

11 mai 2020



Haute Ecole Economique et Technique

Projet Administration système et réseau

Rapport Technique

Groupe 2TL1-8

Quirynen Gilles, Lambert Maximilien, Gassmann Mathias
Étudiant responsable de la mission 3 : Mathias Gassmann

Méthodologie

Nous suivons les étapes de déploiements habituelles dans un projet pareil à savoir :

1. Documentation
2. Installation
3. Configuration
4. Déploiement
5. Maintenance

Etat d'avancement

1. Web

État d'avancement :

Tout d'abord nous utilisons des Dockerfile qui contiennent les différents sites web que nous avons créés. Une fois ces dockerfiles publiés sur le compte dockerhub de notre groupe, nous y avons accès depuis nos vps.

Nous utilisons ensuite putty pour créer une docker compose de manière à pouvoir lancer les différents conteneurs en une fois. Nous pouvons ainsi également voir l'état de tous les conteneurs lancés avec ce docker-compose et les monitorer adéquatement.




Nous utilisons un reverse-proxy et des server blocks(équivalent nginx des virtual host apache) pour faire la redirection vers la bonne adresse. *Le site b2b est donc capable de récupérer des données depuis la base de données qui se situe sur le même VPS et qui est lancée dans le même docker-compose.*

Les sites accessibles (vitrine et b2b) au public sont configurés en https grâce à un certificat SSL.

Nous avons gardés un reverse proxy dans la DMZ qui s'occupe de la redirection vers les sites web qui ont été déplacés sur autre VPS pour des raisons de sécurité.

Server Hostname

These results were cached from May 30, 2020, 12:30 am PST to conserve server resources.
If you are diagnosing a certificate installation problem, you can get uncached results by [clicking here](#).

-  **b2b.wt1-8.ephec-ti.be** resolves to 51.178.40.70
-  **Server Type:** nginx/1.14.0 (Ubuntu)
-  **The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).**

Fonctionnalités implémentées :

- les fichiers react des sites sont contenus dans des dockerfiles
- les sites webs peuvent être lancés à l'aide d'un docker compose
- l'adresse wt1-8.ephec-ti.be affiche le site mail vitrine
- l'adresse b2b.wt1-8.ephec-ti.be affiche le site web b2b
- *les sites sont configurés en https*
- *les sites sont sortis de la DMZ*
- *Le reverse-proxy est le seul service restant sur la DMZ (partie web) et s'occupe de la redirection des adresses*

2. DNS

État d'avancement :

Concernant le dns externe, le sous-domaine "*wt1-8.ephec-ti.be*" du domaine "*ephec-ti.be*" a bien été mis en place et les requêtes aboutissent bel et bien sur notre infrastructure. Les fichiers de zone ont bien été configurés afin de pouvoir accéder aux sites web publics et aux services mails et VOIP.

Concernant le dns interne, nous avons configuré un serveur soa interne qui permet aux utilisateurs de l'entreprise au sein du réseau interne d'accéder aux services internes de l'entreprise, à savoir l'outil ERP Web. Par ailleurs, nous avons également configuré un résolveur DNS permettant de rediriger les postes utilisateurs vers le soa interne en premier lieu, puis vers le dns de google si c'est une requête à un service externe.

Fonctionnalités implémentés :

- Sous-domaine "*wt1-8.ephec-ti.be*" fonctionnel
- MX record permettant l'accessibilité au service mail
- A records permettant l'accessibilité aux sites web externe (vitrine + b2b)

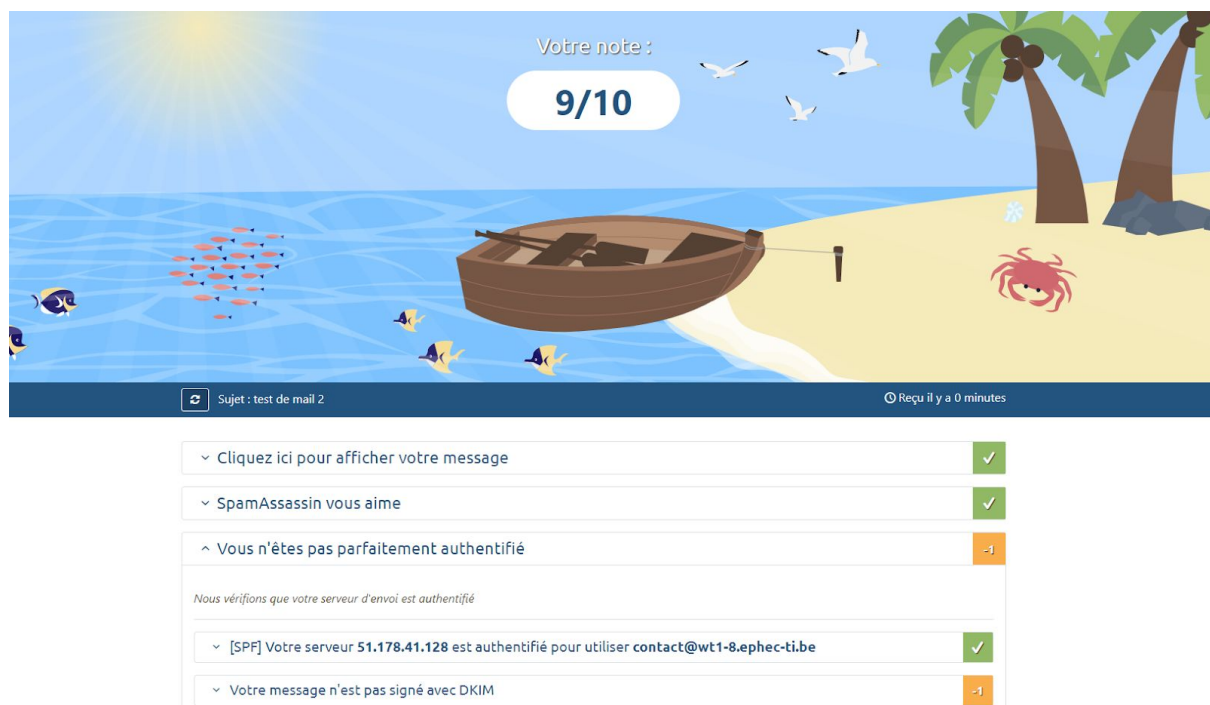
- Accessibilité aux services internes (outil ERP Web) par les utilisateurs de l'entreprise
- Accessibilité aux services externes par les utilisateurs de l'entreprise

3. Mail

État d'avancement :

Concernant le mail, notre domaine wt1-8.ephec-ti.be existe et est fonctionnel. Nous avons pour ce faire installé Postfix, Dovecot mais également apache2, php7. Nous avons testé la connexion et les envois/receptions de mail via Squirrelmail. Tous les tests se sont avérés concluants.

Un autre test via mail-tester.com a été réalisé, nous avons obtenu la note de 9. Le point manquant concerne DKIM mais après plusieurs tests sur d'autres sites (mxtoolbox,...) notre clé DKIM est bonne et fonctionnelle.



Fonctionnalités implémentées :

- Les adresses mail pour les employés ainsi que contact@wt1-8.ephec-ti.be sont créées
- Il est possible d'envoyer des mails depuis n'importe quel adresse vers une des adresse de l'entreprise
- Il est possible d'envoyer des mails depuis une adresse de l'entreprise vers n'importe quel adresse (également vers une autre adresse de l'entreprise)
- Une procédure d'ajout/retrait d'utilisateurs est prévue et documentée
- Il existe un RR PTR pour le serveur SMTP de l'entreprise
- Sécurité: les mécanismes DKIM sont déployés
- Sécurité: les mécanismes SPF sont déployés
- Sécurité: les mécanismes SMTP n'accepte de relayer que les mails de l'entreprise

4. VOIP

État d'avancement :

Dans un premier temps, nous avons réussi à mettre en place une image docker VOIP fonctionnelle et à la faire tourner dans un conteneur docker. Nous avons ensuite développé un plan de numérotation et nous nous sommes ensuite occupés de modifier les fichiers de configurations afin de répondre aux demandes du client. Nous avons surtout passé du temps dans les fichiers de configuration "extensions.conf" (permettant d'ajouter les règles de communication), "users.conf" (permettant de gérer les postes de téléphonie des utilisateurs de l'entreprise) et le fichier "voicemail.conf" (permettant de gérer les boîte vocales des différents postes de l'entreprise).

Dans un second temps, nous avons pris contact avec un autre groupe (Numéro de groupe : 2TL2-3) afin de fusionner nos réseaux téléphoniques. Nous avons mis en commun nos plans d'adressages en minimisant les changements nécessaires :

Contexte entreprise 2TL2-3	Identifiant VOIP 2TL2-3	Utilisateurs 2TL2-3
Ouvriers	3001	Atelier et voicemail atelier
	3002	Hangar et voicemail hangar
Commerciaux	5001	Commercial et voicemail commercial
Comptables	4000	Bureau comptables
	4001	Comptable 1
	4002	Comptable 2
Secrétaire	6001	Secrétaire et voicemail secrétaire
Directeur	7001	Directeur et voicemail directeur

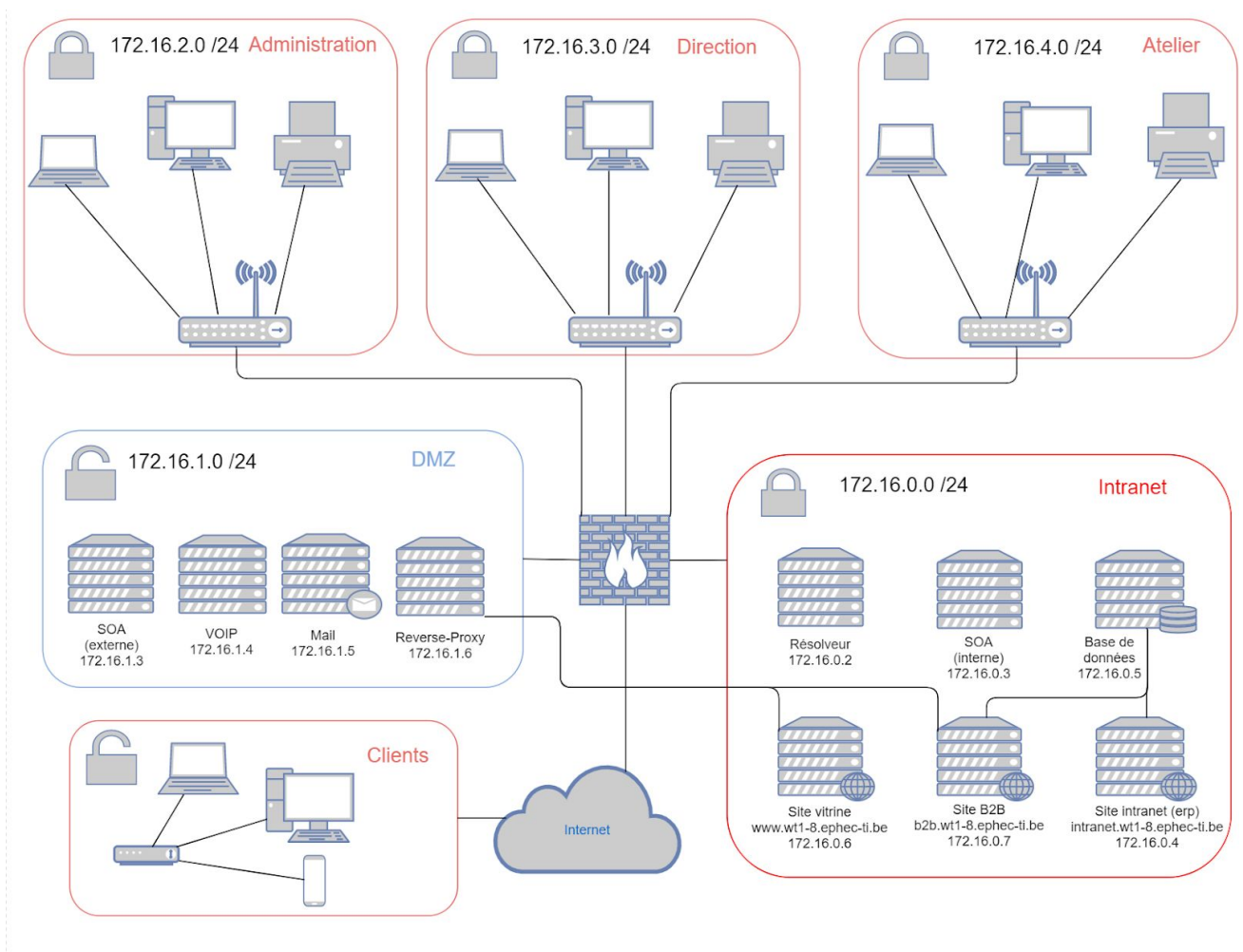
Contexte entreprise 2TL1-8	Identifiant VOIP 2TL1-8	Utilisateurs 2TL1-8
Ouvriers	100	Atelier et voicemail atelier
	101	Hangar et voicemail hangar
Commerciaux	301	Commercial et voicemail commercial
Comptables	200	Bureau comptables
	201	Comptable 1
	202	Comptable 2
Direction	400	Directeur et voicemail directeur
	401	Secrétaire et voicemail secrétaire

Fonctionnalités implémentés :

- Un plan de numérotation est fourni et reprend toutes les demandes du client
- Chaque poste de l'entreprise possède un identifiant SIP fonctionnel
- Un appel vers le numéro du directeur aboutit sur le poste de la secrétaire qui peut le rediriger vers le poste du directeur
- Chaque département peut joindre les autres
- Un numéro unique permet d'appeler le service comptable (le numéro 200). L'appel sera pris par le premier comptable disponible.

- Les employés disposent d'une boîte vocale.

Schéma réseau WoodyToys

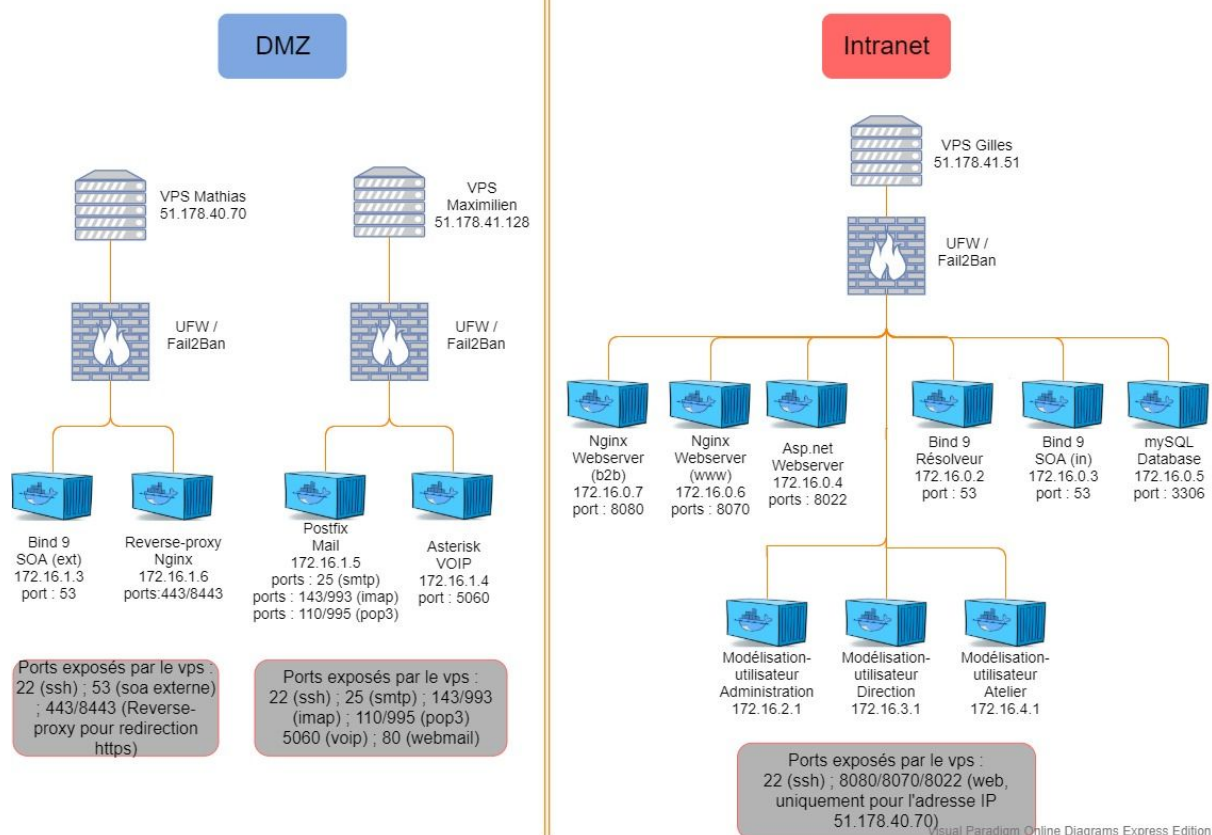


Nous avons divisé l'infrastructure réseau en 3 parties : le réseau externe (DMZ), le réseau interne et le réseau utilisateur (Administration, Direction et Atelier).

- Le réseau externe (DMZ) contient tous les services devant être accessible depuis l'extérieur, à savoir : le serveur DNS externe, mail, voip ainsi qu'un serveur reverse-proxy permettant de faire la redirection des accès aux serveurs web vitrine et b2b.
- Le réseau interne contient tous les services ne devant pas être accessible depuis l'extérieur, à savoir : le serveur DNS interne, le résolveur permettant de rediriger les utilisateurs vers le DNS interne, les 3 sites web de l'entreprise (vitrine, b2b et erp) ainsi que la base de données qui doit uniquement recevoir des requêtes provenant des sites web b2b et erp (intranet). Seuls les sites vitrine et b2b auront un lien avec l'extérieur mais celui-ci sera protégé par une règle de firewall ne permettant l'accès à ces sites que depuis l'adresse IP du VPS sur lequel est hébergé sur le serveur reverse-proxy à savoir 51.178.40.70 et seulement sur le port 80/443 (web).
- Le réseau utilisateur contient les différents périphériques utilisés par les utilisateurs de l'entreprise et ceux-ci seront connecté au réseau interne de l'entreprise afin de ne pas être accessible depuis l'extérieur. Chaque département (administration, direction et atelier) sont séparés dans des sous-réseaux différents permettant de bien les différencier.

Schéma du prototype

Visual Paradigm Online Diagrams Express Edition



Nous avons divisé ce schéma en 2 parties : la partie DMZ (services externes) et la partie Intranet (services internes).

- Concernant la partie DMZ, nous avons le VPS de Mathias qui s'occupe de gérer le serveur DNS externe ainsi que le reverse-proxy qui fera la redirection des accès aux sites web externe de l'entreprise (qui eux, se trouve sur le VPS de Gilles dans la partie Intranet). Nous avons également le VPS de Maximilien qui lui s'occupera des services mails et voip.
- Concernant la partie Intranet, le VPS de Gilles y est exclusivement consacré. Il contient les différents serveurs web (internes et externes), le résolveur et le dns interne, la base de données ainsi que les différents conteneurs modélisant chacun un utilisateur d'un département (vlan) de l'entreprise. L'objectif étant d'exposer le moins possible ce VPS au monde extérieur, nous n'avons comme ports ouverts que le port 22 (permettant une connexion ssh à celui-ci) et les ports 80/443 accessibles uniquement par l'adresse IP du VPS de Mathias sur lequel se trouve le serveur reverse-proxy permettant d'accéder aux sites web externes.

Grâce à cette architecture, nous avons pu mettre en place une seule et unique base de données accessible par le site web externe b2b et le site web interne (erp) via le réseau interne sans aucun risque d'accès depuis l'extérieur.

Plan d'adressage IP

Nous avons découpé le plan d'adressage en 5 pools d'adresses liés aux différents VLAN utilisés dans notre infrastructure réseau. Chaque pool d'adresse contient 254 adresses IP utilisables.

- le VLAN Intranet : 172.16.0.0 /24
- le VLAN DMZ : 172.16.1.0 /24
- le VLAN Administration : 172.16.2.0 /24
- le VLAN Direction : 172.16.3.0 /24
- le VLAN Atelier : 172.16.4.0 /24

Difficultés rencontrées

1. Web

Nous avons d'abord rencontré des difficultés avec l'utilisation du docker-compose, mais nous avons réussi à les résoudre grâce à la documentation présente sur le site de Docker. La grosse difficulté suivante fut la redirection entre le site vitrine et b2b que nous avons finalement résolu grâce à l'utilisation d'un reverse proxy et de server blocks.

2. DNS

Nous n'avons pas rencontré de difficultés concernant la mise en place du serveur DNS externe. Par contre, l'architecture à mettre en place pour le réseau interne a été plus difficile à comprendre aux premiers abords. En effet, nous n'avions pas de résolveur et attribuions l'adresse IP de notre soa interne comme résolveur dns de nos utilisateurs. Or cela nous a posé quelques problèmes, nous avons donc changé notre architecture en configurant notre propre résolveur DNS qui redirige les requêtes vers le soa interne.

3. Mail

De nombreuses difficultés ont été rencontrées lors de la création de l'image docker. Il est très simple de faire tourner un serveur mail directement sur le VPS mais dès lors que l'on souhaite le transcrire dans un Dockerfile de nombreux problèmes inconnus apparaissent même pour les commandes les plus basiques.

Exemple:

```
usermod -m -d /var/www/html/myusername myusername
```

après cette commande un message d'information nous indique que le fichier existe déjà mais la commande a bien été exécutée. Or dans le Dockerfile cette commande est interprétée comme une erreur et n'est pas acceptée.

Procédure de validation du déploiement de la solution

Chaque service a été testé individuellement par le responsable du service via commandes et/ou sites web spécialisés (exemple: dig pour le dns, mail-tester.com pour le mail, ...).

Chaque service a été transcrit dans un Dockerfile afin de pouvoir le déployer rapidement et facilement. Il y a donc plusieurs vérifications à faire sur le container pour s'assurer de sa validation :

- Le container est-il actif et running ?
- Les services sont-ils accessibles ? (vérification des ports ouverts)
- Les services sont-ils opérationnels ?

Monitoring

Nous utilisons docker-compose pour lancer nos conteneurs en même temps, cela nous permet d'utiliser la commande : *docker-compose ps*.

Cette commande affiche les services qui tournent et ceux qui sont arrêtés sur le VPS.

Concernant les outils de monitoring, nous en avons utilisés plusieurs :

- Webmin nous a permis d'administrer et de monitorer notre service DNS.
- Squirrelmail nous a permis d'administrer et de tester notre service mail.