Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

AUTHENTIFICATION FORTE

NICAISE Alexandre
Institut Paoli-Calmettes

Responsable entreprise : Eric Mauge

Responsable académique : Merad Djamal

2018

Remerciements

Je tiens à remercier mon responsable de stage Eric Mauge ainsi que l'équipe de l'infrastructure, Julien Aliaga, Michael Weber, Fabrice Etienne et Renaud Landi pour leur accueil. Mais aussi Sylvain Fluzin, le Directeur du Système d'Information et de l'Organisation, de m'avoir accepté en tant que stagiaire au sein du service de la DSIO.

Je remercie également Mehdi Kardous pour son accueil et son soutien technique.

D'une façon plus générale, je remercie l'ensemble de la DSIO, que ce soit l'assistance ou le fonctionnel, pour l'aide qu'ils m'ont apporté durant l'ensemble de mon stage.

Je remercie de même mon tuteur de stage pour son encadrement pendant celui-ci.

Sommaire

I. Présentation de l'entreprise

1. L'entreprise

Fondé en 1923, l'institut Paoli-calmettes est une structure privée à but non lucratif.
L'institut est un des 18 centres régionaux de lutte contre le cancer en France, il se situe à Marseille.

En tant que Centre de Lutte Contre le Cancer (CLCC), il est qualifié d'Etablissement de Santé Privé (ESPIC) par le code de la santé publique et est chargé d'une mission de service public hospitalier en cancérologie : prévention et dépistage du cancer, recherche en cancérologie, prise en charge des patients (diagnostique et clinique) et enseignement/formation continue en cancérologie.

2. Le service informatique

Le service informatique ou DSIO (Direction du Système d'Information et de l'Organisation) s'occupe de la maintenance informatique de l'institut. Il gère également le réseau de l'institut, ses serveurs et la mise en place des différents logiciels pour la vie de celui-ci. La DSIO est composée de plusieurs parties :

- La cellule assistance, qui s'occupe de conseiller et de résoudre les problèmes que peuvent rencontrer les utilisateurs
- L'équipe infrastructure, qui gère toute la partie réseau et serveurs de l'Institut
- Le groupe projet, qui s'occupe des projets logiciels pour améliorer le quotidien des utilisateurs

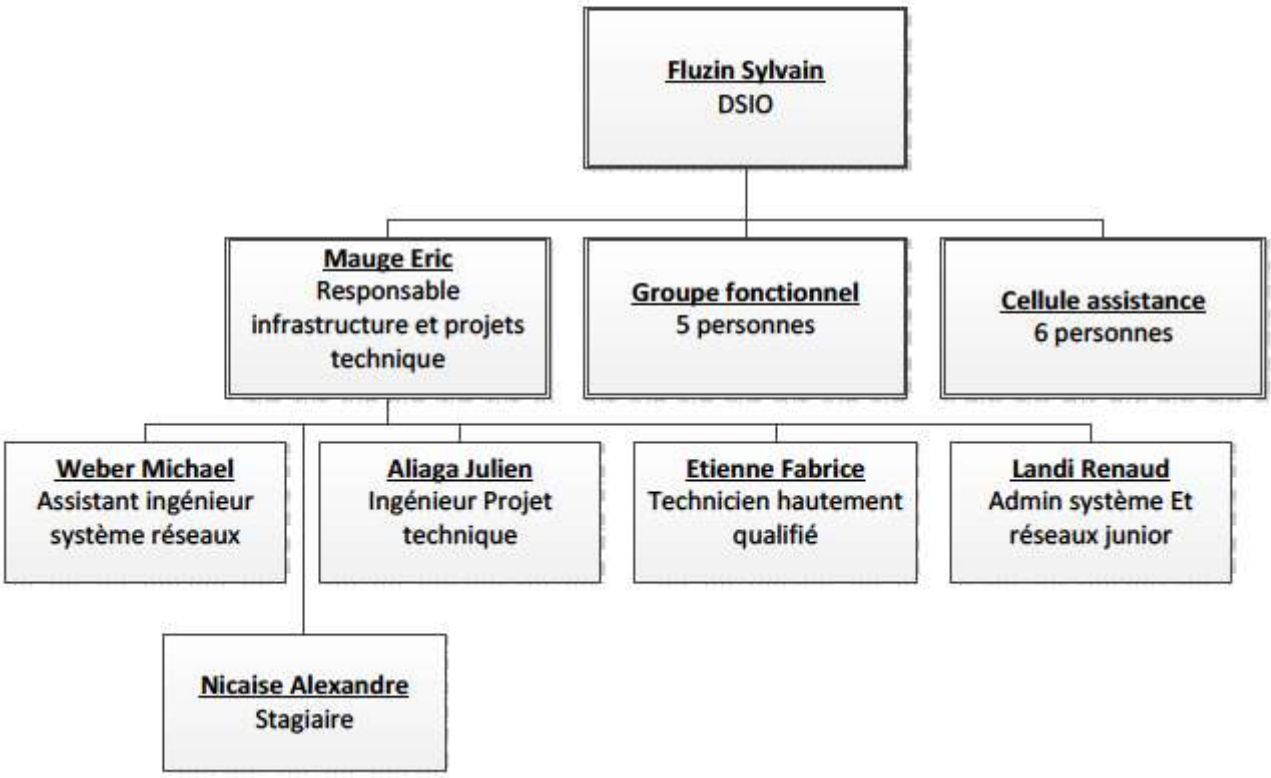


Figure 1 : Organigramme DSIO

Voici ci-dessus l'Organigramme de la DSIO, j'ai effectué mon stage aux seins de l'infrastructure qui a pour responsable Mauge Eric.

Dans l'équipe : Weber Michael s'occupe de la partie Administration et système réseaux, Aliaga Julien s'occupe de la partie réseaux et matériel Biomédical, Etienne Fabrice de la partie gestion des comptes utilisateurs (création, modification, suppression) et Landi Renaud étudiant en alternance gère la téléphonie des bâtiments.

II. Présentation du sujet de stage

1. Enoncé du projet

Du 09 Avril 2018 au 15 Juin 2018, j'ai effectué un stage au sein de l'Institut Paoli-Calmettes (situé à Marseille). Au cours de ce stage au département informatique de l'IPC, j'ai pu m'intéresser à l'infrastructure réseaux d'une grande entreprise, et à l'aspect relationnel des projets. Le premier projet pour lequel la DSIO m'a choisi était la mise en place du réseau et de la téléphonie dans un nouveau bâtiment, malheureusement la construction de celui-ci a pris du retard, provoquant un changement d'objectif pour mon stage. Je dois maintenant installer l'authentification forte sur les serveurs, puis enrôler les utilisateurs concernés c'est-à-dire les cadres et les médecins. Au-delà d'enrichir mes connaissances en informatique et en sécurité, ce stage m'a permis de comprendre dans quelle mesure les relations humaines sont importantes pour mener à bien des projets.

2. Authentification forte

L'authentification forte est, en sécurité informatique, une procédure d'identification qui requiert la concaténation d'au moins deux facteurs d'authentification. C'est une méthode de connexion sécurisé et obligatoire dans les établissements sensibles (hôpitaux, militaire...) Il existe 3 facteurs d'authentification :

-Quelque chose que l'on connaît : mot de passe
-Quelque chose que l'on possède : son téléphone, une carte à puce
-Quelque chose que l'on est ou fait : empreinte digitale, rétinienne

Cette méthode est aussi de plus en plus fréquemment proposée par des services en ligne grand public : les banques, réseaux sociaux… Selon l'importance du service il est recommandé d'activer l'authentification à deux facteurs lorsque celle-ci est disponible.

3. Problématique

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de l'informaticien mais est étendue à tous les utilisateurs, c'est-à-dire a tous les professionnels de santé qui souhaitent accéder aux dossiers des patients depuis l'extérieur. En effet ces professionnels ont la capacité de remplir des prescriptions informatisées, de prendre des rendez-vous ou de rédiger des comptes rendus.

Les systèmes de sécurité des établissements de santé sont fortement recommandés, pour les accès extérieurs par deux acteurs :

-l'ASIP santé (Agence des Systèmes d'Information Partagés)

- la MS santé (Messagerie Sécurisée).

L'Institut Paoli-Calmettes a reçu une demande de l'ASSIP santé pour mettre en place l'authentification à deux facteurs d'authentification, pour les connexions extérieures.

III. Présentation du travail réalisé

PARTIE 1 : Mise en place

1. Introduction

Comme vu précédemment dans la problématique, l'IPC a décidé de mettre en place une connexion sécurisée depuis l'extérieur. Cela répond à la demande de l'ASIP et de la MS santé.
Nous voulons donc rendre notre infrastructure VDI sécurisée, pour cela nous allons mettre en place des reverses proxy Vmware via un portail unifié avec l'association du partenaire historique de l'IPC qui est Imprivata[1] pour la partie One Time Password sur le portail d'accès.

Pour ce faire il a fallu mettre à jour et installer différents logiciels, certains étaient déjà mis à jour, les plus sensibles, pour le reste je m'en suis occupé à l'aide de mon tuteur.
La mise en place est séparée en 4 étapes :

- MAJ vcenter/vsphere pour serveur
- MAJ de la replication de vsphere pour une Virtual Machine
- Installation du cluster SQL
- Installation de View (Connexions serveur, Workspace One et Access Point)

1 : Imprivata est une société de sécurité informatique.

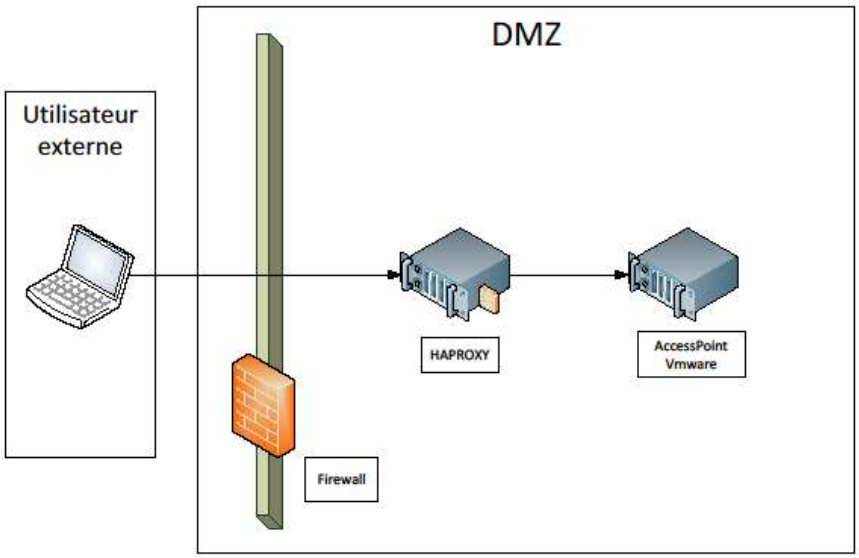
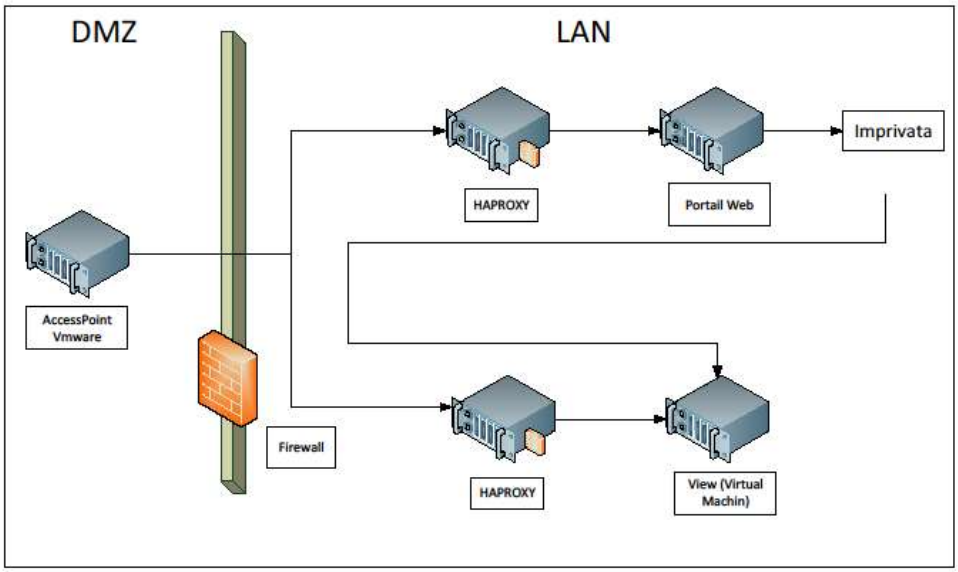


Figure 2 : Schéma de la solution user/DMZ

La Base de la connexion s'effectue dans ce schéma. Lors de cette phase l'utilisateur rentre l'adresse du portail web depuis l'extérieur (https://portail.ipc.unicancer.fr). Sa requête rentre dans la DMZ[1] de l'IPC, puis passe par le firewall et est intercepté par le HAPROXY (qui est le reverse proxy) pour être analysée. Quand la requête est validée, elle est envoyée à l'access point qui va permettre de continuer la connexion, voir Figure 3 :



3 : Schéma de la solution DMZ/LAN

1 : Zone dématérialisé, c'est une zone public séparée d'internet par un pare-feu.

Dans la deuxième phase, la requête de l'utilisateur passe dans la partie privée de l'infrastructure, pour ce faire, elle traverse un autre firewall. Puis arrive sur le HAProxy du portail web. A ce moment l'utilisateur renseigne ses identifiants sur le portail web, si toutes les informations concordent avec la base de données d'Imprivata alors l'utilisateur est redirigé sur le HAProxy de sa machine virtuelle. L'utilisateur est connecté à sa machine virtuelle depuis l'extérieur de l'IPC.

2. Les bases avant mon arrivé

Le jour de mon arrivée, certaines étapes du projet étaient déjà validées, les plus compliquées ou les plus sensibles tels que les HAProxy ou le cluster SQL. Certaines méthodes nécessaires à l'authentification forte étaient aussi nécessaires auparavant comme le VDI.

a. Virtual Desktop Infrastructure

L'Institut Paoli-Calmettes ne possède pas (ou très peu) de PC lourd c'est-à-dire d'ordinateur physique, pour remplacer ce genre de PC, la DSIO a installé des Client Léger qui permettent la connexion à une machine virtuelle. Les utilisateurs son capables de se connecter à n'importe quel client léger via leur identifiant et leur code IPC ou via une carte magnétique.

Figure 4 : Client léger

Figure 5 : boitier Imprivata

Figure 5 : écran de connexion

La session de l'utilisateur est hébergée sur le serveur et non sur un PC d'où l'utilité des clients légers, l'utilisateur se retrouve alors toujours avec la même session même si il se connecte avec un client léger différent à chaque fois. Cela est très utile pour les interventions de la DSIO ou pour les infirmiers qui sont amenés à bouger dans le service. L'utilisateur pourra alors choisir sa machine après la page d'authentification

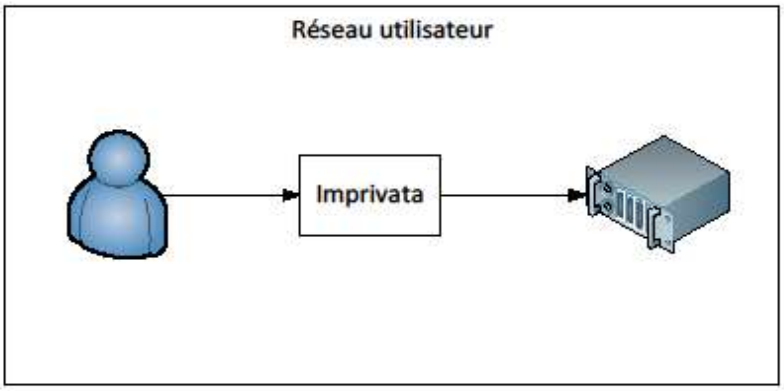


Figure 6 : Réseau Utilisateur

Pour la partie réseau interne, la connexion est beaucoup plus simple, l'utilisateur arrive sur un poste avec l'écran de connexion, puis il s'authentifie. Si l'authentification est validé par Imprivata, alors l'utilisateur ce connecte à sa machine.

b. HAProxy

C'est la partie que mes collègues ont finalisé avant mon arrivée. Weber Michael c'est occupé de cette fonctionnalité, pour ce faire il a utilisé des serveurs Proxy existants. Le HAProxy gère le LoadBalancing et la tolérance de panne, tous nos serveurs sont doublés.C'est un logiciel OpenSouce trouvable sur Google. Le HAProxy est séparé en 2 parties, le frontend et le backend. Les deux fonctionnent ensemble.

-le frontend est la partie qui relie l'utilisateur au proxy.

-le backend est la partie qui dialogue avec le serveur.

Le proxy inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes.

c. SQL

Le cluster SQL a dû être mis à jour pour pouvoir accepter les connexions sécurisées depuis l'extérieur, il contient les bases de données et stocke les informations des machines virtuelles. Ces informations sont reliées à un site d'administration du cluster.

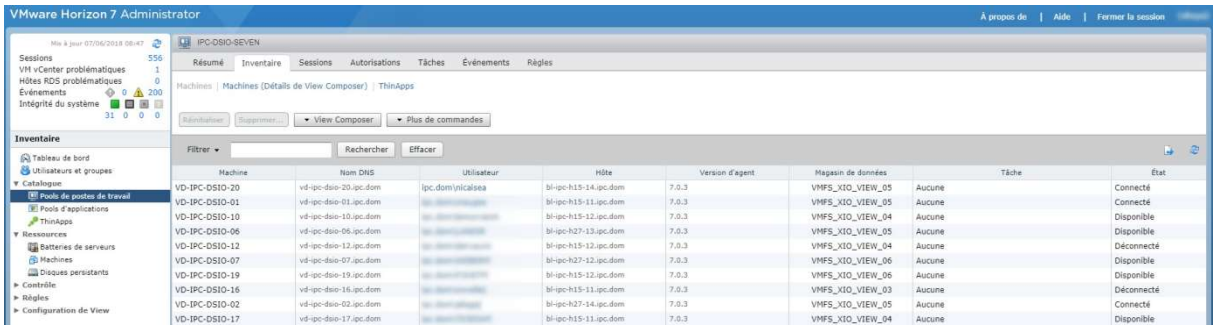


Figure 7 : vue d'ensemble du site

On peut y voir qui est connecté, le nom de la machine et le serveur de connexion.

Machine	Nom DNS	Utilisateur	État
VD-IPC-DSIO-20	vd-ipc-dsio-20.ipc.dom	ipc.dom\nicaisea	Connecté
VD-IPC-DSIO-01	vd-ipc-dsio-01.ipc.dom	[illegible]	Connecté
VD-IPC-DSIO-10	vd-ipc-dsio-10.ipc.dom	[illegible]	Disponible
VD-IPC-DSIO-06	vd-ipc-dsio-06.ipc.dom	[illegible]	Disponible
VD-IPC-DSIO-12	vd-ipc-dsio-12.ipc.dom	[illegible]	Déconnecté
VD-IPC-DSIO-07	vd-ipc-dsio-07.ipc.dom	[illegible]	Disponible
VD-IPC-DSIO-19	vd-ipc-dsio-19.ipc.dom	[illegible]	Disponible
VD-IPC-DSIO-16	vd-ipc-dsio-16.ipc.dom	[illegible]	Déconnecté
[illegible]	[illegible]	[illegible]	Connecté

Figure 8 : Utilisateur VDI (pool DSIO)

Et plus précisément pour chaque utilisateur :

Utilisateur	Type	Pool ou batterie de ser...	Nom DNS
ipc.dom\NICAISEA	Poste de travail	IPC-DSIO-SEVEN	vd-ipc-dsio-20.ipc.dom

Heure de début	Durée	État de session
06/06/2018 14:06:03	18 heures 56 minutes	Connecté

Figure 9 : détails utilisateur

On peut donc savoir le début de la connexion et la durée. Suivant la Pool de session qui est attribué à l'utilisateur, sa session peut rester allumée pendant plusieurs jours, tant que l'utilisateur ne la ferme pas.

3. Service d'authentification

L'authentification au sein d'une entreprise est basée sur énormément d'éléments. Ces éléments facilitent le travail des ressources humaines mais aussi des utilisateurs. Tel que le Single Sign-On ou la Gestion des Identités et des Accès (GIA ou IAM en anglais).

a. SSO

Le Single Sign-On ou SSO a pour objectif de simplifier, pour l'utilisateur, la gestion de ses mot de passe. Plus l'utilisateur doit gérer de mot de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité.

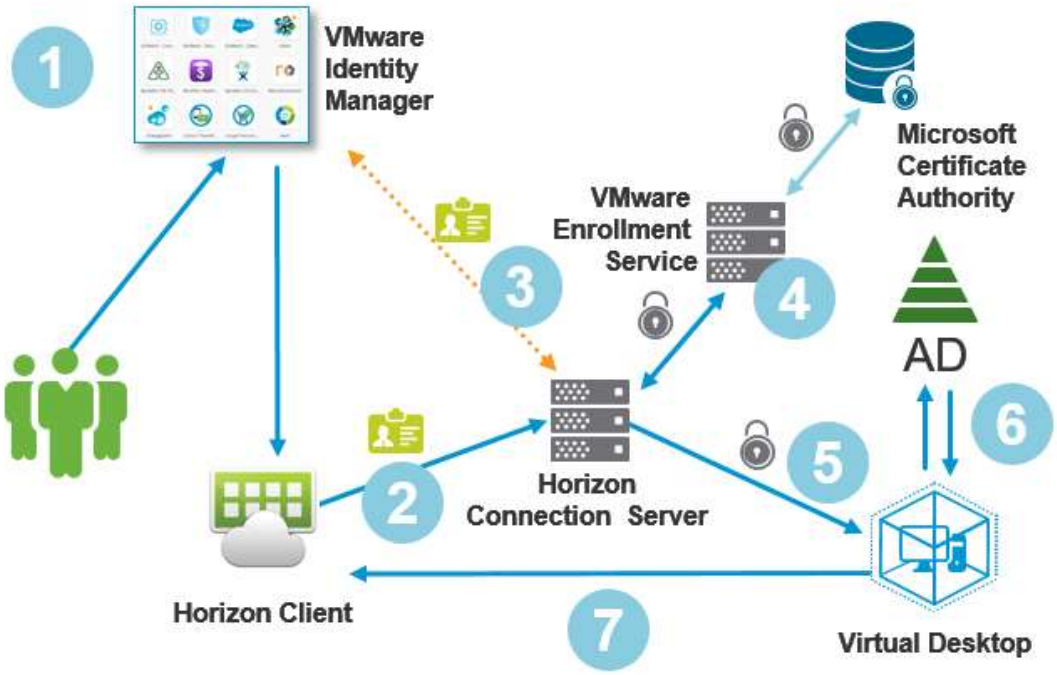
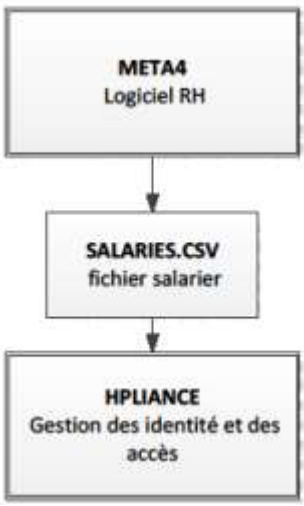


Figure 10 : Single Sign-On

Pour pallier à ces problèmes la DSIO a mis en place une approche centralisée c'est-à-dire : une base de données globale et centralisée de tous les utilisateurs. Cela permet également de centraliser la gestion de la politique de sécurité. Voilà pourquoi l'utilisateur n'a besoin de s'authentifier qu'une seule fois sur sa session.

b. IAM



La Gestion des Identités et des Accès consiste à déterminer qui a accès à quelle information sur une période donnée. Elle se base sur les informations des Ressources humaines qui son renseignées dans META4 et transmise par le fichier SALARIES.CSV. Donc cette gestion ne relève pas directement de la DSIO mais concerne la direction. Les processus de cette gestion permettent d'initialiser, d'identifier, d'enregistrer et de gérer les identités des utilisateurs et les droits d'accès aux informations de l'IPC qui leur sont associées. HPLIANCE alimente l'Active Directory qui est le dossier contenant tous les utilisateurs.

Figure 11 : IAM

Partie 2 : Authentification forte

1. Application

Avant la mise en place de l'authentification forte, les utilisateurs était autorisés à utiliser le logiciel VMware Horizon pour se connecter à distance. Seulement la connexion était sécurisée par un mot de passe seul. Nous allons donc maintenant passer par un portail internet qui lui est sécurisé par un code pin à 4 chiffres et un One Time Password.

a. Configuration du compte

Pour mettre en place le code Pin on utilise la console d'administration internet d'Imprivata. Cette page internet est relié à l'Active Directory ce qui permet de retrouver directement les comptes utilisateurs dans l'interface web. Tout d'abord on associe le compte utilisateur a un token VASCO. Les token VASCO nous sont fournis en nombre limité par VASCO, voilà pourquoi nous limitons l'enrôlement aux cadres et aux médecins.

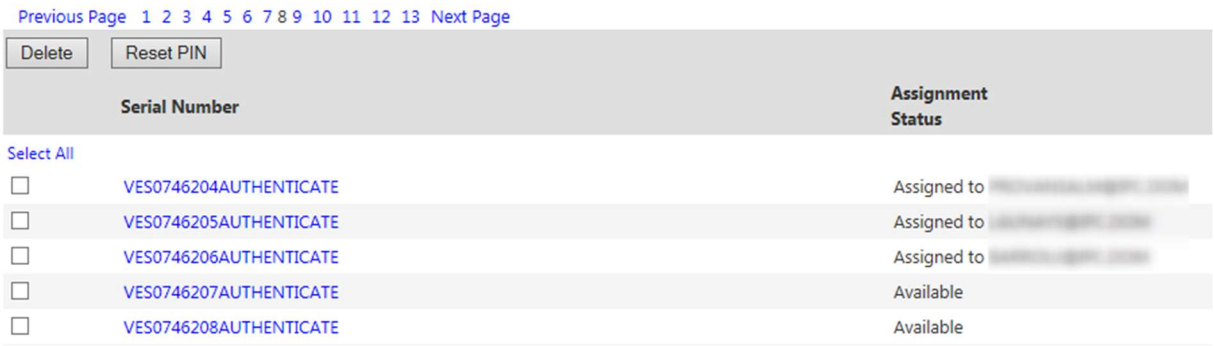
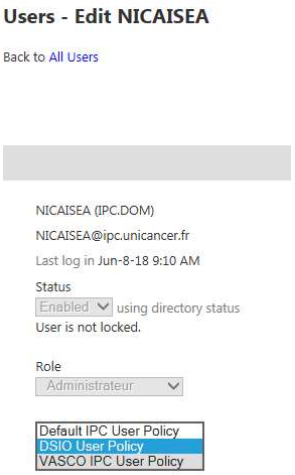


Figure 12 : Token VASCO



Quand un code est associé à une personne alors on peut définir le groupe de la personne comme étant utilisatrice de VASCO en changeant son groupe utilisateur.

Le groupe d'utilisateur VASCO IPC User Policy va permettre aux utilisateurs d'utiliser la technologie d'authentification forte. Ainsi leur compte IPC est relié à l'application qui génère les codes uniques.

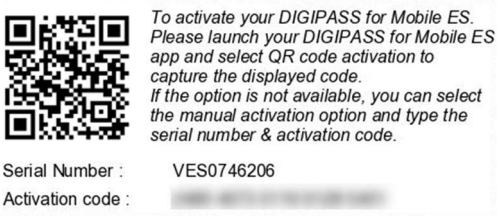
Figure 13 : Groupe utilisateur

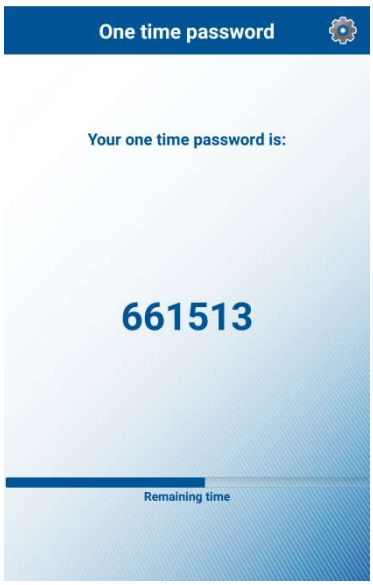
Pour finir on configure le code PIN de l'utilisateur sur la page des tokens VASCO. Cette étape conclu la configuration du compte utilisateur depuis le site Imprivata. Maintenant nous devons configurer les appareils qui génèrent le code à usage unique.

b. Application téléphone

Comme indiqué précédemment l'authentification lourde nécessite 2 facteurs, le code pin généré par l'utilisateur lors de son enrôlement et un code généré par une application partenaire a l'IPC.

Le QR code doit être scanné dans l'application.
Lors de la demande d'activation l'utilisateur choisi QR code puis scanne le QR code relié au token VASCO, relié par le Serial Number. Cela associe son compte IPC à son compte VASCO pour l'OTP.





Le QR code va synchroniser l'appareil de l'utilisateur avec le serveur VASCO, ils vont par la même occasion échanger une calculette et synchroniser leurs horloges pour générer le même code à l' instant t.

Après cette étape l'utilisateur est capable de générer un code à usage unique et valable 1 minute.
Au-delà de cette minute l'application générera un nouveau code etc.

Figure 14 : OTP

2. Formation

Pour mettre en place le projet le Directeur de l'institut devait valider l'utilisation et le fonctionnement. Pour ce faire il fallait tester l'authentification forte avec des utilisateurs « test ». Toute la DSIO était présente dans la Pool de test, plus le directeur de l'établissement et deux autres personnes. Quelques bugs mineurs sont apparus pendant la phase de test mais le directeur a rapidement accepté la technologie. Il a autorisé la mise en place du produit pour tous les utilisateurs.

Name	Applied Users
Default IPC User Policy*	1580
DSIO User Policy	19
VASCO IPC User Policy	132

Ainsi avec l'aide de Mr LANDI Renaud, j'ai enrôlé plus de 130 personnes. Pour ce faire les médecins ou les cadres devaient faire une demande au support, ou s'adresser directement à l'un de nous deux, pour convenir d'une date de rendez-vous. Le jour du rendez-vous l'utilisateur apporte son appareil mobile pour la partie application et son ordinateur portable s'il en possède un. On configure le compte utilisateur comme vu précédemment, en liant son compte IPC a un token et son téléphone au QR code.

Quand toute la configuration est terminée je vérifie que l'utilisateur possède la dernière version du logiciel VMware Horizon, si l'utilisateur ne l'a pas installé je lui installe. Puis je rajoute un favoris sur le PC de l'utilisateur avec le lien menant vers le portail IPC (https://portail.ipc.unicancer.fr).

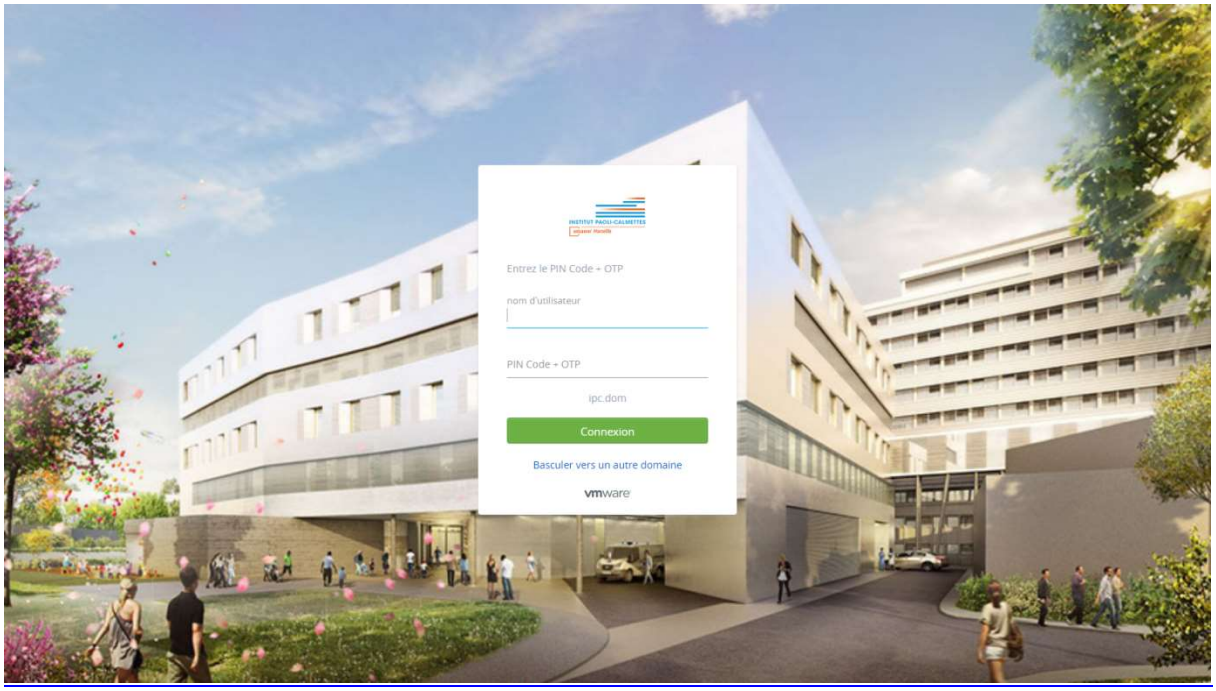


Figure 15 : Portail IPC

L'utilisateur s'authentifie au portail de la façon suivante : il renseigne son nom d'utilisateur donc le nom et l'initiale exemple : nicaisea. Puis pour le mot de passe l'utilisateur renseigne le code PIN renseigné plus tôt et il concatène le code généré par le téléphone voir Figure 14.

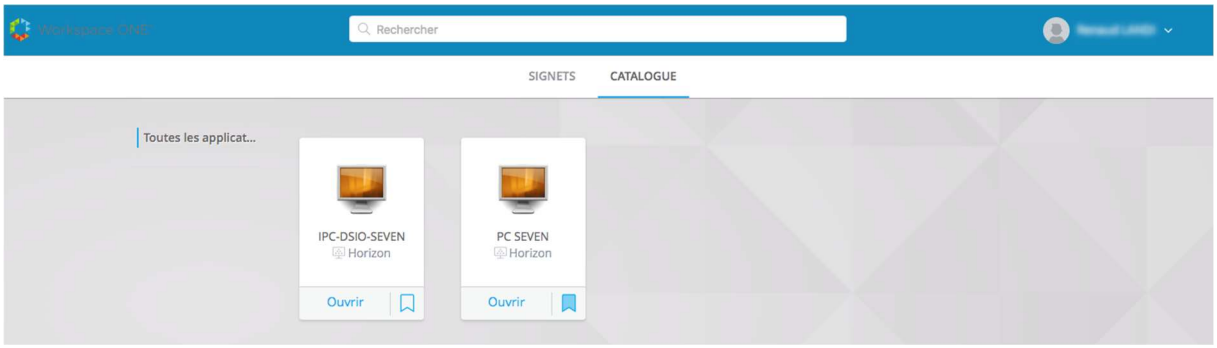
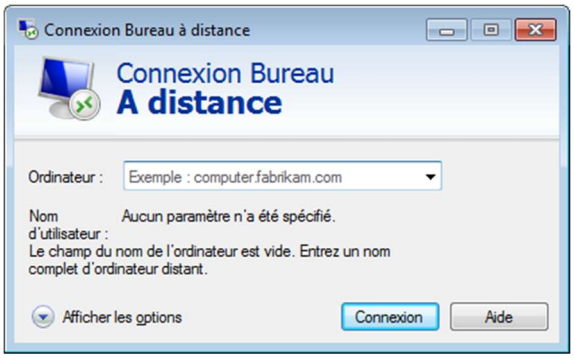


Figure 16 : Catalogue VM Portail

Après la connexion l'utilisateur arrive sur le portail web avec deux onglets différents. Les Signet qui sont les raccourcis pour ouvrir une machine, et le Catalogue qui contient les machines de l'utilisateur. Dans l'exemple l'utilisateur a accès à une machine de la DSIO et a un PC utilisateur standard.

Quand l'utilisateur va cliquer sur la machine voulue le portail web va demander l'autorisation pour exécuter le logiciel VMware Horizon, préalablement installé, et lancer la machine avec l'application.



Certains utilisateurs possèdent, dans leur bureau, des PC lourd et non des clients légers reliés au serveur. On propose pour ces utilisateurs de mettre en place une connexion bureau à distance entre leur session virtuelle et leur PC de bureau. On récupère le nom du PC Lourd exemple m130256. Puis depuis la session virtuelle on connecte le PC Lourd.

3. Travaux annexes

En plus du projet qui m'a était confié, lors de mon stage j'ai pu effectuer des taches annexes. Que ce soit de la téléphonie ou des réseaux j'ai pu toucher à différents domaines.

a. Sophos

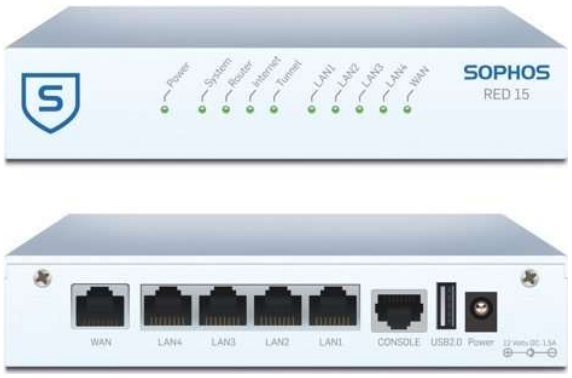
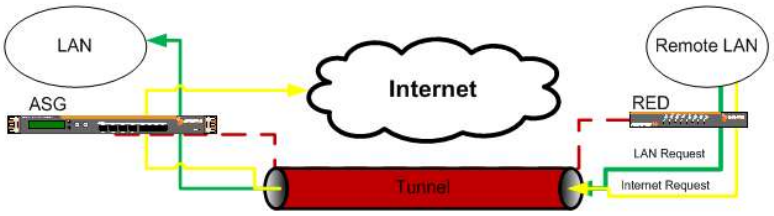


Figure 17 : Sophos Red

Le premier sujet pour lequel j'ai aidé a pour but de donner l'accès à des secrétaires au réseau de l'IPC depuis l'extérieur à partir d'un VPN.

Avec Mr LANDI nous avons configuré 27 Sophos Red. Pour les configurer Mr Mauge nous a donné une plage d'adresse pour les connecter.

Ce projet nous a pris une journée à deux.



Tout le trafic provenant du Remote LAN[1] passera au travers du VPN, le tunnel rouge, s'il se dirige vers le LAN ou Internet. Le trafic entre le LAN et le Remote LAN peut être bloqué ou autorisé par des règles de firewall. L'ASG est le serveur en interne qui connecte les boitiers Red.

b. Réseaux

Durant le stage 2 switch sont tombés en panne, plus exactement le POE[2] des ports. Il a donc fallu reconfigurer deux nouveaux switch pour les remplacer. On a donc injecté la configuration à l'aide d'une clé USB.

Figure 18 : Cisco catalyst 2960-X

J'ai aussi aidé pendant un changement de switch, c'est-à-dire le remplacement d'un ancien switch par un nouveau. Nous avons configuré un switch à l'avance, avec les ports configurés de la même façon que l'ancien switch. Au moment de l'installation nous avons prévenu les utilisateurs en question que la connexion risquait d'être coupée pendant quelques secondes le temps de débrancher rebrancher le switch. Pendant cette opération nous avons remarqué les erreurs de câblage d'anciens prestataires :

Le câblage suivant est certe propre mais pas pratique, si un câble s'arrête de fonctionner alors tout le lot de câble doit être retiré pour le changer. Et cela soulève un autre problème, l'impossibilité de suivre le câble pour savoir où il est branché.

Le réseau de l'IPC est constitué de 36 locaux techniques, contenant des baies réseaux ou des serveurs. Numéroté de h1 à h36 et contenant chacune, des armoires numéroté : hx.y
x étant le numéro du local et y le numéro de l'armoire.

1 : Connexion à distance au réseau Local.
2 : Power Over Internet

Mr LANDI étant en alternance il m'arrivé de devoir gérer les problèmes de téléphonie tel qu'un changement de téléphone, ou une assistance depuis le site d'administration AVAYA.

Voici les deux modèles de téléphones utilisé dans l'IPC :

Figure 20 : AVAYA E129

Figure 21 : AVAYA 9608G

Au début de mon stage, une mise à jour des téléphones en a éteint la moitié. Il a donc fallu que j'aille en rallumer un bon nombre en me baladant dans les locaux. Cela m'a permis de découvrir les différents bâtiments, qui sont au nombre de 4 : IPC1 qui est le bâtiment principal, IPC2 le bâtiment des consultations, IPC3 consacré à l'hôpital de jour chirurgical et au nouveau plateau technique (blocs, réanimation) et enfin IPC4 qui contiendra des bureaux anciennement présent dans IPC1.

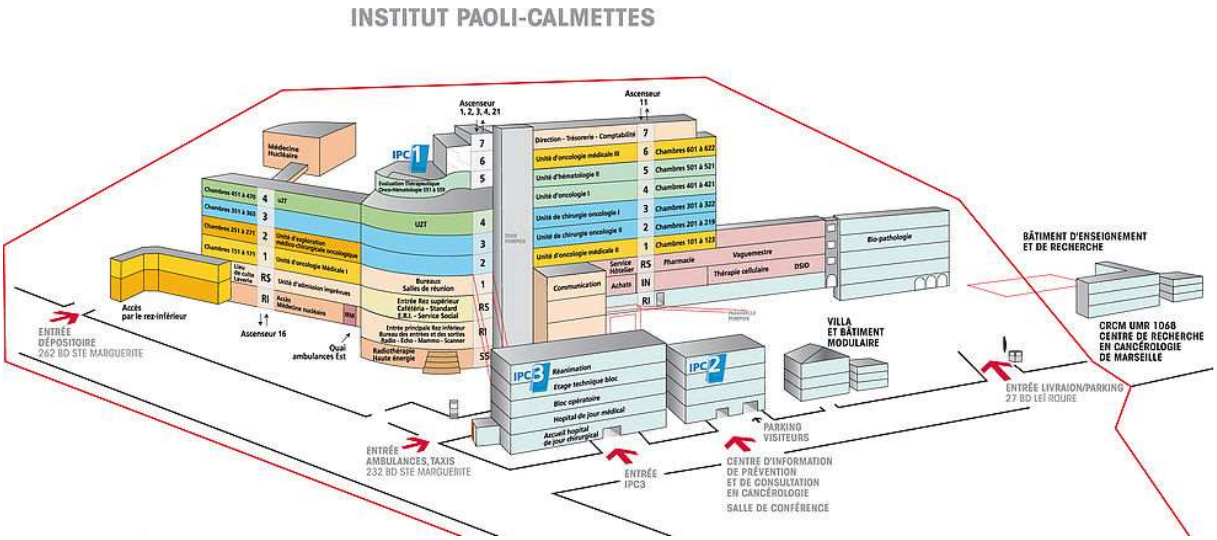


Figure 22 : Plan IPC

IV. Bilan et Conclusion

Pendant le déroulement de mon stage, j'ai eu l'opportunité de travailler sur différents aspects, et d'avoir différentes approches des métiers des réseaux et télécommunications.

En effet, j'ai pu découvrir ce qu'était et grâce à quels outils fonctionnait l'authentification forte, une solution qui va devenir de plus en plus courante et demandée dans les entreprises au vu de la demande en sécurité qui ne fait qu'augmenter. J'ai ainsi eu l'occasion de rencontrer énormément de personne, ce qui m'a permis de développer mon sens du relationnel. Pendant ce travail d'enrôlement d'utilisateur j'ai eu l'occasion de faire de la pratique en mettant en place des switch et des serveurs. J'ai donc pu mettre en pratique mes compétences techniques et mes connaissances théoriques acquises dans le cadre de ma formation à l'IUT afin de déployer cette solution. Cela m'a permis de mieux comprendre et de pouvoir approfondir certaines des compétences qui m'ont été enseignées durant mes deux années d'IUT.

En plus de cela, ce stage m'a fait découvrir le fonctionnement d'une entreprise, et par là, il m'a permis de me donner une idée plus précise de ce qu'est le monde du travail et le travail en équipe au sein d'une structure de plusieurs collaborateurs. Il m'a donc apporté une bonne expérience professionnelle et humaine, ce qui sera un atout dans le cadre de ma poursuite d'étude mais également lorsque je me lancerai dans la vie active. De plus, ce stage s'inscrit parfaitement dans la fin de ces deux années d'IUT puisqu'il arrive à un moment où nous avons acquis assez de connaissances pour pouvoir travailler sur des sujets intéressants et enrichissants, ce qui ne fait qu'accroitre mon envie de poursuivre mes études.

V. Sitographie

Documentation et description des produits :

https://www.vmware.com/fr.html
https://www.imprivata.fr/fr
https://www.sophos.com/fr-fr.aspx