WoodyToys - Rapport client

EPHEC - Groupe 13

Melvin Campos Casares, Guillaume Vanden Herrewegen,
Hubert Van De Walle

6 juin 2019

Rapport client

1. Responsables

- **Partie DNS & Web :** Melvin Campos Casares
- **Partie Mail :** Guillaume Vanden Herrewegen
- **Partie VoIP :** Hubert Van De Walle

2. Cahier des charges

Dans le cadre de la mise en place de l'infrastructure réseau de l'entreprise WoodyToys, plusieurs aspects doivent être tenus en compte et seront expliquées ci-dessous.

2.1. Services internes

Il est demandé d'offrir l'accès Internet sur les postes de travail fixes et mobiles des employés tout comme l'accès aux différents services internes (comme l'ERP) sans se reposer sur le fournisseur d'accès ni les fournisseurs extérieurs. Concrètement, il nous est demandé d'utiliser notre propre DNS afin de ne pas dépendre du fournisseur d'accès ou fournisseur extérieur afin d'accéder à Internet et aux différents services internes (comme l'ERP).

Un contrôle de trafic Web généré par les employés est une préférence.

Il y a un certain intérêt pour la gestion des identités des employés pour l'utilisation des services internes même si pas obligatoire.

2.2. Web

La vente des produits s'effectue avec les revendeurs via une plateforme accessible en ligne, expliqué un peu plus loin.

La gestion des contacts clients, commandes, stocks et l'organisation de la production est basée sur un outil ERP web accessible uniquement en interne. Il s'agit donc d'un Intranet, accessible *uniquement* dans l'enceinte du réseau de l'entreprise.

La différence entre le site internet pour les revendeurs et l'outil ERP est que l'outil ERP n'est disponible qu'en interne et uniquement que par les employés de l'entreprise WoodyToys alors que le site pour les revendeurs est accessible publiquement et ne donne accès qu'à un catalogue et un moyen de commande. L'outil ERP permet donc de voir, faire et gérer bien plus de choses que le site pour les revendeurs.

Un portail Web présentant les produits (www.woodytoys.be) et un site de vente en ligne réservé aux revendeurs (b2b.woodytoys.be) sont disponibles publiquement.

Le code source des 3 sites est préexistant :

- Le site vitrine est un site statique en HTML/CSS,
- Le site de vente en ligne pour les revendeurs (b2b) et l'ERP (intranet) sont des sites dynamiques en PHP/MySQL.

2.3. Mail

Une adresse mail est fournie à chaque employé et respectant le format suivant : `nom.prenom@woodytoys.be`.

Il y a également présence d'adresses mails générique :

- contact@woodytoys.be, redirigée vers la secrétaire,
- b2b@woodytoys.be, redirigée vers les commerciaux.

Toutes les adresses mails doivent être consultables à l'aide d'un client mail classique depuis l'entreprise et la réception/envoi des mails doit être possible n'importe où (au bureau, en déplacement ou à domicile).

2.4. Téléphonie IP

L'entreprise doit être accessible en VoIP depuis Internet afin que les clients puissent être en relation avec l'entreprise. Les appels aboutissent sur le poste de la secrétaire. L'adresse de contact est : contact@woodytoys.be.

Les employés de l'entreprise doivent pouvoir communiquer entre eux tant au bureau qu'en déplacement.

Les communications identifiées sont les suivantes :

- ***Ouvriers :*** un poste de téléphonie IP dans l'atelier et dans le hangar pour joindre les autres départements internes.
- ***Secrétaire :*** dispose d'un PC sur lequel se trouve un softphone permettant de contacter n'importe qui.
- ***Service comptabilité :*** numéro unique permettant de joindre le premier comptable disponible et un numéro spécifique par bureau (le service est réparti en 2 bureaux). Ils peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur.

- ***Commerciaux :*** réunis dans un bureau, ils peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur. Ils disposent de smartphones avec lesquels ils peuvent téléphoner en déplacement.
- ***Direction :*** il dispose d'un numéro qui peut joindre n'importe quel poste en interne et l'extérieur. Il ne peut être joint directement (les appels transitent d'abord auprès de la secrétaire).

Tous les employés disposeront d'une boite vocale.

Une fusion est à prévoir entre deux réseaux téléphoniques, ce qui signifie qu'il faut minimiser les changements et les deux serveurs de téléphonie doivent être configurés pour que les deux sites puissent se contacter entre elles.

La visio-conférence, l'utilisation de téléphones ou passerelles SIP vers la téléphonie classique sont des petits plus éventuellement envisageables.

2.5. Fichiers de l'entreprise (Bonus)

Un système de fichiers partagés est à prévoir.

- Chaque employé doit pouvoir disposer de son répertoire personnel, tout comme le directeur et la secrétaire.
- Chaque groupe d'employés disposeront d'un répertoire commun.
- Les employés doivent pouvoir accéder aux fichiers partagés via l'explorateur de fichiers de leur ordinateur.
- Un système de backup facile doit être prévu.
- Les employés doivent pouvoir y accéder même en déplacement (PC portable, smartphones, tablettes).

3. Traduction des besoins du client en langage informatique

Au vu des besoins du client, ce projet sera divisé en plusieurs parties :

- Le client demande à intégrer un DNS (un ou plusieurs serveurs) avec la gestion des noms de domaines ainsi que des zones.
- Il est demandé de mettre en place 3 sites web avec une intégration d'une base de données :
  - Un premier site web statique pour présenter l'entreprise,
  - Deux autres sites, dynamique tous deux, pour la partie vente en ligne pour les revendeurs ainsi que l'ERP.

- La création d'un serveur mail permettant la gestion des envois et réception, une consultation via client mail et ce, de n'importe où.
  - Ce serveur mail doit héberger le nom de domaine de l'entreprise et notamment gérer les éventuelles redirections.
  - Il stockera les mails envoyés et reçus.
- La mise en place d'un système de téléphonie sur IP (Voice-Over IP) :
  - Une série de compte est à créer ainsi que des spécifications précises concernant la prise de contact avec la direction à rediriger vers le secrétariat lorsque le service comptabilité et les commerciaux veulent joindre le directeur.

3.1. DNS et accès web interne

Un service DNS interne et externe est en cours de finalisation. Ce service est développé sur `Bind9` et devrais être achevé dans les prochains jours.

Même si `Bind9` existe depuis un certain temps et que d'autres alternatives plus récentes et, par conséquent, plus performantes existent, il reste très largement utilisé. De plus, de par sa popularité, il profite encore aujourd'hui de nombreuses mises à jour de sécurité ainsi que d'une documentation variée et complète.

3.2. Web

Le déploiement et la configuration des services nécessaires pour l'hébergement est en cours de développement.

Nous avons choisi `lighttpd` pour les performances qu'il offre en comparaison d'`apache` et `nginx`. `Lighttpd` est un serveur web sécurisé, rapide et flexible qui a été optimisé pour des environnements à hautes performance. Il a une très faible empreinte mémoire en comparaison d'autres serveurs web et gère de manière effective la charge du processeur.

En pratique, nous avons constaté une utilisation processeur de 0% et de mémoire de 0,1% sur nos serveurs lorsqu'il n'y avait pas de trafic web.

Les sites sont accessibles en ligne sur notre plateforme de test `51.77.203.41` aux adresses suivantes :

- www.wt13.ephec-ti.be
- b2b.wt13.ephec-ti.be
- intranet.wt13.ephec-ti.be

3.2.1. Certificat SSL

Afin de protéger au mieux les sites internet, un certificat menant au protocole HTTPS est à intégrer.

Pour ce faire, `Let's Encrypt` est notre choix retenu étant donné que les certificats auto-signés sont difficile à renouveler aisément.

`Let's Encrypt` est une autorité de certification gratuite, automatisée, et fourni par le Internet Security Research Group (ISRG). Les principes clés de Let's Encrypt sont :

- Gratuit : toute personne possédant un nom de domaine peut utiliser Let's Encrypt pour obtenir un certificat de confiance, sans frais,
- Automatique : sa configuration et son renouvellement automatique est aisé puisqu'il est compatible avec la plupart des logiciels exécutés sur un serveur web,
- Sécurisé : Let's Encrypt sert également de plate-forme pour faire progresser les meilleures pratiques de sécurité TLS, du côté des autorités de certification et du côté des opérateurs de sites en les aidant à sécuriser correctement leurs serveurs,
- Transparent : tous les certificats délivrés ou révoqués sont enregistrés publiquement et mis à disposition de toute personne souhaitant les inspecter,
- Ouvert : le protocole d'émission et de renouvellement automatique sera publié en tant que norme ouverte que d'autres peuvent adopter.
- Coopérative : à l'instar des protocoles Internet sous-jacents eux-mêmes, Let's Encrypt est un effort commun visant à bénéficier à la communauté, au-delà du contrôle de toute organisation.

3.3. Mail

Concernant la partie mail, nous utilisons `Postfix`, étant donné qu'il s'agit du système de server mail répandu et bien connu de tous.

`Postfix` n'est certes pas des plus récents mais on profite, tout comme pour Bind9, d'une documentation complète.

3.4. VoIP

Nous utilisons `Asterisk` comme moyen de communication en Voice over IP. Il est fort répandu mais nous profitons d'une documentation minimale. Heureusement, de nombreux utilisateurs proposent du contenu pour mieux comprendre son utilisation.

D'autres systèmes ont retenu notre attention comme *Dimelo (a RingCentral Company)* ou *Skype Connect* qui malheureusement sont payant et ne correspondent pas totalement à ce que nous recherchons. Dans le cadre de *Skype Connect*, il s'agit d'un système PBX SIP proposé pour les professionnels

avec système de location de canaux et est basé sur le Cloud PBX, ce que nous ne cherchons pas à avoir. *Dimelo* semble être dans le même principe même s'il propose.

4. Solutions techniques

4.1. Comparatifs des alternatives possible

4.1.1. DNS et accès web interne

Nom	Système d'exploitation supporté	Configuration	Documentation	Popularité
Bind	Linux, Windows, macOS, BSD	Aisée	Complète	Très importante
dnsmasq	Linux, Android, BSD, macOS	Aisée	Importante	Importante
Unbound	Linux, Windows, macOS, BSD	Aisée	Très complète	Importante

4.1.2. Web

Apache_ fournit une variété de modules MPM (MultiProcessing Modules) qui lui permet de s'exécuter en mode process-based, hybride (processus et thread) ou hybride évènementiel. Apache est conçu pour réduire les temps de latence tout en augmentant le débit par rapport au traitement d'un grand nombre de demandes (garantie d'un traitement cohérent et fiable des demandes dans un délai raisonnable. Il s'agirait du serveur web (tout confondu) le plus utilisé dans le monde.

Microsoft IIS *(Internet Information Services)* est un serveur web extensible utilisé sur les systèmes Windows NT. Sur des Workstation Windows, IIS ne supporte que 10 connexions TCP/IP en simultané contrairement sur les serveurs Windows ou le nombre est illimité. Il s'agirait du deuxième serveur web (tout confondu) le plus utilisé dans le monde.

Lighttpd est optimisé pour des environnements où la rapidité est le plus important tout en restant conforme aux normes, sécurisé et flexible.

Nginx s'agit d'un serveur web, reverse proxy, load balancer, proxy mail et cache HTTP. Nginx utilise une approche événementielle asynchrone au lieu de threads afin de traiter les requêtes et fournir des performances plus prévisibles sous des charges élevées. Il s'agirait du deuxième serveur web open source et du troisième serveur web (tout confondu) le plus utilisé dans le monde.

Nom	Gratuit d'utilisation	Open Source	OS supporté	Configuratio
Apache	Oui	Oui, *Apache License 2.0*	Tous	Aisée
Microsoft IIS	Oui	Non, *Shareware / Windows NT*	Windows	Complexe
Lighttpd	Oui	Oui, *BSD License 2.0*	Windows, Linux, macOS, BSD	Très aisée
Nginx	Oui	Oui, *FreeBSD License*	Windows*, Linux, macOS, BSD	Aisée

Le support des systèmes d'exploitation concernant : Windows, Linux, macOS, BSD, etc.

*Nginx: support de Windows via Cygwin.

4.1.2.1. Certificats SSL

- **Autorité de certification commerciale :**
  - Processus: Manuel
  - Coût : Entre 10$ et 1000$
  - Validation : DV, OV, EV
  - Confiance : Approuvé par défaut
  - Certificat générique : Oui
  - Certificat uniquement IP : Certains pour adresses IP publiques
  - Période de validité : 1 à 3 ans
- **Let's Encrypt :**
  - Processus : Automatique
  - Coût : Gratuit
  - Validation : DV
  - Confiance : Approuvé par défaut
  - Certificat générique : Oui
  - Certificat uniquement IP : Non
  - Période de validité : 90 jours
- **Certificat auto-signé :**
  - Processus : Manuelle (création de certificat uniquement)
  - Coût : Gratuit
  - Validation : DV, OV
  - Confiance : Aucun par défaut, doit être manuellement marqué comme de confiance (aucun AC commun impliqué)

  - Certificat générique : Oui
  - Certificat uniquement IP : Oui, toute propriété intellectuelle
  - Période de validité : n'importe lequel

- **Autorité de certification privé :**

  - Processus : Manuel
  - Coût : Gratuit
  - Validation : DV, OV
  - Confiance : Aucun par défaut, distribution manuelle
  - Certificat générique : Oui
  - Certificat uniquement IP : Oui, toute propriété intellectuelle
  - Période de validité : N'importe lequel

- CA : Autorité de Certification
- DV : Domaine de Validation
- OV : Validation de l'organisation
- EV : Validation étendue

4.1.3. Mail

Nom	Niveau de sécurité	Niveau de performance	Année de création	Communauté
Exim	Assez bon	Très bon	1995	Large
Postfix	Bon	Excellent	1997	Taille moyenne
Sendmail	Moyen	Ok	1982	Large

4.1.4. VoIP

Nom	Gratuit d'utilisation	Open Source	support vidéo	IM/Chat	WebRTC
Asterisk	Oui	Oui	Oui	Oui	Oui
Dimelo	Non	Oui, commercial	Live Chat*	Oui	Non
Skype Connect	Non	Non, commercial	Oui	Oui	Oui
OpenPBX	Oui (*Advanced* payant)	Oui	Non	Non	Non
FreePBX	Oui	Oui	Oui	Oui	Oui

Nom	Gratuit d'utilisation	Open Source	support vidéo	IM/Chat	WebRTC
OpenSIPs	Oui	Oui	Oui	Oui	Non

*Live Chat : système de streaming

4.2. Choix et justification de la solution

Nos choix se sont reposés sur :

- **DNS : Bind9**
- **Web : Lighttpd**
  - **Certificat : Let's Encrypt**
- **Mail : Postfix**
- **VoIP : Asterisk**

Lighttpd a été retenu étant donné qu'il est pensé pour la rapidité, fonctionne sur des systèmes avec peu de mémoire vive, tient compte de la charge du processeur, apporte une bonne sécurisation et flexibilité.

Let's Encrypt pour les certificats SSL menant au protocole HTTPS pour sa configuration aisée, son renouvellement automatisé et surtout qu'il s'agit d'un certificat de confiance et réputé.

Bind9 et Postfix ont été choisis pour leur documentation conséquente et popularité.

Asterisk, quant à lui, est fort répandu, mais sa documentation est minimaliste et ne comprend que sa configuration de base ainsi qu'une liste sommaire de toutes ses fonctions et fichier de configuration. Heureusement, de nombreux utilisateurs proposent du contenu pour mieux comprendre son utilisation. De nombreux modules compatibles avec ce dernier sont également disponibles en ligne.

Si besoin, nous pouvons créer de nouveaux utilisateurs tant au niveau des mails qu'au niveau du Voice-Over IP. Pour ce faire, il suffit simplement de nous contacter et nous intégrerons les nouvelles informations.

Toute mise à jour du site internet peut également se faire aisément sur simple demande. La base de données peut être mise à jour à distance directement par vous et nous vous donnerons les informations de connexion pour cela.

5. Besoins en maintenance

Comme dans tout bon système administré, il est nécessaire de vérifier de façon régulière les logs générés par nos différents serveurs déployé. Les logs sont considérés comme étant la boîte noire des services dans laquelle tout évènement est enregistré.

Pour ce faire, nous conviendront d'un moment pour effectuer les vérifications de façon régulière sans perturber l'entreprise.

5.1. Web

Un suivi au niveau du certificat est nécessaire afin de réaliser le renouvellement de Let's Encrypt.

6. Déploiement

Serveur	Composants	Etat
DNS	Bind9	Lancé
Web	Lighttpd, PHP, HTTPS	Lancé
DB	MariaDB	Lancé
Mail	Postfix	Lancé
VoIP	Asterisk	Lancé