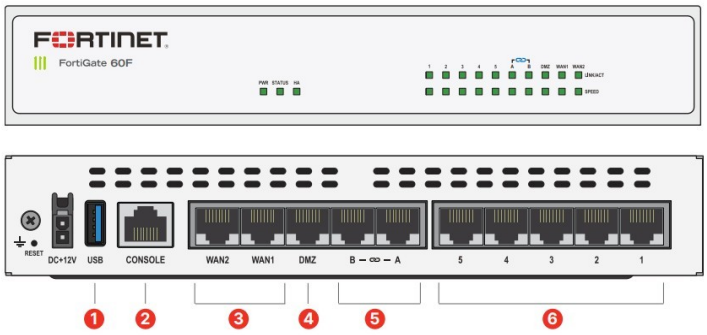
- Processeur : Intel Xeon Scalable de 3ème génération (Garantissant des performances multitâches extrêmes).
- Mémoire Vive (RAM) : 128 Go de RAM DDR4 ECC par serveur, évolutif jusqu'à 512 Go pour anticiper la croissance.
- Stockage : 4 baies de disques SAS/SATA "Hot-Plug" (remplaçables à chaud) en façade, gérés par un contrôleur RAID matériel doté d'une batterie de sauvegarde (BBU).
- Gestion hors-bande : Contrôleur Lenovo XClarity (IMM2) avec un port réseau totalement dédié, permettant de démarrer ou dépanner le serveur.
- Alimentation : Double bloc d'alimentation redondant (Hot-plug) pour pallier une coupure électrique sur l'un des circuits.

3.2 Le Pare-feu Périmétrique : Fortinet FortiGate 60F

Le FortiGate 60F est l'équipement de sécurité de nouvelle génération (NGFW) qui assure la sécurité périmétrique complète de l'agence Vénus de la SARL Fantôme, ainsi que le routage complexe entre les différents sous-réseaux.

Caractéristiques de sécurité :

- Débit de traitement (Firewall Throughput) : 10 Gbps, assurant qu'aucun goulot d'étranglement n'impacte la productivité des employés.
- Débit VPN IPsec : 1,8 Gbps, offrant des vitesses excellentes pour les administrateurs distants.
- Fonctionnalités UTM (Unified Threat Management) : Capacité à opérer de l'inspection antivirale en temps réel, de la prévention d'intrusion (IPS), du filtrage web et du contrôle applicatif.



3.3 Le Cœur de Réseau : Switch Cisco Catalyst 9200 (ou 2960-X)

Le commutateur Cisco est le cœur névralgique de la distribution filaire de la baie. Il assure la commutation de niveau 2 à une vitesse de 52 Gbps, tout en appliquant les politiques de sécurité des ports.

Ses ports Gigabit PoE (Power over Ethernet) ont été dimensionnés spécifiquement pour être capables d'alimenter les futures bornes Wi-Fi de l'entreprise et le parc de téléphonie IP, sans nécessiter d'injecteurs électriques supplémentaires.

4. Étude Comparative et Justification des Choix

Avant de procéder aux commandes et aux installations, j'ai réalisé une analyse comparative poussée des différentes technologies du marché pour justifier de manière argumentée mes choix techniques.

4.1 Comparatif des solutions de Virtualisation

L'enjeu majeur était de fournir un cluster de Haute Disponibilité (HA) capable de migrer des machines virtuelles d'un serveur à l'autre.

• VMware vSphere (ESXi) : C'est le leader historique du marché. Très mature et doté de la fonctionnalité vMotion. Cependant, l'utilisation de la Haute Disponibilité requiert l'achat d'un serveur vCenter et des licences extrêmement coûteuses par cœur de processeur. Solution rejetée pour budget limité.

• Microsoft Hyper-V : Parfaitement intégré à l'écosystème Windows, mais nécessite des licences Windows Server Datacenter hors de prix pour exploiter un cluster performant. Solution rejetée.

• Proxmox VE : Hyperviseur Open Source gratuit, basé sur un noyau Linux Debian. Il intègre nativement et gratuitement le système de cluster "Corosync", le support des VM (KVM) et des conteneurs (LXC), ainsi qu'une solution complète de sauvegarde. Solution retenue.

4.2 Comparatif des solutions Pare-feu

• pfSense / OPNsense : Solutions open-source excellentes et gratuites, mais nécessitant du matériel dédié (non fourni) et dénuées de support officiel constructeur en cas de panne critique. Rejeté.

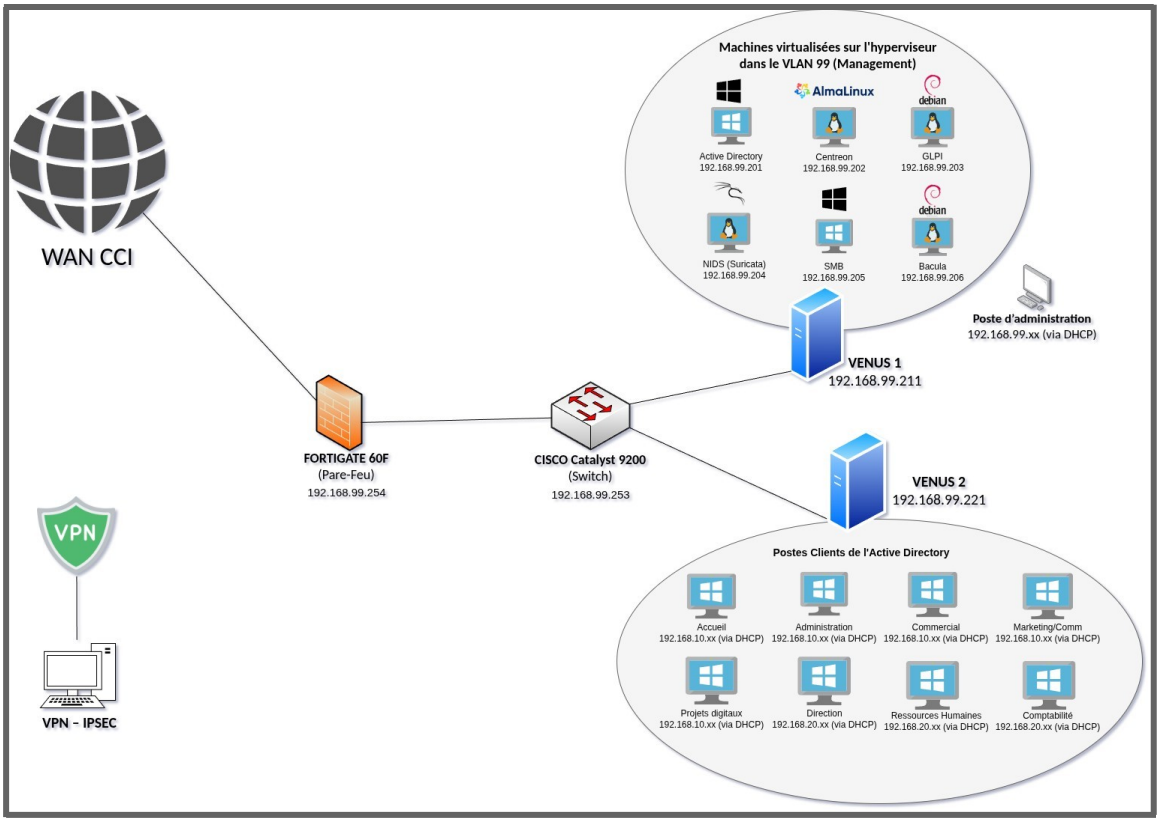
• Cisco ASA : D'une robustesse légendaire, mais la courbe d'apprentissage de son CLI (ligne de commande) est très abrupte et les licences sont onéreuses. Rejeté.

• Fortinet FortiGate : Offre une solution professionnelle clé en main. Son interface graphique orientée objet est redoutablement efficace. Il intègre le VPN IPsec natif et bénéficie du support constructeur (FortiCare). Solution retenue.

5. Topologie Réseau et Stratégie d'Adressage

5.1 Architecture Logique et Routage

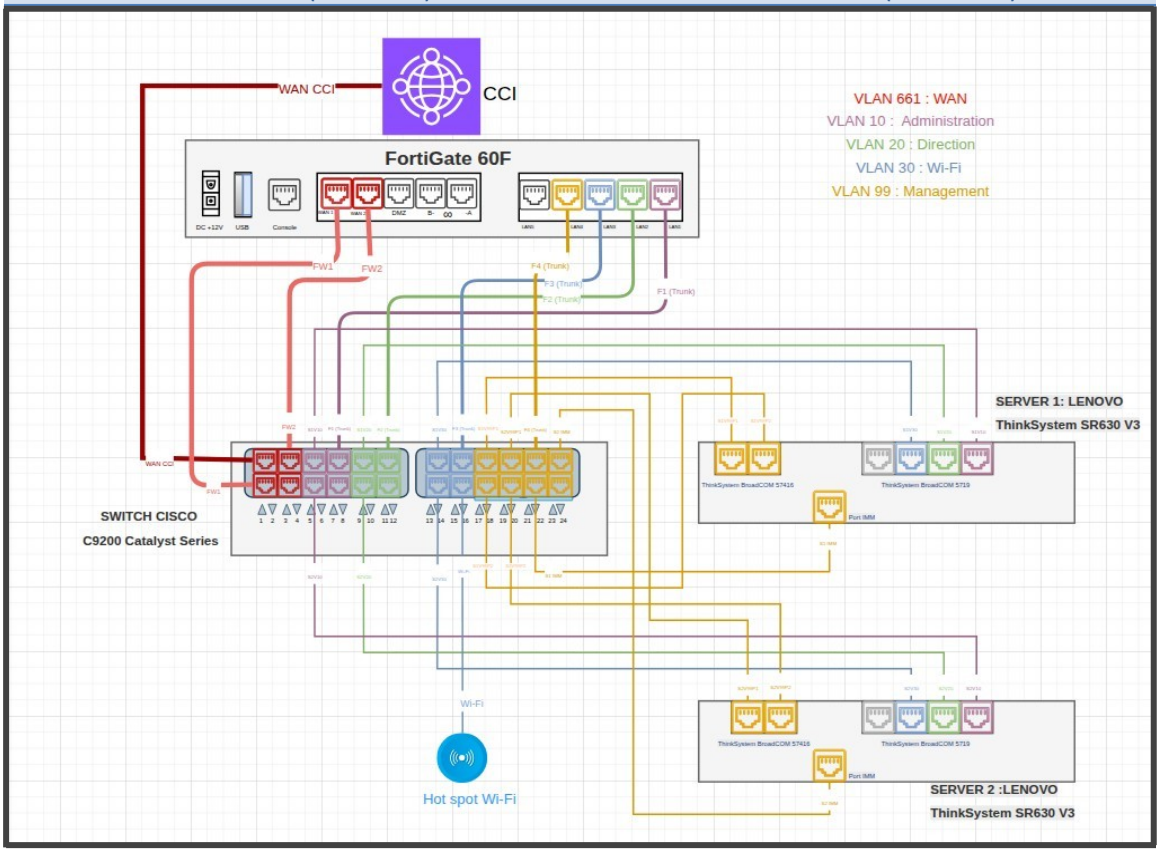
La topologie réseau s'appuie sur une segmentation logique poussée via des VLANs (Virtual Local Area Networks). Tous les flux inter-VLAN sont strictement contrôlés par le pare-feu FortiGate, suivant la politique du "Deny by Default" (Tout ce qui n'est pas explicitement autorisé est interdit).



5.2 Table Complète du Plan d'Adressage IP

ID VLAN	Désignation	Réseau (CIDR)	Adresse de la Passerelle
661	WAN (Interconnexion CCI)	172.16.60.0/22	172.16.63.254 (Opérateur)
10	Acc-Admin (Administration)	192.168.10.0/24	192.168.10.254 (FortiGate)
20	Direction	192.168.20.0/24	192.168.20.254 (FortiGate)
30	Wi-Fi Invités	192.168.30.0/24	192.168.30.254 (FortiGate)

99	Management IT (Serveurs)	192.168.99.0/24	192.168.99.254 (FortiGate)



5.3 Plan d'Adressage Statique (VLAN 99)

Le VLAN 99 est le cœur du système. Il ne distribue pas d'adresses dynamiques (Pas de DHCP). Toutes les adresses sont statiques et soigneusement répertoriées pour éviter les conflits d'IP.

Équipement / Serveur	Adresse IP Assignée	Rôle dans l'infrastructure
Windows Server 2025	192.168.99.1	AD DS, Serveur DNS et Serveur DHCP Central
Proxmox Node 1 (pve1)	192.168.99.211	Hyperviseur primaire
Proxmox Node 2 (pve2)	192.168.99.221	Hyperviseur secondaire (Cluster)
Cisco Catalyst (SVI)	192.168.99.10	Interface d'administration SSH du Switch
Lenovo XClarity (IMM1)	192.168.99.201	Gestion matérielle hors-bande Serveur 1
Lenovo XClarity (IMM2)	192.168.99.202	Gestion matérielle hors-bande Serveur 2

6. Phase 1 : Installation et Paramétrage de Proxmox VE

6.1 Installation de l'Hyperviseur Base

L'installation a débuté par la création d'une clé USB bootable à l'aide de l'utilitaire Rufus en mode DD Image, contenant l'image officielle de Proxmox VE 8.x.

Après insertion sur le serveur Lenovo, j'ai accédé au menu de démarrage (Boot Menu) pour lancer le programme d'installation. Les choix suivants ont été opérés :

- Système de fichiers : Sélection de ext4, reconnu pour sa simplicité et sa robustesse en environnement serveur.
- Paramètres de localisation : Fuseau horaire Europe/Paris et agencement clavier AZERTY.
- Configuration Réseau (Node 1) : Attribution de l'IP 192.168.99.211/24, Passerelle 192.168.99.254, DNS 192.168.99.1 et Hostname pve1.fantome.local.

6.2 Configuration des ponts réseaux (Linux Bridges)

Pour relier les futures machines virtuelles aux réseaux correspondants (VLANs), Proxmox utilise la technologie des "Linux Bridges" (Ponts virtuels). Chaque interface réseau physique du serveur Lenovo (ex: ens2f0) a été mappée à un pont virtuel (ex: vmbr2) rattaché au VLAN 10.

```
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#
```

6.3 Création du Cluster de Management (Grappe)

Afin de centraliser l'administration sur une seule interface Web et de préparer la redondance, j'ai configuré les deux serveurs en mode cluster.

Il est important de noter qu'un lien physique exclusif (un câble dédié) a été assigné au trafic de synchronisation du cluster (Corosync). Cette pratique garantit que la communication de

gestion inter-nœuds ne viendra jamais saturer la bande passante réservée au trafic de production des employés.

7. Phase 2 : Configuration du Cœur de Réseau (Cisco)

La configuration du switch a été réalisée entièrement en ligne de commande (CLI) via le port console (liaison série).

7.1 Création des VLANs et Affectation des Ports d'Accès

La première étape fut de déclarer les VLANs dans la base de données du commutateur, puis d'affecter les ports physiques selon le plan de brassage.

```
enable
configure terminal

vlan 10
 name Acc-Admin
vlan 20
 name Direction
vlan 30
 name WiFi
vlan 99
 name Management
exit

interface range FastEthernet0/5-8
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
exit

interface range FastEthernet0/9-12
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
exit
```

7.2 Agrégation de liens (Mode Trunk)

Pour acheminer les multiples VLANs jusqu'au pare-feu FortiGate via un seul câble réseau, le port de liaison montante a été configuré en mode "Trunk" avec encapsulation 802.1Q.

```
interface GigabitEthernet0/1
 description TRUNK-TO-FORTIGATE
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,99,661
exit

interface range GigabitEthernet0/23-24
 description TRUNK-TO-PROXMOX
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 20,99
exit
```

7.3 Sécurisation de l'accès distant (SSH)

Pour prévenir les attaques de type "Man-in-the-Middle", le protocole non sécurisé Telnet a été banni au profit de SSH (Secure Shell). Une clé de chiffrement RSA de 2048 bits a été générée.

```
interface vlan 99
 ip address 192.168.99.10 255.255.255.0
 no shutdown
exit
ip default-gateway 192.168.99.254

line vty 0 4
 transport input ssh
 login local
exit

username admin privilege 15 secret MonMotDePasseFort!
crypto key generate rsa modulus 2048
ip ssh version 2
write memory
```

8. Phase 3 : Déploiement du Pare-Feu (FortiGate)

Le FortiGate est le point de passage obligé pour tous les paquets du réseau. Toute sa configuration a d'abord été initiée en CLI, avant de basculer sur l'interface graphique HTTPS.

8.1 Déclaration de l'interface WAN (Accès Internet)

```
config system global
 set hostname FortiGate-Venus
 set timezone Europe/Paris
end

config system interface
 edit wan1
  set mode static
  set ip 172.16.60.10 255.255.252.0
  set allowaccess ping https ssh
  set role wan
 next
end

config router static
 edit 1
  set gateway 172.16.63.254
  set device wan1
 next
end
```

8.2 Création des interfaces virtuelles et Routage inter-VLAN

Pour que le Fortigate agisse comme routeur, des sous-interfaces ont été créées sur le port connecté au switch.

```
config system interface
 edit vlan10
  set ip 192.168.10.254 255.255.255.0
  set allowaccess ping
  set interface internal
  set vlanid 10
  set role lan
 next
 edit vlan99
  set ip 192.168.99.254 255.255.255.0
  set allowaccess ping https ssh snmp
  set interface internal
  set vlanid 99
 next
end
```

8.3 Configuration avancée du Relais DHCP (DHCP Relay)

C'est une étape cruciale. Plutôt que de laisser le routeur gérer le DHCP, j'ai configuré le FortiGate pour qu'il intercepte les requêtes DHCP des ordinateurs (qui sont des broadcasts bloqués par les routeurs) et les transfère spécifiquement (en unicast) vers le Serveur Active Directory (192.168.99.1).

```
config system dhcp server
 edit 1
  set default-gateway 192.168.10.254
  set interface vlan10
  set relay-agent enable
  set relay-server 192.168.99.1
 next
 edit 2
  set default-gateway 192.168.20.254
  set interface vlan20
  set relay-agent enable
  set relay-server 192.168.99.1
 next
end
```

8.4 Mise en place des politiques de pare-feu (Firewall Policies)

L'architecture de sécurité réseau repose sur trois règles fondamentales :

- Règle 1 : L'accès à Internet sortant. Le trafic émanant des VLANs 10, 20 et 30 vers l'interface WAN est autorisé avec les protocoles HTTP, HTTPS et DNS. L'option NAT (Network Address Translation) est activée pour masquer les IP privées derrière l'IP publique.
- Règle 2 : L'accès aux serveurs internes. Le trafic des utilisateurs vers le VLAN 99 est autorisé mais strictement limité aux protocoles essentiels (LDAPS pour l'authentification). Le NAT est désactivé sur cette règle.
- Règle 3 : Le cloisonnement. Le trafic du réseau invité (Wi-Fi VLAN 30) vers tous les autres réseaux de la SARL Fantôme est bloqué et enregistré dans les journaux (Logs) pour détecter d'éventuelles tentatives d'intrusion internes.

9. Phase 4 : Mise en place de l'Accès Distant (VPN IPsec)

Pour répondre à la demande d'administration à distance, la technologie de tunneling IPsec (IP Security) en mode "Client-to-Site" a été implémentée.

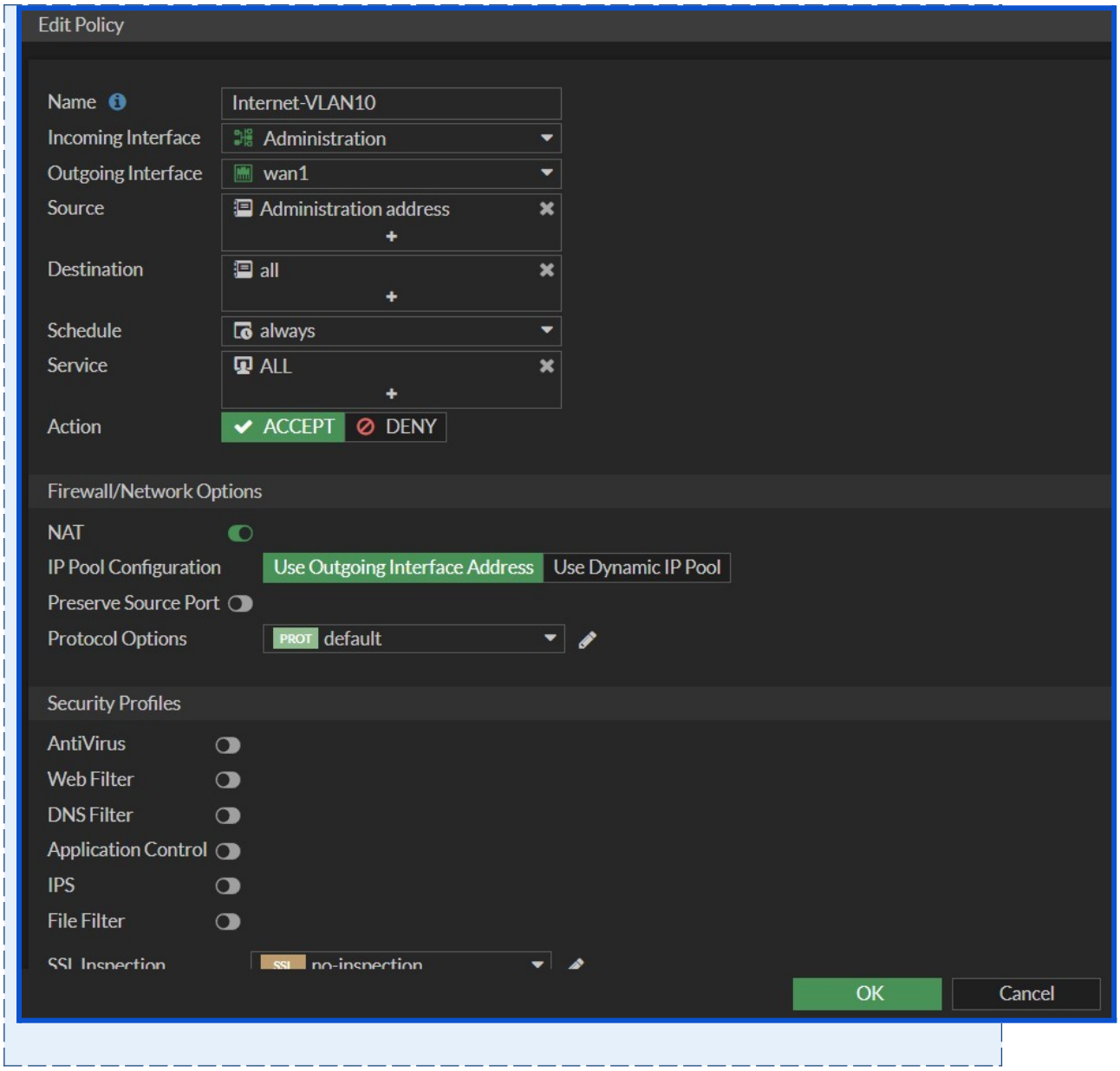
9.1 Négociation cryptographique (Phase 1 et 2)

La sécurité du VPN repose sur un très haut niveau de chiffrement :

- Authentification : Réalisée via une Clé Pré-partagée (Pre-Shared Key) complexe combinée au logiciel FortiClient.
- Chiffrement et Intégrité : Utilisation de l'algorithme AES-256 pour chiffrer les données, et SHA-256 pour garantir que les paquets ne sont pas altérés en transit.
- Perfect Forward Secrecy (PFS) : Le groupe Diffie-Hellman 14 (DH 14 - 2048 bit) a été configuré pour la génération asymétrique des clés.

```
config vpn ipsec phase1-interface
 edit VPN-IPsec-Remote-Admin
  set type dynamic
  set interface wan1
  set ike-version 2
  set peertype any
  set net-device disable
  set proposal aes256-sha256
  set dhgrp 14
  set psksecret ClefPrePartageeComplexe!
  set ipv4-start-ip 192.168.150.1
  set ipv4-end-ip 192.168.150.10
  set ipv4-netmask 255.255.255.240
 next
end
```

Les clients VPN qui se connectent avec succès recevront donc une adresse IP dynamique, située entre 192.168.150.1 et 192.168.150.10, et pourront accéder aux serveurs du VLAN 99.


Edit Policy
Name
Internet-VLAN10
Incoming Interface
Administration
Outgoing Interface
wan1
Source
Administration address
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Firewall/Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
IPS
File Filter
SSL Inspection
SSL
no-inspection
OK
Cancel

10. Phase 5 Le Serveur d'Infrastructure (Active Directory)

Une machine virtuelle Windows Server 2025 (4 cœurs, 8 Go de RAM) a été provisionnée avec l'IP statique 192.168.99.1.

J'y ai déployé le rôle Active Directory Domain Services (AD DS) pour créer le domaine forestier "fantome.local". Ce domaine permet désormais une gestion centralisée des identités de la SARL Fantôme et l'application de Stratégies de Groupes (GPO) pour durcir la sécurité des postes clients (complexité des mots de passe fixée à 12 caractères).

Le rôle Serveur DHCP a également été configuré avec trois étendues distinctes correspondant parfaitement aux sous-réseaux définis pour les VLANs 10, 20 et 30.

10.1 Évolutivité vers des solutions applicatives tierces

Grâce à la flexibilité offerte par la solution Proxmox, cette infrastructure est parfaitement dimensionnée pour accueillir des serveurs Linux (AlmaLinuxou ou Debian) supplémentaires à l'avenir.

L'architecture réseau permet l'intégration immédiate d'outils de ticketing ou de gestion de parc informatique. De la même façon, la séparation en VLANs facilite le déploiement d'une solution de supervision (qui pourrait facilement interroger l'ensemble des équipements de la baie Vénus grâce au routage configuré dans le FortiGate).

11. Bilan, Tests de Validation et Conclusion

11.1 Validation du fonctionnement

Avant la livraison finale de l'infrastructure, une série de tests (Ping inter-VLANs, tentatives de connexion non autorisées, établissement du tunnel IPsec depuis une connexion mobile externe) ont été menés. Tous ces tests se sont révélés concluants, validant la pertinence des politiques de sécurité imposées au FortiGate.

11.2 Bilan du Projet Vénus

Ce projet d'infrastructure m'a permis de mettre en pratique et d'orchestrer l'ensemble des compétences attendues d'un administrateur système et réseau SISR.

La livraison de la baie Vénus fournit à la SARL Fantôme un environnement matériel réseau haut de gamme, sécurisé et redondant.

Le socle technique est sain, évolutif et prêt à absorber la charge des utilisateurs. Il constitue surtout l'écrin parfait pour l'exploitation de futurs projets professionnels applicatifs subséquents.