BTS SIO 2025

☒ **Administration des systèmes et des réseaux (E6 – SISR)**

☐ **Conception et développement d'applications (E6 – SLAM)**

PAGE DE PRÉSENTATION DU DOSSIER

N° d'inscription[1] : |0|2|4|4|2|7|4|3|7|4|8|

NOM : PLATEL

PRÉNOM : Ginkgo

Date de passage[1] : 12 / 06 / 2025	Heure de passage[1] : 13 h 30

CATÉGORIE CANDIDAT[2] (UNE CASE À COCHER)	
❑ Scolaire	❑ Ex-scolaire
☒ Apprenti	❑ Ex-apprenti
❑ Formation professionnelle continue	❑ Ex-formation professionnelle continue
❑ Expérience professionnelle 3 ans	

[1] Informations communiquées sur votre convocation envoyée courant mars 2025 sur votre compte Cyclades

[2] Informations communiquées sur votre confirmation d'inscription.

Tampon de L'établissement

SIEC – maison des examens
7 rue Ernest Renan
94749 ARCUEIL CEDEX
Tél : 01 49 12 23 00
www.siec.education.fr

ESPL
Ecole Supérieure des Pays de Loire
SAS au capital de 47590 €
19 rue André Le Nôtre
49066 ANGERS Cedex 01
Tél. 02.41.73.20.30 - Fax 02.41.73.91.54
espl@espl.fr - www.espl.fr
SIRET 443 444 724 00027 - APE 8542Z

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[1]	PLATEL, Ginkgo Numéro de candidat : 02442743748 Centre d'examen : ESPL, Angers	**SISR**

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	J'ai mis en place un active directory avec des utilisateurs dans des OU.	
Un SGBD		
Un accès sécurisé à internet	Pour l'infrastructure du dossier E6, un pare-feu pfSense est present, avec des ACL	
Un environnement de travail collaboratif	Utilisation de Teamviewer	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	Il y a actuellement 6 serveurs virtuels, 4 sous Debian 12, 1 sous AlmaLinux 8 et 1 sous Windows Server 2025	

[1] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution de sauvegarde		
Des ressources dont l'accès est sécurisé et soumis à habilitation		
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)		

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Gestion des incidents		
Détection et prévention des intrusions		
Chiffrement		
Analyse de trafic	Wireshark est present sur les postes des utilisateurs support_IT	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : **« *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »**

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un réseau comportant plusieurs périmètres de sécurité	Il y a 3 zone du réseau, le LAN avec tout les serveurs, le client, avec tout les clients et switches et routeur ainsi qu'une DMZ.	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Le serveur DHCP est soumis a la haute disponibilité en ayant mis en place une redondance de ce dernier.	
Un logiciel d'analyse de trames		
Un logiciel de gestion des configurations		
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Les switches et routeur sont configures pour être administrable en SSH uniquement par le service support_IT	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Un serveur Centreon pour la supervision est mis en place, remontant les donnés d'utilisation matériel des serveurs	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)		

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service		
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion		
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion		

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	Un VPN OpenVPN via wireshark est active et fonctionnel	
Une solution permettant le déploiement des solutions techniques d'accès	Sur l'active directory, des GPO permettent de faire du deployment de masse	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*		
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau		

SOMMAIRE

VIII bis.- Switch #2 (Cisco 2960-X)

1. Création des vlans
2. Création des trunks
3. Sécurité

IX- Routeur (Cisco 1921)

1. Routing
2. Sécurité

X- Annexe

1. Annexe n°1 : Schéma réseau
2. Annexe n°2 : Plan de câblage

I- Introduction

Le projet présenté met en situation le service informatique d'une entreprise fictive nommé "Techcorp".
Ce dossier a pour objectif de présenter, étape par étape, les services à mettre en place, ainsi que leurs configurations, pour avoir une infrastructure d'entreprise type TPE/PME fonctionnelle et sécurisée, sans avoir recours à des prestataires extérieurs pour un fonctionnement classique.

Liste des services :

- -DHCP / DHCP failover
- -DNS
- -Pare-feu
- -Supervision
- -Contrôleur de domaine

Liste du matériel :

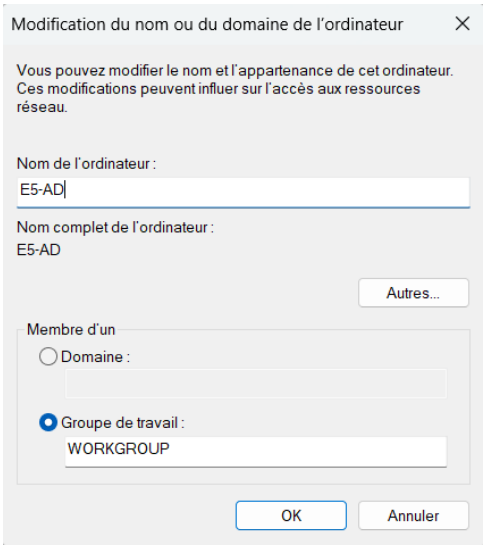
- -Ordinateur servant de serveur pour les services via VMware
- -Ordinateur client
- -x2 switch
- -Routeur

II- Contrôleur de domaine (Active Directory)

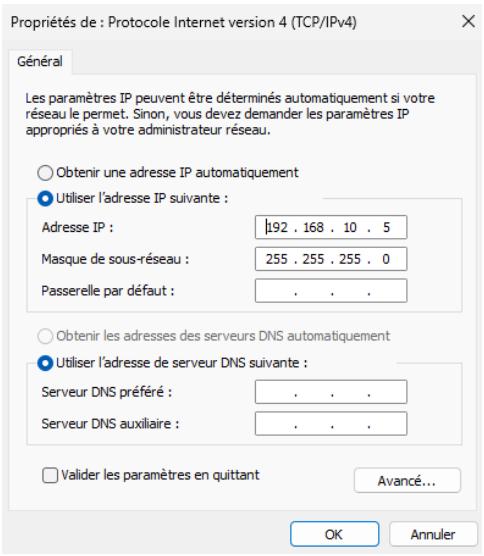
1. Installation du contrôleur de domaine

Pour l'active directory, nous allons utiliser la dernière version du système d'exploitation disponible, à savoir Windows Server 2025.

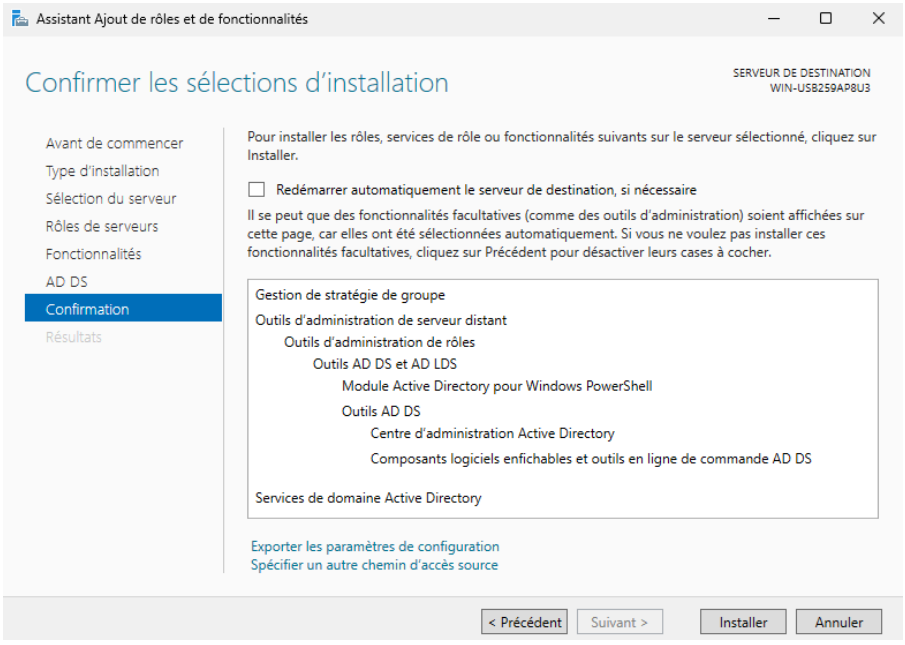
Une fois Windows initialité nous allons en premier temps renommer notre machine pour une meilleur visibilité à terme.



Nous allons par la suite définir une IP fixe à notre serveur. Cette IP doit être dans le même réseau que le vlan/vmnet indiqué sur le schéma réseau. Dans notre manipulation, ce réseau sera 192.168.10.0/24.

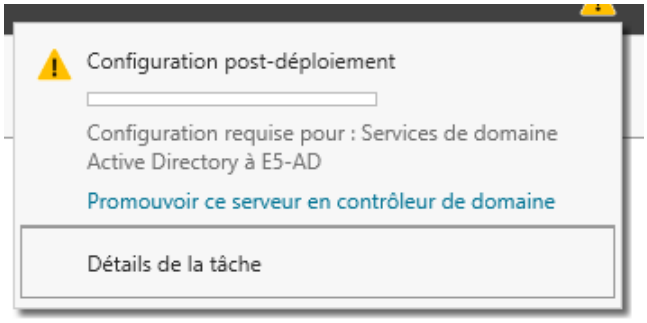


Une fois l'IP définis, on va pouvoir ajouter le rôle AD DS dans le gestionnaire de serveur -> gérer -> Ajouter des rôles et fonctionnalités.

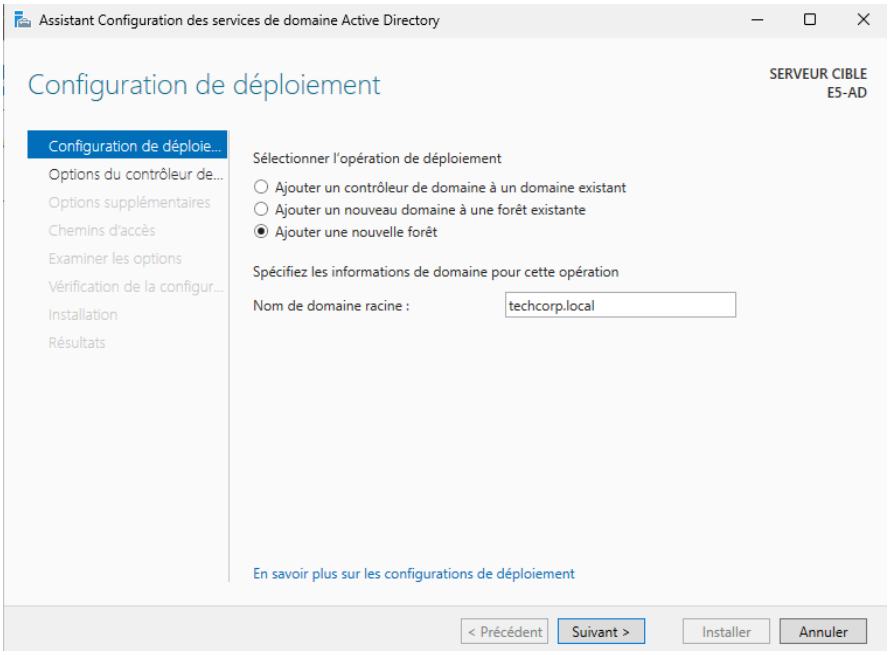


2. Création de la forêt

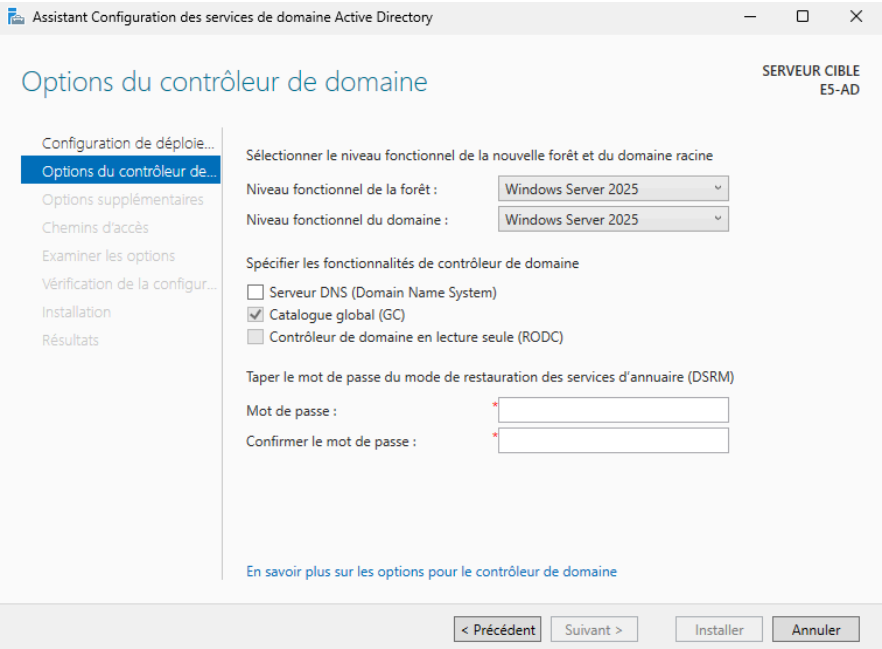
Une fois installé, nous pouvons promouvoir notre serveur en contrôleur de domaine.



Nous allons créer la forêt, et lui donner un nom, dans notre cas, techcorp.local



Nous allons ensuite pouvoir choisir les options du contrôleur de domaine. Dans notre cas, nous n'allons pas utiliser le DNS Windows, donc nous le décochons. Puis par la suite définir un mot de passe DSRM.



Puis, nous pourrons installer le contrôleur de domaine.

III- Pare-feu (pfSense)

1. Création des interfaces

Pfsense ne nécessite pas beaucoup de ressources pour fonctionner.
Après avoir fait l'installation de Pfsense, nous allons pouvoir configurer les interfaces. Au préalable, il faudra quatre (4) interfaces pour le fonctionnement de notre infrastructure.

WAN;LAN;OPT1;OPT2, qu'on nommera par la suite.

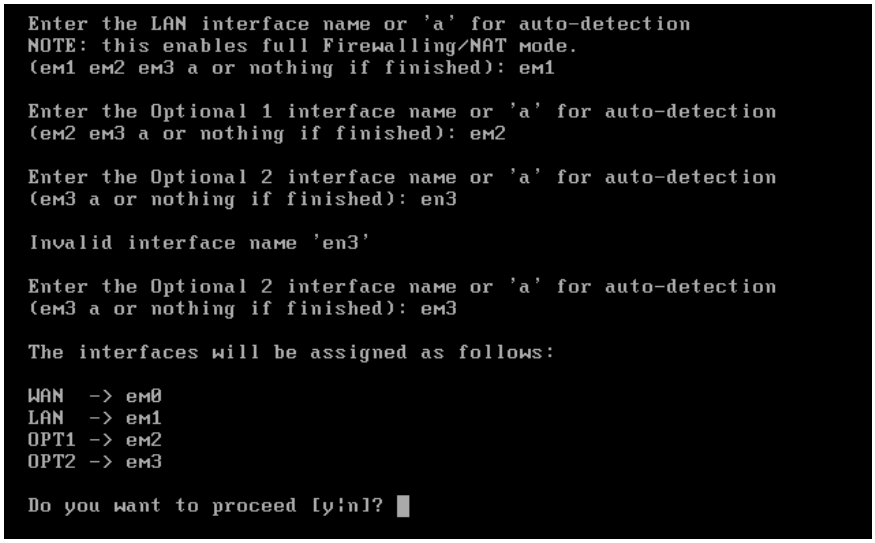
Pour commencer, nous allons définir quelle interface sera le WAN, LAN …..
Pour s'assurer que l'interface souhaitée soit la bonne, il faut s'assurer qu'elle conviendra au bon vlan.

Le WAN sera simplement l'entrée/sortie d'internet. Son adresse IP sera définie en DHCP, le fournisseur d'accès internet lui attribuant l'IP.

Le LAN sera le vlan utilisé par les services type DHCP, DNS, AD …..

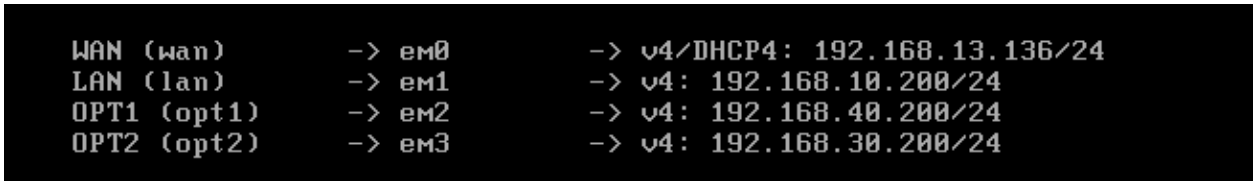
OPT1 sera le vlan pour les clients (Collaborateurs de Techcorp)

OPT2 sera pour la DMZ.



2. Routing

Une fois les interfaces assignées, nous allons pouvoir définir les adresses IP des interfaces, pour ce faire, sur Pfsense, nous allons sélectionner l'option "2" et définir les IPv4 de la sorte à quelles correspondent au schéma réseau.



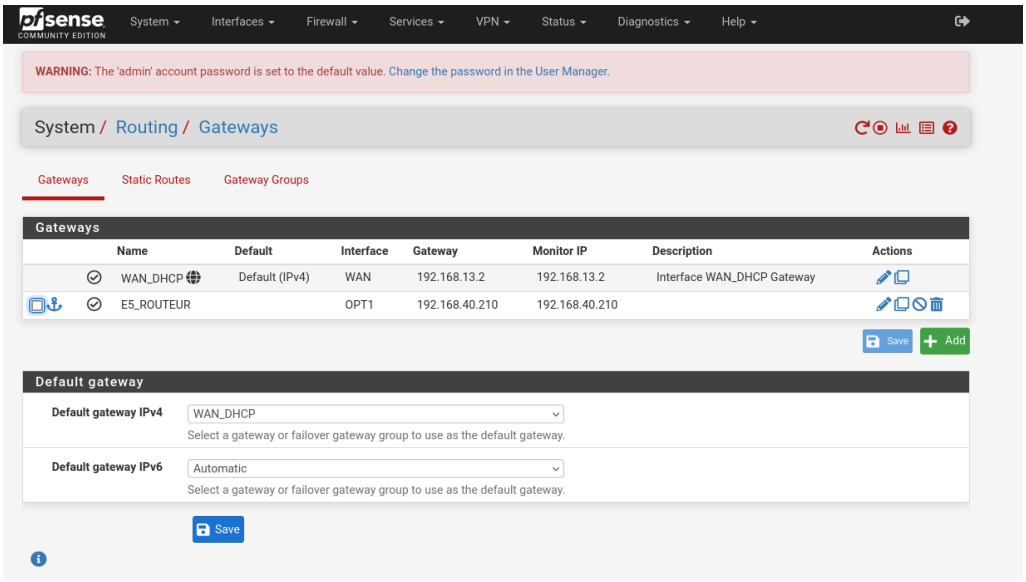
Nous allons ensuite pouvoir nous rendre sur l'interface web de pfSense, pour ce faire, nous allons nous connecter, depuis un poste client test, sur le réseau 192.168.10.0/24.

Sur le navigateur web, nous allons rechercher l'adresse IP 192.168.10.200, et pouvoir nous connecter à l'interface web de pfSense avec comme accès, login : admin | mot de passe : pfsense.

Une fois sur l'interface web, nous allons nous rendre dans system/routing puis dans la catégorie Gateways, nous allons ajouter comme gateway, notre futur routeur pour les clients.

Pour ce faire, nous allons cliquer sur “add”.

Décocher la case disable gateway si elle est coché
Dans interface, choisir OPT1,
Dans name, définir le nom souhaité
Dans Gateway, indiquer l’adresse IP de la gateway vers le routeur : 192.168.40.210
Puis pour finir, on oublie pas de save et de apply les modifications.

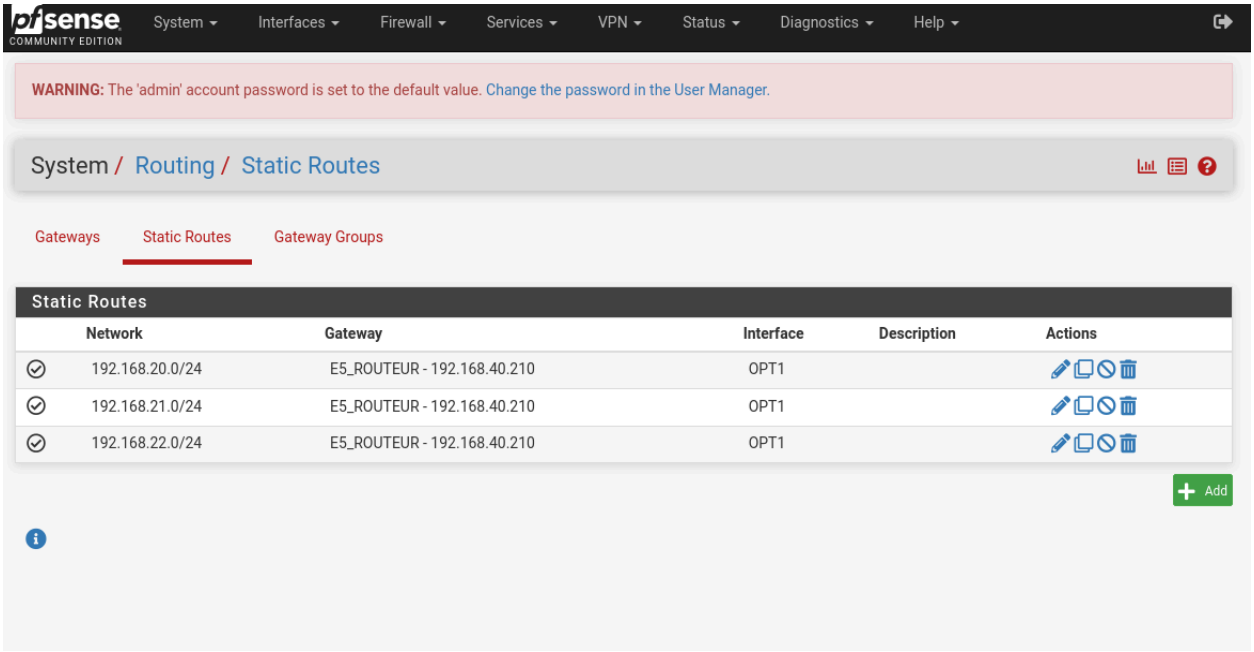


Puis dans default gateway IPv4, indiquer la gateway WAN.

Nous allons ensuite aller dans static routes, de là, nous allons ajouter nos trois (3) routes statiques pour nos trois (3) interfaces internes.

Dans add, nous allons définir comme destination network, le réseau souhaité, 192.168.20.0/24 pour le support IT, 192.168.21.0/24 pour le service commercial et 192.168.22.0/24 pour le service comptabilité.

A chaque réseau, la gateway sera celle du routeur tout juste créé.



3. Création des règles

IV- DHCP (ISC DHCP)

1. Installation

Nous allons maintenant mettre en place le serveur DHCP sur une machine virtuelle Debian 12 CLI.
Pour les premières installations, la machine restera en NAT, puis une fois en production, devra être mit sur la même interface que pfSense, soit l'interface LAN.

Une fois l'os installé, nous allons nous mettre en root, puis procéder aux installations.

Avant tout, nous devons mettre à jour la machine à l'aide de la commande apt-get update.

Suite à ça, nous allons installer le package isc-dhcp-server.

2. Configuration + Failover

Nous allons nous rendre dans le fichier dhcpd.conf grâce à la commande nano/etc/dhcpd.conf

De là, nous allons pouvoir faire nos configurations.

```
  GNU nano 7.2                                                  /etc/dhcp/dhcpd.conf
authoritative;
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "techcorp.local";
option domain-name-servers 192.168.10.4;

failover peer "dhcp-failover" {
   primary;
   address 192.168.10.1;
   port 647;
   peer address 192.168.10.10;
   peer port 647;
   max-response-delay 60;
   max-unacked-updates 10;
   mclt 1800;
   split 128;
   load balance max seconds 3;
}

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;
```

option domain-name : techcorp.local
option domain-name-servers : 192.168.10.4, ce sera l'ip de notre serveur DNS
Par la suite, nous allons configurer le failover pour la redondance du serveur dhcp.

Pour ce faire, indiquer ce serveur en serveur primaire, avec son adresse 192.168.10.1. Le port sera celui par défaut pour cette redondance : 647. Notre serveur de secours aura pour IP 192.168.10.10

Nous allons ensuite faire nos plages d'adresse IP par services

Le LAN sera sur le réseau 192.168.10.0/24
Support IT sur le réseau 192.168.20.0/24
Commercial sur le réseau 192.168.21.0/24
Comptabilité sur le réseau 192.168.22.0/24
La DMZ sur le réseau 192.168.30.0/24

```
subnet 192.168.10.0 netmask 255.255.255.0 {
#subnet LAN
 pool {
  failover peer "dhcp-failover";
  range 192.168.10.1 192.168.10.189;
}
  option routers 192.168.10.200;
  option subnet-mask 255.255.255.0;
}

subnet 192.168.20.0 netmask 255.255.255.0 {
#subnet SUPPORT_IT
 pool {
  failover peer "dhcp-failover";
  range 192.168.20.1 192.168.20.189;
}
  option routers 192.168.20.190;
  option subnet-mask 255.255.255.0;
}

subnet 192.168.21.0 netmask 255.255.255.0 {
#subnet COMMERCIAL_1
 pool {
  failover peer "dhcp-failover";
  range 192.168.21.1 192.168.21.189;
}
  option routers 192.168.21.190;
  option subnet-mask 255.255.255.0;
}
```

```
subnet 192.168.22.0 netmask 255.255.255.0 {
#subnet COMPTABILITE
 pool {
  failover peer "dhcp-failover";
  range 192.168.22.1 192.168.22.189;
}
  option routers 192.168.22.190;
  option subnet-mask 255.255.255.0;
}

subnet 192.168.30.0 netmask 255.255.255.0 {
#subnet DMZ
 pool {
  failover peer "dhcp-failover";
  range 192.168.30.1 192.168.30.189;
}
  option routers 192.168.30.200;
  option subnet-mask 255.255.255.0;
}
```

Puis faire nos réservations d'adresse via les adresse MAC

```
host e5_dns {
   hardware ethernet 00:0c:29:ea:b9:9b;
   fixed-address 192.168.10.4;
   option host-name e5_dns;
}
host e5_ad {
   hardware ethernet 00:0c:29:fa:2d:16;
   fixed-address 192.168.10.5;
   option host-name e5_ad;
}
host e5_centreon {
   hardware ethernet 00:0c:29:35:f0:12;
   fixed-address 192.168.10.6;
   option host-name e5_centreon;
}
```

Nous allons pouvoir ensuite recommencer à 0 avec un nouveau serveur Debian 12 CLI, cette fois-ci pour le failover.

La seule différence va être sur le fichier dhcpd.conf, au lieu d'indiquer le serveur en primary, on le mettra en secondary, puis en premier l'adresse ip du serveur secondaire, 192.168.10.10 puis ensuite le primaire

```
# option definitions common to all supported networks...
option domain-name "techcorp.local";
option domain-name-servers 192.168.10.4;

failover peer "dhcp-failover" {
   secondary;
   address 192.168.10.10;
   port 647;
   peer address 192.168.10.1;
   peer port 647;
   max-response-delay 60;
   max-unacked-updates 10;
   mclt 1800;
   load balance max seconds 3;
}

default-lease-time 600;
max-lease-time 7200;
```

V- DNS (Bind9)

1. Installation

Tout comme les serveurs DHCP, le serveur DNS sera un Debian 12 CLI.

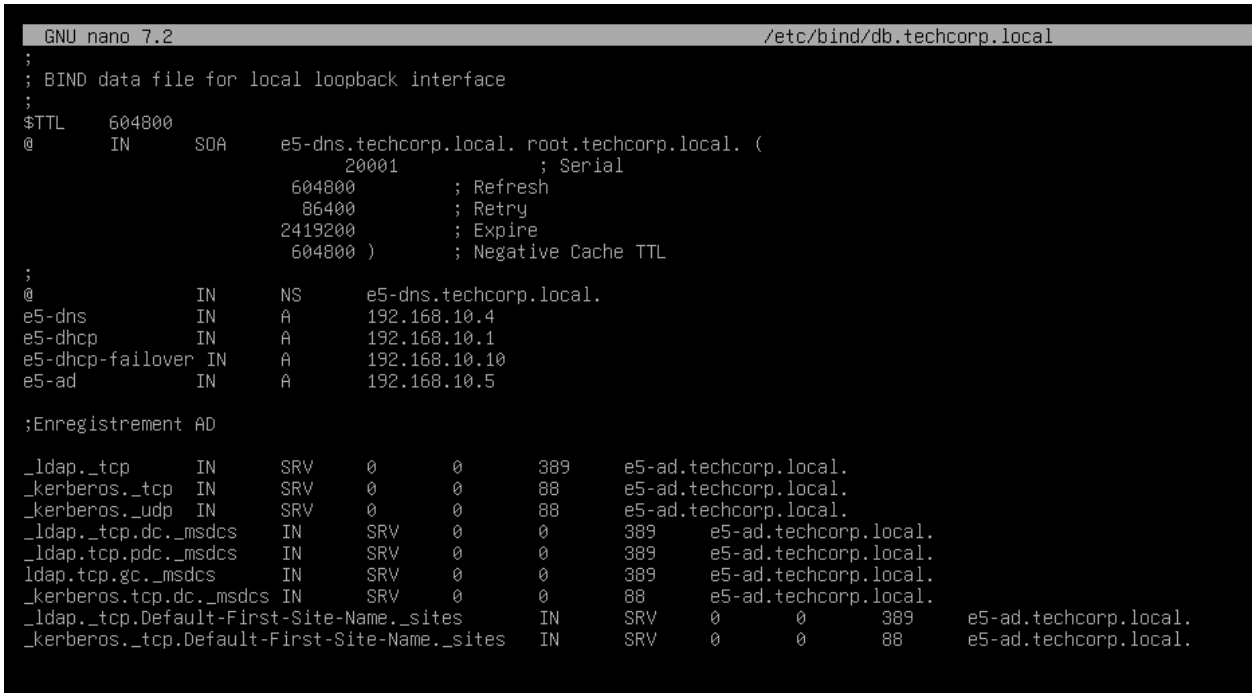
Une fois les packages mis à jour, il faudra installer bind9.

Une fois installé, nous allons en premier temps configurer le fichier /etc/bind/named.conf.options

```
 GNU nano 7.2                                                  /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
                1.1.1.1;
                8.8.8.8;
         };

        recursion yes;

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================

        dnssec-validation auto;

        allow-query { any; };
        listen-on { any; };
        listen-on port 53 { any; };
};
```

2. Zone direct

nous allons pouvoir configurer notre zone direct, pour ce faire, on va copier le fichier db.local dans /etc/bind/db.local qui nous servira de base saine pour nos configurations.



```
  GNU nano 7.2                                                    /etc/bind/db.techcorp.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     e5-dns.techcorp.local. root.techcorp.local. (
                              20001           ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      e5-dns.techcorp.local.
e5-dns          IN      A       192.168.10.4
e5-dhcp         IN      A       192.168.10.1
e5-dhcp-failover IN     A       192.168.10.10
e5-ad           IN      A       192.168.10.5

;Enregistrement AD

_ldap._tcp      IN      SRV     0       0       389     e5-ad.techcorp.local.
_kerberos._tcp  IN      SRV     0       0       88      e5-ad.techcorp.local.
_kerberos._udp  IN      SRV     0       0       88      e5-ad.techcorp.local.
_ldap._tcp.dc._msdcs    IN      SRV     0       0       389     e5-ad.techcorp.local.
_ldap.tcp.pdc._msdcs    IN      SRV     0       0       389     e5-ad.techcorp.local.
ldap.tcp.gc._msdcs      IN      SRV     0       0       389     e5-ad.techcorp.local.
_kerberos.tcp.dc._msdcs IN      SRV     0       0       88      e5-ad.techcorp.local.
_ldap._tcp.Default-First-Site-Name._sites       IN      SRV     0       0       389     e5-ad.techcorp.local.
_kerberos._tcp.Default-First-Site-Name._sites   IN      SRV     0       0       88      e5-ad.techcorp.local.
```

Une fois configuré, il faudra l’enregistrer avec le nom db.techcorp.local

La particularité de notre fichier, c’est que pour le fonctionnement de l’active directory, il accueille aussi les enregistrements SRV obligatoire pour le bon fonctionnement de ldap et kerberos.

3. Zone inversée

Par la suite, on a a nouveau pouvoir copier le fichier db.local, cette fois ci pour faire notre zone inversée

```
  GNU nano 7.2                                                    /etc/b
;
; BIND data file for 10.168.192.in-addr.arpa
;
$TTL    604800
@       IN      SOA     e5-dns.techcorp.local. root.techcorp.local. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      e5-dns.techcorp.local.
4       IN      PTR     e5-dns.techcorp.local.
1       IN      PTR     e5-dhcp.techcorp.local.
10      IN      PTR     e5-dhcp-failover.techcorp.local.
5       IN      PTR     e5-ad.techcorp.local.
```

Une fois configuré, on va pouvoir l'enregistrer sous le nom db.reverse.techcorp.local, toujours dans le dossier /etc/bind/

Et pour finir, on va pouvoir notifier nos nouvelles zones dans le fichier /etc/bind/named.conf.local

```
  GNU nano 7.2                                        /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "techcorp.local" {
        type master;
        file "/etc/bind/db.techcorp.local";
        allow-update { 192.168.10.5; };
};

zone "10.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.reverse.techcorp.local";
        allow-update { 192.168.10.5; };
};
```

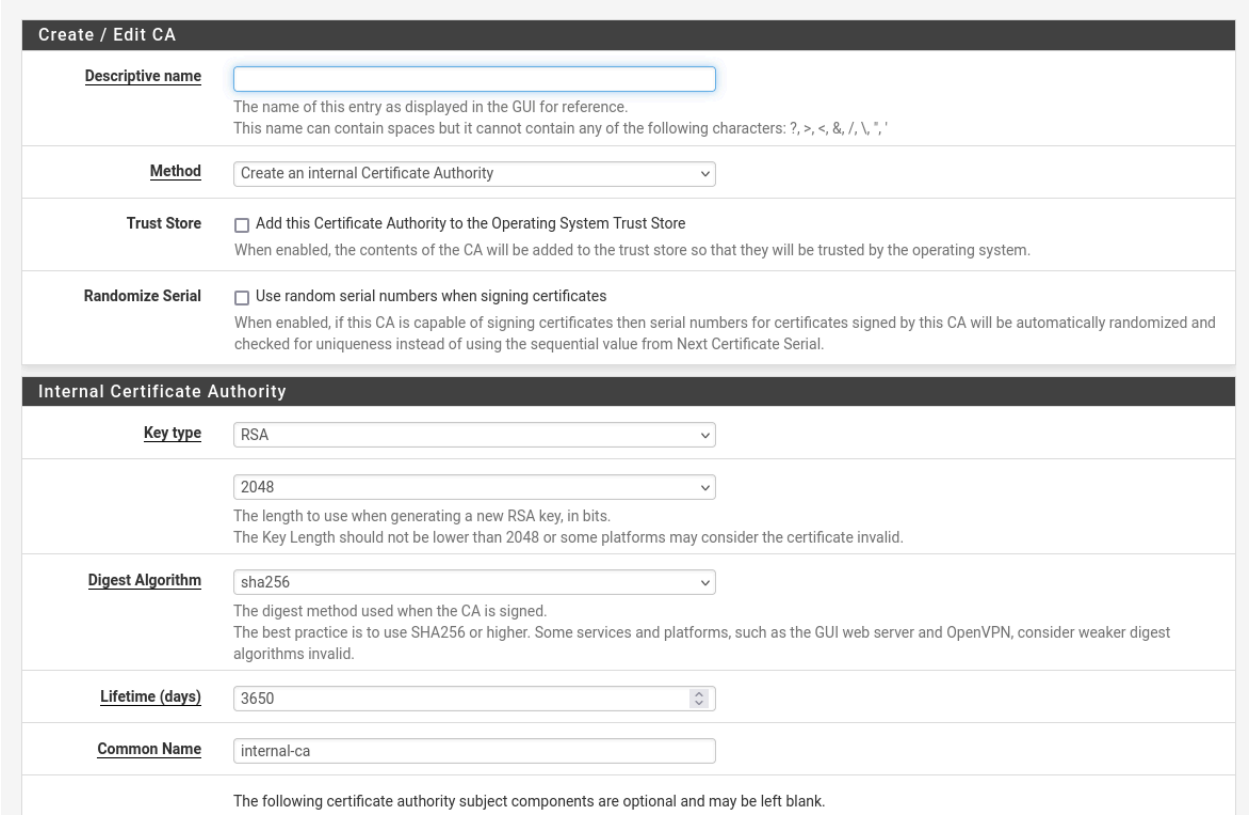
Malgré tout, on va autoriser notre serveur AD (192.168.10.5) à venir écrire dans nos zones, vu que nous n'utilisons pas le DNS Windows comme redirecteur.

VI- VPN (OpenVPN)

1. Création du certificat

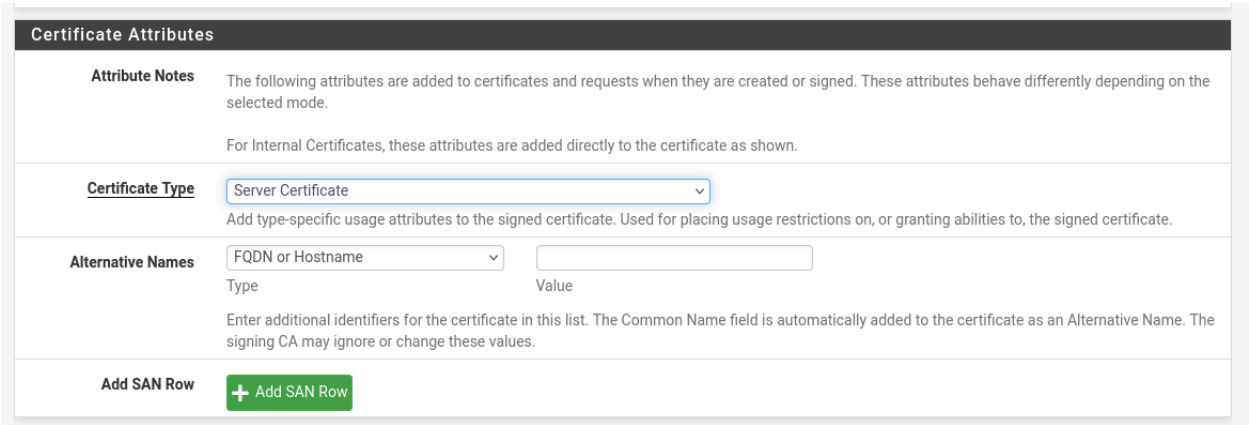
Nous allons retourner sur notre machine pfSense, sur l'interface web. Puis dans systeme->certificate, nous allons créer notre autorité de certificat

En descriptive name, on y note ce que l'on souhaite, pour s'y repérer, la méthode, il faudra choisir de créer une autorité de certificat interne. Puis ensuite choisir un nom commun "common name" qui sera le nom de l'autorité.



Ensuite, nous nous rendrons dans certificat pour créer notre certificat VPN

Le descriptive name, encore une fois, est le nom donné pour se repérer.
Il faudra alors choisir notre autorité de certificat créé précédemment dans certificat authority puis encore une fois définir un nom dans common name. Puis pour finir, bien sélectionner server certificate dans le type de certificat



Une fois validé, nous avons créé le certificat nécessaire.

2. Création des utilisateurs

Ensuite, nous allons créer nos utilisateurs, pour ce faire, dans systeme->user management->users nous allons ajouter un utilisateur.

On lui définit bien son login et mot de passe, puis il faudra sélectionner la case “create user certificate”

Nous choisirons notre autorité de certificat du VPN puis une fois l'algorithme de sécurité choisis, nous allons pouvoir le créer

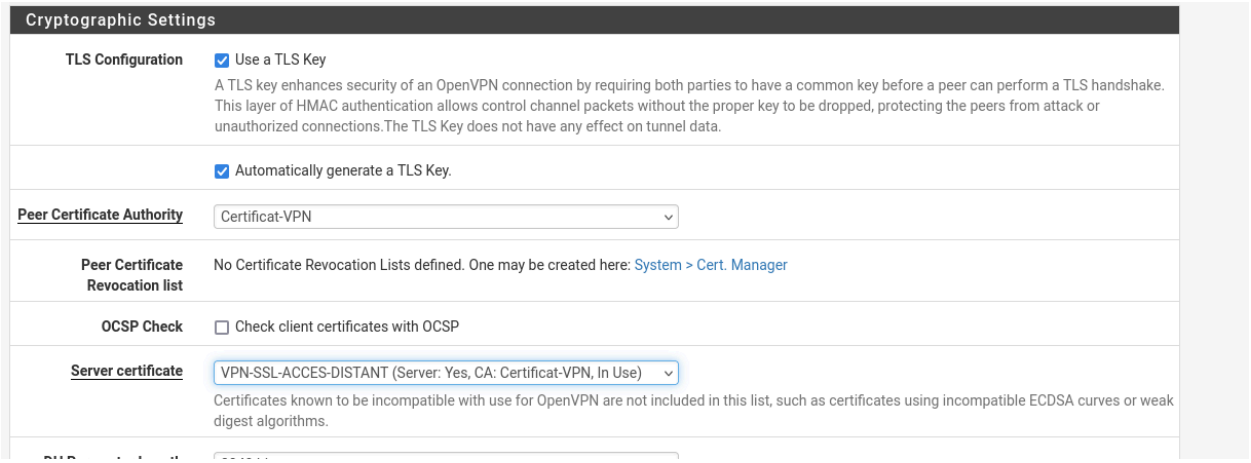
Nous pourrons répéter cette manipulation le nombre de fois souhaité, en fonction du nombre d’utilisateurs.

3. Configuration du VPN

Ensuite, dans le menu VPN, puis dans openVPN, dans la catégorie servers, on va venir ajouter un serveur openVPN.

On va choisir le mode de server Remote Acces SSL/TLS + user auth et choisir le port 1194. Évidemment on laisse le WAN comme interface, puisque le VPN va devoir passer par l’interface WAN pour accéder à notre réseau.

On va ensuite choisir notre autorité de certification créée précédemment, puis le certificat serveur qu'on a créé, le certificat VPN.



On choisit le cryptage souhaité, puis on définit ensuite la configuration du tunnel.

Le réseau sera 10.10.5.0/24
On redirige tout le trafic IPv4 dans le tunnel
L'adresse 192.168.10.0/24 sera le réseau IPv4 local
Et on va choisir un total de 30 connexions simultanées.

On va cocher ensuite dynamic IP, empêchant une déconnexion en cas de changement d'IP du FAI puis on va choisir la topology net30 - isolated /30 network per client pour une isolation de chaque clients.

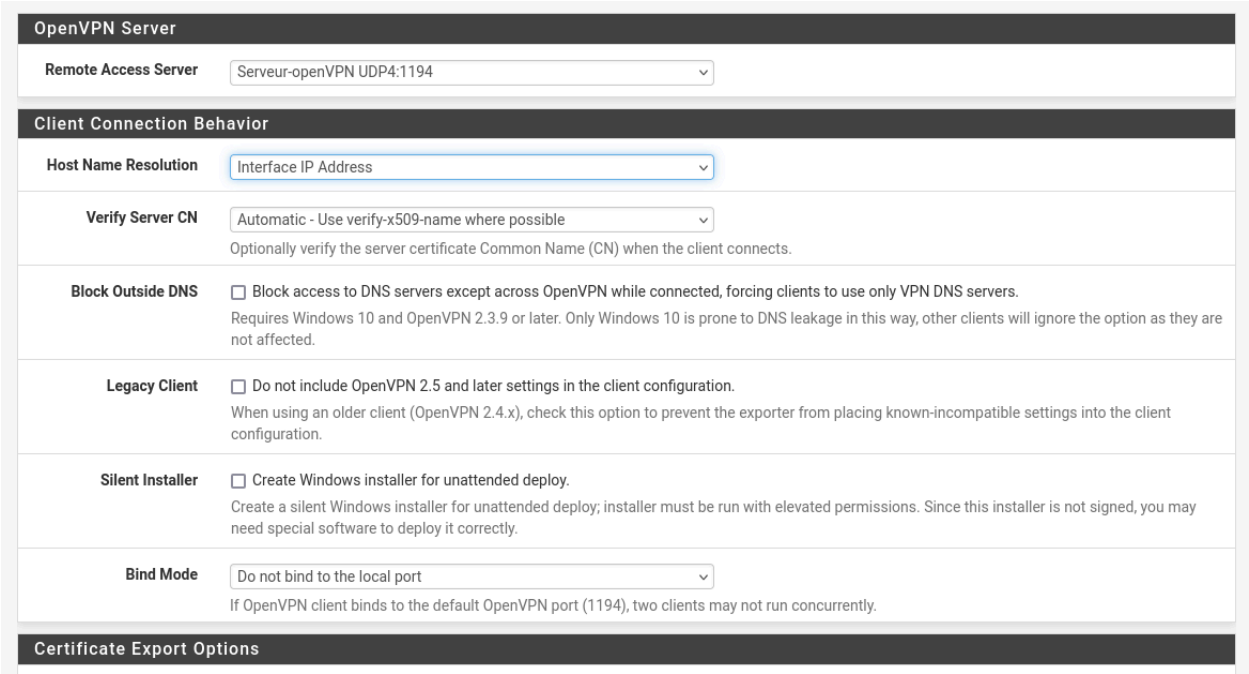
Dans les paramètres clients avancés, on va mettre notre nom de domain techcorp.local ainsi que l'adresse IP de notre DNS 192.168.10.4

Puis on va ensuite pouvoir valider.

Nous allons ensuite exporter la configuration. Pour ce faire, dans Package Manager, nous allons ajouter le package openvpn-client-export.

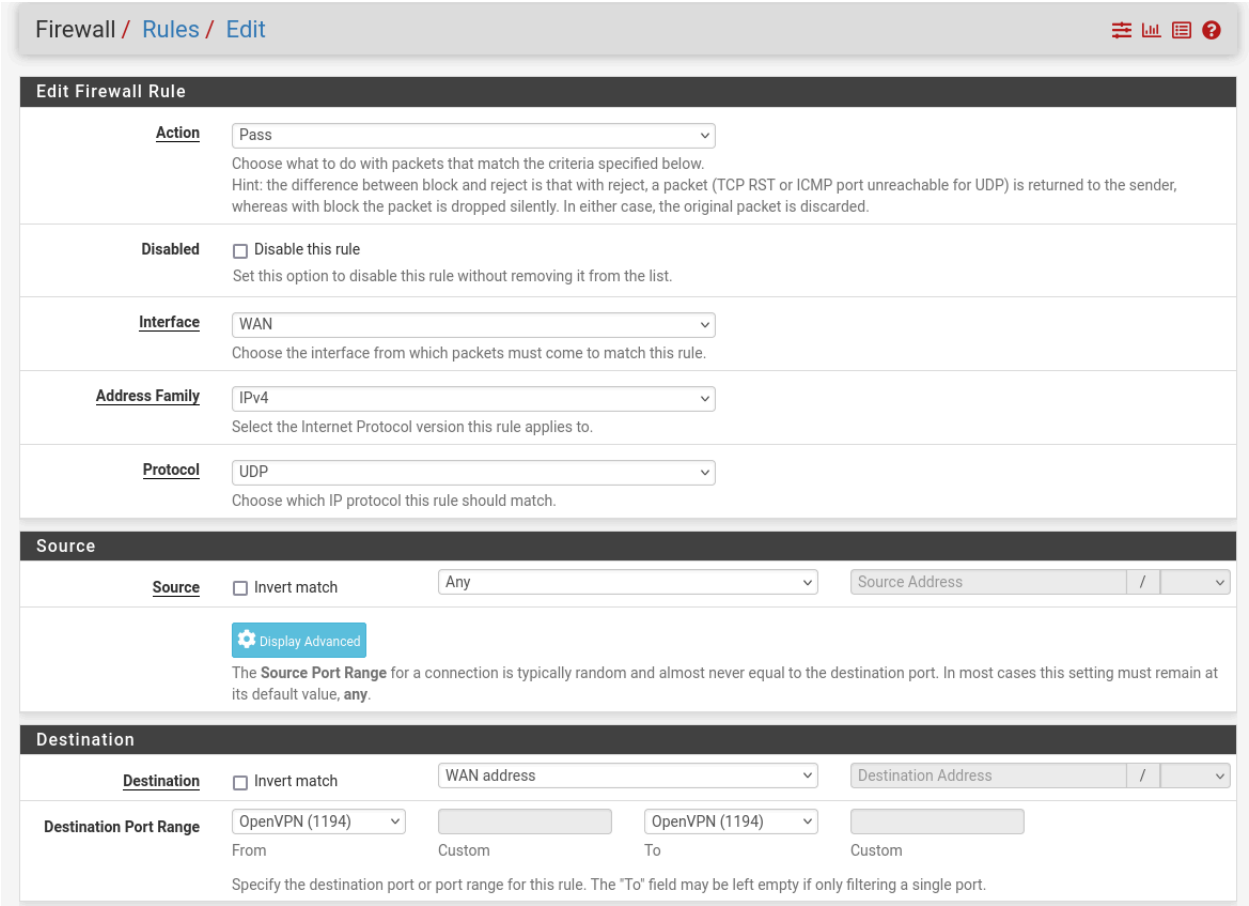
Une fois installé, dans openVPN, nous allons pouvoir exporter la configuration client.

On va choisir comme serveur d'accès à distance, notre serveur openVPN, puis comme résolution de nom d'hôte, "interface IP address"



Nous allons ensuite pouvoir télécharger l'archive. Les trois (3) fichiers se trouvant dans l'archive seront les fichiers permettant la connexion à notre infrastructure.

Par la suite, nous allons créer des règles permettant l'accès du VPN à notre infrastructure. Dans les règles pfSense, nous allons laisser passer le protocol UDP sur l'interface WAN, avec comme destination le WAN et comme port 1194.



Suite à ça, nous pouvons aussi ajouter des règles pour permettre au VPN d'accéder aux ressources de notre infrastructure.

Pour finir, sur le poste client qui doit avoir accès au VPN, il faudra installer OpenVPN. Une fois installé, dans le dossier de configuration (C:\Programmes\OpenVPN\Config), nous allons pouvoir copier ces trois (3) fichiers provenant de l’archive télécharger et les coller.

Par la suite, il n’y a plus qu’à se connecter avec l’utilisateur créé dans la base de donnée pfSense.

VII- Supervision (Centreon)

1. Installation

Pour la supervision, il nous faudra une machine AlmaLinux 8 graphique.

Une fois les packages mis à jour, nous pourrons installer le package grâce à la commande curl -L -s https://download.centreon.com/24.10/unattended.sh | sh

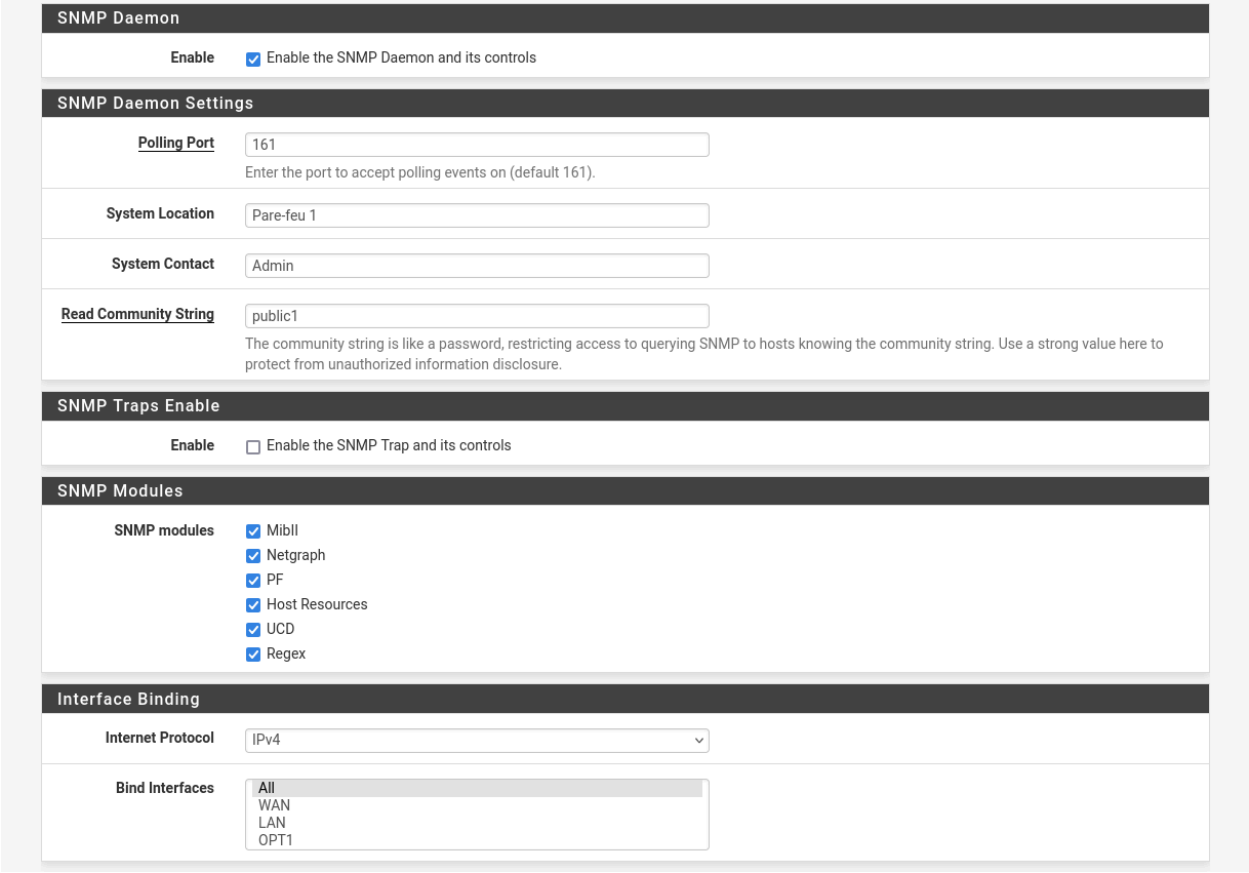
Par la suite, via l'interface web 192.168.10.6, nous allons continuer la configuration web.
On va tout laisser par défaut jusqu'à arriver à la page de création du compte administrateur.

A ce moment là nous allons choisir un mot de passe, un nom prénom ainsi qu'une adresse mail, qui sera centreon@techcorp.local

Puis sur la page suivante, nous définirons les mots de passe nécessaires pour tous les services. Une fois fait, il nous restera plus qu'à nous connecter à l'interface de supervision avec les logins et mot de passe choisis.

2. Configuration des sondes

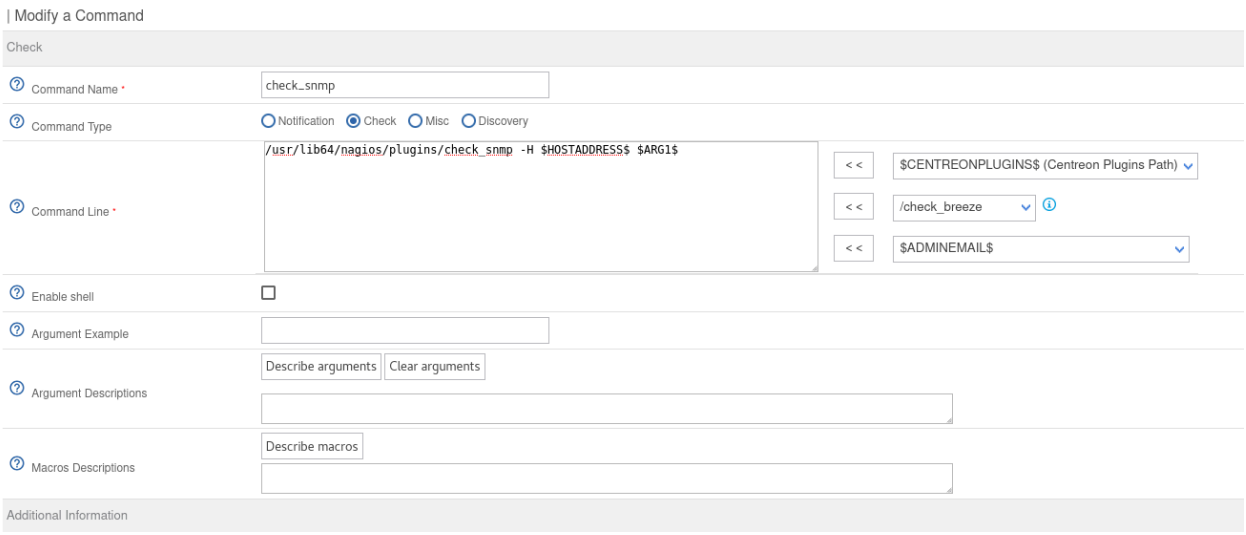
Nous allons ensuite configurer la sonde de pourcentage d'utilisation moyen du CPU de pfSense, pour ce faire, nous allons nous rendre sur l'interface web de pfSense, dans service->SNMP, puis nous allons activer SNMP. Il faut ensuite choisir un mot dans Read Community String, qui servira de "code" pour que la sonde puisse remonter jusqu'à Centreon.



Nous devons ensuite, dans les règles de pfSense, laisser passer le protocole UDP sur le port 161 pour l'interface LAN.

Ensuite, dans l'interface web de Centreon, dans configuration -> commands -> checks, nous allons ajouter une nouvelle commande.

Le nom sera check_snmp
Le type de commande sera check
La ligne de commande sera /usr/lib64/nagios/plugins/check_snmp -H $HOSTADDRESS$ $ARG1$



Par la suite, dans configuration->hosts, nous allons créer un nouvel host.

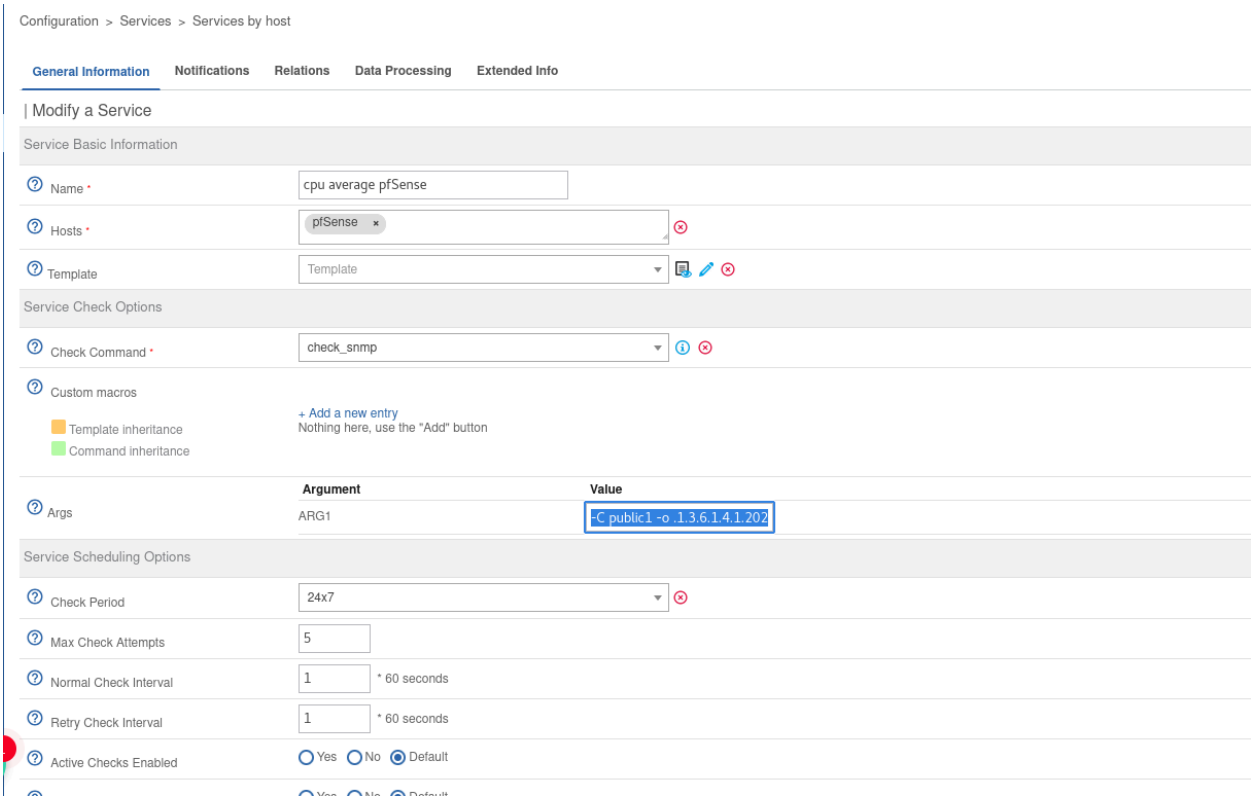
Le name et l'alias sont au choix, et nous indiquerons l'interface LAN de pfSense comme address : 192.168.10.200

par la suite, en check command, nous mettrons check_snmp, que nous venons tout juste de créer, puis nous pouvons sauvegarder.

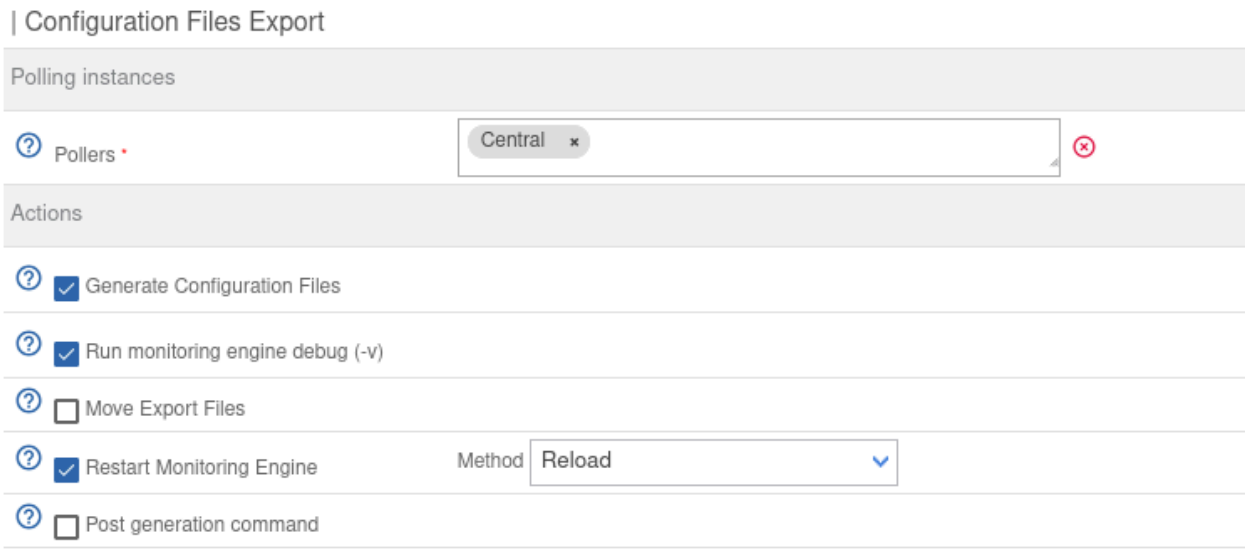
Ensuite, nous allons ajouter notre nouveau service dans configuration->service->service by host

Le nom est à choisir puis, dans host, il faudra sélectionner le host créé précédemment.
A nouveau dans check_command, il faudra choisir check_snmp puis cette fois ci dans argument, il faudra ajouter cette ligne : -C public1 -o .1.3.6.1.4.1.2021.10.1.3.1 -P 2c -w 1 -c 2

Enfin, nous pouvons choisir les intervalles de check à notre guise.



Par la suite, il nous restera plus qu'à aller dans pollers-> configure pollers, puis choisir d'exporter la configuration. A ce moment-là il faudra choisir le pollers, puis cocher les cases generate configuration files ; run monitoring debug ainsi que restart monitoring engine, en reload et non restart. Puis ensuite cliquer sur Export



Une fois fait, la sonde remontera le pourcentage d'utilisation moyen du CPU de pfSense.

VIII- Switch #1 (Cisco 2960-X)

1. Création des vlans

Pour que les clients physiques aient accès à l'infrastructure informatique, il faut évidemment configurer des switches. Techcorp utilise actuellement deux (2) switches de niveau 2.

Pour ce faire, sur le switch #1, nous allons configurer les vlans de la façon indiquée sur le schéma réseau.

Pour commencer, une fois le switch initialisé, nous allons définir le mot de passe administrateur.

Une fois en accès enable, puis en conf t, nous allons créer notre premier vlan

Pour ce faire, on va indiquer ces commandes

```
vlan 2
name SUPPORT_IT
exit
```

Ensuite pour les ports, toujours en conf t :

```
interface range gi1/0/2 - 1/0/23
switchport mode access
switchport access vlan 2
```

On peut recommencer ensuite pour le vlan Commercial.

```
E5_SWITCH1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48, Te1/0/1
                                                Te1/0/2
2    SUPPORT-IT                       active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
3    COMMERCIAL_1                     active    Gi1/0/12, Gi1/0/13, Gi1/0/14
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
11   COMPTABILITE                     active
66   VLAN_GESTION                     active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

2. Création des trunks

Certains services ont besoin d'un trunk pour accéder à un autre switch, c'est le cas du service Comptabilité.

De ce fait, il faudra aussi créer le vlan COMPTABILITE, vlan 11, mais ne pas lui attribuer de port en access mode.
Pour le mettre en trunk, il faudra utiliser la commande

interface Gi1/0/25
switchport mode trunk
switchport trunk allowed vlan 11

Même manipulation pour le vlan 66, qui sera notre vlan de gestion du switch #1 et #2, sur le port Gi1/0/24
Même manipulation aussi pour le vlan 3, qui sera sur le port Gi1/0/11.

Et enfin, il faudra faire la même manipulation sur le port Gi1/0/1, mais cette fois ci, il faudra allowed les vlan 2,3,11 et 66, c'est ce trunk qui permettra à tous nos vlan de remonter au routeur.

```
E5_SWITCH1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         trunking      1
Gi1/0/11    on               802.1q         trunking      1
Gi1/0/24    on               802.1q         trunking      1
Gi1/0/25    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/0/1     2-3,11,66
Gi1/0/11    3
Gi1/0/24    66
Gi1/0/25    11

Port        Vlans allowed and active in management domain
Gi1/0/1     2-3,11,66
Gi1/0/11    3
Gi1/0/24    66
Gi1/0/25    11

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     2-3,11,66
Gi1/0/11    3
Gi1/0/24    66

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/25    11
```

3. Sécurité

Enfin, pour finir, nous allons activer le SSH, mais ajouter une règle pour que seulement les clients câblé sur le vlan 2, puisse avoir accès à la gestion du switch. l'IP pour le SSH sera intégré au vlan 66.

Tout d'abord nous allons créer la règle ACL_ACCES_SSH, permettant uniquement aux membres de notre réseau choisis, d'accéder au ssh.

Pour ce faire, via les commandes

ip access-list standard ACL_ACCES_SSH
permit 192.168.20.00 0.0.0.255
deny any

Ensuite, nous allons créer un utilisateur local pour l'accès en SSH.
En configuration terminal, nous allons créer l'utilisateur admin via la commande

username admin privilege 15 motdepasse

Une fois fait on oublie pas de configurer le nom de domain, avec la commande ip domain-name techcop.local . Puis, nous allons ensuite mettre en place le SSH.

Pour commencer, il faudra générer une clef RSA de taille 2048, via la commande crypto key generate rsa.

Ensuite, toujours en configuration terminal, nous allons activer le SSH

line vty 0 15
transport input ssh
login local
access-class ACL_ACCES_SSH in
exit

Et pour finir, on reste en configuration terminal, et nous allons mettre une IP de gestion sur le vlan 66 via ces commandes :

interface vlan 66
ip address 192.168.66.98 255.255.255.240
no shutdown

Il manquera plus que la commande write memory sauvegarder nos modifications, et le SSH sera fonctionnel.

```
E5_SWITCH1#show access-list
Standard IP access list ACL_ACCES_SSH
    10 permit 192.168.20.0, wildcard bits 0.0.0.255
    20 deny   any log
Extended IP access list preauth_ipv4_acl (per-user)
    10 permit udp any any eq domain
    20 permit tcp any any eq domain
    30 permit udp any eq bootps any
    40 permit udp any any eq bootpc
    50 permit udp any eq bootpc any
    60 deny ip any any
IPv6 access list preauth_ipv6_acl (per-user)
    permit udp any any eq domain sequence 10
    permit tcp any any eq domain sequence 20
    permit icmp any any nd-ns sequence 30
    permit icmp any any nd-na sequence 40
    permit icmp any any router-solicitation sequence 50
    permit icmp any any router-advertisement sequence 60
    permit icmp any any redirect sequence 70
    permit udp any eq 547 any eq 546 sequence 80
    permit udp any eq 546 any eq 547 sequence 90
    deny ipv6 any any sequence 100
```

VIII- Switch #2 (Cisco 2960-X)

1. Création des vlans

Le switch #2 va être configuré de la même manière que le switch #1, cependant, avec quelques détails qui diffèrent.

Il faudra créer à nouveau les vlan 3 COMMERCIAL et 11 COMPTABILITE, et leur définir leurs ports.

Il faudra aussi créer le vlan 66 pour la gestion du switch

```
E5_SWITCH2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/12, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Te1/0/1, Te1/0/2
3    COMMERCIAL_2                     active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10
11   COMPTABILITE                     active    Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17
66   VLAN_GESTION                     active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

2. Création des trunks

Par la suite, il faudra passer le port Gi1/0/11 en trunk, pour laisser passer le vlan 3, le port Gi1/0/18 en trunk, pour laisser passer le vlan 11 et le port Gi1/0/24 en trunk pour laisser passer le vlan 66.

```
E5_SWITCH2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/11    on               802.1q         trunking      1
Gi1/0/18    on               802.1q         trunking      1
Gi1/0/24    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/0/11    3
Gi1/0/18    11
Gi1/0/24    66

Port        Vlans allowed and active in management domain
Gi1/0/11    3
Gi1/0/18    11
Gi1/0/24    66

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/11    3
Gi1/0/18    11
Gi1/0/24    66
```

3. Sécurité

Enfin, il faudra aussi activer le SSH. Pour ce faire, c'est la même manipulation que sur le switch #1.

Les commandes et l'ACL sont les même, cependant, cette fois ci, l'IP de gestion sur le vlan 66 sera 192.168.66.99 255.255.255.240

IX- Routeur (Cisco 1921)

1. Routing

Pour que nos clients sur les vlan 2,3 et 11 puissent accéder à notre réseau, il faudra créer des routes pour indiquer à pfSense, que les clients se trouvent à tel ou tel endroits, et inversement, indiquer aux clients que pfSense est à tel ou tel chemin.

Pour ce faire, on va devoir d'abord créer notre interface physique qui va relier notre routeur a pfSense.

Une fois la configuration initiale effectuée, on va venir en accès enable, puis en configuration terminal.

Puis avec cette commande, on créer notre interface physique :

```
interface GigabitEthernet0/1
ip address 192.168.40.210 255.255.255.0
no shutdown
```

Par la suite, on va passer aux sous-interfaces pour tout nos vlans

La seule différence, c'est qu'on va devoir encapsuler notre vlan, pour qu'ils puissent tous passer sur le même port

Pour le vlan 2 :

```
interface GigabitEthernet0/0.2
encapsulation dot1Q 2
ip address 192.168.20.190 255.255.255.0
ip address 192.168.10.1 255.255.255.0
```

Vlan 3 :

```
interface GigabitEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.21.190 255.255.255.0
ip address 192.168.10.1 255.255.255.0
```

Vlan 11 :

interface GigabitEthernet0/0.11
encapsulation dot1Q 11
ip address 192.168.22.190 255.255.255.0
ip address 192.168.10.1 255.255.255.0

Et pour finir, le vlan 66

interface GigabitEthernet0/0.66
encapsulation dot1Q 66
ip address 192.168.66.97 255.255.255.240

```
E5_ROUTEUR#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.2       192.168.20.190  YES NVRAM  up                    up
GigabitEthernet0/0.3       192.168.21.190  YES NVRAM  up                    up
GigabitEthernet0/0.11      192.168.22.190  YES manual up                    up
GigabitEthernet0/0.66      192.168.66.97   YES NVRAM  up                    up
GigabitEthernet0/1         192.168.40.210  YES NVRAM  up                    up
```

2. Sécurité

Après avoir défini le nom de domaine du routeur puis générer une clef RSA, on pourra mettre en place, comme sur les switches, le SSH.

Il faudra créer un utilisateur au préalable

username admin privilege 15 secret motdepasse

Puis une fois l'ACL créé, de la même manière que sur les switch, pour autoriser uniquement le vlan 2, à accéder en SSH, on va pouvoir mettre en place l'accès SSH.

```
E5_ROUTEUR#show access-lists
Standard IP access list ACL_ACCES_SSH
    10 permit 192.168.20.0, wildcard bits 0.0.0.255
    20 deny   any log
```

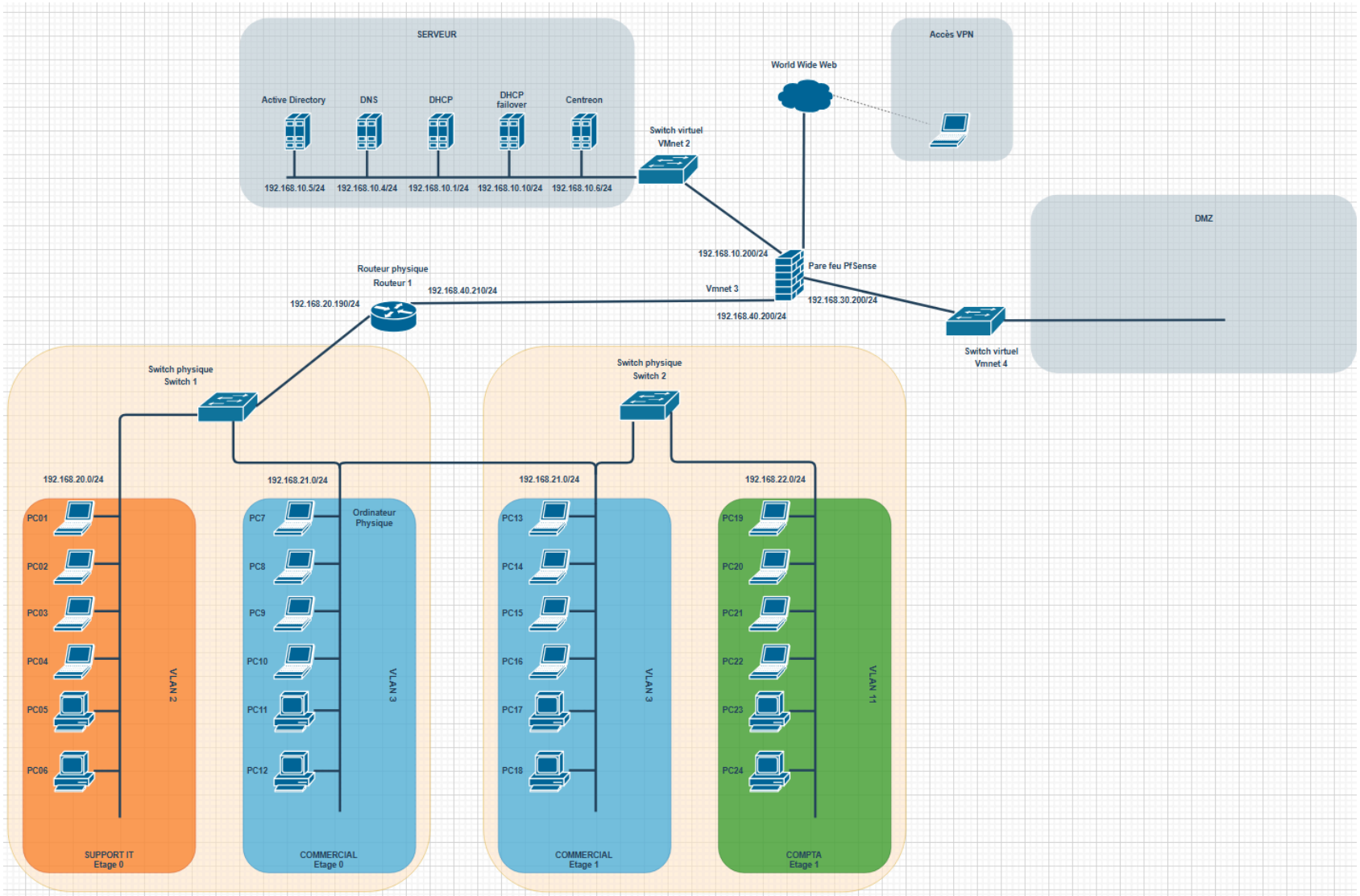
```
conf t
ip ssh source-interface GigabitEthernet0/0.66
line vty 0 15
transport input ssh
login local
access-class SSH_ACCES in
exit
```

Nous pouvons à présent nous connecter en SSH à l'adresse 192.168.66.97

Pour finir, il ne restera plus qu’à suivre le schéma de câblage pour câbler les trunks entre eux, puis câbler les clients sur les switches pour que tout fonctionne.

X- Annexes

1. Annexe n°1 : Schéma réseau



2. Annexe n°2 : Plan de câblage