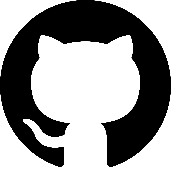
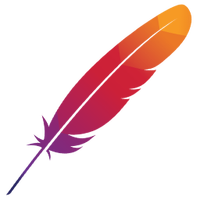


Rapport **technique**

Par :

PERSYN Loïc – ROSAR Nicolas – VANKEERBERGHEN Jordan

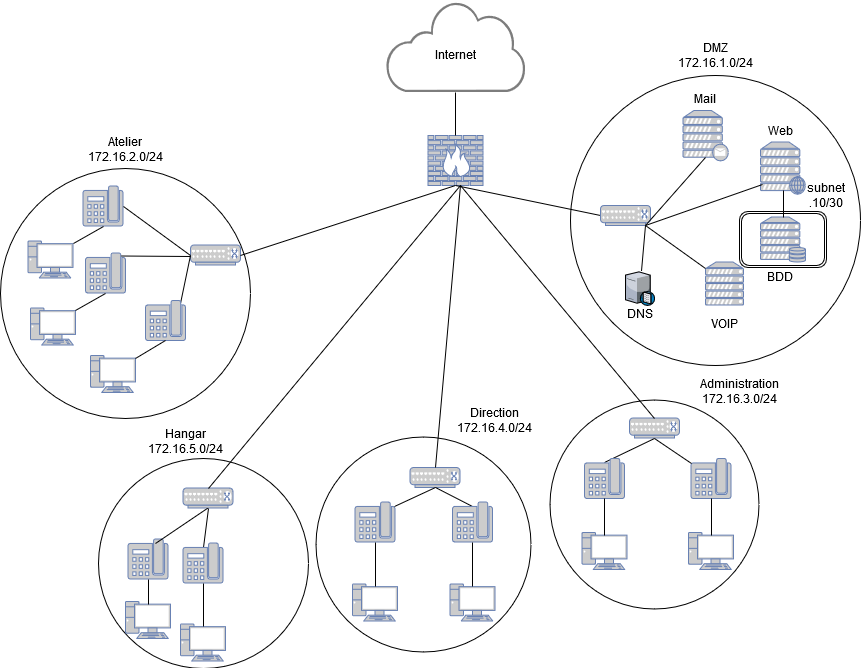




Date de remise : 11-05-2018

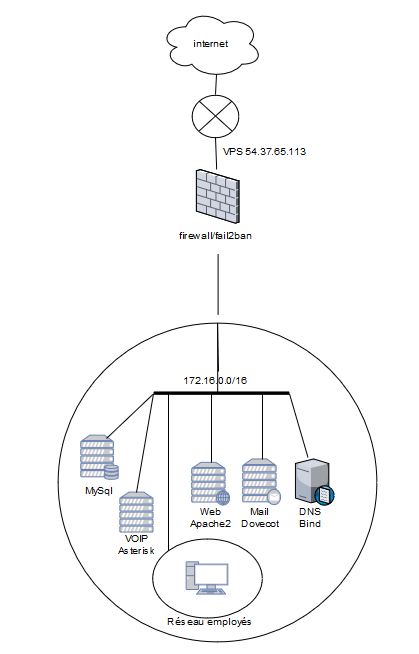
1. Schémas réseau

# Schéma logique



Notre implémentation est composée de 3 sites web placé sur le même VPS grâce à du virtual hosting. La base de données SQL qui ne communique qu’avec le site b2b est située dans le VPS avec les serveurs Web mais communiquent avec le site b2b via un sous-réseau à part des autres. Le serveur DNS renvoie vers le même VPS puisque nous n’en utilisons qu’un mais est forcément capable d’effectuer la résolution. Il possède le NS et, avec le glue record, toute demande faite à wt3.ephec-ti.be renverra sur ce serveur DNS qui, lui renverra vers le VPS.  
Au niveau VOIP il existe 4 zones différentes qui sont dans des sous-réseaux différents.

# Schéma physique



Dans notre VPS nous avons le site vitrine et b2b accessible via le DNS. Nous avons ensuite le site intranet accessible seulement par les employés. Nous avons les services mails Dovecot qui communiqueront via les port 143, 110 et 25. Dans ce VPS nous avons aussi le DNS qui redirige les requêtes en fonction de l’adresse demandée. Ensuite nous avons le site b2b avec la base de données qui communique via le réseau privé de Docker.  
Pour finir nous avons le serveur Asterisk qui gère les communications et qui renvoie les appels dans le réseaux employés à la personne concernée.

1. Problèmes rencontrés

# Symptômes

1. Problèmes de compréhension pour la mise en place du DNS.
2. Impossibilité de créer de nouveaux volumes. La commande de création fonctionne mais l’emplacement (trouvé avec volume *inspect*) dans lequel celui-ci est supposé se trouvé est vide.
3. Bannissement par Fail2Ban de notre propre VPS.
4. Impossibilité d’utiliser le PDO du service php dans apache.
5. Connexion à la base de données
6. Astérisk : connexion impossible au client X-Lite sans avoir ouvert l’invite de commande Astérisk.

# Causes

a) x

b) Oubli de la création du dossier ad-hoc.

c) Inconnues. Malgré la spécification de l’IP à ne pas bannir.

d) Utilisation d’une mauvaise version de php (7.0 a la place de 7.2)

e) Nécessité de fournir des droits supplémentaires à l’utilisateur

f) Une réinstallation a réglé ce problème.

Dans l’ensemble nous n’avons pas rencontrés énormément de problèmes. La plupart des « problèmes » s’est située dans la compréhension ; la compréhension de l’installation, la configuration et la communication avec tous ces différents services.  
Un autre problème qui a été très handicapant pour notre groupe fut l’impossibilité pour l’un des membres de configurer sa machine afin d’accéder facilement à son VPS.

1. Sécurité et mise en place

# VPS

Afin de garantir un maximum la sécurité de notre VPS, voici la procédure que nous avons suivi :

1. Nous avons créé un user personnel pour notre utilisation ainsi qu’un user *vvandens* pour le professeur ;
2. Utilisation de la cryptographie asymétrique pour l’authentification. Dépôt de chaque clé publique dans les VPS correspondants. Concrètement la clé publique *vvandens.pub* a été ajoutée au fichier *authorized\_keys* dans le VPS attribué à l’user *vvandens*. La même manipulation a été réalisée pour ajouter notre clé publique dans note compte VPS personnel. Cela dans le but d’authentifier le compte qui veut se connecter au VPS par une comparaison entre la clé privée de l’user et la clé publique présente sur le VPS
3. Suppression de l’accès SSH au compte root car il est le premier ciblé par les attaques du fait qu’il possède tous les droits d’administration sur le serveur en question ;
4. Installation de Fail2Ban afin de prévenir des intrusions dans notre VPS. *Fail2ban* lit les logs de divers services tels que SSH, Apache, FTP… à la recherche d’erreurs d'authentification répétées et ajoute une règle [bien](https://doc.ubuntu-fr.org/iptables) spécifique pour bannir l'adresse IP de la source.

Implémentation future et idéale :

* Installation de dnsec pour sécuriser le DNS
* Implémentation de SSL pour le protocole https
* Implémentation d’un anti spam
* Implémentation d’un firewall (UFW)

# Services

## 3.2.1 Web

## 3.2.2 MySql

## 3.3.3 DNS

## 3.3.4 Dovecot

## 3.3.5 Asterisk

1. Validation du déploiement

Nous allons utiliser la stratégie dite du « pilote ». Cela signifie que nous le mettrons en place seulement sur une zone géographique, pour notre unique. Grâce à cette méthode nous allons pouvoir valider et approuver l’ensemble des processus à mettre en place. Une fois que tout est validé, on peut lancer le déploiement pour plusieurs entités.

1. Monitoring

On pourrait mettre en place un MRTG (Multi Router Traffic Grapher) qui va nous permettre de récupérer des informations sur le trafic dans le réseau. Il utilise un protocole bien précis qu’est le SNMP pour interroger des équipements comme des routeurs, switchs ou serveurs.

Une autre solution serait d’utiliser les services de monitoring proposés par OVH. Ils vont vérifier l’état du serveur ainsi que le bon fonctionnement des applications de notre serveur.

L’utilisation de d’outil comme dnslookup ou mxlookup nous permettent de vérifier si nos services sont toujours actifs avec un certain degré dans le fonctionnement d’un service.

6.Risque de sécurité

* Le Spam : C’est un courrier indésirable, autrement dit une technique d’envoi de mails à but publicitaire ou frauduleux à des personnes qui ne l’ont pas demandé. Souvent envoyé de manière massive et parfois à multiples reprises, le spamming est tellement important qu’il peut très vite saturer votre communication ou votre boite mail.
* Le Phishing (hameçonnage) : Cette technique consiste à tromper les utilisateurs par le biais d'un courrier électronique semblant provenir d'une personne de confiance. Le mail propose de se connecter en ligne par le biais d'un [lien hypertexte](https://www.commentcamarche.com/contents/496-liens-hypertextes-et-ancres-html) et de compléter un formulaire factice. Via ce formulaire des personnes mal intentionnées peuvent récupère beaucoup d’informations sur une multitude de gens.
* Le Cache Poisoning : Si une personne mal intentionnée connaît une faille de sécurité sur l'un des serveurs DNS, il peut pirater le serveur afin de modifier l'adresse IP correspondant à un nom de domaine bien précis et de la remplacer par un lien menant vers un site malveillant.
* Les attaques DDoS (Distributed Deny Of Service) : Cette attaque vise à rendre un serveur, un service ou une infrastructure indisponible en surchargeant sa bande passante ou en accaparant ses ressources jusqu'à épuisement. Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément au serveur, ce qui le rend instable ou indisponible.