

**Institut Universitaire de Technologie,
Aix-Marseille Université**

**RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications**

ADMINISTRATEUR SYSTEME/RESEAUX

Narong CHUM

ABSYS INFORMATIQUE

Responsable entreprise : Michael ADAMANTIADIS

Responsable académique : Eric SOCCORSI

2017

Remerciements

Je tiens à remercier l'ensemble des personnes qui ont participé à la réussite de mon stage et qui ont permis la rédaction de ce rapport.

Tout d'abord j'adresse mes remerciements à toute l'équipe pédagogique qui m'a accompagné durant deux années et qui a ainsi pu m'aider à la construction d'un réel projet professionnel.

Je tiens également à remercier particulièrement mon maître de stage M. Michael ADAMANTIADIS, responsable des techniciens présents dans l'entreprise Absys Informatique, pour son accueil, le partage de ses connaissances dans le domaine de l'informatique, la confiance qu'il m'a accordée et son aide pour l'aboutissement de mon rapport de stage.

Je remercie aussi l'ensemble des techniciens, M. Frédéric SOURET, M. Ludovic CASCINO, M. Alexandre TRACHINO, M. Alexandre CABAREZ, M. Fabien BEDROSSIAN, M. Simon SITEBOUN et M. Patrice ROATTA, pour le temps passé ensemble, l'aide qu'ils m'ont fourni pour le bon déroulement de mes missions, et toute leur confiance qu'ils m'ont accordé durant ces 10 semaines de stages.

Je remercie de même M. Philippe DIVO, chef de projet de développement, ainsi que M. Rémy BARBA et M. Cédric TITTON développeurs, M. Max PEGURET gérant, responsable commercial et administratif, M. Cyril DOUMAS, Mme Valérie MARTEL comptables et Mme Caroline VILLEMAUX pour leur accueil chaleureux et leur professionnalisme tout au long de cette période.

Enfin, je remercie Mme Nathalie TAILLEFER, stagiaire en formation de technicienne réseaux et télécommunication d'entreprise AFPA d'Istres avec qui j'ai travaillé en binôme tout au long du stage sur des missions et projets qui nous étaient attribués.

Table des matières

1	Introduction	7
2	L'entreprise Absys Informatique.....	7
2.1	Son historique	7
2.2	Organisation de l'entreprise.....	8
2.3	Activités de l'entreprise.....	8
2.3.1	Audit et Conseil.....	8
2.3.2	Hotline.....	9
2.3.3	Sécurité et sauvegarde	9
2.3.1	Développement, optimisation d'application et interface.....	9
2.3.1	Dépannage informatique	9
3	Mes missions	10
3.1	La préparation de postes	10
3.2	La mise en place d'un VPN	13
3.2.1	Présentation de l'équipement	13
3.2.2	Présentation de la problématique	14
3.2.3	Présentation de la configuration du Fortigate 30E, étape par étape	15
3.3	Mise en place et administration d'un serveur	20
3.3.1	Configuration d'un RAID	20
3.3.2	Installation de l'Hyper-V sur un serveur physique et création des machines virtuelles	20
3.3.3	Serveur AD.....	21
3.3.4	Serveur TSE	22
4	Les interventions	23
4.1	Les installations de postes	23
4.2	La relation avec le client.....	24
5	Conclusion.....	25
6	Glossaire.....	26
7	Bibliographie	28

1 Introduction

L'informatique occupe une place importante dans nos vies, preuve de l'avancée technologique dans le monde. Aujourd'hui toutes les entreprises sont équipées d'ordinateurs, que ça soit des PME* ou des grandes entreprises.

Afin de valider mon DUT* Réseaux et télécommunications à l'université de Luminy, j'ai choisi de réaliser mon stage dans une entreprise qui montre toute l'importance de l'informatique de nos jours tout en me formant aux métiers d'administrateur réseaux et système que ma formation m'a fait découvrir.

La société Absys Informatique avec un chiffre d'affaire de 2,4M € en 2016, s'adapte et répond parfaitement à l'évolution du monde informatique qui ne cesse de progresser. Absys Informatique administre, accompagne, et conseil plus de 200 entreprises clientes dans leur choix et l'évolution de leur infrastructure informatique. Durant les dix semaines, je serai affecté au service technique.

Mon rapport de stage présentera l'entreprise Absys Informatique, son organisation et ses activités. Ensuite, je vous exposerai ma contribution par les missions confiées et réalisées. Pour finir je parlerai des interventions menées par les techniciens et de la relation qu'entretient Absys et ses clients avant d'évoquer ce que ce stage m'a apporté sur un plan personnel.

2 L'entreprise Absys Informatique

2.1 Son historique

La société Absys Informatique a été créée en 1994, en créant une S.C.O.P* (4 associés).

L'ambition d'Absys Informatique est d'offrir une palette de services assez vaste pour ses clients, développement, administrations système et réseaux, maintenance, dépannage, revente de postes... L'entreprise se positionne sur tous les plans de l'informatique pour pouvoir répondre au mieux aux besoins des clients.

Pour respecter cet objectif, une équipe de professionnels, dont la responsabilité est le meilleur garant de la réussite et de la satisfaction, a été constituée. Lors du lancement du projet Absys, l'entreprise avait à son compte 5 employés, aujourd'hui elle en possède 16.

En 2012, le chiffre d'affaires était de 1,3 millions d'euros, et de 2,4 millions en 2016. La croissance est régulière et maîtrisée. L'objectif est de consolider les acquis par une progression de 3%-5% par an.

2.2 Organisation de l'entreprise

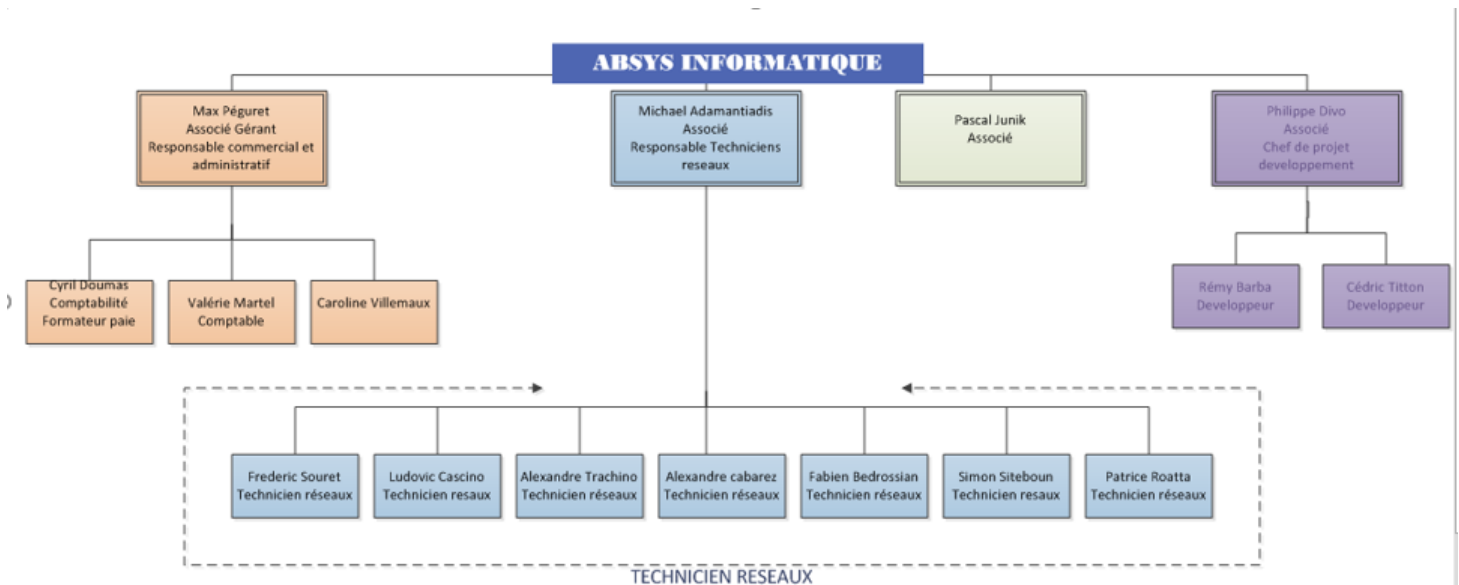


Figure 1 : Organigramme de la société Absys Informatique

A la tête de l'entreprise 4 associés M. Michael ADAMANTIADIS, M. Pascal JUNIK, M. Philippe DIVO, et M. Max PEGURET.

Le service Technique : Avec pour responsable M. Michael ADAMANTIADIS, s'occupe des problèmes informatiques que rencontrent les clients au quotidien, gère les serveurs des clients, configure le matériel informatique pour les clients, configuration de routeurs.

Le service de Développement : Avec pour responsable M. Philippe DIVO, crée de multiples outils spécifiques répondant aux besoins des clients en complément de leurs solutions de gestion et développe des interfaces vers leurs différents logiciels métier ou vers leur site web marchand.

Le service Commercial : Gère les commandes des clients, se charge de la réception et les expéditions des produits.

2.3 Activités de l'entreprise

2.3.1 Audit et Conseil

La maîtrise des réseaux, systèmes et couches applicatives permet de mener efficacement les missions d'assistances, de conseils et d'études d'architectures de systèmes d'informations et interconnexions de différents sites ou de nomades (VPN*, filtrage, Firewall*...), optimisés par la connaissance des offres opérateurs.

2.3.2 Hotline

Fort de son expérience, ABSYS résout environ 80% des problèmes informatiques dans la maintenance à distance. La Hotline est une des activités principales de la société.

Les mails des clients qui se plaignent de problèmes informatiques affluent tous les jours. Les techniciens sont munis d'un téléphone et de Teamviewer, un logiciel indispensable pour cette activité. Il permet de prendre la main sur le poste du client sans avoir à se rendre sur place. Il peut y avoir tous types de problèmes et de niveaux de difficultés très variés.

Toute l'équipe des techniciens intervient alors. Ils sont au minimum 2 à assurer la hotline pendant que les autres se rendent sur le terrain pour assurer le travail physiquement.

Exemple de problèmes rencontrés par les clients : ordinateur qui ne démarre plus, mot de passe oublié, récupérer les sauvegardes, connexion lente, problème d'imprimante, plus d'accès web...

Chaque intervention physique ou à distance est décomptée, en effet le client dispose d'un crédit d'heure mensuel prépayé. Différents niveaux de contrat peuvent être établis, en fonction des besoins, du budget et du degré d'importance du S.I* de l'entreprise. Ces contrats vont de l'engagement de moyens à l'engagement de niveaux de service. C'est M. Max PEGURET et M. Michael ADAMANTIADIS qui négocient les contrats en fonction des besoins estimés. Les plus grandes entreprises peuvent payer à l'année afin d'avoir un nombre d'heures de dépannage illimitées.

2.3.3 Sécurité et sauvegarde

Absys propose à ses clients des serveurs ainsi que des offres d'anti-virus, d'anti-spam et de firewall.

Ces produits sont installés par les techniciens puis surveillés et maintenus constamment, le plus souvent à distance.

2.3.4 Développement, optimisation d'application et interface

L'entreprise étant spécialisée dans la programmation en environnement réseau, les techniciens peuvent proposer des solutions de développement aux clients.

Les clients peuvent aussi faire la demande d'eux même de création de sites web.

Cette partie-là est assurée par M. Philippe DIVO et son équipe de développement.

2.3.5 Dépannage informatique

Absys informatique s'occupe aussi de pannes diverses rencontrées par les clients sur les ordinateurs, que ce soit un particulier ou un professionnel. Disques durs défaillants, ordinateurs infectés par un virus, alimentation qui ne fonctionne pas, et tout autre problème est résolu par les techniciens d'Absys.

3 Mes Missions

Dès mon arrivée dans l'entreprise, j'ai été placé en observation durant une semaine pour m'intégrer et comprendre le fonctionnement de l'entreprise, j'ai été rapidement sollicité par les techniciens pour les épauler dans différentes tâches. Je me suis vu confié par la suite trois projets qui sont :

- La préparation de postes pour la société DALTYS
 - La mise en place d'un VPN grâce à un fortinet chez un client possédant 3 sites distants
- La mise en place d'un serveur avec configuration et administration.
- La mise en place et administration d'un serveur

3.1 La préparation de postes

Au bout de quelques semaines en entreprise, je me suis vu confié ma première mission : La préparation de 8 postes pour le groupe DALTYS.

En effet, le client a commandé 8 postes que nous avons réceptionné, afin de pouvoir les préparer pour qu'ils soient opérationnels, ensuite il faut les renvoyer au client.

L'activité a été réalisée sur 2 jours avec les conseils de M. Patrice ROATTA. Une check-list (annexe 1) m'a été remise pour la réalisation des opérations. Il faut être très précis et rigoureux dans la tâche, car la moindre faute ou oubli poussera le client à passer en Hotline et donc fera perdre un temps précieux aux techniciens.

Dans un premier temps, il faut désinstaller quelques programmes liés à l'installation initiale prévue par le constructeur et lancer les mises à jour Windows Update. Ensuite, j'active le compte administrateur qui est désactivé par défaut (figure 2), pour pouvoir intervenir plus tard si l'utilisateur a des soucis avec son compte, ou bien pour pouvoir modifier certains paramètres dont seul l'administrateur a accès.

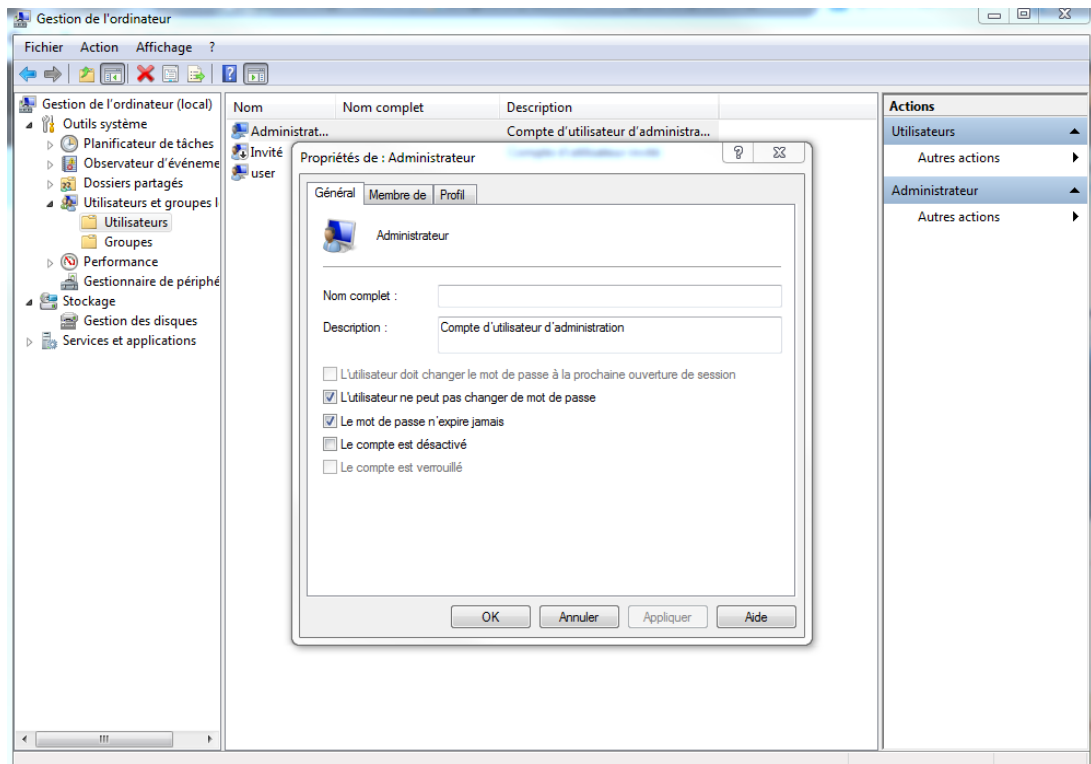


Figure 2 : Activation du compte administrateur

Une fois ces premières étapes réalisées, il faut entrer les machines dans le domaine* de l'entreprise : *sgda.domaine.net*. Mais pour ce faire il faut d'abord changer le DNS* du poste : *10.100.19.241*. (Figure 3 et 4)

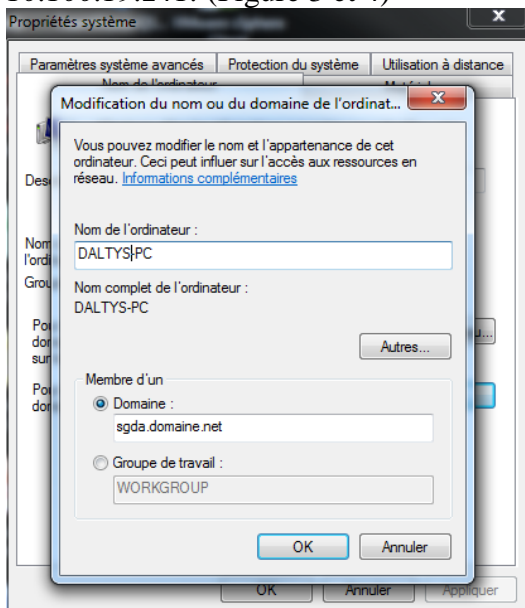


Figure 3 : Ajout de la machine au domaine

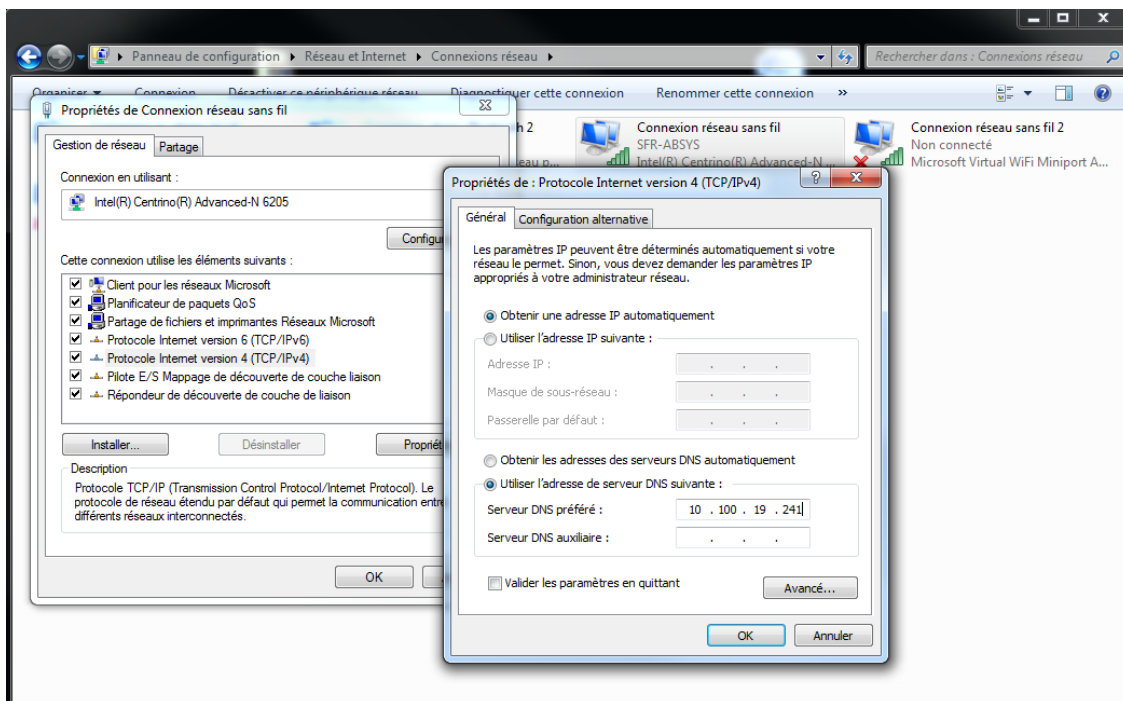


Figure 4 : Changement de DNS

Dès que le poste est sur le domaine, on peut aller chercher son utilisateur et le mettre en tant qu'administrateur du poste pour qu'il ait tous les droits. (Figure 5)

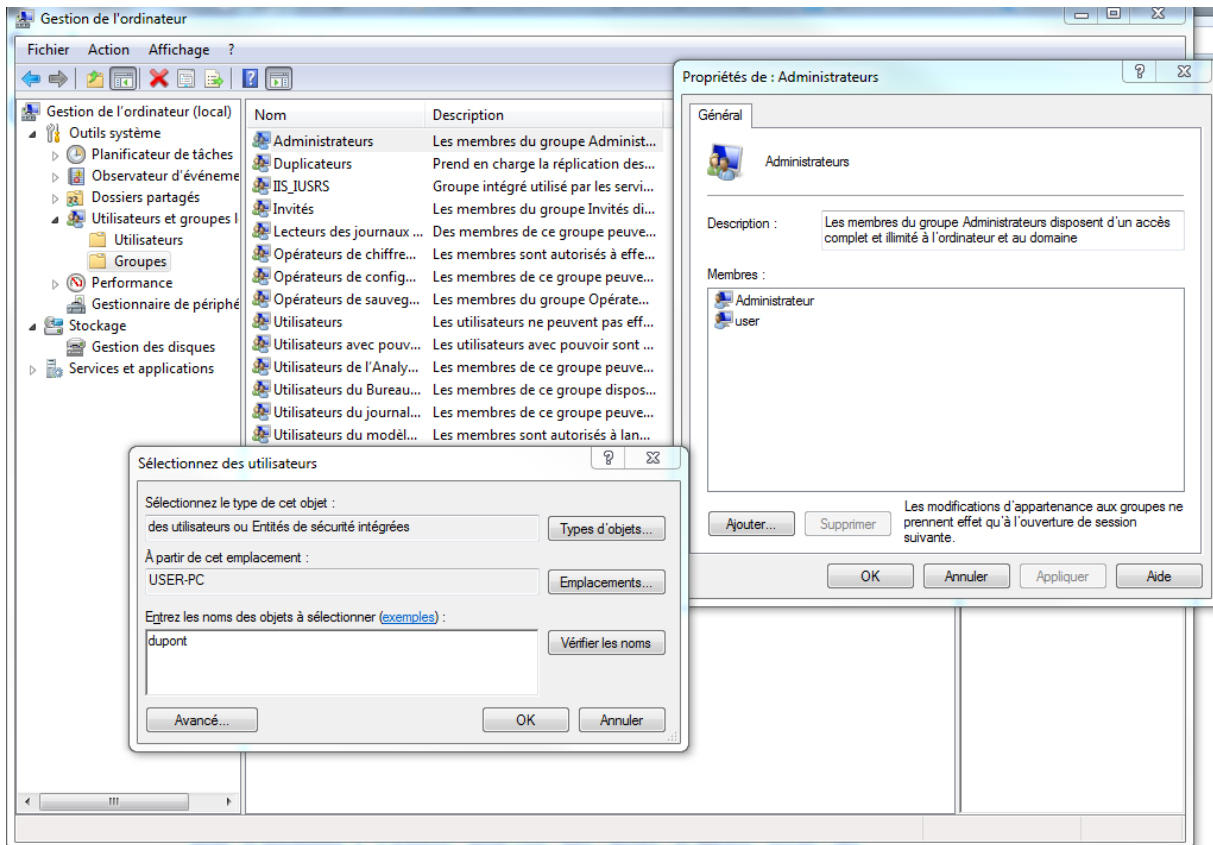


Figure 5 : ajouts du compte utilisateur dans le groupe administrateur

Par la suite, on va installer les programmes de base comme Firefox, Adobe Reader, Flash, Java, le pack Office 2010 avec une clé fournie par le client ainsi que Teamviewer.

On installe également la protection Symantec Endpoint Protection.

Cependant, l'utilisateur aura accès au domaine seulement sur son lieu de travail, il ne pourra donc pas travailler chez lui si le besoin est, c'est pour cela que l'on installe également : *FortiClient SSLVPN* qui un petit outil qui va permettre à l'utilisateur du poste de se connecter au domaine de n'importe quel endroit (figure 6).

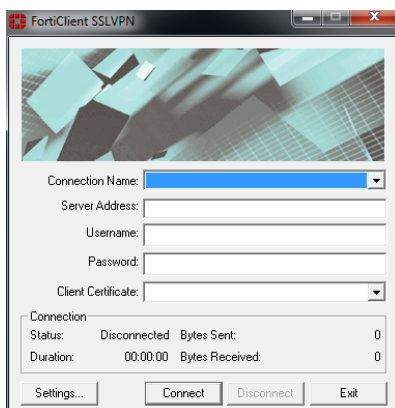


Figure 6 : Interface du FortiClient VPNSSL

Pour ce faire on renseigne : l'adresse IP publique du domaine que l'on veut atteindre, nom d'utilisateur du domaine ainsi que son mot de passe. Il nécessite juste une connexion internet.

Pour finir, on installe un raccourci sur le bureau pour le serveur (figure 7)

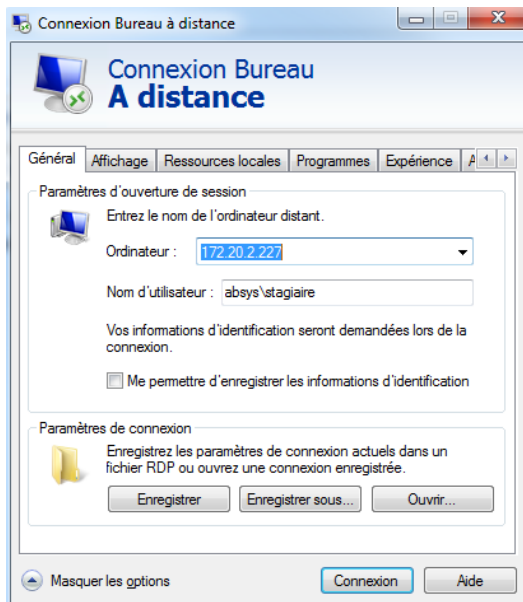


Figure 7 : création du raccourci au serveur

Pour se connecter au serveur, j'utilise l'application Microsoft, on renseigne l'adresse ip du serveur, le nom d'utilisateur et je l'enregistre sur le bureau. L'utilisateur n'a plus qu'à double cliquer sur l'icône pour se connecter au serveur.

Après les dernières opérations, je range le bureau en plaçant sur le bureau public Word, Excel, PowerPoint, Outlook (dont la configuration se fera automatiquement une fois sur le poste placé dans le domaine), Teamviewer, FortiClient VPNSSL et le raccourci au serveur.

Le poste est maintenant opérationnel. Je le remballage ensuite dans son emballage et je remets le paquet à Mme Caroline VILLEMAUX qui le prépare pour l'envoyer au client.

Tout au long du stage j'ai eu à préparer des postes, mais selon le client, les procédés peuvent varier légèrement. Tout dépend de ce que demande le client.

3.2 La mise en place d'un VPN

Pour ce projet, j'ai été sous la direction de M. Fabien BEDROSSIAN. C'était pour moi l'occasion de découvrir et manipuler un produit de chez Fortinet. Essentiel pour la suite de mon stage, afin de comprendre la méthodologie ainsi que la logique des techniciens.

3.2.1 Présentation de l'équipement

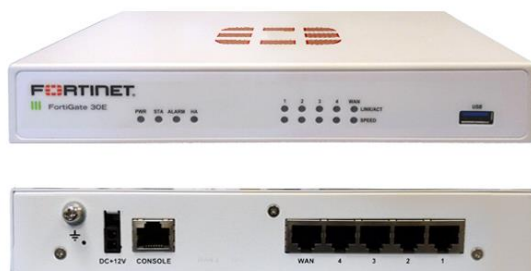


Figure 8 : Fortigate 30E de chez Fortinet

Absys Informatique travaille essentiellement avec du matériel de chez Fortinet (Figure 8).

Pour réaliser ce projet, nous avons eu à configurer un Fortigate 30E qui possède 4 ports LAN* et 1 port WAN*. La particularité de cet équipement est qu'on peut le qualifier de UTM*.

Le Fortigate 30E possède donc plusieurs fonctionnalités telles qu'un pare-feu traditionnel, un routeur, mais aussi anti-virus ou encore détection et prévention dynamique des intrusions. C'est l'un des avantages de cet équipement.

3.2.2 Présentation de la problématique

La société COOP AGRICOLE DE CEREALES, qui est une société de coopérative agricole spécialisée dans commerce de gros de céréales, possède 3 sites distants dont **Le Silo** à Le Thor, **Mejean** à Le Thor, et le troisième à **Bollene**.

Le fortinet situé au **Silo** à Le Thor est tombé en panne, il permettait le VPN entre **Le Silo** et **Mejean**, ainsi que **Le Silo** et **Bollene**.

Le client a fait appel à nous pour racheter un nouveau Fortinet afin de rétablir le lien VPN reliant **le Silo** à **Mejean** mais aussi **le Silo** à **BOLLENE**. (Figure 9)

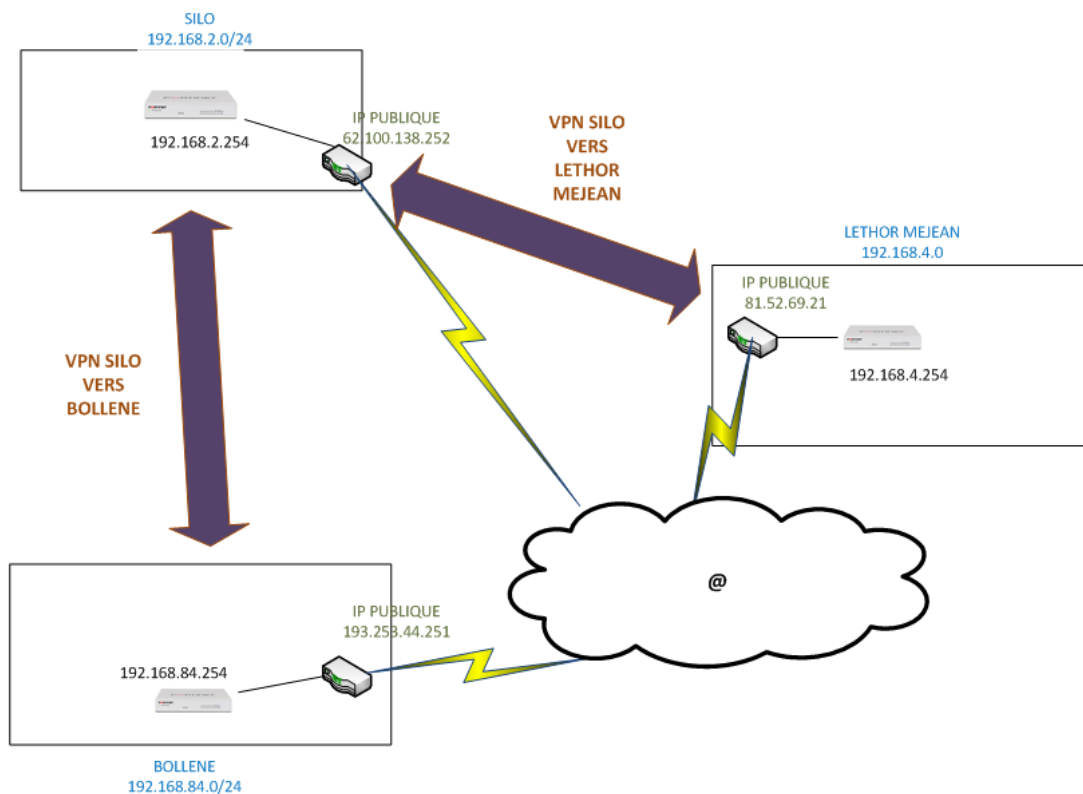


Figure 9 : Schéma illustrant la problématique

3.2.3 Présentation de la configuration du Fortigate 30E, étape par étape

Dans un premier temps, il faut savoir que le fortigate 30E possède une configuration de base par défaut, qui donne la fonctionnalité aux ports LAN de se comporter comme un switch physique. Nous allons chercher à réinitialiser la configuration de base, afin de pouvoir reconfigurer le fortigate pour faire en sorte que les ports LAN fonctionnent comme un switch virtuel. Cela va permettre de manipuler les port LAN à notre guise comme par exemple : regrouper tous nos ports, ajouter ou enlever des ports, ou encore transformer un ou plusieurs ports en sortie WAN si le besoin est. Ce qui est impossible avec la configuration de base. Grâce à cette manipulation, nous pouvons modifier les fonctionnalités des ports dans le futur si le client désire une modification dans la topologie du réseau sans pour autant refaire toute la reconfiguration du boitier.

Pour commencer :

Se connecter au fortinet via Putty à l'aide câble console pour pouvoir configurer notre interface LAN, afin de créer un switch virtuel. Il est aussi possible de configurer le fortinet via une interface web (Figure 10).

VDOM*, cette commande permet de virtualiser sur les ports LAN physiques d'autres fortigates, ce qui va permettre d'attribuer plusieurs configurations sur un port physique, pour que le port se comporte de manière différente selon les cas. Par exemple, on peut faire passer deux accès internet sur un même port, un principale, un secondaire, si le principal tombe en panne, on bascule sur le second automatiquement.

```
COM3 - PuTTY
FGT30E3U17008080 login: admin
Password:
Welcome !

FGT30E3U17008080 # config system switch-interface
FGT30E3U17008080 (switch-interface) # edit LAN
new entry 'LAN' added

FGT30E3U17008080 (LAN) # set vdom root
FGT30E3U17008080 (LAN) # set member lan1
FGT30E3U17008080 (LAN) # end

FGT30E3U17008080 # config system interface
FGT30E3U17008080 (interface) # edit LAN
FGT30E3U17008080 (LAN) # set ip 192.168.2.254 255.255.255.0
FGT30E3U17008080 (LAN) # set allowaccess https ping
```

Figure 10 : Réinitialisation du Fortigate

Autoriser l'accès via https et aux pings

Ajout du port lan1 dans le vdom

Une fois cette première étape passée, se connecter via l'interface Web au fortinet grâce à l'adresse que je lui ai attribuée précédemment en entrant l'url <https://198.168.2.254> dans un navigateur web afin de commencer la configuration (Figure 11).

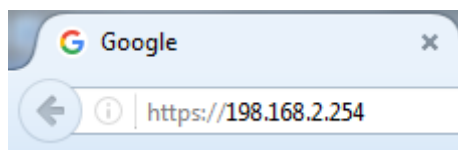


Figure 11 : Connexion au fortigate via l'interface Web

Arrivé sur l'interface web, il faut se connecter. Par défaut le login est « admin » et il n'y a pas de mot de passe (Annexe 2). Le premier paramètre à configurer est donc le mot de passe (Annexe 3).

Je peux désormais configurer la partie réseau du fortigate. Je vais commencer par changer le numéro de port attribué par défaut à l'administration en https qui est 443. En effet si nous laissons le port par défaut, nous ne pouvons plus le rediriger pour une autre utilisation par le client. Par exemple dans le cas où ce dernier possède un serveur exchange, nous ne pourrions plus le rediriger pour avoir accès à notre Webmail (Annexe 4).

Je crée ensuite les objets, c'est-à-dire que je crée les adresses IP de chaque réseau local pour pouvoir les configurer (figure 12).

1 POUR BOLLENE
1 POUR LE THOR-MEJEAN
1 POUR LE SILO

Name	Type	Details	Interface	Visibility	Ref.
Adobe Login	Wildcard FQDN	*.adobe*.com	any	✓	1
Gotomeeting	Wildcard FQDN	*.gotomeeting.com	any	✓	1
LAN-BOLLENE	Subnet	192.168.84.0/24	any	✓	1
LAN-LETHOR	Subnet	192.168.4.0/24	any	✓	1
LAN-SILO	Subnet	192.168.2.0/24	any	✓	2
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	✓	1
Windows update 2	Wildcard FQDN	*.windowsupdate.com	any	✓	1
adobe	Wildcard FQDN	*.adobe.com	any	✓	1
all	Subnet	0.0.0.0/0	any	✓	0
android	Wildcard FQDN	*.android.com	any	✓	1
apple	Wildcard FQDN	*.apple.com	any	✓	1
appstore	Wildcard FQDN	*.appstore.com	any	✓	1
auth.gfx.ms	FQDN	auth.gfx.ms	any	✓	1
autoupdate.opera.com	FQDN	autoupdate.opera.com	any	✓	1
citrix	Wildcard FQDN	*.citrixonline.com	any	✓	1
dropbox.com	Wildcard FQDN	*.dropbox.com	any	✓	1
easee	Wildcard FQDN	*.easee.com	any	✓	1

Figure 12 : Tables des objets

Pour ce faire, je renseigne le nom de l'objet et je lui attribue une adresse (Annexe 5). Je répète la manipulation pour LAN-LETHOR et LAN-BOLLENE.

Mes objets sont maintenant créés.

Je peux désormais créer nos deux tunnels VPN :

Un tunnel SILO  Bollene

Un tunnel SILO  Le Thor-Mejean

Pour ce faire, j'indique les adresses IP publiques des deux sites distants que l'on veut atteindre, j'indique aussi l'interface des ports des adresses IP publiques* renseignées précédemment qui est le WAN. Et enfin, on désactive le NAT* car les adresses des sites qui cherchent à se joindre sont connues de part et d'autre (Annexe 6). On réalise cette tâche deux fois, pour BOLLENE et Le THOR

Il faut maintenant sécuriser les tunnels VPN (figure 13) :

Méthode de chiffrements → les deux pairs d'un échange VPN doivent utiliser la même configuration. Les méthodes les plus connues sont le DES, le Triple DES et l'AES pour le chiffrement symétrique, et le RSA pour le chiffrement asymétrique.

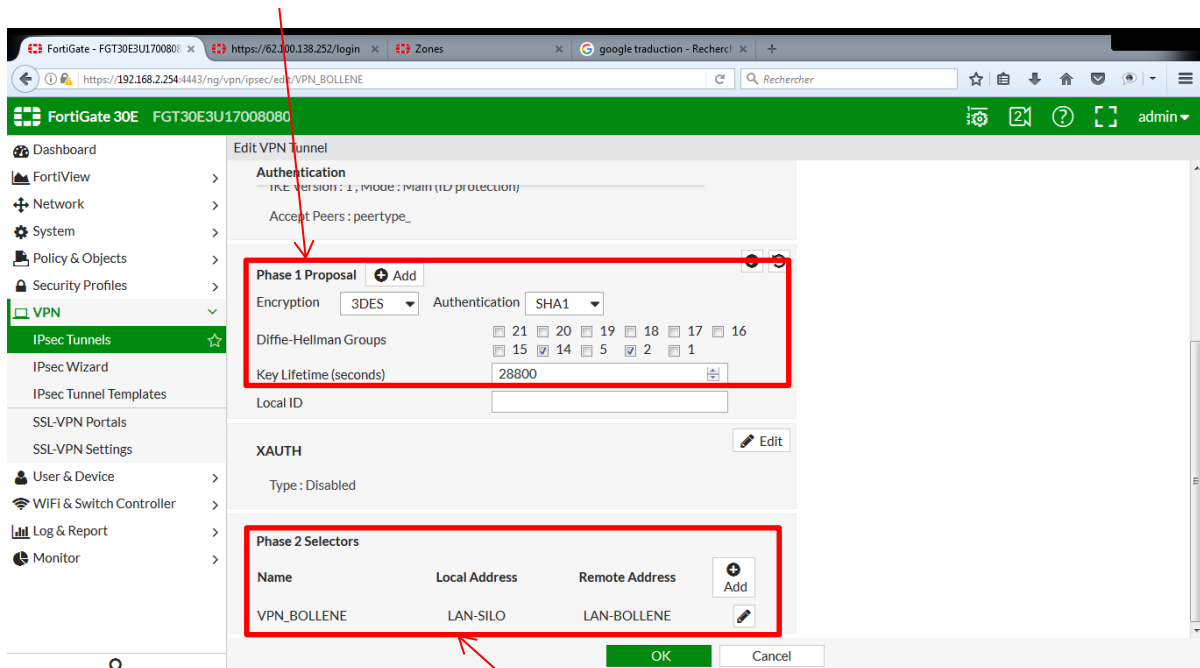


Figure 13 : Paramètre de chiffrement du VPN

Je renseigne ici le sens du tunnel VPN : Le tunnel VPN_BOLLENE a pour adresse locale le SILO et pour adresse distante BOLLENE

Mes tunnels sont désormais créés (figure 14).

Tunnel	Interface Binding	Template	Status	Ref.
VPN_BOLLENE	wan	Custom	Inactive	3
VPN_LETHOR	wan	Custom	Inactive	3

Figure 14 : table des tunnels créés

La création de routes (figure 15) permet de donner la direction à suivre. D'où est-ce que le flux part, et où est-ce qu'il arrive.

Pour joindre l'hôte distant, passer par le tunnel VPN

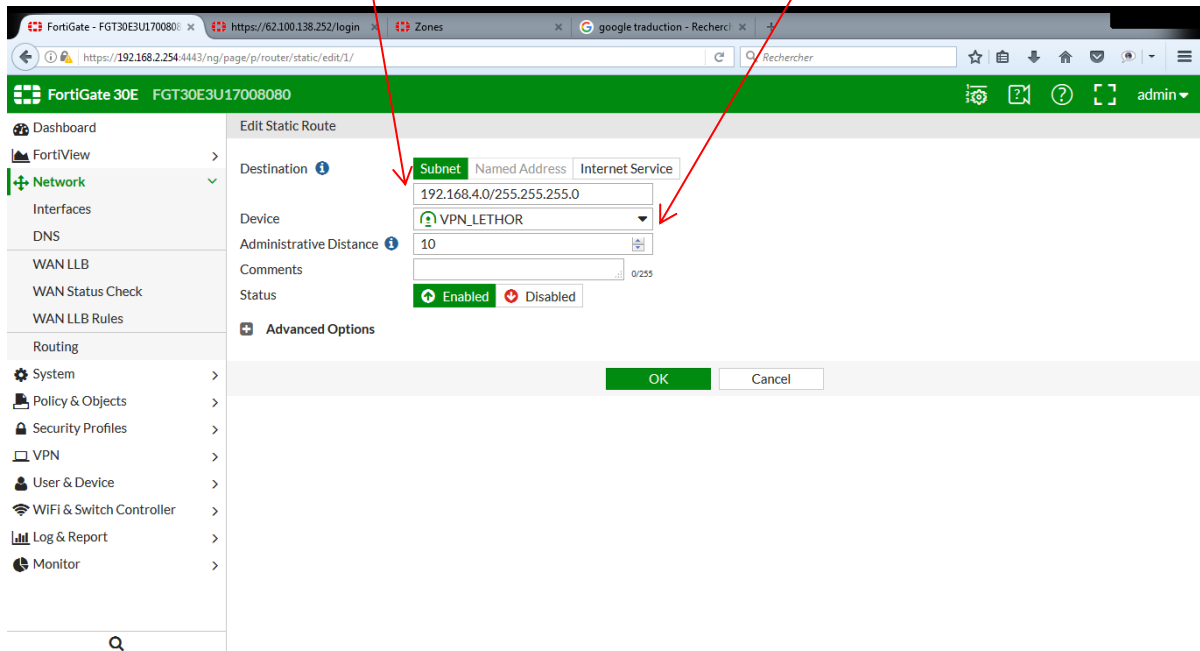


Figure 15 : Création des routes

Ici je renseigne l'adresse publique de destination et le moyen de l'atteindre. Par exemple, pour atteindre l'adresse 192.168.4.0 on utilise le VPN_LETHOR.

Pour simplifier et surtout anticiper les prochains besoins du client dans le futur, je vais créer une zone VPN qui regroupe mes VPN : cette manipulation me permet d'ajouter de nouveaux tunnels si besoin est à l'avenir dans cette zone, pour faciliter la prochaine étape qui est la création des politiques* (Annexe 7).

La configuration des Politiques est primordiale. Les politiques permettent d'autoriser les trafics entrants et sortants. Ils sont plus communément appelés ACL*.

Premièrement je vais configurer la Policy ZONE-VPN → LAN-SILO. C'est donc la règle qui va permettre à la ZONE-VPN que j'ai créé précédemment, d'entrer vers le LAN-SILO. On gère donc ici le trafic entrant. (Figure 16)

La ZONE-VPN créée précédemment nous permet de créer qu'une seule Policy. Sans cela nous aurions dû créer 2 Politiques : VPN_LETHOR → LAN-SILO

VPN_BOLLENE → LAN-SILO

Interface entrante : ZONE-VPN qui se dirige / sort sur l'interface LAN de SILO

Toutes les sources de ZONE_VPN ont pour destination le LAN de SILO

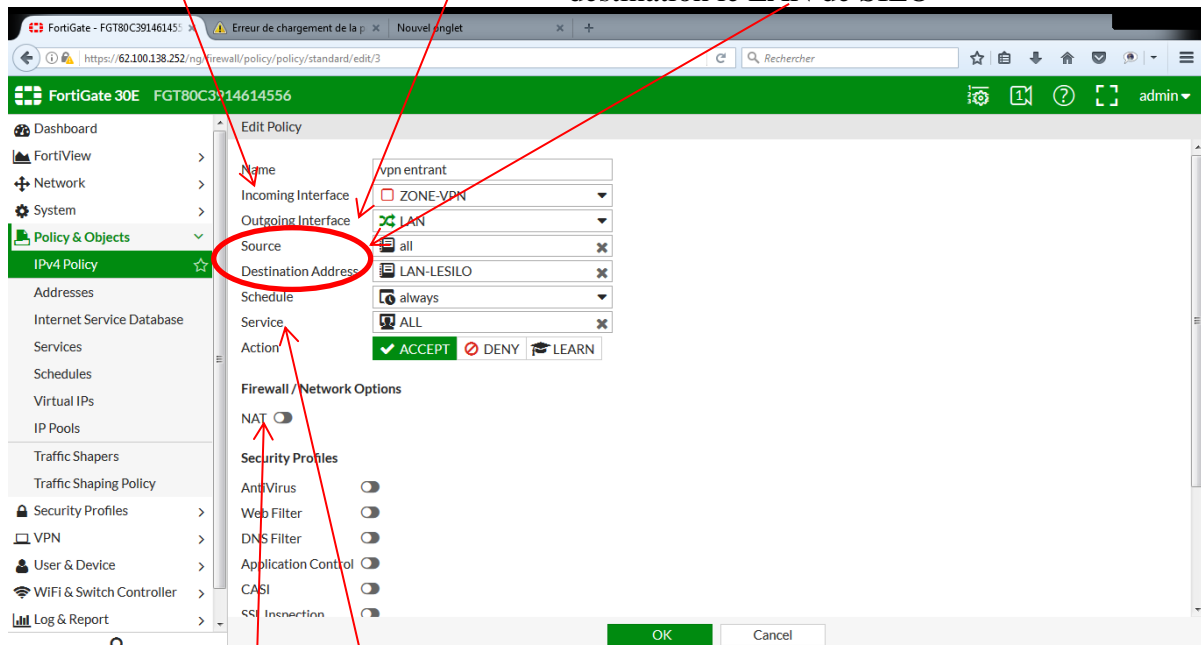


Figure 16 : Création de Policy

Autorisation aux différents services comme les pings, https, ssh...

Désactivation du NAT car on utilise un VPN, les adresses sont déjà connues

Dans un second temps, je configure ensuite la Policy LAN SILO → ZONE_VPN. Je veux que le réseau LAN SILO sorte sur la ZONE_VPN. La source LAN SILO a pour destination toutes les adresses de la ZONE_VPN (Annexe 8).

Et enfin, on configure ensuite la Policy LAN → WAN. Je crée aussi une policy pour gérer le trafic du LAN vers le WAN. En créant cette policy, cela va me permettre de sortir sur Internet, mais elle autorise aussi le chemin inverse. De plus, cette policy est la seule où l'on doit activer le NAT car on ne connaît pas l'adresse de destination (Annexe 9).

Pour finir, en regardant la table des politiques, il y a une règle toujours active que nous n'avons pas configuré, elle est toujours présente. C'est une policy par défaut qui dit que tout ce qui n'est pas autorisé est interdit (annexe 10).

Nous avons pu ainsi créer deux tunnels VPN reliant le site SILO aux deux autres sites. Pour conclure, la réalisation de cette mission s'est donc faite en plusieurs étapes : la création des objets, la création des VPN avec la configuration des chiffrements, et pour finir la mise en place des Politiques. Le temps de configuration du Fortigate pour ce genre de demandes est d'environ 20 minutes pour un technicien confirmé.

3.3 Mise en place et administration d'un serveur

Lors de mon stage, j'ai donc eu à installer un serveur avec la configuration d'un RAID*, j'ai ensuite dû, depuis un Hyper-V*, créer deux serveurs virtuels :

- Un serveur TSE*
- Un serveur Active directory* qui va permettre d'administrer le serveur TSE.

3.3.1 Configuration d'un RAID

J'ai appris au cours de mes dix semaines d'entreprises ce qu'était un RAID. J'ai effectué de mon côté quelques recherches qui m'ont permis d'en savoir un peu plus sur cette notion-là (Annexe 11).

J'ai commencé tout d'abord, par créer un RAID 1 sur deux disques durs et un RAID 5 sur cinq disques durs à la demande de mon maître de stage. Ce qui va permettre d'avoir une tolérance sur deux disques durs au maximum, et une bonne performance en écriture/lecture.

Pour pouvoir configurer le système de RAID, lors du démarrage il faut appuyer sur F8 afin de pouvoir entrer dans le menu de configuration qui va nous permettre de créer nos RAID (Annexe 12 13).

Une fois dans le menu, il faut sélectionner les disques que l'on veut configurer, d'abord les deux disques pour le RAID 1, et ensuite les cinq autres disques pour le RAID 5 (annexe 14).

Une fois les RAID configurés, j'installe Windows Server 2012 R2 avec un CD que me fournit mon maître de stage. Et je lance les mises à jour Windows Update.

3.3.2 Installation de l'Hyper-V sur un serveur physique et création des machines Virtuelles

Une fois les mises à jour Windows Update installées, je peux configurer le serveur. Je commence d'abord par installer le rôle Hyper-V sur le serveur physique grâce à l'assistant d'ajout de rôle (Annexe 15).

Hyper-V préalablement installé, je mets en place un commutateur virtuel à partir du gestionnaire Hyper-V. Cela va permettre aux machines virtuelles, qui vont être créées par la suite, d'avoir accès à Internet. Je vais donc choisir un switch virtuel de type Externe afin de permettre aux machines virtuelles de communiquer vers l'extérieur. J'attribue ensuite un nom au switch virtuel et je lui indique la carte réseau associée (Annexe 16 17).

C'est donc à partir du gestionnaire Hyper-V que je vais créer mes machines virtuelles (Annexe 18 à 22) et que je les gérerai. Il faudra également renseigner le nom de notre machine virtuelle, la RAM allouée à notre machine virtuelle, configurer la mise en réseau et indiquer le commutateur virtuel préparé au préalable et créer un disque dur virtuel en lui affectant une taille. La machine virtuelle maintenant créée, il faut faire la manipulation une deuxième fois afin d'avoir nos deux machines virtuelles (figure 17).

Ordinateurs virtuels				
nom	État	Utilisation d...	Mémoire affectée	Temps d'activ
SERV AD	Exécution	0 %	1139 Mo	02:31:42
serveur TSE	Exécution	0 %	4096 Mo	02:20:03

Figure 17 : Les deux machines virtuelles

3.3.3 Serveur AD

Sur l'une des deux machines virtuelles installées, je vais en dédier une pour Active Directory. Pour installer AD il faut cocher « Services AD DS » dans l'assistant d'ajout de rôles et de fonctionnalités.

Après l'installation il ne faut pas oublier de créer le domaine (figure 18 et 19). Les serveurs TSE auront pour DNS* l'adresse IP du serveur AD. Il deviendra un contrôleur de domaine*.

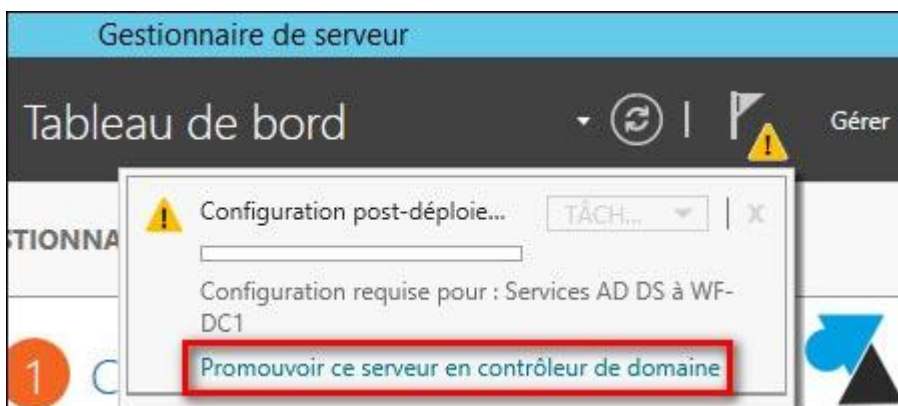


Figure 18 : On donne le rôle au serveur de contrôleur de domaine

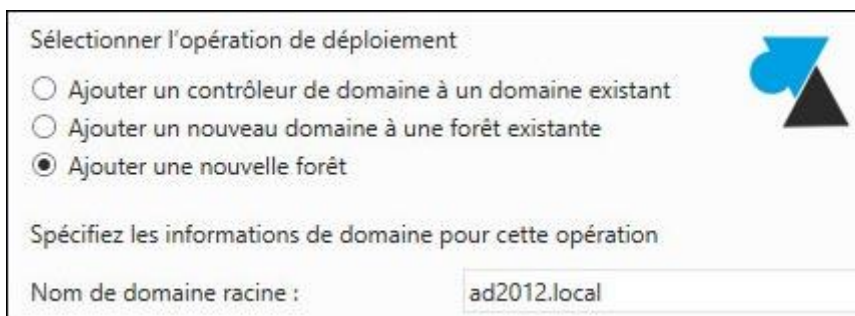


Figure 19 : Création d'un nom de domaine

C'est ce serveur qui va permettre d'administrer le serveur TSE. Je vais commencer par créer des utilisateurs. Pour cela il faut ouvrir l'application « Utilisateurs et ordinateurs Active Directory ».

Une fois dans l'application, je vais pouvoir créer des utilisateurs, leur donner un nom d'ouverture de session ainsi qu'un mot de passe (Annexe 23 à 26).

On peut également créer des groupes distincts et joindre les utilisateurs dans les groupes.

Et enfin, la mise en place des GPO*. Pour ce faire il faut dans l'outil d'administration choisir l'application « Gestion des stratégies de groupe ». C'est ici que je vais pouvoir administrer le serveur TSE. À la demande de mon maître de stage, je vais donc masquer tous les lecteurs aux utilisateurs. Je crée donc une nouvelle GPO en lui donnant un nom et en lui attribuant la règle correspondante (Annexe 27 à 32).

Ensuite, toujours avec une GPO je vais créer un lecteur réseau avec un chemin que j'ai défini spécifiquement. Les utilisateurs n'auront accès qu'à ce lecteur-là (figure 20).

▲ Emplacement réseau (1)

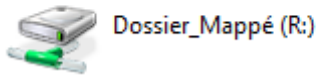


Figure 20 : Lecteur R créé avec un chemin spécifique

L'avantage de faire des groupes d'utilisateurs permettra de faciliter la gestion des GPO. Il se peut que certains utilisateurs n'aient pas les mêmes droits que d'autres, ou les mêmes règles. Faire des groupes permettra d'attribuer des règles à tout un groupe et ne pas administrer utilisateur par utilisateur.

Par le même principe j'ai interdit l'accès au panneau de configuration à tous les utilisateurs et défini un emplacement d'enregistrement par défaut World, Excel, et PowerPoint.

3.3.4 Serveur TSE

La deuxième machine virtuelle sera donc pour le serveur TSE, c'est ici que les utilisateurs se connecteront pour pouvoir accéder à des applications, des données ou un environnement de travail. Il ne faut pas oublier de changer le DNS du serveur TSE, il faut lui attribuer l'adresse statique du serveur AD.

Avant de commencer, je vais installer les fonctionnalités et rôles nécessaire à un serveur TSE. « Services Bureau à distance » qui va permettre aux utilisateurs d'accéder à des connexions à distance à partir d'un réseau d'entreprise d'Internet. En installant ce rôle, on a aussi la possibilité de publier des applications sur une interface web. Une fois installé il faut activer le « Bureau à Distance », désormais l'utilisateur se connecte au serveur TSE grâce à l'application Windows « Connexion Bureau à Distance » (figure 21).

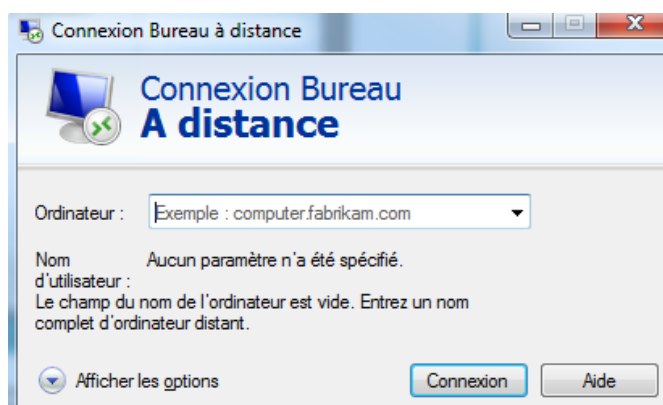


Figure 21 : Application Connexion bureau à Distance

L'utilisateur se connectera en indiquant l'adresse IP du serveur TSE, et il accèdera au serveur en s'authentifiant avec le nom d'utilisateur et le mot de passe que je lui aurai attribué sur le serveur AD.

Ce projet était un exercice que m'a demandé de réaliser M. Michael ADAMANTIADIS. Il s'est déroulé sur 4 jours et m'a permis d'acquérir de nombreuses connaissances dans le domaine de l'administration systèmes sous Windows, ce qu'était la virtualisation de machine, et comprendre le fonctionnement qui a lieu entre l'entreprise et ses clients.

4 Les Interventions

Dans la semaine, un technicien a 2 jours de Hotline, et le reste du temps il est en intervention physique chez un client. Au cours de mon stage, j'ai donc eu l'occasion d'accompagner les techniciens chez des clients. Dans un premier temps j'aborderai la mission la plus fréquente en intervention, les installations de postes et enfin la relation avec le client.

4.1 Les installations de postes

Le plus souvent, les missions d'interventions auxquelles j'ai pu participé avec un technicien étaient des installations de matériels informatiques. En effet les clients passent par Absys pour acheter leur matériel informatique. L'entreprise achète ce que le client souhaite et prépare les postes en atelier. Une fois le produit prêt à l'utilisation, si le client est situé dans la région, c'est aux techniciens d'aller l'installer sur place. Parfois il peut s'agir de remplacement, par exemple, le poste est ancien, le client veut donc changer d'ordinateur ou bien simplement installer un poste.

Le but est de réaliser la tâche le plus efficacement possible, en un minimum de temps, car il est rare qu'il n'y ait qu'un seul poste à installer chez un client. C'est dans cette situation là qu'on peut voir l'importance du travail en atelier. Effectivement, dans le cas d'un remplacement de poste, une fois arrivé sur place, le technicien copie les données de l'ancien poste sur un disque dur externe. Une fois cette tâche réalisée, il n'a plus qu'à installer le nouveau poste et coller les données copiées dans le disque dur sur le nouveau poste. L'ordinateur étant déjà configuré et préparé en atelier, le temps passé chez le client est donc minimisé au maximum.

Grâce à mes nombreuses interventions en tant que soutien d'un technicien j'ai pu acquérir de l'expérience. Ainsi, je me suis vu confié lors de ma dernière semaine de stage une intervention seul. J'ai dû me rendre chez un client, API Equipement situé à Bollene, pour une installation de poste. Le matin même j'ai donc préparé un poste en atelier avec l'installation d'un pack office, d'un anti-virus, d'un raccourci pour permettre au client d'accéder au serveur et les mises à jour Windows Update. Une fois ceci prêt, je me suis rendu chez le client muni d'un switch 8 ports, de câbles RJ45 et d'une multiprise, qui sont des matériels indispensables pour un technicien. Dès mon arrivé chez le client, on m'a tout de suite indiqué où devait être installé le poste. Grâce à la préparation en atelier, il ne m'a fallu qu'une dizaine de minutes pour mettre en route l'ordinateur et répondre aux questions du client concernant son nouveau poste.

Ainsi j'ai pu mener à bien la mission qui m'a été confié en étant rapide et efficace.

Les techniciens peuvent aussi être amenés à installer toutes sortes de matériels informatiques et pas seulement des postes.

4.2 La relation avec le client

Chaque technicien d’Absys Informatique se voit attribué des entreprises clientes. C’est avec ces entreprises que le technicien va effectuer le plus souvent des interventions, des installations de postes, d’imprimantes mais il sera aussi chargé de la préventive. Une préventive a lieu tous les mois, lors de la préventive, le technicien va faire le tour des bureaux pour s’assurer que chaque utilisateur puisse travailler de bonnes conditions avec leurs ordinateurs. C’est aussi l’occasion pour les utilisateurs de poser quelques questions sur le fonctionnement d’un logiciel ou de faire remarquer quelques soucis informatiques qui n’empêchent pas le client de travailler mais qui peuvent le gêner par exemple, la résolution de la fenêtre d’une application qui ne convient pas à l’utilisateur.

La première règle qui permet le succès d’Absys Informatique est la satisfaction du client. Le client doit pouvoir continuer à travailler en permanence, c’est pour cela que les interventions doivent être rapides. La seconde, est de créer un lien entre les clients et les techniciens. C’est pour cela que chaque technicien a son entreprise assignée. Cela permet au client de voir le plus souvent un seul technicien. La relation humaine est un élément essentiel à la réussite de la société. Absys Informatique depuis ses débuts a fait le choix de ne pas faire de publicités ou se médiatiser. C’est par le bouche à oreille qu’Absys s’est construit une renommée et est parvenu à signer de gros contrats, pas seulement au niveau national, mais aussi au niveau international.

5 Conclusion

Ces dix semaines de stages ont été plus que bénéfique pour moi. Dès mon arrivée dans l'entreprise, j'ai pu appréhender la complexité du métier de technicien ainsi que découvrir en profondeur le domaine de l'administration systèmes et réseaux. Il faut faire preuve de concentration et d'une grande rigueur car nous sommes souvent confrontés à de différents problèmes. Pour mener à bien les actions qui m'ont été confiées, j'ai dû faire preuve d'une grande autonomie. Malgré cela, il m'a parfois été nécessaire de poser certaines questions me permettant d'avancer dans mes missions et de participer au bon fonctionnement de l'entreprise. Ces missions m'ont aidé à développer mon sens de l'autonomie et des responsabilités.

Étant étudiant dans le domaine de l'informatique, il m'était facile de comprendre certains termes employés par les techniciens et d'assimiler leurs méthodes de travail. Après dix semaines passées chez Absys Informatique, j'ai réalisé l'ampleur du besoin de l'informatique dans le milieu professionnel.

J'ai pu enrichir mes connaissances dans l'administration systèmes et réseaux. J'ai aussi acquis des connaissances informatiques qui me serviront sûrement dans, la suite de mes études, mon projet professionnel et ma vie de tous les jours. C'était l'un des objectifs pour moi durant ce stage, consolider mes acquis vu en cours et gagner en autonomie. Mais le but pour moi était aussi en pouvant observer le métier de plus près, voir ce qui me manquait pour pouvoir prétendre un jour à un poste similaire dans une entreprise. L'entreprise jouant beaucoup sur les relations humaines entre ses employés et les clients, cela m'a permis de prendre conscience que le sens de la communication est un facteur important à la réussite d'Absys Informatique. Et c'est sur ce point que je dois encore progresser, la communication avec le client.

Arrivé au terme de ce stage, je suis désormais capable d'avoir une idée fixe sur mon avenir professionnel. Je souhaiterai me tourner vers un métier d'administration systèmes et réseaux, car j'ai pu constater que système et réseau sont étroitement lié.

Cette expérience m'a donc permis d'atteindre mes objectifs et j'aimerai beaucoup par la suite intégrer une formation en alternance orienté vers les réseaux.

6 Glossaire

PME, Petite et Moyenne entreprise

DUT, Diplôme Universitaire de Technologie

SCOP, Sociétés coopératives et participatives

VPN, Virtuelle Private Network, Réseau privé virtuel, une connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel

Firewall, Pare-feu

S.I, Système d'information c'est ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information

Domaine, Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble de machines partageant des informations d'annuaire

DNS, Le Domain Name System est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom

LAN, Un réseau local, souvent désigné par l'acronyme anglais LAN de Local Area Network, est un réseau informatique tel que les terminaux qui y participent (ordinateurs, etc.) s'envoient des trames au niveau de la couche de liaison sans utiliser d'accès à internet.

WAN, (*Wide Area Network*), est un réseau informatique ou un réseau de télécommunications couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière.

UTM, Unified threat management en français : *gestion unifiée des menaces*, utilisé pour décrire des pare-feu réseau qui possèdent de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feux traditionnels.

VDOM, Virtual Domain peut être utilisé pour diviser une seule unité Fortigate en deux ou plusieurs instances virtuelles de FortiOS qui fonctionnent comme des unités Fortigate indépendantes

IP, Internet Protocol

IP Publique, les adresses IP publiques ne sont pas utilisées dans un réseau local mais uniquement sur internet. Les routeurs disposent d'une adresse IP publique côté internet, ce qui rend votre box visible sur internet. Mais aussi, lorsque vous accédez à un site web vous utilisez l'adresse publique du serveur web

NAT, network address translation, un routeur fait de la traduction d'adresse réseau lorsqu'il fait correspondre des adresses IP à d'autres adresses IP.

Policy (Policies pl.), ACL

ACL, Access Control List est une liste de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe à un réseau. Ici, gère les entrées et sorties du flux.

RAID, Redundant Array of Independent Disks, est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

Hyper-V, également connu sous le nom de Windows Server Virtualisation, est un système de virtualisation basé sur un hyperviseur. Il permet de gérer des serveurs virtuels

TSE, Terminal Services permet à un utilisateur d'accéder à des applications et des données sur un ordinateur distant, via n'importe quel type de réseau. Son utilisation est optimisée sur des réseaux locaux

Active Directory, est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. 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.

Contrôleur de domaine, lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine. De ce fait, il devra vérifier les identifications des objets, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe

GPO, group Policy, les stratégies de groupe sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.

7 Bibliographie

<http://www.les-scop.coop/sites/fr/les-scop/qu-est-ce-qu-une-scop.html>

<http://cookbook.fortinet.com/vdom-configuration/>

<http://www.absys-info.fr/>

https://fr.wikipedia.org/wiki/Unified_threat_management

<http://www.supinfo.com/articles/single/1176-raid-ses-differents-types>