Projet Administration Réseau : Web et DNS

Fantuzzi Sébastien
Verschraegen Gauthier
Sanglier Joachim

2TL1
Groupe 9

Fantuzzi Sébastien
Verschraegen Gauthier
Sanglier Joachim

Rapport client (Web, DNS et Mail et VoIP)

Nous avons été joint par l'entreprise Woodytoys afin de lui offrir différents services au niveau de son architecture réseau. Vous trouverez donc ci-après l'approche que nous avons eu ainsi que le développement de ces différents services.

Cahier des charges :

L'entreprise a à disposition une connexion à Internet et un réseau WiFi, ainsi qu'une infrastructure téléphonique IP. Elle souhaite que nous mettions de nouveaux services à disposition de l'usine, ainsi que d'assurer la maintenance et le remplacement des serveurs pré-existants, tout en gardant une architecture réseau offrant un accès à internet.
Chaque département de l'entreprise doit pouvoir avoir accès à internet ainsi qu'un accès aux services internes et externes fournis par l'entreprise.
WoodyToys contient deux sites web accessibles par leurs clients ainsi que par leurs fournisseurs, en plus d'un outil ERP Web uniquement accessible sur leur réseau interne.
Chaque employé se voit mettre à disposition une boîte mail accessible à tout endroit. Certaines addresses plus globales sont également à définir.
Le réseau téléphonique doit rendre l'entreprise accessible via Internet depuis l'extérieur, ainsi que d'assurer la communication en interne entre les différents départements selon les règles suivantes ;

- Ouvriers : Un poste pour pour joindre les autres départements, et joignable par tout le monde
- Secrétaire : Un poste pouvant joindre et joignable par n'importe qui
- Comptables : Un seul numéro permettant de joindre plusieurs postes ainsi que d'un numéro par bureau pour joindre celui-ci uniquement. Ils peuvent joindre n'importe qui sauf le directeur
- Commerciaux : Joignable par n'importe qui et pouvant joindre tout le monde sauf le directeur
- Direction : Pouvant joindre tout le monde. Joignable directement uniquement via la secrétaire.

Enfin, une boîte vocale doit être à disposition de chaque poste.

Traduction des besoins :

Nous devons mettre en place différent serveurs. Concernant les services web, il faut deux serveurs distincts pour traiter d'une part les pages accessibles par l'extérieur, et d'autre part l'outil ERP seulement accessible par le réseau interne. il faudra également un service de consultation et de transfert de mail. Le service VoIP est également à configurer pour chaque poste, ainsi qu'un serveur dédié au service.
Afin de permettre la bonne utilisation des différents services mis à dispositions, deux serveurs de nom (interne et externe) permettront de répertorier les services mis en place. Un résolveur DNS sera ajouté en interne afin de permettre le bon fonctionnement du serveur de nom de cette zone.
Un pare-feu devra être ajouté afin de gérer les accès aux différents services ainsi que d'assurer la sécurité de ceux-ci et des utilisateurs.

Propositions de solutions techniques :

Les différents serveurs pouvant être utilisé par l'extérieur seront dans un sous-réseau à part. L'autre partie du réseau englobera donc tout le réseau interne accessible uniquement par les employés de l'usine. Nous installerons les différents services via un outil de conteneurisation.
Les services extérieur comprennent le serveur web contenant les 2 sites accessible au public et aux revendeurs, le serveur mail de transfert ainsi que le serveur de nom permettant de joindre les deux services précités.

En interne, nous retrouverons le serveur web interne permettant de joindre l'outil ERP, le serveur de consultation de mail ainsi que le serveur de noms permettant de joindre ces services.

Liste des services utilisés :

- Service de conteneur : Docker
- Service Web : Apache
- Service DNS : Bind9
- Transfert de mail : Dovecot
- Consultation de mail : Postfix
- VoIP : Asterisk

Choix et justification de la solution :

Une telle structure du réseau permet de n'exposer à l'extérieur (et donc à toute potentielle attaque) que les services nécessaires aux personnes extérieures. Nous limiterons les attaques vers ces services plus vulnérables via le pare-feu.

En ce qui concerne Apache, nous l'avons choisi plutôt que Nginx par exemple car il reste leader dans son domaine en plus d'être libre d'accès. Ses fonctionnalités sont très connues et appréciés, choses pour lesquelles nous avons choisi ce service.
Docker a été choisi parce qu'il est également très répandu, pour sa fonctionnalité de lien avec GitHub et qu'il est libre d'accès contrairement à Azure par exemple.
Bind9 et Asterisk n'ayant pas de réels concurrents, il paraît évident de les choisir eux.
Dovecot, Postfix et MySQL ont été choisi ensemble car ils forment un trio très répandu, pouvant directement fonctionner l'un avec l'autre et proposant les meilleurs services d'authentifications, de sécurité et de rapidité.

Etat des lieux

Les différents serveur web sont configurés et fonctionnels.
La résolution DNS en interne fonctionne. Les services DNS actuels permettent d'accéder à la résolution DNS en interne, au services web en interne et externe ainsi que les services mail. Les serveurs de noms seront encore modifiés au fur et à mesure de l'implémentation des différents services.
Les services liés au mail et à la téléphonie par voix IP fonctionnent.

Plan d'adressage VoIP :

Hangar :301

Atelier :302

Secrétaire : 401

Bureau comptable n°1 : 501

Bureau comptable n°2 : 502

Commerciaux : 601

Directeur : 701

La boîte vocale de chaque entité est disponible en composant son propre numéro.

Ajustements et maintenance

Il est possible pour les services web d'ajouter de nouvelles pages et/ou de modifier celles pré-existantes.
Pour les serveurs de noms des différentes zones, ils peuvent être modifier en fonction des services disponibles.
L'incorporation d'une nouvelle zone interne est implémentable via le résolveur DNS, ainsi que la modification des noms des sous-domaine existants.
L'ajout de nouveau utilisateur mail est faisable et simple à mettre en oeuvre.
L'ajout d'une ligne téléphonique est simple à mettre en oeuvre, et nécessite un poste téléphonique supplémentaire.
Chaque modification apportée nécessite un besoin de maintenance proportionnel à l'ampleur de la modification.

Fantuzzi Sébastien
Verschraegen Gauthier
Sanglier Joachim

Schémas réseaux

Schéma WoodyToys :

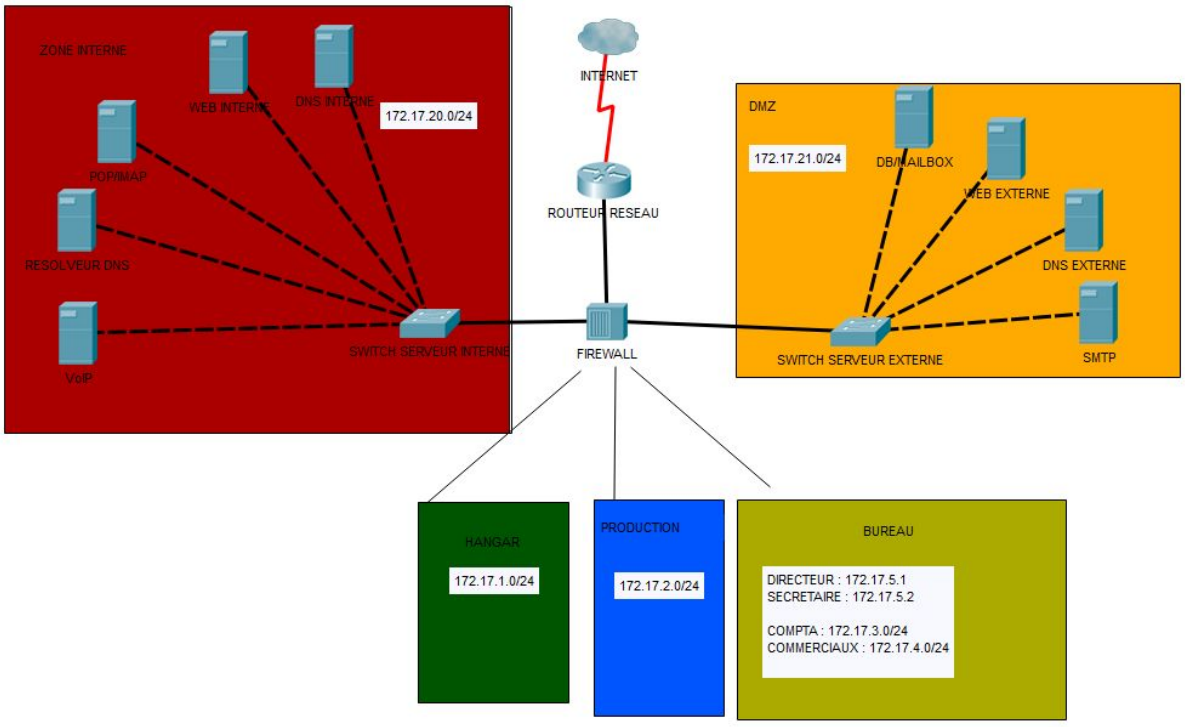
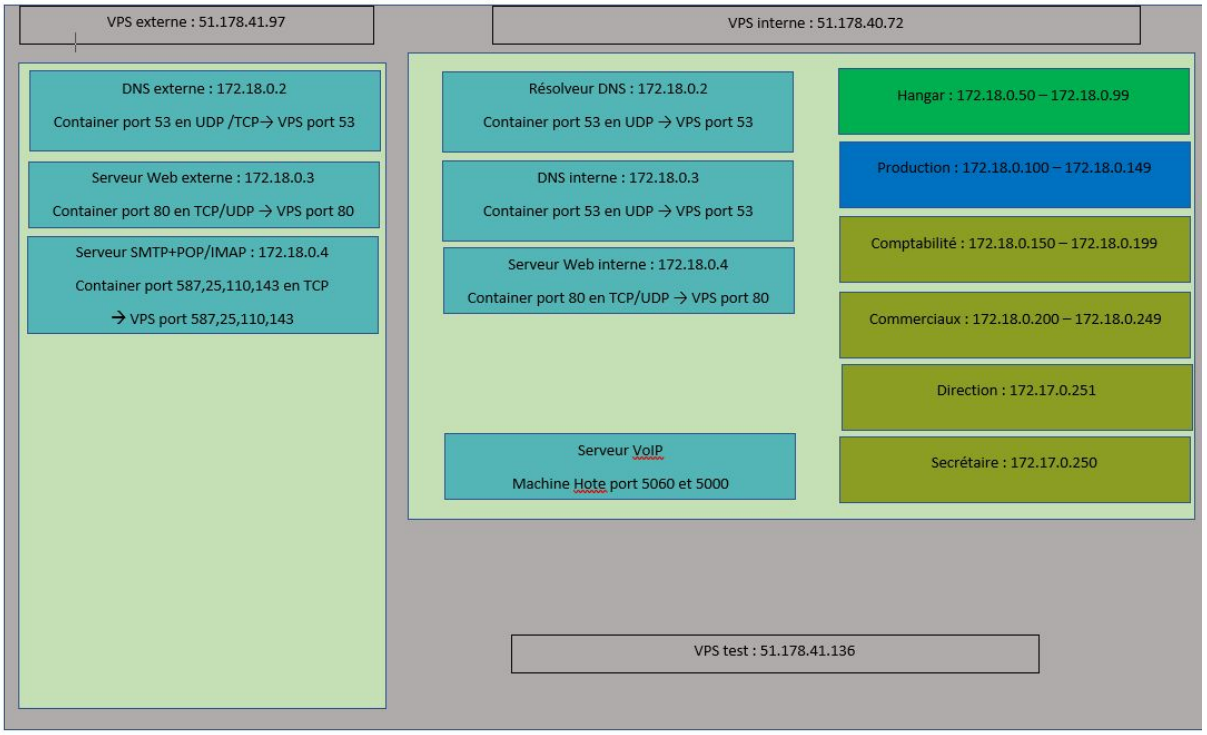


Schéma prototype :



Fantuzzi Sébastien
Verschraegen Gauthier
Sanglier Joachim

Rapport technique

Présentation du bilan du projet :

Nous sommes à la fin du projet. Nous avons atteint les objectifs que nous nous étions fixé avec notre équipe plus réduite. Tous les services demandés sont implémentés à l'exception de la base de données.

Etat d'avancement :

Tout les services ont été configuré à bien afin de suivre les besoins de l'entreprise.

Commentaire explicatif des schémas réseaux :

Schéma WoodyToys :

Nous avons répartis le réseau en 3 parties : le réseau externe (ou DMZ), le réseau interne et le réseau utilisateur. Le réseau externe contient toutes les machines ayant à subir des requêtes provenant de l'extérieur. Nous y avons donc placé le serveur DNS externe ainsi que le serveur de transfert de mail SMTP et le serveur web externe.
Vient ensuite le réseau interne, qui contient donc tous les serveurs n'ayant pas à subir des requêtes venant d'internet. Il est constitué du serveur Web interne,du résolveur DNS, du serveur DNS interne et du serveur de consultation POP/IMAP.
Enfin, le réseau utilisateur représente l'ensemble des périphériques utilisés pour garantir une connectivité vers internet et les différents serveurs mis à disposition. Nous allons créer un VLAN par service, à savoir les ouvriers, les comptables, les commerciaux et la production. La direction et la secrétaire constitueront un VLAN à eux-deux. Ceci permettra d'identifier les utilisateurs sur le réseau et d'appliquer des règles de sécurité en fonction de l'identité de l'utilisateur.

Schéma prototype :

Nous utiliserons majoritairement deux VPS pour simuler le réseau externe et le réseau interne (ce dernier incluant les utilisateurs et les serveurs internes). Quelques différences sont à noter par rapport à l'autre schéma. Tout d'abord, les IP assignées aux serveurs. *En effet, là ou sur le schéma Woodytoys nous avons bien utiliser deux sous-réseaux différents, nous avons utilisé un même réseau Docker 172.18.0.0/24 par soucis de facilité du fait que ces serveurs ne soient pas physiquement sur le même hôte. Nous avons également dû rassembler le réseau utilisateur dans ce sous-réseau car les réseaux Docker ne permettent pas de communiquer entre-eux*. Nous avons également dû unir le serveur POP/IMAP et SMTP, étant donné que ce premier service nécessite un accès direct aux fichiers du second.

Difficultés rencontrées :

Nous avons rencontré bon nombre de difficultés lors de l'installations des serveurs web et DNS. La plupart de ces difficultés sont survenues pendant l'installation de Bind9. En effet, il nous a fallu de longs moments de réflexions pour démarrer l'image docker. Ces erreurs sont survenues lors de l'exécution de l'image docker, plus particulièrement celle de Bind, la commande étant longue et complexe. Les soucis de connexion au VPS ainsi que de ports ont également rendu notre tâche plus ardue. *L'application d'Asterisk ainsi que du service mail sous Docker fut également problématique, au même titre que la communication entre différents réseaux Docker nous ayant au final contraint à n'en utiliser qu'un seule*

Méthodologie

N'ayant découvert que tardivement la réelle utilité du lien entre GitHub et DockerHub, nous n'avons dans un premier temps pas usé de cette fonctionnalité et sommes simplement passé par des docker push et pull afin de publier et récupérer nos images "pré-construites" sur nos machines personnelles. Une fois amenée sur nos VPS, nous avons alors docker run nos différents images dans différents conteneurs.
Le serveur Apache a été validé comme fonctionnel une fois qu'une commande curl sur lui-même rendait bien la page pré-conçue d'Apache, tandis que la résolution DNS fut validée lorsqu'une commande dig via le conteneur en question affichait des résultats cohérents au site passé en paramètre.
Il est possible de surveiller le fonctionnement des deux services nommés ci-dessus via les logs disponibles pour chacun de ces services.
Le serveur mail a été validé une fois que la réception et l'envoie d'émail était fonctionne avec n'importe quel client mail.
La téléphonie sous IP à été validée une fois que différents appels furent effectués entre différents postes.

Analyse de la sécurité

La sécurité est un point important d'un réseau tel que celui demandé dans ce projet. En effet, il est nécessaire de mettre en place une zone démilitarisée (DMZ) accessible via un firewall. Cette zone nous permettra d'y placer nos serveurs public et ainsi éviter toute entrée intrusive dans notre réseau privé.
Les VPS ont été sécurisé via une authentification exclusivement par clé, dont nous sommes les seuls propriétaires. De plus, l'authentification par l'utilisateur "root" a été désactivée.
Les VPS disposent d'une protection contre les attaques en sshd grâce à fail2ban.

Fantuzzi Sébastien
Verschraegen Gauthier
Sanglier Joachim

Analyse des feedbacks.

Pour ce dernier rapport, nous avons reçu un retour relativement positif sur notre travail. En effet, tout était bien noté là ou nous avions travaillé, et mauvais là où ne l'avions pas. Nous n'avons pas donc eu de réel application du feedback de la correction croisée.