Projet SCOP-TI

Amélioration d'une infrastructure informatique

Sommaire

I – Présentation du projet

A/ Contexte

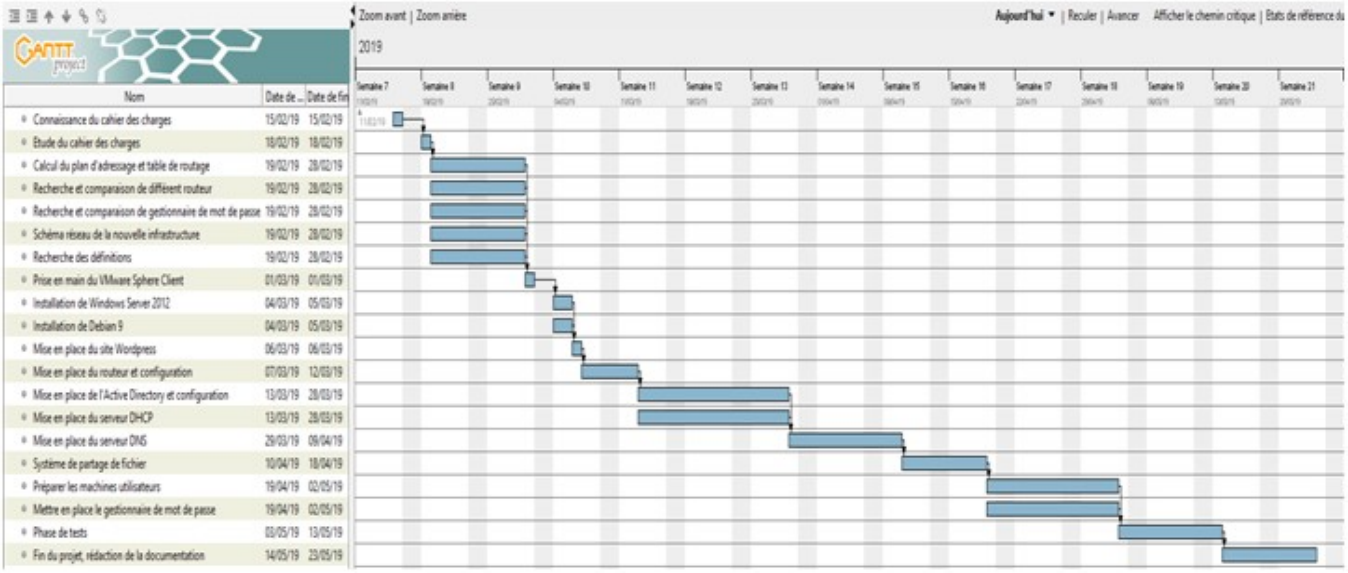
Vous venez d'intégrer l'équipe d'administration systèmes et réseaux de la SCOP et vous êtes en charge de la migration et de l'amélioration du SI. L'infrastructure informatique est vieillissante. L'entreprise dispose de 60 postes clients sous Windows 7 et d'un vieux serveur servant aux sauvegardes.

B/ Objectifs

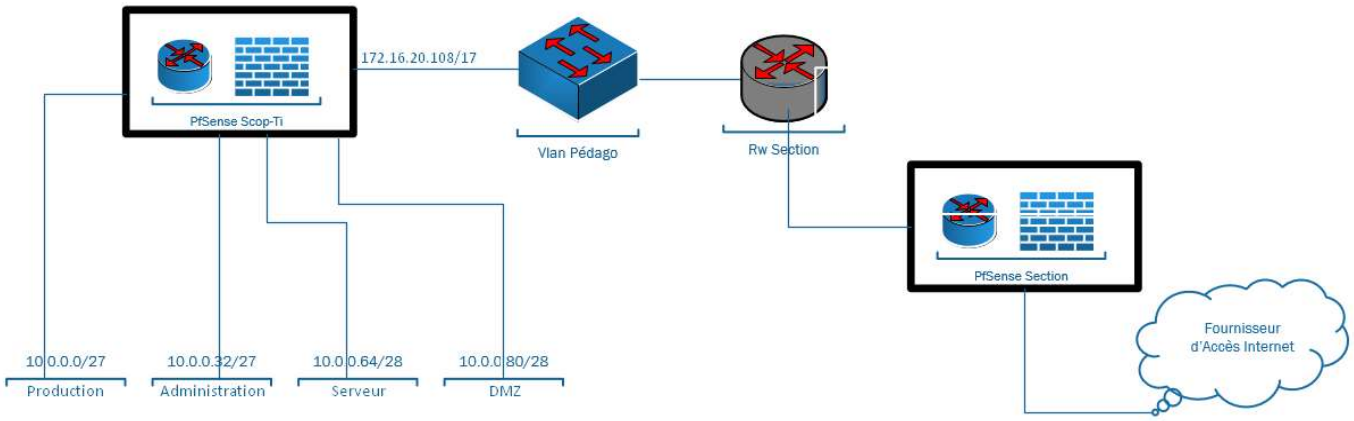
Les différentes manipulations seront effectuées virtuellement dans la ferme de serveurs sous VMware vSphere 5.

L'objectif de notre projet est de créer 4 sous-réseaux (Production, Administratif, Serveurs, DMZ) séparé par un routeur. Dans le réseau Serveurs, il faudra créer un serveur Windows Server 2016 avec : Active Directory, DHCP, DNS faisant autorité, partage de fichiers. Dans le réseau DMZ, il faudra créer un serveur Débian pour héberger le site Web de l'entreprise. Il faudra créer un serveur Débian pour le DNS récursif ainsi qu'un dossier partagé par utilisateur et par groupe avec les droits nécessaire. Il faudra mettre en place un service de sauvegarde sur un NAS Synology, ainsi qu'avoir des mots de passe fort sur tous les équipements stocké dans un gestionnaire de mots de passe.

C/ Diagramme prévisionnel de Gantt



D/ Schéma réseau



E/ Plan d'adressage réseau

Nom du ss réseau	Nombre hôtes	Masque	@ sous réseau	@ Diffusion
Production	30	/27	10.0.0.0	10.0.0.31
Administration	30	/27	10.0.0.32	10.0.0.63
Serveur	14	/28	10.0.0.64	10.0.0.79
DMZ	14	/28	10.0.0.80	10.0.0.95

F/ Table de routage de PfSense Scop-Ti

Nom sous-réseau	Destination	Masque	Passerelle	Interface
Production	10.0.0.0	/27	10.0.0.30	10.0.0.30
Administratif	10.0.0.32	/27	10.0.0.62	10.0.0.62
Serveur	10.0.0.64	/28	10.0.0.78	10.0.0.78
DMZ	10.0.0.80	/28	10.0.0.94	10.0.0.94
Route par défaut	0.0.0.0	/0	172.16.127.254	172.16.20.107

II – Déroulement du projet

A/ Installation du routeur PfSense

Rappel sur qu'est-ce qu'un routeur :
Le routeur est un appareil physique ou virtuel qui fait la liaison entre Internet et les terminaux rattachés à cette dernière. Sa principale fonction est de router les flux Internet sur les réseaux.

Nous avons choisi de faire un routeur PfSense. C'est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise un pare-feu, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il s'administre à distance depuis une interface web ce qui rend la prise en main plus agréable.

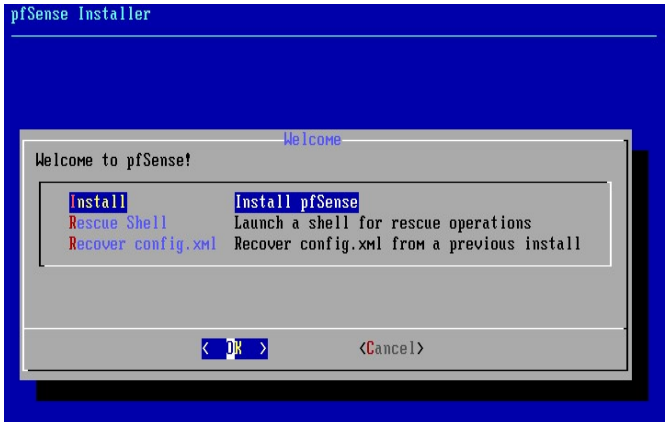
Configuration requise :

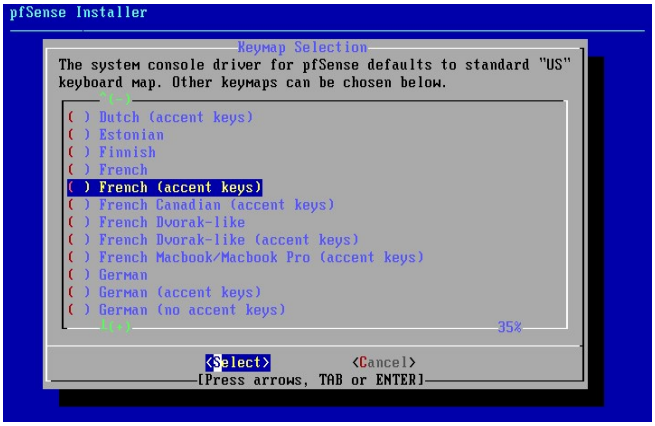
	Minimale	Recommandée
Processeur	500 MHz	1 GHz
Mémoire vive	256 Mo	1 Go
Stockage	> 1 Go	

Tout d'abord, nous avons crée une nouvelle machine virtuel avec :

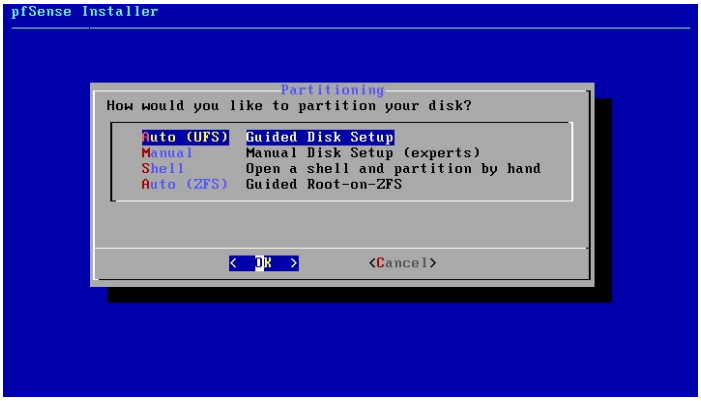
- l'image ISO de pfSense téléchargeable depuis le site officiel
- 5 cartes réseau
- 1 Go de RAM
- 8 Go d'espace de stockage

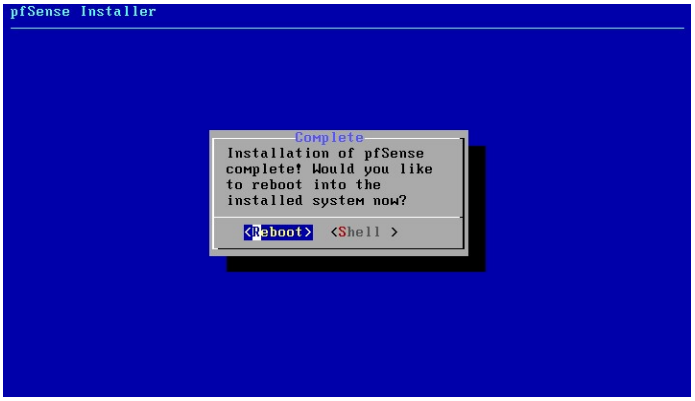
Nous allons démarrer la machine et lancer l'installation. Pour une utilisation du clavier en français faite comme ci-dessous et continuer avec « fr.acc.kbd keymap » :





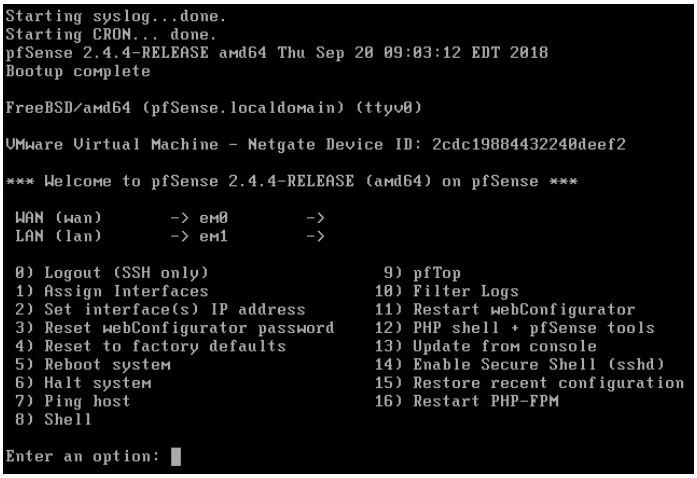
Il va falloir partitionner le disque et il sera fait de manière automatique et enfin lancer le redémarrage.

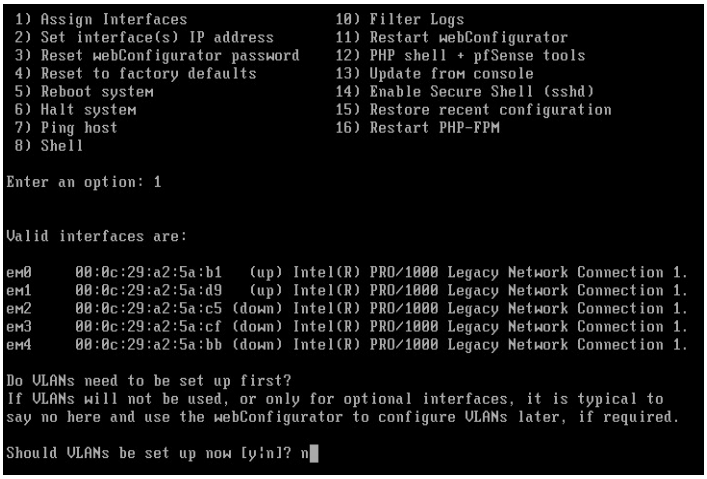




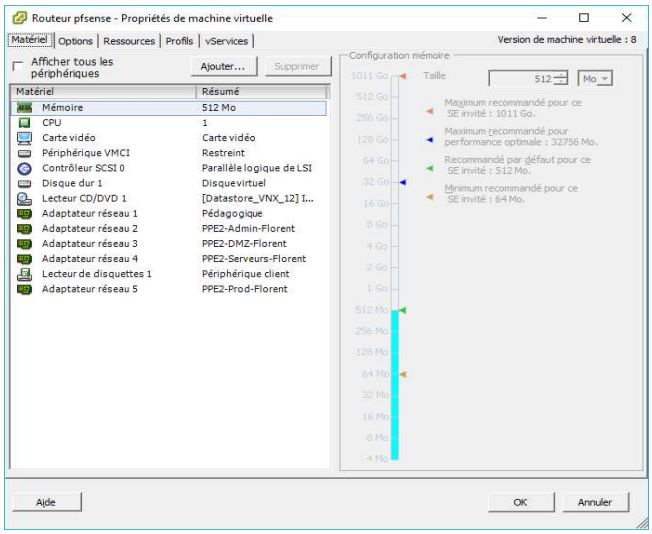
Une fois le redémarrage fait, on va pouvoir assigner les interfaces de notre machine virtuelle aux interfaces du routeur en choisissant l'option « **1** ».

Il va aussi nous demandez si nous voulons configurez des interfaces VLAN mais cela ne sera pas utile pour notre projet donc mettre « **n** ».





Il va falloir entrer le nom des interfaces correspondant au WAN[1], au LAN[2] et les interfaces restantes aux options en fonction des réseaux attribués dans les paramètres de la machine virtuelle, puis valider :




```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 a or nothing if finished): em4

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4

Do you want to proceed [y|n]? y
```

Ensuite entrer l'option « **2** » pour configurer les adresses IP sur chaque interfaces, puis sur « **1** » pour choisir l'interface WAN :

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.16.20.108

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 17

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.127.254

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
 Restarting webConfigurator...

The IPv4 WAN address has been set to 172.16.20.108/17

Press <ENTER> to continue.
```

[1] *Interfaces WAN (Wide Area Network) : réseau informatique ou réseau de télécommunication couvrant une grande zone géographique (Internet).*

[2] *Interfaces LAN (Local Area network) : utilisée pour connecter les câbles de connexion aux périphériques de réseau local, tels que des ordinateurs et des commutateurs dans une zone limitée.*

Il faudra refaire la même manipulation **pour chaque interface** pour obtenir ceci :

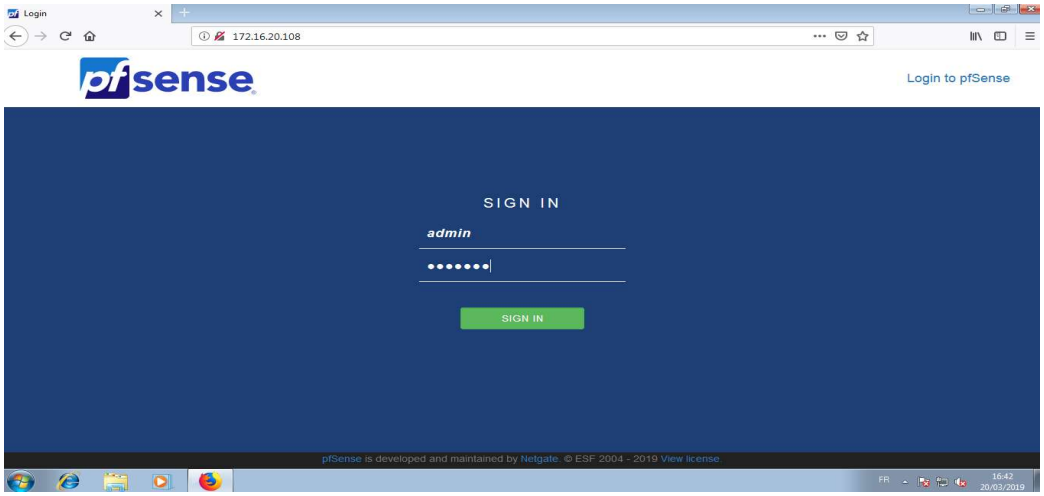
```
The IPv4 OPT3 address has been set to 10.0.0.30/27

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 49b344910cd909f2f6b0

*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 172.16.20.108/17
 LAN (lan)       -> em1        -> v4: 10.0.0.62/27
 OPT1 (opt1)     -> em2        -> v4: 10.0.0.94/28
 OPT2 (opt2)     -> em3        -> v4: 10.0.0.78/28
 OPT3 (opt3)     -> em4        -> v4: 10.0.0.30/27

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Une fois que toute les interfaces sont configurées, On va faire un **reboot** (« 5 ») pour être sur que tout les paramètres indiquées soient bien pris en compte.

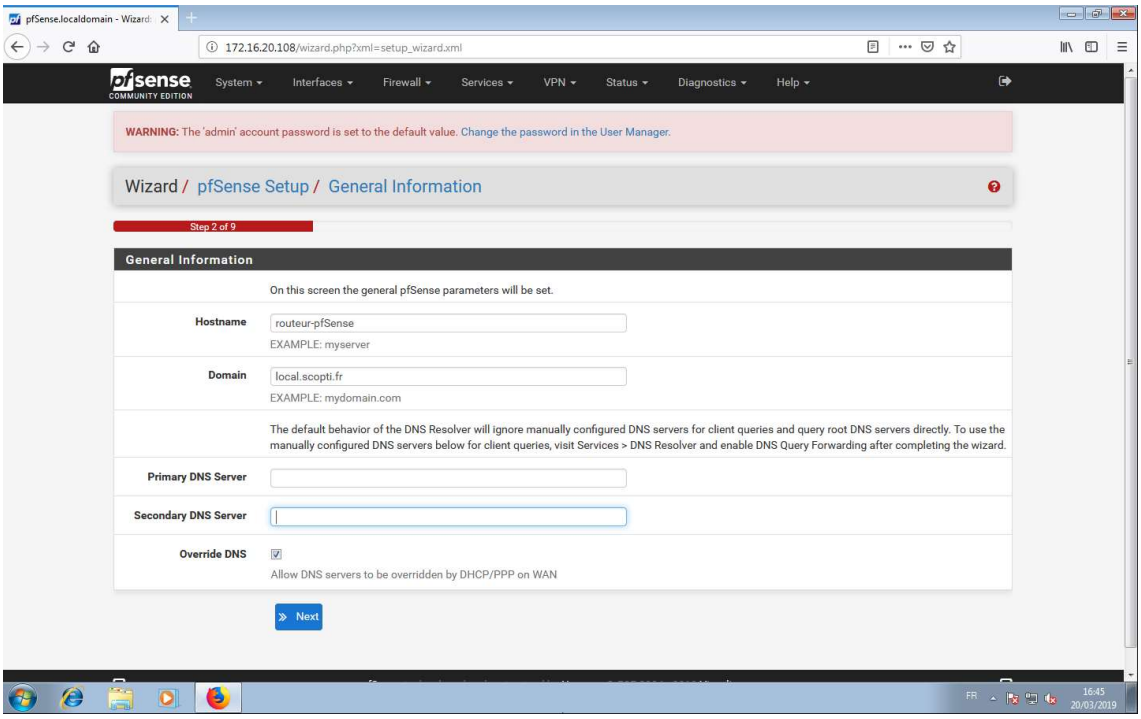
B/ Configuration du routeur par interface Web

Il faut maintenant à partir d'un sous-réseau crée précédemment (Admin, DMZ, Serveur, Prod) :

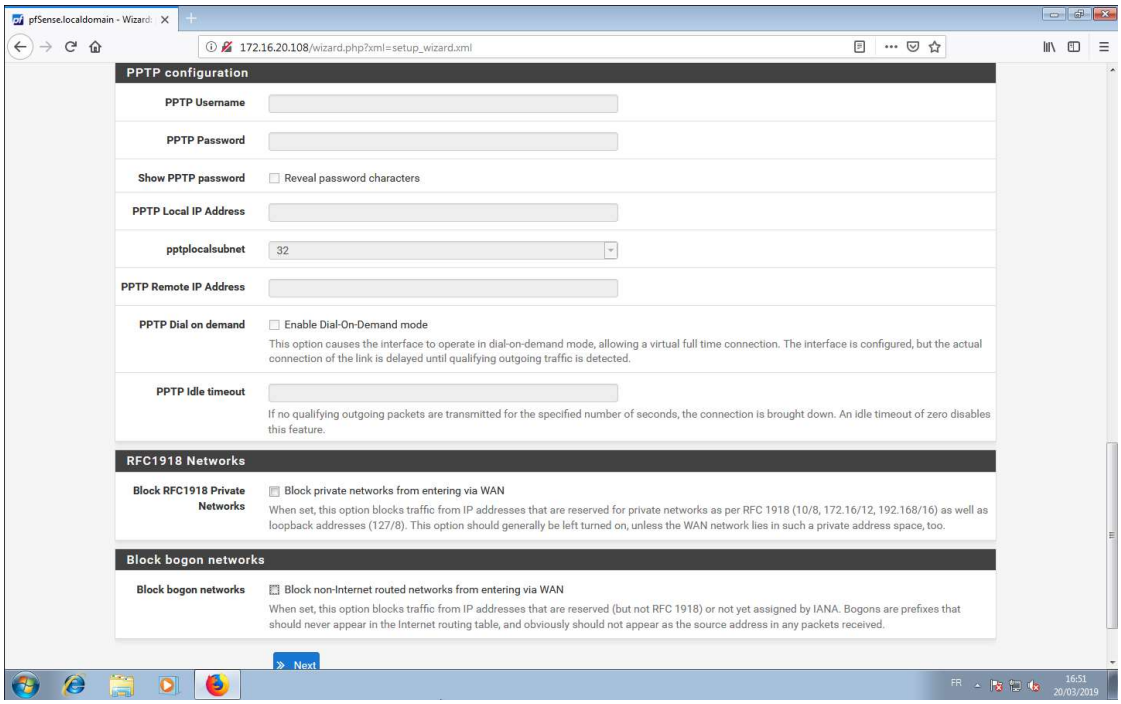
- ➔ **Créer** une nouvelle machine virtuelle possédant une interface graphique.
- ➔ Dans votre navigateur web préféré, **entrer l'adresse ip** correspondant à l'interface **WAN** pour arriver sur la page de configuration.
- ➔ Par défaut : **login** – admin et **mot de passe** – pfsense



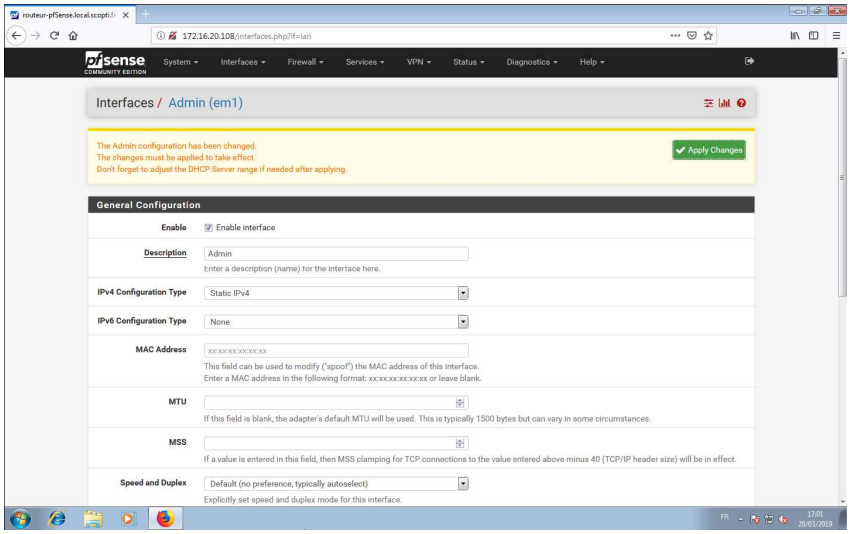
Après connexion, il faut entrer le nom du routeur ainsi que le nom de domaine. On peut aussi renseigner les adresses des serveurs DNS si vous en avez mais il est possible de le faire plus tard.



Il sera aussi possible de configurer l'interface WAN à partir d'ici mais c'est déjà fait pour nous. Il faudra **décocher** les 2 cases pour que les adresses IP privées puissent se connecter par l'interface WAN. **Continuer** l'installation jusqu'au redémarrage.



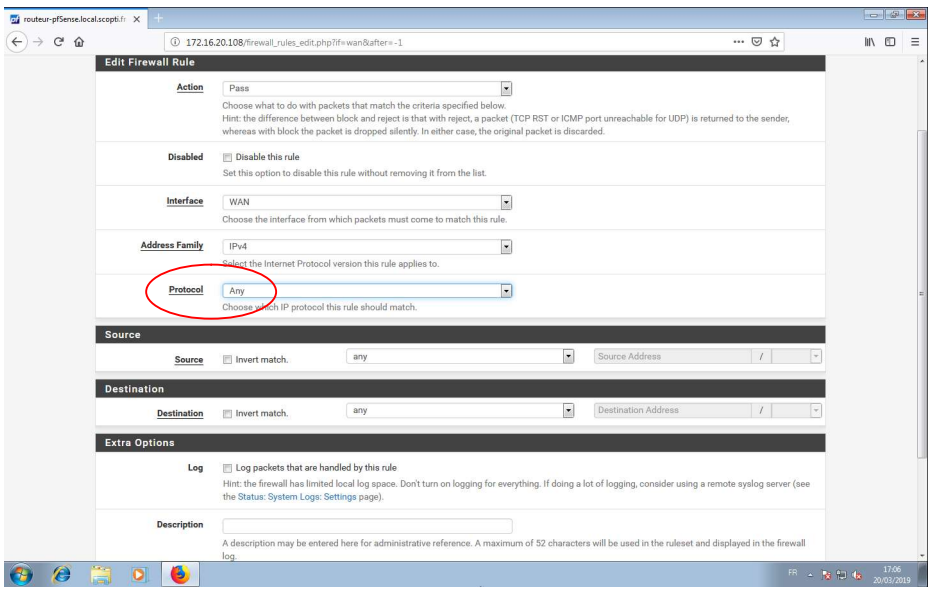
On va pouvoir ensuite **renommer** les interfaces pour plus de **facilité** dans le menu « Interfaces ».



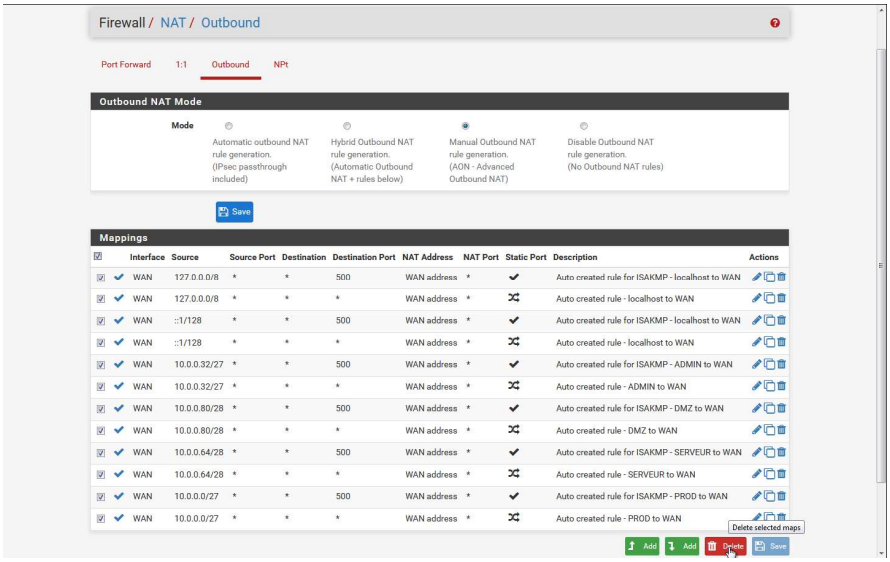
B - 1 – Configuration du pare-feu (Firewall) PfSense

<u>Objectif d'un pare-feu :</u> outil informatique conçu pour protéger les données d'un réseau en définissant une politique de sécurité. Il contrôle les applications et les flux de données.

Dans le menu « Firewall » -> « Rule », créer une nouvelle règle qui autorise tout et supprimer les règles existantes sur chaque interface.



Maintenant dans « Firewall » -> « **NAT** »-> « Outbound » puis sélectionner « Manuel » et supprimer toutes les règles existantes :

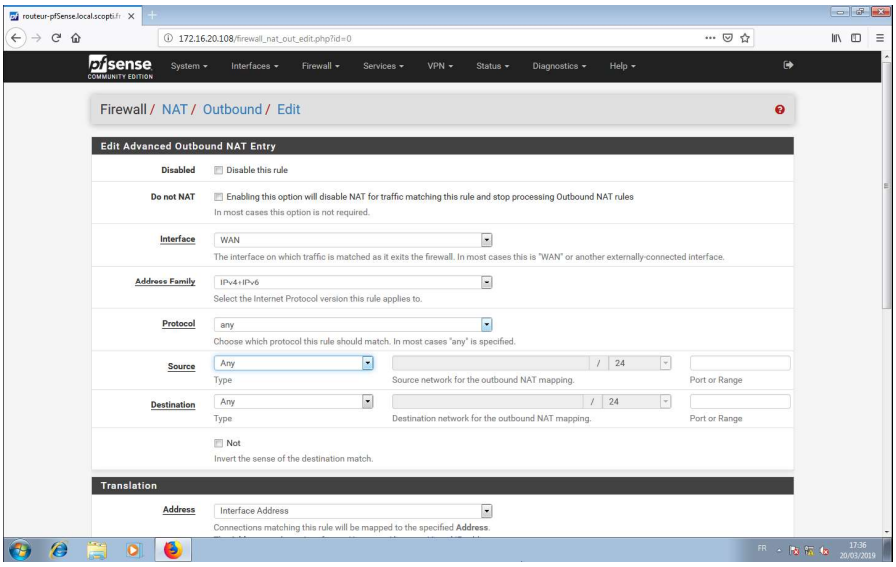


La **Network Address Translation** (NAT) permet de « transformer » une adresse privée en adresse publique afin de pouvoir avoir accès à l'extérieur.

Il y a 2 types NAT :

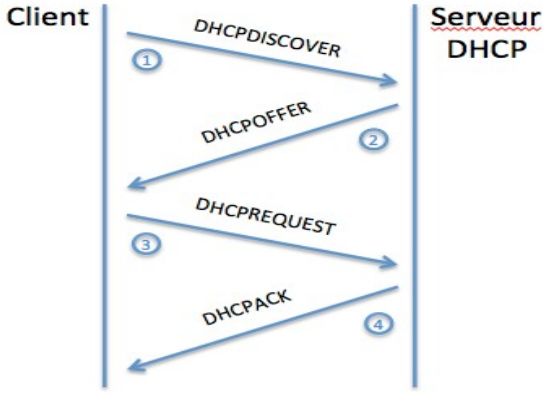
- NAT dynamique : associe des adresses privées à une seule adresse publique, permet d'économiser des adresses.
- NAT statique : une adresse publique pour une adresse privée.

On va créer une nouvelle règle en autorisant tout les protocoles et tous les sous-réseaux :



B – 2 – Configuration de l'agent relais DHCP

Protocole DHCP :



1/ DHCP Discover : le poste client va emmètre une trame de diffusion pour trouver un serveur DHCP

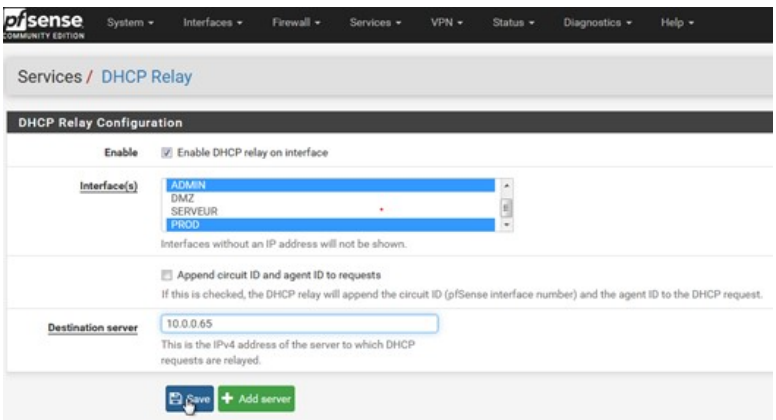
2/ DHCP Offer : le serveur va proposer une configuration réseau au client (adresse IP, masque, passerelle, ...)

3/ DHCP Request : le client va signaler au serveur qu'il accepte la configuration.

4/ DHCP Ack : le serveur indique au client que l'ensemble est validé et que l'échange peut terminer.

L'agent relais DHCP est un programme activé sur une ou plusieurs interfaces de la machine servant de relais DHCP au client. Il sera capable de relayer la trame de diffusion (DHCP Discover) dans les autres sous réseaux et ainsi, on peut gérer plusieurs sous-réseaux avec un seul serveur DHCP.

Pour configurer le relais DHCP, il faut aller dans le menu « Services » -> « DHCP Relay » en sélectionnant les sous-réseaux voulu et l'adresse IP du serveur DHCP.

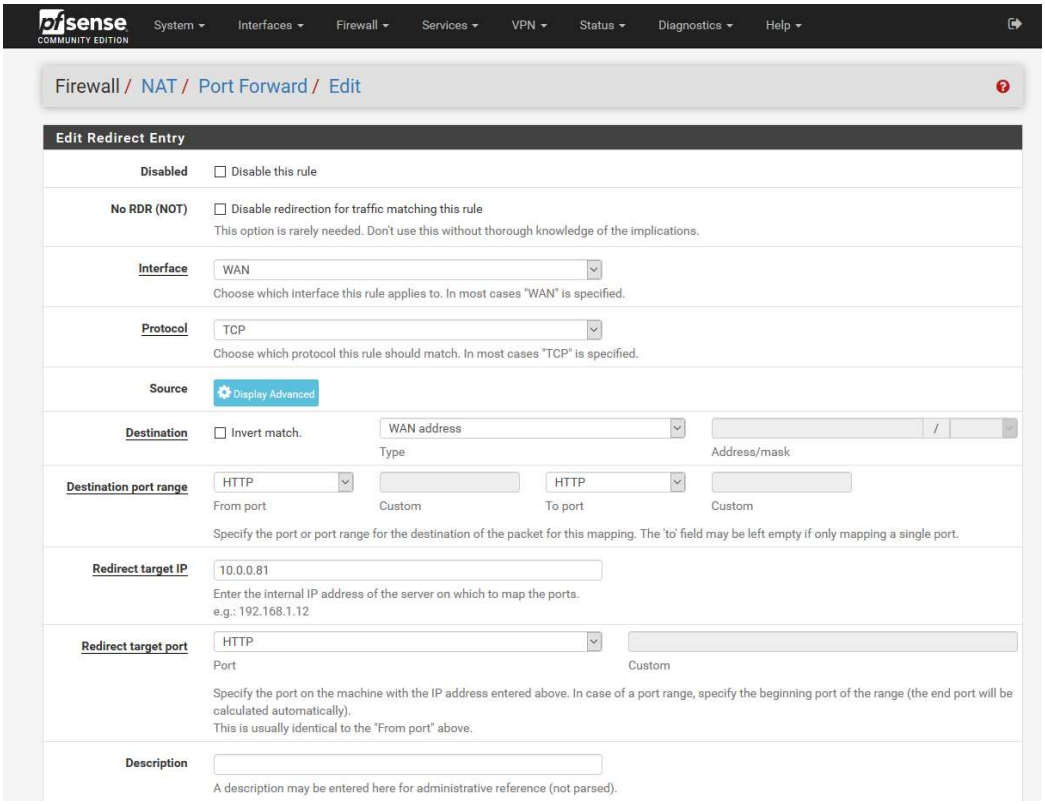


B – 3 – Redirection de port

La redirection de port consiste à rediriger des paquets réseaux reçus sur un port donné d'un ordinateur ou un équipement réseau vers un autre appareil ou réseau sur un port donné. C'est utile pour accéder à un périphérique ou à un service connecté à Internet à partir de n'importe où dans le monde.

Nous allons faire une **redirection de port** dans le menu « System/Adavanced/ Admin Acces » en commençant par changer le port d'accès à l'interface Web qui est **8080** par défaut.

On va maintenant faire en sorte que tout ce qui arrive par l'interface WAN sur le port 8080 soit **redirigé** vers le site Web qui se trouve dans le sous-réseau **DMZ**



Zone démilitarisée (DMZ) : c'est un sous-réseau qui est séparé du réseau local et isolé par un pare-feu. Il permet de mettre les machines qui sont accessibles depuis Internet et qui non pas besoin d'accéder au réseau local.

C/ Mise en place du site Web

C – 1 – Installation du site

Tout d'abord, nous avons crée une machine virtuel (VMWare Workstation 14) sous Debian9 et lui attribuer une configuration IP fonctionnelle. Une fois installé, nous allons mettre à jour le système :

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

On installe ensuite apache2, php7.0, php7.0-mysql, serveur mysql :

```
$ sudo apt-get install apache2 php7.0 php7.0-mysql mysql-server
```

On redémarre le service apache2 :

```
$ sudo service apache2 restart
```

On télécharge ensuite Wordpress depuis le site officiel :

```
$ wget https://fr.wordpress.org/wordpress-5.1-fr_FR.tar.gz
```

On désarchive le dossier Wordpress :

```
$ tar zxvf wordpress-5.1-fr_FR.tar.gz
```

On supprime le dossier html pour y mettre Wordpress :

```
$ sudo rm –R /var/www/html
```

On copie le dossier désarchivé dans le dossier par défaut d'apache2 :

```
$ sudo cp –R wordpress /var/www/html
```

On attribue ensuite l'utilisateur www-data et le groupe www-data comme propriétaires du dossier /var/www/html :

```
$ sudo chown -R www-data:www-data /var/www/html/
```

On démarre le serveur mysql :

```
$ sudo service mysql start
```

On change ensuite le mot de passe de l'utilisateur root de mysql :

```
$ sudo /usr/bin/mysql_secure_installation
```

On se connecte en root à mysql :

```
$ mysql –u root –p
```

(Si vous êtes connecté en root sur votre machine, il n'est plus nécessaire d'indiquer le mot de passe pour l'utilisateur root de mysql depuis debian 9)

On crée ensuite un nouvel utilisateur qui servira à Wordpress :

```
mysql> CREATE USER scopti@localhost IDENTIFIED BY '
@t&SCaub$b#J';
```

On crée ensuite la base de données qui sera utilisé par Wordpress :

```
mysql> CREATE DATABASE scopti;
```

Puis on donne un accès total à l'utilisateur « scopti » sur la base de données scopti :

```
mysql> GRANT ALL PRIVILEGES ON scopti.* TO scopti@localhost;
```

Une fois les commandes tapées, il faut taper l'adresse IP de votre serveur qu'on a précédemment configuré sur un navigateur Web, cela nous enverra sur l'interface Web et où il faudra rentrer des données.

C – 2 – Sécurisation du site

- ➔ Il faut **supprimer le compte admin** car il est proposé par défaut donc massivement utilisé par les pirates pour accéder au site. Il faut créer un nouvel utilisateur avec tout les droits administrateurs pour pouvoir le supprimer. **Attention** avant de supprimer le compte admin, il faut attribuer tous les articles et les liens au nouvel utilisateur crée.
- ➔ Modifier l'adresse de connexion qui elle aussi est par défaut.
- ➔ Toujours être à jour

III – Tutoriel

Au préalable, nous avons installé un Windows Server 2012 sur une machine virtuelle (VMWare vSphere).

A/ Installation et configuration de l'AD/DNS

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

Pour installer l'AD (Active Directory), dans le Gestionnaire de serveur cliquez sur « **Gérer** » (en haut à droite).
Ensuite, cliquez sur « **Ajouter des rôles et des fonctionnalités** ».

Cliquez sur « **Suivant** », laissé cocher ce qui est par défaut : Installation basée sur un rôle ou une fonctionnalité, puis cliquez sur « **Suivant** ».

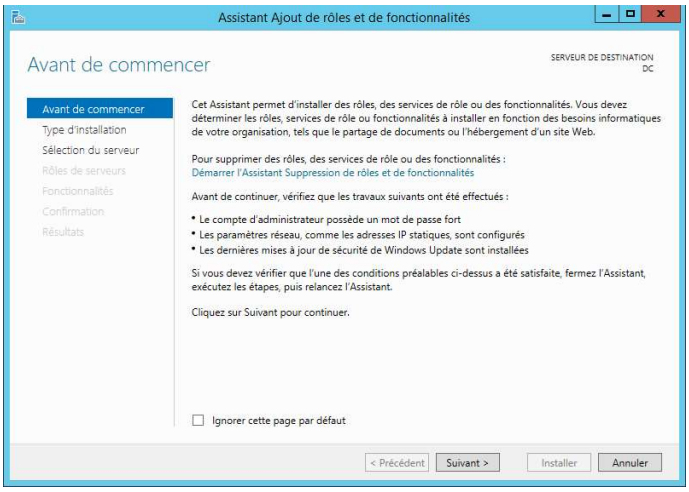
Ensuite, cliquez à nouveau sur « **Suivant** ».

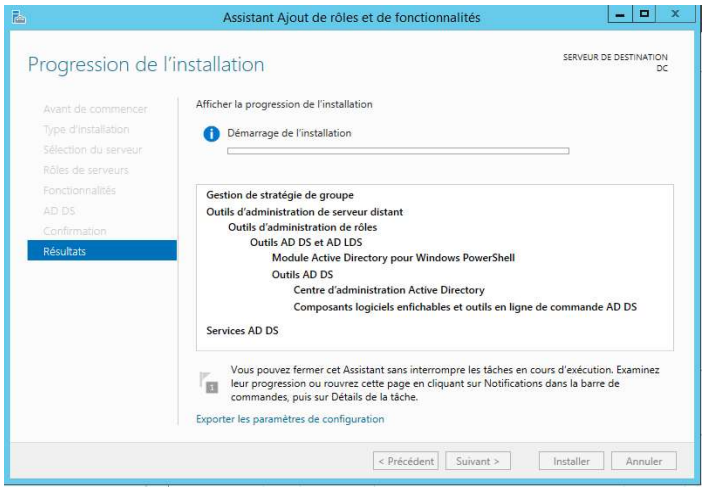
Maintenant, cocher le rôle « **Services AD DS** », puis cliquer sur « **Ajouter des fonctionnalités** ».

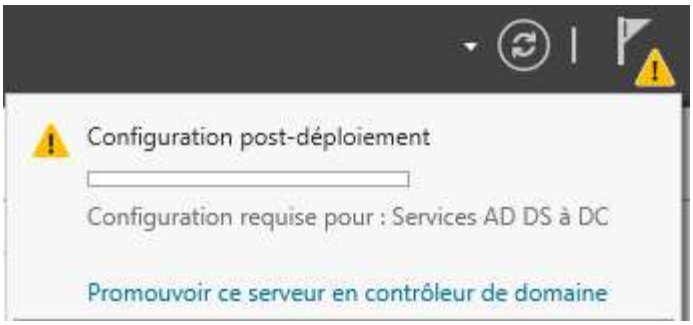
Cliquez ensuite sur « **Suivant** » (3 fois).

Cliquez maintenant sur « **Installer** ».

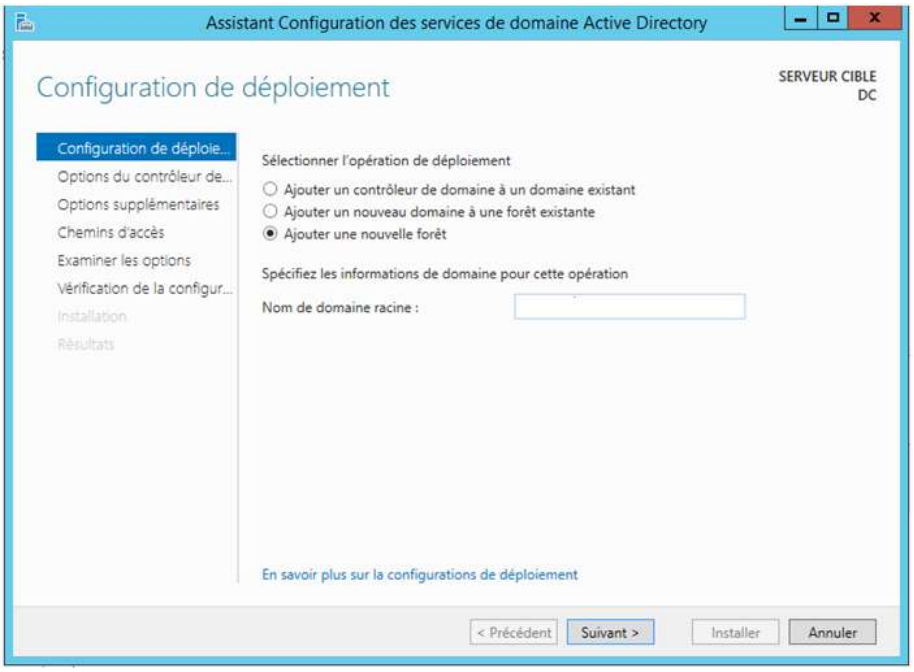
Vous obtenez ceci :





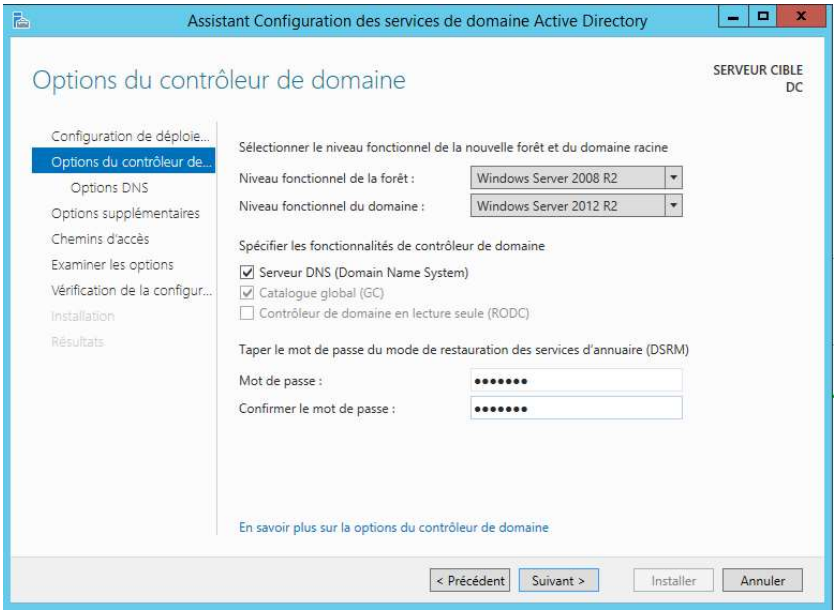


Une fois la configuration terminée, cliquer sur « Fermer ». Nous allons promouvoir ce serveur en contrôleur de domaine, en cliquant sur le drapeau jaune, puis « promouvoir ce serveur en contrôleur de domaine ».



Cliquer sur Ajouter une nouvelle forêt, et renseigner le nom de votre domaine.
Dans mon cas « local.scopti.fr ».

Pour poursuivre, cliquez sur « Suivant ».

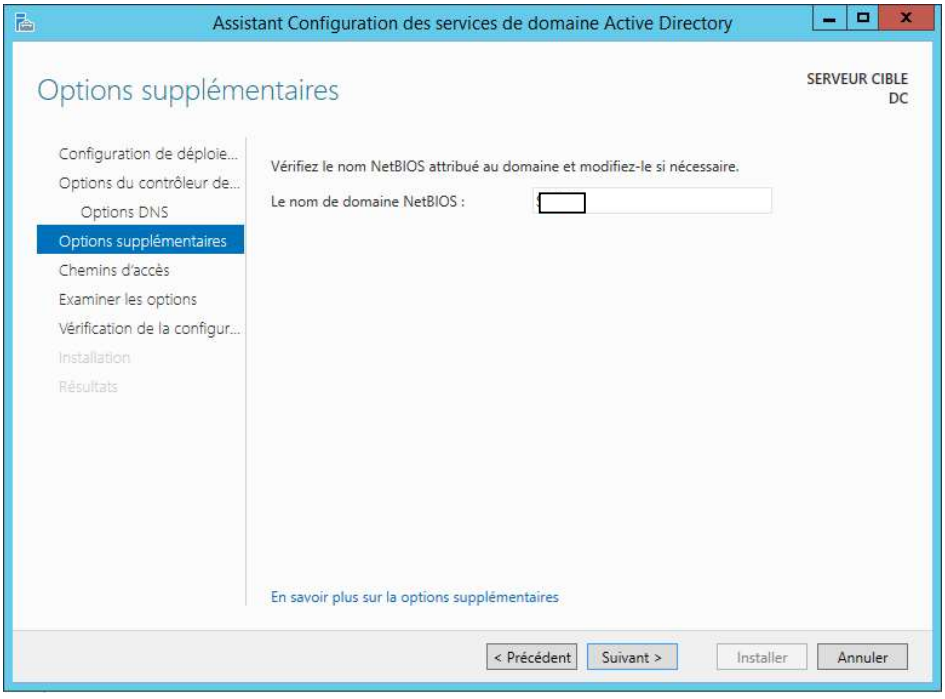


NB : Si dans votre architecture vous disposez d'un serveur antérieur à Windows 2012. Je vous recommande de mettre en niveau fonctionnel de la forêt le nom de l'OS antérieur de votre infrastructure.

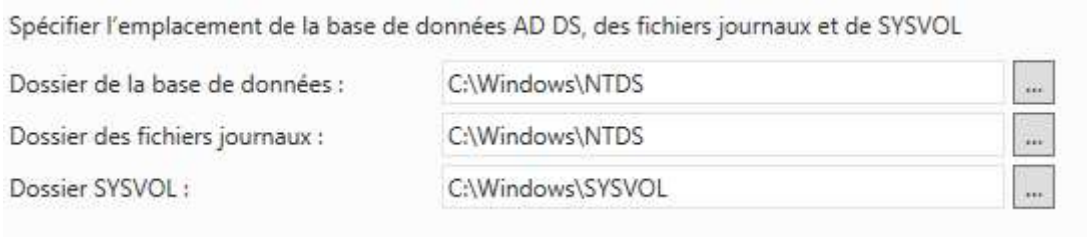
Cliquez sur « Suivant » pour poursuivre

Une erreur apparaît sur l'écran suivant. Ce message survient, car aucun serveur DNS n'est installé sur la machine. Cliquez simplement sur « Suivant » pour le créer

Ensuite, indiquer un nom NetBIOS au domaine « SCOPTI ».



Cliquez sur « Suivant ».
Laisser les valeurs de l'écran suivant par défaut (NTDS et SYSVOL).



Puis cliquez sur « Suivant ».
L'installation est prête et un récapitulatif est affiché pour vérifier la configuration.

Cliquez sur « Suivant ».

Une vérification système est effectuée, cliquer sur « Installer ».

Le serveur va ensuite redémarrer automatiquement.

Le login se fait maintenant avec votre compte et mot de passe du domaine.

Votre contrôleur de domaine est maintenant prêt.

B/ Installation du serveur DHCP sur Windows Serveur 2012

Dans ce tutoriel nous allons voir ensemble une installation complète simpliste de l'outil DHCP sur un Windows Serveur 2012. Cependant pour aller un peu plus loin, il est important de comprendre certaines terminologies.

Terminologie :

Étendue : Une *étendue* est la plage consécutive complète des adresses IP probables d'un réseau. Les étendues désignent généralement un sous-réseau physique unique de votre réseau auquel sont offerts les services DHCP. Les étendues constituent également pour le serveur le principal moyen de gérer la distribution et l'attribution d'adresses IP et de tout autre paramètre de configuration associé aux clients du réseau.

Étendue globale : Une *étendue globale* est un regroupement administratif des étendues pouvant être utilisé pour prendre en charge plusieurs sous-réseaux logiques IP sur le même

sous-réseau physique. Les étendues globales contiennent uniquement une liste d'*étendues membres* ou d'*étendues enfants* qui peuvent être activées ensemble.

Plage d'exclusion : Une *plage d'exclusion* est une séquence limitée d'adresses IP dans une étendue, exclue des offres de service DHCP. Les plages d'exclusion permettent de s'assurer que toutes les adresses de ces plages ne sont pas offertes par le serveur aux clients DHCP de votre réseau.

Pool d'adresses : Une fois que vous avez défini une étendue DHCP et appliqué des plages d'exclusion, les adresses restantes forment le *pool d'adresses* disponible dans l'étendue. Les adresses de pool peuvent faire l'objet d'une affectation dynamique par le serveur aux clients DHCP de votre réseau.

Bail : Un *bail* est un intervalle de temps, spécifié par un serveur DHCP, pendant lequel un ordinateur client peut utiliser une adresse IP affectée. Lorsqu'un bail est accordé à un client, le bail est *actif*. Avant l'expiration du bail, le client doit renouveler le bail de l'adresse auprès du serveur. Un bail devient *inactif* lorsqu'il arrive à expiration ou lorsqu'il est supprimé du serveur. La durée d'un bail détermine sa date d'expiration et la fréquence avec laquelle le client doit le renouveler auprès du serveur.

Réservation : Utilisez une *réservation* pour créer une affectation de bail d'adresse permanente par le serveur DHCP. Les réservations permettent de s'assurer qu'un périphérique matériel précis du sous-réseau peut toujours utiliser la même adresse IP.

Types d'options : Les *types d'options* sont d'autres paramètres de configuration client qu'un serveur DHCP peut affecter lors du service de baux aux clients DHCP.

Classes d'options : Une *classe d'options* est un moyen pour le serveur de continuer à gérer les types d'options proposés aux clients. Lorsqu'une classe d'options est ajoutée au serveur, les clients de cette classe peuvent être fournis en types d'options spécifiques à la classe pour leur configuration.

Avant de commencer :

Il est nécessaire de configurer son serveur en **IP fixe** et de l'avoir renommé. Nommer votre serveur en fonction de la convention de nommage de votre entreprise. Ici, nous installerons le rôle DHCP sur notre contrôleur de domaine, celui-ci porte déjà le nom **sr-serv-WinServ-PPE-serveurDHCP-DNS-AD** et **local.scopti.fr** pour **Domain Controller**.

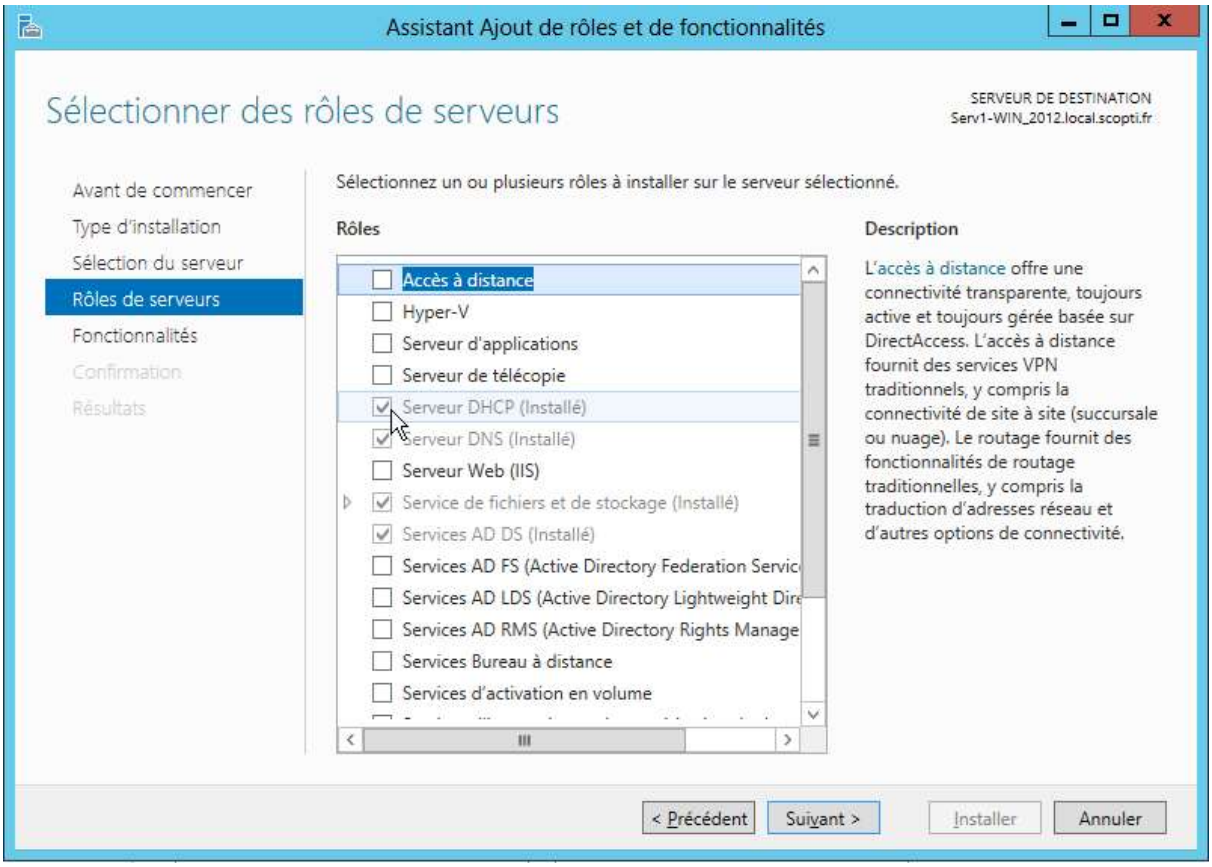
B – 1 - Installation du DHCP

Depuis le **Gestionnaire de serveur**, cliquer sur l'étape **Gérer** puis A**jouter des rôles et fonctionnalités.**

Sélectionner le type d'installation « **Installation basée sur un rôle ou une fonctionnalité** »

Sélectionnez le serveur de destination, pour votre serveur DHCP, et cliquez sur **Suivant**.

Vous êtes maintenant sur la fenêtre de sélection des rôles. Nous allons donc installer le rôle DHCP. Pour cela, cocher simplement **DHCP** dans la fenêtre de sélection des rôles. Enfin, cliquer sur **Suivant**.



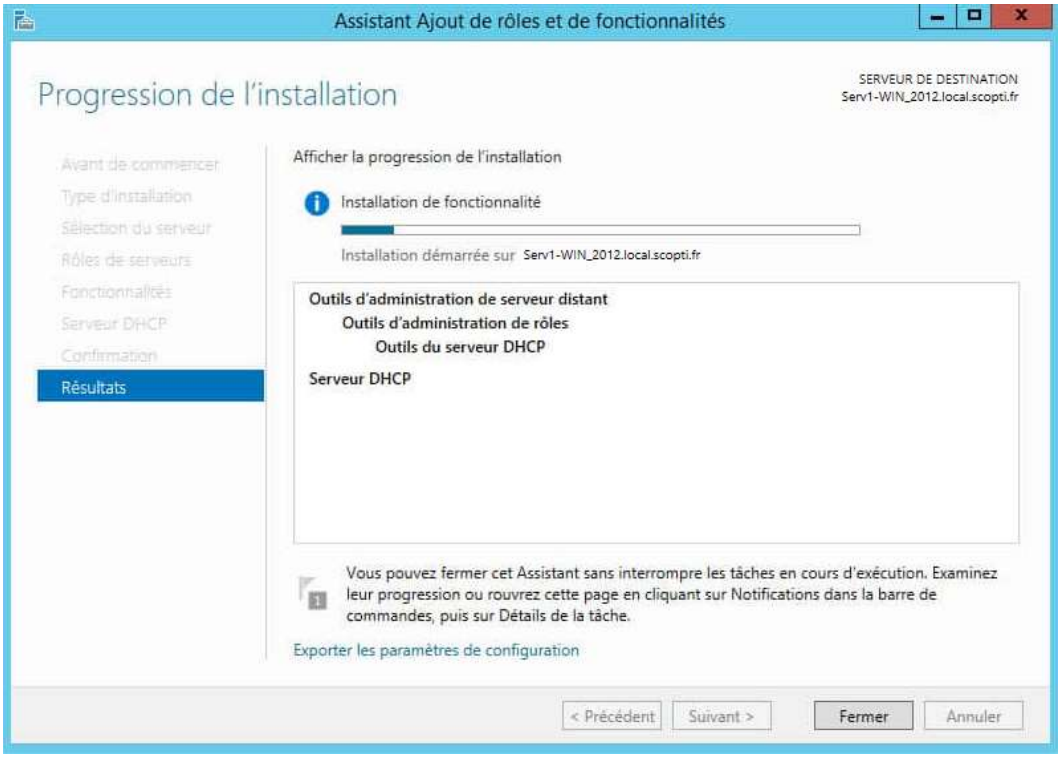
Des fonctionnalités supplémentaires sont automatiquement sélectionnées pour vous, ajoutez-les.

Après avoir ajouté des rôles, vous pouvez ajouter des fonctionnalités supplémentaires. En général, toutes les caractéristiques qui sont nécessaires pour soutenir le rôle de cible sont déjà sélectionnées de sorte que vous pouvez simplement cliquer sur le bouton **Suivant** pour continuer.

Vous aurez alors quelques infos sur le rôle que vous êtes en train d'ajouter (« Serveur DHCP »). Cliquez sur **Suivant** après en avoir pris connaissance.

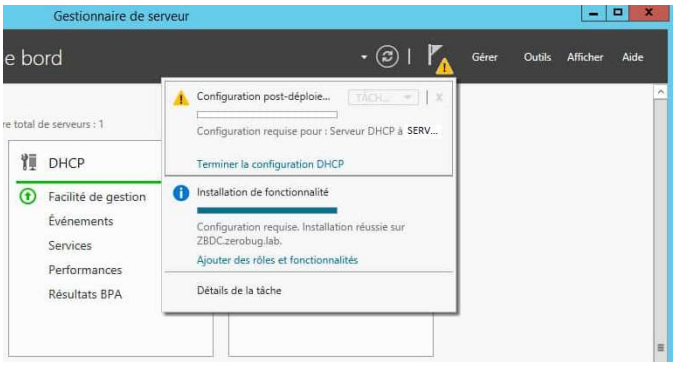
Vous devez maintenant **confirmer** l'ajout du rôle DHCP sur votre serveur. Cliquez sur **Installer**.

Votre serveur est maintenant en cours d'installation, après quelques minutes, l'installation sera terminée. **L'installation du rôle DHCP ne nécessite pas de redémarrage du serveur.**



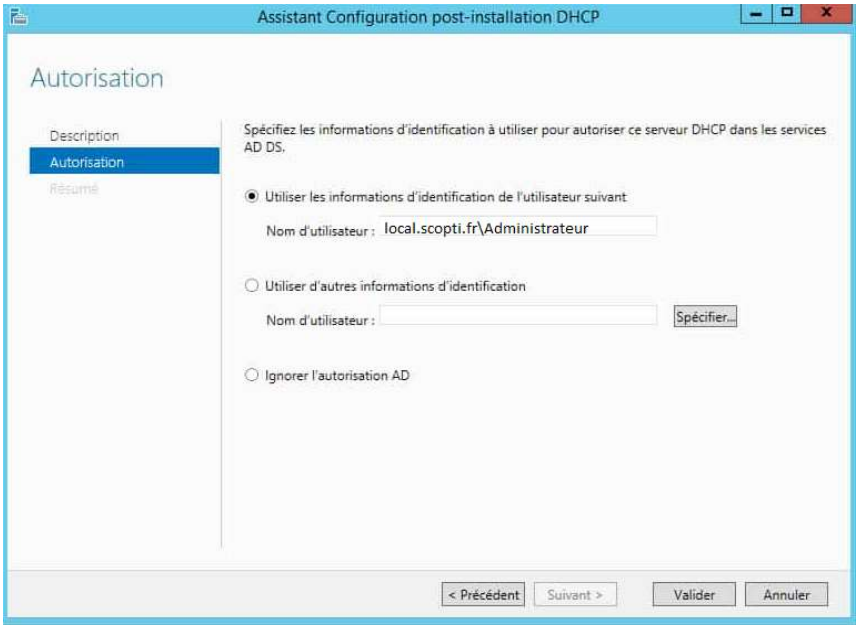
Maintenant que votre serveur DHCP est installé, il faut le configurer. Pour cela, depuis le Gestionnaire de serveur, vous devriez avoir une alerte (Configuration post-déploiement), cliquez sur **Terminer la configuration DHCP**.

B – 2 – Configuration du rôle DHCP



Ici on va autoriser DHCP dans le domaine, pour cela il vous faudra un compte administrateur du domaine.

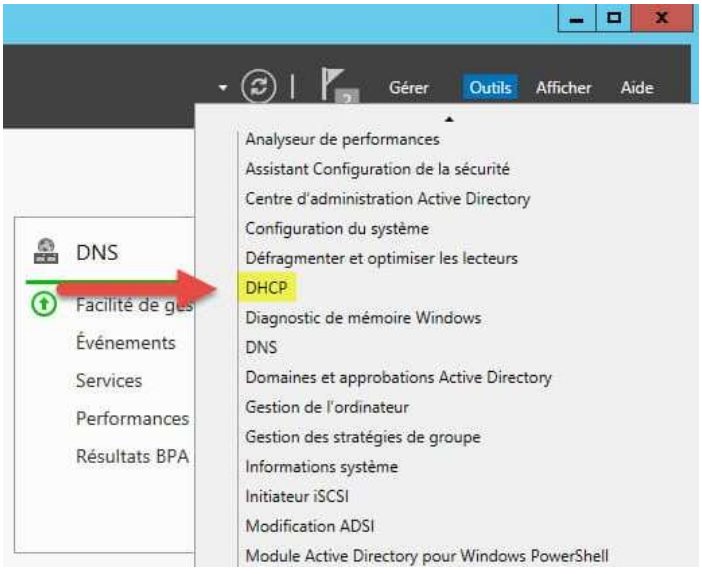
Vous pouvez utiliser le compte sur lequel vous êtes actuellement connecté ou bien un autre compte. Une fois le compte choisi cliquez sur **Valider**.



L'assistant Configuration post installation DHCP va alors créer des groupes de sécurité dans ADDS et autoriser le serveur DHCP. Cliquez sur **Fermer**.

On a passé la partie la plus simple, passons aux choses sérieuses, la configuration des étendues (aussi appelé Scopes).

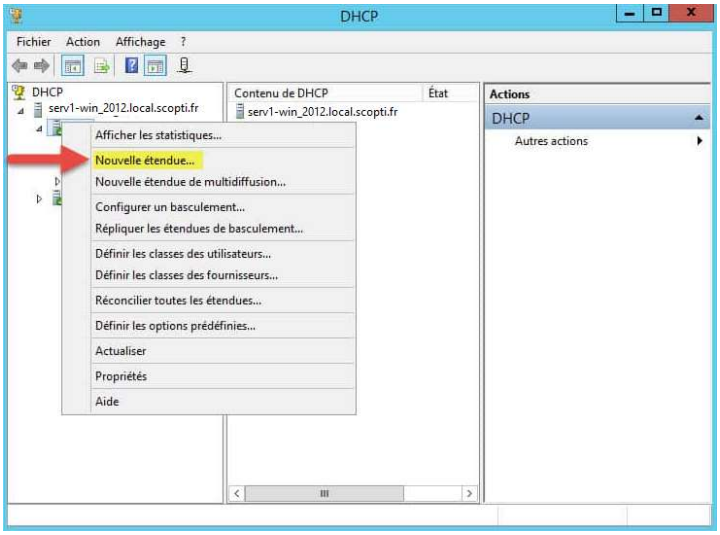
Pour créer vos étendues, lancer la console DHCP via votre gestionnaire de serveur.

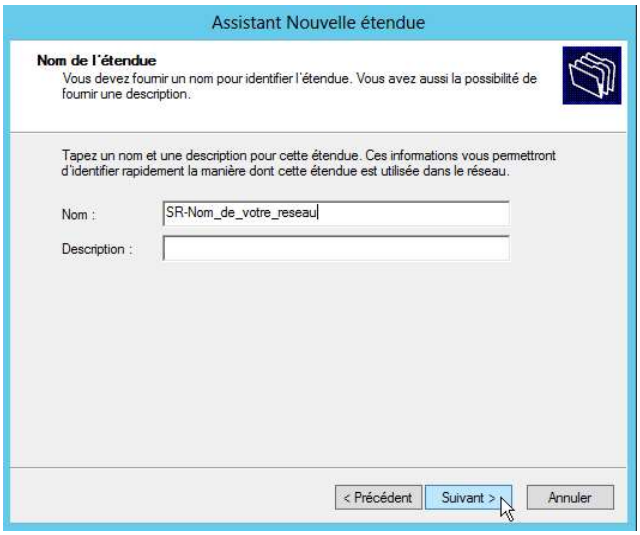


Depuis cette console, vous allez pouvoir **créer vos étendues DHCP**. Nous allons créer notre première étendue IPv4 pour que les clients puissent obtenir une adresse IP automatiquement.

Effectuer un clic droit sur IPv4, puis sélectionner « **Nouvelle étendue… »**.

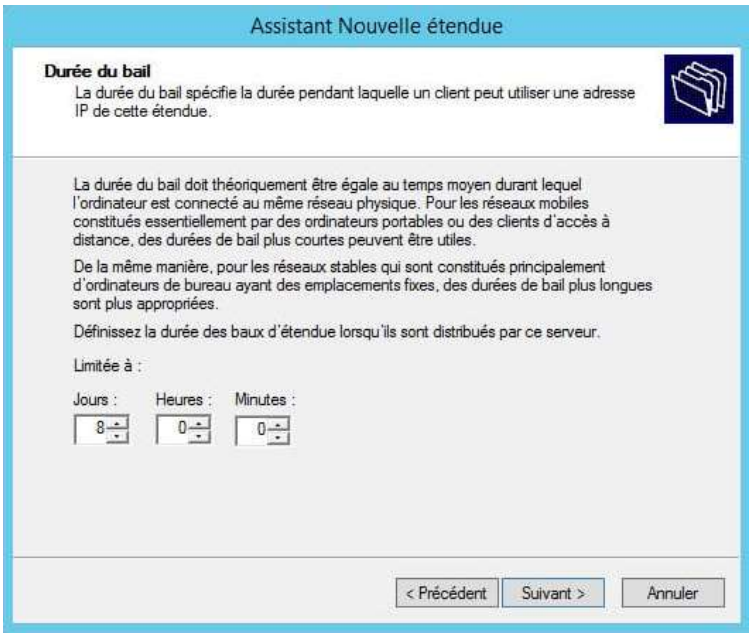
Donnez un nom à votre nouvelle étendue.





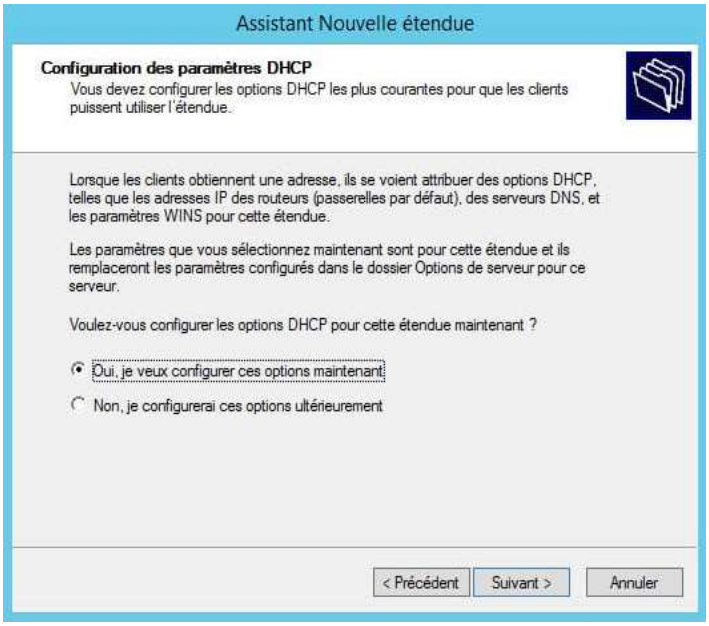
Vous pouvez maintenant définir la plage d'adresses IP pour cette étendue. Cliquez ensuite sur **Suivant**.
Vous pouvez si vous le souhaitez, ajouter une ou plusieurs **plages d'exclusions**. Ce sont les adresses qui ne seront pas distribuées par le serveur DHCP (par exemple son adresse ipv4).

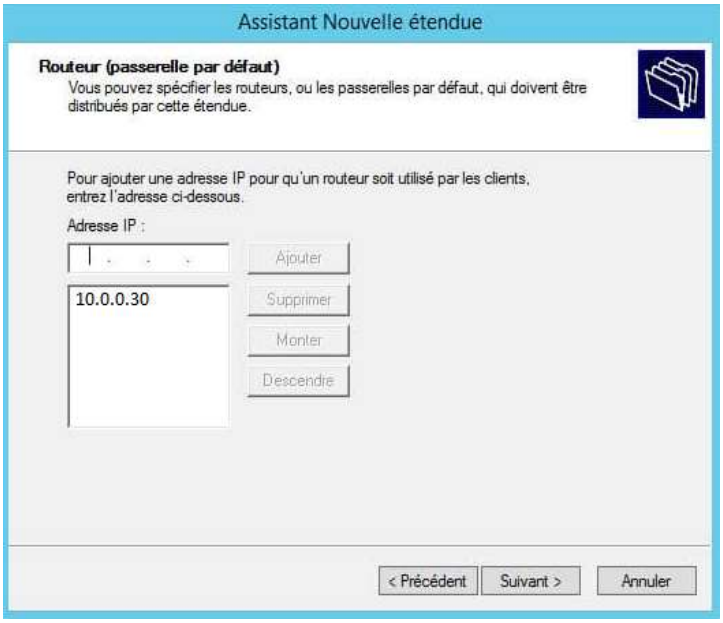
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de l'étendue que vous êtes en train de créer, par défaut, le bail est limité à 8 jours. Vous pouvez le modifier suivant vos besoins. Par exemple si vous créer un serveur DHCP pour un réseau WiFi public, un bail de 24H est suffisant.



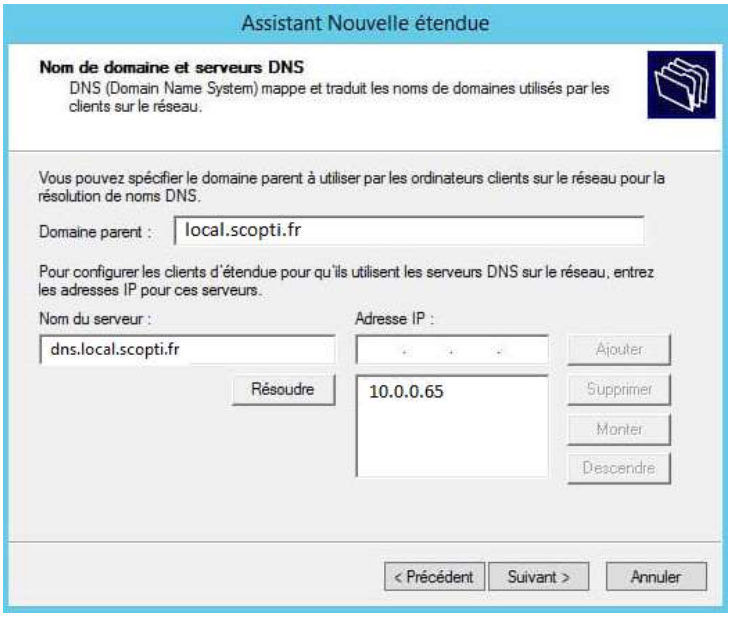
Lors de la Configuration des paramètres DHCP, cliquez sur « **Oui, je veux configurer ces options maintenant** » puis cliquez sur Suivant.

Lors de la configuration des paramètres DHCP, vous allez **pouvoir ajouter la passerelle par défaut**, c'est cette passerelle qui sera ajoutée sur tous les clients de l'étendue.





Même chose au niveau du serveur DNS, ajouter la ou les adresses des serveurs DNS que vous souhaitez utiliser.

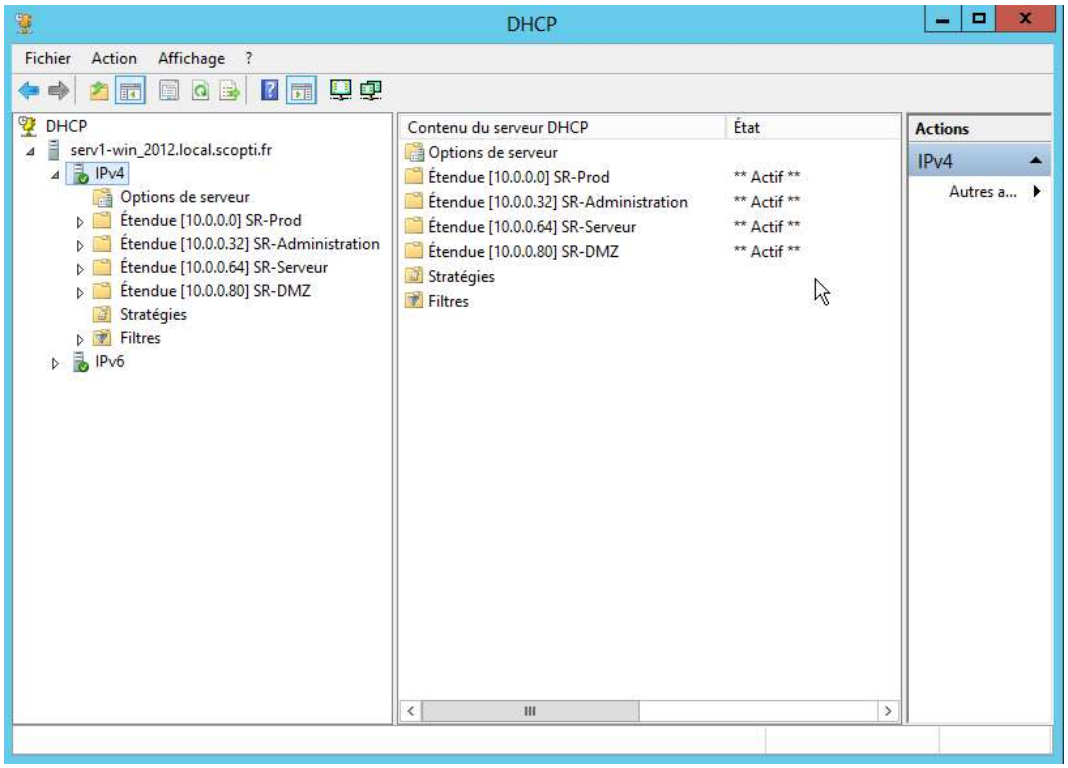


Si vous utilisez des serveurs WINS, ajoutez-les ici. Cliquez ensuite sur suivant.

Vous pouvez maintenant activer l'étendue maintenant ou ultérieurement.

Répéter autant de fois qu'il vous est nécessaire cette opération.

Maintenant, dès lors ou vous connecterez des clients sur votre réseau, le DHCP attribuera une adresse IP en fonction de la plage que vous avez créé.



Et voila, votre serveur DHCP est fonctionnelle dans ces grandes lignes.
PS : Pour que votre serveur DHCP puisse fonctionner dans vos sous-réseau ip n'oubliez pas de mettre en place l'agent DHCP de votre routeur, sinon il y aura des dysfonctionnements.

C – Gestionnaire de mot de passe

Tableau comparatif de gestionnaire de mot de passe :

	KeePass	Dashlane	LastPass
Avantages	Hachage de 256 bits (AES et Twofish) - Stock les mots de passe dans un fichier crypté sur l'appareil utilisateur - Recommandé par l'ANSSI - Gratuit	- AES-256 - Interface - 50 mots de passe	- AES 256 bits avec SHA-256 PBKDF2 et hachage salt - Interface - Possède une version gratuite
Inconvénients	Interface	Version gratuite limitée	Par navigateur web
Système d'exploitation	- Windows (98 à 10), - OS X - Linux	- Mac - Windows - Linux	- Windows - Mac - Linux

Notre choix se portera sur le gestionnaire de mot de passe KeePass (Version 2.42), il est assez complet malgré l'interface un peu vieillissante, la recommandation de ce gestionnaire par l'ANSSI montre que c'est une source sûre pour nous protéger d'éventuelles attaques.

Présentation de KeePass :

C'est un gestionnaire de mot de passe open source gratuit (certifié OSI et recommandé par l'ANSSI) qui va nous aider à gérer nos mots de passe de manière sécurisée. On peut mettre tous nos mots de passe dans une base de données, qui est verrouillée avec une clé principale ou un fichier de clé. Il nous suffit donc de ne mémoriser qu'un seul mot de passe principal ou de sélectionner le fichier de clé pour déverrouiller l'ensemble de la base de données. Les bases de données sont cryptées à l'aide des algorithmes de cryptage les plus fiables et les plus sécurisés du moment (AES et Twofish).

Source : https://keepass.info/

Facultatif : Télécharger le fichier French dans Translation (également sur le site) qu'il faut extraire, récupérer le fichier « French.lngx » et le coller dans le dossier KeePass Password Safe 2 > Languages.

Lancer KeePass, cliquer sur **CLOSE** puis cliquez sur le menu **VIEW** puis choisir le langage voulu, validez et confirmer le redémarrage.

KeePass est désormais en français.

Créer la base de données qui contiendra tout les mots de passes qui se sera sécurisé par un mot de passe unique dont il est conseillé de mettre un mot de passe fort et pouvoir s'en souvenir car il n'y aura aucune possibilité pour le récupérer.

Partage du fichier :

Pour avoir accès à la base de données du gestionnaire de mot de passe par les différents comptes administrateurs, il faut au préalable avoir créé un réseau de partage accessible par les différents postes administrateurs et y partager un dossier inaccessible à d'autres.

Ensuite, créer un dossier partagé, accessible que pour les administrateurs qui contiendra la base de données du gestionnaire de mot passe. Cela va permettre d'avoir accès au mot de passe de n'importe quel poste sur le réseau avec un compte administrateur.

D – Installation d'un DNS récursif avec Unbound

Le protocole **DNS** ***(Domain Name System)*** est un protocole de résolution de noms. Il permet d'associer un nom de domaine à un enregistrement. Le serveur récursif permet d'interroger les serveurs faisant autorité sur Internet pour résoudre le nom de domaine.
Nous avons décidé d'utiliser Unbound pour faire le DNS récursif.
Pour installer Unbound :

```
$ sudo apt-get update
$ sudo apt-get upgrade
$ sudo apt-get install unbound
```

Editer le fichier de configuration pour obtenir celui la :

```
$ nano /etc/unbound/unbound.conf
```

```
# Unbound configuration file for Debian.
#
# See the unbound.conf(5) man page.
#
# See /usr/share/doc/unbound/examples/unbound.conf for a commented
# reference config file.
#
# The following line includes additional configuration files from the
# /etc/unbound/unbound.conf.d directory.
include: "/etc/unbound/unbound.conf.d/*.conf"

server:

# Interface d'ecoute IPv4 sur le reseau
interface: 10.0.0.82
interface: 127.0.0.1

# Autorise les reseaux renseignes a se servir du serveur DNS
access-control: 10.0.0.0/8 allow
access-control: 0.0.0.0/0 refuse

# Cache la version d'Unbound et empeche de connaitre le nom du serveur et l'ID du service
hide-version: yes
hide-identity: yes

# Autorisation de l'IPv4
do-ip4: yes
do-udp: yes
do-tcp: yes
```

On peut vérifier qu'il n'y est pas d'erreur sur le fichier :

```
$ sudo unbound-chekconf /etc/unbound/unbound.conf
```

Il faut maintenant crée le fichier qui accueillera les logs :

```
$ sudo mkdir /var/log/unbound
$ sudo touch /var/log/unbound/unbound.log
$ sudo chown -R unbound:unbound /var/log/unbound
```

Il faut renseigner son adresse IP dans le fichier resolv.conf :

```
$ sudo nano /etc/resolv.conf
```

On peut enfin démarrer unbound :

```
$ sudo service start unbound
```

IV – Charte informatique

L'entreprise SCOP TI met en œuvre un système d'information (SI) et de communication nécessaire à son activité, comprenant un réseau informatique.

Les employés, dans l'exercice de leurs fonctions sont conduits à accéder aux moyens de communication mis à leur disposition et a les utiliser. Ainsi, l'utilisation du système d'information (SI) et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

A/ Champ d'application

A - 1 - Utilisateurs

La présente charte s'applique à l'ensemble des utilisateurs du SI et de communication de l'entreprise, quel que soit leur statut (y compris mandataires sociaux, intérimaires, stagiaires, visiteurs …).

A - 2 - Système d'information et de communication

Le SI et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes et/ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), logiciels, fichiers, base de données et données …

Pour des raisons de sécurité du réseau, le matériel personnel des salariés connecté au réseau de l'entreprise ou qui contiennent des informations concernant l'entreprise sont considérés comme faisant partie du système d'information et de communication.

B/ Confidentialité des paramètres d'accès

L'accès à certains éléments du SI (comme les sessions sur les postes de travail, le réseau, certaines applications ou certains services interactifs) est protégé par des paramètres de connexion (mots de passe et identifiants).

Ce sont des paramètres personnels à chaque utilisateur et doivent être gardés confidentiels. Ils permettent de contrôler l'activité des utilisateurs.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils seront à saisir à chaque accès et ne devront pas être conservés en mémoire dans le SI.

Le mot de passe à enregistrer doit respecter un certain degré de complexité et il sera à changer tous les 4 mois. Les consignes de sécurité sont élaborées par le service informatique afin de recommander les bonnes pratiques.

C/ Protection des ressources sous la responsabilité de l'utilisateur

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du SI et de communication. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisions nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.
Le service informatique est responsable du contrôle du bon fonctionnement du SI et de communication. Il veille à l'application des règles de la présente charte. Les membres du service informatique sont soumis au secret professionnel.

L'utilisateur est quant à lui est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit faire preuve de prudence.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel. Mais aussi en cas d'utilisation de matériel personnel, il appartient de veiller à l'utilisateur de veiller à la sécurité utilisé et à son innocuité.

L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques au sein de l'entreprise. Il doit dans tous les cas en alerter le service informatique.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

D/ Accès à Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le < SERVICE INFORMATIQUE >. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite OU autorisée, sous réserve d'autorisation préalable du < SERVICE COMMUNICATION > OU autorisée. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.
Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

E/ Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.
Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978. (Indiquer ici les traitements réalisés au sein de l'entreprise et les règles d'accès / modification / suppression)
Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être déclarés à la Commission nationale de l'informatique et des libertés, en vertu de la loi n° 78-17 du 6 janvier 1978. Les utilisateurs souhaitant réaliser des traitements relevant de ladite loi sont invités à prendre contact avec < CORRESPONDANT > avant d'y procéder.

F/ Contrôle des activités

F - 1 - Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (" logs "), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information. Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- ➔ à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers ;

- ➔ aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le

téléchargement de fichiers. L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

G/ Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées la gravité des faits concernés.
Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.
VIII. Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié.
Le < SERVICE INFORMATIQUE > est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des nouvelles technologies de l'information et de la communication (NTIC). Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'entreprise.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.
Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

H/ Entrée en vigueur

La présente charte est applicable à compter du 25 mai 2019.