



3TI - 2017-2018

Réseau d'entreprise

OKLN

Groupe B

5 Février 2018

1 Introduction

La définition des rôles et des stratégies organisationnelles a été le point le plus important de cette journée.

La première étape a été l'élection du chef de projet et de son assistant. Pour effectuer cette tâche, nous avons procédé par vote.

Par la suite, chaque membre du groupe a été assigné à une tâche, en fonction des affinités de chacun.

Une fois les grandes lignes directrices tracées, chaque groupe a pu se concentrer plus en profondeur sur les problèmes qui les concernaient. C'est sur ces points que notre discussion se focalisera.

2 Infrastructure réseau

2.1 Tâches réalisées

La première étape a été la réalisation des schémas logiques et physiques. Nous avons ensuite procédé à la réalisation du plan d'adressage IP et à la mise en place des VLANs.

L'étude de l'infrastructure est un élément essentiel pour la réalisation d'un réseau respectant les normes de sécurité.

2.2 Difficultés rencontrées

La difficulté principale rencontrée lors de l'étude de l'infrastructure aura été la séparation entre la zone utilisateur et la zone démilitarisée (DMZ). La mise en place d'une infrastructure sécurisée demande de prendre en considération de nombreux éléments techniques et de distinguer les composants fondamentaux du réseaux afin de définir, par la suite, les politiques d'accès.

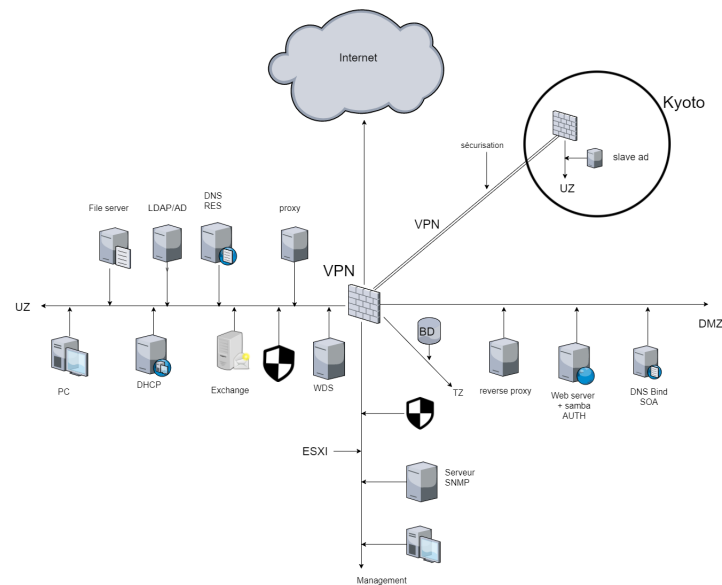
2.3 Remarques importantes

Nous avons décidé d'imposer une séparation entre le wi-fi interne de l'entreprise et le wi-fi public, pour des raisons de sécurité et de simplicité pour l'administration.

Afin de palier au problème de crash, l'infrastructure adopte une topologie en étoile, réalisée par le biais de 2 Switch layer 3.

La DMZ est située dans son propre VLAN pour des raisons de sécurité.

2.4 Topologie



3 Mail

Les mails sont un outil très important dans une entreprise car ils permettent la communication entre les employés mais aussi entre les employés et les clients de l'entreprise.

Ils ont aussi un rôle d'archivage et d'authentification de la communication.

3.1 Technologies utilisées

Nous avons décidé d'utiliser le service de Microsoft : Microsoft Exchange. Celui-ci est disponible sur Windows Server 2016.

Plusieurs raisons ont motivé notre choix :

- C'est un service de messagerie complet qui englobe un serveur mail, un client de messagerie et des applications destinées au travail collaboratif.
- Exchange est fiable, très sécurisé et qui intègre une protection contre un grand nombre de menaces pouvant affecter les mails. (Filtres anti spam, anti phishing, anti malware,).
- Nous disposons déjà d'une infrastructure Windows Server qui se compose d'un active directory pour la gestion des ressources et des utilisateurs.
- Il comporte aussi un module de calendrier qui peut être facilement combiné avec Outlook (Client mail, Calendrier, Contacts, outils de collaboration).

4 Sécurité

4.1 Tâches réalisées

Notre choix s'est tourné vers trois technologies :

pfSense qui sera la véritable plaque tournante pour la sécurité de notre infra

OpenVPN client-to-site pour la liaison VPN client-to-site

VPN IPsec site-to-site pour la liaison VPN site-to-site

4.2 Motivation technologies/infrastructures

pfSense OpenSource, portable, puissant, dispose de nombreuses fonctionnalités

OpenVPN Portabilité cross-platform, une bonne stabilité. Il permet l'évolution (notamment au niveau de l'adaptation à la charge) tout en ayant une installation relativement simple. OpenVPN offre un support pour gérer les IP dynamiquement et le NAT. Il possède une interface de management pour pouvoir le contrôler à distance ou localement de façon sécurisé (support du X509 PKI, SSL, TLS, ...)...

IPSEC techno très répandue, safe, et qu'on a appris en cours avec Schalkwijk

5 Logistique

5.1 Tâches réalisées

La liste du matériel nous a été communiquée dans le dossier du projet d'entreprise. Nous avons vérifié que le matériel qui nous a été donné correspond bien à la liste que nous avons reçue. Nous avons également vérifié qu'il était bien fonctionnel.

Nous avons organisé le local de façon optimale pour que les équipes puissent travailler ensemble et qu'elles aient ce dont elles ont besoins (multi-prises, accès au serveur, accès au switch,...).

Nous avons branché le serveur sur secteur dans le local pour éviter de devoir le brancher/débrancher à chaque fermeture du local. Afin d'éviter des problèmes de surchauffe, l'alimentation des ordinateurs de l'équipe est effectuée depuis le couloir. Nous évitons ainsi de dépasser les 3000W par prise.

5.2 Difficultés rencontrées

Un des commutateurs était probablement défectueux. Il nous était impossible de le flasher. Nous avons donc décidé de le faire remplacer.

5.3 Remarques importantes

En plus du matériel fourni, nous avons utilisé un commutateur c35/50 layer 3. Cette décision a été prise par l'équipe de l'infrastructure réseau.

6 Services internet

6.1 Tâches réalisées

Nous avons commencé par réfléchir à la meilleur approche pour la mise en place du service web, avec une considération accrue des bonnes pratiques de sécurité.

6.2 Difficultés rencontrées

L'infrastructure n'étant pas encore complètement déployée, il n'était pas possible de mettre en place les services web.

6.3 Technologies utilisées

Pour le serveur web, notre choix s'est porté sur Nginx. Celui-ci est réputé pour sa légèreté et sa fiabilité. Nous utilisons de plus PhpStorm comme IDE.

7 Déploiement

7.1 Tâches réalisées

Petit serveur Configuration d'un Raid 1 pour le stockage de toutes les infos et installation de Esxi 6.5 sur clé USB.

Serveur principal Configuration d'un raid 1 avec 2 ssd (os) et configuration d'un raid 10 avec les 4 hdd pour les data (.iso, file serveur). Nous avons également installé esxi 6.5 sur clé USB.

Autre Installation d'un client linux afin d'uploader les fichiers iso (windows,pfsense,debian).

7.2 Difficultés rencontrées

Sur le petit serveur nous avons confondu la carte raid et la carte bios.

7.3 Motivation techonologies/infrastructures

On a choisi un hyperviseur afin d'installer plusieurs OS sur la même machine et les isoler entre eux. Nous avons fait le choix de ESXI pour notre bonne connaissance de celui-ci.

7.4 Remarques importantes

Nous avons besoins d'une configuration ip afin d'installer ESXI et les différents services.

8 Rapports & organisation

8.1 Tâches réalisées

Réflexion autour des problèmes de centralisation des informations et des documentations. Mise en place de l'infrastructure de soutien de la communication entre les sous-groupes et de facilitation de l'élaboration des rapports au jour le jour.

8.2 Motivation des technologies/infrastructures

Discord : Pour communiquer plus rapidement entre nous, nous utilisons un serveur Discord dédié à ce projet. Nous avons créé une partie commune visible par tout le monde et une partie visible uniquement des membres d'un sous-groupe de travail. La partie commune nous permet de partager toutes les informations importantes, liens et fichiers. Cette partie nous permet également de nous organiser pour les repas de midi. La partie spécifique pour les différentes parties du projet, est, comme dit plus haut, visible seulement des membres dudit groupe de travail. Quant aux responsables de chaque groupe, ils ont la possibilité de voir les discussions des autres "channels" pour, si besoin, établir plus facilement une communication.

Github : Pour gérer la centralisation des documents et des codes sources nous avons décidé de créer une organisation github (EPHEC-OKLN). Une organisation permet de créer plusieurs repository indépendants structurellement ("pushable et pullable" de façon individuelle) et permettant aux gens de travailler sur leur propre partie du projet sans risquer de gêner le travail des autres mais qui permet une solution centralisée car tournant autour du même projet. Chaque groupe se retrouve avec un repository à son nom qu'il gère comme il veut. Un dossier commun à tous "Rapport-Doc", contenant un fichier par jour du projet dont la structure est faite pour faciliter la prise de notes et la documentation des groupes au jour le jour.

Trello : Pour rythmer le travail de chacun et visualiser les avancées réalisées nous avons choisi Trello, dynamique et connu de tout le groupe. A l'intérieur d'un Trello centralisé chaque "sous-groupe", a lui aussi un tableau trello qu'il gère comme il le souhaite, servant à rythmer le travail de chacun et à voir si tout avance bien.

ShareLatex : Pour la mise en commun des rapports des différents sous-groupe nous utilisons ShareLatex qui nous permet non seulement de travailler en temps réel sur un même document mais de pouvoir se préoccuper de façon très superficielle de la mise en page (gérée grâce au format LaTeX). Enfin ShareLatex nous offre un export PDF facile et un backup online de nos rapports.

8.3 Difficultés rencontrées

Afin de pouvoir inviter/ faire rejoindre toute l'équipe aux différentes infrastructures mises en place, il a fallu récolter les noms/identifiants/mails respectifs sur chaque plate-forme (discord, trello et github. Il a été un peu fastidieux et lent de faire bouger tout le monde pour qu'ils prennent 3 minutes pour remplir un fichier de 3 champs. Ils ne venaient vers nous que quand ils se rendaient compte qu'ils en avaient en fait besoin. Nous avons du nous plonger plus profondément dans le langage LaTeX dont nous n'avions que des connaissances partielles.

8.4 Remarques importantes

9 sources

9.1 sécurité

- Infrastructure réseau base de Laurent Schalkwijk (cours de 2TI)
- <https://forum.pfsense.org/index.php?topic=76015.0>
- https://doc.pfsense.org/index.php/OpenVPN_Remote_Access_Server
- <https://openvpn.net/index.php/open-source/documentation/howto.html>
- <https://forum.pfsense.org/index.php?topic=76015.0>
- <https://openvpn.net/index.php/open-source/335-why-openvpn.html>

9.2 déploiement

- <https://techmikeny.com/h700-array-guide>

9.3 rapports

- <https://openclassrooms.com/courses/redigez-des-documents-de-qualite-avec-latex>
- https://fr.sharelatex.com/learn/Inserting_Images

9.4 Services internet

- <https://korben.info/configurer-nginx-reverse-proxy.html>
- <https://docs.microsoft.com/fr-fr/windows-server/identity/ad-fs/deployment/install-the-federation-service-proxy-role-service>