Rapport client

Groupe 7
Foureau Emmanuel, Crompton Glenn, Hassaine Celia

1. Cahier des charges :
    a. Demande du client

Le client est une entreprise de jouet nommé WoodyToys. Cette société nous demande de mettre en place une infrastructure réseau couvrant plusieurs services.

Tout d'abord, nous devons assurer le services web qui hébergera les trois sites fournis par l'entreprise : un site statique pour la vitrine (www.woodytoys.be), un site dynamique pour l'ERP et le site de vente en ligne (b2b.woodytoys.be). Ce service utilisera le nom de domaine "wt7.ephec-ti.be". De plus, il nous demande de mettre en place un intranet auquel seulement les employés de l'entreprise peuvent accéder. Ces employés doit donc avoir accès à l'intranet et à l'internet. *Ce réseau interne s'étend plus loin que le service web. Il concerne également le service mail et voip. Nous devons pouvoir assurer des échanges sécurisés. Un service de résolution des noms est disponible pour les employés de l'entreprise et seulement pour ces employés.*

Nous devons également mettre en place un service de mail permettant aux employés de s'envoyer des mails grâce à des adresses créées au préalable pour chacun d'eux. Nous devons également implémenter un service mail qui redirige soit vers la secrétaire soit vers les commerciaux.

De plus, nous devons mettre en place un serveur DNS qui s'occupera de donner l'accès au site de l'entreprise. Il dirigera les recherches vers notre site lorsque les utilisateurs auront la permission d'y accéder. De plus, il s'occupera des requêtes interne vers l'extérieur.

Au niveau du VoIP, il nous est demandé de créer un service qui va permettre aux employés de s'appeler entre eux grâce à des numéros qu'on leur attribue avec des redirections en fonction de leur hiérarchie (ex: Si un employé veut appeler le directeur, l'appel sera redirigé vers la secrétaire.).

    b. Point de vue technique

Plus concrètement, nous devons mettre en place une architecture web qui met en place les services suivants :
- Web: Nous utilisons Apache. *Il utilisera une configuration pour un site www, une pour un site b2b et une dernière pour un site intranet. Ces trois sites seront en php. le site intranet* ***intranet.wt7.ephec-ti.be*** *doit être accessible depuis un poste employé et seulement dans ce cas-là. Le site b2b*

b2b.wt7.ephec-ti.be *et le site global www.wt7.ephec-ti.be doivent quant à eux être joignable par tout le monde. Le site b2b possède une connexion sécurisée à la base de données (en utilisant mysql) car c'est à cet endroit que les ventes se feront. Ce site doit donc être dynamique; il pourra effectuer des ajouts dans la base de données.*

- DNS / SOA / résolution: Bind9. *Ce service exigera un nom de domaine.*
- Un service mail fonctionnel pouvant envoyer et recevoir sans difficulté. *Nous utiliserons postfix pour le protocol SMTP et dovecot pour le protocol IMAP et POP3.*
- Un service VoIP permettant aux différentes personnes de l'entreprise de communiquer entre elles.

2. Choix d'implémentation :

a. Serveur Web

Afin de pouvoir accéder aux 3 pages web demandées, nous avions premièrement besoin d'un serveur web. Nous avons choisi d'utiliser le serveur web Apache, car c'est le web server le plus répandu sur les machines Linux, et le deuxième plus répandu, tous systèmes d'exploitation confondus. Le serveur web Apache ayant été le serveur le plus populaire depuis 1996, celui-ci dispose d'une documentation très complète. Sa popularité n'est bien sûr pas le seul élément ayant contribué à notre choix, car, en effet, Apache perd en popularité, contrairement à son concurrent, Nginx. Ce qui nous a fait décider d'utiliser Apache est tout simplement son support interne natif pour les contenus dynamiques, contrairement à Nginx qui nécessite une intervention extérieure. Ce support natif rend la configuration plus simple à déployer. C'est pourquoi nous avons utilisé ce logiciel et pas NGIN.

Programme utilisé : **Apache**

b. Serveur DNS

Pour accéder aux 3 pages web demandées, nous avions aussi besoin d'un résolveur DNS. Cela permet de pouvoir visiter les pages web via leur nom de domaine et pas l'adresse IP du serveur sur lequel elles se trouvent. Nous utilisons ici BIND, qui est le serveur DNS le plus utilisé sur internet.
BIND est destiné à être totalement conforme aux normes DNS et aux projets d'IETF. Il supporte nsupdate, IPv6. Il prend en charge plusieurs processus et limite le taux de réponses (RRL).
Au niveau de la sécurité, les auteurs officiels du logiciel (Internet Systems Consortium) tiennent à jour une liste complète des problèmes de sécurité découverts et révélés par BIND9.
Une partie des alternatives à BIND9: Unbound (résolveur DNS validant, récursif et mettant en cache), PowerDNS (fonctionne sur la plupart des dérivés Unix), dnsmasq (serveur DHCP léger et facile à configurer) et djbdns (collection d'outils de système de noms de domaine).

Programme utilisé : **Bind**

c. Serveur de base de données

Pour le site d'e-commerce, nous avions aussi besoin d'une base de données, afin de pouvoir enregistrer l'ensemble des produits. En décidant de mettre notre base de données sur un serveur local, nous avons un contrôle intégral dessus. Nous avons choisi d'utiliser un serveur MySQL.
En effet, MySQL est le serveur de base de données le plus populaire, ce qui implique que nous disposons d'une grande documentation à son sujet (beaucoup d'informations sur son téléchargement, par exemple) et de nombreux forums répondent à de multiples problèmes auxquels les utilisateurs font face. De plus, étant le plus utilisé, on y consacre plus de temps et d'effort dans son évolution permanente.

Programme utilisé : **MySQL**

d. Service mail

Pour le serveur mail, nous avions besoin de mettre en place plusieurs services permettant d'envoyer des emails et de récupérer ceux reçus dans une boîte de messagerie.

Toute l'entreprise peut envoyer des mails en interne ou externe. Des adresses emails ont déjà été créés comme:

- *contact@wt7.ephec-ti.be*
- *directeur@wt7.ephec-ti.be*
- *atelier@wt7.ephec-ti.be*
- *secretaire@wt7.ephec-ti.be*

Les boîtes de messagerie sont aussi accessibles depuis l'"extérieur.
La sécurité est fonctionnelle et les communications sont cryptés grâce à une extension de protocol appelé StartTLS.

Programmes utilisés: Docker, postfix et dovecot

e. Service VOIP

Pour le serveur VOIP, nous avions besoin d'un réseau de téléphones qui pouvaient tous s'appeler les uns avec les autres mais en suivant certaines règles (Rouge = pas implémenté):

- *Nous avons un plan d'adressage de téléphonie ip.*
- *L'entreprise doit être accessible en VoIP depuis internet pour les clients (adresse de contact : contact@woodytoys.be) et les appels doivent aboutir chez la secrétaire.*
- *Les employés doivent pouvoir communiquer entre eux à l'intérieur de l'entreprise mais également depuis l'extérieur.*

Les ouvriers disposent d'un poste de téléphonie ip dans le hangar et dans l'atelier pour joindre les autres départements internes.
La secrétaire peut contacter n'importe qui.

Le service comptable dispose d'un numéro unique permettant de joindre le premier comptable disponible ainsi qu'un numéro spécifique pour chaque bureau.
Les comptables peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur.
Les commerciaux peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur. Et disposent aussi d'un numéro unique qui permet de joindre le premier commercial disponible.

La direction dispose d'un numéro et peut joindre tout le monde (interne comme externe). Ce numéro ne peut être joint directement, les appels sont redirigés vers la secrétaire qui peut alors transférer les appels vers la direction.

- *Tous les employés disposent d'une boîte voicemail.*
- *Possibilité de communiquer avec le serveur de téléphonie ip d'une entreprise qui aurait fusionné avec Woodytoys*

Programme utilisé: ***Asterisk***

3. Maintenance :

a. Web et DNS

Définir des zones publiques et privées serait bien utile d'un point de vue sécurité. On peut ainsi y entreposer des informations qui ne sont pas destinées au public et y cacher des dossiers personnels.
De plus, l'accès aux sites doit se faire de manière sécurisée en utilisant des certificats HTTPS gratuits via Certbot. De nouveau, en matière de sécurité, des reverse proxy pourraient se montrer efficaces pour éviter les attaques directes envers le réseau interne

Pour vérifier le trafic sur notre DNS, un outil bien pratique à installer s'offre à nous: dnstop. Il offre diverses tables du trafic. la simple commande "sudo dnstop NomInterface" permet de surveiller le trafic sur cette interface. Evidemment, une série d'options est disponible. Par exemple, l'option -l 2 permet de conserver 2 tables: une avec des noms de domains de premier niveau et une autre avec des noms de domaine de second niveau. La liste des options est bien longue donc je vous invite à consulter la page manuel de cet outil.

Pour ajouter un site, il suffit d'ajouter sa configuration dans /etc/apache2/sites-available et ensuite, dans ce fichier, exécuter la commande sudo a2ensite nomDuFichier. La suppression d'un site se fait au même endroit mais avec la commande sudo a2dissite nomDuFichier.

Ajouter une adresse IP dans les privilégiés de l'intranet, Il suffit d'ajouter l'adresse IP dans l'access list situé dans le fichier /etc/bind/named.conf.local.

Le certificat SSL devrait se remettre à jour automatiquement mais si cela n'est pas le cas, la commande sudo certbot --apache crée un certificat et le met en application.

b. Mail

Pour effectuer des modifications sur les utilisateurs, un fichier du serveur mail est là pour ça (/etc/docker/MX/setup.sh). Il y a plusieurs commandes pour la gestion des utilisateurs

Dans le fichier ci dessus (/MX) on peut effectuer :

- *Un ajout d'utilisateur*
- *Une suppression d'utilisateur*
- *Lister les utilisateurs*

c. VoIP

Pour effectuer des modifications au niveau de asterisk (ajouter des utilisateurs ou des extensions...) il sera nécessaire de changer quelques fichiers:

-sip.conf
-extensions.conf
-users.conf

Je ne conseille donc pas de se lancer là dedans sans avoir quelques connaissances en VOIP.

Rapport sur le déploiement :

d. Avancement

Au niveau du web, tous les sites sont créés mais ni le b2b ni l'intranet ne sont liés à une base de données. Le DNS est fonctionnel et possède un intranet qui n'ouvre l'accès au site intranet qu'aux ip's autorisées.

Au niveau du mail, les services mails sont fonctionnelles. On peut envoyer des mails à l'intérieur et l'extérieur de l'entreprise. On peut aussi vérifier ses emails dans une mailbox externe.

Au niveau de VOIP, tous les SIP Peers (aussi connu sous téléphones) sont up et fonctionnent. Les appels se font comme noté sur le plan d'adressage, mais il n'est pas lié à un SIP externe et donc ne peut pas recevoir des appels de l'extérieur, nous avons quand même simulé un utilisateur externe, qui quand il appelle aboutit toujours sur la secrétaire.