Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

ADMINISTRATEUR SYSTÈME ET RÉSEAU

Nicolas Grosjean

Admicom

Responsable entreprise : Thomas Dubois

Responsable académique : Djamal Merad

2019

Table des matières

1 Introduction

Dans le cadre de mon DUT réseau et télécommunication j'ai était amener à faire un stage de 2 mois afin de parfaire ma formation. Cette expérience m'a permis d'acquérir de nombreuse compétence, mais également d'affirmer mon choix professionnel qui est de devenir Administrateur systèmes et réseaux.

J'ai donc effectué mon stage d'administrateur système et réseaux chez Admicom, entreprise de cloud privé. Lors de ce stage, j'ai pu suivre et aider l'administrateur système et réseaux. Cela m'a permis d'en apprendre plus sur ce métier, mais également d'acquérir de nombreuse connaissance et compétence, j'ai aussi approfondi tout ce que j'ai pu apprendre à l'IUT.

Lors de mon stage j'ai donc pu, en tant qu'Administrateur système et réseaux mener divers projets au sein de Admicom, mais également dans le DataCenter Dc4Data à Lyon (Figure 1).

Je vous propose dans un premier temps une présentation de l'entreprise Admicom, en seconds lieux les différents projets et différentes taches effectuer lors de mon stage. Pour finir, la conclusion.

Figure 1 : Logo DC4DATA

2 Présentation de l'entreprise

2.1 Géolocalisation

L'entreprise Admicom se situe à Lyon plus exactement à 14, CHEMIN DU JUBIN 69570 DARDILLY (Figure 2).

Figure 2 : Géolocalisation de Admicom

2.2 Admicom

2.2.1 Historique

Admicom est une entreprise de cloud computing depuis 2006 basé à Lyon.
Elle est composée de six collaborateurs. Elle a récemment déménagé afin de grandir et d'être plus proche de son data center afin d'apporter encore plus d'efficacité dans ces prestations.

2.2.2 Activité

Admicom est une entreprise fournissant un service de cloud privé, permettant aux entreprises d'externaliser leurs informatiques afin de ce concentré sur leur cœur du métier. Accompagner et conseiller sont les maitres mots du cloud privé Admicom.

3 Présentation du sujet de stage

3.1 Routeur Virtuel

3.1.1 Présentation

Un routeur virtuel est un ordinateur que l'on transforme en routeur, lors de mon stage il s'agissait d'une machine virtuelle installer sur les serveurs présents dans le Datacenter. Pour ce faire on utilise en général des systèmes d'exploitation de type Unix (Linux).

Dans le cadre de mon stage, je devais concevoir entièrement avec l'aide de mon tuteur une toute nouvelle infrastructure réseau basée sur un minimum de deux routeurs virtuels en redondance, afin de remplacer les deux routeurs Cisco (3845) présents en raison d'un besoin de performance plus élevé, mais également le coût nettement inférieur à l'utilisation de vrai routeur. En effet dans notre cas possédant déjà les serveurs permettant d'héberger nos routeurs virtuels, le coût de mise en place était de l'ordre de 0, le routeur virtuel choisi est entièrement Open Source. La seule contrainte lors de mon stage était l'utilisation de routeur virtuel Pfsense (Figure 3).

Figure 3 : Logo de Pfsense

3.1.2 Pfsense

Pfsense est donc le routeur virtuel que j'ai utilisé afin de mettre en place la nouvelle infrastructure réseau. C'est un routeur/pare-feu virtuel open source basé sur le système d'exploitation Unix FreeBSD. Ce routeur permet de faire tout ce qu'un routeur classique fait, c'est-à-dire routage, NAT*, firewall, utilisation de vlan, etc.

Pfsense est configurable facilement via une interface web intuitive (Figure 4), mais également via ligne de commande Linux (Figure 5).

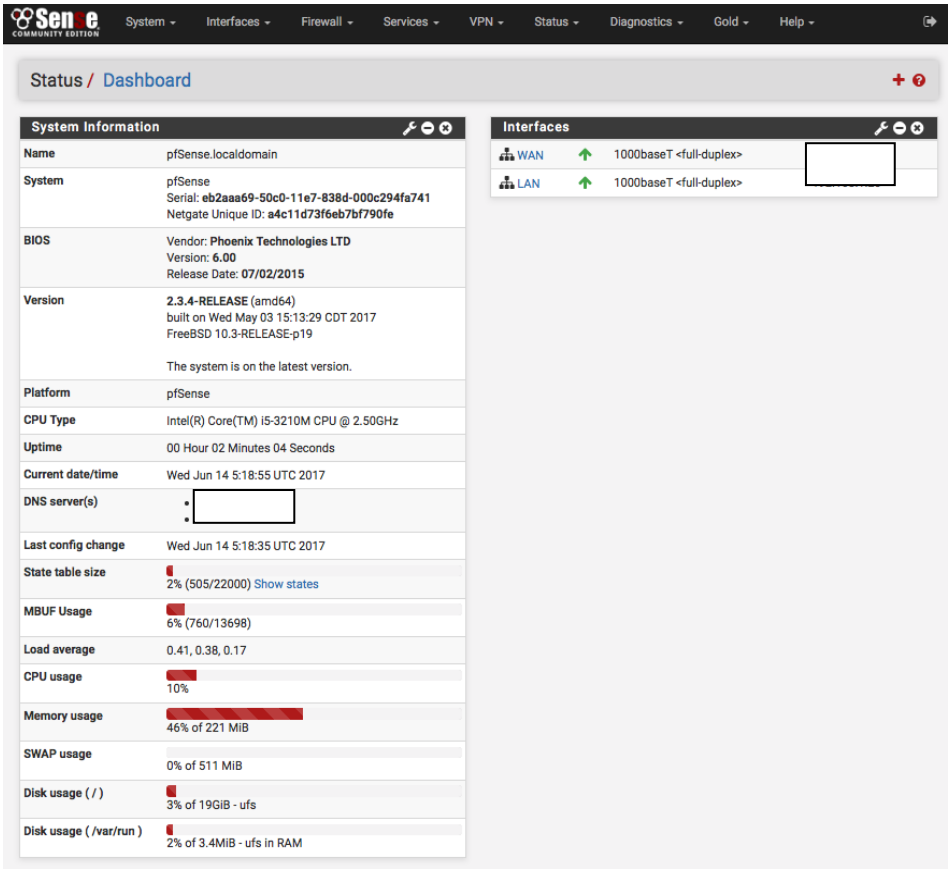


Figure 4 : Page d'accueil Pfsense (WEB)

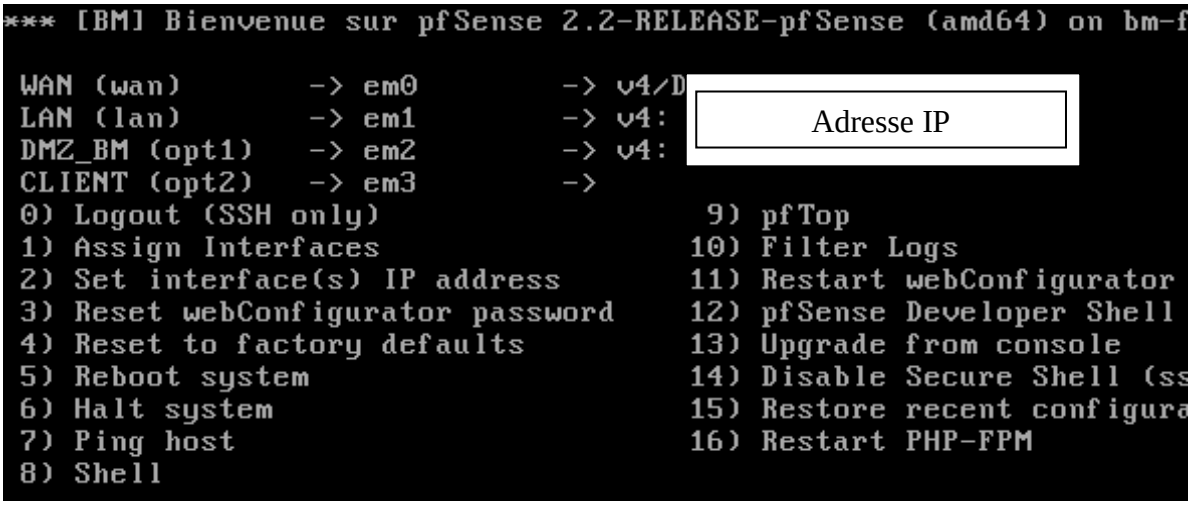


Figure 5 : Pfsense en ligne de commande

3.2 Maintenance des systèmes et des réseaux

Ma deuxième mission consistait à administrer, configurer, entretenir les systèmes et les réseaux présents dans l'entreprise.

En effet je devais vérifier le bon fonctionnement du réseau et des différentes machines virtuelles afin que les utilisateurs utilisant le cloud privé ne soient pas affectés par des lenteurs, des déconnexions ou quelconques problèmes qui pourrait affecter leurs expériences utilisateur.

Je devais également veiller au bon fonctionnement des routeurs Cisco (Figure 6), en cas d'attaque je me devais d'être réactif afin de corriger le problème le plus rapidement possible.

Afin que l'utilisateur puisse se connecter à leur session sur leur machine virtuelle présente sur nos serveurs, j'ai dû configurer plusieurs règles NAT.

J'ai également configuré et monitoré plusieurs VPN. Ces VPN (Figure 7 et 8) permettaient de relier les imprimantes configurer en mode réseaux chez les clients à leurs machines virtuelles présente dans notre réseau, afin de leur permettre d'imprimer directement depuis leur session dite « Admicom » et donc d'améliorer leur expérience utilisateur.

Figure 6 : Logo Cisco

Figure 7 : Logo IPsec

Figure 8 : Logo OpenVpn

4 Présentation du travail réalisé

4.1 Routeur Virtuel

Le principal projet de mon stage était donc de remplacer les deux routeurs Cisco présent par au minimum deux routeurs virtuel Pfsense afin d'améliorer les performances du cloud privé et donc l'expérience utilisateur.

Afin de trouver la configuration la plus optimal pour la nouvelle infrastructure réseau, j'ai été amener à effectuer plusieurs tests.

J'ai effectué tous ces tests sur des machines virtuelles avec Pfsense comme système d'exploitation à l'aide de VMware Workstation Pro (figure 9), qui permet une solution de virtualisation de machine sous n'importe quel système d'exploitation.

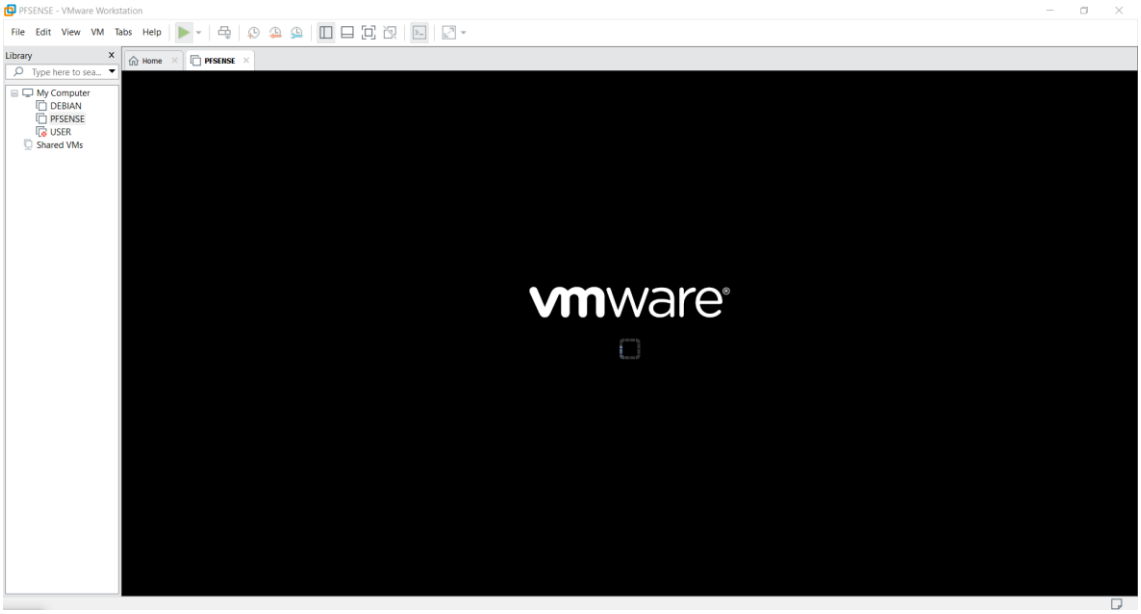


Figure 9 : VMware Workstation Pro

4.1.1 Première configuration

La première configuration (Figure 10) consistait donc à utiliser deux Pfsense en redondance pour une tolérance aux pannes optimales. Afin d'établir la connexion entre les deux Pfsense, je me

suis servie du système de haute-disponibilité intégrer directement à Pfsense afin que le deuxième Pfsense récupère automatiquement la configuration du premier.

J'ai également été amené à utiliser le protocole CARP (Common Address Redundancy Protocol) qui permet de créer un réseau virtuel. Par exemple ici entre les deux Pfsense il y a un protocole CARP ce qui permet de configurer le réseau virtuel comme Gateway du réseau des serveurs Admicom.

Il y a donc un système de « Maitre esclave » entre les deux Pfsense bien entendu pour le routage, mais également pour les VPN.

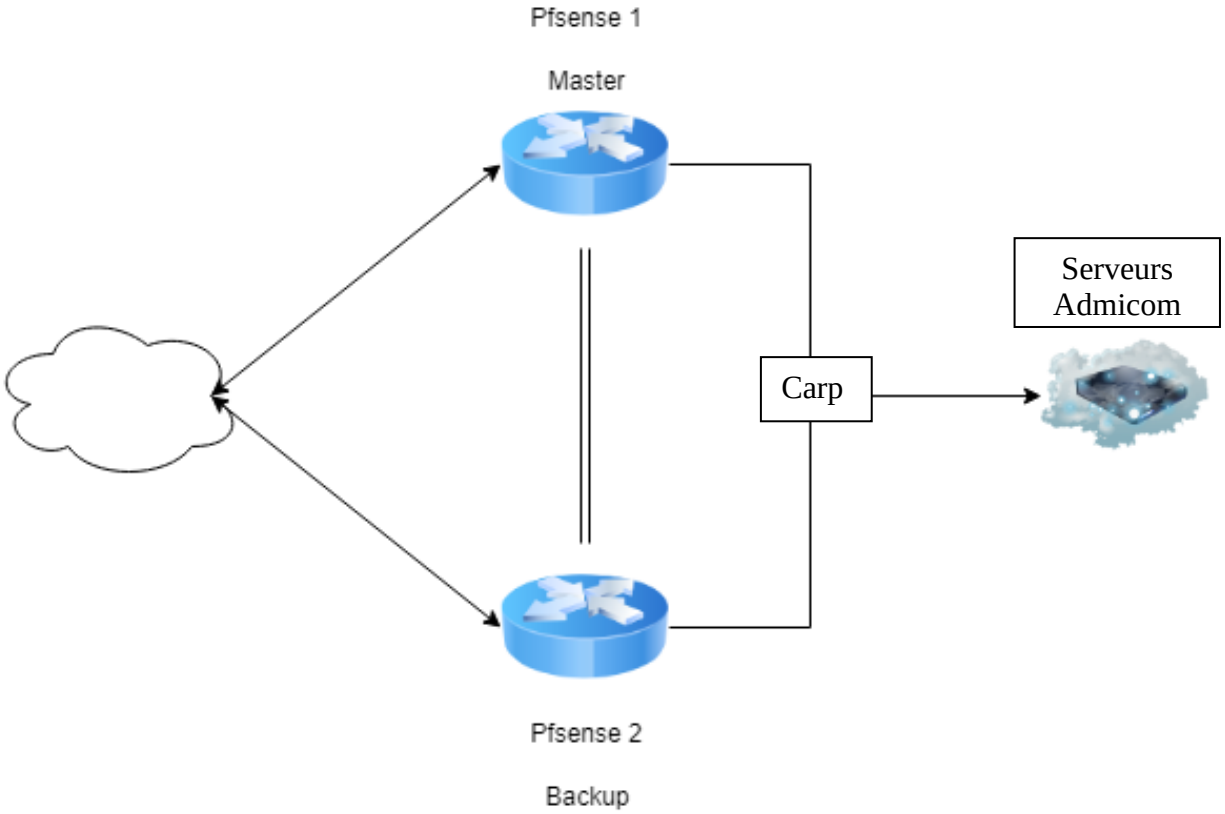


Figure 10 : Schéma configuration 1

Après de nombreux tests, mon tuteur et moi-même avons décidé d'abandonner cette configuration. En effet à cause de l'impossibilité de faire du NAT post-routing, c'est-à-dire faire en sorte que le NAT se fasse uniquement après le routage donc après être arrivé au bon Pfsense (Le Master).

4.1.2 Seconde configuration

Dans un deuxième temps nous avons donc décidé de revoir totalement la configuration et de faire un équilibrage des charges entre les deux Pfsense (Figure 11).

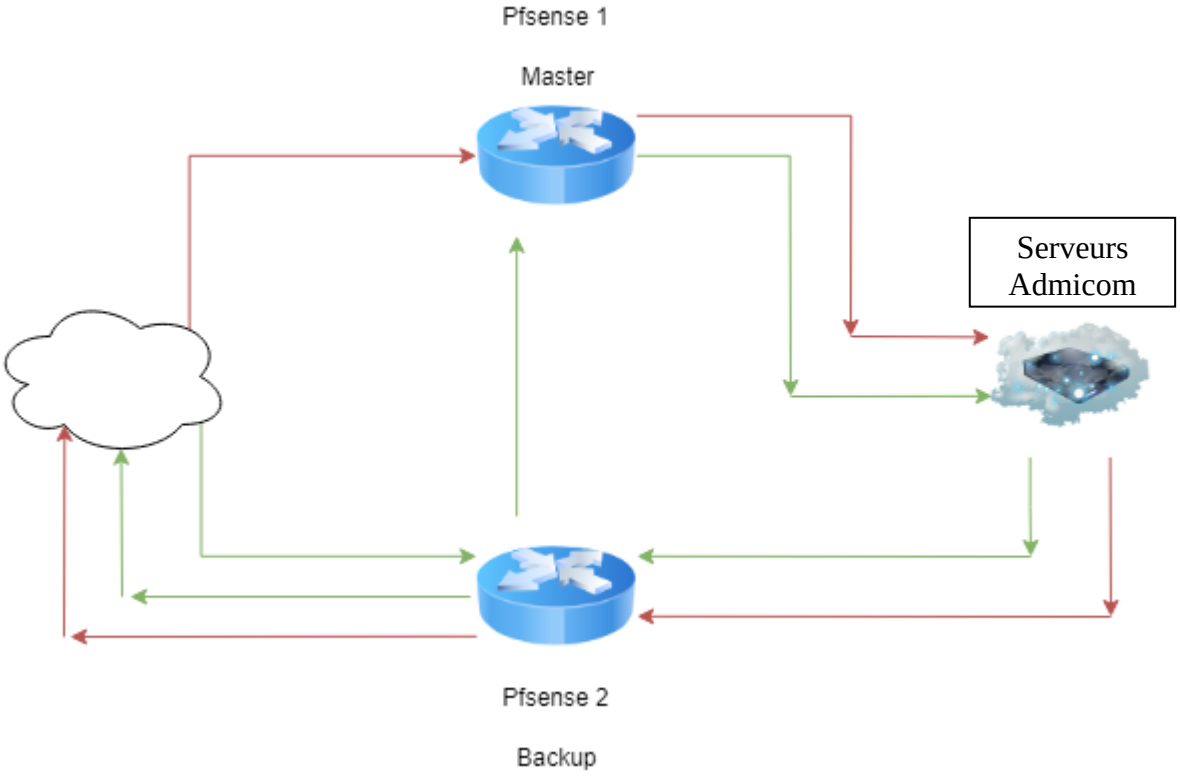
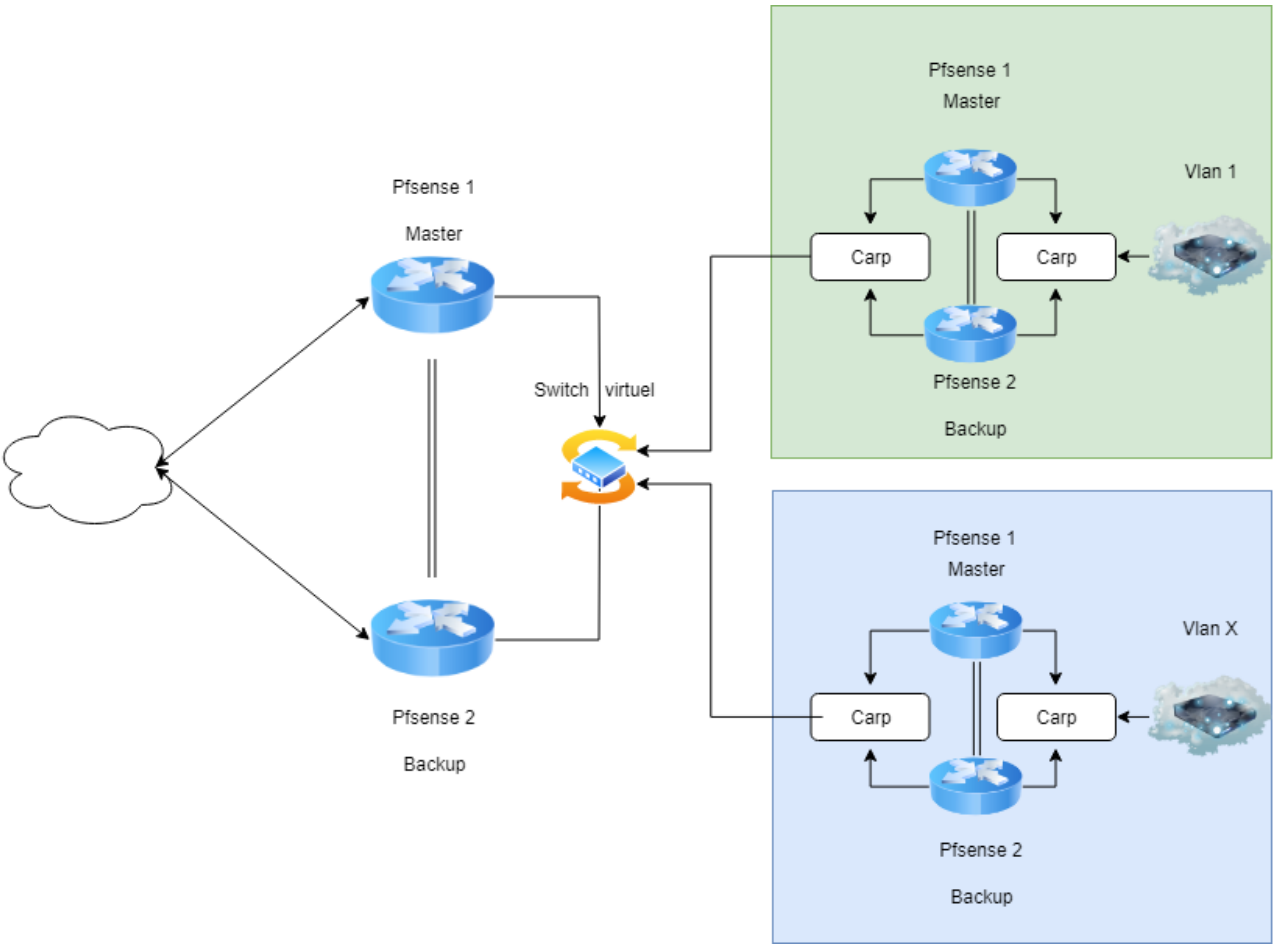


Figure 11 : Schéma configuration 2

L'idée était donc de faire passer tout le trafic entrant par un Pfsense et tout le trafic sortant par l'autre. Mais après plusieurs tests nous nous sommes rendu compte que cela était certes faisable, mais pas du tout tolérant aux pannes, mais également pas optimal pour notre cahier des charges. En effet les VPN ne fonctionnaient pas convenablement et le réseau avait une petite lenteur non tolérable pour les utilisateurs. Après concertation nous avons décidé de ne pas continuer dans cette voie-là et de revenir sur la première configuration en ajoutant plusieurs autres Pfsense.

4.1.3 Configuration finale

Pour la configuration finale (Figure 12) nous avons donc en effet décidé de revenir sur la première configuration, mais en ajoutant plusieurs Pfsense.



Nous avons utilisé un nombre de Pfsense assez conséquent, soit 2 fois le nombre de VLAN (1 VLAN par client) présent dans l'infrastructure réseaux. Cette méthode nous permet d'utiliser les deux premiers Pfsense uniquement pour la partie routage, le routage BGP (Border Gateway Protocol) est le protocole de routage choisi dans notre infrastructure. Les autres Pfsense sont uniquement dédiés au VPN et au NAT. Après plusieurs tests et concertations, nous avons donc décidé d'utiliser ce modèle pour mettre en place la nouvelle infrastructure réseau.

Mais malheureusement suite à des problèmes avec notre fournisseur internet et un manque d'adresse IP publique nous n'avons pas pu finir la mise en place de cette nouvelle infrastructure. Mais tous les tests effectués on était concluant et cette infrastructure sera bien la future infrastructure réseau en place.

4.2 Maintenance des systèmes et des réseaux

4.2.1 Datacenter

J'ai eu la chance d'être en charge d'aller au Datacenter en cas de besoin urgent ou non. Parmi les missions que j'avais au Datacenter il y avait les missions dites « de maintenance », c'est-à-dire changer les câbles réseaux, ajouter des câbles réseaux en cas de besoin, changer les disques dures défaillants, en ajouter de nouveau.

J'ai également eu la chance de mettre en place un nouveau NAS Qnap (Figure 13) au Datacenter.

Figure 12 : Logo de Qnap

Malheureusement j'ai eu la chance de devoir analyser, traiter, et contrer plusieurs attaques subites sur notre réseau. En effet, suite à plusieurs attaque subit sur notre réseau j'ai été amener à travailler dans le Datacenter directement sur le routeur Cisco via un câble console et le logiciel Putty afin d'avoir accès au routeur Cisco en « console » (Figure 14).

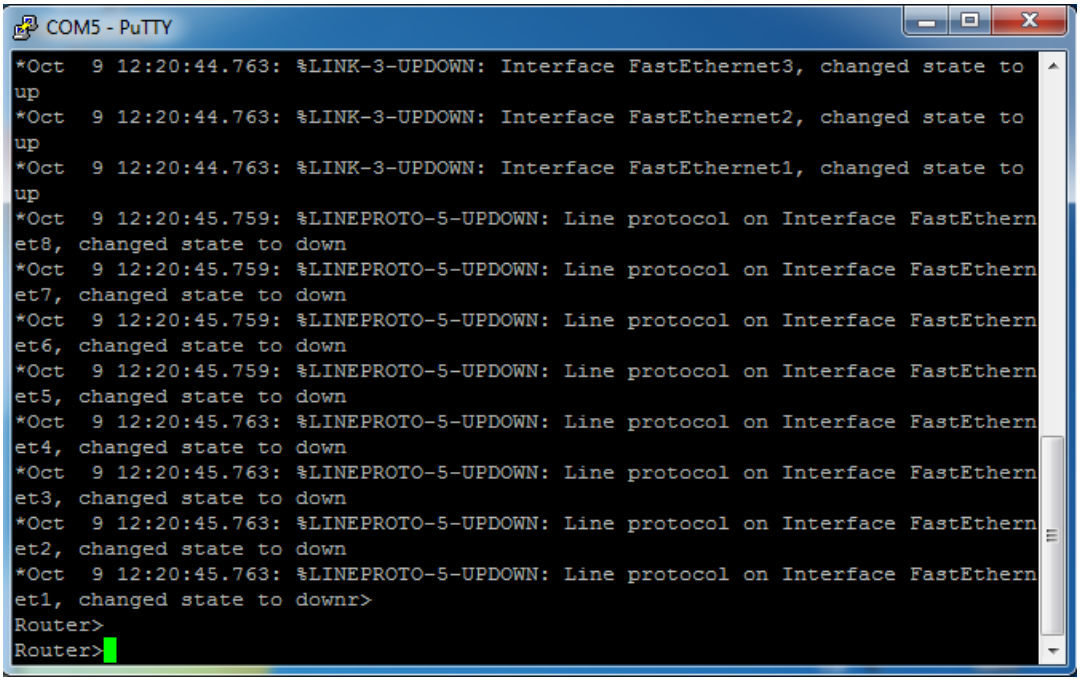


Figure 13: Fenêtre Putty de l'accès en console sur le routeur Cisco

4.2.2 Résolution de problème réseau

Nous avons subi plusieurs types d'attaques, la première étape était d'identifier le problème.

La première attaque était des robots qui tentait de se connecter aux machines virtuelles en boucle via une attaque par Brute-Force, qui consiste à essayer toutes les combinaisons possibles de mot de passe afin de trouver le bon.

Suite à ce genre d'attaque il a fallu mettre en place un script qui au bout de X tentatives, une ACL (Acces List) était créée automatiquement afin de bloquer l'adresse IP utiliser par le robot. Après plusieurs essaie mon tuteur et moi-même avons fini par mettre en place le script qui crée une ACL toutes les 10 minutes avec toutes les adresses IP à bloquer et qui supprimer l'ancienne ACL.

Suite à la mise en place de se script il a également fallu mettre en place une 'whitelist' afin de ne pas bloquer les adresses IP des utilisateurs qui aurait éventuellement fait trop de tentative de connexion et qui aurait était détecter par le script.

Le deuxième type d'attaque était des attaques par DOS (attaque par déni de service). En effet nous avons subi plusieurs attaques par inondation du réseau, c'est-à-dire de nombreuse tentative de connexion afin d'empêcher le bon fonctionnement du réseau.

Dans notre cas cella rendait la table NAT trop importante ce qui entraine un fort ralentissement du routeur et de toutes les connexions établies, et donc de forts ralentissements pour nos utilisateurs.

Pour pallier ce problème dans l'urgence il fallait vider la table de NAT du routeur à l'aide de la commande « clear ip nat translation ». Mais cela entrainait malheureusement la coupure de toute les connexions actives et donc la déconnexion de tous les utilisateurs connecter sur nos serveurs. Avant cela il fallait tout de même essayer d'identifier l'IP public des attaquants afin de les bloquer pour éviter qu'ils réitèrent leurs attaques.

Nous avons également subi certains problèmes réseau qui entrainait de forts ralentissements sur notre réseau.

Le premier problème s'agissait également de table de NAT trop importante. En effet suite à la mise en place de nouvelles imprimante coté client et d'une mauvaise configuration de leur part, les imprimantes tenter de se connecter aux machines virtuelles par le VPN mis en place, mais suite à une mauvaise configuration la connexion ne s'établissant pas, les imprimantes relancer la connexion et donc remplissait la table de NAT.

Pour pallier ce problème, nous avons mis en place une ACL afin de bloquer les connexions du réseau privé des machines virtuelles au réseau privé de nos serveurs.

Suite à la mise en place de cette ACL il nous a fallu nous assurer qu'aucun utilisateur n'était impacté par cette ACL.

Le second problème était les différentes erreurs faites par nos utilisateurs, par exemple une utilisation de serveur/client FTP trop importante et donc une utilisation de la bande passante trop importante qui entrainait des ralentissements pour l'ensemble des collaborateurs utilisant la même machine virtuelle. Pour pallier ce genre de problème nous avons dû sensibiliser nos utilisateurs.

4.2.3 Amélioration et création des outils.

Durant mon stage j'ai été amené à améliorer et créer différents outils afin d'améliorer l'expérience utilisateur.

En effet j'ai dû créé un site web (Figure 14) qui permettait de vérifier le statut de la connexion entre le client et le serveur Admicom mais également le statut de la connexion entre le serveur Admicom et les différents sites importants comme google.fr, orange, OpenDNS. J'ai également ajouté sur cette page un lien direct pour télécharger TeamViewer pour faciliter le téléchargement de TeamViewer par l'utilisateur.

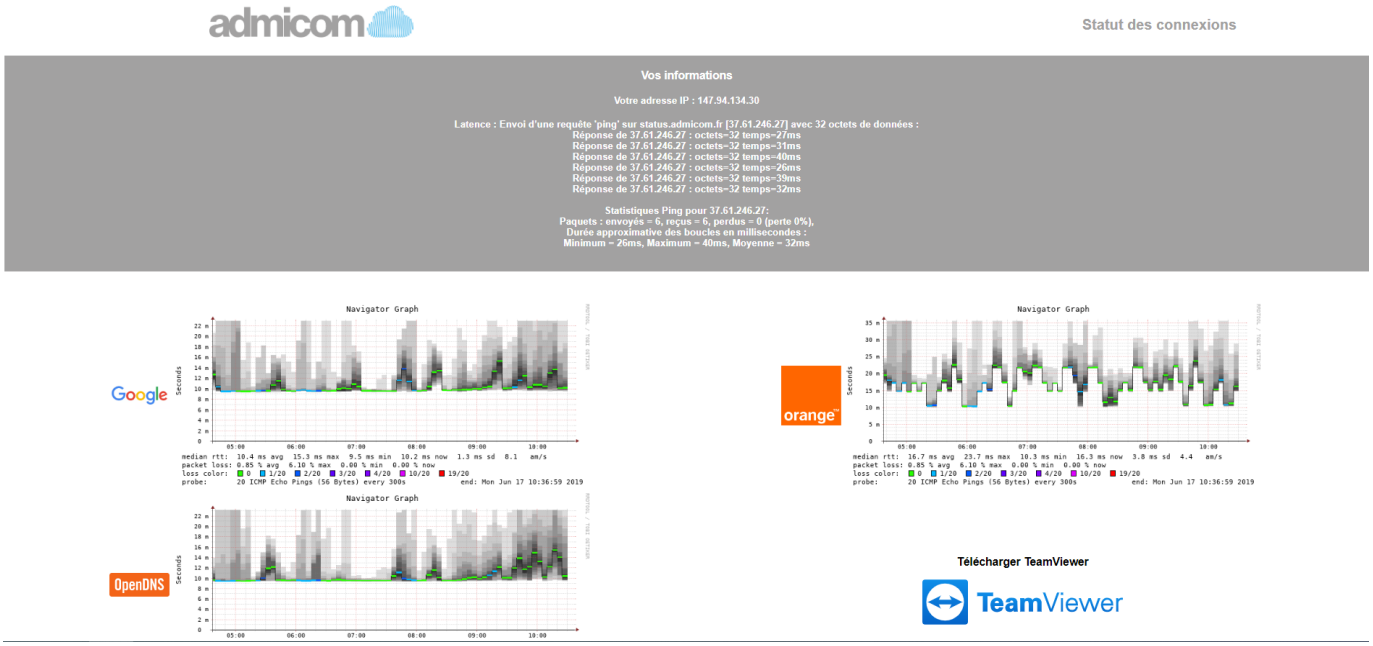


Figure 14 : http://status.admicom.fr

Les graphiques présents sur le site sont des graphiques mis à jour à chaque rechargement de page. Ces graphiques sont générés avec l'outil SmokePing (figure 15) que j'ai était amené à installer sur une machine virtuelle CentOS déjà présente et qui sert à monitoré différent aspect du serveur Admicom. SmokePing est un logiciel qui permet de conserver un historique de la latence du réseau.

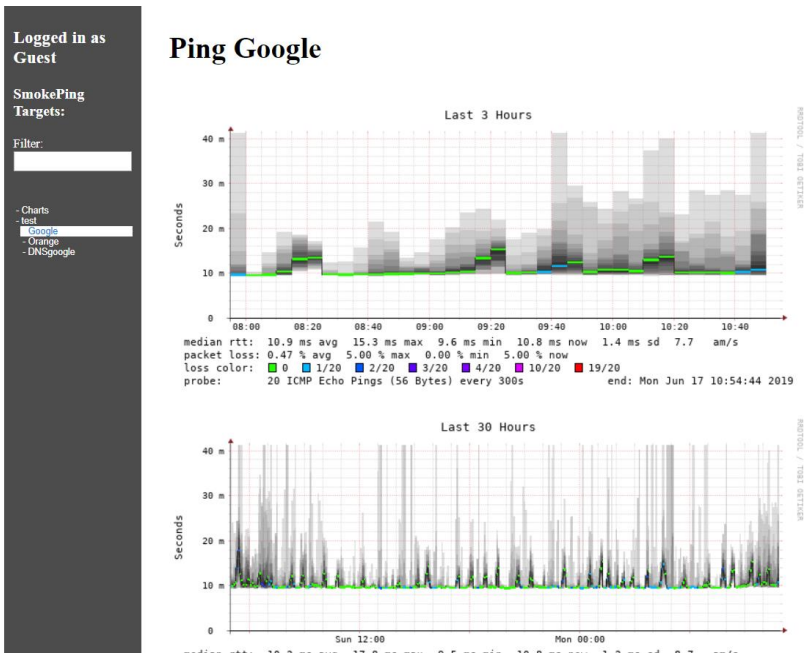


Figure 15 : Onglet Google du SmokePing mis en place

J'ai également était amené monitoré une page web (figure 16) permettant de faciliter le travail des collaborateurs Admicom, en particulier le travail du support informatique. Cette page permet d'avoir des informations sur les différents clients, leurs machines virtuelles, leurs vlans, etc.

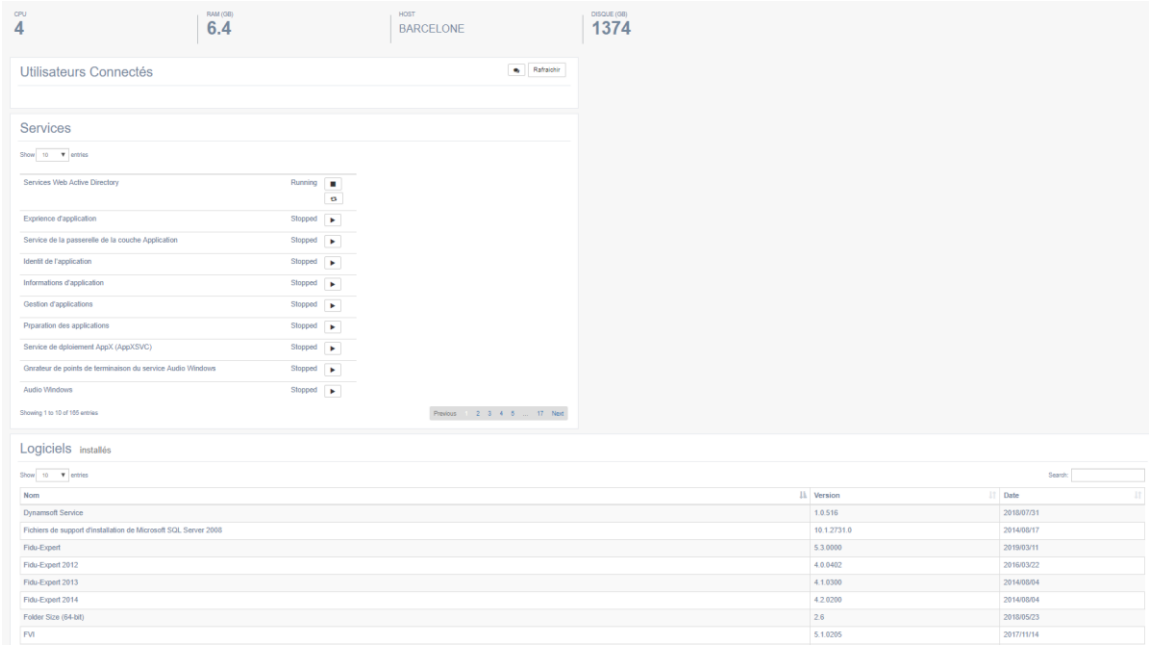


Figure 16 : exemple d'information sur une VM client

Pour des raisons de confidentialité, je ne peux divulguer plus d'information sur cette page web.

4.2.4 Raspberry

Afin d'améliorer l'expérience utilisateur, j'ai dû configurer un Raspberry PI avec un serveur d'impression CUPS (Figure 17). Le Raspberry devait également avoir un client OpenVpn relier au Pfsense afin d'assurer la connexion entre le Raspberry et le Pfsense quelque soit l'endroit où sera mis en place le Raspberry PI. (cf. annexe)

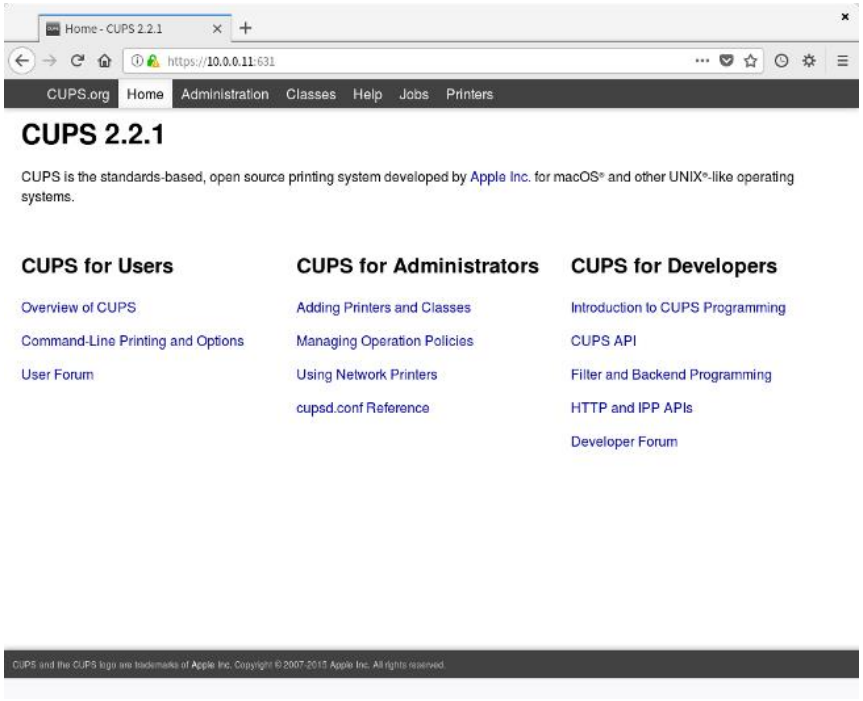


Figure 17 : Page d'accueil CUPS

Le Raspberry PI une fois mis en place, chez tous les clients ayant besoin d'imprimantes en VPN, permettra d'éviter de devoir configurer un VPN site-a-site (Figure 18) directement sur notre routeur Pfsense et sur le routeur client.

Un VPN site-a-site permet de relier deux réseaux privés distants sans avoir besoin de configurer du NAT en redirection de port. Cette configuration permet donc de faciliter le travail de l'équipe technique Admicom, mais également d'améliorer l'expérience utilisateur.

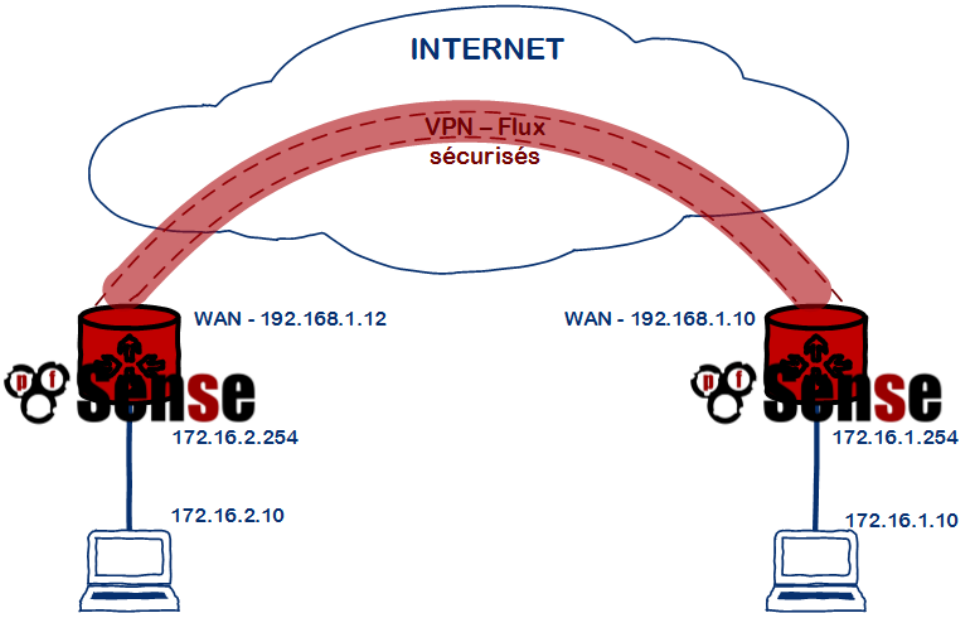


Figure 18 : Schéma VPN site-a-site entre deux Pfsenses

4.2.5 NextCloud

Mon dernier projet a été de créer une machine virtuelle avec Ubuntu et d'installer OwnCloud qui est un serveur de fichier pour un client. Le but était donc d'installer et de configurer OwnCloud afin que l'utilisateur puisse stocker et consulter leurs fichiers de n'importe où, mais également monter ce serveur de fichier en chemin réseau sur Windows (Figure 19).

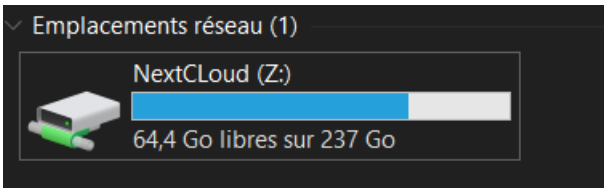


Figure 19 : Lecteur réseau monter sur Windows 10

Pour ce faire il fallait connecter la machine virtuelle au même domaine que la VM client. Par la suite à l'aide de LDAP (Lightweight Directory Acces Protocol) j'ai dû configurer la liaison entre OwnCloud et l'AD (active directory) afin de synchroniser automatiquement les identifiants de connexion de tous les utilisateurs des RDP (Remote desktop protocol) afin qu'ils puissent se connecter au serveur OwnCloud avec les mêmes identifiants.

Après la mise en place de OwnCloud et quelques tests, mon tuteur et moi-même avons décidé de tester NextCloud qui est un dériver de OwnCloud. Et après plusieurs tests concluants, nous avons décidé d'utiliser NextCloud (Figure 20) qui est beaucoup plus complet et correspondait au cahier des charges donné par le client.

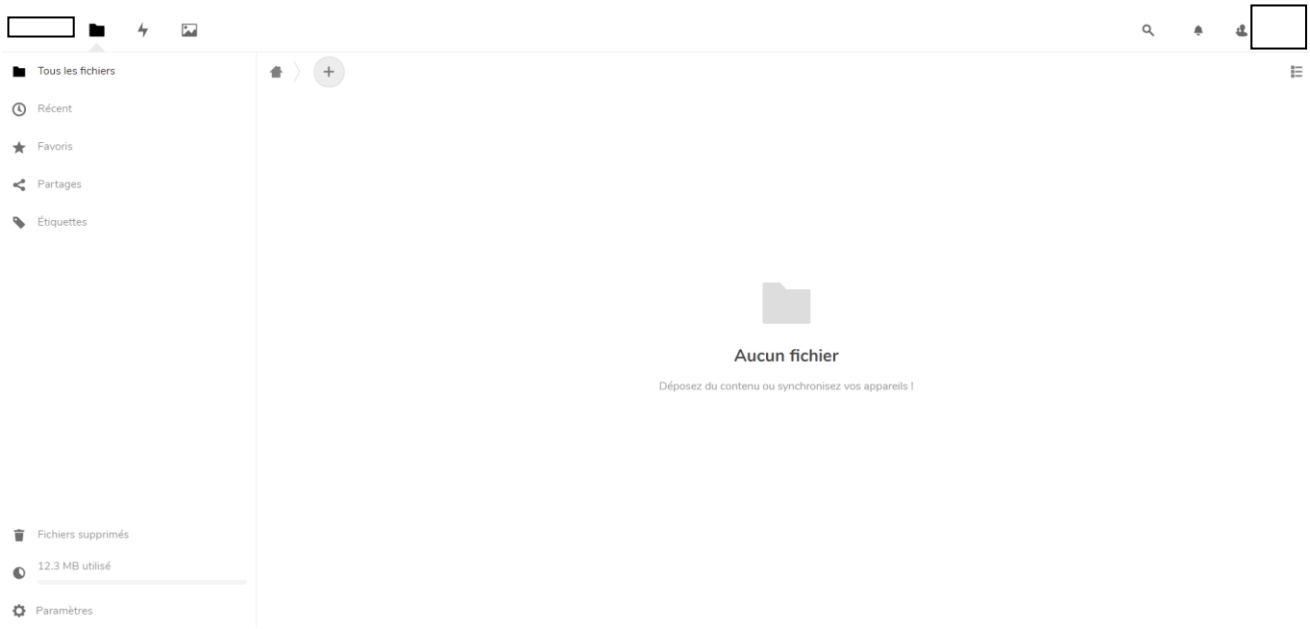


Figure 20 : Page d'accueil NextCloud

4.3 Cloud

4.3.1 Gestion de machine virtuelle

Lors de mon stage, j'ai été amené à travailler sur le Cloud de Admicom en particulier sur le management des serveurs. Mon travail consister à monitoré les serveurs, c'est-à-dire surveiller la RAM et le processeur afin d'éventuellement déplacer certains VM client sur un autre hôte afin d'équilibrer la charge sur les serveurs.

J'ai également été amené à travailler sur Hyper-V (Figure 21) qui est l'outil de virtualisation de Microsoft.

Figure 21 : Logo Hyper-V

En effet je devais également monitorer les VM clients, de la même façon que les serveurs, mais également vérifier leurs espaces de stockage afin que l'utilisateur ne soit jamais impacté par un manque de place. J'ai donc été amené à utiliser des outils comme CCleaner.

4.3.2 Support

Durant mon stage j'ai également participé au support technique, j'ai tout d'abord fait un travail d'observation afin de me former.

En seconds lieux j'ai effectué le travail de support téléphonique. J'ai donc été amené à appeler des clients ou prendre des appels téléphoniques. Pour ce faire j'ai eu à utiliser différents outils comme par exemple TeamViewer (Figure 22) qui est un logiciel de prise en main à distance d'un ordinateur.

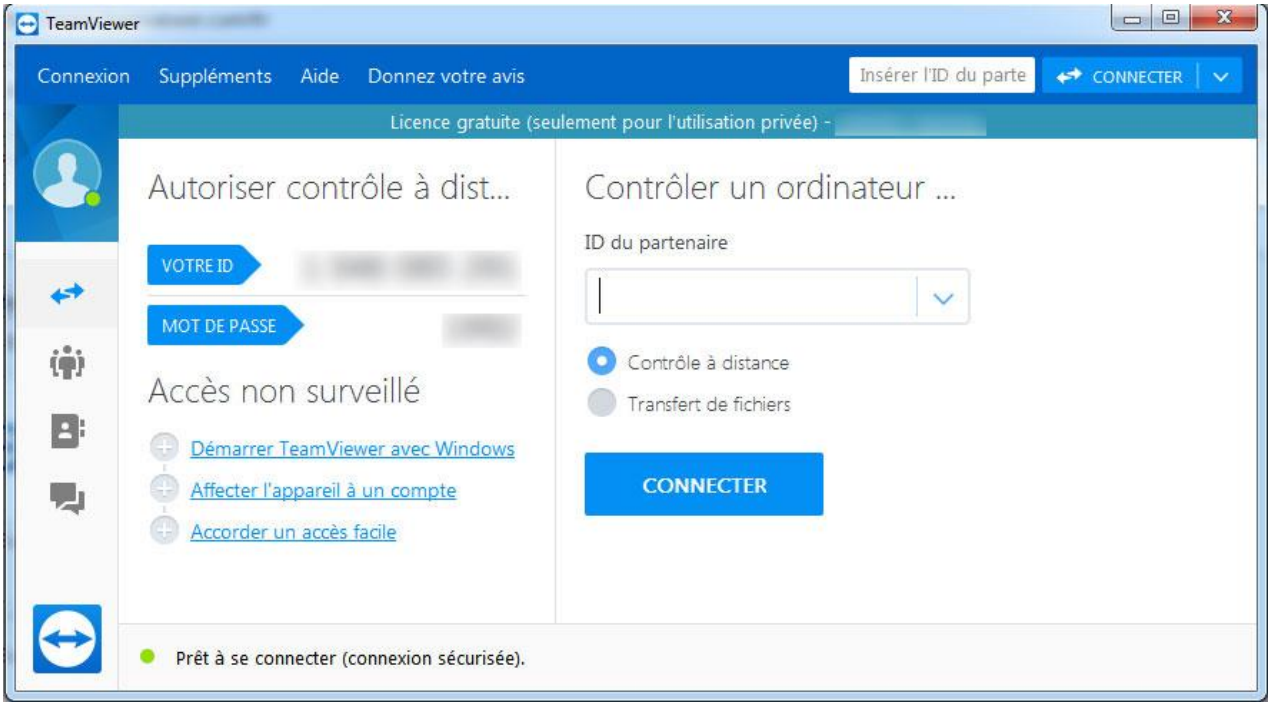


Figure 22 : Page d'accueil de TeamViewer

J'ai utilisé également tous les outils Admicom nécessaires au travail de support que je ne pourrais détailler pour des raisons de confidentialité.

5 Conclusion

Pour conclure, j'ai eu la chance de participer à plusieurs projets notamment le projet de changement de l'infrastructure réseau, mais malheureusement j'ai n'ai pas eu l'occasion de voir la fin du projet. Mais également des petits projets comme NextCloud ou la page statuts.amdicom.fr qui m'ont permis de découvrir de nouveaux outils comme Smokeping, mais aussi de m'améliorer dans le domaine de la virtualisation.

Le projet qui ma tenue le plus à cœur a donc était la virtualisation des routeurs. L'initiation au travail de support informatique m'a permis d'élargir mon panel de compétence et de découvrir un tout autre aspect du travail d'administrateur système et réseau.

Ce stage en tant qu'administrateur système et réseau ma également permis d'affirmer mon choix professionnel de devenir un administrateur système et réseau.

Remerciements

Je tiens tout d’abord remercier Nicolas Moret le dirigeant de Admicom de m’avoir accepté en tant que stagiaire au sein de Admicom.

Je remercie également mon tuteur de stage Thomas Dubois, ainsi que toute l’équipe Admicom pour leur accueil et leur bienveillance.

Je souhaite remercier toute l’équipe pédagogique de l’IUT qui mon permit d’acquérir de nombreuses connaissance et compétences.

6 Glossaire

DUT, Diplôme Universitaire de Technologie

Cloud, Consiste a exploité la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet

VPN, Virtual Private Network

NAT, Network Address Translation

VM, Virtual machine

7 Sitographie

https://doc.ubuntu-fr.org/ documentation Ubuntu, utilisé pendant tout le stage.

https://nextcloud.com/ documentation nextcloud, utilisé pendant la semaine du 10 juin.

https://owncloud.org/ documentation owntcloud, utilisé pendant la semaine du 10 juin.

https://docs.netgate.com/pfsense/en/latest/ documentation Pfsense, utilisé pendant tout le stage.